

情報セキュリティ基礎

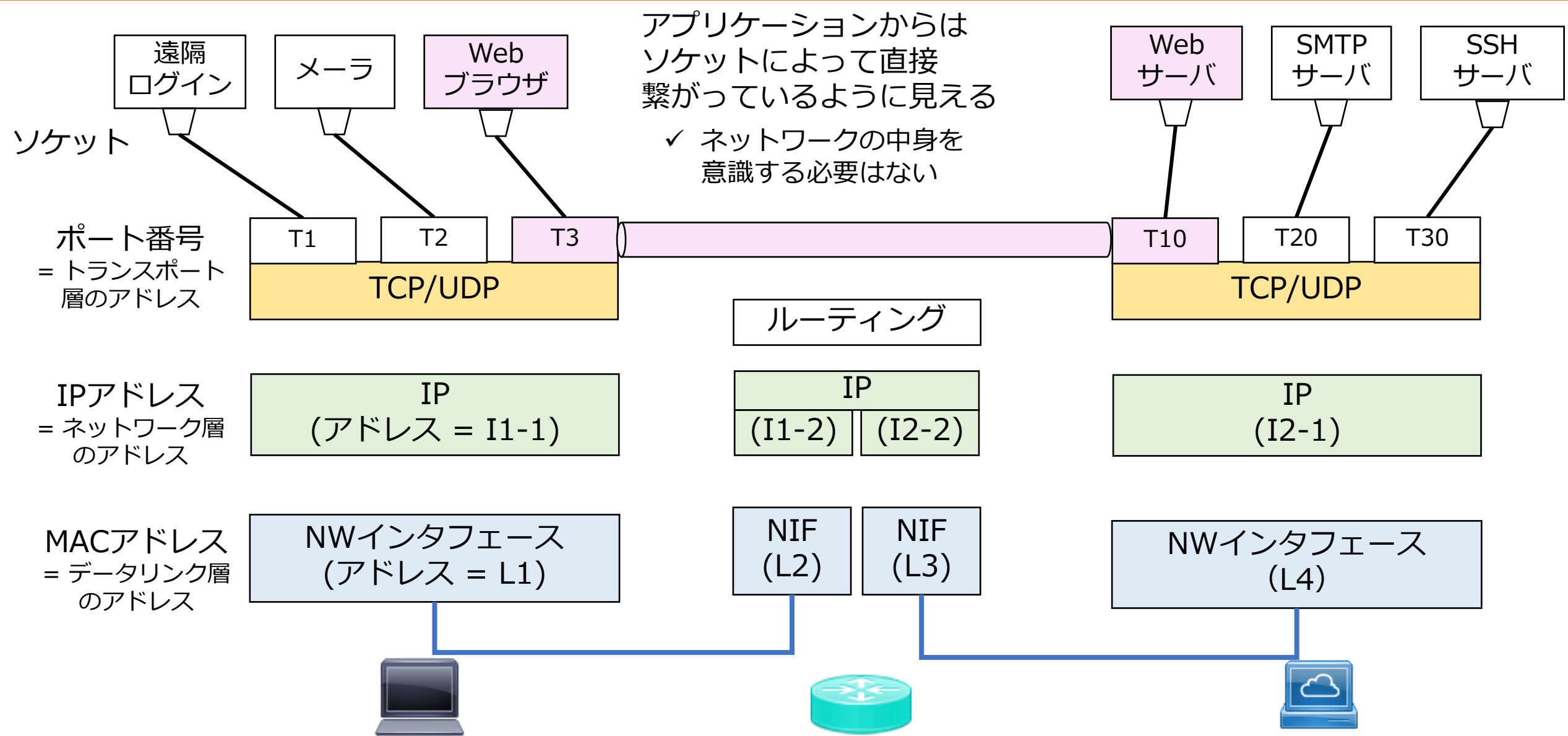
第4回 TCP/IPの基礎と脅威（2）

藤本 章宏

今回の目標

- トランスポート・プロトコルの代表格であるTCPの動作について確認する
- 簡単な演習を通し, トランスポート層における脅威を確認する

ネットワークの階層化



トランスポートプロトコル

上位層（TCP/IPではアプリケーション）に対して
通信サービスを提供するためのプロトコル

要求される機能

- アプリケーションから受け取ったデータを適切なサイズに分割して送信
- コンピュータが受信したパケットを**正しくアプリケーションに届ける**

✓ 受信したパケットが壊れていた場合は破棄

UDP

TCP

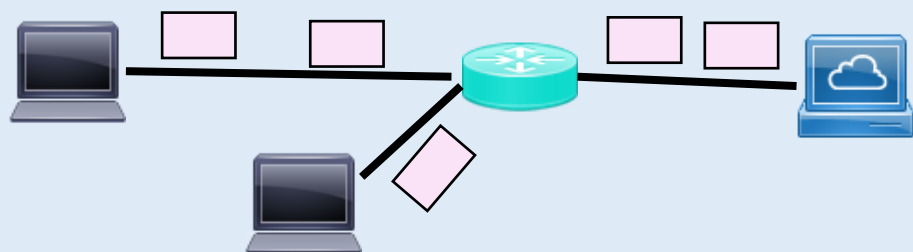
✓ 破棄したパケットの再送を要求

✓ 受信側がパケットを取りこぼさないよう，送信量を調整

✓ 受信したパケットを正しい順序に並び替え

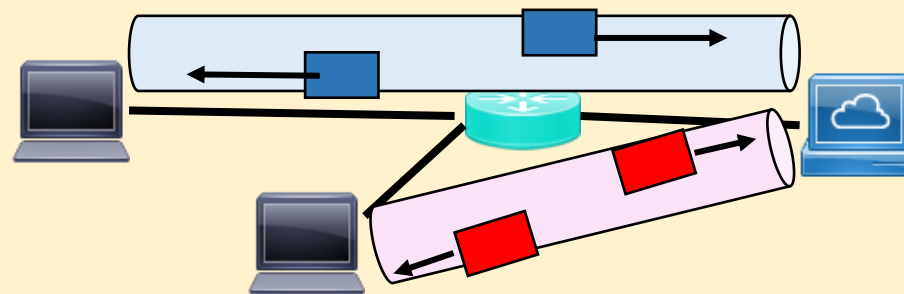
TCPとUDP

UDP (User Datagram Protocol)



- コネクションレス型
 - ✓ パケット1つ1つを独立したものとして扱う
 - ✓ 郵便のようなイメージ
- 最低限の制御で高速な転送

TCP (Transmission Control Protocol)



- コネクション型
 - ✓ 通信要求毎にコネクションを確立
 - ✓ 電話のようなイメージ
 - ✓ コネクション毎に通信状態を管理
- 再送制御などによる高信頼な通信

ポート番号

トランスポート層におけるアドレス

- ✓ どのアプリケーションの通信なのかを識別するための番号
- ✓ 一部の番号はIANA (Internet Assigned Numbers Authority)によって管理

システムポート (Well-Known ポート) [0-1023] :

よく利用されるアプリケーションのために予約されたポート番号

ユーザポート (登録済みポート) [1024-49151] :

IANAを通じて用途が登録されているポート番号

ダイナミックポート [49152-65535] :

自由に利用可能なポート番号

- ✓ 代表的な用途として, クライアント側が利用する一時ポート (エフェメラルポート)

ポート番号	用途
22	SSH (遠隔ログイン)
25	SMTP (電子メールの配送)
53	DNS (ドメイン名の解決)
80	HTTP (Web)
110	POP3 (電子メールの受信)
123	NTP (時刻同期)

