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

2006－DPS－126（48）
2006－CSEC－32（48）
2006／3／17

未知ワームを遮断すべきタイミングについて

面 和成　　下山 武司　　鳥居 悟

（株）富士通研究所
〒２１１－８５８８　川崎市中原区上小田中４－１－１
E-mail: {komote, shimo, pro104}@labs.fujitsu.com

あらまし　企業内ネットワークにおけるワーム対策は，近年ますます重要性を増している．従来のワーム対策としては，ベンダから提供されるパターンファイルによる対策が主流となっている．一方で，これは既知のワームにしか適用されず，常に後手に回る傾向にある．これとは別に，ネットワークアクセスの振る舞いから未知／既知を問わずワームを検知・遮断する方式がある．この方式では，パケットの振る舞いでワームの検知を行うため，検知アルゴリズムがワームパケットと判定するまでに一定量のパケットを監視する必要がある．企業内ネットワークのノードが感染したとしても，必ずしも企業内ネットワークでワームが蔓延してしまうとは限らないが，ワームパケットをどのくらいの量で判定・遮断すればワームの蔓延を防止できるのかについては未解決の問題であった．本論文では，蔓延を防止するという立場になって考察することで，どのくらいの量でワームパケットを正しく判定しなければならないかを導出する一つの手法を提案する．

A Study of Timing to Block Unknown Worms

Kazumasa OMOTE　Takeshi SHIMOYAMA　Satoru TORII

Fujitsu Laboratories Ltd.
Kamikodanaka 4-1-1, Nakahara, Kawasaki, Kanagawa 211-8588 Japan
E-mail: {komote, shimo, pro104}@labs.fujitsu.com

Abstract　The worm countermeasure in an enterprise network is increasingly important. The major worm countermeasure detects a worm with the pattern files offered by the vender. The method applies only to known worms, and always ends up reacting after the worm spreading. On the other hand, there are some methods to detect and intercept a known / unknown worm from the behavior of network packets. To detect the worm from its behavior of packets, the methods need to observe some amount of packets until they detect the worm packets. The worm does not spread completely in the enterprise network even if a single node is infected by a worm. So, we need to know the number of worm packets to prevent them from spreading in the enterprise network. In this paper, we propose the method to give the maximum number of worm packets using the discrete mathematical model.

1.　はじめに

2001 年の CodeRed ワームの出現以降，インターネット上のホストに多大な被害を与える様々なワームが出現している．企業内ネットワークにおいても，依然としてワームの感染によるネットワーク停止に伴う企業活動の阻害など，さまざまな問題を引き起こしている．

従来のワーム対策としては，ベンダから提供されるパターンファイルによる対策が主流となっている．一方で，これは既知のワームにしか適用されず，常に後手に回る傾向にある．

これとは別に，ネットワークアクセスの振る舞いから未知／既知を問わずワームを検知・遮断する方式がある．この方式では，パケットの振る舞いでワームの検知を行うため，検知アルゴリズムがワームパケットと判定するまでに一定量のパケットを監視する必要がある．

また，ワームパケットは確率的に企業内の脆弱なノードに到達するため，企業内ネットワークのノードが感染したとしても，必ずしも企業内ネットワークでワームが蔓延してしまうとは限らない．しかし，ワームパケットをどのくらいの量で判定・遮断すればワームの蔓延を防止できるのかについては未解決の問題であった．

本論文では，蔓延を防止するという立場に立って考察することで，どのくらいの量でワームパケットを正しく判定しなければならないかを導出する一つの方法を提案する．これは，企業内ネットワークの脆弱（パッチ未適用等）なノード数およびワーム感染先選択アルゴリズムから，離散数学モデルを用いてｎ次感染ノードまでを考慮した全感染ノード数を求め，時間が十分に経過してもこの感染ノード数が発散しないための判定上限パケット数を導出する方法である．

以下本論文の構成を述べる．2 章ではワームに関する数学モデルを用いた関連論文を紹介し，3 章では判定上限パケット数について説明する．4 章では判定上限パケット数の導出について述べ,5 章では蔓延を防止するための判定上限パケット数を求める提案手法を述べ，6 章では具体的なワームおよびネットワークを例として思考実験を行う．7 章で実験結果に対する考察を行い,8 章でまとめを述べる．

