キャッシュレス時代のITの基礎知識 >>> 第2回

スマートフォンを安全に使うための基礎知識

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。

今回はまず、皆さんがいま、手元に持っているであろう「スマートフォン（スマホ）」とは何かを考えるところから始めてみましょう。

数年前までなら、家にある電話が単に持ち出せるものになった、という程度のものだったかもしれません。しかしいまやその画面も大きくなり、一昔前のパソコンよりも高性能な処理装置が内蔵され、大容量の記憶装置までも備えています。**もはやスマホは「超小型のパソコン」である**と考えたほうが良さそうです。

ここで考えておきたいのは、パソコンであると同時に、知人や取引先の電話番号が含まれる「連絡帳」であり、ごくごく個人的な写真が大量に収められた「写真集」であり、場合によっては銀行口座へアクセスするための「印鑑」や「通帳」にもなり得るという点です。さらにはそこに、現金と同様の「おサイフ」となり得る機能まで付けられています。

だからこそ、スマホは家の電話の延長という考え方はいったん横に置いて、**「個人情報が詰め込まれたデバイス（機器）」である**という認識で、スマホをどう安全に使っていくべきか考えましょう。

そもそも、スマホをおサイフにしていいの？

新型コロナウイルス感染症が広まってしまうほんの少し前、「○○Pay（ペイ）」など「スマホを使った電子マネー」の事業者たちが一気に攻勢をかけてきました。2020年10月に行われた消費税率改定、そしてマイナンバーカードと連携した「マイナポイント」施策に合わせるように、各社は大量のポイント還元キャンペーンを繰り広げ、電子マネーのシェアを獲得しようと普及を目指しました。皆さんの周りでも、これを機に「○○Pay」などを使い始めた人がいたかもしれません。

そうなると、最も気になるのは「〝○○Pay〟を、ポイントを集めるために使うべきか？」という疑問です。先に個人的な結論を述べると、「無理して使う必要は全くない」と考えています。おそらく多くの方は既にクレジットカードを所持しているでしょうし、SuicaやPASMO（スイカ、パスモ）といったプリペイド型（先に入金を行うタイプ）の交通系電子マネーも使っているでしょう。この時点で既に、キャッシュレス時代に合わせた行動ができていると自信を持ってかまいません。

正直に言ってしまえば、「○○Pay」の狂乱が起きているのは、サービス開始初期の（過大な）ポイント還元のためだけです。それが一段落すれば、無理にそれらを使うことにはほぼ意味がなく、メリットよりもリスクのほうが大きいと私は考えています。クレジットカード、もしくは交通系電子マネーで十分です。

では、キャッシュレス決済をわざわざ「スマホ」で行う必要はないのでしょうか？この点に関して、私はスマホを使うメリットが大きいと思っています。ただしそこには「いくつかのポイントさえ押さえておけば」という前提条件が付きます。

スマホを安全に使うための第一歩

高性能な頭脳を持ち、記憶容量も大きなスマホ。最近はキャッシュレス決済機能も付いている――そのような物を〝持ち歩く〟のが現代のライフスタイルです。ならば、それ相応の守り方を考えておくべきでしょう。

とは言え、難しく考えることはありません。やるべきことは「画面のロックをしよう」という1点につきます。スマホは小さいのでつい会社の机の上に置きっ放しにしたり、カフェで席取りのために放置することがあるかもしれません。まずはそのような〝放置〟を止めることが一番ですが、次の段階として画面ロックを行い、自分以外の人間が操作できないようにしておきましょう。

方法は簡単。顔認証が搭載されたiPhoneならば「設定」→「Face IDとパスコード」から「Face IDをセットアップ」し、「パスコードを要求」を「即時」にしておきます【図1】。Androidも「設定」から画面ロックをオンにしておきましょう。

画面ロックの際、顔認証や指紋認証など生体認証に対応したスマホであれば、ぜひ積極的に利用してください。数字4桁のパスコードですら入力は面倒です。画面ロックの解除は1日に数十回も行うものなので、できる限り簡易に解除できるよう生体認証を活用したほうが便利です。

