キャッシュレス時代のITの基礎知識 ≫ 第3回

プライベートでも使う パソコンとうまく付き合おう

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IT知識の基礎として、「パソコン」を取り上げたいと思います。

スマートフォン全盛時代とは言え、仕事ではパソコンを使うことがほとんどでしょう。加えて、ご自宅でも、メールや写真管理などはパソコンで行っているのではないでしょうか。年賀状を印刷したり、ちょっとした趣味のデータベースを作ったりと、今もパソコンは活躍しているはずです。インターネットショッピングや株の売買などで活用されている方もいるでしょう。

そこで、今や生活の一部になったパソコンのセキュリティについて考えてみます。

今、パソコンに起きていること

まず、パソコンが置かれている現状を知っておきましょう。皆さんにとってパソコンはおそらく「写真」や「動画」を置く場所であり、「メール」を読み、Google Chrome（クローム）やsafari（サファリ）といった「Webブラウザ（Webサーバに接続するためのソフト）」でインターネット検索をし、情報を見るためのものではないかと思います。キーボードがあり、大画面で情報を処理できるパソコンは、スマートフォンより活用の幅が広いはず。スマートフォンとの大きな違いは、大量のデータを保存し、処理できる機械であるということでしょう。

そこに保存されるデータは、家族の写真であり、思い出の映像だと思います。これらは世界中を探してもあなたしか持っていない、唯一無二のデジタル情報です。もはや写真はデジタルカメラで撮影するものであり、音楽や映像もモノとしてではなくデジタルデータで保存する時代です。

デジタルデータは複製が容易で劣化せず、高性能なCPUでさまざまに加工できることが特徴です。実は、それこそが利点であり、難点でもあります。なお、CPU（Central Processing Unit）とは、日本語で「中央処理装置」と訳される、言わばコンピュータの頭脳部分のことです。

今、CPUの難点が攻撃者に狙われています。皆さんは「ランサムウェア」という言葉を聞いたことがありますでしょうか。**ランサムウェアとは、**「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた言葉で、あなたが持つ唯一無二の、そして〝思い出〟でもあるデジタルデータを**勝手に暗号化し、「元に戻してほしければ、身代金を支払え」と恐喝する、非常に狡猾なコンピューターウイルス**です。「暗号化される」とはすなわち、見られないデータに変えられてしまうということです。

昨今は標的が個人から法人に移り、個人における大規模な感染はあまり聞かなくなったものの、この**ランサムウェアこそ、パソコンを使う上で絶対に避けなくてはならない攻撃**です。狙われているのはあなた

の思い出であり、万が一感染してしまい暗号化されたときには目も当てられません。単なるコンピューターウイルスのように駆除ができたとしても、大切な写真や動画といったデータは戻ってこないからです。

もちろん、身代金を払うという選択肢もないわけではありません。多くの場合、身代金はビットコインを始めとする仮想通貨が利用されます。仮想通貨には現金をやり取りするよりも〝足〟が付きにくく、日本国外からも攻撃、集金が可能になるという攻撃者側のメリットがあります。しかし、ほとんどの人にとって「ビットコインを用意して、指定の口座に振り込む」ことは難しいでしょう。ですので、まずはこのランサムウェアを〝未然に防ぐ〟ことを考えます。

シンプルなルール「新しいものはすべてよい」

ランサムウェア対策の最も簡単な方法は、「ハード、ソフトをすべて最新にする」ことです。

もし皆さんが「Windows 95」や「Windows 7」といった、古いＯＳ（Operating System：パソコンを動かすベースとなる基本ソフト）が動いているパソコンを今も使っていて、今後も使い続けたいのならば、今すぐ最新のパソコンに買い換えるようにしてください。もはやそれらはサポートされておらず、不具合があっても修正されない運命です。

日本人はモノを大事にするという美学があるのは重々承知しています。しかし、残念ながらデジタルの世界において、長く使い続けることにメリットはありません。古いものはすなわち「攻撃者が研究するための時間がたくさんあるもの」なのです。

