2004-9-1

混沌とした中から

第3号
発行責任者　稲崎義明

ＩＴ情報社会の進歩の中で（２）

住民基本台帳ネットワークも始まったころはいろいろ話題にもなったのがだんだん既成事実化されていくのが怖いところですが、そのほかにも気になるものがあります。その１つが、インターネットに一部で話が出てくるスパイウェアと呼ばれているものです。スパイウェアは、インターネットのホームページや販売されているアプリケーションの一部に含まれているもので、名前が示すとおりスパイ的な動きをします。スパイウェアは、含まるアプリケーションの使用状況をモニタリングしたり、インストールされているハードウェア、ＯＳ環境などをモニタリングし、アプリケーション作成側に送る機能を持っています。他に関連の宣伝ウィンドを表示したり、いわば勝手なことをしています。アプリケーションに含まれるスパイウェアは、実はインストールする際の使用許諾文書の中に記載されているのですが、それを細かく読む人はまずいないでしょうし、入っているからといって、許諾内容を「ＯＫ」しないとプログラム自体がインストールできず、使えないということになるわけですから。アプリケーションに含まれるものはまだいいのですが、問題はホームページなどを見たときに含まれているものです。ウィルスもそうなのですが、ホームページを見ただけでプログラムをダウンロードさせることは可能です。悪意を持ったものであれば、たとえばキー操作のログを残して、その中からクレジットカードに関するものを探して特定のところに送るものまであります。ホームページを閉じてしまえば、メールソフトを使っていなければ大丈夫だと考えがちですが、このようなソフトは自分でデータを転送する機能を持っています。困ったものですが、全部が全部問題のあるものでもないので、スパイウェア対策ソフトでも無条件ですべてを削除するわけに行かない（親のアプリケーションが動かなくなることもあるので）のです。ＩＴ情報社会で問題だと思うのは、このように外から何がどのように動いているのかわからない、知らないうちに変なものが裏で動いている、被害者だと思っていたら加害者側になってしまっていたといった、このようなことが日常茶飯事に起こりうることです。これまでであれば、クレジットカードが盗まれた、貯金通帳が盗まれた、財布を落としたなどというように物理的に目に見えることがあったので、それなりに警戒もできるのですが、パソコンの中で勝手に動かれていては、データを盗まれたことすら気づかないことになってしまいます。それよりも問題なのは、このようなことでデータが盗まれるという事件があっても対岸の火事のように、まったく気にしない人が多いことです。これはウィルス対策にもいえることでもあるのですが。もう少し自分のパソコンのセキュリティに注意をはらってもらいたいものです。ウィルスやスパイウェアなんかはいろいろいわれているけど、自分のパソコンまでくることはないだろうなんて、大変な考え違いです。近頃、何も操作してないのに突然ＨＤＤのランプがつくことが多くなった（すべてが問題ではありませんが）、パソコンが急に遅くなったような気がする（使っていればある程度は遅くなりますが）、といったことがあれば、ウィルスが侵入しているかもしれません。勝手に別なことをしているかもしれません。メールソフトに記録が残っていなくても大量のメールを出しているかもしれません。あなたのパソコンが乗っ取られているかもしれません。

ＩＴ情報社会でインターネットなどの急激な普及で気になっているのはこのようなことです。もちろん一番問題なのは、使っている人に危機意識がまったくといっていいほどないことなのですが。

（次回へ続く）

(今週の情報誌から)

○日経パソコン　８月３０日号

特集　ネットに残るあなたの“足跡”

→今回の特集は、ちょうど連載記事に書いたのと同じインターネットでの個人情報関連の話。確かに、cookieなどを使って、アクセスしたページに自分の名前を表示されてしまうことがあるが、それだけで個人情報が漏れたわけではない。IPアドレスがわかったしても個人の住所までわかるわけではない。など、不安がいっぱいになる必要もないが、安心しきってしまうのも問題がある。クレジットカード会社を語って利用状況を確認するためにカードのIDとパスワードを入れさせるフィッシング詐欺もある。専用ソフトを利用したり十分注意するのに越したことはない。

○日経システム構築　９月号

特集　オープンソースの高速Webサーバ「TUX」の実力

→RedHatが作ったオープンソースのWebサーバソフトに「TUX」があるが、その実力測定。現在主流の「Apache」と比べて、Webサーバ機能がOSのカーネル上で動作するため、約１．５７倍速い。最も速いのは、RedHat９．０の後継のFedoraCore２．０と組み合わせた場合。

○Ｎ＋Ｉ　ＮＥＴＷＯＲＫ　１０月号

特集　「ブラックリスト」の作り方

→顧客情報漏えい事件を発端として、社員一人一人を監視しようとする動きが広がりつつある。監視することを公表した上で、監視することになるが、個人情報保護法の施行を控え、従業員の監督に、監視・モニタリングが不可欠となってきている。ブラックリストは、ネットワークログ、パケットの監視、個人端末のログ、電子メールのログなどの解析から作成する。

○ＮＥＴＷＯＲＫ　ＷＯＲＬＤ　１０月号

特集　まるごとわかる「ネットワーク監視」の秘訣

→ネットワーク管理者は、いつ起こるかわからないネットワークトラブルに備えて監視しておく必要がある。ネットワーク障害は起こるものとして、「稼動監視」、「プロセス監視」、「リソース監視」を行う。監視ツールとして「ＢｉｇＢｒｏｔｈｅｒ」による監視テクニックを紹介。このツールは基本的にポーリングで監視するもので、オープンソースと商用版のあるＵＮＩＸ版と商用版だけのＷｉｎｄｏｗｓ版がある。管理者にはＨＴＭＬ形式で情報が提供され、監視対象ノードの稼動状況が一目でわかるようになっている。