CHAPTER 14

AAA サーバとローカル データベースの設定

この章では、Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）（[トリプル A］と発音）のサポートと、AAA サーバおよびローカル データベースを設定する方法について説明します。

この章で説明する内容は、次のとおりです。

AAA の概要

AAA により、FWSM はユーザの識別（認証）、ユーザが実行できる作業（許可）、ユーザが実行した作業（アカウンティング）を判別できます。

AAA は、アクセス リストだけを使用する場合よりも、ユーザ アクセスに関する保護および制御をさらに強化します。たとえば、すべての外部ユーザに対して、内部インターフェイス上のサーバへの Telnet アクセスを許可するアクセス リストを作成できますが、サーバへのアクセスを一部のユーザだけに限定する場合で、対象ユーザの IP アドレスが必ずしも明らかでないときには、AAA をイネーブルにして、認証または許可されたユーザだけに FWSM を通過させることができます（Telnet サーバは認証を実行しますが、FWSM は不正ユーザによるサーバへのアクセス試行を防止します）。

認証は単独で使用することも、許可およびアカウンティングと併用することもできます。許可を適用するには、最初にユーザを認証する必要があります。アカウンティングは単独で使用することも、認証および許可と併用することもできます。

複数のセキュリティ コンテキストを使用する場合、コンテキスト単位で別々に AAA を設定できますが、コンテキストの間で共有することはできません。そのため、アクセス制御、リソースとコマンドの許可、アカウンティングをコンテキスト間で別々に実行することができます。

次の内容について説明します。

- 認証の概要（p.14-2）
- 許可の概要（p.14-3）
- アカウンティングの概要（p.14-3）

認証の概要

認証では、有効な証明書（一般にはユーザ名とパスワード）を要求することによって、アクセスを制御します。FWSM では、次の項目の認証を設定できます。

- 次のセッションを含む、FWSM へのすべての管理接続：
  - 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

許可の概要

許可では、ユーザを認証したあと、*各ユーザ*のアクセスを制御できます。FWSM では、次の項目の許可を設定できます。

- 管理コマンド
- ネットワーク アクセス
- 管理接続用の VPN アクセス

認証された各ユーザが使用できるサービスとコマンドを許可によって制御することができます。許可をイネーブルにせずに認証だけを使用する場合、認証されたすべてのユーザに対し、サービスへのアクセスが一様に提供されます。

許可する内容を制御する必要がある場合は、広範囲の許可ルールを定義して、詳細な許可を設定できます。たとえば、内部ユーザを認証して外部ネットワークの任意サーバにアクセスできるようにしたあと、外部サーバへのアクセスを制限して、特定のユーザだけが許可を使用してアクセスできるように設定することができます。

FWSM は、ユーザごとに最初の 16 の許可要求をキャッシュします。したがって、ユーザが現在の許可セッション中に同じサービスにアクセスする場合は、FWSM から認証サーバに要求が再送信されることはありません。

アカウンティングの概要

アカウンティングでは、FWSM を通過するトラフィックを追跡し、ユーザ アクティビティを記録できます。トラフィックの認証をイネーブルにした場合は、ユーザごとにトラフィックをアカウントできます。トラフィックを認証しない場合は、IP アドレスごとにトラフィックをアカウントできます。アカウンティング情報には、セッションの開始時および終了時、ユーザ名、セッション中に FWSM を通過したバイト数、使用されたサービス、および各セッションの長さが含まれます。

AAA サーバおよびローカル データベースのサポート

FWSM は、さまざまな AAA サーバ タイプのほか、FWSM に保管されるローカル データベースをサポートします。ここでは、各 AAA サーバ タイプおよびローカル データベースのサポートについて説明します。

ここでは、次の内容について説明します。

サポートの概要

表 14-1 に、ローカル データベースを含めた、各 AAA サーバ タイプ別の AAA サービス タイプを説明します。特定の AAA サーバ タイプのサポートの詳細については、表の下の説明を参照してください。

