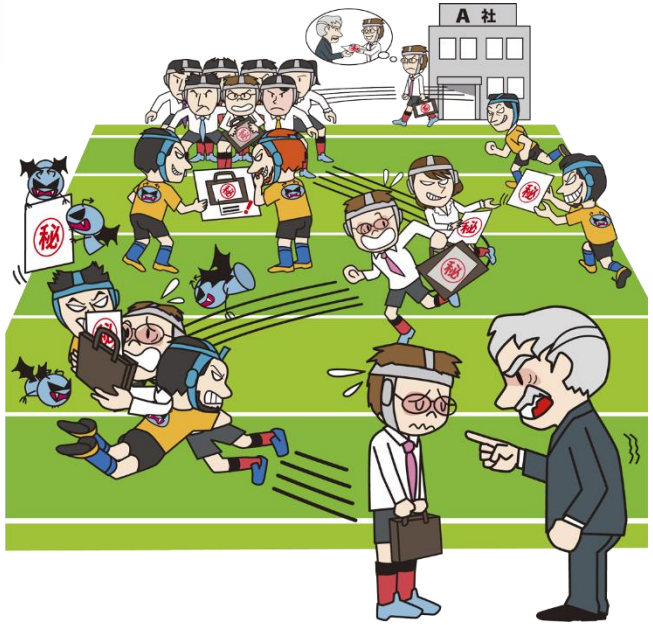
IPA Better Life with IT

情報セキュリティ10大脅威 2020 個人編

【一般利用者向け】
～インターネットトラブルを避けるために～



独立行政法人情報処理推進機構（IPA）
セキュリティセンター
2020年8月

本資料の位置づけ

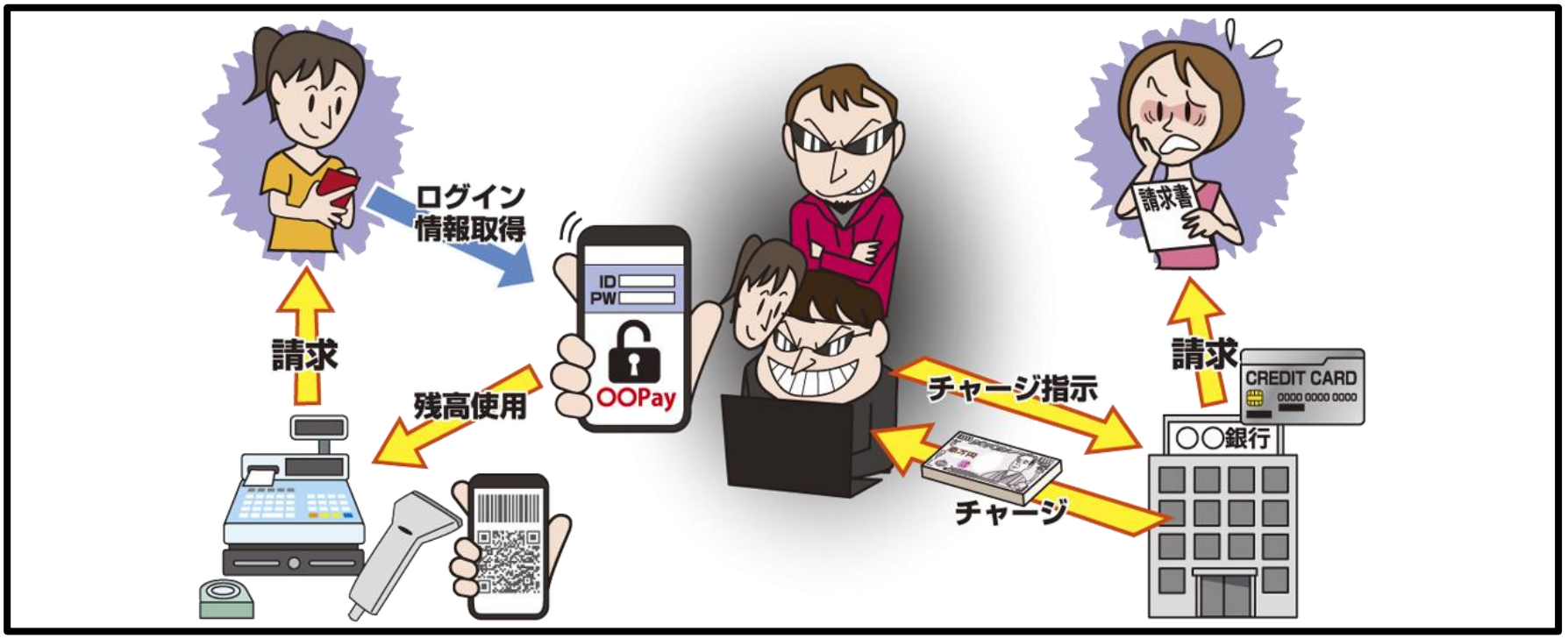
- IPAが公開している「情報セキュリティ10大脅威 2020 個人編」の中からポイントとなる箇所をよりわかりやすく解説
- 主に個人のパソコンやスマホでインターネットを利用する人の視点でインターネットトラブルを避けるための対策に着目
- 10大脅威からみえる日々のインターネット利用における注意点についてワンポイントアドバイス
- 本書の解説内で登場する「クレジットカード情報※1」、「SMS※2」のように黄色のマーカーと(※)が付いている用語については、後段「用語解説(補足解説)」のページで補足解説をしています。

情報セキュリティ10大脅威 2020 脅威ランキング

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

【1位】スマホ決済の不正利用

～スマホ決済サービス利用時は二要素認証等のセキュリティ機能を有効に～



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。

【1位】スマホ決済の不正利用

～スマホ決済サービス利用時は二要素認証等のセキュリティ機能を有効に～

● 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【2位】の項目（7ページ～9ページ）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。