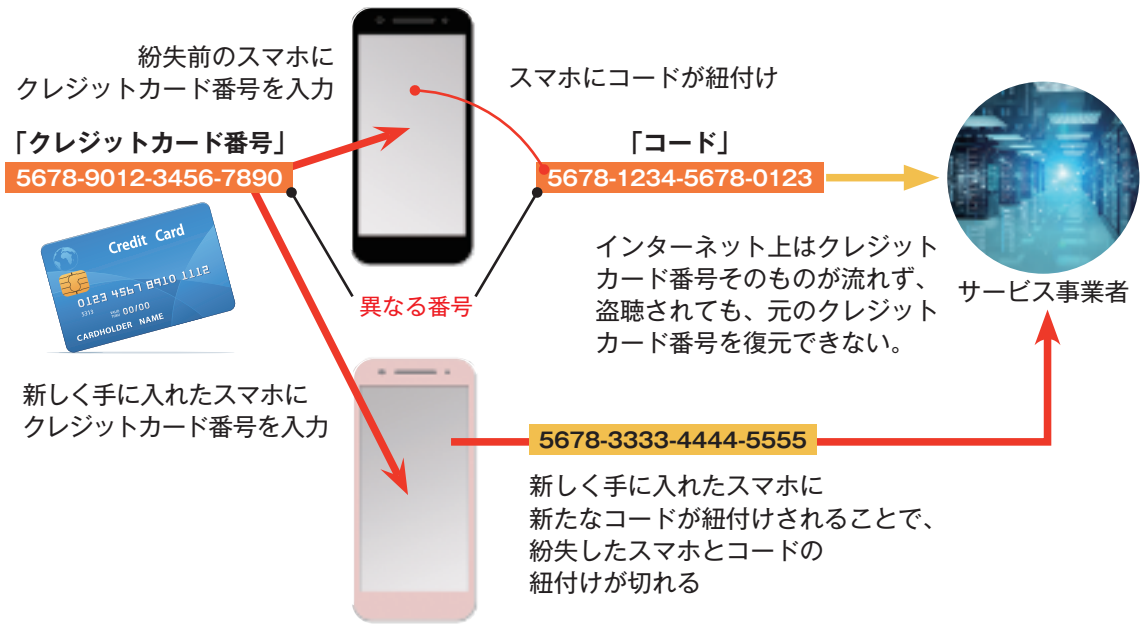
こうしておくことで、もしスマホでキャッシュレス決済機能を有効にしていたとしても、他人が簡単に使うことはできなくなります。これこそが重要なポイントです。例えばプラスチックのクレジットカードであれば、サインをごまかすことで店舗での決済が通ってしまうリスクがあるでしょう。最近はクレジットカードを使う時に「PIN（ピン）」と呼ばれる数字4桁の入力を求められることが増えましたが、スーパーなどでは少額ならばサインもPINも要求されません。物理的なカードよりも、スマホのキャッシュレス決済機能を使うほうが安全、という場合もあるのです。

また、スマホをおサイフ代わりに使うことで、「紛失時の面倒さ」が変わってきます。おサイフを失くしてしまった場合、現金はもうあきらめるしかありません。クレジットカードはカード会社に連絡することで、再発行が可能なはずです。この場合、リスクはかなり減りますが、それでもカード番号が変わることによる引き落とし処理の変更など、面倒さは想像以上にあります。

しかし、スマホがクレジットカード代わりになった場合、紛失時には画面ロックが施されているはずなので、そう簡単に第三者が使うことはできません。さらにスマホは通信が可能なので、遠隔操作によりスマホが使えないようにロックをかけたり、保存

【図1】iPhoneの画面ロックの方法

【図2】スマホがクレジットカード代わりになっている仕組み



された情報を消去したりできます。

そして前回お伝えしたように、スマホがクレジットカード代わりになっている場合、トークン化技術により、クレジットカード番号と異なるコードを元に決済が行われています。このコードはスマホの個体に紐付いているため、登録されたコードと、登録時に利用されたスマホのセットで決済が行われます。万が一スマホを紛失した場合、新しいスマホを手に入れたら再度同じクレジットカードを登録するだけで、新しいスマホと紐付けされることになるため、カードの再発行は不要です【図2】。もちろん、**前提として「スマホに画面ロックを行うこと」が必要**です。だからこそ、**スマホそのものをしっかり守ることをお忘れなく！**

スマホ特有の「アプリ」対策は？

スマホは従来の携帯電話とは異なり、電話以外にもさまざまな用途で使えることが大きな特徴です。ただ、無理に使いこなす必要はありません。「やりたいことがあれば、適宜その機能を拡張していく」くらいの心持ちで十分です。

