情報セキュリティ10大脅威　2026
個人編　ハンドブック

[一般利用者向け]

QRコード

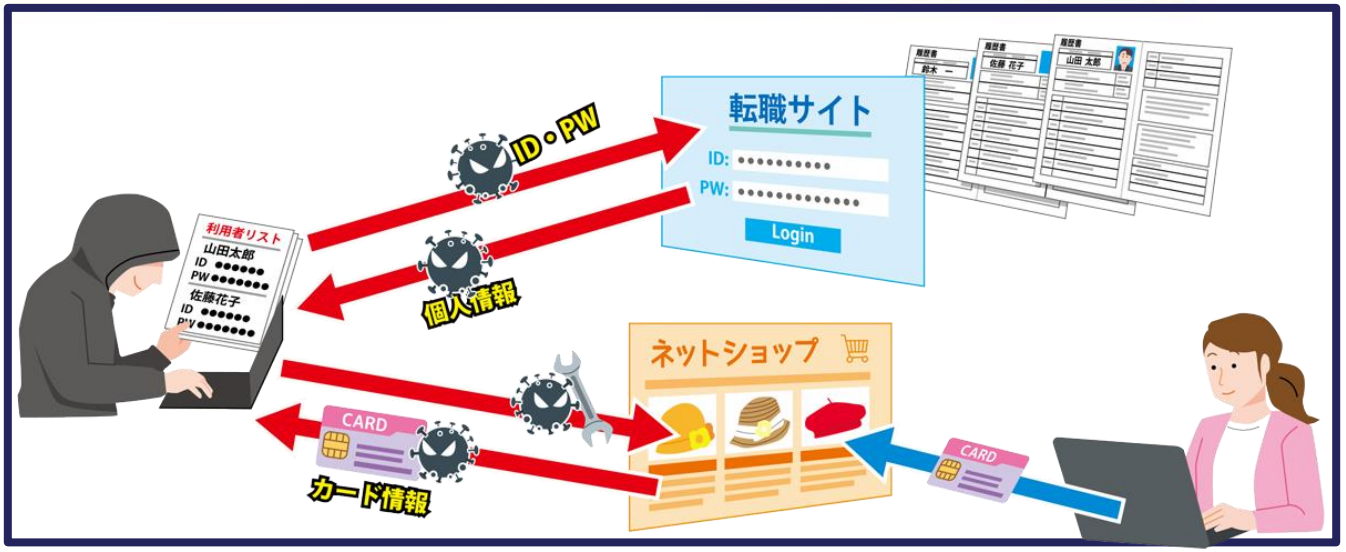
ウェブサイトのURL

https://www.ipa.go.jp/security/10threats/10threats2026.html

情報セキュリティ10大脅威 2026

「個人」向け脅威（五十音順）	初選出年	10大脅威での取り扱い
インターネット上のサービスからの個人情報の窃取	2016年	7年連続10回目
インターネット上のサービスへの不正ログイン	2016年	11年連続11回目
インターネットバンキングの不正利用	2016年	**4年ぶり8回目**
クレジットカード情報の不正利用	2016年	11年連続11回目
サポート詐欺（偽警告）による金銭被害	2020年	7年連続7回目
スマホ決済の不正利用	2020年	7年連続7回目
ネット上の誹謗・中傷・デマ	2016年	11年連続11回目
フィッシングによる個人情報等の詐取	2019年	8年連続8回目
不正アプリによるスマートフォン利用者への被害	2016年	11年連続11回目
メールやSNS等を使った脅迫・詐欺の手口による金銭要求	2019年	8年連続8回目

● インターネット上のサービスからの個人情報の窃取



● どんな手口・被害？
- ショッピングサイト、転職支援サイト等に登録しておいた個人情報が攻撃者に窃取、悪用される

● 被害に遭うとどうなるの？
- アカウントに登録されていた個人情報が窃取される
- 窃取された個人情報が複数の犯罪者間で共有・売買される
- 窃取された自分のメールアドレスにフィッシング等の詐欺メールが送付される。
- 窃取されたクレジットカード情報などが悪用され金銭被害が発生する。

