IPA Better Life with IT

情報セキュリティ10大脅威　2023

［個人編］

独立行政法人情報処理推進機構（IPA）
セキュリティセンター
2023年3月

「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 2023 脅威ランキング

IPA

「個人」向け脅威	順位	「組織」向け脅威
フィッシングによる個人情報等の詐取	1	ランサムウェアによる被害
ネット上の誹謗・中傷・デマ	2	サプライチェーンの弱点を悪用した攻撃
メールやSMS等を使った 脅迫・詐欺の手口による金銭要求	3	標的型攻撃による機密情報の窃取
クレジットカード情報の不正利用	4	内部不正による情報漏えい
スマホ決済の不正利用	5	テレワーク等の ニューノーマルな働き方を狙った攻撃
不正アプリによる スマートフォン利用者への被害	6	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）
偽警告によるインターネット詐欺	7	ビジネスメール詐欺による金銭被害
インターネット上のサービスからの 個人情報の窃取	8	脆弱性対策情報の公開に伴う悪用増加
インターネット上のサービスへの 不正ログイン	9	不注意による情報漏えい等の被害
ワンクリック請求等の 不当請求による金銭被害	10	犯罪のビジネス化 （アンダーグラウンドサービス）

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」は常に意識

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

情報セキュリティ対策の基本＋α

- 昨今はクラウドサービスの利用も一般的になってきている
- クラウドサービスを利用を想定した＋αの対策を行い備える必要がある

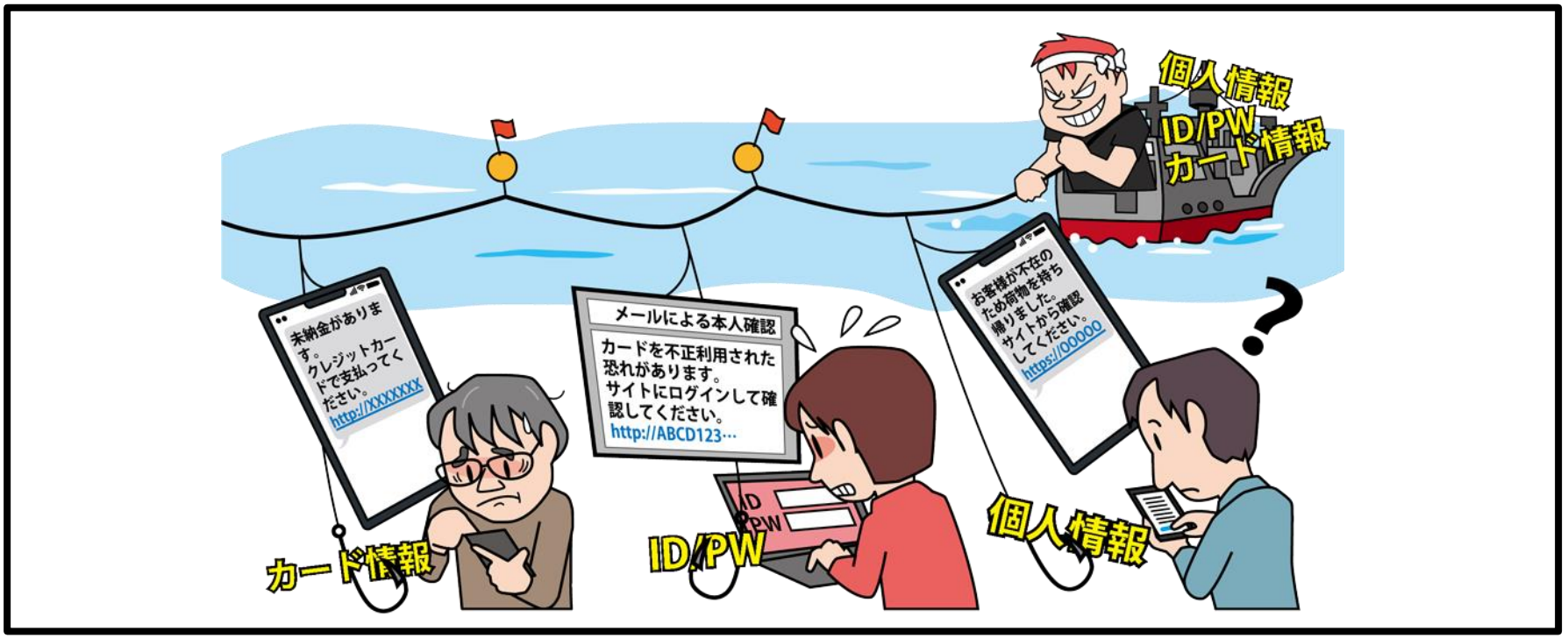
備える対象	情報セキュリティ対策の基本＋α	目的
インシデント全般	責任範囲の明確化（理解）	インシデント発生時に誰（どの組織）が対応する責任があるのかを明確化（理解）する
クラウドの停止	代替案の準備	業務が停止しないように代替策を準備する
クラウドの仕様変更	設定の見直し	仕様変更により意図せず変更された設定を適切な設定に直す（設定不備による情報漏えいや攻撃への悪用を防止する。）

情報セキュリティ10大脅威 2023
個人編　各脅威の解説

※以降の各脅威の対策では、前項の「情報セキュリティ対策の基本」は実施されている前提とし、記載には含めていません。

【1位】フィッシングによる個人情報等の詐取

～不安を煽る巧妙なフィッシングメールに注意！～



- 金融機関や有名企業を装った**偽のウェブサイト**（フィッシングサイト）へ利用者を誘導
- 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

【1位】フィッシングによる個人情報等の詐取

～不安を煽る巧妙なフィッシングメールに注意！～

● 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ウェブサイトを**模倣**したフィッシングサイトを用意
- 公的機関や有名企業を**装ったメールやSNS、 SMS**（スミッシング）を不特定多数に送信し、フィッシングサイトに誘導
- フィッシングサイトで**利用者が入力した情報を詐取**

■ 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**偽の広告を表示**させ、フィッシングサイトへ誘導

【1位】フィッシングによる個人情報等の詐取

～不安を煽る巧妙なフィッシングメールに注意！～

● 2022年の事例/傾向①

■ 過去の本物の内容を模したフィッシング（※1）

・2022年3月、JR東日本が同社のチケット予約サービス「えきねっと」を騙った不審メールを確認したとして注意喚起

・不審メールは、過去に同サービスが発信していた「【重要】アカウントの自動退会処理について」という**文章を模していた**

・「2年以上サービスにログインしていないと自動退会になる」として、**メール内のリンクからログインを促す**内容

・リンクからアクセスすると、偽のウェブサイトが表示され、個人情報の入力を求められる。**入力するとその情報が盗まれる。**

【出典】

※1 「これ詐欺だったの？」――「えきねっと」をかたるメール、手口の巧妙さが話題に “自動退会処理”に注意（ITmedia NEWS）
https://www.itmedia.co.jp/news/articles/2203/07/news095.html

【1位】フィッシングによる個人情報等の詐取

～不安を煽る巧妙なフィッシングメールに注意！～

● 2022年の事例/傾向②

■「国税庁」を騙ったフィッシング（※1,2）

・2022年8月、国税庁が、同庁を騙った不審メールやSMSが確認されているとして**注意喚起**

・不審メールはe-Tax利用者に**実際に送られたメールに似通っていたり**、税金が未払いであると**不安を煽ったり**する内容

・メールやSMSからアクセスした不審サイトでは、未払い税金の納付のため、個人情報やクレジットカード情報の入力を求められる。**入力してしまうとその情報が盗まれる**。

【出典】

※1　不審なショートメッセージやメールにご注意ください（国税庁）
https://www.e-tax.nta.go.jp/topics/topics_20220815.htm

※2　国税庁をかたるフィッシング（2022/09/20）（フィッシング対策協議会）
https://www.antiphishing.jp/news/alert/nta_20220920.html

【1位】フィッシングによる個人情報等の詐取

～不安を煽る巧妙なフィッシングメールに注意！～

● 2022年の事例/傾向③

■ 報告件数は依然として増加傾向 (※1,2)

・フィッシング対策協議会の報告書によると、2022年のフィッシング報告件数は97万件(前年は53万件)と**2倍弱に増加**

・フィッシングサイトへの誘導に**QRコードを用いる手口**も確認

・フィッシングメールやSMSの内容はクレジットカードの利用確認や、宅配業者の不在通知、Amazon等のショッピングサイト、通信事業者を**装ったものを引き続き確認**