2. 関連論文

これまでワームに関する数学モデルがいくつか提案されている．具体的には，インターネット上におけるワームの蔓延を忠実に再現するモデル化に関するもの[1,2]や，これまで提案されている様々なワーム対策を用いることによってインターネット上でワームの感染拡大を防止できるかを数式モデルによって評価したもの[3]が提案されている．これらの論文の中で用いられている数式モデルでは，インターネット上でのワーム蔓延および隔離に関する議論が主であり，また連続分布を用いた数式モデルが主であった．

本稿で提案されている手法は，これまで提案された連続分布を用いた数式モデルを用いた手法とは異なり，離散分布に基づくより厳密な統計モデルを用いたワームの蔓延防止に関する手法である．著者らの知る限りでは，離散分布に基づく手法は見当たらなかった．

3. 判定上限パケット数

判定上限パケット数とは，企業内ネットワークにおいて，蔓延防止の観点から検知アルゴリズムが判定結果を出すまでに必要なパケット数の上限のことである．

１つのワームパケットは，企業内ネットワークの有効ノード（ワームパケットが到達すると必ず感染するノード）に確率的に到達する．有効ノード数が多くなればなるほど，この確率が高くなりワームの感染拡大の速度が増す．つまり，ワームの感染確率は，企業内ネットワークの有効ノード数によって異なると考えられる．

判定上限パケット数はワームパケットを遮断するタイミングに影響する．そのため，ワームの感染確率が高いと，それだけワームパケットの遮断を早める必要があるため，判定上限パケット数を小さくしなければならない．つまり，判定上限パケット数は，ワームの感染確率によって異なると考えられる．

また，最初の感染ノードが発信したワームパケットだけでなく，２次感染以上の感染ノードが発信したワームパケットも考慮して，トータルでワームの蔓延防止が出来なければならない．

4. 判定上限パケット数の導出

判定上限パケット数を導出するにあたり，以下の２点を考慮する．

1. 有効ノードに到達する確率を導出するのに，企業内ネットワークの有効ノード数を考慮する．

2. n 次感染までを考慮する.

1 に関しては，企業内ネットワークの有効ノード数に応じた判定上限パケット数を導出することをねらう.

2 に関しては,ワームの感染拡大が珠つなぎに n 次感染まで起こるため， 1～n 次感染ノード数を全て足し合わせて全感染ノード数を導出する.

5. 提案手法

5.1. 目的

企業内ネットワークの有効ノード数およびワーム感染先選択アルゴリズムから，離散数学モデルを用いて n 次感染ノードまでを考慮した全感染ノード数を求め，時間が十分に経過してもこの感染ノード数が発散しないための判定上限パケット数を導出する.

5.2. 前提

以下に，提案手法の前提を７つ示す.

1. １つのワームパケットが有効ノードに到達するとそのノードが感染する.
2. 有効ノードが企業内ネットワーク内に均一に配置されている.
3. 感染ノードから送出されるワームパケットの間隔を一定とする
4. ネットワークアクセスの振る舞いからワームを検知するワーム対策技術が各ノード（PC）にインストールされており，各ノードにおけるワーム判定のために必要なパケット数を一定とする
5. １つのワームパケットが有効ノードに到達する確率（感染確率）を一定とする
6. １ワームパケット送出する毎に１クロック経過する
7. 感染からワームパケット送出までの時間を無視する

前提１では，実際は感染するためには複数のパケット（SYN パケットやデータパケットなど）を必要とする場合が多いが，今回は簡単のため１つのワームパケットで感染するとした．前提2,3,4 では，簡単のための前提である．前提５では，実際は感染ノード数が増加するに従って，有効ノード数は減少する．しかし，感染ノード数は全アドレス空間に比べて非常に少なく抑えられることから本モデルでは感染確率を一定とした.前提６では，１パケット送出する毎に１クロック経過すると定義し，時間の概念を入れる．前提７では，実際のワームは感染してからワームパケットを送出するのにいくらかの時間を要するが，簡単のためこの時間を無視する.

5.3. パラメータ

以下に，提案手法で使用するパラメータを整理する.

