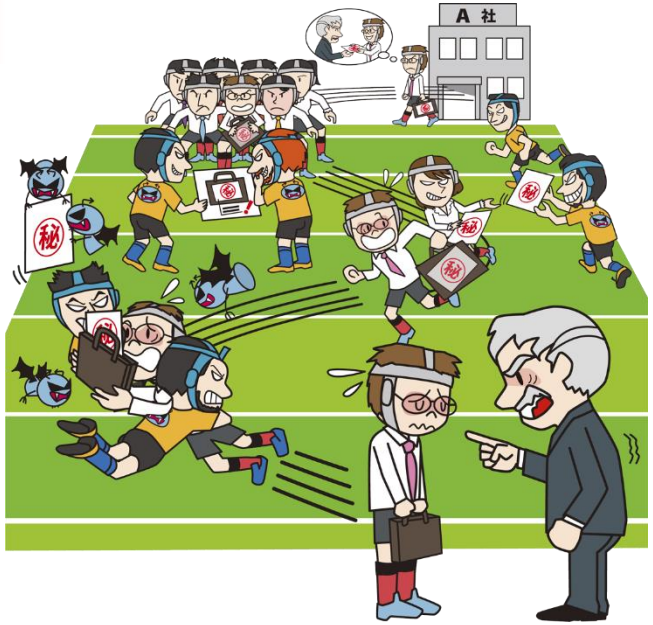
IPA Better Life with IT

情報セキュリティ10大脅威 2020

～セキュリティ対策は一丸となって、Let's Try!!～

［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
2020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」**

- 企業や政府機関などの組織
- 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 2020

IPA

- 「情報セキュリティ10大脅威 2020」の章構成
  - 1章. 知っておきたい用語や仕組み
    パソコンやスマホ、インターネットを安全に使用するための知識を習得するにあたってよく登場する用語や仕組みについて解説
  - 2章. 情報セキュリティ10大脅威 2020
    2019年の事例や傾向をもとに選出した「情報セキュリティ10大脅威 2020」について各脅威の概要や対策等について解説
  - 3章. 情報セキュリティ10大脅威の活用法
    組織や自分の立場・環境によって重要度の高い脅威が異なることを踏まえ、サービスや顧客情報等の「守るべきもの」を明らかにした上で、情報セキュリティ10大脅威を活用しながら効率的に対策を講じるための手順を解説

情報セキュリティ10大脅威 2020 脅威ランキング

IPA

「個人」向け脅威	順位	「組織」向け脅威
スマホ決済の不正利用	1	標的型攻撃による機密情報の窃取
フィッシングによる個人情報の詐取	2	内部不正による情報漏えい
クレジットカード情報の不正利用	3	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	4	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	5	ランサムウェアによる被害
不正アプリによるスマートフォン利用者への被害	6	予期せぬIT基盤の障害に伴う業務停止
ネット上の誹謗・中傷・デマ	7	不注意による情報漏えい
インターネット上のサービスへの不正ログイン	8	インターネット上のサービスからの個人情報の窃取
偽警告によるインターネット詐欺	9	IoT機器の不正利用
インターネット上のサービスからの個人情報の窃取	10	サービス妨害攻撃によるサービスの停止

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

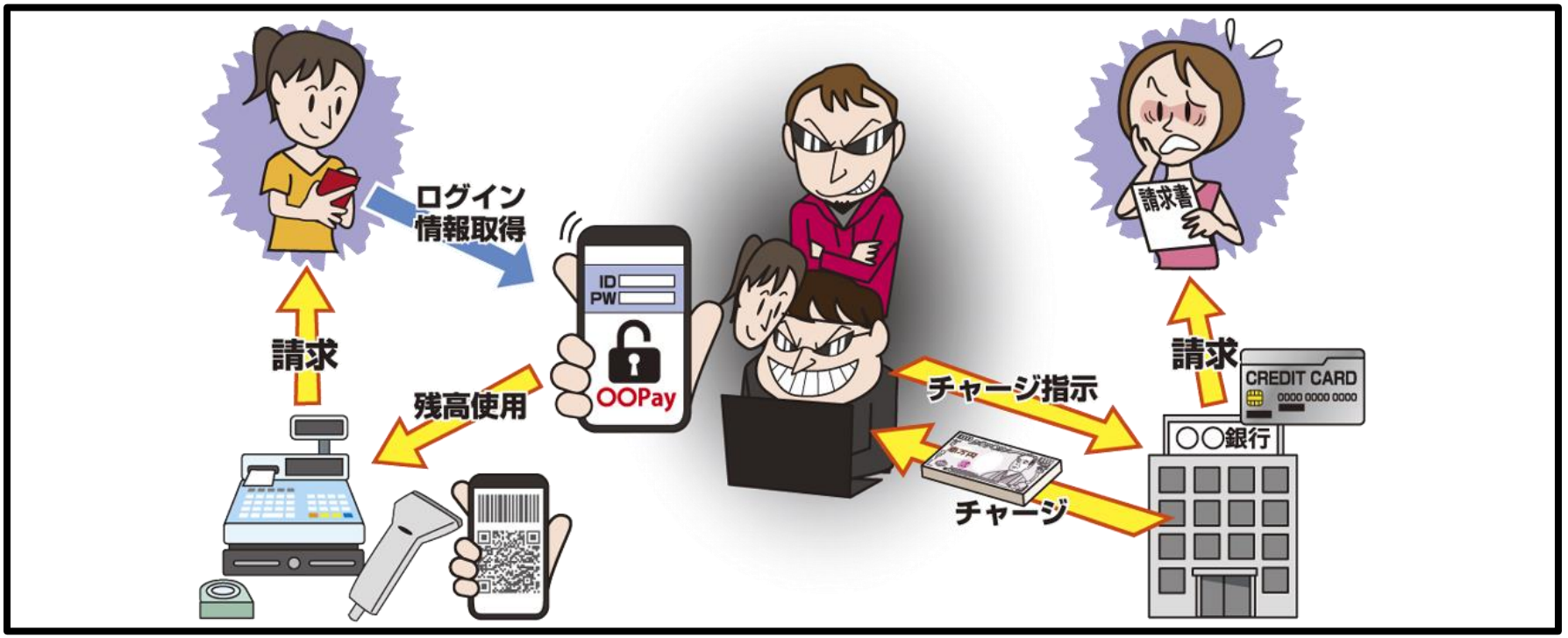
攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視するべき対策を理解する

情報セキュリティ10大脅威 2020
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】スマホ決済の不正利用

～スマホ決済サービス利用時は二要素認証等のセキュリティ機能を有効に～



- 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

【1位】スマホ決済の不正利用

～スマホ決済サービス利用時は二要素認証等のセキュリティ機能を有効に～

● 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
- 二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

【1位】スマホ決済の不正利用

～スマホ決済サービス利用時は二要素認証等のセキュリティ機能を有効に～

● 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

・二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

【1位】スマホ決済の不正利用

～スマホ決済サービス利用時は二要素認証等のセキュリティ機能を有効に～

- 2019年の事例/傾向
  - スマホ決済サービスに不正ログイン(※1)
    - ・登録したクレジットカードからの不正チャージや、チャージ残高の不正利用により、約3,800万円の被害
    - ・不正に入手したIDやパスワードを悪用した可能性が高い

【出典】
※1　認定廃止のセブンペイ、払い戻し受付期限25万人が未申請
https://www.asahi.com/articles/ASN1B5FQKN1BULFA02C.html

