コンピュータネットワーク

大滝 博祐

August 15, 2025

Chapter 1

コンピュータネットワーク

1.1 コンピュータ・ネットワークとは

コンピュータネットワークとは、複数のコンピュータがお互いに繋がりあったもの。この無数のコンピュータネットワーク同士がさらに繋がり合ってできたのが**インターネット**。つまり、世界中の無数のコンピュータネットワークがつながったネットワークのネットワークがインターネット。

1.2 Wi-Fi と携帯会社

Wi-Fi とは無線 LAN のことで、ワイヤレスで機器をルータに繋ぐ技術。Wi-Fi そのものは電波のやり取りにすぎず、インターネットにつなげるには別に回線が必要。
Wi-Fi や 4G や 5G でスマホや PC からルータもしくは全国に設置されている携帯基地局に繋ぐ。
携帯会社はスマホなどをインターネットや電話につなげるためのインフラとサービスを提供する会社。携帯会社はインターネットにアクセスする 1 つの手段にすぎない。
携帯会社はもっと大きい会社とつながって、そこからインターネットに出ている。大きい会社は大きい会社同士がつながってインターネットができてる。

1.3 OSI 参照モデル (アプセトネデブ)

第 7 層	アプリケーション層	具体的な通信サービスを提供
第 6 層	プレゼンテーション層	データの表現形式に関する機能を提供
第 5 層	セッション層	通信の開始から終了に至るまでの手順を提供
第 4 層	トランスポート層	エラー訂正や再送など通信管理機能を提供
第 3 層	ネットワーク層	経路選択や中継によって任意の対象同士の通信を提供
第 2 層	データリンク層	直接的に接続した機器間の情報のやりとりを提供
第 1 層	物理層	コネクタ形状、ピン数、電気信号の形状などを決める

1.4 基本的な用語 1

ポート	接続口、コネクタ、端子
フレーム	データリンク層を流れるデータのこと
MAC アドレス	フレームをどの端末へ送れば良いのかを示すもの (=物理アドレス)
再送	通信の上位プロトコルが送ったデータが相手に届いてない、もしくは届いたか確認できないと判断したときに、もう一度同じデータを送ること

1.5　2 進数表現

ポート	接続口、コネクタ、端子
フレーム	データリンク層を流れるデータのこと
MAC アドレス	フレームをどこへ送ればいいかを示すもの (=物理アドレス)

bit	2 進数の 1 桁
8bit のまとまり	1 オクテット
バイト	8bit のまとまり
バイトは普通は 8bit。バカなメーカーとかだと 7bit のこともある。オクテットは必ずバカでもなんでも 8bit を指す	

2^0	1
2^1	2
2^2	4
2^3	8
2^4	16
2^5	32
2^6	64
2^7	128
2^8	256
2^9	512
2^{10}	1024

1 オクテット (8 ビット) フルビット=255

1.6　用語 2

ユニキャスト	指定する相手に 1 対 1 で送信
ブロードキャスト	ネットワーク内の全てに送信
マルチキャスト	グループに属するすべてに送信

1.7　ハブ、スイッチ、ルータ

ハブ	制御できない。複数のデバイスを接続して、送信元以外のすべてのポートにデータ送る。だから、データの衝突が起こる。なんですべてに送るの？ どこに送ればいいかわからないから当たるといいなって全部に送るの？ バカなんですか？ A. バカハブと呼ばれたりする。レイヤー 1
スイッチ	ネットワーク内で MAC アドレスでフレームの送信の制御をする。データの衝突が起こらないように制御をする。レイヤー 2
ルータ	他のネットワークとのやり取りを制御する。スイッチと同じように衝突が起こらないように制御する。レイヤー 3

スイッチやルータは MAC アドレステーブル (MAC アドレスと接続ポートの対応表) で制御する。つまり、MAC アドレステーブルはスイッチやルータが内部で管理している。

1.8　データリンク層

MAC アドレスは、6 オクテットの唯一無二で、製造時に書き込まれた変更不能な番号。6 オクテットなのは MAC アドレスで、IPv4 アドレスは 4 オクテット。別物。

- スイッチ (スイッチングハブ) は、ポートに**入ってくるフレームから、送信元 MAC アドレスを**一定時間 MAC アドレステーブルに記録する。**宛先じゃないよ。入ってきたやつを記録するんだよ。**
- 通常の動作 (宛先がユニキャストフレーム、つまりブロードキャストフレーム FF:FF:FF:FF:FF:FF 以外) のときは、MAC アドレステーブルを参照して特定のポートにフレームを転送する。
- 宛先 MAC アドレスが MAC アドレステーブルに記録されてないときは、入ってきたポート以外のすべてのポートにフレームを転送する。これを**フラッディング**という。

- **上のフラッディングとは別のお話**で、入ってきたフレームの送信元 MAC が MAC アドレステーブルにないときは、次回以降もしその送信元 MAC に転送することがあったら転送できるように、スイッチがこの**送信元 MAC アドレスを MAC アドレステーブルに追加する。フラッディングした宛先 MAC を保存することはできない。**
- 宛先がブロードキャストフレーム FF:FF:FF:FF:FF:FF のときは、入ってきたポート以外のすべてのポートにフレームを転送する。
- 宛先 MAC アドレスに対応するポートが送信元 MAC アドレスと同じだった場合、スイッチはフレームを破棄する。なぜなら、転送する意味がないから。

