

本資料の位置づけ

- IPAが公開している「情報セキュリティ10大脅威 2022 個人編」の中からポイントとなる箇所をよりわかりやすく解説
- 主に個人のパソコンやスマホでインターネットを利用する人の視点でインターネットトラブルを避けるための対策に着目
- 10大脅威からみえる日々のインターネット利用における注意点についてワンポイントアドバイス
- 本書の解説内で登場する「クレジットカード情報※1」、「SMS※2」のように黄色のマーカーの(※)が付いている用語については、後段「用語解説(補足解説)」のページで補足解説をしています。

情報セキュリティ10大脅威 2022 脅威ランキング



順位	個人向けの脅威ランキング
1	フィッシングによる個人情報等の詐取
2	ネット上の誹謗・中傷・デマ
3	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	クレジットカード情報の不正利用
5	スマホ決済の不正利用
6	偽警告によるインターネット詐欺
7	不正アプリによるスマートフォン利用者への被害
8	インターネット上のサービスからの個人情報の窃取
9	インターネットバンキングの不正利用
10	インターネット上のサービスへの不正ログイン

【1位】フィッシングによる個人情報等の詐取

～宅配の不在通知を装うフィッシング詐欺に要注意！！～



公共機関や有名な企業などを装ったメールやSMS※2が送られてきて、偽のウェブサイトに誘導されます。そこでIDやパスワードなどの情報を入力してしまうと、その情報は悪者の手に渡ってしまいます。IDやパスワードが奪われると、自分が利用しているサービスに不正ログインされてしまい、様々な被害につながります。

【1位】フィッシングによる個人情報等の詐取

～宅配の不在通知を装うフィッシング詐欺に要注意！！～

● フィッシングの手口

フィッシングは実在する様々な公共機関や企業を装い、様々な内容のメールやSMS※2を送り付けてインターネット利用者を騙そうとします。

例1：水道局を装ったメール

例2：宅配便業者を装ったSMS

例3：カード会社を装ったメール

日頃のご利用ありがとうございます。
水道料金を支払っていない場合、
2022年9月5日までに料金を
払っていないと断水する可能性
がありますので、下のリンクを
クリックしてお支払い下さい。
<http://www.■■■■.com/~>

X月X日
お客様宛にお荷物のお届け
にあがりましたが不在のため
持ち帰りました。
配送物は下記よりご確認ください。
<http://www.■■■■.com/~>

いつもXXXXカードをご利用頂き
ありがとうございます。
この度、ご本人様のご利用が
確認させて頂きたいお取引が
ありましたのでカードのご利用を
一部制限させて頂きご連絡させて
頂きました。つきましては、以下
へアクセスの上、ご利用確認に
ご協力をお願い致します。
■ご利用確認は[こちら](#)

偽のウェブサイトのURLやリンク

メールやSMSの文面は本物に見えても、
クリックすると偽のウェブサイトが開かれるので要注意！

【1位】フィッシングによる個人情報等の詐取

～宅配の不在通知を装うフィッシング詐欺に要注意！！～

● 対策

メールやSMS※2は偽物ではないかと疑うという心構えが大事です

★ワンポイントアドバイス★

～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

普通だったら
他人に教えない情報
の入力を求められたら
特に注意！



一、慌てない

メールやSMSには慌てさせられたり、心配させられるような記載があっても
まずは一呼吸おく。慌てていると判断ミスをしがちですよね。

二、まずは疑う

公的機関や企業からメールやSMSが届いたら本物なのかまずは疑う。
さらに、ウェブサイトに誘導されてクレジットカード情報※1や口座番号、
パスワードなどの情報入力を求められたら操作を中断！

【1位】フィッシングによる個人情報等の詐取

～宅配の不在通知を装うフィッシング詐欺に要注意！！～

● 対策

三、本物か確認

疑ったあとは本物かどうかを確認しましょう。

～本物かどうか確認する方法の例～

- ・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※2を送ってき人に聞き返す

- ・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書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

- ・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。「詐欺」や「フィッシング」という情報が出てくるかも。



【2位】ネット上の誹謗・中傷・デマ

～1つの発言が人生を脅かす可能性も～



SNS※³や掲示板などで他人を誹謗・中傷したり、脅迫や犯罪予告ととられる書き込みをしたりすると**事件に発展する**場合があります。

また、デマを発信したり拡散したりすることで、世間の不要な混乱や自分自身の炎上問題に発展するおそれもあります。それだけでなく被害を受けた会社や個人に**訴えられる可能性**もあります。

【2位】ネット上の誹謗・中傷・デマ

～1つの発言が人生を脅かす可能性も～

● なぜそのような書き込みをしてしまうのか？

考えられる要因はたくさんあります。

■ 問題となる書き込みをしてしまう要因

- ・日頃の不満やストレスの捌け口としてしまう
 - ・面白い書き込みをして目立ちたいと考える
 - ・炎上したり、問題になったりするリスクを意識できていない
- など

■ デマを拡散してしまう要因

- ・情報がデマであるかもしれないという意識が不足
- ※見ず知らずの人が匿名で書いていることなのに、インターネット上で見た情報は何故か本当のことであると感じてしまいがち。
- ・災害対策情報などに関するデマ拡散は親切心が裏目に。
- など

【2位】ネット上の誹謗・中傷・デマ

～1つの発言が人生を脅かす可能性も～

● 対策

- ・インターネット上でもモラルに反したことはしないようにしましょう。
- ・インターネット上の情報には嘘も多いことを意識しましょう。

★ワンポイントアドバイス★

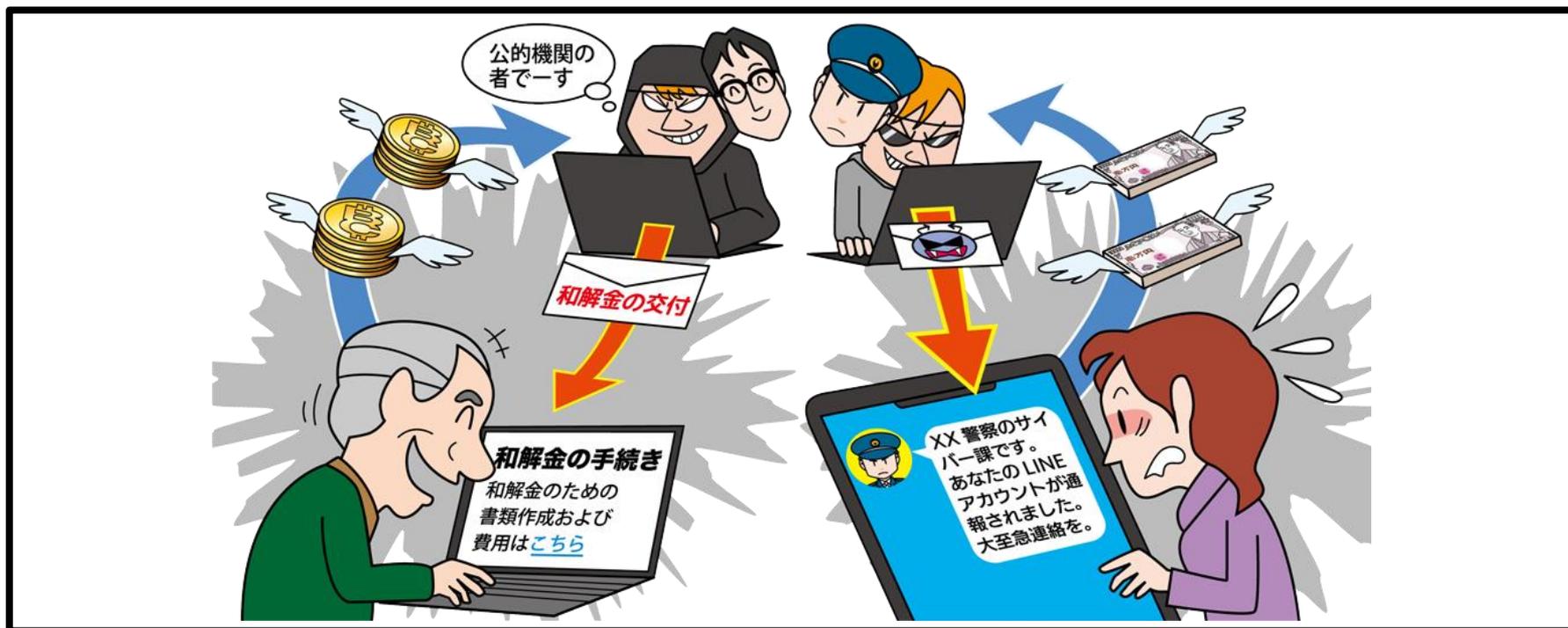
大勢の前で名乗って言えないこと、できないことはインターネットでもやらないという心構えも大事です。



