

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ましょう

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。



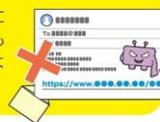
4 偽メールや偽サイトに騙されないように用心しよう

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。



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/>



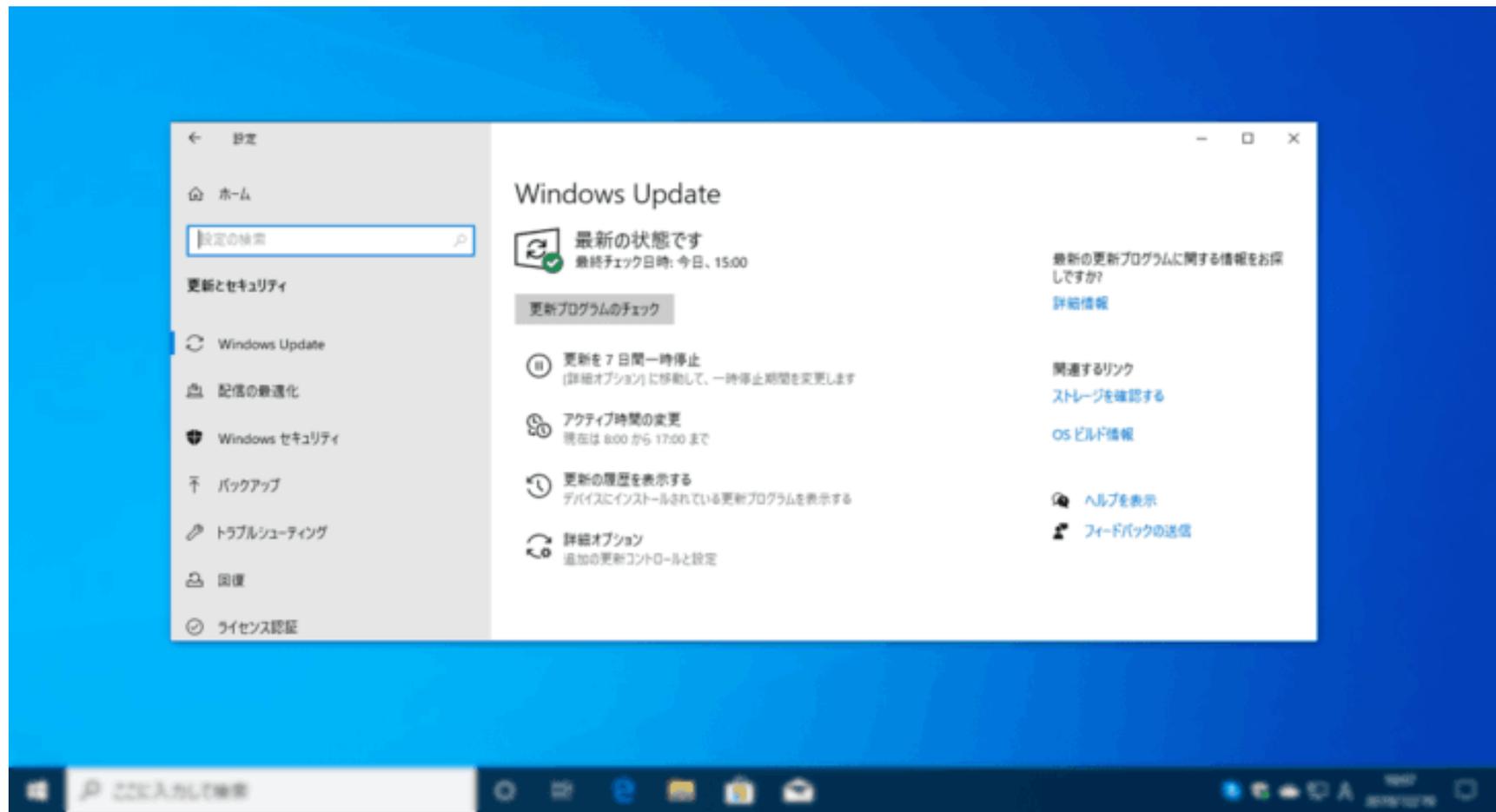
1

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

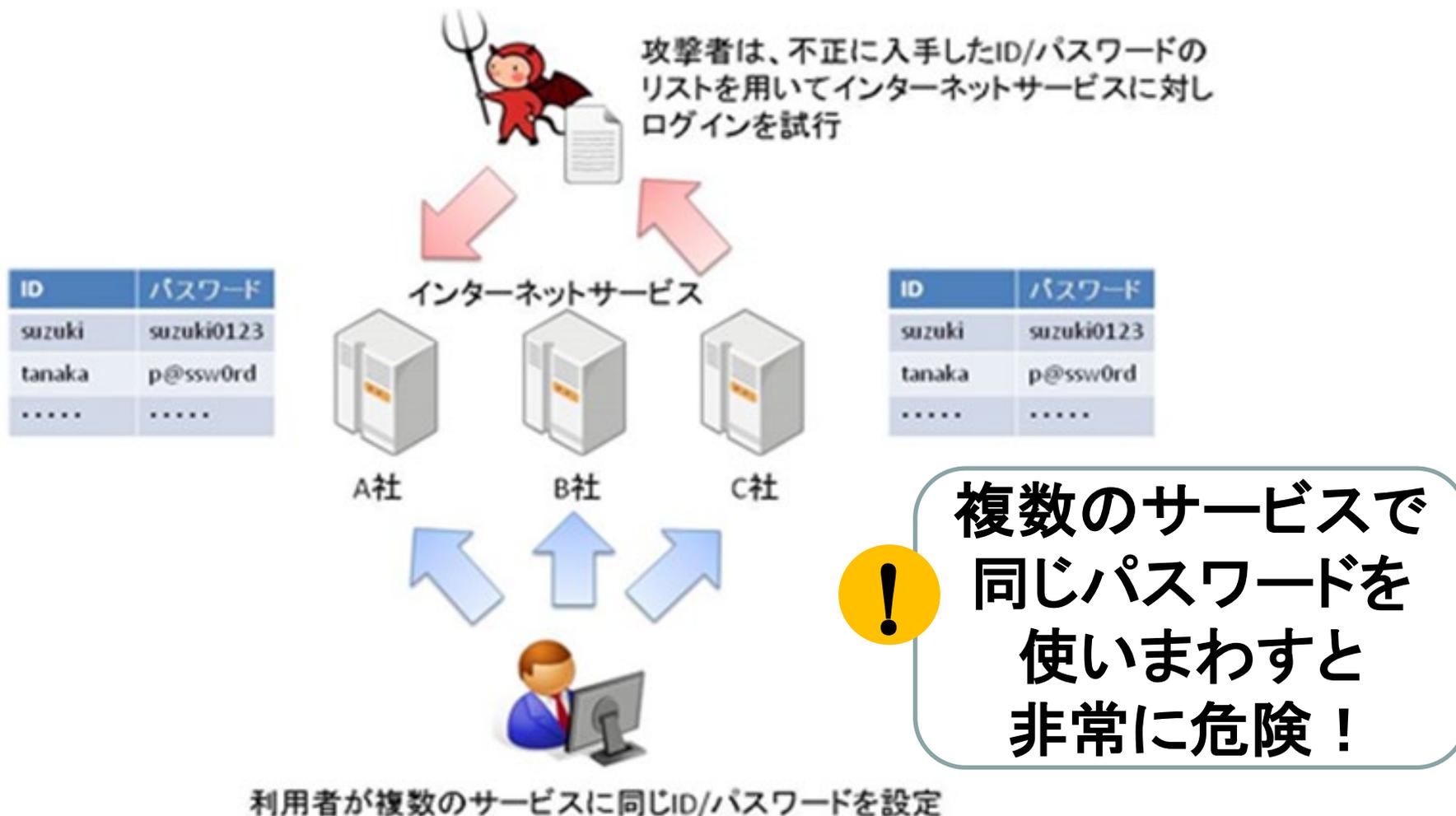
パスワードは長く複雑にして、 他と使い回さないようにしましょう

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。



FC%&D)hmvEy34%
TPkhFmRj-+

パスワードリスト攻撃の概要



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～



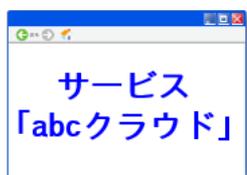
使い回しを回避するパスワードの作成・管理例

～②サービス毎に異なるパスワードの作成～



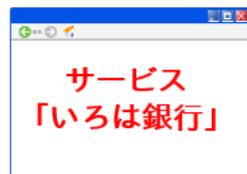
サービス毎の
識別子

コアパスワード



abc

terebiGAsuki!!06



irh

terebiGAsuki!!06



IPA

terebiGAsuki!!06

IPAメールのパスワードは「IPA」とコアパスワードだから「IPAterebiGAsuki!!06」だな



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～



サービス名称

サービス毎の
識別子

「abcクラウド」

abc

「いろは銀行」

irh

「IPAメール」

IPA

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、2つ以上を使って認証すること

知識情報

パスワード

PIN

秘密の質問

▼
 など

出典：日経NETWORK

所持情報

セキュリティーキー

スマートフォン

タブレット

スマートウォッチ
 など

生体情報

指紋

虹彩

手の平の静脈

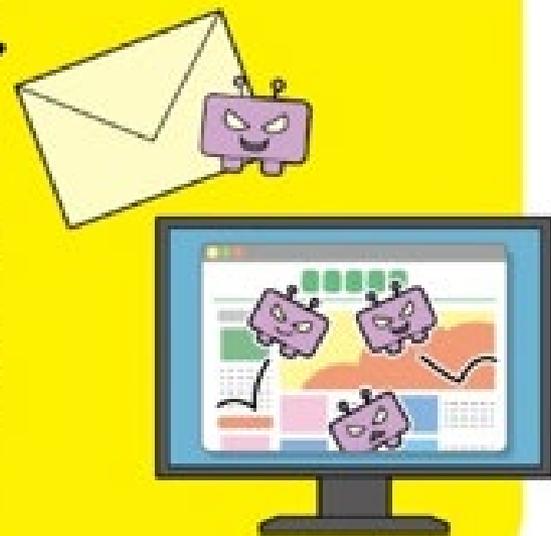
顔

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

■ フィッシングメール

金融庁
Financial Services Agency

