情報セキュリティ10大脅威　2024

[個人編]

IPA Better Life with IT

「情報セキュリティ10大脅威」とは？

- IPAが2006年から毎年発行している資料
- 前年に発生したセキュリティ事故や攻撃の状況等から**ＩＰＡが脅威候補を選出**
- セキュリティ専門家や企業のシステム担当等から構成される**「10大脅威選考会」が投票**
- **TOP10入りした脅威を「10大脅威」**として脅威の概要、被害事例、対策方法等を解説

10大脅威の特徴

脅威に対して様々な立場の方が存在

立場ごとに注意すべき脅威も異なるはず

- 家庭等でパソコンやスマホを利用する人「個人」

- 企業や政府機関等の組織
- 組織のシステム管理者や社員・職員

「組織」

「個人」と「組織」の２つの立場で脅威を解説

情報セキュリティ10大脅威 2024

「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	5年連続8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	9年連続9回目
クレジットカード情報の不正利用	2016年	9年連続9回目
スマホ決済の不正利用	2020年	5年連続5回目
偽警告によるインターネット詐欺	2020年	5年連続5回目
ネット上の誹謗・中傷・デマ	2016年	9年連続9回目
フィッシングによる個人情報等の詐取	2019年	6年連続6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	9年連続9回目
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	2019年	6年連続6回目
ワンクリック請求等の不当請求による金銭被害	2016年	2年連続4回目

情報セキュリティ10大脅威 2024

「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[illegible]取	2016年	5年連続8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	9年連続9回目
クレジットカード情報の不正利用	[illegible]16年	9年連続9回目
スマホ決済の不正利用		[illegible]回目
偽警告によるインターネット詐[illegible]		
ネット上の誹謗・中傷・デ[illegible]		
フィッシングによる個人情報等の[illegible]		
不正アプリによるスマートフォン利用者への被[illegible]		[illegible]回目
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	2019年	6年連続6回目
ワンクリック請求等の不当請求による金銭被害	2016年	2年連続4回目

自身により強く関係する脅威から対策することが重要

情報セキュリティ対策の基本

- 多数の脅威があるが「攻撃の糸口」は似通っている
- 基本的な対策の重要性は長年変わらない
- 下記の**「情報セキュリティ対策の基本」を常に意識することが重要**

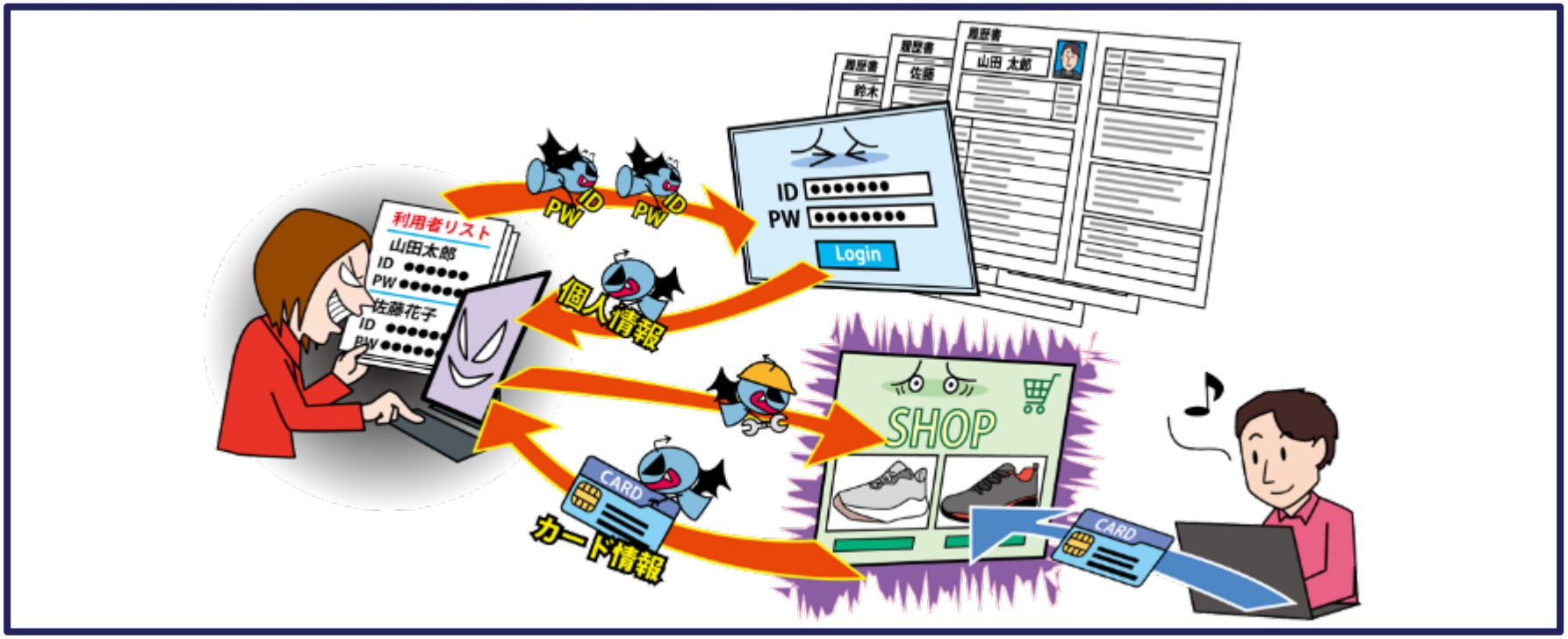
攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視するべき対策を理解する

「個人」向け脅威の解説

- ここからは脅威毎に解説します
- 自身により強く関係する脅威から確認しましょう
- **各脅威の対策の説明では前項の「情報セキュリティ対策の基本」は実施していることを前提とし、記載には含めていません。**

インターネット上のサービスからの個人情報の窃取

～情報が盗まれたことに気付いたら、即座に対応を～



- 攻撃者がショッピングサイト等、インターネット上のサービスの脆弱性等を悪用し、個人情報を窃取する
- 窃取された情報が悪用されると、クレジットカードを不正利用されたり、詐欺メールを送信されたりする

インターネット上のサービスからの個人情報の窃取

～情報が盗まれたことに気付いたら、即座に対応を～

- **攻撃手口**
  - **脆弱性や設定不備を悪用して不正アクセス**
    - 適切なセキュリティ対策が行われていないショッピングサイト等に対し、攻撃者が脆弱性や設定の不備を悪用した攻撃を行い、Webサイト内の個人情報を窃取する

  - **脆弱性や設定不備を悪用してWebサイトを改ざん**
    - Webサイトが攻撃者に改ざんされたことに、利用者が気付かず、そのWebサイト上で情報を入力してしまうと、入力した情報を窃取される

インターネット上のサービスからの個人情報の窃取

～情報が盗まれたことに気付いたら、即座に対応を～

- **攻撃手口**
  - **不正に入手した認証情報を悪用**
    - 他のサービスから窃取したIDとパスワードを悪用して、攻撃者がサービスに不正ログインし、個人情報を窃取する
    - 利用者がパスワードを他のサービスで使いまわしている場合、パスワードが窃取された際に、他のサービスにも不正ログインされてしまい、被害が大きくなるおそれがある

インターネット上のサービスからの個人情報の窃取

～情報が盗まれたことに気付いたら、即座に対応を～

- **2023年の事例/傾向①**
  - **不正に入手された認証情報の悪用**
    - 2023年3月、エン・ジャパンが、総合転職情報サイト「エン転職」に登録された個人情報が漏えいしたことを公表
    - 原因はパスワードリスト攻撃による不正アクセスであった
    - 「エン転職」に登録したユーザーの内、約25万5,000人のWeb履歴所にアクセスされたおそれがある
    - 同社は全ユーザーのアカウントのパスワードをリセットし、再設定をユーザーに求めた

【出典】「エン転職」への不正ログイン発生に関するお詫びとお願い（エン・ジャパン株式会社）
https://corp.en-japan.com/newsrelease/2023/32484.html

インターネット上のサービスからの個人情報の窃取

～情報が盗まれたことに気付いたら、即座に対応を～

- **2023年の事例/傾向②**
  - **不正アクセスにより顧客情報の窃取のおそれ**
    - 2023年10月、ビッグモーターが、個人情報が漏えいしたおそれがあることを公表
    - 原因は同社のWebサイトが不正アクセスされたことであった
    - 漏えいした個人情報は2016年11月から2023年8月にお問い合わせページに入力された情報であり、氏名、住所、電話番号、メールアドレスが含まれていた
    - 同社が取り扱う顧客情報は別システムで保管されているため、顧客情報の漏えいは無いとしている

【出典】 不正アクセスによる個人情報漏えいの可能性に関するお詫びとお知らせ（株式会社ビッグモーター）
https://www.bigmotor.co.jp/lib/news/news_list.php?id=703&page=

インターネット上のサービスからの個人情報の窃取

～情報が盗まれたことに気付いたら、即座に対応を～

- **2023年の事例/傾向③**
  - **不正アクセスで個人情報窃取**
    - 2023年10月、カシオ計算機は、契約している利用者の個人情報が漏えいしたことを公表
    - 原因はシステムのネットワークセキュリティ設定の一部が解除状態になり、開発環境のデータベースへ不正アクセスが行われたことであった
    - 漏えいした個人情報は国内では個人や教育機関等から約9万件、海外では148の国と地域から約3万5,000件で、合計約12万5,000件としている

【出典】 不正アクセスによる個人情報漏えいのお詫びとご報告（カシオ計算機株式会社）
https://www.casio.com/jp/information/1018-incident/

インターネット上のサービスからの個人情報の窃取

～情報が盗まれたことに気付いたら、即座に対応を～

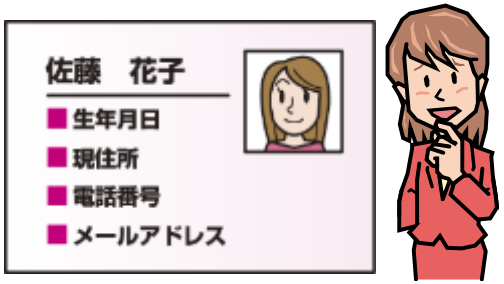
- **対策**
  - **インターネット利用者**

【被害の予防】

- サービス利用の必要性を判断し、不要なサービスには登録しない
  - 利用しなくなったサービスからは退会する
- 必要項目以外の情報は極力登録しない
- 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
- 不正ログイン対策を実施する

