特別寄稿

「知らなかった」では済まされない情報セキュリティ

～意識を高めるために自宅のパソコンでやるべき対策～

増井技術士事務所代表　増井敏克

増井技術士事務所代表
増井敏克（ますいとしかつ）
奈良県出身。大阪府立大学大学院修了。技術士（情報工学部門）。テクニカルエンジニア（ネットワーク、情報セキュリティ）、その他情報処理技術者試験に多数合格。ITエンジニアのための実務スキル評価サービス「CodeIQ」にて、情報セキュリティやアルゴリズムに関する問題を多数出題している。著書に『おうちで学べるセキュリティのきほん』『プログラマ脳を鍛える数学パズル』（ともに翔泳社）、『シゴトに役立つデータ分析・統計のトリセツ』（ソシム）がある。

家庭のパソコンでも必須のウイルス対策

情報漏えいや不正アクセスといったニュースを聞かない日がないくらい、情報セキュリティに関する事件がたくさん発生しています。企業や組織でこういった事件が発生すると信用の失墜により多大な影響が出るため、セキュリティは何よりも優先すべき事項になっています。

仕事で使うパソコンであれば、ウイルス対策ソフトが導入されていない会社はほとんどないでしょう。しかし、自宅のパソコンになると導入していない人がいるかもしれません。なぜ使わないのかを尋ねてみると、「怪しいメールは開かないし、怪しいサイトは閲覧しないから大丈夫」という答えが返ってきます。

しかし、最近の標的型メールの手口を見ていると、「怪しい」と判断できないメールが増えています。個人を相手に標的型メールはないだろう、という声も聞こえてきますが、最近はメールから感染するだけではありません。

官公庁だけでなく、企業の公式サイトなどでも改ざん被害が次々と報告されています。改ざんにより、ウイルスが仕込まれてしまうと、利用者が該当のサイトにアクセスするだけでウイルスに感染してしまいます。つまり、怪しいサイトかどうかの判断は意味がありません。

もちろん、怪しいサイトは今でも多く存在します。そのようなサイトにはアクセスしないと思っている人でも、怪しいサイトをどうやって判断しているでしょうか？

URLを見て判断できれば良いのですが、「短縮URL」が使われる場面も増えています。SNSなどに投稿できる文字数を増やせる便利な仕組みですが、URLを見ただけではリンク先が怪しいかどうか判断できません。

何よりも問題なのが、ウイルスに感染したことに利用者が「気付かない」ことです。昔はウイルスに感染させる目的が技術力のアピールや愉快犯であり、利用者の画面に見た目の変化がありました。現在は利用者が気付かないうちに情報を盗み出す、金銭を奪う、といった目的に変わってきており、画面には何の変化もありません。

金銭を奪う方法として有名なのが銀行の不正送金です。警察庁の調査（https://www.npa.go.jp/cyber/pdf/H280303_banking.pdf）によると、2015年度は被害額が30億円を超え、メガバンクだけでなく地方銀行でも被害が発生しています。しかも、被害額の半分以上は個人の口座で発生しています。ウイルスに感染すると、通常の振込操作を行ったときに、振込先や金額を変更して送金できてしまいます。

ウイルス対策ソフトの導入は必須ですが、限界もあります。攻撃者が新種のウイルスを作成するときには、一般的なウイルス対策ソフトで検出されないことを確認したうえで配布できますので、利用者側がウイルス対策ソフトを導入しても検出できません。つまり、既存のウイルスに対応するためにパターンファイルを最新にすることは必要ですが、すべてのウイルスから防げるものではない、という認識を持っておくことは重要です。

ウイルス感染を防げないという視点に立つと、バック

アップの取得についても意識を変える必要があります。ディスクの故障やファイルを誤って削除してしまうことを意識してバックアップを取得しているかもしれませんが、ウイルスに感染してファイルを破壊されたことも考慮に入れるべきです。このとき、外付けのハードディスクなどを接続してバックアップしていると、ウイルスがアクセスしてバックアップも失ってしまう可能性があります。DVDなど書き換えできないメディアを使用して、世代を管理した保存も意識しておきましょう。

OSやアプリケーションは常に最新の状態に

会社であれば定期的にWindows Updateなどを適用するような指示があるかもしれません。しかし、自宅のパソコンは更新作業が面倒なため、更新があっても通知しないように設定している人がいます。

WindowsといったOSだけでなく、文書作成や表計算ソフト、Webブラウザや PDF閲覧ソフトなど、パソコンには多くのソフトウェアが導入されています。ソフトウェアは人間が開発したものですので、不具合をなくすのは大変です。使っていて問題に気付くようなバグもありますが、使用する上で問題がなくても攻撃者が悪用に使える不具合を「脆弱性」と呼びます。

脆弱性が存在するソフトウェアを使用していると、管理者権限を乗っ取られ、情報の漏えいにつながる可能性があります。個人のパソコンであれば重要な情報は保存していないと思っているかもしれませんが、アドレス帳や写真などが漏えいすると、友人関係に溝ができてしまうかもしれません。