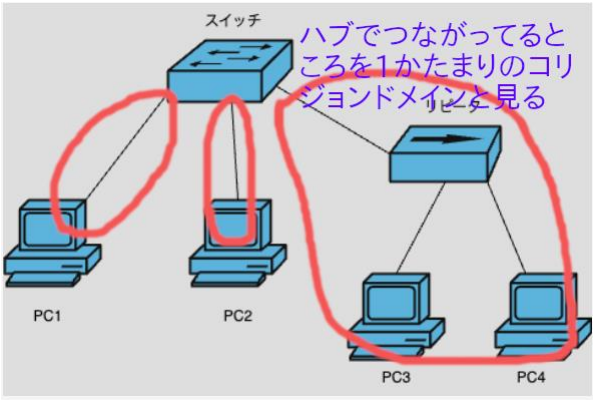
すべてのポートに転送されるフレームも、実際には接続先がないポートには転送されないので、テストのときは FF:FF:FF:FF:FF:FF やフラッディングですべてのポートに転送するときは、送信元ポートの他に**接続先がないポート**も**除外**すること。
リンクアップ状態 (接続されて正常に動いている状態) のポートのみに実際に電気信号が出力されて、リンクダウン状態 (切断されて動いていない状態) のポートには実際に電気信号が出力されない。

1.8.1 コリジョンドメイン

コリジョンドメインとは、データの衝突が発生する可能性がある範囲のこと。リピータ、リピータハブは送られてきたデータを接続されている機器すべてに送るので、衝突が起こる。ブリッジ、スイッチは、コリジョンドメインを分割する。ブリッジやスイッチは通信の制御を行い、宛先だけにフレームを転送する、つまり不要なフレームを宛先以外には送らないので衝突する範囲を分けることができる。言い方変えると、分けるんだからコリジョンドメインを増やす。衝突する恐れのある範囲を小さくする。

1.8.2 ブロードキャストドメイン

ブロードキャストフレーム (FF:FF:FF:FF:FF:FF のネットワーク内すべてに送信するフレーム) が届く範囲。ある端末からスイッチへブロードキャストフレームが送られると、スイッチはそのフレームをすべての端末へ送信する。だから、スイッチはブロードキャストドメインをまとめる。ルータは、ネットワークを分けるので、ブロードキャストフレームが届く範囲 (ブロードキャストドメイン) を分割する。言い方を変えると、分けるんだからブロードキャストドメインを増やす。届けなきゃいけない範囲を小さくする。



ハブから伸びてるところ (ハブでつながってるところ) を、1 つのかたまりと見る。上に繋がってるとか下に繋がってるとか関係ない。ハブから伸びてるのは全部同じ。
(ハブでつながってるところはデータの衝突が起こるから。)

1.9 フレームの中身

フレームには、宛先 MAC アドレス、送信元 MAC アドレス、送りたいデータ (パケット、ペイロード) が含まれる。他にもタイプ (データのデータの種類や長さを示す)、FSC(フレームチェックシーケンス、エラー検出用の CRC コード)、プリアンブル (通信開始を知らせて機器の同期を取るための信号) が含まれる。フレームは複数のフィールド (項目) で構成されてるため、よく表 (フォーマット表) で表される。

プリアンブル	宛先 MAC	送信元 MAC	長さ/タイプ	パケット (カプセル化されたデータ)	フレームの最後

1.10 IP アドレス

世界中のコンピュータと通信したい。コンピュータを区別するには番号をつければ良い。インターネットを作った人たちは、4 オクテットあれば十分だと考えて作った。この 4 オクテットのコンピュータを区別する番号が IPv4 アドレス。4 オクテット (32 ビット) だと扱いにくいので表現するときは、4 つのオクテットの分割して、それぞれを 10 進数に直し、ドット区切りで表す。IP アドレスをコンピュータなどのホストにくばるのに、ホスト 1 台 1 台にバラバラに配るのは大変。そこで、ある組織に先頭から n 番目までのビットまで配って、残りはその組織内に任せたほうが楽。だから、組織内では IP アドレスの先頭から n 番目までのビットが共通している。この共通した部分を IP アドレスの**ネットワーク部**、残りの部分を**ホスト部**という。つまり、ネットワーク部が長いとホスト部で使える分が小さくなるし、ネットワーク部が短いと、ホスト部で使える分が大きくなる。短い

ネットワーク部だと、それ以下の数字のアドレスはすべて占領されることになる。だから大して IP アドレスを使わないのに、短いネットワーク部をもらってしまうと、多くの IP アドレスを占領してしまうことになる。IPv4 アドレスは枯渇してしまったので、新規に割り当てる余地はないので、根本的には 16 オクテットの IPv6 アドレスへの以降が必要。(v4 は 4 オクテット、v6 は 16 オクテット)
上記の通り、ネットワーク部のアドレスが割り当てられ、ホスト部は自由に割り当てて良いが、2 つ、ホスト部に割り当てられないアドレスがある。ホスト部がすべて 0 のアドレスは組織のネットワーク自体を表す**ネットワークアドレス**というアドレスとして決められている。もう一つは、ホスト部がすべて 1 のアドレスで、組織内のすべてに一斉にメッセージを送るための**ブロードキャストアドレス**と決められている。

1.11 ネットマスク

- IP アドレスの中でネットワーク部が先頭から N ビットであることを示すため、IP アドレス/N という記法 (マスクビット) を使う。(/マスクビット)

- もう一つ、どこまでがネットワーク部かを示す方法があって、それがネットマスク。2 進数で IP アドレスを見て、ネットワーク部の数字をすべて 1 にして、残りのホスト部の数字をすべて 0 にした極端な IP アドレスを作り、それぞれを 10 進数にして IP アドレス表現をする。これでできたのがネットマスク。