例えば

- パスワードは長く、複雑にして、使い回さない
- 不審なWebサイトで安易に認証情報を入力しない　等
  （フィッシングに注意）



インターネット上のサービスからの個人情報の窃取

～情報が盗まれたことに気付いたら、即座に対応を～

- **対策**
  - **インターネット利用者**

【被害の早期発見】

- クレジットカード利用明細を定期的に確認する
  - クレジットカード会社の公式アプリをインストールし、通知を有効にしておくことでリアルタイムに確認できる
- 漏えいしたメールアドレスを検索できるサービスを使う
  - 自身が使用しているメールアドレスで検索し、アカウント情報が窃取されていないか確認する

アカウント情報漏えいの有無を確認できるサービス※1

【出典】※1 Have I Been Pwned?（HaveIBeenPwned.com）
https://haveibeenpwned.com/

インターネット上のサービスからの個人情報の窃取

～情報が盗まれたことに気付いたら、即座に対応を～

- **対策**
  - **インターネット利用者**

【被害を受けた後の対応】

- サービス運営者（コールセンター等）へ相談する
- クレジットカードの利用停止手続きをする
  （クレジットカードを不正利用されていた場合）
- 都道府県警察本部のサイバー犯罪相談窓口に相談する※1
- パスワードを変更する
  - 同じパスワードを使い回している場合、そのサービス全てのパスワードを変更する

【参考】※１都道府県警察本部のサイバー犯罪相談窓口
https://www.npa.go.jp/bureau/cyber/soudan.html

インターネット上のサービスへの不正ログイン

～そのパスワード、本当に安全？個人情報を含めないよう注意！～

- 利用しているインターネット上のサービスの認証情報（ID、パスワード）が窃取または推測され、不正ログインされる
- 別のサービスで使い回しをしていた認証情報が漏えいし、不正ログインされる
- インターネット上のサービスの機能に応じて発生する被害は様々

♦ 攻撃手口

・不正に入手した認証情報で不正ログインする

- **フィッシング詐欺**
  - メールやSMS等を使い、受信者を騙してフィッシングサイトに誘導し、認証情報等を詐取する
- **パスワードリスト攻撃**
  - 何らかの方法で入手した認証情報をリスト化し、それを利用して複数のサービスにログインを試みる攻撃
  - 複数のサービスでパスワードを使いまわしている場合、1つのパスワードが漏えいすると他のサービスにも不正ログインされるおそれがある

♦ 攻撃手口

・不正に入手した認証情報で不正ログインする

- **パスワード類推攻撃**
  - 利用者が使いそうなパスワードを類推して不正ログインを試みる
  - 名前や誕生日などをパスワードに使用していると推測されやすくなる
  - SNSで公開している情報などから推測されるおそれもある
- **ウイルス感染による窃取**
  - 悪意あるWebサイトやメール等でウイルス感染させ、その端末で入力したパスワード等を窃取

- **2023年の事例/傾向①**
  - **乗っ取った著名人のアカウントを販売**
    - 2023年5月、著名人のアカウントを乗っ取り、売買した7人が不正アクセス禁止法違反の容疑で書類送検された
    - 公開しているプロフィール情報内の氏名、生年月日等からパスワードが推測されて、不正ログインされていた
    - 不正ログインされたアカウントはWebサイトで売買されたり、さらなる転売をされていた
    - アカウントを購入した人は、乗っ取ったことを自慢したりしていたとされる

【出典】 著名人を狙った金銭目的のSNS公式アカウントののっとりについてまとめてみた（piyolog）
https://piyolog.hatenadiary.jp/entry/2023/05/12/002134

- **2023年の事例/傾向②**
  - **二段階認証を突破し、不正ログインして買い物**
    - 2023年9月、でAmazonのアカウントを不正利用されたとの報告がX（旧Twitter）上で次々投稿された
    - 不正ログインされたアカウントは購入履歴を非公開にされ不正利用に気付きにくくなっていた
    - 不正ログインされたアカウントの中には二段階認証を突破してログインされたパターンもあった
    - Amazonは手口について調査中としている

【出典】「Amazonを不正利用された」――SNS上で報告相次ぐ 「二段階認証を突破された」などの声も（ITmedia NEWS）
https://www.itmedia.co.jp/news/articles/2309/14/news152.html

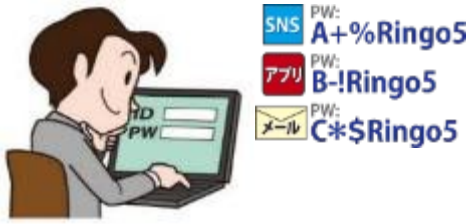
- **2023年の事例/傾向③**
  - **不正に入手した情報で第三者がログイン**
    - 2023年9月、SMBC日興証券が、システムに不正ログインが行われたことを公表
    - 悪意のある第三者が窃取したと思われる口座番号やパスワード等を用いて不正ログインが行われた
    - オンライントレードサービスで、不正に保有株式の売却を行ったと思われる取引が1件あった
    - 同社は利用者にパスワード変更依頼や注意喚起を行った

【出典】 お客様へのお知らせ：日興イージートレードにおける不正アクセスにご注意ください（ＳＭＢＣ日興証券株式会社）
https://www.smbcnikko.co.jp/news/customer/2023/n_20230904_01.html
ネット取引サービスに不正ログイン、株式不正売却も - SMBC日興証券（SecurityNEXT）
https://www.security-next.com/149297

IPA

- **対策**
  - **利用者**

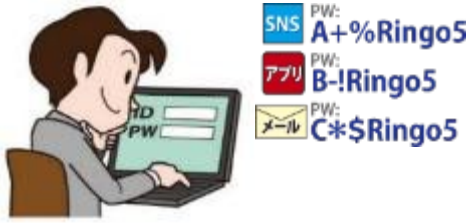
【被害の予防】



- メールの添付ファイル開封や、メールやSMSのリンク、URLのクリックを安易にしない
- パスワードは長く、複雑にして、異なるサービスで使いまわさない
- パスワードを覚えきれない場合は、パスワード管理ソフトを利用する
- 利用しているサービスが対応しているならばパスキーを利用する
- 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
- 不審なWebサイトで安易に認証情報を入力しない（フィッシングに注意）
- 利用していないサービスからは退会する
- 利用頻度が低いサービスではクレジットカード情報を都度入力する

インターネット上のサービスへの不正ログイン

～そのパスワード、本当に安全？個人情報を含めないよう注意！～



- **対策**
  - **利用者**

【被害の早期検知】

- 利用しているサービスのログイン履歴を確認する
- 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する

【被害を受けた後の対応】

- クレジットカードの利用停止手続きをする
- パスワードを変更する
  - 他のサービスで同じパスワードを使っていた場合は同様に対応する
- サービス運営者（コールセンター等）へ相談する
- 都道府県警察本部のサイバー犯罪相談窓口に相談する※1

【参考】※1 都道府県警察本部のサイバー犯罪相談窓口
https://www.npa.go.jp/bureau/cyber/soudan.html

クレジットカード情報の不正利用

～一度も使っていないクレジットカードが不正利用される！？～

- ウイルス感染やフィッシング詐欺、改ざんされたWebサイトにより<u>クレジットカード情報を詐取される</u>
- クレジットカード情報を<u>ショッピングサイト等で不正利用される</u>

クレジットカード情報の不正利用

～一度も使っていないクレジットカードが不正利用される！？～

IPA

♦ 攻撃手口

・攻撃者が用意した偽のページに情報を入力させて詐取

- **フィッシング詐欺による情報詐取**
  - 実在する企業を模した偽のWebサイト（フィッシングサイト）を攻撃者が用意し、メールやSMSでサイトへ誘導してクレジットカード情報を入力させる

- **正規の決済画面を改ざんして情報窃取**
  - ショッピングサイトの脆弱性等を悪用して正規Webサイトの決済画面を改ざんし、利用者を誘導してクレジットカード情報を入力させる
  - 正規のWebサイト上に偽画面があるため、気付くことが困難

クレジットカード情報の不正利用

～一度も使っていないクレジットカードが不正利用される！？～

IPA

- **攻撃手口**

・不正アクセスや不正な売買で入手した情報を悪用

- **不正アクセス**
  - 決済代行会社のシステムの脆弱性を悪用し、システムに不正アクセスし、クレジットカード情報を窃取する
- **漏えいした情報の悪用**
  - インターネット上のサービスから漏えいした情報はダークウェブと呼ばれる闇サイトで売買されることもある
  - 攻撃者が闇サイトで得たクレジットカード情報を不正に利用

クレジットカード情報の不正利用

～一度も使っていないクレジットカードが不正利用される！？～

- **攻撃手口**

・クレジットカード情報を特定して悪用

- **クレジットカードマスター攻撃**
  - クレジットカード番号、有効期限、セキュリティコードは桁数やパターンが限られている。これらの組み合わせをツールにより総当たりで入力し、クレジットカード情報を特定、悪用する。

クレジットカード情報の不正利用

～一度も使っていないクレジットカードが不正利用される！？～

- **攻撃手口**

・ウイルスに感染させて情報を窃取

- **メールを利用したウイルス感染の手口**
  - 攻撃者が悪意のあるプログラムを含むファイルを作成し、それを添付してメールを送信する。その後、送信したメールの受信者に添付ファイルを開かせることでウイルス感染させる
  - クレジットカード決済の利用者が、ウイルス感染した端末上で決済を行うことでクレジットカード情報を窃取される

クレジットカード情報の不正利用

～一度も使っていないクレジットカードが不正利用される！？～

- **2023年の事例/傾向①**
  - **「NICO ONLINE SHOP」でクレジットカード情報流出**
    - 2023年10月、クレジットカード情報が流出したおそれがあることをFANSMILEが公表した
    - 流出したおそれがあるクレジットカード情報は、2021年3月から2022年12月にかけて「NICO ONLINE SHOP」で利用された13,084件であった
    - 原因は、同社が運営するWebサイトが攻撃者に不正アクセスされ、決済アプリケーションを改ざんされたことであった

【出典】 当サイトへの不正アクセスによる個人情報漏えいに関するお詫びとお知らせ（株式会社FANSMILE）
https://nico-online.com/news/54