シーケンス番号と確認応答番号

シーケンス番号：

送信データの位置を示す
順序番号

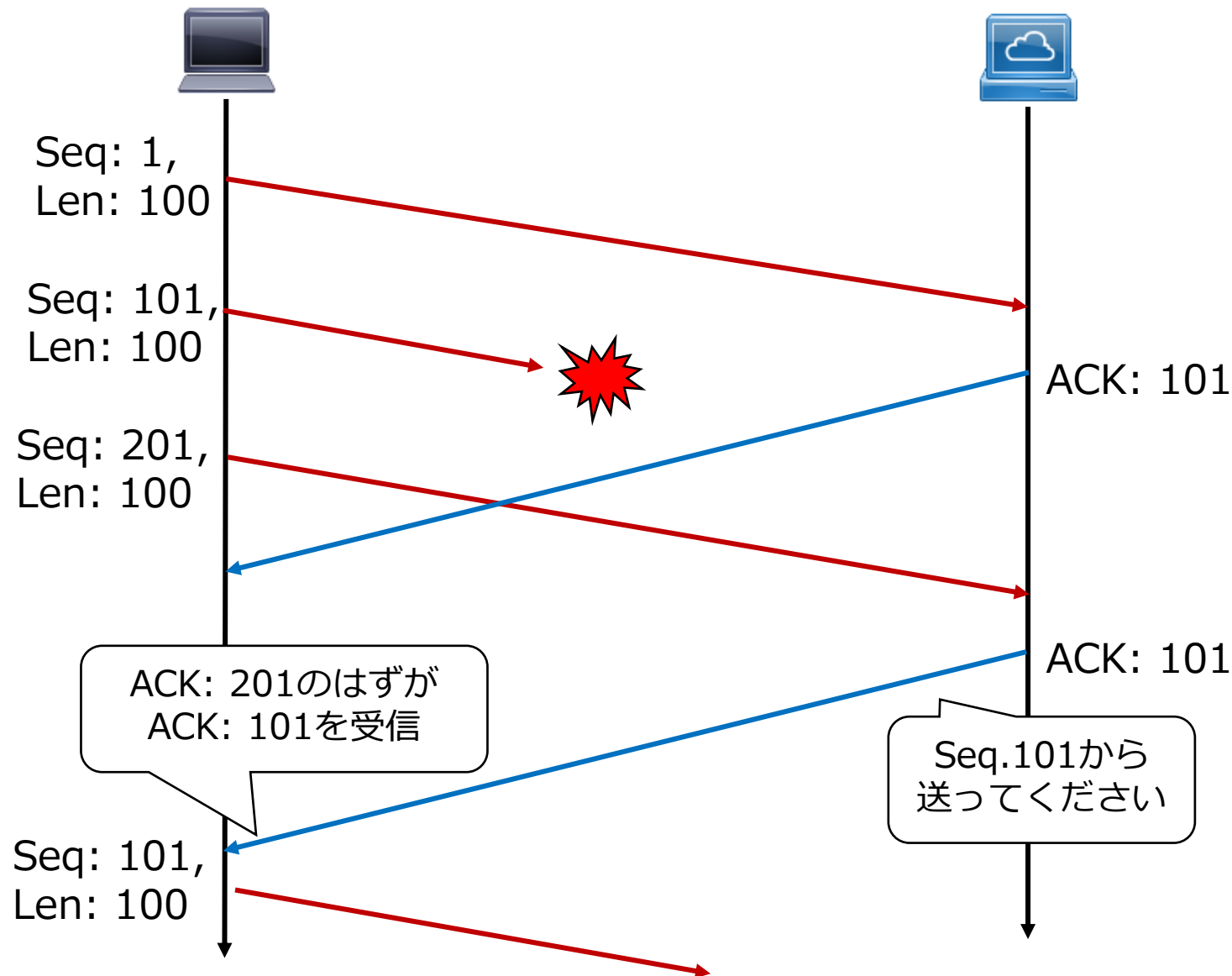
- ✓ 正しい順序に並び替え
- ✓ どのパケットが喪失したかを認識

確認応答番号：

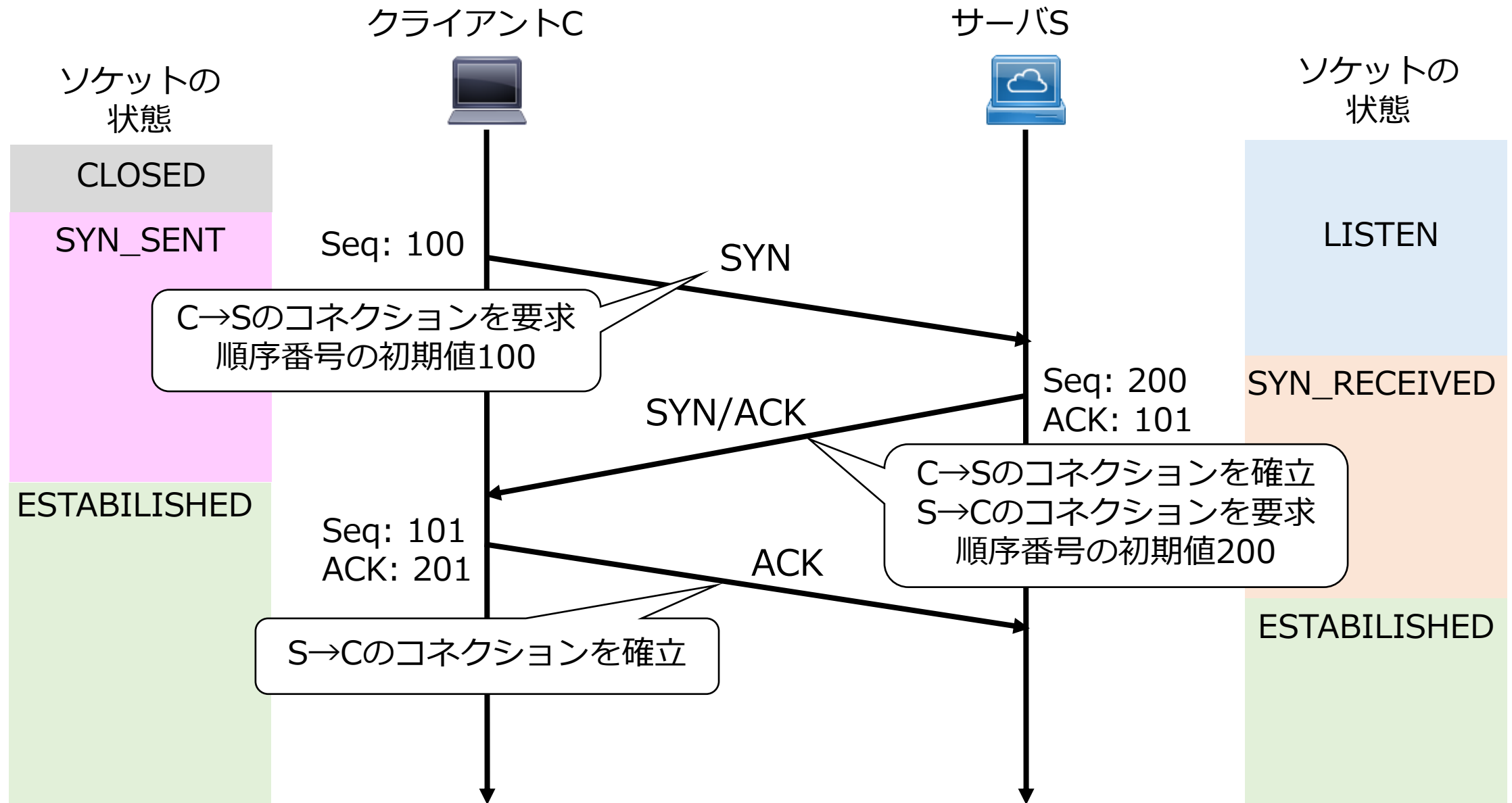
どのデータまで受信できているかを示す番号

- 次に受信すべき順序番号

- ✓ パケットが受信されたことを確認
- ✓ 期待したACKを受け取れなかった場合、パケットが喪失したと判断 → **再送**



コネクションの確立 (3-way ハンドシェイク)



