

インターネット基礎理論 07 インターネットのプロトコル

はじめに

資料置き場

<https://sammyppr.github.io>

に授業資料を置いていきます。復習に使ってください。

欠席した場合などはスライドを確認して追いつくようにしましょう。

スライドあるなら授業受けなくていいや

なんてことは思わないようにお願いします。



コンピュータ基礎理論

前回のDNS,IPアドレスに引き続き、
TCP/IPの仕組み,サーバ・クライアント,プロトコル等について学習します。

おさらい

- IPアドレス (IPv4, IPv6)
- WAN/LAN
- プライベートアドレス・サブネットマスク・ルータ・ゲートウェイアドレス
- DHCP
- DNS

インターネットのプロトコル

コンピュータの情報のやりとりの仕方

コンピュータとコンピュータとを繋ぐにあたって、様々な場所を経由して、情報をやりとりする、ということを説明しました。

実際に、どのように情報をやりとりしているのでしょうか？

例えば...

複数の糸電話を考えてみましょう。

特定の二人が話続けていると、他の人はその糸を使うことはできません。

混信してしまいます。

このようなやり方では、いろんな人が情報をやりとりすることができません。

そこで...

同時に複数のコンピュータが情報をやりとりすることができるように、一つの情報を小分けにしてバケツに入れて運ぶやり方がとられています。

このバケツのことを

パケット(packet...直訳：小さな包み)

と呼びます。

小分けにすることによって、ネットワークの帯域を連続して専有することがなくなるため、同時に複数の通信が可能となっています。

小分けでうまくいくの？

一つの情報を送るのに、例えば10個のパケットに分けることができたとします。

10個全部送れた場合は問題がないのですが、ネットワークには障害がつきものです。

9個しか送れなかった場合、どうなるのでしょうか？

小分けでうまくいくの？

もちろん、1/10の情報が欠落してしまうために、情報は正しく送ることができないため、送られたほうは困ってしまいます。

さて、では実際にTCP/IPではどのように情報をやりとりしているのでしょうか。

TCP/IPはいい加減

10個送って10個届く技術を研究するより、

どうせ、どっかでなくなるでしょ？

と思ってたほうがうまくいく、という良い意味での発想の転換によりTCP/IPは生まれました。

それじゃ、情報やりとりできないじゃん

どうせどっかでなくなるのに、正しく全ての情報を到達させるにはどうしたらいいでしょうか？

8番目の荷物がきてないんだけど、
もう一度送って！

とリクエストすればいいのです。

情報は荷物と違い複製可能

デジタルの情報は実際の荷物と異なり、複製が可能です。

よって、なくなってもそんなに困らないわけです。

この利点を利用した素晴らしい方法だと思います。

もちろん、届かない場合もある

もちろん、受け取り側が拒否をすれば、情報は届きません。

そういう場合は、エラーとなります。

動画で見よう

- パケットの中身を見てTCP/IPを絶対に理解したい

パケットを見てみよう！

では、実際に、パケットを見てみましょう。

ソフトウェアはgoogleで

| packet sniffer mac/win

等とすると、直ぐに見つかります。

ここでは、Wiresharkというソフトウェアを利用します。

サーバ・クライアント

一般社会でいう「クライアント」

「クライアント」という言葉は日常生活でも仕事を始めるとよく使われます。

どういう意味だかわかりますか？

仕事上の取引先、つまりその仕事の依頼人のことを指します。

コンピュータの世界の「クライアント」

コンピュータの世界でも「クライアント」という言葉をよく使います。

例えば、ブラウザでgoogleのページを表示したい、という場合

表示したいと思うコンピュータのことを「クライアント」
と呼びます。

サーバ

それに対して、googleのページのデータを送り出すコンピュータのことを

「サーバ」

と呼びます。

サーバ・クライアント

まとめると

サーバ(server): サービスを提供するコンピュータ

クライアント(client): サービスを受けるコンピュータ

となります。

ちなみに

サーバ・クライアントを、それぞれ

サービスをする・サービスを受けるコンピュータ

と定義しましたが、その機能を持つアプリケーションのことを指すこともあります。

プロトコル

OSI参照モデル

プロトコルとは「約束事」のことですが、いくつかのレイヤーに分けて考えます。

一番詳しいのは

- [OSI参照モデル] (<https://www.itmanage.co.jp/column/osi-reference-model/>)

