高校生のスマホセキュリティ

この教材の全てのイラストは生成AIを使用して作成しました

学校法人 YIC学院
YIC 情報ビジネス専門学校

実はとても危ない（かもしれない）インターネットの世界

自分を守るために気を付ける２６のこと

カテゴリー1：OS・アプリの基本管理
デバイスの「土台」を清潔に保つための対策です。

1．OSの即時アップデート:
脆弱性を塞ぐ最優先事項

- OSの即時アップデート

2026年初頭に発覚した「Dolbyコンポーネントの脆弱性」のように、操作不要（ゼロクリック攻撃）で侵入されるリスクを防ぐため、通知が来たら即更新します。

✓「iOS、androidの更新」を検索してみよう

2．アプリの自動更新:
常に最新のセキュリティ状態を維持。

- アプリの自動更新設定

アプリ側の脆弱性も攻撃の入り口になります。常に最新版が保たれるよう自動更新を有効にします。

✓「アプリの自動更新」を検索してみよう

３．公式ストア利用: 審査済みの安全なアプリのみ使用。

- 公式ストアのみを利用

App StoreやGoogle Play以外の「野良アプリ」は、ウイルス混入率が極めて高いため避けます。

４．不要アプリ削除:
攻撃の入り口を物理的に減らす。

- 不要なアプリの削除

使っていないアプリは「攻撃の隙（アタックサーフェス）」を増やすだけです。定期的に整理しましょう。

５．権限の最小化:
アプリに過剰な情報を与えない。

- 権限（パーミッション）の最小化

「計算機アプリが位置情報を求める」といった、機能に無関係な権限要求は拒否します。

✓「アプリの権限設定」を検索してみよう

6．サポート終了アプリの移行:
古いアプリを捨て、新しい代替品へ。

- 提供終了アプリのアンインストール 開発者がサポートを止めた古いアプリはセキュリティの穴になりやすいため、代替アプリへ移行します。

カテゴリー2：認証・ログインの強化
「本人確認」を二重三重にして、他人の侵入を阻みます。。

7．パスキー（PASSKEYS）の導入:
盗まれるパスワードをなくす最新技術。

- パスキー（Passkeys）の導入

パスワードを「覚える」から「デバイスで承認する」形式へ移行。フィッシング詐欺に物理的に耐性があります。

✓「パスキー」を検索してみよう

8．生体認証の活用:
覗き見のリスクを排除。

- 生体認証の活用

顔認証や指紋認証をメインにし、外出先でのパスコード入力を覗き見られるリスク（ショルダーハッキング：銀行のATMで高齢者の方が暗証番号を入力する時、悪い奴が横見や覗き見することをイメージしてみて）を減らします。

９．多要素認証（MFA）必須化:
IDが漏れてもログインさせない。

・多要素認証（MFA）の必須化

　標準ではMFAが使えないサービスでは、必ずアプリやSMSによる二段階認証（パスワード入れてもSMSなどに送られてくる番号を入力しないと先に進めない）を設定します。