金融庁と警察庁の安全改革法令によって、2022年10月1日より、カードを所持する日本人は「マネー・ローンダリング及びテロ資金供与対策に関するガイドライン」に基づく審査と認証の実施に協力しなければなりません。

▼ご本人確認

← クリック/タップしない

金融庁から審査に関するメールが届いた場合、1日以内に個人アカウントの審査と認証を完成しなければなりません。完成できない場合、金融庁の法令審査法に基づきお持ちのカードを全て凍結されます。この場合、審査と認証を完了させるまで、お持ちのカードは全て使えなくなります。ご迷惑をおかけしてしまい誠に申し訳ございませんが、ご理解・ご協力のほどよろしくお願いたします！

情報セキュリティ審査認証を防止するため、メール内で指定された確認コードログインしてください。そうでなければログインできません。確認コードは：5578です。ブラウザ内に記入してください。自分の確認コードをよく保存してください。

〒100-8967 東京都千代田区千代田3-2-1 中央合同庁舎第7号館
電話番号：03-3506-6000

■ フィッシングサイト（偽サイト）

警察庁 金融庁

金融庁と警察庁の安全改革法令によって、2022年10月1日より、カードを所持する日本人は「マネー・ローンダリング及びテロ資金供与対策に関するガイドライン」に基づく審査と認証の実施に協力しなければなりません。

金融庁から審査に関するメールが届いた場合、1日以内に個人アカウントの審査と認証を完成しなければなりません。完成できない場合、金融庁の法令審査法に基づきお持ちのカードを全て使えなくなります。この場合、審査と認証を完了させるまで、お持ちのカードは全て使えなくなります。ご迷惑をおかけしてしまい誠に申し訳ございませんが、ご理解・ご協力のほどよろしくお願いたします！

認証コードを入力してください

例) 1234

へ進む

警察庁 金融庁

審査登録のために、お持ちのクレジットカードのいずれの情報及び次の情報を記入してください。審査時間は1営業日となり、完了したら自動的に解除します。

カード名義人:
例) KAZUO YAMAMOTO

カード番号:
例) 1234567890123456

有効期限:
例) 月 年

セキュリティコード:
例) 123

都道府県:
都道府県

住所:(番地を入力してください)

郵便番号:(郵便番号を入力してください)

電話番号:(電話番号を入力してください)

- メール内のリンクをクリック/タップしない！
- サイトに情報を入力しない！

宅配便業者を騙ったSMS

Android 最近の事例

佐川急便よりお荷物のお届けに上がりましたが宛先不明の為持ち帰りました。
<http://su...s.org>



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

佐川急便よりお荷物のお届けに上がりましたが宛先不明の為持ち帰りました。
<http://ut...s.org>



SMSのURL
をタップし
ない！

IDやパス
ワードを入
力しない！

Appleのすべてのサービス
で使用するアカウントで

SMS→本人確認書類を狙う手口

(2021年5月)