クレジットカード情報の不正利用

～一度も使っていないクレジットカードが不正利用される！？～

- **2023年の事例/傾向②**
  - **「志布志市ふるさと納税特設サイト」でクレジットカード情報流出**
    - 2023年6月、クレジットカード情報が流出したおそれがあることを鹿児島県志布志市が公表した
    - 流出したおそれがあるクレジットカード情報は、「志布志市ふるさと納税特設サイト」で2021年3月から12月にかけて利用された910件であった
    - 原因は、当該Webサイトが改ざんされ、クレジットカード決済時に情報を窃取する不正なソフトウェアが実行されたことであった

【出典】 本市が運営する「志布志市ふるさと納税特設サイト」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ（志布志市）
https://www.city.shibushi.lg.jp/soshiki/5/22233.html

クレジットカード情報の不正利用

～一度も使っていないクレジットカードが不正利用される！？～

- **2023年の事例/傾向③**
  - **クレジットカード情報の不正利用被害額が昨年より増加**
    - 2023年12月、日本クレジット協会が「クレジットカード不正利用被害実態調査の結果」を公開した
    - 2023年1月～9月の被害額は401.9億円となり、2022年同期間の被害額309億円と比較して増加しており、過去最悪のペースで被害が発生していた
    - 正規の利用者が騙されていなくてもクレジットカード情報を攻撃者に入手され、正規の利用者が被害に遭うおそれがあるクレジットマスター攻撃をIPAが複数確認しており、注意を促した

【出典】 クレジットカード不正利用被害の集計結果について（一般社団法人日本クレジット協会）
https://www.j-credit.or.jp/download/news20231228_a1.pdf
コンピュータウイルス・不正アクセスの届出事例［2023 年上半期（1 月～6 月）］（IPA）
https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/2023-h1-jirei.pdf

クレジットカード情報の不正利用

～一度も使っていないクレジットカードが不正利用される！？～

- **対策**
  - **利用者**

【被害の予防】

- クレジットカード会社が提供している本人認証サービス（3Dセキュア等）を利用する
- メールの添付ファイル開封や、メールやSMSのリンク、URLのクリックを安易にしない
- 普段は表示されないような画面やポップアップが表示された場合、情報を入力しない
- プリペイドカードやデビットカードの利用を検討する
  - 不正利用被害額となる利用可能金額の範囲を限定する
- 利用頻度が低いサービスではクレジットカード情報を保存しない
- 利用していないクレジットカードは契約解除や物理的破棄を検討する

クレジットカード情報の不正利用

～一度も使っていないクレジットカードが不正利用される！？～

- **対策**
  - **利用者**

【被害の早期検知】

- クレジットカードの利用明細を定期的に確認する
- サービス利用状況の通知機能等を利用する

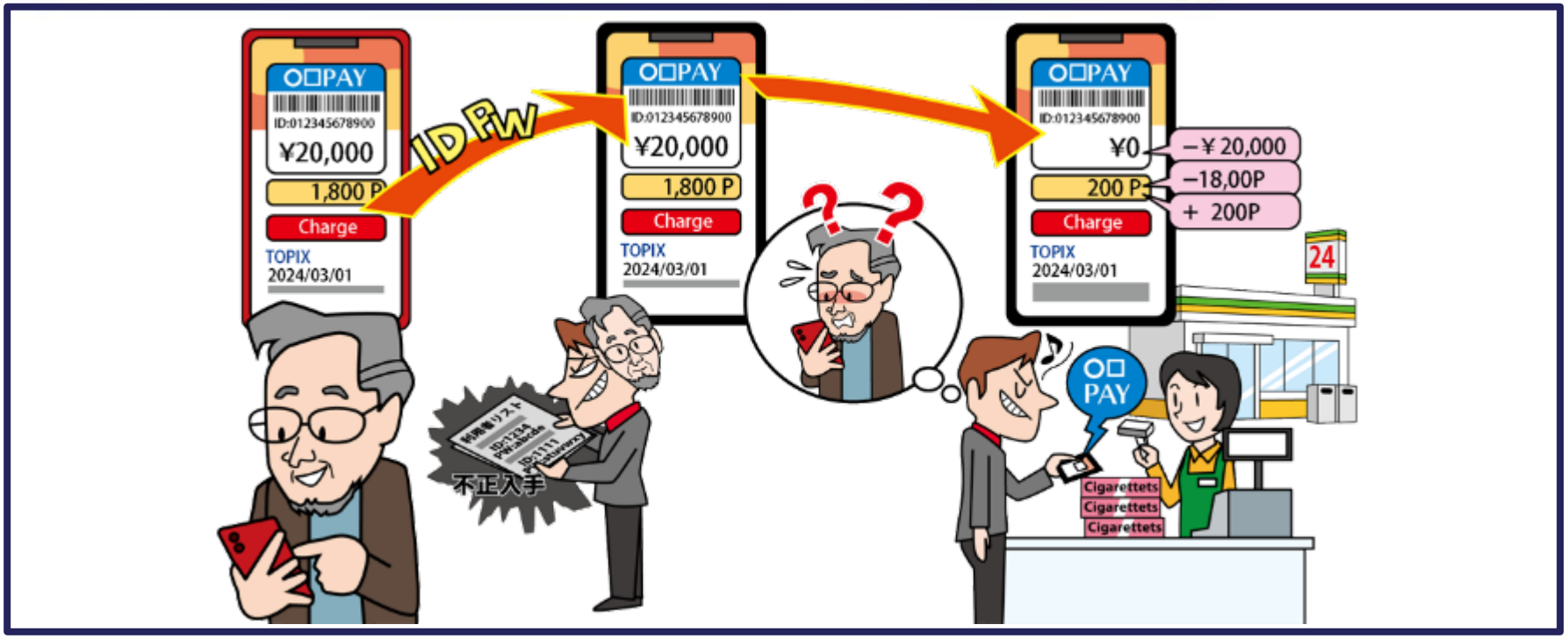
【被害を受けた後の対応】

- クレジットカードの利用停止手続きをする
- ウイルス感染した端末の初期化
- サービス運営者（コールセンター等）へ相談する
- 都道府県警察本部のサイバー犯罪相談窓口に相談する※1
- パスワードを変更する
  - 他のサービスで同じパスワードを使っていた場合は同様に対応する

【参考】※1 都道府県警察本部のサイバー犯罪相談窓口
https://www.npa.go.jp/bureau/cyber/soudan.html

スマホ決済の不正利用

～スマホで簡単決済。悪用されると攻撃者も簡単決済。～



- スマホ決済サービスに不正ログインして<u>アカウントを乗っ取る</u>
- スマホ決済サービスの<u>脆弱性等の不備を悪用</u>
- クレジットカード情報等の<u>窃取</u>や、利用者が<u>意図しない金銭取引</u>を行う

スマホ決済の不正利用

～スマホで簡単決済。悪用されると攻撃者も簡単決済。～

- **攻撃手口**
  - **不正アクセスによるアカウントの乗っ取り**
    - 過去に漏えいしたパスワードをリスト化し、不正ログインを試みる
      ※パスワードリスト攻撃と呼ばれる攻撃手口
    - フィッシング攻撃等により詐取したIDやパスワードで不正ログインを試みる
    - パスワードの使いまわしを想定して、同一のパスワードで複数のサービスへの不正ログインを試みる
    - 多要素認証等のセキュリティ機能を利用していない場合、パスワードのみでログインが可能になるため、不正ログインされやすくなる

スマホ決済の不正利用

～スマホで簡単決済。悪用されると攻撃者も簡単決済。～

- **攻撃手口**
  - **サービスのセキュリティ上の不備を悪用**
    - 決済用システムやアプリの脆弱性を悪用し、利用者の意図しない決済を行う
    - 当該サービスだけでなく、金融機関等の他のサービスとの連携にセキュリティ上の不備があると悪用される場合がある
    - 多要素認証が提供されていない場合、攻撃者に悪用されやすくなり、サービス利用状況の通知サービスが提供されていない場合、正規の利用者が被害に気が付きにくくなる

スマホ決済の不正利用

～スマホで簡単決済。悪用されると攻撃者も簡単決済。～

- **攻撃手口**
  - **不正に入手したスマートフォンで決済をする**
    - ロックをかけていない、またはロックを解除した状態のスマートフォンを紛失したり、盗難されると不正にスマホ決済を利用される
    - 攻撃者がeSIM（スマホ等に内蔵されたデジタルSIM）を乗っ取り、不正にスマホ決済を利用する

スマホ決済の不正利用

～スマホで簡単決済。悪用されると攻撃者も簡単決済。～

- **2023年の事例/傾向①**
  - **「PayPay」を用いて自身のアカウントに不正送金**
    - 2023年4月、「PayPay」の他人のアカウントから、自身のアカウントに約8万円を不正送金した容疑者を兵庫県警が逮捕した
    - 容疑者と被害者は飲食店で知り合い、被害者は自身のスマートフォンのロックが解除されていたことと「PayPay」の残高がなくなっていたことに気が付き警察に相談した
    - その後、送金履歴等から容疑者が特定された

【出典】 ＰａｙＰａｙの送金で８万円をだまし取る 神戸市職員を逮捕（産経新聞）
https://www.sankei.com/article/20230412-XQE4VBCLEFMZTGDR4YSJUDUWVY/

スマホ決済の不正利用

～スマホで簡単決済。悪用されると攻撃者も簡単決済。～

- **2023年の事例/傾向②**
  - **他人の「auPAY」アカウントで不正に決済**
    - 2023年1月、佐賀県警と蕨署等が不正アクセス禁止法違反と詐欺等の疑いで中国籍の男女を再逮捕した
    - 容疑者はコンビニエンスストアで「auPAY」を使用し、他人名義の決済用バーコードを用いて約55,000円の物品を購入していた。
    - その後、被害者が不正な決済に気が付き、佐賀県警に相談したことで事件が発覚した。その後、店舗の防犯カメラの映像等から容疑者が特定された

【出典】 レジで支払った女逮捕、一緒にいた男も…関係ない女性の「auPAY」を使っていた　夜のコンビニで（埼玉新聞）
https://www.saitama-np.co.jp/articles/15070/postDetail

