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

2004－ＣＳＥＣ－26　(31)
2004／7／21

サイトレベルプロファイリングを用いたワームの感染規模推定方法の提案

小　泉　芳[1]　小池　英樹[2]　安村　通晃[3]

慶應義塾大学 大学院政策・メディア研究科[1]
電気通信大学 大学院情報システム学研究科[2]
慶應義塾大学 環境情報学部[3]

ワームの感染規模を推定するには，観測点へのスキャン (標本) からインターネット全体での感染台数 (母集団) を計測する必要がある．先行研究では，ワームのランダムスキャンの特性から推定する方法が報告されているが，ローカルスキャンを含むワームに対しては充分な検討がなされていない．本研究では，ローカルスキャンを含むワームの特徴抽出方法としてサイトレベルプロファイリングを用いたワームの感染規模推定方法を提案する．これは，ワームのターゲット選択単位ごとに感染規模の重みづけをする方法である．本論文では，提案手法を用いた，W32.Welchia.Worm 及び W32.Sasser.D.Worm の解析結果について報告する．

A Proposal of Estimation Method of Magnitude of Worm Infection by using Site Level Profiling

KANBA KOIZUMI[1] , HIDEKI KOIKE[2]
and MICHIAKI YASUMURA[3]

Graduate School of Media and Governance, Keio University[1]
Graduate School of Information Systems, University of Electro-Communications[2]
Faculty of Environmental Information, Keio University[3]

It is neccesary to estimate the magnitude of worm infection from the log of scanning packets that come form infected hosts to observation points. In a previous research, an estimation method by feature extraction of random scanning is proposed. But such a method is not applicable to a worm that includes local scanning. In this paper, we propose an estimation method of the magnitude of worm by using site level profiling. Site level profiling is a feature extraction method of worms that includes local scanning. With the proposed method, we report the analysis results for W32.Welchia.Worm and W32.Sasser.D.Worm.

1. はじめに

近年、コンピュータウイルスが多発しており、社会問題となっている．ウイルスはメールの添付ファイルの実行などにより広まるウイルス (メール型ウイルス) と，セキュリティホールを狙い自己増殖するウイルス (以下，ワーム) が主流である．本研究では，自己増殖するタイプのウイルス「ワーム」に注目し，その定量的な評価手法の確立を目指している．ワームの流行性の評価方法として２つの視点がある．観測点ごとの視点と，インターネット全体による視点である．本論文では，インターネット全体からの視点によるワームの流行性評価手法について記述する．

インターネット全体でのワームの流行性の評価には，評価尺度として，一般にワームの感染規模が用いられる．感染規模の計測方法として，２つの考え方がある．１つ目は被害ホストの報告を収集することであり，日本においては IPA，世界では CERT/CC，アンチウイルスベンダーなどが行なっているが，ユーザの報告義務はないことなどから正確な測定は困難な作業である．２つ目の方法は，ワームを監視する観測点を設け，観測点への感染行為 (攻撃やスキャン，以下まとめてスキャンと呼ぶ) を標本抽出し，母集団であるインターネット全体でのワームの感染規模を推定するものである．本研究は，後者の立場で，観測点に対する感染行為から，感染規模を推定する方法を提案する．先行研究では，ワームのランダムスキャンというターゲット選

表 1 ワームのターゲット選択方法

	スキャン方法	切り替え方法
CodeRed	ランダム	-
SQL Worm	ランダム	-
Welchia	ランダム，ローカル	連続型
Sasser	ランダム，ローカル	並行型

択方法 (Target Selection Mechanism) の特徴抽出した方法が提案されている．しかしこれらの方法は，ランダムスキャン以外のターゲット選択方法を含むワームには一概に適用できない．本研究では，ローカルスキャンという感染したワームが近傍の IP アドレスに優先的に感染を試みる特徴を含むワームを対象とした感染規模の推定方法を考案した．提案手法は，ワームのターゲット選択単位からの特徴抽出法としてサイトレベルプロファイリングをワームの感染規模推定方法に応用するものである．サイトとは IP アドレス上位 16 ビットごとの集合であり，ワームのローカルスキャンのターゲット選択単位である．

