

# ネットワーク

## 出題ポイントまとめ

- アドレス長
  - IPv4：32ビット
  - IPv6：128ビット
- 表記方法
  - IPv4：10進数をドットで区切り（例：192.168.0.1）
  - IPv6：16進数をコロンで区切り（例：2001:db8::1）
- アドレス枯渇問題
  - IPv4：枯渇 → NAT 対応
  - IPv6：ほぼ無限 → NAT 不要
- セキュリティ
  - IPv4：IPSec は任意
  - IPv6：IPSec が標準仕様

## UPS (Uninterruptible Power Supply：無停電電源装置)

- 停電時に 一時的に電力を供給する装置
- サーバやネットワーク機器を守る目的

## PoE (Power over Ethernet)

- LANケーブルで 電力とデータを同時に供給できる技術
- コンセント不要で機器を設置可能

## PLC (Power Line Communication：電力線通信)

- 電力線を通信回線として利用する技術
- 家庭のコンセントを利用して通信可能

## SSID (Service Set Identifier) とは

無線LAN (Wi-Fi) ネットワークを識別するための名前

SSID = 無線LANネットワークの識別名

「アクセスポイントを区別するための識別子」と覚える

暗号化方式 (WEP, WPA2, WPA3) とセットで問われやすい

アクセスポイント -> 有線LANと無線LANをつなぎ、無線端末がネットワークに接続できるようにする装置

無線LAN (Wi-Fi) の「基地局」のような役割

スマホやPCなどの端末を、LANやインターネットに接続させる

通常はルータやスイッチと接続され、そこから外部ネットワークに出ていく

## OSI基本参照モデル (7階層)

### 7. アプリケーション層

- 役割：利用者に最も近い層。アプリケーションサービスを提供
- 代表例：HTTP, FTP, SMTP, POP3, DNS

## 6. プレゼンテーション層

- 役割：データの表現形式を変換（文字コード、暗号化、圧縮など）
- 代表例：MIME, JPEG, SSL/TLS（暗号化部分）

## 5. セッション層

- 役割：通信の開始・維持・終了を管理（対話の制御）
- 代表例：RPC, NetBIOS, TLSのセッション管理

## 4. トランスポート層

- 役割：アプリ間での信頼性あるデータ転送（誤り制御、再送、順序制御）
- 代表例：TCP（信頼性あり）, UDP（高速・信頼性なし）

## 3. ネットワーク層

- 役割：異なるネットワーク間での経路選択（ルーティング）
- 代表例：IP, ICMP, ARP（実際はL2寄りだが応用情報ではここで問われることあり）

## 2. データリンク層

- 役割：同一ネットワーク内での転送（フレーム単位、MACアドレス利用）
- 代表例：Ethernet, PPP, スイッチ, ブリッジ

## 1. 物理層

- 役割：ビット列を電気信号や光信号として送受信
- 代表例：ケーブル（UTP, 光ファイバ）, ハブ, NIC

SDN (Software-Defined Networking)

SDNとは、ネットワーク機器の制御機能と転送機能を分離し、ソフトウェアで集中管理する仕組み。

## 応用情報試験で狙われやすいポイント

- TCPとUDPはトランスポート層
- IPはネットワーク層、MACはデータリンク層
- ハブは物理層、スイッチはデータリンク層、ルータはネットワーク層
- 暗号化はプレゼンテーション層、セッション管理はセッション層

## ネットワーク関連アルファベット集（応用情報向け）

### 1. ネットワーク基盤・IP関連

- **IP (Internet Protocol)**：ネットワーク層のプロトコル
- **IPv4 / IPv6**：32ビットアドレスと128ビットアドレス
- **TCP (Transmission Control Protocol)**：信頼性のあるトランスポート層プロトコル
- **UDP (User Datagram Protocol)**：高速で信頼性なしのトランスポート層プロトコル
- **ICMP (Internet Control Message Protocol)**：エラーメッセージや制御用（例：ping）
- **ARP (Address Resolution Protocol)**：IP ⇄ MAC アドレス変換
- **NAT (Network Address Translation)**：アドレス変換
- **DHCP (Dynamic Host Configuration Protocol)**：IPアドレス自動割当

