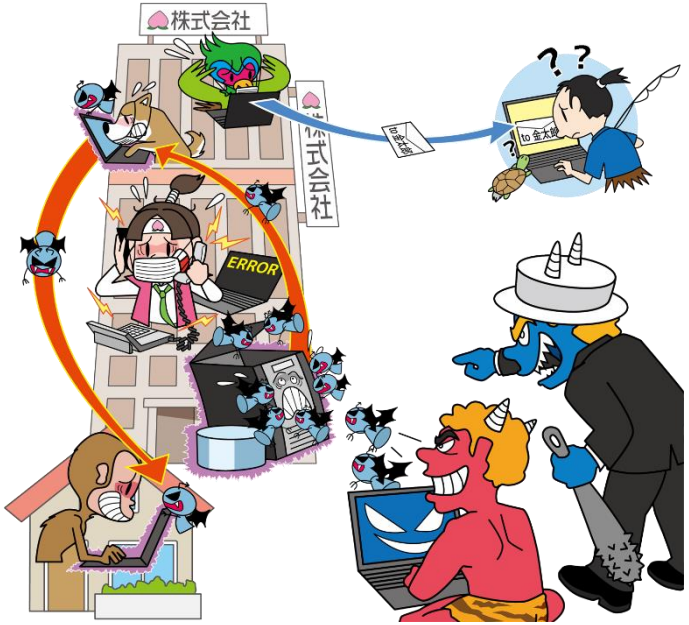
IPA Better Life with IT

情報セキュリティ10大脅威　2021

～よもや自組織が被害に！呼吸を合わせて全力防御！～

［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
2021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 2021 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	ランサムウェアによる被害
フィッシングによる個人情報等の詐取	2	標的型攻撃による機密情報の窃取
ネット上の誹謗・中傷・デマ	3	テレワーク等の ニューノーマルな働き方を狙った攻撃
メールやSMS等を使った脅迫・詐欺の手口 による金銭要求	4	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	5	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	6	内部不正による情報漏えい
インターネット上のサービスからの 個人情報の窃取	7	予期せぬIT基盤の障害に伴う業務停止
偽警告によるインターネット詐欺	8	インターネット上のサービスへの不正ログイン
不正アプリによる スマートフォン利用者への被害	9	不注意による情報漏えい等の被害
インターネット上のサービスへの不正ログイン	10	脆弱性対策情報の公開に伴う悪用増加

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

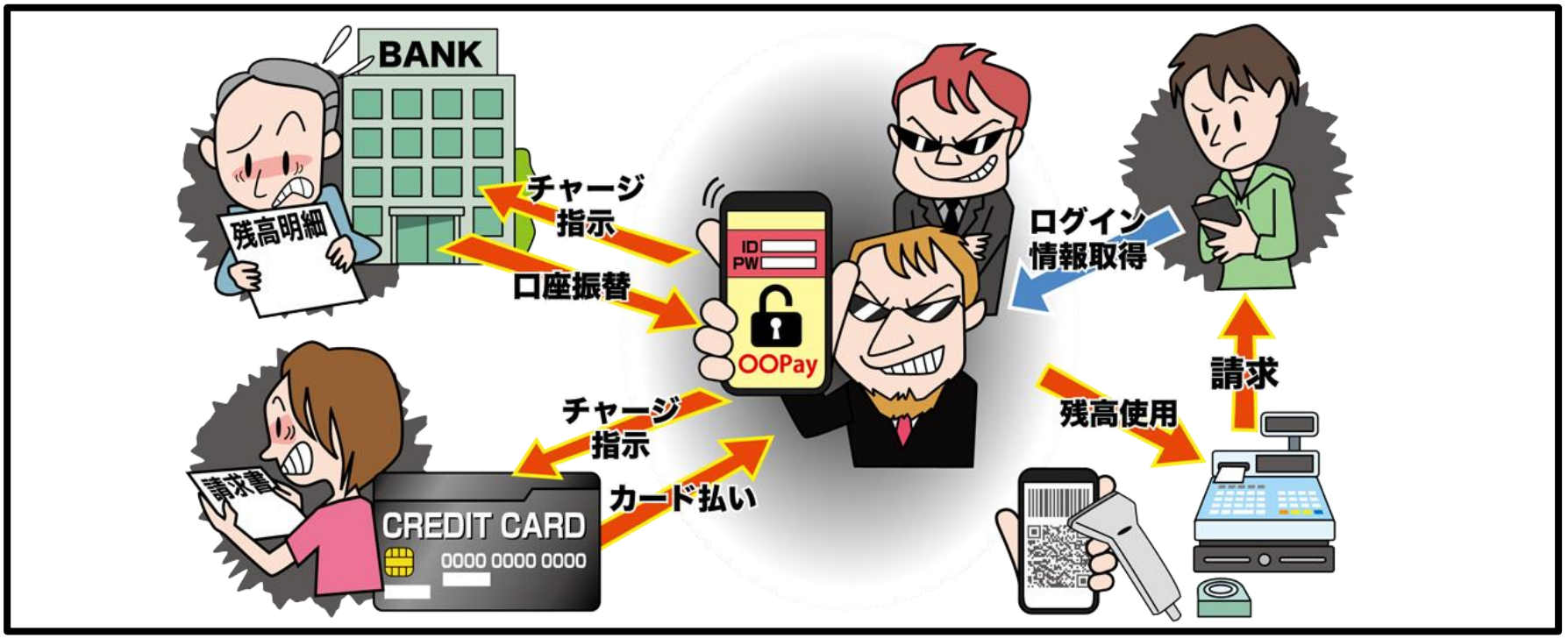
攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視するべき対策を理解する

