コンピュータセキュリティ 18－8
(2002. 7. 18)

仮想サーバを使った未知ウイルス検知システムの提案

三宅 崇之† 白石 善明‡ 森井 昌克†

†徳島大学 工学部 知能情報工学科 〒770-8506 徳島県徳島市南常三島 2-1
‡近畿大学 理工学部 情報学科 〒577-8502 東大阪市小若江 3-4-1
E-mail: †{miyake,morii}@is.tokushima-u.ac.jp, ‡zenmei@is.kindai.ac.jp

あらまし 電子メールを利用して感染活動を拡大するコンピュータウイルスが社会問題となっている．ウイルス検知手法として最も一般的に用いられているパターンマッチング方式の場合，ウイルスを検知するためにウイルスを解析し，そのウイルスを判定するためのパターンファイルを作成する．このパターンファイルによって解析済みのウイルスは確実に検知することが可能である．しかしながら，この方式では未知ウイルスを検知することができない．本稿ではユーザが電子メールを受信する前にメールサーバ内の仮想マシン上でウイルスの可能性がある添付ファイルを受信し，その挙動を監視することで未知ウイルス検知を行うシステムを提案する．

キーワード コンピュータウイルス，未知ウイルス，パターンマッチング方式，仮想マシン

A Method to Detect Unknown Computer Virus Using Virtual Server

Takashi MIYAKE† Yoshiaki SHIRAISHI‡ and Masakatu MORII†

† Department of Information Science and Intelligent Systems, Tokushima Universiry
Minamijosanjima-cho 2-1, Tokushima, 770-8506 Japan
‡ Department of Informatics, School of Science and Engineering, Kinki University
Kowakae 3-4-1, Higashi-Osaka City, 577-8502 Japan
E-mail: †{miyake,morii}@is.tokushima-u.ac.jp, ‡zenmei@is.kindai.ac.jp

Abstract The spread of computer virus via E-mail is a social problem. In some virus detection system with pattern matching mechanism, they can detect the virus as long as they have pattern files corresponding to that. However, such a system can not detect an unknown virus. In this paper, we propose a system to detect unknown virus. The system receives all E-mail in user's place. That opens and executes the mail with attached file and watches its behavior against Operating System etc. in order to detect the unknown virus.

Keyword Computer Virus, Unknown Virus, Pattern Matching Mechanism, Virtual Machine

1. まえがき

近年のインターネット利用者の拡大に伴い，ネットワークを用いた犯罪件数が増加し社会問題となっている．その代表として「不正アクセス」，「サービス拒否攻撃（DoS 攻撃）」，「コンピュータウイルス」などが挙げられる．特にコンピュータウイルス（以下，ウイルス）は増殖能力を持ち不特定多数のユーザを標的とするため，その影響は大きく，またその被害報告数は毎年増加する一方である．これらの被害を最小限に抑えるためのウイルス検知技術の開発は今後のインターネット社会を支える重要な課題として盛んに研究・開発が行われている．

情報処理振興事業協会（IPA）[7]が公表している国内のウイルス被害届出状況によると，1990 年から 1996 年の間では年間 1000 件程度の届出であったのに対し，1997 年以降では 2000 件を超え，2000 年は 11,109 件，2001 年では 24,261 件とその被害数は急激に増加しており，2002 年では現時点で既に前年を上回っているという報告もされている．

このようにウイルス被害が増加し続ける背景にはインターネット利用者の急増，個人や企業のセキュリティ意識の低さなどが理由として挙げられる．しかし近年ウイルス被害が急増した最も大きな原因は新種の非常に強い感染力を持ったワームウイルスの出現である．ワームウイルスはネットワークを通じて他のコンピュータへと拡散し，自己増殖活動を繰り返すことによって被害を拡大させる能力を持つ．現在も猛威を奮い続けている W32.Klez の場合，昨年 10 月にオリジナルが発見された時は月の被害届出件数が十件程度であったのに対し，今年 1 月末に亜種が出現してからは一気に被害が拡大し，さらに亜種が増えた 4 月には Klez による被害が 2012 件と被害届出件数の全体の 8 割を占

める結果となった．これは現在主流となっているパターンファイルを用いたウイルス検知技術が既知のウイルスに対しては非常に有効な技術ではあるが，新種，亜種のウイルスに対して脆弱であるためにここまで被害が拡大したと言える．