【出典】
※1 2021/12 フィッシング報告状況(フィッシング対策協議会)
https://www.antiphishing.jp/report/monthly/202112.html
※2 2022/12 フィッシング報告状況(フィッシング対策協議会)
https://www.antiphishing.jp/report/monthly/202212.html

【1位】フィッシングによる個人情報等の詐取

～不安を煽る巧妙なフィッシングメールに注意！～

● 対策

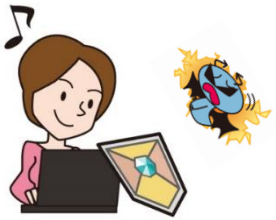
■ インターネット利用者

・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**

－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



・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確認

－利用しているサービスの**ログイン履歴の確認**

－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**

【1位】フィッシングによる個人情報等の詐取

～不安を煽る巧妙なフィッシングメールに注意！～

対策

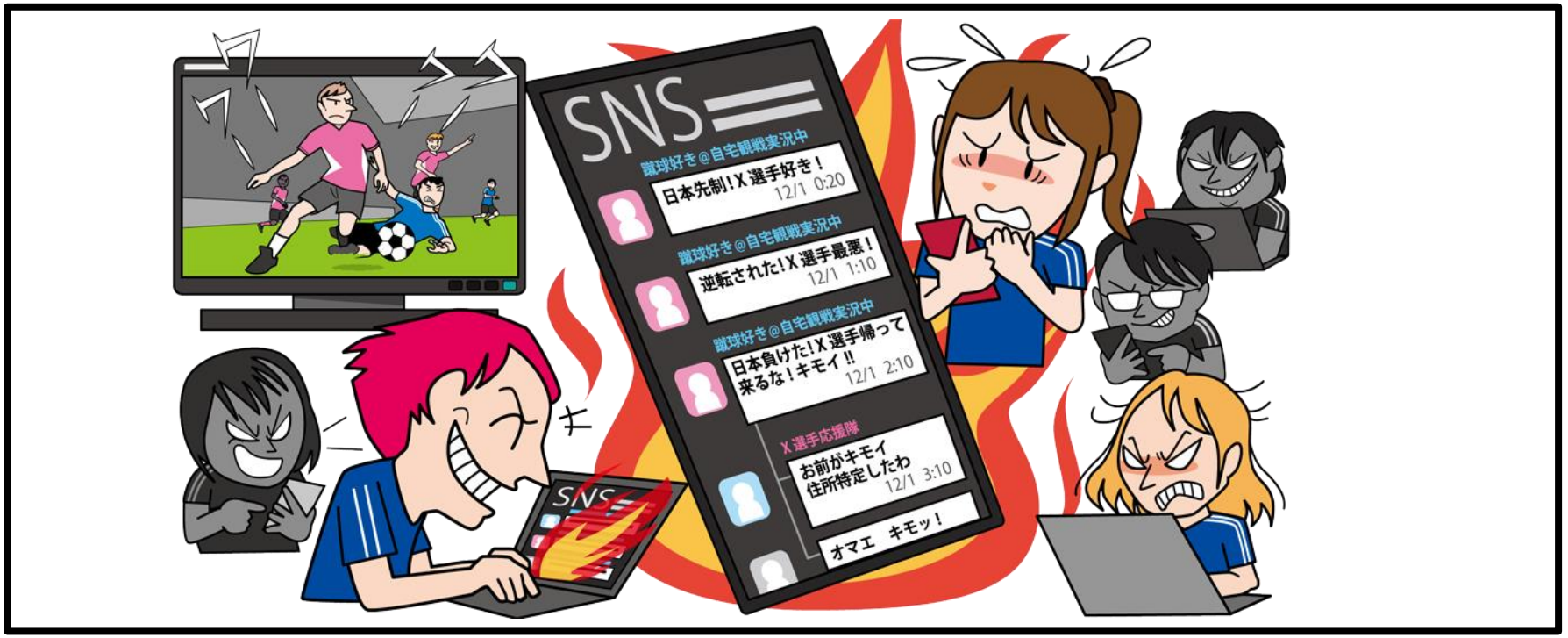
インターネット利用者

・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（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）
- サービス運営者（コールセンター等）へ**連絡**する
- 信頼できる機関に**相談**する

【2位】ネット上の誹謗・中傷・デマ

～昨日の友は今日の敵？熱くなりすぎず冷静な対応を！～



- 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**

【2位】ネット上の誹謗・中傷・デマ

～昨日の友は今日の敵？熱くなりすぎず冷静な対応を！～

● 要因

・匿名性の悪用、第三者による不用意な拡散

■ 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

（警察が調査すれば身元を**特定できる場合が多い**）

■ 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

・さらに別の第三者の真偽不明な情報と紐づけて拡散することで、その第三者にも誹謗中傷が広がる

【2位】ネット上の誹謗・中傷・デマ

～昨日の友は今日の敵？熱くなりすぎず冷静な対応を！～

IPA

- 2022年の事例/傾向①
  - 「教材に反ワクチンのチラシ封入」のデマ拡散 (※1,2)
    - 2022年3月、「ベネッセの小学1年生用教材に反ワクチンを呼び掛けるチラシが入っていた」という**デマの投稿がTwitter上で拡散された**
    - 投稿はチラシの画像付きであったが「デマなのでは？」と疑う者もいた
    - しかしTwitter上で話題になったため、ベネッセに**問合せ**が寄せられ、本来不要であった対応をする事態となった

【出典】

※1 ベネッセに風評被害 「教材に反ワクチンのチラシを封入」デマ対応に追われる（ITmedia NEWS）
https://www.itmedia.co.jp/news/articles/2203/23/news085.html

※2 反ワクチンチラシ「チャレンジに入ってた」デマ投稿が話題に、偽計業務妨害罪の可能性も（弁護士ドットコムニュース）
https://www.bengo4.com/c_23/n_14277/

【2位】ネット上の誹謗・中傷・デマ

～昨日の友は今日の敵？熱くなりすぎず冷静な対応を！～

IPA

- 2022の事例/傾向②
  - デマの投稿者に名誉棄損等で有罪判決（※1,2）
    - ・コンビニ店長の写真を添付し、「私コロナ感染者と近寄って来た」「この店には絶対行かないで」とSNSにデマを投稿した女に有罪判決（懲役8月、執行猶予3年）
    - ・Twitter等に「煽り運転事件で起訴された被告と関わりがある」と同姓の他人に関するデマを投稿し、有罪判決
    - ・被害者が経営する会社が休業する事態になり、社会的評価を低下させたことを裁判所が認めた（231万円の損害賠償）

【出典】

※1　SNSデマ投稿の女に有罪判決 「コンビニ店長がコロナ感染」名誉棄損（京都新聞）
https://www.kyoto-np.co.jp/articles/-/901904

※2　デマ投稿5人の賠償増額　東名あおり事故　福岡高裁（産経新聞）
https://www.sankei.com/article/20221027-ODQDEYMWLVMNNOCAOTI72GJJEQ/