情報セキュリティ10大脅威 2021
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

～スマホ決済の不正利用被害に備え利用状況の確認を～



- 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

【1位】スマホ決済の不正利用

～スマホ決済の不正利用被害に備え利用状況の確認を～

IPA

● 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

～スマホ決済の不正利用被害に備え利用状況の確認を～

● 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

・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

～スマホ決済の不正利用被害に備え利用状況の確認を～

- 2020年の事例/傾向
  - スマホ決済サービスで他人の口座から不正引き出し(※1)
    - ・他人のスマホ決済サービスに銀行口座から不正に残高をチャージ(入金)されてしまう被害が確認された
    - ・攻撃者は他人の口座番号や生年月日などの情報をスマホ決済サービスの自分のアカウントに紐付け、不正にチャージしたとみられる

【出典】
※1 ペイペイ悪用、他人の預金詐取＝不正チャージ疑いで2人逮捕―警視庁
https://sp.m.jiji.com/article/show/2476202

【1位】スマホ決済の不正利用

～スマホ決済の不正利用被害に備え利用状況の確認を～

- 2020年の事例/傾向
  - スマホ決済サービスと連携する銀行口座から不正引き出し(※1)
    - スマホ決済サービスと銀行口座を連携してウェブ上で口座振替を行う手続きの不備を悪用され、銀行口座から不正な引き出しをされる被害が確認された

【出典】
※1 LINE Payでもゆうちょ銀行から不正引き出し
https://www.itmedia.co.jp/business/articles/2009/16/news075.html

【1位】スマホ決済の不正利用

～スマホ決済の不正利用被害に備え利用状況の確認を～

- **対策**
  - **スマホ決済サービスの利用者**
    - ・被害の予防
      - –強い認証方式の利用
      - –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
      - –認証に不備がある銀行口座と連携しない
      - –不審なウェブサイトで安易に認証情報を入力しない（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

～スマホ決済の不正利用被害に備え利用状況の確認を～

- 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機能の利用
      - –スマホ決済サービスの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
      - –パスワードの変更
      - –スマホ決済サービス運営者への連絡
      - –連携する金融機関への連絡
      - –警察への連絡
      - –二要素認証等の追加設定

【2位】フィッシングによる個人情報等の詐取

～コロナ禍の生活の変化に乗じてオンラインショッピングに関連するフィッシングが急増～

- 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等の詐取

～コロナ禍の生活の変化に乗じてオンラインショッピングに関連するフィッシングが急増～

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

■ 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
- 正規のウェブサイトの問い合わせフォームの自動返信機能を悪用してメールをばらまく方法も
- 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

【2位】フィッシングによる個人情報等の詐取

～コロナ禍の生活の変化に乗じてオンラインショッピングに関連するフィッシングが急増～

- 2020年の事例/傾向
  - 特別定額給付金に便乗したフィッシング（※1,※2）
    - 新型コロナウイルス感染症に係る特別定額給付金の申請用のウェブサイトを偽装したフィッシングサイトが確認された
    - 申請手続きの代行を装って、重要情報等を詐取する事例も
    - 総務省が注意喚起を行った

【出典】
※1　特別定額給付金の給付を騙ったメールに対する注意喚起
https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000438.html
※2　特別定額給付金に関する通知を装うフィッシング（2020/10/19）
https://www.antiphishing.jp/news/alert/kyufukin_20201019.html

【2位】フィッシングによる個人情報等の詐取

～コロナ禍の生活の変化に乗じてオンラインショッピングに関連するフィッシングが急増～

- 2020年の事例/傾向
  - 報告件数は依然として増加傾向 (※1)
    - ・2020年はフィッシングメールの配信頻度が増加傾向
    - ・フィッシングの報告件数も過去最多となった
    - ・ショッピングサイトや金融機関、クレジットカードブランド等を騙るフィッシングが継続して報告され、宅配業者の不在通知を装ったSMSを悪用する事例も確認されている
    - ・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 2020/12 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202012.html

【2位】フィッシングによる個人情報等の詐取

～コロナ禍の生活の変化に乗じてオンラインショッピングに関連するフィッシングが急増～

対策

インターネット利用者

・被害の予防
- 二要素認証を利用
- メール、SMS、SNSの投稿内の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
- 利用しているサービスへの利用停止を連絡
- 信頼できる機関に相談

【3位】ネット上の誹謗・中傷・デマ

～安易な書き込みが、他者と自分の人生を脅かす～

- 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

【3位】ネット上の誹謗・中傷・デマ

～安易な書き込みが、他者と自分の人生を脅かす～

● 要因

・情報モラルの欠如、匿名性の悪用

■ 影響を考慮しないインターネット上への発信

・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考慮せずに、インターネット上に発信してしまう

■ 匿名性を過信した安易な発信

・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）

【3位】ネット上の誹謗・中傷・デマ

～安易な書き込みが、他者と自分の人生を脅かす～

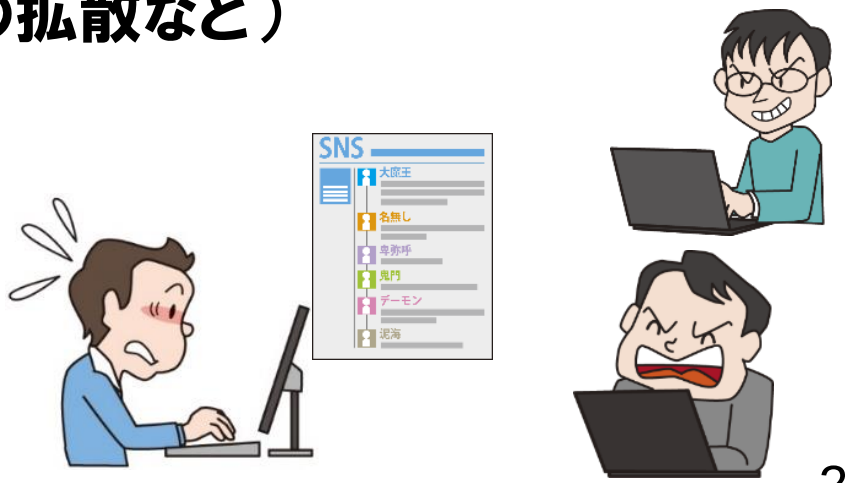
● 要因

・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）



【3位】ネット上の誹謗・中傷・デマ

～安易な書き込みが、他者と自分の人生を脅かす～

- 2020年の事例/傾向
  - 新型コロナウイルスに感染していると虚偽の書き込み（※1）
    - 商店関係者が新型コロナウイルスに感染しているという虚偽の情報を、ネット掲示板に書き込む事例が発生
    - 名前を書き込まれた商店には、複数回の無言電話、風評被害による売り上げの減少といった被害が確認された

