インターネット安全講演会

2024年7月31日（水）

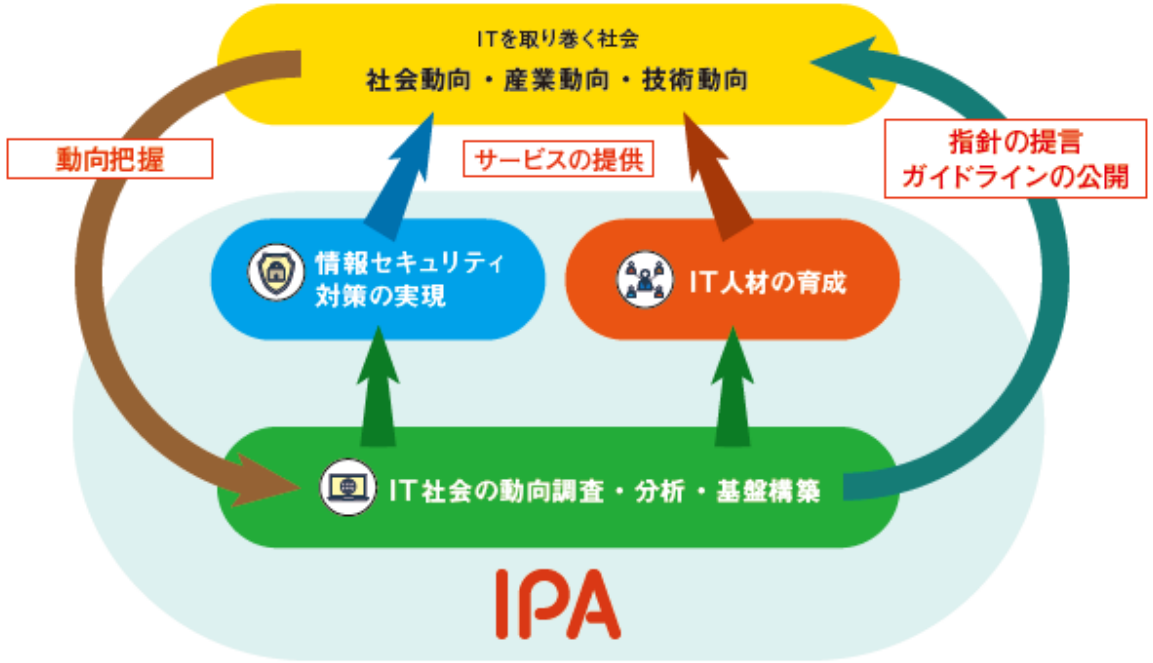
独立行政法人情報処理推進機構
セキュリティセンター 普及啓発・振興部
相談・支援グループ
グループリーダー 中島尚樹

IPA Better Life with IT

IPAのご紹介

独立行政法人**情報処理推進機構**
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**
- 安全で利便性の高い**「 頼れるIT社会 」**の実現に貢献しています



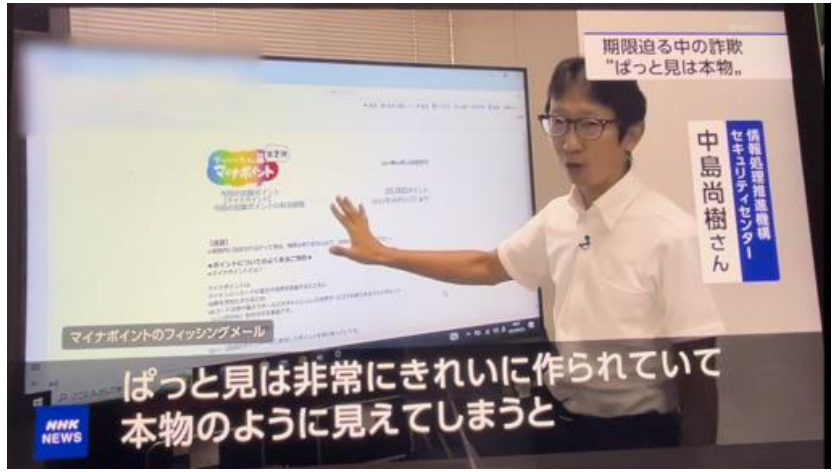
自己紹介

■中島尚樹（なかじま　なおき）

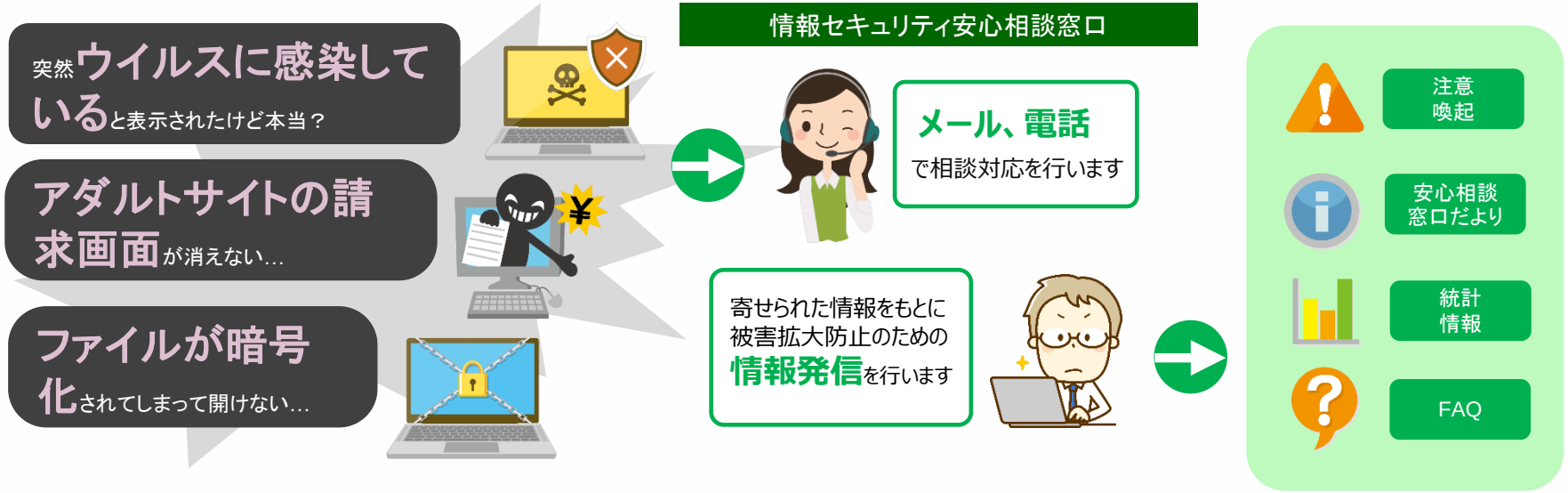
独立行政法人情報処理推進機(IPA)
セキュリティセンター セキュリティ普及啓発・振興部
セキュリティ相談・支援グループ　グループリーダー

IPA**「情報セキュリティ安心相談窓口」**における情報セキュリティ関連相談への対応や、情報セキュリティ対策全般の普及啓発活動に従事。

・情報セキュリティ大学院大学 客員研究員
・横浜国立大学 非常勤講師



IPA情報セキュリティ安心相談窓口



https://www.ipa.go.jp/security/anshin/about.html

電話
03-5978-7509
平日10:00-12:00 、13:30-17:00

メール
anshin@ipa.go.jp

ポータル
IPA安心相談 検索

目次

本日お伝えしたいこと

個人に対する最大の脅威は「ネット詐欺」

- 人の心理的な弱点に付け込み、被害者を騙すための道具として、既存のインターネットサービスやアプリを悪用
- サポート詐欺やフィッシングはその典型

ネット詐欺の対策

- 詐欺の**手口を知り「騙されない」**こと

ネット詐欺には代表的な手口がある

- 目次に示した**手口が主要なもの**

資料の構成

手口

手口についてその流れや仕組み、発生する被害について説明します。

対処

その手口にひっかかった場合に必要な対処を説明します。

対策

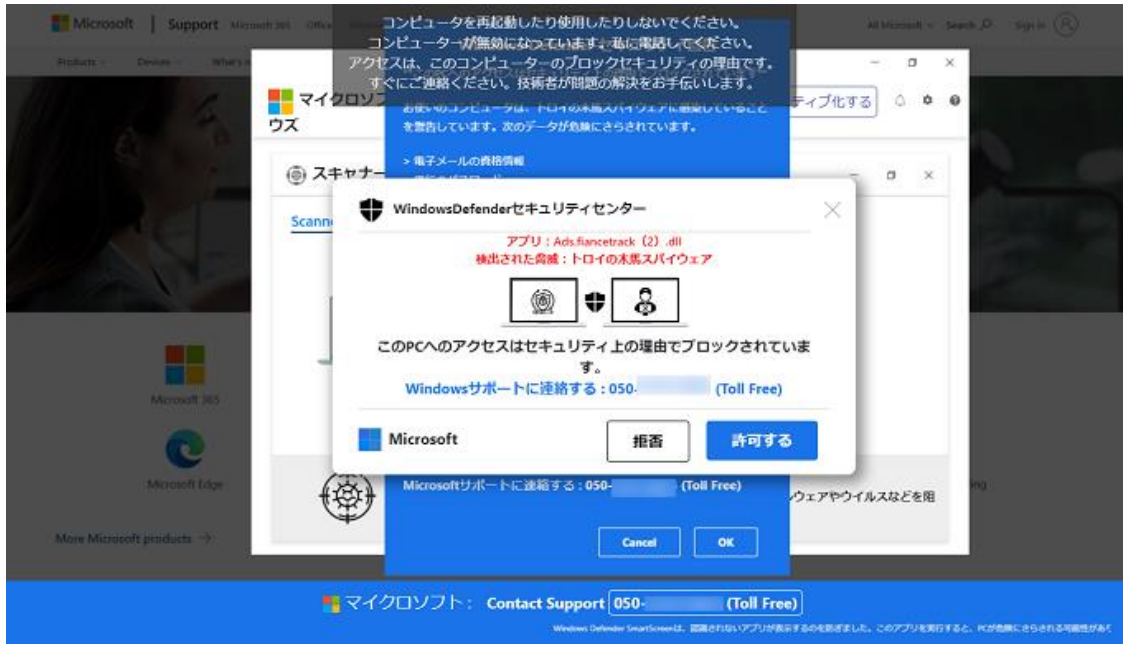
そもそも、その手口の被害にあわないための日ごろの対策について説明します。

1.サポート詐欺

1. サポート詐欺（偽のセキュリティ警告）

1.サポート詐欺

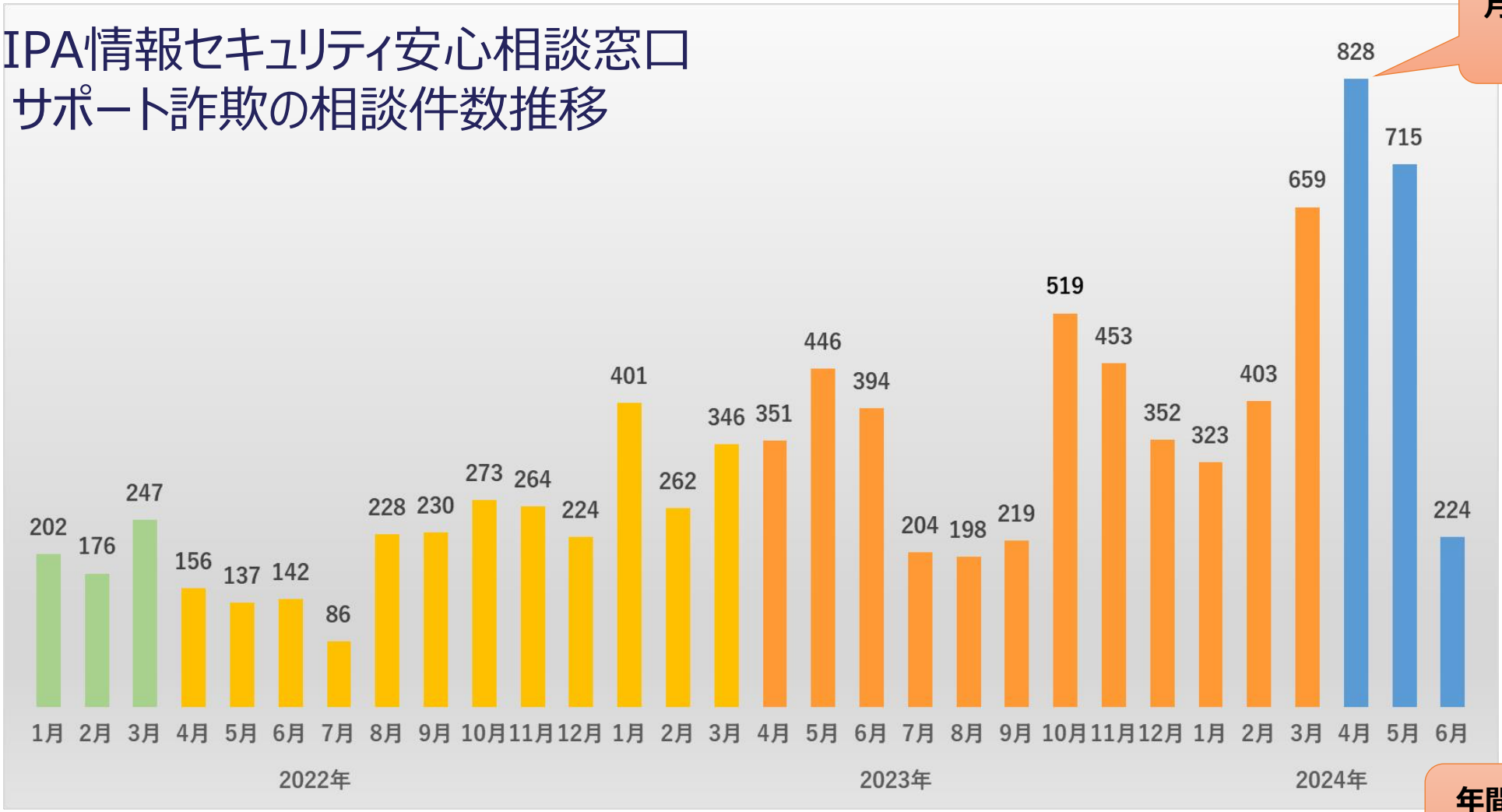
- パソコンでサイトを見ているときに、突然ウイルス感染の警告が表示される。



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！]