- 有効ノード数（N, Na, Nb）：それぞれ，企業内ネットワークの脆弱なノード数，最初の感染ノードと IP アドレスの第一オクテットが等しいネットワークに属する脆弱なノード数,最初の感染ノードとIPアドレスの第一，第二オクテットが共に等しいネットワークに属する脆弱なノード数
- 判定上限パケット数（w）：１つの感染ノードでワームを判定するまでに必要なパケット数
- 感染確率（p）：１つのワームパケットが企業内ネットワークの有効ノードに到達する確率
- クロック数（T）：１パケット送出する毎に経過する時間
- 感染次数（n）：最初の感染ノードからの経路の深さ（企業内ネットワークの全有効ノード数以下の値）
- En(p, T, w)：感染確率 p，判定上限パケット数 w であるときの T クロック後の n 次感染ノード数の期待値
- E(p, T, w)：感染確率 p，判定上限パケット数 w であるときの T クロック後の全感染ノード数の期待値
- I(p, w)：時間が十分経過した後の感染確率 p，判定上限パケット数 w における全感染ノード数の期待値

5.4. 有効ノード数と感染確率

企業内ネットワークのアドレス空間が全て使用されていることは稀である．アドレス空間はたいてい部分的にしか使用されていない．ワームは確率的に感染先ノードを選択するため，送出された

ワームパケットが必ず有効ノードに届くとは限らない．そのため，ある感染ノードからの感染確率は企業内ネットワークの有効ノード数に依存する．

既存のワームでは，感染先選択確率が完全にランダムのものと，感染ノードの IP アドレスの各オクテットと部分的に等しいネットワーク毎で確率が異なるものが存在する．例えば CodeRedII ワームの場合，図１のように，感染ノードの IP アドレスが A.B.C.D のとき，p1=0.125%の確率でランダムなネットワークへ，p2=0.500%の確率で IP アドレスが A.*.*.*のネットワークへ，p3=0.375%の確率で IP アドレスが A.B.*.*のネットワークへワームパケットが送出される（*は 0～255 の整数）．したがって，感染ノード a からの感染確率 p は式(1)のように表せる．ただし，p1 の確率で届くアドレス空間は２の３２乗であり企業内ネットワーク外部へも送出されるが，ここでは企業内ネットワークのみの感染ノードが考慮されている．また，N は Na を含み，Na は Nb を含む．

$$p = p1\times\left(\frac{N-1}{2^{32}}\right)+ p2\times\left(\frac{Na-1}{2^{24}}\right)+ p3\times\left(\frac{Nb-1}{2^{16}}\right) \qquad (1)$$

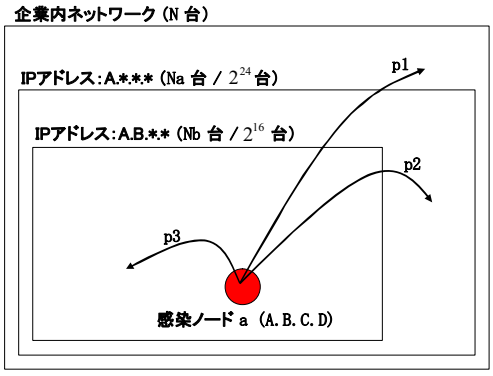

図１： 感染確率の説明図

5.5. ０次感染ノード数

０次感染ノード数とは，最初の１つの感染ノードのことであり式(2)のように表すことができる．

$$E_0(p,T,w)=1 \qquad (2)$$

5.6. Ｔクロック後の１次感染ノード数の期待値

Ｔ クロック後の１次感染ノード数とは，最初の１つの感染ノードがＴクロックまでに直接感染させるノード数を指す．例えば，図２にある通り，４クロック後の１次感染ノード数は，以下のように確率的に０～４となる．このとき，１次感染ノード数の期待値は下式のように表すことができる．

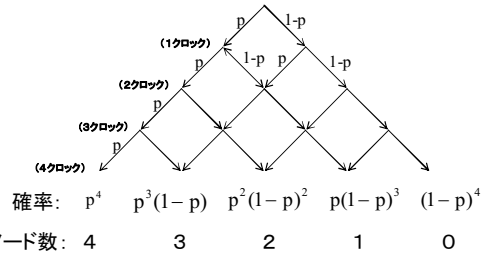

図２： ４クロック後の確率と１次感染ノード数

$$\begin{aligned}E_1(p,4,w) &= 1\cdot{}_4C_1\cdot p\cdot(1-p)^3+2\cdot{}_4C_2\cdot p^2\cdot(1-p)^2\\ &\quad+3\cdot{}_4C_3\cdot p^3\cdot(1-p)+4\cdot{}_4C_4\cdot p^4\\ &=\sum_{i=1}^{4} i\cdot{}_4C_i\cdot p^i\cdot(1-p)^{4-i}\end{aligned}$$

