2004－CSEC－27　(9)
2004／12／20

エージェントベースアプローチによるワーム拡散モデルの提案

航空自衛隊 航空システム通信隊　○ 石西　正幸
東京大学 医科学研究所　田沼　英樹
東京工業大学 大学院総合理工学研究科　出口　弘

あらまし: 近年のワームの流行は，官公庁や企業におけるネットワークに大きな被害をもたらし，我々の生活に多大な影響を与え，深刻な問題を引き起こしている．本研究では、このようなワームの伝染に対して、被害を局限しシステムを防護するための対処方法を得ることを目的とし，エージェントベースアプローチによるシミュレーションを通じて拡散現象を分析する。

A Diffusion Model of Computer Worms Using Agent-based Approach

○ Masayuki ISHINISHI, Air Communications and Systems Wing, JASDF
Hideki TANUMA, The Institute of Medical Science, The University of Tokyo
Hiroshi DEGUCHI, Interdisciplinary Graduate School of Science and Engineering, Tokyo Institute of Technology

Abstract: An increase of computer worms in recent years caused big damage on the network in public offices and enterprises. So the damage influences at the life of the people and becomes serious problems. The authors aim to clarify diffusion phenomena by the simulation so as to obtain anti-virus policies . This paper proposes the diffusion model of computer worms using agent-based approach. The authors employ the SOARS language which is a spot-oriented model and compare it with the conventional method.

Key Words: コンピュータウイルス，拡散現象，スポット指向モデル

1　まえがき

2003 年の Slammer, Blaster, そして Welchia 等のワームの流行は，企業や官公庁における情報通信システムで大きな被害をもたらし，ネットワークセキュリティ対策の重要性を認識させるきっかけとなった．その後も Sasser のように，基本ソフトウェア (以後 OS と呼ぶ) の脆弱性を利用した，ネットワークに接続しているだけで感染するワームが発生している [1]．ワームの流行は，行政や経済活動に大きなダメージを与えるおそれがあることから，早急な対策が求められており，さまざまなベンダー等からソリューションが提案されている．

そもそもワームの感染を防止するには，ベンダーから提供されている修正プログラムを適用することにより可能となる．しかしながら，修正プログラムのなかには適用後にシステムの再起動が必要になるほか，修正プログラムの副作用による不具合が発生するものが存在する．そのため，中断の絶無が求められる業務システムにおけるサーバ等では，運用に与える影響を事前にテストする必要があるため，修正プログラムの早期適用は困難であるといえる．

このため，情報システムによっては，インターネットには接続しないクローズなネットワークを設けることにより，組織内のコンピュータへのワームの感染を防止する方法を取ってきた．

ところが，2003 年の Blaster の流行では，インターネットに接続しワームに感染したノートパソコン等を企業や官公庁等に持ち込み，情報通信システムに接続することにより，クローズなネットワークであってもワームの流行が発生した [2]．これに対する方策として，正規のコンピュータ以外の持ち込みを禁じたセキュリティポリシーの制定や，検疫ネットワークの導入が考えられるが，ワーム流行を予防するには限界がある．

本研究では，組織内のイントラネットにおけるワーム伝染の事案が発生する場合において，被害を局限しシステムを防護するための対処方法について，主に運用的側面から検討することを目的としている．本稿では，社会システム科学において用いられているエージェントベースアプローチによるモデル化及びシミュレーションについて報告する．

2　コンピュータウイルスに関する先行研究

コンピュータウイルスの対策に関する研究は，個々の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と，ウイルス全体の現象を解析するマクロレベルの研究

とに分けられる．この中でマクロレベルの研究には，伝染病とコンピュータウイルスの類似性に着目して，コンピュータウイルスの拡散を伝染病の伝播モデルで解析したものが多い．

