情報システムと社会環境　72－8
（1999．9．27）

教育用コンピュータシステムの運用管理に関する研究
―学部内サーバおよびＰＣクライアントのウィルス対策―

遠藤教昭† 高橋勝彦†

1999年に入って、悪質なウィルスの話題がマスコミを賑わせている。最近は特に、マクロウイルスといって、ワードプロセッサや表計算のソフトウェアで作成されたファイルに潜んだウィルスの被害が多い。

本学部におけるこれまでの運用結果からみても、短期間の間に比較的多くのウィルスが発見されている。ボーダレスな現代のネットワーク社会においては、大学や企業におけるネットワーク型ウィルス対策ソフトウェアの導入は不可欠と思われる。

Anti Virus Software for PC Servers and Clients in University

NORIAKI ENDO† and KATSUHIKO TAKAHASHI†

In 1999, the appearance of malignant virus has been frequently announced. Recently, the infections of macro virus have increased significantly.

We have been using network-oriented anti virus software for some time. According to our experiences, it is strongly recommended to install network-oriented anti virus software for PC servers and PC clients both in universities and companies.

1. ウィルスとは

1.1 人間に感染するウィルス

ウィルスと言えば、本来は生物に寄生して繁殖する微生物のことである。人間に感染するものとしては、インフルエンザ、ヘルペス、B型肝炎、C型肝炎、成人T細胞白血病、エイズなどのウィルスがある。

感染や発病の防止には、ウィルスと接触しないこと、睡眠や栄養など健康管理に気を付け、場合によってはワクチンの接種を受けて、自己の免疫力を高めることなどが考えられる。

1.2 コンピュータウィルス

一方、コンピュータウィルスの正体はたちの悪いプログラムである。1984年にフレデリック・コーエン氏（米国カリフォルニア大学）が命名した。

パソコンを対象にしたウィルスとしては、1986年に発見されたBrainや、1987年に見つかったJerusalem（エルサレム、13日の金曜日ウィルス）などがその走りである。

他人に悪影響を与えるプログラムという共通点から、狭義のウィルスだけではなく、ワームとトロイの木馬を加えた3種類を総称して、ウィルスと呼ぶこともある[1)]。各社のウィルス対策ソフトウェアも、それら「広義のウィルス」に対処している。

以下にそれら3種の性質を述べる。

1.2.1 ウィルス

本来のウィルスが生物に寄生するように、コンピュータウィルスも他のファイルに感染（寄生）して増殖する。単独では増殖できない。

アプリケーションソフトウェア、マクロ（アプリの操作を自動実行する仕組み）、ディスクのブートセクタ（起動時に最初に読み込まれる部分）に感染する。

1.2.2 ワーム

単独で動作するプログラムで、他のファイルには感染しないが、ネットワーク上を自己増殖していく性質を持つ。

主に電子メールなどを通じて送り込まれる。最近のものとしては、Happy99（1999/1）やExploreZip（1999/6）などがある。

1.2.3 トロイの木馬

単独で動作するプログラムで、他のファイルへの感染も増殖もしない。悪質な者が不正アクセスなどの目的で、他に送り込むプログラムである。

† 岩手大学人文社会科学部
Faculty of Humanities and Social Sciences, Iwate University

一見無害なオモテの機能をもつプログラムだが、相手の情報を盗むというようなウラの機能を隠し持っている。最近では、ダウンロードしたプログラムに隠されているということも多い。

1.3 コンピュータウィルスの行うこと

感染し発病するとコンピュータウィルスは以下のようなことを行う[2]。

- ユーザが知らないうちにコンピュータの制御を奪う。
- コンピュータ上で奇妙な現象（たとえば、ビープ音が鳴る、不快なメッセージが表示されるなど）を誘発する
- 一部のウィルスは破壊的な活動をする。ファイルを損傷、削除したりHDDを完全に消去する場合もある。
- 一部のウィルスは、事前定義されたトリガ日（例えば13日の金曜日）までは潜伏し、トリガ日になると活動する。

2. 望まれるウィルス対策

1999年3月に現れたMelissa、1999年6月に現れたExploreZipなど、最近、悪質なコンピュータウィルスやワームがマスコミを賑わせている。

Melissaは、特定のメールソフトを使用している場合に、多数の感染メールをばらまくというウィルスで、企業のメールサーバがパンクするなどの被害が出た。

ExploreZipは、1999年6月9日に発見された。ローカル・エリア・ネットワーク (Local Area Network; LAN) 上の共有ディスクドライブにも感染し、ファイルを削除するという悪質なワームである。

