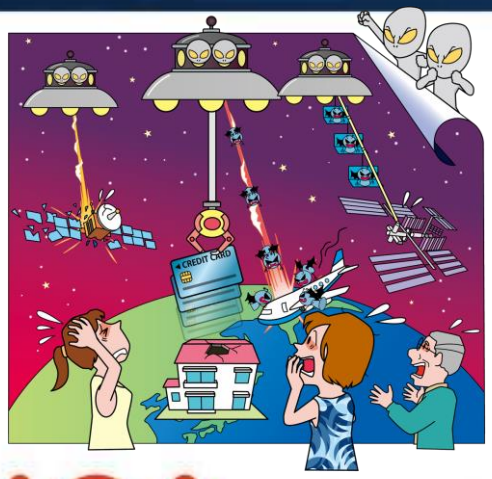
情報セキュリティ10大脅威　2025
個人編　ハンドブック

[一般利用者向け]



IPA Better Life with IT

QRコード

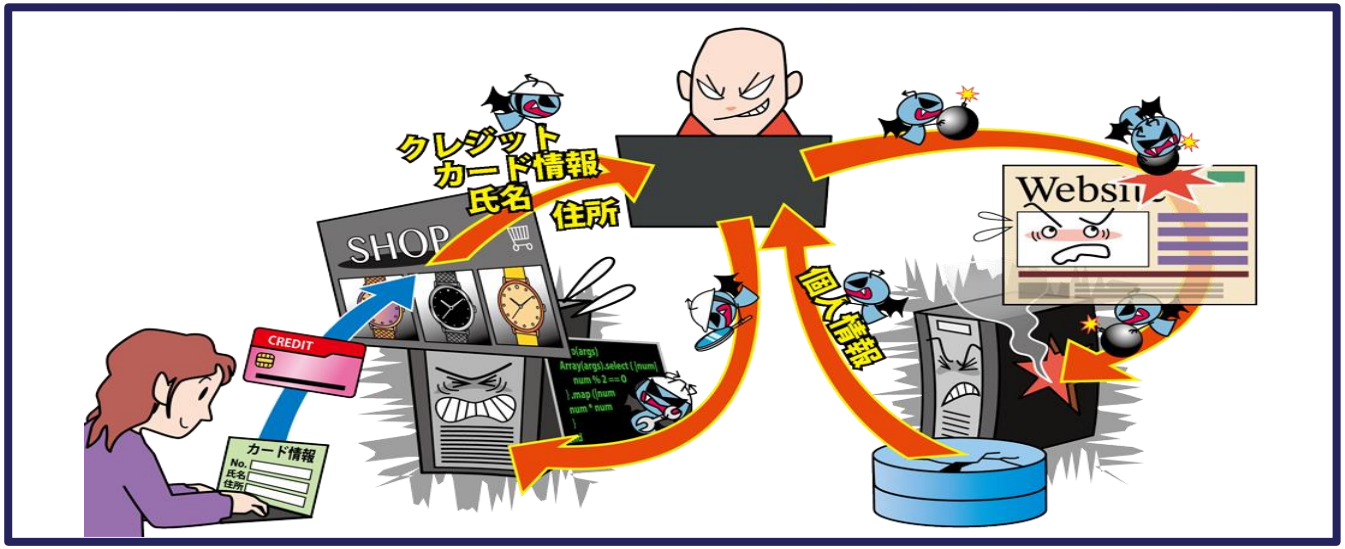
WebサイトのURL

https://www.ipa.go.jp/security/10threats/10threats2025.html

情報セキュリティ10大脅威 2025

「個人」向け脅威（五十音順）	初選出年	10大脅威での取り扱い
インターネット上のサービスからの個人情報の窃取	2016年	6年連続　9回目
インターネット上のサービスへの不正ログイン	2016年	10年連続10回目
クレジットカード情報の不正利用	2016年	10年連続10回目
スマホ決済の不正利用	2020年	6年連続　6回目
偽警告によるインターネット詐欺	2020年	6年連続　6回目
ネット上の誹謗・中傷・デマ	2016年	10年連続10回目
フィッシングによる個人情報等の詐取	2019年	7年連続　7回目
不正アプリによるスマートフォン利用者への被害	2016年	10年連続10回目
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	2019年	7年連続　7回目
ワンクリック請求等の不当請求による金銭被害	2016年	3年連続　5回目

