AAA（設定と運用）

学習内容

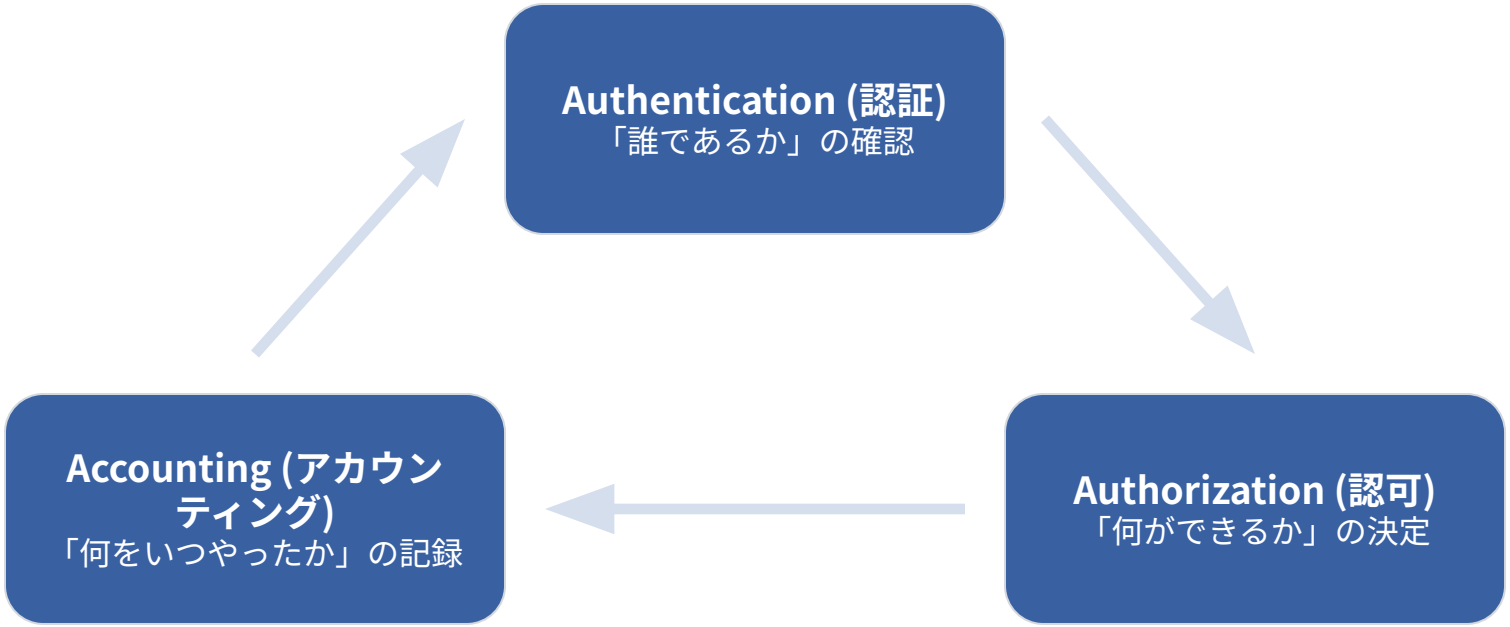
1. AAAの基本と構成要素
2. RADIUSクライアント設定：新旧方式の比較
3. TACACS+クライアント設定：新旧方式の比較
4. AAA認証（Authentication）の設定
5. AAA認可（Authorization）の設定
6. AAAアカウンティング（Accounting）の設定
7. IEEE 802.1X認証におけるAAA設定

01

AAAの基本と構成要素

AAA: ネットワークセキュリティの三本柱

AAAはセキュリティと運用効率を高めるための集中管理の仕組み



02

RADIUSクライアント設定：新旧方式の比較

RADIUS設定：新しい方式 vs レガシー方式

現在は『`radius server` + `aaa group server radius`』の新方式が推奨

新しい設定方法	レガシーな設定方法 (旧IOS)
個別の`radius server`でサーバを登録	`radius-server host`でサーバを直接登録
`aaa group server radius`でサーバグループ化	グループ化はされない
AAA方式リストにグループを指定	AAA方式リストに`group radius`を指定
グループを利用するため柔軟性が高い	設定順に優先順位が決まる