千石らはネットワークにおけるウイルスの拡散過程をシミュレーションと理論式により解析し，ウイルスの感染に対するアンチウィルスソフトの駆除の効果及び保有率による効果の違いを明らかにしている [3][4]．一方，岡本らは，メール送信機能を有し，短期間に広域に拡散可能なウイルスの拡散モデルを構築し，感染数の時間変化，コンピュータ間の接続数と感染数の関係，その拡散現象を明らかにしている [5]．また，林らは，電子メールによるウイルスの拡散モデルについて，電子メールの送受信関係がべき乗分布に従うスケールフリーネットワークとなることを示し，新規使用者によるネットワーク成長によって再流行現象が引き起こされることを示している．また，ウイルスの拡散を抑えるには，ハブとなる箇所を免疫化することが効果的であることを示している [6]．

これらの先行研究は，ウイルス拡散における挙動の分析を中心としているが，ウイルス拡散現象に対して，ユーザやシステム管理者，そして事案対処要員のウイルス対処活動を考慮し，個々の人間の行動による伝染防止の効果を検討している研究は少ない．また，ウイルス伝染時において対処活動が動的かつ適応的に変化するような場合，それを既存のシミュレーションで記述することは困難である [7]．したがって，これらを考慮した問題の記述に適した手法が求められる．

3　エージェントベースアプローチ

エージェントベースアプローチは，エージェントと呼ぶ内部状態と意思決定能力とを備えた複数の主体の概念を利用したボトムアップなモデル化とコンピュータシミュレーションとに特徴づけられる．すなわち，エージェントに基づくシミュレーションは，(1) ミクロ的な観点においてエージェントが（個別の）内部状態を持ち，自律的に行動・適応し，情報交換と問題解決に携わる事，(2) その結果として対象システムのマクロ的な性質が創発する事，(3) エージェントとエージェントを囲む環境とがミクロ・マクロリンクを形成し，互いに影響を及ぼしあいながらシステムの状態が変化していく事を特徴とする [8]．

筆者らは，ワーム伝染時におけるユーザや管理者等の対処行動からシステム全体に及ぼす影響の分析において，上記の特徴が問題の記述に適していることから，エージェントベースアプローチを採用した．

4　エージェントベースアプローチによるワーム拡散モデル

エージェントベースアプローチにおけるモデリングでは，その多くがエージェントの位置関係を重視したセル型モデルを用いている．しかしながら，本研究のようにネットワークの接続形態が変化するといった，エージェント同士の相互作用の場が動的に変化する場合においては，セル型モデルでシミュレーションを記述することは困難である．

そこで本研究では，セル型モデルに代わるワームの拡散現象を分析するためのシミュレーション環境として,「スポット指向モデル」と呼ばれる相互作用の形態を用いたSOARS(Spot Oriented Action Role Simulator)[9][10]を採用している．

4.1　エージェントベースシミュレーション環境 SOARS

SOARS はエージェントベースモデリング (ABM) において，シミュレーションによる分析のためのツールとして開発されたものであり，エージェントの役割行為を適切に表現することを目的としている．

SOARS は，エージェントの役割行為を記述する宣言型のスクリプト言語と，それを複数の因果的に順序関係を持つステージという概念に基づいた手続き型の実行順序制御が実装されており，Java 上で動作する．SOARS では，エージェントが移動したり相互作用する場を「スポット」といい，スポットは状態を特徴づけるオブジェクトと，相互作用を記述するオブジェクトである「レゾルバ」から構成される．SOARS の動的な制御構造は，シミュレーション上の離散時間の基本単位を表す「ステップ」，ステップの内部において因果的な順序関係を表す「ステージ」，ステージの内部においてエージェント及びレゾルバを選択し，それぞれの役割ルールを実行するための単位を表す「フェーズ」，フェーズの内部において個々のエージェントのルールの実行単位を表す「ターン」から構成されている．

4.2　ネットワークのモデル化

本研究で取り扱うネットワークは，イントラネットとインターネットに分類される．イントラネットでは，インターネットには接続されていないクローズな環境が想定されており，Fig.1 のように部・課等の組織別に設置した LAN と，LAN 同士をルータ等の接続装置から専