スマホ決済の不正利用

～スマホで簡単決済。悪用されると攻撃者も簡単決済。～

- **2023年の事例/傾向③**
  - **スマートフォンを乗っ取り、スマホ決済を不正に利用**
    - 2023年9月、名古屋県警等がブラジル国籍の容疑者を詐欺容疑で逮捕した
    - 容疑者は他人名義の決済サービスを利用して約8,000円相当の物品を不正に購入した疑いがあった
    - 被害者の女性のスマートフォンの「eSIM」（スマホ等に内蔵されたデジタルSIM）を乗っ取って不正に決済したと見られている

【出典】 スマホ決済不正利用容疑　３９歳逮捕　ｅＳＩＭ乗っ取りか（読売新聞オンライン）
https://www.yomiuri.co.jp/local/aichi/news/20230927-OYTNT50233/

スマホ決済の不正利用

～スマホで簡単決済。悪用されると攻撃者も簡単決済。～

- **対策**
  - **スマホ決済サービスの利用者**

【被害の予防】

- 多要素認証の設定を有効にする
- クレジットカード連携をする場合は3Dセキュアを利用する
- パスワードは長く、複雑にする
- パスワードを使い回さない
- パスワード管理ソフトを利用する
- パスワードを他人に教えない
- 提供されているならば、パスキーを利用する
- フィッシングに注意する
- 利用していないサービスからは退会する
- スマートフォンの紛失対策をする（画面ロック等のセキュリティ対策を実施）

スマホ決済の不正利用

～スマホで簡単決済。悪用されると攻撃者も簡単決済。～

IPA

- **対策**
  - **スマホ決済サービスの利用者**

【被害の早期検知】

- スマホ決済サービスの利用状況通知機能の利用および利用履歴を定期的に確認する
- 連携する銀行口座の出金履歴を確認する

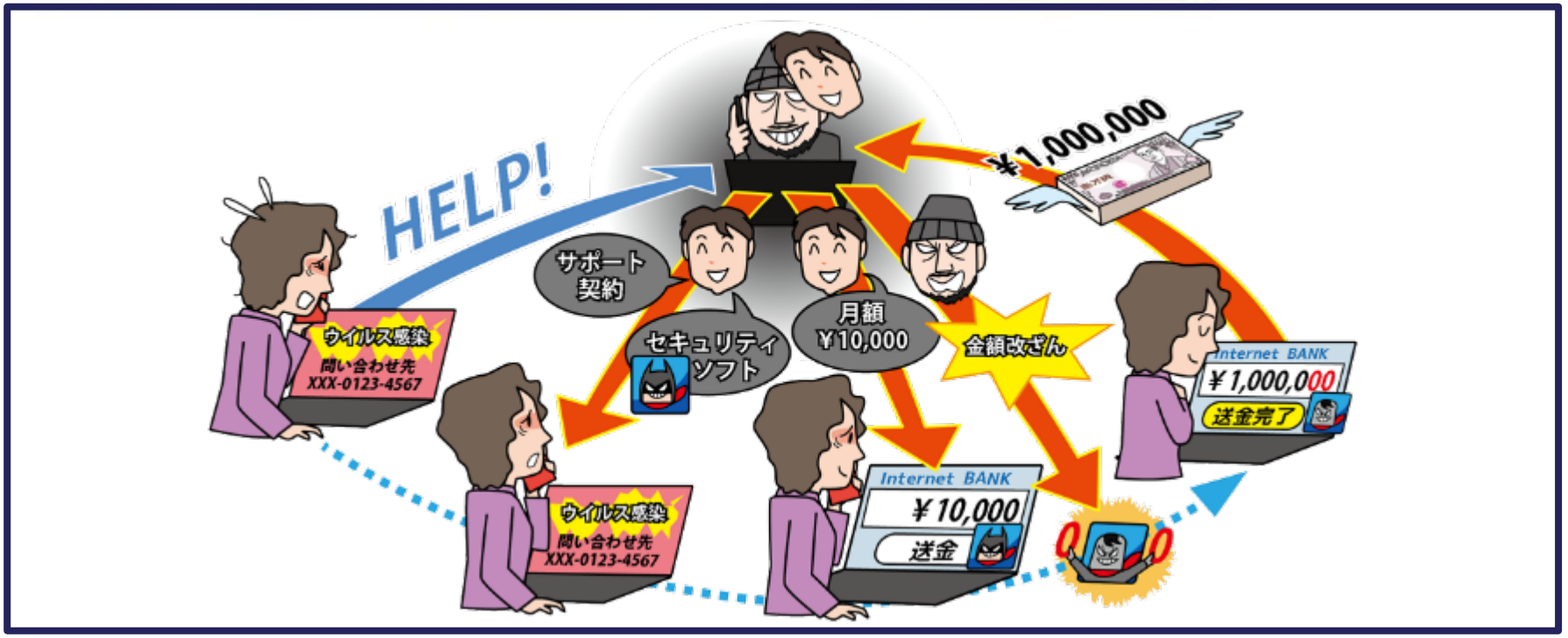
【被害を受けた後の対応】

- パスワードを変更する
  - 他のサービスで同じパスワードを使っていた場合は同様に対応する
- サービス運営者（コールセンター等）へ相談する
- 連携している金融機関へ相談する
- 都道府県警察本部のサイバー犯罪相談窓口に相談する※1

【参考】※1 都道府県警察本部のサイバー犯罪相談窓口
https://www.npa.go.jp/bureau/cyber/soudan.html

偽警告によるインターネット詐欺

～表示された番号に電話をかけないで！突然の警告画面に要注意～



- インターネット閲覧中にウイルス感染やシステム破損に関する偽の警告画面（偽警告）を表示させる
- 被害者は偽警告の内容を信じて、警告の内容に従ってしまうと不要なソフトウェアのインストールやサポート契約を結ばされる
- 最終的に、修復費用等として金銭を騙し取られる

偽警告によるインターネット詐欺

～表示された番号に電話をかけないで！突然の警告画面に要注意～

- **攻撃手口**
  - **巧妙に細工が施された偽の警告画面**
    - PCやスマートフォンがウイルス感染したかのように見せかけて、利用者を慌てさせるような偽の警告画面を表示させる
    - 実在の企業ロゴを表示したり、警告音や警告メッセージを音声で流す
    - 警告画面を繰り返しポップアップで表示させ偽警告を閉じられないと誤解させる

【参考】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

偽警告によるインターネット詐欺

～表示された番号に電話をかけないで！突然の警告画面に要注意～

- **攻撃手口**
  - **サポート詐欺**
    - PCやスマートフォンの利用者に、偽警告の画面に表示させた偽のサポート窓口へ電話をかけさせる
    - オペレーターによる遠隔操作で対策したように見せかけ、修復費用の支払いへ誘導する
    - 支払い方法はコンビニエンスストアで販売されているプリペイド型電子マネーやギフトカードを指定されるケースがある
    - インターネットバンキングの画面で、遠隔操作をしながら振り込みをさせるケースもある

偽警告によるインターネット詐欺

～表示された番号に電話をかけないで！突然の警告画面に要注意～

- **攻撃手口**
  - **スマホアプリのインストールへ誘導**
    - スマートフォンに表示させた偽警告の解決方法として、スマホアプリのインストールへ誘導する

      ※誘導先は公式マーケット

      ※アフィリエイト収益や、料金請求(自動継続課金)が目的と考えられる
  - **有償セキュリティソフトの購入へ誘導**
    - 偽のセキュリティソフトをインストールさせ、有償ソフトウェアの購入へ誘導する

【参考】 スマートフォンの偽セキュリティ警告から自動継続課金アプリのインストールへ誘導する手口にあらためて注意！（IPA）
https://www.ipa.go.jp/security/anshin/attention/2022/mgdayori20221025.html

偽警告によるインターネット詐欺

～表示された番号に電話をかけないで！突然の警告画面に要注意～

- **2023年の事例/傾向①**
  - **偽警告による詐欺で4,400万円騙し取られる**
    - 2023年4月、埼玉県警浦和署は偽警告を使った詐欺の被害が発生したと発表した
    - 被害者がPCでインターネットを閲覧していた際、「ウイルスに感染しました」との警告が表示され、表示された連絡先に電話した
    - パソコン関連会社の社員を名乗る人物から「ウイルスに感染している」「パソコンを遠隔操作で確認する」「ハッキングされて口座に入っているお金が危ないので、別の口座に振り込む必要がある」等と不安を煽られた
    - 指定された口座にインターネットバンキングで20回にわたり計約4,400万円を振り込んでしまった

【出典】 大惨事…男性のPCに驚きの警告出現　表示された番号に電話し、片言の男に案内され4400万円失う　何があった（埼玉新聞）
https://www.saitama-np.co.jp/articles/23485

偽警告によるインターネット詐欺

～表示された番号に電話をかけないで！突然の警告画面に要注意～

- **2023年の事例/傾向②**
  - **PCを遠隔操作され、振込金額の変更により被害増大**
    - 2023年1月、兵庫県警は、偽警告によるサポート詐欺でPCを遠隔操作され、金銭を騙し取られる被害が相次いでいると発表
    - 被害者の1人は、PCに表示された「ウイルスに感染」との警告に従い自宅の電話番号を入力した
    - ソフトウェア会社の社員を名乗る人物から電話があり、指示に従って遠隔操作用ソフトウェアをインストールさせられた
    - サポート費用1万円と手数料490円を要求され、インターネットバンキングから振り込む際に、PCを遠隔操作されて振込金額の桁数を増やされてしまい、49万円が送金されていた

【出典】 個人のパソコンを遠隔操作、ネットバンキングから現金だまし取る　新たな手口、兵庫で被害相次ぐ（神戸新聞NEXT）
https://www.kobe-np.co.jp/news/sougou/202302/0016081001.shtml

偽警告によるインターネット詐欺

～表示された番号に電話をかけないで！突然の警告画面に要注意～

- **2023年の事例/傾向③**
  - **偽警告被害の相談件数が大幅に増加**
    - IPA 安心相談窓口によると、偽のセキュリティ警告に関する相談件数が2023年は4,145件となり、2022年の2,365件と比較して約1.75倍と大きく増加した
    - 相談件数は2022年第2四半期から概ね増加傾向が続いており、特に2023年第4四半期は1,324件と、過去6年間で最多となった

【出典】 情報セキュリティ安心相談窓口の相談状況［2023年第4四半期（10月～12月）］（IPA）
https://www.ipa.go.jp/security/anshin/reports/2023q4outline.html
情報セキュリティ安心相談窓口の相談状況［2022年第4四半期（10月～12月）］（IPA）
https://www.ipa.go.jp/security/anshin/reports/2022q4outline.html
情報セキュリティ安心相談窓口公開レポート（IPA）
https://www.ipa.go.jp/security/anshin/reports/index.html

