情報セキュリティ基礎

第３回　TCP/IPの基礎と脅威

藤本 章宏

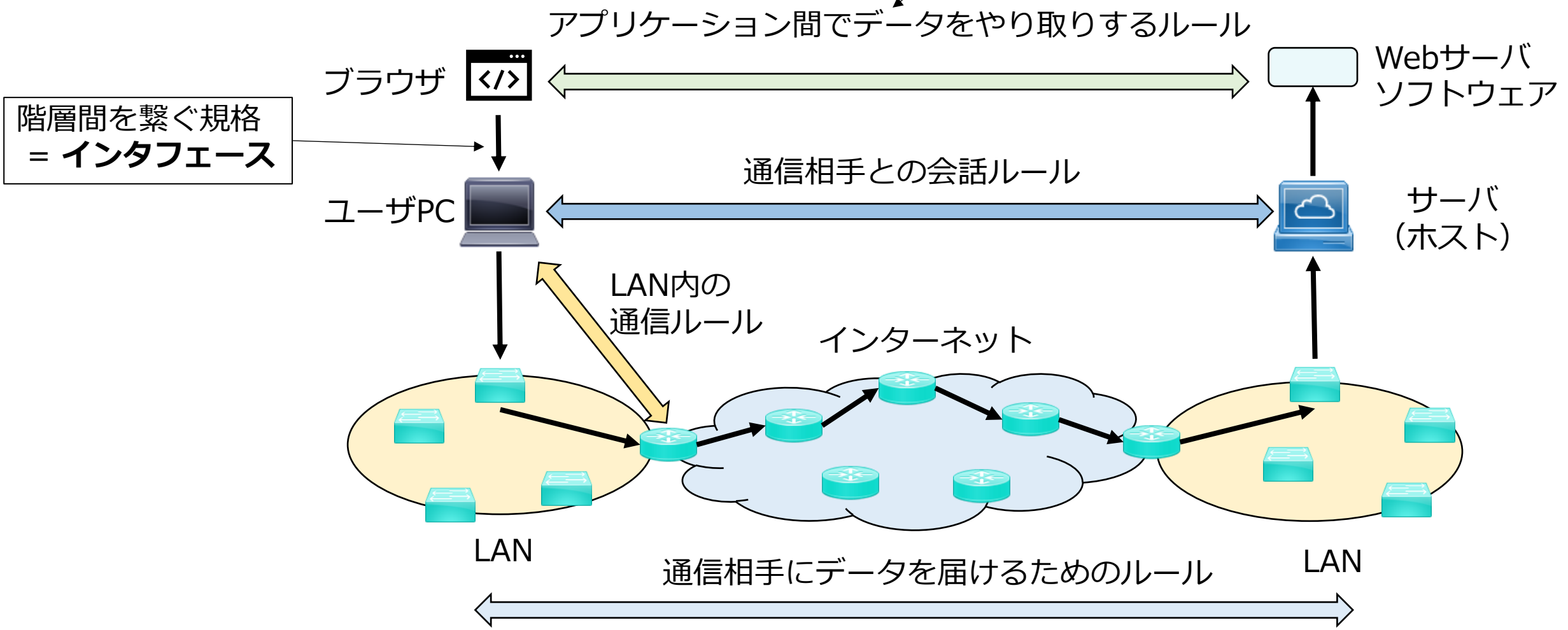
今回の目標

- インターネットにおける通信の流れと，IP通信の基本的な動作を確認する
- 簡単な演習を通し，IP通信に関する攻撃手法の基礎的な手口を知る

階層モデルとプロトコル

機能を階層化し，設計の複雑度を軽減
⇨各層は，他の階層の詳細を知らずに済む

通信するための約束事
＝ **プロトコル**



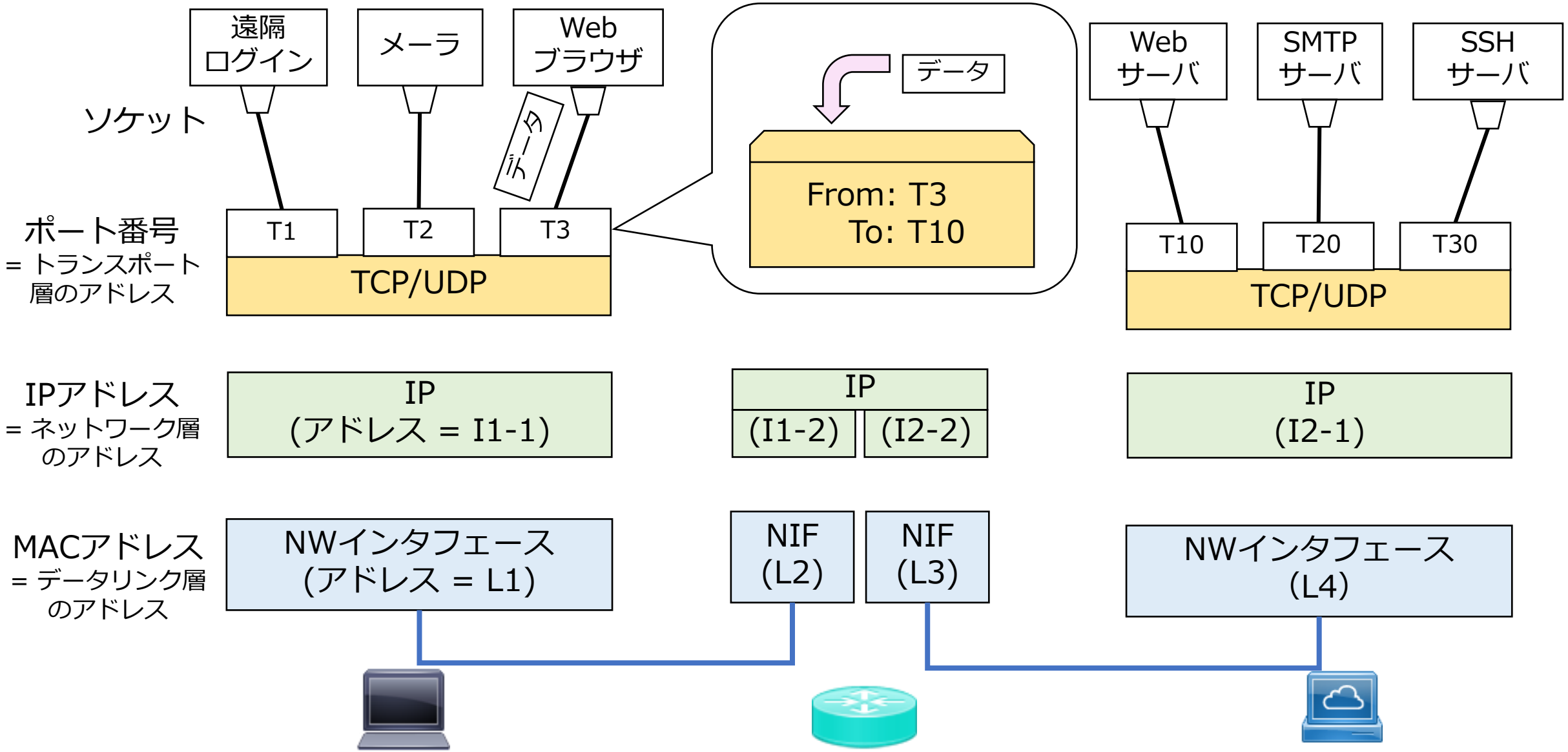
TCP/IP 4階層モデル

TCP/IP：インターネットで標準的に利用されるプロトコル群

- 中心的な役割を果たすTCPとIPの名前をとってTCP/IPと呼ばれる
- ネットワークを４つの機能からなる階層モデルとして定義し，プロトコル群を整理

階層名	提供するサービス	定義されているプロトコル
アプリケーション層	ユーザ向け/システム向けのサービスを提供	TELNET, FTP, DNS等
トランスポート層	エンド間の通信サービスを提供	TCP, UDP
インターネット層	インターネットを通じてパケットを宛先に届ける機能を提供	IP，ICMP, IGMP
リンク層（ネットワークインタフェース層）	直接接続されているネットワークで通信するための機能を提供	（個々のネットワーク規格におけるIPパケットの伝送）