インターネット上のサービスからの個人情報の窃取

● 対策

【予防】

- 利用していないサービスのアカウントを削除する、または退会する
- サービスへの登録時には必須項目以外の情報は登録しない

【個人情報悪用の抑止】

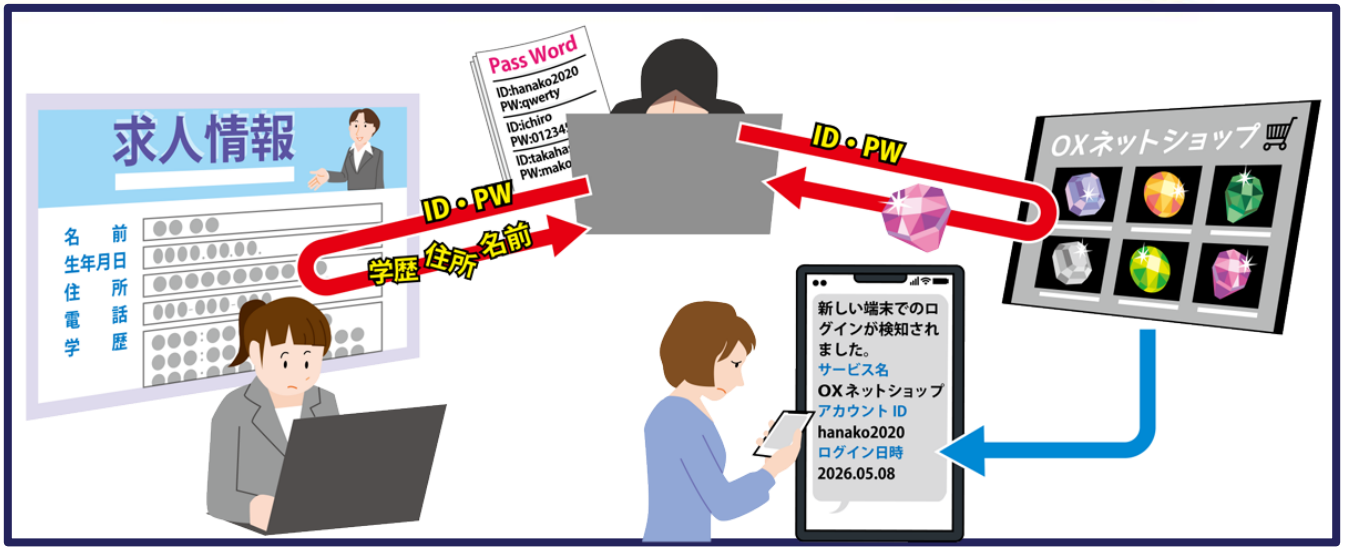
- 多要素認証を利用する
- ワンタイムパスワード、生体認証等の本人認証（3Dセキュア）の利用
- パスキー※1が利用可能な場合は、極力利用する
- 認証情報を適切に運用する（P.7＜基本のキ＞適切にパスワードを設定する）

【早期検知】被害に遭っていないかを確認することが大事

- ログインすると通知されるログインアラート機能の利用
- ログイン履歴の確認
- クレジットカード利用明細の定期的な確認（不正な利用履歴の早期発見）

※1 パスワードを使わずに、ウェブサイトにログインする手段（生体認証（指紋、顔認証））やスマートフォン等の端末に登録しておいたPINコード（パスコード）

● インターネット上のサービスへの不正ログイン



● どんな手口・被害？

- フィッシング・マルウェア等で窃取されたログイン情報を悪用し、ショッピングサイト、SNS、オンラインゲーム等のサービスに悪意ある第三者からログインされる

● 被害に遭うとどうなるの？

- パスワードを勝手に変更され、本人はログインできなくなる
- 不正な買い物をされ、クレジットカードの不正利用等の金銭被害に遭う
- パスワードを使い回していると他のサービスでもログインされ、クレジットカードの不正利用により、身に覚えのない高額請求通知が届く
- 本人になりすまし、第三者にSNS投稿、フィッシングメールが送信され、受信者に被害が拡大するおそれがある

インターネット上のサービスへの不正ログイン

● 対策

【予防】

- P.30「情報セキュリティ対策の基本」 ③、⑥ の実施
- よくアクセスするウェブサイトはブックマーク（お気に入り）に登録し、検索エンジン等のブックマーク以外からアクセスしない
- 安易に添付ファイルの開封、メールやSMSのURLリンクのクリック/タップをしない
- 認証情報を適切に運用する（ P.7＜基本のキ＞ 適切にパスワードを設定する）
- 利用していないサービスは退会する
- ワンタイムパスワード、生体認証等を含めた多要素認証を利用する
- クレジットカード情報は極力、登録しない
- セキュリティソフトでアクセスブロック機能を活用する
- P24「フィッシングによる個人情報等の詐取」の対策を実施

【早期検知】被害に遭っていないかを確認することが大事

- ログインすると通知されるログインアラート機能、利用状況の通知機能の利用
- 利用しているサービスのログイン履歴を確認
- クレジットカードやポイント等の利用履歴を定期的に確認

