



# CHAPTER 4

## AAA の設定

---

この章では、Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウンティング) を設定する手順について次の内容で説明します。

- [「AAA の概要」 \(P.4-1\)](#)
- [「AAA の前提条件」 \(P.4-4\)](#)
- [「AAA の注意事項および制限事項」 \(P.4-4\)](#)
- [「デフォルト設定」 \(P.4-4\)](#)
- [「AAA の設定」 \(P.4-4\)](#)
- [「AAA 設定の確認」 \(P.4-8\)](#)
- [「AAA 設定例」 \(P.4-9\)](#)
- [「その他の関連資料」 \(P.4-9\)](#)
- [「AAA 機能の履歴」 \(P.4-10\)](#)

## AAA の概要

ここでは、次の内容について説明します。

- [「AAA セキュリティ サービス」 \(P.4-1\)](#)
- [「AAA サーバ グループ」 \(P.4-4\)](#)

## AAA セキュリティ サービス

AAA は、ユーザ ID とパスワードの組み合わせに基づいて、ユーザを認証および許可するために使用します。鍵は、AAA サーバとの通信を保護します。

多くの場合、AAA は RADIUS または TACACS+ などのプロトコルを使用してセキュリティ機能を管理します。ルータまたはアクセス サーバがネットワーク アクセス サーバとして動作している場合は、ネットワーク アクセス サーバと RADIUS または TACACS+ セキュリティ サーバとの間の通信を確立する手段に、AAA を使用します。

AAA は主要な (推奨される) アクセス コントロール方式ですが、さらに、ローカル ユーザ名認証、回線パスワード認証、イネーブルパスワード認証など、AAA の範囲外で簡単なアクセス コントロールを行う機能も用意されています。ただし、これらの機能では、AAA を使用した場合と同レベルのアクセス コントロールは実現できません。

次のサービスごとに別個の AAA 設定を作成します。

- ユーザの Telnet または Secure Shell (SSH; セキュア シェル) ログイン認証
- コンソール ログイン認証
- ユーザ管理セッション アカウンティング

表 4-1 に、AAA サービスを設定するための CLI の関連コマンドを示します。

表 4-1 AAA サービス コンフィギュレーション コマンド

AAA サービス設定オプション	関連コマンド
Telnet または SSH ログイン	<code>aaa authentication login default</code>
コンソール ログイン	<code>aaa authentication login console</code>

AAA では次の保護を行います。

- 「認証」(P.4-2)
- 「許可」(P.4-3)
- 「アカウンティング」(P.4-3)

