社団法人　情報処理学会　研究報告
IPSJ SIG Technical Reports

2005－ＣＳＥＣ－30（15）
2005／7／21

コンピュータ・ウイルス対策における疫学的アプローチに関する研究（その２）
－マスメール型ウイルス対策モデルへの適用－

関　聡司[†1]　佐々木　良一[†2]　岩村　充[†3]　本杉　洋[†4]

†1 早稲田大学国際情報通信研究センター　〒169-0051 東京都新宿区西早稲田 1-3-10　早大 29-7 号館

†2†4 東京電機大学工学部　〒101-8457 東京都千代田区神田錦町 2-2

†3 早稲田大学大学院アジア太平洋研究科　〒169-0051 東京都新宿区西早稲田 1-21-1　早大西早稲田ビル

E-mail: †1 sseki@kurenai.waseda.jp, †2 sasaki,@im.dendai.ac.jp,

†3 iwamuram@waseda.jp, †4 motosugi@isl.im.dendai.ac.jp

あらまし　コンピュータ・ウイルスと生物界のウイルスとの様々な類似性から生物界の研究手法である疫学的手法をマスメール型のコンピュータ・ウイルス対策に適用する。マスメール型のコンピュータ・ウイルスは、感染したPCのユーザに直接の被害をそれほど与えないことから、感染に気づかれにくく、ユーザによる対策や駆除に期待することは適当ではない。ユーザに依存しない対策手法として、LAN内におけるSMTPの送信先ポートを変換する方法及びゲートウェイにおいて特定条件下でウイルスの通過を制御する方法の概念を提案し、理論疫学的手法の一つであるシミュレーションがこれら対策手法による効果の検証に適用し得るか確認する。

キーワード　コンピュータ・ウイルス，　シミュレーション，　疫学，　対策評価

Research of Epidemiologic Approach for Anti Computer Viruses - 2
-Application on a model of anti mass-mail viruses-

Satoshi SEKI[†1]　Ryoichi SASAKI[†2]　Mitsuru IWAMURA[†3]　and　Hiroshi MOTOSUGI[†4]

†1 Global Information and Telecommunication Institute, Waseda University　1-21-1-29-7, Nishi-Waseda, Shinjuku-ku, Tokyo, 169-0051 Japan

†2†4 School of Engineering, Tokyo Denki University　2-2 Kandanishikicho, Chiyoda-ku, Tokyo, 101-8457 Japan

†3 Graduate School of Asia-Pacific Studies, Waseda University　Sodai-Nishiwaseda Bldg., 1-21-1 Nishi-Waseda, Shinjuku-ku, Tokyo, 169-0051 Japan

E-mail: †1 sseki@kurenai.waseda.jp, †2 sasaki,@im.dendai.ac.jp,

†3 iwamuram@waseda.jp, †4 motosugi@isl.im.dendai.ac.jp

Abstract　Epidemiologic methods that are the research technique of the living thing field are applied to the anti-virus of mass mail type from various similarities of the computer virus and virus of the living thing field. Infection is not noticed easily as for the computer virus of the mass mail type because direct damage is not given to the user of infected PC too much, and expecting measures and disinfestation by the user is not suitable. We propose the concept of the method of converting the destination port of SMTP in LAN and the method of controlling the traffic of the virus with the gateway under a specific condition as measures techniques for not depending on the user, and we confirm whether the simulation that is one of the theoretical epidemiology techniques can be applied to the verification of the effect by these measures techniques.

Keyword　Computer Virus, Simulation, Epidemiology, Measures Evaluation

1. はじめに

1.1. 研究の目的

コンピュータ・ウイルス（ワームを含む。）のうち、それが感染したPCから特定・不特定多数のメール・アドレス宛に多量のウイルスメールを送信するいわゆるマスメール型のコンピュータ・ウイルスについては、自らSMTPエンジンを動作させてメールを送信するものが多い。そのため、ユーザはメールを送信していることに気が付きにくく、他に特段の不具合が生じなければユーザによる自発的なウ

イルス対策が行われにくい。このようなコンピュータ・ウィルスは、感染した個々の PC に対してはそれほど大きな影響を顕在化させないので、ウィルス削除等の対策がなかなか採られず結果としてコンピュータ・ウィルスとしての寿命を延ばし感染事例が長期に渡って見られるという傾向がある。2004 年度において、最も感染事例の多かったコンピュータ・ウイルスは、マスメール型の Netsky (亜種も含む。) であった。Netsky は、感染した PC 内の特定の種類のファイルからメールアドレスを収集し、独自の SMTP エンジンを用いて、収集したメールアドレス宛に発信者を偽造し自分自身のコピーを添付したメールを多数発信する性質を持つ。感染した PC 及びそのユーザそのものにとっては、感染による直接的な被害はほとんど無いに等しいが、この PC が接続するネットワークやそれに接続する他の PC ユーザには大きな被害を及ぼしている。このようなウィルスの感染拡散を防ぐためには、個々のユーザの対策実施に依存することは適当ではなく、ネットワーク環境として感染拡散防止機能を備えることを検討すべきである。

