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

2004－GN－53　(2)
2004／9／16

人間の行動を考慮したワーム感染シミュレーション

小畑 直裕*　川口 信隆*　塩澤 秀和†　重野 寛*　岡田 謙一*

年々ワームによるセキュリティ侵害が増加している. そういった状況の中ワームの脅威の認知度は高いが, ワームに対する対策を行っている所は少ない. これには様々な原因が考えられるが, 一つには感染した時の被害の実態が分かりにくいというのがある. そのため本稿ではマシンの稼働時間とパッチをあてるなどの人間の対策行動を新たに考慮した, ワームシミュレーションを行い, 被害予測に有用であることを述べる.

Worm Propagation Simulation Considering Human Action

Naohiro OBATA *　Nobutaka KAWAGUCHI*
Hidekazu SHIOZAWA†　Hiroshi SHIGENO*　Kenichi OKADA*

In this paper, we propose Internet worm propagation simulation considering “Human Action” and online hosts, to help considering damage caused by worms. Many people thinks worms are threat but most of them do not prevent attacks properly. So our simulation could be used to know how threatful worm is, and they’ll understand the need of blocking worms’ attack.

1　はじめに

近年, コンピュータ・ワーム (ウィルス) によるセキュリティ侵害が増加している.

ワームに対する対策として, OS のセキュリティホールに対するパッチをあてる, アンチウィルスソフトを導入するといったことが考えられるが, これらの対策を万全に行っている所は意外と少ない.

対策が不十分になってしまう要因として, 組織が従業員に対して提供するワームに関する情報が不十分である, またそれを活用できていないことや, 実際に組織内にワームが侵入してきた場合の被害の大きさが分かりにくいといったことがあげられる.

よって本研究では「ワームが侵入してきた場合の被害の程度がわかりにくい」という点に着目し, 組織やプロバイダ等の現実的にあり得るネットワーク環境を想定し, どのくらいの時間でどれくらいの被害が出るかという被害予測を行う. このシミュレーションでは「マシンの稼働時間帯」を新たなパラメータとして導入することで, より現実に近いモデルを生成する.

* 慶應義塾大学 理工学部 情報工学科
Department of Instrumentation(Information), Faculty of Science and Technology, Keio University

† 玉川大学工学部知能情報システム学科
Department of Intelligent Information Systems, Faculty of Engineering, Tamagawa University

本論文では，まず，2 章においてワームの概要、対策について述べる．そして，3 章で新たなパラメータを導入したシミュレーションモデルを提案し 4 章において，3 章で提案したシミュレーションモデルを実装して第 5 章で評価を行なう．第 6 章で関連研究について述べ、7 章を本論文のまとめとする.

2　ワームの概要とその対策

本章ではワームの概要と対策の現状について述べる。

2.1　ワームの概要

ワームとはサービスのセキュリティホールを利用し, ネットワークを介して自己増殖するプログラムである. ワームは以下の手順で感染・増殖する。

ワームはまず感染先となるターゲットを見つける. このときワームはスキャニングを行う. スキャニングとは感染先ホストを発見するために IP アドレスを調べる行為であり, シーケンシャルスキャンとランダムスキャンの 2 種類がある. シーケンシャルスキャンは、ある一定範囲のＩＰアドレスを順にスキャンしていく方法である。ランダムスキャンはランダムに生成されたＩＰアドレスに対してスキャンを行う。

次にワームはプロセスの奪取を行う. 奪取した後, ワームはターゲットマシンに自身をインストールし、再びスキャニングにより新たなターゲットを探す. 上

記の内容を繰り返すことによりワームは感染を広めていく.

2.2 ワームへの対策の現状

IPA が 2003 年に民間事業所、自治体合わせて 1812 の団体に行った調査によるとワームの存在を認知し脅威と感じている所は 95.7%でウィルスソフト対策状況は「9 割以上の PC に導入」(70.1%) と比較的高い数値を示している. しかしクライアントマシンに「常に最新のパッチを当てている」は 24.7%と低い. このようにワームに対する対策意識は低いと言える.

3 人間の行動を考慮したイントラネットワークにおけるワーム感染シミュレーション

本章では人間の行動を考慮したイントラネットワークにおけるワーム感染シミュレーションを提案する.