偽警告によるインターネット詐欺

～表示された番号に電話をかけないで！突然の警告画面に要注意～

- **対策**
  - **インターネット利用者**

【被害の予防】

- 表示される警告を安易に信用しない
  - 慌てず冷静に判断し、判断が難しい場合は信頼できる周りの方に相談
- 偽警告が表示されても従わない
  - 警告に指示されたアプリやソフトウェアをインストールしない
  - 電話をかけない
  - 電話してしまったとしても遠隔操作をさせない、サポート料金を払わない、プリペイド型電子マネーを購入しない
- 偽警告が表示されたらブラウザを終了※1
- ブラウザの通知機能を不用意に許可しない※2
- ポップアップや広告のブロック機能などを設定する

【参考】 ※1 サポート詐欺で表示される偽のセキュリティ警告画面の閉じ方（IPA）
https://www.ipa.go.jp/security/anshin/doe3um0000005cag-att/20231115173500.pdf
※2 安心相談窓口だより「ブラウザの通知機能から不審サイトに誘導する手口に注意」（IPA）
https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210309.html

偽警告によるインターネット詐欺

～表示された番号に電話をかけないで！突然の警告画面に要注意～

- **対策**
  - **インターネット利用者**

【被害を受けた後の対応】

- PCを遠隔操作された場合はシステムの復元や初期化を行う
- アプリをアンインストールする
  - 自動継続課金設定をされていないかも確認し、設定されていたら解除
- 虚偽のサポート契約の解消
- クレジットカード会社へ相談する
  （クレジットカード情報を表示された画面に入力してしまった場合）
- 国民生活センター／消費生活センターへ相談する※1
- 都道府県警察本部のサイバー犯罪相談窓口に相談する※2

【参考】※1 国民生活センター／消費生活センター
https://www.kokusen.go.jp/map/
※2 都道府県警察本部のサイバー犯罪相談窓口
https://www.npa.go.jp/bureau/cyber/soudan.html

ネット上の誹謗・中傷・デマ

～その情報、本当に本物でしょうか？～

- SNS等で他人を誹謗・中傷したり、脅迫・犯罪予告を書き込み、事件になる
- 誹謗・中傷やデマの発信は犯罪になり、安易に拡散した人も、その行為を特定され、社会的責任を問われる場合がある
- AI技術を用いて加工された音声や画像、動画は本当か見分けがつきにくく、一層注意が必要になっている

- **要因**
  - **匿名性を利用した影響ある情報発信**
    - 自身の意見や感情を発言する際に、その内容の影響を考慮せずに発信してしまう
    - 匿名の発信であることでその内容が過激になりやすい
      （法律に基づいた手続きにより身元を特定される）
  - **第三者による情報の拡散・改変**
    - 誹謗・中傷やデマを見た第三者が、悪意の有り無し関係なく、真偽を確認せずに拡散する
    - 拡散が繰り返されたり、別の情報と紐づけられたりすることで内容が改変されて誹謗・中傷やデマが広がるおそれがある

- **2023年の事例/傾向①**
  - **反応欲しさに…、ネット掲示板で名誉を毀損**
    - 2023年5月、匿名掲示板に誹謗・中傷の内容の投稿を実施した大学生が、名誉毀損の罪で有罪判決を受けた
    - 投稿では被害者を名指しした上で、被害者が交通死亡事故を起こし逮捕されたというものであった
    - 逮捕された大学生は「過激な投稿をすれば多くの人に反応してもらえる」と考えて掲示板に投稿していた

【出典】 高須克弥氏への名誉毀損事件で大学生に有罪判決　さいたま地裁（朝日新聞 DIGITAL）
https://www.asahi.com/articles/ASR5C54TZR5CUTNB00D.html

- **2023年の事例/傾向②**
  - **インフルエンサーにデマ広告を依頼し、個人情報を窃取**
    - 2023年10月、京都府警が不正アクセス禁止法と窃盗の疑いで、20代の男性を逮捕した
    - その男性は、被害者の情報を窃取し、消費者金融から被害者名義で20万円を借り入れ、現金を盗んだとされる
    - 男性は、SNSで多数のフォロワーを持つ、インフルエンサーと呼ばれるユーザーに「登録するとポイントが受け取れる」と虚偽の広告を投稿するように依頼し、その広告から登録した被害者の情報を悪用したとみられている

【出典】 消費者金融を不正利用疑い　ＳＮＳに偽広告、男逮捕（熊本日日新聞）
https://kumanichi.com/articles/1206209

- **2023年の事例/傾向③**
  - **生成AIを悪用し、報道番組風動画を公開**
    - 2023年11月、日本テレビの報道番組かのようなフェイク動画がSNS上に投稿された
    - フェイク動画は生成AIを用いて作成され、総理大臣が実際に発言したかのように、声や口元の動き等を模倣していた
    - 製作者は業務を妨害するつもりはなかったと謝罪を行い、投稿されたフェイク動画は削除されている
    - 日本テレビはフェイク動画について今後も必要に応じてしかるべき対応をするという姿勢を見せている

【出典】 番組に似せた岸田首相の偽動画拡散 日本テレビが注意呼びかけ（NHK NEWS WEB）
https://www3.nhk.or.jp/news/html/20231104/k10014247171000.html

♦ 対策

• 発信者、閲覧者

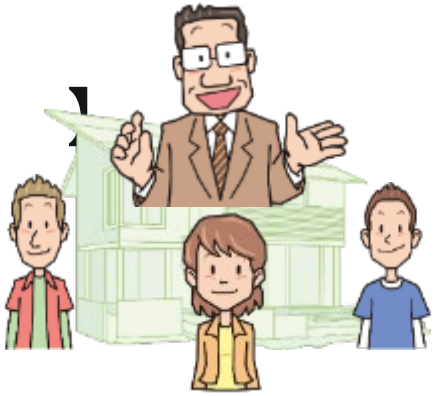
【被害の予防（被害に備えた対策含む）】

- 情報モラルや情報リテラシーの向上、法令遵守の意識の向上
  - 情報を閲覧する際は鵜呑みにせずに信頼性を確認する
  - 安易に情報を拡散しない
  - 誹謗・中傷や公序良俗に反する内容の投稿をしない
  - 投稿したり拡散したりする際はその前に内容に問題がないか再確認する
  - 匿名性があっても投稿や拡散の責任を問われることを理解する

• 家庭、教育機関

【被害の予防（被害に備えた対策含む）】

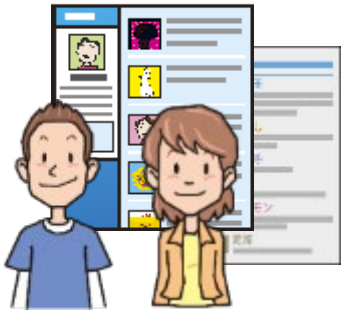
- 情報モラル、情報リテラシーの教育
  - 子供たちへの教育の実施



IPA

- **対策**
  - **被害者**

【被害を受けた後の適切な対応】



- 冷静な対応と支援者への相談をする
  - 一人で抱え込まず、信頼できる周囲の人や公的相談機関へ相談する
  - 犯罪と思われる誹謗・中傷の投稿は、警察へ被害届を提出し、必要に応じて弁護士にも相談する
- 管理者やプロバイダーへ情報削除依頼
  - 情報削除により事態が悪化するおそれもあるため、周囲の人や弁護士等に相談して慎重に行う

【参考】 インターネット上の誹謗中傷への対策（総務省）
https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/hiboutyusyou.html
ネットの誹謗中傷(セーファーインターネット協会)
https://www.saferinternet.or.jp/bullying/
都道府県警察本部のサイバー犯罪相談窓口
https://www.npa.go.jp/bureau/cyber/soudan.html
弁護士、日本司法支援センター法テラス
https://www.houterasu.or.jp/

フィッシングによる個人情報等の詐取

～金融機関や公的機関を装うフィッシング詐欺に注意を～

- 金融機関や有名企業を装ったフィッシングサイト（偽のWebサイト）へ利用者を誘導する
- フィッシングサイト上でIDやパスワード、クレジットカード情報等の個人情報を入力させて窃取する

【参考】 URLリンクへのアクセスに注意（IPA）
https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210831.html

フィッシングによる個人情報等の詐取

～金融機関や公的機関を装うフィッシング詐欺に注意を～

IPA

♦ 攻撃手口

・攻撃者が用意した偽のサイトに情報を入力させて詐取

- **フィッシングサイトへ誘導するメール等を送信**
  - 攻撃者が公的機関や有名企業のWebサイトを模倣したフィッシングサイトを用意する
  - 公的機関や有名企業を装ったメールやSNS、SMSを不特定多数に送信し、フィッシングサイトに誘導する
  - 近年ではSMSによる誘導（スミッシング）が多くみられるが、QRコードによる誘導（クイッシング）も見られている
  - フィッシングサイトで利用者が入力した情報を詐取する
- **検索サイトの検索結果に偽の広告を表示させる**
  - 検索エンジンの検索結果等に表示される広告の仕組みを悪用して虚偽の不正な広告を表示させ、フィッシングサイトへ誘導する

フィッシングによる個人情報等の詐取

～金融機関や公的機関を装うフィッシング詐欺に注意を～

- **2023年の事例/傾向①**
  - **給付金の受給申請を装ったフィッシング**
    - 2023年12月、デジタル庁はマイナポータルを騙った詐欺メールおよび偽サイトについて注意喚起を行った
    - 詐欺メールの件名は「電力・ガス・食料品等価格高騰緊急支援給付金（5万円／1世帯）のご案内」等とされており、給付金の受給申請を促して偽のマイナポータルサイトへ誘導する内容であった
    - 誘導先のサイトでは個人情報、クレジットカード情報等の入力が求められ、入力するとその情報が窃取される

【出典】 マイナポータルをかたるフィッシング（2023/12/06）（フィッシング対策協議会）
https://www.antiphishing.jp/news/alert/mynaportal_20231206.html
マイナポータルを騙った詐欺メール及び偽サイト（フィッシング詐欺）に関する注意喚起（デジタル庁）
https://www.digital.go.jp/news/4750a8f5-1061-4ae6-903b-cfb327a50465

