多様化するリスク管理の実際

ハニーポットWGリーダー
園田　道夫

1. 便利になりすぎた？PC

モバイルPC、ノートパソコンを見てみよう。ごく普通に無線LANが付いている。USBインタフェースも付いている。CDだけでなくDVDも読めるし書けるものまである。

もちろん従来からのethernetインタフェースはもはや標準だ。PCMCIAのスロットも同じ。56Kモデムもついているし、メモリスティックを食べてしまうものまである。

外部記憶を担うメディアも種類が増えた。USBメモリはギガ単位の容量になり、PCMCIA経由メモリカードがあったり、メモリスティックがあったり、もちろんCDやDVDがあったりもする。

そしてネットワーク。ethernetやモデムはもちろん、無線LANインタフェース内臓のものも珍しくないし、USBから無線LANにつないだりもできる。PCMPIAのアダプタとPHSカードからデジタルでダイヤルアップするのは、無線LAN利用よりも広がっているようだ。

高機能化は現在こんなに進んでいる。

裏を返せば、それだけリスクも多様化が進んでいるということでもある。

便利な機能はそれだけリスクもある。例えば、無線LANはいちいち線を用意しなくとも、電波が入る位置ならばどこででもネットワークに接続ができる。しかしこれは、電波が入る位置に居る人間ならば、誰でもネットワークに接続できる、ということでもある。そして問題は、電波が届く範囲を、今の技術とコストでは制御できない、ということである。つまり、リスクの程度としては、誰がいつ繋いでくるか分からない＝インターネットと同じ、ということになる。それをLAN（Local Area Network）などと言ってしまうから、安易に抜け道を作ってしまうわけだ。

外部記憶メディアが高機能で、かつ超小型化してきているのも厄介だ。例えばUSBメモリならば、たいていのものは余裕でおさまる容量である。それがどこにでも隠せるほどの大きさなのだ。

こういう時代に何をどう管理していかなければいけないのか？

2. 管理者、普通のユーザー、それぞれの言い分

リスクは確実に増えているのに、管理運用する側のリソースは増えていない。それどころか戦力はまっさきに削減されることすらある。

そうなると現場は目先の仕事をこなすことだけに追われることになる。目先の仕事の主なものは、多機能化したコンピュータの面倒を見ることだ。多機能化するということは、裏を返せばそれだけ不安定要素を抱え込むことでもある。流石に以前のようにいきなりブルースクリーンとか、いきなり起動しなくなるとか、そういうことは減っているが、動かない使えないという事象はそれほど減ってはいない。

いや、むしろ以前よりも依存度が高くなっているだけ、クレームやお助けのお願いの総量は増えているのではないだろうか。

減らされるリソースで増え続けるクレーム処理にあたりながら、さらに新しいリスクを管理する方法について考える余裕などあるわけがない。そんな過酷な状況で、いったいどうやってセキュリティを守ればいいのか？

管理者ではなく普通のユーザー側にも言い分がある。・・・だいたい会社でPCを全員使わないと仕事にならない仕組みなのに、そこまで不可欠に近いものになってきているはずなのに、なんでこんなによく止まったり、ウイルスだ何だとわけのわからない障害が起きたり、パッチとかサービスパックとか面倒な手間ばかりかかったりするのだろう？ウイルス対策ソフトウエアのパターンファイル（これがまたわけがわからん仕組みだが）を毎日更新しろとか、WindowsUpdateとかいう仕組みを使ってチェックしろとか、何か昔より確実にやることが増えて、折角PCを入れているのにいっこうに楽にならないし効率も上がらない。そんな

気がして仕方が無いのだがどうなのか？

そもそもなんでこう急いでいるときに限って動かなくなるのだ？

いや、それ以前に、長いパスワードをつけておぼえろとか、おぼえやすい単語は使うなとか、そればかりか3ヶ月に1回変えろとか、そんなことができると思っているのだろうか？急にある文書を印刷しなければならなくなったとき、いちいちPCを起動してファイルを探してとかやっていたら平気で10分とか15分とかかかってしまうし、つけっぱなしは止めろと言われても会議に資料が間に合わなくて怒られるのは自分だし、いちいち煩雑な手順など守っていられない。