【出典】
※1 コロナ感染とネットに虚偽業務妨害容疑で会社員逮捕福島県警
https://www.sankei.com/affairs/news/200527/afr2005270010-n1.html

【3位】ネット上の誹謗・中傷・デマ

～安易な書き込みが、他者と自分の人生を脅かす～

- 2020年の事例/傾向
  - テレビ番組出演者に対する誹謗・中傷（※1）
    - ・バラエティ番組の出演者が、SNS上で相次いだ誹謗・中傷によって精神的苦痛を受け、亡くなる事件が発生
    - ・SNSで誹謗・中傷を書き込んでいた男性が侮辱容疑で書類送検された
    - ・事件後、多くの誹謗・中傷コメントや書き込んだアカウントが投稿者によって削除されたが、コメントの画像が被害者によって保存されており、警察は捜査を継続する方針

【出典】
※1 「テラハ」木村花さんを侮辱の疑い20代男「復讐で」
https://www.asahi.com/articles/ASNDK33MCNDKUTIL009.html

【3位】ネット上の誹謗・中傷・デマ

～安易な書き込みが、他者と自分の人生を脅かす～

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

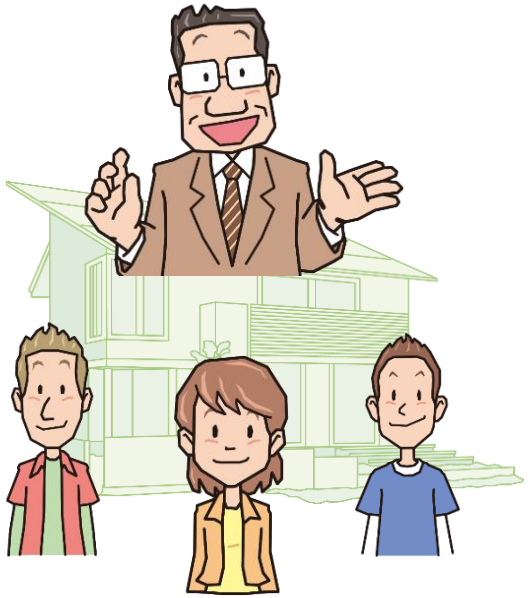
－投稿前に内容を再確認

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



【3位】ネット上の誹謗・中傷・デマ

～安易な書き込みが、他者と自分の人生を脅かす～

対策

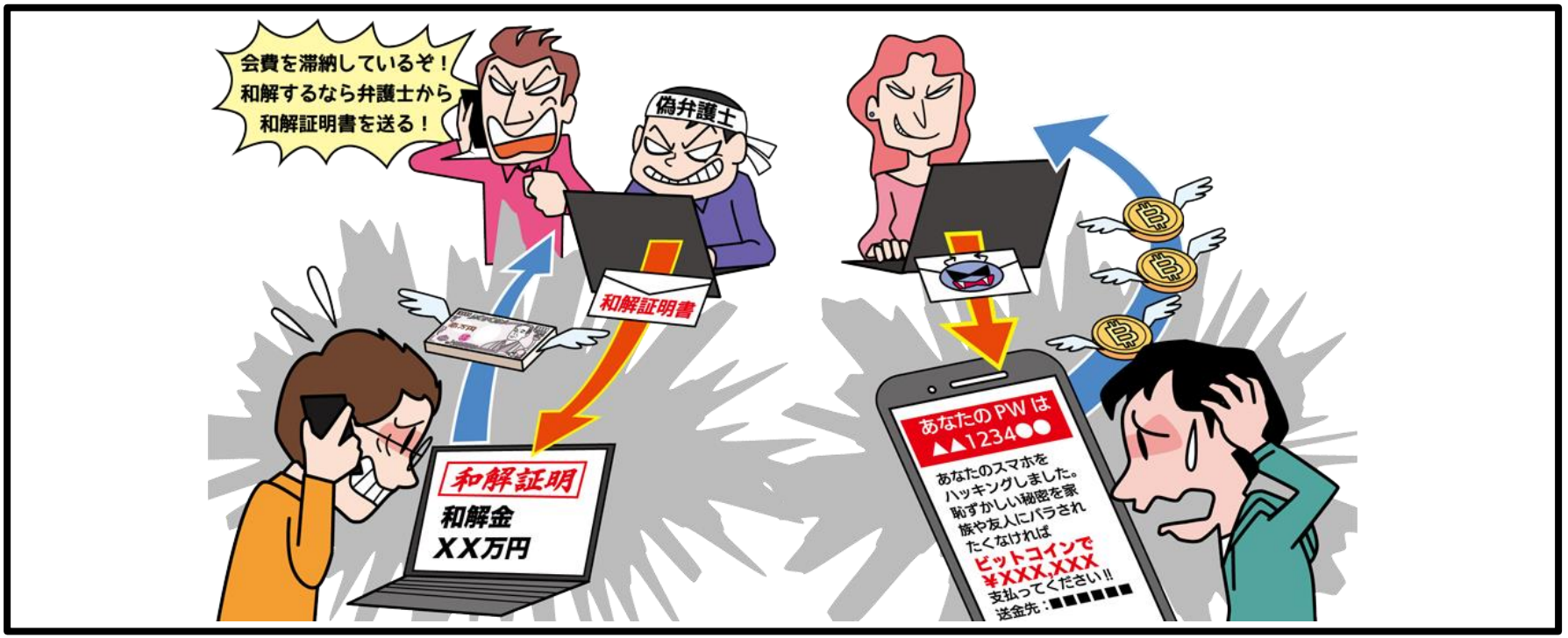
閲覧者

・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

・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

【4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
～脅迫・詐欺メールの指示に従うと相手のおもうつぼ～