本研究では従来手法であるパターンマッチング方式とは異なり，新種あるいは亜種のウイルスを効果的に検知するとともに，ユーザによって不用意にウイルスが実行されることを防止することを目的としたシステムを提案し，その構築を行う．また，今回提案するシステムはウイルスの侵入経路として最も大きな割合を占めている電子メールの添付ファイルを検知対象としたものになっている．以下，2 章にてコンピュータウイルスについての定義とその検知手法について説明を行い，3 章にて今回提案するシステムについて述べる．4 章にてシステムの一部を用いた有効性の検証実験を行った結果と考察を述べ，5 章にて諸考察，そして最後にまとめを述べる．

2. コンピュータウイルス

2.1. コンピュータウイルスの概要

コンピュータウイルスとは不特定多数のコンピュータに何らかの意図的な被害をもたらすために作られたプログラムの総称を指す．経済産業省の「コンピュータウイルス対策基準」[6]によると，コンピュータウイルスとは『第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり，次の機能を一つ以上有するもの』と定義されている．その機能とは以下の 3 つである．

(1) 自己伝染機能
(2) 潜伏機能
(3) 発病機能

2.2. コンピュータウイルスの特性

コンピュータウイルス感染時の症状はその被害によって大きく以下の 3 つに分類することができる．

(1) ワーム的動作
ワームはネットワークを通じて他のコンピュータに拡散し，ウイルスによる被害を拡大することを目的とする．主に自分自身のコピーを電子メールの添付ファイルとし，他のコンピュータに送信することで拡散する．

(2) ファイルの改ざん
ウイルスがコンピュータに感染するために自分自身のコピーを行う時，ファイルの改ざんが発生する．感染活動の内容としては実行ファイルへの寄生，Word, Excel などのテンプレートファイルの変更，特定の拡張子を持つファイルの内容の変更，削除，Windows の場合であればレジストリの変更，削除などがある．

(3) 不正な情報流出
トロイの木馬型の一種であり，ネットワークを介して他のコンピュータに不正なプログラムを侵入させ，外部から操作することによって，パスワードなど重要な情報を盗む．

以上 3 つの動作がウイルスによる主な被害であると考えられる．これらのウイルスに対して次に述べる手法を用いてウイルス検知を行う．

2.3. ウイルス検知手法

ウイルスの検知手法は現在のところ既知ウイルスに対して有効な手法であるパターンマッチング方式と未知ウイルスに対して有効なヒューリスティック方式に分類されている．

2.3.1. パターンマッチング方式

パターンマッチング方式は既知ウイルスに対して有効なウイルス検知手法であり，通常のアンチウイルスソフトで多く用いられている．その検知方法はウイルスプログラム内の特徴的な部分をパターンとしてデータベース化しておき，そのパターンを用いて検知対象のファイル内容の検査を行う．同じパターンを持っているプログラムが発見された場合，そのファイルはウイルスであると判断する[2]．

この方式では新種のウイルスが発見されるたびにウイルスを解析し，識別用のパターンを抽出してパターンファイルを追加登録する．よって新種のウイルスに対応するためには，常にパターンファイルを定期的に更新し続けなければならない．

結果としてこの方式を用いた場合，パターンファイルが用意されている既知ウイルスについては確実に検知できるが，新種のパターンファイルが定義されていない未知ウイルスに対しては検知することができない．このような短所から未知ウイルスに対応するための検知技術としてヒューリスティック方式が考案されている．

2.3.2. ヒューリスティック方式

ヒューリスティック方式とは，「試行錯誤を繰り返すことによってウイルスを発見する方式」である．すなわちパターンマッチング方式のようにパターンファイルとの単純な比較によってウイルス検知を行うのではなく，プログラムを解析することによって，そのプログラムが取る行動パターンを収集し，ウイルスであ

るか否かを判断する方式である．ヒューリスティック方式は行動パターンの収集方法の違いによってスタティックヒューリスティック方式とダイナミックヒューリスティック方式に分けられる[2][3].

