CHAPTER 11

AAA サーバとローカル データベースの設定

この章では、AAA（「トリプル エー」と発音）のサポート、および AAA サーバとローカル データベースの設定方法について説明します。

この章では、次の内容について説明します。

- 「AAA の概要」（P.11-1）
- 「AAA サーバおよびローカル データベースのサポート」（P.11-3）
- 「ローカル データベースの設定」（P.11-7）
- 「AAA サーバ グループおよびサーバの識別」（P.11-9）

AAA の概要

AAA によって、FWSM が、ユーザが誰か（認証）、ユーザが何を実行できるか（認可）、およびユーザが何を実行したか（アカウンティング）を判別することが可能になります。

AAA には、ユーザ アクセスに対して、アクセス リストだけを使用する場合よりもレベルの高い保護および制御機能が用意されています。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 サーバもまた、認証を実行します。FWSM は、認可されないユーザがサーバにアクセスできないようにします）。

認証は、単独で使用するか、認可およびアカウンティングとともに使用することができます。認可については、常に最初にユーザが認証されて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。

マルチセキュリティ 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、コンテキスト間で共有することはできません。そのため、アクセス コントロール、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。

ここでは、次の内容について説明します。

- 「認証の概要」（P.11-2）
- 「認可の概要」（P.11-2）
- 「アカウンティングの概要」（P.11-2）

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。次の項目を認証するように、FWSM を設定できます。

- FWSM 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

認可の概要

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。次の項目を認可するように、FWSM 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

認可は、認証された個々のユーザが使用できるサービスおよびコマンドを制御します。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。

認可で提供される制御を必要とする場合は、広範な認証規則を設定してから、詳細な認可を設定できます。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 はユーザあたり最初の 16 件の認可要求をキャッシュするため、ユーザが現在の認証セッション中に同じサービスにアクセスした場合、FWSM は認可サーバに要求を再送信しません。

アカウンティングの概要

アカウンティングは、FWSM を通過するトラフィックを追跡して、ユーザ アクティビティを記録できるようにします。このようなトラフィックの認証をイネーブルにすると、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刻と終了時刻、ユーザ名、FWSM を通過するセッションのバイト数、使用されたサービス、および各セッションの継続時間などの情報が含まれます。

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 タイプおよび FWSM に保存されているローカル 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。

- 「サポートの要約」（P.11-3）
- 「RADIUS サーバ サポート」（P.11-4）
- 「TACACS+ サーバのサポート」（P.11-5）
- 「SDI サーバのサポート」（P.11-5）
- 「NT サーバのサポート」（P.11-6）
- 「Kerberos サーバのサポート」（P.11-6）
- 「LDAP サーバのサポート」（P.11-6）
- 「ローカル データベースのサポート」（P.11-6）

サポートの要約

表 11-1 に、各 AAA サービスのサポート状況の要約を AAA サーバ タイプ（ローカル データベースを含む）別に示します。特定の AAA サーバ タイプのサポートの詳細については、表に続く項目を参照してください。

表 11-1　AAA サポートの概要

	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]	Yes	Yes	Yes	Yes	Yes	Yes	No
ファイアウォール セッション	Yes	Yes	Yes	No	No	No	No
管理者	Yes	Yes	Yes	No	No	No	No
許可 ..							
VPN ユーザ[1]	Yes	Yes	No	No	No	No	Yes
ファイアウォール セッション	No	Yes[2]	Yes	No	No	No	No
管理者	Yes[3]	No	Yes	No	No	No	No
アカウンティング ..							
VPN 接続[1]	No	Yes	Yes	No	No	No	No
ファイアウォール セッション	No	Yes	Yes	No	No	No	No
管理者	No	No	Yes	No	No	No	No

1. VPN は管理接続の場合だけ、利用できます。

2. ファイアウォール セッションの場合、RADIUS 認可はユーザ固有のアクセス リストだけでサポートされます。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。
3. ローカル コマンド認可は、権限レベルだけによってサポートされます。

RADIUS サーバ サポート

FWSM は RADIUS サーバをサポートします。

次の事項について説明します。

- 「認証方式」（P.11-4）
- 「属性のサポート」（P.11-4）
- 「TACACS+ サーバのサポート」（P.11-5）

認証方式

FWSM は、RADIUS で次の認証方法をサポートします。

- PAP
- CHAP
- MS-CHAPv1
- MS-CHAPv2

  MS-CHAPv2 は、RADIUS サーバと Windows Active Directory サーバの通信時におけるパスワード管理をサポートします。パスワードが期限切れになると、パスワードを変更するように求められます（**auth-prompt** コマンドを参照）。

