

# インターネットの基本的仕組み

情報社会とセキュリティ  
2024年度前期  
佐賀大学工学部 只木進一

- 1 階層構造とパケット通信
- 2 IP アドレスとネットマスク
- 3 IP ルーティング (routing)
- 4 ドメイン名と DNS
- 5 DHCP: Dynamical Host Configuration Protocol
- 6 アプリケーションとサービス
- 7 IPv4/IPv6
- 8 課題

# インターネットの特性: パケットとプロトコル

- 回線を占有しない
  - データを小さな塊 (packets) に分けて送信
    - MTU (Maximum transmission Unit): 1500 bytes
  - パケットには通信情報を示すヘッダがある
- 多様な機器で共通の仕様
  - 階層的プロトコル: 機能を限定
  - 階層間インターフェース (interfaces) を規定
  - protocol: a set of rules that control the way data is sent between computers.

# インターネットで使用するアドレス

- 二つのアドレス
  - IPv4 アドレス: 153.126.149.71
  - ドメイン名: www.cc.saga-u.ac.jp
  - DNS: 二つを繋ぐサービス
- サブネット: ネットワークアドレス
- ネットワークを相互に繋ぐルータ (routers)

# TCP/IP 階層モデル

- ネットワークの物理実装に依存せず、各コンピュータ・通信装置が稼働するように設計
- 各層の機能を限定
- 各層は下の層を信頼 (エラーメッセージを含む)



# TCP/IP 階層モデル

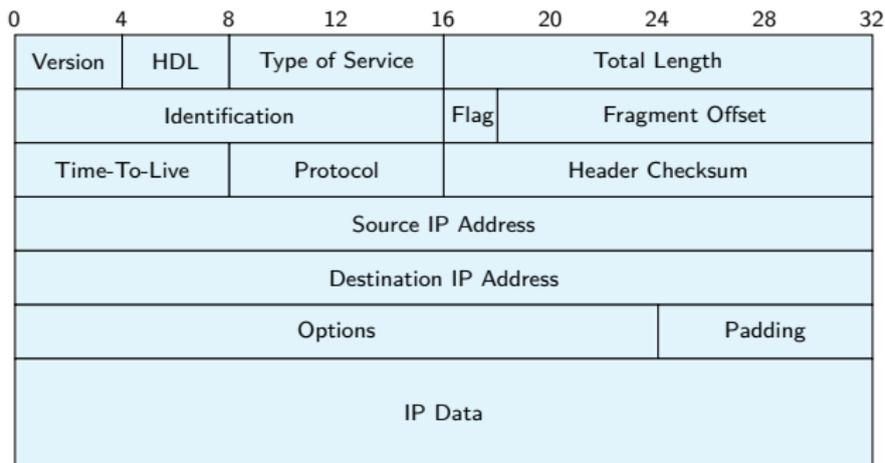
階層	機能
トランスポート層	<ul style="list-style-type: none"><li>● TCP または UDP プロトコル</li><li>● 通信のパケット化とパケットからの復元</li></ul>
インターネット層	<ul style="list-style-type: none"><li>● ルーティング、つまり配送経路を制御</li><li>● layer 3 とも言う</li></ul>
ネットワーク層	<ul style="list-style-type: none"><li>● 通常は ethernet プロトコルに相当</li><li>● 同一ネットワーク内の通信を制御</li><li>● layer 2 とも言う</li></ul>

# パケット: packets

- トランスポート層以下では、データはパケットという小さな塊で送受信
  - 番号が付いている
- 上層から下層
  - 各階層でヘッダ (header)/エンベロップ (envelope) を付ける
- 下層から上層
  - 各階層でヘッダ (header)/エンベロップ (envelope) を剥がす
- ヘッダには、各層の制御に必要な情報
  - 送信元、受信先、サービス番号 (TCP/UDP の場合) など



## 例: IP datagram



送信元と送信先の IP アドレス、ルータでの転送回数がヘッダにある

# IP アドレス: IP addresses

- IP アドレスは、インターネット上の住所
  - 32 ビット (IPv4 の場合)
- 通常は 8 ビット (octet) 毎にピリオドで区切って表記
  - 例: 133.49.4.7
- ネットワーク部とホスト部で構成
  - ネットワークは、適切な大きさに分割して管理
  - ピリオドの位置で分かれているとは限らない

# ネットマスクとネットワークアドレス

- ネットマスクも 32 ビット
  - 上位からあるビットまで 1、それより下位は 0
- ネットワークアドレス
  - IP アドレスとネットマスクのビット毎の and 演算で算出
  - 送信先が自ネットワークかを判定する際に利用

## 例: 24ビットネットマスク

10 進	255	255	255	0
16 進	FF	FF	FF	00
2 進	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 0 0 0 0 0 0 0
10 進	133	49	51	12
2 進	1 0 0 0 0 1 0 1	0 0 1 1 0 0 0 1	0 0 1 1 0 0 1 1	1 0 0 0 0 1 1 0
2 進	1 0 0 0 0 1 0 1	0 0 1 1 0 0 0 1	0 0 1 1 0 0 1 1	1 0 0 0 0 0 0 0
10 進	133	49	51	0