● インターネット上のサービスからの個人情報の窃取



● どんな被害？

ショッピングサイト、転職支援サイト等に登録しておいた個人情報が盗まれる

● 被害に遭うとどうなるの？

- 窃取した情報でサービスへのログインを試され、パスワードを使いまわしていると、他のサービスでもログインされてしまい、さらに被害を生むことに
- 盗んだ個人情報がダークウェブで売買される
- 自分のメールアドレスに詐欺メールが飛んでくる

インターネット上のサービスからの個人情報の窃取

- 対策

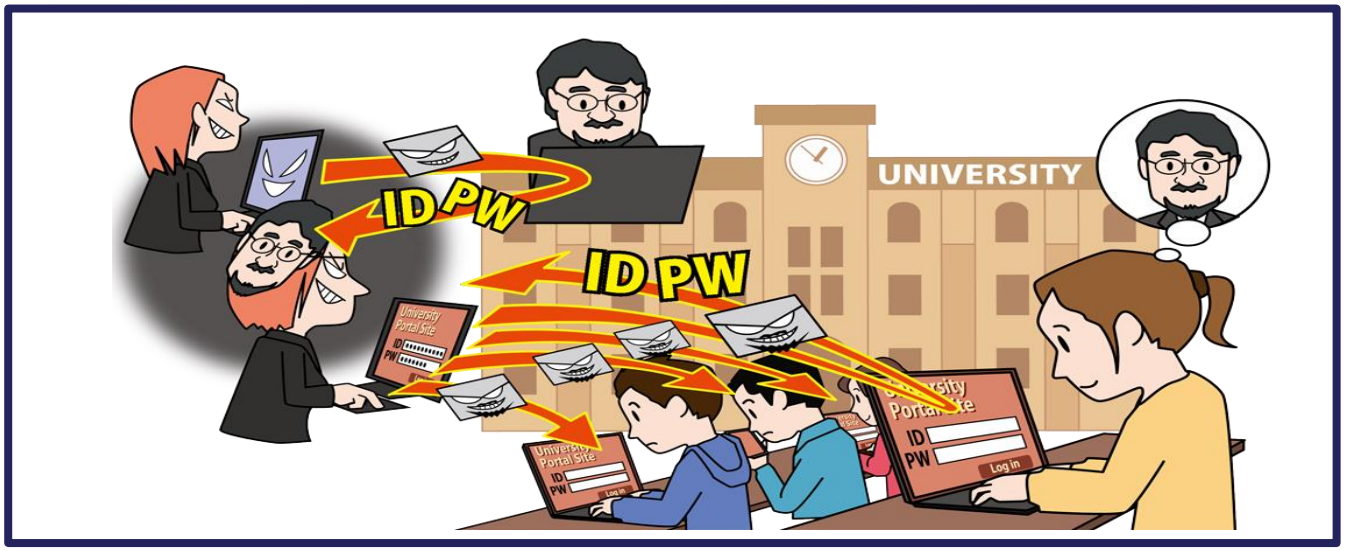
【予防】

- 利用していないサービスは退会する
- サービスへの登録時には必須項目以外の情報は登録しない
- ワンタイムパスワード、生体認証等を含めた多要素認証を利用する
- 認証情報を適切に運用する（★共通対策）