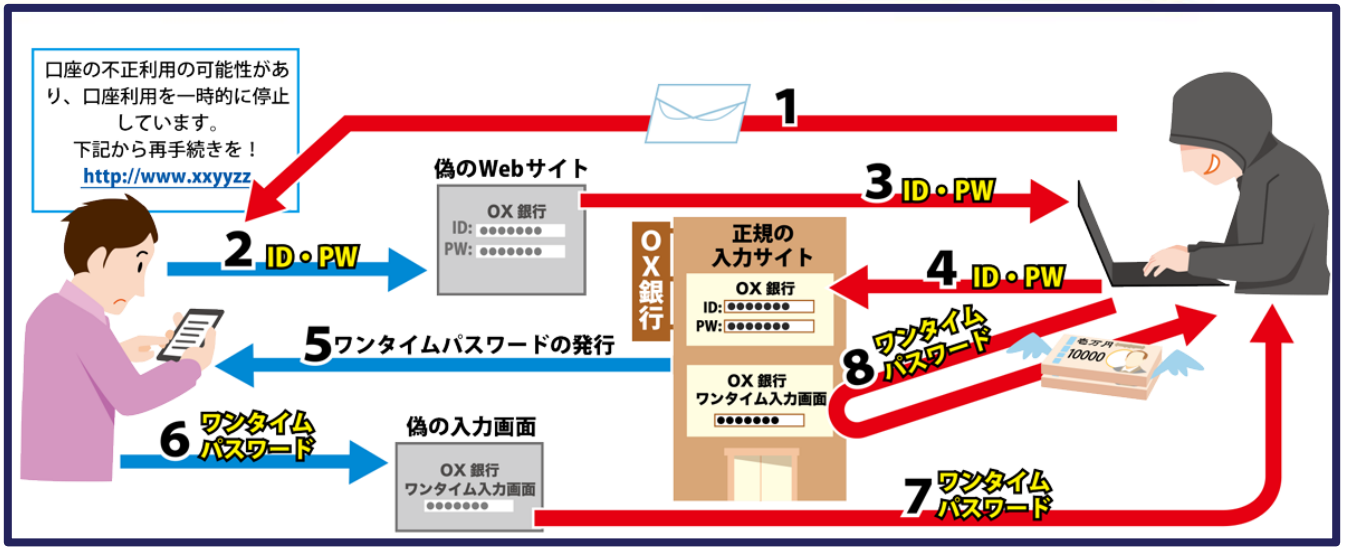
インターネット上のサービスへの不正ログイン

● 対策＜基本のキ＞：適切にパスワードを設定する

- 推測されにくいパスワードにする
  - ① ID とパスワードを同じ文字列にしない
  - ② 生年月日やSNSで使っているニックネーム、名前を使わない
  - ③ キーボードの連続した文字列等、規則的な配列にしない
    （例：123456、qwerty、111111）
  - ④ 辞書に載っている（単純な）単語一語だけにしない
    （例：password、baseball）

- パスワードは長く複雑にして、使い回さない
  複数のサービスでパスワードを使い回していると、それら全てのサービスに不正ログインされるおそれがある
- パスキーが利用可能な場合は、極力利用する
- パスワードマネージャーの利用を検討する

● インターネットバンキングの不正利用



● どんな手口・被害？
- 主にサービス提供元を偽ったメール等でフィッシング※2サイトに誘導され、ログイン情報が詐取される
- マルウェアに感染し、ログイン情報が窃取される

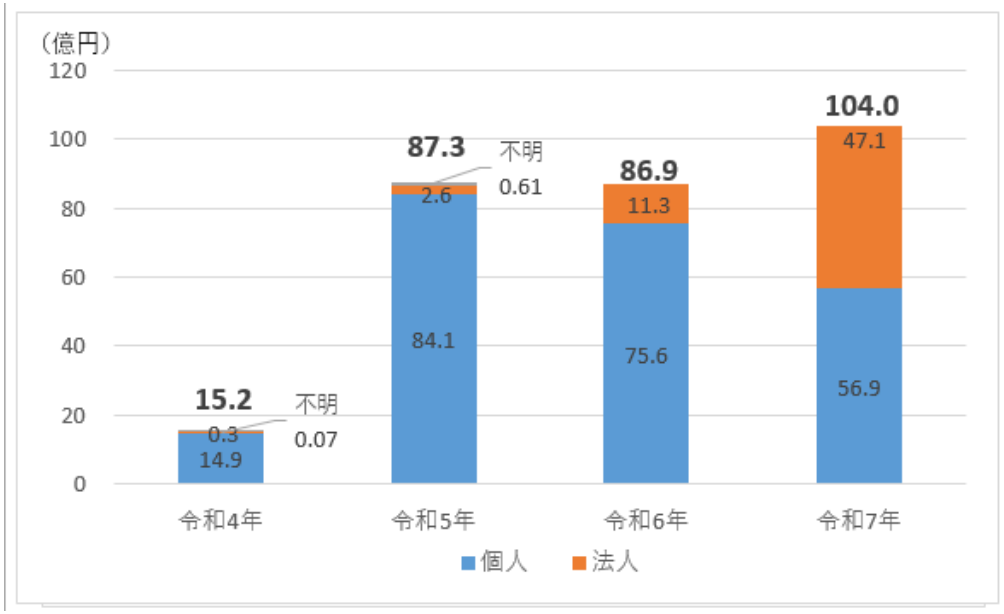
● 被害に遭うとどうなるの？
- インターネットバンクの口座に不正ログイン、不正送金され、金銭被害に遭う
- マネーロンダリングなどに口座を悪用され、違法行為に巻き込まれる

※2 実在する組織を騙って、メール等のリンクから偽サイトに誘導し、個人情報を入力させ、窃取する手口
出典：フィッシング対策協議会

インターネットバンキングの不正利用

● 事例

・不正送金の被害総額は、過去3年増加傾向



※出典　令和7年におけるサイバー空間をめぐる脅威の情勢等について　統計データ　図表21

・近年、リアルタイム型フィッシング※3により、二要素認証を突破する手口が横行

※3　サービス提供元を装った偽メール（フィッシング）に騙され、誘導されたフィッシングサイトでIDとパスワードを入力してしまうと即座（リアルタイム）に攻撃者もそのIDとパスワードを悪用し、ログインする。次に正規の利用者宛にワンタイムパスワードが送付され、正規の利用者が偽サイトに入力（または電話で伝達）してしまうと、二要素認証を有効にしていても攻撃者がログインできてしまう。

インターネットバンキングの不正利用

● 対策

【予防】

- P.30「情報セキュリティ対策の基本」 ②、③、⑥ の実施
- 多要素認証、本人認証サービス（3Dセキュア等）が使える銀行を極力利用し、設定を有効にする
- パスキーが利用可能な場合は、極力利用する
- 認証情報を適切に運用する（P.7＜基本のキ＞ 適切にパスワードを設定する）
- 無闇に信用しない
  - 相手の言い分（電子証明書の更新、ネット銀行の情報更新）
  - 相手が名乗る、組織名、肩書
- 安易に添付ファイルの開封、メールやSMSのURLリンクのクリック/タップをしない
- セキュリティソフトを導入し、アクセスブロックを有効化し危険なウェブサイトへのアクセスをブロックする
- P24「フィッシングによる個人情報等の詐取」の対策を実施