(1) **スタティックヒューリスティック方式**
スタティックヒューリスティック方式はあらかじめウイルスが取る可能性の高い行動パターンとして記述されているプログラムコードをデータベースに登録する．検査対象となったウイルスの疑いがあるファイルに対してはコードによるパターンマッチングを用いた検査を行い行動パターンの収集を行う．収集した行動パターンの少なくとも 1 つがウイルスの特徴と同様のものであった場合，ウイルスと判断する．しかし，この方式ではウイルスが取る可能性の高い行動パターンを収集しているため，ウイルスに似た行動を取る正常なプログラムをウイルスと誤検知してしまう可能性がある．また，同じ行動パターンを表すプログラミング方法は 1 つとは限らず，そのすべてのコードを登録することは困難である．

(2) **ダイナミックヒューリスティック方式**
ダイナミックヒューリスティック方式はウイルス感染の疑いのあるファイルをメモリ上，もしくは隔離された実マシン上で実行し，その行動パターンを収集する．収集した行動パターンがウイルスの動作であると確認された場合，ウイルスと判断する．この場合，ウイルスは隔離された環境で実行されるため，システムがウイルスに感染することはない．スタティックヒューリスティック方式との違いは前者が静的にプログラムファイル中のウイルスの行動パターンを表したコードを探し出すのに対し，後者は実際に実行し，その実行結果を行動パターンとして収集する点である．このため，スタティックヒューリスティック方式のようにプログラミング方法に影響されることもなく，結果としての行動パターンにだけ着目すれば良い．

いずれの手法も未知ウイルスを完全に検出できる保障はなく，ウイルスである可能性を指摘しているにすぎない．本研究では 2 つの手法を組み合わせ，効率的に未知ウイルスを検知するシステムを提案する．特に提案手法では，ウイルスの実行を仮想マシン上で行い，正常なコンピュータの動作に支障をきたすファイルの改ざんを高速に検知するところに特色がある．

3. 提案手法

3.1. システム概要

今回提案するシステムのウイルス検知はウイルスの侵入経路として最も大きな割合を占めている電子メールの添付ファイルを対象に行う．具体的には「メールを受信する時」,「メールを送信する時」の 2 つの状況において送受信されるメールに添付ファイルが含まれている場合，ウイルス検知を実行する．

3.1.1. メールを受信する場合

図 1 は提案システムを用いてメールを受信する場合を表したものである．添付ファイル付きのメールを受け取る場合，メールはウイルス検知サーバに送られ検査が行われる．そこで添付ファイル実行時の行動パターンの収集が行われ，ユーザには添付ファイルの動作を示した検査結果メール(図 2)が送信される．検査結果メールには添付ファイル取得用の URL が記述されており，ユーザに直接添付ファイルが届けられることはない．ユーザは添付ファイルの動作検査結果を確認した上で安全な領域に保存してある添付ファイルの取得を行う．このようにすることでユーザが受信したメールを不用意開封して発生するウイルス感染の可能性を減少させることができる．

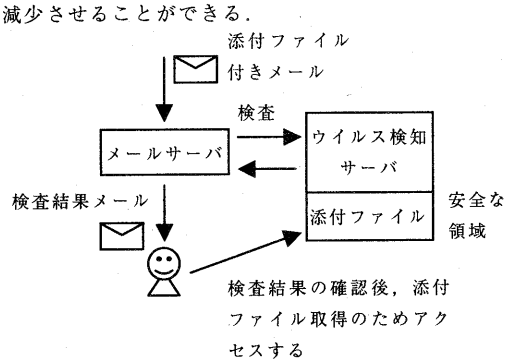

図 1:メールを受信する場合

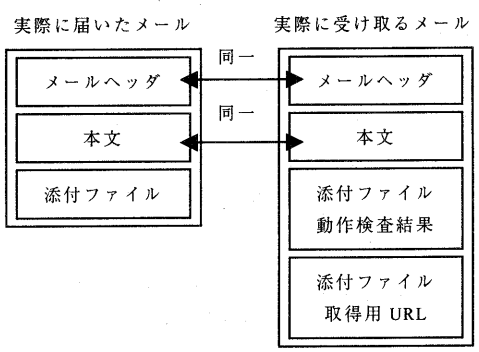

図 2:検査結果メールの詳細内容

3.1.2. メールを送信する場合

図3は提案システムを用いてメールを送信する場合を表したものである．ユーザが添付ファイル付きメールを送信する際，そのメールは一度ウイルス検知サーバに渡され検査が行われる．異常がなければそのまま送信される．しかし，添付ファイルに何らかの異常が発見された場合，ユーザに通知を行い，そのメールの送信は行わない．よって，ウイルスに感染したユーザから他のユーザへの感染拡大を最小限に抑えることができると考えられる．