■ その他の対策

- ・インターネットで得られた情報の真偽確認は慎重に。
(見ず知らずの人の言うことを鵜呑みにしない。)
- ・インターネット上の書き込みなどに過剰に反応しない。
- ・他の人が書いているから自分も書いて大丈夫と思わない。
- ・他人が発信した情報の「拡散(Twitterであればリツイート)」も問題になるかもしれないことを意識する。

【3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 ～公的機関を装ったメール等に注意～



金銭を支払わせようと脅迫するメールやSMS※2がいきなり送りつけられます。請求内容に身に覚えがなかったとしても、支払いを迫る脅迫的な内容が記載されているケースもあります。その内容に騙されて不安に思った結果、相手の要求に従い、金銭を支払わされてしまいます。

【3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 ～公的機関を装ったメール等に注意～

● どのような脅迫をしてくるのか？

脅迫の内容は世の中の状況により様々です。多くの人に身に覚えがありそうな内容にするなど、あの手この手を使って騙そうとしてきます。

■ 脅しの手口

ポイント① “怖がらせる”

「あなたのパソコンをハッキングした」「あなたが通報されている」など

ポイント② “信じ込ませる”

「あなたのパスワードはXXXXだ」「電話で弁護士を名乗る」など

※パスワードを言い当てて、あたかも本当にハッキングしたと信じ込ませる

(パスワードは過去にどこかで漏えいしたもの)

※メールやSMS※2で電話を掛けるよう誘導し、電話を掛けると弁護士等を名乗る者などが

応答し、詳細を説明することで信じ込ませる

ポイント③ “相談しにくい内容に” (アダルト関連など)

「あなたの恥ずかしい動画を撮影した」

「アダルトサイトの未納料金があり裁判沙汰になる」など

【3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 ～公的機関を装ったメール等に注意～

● 対策

身に覚えのない不審なメールは無視しましょう。

（脅しの内容は事実にもとづかないものであることがほとんどです）

身に覚えがあっても、本当に支払う必要がある要求なのか不安な場合は
まずは信頼できる人に相談する

★ワンポイントアドバイス★

まずは冷静になりましょう。

相談できる人がいない時や相談しても解決できない時は公的機関
の相談窓口※12へ相談するのも有効です



■ その他の対策

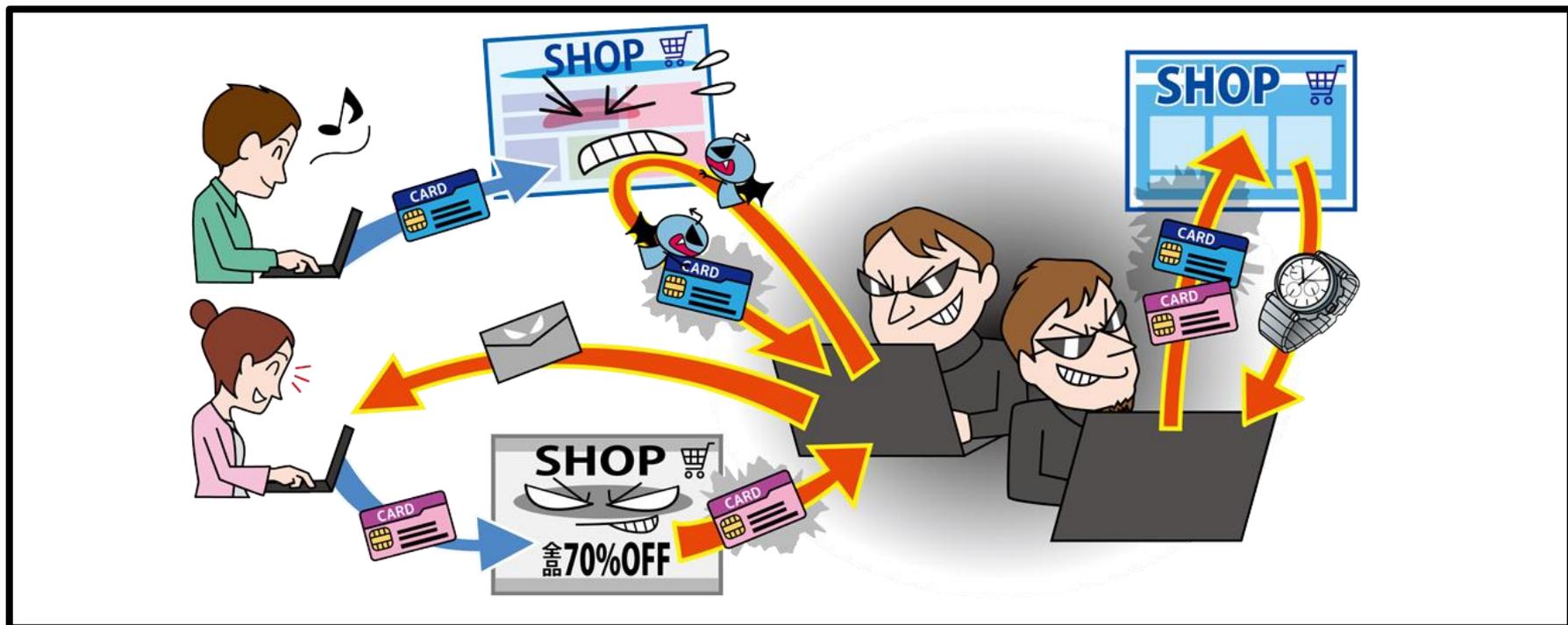
・この手のメールは世の中の不特定多数にばらまかれている。

タイトルや本文中の特徴的なキーワードでインターネット検索してみると
同様の事例や対策に関する情報が見つかるかも。

（冷静になれたり安心につながる）

【4位】クレジットカード情報の不正利用

～不審な利用記録がないか今一度確認を～



クレジットカード自体は大切に保管していても、クレジットカード情報※1を盗まれ、さらにショッピングサイトなどで自分のクレジットカードを不正利用されてしまうおそれがあります。自分の銀行口座から不正利用された分が支払われ、金銭的な被害を受けます。

【4位】クレジットカード情報の不正利用

～不審な利用記録がないか今一度確認を～

● どうするとクレジットカード情報※1を盗まれるか？

最近ではクレジットカード情報を狙うフィッシングという手口が多く確認されています。また、メールを利用したウイルス※4感染による手口もあります。

■ フィッシングとは

偽のウェブサイトへ誘導してクレジットカード情報や個人情報を入力させようとしてくる手口です。

フィッシングについての詳細は【1位】の項目で解説していますのでそちらをご確認ください。

■ メールを利用したウイルス感染とは

メールに、ウイルスが付いたファイルを添付して送り付け、PCなどに感染させようとしてくる手口です。添付ファイルを開くとウイルスに感染してしまう場合があります。ウイルス感染した端末で決済を行うとクレジットカード情報が盗まれてしまいます。

