

デジタル空間の 「戸締まり」ガイド

スマホ・パソコンの安全を守る、
今日からできる防犯対策

松葉町新技術勉強会
中村年雄





昔のイメージ：システムを破壊する
「ウイルスはパソコンに無理やり入り込む高度な技術」というイメージがありました。



今の現実：人をだまして鍵を開けさせる
現代のサイバー犯罪の大部分は、難解なハッキングではありません。
「詐欺は『人をだます技術』です」

重要な事実：泥棒はもう窓を割りません。偽の「不在通知」や「警告」を使って、あなた自身に玄関の鍵を開けさせるのです。

なぜ、シニア世代が狙われやすいのか？

インターネットという「新しい町」には、交番がありません。
詐欺集団は、以下のような理由からシニア層を意図的に狙っています。



1. 豊かな資産

長年かけて築いた大切な資産や貯蓄があるため、詐欺グループにとって最も「見返りが大きい」標的とされています。



2. 誠実さと信頼

「公的機関」や「有名企業」を名乗る連絡に対して、真面目に対応しようとする誠実な性質が逆手に取られています。



3. デジタルへの不慣れ

スマホやパソコンの急速な進化に対し、「よくわからない」「怖い」という不安を抱えている心の際が狙われます。

被害に遭うのは「あなたが悪いから」ではありません。
手口を知ること、この町は安全に歩けます。

シニアが遭いやすい詐欺トップ5

これらが、デジタル空間の玄関を狙う「5つの手口」です。



① フィッシング詐欺 (偽メール・偽SMS)

銀行・宅配業者・マイナポータルを装い、情報を盗む。



② 偽の警告画面 (サポート詐欺)

「ウイルス感染!」と嘘をつき、電話をかけさせる。



③ 偽ショッピングサイト

「激安・在庫処分」を装い、お金だけを奪う。



④ 投資詐欺 (SNS・LINE)

「必ず儲かる」「有名人が推奨」とLINEで誘導する。



⑤ アカウント乗っ取り

パスワードの使い回しを狙い、本人になります。

→ 次ページから、特に危険な手口の「実際の画面」を見てみましょう。

手口①：フィッシング詐欺の「罠の仕組み」

被害に遭うまでの流れ



SMSが届く（例：「宅配便の不在通知」）



← ここが運命の分かれ道！



慌ててURLを押す



本物そっくりの偽サイトが開く



個人情報や暗証番号を入力してしまう

見破るためのポイント（Amazonや銀行の例）

【偽物】（危険）

- 🔒 URLが不自然（例：sq23.akanamujer.com）。
- !! 日本語に違和感がある。
- ! 「今すぐ確認」など不安を煽る。
- ! 電話番号が050から始まる。

