# 1　ネットワークアーキテクチャ

◎ネットワークアーキテクチャとは通信モデルのことである。

パケット通信を行う場合、転送されるデータにはヘッダがつけられる。ヘッダには制御情報が入っている。ヘッダが取り付けられたデータをパケットという。

実際のパケットは以下のようにパケットのデータ部分にパケットをセットしている。

| ヘッダ | ヘッダ | ヘッダ | データ |
|---|---|---|---|

## 1.1　プロトコル

プロトコルとは通信を行う上での約束ごとである。

例) ネットワーク層はパケットのルーティングを行うこと。など

プロトコルに適合していればどのような機器・プログラムを用いてもよいことになっている。

プロトコルは階層構造をとっている。これにより異種の機器・プログラム同士の通信が可能になる。

例) 電話

「言語層」を「言葉を音声として通信装置との間でやりとりするプロトコル」と定義し、「通信装置層」を「音声データを他の通信装置に送信および受信するプロトコル」と定義する。

この時、A さん、B さんはともに好きな言語 (日本語・英語 etc...) 及び通信装置 (固定電話・携帯電話 etc...) を使用することができる。

ただし、「言葉のデータを他の言語に翻訳するプロトコル」は定義されていないので、異言語間での通話が成立するとは限らない。

## 1.2　有名なネットワークアーキテクチャ

- OSI 基本参照モデル
  - ISO(国際標準化機構) が制定
  - デジュリスタンダード (標準化機関で採用された公式の標準)
- TCP/IP モデル
  - インターネットで使用されているプロトコル
    * IP(Internet Protocol) は複数のネットワークを接続して通信経路 (IP ネットワーク) を作るプロトコル
    * TCP は IP ネットワークの 2 点間の通信の信頼性を高めるプロトコル
    * TCP/IP の TCP にはそれほど意味がない。(UDP を用いても UDP/IP とは言わず、よく TCP/IP といったりする)

- 元は軍用で、ひとつの通信基地が破壊されても通信が途絶えないように (分散管理) するためにアメリカの大学で開発された
- 軍務機密を持ち出すことはできなかったので RFC(Request For Comments) という形で公開
- デファクトスタンダード (標準化機関に採用されたわけではないが、事実上の標準となっている)

# 2　OSI 参照モデル

| | |
|---|---|
| 第 7 層 | アプリケーション層 |
| 第 6 層 | プレゼンテーション層 |
| 第 5 層 | セッション層 |
| 第 4 層 | トランスポート層 |
| 第 3 層 | ネットワーク層 |
| 第 2 層 | データリンク層 |
| 第 1 層 | 物理層 |

## 2.1　物理層

電気信号を”1”,”0” のデータに変換して、通信媒体に**流す (送るではない)** 層。具体的に言うと、コンピュータの中のデータは”1”,”0” からなるが、これをそのまま他の機器に送ることはできない。(USB メモリはここでは忘れて) 他の機器に送るためには無線 LAN や LAN ケーブルなどの**通信媒体**に電気信号を送らないといけない。そのために、”1”,”0” を電気信号 (電圧とか) に変換する必要がある。

物理層が提供する仕様は「**ビット (”1”,”0”) を電気信号に変換し、通信媒体に流す**」である。

- キーワード
  - LAN

    Local Aria Network。インターネットを” 外側” とした時の” 内側” のネットワーク。LAN 内では LAN 内用の IP アドレス (プライベートアドレス) が与えられる。
- 該当する機器
  - ツイストペアケーブル (いわゆる青とか白の LAN ケーブル)・光ケーブル
  - リピータハブ

    ただただ送られてきた電気信号をつながっている線に垂れ流すだけのハブ。馬鹿ハブともいう。馬鹿なので、これはどの PC 向けのデータだなということはしないで、つながっている機器全てに電気信号をコピーして送る。
  - 搬送波

    無線 LAN と書きたいが、無線 LAN アクセスポイントはもっと上位層なので、物理層に定義される「無線通信」をモノで表すなら電波を載せて運ぶ搬送波ということになる。
- 該当するプロトコルスイート