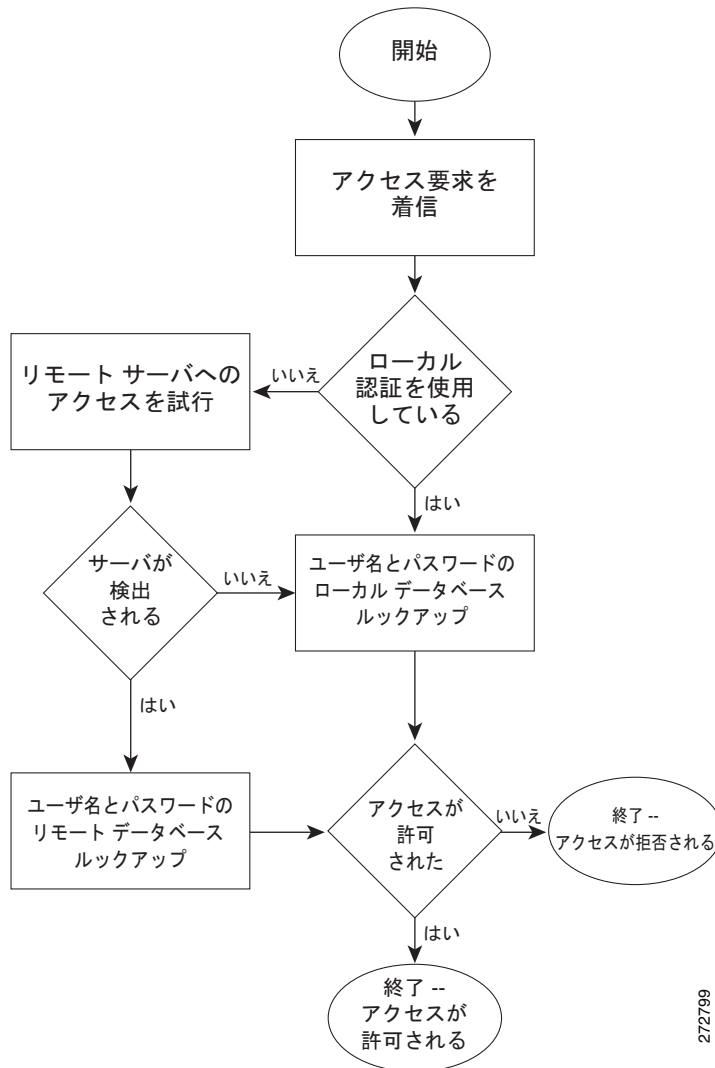
## 認証

認証では、ログインとパスワード、メッセージング、および暗号化によってユーザを識別します。

認証は次のように実行されます。

認証方式	説明
ローカル データベース	ユーザ名またはパスワードのローカル ルックアップ データベースによって次の認証を行います。 <ul style="list-style-type: none"> <li>• コンソール ログイン認証</li> <li>• ユーザ ログイン認証</li> <li>• ユーザ管理セッション アカウンティング</li> </ul>
リモート RADIUS または TACACS+ サーバ	ユーザ名およびパスワードのリモート サーバルックアップ データベースを使用して次の認証を行います。 <ul style="list-style-type: none"> <li>• コンソール ログイン認証</li> <li>• ユーザ ログイン認証</li> <li>• ユーザ管理セッション アカウンティング</li> </ul>
なし	ユーザ名だけで次の認証を行います。 <ul style="list-style-type: none"> <li>• コンソール ログイン認証</li> <li>• ユーザ ログイン認証</li> <li>• ユーザ管理セッション アカウンティング</li> </ul>

図 4-1 ユーザ ログインの認証



## 許可

許可では、ユーザが実行を許可される操作を制限します。

## アカウントティング

アカウントティングでは、すべての SVS 管理セッションを追跡し、ログに記録して管理します。この情報を使用してレポートを生成し、トラブルシューティングや監査に役立てることができます。アカウントティング ログは、ローカルに保存するか、またはリモートの AAA サーバに送信することができます。

## AAA サーバ グループ

リモート AAA サーバ グループは、1 つのリモート AAA サーバが応答できない場合に備えて、フェールオーバーを提供することができます。グループ内の最初のサーバが応答しない場合は、同じグループ内の次のサーバが試行され、サーバが応答するまでこの処理が行われます。これと同じように、複数のサーバグループが相互にフェールオーバーを提供できます。

すべてのリモートサーバグループが応答しない場合は、ローカルデータベースが認証に使用されます。

## AAA の前提条件

リモート AAA サーバを使用する認証では、次の準備が整っている必要があります。

- 少なくとも 1 台の TACACS+ サーバが IP で到達可能になっていること。  
「[TACACS+ サーバホストの設定](#)」(P.6-11) を参照してください。
- SVS が AAA サーバのクライアントとして設定されていること。
- 共有秘密鍵が SVS およびリモート AAA サーバに設定されていること。  
「[共有鍵の設定](#)」の手順 (P.6-9) を参照してください。

## AAA の注意事項および制限事項

Cisco Nexus 1000V は、すべて数字で構成されたユーザ名をサポートしていません。そのため、すべて数字で構成されたローカルユーザ名は作成しません。すべて数字で構成されたユーザ名が AAA サーバ上に存在していて、ログイン時に入力された場合には、そのユーザは SVS で認証されます。

