Javaセキュリティ・ホールにみる企業責任

高木 浩光／電子技術総合研究所

どんなに高度なセキュリティ機構が発明されようが，その安全性は実装段階でのミスが無ければの話である．Javaアプレットは「安全」とされ，暗黙の了解の下，何も知らないウェブ閲覧者に利用されてきたが，今年発覚したJava VMのセキュリティ・ホールは，それまでに知られていたものとは一線を画す大穴だった．それでもなお，無垢なユーザは何も知らないまま今もそれを使い続けている．

各社のJava VMにずさんなセキュリティ・ホールが発覚

2000年1月，筆者が主宰する「Java House」メーリングリスト[1]において，Internet Explorer（以下「IE」と略す）のJava VM☆1に新たなセキュリティ・ホールの存在が発覚した[2]．続いて4月には，Mac OS用のJava VMである「MRJ」（Mac OS Runtime for Java）にも，別のセキュリティ・ホールが存在することが発覚した[3]．

これまでにもJava関連のセキュリティ・ホールはすでに多数報告されている[4]が，それらのほとんどは，実際に悪用するには比較的高度な知識を必要とするものである☆2．ところが，今回見つかったものは，どちらも，ごくありふれたAPIをただ普通に呼び出すだけで悪事を働けてしまうという，これまでになく現実的な脅威をもたらすものである．

「Javaアプレット」とは，ウェブ閲覧者の確認なしに（ただサイトを訪れただけで）プログラム・コードをダウンロードして実行する仕組みである．これは，「サンド・ボックス」と呼ばれるJavaのセキュリティ機構によって安全確実に保護されていることを前提に成り立っている．この仕組みは本来ならば，「利便性と安全性を理想的に両立させる技術」として評価されるべきものであるが，確実な安全性を前提としているだけに，ひとたびセキュリティ機構に欠陥があればそれがもたらす脅威は甚大なものとなる．

ソフトウェアにバグはつきものではあるが...

「ソフトウェアにバグはつきものであって完全に無くせというのは無理な話である」と一般には言われる．だが，今回の欠陥に関してはそうした一般論を当てはめるのは適切でない．「セキュリティ・ホール」という言葉からは，「ドアの隅に開いた小さな穴を潜り抜けて錠をこじ開ける」というイメージを受ける．しかし，今回発覚した欠陥は「そもそもドアが存在しなかった」ようなものである．

MRJの欠陥は，「URLConnection」と呼ばれるJavaのネットワーク機能の基本的な部分について，セキュリティ機能がまったく働いていなかったというものである．本来のJavaアプレットのネットワーク機能では，アプレットはアプレットが置かれたホストにしか接続できないように制限されている．しかし，MRJのURLConnectionでは，この制限が正しく動作しないため，裏技を駆使するまでもなく，ただ普通にAPIを呼び出すだけで，任意のホストとの接続ができてしまう．この欠陥がもたらす脅威については文献5）で詳しく説明されている．この欠陥は，基礎的なテストで簡単に発見できるはずのものである．セキュリティ機構の検証なしに製品が出荷されていたのではないだろうか．

IEの欠陥は，「getResourceAsStream」と呼ばれるリソース読み出しのAPIでカレントディレクトリ以下のローカルファイルが読めるというものである．Microsoft VMでは，SunのJDKと異なり，どんな場合でもクラスパス（Java VMがクラスファイルを検索するディレクトリのリスト）にカレントディレクトリを含めるという独自仕様を持っている．getResourceAsStreamが，Javaのクラスパスを順に検索してファイルを見つけることを理解していれば，このことが引き起こす問題に気づけたはずではないだろうか．また，UNIXの文化では昔から，コマンド・パスにカレントディレクトリを入れてはならないというのは，セキュリティ上の常識になっている．それと対照的に，MS-DOSの時代からの，環境変数PATHに設定しなくてもカレントディレクトリがコマンドパスに含まれてしまうというMicrosoftの文化が，ここで仇となったようだ．

ベンダは本気でユーザに知らせるつもりがあるのか?

Microsoftは，続々と発覚する製品のセキュリティ問題を自社のウェブページで詳細に解説している[6]．この

☆1「Java VM」という用語は，本来はJavaのインタプリタやJITコンパイラなどのバイトコードを実行するための機構を指すものであるが，Microsoftの用語では，コアライブラリを含めたランタイム・システム全体を「Microsoft VM for Java」と呼んでいるため，ここではそれに合わせて，Javaのランタイム・システム全体を「Java VM」と呼ぶことにする．