## 3通りのネットワークアドレス標記

- 133.49.51.0/**24**
- 133.49.51.0/**255.255.255.0**
- 133.49.51.0/**FFFFFF00**

## 例: 22 ビットネットマスク

10 進	255	255	252	0
16 進	FF	FF	FC	00
2 進	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 0 0	0 0 0 0 0 0 0 0
10 進	133	49	51	12
2 進	1 0 0 0 0 1 0 1	0 0 1 1 0 0 0 1	0 0 1 1 0 0 1 1	0 1 1 0 0 0 0 1
2 進	1 0 0 0 0 1 0 1	0 0 1 1 0 0 0 1	0 0 1 1 0 0 0 0	0 0 0 0 0 0 0 0
10 進	133	49	48	0

## 3通りのネットワークアドレス標記

- 133.49.48.0/**22**
- 133.49.48.0/**255.255.252.0**
- 133.49.48.0/**FFFFFFC00**

24ビットのネットワークが4つまとまっている

# 質問

IP アドレス 133.49.4.1 に対して、16 ビットネットマスクの場合のネットワークアドレスを求めなさい。

# ネットワーククラス: Network classes

クラス	アドレス範囲	説明
A	0.0.0.0 – 127.255.255.255	8ビットネットワーク アドレス 先頭は0
B	128.0.0.0 – 191.255.255.255	16ビットネットワーク アドレス 先頭は10
C	192.0.0.0 – 223.255.255.255	24ビットネットワーク アドレス 先頭は110

- 佐賀大学は 133.49.0.0/16 というクラス B アドレスを保有

# グローバルアドレスとプライベートアドレス

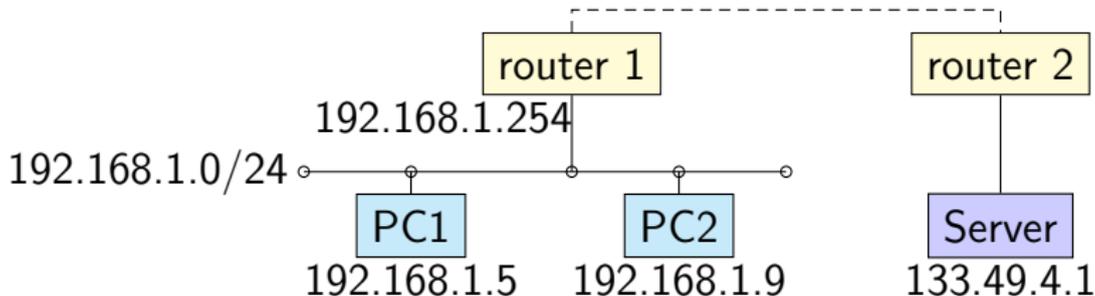
- グローバルアドレス (global addresses)
  - インターネット上で唯一 (unique) にしなければならない
  - 日本では JPNIC (Japan Network Information Center) が割り当て業務を担っている  
<https://www.nic.ad.jp>
  - 有料  
<https://www.nic.ad.jp/ja/ip/member/fee-table-2012.html#fee-table>
- プライベートアドレス (private addresses)
  - 組織内で自由に割り当て可能
  - 外部に出してはならない
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16

# IP ルーティング

- 一つのネットワークには、一つのネットワークアドレス
- ルータ (router): 異なるネットワークを繋ぐ通信機器
- 宛先 IP アドレスから、宛先ネットワークアドレスを計算
  - ネットワークインターフェースのネットマスクを使用
  - 宛先ネットワークに応じて、パケットを送り出すネットワークインターフェースを選択
- ルーティングテーブル
  - ネットワークアドレス毎に使用するインターフェースを定義
  - デフォルトルート: 知らないネットワークアドレス宛に使用する

## 例: クライアント PC など

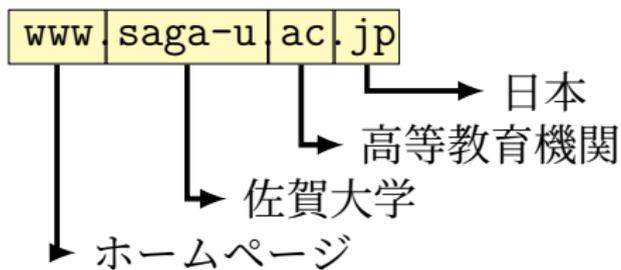
- 宛先 IP アドレスから、宛先ネットワークアドレスを計算
  - 自身のネットマスクを使用
- 自身のネットワークでない場合には、デフォルトルートへ
- 自身のネットワークである場合には、イーサネットプロトコルで通信