表 14-1　AAA サポートのまとめ

	データベース タイプ						
AAA サービス	**ローカル**	**RADIUS**	**TACACS+**	**SDI**	**NT**	**Kerberos**	**LDAP**
認証 . .							
VPN ユーザ[1]	あり	あり	あり	あり	あり	あり	なし
ファイアウォール セッション	あり	あり	あり	なし	なし	なし	なし
管理者	あり	あり	あり	なし	なし	なし	なし
許可 . .							
VPN ユーザ [1]	あり	あり	なし	なし	なし	なし	あり
ファイアウォール セッション	なし	あり[2]	あり	なし	なし	なし	なし
管理者	あり[3]	なし	あり	なし	なし	なし	なし
アカウンティング . .							
VPN 接続 [1]	なし	あり	あり	なし	なし	なし	なし
ファイアウォール セッション	なし	あり	あり	なし	なし	なし	なし
管理者	なし	なし	あり	なし	なし	なし	なし

1. VPN は管理接続の場合のみ、利用できます。
2. ファイアウォール セッションの場合、RADIUS 許可は、ユーザ指定のアクセス リストでのみサポートされます。アクセス リストは、Remote Authentication Dial-In User Service（RADIUS）認証応答で受信または指定されます。
3. ローカル コマンドによる許可はイネーブル レベルでのみ、サポートされます。

RADIUS サーバのサポート

FWSM は RADIUS サーバをサポートします。

ここでは、次の内容について説明します。

認証方法

FWSM は、RADIUS を使用した次の認証方法をサポートします。

- PAP
- CHAP
- MS-CHAPv1
- MS-CHAPv2（パスワードの有効期限を含む）（IPSec ユーザ専用）

属性のサポート

FWSM は、次の RADIUS 属性をサポートします。

- RFC 2138 で定義された認証属性
- RFC 2139 で定義されたアカウンティング属性
- RFC 2868 で定義されたトンネル プロトコル サポートの RADIUS 属性
- Cisco IOS VSA（RADIUS ベンダー ID 9 で識別）
- Cisco VPN 関連 VSA（RADIUS ベンダー ID 3076 で識別）
- RFC 2548 で定義された Microsoft VSA

RADIUS の機能

FWSM は、表 14-2 に示す RADIUS サーバの機能を使用できます。

表 14-2　RADIUS の機能

機能	説明
CLI アクセスのユーザ認証	ユーザが Telnet、SSH、HTTP、またはシリアル コンソール接続を使用して FWSM へのアクセスを試み、トラフィックが認証ステートメントと一致すると、FWSM はユーザ名とパスワードを照合し、RADIUS サーバへ証明書を送信し、サーバからの応答に基づいてユーザの CLI アクセスを認可または拒否します。
enable コマンドのユーザ認証	ユーザが **enable** コマンドへのアクセスを試みると、FWSM はユーザのパスワードを照合して、ユーザ名とイネーブル パスワードを RADIUS サーバへ送信し、サーバからの応答に基づいてユーザ アクセスを認可または拒否して、モードをイネーブルにします。
ネットワーク アクセスのユーザ認証	ユーザが FWSM 経由でネットワークへのアクセスを試み、トラフィックが認証ステートメントと一致すると、FWSM は RADIUS サーバにユーザ証明書（通常ユーザ名とパスワード）を送信し、サーバからの応答に基づいてユーザのネットワーク アクセスを認可または拒否します。