【2位】ネット上の誹謗・中傷・デマ

～昨日の友は今日の敵？熱くなりすぎず冷静な対応を！～

対策

発信者

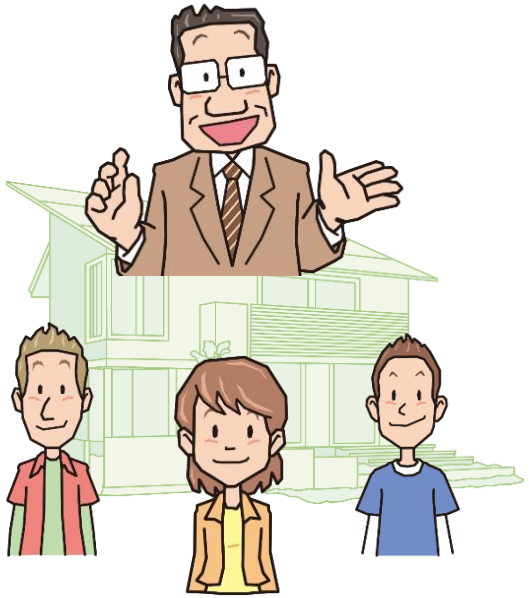
・情報モラルや情報リテラシーの向上、法令遵守の意識の向上

- 誹謗・中傷や公序良俗に反する投稿をしない
- 投稿前に内容を再確認
- 匿名性がある場合でも発言には責任を持つ

家庭、教育機関

・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



【2位】ネット上の誹謗・中傷・デマ

～昨日の友は今日の敵？熱くなりすぎず冷静な対応を！～

● 対策

■ 閲覧者

・情報モラルや情報リテラシーおよび法令遵守の意識の向上

－**情報の信頼性の確認**

■ 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

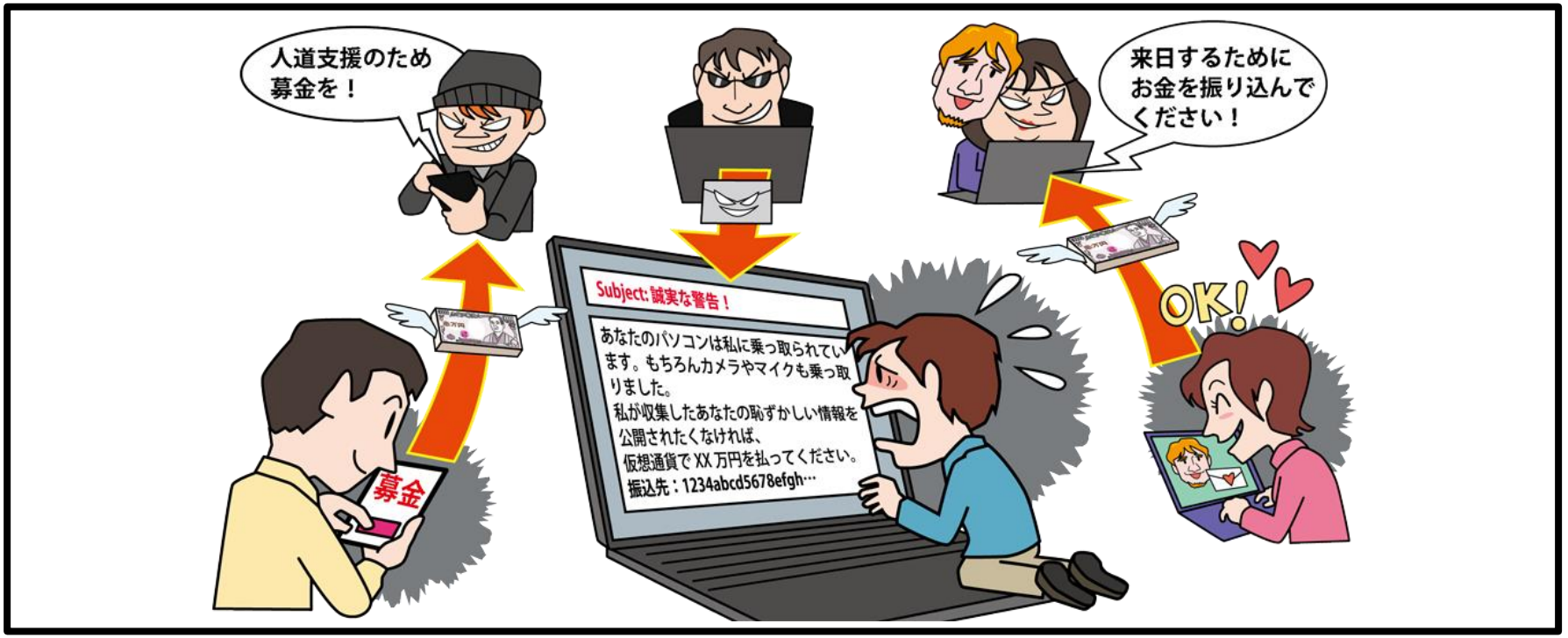
－**一人で抱え込まず**、信頼できる周囲の人や公的相談機関へ**相談**する

－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

【3位】メールやSMS等を使った脅迫・詐欺の手口による金銭要求
～人の心の弱みに付け込む詐欺に注意～



- 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、金銭を要求
- 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受信者が金銭を支払ってしまう

【3位】メールやSMS等を使った脅迫・詐欺の手口による金銭要求
～人の心の弱みに付け込む詐欺に注意～

● 攻撃手口

・脅し、騙しのメールを送り付け金銭を要求

- **メール等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く
  - ・金銭を要求する（暗号資産での支払いを要求する場合も）
- **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する

【3位】メールやSMS等を使った脅迫・詐欺の手口による金銭要求
～人の心の弱みに付け込む詐欺に注意～

IPA

- **攻撃手口**

・脅し、騙しのメールを送り付け金銭を要求

- **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、本当にメール受信者のPCを**ハッキングしているかのように装い**、脅しの内容を信じさせようとする
- **公的機関を装う**
  - ・**信頼できる組織の発信を装い**信憑性、緊急性を高めて騙す

【3位】メールやSMS等を使った脅迫・詐欺の手口による金銭要求
～人の心の弱みに付け込む詐欺に注意～

IPA

- **攻撃手口**

・脅し、騙しのメールを送り付け金銭を要求

- **メールや電話を併用して信憑性を高める**
  - ・メール内の電話番号宛に被害者が**電話を掛けるよう誘導**する
  - ・電話を使ってさらに脅迫を行う（弁護士等を騙る場合もある）
- **SNS等で親交を深めた後に金銭を要求する**
  - ・SNS等で**海外の異性を装い**オンライン上で交際を持ち掛ける
  - ・被害者の恋愛感情を利用し、様々な名目で金銭を要求する（ロマンス詐欺）

【3位】メールやSMS等を使った脅迫・詐欺の手口による金銭要求
～人の心の弱みに付け込む詐欺に注意～

- 2022年の事例/傾向①
  - 大学内のメールアドレス宛に脅迫メール送信（※1）
    - 2022年8月、電気通信大学が学内に複数の迷惑メールが届いていることを確認し、学内に注意喚起を実施
    - 迷惑メールには「デバイスを**ハッキングした**」「あなたの**恥ずかしい場面を録画**した」「暗号資産を**送金すれば内容を削除**する」等が記載されていた

【出典】
※1 【2022/8/11 9:20】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/2022/08/20220811scammail.html

【3位】メールやSMS等を使った脅迫・詐欺の手口による金銭要求
～人の心の弱みに付け込む詐欺に注意～

- 2022年の事例/傾向②
  - 巣ごもりでロマンス詐欺が増加傾向 (※1,2)
    - 2022年10月、滋賀県東近江署は、**ロマンス詐欺により女性が約440万円を騙し取られた**と発表
    - 被害者は、SNSで外国人宇宙飛行士を名乗る男とやり取りを交わし、**親密な間柄**になった。その後、「地球に戻るためのロケット費用」等の名目で**金銭を要求された**
    - 支払ってしまった後、不審に思い警察署に相談して**詐欺と発覚**

【出典】
※1 自称ロシア人宇宙飛行士に440万円だまし取られる ロマンス詐欺か（朝日新聞）
https://www.asahi.com/articles/ASQB95TH6QB7PTJB00J.html
※2 国際ロマンス詐欺増加、外国人名乗りSNSで甘言（中日新聞）
https://www.chunichi.co.jp/article/573151?rct=shiga

【3位】メールやSMS等を使った脅迫・詐欺の手口による金銭要求
～人の心の弱みに付け込む詐欺に注意～

- **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）
      - －受信した脅迫・詐欺メールは**無視する**
        ※詐欺メールに自分のパスワード等が記載されていても
        実際にハッキングされていることを示すものではない
      - －メールに記載されている番号に**電話をしない**
        ※受信した脅迫や架空請求のメールについて専門機関に相談したい場合は、その**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電話番号やメールアドレスに連絡する
      - －メールで要求された**支払いには応じない**
      - －多要素認証の設定を有効にする

【3位】メールやSMS等を使った脅迫・詐欺の手口による金銭要求
～人の心の弱みに付け込む詐欺に注意～

- **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
        （不審なウェブ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）
        ※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
      - –警察に**相談**する

【4位】クレジットカード情報の不正利用
～狙われているのは組織、しかし個人でも対策が必要！～

- **ウイルス感染やフィッシング詐欺、改ざんされたウェブサイト**によりクレジットカード情報を詐取される
- クレジットカード情報をショッピングサイト等で不正利用される

