

パソコンとスマートフォンのセキュリティ対策

ー 共通点と相違点のまとめ ー

1. パソコンとスマホに共通するセキュリティ対策

(1) 怪しいメール・リンクを開かない

- ・ フィッシング詐欺はどちらも同じ手口で発生する。
- ・ 「アカウント停止」「未払い」「還付金」などの文言に注意。

(2) OS・アプリを常に最新にする

- ・ 更新を怠ると脆弱性が残り、攻撃されやすくなる。
- ・ 自動更新をオンにすることが基本。

(3) パスワードの使い回しをしない

- ・ どちらもアカウント乗っ取りの被害が多い。
- ・ 2段階認証を設定すると安全性が大幅に向上。

(4) 公共Wi-Fiの利用に注意

- ・ 暗号化されていないWi-Fiは盗み見のリスクがある。
 - ・ 金融・買い物・個人情報入力は避ける。
-

2. スマートフォン特有のセキュリティリスク（パソコンとの違い）

(1) SMS（ショートメッセージ）詐欺が多い

- ・「宅配不在」「料金未払い」「アカウント停止」などの偽SMSが多発。
- ・ URLをタップさせる手口が主流。

(2) アプリ経由の情報抜き取り

- ・ 偽アプリや、過剰な権限を要求するアプリに注意。
- ・ 連絡先・写真・位置情報が勝手に送信されるケースもある。

(3) 画面が小さく、偽サイトを見抜きにくい

- ・ URLの違いが見えにくく、ロゴやデザインが本物そっくりでも気づきにくい。

(4) 生体認証（指紋・顔認証）が標準装備

- ・ パソコンよりも強力なロックが簡単に使える。
- ・ PINより安全で、設定を推奨。

(5) 紛失・盗難リスクが高い

- ・ 持ち歩くため、物理的な紛失が最大のリスク。
- ・ 「端末を探す」機能の設定が必須。
 - iPhone：iCloud の「探す」
 - Android：「デバイスを探す」

3. パソコン特有のセキュリティリスク（スマホとの違い）

(1) 偽警告（サポート詐欺）が圧倒的に多い

- ・ 「ウイルスに感染しています！」
- ・ 「今すぐ電話してください！」
- ・ スマホよりパソコンでの発生率が高い。

(2) USBメモリ経由のウイルス感染

- ・ スマホではほぼ起きない。
- ・ パソコン教室では特に注意が必要。

(3) ソフトの自由インストールによるリスク

- ・ パソコンは自由度が高い分、悪意あるソフトも入りやすい。
 - ・ スマホはアプリストア経由が基本で比較的安全。
-

4. まとめ（講習用の1ページ要約）

● パソコンとスマホに共通すること

- ・ 怪しいリンクを開かない
- ・ 更新をする
- ・ パスワード使い回し禁止
- ・ 公共Wi-Fiに注意

● スマホだけの注意点

- ・ SMS詐欺
- ・ 偽アプリ
- ・ URLが見えにくい
- ・ 紛失リスク

● パソコンだけの注意点

- ・ 偽警告（サポート詐欺）
 - ・ USB感染
 - ・ ソフトの自由インストール
-