

# 「IP 防犯ネット」情報 Vol.258

## ～SMS 詐欺について～

令和元年 7 月 22 日  
石川県警察本部  
生活安全企画課

### 実在する宅配業者を装ったSMSに注意

ショートメッセージサービス（SMS）を使用して偽サイト等に誘導する、いわゆる「SMS 詐欺」が依然として流行しており、被害に遭わないためのセキュリティ対策が必要です。

情報処理推進機構（IPA）等によると、平成 30 年 7 月頃から、佐川急便の不在通知を装った不審な SMS が出現し、偽サイト等に誘導される被害が報告されています。同年 12 月にはヤマト運輸を騙る不審な SMS が現れるなど、手口が様々に変遷しているので引き続き注意が必要です。

### 日本郵便（jppost）を騙る不審なSMSが

令和元年 5 月には、日本郵便を騙る同様の SMS が新たに確認されたと報告されました。

佐川急便等の場合と同様に、「お荷物のお届けにあがりませんが不在の為持ち帰りました。」など、宅配業者の不在通知を装った文言とともに、偽サイトの URL が記載されているものです。

誘導先の偽サイトの URL については **重要！！**

<http://jppost-〇〇.top:81>

等、日本郵便を連想させるものが確認されています。

#### (1) Android 端末の場合

誘導先の偽サイトでは、不審なアプリをインストールさせられるとのこと。

「提供元不明のアプリ」の場合、通常は警告画面が表示されますが、偽サイトによってはこのような画面を無効にするよう誘導し、巧みに不審なアプリをインストールさせられる場合もあります。

不審なアプリをインストールすると、

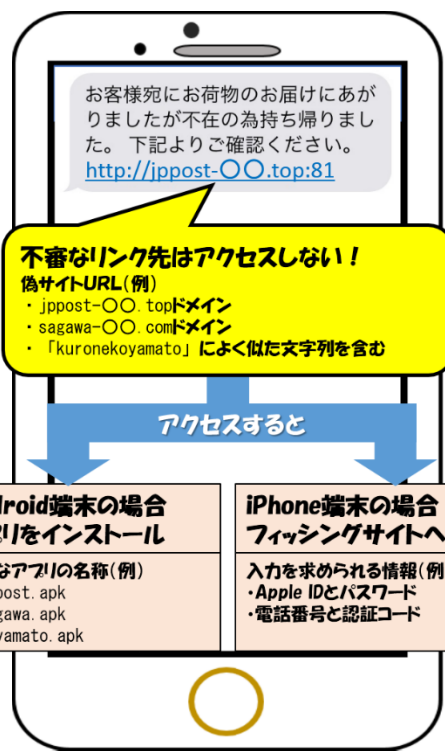
- ・ 端末内の「連絡先」データが盗み取られる
- ・ 決済用の SMS 認証コードが盗み取られる
- ・ 他の電話番号に同様の SMS が勝手に大量に送信されて被害が拡大する

などのおそれがあります。

#### (2) iPhone 端末の場合

不審なアプリのインストールの代わりに、フィッシングサイトに誘導されるおそれがあります。

フィッシングサイトで ID、パスワード等を入力してしまうと、決済手段の悪用や、パスワードリスト型攻撃による不正アクセス等の被害が考えられます。



誘導先の偽サイトの画面 (例)

### 被害に遭わないためのセキュリティ対策

- ・ 心当たりの無い SMS は、不用意にリンク先を開かずに削除する。(PC でアクセスした場合)
- ・ 提供元不明のアプリをインストールしない。
- ・ インストールしてしまったら、直ちに「設定」からアンインストールする。