【早期検知】被害に遭っていないかを確認することが大事

- ログインすると通知されるログインアラート機能、利用状況の通知機能の利用
- 利用しているサービスのログイン履歴を確認
- クレジットカードやポイント等の利用履歴を定期的に確認

身近に相談できる人がいない場合は、公的機関の相談窓口等に相談するのも一考です。
P31「困ったときの相談先」

● クレジットカード情報の不正利用

- どんな手口・被害？
  - ウェブサイトの管理側が不正アクセスされてカード情報を窃取される
  - 正規のウェブサイトが改ざんされていて、入力された情報を窃取される
  - フィッシングサイトで、入力された情報を詐取される
  - 偽ショッピングサイトで、入力された情報を詐取される

- 被害に遭うとどうなるの？
  - 盗まれたクレジットカード情報が使われ、金銭被害が発生する
  - 盗まれたクレジットカード情報が複数の犯罪者間で共有・売買される

クレジットカード情報の不正利用

● 対策

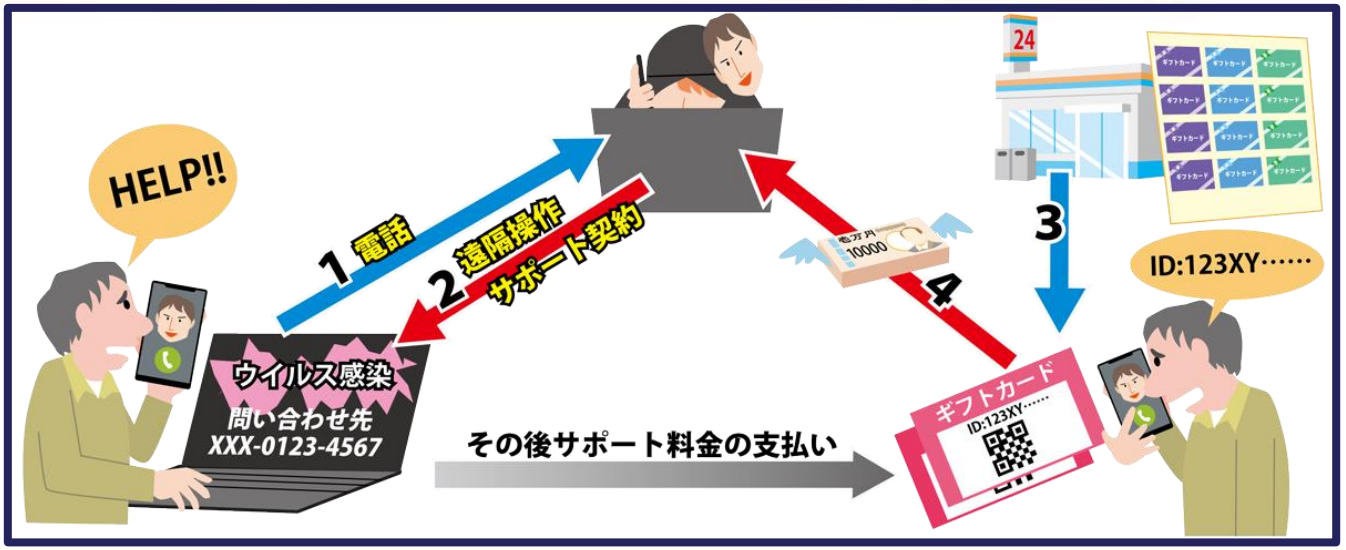
【予防】

- P.30「情報セキュリティ対策の基本」 ②、③、⑥ の実施
- クレジットカード会社が提供している本人認証（3Dセキュア）の利用
- クレジットカードの利用限度額を抑える
- クレジットカード情報は極力、登録しない
- 使っていないクレジットカードは契約解除し、ICチップを破断し物理的破棄を検討する
- フィッシングに注意する
  - カード情報は公式ウェブサイト、公式アプリから入力する
  - 普段表示されない画面やポップアップが表示された場合、クリックしたり、情報を入力しない
- P24「フィッシングによる個人情報等の詐取」の対策を実施

【早期検知】被害に遭っていないかを確認することが大事

- クレジットカードの利用履歴を定期的に確認
- サービス利用状況の通知機能を利用する

● サポート詐欺（偽警告）による金銭被害



● どんな手口・被害？

- ウェブサイトの閲覧中に、突然、実在する企業のロゴが配置されたセキュリティの警告画面が表示（偽の警告）され（画面を閉じることができない）、警告音が鳴る
- 慌ててしまい、画面に表示される電話番号に連絡してしまうことで詐欺被害の発端となる

● 被害に遭うとどうなるの？

- マルウェア駆除と称し遠隔操作ソフトをインストールされ、PCやスマートフォンを遠隔操作される
- サポート料金や修復費用をギフトカードなどのプリペイドカードで複数回請求されたり、インターネットバンキングの振込時に送金額を遠隔で増額され、想定外の金額が送金される