- Ethernet

  LAN の中で通信するならこうしましょうという決まり。

## 2.2 データリンク層

ネットワーク層から指示を受けて物理層を扱う層。というよりは、LAN の中で「このデータは PC1 に渡してください」って言われた時に、PC1 を探してその**方向**にデータを送る人。方向と言ったのは、データリンク層では隣接間通信しか定義されていないので、隣の (直接接続された) 機器にしかデータを送れないからである。

データリンク層が提供する仕様は**「隣接する、目的の機器に近い機器にデータを転送する」**である。

- キーワード
  - MAC アドレス

    NIC 固有の値で、データリンク層でデータを受け渡しするときの目印となるアドレス。48 ビット (6 バイト) の値で、1 バイトごとに:(コロン) で区切られている。表記は一般的に 16 進数で、前半 3 バイトがベンダ ID、後半 3 バイトが製品固有番号である。
- 該当する機器
  - ブリッジ

    データの宛先を理解してその方向にデータを送信する機器。
  - L2SW

    スイッチングハブとも言う。ポート (口) が複数個あり、内蔵の ASIC というハードウェアで高速に処理できる特徴がある。
- 該当するプロトコルスイート
  - IEEE 802.11

    無線でデータをやり取りするときの決まり。(パソコンのネットワークインタフェースカード (NIC) のところとかにある 802.11 a/b/g/n みたいなやつの通信ルールを決めている。NIC が対応してないと使えない。)
  - PPP

    Point-to-Point Protcol。直訳して点と点との約束。隣接間通信の決まりを定める。PPPoE(PPP over Ethernet) は PPP の拡張で、Ethernet の上でも読めるような宛先の書き方をしたりして融通の聞かない Ethernet を挟んだ通信を可能にしている。

## 2.3 ネットワーク層

データリンク層・物理層のの機器が集まっているエリアを LAN と言った。LAN はネットワークである。ネットワーク層は複数のネットワークをつなげる層である。イメージで言うと、いくつかの国 (LAN) があって、ある国からある国へ旅をするとする。地図を見てどの国を経由するのが最も楽かを考えて決めて、また、国境の衛兵と話をして国境を通れるようにする人がネットワーク層である。どの国を経由するか (どのルートを通るか) を決めることをルーティングという。ちなみに国境に立っている衛兵もネットワーク層の人である。

ネットワーク層が提供する仕様は**「ネットワーク A からネットワーク B への通信経路を決め、また、ネットワーク間でのデータ転送を取り持つ」**である。

- キーワード
  - IP アドレス

    IP で参照する、送信者・受信者を指定するためのアドレス。32 ビットの IPv4 と 128 ビットの IPv6 とがある。
  - VLAN

    Virtual LAN。主に L3SW で利用できる機能で、同じ SW につながっている機器でも、異なる LAN に所属しているように見せるもの。利点は以下のようなものが挙げられる。
    * ブロードキャスト範囲が限定される。
    * フィルタリングルールが柔軟に設定できる。
    * 物理的な機器を節約できる。
- 該当する機器
  - ルータ (経路選択と別のネットワークへのルーティングを行う機器。家にインターネット回線を引いてくるには、ネットワークの入り口にルータを置いておく必要がある。そうでないと、誰も LAN 内にパケットをルーティングしてくれないし、誰も外のネットワークでの通信経路を決められない。つまりネットに繋がらない。)
  - L3SW(もともとは L2SW+ ルータくらいの意味だったが、今はルータも強化されてきているので実質的な違いは ASIC を使っているか否かくらいらしい。問題で出てきてもルータと読み替えても大きく問題はない。)
- 該当するプロトコルスイート
  - ICMP

    ping(ピン。ピングじゃない) コマンドを打ったら飛んでいくパケットのルールを決めている。

    ping を打ったら飛んでいくパケットには「タイプ」というデータがある。主なタイプの特徴は以下の通り。

| | |
|---|---|
| タイプ 8 | 受け取ったら返事返して |
| タイプ 0 | 届いた |
| タイプ 3 | そんな奴はいない (宛先が見つからない) |
| タイプ 5 | 俺に渡すな (別のところに転送しておいたけど、今度からはそっちを使ってくれ) |
| タイプ 11 | 時間切れ (ネットワークの中で無限ループした) |