フィッシングによる個人情報等の詐取

～金融機関や公的機関を装うフィッシング詐欺に注意を～

- **2023年の事例/傾向②**
  - **フィッシングを発端としたインターネットバンキング不正送金被害急増**
    - 2023年12月、 警察庁と金融庁が連名で、メールやSMSに記載されたリンクからアクセスしたWebサイトにIDやパスワード等を入力しないよう注意喚起を行った
    - 2023年1月から11月末におけるフィッシングによるものとみられるインターネットバンキングの不正送金の被害件数は5,147件、被害額は約80.1億円となり、いずれも過去最多を更新している

【出典】 2023年4月24日 フィッシングによるものとみられるインターネットバンキングに係る 不正送金被害の急増について（警察庁）
https://www.npa.go.jp/bureau/cyber/pdf/20230424_press3.pdf
2023年8月8日 フィッシングによるものとみられるインターネットバンキングに係る 不正送金被害の急増について（警察庁）
https://www.npa.go.jp/bureau/cyber/pdf/20230808_press.pdf
2023年12月26日 フィッシングによるものとみられるインターネットバンキングに係る 不正送金被害の急増について（警察庁）
https://www.npa.go.jp/bureau/cyber/pdf/20231225_press.pdf

フィッシングによる個人情報等の詐取

～金融機関や公的機関を装うフィッシング詐欺に注意を～

- **2023年の事例/傾向③**
  - **QRコードを用いたフィッシング攻撃に注意**
    - 2023年12月5日、米連邦取引委員会はQRコードに隠された有害なリンクに注意するよう警告文を公開した
    - 2023年11月、サイバー情報共有イニシアティブ（J-CSIP）においても、マイクロソフトを装った、QRコードを用いたフィッシングメールを確認していることを公開している
    - フィッシングメールではQRコードを読み取ってメールアカウント情報を期限までに更新するように促す内容であり、QR コードを読み取ることでフィッシングサイトが開かれるものであった

【出典】 米FTC、QRコードを用いた「クイッシング」攻撃について注意喚起（CNET Japan）
https://japan.cnet.com/article/35212658/
サイバー情報共有イニシアティブ（J-CSIP） 運用状況 [2023年7月～9月]（IPA）
https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/fy23-q2-report.pdf

- **対策**
  - **インターネット利用者**

【被害の予防（被害に備えた対策含む）】

- SMSやメールで受信したURLや、SNSの投稿内のURLを安易にクリックしない
  - どうしても内容が気になる場合は、よく使うサービスはあらかじめ公式アプリをインストールしておくことや、Webサイトをブックマーク（お気に入り登録）しておくことで確認時に利用する
- 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
- 迷惑メールフィルターを利用する

♦ 対策

• インターネット利用者

【被害の早期検知】

- 利用しているサービスで、いつもと異なるログインがあった場合に通知する設定を有効にする
  - 通知があった際は自身のログインによるものかを確認する
- 利用しているサービスのログイン履歴の確認する
- クレジットカードやインターネットバンキングの利用明細を確認する

フィッシングによる個人情報等の詐取

～金融機関や公的機関を装うフィッシング詐欺に注意を～

- **対策**
  - **インターネット利用者**

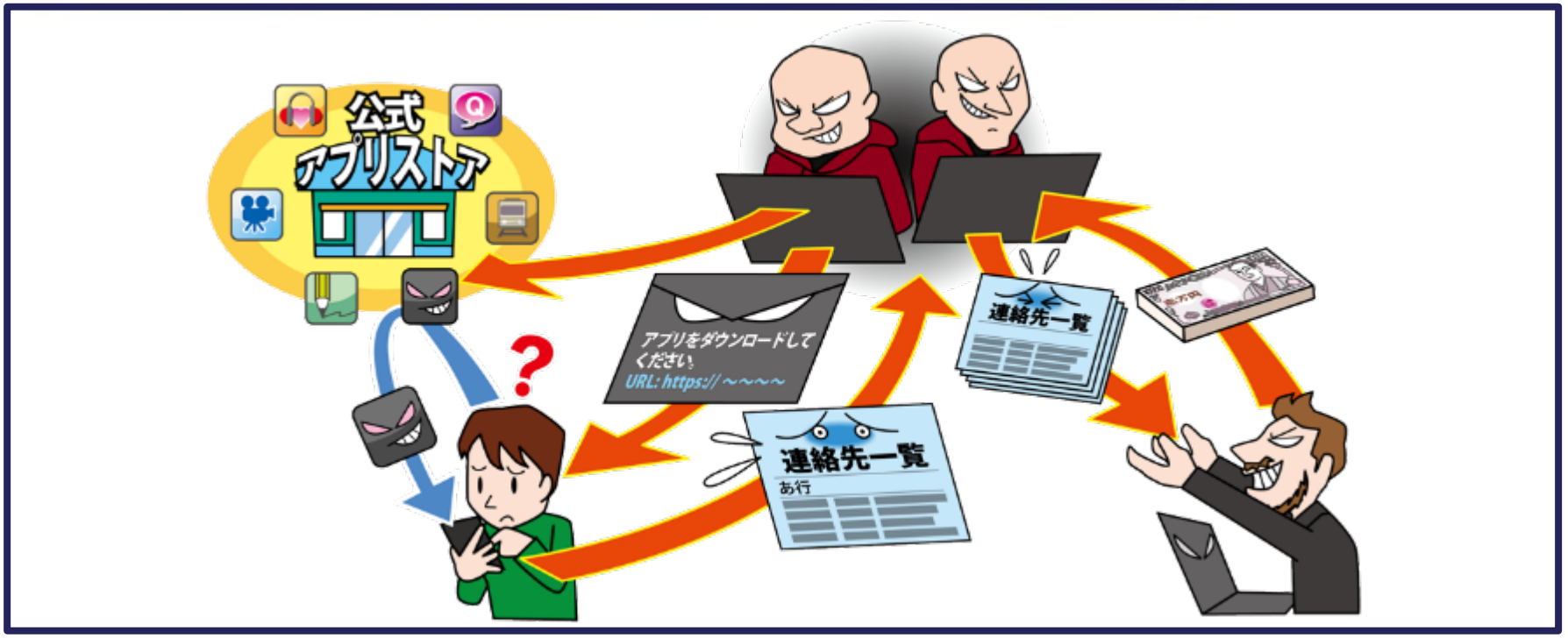
【被害を受けた後の対応】

- 大量のフィッシングメールを受信している場合はメールアドレスの変更を検討する（メールアドレスの漏えいを懸念した対応）
- パスワードを変更する
  - 他のサービスで同じパスワードを使っていた場合は同様に対応する
- サービス運営者（コールセンター等）へ相談する
- 信頼できる機関に相談する

【参考】 迷惑メール相談センター（日本データ通信協会）
https://www.dekyo.or.jp/soudan/index.html
フィッシング対策（警察庁）
https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html
フィッシング対策協議会
https://www.antiphishing.jp/registration.html

不正アプリによるスマートフォン利用者への被害

～アプリ提供者やアクセス権の確認を忘れずに～



- 不正アプリをスマートフォンにインストールしてしまうことで、スマートフォン内の連絡先情報等の個人情報が窃取される
- スマートフォンの一部の機能を不正利用される
- 攻撃の踏み台にされることで意図せず加害者になるおそれも

不正アプリによるスマートフォン利用者への被害

～アプリ提供者やアクセス権の確認を忘れずに～

- **攻撃手口**
  - **不正アプリのダウンロードサイトへ誘導する**
    - 攻撃者が不正アプリの偽のダウンロードサイトを用意し、実在の企業を騙ったメールやSMS等で偽サイトへ誘導する
    - 実在の企業からの連絡と誤認させてインストールさせる
  - **公式マーケットに不正アプリを紛れ込ませる**
    - 不正アプリを正規のアプリと見せかけて公式マーケットに公開する
    - 正規のアプリと思い込ませ、インストールさせる
  - **アプリの更新で不正アプリに変化する**
    - インストール後のアプリの更新で悪意ある機能が顕在化する

不正アプリによるスマートフォン利用者への被害

～アプリ提供者やアクセス権の確認を忘れずに～

- **2023年の事例/傾向①**
  - **公式マーケット以外にある複数の不正アプリ**
    - 2023年12月、SBI EVERSPIN は、「Fake Finder for SBI Group」において複数の不正アプリを検出したため、注意喚起を行った
    - 検出した不正アプリには、金融機関または公共機関等を詐称する偽アプリ等があった
    - 不正アプリには電話、ファイルとメディア、SNS、連絡先へのアクセス権限を要求するもの等もあり、開発元の信頼性やアプリの機能、利用規約等を慎重に確認するよう注意を呼び掛けた

【出典】 Android向けAI基盤の不正アプリ検知アプリ「Fake Finder」が検知した悪性アプリに関する注意喚起のお知らせ
～2023年10月における不正アプリ状況をレポート～（SBIホールディングス株式会社）
https://www.sbigroup.co.jp/news/2023/1206_14275.html
App Store以外の配信アプリによるセクストーション被害を確認（IPA）
https://www.ipa.go.jp/security/anshin/attention/2019/mgdayori20191224.html

不正アプリによるスマートフォン利用者への被害

～アプリ提供者やアクセス権の確認を忘れずに～

- **2023年の事例/傾向②**
  - **Google Play にもある多数の不正アプリ**
    - 2023年11月、カスペルスキーは、Google Play 上の悪意のあるアプリの合計ダウンロード数が 6 億回を超えていることを発表した
    - 悪意のあるアプリには盗聴を行うトロイの木馬、端末内の情報や位置情報を窃取するスパイウェア等が見つかっている
    - アプリの真正性を確認することや、アプリの評価を過信しないこと、信頼性の高い保護アプリをインストールすること、デバイススキャンをすること等の対策が必要であることを紹介した

【出典】 Google Playのアプリにマルウェア 2023年は６億回以上ダウンロードされる（kaspersky daily）
https://blog.kaspersky.co.jp/malware-in-google-play-2023/35124/