1.12 IP アドレスのクラス

昔は、ネットワーク部が N ビットであることを表す/N という書き方は発明されていなかった。IP アドレスが決まればネットワーク部が何ビットかが自動的に決まる仕組みだったから。ドットで区切られたアドレスの 1 つを 1 オクテットの 2 進数で見たときに、最初のビットが 0 だったらネットワーク部は 8 ビットと決められていた。これをクラス A の IP アドレスという。クラス A の IP アドレスでは、最初のアドレスが 0 から始まるので、1 オクテット目は 00000000 から 01111111 までなので、10 進数にすると 0 から 127 で、このときネットワーク部は 1 オクテット目までなので、ネットマスクは 255.0.0.0 になる。
先頭の 2 ビットが 10 であれば、ネットワーク部は 16 ビットまでと決められていた。これをクラス B の IP アドレスという。
先頭の 3 ビットが 110 であれば、ネットワーク部は 24 ビットまでと決められていた。これをクラス C の IP アドレスという。
IP アドレスのクラスだと、ネットワーク部は 8 ビット、16 ビット、24 ビットと 1 オクテット区切りだったが、/n が使われるようになってから、1 オクテット区切りの途中までネットワーク部で、途中からホスト部というオクテットがあってもよくなった。

1.13 サブネットの設計

たいていの組織では、組織の中に、さらに組織 (部門、部署) がある。部門ごとにグループ分けをする。与えられたネットワークにおいて、ネットワークを分割して、それぞれの部門が独立したネットワークであるようにしたい。分割されたネットワークを**サブネット**という。

1.13.1 2 等分

192.168.10.0/24 を 2 つに分けるとき、もともとのホスト部の長さが 8 ビットの長さなので、この最初の 1 ビットをネットワーク部にしちゃって (貸出し)、ホスト部の最初の 1 ビットをネットワーク部のように扱う。そうすと、ネットワークアドレスは、ホスト部 8 ビット分が 00000000 と 1000000 の 2 つができる。よって、2 分割後のネットマスクは、11111111.11111111.1111111.00000000 と 11111111.11111111.1111111.10000000。2 つのネットワークアドレス (ホスト部がすべて 0) は 11000000.10101000.00001010.00000000 192.168.10.0/25 (ホスト部の最初の 1 ビットを含めた 25 ビットまでがネットワーク部みたいにしてるから) と 11000000.10101000.10000000 ⇔ 192.168.10.128/25

1.13.2 4 等分

ネットワークを 4 頭分するには借りるビットを 2 ビットにすればいい。なぜなら、2 ビットで表現できる数は 00, 01, 10, 11 の 4 つあるから。ネットマスクだと、ネットワーク部はすべて 1 にするが、得られるネットワークはその借りたビットが 0 のときのネットワークと 1 のときのネットワークが得られる。だって借りたネットワーク部は元々ホスト部だったのでこっちで自由に変えられるから。元々与えられたネットワーク部はもっと上に割り当てられたものだから変えられない。ネットマスクと得られるネットワーク、オクテット (8 ビットの 2 進数) という指定に気をつける。

1.13.3 8 等分

$2^3 = 8$ より 8 等分する (8 個のアドレスを生み出す) には 3 ビット借りれば良い。

1.13.4 サブネット ID

サブネット ID とは、ホスト部からもらったビット (4 等分なら 00, 01, 10, 11) を 10 進数にしたもの。(ホスト部からもらった (借りた) ビットを拡張ビットという。) だから、4 等分ならサブネット ID は、(00 = 0, 01 = 1, 10 = 2, 11 = 3) の 4 つ。だか

ら、サブネット ID が 3 のときと指定があれば、何桁かの 2 進数に 1 足してったときの 0 から数えて 3 番目。
求め方は、

1. 元のネットワーク部のビット数より、ホスト部を確認。
2. 実際のサブネット (/N なら N) と比較して、借りたビット数を計算する。
3. サブネットの元のホスト部だった部分を 2 進数にして、借りたビットを抜き出して、2 進数から 10 進数に変換する。これがサブネット ID となる。

実際に求めてみる。

1. 192.168.10.0/24 のネットワーク を 4 等分したとき、192．168．10．64 / 26 のサブネット ID を求める。
2. 元のネットワークのネットワーク部は/24 なので、24 ビットまでだから、ホスト部は 8 ビット。
3. サブネットマスクは/26 なのでネットワーク部が 26 ビットで、ホスト部が 6 ビット。つまり、借りたのは 8 - 6 = 2 ビット分。
4. 64 を 2 進数にすると 01000000(8 ビットで表す) で、上位 2 ビットを借りているので、上位 2 ビット 01 を十進数にしたのがサブネット ID = 01 = 1//

1.14 固定長サブネットマスク

これまでのサブネットマスクはネットワークを、すべて同じ大きさに等分している。これを**固定長サブネットマスク**という。だから x ビット確保すると、2^x 個のアドレスを確保する。2 の累乗個のアドレスしか確保できないので、5 つのサブネットを得るには、2 ビットだと 4 個なので足りないので、3 ビット借りて 8 個得る必要がある。このとき 3 つも利用されないサブネットができてしまう。

1.15 ネットワーク層 レイヤ 3

外のネットワークとの接続、通信するための経路選択 (ルーティング) を行う。別のネットワークに属するホスト同士でデータをやり取りするために IP アドレスを用いる。

