

ワクチンを持たないノードを考慮したネットワーク上における コンピュータウイルスの拡散と消滅

千石 靖[†] 岡本 栄司^{††} 服部 進実[†]

近年、多くのパーソナルコンピュータがネットワークに接続するようになり、ウイルス対策はネットワークの安全管理上重要な位置を占めるようになってきている。ネットワーク環境においては、すべてのノードでウイルス対策を実施することが重要であるが、コストなどの問題で全域的対策ができない場合も存在する。そこで、本稿ではネットワークのワクチン保有率を考慮し、ウイルスやワクチンの働きを理論式とシミュレーションによって解析している。また、ワクチン保有率がウイルス対策に及ぼす影響を明らかにしている。本結果は、パーソナルコンピュータを利用したネットワークでの、効率的でより現実的なウイルス対策の指標を提示する。

Computer Virus Diffusion and Extinction Evaluation in Networks with Vaccine-free Nodes

YASUSHI SENGOKU,[†] EIJI OKAMOTO^{††} and SHIMMI HATTORI[†]

In this paper, we examine diffusion and extermination of computer viruses in a network constructed with personal computers. Since computer vaccines cannot always be installed in whole nodes in the network, we especially clarify by computer simulations 1) the influence of the hold vaccine rate on the diffusion and extermination processes of viruses, and 2) the relation of the hold vaccine rate and the extermination rate caused by the vaccine. Moreover, those influences are theoretically analyzed in a complete graph network and some expressions are obtained. These results give us a useful indication for a practical and effective anti-virus measure in a network connecting personal computers.

1. はじめに

社会の情報化や情報機器のダウンサイジングによって、パーソナルコンピュータ(PC)は著しく普及しつつある。しかし、PCはもともとスタンドアロンで使用することを前提に開発されてきたため、現在流通しているハードウェアやソフトウェアの多くはセキュリティ機能が十分であるとはいえない状態である。このようなPCを情報ネットワークに利用することにより、情報ネットワークのセキュリティ度の低下という問題が生じてきている。最近では特に、コンピュータウイルス(以下ウイルスと呼ぶ)が問題視されており、日本国内においても情報処理振興事業協会(IPA)へ

の被害届は急増している状況にある¹⁾。

ウイルスに関する研究は海外の様々な大学や企業等の研究機関で行われており、日本国内においても、いくつかの大学で研究論文が発表されたり、ソフトハウスがウイルス対策ソフトウェア(以下ワクチンと呼ぶ)を開発してきた。これらの研究は、ウイルスの解析に重点をおいたマイクロなものと、疫学になぞらえてウイルスの拡散をとらえたマクロなものに大別できる。

ミクロ的研究の成果としてはワクチンがある。現在では、国内でも数社からワクチンが販売されており、ウイルス対策がだれにでも簡単にできるようになっている。しかし、現在実施可能なウイルス対策のほとんどは、安全性を第一としているためか多くのCPUパワーを必要とし、本来の業務の効率低下を受け入れざるをえない状況となっている。

大学においても、新種の突然変異型ウイルスの解析²⁾やUNIXベースのネットワークにおけるウイルス(トロイの木馬)対策法³⁾等、それぞれ機械語コードの分析やネットワークセキュリティの専門家の立場で

[†] 金沢工業大学人間・情報・経営系

Division of Human, Information, and Managerial Engineering, Kanazawa Institute of Technology

^{††} 北陸先端科学技術大学院大学情報科学研究科

School of Information Science, Japan Advanced Institute of Science and Technology, Hokuriku

研究されてきている。

また、通産省とIPAを中心に、従来の検索タイプのワクチンよりも確実に感染を発見するインテグリティ・チェック法を利用したワクチンの研究・開発が進められている。インテグリティ・チェック法とは、各プログラムにデジタル署名を施しておくことにより、もしウイルスに感染すればユーザが容易に検知できるような方法である⁴⁾。これは、新規ウイルスを含むどんなウイルスにも有効であり、ウイルス数に依存しない時間でチェックできるものであるが、ウイルスの特定や駆除の機能は持っていない。

