キャッシュレス時代のITの基礎知識 ≫ 第4回

お金と個人情報を守るための基礎知識

IT編集者
宮田 健

［みやた・たけし］アイティメディア「@IT」記者を経て、現在はセキュリティに関するフリーライターとして活動する。「ITセキュリティ」を、普通の人にも興味を持ってもらえるためにはどうしたらいいか、日々模索を続けている。著書に『Q＆Aで考えるセキュリティ入門「木曜日のフルット」と学ぼう!』『デジタルの作法 1億総スマホ時代のセキュリティ講座』がある。

セキュリティに関して記事を書く仕事をしていると、よく「クレジットカードの不正利用に遭ったのだが、どうしたらいいか」と相談を受けます。多くの場合はクレジットカード会社側で不正を検知していたため、直接の金銭的被害がないことが多いようです。

多くの方が原因を自己分析して、外出先の公衆Wi-Fiを使ったことや直近で利用したEC（Electronic Commerce：電子商取引）サイトからの情報流出などを疑いますが、個人レベルでの原因追及は難しいです。むしろ、被害がなかったことを喜ぶべきかもしれません。これこそが、お金の流れを追跡でき、不正利用を検知できるクレジットカードの利点とも言えるわけですから。

とは言え、自衛をしなくていいというわけではありません。今回は私たちが守らねばならない、お金と個人情報をどう守っていくかを考えてみましょう。

「認証」を守る

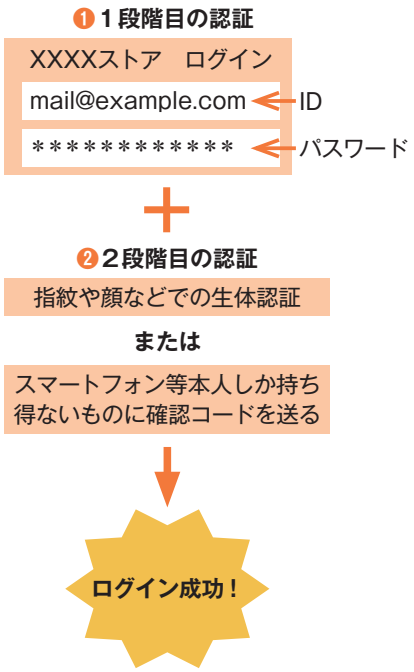
最も重要なことは、あなたが、あなたであることを奪われないことです。サイバー空間（コンピューターやネットワークにより構築された仮想的な空間）では、顔も見えず、声で判断することもできません。そんな状況で、「あなたが、あなたであること」を判断するために、「パスワード」が多く使われます。パスワードであれば、あなたの頭の中にしかない情報ですので、「あなたが、あなただ」と判断することができました。実はパスワードは、〝合い言葉〟として、古くはギリシャ時代から活用される認証手法でした。

ただし、現在はその原則も破られつつあります。あまりにパスワードの必要なサービスが増えた結果、「パスワードを使い回してしまう」こと、そしてサービス提供側にセキュリティの意識が低いことにより、「パスワード情報そのものが漏えいする」ことが重なり、もはやパスワードは秘密のものではなく、サイバー攻撃者が知ることができる情報になってしまったからです。

本連載でも何度か触れてきましたが、パスワードだけに頼ってきた認証方法は既に古く、いまは「2段階認証」と呼ばれる手法が一般的になりつつあります【図1】。記憶情報であるID、パスワードだけでなく、ログイン時にスマートフォンに届くSMSに書かれた、その時限りの数字列を入力させることで、スマートフォンの持ち主であるという所持情報を組み合わせ、あなたがあなたであることを認証する手法です。

認証を守るには、できる限り前述の**「2段階認証を利用する」**こと。そして、**「パスワードは生年月日や電話番号など誰もが知る情報をもとに設定しない」**こと、**「できる限り使い回しはしない。特に〝お金〟**

【図１】２段階認証のイメージ



に関係するものだけは、長いパスワード文字列にすることを強くお勧めします。覚えにくい場合、紙に書いてその紙を厳重に保管することもお勧めします。「原始的な！」と思われるかもしれませんが、使い回してしまうよりは十分よいはずです。

偽サイト、偽メールを見て「怪しいかも？」と思えるようになろう

「認証」が重要だということは、私たちよりもむしろサイバー攻撃者の方が正しく理解しています。サイバー攻撃者は生活がかかっていますので、認証を奪うことにすべての労力をかけるのです。なぜなら、サイバー攻撃が成功すれば〝現金〟が手に入れられるからです。

サイバー空間において、サイバー攻撃者ほど「費用対効果」を考える人たちはいないでしょう。彼らは世界中の犯罪者と分業し、最先端の技術を使ってくるのです。もはやこれはＩＴ技術ではなく〝詐欺〟の世界。だまされるのは機械ではなく、あなたなのです。