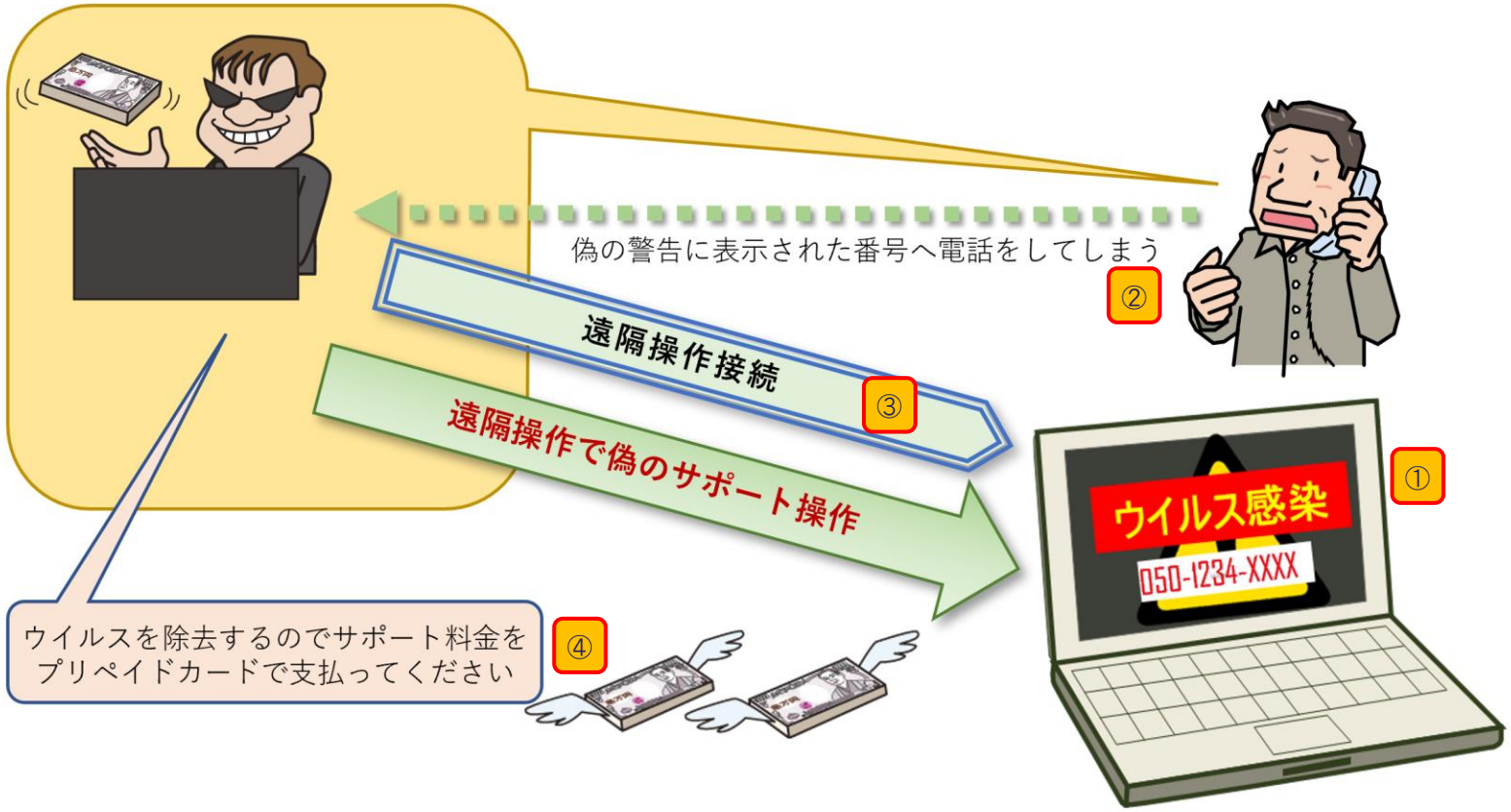
1.サポート詐欺

■ IPA情報セキュリティ安心相談窓口
サポート詐欺の相談件数推移



1.サポート詐欺

手口



■ 手口の流れ

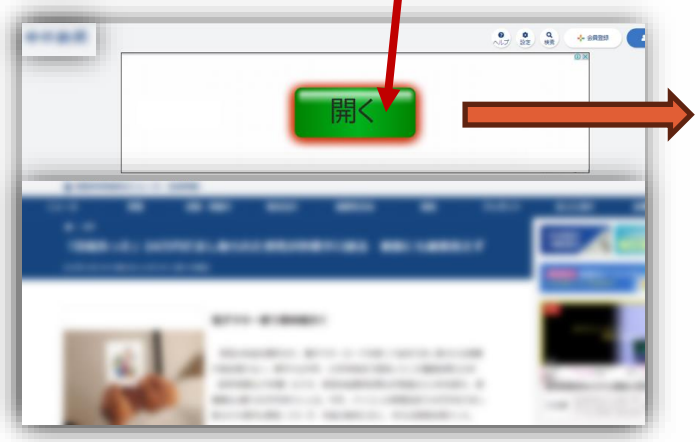
① パソコンに偽のウイルス感染警告が表示される。
② サポートに電話をする。
③ パソコンの遠隔操作へ誘導される。
④ うそのサポート料金を請求される。

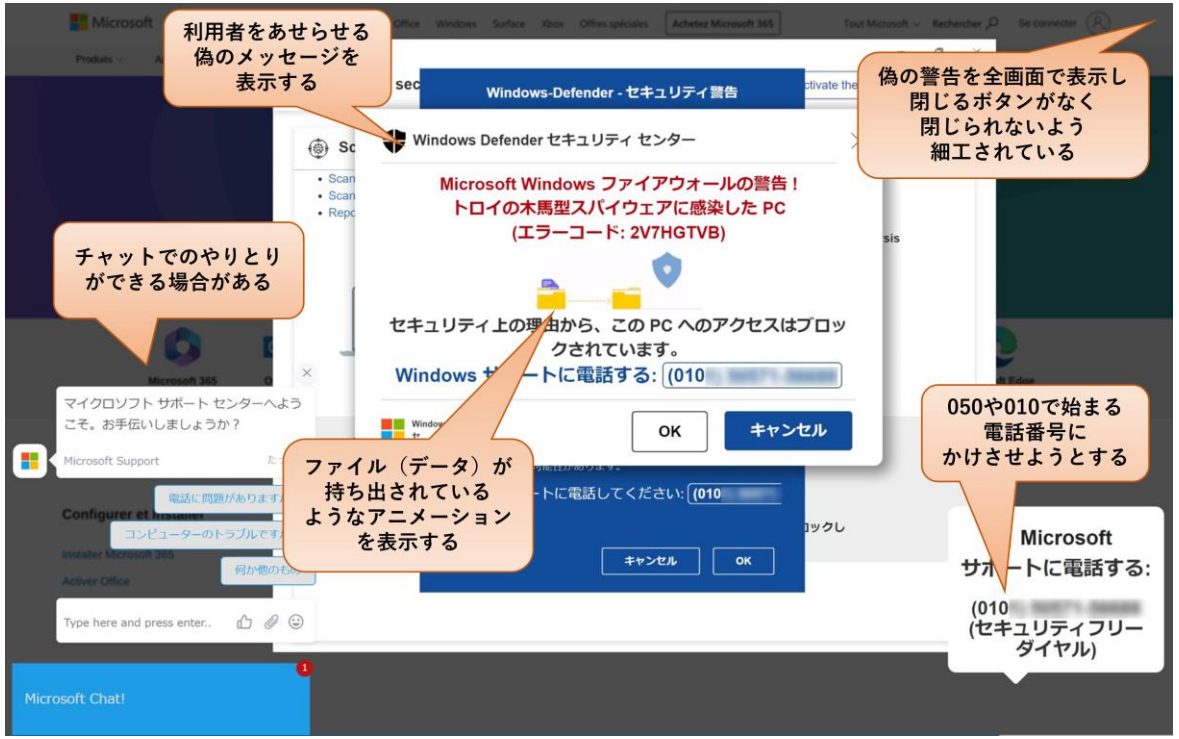
1.サポート詐欺

手口

■ 偽のセキュリティ警告画面

普通のサイトに
表示されている広告





■ どういうときにでるか？

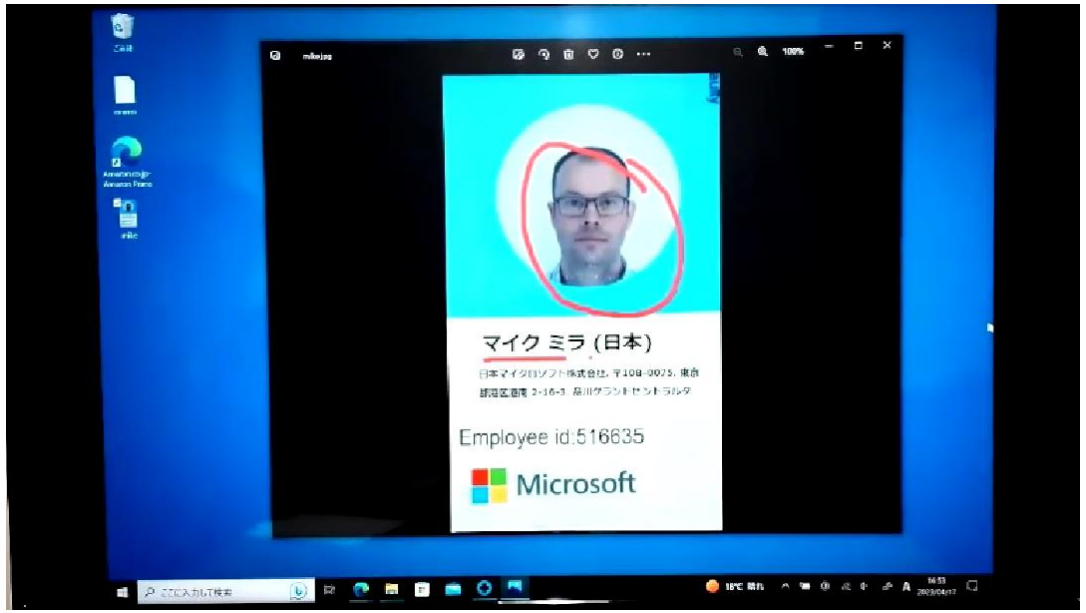
- 普通のサイトに表示されている広告からでる。
- ネット検索の結果一覧からでる。
- アダルトサイトなどの不審サイトからでる。

➢ そのようなサイトを事前に把握することは困難。

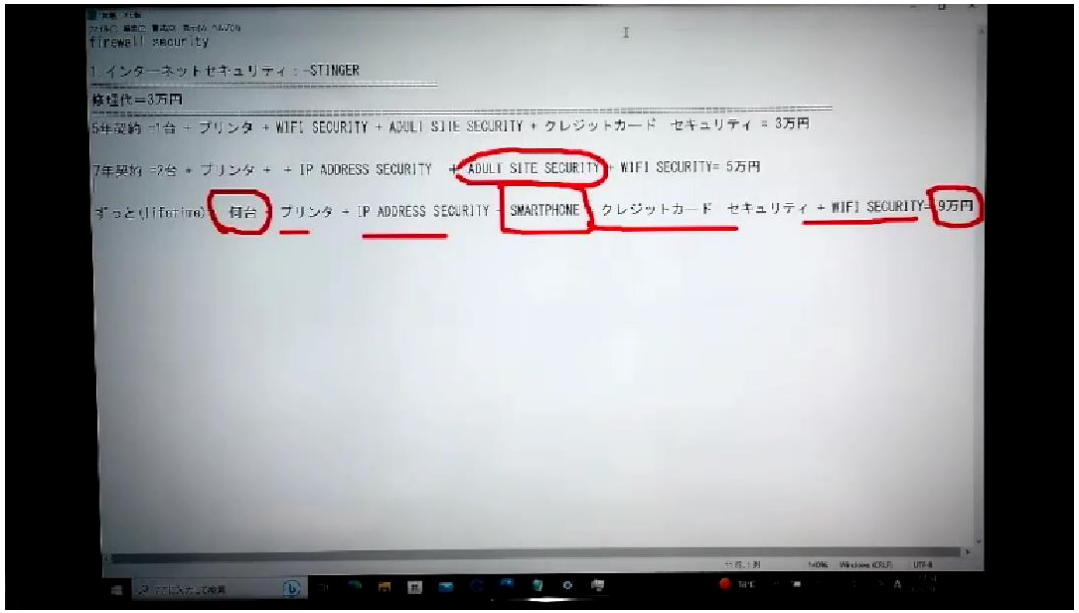
1.サポート詐欺

手口

- 実際に遠隔操作されたときの画面



偽の社員証



契約コースの案内

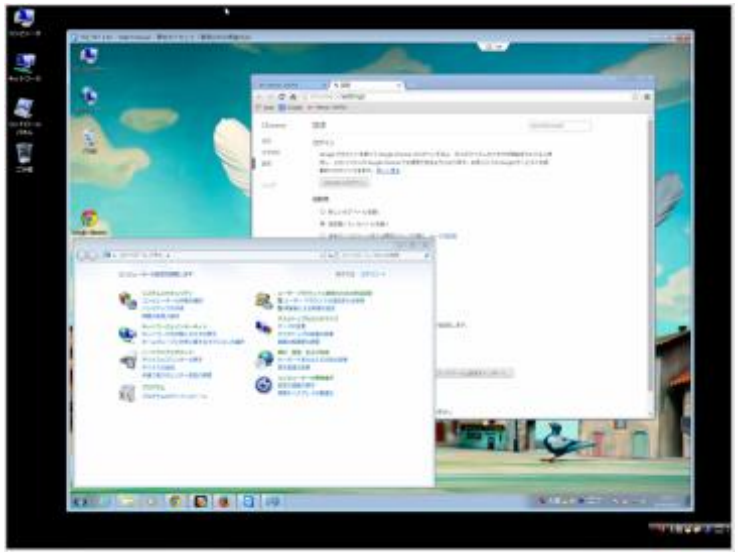
1.サポート詐欺

手口

■ 遠隔操作

遠隔操作される側

遠隔操作する側



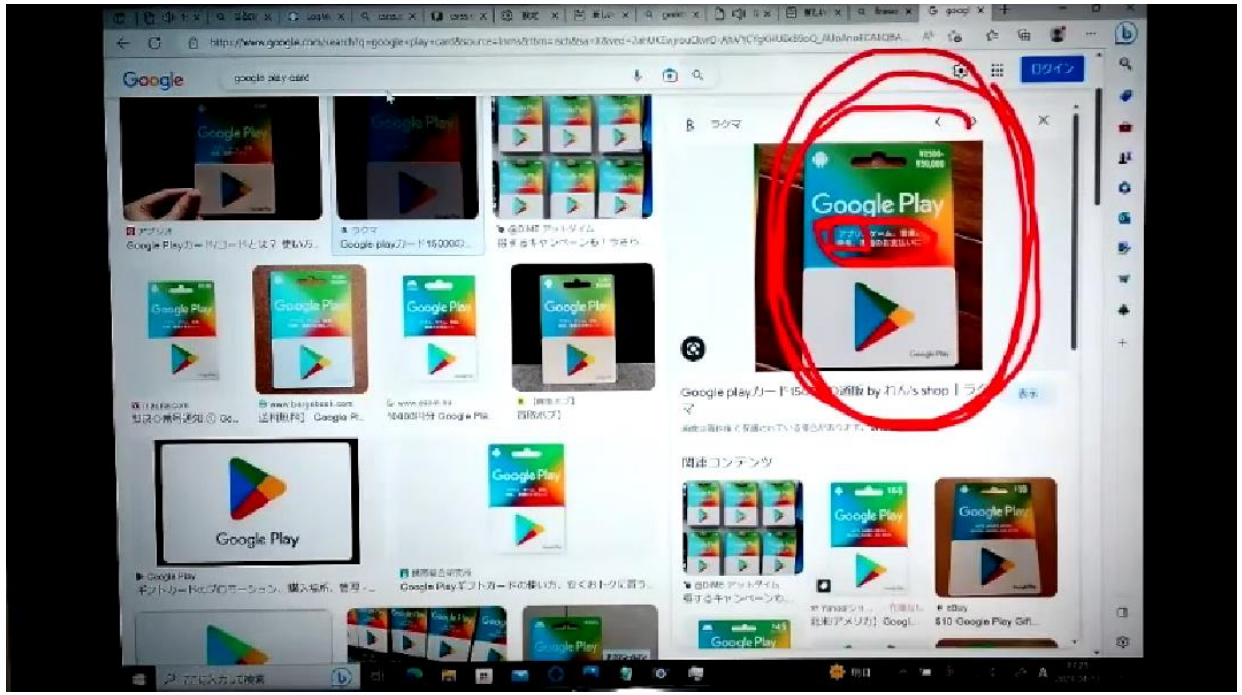
- 遠隔操作でウイルスを駆除するふりをする。
- 一度接続を切った場合は、操作される側が再び「承諾」をしないと遠隔操作はできない。

