

マイクロソフトのセキュリティへの 取り組みと今後の展望

講師：楠 正憲

(マイクロソフトアジアリミテッド 政策企画本部企画部技術政策ストラテジスト)

ふとしたことで体調を崩すと「風邪を引くのは普段の健康管理がなってないからだ」などと、生身の人間なら責められるところだが、実はコンピュータの健康管理についても、多かれ少なかれ似たようなことが言われてきた。

もちろん、ここでいうコンピュータの「健康管理」とは、ウィルスやワームなどの不正ソフトウェアへの対策のことだ。不正ソフトウェア対策は、システム管理者の判断と力量にかかっており、その意味でシステム管理者の責任は重い。そのため、コンピュータがウィルスやワームの被害を受け、さらにその被害を拡大させてしまうのは、システム管理者がコンピュータの健康管理という責任を十分果たしていないことが原因だと考えられがちだった。

2003年1月に韓国のインターネットを麻痺させるほどの被害をもたらしたSQL Slammerのときにも、対策ソフトウェアを適用していなかったことが大きな原因とされ、挙句の果てには違法コピーの普及までもがウィルス被害を拡大させた(違法コピーは、対策ソフトウェアについてのお知らせがこないため、対策が後手に回る)などと言われた。このような事例もやはり、管理者の管理責任への注意を喚起するエピソードとして捉えられていったのではないだろうか。

5月17日のIECP研究会で講師の楠正憲氏は、マイクロソフトがこれまでにとってきた不正ソフトウェア対策の経緯を振り返ったうえで、「2003年8月のBlasterは、それまでの方針の転換を迫るきっかけになった」と述べた。Blasterは、ワーム型と呼ばれる不正ソフトウェアで、マイクロソフトのウィンドウズXPや2000に感染する。そして、感染したコンピュータを踏み台にしてさらに別のコンピュータに感染するという特徴をもつ。Blaster自身は、データの破壊や削除を行うものではなかったが、感染するとウィンドウズが再起動を繰り返すなどの症状が出るというものだった。

一見、被害の少なそうなBlasterが不正ソフトウェア対策の転機となったというのは、このウィルスの感染や被害が、従来のターゲットであったサーバーだけでなく、一般利用者が使用するコンピュータにも広がったことにあるという。ブロードバンドの普及により、家庭で常時接続されているコ

ンピュータが被害の対象になる可能性が格段に高まることになったのだ。サーバーの場合には、企業内で専門の人員により運用される。そのため、不正ソフトウェア対策が自主的に取られることが期待できる。しかし、家庭で常時接続されるコンピュータでは、そこまでの管理は期待できない。楠氏は、対策ソフトウェアのダウンロードの件数から見る限り、家庭用の利用者の5分の1から4分の1程度しか対策ソフトウェアを適用しておらず、ここでは従来の専門家向けの対策は通用しないと述べた。

このとき、私たちには選択肢が二つある。「健康管理はきちんとしなければダメなのだ」という選択肢と、「生活習慣病を改善するには、社会全体の生活スタイルを変えていかなければならない」という選択肢の二つだ。この数年、マイクロソフトが不正ソフトウェアへの対策を通して学んだことは、後者だった。従来のアプローチでは、増えつつあるブロードバンド利用者への不正ソフトウェアに関する対応は不十分なままに終わってしまう。これからは、利用者の視点から、この溝をどのようにして埋めていくのかを考えていく必要があるということだろう。

今回のIECP研究会では、Trustworthy Computing(信頼できるコンピュータ環境)を創出するためにマイクロソフトが進めている活動の紹介について時間の多くが割かれることになったが、実のところ、不正ソフトウェアへの対策を通じて、ソフトウェアやハードウェアが変化するだけでなく、それを使う利用者像も同じように変化しているということが具体的に明らかになったことのほうが意義のある発見だったのではないか。同社には気の毒な言い方だが、不正ソフトウェア対策という大きな実証実験から導き出すことができた貴重な成果と言えるだろう。

上村圭介(GLOCOM主任研究員)