## デフォルト設定

次の表に、AAA のデフォルトを示します。

パラメータ	デフォルト
コンソール認証方式	local
デフォルト認証方式	local
ログイン認証エラーメッセージ	ディセーブル

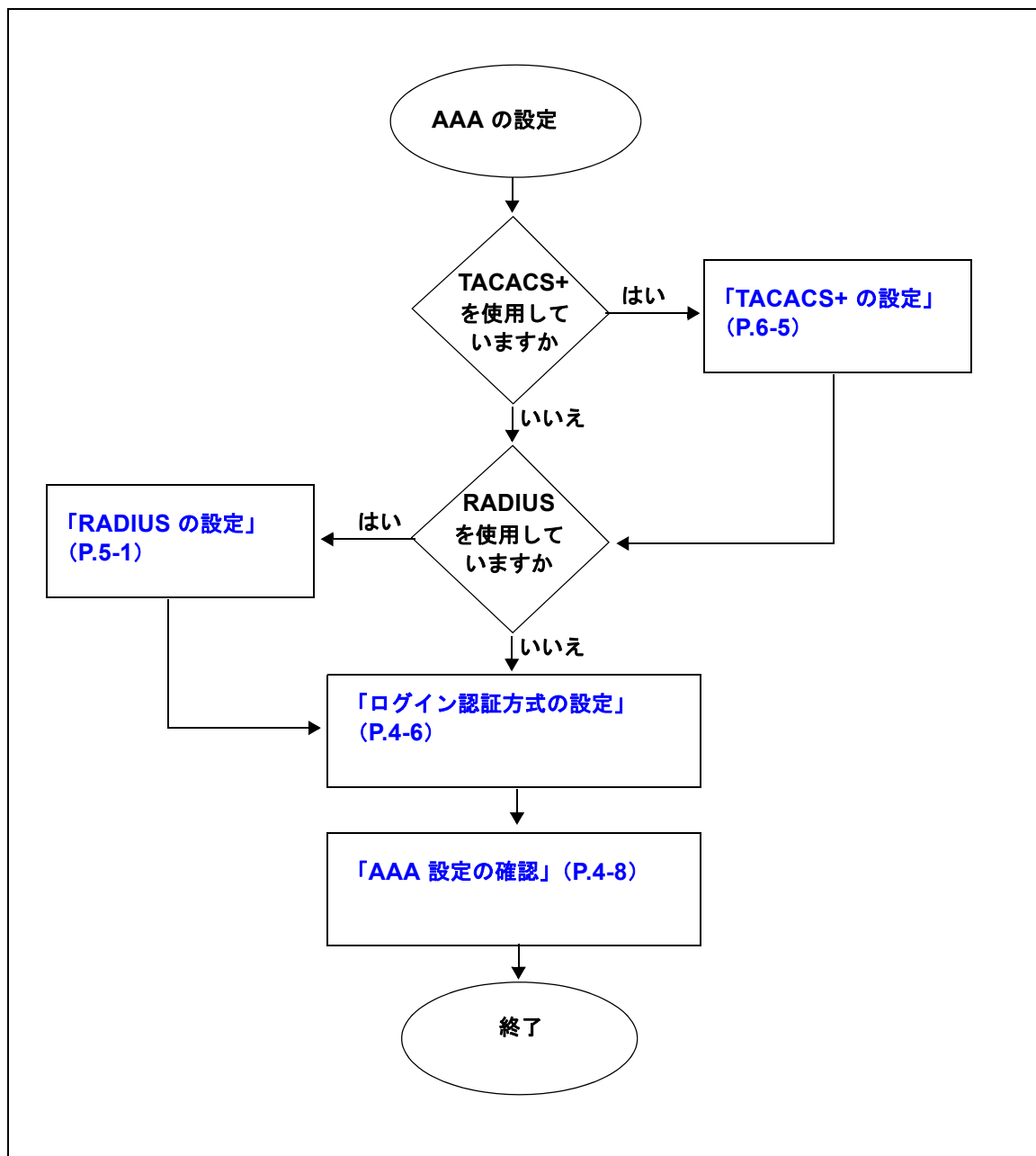
## AAA の設定

ここでは、次の内容について説明します。

- 「[ログイン認証方式の設定](#)」(P.4-6)
- 「[ログイン認証エラーメッセージのイネーブル化](#)」(P.4-7)

AAA を設定するには、次のフローチャートを使用します。

#### フローチャート：AAA の設定



## ログイン認証方式の設定

ログイン認証方式を設定するには、次の手順を実行します。

### 始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしています。
- TACACS+ サーバ グループを使用して認証が行われる場合は、グループが追加済みです。詳細については、「[TACACS+ サーバ グループの設定](#)」(P.6-12) を参照してください。

### 手順の概要

1. `config t`
2. `aaa authentication login {console | default} {group group-list [none] | local | none}`
3. `exit`
4. `show aaa authentication`
5. `copy running-config start-config`