コンピュータ・ウイルスの感染や拡散等の振る舞いは、生物界のウイルスとの類似性を想起させるが、発病症状の多様化や感染スピードの拡大など集団としての現象把握が必要とされると考えられる[10]ように研究手法についても生物界のそれを適用できる可能性がある。生物界における研究アプローチである疫学的手法：特に理論疫学として分類されるシミュレーションの手法を用いれば、具体的なコンピュータ・ウイルスの検体や大規模なネットワーク環境が無くても、コンピュータ・ウイルスの感染拡散及び制御モデルを作成して、実装前段階の概念的な対策手法についてそれほどコストを必要とせずに対策の効果について一定の評価・確認を行うことが可能ではないかと考えられる。本研究は、マスメール型ウイルスに対する対策手法の概念を提案するとともに、シミュレーション・モデルによる当該対策手法の有効性評価の可能性を探ることを目的としている。

なお、本研究は、早稲田大学プロダクティブＩＣＴアカデミアプログラム(文部科学省２１世紀センターオブエクセレンス(ＣＯＥ))プロジェクトの一環として行ったものである。

1.2. 研究方法

本研究では、まず、マスメール型のコンピュータ・ウイルスに対する対策手法について、感染拡散特性を分析した上で、個々のユーザの対策実施に依存しない対策手法の概念を２つ提案する。

①LAN 内において通常使われる SMTP の送信先ポート番号 25 を全て他の番号に変更する対策手法

②LAN と WAN との間に特定条件下でウィルスの通過を制御する性質を持つゲートウェイを設ける対策手法

次に、これらの２つの対策手法による感染拡散の防止効果を確認するため、文献[6]の研究成果を発展させて、コンピュータ・ウイルスの感染拡散及びその制御に関するマクロモデルをシステムダイナミクスの考え方により規定し、シミュレーションシステムを構築する。このシミュレーションシステムを用いて、対策無しの状態及び次の３つの対策手法のそれぞれについてシミュレーションを実施する。

A. ①の対策を実施

B. ②の対策を実施

C. ①及び②の対策を実施

シミュレーション結果に基づき、対策無しの状態との比較等によりそれぞれの対策の効果について分析を行う。

2. マスメール型ウイルスの感染拡散特性

2.1. 感染拡散の特徴

コンピュータ・ウイルスに感染すると、感染した PC のデータが書き換えられるなどの様々な症状が発生する。感染した PC の使用者にとっては、データを破壊するウイルス、個人情報や事業上の機密情報などを漏洩させるウイルスに感染すると直接的に大きな打撃を被るが、ウイルスに感染してウイルスをばらまいただけでも信用失墜等につながり得る。

ウイルスをばらまく際に送信元アドレスを詐称するウイルスは、ネットワーク全体には大きな影響を及ぼし得るものの、感染者の特定が困難であることから、単にウイルスのコピーをばらまくという症状である限り、感染者本人 (PC)にとってはほとんど支障が無く、感染対策のインセンティブが生じない。感染したことにも気がつかないということが多い。また、ウイルスを受け取った側から、送信者にウイルス駆除等するよう連絡しようとしても簡易にそれをする方法が無い (発信者の IP アドレスは特定し得る場合もあるが当該 IP アドレス宛にメッセージを送る手段が一般的には無い。)。感染者に直接的な支障を与えないという特性は、ウイルスの側から見れば、駆除されずに生き延び、感染を拡大する戦略の一つと考えることもできる。2003 年８月頃に流行した Blaster は急激に感染拡大したものの PC を使用不能にしたことからユーザが対策を取らざるを得ず、比較的早く収束したのに比較して、2004 年３月頃から発生のみられる NetSky 等破壊活動が穏やかなウイルスは、上記の理由故に収束までの時間が長くかかっているのではないかと考えられる。