☆2 多くはバイトコード・ベリファイアの検証機能が十分でないことが原因で発生する問題であった．

ことは高く評価できる．しかし，そこにはユーザを誤解させかねない「言い訳」が目立つ．たとえば，任意のホストに接続できてしまう欠陥が発覚したときには，たいてい，

── ただし，対象のページの正確な場所と名前（つまりURL）を知らなければ，悪質なウェブサイトオペレータが内容を読み取ることはできません．

という断り書きがされている．この文言自体に誤りはないが，読んだ者に「なんだ，じゃあほとんど大丈夫なんだ．」という印象を与えかねない．ところが実際には，攻撃対象のURLは容易に悪質なウェブサイトオペレータに知られてしまうというのも事実であって，ちっとも大丈夫ではない（詳しくは文献5）を参照されたい）．

今回発覚したgetResourceAsStreamの欠陥についても，その解説ページ[7]で巧妙なごまかしがあった．たまたま別のセキュリティ・ホールが同時期に報告されたため，2つの欠陥が同一のリリースによって解決されたのだが，解説では，悪用が簡単ではない後者の問題についてだけ触れられていて，こう書かれていた．

── What is the vulnerability?

Among the inappropriate actions that the sandbox should prevent a Java applet from taking is reading files on the user's computer. However, through a complex series of steps, it is possible for anapplet to bypass this restriction.

── Could this vulnerability be exploited accidentally?

No. The set of steps needed to bypass the sandbox restrictions in this case are extremely unlikely to happen accidentally.

「これが悪用されることは簡単ではないのでその危険性は小さい」ということが暗に主張されているように読める．しかし，getResourceAsStreamの欠陥は，ただ単にファイル名を指定して呼び出すだけなのであって，「complex series of steps」など必要ない．詳しくは文献8）を参照されたい．

次に，Apple Computerの場合は，こうしたセキュリティ専門の情報ページが用意されていない．今回，MRJの欠陥を報告した際に，日本のApple Computer社に対して，ユーザに適切な告知をするよう求めたが，私の意見は聞き入れてもらえなかった．

Appleは同社の「TIL（Tech Info Library」というウェブサイトで今回のMRJの欠陥に関する説明を告示した[9]．しかし，いったいどれだけのユーザがこの告示に気づいたかは疑問である．セキュリティの不具合は通常の不具合とは異なる．通常の不具合では，ユーザ自身が不具合に気づくために，問題を解決しようと思って自らTILのページの情報にたどり着くこともあるだろう．しかしセキュリティの不具合の場合は事情が異なる．ユーザは気づかないうちに情報を盗まれてしまう．気づかない人がTILのページを見ようなど思うはずがない．セキュリティ上の問題が見つかった場合になすべきことは，その存在を知らない人に知らせることである．

この理由を添えて，ユーザへの告知をすべきだと意見を送ったところ，当初Appleは，

── TILで更新された内容は，eNewsというメールでユーザに毎回告知しております．そのため，かなりのユーザに告知されるものと考えております．

と返答してきた．ところが，いつまでたってもeNewsで告知が流れてこないので再度，問い合わせたところ，

── 先日のメールでは「eNewsで配信を予定」とお伝えしましたが，Apple eNews はマーケティングの管轄のもと，主にセールス／マーケティング情報に特化したメールサービスですので，技術的な情報としてのTIL Update Newsにてメールニュース配信を行いました．

という返事がきた．つまり，元々TILを読んでいる者にしか告知されなかったわけだ．

「バグを完全に無くすことは無理」というのであれば，せめて，セキュリティ上の問題が発覚したときは直ちにユーザに対して告知するのが企業倫理ではないだろうか．そうでなくてはインターネット関連製品を販売する資格がないと思う．

パソコンメーカは他人事のふり

Windowsには「Windows Update」という機能があり，面倒な手順なしに誰にでも簡単に修正モジュールをインストールできるようになっている．この仕組み自体は評価できるものであるが，getResourceAsStreamの欠陥は，発覚して4カ月以上が過ぎた6月の時点でも，このWindows Updateの機能では修正されない．しかも，ひどいことに，IEのホームページからすぐにたどれるようになっている「Internet Explorerセキュリティ情報」というページ[10]には，この欠陥の修正モジュールについての記載がない（7月10日現在）．

そこで，6月に，国内のパソコンメーカ2社に対してサポート窓口に電話で問い合わせてみたところ，現在販売中のパソコンには，この欠陥が修正されないままのWindowsがプレインストールされているとのことである．また，3社に対して，「ユーザに対して告知をすべきではないか？」と問うてみたところ，どのメーカも口をそろえて，

── Internet ExplorerはMicrosoft社の製品で，うちはOEMで出しているだけなので，当社からお客様に告知することはしない．

と回答した．そのうち2社に対して，「欠陥があると知りながら無警告に販売するのはいかがなものか？」と問い合わせたところ，

── セキュリティ問題の修正モジュールがMicrosoftのサイトで提供されているので，お客様はそれをダウンロードしてインストールできる．

という回答だった．そこで，「そんなことにどうやって普通のユーザが気づくのか？」と問うてみたところ，

── IEを起動するとMicrosoftのホー

ムページが開かれるはず．そこからセキュリティ情報のページにたどり着けるはず．

という．そこで，「では私にそれのインストール方法を教えてください．」と尋ねてみたところ，教えてもらえたのは別のセキュリティ問題の修正モジュールで，getResourceAsStreamの問題の修正モジュールはサポート窓口の担当者でも見つけ出すことができなかった．