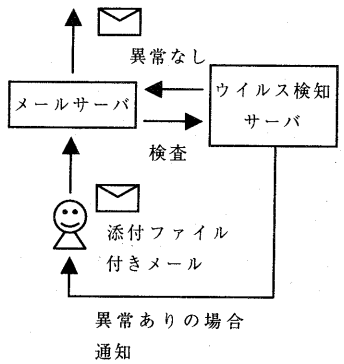

図3:メールを送信する場合

3.2. ウイルス検知サーバ実装手法

提案手法で用いるウイルス検知手法はこれまで紹介してきたパターンマッチング方式，スタティックヒューリスティック方式，そしてダイナミックヒューリスティック方式を用いる．特にダイナミックヒューリスティック方式では，これまでユーザホストのメモリ上でシステムやOSと切り離された特別な対話ルーチンを用意し，この対話ルーチンを用いて添付ファイルを仮想実行することで，ウイルス特有のファンクションコールの有無を監視する手法が提案されていた．しかし，この方法では予想される全てのファンクションコールに対応する必要があり，未対応のファンクションコールや作成ミスがあることで検査用ホスト自体が感染してしまうなどの問題があった．そこで本手法ではホストエミュレータを用いることで完全な仮想ホストマシンを構築し，メールに添付されているファイルを実行・検査する手段を提供する．

3.2.1. 検知手順

検知手法としては検査が容易な，すなわち短時間で検知可能な方法から，詳細な検査を必要する方法へと移行するふるい法を用いる(図4).

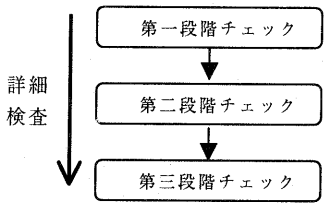

図4:三段階に分けた検査方法

各段階の機能の詳細について述べる．

- **第一段階:メールヘッダ，添付ファイルの検査**
  過去に発見されたウイルスの特徴から明らかにウイルスメールと判定できる要素を持つメールを検出するために，メールヘッダ内のパターンマッチングを行う（例:From欄が空白）．また添付ファイルが以前にウイルスとして検知されていないか確認を行う．検査対象ファイルのハッシュ値を以前取得したウイルスファイルのハッシュ値と比較することによって検査を行うことができる．新たにウイルスを検出した場合，その特徴を学習し，次回の検知に用いる．
- **第二段階:プログラムコードの検査**
  添付ファイルを検査対象とし，ウイルスが取る可能性の高い行動パターンを表すプログラムコードの存在の確認を行う（例:外部と通信を行う関数の呼び出し）．第二段階でも第一段階と同様の学習機能を持つ．
- **第三段階:仮想実行後の行動パターンの検査**
  仮想マシンを用いて添付ファイルを仮想的に実行し，行動パターンの収集を行う．そしてその行動パターンがウイルスのものであるか検査を行う．検査方法は2つあり，ワーム対策として自動的にウイルス付きメールを送信する動作の検出，ファイルの改ざん対策としてファイルのハッシュ値を取得し，以前取得したハッシュ値との比較を行い，改ざん等の検出を行う．また，第三段階も第一，第二と同様の学習機能を持つ．

この検査の流れによって，第一段階では主に既知ウイルスの検知，第二，第三段階において未知ウイルスの検知を行う．

3.2.2. 仮想マシン

第三段階にて仮想実行を行う為の仮想マシンには今回 VMware[8]を利用する．この理由は VMware の Host-only モードを利用することで1台の PC の中に閉じた仮想ネットワークを構築できること，また，

Nonpersistent モードでは起動後行ったすべて動作がVMware を終了することで破棄できるからである．よってウイルスに感染しない仮想実行環境を実現することが可能となる．各モードの詳細について述べる．

- **Host-only モード**
  Host-only モードの概要を図 5 に表す．特徴は
  1) 実機と仮想マシンだけで独立した仮想ネットワークが構築可能．
  2) 通信は仮想ネットワーク上だけに限定され，実ネットワークとは通信不可能なように設定可能．つまり，ウイルスを実行した際に他のネットワークに被害を与えることのない閉じたネットワークの構築が可能となる．

