追跡能力を有するワクチンを用いたウイルス駆除手法

中谷直司† 厚井裕司† 鈴木正幸†

近年のコンピュータウイルスの増加により，ネットワークを安全に管理するうえでウイルス対策は重要な位置を占めつつある．しかし，従来のウイルス対策は個々のユーザによる対処に依存しており，ネットワークの管理者による管理が難しい状況となっている．そこで本論文では，ウイルスを駆除するワクチンにウイルスと同様の感染能力を持たせることで，管理者がウイルス検出を行うコンピュータをいくつか用意しウイルスの検出とワクチンによる駆除を行えば，ウイルス対策を管理者レベルで一元管理することが可能となる新しいウイルス駆除手法を提案し，シミュレーションによりその有効性を示す．

Virus Extermination Method Using Vaccine with Chase Ability

Naoshi Nakaya,† Yuuji Koui† and Masayuki Suzuki†

By the recent increase of computer viruses, anti-virus measures for the safety control of network occupy the important position. However, general anti-virus measures depend on the countermeasure by individual user, so it is difficult for the manager of network to manage. Then, in this paper, we propose the novel virus extermination method that anti-virus measures are controlled by the manager level becomes possible, and the computer simulation shows the effectiveness of the proposed method. In this method, the vaccine can exterminate the virus, and chase the virus because it has the infection ability equal to the virus. Therefore, it is possible to exterminate all viruses, if the manager prepares some computers that check and exterminate the virus.

1. まえがき

近年のインターネットをはじめとするネットワークの急速な発展にともない，クラッキングやコンピュータウイルスなどのコンピュータの不正利用による被害は年々深刻なものとなってきている．特にその中でもコンピュータウイルスによる被害は，時間経過にともない不特定多数に対し加速度的に被害を与える点や，本来は被害者であるユーザが気付かないうちに加害者となる点などで他の不正利用とは大きく異なっており，予想外の事態を招き社会に深刻なダメージを与える可能性も考えられる．したがって，これらのウイルスに対し何らかの対策を行うことはきわめて重要であり，そのための研究も以前から行われてきている．

ウイルスに関する研究は大きく分けて2つに分けられる．1つはウイルス全体の振舞いを解析するマクロレベルの研究であり，生体における伝染病の伝播モデルをベースに解析したものや[1),2)]，独自のモデルを用いたもの[3)~5)]などがある．もう1つはウイルスの発見と駆除を目的としたミクロレベルの研究である．ミクロレベルの研究としては免疫機能からヒントを得たディジタル免疫システム[6)]や，クローン選択説からヒントを得た自己・非自己認識システム[7)]，生体の防衛システムに学んだ生物指向型ウイルス発見・修復システム[8)]，データマイニングの手法を用いたメールフィルタリングシステム[9),10)]などがある．本論文で提案するウイルス駆除手法は，この両者の中間に位置するものであり，ミクロレベルの研究成果である従来のワクチンに新たな機能を付加することで，ネットワーク全体からウイルスを駆除することを目的としている．

現在のウイルス対策においては，ウイルスの検出は各ユーザが導入したウイルス対策ソフト（アンチウイルス）を利用して行うことが原則となっている．そしてウイルスに感染していた場合には，ワクチンでウイルスを駆除するとともに，ユーザの責任に基づき関係者に通知している．このような状況ではユーザのアンチウイルスが最新のウイルスに対応している保証はなく，またユーザがアンチウイルスを導入していない場合には，自分のコンピュータがウイルスに感染しているこ

† 岩手大学工学部
Faculty of Engineering, Iwate University

とに気付かないことも十分にありうる．しかし，ネットワークを利用して感染・増殖するウイルスが主流となっている現状においては，ウイルスの影響は感染したコンピュータだけにとどまるものではない．すなわち，ネットワーク上でウイルスが増殖することによってネットワークトラフィックの増大を招き，各種サーバが処理限界を超えることでダウンするなどのネットワーク全体にかかわる問題を生じている．したがってネットワーク管理者としては，安全にネットワークを管理・運営するためにはネットワーク内のコンピュータからウイルスをすべて駆除する必要がある．しかしすでに述べたように現状ではウイルス対策は各ユーザ単位で行われており，ネットワーク管理者としてはユーザ教育などにより各コンピュータにアンチウイルスを導入させ，日々増え続ける最新のウイルスへの対応やウイルスの検出と駆除を徹底させるしか有効な手段は存在しない．そこで本論文では，ユーザをはじめとする人手の介入をできるだけ避け，管理者による一元管理が可能な新しいウイルス駆除手法を提案する．

提案する手法は，ウイルスを駆除するワクチンにウイルスと同様の感染能力を持たせることで，ウイルスを駆除すると同時に，ウイルスが感染したであろう他のコンピュータにワクチンを送り込む機能を中心に構成されている．すなわち，あるコンピュータでウイルスが検出されワクチンが実行されれば，ウイルスの感染先にアンチウイルスが導入されていない場合でも，感染先に自動的にワクチンが送られてきてウイルスは駆除可能となる．さらに，感染先でもウイルスが他のコンピュータに感染していた場合は，それに対してワクチンを送り込み以後これを繰り返す．この機能によりウイルスの検出がネットワーク上のすべてのコンピュータで行われなかったとしても，感染したすべてのコンピュータからウイルスを駆除可能となる．したがって，管理者がウイルス検出を行うコンピュータを少数用意しウイルスの検出とワクチンによる駆除を行えば，ウイルス対策を管理者レベルで一元管理することが可能となる．

以下，2 章では本提案手法がより有効に機能し，また現状のウイルスの大部分を占めるメール感染型ウイルス[11] の特徴を，3 章ではウイルス駆除の現状と課題について述べ，4 章ではこれらの課題を解決するためのウイルス駆除手法を提案する．5 章において提案手法と従来手法のウイルス感染と駆除のモデル化を行い，6 章では計算機を用いたシミュレーションの各種条件を示すとともに，シミュレーション結果に基づき提案手法の有効性を示す．7 章はむすびである．