サポート詐欺（偽警告）による金銭被害

- 対策

【予防】

- 慌てない、一呼吸して冷静になる
- P.30「情報セキュリティ対策の基本」 ②、③、⑥ の実施
- セキュリティソフトを導入し、アクセスブロック機能を活用する
- パソコンで突然警告画面が出現したら、偽物の可能性を疑う
- 突然出現した警告画面に表示されたサポート窓口の番号に電話をかけない
- 過剰に表示される警告は詐欺の可能性を疑う
- 警告を無視して信頼する人に速やかに相談する
- サポート料金を支払わない

実際の画像を多用した、手口の解説ページを見ることで、対策への理解がより深まります。
パソコンに偽のウイルス感染警告を表示させるサポート詐欺に注意（IPA）
https://www.ipa.go.jp/security/anshin/attention/2024/mgdayori20241119.html

サポート詐欺（偽警告）による金銭被害

- 「偽警告」が表示されるのにはワケがある！？

偽警告が表示されるのには多くの場合きっかけがあります。

  - ブラウザに表示された広告をクリックしませんでしたか？
  - 検索結果に表示された上位の結果をクリックしませんでしたか？
  - 動画再生ボタンをクリックしませんでしたか？
  - ブラウザに「許可しますか」と表示され、許可をクリックしませんでしたか？

  このように直前の操作がきっかけとなり、偽警告は出現します。

- マルウェア感染の警告画面が出ても、電話を掛けない！
- 正規のセキュリティサービスの警告画面に電話番号は表示されません。
- 下記のページで偽警告画面の閉じ方を体験してみましょう！

偽セキュリティ警告（サポート詐欺）対策特集ページ（IPA）
https://www.ipa.go.jp/security/anshin/measures/fakealert.html

● スマホ決済の不正利用

● どんな手口・被害？
- 実在する企業・金融機関・行政機関等を装い、なりすましメールが送信され、メール本文のリンクからスマホ決済での送金に誘導する
- ネットで購入した商品が欠品で、決済アプリで返金すると連絡があり、操作すると返金ではなく送金される
- 悪意あるQRコードを読み取ると、意図しない先に送金してしまう(クイッシング)
- 自分のアプリから支払うためのQRコードを他人に盗まれると、自分の知らないところで勝手に決済されてしまう

● 被害に遭うとどうなるの？
- 窃取されたクレジットカード情報が別の決済サービスに登録され、スマホ決済を不正利用される
- 決済アプリで返金すると連絡があり、注文コードや確認コードと称する処理を行うと、入力した数字が金額として相手に送金されてしまう