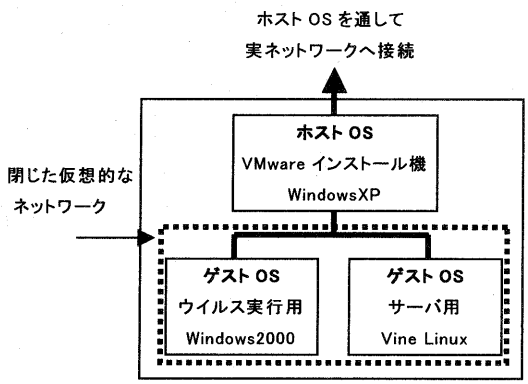

図 5:Host-only モード

- **Nonpersistent モード**
  起動後行われたすべての動作が元の仮想ディスクにまったく影響を与えることがない．VMware を終了するとすべて破棄され，前回起動直後の状態を復元することが可能である．よって，ウイルスの行動パターンを収集するためにウイルスの実行を行ったとしてもシステムが感染することはない．

3.2.3. ウイルスの実行方法

ウイルスは直接実行できる場合もあれば，特定の条件下でなければ実行できない場合も存在する．主な発病条件として，第一に日付，曜日，月など時間的な条件，また特定のソフトウェアが導入されているなどといったコンピュータの使用環境的な条件の 2 つが挙げられる．提案システムではこれらの発病条件をシステム上で実現するために以下の方法を用いる．

(1) 既知ウイルスの発病条件の収集，整理．
(2) 未知ウイルスの場合，プログラムコードを解析し，新たな発病条件の発見．

ただし，プログラムコードの解析によって新たな発病条件の発見が可能かどうかについては現在検討中である．近年主流となっているウイルスはメールをプレビューした際に感染活動を行うため，ほとんどのウイルスは直接実行可能なプログラム形式となっていることが多い．

3.2.4. ワームウイルスの検知手法

ワーム的特徴を持つウイルスは主にメールを感染媒体として他のコンピュータへと拡散し，その被害を拡大することを目的としている．ワームウイルスは実行されるとコンピュータ内のアドレス帳，またはキャッシュの中を検索し，メールアドレスを探し出す．そして探し出されたアドレスに対し，自分自身を添付したウイルス付きメールを送信する．つまり，このようにメールを用いて感染を拡散させるワームウイルスに対して有効な検知方法は，実行した際にメールを送信するかどうかという点に着目することである．そこで以下の手順にてワームウイルスの検知を行う．

【ワームウイルスの検知手順】

(1) VMware にゲスト OS としてインストールした Windows の標準アドレス帳に宛先の存在しないダミーのメールアドレスを登録．また，標準メーラである OutlookExpress にはウイルス検知に用いる SMTP サーバへのアドレスを設定する．
(2) 仮想マシン上でメールの添付ファイルを実行する．
(3) 実行した添付ファイルがワームウイルスの場合，アドレス帳を参照しリストに存在するアドレスに対してウイルス付きメールの送信を行う．
(4) (3)で送信されたメールはもう一つのゲスト OS である Linux 上の自作 SMTP サーバへと渡される．
(5) 自作 SMTP サーバはメールを受信した段階でこのプログラムをウイルスであると判断する．
(6) ウイルスと判断された場合，SMTP サーバでは受領したメールを解析し，ウイルスの特徴を抽出する．
(7) 抽出した特徴を検知用データとして学習する．

この検知方法を用いることでメールを媒体として感染を拡散させるウイルスに関しては検知可能となる．

3.2.5. ハッシュ値を用いた改ざん検知手法

ウイルスはワーム活動を行うだけでなく，感染活動も行う．感染活動とはコンピュータのシステムファイルなどにウイルスコードを書き加えたり，自分自身のコピーを感染マシン内に置き実行可能な状態にするこ

とである．感染することによってコンピュータ内部に侵入したウイルスは，特定のトリガ，あるいはWindowsであればレジストリの変更によって起動時に発病する．ウイルスが発病した場合，システム内の重要なファイルの改ざん，削除などさまざまな被害をもたらしかねない問題を引き起こす．このため，ハッシュ値の比較を用いてファイルの改ざんを検出することで，そのような問題を引き起こすウイルス検知を行うことができると考えられる．以下にその手順を示す．

【ハッシュ値を用いた改ざん検出手順】

(1) 標準状態におけるファイルのハッシュ値をあらかじめ取得．
(2) 仮想マシン上でメールの添付ファイルを実行．
(3) 添付ファイルがウイルスの場合，自分自身のコピー，特定の拡張子を持つファイルの改ざん，レジストリの変更などが行われる．
(4) 再度，ファイルのハッシュ値を取得する．
(5) 改ざんが行われている場合はハッシュ値が異なるため検出可能．

