IPA Better Life with IT

情報セキュリティ10大脅威　2022

～誰かが対策をしてくれている。そんなウマい話は、ありません！！～

［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
2022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 2022 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	標的型攻撃による機密情報の窃取
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	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	4	テレワーク等の ニューノーマルな働き方を狙った攻撃
スマホ決済の不正利用	5	内部不正による情報漏えい
偽警告によるインターネット詐欺	6	脆弱性対策情報の公開に伴う悪用増加
不正アプリによる スマートフォン利用者への被害	7	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）
インターネット上のサービスからの 個人情報の窃取	8	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	9	予期せぬ IT 基盤の障害に伴う業務停止
インターネット上のサービスへの 不正ログイン	10	不注意による情報漏えい等の被害

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

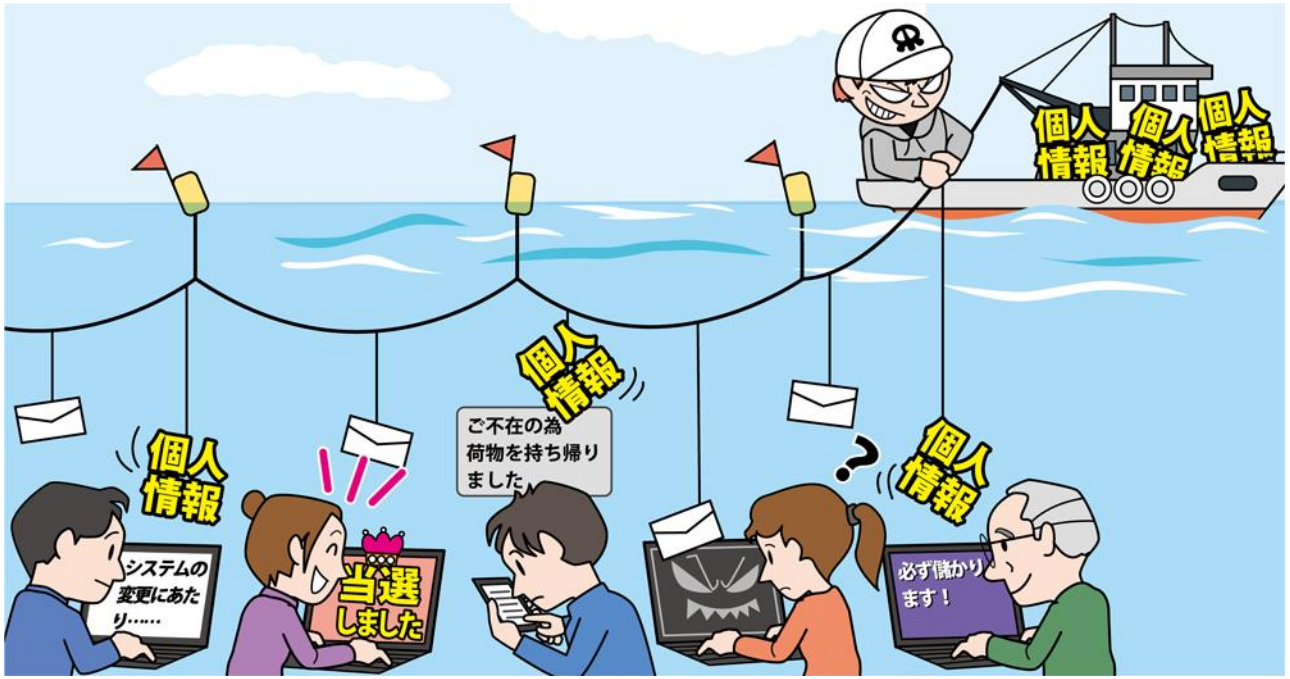
攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視するべき対策を理解する

情報セキュリティ10大脅威 2022
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

～宅配の不在通知を装うフィッシング詐欺に要注意！！～



- 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

～宅配の不在通知を装うフィッシング詐欺に要注意！！～

● 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
- 有名企業を騙ったメールやSNS、 SMS（スミッシング）で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

～宅配の不在通知を装うフィッシング詐欺に要注意！！～

- 2021年の事例/傾向①
  - 公共料金の未払いなどを装ったフィッシング（※1）
    - 水道局を騙り「料金を払わなければ断水する」などといった不安を煽り、偽のサイトにアクセスさせるメールを確認
    - メール内のリンクをクリックすると水道局のサイトを模倣したフィッシングサイトに移動
    - フィッシングサイトにアクセスするとクレジットカード情報などが盗まれたり、ウイルス感染のおそれがある

【出典】
※1 料金請求に関する不審メールについて（東京都水道局）
https://www.waterworks.metro.tokyo.lg.jp/press/r03/press211201-01.html

【1位】フィッシングによる個人情報等の詐取

～宅配の不在通知を装うフィッシング詐欺に要注意！！～

- 2021年の事例/傾向②
  - 宅配便の再配達受付を装ったスミッシング（※1）
    - 2021年8月、宅配便の再配達受付サービス装うSMSが届き、SMS内のリンクから偽サイトに誘導される事例を確認
    - 偽サイトは、URLが異なるが宅配業者のページを模倣して作成
    - 電話番号やマイナンバーカード等の本人確認書類、Apple IDやパスワードの入力を求めてくる

【出典】
※1 佐川急便を装った迷惑メールにご注意ください（佐川急便株式会社）
https://www2.sagawa-exp.co.jp/whatsnew/detail/721/

【1位】フィッシングによる個人情報等の詐取

～宅配の不在通知を装うフィッシング詐欺に要注意！！～

2021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、2021年は2020年のフィッシングの報告件数を大幅に上回っている
- Amazon、三井住友カードを騙るフィッシングが継続して報告
- スミッシングについては、宅配業者の不在通知を装ったSMSを悪用する事例が依然として確認
- 2021年10月～12月にかけては、Amazon、au、ドコモを騙るものも確認

【出典】
※1 2020/12 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/202012.html
※2 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

【1位】フィッシングによる個人情報等の詐取

～宅配の不在通知を装うフィッシング詐欺に要注意！！～

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
- 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
- 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

・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

～宅配の不在通知を装うフィッシング詐欺に要注意！！～

対策

インターネット利用者

・被害を受けた後の対応

- 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
- 信頼できる機関に相談

【2位】ネット上の誹謗・中傷・デマ
～1つの発言が人生を脅かす可能性も～

- 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
～1つの発言が人生を脅かす可能性も～

IPA

- **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**
  - ・特定の個人、企業に対する意見や感情を発言する際に、その内容についての影響を考慮せずに発信してしまう
  - ・匿名での発信であることでその内容が過激になりやすい（匿名でも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**
  - ・誹謗中傷や真偽不明のデマについて、それを見た第三者が、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
～1つの発言が人生を脅かす可能性も～

- 2021年の事例/傾向①
  - オリンピック出場選手に向けての誹謗・中傷 (※1)
    - ・オリンピックに出場した選手のSNSに対して誹謗・中傷が大量に送られていることを選手自身が告白
    - ・選手はあまりに悪質なものについてはデータを保存し然るべき対応を取ると意思を示した