【4位】クレジットカード情報の不正利用

～不審な利用記録がないか今一度確認を～

● 対策

メールやSMS※2に騙されて安易に操作しないようにしましょう。
フィッシングにもウイルス※4感染にも有効です。

★ワンポイントアドバイス★

～騙されない三箇条～
一、慌てない
二、まずは疑う
三、本物か確認する

【1位】でも紹介している
“騙されない三箇条”
は色んな所で
役に立つんだ！



■メールやSMSに注意！

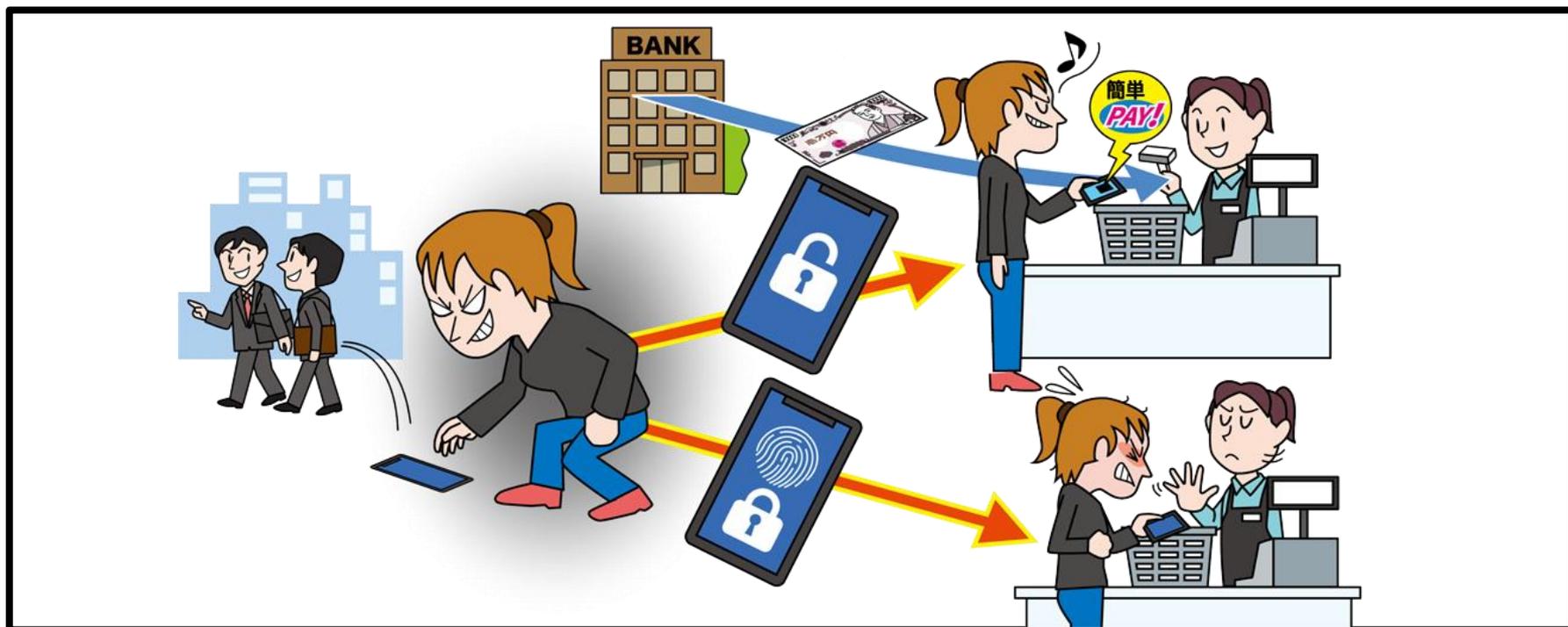
“騙されない三箇条”を要チェック！！

■メールは添付ファイルにも注意！

メールに添付ファイルがあって、気になることが本文に書いてあっても
安易に開かない。開いてしまった後、見慣れない画面や警告が表示
されても大事な情報を安易に入力してはいけない。

【5位】スマホ決済の不正利用

～今や「スマートフォン」＝「個人情報、財産」の時代！日頃からリスク管理の徹底を～



スマホ決済サービスの自分のアカウントを乗っ取られると、チャージ済みの**残高**を利用して**決済**されたり、さらにチャージ用に登録しているクレジットカードや銀行口座から**勝手に残高をチャージ**されてそれを利用されたりするおそれがあります。

【5位】スマホ決済の不正利用

～今や「スマートフォン」＝「個人情報、財産」の時代！日頃からリスク管理の徹底を～

● どのようにして不正ログインされるのか？

■ 盗んだIDやパスワードを使ってサービスに不正ログイン

パスワードを盗むためにフィッシングという手口が多く確認されています。フィッシングについての詳細は【1位】の項目で解説していますのでそちらをご確認ください。

■ ”パスワードの使いまわし”をしている人を狙って不正ログイン

世の中にはたくさんのサービスがあり、ひとりで複数のサービスを利用するのがあたりまえとなっています。その中で利便性の観点から同じIDやパスワードを使いまわしてしまっているケースがあります。

悪意のある人は盗んだIDやパスワードを使って、複数のサービスに不正ログインしようと試みてくることがあり、同じIDやパスワードを使いまわしていると、複数のサービスに不正ログインされるおそれがあります。

【5位】スマホ決済の不正利用

～今や「スマートフォン」＝「個人情報、財産」の時代！日頃からリスク管理の徹底を～

● 対策

- ・パスワードの使いまわしをしないようにしましょう
(ひとつのパスワードが漏れるとその他のサービスでも被害にあうかも)
- ・パスワードは長く、複雑なものにしましょう

×簡単に予想されるこんなパスワードは絶対NG！

名前や生年月日にちなんだパスワード、“password”、“123456”
キーボードの連続した文字列(“1qaz2wsx”、“qwerty”等)

- ・多要素認証※7や3Dセキュア※8が利用できるサービスであれば利用。

★ワンポイントアドバイス★

特に”パスワードの使いまわし”をしないことが大事です。

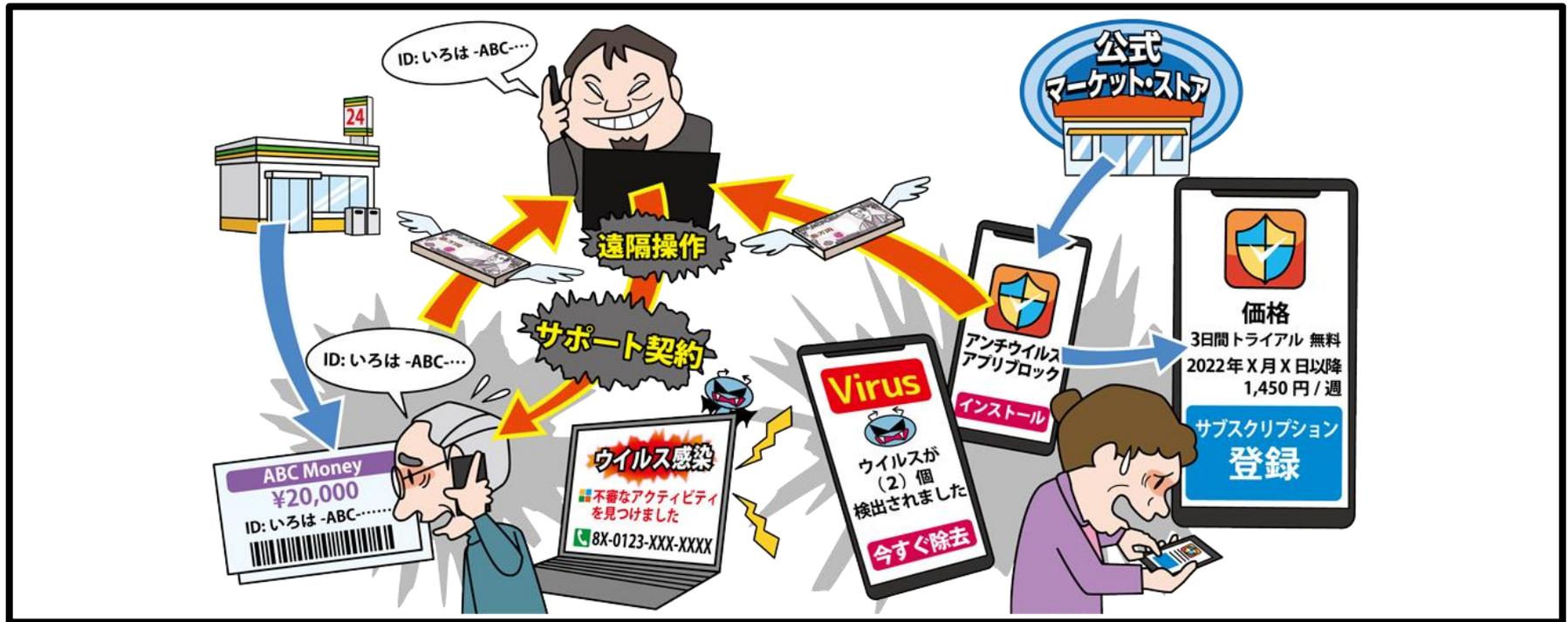


■その他の対策

- ・不正ログインされたときにすぐ気づけるようにログイン通知機能※11などを利用。

【6位】偽警告によるインターネット詐欺

～それは詐欺です。慌てる、焦るは思うツボ！～



インターネットを閲覧中に「あなたのパソコンがウイルス※4に感染している」などの警告(偽警告)が表示され、電話のサポート窓口へ誘導されます。その窓口で電話すると、不要なサポート契約やソフトウェアの購入を勧められ金銭被害につながります。

【6位】偽警告によるインターネット詐欺

～それは詐欺です。慌てる、焦るは思うツボ！～

● どのようにして電話窓口へ誘導されてしまうか？

あの手この手を使って偽警告を信じ込ませようとしてきます。

■ 偽警告で不安を煽る

- ・「ウイルス※4に感染している」という不安を煽る偽警告
- ・偽警告が簡単には閉じられないように工夫されている
※警告が次々に表示される、画面を閉じても再び表示される、×や閉じるボタンが無い、“更新する”や“インストール”のボタンしかないなど。
- ・偽警告を画面に表示するとともに警告音も鳴らしてさらに不安を煽る
- ・正規のセキュリティソフトがウイルスを検知したかのような偽の画像を表示する
- ・公式を装う偽の窓口の電話番号を表示し、電話をかけさせるよう誘導するなど

【6位】偽警告によるインターネット詐欺

～それは詐欺です。慌てる、焦るは思うツボ！～

● 対策

不安に感じる警告が表示されても、慌てて言われるがままに対応しない。

警告の内容は様々です。偽物なのか本物なのか判断ができない場合は警告の指示に安易に従わず、まずは信頼できる人に相談しましょう。

★ワンポイントアドバイス★

電話をかけさせようとしてきたら特に注意。

(偽警告以外にもワンクリック請求やその他の詐欺にも共通する常套手段)



