

ワームのノード探索特性の定量化に関する提案

仲小路 博史[†] 寺田 真敏[†] 洲崎 誠一[†]

[†]株式会社日立製作所システム開発研究所 〒212-8567 神奈川県川崎市幸区鹿島田 890

あらまし ネットワークワームに関する情報として、どのような脆弱性を利用するかといった感染手法や感染時の症状、駆除方法等が公開されているが、ワームが感染活動を行う際にネットワーク上でどのような挙動を示すのかといった「伝搬特性」に関する情報はほとんど提供されていない。伝搬特性のうち、ノード探索特性は、ネットワークワームの感染範囲や感染拡大速度を推定する上で重要な情報の1つである。ノード探索特性を分かりやすい形でネットワーク管理者に提示することは、ネットワークワームの脅威からネットワークを守るための対策を立案する上で重要であるが、現在、十分な情報が提供されているとは言えない。また、過去のワームとの類似性比較や、ノード探索特性を用いた検知を実現するためには、その定量化が課題となる。

本稿では、ノード探索特性としての周期性、走査範囲ならびに均一性の定量化を試みる。さらに、定量化したノード探索特性に基づいたワームの検証を通して、提案するアプローチの有効性を示す。

キーワード ワーム、ノード探索特性、定量化

Proposal for the quantitative method of searching characteristics of node

Hirofumi NAKAKOJI[†] Masato TERADA[†] and Seiichi SUSAKI[†]

[†] Systems Development Laboratory, Hitachi, Ltd. 890 Kashimada, Saiwai-ku,

Kawasaki-shi, Kanagawa, 212-8567 Japan

Abstract Information about the network worms, such as how they exploit vulnerabilities, infection symptoms, how to remove them, is widely published, but "worm propagation characteristics" - how they behave on the networks to cause infection - are hardly provided. Among other characteristics, the way a worm looks for potential targets is especially beneficial in estimating the infection rate and range. It would also help network managers in implementing countermeasures to protect their network and the Internet itself, but the information needed is not sufficiently available. On the technical side, quantifying the characteristics is a key task to make a comparison with the past worms or develop a detection technique using the target-searching characteristics. In this paper, we present a method to quantify periodic patterns the worms exhibit when looking for the targets, and the range and randomness of IP addresses they target. Furthermore, we show the effectiveness of our approach through worm categorization and comparison based on the quantified target-searching characteristics of the worms.

Keyword worms, target-searching characteristics, quantitative

1. はじめに

2001年に甚大な被害をもたらした Nimda[1]や CodeRed[2]の発生を皮切りに、高度な機能を持ったネットワークワーム（以降、単にワームと記す）が相次いで発生し、ネットワーク管理者や利用者は幾度となくそれらの脅威に対抗してきた。近年、脅威の傾向はボットやフィッシングへと移りつつあり、上記のようなワームに起因する大規模なインシデントの発生は減少傾向にある。しかし、文献[3]からもわかるように、ワームの感染活動は現在もなお継続しており、脅威がなくなったわけではない。

それらワームに関する情報は、（独）情報処理推進機構（IPA）[4]やウイルス対策ベンダ各社から提供されているが、その内容は、どのような脆弱性を利用するかといった感染手法や感染時の症状、駆除方法等が主であり、実際にワームに感染しているノードがネットワーク上で示す活動を継続的に観測して、感染活動時のパケットの送信頻度や感染先ノードの選択順序などに見られる感染先ノード探索活動の特徴や、攻略パケットの送信活動の特徴などを示した「伝搬特性」に関する情報はほとんど提供されていない。

伝搬特性のうち、ノード探索特性は、ワームの感染

範囲や感染拡大速度を推定する上で重要な情報の1つである。ノード探索特性を分かりやすい形でネットワーク管理者に提示することは、ワームの脅威からネットワークを守るための対策を立案する上で重要となるが、現在、十分な情報が提供されているとは言えない。また、過去のワームとの類似性比較や、ノード探索特性を用いた検知などを実現するためには、ノード探索特性の定量化が課題となる。

以上のような背景から、著者らは、ネットワーク管理者の分析活動を支援するために、文献[5]のように、ワームが新たな感染先ノードを探索する際にネットワークへ送信するノード探索パケットの宛先 IP アドレスに含まれる4つのオクテットの値に注目してそれぞれのオクテットの値の走査範囲、均一性、周期性に見られる特徴を可視化することでワームのノード探索特性を表現した。しかし、ノード探索活動の可視化は、特性の直感的な把握が可能になるというメリットがある一方で、人間の感性に依存する部分が大きいために、特性に基づいた類似性の比較やワームの検知が難しいというデメリットもある。そこで本稿では、ノード探索特性に基づくワームの分類や、検知、伝搬活動のシミュレーションのために、これらの特性の定量化を試みる。これらの情報をISPやイントラネットなどのネットワーク管理者が、これらの情報をワームによるインシデント発生の発見に活用したり、過去のワームと比較したり、前述したコード解析結果の補完的な情報として利用することで、より迅速で的確な対策の立案や、ワームによるトラフィックの自動制御が可能になると考える。