不正アプリによるスマートフォン利用者への被害

～アプリ提供者やアクセス権の確認を忘れずに～

- **2023年の事例/傾向③**
  - **宅配業者を装った偽SMSによる不在通知**
    - 2023年11月、安中市は、宅配業者を装った偽SMSによる不在通知が増加しているとして注意喚起を行った
    - 被害者は、宅配便の不在連絡のようなSMSが届いた際に、記載されていたURLにアクセスをした。このときに氏名などの個人情報を入力してしまった可能性があった
    - その後、約11万円がキャリア決済され、電子マネーを購入されていることが発覚した

【出典】 宅配便業者を装った「不在通知」の偽SMSに注意しましょう（安中市）
https://www.city.annaka.lg.jp/page/1591.html

不正アプリによるスマートフォン利用者への被害

～アプリ提供者やアクセス権の確認を忘れずに～

- **対策**
  - **スマートフォン利用者**

【被害の予防】

- アプリは公式マーケットから入手する
  - 公式マーケットであっても様々な情報（レビュー評価等）を確認して信頼できるアプリのみ利用する
- アプリインストール時のアクセス権限を確認する
  - アプリの機能に対して適切かどうか確認する
- アプリインストールに関する設定に注意する
  - Android端末の設定で提供元不明のアプリのインストールを許可しない
  - iPhoneの設定で、「信頼されていないエンタープライズデベロッパ」の表示がされるアプリを信頼しない
- 不要なアプリをインストールしない
- 利用しないアプリやインストールした覚えのないアプリはアンインストールする
- セキュリティソフトをインストールする

♦ 対策

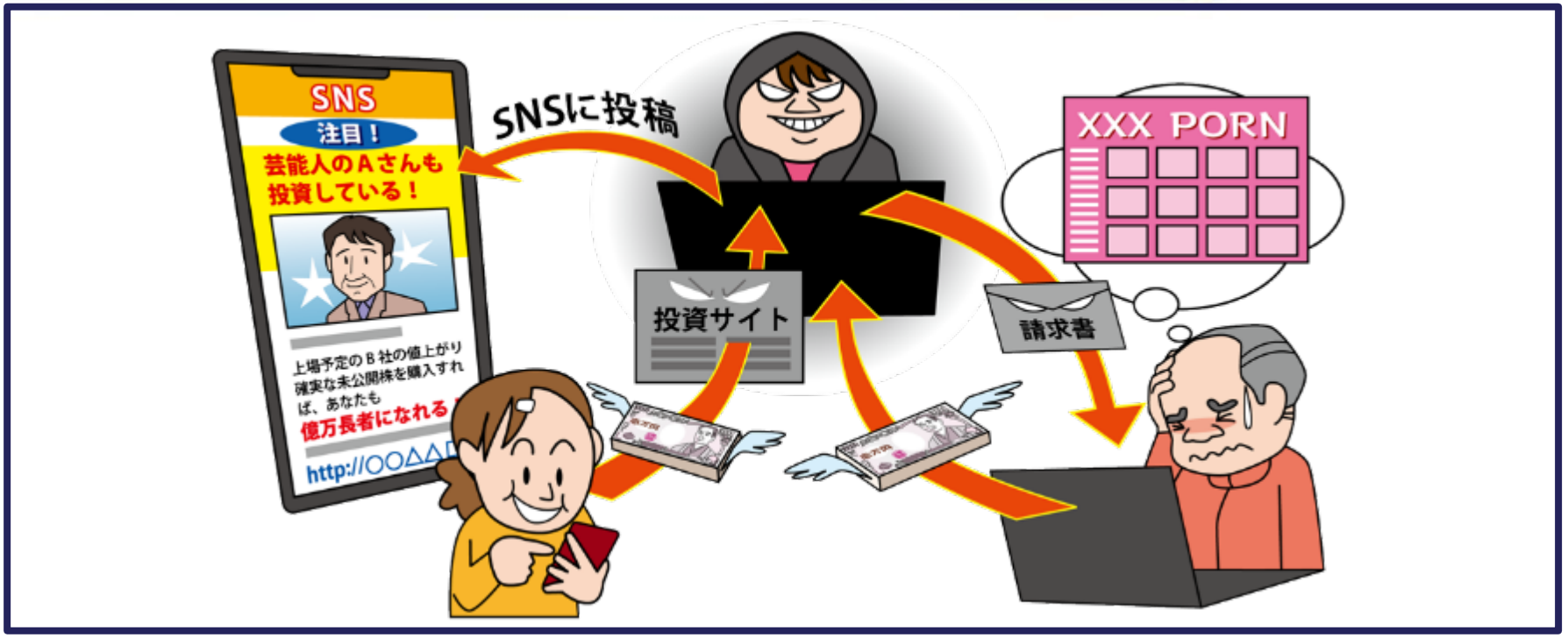
• スマートフォン利用者

【被害を受けた後の対応】

- 不正アプリをアンインストールする
  - アンインストールできない場合は端末を初期化する
- ショッピングサイトやSNS等、サービスの認証情報を入力してしまった場合はそのサービスのパスワードを変更する

メールや SMS 等を使った脅迫・詐欺の手口による金銭要求

～人生いろいろ。詐欺の手口もいろいろ～



- 周囲に相談しにくいセクストーション（性的脅迫）等のメールやSMS等を送り付けられ、金銭を要求される
- 脅迫・詐欺のメールの内容は虚偽のものであるが、その内容に騙され、不安に思ったメールやSMS等の受信者が金銭を支払ってしまう

メールや SMS 等を使った脅迫・詐欺の手口による金銭要求

～人生いろいろ。詐欺の手口もいろいろ～

- **攻撃手口**
  - **メールやSMSで金銭を要求する脅迫メールを送信**
    - 脅しや騙しの内容を記載したメールやSMS等を不特定多数にばらまき、金銭を要求する
      - プリペイド型電子マネーや暗号資産（仮想通貨）で支払うよう指定されることが多い
  - **周囲に相談しにくいセクストーション（性的脅迫）**
    - 「アダルトサイトを閲覧している姿を撮影した」等、被害者が周囲に相談しにくい性的な内容で脅迫して金銭を要求する
      - スマートフォンに不正アプリをインストールさせようと誘導する場合もある

【参考】 性的な映像をばらまくと恐喝し、仮想通貨で金銭を要求する迷惑メールに注意（IPA）
https://www.ipa.go.jp/security/anshin/attention/2018/mgdayori20181010.html
App Store以外の配信アプリによるセクストーション被害を確認（IPA）
https://www.ipa.go.jp/security/anshin/attention/2019/mgdayori20191224.html
遠隔操作ソフト（アプリ）を悪用される手口に気をつけて！（IPA）
https://www.ipa.go.jp/security/anshin/attention/2023/mgdayori20230411.html

メールや SMS 等を使った脅迫・詐欺の手口による金銭要求

～人生いろいろ。詐欺の手口もいろいろ～

- **攻撃手口**
  - **ハッキングしたように見せかける**
    - メール受信者のパスワード（過去に何らかの原因で漏えいしたもの）を記載し、あたかもメール受信者のPCをハッキングしてパスワードを得たかのように装い、不安を煽り、金銭を要求する
  - **公的機関を装ったり、電話を掛けたりして騙す**
    - 公的機関等の社会的な信用のある組織からの発信を装うことで信憑性、緊急性を高めて、被害者の不安を煽り、金銭を要求する
    - 攻撃者から被害者に金銭を要求する電話を掛け、その後に弁護士等を装って和解を求める旨のメールを送信して騙す

メールや SMS 等を使った脅迫・詐欺の手口による金銭要求

～人生いろいろ。詐欺の手口もいろいろ～

- **攻撃手口**
  - **SNS等で親交を深めた後に金銭を要求する**
    - SNSを利用して有名人を装い、親交を深めた後に投資の勧誘をして、詐欺を行う
    - 海外の異性を装い、SNS上で交際を持ち掛け、親密になった上で、被害者の恋愛感情を利用し、様々な名目で金銭を要求したり、投資の勧誘をしたりする（ロマンス詐欺）

メールや SMS 等を使った脅迫・詐欺の手口による金銭要求

～人生いろいろ。詐欺の手口もいろいろ～

- **2023年の事例/傾向①**
  - **大学のメールアドレス宛に脅迫メールを送信**
    - 2023 年 5 月、電気通信大学は、学内のメールアドレスにセクストーションを目的とした複数の迷惑メールが届いていることの注意喚起を行った
    - 迷惑メールには、「私のソフトウェアはあなたのカメラとマイクも制御しました。あなたを主演とした価値ある卑猥なビデオをいくつか作成しました」等の記載があった
    - 金銭を支払わなければそれをWebサイト上で公開するなどといった脅迫の文面が記載されていた

【出典】【2023/5/25 6:50】ばらまき型脅迫詐欺メール（性的脅迫メール）に関する注意喚起（国立大学法人 電気通信大学情報基盤センター）
https://www.cc.uec.ac.jp/blogs/news/2023/05/20230525scammail.html

- **2023年の事例/傾向②**
  - **支援金を受け取れると嘘のメールを送信**
    - 2023年1月、大阪の70代の男性に「もうすぐがんで死ぬため支援金として 9,000 万円を譲りたい」といったメールが届き、メッセージのやり取りが始まった
    - 男性は、支援金を受け取るための費用として、現金を振り込むことを繰り返し指示され、指定された口座に総額5,000万円あまりを振り込んだ
    - 警察は特殊詐欺事件として捜査をするとともに、現金がもらえるといった内容のメールは信憑性に欠けるため、すぐに相談するようにと注意を呼び掛けている

【出典】「もうすぐがんで死ぬ」メールで詐欺被害 警察が注意呼びかけ（NHK NEWS WEB）
https://www3.nhk.or.jp/news/html/20231110/k10014254201000.html

メールや SMS 等を使った脅迫・詐欺の手口による金銭要求

～人生いろいろ。詐欺の手口もいろいろ～

- **2023年の事例/傾向③**
  - **SNS を利用した投資詐欺が横行中**
    - 2023年12月、札幌市の女性が攻撃者の口座に総額約1億5,000万円を振り込むという事件が発生した
    - 女性はSNSで知り合った男から暗号資産の投資を持ち掛けられ振り込みを行っていた
    - 女性が現金を引き出そうとすると、「引き出すのにも金がかかる」と男に言われ、騙されたことに気付き警察に相談して事件が発覚した

【出典】 “約1億5000万円の詐欺”2023年北海道内最高被害額 SNSで知り合った男「収益利率20%を超える」札幌の女性『暗号通貨の投資話』でだまされる（北海道ニュースUHB）
https://nordot.app/1106921703885538061?c=900039697665425408

