Su-Tek-I TREEWARE
Step-up Technology Information
Vol. 001 / 2011-02-09 発行
この文書は以下よりアクセスできます
http://treeware.jp-help.net?dstk001

● 簡単な「セキュリティ」の知識

インターネットは，「外に出なくても外部の人とコミュニケーションできる」という点で，「元々外にあまり出られない人たち」にとって，大きな恩恵をもたらす可能性のあるものです。しかも最近は，タブレット型パソコンやスマートフォンなどの「指で触れるだけで操作する機器」の普及により，マウスやキーボードなどの操作が難しかった障害者や高齢者などでも使える可能性が出てきました。一方で，様々な内部情報を扱う機関や施設では，「インターネット」の扱いをどう考えるかは，どこも悩むところではないかと思います。しかし，ネットワークの仕組みをよく知らないまま，「情報漏えい」に極端に過敏になることによって，インターネット接続を必要以上に制限してしまい，そうした恩恵を受けるべき人たちの活動の機会を奪ってしまっているとしたら，たいへん残念なことではなかと思うのです。ここではその辺りについて，簡潔な説明を試みようと思います。

◆ 漏えいに「過敏」になる要因

コンピュータのネットワークの目的は，大雑把に言うと2種類あります。「インターネット」と「イントラネット」です。

「インターネット」というのは，ご存知のとおり，他の機関や企業のホームページ閲覧やウェブサービスの利用など，主に「外部と」情報通信をするもの，いわば「対外接続」です。

一方「イントラネット」というのは，主としてその施設や企業の「内部情報」を交換するもので，いわば「構内接続」です。そのため，時として外部に出せないような内容がやりとりされる可能性もあります。

ところがこの2つ，名前が紛らわしいだけでなく，「仕組み」もほぼ同じで，つまり「外部に出せない」ような内部情報も，「外部とつながる仕組み」を利用してやりとりされます。そこに「セキュリティ上の問題」も感じるところではないでしょうか。

◆ どのように「漏えい」は起きるか

ただ確実に言えるのは，たとえ対外接続されたパソコンでも，内部情報が扱えない状況下で，「漏えい」が起こることはありません。ですから，流出を防ぐためには，内部情報を扱うパソコンとインターネット用のパソコンをはっきりと使い分ければいいわけです。

ところが，そうして分けていても，流出したケースが時々報道されます。その手のケースで「漏えい」が起きる条件は，1：対外接続しているパソコンで（外部に出すべきでない）内部情報を読める状態にしてしまい，2：それが何らかの原因で外部に送信されてしまう……の2つです。

たとえば誰かが，時間中に終わらなかった仕事の続きを処理しようとして，何らかの媒体……たとえば「USB 記憶装置」や「CD-R」に内部情報をコピーして，インターネット接続可能な自分のパソコンで読める状態にしてしまうと，この時点で1番目の条件を満たしてしまいます。

ただ，2番目の条件はかなり限定的です。そのパソコンに「ウイニー」などと呼ばれる「ファイル共有ソフト」がインストールされ，しかもそのソフトを狙った「ウイルス」にも感染していたため，ウイルスが勝手に外部に情報を送信してしまい，漏えいが起きる……というケースが多いのです。

考えようによっては，「ここまで悪条件が重なって」起きているわけです。

特に注目すべきは，対外的な（インターネット）接続と構内接続が，必ずしも「同時に使えるようになっていない」状況で起きているという点です。「インターネットに接続するから『漏えい』が起きる」といった考えは，裏返せば「インターネットに接続していないから大丈夫」と安心してしまい，むしろ危険なのかもしれません。重要なのは，上記条件の「全てを満たす」ことがないようにすることで，特に1番目の条件「外部接続できるパソコンに内部情報を入れない」よう，現場の業務管理を適切にすることだと思われます。

◆ 無線 LAN のセキュリティ

最近普及してきたタブレット型パソコンや，スマートフォンと呼ばれる情報端末には，たいてい「無線 LAN」と呼ばれる機能があり，ケーブルをつながなくてもネットワークに接続できるようになっています。と言うと，「漏えい」を心配する方は，「『電波』を使うわけだから，傍受されてしまったら……」といった懸念を抱くかもしれません。

しかし，無線 LAN がここまで普及した理由は，それなりに機密性を保つ仕組みがあったから，とも言えます。無線 LAN には「暗号化」の技術が導入されていて，共通する「鍵」となるデータを持っている機械同士でないと，相互に意味のある通信ができない仕組みです。そのため，たとえ同じ無線方式で通信する機械が複数あっても，「暗号化」技術を使っている限り，同じ「鍵データ」が設定されていないと通信できません。

もちろん，前述の「タブレット PC」や「スマートフォン」などにも導入されている技術ですから，たとえば，構内の情報交換に無線 LAN を使っている施設でそれらの機器を利用したとしても，「鍵データ」が構内接続と異なる限り，情報が読み取られたりする可能性はまずありません。正しく利用すれば，ケーブルを接続せずに通信ができる無線 LAN は，たいへん便利な機能です。

◆ 「流出しても見れない」仕組みの利用

しかし，海上保安庁の中国漁船衝突映像や，北海道サミットの警備情報の漏えい問題などが示すとおり，どんなに厳しく管理された部署でも「漏えい」は起きます。

たとえば「無線 LAN」においては，暗号の「鍵データ」を解析する装置が闇で出回り，そしてまた，その解析を困難にする新たな暗号化技術が開発されたりと，「いたちごっこ」の感は拭えません。

極端な話では，ネットワークに接続していなくても漏れるケースもあります。コンピュータがデータを処理する時は「電波」を出すので，それを傍受され，解析されてしまったらアウトです。

ただ，そうした「解析」には，一部でしか手に入らない特殊な機器が必要なので，可能性としては「ゼロではない」ですが，そう大きくもないと考えられます。

いずれにせよ，インターネットに接続していようといまいと，起きる時は起きるのが「情報漏えい」と考えて，対策をしておくのがベストでしょう。

では，どう対策すべきでしょうか。

たとえば「流出しても，関係者以外は見れない」ようにする仕組みの利用は即効的です。じつはわりと簡単に，ファイルを暗号化して，「パスワードを知る人でないと開けない」ようにする技術があります。身近には，ワードやエクセルなどのデータにも，「パスワード」を付加して，関係者以外は開けないようにする機能があります。

ただ，残念ながらその辺りの知識は浸透していないのが実情です。海上保安庁の漁船衝突映像流出の例では，映像データが「誰でも見れる状態だった」とされていますが，もし「暗号化」されていれば，あのような「誰でも見れる」かたちでインターネットに公開はされなかったでしょう。管理者には，「知識のある人に協力を求める」など，的確な意識を持った対応が求められます。

◆ 適切な知識で快適な活動を！

述べてきましたとおり，タブレット型パソコンや無線 LAN などの普及で，コンピュータの操作性は向上し，誰でも手軽にインターネットが使えるようになっても，適切な知識のないまま情報漏えいに過敏になり，その恩恵を受けるべき人たちが受けられないのでは，なんとも「もったいない」感じもします。適切な知識を知り，役立つ「道具」としてうまく活用できるようにしてこそ，そうした人たちの生活向上につながるのではないかと考えています。