ACL（種類）

学習内容

1. 標準ACL（Standard ACL）の基本
2. 拡張ACL（Extended ACL）の基本と応用
3. 名前付きACL（Named ACL）による運用効率化
4. ACL設計・運用における重要ポイント

01

標準ACLの基本と設定

標準ACLとは？：送信元IPアドレスのみで判断

パケットの「どこから来たか」だけを見て制御する

標準ACLは、パケットの**送信元IPアドレス**だけを基準に通すか止めるかを判断する仕組み

通信の中身（プロトコルやポート）や宛先は見ず、フィルタリング基準が非常にシンプル

番号付きACL（1-99, 1300-1999）と**名前付きACL**が存在する

標準ACLの作成コマンドと引数

番号付き標準ACLの基本設定

引数	説明	設定例
番号	ACL番号。通常1〜99を使用	access-list **1**
permit/deny	パケットを許可(permit)するか拒否(deny)するか	access-list 1 **permit**
送信元アドレス	フィルタ対象となる送信元IPアドレス	access-list 1 permit **192.168.0.0**
ワイルドカード	許可／拒否する範囲を指定。省略時は0.0.0.0	access-list 1 permit 192.168.0.0 **0.0.0.255**

ACL設定の最重要ルール：暗黙のDeny Any

パケットフィルタリングの基本原則

暗黙のDeny Any
作成した条件文に一致しなかったパケットは、最後に自動的に追加される**全拒否**ルール（暗黙のdeny any）により全て捨てられる

通信途絶を避ける
特定の通信を拒否したい場合でも、その後に必要な通信を許可する『permit any』を明示的に追加しないと、全ての通信が遮断される危険がある

インターフェースへの適用
作成したACLは、`ip access-group 番号 [in | out]` コマンドでインターフェースに適用して初めて有効になる

02

拡張ACL：より詳細な制御

拡張ACLで可能な詳細制御

フィルタリングの基準となる5つの要素

送信元IPアドレス	宛先IPアドレス	プロトコル
どのネットワーク、ホストから来たか	どのネットワーク、ホストへ向かうか	TCP、UDP、ICMPなどの種類

送信元ポート番号	宛先ポート番号
クライアント側が使用するポート	サーバー側が使用するポート（例: 80, 23）

標準ACLと拡張ACLの比較

機能と配置場所の違い

標準ACL（番号: 1-99）	拡張ACL（番号: 100-199）
制御基準：**送信元IPアドレスのみ**	制御基準：**送信元/宛先IPアドレス、プロトコル、ポート番号**
設定がシンプルで分かりやすい	設定が複雑だが、詳細な制御が可能
できるだけ宛先側のルータに配置するのが原則	**できるだけ送信元側**のルータに配置するのが原則

03

名前付きACL：運用効率化

番号付きACLの課題と名前付きACLの利点

運用上の大きな違い

番号付きACL	名前付きACL
番号だけでは役割が不明確	ACLに**直感的な名前**を付けられる
特定の行を消せない（削除すると全行消える）	**シーケンス番号**で特定の行を個別に編集・削除可能
大規模な編集が困難	大規模ネットワークでの管理が容易

名前付きACLの作成と編集

シーケンス番号を活用した設定

1. アクセスリストの種類と名前を指定してACL設定モードに入る（例: `ip access-list standard WEB_ACCESS`）
2. ACL設定モードで**シーケンス番号**を付与し、許可/拒否の条件文を作成する（例: `10 permit host 192.168.1.1`）
3. 後から特定の行を削除したい場合は、シーケンス番号を指定して `no` コマンドを実行する（例: `no 10`）
4. インターフェースへの適用は、`ip access-group 名前 [in | out]` で実行する