TCP/IPにおけるアドレス



TCP/IPにおけるアドレス

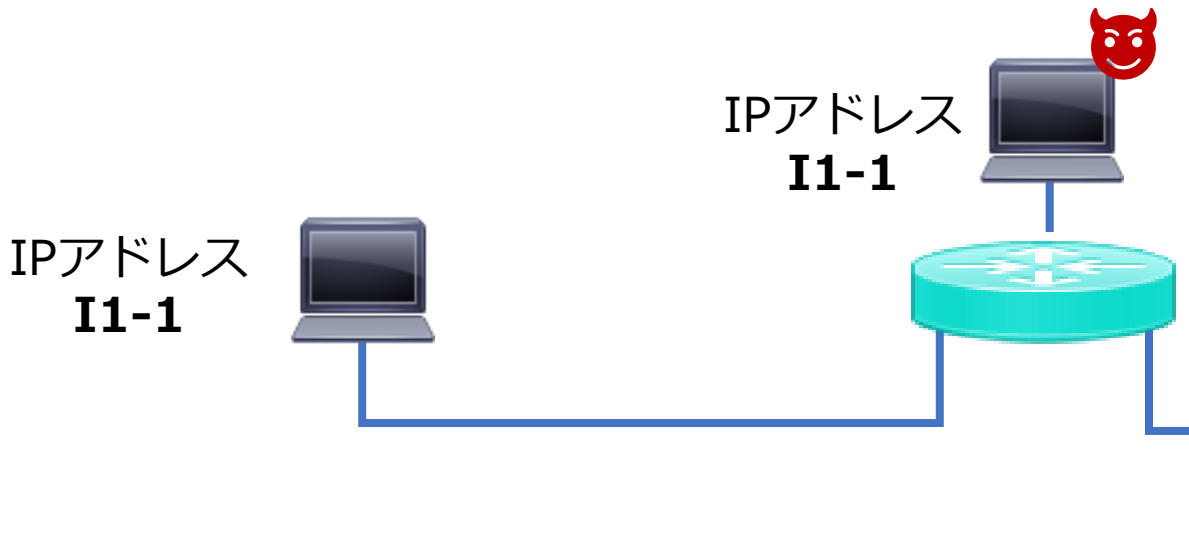
通信するためには３種類のアドレス

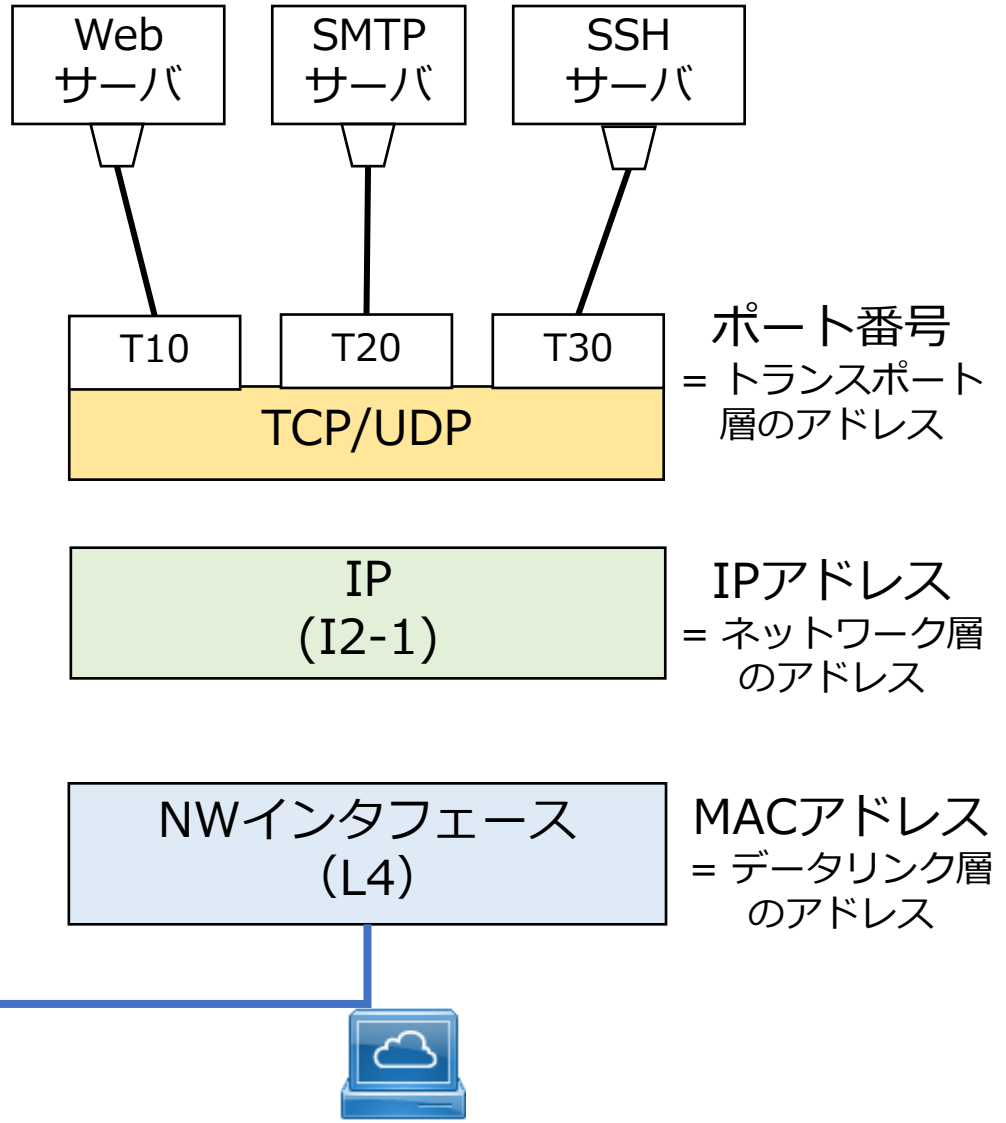
アドレスを偽装して不正に通信

⇨ スプーフィング（なりすまし）