■ その他の対策

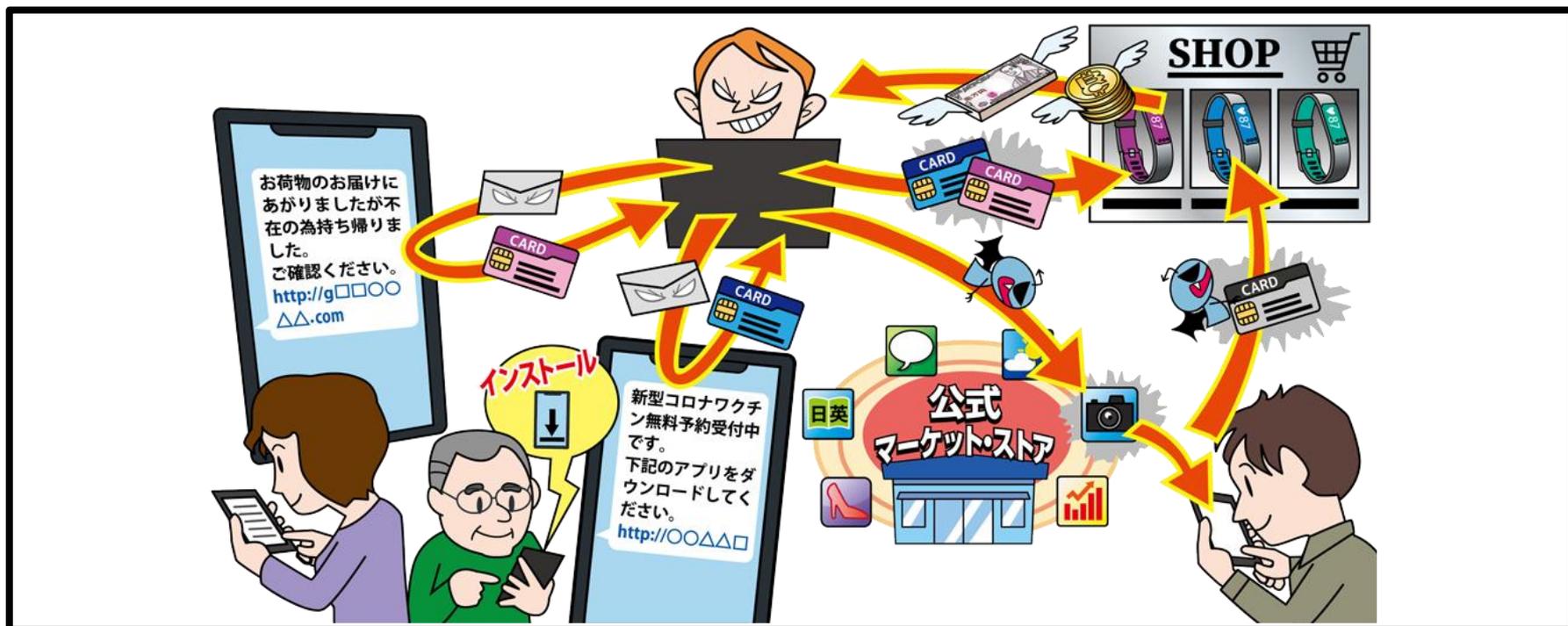
- ・相談できる人がいない時や、相談しても解決できない時など対応に困ってしまった場合は公的機関の相談窓口※12に相談するのも有効。

※とりあえず警告音を消したいという場合は、パソコンのボリューム調整やシャットダウンを

- ・偽警告は不特定多数に対して行われる手口。表示された警告内の特徴的なキーワードなどでインターネット検索して事例や対策の情報を確認。
- ・ソフトウェアインストールや個人情報入力を促してくるパターンにも要注意。

【7位】不正アプリによるスマートフォン利用者への被害

～偽装 SMS の URL リンクや不正アプリへの誘導に注意～



スマホには便利なアプリがたくさん。ただし中には悪意のある人が作成した不正アプリ※5もあります。不正アプリを自分のスマホにインストールしてしまうと、スマホ内の連絡先情報がとられたり、悪意のある人に不正操作(不正なSMS※2の拡散等)され、加害者にされてしまう可能性もあります。(踏み台※10)

【7位】不正アプリによるスマートフォン利用者への被害

～偽装 SMS の URL リンクや不正アプリへの誘導に注意～

● どうすると不正アプリがスマホに入ってしまうのか？

スマホアプリをインストールするには、スマホ上でのインストールの操作が基本です。そのため、不正アプリ※5も 自分で入れてしまっているということになります。

■ 有用なアプリであると騙されて不正アプリを自分で入れてしまう

パターン①

メールやSMS※2などで不正アプリを 配布しているサイトへ誘導されて、インストールしてしまう。

実在の企業等を
名乗っているからと
安易に信じてはいけない！

パターン②

公式マーケットに紛れ込んでいる
不正アプリを気づかずに
インストールしてしまう。

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！！

【7位】不正アプリによるスマートフォン利用者への被害

～偽装 SMS の URL リンクや不正アプリへの誘導に注意～

● 対策

不正アプリ※5の存在を知り、不正アプリをインストールしないようにしましょう。

★ワンポイントアドバイス★

アプリをインストールするときは信頼できるか確認

- ・アプリの提供元は信頼できるか
- ・アプリ自体は信頼できるか



■確認ポイント

- ・まず“アプリのインストールは公式マーケットから”を心がける

Androidスマホは「Google Play」、iPhoneは「App Store」

※Androidの場合は「提供元不明のアプリのインストール」を許可しない

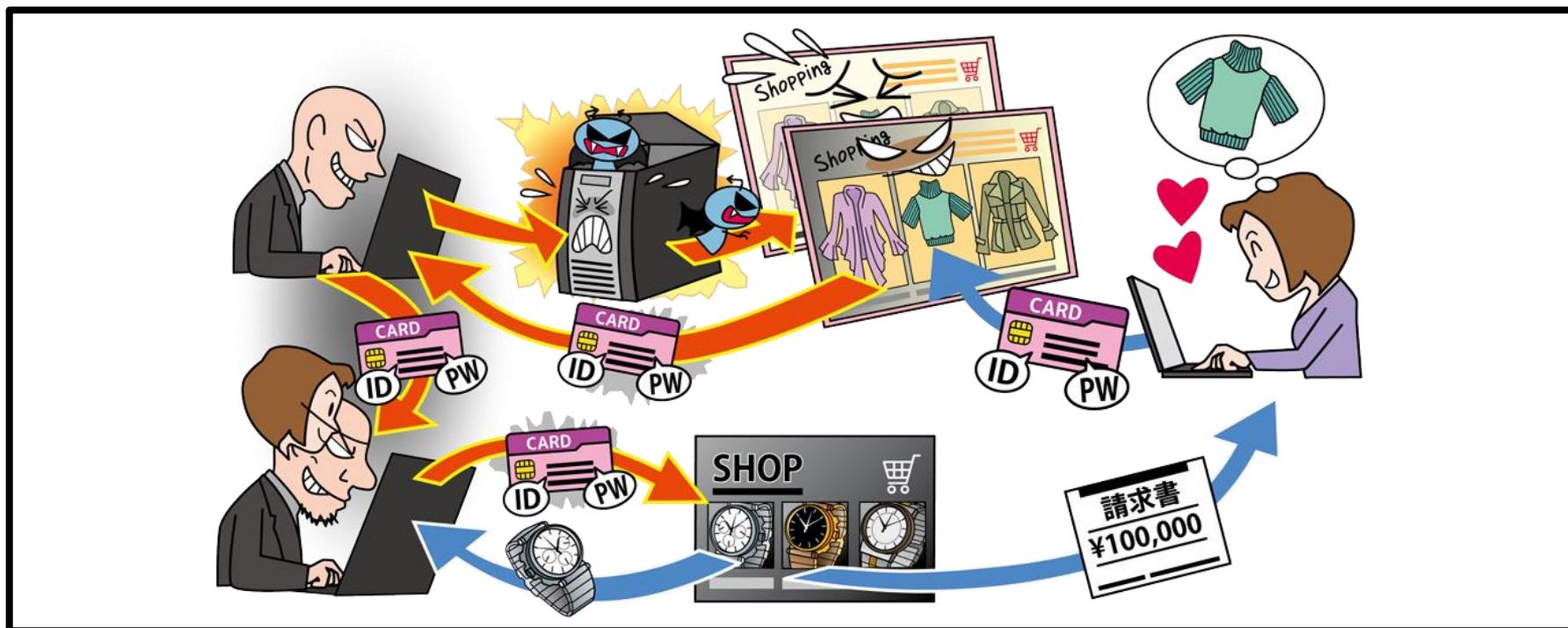
- ・公式マーケットだからといって安心しない。アプリ自体の評判も確認。

(マーケットのレビューを参考にしたり、インターネットで検索してみたり。)