2. メール感染型ウイルス

経済産業省の定義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，自己伝染機能，潜伏機能，発病機能のうち 1 つ以上を有するもの，とされている．初期のコンピュータウイルスは，これら 3 つの機能をすべて有し，感染，潜伏，発病というサイクルを繰り返すものが主であった．しかし，最近では潜伏期間を持たずにすぐに活動するウイルスや，発病することなく感染を繰り返すウイルスなどが出現している．そこで，現在では狭義のウイルスの定義では含まれなかったワームやトロイの木馬といったものも含めた，不利益をもたらす不正プログラム全体を広義のウイルスと呼んでいる．本論文で扱うコンピュータウイルスは，この広義のウイルスとする．

コンピュータウイルスは感染経路や感染対象，プログラミング言語などによりいくつかの分類が存在する．そういった分類の中で，近年急速に増加し続けているウイルスとしてメール感染型ウイルスがある．文献 11) によるとメール感染型ウイルスは，感染が報告されたウイルス全体のおよそ 85%を占めるまでになっており，その割合は増加し続けている．メール感染型ウイルスは，次のような特徴を持つと考えられる．

(1) 一度に多くのコンピュータに感染する．
この種のウイルスの多くは，ユーザがメールシステムに登録したメールアドレスなどを利用して，一度に数十件のウイルス付きメールを送信する．基本的に送信されたウイルスは，受信先で実行されない限りコンピュータに感染することはない．しかし一度に大量のウイルスが送信されるため，メールの受信先すべてで感染しなくても，ウイルスは急速に増殖する．

(2) 物理的接続形態には依存しない．
従来のディスクなどのメディアを媒体とした増殖では，物理的にメディアを受け渡す必要があった．また，メール以外のネットワーク接続によって増殖する場合には，アクセス制限などの点から同一の LAN 上などに増殖が制限される．しかしメールを利用する限りでは，そういった物理的接続形態は基本的に関係がなく，メールの送受信さえできれば増殖しうる．

(3) 増殖範囲はある程度限定される．
この種のウイルスの多くは，ユーザがメールシステムに登録したメールアドレスなどを利用して，ウイ

ルス付きメールを送信する．このことにより，ウイルスは物理的接続形態による制限ではなく，むしろユーザの社会的人間関係により増殖先が制限される．多くのユーザがシステムに登録し利用するメールアドレスは，そのユーザにとって親密な人間やある程度頻繁に連絡する者に限られると予想される．したがって，それらのメールアドレスは少数の例外を除いて，同一組織内などのある程度の大きさで閉じていると仮定される．

本論文で提案するウイルス駆除手法は，あらゆる感染経路，感染対象，プログラミング言語などのウイルスに対し，効果を持つものと考えられる．しかし，現実に感染が報告されているウイルスの大部分はメール感染型ウイルスであることと，その感染能力の高さから他のウイルスに比べても大きな被害をもたらす点を考慮して，メール感染型ウイルスを対象にモデル化を行い，シミュレーションによりその有効性を示す．

3. ウイルス駆除の現状と課題

ウイルスが感染したコンピュータではウイルス対策ソフト（アンチウイルス）を実行することで，ウイルスの検出と駆除を行うことができる．アンチウイルスは一般に大きく 2 つの機能から成り立っている．1 つはウイルス検出機能であり，これはコンピュータに感染し潜伏しているウイルスを発見するものである．ウイルスの検出は多くの場合，ウイルスパターンやシグネチャと呼ばれるウイルス固有の情報を元にスキャン法により行われる．このウイルスパターンは既知のウイルスを解析することで得たものであるため，未知のウイルスには基本的に対処できない．また，既知のウイルスであったとしても日々発見されるウイルスすべてに対処するには，頻繁にウイルスパターンを更新する必要がある．アンチウイルスのもう 1 つの機能は，ウイルス駆除機能である．これはコンピュータからウイルスを排除し，正常な状態に復帰するための，各ウイルスに対応したワクチンを用い実行される．ただし，ワクチンはウイルスパターンと違いウイルスが検出された後に初めて意味を持つものであるため，ユーザレベルで頻繁に更新する必要はなく，駆除が必要なときに入手可能でさえあれば問題はない．アンチウイルスはこの 2 つの機能を連携させたソフトウェアであることが多いが，機能的には独立したものと考えられる．そこで，本論文では必要に応じてウイルス検出を行う検出ソフトと，駆除を行うワクチンとを分けて扱うこととする．

現状のウイルス駆除は前述のアンチウイルスを用い，各コンピュータ，各ユーザレベルで実行されているものがほとんどである．すなわち，自分が利用しているコンピュータにアンチウイルスを導入するかどうかは，ユーザの判断によるものであることが多く，さらにウイルスパターンの更新や，実際のウイルスチェックの頻度などはユーザにより異なる．したがって，ウイルス対策を十分に行っているユーザのコンピュータはウイルスに感染することはないが，逆にまったく対策を行っていないユーザのコンピュータにはウイルスが感染し，長期にわたり発見されることなく活動し続けることが考えられる．対策を行っていないユーザのコンピュータにウイルスが感染することは，一見すると対策を行っているユーザにとっては無関係なことと思えるが，実際には次のような点で影響がある．現在のウイルスの多くはその増殖にメールをはじめとするネットワーク資源を利用している．これらネットワーク資源はすべてのユーザにとって共有の資源であり，それをウイルスにより不正に利用されることで本来の利用に不都合を生じる可能性がある．具体的には，ネットワークトラフィックの増大による遅延や，各種サーバの処理限界を超えることでのサーバダウンなどにより，ネットワーク本来の性能や機能を果たさなくなることが考えられ，実際に被害を生じたケースも報告されている．また，これらネットワーク資源のウイルスによる不正利用の問題は，ウイルスに感染したすべてのコンピュータからウイルスを除去しない限り解決することはない．しかし，現状ではウイルス対策はユーザ個人のレベルで行われているため，ウイルスに感染しているコンピュータをすべて発見するだけでも多くの時間と人手を必要とし，最終的にウイルスをすべて駆除するまでには，さらに時間と人手を要するものと考えられる．