ウイルスがコンピュータ社会の中でどのように拡散していくか、疫学と対比させたマクロ的な研究も行われてきた。文献5)では、生物学のウイルスとコンピュータのウイルスを対応付け、数学的疫学の技法をコンピュータウイルスの伝播に適合させて研究している。これは、ウイルスを疫学的観点でとらえ、微分方程式でマクロ的に解析したものである。

これに対し、我々は、より現実に近い結果を得るために個々のウイルスの動作に注目し、ネットワークにおけるウイルスの拡散過程やワクチンによるウイルス駆除の効果を明らかにし⁶⁾、感染率 R_i のウイルスの拡散が駆除率 R_e のワクチンによって定常状態に至ったときの感染ノードの割合 x を求める理論式(式(1))や、感染率 R_i のウイルスを完全駆除するために最低限必要なワクチンの駆除率 R_e を求める理論式(式(2))を得た⁷⁾。

$$x = 1 - \frac{R_e}{R_i(1 - R_e)} \quad (1)$$

$$R_e = \frac{R_i}{1 + R_i} \quad (2)$$

ただしこれらは、ネットワーク内のすべてのノードがワクチンを保有していることを仮定したものであった。

しかし現実には、コスト的な問題でワクチンを持たないノードが存在したり、ワクチンを持っていても、業務やネットワーク運用の効率の問題でワクチンを動作させないノードがあったりするだろう。また、フロッピーディスク等のリムーバブルメディアにウイルスが侵入した場合はワクチンの手が届き難く、それらのメディアはワクチンを持たないノードと同じ影響を及ぼすといえる。ワクチンによって全域的なウイルス対策を実施しているネットワークであっても、時々ネットワーク内からウイルスが発見されることがあると聞く。これは、ネットワーク内にワクチンを使用していないノードがあるか、ワクチンが効果的に働いていないことの顕れである。さらにいえば、CD-ROMやCD-R

などのメディアに書き込まれたウイルスはどんなワクチンを用いても駆除できない。そのような書換え不可能な感染メディアを利用することがあるならば、そのコンピュータシステムのワクチンは存在しないに等しい。ウイルス対策の効果を上げるためにはすべてのノードでワクチンが利用されることが望ましいが、上述のとおり、現実のコンピュータネットワークは必ずしもそうなっているとはいえないのである。

本稿はこの問題を考慮し、ワクチンを持たないノードが存在するネットワークにおいて、そのネットワークのワクチン保有率とそこでのウイルス拡散およびワクチンによる駆除効果の関係を明らかにし、効率のかつより現実的なウイルス対策の指標を提示する。

2. モデル化

ネットワークにおけるウイルスの拡散を解析する際、ネットワーク、ノード、通信路、ウイルス、ワクチンの各要素を簡略化して使用する。

2.1 ウイルスのモデル化

本稿では、ウイルスの感染動作に重点を置き、ネットワークを通じて一定の感染率を持つウイルスを想定している。また、発病によるシステムダウンなどの影響は考えないこととする。

ウイルスの持つ感染率は、宿主であるノードが通信動作を行ったときに感染動作を行う確率とする。ウイルスの動作は通常、ノードのデータ送信動作に紛れて行われる。ただし、すべてのノードはつねに通信動作を行っているとする。

ウイルスの感染動作は、感染ノードのウイルス1つが通信路を介して他のノード1つにウイルスのコピーを作ろうとする動作とする。ここで、通信路とはウイルスから見たウイルス自身の感染経路であり、物理的な接続ではなく、通信頻度の高いノード間の関係を通信路と見なす。ウイルスにとっては、発見・駆除されることは最も避けなければならない、実際のウイルスを見ても、その感染動作は決して目立つものではない。1回の通信動作において感染動作が1回だけ行われ、対象ノードの1つにだけ感染するという動作は、実際のウイルスを解析して得た妥当な動作であると考え、定めたものである。

ここで、通信などの動作の基準となるターンという単位を導入する。1ターンは、ウイルスの感染動作すなわちウイルスフェイズと、ワクチンを使用してノード内のウイルスを駆除する駆除動作すなわちワクチンフェイズから成る。

本稿では、ウイルスの拡散を感染ノード数の推移で

見ているため、1つのノードは1つのウイルスにしか感染しないと、既感染ノードにさらに感染するような重複感染はしないものとする。つまり、相手ノードがすでに感染しているならばそのターンの感染動作は無効とする。