【1位】スマホ決済の不正利用

～スマホ決済サービス利用時は二要素認証等のセキュリティ機能を有効に～

- 2019年の事例/傾向
  - 経済産業省によるガイドライン遵守要請(※1)
    - ・経済産業省は決済事業者等に対し、不正利用防止のための各種ガイドラインの遵守とセキュリティレベル向上に努めるよう要請

【出典】
※1 コード決済サービスにおける不正アクセス事案を踏まえ、決済事業者等に対し、不正利用防止のための各種ガイドラインの徹底を求めました
https://www.meti.go.jp/press/2019/07/20190705003/20190705008.html

【1位】スマホ決済の不正利用

～スマホ決済サービス利用時は二要素認証等のセキュリティ機能を有効に～

- 対策
  - 利用者
    - ・被害の予防
      - –パスワードは長く、複雑にする
      - –パスワードの使いまわしをしない
      - –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）
      - –利用頻度が低いサービスや不要なサービスのアカウント削除
      - –過剰なチャージはしない（被害額を抑える）
      - –スマートフォンの盗難・紛失対策

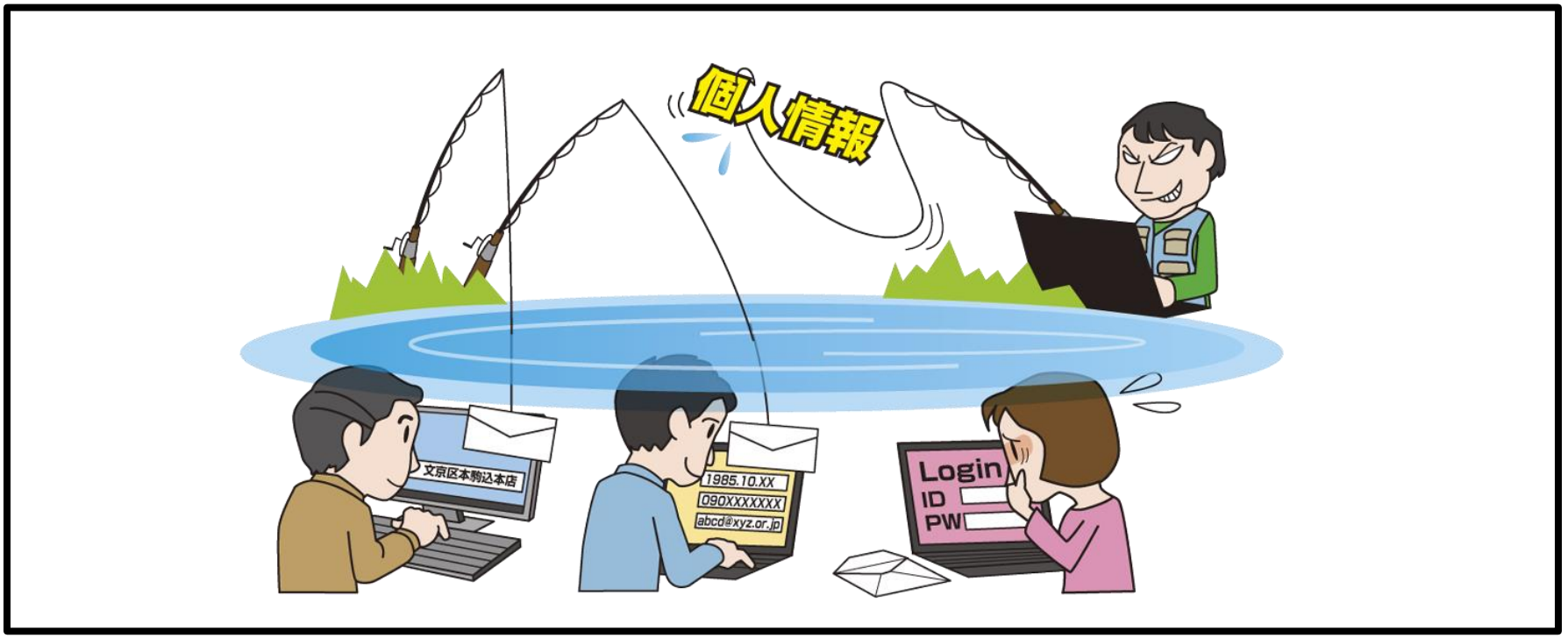
【1位】スマホ決済の不正利用

～スマホ決済サービス利用時は二要素認証等のセキュリティ機能を有効に～

- 対策
  - 利用者
    - ・被害の早期検知
      - –不正なログイン履歴の確認
      - –スマホ決済サービスの利用履歴の確認
      - –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
      - –パスワードの変更
      - –クレジットカードの停止
      - –スマホ決済サービス運営者への連絡

【2位】フィッシングによる個人情報の詐取

～フィッシングの件数は増加傾向、世界的なイベントに便乗したフィッシング詐欺にも注意～



- 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

【2位】フィッシングによる個人情報の詐取

～フィッシングの件数は増加傾向、世界的なイベントに便乗したフィッシング詐欺にも注意～

● 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

■ 有名企業を装ったメールをばらまく

・実在する企業を装いフィッシングサイトへのリンクが記載されたメールやSMS等を送信し、フィッシングサイトへ誘導

・フィッシングサイトで利用者が入力した情報を詐取

■ 二要素認証の情報も入力させる

・ワンタイムパスワード等、二要素認証の情報も入力させて詐取する

【2位】フィッシングによる個人情報の詐取

～フィッシングの件数は増加傾向、世界的なイベントに便乗したフィッシング詐欺にも注意～

IPA

- 2019年の事例/傾向
  - フィッシングの報告件数が増加傾向(※1)
    - 2019年はフィッシングの報告件数が増加傾向
    - 12月は1月の約5倍にあたる8,208件の報告があった
    - 11月までは大手銀行を騙るものが主だったが、12月は地方銀行やネット銀行等を騙るフィッシングも

【出典】
※1 2019/12 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/201912.html

【2位】フィッシングによる個人情報の詐取

～フィッシングの件数は増加傾向、世界的なイベントに便乗したフィッシング詐欺にも注意～

- 2019年の事例/傾向
  - 世界的なイベントに便乗したフィッシング詐欺 (※1)
    - ・世界的な注目を集めたスポーツ大会の無料ライブ動画配信サービスを装ったフィッシングサイトが確認された
    - ・会員登録と称してクレジットカード情報等の入力を求める
    - ・入力した情報は詐取され、不正に利用されるおそれ

【出典】
※1 【注意喚起】ラグビーワールドカップ人気に便乗したフィッシング詐欺に注意
https://is702.jp/news/3568/partner/97_t/

【2位】フィッシングによる個人情報の詐取

～フィッシングの件数は増加傾向、世界的なイベントに便乗したフィッシング詐欺にも注意～

対策

インターネット利用者

・被害の予防
  －メール内のURLを安易にクリックしない
  －受信メールやウェブサイトの十分な確認
・被害の早期検知
  －利用するウェブサイト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等の利用明細を確認
・被害を受けた後の対応
  －パスワードの変更
  －金融機関等への利用停止を連絡
  －信頼できる機関に相談

【3位】クレジットカード情報の不正利用

～ショッピングサイトでのクレジットカード情報の詐取被害が拡大～

- 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

【3位】クレジットカード情報の不正利用

～ショッピングサイトでのクレジットカード情報の詐取被害が拡大～

● 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窃取

・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

・正規ウェブサイト上に偽画面があるため、気付くことが困難

【3位】クレジットカード情報の不正利用

～ショッピングサイトでのクレジットカード情報の詐取被害が拡大～

● 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

【3位】クレジットカード情報の不正利用

～ショッピングサイトでのクレジットカード情報の詐取被害が拡大～

- 2019年の事例/傾向
  - クレジットカード番号の盗用被害が増加（※1）
    - 2019年1月～9月の被害額は167億円（前年同期間は約132億円）
    - クレジットカードの被害額の81.5％が番号盗用による被害
    - 不正利用被害に遭った500人に対するアンケート調査で、被害者の内57.2％は不正利用された原因や手口を把握していない（※2）