そこで本論文では，このウイルス対策におけるユーザ意識と，ウイルスパターンの更新などでの人手への依存を避けることを目的に，新しいウイルス駆除手法を提案する．

4. 提 案 手 法

本論文では，ウイルスへの各ユーザの対策の違いや，検出や駆除への人手の必要性を削減することを目的に，次のような機能の実現を目指し新しいウイルス駆除手法を提案する．

(1) 仮にウイルスの検出がすべてのコンピュータで行われなかったとしても，感染したすべてのコンピュータからウイルス駆除を可能とする．

(2) あるコンピュータでウイルスの検出が行われた

か否かには関係なく，そのコンピュータからウイルスを駆除可能とする．

これらの機能が実現されれば，ユーザ個人によるウイルス検出ソフトの導入に依存することなく，管理者によって用意されたコンピュータ上で少数の検出ソフトを動作させウイルス駆除を行えば，すべてのコンピュータからウイルスを駆除可能となる．

提案する手法は従来のウイルス対策手法と同様に，ウイルスの検出と駆除という2つの段階を持つものとする．このうちウイルス検出の部分に関しては基本的には従来手法と同様とし，ウイルスパターンや何らかの発見的手法などによりウイルスを検出するものとする．しかし以下に提案する駆除手法を用いることで，提案手法では検出ソフトの導入率を従来のものよりも低く抑えることができる．ウイルス駆除に関する部分についても，各ウイルスに対応したワクチンによりウイルスを駆除するという点では従来手法と同様である．ただし提案手法では，このワクチンに次のような機能を付加する．

(1) ウイルスと同様の感染能力
ワクチンそれ自体に対応するウイルスの駆除能力に加え，対応するウイルスと同様の感染能力を持たせる．これによりワクチンはウイルスと同様に感染することで，他のコンピュータのウイルスを駆除可能となる．

(2) ウイルスの追跡と駆除を行う機能
ワクチンは対応するウイルスと同様の感染能力を用いることで，あるコンピュータからウイルスを駆除すると同時に，ウイルスが感染したであろう他のコンピュータに自動的に感染を試みてウイルスを追跡する．そして追跡先のコンピュータでも同様のことを繰り返す．これにより感染したコンピュータのウイルスは，追跡してきたワクチンにより駆除可能となる．

(3) 一定期間免疫状態とする機能
ワクチンはウイルスを駆除，追跡後に，一定期間コンピュータをウイルス感染から防護（免疫状態）し，その後消滅する．また，ワクチン感染先のコンピュータがウイルスに感染していなかった場合も，一定期間免疫状態を維持し，その後消滅する．

(4) 認証機関による認証
上記の機能をワクチンに持たせることで，ワクチンはいわば良性のウイルスとでもいうべきものになるが，このままでは悪性の本来のウイルスと区別することが困難となる．そこで，ワクチンに認証機関による認証に必要な情報を持たせ，外部プログラムでの認証を可能とする．なお，具体的な認証の実現方法は提案手法の動作には影響を与えないため，ここでは情報を付加することを提案するにとどめる．

上記機能をワクチンに加えることで，前述のように提案手法では検出ソフトの導入率を従来のものよりも低く抑えても従来手法と同等，もしくはそれ以上の駆除効果を得ることができる．すなわち，付加されたワクチンの感染能力によりウイルス感染経路の追跡が行われ，検出ソフトが導入されていないコンピュータにおいてもワクチンが動作するようになり，ウイルスを駆除可能となる．

なお，上記のようにワクチンにウイルス同様の感染能力を持たせることは，悪意のあるユーザによるワクチンのウイルスへの転用などの問題を発生させる．特にマクロウイルスなどのプログラムソースの可視性があるウイルスに対応するワクチンでは，ソースの可視性を取り除いて容易な転用を回避する必要がある．一般的にはソースの可視性を取り除き，なおかつマクロとして動作するワクチンを作ることは難しいものと思われる．しかし，現実問題としてマクロウイルスなどはMicrosoftの製品をターゲットとしており，Microsoftはマクロを暗号化する機能を提供している．したがって，現状ではマクロウイルスなどを含むすべてのウイルスのワクチンからソースの可視性を取り除くことが可能であり，悪意のあるユーザによるワクチンのウイルスへの容易な転用は回避することができる．

5. モデル化

提案手法の有効性を確認するための計算機シミュレーションを行うにあたり，本論文でのウイルス感染と駆除のモデル化を行う．本モデルではウイルス感染に対する各コンピュータの状態を，未感染状態，感染状態，免疫状態，未感染状態のループをとるものとする．またウイルスの現状も考慮して，対象とするウイルスをメール感染型ウイルスとする．

5.1 ネットワークのモデル化

ここでは，ウイルスの感染と駆除をシミュレーションするための，ネットワーク全体の構成に関するモデル化を行う．

- ネットワークは複数の「ノード」で構成されるとする．なお，メール型ウイルスを対象とすることから，ノード間の物理的な接続状態は考慮しない．
- ノード間の通信はウイルスおよびワクチンの送信に関するものしか考慮せず，感染に関係しない一般の通信は無視する．また，処理を簡略化するため通信は同期的として扱い，その時間単位を「ターン」

と呼ぶこととする．

5.2 ウイルスのモデル化

次にウイルスのモデル化について，いくつかのパラメータを設定する．なお，ウイルスはメール感染型ウイルスに限定するものとする．

- ウイルスはノードに到達すると同時に「ウイルス感染確率」で感染する．このときウイルスの二重感染はしないものとする．また，ウイルス感染確率には利用者がメール受信時にウイルスを発見し，感染が阻止される場合の確率低下も含まれる．
- ウイルスは 1 ターンに「ウイルス増殖数」のノードに，同時に感染を試みる．また，メール型ウイルスのため，ウイルスによっては感染を試みたノードはメールの履歴などの形で記録され，後に参照できるものとする．
- ウイルスは感染直後は “増殖状態” となり他のノードに感染を試みる．そして「増殖期間」分だけのターンが経過した後，“潜伏状態” へと移行し感染動作は停止する．
- 初期状態では，全ノード中の「ウイルス初期侵入率」で表される割合のノードにウイルスが感染しているものとする．

