ACL（設定と活用）

学習内容

1. ACLの状態を確認する基本コマンド
2. 暗黙のdeny anyの理解とパケットの一致数
3. シーケンス番号を活用したACLの編集（追加・削除）
4. VTY（管理アクセス）へのACL適用

01

1. ACLの状態を確認する基本コマンド

ACLの状態を確認する基本コマンド

設定状況の確認とプロトコルによる使い分け

全てのACLを一覧表示する基本コマンドは `show access-lists`。

特定のACLのみを確認したい場合は、`show access-lists **番号または名前**` を指定。

IPプロトコルに関するACLのみを表示する場合は `show ip access-lists` を用いる。

インターフェースへの適用状況は `show ip interface` や `show running-config` で確認可能。

ACLの実行結果 – パケット一致数の確認

ACLのルールごとのヒット数（マッチ数）を把握する

コマンド

show access-lists

基本

表示結果

～ matches

パケット数

シーケンス番号

条件文ごと

識別子

暗黙のDeny

必ず存在

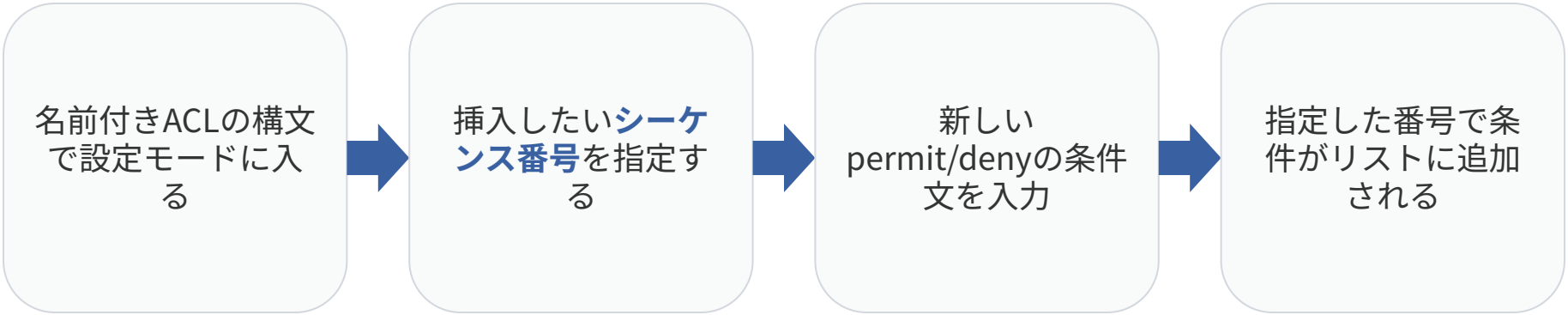
表示なし

02

2. シーケンス番号を活用したACLの編集

シーケンス番号による条件の追加（挿入）

任意の位置にルールを挿入するための設定手順



ACLの部分削除：正しい手順と落とし穴

ACL全体を消さずに特定のルールだけを削除する

✅ 正しい手順（部分削除）

show access-listsで**シーケンス番号**を確認

ip access-list standard/extended でACL設定モードに入る

no [シーケンス番号] で**該当行のみ**を削除

❌ 誤った手順（全体削除）

no access-list [ACL番号] [条件文] と入力

ACL全体が削除されてしまう落とし穴

特に番号付きACLでこの誤操作に注意

03

3. VTY（管理アクセス）へのACL適用

VTY回線とは何か？

ルータへの管理アクセス経路の制御

管理アクセス制御

ACLは通常通過トラフィック制御に使うが、ルータへのTelnet/SSH接続も制御可能

VTYポート経由

これらの管理アクセスは**VTY（Virtual Teletype）**ポートを必ず通過する

設定の簡素化

VTYに標準ACLを適用すれば、単一設定で**ルータ全体**の管理アクセスを制御できる

VTYへのアクセス制御の設定手順（インバウンド）

ルータへの接続元を制限する一般的な設定

1. 許可/拒否したい送信元アドレスを定義する**標準ACL**を作成
2. ACLを適用したいVTY回線（例: vty 0 15）に入る
3. `access-class [ACL番号] in` コマンドで適用（ルータへ入る通信）

アウトバウンドでのVTYアクセス制御

ルータ自身が生成する通信（Telnet/SSH）の制御

目的の逆転: 通常のinboundとは異なり、ルータ自身が他の機器へTelnet/SSHする際の通信を制御。

判断基準が変化: 標準ACLは送信元アドレスで判断するが、この場合は**宛先アドレス**で判断する。

設定例: `access-list 15 deny 10.1.1.1` → ルータから10.1.1.1へのTelnet接続を禁止。

適用コマンド: `access-class [ACL番号] out`（ルータから出ていく通信）