無線LANなんて便利なシロモノを「危ないから使うな」と言われても全然納得できないし、だいたいどこが危ないのかよくわからない。外から繋いでくるやつが居たとして、ウチみたいに何もない会社から何を盗み出すっていうのか？ウチみたいなところに興味を抱くような悪者が居るとも思えないし。

まあでも、いろいろ大変なのはわかるので、せめてPCが止まったときにすぐ何とかなるような仕組み？連絡先？ヘルプ依頼先がはっきりしていて欲しいのだが、お助け連絡を入れても誰も出ないし、返事が遅いし、半日も1日もふらふらしなければならず「遊んでいるのか」とか言われてしまうし、そこだけでもなんとかして欲しいのだが。

こんな厄介なPCなんてシロモノ、いつまで使いつづけなければならないのだ？

3. 最も大きなリスク

結局のところ、現在最も大きなリスクとは「普通のユーザー」ではないだろうか。なぜなら、「普通のユーザー」は今のコンピュータが持つ機能とそのリスクを理解していないからだ。だがそれも無理は無い。「普通のユーザー」は専門家ではないからこそ「普通」なのだから。

「普通のユーザー」は便利さ、面白さは体感しているが、そのリスクがわからないし、そもそも何がどう危険なのかわかっていない。また、何でパッチだアップデートだが必要なのか、ウイルスってそもそも何でマズいのかも理解していないし、そもそもただでさえわけがわからないPCを言われたとおりに使うだけで精一杯だ。

そういう非専門家ユーザーのリテラシーを向上させるのは、いったいどうすればいいのだろうか？

ここで言うリテラシーの向上とはこういうことだ。「非専門家ユーザー」が、Windows系パッチ情報が出たらWindowsUpdateをきちっとチェックして必要ならば即導入し、ウイルス対策ソフトウエアのパターンファイルは1日1回は更新し、パスワードはランダム英数字8文字以上で辞書には載っていないものを用いて3ヶ月に1回は変更する。万が一怪しげなWebサイトに誘導されたとしても、そこが本当に「怪しい」かどうか様々な材料を見て判断し、怪しいとわかったら即回避する。お買い物サイトなどでも不要な個人情報を登録しないように気をつけて、目的のために止むを得ず登録した個人情報もちゃんと管理されているのかこれまた様々な材料を見て判断し、危ないようなら即回避する。そして、メールの添付ファイルはいきなりダブルクリックせず、ウイルスかどうか確認してから開けてみる。・・・リテラシーが十分に高いと言えるユーザーは、この程度のことは普通にできなければならない。

しかし、正直なところこのレベルにスタッフ全員が到達する、というのは無理だろう。

もちろん手順が決まっていることはできるだろう。だが残念ながらその手順が煩雑であることも多く、それでなくても仕事仕事で追われているのに手間も時間もかかると真面目なユーザーでもサボりたくなるのが人情だ。手順が決まっているものですらそうなのに、決まっていないとどうなるだろうか？専門家ですらそのお買い物サイトが危険なのかどうか判断できないこともあるのに、「非専門家ユーザー」には無理だ。

さらに追い討ちをかけるようだが、仕事のやり方そのものも多様化してきている。

今や仕事場だけが「仕事場」ではない。そこらじゅ

うに無線のアクセスポイントが存在するし、つなぎ放題でも安目のPHSカードも売れているし、常時接続は当たり前のように普及しているし、外出先でも家でも場所を選ばずに仕事ができるわけだ。そして例によってそうした便利さの裏にはリスクが有り、外出先でも家でもおかしなアクセスに晒されてしまう危険があるのだ。

現在、PCのユーザーが直面しているリスクには、ざっくり見てきただけでもこれだけの種類がある。厄介なことにこれだけのリスクのうちのどれかひとつを怠るだけで、ブラスターなどのワームを社内に呼び込んでしまうことになる。実際、IPA（情報処理振興事業協会）の「W32/MSBlaster及びW32/Welchiウイルス被害に関する企業アンケート調査」（2003年9月）によれば、ブラスターは持込PCから入り込んだ、というのが25％もある。やはり仕事のやり方が多様化してきていて、今までとは異なる経路でワームが持ち込まれているということが浮き彫りになっている。

