情報セキュリティ10大脅威 2024
個人編

サイバーセキュリティセミナー2024

2024年 2月 21日

独立行政法人情報処理推進機構
セキュリティセンター
内海　百葉

IPA（情報処理推進機構）のご紹介

Information-technology Promotion Agency, Japan

- 日本のIT国家戦略を技術面、人材面から支える経済産業省所管の独立行政法人
- **「頼れるIT社会」**の実現を目指しています

● サイバーセキュリティの確保

・ウイルス、不正アクセス等の届出機関
・情報セキュリティの調査研究、普及啓発活動
・標的型サイバー攻撃の情報共有・初動対応の実施

● デジタル人材の育成

・国家試験「情報処理技術者試験」の実施機関
・IT人材の育成・発掘・スキル明確のとりくみ。若手人材育成。

● デジタル基盤の提供

・Society 5.0実現のための基盤の提供

「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で
  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

２つの「10大脅威」

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 2024（組織）

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目

順位＝危険度ではない

情報セキュリティ10大脅威 2024（組織）

「組織」向け脅威	
ランサムウェアによる被害	「脆弱性」+「騙し」
サプライチェーンの弱点を悪用した攻撃	「脆弱性」
内部不正による情報漏えい等の被害	「内部」
標的型攻撃による機密情報の窃取	「騙し」+「脆弱性」
修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	「脆弱性」
不注意による情報漏えい等の被害	「内部」
脆弱性対策情報の公開に伴う悪用増加	「脆弱性」
ビジネスメール詐欺による金銭被害	「騙し」
テレワーク等のニューノーマルな働き方を狙った攻撃	「脆弱性」+「内部」
犯罪のビジネス化（アンダーグラウンドサービス）	その他

外部からの攻撃だけでなく、内部の人への対策も必要

情報セキュリティ10大脅威 2024（個人）

「個人」向け脅威（五十音順）	初選出年	10大脅威での取り扱い（2016年以降）
インターネット上のサービスからの個人情報の窃取	2016年	5年連続8回目
インターネット上のサービスへの不正ログイン	2016年	9年連続9回目
クレジットカード情報の不正利用	2016年	9年連続9回目
スマホ決済の不正利用	2020年	5年連続5回目
偽警告によるインターネット詐欺	2020年	5年連続5回目
ネット上の誹謗・中傷・デマ	2016年	9年連続9回目
フィッシングによる個人情報等の詐取	2019年	6年連続6回目
不正アプリによるスマートフォン利用者への被害	2016年	9年連続9回目
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	2019年	6年連続6回目
ワンクリック請求等の不当請求による金銭被害	2016年	2年連続4回目

古くから存在し続ける脅威が半数以上

初選出後、連続で選出され続ける脅威が多数

情報セキュリティ10大脅威 2024（個人）

「個人」向け脅威 （五十音順）	
インターネット上のサービスからの個人情報の窃取	「脆弱性」
インターネット上のサービスへの不正ログイン	「脆弱性」+「騙し」
クレジットカード情報の不正利用	「騙し」+「脆弱性」
スマホ決済の不正利用	「騙し」+「脆弱性」
偽警告によるインターネット詐欺	「騙し」
ネット上の誹謗・中傷・デマ	その他
フィッシングによる個人情報等の詐取	「騙し」
不正アプリによるスマートフォン利用者への被害	「騙し」
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	「騙し」
ワンクリック請求等の不当請求による金銭被害	「騙し」

「騙し」を起因とした脅威が非常に多い

情報セキュリティ10大脅威 2024（個人）

「個人」向け脅威（五十音順）	
インターネット上の	
インターネット上	
クレジットカ	
スマホ	
偽警告に	
ネット上の	
フィッシング	
不正アプリによるスマ	
メールやSMS等を使った脅迫・詐欺の手口	「騙し」
ワンクリック請求等の不当請求による金銭被害	「騙し」