【出典】
※1　水谷隼「しかるべき措置をとる」実際の誹謗中傷DMを公開（grape）
https://grapee.jp/991168

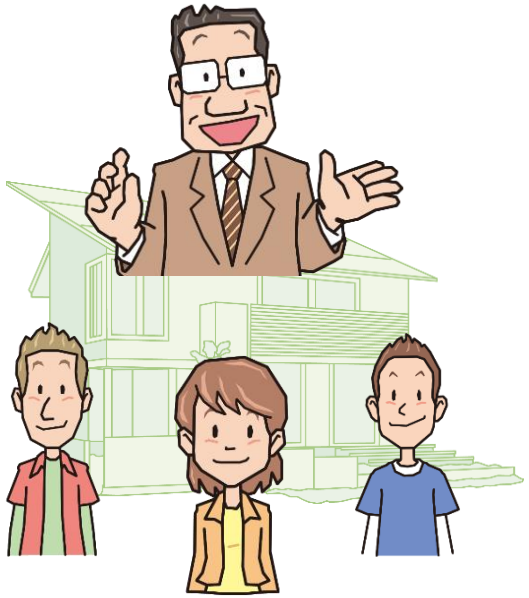
【2位】ネット上の誹謗・中傷・デマ
～1つの発言が人生を脅かす可能性も～

- 2021の事例/傾向②
  - デマ画像によるデマの拡散（※1）
    - ・新型コロナウイルスのワクチン接種を批判する内容にネオン表示が編集された通天閣のデマ画像がSNSで拡散
    - ・デマ画像の元になった通天閣の運営会社には事実確認の問い合わせが相次ぐ事態となった
    - ・運営会社は再度デマ画像が拡散された場合、法的措置を検討するとした

【出典】
※1　通天閣に「射っちゃダメ」デマ画像拡散に怒り（ITmediaビジネスONLiNE）
https://www.itmedia.co.jp/business/articles/2111/07/news020.html

【2位】ネット上の誹謗・中傷・デマ
～1つの発言が人生を脅かす可能性も～

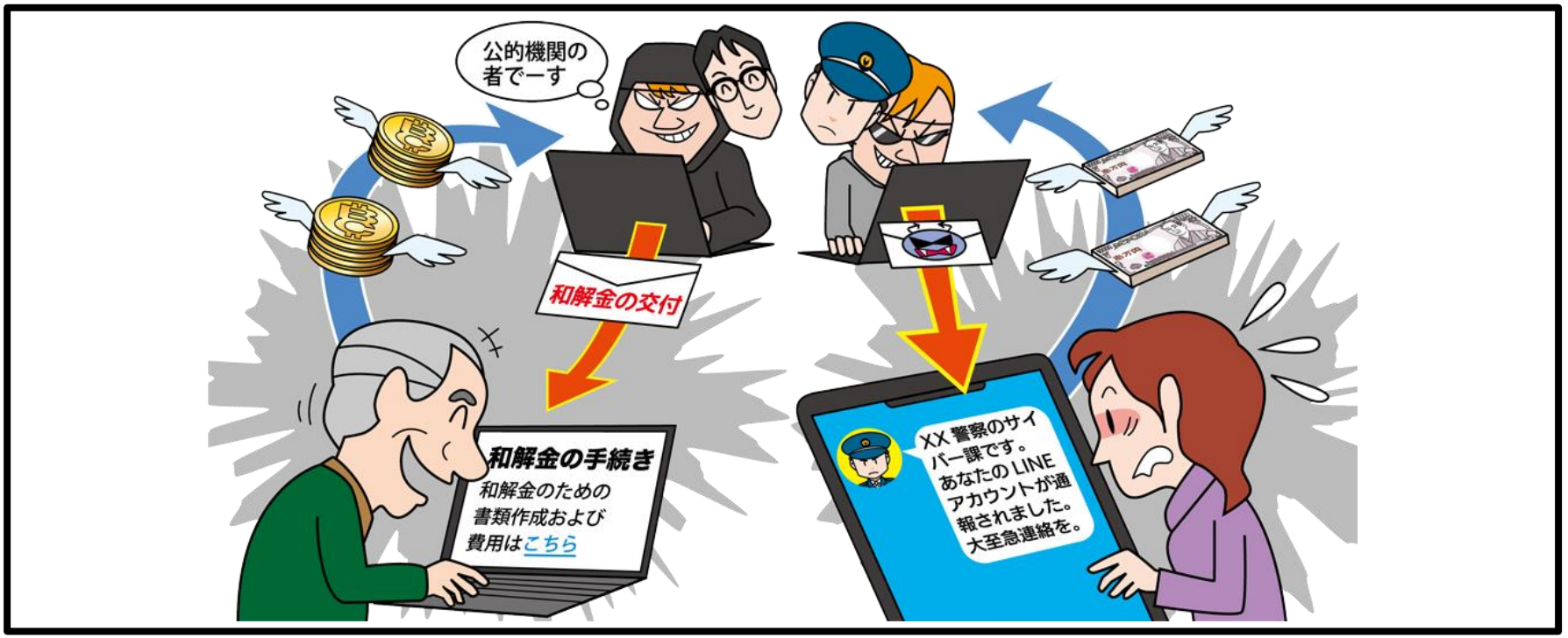
- 対策
  - 発信者
    - ・情報モラルや情報リテラシーの向上、法令遵守の意識の向上
      - －誹謗・中傷や公序良俗に反する投稿をしない
      - －投稿前に内容を再確認
      - －匿名性がある場合でも発言には責任を持つ
  - 家庭、教育機関
    - ・情報モラル、情報リテラシーの教育
      - －子供たちへの教育の実施



【2位】ネット上の誹謗・中傷・デマ
～1つの発言が人生を脅かす可能性も～

- 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
        - ※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
～公的機関を装ったメール等に注意～



- 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
～公的機関を装ったメール等に注意～

- **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
～公的機関を装ったメール等に注意～

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
- **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）

【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
～公的機関を装ったメール等に注意～

- 2021年の事例/傾向①
  - 公的機関を騙り、金銭を要求（※1）
    - ・2021年10月、「消費者庁」、「国民生活センター」等を騙り、架空の「和解金」の交付を持ち掛け、「書類作成費用」等の名目で金銭を支払わせるメールやSMSを確認
    - ・電子マネーを購入して金銭を支払うように誘導
    - ・受信者がメールを無視すると「罰則を科せられる」等、脅かすようなメッセージを送信

【出典】
※1　消費者庁などの公的機関の名称をかたり、架空の「和解金」などの交付を持ち掛けて金銭を支払わせる事業者に関する注意喚起（消費者庁）
https://www.caa.go.jp/notice/entry/026250/

【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
～公的機関を装ったメール等に注意～

- 2021年の事例/傾向②
  - 警察のLINEアカウントを装い連絡、架空請求の可能(※1)
    - ・2021年9月、広島県警のサイバー犯罪対策課を装うLINEアカウントを確認
    - ・「あなたのLINEアカウントが通報された」、「自宅または連絡可能な所在地へ郵送にて通達文を送付する」等、不安を煽り、連絡を取るよう求める

【出典】
※1 「あなたのアカウントが通報された」- 偽警察のLINEアカウントに注意（Security NEXT）
https://www.security-next.com/129668

【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
～公的機関を装ったメール等に注意～

- 2021年の事例/傾向③
  - 暗号資産で金銭を要求するメールの相談件数が増加 (※1,2,3)
    - IPAの情報セキュリティ安心相談窓口へ寄せられた、仮想通貨で金銭を要求する脅迫メールに関する相談件数が大幅に増加
    - 2021年に寄せられた相談件数が、2020年の2倍以上に
    - ビットコインでの送金を要求するセクストーションも引き続き確認
    - メール文面も英語の機械翻訳のような日本語から、年々、違和感の少ないものとなってきている