【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
https://www.j-credit.or.jp/download/news20191227b.pdf
※1　三井住友カード、クレジットカードの不正利用被害にあった500人に調査
http://www.atpress.ne.jp/releases/202935/att_202935_1.pdf

【3位】クレジットカード情報の不正利用

～ショッピングサイトでのクレジットカード情報の詐取被害が拡大～

- 2019年の事例/傾向
  - 不正ログインによるカードの不正利用(※1)
    - ・会員制のインターネットサービスおよびスマホアプリへの不正ログイン
    - ・不正ログインされた被害者は1,917名、クレジットカードが不正利用されたのは708名、被害総額は2,200万円
    - ・不正ログインはパスワードリスト攻撃によるものと見られる

【出典】
※1 インターネットサービス「暮らしのマネーサイト」での不正ログイン発生のお知らせおよびパスワード変更のお願いについて
https://www.aeon.co.jp/information/201906_info/index.html

【3位】クレジットカード情報の不正利用

～ショッピングサイトでのクレジットカード情報の詐取被害が拡大～

- 対策
  - 利用者
    - ・被害の予防
      - –パスワードの使いまわしをしない
      - –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
      - –受信メールウェブサイトの十分な確認
      - –添付ファイルやURLを安易に開かない
      - –信頼できるインターネットサービスの利用
      - –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

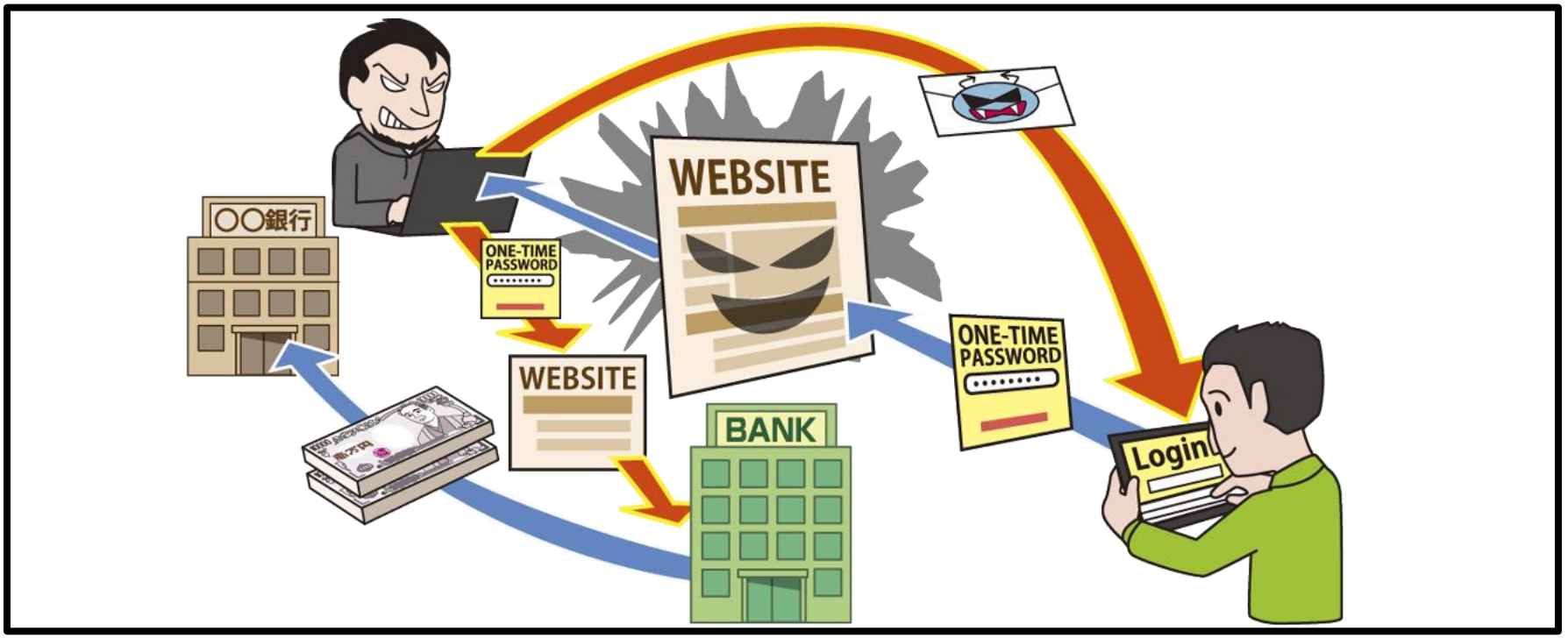
【3位】クレジットカード情報の不正利用

～ショッピングサイトでのクレジットカード情報の詐取被害が拡大～

- 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
      - －該当サービスのコールセンターへの連絡
      - －クレジットカードの再発行
      - －パスワードの変更
      - －ウイルス感染した端末の初期化
      - －警察への被害届の提出

【4位】インターネットバンキングの不正利用

～フィッシングによる不正送金の被害が急増～



- 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

【4位】インターネットバンキングの不正利用

～フィッシングによる不正送金の被害が急増～

● 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

【4位】インターネットバンキングの不正利用

～フィッシングによる不正送金の被害が急増～

- 2019年の事例/傾向
  - インターネットバンキングの不正送金が急増 (※1,※2)
    - ・2019年9月から不正送金が急増
    - ・11月の発生件数は573件、被害額は約7億7,600万円
    - ・2012年以降最多の水準
    - ・原因の多くはフィッシング詐欺によるものとみられる

【出典】
※1 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（全銀協等と連携した注意喚起）
https://www.npa.go.jp/cyber/policy/caution1910.html
※2 平成30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 [H30.9.20掲載]
https://www.npa.go.jp/publications/statistics/cybersecurity/data/H30_kami_cyber_jousei.pdf

【4位】インターネットバンキングの不正利用

～フィッシングによる不正送金の被害が急増～

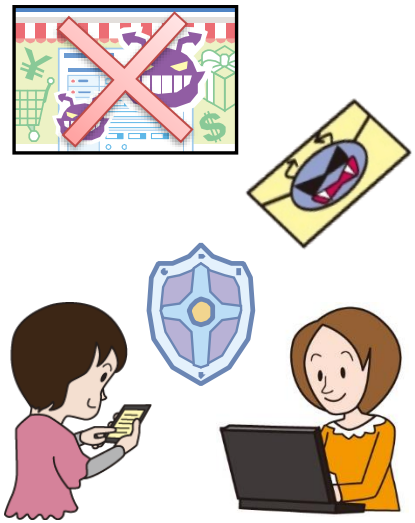
- 2019年の事例/傾向
  - 二要素認証を突破する攻撃が激化(※1)
    - ・二要素認証を突破して不正送金を試みる攻撃の拡大が確認された
    - ・フィッシングサイトで二要素認証で使う情報（ワンタイムパスワード等）を入力させて認証情報を詐取する

【出典】
※1　国内ネットバンキングの二要素認証を狙うフィッシングが激化
https://blog.trendmicro.co.jp/archives/22696

【4位】インターネットバンキングの不正利用

～フィッシングによる不正送金の被害が急増～

- **対策**
  - **利用者**
    - ・被害の予防
      - –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
      - –ファイルの拡張子を表示させる設定
      - –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等の確認
      - –二要素認証等、金融機関が推奨する認証方式の利用