用線等を介して接続するための WAN とで構成される．一方インターネットは，イントラネットから独立しており，使用者が自宅や出張先からネットワークを利用するために接続される．

本研究では，ネットワークをスポットとし，コンピュータをエージェントとして取り扱う．コンピュータのネットワークへの接続は，スポット内におけるエージェントの存在により表される．スポットは次のように分類される．

切断スポット コンピュータは，ネットワークから切り離され，スタンドアロンの状態にある．

LAN スポット コンピュータは，LAN に接続されている．

WAN スポット コンピュータは，WAN に接続されている．

Internet スポット コンピュータは，外部インターネットに接続されている．

Fig.1 で表されるネットワーク構造を SOARS のスポット構成で示すと，Fig.2 のようになる．例えば利用者がコンピュータを WAN に接続されたネットワークに接続し，データの交換を行うとき，シミュレーション上では同一ステップ内でエージェントが LAN スポット→ WAN スポットの順に移動し，各スポットでエージェント間のデータの交換が行われる．同様に WAN から切り離されたネットワークの場合，エージェントは LAN スポットのみに存在し，WAN スポットへの移動は行われない．

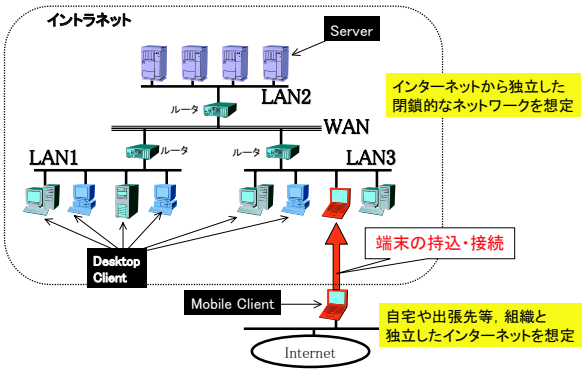


Fig. 1 対象とするネットワーク

4.3 ステージ構成

SOARS におけるワーム拡散モデルのステージ構成は以下のようになる．

設定ステージ エージェント，スポットの設定

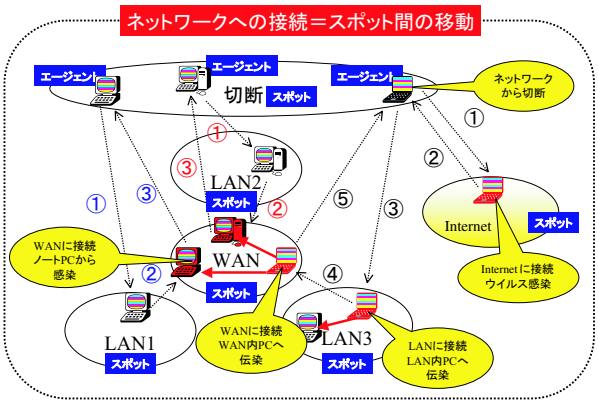


Fig. 2 スポット構成

移動ステージ スポット間のエージェントの移動

Internet 感染ステージ Internet におけるワーム感染

LAN 感染ステージ LAN におけるワーム感染

WAN 感染ステージ WAN におけるワーム感染

発症ステージ ワーム感染したコンピュータによるデータの破壊

発見・通報ステージ ワーム感染の発見及び他ユーザ・管理者への通報

切断ステージ ネットワークからの切断

対策ステージ 修正プログラムの適用

4.4 コンピュータのモデル化

4.4.1 コンピュータの種類

本研究では，ネットワーク上におけるコンピュータ同士のデータのやりとりによるワームの感染を，ネットワークに該当するスポット内におけるエージェント同士の相互作用として表す．

ネットワークに接続されるコンピュータの種類を Table.1 に示す．

4.4.2 コンピュータの状態

コンピュータの状態は，ワーム感染の状態，データの状態，そして OS の状態に分類される．詳細を Fig.3 に示す．

ワーム感染の状態は，「未感染状態 (Susceptible)」「感染状態 (Infected)」「対策済み状態 (Recovered)」に分けられる．未感染状態のコンピュータは，ワームに感染す