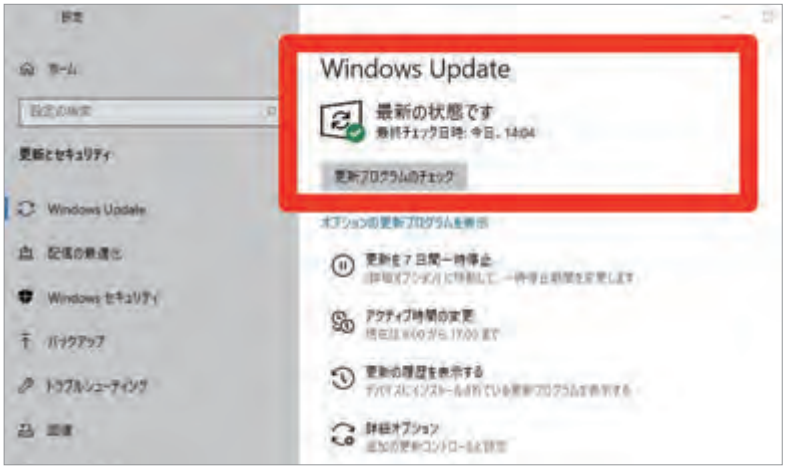
そして、最新のWindows 10やmacOSを使っている方は、設定のアップデートから、**常に最新の状態にアップデートされていることを確認**してください**【図1】**。特にアップデートが必要なのは、基本ソフトであるWindowsなどのＯＳ、そしてGoogle ChromeやsafariといったＷｅｂブラウザです。また、WordやExcel、PowerPointなど利用しているアプリケーションソフト（以下「アプリ」）も、なるべく最新のものにしてください。

多くの場合、アプリのメニューや設定から「アップデートを確認する」機能があるはずです。そこから簡単に最新版にすることができるでしょう。よく使っているにもかかわらずアップデートがないアプリや、そもそも大昔のアプリである場合、アプリの買い換えも検討してください。**最近ではブロードバンドルーター（ネットワーク同士を相互接続する機器）も狙われることが多く、こちらもできれば、3年おき程度に最新のものに買い換えることをお勧め**します。

なぜ「最新」が重要なのでしょうか。これは「脆弱性」と呼ばれる既知の不具合が修正されているからです。脆弱性とは機能的な不具合というより、攻撃者が〝裏技〟のような方法で見つけたプログラムの穴です。この脆弱性により、本来は動かないはずのプログラムが勝手に動いてしまうのです。例えば、あなたの大事なデータを勝手に暗号化してしまうような…。

だからこそ、すべてのＯＳ、アプリ、そしてブロードバンドルーターは「最新」にしておく必要があります。古いパソコンやブロードバンドルーターだと、そもそも最新のアップデーターが提供されていません。ここ3年ほどパソコンを買い換えていないという方は、後で述べる選択肢も含め、買い換えを検討してみてください。

【図1】Windows 10のアップデートの確認



Windows 10のアップデートは、「設定」の画面から「更新とセキュリティ」を開き、更新プログラムのチェックを行う。「最新の状態です」と表示されていればOK

【図3】OneDriveの「個人用Vault」

マイクロソフトが提供するクラウドストレージサービスOneDriveの「個人用Vault」にアクセスするためには生体認証を含む高度なセキュリティの仕組みを必要とする

【図2】クラウドの概念図

パソコンやスマートフォンがインターネットに接続することを図示するときに「雲」を使うことが多かったことから、インターネットの先にあるものを「クラウド」と呼ぶようになった

新しい考え方――クラウドを活用しよう

OS、アプリ、ブロードバンドルーターを最新にしたついでに、パソコンの使い方でもう1つ提案したいと思います。それは「クラウド」に関することです。

クラウドとは「雲」のことですが、ITの世界におけるクラウドとは、ネットワークの向こう側にあるサービスのことを指します【図2】。皆さんのパソコンには、ハードディスクなどデータを保存する機器が内蔵されているでしょう。最近では、これを「クラウド」つまりネットワークの向こう側に全部保存してしまうことができます。これを「クラウドストレージ」と言います。ストレージ（storage）は、保管、保存、倉庫などを意味します。**これからパソコンを活用するなら、クラウドストレージを活用することを強くお勧めします。**

その理由ですが、まず**クラウドストレージは「故障」に強い**です。パソコンのハードディスクは可動部分があるため振動に弱く、故障するとすべてのデータがなくなってしまう可能性が高くなります。

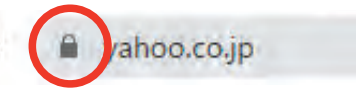
クラウドストレージの場合、多くはクラウドストレージサービス側で複数の故障対策が行われており、データがすべてなくなることはまれです（ゼロではないことに気を付けましょう）。そのため、例えばWindows 10であればマイクロソフトが提供するクラウドストレージサービス「OneDrive」を活用しましょう。無料でも5ギガバイトが利用可能です。

そして**クラウドストレージは、データの簡易的な「バックアップ」にもなります。**

先述のランサムウェア対策の1つとして、暗号化されたら困るデータを常にバックアップすることが挙げられます。とは言え、このバックアップというものはパソコンに詳しい人でも難しく、バックアップ用のアプリを買っても面倒くさく、なかなかうまくできないものです。クラウドストレージを利用しているのであれば、万が一、目の前のパソコンがランサムウェアに感染し暗号化されても、クラウドストレージ側に保存されたデータから復旧できる可能性があります。まずはここから、ランサムウェア対策を始めるのもいいでしょう。

