IPA Better Life with IT

インターネット社会の被害者にならないために
～安全安心な使い方とセキュリティ対策～

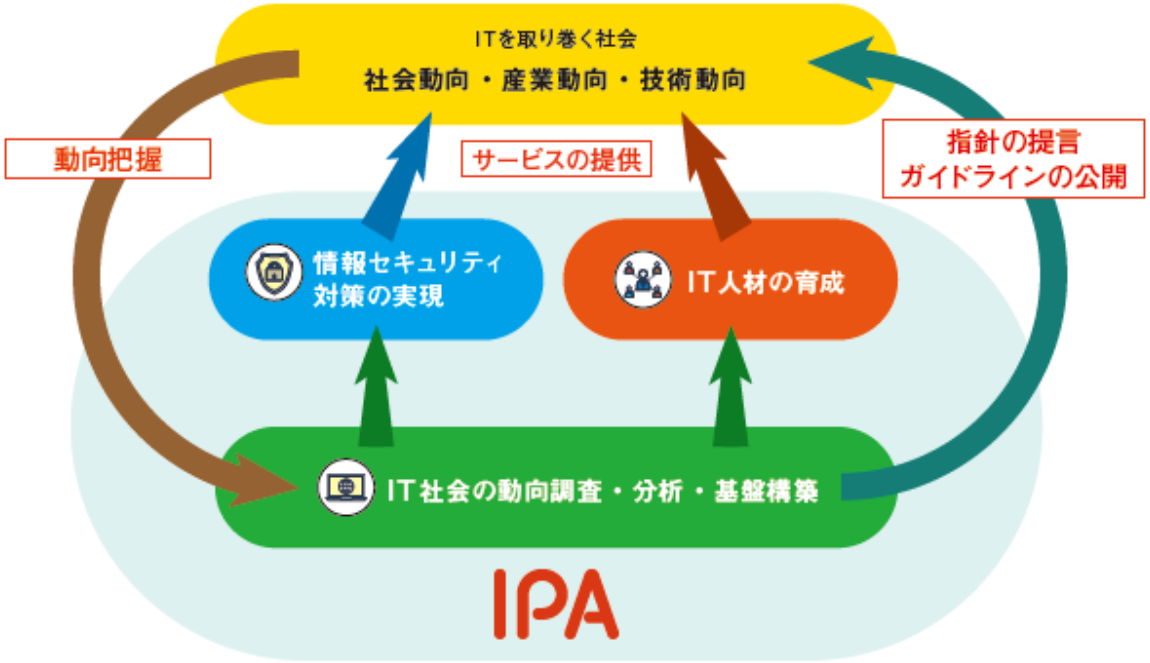
2023年6月10日

独立行政法人情報処理推進機構
セキュリティセンター　企画部
副部長　加賀谷 伸一郎
情報処理安全確保支援士
第021252号

IPAのご紹介

IPA 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



情報セキュリティ10大脅威　2023

「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	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	3	標的型攻撃による機密情報の窃取
クレジットカード情報の不正利用	4	内部不正による情報漏えい
スマホ決済の不正利用	5	テレワーク等の ニューノーマルな働き方を狙った攻撃
不正アプリによる スマートフォン利用者への被害	6	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）
偽警告によるインターネット詐欺	7	ビジネスメール詐欺による金銭被害
インターネット上のサービスからの 個人情報の窃取	8	脆弱性対策情報の公開に伴う悪用増加
インターネット上のサービスへの 不正ログイン	9	不注意による情報漏えい等の被害
ワンクリック請求等の 不当請求による金銭被害	10	犯罪のビジネス化 （アンダーグラウンドサービス）

みなさんの悩み・・・（予想）

全ての脅威を知っておくのは難しい、分からない、時間が無い・・・

最低限、何をすればいいかだけ教えてくれれば・・・

インターネットの

安全・安心ハンドブック

インターネットを安全・安心に利用するための

サイバーセキュリティ対策 9 か条

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

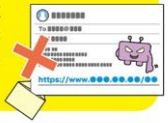
サービスへのログインを安全に行うために、認証用アプリや生体認証を使った多要素認証を利用しましょう。

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。

NISCポータルサイト 案内窓口ページ

https://security-portal.nisc.go.jp/support/

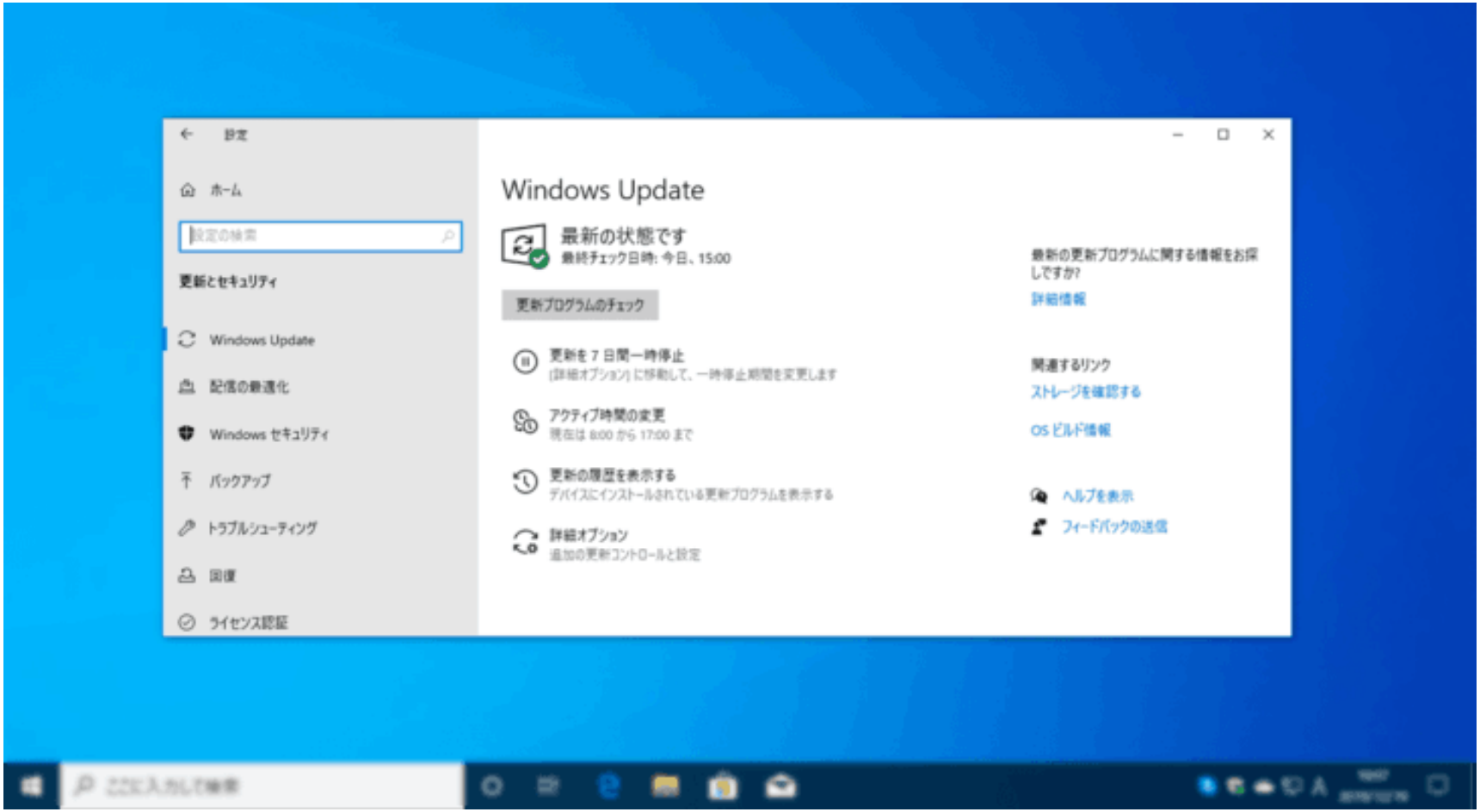
NISC 内閣サイバーセキュリティセンター National center of Incident readiness and Strategy for Cybersecurity

