



サイバーセキュリティ対策キャラクター
さいばみやくん

地域安全情報

(犯罪の起きにくい社会づくりのために)

令和6年12月25日

(No. 90)

発信者：宮崎県警察本部サイバー戦略局
(代) 0985-31-0110

〇〇銀行等の金融機関を名乗るフィッシングメールに注意！

日本サイバー犯罪対策センター（JC3）は、金融犯罪に繋がるスミッシングを観測しており、金融機関を騙るフィッシングメールを多数観測しました。

各金融機関の利用者が不正送金等の被害を受ける可能性があるため、ご注意ください。

「スミッシングとは・・・」

SMS（ショートメールサービス）を悪用したフィッシング詐欺で、SMSとフィッシングを組み合わせた造語になります。

スミッシングの主な手口は、スマートフォン等の電話番号宛てに、実在する企業や組織を偽ってメッセージを送信し、悪意のあるURLリンクを受信したユーザーにタップするよう促し、個人情報等を窃取することを目的とした犯罪のことをいいます。

攻撃の流れ



受信するSMS例

お荷物のお届けがありました、
不在の為持ち帰りました。

<http://xxx.com>

【緊急】

お客様の銀行口座の取引停止の
お知らせ

<http://xxx.com>

- 1 金融機関を騙ったSMSを受信し、文面に「**緊急**」等の言葉が含まれ不安や焦りを誘発する。
- 2 受信者がSMS文面に記載されたURL（攻撃側が用意するフィッシングサイト）にアクセスする。
- 3 受信者が該当のサイトに認証情報等の個人情報を入力する。
- 4 攻撃側はなりすましログインや、アプリののっとりにより受信者の口座から金銭を窃取する。

対策



- 心当たりのないメールやSMSは開かない
- メールやSMSに記載されたリンクをクリックしない
→ 内容の確認は、公式サイトやアプリを利用する
- 安易にIDやパスワードを入力しない。

参考：日本サイバー犯罪対策センター（JC3）「あなたのスマートフォンが犯罪のインフラに」

URL：<https://www.jc3.or.jp/threats/examples/article-592.html>