【1位】スマホ決済の不正利用

～スマホ決済サービス利用時は二要素認証等のセキュリティ機能を有効に～

● 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
（簡単に推測されるようなパスワードは漏れる以前の問題）
・**二要素認証**※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★

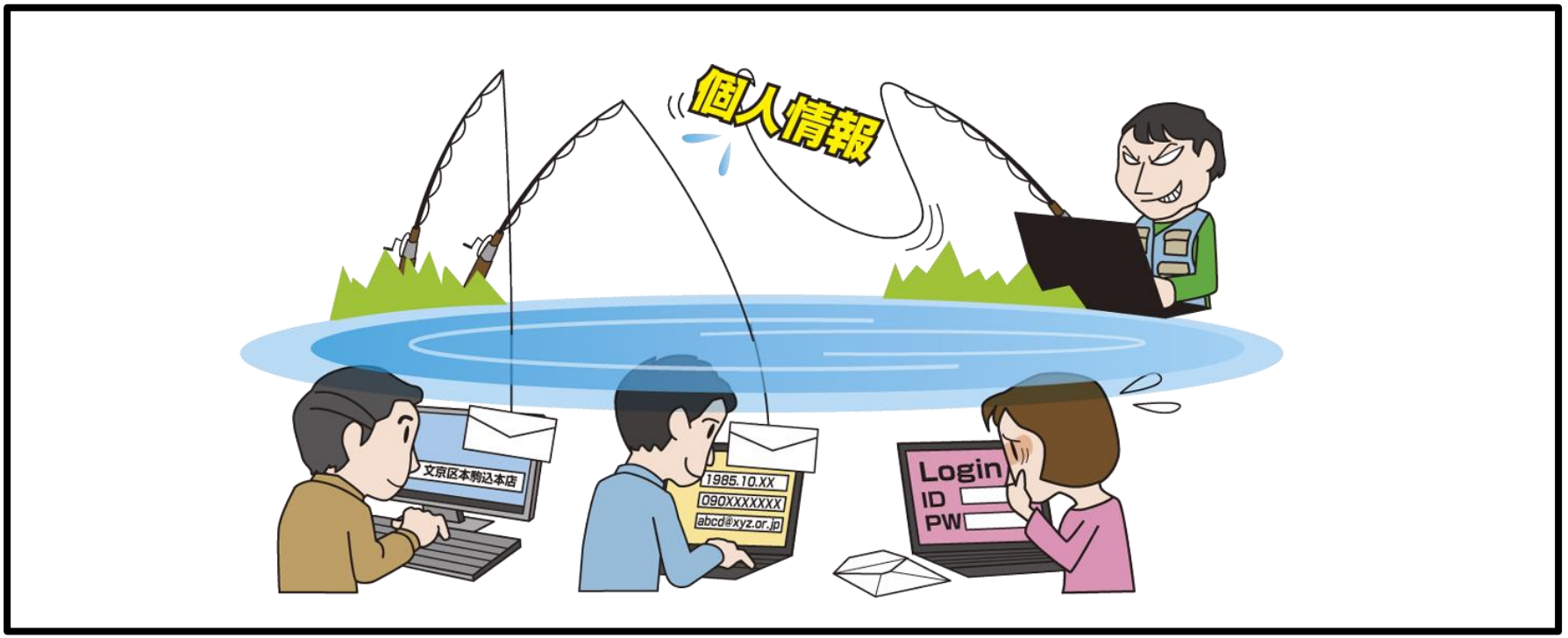
特に”パスワードの使いまわし”をしないことは大事です。

■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などを利用。

【2位】フィッシングによる個人情報の詐取

～フィッシングの件数は増加傾向、世界的なイベントに便乗したフィッシング詐欺にも注意～



銀行やカード会社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。

【2位】フィッシングによる個人情報の詐取

～フィッシングの件数は増加傾向、世界的なイベントに便乗したフィッシング詐欺にも注意～

● 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てきます。

・カード会社を装ったメールの例

いつもXXXXカードをご利用いただき、
ありがとうございます。
この度、お客様のアカウントに対し第三者によるアクセスを確認いたしました。
下記URLからログインいただき、任意のIDへの再変更をお願いいたします。

http://www.[redacted].com/～

偽のウェブサイトのURL

・宅配便業者を装ったSMSの例

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.[redacted].com/～

偽のウェブサイトのURL

【2位】フィッシングによる個人情報の詐取

～フィッシングの件数は増加傾向、世界的なイベントに便乗したフィッシング詐欺にも注意～

IPA

● 対策

【1位】の対策と同様、大事なのはフィッシングに騙されないことです。

★ワンポイントアドバイス★

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

・メールやSMS※2でウェブサイトに誘導してきたらまずは疑う

・誘導先でクレジットカード情報※1や口座番号などの 情報入力を求められたらもっと疑って、操作を中断する。

■疑ったあとは本物かどうかを確認

・信頼できる人に相談してみる。

・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。

※偽物かもしれないメールやSMS※2に記載された窓口に連絡するのは危険

・受信したメールやSMS※2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」とか「フィッシング」という情報が出てくるかも。

【3位】クレジットカード情報の不正利用

～ショッピングサイトでのクレジットカード情報の詐取被害が拡大～

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を盗まれて、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。

【3位】クレジットカード情報の不正利用

～ショッピングサイトでのクレジットカード情報の詐取被害が拡大～

● どうするとクレジットカード情報を盗まれるか？

最近では**クレジットカード情報**※1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。

■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**※1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【2位】の項目（7ページ～9ページ）で解説していますのでそちらをご確認ください。

