SNMP

学習内容

1. SNMPの基本概念と構成要素
2. SNMPを支えるコア技術（MIB/RMON）
3. SNMPコミュニティとアクセス制御
4. SNMPのバージョンとセキュリティ強化
5. SNMPv1/v2c 設定の重要ポイント（Cisco例）
6. SNMPv3の特徴と高度な構成

01

SNMPの基本概念と構成要素

SNMPとは何か？その役割

ネットワーク機器を監視・制御するための標準プロトコル

SNMP（**Simple Network Management Protocol**）は、ルータ、スイッチ、サーバなどの**通信機器をネットワーク経由で監視・制御**するためのアプリケーション層プロトコル

目的は、ネットワーク障害発生時、**どの機器に問題があるかを迅速に特定**し、障害対応に役立てること

SNMPの構成要素：マネージャとエージェント

「管理する側」と「管理される側」の役割分担

SNMPマネージャ（監視側）

情報要求や監視を**行う側**

監視結果の集約、**可視化**を担当

代表例: net-snmp, JP1/NNMi, TWSNMP Manager

SNMPエージェント（被監視側）

マネージャの要求に**応答する側**

機器の状態変化をマネージャに通知（トラップ）

搭載機器: ルータ、スイッチ、サーバなど

SNMPの通信ポート

問い合わせと通知で異なるUDPポートを使用

1. SNMPエージェント（ルータ・スイッチなど）: **UDPポート161**を使用
2. SNMPマネージャ（監視サーバーなど）: **UDPポート162**を使用
3. マネージャ → エージェントへの問い合わせはポート161宛
4. エージェント → マネージャへのトラップ通知はポート162宛

02

SNMPを支えるコア技術（MIB/RMON）

MIB（Management Information Base）とは

機器情報を格納するデータベース

情報の格納庫

SNMPエージェントが持つ機器情報の**データベース**

ツリー構造とOID

情報は**ツリー構造**で管理され、**OID**（オブジェクトID）で識別される

標準MIBと拡張MIB

標準MIB（例: MIB2）とベンダ独自の**拡張MIB**がある

RMON（Remote Monitoring）による拡張

ネットワーク回線全体のトラフィック監視を実現

RMONは、SNMPを拡張してLANの通信状況を**遠隔監視**する仕組み

MIBが**「機器単体」**の監視情報を提供するのに対し、RMONは**「ネットワーク回線全体」**のトラフィック統計情報を取得可能

ルータなどのインターフェースに組み込まれ、セグメント単位で統計情報を収集する

03

SNMPメッセージとコミュニティ

SNMPメッセージの種類（v1/v2c）

情報取得、設定変更、応答、通知の4つの基本動作

メッセージ	送信側	内容
Get Request	マネージャ	OIDを指定して情報を要求
Set Request	マネージャ	OIDを指定してエージェントの**設定を変更**
Get Response	エージェント	マネージャの要求に応答して値を返す
TRAP	エージェント	機器の状態変化をマネージャに通知