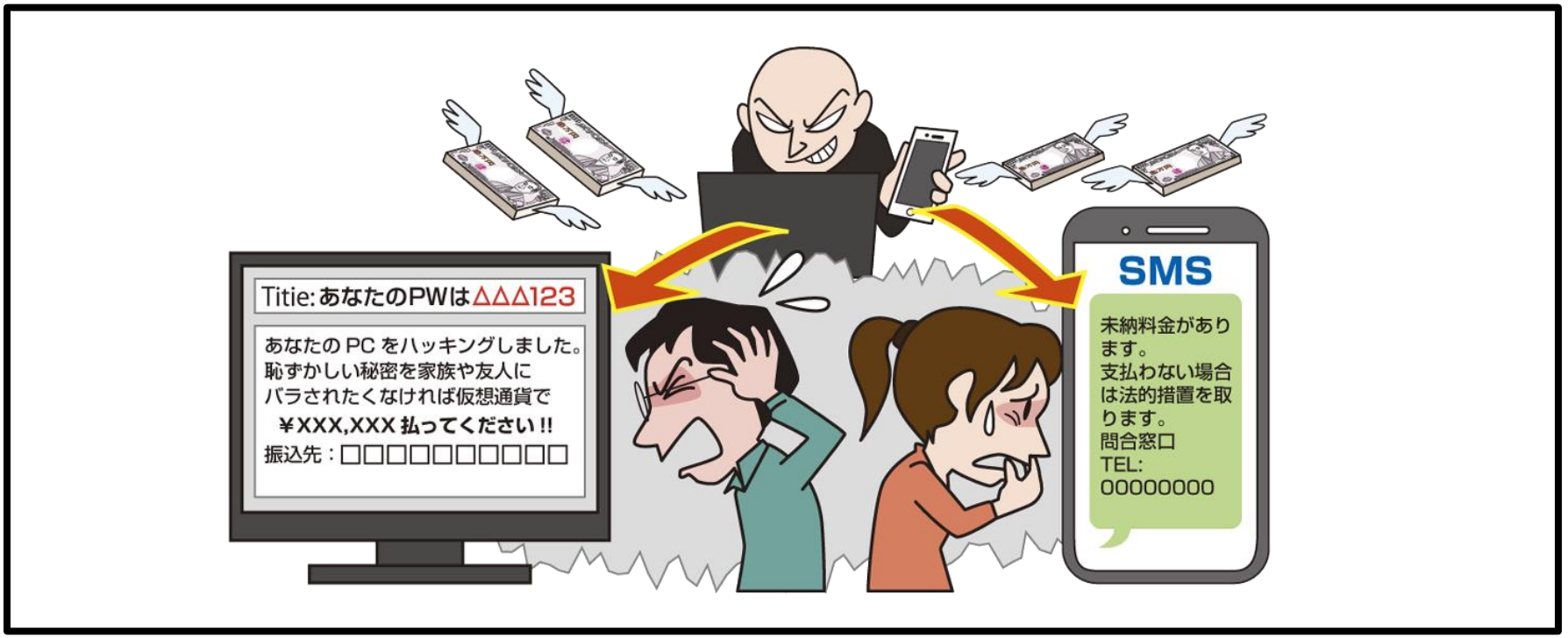


【4位】インターネットバンキングの不正利用

～フィッシングによる不正送金の被害が急増～

- 対策
  - 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等の利用
    - ・被害を受けた後の対応
      - –該当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
      - –パスワードの変更

【5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
～金銭を要求する脅迫・詐欺メールは無視を～



- 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等を送り付ける
- 受信者は脅迫を受けて不安になり金銭を支払ってしまう
- 脅迫内容は事実に基づいていないケースが多い

【5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
～金銭を要求する脅迫・詐欺メールは無視を～

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（仮想通貨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」、「アダルト動画を見られる有料サイトを使用した料金が未納である」等、被害者が周囲に相談しにくい内容で脅迫する

【5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
～金銭を要求する脅迫・詐欺メールは無視を～

- 攻撃手口

・脅し、騙しのメールを送り付け金銭を要求

- 脅し文句の中に受信者の情報を記載する
  - ・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
- 電話窓口へ誘導する
  - ・脅迫メール等に電話番号を記載し、電話を掛けさせる
  - ・電話を掛けてきた被害者に対し、電話口で更に脅迫や催促を行う

【5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
～金銭を要求する脅迫・詐欺メールは無視を～

- 2019年の事例/傾向
  - 探偵社を装った脅迫メール(※1)
    - ・探偵社の調査員を名乗り金銭を要求する脅迫メール
    - ・メール本文の日本語は不自然な文章
    - ・他のクライアントからの調査依頼で得た秘密を家族に知らせると脅迫
    - ・支払い方法として仮想通貨での支払いを要求

【出典】
※1　探偵社を装って「貴方の秘密をばらす」と脅迫、ビットコインを要求してくるメールが拡散中、件名は「仕事のご健闘を祈り致します。」
https://internet.watch.impress.co.jp/docs/news/1201267.html

【5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
～金銭を要求する脅迫・詐欺メールは無視を～

- 2019年の事例/傾向
  - 偽の消費生活センター相談窓口へ誘導する新手口(※1)
    - ・攻撃者が有料サイトの料金が未納であるという脅迫メールを送信し、被害者から電話を掛けさせる
    - ・電話で更に偽の消費生活センターへ誘導し、そこへ電話を掛けさせて料金未納が事実であると信じ込ませる

【出典】
※1 “ニセ”消費生活センターを案内する新手の架空請求の手口にご注意！
http://www.kokusen.go.jp/news/data/n-20190718_1.html