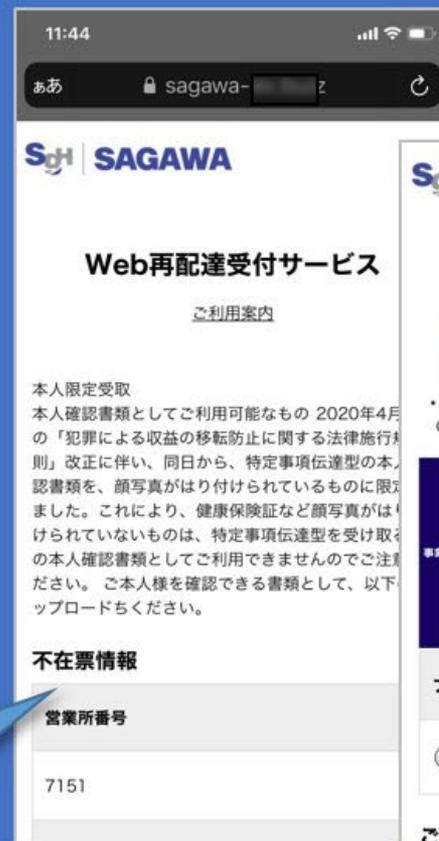
ご本人様不在通知為お荷物を持ち帰りました。ご確認ください。<https://sawaga-...u/>

不在通知の偽SMS

URLをタップしないで！

再配達受付の偽サイト

本人確認書類などの情報を送らないで！



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

国税庁をかたる偽のSMSに注意！！

【国税庁】未払い税金お支払い
のお願い。詳細はこちら：
<https://c.../IN>

SMS内のURL
をタップしない！
サイトに情報を
入力しない！

差押最終通知

納税確認番号:****3697

あなたの所得税（または延滞金（法律により計算した額）について、これまで自主的に納付されるよう催促してきましたが、まだ納付されておりません。もし最終期限までに納付がないときは、税法のきめるところにより、不動産、自動車などの登記簿財産や給料、売掛金などの債権などの差押処分に着手致します。

滞納金合計:40000円

納付期限:2022/8/11

最終期限:2022/8/11（支払期日の延長不可）

お急ぎで対応してください。下記の方法でオンライン納付もご利用いただけます。

本人情報の確認を入力

メールアドレス入力

メールアドレス入力

電話番号をご入力ください

携帯電話番号

お名前（漢字）

（例：山田太郎）

お支払い方法選択

電子マネー（vプリカ発行コード）

クレジットカード

コンビニエンスストア

お申し込み金額 | 発行コード額面合計 | 不一致

40000円	40000円	0円
--------	--------	----

お支払いへ進む

全て偽のサイトです

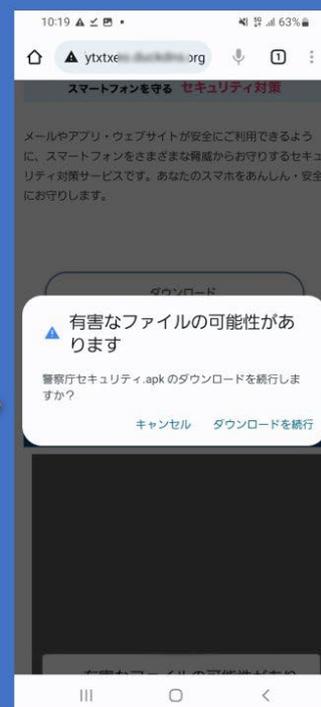
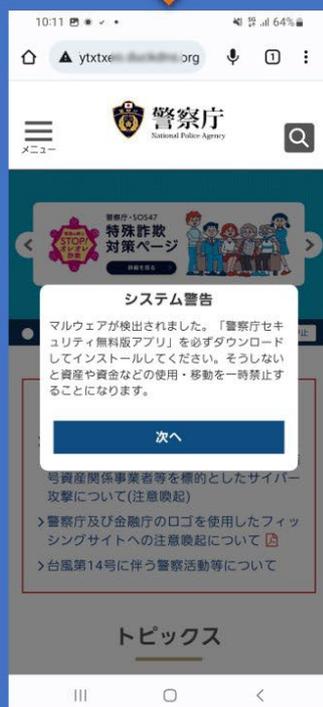
警察庁をかたる偽SMSなど

(2022年10月)

警察庁をかたる偽SMS、偽サイト、偽アプリに注意!!

【警察庁】重要なお知らせ、必ずお読みください。<https://cui.67>

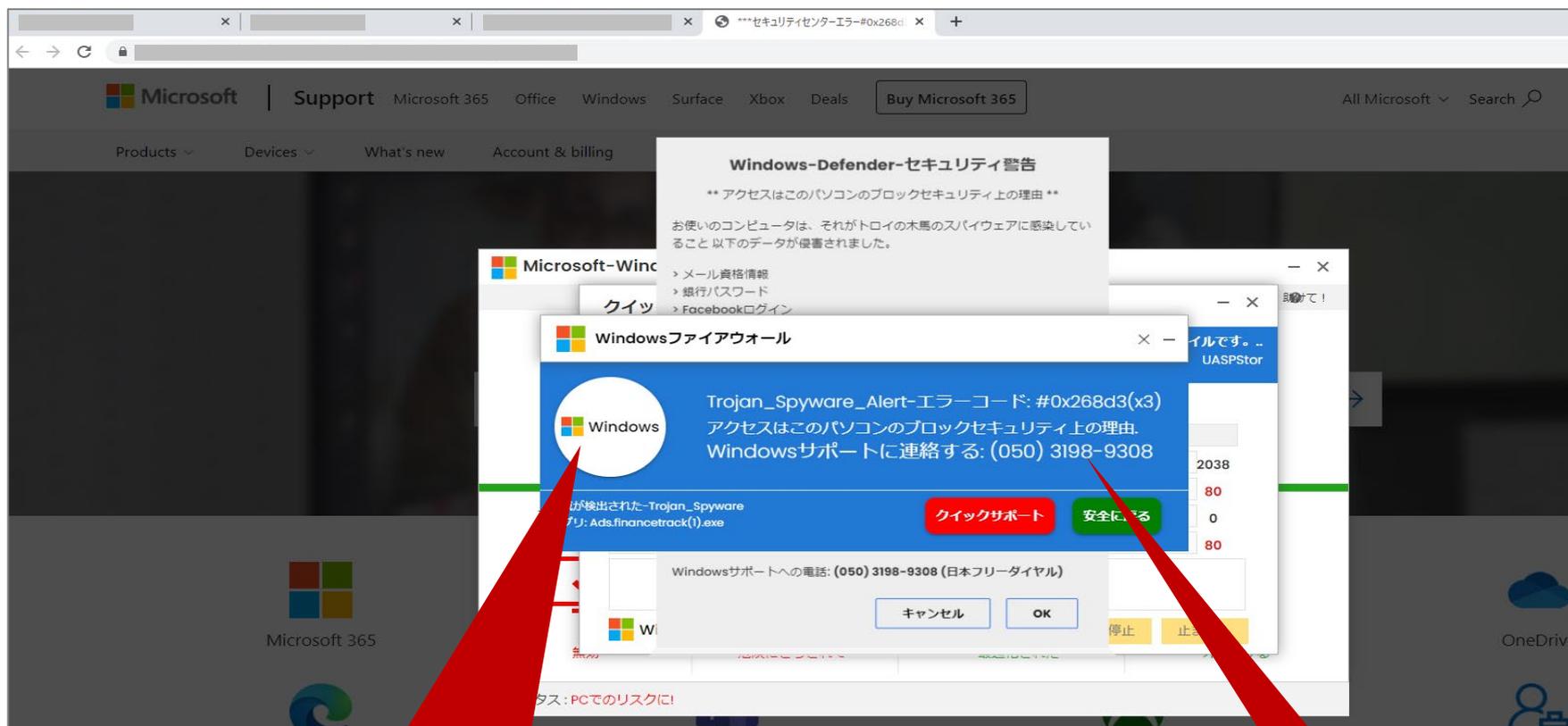
- SMSのURLをタップしない!
- サイトのリンクボタンをタップしない!
- サイトに情報を入力しない!