【3位】クレジットカード情報の不正利用

～ショッピングサイトでのクレジットカード情報の詐取被害が拡大～

IPA

● 対策

情報を奪う常套手段であるフィッシングに騙されないようにしましょう。

★ワンポイントアドバイス★

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

・メールやSMS※2でウェブサイトに誘導されたらまずは疑う

・誘導先でクレジットカード情報※1や口座番号などの情報入力を求められたらもっと疑って、操作を中断する。

■疑ったあとは本物かどうかを確認

・信頼できる人に相談してみる。

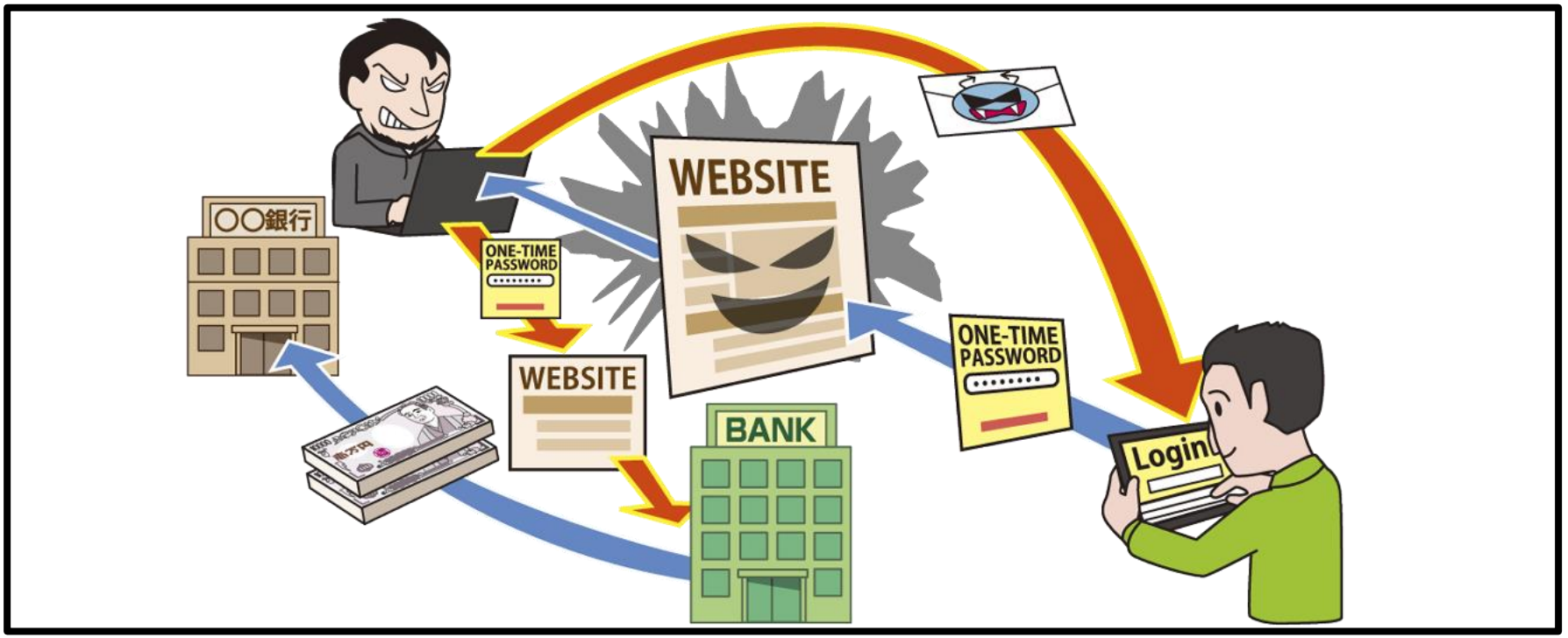
・サービスの正規の問い合わせ窓口に電話などで確認してみる。

※偽物かもしれないメールやSMS※2に記載された窓口に連絡するのは危険

・受信したメールやSMS※2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」とか「フィッシング」という情報が出てくるかも。

【4位】インターネットバンキングの不正利用

～フィッシングによる不正送金の被害が急増～



盗まれたIDやパスワードを使い、インターネットバンキングに不正ログインされることで自分の口座から不正送金されて金銭被害を受けます。IDやパスワードを盗む手口として、フィッシングやウイルス※4が使われます。

【4位】インターネットバンキングの不正利用

～フィッシングによる不正送金の被害が急増～

IPA

● 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【2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。

■ウイルス※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イルス※4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イルス※4に感染してしまう

【4位】インターネットバンキングの不正利用

～フィッシングによる不正送金の被害が急増～

IPA

● 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【2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★

