2004－ＤＰＳ－117　(12)
2004－CSEC－　24　(12)
2004／3／4

ウイルスとワクチンの拡散形態によるウイルス感染状況の変化

中村太一*，中村逸一**，曽我正和***，西垣正勝*
*静岡大学情報学部，**NTT データ，***岩手県立大学ソフトウェア情報学部

あらまし　ウイルスやクラッカーの攻撃とセキュリティ対策はしばしばイタチゴッコにたとえられるが，本稿では，ネットワーク管理者とクラッカーとの攻防をゲーム理論の先読みによって解析する試みを提案する．その初期実験として，他のコンピュータへ P2P で広がりウイルスを駆除するワクチンを仮定し，ウイルスとワクチンの拡散形態によって，ネットワーク内におけるウイルスの蔓延がどのように変化するかをシミュレーションにより確かめる．

A virus infection simulation under various conditions of virus's and vaccine's infection

TAICHI NAKAMURA*, ITSUKAZU NAKAMURA**, MASAKAZU SOGA***, MASAKATSU NISHIGAKI*
*Shizuoka University,　**NTT Data Corp.,　***Iwate Prefectural University

Abstract　This paper proposes to apply game theory for analyzing the offense and defense between a network manager and a cracker. As the first trial, several virus infection simulations under various conditions of virus's and vaccine's infection are carried out here. Simulation results show that it would be effective to use a vaccine tailored to virus's type.

1 まえがき

インターネットの普及に伴い，人々が様々なコミュニケーションの手段としてインターネットを利用するようになり，今やインターネットは欠く事のできないものとなっている．しかし，その反面，不正アクセスやコンピュータウイルスなどのインターネット上の犯罪も急増している．世界中のコンピュータを繋ぐネットワークは高い利便性を持つが，それ故に，対策を怠るとウイルスやクラッカーの攻撃はまたたく間に広範囲に蔓延してしまう．

これを防ぐために，ネットワーク管理者やユーザはセキュリティパッチの適用やアンチウイルスソフトのデータの更新など，コンピュータの対策を常に万全にしておくことが要求される．しかし，クラッカーの攻撃方法も日々進歩しており，攻撃と対策はしばしばイタチゴッコにたとえられる．そこで本稿では，ネットワーク管理者とクラッカーとの攻防をゲーム理論の先読みにより解析する試みを提案する．

本稿では，その初期実験としてコンピュータウイルスの駆除を取り上げ，ウイルスとワクチンの拡散形態によって，ネットワーク内におけるウイルスの蔓延がどのように変化するかをシミュレーションにより確かめる．本シミュレーションでは，特にメール感染型ウイルスを対象としている. また, 他のコンピュータへ P2P で広がりウイルスを駆除するタイプのワクチンを仮定する．

2 ゲーム理論による攻防の解析

例えばコンピュータウイルスを例に採った場合，初期のファイル感染型ウイルスから始まり，最近のメール感染型およびネットワーク感染型のウイルス（ワーム）に至るまで，ウイルスは日進月歩で進化・分化している[1]．一方，防御側も多くの企業や研究者がファイアウォールやアンチウイルスソフト，IDS の開発・改良に力を注いでおり，それらを統合したソリューション製品[2]なども発表され始めた．クラッカーとネットワーク管理者の攻防は「ある攻撃に対して防御策を施すと，それを破る攻撃が現れ，更にそれに対する防御を実施する」ということが無限に繰り返されるイタチゴッコであり，対策として真に完璧な対策は存在しないと考える者も多い．

しかし，世の中にはそもそも攻撃側と防御側の力量が拮抗する事象が多く存在する．その最た

るものが野球やサッカーなどのスポーツや，チェスや将棋などのゲームである．そして，その攻防には戦略論や戦術論およびゲーム理論など，多くのインテリジェンスが導入されている．

そこで本稿では，ネットワーク管理者とクラッカーとの攻防をゲーム理論の先読みにより解析する試みを提案する．すなわち，クラッカーの攻撃形態やウイルスの拡散形態から，その展開を解析し，予測することにより，被害が広まりにくいような対策を講じることができないかを探ることが本研究の目的である．例えば将棋では，「ここに金を打ちたいのだが，あそこの飛車が効いているので打てない」とか，「ここに角を打つと，相手はその角をあの桂馬で取るしかなく，そこで次ぎに金を打てば・・・」という理論的考察により次の一手を考える．このような「この対策が効いている」というコンセプトや，「ここにこういう対策を施しておくと，クラッカーはこういう攻撃をせざるを得ない」という攻防の駆け引きなどを導入することができれば，ネットワーク上のどこにどういう対策を施せば必要十分であるかを解析することも可能になってくるのではないかと期待できる．