P.22 「フィッシングによる個人情報等の詐取」も併せて確認！

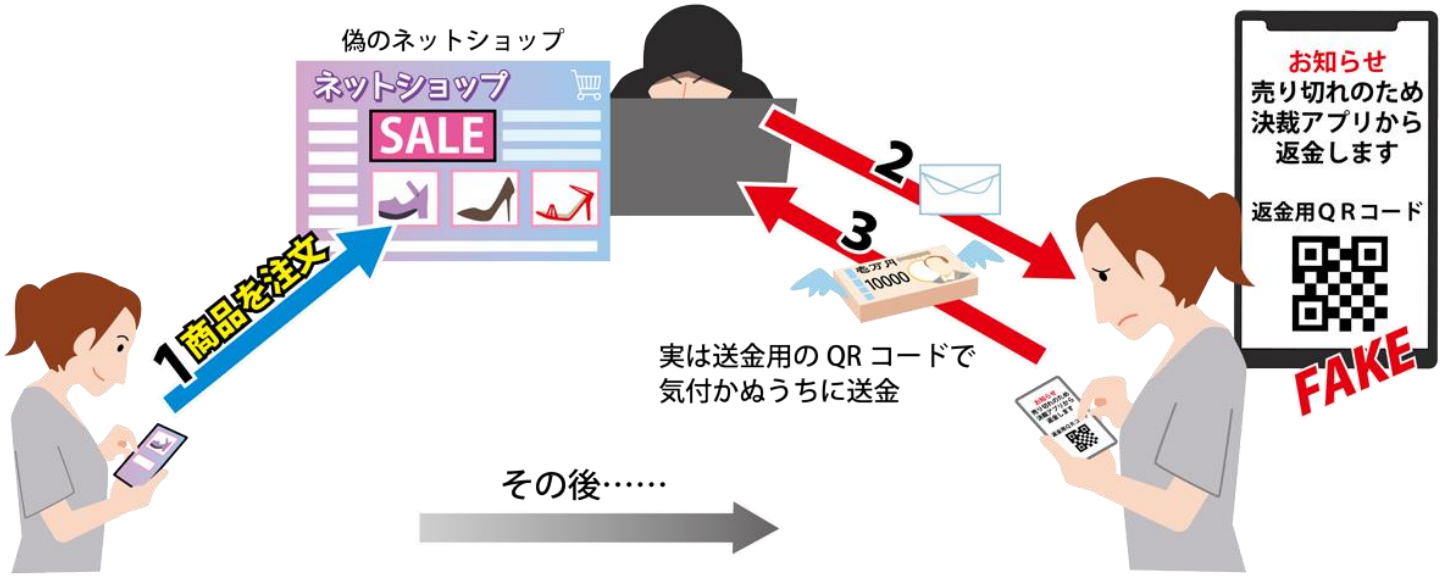
スマホ決済の不正利用

● 事例

- **偽の通販サイトで決済アプリを用い、商品の返金手続きを装った不正送金**

ウェブサイトで商品を注文した消費者が、「欠品のため決済アプリで返金します」と連絡を受け、返金手続きを行ったところ、返金ではなく、逆に相手方に送金された

※ 消費者庁 注意喚起 令和7年2月28日
<https://www.caa.go.jp/notice/entry/041215/>



スマホ決済の不正利用

● 対策

【予防】

- P.30「情報セキュリティ対策の基本」③、⑥の実施
- 多要素認証の設定を有効にする
- 本人認証（3Dセキュア）が採用されているクレジットカードを極力利用する
- 認証情報を適切に運用する（P.7＜基本のキ＞適切にパスワードを設定する）
- 決済サービス利用時には、必ず公式ウェブサイト、または公式アプリからアクセスする
- 決済アプリで返金すると称し、コード決済へのアクセスを促されても安易に応じない
- スマートフォン紛失時の対策として、端末を探すために設定を行う
  - iPhone：「iPhoneを探す」
  - Android：「デバイスを探す」

【早期検知】被害に遭っていないかを確認することが大事

- スマホ決済サービスの利用状況の通知機能の利用、利用履歴の定期的な確認
- スマホに紐づいている銀行口座の出金履歴やクレジットカードの利用明細の確認

● ネット上の誹謗・中傷・デマ

● どんな手口・被害？
- 誹謗、中傷、脅迫、犯罪予告、デマをSNS等のメッセージや画像を介して投稿され、それらが伝言ゲームのようにさらに拡散することで、悪影響を及ぼす
- 拡散時に内容が改変され、第三者の情報に紐づけられることで、誹謗・中傷がさらに広がる

● 投稿されるとどうなるの？
- 不特定多数から心無いメッセージが届く
- 精神的苦痛 等

● 投稿するとどうなるの？
- 不特定多数から心無いメッセージが届く
- 風評被害
- 社会的混乱

不適切な投稿は、訴えられ、裁判沙汰になることも

・法的責任を問われる可能性があるので、投稿や拡散の内容を十分に確認し、慎重に行動する
・ 匿名の投稿であっても、投稿者情報の開示請求により、発信者が特定される場合がある

ネット上の誹謗・中傷・デマ

● 対策

【誹謗・中傷・デマをしないために】

- 慌てない、一呼吸して冷静になる
- 情報リテラシー、情報モラルの向上、法令遵守の意識向上
- 情報の信頼性を確認する
- 誹謗・中傷や公序良俗に反する投稿や拡散をしない
- 投稿や拡散の責任を問われることを認識する

大勢の前で名乗って言えないこと、できないことはインターネットでも発信しないという心構えが大事

なぜやってしまうのか？

・日頃の不満やストレスの捌け口
・自己承認欲求(関心、注目を集めたい)
・炎上や訴訟等リスクを認識できていない
・匿名だから自分の投稿であると特定されないと誤解している
・情報がデマである可能性を理解できていない
※見ず知らずの人が匿名で書いていることも、インターネット上の情報はなぜか本当のことであると考えがち
・拡散すれば人の役に立つと親切心が裏目に（災害対策情報をデマとわからず拡散）

ネット上の誹謗・中傷・デマ

● 対策

【誹謗・中傷を受けてしまったら】

- 投稿、掲載された情報の記録・保存
- 相談する
  （違法・有害情報相談センター、人権相談、誹謗中傷ホットライン）
- 書き込みの削除を検討し、依頼する場合は掲示板等の作成者、管理人等に連絡
- 管理人等に連絡が取れない場合は、プロバイダー等に削除を依頼する
- 弁護士への相談
- 警察への通報・相談

警察庁　インターネット上の誹謗中傷等への対応
https://www.npa.go.jp/bureau/cyber/countermeasures/defamation.html

● フィッシングによる個人情報等の詐取

● どんな手口・被害？

- 実在の企業、公的機関、金融機関、ショッピングサイト等のサービス提供元を騙った偽のウェブサイトのURLが記載されたメールやSMSが送信されてくる
- 偽のメールやSMSは確定申告等、実社会の動きに合わせ、時宜を得て送信されてくる
- URLリンクのクリックやQRコードを読み込んで情報を入力すると、入力した情報が詐取される

● 被害に遭うとどうなるの？

- サービスの認証情報を入力した場合、不正ログインされ、不正送金、物品等購入により金銭被害に遭う
- 個人情報を入力した場合、個人情報が詐取され、詐取された情報が複数の犯罪者間で共有・売買される

フィッシングによる個人情報等の詐取

- 事例
  - **クイッシング（QRコード詐欺）**

看板やチラシ、郵送物に掲載されているQRコードの中には、偽サイトにアクセスさせる有害なものが確認されている。

QRコードのリンク先は目視ではアクセス前に確認できないので、支払先や送金といった、自身の意図に合致しているかを慎重に確認することが重要

【報告】京王線内の本学広告への虚偽のQRコードが貼られた件について　令和7年10月24日
＜https://www.uec.ac.jp/news/announcement/2025/20251024_7249.html＞

フィッシングによる個人情報等の詐取

● 対策

【予防】

- P.30「情報セキュリティ対策の基本」 ②、③、⑥ の実施
- 突然届いた身に覚えのないメールやSMSは真偽を見分けようとせず、基本的に無視し、削除する
- 安易に添付ファイルの開封、メールやSMSのURLリンクのクリック/タップ、QRコードにアクセスしない
- よくアクセスするウェブサイトはブックマーク（お気に入り）に登録し、ブックマーク以外からアクセスしない
- セキュリティソフトでアクセスブロック機能を活用する
- パスキーが利用可能な場合は、極力利用する
- 迷惑メールフィルターを利用する