5.3 ウイルス検出ソフトのモデル化

本論文で用いるモデルでは，アンチウイルスの機能をウイルスの検出部分と駆除部分に分けて扱うものとし，ここでは検出部分に関するモデル化を行う．

- ウイルス検出ソフトは全ノード中の「検出ソフト導入率」で表される割合のノードに導入されている．これには，ウイルスパターンが古く実質的に意味をなさない場合や，定期的なチェックを行わないためにウイルスが検出されない場合の導入率低下なども含まれる．
- ウイルスに感染してからウイルスチェックが行われ，ウイルスが検出されるまでには「ウイルスチェック間隔」だけのターン数を要する．ウイルス検出ソフトが導入されているノードでは，ウイルスチェック間隔経過後ウイルスは必ず検出され駆除用のワクチンが実行される．

5.4 従来のワクチンのモデル化

ここでは従来のワクチンについてモデル化を行う．すなわち，前述したネットワーク，ウイルス，ウイルス検出ソフトのモデル化については，従来手法と提案手法で共通のものとするが，ワクチンに関する部分は本節と次節でそれぞれモデル化を行う．

- ワクチンは実行されると同時に「ウイルス駆除確率」でウイルスを駆除する．これには何らかのトラブルによりワクチンが実行されない場合や，駆除に失敗した場合の確率低下も含まれる．
- 一度ウイルスに感染した利用者はしばらくは用心するものと思われる．そこでワクチンによる駆除後は，ウイルス検出ソフトによるリアルタイムチェック機能の常駐が行われ「免疫期間」の間はウイルスの侵入を阻止するものとする．しかし，一般にリアルタイムチェックはシステムに負荷がかかるため，利用者はウイルス感染から時間がたてばリアルタイムチェック機能を停止すると考え，免疫期間経過後はリアルタイムチェック機能が停止し再感染可能な状態に戻るものとする．

5.5 提案するワクチンのモデル化

最後に提案する手法におけるワクチンのモデル化を行う．

- ワクチンは実行されると同時に「ウイルス駆除確率」でウイルスを駆除する．これには何らかのトラブルによりワクチンが実行されない場合や，駆除に失敗した場合，さらに次に述べるウイルスの追跡に失敗した場合の確率低下も含まれる．
- ワクチンはノードからウイルスを駆除すると同時に，ウイルスが感染を試みたノードに “感染” を試みる．このときワクチンの二重感染はしないものとする．ウイルスが感染を試みたノードの特定には，ウイルスの感染先を示すメールの履歴が存在すればそれを利用する．メールの履歴が存在しない場合には，ウイルス同様の感染方法を用いて感染先を特定する．すなわち，感染先の選択に登録したメールアドレスを利用するウイルスのワクチンは，同じく登録したメールアドレスを利用して感染先を決定する．ただし，この場合にはウイルスとワクチンが感染を行うターン数にずれが存在するため，登録したメールアドレスの変更などによりウイルスの追跡に必ずしも成功するとは限らない．そこで，ここではモデルの複雑化を避けるために，ウイルスの追跡に失敗した場合の影響はウイルス駆除確率の低下に含まれるものとする．
- ワクチンはウイルス同様 1 ターンに「ウイルス増殖数」のノードに，同時に感染を試みる．
- ワクチンはウイルスの駆除後は自動的にシステムに常駐し，「免疫期間」の間はウイルスの侵入を阻止する．また，ワクチンはノードにウイルスが感染していない場合も自動的にシステムに常駐し，免疫期間の間はウイルスの侵入を阻止する．免疫期間経過後はワクチンは自動的に常駐を止め消滅し，ノードは再感染可能な状態に戻る．

ここで，ノードが 6 つの場合における提案手法の例を**図 1**，**図 2**，**図 3** に示す．ここでは図 1 のようにウイルスがノード E に侵入し，図中の 1 から 4 の順に 1 ターンに 1 ノードの速さで次々に感染した場合を考える．ただし，4 ターン目のノード E への感染は二重感染になるため実行されず増殖動作はこの段階で停止する．このときウイルスチェック間隔が 2 ターンとすると，ノード A のウイルス検出ソフトがウイルスを検出し，ワクチンを起動するのは 3 ターン目となる．そして，4 ターン目にはワクチンはウイルスの感染経路を追いノード B に感染，以降この動作を繰り返すことで 6 ターン経過後にはウイルスはすべて駆除される（図 2）．その後は，ウイルス駆除後に常駐したワクチンによる免疫状態（図 3）となり，免疫期間経過後はワクチンが自動消滅することで再感染可能な状態に戻る．

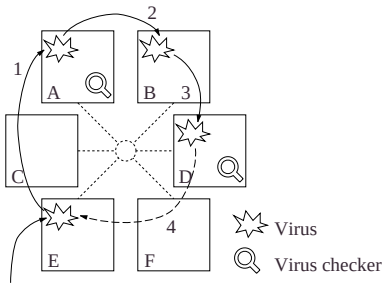

図 1 提案手法の例（ステップ 1）
Fig. 1 Example of proposed method (step 1).

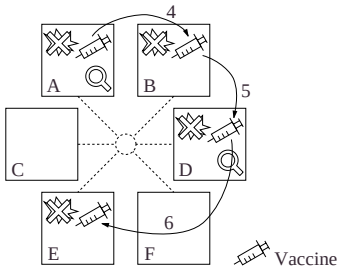

図 2 提案手法の例（ステップ 2）
Fig. 2 Example of proposed method (step 2).

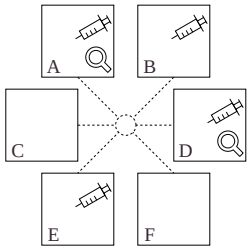

図 3 提案手法の例（ステップ 3）
Fig. 3 Example of proposed method (step 3).

