L2セキュリティ（Catalyst ACL）

学習内容

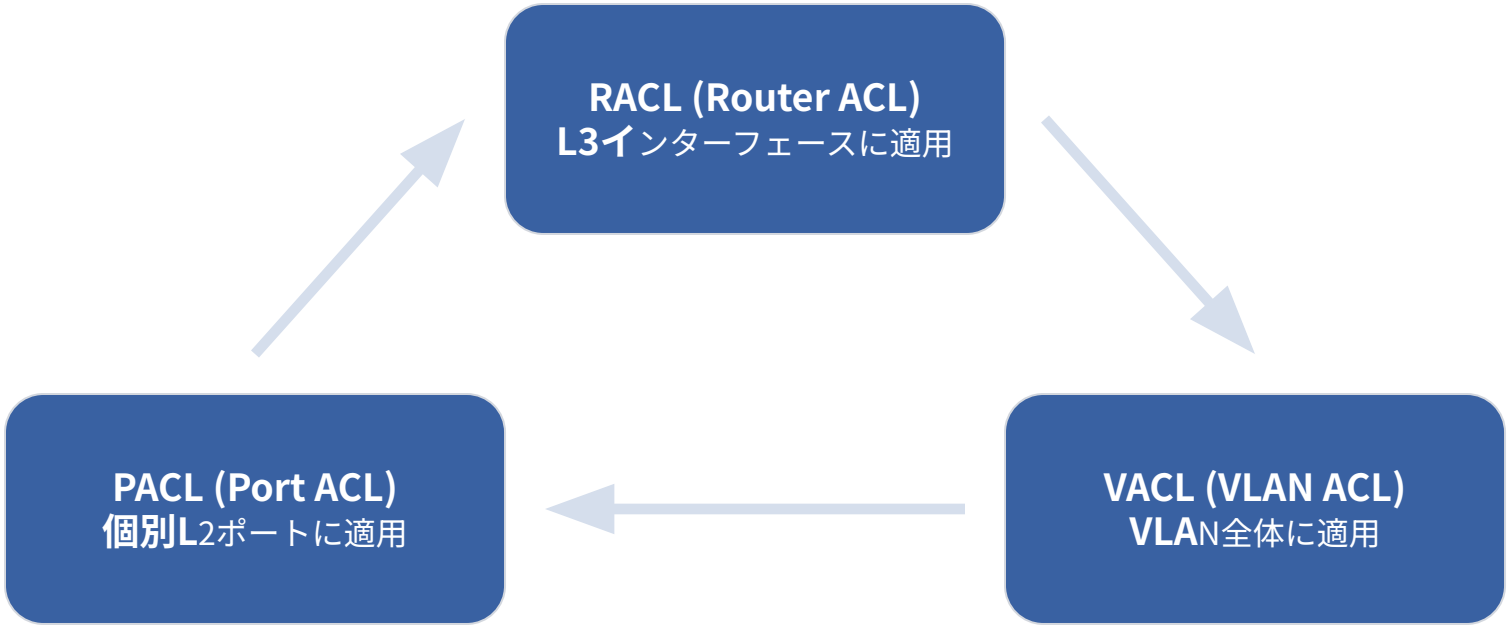
1. Catalyst ACLの全体像と種類
2. RACL（Router ACL）の仕組みと特徴
3. VACL（VLAN ACL）の仕組みと設定
4. PACL（Port ACL）の仕組みと設定
5. 重要：ACLの評価優先順位

