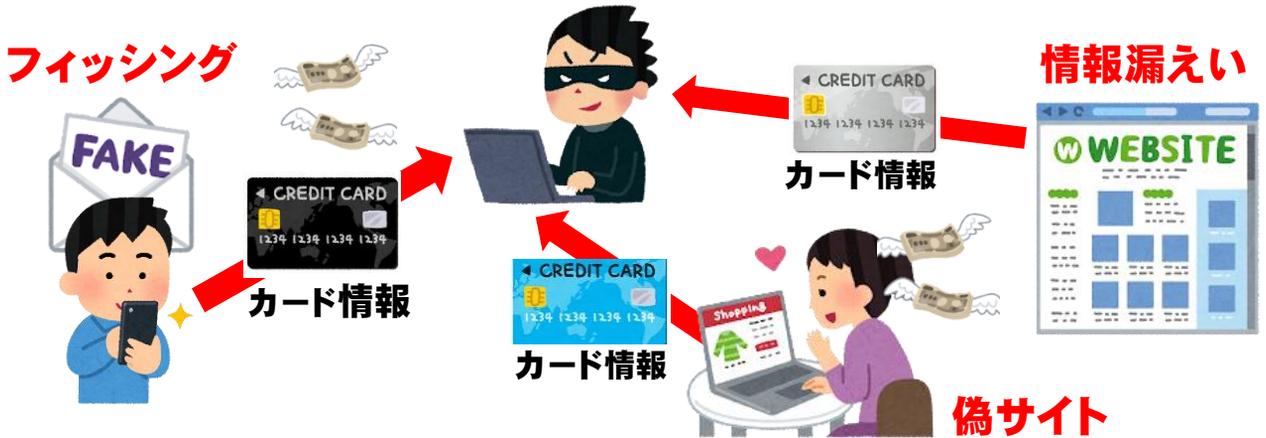




クレジットカード情報が狙われている!



不正利用の手口

- ・ フィッシング
メール等であらかじめ用意した偽サイトに誘導し、カード情報を入力させる
- ・ 改ざんされたウェブサイト
正規サイトの脆弱性を悪用し、偽の決済画面を表示させてカード情報を入力させる
- ・ ウイルス感染
ウイルスファイルをメールに添付して送信し、ファイルを開かせることでウイルスに感染させ、利用者がカード情報を入力すると、その情報が攻撃者に送信される
- ・ 不正アクセス
ショッピングサイトなどに第三者のアカウントで不正アクセスし、決済サービスに紐付けられているカード情報を悪用する
- ・ 漏洩した情報の悪用
企業等から漏えいした情報を悪用する

被害防止の対策

- ・ メールや閲覧ウェブサイトの十分な確認
添付ファイルやURLを安易に開かない
カード情報を安易にウェブサイトに入力、保存しない
- ・ 不正アクセスへの対策
サービスごとに異なるパスワードを設定し、二段階（二要素）認証を設定する
- ・ 本人認証サービスの利用
カード会社が提供している本人認証サービス（3Dセキュア等）を利用する
- ・ 被害の早期発見
利用明細をこまめに確認する（カード会社ごとの確認方法を知っておく）
- ・ 被害を確認した場合の対応
該当サービスのコールセンターへの連絡を行う（補償の範囲、期間を知っておく）
クレジットカードの再発行の手続きを行う