表 14-2　RADIUS の機能（続き）

機能	説明
ユーザ単位のダイナミック ACL を使用したネットワーク アクセスのユーザ認証	ダイナミック アクセス リストを実行するには、RADIUS サーバがこの認証をサポートするように設定しておく必要があります。ユーザが認証されると、RADIUS サーバから FWSM にダウンロード可能なアクセス リストが送信されます。特定サービスへのアクセスは、このアクセス リストによって許可または拒否されます。認証セッションがタイムアウトになると、この アクセス リストは FWSM から削除されます。
ダウンロードしたユーザ単位の アクセス リスト名を使用したネットワーク アクセスのユーザ認証	ダウンロードしたアクセス リスト名を実行するには、RADIUS サーバがこの認証をサポートするように設定しておく必要があります。ユーザが認証されると、RADIUS サーバから、アクセス リストの名前が送信されます。指定された名前を含んだアクセス リストが FWSM に存在する場合、特定サービスへのアクセスは、このアクセス リストに基づいて許可または拒否されます。複数のユーザに同じ アクセス リスト を指定できます。
VPN 認証	ユーザが VPN を使用して管理接続の確立を試み、適用可能なトンネル グループ レコードが RADIUS 認証サーバ グループを指定する場合、FWSM は RADIUS サーバにユーザ名とパスワードを送信してから、サーバからの応答に基づいてユーザのアクセスを認可または拒否します。
VPN 許可	VPN アクセスのユーザ認証が成功し、適用可能なトンネル グループ レコードが RADIUS 許可サーバ グループを指定すると、FWSM は RADIUS 許可サーバに要求を送り、受信された許可を VPN セッションに適用します。
VPN アカウンティング	VPN アクセスのユーザ認証が成功し、適用可能なトンネル グループ レコードが RADIUS アカウンティング サーバ グループを指定すると、FWSM は VPN セッションに関する RADIUS サーバ グループ アカウンティング データを送信します。
ユーザまたは IP アドレスごとのネットワーク アクセスのアカウンティング	FWSM を通過する任意のトラフィックについて、FWSM から RADIUS サーバにアカウンティング情報を送信できます。

TACACS+ サーバのサポート

FWSM は、表 14-3 に示す Terminal Access Controller Access Control System Plus（TACACS+）サーバの機能を使用できます。FWSM は、ASCII、PAP、CHAP、MS-CHAPv1 を使用して TACACS+ 認証をサポートします。

表 14-3　TACACS+ 機能

機能	説明
CLI アクセスのユーザ認証	ユーザが Telnet、SSH、HTTP、またはシリアル コンソール接続を使用して FWSM へのアクセスを試み、トラフィックが認証ステートメントと一致すると、FWSM はユーザ名とパスワードを照合し、TACACS+ サーバへ証明書を送信し、サーバからの応答に基づいてユーザの CLI アクセスを認可または拒否します。
enable コマンドのユーザ認証	ユーザが **enable** コマンドへのアクセスを試みると、FWSM はユーザのパスワードを照合して、ユーザ名とイネーブル パスワードを TACACS+ サーバへ送信し、サーバからの応答に基づいてユーザ アクセスを認可または拒否して、モードをイネーブルにします。
CLI アクセスのアカウンティング	管理セッションに関するアカウンティング情報を TACACS+ サーバに送信するよう FWSM を設定できます。

表 14-3　TACACS+ 機能（続き）

機能	説明
ネットワーク アクセスのユーザ認証	ユーザが FWSM 経由でネットワークへのアクセスを試み、トラフィックが認証ステートメントと一致すると、FWSM は TACACS+ サーバにユーザ証明書（通常ユーザ名とパスワード）を送信し、サーバからの応答に基づいてユーザのネットワーク アクセスを認可または拒否します。
ネットワーク アクセスのユーザ許可	ユーザが認証後に FWSM 上の許可ステートメントと一致した場合、FWSM は TACACS+ サーバを使用してユーザのアクセス権限を照合します。
VPN 認証	ユーザが VPN を使用して管理接続の確立を試み、適用可能なトンネル グループ レコードが TACACS+ 認証サーバ グループを指定する場合、FWSM は TACACS+ サーバにユーザ名とパスワードを送信してから、サーバからの応答に基づいてユーザのアクセスを認可または拒否します。
VPN アカウンティング	VPN アクセスのユーザ認証が成功し、適用可能なトンネル グループ レコードが TACACS+ アカウンティング サーバ グループを指定すると、FWSM は VPN セッションに関する TACACS+ サーバ グループ アカウンティング データを送信します。
管理コマンドのユーザ許可	TACACS+ サーバ上で、CLI アクセスの認証後にユーザが使用できるコマンドを設定します。ユーザが CLI から入力したコマンドはすべて、TACACS+ サーバによって検証されます。
ユーザまたは IP アドレスごとのネットワーク アクセスのアカウンティング	FWSM を通過する任意のトラフィックについて、FWSM から TACACS+ サーバにアカウンティング情報を送信できます。