ソフトウェアに脆弱性が発覚すると、開発元から修正プログラムが提供されることが一般的です。自動で更新できる設定が可能であれば、可能な限り設定しておきましょう。これはパソコンに限った話ではありません。最近はスマートフォンやタブレット端末を使用している人が多く、自宅ではパソコンを使っていない人も多いかもしれません。スマートフォンやタブレット端末もパソコンと同じようにウイルス対策やソフトウェアのアップデートが必要です。

注意が必要なのは、ソフトウェアの修正プログラムが提供されない場合です。製品のサポート期間が終了した、修正プログラムの適用により他のソフトウェアが動作しなくなる、開発元が倒産した、などの理由で更新できないことに気付かずに使っている可能性があります。

（図1）MyJVNバージョンチェッカ

更新するためには、自分が使っているソフトウェアを把握しておかなければなりません。購入時にすでに導入されていたソフトウェアは意識していない人も多いのではないでしょうか？　使っているパソコンやスマートフォンに導入されているアプリケーションなどを定期的に確認し、最新のバージョンが導入されているか確認することをオススメします。独立行政法人情報処理推進機構（略称＝IPA）により提供されているMyJVNバージョンチェッカ（図1／http://jvndb.jvn.jp/apis/myjvn/）のようなソフトウェアを使用して、最新バージョンになっているか調べる方法もあります。

普段からニュースなどに注目しておくことも重要です。使用ソフトウェアの新しいバージョンが登場していないか、情報漏えい事件が発生したらその原因は何なのか、というようにニュースで報じられている内容をチェックすることで、世の中の傾向が見えてくることがあります。

パスワードを覚えるのはもう古い？

自宅でパソコンやスマートフォンを使う人が増えた背景には、インターネット上に便利なサービスが次々と登場したことが挙げられます。メールやSNS、ブログなど複数のサービスを使い分けている人は多いのではないでしょうか。このとき、利用者の認証に使われるのが「パスワード」です。「長いパスワードを使う」「複雑なパスワードを使う」「定期的に変更する」など様々な対策が言われてきましたが、いまだに他人による乗っ取りやなりすましが後を絶ちません。単純なパスワードを使う

ことも問題ですが、複数のサービスでパスワードを使いまわしている人が多いことが話題になっています。

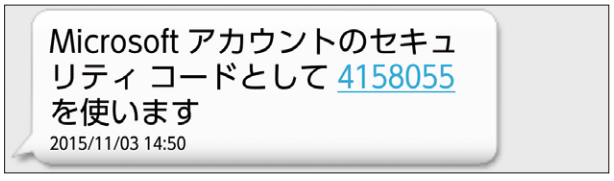
パスワードを使いまわすことの問題点は、パスワードが漏えいすると他のサービスにも次々とログインできてしまうことです。フィッシング詐欺による偽サイトでのIDやパスワードの入力や、有名なサイトでの情報漏えい事件など、パスワードが漏えいする事案は数多く発生しています。こういったパスワードの一覧が攻撃者の手に渡り、不正なログインを繰り返すことは「パスワードリスト攻撃」とも呼ばれます。

パスワードが漏えいすると、ウイルスに感染させなくても、不正送金に悪用できる可能性もありますし、SNSに不適切な投稿が行われて友人を失ってしまう可能性もあります。では、どうやってパスワードを管理すればよいのでしょうか？　パスワードの使いまわしを避けるには、「パスワード管理ソフト」を使う方法があります。長く複雑なパスワードを人間が覚えるよりも、パスワード管理ソフトに記憶させておけば、使用しているサービスが増えてもパスワードを使い分けられます。

しかし、フィッシング詐欺でIDやパスワードを盗まれる、利用しているサービスそのもので情報漏えいが発生する、といった場合、パスワードを使い分けても該当のサービスについては防げません。ログイン履歴を見ることで気付く可能性はありますが、チェックしている人は少ないでしょう。

このような被害を防ぐためには、「二段階認証」（図2）や「二要素認証」を使うことが有効です。銀行などはIDとパスワードだけでなく、パスワードカードを配布する場合があります。振込などの重要な処理を行うときに、パスワードカードに表示される数字を入力しないと処理できない仕組みです。最近のインターネットのサービスではスマートフォンのアプリを使った方法や、左下の図のようにログイン時にメールやSMSでワンタイムパスワードを通知するといった手法も多く使われています。

（図2）Googleによる二段階認証（メール通知）（上）と、Microsoftによる二段階認証（SMS）（下）



二段階認証や二要素認証に対応しているサービスでは、設定しておけばパスワードが漏えいしてもログインするときにもう一つのステップが必要です。本人以外はログインできませんし、パスワードが漏れたことに気付けるかもしれません。面倒だと思うかもしれませんが、最初に設定さえしてしまえば、同じパソコンの同じブラウザでログインしている限り、何度も入力しなくて済むサービスが多く、それほど手間ではないことが一般的です。