✓「MFA」を検索してみよう

１０．複雑なパスコード:
推測されやすいパターンを避ける。

- 推測されにくいパスコード

「1234」や誕生日、Z字型のパターンなどは一瞬で見破られます。複雑なコードを設定しましょう。

✓「良いパスコード」を検索してみよう

１１．パスワードマネージャー:
全サイトで異なる強固な鍵を作成。

- パスワードマネージャーの利用

　何百ものパスワードを安全に生成・管理し、使い回しによる「芋づる式被害」を防ぎます。一つのパスワードを複数のサイトで使うと全滅してしまいます。

✓「パスワードマネージャー」を検索してみよう

カテゴリー3：通信とネットワークの安全
目に見えない「通信の通り道」を守ります。

１２．公共WI-FI（フリーWI-FI）の回避:
偽のアクセスポイントに繋がない。

- 公共Wi-Fiの原則利用停止

暗号化されていない、または不審なWi-Fiには繋がないのが鉄則です。

✓「怪しいFree wi-fi」で検索してみよう

１３．　VPNの利用:
通信内容を暗号化のトンネルで包む。

- VPNの常時・スポット利用

　信頼できないネットワークを使う際は、VPNで通信内容を暗号化して盗聴を防ぎます。

✓「VPN」を検索してみよう

１４．BLUETOOTH/NFCのオフ:
不要な通信窓口を閉じる。

- Bluetooth/NFCのオフ

　使わない時はオフにし、近距離からの不正ペアリングやデータ抜き取りを防止します。

✓ Bluetooth/NFCの落とし穴」を検索してみよう

１５．テザリングパスワード:
自分の電波にタダ乗り・侵入させない。

- テザリングのパスワード強化

スマホをルーターとして使用する際、パスワードの設定によっては、他人に悪用される恐れがあります。

✓「テザリング」「テザリングのリスク」を検索してみよう

カテゴリー４：物理的・紛失リスク対策
スマホそのものの盗難や、物理的なハッキングに備えます

１６．「デバイスを探す」有効化:
地図上で場所を特定。

- 「デバイスを探す」機能の有効化

紛失時にGPSで場所を特定し、遠隔で音を鳴らすための基本設定です。

✓「デバイスを探すには」を検索してみよう。

１７．リモートワイプ:
諦める時は遠隔でデータを消し去る。

- リモートワイプの準備

　盗難時に、遠隔操作でスマホ内の個人情報を全消去できる状態にしておきます。

✓「リモートワイプ」を検索してみよう

１８．　SIMカードのPINロック:
SIMを抜かれて別の端末で使われないように

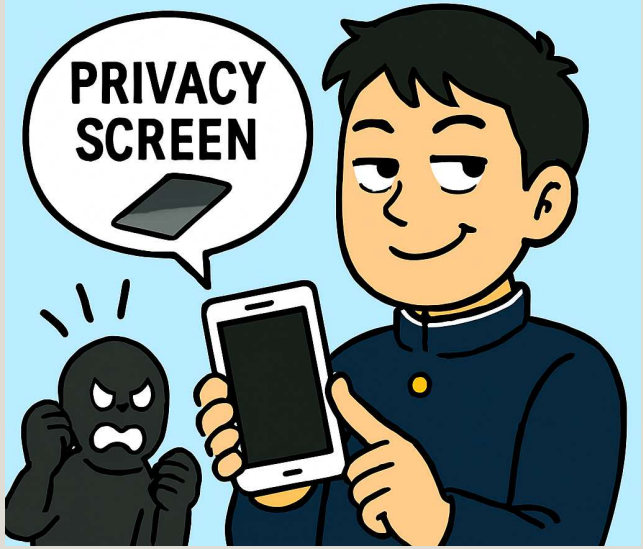
SIMカードへのPINロック

　スマホが盗まれた際、SIMカードを抜いて別の端末で使われ、SMS認証を突破されるのを防ぎます。

✓「SIMカードへのPINロック 」「SMS認証」を検索してみよう

１９．覗き見防止フィルム:
背後からの盗み見を物理的に遮断。

画面を見れない悪人



- 覗き見防止フィルムの貼付

　物理的に画面を見られないようにし、ログイン情報やメッセージ内容を保護します。

２０．公共充電ポートの回避:
USBからデータを盗む「ジュースジャッキング」を防ぐ。

- 公共充電ポートの使用回避

USBポートからウイルスを送り込む「ジュースジャッキング」対策。自分の充電器とコンセントを使いましょう。

✓「ジュースジャッキング」を検索してみよう

カテゴリー5：最新のＡＩ・詐欺トレンド対策
技術（ＡＩ）を悪用した心理的な罠に備えます。

２１．クィッシング（QR詐欺）：偽のQRコードから偽サイトへ。

- クィッシング（QRコード詐欺）への警戒

公共の場に貼られた偽のQRコードをスキャンし、偽サイトへ誘導される被害が増えています。

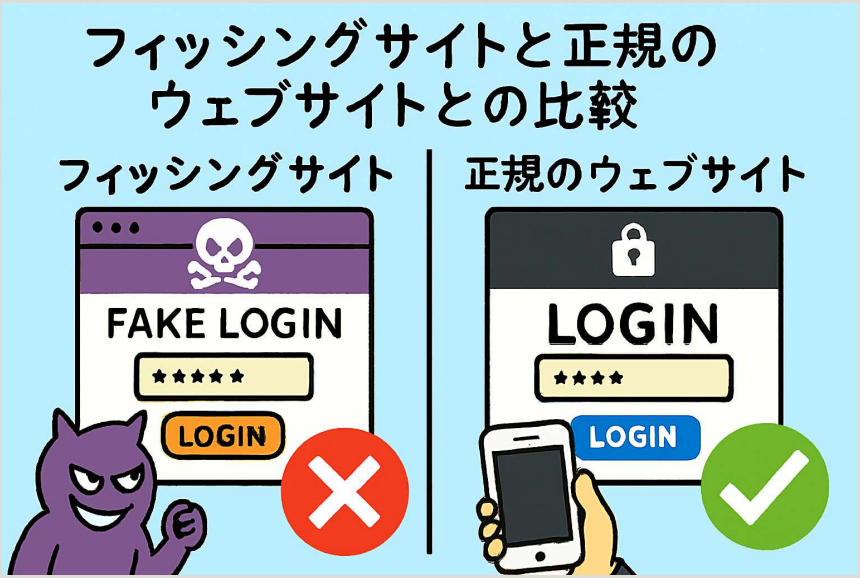
✓「クイッシング」を検索してみよう

２２．AIボイス・ディープフェイク:
家族を装う合成音声に騙されない。

- AIボイス・ディープフェイク対策

家族の声に似せたAI合成音声での金銭要求が増えています。「合言葉」を決めるなどの自衛が必要です。

２３．フィッシングの無視:
メールやSMSのURLは絶対に踏まない。



- フィッシングメールの無視