ネットワーク管理者とクラッカーとの攻防を解析するにあたり，その攻防をシミュレーションにより確認することが肝要であると考えられる．よって本稿では，その初期実験としてコンピュータウイルスの感染とワクチンの拡散に関するシミュレーションを実施する．

3 コンピュータウイルスとワクチンの定義

3. 1 コンピュータウイルス

近年，増加しているコンピュータウイルスの中で代表的な物には，以前から大きな問題になっている「メール感染型ウイルス」と，最近その被害が急増している「ネットワーク感染型ウイルス」がある[1]．メール感染型ウイルスは，感染後，コンピュータに存在するメールのアドレス帳を参照し，ユーザに親しい関係にあると思われる人物（親しい人なのでアドレス帳に登録されている）のコンピュータに感染を試みる．ネットワーク感染型ウイルスは，感染後，他のコンピュータに不正アクセスを試み，OS などの脆弱性を突いて感染する．

文献[3]にメール感染型ウイルスに関する感染シミュレーションが報告されており，その結果との比較なども行えると考え，本稿ではまずはメール感染型ウイルスに焦点をしぼることとする．

3. 2 ワクチン

一般にコンピュータウイルスに対処するためには，ウイルスの検出と駆除の機能を有するアンチウイルスソフトの使用と，ウイルスが利用するセキュリティホールに対するセキュリティパッチの適用が肝要である．本稿では，これらを総称して「ワクチン」と呼ぶ．既存のアンチウイルスソフトは一般に，最新のウイルスパターンファイルを用いて既知ウイルスをスキャンする．また，セキュリティホールは日々発見されており，それに対応してセキュリティパッチがリリースされる．よって，ワクチンを有効に働かせるためには，ワクチンを最新の状態に保つ必要がある．

文献[3]では，ワクチンにウイルスの追跡能力（ウイルスと同様の感染能力）を与えることにより，最新のワクチンがウイルスを追いかける形でコンピュータに届き，非常に効果的にウイルスの駆除が可能となることがシミュレーションで確かめられている．一方，現実に，P2P 配信機能を利用してウイルスパターンファイルを高速に自動更新するアンチウイルスソフト製品が市場に投入され始めた[4]．そこで本稿では，ウイルスの感染が検出されたコンピュータから，そのコンピュータに存在するメールのアドレス帳を参照し，ユーザに親しい関係にあると思われる人物のコンピュータに最新ワクチンを P2P 通信により配信するタイプのワクチンを取り扱うこととする．

4 モデル化

4. 1 ネットワークのモデル化

まず，シミュレーションのためのネットワークのモデル化を行う．本稿では，メール感染型ウイルスを対象とする事から，文献[3]と同様，コンピュータの物理的接続形態は考慮する必要はな

い．しかし，今回のシミュレーションでは，メールのアドレス帳を参照して親しい間柄であると思われる人物のコンピュータに自分自身を送信するタイプのウイルスおよびワクチンを想定するため，ネットワークに接続されるコンピュータ間の距離に「ユーザどうしの親しさ」が反映されるようなモデル化を行う．

(1) ネットワークは碁盤のような「マス目」を複数個並べて構成し，それぞれの「マス目」をネットワークに接続されているコンピュータとする．各コンピュータにそれを定常的に利用するユーザが一人ずつ存在しているとする．閉じたネットワークを仮定し，マス目の数は有限とする．

(2) 各コンピュータのメールのアドレス帳には 8 人のユーザ（のコンピュータ）が登録されているとする．親しい間柄にある二人のユーザはお互いに相手のメールアドレスを登録しているとする．全てのコンピュータに対して，あるマス目に対応するコンピュータのアドレス帳に登録されている 8 台のコンピュータを，そのマス目に隣接する 8 個のマス目に対応させることが可能であるとする．これにより，本ネットワークのモデルでは隣接するマス目のコンピュータどうしが親しいという事になり，ウイルスおよびワクチンは距離的に近いコンピュータから順に感染，伝播していく．