IPA 独立行政法人 情報処理推進機構

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。

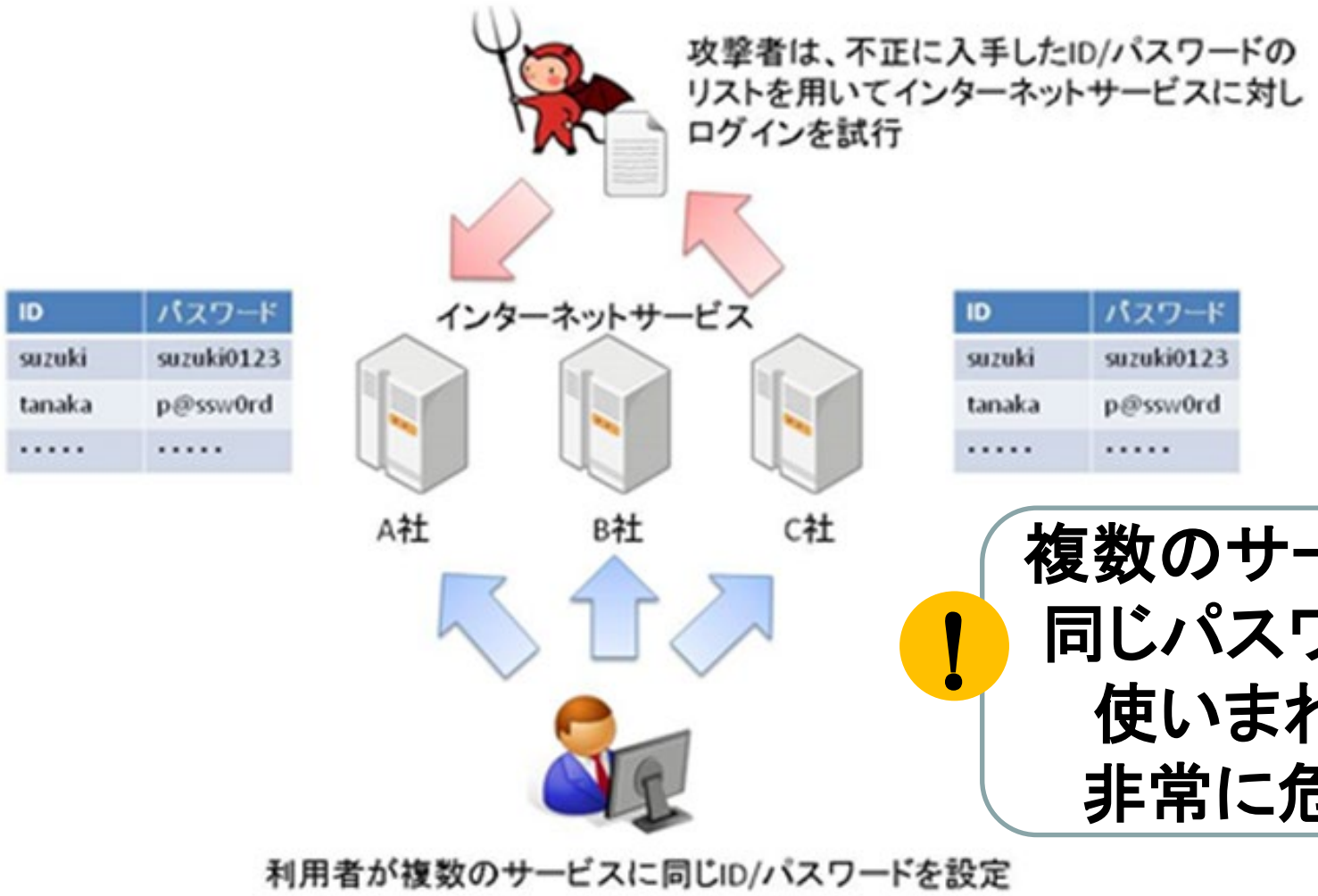
OSをアップデートしましょう！



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。

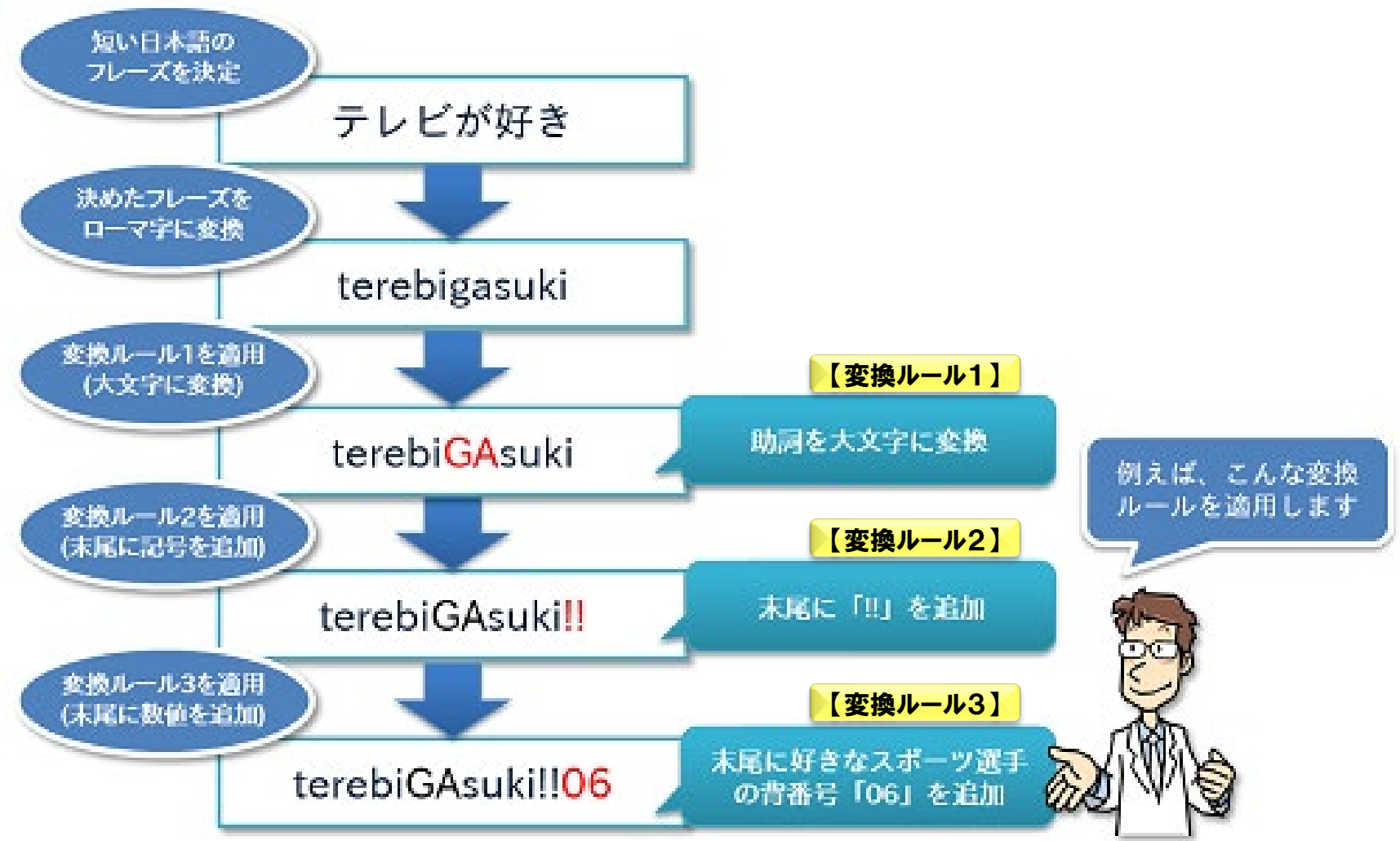
パスワードリスト攻撃の概要



複数のサービスで
同じパスワードを
使いまわすと
非常に危険！

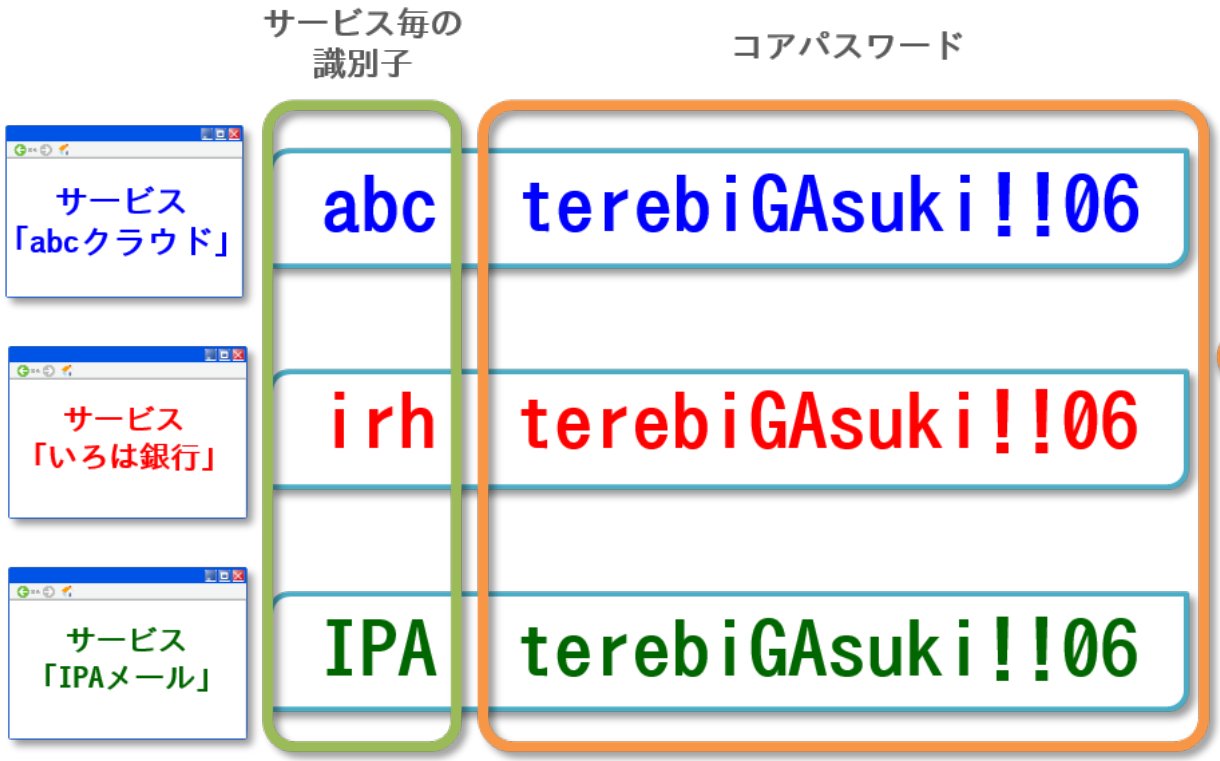
使い回しを回避するパスワードの作成･管理例

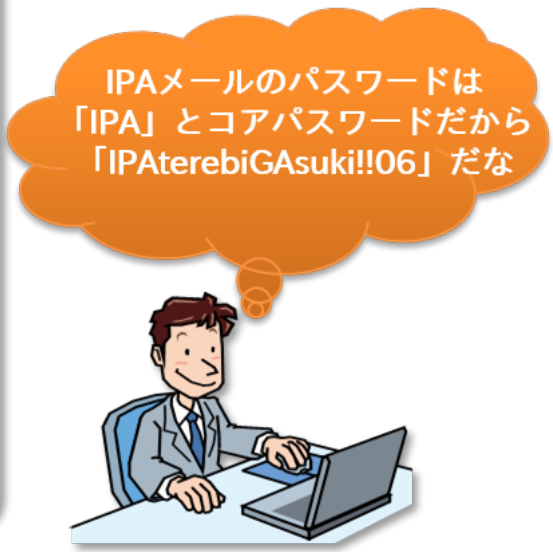
～①コアパスワードの作成～



使い回しを回避するパスワードの作成･管理例

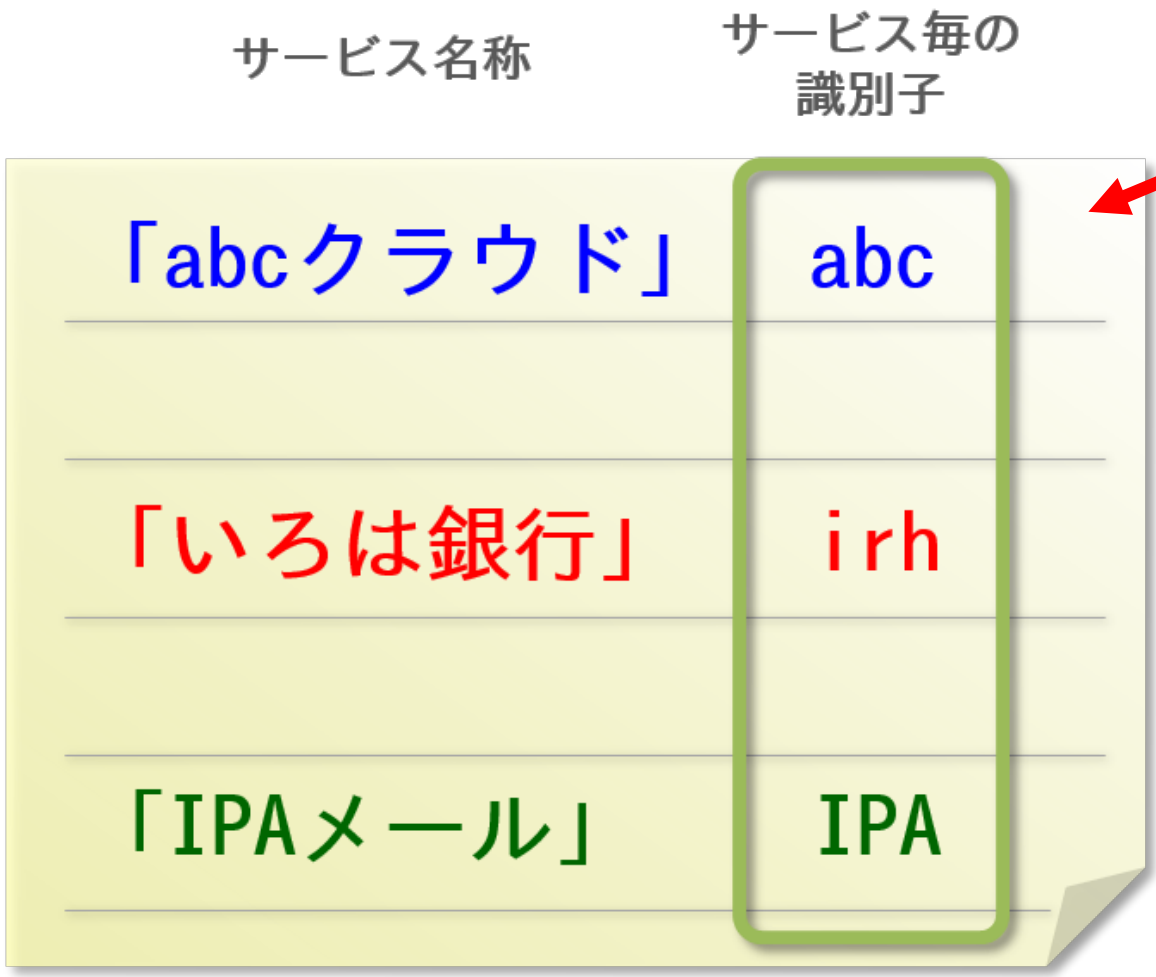
～②サービス毎に異なるパスワードの作成～





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

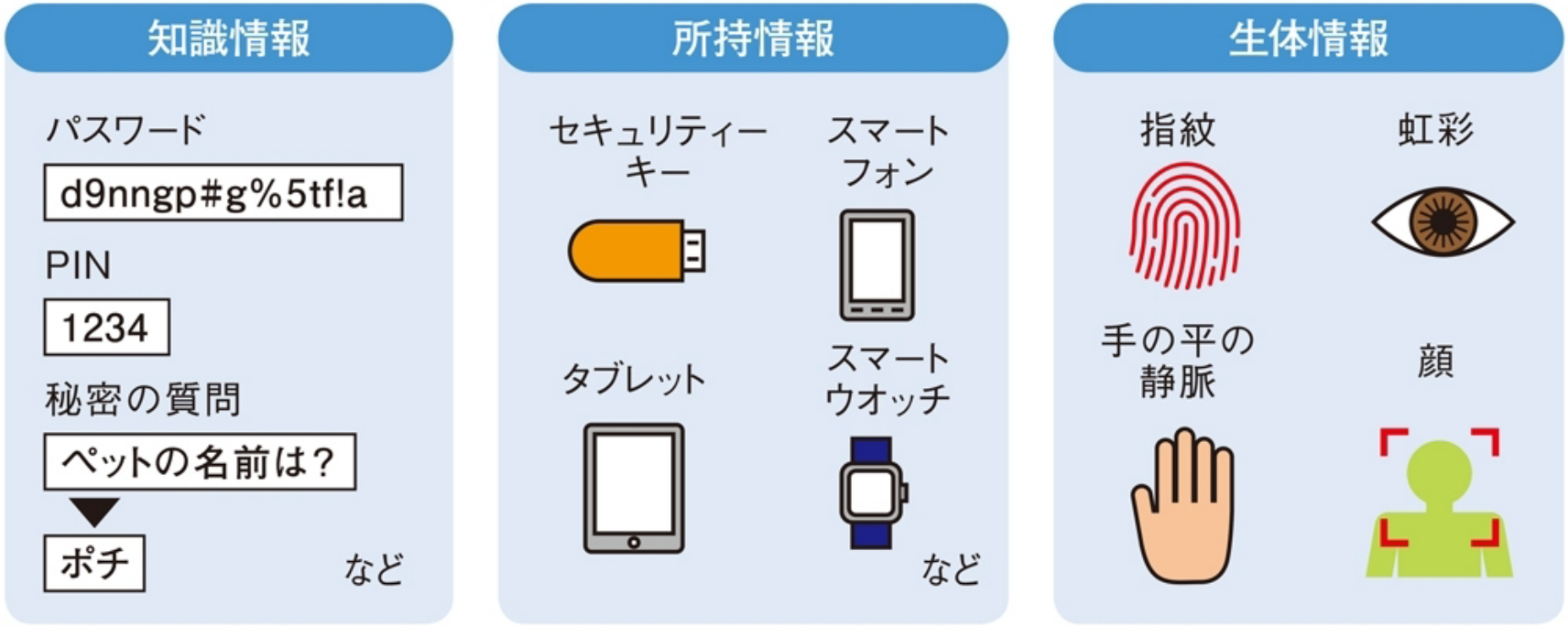