  - IP

    Internet Protocol。パケットを中継するときのルールを決めている。IP ではあくまでパケットを近くのルータに向けて送信することを保証しているだけで、実はちゃんとパケットが届くかどうかには責任を持っていない。それを保証したい場合はトランスポート層の TCP を使ったりする必要がある。
  - IPSec

    IP Security Architecture。暗号化によって、IP パケットのデータの改ざんや盗聴を防ぐプロトコル。
      * AH(Authentication Header) という認証・完全性保証用のヘッダ
      * ESP(Encapsulated Security Payload) というデータの暗号化などのためのプロトコル
      * IKE(Internet Key Exchange protocol) という鍵交換のためのプロトコル

    から構成されている。

## 2.4 トランスポート層

ネットワーク層が保証する事項は「経路選択と中継」である。しかし、「中継先がデータを正しく受け取るか」や、「中継に失敗したらどうするか」ということはネットワーク層の知るところではない。トランスポート層はネットワーク層の上位に立ち、各ゲートウェイ間で正しくデータが受け渡しされているかを管理する。また、ポート番号の概念を追加して、特定のアプリケーションに対するコネクションを提供している。

多くのアプリケーションはサービスを提供するサーバと、サービスを利用するクライアントに分かれる、クライアント/サーバ方式をとっている。

- 該当するプロトコルスイート
  - TCP:コネクション型通信
    * 受信・送信ともに、通信相手の応答を確認しながら通信する。
    * 再送要求などができるため、信頼性は高い。
    * 応答を確認しながらのため、通信速度は遅い。
  - UDP:コネクションレス型通信

    * 受信・送信ともに、通信相手の応答を確認しない。
    * 相手にちゃんとデータが届いているかわからないので信頼性が低い。
    * 一方的にデータを送信し続けられるので、通信速度は速い。
    * リアルタイム通信・ブロードキャスト通信・高速通信に用いられる。

- キーワード
  - ポート番号

    利用するアプリケーションやサービスを識別するための番号。ポート番号の種類には以下のものがある。

    * ウェルノウンポート:0-1023

      標準で「このサービスはここ！」と決められているポート。有名なものには、以下のようなものがある。

      21 :ftp
      22 :ssh
      25 :smtp(Simple Mail Transfer Protocol:簡易メール転送プロトコル)
      80 :http
      110 :pop3(メール受信)
      143 :imap(メール受信)
      443 :https

      デフォルトで使われるポートのため、これらのポートには不特定多数からの接続要求がくる。

    * 登録ポート:1024-49151

      ユーザや開発者が、あるアプリケーション/サービスに割り当てられる範囲のポート。rails サーバや Python-bottle サーバなどは 5000 や 8000 という番号をよく使う。この間僕が携わった Unity 製のゲームはデフォルトで 7777 を使っていた。攻撃を避けるために ssh を 8022 にしたり、http を 8080 にしたりということもよく行われる。(この場合、22 や 80 ではコネクションを受けられなくなる、つまりそのことを知っている人間以外からの通信を遮断できる)

    * 短命ポート:49152-65535

      単一のユーザからの複数のリクエストを区別するために用意されている範囲のポート。例えば、80 番ポートで受けた http 要求のコネクションを 80 番の代わりに 49152 番で結ぶ、というようなことができる。

  - 3 ウェイ・ハンドシェイク

    コネクションを開始する際のサーバとクライアントとの間で交わされるパケットのやり取りのこと。全部で 3 工程あり、その後にコネクションが確立される (握手する) ことからこの名がついた。3 ウェイ・ハンドシェイクの手順は以下のとおりである。

    (1) クライアントはサーバに「今、手空いてるか？」という **SYN パケット**を送る。

(2) サーバはクライアントに「手空いてるで。まだ間に合うか？」という **ACK/SYN パケット**を送る。
(3) クライアントはサーバに「間に合うで」という **ACK パケット**を送る。