1.15.1 単語 3

ホスト	つながっているコンピュータ
ルータ	ネットワーク同士をつなげて、必要に応じてデータを転送する。宛先 IP アドレスを見て、どのネットワークにどのネットワークにデータを転送すればよいかを決める
ルーティングテーブル	ルータが記録しているネットワークの経路表。あるルータ以下にあるネットワークに送りたいとき、ここのルータに送ればあとはルータがやってくれるという IP アドレスがあるやつ。
パケット	ネットワーク層を流れるデータ
デフォルトゲートウェイ	ある機器が属しているネットワークの出入り口。ある機器が属しているネットワークの出入り口。
直接繋がっているネットワーク	別のルータを介さずに繋がっているネットワーク
スタブなネットワーク	ネットワークの末端。スタブなネットワークに繋がってる PC を選べと言われたら、ネットワークの末端になってる PC すべてを選ぶ。1 つじゃなくてもいい。ネットワークの末端なら、2 つでもいい。そのネットワークからどこかのルーターから下に伸びてないネットワーク の末端全部。 (外部との接続経路が一つしかない。スタブなネットワークでは、他のネットワークに出るにはその唯一のルータ (ゲートウェイ) を通るしかないので、デフォルトルートとしてホストに設定する。)

1.16 ARP(アープ)(Address Resolution Protocol)

ARP とは、同じメディアにぶら下がっている（共有メディアにぶら下がっている）ホストが IP アドレスを使って MAC アドレスを知る方法のこと。同じメディアにぶら下がっているといういうことは、同じグループということ。同じグループということは IP アドレスのネットワーク部が同じということ。同じメディアにぶら下がっているということはブロードキャストが届くということ。ブロードキャストが届く範囲が同じネットワークということになる。通常は宛先 MAC が自分の MAC であるフレームのみをホストは受け取る。そうでなければフレームは破棄される。ただしブロードキャストフレーム (FF:FF:FF:FF:FF:FF) は全てのホストが受け取る。
（教科書 p167 図 6-37 ARP 処理の流れ）

ホスト A が，192.168.1.4 のホストと通信したいが，MAC アドレスがわからない．
ホスト A からブロードキャストフレームを宛先 MAC として，「この IP を持っているホストは，MAC アドレス教えて」という **ARP リクエスト**のパケットを，同じメディアにつながっているホスト全てに問い合わせる．
該当の IP アドレスを持つホスト D は，**ARP リプライ**のパケットをホスト A の MAC アドレス宛てに送る．
ホスト A は，192.168.1.4 のホストと通信するには，ホスト D の MAC アドレスを宛先にすればよいことがわかる．
ARP の仕掛けのおかげでネットワーク内で IP アドレスから MAC アドレスを知ることができる．

Chapter 2

実技

2.1 RaspberryPi3 の設定

実験室では、大量の LinuxPC を買うのにお金がかかるから RaspberryPi3 を使用する。RaspberryPi も Linux ベースに作られているので RaspberryPi でできることはほとんど Linux でできる。

1. HDMI ケーブルをつなげる
2. コンソールケーブル -> LAN ケーブルの繋げ方
   - RaspberryPi3 でルータの (Linux でいう端末) を見るために、ルータからコンソールケーブルを RaspberryPi に接続。
   - ハブにネットワークを送るために、LAN ケーブルをスイッチに接続。(スイッチを通してネットワークを拡張
   - で、そのスイッチからネットワークを引っ張ってくるために、スイッチから RaspberryPi に LAN ケーブルを繋げる。
   - 学校のスイッチでは、1 4 番ポートで給電ができる。
   - ケーブルの違い
     色が違っても中身は同じ LAN ケーブル。8 つのピンがある差込口にいれる。CATEGORY なんとかって書かれてるやつはだいたい LAN ケーブル。明らかに様子が違う青い USB 変換アダプタが接続されているやつは、コンソールケーブル。

2.2 RaspberryPi のネットワーク設定

netplan という yaml 形式の設定ファイルで設定する。yaml 形式はスペースによるインデントで構造を表す。タブだとエラーになる。netplan では/etc/netplan/以下にある.yaml ファイルを名前順に読み込み、順に上書きしていく。だから、/etc/netplan/99_config.yaml だと 99 と遅いので、デフォルトの設定だと最後に読み込まれてこれで設定されるでしょう。

2.3 netplan(ネットワーク設定) の yaml ファイル

```
network:
  version: 2
  renderer: networkd
  ethernets:
    eth0:
      dhcp4: false
      addresses:
        - 192.168.99.1/24
      routes:
        - to: default
          via: 192.168.99.254
      nameservers:
       addresses: [157.114.162.4]
```

- network:
  netplan の設定バージョン。常に version: 2 を指定する。これは、YAML ファイルの構文バージョンで、現在の構文は version2 として定義されている。
- renderer: networkd
  イーサネットのインターフェースを定義する

- routes:
  デフォルトゲートウェイを指定する

- nameservers:
  DNS サーバーの IP アドレスを指定する。

2.3.1 ネットワーク設定を反映させる

ネットワークの設定ファイルを変更した場合、それを反映させる必要がある。

- sudo netplan try
  120 秒がすぎると設定が取り消されるという猶予がある。Enter を押して確定する。

- sudo netplan apply
  実行したらすぐに設定を反映させる。sudo netplan try で Enter を押したならこれをやる必要はない。