※コアパスワードは、別途、紙などで管理

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。

多要素認証とは？

認証の３要素「知識情報」「所持情報」「生体情報」のうち、<u>２つ以上</u>を使って認証すること



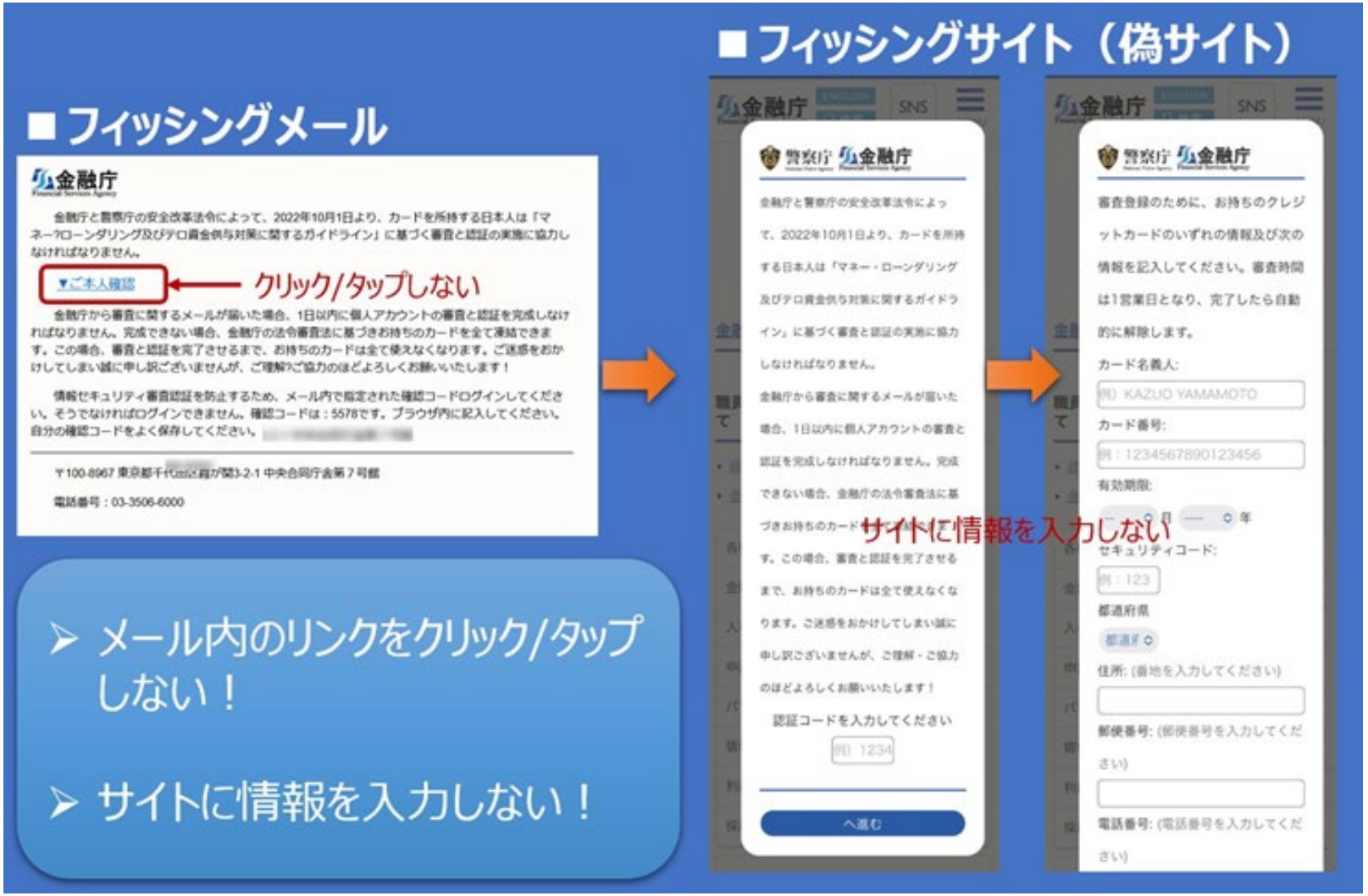
出典：日経NETWORK

PIN：Personal Identification Number

4 偽メールや偽サイトに騙されないように用心しよう

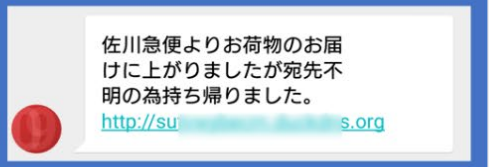
フィッシング詐欺メールは年々手口が巧妙になっています。心当たりがあるものでもメールやメッセージのURLには安易にアクセスしないようにしましょう。

金融庁を騙ったフィッシングメール



宅配便業者を騙ったSMS

Android 最近の事例

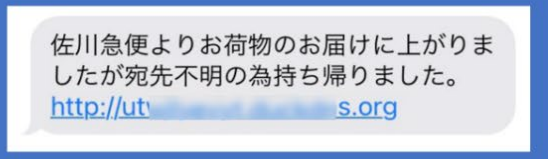


SMSのURLをタップしない！

アプリの保存をOKしない！

OKではなくキャンセルをタップする

iPhone 最近の事例



SMSのURLをタップしない！

IDやパスワードを入力しない！