ここで考えられる問題点として，

- 通常の正常なプログラムであってもファイル内容の変更（改ざん）を行う可能性．
- すべてのファイルのハッシュ値を取得するためには比較的処理時間が必要．

ということが考えられる．特に処理時間の短縮を図るためにはハッシュ値を取得するファイルは過去に改ざんが行われた拡張子だけに限定する．あるいは，改ざんによってシステムに被害を及ぼす可能性があるファイルだけに限定するといった措置が考えられる．よって処理速度の向上を図るとともに，変更されたファイルによってあらかじめ付けて置いた危険度によって検査対象となった添付ファイルの危険度指数の通知を行うことも可能となる．

4. 実験

4.1. 実験内容

提案した手法の一部のシステムが完成したため検証実験を行った．実験内容は検知手順の第三段階におけるワームウイルスの検知手法とハッシュ値を用いた改ざん検知手法を用いた場合におけるウイルス検知手法の有効性の確認である．提案手法は未知ウイルスを検知することを目的としているが，今回の実験では未知ウイルスではなく最近社会問題となったウイルスの代表として W32.Klez.H，W32.FBound，W32.Hybris を用いた実験を行った．これら3つのウイルスを仮想マシン上で実行し，作成した2つの検知手法を用いて検査を行う．表1に実験環境を示す．

表 1 実験環境

CPU	Athlon 700Mhz
Memory	384 Mbyte
HD	ATA66
ホスト OS	WindowsXP Professional
仮想マシン	VMware workstation3.1
ゲスト OS 1	Windows2000 Professional
ゲスト OS 2	Vine Linux 2.5 Commercial Release

4.2. 実験結果

表2に実験結果を示す．表2は検査対象となったウイルスがワームウイルスの検知手法（以下，手法 1）とハッシュ値を用いた改ざん検知手法（以下，手法 2）のどちらの手法によって検知されたかを表したものである．

表 2 実験結果

	手法 1	手法 2
W32.Klez.H	×	○
W32.FBound	○	×
W32.Hybris	×	○

4.3. 実験結果に対する考察

実験結果から今回実験に使用した3つのウイルスは提案手法を用いて検知することが可能であることが分かる．以下にそれぞれのウイルスが持つ特徴と合わせて考察を行う．

- **W32.Klez.H の場合**
  W32.Klez.H は大量の電子メールを送信し，また感染マシン上にある特定のファイルを電子メールの添付ファイルとして外部に送信する能力を持つ．W32.Klez.H が実行されると，自分自身を Windows のシステムフォルダ内にコピーし，レジストリに値の追加，あるいは新たに作成を行うことによって，Windows が起動されるたびに毎回ウイルスが実行されるように変更する．このため手法 1，2 の両方によって検知されると予想していたが，実際には手法 2 だけでしか検知されなかった．理由として W32.Klez.H は独自の SMTP エンジンを用いて電子メールの送信を行うため，Outlook で指定した SMTP サーバにアクセスを行わないことが考えられる．このため，コネクション監視ツールを用いて W32.Klez.H によって行われる外部との通信を監視したが，特に通信を行う様子は確認できなかった．これらの結果から，仮想マシンの設定がウイルスによって電子メール

を送信するための条件を満たしていなかったと考えることができる．

- **W32.FBound の場合**
  W32.FBound は感染マシン上のレジストリに登録されている標準の SMTP サーバと Windows 標準のアドレス帳に登録されている全てのメールアドレスに対して自分自身を添付したメールの送信を行う．ファイルのコピーや改ざん等は行わないため，手法 2 によって検出することは不可能である．しかし，手法 1 によって容易に検知することが可能であった．

- **W32.Hybris の場合**
  W32.Hybris が実行されると，WSOCK32.DLL の改ざんが行われ，ユーザが電子メールを送る際，すべての送信メールに対して自分自身を添付する能力を身につける．よって，実行時に電子メールが送信されるわけではないので，手法 1 による検知は不可能であるが，ファイルの改ざんが発生しているため，手法 2 によって検知することが可能であった．

これらの考察から感染時にコピーや改ざんを行うウイルスは確実に検出することが可能だが，W32.FBound のように感染活動は行わず，電子メールの送信のみを行うウイルスの場合，手法 2 を用いた検知を行うことができない．今回，実験に用いた W32.FBound は登録されている標準の SMTP サーバを用いて電子メールを送信するため手法 1 によって検知することができたが，独自の SMTP エンジンによって，他の SMTP サーバを用いて送信を行おうとするウイルスに関しては今後の課題とする必要がある．

