

# セキュリティ対策

---

はしもとじょーじ

# ネットワークを利用する人の義務

---

## セキュリティ対策をきちんとする

- セキュリティ更新プログラムの適用
- ウィルス対策ソフトの使用

個人所有のパソコンもネットワークにつながら  
ら、きちんと**義務**を果たすこと

# ウィルス， マルウェア

---

害を及ぼす悪質なプログラム

## 感染経路

- メール添付で送られたきたファイル
- Webで取ってきたファイル
- Webサイトにアクセスするだけで感染することも

## 感染方法による分類

- **ファイル感染型ウィルス(狭義のウィルス)**  
ほかのプログラム(ファイル)に自分自身を埋め込む
- **ワーム(ネットワークワーム)**  
ネットワーク経由でほかのコンピューターに自分自身をコピーする(自己増殖する)
- **トロイの木馬**  
有用なプログラムなどを装ってユーザーに実行させる。  
ファイル感染や自己増殖の機能は持たない

## 挙動による分類

### – ボット

感染パソコンをネット経由で操作できるようにする

### – 偽ソフト

偽のセキュリティソフトなどを購入させる

### – スパイウェア

個人情報などを盗む

### – ダウンローダー

別のウィルスをダウンロードして感染させる

### – ワンクリック詐欺ウィルス

架空の料金請求などを表示する

# 脆弱性

---

セキュリティ上の問題を引き起こすソフトウェアの欠陥(バグ)

人間の作る物に100%はない

セキュリティ更新プログラム(パッチ)を適用して脆弱性を解消する

- Microsoft Update (Microsoft 製品)
- ソフトウェア・アップデート (Mac OS)

# 対策

---

ウィルス対策ソフトを使用する

セキュリティ更新プログラム(パッチ)の適用

信用できないファイルを開かない

信頼できないサイトにはアクセスしない

バックアップをとる

対策をしていても被害に遭う可能性はある

- 「ゼロデイ攻撃」 未対応の脆弱性を突く攻撃