Table. 1 コンピュータの種類

コンピュータの種類	機能
Server	24 時間運用を目的とするため，システムの停止・再起動に制約があり，修正プログラムの適用が困難
Desktop	電源断や再起動及び修正プログラムの適用が任意に可能.
Mobile	イントラネット及びインターネットのどちらにも接続可能. 他は Desktop と同じ

ると感染状態へ移行し，修正プログラムを適用することにより，対策済み状態へ移行する．また，感染状態のコンピュータは，未感染状態のコンピュータと同様に修正プログラムの適用により対策済み状態へ移行する．

データの状態は,「正常 (Normal)」と「破壊 (Crashed)」に分けられる．発症ステージにおいて，コンピュータが未感染状態から感染状態に移行し，確率 p_1 によりワームが発病した場合に，正常から破壊に状態が変化する．

OS の状態は,「正常 (Normal)」と「異常 (BreakDown)」に分けられる．対策ステージにおいて，コンピュータが未感染状態または感染状態のとき，修正プログラムを適用することにより，確率 p_2 で修正プログラムの副作用によるシステムの異常が発生し，正常から異常に状態が変化する．

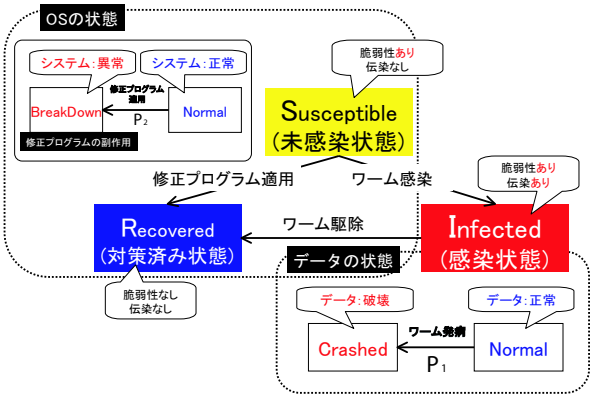


Fig. 3 ワーム感染の状態

4.5 ワームのモデル化

本研究で取り扱うワームは，ワーム型を対象としており，ワームに感染しているコンピュータとワームに関する脆弱性のあるコンピュータが互いにネットワーク上で接続されるとき伝染する．ワームは LAN，WAN，そして Internet において，感染ステージで感染状態のコンピュータから未感染状態のコンピュータへ伝染する．ワームの感染動作は，以下に示される．

LAN における感染 ワームは，LAN スポットに存在している未感染状態のコンピュータから，１台をランダムに選択する．

WAN における感染 LAN のときと同様に，ワームは，WAN スポットに存在している未感染状態のコンピュータから，１台をランダムに選択する．

インターネットにおける感染 Internet スポットに存在する未感染状態のコンピュータは，確率 p_3 でワームに感染する．

ワームの感染動作をスポット指向モデルで記述すると，ワームはコンピュータを表すエージェントの内部属性の変化として取り扱われる．

5 シミュレーション

本章では，4 章において定式化した問題に対するシミュレーションを実施し，その結果を考察する．

5.1 シミュレーション条件

本稿におけるシミュレーションでは，Desktop と Mobile が接続されたネットワークにおいて，修正プログラムのリリースがないときにワームが伝染する場合を想定した．特に，実際にワーム伝染の事案発生時には，得られる情報は限定的であり，伝染しているワームの種類や使用しているポート等を特定することが困難であることから，対処方法はコンピュータのネットワークからの切断に限定される．本稿では，このような状況下でワームの被害を局限する方法を検討するため，次のような条件によるシミュレーションを実施した．

まず，ユーザはワームが発病しデータが破壊された「破壊」状態になったとき，ワームの感染を発見する．そして，以下の方法によりワーム感染を通報する．

1. 自分のコンピュータが接続されている LAN のユーザ全員に通報する．
2. ネットワーク管理者に通報し，ネットワーク管理者から全ユーザに警告が発せられる．

一方，対処方法として，以下の方法がある．

1. ユーザにより LAN からコンピュータを切り離す

2. WAN 全体を管理するネットワーク管理者により WAN から LAN 自体を切り離す.

これらの組み合わせから，シミュレーション条件を以下のように設定した.

