わたしは ダマサレナイ!!

第47話

携帯電話会社を装ったSMSに注意！
キャリア決済を不正利用する新手のフィッシング詐欺

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あいやすいのです。

監修／大井菜子 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　　マンガ／まきのこうじ

POINT! SAGI 1 新手のフィッシング詐欺 キャリア決済が不正に利用される！

金融機関などを装ったメールで偽サイトに誘導し、クレジットカード番号などの重要な個人情報を盗み出すフィッシング詐欺。最近は、新たな手口として、キャリア決済を不正利用される被害が急増しています。

キャリア決済とは、スマートフォンやパソコンなどで購入した商品などの代金を、月々の携帯電話の利用料金とまとめて支払うことのできる決済サービスです。特別な申込みをしなくても、自分が契約している電気通信事業者（以下、携帯電話会社）でふだん用いているIDやパスワードなどを入力するだけで簡単に利用できるため、誰しもが、この手口のターゲットになり得るのです。

POINT! SAGI 2 携帯電話会社そっくりのSMSとサイトで巧妙に個人情報を搾取

手口は、携帯電話会社を装ったショートメッセージサービス（以下、SMS）を消費者に送り、偽の携帯電話会社サイトへ誘導。そこでIDやパスワードなどを入力させ、キャリア決済に必要な情報を搾取したら、デジタルコンテンツやショッピングサイトでの商品購入で、消費者のキャリア決済を不正利用します。

単純な手口ですが、文面や差出人の情報が少ないため、偽物と判断しにくいSMSを使用するなどの巧妙な仕掛けにより、ふだん注意している人でもだまされやすいのです。さらに、SMSに記載されているリンク先のURLには、携帯電話会社名が入っていることもあるほか、中には、携帯電話会社の公式SMSが届く正式なスレッドに、偽のSMSが入り込んでくるケースもあり、こうなると見破るのはきわめて困難です。

具体的な事例をご紹介します。携帯電話会社の公式SMSが届くスレッドに、「利用料金が高額になっ

ているので確認してください」、「期間限定でクーポンプレゼント」といった偽のSMSが届きます。記載されているURLにアクセスすると、携帯電話会社サイトにそっくりの偽サイトが開き、IDやパスワードなどの入力を求められます。入力すると、画面が真っ白になったり、エラー画面が表示されたりします。この時点でキャリア決済に必要な情報を搾取されているので、そのまま放っておくと、キャリア決済を不正利用されてしまいます。

この手口のもう一つの特徴が、不正利用に気づくタイミングです。携帯電話会社から、キャリア決済利用通知やキャリア決済利用の限度額に達したという通知が届いて初めて、不正利用されたことに気づくことが多いため、限度額まで不正利用されてしまい、被害額が大きくなりやすいのです。