【出典】
※1 情報セキュリティ安心相談窓口の相談状況[2020年第4四半期(10月～12月)](IPA)
https://www.ipa.go.jp/security/txt/2020/q4outline.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/txt/2021/q4outline.html
※3 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/mgdayori20181010.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
～公的機関を装ったメール等に注意～

- **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
～公的機関を装ったメール等に注意～

- **対策**
  - **インターネット利用者**
    - ・被害を受けた後の対応
      - –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
～不審な利用記録がないか今一度確認を～

- ウイルス感染やフィッシング詐欺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
～不審な利用記録がないか今一度確認を～

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
～不審な利用記録がないか今一度確認を～

IPA

- **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
～不審な利用記録がないか今一度確認を～

- 2021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（※1,2）
    - ・化粧品会社が運営するオンラインショップが不正アクセスを受け、1,863 件のクレジットカード情報が流出したことを公表した。
    - ・ドラックストア運営会社が運営するオンラインショップが不正アクセスを受け、2万 5,484 件のクレジットカード情報が流出したことを公表した。

【出典】
※1 化粧品通販サイトに不正アクセス - クレカ情報流出の可能性（Security NEXT）
https://www.security-next.com/126477
※2 弊社が運営する「コスモスオンラインストア」への不正アクセスによるお客様情報流出に関するお詫びとお知らせ（株式会社コスモス薬品）
https://www.cosmospc.co.jp/notice/upload/ed661581b067c469eb29047679fa8a86e6446fe7.pdf

【4位】クレジットカード情報の不正利用
～不審な利用記録がないか今一度確認を～

- 2021年の事例/傾向②
  - 被害額は増加傾向、盗用被害の割合増加 (※1)
    - ・2021年1～9月における不正利用被害額は約236億9,000万円となった。前年の同期間の約180億2,000万円から大幅に増加
    - ・被害額全体の94.5%を番号盗用被害が占めており、その割合は年々増加している

【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(（一社）日本クレジット協会）
https://www.j-credit.or.jp/download/news20211228a1.pdf

【4位】クレジットカード情報の不正利用
～不審な利用記録がないか今一度確認を～

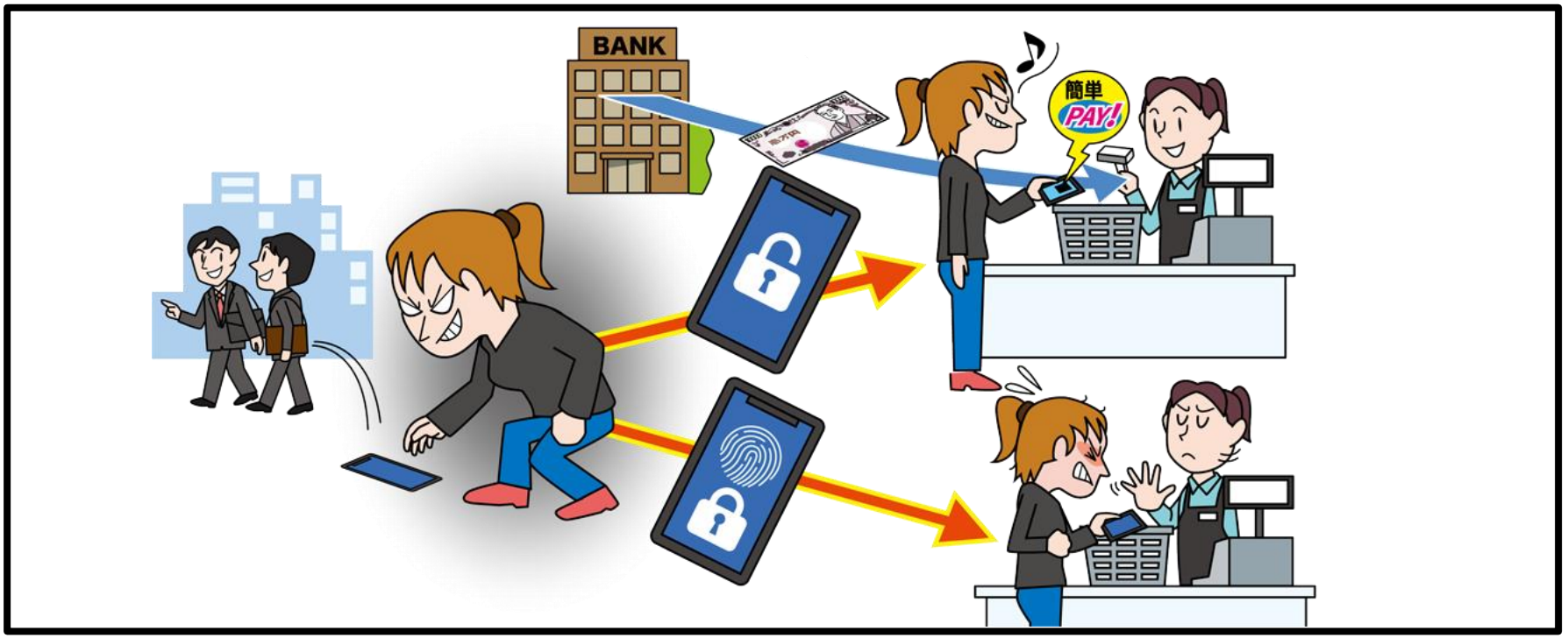
- 対策
  - 利用者
    - ・被害の予防
      - –クレジットカード会社が提供している本人認証サービス（3Dセキュア等）の利用
      - –添付ファイルやURLを安易に開かない
      - –普段は表示されないような画面やポップアップが表示された場合、情報を入力しない
      - –プリペイドカードの利用を検討
        ※不正利用被害額となる利用可能金額の範囲を限定する

【4位】クレジットカード情報の不正利用
～不審な利用記録がないか今一度確認を～

- 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
      - –サービス運営者（コールセンター等）へ連絡
      - –クレジットカードの再発行
      - –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）
      - –ウイルス感染した端末の初期化
      - –警察への被害届の提出

【5位】スマホ決済の不正利用

～今や「スマートフォン」＝「個人情報、財産」の時代！日頃からリスク管理の徹底を～



- 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

～今や「スマートフォン」＝「個人情報、財産」の時代！日頃からリスク管理の徹底を～

● 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

～今や「スマートフォン」＝「個人情報、財産」の時代！日頃からリスク管理の徹底を～

● 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に作りこまれた脆弱性を悪用し、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

～今や「スマートフォン」=「個人情報、財産」の時代！日頃からリスク管理の徹底を～

- 2021年の事例/傾向①
  - 拾ったスマートフォンで不正チャージ（※1）
    - 2021年10月、拾ったスマートフォンでスマホ決済サービスPayPayに不正チャージを行った攻撃者が「電子計算機使用詐欺」容疑で逮捕
    - 被害者は携帯電話会社に連絡し、通話や通信機能は使用不能にしていたが、PayPayには届け出ていなかった

【出典】
※1 スマホ拾った男、「ペイペイ」で電子マネー詐取…ネット上の撮影写真データで発覚（読売新聞オンライン）
https://www.yomiuri.co.jp/national/20211020-OYT1T50001/