6. シミュレーション

提案手法の有用性を確認するため計算機を用いシミュレーションを行った．シミュレーションではモデル化において定義したパラメータのうち，いくつかのものを変動させウイルスの感染と駆除の過程を見るが，そのとき変動させない各パラメータのデフォルトは次のように定めた．

6.1 シミュレーション条件

シミュレーションでは各パラメータのデフォルトを**表 1** に示す値に定めた．以下では各パラメータについて述べる．

(1) ネットワーク

ウイルスの感染対象となりうるノード数は理論的には無限に近い数だけ存在しうる．しかし本論文では対象とするウイルスをメール感染型としたため，感染対象は 2 章で述べたようにユーザの社会的人間関係により制限される．そこでシミュレーションではノード数を 1,024 とした．また，ターン数は感染と駆除の過程が十分に収束する 100 ターンまでとした．

(2) ウイルス

ウイルス感染確率はユーザによる発見も考慮して 0.2 とした．また増殖期間は，ウイルス感染時のみ増殖するとして 1 とした．

(3) ウイルス検出ソフト

検出ソフト導入率はデフォルト 0.5 としたが，提案手法の特徴である導入率が低い場合での効果的な動

表 1 シミュレーション条件
Table 1 Simulation conditions.

ネットワーク	
ノード	1,024
ターン数	100
ウイルス	
ウイルス感染確率	0.2
ウイルス増殖数	10
増殖期間（ターン）	1
ウイルス初期侵入率	0.05
ウイルス検出ソフト	
検出ソフト導入率	0.5
ウイルスチェック間隔（ターン）	2
ワクチン	
ウイルス駆除確率	0.5
免疫期間（ターン）	7

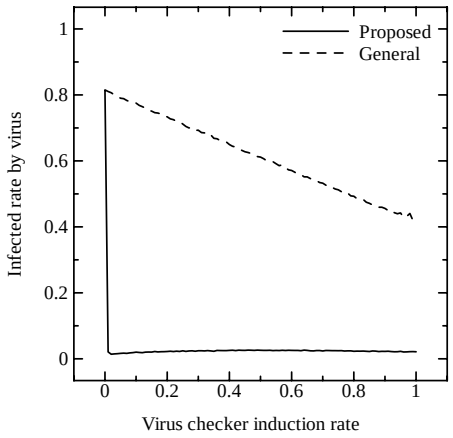

図 4 ウイルス検出ソフト導入率の影響
Fig. 4 Effect of virus checker introduction rate.

作を示すため，導入率を変動させたシミュレーションも行った．また，ウイルスチェック間隔もデフォルト 2 ターンとしたが，これも変動させたシミュレーション結果を後に示す．

(4) ワクチン

ワクチンは提案手法と従来手法では異なった機能を持つものではあるが，パラメータとしては同一のものを用いた．

なお，シミュレーションで用いるパラメータのいくつかは確率によるため，同一パラメータで 100 回のシミュレーションを行い，その平均を結果とした．

6.2 シミュレーション結果

6.2.1 ウイルス検出ソフト導入率

本論文で提案する手法は従来手法に比べ，ネットワーク全体へのウイルス検出ソフトの導入率が低い場合でも有効に機能すると考えられる．そこで，ウイルス検出ソフトの導入率を 0〜100%まで変えた場合の，100 ターン経過後の最終的な全ノードに対するウイルス感染率を**図 4** に示す．なお，検出ソフト導入率以外のパラメータは表 1 に示す値を用いた．

図からも明らかのように，従来手法ではウイルス検出ソフトの導入率の増加に対し一定の割合で下がっていたウイルス感染率が，提案手法ではわずか 1%でもウイルス検出ソフトが導入されていれば，ウイルス感染率で 2〜3%までウイルスを駆除可能となっている．

また，検出ソフト導入率が 1%のときのターン経過におけるウイルスとワクチンの感染率の推移を，提案手法については**図 5** に従来手法については**図 6** に示す．まず提案手法では，提案した機能によりワクチンがウイルスを追跡するため，ウイルス検出ソフトが導入されていないノードでもウイルスの駆除が行われ多

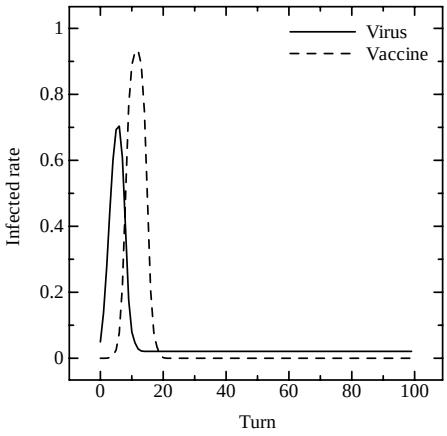

図 5 検出ソフト導入率：1%（提案手法）
Fig. 5 Virus checker introduction rate: 1% (proposed method).

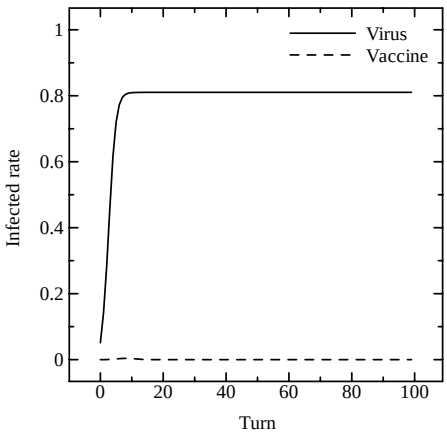

図 6 検出ソフト導入率：1%（従来手法）
Fig. 6 Virus checker introduction rate: 1% (general method).