※レビューは悪意のある人も投稿できるので様々な種類の情報を参考にする。

【8位】インターネット上のサービスからの個人情報の窃取

～頻発する個人情報の漏えい、利用者もできる限りの対策を～



ショッピングサイトなどのインターネット上のサービスに対し、サービスの脆弱性^{※9}を悪用した不正アクセスや不正ログインが行われ、利用者がサービスに登録している個人情報などの重要な情報を窃取されるおそれがあります。

窃取された情報を悪用されるとクレジットカードを不正利用されたり、詐欺メールが届くようになりたりします。

【8位】インターネット上のサービスからの個人情報の窃取

～頻発する個人情報の漏えい、利用者もできる限りの対策を～

● どのようにして個人情報が窃取されるのか？

■ サービスの脆弱性※9を悪用して不正アクセスして情報窃取

サービスで利用しているソフトウェアなどで適切なセキュリティ対策が行われていない場合、サービスへの不正アクセスが行われ、登録されている情報が窃取されるおそれがあります。

■ サービスの脆弱性を悪用してウェブサイトを改ざんし、情報窃取

まず、攻撃者が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します。その後、利用者がウェブサイトの改ざんに気が付かずに個人情報を入力してしまうと、その情報が窃取されてしまいます。

■ サービス利用者のアカウントに不正ログインして情報窃取

詳細は【10位】の項目で解説していますのでそちらをご確認ください。

【8位】インターネット上のサービスからの個人情報の窃取

～頻発する個人情報の漏えい、利用者もできる限りの対策を～

● 対策

サービス自体に脆弱性※9があった場合は**利用者での対策には限界があります**。
ウェブサイトなどでサービス内容をよく確認し、適切に脆弱性対策を実施して
くれるような**信頼できるサービスを利用する**ように心がける意識が大事です。

★ワンポイントアドバイス★

- ・不要なサービスは利用しない(利用していないサービスの退会)
- ・サービス利用にあたって**不要な情報は安易に登録しない**



■ その他の対策

重要な情報を窃取されてしまう可能性は常に意識しましょう

- ・クレジットカード**利用明細の定期的な確認**(不正利用されていないか確認)
- ・**実際に被害に遭ったときの対応を整理しておく**(サービス運営者への問い合わせ、クレジットカードの停止連絡、パスワードの変更など)

【9位】インターネットバンキングの不正利用

～金融機関からSMSが送られてきても、ひとまず落ち着こう～

● どのようにしてIDやパスワードが盗まれるのか？

■ フィッシングで盗まれる

- ・脅威の【1位】で出てきた手口です。詳細はそちらをご確認ください。
- ・インターネットバンキングの不正利用を狙った攻撃の場合、銀行を騙ったメールやSMS※2などを使って偽サイトに誘導される手口が良く使われます。例えば、「不正利用の疑いがあるのでログインして確認を」などの理由をつけてIDやパスワードの情報を入力させようとします。

■ ウィルス※4で盗まれる(パソコンの場合)

- ・IDやパスワードを盗むためのウィルスをメールに添付してばらまく
- ・そのメールの添付ファイルを開くとウィルスに感染してしまう場合がある

■ 不正なアプリで盗まれる(スマホの場合)

- ・脅威の【7位】で出てきた手口です。詳細はそちらをご確認下さい。

【9位】インターネットバンキングの不正利用

～金融機関からSMSが送られてきても、ひとまず落ち着こう～

● 対策

- ・フィッシングに騙されないようにしましょう。(詳細は【1位】を確認)
- ・ウイルス※4に感染しないように注意しましょう。
(セキュリティソフトを利用。メールの添付ファイルを安易に開かない。
利用するソフトウェアは日々更新して脆弱性※9対策。)
- ・アプリのインストールに注意しましょう。
(アプリは公式マーケットからインストールする。インストールする前に
アプリのレビューや評価を見て、信頼できるかを判断する。)
- ・アプリの使い方に注意しましょう。
(IDやパスワードなど重要な情報をメモアプリで管理しない。メモアプリに
保存した情報は盗み見られる可能性があることを意識しましょう。)

メモアプリに保存していたインターネットバンキング
のIDとパスワードを窃取され、不正送金された
事件が2021年に実際に起きているんだ。



【9位】インターネットバンキングの不正利用

～金融機関からSMSが送られてきても、ひとまず落ち着こう～

● 対策

★ワンポイントアドバイス★

ワンタイムパスワード※6による多要素認証※7など、銀行が推奨する認証方式を利用しましょう。

(パスワードが盗まれても不正ログインされない対策を)



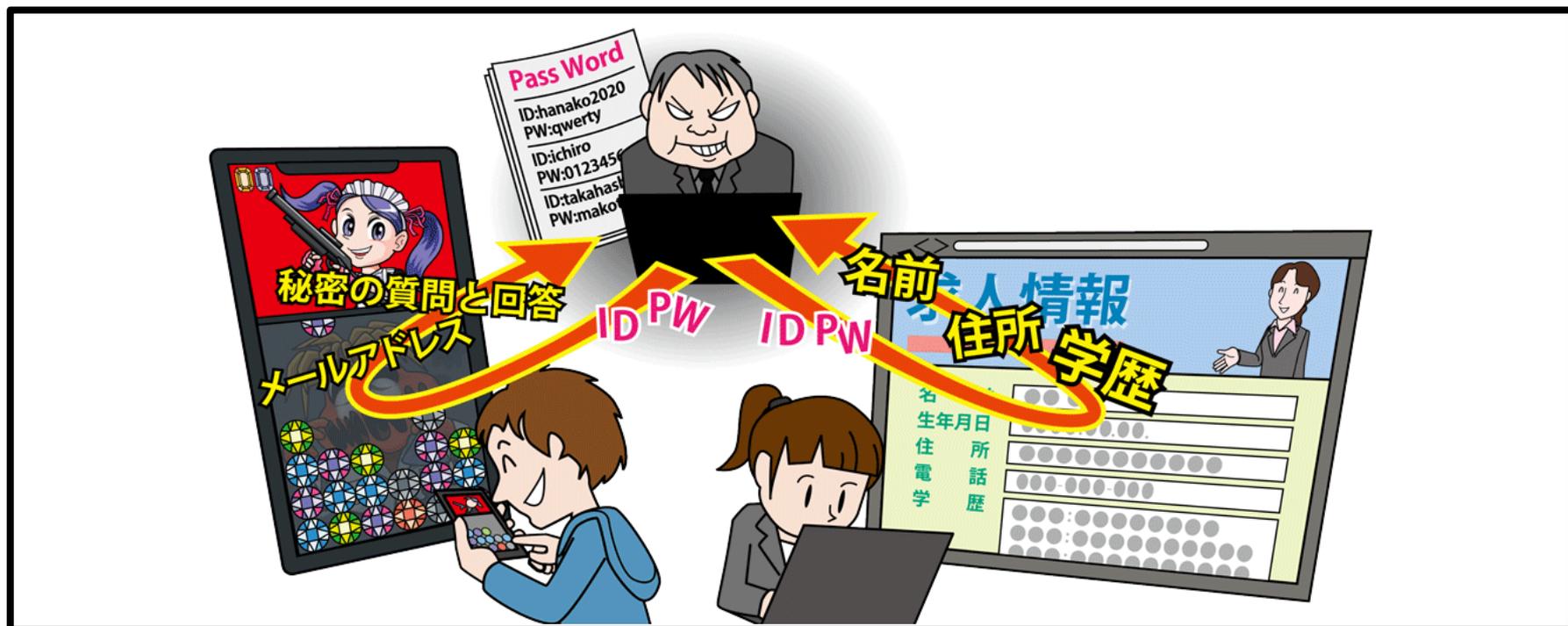
■その他の対策

- ・ワンタイムパスワードの利用方法は専用の機器を使用したりスマホのアプリを使用したりなど銀行により様々。詳細は銀行のサイトなどで確認。
- ・ウイルス※4に感染しないための対策は様々。

まずは“パソコンで不審なメールの添付ファイルを開くとウイルスに感染する可能性がある”ことを知る。

【10位】インターネット上のサービスへの不正ログインIPA

～パスワードの使い回しに注意、あなたの個人情報が閲覧されるかも～



【9位】で登場したインターネットバンキング以外にも、便利なインターネット上のサービスがたくさんあります。（オンラインショッピング、動画配信、電子書籍、SNS※3など）

IDやパスワードでログインして利用するサービスは、IDやパスワードが盗まれると不正ログインされて勝手にそのサービスの機能を使われてしまいます。

【10位】インターネット上のサービスへの不正ログインIPA

～パスワードの使い回しに注意、あなたの個人情報が閲覧されるかも～

● どのようにして不正ログインされるのか？

■ 盗んだIDやパスワードを使ってサービスに不正ログイン

【1位】で紹介したように、主にフィッシングで盗まれたIDやパスワードを使われます。

■ ”パスワードの使いまわし”をしている人を狙って不正ログイン

世の中にはたくさんのサービスがあり、ひとりで複数のサービスを利用するのがあたりまえとなっています。その中で利便性の観点から同じIDやパスワードを使いまわしてしまっているケースがあります。

悪意のある人は盗んだIDやパスワードを使って、複数のサービスに不正ログインしようと試みてくることがあり、同じIDやパスワードを使いまわしていると、複数のサービスに不正ログインされるおそれがあります。

【10位】インターネット上のサービスへの不正ログインIPA

～パスワードの使い回しに注意、あなたの個人情報が閲覧されるかも～

● 対策

- ・パスワードの使いまわしをしないようにしましょう
(ひとつのパスワードが漏れるとその他のサービスでも被害にあうかも)
- ・パスワードは長く、複雑なものにしましょう

×簡単に予想されるこんなパスワードは絶対NG!