【5位】スマホ決済の不正利用

～今や「スマートフォン」＝「個人情報、財産」の時代！日頃からリスク管理の徹底を～

- 2021年の事例/傾向②
  - 決済音鳴らし決済完了に見せかける（※1）
    - 2021年8月、ディスカウントストアでの会計時にスマホ決済サービスPayPayの決済完了音を鳴らし、あたかも決済が終了したかのように見せかける事例が発生した
    - ディスカウントストアの売り上げとPayPayからの支払いに差額があったことから判明

【出典】
※1 「ペイペイ」決済音鳴らし食品だまし取った疑い、男逮捕（朝日新聞DIGITAL）
https://www.asahi.com/articles/ASP7Y2SXWP7WUTNB011.html

【5位】スマホ決済の不正利用

～今や「スマートフォン」＝「個人情報、財産」の時代！日頃からリスク管理の徹底を～

- 2021年の事例/傾向③
  - スマホ決済で身に覚えのない不正な支払い（※1）
    - ・消費者行政センターによると、スマホ決済サービスで身に覚えない不正な支払いの相談を受けたとのこと
    - ・履歴から15分間で10件の購入されており、利用限度額いっぱいの25万円が使用されていた

【出典】
※1　キャッシュレス決済の不正利用トラブル（神奈川県川崎市 経済労働局産業政策部消費者行政センター）
https://www.city.kawasaki.jp/280/page/0000135952.html

【5位】スマホ決済の不正利用

～今や「スマートフォン」＝「個人情報、財産」の時代！日頃からリスク管理の徹底を～

- 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

【5位】スマホ決済の不正利用

～今や「スマートフォン」＝「個人情報、財産」の時代！日頃からリスク管理の徹底を～

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

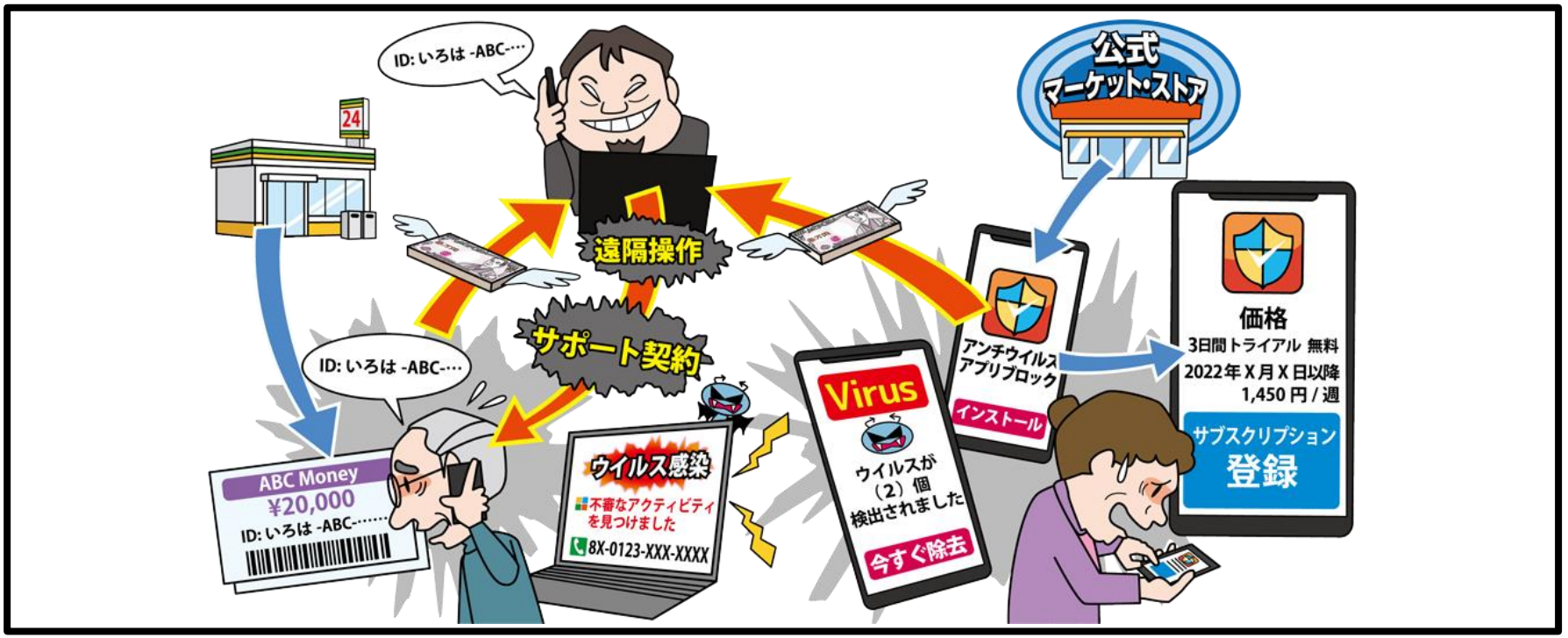
－パスワードを変更する（他のサービスで同じパスワードを使っていた場合は同様に対応）

－サービス運営者（コールセンター等）へ連絡

－連携する金融機関への連絡

－警察に相談する

【6位】偽警告によるインターネット詐欺
～それは詐欺です。慌てる、焦るは思うツボ！～



- 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

【6位】偽警告によるインターネット詐欺
～それは詐欺です。慌てる、焦るは思うツボ！～

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させない

【6位】偽警告によるインターネット詐欺
～それは詐欺です。慌てる、焦るは思うツボ！～

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

【6位】偽警告によるインターネット詐欺
～それは詐欺です。慌てる、焦るは思うツボ！～

- 2021年の事例/傾向①
  - 電話をかけさせて偽のサポートへ誘導（※1）
    - IPA安心相談窓口によると、2021年は偽のセキュリティ警告画面に電話番号を表示し、電話をかけさせるよう誘導する手口の相談を多く受けたとのこと
    - 電話をかけると虚偽の説明や遠隔操作用ソフトウェアのインストールを促され、修理費用という名目で電子マネーを請求される
    - 遠隔操作用ソフトウェアをインストールするとデータの閲覧や消去、PC を起動させなくするといった悪質な操作が行われるおそれがある

【出典】
※1　安心相談窓口だより「偽のセキュリティ警告に表示された番号に電話をかけないで！」（IPA）
https://www.ipa.go.jp/security/anshin/mgdayori20211116.html

【6位】偽警告によるインターネット詐欺
～それは詐欺です。慌てる、焦るは思うツボ！～

- 2021年の事例/傾向②
  - パソコン PC 修理名目のサポート詐欺事件 (※1)
    - ・2021年12月、新潟中央警察署はサポート詐欺事案の届出を受理し、特殊詐欺(架空料金請求詐欺)として捜査開始
    - ・被害者は、自宅でPC を使用していたところ、画面上に「中国にハッキングされている」等のメッセージと電話番号が表示された
    - ・電話番号に連絡したところ、遠隔操作での修理代金として電子マネーを請求され、合計7万5,000円分騙し取られた

