



## 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、実在する宅配業者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。続いて、他の宅配業者を騙る不審な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。

## 偽サイト等への誘導の手口

代表的なものは、「お荷物のお届けにあがりました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。

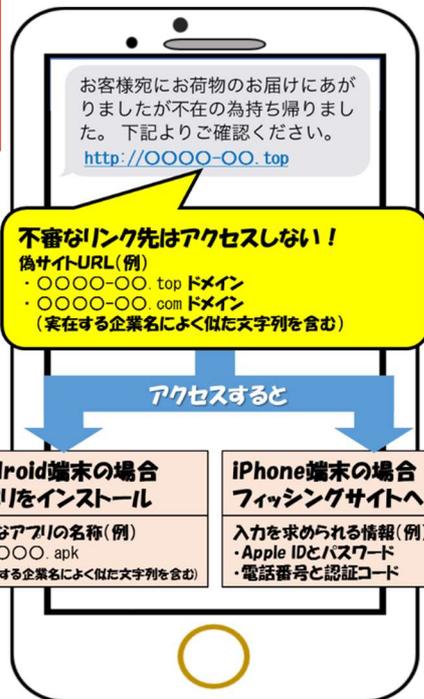
誘導先の偽サイトのドメインについては

http://○○○○-○○.top

http://○○○○-○○.com

**重要**

等、実在する宅配業者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です。

「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)  
(PCでアクセスした場合)

## 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。
- ・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。



サイバー犯罪（インターネットに関する犯罪）の通報やご相談は…

石川県警察本部生活環境課サイバー犯罪対策室



076-225-0110



cyber@police.pref.ishikawa.lg.jp