NetSky は、メールに添付されて送付される錯誤誘発型のウイルスである。このウイルスは、最近のウイルスによくみられる PC 内ファイルからの送信先抽出、発信元アドレスの詐称、Outlook/OutlookExpress のプレビュー脆弱性利用による自動感染などの機能により急速に感染を拡大した。一方で、感染後に感染した PC に対するファイル破壊等の症状を伴わないことから、感染しても PC のユーザはそれに気がつかないことも多く、ウイルス駆除等が行われないままこのウイルスをばらまき続けるという状態になっている。また、NetSky の感染発生初期の段階では、ウイルス対策ツールがこのウイルスに対応するまでに時間がかかり、ゲートウェイ及び PC の双方でウイルスの検知が不能の状態が長く続いた。これが感染拡大を招いた一因となっていると考えられる。

2.2. Netsky の感染プロセス

Netsky の感染・発症・拡散のプロセスは、もう少し具体的には次のようである。

(1) 感染

Netsky(W32/Netsky.ab@MM を例にとると)は、メールとして送られてきて、ユーザの錯誤により添付ファイルを起動することにより感染する。なお、当該メールには特定の拡張子(PIF 等)のファイルが添付されている。

Netsky は、感染すると PC に Netsky 本体(CSRSS.EXE)をシステムディレクトリにインストールする。また、特定のレジストリキーを

追加することにより、Windows起動時にNetskyも自動起動されるようにする。

(2) 発症

感染すると直ちに発症し、感染したPCの特定の拡張子(htm,doc,cfg等)を持つファイルを調べ電子メールアドレスを収集する。

(3) 拡散

自身のSMTPエンジンを使用して電子メールメッセージを作成し、収集した電子メールアドレス宛にSMTPにより送信する。

当該電子メールメッセージにおいては、

・差出人のアドレスを偽装（収集した電子メールアドレスの中から選択）
・正当なメールと紛らわしい件名（Question等）をつける。
・いくつかのパターン("Are your numbers correct?"等)から本文を選択する。
・いくつかの特定の名称から選択した名前を付けられたファイル(corrected_doc.pif等)を添付する。

3. 対策内容

前述のとおり、マスメール型ウイルスに対しては個々のユーザの対策について万全を期待することができない状況であるので、ネットワーク環境の変更のみでウイルス対策の効果が得られる方法として、ゲートウェイにおける対策の向上を検討する。現状行われているゲートウェイ対策の多くは、メールの添付ファイルをスキャンしてウイルスを検知した場合に駆除等の措置を講ずるものであるが、パターンファイルが用意されていない新種や亜種のコンピュータ・ウイルスには効果を持たない。最近、パターンファイルが提供されるまで時間がかかるケースが見られ、その間にコンピュータ・ウイルスが感染拡大してしまうことが少なからず発生している。

ここでは、①LAN内において送信先ポート番号を一律に変更してウィルスのSMTPエンジンからの送信を制限する対策手法(送信先ポート変更方式)と②特定条件下(例:統計分析による判断等)でLAN・WAN間のメール送受信を制限する性質を持つゲートウェイによる対策（ゲートウェイ遮断方式）とを考える。

3.1. 送信先ポート変更方式

ＬＡＮ内において、次のような対策を実施する。

①ＰＣのメーラのＳＭＴＰポートを通常の２５番から別の番号（例えば１００２５番）に変更する。
②ＳＭＴＰサーバは、２５番ポート宛のメール送信要求を受け付けず、１００２５番宛のメール送信要求があった場合には送信先の１００２５番宛中継する。
③ゲートウェイでは、
・ＬＡＮ内からの２５番ポート宛パケットを受け付けない。１００２５番宛パケットは２５番宛に変更して送信する。
・ＬＡＮ外からの２５番ポート宛パケットは、１００２５番宛に変更してＬＡＮ内に送信する。
④ゲートウェイを介さないLAN外へのメール送信は許可しない。

この対策方法の特徴は、

①ＬＡＮ外からＬＡＮ内に送信されるウイルスメールには効果がない。
②ＬＡＮ内からＬＡＮ外へのウイルスメールはシャットダウンできる。
③ＬＡＮ内におけるウイルスメールの送受信も防止できる。
④ＬＡＮ外のＳＭＴＰサーバによるメール送信も行うことができる。

特に④については、最近、ISPや企業において採用されることの多くなった標準メールサーバ以外による２５番ポートの使用制限に比べて、ユーザに対する利便性が高いと言える。２５番ポートの使用制限を採用したISP等では、LAN外部のメールサーバにおいて認証の伴うSubmission Port(587番)を使用することができれば当該外部メールサーバによるメール送信が可能となるが、現状それが利用できるサーバはまだ少ないなどユーザの利便性の点では課題を有する。