【早期検知】

- クレジットカード利用明細の定期的な確認
- ログインすると通知されるログインアラート機能の利用
- ログイン履歴の確認

● インターネット上のサービスへの不正ログイン



● どんな被害？

第三者にオンラインショッピング、SNS、電子書籍等のインターネットサービスにログインされる

● 被害に遭うとどうなるの？

- パスワードを勝手に変更され、本人はログインできなくなる
- さらに本人がログインできなくなったサービスで買い物をされ、金銭被害に遭う
- 本人になりすまし、フィッシングメールがばらまかれ、受信者に被害が拡大するおそれがある
- アカウントに登録されていた個人情報が盗まれる
- 盗まれた個人情報はダークウェブで売買され、悪用される

インターネット上のサービスへの不正ログイン

● 対策

【予防】

- 「情報セキュリティ対策の基本」の実施
- よくアクセスするWebサイトはブックマークに登録し、ブックマークからアクセスする
- セキュリティソフトでアクセスブロック機能を活用する
- 安易に添付ファイルの開封、メールやSMSのURLリンクのクリック/タップをしない（★共通対策 ）
- 認証情報を適切に運用する（詳細はこちら）
- 利用していないサービスは退会する
- ワンタイムパスワード、生体認証等を含めた多要素認証を利用する
- 利用頻度の低いサービスではクレジットカードは登録しない

【早期検知】

- ログインすると通知されるログインアラート機能の利用
- 利用しているサービスのログイン履歴を確認
- クレジットカードやポイント等の利用履歴を定期的に確認

インターネット上のサービスへの不正ログイン

● 対策＜基本のキ＞：適切にパスワードを設定する

- 推測されにくいパスワードにする
  - ① ID とパスワードを同じ文字列にしない
  - ② 数字、英大文字小文字等、複数の文字種を組み合わせる
  - ③ 生年月日や名前を使わない
  - ④ 規則的な配列にしない
  - ⑤ 単純な単語一語だけにしない

- パスワードを使い回さない

  複数のサービスでパスワードを使い回していると
  それら全てのサービスに不正ログインされるおそれ
  がある

NG例

- **簡単に推測される文字列**
  名前や生年月日にちなんだパスワード
- **キーボードの連続した文字列**
  ”1qaz2wsx”、”qwerty” 等
- **パスワードの使いまわし**
- **単純な文字列**
  ”abcdef”,”123456”,”password”
- **SNSで公開している情報**
  名前やニックネーム、生年月日などの組み合わせ

等

● クレジットカード情報の不正利用

● どんな被害？

フィッシングメール等に記載されたURLリンクをクリックし、偽のショッピングサイトとは気が付かずに、クレジットカード情報を入力し、そのクレジットカード情報が不正に利用される

● 被害に遭うとどうなるの？

- 盗まれたクレジットカード情報が使われ、金銭被害が発生する
- 盗まれたクレジットカード情報がダークウェブなどで売買される

クレジットカード情報の不正利用

● 対策

【予防】

- 「情報セキュリティ対策の基本」の実施
- クレジットカード会社が提供している本人認証（3Dセキュア）の利用
- 安易に添付ファイルの開封、メールやSMSのURLリンクのクリック/タップをしない（★共通対策_）
- 普段表示されない画面やポップアップが表示された場合、情報を入力しない
- プリペイドカード、デビットカード利用を検討する
- クレジットカードの利用限度額を抑える
- 利用頻度の低いサービスではクレジットカードは登録しない
- 利用していないクレジットカードは契約解除および物理的破棄を検討する

【早期検知】

- クレジットカードの利用履歴を定期的に確認
- サービス利用状況の通知機能を利用する

● スマホ決済の不正利用

● どんな被害？

キャッシュレス決済(スマホ決済)サービスに、事前に登録しておいたクレジットカード情報や銀行口座番号が第三者のなりすましによる不正取引で金銭被害が発生する

● 被害に遭うとどうなるの？

- 不正に入手したIDとパスワードでスマホ決済に不正ログインし、クレジットカード情報を窃取する
- 別の決済サービスに窃取したクレジットカード情報を登録してスマホ決済を不正利用する