3.1 目的

本稿では, 現実の世界で利用されているようなネットワークを想定して, シミュレーションを行う.

CodeRed ワームなどを対象としたワームシミュレーションは数多く行われているが [1]、これらの研究では大規模ネットワーク、２４時間稼動するマシンを前提としている上に人間の行動を考慮していない.

本稿ではシミュレーションのパラメータとして新たに,
企業や大学などの組織、プロバイダなどの現実的なネットワークトポロジ, ＯＳなどのマシン属性、マシンが稼動する時間帯の考慮, 組織によって異なるワームに対する事前対策、事後対策の対応時間の違いを導入した. これらの項目を考慮することで、より現実的で実際に近いシミュレーションを実現する.

個々の内容について、以下に説明する.

3.2 ネットワークトポロジ, ホスト属性, 対策の有無

本提案では対称ネットワーク、プロバイダ型ネットワーク、組織型ネットワークの異なる３パターンのネットワークトポロジを想定してシミュレーションを行う. 3.2.1 以降で詳しく述べる.

ホスト属性とは, OS の種類や稼働時間帯のことである. 従来研究では OS の考慮はせずに全てのマシンに感染するという前提でシミュレーションを行っていたが, 実際は OS によって感染しないこともある. また, 今まではマシンの稼働時間帯を考慮した研究もなかった. だが現実にはクライアントマシンには起動している時間とそうでない時間帯があり, これもワームの感染速度を考える上で重要な要素と考え導入した.

本研究ではクライアントを「組織型」と「一般家庭型」に分け、さらに「組織型」クライアントは一定時間帯で稼動するもの、24 時間稼動し続けているものの２つに大きく分けてそれぞれで稼動時間帯を設定した. また、「一般家庭型」のクライアントに関しては 24 時間でホストが稼動している率を変化させ稼動しているホスト数を変化させることで、より現実に近いネットワークを設定する.

ワーム対策として人間が行うと考えられる行動は、大きく「事前対策」と「事後対策」に分けられる.

事前対策は主に、セキュリティホールが発見されたときにセキュリティパッチを当てるなどして、実際に攻撃を受ける前に攻撃対象を防御する方法である. 実際にセキュリティパッチを適応するか否か、また対応がどのくらいの早さで行われるかはワームの伝播速度に大きな影響を与える.

事後対策はワームに感染した後にとられる対策である. この事後対策については組織と個人では対応速度に大きな差がある.

本提案ではこのような事前対策、事後対策を考慮することでより現実に近いシミュレーションを実現する.

3.2.1 対称型ネットワーク

このネットワークは図 1 に示す通り、完全に対称型のネットワークである. 1 つのルータは同数のルータに接続されており、その下には同数のエンドホストが接続される. よって階層は全て同じである. このネットワークは末端が全て LAN でし、LAN 内のエンドホスト数は全て同じである.

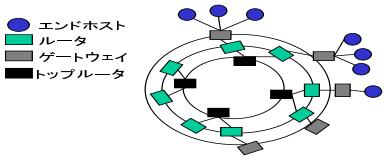

図 1: 対称ネットワーク

3.2.2 プロバイダ型ネットワーク

プロバイダを想定した階層型のネットワークがプロバイダ型ネットワークである. 末端は企業が利用している場合と一般家庭の場合を想定した.

3.2.3 組織型ネットワーク

このネットワークは、企業や大学などの 一般的な組織のネットワークを想定して構成したネットワー

クである. 最上位のルータを並列におき, 末端は全て LAN で構成されているが, LAN 内のエンドホスト数は異なり, LAN の規模は大小異なるものが複数あるという設定とした.

4 実装

本章では前章で提案したシミュレーションの実装について述べる.

4.1 実装環境

本シミュレーションの実装環境は以下の通りである.

実装環境 JDK1.4.2
オペレーティングシステム Windows XP
CPU Pentium4 3GHz
RAM 2GByte

4.2 ネットワークモデル

今回シミュレーションで使用したネットワークモデルは以下の通りである. またここでホスト属性の定義を以下に示す.