以下の構成は，2 章で先行研究，3 章で提案手法，4 章で解析例，5 章で考察とまとめである．

2. 先行研究

この章では，ワームのターゲット選択方法と感染規模の推定方法に関する先行研究について述べる．

2.1 ターゲット選択方法

感染したワームが次のターゲットを選ぶさいに，各ワームごとに特徴が異る．例えば，IP アドレスをランダムに選ぶランダムスキャンや，感染したホストの上位アドレスに固定して下位アドレスを変更するローカルプレファレンススキャン (以下，ローカルスキャン) などが代表的である．

ワームにより，これらのスキャン方式の組み合わせ方で，特徴づけが行なわれる．代表的なワームのスキャンの組み合わせ方法を表 1 に示す．スキャン方法において，ローカルスキャンを含むかどうかにより大きく分類ができる．本研究の対象はローカルスキャンを含むワームが対象である．またローカルスキャンを含む場合に，ランダムスキャンとローカルスキャンの比率においても更に特徴が別れる．連続型とは，一定期間ローカルスキャンをした後に，一定期間ランダムスキャンをするタイプである．また並行型とは，ランダムスキャンとローカルスキャンを一回ごとに切り替えながらスキャンをするタイプである．

多くの研究者がさまざまなスキャン方法の組み合わせをモデル化することで，シミュレーション実験を行なっており，これらの結果，スキャン方法により感染速度に影響を与えることが明らかにされている [2)3)]．

2.2 感染規模の推定

Staniford は，ワームの感染規模の正確な近似には，多くの IP アドレスが必要であると報告している [3)]．また，Moore の研究では，CodeRed ワームの感染のモデル化を試みたところ，観測されたワームの IP アドレスの種類数ではなく，ワームのスキャン数が全体での感染規模に近似したと報告している [4)]．

Zou は，このワームの観測数が，実際の感染規模より過少評価になっている問題に対して 2 つの対策を提案している．どちらもランダムスキャンの特徴に注目したものであり，1 つ目は観測点での単位時間当りのスキャン数から確率的にネットワーク全体での感染規模を求める方法である．2 つ目は，観測されたワームの累積数に対して，ワームが感染してから観測点にスキャンが届くまでの時間の遅延を考慮にいれて，感染規模のバイアスを上乗せする方法である．Zou は，この方式により，ランダムスキャン型の CodeRed と SQL ワーム (Slammer) に対するシミュレーション実験結果を報告している [1)]．また Zou は，ローカルスキャンを含む W32.Blaster.Worm (以降，Blaster) に対しても報告しており，ローカルスキャンを行なう Blaster への対策として，まとまった大規模な IP アドレス範囲ではなく，監視範囲を断片化させてさまざまな環境に観測点を設ける必要があると報告している [2)]．Zou の方法は，いづれも多くの監視用 IP アドレスが必要であり，正確な近似のために 2 の 20 から 24 乗個もの監視用 IP 空間が必要であるとしている．またランダムスキャン以外のワームに対処するためには，インターネット上のさまざまな場所を監視する必要があるとしており，推定に必要なデータの入手は困難である．

提案方法は，従来研究では充分に議論されていなかった，ローカルスキャンを含むワームの特徴抽出を行ない，より小規模の監視用 IP アドレスでワームの感染規模を推定する方法を考案したものである．提案方法の詳細を次章以降で述べる．

3. 提案方法

本章では，当初ワームの 2 つのスキャン方法の時間的比較を行ない特徴抽出を行なう．次に，その時間的特徴から導出した提案手法について説明する．

3.1 スキャン方法の比較

ここでは，ローカルスキャンとランダムスキャンを両方行なうワームの特徴抽出として，両方法の時間的な特徴の比較を行う．比較したのは次の 2 項目である．

(1) ランダムスキャン時間

ワームのランダムスキャンが、少なくとも一回観測点に届くまでの時間 T_1．この場合，観測点とワームが感染したサイトは異っている前提であり，またランダムスキャン空間は 2^{32} とする．