スマホを電話やインターネット検索など基本的な用途以外で使う際には、「アプリ」と呼ばれるスマホ用のソフトウェアをダウンロードする必要があります。実は**スマホのアプリこそ、スマホのリスクの大部分を占めています。**特にAndroidにおいては「誰もがアプリを作り、提供できる」という自由度がある反面、悪意あるアプリもそれなりに存在します。スマホがおサイフや銀行の窓口にもなるキャッシュレス時代、このリスクが無視できない状況にあります。

Androidをご利用の方は、まず画面ロックに加え、悪意あるアプリが登録されるのを防ぐ設定を確認しましょう。「設定」からセキュリティ／プライバシーなどにある「提供元不明のアプリ」が「オフ（許可しない）」になっていることを確認します【図3】。これはGoogleなどのアプリストアに存在しないアプリをインストールさせない設定で、こうしておけば「○○Pay」の公式アプリにそっくりな、悪意ある偽アプリが防げます。誰かに「セキュリティのため」と説明されても、この設定はオンにしないようにしてください。それこそが、あなたをだます攻撃者のテクニックかもしれません。

その上で、あなた自身もだまされないようにしなければなりません。あなたのスマホのメールボックスに「荷物を届けましたが不在でした。再配達には…」というメッセージが届き、そこにリンクが張られていたとします【図4】。そのリンクをクリックすると、たまたまあなたが口座を持っている銀行名のWebサイトが開きます。そこでログイン画面が開いたので、自分のログインIDとパスワードを入力して確かめてみると…。実はもう、あなたはだまされてしまっているのです。

そもそも不在通知のメールから銀行のWebサイトに遷移するのはおかしいのですが、それでもなんとなくだまされてしまうのではないでしょうか。実際にこのような

攻撃は問題になっており、高齢者ならずともだまされてしまうことが多々あります。

問題は、銀行のＩＤとパスワードが漏れてしまうことで、口座にある資産が根こそぎ持っていかれてしまう可能性があることです。インターネット越しのやり取りでは顔も見えませんので、ＩＤとパスワードだけが頼りです。「お金に関係するインターネットサービス」を、ＩＤとパスワードだけではなく「２段階認証」で守るべきである理由はここにあります。

【図３】Androidで悪意あるアプリが登録されるのを防ぐ設定

設定から「セキュリティ」→「不明なアプリをインストール」をタップ

ここに表示される項目はすべて「許可しない」とする

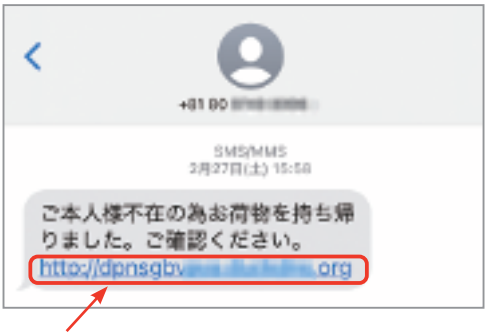
少なくとも、お金関係のサービスに関するパスワードだけは、これまで使い回してきたパスワードとは異なる、ちょっとだけ豪華なものにしてあげてください。これだけで、安全性はかなり変わるはずです。

「見分けてやろう！」という気持ちを捨てよう

情報を盗むため、悪意をもったハッカーなどの攻撃者は本物そっくりなＷｅｂサイトや本物そっくりなアプリを作って、そこになんとか誘導し、ＩＤとパスワードを入力させようとします。いわゆる「フィッシングサイト」と呼ばれる偽のＷｅｂサイトは、もはや見分けることができないほど精巧に作られることが増えてきました。

以前なら、例えば日本語がおかしいなどのヒントがあったかもしれません。しかし、Ｗｅｂサイトやアプリはデジタルなものであるため、労力をかけずとも、本物と寸分たがわぬものが複製できてしまいます。もはや「見分けよう」と思うことは無駄で、**「人間には見分けられない」という前提で考えたほうが賢明**です。

