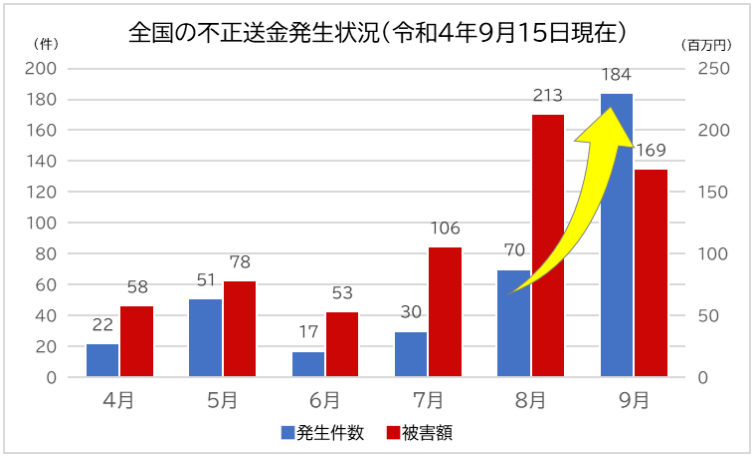
サイバーセキュリティの置き薬

2022年 第14号

インターネットバンキングでの不正送金被害が急増中！

令和４年８月下旬から、全国的にインターネットバンキングによる不正送金被害が急増しており、県内でも確認されています。被害の多くは、フィッシングによるものとみられ、注意が必要です。



フィッシングによる不正送金の手口

① 実在する金融機関を装い電子メールやSMSを送りつける。
② 電子メールやSMSに記載されたURLをクリックさせ、フィッシングサイト（偽のインターネットバンキングサイト）へ誘導する。
③ フィッシングサイト（偽のインターネットバンキングサイト）で、IDやパスワード等を入力させる。
④ 入力されたIDやパスワード等を窃取して不正送金を行う。

インターネットバンキングを利用するときの注意点

- 心当たりのない電子メールやSMSは開かない。
- 電子メールやSMSに記載されたURLからアクセスしない。
  （ブラウザから公式サイトへアクセスする、または金融機関が提供する公式アプリを利用する。）
- 電子メールやSMSに記載されたURLにアクセスしてしまった場合は、IDやパスワード等を入力せず、そのまま画面を閉じる。
- 利用状況を通知する機能を使って、覚えのない操作（ログイン、パスワード変更、送金・出金等）が行われていないか確認する。
- こまめに口座残高、入出金明細を確認する。

インターネットバンキングで身に覚えのないログインや入出金を確認した場合は、速やかに金融機関や最寄りの警察署へ相談してください。

【参考】警察庁「フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（注意喚起）」
https://www.npa.go.jp/cybersecurity/pdf/20220922press.pdf
一般財団法人日本サイバー犯罪対策センター（JC3）「インターネットバンキングの不正送金による被害を防ぐために」
https://www.jc3.or.jp/threats/topics/article-463.html
金融庁「インターネットバンキングによる預金の不正送金事案が多発しています。」
https://www.fsa.go.jp/ordinary/internet-bank_2.html