- 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

【4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
～脅迫・詐欺メールの指示に従うと相手のおもうつぼ～

- **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」等、被害者が周囲に相談しにくい性的な内容で脅迫する

【4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
～脅迫・詐欺メールの指示に従うと相手のおもうつぼ～

- **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
- **メールや電話を併用して信憑性を高める**
  - ・攻撃者が被害者に対して金銭を要求する電話をかける
  - ・その後に弁護士を装った攻撃者から和解を求める旨のメールを送信し、信憑性を高めて騙そうとする

【4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
～脅迫・詐欺メールの指示に従うと相手のおもうつぼ～

- 2020年の事例/傾向
  - 電話やメールを併用した架空請求新手口（※1）
    - ・債権回収業者を名乗り、過去の契約の未納料金があるという内容の架空請求の電話をする
    - ・その後、弁護士を装い和解を求める場合に必要な対応が記載されたメールを送信し、信じ込ませようとする

【出典】
※1　新手の架空請求手口にご注意！債権回収業者から「過去の契約の未納料金・損害金の和解」を求める電話！？
http://www.kokusen.go.jp/news/data/n-20200130_2.html

【4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
～脅迫・詐欺メールの指示に従うと相手のおもうつぼ～

- 2020年の事例/傾向
  - 仮想通貨を要求する脅迫メールの相談増加 (※1)
    - ・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増加傾向
    - ・2020年の第4四半期に寄せられた相談件数が、同年第1四半期の2倍以上に増加した

【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)]
https://www.ipa.go.jp/security/txt/2020/q4outline.html

【4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
～脅迫・詐欺メールの指示に従うと相手のおもうつぼ～

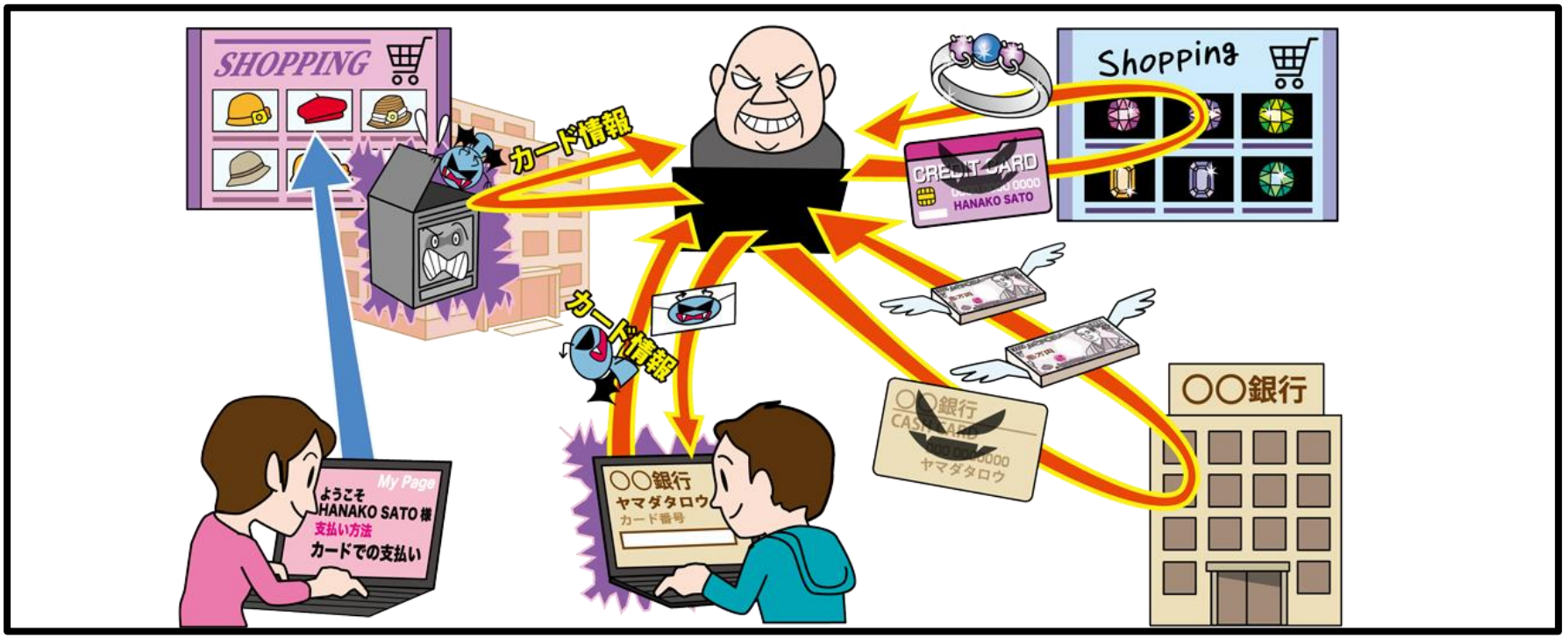
- 対策
  - インターネット利用者

・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
- –パスワードを使いまわさない

・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

【5位】クレジットカード情報の不正利用

～知らない間に流出し不正利用されているかも～



- 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

【5位】クレジットカード情報の不正利用

～知らない間に流出し不正利用されているかも～

● 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

【5位】クレジットカード情報の不正利用

～知らない間に流出し不正利用されているかも～

● 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

【5位】クレジットカード情報の不正利用

～知らない間に流出し不正利用されているかも～

- 2020年の事例/傾向
  - オンラインショップでクレジットカード情報流出（※1）
    - 芸能事務所が運営する公式サイトが不正アクセスを受け、4万4,663件のクレジットカード情報が流出したおそれ
    - 流出したクレジットカード情報は、カード名義人、カード番号、有効期限、セキュリティコード
    - 209件のカード情報が第三者に不正利用されたおそれ

