キャッシュレス時代のITの基礎知識 >>> 第1回

加速するデジタル化。現金からキャッシュレスの時代へ

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。

加速するデジタル化、キャッシュレス化の流れ

多くの人が「IT」の恩恵を受けられる時代になりました。インターネットが各家庭、そして小さな企業にも行き渡り、前世紀とは比較にならない超高速な接続環境を比較的安価で手に入れることができます。「ITなんて分からないよ」と言う方の手にも、超小型のスーパーコンピューターとも言えるスマートフォンが握られています。地方の商店であっても、インターネットとスマートフォン、デジタル決済を活用することで、世界中から注文を受け付けられるようになったのです。

「インターネットは個人を解放する」と表現している方もいました。インターネットをはじめとするIT技術で、人生が変わったという方もいるのではないでしょうか。

そして今、新型コロナウイルス症候群の影響で、さらなる変化の波が押し寄せてきています。2021年は、「ニューノーマル時代」を本格的に考えなければならないでしょう。ニューノーマル時代とは、ITを活用し、インターネット上で経済を回すことにほかなりません。重要なのは、**キャッシュレスをはじめ、新しい技術をいかに安全に使うか**ということです。

キャッシュレスとは「いかに私たちの経済活動をデジタルに置き換えるか」とも考えることができるでしょう。デジタルへの置き換えは既に身近なものとなっており、例えば多くの銀行はインターネットバンキングサービスを提供し、窓口に並ばずとも送金や残高確認ができるだけでなく、もはや紙の通帳を廃止したり、有料化したりとデジタル化の方向にかじを切っています。

「デジタル化」の〝鍵〟となるのは、ICチップに機能を詰め込んだ1枚の「マイナンバーカード」かもしれません。見た目は会員番号が印刷された、街中でよく見るプラスチックのポイントカードにしか見えませんが、このカードはIT技術とセキュリティ機能を詰め込んだスマートカードです。将来的にはこのカードが健康保険証や免許証を取り込み、マイナンバーの機能とともに、デジタル時代の本人認証機能を一手に引き受けるはずです。

……と、近未来の話をする前に、今回はもっとも身近な「お金」とITを巡る基本的な話を取り上げます。本連載ではなるべく平易に「ITなんて分からないよ」と言う方のために、まとめていきたいと思います。

既に身近にあるキャッシュレスとデジタル化

もしかしたら、ITとは「余計なことをするもの」という印象の方も少なくないのかもしれません。これまで通りのアナログなやり方で問題がないのなら、これまで通

>>> キャッシュレス時代のＩＴの基礎知識

【図１】ＱＲコード決済のイメージ

りのやり方でやりたいという意見も分かります。しかし、ＩＴは正しく活用すれば、必ず私たちの生活にプラスになるはずです。少なくとも、ＩＴを推進しようと考えている人たちは、この仕組みがこれまでの煩わしさを減らし、生活を豊かにするために活動をしているはずです。

例えばキャッシュレスの元祖とも言うべき「クレジットカード」を考えてみましょう。日本では現金主義が根強いため、クレジットカードの利用はまとまった金額の時のみに限定している方もよく見受けられます。クレジットカードの利用を避ける方の多くは「いくら使ったか分からないから怖い」と考えているはずです。**問題はこの「怖い」という感覚。**ＩＴセキュリティが面倒くさい、ＩＴがなじまないと考えている理由のほとんどは、この「怖い」にあると推測されます。本連載の目標は、この「怖い」のコントロールにあります。

それでは、クレジットカードをはじめとするキャッシュレス決済の利点を考えてみましょう。まず、ここ数年で一気に、身近な場所で現金以外の決済が利用できるようになったと思いませんか？　街中のコンビニエンスストアでもクレジットカードやプリペイドカード（先に入金してから使うカード）、「～Ｐａｙ（ペイ）」などと呼ばれるＱＲ（キューアール）コード決済が利用可能になりました**【図１】**。

首都圏近辺なら、電車やバスに乗るのにＳｕｉｃａ（スイカ）やＰＡＳＭＯ（パスモ）などプリペイド型電子マネーが普及し、切符を買う人も少なくなりました。いまやＳｕｉｃａなどを利用すると、紙の切符よりも運賃が安くなる時代です。これだけでもキャッシュレス決済のメリットはあるでしょう。

それだけではありません。クレジットカードやデビットカード（口座から直接現金が引き落とされる）を扱う**「ペイメントカード事業者」と呼ばれる会社は、不正利用を検出する仕組みを用意**しています。

私は以前、アメリカにあるＶＩＳＡのデータセンターを取材したことがありますが、全世界で日々行われている決済を１カ所のデータセンターで処理しています。そこでは、例えば日本に住む人が持つクレジットカードが、なぜか中南米で決済された情報が挙がってくると、即座に決済を止める等の仕組みが動いています。不正に決済が行われたとしても、ペイメントカード事業者による補償が行われるので、この点においては現金以上に安全であると言えるでしょう。