★ P16 「フィッシングによる個人情報等の窃取」も併せて確認！

スマホ決済の不正利用

● 対策

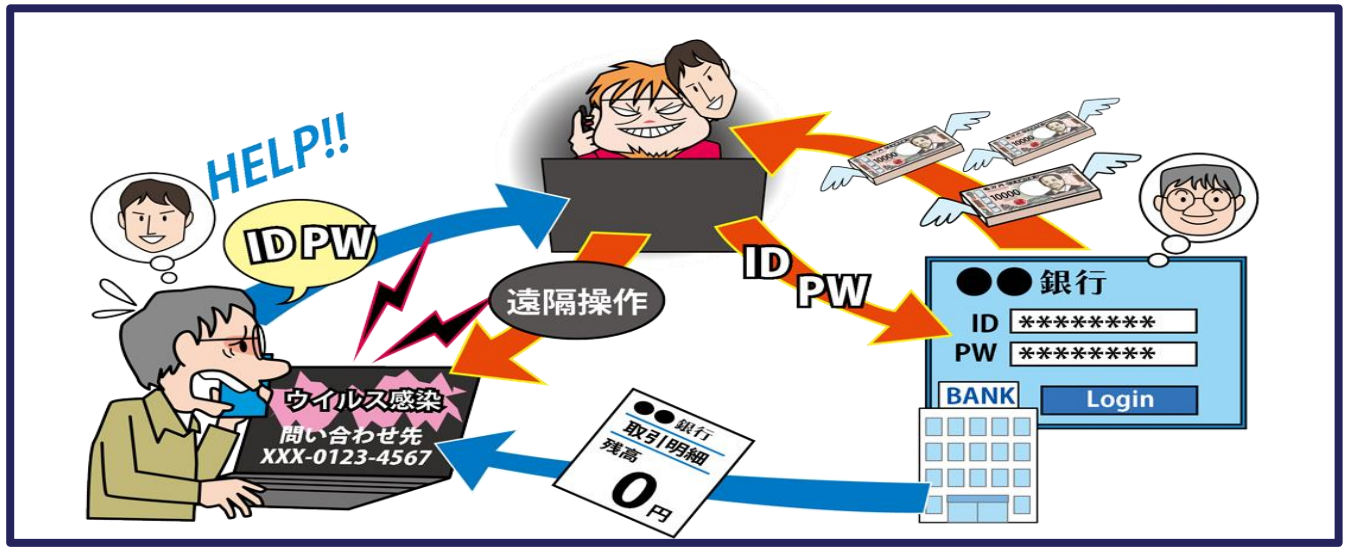
【予防】

- 「情報セキュリティ対策の基本」の実施
- 多要素認証の設定を有効にする
- 本人認証（3Dセキュア）の利用
- 認証情報を適切に運用する（詳細はこちら）
- フィッシングに注意する
- スマートフォンの紛失時の対策を行う

【早期検知】

- スマホ決済サービスの利用状況の通知機能の利用、利用履歴の定期的な確認
- スマホに紐づいている銀行口座の出金履歴やクレジットカードの利用明細の確認

● 偽警告によるインターネット詐欺



● どんな被害？

Webサイトの閲覧中に、突然、実在する企業のロゴが配置されたセキュリティの警告画面が表示される。これは偽の警告である。表示された画面の閉じ方や警告音の消し方がわからず、慌ててしまい、画面に表示される電話番号に連絡してしまうことで詐欺の発端となる。

● 被害に遭うとどうなるの？

- マルウェア駆除の名目で遠隔操作ソフトをインストールされ、PCやスマートフォンを遠隔操作
- サポート料金や修復費用の請求、振込時に金額を操作され想定外の被害金額の発生も
- 偽のサポート画面に入力した氏名、メールアドレス、クレカ情報等の個人情報の詐取

偽警告によるインターネット詐欺

● 対策

【予防】

- 「情報セキュリティ対策の基本」の実施
- セキュリティソフトを導入し、アクセスブロック機能を活用する
- 表示される警告を安易に信用しない（警告を無視して信頼する人に相談）
- 偽警告の画面の指示に従わない
- サポート料金を支払わない
- 偽警告が表示されたらブラウザを終了する

