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 について

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

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されます。キーは、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 が使用されます。

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 設定が作成されます。

- User Telnet または Secure Shell（SSH）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 コンフィギュレーション オプション	関連コマンド
Telnet または SSH ログイン	**aaa authentication login default**
コンソール ログイン	**aaa authentication login console**

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）

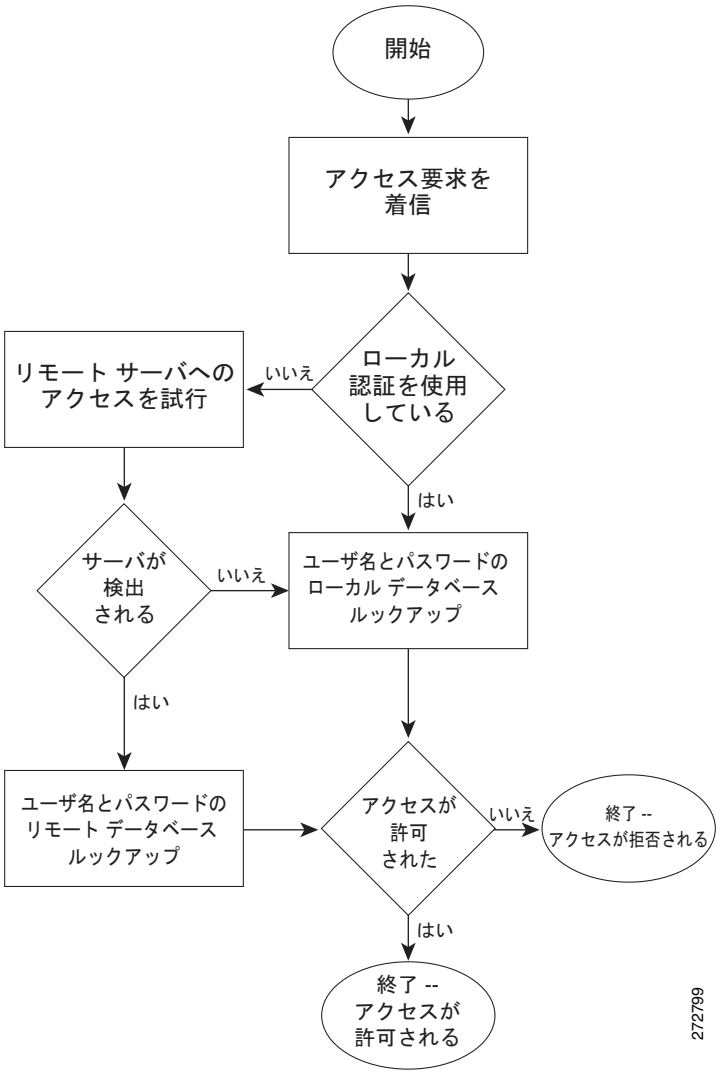
認証

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。

認証方法	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。 • コンソール ログイン認証 • ユーザ ログイン認証 • ユーザ管理セッション アカウンティング
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。 • コンソール ログイン認証 • ユーザ ログイン認証 • ユーザ管理セッション アカウンティング
なし	ユーザ名だけで次の認証を行います。 • コンソール ログイン認証 • ユーザ ログイン認証 • ユーザ管理セッション アカウンティング

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。

アカウンティング

アカウンティングでは、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、トラブルシューティングや監査のためのレポートを生成できます。アカウンティング ログは、ローカルに保存することもできれば、リモート AAA サーバに送信することもできます。

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+ サーバまたは RADIUS サーバが IP で到達可能になっていること。
- VSM が AAA サーバのクライアントとして設定されていること。
- 共有秘密キーが VSM およびリモート AAA サーバに設定されていること。

「共有キーの設定」（P.6-9）の手順を参照してください。

AAA のガイドラインと制限事項

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 Cisco Nexus 1000V 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。