もう一つ、最近の電子マネーに関しても安全策が施されています。ｉＰｈｏｎｅ（アイフォーン）で使用される「Ａｐｐｌｅ Ｐａｙ（アップル ペイ）」をはじめとする各種電子マネーは、単にクレジットカードの決済を電子化したわけではありません。クレジットカードはオンラインで決済できる便利なものですが、そもそもクレジットカードは、店舗などで「対面で」処理するために作られたもの。そのため、オンラインの「非対面で」の決済には、やや課題が残されているのが実情です。

以前はクレジットカード番号が漏えいすることや、対面決済時に店員が不正にカード番号を記録することで、あなたではない誰かがインターネット上でなりすまし、クレジットカード決済ができてしまうことが問題になりました。カード番号と氏名、有効期限と裏面に記載された３桁程度の数字が分かれば、あなたのお金を奪うことができてしまうのです。

この問題は、決済にクレジットカード番号そのものを利用しているからと言えるでしょう。クレジットカードよりも新しい**「トークン化技術」を使った電子マネー決済では、クレジットカード番号とは別に用意された取引コード（トークン番号）を利用**します**【次ページの図２】**。トークン化技術では、その時１回だけのパスワード（ワンタイムパスワード）が使われます。このワンタイムパスワードが、即ち「取引コード（トークン番号）」です。決済情報としては、取引コード（トークン番号）だけをインターネット上に流すため、万が一その経路を盗聴されたとしても、また店舗で店員が悪意を持ってそれを眺めようとしても、他人のカード情報を悪用することができないようになっています。

このように、**ＩＴはより安全になるように努められています。特に「お金を守る」点に関しては、事業者側も非常に気をつか**

【図2】電子マネー決済で使われるトークン化技術のイメージ

インターネット上はクレジットカード番号そのものが流れず、
盗聴されても、もとのクレジットカード番号を復元できないため、安全に利用できる。

＜ トークン化のメリット ＞

・インターネット上にはクレジットカード番号そのものが流れず、 盗聴されたとしても無意味な文字列しかない。
・サービス事業者も顧客のクレジットカード番号そのものは分からず、情報漏えいしても取引コード（トークン番号）の再利用はできない。

ってシステムを作り、運用しています。

電子マネーやクレジットカードについても、紛失時や不正利用に対する補償が用意されていることが多く、**正しく利用している限りでは、現金よりも安全**と言えるかもしれません。

知らなかったでは済まされない？デジタル化のリスクをどう考えるか

ただし、クレジットカードをはじめとするキャッシュレス決済のメリットには、**あくまで「正しく利用している限り」という条件が付きます。**

デジタル化が進んでいる現代は、なんでもインターネットとスマートフォンでできてしまう時代です。インターネットバンキングで遠く離れた場所へも顔を合わせることなく送金できるのは便利ですが、それは裏を返すと「あなたが誰かをはっきりさせないまま、なんでもできてしまうかもしれない」という危うさも持っています。「ＩＴが苦手」と言う方が一番気にしているのは、そんなリスクがあるからかもしれません。

実際、その不安は現実のものになっています。インターネットバンキングなどのシステムを作るプログラマは、利用者の動きを想定しながらシステムを作り上げます。口座番号を間違って入力した時にちゃんとエラーが表示されるのは、プログラマが最初から想定できている使い方ですので、問題はありません。しかし、世の中にはあっと驚くような方法で、それを欺こうとする悪意ある者もいます。

例えば２０１９年７月、大手コンビニエンスストアチェーンのセブン-イレブンで利用可能だったＱＲコード決済の「７ｐａｙ（セブンペイ）」で事件が起きました。セブン&アイ・ホールディングスのグループ企業「セブン・ペイ」が運営する電子マネーで、サービス開始直後、利用者に身に覚えのない取引が多発しているという情報が広まりました。

原因の一つは、「７ｐａｙ」を利用する際に登録したＩＤ（身分証明）とパスワードが、第三者に推測できてしまったことが挙げられます。推測された要因としては、パスワードが弱かった、全く別のサービスで情報漏えいしたＩＤとパスワードでたまたまログインできた（利用者がパスワードを使い回していた）などがあります。

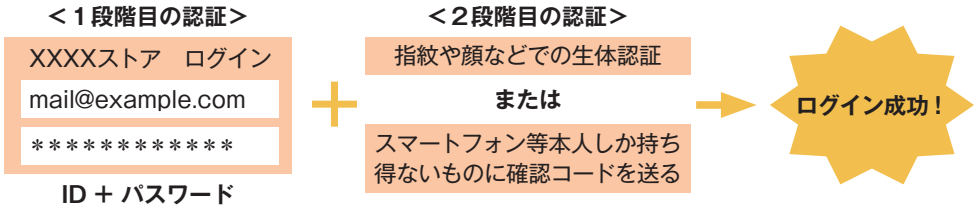
それ以外にもシステムの不備を突き、パスワード無しで他人になりすましができてしまうなど、利用者側では何も対策できないパターンもありました。これは、システムを作る人間が「パスワードはその本人しか知らないはずだ」と思い込んでいたことが原因かもしれません。皆さんももしかしたら、パスワードを単純な誕生日などにしていませんか？