なお、送信先ポート変更方式については、PCにおけるポート変更の自動化の仕組みとコンピュータ・ウイルスによる変更後のポート使用を防止する仕組みが課題となる。

3.2. ゲートウェイ通過制限方式

この対策方式では、ゲートウェイにおいて、次のような通過トラフィックに関する監視と制限を行うものである。

①ＬＡＮ外から内へ、及びＬＡＮ内から外へのＳＭＴＰ通信のトラフィック変動を監視する。
②トラフィック変動の分析結果から、一定条件（マスメール型ウイルス特有のトラフィック特性）に合致した場合には、ＳＭＴＰパケットの通信を制限する（遮断対象は特定アドレスからのパケットに制限するなどできるだけ限定する）。

この対策方法は、次のような特徴を有する。

①LAN外からLAN内へのウイルスメールの送信は特定条件下で一定限度制限できる。
②ＬＡＮ内からLAN外へのウイルスメールの送信も一定限度制限できる。
③LAN内からLAN内へのウイルスメールには効果がない。

ゲートウェイ通過制限方式、送信先ポート変更方式を補完する性格を有しており、それぞれの方式で効果を期待できないウイルスメールの送受信を相互に補って防止することが期待できる。

4. シミュレーションモデル

4.1. システムダイナミクス

システムダイナミクスは、現象を因果関係の結果としてとらえ分析するという考え方に基づく理論である。システムダイナミクスによるシミュレーションでは、レベル、レートといった要素を組み合わせたフローダイアグラムをベースとしてシミュレーションモデルを構築し、これにより因果関係を規定する。

例えば、図1のモデルでは、因果関係は、

$$Level_k = Level_j + dt(Rate_{jk})$$
$$Rate_{kl} = Level_k \times R$$
(R=定数)

のように表される。

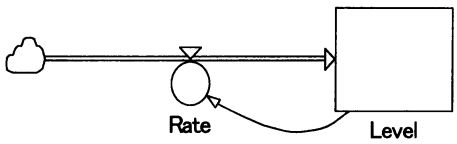

図1　シミュレーションモデルの例（流入モデル）

シミュレーションは、非線形・多元連立常微分方程式に初期値を与えて、数値解法によりその後の時間軸に沿った各要素の挙動を解くことによって行われる。

4.2. 感染拡散モデル

感染拡散の基本モデルとして、1つのLAN内におけるウィルス拡散を考え、「未対策PC」（ウイルス対策ソフトが未導入、パターンファイルがアップデートされていないなどウイルスに感染し得る状態のPC)、「感染PC」（ウイルスに感染しているPC）及び「対策済みPC」（感染PCからウイルスを駆除してウイルス対策ソフトを適正に導入するなどしてウイルスに感染し得ないPC）のそれぞれの台数間の因果関係について、システムダイナミクスの手法で規定したモデルを考える（図2)。このLANの中では、ウイルスメールはInternetから到達して未対策PCが受信するか、又はLAN内の感染PCからのウイルスメールを未対策PCが受信する。その上でユーザの錯誤により添付ファイルを開くことにより感染する（未対策PCの台数が1つ減り、感染PCの台数が1つ増える)。LAN内において、感染PCに対しウイルス駆除を行っている場合には、駆除をする毎に感染PCの台数が1つ減り、対策済みPCの台数が1つ増える。

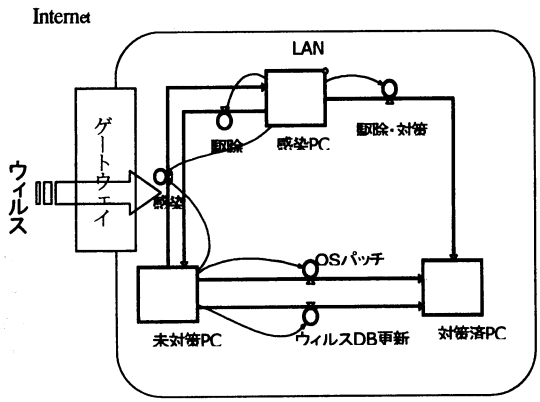

図2　感染拡散・制御の基本モデル

この基本モデルをベースとして、3．で説明した対策手法を備えた1つのLANと対策の施されていない3つのLANの間でマスメール型ウイルスが拡散するモデルを考えた（図3)。