Home Client 家庭のマシンを想定したクライアント
Organization Client 企業のマシンを想定したクライアント
Lab Client 研究室のマシンを想定したクライアント
Univ Client 組織の管轄で管理されていることを想定したクライアント
Clasroom Client 大学の教室, または会議室にモバイルマシンをネットワークに接続していると想定したクライアント

また, OS の設定は 42%の割合で WindowsXP, 以下 37.5%Windows2000, 20.5%を WindowsMe とした.

4.2.1 対称ネットワーク

前章で述べた形状の対称ネットワークを設計した.

- トップルータの数 : 4 台
- 各トップルータには 2 台ずつの中間ルータを設置、その中間ルータの下に末端の LAN のゲートウェイを設置
- 末端 LAN のエンドホスト数 : 16000 台
- 末端 LAN のネットワークスピード 10Mbps

エンドホストを 3 割の割合で Organization Client, 他の 7 割を Home Client にランダムに決定した.

4.2.2 プロバイダ型ネットワーク

設計したプロバイダ型ネットワークを図 2 に示す.

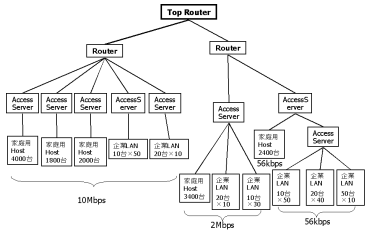

図 2: 設計したプロバイダ型ネットワーク

- トップルータは 1 台
- その下にルータが 2 台あり, それぞれ 5 台, 2 台のアクセスサーバを持つ.
- アクセスサーバは家庭用ホストが接続されているものと, 企業の LAN が接続しているものがある.
- 末端のホストの合計は 16600 台で内 13600 台が家庭用ホスト, 残りが企業 LAN のクライアントとした.
- 末端のスピードは 10Mpbs が 8500 台, 2Mbps が 3900 台, 56kbps が 4200 台とした.

LAN として構築されているネットワークのホストを Organization Client, アクセスサーバに直接接続されているホストを Home Client とした.

4.2.3 組織型ネットワーク

今回の実装では本大学のネットワークトポロジを参考にして組織型ネットワークを設計した. 図 3 に示されるように 12 のネットワークの上位ルータが並列に接続されている. それぞれのネットワークの

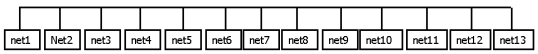

図 3: 設計した組織型ネットワーク

詳細は以下のとおりである. また, エンドホストの総数は 15450 台とした.

[**net1**] 30 台× 30, 60 台× 8, 400 台× 3, 200 台× 3, 120 台× 1, 40 台× 36 の計 4740 台
[**net2**] 60 台× 38, 400 台× 2, 200 台× 1 の計 3280 台
[**net3**] 200 台× 2, 40 台× 3, 60 台× 1, 100 台× 9 の計 1480 台
[**net4**] 200 台× 2, 40 台× 1, 60 台× 1, 100 台× 1 の計 600 台
[**net5**] 200 台× 2, 60 台× 1, 100 台× 8, 260 台× 1, の計 1520 台
[**net6**] 60 台× 2, 120 台× 1, 220 台× 1 の計 480 台
[**net7**] 60 台× 1, 80 台× 1, 120 台× 1, 220 台× 1 の計 500 台

[**net8**] 60 台× 1, 30 台× 1, 160 台× 1, 200 台× 1 の計 450 台
[**net9**] 60 台× 2, 120 台× 1, 220 台× 1 の計 480 台
[**net10**] 60 台× 2, 120 台× 1, 220 台× 1 の計 480 台
[**net11**] 60 台× 1, 80 台× 1, 120 台× 1, 220 台× 1 の計 500 台
[**net12**] 60 台× 1, 40 台× 1, 160 台× 1, 200 台× 1 の計 460 台
[**net13**] 60 台× 2, 120 台× 1, 220 台× 1 の計 480 台

ホスト属性は以下のように設定した.

- net1, net2 の LAN でエンドホストの総数が 100 台以下のネットワークのクライアントは Lab Client とした
- net3〜net13 の 100 台以下のネットワークのクライアントは Organization Client とした
- net1, net3, net4, net5 のエンドホストが 100 台以上のネットワークのクライアントは Univ Client とした
- net2, net6〜net13 のエンドホスト 100 台以上のネットワークのクライアントは Classroom Client とした

4.3 稼働時間帯の設定

以下のような稼働時間帯を設定した.