感染動作はすべてのノードで同期して行われる。

2.2 ワクチンのモデル化

ワクチンとは、ウイルスを発見し駆除するためのソフトウェアである。また、ここでは、オペレータによってウイルスが発見され、プログラムを再インストールすることによるウイルスの駆除など、ワクチンソフトウェアを使用しないウイルス対策手段もワクチンと呼ぶことにする。ワクチンは一定の駆除率を持っていると考える。ただし、駆除後に起こりうる再感染を防止する機能はないとする。

駆除率とは、本来、ワクチンを保有するノードがワクチンを使用したときに、ノード内のウイルスを駆除する割合として考えられる。しかし、今回の解析ではノード内のウイルスの有無しか考えていないため、ウイルスの駆除も完全に駆除するかまったく駆除しないかが問題となる。したがって、本稿での駆除率は、ウイルスを完全に駆除する万能ワクチンを何ターンに1回の割合で起動するかということを意味する。これは本来ワクチン起動率というべきであるが、感染率に対応させて駆除率と呼ぶことにする。

ワクチンの駆除動作は、ワクチンを保有し、かつウイルスに感染しているノードが通信動作を行った後に、駆除率に応じてワクチンが動作することによって行われる。動作したワクチンはそのノード内のウイルスを完全に駆除するが、その効果はそのターンでのみ有効であり、あとで起こるであろう再感染を防ぐものではない。

駆除動作はすべてのノードで同期して行われる。

2.3 ネットワークのモデル化

ネットワークは1024個のノードで構成されている。ノードはパーソナルコンピュータであり、ネットワーク機能を持ったOSを搭載している。ノードはすべて、直接他のノードすべてと通信路によって接続している。現実のネットワークの形態は様々であるが、本稿では、ウイルスが最も拡散しやすい形態である完全グラフ型ネットワークとする。

各ノードは通信路を通じて他のノードとデータを交換している。ノード間を結ぶ通信路は、通常は物理的に結線された通信回線を指すが、ウイルスのモデル化で触れたように、本稿では通信頻度の高いノード間の関係を、たとえそれがフロッピーディスクの交換で

あっても通信路と見なすことにする。以後、このような意味で通信路と呼び、同様にフロッピーディスクでのデータの受渡しを含めた意味で送受信という言葉を使用する。

ワクチンを保有しているノードの割合はワクチン保有率によって決定される。各ノードは常時稼働しており、通信路によってデータを送受信しているが、ワクチンを保有しているノードが感染しているならば、そのノードは駆除率に応じてワクチンを動作させ、ノード内のウイルスを駆除する。

各ノードの動作は通信動作とウイルス駆除動作であり、送信も駆除も1ターンに1回までとする。ただし、接続している他ノードの送信動作によってデータを受信する回数には制限を設けない。

3. シミュレーションによる解析

前章のモデルを利用して、まず、ウイルスが増殖し拡散していく過程とワクチンの投入による感染ノード数の変化の様子を調べる。

ある感染率を持ったウイルスがネットワーク内に侵入すると、あるタイミングによって感染動作が実行され感染ノードの数は増加していく。そして、各ノードがある駆除率を持ったワクチンを使用することによって感染ノード数は減少する。

シミュレーションでは、このようなウイルスの感染とワクチンによる駆除を交互に繰り返しながら、感染ノード数がどのように増減していくかという時系列データをとる。ここで、乱数を用いたシミュレーションで1度試行しただけでは結果の信頼性が低いため、感染率、駆除率、保有率の1組に対して100回程度試行し、得られた感染ノード数の推移を平均してグラフ化する。

拡散シミュレーションは、ランダムに決定した1つのノードにウイルスが侵入したところから開始しており、ウイルスの駆除は行わない。また、拡散・駆除シミュレーションは、ウイルスがネットワーク内に完全に拡散した状態から駆除および拡散を実行している。

感染率と駆除率の値によっては、感染ノード数がある値を中心に大きく増減しない定常状態となることが予想される。感染率が小さいもしくは駆除率が大きいとウイルスの絶滅という状態で定常状態に達するが、そうでない場合はどの程度の定常量になるのかも結果として得られる。