【本物】（安全）

- 🛡️ 公式アプリに直接お知らせが届く。
- ✅ URLが正しい公式ドメイン。

手口②：偽の警告画面（サポート詐欺）

警告文：

「トロイの木馬に
感染しました！」
「PCが破損しています！」

音・音声：ピー！という
大きな警告音が鳴り続ける。



電話番号：「今すぐ
サポートセンター
(050-XXXX...) に
電話してください」



真実と対策：これはすべて「嘘の画面」です。ウイルスには感染していません。絶対に電話を
かけないでください。遠隔操作ソフトを入れられ、お金を請求されます。

解決策：慌てずに、画面の右上にある「×（バツ）」ボタンを押して閉じるだけで安全です。

スマホ特有の危険地帯（マップ）

LINEアプリへ：
アカウント乗っ取り



知人から「WebMoney（プリペイドカード）を買ってきて」と頼まれたら、乗っ取りの証拠。

Wi-Fi設定へ：
公衆Wi-Fiの罠



駅やカフェの暗号化されていない無料Wi-Fiでは、パスワードの入力や買い物はしない。

SMS（ショートメール）アプリへ：
ほぼ100%詐欺の入り口

「料金未払い」「ETCの更新」などの連絡がSMSで来たら、リンクは絶対に押さない。

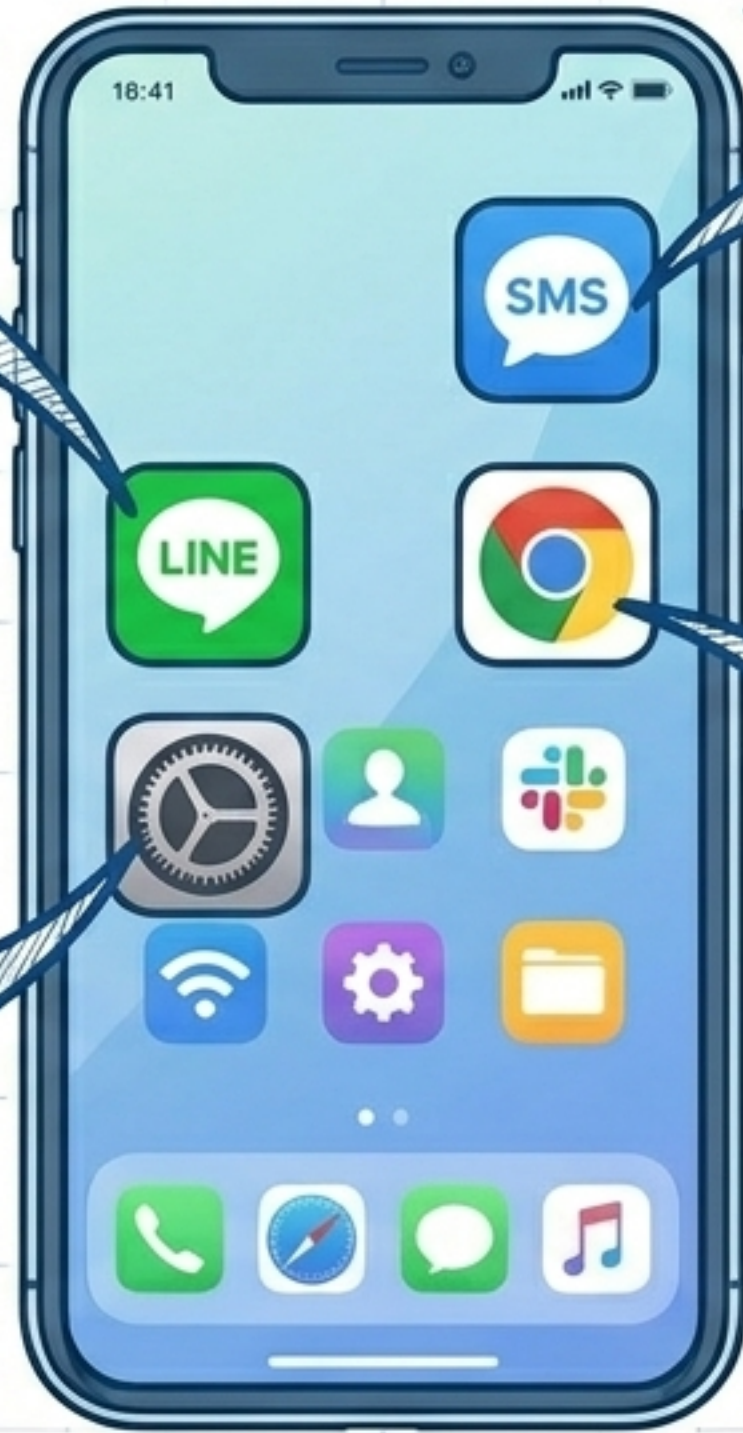


ブラウザ（インターネット）アプリへ：

！ 偽の警告画面



ネットサーフィン中に突然「スマホが破損！」と出ても、触らずにタブを閉じる。



パソコンの「戸締まり」と侵入ルート

郵便ポスト（メール）：
偽の請求書や領収書の添付ファイル

壊れた窓の鍵（古いOS・ソフト）：
古いブラウザやOfficeの「穴（脆弱性）」



勝手口（USBメモリ）：
他人のUSBを挿すことでの
持ち込み感染

Windows 10の罠（2025年10月サポート終了）

サポート終了とは、家の警備員（Microsoft）がいなくなり、「鍵の壊れた家」に住み続けるのと同じです。新しいウイルスが出ても修理されず、個人情報やネットバンキングが乗っ取られる危険性が極めて高くなります。早めの対策（買い替え等）が必要です。

