第4回 プログラミング入門

目次

- 情報セキュリティ
  - セキュリティの考え方
  - セキュリティ対策
  - サイバー攻撃の種類

イントロダクション

本日の目標

- ネットワークについての理解を深める。
  - インターネットとは
    - インターネットはどのような構造なのか
    - IPアドレスとルーティング
    - VPNでなにができるか
  - 情報セキュリティ
    - なぜ情報セキュリティが重要なのか
    - おもなセキュリティ対策の種類
    - おもなサイバー攻撃の種類

インターネット

インターネットとは

- 世界中のコンピュータなどの情報機器を接続する巨大なネットワークです。
- 一般に、インターネットサービスプロバイダ（インターネットに接続してくれるサービス事業者）と契約することによって、インターネットに接続できるようになります。

インターネットの全体像

- 別添の図をご確認ください。

ネットワーク機器

- ネットワークを構築するための情報機器として、以下のようなものがあります。
  - ルーター・L3スイッチ
  - スイッチ
  - ハブ

IPアドレスとは（1）

- 端末（PC・タブレット・スマホ）を識別するための情報です。
- ネットワーク内で重複がない必要があります。
    - 同じIPアドレスを持っている端末が存在していると、どちらに送っていいのかがわからなくなるため通信が不安定になったりできなくなったりします。

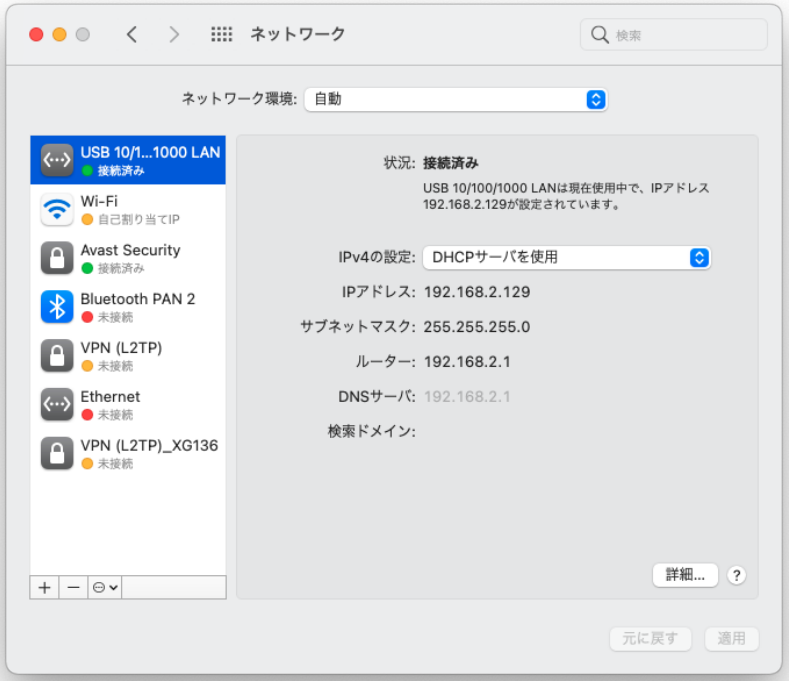
IPアドレスとは（2）

- IPアドレスは XXX.XXX.XXX.XXXのようにしてされる0~255の数字4角組合わせです。

```
10.1.10.123
172.16.1.3
192.168.2.10
```

DHCP

- コンピュータでの通信を行う際には、端末にアドレスを設定する必要があります。
    - このような設定は煩雑であるため設定ミスが起こりやすく、また台数が増えてくると手動での対応はできなくなります。



プライベートIPアドレスとグローバルIPアドレス

- IPアドレスは0~255の数字4つの組み合わせです。
  - $2^{32} = 4294967296$ →**世界中のコンピュータを網羅できない**
- そのため、インターネットに接続された機器のIPと組織内で使うIPアドレスを分けます。
  - グローバルIPアドレスは、**インターネット通信用IPアドレス**
  - プライベートIPアドレスは、**組織内での通信用IPアドレス**

NAT

- 組織内で使うIPアドレスとインターネットで使うIPアドレスは異なります。
    - ではどのように切り替えしているのか
- インターネットに接続する機器をルータといいますが、ルータには**NAT**と呼ばれる機能があり、組織内での**IPアドレスとインターネット用のIPアドレスを中継**してくれます。

ルーティング

- データを転送する際、どこのルータを中継して宛先にデータを送るかということを決めることを**ルーティング**と呼びます。
    - 例えば、西淀川から東京へ郵便を送るときに、西淀川郵便局→淀川郵便局→東京の郵便局と経由しているイメージです
- ネットワーク機器のルータは、パケットを転送するときにIPアドレスに基づいて経路を決める役割があります。