2.4 CISCO ルータへアクセスしてルータの設定

ルータを設定するために、ラズパイとルータをコンソールケーブルで接続し、minicom というシリアル通信用のソフトを起動して、ルータにアクセスする。
やり方は

1. $ sudo minicom -D /dev/ttyUSB0 -b 9600
   これによって、CISCO ルータの画面になる。

minicom	ターミナルエミュレータの 1 つで、ルータやスイッチなどのネットワーク機器を設定するとき、シリアルポートを使ってデバイスと通信するために使用される。
-D	デバイスファイルを指定するオプション
-b 9600	-b はボーレート (通信速度) を指定するオプション。9600 は、1 秒間に 9600 ビットのデータが転送される。

2. — System Configuration Dialog —
   Continue with configuration dialog? [yes/no]: no

   これは、dialog(ダイアログ=対話) で設定するか聞かれるので no で答える。

2.5 ルータのターミナルのモード

モード

> ユーザーモード ⇔ 設定の変更はできない。システムの状態を確認するためのコマンドを実行できる。(show, ping, traceroute)
特権 (イネーブル) モード ⇔ 最も高い特権。設定変更ができる。ユーザーモードから en で入る。グローバルコンフィグモードにはいる conf t が使える
(config) グローバルコンフィグモード ⇔ ネットワーク機器の基本設定 (ホスト名、インターフェースの設定、ルーティング設定) を行う。
(config-hoge) hoge-コンフィグモード ⇔ 特定の設定を行うモード。hoge には特定の設定内容に応じた名前が入る。

それぞれ exit で手前のモードに戻る。

2.6 ルータのターミナルのコマンド

- sh run(show running-config)
  現在の設定を見る

- show startup-config
  電源投入時に実行されるスタートアップコンフィグを見る

- copy running-config startup-config
  現在の設定をスタートアップコンフィグにコピー (上書き) する。

- コマンドを間違えてしまったとき、間違えたコマンドの先頭に no をつけて実行すると、取り消すことができる。

2.7 ルータの基本的な設定

2.7.1 ホスト名を hoge にする

グローバルコンフィグモードから
Router(config)# hostname hoge でホスト名を hoge に変更
プロンプトは、ホスト名 (config)#
デフォルトのホスト名 Router -> hoge になる。

2.7.2 domain-lookup を無効にする

hoge(config)# no ip domain-lookup
domain-lookup とは、ホスト名という文字列を IP アドレスに変換しようとする機能、つまり名前解決 DNS を有効にする機能 (ルータやスイッチで)
無効にする理由は、間違ったコマンドを打っても、ルータが名前解決を試みないので、すぐにエラーになる。(解決できずに数十秒フリーズしてタイムアウトにならない)

2.7.3 各種パスワードを設定

- 特権モードに移行するときのパスワードを class に設定
  hoge(config)# enable secret class
- コンソールのパスワードを cisco に設定
  hoge(config)# line console 0
  コンソールのパスワードとは、シリアルケーブルなどでルータに物理的に接続して操作するときに求められるパスワード。
  設定対象が回線 (line) になったので、プロンプトは config-line に変わる。
  hoge(config-line)# password cisco

  hoge(config-line)# login
  上のコマンドだけじゃ不完全で、login を書くことによってログインするときにパスワードを求めさせる。
  hoge(config-line)# exit
  line(config-line) から上の階層 (config) に戻る
- VTY(仮想端末) のパスワードを cisco に設定
  VTY(仮想端末) とは、Cisco ルータやスイッチにリモート接続するための” 仮想的なログイン回線”。
  rt0(config)# line vty 0 15 rt0(config-line)# password cisco rt0(config-line)# login rt0(config-line)# logging synchronous
  show コマンドや設定コマンドを入力している最中にエラーメッセージやシステムログが表示されると操作しにくいので、logging(ログ) synchronous(同期的) で、ログメッセージを表示させるタイミングを調整して、ユーザーの入力に干渉しないようにする設定
  rt0(config-line)# exit

2.7.4 ルータでインターフェースの状態を確認

インターフェースとは、接点ややりとりの窓口 (通信口) のこと。また、物理ネットワークインターフェースとは、実際にケーブルを差し込める、ネットワーク用のポートのこと。
GigabitEthernet 0/0 のポートとは、ルータやスイッチにある物理ネットワークインターフェースの 1 つで、機器に付いているギガビット対応のネットワークポート（LAN ポート）のうち、“0 番目のカードの、0 番目のポート” を表す。

インターフェースとはルータのポート

hoge# show interface gigabitEthernet 0/0 (sh int gigabitEthernet 0/0)

このコマンドの出力は以下の通りで、インターフェースの状態 (link up or link down) や IP アドレスが割り当てられているか、機器の MAC アドレスなどが見ることができる。

出力

GigabitEthernet0/0 is up #インターフェースが物理的に有効 , line protocol is up #通信プロンプトが動作 Hardware is CN Gigabit Ethernet, address is 4c00.82a1.f120 #MAC アドレス (bia4c00.82a1.f120) Internet address is 10.88.88.100/24 #IP アドレス MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set Keepalive set (10 sec) Full Duplex, 1Gbps, media type is RJ45

2.7.5 インターフェースの状態を確認

sh int ですべてのインターフェースの状態を確認

$$\begin{cases} hoge\#\ sh\ int gigabitEthernet 0/0 & \text{指定した1つのポートの情報を表示} \\ hoge\#\ sh\ int & \text{すべてのインターフェースの状態を表示} \end{cases}$$

2.7.6 ルータの IP アドレスを DHCP で自動で設定する

1. hoge(config)# interface gigabitEthernet 0/0
   GigabitEthernet 0/0 の設定モードに入る。プロンプトが (config-if)#になり、インターフェース設定モードに切り替わる。
   hoge(config)# interface インターフェース名 でインターフェースの設定モードに入る。