(2) ローカルスキャン時間

ワームがローカルスキャンにより、ローカル IP 空間をすべて選択し尽くすまでの時間 T_2．本論文では指

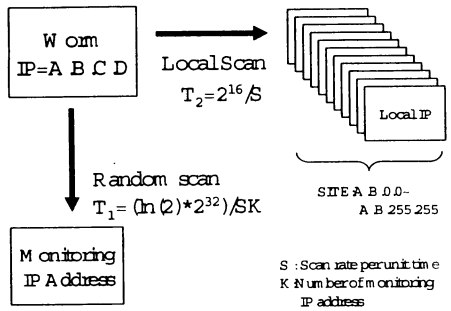

図 1 比較項目

定がない限り, ローカルスキャンとは, ワームが感染したIPアドレスの上位16ビットを固定して下位16ビットをランダムもしくは連続的に選択する方法とし, ローカルIP空間とは,2^{16} とする. このようにIPアドレス上位16ビットごとの集合をサイトと呼ぶことにする.

3.2 比較方法の説明

図 1 に比較の概要を示す. ローカルスキャンの時間見積もりは, 単純化のためサイト内の宛先IPを連続的に選択する場合を考える. この場合, 下位16ビットの0.0から255.255までの $2^{16} = 65536$ 個のIP数を全部選択するまでの所用時間 T_2=(ローカルIP空間÷単位時間のローカルスキャン数) である.

次に, ランダムスキャンの時間見積もりを行なうために用いる誕生日定理 (Birthday Paradox) について述べる [6].

定理 1 ある人が253人に会えば, 自分と同じ誕生日 (月日) の人間に少なくとも一人出会う確率が50%を超える.

この定理の導出過程を用いて, ワームのランダムスキャンに応用した方法を説明する. 観測点のIP数を k 個とする.

- ワームの一回のランダムスキャンが観測点に当る確率：$k/2^{32}$.
- ワームの一回のランダムスキャンが観測点に当らない確率：$1 - k/2^{32}$.
- ワームの m 回のランダムスキャンが観測点に当らない確率：$(1 - k/2^{32})^m$.
- ワームの m 回のランダムスキャンが、少なくとも一回観測点に当たる確率:

$$P[m,k] = 1 - (1 - k/2^{32})^m \quad (1)$$

また, 一般に以下の不等式が成り立つ。

$$(1-x) \leqq e^{-x} \text{ただし、} x >= 0 \quad (2)$$

ここで少くも一回観測点にランダムスキャンが当る確率：P(m,k) = 0.5 (50%) とすると、式 (1),(2) より以下が成り立つ.

$$0.5 = 1 - e^{-km/2^{32}}$$

$$e^{-km/2^{32}} = 1/2$$

$$m = 2^{32} \times ln(2)/k$$

この m の値が、少くとも一回観測点にランダムスキャンが届くまでの必要スキャン数であり、観測点のIP数:k により定まる。単位時間 t におけるワームのスキャン回数を s 回とすると $m = st$(スキャン数=単位時間のスキャン数×時間) の関係より所用時間

$$T_1 = ln(2) \times 2^{32}/sk \quad (3)$$

が求まる.

3.3 特徴抽出

ランダムスキャン, ローカルスキャン (上位8ビット固定), ローカルスキャン (上位16ビット固定) の比率としては、過去のウイルスの比率では (5 : 2.5 : 2.5), (3.3 : 3.3 : 3.3), (5 : 5 : 0) が多く用いられている [8]. 本研究でもこの3つの比率を対象として議論を行なう.

図 2 において、単位時間当りのスキャン数が10回の場合のランダムスキャンとローカルスキャンの所用時間を表示する。横軸は観測点のIP数の指数部であり、縦軸は時間であり, ランダムスキャンが観測点に少くとも一回届くまでの所用時間 T_1 とローカルスキャンがローカルIPを全て選択する時間 T_2 を表す。各線は, 比率ごとのスキャン方法を表し, 例えば, Random 5 はランダムスキャンで比率が5の場合, Local 5 は上位16ビット固定ローカルスキャンで比率5の場合である. ローカルスキャンは上位16ビット固定のみを対象としている.

各比率でのローカルスキャンの所用時間 T_2 は観測点の大きさによらず一定である。また, ランダムスキャンの所用時間 T_1 は、観測点のIP数:k の関数であり, k が小さくなる程、所用時間 T_1 が大きくなる.