最近は、インターネットの利用が常識的に行われ、電子メールやWWW(World Wide Web)が、大学における研究・教育や、企業における業務に不可欠のものとなっている。

したがって、電子メールの添付ファイルやWWW上のファイル（表計算やワードプロセッサの文書）に含まれるマクロウィルスやワームによる被害が、もっとも懸念されるところである。

また、本学部においては、そのようなものだけではなく、チャットプログラムによるファイル交換時にトロイの木馬を送り込まれたような形跡も見られた。

大学においても企業においても、ウィルスへの対応が急務となっていると言えよう。

3. ウィルス対策の現状

3.1 ある調査について

日経オープンシステム編集部により、その読者における最近のウィルス対策の現状が報告されている[3]。

この調査では、無作為に選ばれた読者270名に調査票を送り、うち106名から回答を得ている（表1～3）。

回答者の内訳は、情報システム部門40%、研究開発部門25%、営業・販売・マーケッティング部門10%の割合であり、主に企業ユーザであった。

3.2 調査結果の分析と考察

この雑誌の主な読者はシステムエンジニアなので、調査対象は元々ウィルスに対する認識の高い集団であると思われる。さらに、回収率(39.3%)が低いことから、回答者はその中でも特にウィルスに関する関心の高い人々であったということが推測される。

それでも、サーバに関してウィルス対策を施している割合は半分程度であった。今後は、この割合を高める必要があると思われる。サーバが感染すれば多くのクライアントに感染するのは避けられないからである。

一方、PCクライアントに対策をしている割合が相対的に大きいのは、PC購入時にウィルス対策ソフトが附属してくることが多いからかも知れない。

ただ、導入していても最新版が動いているとは限らないので、きちんとパターンファイルの更新をしているか、その頻度はどうかなども合わせて調査する必要があろう。

表1 ここ1年のウィルス感染
Table 1 Virus infections in recent 12 monthes

	比率
感染あり	13.6%
感染なし	86.4%

表2 対策ソフトの導入率（複数回答）
Table 2 Installation ratio of anti virus software

	比率
自分の *PC* に導入	73.6%
社内サーバに導入	49.1%
導入していない	7.5%

表3 使用ソフトウェア（複数回答）
Table 3 Software in use

	使用者数
ウィルスバスター（トレンドマイクロ）	42人
Virus Scan（ネットワークアソシエイツ）	37人
Norton Anti Virus（シマンテック）	29人
その他	3人

さらに、使用ソフトウェアに関しては、サーバ用とクライアント用を分けて調査すべきである。

以上のように、本来はもう少し詳しい調査が必要と考えられるが、この調査は有意義なものであると思われる。

4. ウィルス対策ソフトウェアの条件

著者らは 1998 年に本学部の計算機室 [4] におけるウィルス対策について検討し、対策ソフトウェアの満たすべき要件を検討した。

4.1 本学部で採用するウィルス対策ソフトの要件

(1) サーバーの対策とクライアントの対策が同時にできる。

(2) サーバー上のパターンファイル（いわばワクチンの処方箋のようなもの）の更新が自動でできる。

(3) クライアントに対するワクチンソフトウェアとパターンファイルの配布が、サーバを用いて自動的にできる。

(4) 価格体系がわかりやすく安い。学校に対してはアカデミック割引があれば望ましい。それらがWWWでわかりやすく公開されていること。

4.2 注目した製品

1998 年 8 月に、1997 年の雑誌記事 [5] や各社の WWW ページ（付録参照）を参考に調査したところ、以下のソフトウェアが上記 (1), (3) の条件を満たすように思われた。(なお、ソフトウェアの進歩は速いので、これから導入する方はさらに調査が必要である。)

- InocuLAN (Netware, NT) ☆1
- F-FRONT Professional (Netware, NT, OS/2) ☆2
- LANDesk Virus Protect(Netware, NT) ☆3
- Sophos Anti Virus (Netware, NT) ☆4

最終的に導入を考えたソフトウェアは上記のうち Sophos Anti Virus for Netware である。

(1), (3) に加え (4) の条件☆5 を満たすこと、サーバ用とクライアント用の連携がシームレスであること、アフターサポートがよいことなどを選択基準にした。

また、Sophos Anti Virus は、本学部で使用している Netware4.1 + SFT3（サーバ・ミラーリング）に唯一完全に対応しているということも重要だった。