ポートスキャン

ポートはアプリケーションと通信するための窓口



ポートスキャン

通信可能な（特に脆弱性のある）アプリケーションを見つけるため、
ポートにアクセスしてみて反応を伺う

✓ **サイバー攻撃の前兆**とみなされる

ポートスキャンでわかる（可能性がある）こと

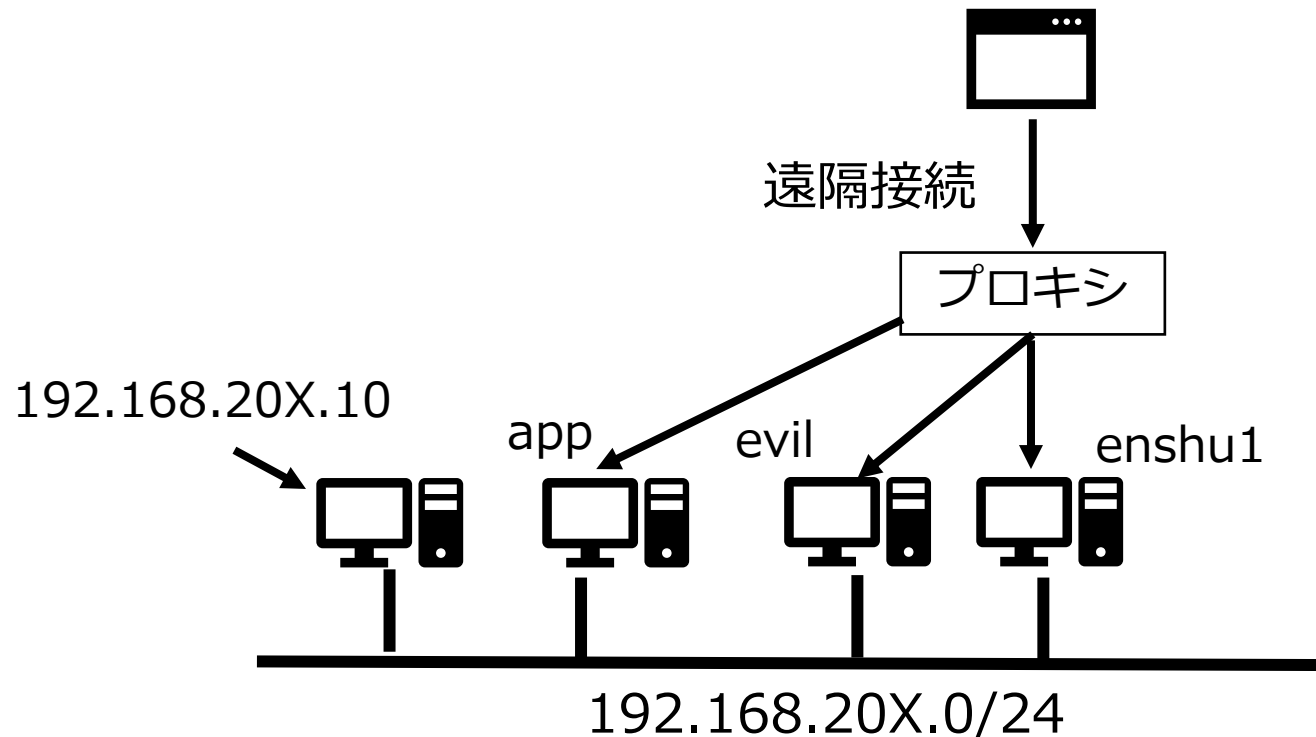
- ✓ そのポートで動作しているアプリケーションがあるかどうか
- ✓ アプリケーションの種類やバージョン
- ✓ OSの種類やバージョン