【早期検知】

- スマホ決済サービスの利用状況の通知機能の利用、利用履歴の定期的な確認
- スマホに紐づいている銀行口座の出金履歴やクレジットカードの利用明細の確認

実際の画像を多用した、手口の解説ページを見ることで、対策への理解がより深まります。
IPA　偽セキュリティ警告（サポート詐欺）対策特集ページ（IPA）
https://www.ipa.go.jp/security/anshin/measures/fakealert.html

偽警告によるインターネット詐欺

- 「偽警告」が表示されるのにはワケがある！？

偽警告が表示されるには必ずきっかけがあります。

- ブラウザに表示された広告をクリックしませんでしたか？
- 検索結果に表示された上位の結果をクリックしませんでしたか？
- 動画再生ボタンをクリックしませんでしたか？
- ブラウザに「許可しますか」と表示され、許可をクリックしませんでしたか？

このように直前の操作がきっかけとなり、偽警告は出現します。

- マルウェア感染の警告画面が出ても、電話を掛けない！
- 正規のセキュリティサービスの警告画面に電話番号は表示されません。

● ネット上の誹謗・中傷・デマ

● どんな被害？

誹謗、中傷、脅迫、犯罪予告、デマをSNS等のメッセージや画像を介して投稿し、それらが伝言ゲームの様にさらに拡散され、悪影響を及ぼす。また、拡散時に内容が改変されたり、別の第三者の情報に紐づけられることで、誹謗・中傷がさらに広がる恐れがある。

● 被害に遭うとどうなるの？

- 不特定多数から心無いメッセージが届く
- 社会的混乱
- 風評被害
- 精神的苦痛 等

訴えられ、裁判沙汰になることも

・投稿や拡散の責任を問われることを理解する
・匿名で投稿しても、権利侵害があった場合は被害者がプロバイダー等に発信者情報の開示を請求できる。
・発信者の特定は可能で、投稿や拡散の内容次第では、犯罪になりうるという認識を持ち、十分留意し発信する。

ネット上の誹謗・中傷・デマ

● 対策

【予防】

- 情報リテラシー、情報モラルの向上、法令遵守の意識向上（★共通対策 ）
- 情報の信頼性を確認する
- 誹謗・中傷や公序良俗に反する投稿や拡散をしない
- 投稿や拡散の責任を問われることを認識する

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発信しないという心構えが大事

Why do it ?

- 日頃の**不満やストレスの捌け口**
- 自己承認欲求(**関心、注目を集めたい**)
- 炎上や訴訟等**リスクを認識できていない**
- **匿名**だから自分の投稿だと特定されないと**誤解**している
- 情報が**デマである可能性**を理解できていない

  ※見ず知らずの人が匿名で書いていることも、インターネット上の情報は何故か本当のことであると考えがち
- 拡散すれば人の役に立つと**親切心が裏目に**（災害対策情報をデマと分からず拡散）

● フィッシングによる個人情報等の詐取

● どんな被害？

実在の企業、公的機関、金融機関、ショッピングサイトを騙った偽のウェブサイトのURLが記載されたメールやSMSが送信されてくる。一見して偽だと見分けがつかない場合もある。URLリンクをクリックし情報を入力してしまうと、入力した情報が窃取される

● 被害に遭うとどうなるの？

- サービスの認証情報を入力した場合、不正ログインされ、不正送金、物品等購入により金銭被害に遭う
- 個人情報を入力した場合、個人情報が窃取され、窃取された情報がダークウェブで売買される