SMS→本人確認書類を狙う手口

（2021年5月）

通信事業者をかたる偽SMS

（2022年4月）

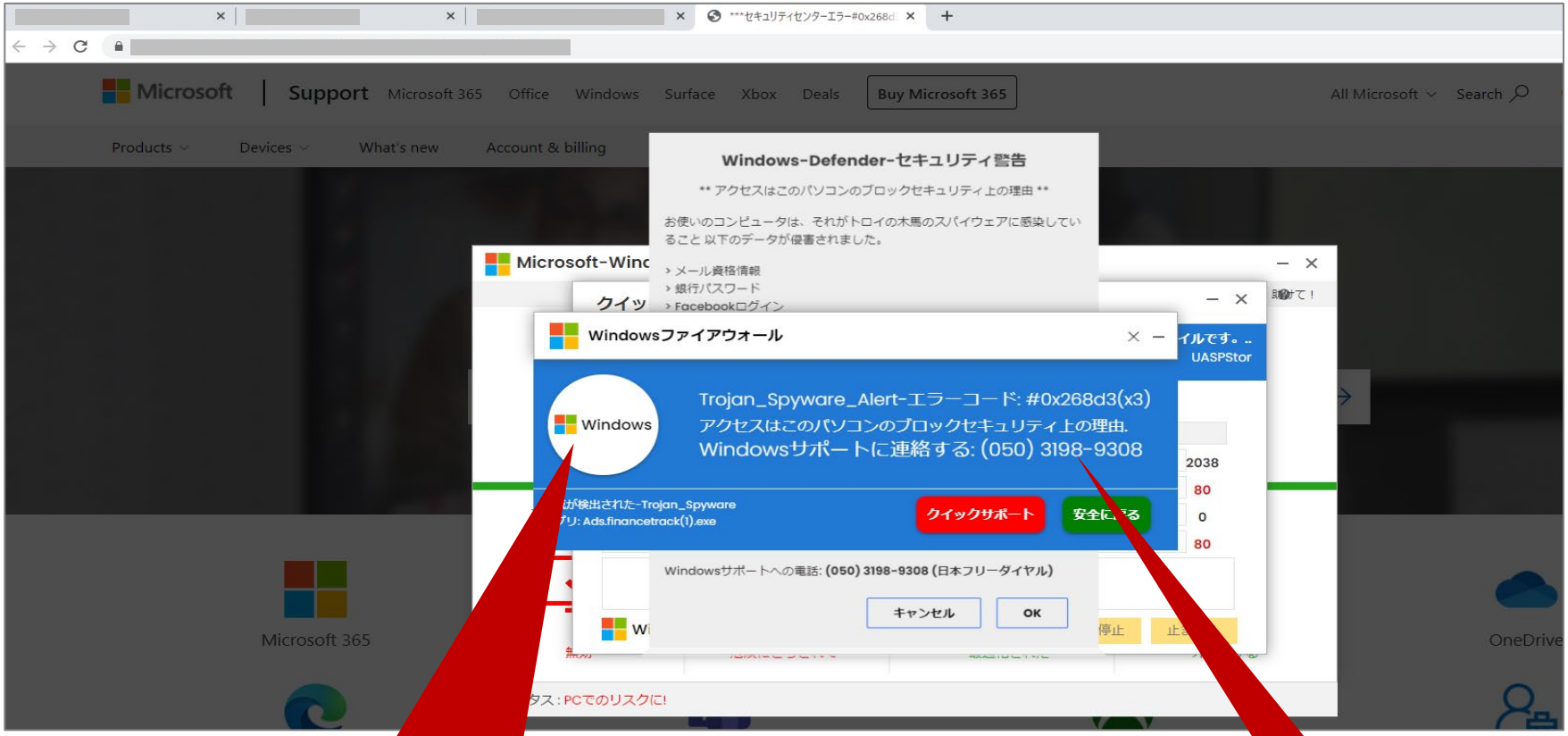
国税庁をかたる偽SMSやメール

警察庁をかたる偽SMSなど

（2022年10月）

偽警告：パソコンの場合

ウェブ閲覧中に突然出現する警告例（2020年）



ホンモノのマイクロソフトっぽい

電話番号

2015年から見られる手口

遠隔操作を悪用した「サポート詐欺」

遠隔操作を安易に許可してはダメ！

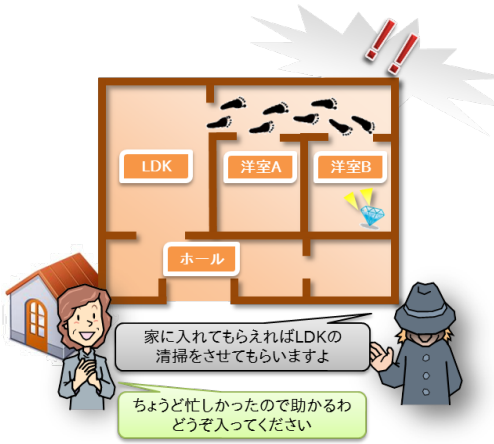
サービス利用者
操作される側

サービス提供者
操作する側

①遠隔操作ソフトのダウンロード
およびインストールの指示

②遠隔操作ソフトのインストールと
接続情報(パスワード等)の通知

③通知された接続情報を入力して
利用者のパソコンを操作して作業



被害者

悪意ある第三者

①「セキュリティソフト」と偽って
遠隔操作ソフトをインストール
するように指示

②遠隔操作ソフトと知らずにソフト
をインストールして接続に必要な
パスワード等の情報を連絡

③遠隔操作ソフトと接続情報を悪用
して被害者のパソコンを不正操作
(個人情報の窃取、なりすまし等)