シミュレーション手順

具体的なシミュレーション手順を以下に示す。これを指定した回数もしくは条件を満たすまで繰り返し実

行することで、感染率、駆除率、保有率の3点でウイルスの拡散の違いを見る。

(1) 次のウイルス感染手続きをすべてのノードについて行う。

ウイルスが存在するノードは、生成した乱数が感染率未満であれば、接続相手のノードのうち、生成した乱数で決定した1つにウイルスを感染させる。ただし感染した結果はすぐには反映されず、このターンで新しく感染したノードは次のターンにならないと感染動作を起こせないとする。

(2) すべてのノードの感染状態を更新する。

(3) 次の駆除手続きをすべてのノードについて行う。ウイルスが存在するノードは、生成した乱数がワクチンの駆除率未満ならばウイルスを駆除し、感染状態を更新する。

(4) 感染ノードの数をファイルに出力する。

3.1 ウイルス拡散・駆除過程

まず、ウイルスの拡散と駆除の過程がワクチン保有率によってどう変わるかを見た(図1)。これは感染率50%のときのウイルスの拡散過程と、駆除率20%のワクチンを使用したときの拡散・駆除過程をプロットしたものである。横軸はターン数であり、縦軸はそのときの感染ノード数を表している。

ウイルスの拡散過程ではワクチンを効かせていないため、ウイルスの純粋な増殖状況が表れている。感染ノード数は最初のうちは高次関数的に増加しているが、ネットワークを構成するノードの数が有限であるため、次第に飽和して頭打ちとなっている。

すべてのノードが感染している状態からワクチンを効かせた拡散・駆除過程では、感染ノード数はすぐに感染率と駆除率およびワクチン保有率によって決まる定常量に落ち着く。ワクチン保有率は小さいほどウイルスの拡散を助け、定常量を多くする。保有率が大きければ定常量は小さくできるが、駆除率がしきい値⁷⁾を下回ってれば保有率が100%であってもウイルスを完全に駆除することはできない。この保有率と定常値との関係を次に示す。

3.2 保有率による定常値の差

ワクチン保有率の変化が定常状態の感染ノード数に与える影響を図2に示す。これはウイルスの感染率が50%の場合において、ある駆除率のワクチンを使用したときに達する定常状態の感染ノード数をプロットしたものである。横軸は駆除率であり、縦軸は感染ノード数を表している。

この図より、たとえばワクチン保有率70%における

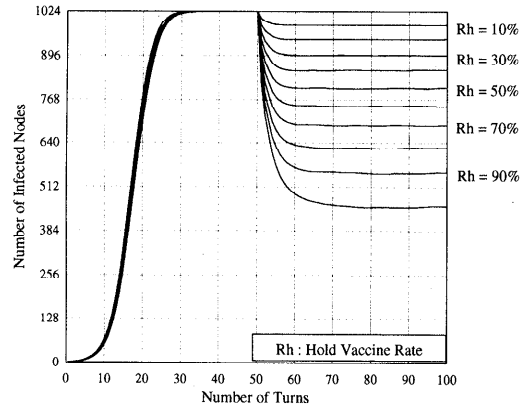


図1 ウイルス拡散・駆除過程(感染率50%, 駆除率20%)
Fig. 1 Diffusion and extermination processes (Infection rate = 50%, Extermination rate = 20%).

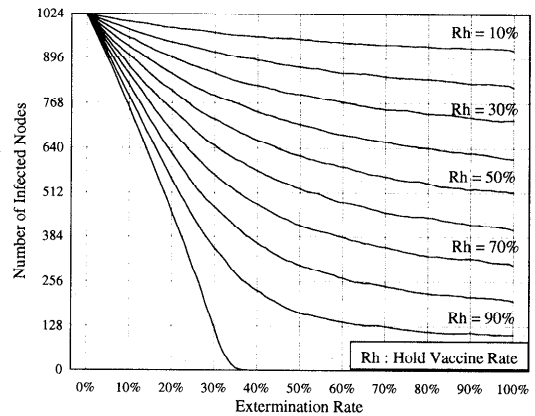


図2 定常状態の感染ノード数(感染率50%)
Fig. 2 Number of infected nodes in stationary state (Infection rate = 50%).