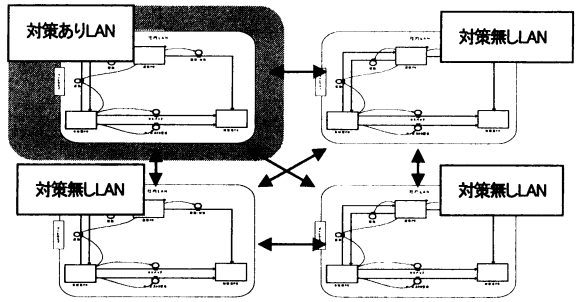

図3　LAN間におけるウイルス拡散モデル

このモデルにおいては、ウイルス感染拡散・制御に関する主な条件として次のような条件を設定した。

(1) 各LANにおけるPC台数はそれぞれ5,000台とし、初期状態としては1つの「対策無しLAN」に1台のみウイルス感染PCが存在するとした。
(2) ウイルスに感染したPCは、一定間隔（1分)で1通のウイルスメールを送信する。送信先は、50%が同一LAN内で他の50%はLAN外(他のLAN)とした。
(3) LAN外に発出されたウイルスメールの10%がモデル内の他のLAN向けであるとし、3つのLANに均等に（1／3ずつ）到達する。
(4) 到達したウイルスメールは、一定時間(1時間)後に100人に対し1人の割合いでファイルを開封（感染）するとした。
(5) 感染数は、未対策PC台数の全PC台数に対する割合いに比例することとした。

このような条件設定の下、シミュレーションを実施し、その結果を分析した。

5. シミュレーション結果の分析

5.1. ポート番号変更方式

ポート番号変更方式については、前述のとおり、その対策を施したLANとLAN外(WAN)とのウイルスメールの送信制限について、

A. LAN内からLAN外へのウイルスメール送信は完全にブロックされる。
B. LAN内からLAN内へのウイルスメール送信は完全にブロックされる。
C. LAN外からLAN内へのウイルスメール送信は制限されずに通過する。

という特性がある。このようなネットワークの特性がウイルス拡散にどのような影響を与えるかシミュレーション結果により確認する。

まず、ゲートウェイから侵入してくるウイルス数（ウイルスメールの数）の時間変化は図4で表される(時間軸=day)。

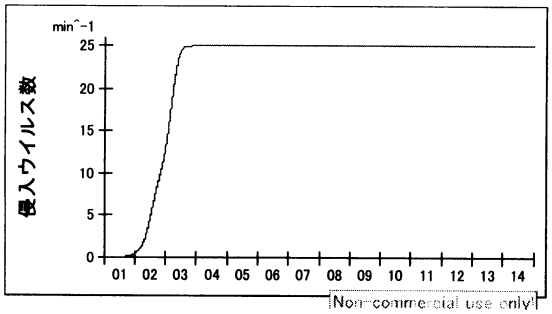

図4　LANに侵入（到達）するウイルスメールの時間変化

一切の対策を施していない状態、すなわち「対策あり LAN」において感染防止対策を採らない場合には、感染ＰＣ台数及び時間当たり感染台数は次のような経過をたどる（図５及び図６）。一般に、コンピュータ・ウイルスの感染拡大は、ロジスティック関数で表されると言われているが、このグラフはそれを裏付けている。