Case1 対策なし

Case2 発病したコンピュータのユーザから接続している LAN のユーザのみに通報し，そのコンピュータを切断する.

Case3 発病したコンピュータのユーザから全てのユーザに通報し，全コンピュータを切断する.

Case4 発病したコンピュータのユーザからネットワーク管理者へ通報し，管理者は発病したコンピュータの存在する LAN のみを WAN から切断する.

Case5 発病したコンピュータのユーザからネットワーク管理者へ通報し，管理者は全ての LAN を WAN から切断する.

Table.2 にシミュレーション条件を，Table.3 にシミュレーションシナリオの概要を示す.

Table. 2 シミュレーション条件

LAN ノード数	100
ノード内のコンピュータ (エージェント) 数	Desktop:100, Mobile: 1(LAN1 のみ)
初期感染台数	1 (Mobile)
発病確率	$p_1 = 0.01$

Table. 3 シミュレーションシナリオ

ケース	通報先	切断箇所
1	なし	なし
2	同一 LAN 内の全コンピュータ	発症した LAN 内のコンピュータ
3	全てのコンピュータ	全てのコンピュータ
4	管理者	発症した LAN のノード
5	管理者	全ての LAN のノード

5.2 結果と考察

Fig.4 にシミュレーションの結果を示す．Fig.4(a) は Case1: ワームの伝染に対する対策を行わなかった場合であり，グラフ中の感染数が S 字カーブを描きながら，全コンピュータが感染する結果となる.

一方，Fig.4(b) は Case2 の場合を示している．発症したコンピュータは，同一 LAN 内のコンピュータへの伝染だけでなく，他ノードの LAN への伝染も試みる．そのため，LAN 内のコンピュータの接続を切り離しても，全てのノードからの切断が完了するまではワームの伝染が行われる.

Fig.4(c) は Case3 の場合を示している．発症したコンピュータのユーザが全てのユーザに通報し，全てのコンピュータを切断することから，伝染はほとんど行われない．しかしながら，全てのユーザに通報し切断することは，現実には非常に困難であるといえる.

Fig.4(d) は Case4 の場合を示している．発症したコンピュータの接続されている LAN のノードを逐次的に切断する場合，それ以前に，他のノードへのワームの伝染が起こっていることから，この対処方法ではほとんど効果はない.

Fig.4(e) は Case5 の場合を示している．発症したコンピュータのユーザから管理者に通報され，管理者が LAN の全ノードを WAN から切り離すことにより，感染の拡大を防いでいることが分かる.

これらのシミュレーションの結果，修正プログラムやアンチウイルスソフト等のワーム対策が適用できない状況下では，ワーム伝染事案の発生時において，発症した LAN のノードのみを切断するだけでは，感染の拡大を防ぐには不十分であることがわかる.

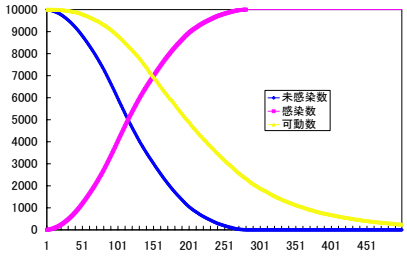
このことから，ワームの伝染を防ぐためには，発症を発見したユーザがすみやかにネットワーク管理者や事案対処要員に通報すること，または管理者等がワームの感染を発見できる環境を整備することが必要であり，管理者はワームの伝染を発見した場合，的確なノードの切断による被害局限を行うことが求められる.