フィッシングによる個人情報等の詐取

● 対策

【予防】

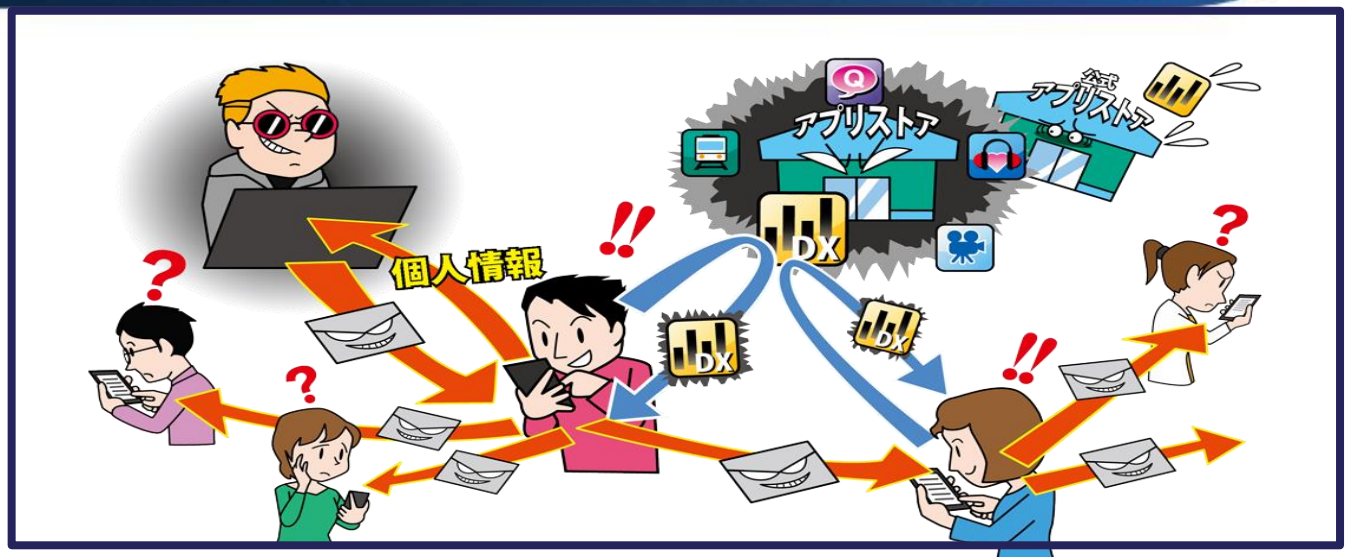
- 「情報セキュリティ対策の基本」の実施
- 突然届いた身に覚えのないメールやSMSは基本的に無視し、削除する
- 安易に添付ファイルの開封、メールやSMSのURLリンクのクリック/タップ、QRコードにアクセスしない
- 利用しているサービスの多要素認証の設定を有効にする
- 迷惑メールフィルターを利用する
- 危険なWebサイトのアクセスをブロックする

普段、他人に教えない情報の入力を求められたら要注意！

【早期検知】 被害に遭っていないかを確認することが大事

- ログインすると通知されるログインアラート機能の利用
- クレジットカードの利用明細やインターネットバンキング等の利用状況をこまめに確認

● 不正アプリによるスマートフォン利用者への被害



● どんな被害？

興味を引く内容が記載されたメールやSMS内のURLリンクをタップさせ、不正アプリをインストールさせる。SNSでダウンロードサイトに誘導する手口も確認されている。

● 被害に遭うとどうなるの？

- スマホに保存されている情報を窃取される
  - 認証情報を窃取された場合、キャリア決済等を悪用され金銭被害やオンラインサービス等への不正アクセスにもつながる
  - 連絡先情報が窃取された場合、連絡先宛に不正なメール、SMSがばらまかれる
- スマホを不正操作される
- DDoS攻撃の踏み台に悪用される

不正アプリによるスマートフォン利用者への被害

● 対策

【予防】

- 「情報セキュリティ対策の基本」の実施

鉄則 アプリは公式マーケットから入手する
(Androidは「Google Play」、iPhoneは「App Store」)

- アプリインストール時のアクセス権限の確認
- アプリインストールに関する設定に注意する
- 不用なアプリをインストールしない
- インストールされているアプリを確認する
- アプリ更新時に更新内容を確認する

Why do it ?