【出典】
※1 EXILEの公式ECサイトに不正アクセスカード情報4万4000件が流出か
https://www.itmedia.co.jp/news/articles/2012/08/news139.html

【5位】クレジットカード情報の不正利用

～知らない間に流出し不正利用されているかも～

- 2020年の事例/傾向
  - 被害額は減少傾向、盗用被害の割合増加 (※1)
    - ・日本クレジット協会によると、2020年の1～9月において不正利用被害額は約178.5億円で、前年の同期間の約205億円から減少した
    - ・被害額全体の87.7%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額の発生状況
https://www.j-credit.or.jp/information/statistics/download/toukei_03_g.pdf

【5位】クレジットカード情報の不正利用

～知らない間に流出し不正利用されているかも～

- 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
      - –メールや閲覧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
      - –クレジットカード情報を安易にウェブサイトに保存しない
      - –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

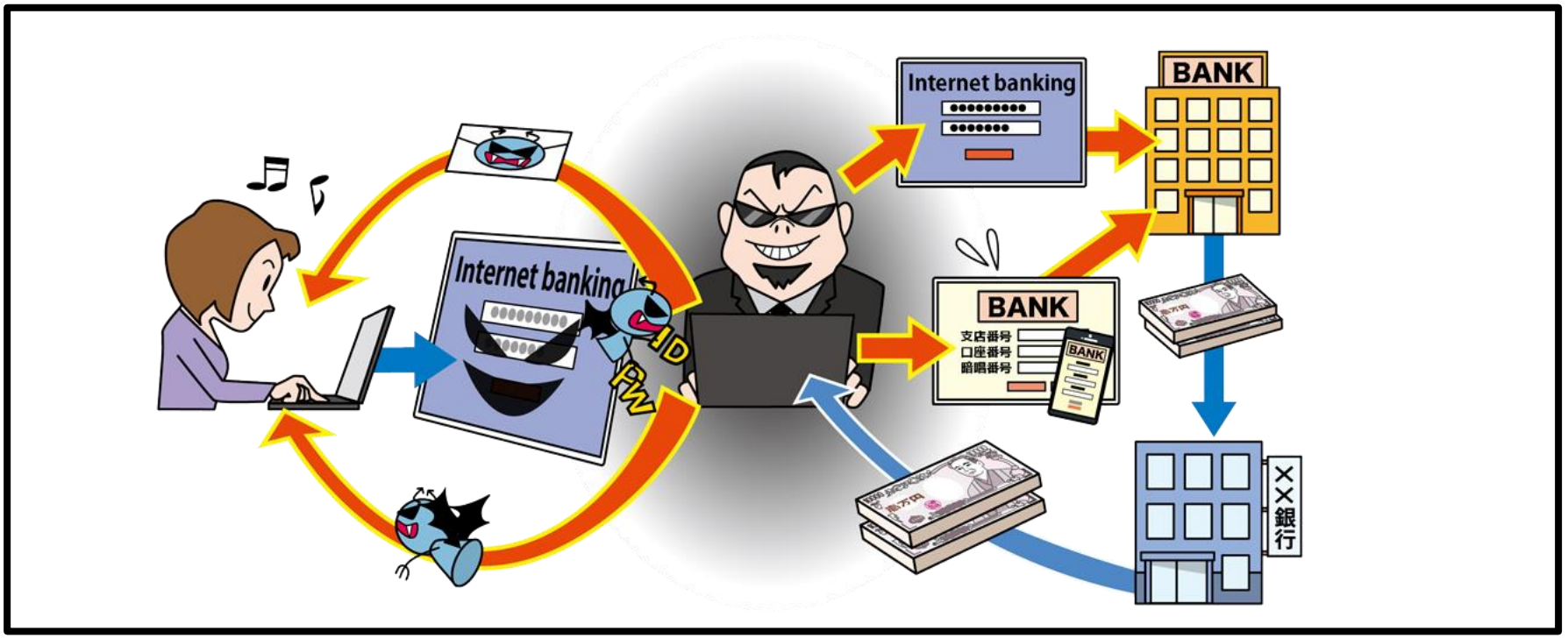
【5位】クレジットカード情報の不正利用

～知らない間に流出し不正利用されているかも～

- 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

【6位】インターネットバンキングの不正利用

～こまめな口座の利用履歴の確認および不審なログイン履歴がないかの確認を～



- **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**

【6位】インターネットバンキングの不正利用

～こまめな口座の利用履歴の確認および不審なログイン履歴がないかの確認を～

● 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

【6位】インターネットバンキングの不正利用

～こまめな口座の利用履歴の確認および不審なログイン履歴がないかの確認を～

- 2020年の事例/傾向
  - 決済サービスを悪用した不正送金被害 (※1,※2)
    - ・2020年9月、決済サービスを悪用した不正送金が複数の銀行で相次いで確認された
    - ・メールアドレスだけで開設できる決済サービスと、口座番号や暗証番号等が分かってしまえば他人になりすまして口座の連携ができてしまう銀行側、双方のセキュリティの弱点を突かれた

【出典】

※1 厄介な「ドコモ口座」不正引き出し問題、解決に求められるのは
https://xtech.nikkei.com/atcl/nxt/column/18/00086/00137/

※2 ゆうちょ銀行の不正引き出し、被害額が6000万円に拡大
https://xtech.nikkei.com/atcl/nxt/column/18/01421/092400025/

【6位】インターネットバンキングの不正利用

～こまめな口座の利用履歴の確認および不審なログイン履歴がないかの確認を～

- 2020年の事例/傾向
  - 不正送金被害の多くは個人の被害(※1)
    - 2020年第3四半期(7月～9月)におけるインターネットバンキングの被害件数は、前四半期の408件から261件、被害金額は約4億5,600万円から約1億7,300万円と減少
    - 261件中の255件、約1億7,300万円中の約1億6,600万円は個人の不正送金被害