駆除率20%の駆除効果(感染ノード数約690)は、ワクチン保有率100%における駆除率12%程度の駆除効果と同等であることが分かる。これは、ワクチン保有率が100%から30%落ちると、その埋め合わせには駆除率が1.7倍必要になることを示している。この保有率と駆除率の関係に次に示す。

3.3 駆除率と保有率の関係

図3は、定常値を一定に保つための駆除率と保有率の関係を表している。これは、ウイルスの感染率が50%の場合に、定常値がある値(128, 256, ..., 896)となる駆除率と保有率の組をプロットしたものである。横軸はワクチン保有率であり、縦軸はワクチンのウイルス駆除率である。

この図から、保有率を下げたときに、ある定常値を

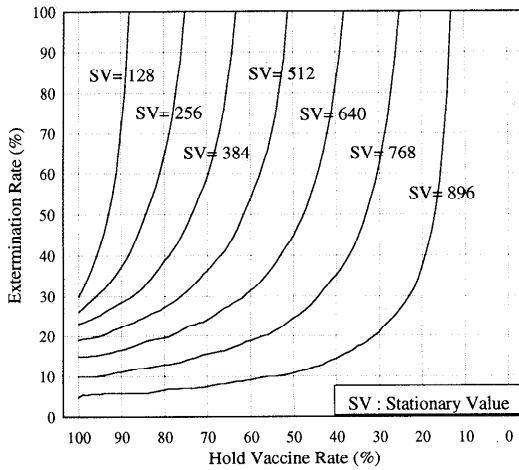


図3 駆除率と保有率の関係 (感染率 50%)

Fig. 3 Relation between extermination rate and hold vaccine rate (Infection rate = 50%).

維持するために駆除率をどれだけ上げなければならないかを読み取ることができる。たとえば、コスト的な問題があってワクチンは90%のノードにしか持たせられない(保有率=90%)が、定常的な感染ノード数は12.5% (定常値=128) 以下に抑えたい、という要求がある場合、駆除率が70%あればこの条件を満たすことができる。逆に、ネットワークの性能を上げるためにワクチンの実行をできるだけ減らしたいが、定常値は128以下に抑えたい、という場合は、ワクチン保有率を100%にすることで駆除率を30%にまで減らせることが分かる。

4. 理論的解析

次に、ウイルスやワクチンの個々の動作に注目し、ウイルスの拡散や定常値などを理論的に解析する。

4.1 拡散・駆除過程

$N (\geq 2)$ 個のノードが完全グラフ状に接続しているネットワークがあり、ターン t において感染率 R_i を持つウイルスに $I_t (\geq 1)$ 個のノードが感染しているとす。ただし、 N 個のうちワクチン保有率 R_h に相当するノードがウイルス駆除率 R_e のワクチンを持っているとする。したがって、 I_t 個のうちワクチンを持っていない感染ノードの数 U_t の期待値は $I_t(1 - R_h)$ 個となる。

まず、 I_t 個の感染ノードのウイルスのうち、 $I_t R_i$ 個が感染動作を起こす。ウイルスの感染動作はこれらのノードでいっせに行われ、このときウイルスは各個別に通信路数 $L = N - 1$ 個の接続相手ノードから1つを感染対象として選択する。

この選択は各ウイルスが独立に行うため、感染対象として選択されるノードに重複が生じることがある。このとき、重複感染はしないとの仮定のため、重複数-1の感染動作が無効となる。このような感染対象ノードの重複とそれによって無効となる感染動作数を差し引いた、ネットワーク内の感染動作全体の中の有効感染動作数は、通信路数 L と感染動作数 $I_t R_i$ を引数とする関数 $valid(L, I_t R_i)$ によって求められる。

