【事例３】　宅配業者を装ったSMSをきっかけに生じたトラブル

～届いてもURLにアクセスしたり、電話をしないで！～

＜相談内容＞

① 宅配業者から荷物を届けたが不在だったと SMS（※１）が届いた。集荷センターに取りに行くと、詐欺だと言われた。（70 歳代　男性）

② 宅配業者から荷物を届けたが不在だった。詳細はURLを確認するようにというSMSが届いた。記載があった電話番号に電話をして住所と氏名を伝えたが、大丈夫か。（50 代歳　女性）

③ 宅配便を届けたが、不在のため持ち帰ったとスマートフォンにSMSが届き、URL をタップしアプリをダウンロードした。すぐにアンインストールしたが、スマートフォンの乗っ取りが心配だ。（40 歳代　女性）

④ 宅配便が届いたとSMSが届き、本文にあったURLを開くと銀行のログイン画面になり、ID と暗証番号を入れるようになっていた。銀行に確認すると半月前から同様の問い合わせが増えていると言われた。URL を開いてしまったが、大丈夫か。（40 歳代　男性）

⑤ スマートフォンに宅配業者から荷物を届けたが不在だった。詳細はURLから確認するようにとSMSが届いた。荷物が届く予定だったのでURLにアクセスするとアプリがダウンロードされた。その後、宅配便に関する問い合わせ電話が次々入るようになった。また、デジタルコンテンツの不正利用で１万円、私のスマートフォンからSMSを多数発信され、通信料約２万円を利用中の携帯電話会社から請求されているが、払いたくない。（40 歳代　男性）

※１　SMSとはショートメッセージサービスの略称で、電話番号等でメッセージを送受信できるサービスです

＜助　言＞

事例①は、宅配業者に直接確認ができたため、トラブルは生じませんでした。宅配業者各社のホームページには「SMS で不在連絡のお知らせはしていない、架空のWebサイトが発見されている」と注意喚起がされています。

事例②については、伝えてしまった情報を取り戻すことはできないため、様子をみて何か問題が生じるようであれば、再相談するよう伝えました。

事例③はアプリをダウンロードしています。スマートフォンへの影響範囲は不明です。アプリのアンインストールに加えてスマートフォンの初期化をするとよいでしょう。独立行政法人情報処理推進機構のホームページを参考にして

ください。

事例④は SMS をきっかけに情報を取ろうとするフィッシング詐欺だと思われます。情報を入力しなければ、問題は生じないと考えられます。情報を入力したときには、不正に使用されていないかを口座の取引明細を確認し、不正な引出しがある場合は速やかに銀行に申し出しましょう。他のアカウントで同じパスワードを使用している場合は、そちらも変更しましょう。

事例⑤は、偽サイトに誘導され、不審なアプリをインストールした結果、自身のスマートフォンから自動的に多数の宛先に SMS が送信されてしまい、覚えのない請求が生じた上、問い合わせの電話が入りました。また、偽サイトに入力した ID・パスワード等が携帯電話会社のキャリア決済などで不正に利用されたため、請求されました。今回のケースは携帯電話会社への申し出を助言し、一部は請求が取り消されました。

事例③～⑤はアプリをダウンロードした場合、被害拡大を防ぐために機内モードにし、アプリのアンインストール、初期化し、不正な使用、請求がないか確認しましょう。

宅配業者からの SMS が届いたことをきっかけにさまざまのトラブルが生じています。不審な SMS に記載された URL は絶対にタップしない、また、電話番号が記載されていても電話はしないようにしましょう。宅配業者から荷物について SMS が届くことはありません。宅配業者の公式サイト見るなど、日ごろから確かな情報源で真意を確認するようにしましょう。

（参考）　独立行政法人情報処理推進機構 ホームページ
https://www.ipa.go.jp/security/anshin/mgdayori20180808.html