特にOneDriveでは、「個人用Vault（ボルト）」という機能があります。パスポートや保険関係書類のような機密情報でも、この特別なフォルダなら生体認証やSMS（ショートメッセージサービス）コードで本人確認しなければ中身をのぞくことができず、デジタルの〝金庫〟として使うことができます。これを活用すれば、万が一離席時に誰かがあなたのパソコンを操作した場合でも、大事な情報を盗み見ることはできません（ただし、できる限り離席時は画面をロックしましょう！）。無料版でも3つまでのファイルを保存可能ですので、Windowsを利用して

【図４】HTTPSの場合に表示される錠のマーク



いる方は一度試してみてください。

パソコンならではの悩み――無料 Wi-Fi って危険なの？

もはや、パソコンはインターネットにつながらないと、何もできない時代になりつつあります。特に先に紹介したクラウドを活用する場合、インターネットにつながることは必須です。スマートフォンであればＳＩＭ（Subscriber Identity Module：契約者の電話番号やＩＤ番号等が記録されてされている小型カード）の契約情報をもとに、携帯電話回線でインターネットに常に接続されています。ほとんどのパソコンは無線ＬＡＮか有線ＬＡＮですから、外出先では公衆無線ＬＡＮや、ホテルならば有線ＬＡＮを活用することになるでしょう。

もしかしたら、皆さんも「公衆無線ＬＡＮは怖いから、つなげてはならない」という話を聞いたことがあるかもしれません。公衆無線ＬＡＮにつなぐとその瞬間にウイルスがやってきて、あなたのパソコンに感染してしまう――少々昔ならば、ない話ではありませんでした。が、結論から言うと、今ではそこまで気にする必要はないと私は考えています。もちろん、先に紹介した「最新の状態にする」ことを行っていれば、という前提条件はあります。

その昔、メールを受信するためにはWindows Live メールなどメール専用アプリを使い、ＰＯＰ３と呼ばれるメール受信のための特別な方式で通信が行われていました。実は昔はこのメールやり取りの通信は暗号化されておらず、第三者が簡単にパスワードを抜き取ることができました。Ｗｅｂサイトを見るのも同様で、暗号化されていない通信でやり取りしていたため、誰がどこのサイトを見ているかが分かってしまいました。だから、公衆無線ＬＡＮのような信頼できない通信経路を使うことは、あまりお勧めできませんでした。

しかし、**もはや多くの通信は暗号化されています。**メールもほとんどの方はGmailなどＷｅｂブラウザメールサービスを使い、暗号化が行われる「HTTPS」という方式で通信が行われているでしょう。HTTPSはＷｅｂブラウザで錠のマークが表示され、ほとんどのサイトが暗号化対応を終えています**【図４】**。このようなサイトであれば、公衆無線ＬＡＮであっても簡単には盗聴ができません。ですので、カフェや空港などで提供されている公衆無線ＬＡＮも、安全に活用することができます。

逆に、今もメール専用アプリを使ってメールをやり取りしていて、そのメール設定も5年近く変更していない（暗号化しないＰＯＰ方式を利用したままになっている）場合、公衆無線ＬＡＮなどの見知らぬ通信経路を利用することはお勧めしません。こちらでも、やはり「最新」が重要になります。できる限り、メールはＷｅｂブラウザで見る仕組みに移行することをお勧めします。

パソコンもスマートフォンも使いこなす必要はない

最近のパソコン事情はかなり進化しており、例えばこれまでであれば必須のアイテムだったWordやExcel、PowerPointといったアプリについても、今ではGoogleが〝Ｗｅｂブラウザ上で〟提供する「Google ドキュメント」「Google スプレッドシート」などがクラウド上で提供されています。保存先もクラウドで、Ｗｅｂブラウザがあればそれだけで（無料で）活用できます。クラウドの利点として、パソコンで作業をした後、出先でちょっと修正したいならそのままスマートフォンで行えることも挙げられます。

前回までにお伝えしているように、これらの最新機能はすべてを使いこなす必要は全くありません。使えるものから、使えるだけを活用するだけでも十分です。もし今、使っているパソコンが古く、買い換えに躊躇する場合は、タブレット端末に移行してしまう方法もあるでしょう。

タブレット端末は管理が楽で、パソコンよりも安価。しかも、クラウドを前提としているのでスマートフォンとの親和性も高いことがメリットです。今ではスマートフォンの延長であるタブレット端末である「Chromebook」や「iPad」なども人気で、自動的にアップデートが行われる上にクラウドですべてが完結しており、メールやＷｅｂだけなら、これでも十分かもしれません。