通信可能なアドレス（=攻撃対象）の調査

⇨ スキャン活動





IPv4アドレス

ネットワーク群を相互接続するために，ネットワーク機器を一意に識別するためのアドレス

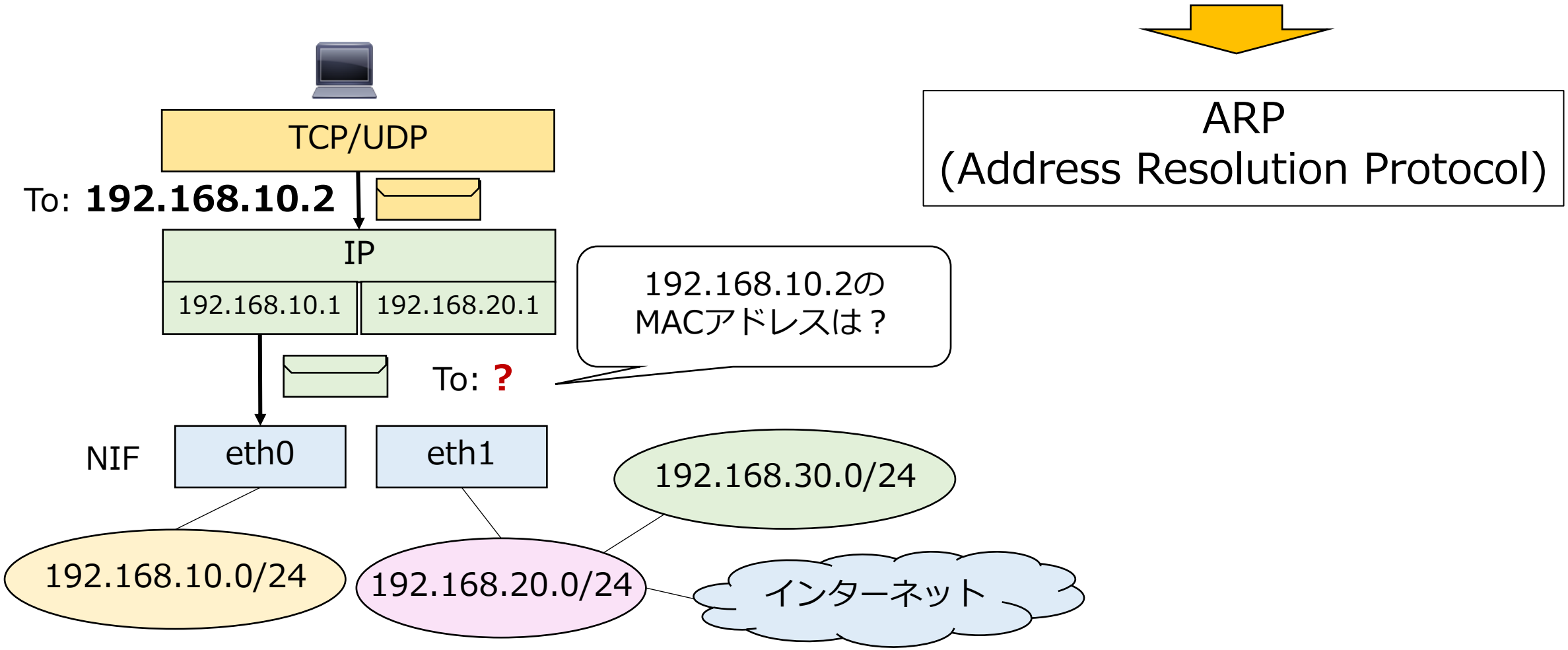
- ✓ 32bitのアドレス
- ✓ 8bit毎にピリオドで区切られた10進数で表現