偽警告→アプリインストールへ誘導

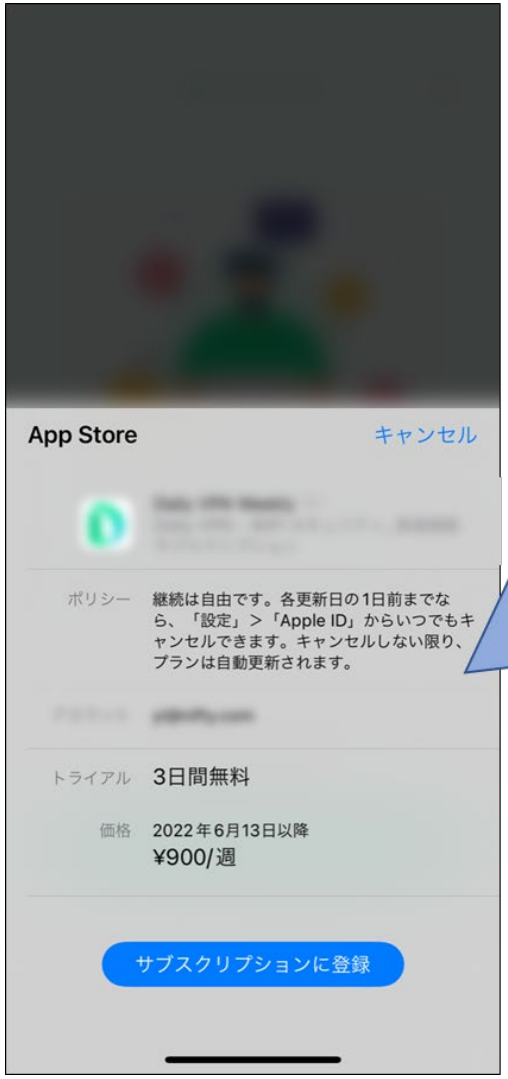
偽のセキュリティ警告からアプリのインストールに誘導される画面事例

自動継続課金である旨の確認メッセージの例（Android）（2022年10月）

「有料であること」が示されている。

今後の請求予定
開始日: 今日
3 日間無料トライアル
開始日: 2022/06/09
￥24,200 / 年
Play で定期購入中
• Google Play の [定期購入] でいつでも解約できます
• 2022/06/09までに解約された場合は、請求は発生しません
• 試用期間が終わる 2 日前にお知らせします

自動継続課金である旨の確認メッセージの例（iPhone）（2022年10月）

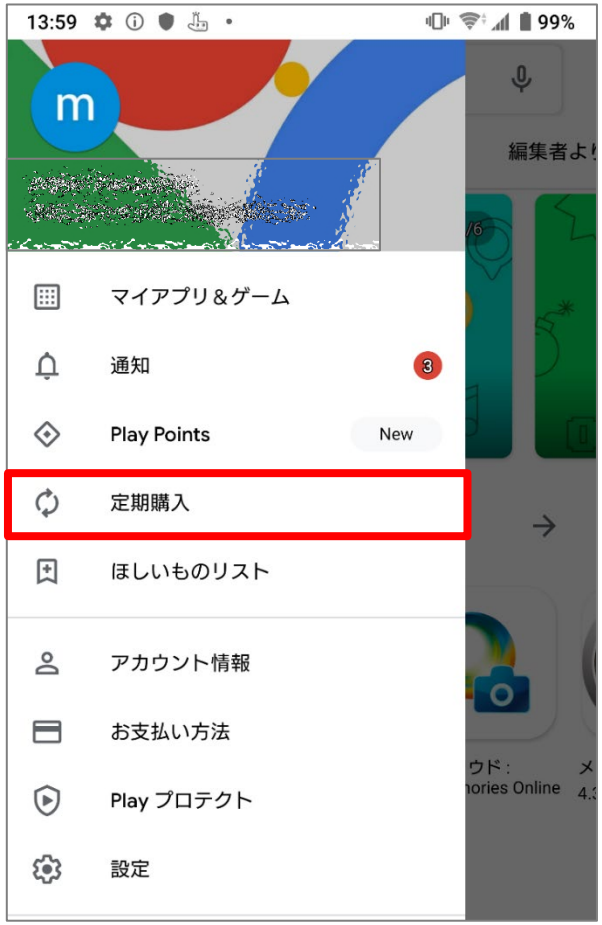


「有料であること」が示されている。

サブスクリプションの確認方法

<Android 10,11の場合>

Google Play ストア ＞ 定期購入



解約方法の詳細はサービス提供者のヘルプページ参照

◆ Android端末で、定期購入を解約する

「Google Play での定期購入の解約、一時停止、変更」

https://support.google.com/googleplay/answer/7018481

サブスクリプションの確認方法

<iPhone、iOS14の場合>

設定 ＞ 名前＞ サブスクリプション

解約方法の詳細はサービス提供者のヘルプページ参照

◆ iPhoneで、サブスクリプションを解約する
「Appleのサブスクリプション解約する方法」
https://support.apple.com/ja-jp/HT202039

ブラウザの通知機能から不審サイトへ誘導する手口

ステップ1

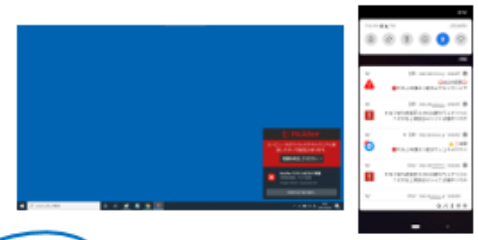
ウェブサイト上でブラウザの通知を許可するように誘導される

対策

安易に通知の許可をしない！

ステップ2

ブラウザ起動中に偽の通知が表示される



対策

表示された通知を鵜呑みにしない！

ステップ3

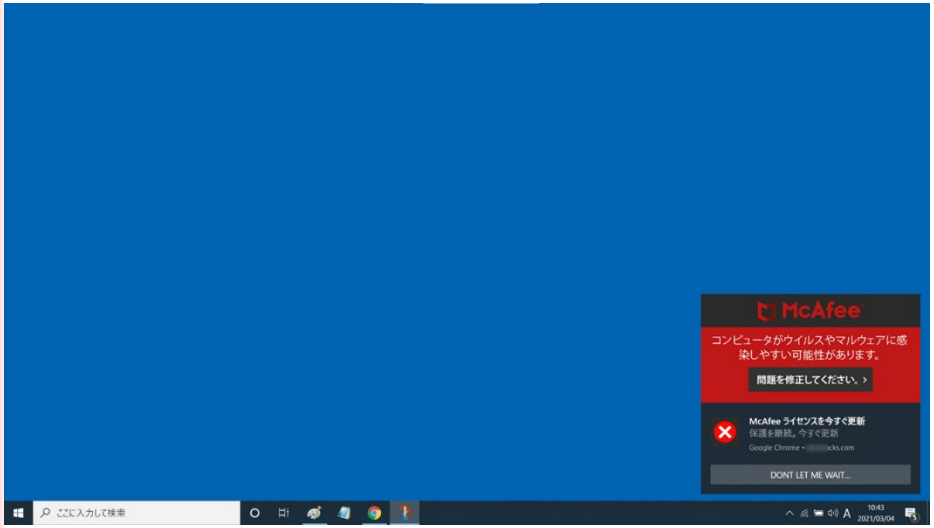
通知表示をクリックすると不審なサイトに誘導される

対策

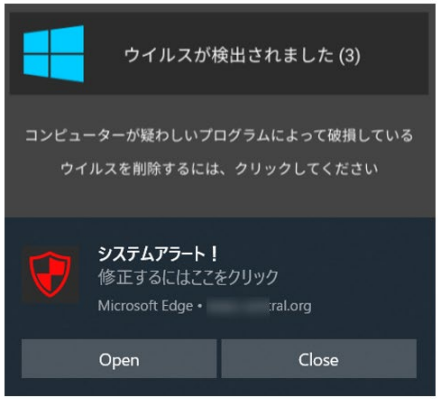
通知から誘導されたサイトで操作をしない！

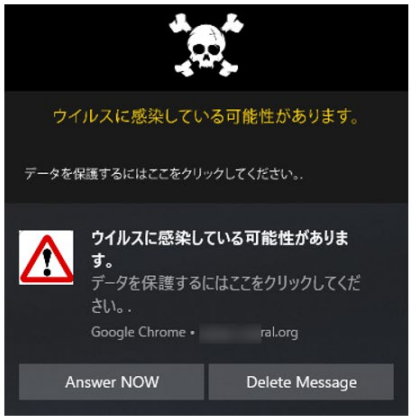
https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210309.html

