

わたしは

# ダメサレナイ!!

第52話



ATTENTION

## 新たな手口でさらに広がる！ 宅配業者を装った不在通知のSMS被害

ショートメッセージサービス

このコーナーで紹介するマンガは、実際に起きた事件を基に、「だましのシーン」を再現したものです。「私だけは大丈夫」なんて甘く考えていませんか？ 実はそう考える人こそ被害に遭いやすいのです。

監修/NACS（公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会）消費者相談室/大井菜子 マンガ/まきのこうじ



現在横行している主な手口は二つあり、偽SMSで偽WEBサイトに誘導するまでは同じですが、そこから先のだまし方に違いがあります。

《従来からの手口》

宅配業者の偽WEBサイトで、消費者にIDやパスワード、認証コードなどを入力させて個人情報やクレジットカード情報を窃取する手口です。窃取された個人情報はキャリア決済などに不正利用されて、身に覚えのない請求を受けるケースもあり、次のような被害事例が報告されています。

「SMSで宅配業者の不在通知が届き、記載されているURLにアクセス。通販サイトのIDとパスワードの入力を誘導されて入力したら、後日通販サイトで5万円も決済されてしまった」。



### 2 新手法！ スマートフォンを乗っ取る不正アプリ

増加しています。

現在横行している新しい生活様式として、通信販売の利用が推奨されている中、新たな手口の発生も起因して、2020年度は、消費生活センターなどへ寄せられた「不在通知のSMS」に関する相談の件数が、前年度同時期（10月まで）比で2倍近くに増加しています。



### 1 宅配業者を装ったSMSによるフィッシング詐欺が増加

宅配業者を装ってスマートフォンに不在通知のショートメッセージサービス（以下、SMS）を送り、本物の宅配業者のWEBサイトにそっくりな偽WEBサイトへ誘導して、IDやパスワードなどの個人情報を窃取するフィッシング詐欺。この詐欺は2018年度に多発しましたが、SMSはメールより開封率が高いうえ、情報量が少ないため偽物と判断するのが難しく、今なお多くの被害者が出ています。

「今、注文しているのは焼肉セットだね！」

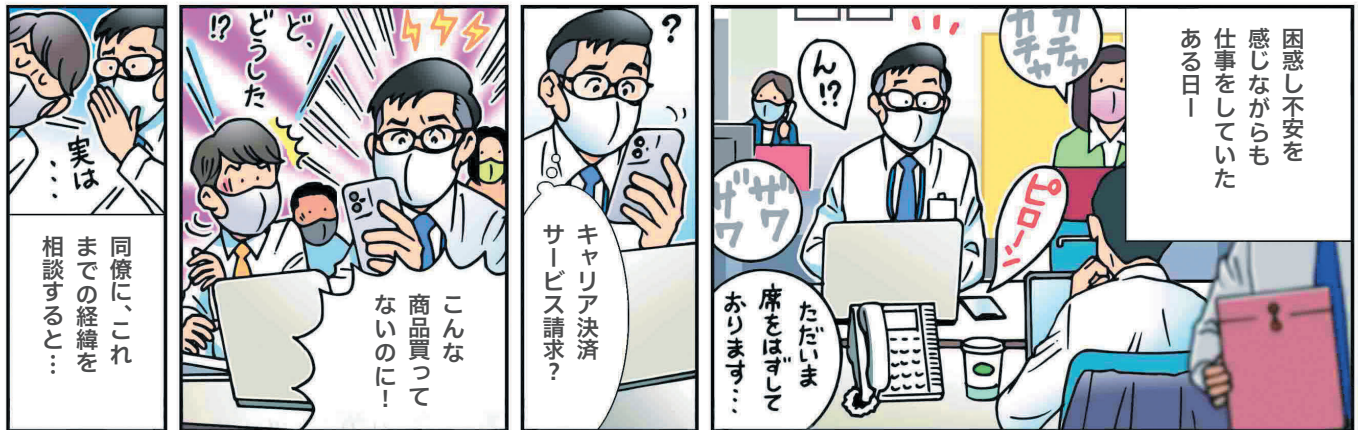
「すっかりリピーター!!」

「へ～そんなにうまいんだ」









**関連情報**

- 国民生活センター  
「宅配便業者を装った『不在通知』の偽SMSに注意しましょう-UURLにはアクセスしない、ID・パスワードを入力しない!」  
[http://www.kokusen.go.jp/pdf/n-20201126\\_2.pdf](http://www.kokusen.go.jp/pdf/n-20201126_2.pdf)

**万一の相談先**

- 消費者ホットライン  
☎188 (「いやや!」と覚える)  
※最寄りの消費生活センターや消費生活相談窓口につながります。相談受付時間は相談受付先によって異なります。
- 警察相談専用電話  
☎#9110

直接アクセスして確認しましょう。また、公式マーケット以外からのアプリのインストールを、できるだけ避けることをお勧めします。日ごろからの対策として、あらかじめスマートフォンの設定で、「提供元不明のアプリのインストール許可(端末機種によって名称が異なります)」をオフにしておくといでしょう。

また、2段階認証や携帯電話会社のセキュリティサービス、セキュリティソフトを活用し、定期的にスマートフォンをチェックしておくといでしょう。

万一、偽のWEBサイトにIDやパスワードを入力してしまったと気づいたり、覚えのないキャリア決済やSMSなどの請求が届いた場合は、すぐにIDやパスワードなどを変更して、携帯電話会社に確認しましょう。不正アプリをインストールしてしまったときは、通信を無効化するために、スマートフォンを機内モードに設定して、不正アプリをただちに削除してください。インストールされている間に不正アプリが、スマートフォンの機能や情報に悪影響を及ぼしている可能性があるため、アプリの削除だけではなく、スマートフォンの初期化を推奨します。また、各サービスアカウントのパスワードは変更しましょう。

不安に思ったりトラブルに遭ってしまったら、迷わず消費者ホットラインや警察相談専用電話に相談してください。