【4位】クレジットカード情報の不正利用
～狙われているのは組織、しかし個人でも対策が必要！～

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**偽のウェブサイト**（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**正規ウェブサイト上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

・正規のウェブサイト上に偽画面があるため、気付くことが困難

【4位】クレジットカード情報の不正利用
～狙われているのは組織、しかし個人でも対策が必要！～

- **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**
  - ・悪意のあるプログラムを含むファイルを作成し**メールに添付**
  - ・メール受信者が**このファイルを開くとウイルス感染**のおそれ
  - ・**ウイルス感染した端末上で決済を行う**とクレジットカード情報を窃取される

【4位】クレジットカード情報の不正利用
～狙われているのは組織、しかし個人でも対策が必要！～

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

【4位】クレジットカード情報の不正利用
～狙われているのは組織、しかし個人でも対策が必要！～

- 2022年の事例/傾向①
  - オンラインショップでクレジットカード情報流出（※1）
    - 2022年5月、machattが運営するオンラインショップにおいて、16,093件のクレジットカード情報が流出
    - 一部は不正利用されたおそれがあった
    - 原因は、攻撃者にシステムの脆弱性を悪用され、ペイメントアプリケーションを改ざんされていたことであった
    - 同社は身に覚えのない請求項目がないかを確認し、ある場合はクレジットカード会社に問い合わせるよう呼びかけた

【出典】
※1 お知らせ（株式会社machatt）
https://machatt.jp/support/information/20220518.html

【4位】クレジットカード情報の不正利用
～狙われているのは組織、しかし個人でも対策が必要！～

- 2022年の事例/傾向②
  - クレジットカードの情報の不正利用被害額が年々増加傾向（※1）
    - 2022年1月～9月の被害額は309.2億円となった。2021年同期間の被害額236.9億円と比較して、**約30%増加**
    - 全体の被害額291.3億円の**94.2%が番号盗用被害**によるものであった。

【出典】
※1 クレジットカード不正利用被害の集計結果について（一般社会法人日本クレジット協会）
https://www.j-credit.or.jp/download/news20220930c1.pdf

【4位】クレジットカード情報の不正利用
～狙われているのは組織、しかし個人でも対策が必要！～

- 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）の利用
      - –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**
      - –プリペイドカードの利用を検討
        ※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**

【4位】クレジットカード情報の不正利用
～狙われているのは組織、しかし個人でも対策が必要！～

- 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の**定期的な確認**
      - **サービス利用状況の通知機能**等の利用
    - 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**連絡**する
      - 警察へ**被害届を提出**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）

【5位】スマホ決済の不正利用

～フィッシングメールに注意、知らないうちにあなたのスマホ決済が悪用されているかも～

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

【5位】スマホ決済の不正利用

～フィッシングメールに注意、知らないうちにあなたのスマホ決済が悪用されているかも～

● 攻撃手口

・不正アクセスによるアカウントの乗っ取り

■ パスワードリスト攻撃による不正ログイン

- 過去に漏えいしたパスワードをリスト化し、不正ログインに悪用
- 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、パスワードのみで不正ログインされるおそれがある

【5位】スマホ決済の不正利用

～フィッシングメールに注意、知らないうちにあなたのスマホ決済が悪用されているかも～

● 攻撃手口

・スマホ決済サービスの不備を悪用する

■ 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等を行う

・当該サービスだけでなく、**連携している他のサービスのセキュリティ上の不備**も悪用される場合がある

・多要素認証やサービス利用状況の通知等のサービスが提供されていない場合、攻撃者に悪用されやすい

【5位】スマホ決済の不正利用

～フィッシングメールに注意、知らないうちにあなたのスマホ決済が悪用されているかも～

● 2022年の事例/傾向①

■ メルペイを不正利用 (※1)

・2022年5月、警視庁は電子決済サービス「メルペイ」を悪用し、美容品を詐取したとして、中国籍の複数の女を**逮捕**

・被疑者は、**他人の名義で登録されたメルペイ**の決済用バーコード画像を示し、洗顔フォームや美容液等、55点（約50万円）を不正に購入した疑い

・中国に住む仲間が**フィッシングメールで盗んだIDとパスワード**でメルペイに不正接続し、決済用バーコードの画像を被疑者に送っていた

【出典】

※1 他人のメルペイに接続、中国人グループが2300万円不正購入か…中国で転売（読売新聞オンライン）
https://www.yomiuri.co.jp/national/20220526-OYT1T50124/

【5位】スマホ決済の不正利用

～フィッシングメールに注意、知らないうちにあなたのスマホ決済が悪用されているかも～

- 2022年の事例/傾向②
  - au PAYを不正利用 (※1)
    - 2022年9月、京都府警は**他人名義のアカウントで商品を不正に購入**したとして複数の中国人留学生を逮捕
    - 被害者にauを装った**偽メールを送り、偽サイトに接続させ、入力させたIDとパスワードを窃取**
    - 偽メールでは「auでお支払いしている継続利用サービスを更新する必要があります」と記載して**被害者を騙していた**
    - 京都府警に「au PAY」の不正利用に関する相談が相次ぎ、202件に上った

【出典】

※1 「au PAY」アカウント不正使用で詐欺の罪 被告無罪主張(関西 NEWS WEB)
https://www3.nhk.or.jp/kansai-news/20220916/2000066361.html

【5位】スマホ決済の不正利用

～フィッシングメールに注意、知らないうちにあなたのスマホ決済が悪用されているかも～

● 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
- **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の利用
- **フィッシングに注意**
- 利用していないサービスからの退会
- スマートフォンの紛失対策
  （画面ロック等のセキュリティ対策を実施）

【5位】スマホ決済の不正利用

～フィッシングメールに注意、知らないうちにあなたのスマホ決済が悪用されているかも～

● 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
利用履歴の定期的な確認

－連携する銀行口座の**出金履歴の確認**

・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）

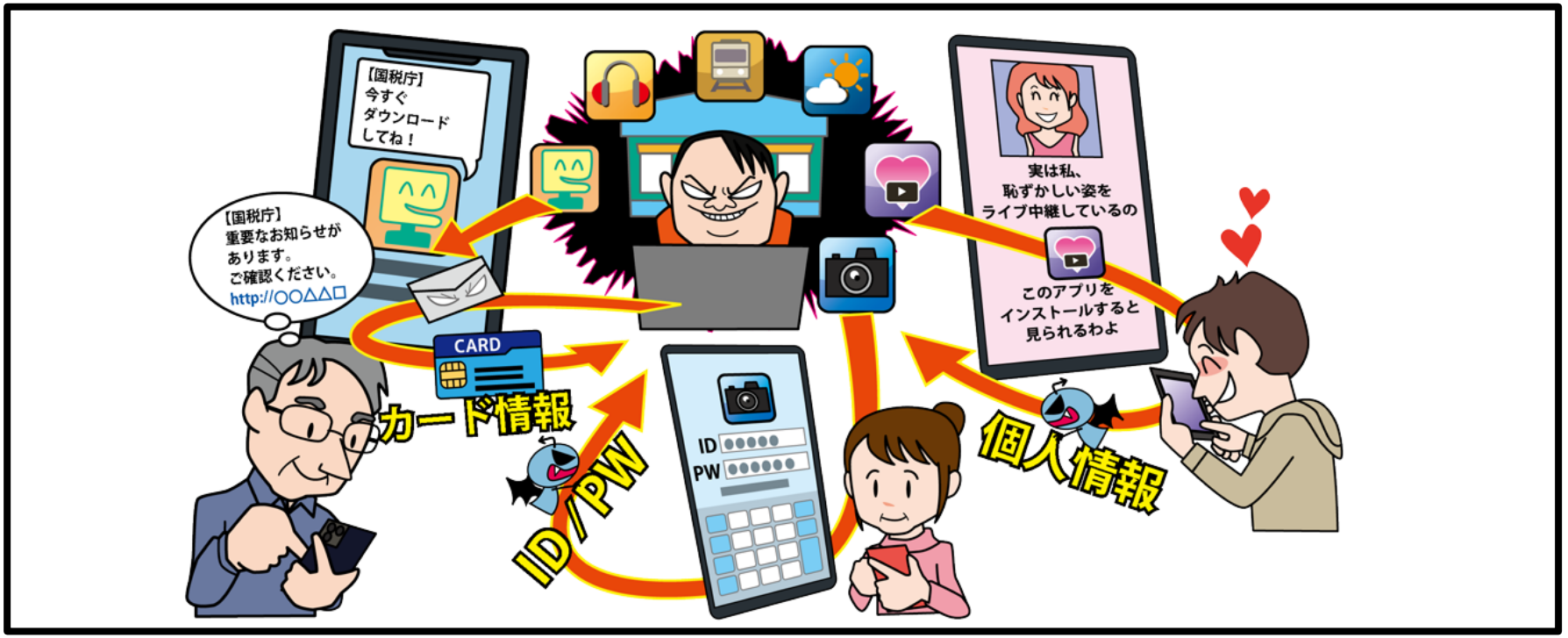
－サービス運営者（コールセンター等）へ**相談**する

－連携している金融機関へ**相談**する

－警察に**相談**する

【6位】不正アプリによるスマートフォン利用者への被害

～言葉巧みに不正アプリのインストールを誘導する手口に注意～



- 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が窃取される
- スマートフォンの一部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