【出典】

※1 不盗難通帳、インターネット・バンキング、盗難・偽造キャッシュカードによる預金等の不正払戻し件数・金額等に関するアンケート結果および口座不正利用に関するアンケート結果について

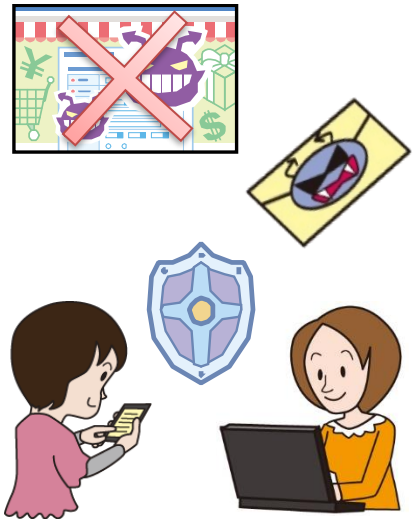
https://www.zenginkyo.or.jp/news/2020/n122201/

【6位】インターネットバンキングの不正利用

～こまめな口座の利用履歴の確認および不審なログイン履歴がないかの確認を～

● 対策

■ インターネットバンキング利用者



・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
- 口座連携済みサービスの確認
- 認証に不備がある銀行口座の利用停止

【6位】インターネットバンキングの不正利用

～こまめな口座の利用履歴の確認および不審なログイン履歴がないかの確認を～

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

【7位】インターネット上のサービスからの個人情報の窃取

～利用者でできる対策を忘れずに、IDやパスワードの使いまわしに注意～

- 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

【7位】インターネット上のサービスからの個人情報の窃取

～利用者でできる対策を忘れずに、IDやパスワードの使いまわしに注意～

● 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

【7位】インターネット上のサービスからの個人情報の窃取

～利用者でできる対策を忘れずに、IDやパスワードの使いまわしに注意～

● 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

【7位】インターネット上のサービスからの個人情報の窃取

～利用者でできる対策を忘れずに、IDやパスワードの使いまわしに注意～

- 2020年の事例/傾向
  - なりすましによる不正ログインで情報漏えい （※1,※2）
    - 通販サイトが会員へのなりすましによる不正アクセスを受けた
    - 約40万件の個人情報が閲覧されたおそれ
    - 不正アクセスに使われたメールアドレス等は当該サイトから漏えいしたのではなく、外部で取得されたものとみられる

【出典】
※1 「カメラのキタムラネットショップ」への“なりすまし”による不正アクセス発生について
https://www.kitamura.jp/topics/2020/20200615_01.html
※2 「カメラのキタムラ」通販サイトに不正アクセス個人情報40万件が閲覧された可能性二段階認証を採用せず
https://www.itmedia.co.jp/news/articles/2006/15/news138.html

【7位】インターネット上のサービスからの個人情報の窃取

～利用者でできる対策を忘れずに、IDやパスワードの使いまわしに注意～

- 2020年の事例/傾向
  - サービスの脆弱性を悪用されて情報漏えい（※1）
    - 企業のホームページから、登録されていた個人情報、最大約3万件が流出したおそれ
    - サービスの脆弱性を突いた攻撃と見られる
    - 流出した情報はインターネット上の掲示板にアップロードされていることから、金銭目的ではなく愉快犯の犯行の疑いがある

【出典】
※1　人材派遣のアスカが最大3万件の個人情報を流出…1カ月以上も周知せず
https://president.jp/articles/-/36907?page=1