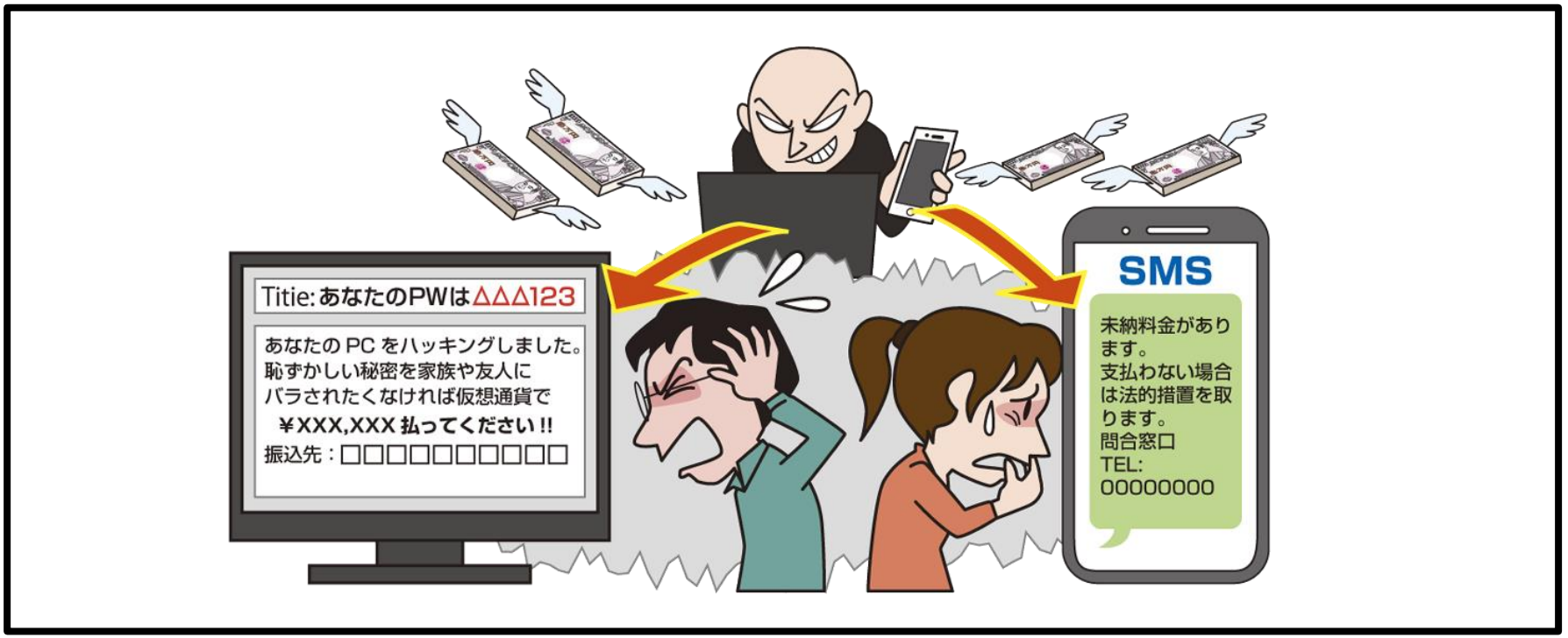
ワンタイムパスワード※6による二要素認証※7など、銀行が推奨する認証方式を利用しましょう。
（パスワードが盗まれても不正ログインされない対策を）

■その他の対策

・ワンタイムパスワード※6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※4に感染する場合がある”ことを知る。

【5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
～金銭を要求する脅迫・詐欺メールは無視を～



金銭を支払わせようと脅迫するメール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。その結果、騙されて相手の要求に屈してしまうことで金銭を奪われます。

【5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
～金銭を要求する脅迫・詐欺メールは無視を～

● 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」 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」 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）

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

【5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
～金銭を要求する脅迫・詐欺メールは無視を～

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

★ワンポイントアドバイス★

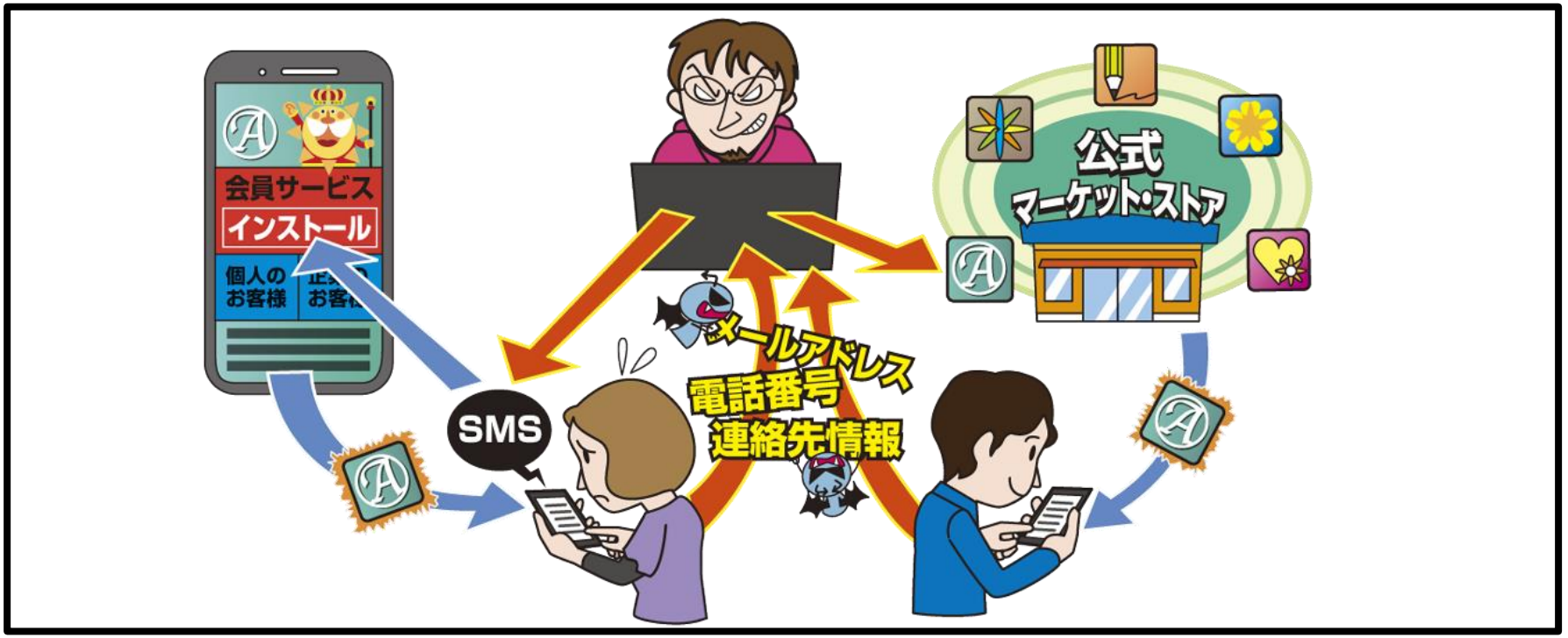
まずは冷静に
不安な時は**公的機関の相談窓口**※9へ相談

■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）

【6位】不正アプリによるスマートフォン利用者への被害

～インストールしているのは本当に正規のアプリ？～



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**※5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**SMS**※2の送信に使われたりします。