こんな状況で，一般のユーザが自分でセキュリティ・ホールを塞げるわけがない．

パソコン雑誌の責任は？

インターネット初心者が購読していると予想される，いわゆる「パソコン雑誌」には，付録のCD-ROMにIEを収録しているものが多い．しかし，Microsoftのウェブサイトで提供されている，セキュリティ問題を修正するアップデート・モジュールは，どの雑誌にも収録されていないようである．このことについて，インプレス社のインターネット・マガジン誌の編集長と，Infotalkメーリングリスト[11]という公開の場において，5月に意見交換をさせていただいた．

── IEを収録するのであれば，そのアップデート・モジュールも収録すべではないか．

と提案したところ，早速検討していただくことができた．しかし，最終的な結論は，

── Microsoft社の許諾が得られないので収録できない．

というものであった．そのときMicrosoft社が示した，収録を許諾しない理由とは，

── アップデート・モジュールは常に最新のものをご提供する必要があり，ウェブサイトでの配布がベストである．タイムラグの発生する雑誌への添付はご遠慮いただきたい．

というものだったそうだ．この理由付けはいかにも不可思議なものだ．アップデート・モジュールが「常に最新のものを提供する」必要のあるものならば，当然同じ理屈によって，本体も「常に最新のものを提供する」必要があるはずである．というか，そもそも「アップデート・モジュール」とは，その言葉の定義の通り，本体を最新のものにアップデートするためのものではないか．

アップデート・モジュールをCD-ROMで配布することに，いったいどんな問題があるというのだろう？　強いて言うならば，

── アップデート・モジュールが雑誌の付録で配布されるようになると，ユーザが「これですべてのアップデート・モジュールを適用した」と安心して，ウェブサイトの確認をしないようになってしまいかねない．

ということくらいか．そういうことならこう注意書きをしておけばよい．

── この付録に収録したアップデートモジュールは，○月×日の時点でのものです．それ以降にも新しいモジュールが提供されている可能性がありますから，必ず，○○のウェブページを確認するようにしてください．

この程度の交渉もせず引き下がってしまうのは理解に苦しむ．アップデート・モジュールを収録できないのであれば，本体の収録をやめてしまうべきだ．IEの収録をやめてしまうと読者の評判が落ちるというのであれば，収録を中止せざるを得ない理由を読者に説明すればよい．たとえば，

── IE 5.01には複数のセキュリティ問題が確認されています．弊誌では，それらの問題を修正するアップデート・モジュールをCD-ROMに収録すべく努力いたしましたが，Microsoft社の意向により許可されませんでした．弊誌では，セキュリティ問題の確認されているソフトウェアをCD-ROMで配布する場合には，アップデート・モジュールも同時に配布することが読者の皆様の安全を確保する上での責務であると考えております．このたび，IEのアップデート・モジュールの収録が許可されなかったことを受け，まことに残念ではありますが，今号よりIEのCD-ROMへの収録を断念することにいたしました．なにとぞご理解くださいますようよろしくお願いいたします．

などと説明すればよいだろう．

参考文献

1) Java House Mailing List, http://java-house.etl.go.jp/ml/
2) [JavaHouse-Brewers:30376] Warning: Yet Another Security Hole of 'Microsoft VM for Java', http://java-house.etl.go.jp/ml/archive/j-h-b/030376.html
3) [JavaHouse-Brewers:33152] 警告: Mac OS版IEとMRJのURLConnectionにセキュリティホール, http://java-house.etl.go.jp/ml/archive/j-h-b/033152.html
4) McGraw, G. and Felten, E. W.: Securing Java: Getting Down to Business with Mobile Code, John Wiley & Sons (1999).
5) [JavaHouse-Brewers:33024] 任意のホストに接続できてしまうセキュリティ上の欠陥がもたらす危険性, http://java-house.etl.go.jp/ml/archive/j-h-b/033024.html
6) Microsoft Security Bulletins, http://www.microsoft.com/technet/security/current.asp
7) Microsoft Security Bulletin (MS00-011): Frequently Asked Questions, http://www.microsoft.com/technet/security/bulletin/fq00-011.asp
8) [JavaHouse-Brewers:31072] 「Microsoft VM for Java」のセキュリティホールに関する再警告, http://java-house.etl.go.jp/ml/archive/j-h-b/031072.html
9) Mac OS Runtime for Java (MRJ): セキュリティ問題について, http://til.info.apple.co.jp/cgi-bin/WebObjects/TechInfo.woa/wa/showTIL?id=100390JO
10) Internet Explorer セキュリティ情報, http://www.microsoft.com/windows/ie_intl/ja/security/
11) Infotalk Mailinglist, http://www.brl.ntt.co.jp/people/takada/ml/infotalk/