と呼ばれ、7つのレイヤーに分けて考えます。

TCP/IPプロトコル通信の階層

- アプリケーション層
- トランスポート層
- インターネット層
- ネットワークインターフェイス層

と4つのレイヤーに分けて考えます。(少し簡略化して考えます。)

- TCP/IPとは？通信プロトコルの階層モデルを図解で解説

TCP/UDP(後述)がトランスポート層となりますが、普通の人はこちらまで気にしないでいいです。

Webサービス

ホームページを見るためには、

Webサーバ: Webの情報を保持し、依頼に応じて、情報を提供するコンピュータ

Webクライアント: Webを見るためのブラウザ

が必要であり、

Webサーバー: Apache, Microsoft, nginx

Webクライアント: InternetExplorer, Google Chrome, Firefox, Safari, Opera, Sleipnir

が代表的なソフトウェアになっています。

最近ではArcと呼ばれるブラウザが注目されています。

Web用のプロトコル

TCP/IPを利用して、情報をやり取りしているのですが、Webの情報のやり取りにはその上の概念として

http: HyperText Transfer Protocol

https: HyperText Transfer Protocol Secure

が規定されています。

httpsは個人情報を扱ったり等セキュリティが重要となる通信で広く用いられています。

httpとの違いは、暗号化されている、ということです。

httpsの必要性

先ほどのように、パケットを盗み見ることは簡単です。その中には人が読めるデータも存在しました。

例えば、ID,Passwordが暗号化されていなければ、簡単にバレてしまうことになります。

よって、暗号化する必要があります。

ファイル転送サービス

ファイルをやり取りするにはもちろんwebサービスも利用できますが、元々はFTPというやり方を利用していました。

FTPサーバー: ファイル置き場を提供するコンピュータ

FTPクライアント: FTPサーバにファイルの設置などを依頼するコンピュータ

ファイル転送用のプロトコル

ファイル転送用のプロトコルは

FTP: File transfer protocol

SFTP: SSH File transfer protocol

と呼ばれています。

SSHはSecureShellという、暗号や認証の技術を利用して、安全にリモートコンピュータと通信するためのプロトコルであり、それを利用してファイルを転送するのがSFTPとなっています。

その他のファイル転送用のプロトコル

WebDAV: Web-based Distributed Authoring and Versioning

というものがありません。

これは、httpを拡張したものであり、Webサーバに対して直接ファイルのコピーや削除を行ったりすることが可能になります。

が、現在では非推奨となっています。

WebDAVは、設計が古いプロトコルを使用しているため、現代のセキュリティ要件を十分に満たせないという問題があります。特にパスワード認証の仕組みが弱く、強固なセキュリティ対策が求められる現代の標準では不十分となります。例えば、過去にWebDAVに関連する複数のセキュリティ脆弱性が報告されており、攻撃者に悪用されるリスクがあります。このように、WebDAVはセキュリティ上に不安があるとして利用が推奨されなくなりました。(WebDAVとは？リスクと非推奨の理由、代用ツールを解説！)

メール用のプロトコル

メールには2つの役割の違うサーバがあります。

- メール送信用
- メール受信用

どうしてこのようになっているのでしょうか？

メールの仕組み

メールを送信するコンピュータが送信しようとするとき、受信するコンピュータの電源が入っているとは限りません。

メールを送ることができません。

それではメールを利用することができなくなります。さて、どうしましょう？

私書箱

インターネット上に私書箱を用意し、
必要な時にメールが届いているかどうかを確認する
という仕組みになっています。

送信用プロトコル

送信用には

SMTP: Simple Mail Transfer Protocol

を利用します。

「シンプル」とついている理由は、このプロトコルはほんの僅かな命令しか必要としないからです。

(HELO, MAIL FROM, RCPT TO, DATA, QUIT)