詐欺に遭わないための「3つの鉄則」

技術的な知識がなくても、この3つの習慣（戸締まりのルール）を守るだけで、被害の大部分を防ぐことができます。



鉄則1：メール・SMSのリンクは押さない

不安を煽るメッセージが届いても、そこにあるURL（リンク）は絶対に押さない。確認する時は、必ず「公式アプリ」や、自分で登録した「ブックマーク（お気に入り）」からアクセスする。



鉄則2：電話番号を自分で調べてかけ直す

画面に突然表示された「サポート窓口」の番号には絶対にかけない。本物か確かめたい時は、クレジットカードの裏面や、公式サイトを自分で検索して、正しい番号に電話する。



鉄則3：パスワードを使い回さない

全ての玄関（サービス）を同じ鍵（パスワード）で開けられるようにするのは大変危険。1つのサービスから鍵が漏れたら、全ての財産が奪われます。

3つの鉄則が、すべての詐欺をブロックする

「5つの手口に、5つの対策は必要ありません。3つの鉄則で防げます。」

狙われる詐欺の手口	鉄則1: リンクを押さない	鉄則2: 自分で調べる	鉄則3: 使い回さない
① フィッシング詐欺	✓ 偽サイトに行かない		
② 偽の警告(サポート詐欺)		✓ 偽番号に電話しない	
③ 偽ショッピングサイト	✓ 偽サイトを踏まない		
④ 投資詐欺(SNS誘導)	✓ 怪しいURLを開かない		
⑤ アカウント乗っ取り			✓ 他で漏れても安全

複雑なセキュリティソフトよりも、皆さんの「日常の行動(習慣)」が最強の防御壁(シールド)になります。

最後の弱点:「パスワード」という鍵の限界



パスワードの弱点

- 🔑 ・盗まれる: フィッシング詐欺で入力させられる。
- ❓ ・推測される: 誕生日や短い単語はすぐに見破られる。
- 💡 ・忘れる: 複雑にすると自分が覚えられない。

どんなに「使い回しをしない」よう気をつけても、企業側（サービス提供者）からデータが流出してしまえば、パスワードは悪意のある集団（攻撃ロボット）の手に渡ってしまいます。

これからの時代、「パスワード自体を使わない」という究極の防犯対策が始まっています。

次世代の究極の鍵：「パスキー」とは？

	 これまでのパスワード	 パスキー (Passkey)
鍵の保管場所	ネット上のサービス側 (流出の危険あり)	自分のスマホ・PCの中だけ (流出しない)
認証の方法	文字を記憶して、 手で入力する	指紋や顔をかざすだけ (覚える必要なし)
偽サイト対策	騙されて入力すると 盗まれる	偽サイトでは反応しない (絶対盗まれない)



「パスキーの強み」

秘密の鍵はあなたの端末から一步も外に出ません。指紋や顔認証（生体認証）を使うため、万が一データ流出事件が起ても、あなたの情報は完全に守られます。

まとめ：デジタル空間を安全に楽しむために



テクノロジーは怖くありません。
正しい「戸締まり」を知るだけです。



1. 立ち止まる勇気

急かすようなSMSや警告画面が出たら、まずは「深呼吸」。絶対にその場でリンクを押したり、電話をかけたりしない。



2. 公式からの確認

不安なこと（宅配や銀行の連絡）があれば、必ず「公式アプリ」か「自分で調べた正しい連絡先」から確認する。



3. 最新の鍵を取り入れる

古いパソコン（Windows 10）は早めに新しくし、パスワードの代わりに「パスキー」などの安全な仕組みを積極的に活用する。

デジタル空間の「玄関の鍵」を握っているのは、あなた自身です。
今日学んだ3つの鉄則で、安全で便利なインターネット生活を楽しみましょう。