(3) ネットワークにおける通信はウイルスとワクチンの送信に関するもののみを考慮することとし，これらに関係のない通信は無視する．また，シミュレーションを簡略化するためにウイルスとワクチンの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．

4．2 ウイルスのモデル化

ウイルスのモデル化を行う．ウイルスは 3.1 節で定義したようにメール感染型ウイルスである．

(1) ウイルスは 1 ターンの間に隣接する 8 台のコンピュータに感染するものとする．ただし，各コンピュータはユーザのセキュリティ意識や既実施の対策が異なると考えられるので，ウイルスの感染には「ウイルス感染確率」が存在するとする．例えば「ウイルス感染確率」が 75%なら，次のターンで隣接する 8 台のコンピュータの内からランダムに 6 台のコンピュータが選ばれ，感染する．なお，すでにウイルスに感染しているコンピュータへの二重感染はないものとする．

(2) ウイルスは駆除されるまで，毎ターン感染を行う．

(3) 初期状態では，ネットワークの中心の 1 台のコンピュータにのみウイルスが感染しているものとする．

4．3 ワクチンのモデル化

本シミュレーションでは，3.2 節で定義したように，ワクチンにもメールのアドレス帳を参照して親しい関係にあると思われる人物のコンピュータに最新ワクチンを転送する機能を与えている．最新ワクチンは P2P 通信により配信されるとする．なお，ワクチンの転送方法に関しては本稿では規定しない．すなわち，文献[3]のようにホワイトウイルス的に自分自身を転送してもよいし，文献[4]のようにウイルスパターンファイルやパッチファイルのみを転送した上で，先方にウイルスのチェックまたはパッチの適用をうながすという方法でも構わない．

(1) ワクチンは毎ターン，自分のコンピュータのウイルスチェックを行い，ウイルスの侵入があれば駆除を行う．ウイルスを検出したときのみ，ワクチンはそのターンの間に隣接する 8 台のコンピュータにワクチンを転送するものとする．ただし，P2P 通信の失敗などを考慮して，ワクチンの転送には「ワクチン受理確率」が存在するとする．例えば「ワクチン受理確率」が 75%なら，次のターンで隣接する 8 台のコンピュータの内からランダムに 6 台のコンピュータが選ばれ，ワクチンが転送される．

(2) ワクチンが届くと，パッチなどによりウイルスの感染経路を塞いだ状態となり，その後ウイルスには感染しない．ワクチンが届いた先のコンピュータにおいては，ワクチンが届いてから 1 ターン以内にウイルスの侵入がなければ，ワクチンは自動的に消滅し，更に隣のコンピュータにワクチンを転送することはない．すなわち一般のコンピュータにおいてはワクチンは常駐しない．

(3) ワクチンは，ネットワーク中の全コンピュータの内,「ワクチン設置確率」で指定される数のコンピュータに前もって導入されているものとする．例えば，全コンピュータが 1000 台でワクチン設置確率が 10%であれば，1000 台の中からランダムに 100 台が選ばれ，この 100 台にワクチンが常駐している状態からシミュレーションが開始される．前もってワクチンが導入されているコンピュータにおいてのみ，ワクチンは永久的に常駐し，消滅することはないとする．

5 シミュレーション

本シミュレーションの目的は，ウイルスとワクチンの攻防の様子を知ることにある．そこで，ウイルス感染確率，ワクチン受理確率，ワクチン設置確率を変更し，様々なパターンでシミュレーションを行う．ネットワークに接続されているコンピュータは有限であるので，ウイルスの感染とワクチンの伝播はいずれ収束する．状況が収束するまでターンを進め，シミュレーション終了時にウイルスもワクチンも感染していない「未感染コンピュータ」の数を調べる（当然，前もってワクチンが与えられているコンピュータは未感染コンピュータに含まれない）．なお，シミュレーションのいくつかの要素は乱数による確率に左右されるため，同一の条件で 100 回のシミュレーションを行い，未感染コンピュータ数の平均値を算出する．

5. 1 シミュレーション条件

ネットワークは 32×32 の 1024 個のマス目(コンピュータ)とした. ウイルス感染確率は 25%, 50%，75%，100%の 4 種類とした．なお，いずれの場合も，初期状態ではネットワークの中心の 1 台のコンピュータにのみウイルスが感染している. ワクチン受理確率は 25%, 50%, 75%, 100%の 4 種類とした．ワクチン設置確率は 1/32，1/16，1/8，3/16，1/4 の 5 種類とした.