(2000.7.13)

エディタから ──

高木氏の最初の記事には，実名入りで2社1雑誌と匿名企業3社の対応状況が書かれている．これらを一方的に取り上げるのはアンフェアと考え，当該2社1雑誌のしかるべき窓口には本件に関する対応について，また，同業のPC開発企業何社かの関係者には，テスト等技術的観点からのコメント執筆を依頼した．しかし，社長が海外出張から帰国しだい検討しますと態度を保留しているApple社以外からは，断られてしまった．

なお，高木氏の最後のコメントは紙面の都合で短縮されている．詳細版はWWWをご覧ください．

経営倫理の立場からの一意見

米田 英一／元(株)東芝

高木さんの問題提起に対して，エディタの塚本さんがソフトウェアベンダ，パソコンメーカ，パソコン関連の雑誌等のメディアにコメントを依頼されたところ，依頼先すべてから断られたということで，私の援助を求めてこられた．率直に言って，私には高木さんの問題提起に含まれている技術的問題の詳細については，その是非を云々するだけの知識はない．そもそもJavaのアプレットなど書いたこともないのである．しかし，そういう私でも，パソコン用のソフトウェアの惨澹たる品質については毎日のように泣かされている．したがって，技術的な詳細は分からないまでも，高木さんがパソコン用ソフトウェアのベンダを厳しく批判される気持ちはよく分かる．ましてや，テーマはインターネットにおけるセキュリティである．ソフトウェアベンダ，パソコンメーカ，パソコン関連の雑誌などのメディアが塚本さんの要請を拒否していることは，情報技術関連企業の経営倫理の根幹にかかわる大問題であると言える．そこで，私のコメントはもっぱら，企業の倫理，経営者の倫理，情報処理技術者の職業倫理に関するものに限定する．これなら，情報処理学会の倫理綱領をまとめた倫理綱領調査委員会の幹事を務めた人間として一言書く資格があるものと考える．

さて，いうまでもなく，高木さんの問題提起の主題はインターネットにおけるセキュリティの問題である．私がこの原稿を書いているのは2000年7月21日であるが，この日から九州・沖縄サミットの首脳会議が始まる．この首脳会議の目玉は情報技術(IT)だそうだが，仮に『インターネットにおけるセキュリティの問題』がこの首脳会議のテーマとして提出されたとしたら，クリントン大統領なり森首相なりが，「いや，これは我が国の企業の弱みを衝く問題なので，議題に取り上げるのはやめてほしい」などといって拒否するであろうか？そんなことを言い出せば，他の先進諸国の首脳連から足許を見透かされるのがオチであろう．今回のインタラクティブ・エッセイではそのような重要問題が提起されているにもかかわらず，ソフトウェアベンダやパソコンメーカやパソコン関連の雑誌などのメディアに所属する人たちが軒並み塚本さんの依頼を断っている姿は，一種の情報開示の拒否であり，技術者の職業倫理に反する行為であり，正に『IT時代の歪み』そのものであると言えよう．

しからば，このような情けない状況を招いたのは，塚本さんの依頼を受けた特定の人たちだけの責任であると言えるであろうか？　断じてNOである．実は，情報処理学会の倫理綱領調査委員会で検討を始める際，私は特に議論すべき7つの争点を挙げた．その7番目は，『従業員としての観点と市民としての観点をどのように調和させるか』というものであった．これは「企業などの組織に属する個人は，自分の技術者としての良心と企業の要求との間に矛盾がある場合にどうすべきか？」という問題である．塚本さんから原稿執筆の依頼を受けた人がどなたであるのか知らないが，彼または彼女は，「技術者としては何か書かねばならない」という自己の良心と所属企業が求めるであろう従順な姿勢との間の相剋に悩んだ末に，塚本さんに断ったのであると考えたい．「では，東芝に在籍していたときのお前さんならどうする？」と問われそうだが，私なら間違いなく原稿を書いている．ただし，社外発表許可が得られるかどうかは別問題である．皮肉な人からは「社外発表許可が得られないことを見透かして原稿を書くのは卑怯な自己満足に過ぎないのではないか」とからかわれそうだが，これについては深入りはやめておく．

いずれにしても，この種の問題を，技術者だけの職業倫理の問題として捉えるのは適切ではない．技術者にも責任があることは否定すべくもないが，同時に彼または彼女の所属機関(企業または官公庁・団体)とその機関の経営者や上位管理者の倫理を問うことが重要である．高木さんが問題提起されているソフトウェアの欠陥は，このまま放置しておくなら，昨年9月のJCO事故やつい最近発生した雪印乳業の中毒事故にも匹敵する大事故につながりかねない大問題であると思うが，この2つの事故における経営者(JCOの場合は親会社の経営者を含む)の醜態は我々の記憶に新しいところである．一方，雪印乳業の中毒事故の少し前に発生した参天製薬の目薬に対する悪質な『攻撃』の際の参天製薬経営者の毅然とした意思決定は，消費者を大いに感激させた．経営者の経営倫理観は人によってかくも異なるのである．