ブラウザ起動中に偽の通知が表示される（パソコン）



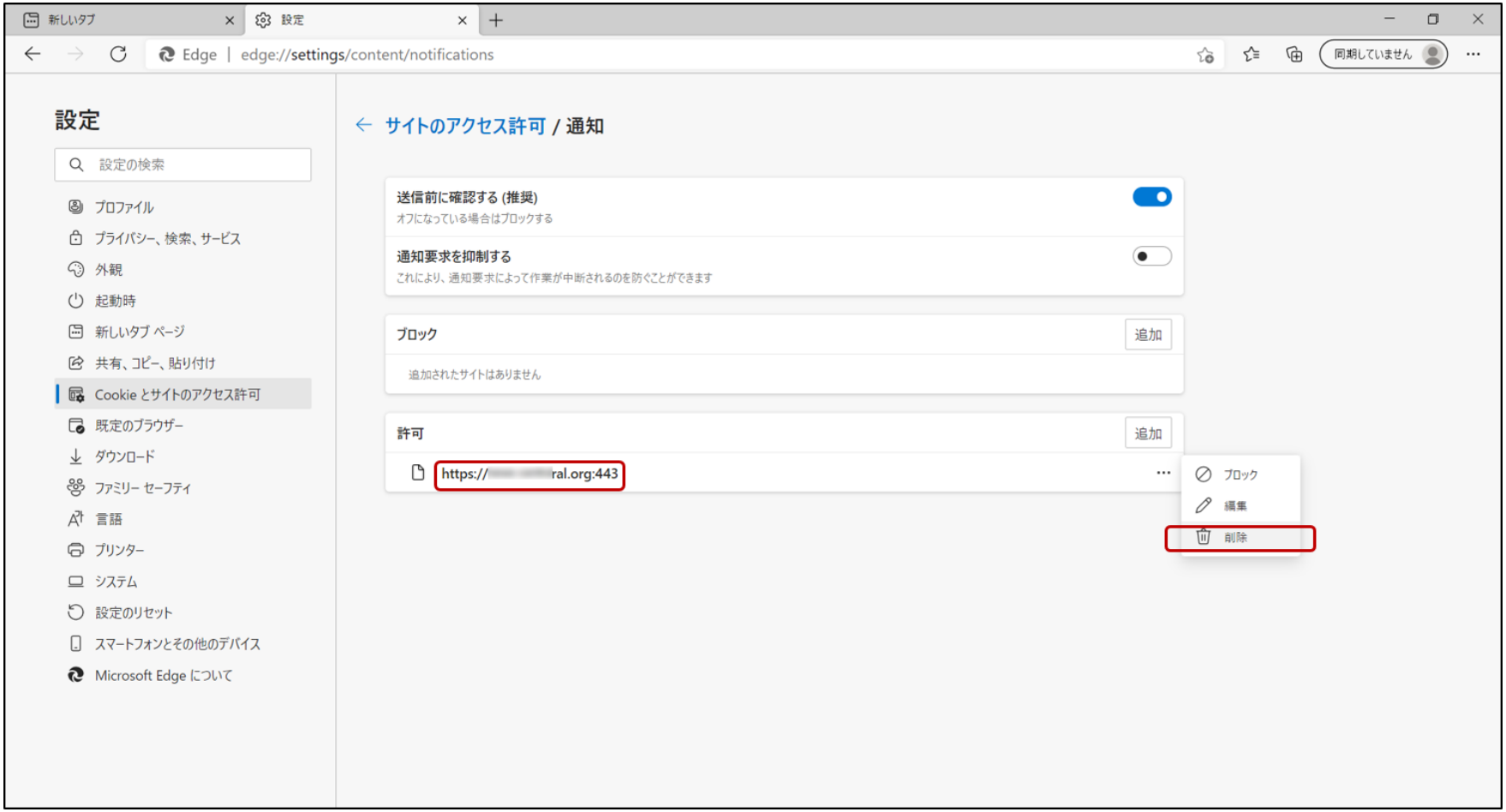
※デスクトップ右下に通知が出現





※様々なバリエーション

対処：ブラウザに登録した通知許可を削除

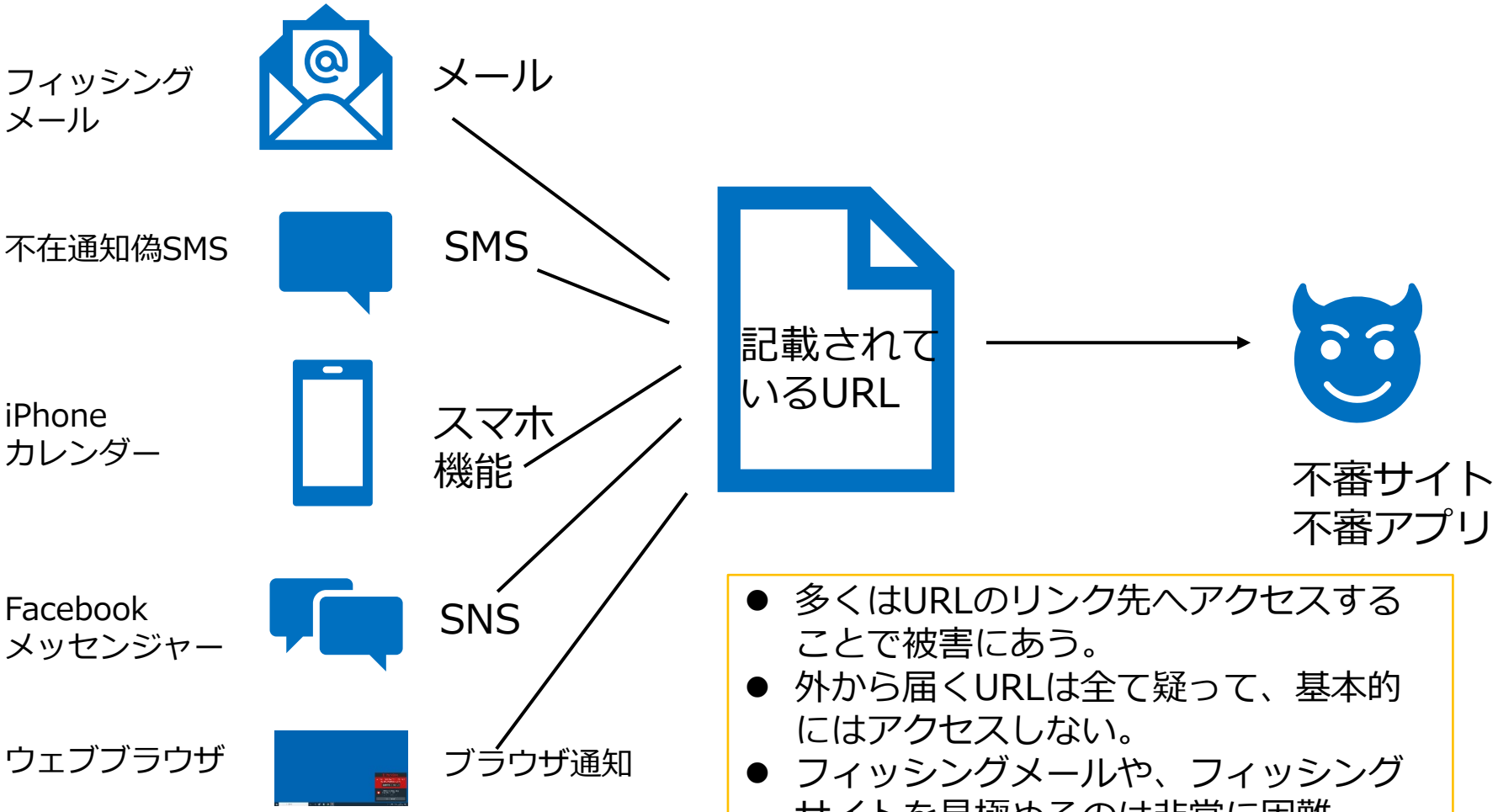


※Microsoft Edgeの通知削除画面
（ブラウザ毎に削除画面は異なります）

サイバー詐欺のまとめ

https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210831.html

基本的には送られてきたURLリンク先に安易にアクセスしないこと



- 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。

サイバー詐欺から身を守るために

3つの基本対策

■ URLを安易にタップ／クリックしない

- お気に入り登録している正規サイトのURLは問題ないが、知らない人からのメールやSMS、SNSのメッセージなどのURLは「偽サイトへの誘導かもしれない」と疑ってかかるくらいが安全。
- 少しでもおかしいと感じたらアクセスしないこと。これだけでも被害に遭うリスクは減るはず。

■ アプリのインストールは慎重に

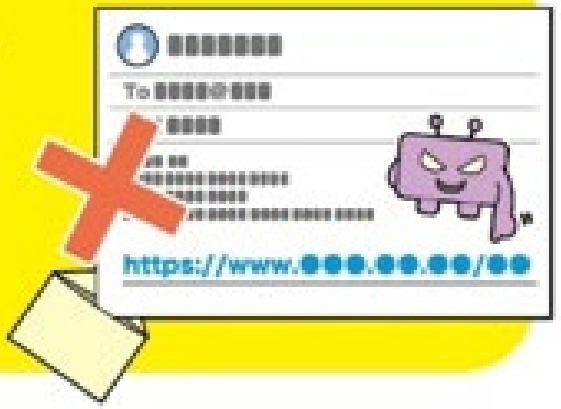
- スマホのアプリをインストールする前に、アプリの説明文やレビュー内容を確認する。
- アプリをインストールした後も、そのアプリがスマホのどの機能やデータにアクセスできるようにするかを許可する「アクセス権限」に注意する。
- アプリを使い始めると「アクセス権限」の許可について確認が表示されるので、その権限がそのアプリに本当に必要かを考えて少しでも不安を感じたら、いったんは「許可しない」を選ぶのが賢明。

