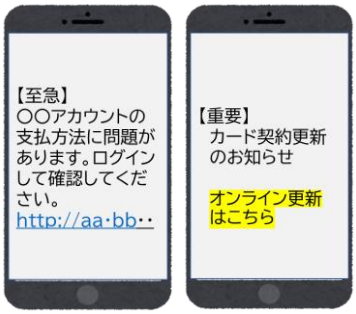
メールや広告を「ついクリックしたら・・・」「欲しかったあの商品が安くて急いで注文したけれど・・・」などのスマホトラブルを回避するためのポイントをまとめました。
トラブルに遭わないために「手口」を知ることが大切です。

## 1、フィッシング詐欺

2024 年度 クレジットカード不正被害額
555 億円（日本クレジット協会）

企業をよそおったメール・SMS や偽の広告から誘導し
クレジットカード情報やログイン情報、口座情報などを抜き取って悪用しようとする詐欺の手口。

| どこから？ | 例えば、どんな内容？ | もし、クリックや連絡してしまったらどうなる？ |
|---|---|---|
| 金融機関<br>証券会社<br>カード会社<br>宅配会社<br>通販サイト<br>Instagram<br>X<br>警告メッセージ |  <br>別のサイト（偽）への誘導<br>「ウイルスに感染」 | ・**記載されたURL（https://・・・）へのアクセス、偽アプリのインストールを誘導される**<br>①クレジットカード情報やパスワード、住所等の入力を求められる⇒個人情報を盗まれ不正被害<br>②アカウント情報の入力を求められる⇒アカウントを乗っ取られ、お金を奪われる、勝手に買い物をされる<br>**・代金を支払っても商品が届かない、偽物が届く**<br>**・投資詐欺やロマンス詐欺に誘導される**<br>**・問題解決をうたって金銭を要求される** |

ポイント

**フィッシング詐欺に騙されないために**

- ❖ URL や添付ファイルを不用意に開かない！
- ❖ 「確認するにはここをクリック」などと記載されたリンクにアクセスすると、偽サイト画面に遷移しログインを誘導されます。送信元メールアドレスのドメイン、および誘導先の Web サイト URL が、正しいドメイン、URL かどうかか必ず確認しましょう。
- ❖ 商品を注文したばかりの時や、急いでいる時に被害に遭いやすいので要注意！

個人情報やログイン情報を入力してしまったら？
- ● すぐに銀行やクレジットカード会社に連絡
- ● 同じパスワードを使っているサイトも含めパスワードを変更
- ● サイトにクレジットカード情報を登録している場合は一度その情報を削除

偽サイトに誘導されないために
①公式アプリやサイトをお気に入りやブックマーク登録
②そのアプリやブックマークからアクセスする

## 2.SNS 型投資詐欺（ロマンス投資詐欺、FX 取引、暗号資産）

2024 年 10,237 件
被害額 1,286 億円（警察庁）

投資に関するメッセージのやりとりを重ねて被害者を信用させ、
「投資金」や「手数料」などの名目で、ネットバンキングなどの手段により金銭等を振り込ませる手口。


SNS、Web検索、マッチングアプリ、DMで直接勧誘など入り口はいろいろ。
⇒LINEの「友達登録」
⇒電話、Zoomなどで投資方法、オンラインセミナーへの誘導、サポート等の契約など
⇒ネットバンキングの口座開設、海外取引所（偽？）への入金、借金
⇒利益が出る（と思いこませる。見せられた口座自体が偽物かも）
⇒得た利益を出金しようとすると、引き出せない、連絡が取れない

裏面へ！

「簡単に稼げる」「必ず儲かる」など、「あなたに届く魅力的な」広告には要注意！

ポイント

**SNS型投資詐欺に騙されないために**

- ❖ お金は個人名義の口座には絶対に振り込まない、借金しない
- ❖ 「広告⇒個人のアカウントLINE」の流れで契約はしない
- ❖ SNS型副業トラブルも同じような手口です。十分注意しましょう。

金融庁に登録のある
金融商品取引業者、
暗号資産交換業者
以外には預けない

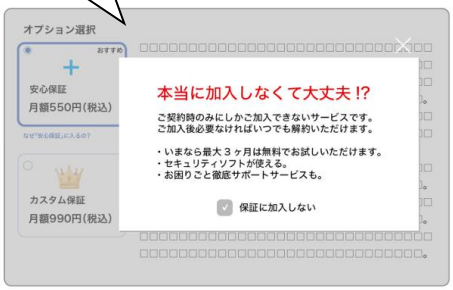
## 2、ダークパターン

年間被害額は1兆7,000億円を超える試算
（一人当たりおよそ33,000円）

スマートフォンのアプリや大手通販サイトなどで
消費者が気付かない間に不利な判断・意思決定をしてしまうよう誘導する手口などを指します。

① **行為の強制**（必須であると偽り会員登録させるなど）
② **インターフェース干渉**（虚偽の高値に対して割引した値段を表示するなど）
③ **執拗な繰り返し**（通知や位置追跡機能を有効にするようにしつこく要求するなど）
④ **妨害**（サービス登録の容易さに比べて、解約を困難にするなど）
⑤ **こっそり**（消費者の明確な同意を得ずにトライアル期間後などに契約を自動更新するなど）
⑥ **社会的証明**（誤解を招く、または虚偽である「お客様の声」を掲載するなど）
⑦ **緊急性**（割引期間の終了をカウントダウンタイマーによって表示するなど）

①の例




ダークパターン事例イラスト集（「いわゆる「ダークパターン」に関する取引の実態調査」（2025年3月 消費者庁新未来創造戦略本部国際消費者政策研究センター）より
https://www.caa.go.jp/policies/future/icprc/research_010/assets/caa_futurer101_0407_03.pdf

②の例


図5 不当参照価格の事例
（オ(ウ)隠れ定期購入/強制的継続、
キ(イ)カウントダウンタイマー/期間限定にも該当）

⑥の例


図13 お客様の声の事例②
）隠された情報、イ(イ)偽りの階層表示にも該当）

ポイント

**ダークパターンに騙されないために**

- ❖ ダークパターンの手口を知ろう！
- ❖ 「一呼吸置く」→ダークパターンは「人がついやってしまうこと」を利用しています。この感情に左右されないためには落ち着いて考えることが大切です。
- ❖ 取引条件（購入回数、期間、金額、解約ルールなど）を確認し、広告や最終確認画面のスクリーンショットを残しましょう。

**AIにより、偽メールや偽ショッピングサイト、偽広告、偽動画がさらに巧妙になっています。
手口を知り、「慌てず」「焦らず」「すぐに飛びつかず」、スマホを活用しましょう！
トラブルに遭ってしまったとき、困った時は消費者ホットライン「188（いやや）」に相談しましょう。**

作成・問合せ先：NPO法人 埼玉消費者被害をなくす会
048-844-8972（月・火・金 10-15時）