- 個人の脅威は「騙す」手口が多い
- 「騙し方」は古典的な方法が多い

↓

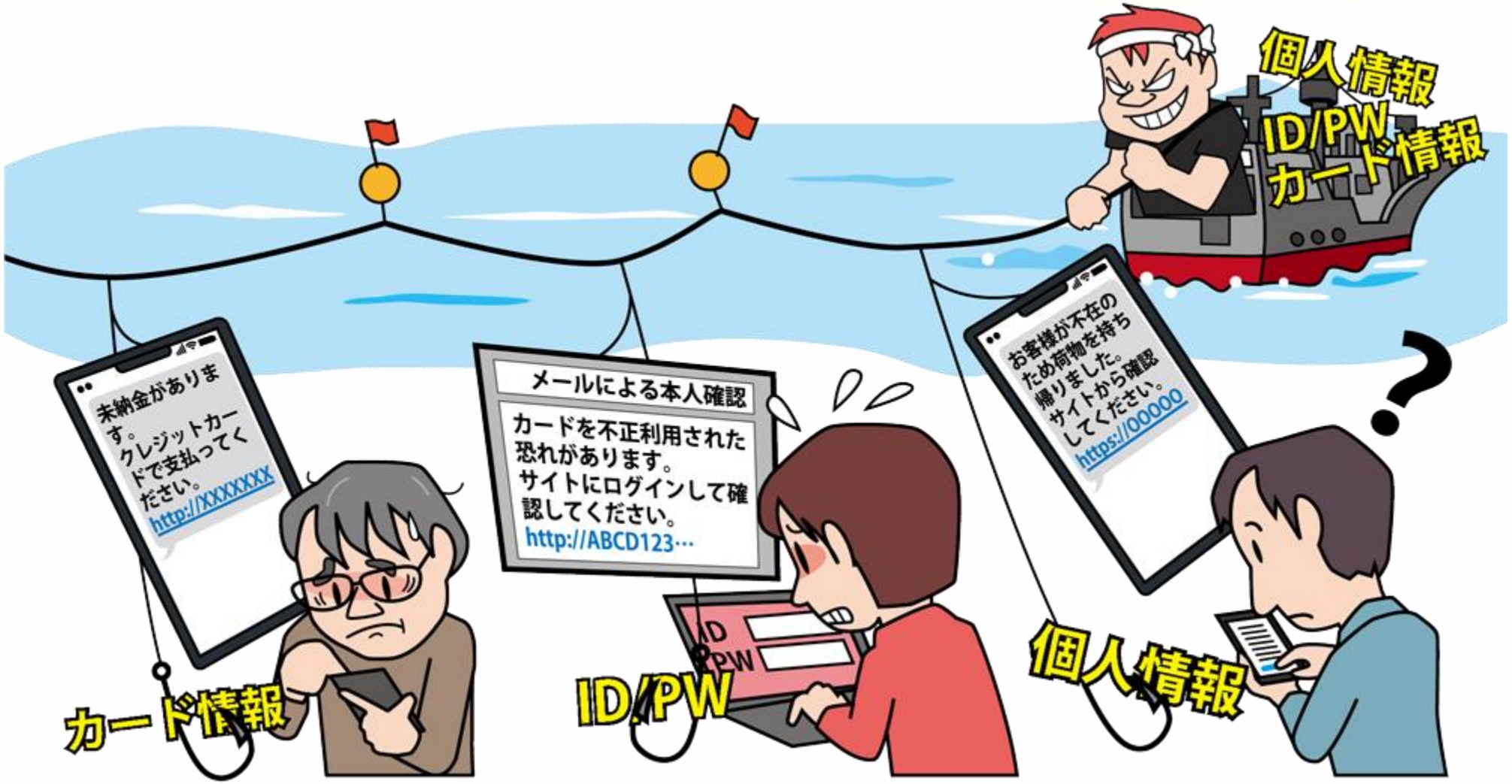
今ある手口を知っているだけで被害を予防できる可能性が高い

「騙し」を起因とした脅威が非常に多い

情報セキュリティ10大脅威 2024（個人）

「個人」向け脅威 （五十音順）	初選出年	10大脅威での取り扱い （2016年以降）
インターネット上のサービスからの個人情報の窃取	2016年	5年連続8回目
インターネット上のサービスへの不正ログイン	2016年	9年連続9回目
クレジットカード情報の不正利用	2016年	9年連続9回目
スマホ決済の不正利用	2020年	5年連続5回目
偽警告によるインターネット詐欺	2020年	5年連続5回目
ネット上の誹謗・中傷・デマ	2016年	9年連続9回目
フィッシングによる個人情報等の詐取	2019年	6年連続6回目
不正アプリによるスマートフォン利用者への被害	2016年	9年連続9回目
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	2019年	6年連続6回目
ワンクリック請求等の不当請求による金銭被害	2016年	2年連続4回目

フィッシングによる個人情報等の詐取



フィッシングによる個人情報等の詐取

- **どのような脅威？**
  - 攻撃者が用意する**様々な罠**により、偽のWebサイトに誘導される
  - その後、誘導された**偽のWebサイトで入力した個人情報を盗まれる**