遠隔操作中は、相手の操作内容が見える

1.サポート詐欺

手口

■ 強引に有償サポート契約を勧める



- ほとんどの場合コンビニにプリペイドカードを買いに行くように指示をする。
- カードを買ってくると「番号が無効だ」などとでたらめを言って、繰り返し買いに行くことを指示する。
- ネットバンキングにログインをさせて振り込みを指示するケースも確認されている。

1.サポート詐欺

■日本テレビ　news every.　2024年1月8日放送

年々増える「サポート詐欺」 “ウイルス感染”電話すると「マイクロソフト」名乗る人物が…

https://news.ntv.co.jp/category/society/141f90c7b9cd4d1f8d70c22a0be137e6

1.サポート詐欺

対処

今日の内容で一番覚えてもらいたいこと！

偽の警告画面に記載されている
電話番号に
電話をかけないでください。

1.サポート詐欺

対処

■ 偽のセキュリティ警告画面を閉じる

偽の セキュリティ警告画面の消しかた

簡単な操作方法

まずこの方法を試してください。

① ESC を2～3秒間押下します。（長押し）

② 偽の警告画面がひと回り小さい表示となり、ウィンドウの右上に『閉じるボタン』（×）が表示されますので、クリックしてください。

強制再起動による方法

左の操作で消せない場合に試してください。
遠隔操作中の場合はこの方法を推奨します。

① Ctrl と Alt と Delete を押下します。

② 画面右下の『電源ボタンアイコン』をクリックして、『再起動』を選択してください。
※再起動すると保存していないデータは失われる場合があります。

「ブラウザの閉じ方」の実施手順書

1.サポート詐欺

対処

- 偽セキュリティ警告（サポート詐欺）画面の閉じ方体験サイト
- 画面の閉じ方が練習できます！！

パソコンでの体験のみ

https://www.ipa.go.jp/security/anshin/measures/fakealert.html

1.サポート詐欺

対処

■ 遠隔操作ソフトのアンインストールとシステムの復元

- 当該ソフトウェアのアンインストールをしてください。アンインストールすることで遠隔操作ソフトは削除されます。
- より安全な対処として「システムの復元」を行い、不審なソフトをインストールする前の状態にパソコンを戻すことを推奨します。
- 「システムの復元」が実行できない場合はパソコンの初期化を推奨しています。
- 操作方法などはパソコンメーカーにお問い合わせください。

「アンインストール」の実施手順書

「システムの復元」の実施手順書

1.サポート詐欺

対策

- 警告画面記載の電話番号に電話をかけない
- 遠隔操作ソフトをダウンロードもインストールもしない
- 購入・契約しない

2.不在通知の偽SMS

2. 不在通知の偽SMS

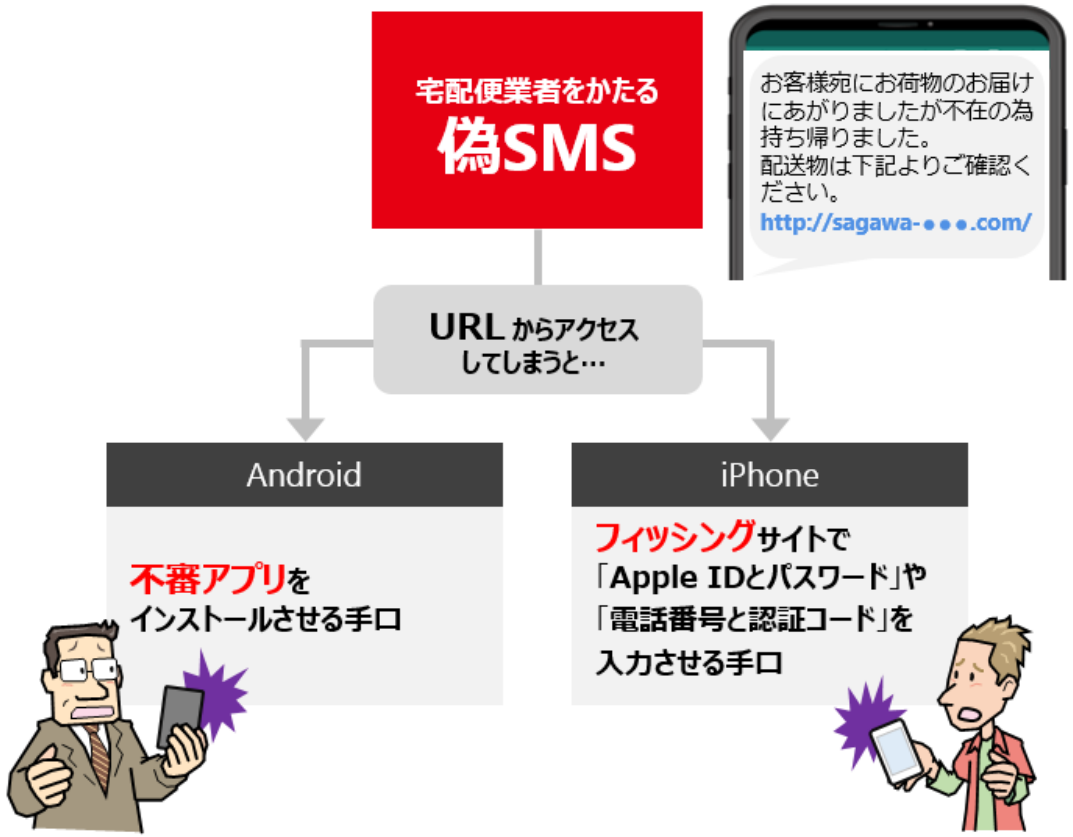
2.不在通知の偽SMS

- 宅配便業者を騙った不在通知の偽SMSが届く

安心相談窓口だより
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

2.不在通知の偽SMS

手口



- SMS内に書かれたURLから偽サイトに誘導される。
- **アクセスした端末のOSごとに、偽サイトアクセス後の手口が異なる。**
- Androidは不正アプリのインストールへ誘導する手口。
- iPhoneはフィッシングサイトでの情報を入力へ誘導する手口。

2.不在通知の偽SMS

手口　Android

- 偽SMS　⇒　偽のサイトに誘導　⇒　不正アプリのダウンロード

2.不在通知の偽SMS

手口　Android

- 提供元不明アプリのインストール許可　⇒　不正アプリのインストール

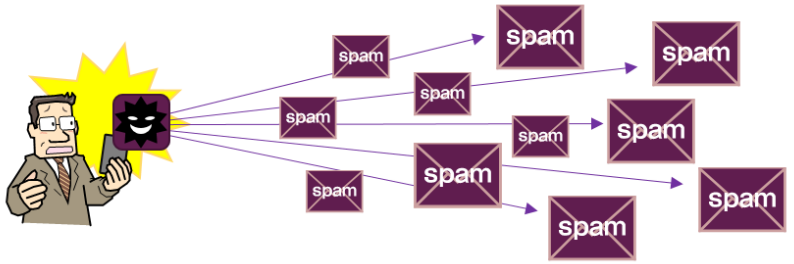
2.不在通知の偽SMS

手口　Android

● 不正アプリをインストールした場合の影響

■ 同じ内容の偽SMSを送信される

- そのSMSを受信した相手から、折り返しの電話やSMSの返信が来る場合があります。
- SMSメッセージ送信料金が発生するため、電話料金が増大します。



■ スマートフォン内のデータの不正使用

- 不正なアプリによりスマートフォン内のデータやSMSメッセージが窃取され、不正使用される可能性があり、当窓口には、次のような相談が寄せられています。
  - ➢ 携帯電話会社が提供するキャリア決済サービスにて、身に覚えのない請求が発生した。
  - ➢ フリーマーケットサービス、後払い決済サービス、その他のアカウントサービス等にアカウントを勝手に作成され、不正使用された。

2.不在通知の偽SMS

対処　Android

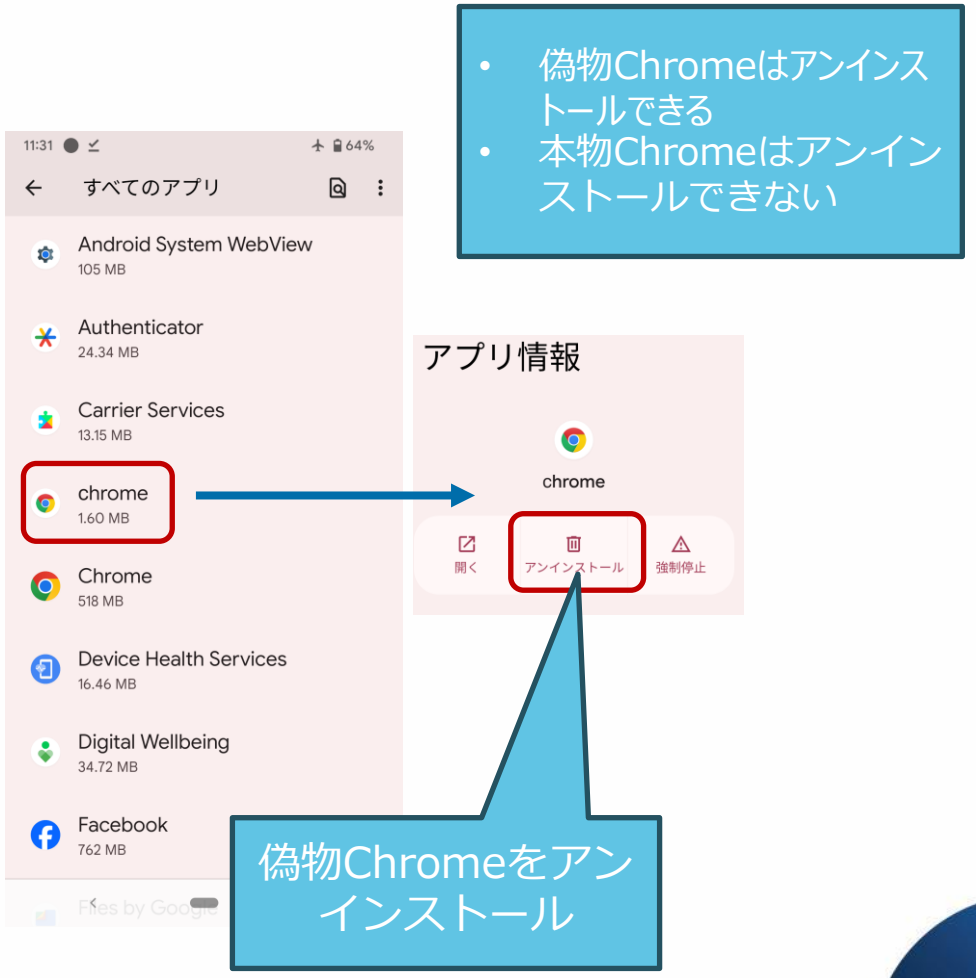
■ 不正なアプリの削除と影響の軽減

(1)スマートフォンを機内モードに

- スマートフォンを機内モード（Wi-Fi接続もオフ）に設定してください。これにより、通信を無効化し、当該スマートフォンからSMSの送信を抑止することが可能です。また、当該スマートフォン内の情報が外部に送信されることもなくなります。

(2)不正アプリのアンインストール

- 機内モードの状態で、不正なアプリのアンインストールを実施してください。アンインストールすれば、これ以降新たにSMSは送信されません。
- アプリはスマートフォンのホーム画面には表示されない場合もありますので、設定アプリのアプリ一覧から探してアンインストールを実施してください。



2.不在通知の偽SMS

対処　Android

■ 不正なアプリをインストールした場合の対処

(3)スマートフォンの初期化

- 不正なアプリのインストールによる、スマートフォン本体への影響範囲は不明です。そのため、より安全な対処として、アプリのアンインストールだけではなく、スマートフォンの初期化を推奨します。

- 初期化の実施後にデータの復元を行う際は、不正なアプリをインストールした時点より前のバックアップデータを使用してください。初期化の操作方法はお使いのスマートフォンを契約している携帯電話会社等にお問い合わせください。

(4)アカウントのパスワード変更

- 初期化後にGoogleアカウント、およびスマートフォンで利用しているサービスの各アカウントのパスワードを変更してください。

- 各アカウントのパスワードはできるだけ「長く」、「複雑」なものとしてください。そして、それらのパスワードを「使い回さない」ようにしてください。また、「多要素認証」が提供されている場合、利用することを推奨します。

2.不在通知の偽SMS

対処　Android

■ 不正なアプリをインストールした場合の対処

(5)キャリア決済の請求確認

- 身に覚えのないキャリア決済の請求が発生していないか、使用している携帯電話会社に確認してください。

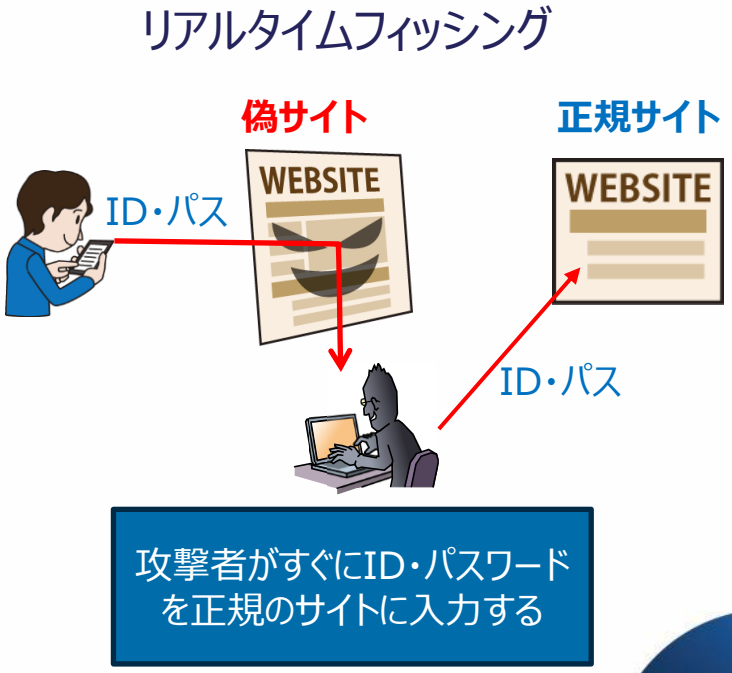
(6)その他アカウントサービス等の不正使用確認

- 不正アプリのインストール以降、携帯電話会社、フリーマーケットサービス、後払い決済サービス、その他のアカウントサービス等から登録や変更に関するメールやSMS等が届いていた場合は、当該サービス提供会社へ不正使用が発生していないか等を確認してください。

