AAA（基礎）

学習内容

1. AAAとは？：基本概念と構成要素
2. AAAの3つの機能と導入の利点
3. Cisco IOSでのAAA認証設定のポイント
4. プロトコルの違い：RADIUSとTACACS+の比較

01

Chapter 1：AAAの基本概念

AAAとは？：セキュリティ管理の基本枠組み

Authentication, Authorization, Accountingの頭文字

Authentication（認証）

ユーザが正規の利用者か確認

Authorization（認可）

許可する操作やサービスを制御

Accounting（アカウンティング）

操作や接続情報を記録・監査

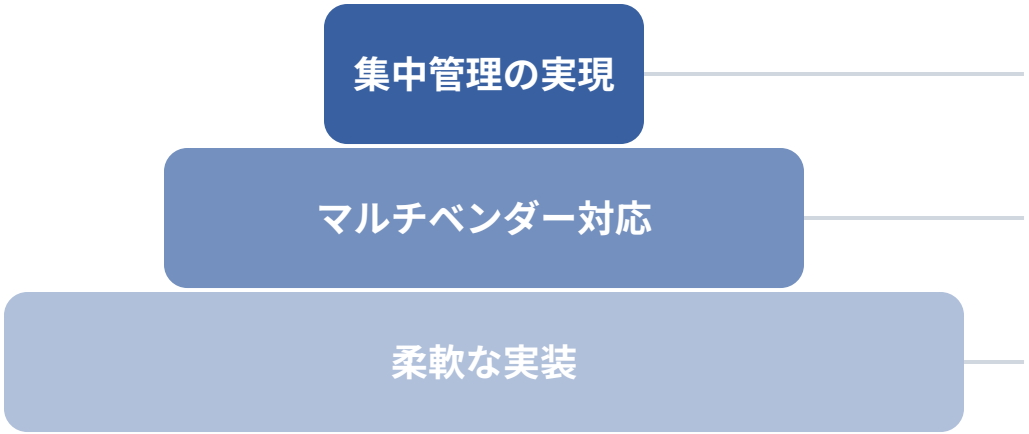
AAAの3つの機能：何を行い、何を制御するか

認証成功後に認可とアカウンティングが続く

認証 (Authentication)	認可 (Authorization)	アカウンティング (Accounting)
ユーザID・パスワードやデジタル証明書などの**資格情報**を検証する仕組みです。チャレンジ/レスポンス方式や暗号化通信も利用されます。	認証成功者に対し「どの操作やサービスを許可するか」を制御します。発行できるコマンド制限や、**ネットワークへのアクセス範囲**を絞ることが可能です。	認証されたユーザが行った操作や接続情報を記録します。**ログイン・ログアウト履歴**や入力コマンドを収集し、監査やレポート作成に利用されます。

AAA導入の主要な利点

セキュリティポリシーの統一と運用効率の向上



TACACS+やRADIUSサーバでユーザ情報を**一元管理**。運用効率が向上し、ポリシーを統一

標準規格であるRADIUSがサポートされ、**他社製RADIUSサーバ**とも連携可能

リモートサーバ認証に加え、小規模向けにローカル認証も利用可能

02

Chapter 2：Cisco IOSでのAAA認証設定

Cisco IOSでのAAA認証設定の3要素

認証を設定する際に決定すべき要素

1. 認証タイプ：対象となるアクセス種別（login, dot1x, enable, ppp）を選択
2. リスト：設定を適用する回線範囲（defaultまたは任意のリスト名）を定義
3. 認証方式：どのデータベース（サーバグループ, radius, tacacs+, local, none）を参照するか指定

03

Chapter 3：RADIUS vs TACACS+の徹底比較

RADIUSとTACACS+の基本機能比較

設計思想と動作の仕組みに明確な違いがある

RADIUS		TACACS+
IETF標準	プロトコル	Cisco独自
UDP 1812/1813	トランスポート層	TCP 49
パスワード情報のみ	暗号化	パケット全体
認証/認可は一体化	AAAの分離	**完全分離**

ユースケースと適用範囲の明確な違い

用途に応じたプロトコル選択が重要

RADIUSの主な特徴

IEEE 802.1X認証で使用できる唯一のプロトコル

マルチベンダー環境でのネットワークアクセス認証に最適

VLAN番号やACLなどの属性情報付与が可能

通信フローが比較的シンプル

TACACS+の主な特徴

コマンドごとの詳細な認可制御が可能

ネットワーク機器の**管理アクセス**認証に最適

認証・認可・アカウンティングが完全に独立

管理者の操作履歴を細かく記録（アカウンティング）