くのウイルスが駆除される．シミュレーションではウイルス駆除確率を 50%としているため，すべてのノードからウイルスを駆除することはできないが，最終的なウイルス感染率を約 2%にまで低下させることに成功している．それに対し従来手法では，ワクチンはウイルス検出ソフトが導入されているノードでしか動作しないため，ほんの一部のウイルスしか駆除されず最終的には 80%以上のノードがウイルスに感染する．

6.2.2 ウイルスチェック間隔

次に，ウイルスチェック間隔の影響について評価を行った．**図 7** にウイルスチェック間隔を 1〜50 ターンまで変化させたときの最終的なウイルス感染率を示す．なお，今回もウイルスチェック間隔以外のパラメータは表 1 に示す値を用いた．

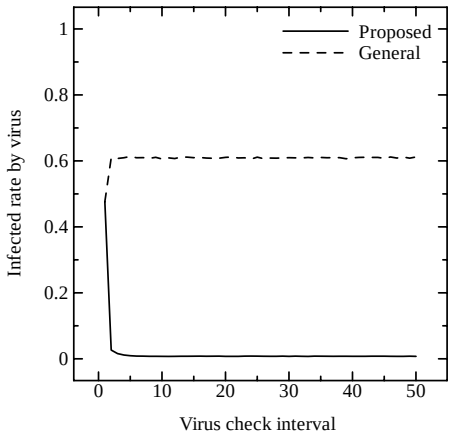

図 7 ウイルスチェック間隔の影響
Fig. 7 Effect of virus check interval.

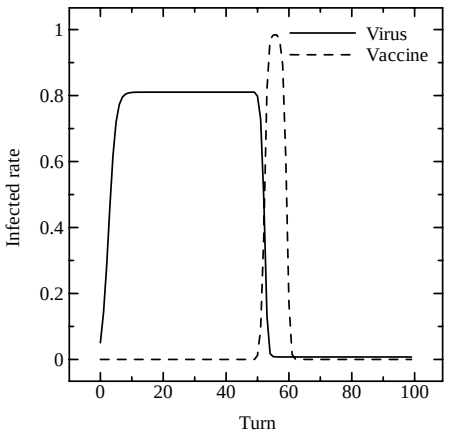

図 8 ウイルスチェック間隔：50 ターン（提案手法）
Fig. 8 Virus check interval: 50 turns (proposed method).

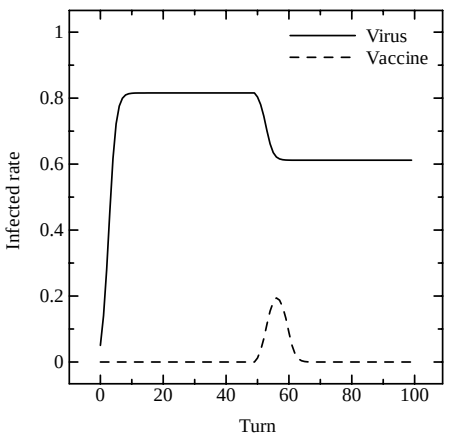

図 9 ウイルスチェック間隔：50 ターン（従来手法）
Fig. 9 Virus check interval: 50 turns (general method).

図 7 より，従来手法ではウイルスチェック間隔が短いほどウイルス駆除には有効だったものが，提案手法では逆にウイルスチェック間隔があまりに短いと有効に機能していないことが分かる．ただし，提案手法が有効に機能していないとはいっても，ウイルス感染率から見たウイルスの駆除能力は従来手法と同等である．提案手法でウイルスチェック間隔が短い場合に性能の低下が見られるのは，次のような理由によるものと考えられる．本論文で提案したワクチンによるウイルス追跡機能は，あくまでウイルスの追跡を行うものでありウイルスが感染してはじめて意味を持つものである．したがって，ウイルスチェックの間隔が短くなることでウイルス感染の機会が減少すると，ワクチンが追跡する機会も減少し結果として性能が低下する．

また，ウイルスチェック間隔が 50 ターンのときのターン経過におけるウイルスとワクチンの感染率の推移を，提案手法については**図 8** に従来手法については**図 9** に示す．提案手法では初期段階ではウイルス検出が行われずワクチンも動作しないことから，80%以上のノードがウイルスに感染する．しかし，50 ターン経過後にワクチンが駆除とウイルスの追跡を開始すると，ワクチンが急速に普及しウイルスを駆除するため，わずか数ターン後にはウイルス感染率は 1%以下にまで低下する．なお，すでに述べたように 50 ターンという時間経過はメールの履歴情報の欠落や登録したメールアドレスの変更などにより，ワクチンによるウイルスの追跡に一部失敗を生じさせる可能性も考えられ，それをシミュレーションではウイルス駆除確率の低下という形で表現している．すなわちシミュレーションで用いたウイルス駆除確率は，ウイルス追跡成功率と各ノードにおける純粋なウイルス駆除確率の積と考えることができる．したがって，このシミュレーションでのウイルス駆除確率 50%は，たとえばウイルスの追跡に 20%失敗しウイルス追跡成功率が 80%の場合には，純粋なウイルス駆除確率が 62.5%であることを意味している．実際の場面においてウイルス追跡成功率がどの程度になるのかは，ウイルスの感染対象選択方法やウイルスチェック間隔，そして何よりもユーザの利用状況に依存するため特定することは困難と思われる．しかし，ワクチンによる純粋なウイルス駆除確率は高い水準を維持するものと思われるので，ウイルス追跡にある程度失敗しても提案手法は有効に機能するものと考えられる．従来手法では初期段階で 80%以上のノードがウイルスに感染した後，ワクチンが実行されることでウイルス感染率は 60%まで減少する．しかし，それ以上の駆除は行われないため，結果としてネットワーク全体ではかなりの数のノードがウイルス

に感染したままで残ることになる．

6.2.3 ウイルス感染確率と駆除確率

ウイルス感染確率と駆除確率の最終的なウイルス感染率への影響を示すグラフについて，提案手法を**図 10** に従来手法を**図 11** に示す．ここでも，ウイルス感染確率と駆除確率以外のパラメータは表 1 に示す値を用いた．

提案手法においては感染確率によらず駆除確率が増加するにつれて最終的なウイルス感染率が急激に低下し，駆除確率が 50%を超えたあたりでは全ノード中のウイルス感染率が 5%以下となり有効に機能していることが確認できる．ただし，ウイルス感染確率が 10%前後の部分では全体に対するウイルス感染率の低下が鈍くなっている．これは前項のウイルスチェック間隔の影響と同様に，提案手法ではウイルスの感染がある程度進行してはじめてワクチンのウイルス追跡機能が有効に機能する結果である．

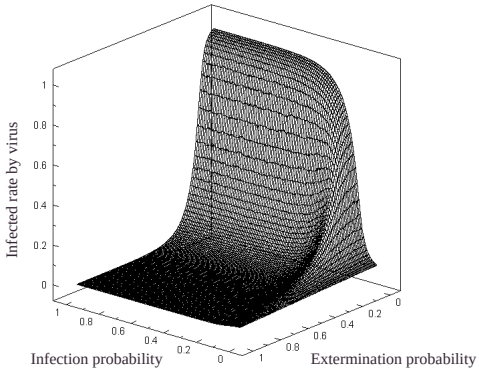

図 10 ウイルス感染確率と駆除確率の影響（提案手法）
Fig. 10 Effect of virus infection probability and extermination probability (proposed method).