Home Client Home Client の稼働時間帯はホストの時間帯・稼働率をそれぞれ以下のとおりに設定し, 2 時間毎にクライアントの中からランダムに稼動するホストを決定した.

表 1: Home Client の稼働時間

時間	稼働率	時間	稼働率
0-2	0.3	12-14	0.28
2-4	0.09	14-16	0.32
4-6	0.08	16-18	0.31
6-8	0.17	18-20	0.38
8-10	0.28	20-22	0.58
10-12	0.36	22-24	0.62

Organization Client 企業のクライアントを想定しているため, 稼働時間帯を 9 ー 18 時とした.
Lab Client 研究室のクライアントを想定しているため, 稼働時間を 24 時間とした.
Univ Client 稼働時間を 9 ー 20 時とした.
Classroom Client 教室, 会議室で使用されるクライアントを想定したため, 表 2 のような稼働率を設定し, 1 時間毎にクライアントの中からランダムに稼働するホストを決定した.

4.4 事前対策, 事後対策の対応時間の決定

ホスト属性ごとの事前対策の対応時間設定を図 4, 事後対策の対応時間設定を図 5 に示す. これは [2]

表 2: Classroom Client の稼働時間

時間	稼働率	時間	稼働率
9-11	0.3	15-17	0.5
11-13	0.4	17-19	0.3
13-15	0.6	19-9	0

などを参考に設定した. Classroom Client はユーザがモバイル PC を持ち込んだ形を想定しているため, 事前対策, 事後対策は行なわれないものとする.

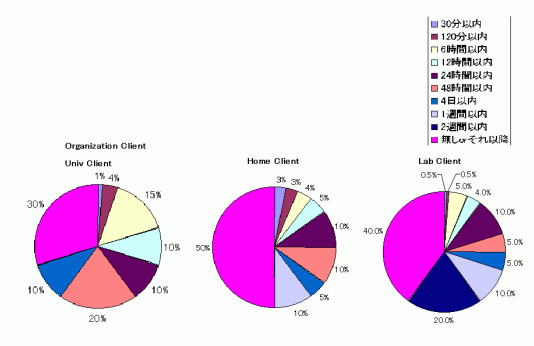

図 4: 事前対策の対応時間設定

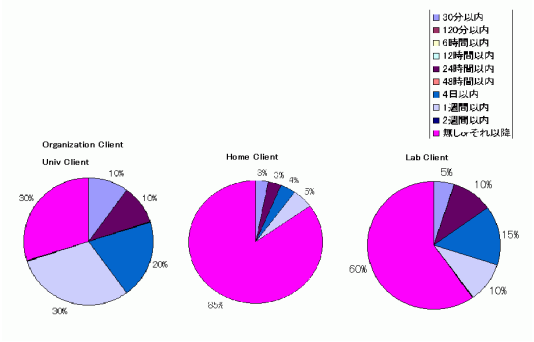

図 5: 事後対策の対応時間設定

4.5 ワームの活動モデル

今回のシミュレーションでモデルとしたワームは Blaster である. このワームは Windows 2000 または Windows XP を攻撃対象とし, 1/5 の確率で Windows 2000 が攻撃され, 4/5 の確率で Windows XP が攻撃される.

ランダムスキャンを行う確率が 40%, シーケンシャルスキャンを行う確率が 60% であり, このような感染活動を繰り返し行う.

今回のシミュレーションでは上述のような探索活

動, 感染活動を行なうワームのクラスを作成し, 実行させた.

5 シミュレーションの評価

5.1 シミュレーション条件項目

以下のような条件においてシミュレーションを実行した.

(1) 稼働時間を考慮せず, 事前事後対策を行わない場合の感染台数

(2) 稼働時間を考慮し, 事前事後対策を行わない場合の感染台数

(3) 稼働時間を考慮せず, 事前対策と事後対策を考慮した場合の感染台数

(4) 稼働時間を考慮し, 事前対策と事後対策を考慮した場合の感染台数

稼働時間を考慮しない場合、全てのホストは 24 時間稼動するものとし、事前事後対策を行わない場合、ワームに対して何の対処も行わないものとする. 次節で、それぞれの結果について示す.