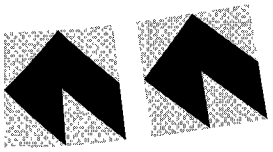
このように考えると，学士会会報の最近号に載った水谷雅一氏の「わが国産学における「経営倫理」の遂行性について」の主張は非常に時宜を得たものであると言える．この記事によると，日本アイ・ビー・エムでは従業員がコード(倫理綱領)を守れるかどうかについて，一定期間ごとに人事部が中心になってチェックを行うのだそうである．見事であると言える．その日本アイ・ビー・エムの従業員が，技術的コメントとは言え今回塚本さんの依頼に対して「や

はり書けない」として断ってきたという事実をどのように考えるべきか？　九州・沖縄サミットで真に論ずべきIT問題とは，まさにこの種の問題なのではないのか？

昨今，情報通信技術については規制緩和論だけが盛んであるが，ことソフトウェアの品質に関する限り，日本政府はむしろ規制強化を主張するくらいのことをやってはどうか？ ITをおっしゃるのであれば，その程度の誠意と気概はぜひ持ってほしいものである．

参考文献
1) 倫理綱領調査委員会報告書，情報処理学会（平成9年）．
2) 水谷雅一：わが国産学における「経営倫理」の遅行性について，学士会会報，2000-III，No.828，pp.83-96.

(2000.7.21)



由らしむべし知らしむべからず？ より根本的なセキュリティ対策のあり方を考えよう

棟上 昭男／東京工科大学メディア学部

筆者が「Java House」を初めて覗いたのは，Windows2000 が発売になる直前の本年2月初め，電総研の松井俊浩君から今回提起されている問題のうちの最初の方の件で相談を受けたときのことである．事の重大さは別にして，このメーリングリスト上における多くの若い人たちの活発で詳細な議論には感動もし，またこうであればこそ思いがけないシステムのバグや，セキュリティ上の問題を見つけることも可能になるのだと確信もした．その2カ月後に，今度はMac OSにもJava関連のセキュリティ・ホールが見つかったのだということは今回初めて知ったのだが，もちろんこれも同じように熱心な活動の賜物であることは疑いない．Apple社ともあろうものが，なぜ敵失を他山の石として速やかに活用することをしなかったのか，多少訝しい思いは残るのだが．

今回の件で原告の高木浩光君が，事の重大さや危険性を通常のメディアだけでなく，インターネット上のメディアも含めて，さまざまなメディアに訴えても，なかなか一般の人には理解してもらえず，認識も高まってこない，またMicrosoftやAppleなどベンダ側の対応もはかばかしくないだけでなく，何となく事の詳細をつまびらかに周知させることなく，時が過ぎ去るのを待っているように見える，さらに日本のベンダには当事者能力はまったくなさそうだし，役所筋や公的機関もあまり思うように は動いてくれそうにない．ということで相当にイライラされているのだろうことは想像に難くない．筆者自身も多くの点でこれらの問題に共感を覚えるし，特に上記の最後の問題に関しては後述の理由もあって，もう少し積極的に取り組んでもらえるよう働きかけてゆきたいと思っているところでもある．けれどもセキュリティ問題全体としては，皆がうんと痛い目に遭うというようなありがたくない追い風でも吹かない限り，本質的に社会全体に対する多面的で粘り強い働きかけが必要な問題であって，ヤケを起こさないことも大切だと思うのである．

筆者は昨年3月まで，国内では初めてセキュリティ問題に対処するための公の機関として設置された，セキュリティセンタを抱える，IPA（情報処理振興事業協会）に所属していた．その関係で，コンピュータウィルスや不正アクセス問題など，コンピュータセキュリティに関連する情報を，一般の人よりは多少詳しく身近に知る立場にある．確かに今回発見されたIEのセキュリティ・ホールは，悪用するのに込み入った高度なスキルを必要としない，それだけに相当に深刻なものであるようだ．しかしこれは筆者がたまたまその内容を知ってしまったから確信を持って言えることで，通常の一市井人としてなら，なかなかそのような状況に立ち至ることはないだろう．非常に簡単に利用できるホールなのかどうか，あるいはそのホールがどの程度深刻なものなのかどうか等々だけでなく，ネットワークセキュリティの問題そのものすら，一般市民はもちろんのこと，かなりのレベルの技術者でも実感することは相当に困難だろうと思われる．