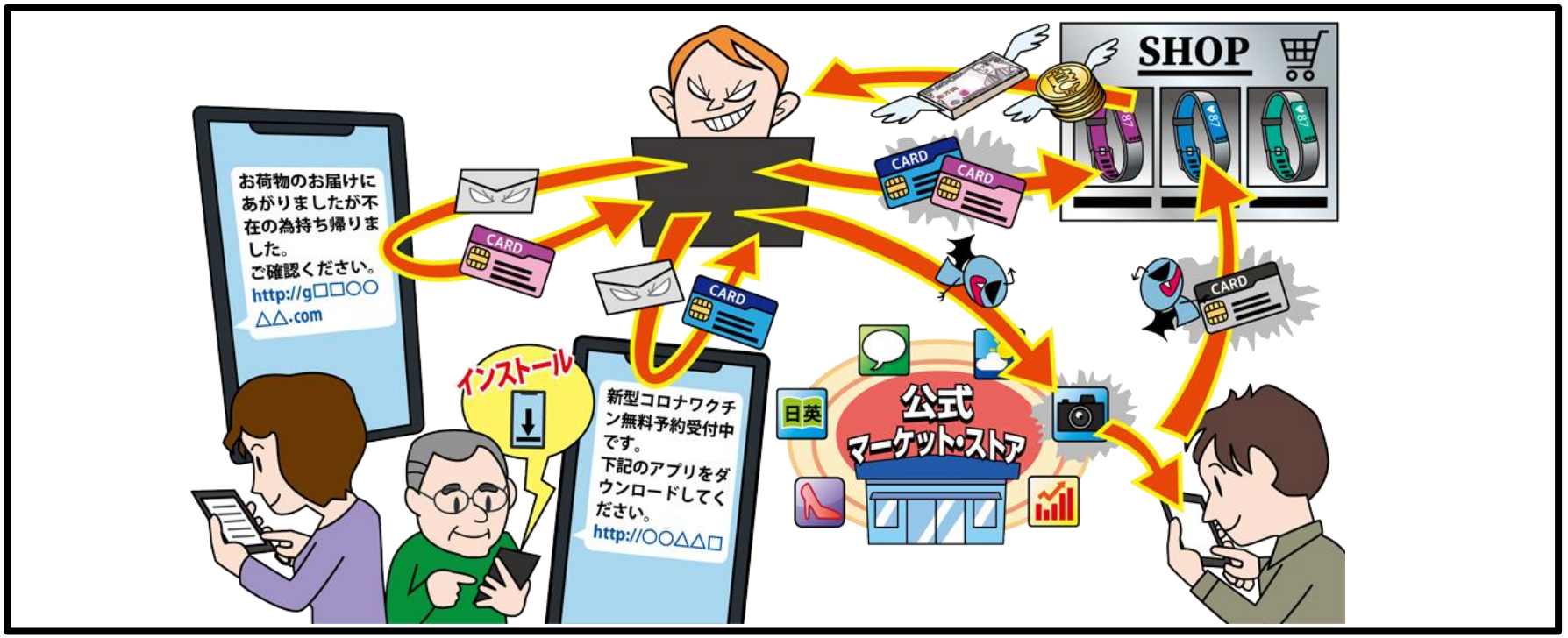
【出典】
※1 新潟中央警察署「パソコン修理名目の特殊詐欺被害が発生！！慌てず落ち着いた行動を」(新潟中央警察署)
https://www.pref.niigata.lg.jp/uploaded/attachment/293015.pdf

【6位】偽警告によるインターネット詐欺
～それは詐欺です。慌てる、焦るは思うツボ！～

- 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
      - －偽警告が表示されても従わない
      - －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
    - ・被害を受けた後の対応
      - －端末を初期化
      - －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
      - －クレジットカード会社へ連絡

【7位】不正アプリによるスマートフォン利用者への被害

～偽装 SMS の URL リンクや不正アプリへの誘導に注意～



- 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

【7位】不正アプリによるスマートフォン利用者への被害

～偽装 SMS の URL リンクや不正アプリへの誘導に注意～

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

■ 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

■ 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

■ 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

【7位】不正アプリによるスマートフォン利用者への被害

～偽装 SMS の URL リンクや不正アプリへの誘導に注意～

● 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

■ 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

【7位】不正アプリによるスマートフォン利用者への被害

～偽装 SMS の URL リンクや不正アプリへの誘導に注意～

- 2021年の事例/傾向①
  - 通信事業者を騙った SMS から不正アプリのダウンロードサイトに誘導 (※1)
    - 通信事業者になりすました SMS が届き、本文に記載したURL(偽のサイト)にアクセスさせられ、不正アプリをインストールさせられる手口を確認
    - OS毎に手口が異なり、Android端末の場合は不正アプリ(*.apk)、iPhoneの場合は構成プロファイルをダウンロードさせて、不正アプリをインストールさせる
    - インストールした不正アプリで認証情報を入力すると、攻撃者にその情報が詐取される

【出典】
※1 通信事業者を装ったフィッシング((一財)日本サイバー犯罪対策センター)
https://www.jc3.or.jp/threats/examples/article-409.html

【7位】不正アプリによるスマートフォン利用者への被害

～偽装 SMS の URL リンクや不正アプリへの誘導に注意～

- 2021年の事例/傾向②
  - 偽のワクチン接種予約案内 (※1)
    - 新型コロナウイルスのワクチン接種予約を装う偽のSMSが送信され、不正サイトに誘導される事例を確認
    - 不正サイトから不正アプリをインストールしてしまうと、踏み台にされる
    - 踏み台後、様々な文言の偽装SMSを不特定多数に対して送り付け、そこから別の第三者を不正サイトに誘導してしまう

【出典】
※1【注意喚起】偽のワクチン接種予約案内に注意（トレンドマイクロ株式会社）
https://www.is702.jp/news/3864/

【7位】不正アプリによるスマートフォン利用者への被害

～偽装 SMS の URL リンクや不正アプリへの誘導に注意～

- 2021年の事例/傾向③
  - トロイの木馬が仕込まれたゲームアプリからの情報窃取 (※1)
    - Android 端末のゲームアプリ 190 種にトロイの木馬が仕込まれており、930 万以上のスマートフォンにインストールされている可能性が指摘されている
    - 対象のゲームアプリをインストールするとリ携帯電話番号等の個人情報が収集され、リモートサーバに送信される
    - 対象のゲームアプリは既にアプリストアから削除されている

【出典】
※1 トロイの木馬仕込まれたゲームアプリ、Androidユーザー 930万人がダウンロード（株式会社マイナビ）
https://news.mynavi.jp/article/20211125-2198828/