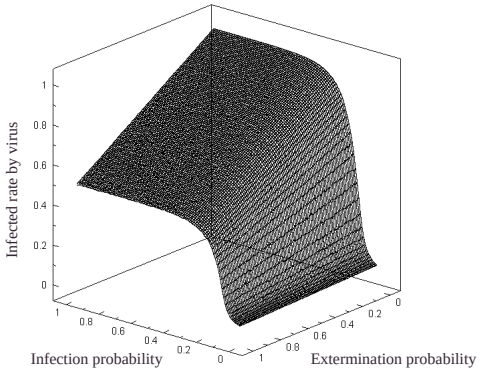

図 11 ウイルス感染確率と駆除確率の影響（従来手法）
Fig. 11 Effect of virus infection probability and extermination probability (general method).

次に，従来手法におけるウイルス感染確率と駆除確率の影響について述べる．まず駆除確率が増加するにつれて，ほぼ一定の割合で全ノード中のウイルス感染率が低下することが分かる．ただし，駆除確率が 100%となってもすべてのノードからウイルスを駆除することはできていない．これはウイルス検出ソフト導入率を 50%としているためで，検出ソフトによってウイルスが検出されない限りワクチンによる駆除は行われないからである．そして実際問題としてウイルス検出ソフトの導入は，ユーザのウイルス対策に関する意識やコストの問題があるため，導入率が 50%を超えることはほとんどないと思われる．ウイルス感染確率の影響についてだが，感染確率が低い段階では確率が増加するにつれて全体に対するウイルス感染率は急激に増加する．しかし感染確率が 40%前後からウイルス感染率は頭打ちとなり飽和している．これはシミュレーションで用いたノード数に限りがあるためだが，実際のネットワークにおいても同一組織内にあるコンピュータには限りがあり，メール型ウイルスはユーザの社会的人間関係に影響されることを考慮すると，ネットワーク内でのウイルス感染率はある値で飽和するものと思われる．

6.2.4 トラフィックへの影響

提案手法は従来のウイルス対策とは違い，ワクチンによるウイルス駆除と同時にワクチンの感染を行うため，ワクチン自体がトラフィックを発生させネットワーク全体に影響を与えるものと考えられる．しかし，実際にはウイルスを駆除すると同時にワクチンを感染させるため，ウイルスが生じさせていたトラフィックの代わりにワクチンのトラフィックが生じることになり，全体のトラフィック量が増加することはない．また，ワクチンはウイルスとは違い免疫期間経過後は自動消滅するため，最終的にはトラフィックも消滅する．このことを**図 12** に示す．シミュレーションでは増殖期間に制限を設けずウイルスに感染している間はつねに増殖するとし，またウイルスチェック間隔を 50 ターンとすることで，十分にウイルスがネットワーク全体に増殖した状態でのワクチンの実行を想定している．なお，上記以外のパラメータは表 1 に示す値を用いた．

図の縦軸はすべてのノードがウイルスまたはワクチンに感染し，かつ増殖動作をしているときに生じる最大トラフィックを 1 として，ネットワーク全体のトラフィックを示したものである．まず，感染の初期段階ではウイルスによるトラフィックが生じ，ウイルスの増殖動作が止まらないこともあって数ターンで最大ト

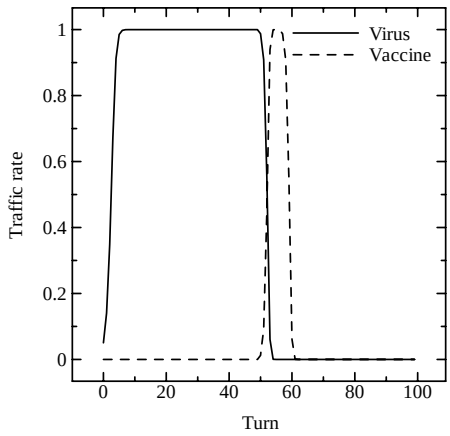

図 12 提案手法のトラフィックへの影響
Fig. 12 Effect on traffic in proposed method.

ラフィックに達する．50 ターン経過後ワクチンが実行されると，ウイルスが駆除されることでウイルスによるトラフィックが減少し，その代わりに同じだけのワクチンによるトラフィックが生じる．すなわち，この期間での両者の和はつねに 1 である．そして，免疫期間経過後はワクチンが自動的に消滅するため，トラフィックもまた消滅する．この結果からも分かるように，また提案手法のウイルスを駆除し同時にワクチンを感染させるという動作からいっても，ウイルスが生じさせていたトラフィックをワクチンのトラフィックが上回ることは考えられず，提案したワクチンの感染機能によりトラフィックが悪化することはない．また，ワクチンのトラフィックは免疫期間経過後には必ず消滅すること，さらには今回のシミュレーションには含まれていないが，ウイルスの発病によるシステムやデータへの被害を考えると，ワクチンを感染させることでトラフィックが一時的に生じるとしても，ウイルスの駆除を優先させた方が望ましいものと思われる．

6.3 考　　察

6.2.1 項に示したシミュレーション結果からも明らかなように，提案手法ではウイルス検出がたとえ全体の 1%のコンピュータでしか行われなかったとしても，ネットワーク全体からウイルスを駆除可能となっている．したがって，このウイルスの検出を各ユーザにゆだねることなく，ネットワークの管理者が用意した管理用のシステムの上で行えば，管理者によりネットワーク全体のウイルスを駆除可能となる．このことによりユーザの教育や，ユーザ個々のコンピュータに導入されているアンチウイルスの管理などのコストが不要となり，また管理者による一元管理が行えることからウイルス対策の確実性を上げることができる．