Android端末
に表示される
偽サイト事例

すべて
偽物

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

2015年から見られる手口

電話番号

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



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

サービス提供者
操作する側



被害者

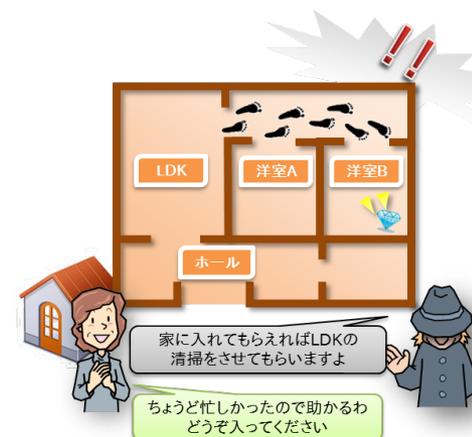


① 「セキュリティソフト」と偽って
遠隔操作ソフトをインストール
するように指示

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)

悪意ある第三者



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

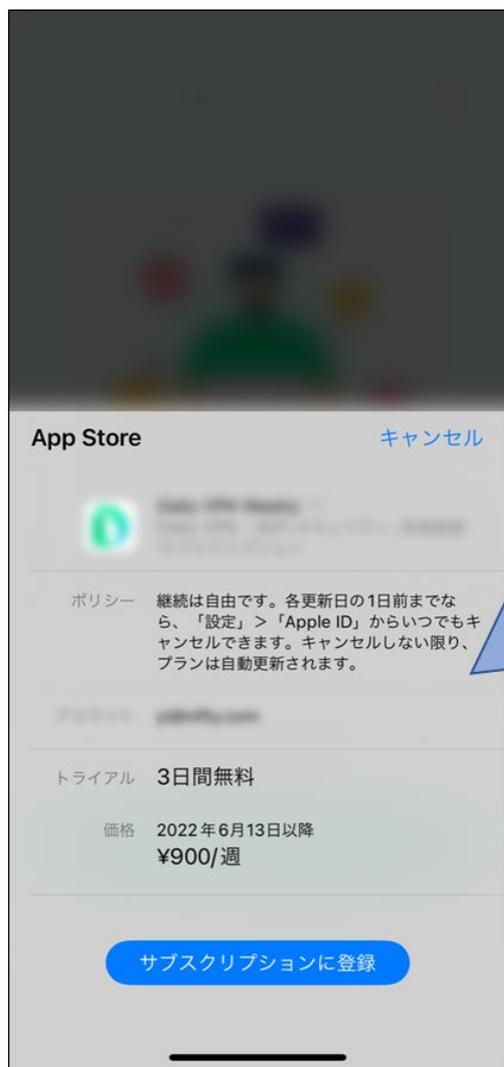
開始日: 今日 3日間無料トライアル

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。

ポリシー 継続は自由です。各更新日の1日前までなら、「設定」>「Apple ID」からいつでもキャンセルできます。キャンセルしない限り、プランは自動更新されます。

