# 宅配業者を装ったSMS

独立行政法人 情報処理推進機構(IPA) セキュリティセンター

連載の最終回となる本稿では、「宅配業者を装ったSMS」について取り上げます。

## 宅配業者を装った SMS

2018年7月中旬より「佐川急便を騙った不在通知のショートメッセージ（SMS）から、偽のサイトに誘導された」という相談が多く寄せられるようになりました。IPAではこの件に関して、8月初旬に注意喚起を行いました[*1]。

この SMS は不特定の電話番号から突然送られてきます（**図 1**）。SMS の内容は不在通知を装っていて、日本語に違和感がありません。また、佐川急便の公式であると思わせる URL[*2] がメッセージに含まれていました。

**図 1** 不在通知を装った SMS の例


この URL をタップすると、佐川急便の公式ホームページそっくりの偽サイトが開きます（**図 2**）。この偽サイトには、Android 端末で「提供元不明のアプリ」のインストールをするための手順が、画像付きで説明されています。Android 向けに作られているように見えますが、iPhone でアクセスしても同じ偽サイトが開かれることを確認しています。

**図 2** 佐川急便を装った偽サイトの例

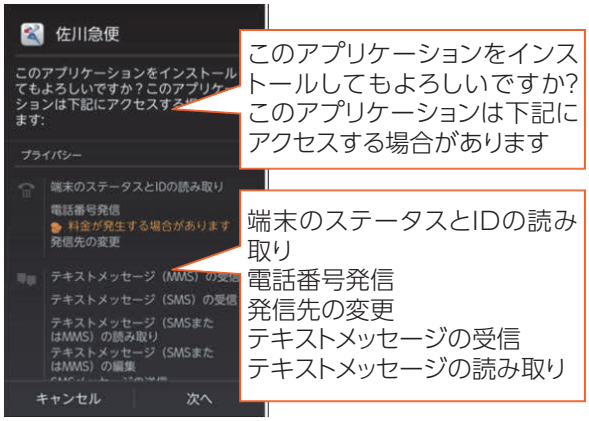

ここから先の手口は、攻撃対象のスマートフォンがAndroidかiPhoneかによって異なります。

## Android における手口と対処方法

偽サイトには本物と同じようにボタンやバナー等がありますが、これらのどこをタップしても「sagawa.apk[*3]」という不正なアプリがダウンロードされます。アプリはダウンロードされただけであれば、すぐに被害に発展することはありません。スマホ内に保存されたこの「sagawa.apk」をタップすると、インストールが開始されます。端末購入時から特に設定を変更していないのであれば、「提供元不明のアプリ」はインストールできなくなっているため、インストールは完了しません。「提供元不明のアプリ」とは、Androidの公式マーケット（Google Play）にあるもの以外のアプリを指します[*4]。しかし、偽サイトに書かれてい

*1 IPA「安心相談窓口だより 宅配便業者をかたる偽ショートメッセージに関する相談が急増中」（2018 年 8 月 8 日）
https://www.ipa.go.jp/security/anshin/mgdayori20180808.html
*2 実際の佐川急便の公式サイト http://www.sagawa-exp.co.jp/
*3 APK とは Android application package の略で、Android 専用アプリをインストールできる形式にパッケージしたファイル。
*4 公式マーケット以外のアプリをインストールできるところを「サードパーティー」という。

**図 3** 不正なアプリが求める権限一覧（一例）




る「提供元不明のアプリ」のインストールを許可する手順を実施してしまうと、インストールが完了してしまいます。

不正なアプリをインストールするとき、スマートフォン内の機能へのアクセス権限を求める確認画面が表示されます（**図 3**）。こうした画面は一般的なアプリをインストールする際にも見られますが、この画面に書かれた内容をよく読むことで、このアプリがどういう動きをするものなのか、ある程度推測できます。

今回の不正なアプリの場合、求める権限の中に「テキストメッセージ（SMS または MMS）の読み取り」「SMS メッセージの送信」「連絡先の読み取り」とあることから、Android 内に保存されている SMS や MMS の内容や、電話帳に登録した連絡先の内容が読み取られ、さらにアプリによって自動的に SMS メッセージが任意の宛先に送信されるだろうことが推測されます。

**■Androidにおける被害**

1） SMSの大量送信

不正なアプリを入れてしまうと、Android端末は自分のスマホに届いたものと同じ不在通知SMSを、不特定多数に送り付けることになってしまいます。不正なアプリが自動的に行うため、相談の中には、1日のSMS送信数が200通に達した[*5]という事例もありました。

2）キャリア決済の悪用

「身に覚えのないキャリア決済の請求が発生した」という相談もありました。請求元は、Apple やオンラインゲームが多いことが確認されています。悪意のある者がキャリア決済の設定を完了するには、SMS で届く認証コード（**図 4**）を入力する必要があるため、そう簡単に悪用はできません。しかし、不正なアプリを入れてしまった場合、SMS メッセージが悪意のある者に読み取られてしまうため、この認証コードの情報も知られてしまい、キャリア決済の設定がなされてしまうものと思われます。