【6位】不正アプリによるスマートフォン利用者への被害

～インストールしているのは本当に正規のアプリ？～

● 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※5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※5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。

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※5を気づかずにインストールしてしまう。

【6位】不正アプリによるスマートフォン利用者への被害

～インストールしているのは本当に正規のアプリ？～

● 対策

不正アプリ※5の存在を知り、不正アプリ※5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

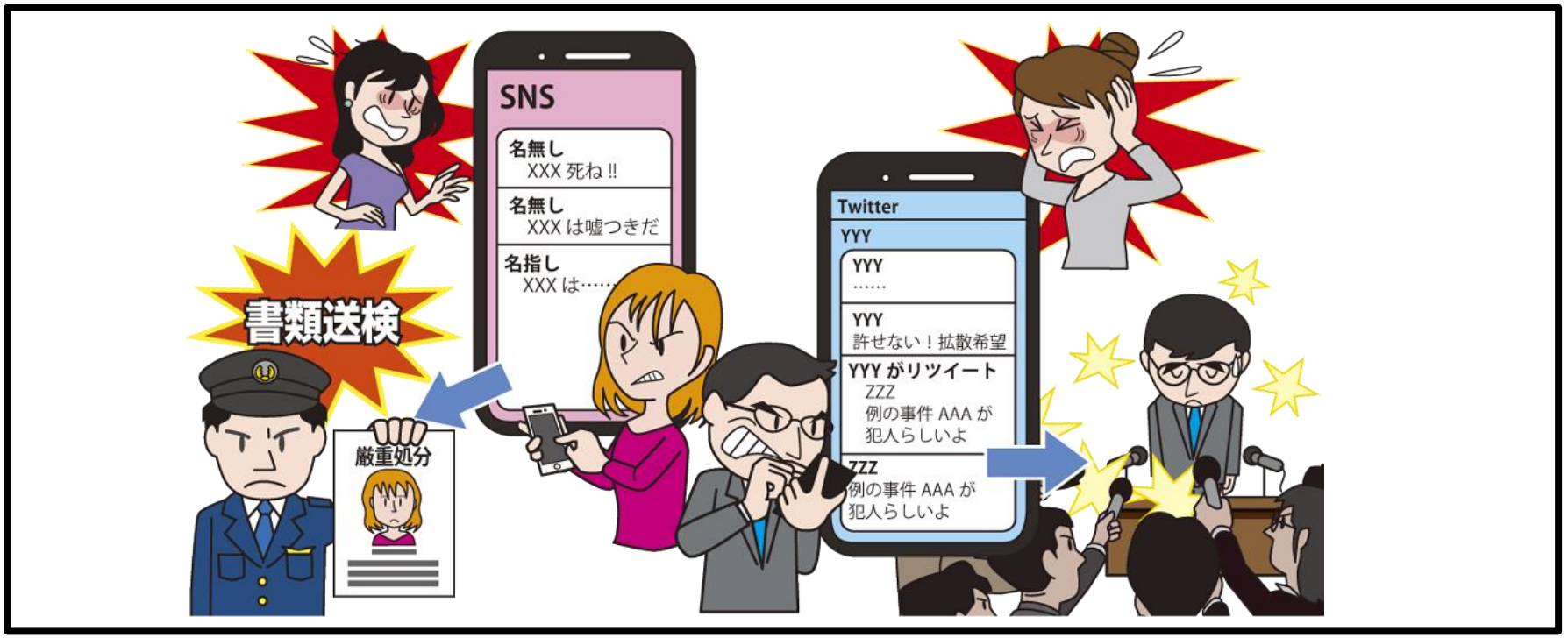
■確認ポイント

・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。

【7位】ネット上の誹謗・中傷・デマ

～安易な拡散により、他者も自身も不幸に～



SNS※3や掲示板などで他人を誹謗・中傷したり、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。

【7位】ネット上の誹謗・中傷・デマ

～安易な拡散により、他者も自身も不幸に～

● 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

【7位】ネット上の誹謗・中傷・デマ

～安易な拡散により、他者も自身も不幸に～

● 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★

大勢の目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上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。