- **DNS (Domain Name System)** : ドメイン名 ⇔ IP アドレス変換

## 2. ネットワーク機器関連

- **AP (Access Point)** : 無線LANのアクセスポイント
- **SSID (Service Set Identifier)** : 無線LANの識別子 (ネットワーク名)
- **MAC (Media Access Control) アドレス** : LANカードに割り当てられる一意の識別子
- **VLAN (Virtual LAN)** : 論理的に分割したLAN

## 3. セキュリティ関連

- **SSL/TLS (Secure Sockets Layer / Transport Layer Security)** : 暗号化通信
- **IPsec (IP Security Protocol)** : IPレベルの暗号化
- **VPN (Virtual Private Network)** : 仮想専用線 (インターネット上で安全な通信)
- **WEP (Wired Equivalent Privacy)** : 古い無線LAN暗号化方式 (弱い)
- **WPA2/WPA3 (Wi-Fi Protected Access)** : 無線LANの暗号化方式
- **PKI (Public Key Infrastructure)** : 公開鍵基盤
- **CA (Certificate Authority)** : 認証局
- **CRL (Certificate Revocation List)** : 失効証明書リスト

## 4. ネットワーク構築・管理関連

- **LAN (Local Area Network)** : 構内ネットワーク
- **WAN (Wide Area Network)** : 広域ネットワーク
- **MAN (Metropolitan Area Network)** : 都市内ネットワーク
- **ISP (Internet Service Provider)** : プロバイダ
- **SDN (Software-Defined Networking)** : ネットワークをソフトで集中制御
- **NFV (Network Functions Virtualization)** : ネットワーク機能の仮想化
- **QoS (Quality of Service)** : 通信品質の保証
- **SNMP (Simple Network Management Protocol)** : ネットワーク管理

## 5. 電源・通信関連

- **UPS (Uninterruptible Power Supply)** : 無停電電源装置
- **PoE (Power over Ethernet)** : LANケーブルで電力供給
- **PLC (Power Line Communication)** : 電力線通信

## 6. その他よく出る略語

- **HTTP / HTTPS (HyperText Transfer Protocol / Secure)** : Web通信
- **FTP (File Transfer Protocol)** : ファイル転送
- **SMTP (Simple Mail Transfer Protocol)** : メール送信
- **POP3 / IMAP** : メール受信
- **URL (Uniform Resource Locator)** : Webアドレス
- **HTML (HyperText Markup Language)** : Webページ記述言語

サブネットマスクとは、IPアドレスのうち「ネットワーク部」と「ホスト部」を区別するためのビット列

- IPアドレスは「ネットワーク部 + ホスト部」で構成される
- サブネットマスクで「どこまでがネットワーク部か」を指定する

インターネットの情報の送り方

## CSMA/CD方式

Carrier Sense Multiple Access with Collision Detection

### 仕組み

- イーサネット (Ethernet) で使われるアクセス制御方式
  - 複数の端末が同じ伝送路を使うときに、衝突 (コリジョン) を避ける仕組み
1. **Carrier Sense** : 送信前に通信路が空いているか確認
  2. **Multiple Access** : 空いていれば送信
  3. **Collision Detection** : 同時に送信して衝突したら、それを検知し送信を中止
  4. 一定時間ランダムに待って再送

### 特徴

- 衝突が発生するため効率は落ちる
- 半二重通信、バス型 LAN で利用された
- 今はスイッチで衝突がほぼ解消され、CSMA/CD はほとんど使われない

## トークンリング方式

### 仕組み

- リング型 LAN で使われるアクセス制御方式
- ネットワーク上を「トークン」と呼ばれる制御フレームが巡回
- トークンを受け取った端末だけが送信可能
- 送信が終わるとトークンを返して次の端末に渡す

### 特徴

- 衝突が発生しない (トークンを持った端末しか送信できないため)
- 公平性が高い (順番に通信できる)
- ただしトークンが紛失・破損するとネットワーク全体に影響

