Wat00043 「コンピュータウイルス」について
#0000 dando　8809241222

　この項目は、科学フリートークの＃１２３、科学記事ウオッチの＃３９及びパソコン通信の＃４４に分散している「コンピュータウイルス」の話題を集約して、まとまった議論を展開していただくために設けました。
（団藤）

#0001 匿名　8809241709

先日のＰＣ－ＶＡＮであったウィルス事件は、実際はウィルスではないと思います。あれは、トロイの木馬というものだとおもいます。多分、現在アメリカでウィルス（本当の）が流行っていたので、それに便乗したものだと、私はおもいます。

#0002 sci1113　8809242033

ところでウイルスってどうやって作るのですか？
異機種間でも感染するのでしょうか
初歩的ですみません
ｓｃｉ１１１３

#0003 sci1012　8809250018

いつのまにか、議論が終結してしまっているようですが、せっかくですので、昔の話を蒸返すようにアップします。

今週の TIME(Sept 26,1988,No39)の cover story は、Computer Virus についてです。
TIME はアメリカでは朝日新聞ぐらいメジャーなもので、そのカバーストーリーは、一面トップ＋社説といった程度の重みを持つものですから、ちょうど機を一にして日米でコンピュータ・ウィルスが話題になったということになりますね。
ただ、朝日の場合とは違って、５ページも使って、漫画もまじえながらわかりやすく話を展開しているのは、さすがアメリカンジャーナリズムという感じで、典型的な日本の新聞である朝日とは比較にならないぐらい面白い記事でした。
こんなことを書くと朝日の記者さんに怒られそうですが、朝日新聞と TIME とを購読
しているものとしては、角間隆氏が The English Journal で書いている通り、TIME の
ほうが、読む気をそそるような書き方だし、背景の説明は親切だし、予備知識を要求しないし…と、格段に親切です。
例えば、政治欄なんかは、連載小説と同じで、途中から読むものにはちんぷんかんぷんという感じがします。科学面はその点は比較的親切で、なんとか読者にわかるように書こうと努力している様が伝わってきますが、紙面の都合のせいか、結局中途半端になってしまっていますね。

なんか論旨がぐしゃぐしゃになってしまいましたが、要するに言いたいことは、ウィ
ルスの記事が一面トップだったのは、とくに大げさというほどのことではないし、素人にわかるわからないという議論も、日本の新聞記事の何割が”素人”にわかるかと考えれば、とくにほかの記事と違いがあるというほどではない、ということです。
なお、私は、「こっちだって狭い紙面に出来るだけわかりやすく、しかも出来るだけ多くの情報を詰込もうとしているんだ。毎日読んでるんだから、多少のことは説明しなくてもわかるだろう。毎日読んでればそのうちわかるさ」という、突放したような態度が好きで、TIME の様にこってりくってりと毎日やられると、「しつこい」と癇癪を起こしてしまうでしょう。

OMEGA

004 komor　　8809261832

東京本社管内の紙面には、９月１６日の解説面で岡記者のＰＣ－ＶＡＮのウ

イルス解剖記事が掲載されましたが、ほかの地域はページ数が少ないので掲載されていません。ーーーー　同じ値段なのに、と怒らないでネ。
そこで、読めなかった人のためにアップします。

○　コンピュータウイルスの脅威　侵入後、基本ソフト書き換え

　ディスクに感染して増殖も

　今年初めから主に米国で騒がれ始めた「コンピューターウイルス」というやっかい者が、日本の大手パソコン通信網にも侵入し、その脅威がわが国でも現実味を帯びてきた。このウイルス、本体は０と１の符号列にすぎないが、潜り込んだコンピューターの中でとんでもない悪さをする。目にみえず、他のコンピューターに「感染」し、症状が出るまでに「潜伏期」があったり、特定の相手を傷める「種特異性」をもっていたりする点は、生物に感染するウイルスとそっくり。その正体と対策は――。（岡明人記者）