ただ、このソフトウェアは、(2) に関しては自動でなく手動 FTP である。また (3) に関しては、クライアントに対しパターンファイルの配布をするのではなく、サーバにおいたパターンをクライアントが通信により参照するという、高度なテクニックが使われている。そのため、クライアントに対するワクチンソフトウェアの配布を行わない方法が取れる（ネットワーク型クライアント）。サーバ接続のない PC には、クライアント専用（スタンドアロン）版も使える。

なお、ベンダーに資料を請求したところ、期間限定の評価版を提供していただいたが、フル機能版であったので製品購入の検討にとても有用であった。

5. 稼働実験

Sophos Anti Virus は英国 Sophos 社 [6] の製品で、ウィルス検知エンジンである Sweep と、それとクライアントが情報を交換するためのエージェント InterCheck の 2 つの要素で構成される。1998 年 8 月末から、これを試験運用してみた。

サーバについては、サーバ内の Sweep プログラムによって、HDD の定期的なウィルス検査と駆除が自動スケジュール運転で行える。

クライアントについては、サーバログイン時にログインスクリプトにより、InterCheck プログラムが自動的にメモリに常駐させられる。ユーザが特に意識する必要はないので、非常に便利であった。

これだけで、FD のファイルや WWW からダウンロードしたファイルも全てリアルタイムでウィルス検査できる。DOS, Win3.1, Win95/98/NT, Macintosh 全てのクライアントに対応している。

ただし、本学部の計算機室 PC では、当時、Windows95 のオプションである Plus のエージェントで、1 日に 1 回必ず Scandisk を実行していたのだが、それと InterCheck がバッティングしてしまうようで、Scandisk の実行中に、時々マシンがフリーズするという事態が生じてしまった。

ベンダーに調査を依頼したところ、Scandisk と他の常駐ソフトの同時実行は保証されていないということであった。ベンダーからは、Scan disk のあと InterCheck を常駐させればいいとのアドバイスもいただいたが、そうすると起動時に煩雑になる（途中でユーザがエンターキーを押す必要が生じる）ということなので採用はしなかった。

☆1 http://www.caj.co.jp/products/inoculan/index.htm

☆2 http://www.europe.datafellows.com/japan/

☆3 現在は販売されていない。

☆4 http://www.cseltd.co.jp/SWEEP/index.htm

☆5 一般サイトでは、1 年間の契約料金 22.4 万円で、サーバ 1 台とクライアント 199 台までがカバーできる。(ただ、クライアントがそれ以上の台数の場合は、別の契約方式となり割高になる。) 学術サイトには割引契約があり、1 年間 8.8 万円で、サーバ+クライアントの合計 200 台までがカバーできる。契約すると、毎月アップデート用 CD-ROM が送られてくる。

そのような経緯で、残念ではあったがSophos Anti Virusの使用をあきらめ、ほぼ1ヶ月で稼動試験は打ち切ることにした。学生がPCを乱暴に扱うことがあるので、当時は、Scandiskははずせないと考えたからである。

6. 本格稼働

1999年に入ってから、危険なウィルスのうわさが多すぎるので上記を考え直し、1999年6月にSophos Anti Virusを本格稼動することにした。

まず、サーバ+クライアントで200台まで対応するライセンスを購入した。なお、計算機室のPCは80台である。

そして、授業のときに学生に協力してもらい、起動時にScan diskを実行する設定をはずして、Netware4.1サーバでSophos Anti Virusを再稼働させた。

1999年6月の再導入後、8月までのわずか2ヶ月の間に、Laroux , Cap, Happy99のウィルスが発見された。また、いくつかのトロイの木馬も発見された。

頻繁なウィルス感染はないと思っていたが、予想に反してかなり見つかることがわかった。

一般にも、知らぬ間にウィルスに感染し、さらに感染の拡大を助長してしまっているいうケースが多いのではないかと考えられ、対策は急務であると感じた。

本学部のライセンスには余裕があるので、今後は、計算機室以外の学部共用PCや教官のPCを使う場合も、サーバログインしてチエックすることが望ましいと考えている。

6.1 クライアントPCに与える影響

6.1.1 パターン更新に伴うPCの起動時間の延長

Sophos Anti Virusを利用すると、PCの起動時間がやや長くなる。通常は10秒程度の延長であるからほとんど影響はない。ただ、サーバのパターンファイルを更新したときは、クライアントHDDのフルスキャンを行うので、数分～10分程度は待たされる。なお、この時間はPCのCPU速度や、HDD使用容量などに依存する。