SNMPコミュニティの役割

マネージャとエージェント間のアクセス制御

監視グループの定義

SNMPで管理されるネットワークの**グループ名**のようなもの

アクセス権限の分離

コミュニティ名が一致した機器同士のみ情報交換が可能

RO（Read-only）

MIBへの**読み取りのみ**許可する権限

RW（Read-write）

MIBへの**読み取りと書き込み**を許可する権限

04

SNMPのバージョンとセキュリティ強化

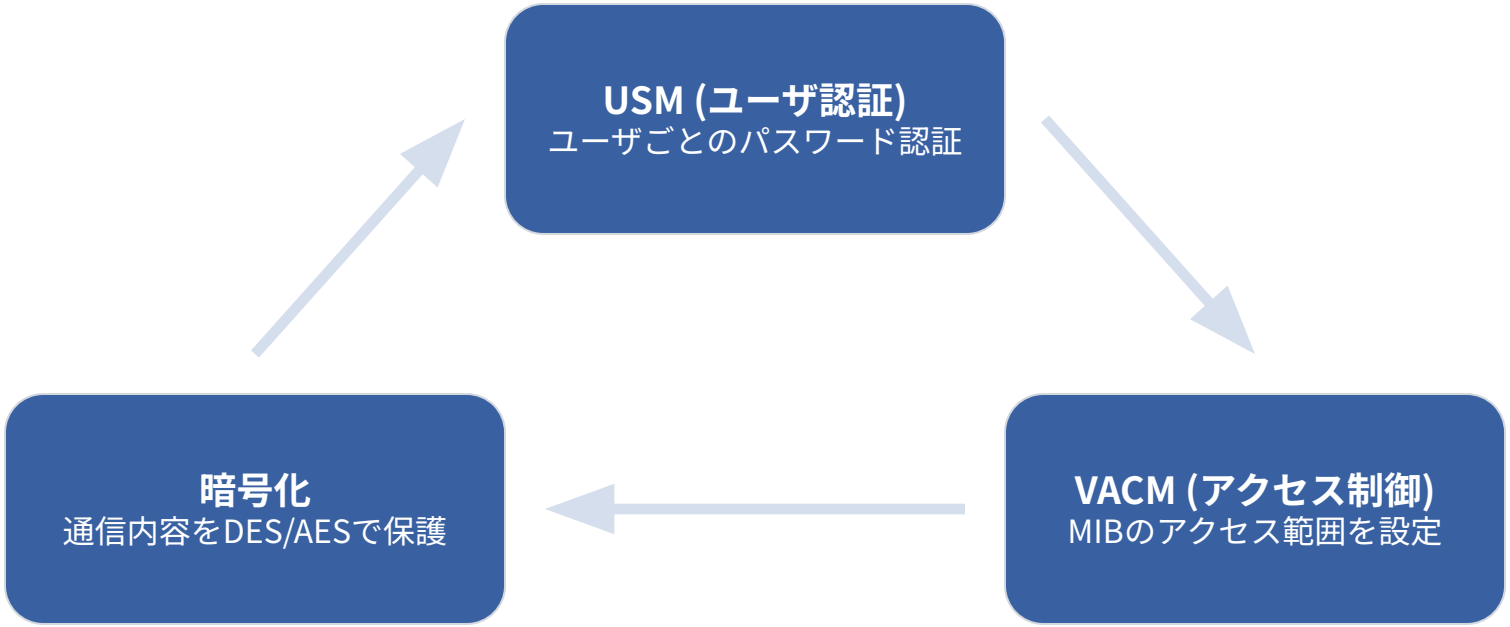
SNMPv1, v2c, v3の比較

セキュリティ機能の変遷

v1/v2c (平文認証)		v3 (パスワード認証/暗号化)
コミュニティ名 (平文)	認証方式	ユーザ単位のパスワード認証
なし	暗号化	DES/AESによる暗号化
低	安全性	高 (実運用推奨)
v1: なし / v2c: あり	トラップ再送確認	あり

SNMPv3のセキュリティ機能

3つの鍵となる仕組み



05

SNMPv1/v2c 設定の重要ポイント（Cisco例）

v1/v2cの基本設定コマンド

読み取り、書き込み、トラップの3点セット

読み取り専用設定

snmp-server community Public01 ro (MIB取得のみ許可)

書き込み可能設定

snmp-server community Private01 rw (設定変更も可能)

Trap送信先設定

snmp-server host [IP] version 2c Public01

SNMPトラップの有効化と限定

イベント発生時の能動的通知

Trap送信を有効化: **snmp-server enable traps**

特定のイベントのみを通知対象とすることが可能（例: **snmp-server enable traps snmp linkdown**）

セキュリティ向上のため、**ACLと組み合わせてマネージャホストを限定**できる

06

SNMPv3の特徴と高度な構成

SNMPv3の設定手順（グループとユーザ）

認証とアクセス制御を構築する流れ

ビューを定義（snmp-server view）

→

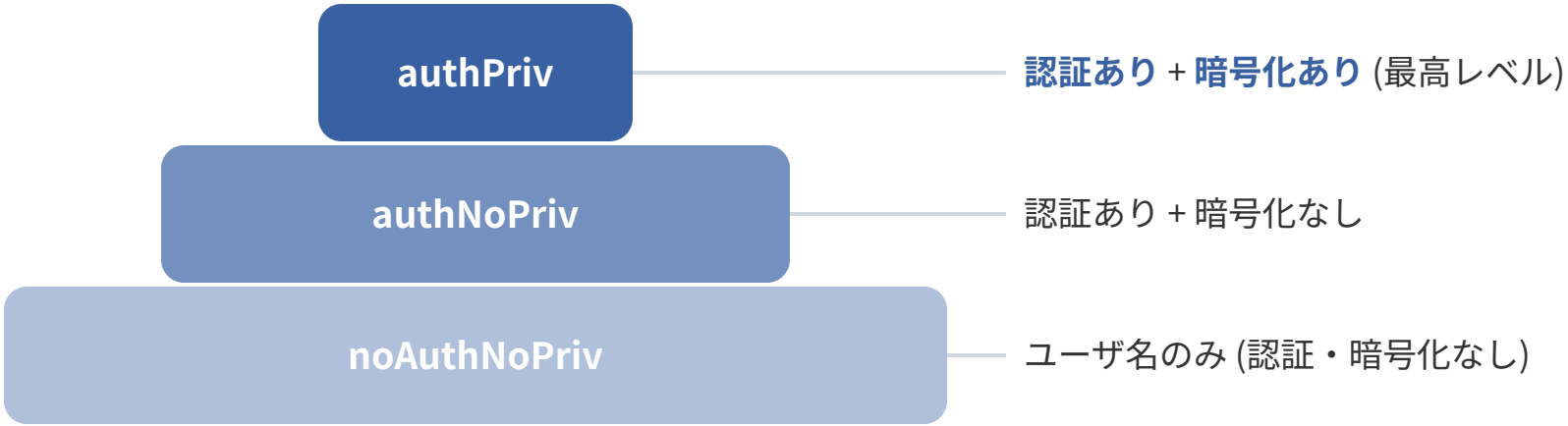
グループを定義しビューとセキュリティレベルを紐づけ（snmp-server group）

→

ユーザを作成しグループに所属させ認証/暗号化を設定（snmp-server user）

SNMPv3のセキュリティレベル

ユーザごとに設定可能な3段階のレベル



試験対策重要ポイントまとめ

必ず押さえておくべき3大要素

デフォルト設定

SNMPは無効

バージョン指定なし→v1

v1/v2c設定

ro/rwとホスト設定

hostとenable trapsはセット

v3セキュリティ

authPrivを推奨

ユーザ・グループ・ビューの関連