ACL（基礎）

学習内容

ACLの基礎知識から、主要な種類、そして現場で役立つ注意事項までを解説します。

1. ACLとは？基本概念の整理
2. ACLの2つの種類：標準ACLと拡張ACL
3. ACLの適用方向（インバウンドとアウトバウンド）
4. ACL設定時の最重要注意事項
5. ワイルドカードマスクの仕組みと計算方法

01

1. ACLとは？基本概念の整理

ACL（アクセスコントロールリスト）の役割

ルータに設定し、ネットワークトラフィックの許可/拒否を制御する「門番」機能

ルータに設定する、パケットの通過可否を決定する**ルールリスト**

リスト内のルールは**上から順番に照合**され、最初に一致したルールが適用される

一度ルールが適用されたパケットは、それ以降のルールは**無視される**（順序が極めて重要）

ACLにおける「暗黙のdeny any」の原則

リストの最後には必ず「すべてのパケットを拒否」という隠れたルールが存在する

ルールの末尾に自動追加

設定には表示されないが、ACLの**末尾で必ず動作**している

「許可」がなければ拒否

明示的に『許可』ルールを書かない限り、全ての通信は最終的にこの暗黙のルールにより**拒否**される

試験頻出ポイント

特定の通信を許可したい場合、拒否ルールの後に**明示的な許可ルール**が必要となる

02

2. ACLの2つの種類

標準ACLと拡張ACLの比較

判定基準の違いを理解することが、適切なACL選択の鍵となります。

標準ACL		拡張ACL
送信元IPアドレス	主な判定基準	送信元/宛先IPアドレス
不可（通信全体）	詳細制御の可否	可（プロトコル/ポート番号）
宛先に近い場所	適用場所（原則）	送信元に近い場所

03

3. ACLの適用方向

インバウンド (IN) と アウトバウンド (OUT) の違い

パケットがインターフェースに「入る」か「出る」かで、適用タイミングが異なります。

インバウンド (IN)	アウトバウンド (OUT)
インターフェースに**入ってくる**パケットに対して適用	インターフェースから**出ていく**パケットに対して適用
ルータがパケットを受信し、ルーティングする前にチェック	ルーティングテーブルで転送先が決定された**後**にチェック
拒否されたパケットは即座に**破棄**される	ルータ自身が生成したパケットは**対象外**となる

04

4. ACL設定時の最重要注意事項

ACL設定の鉄則：ルールの処理順序

狭い条件を先に、広い条件を後に書くのが、意図した動作を実現する鉄則です。

全件チェックではない

一致した時点で処理決定され、**残りのルールは無視**される

狭い条件を先に

特定のホストやネットワークなど、**限定的な条件**を上位に記述する

広い条件を後に

ネットワーク全体や『any』など、**広範囲の条件**を下位に記述する

ACLのその他重要事項

ACLの適用数や適用場所の原則についても確認しましょう。

適用できる数

1つのインターフェースには、INで1つ、OUTで1つ、合計**2つのACL**を適用可能

標準ACLの適用場所

送信元IPしか見ないため、誤って広い範囲を止めないよう**宛先に近い場所**が推奨

拡張ACLの適用場所

詳細な制御が可能なため、無駄なトラフィックを減らすため**送信元に近い場所**が推奨

ルータ自身

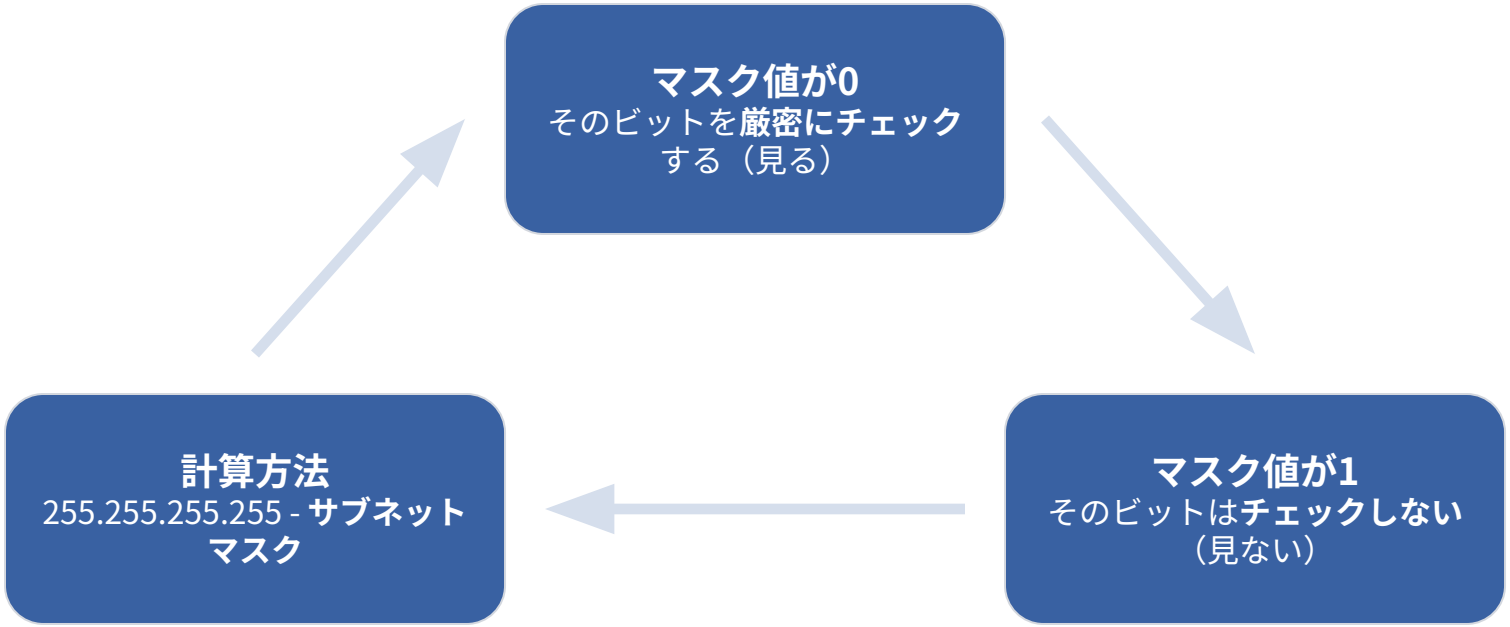
ルータが生成するパケット（ルーティング更新など）には、**アウトバウンドACLは適用されない**

05

5. ワイルドカードマスクの仕組み

ワイルドカードマスクの基本ルール

サブネットマスクとは逆の意味を持つ「見る」「見ない」の概念



ワイルドカードマスクの指定例と省略形

ホストやネットワーク、全体を指定する場合の表記方法を整理

指定したい対象	IPアドレス	ワイルドカードマスク	省略形
特定のホスト1台	172.16.1.1	0.0.0.0	host 172.16.1.1
/24のネットワーク	172.16.1.0	0.0.0.255	なし
全てのIPアドレス	0.0.0.0	255.255.255.255	any