よって，Ｔ クロック後の１次感染ノード数の期待値は，式(3)のように表すことができる．

$$E_1(p,T,w)=\begin{cases}\displaystyle\sum_{i=1}^{T} i\cdot{}_TC_i\cdot p^i\cdot(1-p)^{T-i} & (T<w)\\ \displaystyle\sum_{i=1}^{w} i\cdot{}_wC_i\cdot p^i\cdot(1-p)^{w-i} & (T\ge w)\end{cases} \qquad (3)$$

5.7. Ｔクロック後の2次感染ノード数の期待値

Ｔ クロック後の２次感染ノード数の期待値は，１次感染ノード数の期待値を用いて，式(4)のように表わすことができる．ただし，一度１次感染したノードは２次感染しないため，２次感染以降の感染ノード数に含まれない．

$$\begin{aligned}E_2(p,T,w) &= E(1,p,1,w)\cdot E(1,p,T-1,w)\\ &\quad+\big(E(1,p,2,w)-E(1,p,1,w)\big)\cdot E(1,p,T-2,w)\\ &\quad+\big(E(1,p,3,w)-E(1,p,2,w)\big)\cdot E(1,p,T-3,w)\\ &\quad\cdots\\ &\quad+\big(E(1,p,w,w)-E(1,p,w-1,w)\big)\cdot E(1,p,T-w,w)\end{aligned} \qquad (4)$$

5.8. Tクロック後の全感染ノード数の期待値

T クロック後の全感染ノード数の期待値は，0 次感染ノード数から T 次感染ノード数までの総和であるため，式(5)のように表すことができる.

$$E(p,T,w)=\sum_{i=0}^{T}E_i(p,T,w) \quad (5)$$

5.9. 全感染ノード数の期待値

全感染ノード数の期待値は,式(5)において時間が十分に経過した（クロック T を無限大にした）ときの値であり,式(6)のように表すことができる.

$$I(p,w)=\lim_{T\to\infty}\sum_{i=0}^{T}E_i(p,T,w) \quad (6)$$

5.10. 判定上限パケット数の導出

判定上限パケット数は，全感染ノード数の期待値が所定の有限値α以下となる w である. よって，判定上限パケット数を導出するには,式(7)を満たす w を求めればよい.

$$I(p,w)\le\alpha \quad (7)$$

6. 実験

6.1. 目的

全感染ノード数の期待値 I(p,w)が発散すれば，式(7)を満たす判定上限パケット数(w)を導出することが出来ない．そこで，いくつか想定される企業内ネットワークにおいて，判定上限パケット数が導出可能であるかを確認する.

6.2. 環境

表１は，総務省による，平成１４年度の情報化基本調査結果報告書規模別の主要システム数の調査結果である[4].

表１：企業内ネットワークの機器接続数の割合

規模	機器接続数	割合
小規模	50～500 台	76.9%
中規模	501～1,000 台	9.9%
大規模	1,001～10,000 台	12.1%
	10,001 台～	1.1%

思考実験の事例として，表１の機器接続数を参考にして以下のように３種類の企業内ネットワーク（小規模，中規模，大規模）を設定する.

- 小規模 : 有効ノード数５百（アドレス空間は A.B.*.*）
- 中規模 : 有効ノード数１千（アドレス空間は A.B.*.*）
- 大規模 : 有効ノード数１万（アドレス空間 A.*.*.* 内に１万,アドレス空間 A.B.*.* 内に２千）

３種類の企業内ネットワークにおいて，有効ノード数が均一に配置されているものとする．また，想定するワームとして，企業内ネットワークにおいて感染ノードと近いネットワーク内の脆弱マシンを高い確率で狙う CodeRedII ワームを用いた.

6.3. 評価項目

評価項目は，以下の２つである.

1. 式(6)より,w を１から順にインクリメントして全感染ノード数の期待値 I(p,w)を導出する．ここで，I(p,w)が導出可能かどうかを評価する.
2. 式(7)を満たす最大の w を判定上限パケット数として導出する．ここで，w が導出可能かどうかを評価する.

