研究室内ＰＣ－ＬＡＮにおけるウィルス対策について

5Ｇ－5

大網啓之　菅野文友
帝京平成大学大学院情報学研究科

１．はじめに

現在ダウンサイジングによるクライアント／サーバシステムが活用されている．その構築にパソコンだけを利用したＰＣ－ＬＡＮ（パソコンＬＡＮ）も多用され，そのＯＳは，ＧＵＩ環境のものとなっている．ＧＵＩ環境のＯＳをもつパソコンを使ったＰＣ－ＬＡＮを本研究室内に設定し，このようなネットワーク環境で，実際に発見されたウィルスに近い機能をもつ仮想ウィルスを作成して，マシン単体での影響とネットワーク上での影響を検討した．また，現在利用が急増しているインターネットのanonymousFTPサーバ等から持ち込まれる圧縮ファイル解凍時に出てくるウィルスを想定し，その検出についても検討した．

２．利用システムの構成

図１のように，サーバにアップル社のQuadra840AV，クライアントにアップル社のLC-520と，Centris660AVおよびCentris610を使ったクライアント／サーバシステムのＰＣ－ＬＡＮを，利用した．

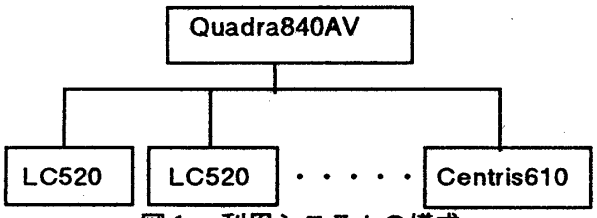

図１　利用システムの構成

３．仮想ウィルス

３．１　ファイルについて

ＭＳ－ＤＯＳで使用されるファイルは，実行可能なプログラムファイルと，プログラムが利用するデータファイルにわけられる．マッキントッシュのファイルは図２のように，リソースフォークとデータフォークの二つから構成されている．

３．２　マッキントシュ用ウィルス

多くのマッキントッシュのウィルスは，実行コードが存在するリソースフォークに感染する．これだけでは，マッキントシュとＭＳ－ＤＯＳの両者のウィルスは，ファイル構造の違いからは全く違うようにもみられるが，基本的な構造は同じであり，両者とも感染先として，次のような３つの条件があげられる．

１）プログラムに制御が回ってくる
２）プログラムの書き換えができる
３）ウィルスプログラムが発見されにくい

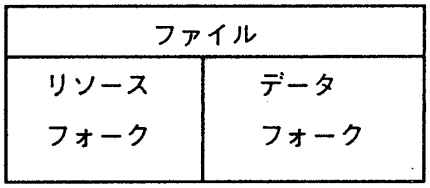

図２　マッキントシュのファイル構成

今回作成して利用した仮想ウィルスは，上の３つの条件を満たし，そして，マッキントッシュのウィルスに多いリソースフォークへ感染するように設定した．以下に、その設定概要を示す．

１）ＷＤＥＦ（ウィンドウ定義関数）という実行コードを持つリソースになりすまして侵入する．
２）指定したアプリケーションにだけ感染する

Virus countermeasures in laboratory PC-LAN

Hiroyuki OHAMI, Ayatomo KANNO
Graduate School of Information Sciences,
Teikyou Heisei University

3）発病のきっかけ（発病トリガ）は，感染ファイル実行時にＷＤＥＦリソースを利用したときとし，その発病症状は，任意の文字列の表示とビープ音の鳴動とする．
4）ネットワーク上のことは，考慮しないものとする．

4．ウィルス対策について

仮想ウィルスを使って検討した結果，次のことがわかった．

4．1　マシン単体

（1）ウィルス侵入の判断

1）発病症状
2）アプリケーションからの警告
3）動作不安定

がでない限り，難しい．

（2）感染ファイルについて

ファイルのもとからある部分に上書きして，感染するウィルスもある．したがって，

1）ワクチンを使っても完全には回復できない場合がある．
2）ワクチンで処理しても，１度感染されたファイルは，更新または再インストールしたほうが良い．

4．2　ネットワーク上

（1）ウィルスの侵入について

1）ログイン後に，サーバにアクセスできる状態において，サーバの共有ファイルに完全な感染をすることはできない．
2）アクセス権設定がしっかりされていない，もしくは書き込み禁止にできない場合，サーバ上のファイルをただ壊したり，ファイルのリソースを消したりすることは可能である．
3）2）のような場合，共有ファイルは，定期的なバックアップや点検が必要である．

5．圧縮ファイル解凍の際に出てくるウィルス検出

（1）ファイルが圧縮されている状態

圧縮アルゴリズムが公開されていなければ，暗号化された状態と同じになっている．したがって，既知ウィルスのウィルスコードと比較してウィルスの有無を調べる検索タイプのワクチンでは，圧縮ファイル中のウィルスの発見は難しい．

（2）ファイル解凍後のワクチン処理

圧縮ファイル解凍のたびにワクチンで調べるのは手間がかかる，また，それを忘れる可能性もある．

（3）（1），（2）を考慮したウィルス検出

以下に説明するプロセスで，圧縮ファイル解凍の際に出てくるウィルスの検出を行った．

1）バックグラウンドで圧縮ファイルを識別し，解凍時にリソースフォークへのアクセスを監視する．
2）他ファイルのリソースフォークに変更がないかどうかを確認する．
3）変更があった場合，そのことをダイアログボックスで知らせる．

こういったことによって，ウィルスに侵入された可能性があることがわかったときに，既存のワクチンを利用して、ウィルスが広がることを防ぐことができる．また圧縮ファイル解凍の際のウィルス感染の確認作業を，簡略化できる．

6．おわりに

今後，この圧縮ファイル解凍の際のウィルス検出を，ＰＣ－ＬＡＮシステム全体で使い，サーバへのアクセス権をコントロールできるようにすることを計画している．

参考文献

[1] 渡部　章：”コンピュータウィルス辞典”，オーム社（１９９３）
[2] 実吉，崔，青木：”コード変更によるコンピュータウィルスの防御”，電子情報通信学会総合大会論文集，基礎・境界，A-337,pp.337（１９９５）