【5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
～金銭を要求する脅迫・詐欺メールは無視を～

- 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

※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

・被害を受けた後の対応

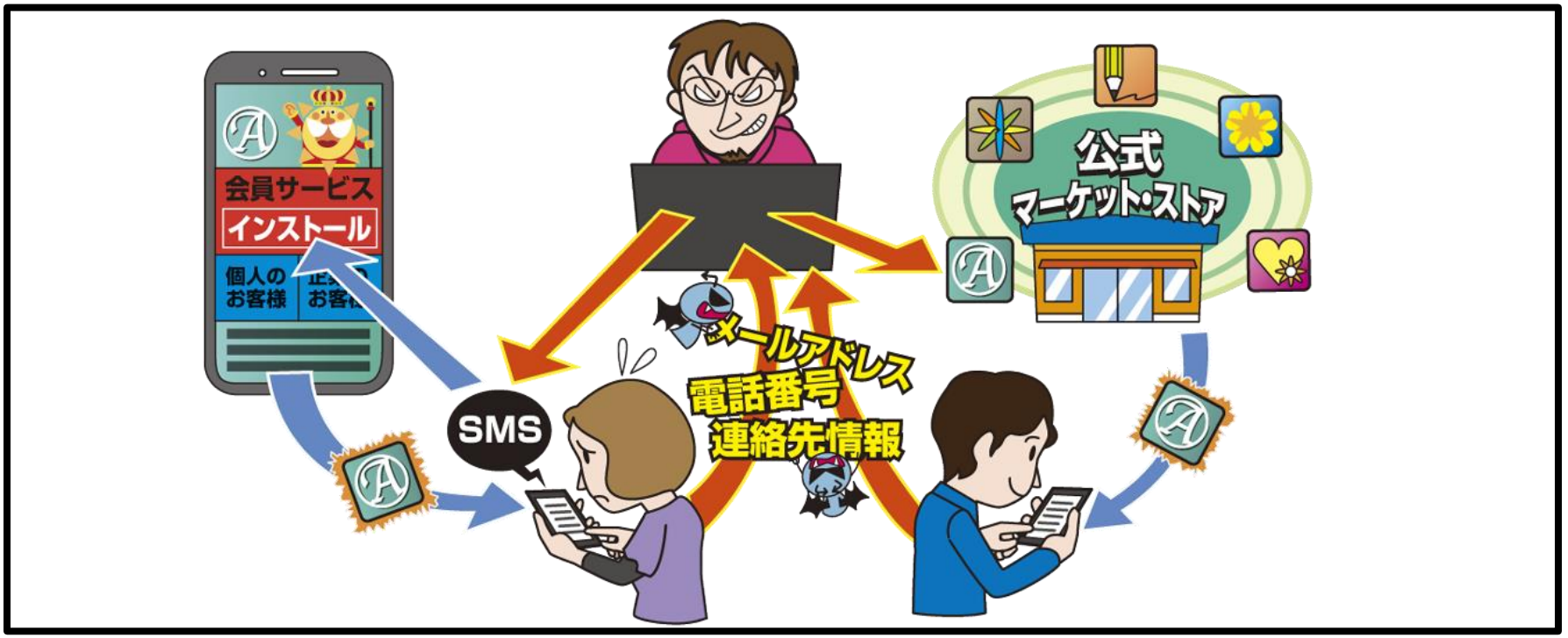
－パスワードを変更する

※脅迫・詐欺メールに記載されたパスワードが自分のもの
と一致しているのであれば、どこかからパスワードが漏えい
したおそれがある

－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

～インストールしているのは本当に正規のアプリ？～



- 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

～インストールしているのは本当に正規のアプリ？～

● 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

・公式マーケットは安全だと考える利用者を狙う

■ 不正アプリのダウンロードサイトへ誘導

・実在の企業をかたってメールや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

・正規のアプリであると誤認させて不正アプリを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

～インストールしているのは本当に正規のアプリ？～

● 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

■ 不正アプリをインストールしてしまうと様々な被害が

- ・連絡先等の端末内の重要な情報を窃取される
- ・仮想通貨のマイニングに利用される
- ・端末の一部機能（録画、写真、録音など）を不正に利用される
- ・DDoS攻撃や悪意あるSMSの拡散等の踏み台に利用される

【6位】不正アプリによるスマートフォン利用者への被害

～インストールしているのは本当に正規のアプリ？～

- 2019年の事例/傾向
  - 郵便サービスを騙ったSMSによる誘導 (※1)
    - 偽の不在通知をスマートフォン利用者に対してSMSで送信
    - SMSに記載されたURLにAndroid端末でアクセスすると、不正なアプリがダウンロードされる
    - iPhoneでアクセスした場合はApple IDの入力を求めるフィッシングサイトへ誘導される

【出典】
※1 当社の名前を装った迷惑メール及び架空Webサイトにご注意ください。
https://www.post.japanpost.jp/notification/notice/2019/1031_01.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

～インストールしているのは本当に正規のアプリ？～

- 2019年の事例/傾向
  - 不正アプリで窃取した電話番号を詐欺に利用（※1）
    - 宅配業者を装ったSMSに記載されたURLにアクセスした被害者のスマートフォンに、不正アプリがダウンロードされ、電話番号が窃取された
    - 窃取された電話番号はスマホ決済サービスのアカウント作成に利用された
    - さらにそのスマホ決済サービスに第三者のクレジットカードを登録して不正利用

【出典】
※1　宅配業者装うSMSに注意スマホ乗っ取られ詐欺に悪用
https://www.asahi.com/articles/ASM663JGXM66OIPE00G.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

～インストールしているのは本当に正規のアプリ？～

- 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

–アクセス権限の確認

–アプリインストールに関する設定に注意

※Androidの端末では提供元不明のアプリのインストールを許可しない

※iPhoneでは信頼されていないエンタープライズデベロッパを信頼しない

–不要なアプリをインストールしない

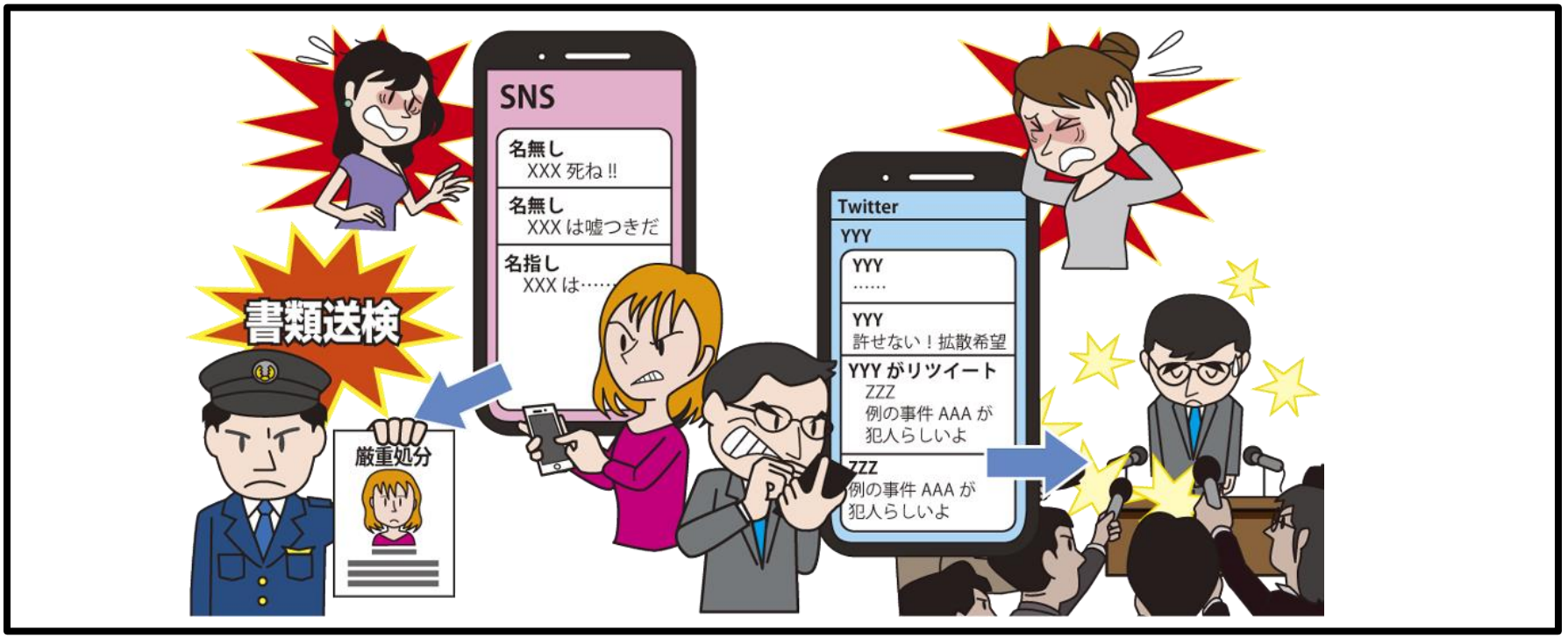
・被害を受けた後の対応

–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

【7位】ネット上の誹謗・中傷・デマ

～安易な拡散により、他者も自身も不幸に～



- 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
- 嘘情報（フェイクニュース等）が安易に拡散されることで大きな問題になる

