令和7年度キャンパス情報ネットワーク利用ガイダンス
～情報セキュリティ～

岐阜大学情報セキュリティ最高責任者　松原正也

■ 1. サイバー攻撃ってなに?

▶1.1 サイバー攻撃

•パソコン(PC)やスマートフォン(スマホ)などに対し，ネットワークを通じて，破壊，データの窃取(盗み取り)，改竄(悪意のある書き換え)などを行うこと
•標的(特定の企業や個人，不特定多数など)や目的(金銭目的，いたずら)はさまざま

▶1.2 サイバー攻撃の目的

- 攻撃するものにとって利益となるもの(お金，個人情報，etc...)
- 利益目的の攻撃=ビジネス
- 攻撃しにくくすることで，被害にあう確率を減らせる
- サイバー攻撃者が標的にするもの→パソコン(PC)，スマートフォン(スマホ)，タブレット端末，無線LANルータ，プリンタ・複合機... etc.

▶1.3 サイバー攻撃の例

- フィッシング詐欺・マルウエア
- ランサムウエア
- ボットネット, etc...

■ 2. セキュリティを守る四つのポイント

▶2.1 ソフトウエアを最新に・セキュリティソフトの導入

- PCのOS(Windows, macOS…)やファームウエア，スマートフォン等を更新して最新の状態に
  - 自動更新する設定にする
  - セキュリティ関係の情報(ニュース)が流れたら手動でも更新を
- インストールされているソフトウエアも更新する
- 不要なソフトは入れない(アンインストール)ようにする
- PCやスマホにはウイルス対策ソフトを導入する
  - ウイルス対策ソフトだけでは万全とはいえないが…
  - ウイルス対策ソフトでは対処できないマルウエアがある
  - セキュリティホールが発見され，対策前に攻撃される「ゼロデイ攻撃」
  - とにかく導入しておくのが安全
- PCやスマホのソフト・アプリは安全なところから入手
  - 不審なところからダウンロードしたソフト・アプリは危ない
  - 不審メール・不審メッセージに添付されたソフト・アプリは間違いなく危険
  - ソフト・アプリの権限(ID，連絡先，位置情報(GPS)，SMS，電話，メディア，カメラ，マイク…)にも注意

▶2.2 安全なパスワードと認証を使う

- 短い文字列，数字だけの組み合わせだとすぐに見つけられてしまう
- パスワードは少なくとも10文字以上
- 英大文字小文字＋数字＋記号をすべて使う
- 辞書に載っている見出し語・一般によく知られている固有名詞は辞書攻撃で見つけられてしまう
- 長くてランダムな文字列が望ましい
- 複数のサービスでパスワードの使い回しをしない
- パスワードはメモしない・パソコンの中に保存しない
- 生体認証(指紋・顔認証)はあくまで補助的な手段

▶2.3 攻撃させないために，手間がかかるようにする

- 「攻撃にかかる手間」≒「安全」
- 個人情報はネットに上げない
- リアルで知り合いでない人と安易に友だちにならない

▶2.4 心の隙を作らないようにする

- ソーシャルエンジニアリング
  - 人間の心理的な隙やミスにつけこんだ攻撃手法
  - 攻撃者にコンピュータやネットワークの知識がなくても情報を盗み取ることができてしまう
  - トラッシング/スキャベンジング: ゴミ箱に捨てられた廃棄物をあさられて情報を盗む
    - 機密文書(紙)やディスクはシュレッダで細断
    - USBメモリやハードディスクは物理的に破壊
  - ネームドロップ・ハリーアップ: 立場がある人物を装い，冷静な判断を失わせて強引に情報を聞き出す
    - 落ち着いて行動・本人確認・だれかに相談
  - ショルダーハッキング: 公共の場などで背後からパスコードやパターンロックを盗み見る
    - 背後に立つ人に注意/スマホを席・テーブルに置きっぱなしにしない

■ 3. 安全なインターネット利用のために

- 無線LANの利用
  - 暗号化(WPA2-PSK以上)・安全なパスワード・不審なアクセスポイントにアクセスしない
- ファイル共有ソフトは学内では一切利用禁止
- データのバックアップはこまめにしておく

■ 4. まとめ

- 大学内の利用ルールを確認しよう
- 日頃からセキュリティに関心をもとう
- 不安に思ったら相談できる人や窓口に相談しよう

■ 参考資料

「インターネットの安全・安心ハンドブック」
https://www.nisc.go.jp/security-site/handbook/index.html
令和7年3月11日　Ver 5.10発行
内閣サイバーセキュリティセンター(NISC)

■ 情報セキュリティに関する相談窓口

岐阜大学情報館
imc-help@t.gifu-u.ac.jp