2. hoge(config-if)# ip address dhcp
   このインターフェースが DHCP で IP アドレスを自動取得するように設定する。

3. hoge(config-if)# no shutdown
   CISCO ルータのインターフェースは初期状態で shutdown(無効) になっているので、それを取り消すっていうコマンド。
   このコマンドによりポートが up 状態になる。

4. hoge(config-if)# exit
   (config-if) から抜けてグローバル設定モード (config) に戻る。

DHCP とは

DHCP とは、IP アドレスなどのネットワーク設定を、自動で割り当ててくれる仕組みのこと。(ダイナミック・ホスト・コンフィギュレーション・プロトコル)

2.8 ping

ping

$ ping 宛先の IP アドレスまたはホスト名

ping で、ネットワーク接続の確認 (落ちてない？)、IP アドレスが有効か、応答速度 (遅延が大きいか) を判断できる。

2.9 ssh

ssh の書き方

$ ssh ユーザー名@IP アドレス

ssh(**S**ecure **Sh**ell) とは、ネットワークを通じて別のコンピュータを安全に操作するためにプロトコル。
自分が許可されたユーザー (ログインできるユーザー名とパスワードがある) で、SSH サーバーが動いている (sshd が起動し、ルーターでポート 22 が開放されている)、IP アドレスがわかっていて、ルーターやファイアウォールでブロックされていなかったら ssh でアクセスできる。

2.9.1 mac から ubuntu に ssh

Ubuntu 側で sudo apt install openssh-server
ip a で ip アドレスを確認。ip アドレスはネットワークに繋がっている機器に振られる番号。fuga だとする。
whoami でログインしているユーザー名を確認。whoami で hoge が出力されたとすると
mac 側で ssh hoge@fuga で Ubuntu 側のパスワードを入力。

mac に接続した USB メモリのファイルを ssh 先にコピー

scp -r /Volumes/STORE N GO 1/godot/* hirosuke@192.168.3.14: /Documents/

- scp
  secure copy protocol
  scp [オプション] [コピー元のパス] [コピー先のパス]
  リモートのパスはこうなる
  `[ユーザー名]@[IP アドレス]:[リモートのパス]`

  #### ローカルからリモート先にコピー

  scp Documents/temp.tex hirosuke@192.168.3.14:/home/hirosuke/

ディレクトリをコピー

(例) ローカルのディレクトリを ssh 先のディレクトリにコピーする。再帰的コピーが必要。
hirosuke@hoge:~/Documents/3J$ scp -r automata hirosuke@192.168.3.14:Document/

Chapter 3

IT パスポート

コンピュータとコンピュータを接続したものを、ネットワークという。

3.1 ネットワークの種類

- LAN (Local Area Network)
  企業や家庭などの、比較的狭い限られた範囲内でのネットワーク。
- WAN (Wide Area Network)
  企業と本社と支社みたいに、遠隔地にある LAN と LAN をつないだネットワーク。
- インターネット
  世界中のコンピュータや LAN を接続した巨大なネットワーク
- イントラネット
  インターネットの技術を使用して構築された、組織内ネットワーク

3.2 無線 LAN

コンピュータやネットワーク機器を LAN ケーブルで接続せず、電波でデータのやり取りを行う LAN のこと。無線 LAN を構築するには、無線通信を中継する**アクセスポイント** (通常は、アクセスポイントの機能つきの無線 LAN ルータ) が必要。コンピュータ自身には、無線 LAN アダプタが必要。
無線 LAN では、LAN ケーブルのようにネットワークの境界を物理的に設けるのが難しいため、各ネットワークを識別するための文字列である **ESSID** が使用される。アクセスポイントが、自身に設定された ESSID と同じ ID を持つ機器の通信のみを中継することで、同一ネットワークに属する機器のみで通信を行うということが可能になる。
コンピュータなどを無線 LAN に接続するには、コンピュータに ESSID や暗号化キーなどの設定を行う必要があるが、アクセスポイントからコンピュータへ設定情報を転送するだけですべての設定を完了させる規格を **WPS** という。また、LAN ケーブルで電力供給もする技術を **PoE**(**Power over Ethernete**) という。

3.2.1 無線 LAN の規格

無線 LAN の規格にはさまざまな種類があり、かつては対応する規格がバラバラで、互いに通信できないものが多くあった。現在は、Wi-Fi Alliance という団体が無線 LAN の標準規格であるアイ・トリプル・イーハチマルニドットイレブン (IEEE 802.11) に準拠した機器に対して、異なるメーカーの無線 LAN 機器どうしで相互接続を保証するブランド名 **Wi-Fi** のロゴマークを提供している。ユーザはロゴマークを見て機器をそろえればいいため、利便性が向上した。

3.2.2 無線通信の正体は電場と磁場

無線通信で使われる電波は、電場と磁場が互いに影響を与えて、電気エネルギーが波として空間を振動させることで情報を伝える。
1 秒間に何回振動するかを表したものが周波数であり、周波数の範囲を表したものが**周波数帯**。無線 LAN で使用されている周波数帯には、**2.4GHz 帯**、**5GHz 帯**と、**6GHz 帯**がある。2.4GHz 帯は、壁などの障害物に強く電波が届きやすいものの、Bluetooth 機器や電子レンジなどが出す電波から干渉を受けやすく、通信が不安定になることがある一方、5GHz 帯は、2.4GHz 帯に比べて速度が速いものの障害物に弱い。6GHz 帯は、家電などの電波から干渉されないので、安定した高速通信が可能。Wi-Fi 6E という規格では 6GHz 帯が利用可能。(Wi-Fi には 4/5/6/6E という規格がある。)