属性のサポート

FWSM は、次の RADIUS 属性のセットをサポートします。

- RFC 2138 に定義されている認証属性
- RFC 2139 に定義されているアカウンティング属性
- RFC 2868 に定義されているトンネル プロトコル サポート用の RADIUS 属性
- RADIUS ベンダー ID 9 によって識別される Cisco IOS VSA
- RADIUS ベンダー ID 3076 によって識別される Cisco VPN 関連 VSA
- RFC 2548 に定義されている Microsoft VSA

RADIUS 許可の機能

FWSM では RADIUS サーバを使用して、ダイナミック アクセス リストまたはユーザごとのアクセス リスト名を使用するネットワーク アクセスに対して、ユーザ認可を実行できます。ダイナミック アクセス リストを実装するには、これをサポートするように RADIUS サーバを設定する必要があります。ユーザが認証されると、RADIUS サーバからセキュリティ アプライアンスにダウンロード可能なアクセス リストまたはアクセス リスト名が送信されます。所定のサービスへのアクセスがアクセス 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 リストはセキュリティ アプライアンスから削除されます。

TACACS+ サーバのサポート

セキュリティ アプライアンスは、ASCII、PAP、CHAP、MS-CHAPv1 を使用して TACACS+ 認証をサポートします。

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。

次の事項について説明します。

- 「SDI バージョンのサポート」（P.11-5）
- 「2 ステップ認証プロセス」（P.11-5）
- 「SDI プライマリ サーバとレプリカ サーバ」（P.11-5）

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。各プライマリおよびそのレプリカは、単一ノード シークレット ファイルを共有します。そのノード シークレット ファイルの名前は、.sdi が付加された ACE/ サーバ IP アドレスの 16 進数値に基づきます。

  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。ユーザ認証のための SDI エージェントによるサーバの選択方法の詳細については、「SDI プライマリ サーバとレプリカ サーバ」（P.11-5）を参照してください。

2 ステップ認証プロセス

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て、別の（レプリカ）サーバがユーザ名を受信できないようにします。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。ユーザ名のロックに成功すると、FWSM 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

FWSM は、最初のユーザが設定済みサーバ（プライマリでもレプリカでもかまいません）に認証を証明するときに、サーバ リストを取得します。次に、FWSM はリスト上の各サーバにプライオリティを割り当て、その後のサーバ選択では、この割り当てられたプライオリティのサーバから無作為に抽出します。最もプライオリティの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 サーバでは、ユーザ パスワードの最大長は 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 は、3DES、DES、および RC4 暗号タイプをサポートしています。

（注）　FWSM は、トンネル ネゴシエーション中のユーザ パスワードの変更はサポートしていません。この状況が意図せずに発生することを回避するために、FWSM に接続するユーザの Kerberos/Active Directory サーバでのパスワード期限切れをディセーブルにします。

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。

次の事項について説明します。

- 「ユーザ プロファイル」（P.11-6）
- 「フォールバック サポート」（P.11-7）

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。通常、パスワードはオプションですが、各ユーザ名にパスワードが割り当てられます。

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。

フォールバック 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 11-1 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。この動作は、FWSM 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。

フォールバック サポートを必要とするユーザでは、ローカル データベース内のユーザ名とパスワードと AAA サーバ内のユーザ名とパスワードを一致させることをお勧めします。これにより、トランスペアレント 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。
- **コマンドの許可**：**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 アクセスがイネーブルになります。**authentication-server-group** コマンド（トンネルグループ一般属性モードで使用可能）を使用すると、トンネル グループの属性を設定するときに、**LOCAL** キーワードが指定できます。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の管理方法について説明します。ローカル データベースは、CLI アクセス認証、特権モード認証、コマンド認可、ネットワーク アクセス認証、および VPN 認証および認可に使用できます。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。ローカル データベースはアカウンティングをサポートしません。

システム実行スペースでは、**username** コマンドを入力できません。ただし、システムで **login** コマンドを使用するか、スイッチから FWSM へのセッションを開始するときに Telnet 認証を使用する場合は、FWSM では管理コンテキストのユーザ名のデータベースが使用されます（管理コンテキストでは、システム実行スペースの Telnet 認証も設定されます）。