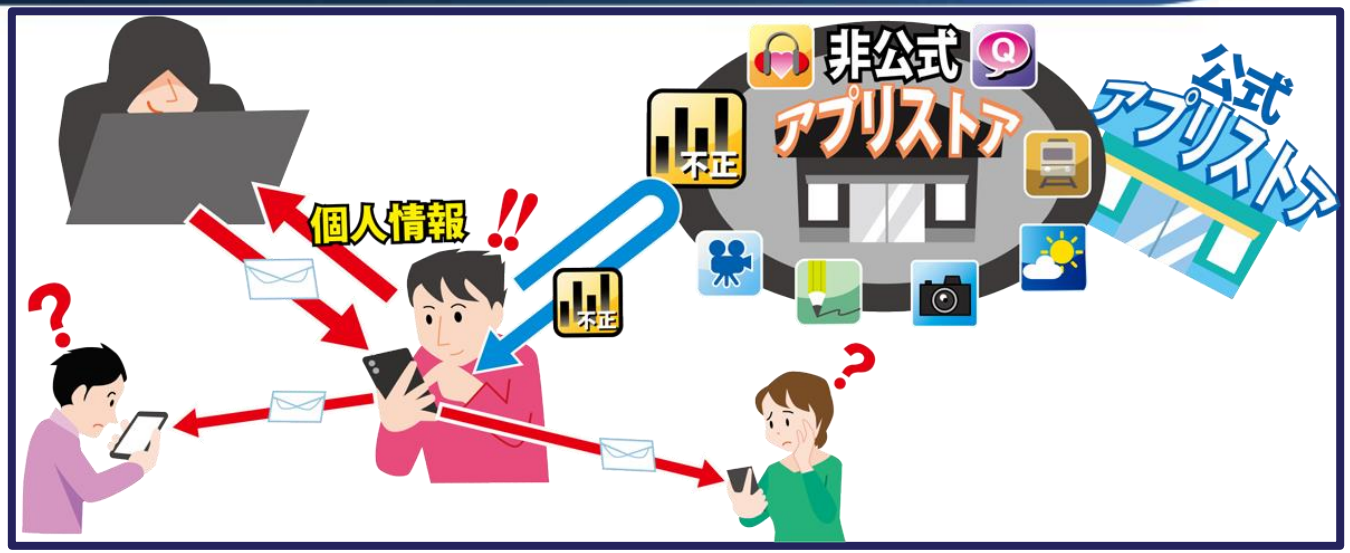
【被害拡大予防】

- 利用しているサービスの多要素認証の設定を有効にする

【早期検知】 被害に遭っていないかを確認することが大事

- ログインすると通知されるログインアラート機能の利用
- クレジットカードの利用明細やインターネットバンキング等の利用状況をこまめに確認

● 不正アプリによるスマートフォン利用者への被害



● どんな手口・被害？

- 興味を引く内容が記載されたメールやSMS内のURLリンクをタップし、不正アプリをインストールさせられてしまう
- SNSでダウンロードサイトに誘導する手口も確認されている

● 被害に遭うとどうなるの？

- スマホに保存されている情報が窃取される
  - ・認証情報を窃取された場合、オンラインサービス等への不正アクセスやキャリア決済等による金銭被害につながる可能性がある
  - ・連絡先情報が窃取された場合、連絡先宛に不正なメール、SMSがばらまかれる
- 遠隔操作により勝手に詐欺SMSを送信される
- サイバー攻撃に悪用される

不正アプリによるスマートフォン利用者への被害

● 事例

・携帯電話会社を騙り、不正なアプリのインストールを誘導するウェブサイトが確認されている
不正アプリをインストールするとスマートフォンがマルウェアに感染するおそれがあり、端末内の情報を窃取する可能性がある

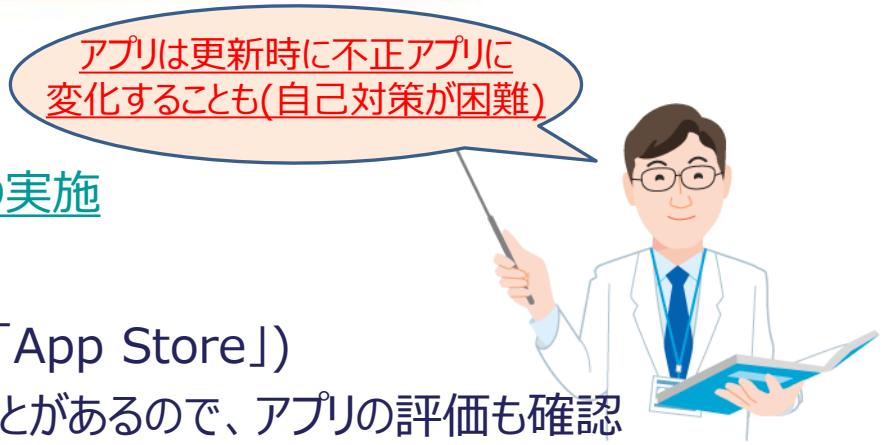
【注意喚起】ドコモを装った不正なアプリのインストール、マルウェア感染にご注意ください
https://www.docomo.ne.jp/info/notice/page/260114_00.html