■ パスワードや認証コードなどを安易に入力しない

- 最近のインターネットサービスはサービス同士が連携したり、クラウドにデータが同期したり、またさまざまな決済サービスと連携したりといった機能が備わっている。
- サービスの範囲が広い分、IDやパスワードが第三者に知られて悪用されると、想定外の被害が発生しかねない。そのため、アカウント情報は絶対に第三者に知られないようにすること。
- 電話番号やパスワード、認証コード、クレジットカード番号など、重要な情報は安易に入力しない。

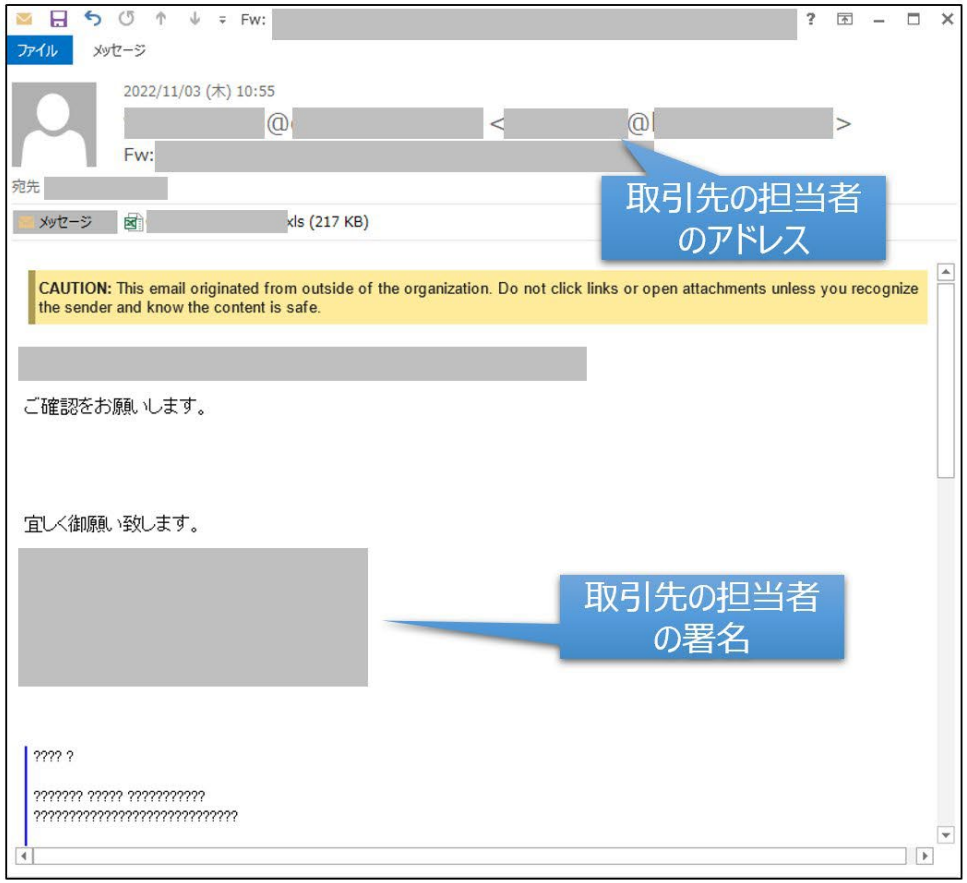
5 メールの添付ファイルや本文中のリンクに注意しよう

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。



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！

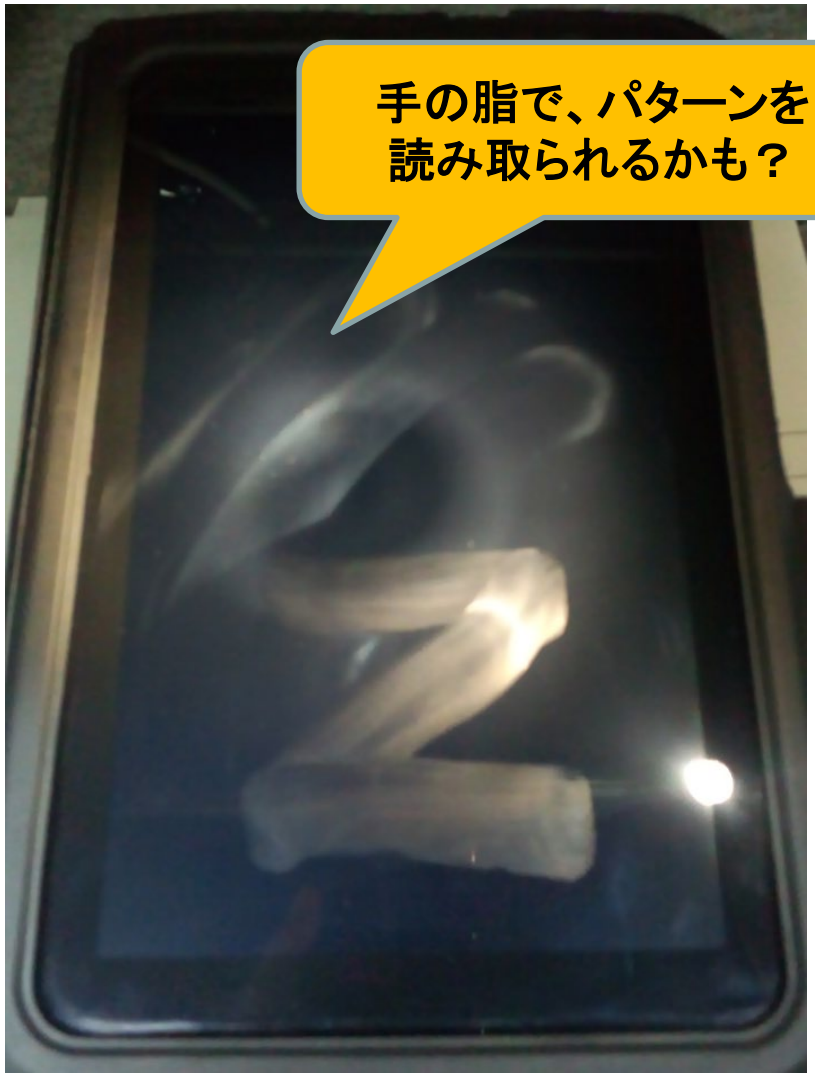
・安易に添付ファイルを開かない
・安易にURLをクリックしない

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。

スマホ：画面ロックの落とし穴　その1

Android



スマホ：画面ロックの落とし穴　その2

iPhone

4ケタ

手の脂で、タッチした位置を読み取られるかも？

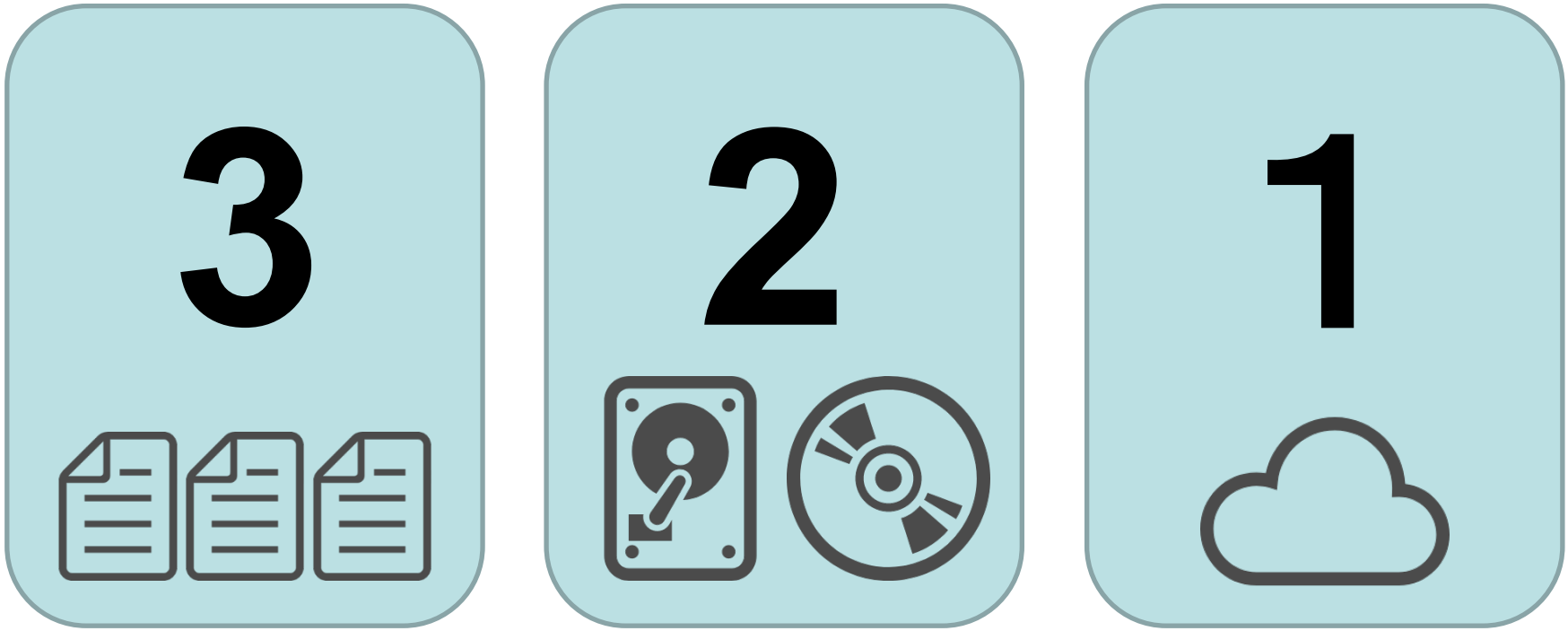
4ケタ4数字だと、24通りしかない

再起動直後は生体認証が無効！

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。

3-2-1　バックアップルール

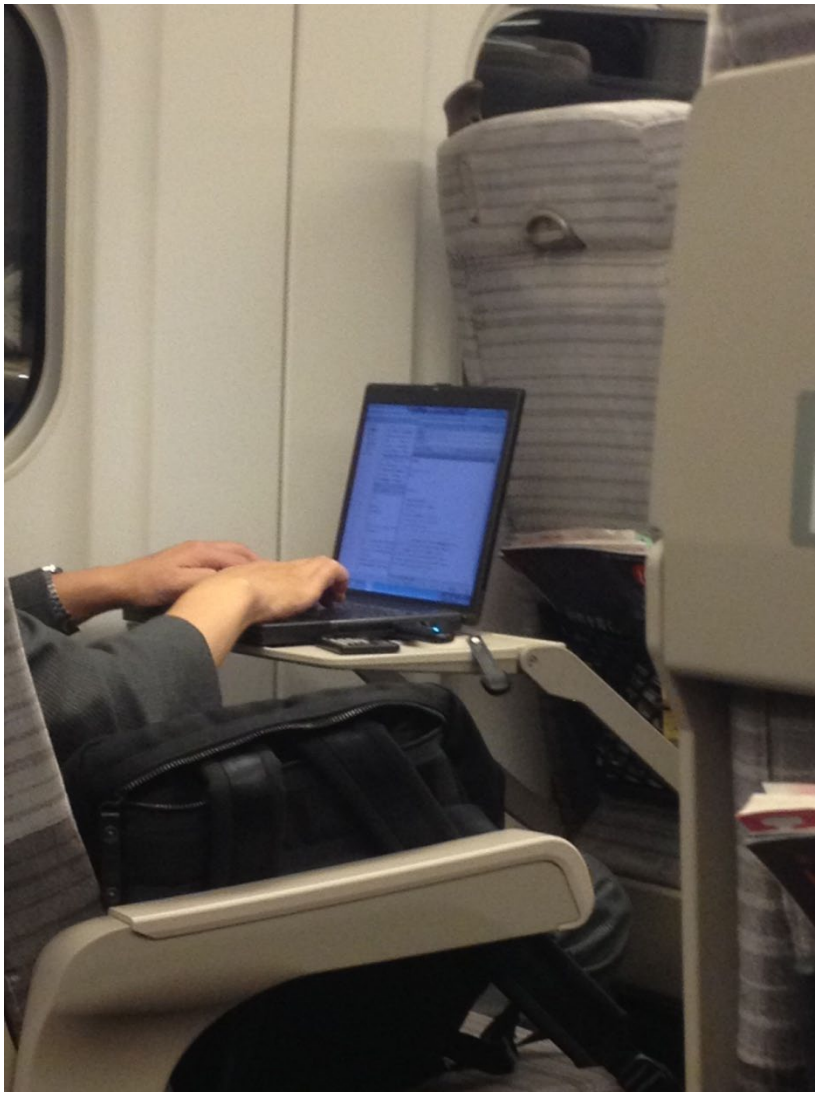


3つのコピー　**2種の媒体**　**1つは別の場所**

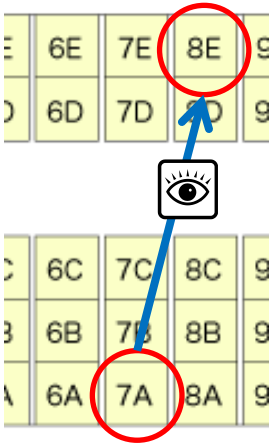
8 外出先では紛失・盗難・覗き見に注意しよう

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。

新幹線で後ろから覗かれるの図1



パソコンやタブレットは左右、後ろから丸見えです！



新幹線で後ろから覗かれるの図2

新幹線で後ろから覗かれるの図3

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。

情報セキュリティ安心相談窓口

IPA

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

突然**ウイルスに感染している**と表示されたけど本当？

アダルトサイトの請求画面が消えない…

ファイルが暗号化されてしまって開けない…

情報セキュリティ安心相談窓口

メール、電話で相談対応を行います

寄せられた情報をもとに被害拡大防止のための**情報発信**を行います

- 注意喚起
- 安心相談窓口だより
- 統計情報
- FAQ

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

IPA 安心相談窓口だより

安心相談窓口だより 2023年度

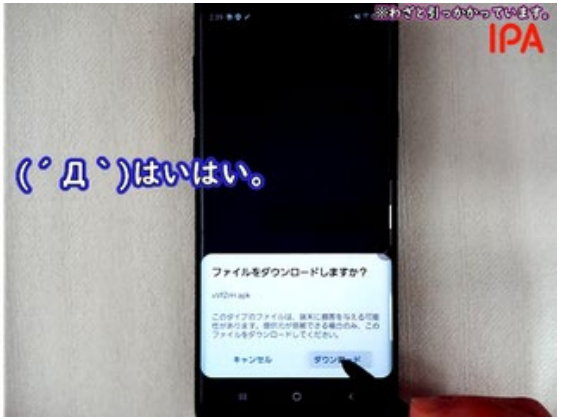
- 遠隔操作ソフト（アプリ）を悪用される手口に気をつけて！

安心相談窓口だより 2022年度

- ワンクリック請求の手口に引き続き注意
- 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！
- 国税庁をかたる偽ショートメッセージサービス（SMS）や偽メールに注意