名前や生年月日にちなんだパスワード、“password”、“123456”
キーボードの連続した文字列(“1qaz2wsx”、“qwerty”等)

★ワンポイントアドバイス★

特に”パスワードの使いまわし”をしないことが大事です。



■その他の対策

- ・ワンタイムパスワード※6など多要素認証※7が利用できるサービスであれば利用。
- ・不正ログインされたときにすぐ気づけるようにログイン通知機能※11などを利用。

1. 【フィッシングに騙されないようにする】

受信したメールやSMS※2、閲覧しているウェブサイトは偽物でないかを疑う

- 判断に迷う場合は信頼できる人に相談する
- 正規の問い合わせ窓口に本当に送信したか確認する
- 送られてきたメールやSMSのタイトル、本文の一部をインターネットで検索して同様の事例がないか確認してみる

2. 【偽警告や不審なメールに騙されないようにする】

身に覚えのない警告やメールは無視する

- 脅しや心配になるような記載があっても慌てて対応しない
- 警告やメール内の特徴的なキーワードをインターネットで検索して、同様の事例がないか確認したり、信頼できる人に相談する
- 相談しても解決できなかつたり不安な時は公的機関の相談窓口※12へ

3. 【不正ログインされないようにする】

パスワードは適切に管理する

- パスワードの使いまわしはせず、長く複雑なパスワードにする
- ワンタイムパスワード※6など多要素認証※7が使える場合は利用する
- 初期パスワードが設定されている場合はパスワードを変更する

4. 【不適切な情報発信(拡散も含む)はしないようにする】

インターネット上での情報発信やコミュニケーションもモラルを大切に

- 日頃の不満やストレスの捌け口にして過激なことを書かない
- どんな情報も安易に信じず、まずはデマでないかを確認する
- 他人が発信した情報を拡散しただけでも責任を問われる可能性があることを意識する
- 炎上したり問題になったりした時のリスクを意識する

5. 【スマホの不正アプリ※5はインストールしないようにする】

スマホにアプリをインストールするときは信頼できるものか確認

- アプリは公式マーケットからインストールする
- アプリの提供元が信頼できるか確認する
- アプリ自体の評判を確認する

6. 【パソコンのウイルス※4対策を実施する】

- セキュリティソフトを利用する
- 利用しているソフトウェアを更新する
- メールの添付ファイルを安易には開かない
- ランサムウェア対策のために重要なファイルはバックアップを取っておく

よくある事例

**最近のよくある事例を3つご紹介します。
これまでの内容を踏まえて対応を考えてみましょう。**



【事例1】SMSを悪用したフィッシング

～携帯電話に宅配便業者から不在通知のSMSがきた～

■危険な対応



なにか荷物が届いたのかな？
記載されているページに
アクセスしてみよう。

SMS※2の内容

お客様宛にお荷物のお届けにあがりましたが不在のため持ち帰りました。配送物は下記よりご確認ください。

<http://www.■■■■.com/~>



宅配便業者を装った偽のSMSです。一般的に宅配便業者は不在通知をSMSでは送りません。

誘導先のページは、不正アプリ※5のインストールサイトやフィッシングサイト等です。



【事例1】SMSを悪用したフィッシング

～携帯電話に宅配便業者から不在通知のSMSがきた～

■安全な対応

SMS※2の内容

お客様宛にお荷物のお届けにあがりましたが不在のため持ち帰りました。配送物は下記よりご確認ください。

<http://www.■■■■.com/~>



偽のSMSだと思うから
無視しよう。



本当に荷物が届いたのかも。
でもこのSMSは怪しいので
宅配便業者の正しい窓口に
電話で確認してみよう。



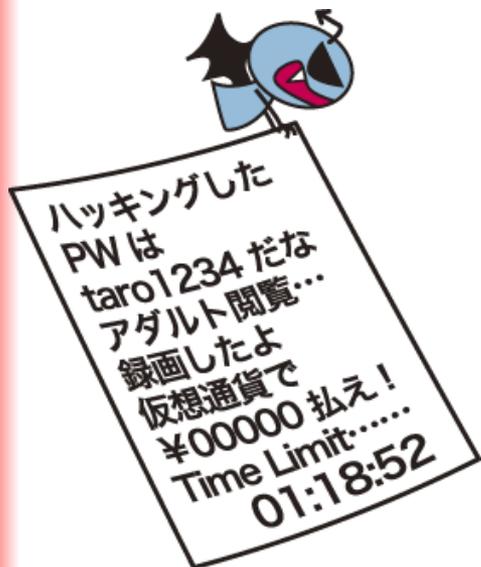
【事例2】 金銭を要求する脅迫メール

～脅迫内容が書かれた金銭を要求するメールがきた～

■危険な対応



自分のパスワードが書いてある！
アダルト閲覧も身に覚えがある
し…。お金を払ってしまおう。



実際にハッキングされている
ということではありません。

パスワードが当たっているのは、
どこかで漏えいしてしまった情報
がインターネットに出回っている
ものを悪用されたことなどが
考えられます。

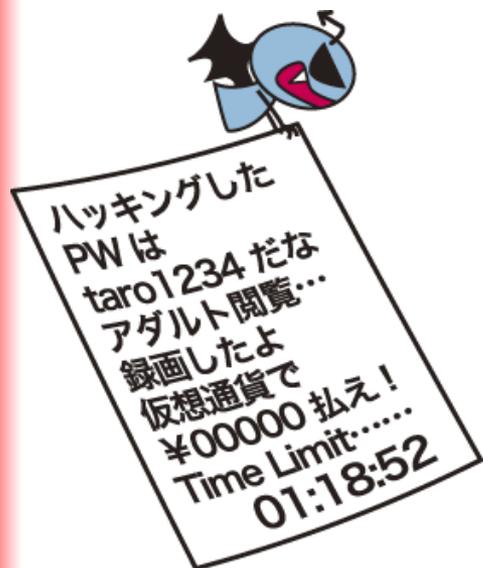
要求された金銭を支払うと
不要な金銭被害になります。



【事例2】 金銭を要求する脅迫メール

～脅迫内容が書かれた金銭を要求するメールがきた～

■安全な対応



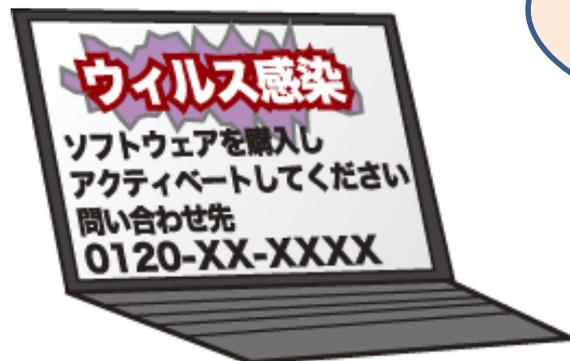
よくある迷惑メールの一種
だな。**無視**しよう。

パスワードが当たっているとい
うことは自分のパスワード情報
が漏れているのだろうか。
パスワードは変更しておこう。

【事例3】インターネット中に表示される偽警告

～パソコンでインターネットをしていたらウイルス感染の警告が出た～

■危険な対応



ウイルス※4に感染した！！
書いてある問い合わせ先に
電話してみよう。



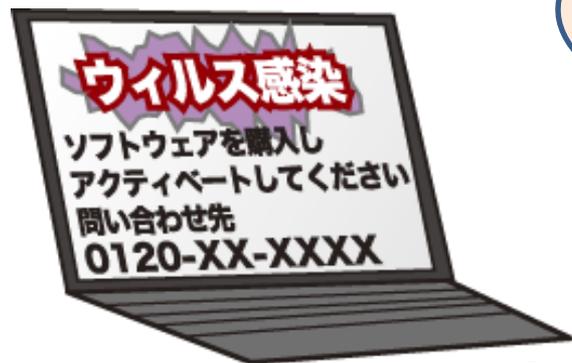
これは偽の警告です。
実際にウイルスに感染
しているわけではありません。
誘導された問い合わせ先に
連絡すると、不要なソフトの
購入や不要なサポート契約を
促されます。