なぜ、不正アプリをインストールしてしまうのか

パターン1： 実在の企業を名乗っていても安易に信じるのはNG
メールやSMSなどで不正アプリを配布しているサイトへ誘導され、インストールしてしまう

パターン2： 公式マーケットの全てのアプリが安全とは限らない、アプリの評判も確認
公式マーケットに紛れ込んでいる不正アプリと気づかずにインストールしてしまう

●メールや SMS 等を使った脅迫・詐欺の手口による金銭要求

● どんな被害？

メールやSMS等の非対面のコミュニケーションを用い、公的機関や出会いのきっかけを装い、相手を脅したり、信用させ、金銭を詐取する。具体的にはロマンス詐欺/投資詐欺、セクストーション等がある。

● 被害に遭うとどうなるの？

- PCをハッキングした、示談の和解金が必要、アダルトサイトの未納料金がある、至急対応が必要等とメールやSMS等で不安をあおり、冷静さを失わせ、金銭要求に応じてしまう
- SNSで親交を深め、恋愛感情を逆手に、投資詐欺をしかける
- SMS等での性的なやりとりを経て、不正アプリのインストールに誘導され、スマホに保存されている連絡先宛に性的な動画をばらなくと脅される

メールや SMS 等を使った脅迫・詐欺の手口による金銭要求

● 対策

【予防】

- 冷静になる
- 「情報セキュリティ対策の基本」の実施
- 受信した脅迫、金銭要求、唐突、不自然なメールは無視する
- 利用しているサービスのワンタイムパスワード、生体認証等の多要素認証を利用する
- メールに記載されている電話番号に絶対電話しない
- 信じない、疑う、公的機関や信頼できる人に相談する
- 受信したメッセージからキーワードをインターネット検索してみる