したがって、パターンファイルをどの程度の頻度で更新するかを十分検討し、その方針を決めなくてはいけない。たとえば、以下のような更新頻度が考えられる。

(1) 新規パターンファイルが出るたび毎回

(2) 一定期間ごと（例えば2週ごと）

本来は(1)が望ましいが、ユーザの利用勝手も考える必要がある。本学部では、当面、悪質な新種ウィルスが発見された場合は(1)で、通常は2週間から1ヶ月に1度程度の頻度で更新する予定である。

6.1.2 ウィルスチェックによるPC動作速度の低下

また、実行ファイルやマクロが含まれる文書がリアルタイムにチエックされるので、遅いマシンの場合、若干もどかしく感じるかも知れない。(一般にはほとんど影響はない。)

ただ、以下のような工夫がされており、待たされることによるユーザの心理的な負担は最小限になるよう工夫されている。

あるクライアントが使用して一度チェックされたファイルは、安全性がサーバに登録され、次回からは、どのクライアントがそのファイルのコピーにアクセスしても、チェックは省略され、すぐに使用が許可される。

新規にソフトウェアを導入するときは、Sweepサーバに登録されていない実行ファイルが数多く出現するので、チェックが頻繁になるのは避けられないが、その程度は、得られるメリットから許容範囲と考えるべきであろう。

6.2 運用上の問題

6.2.1 サーバソフトウェアのアップデート

Sophos Anti Virusの場合は、これがやや面倒であった。CD-ROMからファイルを手動でサーバのディレクトリにコピーしなくてはならない。それほど難しくはないが、毎月なので煩雑に感じる。

アップデート作業は、プログラムで自動的にできると便利である。ユーザがスクリプトを自作してもいいが、できればベンダーで用意してくれた方が安心である。

このあたりの使い勝手がソフト選択のポイントの一つとの見方もあるが[1]、著者も作業していて同様に感じていた。

6.2.2 DOS環境で使うとフリーズ

計算機室のWindows95 PCで使用する場合は関係ないが、著者のPCでおきたことを参考までに記す。

DOS (Windows3.1を使う場合も、まずDOSが起動されるので同様) で使用する場合、InterCheckでメモリとHDDのチエックが終わった後に、なぜかフリーズしてしまう。

原因は不明だが、DOSでの使用環境は、Netwareクライアント (NETX) を常駐させていて、コンベンショナルメモリの空きがやや小さいという状況であるので、それらが影響している可能性がある。

本学部でWindows3.1を残しているのは著者だけのようなので、ほとんど問題はないが、企業などで導入する場合は対策を検討する必要がある。

7. 感染時の対応

7.1 Sophos Anti Virus に固有の事項

前述のように、Sophos Anti Virus はウィルス検知・駆除エンジンである Sweep と、それとクライアントが情報を交換するためのエージェント InterCheck の2つの要素で構成される。

サーバのログインスクリプトで、InterCheck をクライアントのメモリに常駐させた場合は、ウィルスが検知されたときに、即駆除するということはできない。

InterCheck は Sweep と交信してウィルスを検出する機能だけを持つので、駆除はクライアント（スタンドアロン）版 Sweep（Sweep for Windows95 など）をインストールして行うことになる。

もちろん、ウィルスが検知された時点でファイルの実行は許可されないので安全上の問題はない。

クライアント版 Sweep を前もってインストールしておくのもいいが、クライアントソフトをインストールしていなくてもウィルスチエックできるという Sophos Anti Virus のメリットも大きいので、ケースバイケースで考えればいいと思われる。

7.2 一般的な事項

Sophos Anti Virus だけではなく、クライアント専用版を含め、ウィルス対策ソフト一般に当てはまる事項である。

(1) マクロウィルスは一般に駆除可能である。

(2) ブートセクタ型ウィルスの場合は、安全なブート FD と MS-DOS 版ソフト（Sophos Anti Virus では Sweep for DOS）を用いて駆除を行う。

(3) 実行ファイル型ウィルスは一般に駆除ではなく、感染ファイルの削除によって対処する。

8. クライアント版ウィルス対策ソフトとの比較

Sophos Anti Virus のようなネットワーク型を導入した場合とは異なり、クライアント専用版を使う場合は、ユーザ自身が定期的に自分の PC のパターンファイルを更新する必要がある。その頻度は、少なくとも月1回程度にはしたい。