しかし、これらが感染対象として選択したノードのうち、自分を除く $(I_t - 1)/L$ の割合のノードはすでに感染している。したがって、ターン t において増加する感染ノード数 ΔI_t は

$$\Delta I_t = valid(L, I_t R_i) \left(1 - \frac{I_t - 1}{L}\right) \quad (3)$$

となる。

なお、関数 $valid(L, I_t R_i)$ は、 L 個から重複を許して $I_t R_i$ 個とったときに、その $I_t R_i$ 個には異なるものが平均して何個現れるかを表すものである。文献8)によると、 L 個の集団から重複を許して抽出を行ったとき、 r 個の異なるものを得るための抽出ステップ数 S_r の平均値 $E(S_r)$ は、近似的に

$$E(S_r) \approx L \log \frac{L + 1/2}{L - r + 1/2} \quad (4)$$

で与えられる。この式を $E(S_r) = I_t R_i$ として r について解くと、求める次の式が導き出せる。

$$valid(L, I_t R_i) = \left(L + \frac{1}{2}\right) \left(1 - e^{-\frac{I_t R_i}{L}}\right). \quad (5)$$

次に、ワクチンを持つノードにおいてワクチンが動作したとき、感染ノード数はワクチンを持つもののみだけ駆除率 R_e に応じて減少する。ここで、ワクチンを持たない感染ノードの数 U_{t+1} は平均的にターン t での感染ノードの $1 - R_h$ の割合となり、これは減ることはないため、

$$U_{t+1} = \max((I_t + \Delta I_t)(1 - R_h), U_t) \quad (6)$$

となる。こうして、ワクチンのウイルス駆除動作後の感染ノード数、すなわちターン $t+1$ での感染ノード数 I_{t+1} は式 (7) により求められる。

$$I_{t+1} = (I_t + \Delta I_t - U_{t+1})(1 - R_e) + U_{t+1}. \quad (7)$$

この式 (7) を用いてターンごとに計算を行った結果と、計算機シミュレーションを50回行った結果の平均値をプロットしたものを図4に示す。横軸がターン数であり、縦軸はそのときの感染ノードの数を表している。これは感染率50%、駆除率20%、感染ノード数1という条件で計算およびシミュレーションを開始したものである。ただし、ウイルスの純粋な拡散の様

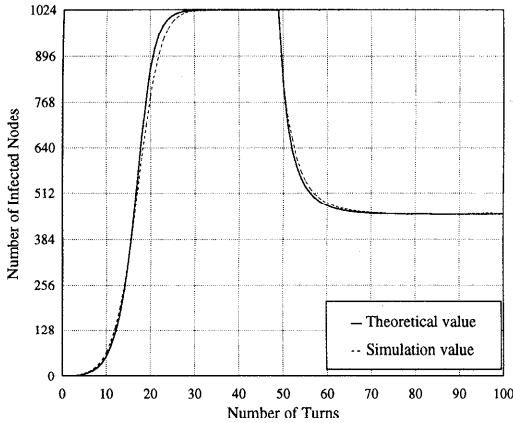


図4 拡散・駆除過程の理論値と実験値の差 (感染率 50%, 駆除率 20%)

Fig.4 Comparison of theoretical value and simulation value on diffusion and extermination process (Infection rate = 50%, Extermination rate = 20%).

子と定常状態の様子を別々に見るため、ワクチンの効果はウイルスがネットワーク全体に完全拡散した後の50ターン目から有効とした。解析式による理論値とシミュレーションによる実験値との間には、1ターン程度のわずかな誤差しかなかった。

式 (3), (5), (7) から、ウイルスの拡散は感染率と感染ノード数の積に対して指数関数的に働き、ワクチンによるウイルス駆除は線形に効くことが分かる。

完全グラフ型ネットワークはウイルスにとって最も拡散しやすい形態であると先に述べた。したがって、この漸化式を用いて計算した結果は、ある感染率、駆除率、保有率の組に対するウイルス拡散の限界を表すことになる。

4.2 定常状態

ワクチンの駆除率がしきい値より低いか、ワクチン保有率が100%でない場合、ウイルスは完全には駆除されず、感染ノード数はある定常値に落ちつく。この値は式 (7) を用いて理論的に解析できる。

定常状態のウイルス拡散率 $\lim_{t \rightarrow \infty} I_t/L$ を x とおき、 L が十分大きいと仮定して近似的に式 (7) を変形すると、 $\lim_{t \rightarrow \infty} U_t = N(1 - R_h)$ 、 $N \approx L$ であるから、

$$I_{t+1} = (I_t + LA - N(1 - R_h))(1 - R_e) + N(1 - R_h) \quad (8)$$

$$\frac{I_{t+1}}{L} = \left(\frac{I_t}{L} + A\right)(1 - R_e) + R_e(1 - R_h) \quad (9)$$

$$x = (1 - R_e)\left(x + (1 - e^{-R_i x})(1 - x)\right) + R_e(1 - R_h) \quad (10)$$