【7位】不正アプリによるスマートフォン利用者への被害
～偽装 SMS の URL リンクや不正アプリへの誘導に注意～

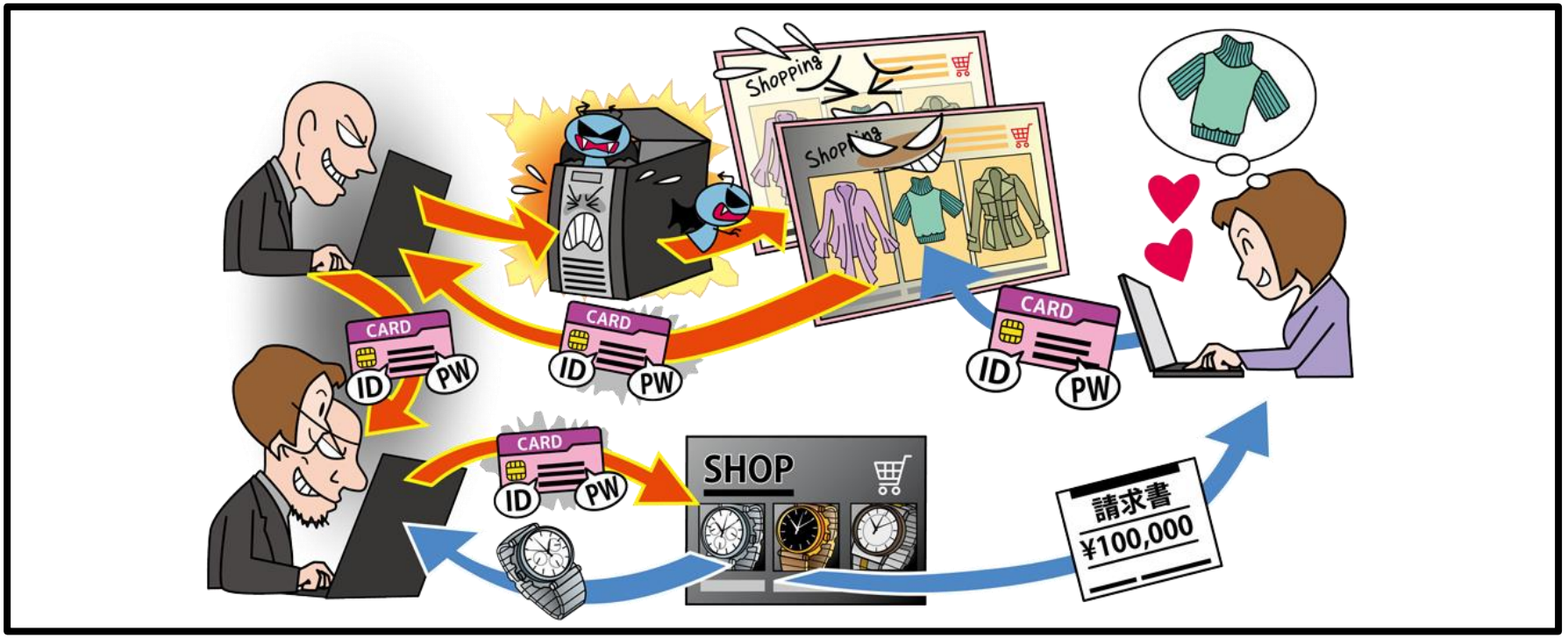
- 対策
  - スマートフォン利用者
    - ・被害の予防
      - –アプリは公式マーケットから入手
        - ※公式マーケットのアプリでも油断は禁物
          様々な情報（レビュー評価等）を確認して信頼できるアプリのみ利用
      - –アプリインストール時のアクセス権限の確認
        - ※アプリの機能に対して適切かどうか確認
      - –アプリインストールに関する設定に注意
        - ※Android端末の設定で提供元不明のアプリのインストールを許可しない
        - ※iPhoneの設定で、「信頼されていないエンター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

【7位】不正アプリによるスマートフォン利用者への被害
～偽装 SMS の URL リンクや不正アプリへの誘導に注意～

- **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

【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

～頻発する個人情報の漏えい、利用者もできる限りの対策を～



- 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
～頻発する個人情報の漏えい、利用者もできる限りの対策を～

● 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
～頻発する個人情報の漏えい、利用者もできる限りの対策を～

● 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や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IDや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
～頻発する個人情報の漏えい、利用者もできる限りの対策を～

- 2021年の事例/傾向①
  - クラウドサーバーへの不正アクセス（※1,※2）
    - 2021年5月、マッチングアプリの利用者の年齢確認書類の画像171万1,756件が流出したと運営会社から公表された
    - 画像が保存されていたクラウドサーバーにアクセスするための情報を不正に取得した第三者によって、正規のアクセスを装って不正アクセスが行われていた

【出典】
※1　不正アクセスによる会員様情報流出の調査結果と今後の対応について（株式会社ネットマーケティング）
https://www.net-marketing.co.jp/news/6001/
※2　Omiaiの「個人情報流出」が深刻化した根本原因（東洋経済ONLINE）
https://toyokeizai.net/articles/-/431661

【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
～頻発する個人情報の漏えい、利用者もできる限りの対策を～

- 2021年の事例/傾向②
  - 改ざんされたECサイトからの情報流出(※1)
    - ・2021年7月、ECサイトから、登録されていた1,301人分のクジットカード情報が流出したと運営会社から公表された
    - ・一部のクレジットカード情報は悪用され総額767万4,605円の金銭被害が発生
    - ・原因は不正アクセスによって決済処理プログラムの改ざんが行われていたため

【出典】
※1　読売新聞子会社でクレカ情報流出 すでに767万円の金銭的被害も確認(ITmedia NEWS)
https://www.itmedia.co.jp/news/articles/2107/14/news116.htm

【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
～頻発する個人情報の漏えい、利用者もできる限りの対策を～

- 2021年の事例/傾向③
  - SQLインジェクション攻撃による被害(※1)
    - 2021年9月、ホームページから登録されたメールアドレス約12万8,000件が流出したと運営会社から公表された
    - データベースに対して不正に操作を行うSQLインジェクション攻撃を受けたことが原因
    - 登録ユーザのメールアドレス宛に迷惑メールが届くようになり発覚

【出典】
※1 弊社ホームページへの不正アクセスによる被害発生のお詫びとお知らせ(ロゴヴィスタ株式会社)
https://www.logovista.co.jp/lverp/information/information/emergency.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
～頻発する個人情報の漏えい、利用者もできる限りの対策を～

- 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する
      - –不要な情報は安易に登録しない
      - –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の退会
      - –不正ログイン対策を実施する
        （個人10位「インターネット上のサービスへの不正ログイン」参照）
    - ・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

【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
～頻発する個人情報の漏えい、利用者もできる限りの対策を～