5. 諸考察

5.1. 処理速度に関する問題

提案システムでは三段階の処理を経てウイルス検知を行う．特に第三段階では仮想実行，ハッシュ値取得といった複雑な処理を行うため比較的処理時間を必要とする．その中で最も処理時間を必要とするハッシュ値の取得に関しては，ハッシュ値を取得するファイルを限定するなどして処理の高速化を図っている．しかし，第一，第二段階は単純なパターンマッチング処理を行っているだけなので，その処理時間を比較した場合，ハッシュ値の比較には数十倍の処理時間を必要とする．したがってシステム全体としての処理の高速化を考えた場合，できる限り第二段階までに検知を終了させる必要性がある．そのため学習機能を用いることによって，一度検知したウイルスについては既知ウイルスとし，次回以降は早期段階で検知する必要がある．

5.2. 正常ファイルが必ず第三段階に到達する問題

現在の仕様ではウイルスではない正常なファイルが必ず第三段階にまで到達してしまうことが考えられる．この解決策として近年のウイルスはメールのプレビュー時に感染することを目的としているため，直接実行できる形式を取っている場合が多い．したがってウイルスである可能性のあるファイルの拡張子はある程度限定することができる．よって特定の拡張子を持つファイルのみを検査対象とし，害のない正常なファイルを検査する回数を減少させることができると考えられる．また，Word，Excel などのファイルに関しては第一，第二段階にてマクロが含まれていないことが判定した時点で正常なファイルであると判断することが可能である．

6. まとめ

提案したウイルス検知システムはアンチウイルスソフトで一般的に用いられているパターンマッチング方式では検知できない未知ウイルスの検知を行うだけではなく，ユーザによる不用意なウイルスファイルの実行を防止する効果を持つものである．

従来手法で用いられていた仮想実行は OS から切り離された特別な対話ルーチン上でウイルス特有のファンクションコールの監視を行うものであった．しかしこの方法では予想されるすべてのファンクションコールに対応する必要があり，またそれが不完全である場合，ウイルスに感染する可能性がある．そこで本稿ではホストエミュレータを用いて完全な仮想マシンを構築し，その仮想マシン上でウイルスの実行を行い，その際の動作の監視をすることによってウイルス検知を可能にする手法を提案した．提案手法は検査時のウイルス感染の恐れがなく，また次々と出現する新種の未知ウイルスに対しても有効に検知を行うことが可能な技術である．

今回，第三段階にて用いる手法の検証実験において利用したウイルスが既知のものではあったが，特にそのウイルスを検知するための特別な措置をしているわけではない．したがって提案システムは現在猛威を振るっているウイルスが出現する前に利用していた場合，未知ウイルスとして検知することが可能であったといえる．よって本システムの有効性を確認することができた．

謝辞

有益な御討論を頂いた中尾康二氏をはじめとするKDDI 研究所ネットワークセキュリティーグループの各位に感謝する．

文　献

[1] 三宅崇之，白石善明，森井昌克，“未知のコンピュータウイルス検知方法の提案とそのシステム開発，”信学技法 TECHNICAL REPORT OF IEICE OIS2002-4(2002-5)，pp.19-24，May.2002.

[2] 竹内大輔，千石靖，服部進実，“仮想マシンを用いた実行形型ウイルスの検出，”コンピュータセキュリティシンポジウム 2001，pp.179-184，Oct.2001.

[3] 伊吹賢一，千石靖，服部進実，“ウイルスコードの自動解析を行う学習型ウイルス検出システムの構築，”コンピュータセキュリティシンポジウム 2001，pp.185-190,Oct.2001.

[4] 岡本剛，石田好輝，“電子メールにより拡散するコンピュータウイルスの拡散モデルの解析，”電子情報通信学会論文誌，D-I，Vol.J84-D-I,No.5,pp.474-482,May.2001.

[5] 末松俊成，今井秀樹，“MCMP を利用したコンピュータウイルス対策，”情報処理学会 コンピュータセキュリティ，No.13,pp.1-6,May.2001.

[6] “コンピュータウイルス対策基準”，通商産業省告示 第952号，平成12年12月．

[7] IPA セキュリティセンター
http://www.ipa.go.jp/

[8] VMware. Inc.
http://www.VMware.com/