【7位】ネット上の誹謗・中傷・デマ

～安易な拡散により、他者も自身も不幸に～

IPA

● 要因

・情報モラルの欠如、匿名性の悪用

■ 情報モラルや自己抑制力の欠如

・恨みや妬み等から湧く攻撃的な感情や、ストレス発散等の身勝手な理由での感情を、そのまま発信してしまう。

・自分の発言が他者や社会に及ぼす影響を気にすることなく、安易にネットに投稿してしまう

■ 個人が匿名で発信できる場の増加

・匿名性を利用し、普段は人前で言えないようなことを安易に発信しやすい（匿名でも裁判所命令等に基づき発信者情報の開示請求を行えば身元を特定できる場合が多い）

【7位】ネット上の誹謗・中傷・デマ

～安易な拡散により、他者も自身も不幸に～

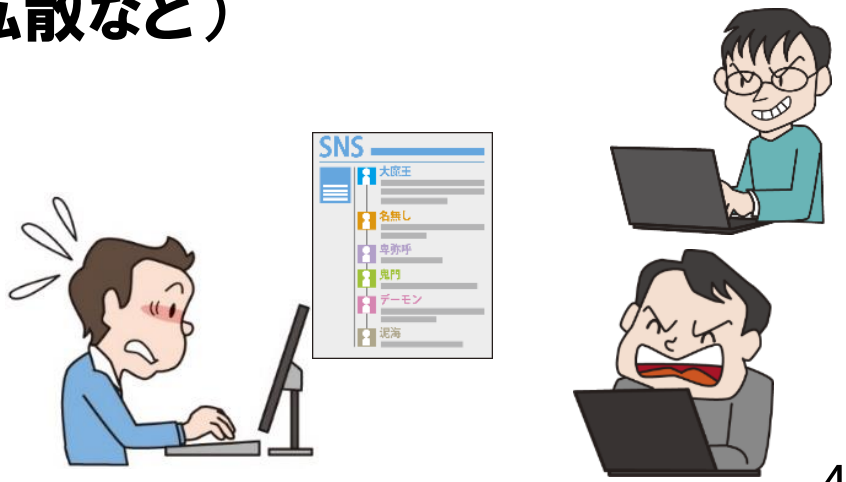
● 要因

・インターネット上の情報を安易に信じてしまう

■ 情報の真偽を確認せずに拡散

・インターネット上にある多くの嘘情報や真偽不明な情報を真偽を確かめることなく拡散してしまう

・有用な情報を周知してあげたいという親切心や正義感による場合も多い（災害情報の拡散など）



【7位】ネット上の誹謗・中傷・デマ

～安易な拡散により、他者も自身も不幸に～

- 2019年の事例/傾向
  - デマを拡散した市議、名誉棄損で提訴され辞職(※1)
    - ・世間で注目を浴びた事件の関係者として、無関係な女性の名前や顔写真がネット上で拡散される事例が発生
    - ・デマ情報を信じて拡散した市議を、当該女性が名誉棄損で提訴し、市議は謝罪会見を行ったうえで辞職

【出典】
※1　あおり運転「デマ拡散」で訴えられた豊田市議、“私も被害者”と独特な持論を展開
https://news.livedoor.com/article/detail/17382809/

【7位】ネット上の誹謗・中傷・デマ

～安易な拡散により、他者も自身も不幸に～

- 2019年の事例/傾向
  - 芸能人に対する誹謗・中傷で主婦書類送検 (※1)
    - ・芸能人のブログに対し「死ね」「消えろ」等の誹謗中傷を何度も書き込んだとして、50代の主婦を脅迫容疑で書類送検
    - ・「みんな書いてる」、「たたく人が多いのでなんとなく」等の理由で書き込んだと主張

【出典】
※1　堀ちえみのブログに誹謗中傷「死ね消えろ」、50代主婦が書類送検
https://www.sanspo.com/geino/news/20190717/sca19071705030001-n1.html