## トークンアクセス方式とは

👉 トークンと呼ばれる制御用フレームをネットワーク上で回し、トークンを持った端末だけが送信できる方式。

### 仕組み

1. ネットワーク上を「トークン (送信許可証)」が順番に巡回する
2. トークンを受け取った端末だけが一定時間データを送信できる
3. 送信が終わるとトークンを次の端末に渡す

### 特徴

- 衝突 (コリジョン) が発生しない (CSMA/CD との大きな違い)
- 公平性が高い (全端末に順番が回るため)
- ただし、トークンが紛失・破損すると通信全体が止まる

- 遅延は「トークンが回ってくるまでの待ち時間」に依存

## 1. パケット交換 (Packet Switching)

### 定義

👉 データを小さなパケット単位に分割して送信し、ネットワーク内のノードがパケット単位で転送する方式。

### 特徴

- データを分割 → パケットごとに宛先アドレスを付与 → 経路を選んで送信
- 各パケットは必ずしも同じ経路を通らず、到着後に再構成される
- 代表例：インターネット (IP ネットワーク)

## 2. フレームリレー (Frame Relay)

### 定義

👉 パケット交換の一種で、OSI 参照モデルの第2層 (データリンク層) で動作する通信サービス。

(1990 年代に WAN 接続で広く利用された)

### 特徴

- フレーム単位でデータを転送
- エラーチェックはするが再送制御は行わない (上位層に任せる)
- その分、高速・低遅延

## IP アドレスのクラス (A ~ D)

### 基本ルール

IP アドレスは 32 ビット (4 オクテット) = 0.0.0.0 ~ 255.255.255.255

先頭ビットで「クラス」を区別していました (昔の方式、今は CIDR が主流ですが試験では出ます)。

### クラス A

- 先頭ビット：0
- 範囲：0.0.0.0 ~ 127.255.255.255
- ネットワーク部：8 ビット
- ホスト部：24 ビット
- 特徴：
  - 1 ネットワークで 約 **1677 万** ホスト 利用可
  - 大規模ネットワーク用

### クラス B

- 先頭ビット：10
- 範囲：128.0.0.0 ~ 191.255.255.255
- ネットワーク部：16 ビット
- ホスト部：16 ビット
- 特徴：
  - 1 ネットワークで 約 **6.5 万** ホスト 利用可
  - 中規模ネットワーク用

## クラスC

- 先頭ビット：110
- 範囲：192.0.0.0 ～ 223.255.255.255
- ネットワーク部：24ビット
- ホスト部：8ビット
- 特徴：
  - 1ネットワークで **254** ホスト 利用可
  - 小規模ネットワーク用

## クラスD

- 先頭ビット：1110
- 範囲：224.0.0.0 ～ 239.255.255.255
- 用途：マルチキャストアドレス（特定グループに一斉送信）

## まず「プロキシ」とは？

👉 プロキシ (Proxy) =代理

ネットワークにおいて「クライアントやサーバの代理として通信を行う装置や仕組み」のことです。

## フォワードプロキシ (Forward Proxy)

### 定義

- クライアント側に立って、インターネットにアクセスする代理をするプロキシ
- 企業や学校で使われる「Webアクセスの仲介」が典型例

### 特徴

- クライアント → フォワードプロキシ → インターネットのサーバ
- クライアントの直接アクセスを隠せる
- キャッシュ機能で高速化できる
- フィルタリング（アクセス制御）に利用できる

👉 利用者の代理人 となるプロキシ

## リバースプロキシ (Reverse Proxy)

### 定義

- サーバ側に立って、クライアントからのアクセスを代理するプロキシ
- Webサービスや大規模サイトでよく利用される

### 特徴

- クライアント → リバースプロキシ → 内部のWebサーバ
- 負荷分散（ロードバランサとして利用）
- キャッシュで応答高速化
- サーバの実IPアドレスを隠せる（セキュリティ強化）

👉 サーバの代理人 となるプロキシ

## 図でイメージ (テキスト版)

[クライアント] --(代理)--> [フォワードプロキシ] --→ [インターネットのWebサーバ]

[クライアント] --→ [リバースプロキシ] --(代理)--> [内部のWebサーバ群]