　銀行や運送会社を装うメールのリンクは踏まず、必ず「公式アプリ」から状況を確認します。

✓「フィッシング」「フイッシングメール」を検索してみよう

２４．SNSの公開範囲制限:
写真一枚から生活圏を特定させない。

- SNSの公開範囲設定

背景の写真から自宅や勤務先が特定されるリスクを避けるため、投稿の公開範囲を絞ります。

✓「SNSの公開範囲設定 」を検索してみよう

カテゴリー6：法規とデータ保護
ICチップやデータのバックアップについて学びます。

２５．ICチップ読み取り:
改正法に合わせた、より安全な本人確認。

- マイナンバーカード等のIC読み取り活用

2026年4月施行の改正法により、厳格な本人確認にはICチップ読み取りが主流となります。偽造書類に騙されない安全な認証を意識しましょう

✓「マイナンバーカード等のIC読み取り活用」を検索してみよう

２６．定期的なバックアップ:
最終的にデータを守る最後の砦

- 定期的なバックアップ

　ランサムウェア（身代金ウイルス）や故障でデータがロックされても、復旧できるようにしておきます。

✓「スマホのバックアップ」を検索してみよう

マルウェアについて

- スライド２６の「ランサムウェア」のように現在はコンピュータウィルスを含むいわゆる「悪さ」をする「マルウェア」が存在しています。機会があればそれらを調べてもいいでしょう。しかし専門家ではない私たちがその名前を知ったところで、できることはあまりありません。本教材では**私たちが、被害を受けない、被害を最小限に留めるためには、どういうことに留意し、準備し、どう行動すべきか**について学びました。できることから始めていきましょう。

さらに詳しく
情報セキュリティの教材のURL

- 情報セキュリティ教材・ツール

https://www.ipa.go.jp/security/sec-tools/general_security_materials.html

- 映像で知る情報セキュリティ

https://www.ipa.go.jp/security/videos/list.html

IPA（独立行政法人情報処理推進機構）のHPより

本教材の特徴ついて
その１

- この教材は「著作権」を考慮してすべてのイラストと文章の一部は生成AIで作成しています。皆さんも機会があったら「著作権」について調べてみるのもいいでしょう。著作権について知ることも、皆さんを守る「広い意味でのセキュリティ」といえるでしょう。
- お役立ちサイト
  https://www.cric.or.jp/education/eizoushiryou.html
  （公益社団法人著作権情報センター）

本教材の特徴ついて
その２

- この教材は皆さんに多くのキーワードについて、「検索」することを促すように作成しました。
- 教科書は過不足なく説明を記載しています。その説明が皆さんにとって合う、合わないが起こることもあるでしょう。
- 幸いなことに昔と違って、一つのことについて多くの解説サイトや動画があります。皆さんは検索することで自分に合った副教材を見つけることが可能になっており、素晴らしい環境にいるのです。
- ぜひ「検索力」を磨いてください

その指先は世界を変える！
ググってググッてっググりまくろう！

- この教材は、自主学習で使ってもOK。思いついたら検索しよう。

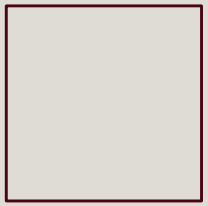
参考：この教材はブラウザで見れますが、スマホでちょっとおもしろい見方もできます。その１

- まず教材をダウンロード

ダウンロードＵＲＬ（仮）

https//yic.ac.jp/ib/xxxxx.pdf

ＱＲコード（仮）



- 次に下記にアクセス

https://online.visual-paradigm.com/ja/flipbook-maker/pdf-to-flipbook-converter/

参考：この教材はブラウザ見れますが、ちょっとおもしろい見方もできます。その２

- こんなサイトに行きます

- さっきダウンロードしたＰＤＦファイルを指定すると本のようにめくれます。ヨコがオススメ。

注意！：ただし、スマホでは大丈夫ですがパソコンではスライドが切れて見えることもあります