無線LANは便利だが安易に接続すると危険

自宅ではデスクトップパソコンよりもノートパソコンやタブレット端末を使う人が多いのではないでしょうか？　無線LANを使えば場所を決めずに作業できますし、場合によっては、光ファイバーなどの有線は使わず、携帯電話事業者などの回線だけを使っている人がいるかもしれません。街の中でも、公衆無線LANが普及してきました。携帯電話事業者が提供する無線LANもありますし、独自の無線LANを設置してIDとパスワードを教えてくれるお店もあります。

このときに気になるのが無線LANの安全性です。無線LANには誰が接続しているのかわかりません。フォルダの共有設定を有効にしていると、同じネットワークに接続している人が他人のパソコンの中にあるファイルを閲覧できるかもしれませんし、ウイルスなどを送り込まれる可能性もあります。公共の場で無線LANに接続するときは、共有設定などを確認するようにしましょう。

無線の電波は盗聴されている可能性もあります。暗号化の設定が必要だという認識は広まっていると思いますが、その強度について正しい認識を持っておきましょう。少し前によく使われていた暗号方式であるWEPは、現在は短時間で解読する方法が発見されています。ゲーム機などWEPにしか対応していない端末もありますが、

基本的には使用しないようにしましょう。

WPA2などの暗号化方式を選んでいれば安心だと思っている人もいますが、暗号化されているのはあくまでも「パソコンなどの端末」から「無線LANのアクセスポイント」までです。偽のアクセスポイントを設置されている可能性もあります。自身が管理するアクセスポイント以外を使用するときは、危険性を理解したうえで、以下に記述するような鍵マークの確認などを行うようにしてください。

鍵マーク、確認してますか？

無線LANを使用しているかどうかに関わらず、重要なデータの送受信に暗号化通信は必須です。インターネット上で商品を購入する、問い合わせフォームに個人情報を入力する、など「鍵マーク」（正確には「錠マーク」ですね）を確認する意識は高まってきたように思います。

無線LANの通信で暗号化されている範囲はWebサイトの閲覧で暗号化されている範囲とは異なります。Webブラウザに鍵マークが表示されているとき、暗号化されるのはあくまでも「Webサイトの閲覧」による通信だけです。つまり、Webサイトの閲覧以外の通信、例えばメールソフトを使ってメールを送受信していると、その通信は暗号化されておらず、メールサーバーとの認証に使われるIDやパスワードがそのままネットワーク上を流れていたりします。

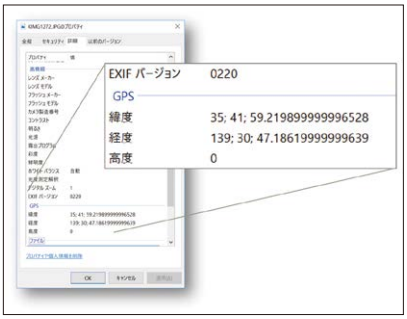
なお、Webサイトの閲覧時に鍵マークが表示されているからといって安心できるわけではありません。最近では、フィッシング詐欺サイトでも暗号化通信に対応しており、鍵マークが表示されているものが増えています。

このとき、証明書を確認することは一つの対策です。鍵マークは暗号化通信を表現しているだけでなく、「サーバーが認証を受けていること」を示す役割も果たしています。つまり、アクセスしているサイトが「信頼できる認証局により認証された正当なサイト」であることが鍵マークをクリックすることでわかります。

そのサイトがどのように認証されているか、認証方法により証明書の信頼度が異なります。ブラウザのアドレスバーが緑色に変わる「EV SSL証明書」はわかりやすいでしょう（図3）。EV SSLに対応している銀行なども増えていますので、証明書の種類や内容も確認してみるなど、少し意識を高めてみましょう。

（図3）鍵マークの有無とEV SSL証明書による表示の違い。上から鍵マーク無し、鍵マーク有り、EV SSL証明書

（図4）画像ファイルに記録される位置情報の例



便利だがリスクも抱える位置情報

携帯電話やスマートフォンの普及により、位置情報（図4）を取得できる端末が増えてきました。GPSの機能をオンにしていると、SNSのチェックイン機能が使えるだけでなく、撮影した写真にも位置情報が付加できます。

旅行に行ったとき、どこで撮影した写真なのかをあとで調べるには非常に便利ですが、位置情報が危険になることがあります。自宅で撮影した写真をブログやSNSで公開すると、その写真に記録されている位置情報から自宅が特定され、女性であればストーカーなどの被害に遭うかもしれません。旅行先でチェックインすると、自宅が留守であることが知られてしまい、空き巣の被害に遭うかもしれません。

なお、位置情報はGPSだけで取得できるわけではありません。携帯電話の基地局を使ってある程度の範囲を取得できますし、無線LANのアクセスポイントの位置情報を使うこともあります。アクセスポイントの位置は固定されていることが一般的ですので、電波の強度や複数のアクセスポイントとの位置関係から高い精度で位置を特定できます。

位置情報を知られるとどのようなリスクがあるのか、普段から意識するようにしましょう。

セキュリティを高めると使い勝手が失われる、という部分もありますが、利便性と安全のバランスを常に意識して使うことが求められています。