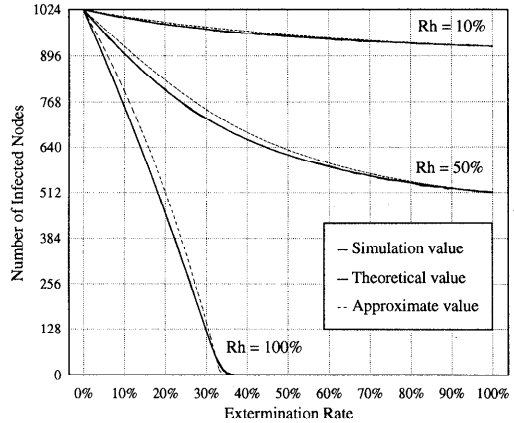


図5 定常状態の理論値と実験値の差 (感染率 50%)

Fig.5 Comparison of theoretical value and simulation value on stationary state (Infection rate = 50%).

ただし

$$A = \left(1 - e^{-\frac{I_t}{L} R_i}\right) \left(1 - \frac{I_t}{L}\right)$$

となる。ここで、 $e^{-R_i x}$ を級数展開して一次近似的に x を求めると、

$$x = \frac{B + \sqrt{B^2 + 4R_i R_e(1 - R_e)(1 - R_h)}}{2R_i(1 - R_e)} \quad (11)$$

ただし $B = (1 - R_e)(1 + R_i) - 1$ を得る。これが定常状態におけるウイルスの拡散率を表し、これを N 倍したものが定常値となる。

この式で計算した結果をシミュレーションによる実験値とともに図5に示す。実験値と式(7)による理論値はきれいに一致したが、式(11)による近似値には指数関数の一次近似による誤差が若干現れている。ただし、これは駆除率が50%以上ある場合は問題ない程度であった。

4.3 ある拡散率を保つために必要な駆除率

式(7)からは、ある感染率および保有率のときにある拡散率を保つために必要な駆除率を求める次の式を導くこともできる。

$$R_e = 1 - \frac{C}{C + (1 - e^{-R_i x})(1 - x)} \quad (12)$$

ただし

$$C = x + R_h - 1.$$

これより、感染率と拡散率を固定すると駆除率は保有率と双曲線の関係になることが分かるが、これは図3と一致する。

4.4 完全駆除に必要な駆除率 (しきい値)

保有率 $R_h = 100\%$ であれば、式(12)は

$$R_e = 1 - \frac{x}{x + (1 - e^{-R_i x})(1 - x)} \quad (13)$$

となり、しきい値では拡散率 $x = 0$ となるから、近似的に

$$R_e = \frac{R_i}{1 + R_i} \quad (14)$$

が得られる。これは、ウイルスを完全に駆除することが可能なしきい値を示す感染率と駆除率との関係であるが、文献7)におけるしきい値の解析結果(式(2))と等しいことが確認できる。

以上のように、ワクチンを持っていないノードがある場合のウイルスの拡散・駆除過程は式(7)によって、定常値は式(11)によって、ある定常値を保つために必要な駆除率は式(12)によって理論的に計算することが可能となった。

5. まとめ

ワクチン保有率を考慮してウイルス拡散および定常状態のシミュレーションと理論的解析を行い、ネットワーク内にワクチンを保有していないノードがある場合のウイルスの拡散や駆除の様子を明らかにし、その効果を計算する理論式を得た。

パーソナルコンピュータを用いたネットワークのウイルス対策においては、ネットワークのすべてのノードが何らかのウイルス対抗手段を持ち、それを適宜実行することが重要である。しかしながら、現実にはすべてのノードがウイルス対策を実行できるとは限らない。本研究の成果は、このような状況のもとでのウイルス対抗手段の実行頻度を適切なものに設定するための、より実用的で効果的な指標を与えるものであり、これによりウイルス対策のコストを削減することが可能となるだろう。