6.4. 結果

まず，評価項目１に関して，w と I(p,w)がどのような関係になるかを調べた．そこで，大規模ネットワークを例にとり，横軸を判定上限パケット数 w とし，縦軸を全感染ノード数の期待値 I(p,w)としたグラフを描いた(図3).図3のグラフでは，判定上限パケット数が増加するに従って，I(p,w)が指数的に増加し，w≧86 で I(p,w)が無限大になった．これより，大規模ネットワークにおいて，w≦85 の範囲で I(p,w)が導出可能であることが確認できた.

次に，評価項目２に関して，３種類の企業内ネットワークにおいて，α=2（次の１ノードの感染まで)とした場合の式(7)を満たす判定上限パケット数 w を求めた．これは，最初の感染ノードが次の１台のマシンまで感染させて，全感染マシン台

数が合計２台で収束するというケースである．

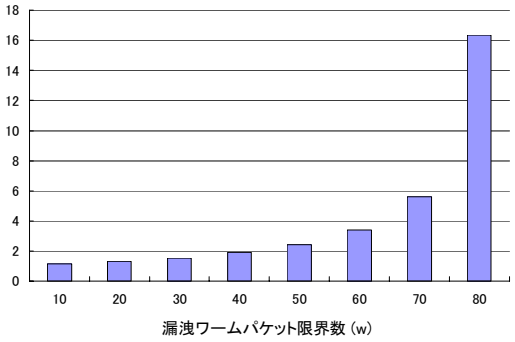

図３： 全感染ノード数の期待値（大規模ネット）

I(p, w)≦2 となる w を求めた結果，小規模ネットワークの場合は w=174，中規模ネットワークの場合は w=87，大規模ネットワークの場合は w=42 という値が得られた．これより，３種類のネットワーク規模において，α=2 とする式(7)を満たす判定上限パケット数が導出できることが確認できた．

7. 考察

6 章の実験結果より，３種類の企業内ネットワークにおいて，全感染ノード数を平均で２（自身のノードも含む）に抑えるためには，ワームパケットを 42 パケットまでに判定･遮断すべきという結果が得られた．また，表１より接続機器が１万台以下である企業ネットワークが全体の 98.9%を占めるため，本手法が大部分のネットワークで導出可能ではないかということが考えられる．

しかし，今回の結果はあくまでも確率に基づいた期待値であるため，42 という結果には，ある確率での誤差が存在すると考えられる．そのため，この誤差をσとすると，実際のネットワーク環境では，適用すべき判定上限パケット数が 42±σとなることが予想される．

また，ネットワークアクセスの振る舞いからワームを検知・遮断するワーム対策装置において，この判定上限パケット数 42 からワーム検知のための閾値を決めることができるのではないかと考えられる．しかし，単純に閾値を最大で 42 に設定するというわけにはいかない．なぜならば，この判定上限パケット数 w は，この値を超えるパケットが送出されると企業内ネットワークでワーム我蔓延してしまうからである．すなわち，ワーム対策装置は，この値のパケット数が送出される前に遮断完了しなければならない．一方で，検知アルゴリズムがワームパケットと判定するまでに一定量のパケットを監視する必要があり，これが閾値に相当する．また，ワーム対策装置はワーム判定から遮断完了までに一定時間要する．したがって，ワーム対策装置の閾値は遮断完了までの時間を考慮したものである必要があると考えられる．

8. まとめ

本稿では，企業内ネットワークにおける有効ノード数を入力値とし，時間が十分経過しても企業内ネットワークのワームの感染ノード数が発散しないための判定上限パケット数を導出する手法を提案した．また，提案手法を３種類の企業内ネットワークに適用して実際に判定上限パケット数を導出することができた．

今後の課題としては，今回導出した判定上限パケット数の理論値の妥当性検証が必要であると考えている．

参考文献

[1] S. Staniford, V. Paxson, and N. Weaver, “How to 0wn the Internet in Your Spare Time”, In Proceedings of the 11th USENIX Security Symposium (Security '02), 2002.

[2] C. C. Zou, W. Gong, and D. Towsley, “Code Red Worm Propagation Modeling and Analysis”, in Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS), November 2002.

[3] D. Moore, C. Shannon, G. M. Voelker, and S. Savage, “Internet Quarantine: Requirements for Containing Self-Propagating Code”, In IEEE INFOCOM, 2003.

[4] 総務省行政管理局, ”平成 14 年度 独立行政法人等 情報化基本調査結果報告書”, http://www.soumu.go.jp/gyoukan/kanri/pdf/doku2002.pdf