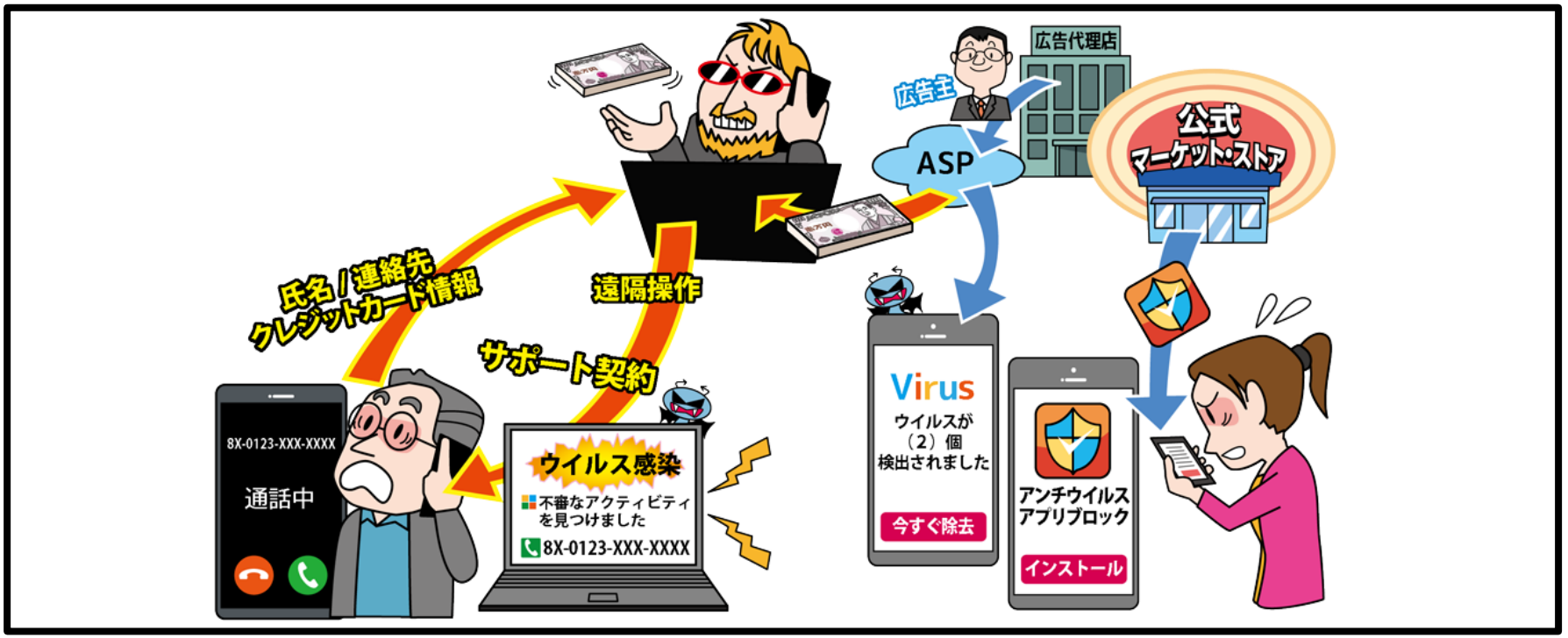
【7位】インターネット上のサービスからの個人情報の窃取

～利用者でできる対策を忘れずに、IDやパスワードの使いまわしに注意～

- 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
    - ・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

【8位】偽警告によるインターネット詐欺

～突然の警告は本物？慌てず、焦らず、落ち着いて～



- 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

【8位】偽警告によるインターネット詐欺

～突然の警告は本物？慌てず、焦らず、落ち着いて～

● 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

【8位】偽警告によるインターネット詐欺

～突然の警告は本物？慌てず、焦らず、落ち着いて～

● 攻撃手口

・偽警告に記載した誘導に従わせる

■ 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

【8位】偽警告によるインターネット詐欺

～突然の警告は本物？慌てず、焦らず、落ち着いて～

- 2020年の事例/傾向
  - 有償サポートを断ると遠隔操作でPCをロック（※1）
    - ・偽の警告画面から遠隔操作に誘導し、有償サポートを断ると遠隔操作でPCをロックして使えないようにする手口が確認されている
    - ・遠隔操作をされてしまうと、データの閲覧や消去、PCを起動させなくする等の悪質な操作が行なわれるおそれがある

【出典】
※1 IPA 安心相談窓口だより「遠隔操作を他人に安易に許可しないで！」
https://www.ipa.go.jp/security/anshin/mgdayori20201125.html

【8位】偽警告によるインターネット詐欺

～突然の警告は本物？慌てず、焦らず、落ち着いて～

- 2020年の事例/傾向
  - iPhoneカレンダーの不審な通知相談が増加 (※1)
    - ・IPA安心相談窓口に寄せられる、iPhoneのカレンダーからウイルス感染しているという通知が出るといった内容の相談の件数が2020年に急増した
    - ・iCloudやiPhoneのカレンダーの機能を悪用して他人のカレンダーに書き込みを行う手口
    - ・カレンダーのイベント詳細に記載されたURLをタップするとフィッシングサイトへ誘導され、そこで個人情報を入力すると情報を詐取されるおそれがある

【出典】

※1 IPA 安心相談窓口だよりiPhoneに突然表示される不審なカレンダー通知に注意！
https://www.ipa.go.jp/security/anshin/mgdayori20200330.html

【8位】偽警告によるインターネット詐欺

～突然の警告は本物？慌てず、焦らず、落ち着いて～

- **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
      - －身に覚えのないカレンダーは削除
    - ・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
      - －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

【9位】不正アプリによるスマートフォン利用者への被害

～宅配業者を装ったSMSにご用心！油断に付け入る不正アプリ～

- 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

【9位】不正アプリによるスマートフォン利用者への被害

～宅配業者を装ったSMSにご用心！油断に付け入る不正アプリ～

● 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

【9位】不正アプリによるスマートフォン利用者への被害

～宅配業者を装ったSMSにご用心！油断に付け入る不正アプリ～

● 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
- ・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

【9位】不正アプリによるスマートフォン利用者への被害

～宅配業者を装ったSMSにご用心！油断に付け入る不正アプリ～

- 2020年の事例/傾向
  - 宅配業者の不在通知を装ったSMSによる誘導 (※1,※2)
    - 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にアクセスするとブラウザアプリを装って利用者に不正アプリをインストールさせる
    - 不正アプリをインストールすると金融機関を装ったポップアップが表示され、更新手続きをするよう誘導
    - 不正アプリをインストールしたことで、意図せず他者を騙す多数のSMSの送信に悪用されていたという被害事例も確認

【出典】
※1 配送業者などを装った不審なメールに関するご注意
https://www.softbank.jp/mobile/info/personal/news/support/20201005a/
※2 宅配便業者を装った「不在通知」の偽SMSに注意しましょう－URLにはアクセスしない、ID・パスワードを入力しない！
http://www.kokusen.go.jp/news/data/n-20201126_2.html

【9位】不正アプリによるスマートフォン利用者への被害

～宅配業者を装ったSMSにご用心！油断に付け入る不正アプリ～

- 2020年の事例/傾向

  - 公式マーケット上で公開されていた偽クリーナーアプリ (※1)
    - Google Play上で公開されていたクリーナーアプリ（不要なファイルやプロセスを削除したり整理したりするもの）に不正アプリが含まれていた
    - 国内でも数多くダウンロードされていることが確認された
    - 利用者になりすまし、モバイル広告詐欺を行ったり、別の不正アプリをダウンロードして感染させようとしたりする
    - 不正アプリが高評価となるように操作しようとする挙動も見られた

【出典】
※1　国内で過去3カ月間に約5万件の感染被害、不正活動を行う偽クリーナーアプリ
https://is702.jp/news/3636/partner/97_t/

【9位】不正アプリによるスマートフォン利用者への被害

～宅配業者を装ったSMSにご用心！油断に付け入る不正アプリ～

- 対策
  - スマートフォン利用者

・被害の予防

–アプリの真偽を慎重に見極める

※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端末で「提供元不明のアプリのインストール」を許可しない