01

Catalyst ACLの全体像と種類

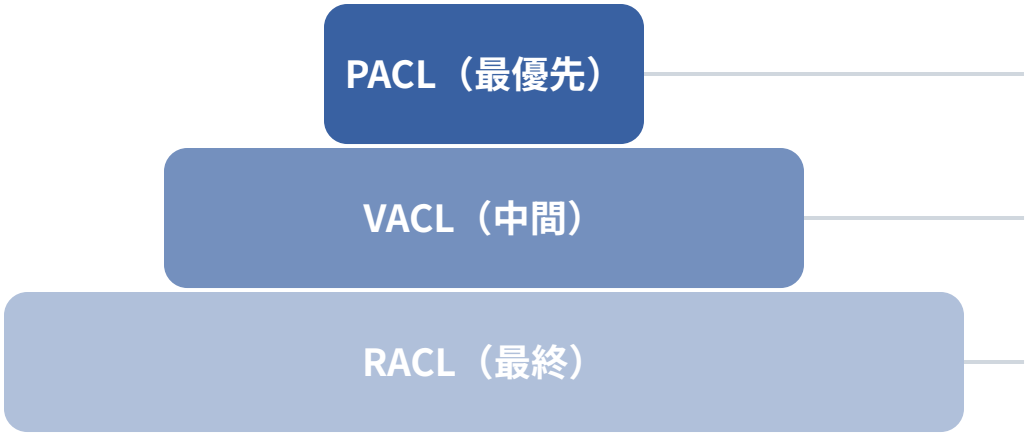
Catalystスイッチにおける ACLの3種類

適用範囲と対象が異なる3つの制御リスト



ACLの評価優先順位（試験重要）

トラフィックが通過する際の制御リスト評価順序



Port ACL: 物理ポートで最初に評価される

VLAN ACL: VLAN全体で次に評価される

Router ACL: L3ルーティング時に最後に評価される

02

RACL（Router ACL）の仕組みと特徴

RACLの適用対象と特徴

CiscoルータのACLとほぼ同等の動作

適用対象

SVI（VLANインターフェース）や**ルーテッドポート**といったL3インターフェース

フィルタ対象

IPルーティングを通過するL3トラフィック

試験でのポイント

ルータACLと同様に、**ブリッジング通信には適用できない**

RACL 設定例の構造

L3インターフェースへのアクセスリスト適用

ACL本体を作成し、許可/拒否条件を定義する（`access-list 101 permit...`）

ACLを適用したいL3インターフェースへ移動する（`interface gigabitethernet 0/1` や `interface vlan 10`）

インターフェース上でACLを適用する（`ip access-group ACL番号 in/out`）

適用方向はルーティングを基準にした**INまたはOUT**で指定する

03

VACL（VLAN ACL）の仕組みと設定

VACLの広範な適用範囲

同一VLAN内のL2通信にも適用可能

ルーティング通信

異なるVLAN間のL3トラフィック

ブリッジング通信

同一VLAN内のホスト間L2トラフィック

非IPトラフィック（MACリスト利用時）

VACLの設定手順（VLANアクセスマップ）

通常のACL適用とは異なる3ステップ

1. 対象トラフィックを定義（IPまたはMACアクセスリストを作成）
2. VLANアクセスマップを定義（matchでトラフィックを、actionでforward/dropを設定）
3. VLANへ適用（`vlan filter V-MAP vlan-list [VLAN ID]`）

VACLで利用できるアクセスリスト

L3/L2通信制御のための構成要素

IPアクセスリスト		MACアクセスリスト
IPv4/IPv6パケット	対象プロトコル	イーサネットフレーム
IPアドレス、ポート番号	フィルタ基準	MACアドレス、EtherType
IP通信	制御対象	**非IP通信**を含むL2通信

04

PACL（Port ACL）の仕組みと設定

PACLの適用対象と特徴

物理ポート単位で適用されるACL

適用範囲	フィルタ対象	処理性能
個別のL2ポート（アクセス、トランク、EtherChannel）の着信トラフィックのみ	VACLと同様に**ブリッジング**と**ルーティング**の両方に適用可能	ハードウェア（TCAM）処理により**高速**に動作する

PACLの設定例の構造

L2ポートへのアクセスリスト適用

アクセスリスト本体を作成する（IPまたはMACアクセスリスト）

ACLを適用したいL2インターフェースへ移動する（`interface gigabitethernet 0/1`）

インターフェース上でACLを適用する（`ip access-group ACL番号 in` または `mac access-group ACL名 in`）

適用方向は**着信（in）のみ**であり、送信方向（out）は指定できない

PACLの動作モード

RACLやVACLとの組み合わせ方法

マージモード（デフォルト）

PACL → VACL → RACLの順で評価される

複数のACLを併用して制御する場合に利用

優先ポートモード

PACLのみが有効になり、VACL/RACLは無効化される

トランクポートで使用する場合など、単独制御したい場合に選択

05

ACLの評価優先順位の再確認

ACLの評価フロー（PACL/VACL/RACL）

トラフィック処理時の制御リスト評価の順番