また、BCN総研による「セキュリティ対策に関するアンケート調査」（2003年9月）という、企業だけではない一般ユーザーを対象とした調査では、「ブラスターをきっかけに何らかのセキュリティ対策を行ったか」という問いに対し、27.6％の人が「全く何もしていない」と回答している。ということはつまり、勤め人のユーザーのリテラシーを100％にしたところで、家庭やプライベートな活動の場などには未だに「何の対策もしていない」ユーザーが多数存在し、その脅威にさらされる、ということだ。常時接続ポイントがルーターでフィルタリングされていたとしても、子供が学校で感染してくるかも知れないし、親もプライベートサークルなどで感染してくるかも知れない。いったんそれが入り込んだらつねに感染する危険はあるわけだ。

切れ目無くどこでも仕事できるようになってしまった現在、ワームなどのリスクはまさしく、風邪などと一緒なのだ。そして、どんなに用心していても風邪は引くときは引いてしまうものだ。

とはいえ、何らかの対策を打たなければ、今までどおりワームが入り込むだろうし、今までどおり内部情報は漏洩するだろう。

4.「普通のユーザー」対策

もちろん、どの組織もただ手をこまねいていたわけではない。これまでにもさまざまなセキュリティ対策が講じられてきた。

しかし、そうした対策の中でも例えば「リテラシー教育による向上」「パッチ管理やパターン更新をユーザーに任せる方法」「PCの持ち出し、持込管理」「セキュリティポリシーの徹底」といった、「普通のユーザー（エンドユーザー）」にある意味依存するような対策はあまり効果が上がっていない。逆に、一定の成果を上げている対策には「ファイアウォールの導入」「サーバー、ゲイトウエイ型ウイルス対策」「IDSの導入」などが上げられるだろう。効果が上がっている対策は、「普通のユーザー（エンドユーザー）」に依存していないものが多いはずだ。

確かに情報システムに予算をかけにくいという状況はわかるが、結果として生じる事故などによって業務を大々的に停止されてしまうと、渋る予算をさらに上回って余りあるような損害を直接的に被ることになりかねない。そしてそういう機会はどんどん増えつづけている。

そろそろ「普通のユーザー」対策に本腰を入れていくべきではないだろうか。しかも「普通のユーザー」に依存しないで実施できる対策に。

対策をいくつか具体的に挙げてみよう。

（1）インベントリー管理

ここへ来て各ベンダーからエンドユーザーのインベントリー管理を行う製品が出始めている。これはエンドユーザーのPCのパッチやサービスパック状況を把握したり、エンドユーザーの行動をログに残したり、外部記憶装置（CD、DVD、USBメモリなど）の使用制限を行ったりするものもある。また、一時的に状

況を把握するだけでなく、例えばモバイル接続時にあらかじめ設定されたポリシーによるチェックを実施し、適合しないPCは繋がせない、などの管理を行えるものもある。

ちなみにマイクロソフト社からは、パッチの更新を行うための仕組みとしてSoftware Update Serviceが無償で提供されている。

さらには、保護すべきファイルに着目した、ファイル管理という手段もある。

(2)パーソナルファイアウォール

個々のPCのアクセスをフィルターするファイアウォールで、ウイルス対策ソフトウエアと同じパッケージになっていることも多い。個々のPCにそのまま入れておくだけでなく、統合的に管理する仕組みも製品として出てきている。上記インベントリー管理とセットになっていることもある。

(3)トラフィックモニター

ネットワークを飛び交う通信をモニターし、あるサーバーへのアクセス記録や相互通信の記録などを残しておく。情報漏洩時などの事後的な監査や追跡に役立てる目的である。

(4)部署ファイアウォール

例えば部署ごとにファイアウォールやルーターによるパケットフィルタリングの仕組みを導入する。いっせいに全社にワームが広がらないように、セグメントごとに防御するための仕組み。

現実的なものはこういうところだろうか。

(1)と(2)は、PCを持つユーザーすべてに導入、あるいはモバイルユーザーだけにでも導入するような対策である。従ってそれなりに個数も多くなるし、当然ながら初期投資もそれなりにかかるものだ。そうした投資を抑える方法はある。例えばフリーソフトウエアでの代用とか、集中管理をある程度あきらめる、などの機能制限を選択すれば、ベンダーが勧めるまんまのゴージャスな仕様のソリューションに大金をはたかないでも済むわけだ。決まったポリシーを適用しておくだけでも効果を上げることができる。