受信用プロトコル

受信用には

POP3: Post Office Protocol Version 3

を利用します。

IMAP: Internet Message Access Protocol

というものもあります。これは、メールの受信状況をサーバーが取得しているため、どこからアクセスしても、同じようにメールを利用できる、というものになっています。

メールまとめ

メーラーは

- 送信するときにはSMTPサーバーを利用
- 受信するときにはPOP,IMAPサーバーを利用

ということになります。

ブラウザを利用してメールを利用できるのはどうなってるの？...黒板で説明します。

ポート

コンピュータにはIPアドレスが振られていますが、

ポート

という概念があります。ポート番号は0-65535の数字が振られ、

- ポート番号にアクセスがある
- それに対応するアプリケーションが反応する

という流れになっています。

ポート番号一覧

ポート開放

ネットワークの環境によっては、うまく動かないアプリケーションなどがあります。

この原因は「ファイヤーウォール」と呼ばれる仕組みによって、ポート番号へのアクセスを拒否しているからです。

その場合には、「このポート番号使いたいんだ！」と設定しないといけません。

その他

他にも

- telnet
- dns
- ntp

等、いろいろなプロトコルがあります。

インターネットのルールの決め方

インターネット上のルール

さて、このようにいろいろなルールが決められ、それを利用しながらインターネットは発展してきたわけですが、

どのようにこのルールは決められてきたのでしょうか。

従来型

従来であれば、いろいろな会社が、「これにしよう」と提案し、市場をとった技術が採用される、というものでした。

インターネットでは？

それに対して

RFC: Request for comments

というやりかたでインターネットは発展してきました。

日本語でいうと「コメント募集」です。

つまり、「こんなの考えたんだけど、どう思う？」というのを繰り返して出来上がったのがインターネットなんです。

インターネット10分講座：RFC

脱線... 他にも

コンピュータの人たちは、そういうちょっとしゃれっぽいのが大好きです。

次がなぜおもしろいかわかりますか？

- FAQ
- GNU

UDP

UDPとTCP

TCPではエラーがあったら再送する、という方法で通信を行っていました。

一方、例えば、ライブ映像を送信するときには正確性は必要でしょうか？ライブで見たいので、多少のデータロスを目を瞑ることができます。

この「送りっぱなし」のプロトコルをUDPと言います。

HTTPのバージョンについて

HTTP/1, HTTP/2, HTTP/3

http,httpsについては暗号化されているかいないか、という話をしましたが、httpにはバージョンがあります。

- HTTP/2とは？HTTP/1.1との違い
- HTTP/3とは？HTTP/2との違い（quic・udp）をわかりやすく紹介
- なぜHTTP/3は急速に普及していったのか、その利点とは？

QUIC

TCPの利点をこれまで説明してきましたが、HTTP/3ではQUICと呼ばれるUDPベースの技術を利用しています。

UDPプロトコルの持つ速さと 発展性 に、TCPプロトコルの持つ信頼性を組み合わせた新しいプロトコル
を利用しています。

- [GoogleのQUICプロトコル](#)：TCPからUDPへWebを移行する

Chromeでは「開発者ツール」 - 「Network」 で、タイトルを右クリックして「Protocol」にチェックを入れることで、どのプロトコルが使われているのか確認できます。

HTTP/3 利用率

- Usage statistics of HTTP/3 for websites

HTTP/3 ? HTTP/2 ?

- HTTP/3として知られるQUICは高速インターネット環境ではHTTP/2に大敗することが判明

HTTP3 動画

- [HTTP/1 to HTTP/2 to HTTP/3](#)
- [HTTP 3 Explained](#)

時間あまっていたら...

- ローカル開発環境
- 仮想環境

小レポート

「サーバ・クライアント・パケット」という言葉を使い、インターネット上でどのように情報がやりとりされているか説明せよ。また、インターネットのプロトコルについて簡単にまとめよ。(manaba)