ここで注目すべきは, ローカルスキャンがサイトのIPを全部選択する時間とランダムスキャンが観測点に届くまでの相対的な早さである. もし、観測点にランダムスキャンが届くまでに, ローカルスキャンによるローカルIP空間 (2^{16} 個) の選択がすべて終えているのであれば, そのローカルIP空間でオンラインになっている脆弱なホストはすべて感染していることになる.

この見積もりは, ワームの感染台数や単位時間当りのスキャン数が増えようともランダムスキャンとローカルスキャンの相対的な比率は変らないため, ワームの感染台数やスキャン数は見積もり時間の相対的な早さに影響はない. 影響があるのはローカルスキャンとランダムスキャンの比率である.

以上より, ローカルスキャンを含むワームでは以下の特徴がある.

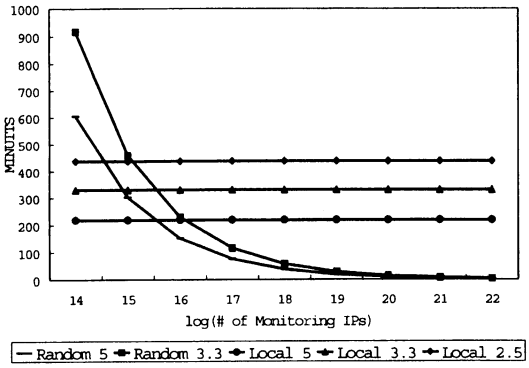

図 2 ランダムスキャンとローカルスキャンの時間比較

特徴 1 観測点の IP 数の指数部が 14 以下 (IP 数が 16384 以下) であれば，ワームのランダムスキャンが観測点に届くまでに，そのワームのローカルスキャンによりそのサイトは全部選択し終えている．

特徴 1 は，ランダムスキャンとローカルスキャンを切り替えながらスキャンをする並行型のワームの場合は，観測点の IP 数 $k < 2^{14}$ が成立の条件となる．また，ローカルスキャンによりサイトを全て攻撃した後にランダムスキャンを行なう連続型のワームの場合は，この特徴は観測点の大きさによらずに一般的に成り立つ．

3.4 感染規模推定方法

この節では、提案方法であるワームの感染規模推定方法について述べる．提案方法は前項で示したランダムスキャンとローカルスキャンの時間的な特徴を利用する．推定方法の概略としては，各サイトごとの脆弱ホスト数を見積もることで，観測点に届くワームのスキャンに各サイトごとの脆弱ホスト数を重みづけして上乗せし，インターネット全体でのワームの感染規模を近似する方法である．

以下に提案方法であるワームの感染規模を推定するアルゴリズムを C 言語風の擬似コードで示す．

```
weigt[SITE]=each_weight_of_site;
new_site[SITE]=YES;
magnitude=0;
NEXT_SCAN=FIRST_SCAN;

  LOOP:
SCAN=NEXT_SCAN;
if(SCAN=LAST)
goto END;
}

  if(new_site[SITE_OF_SCAN] == YES){
magnitude += weight[SITE_OF_SCAN];
new_site[SITE_OF_SCAN]=NO;
goto LOOP;
}

  else{goto LOOP;}
END:
}
```

表 2 スタティックプロファイリングの例

サイト名	IP 使用数	重み (IP 使用数×脆弱率)
4.1	65536	163
4.2	65536	163

特徴としては，サイトごとの最初のワームのスキャンが出現したときにサイトの重みを上乗せする方法であり，以降既出のサイトからのスキャンは累積の対象としない．

3.5 サイトレベルプロファイリング

提案手法では各サイトごとの脆弱ホスト数を見積もる必要がある．本手法はサイトレベルプロファイリングをワームの感染規模推定へ応用している．サイトレベルプロファイリングはワームのターゲット選択単位からみた特徴抽出方法である．脆弱ホスト数を見積もる場合のサイトレベルプロファイリングには次の 2 通りを候補にしている．

(1) スタティックプロファイリング

各環境での脆弱率 (単位 IP 数当りの脆弱なホスト数の割合) は一定であるとし，サイトの脆弱ホスト数= (各サイトの IP 使用数) × (脆弱率) とする．IP 使用数は，各サイトにおいて IP 割り当てが行なわれている IP 数のことである．これは，各国や組織に割り当てられている IP 数という意味で，実際にホストが稼動しているという意味ではない．一般に脆弱率は，ワームが狙うセキュリティホールごとに異る．4 章でクライアントタイプの WindowsOS の脆弱率を 0.0025(全体の 2.5%) と設定している．この方式では，脆弱ホスト数は IP 割り当て状態が変更にならない限り変化はない．なお，IP 割り当て数は Geo-IP[7] を用いてすべてのサイトの IP 割り当て状況を計測した．プロファイリング結果の例を表 **2** に示す．