例えばパーソナルファイアウォールだ。もちろんすべてフリーのソフトウエアである必要は無いが、統合的に管理をするほどの柔軟性が必要なわけでもない。そのPCに対する外からのアクセスはすべて拒否し、内側から張られるTCPのセッションは許可、あとはDNS参照とftp、インターネットを使うときはそれだけで十分だろう。ファイル共有が必要ならば相手のサーバーを特定して該当するポートを許可すればいい。

これを実施するだけで、実はワームへの対策としては完璧とは言わないが十分だろう。ワームはその多くが「ファイル共有」と「OSに潜むセキュリティ上の弱点」を狙ってアクセスしてくる。そもそも仕事する上では必要が無いアクセスを解放してしまっているために、そうしたアクセスが脅威になるわけだ。不要なアクセスはさせないし、自らも行わない。これを実現するには個々のPCに入れるファイアウォールが現在のところは最適解である。個々のPCに入れておけば、モバイル環境であろうと外出先であろうと、危険な家庭内であろうと有効な防護策となる。

ファイアウォールをあまねく行き渡らせることが不可能であるならば(いろいろ事情もあるだろう)、部署ごとのファイアウォールでもう少し範囲を広めて通信制御する手もある。一般にファイアウォールというと運用管理にそれなりの手間がかかってしまうものだが、その組織に1つのファイアウォールなどの場合は、さまざまな要件を集約しなければならなかったり、通信量も多かったりで手間がかかるわけだ。しかしそれが例えば部署という軽い単位であれば、ポリシーもそんなに複雑なことをやらせなければ良いし、通信量もさほどではないだろうし、あまり気にかけず放置に近いくらいでも役には立ってくれる。また、情報漏洩対策として通信のログを取得することも容易だ。

もちろん通信のログをいくら取得したとしても、漏洩があったことを事後的にトレースできる、というこ

とでしかない。しかし、これを告知しておくことでの抑止効果は期待できるし、取得したデータをきちんと証明付きで保管しておけば、仮に民事での訴訟となった場合でも使える証拠となるはずだ。

通信の記録ということでは(3)のトラフィックモニターも同様である。ファイアウォールのログなどと異なり、こちらは使うツールや方法などによって取得するログの内容を加減できる。ただし、モニター対象となるネットワークのユーザーへの事前告知は必要だ。また、暗号化通信対策などは別途配慮しなければならないが、IPヘッダーレベルの情報だけでも取得できればいろいろと使えるだろう。

筆者のお勧めはこんな感じだ。

「ワーム対策」
①パーソナルファイアウォールの導入
②部署ファイアウォール
③インベントリー管理、もしくはパッチ管理（Software Update Serviceなど）

「情報漏洩対策」
①通信ログ管理
②インベントリー管理
③ファイル管理

数字はプライオリティで、2003年末現在のプライオリティだ。ファイル管理やメディア管理など、さらにリーズナブルで使えるソリューションが出現してきたら、このプライオリティは変動するものと思っていただきたい。

最後に1つ付け加えておきたいのは、「検疫」についてである。

PC個々にファイアウォールを行き渡らせることができない場合には、PCを外から持ち込むときに「検疫」させるのだ。ワームなどに感染しているPCには、大量のパケットを撒き散らすなどの特徴がある。その特徴が出ているかどうかを見極めて、もしクロだったら洗浄してから接続させるのだ。

例えばこれを、DHCPサーバーと連携して行うソリューションが出てきている。IPを付与する前にポリシーのチェック等を行うのだ。これはエージェントソフトウエアが必要となる。

他にはVPN接続時にポリシーベースでチェックするソリューションも存在する。ただしこれはVPN接続にしか今のところは対応していないようだ。

筆者は現実的な運用に耐える「検疫」は、もっと手軽でなければならないと考えている。今のところはまだ、十分に手軽なソリューションは存在せず、どこか重たいものばかりだ。LANスイッチなどのトラフィックを常に監視しているようなソリューションもあるが、理想的にはそれを自動化・軽量化したいところだ。

でなければ、疲弊した日本企業では導入してもらえないだろう。重たい仕組みを入れると現場が管理工数の増大で悲鳴を上げ、経営も予算を負い、ということになってしまう。

筆者はトラフィック解析の仕組みを突き詰めることで、重たい仕組みになることを打破できると考えている。だがその前に、予防策の方が重要であろう。しっかり対応できて十分に運用可能な、そういう予防策を選定するために、本稿が役に立つことを願っている。