- **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）へ連絡

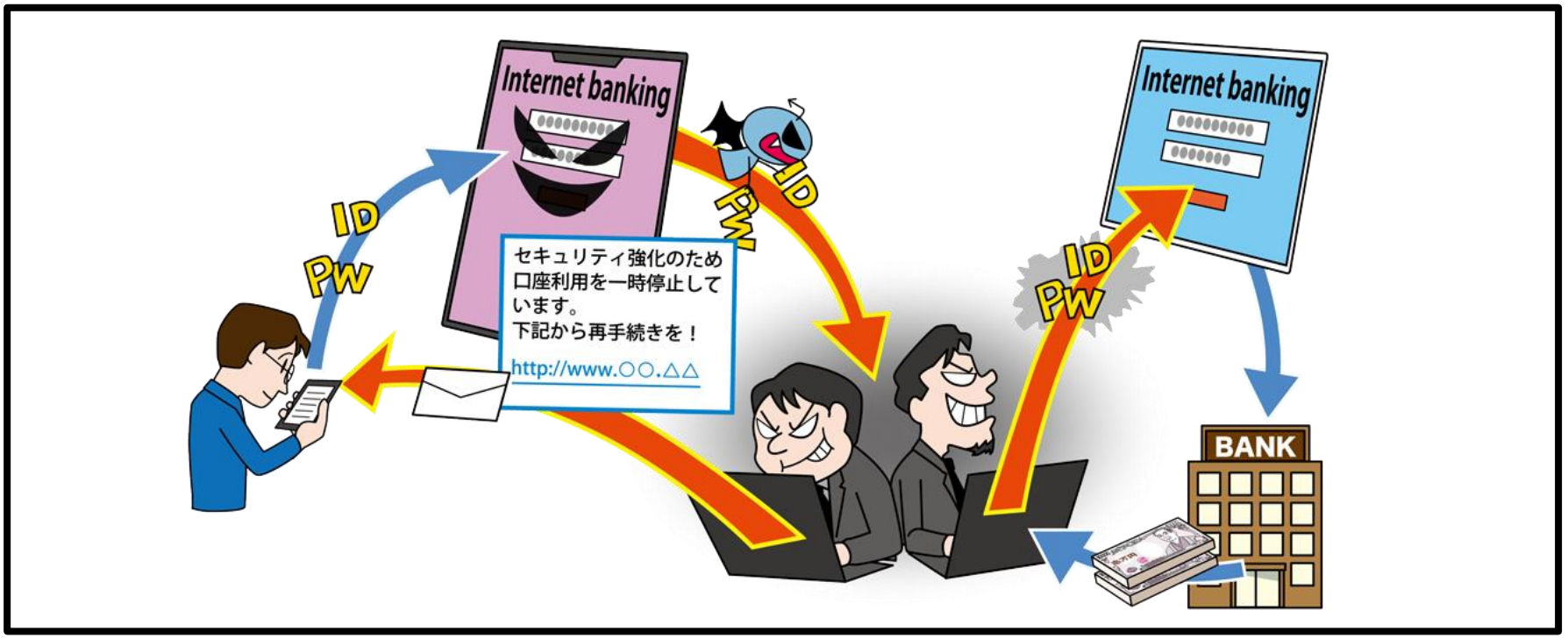
– クレジットカードの停止

– 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）

– 警察への被害届の提出

【9位】インターネットバンキングの不正利用

～金融機関からSMSが送られてきても、ひとまず落ち着こう～



- インターネットバンキングの認証情報を悪用され不正送金される
- 認証情報はフィッシング詐欺やウイルス感染によって漏えいする

【9位】インターネットバンキングの不正利用

～金融機関からSMSが送られてきても、ひとまず落ち着こう～

● 攻撃手口

・インターネットバンキングに関する認証情報を窃取

■ フィッシング詐欺による情報詐取

・実在する銀行等のウェブサイトを模した偽のウェブサイト（フィッシングサイト）を用意する

・フィッシングサイトのリンクが記載されたメールを不特定多数に送信し、フィッシングサイトへ誘導する

■ ウイルス感染による情報窃取

・悪意あるファイルをメールに添付して送信し、ファイルを開かせる

・悪意あるウェブサイトが表示されるリンクをクリックさせる

【9位】インターネットバンキングの不正利用

～金融機関からSMSが送られてきても、ひとまず落ち着こう～

- 2021年の事例/傾向①
  - 件数は半減、1 件当たりの被害額は増加 (※1)
    - ・警察庁によると、インターネットバンキングに関わる不正送金事犯の発生件数は、2020年(１月から6月)と比較し、2021年は減少傾向とのこと
    - ・一方、被害額はやや減少といった状態としている
    - ・被害額の約87%は個人口座からの不正送金であり、依然として個人の被害が多い

【出典】

※1　令和3年上半期におけるサイバー空間をめぐる脅威の情勢等について(警察庁)
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_kami_cyber_jousei.pdf

【9位】インターネットバンキングの不正利用

～金融機関からSMSが送られてきても、ひとまず落ち着こう～

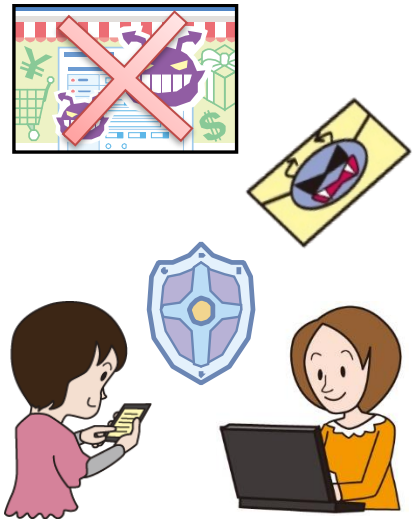
- 2021年の事例/傾向②
  - メモアプリ利用の注意喚起 (※1)
    - 警察庁によると、インターネットバンキング不正利用の事例として、メモアプリに保存されていたインターネットバンキングのID、パスワードを悪用されるものがあった
    - 日本サイバー犯罪対策センター(JC3)によると、メモアプリのフィッシングサイトが確認されており、安易にアクセスしないよう注意喚起がされた

【出典】
※1 .メモアプリ利用時の注意点((一財)日本サイバー犯罪対策センター)
https://www.jc3.or.jp/threats/topics/article-414.html

【9位】インターネットバンキングの不正利用

～金融機関からSMSが送られてきても、ひとまず落ち着こう～

対策



インターネットバンキング利用者

・被害の予防（被害に備えた対策含む）

- 受信メールやウェブサイトの十分な確認
- 添付ファイルやURLを安易にクリックしない
- PC等でファイルの拡張子表示設定をする
  ※不審なファイルに気づきやすくする
- 普段は表示されないポップアップ画面に
  個人情報等は入力しない
- 金融機関や公的機関から公開される注意喚起を確認する
- 多要素認証の設定を有効にする
- 口座連携済みサービスを確認する
- 認証に不備がある銀行口座を利用停止する