とはいえ、７ｐａｙの事件は「７ｐａｙの利用者が被害に遭う」という、単純な構図ではありました。ところが２０２０年９月に発生した、複数の電子決済サービスが不

>>> キャッシュレス時代のＩＴの基礎知識

【図３】２段階認証のイメージ

万が一パスワードが漏れたとしても、あなたが持つスマートフォンに届く確認コードがログインに必要となるため、不正ログインを防ぐことができる。



正引き出しに遭ったという事件は、サービスを利用していなかったとしても、銀行口座から大事なお金が盗まれてしまうという、非常に悩ましい構図でした。

この事件は、当初ＮＴＴドコモの決済サービス「ドコモ口座」で発生したことが注目されたため、もしかしたらそこで情報が止まっていて「自分は使っていないから安心」と思っている方も多いでしょう。しかし、直後にＰａｙＰａｙ（ペイペイ）やＬＩＮＥ Ｐａｙ（ラインペイ）などでも同様の不正引き出しが発覚し、セキュリティ業界が騒然としました。根本的な原因は銀行口座との接続部分にあり、第三者が入手した銀行口座情報をもとに、電子決済サービスを勝手にひも付けることができてしまう点にありました。つまり、**銀行口座を持つ方ならば、各種決済サービスを使っていなくても被害に遭う可能性があった**のです。これも、銀行側の接続部分に問題があるため、利用者が気を付けていても防ぐことはできませんでした。

じゃあ、どうしたらいい？

では、私たち一般の利用者は何をすべきでしょうか。まず皆さんに強くお勧めしたいのは、**特にお金に絡むサービスにおいて「〝あなたがあなたであるか〟を判断する仕組み」を積極的に活用**してくださいということです。具体的には「２段階認証」と呼ばれる仕組みです。詳細は次回以降、改めて解説しますが、**２段階認証はＩＤとパスワードだけで本人かどうかを判定するのではなく、もう一段階加え、指紋や顔などでの生体認証や、スマートフォンなど本人しか持ち得ないものに確認コードを送ることで、本人を特定するという仕組み**です【図３】。

もう一つ**重要なのは「知る」ということ。**一般の人が気を付けるべき攻撃、特に金銭に直接絡むサイバー犯罪では、特定企業の特定情報や特定人物を狙うような「標的型攻撃」よりも、不特定多数を対象とし、広く攻撃を行う「ばらまき型攻撃」が犯人にとって効果的です。おそらく皆さんもそれを迷惑メールなどで体感しているのではないでしょうか。これに対しては、振り込め詐欺対策と同様、**ニュースに敏感に反応し、敵のやり口をあらかじめ知っておくということが、最大の防御**になります。

例えばＱＲコード決済に関しては、日本よりも先に普及していた中国において、店舗が用意したＱＲコードの上に勝手に別のＱＲコードを貼り付ける手口が話題になりました。ＱＲコードには、送金先の情報が埋め込まれています。ですから「別のＱＲコード＝別の送金先」ということになります。あらかじめそれを知っておけば、決済時にＱＲコードが不正に書き換えられていないか、気を付けることもできます。

日本では、代金の支払いでＱＲコードを利用するには、スマートフォンのアプリをいちいち立ち上げなくてはなりません。その点から、**個人的におススメしたいキャッシュレス決済は、**ＱＲコード決済よりも便利で安全、そして多くの人が持っているＳｕｉｃａやＰＡＳＭＯなど**交通系のプリペイド型電子マネーを軸とした利用**です。これであれば、定期券として所持しているであろうＳｕｉｃａやＰＡＳＭＯをそのまま電子マネーとして利用できますし、紛失時もそれなりの対応が受けられます。これで便利だと思ったのならば、怖いと思わずに次のステップに進めるのではないでしょうか。

２０２０年度は、確定申告もマイナンバーカードを活用した「ｅ-Ｔａｘ（イータックス）」において、青色申告特別控除額や基礎控除額が変更となり、電子的に申告すれば控除額が増え、納税額が減るという変化も訪れています。**ＩＴは「活用しなければ損」という時代**です。しかし、新しい仕組みをうまく活用するには、それなりに準備が必要でしょう。

ＩＴとは暮らしを便利にするものに相違ありません。そのためにはまず、事業者にシステムを正しく構築してもらい、サービスを強固なものにしてもらうのは当たり前。その上で、**私たち利用者もシステム、サービスに寄り添い、ほんの少しだけ協力することでグッと安全に活用できる**のです。

本連載では、その「ほんの少しの協力」を行うための知識を提供し、皆さんの周りにいる人に思わず教えてあげたくなるような「パスワードの作り方」などについて、取り上げていきたいと思います。