様々な罠とは？

- 有名企業や公的機関を装った**メールやSMS**
- Webサイトに表示される**偽の広告**　等

これらを駆使して**興味をひいたり、慌てさせたり**してくる

盗まれた個人情報はどうなる？

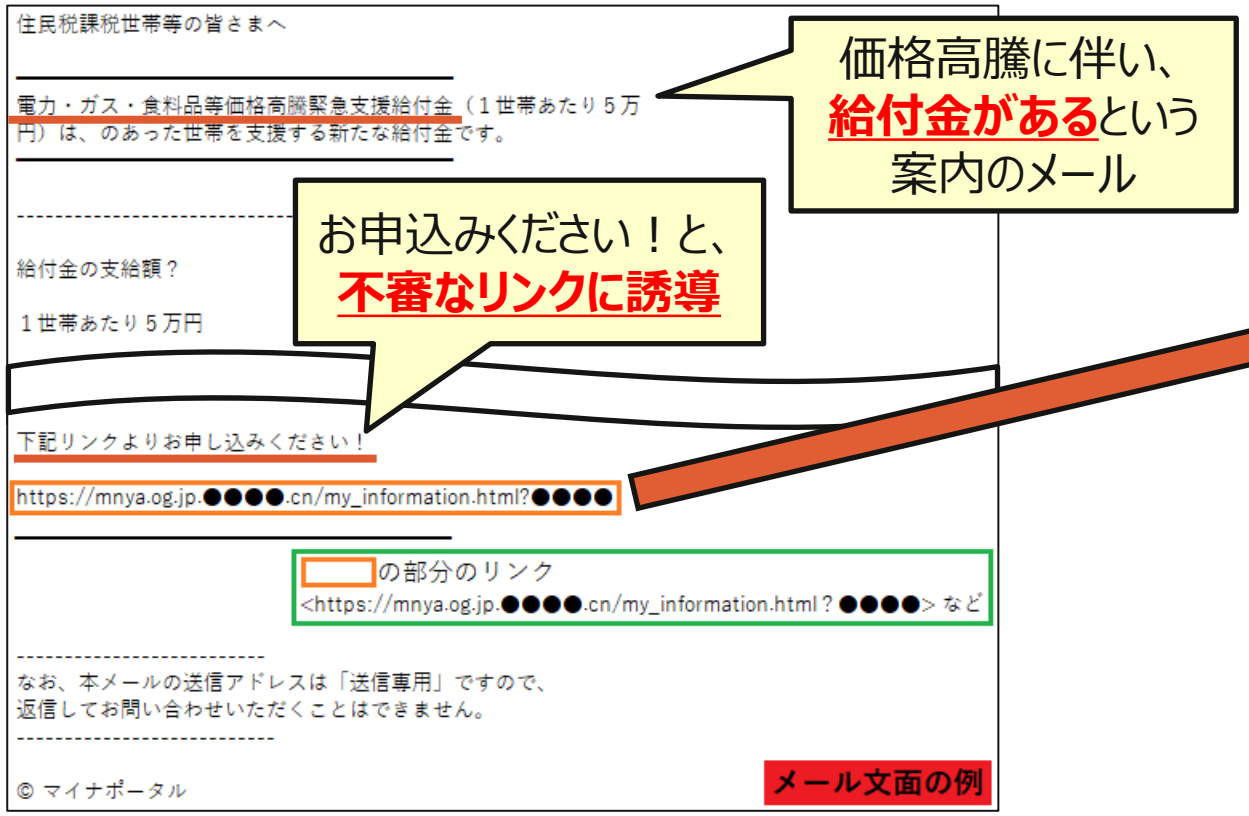
- 第三者に**販売されたり**、さらなる**攻撃に悪用**されたりする

→不正なクレジットカード決済や、銀行口座から不正送金される原因になるおそれがある

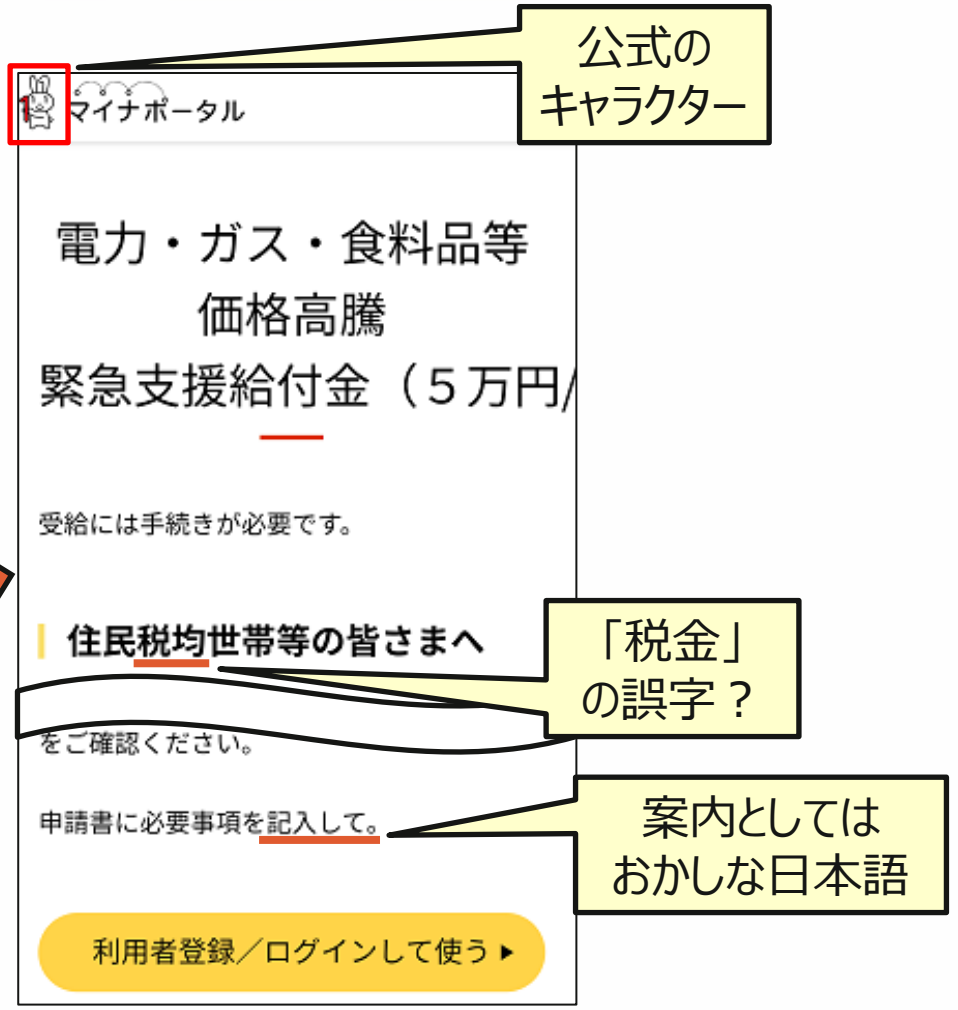
フィッシングによる個人情報等の詐取

- **攻撃手口を事例と共に見る**

例：マイナポータルを装った事例



マイナポータルを装ったフィッシングメール（※1）



マイナポータルを装ったフィッシングサイト（※1）

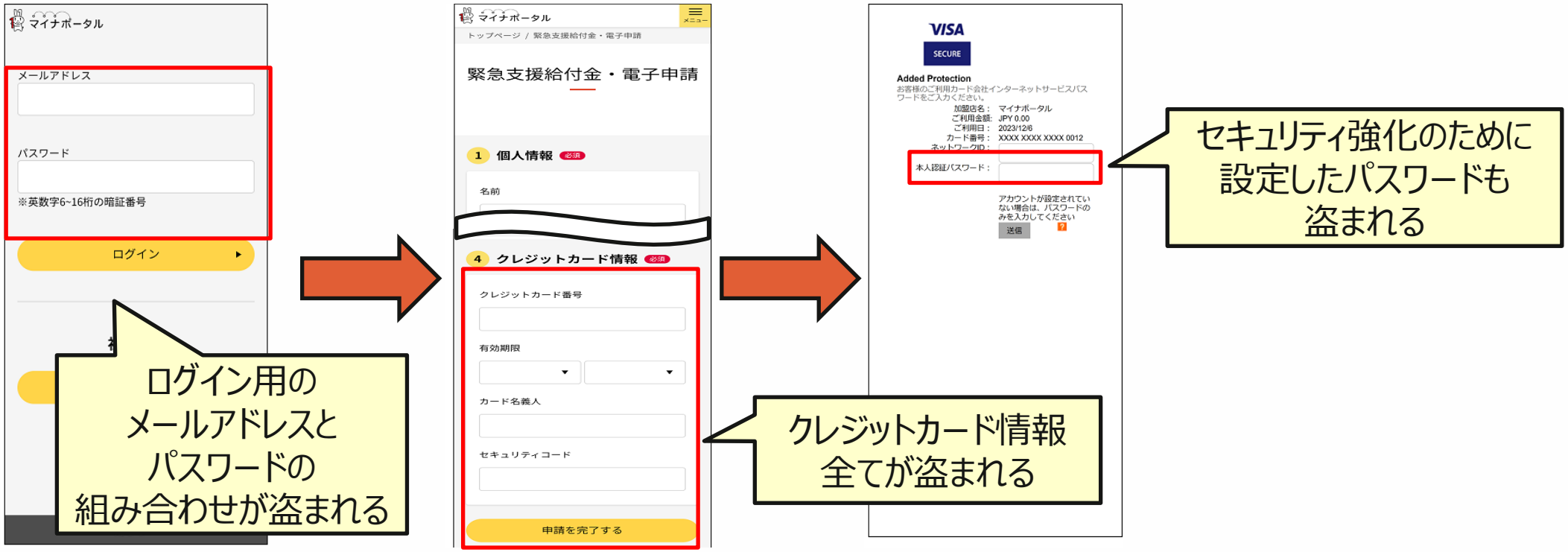
【出典】※1 マイナポータルをかたるフィッシング (2023/12/06) (フィッシング対策協議会)
https://www.antiphishing.jp/news/alert/mynaportal_20231206.html