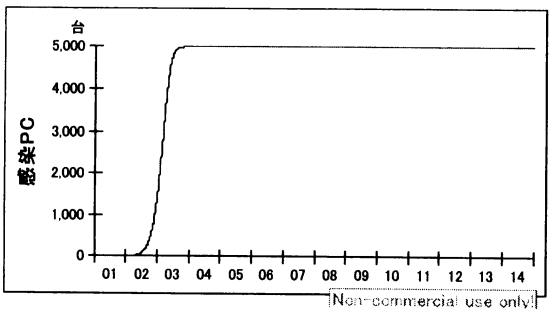

図5　対策無し状態における感染PC台数の変化

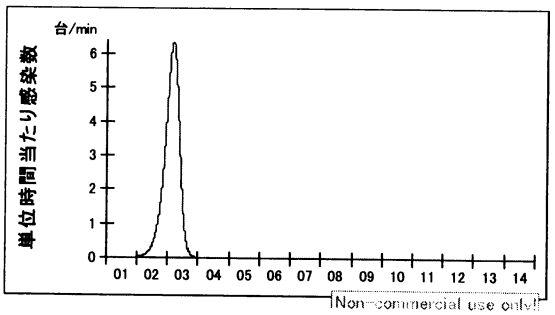

図6　対策無し状態における単位時間当たり感染数の変化

「対策あり LAN」において、ポート番号変更を対策として実施した場合には、感染ＰＣ台数及び単位時間当たり感染台数は図７及び図８のように変化する。

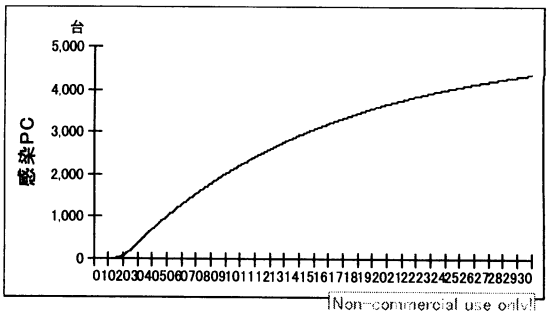

図7　ポート番号変更方式における感染PC台数の変化

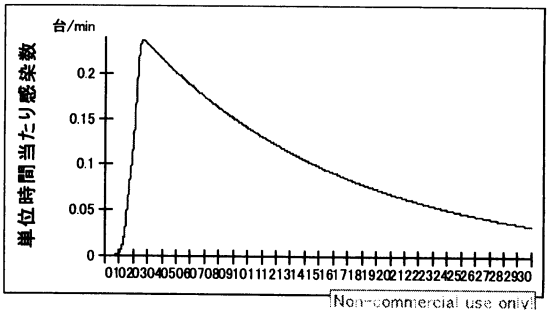

図8　ポート番号変更方式における単位時間当たり感染数の変化

図７のグラフからは、ポート番号変更方式により、ＬＡＮ外へのウイルスメール送信防止に加えて、LAN内PC相互の感染防止の性質により、対策を講じたＬＡＮ内におけるウイルスの蔓延防止にも効果があることが見てとれる。

図７では、ポート番号変更以外の対策を実施していないため、一度ウイルスに感染したＰＣは感染したままであり、感染ＰＣの台数は増えるのみである。図７の条件に加え、「対策あり LAN」内において、感染済みPCに対するウイルス駆除を一定条件で行った場合における感染ＰＣ台数の変化は、図９のようなグラフになる。

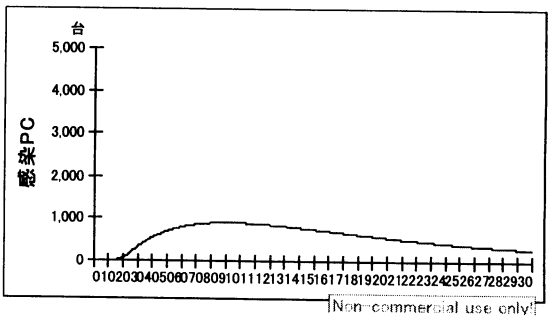

図9　ポート番号変更＋ウイルス駆除における感染ＰＣ台数の変化

なお、ポート番号変更を実施していない状態でウイルス駆除のみを実施した場合には、感染ＰＣ台数の変化は図10のようになる。ウ

イルス駆除のみの効果により感染拡大が制限されているとともに時間経過とともに感染の沈静化が図れていることが見て取れる。

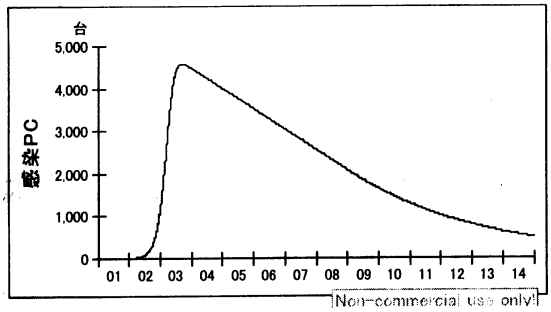

図10　ウイルス駆除のみの環境における感染ＰＣ台数の変化

図9と図10のグラフを比較すると、ウイルス駆除のみの環境(図10)より、ポート番号変更とウイルス駆除の両方を実施した図9では、両対策の相乗効果により、さらなる感染拡大防止と感染の沈静化がもたらされていることが分かる。

これらのシミュレーションの結果から、ポート番号変更による社内LAN内のウイルス蔓延防止の効果を確認することができた。

5.2. ゲートウェイ制御方式

ゲートウェイ制御方式においては、ゲートウェイを通過するウィルスの送受信を一定条件下で制限するものである。実環境において実効が期待できるのは、例えば、通過するメールトラフィック量の変化を常時監視し、送信元メールアドレス毎に統計分析をした結果により、マスメール型ウイルスからのメール送信パターンに合致する場合には係るメールの送信をゲートウェイにて遮断する方法である。しかし、本研究においては、簡単なモデルとして、