【7位】ネット上の誹謗・中傷・デマ

～安易な拡散により、他者も自身も不幸に～

対策

投稿者

・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

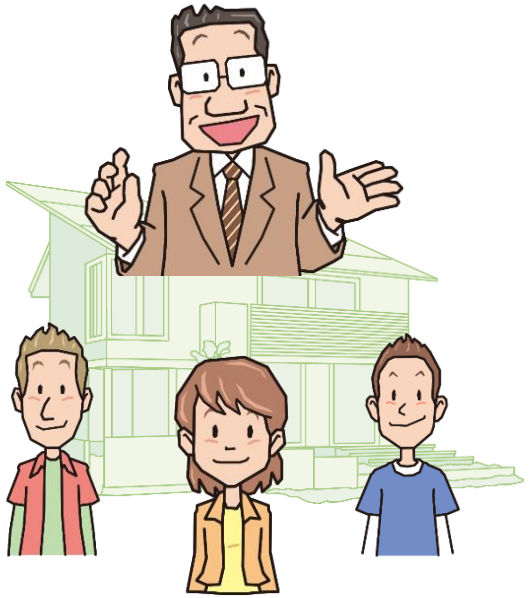
－投稿前に内容を再確認

家庭、教育機関

・情報モラル、情報リテラシーの教育

－自宅や学校で子供たちに情報モラルや
情報リテラシーの教育を行う

－トラブルの事例を伝え、悪質な行為は
犯罪になりうることを理解させる



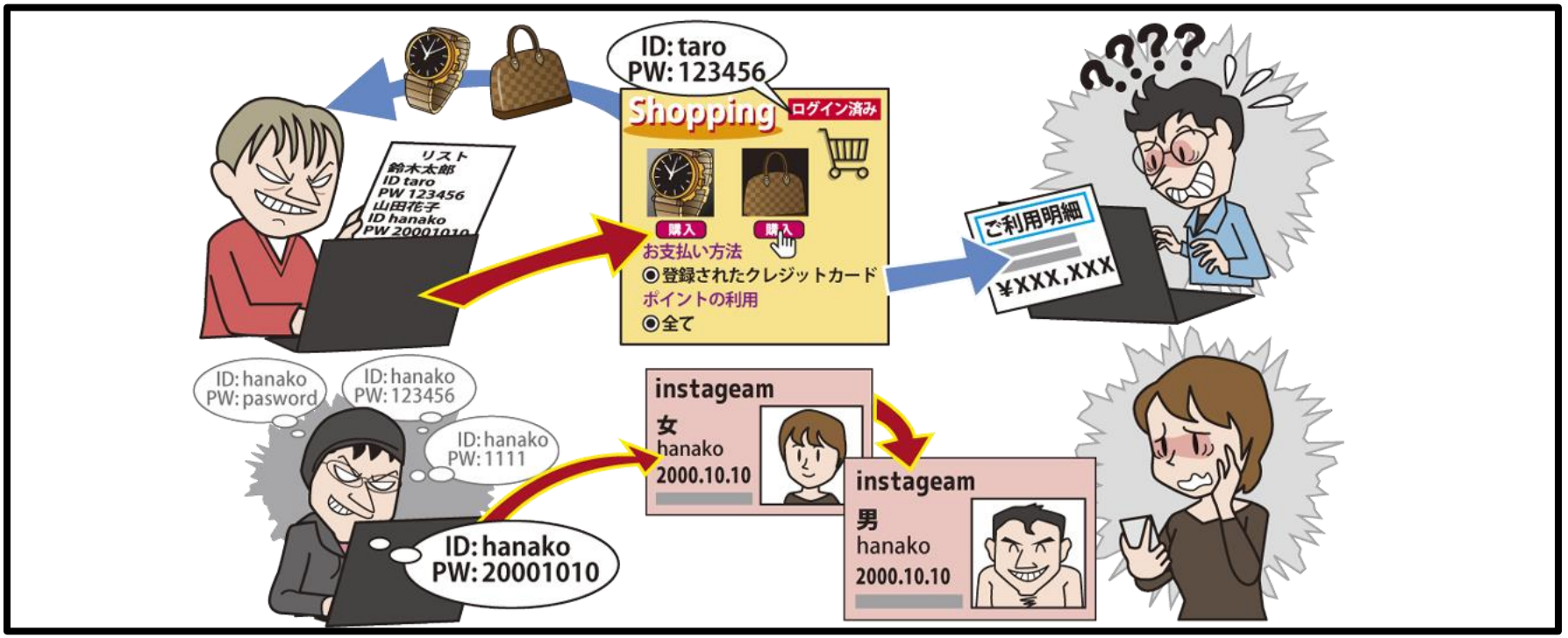
【7位】ネット上の誹謗・中傷・デマ

～安易な拡散により、他者も自身も不幸に～

- 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
      - －安易な拡散をしない
  - 被害者
    - ・被害を受けた後の適切な対応
      - －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
    - ・管理者やプロバイダーへ情報削除依頼
      - ※削除により炎上の火種になるおそれもあるため、関係者等に相談して慎重に行う

【8位】インターネット上のサービスへの不正ログイン

～パスワードリスト攻撃による不正ログインが横行～



- 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
- 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

【8位】インターネット上のサービスへの不正ログイン

～パスワードリスト攻撃による不正ログインが横行～

● 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

【8位】インターネット上のサービスへの不正ログイン

～パスワードリスト攻撃による不正ログインが横行～

● 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

【8位】インターネット上のサービスへの不正ログイン

～パスワードリスト攻撃による不正ログインが横行～

- 2019年の事例/傾向
  - パスワードリスト攻撃で個人情報約46万件流出 (※1)
    - ・複数のオンラインストアにおいて、46万件のアカウントにパスワードリスト攻撃による不正ログインが行われた
    - ・不正ログインされたアカウントでは個人情報が閲覧されたおそれがある

【出典】
※1 「リスト型アカウントハッキング(リスト型攻撃)」による弊社オンラインストアサイトへの不正ログインの発生とパスワード変更のお願いについて
https://www.uniqlo.com/jp/corp/pressrelease/2019/05/19051409_uniqlo.html

【8位】インターネット上のサービスへの不正ログイン

～パスワードリスト攻撃による不正ログインが横行～

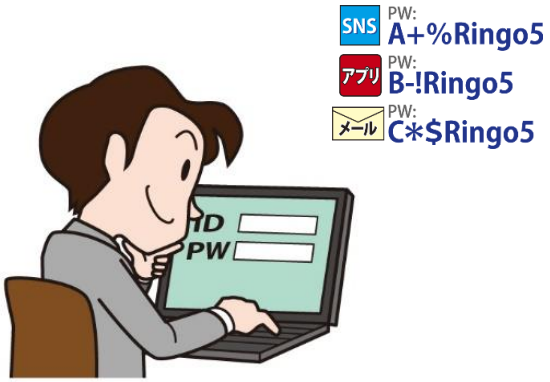
- 2019年の事例/傾向
  - SNSの乗っ取り被害（※1）
    - ・有名歌手のインスタグラムの公式アカウントが不正ログインされ、乗っ取られた
    - ・プロフィール画像が変更される、無関係な動画が投稿される等の被害があった

【出典】
※1 PUFFY大貫亜美インスタ乗っ取り被害「対応中」
https://www.nikkansports.com/entertainment/news/201907280000671.html

【8位】インターネット上のサービスへの不正ログイン

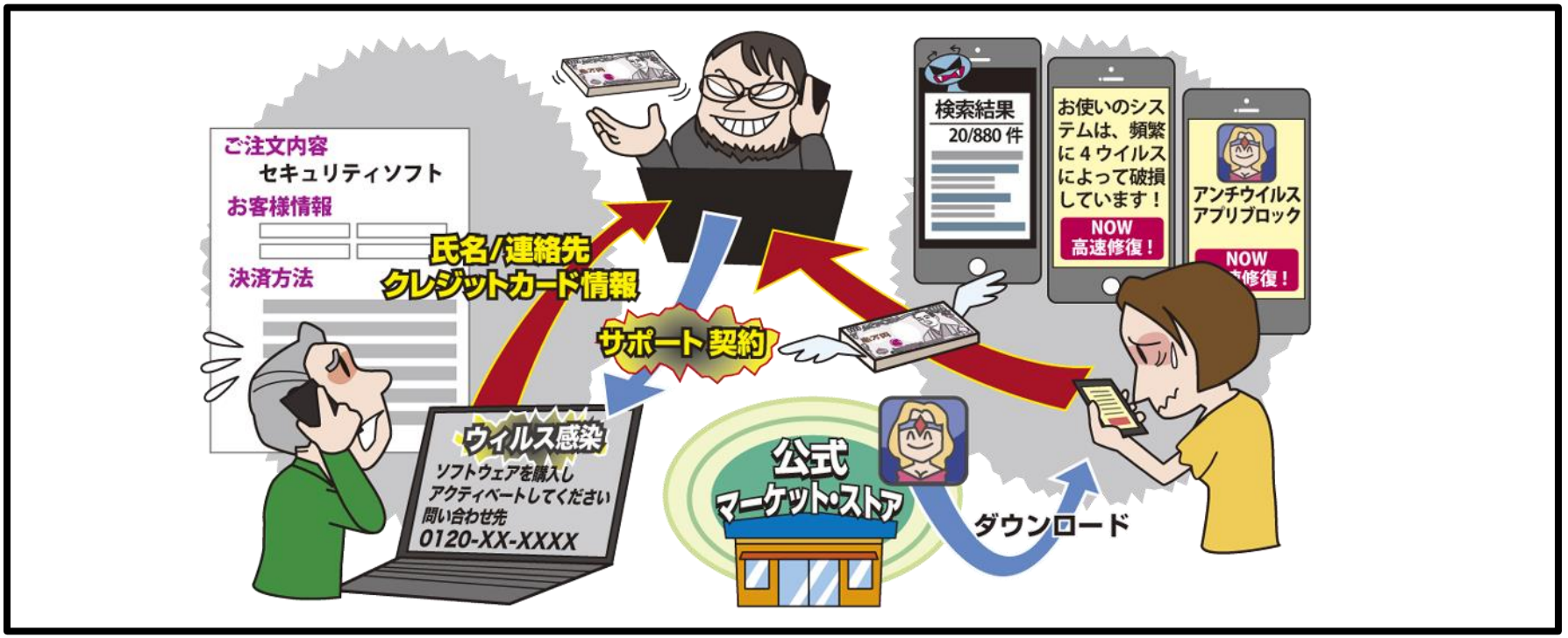
～パスワードリスト攻撃による不正ログインが横行～

- 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
      - –パスワードの使いまわしをしない
      - –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
      - –利用していないサービスからの退会
    - ・被害を受けた後の対応
      - –パスワードの変更
      - –クレジットカードの停止
      - –不正ログインされたサービスの運営者へ連絡



【9位】偽警告によるインターネット詐欺

～落ち着いて！あの手この手の騙しの警告画面～



- 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

【9位】偽警告によるインターネット詐欺

～落ち着いて！あの手この手の騙しの警告画面～

● 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警告

・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

【9位】偽警告によるインターネット詐欺

～落ち着いて！あの手この手の騙しの警告画面～

● 攻撃手口

・偽警告に記載した誘導に従わせる

■ 偽対策ソフト（偽セキュリティソフト）

・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

■ サポート契約詐欺

・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

■ 偽警告スマホ版

・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

【9位】偽警告によるインターネット詐欺

～落ち着いて！あの手この手の騙しの警告画面～

- 2019年の事例/傾向
  - 破棄されたドメインを悪用した偽警告 (※1)
    - ・宮城県が運用していた旧サイトのURLにアクセスすると、システム破損の偽警告が表示されるようになっていた
    - ・旧サイトの閉鎖後に手放されたドメインを攻撃者が取得して不正なサイトを作成していた