しかし一方では，情報技術の大進歩のおかげでPCとインターネットの大衆化は進み，気が付かないうちにクッキーとかアプレットやらが飛び交い，個人情報が知らぬ間に勝手に集められていたり，ラブレターウィルスの場合のように気が付かないうちに間接的加害者になったりする機会は否応なしに増え続けている．けれども現在の状況では，ただ「Outlookを使っていると間接的加害者になる可能性が高いですから気を付けてください」と声高に叫んでみても，あまり効果は期待できそうにない．過度に煽るのは問題だし，実際コンピュータウィルスについては煽り過ぎに注意すべき時期に来ているという指摘もあるようだ．しかし，一方では古くから情報技術を専門とされてきた学会の大先輩で，我が校の最高幹部の方ですら，「だいたい危険だ危険だというが，学会だとか大学の中に守らなければならないほど重要な情報があるのか」とか「これまでインターネットを利用して，カード情報などやりとりしながら買い物もやっているが，一度も被害に遭ったことはない．セキュリティ対策などそんなに大袈裟に考える必要があるのかど

うか疑問だ」と言われるような状況もまだ存在するのである．

これが情報技術関連ではなく，たとえば自動車の場合であれば，その欠陥に関する危険性は，一般大衆にも何の問題もなく理解される．たとえその欠陥の内容が組込みソフトのバグに起因するものであったとしてもである．情報は目に見え難いという困難さのほかに，技術の進歩があまりに急速過ぎて，専門知識と大衆の知識との間のギャップが広がり過ぎたという問題も大きい．しかしすぐ間近にまで迫りつつある遠隔医療とか介護システム，あるいは電子政府の問題も，セキュリティ問題に関する完全なバックアップなしに導入が進んでもらっては困る．選挙権や投票の改竄ぐらいならまだしも（もちろんこれも大問題だが），患者の取り違えのようなとんでもないことは絶対に起こらないようにする必要がある（これも実際の病院では起こってしまったのだが）．

新しい技術の社会への導入に際しては，その技術自身を社会が評価できる仕組みと知恵を持つことが必須の条件だろう．社会が技術を評価することが可能であるためには，その技術自身が相当のレベルの透明性，オープン性を保持することが必要であり，これはセキュリティ問題にも典型的に当てはまる．この問題については他でも少し論じたのでここでは深入りしないが，システムソフトだけでなく，暗号問題などにもこれは当てはまる[1]．

一方の知恵の部分に関しては，基本的には教育しかないわけであるが，痛い目に遭わない限りなかなか分からない問題をどうやって実感させるかは今後の課題だろう．狼少年になっては困るのだが，くどいほど丁寧に繰り返される説明と教育が重要である．また，情報倫理の問題とも重ね合わせながら，情報教育導入の最初の段階からこれを重視してゆく姿勢が必要だと考えられる．また現在の情報関連製品に関する規制が，あまりにベンダ有利になり過ぎている面も，そのうち変えてゆく必要性があるのではないかと思われる．PL法のような法律までゆかないまでも，少なくともかっての「暮らしの手帖」レベルのプレッシャーのかかる仕組みは存在すべきだろう．いずれにせよ一般大衆に知恵がつけば，それだけでも十分なプレッシャーとなって，粗悪品は市場から締め出されてゆくはずである．デビッドサービスの開始とともに，最近銀行のカードは勝手に危険きわまりないものに変身してしまったが，この問題でも大衆のセキュリティに関する知識水準がもう少し高ければ，あんなにスムーズにこのシステムが導入されてしまうことはなかったのではないかと思われる．最近はセキュリティ問題の議論のときにいつも，先般のラブレターウィルス問題に関して書かれたZDNet Newsの記事の皮肉たっぷりのタイトル，

「Microsoftユーザへの愛のむち
一度だまされるのは，だます方が悪い．二度だまされるのは，だまされた方が悪い」

を思い出してしまう[2]．

参考文献
1) 棟上昭男他: 情報技術国際標準化活動の軌跡と展望，情報処理，Vol.41, No.5, pp.561-567 (May 2000)．
2) http://www.zdnet.co.jp/news/0005/16/leibovitch.html (2000.7.23)

Interactive Essay・・・

ソフトにバグはつきものだが

小林 正彦／情報処理振興事業協会セキュリティセンター

情報セキュリティにかかわる仕事をしていると，コンピュータ技術の発展の歴史はこれでよかったのだろうかという思いにしばしばとらわれる．

今年の1月末に中央官庁のホームページが連続クラッキングされて以来，セキュリティポリシーという耳慣れないしろものが重要であることへの理解は広まってきた．しかし各組織でセキュリティ対策を担当する部署の最前線では，リストに次々に付け加わる膨大な数のセキュリティ・ホールとの格闘の毎日を余儀なくされているということは必ずしも経営トップの理解するところとはなっていない．

セキュリティに関する「バグ」や「仕様上の問題」は，（数え方にもよるが）インターネット周辺のメジャーなソフト全体で，毎日1個以上というペースで見つかっている．高木氏が発見した大物クラスに限ってみても相当数ある．そして，同氏のような情熱を持って企業や関係機関と接触した者なら，きっと冒頭の私の思いを共有しているのではないかと勝手に思っている．