2.不在通知の偽SMS

手口　iPhone

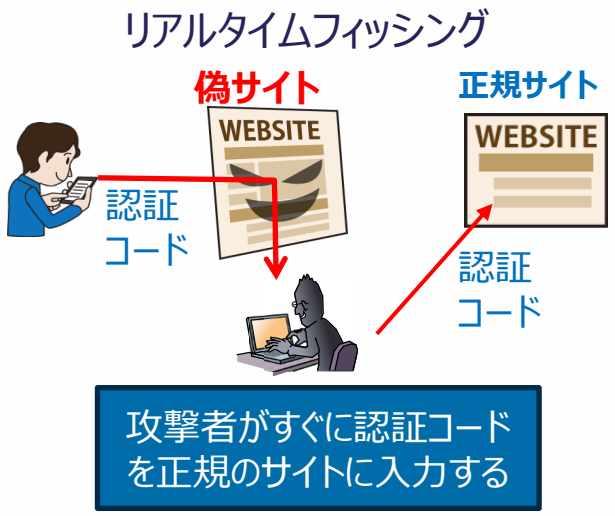
- 偽SMS　⇒　偽のサイトに誘導　⇒　アカウント情報の入力



2.不在通知の偽SMS

手口　iPhone

- 2 要素認証の突破 ⇒ クレジットカード情報の入力



2.不在通知の偽SMS

手口　iPhone

● フィッシングサイトに情報を入力した場合の影響

■ アカウントの不正ログインや不正使用

- フィッシングサイトで情報を入力した場合は、その情報を不正使用される可能性があります。
- 当窓口には、次のような相談が寄せられています。
  - Apple ID、パスワード、認証コードを入力したところ、不正ログインされた。
  - Apple ID に登録してあるキャリア決済等で、身に覚えのない請求が発生した。

■ クレジットカード情報の不正使用

- クレジットカード情報を入力した場合は、その情報を不正使用される可能性があります。

2.不在通知の偽SMS

対処　iPhone

- フィッシングの被害を軽減する
  - フィッシングサイトにアカウントのIDとパスワードを入力した場合
  - アカウントのパスワード変更
    - フィッシングサイトにApple IDとパスワード、またはその他のIDとパスワードなどを入力した場合は、パスワードを至急変更してください。パスワードはできるだけ「長く」、「複雑」なものとしてください。そして、それらのパスワードを「使い回さない」ようにしてください。
    - また、「多要素認証」が提供されている場合、利用することを推奨します。
    - 情報を入力したアカウントサービスで不正使用が発生していないか、当該サービス提供会社へ確認してください。
  - フィッシングサイトにクレジットカード情報を入力した場合
  - クレジットカード会社へ連絡
    - フィッシングサイトにクレジットカード情報を入力した場合は、クレジットカード会社へ至急連絡し相談してください。

2.不在通知の偽SMS

対処　iPhone

■ 受け取ったSMSは削除

- SMSを開いただけでは被害は発生しませんので、削除するだけで大丈夫です。
- SMS本文のURLからフィッシングサイトにアクセスした場合でも、そのサイトで情報の入力等の操作をしていなければ基本的に被害は発生しません。

2.不在通知の偽SMS

対策　Android／iPhone

■ すぐに対応を求めるような内容は偽SMSであることを疑い、メール内のURLを安易にタップしない

- リンク機能は便利ですが、不審なサイトへの誘導にも使われます。これまで見たことのないSMSやメールが届いたら、URLをタップする前に、公式サイトなど確かな情報源を使って真偽を確認してください。
- また、届いたメッセージの全文や一部をインターネット検索することでメッセージに関する情報が得られる場合もあります。

■ アプリは公式マーケット（Google Play、App Store）からインストールする

- 突然送られてきた不審なSMSやメールのURLからアプリをインストールすることは控えてください。

■ パスワードや認証コード等を安易に入力しない

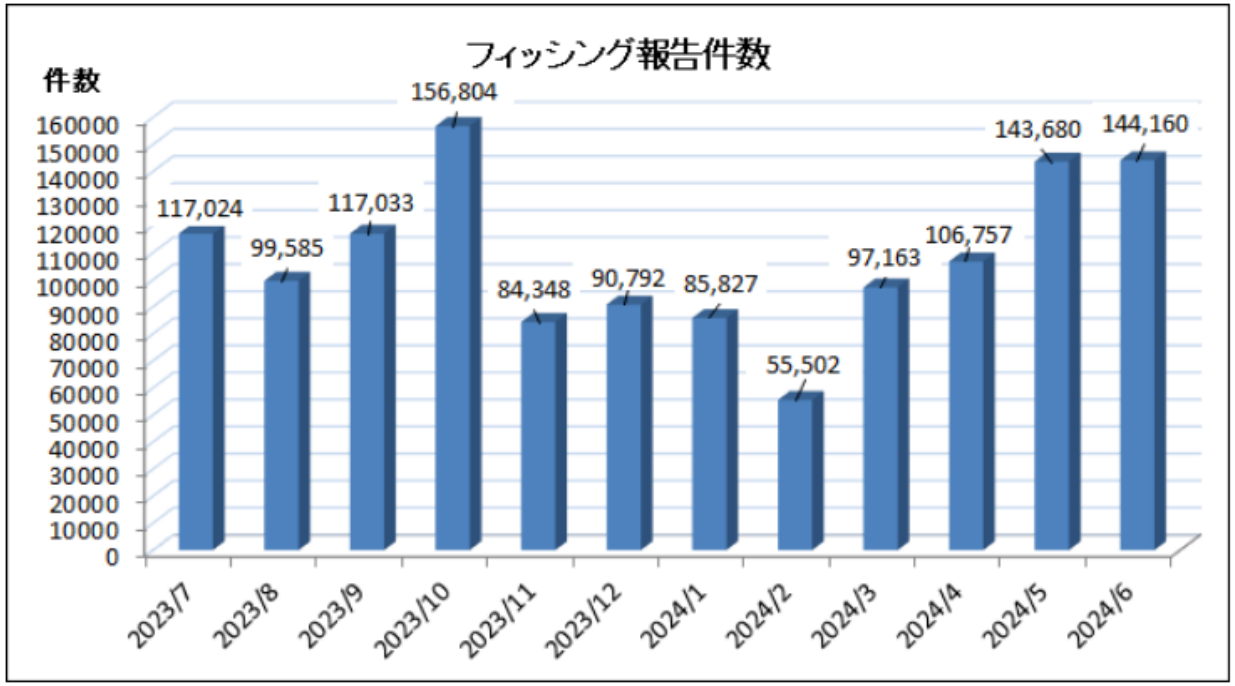
- パスワード、認証コード、クレジットカード情報など、重要な情報は安易に入力しない習慣をつけてください。

3. フィッシング

3.フィッシング

- 2024 年 6 月のフィッシング報告件数は 144,160 件となり、2024 年 5 月と比較すると 480 件増加でほぼ同数となりました。
- Amazon をかたるフィッシングの報告は前月と比較すると減少傾向とはなりましたが、報告数全体の約 26.3 % を占めました。
- 次いで各 2 万件以上の報告を受領した三井住友カード、ヤマト運輸、各 1 万件以上だった東京電力、イオンカードをかたるフィッシングの報告をあわせると、全体の 82.1 % を占めました。
- 特にヤマト運輸をかたるフィッシング報告数は、前月の約 26 倍と急増しました。

フィッシング対策協議会に寄せられたフィッシング報告件数



https://www.antiphishing.jp/report/monthly/202406.html

3.フィッシング

手口（その他）

■ Amazonのフィッシング

偽メール

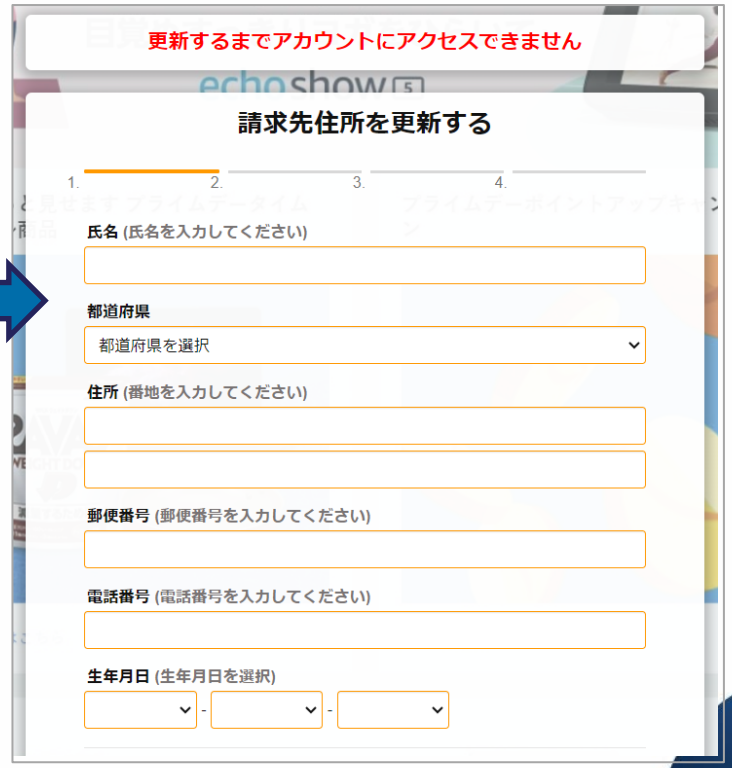
Amazonプライム会員様への重要なお知らせ

※本メールは重要なお知らせのため、メールを受け取らない設定をされている方にも。
Amazon に登録いただいたお客様に、Amazon アカウントの情報更新をお届けします。
残念ながら、Amazon のアカウントを更新できませんでした。
今回は、カードが期限切れになってるか、請求先住所が変更されたなど、さまざまな理由でカードの情報を更新できませんでした。
お客様のアカウントを維持するため Amazon アカウントの 情報を確認する必要があります。下からアカウントをログインし、情報を更新してください。

Amazonログイン

※24時間以内にご確認がない場合、誠に申し訳ございません、お客様の安全の為、アカウントの利用制限をさせていただきますので、予めご了承ください。

偽サイト



3.フィッシング

手口（ヤマト運輸をかたるフィッシング）

偽メール

お荷物お届けのお知らせ【受け取りの日時や場所をご指定ください】

●●様
ヤマト運輸をご利用いただきありがとうございます。
お届けに参りましたが、お届けできず持ち帰りました。
お荷物情報
送り状番号：4108-●●●●-●●●●
サービス名：EAZY（置き配指定可能）
品名：発送商品
＼＼ このお荷物は置き配指定が可能です ／／
再配達を依頼する

お知らせ　新型コロナウイルス対策について
荷物をお受け取りいただく際、玄関先での「受領印・サインの省略」「非対面でのお受け取り」などを推奨しています。
非対面でお受け取りいただく方法は**こちら**
よくある質問は**こちら**
・このメールへの返信は承れません。
・本メールの内容にお心あたりが無い方は、**こちら**から「よくあるご質問」をご確認お願いします。 **ヤマト運輸を装った迷惑メール・通知にご注意ください**
ヤマト運輸を装った不審なメールや通知が発生しています。
記載されたURLや添付ファイルを開いたり、メールに返信したりされないようご注意ください。
また、ヤマト運輸はSMSで通知を配信していません。
ヤマト運輸株式会社

偽サイト

3.フィッシング

手口（東京電力をかたるフィッシング）

偽メール

【重要なお知らせ】未払いの電気料金についてご連絡させていただくものです。お客様のお支払い方法が承認されません

このメールは、未払いの電気料金についてご連絡させていただくものです。お手数ですが、以下の内容をご確認いただき、早急にお支払いいただけますようお願い申し上げます。

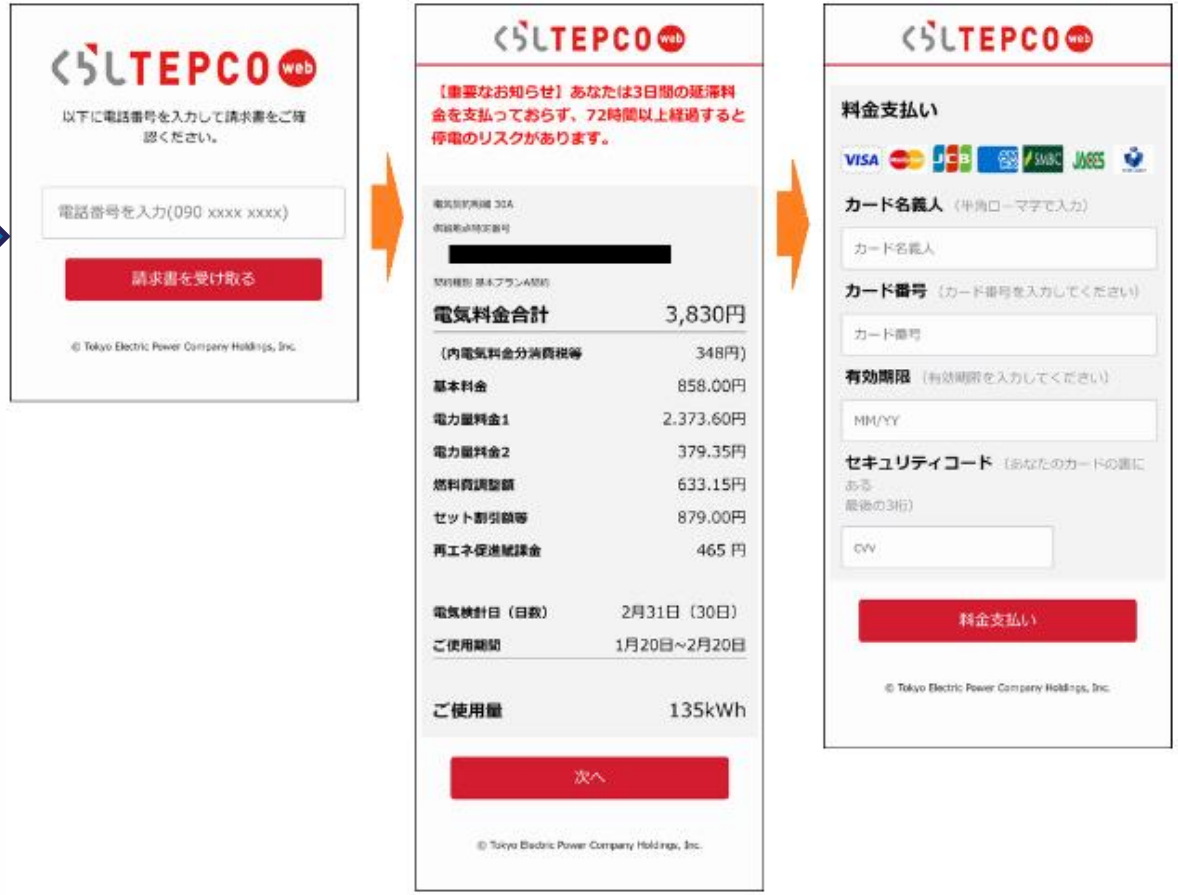
お支払い期限: 07/25/2024
お支払いが確認できておりませんので、お早めにお支払いください。