サイバー攻撃者が認証情報を奪う方法はさまざまですが、一番簡単に奪うには「偽物のホームページに誘い込み、あなた自身にＩＤ／パスワードを入力させる」ことが挙げられます。

例えば、あなたがよく利用する銀行のネットバンキングそっくりのページを作り込み、「あなたのお金が盗まれました！」というような、ドッキリする文言をあなたのメールアドレスに送りつけたとしたら、それをウソだと見抜けるでしょうか？自分が利用していない銀行ならともかく、「荷物を配達しましたが不在でした」というようなメッセージだとしたら、通販をよく利用する方なら反応せざるを得ないかもしれません。

問題は、もはや偽サイトであるかどうかを見抜くことは不可能ということです。多くの場合、偽のサイトに呼び込む偽のメール／メッセージは、偽かどうかを判断するより「すべて無視せざるを得ない」状況にあります。もし、それが切羽詰まった状況であればあるほど――例えば「ワクチン接種ができます」「還付金第２弾が支払われます」「あなたがポルノサイトを見ていた」などなど――これは詐欺かもしれない、とまず考えることができるようになれば、そこでサイバー攻撃は失敗に終わるはずです。

ＩＴ無関係の「詐欺」そのものにも注意！

最近「サポート詐欺」という手法が話題になっています。パソコンを使っていると、あるＷｅｂサイトを開いた瞬間、ド派手な色使いで「あなたのパソコンはウイルスに感染しました。これを直すには XX-XXXX-XXXX に電話してください」というようなメッセージが表示されます。実際に電話をすると、セキュリティ企業を名乗る担当者が話を始め、調査のために特別な設定を行うよう指示されます。すると、目の前のパソコンが遠隔で操作され、特定のソフトウェアを購入するよう促されるのです。

実はこれ、すべてがウソ。サポートをするように見せかけ、指示されるのはあなたのパソコンを遠隔から操作し、マルウェア（悪意あるソフトウェア）をインストールさせる仕組みです。著名なメーカーの名をかたることも多く、パソコンに詳しくなければこれらの指示に疑問を持たず、言われた通りに作業をしてしまうのではないでしょうか。

このように、最近の詐欺はパソコンの脆弱（ぜいじゃく）性を突くなど、映画で見るようなハッキングではなく、あなたそのものをだましにかかります。これも、手口を知ってさえいれば途中で「なんだかおかしいぞ？」と気がつけるかもしれません。Windows 10などをリリースしているマイクロソフトの

調査によると、意外なことに日本ではこういったサポート詐欺被害に遭うのは高齢層ではなく、若年層だと報告しています。日本ではまだまだ、こういった詐欺の耐性が低いのかもしれません。

同様に、そのままお金につながる「キャッシュカード」も狙われています。これはインターネットを通じてではなく、より身近な電話やハガキが入り口として使われます。いわゆる「振り込め詐欺」として話題になっていますが、最近では高齢者宅に電話し、「還付金があります」などとだまし、銀行のATMに誘導した上でお金を振り込むふりをして、実際には振り込ませ、不正に送金させるという手口も一般的になりました。

将来的には、不正な送金を銀行側で（AI等を用いて）検知できるようになり、対策が行えるはずだと考えています。それまでは、そういった**詐欺行為が行われていることを知ることこそが対策**です。これらの問題を身近に感じるためにも、ぜひご家族で話題にしてみてください。

実はすごく重要 ――お金を守る「クレジットカード」の話

もう1つ重要なのは、私たちの現実世界とITのサイバー空間を〝お金〟でつなげる「クレジットカード」に関する守り方です。

クレジットカードを巡る攻撃は、これまでならば「偽造カード」が中心でした。これはクレジットカード番号を盗み見て、それを偽造カードの磁気ストライプにコピーし、所持者がクレジットカードを持ったままもう1枚のコピーカードを不正に使うという手法です。しかし、いまではこの手法による不正利用はほぼ絶滅したと考えてよいでしょう。そもそも、磁気ストライプによる決済が既にほとんど利用されておらず、クレジットカードに内蔵されたICチップによる決済が主流となっているからです。クレジットカードの国際ブランドの1つマスターカードは、既に磁気ストライプの廃止を明言しており、1960年から利用されている手法がまもなく終了する予定です。

しかし、サイバー攻撃者も進化を止めることはしません。いま主流となっているのは、ECサイトなどクレジットカード決済を行うシステムそのものを攻撃し、カード番号をデジタル的に奪い、それをインターネット上で利用するという手法です。これであれば、クレジットカードそのものを物理的に奪う必要もありません。対面で確認されることもなく、いまのところは不正利用が発覚したタイミングでクレジットカードを再発行し、カード番号を変更するという対処しかできません。

