ショートメッセージ（SMS）を利用した フィッシングにご注意ください

「フィッシング」という言葉を知っていますか？
銀行やクレジットカード会社など、実在の**金融機関等を騙って偽のメール等を送信**し、**偽のサイトへと誘導**してIDやパスワード、銀行口座等の情報を盗み取る手口のことです。
金融機関以外にも**宅配便等を騙る手口やSMSを使う手口**もあるため、注意が必要です。

偽のSMSから被害に遭う流れ

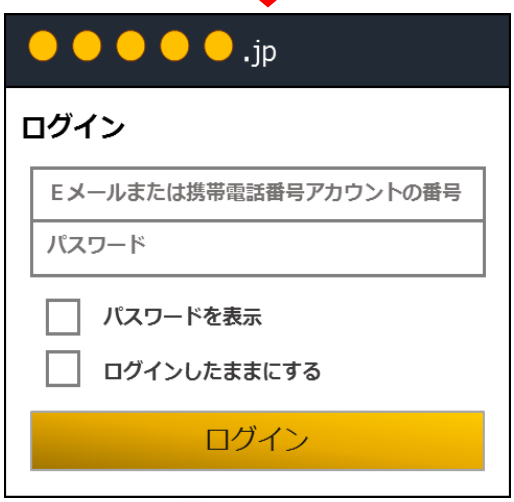
金融機関を騙ったSMS

お客様の○○銀行口座がセキュリティ強化のため、一時停止しております。再開手続きをお願いします。
http://●●●●●●.org

偽のSMS
↓
URLにアクセス
↓
偽サイトに誘導
↓
ログイン情報入力
↓
入力情報は犯人へ

通販サイトを騙ったSMS

お客さま決済に異常ログインの可能性があります。
ウェブページで検証お願いします。
https://account.●●●●●.xyz



不正アクセス被害

銀行口座から不正送金・通販サービスの不正利用

ショートメッセージ（SMS）を利用したフィッシングのことを**「スミッシング」**といいます。
利用者の多いスマートフォンが狙われ、スミッシングによる被害も増えています。
下記の注意事項を守って、フィッシングに備えましょう！

- ふだん利用するサイトはブックマークに登録し、ブックマークや公式アプリからアクセスする
- **ウイルス対策ソフトなどのセキュリティソフト**を導入しておく
- メール等の**URLは安易に開かず**、金融機関等のホームページで注意喚起されているか確認する
- 流出の危険に備えて、ID・パスワードは使い回しをしない

埼玉県羽生警察署　☎０４８（５６２）０１１０