【6位】不正アプリによるスマートフォン利用者への被害
～言葉巧みに不正アプリのインストールを誘導する手口に注意～

IPA

● 攻撃手口

・不正アプリをスマホ利用者にインストールさせる

■ 不正アプリのダウンロードサイトへ誘導

- 実在の企業を騙った**メールやSMS等で偽サイト**（不正アプリのダウンロードサイト）**へ誘導**
- **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**
- **正規のアプリと思い込ませ**、インストールさせる

【6位】不正アプリによるスマートフォン利用者への被害

～言葉巧みに不正アプリのインストールを誘導する手口に注意～

● 攻撃手口

・不正アプリをスマホ利用者に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の悪用例

・連絡先等の端末内の**重要な情報を窃取**される

・DDoS攻撃や悪意あるSMSの拡散等の**踏み台に利用**される

・端末の一部**機能**（録画、写真、録音など）**を不正に利用**される

・暗号資産の**マイニングに利用**される

【6位】不正アプリによるスマートフォン利用者への被害
～言葉巧みに不正アプリのインストールを誘導する手口に注意～

- 2022年の事例/傾向①
  - マッチングアプリで出会った相手を不正アプリのインストールへ誘導（※1）
    - マッチングアプリで知り合った異性に誘導され、**不正アプリをインストールしたことで連絡先情報等の窃取や、金銭を要求される等の脅迫を受けた**との相談が長崎県警に寄せられた
    - 「恥ずかしい姿をライブ中継している」「このアプリをインストールすると見ることができる」等の文言で**利用者の興味を引き**、不正アプリのインストールサイトへ**誘導**

【出典】
※1　国内で脅迫被害、マッチングアプリを装うモバイル不正アプリ（トレンドマイクロ株式会社）
https://www.trendmicro.com/ja_jp/research/22/c/malicious-app-disguised-dating-app.html

【6位】不正アプリによるスマートフォン利用者への被害
～言葉巧みに不正アプリのインストールを誘導する手口に注意～

- 2022年の事例/傾向②
  - 有名SNSの認証情報を狙った不正アプリ(※1)
    - 2022年10月、MetaはFacebookのログイン情報を盗み出す悪質なAndroidアプリ、iOSアプリを400件以上確認
    - 不正アプリは写真編集、カメラ、VPNサービス、ゲーム、広告管理など、利用者の興味を引くような物が多い
    - 不正アプリは利用者にFacebookアカウントでのログインを求め、入力させたIDやパスワードを窃取する
    - Facebookのアカウントが乗っ取られたり、個人情報を窃取されたりするおそれがある

【出典】
※1 「Facebookでログイン」でパスワード盗むアプリ、100万人以上被害(ITmedia)
https://www.itmedia.co.jp/news/articles/2210/08/news049.html

【6位】不正アプリによるスマートフォン利用者への被害
～言葉巧みに不正アプリのインストールを誘導する手口に注意～

- 2022年の事例/傾向③
  - 国税庁を騙り、不正アプリのインストールを誘導 (※1,2)
    - フィッシング対策協議会によると、2022年の8月と9月は**国税庁を騙るフィッシングの報告が多数**
    - SMSを使ったフィッシングでは、Android スマートフォンを利用している場合、**不正アプリのインストールに誘導される**ことがあり、注意を呼び掛けた

【出典】
※1 2022/08 フィッシング報告状況(フィッシング対策協議会)
https://www.antiphishing.jp/report/monthly/202208.html
※2 2022/09 フィッシング報告状況(フィッシング対策協議会)
https://www.antiphishing.jp/report/monthly/202209.html

【6位】不正アプリによるスマートフォン利用者への被害
～言葉巧みに不正アプリのインストールを誘導する手口に注意～

IPA

- **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**

※公式マーケットのアプリでも油断は禁物

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

–アプリインストール時の**アクセス権限の確認**

※アプリの機能に対して適切かどうか確認

–アプリインストールに関する設定に注意

※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**

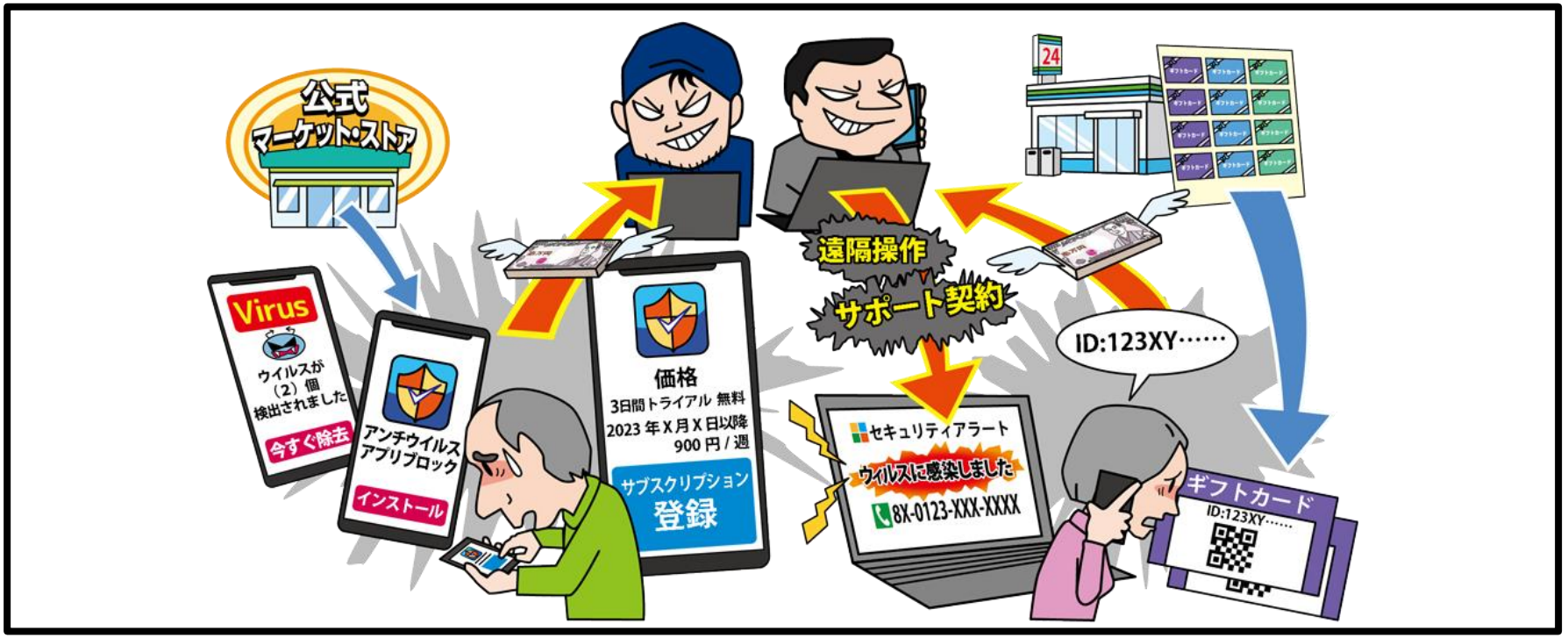
–利用しないアプリは**アンインストールする**

–セキュリティソフトを**インストールする**

【6位】不正アプリによるスマートフォン利用者への被害
～言葉巧みに不正アプリのインストールを誘導する手口に注意～

- **対策**
  - **スマートフォン利用者**
    - ・被害を受けた後の対応
      - –不正アプリの**アンインストール**
        ※アンインストールできない場合は**端末初期化**
      - –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。