　コンピューターウイルスは、電算機網に侵入し、機能妨害あるいは不正使用をねらうハッカーの巧妙な産物だ。日本電気のパソコン通信ネットＰＣ－ＶＡＮで見つかったウイルスは、ハッカーが大勢のネット会員に、電子メールで送りつけたプログラムの中に仕掛けられていた。

　普通の電子メールは日常語で書かれた通信文だが、これはゲームソフトのように、パソコンそのものを動かす命令の塊だ。それには、このソフトはある人が作ったものであなたにもあげます、との文が添えてあった。もらった人は、一体何だろうと興味津々で、そのプログラムを使ってみた。期待に反し、ゲームも何も始まらなかった。

　ところが、その瞬間、「ウイルス」がパソコンに潜り込んでいた。実は、そのプログラムは、パソコン内部の半導体メモリーに記憶された基本ソフト（ＯＳ）を書き換える仕組みになっていたのだ。

　どう書き換えたかというと、その後で通信ソフトを起動し、ＰＣ―ＶＡＮにつながると、その人の本人確認の暗証符号を、ネットの中のある掲示板に暗号化して書き込むようになっていた。仕掛けたハッカーは後で、その書き込みから暗証符号を復元し、その人になりすましてネット侵入を繰り返していた。

　「コンピューターウイルス」は本来、そのプログラム自体を自ら複製し増殖して広がることから名づけられた。こんどの例では、日本電気の専門家によると、まずパソコン本体のメモリーに入り、そこからフロッピーディスクという外部媒体に乗り移る「感染力」をもつ。本体のメモリーを“治療”しないまま別の通信ソフトのフロッピーに差し替えて使うと、やはりそのディスクの内容の一部が書き換えられるという。

　ウイルスプログラムは、本体の半導体メモリーの情報を、フロッピーディスクなどの外部記憶装置にコピーするなどの自動実行命令を組み込む必要がある。ベーシック

などの一般的なプログラム言語で初心者がそれを作るのは不可能なので、犯人は間違いなく相当高度の知識をもっている。

日本電気でも、このプログラムの本格的な構造分析はまだのようだ。しかし、核心の暗証符号を変えて試みると、それに応じ、ネットに書き込まれる暗号文が変化した。さらに、暗証符号は秘密なので、どんな符号が使われているか分からないはずなのに、今回の仕掛け人は手さぐりをした跡を残さず、すんなりネットに入っていることなどから、暗証符号盗用ウイルスと断定した。

ウイルスがその機能を発揮するまでの潜伏期は、パソコンの内部時計や乱数を使って仕掛けられる。今度のは通信ソフトを起動し、ＰＣ―ＶＡＮに接続するという、ある操作を「引き金」として「発病」する型だ。

感染する相手を選ぶというのは、パソコン機種の違いで、プログラムに互換性がないことによる。判明した被害者は、ワープロなどで通信していた人でなく、すべて日本電気のパソコンＰＣ－９８００を、その機種用の基本ソフトＭＳ－ＤＯＳで利用していた人だった。

では、ウイルスの感染防止、発見、追い出し対策はどうか。

まず、ウイルスは第１段階でパソコンの半導体メモリー、それも書き換え可能なＲＡＭというメモリーに忍び込む。だから、ソフトを取りかえたり、別の機能を使う時などにこまめにパソコンの電源を切ってやれば、そこで電気という栄養源を絶たれ、ウイルスはメモリーから消えて死ぬ。電源を切らずそのまま、フロッピーなどを使うとそこに感染する。その場合、フロッピーを書き込み禁止状態にして使えば、ウイルスの侵入は食い止められる。

侵入された場合、ウイルスの大きさ、つまり、プログラムの情報量は、正しいプログラムの中に巧妙に潜り込むので、ウイルス部分を特定しにくい。今度のウイルスは、侵入先のプログラムの長さを、約６０００バイト（英数字で６０００字に相当）増やした。それだけ、発見しやすかったわけだが、米国などではプログラムの大きさを変えないウイルスも登場しているようだ。その場合でも、書き換わったことを、プログラムの全文字を数値としたある合計値の変化で発見できることもある。