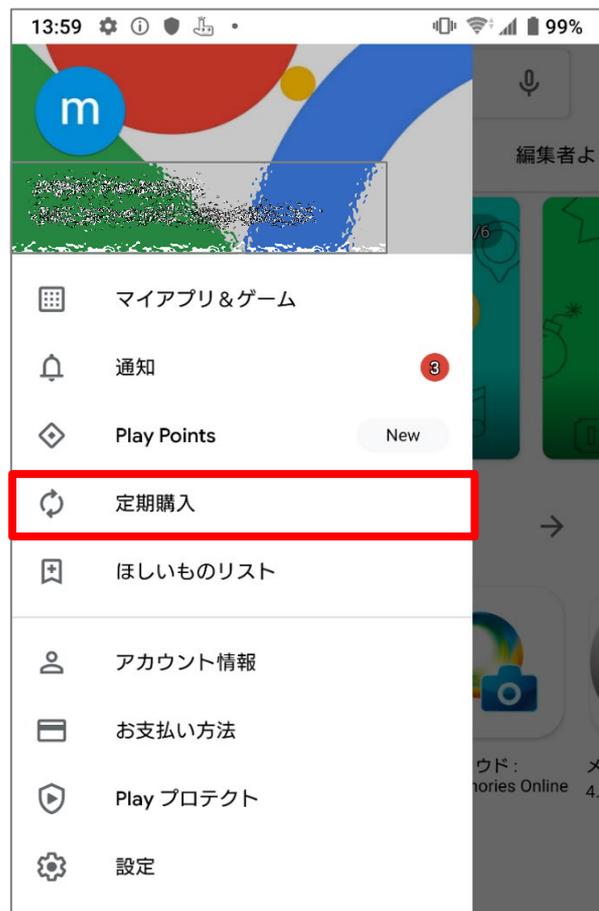
トライアル 3日間無料

価格 2022年6月13日以降
¥900/週

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

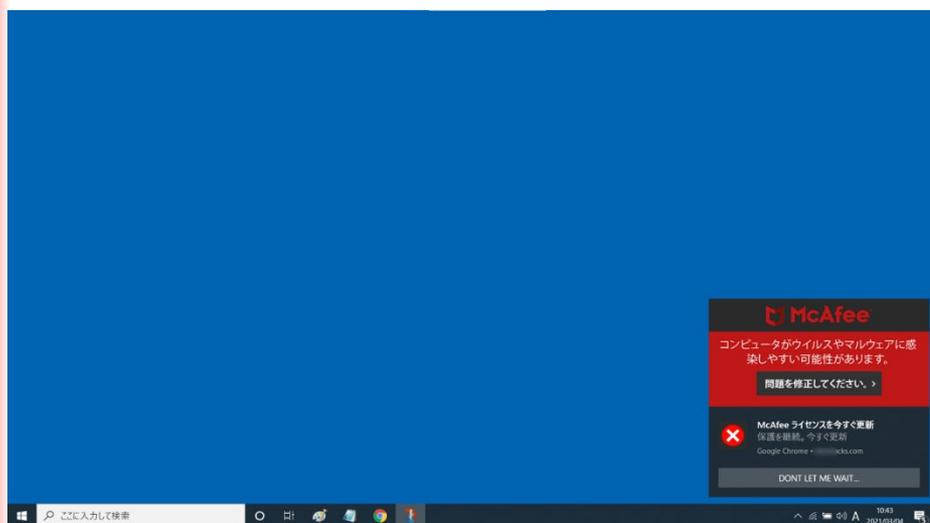


<https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210309.html>

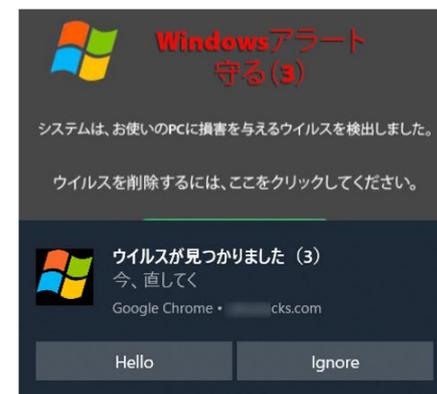
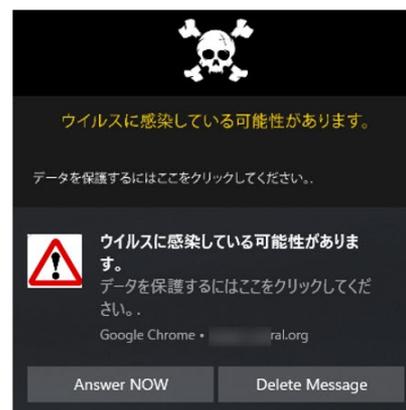
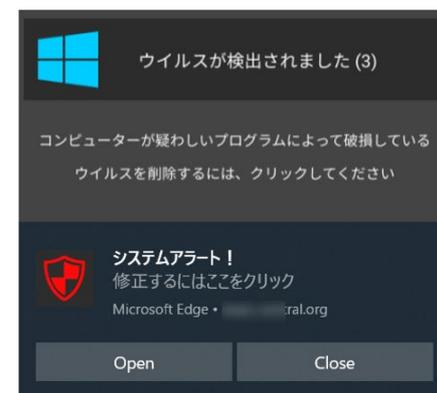


ブラウザ起動中に偽の通知が表示される

(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



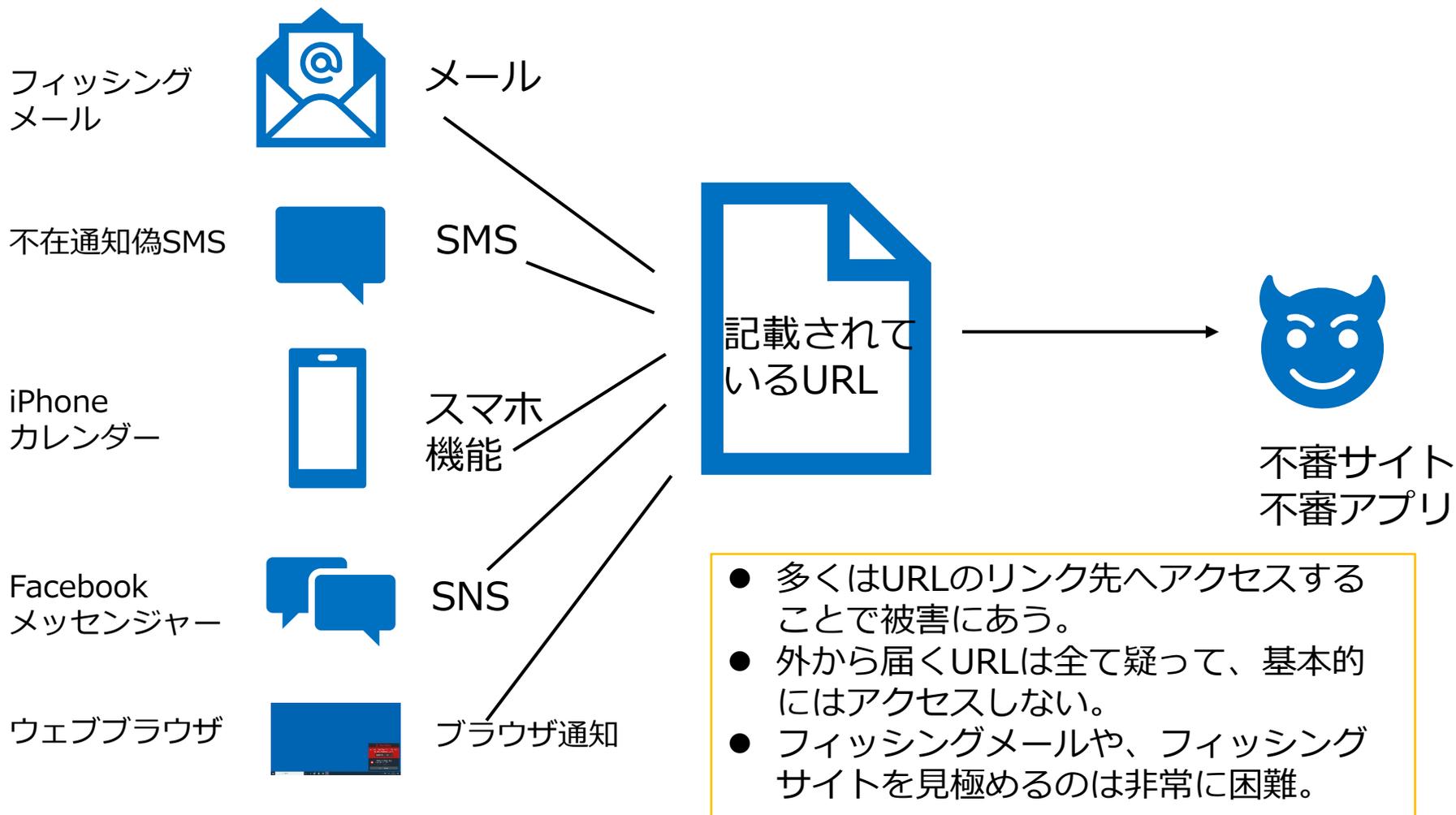
※Microsoft Edgeの通知削除画面
(ブラウザ毎に削除画面は異なります)