SDI サーバのサポート

FWSM では、RSA SecureID サーバを VPN 認証に使用できます。このサーバは、SDI サーバとして知られています。ユーザが VPN アクセスの確立を試み、適用可能なトンネル グループ レコードが SDI 認証サーバ グループを指定する場合、FWSM は SDI サーバにユーザ名と One Time Password（OTP; ワンタイム パスワード）を送信し、サーバからの応答に基づいてユーザのアクセスを認可または拒否します。

ここでは、次の内容について説明します。

SDI バージョンのサポート

FWSM は、次の SDI バージョンをサポートします。

- **バージョン 5.0 以前のバージョン —** バージョン 5.0 以前の SDI バージョンでは、単一ノード シークレット ファイル（SECURID）を共有する SDI マスター サーバおよび SDI スレーブ サーバの概念を使用します。
- **バージョン 5.0 —** SDI バージョン 5.0 では、SDI プライマリ サーバおよび SDI レプリカ サーバの概念を使用します。各プライマリ サーバとそのレプリカ サーバは、単一ノード シークレット ファイルを共有します。ノード シークレット ファイルには、.sdi を付加した ACE/Server IP アドレスの 16 進数の値に基づく名前が付けられています。

  FWSM 上で設定されたバージョン 5.0 の SDI サーバは、プライマリ サーバにも、レプリカ サーバのいずれにもすることができます。SDI エージェントがユーザを認証する方法については、次の 「SDI プライマリ サーバとレプリカ サーバ」（p.14-8）を参照してください。

2 段階の認証プロセス

SDI バージョン 5.0 は、2 段階のプロセスを使用して、侵入者が RSA SecurID 認証要求からの情報を得て別のサーバへの認証に使用するのを防ぎます。ユーザ認証要求を送信する前に、SDI エージェントはまず、SecurID サーバへのロック要求を送信します。サーバは、ユーザ名をロックし、別の（レプリカ）サーバがそのユーザ名を受け入れないようにします。そのため、同じユーザが同じ認証サーバを同時に使用して、2 台の FWSM に認証することができなくなります。ユーザ名を正常にロックできた場合、FWSM コンセントレータはパスコードを送信します。

SDI プライマリ サーバとレプリカ サーバ

最初のユーザが設定済みのサーバに認証すると、FWSM はサーバ リストを取得します。このときのサーバは、プライマリ サーバでもレプリカ サーバでも構いません。次に、FWSM は、リストにある各サーバに優先順位を割り当て、その優先順位からランダムにサーバを選択します。優先順位が一番高いサーバが、選択される可能性が高くなります。

NT サーバのサポート

FWSM は、NTLM バージョン 1 をサポートする Microsoft Windows サーバ オペレーティング システムで、VPN ベースの管理接続の認証をサポートします。Microsoft Windows サーバはまとめて NT サーバと呼びます。ユーザが VPN アクセスの確立を試み、適用可能なトンネル グループ レコードが NT 認証サーバ グループを指定する場合、FWSM は、Microsoft Windows ドメイン サーバでユーザ認証に NTLM バージョン 1 を使用します。FWSM は、ドメイン サーバからの応答に基づいてユーザのアクセスを認可または拒否します。

（注）　NT サーバのユーザのパスワードは最長 14 文字です。15 文字めからは切り捨てられます。これは、NTLM バージョン 1 の制限事項です。

Kerberos サーバのサポート

FWSM は、VPN ベースの管理接続に Kerberos サーバを使用できます。ユーザが VPN アクセスの確立を試み、トラフィックが認証ステートメントと一致すると、FWSM は Kerberos サーバを使用してユーザ認証を照合し、サーバからの応答に基づいてユーザのネットワーク アクセスを認可または拒否します。