フィッシングによる個人情報等の詐取

- **攻撃手口を事例と共に見る**

例：マイナポータルを装った事例

【出典】
※1



マイナポータルを装ったフィッシングサイト（※1）

【出典】※1 マイナポータルをかたるフィッシング (2023/12/06) (フィッシング対策協議会)
https://www.antiphishing.jp/news/alert/mynaportal_20231206.html

フィッシングによる個人情報等の詐取

- **対策①**
  - 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**

そうは言っても
気になる！

よく使うサービスならば・・・
①正規のアプリを**インストール**しておく
②正規のWebサイトを**ブックマーク（お気に入り）**しておく

あまり使わないサービスならば・・・
自分で検索して正規のWebサイトを探すようにする
※メールやSMSに記載された**用件やキーワードでも検索**すると、
「騙されている！」と気づけることも。

  - 迷惑メールフィルターを利用する
  - 多要素認証の設定を有効にする

IDやパスワードが
盗まれてしまっても、
それだけでは
不正ログインされなくなる

フィッシングによる個人情報等の詐取

- **対策②**
  - いつもと異なるログインがあった場合に、通知される設定を有効にする
  - 利用しているサービスのログイン履歴の確認する
  - クレジットカードやインターネットバンキングの利用明細を確認する

  → **早く気が付く**ことができれば被害を小さく抑えられる

被害に遭ってしまったら

- **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**
- 信頼できる知人や公的機関(迷惑メール相談センターや警察など)に**相談する**

クレジットカード情報の不正利用

クレジットカード情報の不正利用

- **どのような脅威？**
  - **何等かの方法**でクレジットカード情報が盗まれてしまう
  - その後、クレジットカード情報が**不正な決済に使われる**ことで、**身に覚えのない請求をされ、金銭被害にあってしまう**脅威
  - クレジット**カード自体**を盗まれていなくても被害にあうおそれがある

何等かの方法とは？

- フィッシングで盗まれる（前章で紹介）
- 自身の**PCやスマホがウイルスに感染**させられ、そのPCやスマホでクレジットカード情報を入力することで盗まれる
- Webサイトやシステムの**脆弱性が悪用されて**盗まれる
- クレジットカード情報を**特定される**

クレジットカード情報の不正利用

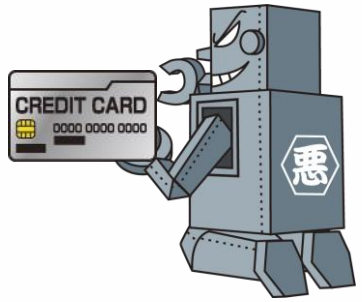
- **攻撃手口**
  - 自身のPCやスマホがウイルスに感染させられ、そのPCやスマホでクレジットカード**情報を入力すること**で盗まれる

    どのようにウイルス感染させられる？

    - 不審なメールの**添付ファイルを開封する**
    - 不審なメールやSMSのリンクから開いたWebサイトで**不審なソフトウェアをダウンロードする**

  - Webサイトやシステムの脆弱性が悪用されて盗まれる
    - サービスの仕組みや機器の脆弱性を悪用され、**企業が顧客の情報を漏えいすること**で盗まれる

  - クレジットカード情報を特定される
    - クレジットカードの番号やセキュリティコードを**総当たりして特定**される



クレジットカード情報の不正利用

- **事例紹介**
  - 2023年6月、鹿児島県志布志市が、クレジットカード情報が流出したおそれがあることを公表
  - 2021年3月から12月にかけて「志布志市ふるさと納税特設サイト」で利用された910件クレジットカード情報が対象

対象が長期間かつ、公表までに時間を要している

利用者では気づけない

それじゃ、自分ではどうしようもないの？

  - 当該Webサイトの脆弱性が悪用されてクレジットカード決済時に情報を窃取する不正なプログラムが実行されたことが原因

【出典】※1　本市が運営する「志布志市ふるさと納税特設サイト」への不正アクセスによる個人情報漏えいに関するお詫びとお知らせ（志布志市）
https://www.city.shibushi.lg.jp/soshiki/5/22233.html