【事例3】インターネット中に表示される偽警告

～パソコンでインターネットをしていたらウイルス感染の警告が出た～

■安全な対応



いきなりソフトウェアを買わせたり電話させたりするのは怪しい。警告は無視して閉じよう。



警告がうまく閉じられない。けどこの問い合わせ先に電話するのは怖いので誰かに相談してみよう。



■安心相談窓口だより

IPAの情報セキュリティ安心相談窓口※12に寄せられたインターネットトラブルの相談内容等を基に、**よくある事例やその対策**について紹介しています。

安心相談窓口だより

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

■手口検証動画シリーズ

相談が寄せられた事例の手口について、**実際に検証した際の様子**を「手口検証動画シリーズ」として公開しています。

手口検証動画シリーズ

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

用語解説(補足解説)

資料内で使用した用語の補足解説です。



■クレジットカード情報※1

クレジットカードでオンライン決済を行う際に必要となる情報のこと

具体的には・・・

- ・クレジットカード番号
- ・カード会員名
- ・有効期限
- ・セキュリティコード ※クレジットカードに記載された3桁または4桁の数字が該当します。

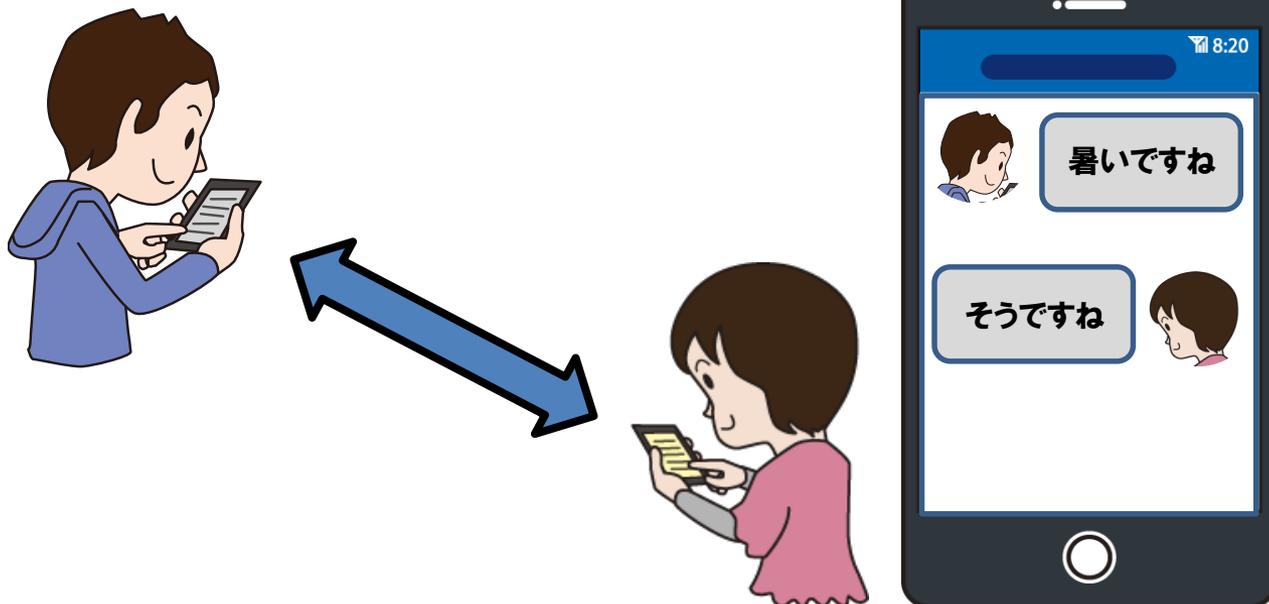
■SMS※2

ショートメッセージサービス(**S**hort **M**essage **S**ervice)の略称のこと

※SNS※3とは別物なので混同しないように注意(次ページ参照)

携帯電話同士で短いメッセージを送受信できるサービスです。

電話番号を宛先にして送信するため、例えば電話番号だけ知っている相手との連絡手段などに利用できます。



■ SNS※3

ソーシャルネットワーキングサービス(Social Networking Service)
の略称のこと

※SMS※2とは別物なので混同しないように注意(前ページ参照)

インターネットを利用して人と人がつながれるようなサービスを指す言葉です。

有名なサービスとしては以下が挙げられます。

- Facebook
- LINE
- Instagram
- Twitter

など

■ウイルス※4(コンピュータウイルス)

パソコン上で悪い動きをする不正なプログラムのこと

病原となるインフルエンザウイルスなどのように、感染を広げたり、潜伏、発症したりなどの動きをする不正なプログラムを、パソコンの世界でもウイルスと呼ぶようになりました。



『マルウェア』って聞いたこと、ありますか？

似たような用語として“マルウェア”があります。これは悪意のあるソフトウェアの総称です。しかし、古くからウイルスという表現が定着しているため、多くの人に伝わりやすいように、マルウェアをウイルスと表現している場合が多いです。厳密に言うとウイルスはマルウェアの一種です。悪意のあるソフトウェアには、ウイルスの他にもトロイの木馬やワームなどがあります。これらを総じてマルウェアと呼びます。

■不正アプリ※5

悪意のある人が作成した**悪い動きをするアプリ**のこと

スマホには、ゲーム、音楽プレイヤー、カメラ、メール、SNS※3、電子書籍など様々な機能があります。これらの機能を実現しているものをアプリと呼んでいます。アプリはとても便利なため、多くの人が様々なアプリをインストールして使っています。それを利用して悪意のある人が不正アプリをインストールさせようとしてくるのです。

不正アプリは勝手にインストールされるんですか？

不正アプリはあくまでアプリなので、通常のアプリと同様、**スマホ上でインストール操作をしない限りは、勝手にスマホに入り込むことは基本的にありません。**



※Androidスマホの場合はGoogleアカウント、iPhoneの場合はApple IDにログインできればアプリのインストールは可能なので、それらの**アカウントが他人にログインされないように要注意**
スマホは他人に触られないようにする対策も意識しましょう。

(画面ロックをかける、スマホを放置しない、など)

■ワンタイムパスワード※6

パスワードに短い有効期限を設け、使用されたらそのパスワードを無効にしてしまう、一度限り有効なパスワード

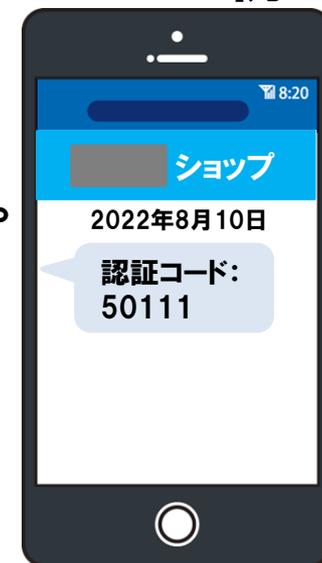
インターネット上のサービスなどにログインする際、利用者はサービスが作り出したパスワード(ワンタイムパスワード)をあらかじめ決めていた方法(SMS※2等)で受け取ります。その後、受け取ったワンタイムパスワードを用いてログインします。また、頭文字をとって”OTP”と略されることもあります。

ワンタイムパスワードを使うと何が良いの？

あらかじめ登録した連絡先に発行することで本人しかログインできなく、不正ログインの防止に役立ちます。

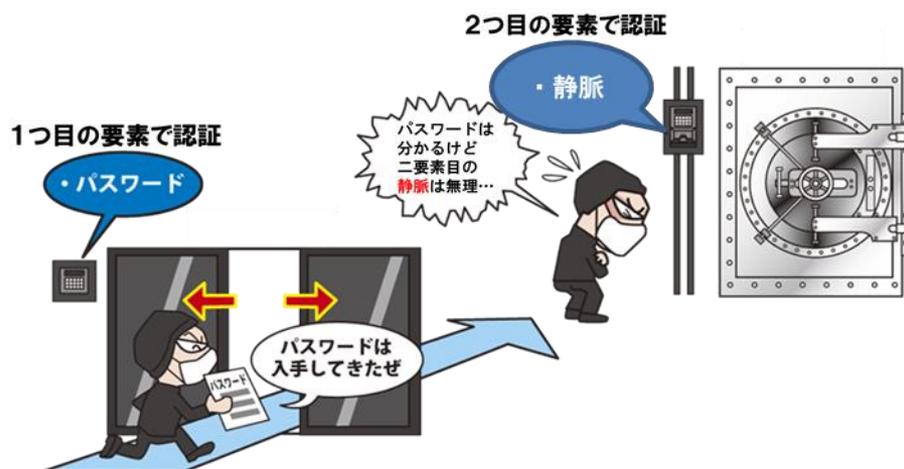
※複数の段階で認証を行う多段階認証のほかにも、複数の要素で認証を行う多要素認証※7もあり、強い認証方式であるとされています。ここでの説明は割愛しますが、興味があればぜひ調べてみましょう。(SMSでの多段階認証は、SMSが自分の電話番号に届くという性質上、多要素認証の要件を満たしています。)