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



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。

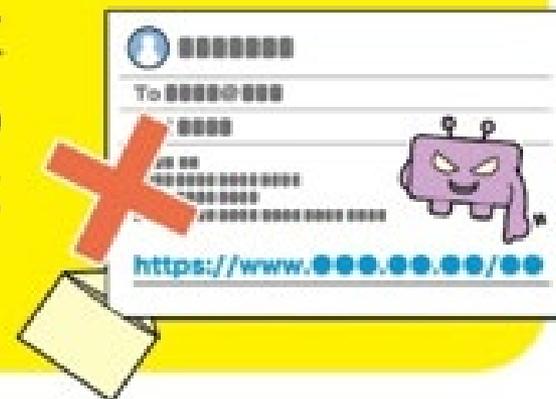
■ パスワードや認証コードなどを安易に入力しない

- 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

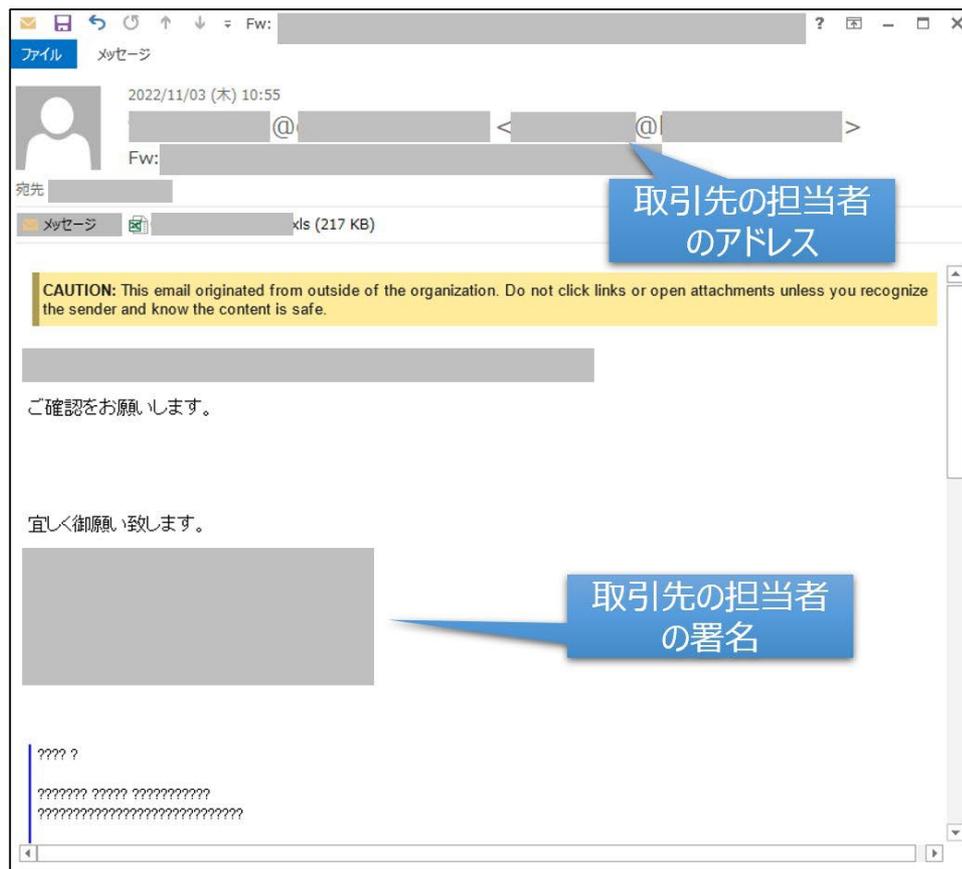
メールの添付ファイルや 本文中のリンクに注意しよう

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。

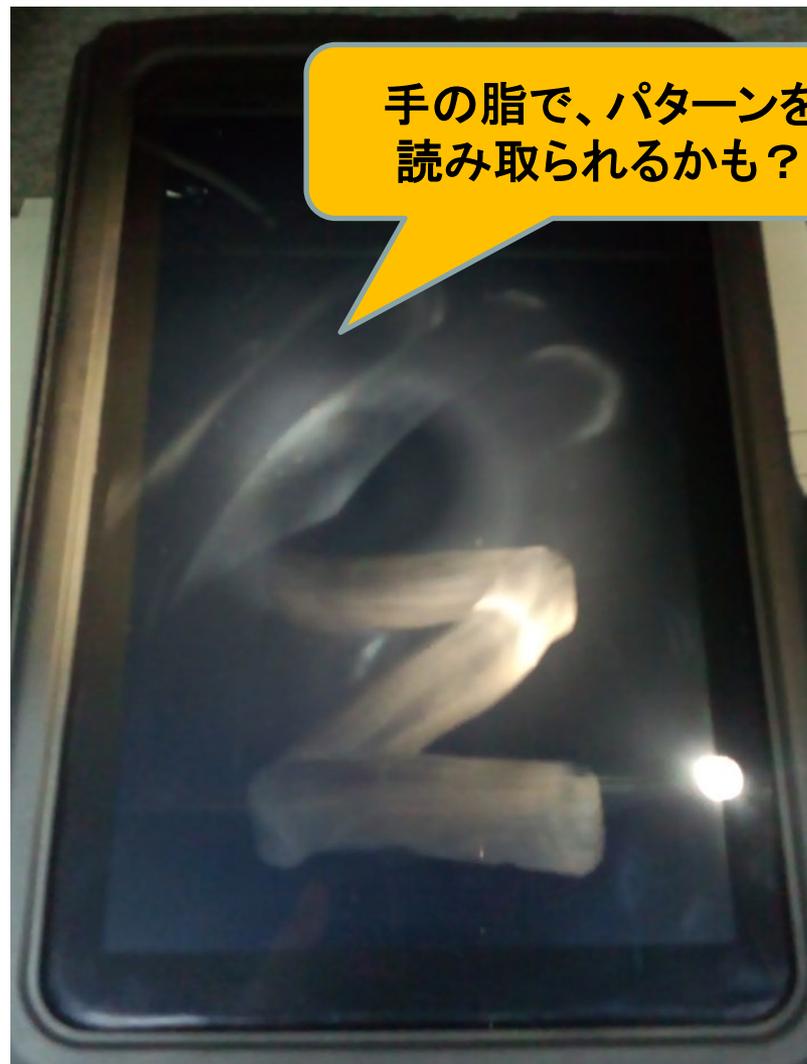


スマホ: 画面ロックの落とし穴 その1

Android



手の脂で、パターンを読み取られるかも？



スマホ:画面ロックの落とし穴 その2

iPhone