- PC1 から Server への通信
  - Server のネットワークアドレス 133.49.4.0 は、自ネットワークではない
  - デフォルトルート 192.168.1.254 へパケットを送信
- PC1 から PC2 への通信
  - PC2 のネットワークアドレス 192.168.1.0 は、自ネットワーク
  - イーサネットプロトコルで直接通信

# ドメイン名

- IP アドレスは覚えられない
- IP アドレスからは、サーバの所属組織や目的が不明
- アプリケーションは、IP アドレスで接続することに注意



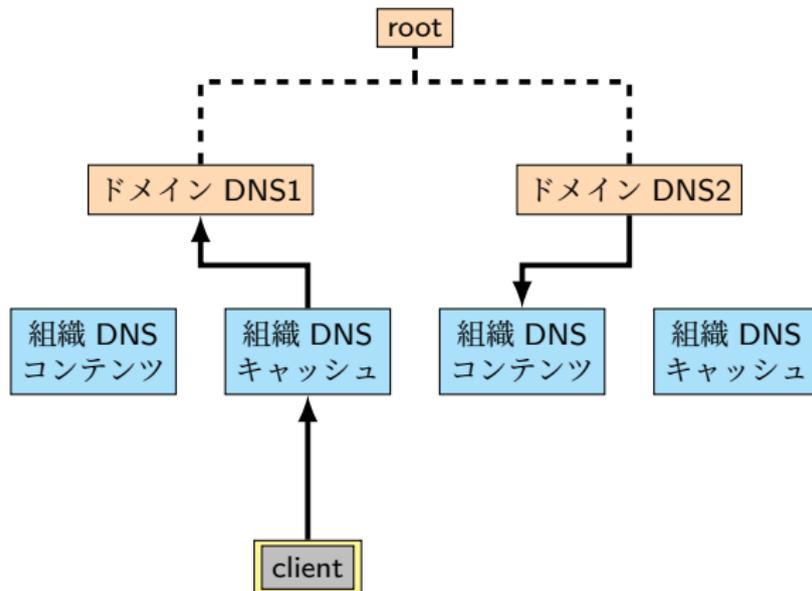
# ドメイン名

- ドメイン名は重要
  - ac.jp: 高等教育機関 (大学、専門学校等) 限定
  - go.jp: 政府機関限定
  - co.jp: 日本で登記している会社組織
- jp ドメイン配下の割り当ては JPRS (Japan Registry Services) が実施
  - `https://jprs.co.jp`
- 政府機関は、組織のドメインを使用することになっている
  - 政府機関等のサイバーセキュリティ対策のための統一基準群
  - `https://www.nisc.go.jp/policy/group/general/kijun.html`

# DNS: Domain Name System

- FQDN (Fully Qualified Domain Name) と IP アドレスの対応付け
- DNS Contents Servers
  - 管理するホスト名の情報を提供する
- DNS Cache Servers
  - 組織内のクライアントの問い合わせを受ける
  - 外部の DNS Contents Servers から情報を取得して、クライアントへ提供
  - 一旦取得してデータは、しばらく保有して、問い合わせに備える

# DNS の階層構造



# 質問

コマンドラインを開いて、DNS を使って名前解決をしましょう。  
コマンドは `nslookup` です。

- `www.cc.saga-u.ac.jp`
- `www.saga-u.ac.jp`
- `www.google.co.jp`

# DHCP: Dynamical Host Configuration Protocol

- インターネット接続のためには、多数の設定が必要
- 正しく設定しないと、接続できない
- 一般ユーザには難しい
- 自動的に設定する方法
- サーバが必要

# DHCPが自動で設定する項目

- IP アドレス
- ネットマスク
- デフォルトゲートウェイ
- DNS サーバ
- デバイスのドメイン名

# アプリケーションとサービス

- トランスポート層以下は、アプリケーションによらず共通
- TCP/UDP ヘッダには、アプリケーションを区別する番号

## 主なポート番号

番号	サービス
22	ssh (secure shell)
25	smtp (simple mail transfer protocol)
53	dns (domain name system)
80	http (hyper-text transfer protocol)
123	ntp (network time protocol)
443	https (hyper-text transfer protocol over TLS/SSL)

# IPv4/IPv6

- IPv4: 従来のプロトコル
  - IP アドレスは 32 ビット:  $2^{32} \simeq 4.3 \times 10^9$
  - アドレスの枯渇: アジア太平洋地域は 2011 年に枯渇
- IPv6: アドレス枯渇に対応した新プロトコル
  - 128 ビットアドレス:  $2^{128} \simeq 3.4 \times 10^{38}$

- IPv6 の利点
  - 全てのデバイスに IP アドレスを
  - IP アドレス設定の自動化
- IPv6 の課題
  - IPv4 からの移行の困難: 一斉移行は不可能
  - 共存できるか?
  - IPv6 に対応できない機材の存在
- 主要サイトは IPv6 対応済み
- 佐賀大学総合情報基盤センターのホームページも IPv6

# 課題

自宅にインターネット環境がある人は、IP アドレスを確認しなさい。