**図 4** 認証コード受信画面の例 (Android)


AndroidスマートフォンはGoogleアカウントとひも付いて利用することができますが、そのアカウントに「身に覚えのないアクセス履歴があった」という相談もありました。アプリによって、パスワード等の認証情報も窃取されてしまう可能性も否定できません。

**■Androidにおける対策と対処**

基本的に、公式マーケット以外に存在するアプリは、その動作内容が保証されていないため、インストールすることは推奨しません。「提供元不明のアプリ」はインストールしない設定にしてください。

もし、不正なアプリを入れてしまった場合は次の対処をしてください。

**・スマートフォンを機内モードにする**

機内モードにすることで、SMSの送信を抑止することが可能です。なお、Wi-Fi機能やBluetooth機能をオフのままにしておくことで、スマートフォン内部の情報が外部に送信される心配もありません。

*5 一般的に、キャリア側で 1 日の SMS 送信上限を 200 通と制限している。

・不正なアプリをアンインストールする

機内モードの状態で、「佐川急便」という名前のアプリをアンインストールしてください。ただし、このアプリはAndroidのホーム画面上では見えません。Androidの設定の「アプリ一覧」から確認できるので、「佐川急便」という名前を探して、アンインストールしてください。

・スマートフォンを初期化する

不正なアプリをインストールしてしまったことによって、今回解説した以外の影響がないともいえません。そのため、より安全な対処として、スマートフォンの初期化を推奨します。

・各アカウントのパスワードを変更する

スマートフォンの初期化後にGoogleアカウントやSNS等のサービスアカウントのパスワードを変更してください。

・キャリア決済の限度額を設定する

キャリア決済の請求について不安がある場合は、契約している電話会社に確認してください。

キャリア決済はその月ごとの限度額を設定できます。限度額が未設定であるなら、この限度額を設けることで、被害を最小限に抑えることができます。この限度額についても、電話会社に問い合わせるといいでしょう。

## iPhoneにおける手口と対処方法

ユーザーがiPhoneで佐川急便の偽サイト上のボタンなどをタップすると、「電話番号」と「認証コード」を入力させて盗み取るフィッシングサイトへと飛ばされます（**図5**）。

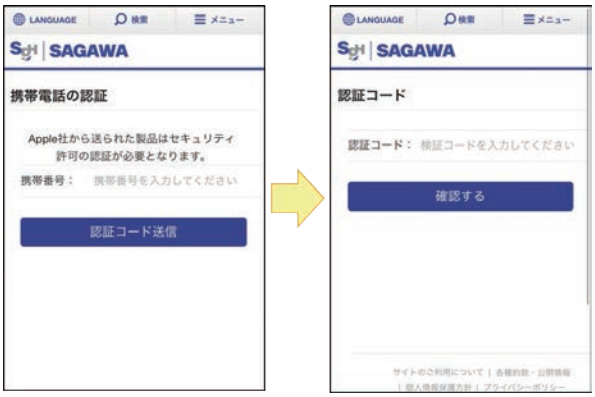
**■iPhoneにおける被害**

iPhoneにおいても、身に覚えのないキャリア決済の請求被害が発生しています。悪意のある者に「電話番号」と「認証コード」を知られてしまったことが原因と思われます。

**■iPhoneにおける対策と対処**

フィッシングサイトに情報を入力しなければ被害には発展しません。情報を入力してしまった場合は、次の対処を推奨します。

**図5** 佐川急便を装ったフィッシングサイトの例




・キャリア決済の限度額を設定する

キャリア決済の請求や限度額について、キャリアに確認することを推奨します。

iPhoneでは公式マーケットであるApp Store以外からアプリをインストールすることはできない仕様となっています。そのためこの手口では、AndroidとiPhoneで対処方法に大きな違いが表れています。

なお、今回の手口に限らず、認証コードをSMSで送信するしくみは、前号[*6]でも紹介した2段階認証でよく見かけるものです。認証コードは本人しか知らない情報であると認識してください。そのため、家族や知人であっても他人に教えてはなりません。インターネット上で入力する際は、フィッシングではないか注意してください。

## 最後に

どれほど技術が進化しても、人を「騙す」手口による被害を未然に防ぐことは難しいのです。騙されないようにするためには、手口を知ることが最も有効です。本連載がインターネットを利用するうえで、騙されないようになるための資料となることを願っています。

*6 ウェブ版「国民生活」2018年11月号「こんなときどうしたら？インターネットのセキュリティガイド」第5回「不正ログイン」
http://www.kokusen.go.jp/wko/pdf/wko-201811_06.pdf