♦ 対策

• インターネット利用者

【被害の予防】

- 受信した脅迫、詐欺メールは無視する
- 多要素認証の設定を有効にする
- メールに記載されている番号に電話を掛けない
  - どうしても相談したい場合はメールに記載された連絡先ではなく、自身で調べた正規の連絡先に連絡する

♦ 対策

• インターネット利用者

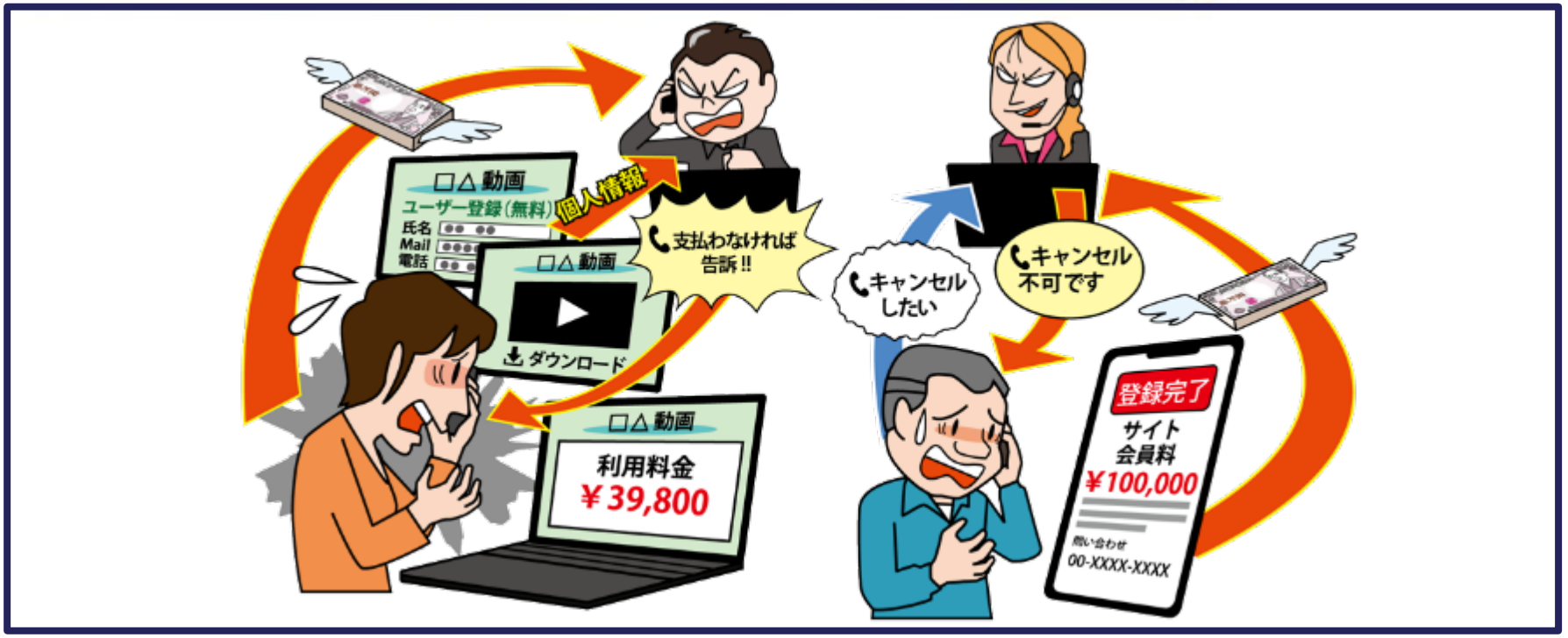
【被害を受けた後の対応】

- クレジットカードの利用停止手続きをする
  ※不審なWebサイト等にクレジットカード情報を入力してしまった場合
- パスワードを変更する
  - 他のサービスで同じパスワードを使っていた場合は同様に対応する
  - 脅迫・詐欺メールに記載されたパスワードが自分のものと一致している場合、どこかからパスワードが漏えいしているおそれがある
- 都道府県警察本部のサイバー犯罪相談窓口に相談する※1

【参考】※１都道府県警察本部のサイバー犯罪相談窓口
https://www.npa.go.jp/bureau/cyber/soudan.html

ワンクリック請求等の不当請求による金銭被害

～不当請求は無視！不安な場合は周りに相談を～



- PCやスマートフォンに請求画面が表示され、金銭を不当に請求される被害が依然として発生している
- 複数回クリックさせることで、請求の正当性を主張するケースや、クリックをしなくても自動的に請求画面に転送されるケースも存在する（ゼロクリック詐欺）

ワンクリック請求等の不当請求による金銭被害

～不当請求は無視！不安な場合は周りに相談を～

IPA

- **攻撃手口**

・不当な請求表示させて不安を煽る、騙す

- **悪意あるWebサイトを閲覧させる**
  - アダルトサイト等の年齢確認や動画再生ボタンをクリックすることにより、会員登録完了の請求画面が表示される
  - 金銭の支払い義務があるように見せ、不当に金銭を請求する
- **メールに記載されたリンクをクリックさせる**
  - 届いたメール等に記載されているリンクをクリックさせることでWebサイトで入会完了画面が表示され、高額な入会金を請求する

ワンクリック請求等の不当請求による金銭被害

～不当請求は無視！不安な場合は周りに相談を～

- **攻撃手口**
  - **不正プログラム・アプリをインストールさせる**
    - 無料動画ダウンロード等と偽り、インストールを促す
    - 請求画面を閉じたり、端末を再起動したりしても再び請求画面が表示されることもある
  - **電話をかけるように誘導する**
    - 請求画面にお問い合わせ先の電話番号を表示し、退会を焦る被害者に電話をかけさせるように誘導する
    - 電話をかけても解約はできず支払いを迫られたり、支払い免除のためと称して個人情報を聞き出そうとする場合がある

ワンクリック請求等の不当請求による金銭被害

～不当請求は無視！不安な場合は周りに相談を～

- **2023年の事例/傾向①**
  - **不当請求で約1,000万円を騙し取られる**
    - 2023年10月、アダルトサイトの登録料等の名目で金銭を騙し取る特殊詐欺事件が発生した
    - 被害者がアダルトサイトを閲覧中、「24時間以内にお金を支払ってください」という内容のメッセージが画面に表示された
    - サイト上で退会を選択したものの翌日にサイトの関係者を名乗る人物から電話があり、登録料等として金銭の支払いを請求された
    - 請求に応じて電子マネーの送金や現金の振り込みを計10回行い、総額約1,000万円を騙し取られた

【出典】 アダルトサイト閲覧…「登録料」要求され1000万円だまし取られる 静岡・伊豆市の男性が特殊詐欺被害（gooニュース）
https://news.goo.ne.jp/article/tvsdt/region/tvsdt-20231222028695 94.html

ワンクリック請求等の不当請求による金銭被害

～不当請求は無視！不安な場合は周りに相談を～

- **2023年の事例/傾向②**
  - **継続して多い不当請求の相談**
    - 国民生活センターによると、アダルト情報サイトに関する相談が2023年1月～5月に786件（2022年同期1,384件）寄せられた
    - 相談内容は、「無料だと思って『18歳以上』をクリックしたら、いきなり会員登録となり料金請求画面になった」等、ワンクリック請求等の不当請求に関わるものが多く見られた
    - 同様の相談の総件数は2021年が12,942件、2022年が10,172件となっており、減少傾向ではあるものの、依然として多くの相談が寄せられていた

【出典】 各種相談の件数や傾向 > アダルト情報サイト（独立行政法人国民生活センター）
https://www.kokusen.go.jp/soudan_topics/data/adultsite.html

ワンクリック請求等の不当請求による金銭被害

～不当請求は無視！不安な場合は周りに相談を～

- **対策**
  - **インターネット利用者**

【被害の予防】

- 不当な請求を安易に信用しない
- 不当な請求には応じない、連絡しない
- 請求画面が表示されたらブラウザを終了する
- SMSやメールで受信したURLや、SNSの投稿内のURLを安易にクリックしない
- パスワード管理ソフトを利用する
- 多要素認証の設定を有効にする
- アクセスするWebサイトを確認する
- 不正プログラムをダウンロードしない

【参考】 ワンクリック請求の手口に引き続き注意（IPA）
https://www.ipa.go.jp/security/anshin/attention/2022/mgdayori20220706.html

ワンクリック請求等の不当請求による金銭被害

～不当請求は無視！不安な場合は周りに相談を～

- **対策**
  - **インターネット利用者**

【被害を受けた後の対応】

- 端末を初期化する（不正プログラムをダウンロードしてしまった場合）
- 公的機関に相談する※1

【参考】※1 IPA（安心相談窓口）
https://www.ipa.go.jp/security/anshin/about.html
※1 国民生活センター／消費生活センター
https://www.kokusen.go.jp/map/
※1 都道府県警察本部のサイバー犯罪相談窓口
https://www.npa.go.jp/bureau/cyber/soudan.html

まとめ

情報セキュリティ対策の基本を実践

- 様々な脅威があるが、基本的な対策の重要性は長年変わらない

各脅威の手口の把握および対策を実践

- 新たな機器やサービスの普及に伴いインターネット利用における脅威なども変化する
- 公的機関の注意喚起やニュースなどから脅威の手口に関する情報を収集し、変化する手口を理解して適切な対策を実践することが重要

まとめ

共通対策を実践

- 対策の種類単位で見ると、複数の脅威に有効な対策がある
- 下記の「共通対策」を「情報セキュリティ対策の基本」と共に実施することでより効率的に広範囲な対策を進めることが可能

※情報セキュリティ10大脅威 2024のページで共通対策の詳細な解説資料を公開中

共通対策
パスワードを適切に運用する
情報リテラシー、モラルを向上させる
メールの添付ファイル開封や、メールやSMSのリンク、URLのクリックを安易にしない
適切な報告/連絡/相談を行う
インシデント体制の整備し、対応を行う
サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う
適切なバックアップ運用を行う

詳細な資料のダウンロード

- 情報セキュリティ10大脅威　2024

  本資料に関する詳細な内容はWebサイトをご覧ください

https://www.ipa.go.jp/security/10threats/10threats2024.html

※こちらのQRコードをスマートフォンのQRコードリーダーアプリで読み込むことでもアクセスできます