そうした手掛かりを使って、ウイルスを見つけソフトを守る「ワクチン」と称するプログラムも出回っている。だが、ワクチンも本物と同様、特定ウイルスにしか効果がない。

なによりの自衛策は、あやしげなプログラムとの接触を絶つことのようだ。

大阪科学部　小森

#0005 reader　8810040647

ウイルスの記事が出たときに、ついに来たかと事の重大さに
みぶるいする思いでしたが、サイエンス・ネットのこれまでの書き込み
を見るとあまり深刻にはとらえられていないようです。
ウイルスはパソコンの問題ではなく、コンピュータ・ネットワークの
問題であるとおもうのですが。
開放系としてのコンピュータ・ネットワークは、パソコン・ネットには
限りません。遊びの世界の、したがってＩＤを不正に使われてもせいぜ
いアクセス料を盗まれる（とはいえこれだって立派な盗みです）レベル
とは違い、最近ととのってきた大学間のネットや、複数企業間を結ぶ
商業ネットワーク、さらに近い将来サービスが始まるであろう（ＩＮＳ
６４などというかたちですでに一部はじまっていますが）公衆データ
通信網などにウイルスを流す人間がいて、システムの防護レベルが今
のレベルに甘んじていたとすれば、大変な社会的問題になるに違いあ
りません。
だからといってチェックやガードを固くしすぎては、せっかくのシス
テムがうまく働かなくなるし、管理社会化が進み、息苦しい世の中に
なってしまうでしょう。
あれはウイルスだ，いや、トロイの木馬だなどという用語論議よりも
もう少し議論するテーマがあるような気がします（用語論議が不要だ
と言っているわけではありません。コンピューター・セキュリテイの
専門家どうしの議論なら、このレベルの用語も厳密につかわれるべき
かとも思います。しかし、新聞の記事レベル、すなわち、コンピュー
タあるいはコンピュータ・ネットワークとそれに対する行為が社会に
与える影響を考えるレベルでは、他人のあるいは公共のシステムにこ
っそりと不法に侵入するプログラムをウイルスと総称するというくら
いでいいのではないでしょうか。
朝日新聞制作局開発部　矢崎　朋夫

#0006 komor　8810041506

ホイ、小森です。

ＰＣ－ＶＡＮのウイルスは「ウイルス」と呼ぶべきか「トロイの木馬」と呼ぶべきかについてチョット発言します。

ＰＣ－ＶＡＮの奴も一応、増殖するのです。
メールで送られてきたプログラムを動かしてもウイルスは、ストレージ上の”ＣＯＭＭＡＮＤ．ＣＯＭ”ファイルに潜り込むだけ。その後、デイスクの”ＣＯＭＭＡＮＤ．ＣＯＭ”にその結果が反映されるのは、別のタイミングになる。その間、ウイルスは、いくつかの”ＣＯＭＭＡＮＤ．ＣＯＭ”に感染することができるわけです。もちろん、犯人がそれを意図したかどうかは別ですけど。

確かに、メールで送られてきたプログラムは「トロイの木馬」だと思うのですが、じゃ、木馬から出てきたやつは何と呼べばいいのでしょうか。
”ＣＯＭＭＡＮＤ．ＣＯＭ”の中に潜んでいて、悪さをするのですからウイルスでいいのではありませんか。

大阪科学部　　小森　真幸

Ｐ．Ｓ．
「トロイの木馬」のルーツは１９６０年代のＭＩＴのドクター論文とか、どなたかコピーを持っている方、送っていただけませんか。

ｓｃｉ１１１３さんへウイルスの作り方は『ラジオライフ』に聞いてください。うちでは、ちょっと・・・・

#0007 ultra　8810041640

寝た子を起こすようですが、はたまた、「こんぴゅーたーういるす」（ウフ、ひらがなだと、とってもキッチュ！）論争に一言。
私が、おかしいと思うのは「あれを、ウイルスと呼ぶのはおかしい」という意見が「まにあ」の皆様の中で沸騰しとるのに、「あのワクチンを、ワク