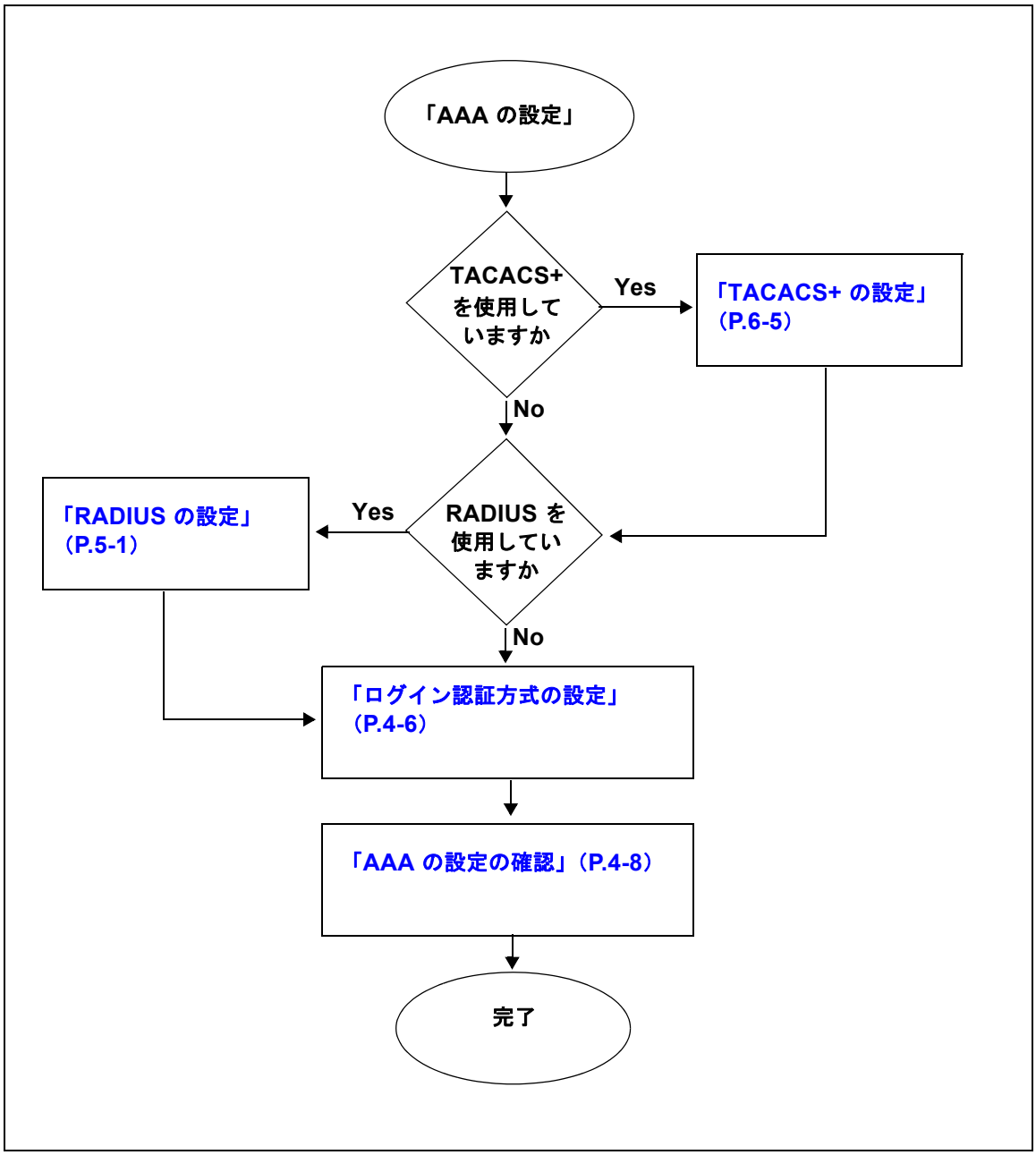
パラメータ	デフォルト
コンソール認証方式	ローカル
デフォルト認証方式	ローカル
ログイン認証失敗メッセージ	ディセーブル

AAA の設定

ここでは、次の内容について説明します。

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。

はじめる前に

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 にログインしていること。
- 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	**config t**
	
	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	**aaa authentication login {console | default}** {**group** *group-list* [**none**]| **local** | **none**} **例：** `n1000v(config)# aaa authentication login console group tacgroup`	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。 • **group**：サーバ グループによって認証が行われます。 – **group-list**：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 none です。 • **local**：ローカル データベースが認証に使用されます。 **（注）** デフォルトは local 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。 • **none**：ユーザ名によって認証が行われます。

ステップ 3	**exit**
	
	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。

	コマンド	目的

ステップ 4	**show aaa authentication**
	
	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	**copy running-config startup-config** **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。

ログイン認証失敗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。

はじめる前に

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 にログインしていること。
- 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	**config t**
	
	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	**aaa authentication login error-enable**
	
	例：
	`n1000v(config)# aaa authentication login error-enable`
	`n1000v(config)#`
		ログイン認証失敗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	**exit** 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	**show aaa authentication login error-enable** 例： n1000v# show aaa authentication login error-enable enabled n1000v#	（任意）ログイン失敗メッセージの設定を表示します。
ステップ 5	**copy running-config startup-config** 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 の設定の確認

AAA の設定情報を表示するには、次のいずれかの作業を行います。

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

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」（P.4-9）

関連資料

関連項目	参照先
システム管理	『*Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(5.1)*』
CLI	『*Cisco Nexus 1000V Installation and Upgrade Guide, Release 4.2(1)SV1(5.1)*』
TACACS+ セキュリティ プロトコル	第 6 章「TACACS+ の設定」

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

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(4)SV1(1)	この機能が導入されました。