3.2.3 もっと掘り下げて、電波とは？

まわりの空間に電場と磁場が存在するから電波 (電磁波) を受信できる。
電波とは、電場と磁場が相互に影響し合いながら空間を伝わる電磁波の一種。
電子の移動によって生じるのが電気。物体が持つ電気を電荷という。

電荷間に働く力を静電気力という。
・近接作用といって、電荷がまわりの空間に電場をつくる。
・まわりの電荷はその点で、周りの電場 (ベクトル) から静電気力を受ける。

3.3 プロトコル

3.4 ネットワークの形態

3.5 ネットワークの構成機器

コンピュータ自身には、ネットワークに繋げるための入り口となる**ネットワークインターフェースカード** (**NIC**) というハードウェアが必要。最近のコンピュータには、購入した時点で内蔵されている。

3.6 モバイル通信

外出先、移動中にスマホやタブレットでインターネットに接続する場合は、電波で通信を行う**モバイル通信**を利用する。

3.6.1 Wi-Fi と携帯会社

Wi-Fi とは無線 LAN のことで、ワイヤレスで機器をルータに繋ぐ技術。Wi-Fi そのものは電波のやり取りにすぎず、インターネットにつなげるには別に回線が必要。
Wi-Fi や 4G や 5G でスマホや PC からルータもしくは全国に設置されている基地局に繋ぐ。
携帯会社はスマホなどをインターネットや電話につなげるためのインフラとサービスを提供する会社。携帯会社はインターネットにアクセスする 1 つの手段にすぎない。
携帯会社はもっと大きい会社とつながって、そこからインターネットに出ている。大きい会社は大きい会社同士がつながってインターネットができてる。

3.6.2 ハンドオーバー

移動しながらスマホを使用する場合、自動的に基地局 (またはアクセスポイント) を切り替えてくれる機能を**ハンドオーバー**という。

3.6.3 SIM カード

携帯会社との契約情報は、**SIM カード**という IC カードに記録されている。ユーザはこのカードが差し込まれたスマホを使用することで通信を行うことができる。また、カード型ではなく携帯電話機にあらかじめ組み込まれた SIM のことを **eSIM** という (embedded 組み込まれた)。後から携帯会社を変えても、ユーザがダウンロードなどによって SIM 内の契約情報を書き換えられる。4

3.6.4 ○G とは

モバイル通信の規格。1G から始まり、2G, 3G, 元 LTE(3.9G), LTE(4G), 5G と進化している。G は Generation の略。世代が上がるにつれて、通信速度が速く、大容量の通信に対応している。5G は、10Gbps 以上の通信速度を持つ。

bps	1 秒間に伝送できるビット数。b/s(bits per second)

3.7 プロトコル

共通の決まりごと、共通の手順のこと。
TCP と IP という基本的なプロトコル群である **TCP/IP** のプロトコルは以下の通り。

- HTTP
  HyperText Transfer Protocol
  Web ページをやりとりする。
- HTTPS
  Hypertext Transfer Protocol Secure
  HTTP に暗号化機能がついたもの。
- FTP
  File Transfer Protocol
  ファイルを転送するときに使う。

- SMPT
  Simple Mail Transfer Protocol
  メールを送信するのに使う。

- POP3
  Post Office Protocol version 3
  メールを受信するのに使う。サーバからメールを受信すると、サーバーから削除する。

- IMAP4
  Internet Message Access Protocol version 4
  メールを受信するのに使う。サーバからメールを受信してもサーバ上に残して管理するので、複数の端末で同じメールを読むことができる。

- NPT
  Network Time Protocol
  ネットワークにアクセスした機器の時計を正しい時刻に合わせるときに使う。

Chapter 4

セキュリティ

4.0.1 情報資産とは

コンピュータには大事な情報がたくさん入っていて、アドレス帳に登録した連絡先の情報や、クレジットカードの情報などもある。これらはすべて大事な**情報資産**であり、失くしてしまったり、盗まれて悪用されてしまわないように対策を行って守る必要がある。
情報資産を失ったり盗んだりする要因になるものを**脅威**という。

情報資産が抱える脅威には、**技術的脅威**、**人的脅威**、**物理的脅威**がある。

4.0.2 技術的要因

マルウェア

マルウェアとは、悪意のこもったソフトウェアのこと。コンピュータやデータに悪さをするために作られたソフトウェア。電子メールの添付ファイルとして送られてきたマルウェアを開いてしまったり、マルウェアの入った USB メモリを使ってしまったりすることによって感染し、さまざまな被害を受ける。通常マルウェアはファイルとして保存されたソフトウェアだが、ファイルという実体を持たずにメモリ上で実行される**ファイルレスマルウェア**もある。被害内容は通常のマルウェアと同じだが、ファイルが存在しないので検知が難しいのが特徴。
マルウェアの種類

