

# サイバーだより



令和元年 第7号  
令和元年11月26日

長野県警察本部  
サイバー犯罪対策室

## インターネットバンキングの不正送金被害が急増!! ～フィッシングにご注意を～

インターネットバンキングの不正送金被害が全国的に増加しています。  
その手口は、金融機関を装ったメールやSMS（電話番号で送受信されるショートメッセージサービス）を送信して、本文に記載された偽サイトのURLリンクにアクセスするよう誘導し、ID・パスワード等を入力させて情報を盗み取る「フィッシング」です。

### 手口例

手口1 セキュリティ強化と言って偽サイトに誘導してID・パスワードを入力させる。

SMS/MMS  
今日 16:48

〇〇銀行を装う偽メールに注意して、安全のために、施設ロックを行ってください。  
<https://〇〇bank.jp/xxbk.asp>

SMSの例

偽サイトに誘導

〇〇銀行  
〇〇銀行インターネットバンキング  
ご契約番号  
または  
店番号 口座番号  
ログインパスワード  
ログイン

本物とそっくり

手口2 リスクを検出したなどといって不安を煽って偽サイトに誘導してID・パスワードを入力させる。

あなたの〇〇銀行口座にはリスクが検出されましたので、口座の資金安全を確保するためにこの口座を制限します。正常な利用に影響しないように、ご自分で制限を解除してください。

下記のURLをクリックしてログインを解除してください。

<https://〇〇bank.jp/xxx.asp>

◆本メールは送信専用となっております。返信メールでのお問い合わせは承りかねますので、あらかじめご了承ください。

<インターネットバンキングヘルプデスク>  
〇〇お電話でのお問い合わせ

メールの例

偽サイトに誘導

〇〇銀行  
〇〇銀行インターネットバンキング  
ご契約番号  
または  
店番号 口座番号  
ログインパスワード  
ログイン

本物とそっくり

重要  
POLICE

## 被害防止対策

重要  
POLICE

- ☑ メールに記載されたURLリンクには絶対にアクセスしない。  
このようなメールからアクセスした先では、ID・パスワード等を入力しない。
- ☑ 普段から利用しているサービスはブックマークしておく。  
このようなメールが来た場合は、ブックマークや利用しているアプリからアクセスする。