・特定の企業名を騙ることなく、“至急”の確認や連絡を求めるような文面でURLへのアクセスを促し、リンク先で不正アプリをダウンロードさせる事例が確認されている

宅配事業者、通信事業者を装った迷惑SMSにご注意ください（2025年11月14日更新）
https://www.docomo.ne.jp/info/spam_mail/column/20180725/

不正アプリによるスマートフォン利用者への被害

● 対策



【予防】

- P.30「情報セキュリティ対策の基本」⑥ の実施
- アプリは公式マーケットから入手する※4
  (Androidは「Google Play」、iPhoneは「App Store」)
  ※公式マーケットに不正アプリが紛れ込むことがあるので、アプリの評価も確認
- インストール時にアプリの機能に不要なアクセス権限を求めていないか確認する
- 不要なアプリをインストールしない
- インストールされているアプリを確認する、利用しないアプリはアンインストールする
- アプリ更新時に不審な機能、悪意ある機能が無いか、更新内容を確認する

なぜ、やってしまうのか？

なぜ、不正アプリをインストールしてしまうのか
- ・実在の企業を名乗っていて、それを信じてしまうから
- ・確認や連絡を“至急”に求める文面で、受信者の冷静な判断を阻害するから
- ・メールやSMSなどで不正アプリの配布サイトへ誘導され、インストールしてしまうから

※4 2025年12月に施行された「スマートフォンにおいて利用される特定ソフトウェアに係る競争の促進に関する法律」では、多様な経路でのアプリ提供が可能になりました。一方で、セキュリティリスクも指摘されており、公式マーケット以外から入手するアプリは慎重に確認する必要があります。

● メールや SNS 等を使った脅迫・詐欺の手口による金銭要求

- どんな手口・被害？
  - メールやSNS等の非対面のコミュニケーションを用い、公的機関や出会いのきっかけを装い、恋愛感情や何らかの信頼感を得たり、脅したりして金銭を詐取する

- 被害に遭うとどうなるの？
  - PCをハッキングした、示談の和解金が必要、アダルトサイトの未納料金がある、至急対応が必要等とメール等で不安を煽られ、冷静さを失い金銭要求に応じてしまう
  - SNSで親交を深め、恋愛感情を逆手に、投資詐欺をしかけられ、送金してしまう
  - SNS等でのやりとりを通して不正アプリのインストールに誘導され、スマホに保存されている連絡先宛に性的な動画をばらまくと脅され、金銭を要求される

メールや SNS 等を使った脅迫・詐欺の手口による金銭要求

● 対策

【予防】

- 慌てない、一呼吸して冷静になる
- P.30「情報セキュリティ対策の基本」⑥ の実施
- 受信した脅迫、金銭要求、唐突、不自然なメールは無視し、メールに記載されている電話番号に絶対電話しない
- 信じない、疑う、公的機関や信頼できる人に相談する

  （警察相談専用電話 #9110、違法・有害情報相談センター、消費者ホットライン　188（いやや！））
- 同様の手口の存在を確認するため、受信メッセージからキーワードを検索してみる

巧妙な手口の数々

パターン1：　怖がらせる

「あなたのパソコンをハッキングした」「あなたが通報されている」「訴えられている」等と不安を煽る

パターン2：　信じ込ませる

社会的信用の高い組織を騙り、事態の深刻さ、緊急性を訴え、冷静さを失わせ、信じ込ませる

有名人や異性を装い交際を持ち掛け、親密になったところで投資など様々な名目で金銭を要求

パターン3：　相談しにくい

「あなたの恥ずかしい動画を撮影した」「アダルトサイトの未納料金があり裁判沙汰になる」等と脅し、金銭を要求

「情報セキュリティ対策の基本」は必ず実施！

- トラブルは、インターネットにアクセスし、ショッピング、SNS等のサービスを利用する際に発生する
- トラブルの手口、糸口は共通点が多く、「情報セキュリティ対策の基本」はトラブルの発生抑止に共通的に有効

攻撃の糸口	情報セキュリティ対策の基本	目的
① ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消して脆弱性を悪用した攻撃によるリスクを低減する
② マルウェアの利用	セキュリティソフトの利用	攻撃を検知してブロックする
③ パスワード窃取	パスワードの管理・認証の強化	パスワード窃取による情報漏えい等のリスクを低減する
④ 設定不備	設定の見直し（初期設定の確認）	誤った設定が悪用され、攻撃を受けないようにする
⑤ データの暗号化	バックアップの取得	PCやサーバーのデータ削除や暗号化に備える
⑥ ソーシャルエンジニアリング（罠にはめる）	脅威・手口を知る	手口から重要視するべき対策を理解する

詳しい説明は、「情報セキュリティ10大脅威2015」 解説書 1章 をご覧ください

困ったときの相談先

■IPA　安心相談窓口

国民からの一般的な情報セキュリティに関する技術的な相談に対してアドバイスを提供しています

https://www.ipa.go.jp/security/anshin/about.html

■他の機関が開設している窓口等

https://www.ipa.go.jp/security/anshin/external.html

困ったときに参考になるIPAのウェブコンテンツ

- IPAでは、被害に遭わないための解説コンテンツも公開中

■安心相談窓口だより

寄せられた相談内容を基に、手口や対策、対処等を図解

https://www.ipa.go.jp/security/anshin/attention/index.html

■手口検証動画シリーズ

寄せられた相談事例の手口を、実際に検証した際の様子を「手口検証動画シリーズ」として公開

https://www.ipa.go.jp/security/anshin/measures/verificationmov.html