【7位】偽警告によるインターネット詐欺
～警告画面の連絡先に電話しないで！！～



- 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しまい、警告の内容に従って**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**

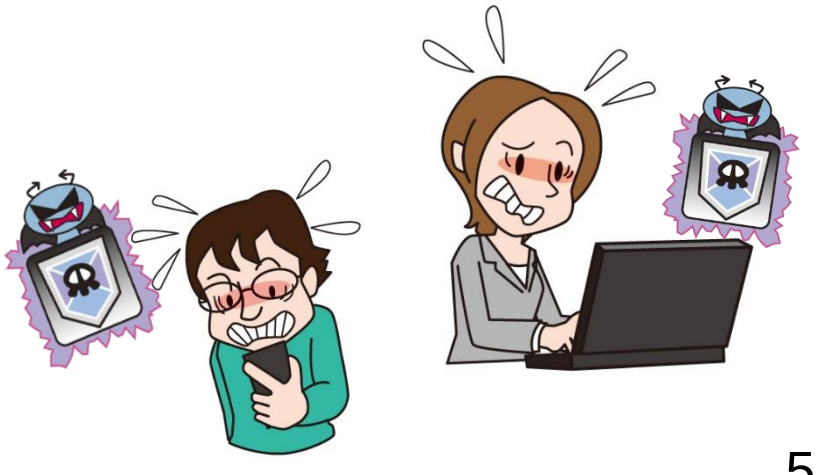
【7位】偽警告によるインターネット詐欺
～警告画面の連絡先に電話しないで！！～

IPA

- **攻撃手口**

・巧妙に作成した偽警告を表示して不安を煽る

- **巧妙に細工が施された偽の警告画面**
  - **実在の企業ロゴを使用**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**



【7位】偽警告によるインターネット詐欺
～警告画面の連絡先に電話しないで！！～

IPA

- **攻撃手口**

・偽警告に記載した誘導に従わせる

- **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**
- **サポート詐欺**
  - ・電話窓口の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、**有償のサポート契約へ誘導**
- **スマホアプリのインストールへ誘導**
  - ・スマホアプリのインストールへ誘導（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）が目的か

【7位】偽警告によるインターネット詐欺
～警告画面の連絡先に電話しないで！！～

- 2022年の事例/傾向①
  - PCを遠隔操作、通信販売で勝手に物品購入(※1)
    - 2022年8月、沖縄県警嘉手納署は**偽警告によるサポート詐欺が発生**したことを発表
    - 被害者のPCに「トロイの木馬スパイウェアに感染」等と記載された**偽警告の画面が音声アナウンスとともに表示**
    - 表示された連絡先に電話をかけてしまい、攻撃者にPC操作を誘導され、**PC を遠隔操作された**
    - 電子マネー等の**不正な購入**や、SNSの**不正利用をされた**

【出典】
※1「スパイウェアに感染」PCから偽の警告と音声が…遠隔操作で乗っ取る「サポート詐欺」 嘉手納署が注意喚起（琉球新報 DIGITAL）
https://ryukyushimpo.jp/news/entry-1563486.html

【7位】偽警告によるインターネット詐欺
～警告画面の連絡先に電話しないで！！～

- 2022年の事例/傾向②
  - 偽警告被害の相談件数が増加傾向 (※1,2,3)
    - 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**2021年と比較して大きく増加**

表 安心相談窓口への偽のセキュリティ警告に関する相談件数

	第1四半期	第2四半期	第3四半期	第4四半期
2021年	246件	232件	192件	420件
2022年	625件	435件	544件	761件

    - 2023年1月の相談件数は401件で、**月間の相談件数として過去最高件数**となった

【出典】
※1 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
※2 情報セキュリティ安心相談窓口の相談状況[2021年第4四半期(10月～12月)](IPA)
https://www.ipa.go.jp/security/anshin/reports/2021q4outline.html
※3 安心相談窓口だより「偽セキュリティ警告(サポート詐欺)の月間相談件数が過去最高に」(IPA)
https://www.ipa.go.jp/security/anshin/attention/2022/mgdayori20230228.html

【7位】偽警告によるインターネット詐欺
～警告画面の連絡先に電話しないで！！～

- 2022年の事例/傾向③
  - 偽警告によるサポート詐欺に対する支払い方法は**プリペイド型電子マネーが大半**（※1）
    - 国民生活センターによると、全国の消費生活センター等への**サポート詐欺に関する相談**がここ数年は**年間5,000件以上**
    - 有償サポートやセキュリティソフトの契約購入金額の平均金額は**年々高額化**
    - **支払い方法は、プリペイド型電子マネーが大半**を占め、2021年度においてはクレジットカードが428件、プリペイド型電子マネーが1,821件であった

【出典】
※1　そのセキュリティ警告画面・警告音は偽物です！「サポート詐欺」にご注意！！（独立行政法人国民生活センター）
https://www.kokusen.go.jp/news/data/n-20220224_2.html

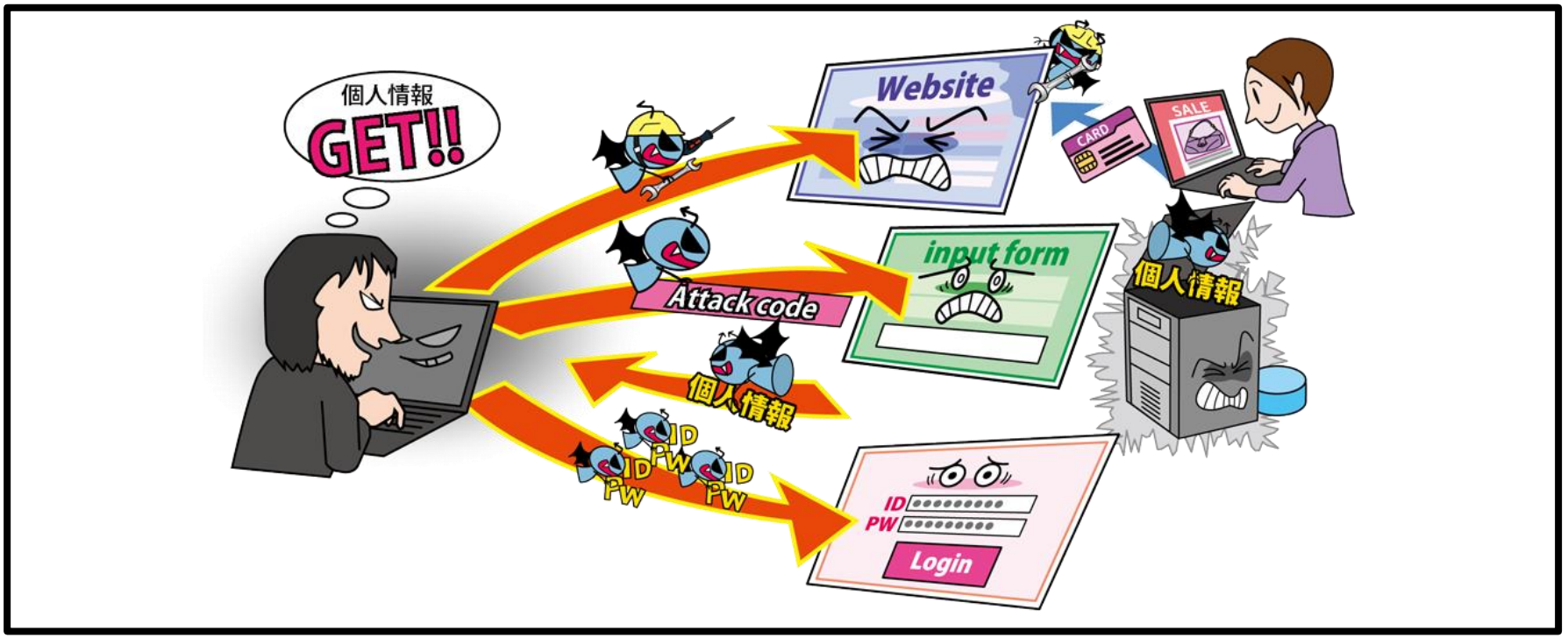
【7位】偽警告によるインターネット詐欺
～警告画面の連絡先に電話しないで！！～

- 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許可しない、契約に応じない、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**
      - －ブラウザの通知機能を**不用意に許可しない**
      - －不用意にカレンダーの照会を追加しない
      - －カレンダー内の不審な予定は削除する