オンラインでのお支払い: ▼ **支払いの詳細リンク**

※更新の有効期限は、24時間です。
お支払い前に、添付の請求書をご確認いただき、お支払い金額が正確であることをご確認ください。
既にお支払いいただいた場合は、このお知らせを無視していただいて結構です。ご不明な点やご質問がある場合は、お気軽にお問い合わせください。お客様サポートチームがお手伝いいたします。
ご協力とご理解に感謝いたします。早期のお支払いをお待ちしております。

東京電力エナジーパートナー株式会社
〒100-8560 東京都千代田区内幸町1丁目1番3号

偽サイト



3.フィッシング

手口（国税庁をかたるフィッシング）

偽メール

国税庁重要なお知らせ

あなたの所得税は未納です、法律により現在あなたは所得税を自主的に納めることが求められています。
期限までに納付されない場合は、税法により不働産、自働車、登記財産、給与などの差し押さえが行われます。

▼納税確認番号：****3694

▼納付期限：2024/07/18

▼最終期限：2024/07/19（支払期日の延長不可）

» 支付の詳細リンクエント→

■本メールはe-tax国税電子申告納税送信専用となっており、返信を受け付けておりませんのでご了承ください。

発行元：国税庁

偽サイト

3.フィッシング

対処

■ 受け取ったメールは削除

- メールを開いただけでは被害は発生しませんので、削除するだけで大丈夫です。
- メール本文のURLからフィッシングサイトにアクセスした場合でも、そのサイトで情報の入力等の操作をしていなければ基本的に被害は発生しません。
- 差出人アドレスや文面からの判断が困難で本物かどうか迷った場合には、メール内のURLや電話番号は使用せず、公式サイトから真偽を確認することをおすすめいたします。

■ フィッシングサイトで情報を入力してしまった場合

- ID・パスワードを入力した場合は、速やかにパスワードを変更してください。
- 入力したパスワードを他のサービスでも使いまわしている場合は、同様にパスワード変更を実施してください。
- クレジットカード情報を入力した場合は、速やかにクレジットカード会社に相談してください。
- オンラインバンキングのID・パスワードや関連情報を入力した場合は、速やかに銀行へ相談してください。
- その他、入力してしまった情報に関係するサービス提供企業に速やかに相談してください。

3.フィッシング

対策

■ 真偽がはっきりしないメールは無視して削除

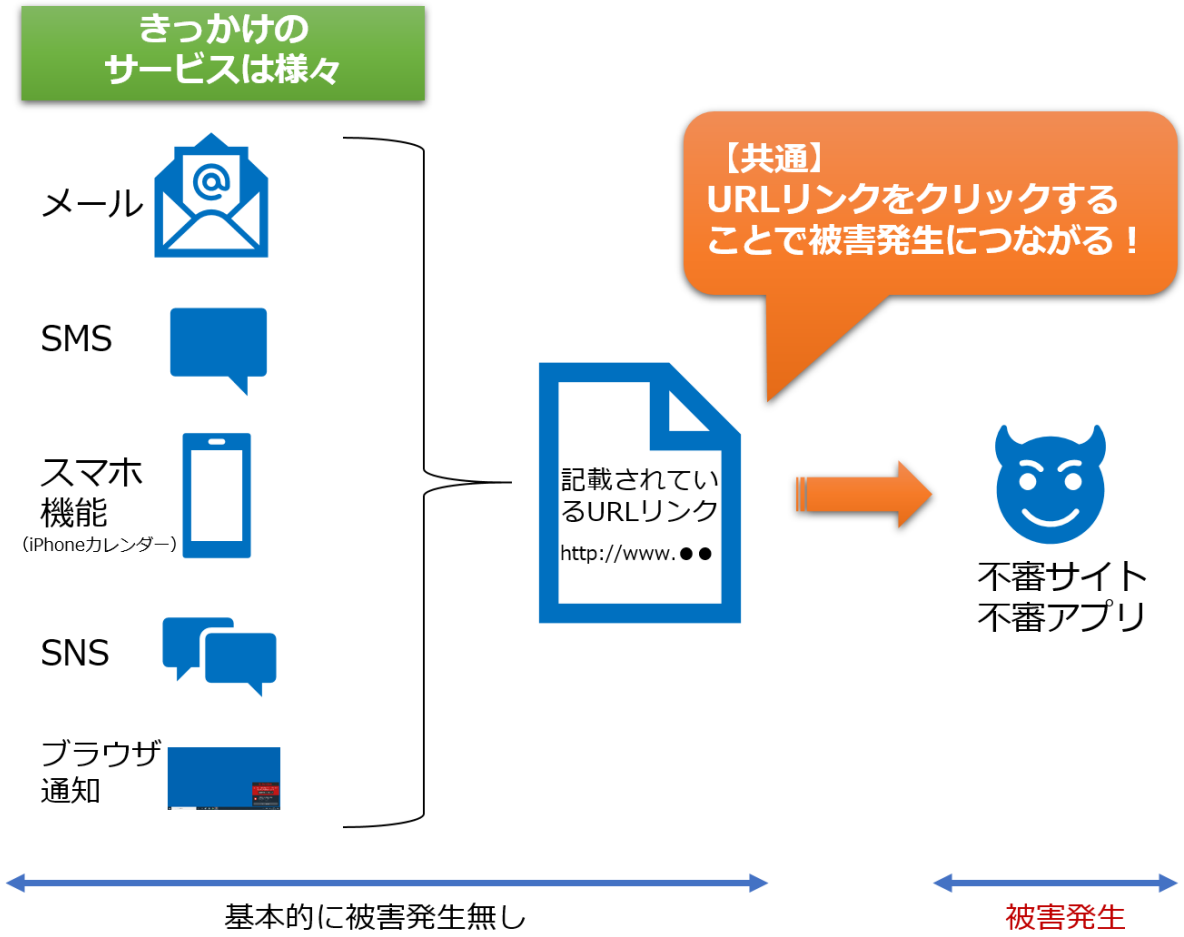
- 記載のURLからウェブサイトにアクセスしない
- 添付ファイルを開かない
- 記載の電話番号に電話をしない
- 返信しない

■ 迷惑メールフィルターを使う

- フィッシングメールは迷惑メールの一種であり、迷惑メールフィルターでその多くが検知、分別、削除できます。
- ほとんどのメールサービスでは迷惑メールフィルターが利用できますが、標準では設定が無効となっていることが多いため、設定を確認し、有効にしましょう。
- メールアプリやセキュリティ対策ツールの迷惑メールフィルター機能も併用すると効果的です。
- しかし、迷惑メールを完全に止める方法はありませんので、自分自身の判断が最も大切です。

3.フィッシング

対策



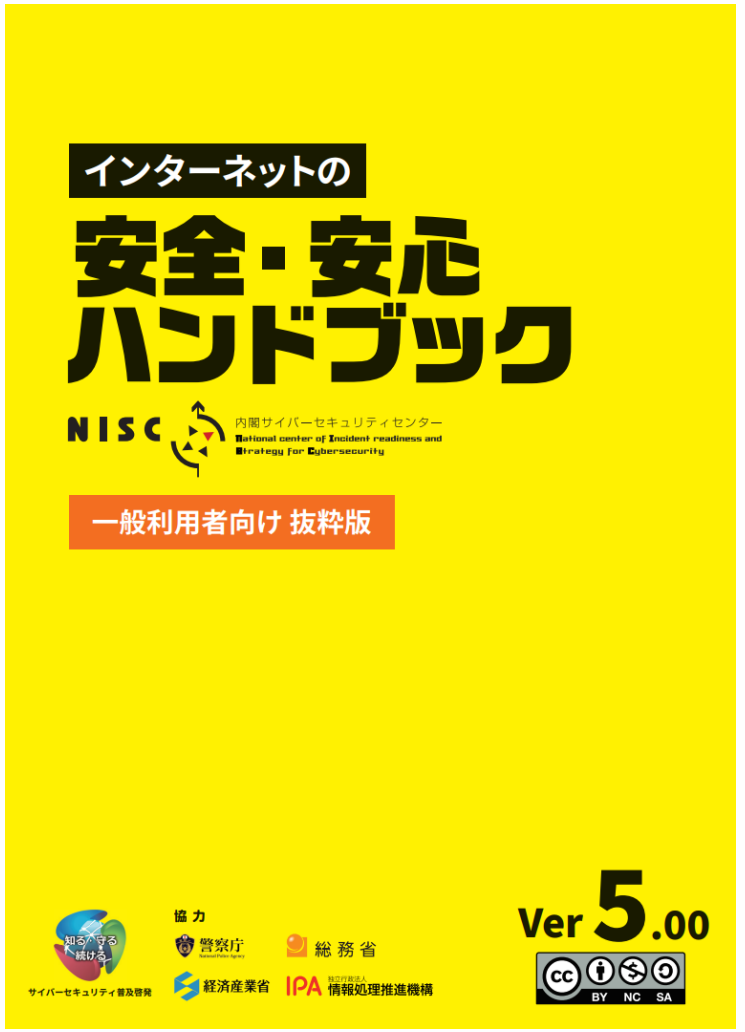
- 多くはURLのリンク先へアクセスすることで被害にあう。
- 外から届くURLは全て疑って、基本的にはアクセスしない。
- フィッシングメールや、フィッシングサイトを見極めるのは非常に困難。

