回　覧　印　印　印　印　印　印　印　印　印　印　印　印

ASAMA Security News Letter Vol.54

あさまセキュリティニュースレター

被害総額4億円超　ネットバンキングの不正送金被害が激増！　（2019年11月11日）

電話番号でメッセージが送れる
SMSによるフィッシングメール
（送信元は偽装可能）

お客様の[redacted]銀行口座がセキュリティ強化のため、一時利用停止しております。再開手続きをお願いします。http[redacted]

↑
偽のログイン画面
（フィッシングサイト）に誘導

JC3　HP抜粋
https://www.jc3.or.jp/topics/banking/phishing.html

偽のログイン画面　（https://や.jpドメインを利用するケースも）

ワンタイムパスワードの搾取（二要素認証の突破を図る攻撃も）

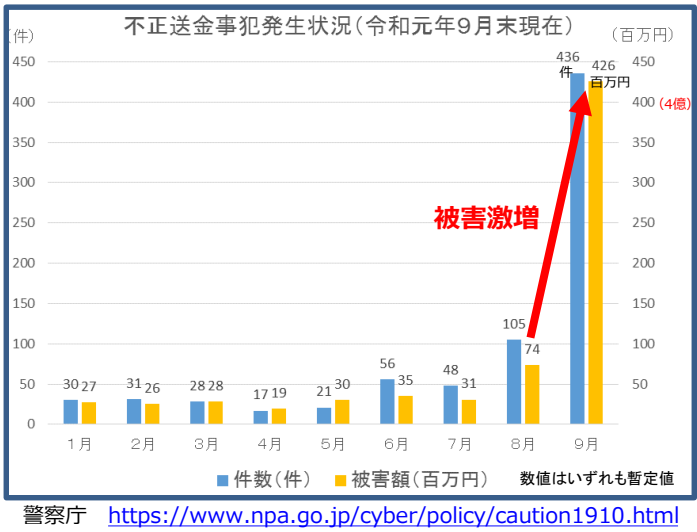
2019年９月における不正送金被害発生件数は436件、**被害額は約４億2,600万円と激増！！**ワンタイムパスワードなど二要素認証も突破する巧妙な手口も

攻撃のパターン

- メールだけでなく、SMS（ショートメッセージサービス）を利用し、偽サイトに誘導
- URLにhttps://から始まるもの、●●●.jpといった.jpドメインを利用し、信用させる
- ネットバンキングのIDパスワード、口座番号・暗証番号、ワンタイムパスワード
  秘密の合言葉等も入力させ搾取する

被害

個人情報等の漏洩　**不正送金被害**



警察庁　https://www.npa.go.jp/cyber/policy/caution1910.html

対策

- SMSを利用した攻撃の手口を知る
- 不審なSMS本文のURLリンクをクリックしない、情報を入力しない、直接銀行のHPで確認する
- 最新の情報、脅威、手口を知る

情報源

フィッシング対策協議会　https://www.antiphishing.jp/　日本サイバー犯罪対策センター　https://www.jc3.or.jp/

浅間商事株式会社　〒110-0005　東京都台東区上野7-15-70 浅間第一ビル　0120-830-414