5. 2 シミュレーション結果

ウイルス感染確率，ワクチン受理確率，ワクチン設置確率の全ての組合せにおける未感染コンピュータの数を図 1(a)〜(d)に示す.

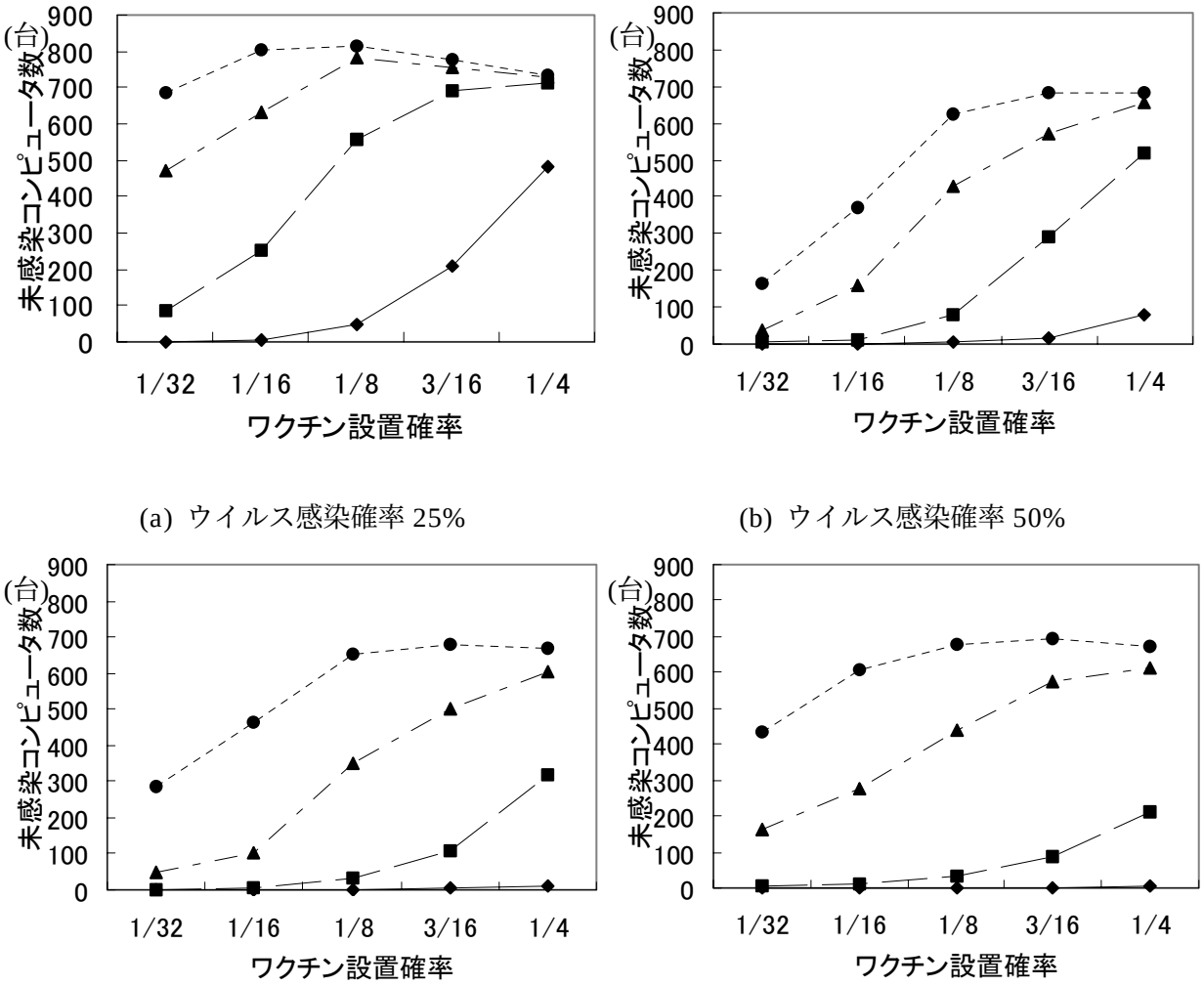
図 1 から，ワクチン設置確率が高くなるほど未感染コンピュータ数は増加傾向があることが読み取れる．前もって多くのコンピュータに最新ワクチンが配信されているほど，ウイルスの感染は抑制されることが確認できる. しかし, ウイルス感染確率がワクチン受理確率より大きいと，ワクチン設置確率を高くしても，ほとんどのコンピュータがウイルスに感染してしまう．逆に，ウイルス感染確率がワクチン受理確率より小さい場合には，ある程度のワクチン設置確率を確保してやれば，ワクチン設置確率をそれ以上高くしても未感染コンピュータ数は減少しない.