チンと呼ぶのは、もっとおかしい」という意見がなんで出ないんでしょ。（それとも、この話はすでに解決ずみで、私が知らないだけならゴメン！）

　だって、ワクチンっていわば、予防接種でしょ。病気にかかる前に、重病にかからないよう、免疫を付けるために打つもんです。それを、ウイルスに感染してから打っても、ワクチンにならない気がするのですが。どちらかというと、病気にかかったかどうかを見る、いわば「診断薬」といったもんじゃないでしょうか。

　なんでこんなこと言うかというと、別にこれ以上言葉の定義で遊ぶつもりはないのです。もともと、コンピューターウイルス関連の言葉なんて、メタファーの部類の言葉でしょうから、自分の良く分かっている分野だけに閉じこもって、他にあまりきつい態度をとっても仕方ないではないか、ということです。

　ウイルス論争をやってる皆様は、きっとパソコンのエキスパートの方々だと思います。だから、私の想像では、思考のベクトルが鋭くパソコン方向に向いてしまい、こんな医学方面からの言葉の定義問題には、関心がなく問題視されないのだと思います。（勝手な想像です）

　ただ、自分達の思考がきつく向いているところに、どうも外来者、それも素人と見なしたくなるような者（まあ、記者のことです）が、迷い混んで来ると、自分達の思考ベクトルに沿って「こら素人、来るのは１０年早いわ、はっはっは」というようなマイナーな反応、対応しかとれないとしたら、やっぱりまだ、こりゃ、成熟してない分野だな、と思い残念でした。

　みんなで仲良くパソコン通信文化を育てましょうね、懐柔策にでるウルトラ久保田であった。

#0008 sci1003　8810071948

コンピュータウイルス報道ウォッチング

１０／７（金）　６：００ｐｍ　ＴＢＳテレビのニュース番組「テレポート」で，コンピュータウイルスが紹介されました．その中で，月刊アスキー誌の編集者の方が，「ウイルスは，メモリー中のデータやプログラムを書き換えたり，このようなディスケット（３．５インチディスクを手にとってカメラに向けながら）や，ハードディスク（パソコンの全面をトントンたたきなが

ら）のデータやプログラムを書き換えてしまうことがある」というようなこ
とを説明していました.
そのとき，画面に「ウイルスはハードを破壊する」というようなテロップが
表示されました．私はその文字をみて，少々うなってしまいました．うーむ.
ひとに物事を説明するのは，めちゃくちゃ難しいという一例でした　RUKAS

#0009 reader　8810100511

えーと関連発言７のウルトラさんのワクチンの語議についてですが
僕が雑誌,net 等で読んだところによると，確かに今日本でＰＤＳ（パブリック　ドメイ
ドメイン　ソフトウェアー）として広がっている　comchk.com（作者　魔女）は
ms-dos　の　command.com　の改変の有無を調べるものですが，アメリカで同じく
ＰＤＳとして配布されているワクチンプログラムの中には　VirALARM, TCELL など
は，（直接見たことがないので正しくは分かりませんが）MS-dos に常駐してファイル
の改変を監視したり，防いだりするそうです．また別のプログラムはある特定の
ビールスプログラムにの情報を持っておりそのビールスをディスクの中からさがし
だす
そうです．こういったプログラムは発病前（ビールスプログラムが最初に動く前）
の免疫と厳密にいえると思います.
また，アスキーネットの pcs では comchk.com について「あのワクチンを、ワクチン
と
呼ぶのは、もっとおかしい」という意味の記事が複数ありました.
というわけで，（私はエキスパート等では全然ありませんが）エキスパートの方
はきつい語議定義をするようです.
ちなみに月刊アスキーの１０月号（次号にも）にウイルス，ワクチンプログラムにつ
い
て比較的詳しい記事が載っていました（上はほとんどその受け売りです）
（７の発言の’仲良く’に賛成する）　　出淵卓

#0010 sci1080　8810310756

この問題、ほとんどアガリになってしまったようですが、個人的にいろいろと興味のある問題ですし、今後ともパソコンユーザーにとって大きな問題を含んでいるのでこのままアガリにしちゃうのはもったいない。気を取り直して書いてみます。ここでの議論が今後の紙面に生かされればいいですね。