クレジットカード情報の不正利用

- **対策**

自分自身でクレジットカード情報を漏洩しない

- フィッシングに**騙されない**こと

前章で紹介した、**不審なメールやSMSのリンクや添付ファイルを安易に開かない**こと

組織からのクレジットカード情報漏えいへの備え

- サービス利用状況の**通知機能を利用**する
- **利用明細を定期的に確認**する

完全に防ぐことは難しい。**被害の最小化は自分でも対策**する

→公式アプリが提供されているクレジットカードならば、アプリをインストールする

- 決済されたタイミングでスマートフォンに通知が表示されて簡単に確認できる
- 利用明細もアプリで確認できる

身に覚えのない利用ならばクレジットカード会社に連絡して**利用停止**する

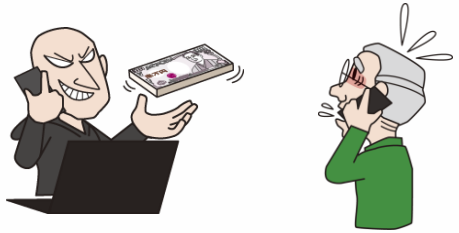
偽警告によるインターネット詐欺


ウィルス検知画面
トロイの木馬スパイウェアアラート-エラーコード: #0x268d3
このPCへのアクセスは、セキュリティ上の理由からブロックされています。
パソコンサポートへのお問い合わせ:
000-1234-5678
クイックサポート
リモートサポート
サポートへのお問い合わせ
000-1234-5678
すぐに パソコン サポートに連絡して、この脅威を報告し、なりすましを防ぎ、このデバイスへのアクセスをロック解除してください。
このウィンドウを閉じると、個人情報が危険にさらされ、パソコン の登録が中断されます。
パソコンサポートへのお問い合わせ: 000-1234-5678
キャンセル
OK
パソコン のセキュリティの向上にご協力ください
フィードバックをお寄せください
プライバシー設定を変更する
パソコン のプライバシー設定を表示および変更するこの 端末.
プライバシー設定
プライバシー ダッシュボード
プライバシーに関する声明

偽警告によるインターネット詐欺

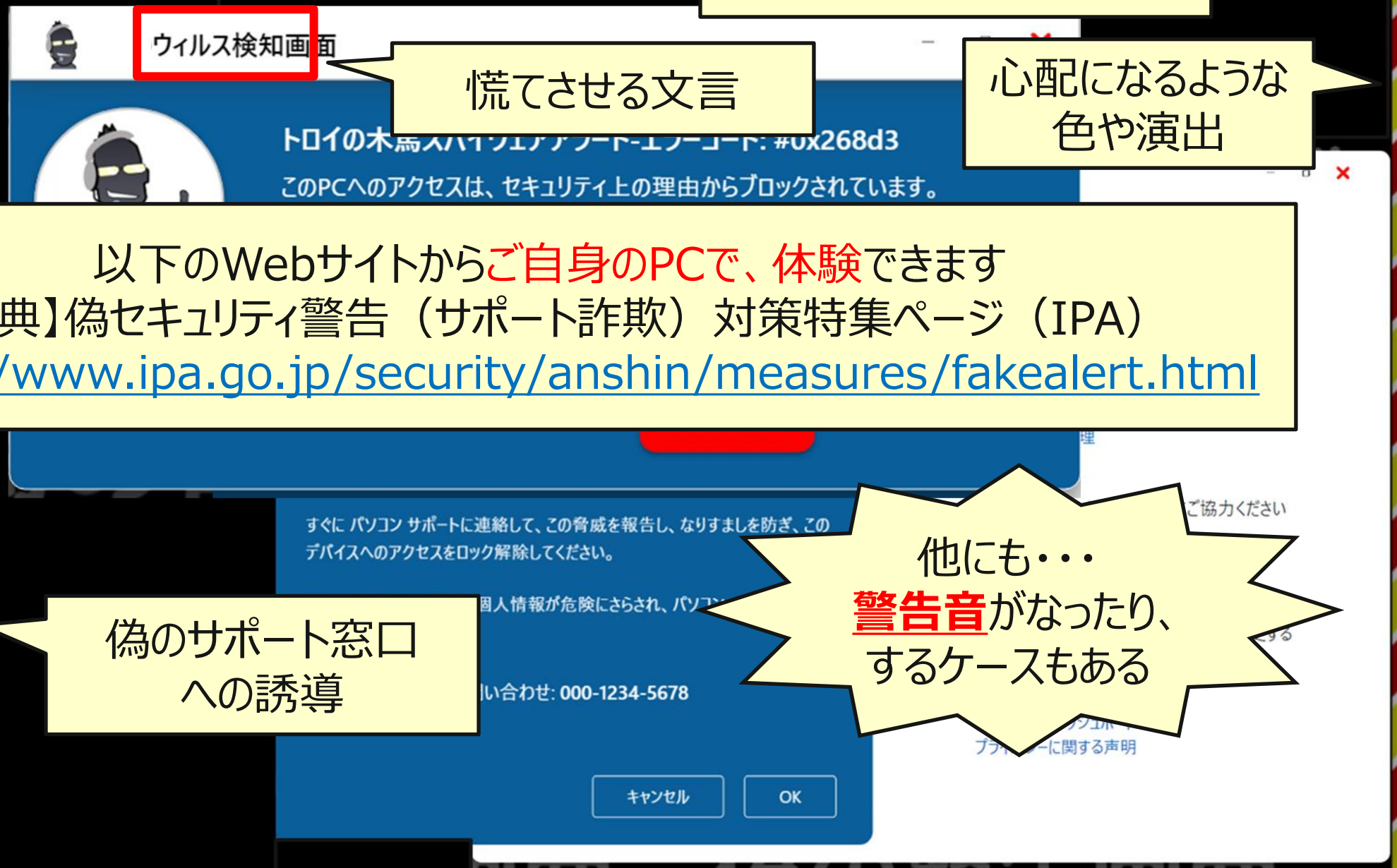
- **どのような脅威？**
  - インターネット閲覧中にPCやスマートフォンに突然**ウイルス感染**や、**端末の破損**に関する**偽の警告が表示**される

  - 表示された偽の警告では、**不審なソフトウェアのインストールに誘導**されたり、**偽のサポート窓口に電話をかけるように誘導**されたりする
  - 案内に従って不審なソフトウェアをインストールしてしまうと、PCやスマートフォンが**遠隔操作**されたり、**ウイルス感染**する等さらなる被害の原因になる
  - 最終的にはソフトウェアの代金やサポート費用等と金銭を要求され、それに応じて支払うことで**金銭被害**に遭う