【7位】偽警告によるインターネット詐欺
～警告画面の連絡先に電話しないで！！～

- **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**
        ※近くの消費生活センターへ**相談**する
      - –クレジットカード会社へ**相談**する

【8位】インターネット上のサービスからの個人情報の窃取
～オンラインショッピングの個人情報に注意！～



- 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**
- 窃取した情報が悪用され、**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

【8位】インターネット上のサービスからの個人情報の窃取
～オンラインショッピングの個人情報に注意！～

● 攻撃手口

・サービスの脆弱性や設定不備を悪用

■ 脆弱性等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、**脆弱性や設定の不備を悪用した攻撃**を行い、ウェブサイト内の**個人情報を窃取**する

■ 脆弱性等を悪用してウェブサイトを改ざん

・ウェブサイトの**脆弱性を悪用**して**ウェブサイトを改ざん**する

・利用者が改ざんに気付かずウェブサイト上に情報を**入力してしまうと、その情報を窃取される**

【8位】インターネット上のサービスからの個人情報の窃取
～オンラインショッピングの個人情報に注意！～

● 攻撃手口

・不正に入手した認証情報を悪用

- **他のサービス等から窃取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**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使いまわしていると被害に遭う可能性が高い

【8位】インターネット上のサービスからの個人情報の窃取
～オンラインショッピングの個人情報に注意！～

- 2022年の事例/傾向①
  - データベースに不正アクセスで個人情報窃取 (※1)
    - 2022年6月、SODAは同社が運営するショッピングサイトから、**個人情報（氏名や購入履歴等）約275万件が漏えい**したことを公表
    - 原因は、不正なリクエストに対する**データベースの処理の不備**であった
    - パスワードも漏洩していたが、ハッシュ化されていたため**複号が不可能な状態**であった

【出典】
※1　不正アクセスによるお客さま情報漏えいに関するお詫びとご報告（08.23追記）（株式会社SODA）
https://snkrdunk.com/information/130/

【8位】インターネット上のサービスからの個人情報の窃取
～オンラインショッピングの個人情報に注意！～

- 2022年の事例/傾向②
  - システム改ざんでクレジットカード情報窃取（※1）
    - 2022年8月、出光クレジットが運営する会員サイトにおいて、攻撃者にシステムを改ざんされる被害に遭ったこと公表
    - 改ざんされた状態のウェブページから新規登録または再登録を行った利用者のクレジットカード番号、有効期限、セキュリティコード、生年月日が漏えいしたおそれがある

【出典】
※1 【重要】個人情報漏洩に関するお詫びとお知らせについて（出光クレジット株式会社）
https://www.idemitsucard.com/important/information2210-02.html

【8位】インターネット上のサービスからの個人情報の窃取
～オンラインショッピングの個人情報に注意！～

- 2022年の事例/傾向③
  - ECサイトへのパスワードリスト攻撃による不正アクセスで会員情報を窃取される（※1）
    - 2022年7月、サンドラッグが運営するECサイトが不正アクセスされ、**約2万件の会員情報**（氏名・住所・電話番号・メールアドレスなど）**が窃取された可能性がある**ことを公表した
    - 攻撃は海外から行われ、**他社サービスから流出したと思われる**IDとパスワードを利用した**パスワードリスト攻撃**と推測されている

【出典】
※1 サンドラッグ e-shop 本店及びサンドラッグお客様サイトへの不正ログインについてのお詫びとお知らせ（株式会社サンドラッグ）
https://contents.xj-storage.jp/xcontents/99890/ee3648ea/747e/4df2/b2eb/b139a2d300bd/140120220712598541.pdf

【8位】インターネット上のサービスからの個人情報の窃取
～オンラインショッピングの個人情報に注意！～

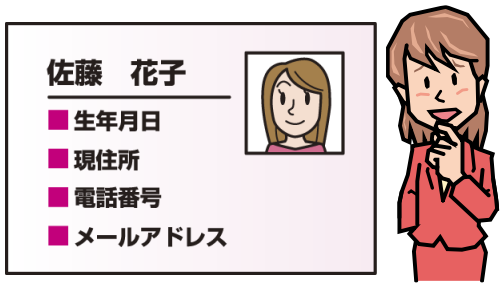
- **対策**
  - **インターネット利用者**
    - ・被害の予防
      - –サービス利用の**必要性を判断**し、**不要なサービスには登録しない**
      - –不要な**情報は安易に登録しない**
      - –利用しているサービスの**多要素認証の設定を有効**にする
      - –**利用していないサービスからの退会**
      - –**不正ログイン対策**を実施する

        例えば・・・

        ・パスワードは長く、複雑にして、使い回さない

        ・不審なウェブ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）

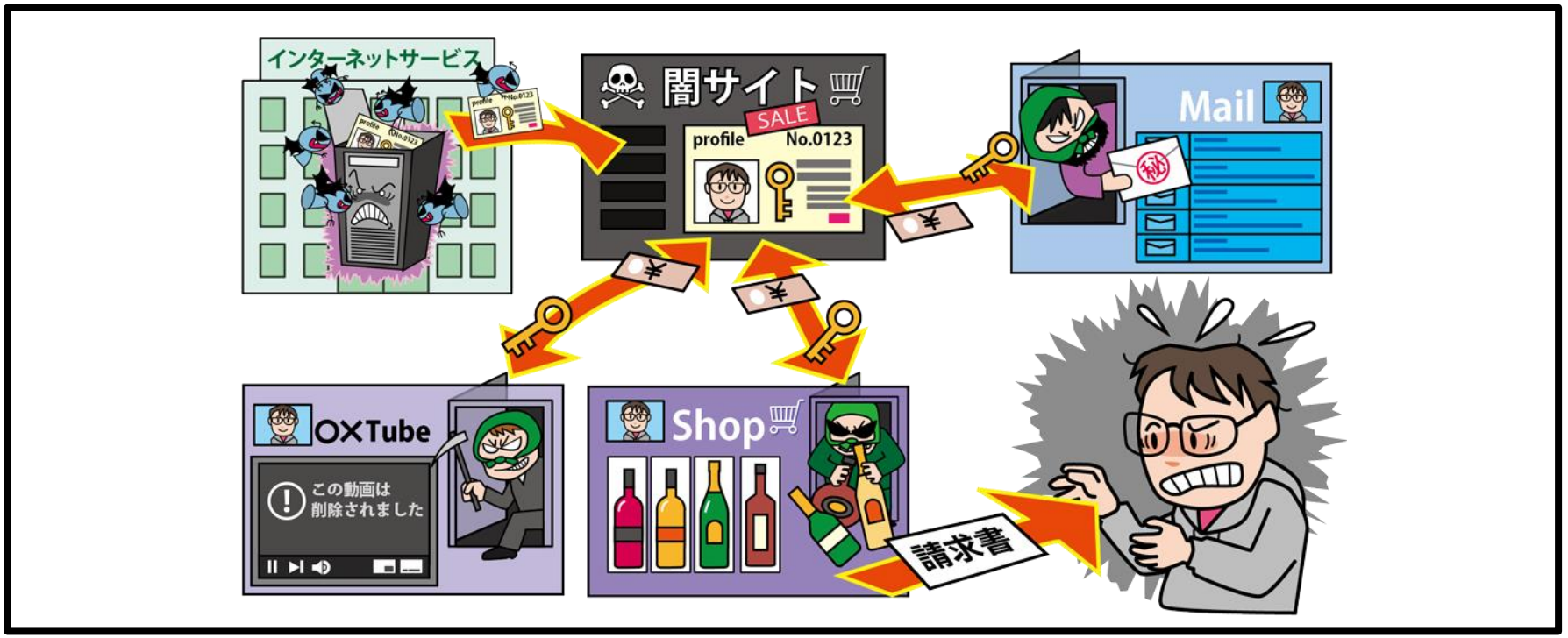


【8位】インターネット上のサービスからの個人情報の窃取
～オンラインショッピングの個人情報に注意！～

- **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**利用明細の定期的な確認**
    - ・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
      - –サービス運営者（コールセンター等）へ**相談**する
      - –警察へ**被害届を提出**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）