もしソフトが PC 附属の試用版などである場合は、早急に製品版にアップグレードする必要がある。

そして定期的にベンダーのホームページをチエックし、危険なウィルスが出現した場合は、とくに迅速に対応しなければならない。

多くのクライアント PC が存在する大学や企業においては、ネットワーク型ウィルス対策ソフトを採用すれば、新規パターンファイルの導入の際などにはシステム管理者だけが留意すればいいので、望ましい運用ができる。

一般ユーザにウィルス対策の必要性を教育することは必要だろうが、そうしたとしても全てのユーザがクライアント専用型対策ソフトを使いこなせるとは思えないからである。

特に学生用の計算機室においては、ネットワーク型以外の選択肢はないだろう。

9. ベンダーの選択

9.1 継続したサポートがあること

某社は最近ウィルス関連ソフトの開発を中止した。今後はある別会社の製品を推奨すると WWW ページに掲載されていた。某社製品は、一時は本学部でも導入の候補として考えただけに若干驚いた。

ウィルス対策ソフトは、購入後のサポートがとても大切なので、ユーザにはそれを見極める目が必要とされる。

9.2 十分な情報公開があること

著者の経験からすると、ホームページが充実しているベンダーは、やはりいいのではないかと思われる。もちろんそれだけではないが、最新のパターンファイルや駆除情報がホームページで公開されるからである。緊急の情報がリアルタイムで得られとても便利である。

新種ウィルスが見つかった場合の電子メールによる通知の無料サービスを行っているところもある。

また、本学で見付かったようなある程度ありふれたウィルスに関しても、きちんと説明[7)8)]があると一般ユーザはとても助かる。

またホームページにウィルス対策入門のような文書やソフトのマニュアルの PDF ファイルを置いているベンダもあり[7),9)]、初心者から管理者までにとても有用である。以前だと、おそらくかなり探さないと得られなかったような情報であるが簡単に手に入る。

10. おわりに

今回の一連のウィルス対策作業を通じ、現代のネットワーク社会においては、大学においても企業においても、ネットワーク型ウィルス対策ソフトの導入は不可欠のものであると感じた。

さて、個々のウィルスを駆除するという作業は、感染した PC を回復させるという観点からは根治的な治療である。

ただ、「ウィルスが蔓延した現代のコンピュータ環

境」の「治療」という観点からは、単なる対症療法にすぎない。

環境全体の根治療法のためには、コンピュータ利用者全体、特にプログラマのモラル向上を図るしか方法はない。

学校におけるコンピュータ教育においても、技術的なことを教えるだけではなく、情報社会におけるモラルを重要視すべき時代に来ているのではないかと思われる。さらに、この種のことについては、高等教育で初めて教えるのでは遅すぎるので、初等・中等教育の段階から時間をかけてゆっくりと教育すべきである。

ボーダレスなネットワーク環境においては、日本だけが頑張っても仕方のないことかも知れないが、世界に範を示すことは可能であろう。

本稿の要旨は、情報処理学会・情報システムと社会環境研究会 (1999 年 9 月 27 日、岩手県立大学) で発表した。

なお、本文からリンクをたどりやすい WWW 版も著者のホームページ[10] でご覧いただければ幸いである。WWW 版は可能なら必要に応じて改訂していく予定である。

参 考 文 献

1) 斉藤栄太郎: 猛威ふるうウィルスの危険度 ―猛威は種類でどう違う、ワクチンソフトは万能か, 日経コミュニケーション (1999/7/5).
2) シマンテック: Norton システムワークスユーザズガイド, シマンテック, 東京 (1999).
3) 日経オープンシステム編集部: ウィルス対策, 日経オープンシステム (1999/6).
4) 遠藤教昭, 五味壮平, 白倉孝行, 高橋勝彦, 進藤浩一: 教育用コンピュータシステムの運用管理に関する研究ー学部内ＰＣクライアントマシンの運用管理ー, 情報処理学会研究報告 (コンピュータと教育研究会), Vol. 98, pp. 1–8 (1998).
5) 麻生次郎, 矢崎茂明: ウィルスと闘う ―被害件数は過去最高、対抗策の整備を急げ, 日経オープンシステム (1997/7).
6) *http://www.sophos.com.*
7) *http://www.nai.com/japan/techinfo/whitepaper.asp.*
8) *http://www.europe.datafellows.com/japan/virinfo/index.html.*
9) *http://www.cseltd.co.jp/SWEEP/menu3/downl.htm#report.*
10) *http://www.hss.iwate-u.ac.jp/endo/index-j.html.*
11) *http://www.virusbtn.com/100/.*