実はこの文を書くはめになったのは，高木発見をきっかけに，あるメーリングリスト上で彼と議論を行った時の参加者の一人が，エディタの塚本氏に私を推薦したからしいのだが，ここではそのときの議論よりももっと大風呂敷を広げて，情報セキュリティ文化論として意見を述べてみたい．

それはやむを得ない選択なのか

「ソフトにバグはつきものである．」この言い訳を社会はいつまで許していくのだろうか．便利だがバグもた

くさん抱えている時限爆弾のようなソフトに囲まれた華やかな高度情報化（脆弱化）社会を「やむを得ない選択」とする決断をいつしたのだろうか．

考えてみれば異常なことだ．「ソフトにバグはつきもの」という言い訳にあぐらをかいた商慣行が堂々とまかり通っていて，そんなアヤシゲなものを使ったIT革命とやらに世界全体の経済と将来インフラが委ねられているという構図は．

現状では，企業にとって，欠陥の補修は契約上の義務ではなく，「見放されないための顧客サービス」に過ぎないと言える．高木氏が憤っているのもこの辺に1つの原因があり，経営倫理とは次元の違う不遜な文化が指導原理になっている．

思い返すと，私がコンピュータとつきあい始めた30年前は，コンピュータのバグに対する社会の対応は今ほど寛容ではなかったように思える．大型計算機もよく転けていたし，バグに泣かされる現場も今と同様多かったが，今ほど諦観的ではなかった認識がある．

当時と今の決定的な違いは，パソコン～始終原因不明のダウンをして恥じない機械～とインターネットがなかったことだ．

パソコンソフトは，「プログラムの使用または使用不能により生じた損害に関していかなる責任も負わないものとします．」というような文言を仕様許諾書に書くことで免罪符を手に入れてきた．

このような脱法的使用契約を許さず，過去のどこかのタイミングでソフトとPLをしっかり結びつけていたとしたら，社会は今とは相当異なる

場所に着地していたことであろう．そこでは，20世紀最後の年のキーワードがITではあり得なかったかもしれない．では，今日に至るコースは歴史的必然だったのだろうか．

パソコン文化とインターネット文化の不幸で宿命的な婚姻

今日の情報セキュリティ環境は，「便利であれば多少の不具合には目をつぶるもやむなし」というパソコン文化と，情報を共有しそれにだれでもアクセスできることが善であるインターネット文化の宿命的な結びつき（それは宿命であったと思う）に源がある．

前者からはPL逃れを許す悪しき文化を引継ぎ，後者からは，悪意への備えに頼りなさがあるインフラを引き継いでしまった．

これが，個人的利用や学術の世界だけで使われているうちは「困ったもんだ」で済ませたかもしれなが，経済取引を始めとする社会の基本インフラに使おうという選択がなされるところで，宿命から脱するべく何らかの抑制がかかってもよかったのではないだろうか．できの悪いインフラを使って構築した社会が，その脆弱性ゆえに後にしっぺ返しを受けるという構図は今までいたるところで経験したことなのだから．

運命の転換点は，もう過ぎてしまったのか．今ならまだ間に合う，というか，私には今が最後のチャンスであるように感じられる．では，どういう道が残されているのだろうか．

準PL的企業責任論

完成度の高いソフトに囲まれた生活などというものは，時代を20年くらい逆行させたものであろうし，瑕疵ありとはいえそこそこに使える便利な道具の味を知ってしまった今日，そのような退行を社会や経済が許すべくもないことは認めざるを得ない．

ソフトの製造物責任を議論する場合，一般法たるPL法が求める厳密な企業責任がソフトについては非現実的であったために，その対極である「まったくの責任放棄」になってしまい，この中間解に社会がたどり着けなかったことに問題があると考えるべきである．これは，パソコンソフトに対する初期の「甘えの構造」をずっと引きずった結果と思える．すなわち，責任の範囲を限定・緩和したソフト版企業責任論の可能性はなかったのだろうかという問いが必要なのではなかろうか．

たとえば，ソフトの欠陥がもたらす結果に対しては厳密な製造物責任を問わないこととする一方で，製造者が知り得た欠陥については，その事実の公表等に一定の社会的ルールを作ることが可能であるように思える．

もう一歩踏み込んで考えると，欠陥に対する責任を社会的に果たす用意がある企業に対しては，欠陥をオープンな型で公表させつつ，その影響と対処策を十分説明する義務を負わせることと引き替えに，結果責任を緩和することとし，企業のこの種の活動に対して第三者的立場から評価を行う，ソフト版消費者センター的機能をボランタリーに成立させるというような将来像ならありそうではないか．

オープンソースへの道

社会的なインフラたるべきソフトは，「枯れた」ものを使うという選択も考えられる．これは必然的に社会の進歩の速度を抑制することになるが，将来にわたる社会的コストを考えた場合，総合的な損得は評価が分かれるところであろう．