VPN

- リモートワークに欠かせない技術
    - インターネットや通信事業者の独自ネットワーク上に作る仮想的なネットワーク
- VPN接続は、**トンネリング**と**暗号化・認証**の組み合わせによって実現されています。
    - トンネリングとは、離れた機器間で仮想的な回線を作る技術
    - 暗号化と認証については後述

まとめ（1）

- インターネットは、世界中のコンピュータなどの情報機器を接続する巨大なネットワーク。
- IPアドレスは、端末を識別する情報でこの情報を使って、サーバーなど他のコンピュータと通信を行う。
    - IPアドレスにはグローバルIPとプライベートIPがあり、NATを利用してインターネットに接続しています。
- パケットを送るときにどこを経由して送るかということを決めることをルーティングと呼ぶ。
- リモートワークに欠かせないVPNは、トンネリングと暗号化と認証の組み合わせで実現

情報セキュリティ

セキュリティの考え方

- セキュリティ対策を考えるとき次の3つの要素のバランスを考えるのが大事です。
    - データの取り回しやすさと機密性は一般にトレードオフです。

1. 機密性(Confidentiality)
2. 完全性(Integrity)
3. 可用性(Availability)

セキュリティ対策 - 認証

- 一般に情報機器やインターネットサービスを利用するときは、IDとパスワードを入力します。
  - IDとパスワードは本人（または関係者）しか知らない
  - 権限のある人かどうかを確認する手順を **認証**と呼びます。
- IDとパスワードだけでは後述するサイバー攻撃に弱いので、最近はMFAとよばれる複数の信用情報を使って認証する方法も普及しています。

セキュリティ対策 - ファイアウォール

- ファイアウォールとは、外部からの攻撃を検知・防御する仕組み
- OSに備えられていたり（WindowsFirewarllなど）、端末とサーバーの中間に設置され、外部との通信を監視して攻撃とみなしたアクセスをブロックします。

セキュリティ対策 -ウィルス対策ソフト

- ユーザに害を与えるソフトウェアをマルウェアと呼びます。
- マルウェアからの完成を防ぐことを目的としたソフトウェアをウィルス対策ソフトといいます
    - アバスト・カスペルスキー・ノートン・ウィルスバスター・ESETなど

セキュリティ対策 - 暗号化

- 暗号化とは、**権限がある人以外読めないように、推定できない形に変換**することで
- データを保存したり誰かに伝送する際、意図せず第三者に盗み見られたり改竄されたりしないために行われます。
- 暗号化には、大きく分けて暗号化と復号化で同じ鍵を用いる **共通鍵暗号方式**と暗号化と復号化で異なる鍵を使用する **公開鍵暗号方式**があります

サイバー攻撃とは

サイバー攻撃の種類 - フィッシング詐欺

- フィッシング詐欺とはインターネット上で行われる詐欺行為の1つ。
- クレジットカードやネットバンクなどの**正規のサービスになりすまして、ユーザーからログイン情報などを盗み出し**ます。

サイバー攻撃の種類 - マルウェア

- **マルウェア(Malware)** とは、不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称です。
- なりすましメールなどを通じて、コンピュータに悪意のあるソフトウェアをインストール（感染）することで
  - 重要なフォルダを人質に身代金を要求する（ランサムウェア）
  - 感染したコンピュータの情報を外部に送信する（スパイウェア）
  - ユーザの意図に反した有害な作用をもち別のコンピュータに感染させる（ウィルス）

サイバー攻撃の種類 - 辞書攻撃

- パスワードを複数のWEBサービスで使い回す利用者が多いという傾向を利用
- Webサービスへの不正侵入やセキュリティ機関が公表しているパスワード情報をもとに**パスワードのリストを作成し、さまざまなWebサービスでログインの試行を繰り返す**
- 利用者の個人情報や金銭などを詐取しようとします。

サイバー攻撃の種類 - ブルートフォースアタック

- ブルートフォースアタック（総当たり攻撃）とは、暗号解読方法のひとつであり、可能な組み合わせを全て試す方法です。
    - パスワードに使用する文字種や桁数が多いほど解読に時間がかかる
- コンピュータはこの手の計算が非常に得意なので、時間的制約がない限りは確実にパスワードを割り出して侵入することができる方法です。

まとめ（2）ー 1

- セキュリティ対策を考えるときはCIAの3要素を考えることが大事
  - 機密性・完全性・可用性
- 主なセキュリティ対策には
  - サービスの利用には、可能な限り認証情報を設定する
    - 複数の信用情報の利用とパスワードを長くすることが好ましい
  - ウィルス対策ソフトのインストール、ファイアウォールの利用
  - 暗号化通信を行う

まとめ（2）ー２

- 主なサイバー攻撃
  - フィッシング詐欺
  - マルウェア
  - 辞書攻撃
  - ブルートフォースアタック

次回

- Pythonプログラミングに入ります。