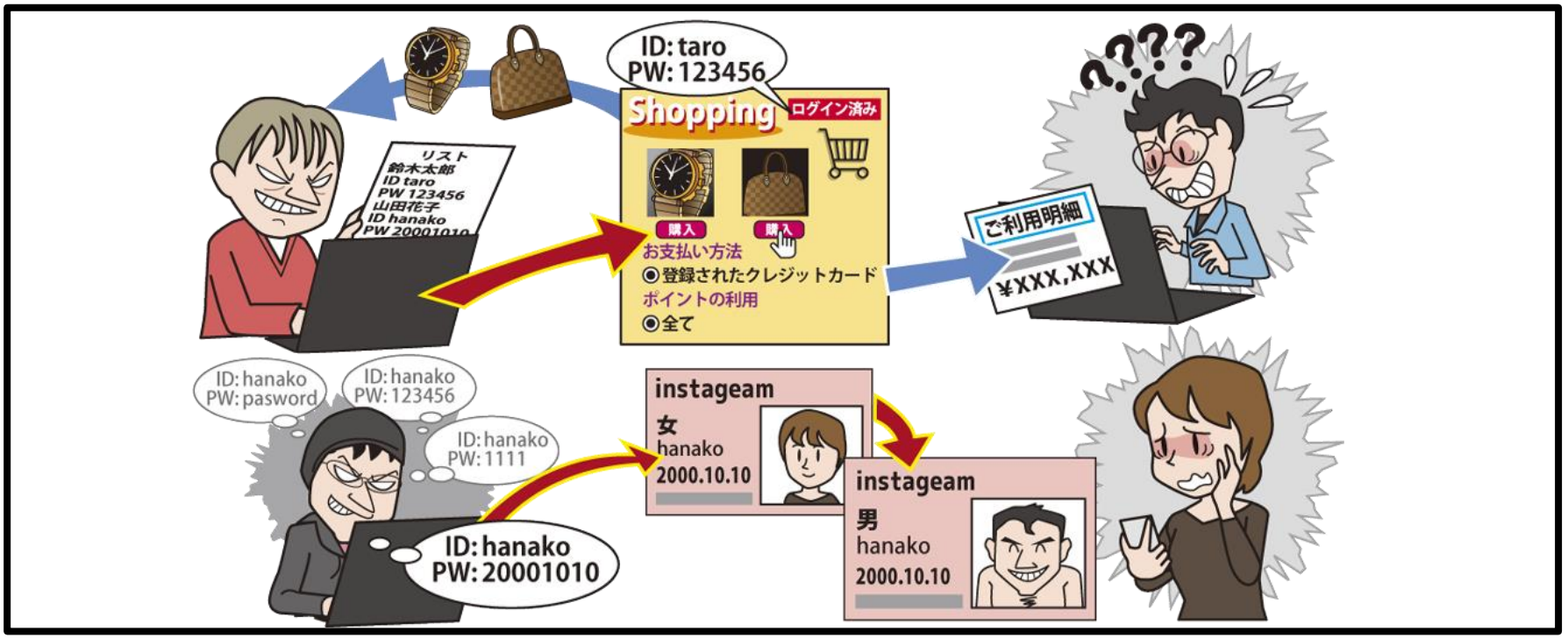
（**見ず知らずの人の言うことを鵜呑みにしない。**）

・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。

【8位】インターネット上のサービスへの不正ログイン

～パスワードリスト攻撃による不正ログインが横行～



世の中には【4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。

【8位】インターネット上のサービスへの不正ログイン

～パスワードリスト攻撃による不正ログインが横行～

● 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

【2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。

【8位】インターネット上のサービスへの不正ログイン

～パスワードリスト攻撃による不正ログインが横行～

● 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
（簡単に推測されるようなパスワードは漏れる以前の問題）

★ワンポイントアドバイス★

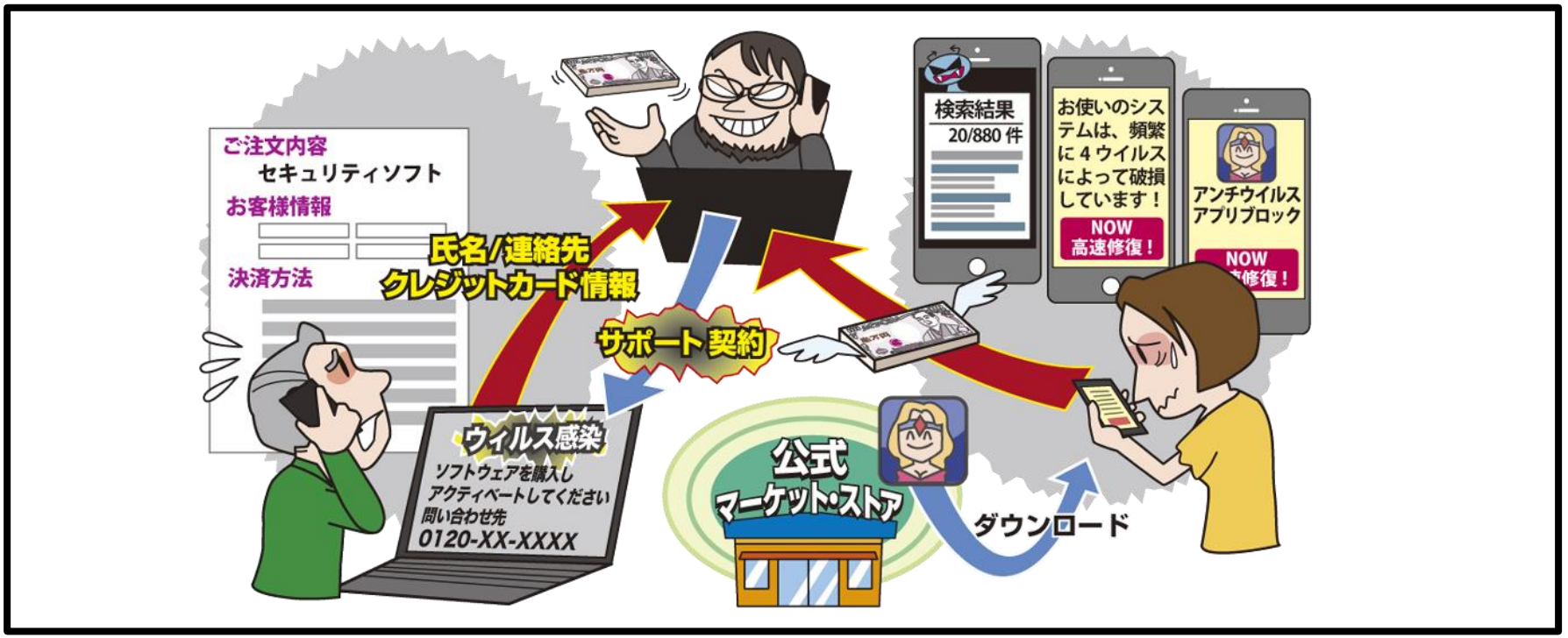
特に”パスワードの使いまわし”をしないことが大事です。

■その他の対策

・**ワンタイムパスワード**※6など**二要素認証**※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などを利用。