提案手法は 6.2.2 項や 6.2.3 項のシミュレーション結果からも分かるように，有効に機能するためにはウイルスがある程度感染しネットワークに広まっている状態の方が都合が良い．これは提案手法の最大の特徴であるウイルスの感染先に対するワクチン追跡機能が，あくまでもウイルスの感染を契機としているためであり，ワクチンが広範囲にわたり活動するにはウイルスもある程度広まっている必要がある．ただ，仮にウイルスがまったく感染しないためにワクチンの追跡が行われなかったとしても，提案手法は従来手法に追跡機能を付加したものであることから，従来手法と同等にウイルス駆除を行うことができる．また現実問題としては，ウイルスの感染から検出までにはある程度の時間が経過し，ウイルスが広く感染した状態での駆除が望まれるものと思われ，その点で提案手法はより有効に機能すると考えられる．

提案手法ではワクチンに感染能力を持たせ，それを増殖させることでウイルスの駆除を行っている．しかし，この状態は良性のウイルスを増殖させているのと同じであることから，本論文のようにネットワークの管理領域を考慮せずにワクチンを送り込むことは，異なる管理領域の管理者には敬遠される可能性がある．したがって，提案手法の実現性，実用性を考えた場合には，管理領域を設定しワクチンの活動を管理領域に限定した場合の有効性などを考慮する必要があるものと思われるが，この点に関しては今後の課題として次の機会に明らかにしたいと思う．

7. む　す　び

本論文ではコンピュータウイルスの駆除に関する新しい手法を提案した．提案手法はウイルスを駆除するワクチンにウイルスと同様の感染能力を持たせることで，ウイルスを駆除すると同時に，ウイルスが感染したであろう他のコンピュータにワクチンを送り込むという，ウイルスを追跡する機能を従来のワクチンに付加した点が最大の特徴となっている．このウイルス追跡機能により提案手法では，ウイルスの検出がネットワーク上のすべてのコンピュータで行われなかったとしても，感染したすべてのコンピュータからウイルス駆除を可能としている．これはいい換えるならば，管理者がウイルス検出を行うコンピュータを少数用意しウイルスの検出とワクチンによる駆除を行えば，ウイルス対策をユーザの意識に依存することなく管理者レベルで一元管理することが可能になることを示している．

提案手法の有効性を確認するため計算機シミュレー

ションを行ったところ，次のことが確認された．

(1) 提案手法はウイルス検出確率がわずかでも有効に機能する．

(2) 提案手法はウイルスが広範囲に感染した状態でより有効に機能する．

今後の課題としては，メール感染型以外のウイルスでの提案手法の有効性の確認，複数のネットワーク管理領域を想定し，その管理領域とワクチンの活動範囲を関連付けた手法の構築，感染機能を持ったワクチンの開発と実際のネットワークでの評価などが考えられる．

参 考 文 献

1) Jones, S.K. and White, Jr. C.E.: The IPM model of computer virus management, *Computer & Security*, Vol.9, pp.411–418 (1990).
2) Kephart, J.O. and White, S.R.: Directed-graph epidemiological models of computer viruses, *Proc. 1991 IEEE Computer Society Symposium on Research in Security and Privacy*, pp.343–359 (1991).
3) 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).
4) 千石 靖，岡本栄司，服部進実：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，情報処理学会論文誌，Vol.39, No.3, pp.818–824 (1998).
5) 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 (2001).
6) Kephart, J.O.: A biologically inspired immune system for computers, *Proc. 14th Int. Conf. on Artificial Intelligence*, pp.20–25 (1995).
7) Forrest, S., D'haeseller, P. and Helman, P.: An immunological approach to change detection: Algorithms, analysis and implications, *Proc. IEEE Symposium on Research in Security and Privacy* (1996).
8) Okamoto, T. and Ishida, Y.: A Distributed Approach against Computer Viruses Inspired by the Immune System, *IEICE Trans. Comm.*, Vol.E83-B, No.5, pp.908–915 (2000).
9) Schultz, M.G., Eskin, E. and Stolfo, S.J.: Malicious Email Filter — A UNIX Mail Filter that Detects Malicious Windows Executables, *Proc. USENIX Annual Technical Conference — FREENIX Track* (2001).
10) Schultz, M.G., Eskin, E., Zadok, E. and Stolfo, S.J.: Data Mining Methods for Detection of New Malicious Executables, *Proc. IEEE Symposium on Security and Privacy* (2001).
11) 2001 年ウイルス発見届出状況，情報処理振興事業協会セキュリティセンター (2002). http://www.ipa.go.jp/security/txt/attach/2002_01-1.html

(平成 13 年 11 月 30 日受付)
(平成 14 年 6 月 4 日採録)

中谷 直司

1994 年埼玉大学工学部電子工学科卒業．1996 年同大学院修士課程修了．1999 年同大学院博士課程修了．同年岩手大学工学部情報システム工学科教務職員．2001 年同科助手，現在に至る．進化型アルゴリズム，ネットワークセキュリティに関する研究に従事．博士（学術）．電子情報通信学会会員．

厚井 裕司（正会員）

1970 年東京理科大学理学部応用物理学科卒業．同年三菱電機（株）入社．2001 年岩手大学工学部情報システム工学科教授，現在に至る．主として，マルチメディアネットワーク，ネットワークセキュリティ，RF-ID タグに関する研究に従事．工学博士．IEEE，電子情報通信学会各会員．

鈴木 正幸（正会員）

1976 年東北大学工学部応用物理学科卒業．1978 年同大学院修士課程修了．1980 年東京大学大学院博士課程中退．同年東京大学理学部情報科学科助手．1984 年理化学研究所情報科学研究室．1993 年岩手大学工学部情報システム工学科助教授，現在に至る．数式処理，コンピュータネットワーク，並列分散計算に関する研究に従事．博士（理学）．日本応用数理学会，日本数式処理学会各会員．