まず用語定義の話ですが、記者の方は例のＰＣＶＡＮのやつを何が何でも「コンピュータウィルス」でいいんだ、ということらしいので、何を書いても無駄みたいですからやめときます。そもそもこの単語の厳密な定義がない状態ですから先に言った方が勝ちです。その結果、ある種の極めて安全な、ごく一般的なプログラムでも、ＯＳの状態を書き換えてある条件のもとで結果的にユーザーに不利益をもたらしたために新聞記事のレベルで「これはコンピュータウィルスだ」と書かれて、そのプログラムを作った人がカンカラカンに怒ったとしてもしかたのないことです。

ぼく自身は、問題のプログラムを「いわゆるコンピュータウィルス」または、「問題のプログラム」と表記することにします。

本題です。

発言４に掲載されている記事に書かれている「いわゆるコンピュータウィルス」の動作は要点をきちんとおさえてあると思います。「ハッカー」という用語の使い方は疑問ですが、新聞記事のレベルではいいとしましょう。「フロッピーを書き込み禁止状態にして使えば」というのは、具体的に「プロテクトシールで」と書くとわかりやすいと思います。あと、問題のプログラムを実行した直後には、COMMAND.COM の大きさは変化しないので、ファイルサイズに頼るのはちょっと危ないと思います。「いわゆるワクチン」とやらは持っていないので、よくわかりませんが、今回のような場合、あれもあまり意味がない。本当は、「ＴＳＲユーティリティ」のようなものを使うべきところでしょうが、これはあまりにも専門的すぎますね。あと、不幸にして「感染」が判明した場合の復旧方法などが書いてあればよかったのに、と思います（復旧方法ったって、システムをコピーしなおすだけですから）。

結局のところ、最後に「なによりの自衛策は、あやしげなプログラムとの接触を絶つことのようだ」が正解となるんですが、これがまた「こんぴゅーたまにあ」としては考え込んでしまうところなんですね。特に、今回の場合、問題のプログラムは「あやしげ」でもなんでもない、正当なプログラムとして送りつけられてきたはずです。少々強引ではありましたが、パソコン通信の慣行上、善意の行為とみなされたであろう行為でした。

ぼくとしては、「あやしげなプログラムとの接触を絶つ」だけではあまりにも安易ではないかということです。できれば、コンピュータユーザーのセキュリティ意識にまで踏み込んでもらいたかった。

今回の事件の教訓とは、パソコンを使うひとりひとりのユーザーがそれぞれシステムのセキュリティ意識を向上させなければならない、ということだとぼくは考えています。

コンピュータという強力な情報処理マシンは、その情報処理能力が強力で柔軟であるが故の弱点を持っています。特にネットワークによって情報の共有化が進めば、さらにセキュリティ意識が重要性を増してきます。

今回の事件は、実害がなく、また問題のプログラムがほとんど「伝染性」を持たず、世間に広がらなかったのですから、具体的な発見方法よりも、コンピュータネットワーク時代に生活する者としての心構えが問われるのではないでしょうか。

発言５に「だからといってチェックやガードを固くしすぎては、せっかくのシステムがうまく働かなくなるし」と書かれているのには同感です。ここでのポイントは、セキュリティ意識の向上は、チェックやガードを固くすることではないということでしょう。昨今、個人情報の保護ということが問題になりつつあります（例の法律はどうなったんだろう？）。これは単にパソコンユーザーだけの問題ではないはずです。

もうひとつ、「あやしげ」に関連してＰＤＳ（フリーウェアなどを含む）の問題があります。

実を言うと、発言４に掲載されている文章の中で、個人的に一番ひっかかったのが「あやしげなプログラム」という下りでした。・・・といっても、ここにひっかかる人はほとんどいないでしょうが・・・。

