

高齢者向けパソコンセキュリティの基本項目

パスワードの重要性と管理方法

簡単すぎるパスワードは避ける（例：誕生日や「1234」など）

紙に書いて保管する方法も一つの選択肢（安全な場所に）

同じパスワードを複数のサービスで使わない

怪しいメールやメッセージに注意

「おめでとうございます」「至急対応してください」などの文言に注意

添付ファイルやリンクはむやみに開かない

知らない差出人からのメールは無視するか削除する

ソフトウェアの更新（アップデート）の大切さ

Windows やウイルス対策ソフトの更新はセキュリティを保つために必要

「更新してください」という通知は基本的に信頼できる

公共の Wi-Fi を使うときの注意点

銀行や買い物など個人情報を扱う操作は避ける

自宅の Wi-Fi のパスワードは他人に教えない

詐欺サイトや偽の広告に注意

「ウイルスに感染しました」「今すぐ修復」などの警告は偽情報の可能性あり

信頼できるサイト（政府・銀行・有名企業）以外では個人情報を入力しない

ウイルス対策ソフトの導入と確認

パソコンにウイルス対策ソフトが入っているか確認

無料のものでも最低限の保護は可能（例：**Windows Defender**）

家族や信頼できる人に相談する習慣

不安なときは一人で判断せず、家族や講習会の仲間に相談する

「これは怪しいかも」と思ったらすぐに聞く

セキュリティの三原則

その1 ソフトウェアを最新に保とう

その2 強固なパスワードの設定と多要素認証を活用しよう

その3 不用意に開かない・インストールしない

△ セキュリティの基本を怠った場合の具体的なトラブル例

弱いパスワードを使っていた場合

他人にアカウントを乗っ取られ、メールや SNS で勝手にメッセージを送られる

ネットショッピングの履歴やクレジットカード情報が盗まれる

怪しいメールを開いてしまった場合

ウイルスがパソコンに入り、動作が遅くなったり勝手に情報が送信される

偽の請求書や振込依頼に騙されて、実際にお金を振り込んでしまう

ソフトの更新を怠った場合

古い状態のままだと、悪意ある人に侵入されやすくなる

知らないうちにパソコンが「迷惑メールの発信元」にされることも

公共 Wi-Fi で個人情報を入力した場合

通信が盗み見られ、ID やパスワードが第三者に知られる

銀行口座に不正アクセスされる危険性も

偽サイトで個人情報を入力してしまった場合

本物そっくりのサイトで、名前・住所・カード番号などを盗まれる

後日、身に覚えのない請求や契約が発生する

ウイルス対策ソフトが入っていない場合

知らないうちにパソコンが壊れたり、情報が外部に漏れる

写真や文書など大切なデータが消えてしまうことも

日本人高齢者のセキュリティ被害データと実例（2024～2025 年）

1. フィッシング詐欺

手口：銀行や自治体を装った偽メールで個人情報を入力させる

被害額：クレジットカード不正利用被害は年間約 555 億円（警察庁 令和 6 年度統計）¹

傾向：高齢者は本物と偽物のメールを見分けるのが難しく、誤って情報を入力してしまうケースが多い

2. サポート詐欺

手口：「ウイルスに感染しています」と偽の警告 → 電話をかけさせる → 架空請求やカード情報の搾取

実例：70 代女性が約 15 万円を支払った後、さらにカード情報を盗まれた¹

3. なりすまし詐欺（医療・行政）

手口：病院職員や役所を装い、保険料や還付金の名目で金銭を要求

実例：高齢者が「保険料の返金手続き」として約 10 万円を振り込んだケース¹

4. ロマンズ詐欺

手口：SNS で恋愛感情を利用 → 「渡航費」「治療費」などの名目で送金を要求

実例：80 代男性が約 300 万円を送金¹

5. 投資詐欺（暗号資産など）

手口：SNS やメールで偽の投資話 → 少額で利益を見せて信用させ → 大金を持ち逃げ

被害額（日本含む国際統計）：1 件あたり平均約 130 万円、60 歳以上が最多¹

高齢者が狙われる理由（日本国内の傾向）

日本の金融資産の約 7 割を 55 歳以上が保有¹

地方では「タンス預金」文化が残っており、現金を狙った詐欺も多発

インターネットやスマホの操作に不慣れな人が多く、詐欺の見分けが難しい