FWSM がサポートする暗号化タイプは、3DES、DES、RC4 です。

（注）　FWSM は、トンネル ネゴシエーション時には、ユーザのパスワード変更をサポートしません。偶発的に起こるこの状況を回避するには、FWSM に接続するユーザに対して、Kerberos/Active Directory サーバ上でのパスワード有効期間を無効にしてください。

LDAP サーバのサポート

FWSM は、VPN ベースの管理接続に LDAP サーバを使用できます。VPN アクセスのユーザ認証が成功し、適用可能なトンネル グループ レコードが LDAP 許可サーバ グループを指定すると、FWSM は LDAP サーバに照会し、許可が受信された VPN セッションに適用されます。

ローカル データベースのサポート

FWSM は、ユーザ プロファイルが登録されたローカル データベースを維持します。

ここでは、次の内容について説明します。

ユーザ プロファイル

ユーザ プロファイルには、少なくともユーザ名が含まれます。パスワードの設定は任意ですが、通常は、各ユーザ名に割り当てられます。

username attributes コマンドを使用すると、username モードを開始できます。このモードでは、別の情報を特定のユーザ プロファイルに追加できます。追加可能な情報には、VPN 関連属性（VPN セッション タイムアウト値など）が含まれます。

ローカル データベースの機能

FWSM は、表 14-4 に示す ローカル データベースの機能を使用できます。

表 14-4　ローカル データベースの機能

機能	説明
CLI アクセスのユーザ認証	ユーザが Telnet、SSH、HTTP、またはシリアル コンソール接続を使用して FWSM へのアクセスを試み、トラフィックが認証ステートメントと一致すると、FWSM はユーザ名とパスワードを照合し、ローカル データベースに対して証明書を検証し、その結果に基づいてユーザの CLI アクセスを認可または拒否します。
enable コマンドまたは **login** コマンドのユーザ認証	ユーザが **enable** コマンドへのアクセスを試みると、FWSM はユーザのパスワードを照合して、ローカル データベースに対してユーザ名とパスワードを照合し、その結果に基づいてユーザ アクセスを認可または拒否して、モードをイネーブルにします。
管理コマンドのユーザ許可	**enable** コマンドで認証された（または **login** コマンドでログインした）ユーザは、FWSM により、ローカル データベースに定義されているイネーブル レベルに設定されます。各コマンドは、FWSM 上で 0 ～ 15 のイネーブル レベルに設定できます。
ネットワーク アクセスのユーザ認証	ユーザが FWSM 経由でネットワークへのアクセスを試み、トラフィックが認証ステートメントと一致すると、FWSM はユーザ名とパスワードを照合し、ローカル データベースに対して証明書を検証し、その結果に基づいてユーザの ネットワーク アクセスを認可または拒否します。
VPN 認証	ユーザが VPN を使用して管理接続の確立を試み、トラフィックが認証ステートメントと一致すると、FWSM はローカル ユーザ データベースに対して受信したユーザ名とパスワードを検証し、その結果に基づいて VPN アクセスを認可または拒否します。
VPN 許可	VPN アクセスのユーザ認証が成功すると、FWSM は、ユーザ名と適用可能なグループ ポリシーに対応付けられたローカル データベースからの属性を、VPN セッションに適用します。

フォールバックのサポート

ネットワーク アクセス認証のフォールバックは別として、ローカル データベースは 表 14-4 に記載された機能のフォールバック方式として動作します。フォールバックにより、FWSM からの意図しないロックアウトを回避することができます。

フォールバック サポートを必要とするユーザの場合、ローカル データベースのユーザ名とパスワードを AAA サーバのユーザ名とパスワードと一致させることを推奨します。これにより、透過的なフォールバック サポートが提供されます。ユーザは、AAA サーバまたはローカル データベースによってこのサービスが提供されているかどうかを判断できないため、ローカル データベースのものと異なる AAA サーバのユーザ名とパスワードを使用すると、ユーザは自分のユーザ名とパスワードが正しいのかどうか確信が持てなくなります。