新しいIOSでのRADIUS設定手順

サーバの登録 → グループ化 → AAA方式リストに適用

1. RADIUSサーバの登録 (`radius server config-name`)：アドレス、ポート、共有鍵を定義
2. 認証サーバグループへの登録 (`aaa group server radius group-name`)：登録したサーバをグループに追加
3. AAA方式リストに適用 (`aaa authentication login default group group-name`)：認証・認可・アカウンティングにグループを指定

03

TACACS+クライアント設定：新旧方式の比較

TACACS+設定：新しい方式 vs レガシー方式

TACACS+も『`tacacs server` + `aaa group server tacacs+`』の新方式へ

新しい設定方法	レガシーな設定方法 (旧IOS)
個別の`tacacs server`でサーバを登録	`tacacs-server host`でサーバを直接登録
`aaa group server tacacs+`でサーバグループ化	グループ化はされない
AAA方式リストにグループを指定	AAA方式リストに`group tacacs+`を指定
グループを利用するため柔軟性が高い	設定順に優先順位が決まる

04

AAA認証（Authentication）の設定

AAA認証 (Authentication) の基本

どの認証方法をどの順番で試行するかを定義する

AAAの有効化は必須

最初のコマンドは `aaa new-model`

認証方式リストの作成

`aaa authentication login [default|list-name] method1 method2...` の形式

認証方式の優先順位

method1, method2 の順に**複数試行**される

代表的な認証方式 (Method)

`default` または `list-name` に紐づける認証の選択肢

認証方式	説明
group radius	RADIUSサーバを利用
group tacacs+	TACACS+サーバを利用
local	ローカルDB（`username`コマンド）を利用
enable	`enable password` を使用
line	回線設定の`password`を利用

リストの適用と利用例

リスト名は回線ごとに使い分けられる

`default`リスト: 全ての回線 (VTY, Console, TTY) に自動適用

`list-name`リスト: `line vty` や `line console` で個別に適用 (`login authentication list-name`)

VTYとConsoleで認証方式を分けたい場合にリスト名を使う

ログイン失敗回数の制御: `aaa authentication attempts login 5` などで変更可能

05

AAA認可（Authorization）の設定

AAA認可 (Authorization) の役割

ログイン後に許可される操作範囲（権限）を決定

Exec認可 (exec)

ログイン直後に与えられる権限（特権モード移行など）を決定

Commands認可 (commands)

ユーザが入力する**個々のコマンド**の実行可否を制御

Console認可の有効化

Consoleポートの認可はデフォルト無効。`aaa authorization console`で明示的に有効化が必要

認可リストの適用

`line vty`などで`authorization exec [list-name]`を指定

実務で一般的な認可設定

RADIUSサーバの属性情報（privilege 15など）を適用

設定コマンド:`aaa authorization exec default group GROUP-ISE local`

通常はRADIUS/TACACS+サーバに登録された**権限属性**（例：privilege 15）を適用する

サーバダウン時は`local`に設定されたローカルユーザ情報（`username admin privilege 15 secret...`）を利用

認証リストと認可リストをセットで適用し、一貫性を持たせる

06

AAAアカウンティング（Accounting）の設定

アカウンティングの仕組みと種類

セッション開始と終了をサーバに通知し記録を残す

STEP 1	Execアカウンティング
STEP 2	Dot1xアカウンティング
STEP 3	Networkアカウンティング
STEP 4	Systemアカウンティング

Execアカウンティングの設定と種類

セッションの開始・終了時刻などを記録

設定コマンド: `aaa accounting exec default start-stop group GROUP-ISE`

`start-stop`: セッション開始時と終了時に通知（**推奨**）

`stop-only`: セッション終了時のみ通知

`none`: アカウンティングを行わない

記録には、ユーザ名、ログイン日時、ログイン時間などが含まれる

07

IEEE 802.1X認証におけるAAA設定

802.1XのためのAAA設定ポイント

アクセス制御には必ずRADIUSサーバを利用する

全体有効化

`dot1x system-auth-control` が必須

認証タイプ

`aaa authentication dot1x default group [GROUP]` を使用

認可タイプ

ネットワーク接続認可として `aaa authorization network default group [GROUP]` を使用

802.1XにおけるAAAの流れ

RADIUSサーバと連携しアクセスを制御

クライアントがスイッチポートに接続

スイッチ（認証者）がRADIUSサーバ（認証局）へ認証要求

RADIUSサーバでユーザ認証を実施

認証成功後、サーバから認可情報（VLAN, ACLなど）をスイッチに返信

スイッチが認可情報に基づきポート制御（アクセス許可）