



サイバーニュース

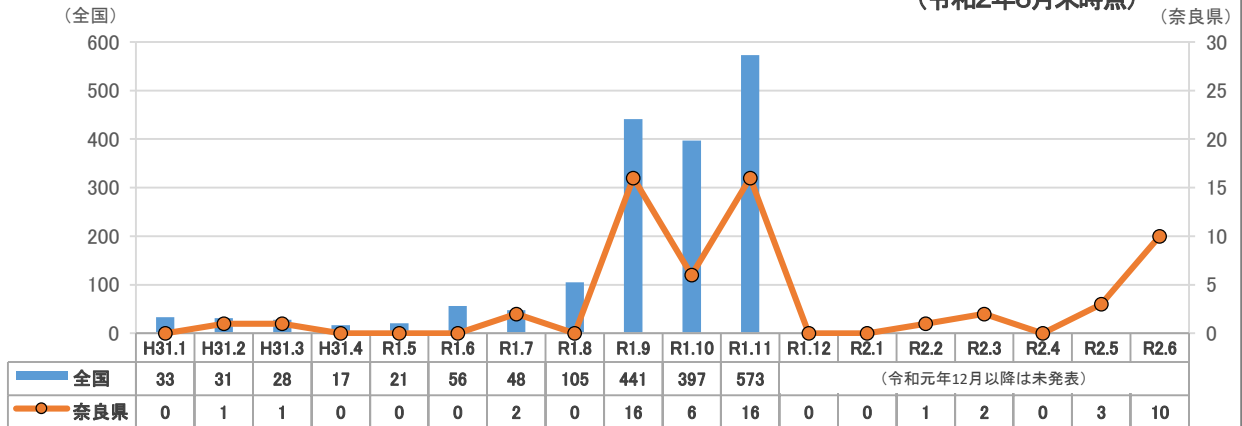
R 2 年 第 7 号
奈良県警察本部
サイバー犯罪対策課

フィッシングメールによる不正送金の被害に注意!

インターネットバンキングに係る不正送金事犯の発生件数

(令和2年6月末時点)

(奈良県)



※令和元年12月以降の全国件数は未発表

最近のフィッシングメールの例

【銀行を騙るSMS】

【■■■■銀行】お客様がご利用の口座が不正利用されている可能性があります。口座一時利用停止、再開手続き：
<https://■■■■.com>

メッセージに記載のURLをクリックすると銀行のフィッシングサイトへ誘導されます。
正規サイトと誤認させるため、フィッシングサイトのURLにHTTPSから始まるものが使用されたり、jpドメインが使用されているものもあります。

【宅配便の不在通知を装うSMS】

お荷物をお届けに上がりましたが不在の為持ち帰りました。ご確認ください。
<http://■■■■.duckdns.org>

一見すると、銀行とは関係のない内容ですが、URLをクリックすると不審なポップアップを表示させ、銀行のフィッシングサイトに誘導します。

【■■■】お客様がご利用の■■■■銀行に対し、第三者からの不正なアクセスを検知しました。ご確認ください。

確認

【警察庁を騙るSMS】

【警察庁】銀行をご利用のお客様に対し不正防止措置の認証確認を行っております、認証の設定はこちらへ：
<https://■■■■>

URLをクリックすると、銀行への認証を促すポップアップが表示されます。

【警察庁】不正送金による犯罪被害が急増しており、■■■■銀行をご利用のお客様に対し不正防止措置の認証確認を行っております、設定は次の通り行って下さい。

閉じる

ポップアップを閉じると、警察庁の偽サイトが表示された後、自動的に銀行のフィッシングサイトへ誘導されます。

被害に遭わないために

- メールに書かれたリンクにアクセスしない。
- 個人情報の入力を求めるメールを信用しない。
- フィルタリング機能もあるセキュリティソフトを導入。

⚠ フィッシングサイトで情報を入力してしまった場合は、すぐ銀行や警察に連絡



【参考】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の被害に注意」
<https://www.jc3.or.jp/topics/banking/phishing.html>