### 手順の詳細

	コマンド	目的
ステップ1	<pre>config t</pre> <p>例: n1000v# config t n1000v(config)#</p>	CLI グローバル コンフィギュレーション モードを開始します。
ステップ2	<pre>aaa authentication login {console   default} {group group-list [none]   local   none}</pre> <p>例: n1000v(config)# aaa authentication login console group tacgroup</p>	<p>コンソールまたはデフォルト ログイン認証方式を設定します。</p> <ul style="list-style-type: none"> <li>• <b>group</b> : サーバ グループによって認証が行われます。</li> <li>– <b>group-list</b> : スペースで区切ったサーバ グループ名のリストです。認証なしの場合は <b>none</b> です。</li> <li>• <b>local</b> : ローカル データベースが認証に使用されます。</li> </ul> <p>(注) デフォルトは <b>local</b> で、方式が設定されていない場合、または設定されたすべての認証方式で応答が得られなかった場合に使用されます。</p> <ul style="list-style-type: none"> <li>• <b>none</b> : ユーザ名によって認証が行われます。</li> </ul>
ステップ3	<pre>exit</pre> <p>例: n1000v(config)# exit n1000v#</p>	CLI グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。

	コマンド	目的
ステップ4	<code>show aaa authentication</code>  例: n1000v# show aaa authentication default: group tacgroup console: group tacgroup n1000v#	(任意) 設定されたログイン認証方式を表示します。
ステップ5	<code>copy running-config startup-config</code>  例: n1000v# copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## ログイン認証エラーメッセージのイネーブル化

リモート AAA サーバが応答しない場合のログイン認証エラーメッセージの表示をイネーブルにするには、次の手順を実行します。

### 始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしています。
- 次に、ログイン認証エラーメッセージを示します。

```
Remote AAA servers unreachable; local authentication done.
Remote AAA servers unreachable; local authentication failed.
```

### 手順の概要

1. `config t`
2. `aaa authentication login error-enable`
3. `exit`
4. `show aaa authentication login error-enable`
5. `copy running-config start-config`

### 手順の詳細

	コマンド	目的
ステップ1	<code>config t</code>  例: n1000v# config t n1000v(config)#	CLI グローバル コンフィギュレーション モードを開始します。
ステップ2	<code>aaa authentication login error-enable</code>  例: n1000v(config)# aaa authentication login error-enable n1000v(config)#	ログイン認証エラーメッセージをイネーブルにします。デフォルトはディセーブルです。

	コマンド	目的
ステップ3	<b>exit</b>  例: n1000v(config)# exit n1000v#	CLI グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ4	<b>show aaa authentication login error-enable</b>  例:  n1000v# show aaa authentication login error-enable enabled n1000v#	(任意) ログイン エラー メッセージの設定を表示します。
ステップ5	<b>copy running-config startup-config</b>  例: n1000v# copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

## AAA 設定の確認

AAA の設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
<b>show aaa authentication [login {error-enable   mschap}]</b>	AAA 認証情報を表示します。 <a href="#">例 4-1 (P.4-8)</a> を参照してください。
<b>show aaa groups</b>	AAA サーバ グループの設定を表示します。
<b>show running-config aaa [all]</b>	実行コンフィギュレーション内の AAA 設定を表示します。 <a href="#">例 4-2 (P.4-8)</a> を参照してください。
<b>show startup-config aaa</b>	スタートアップ コンフィギュレーション内の AAA 設定を表示します。 <a href="#">例 4-3 (P.4-9)</a> を参照してください。

### 例 4-1 show aaa authentication

```
n1000v# show aaa authentication login error-enable
disabled
```

### 例 4-2 show running config aaa

```
n1000v# show running-config aaa all
version 4.0(1)
aaa authentication login default local
aaa accounting default local
no aaa authentication login error-enable
no aaa authentication login mschap enable
no radius-server directed-request
no snmp-server enable traps aaa server-state-change
```



```
no tacacs-server directed-request
n1000v#
```

#### 例 4-3 show startup-config aaa

```
n1000v# show startup-config aaa
version 4.0(1)svs#
```

## AAA 設定例

次に、AAA の設定例を示します。

```
aaa authentication login default group tacacs
aaa authentication login console group tacacs
```

## その他の関連資料

AAA の実装に関する詳細情報については、次を参照してください。

- [「関連資料」 \(P.4-9\)](#)
- [「標準規格」 \(P.4-9\)](#)

## 関連資料

関連項目	マニュアル タイトル
システム管理	『Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)』
CLI	『Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(3)』
TACACS+ セキュリティ プロトコル	<a href="#">第 6 章「TACACS+ の設定」</a>

## 標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

## AAA 機能の履歴

ここでは、AAA のリリース履歴について説明します。

機能名	リリース	機能情報
AAA	4.0	この機能が追加されました。