SYN は”synchronize” の略で、送信すると相手にコネクションの開始を要求する。ACK は”acknowledge” の略で、送信すると相手の要求に OK を返す。

逆にコネクションの終了の手順は以下のようになる。

(1) クライアントはサーバに「終わってええか？」という **FIN/ACK パケット**を送る。
(2) サーバはクライアントに「ええで」という **ACK パケット**を送る。
(3) サーバはクライアントに「終わってええか？」という **FIN/ACK パケット**を送る。
(4) クライアントはサーバに「ええで」という **ACK パケット**を送る。

FIN は”finish” の略で、送信するとコネクションの終了を要求する。

これらのパケットを正しくない方法で使う (コネクションが確立されていない相手に FIN を送るなど) と、ポートスキャンに始まる攻撃を行うことができる。また、コネクション確立の 3 を行わないことで、コネクション情報をサーバ側に大量に溜めさせてサーバのダウンを狙う攻撃を SYN Flood 攻撃という。

## 2.5　セッション層

トランスポート層より上位の層はほとんど直接ネットワークと関連しない。セッション層が保証するのはアプリケーションに対するコネクションが切れないようにすること、また、正常にコネクションを開始、及び終了することである。

## 2.6　プレゼンテーション層

プレゼンテーション層より下層ですでに、インターネット上の相手と切れないコネクションを結んで誤りなくデータを受け渡しすることが保証されている。プレゼンテーション層では、その正しく送られてきた/送るデータを、読めるように/読めないように加工することを保証する。具体的に言うと文字コード変換や、データの抽象構文化などである。

## 2.7　アプリケーション層

アプリケーション層の定義は広く、厳密に定義するのは難しい。さっくり言うと、ユーザが直接見る/触る部分である。

## TCP/IP モデルと OSI 参照モデルとの対応

| TCP/IP モデル | OSI 参照モデル |
|---|---|
| アプリケーション層 | アプリケーション層・プレゼンテーション層・セッション層 |
| トランスポート層 | トランスポート層 |
| インターネット層 | ネットワーク層 |
| ネットワークインタフェース層 | 物理層・データリンク層 |

# 3　IP アドレス

## 3.1　サブネットマスク

32 ビットの IP アドレスは、その中にネットワーク部とホスト部を持つ。ネットワーク部とホスト部の境界線を決めるのがサブネットマスクである。サブネットマスクは IP アドレスと同じく 32 ビットで与えられ、以下のような特徴を持つ。

- 前半 $n$ ビットはすべて 1 で、後半 $32-n$ ビットはすべて 0 である。
- 上記の性質のため、IP アドレス ($aaa.bbb.ccc.ddd$) に対して、$aaa.bbb.ccc.ddd/n$ という形式で与えられることもある。

ある IP アドレス (を 2 進数表記したもの) とサブネットマスク (を 2 進数表記したもの) との AND をとると、「ある IP アドレス」が 1 つ生成される。サブネットマスクによって作られるアドレスをネットワークアドレスという。ネットワークアドレスの意味は、その IP アドレスが属しているネットワークの名前である。

例)192.168.7.53/28 は 192.168.7.48 のネットワークに属している。この時、192.168.7.48/28 ～ 192.168.7.63/28 までの IP アドレスは同一のネットワークに属している。

上記の例で、192.168.7.48/28 をネットワークアドレスというのに対し、192.168.7.63/28 をブロードキャストアドレスという。

## 3.2　CIDR と経路集約

複数のネットワークをまとめて 1 つのネットワークと見て扱うことを集約という。集約によってサブネットマスクの長さがクラスの概念に縛られないようにする技術を CIDR という。

例)

- 192.168.1.0/24
- 192.168.3.0/24
- 192.168.6.0/24

の 3 つのネットワークはどれも 192.168.0.0/21 のネットワークに属している。よって、この 3 つのネットワークを集約すると 192.168.0.0/21 となる。

上記の例のように複数のネットワークを 1 つのネットワークとして再構成することをスーパーネット化という。

集約によってルータのルーティングテーブルを簡略化できる。

イメージ)