【9位】インターネットバンキングの不正利用

～金融機関からSMSが送られてきても、ひとまず落ち着こう～

対策

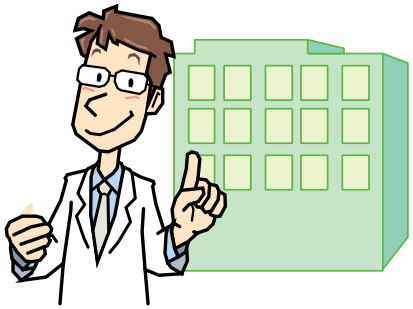
インターネットバンキング利用者

・被害の早期検知

- 不審なログイン履歴の確認
- 口座の利用履歴の確認
- サービス利用状況の通知機能の利用

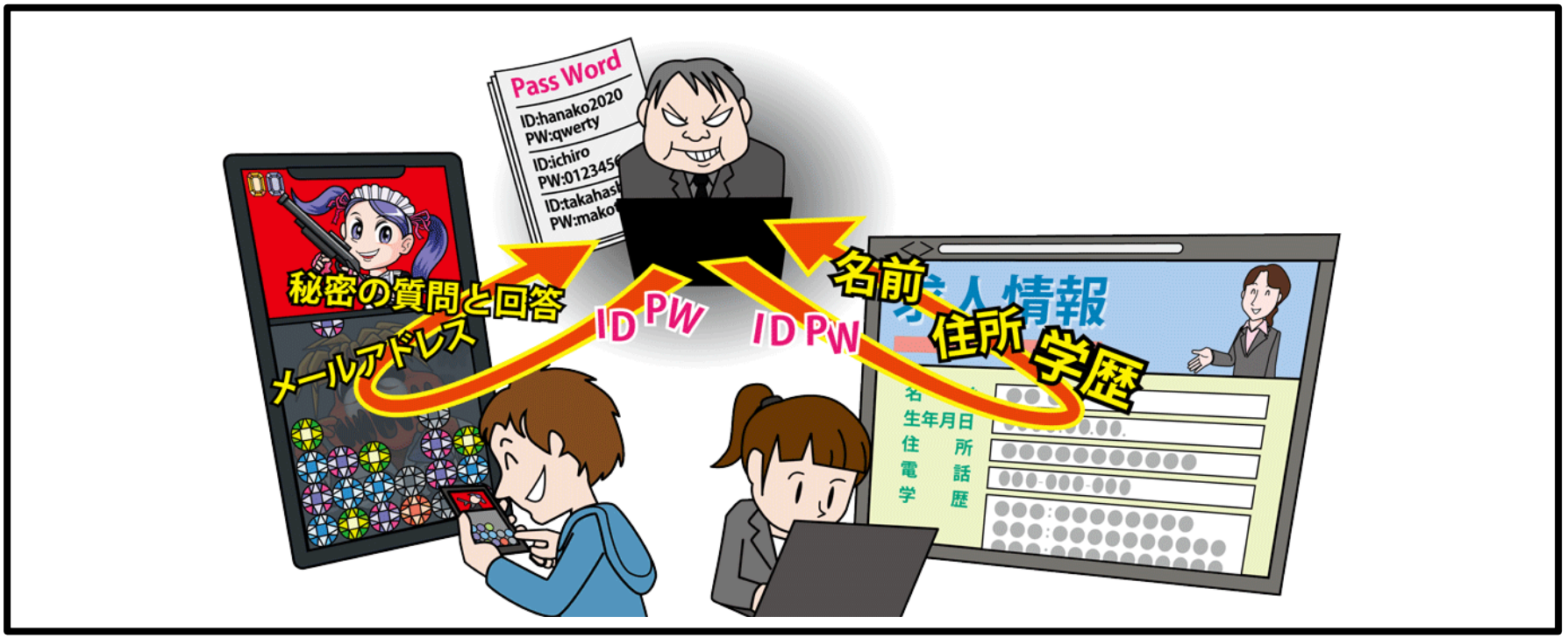
・被害を受けた後の対応

- 当該サービスのコールセンターへの連絡
- 警察への被害届の提出
- ウイルス感染した端末の初期化
- 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）



【10位】インターネット上のサービスへの不正ログイン

～パスワードの使い回しに注意、あなたの個人情報が閲覧されるかも～



- 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

【10位】インターネット上のサービスへの不正ログイン

～パスワードの使い回しに注意、あなたの個人情報が閲覧されるかも～

● 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

【10位】インターネット上のサービスへの不正ログイン

～パスワードの使い回しに注意、あなたの個人情報が閲覧されるかも～

● 攻撃手口

・不正に入手した認証情報で不正ログインする

■ パスワード推測攻撃

- 利用者が使いそうなパスワードを推測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

■ 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

【10位】インターネット上のサービスへの不正ログイン

～パスワードの使い回しに注意、あなたの個人情報が閲覧されるかも～

- 2021年の事例/傾向①
  - 外部で不正取得したパスワードで不正ログイン（※1,2）
    - ・2021年2月、転職情報サイトに外部から入手されたと思われパスワードを用いた攻撃による不正ログイン
    - ・21万2,816人のWeb履歴書が閲覧
    - ・2021年10月、モバイル向けゲームを提供するサイトの会員サービスにパスワードリスト型攻撃での不正ログイン
    - ・2,846件の個人情報が閲覧

【出典】
※1 「マイナビ転職」への不正ログイン発生に関するお詫びとお願い（株式会社マイナビ）
https://www.mynavi.jp/topics/post_29797.html
※2 KLab ID への不正ログインに関するお知らせ（KLab株式会社）
https://www.klab.com/jp/press/info/2021/1027/klab_id_2.html

【10位】インターネット上のサービスへの不正ログイン

～パスワードの使い回しに注意、あなたの個人情報が閲覧されるかも～

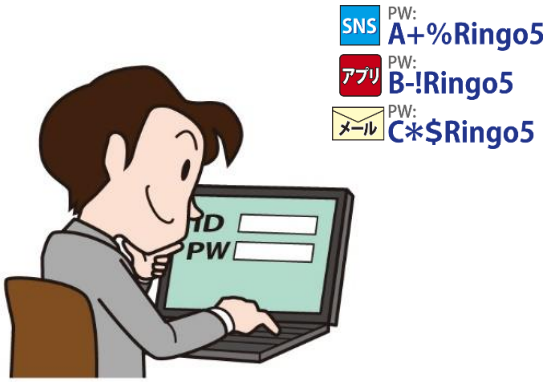
- 2021年の事例/傾向②
  - パスワード類推による不正ログイン（※1）
    - 女子大生のSNSへ不正ログインおよび女性タレントのアカウント情報をインターネット上に保管したとして男が逮捕
    - 被害者は、名前や生年月日にちなんだパスワードを設定
    - 男はアカウント名やプロフィールの情報を組み合わせてパスワードを類推

【出典】
※1　女子大生・タレントのSNSに不正アクセス…男「プライベートのぞきたくて」（読売新聞オンライン）
https://www.yomiuri.co.jp/national/20220107-OYT1T50005/

【10位】インターネット上のサービスへの不正ログイン

～パスワードの使い回しに注意、あなたの個人情報が閲覧されるかも～

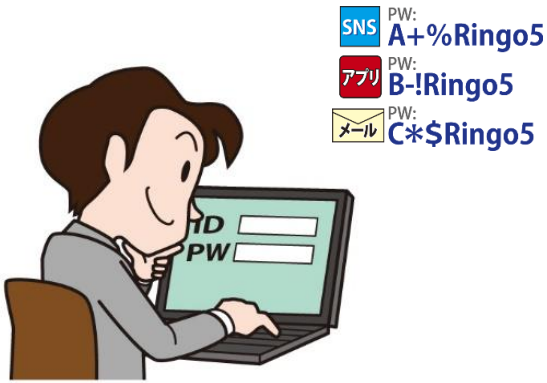
- **対策**
  - **利用者**
    - ・被害の予防
      - –添付ファイルやURLを安易にクリックしない
      - –パスワードは長く、複雑にする
      - –パスワードを使い回さない
      - –パスワード管理ソフトの利用
      - –サービスが推奨する認証方式の利用
      - –不審なウェブサイトで安易に認証情報を入力しない（フィッシングに注意）
      - –利用していないサービスからの退会



【10位】インターネット上のサービスへの不正ログイン

～パスワードの使いまわしに注意、あなたの個人情報が閲覧されるかも～

- 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
      - －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）
      - －クレジットカードの停止
      - －サービス運営者（コールセンター等）へ連絡
      - －警察への被害届の提出



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

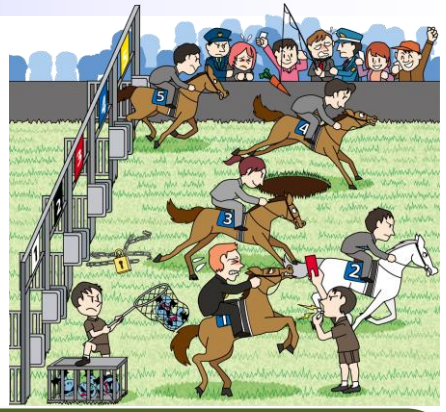
- 新たな機器やサービスの普及に伴いインターネット利用における脅威なども変化する
- 公的機関の注意喚起やニュースなどから脅威の手口に関する情報を収集し、変化する手口を理解して適切な対策を実践することが重要

詳細な資料のダウンロード

■情報セキュリティ10大脅威　2022

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/vuln/10threats2022.html

■アンケートご協力のお願いについて

IPAが公開しているツールや資料の品質向上のため、アンケートへのご協力をお願い致します

https://touroku.ipa.go.jp/?url=http%3A%2F%2Fspd-evsan-ap01.ipa.go.jp%2Fentry%2FMemberLogin%3Fevent_id%3DEA0000000074