4ケタ

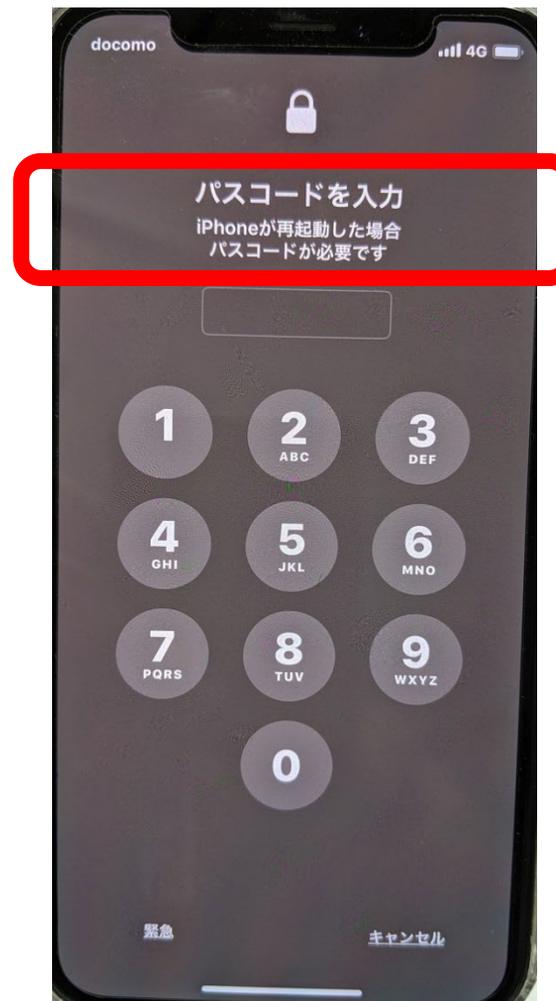


手の脂で、タッチした位置を読み取られるかも？



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。



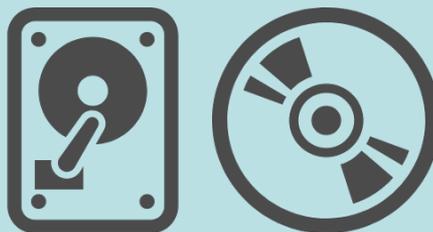
3-2-1 バックアップルール

3



3つのコピー

2



2種の媒体

1



1つは別の場所

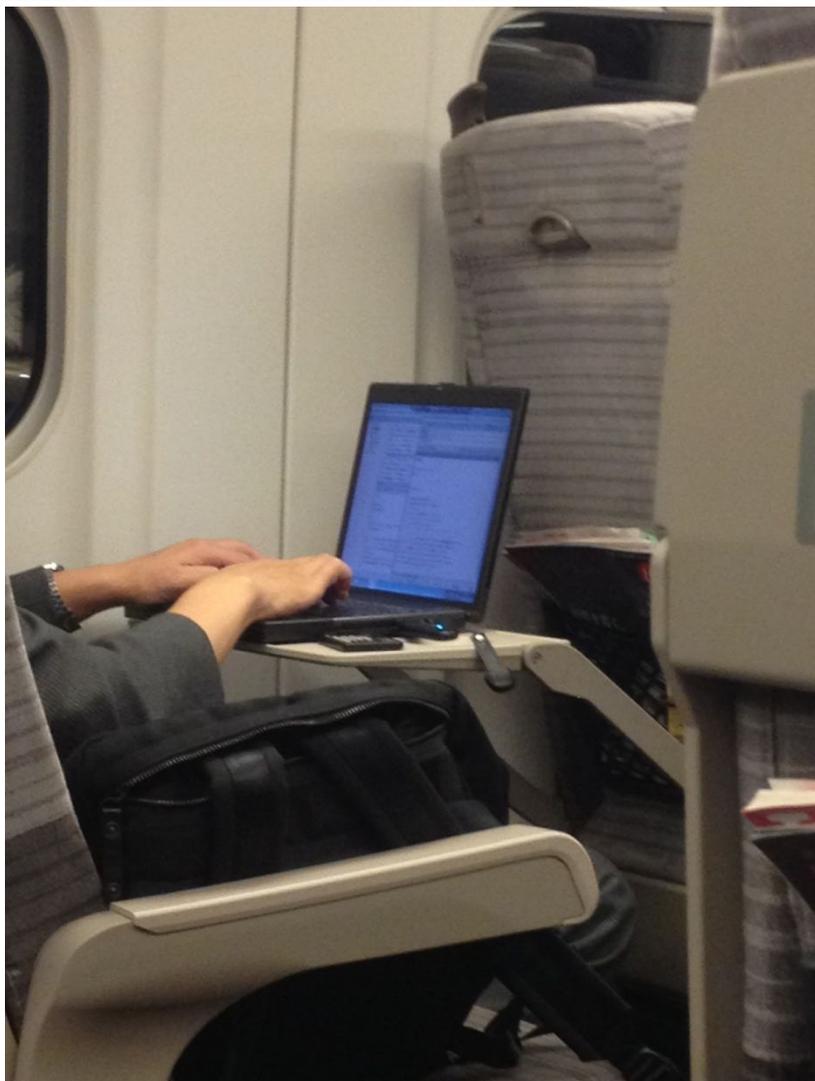
8

外出先では紛失・盗難・ 覗き見に注意しよう

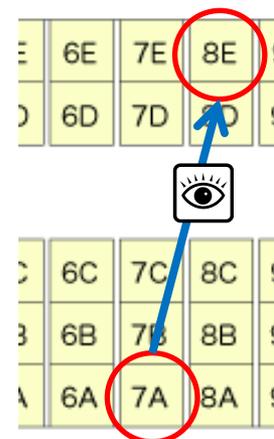
外出先でスマホやパソコンを使う時は、背後からの覗き見に注意しましょう。また、紛失・盗難の危険があるので、公共の場でスマホを放置することは絶対にやめましょう。



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



Zoom!!