A. LAN外からLAN内へのメール送信は、LAN外から到達するウイルスメールの時間当たりの数が一定量を超えた場合に遮断する。ただし、完全に遮断できないという前提で、到達するウイルスメールのうち１％はLAN内に通過することとする。
B. LAN内からLAN外へのメール送信もA.と同様。
C. LAN内からLAN内へのメール送信には制限を設けない。

というネットワーク環境を考えることとした。

ゲートウェイからLANに侵入してくるウイルスメールの数及びゲートウェイから外に発信されるウイルスメールの数の時間変化は、図11及び図12のグラフで表される。

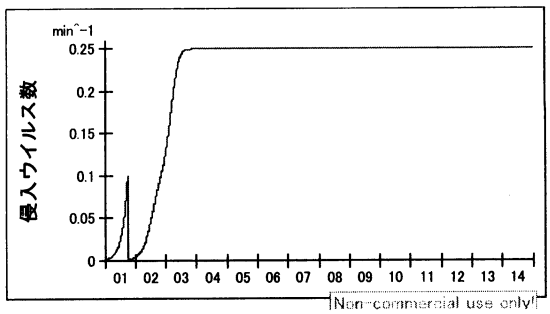

図11　ゲートウェイ制御方式におけるLANへの侵入ウイルスメール数の変化

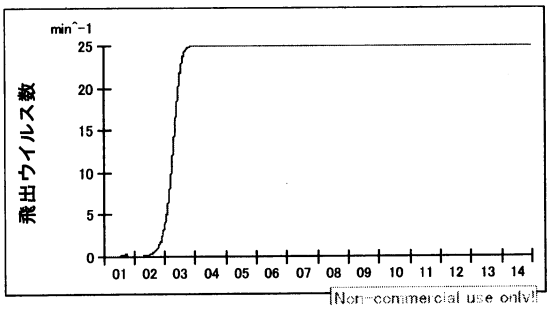

図12　ゲートウェイ制御方式におけるLANからLAN外へのウイルスメールの送信数の変化

このときＬＡＮ内における感染ＰＣ数及び単位時間当たり感染台数は、図13及び図14のグラフになる。

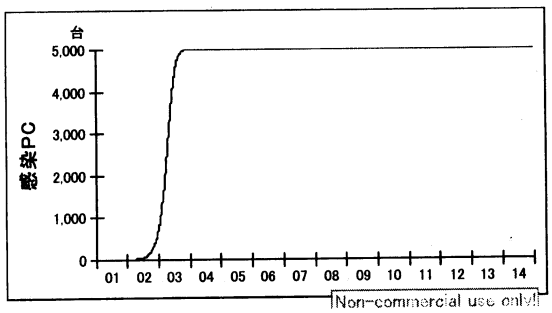

図13　ゲートウェイ制御方式における感染PC台数の変化

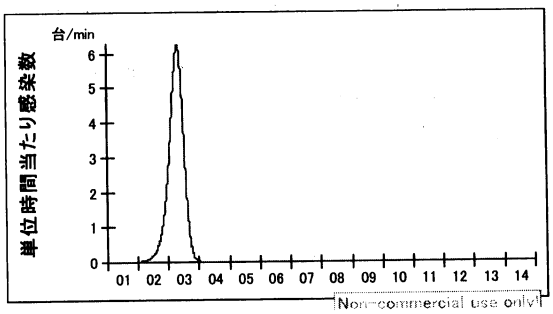

図14　ゲートウェイ制御方式における単位時間当たり感染数の変化

対策無し状態における感染 PC 台数及び単位時間当たり感染数の変化（図5及び図6）と比較すると、ゲートウェイ制御方式のみの対策では、それほどの効果が表れていないことが分かる。

これは、LAN 内における感染拡大と LAN 外から到来するウイルスによる感染とを比較した馬合に、LAN 内における感染拡大の影響が大きいネットワーク環境条件であったために LAN 内における感染拡散防止効果の無いゲートウェイ対策ではそれほどの対策効果が現れなかったと考えられる。