偽警告の特徴の例

画面を閉じるための
×ボタンが無くて閉じれない



慌てさせる文言

心配になるような
色や演出

以下のWebサイトからご自身のPCで、体験できます
【出典】偽セキュリティ警告（サポート詐欺）対策特集ページ（IPA）
https://www.ipa.go.jp/security/anshin/measures/fakealert.html

偽のサポート窓口
への誘導

他にも・・・
警告音がなったり、
するケースもある

偽警告によるインターネット詐欺

- **スマートフォンに表示される偽警告**
  - 偽警告はスマートフォンに表示されることもある

スマートフォンに表示された偽警告（※1）

【出典】※1　安心相談窓口だより「スマートフォンの偽セキュリティ警告から自動継続課金アプリのインストールへ誘導する手口にあらためて注意！」（IPA）
https://www.ipa.go.jp/security/anshin/attention/2022/mgdayori20221025.html

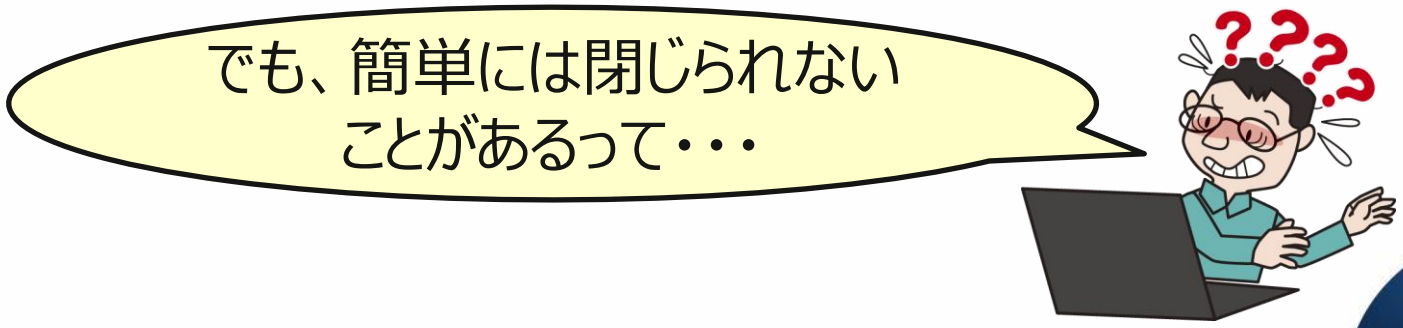
偽警告によるインターネット詐欺

- **事例紹介**
  - 2023年1月、兵庫県警が偽警告によるサポート詐欺でPCを遠隔操作され、**金銭を騙し取られる被害が相次いでいる**と発表
  - ある被害者は、PC利用中に表示された「ウイルスに感染」との**警告に従い、自宅の電話番号を入力**
  - 電話を掛けてきたソフトウェア会社の社員を名乗る人物の**指示に従って、遠隔操作用ソフトウェアをインストール**させられた
  - その後、サポート費用1万円の他、手数料490円を要求され、インターネットバンキングから振り込みを実施
  - 振り込みの際、**PCを遠隔操作されて**振込金額の桁数を増やされており、49万円が送金されていた。

【出典】※1　個人のパソコンを遠隔操作、ネットバンキングから現金だまし取る　新たな手口、兵庫で被害相次ぐ（神戸新聞NEXT）
https://www.kobe-np.co.jp/news/sougou/202302/0016081001.shtml

偽警告によるインターネット詐欺

- **対策（被害に遭ってしまったら）**
  - 慌てて対応せず、落ち着いて、警告に**表示された内容は無視**する
    特に以下3つを守る。
    - **電話を絶対にかけない**
    - **ソフトウェアを絶対にインストールしない**
    - **個人情報を絶対に入力しない**
  - 心配ならば知人や公的機関に相談し、一人で対応しない
  - 偽警告の画面を閉じる