～SMSの例～



■多要素認証※7

認証をするのに、1つの要素(例えばパスワード)だけでなく、他の要素も付け加えて複数の要素を要求される認証のこと



認証するための要素には大きく分けて3つの要素(「記憶」、「所持」、「生体情報」)があります。例えば自分が暗記しているパスワードなどは「記憶」、自分が所持しているクレジットカードなどは「所持」、自分の静脈や指紋、顔の情報などは「生体情報」として位置づけられます。

それら3つの要素から複数の要素を用いる認証を多要素認証と呼びます。

■多要素認証※7

二要素認証と多要素認証って何が違うの？

どちらも複数の要素を用いて認証する方法であることに変わりはありません。
特に、2つの要素を用いる場合を「二要素認証」と呼んでいるだけです。

二要素認証と二段階認証って何が違うの？

1ページ前のイラストを見て、「あれ？これは二要素認証？二段階認証？」
と、迷いませんでしたか？二段階認証とは段階の数が重要であり、要素の数は
いくつでも構わないのです。

例えば…

認証する時、パスワードを入力した後で「秘密の質問の答え」を聞かれることが
あります。「パスワード」も「秘密の質問」の答えも利用者の「記憶」に属する要素
ですね。このように二段階認証は認証に使う要素が1つでも良いのです。

■多要素認証※7

複数の要素？具体的にどうやって認証するの？

例えば最近では、ログイン画面でパスワードを入力したあと、携帯電話宛にSMS※2が送信されてきて、そのSMSに記載されている情報をログイン画面で入力することでログインが完了となるタイプのサービスが多いです。

上記において、1つ目のパスワードは「記憶」、2つ目の携帯電話宛に送信されてくる情報は、携帯電話を所持していないと見ることができない特性を利用して「所持」の条件を満たすことで多要素認証としています。

どうやって使えばいいの？

製品やサービスによって強制的に多要素認証にされていたり、設定画面などで利用者が多要素認証の有効/無効を設定できたり様々です。

もしも設定できるのであれば多要素認証を有効にしておくと安心です。

■3Dセキュア※8

3Dセキュアはクレジットカードにおける**本人認証サービスの名称**のこと

例えば、クレジットカードを紛失して悪意のある人に拾得された場合、不正利用されるおそれがあります。これを避けるための仕組みです。あらかじめクレジットカード会社にパスワードなどを登録しておき、その**パスワードで本人認証した上で決済を完了する**という方式が3Dセキュアです。

3Dセキュアを利用するためには、クレジットカード会社およびそれを使用するショッピングサイト双方が対応している必要があります。

どのように役に立つの？

インターネット上のショッピングサイトなどでクレジットカードを利用してオンライン決済を行う場合、クレジットカード情報※1をショッピングサイトで入力することで決済します。この時、クレジットカードさえ持っていれば、クレジットカード名義人本人でなくとも決済ができてしまいます。しかし、**3Dセキュアを利用していればクレジットカードだけでは本人認証ができず、不正利用を防げる**のです。

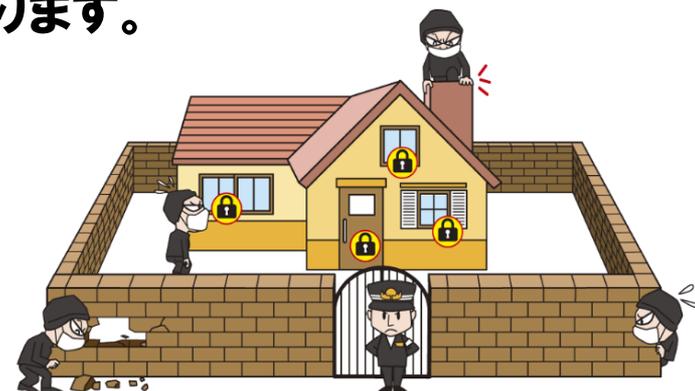
■脆弱性(ぜいじゃくせい)※9

脆弱性とは製品やサービスにある**セキュリティ上の弱点**のこと。

一言に脆弱性と言っても、「情報漏えいしてしまう脆弱性」や「製品が勝手に操作されてしまう脆弱性」など、様々な種類があります。

脆弱性が頻繁に見つかる製品は危険なの？

完全に脆弱性のない製品やサービスを開発することは非常に難しく、**どんな物にも脆弱性はつきもの**です。脆弱性が見つかってしまっても、迅速に対策されてアップデートされているのであれば、良いサポートが提供されているという見方もあります。



利用者にできることはあるの？

利用している製品は**速やかにアップデートして最新の状態にする**ことで脆弱性を対策しましょう。

■踏み台※10

攻撃者が標的を攻撃する際に他人の端末やアカウントを中継地点として使うことがあります。この中継地点のこと。

一般的には、高い所にある物を取る時に足場にする台のことを言いますね。

しかし、IT用語としての「踏み台」は少し違います。

標的を攻撃するための足場のことを「踏み台」と言います。



どんな端末やアカウントが踏み台にされるの？

脆弱性※9がある端末(PCやスマホ等)や、IDやパスワードが漏えいしてしまったサービスのアカウント等が踏み台にされてしまいます。

■ 踏み台※10

踏み台にされるとどうなるの？

あなたの端末(PCやスマホ)やアカウントが踏み台に使われてしまった場合を考えましょう。攻撃者はあなたの端末やアカウントから迷惑メールを送信したり、企業のシステムを攻撃したりします。

すると、攻撃を受けた企業や迷惑メールを受信した人はあなたが攻撃をしてきたと思うのです。

その結果、ある日突然あなたの所に、身に覚えのない嫌疑で警察がやって来る・・・なんてことになってしまうかもしれません。



踏み台にされないためには？

使っている端末やソフトウェア、アプリはアップデートすることで、最新状態を保ち、脆弱性※9をなくしましょう。

また、パスワードは使い回しをしない、長く複雑にする等でリスクを減らせます。



■ログイン通知機能※11

アカウントにログインされた時に、メールやSMS※2等で
利用者に教えてくれる機能のこと

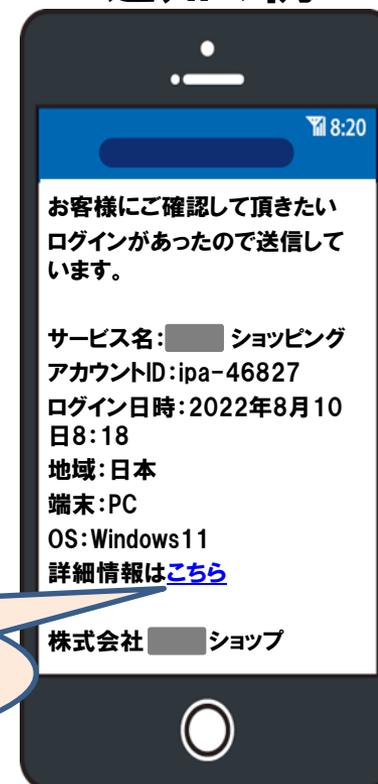
サービスによってはログインされた時、メールやSMSで通知してくれる機能があります。もしもそんなメールやSMSが届いたら記載されているログイン情報が身に覚えのある物かどうか確認しましょう。

もしも身に覚えのないログインだったら？

不正ログインされています。直ちにサービスの提供会社に相談しましょう。個人情報~~を盗まれたり~~、金銭被害~~が出てしまう~~かもしれません。

ログイン通知を装ったフィッシングもあるのでリンクは押さずに自分でサービスのウェブページにアクセスして確認！

～通知の例～



■ 公的機関の相談窓口※12

IPAでは、一般的な情報セキュリティ(主にウイルス※4や不正アクセス)に関する技術的な相談に対してアドバイスを提供する窓口を開設しています。

情報セキュリティ安心相談窓口

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

内容によってはIPAでは承れないご相談もありますが、他の機関が開設している窓口で対応できる場合もあります。

・他の機関が開設している窓口はこちら

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

詳細な資料のダウンロード

■情報セキュリティ10大脅威 2022

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/10threats2022.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%3DEA000000074