ローカル データベースでは、次のフォールバック機能をサポートします。

- **コンソールおよびイネーブル パスワードの認証 — aaa authentication console** コマンドを使用する場合、AAA サーバ グループ タグのあとに **LOCAL** キーワードを追加できます。すべてのグループのサーバが利用できない場合、FWSM 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。これにもイネーブル パスワードの認証を含めることができます。
- **コンソールの許可 — aaa authorization command** コマンドを使用する場合、AAA サーバ グループ タグのあとに **LOCAL** キーワードを追加できます。すべてのグループの TACACS+ サーバが利用できない場合、ローカル データベースを使用して、イネーブル レベルに基づいてコマンドを許可します。
- **VPN 認証および許可 —** VPN サービスを正常にサポートするはずの AAA サーバを利用できない場合、VPN 認証および許可がサポートされ、FWSM へのリモート アクセスからイネーブルになります。トンネル グループの一般属性モードで利用可能な **authentication-server-group** コマンドを使用する場合、トンネル グループの属性を設定するときに **LOCAL** キーワードを指定します。管理者の 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に設定されたトンネル グループを指定する場合、AAA サーバ グループを利用できなくても、ローカル データベースに必要な属性が設定されていれば、VPN トンネルを確立できます。

ローカル データベースの設定

ここでは、ローカル データベース内のユーザを管理する手順について説明します。ローカル データベースは、CLI アクセスの認証、イネーブル モードの認証、コマンドの許可、ネットワーク アクセスの認証、VPN の認証および許可に使用できます。ネットワーク アクセスの許可にローカル データベースを使用することはできません。ローカル データベースでは、アカウンティングはサポートされません。

マルチコンテキスト モードでは、システム実行スペースでユーザ名を設定し、**login** コマンドによって個別ログインを提供できますが、システム実行スペースには **aaa** コマンドを設定することはできません。

注意　CLI へのアクセスが許可され、イネーブル モードの使用が許可されないユーザをローカル データベースに追加する場合は、コマンド許可をイネーブルにします（「ローカル コマンド許可の設定」[p.21-16] を参照）。コマンド許可を使用しない場合、イネーブル レベルが 2 以上（2 はデフォルト値）のユーザは、個人のパスワードを使用して CLI のイネーブル モード（およびすべてのコマンド）にアクセスできます。別の方法としては、RADIUS または TACACS+ 認証を使用してユーザが **login** コマンドを使用できないように設定するか、またはすべてのローカル ユーザをレベル 1 に設定してから、システム イネーブル パスワードを使用してイネーブル モードにアクセスできるユーザを制御します。

ローカル データベースにユーザ アカウントを定義する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、ユーザ アカウントを作成します。

```
hostname/contexta(config)# username username {nopassword | password password}
[encrypted] [privilege level]
```

オプションは次のとおりです。

- *username* — 4 ～ 64 文字の長さの文字列を指定します。
- **password** *password* — 3 ～ 16 文字の長さの文字列を指定します。
- **encrypted** — 指定のパスワードが暗号化されていることを示します。
- **privilege** *level* — 新しいユーザ アカウントに割り当てるイネーブル レベル（0 ～ 15）を指定します。デフォルトは 2 です。イネーブル レベルはコマンド許可と併用します。
- **nopassword** — パスワードを使用しないユーザ アカウントを作成します。

ステップ 2　VPN 属性を持ったローカル ユーザ アカウントを定義する手順は、次のとおりです。

a. 次のコマンドを入力します。

```
hostname/contexta(config)# username username attributes
```

username attributes コマンドを入力すると、username モードが開始されます。このモードで利用できるコマンドは、次のとおりです。

- **group-lock**
- **password-storage**
- **vpn-access-hours**
- **vpn-filter**

- **vpn-framed-ip-address**
- **vpn-group-policy**
- **vpn-idle-timeout**
- **vpn-session-timeout**
- **vpn-simultaneous-logins**
- **vpn-tunnel-protocol**