【9位】偽警告によるインターネット詐欺

～落ち着いて！あの手この手の騙しの警告画面～



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。その窓口に電話すると、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。

【9位】偽警告によるインターネット詐欺

～落ち着いて！あの手この手の騙しの警告画面～

● 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
  （偽物だと気づけても対応に困るケースも多い）
- **偽警告**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

など

【9位】偽警告によるインターネット詐欺

～落ち着いて！あの手この手の騙しの警告画面～

IPA

● 対策

お使いのセキュリティソフト等が出したものではない偽の警告は無視して構いません。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、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★

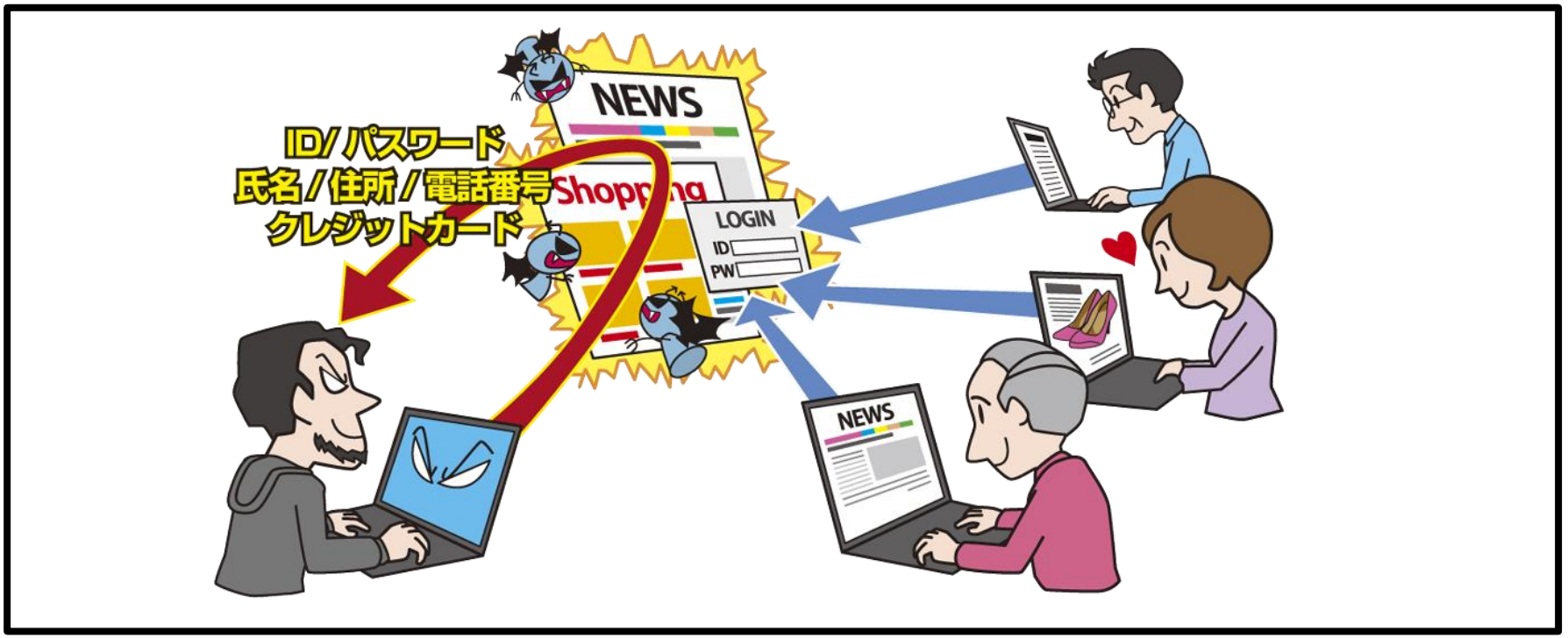
電話をかけさせようとしてきたら特に注意。
（偽警告以外にもワンクリック請求やその他の詐欺にも共通する常套手段です）

■その他の対策

- **偽警告**が閉じられないなど対応に困ったら**公的機関の相談窓口**※9に相談。
  ※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。

【10位】インターネット上のサービスからの個人情報の窃取

～会員サイトやショッピングサイトから情報流出するおそれ～



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。

【10位】インターネット上のサービスからの個人情報の窃取

～会員サイトやショッピングサイトから情報流出するおそれ～

● 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【8位】の項目（25ページ～27ページ）で解説していますのでそちらをご確認ください。

【10位】インターネット上のサービスからの個人情報の窃取

～会員サイトやショッピングサイトから情報流出するおそれ～

● 対策

サービス自体に脆弱性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）

対策のまとめ

1. 【フィッシングに騙されないようにする】
   送られてきたメールやSMS、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. 【スマホの不正アプリ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

対策のまとめ

3.【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

- 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てみる
- 不安な時は公的機関の相談窓口へ

4.【不適切な情報発信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
- 炎上したり問題になったりした時のリスクを意識する
- 情報を拡散するときはデマでないかを確認する

対策のまとめ

5.【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など二要素認証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

6.【パソコンのウイルス対策を実施する】

- 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

SMS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.[redacted].com/～

なにか荷物が届いたのかな？
記載されたページにアクセスしてみよう。

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.[redacted].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

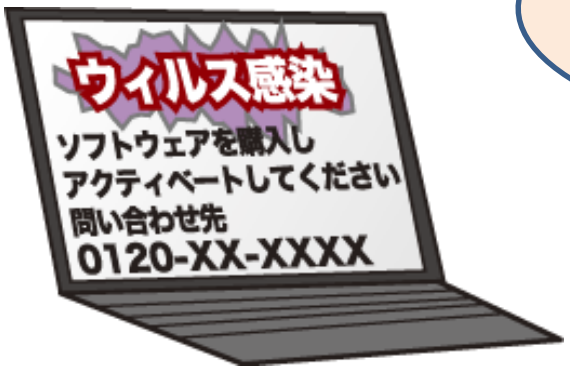
～脅迫内容が書かれた金銭を要求するメールがきた～

■安全な対応

【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。だ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。