(2) ダイナミックプロファイリング

各サイトごとのワームの感染率により脆弱ホスト数を近似する方法である．過去にワームに感染した場合と同程度の規模の感染が起きるという想定に基づくものである．この方式は時間の経過により動的に更新していくものである．本論文では，脆弱ホスト数として，各サイトごとの Welchia ワームの感染台数により適用し，2003 年 8 月から 12 月までのデータにより近似した．プロファイリング結果の例を表 **3** に示す．

3.6 提案方法のまとめ

以上より，ローカルスキャンとランダムスキャンの

表 3 ダイナミックプロファイリングの例

サイト名	重み (ウイルス感染数)
4. 1	1
4. 2	36

時間的特徴から, 観測点にランダムスキャンが届いた場合に, 各サイトごとの重みを上乗せすることにより, ワームの感染規模推定方法について述べた. また, 各サイトごとの脆弱ホスト数の近似方法として,2 種類のサイトレベルプロファリングについて説明した. 次章では, 本手法を用いて実際のワームの解析例を説明する.

4. 解 析 例

本章では提案手法を用いて,W32.Welchia.Worm および W32.Sasser.Worm の感染規模の解析結果について説明する.

4.1 観 測 点

観測点は以下の 4 つのネットワークである. 各観測点に不正検知型 NIDS "snort[5]" を設置し, そのアラート情報を統合して解析を実施した. IP 数の合計は $595 < 2^{14}$ であり, これは特徴 1 が成り立つ条件を充たす.

- SOHO 環境 1(監視 IP アドレス 5 個).
- SOHO 環境 2(監視 IP アドレス 15 個).
- キャンパス環境 1(監視 IP アドレス 63 個).
- キャンパス環境 2(監視 IP アドレス 512 個).

4.2 W32.Welchia.Worm

W32.Welchia.Worm (以降 : Welchia) は,2003 年 8 月 16 日より観測され始めたワームであり,Windows の脆弱性をついて感染をする [9]. Welchia はポート 135 へ攻撃をする前に, ICMP によるスキャンをすることが知られている. snort のアラートファイルには "ICMP PING CyberKit 2.2" としてログが生成される.

4.2.1 ターゲット選択方法 : Welchia

感染ホストの IP アドレスを A.B.C.D と表した場合の,Welchia のターゲット選択方法は以下の 4 ラウンドに分けられている.

- 上位 16 ビット (A.B) を固定し下位 16 ビット (C.D) を 0.0 から 255.255 まで連続的に変更する.
- 上位 16 ビットを (A.B-1)〜(A.B+3) まで変更して固定し, 下位 (C.D) を連続的に変更する.
- 上位 8 ビット (A) を選び固定し, 下位 24 ビット (B.C.D) をランダムに変える (ただし、A はワームの持つ表から選ばれる).
- A.B.C.D をランダムに選ぶ (ただし、A はワームの持つ表から選ばれる).

Welchia のローカルスキャンは連続型であり, 特徴 1 は傾向としてに成り立つ.