安心相談窓口だより
URLリンクへのアクセスに注意！

インターネットの安全・安心ハンドブック

インターネットの
安全・安心
ハンドブック

https://security-portal.nisc.go.jp/guidance/handbook.html



- 内閣サイバーセキュリティセンター（NISC）
- 協力
  - 警察庁
  - 総務省
  - 経済産業省
  - 情報処理推進機構

サイバーセキュリティ対策9か条

IPA

1 OSやソフトウェアは常に最新の状態にしておこう

最新の攻撃に対抗するため、OSやソフトウェアメーカーが提供している修正用アップデートを常に適用しましょう。

2 パスワードは長く複雑にして、他と使い回さないようにしよう

パスワードは長く複雑にし、機器やサービス間で使い回さないことを徹底して安全性を高めましょう。

3 多要素認証を利用しよう

サービスへのログインを安全に行うために、認証用アプリや生体認証を使った多要素認証を利用しましょう。

4 偽メールや偽サイトに騙されないように用心しよう

フィッシング詐欺メールは年々手口が巧妙になっています。心当たりがあるものでもメールやメッセージのURLには安易にアクセスしないようにしましょう。

5 メールの添付ファイルや本文中のリンクに注意しよう

心当たりのない送信元からのメールに添付されているファイルやリンクはもちろん、ファイルやリンクを開かせようとするものには注意しましょう。

6 スマホやPCの画面ロックを利用しよう

スマホやパソコン（PC）の情報を守るには、まず待ち受け画面をロックすることが第一です。短時間であっても端末を手元から離す際はロックを忘れないようにしましょう。

7 大切な情報は失う前にバックアップ（複製）しよう

大切な情報を失っても、バックアップから復元することで被害を軽減することができます。普段からバックアップして攻撃や天災に備えましょう。

8 外出先では紛失・盗難・覗き見に注意しよう

外出先でスマホやパソコンを使う時は、背後からの覗き見に注意しましょう。また、紛失・盗難の危険があるので、公共の場でスマホを放置することは絶対にやめましょう。

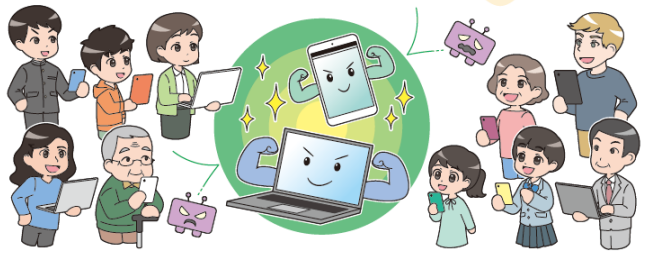
9 困った時はひとりで悩まず、まず相談しよう

インターネットでの被害に遭遇したら、ひとりで悩まず各種相談窓口に相談しましょう。

インターネットを安全・安心に利用するための

NISC IPA

サイバーセキュリティ対策 9 か条



https://security-portal.nisc.go.jp/guidance/cybersecurity9principles.html

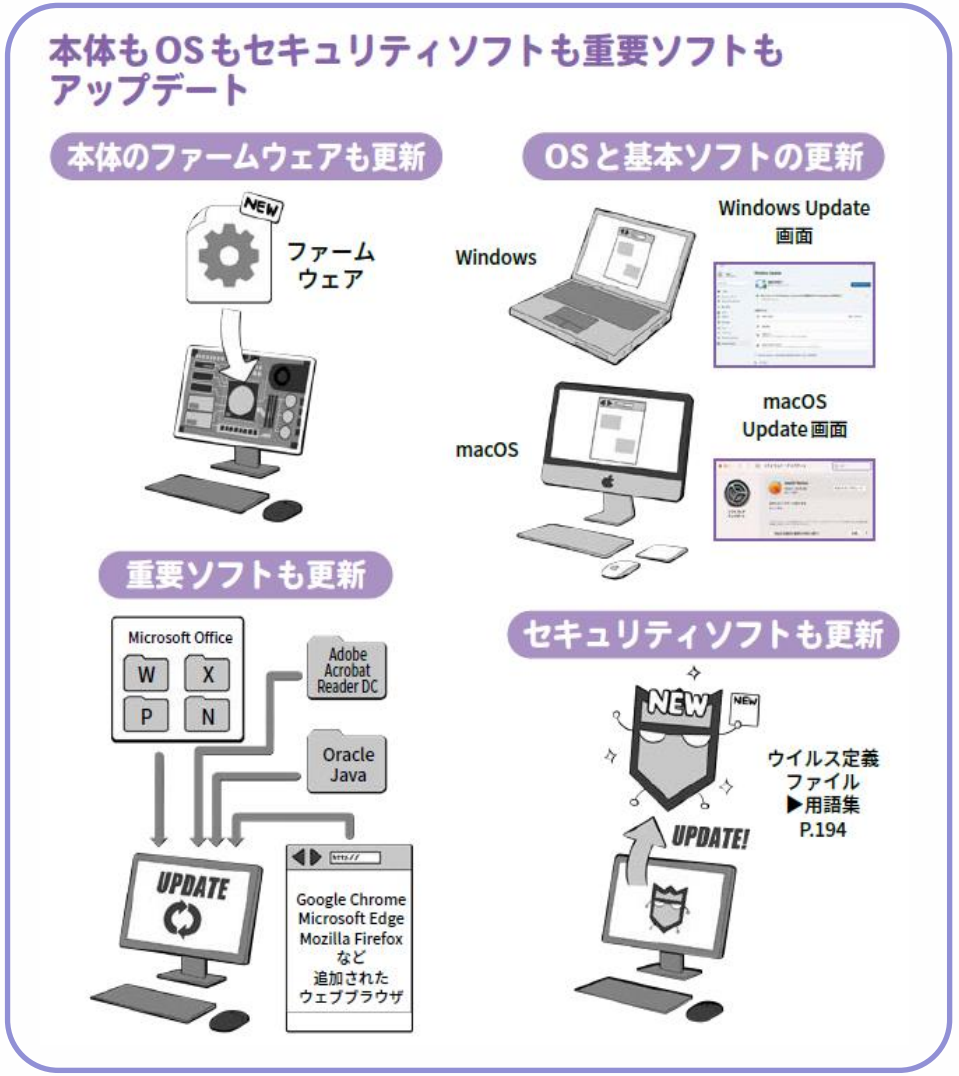
1.OSやソフトウェアは常に最新の状態にしておこう

1 OSやソフトウェアは常に最新の状態にしておこう

最新の攻撃に対抗するため、OSやソフトウェアメーカーが提供している修正用アップデートを常に適用しましょう。

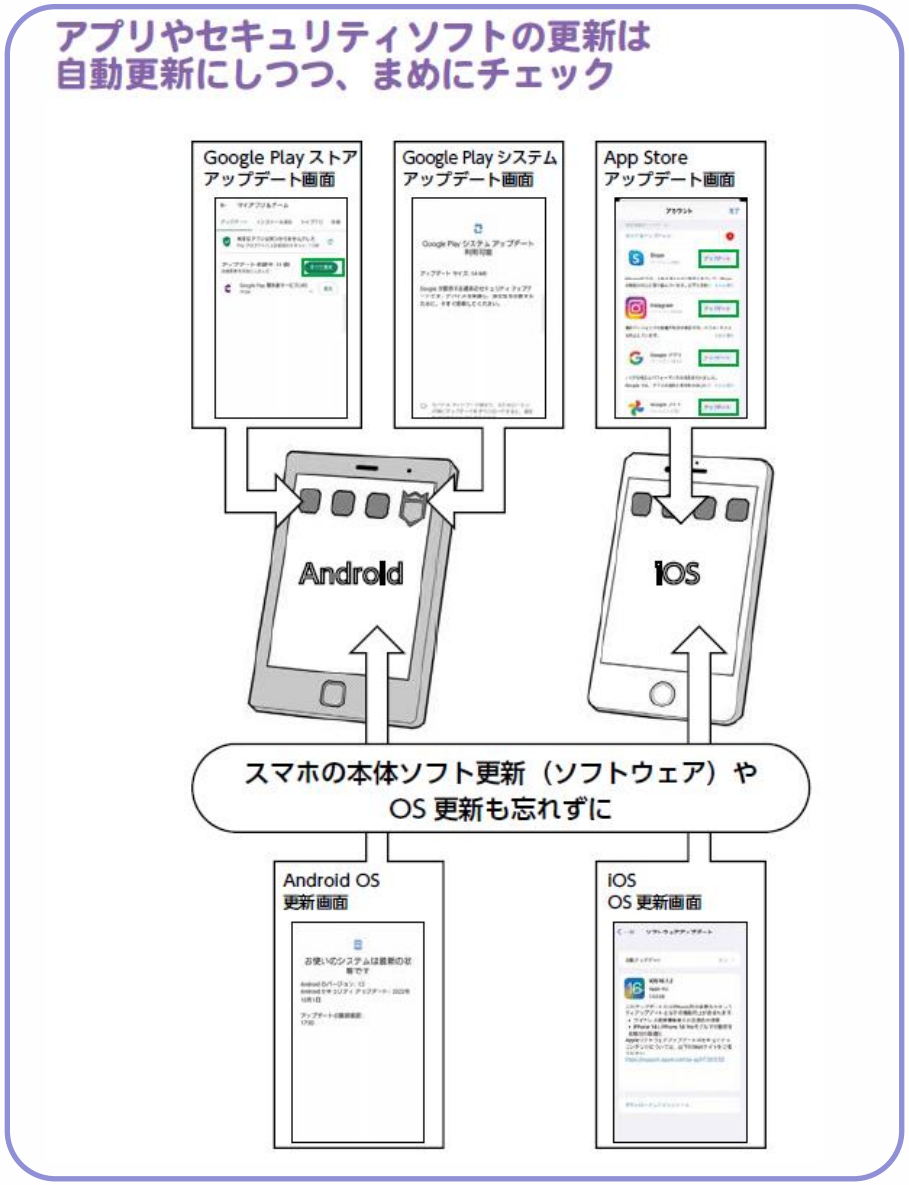
1.OSやソフトウェアは常に最新の状態にしておこう

- 悪意の攻撃からパソコンを守る第一歩は、セキュリティを最新に保ち、各種のアップデートを行いましょう。
- 最近の機種では、OS 関連のアップデート処理は自動で行われるか、アップデートを行うよう通知が出ます。
- セキュリティソフトをインストールしている場合は、最新のウイルス定義ファイルに自動更新されるよう設定しましょう。



1.OSやソフトウェアは常に最新の状態にしておこう

- スマホの場合、比較的アップデートの通知がわかりやすくなっており、自動アップデート機能も充実しています。
- 機器本体のファームウェアのアップデートでも、OS のアップデートでも、いつも使用している一般のアプリのアップデートでも、更新の通知が出たら、マメに適用するようにしましょう。



1.OSやソフトウェアは常に最新の状態にしておこう

- また、ネットワークにつながるルータやIoT機器、スマート家電なども脆弱性を狙った攻撃の対象となるため、ファームウェアが自動更新されるよう設定しておきましょう。
- ルータはここ数年で自動更新機能搭載のものが普及してきているので、可能であれば買い換えしましょう。

ネットにつながるIT機器（ルータやIoT機器）もファームウェア更新や管理者用初期IDとパスワードの変更をしておくこと

無線LANアクセスルータ

ネットワーク対応プリンタ

ネットワークカメラ

2.パスワードは長く複雑にして
他と使いまわさないようにしよう

2 パスワードは長く複雑にして、他と使い回さないようにしよう

パスワードは長く複雑にし、機器やサービス間で使い回さないことを徹底して安全性を高めましょう。

2.パスワードは長く複雑にして 他と使いまわさないようにしよう

■ 不正ログイン被害

- 20代女性9人のインスタグラムのアカウントを不正に乗っ取ったとして、警視庁は、茨城県牛久市の派遣社員の男（28）を不正アクセス禁止法と私電磁的記録不正作出・同供用の疑いで逮捕し、18日発表した。
- 男は容疑を認め、「『リア充』の女性に嫉妬し、嫌がらせをしてやろうと思った」と話しているという。
- 署の調べに対し、「60人以上のアカウントを乗っ取って情報をのぞき見したりDMを送ったりしていた」と供述。
- 男が女性らの投稿内容から誕生日を割り出し、アカウント名と組み合わせるなどしてパスワードを把握したとみている。

朝日新聞デジタル ＞ 記事

「リア充の20代女性に嫉妬して」　インスタ乗っ取り容疑で男を逮捕

遠藤美波　2023年1月18日 11時41分

不正アクセスに使われたとされるパソコンや携帯電

20代女性9人のインスタグラムのアカウントを不正に乗っ取ったとして、警視庁は、茨城県牛久市の派遣社員の男（28）を不正アクセス禁止法と私電磁的記録不正作出・同供用の疑いで逮捕し、18日発表した。男は容疑を認め、「『リア充（リアル、現実の生活が充実している人）』の女性に嫉妬し、嫌がらせをしてやろうと思った」と話しているという。

https://www.asahi.com/articles/ASR1L3TJXR1LUTIL00D.html

2.パスワードは長く複雑にして 他と使いまわさないようにしよう

■ パスワードを破る手段

- 「総当たり攻撃」の他にも様々な手法があります。
- パスワードでよく使われる言葉などを集めた専用の辞書を利用する「辞書攻撃」。
- 流出した名簿やID・パスワードのリストを入力して試す「リスト型攻撃（アカウントリスト攻撃・パスワードリスト攻撃）」など。
- これらに対する防御のためにも、「ログインパスワード」には意味のある単語や、自分に関連の深い語句を使わず、充分に複雑で、かつ他の機器やサービスで使い回していないものを設定してください。

2.パスワードは長く複雑にして他と使いまわさないようにしよう

- 総当たり攻撃を防ぐには、探り当てるまでに膨大な時間がかかるようにするのが一番の防御手段です。
- 英大文字小文字＋数字＋記号混じりで10桁以上を安全圏として推奨します。
- しかし、より組み合わせ数を増やし安全性を高めるにこしたことはありません。

ログイン用パスワードは英大文字小文字＋数字＋記号で10桁以上

「ログインに使うパスワードは、英大文字小文字＋数字＋記号で10桁以上」の理由

「数字のみ」の10乗だと→100億通り

(英大文字小文字＋数字＋記号(88個として))の10乗だと→
約2785京97兆6009億通り

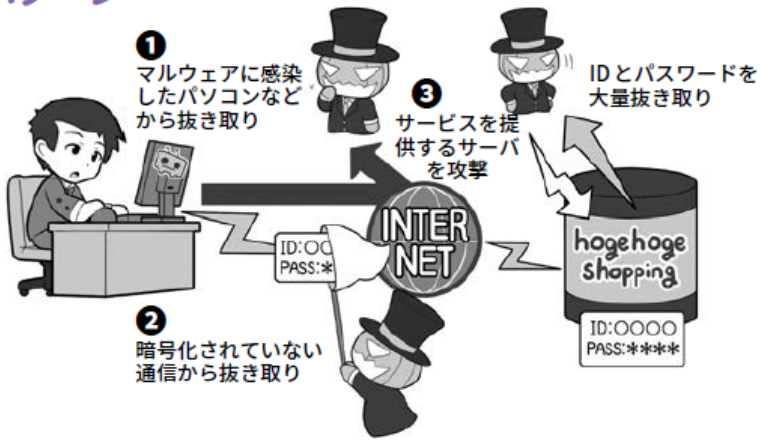
数字だけで10桁と、英大文字小文字＋数字＋記号で10桁では雲泥の差がある。
そしてこれほど多量な組み合わせは、機械入力でも事実上突破不可能。

2.パスワードは長く複雑にして 他と使いまわさないようにしよう

さまざまなIDとパスワードの漏えいパターン

攻撃者にIDとパスワードが漏えいする事態は、機器がマルウェアに感染したり、自分が通信する過程で抜き取られたりする他に、利用しているサービス側からも流出するケースもあります。

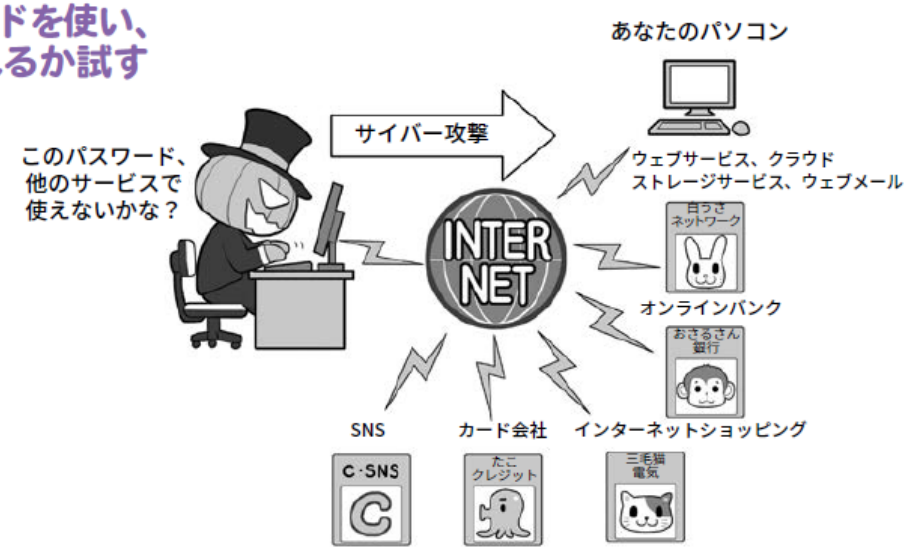
ニュースや通知でサービス側から流出が判明した場合は、速やかにパスワードを変更するなどの対応を取りましょう。



攻撃者は入手したIDとパスワードを使い、さまざまなサービスを乗っ取れるか試す

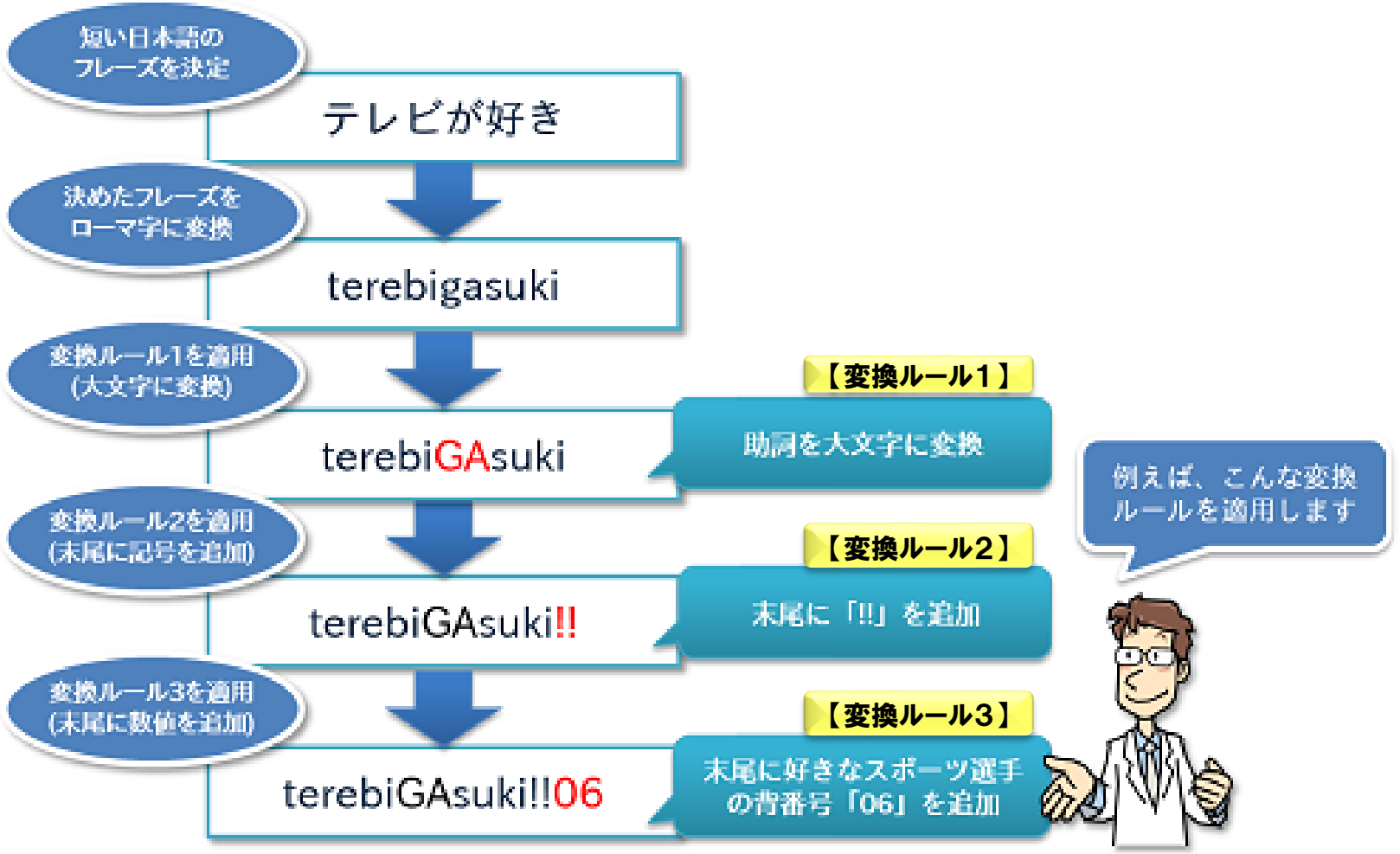
IDとパスワードをなんらかの手段で手に入れた攻撃者は、これをどこか別のサービスで使えないかさまざまな方法で試します。