※iPhoneで「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

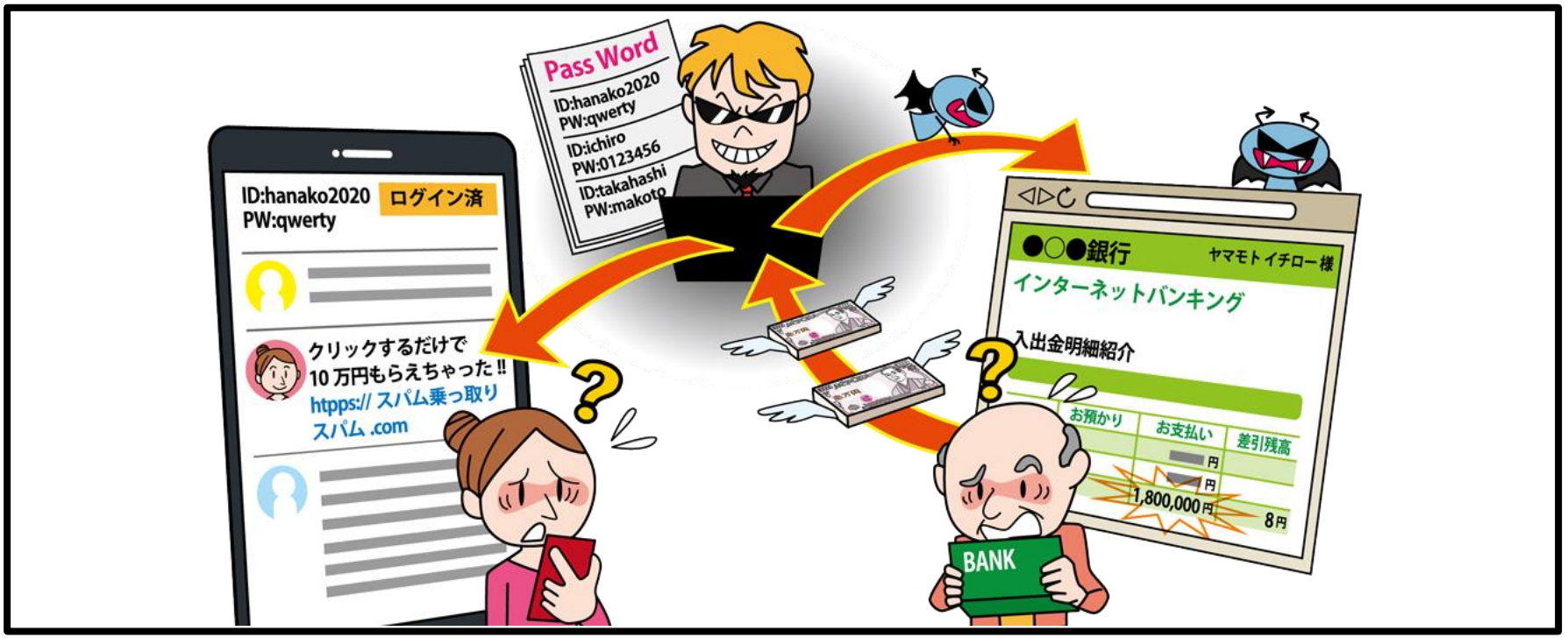
・被害を受けた後の対応

–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

【10位】インターネット上のサービスへの不正ログイン

～不正ログインによる大きな金銭的被害や個人情報漏えいのおそれ～



- 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

【10位】インターネット上のサービスへの不正ログイン

～不正ログインによる大きな金銭的被害や個人情報漏えいのおそれ～

● 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

～不正ログインによる大きな金銭的被害や個人情報漏えいのおそれ～

● 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

～不正ログインによる大きな金銭的被害や個人情報漏えいのおそれ～

- 2020年の事例/傾向
  - 不正ログインによる出金機能の悪用 (※1)
    - ・証券取引サイトにおいて、パスワードリスト攻撃と思われる攻撃による不正ログインが行われ、約1億円の不正送金が発生
    - ・利用者から、身に覚えのない取引がある旨の申告があり発覚した

【出典】
※1 悪意のある第三者による不正アクセスに関するお知らせ
https://www.sbisec.co.jp/ETGate/WPLETmgR001Control?OutSide=on&getFlg=on&burl=search_home&cat1=home&cat2=corporate&dir=corporate&file=irpress/prestory200916_02.html

【10位】インターネット上のサービスへの不正ログイン

～不正ログインによる大きな金銭的被害や個人情報漏えいのおそれ～

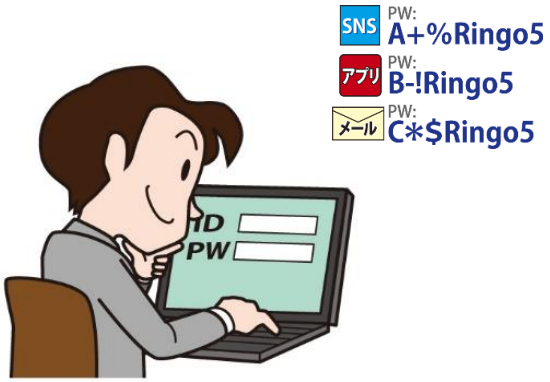
- 2020年の事例/傾向
  - SNSにおける乗っ取り被害 (※1)
    - 約4000人分のLINEアカウントが不正ログインされ、不正にメッセージやタイムライン投稿が行われた
    - 投稿には、購買誘導をするスパムやフィッシング詐欺のためのURLが含まれていた

【出典】
※1 LINEへの不正ログインに対する注意喚起
https://linecorp.com/ja/security/article/251

【10位】インターネット上のサービスへの不正ログイン

～不正ログインによる大きな金銭的被害や個人情報漏えいのおそれ～

- **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
      - –強い認証方式の利用
      - –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
      - –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
    - ・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
      - –サービスの運営者へ連絡



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　2021

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/10threats2021.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