そこで, 各未感染コンピュータ数を初期状態でのワクチン数で割り,「ワクチン 1 つ当たりで守ることができるコンピュータ数」を算出した．以降，これを「コストパフォーマンス」と呼ぶ. 結果を図 2(a)〜(d)に示す．なお，図 2(a)と図 2(b)〜(d)では y 軸の尺度が異なることに注意されたい.

図 2 から，ワクチン感染確率が高ければ，ワクチン設置確率が低いほどコストパフォーマンスが高まることが分かる．ワクチン感染確率が低い場合には，総じてコストパフォーマンスは低いが，ワクチン設置確率が高くなるにつれてコストパフォーマンスは微増する.

5. 3 考察

5.2 節のシミュレーション結果から, ウイルス感染確率がワクチン受理確率より小さい場合には, 前もってネットワーク内の一部のコンピュータにのみ，親しい間柄のユーザに最新ワクチンを P2P で配信するタイプのワクチンを設置しておくことにより，コストパフォーマンスの面から効率的にウイルスの感染を抑制することができる可能性が認められた．ただし，例えばウイルス感染確率 25%，ワクチン受理確率 100%の場合，確かにワクチン設置確率が小さいほどコストパフォーマンスは高いと言える(図 2(a))が，未感染コンピュータの数そのものはワクチン設置確率



(a) ウイルス感染確率 25%　　(b) ウイルス感染確率 50%

(c) ウイルス感染確率 75%　　(d) ウイルス感染確率 100%

図 1　未感染コンピュータ数

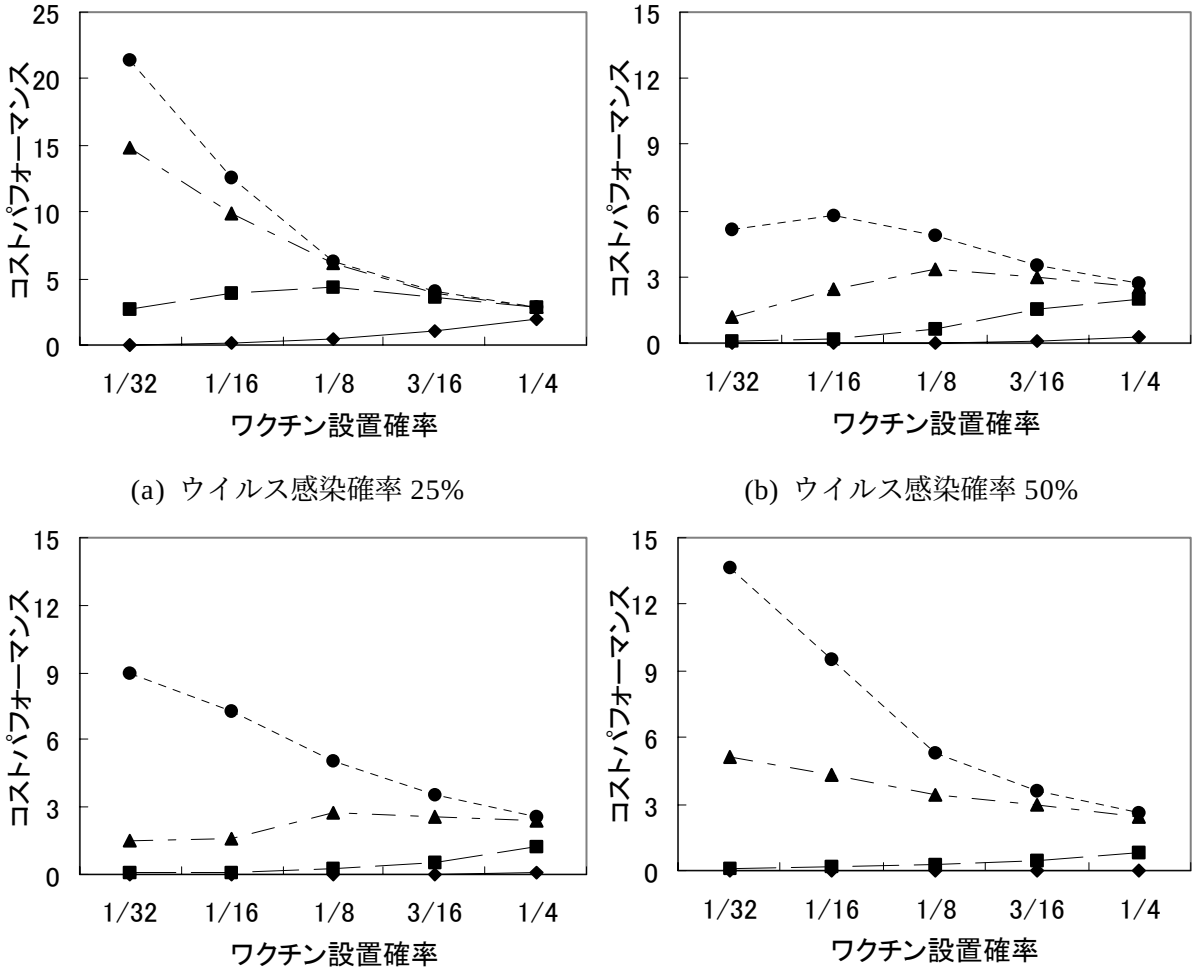
（—●—：ワクチン受理確率 25%，—■—：同 50%，—▲—：同 75%，- -●- -：同 100%）