付　　録

A.1 ウィルス対策製品の主なベンダー

- Trendmicro Japan☆1
- Symantec Japan☆2
- ネットワーク・アソシエイツ☆3
- シー・エス・イー☆4
- コンピュータ・アソシエイツ☆5
- 山田洋行☆6

各ソフトウェアのウィルス検出能力については、英国の雑誌 Virus Bulletin の Virus Bulletin 100 Percent Award[11] が参考になる。

A.2 最近発見されたウィルスやワーム

この節は、シー・エス・イーやネットワーク・アソシエイツの WWW ページを参考にしてまとめた。

A.2.1 W97M/Melissa

Melissa は、Microsoft Word 97、Microsoft Word 2000、および Microsoft Outlook の E メールクライアント上で動作する。

このウイルスは、当初、あるニュースグループで発見された。ある WWW サイト用のパスワードを含んだファイル (List.Doc) が感染元であるとされている。ユーザーがこのファイルをダウンロードし、そのファイルを開くと文書中のマクロ☆7 が実行され、電子メール・アドレスにある 50 人に感染ファイルである List.Doc を転送する。そのメールの受信者も同様に添付ファイルを開くと同様な事が生じる。また、ウイルスはシステムに侵入後、他の文書にも再感染するので、再感染ファイルをメールで送信した時も受信者側で同様な事が生じる。Word 2000 の機能の一つである「セキュリティ」設定をデフォルトの「高」から「低」に変更する。これによって、ユーザーがマクロを含んでいるファイルを開こうとした際に、警告メッセージが表示されず、結果的にこのウイルスは感染するチャンスを増やすことができるのである。

A.2.2 W32/ExploreZip.worm

1999 年 6 月に発見されたこの新種ワームが、世界

☆1 http://www.trendmicro.co.jp/
☆2 http://www.symantec.com/region/jp/products/nav.html
☆3 http://www.nai.com/japan/
☆4 http://www.cseltd.co.jp/sweep/index.htm
☆5 http://www.caj.co.jp/products/inoculan/index.htm
☆6 http://www.europe.datafellows.com/japan/
☆7 マクロとは、作業を自動化するための仕組みであり、表計算ソフトやワードプロセッサソフトなどが持つ機能である。マクロを作成するには、ユーザの手動作業を自動的に記録する方法が使えため、ユーザはあまり意識しないで使用していると思われるが、一種のプログラムである。

各地で報告されている。マイクロソフトのメールソフトを用いて自分自身を送付し、c, cpp, h, asm, doc, xls, ppt の拡張子の付いたファイルを消去する。

ローカルドライブだけでなく、該当マシンからアクセス可能なネットワーク上のドライブ（マップされたドライブ）でも同様な消去が行われるので非常に悪質である。

また、ローカルまたはネットワークドライブに存在するシステムファイルに、マシン起動時にワームが自動実行されるように設定するという機能も持っている。日本でも被害が報告されている。

A.2.3 W97M/JulyKill

このウイルスは英語版 Word97 では繁殖せず、日本語版、台湾語版など2バイト版の Word97 でのみ繁殖する。autoexec.bat を書き換え、次回起動時にファイルの全消去を行うというかなり悪質な機能を持つウイルスである。日本でも被害が報告されている。

A.2.4 W97M/Story

このウイルスは IRC（インターネット・リレー・チャット）を利用して自分を配布するという新しい感染形態を有している。mIRC という米国では定番の IRC クライアントソフトがインストールされていた場合、"C:¥MIRC¥SCRIPT.INI" というスクリプトが落とし込まれる。特定のサイトに電子メールを送付する機能を持つ。

A.3 本学部で見つかったワーム

A.3.1 Win32/Ska.A（Happy99）

電子メール及びニュースグループにより拡がるワームである。感染した PC からの電子メールや、ニュースグループからのダウンロードにより着信する。

まず、メールに添付されてきた Happy99.EXE を実行すると、画面上に花火が上がる。

そのあと、ユーザが使用したことのあるニュースグループや電子メールアドレスに自分自身を送付する（uuencode された Happy99.exe を添付）。

このとき、ワームは感染したマシンのユーザの E-Mail アドレスを送信者として使用するため次の受信者は、知り合いからのメールと思いこみまた上記のように実行してしまうわけである [8]。