2進表現	10000101	00101010	00110111	00001100
10進表現	133.	42.	55.	12

IPアドレスとMACアドレスの対応付け

転送すべきIPアドレスとNIFが決まっても，まだMACアドレスは不明なまま

⇨ 転送先のIPアドレスに紐づいた**MACアドレスを取得する**技術が必要



演習：ARPテーブルの書き換え

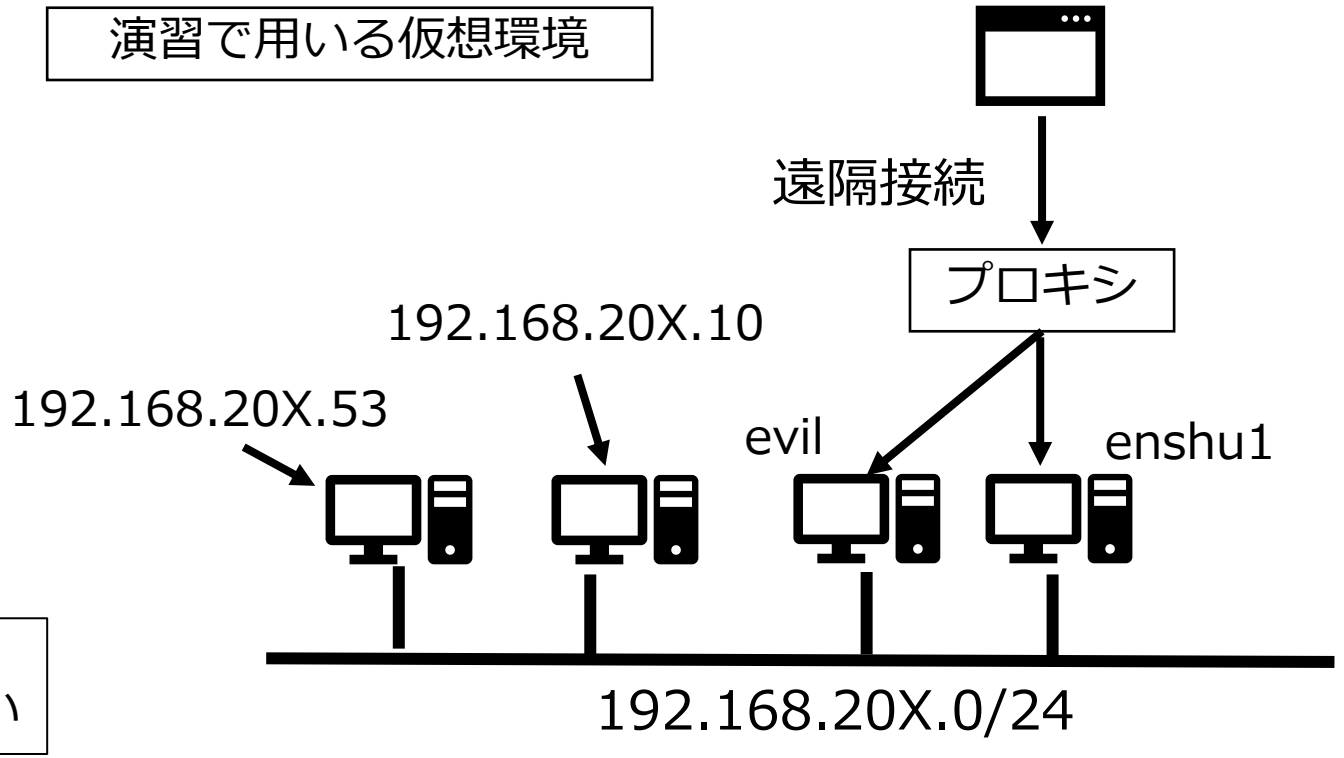
ARPテーブル（IPアドレスとMACアドレスの紐づけ）が
書き換えられると，正常な通信ができなくなります．

⇨ ARPテーブルの書き換えによって不正に通信を受信できるか確かめてみましょう

接続先のマシン

「右クリック→新しいタブで開く」などで，
両方のマシンにアクセスできるようにしてください

演習で用いる仮想環境



演習：送信元の詐称

パケットの送信元は容易に詐称することができてしまいます．

✓ただし，詐称したとしても返信は本来の宛先に届くため，
不正にパケットを受信することはできません

⇨ 送信元の詐称により何ができるか試してみましょう