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 コマンド認可の設定」（P.23-16）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には、次の手順を実行します。

ステップ 1　ユーザ アカウントを作成します。そのためには、次のコマンドを入力します。

```
hostname(config)# username username {nopassword | password password} [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。
- **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。この特権レベルは、コマンド認可で使用されます。
- **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。

通常、**encrypted** キーワードは表示専用です。**username** コマンド内のパスワードを定義すると、FWSM 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は示されません。暗号化されたパスワードとそれに続けて **encrypted** キーワードが示されます。たとえば、test というパスワードを入力した場合、**show running-config** の画面には次のように表示されます。

```
username pat password DLaUiAX3l78qgoB5c7iVNw== nt-encrypted
```

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(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。これら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(config)# username admin password passw0rd privilege 15
```

次のコマンドは、パスワードを指定しないユーザ アカウントを作成します。

```
hostname(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(config)# username user1 password gOgeOus
hostname(config)# username user1 attributes
hostname(config-username)# vpn-tunnel-protocol IPSec
hostname(config-username)# vpn-simultaneous-logins 6
hostname(config-username)# exit
```

AAA サーバ グループおよびサーバの識別

認証、認可、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、Kerberos、LDAP、NT、RADIUS、SDI、または TACACS+ というサーバの 1 つのタイプ専用となります。

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、FWSM は、ローカル データベースがフォールバック方式として設定されていると、ローカル データベースに接続しようとします（管理認証および認可限定）。フォールバック方式として設定されていない場合、FWSM は引き続き AAA サーバにアクセスしようとします。

サーバ グループを作成して、AAA サーバを追加するには、次の手順を実行します。

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

```
hostname(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、TACACS+ を使用して CLI アクセスを認証するには、RADIUS サーバ用に 1 つ、TACACS+ サーバ用に 1 つというように、最低 2 つのサーバ グループを作成する必要があります。

シングルモードの場合は最大 15 個の AAA サーバ グループを使用でき、マルチモードの場合は各コンテキストで最大 4 個のサーバ グループを使用できます。各グループには、シングル モードで最大 16 台のサーバ、マルチ モードでは 4 台のサーバを含めることができます。

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

number の範囲は、1 ～ 5 です。デフォルト値は 3 です。

ローカル データベースを使用してフォールバック方式を設定し（管理アクセスだけの場合は、「システム管理者用の AAA」（P.23-10）および「TACACS+ コマンド許可の設定」（P.23-20）を参照してフォールバック メカニズムを設定）、グループ内のすべてのサーバが応答できなかった場合、グループは非応答と見なされ、フォールバック方式が試行されます。サーバ グループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間（デフォルト）続いたら、た

だちにフォールバック方式が使用されます。この後もサーバがアクセス可能かどうかに関係なく、サーバ グループには up マークが付けられます。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として設定されていない場合、FWSM は引き続きグループ内のサーバにアクセスしようとします。

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。

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. 次のコマンドを入力して、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。

```
hostname(config)# aaa-server server_tag [(interface_name)] host server_ip [key]
[timeout seconds]
```

aaa-server host コマンドを入力すると、AAA サーバのホスト コンフィギュレーション モードが開始されます。

b. 必要に応じて、ホスト モード コマンドを使用して、さらに AAA サーバを設定します。

ホスト モードでのコマンドは、すべての AAA サーバ タイプに適用されるわけではありません。表 11-2 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を示します。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。これら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 11-2　ホスト モード コマンド、サーバ タイプ、およびデフォルト

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	All	10 秒

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(config)# aaa-server AuthInbound protocol tacacs+
hostname(config-aaa-server-group)# max-failed-attempts 2
hostname(config-aaa-server-group)# reactivation-mode depletion deadtime 20
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server AuthInbound (inside) host 10.1.1.1
hostname(config-aaa-server-host)# key TACPlusUauthKey
hostname(config-aaa-server-host)# exit
hostname(config)# aaa-server AuthInbound (inside) host 10.1.1.2
hostname(config-aaa-server-host)# key TACPlusUauthKey2
hostname(config-aaa-server-host)# exit
hostname(config)# aaa-server AuthOutbound protocol radius
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
hostname(config-aaa-server-host)# key RadUauthKey
hostname(config-aaa-server-host)# exit
```

```
hostname(config)# aaa-server NTAuth protocol nt
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server NTAuth (inside) host 10.1.1.4
hostname(config-aaa-server-host)# nt-auth-domain-controller primary1
```