【9位】インターネット上のサービスへの不正ログイン

～狙われるインターネット上のサービス、各自でできる限りの対策を～



- 利用しているインターネットサービスの**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**使い回した認証情報が漏えい**し、悪用される
- 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

【9位】インターネット上のサービスへの不正ログイン

～狙われるインターネット上のサービス、各自でできる限りの対策を～

● 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

■ ウイルス感染による窃取

・**悪意あるウェブ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

【9位】インターネット上のサービスへの不正ログイン

～狙われるインターネット上のサービス、各自でできる限りの対策を～

● 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場合も

■ 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

【9位】インターネット上のサービスへの不正ログイン

～狙われるインターネット上のサービス、各自でできる限りの対策を～

- 2022年の事例/傾向①
  - 不正ログインによる個人情報の流出（※1）
    - 2022年9月、ニトリは同社が提供しているアプリにおいて**不正ログインの被害**があったことを公表
    - **約13万2,000件のアカウントが不正ログインされ**、個人情報が流出したおそれ
    - 同社以外から流出したIDとパスワードのリストを利用し、ログインを試みられた**パスワードリスト攻撃と推測**されている

【出典】

※1　ニトリ、不正アクセスで13万2000件の個人情報流出か　リスト型攻撃で（ITmedia NEWS）
https://www.itmedia.co.jp/news/articles/2209/21/news213.html

【9位】インターネット上のサービスへの不正ログイン
～狙われるインターネット上のサービス、各自でできる限りの対策を～

- 2022年の事例/傾向②
  - SNSにおける乗っ取り被害 (※1,2)
    - 2022年6月、バーチャルYouTuber(VTuber)グループ「にじさんじ」に関わるVTuberのTikTokアカウントで相次いで**乗っ取りの被害が発生**
    - ユーザー名やアイコンが変更されたり、投稿した動画を削除され、無関係の動画が投稿されたりといった被害を確認

【出典】
※1 にじさんじ、VTuberのTikTok乗っ取り相次ぐ 伏見ガク、夢追翔など(ITmedia NEWS)
https://www.itmedia.co.jp/news/articles/2206/29/news094.html
※2 にじさんじのVTuber多数がTikTokの乗っ取り被害に(yutura)
https://yutura.net/news/archives/77843

【9位】インターネット上のサービスへの不正ログイン

～狙われるインターネット上のサービス、各自でできる限りの対策を～

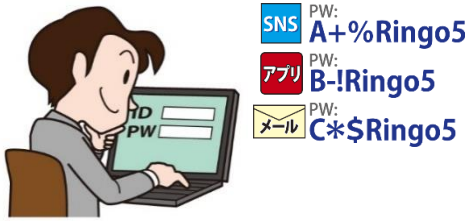
- 2022年の事例/傾向③
  - 二要素認証未実施による不正ログイン被害（※1）
    - 2022年12月、熊本県立大学は同大学の名誉教授のメールアカウントが不正ログインされていたことを公表
    - 同大学のメールユーザーの氏名等や当該教授のメールボックス内のメールと添付ファイルが漏えいしたおそれ
    - アカウントへのログインには二要素認証を用いることを原則としていたが、当該教授はスマートフォン等を未所持のため除外。さらに、簡素かつ使いまわしのパスワードを使用していたことも原因と考えられている

【出典】
※1 熊本県立大学メールアカウントの不正利用事案の発生について（熊本県立大学）
https://www.pu-kumamoto.ac.jp/sys/wp-content/uploads/2022/12/PR_20221213.pdf

【9位】インターネット上のサービスへの不正ログイン

～狙われるインターネット上のサービス、各自でできる限りの対策を～

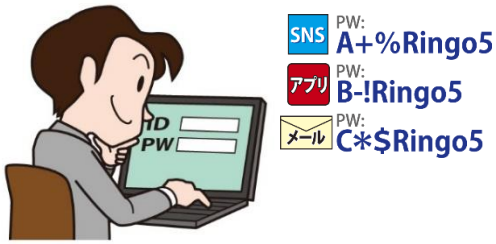
- **対策**
  - **利用者**
    - ・被害の予防
      - –メールの添付ファイル開封や、メールやSMSのリンク、URLのクリックを安易にしない
      - –パスワードは長く、複雑にする
      - –パスワードを使い回さない
      - –パスワード管理ソフトの利用
      - –利用しているサービスの多要素認証の設定を有効にする
      - –不審なウェブサイトで安易に認証情報を入力しない（フィッシングに注意）
      - –利用していないサービスからの退会
      - –利用頻度が低いサービスではクレジットカード情報を保存しない



【9位】インターネット上のサービスへの不正ログイン

～狙われるインターネット上のサービス、各自でできる限りの対策を～

- **対策**
  - **利用者**
    - ・被害の早期検知
      - –利用しているサービスの**ログイン履歴の確認**
      - –クレジットカードやポイント等の**利用履歴の定期的な確認**
    - ・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）
      - –サービス運営者（コールセンター等）へ**相談**する
      - –警察へ**被害届を提出**する



【10位】ワンクリック請求等の不当請求による金銭被害

～見せかけの操作や画面に騙されないで～

- 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
- **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

【10位】ワンクリック請求等の不当請求による金銭被害

～見せかけの操作や画面に騙されないで～

● 攻撃手口

・不当な請求表示させて不安を煽る、騙す

■ 悪意あるウェブサイトの閲覧

・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

■ 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**

【10位】ワンクリック請求等の不当請求による金銭被害
～見せかけの操作や画面に騙されないで～

● 攻撃手口

・ウェブサイトを開いたり電話をかけたりするよう誘導する

■ メールに記載されたリンクのクリック

・届いた**メール等に記載されているリンクをクリック**することで
ウェブサイトで入会完了画面が表示され、高額な入会金を
請求される

■ 電話をかけるように誘導

・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**

・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

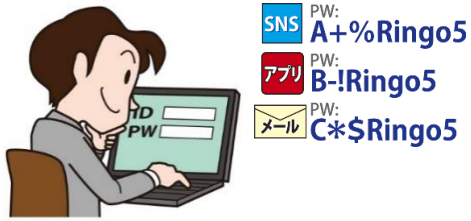
【10位】ワンクリック請求等の不当請求による金銭被害
～見せかけの操作や画面に騙されないで～

- 2022年の事例/傾向①
  - ワンクリック請求の手口に引き続き注意 (※1)
    - 2022年7月、IPA 情報セキュリティ安心相談窓口は、**ワンクリック請求に関する相談が引き続き寄せられている**と改めて注意を呼びかけた
    - 2022年は1月から6月までは**ひと月当たり8～22件の相談**を受け付けている（昨年同時期と同程度）
    - 2013年の多い時でひと月当たり300件以上の相談があり、現在は大きく減少しているが、**古典的な手口が継続しており、いまだに相談が無くならない**

【出典】
※1 安心相談窓口だより「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

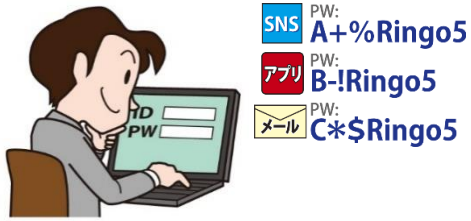
【10位】ワンクリック請求等の不当請求による金銭被害
～見せかけの操作や画面に騙されないで～

- **対策**
  - **ウェブサービス利用者等**
    - ・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**
      - –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**
      - –パスワード管理ソフトの利用
      - –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
      - –アクセスする**ウェブサイトの確認**
      - –不正プログラムを**ダウンロードしない**



【10位】ワンクリック請求等の不当請求による金銭被害
～見せかけの操作や画面に騙されないで～

- **対策**
  - **ウェブサービス利用者等**
    - ・被害を受けた後の対応
      - －**端末を初期化**する
      - －公的機関に**相談**する
        ※国民生活センター、消費生活センター、警察等



まとめ

情報セキュリティ対策の基本を実践

- 「10大脅威」の順位は毎回変動するが、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可能

※情報セキュリティ10大脅威 2023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　2023

本資料に関する詳細な内容は以下のウェブサイトをご覧ください

※以下のURLへアクセス、または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み、ウェブサイトをご覧ください

https://www.ipa.go.jp/security/10threats/10threats2023.html