【出典】
※1　令和元年度「東北文化の日」推進事業について-宮城県公式ウェブサイト
https://www.pref.miyagi.jp/soshiki/syoubun/tohokubunka-2019.html

【9位】偽警告によるインターネット詐欺

～落ち着いて！あの手この手の騙しの警告画面～

- 2019年の事例/傾向
  - スマートフォンでの偽警告の相談が増加 (※1)
    - ・IPA安心相談窓口に寄せられる偽警告に関する相談のうち、スマートフォンにおける偽警告の相談が2019年6月から増加
    - ・インストールさせられるアプリケーションの中には、自動継続課金のものがあり、料金請求を止めるにはアンインストールの他に別途手続きが必要となる

【出典】
※1 IPA 安心相談だより「スマートフォンで偽のセキュリティ警告からアプリのインストールへ誘導する手口に注意」
https://www.ipa.go.jp/security/anshin/mgdayori20190918.html

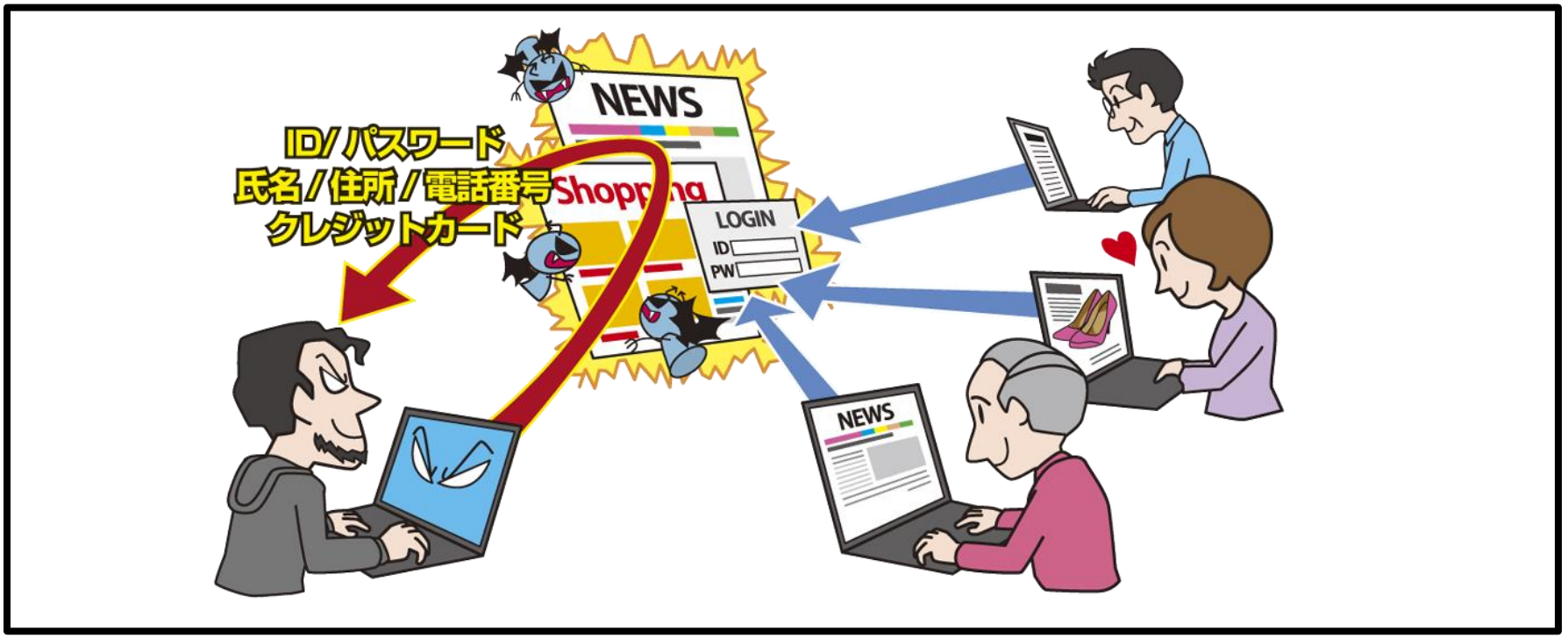
【9位】偽警告によるインターネット詐欺

～落ち着いて！あの手この手の騙しの警告画面～

- 対策
  - インターネット利用者
    - ・被害の予防
      - －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
      - －警告が本物か偽物かの判断は冷静に
    - ・被害を受けた後の対応
      - －ソフトウェアをアンインストール
        ※できない場合は端末を初期化
      - －サポート契約の解消（近くの消費生活センターへ相談）
      - －自動継続課金の停止
      - －クレジットカード会社へ連絡

【10位】インターネット上のサービスからの個人情報の窃取

～会員サイトやショッピングサイトから情報流出するおそれ～



- 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

【10位】インターネット上のサービスからの個人情報の窃取

～会員サイトやショッピングサイトから情報流出するおそれ～

● 攻撃手口

・サービスの脆弱性や設定不備を悪用

■ 脆弱性を悪用した攻撃

・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

■ 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

【10位】インターネット上のサービスからの個人情報の窃取

～会員サイトやショッピングサイトから情報流出するおそれ～

● 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

【10位】インターネット上のサービスからの個人情報の窃取

～会員サイトやショッピングサイトから情報流出するおそれ～

- 2019年の事例/傾向
  - 不正アクセスによりクレジットカード情報流出（※1）
    - ・オンラインストアが不正アクセスを受けた
    - ・決済アプリケーションが改ざんされ、入力した情報が窃取される状態に
    - ・改ざんされていた約1ヶ月の間に約3万7,000件のクレジットカード情報が流出し、一部が不正利用されたおそれがある

【出典】
※1　弊社が運営する「ヤマダウエブコム・ヤマダモール」への不正アクセスによる個人情報流出に関するお詫びとお知らせ
https://www.yamada-denki.jp/information/190529/

【10位】インターネット上のサービスからの個人情報の窃取

～会員サイトやショッピングサイトから情報流出するおそれ～

- 2019年の事例/傾向
  - 窃取されたメールアドレス宛に詐欺メール（※1）
    - ・オンラインストアが不正アクセスを受け、メールアドレス等の個人情報が最大約28万件流出した
    - ・システムの一部の脆弱性を突いた攻撃と見られる
    - ・窃取されたメールアドレス宛にQUOカードの当選詐欺メールが送信され、メールで誘導された偽サイトでクレジットカード情報等を入力した場合、その情報を窃取されたおそれがある

【出典】
※1 【重要】個人情報流出についてのお知らせ（象印でショッピング）
https://www.zojirushi.co.jp/important/info/01.html

【10位】インターネット上のサービスからの個人情報の窃取

～会員サイトやショッピングサイトから情報流出するおそれ～

- 対策
  - インターネット利用者
    - ・情報モラルやリテラシーの向上
      - –不要な情報は安易に登録しない
      - –利用していないサービスの退会
      - –不正ログイン対策
        （個人8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
    - ・被害を受けた後の対応
      - –サービス運営者への問合せ
      - –クレジットカードの停止
      - –パスワードの変更
      - –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　2020

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/10threats2020.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