今回は既知ウイルスとそれに対応したワクチンをもとにウイルス対策を考察したが、今後は、未知ウイルスの対策手法の効率化や、ウイルスによるシステムダウンの影響を考慮した解析を行いたい。また、インターネットに接続しているLANにはウイルス対策を実施している所とそうでない所があるだろう。このような世界規模のネットワークでのウイルス対策に対応するよう、本研究の応用を検討していきたいと思う。

謝辞 本研究に対し、ご助言をいただいた東京工業大学の植松友彦助教授に深謝いたします。また、ご討論いただいた北陸先端科学技術大学院大学の岡本研究室各位および金沢工業大学の服部研究室各位に感謝いたします。

参考文献

- 1) ウイルスの届出状況について(プレス), 情報処理振興事業協会,
<http://www.ipa.go.jp/SECURITY/txt/>.
- 2) Yetiser, T.: *Polymorphic Viruses: Implementation, Detection, and Protection*, VDS Advanced Research Group (Jan. 1993).
- 3) 齊藤忠夫, 相田 仁, 川口洋二: ソースコード分析によるトロイの木馬の防御法, 電子情報通信学会論文誌 A, Vol. J76-A, No.3, pp.466-472 (Mar. 1993).
- 4) 岡本栄司, 山田忠直, 湯藤典夫: 我が国におけるコンピュータウイルスの現状と対策, 情報処理, Vol.33, No.7, pp.811-819 (1992).
- 5) Kephart, J.O., White, S.R. and Chess, D.M.: *Computers and Epidemiology*, *IEEE SPECTRUM*, Vol.30, No.5, pp.20-26 (1993).
- 6) 千石 靖, 満保雅浩, 岡本栄司: コンピュータウイルス拡散の理論とシミュレーション, 1994年暗号と情報セキュリティシンポジウム講演論文集, SCIS94-5A (1994).
- 7) 千石 靖, 岡本栄司, 満保雅浩, 植松友彦: コンピュータウイルスの拡散と消滅の大域的振舞いについて, 情報処理学会論文誌, Vol.37, No.4, pp.579-587 (1996).
- 8) Feller, W.: *An Introduction to Probability Theory and Its Applications*, p.225, John Wiley & Sons, Inc. (1968).

(平成 9 年 10 月 31 日受付)

(平成 10 年 1 月 16 日採録)



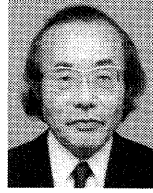
千石 靖 (正会員)

1967年生. 1992年金沢経済大学経済学部商学科卒業. 1994年北陸先端科学技術大学院大学情報科学研究科情報システム学専攻博士前期課程修了. 1997年同大学情報科学研究科情報システム学専攻博士後期課程修了. 博士(情報科学). 同年より金沢工業大学人間・情報・経営系助手. 同年より本学会北陸支部会計. ネットワークセキュリティの研究に従事. 電子情報通信学会会員.



岡本 栄司（正会員）

1950年生。1973年東京工業大学工学部電子工学科卒業。1978年東京工業大学理工学研究科電子工学専攻博士課程修了。工学博士。同年日本電気（株）中央研究所入社。1991年より北陸先端科学技術大学院大学情報科学研究科教授。1997年より同大学評議員。1993～1994年文部省在外研究にてテキサス A&M 大学数学科客員教授。グラフ理論、通信理論、数理計画、アルゴリズム、情報セキュリティをはじめとする情報数理工学の教育・研究に従事。1990年電子通信学会論文賞、1993年情報処理学会ベストオーサ賞受賞。著書「暗号理論入門」（共立出版）、「電子マネー」（岩波書店）など。IEEE シニア会員。電子情報通信学会、情報理論とその応用学会、応用数理学会、日本セキュリティ・マネージメント学会、システム監査学会、IACR（International Association for Cryptologic Research）会員。



服部 進実（正会員）

1964年東北大学工学部電子工学科卒業。同年より富士通にて情報通信システムの研究開発部門に所属。1989年金沢工業大学情報工学科教授。1995年同大学人間・情報・経営系長。1992年電子情報通信学会通信グループ副委員長。1993年同北陸支部長。1997年本学会北陸支部長。工学博士。情報通信システム、分散処理システムの研究に従事。電子情報通信学会、人工知能学会、IEEE 各会員。