本稿の構成について述べる。2章では、ワームのノード探索活動に関わる3つの観測軸を示す。3章では、その観測軸に表れるノード探索特性の定量化を提案する。4章では、既知ワームのノード探索活動の定量化を通して、その特性を示す。5章では、文献[5]において可視化して確認した特性と、定量化により得られた特性との関連性を検証する。6章は結論である。

2. ワームの感染活動

ワームのネットワークに対する振る舞いの主たる活動は、感染拡大活動である。この活動の一環として感染先ノードの探索を行う。このノード探索は、ワームの種類によって異なる特性を持つことが確認されており、特性は下記の3つの観測軸によって表現することができる。

(1) 送信タイミング

本観測軸は、主に周期性に関わるものであり、長期的な周期性としては、CodeRedが1日から19日までを感染活動期間とし、それ

以外については休眠あるいはDoS攻撃期間という事例がある。また、短期的な周期性としては、Nimda.Eのように、感染パケットを多数送信する時間とそれ以外の時間を交互に組合せながら感染活動を試みるという事例がある。

(2) 感染先ノード IP アドレスの生成規則

本観測軸は、感染先となるIPアドレスの生成規則に関するものである。SQLSlammer[6]は、無作為にIPアドレスを生成しながらノードを探索するが、MSBlaster[7]は、感染ノードと同一のネットワークに属するIPアドレスを重点的に生成しながらノードを探索するという事例がある。

(3) 感染先ノードのポート番号とプロトコルの生成規則

本観測軸は、主に標的とするサービスに関するものであり、Nimda.Eのように、80/tcp, 137-139/tcp, 445/tcp番ポートで稼動する複数のサービスを狙って活動するという事例がある。

著者らは、以前に文献[8]においてワーム感染ノードによるパケット送信量を時系列に度数化して周波数分析を行うことにより(1)に示した送信タイミングの周期的な特性を定量化した。本稿では、感染活動において、より顕著に特性が現れる(2)に示した感染先ノードIPアドレスの生成規則に着目する。また、(3)に示した複数のポート番号やプロトコルの生成に着目した検討は今後の課題である。

ここでは、感染先ノードIPアドレスの生成規則を特徴付けるために、IPアドレスを4つのオクテットに分解し、それぞれのオクテットの値に関して、さらに以下に示す3つの観測軸で詳細化を試みる。

(1) 走査範囲

(2) 均一性

(3) 周期性

走査範囲は、ワーム感染ノードの送信する一定量のパケットに含まれる宛先IPアドレスの出現範囲に関わるものであり、ノード探索範囲の広さを表す。また、均一性と周期性は宛先IPアドレスのランダム性に関わるものであり、探索先ノードの推定の難易度を表す。

3. ノード探索特性の定量化手法

本章では、一定期間に生成された宛先IPアドレスを4つのオクテットに分解し、個々のオクテットについて、2章で取り上げた、走査範囲、均一性、周期性の観測軸で定量化を行う。

3.1. 走査範囲の定量化

走査範囲（IP アドレスの生成範囲）に関わる特性を定量的に示す値の算出には、系列の値の網羅性を示す網羅範囲と、系列の値の散らばり度合いを示す分散とを用いる。

3.1.1. 網羅範囲

走査範囲の網羅性に関わる特性を定量的に示す値の算出には、出現割合を利用して R と記す。あるワームが一定期間に生成した n 個の IP アドレスの第 k オクテットからなる系列を $X_k = \{x_{ki}\}_{i=1,2,\dots,n}$ とし、系列 X_k に含まれる値の出現数、すなわち値のユニーク数を r_k としたとき、第 k オクテットの網羅範囲 R_k は式（1）で求められる。

$$R_k = \frac{r_k}{256} \times 100, \quad k = (1,2,3,4) \quad (1)$$

IP アドレスの上位オクテットのアドレスブロックへの影響力の強さにより、 R_k の値が同じでも、 k が小さいほどワームの走査範囲は広いと考えられる。

3.1.2. 分散

走査範囲の散らばり度合いに関わる特性を定量的に示す値の算出には、統計学における分散を利用して V と記す。あるワームが一定期間に生成した n 個の IP アドレスの第 k オクテットからなる系列を $X_k = \{x_{ki}\}_{i=1,2,\dots,n}$ とすると、 V_k は式（2）で求められる。

$$V_k = \sigma_k^2 = \frac{\sum_{i=1}^n (\bar{x}_k - x_{ki})^2}{n}, \quad k = (1,2,3,4) \quad (2)$$

ワームによるノード探索に関わる走査範囲の散らばり度合いが大きければ V_k は大きな値となり、散らばり度合いが小さければ 0 に近い値となる。

3.2. 周期性及び均一性の定量化

周期性及び均一性の算出には、米国国立標準技術研究所（NIST）の発行するランダム性評価手法を制定した NIST Special Publication 800-22[9][10]（以下 SP800-22）を応用する。本ドキュメントには、異なる観点を持つ全 16 種類の乱数評価手法が記載されており、その中の次に示す検定手法に注目する。