- 偽セキュリティ警告（サポート詐欺）の月間相談件数が過去最高に

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

IPA　手口検証動画シリーズ



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

【動画】華麗なる情報セキュリティ対策

#1「修正プログラムの適用」
#2「セキュリティソフトの導入および定義ファイルの最新化」
#3「パスワードの適切な設定と管理」
#4「不審なメールに注意」
#5「USBメモリ等の取り扱いの注意」
#6「社内ネットワークへの機器接続ルールの遵守」
#7「ソフトウェアをインストールする際の注意」
#8「パソコン等の画面ロック機能の設定」

IPA相談窓口の公式Twitter

アカウント名：
@IPA_anshin

IPA相談窓口の公式Facebook

事前にいただいた
ご質問にお答えする
コーナー

質問：
SNSの安全な使用方法を知りたいです。

回答：
以下の点に気を付けましょう。
- ネットに書き込んだものは全世界に公開されるという認識を持つ
- 対面で言えないようなことは書き込まない
- ネガティブ、否定的な感情は書かないことが炎上を避けるコツ

質問:
Googleから、何かの会費が月に数回取られています。なぜだか分かりません。

回答:
料金請求元に確認するしかありません。

質問：
スマートフォンもウィルス対策ソフトは必要ですか。

回答：
パソコンに比べ、スマホはウイルスに感染しにくいです。ウイルス対策アプリは必須ではありませんが、OSのアップデートを怠らず、正規マーケットのアプリのみインストールするようにしてください。

質問:
外出先でフリーWi-Fiを使用する上での注意事項を知りたいです。

回答:
フリー Wi-Fiで通信している内容は、筒抜けになっている可能性があると思いながら使うことを推奨します。

質問：
古い機種を使い続けると危険と聞きましたがなぜですか。

回答：
古すぎる機種は、OSを最新バージョンにアップデートできません。
古いバージョンにはぜい弱性（欠陥）が含まれることが多く、これを悪用されるとウイルスに感染しやすくなったりします。

質問:
フィッシング詐欺や怪しいホームページの見分け方を知りたいです。

回答:
悪者は、見分けがつかないように巧妙にメールやサイトを作りこみます。見分けようとしないことがコツです。
どうしても見分けたいのであれば、「ドメイン名」の仕組みなど技術的な学習が必須です。

質問:
レンタルサーバーを借りてWeb回覧板はWordPressで作成したので、オススメのプラグインがあるなら決済システムを導入してみたい。

回答:
自前でサイトに決済機能を入れるとなると、個人情報や金融情報など機微情報を扱うことになりますので、サイト運営の基本からセキュリティ対策の応用まで身に着けるとともに、事故が起こった際の責任を取る覚悟が必要となります。
学習にはIPAの「安全なウェブサイトの作り方」が参考となります。

質問:
パソコンで画面を操作していると、Windowsファイアウォールに攻撃されていますなどというコメントが繰り返し右下からでてきます。

回答:
怪しいサイトから手元のブラウザへの通知を許可してしまったために出ている通知画面と思われます。本編中のスライドをご参照ください。

質問：
セキュリティについて、カタカナで表記されますが、内容が分かりにくいので教えてください。

回答：
本編中で紹介した「インターネットの安全・安心ハンドブック」などで学習しましょう。
分からない言葉は、ネット検索で調べてみるのも良いでしょう。

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