枯れたソフトを使うための1つの考え方がフランスで提案されている．公的機関が導入するソフトはオープンソースであるべきことという新政策である．つまり，多くの人の監視下に置かれた基盤ソフトの方が，瑕疵を減らせるという哲学である．米国のソフト覇権に対抗するためのフランス流の抵抗という側面はあろうが，味わう価値のある提案ではなかろうか．

（2000.7.23）

結論なんか書けない

高木 浩光／電子技術総合研究所

このエッセイで私はいったい何を言いたかったのだろう？　書き始めた当初の仮題は「Javaは脆弱か？」だった．「安全」と言われてきたJavaアプレットが実は危険なのだということになれば，原子力技術のごとく市民に毛嫌いされかねない．Javaをいとおしむ技術屋の立場からすれば，「あれは実装のミスなのであってJavaに構造的欠陥があるわけではない．」と擁護したいところなのだが，話はそう単純なものではない．JDK 1.1までのJavaの古いセキュリティ機構は，こうした実装ミスを生みやすいものだったと私は思う．その意味では構造的な欠陥があったと言える．それが，JDK 1.2以降（Java 2）では，新たに導入されたセキュリティ機構によって，こうしたミスが起きにくくなっていると私は考えている．情報処理学会の場であるのだから，そうした技術的な議論を書くべきだったかもしれない．しかし，ベンダの態度について書き始めたら筆が止まらなくなってしまった．ミスが起きてしまったときの対応がこんなのであるかぎり，研究屋の重箱の隅をつつくような技術論など，ただただ虚しい．

当事者は返事をくれない

パソコンメーカの「OEMだから何もしない」という態度については，メーカの立場を説明してほしかった．OEMとは本当にそういうものだろうか？　Microsoftのサポート窓口に電話して，Windowsのプロダクト・キーを告げると，「それはOEM版なので，お使いのパソコンのメーカに問い合わせてください．」と門前払いされるのを知ってのことか？

「IEを起動するとMicrosoftのホームページが開かれるのでそこからセキュリティ情報のページにたどり着けるはず．」と答えたメーカのパソコンのIEは，出荷時状態で，そのパソコンのホームページが最初に現れるように設定されている．そしてそこには，Microsoftのセキュリティ情報のページへのリンクは存在しない．

最低でも，各社のパソコンのサポートサイトから，Microsoftのセキュリティ情報のページへリンクを設けるべきなのは明らかだ．そんな簡単なことがなぜできないのか理解に苦しむ．ソニーに対して2月に，東芝に対して3月にそれを提案したが，「検討します」と言っていたのに5カ月経っても何も改善されていない．そして現在も穴のあいたままの製品が警告なしに出荷され続けている．

IPAの小林さんからはPLの観点からコメントをいただいた．私は法的あるいは行政的な議論には門外漢なので，ここでは庶民的倫理観に基づく発言しかできなかったが，私も素人ながら思い描いていた考えを代弁していただくことができた．ただ，オープンソースがこの問題の解決になるとは思わない．

再びAppleの対応について

棟上さんは「Apple社ともあろうものが...訝しい思いは残る」と，アップル信仰がおありのようなので，その幻想を打ち砕いておきたい．

7月22日にAppleのサポートに，「セキュリティ・ホールがあるという報道を見た．どうすればよいか教えてほしい．」と電話してみたところ，「最新のIE 5.0を使用していれば大丈夫です．」という回答だった．この問題は，7月7日にリリースされたMRJ 2.2.2をインストールしないと解決しないのであるから，この回答は誤りである．「本当ですか？　その回答は公式なものですか？」と確認をしたところ，「少々お待ちいただけますか．」と上司に相談に行った窓口のオペレータは，「公式な回答です」と自信満々に同じ回答を繰り返した．「情報源を教えてほしい．」と質問したところ，教えられたのはWindows版のIEのページと1年前に見つかったJavaScriptのセキュリティ・ホールのページだった．ここまでで40分が経過していた．最終的に正しい説明を受けたのは1時間7分30秒が経過した時点であった．このように，先述のTILの告知ページは，Appleのサポートセンタのオペレータでさえ見つけられない場所にひっそりと置かれているのである．

「Apple Computerのトップページ（home page）からリンクせよ」とまでは言わないが，TILのトップページからくらいリンクしてもいいはずだ．実際，TILのトップページには重要な情報へのリンク集である「お読みください」というコーナーがある．なぜここに載せないのか，その理由を説明するよう求めたところ，23日に電話があり，「セキュリティのことですから当社も重大な問題と受け止めています」と言う．そんなことは九官鳥でも言える．サポート係すら知らないという状態が「重大な問題と受け止めている」という態度のはずがない．

ウェブ版で続きを

このまま時間切れで終わるのはなんとも虚しい．Appleとインターネットマガジンからの回答がウェブ版に寄せられることを願う．もし本会誌の出版までに何も掲載されていなかったなら，そういうことだ．

（2000.7.25）

議論の続きは，次のURLをご覧ください．
http://www.ipsj.or.jp/magazine/interessay.html