このコマンドを必要に応じて使用して、ユーザ プロファイルを設定してください。このコマンドの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

b. ユーザ プロファイルの設定を終了する場合、**exit** を入力してコンフィギュレーション モードに戻ります。

次に、admin ユーザのアカウントにイネーブル レベル 15 を割り当てる例を示します。

```
hostname/contexta(config)# username admin password passw0rd privilege 15
```

次に、パスワードを許可しないユーザ アカウントを作成する例を示します。

```
hostname/contexta(config)# username bcham34 nopassword
```

次のコマンドはパスワードのあるユーザ アカウントを作成し、username モードを開始し、2 ～ 3 の VPN 属性を指定します。

```
hostname/contexta(config)# username rwilliams password gOgeOus
hostname/contexta(config)# username rwilliams attributes
hostname/contexta(config-username)# vpn-tunnel-protocol IPSec
hostname/contexta(config-username)# vpn-simultaneous-logins 6
hostname/contexta(config-username)# exit
```

AAA サーバ グループおよびサーバの識別

認証、許可、またはアカウンティングに外部の AAA サーバを使用する場合は、まず、AAA プロトコルごとに 1 つまたは複数の AAA サーバ グループを作成し、各グループに 1 つまたは複数のサーバを追加します。AAA サーバ グループは名前ごとに識別します。各サーバ グループは、Kerberos、LDAP、NT、RADIUS、SDI、または TACACS+ のそれぞれのサーバ タイプで固有です。

FWSM は、グループ内の最初のサーバと通信します。最初のサーバが使用できない場合、FWSM はグループ内の次のサーバ（設定されている場合）と通信します。グループ内のすべてのサーバが使用できない場合、フォールバック方式としてローカル データベースが設定されていれば、FWSM はローカル データベースと通信します（管理認証および許可のみ）。フォールバック方式が設定されていない場合、FWSM は AAA サーバとの通信を継続的に試みます。

サーバ グループを作成し AAA サーバを追加する手順は、次のとおりです。

ステップ 1　作成する必要のある各 AAA サーバ グループには、次の手順を実行します。

a. サーバ グループ名およびプロトコルを識別します。そのためには、次のコマンドを入力します。

```
hostname/contexta(config)# aaa-server server_group protocol {kerberos | ldap | nt |
radius | sdi | tacacs+}
```

たとえば、RADIUS を使用してネットワーク アクセスを認証したり、TACACS+ を使用して CLI アクセスを認証したりするには、2 つ以上のサーバ グループ（1 つは RADIUS サーバ用、1 つは TACACS+ サーバ用）を作成する必要があります。

最大 15 個のシングル モード サーバ グループまたは 4 個のマルチ モード サーバ グループを作成できます。各サーバ グループには、シングル モードで最大 16 個のサーバ、またはマルチ モードで最大 4 個のサーバを含めることが可能です。

aaa-server protocol コマンドを入力すると、グループ モードが開始されます。

b. 次のサーバに移行する前に、グループ内の 1 つの AAA サーバに送信する要求の最大数を指定するには、次のコマンドを入力します。

```
hostname/contexta(config-aaa-server-group)# max-failed-attempts number
```

number の範囲は、1 ～ 5 です。デフォルトは 3 です。

ローカル データベースを使用するフォールバック方式（管理アクセスのみに使用。フォールバック機能の設定方法については 「システム管理者用の AAA」[p.21-13] および 「TACACS+ コマンド許可の設定」[p.21-20] を参照）を設定した場合は、グループ内のすべてのサーバが応答に失敗すると、そのグループは応答不可とみなされ、フォールバック方式が試行されます。サーバ グループが応答不可としてマークされる時間は 10 分間（デフォルト）です。その間、追加の AAA 要求はサーバ グループには送信されず、ただちにフォールバック方式が採用されます。応答不可の時間をデフォルト以外に変更する場合は、次の **reactivation-mode** コマンドを参照してください。