演習：ポートスキャン

実際にパケットを投げてみてポートの開放状況を調べてみましょう

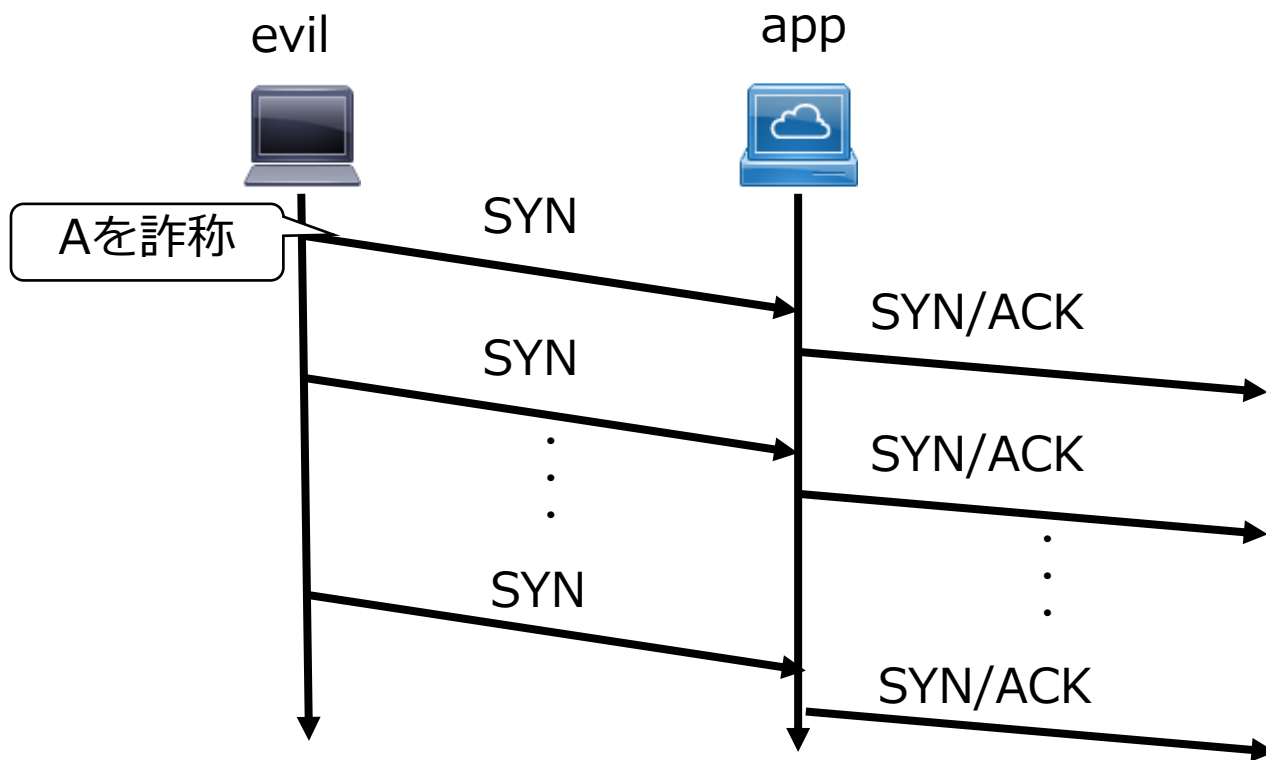
手順

1. Webブラウザからevilにログイン
2. app (192.168.20X.11) に向けて調査用パケットを送信 (詳細は次ページ)
3. appからの応答を見て, ポートの active/非アクティブを推測



演習： 3wayハンドシェイク完了待ちのソケット

evilからappに送信元IPアドレスを詐称してコネクションを要求し、appのソケットがどのような状態になっているかを見てみましょう



手順

1. Webブラウザからevilとappにそれぞれログイン
2. evilからappに向けてhping3で30回SYNパケットを送信
 - ✓ 詐称するアドレスは 192.168.20X.200
 - ✓ どのポートに送信するかも考えてみてください