巧妙な手口の数々

パターン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」「訴えられている」等と不安を煽る

パターン2： 信じ込ませる

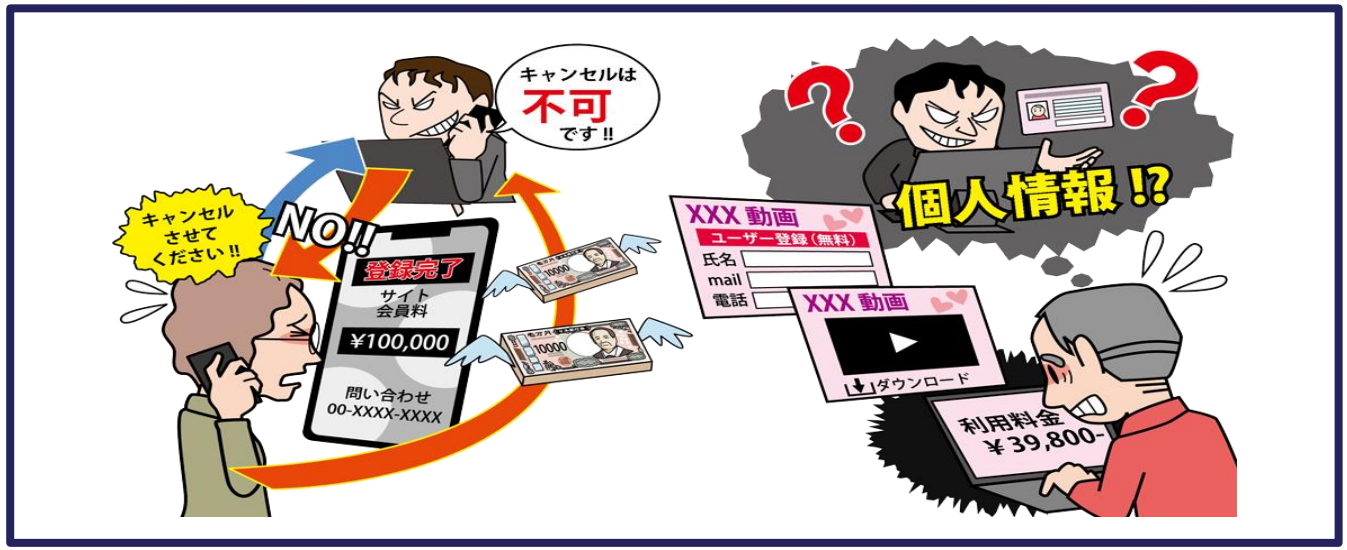
社会的信用の高い組織を騙り、事態の深刻さ、緊急性を訴求し信じ込ませる

有名人や異性を装い交際を持ち掛け、親密になったところで投資など様々な名目で金銭を要求

パターン2： 相談しにくい

「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」等と脅し、金銭を要求

● ワンクリック請求等の不当請求による金銭被害



● どんな被害？

Webサイト閲覧中に、有料サービスの会員登録の完了画面や利用料の請求画面が突然表示され、金銭を請求され、不安と焦りをあおる。

● 被害に遭うとどうなるの？

- 料金請求等の画面を自力で閉じることができず、不安なため助けを求めて、画面に表示された番号に電話してしまう
- 電話すると(相手に電話番号が知られ)、相手の要求に応じ、不当請求を支払ってしまう
- SMS等での性的なやりとりを経て、不正アプリのインストールに誘導され、スマホに保存されている連絡先宛に性的な動画をばらなくと脅される

ワンクリック請求等の不当請求による金銭被害

● 対策

【予防】

- 「情報セキュリティ対策の基本」の実施
- 情報リテラシー、情報モラルを向上させる（★共通対策　）

- 不当な請求を安易に信用しない
- 不当な請求には応じない、連絡しない
- 請求画面が表示されたらブラウザを終了する
- 安易に添付ファイルの開封、メールやSMSのURLリンクのクリック/タップをしない
- セキュリティソフトを導入し、アクセスブロックを有効にすることで危険のウェブサイトのアクセスをブロックする

身近に相談できる人がいない場合は、公的機関の相談窓口(P26)に相談するのも一考です。
IPAではワンクリック不当請求の手口を解説したページを公開しています。
https://www.ipa.go.jp/security/anshin/attention/2022/mgdayori20220706.html

「情報セキュリティ対策の基本」は必ず実施！

・トラブルは、インターネットにアクセスし、ショッピング、SNS等サービスを利用することで発生する。

・トラブルの手口、糸口は共通点が多く、「情報セキュリティ対策の基本」はトラブルの発生抑止に共通的に有効

糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消して脆弱性を悪用した攻撃によるリスクを低減する
マルウェアに感染	セキュリティソフトの利用	攻撃を検知してブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取による情報漏えい等のリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導(罠にはめる)	脅威・手口を知る	手口から重要視するべき対策を理解する

個人向け「共通対策」

・10大脅威にランクインしているほぼ全ての脅威に有効

・日常的にこれら対策を実践することで、インターネットやスマートフォンの利用におけるリスクは一定程度低減される

・P2からP23の各脅威の対策と併せて実施することが重要

1. IDとパスワード(認証情報)を適切に運用する
2. 情報リテラシー、情報モラルを向上させる
3. 安易に添付ファイルの開封、メールやSMSのURLリンクのクリック/タップをしない
4. 適切な報告・連絡・相談をする
5. PC,ネットワーク機器に適切なセキュリティ対策を実施する
6. 適切なバックアップを運用する

情報セキュリティ安心相談窓口

IPAが国民に対し、一般的な情報セキュリティに関する技術的な相談に対しアドバイスを提供し、被害に遭わないための解説コンテンツを公開

■ 安心相談窓口だより

寄せられた相談内容を基に、手口や対策、対処等を図解

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

■ 手口検証動画シリーズ

寄せられた相談事例の手口を、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

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

■ 他の機関が開設している窓口等

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