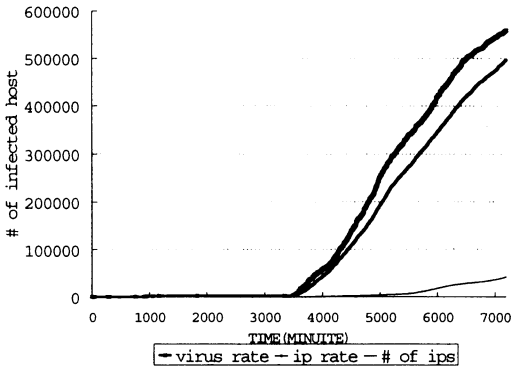

図 3 Welchia worm

4.2.2 感染規模 : Welchia

Welchia 発生からの時系列的な、解析結果を図 3 に示す。横軸が時間 (分) であり、縦軸は感染台数である。各線は IP アドレスの種類数 (# of ips), スタティックプロファイリング (ip rate) およびダイナミックプロファイリング (virus rate) による感染規模の推定値である。本手法を適用させた結果として, 感染規模は約 5 日間で 50 から 55 万台という結果である。一般に Welchia などが利用する連続型のローカルスキャンは感染速度がそれほど早くないことがシミュレーションで明らかにされている [2]. この結果より, Welchia はワームが出現してから指数関数的な増加をする (伝染閾値を超える) までに数日の時間がかかったと推測することができる. なお推定結果の実際の近似の度合いなどの精度についてはまだ明らかではない.

4.3 W32.Sasser.D.Worm

W32.Sasser.D.Worm (以降 : Sasser.D) は,2004 年 5 月 3 日より観測され始めたワームであり,Windows の脆弱性をついて感染をする [10]. これは、同じ脆弱性を攻撃する W32.Sasser.Worm の亜種である.Sasser.D ワームはポート 445 へ攻撃をする前に, ICMP によるスキャンをすることが知られている. snort のアラートファイルには "ICMP PING NMAP" としてログが生成される.

4.3.1 ターゲット選択方法 : Sasser

感染ホストの IP アドレスを A.B.C.D と表した場合の,Welchia のターゲット選択方法は以下の 3 通りとされる.

- 上位 16 ビット (A.B) を固定し下位 16 ビット (C.D) をランダムに変更する.
- 上位 8 ビット (A) を固定し下位 24 ビット (C.D) をランダムに変更する.
- 32 ビット (A.B.C.D) をランダムに変更する.

各選択方法の比率は (ランダムスキャン, 上位 8 ビット固定ローカルスキャン, 16 ビット固定ローカルスキャン) = (5 : 2.5 : 2.5) である. 観測点の IP 数の

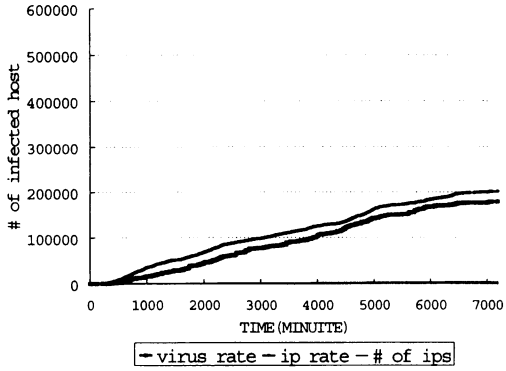

図 4 Sasser.D worm

合計が特徴の条件を充たすので, 提案方法を用いることができる.

4.3.2 感染規模：Sasser.D

Sasser.D 発生からの時系列的な, 解析結果を図 4 に示す. 横軸が時間 (分) であり、縦軸は感染台数である。各線は IP アドレスの種類数 (# of ips), スタティックプロファイリング (ip rate) およびダイナミックプロファイリング (virus rate) による感染規模の推定値である。このワームは 5 日間で 20 万台の感染規模という結果である. 前項の Welchia に比べてやや少めの感染規模となっている. しかし,Sasser が出現してから 10 万台までの感染速度は Welchia よりも早いという相対的な時間比較結果である. これは, Sasser が利用する並行型と Welchia の行なう連続型のスキャン方法の違いにより初期の感染台数の違いが影響していることが原因として考えられる. この結果では Sasser の感染台数は Welchia ほど大規模ではなく, その後の感染台数は Welchia ほどの伸びは見られなかった.

5. 議　　論

この章では、提案手法の有効性・課題について議論する.

5.1 サイトレベルプロファイリング

スタティックプロファイリングは, サイトごとの脆弱ホスト率一定とする理論的なモデル化方法であり, 各ワームごとの感染規模を相対的に比較する場合への適用が考えられる. 例えば今回のような Welchia ワームと Sasser.D ワームのどちらが感染規模が大きいかなどの比較の場合である. しかし, 通常脆弱率は, 各サイトごとに異るのが現実である. その場合はダイナミックプロファイリングにより, 各サイトごとの脆弱数の重みを実際の状態に近く近似する方法を用いることで別の観点からの近似を行なうことができる. これは, 過去のワームと同程度の脆弱なホストが存在するという想定に基づいている.