上述のように、今回の「いわゆるコンピュータウィルス」は正当なプログラムを正当な方法で送り付けています。つまり、優秀なＰＤＳとして定評のある（！）プログラムを、おそらく「素晴らしいＰＤＳだけどＰＣＶＡＮにはアップロードされていないものを持っているので送ってあげましょう」とか何とか言ってメールで送りつけたんでしょう（ボードにアップロードされなかったのは、せめてもの救いです。そこまでやるにはさすがに気が引けたのか、露見を恐れたか？）。

ＰＤＳは無料で、しかも極めて品質の高い有用なソフトとして、今後とも「みんなで仲良く育てる」「パソコン通信文化」のひとつの目玉となるはずのものです。ＰＤＳによって、コンピュータはさらに利用価値があがり、それらがソフトウェアや利用技術全体に及ぼす影響は非常に大きなものがあります。

発言４の問題のくだりは、ぼくとしてはＰＤＳ全体を「あやしげ」よばわりされているような抵抗を覚えたわけです。

　もののついでですが、今回の事件では実害はなかった、というようなことがマスコミで言われていますが、間接的にＰＤＳの作者が被った不利益なり迷惑は大変なものです。犯罪が成立するかどうか、などということも書かれているようですが、ＰＤＳを作者の意図とは全く異なるものに意図的に改変して第三者に渡しているわけですから、明らかな著作権侵害行為ではないのでしょうか。一般的にまだ「知的所有権」や「著作権」の意識は低いようですが、このような無形の権利を不当に侵害する行為にも、もっと敏感であるべきだと思います。

　話がそれました。続きです。
　プログラムには「バグ」という、プログラム上のミスによって、思いがけず利用者がなんらかの損害を被ることがあります。この被害の責任はプログラムであるとすることも出来るでしょう。では、プログラムのバグに損害の原因を求めれば解決する問題でしょうか。原因がどこにあろうとも、プログラム作成者は被害の賠償をしてくれるわけではありません。
　プログラムにはバグがあるもの、コンピュータは壊れるもの、ディスクは読み出せなくなるもの、等々といったことはコンピュータの専門家にとっては常識です。そして、この常識に従ってバックアップなりスペアなりを用意しているからこそ、複雑なシステムもなんとか安定して動いているわけです。
　ここでもやはり重要なことは、ソフトウェアの問題以上に、利用者側のセキュリティ意識です。パソコンは小さいとはいえ、立派なコンピュータですから、上に書いた「常識」はそのままあてはまります。
　確かにＰＤＳは自由にコピーされて流通するソフトとしての性格から、意図的な改変などの危険が入り込む余地はあります。しかしそのような危険はプログラムのバグやコンピュータの故障同様、利用者側の注意で最小限に食いとどめることができるようなものですし、またいやしくもコンピュータの利用者であれば、そうであるべきです。
　今回の記事でも、そうした利用者側のセキュリティ意識にまで持って行けば、単なる「ウィルス騒ぎ」から、さらに一歩踏み込んだ内容のものになったのではないでしょうか。
　また一読者としては、なかなか普通のパソコンユーザーには徹底しない、このようなセキュリティ意識こそ、新聞に書いて欲しいところですし、そのような記事を通じてパソコン利用者以外の読者にもコンピュータとセキュリティの問題に興味を持ってもらいたかったと思います。オンライン犯罪など、現代の日本で生活する限り、コンピュータとは無縁ではいられないのですから。

安田

#0011 sci1901 8811250042

結構前の res ですけどウイルスはハードも壊すのは事実ですよ。
トロイタイプのでそういう奴があったと思います。
Sakaikun sci1901

#0012 sci1501 8811280237

ども、こんにちは。
用語についてですが、「ウイルス」「ワクチン」だけでなく、
「木馬」についても私などは抵抗を感じます。
確かに pc-van で問題となったＩＤ＆ＰＡＳＷ窃盗プログラム
は一見、無害な羊の皮をかぶっているわけで、その意味ではそ
れを「トロイの木馬」と呼んでも意味は･ はおかしくないのでしょ
うが・・・。そうすると、偽装プログラムはすべて「木馬」と
いうことになってしまう。
やはり、システム侵入を計る物に限定して「木馬」と呼びた
いような気がするのですが。
ＴＷ

.