フォールバック方式が設定されていない場合、FWSM はグループ内のサーバへの通信を継続的に試みます。

c. グループ内の失敗したサーバを再開する方法（再開ポリシー）を指定するには、**reactivation-mode** コマンドを使用します。このコマンドの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

d. アカウンティング メッセージを単一 サーバに送信するか（シングル モード）、グループ内のすべてのサーバに送信するか（Simultaneous モード）を指定する場合、**accounting-mode** コマンドを使用します。このコマンドの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

e. AAA サーバ グループの設定を終了する場合、**exit** を入力します。

ステップ 2　使用するネットワークの各 AAA サーバの場合、手順は次のとおりです。

a. AAA サーバが所属する AAA サーバ グループを含め、サーバを識別します。そのためには、次のコマンドを入力します。

```
hostname/contexta(config)# aaa-server server_group (interface_name) host server_ip
```

aaa-server host コマンドを入力すると、host モードを開始します。

b. host モード コマンドを必要に応じて使用し、AAA サーバを設定ください。

host モードのコマンドは、AAA サーバ タイプすべてに適用されるわけではありません。表 14-5 に、使用できるコマンド、適用されるサーバ タイプ、新しい AAA サーバ定義にコマンドのデフォルト値があるかどうか示します。指定したサーバ タイプにコマンドを適用でき、デフォルト値がない（[—] で表示）場合、次のコマンドを使用して値を指定します。このコマンドの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*』を参照してください。

表 14-5　host モード コマンド、サーバ タイプ、デフォルト値

コマンド	適用可能な AAA サーバ タイプ	デフォルト値
accounting-port	RADIUS	1646
authentication-port	RADIUS	1645
kerberos-realm	Kerberos	—
key	RADIUS	—
	TACACS+	—
ldap-base-dn	LDAP	—
ldap-login-dn	LDAP	—
ldap-login-password	LDAP	—
ldap-naming-attribute	LDAP	—
ldap-scope	LDAP	—
nt-auth-domain-controller	NT	—
radius-common-pw	RADIUS	—
retry-interval	Kerberos	10 秒
	RADIUS	10 秒
sdi-pre-5-slave	SDI	—
sdi-version	SDI	sdi-5
server-port	Kerberos	88
	LDAP	389
	NT	139
	SDI	5500
	TACACS+	49
timeout	すべて	10 秒

c. AAA サーバ ホストの設定を終了するには、**exit** を入力します。

たとえば、プライマリ サーバとバックアップ サーバを 1 つずつ指定した 1 つの TACACS+ グループ、単一サーバを指定した 1 つの RADIUS グループ、1 つの NT ドメイン サーバを追加するには、次のコマンドを入力します。

```
hostname/contexta(config)# aaa-server AuthInbound protocol tacacs+
hostname/contexta(config-aaa-server-group)# max-failed-attempts 2
hostname/contexta(config-aaa-server-group)# reactivation-mode depletion deadtime 20
hostname/contexta(config-aaa-server-group)# exit
hostname/contexta(config)# aaa-server AuthInbound (inside) host 10.1.1.1
hostname/contexta(config-aaa-server-host)# key TACPlusUauthKey
hostname/contexta(config-aaa-server-host)# exit
hostname/contexta(config)# aaa-server AuthInbound (inside) host 10.1.1.2
hostname/contexta(config-aaa-server-host)# key TACPlusUauthKey2
hostname/contexta(config-aaa-server-host)# exit
hostname/contexta(config)# aaa-server AuthOutbound protocol radius
hostname/contexta(config-aaa-server-group)# exit
hostname/contexta(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
hostname/contexta(config-aaa-server-host)# key RadUauthKey
hostname/contexta(config-aaa-server-host)# exit
hostname/contexta(config)# aaa-server NTAuth protocol nt
hostname/contexta(config-aaa-server-group)# exit
hostname/contexta(config)# aaa-server NTAuth (inside) host 10.1.1.4
hostname/contexta(config-aaa-server-host)# nt-auth-domain-controller primary1
hostname/contexta(config-aaa-server-host)# exit
```