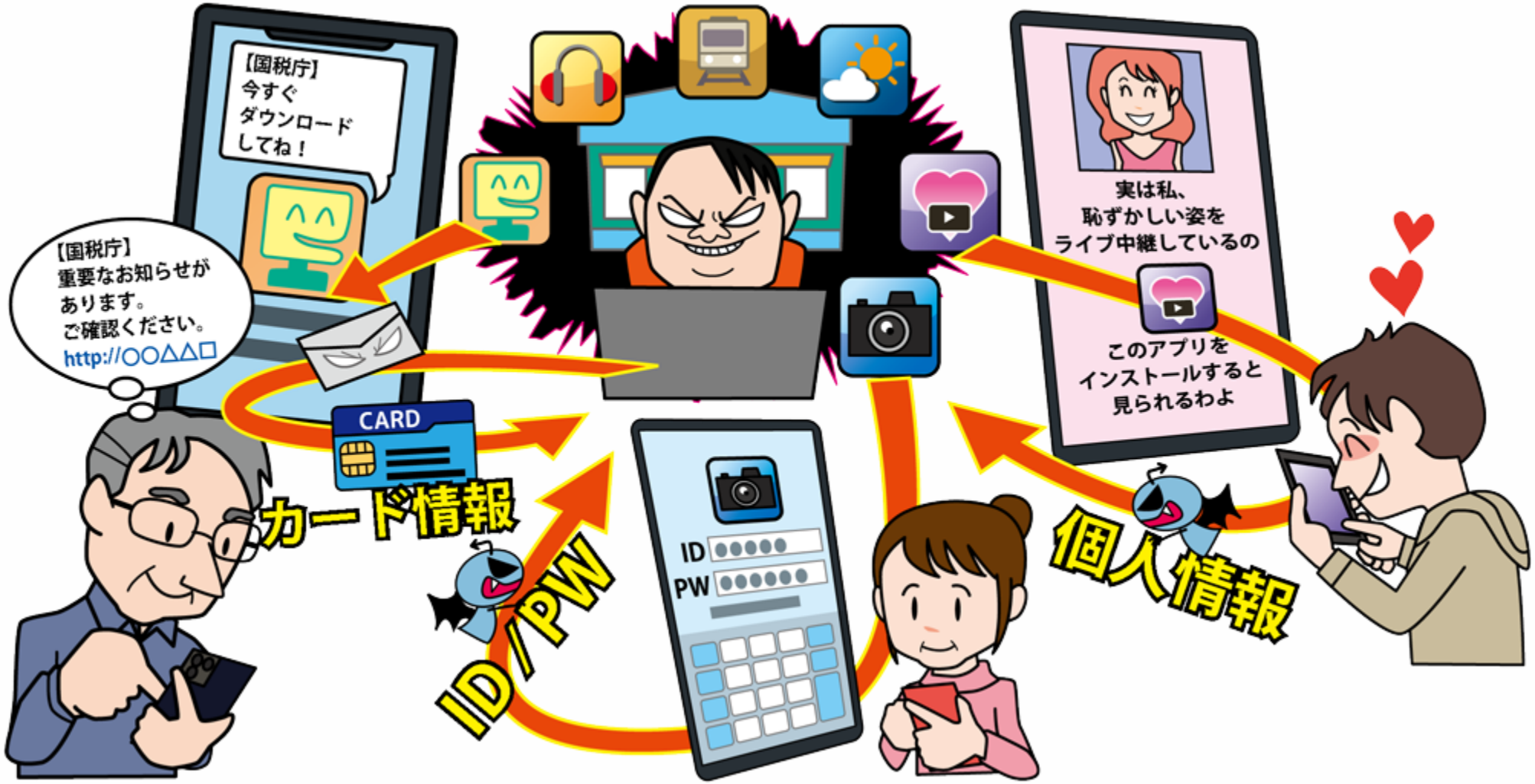
偽警告によるインターネット詐欺

- **対策（被害に遭ってしまったら）**
  - 偽警告が閉じられない時の対処方
    - キーボードの**【Esc】を2～３秒押し続ける**
      →画面右上の×ボタンを表示させることができるので×ボタンを押して画面を閉じる
    - キーボードの**【Ctrl】【Alt】【Delete】を同時に押す**
      →  を押して、「再起動」を選択することで強制再起動する

再起動後に、ブラウザを立ち上げると「復元」するかを聞かれる。
復元すると再度偽の警告画面が開かれてしまうので**復元はしない**

【参考】※1　サポート詐欺で表示される偽のセキュリティ警告画面の閉じ方(IPA)
https://www.ipa.go.jp/security/anshin/doe3um0000005cag-att/20231115173500.pdf

不正アプリによるスマートフォン利用者への被害



不正アプリによるスマートフォン利用者への被害

- **どのような脅威？**
  - 攻撃者が用意する**様々な罠**により、不正アプリをインストールさせられる

様々な罠とは？

- 公式マーケットに不正アプリが**紛れ込んでいる**

公式マーケットだから
全てのアプリが**絶対安全。**
・・・というわけではない！

- 不正アプリのダウンロードサイトへ誘導される
  →誘導する方法の例としては以下がある
  - 本日紹介した「フィッシング」で**興味を引かれたり、慌てさせられて誘導される**
  - 本日紹介した「偽警告」で**慌てさせられて誘導される**

実在の企業等を名乗っていても
安易に信じてはいけない！

- アプリの更新で不正アプリに**変化する**
  - インストール時には問題なく、更新によって悪意ある機能が顕在化する

不正アプリによるスマートフォン利用者への被害

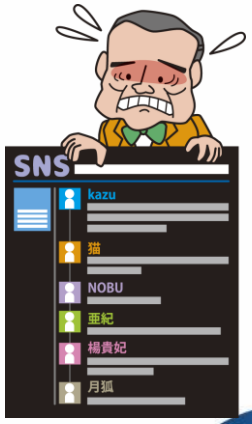
- **どのような脅威？**

不正アプリをインストールするどうなる？

- 不正アプリの種類によって以下のような被害を受けるおそれがある
  - 連絡先等の端末内の**重要な情報を盗まれる**
  - スマートフォンの**一部の機能（録画、写真、録音など）を不正に利用される**
  - **踏み台**に利用される
    →さらなる誰かを攻撃するために勝手にスマートフォンを使われる

企業のシステムを攻撃するために
あなたのスマートフォンが使われた場合、
あなたが攻撃したと疑われる

SNSで誹謗・中傷やデマを勝手に
書き込まれたり、拡散された場合、
あなたが発信したと疑われる



不正アプリによるスマートフォン利用者への被害

- **事例紹介**
  - カスペルスキーのリサーチチームによると、Google Play上の悪意のあるアプリの合計ダウンロード数が**2023年は6億回を超えていた**とのこと
  - 不正アプリには以下のようなアプリが発見されている
    - 利用者の**スマートフォンのマイクから盗聴する**トロイの木馬を含んだ画像編集アプリ
    - 端末に保存された**連絡先**やリアルタイムの**位置情報**、**画像**等を**盗む**スパイウェアを含んだファイル管理アプリ
      →さらに、アンインストールされないようにスマートフォンのホーム画面にアイコンが表示されないようになっている