【図４】ＳＭＳで届いた偽の不在通知の例



偽のWebサイトに誘導するリンクが貼られている。絶対にタップしてはいけない！

偽サイトに引っ掛からないための秘訣は「もはや何も信じない」です。例えばＳＭＳ（Short Message Service：ショートメールともいう）やメールにどんな文言が書かれていようと、どんなに急がせるような内容でも、Ｗｅｂサイトにつながるリンク先が記載されていたら、それが何であろうと「信じない」。実はこれくらいしか対策はありません。

そうは言っても、銀行などから緊急の連絡があるかもしれませんよね。そういう時は、ＳＭＳやメールに書かれたリンク先をタッチしてＷｅｂサイトを開くのではなく、過去に自分の手で記録したブックマークから、自分の手で開いてみてください【図５】。最初だけは、公式の配布物などに印刷されたＵＲＬを手で打つことをお勧めします。**二次元バーコード（ＱＲコード）**をスキャンするのも良いのですが、**悪意ある人が上からシールを貼って別のサイトに誘導していないかを念のためチェック**してくださいね。もしそのＷｅｂサイトに緊急のお知らせが無かったとしたら、送られてきたＳＭＳやメールは〝偽〟だったということになるはずです。

偽サイトを判断するのは無理ですので、「最初から信頼できる方法で正規のWebサイトをブックマークしておき、自分の手で見にいく」ことが重要です。

スマホもパソコンと同様「アップデートが重要」

もう1つ、スマホがおサイフになる時代に簡単にできるセキュリティ対策をお教えします。それは「アップデート」です。

パソコンやスマホは絶えず進化しています。それと同時に、少しずつプログラムなどの修正が行われています。従来の電化製品であれば、不具合が残ったまま発売されることなどあり得なかったかもしれません。しかしパソコンやスマホは非常に高機能であるがゆえに、発売した後に見つかる不具合、特にセキュリティ的な問題である「脆弱性（ぜいじゃくせい）」と呼ばれる不具合が見つかることがあります。これは機能的な不備というよりも、悪意をもった攻撃者がパズルを解くようにプログラムの問題点を見つけ出し、異常を引き起こすようなもので、IT機器である以上、完全に防ぐことは非常に難しいものです。

この不具合を修正するのが、スマホやアプリのプログラムを最新の状態に更新する「アップデート」です。パソコンの中にWindowsなどのOS（Operating System）が入っているように、超小型のパソコンであるスマホの中にもOSが入っています。iPhoneなら「iOS」、Androidなら「Android OS」などです。**OSやアプリのアップデートは必ず適用するようにしてください。**多くの場合、自動でアップデートが行われるはずです。

ただし、Androidをお使いの方には少々問題があります。多くの場合、NTTドコモやau、ソフトバンクなどが販売しているAndroid端末ではアップデートまでに非常に時間がかかったり、アップデート情報が提供されなかったりします。このこともあるので、**できる限りスマホは「2年」をめどに、最新のものに買い換えることをお勧めします。**

日本人は物を大切にし、長く使うことが美徳とされるのは重々承知していますが、こと**スマホに関しては「古い＝危険」**と考えていいです。最近のスマホは安価になってきましたので、安全のためだと割り切って乗り換えていきましょう。

無理に最新機能を使う必要はない。でも1回は触ってみて！

ここまで説明すると「やっぱりスマホじゃなくて、財布でいいのでは？」と思われたかもしれません。これに関しては無理をせず、使いやすいほうを選択していただければと思います。しかし、できれば1度くらい試しに使ってみるのもいいでしょう。

「スマホだと怖い」という気持ちもあるでしょう。しかし現金の入った財布であっても、失くすリスクや落とすリスク、誰かに奪われるリスクはあります。

スマホであれば、失くしても落としても「画面ロック」さえ行っていれば、そう簡単には使われることはありません。奪われたとしても、相手がまごまごしている間に、遠隔操作により画面ロックや情報の消去をすればいいだけ。対処すべき部分が異なるだけで、便利さはかなり向上するのではないかと思います。それを一度体感してしまえば、キャッシュレス時代をより実感できるかもしれません。

スマホも財布も失くしては困る物。失くせない物を1つにまとめることは、合理的なはずです。今回取り上げたほんの少しのルールを守り、ぜひ、スマホをもっと活用してみてください。

【図5】
ブックマークの例（iPhone）

郵送されてきたお知らせや案内など確かな配布物に記載されている正規のWebサイトのURLを「自分の手で入力」して正規のWebサイトを開いた後、「ブックマーク」をつけておく