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。

用語解説（補足解説）

■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を指します。

- 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

用語解説（補足解説）

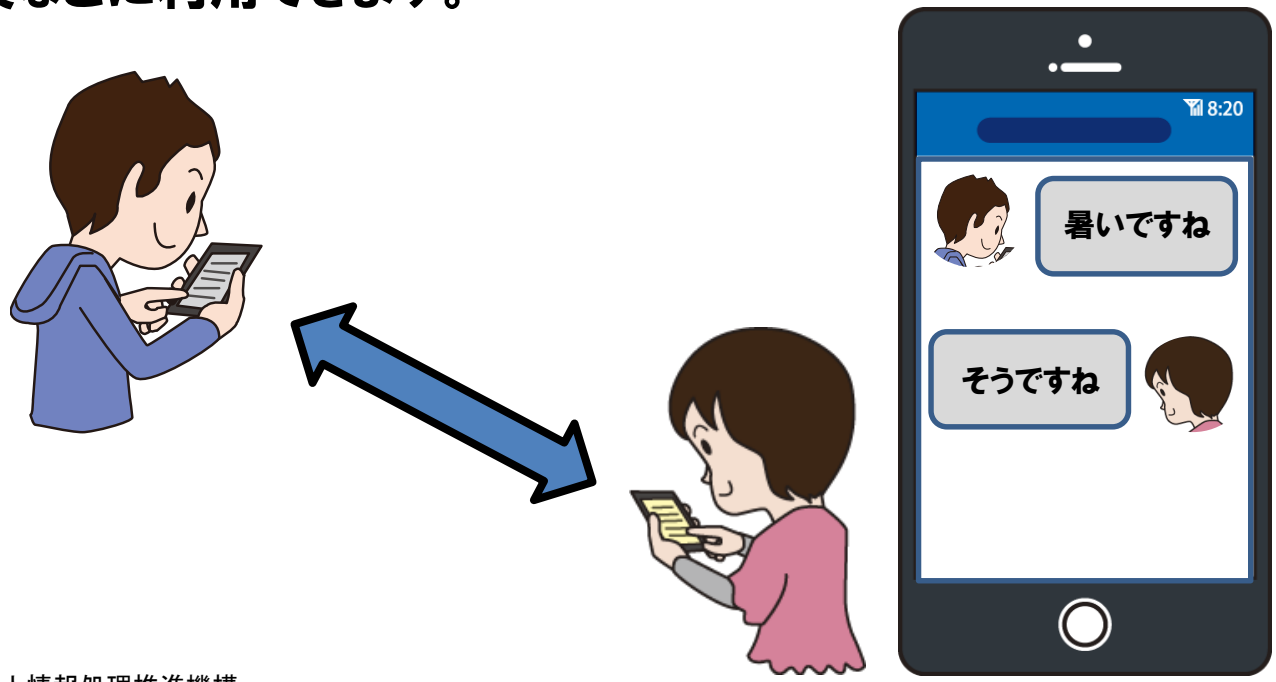
■SMS※2

SMS※2はショートメッセージサービス（Short Message Service）の略称です。

※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。



用語解説（補足解説）

■SNS※3

SNS※3はソーシャルネットワーキングサービス（Social Networking Service）の略称です。

※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　※厳密にはTwitter社としてはTwitterはSNSと定義していないという見解もあります

など

用語解説（補足解説）

■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を指します。

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※4と呼ぶようになりました。

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を指す用語で、厳密にはウイルス※4とマルウェアは別物です。

ただし、古くからウイルス※4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、マルウェアもウイルス※4と表現されている場合が多いです。

（最近の傾向では、悪い動きをするものの多くはマルウェアであり、厳密にはウイルス※4には分類されないものが多いです。）

用語解説（補足解説）

■不正アプリ※5

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ものですが、中には悪意のある人が作成した悪い動きをするアプリもあり、それを不正アプリ※5と呼びます。

パソコン上で悪い動きをするものとしてウイルス※4という用語がありますが、それと同じように、スマホの不正アプリ※5も悪い動きをするものということでスマホのウイルス※4と表現される場合もあります。

不正アプリ※5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）

用語解説（補足解説）

■ワンタイムパスワード※6

インターネット上のサービスなどにログインする際、パスワードが必要です。
パスワードの中でも、パスワードに短い有効期限を設け、一度使用すると
そのパスワードは無効にしてしまうことで、一度限り有効なパスワードとして
いるものがあります。
このようなパスワードをワンタイムパスワード※6と呼びます。

※二段階で認証を行う二段階認証のほかにも、二つの要素で認証を行う二要素認証という言葉もあり、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、余裕があればぜひ調べてみましょう。
（SMSでの二段階認証は、SMSが自分の電話番号に届くという性質上、二要素認証の要件を満たしています。）

用語解説（補足解説）

■二要素認証※7

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2つの要素を用いる認証を二要素認証※7と呼びます。

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※2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個目のパスワードは「記憶」、2個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二要素認証※7としています。

用語解説（補足解説）

■3Dセキュア※8

3Dセキュア※8はクレジットカードにおける本人認証サービスの名称です。

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。この場合、クレジットカードを持っていれば、クレジットカード名義人本人でなくとも決済ができますので、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、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※8です。

3Dセキュア※8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。

用語解説（補足解説）

■公的機関の相談窓口※9

IPAでは、一般的な情報セキュリティ（主にウイルスや不正アクセス）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解説しています。

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　2020

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/10threats2020.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%3DEA0000000074