5.3. ポート番号変更方式＋ゲートウェイ制御方式

次にポート番号変更方式とゲートウェイ制御方式の両方を対策として実施た場合について、シミュレーションを実施した。その結果を図15及び図16に示す。

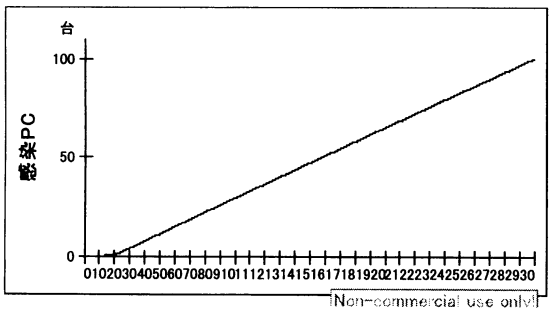

図 15　ポート番号変更方式＋ゲートウェイ制御方式における感染 PC 台数の変化

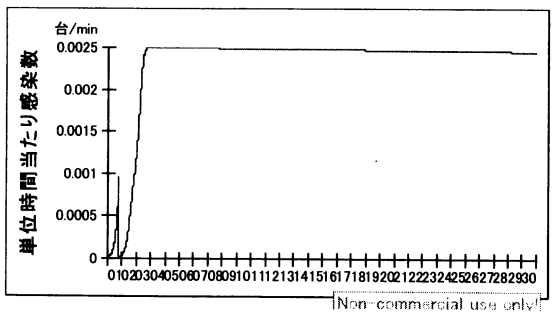

図 16　ポート番号変更方式＋ゲートウェイ制御方式における単位時間当たり感染数の変化

ポート番号変更方式の結果(図7及び図8)並びにゲートウェイ制御方式(図13及び図14)と比較すると、単独ではほとんど効果が現れなかったゲートウェイ制御方式は、ポート番号変更方式と組み合わせることによって、大きな効果が現れていることが分かる。これは、LAN 外から LAN 内へのウイルスメールに効果の無いポート番号変更方式と LAN 内から LAN 内へのウイルスメールに効果の無いゲートウェイ制御方式がそれぞれの弱点を補い合う形で全体として感染拡大防止に効果を発揮したものと考えられる。図17は、各対策方式を一つのグラフ上で比較したものである。

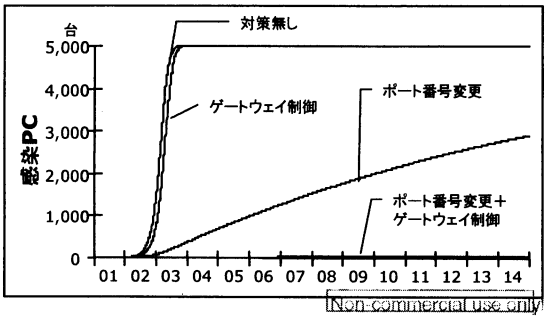

図17　感染PC台数の変化（各方式の比較）

6. おわりに

本研究においては、理論疫学の一つであるシミュレーションの手法を用いて、マスメール型ウィルスの感染拡散・制御モデルを構築し、特定の対策手法について感染拡大防止の効果を評価し得るものなのかを確認した。条件設定等において、まだ改善の余地はあるものの、本研究の結果は、未だ実装されていない対策手法や試験環境の構築が困難な大規模ネットワーク環境等について、仮想的な様々な条件下でウィルス感染拡大対策の効果を調べるための方法論として、このようなシミュレーション（疫学的手法）が有効であることを示唆するものであると言える。

文　献

[1] 中村好一「基礎から学ぶ楽しい疫学」、医学書院、2002 年

[2] 島田俊郎「システムダイナミクス入門」、日科技連、1994 年

[3] J.O. Kephart, S.R. White "Direct-graph Epidemiological Models of Computer Virus", Proceedings of IEEE Symposium on Security and Privacy, (IEEE, Oakland, May 20-22, 1991), 343-359

[4] Jeffrey O. Kephart et. al, "Computers and Epidemiology", IEEE SPECTRUM, May 1993

[5] 関聡司「コンピュータ・ウイルス対策における疫学的手法の適用可能性」、早稲田大学 COE 第3グループ・ワークショップ論文集、2003 年

[6] 関聡司、佐々木良一、岩村充「コンピュータ・ウイルス対策における疫学的アプローチに関する研究（その1）～ウイルス拡散・制御シミュレータの開発～」、情報処理学会 CSEC 研究会、2004 年5月

[7] 佐々木良一他「コンピュータウイルスに対する分析疫学的アプローチ」、電子情報通信学会、SITE 研究会、2004 年5月

[8] 佐藤大輔他「メール型コンピュータウイルス拡散モデル」情報処理学会研究報告、2004-CSEC-26、pp201-206、2004 年

[9] 高橋正和、佐々木良一「ワームの特性に基づく拡散モデルの提案と適用」、情報処理学会シンポジウム CSS2004、2004 年10月

[10] 佐々木良一他「コンピュータウイルスに対する疫学的アプローチの提案」、電子情報通信学会 SCIS2005、2005 年1月