5.2 シミュレーション結果

5.2.1 稼働時間を考慮せず、事前事後対策を行わない場合

まず稼働時間を考慮せず、事前事後対策を行わない場合の感染台数の推移を図 6 に示す. ここでグラフにある「org100」とはエンドホスト数 100 台の LAN の 1 台がワームに感染した場合の結果を意味する. org200, provider20, provider2000 も同様である.

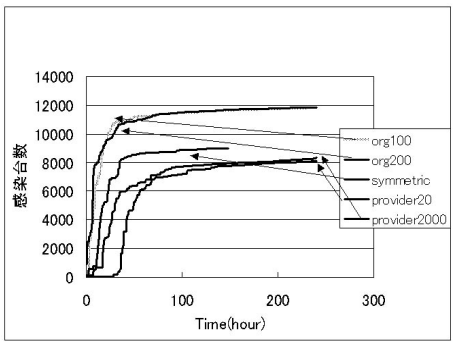

図 6: 稼働時間考慮なし, 対策なし

グラフから 3 パターンのネットワークの中では組織型ネットワークが感染のスピードが早いという結果が見られる. これは組織型ネットワークに 100 台以上のクライアントを持つ LAN が存在し, その LAN にワームが侵入してきてワームが IP アドレスをシーケンシャルにスキャンして感染活動を行なったからであるということが考えられる. また, プロバイダ型ネットワークが対称型や組織型ネットワークと比較して感染台数が少ないのはプロバイダ型ネットワークが 10 台, 20 台で構成される LAN の数が多かったことにあると考えられる.

5.2.2 稼働時間を考慮して、事前事後対策を行わない場合

次に稼働時間帯のみを考慮してシミュレーションした結果を図 7 に示す. 稼働時間帯を考慮していない場合と比較して, よりネットワークの形状による感染台数の違いが顕著に現れている. プロバイダ型ネットワークは, 感染台数が急激に増加し出すまでに 100 時間程度かかっているのが分かる. 組織型のネットワークの増加の仕方が非常に大きいのはワームによって探索されたホストが, 24 時間稼働している Lab Client であったということが大きな要因であると考えられる.

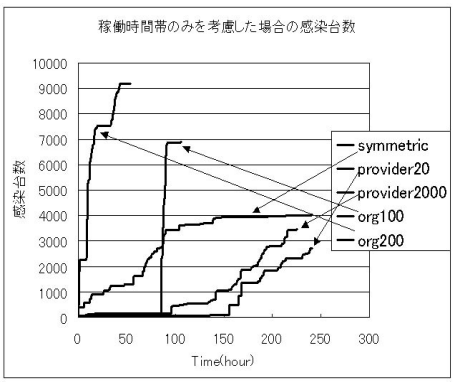

図 7: 稼働時間考慮あり, 対策なし

稼働時間を考慮しない場合とする場合との比較を図 8 に示す. 図 8 より, 稼働時間を考慮すると, 感染台数が増加し始めるまでにある程度時間がかかること, 感染速度（感染ホストの増加の仕方）がネットワーク形状に大きく依存することが分かる. ただ, 対称型ネットワークは稼働時間を考慮しても増加の仕方は変わらなかった.

5.2.3 稼働時間を考慮せず、事前対策事後対策を行う場合

稼働時間を考慮せず, 事前対策, 事後対策を前章で設定した時間に適用した結果を図 9 に示す. どのネットワークにおいても, 最初にワーム対策が行なわれ始める 24 時間後を境に, 対策を行った場合のグラフは減少を始める.