6 むすび

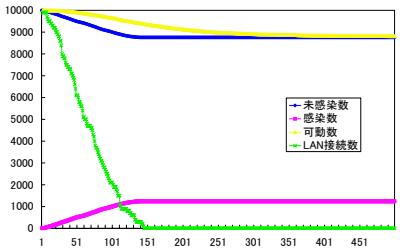
本稿では，ワームの伝染に対する運用上の対処方法を検討するため，エージェントベースアプローチによる拡散モデルを提案した．また，シミュレーションにより，ワームに感染したコンピュータの隔離方法による被害局限の効果を検討した．今後は，ユーザやシステム管理者等の行動のモデル化や，修正プログラム適用のケースを含めたシステム防護方法の検討を実施する予定である.

参考文献

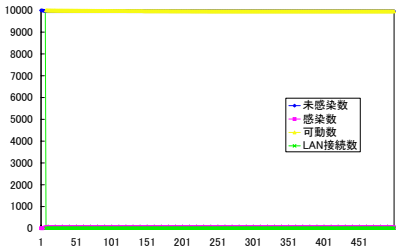
[1] 情報処理推進機構: コンピュータウイルス・不正アクセスの届出状況について（プレスリリース）.



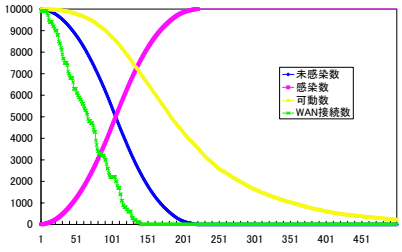
(a) Case1: 対策なし



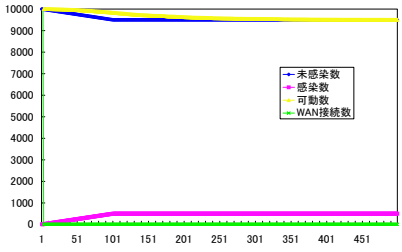
(b) Case2: 発症 LAN 内通報・切断



(c) Case3: 全体通報・切断



(d) Case4: 管理者通報・発症ノード切断



(e) Case5: 管理者通報・全ノード切断

Fig. 4 シミュレーション結果

http://www.ipa.go.jp/security/txt/2004/11outline.html

[2] 大和 哲: 新しいウイルス対策を考える (3) http://internet.watch.impress.co.jp/static/column/antivrs/2003/10/24/

[3] 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. 818–825 (1998).

[4] 千石 靖・服部 進実・岡本 栄司: 完全駆除までの期限を考慮したコンピュータウイルス駆除手法, 情報処理学会論文誌, Vol. 44, No. 1, pp. 106–113 (2003).

[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] 林 幸雄・箕浦 正人・松久保 潤: ネットワーク成長によるメール型ウイルスの再流行と重点的なハブの免疫化の効果, 情報処理学会論文誌 数理モデル化と応用, Vol. 44, No. SIG(TOM9), pp. 1234–1244, (2003).

[7] R.Axelrod: The Complexity of Cooperation, Prinston University Press, (1997) (『対立と協調の科学–エージェント・ベース・モデルによる複雑系の解明』, 寺野隆雄訳, ダイヤモンド社, (2003)).

[8] 寺野 隆雄: エージェント・ベース・モデリングへの招待, オペレーションズ・リサーチ, Vol. 49, No. 3, pp. 3–8 (2004).

[9] Hiroshi Deguchi, Hideki Tanuma and Tetsuo Shimizu: SOARS: Spot Oriented Agent Role Simulator - Design and Agent Based Dynamical System -, Proceedings of the Third International Workshop on Agent-based Approaches in Economic and Social Complex Systems (AESCS'04), pp. 49–56 (2004)

[10] 出口 弘・田沼 英樹・清水 哲男: SOARS: Spot Oriented Agent Role Simulator の設計と応用, 計測自動制御学会 第 32 回システム工学部会研究会資料, pp. 53–60 (2004).