多くの場合、決済を行うクレジットカード会社自身がその不正を検知し、利用者に影響がないようクレジットカード会社による補償が適用され、取引が停止されます。

しかし、利用者も「常に明細をチェック」し、身に覚えのない取引がないかを見る必要があるでしょう。

スマートフォンの時代では、これらのチェックも大変楽になりました。多くのクレジットカード会社はスマートフォンアプリを提供しており、クレジットカードを利用するとほぼ同時に、スマートフォンに利用通知が飛んでくるようになっています。この仕組みを活用することで、身に覚えのない不正利用をすぐに発見できるようになっています。ぜひ、これを活用してください。

そういったスマートフォンアプリを利用していない場合でも、**毎月送られてくる明細書は必ず目を通しておく習慣をつけておきましょう。**多少面倒ですが、大事なお金を奪われるよりはよいはずです。

そして、最近ではクレジットカードそのものにカード番号などを記載しないことで、さらにセキュリティを高めるナンバーレスの仕組みも登場しています。カード番号、有効期限、そしてセキュリティコードもなく、記載されているのは所有者の名前だけ。スマートフォンアプリを見ないとそれらの情報が分からないため、万が一、店舗で店員がカード番号を盗み見ようとしても安全というものです。私も最近このナンバーレス仕様のカードを手に入れました。最も完ぺきな情報漏えい対策は「情報を持たないこと」。その意味ではなかなか面白い仕組みだと思いました。

>>> キャッシュレス時代のＩＴの基礎知識

【図2】セキュリティ関連の情報収集に役立つ「Twitterアカウント」

- 警視庁サイバーセキュリティ対策本部　@MPD_cybersec
- フィッシング対策協議会　@antiphishing_jp
- 埼玉県警察本部サイバー犯罪対策課　@spp_cyber
- IPA（情報セキュリティ安心相談窓口）　@IPA_anshin
- マイクロソフト セキュリティチーム　@JSECTEAM
- カスペルスキー 公式　@kaspersky_japan
- マカフィー・セキュリティ情報局　@McAfee_JP_Sec
- トレンドマイクロ　@trendmicro_jp

知識のアップデートで大切なお金と個人情報を守る

短期連載も今回で終了です。最後に、皆さんに継続的に知識をアップデートしてもらうための方法をお伝えしたいと思います。「情報収集をしましょう」と言うのは簡単ですが、いざやってみようとすると難しいものです。「いつ、どのタイミングで見ればいいのか、よく分からない」というのが本音ですよね。そこでご提案するのが、ＳＮＳを活用した方法です。

Twitter（ツイッター）では、警察やセキュリティベンダー（セキュリティ対策のためのソフトウェアやサービスを開発・提供している事業者）を始め、さまざまな最新の情報が公開されています。特に【図2】のTwitterアカウントには有用な情報が多く投稿されています。詐欺の手法は日々新たなものが登場していますので、これらのTwitterアカウントをフォローしておくと、前もって準備ができるはずです。

そして特にお金に関しては、**不正利用があったときにまずどこに問い合わせを行うべきか、前もって調査をしておく**ことを強くお勧めします。実際に不正利用されてしまった時には慌てふためいているでしょうから、平時であるいまこそが、その調査を行うべきタイミングです。いま持っているクレジットカード、キャッシュカードの一覧を作成し、それぞれどこに連絡すべきかをメモしておきます。「クレジットカードの裏面に書いてあるからその時でいいや」と思わないでください。万が一の時、クレジットカードが手元にあるとは限らないのですから。もし既に利用していないクレジットカードが見つかったならば、解約し整理することも立派な対策でしょう。

万が一、自分がクレジットカード情報を含む個人情報漏えいの対象になってしまったら、まずは毎月の支払が発生しているサービスに対し、１つ１つ新番号に変更をかけましょう。大変な手間かもしれませんが、これもクレジットカードごとに紙にメモとして記録しておくとよいでしょう。

インターネットは現実とは別の空間という認識はもはや古いもの。いまのインターネットとは、リアルそのものと考えるべきです。いまではそのインターネットの空間から、リアルな資産流出が起きてしまう時代です。ＩＴの力で何とかしたいところですが、残念ながらまだそこまで技術は発展していないようですので、大事なお金は、私たち自身がそれなりに自衛し、守っていかなければなりません。

とは言え、考え方はシンプルに「認証を守る」こと。より具体的にはＩＤとパスワードを管理し、これを奪われないよう努力することが挙げられます。そしてパソコン、スマートフォン、アプリは「常に最新にしておく」こと、そして情報を積極的にウォッチし「最新の手口を知っておく」ことで、お金や情報を守ることができます。本連載がその一助になれば幸いです。