コンピュータウイルス	今ピュータ内のファイルを破壊したり、関係のないものを画面に表示したりする。他のソフトに感染することによって増える。ワープロソフトや表計算ソフトのファイルに感染する**マクロウイルス**などがある。
ワーム	コンピュータウイルスと被害内容は同じだが、他のソフトに感染するのではなく、自身をコピーしながらネットワークに接続されたコンピュータ間を移動することで自己増殖する。
トロイの木馬	何も問題のない普通のソフトを装ってコンピュータに侵入し、データの消去やファイルの外部流出などを行う。増えることはない単独のソフト
ボット (BOT) **スパイウェア**	ネットワークを介して他人のコンピュータを操り、パスワードなどの重要な情報を盗んだり、迷惑メールの送信や、特定のサイトへの一斉攻撃などを行う。感染したコンピュータを踏み台 (攻撃するための中継地点) として利用することで攻撃元を詐称する。 ユーザが認識することなく悪意のあるソフトウェアをインストールさせ、感染したコンピュータの行動を監視し、ユーザが入力した個人情報やパスワードなどの情報を盗む。キーボードの入力情報を記録する**キーロガー**プログラムを悪用するなどして実行する。
ランサムウェア	コンピュータに保存されているデータを勝手に暗号化するなどして、ユーザが正常にデータへアクセスできないようにして、元に戻すための代金をユーザに要求する。さらに、代金を支払わなければ暗号化した情報を公開すると脅迫する**二重脅迫** (**ダブルエクストーション**) 型もある。

RAT(Remote Access Tool)

手元にあるコンピュータから、ネットワークを介して遠隔地にいあるコンピュータを操作するツールの総称を RAT という。RAT によりコンピュータに不正侵入されてデータを盗まれたり、ハードウェアを破壊されたりする危険性がある。ただ、本来は自宅から会社にある PC を操作するなどの正当な目的のために使われるツールなので、ウイルス対策ソフトでは検知できない場合がある。

バックドア

backdoor とは裏口の意味で、一度侵入したコンピュータに、後から何度でも不正ログインできるように仕掛ける秘密の入り口を**バックドア**という。

スパムメール

広告などを無差別に送りつけるメールを**スパムメール**という。BOT による踏み台を利用して送信元を偽装しているため、送り主を特定できない。

ダークウェブ

通常の検索エンジンでは見つけることができず、一般的な方法ではアクセスできない Web サイトを**ダークウェブ**という。通信経路を秘匿する特殊なソフトウェアを利用するので、秘匿性が高く、違法性の高い情報や商品の取引に利用されている。悪意のある利用者も多いので、不正にアクセスするとマルウェアに感染したり、サーバー犯罪に巻き込まれる危険性がある。

4.0.3 人的脅威

人が原因である脅威。

- ソーシャルエンジニアリング
  本人を装ったり、緊急事態を装ったりして組織内部の機密情報を聞き出すなど、人間の心理の隙きをついて情報を盗む行為を**ソーシャルエンジニアリング**という。
- 悪意をもって他人のコンピュータの情報を盗み見したり破壊したりする行為を**クラッキング**という。多くはネットワークを介して行われる。
- **BEC(Business Email Compromise) ビジネスメール例文**
  経営層や取引先になりすましてメールを送り、企業の担当者をだまして不正な口座へ送金させる詐欺の手口。

4.0.4 物理的脅威

大雨や地震、落雷などの災害やコンピュータの故障、空き巣によるコンピュータの盗難や破損もこれにあたる。

4.0.5 脆弱性(ぜいじゃくせい)

ソフトウェアやシステムなどのセキュリティ上の弱点や欠点のこと。脆弱性の要因となるものは

- **セキュリティホール**
  プログラムの不具合や設計ミスなどによって生じる欠陥のこと。ソフトウェアのメーカーなどが無償で配布する修正用のプログラムである**セキュリティパッチ**を適用することで、セキュリティホールの脆弱性を狙った攻撃を防ぐことができる。
- **シャドー IT**
  従業員が、企業の IT 部門などの許可を得ていないデバイスを業務で利用すること。デバイスに適切なセキュリティ設定がされていなかったり、盗難や紛失によって外部に情報が漏洩する可能性がある。

4.0.6 不正のメカニズム

情報資産に脅威となるのは、外部からの働きのみとは限らない。組織内で不正行為が行われる場合もある。内部不正は、**機会**、**動機**、**正当化**の 3 要素がそろったときに実行されると考えられている。これを、**不正のトライアングル**という。

4.0.7 脅威となる攻撃手段

4.0.8 暗号化

Chapter 5

Linuxサーバー

apache2 をインストール

apache2 をインストール

```
sudo apt install apache2
```

Ubuntu の標準ファイアウォール ufw(Uncomplicated Firewall)

ファイアウォールの有効化

```
sudo ufw enable
```

ファイアウォールの確認

```
sudo ufw status
```

sudo ufw status

```
有効なら Status: active
無効なら Status: inactive
```

ファイアウォールの無効化

```
sudo ufw disable
```

HTTP 通信用の TCP80 番ポート開放

```
sudo ufw allow http
```

サーバー起動

```
sudo systemctl start apache2
```

サーバー停止

```
sudo systemctl stop apache2
```

Chapter 6

トラブルシューティング

6.0.1　ネットワークの状態を確認するコマンド

- ping
  ホストとの通信ができるかどうか確認する。つまり、相手が生きてるかを確認する。
  https://は入れてはいけない。https://chatgpt.com ではなく ping chatgpt.com
- traceroute
  目的のホストに到達するまでに通るルータの経路を確認
- ss
  ソケットの情報を表示する。
- tcpdump
  CLI でリアルタイムにパケットをキャプチャする
- dig
  DNS の確認

Chapter 7

7.1 curl（カール）

curl は TTP や HTTPS などのプロトコルを使って、ウェブサーバにリクエストを送り、そのページの HTML などのレスポンス内容を表示させるコマンド。ターゲット側では 80 番ポートの開放が必要
sudo python3 -m http.server 80
curl 192.168.3.14

7.2 オプション

- O
  URL のファイル名でそのまま保存
- o
  ファイル名を指定して保存する。curl -o 保存先ファイル名 URL