POINT! SAGI 3

キャリア決済不正利用の補償は携帯電話会社の利用規約に基づく

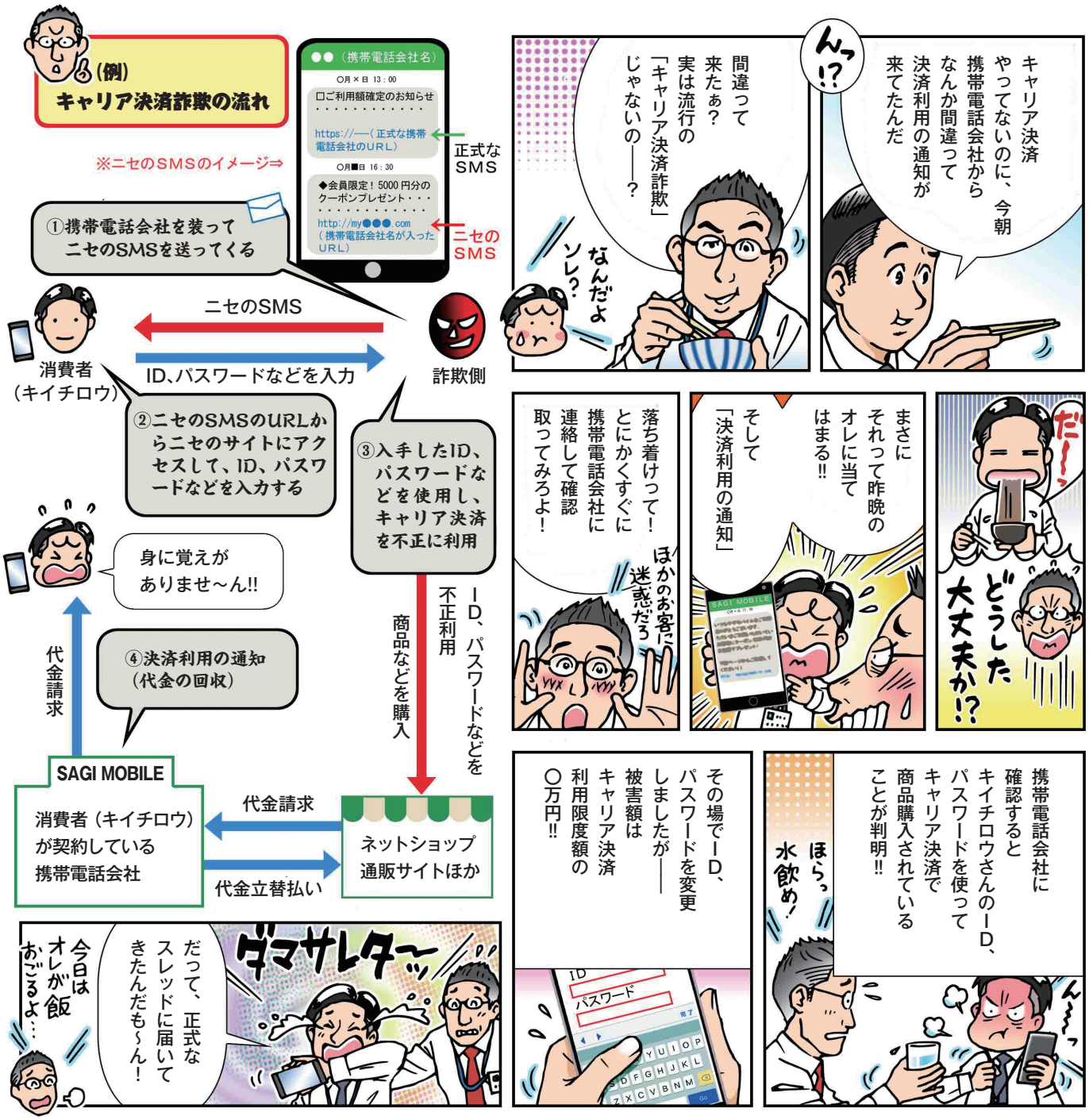
キャリア決済についての規制内容や消費者保護は、基本的に各携帯電話会社の利用規約に基づいています。以前は、フィッシング詐欺によるキャリア決済不正利用への補償を、どの携帯電話会社も利用規約に記載していませんでした。そのため、不正利用による不正購入であっても請求を止めることは難しく、泣き寝入りする人も多かったのです。

現在は、キャリア決済が可能なすべての携帯電話会社が利用規約を改定し、フィッシング詐欺による不正利用の被害補償制度を導入しています。

POINT! SAGI 4

トラブルを避けるための対策といざというときの対処法

こういった手口は無視することが一番なのですが、見分けがつかないことも多いため、いくつかの効果的な対策をお伝えします。



■記載されたURLに安易にアクセスしない

WEBサイトに誘導するSMSは、まず怪しみ、記載されたURLから安易にアクセスしないようにすること。携帯電話会社の公式WEBサイトに直接アクセスするか、事前にマイページをブックマークしておくなど、すぐに問合せや確認ができるように、あらかじめ備えておきましょう。

■セキュリティーの強化

2段階認証（IDとパスワードに加えて、ほかの方法での本人認証が必要となる仕組み）の設定やセキュリティーソフトの導入、迷惑SMSなどの対策サービスを活用しましょう。

■キャリア決済の設定変更

キャリア決済の利用限度額を低額に設定するほか、必要が無ければ、キャリア決済を利用しない設定にしましょう。

こうした対策をしていても、トラブルにあってしまう可能性はあります。少しでも怪しいと感じたり、身に覚えのないキャリア決済利用通知や2段階認証の通知が届いたら、すぐにパスワードを変更して、キャリア決済を停止。携帯電話会社や決済利用通知に記載されている購入店に連絡しましょう。偽のSMSやキャリア決済利用通知などは、不正利用された証拠になるので、必ず保存しておきます。ご自分で判断できなかったり不安に思ったら、消費者ホットライン（188）や警察にご相談ください。

万一の相談先

- 消費者ホットライン
  ☎188（いやや）（「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。

参考情報

- 国民生活センター
  「携帯電話会社をかたる偽SMSにご注意！-あなたのキャリア決済が狙われています-」
  http://www.kokusen.go.jp/pdf/n-20190905_1.pdf