「魚住駅に行きたいなら北に歩いて」
「郵便局に行きたいなら北に歩いて」
「バスに乗りたいなら北に歩いて」

という 3 つの案内をまとめると、「公共施設を利用するなら北に歩いて」となる。それぞれの詳細な位置はひとまず北に歩いてもらってから別の案内人に尋ねてもらう。

このように、経路情報をまとめることを経路集約という。

## 3.3 IPv6

32 ビットの IPv4 が枯渇したため、IPv4 に代えるために登場した IP アドレスの規格を IPv6 という。IPv6 の特徴は

- 128 ビットあり、前半 64 ビットがネットワーク部となる。
- xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx のように、16 進数 4 桁のブロックをコロンで 8 個並べて表記する。
- IPv4 との互換性はない。(ヘッダが軽くなっている)
- IPsec が標準実装されているので通信は暗号化される。

IPv6 を使えば $3.40 \times 10^{38}$ 個の IP アドレスの割り当てが可能になる。

# 4　アプリケーション

## 4.1　DNS(ドメインネームシステム)

IP アドレスとドメイン名とを対応付けるシステム。

例)202.251.88.7 に http GET リクエストを送ると www.akashi.ac.jp の情報が返ってくる。

### 4.1.1　ドメイン名

www.akashi.ac.jp を例に取る。

| | |
|---|---|
| jp | トップレベルドメイン (TLD) |
| ac | セカンドレベルドメイン:組織や地域を表す |
| akashi | サードレベルドメイン:企業や団体の名前を表す |
| www | ホスト名 |

- トップレベルドメイン
  トップレベルドメインには 2 種類ある。
  - ccTLD(カントリーコード TLD)
    jp(日本),fr(フランス),de(ドイツ) などのように国を表す。
  - gTLD(ジェネリック TLD)
    com(企業),net(プロバイダ),org(団体) のように特に国籍を指定せず、組織の性質を表す。ただし、現在ではいくつかの gTLD を組織の性質にかかわらず使用できるようになっている。
- セカンドレベルドメイン
  co,or,ne,ac,ed,go などのように組織の性質を表す。
  TLD が gTLD の場合はやってることがかぶるのでセカンドレベルドメインを省略する。

## 4.2　電子メールシステム

SMTP　Simple Mail transfer Protocol(簡易メール転送プロトコル)。SMTP は 2 つの仕事をする。

- メールクライアント (MUA) からメールサーバにメールを送信する。
- メールサーバのメール転送エージェント (MTA) 間でメールを転送する。

POP　Post Office Protocol(郵便プロトコル)。メールサーバのメールをクライアントにコピーして、メールサーバからメールを削除する。オフラインでもメールが見られるが、複数のコンピュータでメールを共有することはできない。

IMAP　Internet Mail Access Protocol。メールサーバのメールをクライアントにコピーするが、メールサーバからは削除しない。サーバのデータ容量は増えるが、複数のコンピュータでメールを共有できる。

MIME　Multipurpose Internet Mail Extensions(多目的インターネットメール拡張)。電子メールのヘッダフィールドを拡張して、多国語言語 (文字コード) や画像、音楽などを扱えるようにする。

S/MIME　Secure/MIME。MIME を暗号化する。

## 4.3 DHCP(Dynamic Host Configuration Protocol)

クライアントコンピュータは物理的にネットワークに接続されると、とりあえず 255.255.255.255 宛のブロードキャスト通信を行う。DHCP サーバはその要求に対して DHCP ACK を返し、以下のものをクライアントに割りつける。

- IP アドレス
- サブネットマスク
- デフォルトルータ
- DHCP サーバの IP アドレス

など

なお、DHCP ACK は早いもの勝ちなので複数の DHCP サーバを立てていると、正しいネットワークパラメータが割りつけられずネットワークに繋がらないことがある。

## 4.4 WWW

ブラウザが WWW サーバに URL 要求を送ると、リプライとして HTML ファイルが返ってくる。これを HTTP 通信という。

HTTP　HyperText Transfer Protocol。80 番ポートを利用して Web ブラウザと Web サーバとの通信を規定する。