こういった攻撃を成功させないために、パスワードの使い回し▶用語集 P.201や、似たパスワード、パターンのあるパスワード、個人情報などから推測できるパスワードを利用するのはやめましょう。



2.パスワードは長く複雑にして 他と使いまわさないようにしよう

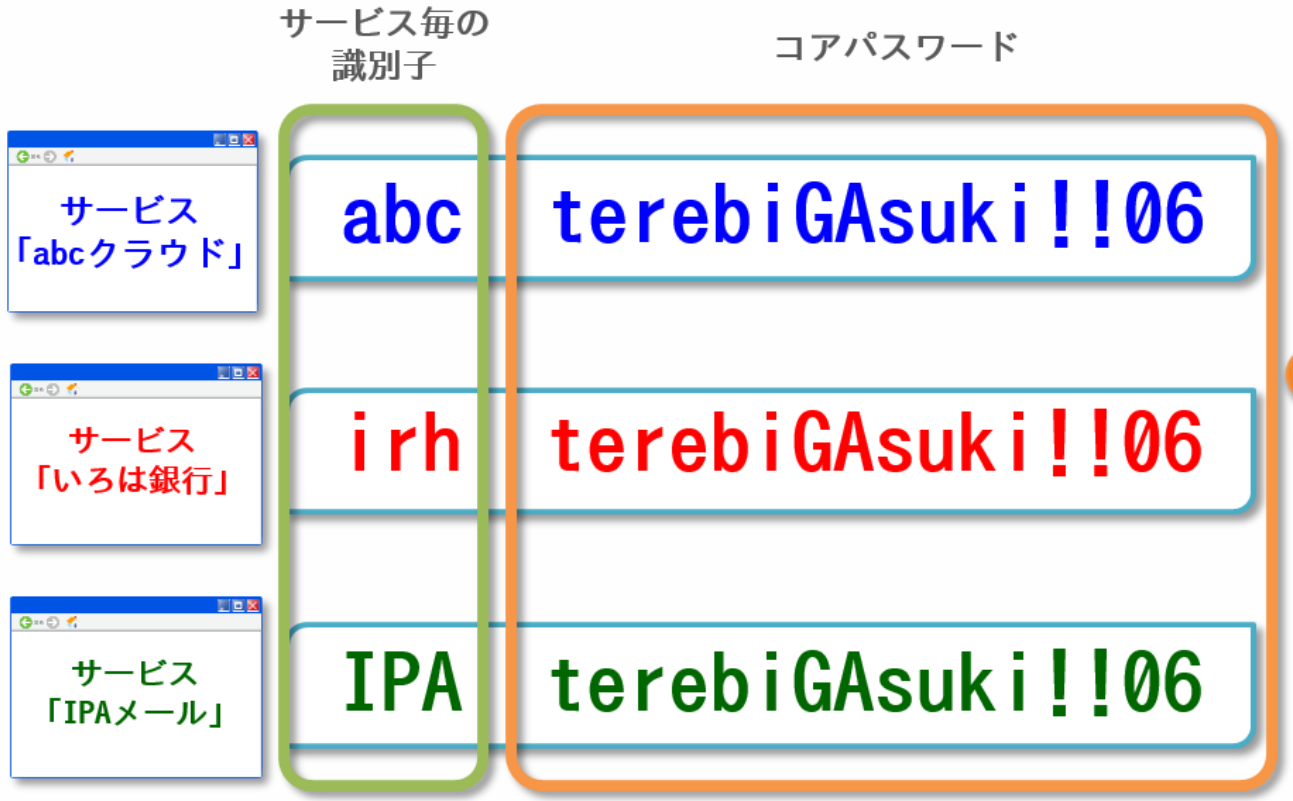
使い回しを回避するパスワードの作成・管理例
～①コアパスワードの作成～

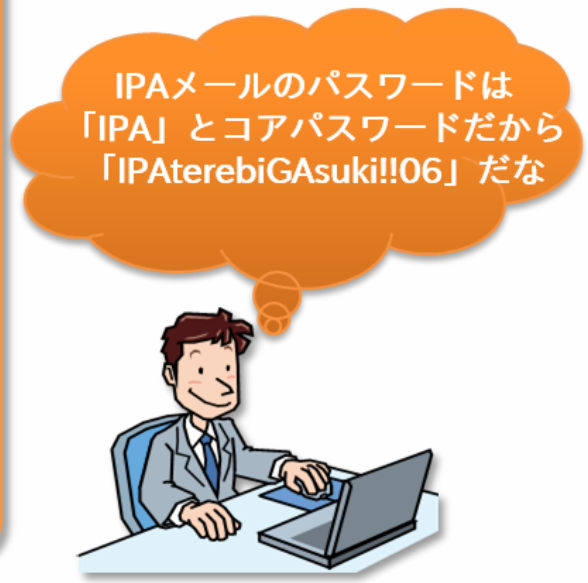


https://www.ipa.go.jp/security/anshin/attention/2016/mgdayori20160803.html

2.パスワードは長く複雑にして 他と使いまわさないようにしよう

使い回しを回避するパスワードの作成・管理例
～②サービス毎に異なるパスワードの作成～





https://www.ipa.go.jp/security/anshin/attention/2016/mgdayori20160803.html

2.パスワードは長く複雑にして 他と使いまわさないようにしよう

使い回しを回避するパスワードの作成・管理例
～③パスワードの管理方法～

これらの情報を電子ファイルなどで保存

※コアパスワードは、別途、紙などで管理

https://www.ipa.go.jp/security/anshin/attention/2016/mgdayori20160803.html

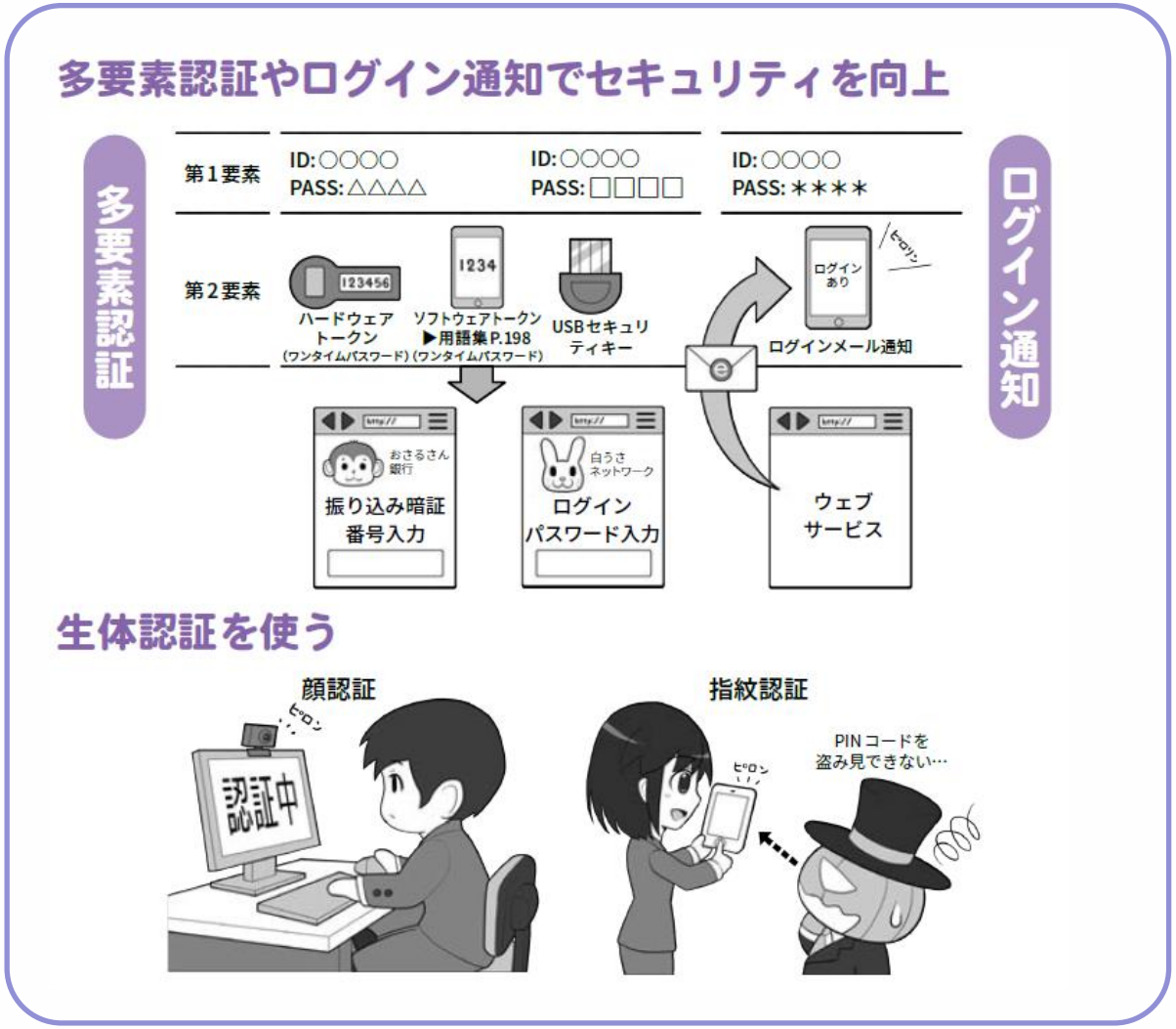
3.多要素認証を利用しよう

3 多要素認証を利用しよう

サービスへのログインを安全に行うために、認証用アプリや生体認証を使った多要素認証を利用しましょう。

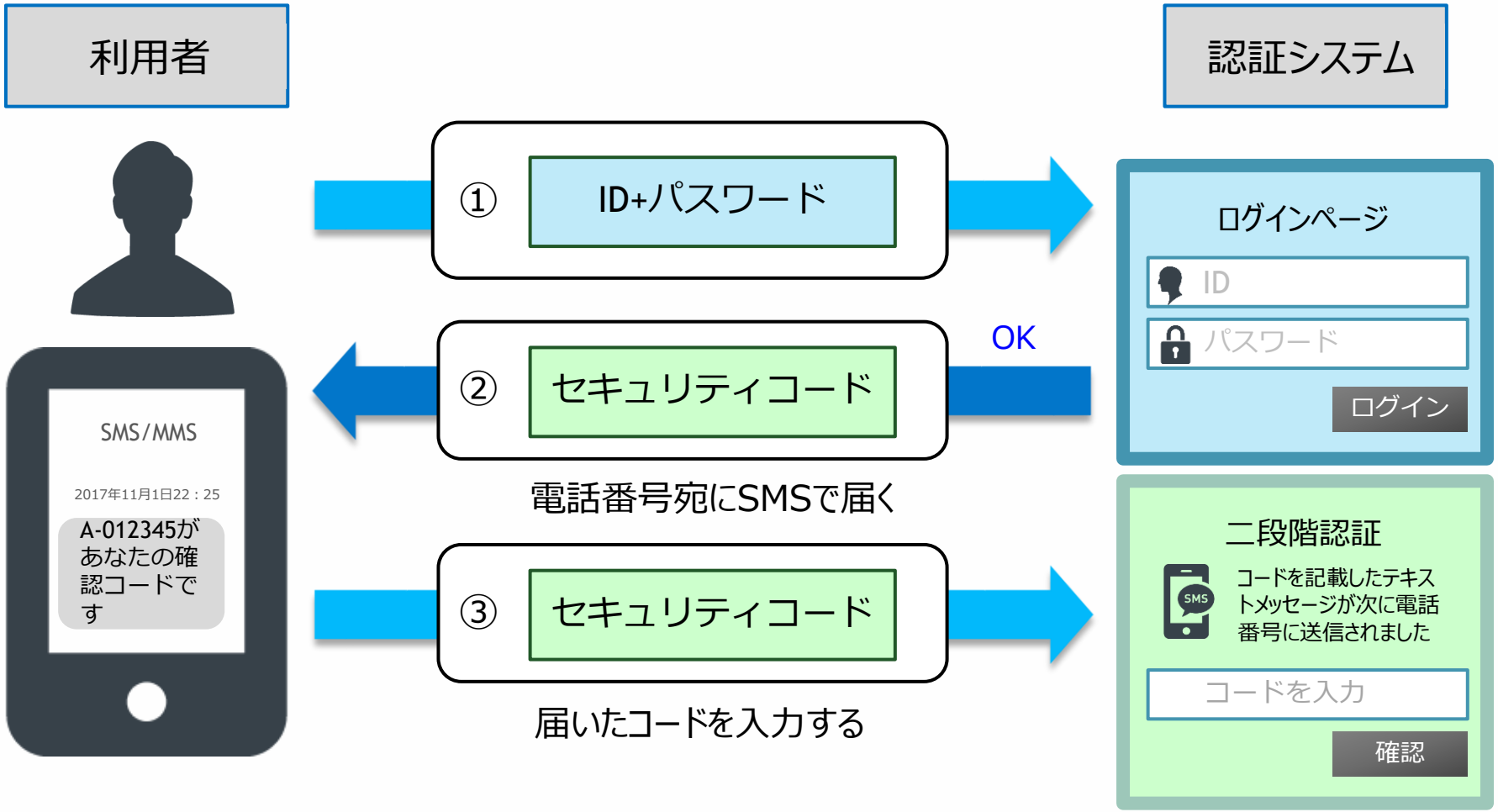
3.多要素認証を利用しよう

- サービスへのログインを安全に行うために、二要素以上を使って認証作業をする多要素認証などの方法が提供されていれば必ず設定しましょう。
- これらの方法では通常のパスワードの他に、使い捨てにする別のパスワードを、ハードウェアトークンや生成アプリで作り、ログイン時に利用者に入力させます。