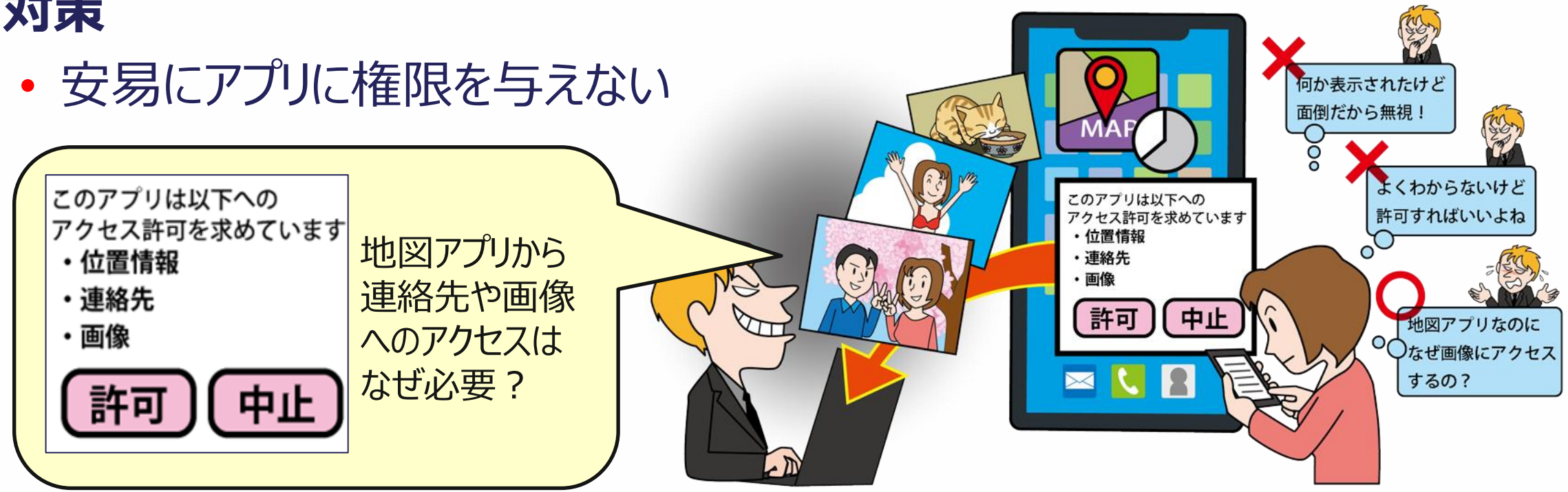
【参考】※1　Google Playのアプリにマルウェア 2023年は６億回以上ダウンロードされる（kaspersky daily）
https://blog.kaspersky.co.jp/malware-in-google-play-2023/35124/

不正アプリによるスマートフォン利用者への被害

- **対策**
  - アプリは公式マーケットから入手
    →公式マーケットであっても**レビュー等から信頼できるか確認**する
  - 不審、不要なアプリをインストールしない
    →「楽しそう」「案内されたから」と、**安易にインストールせずに**一度立ち止まって、
    信頼できるか確認する
    ※Android端末の場合、アプリが**「提供元不明」**になっていないか？
    ※iPhoneの場合、アプリが**「信頼されていないエンタープライズデベロッパ」**
    になっていないか？
  - 利用しなくなったアプリはアンインストールする

不正アプリによるスマートフォン利用者への被害

- **対策**
  - 安易にアプリに権限を与えない



  - アプリから権限を求められたら・・・
    - 画面に表示された求められている権限を確認する（**読まずに許可しない**）
    - 求められた権限は**そのアプリに本当に必要なのか考える**

不正アプリによるスマートフォン利用者への被害

- **対策（被害にあってしまったら）**
  - スマートフォンを**機内モード**にする
    →外部との通信ができなくなるので情報漏えいを防げる
  - 不正アプリを**アンインストール**する
    →アンインストールすることで被害の拡大を防げる
  - スマートフォンを**初期化**する
    →不正アプリがスマートフォンに及ぼす影響はアプリにより異なり、分からない
    初期化することでより安全な状態にすることができる

不正アプリによるスマートフォン利用者への被害

- **対策（被害にあってしまったら）**
  - 利用しているサービスの**アカウントのパスワードを変更**する
    →情報が盗まれている場合、パスワードも漏えいしているおそれがある
  - 利用しているサービスが**不正利用されていないか確認**する
    →パスワードが漏えいしていた場合、不正利用されているおそれがある
  - キャリア決済の利用状況を確認する

Check!!
宅配便業者に加えて通信事業者をかたる偽ショートメッセージサービス（SMS）が増加中（IPA）
※画面中段「不正なアプリをインストールした場合の対処」
https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20211222.html#04

まとめ

まとめ

- **「騙されない」ことが大事**

～騙されない３箇条～
一、慌てない
二、まずは疑う
三、本物か確認する

- 一、慌てない
  - 興味をひかれたり、慌てさせられても、まずは一呼吸おく。
    慌てていると判断ミスをしがちです
- 二、まずは疑う
  - 公的機関や企業からのメールやSMSが届いたり、
    PCやスマートフォンに警告が表示されたりしても、
    まずは本物なのか疑う
- 三、本物か確認する
  - 疑ったあとは本物かどうかを確認しましょう

まとめ

- **誰かに相談しましょう**
  - 信頼できる人に相談してみる

    ○：家族や友人など身の回りの信頼できる人に相談する

    ~~×：メールやSMSを送ってきた人に返信して相談する~~
  - サービスの正規の問い合わせ窓口に電話などで確認してみる

    ○：サービスのウェブページや案内から自分で窓口を探す

    ~~×：偽物かもしれないメールやSMSに記載された窓口に連絡する~~

他にも・・・
受信したメールやSMSのタイトル、本文の**一部をインターネットで検索してみる**ことで、
よくある「詐欺」や「フィッシング」として紹介されていて**自分で気が付くことができる**！

参考情報

- **IPAの相談窓口（安心相談窓口）**
  - Webサイト:https://www.ipa.go.jp/security/anshin/about.html
  - メールでの相談：anshin@ipa.go.jp
  - 電話での相談：03-5978-7509
    ※土日祝日・年末年始は除く、10:00～12:00、13:30～17:00 に受付

Check!!
安心相談窓口だより（IPA）
https://www.ipa.go.jp/security/anshin/attention/index.html
※よくある手口や対策を紹介しているので是非ご覧ください

参考情報

- **情報セキュリティ10大脅威 2024**
  https://www.ipa.go.jp/security/10threats/10threats2024.html

Check!!
6月中旬に以下の初心者向けの資料を公開予定

・簡易説明資料[個人編]（一般利用者向け）
・知っておきたい用語や仕組み

昨年版は以下からご覧いただけます
https://www.ipa.go.jp/security/10threats/10threats2023.html

ありがとうございました