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ご相談しましょう。

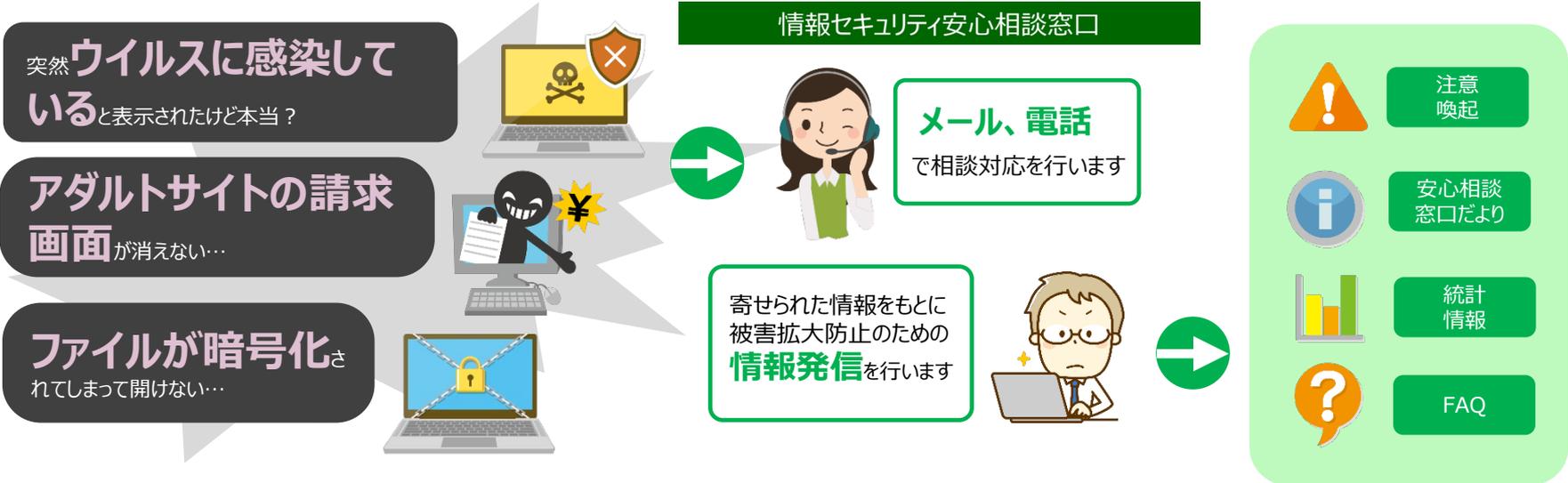




情報セキュリティ安心相談窓口

IPA

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





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





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！

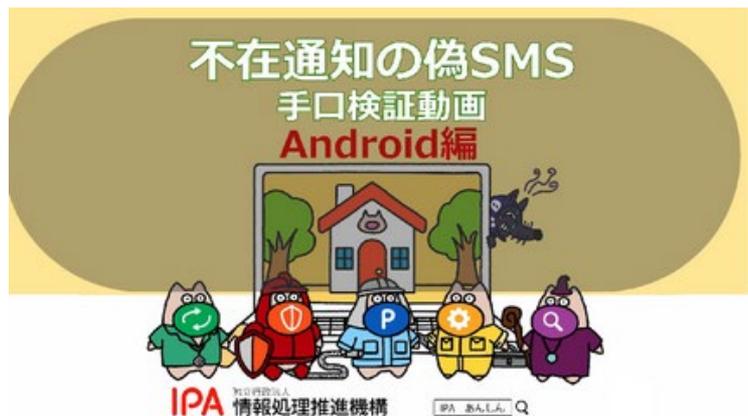
国税庁をかたる偽ショートメッセージサービス（SMS）や偽メールに注意

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



IPA 情報セキュリティ安心相談窓口



～ 情報セキュリティで不安なことや困ったことが発生したら～
電話やメールでアドバイスを提供します

IPA
情報セキュリティ
安心相談窓口

フォロー

IPA (情報セキュリティ安心相談窓口) ✓
@IPA_anshin

IPA情報セキュリティ安心相談窓口の公式アカウントです。
窓口に寄せられる相談をもとに、コンピュータウイルスや不正アクセス等の手口や
対策に関する情報を、皆様にお届けします。
※情報発信専用のアカウントです
ご相談は→ipa.go.jp/security/anishi...

📍 東京都文京区本駒込 🌐 ipa.go.jp/about/socialme...
📅 2019年5月からTwitterを利用しています

4 フォロー中 1.6万 フォロワー

ツイート ツイートと返信 メディア いいね

固定されたツイート

IPA IPA (情報セキュリティ安心相談窓... ✓ @IPA_ans... · 2019年5月10日 ...
IPA情報セキュリティ安心相談窓口では、電話、メール、FAX、郵送での相
談を受け付けています。電話の受付時間は、平日の10:00～12:00、13:30～
17:00です。詳しくは→ipa.go.jp/security/anishi...

🗨️ 3 🔄 24 ❤️ 28 📌

アカウント名：
@IPA_anshin

IPA相談窓口の公式Facebook



IPA 情報セキュリティ安心相談窓口



～ 情報セキュリティで不安なことや困ったことが発生したら～
電話や**メール**でアドバイスを提供します

カバー写真を編集

IPA 情報セキュリティ安心相談窓口

65 件の「いいね！」・フォロワー110人

SCT 

宣伝する 管理 編集

投稿 基本データ メンション レビュー フォロワー 写真 その他

自己紹介

IPA情報セキュリティ安心相談窓口の公式アカウントです。窓口に寄せられる相談をもとに、コンピュータウイルスや不正アクセス等の手口や対策に関する情報を、皆様にお届けします。*情報発信専用のアカウントです。

自己紹介を編集

- ページ・政府関係者
- 東京都文京区
- IPA_anshin
- ipa.go.jp/security/anshin

ウェブサイトを宣伝

その気持ち、シェアしよう

ライブ動画 写真・動画 Reel

注目のコンテンツ

管理

IPA情報セキュリティ安心相談窓口

2022年9月29日

IPA情報セキュリティ安心相談窓口では、電話、メール、FAX、郵送での相談を受け付けています。電話の受付時間は、平日の10:00～12:00、13:30～17:00です。詳しくはー

<https://www.ipa.go.jp/security/anshin/>

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、スマホはウィルスに感染しにくいですが、ウィ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となりますので、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。

The logo for the Information-technology Promotion Agency, Japan (IPA). It consists of the letters 'IPA' in a bold, red, sans-serif font. The 'I' is a simple vertical bar, the 'P' has a rounded top and a curved bottom, and the 'A' has a wide base and a pointed top.

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