3.多要素認証を利用しよう

- SMSを利用した多要素認証の例

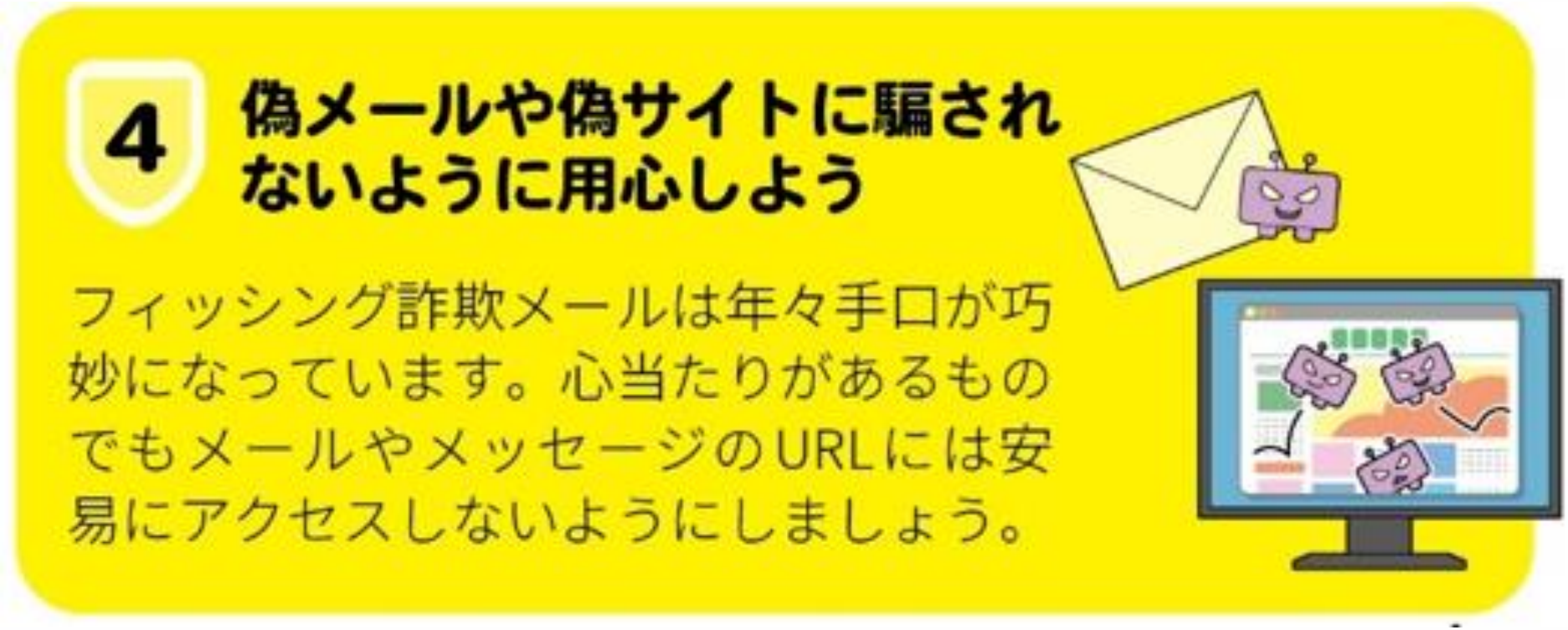


3.多要素認証を利用しよう

■ 2 要素認証を採用しているサービス例

- Googleアカウント（ 2 段階認証プロセス）
- Apple ID（2ファクタ認証）
- Microsoft アカウント（ 2 段階認証）
- Yahoo! JAPAN ID（ワンタイムパスワード）
- Amazon（ 2 段階認証）
- Facebook （ 2 段階認証）
- Instagram（ 2 段階認証）
- Twitter （ログイン認証）
- Dropbox（ 2 段階認証）
- Evernote （ 2 段階認証）

4.偽メールや偽サイトに騙されないように用心しよう

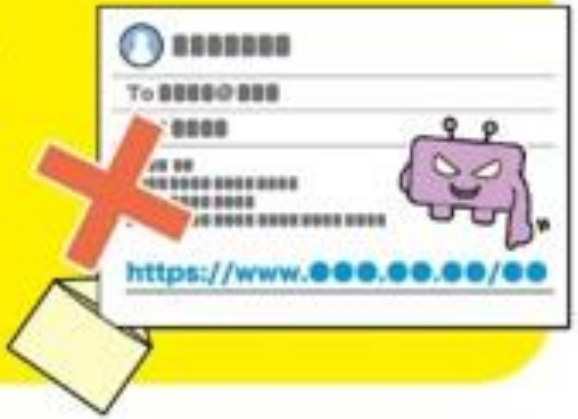


先ほどご説明した、「サポート詐欺」「フィッシング」の手口に注意してください。

5.メールの添付ファイルや本文中のリンクに注意しよう

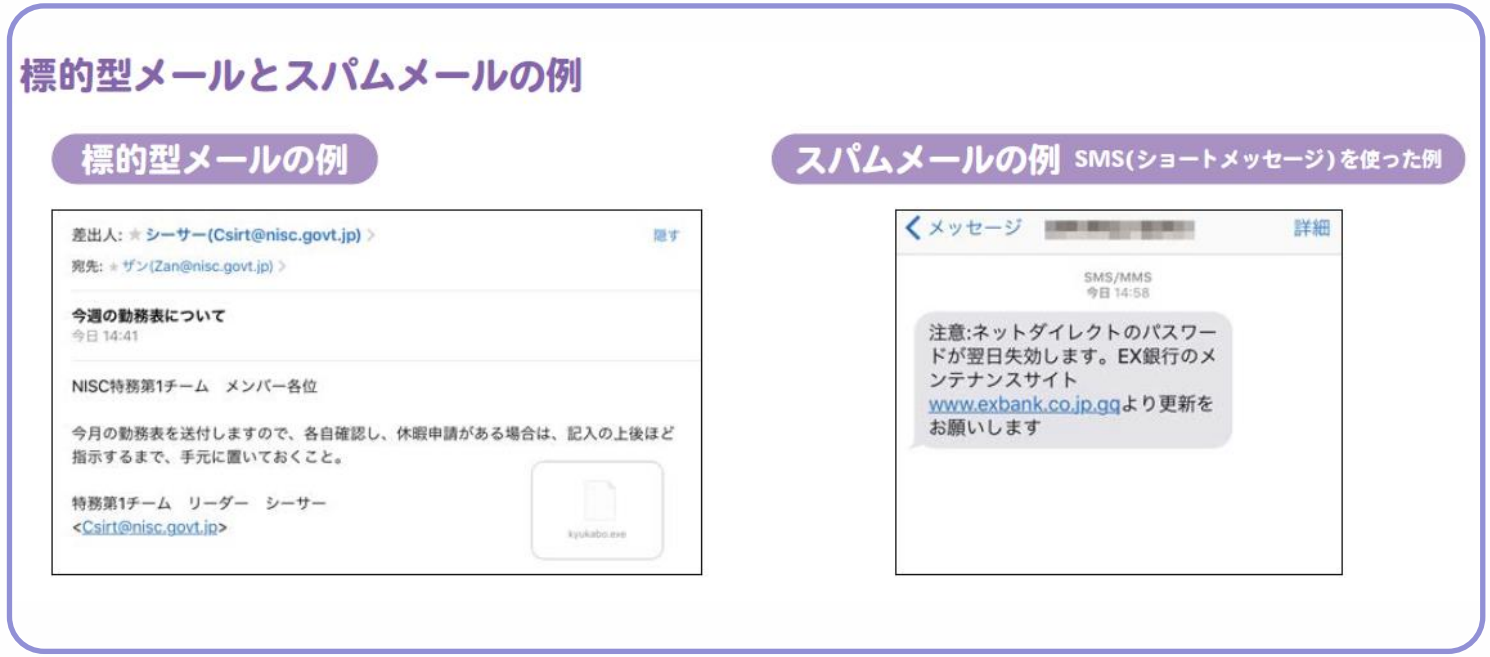
5 メールの添付ファイルや本文中のリンクに注意しよう

心当たりのない送信元からのメールに添付されているファイルやリンクはもちろん、ファイルやリンクを開かせようとするものには注意しましょう。



5.メールの添付ファイルや本文中のリンクに注意しよう

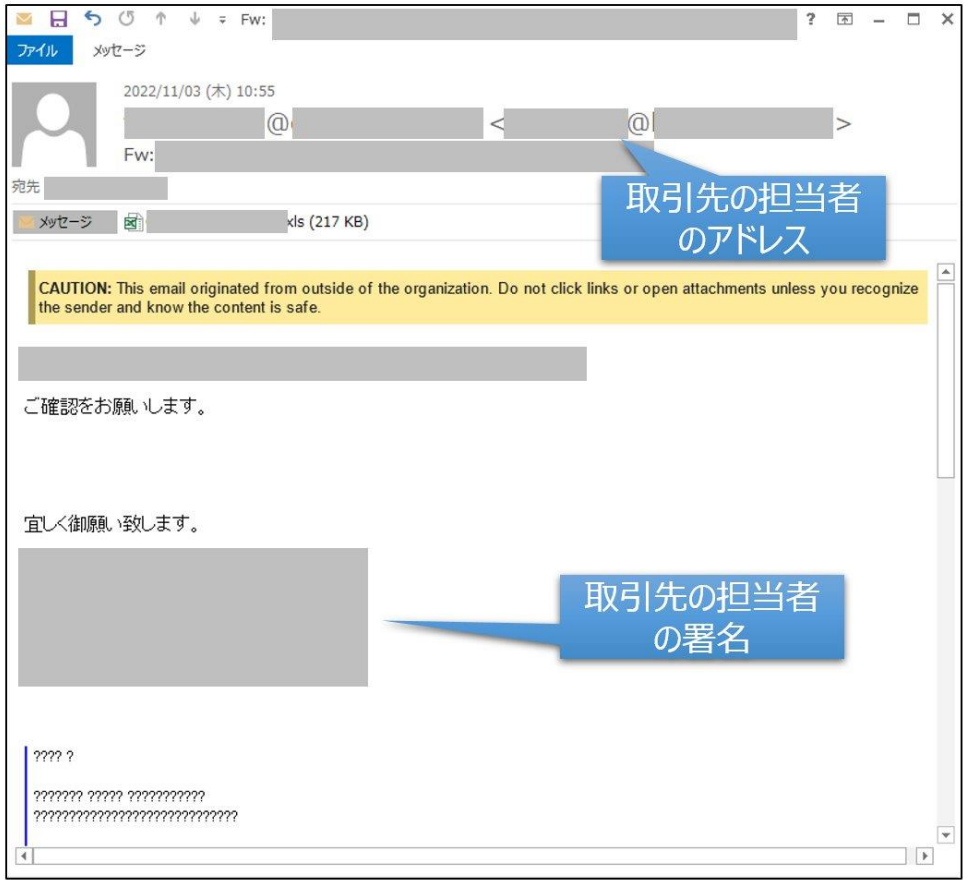
- 心当たりのない送信元からのメールに添付されているファイルやリンクは、基本信用ならないものとして、むやみやたらに開かないようにするとともに、機器の設定などを堅牢に保ち、感染の隙を作らないようにしましょう。



5.メールの添付ファイルや本文中のリンクに注意しよう

- ウイルス感染を狙ったメールの例

Emotetへの感染を狙う攻撃メールに注意！



メールを処理する時は、
メール1つ1つに注意を払ってください！

・安易に添付ファイルを開かない
・安易にURLをクリックしない

https://www.ipa.go.jp/security/emotet/index.html

6.スマホやPCの画面ロックを利用しよう

6 スマホやPCの画面ロックを利用しよう

スマホやパソコン（PC）の情報を守るには、まず待ち受け画面をロックすることが第一です。短時間であっても端末を手元から離す際はロックを忘れないようにしましょう。

6.スマホやPCの画面ロックを利用しよう

- スマホやパソコン（PC）の情報を守る第一歩は、待ち受け画面にロックをかけることです。
- ロック機能は「誰かにスマホを持ち去られるなど、手元からスマホが離れたとき」に情報を確実に守るためのしくみの1つです。
- とくに生体認証は周りから覗かれPIN コードを盗まれる危険性の排除をしつつ、入力の面倒くささを省くので便利な機能です。
- ただし、気を付けておきたいのは、セキュリティ向上のためのロック機能を設定しても、そのパソコンやスマホをロック解除したまま置いてその場所を離れたり、ロックを解除して他人に見せたり貸したりすれば、一瞬で情報を盗み、乗っ取ることが可能です。

7.大切な情報は失う前にバックアップ（複製）しよう

7 大切な情報は失う前にバックアップ（複製）しよう

大切な情報を失っても、バックアップから復元することで被害を軽減することができます。普段からバックアップして攻撃や天災に備えましょう。

7.大切な情報は失う前にバックアップ（複製）しよう

- 各種のサイバー攻撃や、パソコン・スマホの故障などからいち早く復旧して事業を継続するには、システムやデータのバックアップが不可欠です。
- なお、バックアップを取得するだけではなく、できれば取得したバックアップを用いてちゃんとシステムの復元を行えるか確認してください。
- バックアップの「3-2-1 ルール」というものがあります。
- バックアップは本体を含め3個以上、2種類以上の媒体、そして1個は遠隔地に置くというものです。

8.外出先では紛失・盗難・覗き見に注意しよう

8 外出先では紛失・盗難・覗き見に注意しよう

外出先でスマホやパソコンを使う時は、
背後からの覗き見に注意しましょう。
また、紛失・盗難の危険があるので、
公共の場でスマホを放置することは絶対にやめましょう。

8.外出先では紛失・盗難・覗き見に注意しよう

- 勤務先や外出先でスマホやパソコンを使う際に、誰かにスマホやパソコンを覗き見られている、そう感じたことはありませんか？
- 例えば、相手に直接接触せず情報を入手する方法として、電車で座席に座っている人のスマホ操作を見てPIN コードやパターンロック形状を盗む「ショルダーハッキング」、カフェなどのテーブルに放置されているスマホの画面に残る指の脂跡からパターンロックを見破る方法などがあります。

9.困った時はひとりで悩まず、まず相談しよう

9 困った時はひとりで悩まず、まず相談しよう

インターネットでの被害に遭遇したら、ひとりで悩まず各種相談窓口に相談しましょう。

9.困った時はひとりで悩まず、まず相談しよう

- 周りの友達
- 公的機関の相談窓口
- サービス事業者
- インターネット検索

https://www.ipa.go.jp/security/anshin/index.html

https://www.kokusen.go.jp/map/

https://www.npa.go.jp/bureau/cyber/index.html

情報提供

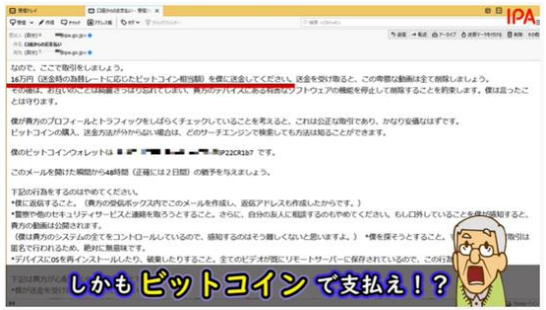
■ 安心相談窓口だより

- 「安心相談窓口だより」では、IPAの情報セキュリティ安心相談窓口に寄せられる相談内容などをもとに、情報セキュリティに関するさまざまテーマをピックアップして紹介していきます。
- 被害防止に向けた自己学習や普及啓発のための資料などとして活用してください。
- 「安心相談窓口だより」は不定期で公開・更新します。

https://www.ipa.go.jp/security/anshin/attention/index.html

情報提供

■ YouTube　手口検証動画シリーズ



- よくある手口に引っかかる様子を動画で分かりやすく説明しています。
- 実存した詐欺サイトにて手口検証したリアリティのある内容です。

https://www.ipa.go.jp/security/anshin/verificationmov.html

情報提供

■ Xアカウント（Twitter）

https://twitter.com/IPA_anshin

■ Facebookアカウント

https://www.facebook.com/ipa.anshin

■ 質疑・応答

独立行政法人**情報処理推進機構**
Information-technology Promotion Agency, Japan