5.2 精　　度

本提案手法の精度については, 課題がある. 先行研究では, 大規模な観測点を必要とするが, 標本数としては充分であり良い近似結果が報告されている [1]. しかし, 本手法は少い観測点での測定を可能とするため, 精度については正確な感染台数を求めるのではなく, 感染規模を推定するという方針となっている. 本研究ではワームの流行性の評価が目的であり, 特に指数的な桁違いがなければ弱冠の誤差の許容範囲と考えている. ただし、精度向上については, 今後も検討する予定である.

5.3 観測点の必要 IP 数

先行研究での必要 IP 数は 2 の 20 乗以上が要求されており, 通常入手できない規模の監視データが必要とされるため, システム管理者などが容易に従来方法を用いて感染規模を計測できるわけではない. 一方本手法は, ローカルスキャンを含むワームであれば, その時間的な特性から少ない観測点の IP 数であっても、サイトごとの重みをつけるという方法となっている. これは先行研究が, ワームの一つ一つのスキャンに対して重みをつけており, 小さい修正の積み重ねをする方針とは異り, 本手法は観測点へのスキャンの到来までの遅延をサイトレベルで大きく修正する方針といえる. 提案手法は先行研究のように多くの IP は必要とせず, 2 の 14 乗以下の IP 数であれば用いることができる. しかし, 監視 IP 数が小規模過ぎても, 遅延時間が大きくなりすぎる可能性がある. 効果的な監視 IP 数を明らかにすることは, 今後の課題である.

6. ま と め

本論文では, ワームの流行性評価として, ローカルスキャンを含むワームのインターネット全体での感染規模の推定として, 観測点へのワームのランダムスキャンにサイトごとの重みを加算して推定する方法を提案した.

当初, ローカルスキャンがローカル IP 空間をすべて選択するまでの時間とランダムスキャンが少くとも一回観測点に届くまでの時間を比較し, 観測点の IP 数が 2 の 14 乗以下であれば, ワームが感染したサイトのオンラインとなっている脆弱なホストは全て感染していると見なすことができる特徴があることを示した.

その特徴を利用して, 観測点に届くワームのスキャンにサイトごとの重みを付けて加算する方法を考案した. 各サイトごとの重みづけに関しては, 2 種類のサイトレベルプロファイリングにより, サイトごとの特徴抽出を行なった. 一つ目は各サイトの脆弱率一定とするスタティックプロファイリングであり, 2 つ目は各サイトごとのウイルス発生数を脆弱ホスト数とし, 将来のワームにおいても同規模の感染台数があると想定するダイナミックプロファイリングである, この両

プロファイリング方法を用いて，Welchia と Sasser.D ワームの感染規模を測定した結果について説明した．また、最後に本手法の有効性や課題について議論を行なった．

謝　　辞

本研究を行なうにあたり，東京海上研究所石井威望氏にアドバイスを頂いたことに感謝致します．

参 考 文 献

1) C.Zou, L.Gao, W.Gong, D.Towsley: Monitoring and Early Earning for Internet Worm, Proceedings of 10th ACM conference on Computer and communication security, Oct, 2003.
2) C.Zou,D.Towsley,W.Gong: On the Performance of Internet Worm Scanning Strategies. ECE Technical Report TR-03-CSE-07,Nov 2003.
3) S.Staniford, V.Paxson and N.Weaver: How to 0wn the Internet in Your Spare Time, In Proceeding of the 11th USENIX Security Symposium.
4) D.Moore, C.Shannon and K.Claffy: Code-Red: a case study on the spread and victims of an Internet worm,In Proceeding of the ACM/USENIX Internet Measurement Workshop, France, Nov, 2002.
5) Snort: The Open Source Network Intrusion Detection System, http://www.snort.org/
6) ウイリアム・スターリングス，暗号とネットワークセキュリティ，ピアソン・エデュケーション．
7) MaxMind:Geolocation IP Address to Country,http://www.maxmind.com.
8) トレンドマイクロウイルスデータベース，http://www.trendmicro.co.jp/vinfo/.
9) TRENDMICRO, WORM.NACHI.A, http://trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_NACHI.A
10) TRENDMICRO, WORM.SASSER.D, http://trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_SASSER.D