が 1/8 より小さくなると減少してしまう(図 1(a)). 実際にはどのような指標を用いてワクチン設置確率を決定すれば実用的であるかの考察が必要となる.

本シミュレーションから，ウイルスおよびワクチンの性質によって両者の攻防の結果が大きく異なることが確かめられた．本シミュレーションは非常に初歩的なものであるが，ウイルスとワクチンの性質を見極めて, ネットワーク管理者がワクチンによる防御の采配を振ることにより, 効果的なウイルス対策が実現できる可能性があることが示唆される結果が得られた．現在のウイルス対策は「全てのコンピュータに最新のセキュリティパッチやアンチウイルスソフトを強制的・自動的に適用する」という方針で進んでいるが，本研究の今後の成果次第では，要となるコンピュータにのみ適切な対策を施すことによりウイルスとの攻防に勝利することができるような理論が体系化できるかもしれない．研究を重ね，その可能性を探りたい.

6 むすび

本稿では，ネットワーク管理者とクラッカーとの攻防をゲーム理論の先読みによって解析する試みを提案し，その初期実験としてウイルスとワクチンの攻防がその拡散形態によって異なる事をシミュレーションにより確かめた．研究を進め，ネットワーク管理者とクラッカーとの攻防を



(a) ウイルス感染確率 25%　　(b) ウイルス感染確率 50%

(c) ウイルス感染確率 75%　　(d) ウイルス感染確率 100%

図 2　コストパフォーマンス

（—●—：ワクチン受理確率 25%，—■—：同 50%，—▲—：同 75%，- -●- -：同 100%）

理論的に考察し，有効な防御方法を解析的に導出できるようにすることが今後の課題である．次のステップとしては，あるコンピュータがウイルスを検出した際に，隣接するコンピュータだけでなく，その他のコンピュータにも同時にワクチンを拡散することにより，ウイルスを閉じられた区間内に効率良く閉じ込めて駆除するような方式をシミュレーションにより構築していくことを予定している．

参考文献

[1] トレンドマイクロ株式会社：ウイルスの種類,
http://www．trendmicro．com/jp/security/general/type/overview．htm

[2] NEC：プレスリリース「社内におけるセキュリティ対策が未完了のパソコンをウイルス対策専用のネットワークに強制的に接続する「検疫システムソリューション」の発売について」,
http://www．nec．co．jp/press/ja/0401/2904．html

[3] 中谷，厚井，鈴木：追跡能力を有するワクチンを用いたウイルス駆除手法，情報処理学会論文誌，Vol．44，No．8，pp．2467-2477，2002 年 8 月．

[4] 日本ネットワークアソシエイツ株式会社：McAfee VirusScan AsaP,
http://www．nai．com/japan/products/mcafee/asap/asap．asp