対称型ネットワークと組織型ネットワークは感染台数の減少が急激であるのに対し, プロバイダ型は

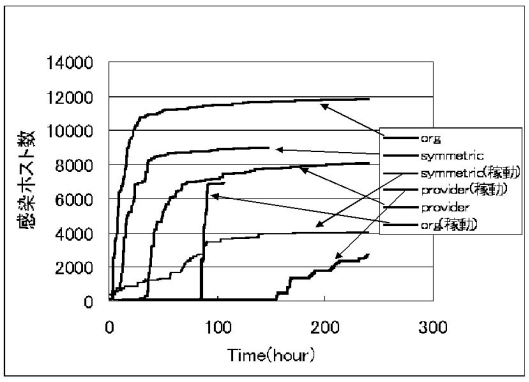

図 8: 稼働時間考慮ありとなしでの比較

そうではない．これはプロバイダ型は 10〜20 台の小規模な LAN が多く, また他の二つのネットワークは 100 台以上の大規模な LAN で構成されているという違いが原因である．すなわち対策をしなかった時に, 感染したであろうマシンの台数がプロバイダ型の場合は少ないため, 一度の対策により減少させられる感染数は少ないと言える．

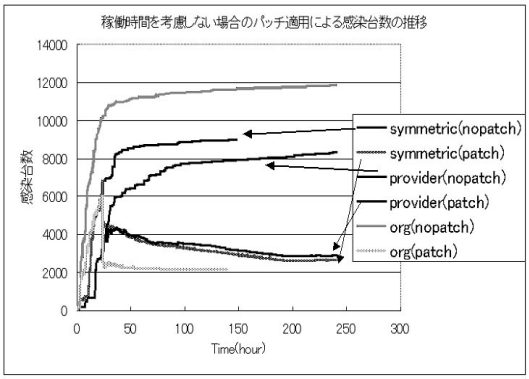

図 9: 稼働時間考慮なし，　対策あり

5.2.4　稼働時間を考慮し、事前対策事後対策を行う場合

稼働時間帯を考慮し, さらに事前対策, 事後対策を 4.4 で設定した時間に適用したシミュレーション結果が図 10 である．稼働時間を考慮しない場合は最初の感染から 150 時間後あたりを境に感染が収束するのに対し, 考慮した場合では感染スピードは圧倒的に遅いものの増加していく傾向にあることが見られた．

また, ネットワークの形状によって減少の仕方, 収束の仕方が全く違うのも見受けられる．事前対策, 事後対策を行なうことによる効果がネットワークの形状によって違いが出る, ということがこれにより分かる．

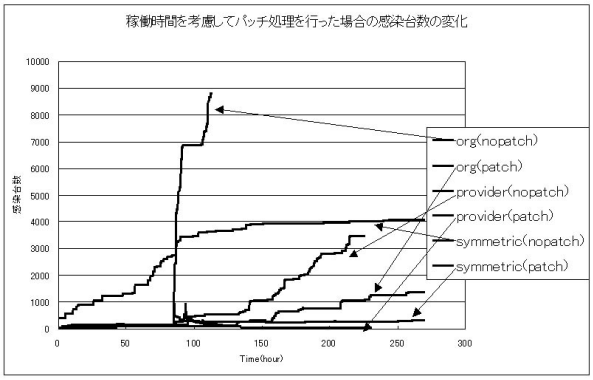

図 10: 稼働時間考慮あり, 対策あり

6　関連研究

数学的モデルを用いたワーム拡散モデルは数多く提案されている [1] [3]. Zescheng Chen らは離散時間モデルを用いたワームシミュレーションを行っており他のマシンへのアクセス開始にかかるタイムラグを導入することで、より現実的な拡散モデルを実現している．

7　まとめ

本稿ではワームによる被害の程度が分かりにくいことにより対策が不充分であることを考慮し, マシンの稼働時間や事前事後対策等の人間の行為もパラメータとして加え, 従来の研究より現実に近い状況を想定してシミュレーションを行った．

その結果からネットワークの形状, 稼働時間帯の考慮, によって感染推移が大きく異なることなど、従来のワームシミュレーションでは得られなかった見解が得られ, 被害予測を行う上で充分有用であると言える．

参考文献

[1] Zesheng Chen, Lixin Gao, Kevin Kwiat: Modeling the Spread of Active Worms, *IEEE INFOCOM* (2003).

[2] W32/MSBlaster 及び W32/Welchi ウイルス被害に関する企業アンケート調査の結果について http:www.ipa.go.jp/ipa/press/15FY/20030918.html , Sep 2003.

[3] David Moore, Vern Pxson, Stefan Savage, Colleen Shannon, Stuart Staniford, Nicholas Weaver: Inside the slammer worm, *IEEE Magazine of Security and Privacy, page.33-39* (July/August 2003).