（1） Discrete fourier transform test

（離散フーリエ変換検定）

（2） Serial test (系列検定)

両者とも暗号強度に関わるランダム性を評価するための一検定手法ではあるが、（1）は系列の周期性を評価し、（2）は系列の均一性を評価することができるため、IP アドレスの値からなる系列の周期性及び均一性の評価に上記の 2 つの検定手法を適用した。

3.2.1. Discrete fourier transform test

系列を DFT（Discrete Fourier Transform：離散フーリエ変換）によって周波数成分に分解し、各周波数における成分強度が閾値を超えた数の偏りを調べる。

本稿における定量化では、第 k オクテットの周期性 s_k を、あるワームが一定期間に生成した n 個の IP アドレスの第 k オクテットからなる系列 $X_k = \{x_{ki}\}_{i=1,2,\dots,n}$ に対して DFT を行うことによって得られる周波数成分について、一定の閾値を超える周波数成分の含有率を求めることにより定量化する。周期性 s_k は、系列の周期性の強さ、すなわち周期性検定におけるランダム性の低さを表す。本稿においては、ワームによって生成される IP アドレスのオクテットの生成規則に周期性があれば s_k は高い値となり、周期性がない、つまりランダム性が高ければ 0 に近い値となる。

3.2.2. Serial test

系列頻度検定とも呼ばれ、0,1 からなる系列における長さ m ビットのパターン、長さ $m-1$ ビット、 $m-2$ ビットのそれぞれのパターンについて、出現頻度の均一性を検定することによりランダム列の一様性・圧縮可能性を評価する。本稿ではオクテット（8 ビット）を検定することから $m=8$ とし、あるワームが一定期間に生成した n 個の IP アドレスの第 k オクテットからなる系列を $X_k = \{x_{ki}\}_{i=1,2,\dots,n}$ とする。次に SP800-22 に従い X_k の検定を行って得られた検定統計量 p -value を p_k とし、 p_k を用いて各オクテットのランダム性の評価を行う。

ワームによって生成される IP アドレスのオクテットの値に均一性があれば p_k は高い値となり、なければ 0 に近い値となる。

4. 既知ワームのノード探索特性の定量化

3 章で述べた 4 つの定量化手法を用いて、表 4.1 に示した 6 種類のワームのノード探索 IP アドレスを、走査範囲及びランダム性の観点から評価した。

なお、本稿では、文献[5]において収集したデータを利用し、各ワームが送信した 1024 個のパケットの宛先 IP アドレスを対象に、第 k オクテットを抽出して構成した系列を $X_k = \{x_{ki}\}_{i=1,2,\dots,n}$ として定量化している。

表 4.1 既知ワーム

名称	発生時期
Nimda.E	2001 年 10 月
SQLSlammer	2003 年 1 月
CodeRed3	2003 年 3 月
MSBlaster	2003 年 8 月
Sasser.B	2004 年 5 月
Zotob	2005 年 8 月

4.1. Nimda.E

表 4.2 に示す Nimda.E の網羅範囲 R_3, R_4 及び分散 V_3, V_4 に表れている高い値は、第 3,4 オクテットの走査範囲が非常に広範囲であることを示している。また、DFT 検定 s_3, s_4 に比較的高い値が表れていることから、第 3,4 オクテットには周期的な振る舞いがみられることを示している。

4.2. SQLSlammer

SQLSlammer は、文献[6]によると、ランダムに生成された IP アドレスにパケットを送信すると報告されている。一方で、以前に著者らの論文[11]において一様にランダムというわけではないと報告していた。この特性は表 4.3 に示す p_1 に表れており、高い精度で均一に値が生成されていることが示されている。さらに、 R_1, R_2, R_3 及び V_1, V_2, V_3 が非常に高い値を示している一方で、 R_1, V_1 が相対的に低くなっている。これは、第 1 オクテットは他のオクテットと比較して走査範囲に何らかの制限があることを示している。

4.3. CodeRed3

表 4.4 に示すように、CodeRed3 の第 3, 4 オクテットの周期性 s_3, s_4 及び均一性 p_3, p_4 は、第 1, 2 オクテットと比較して高い値となっている。これは第 3, 4 オクテットの値の生成に規則性がみられることを示している。また、 R_1, V_1 に示されるように、第 1 オクテットの走査範囲が他のオクテットと比較して狭くなっていることがわかる。

表 4.2 Nimda.E の探索特性

k	網羅範囲 (R_k)	分散 (V_k)	DFT (s_k)	Serial (p_k)
1	42.58	28.04	0.00	0.00
2	60.16	51.53	0.00	0.00
3	90.23	73.55	0.05	0.00
4	91.02	73.53	0.06	0.00

表 4.3 SQLSlammer の探索特性

k	網羅範囲 (R_k)	分散 (V_k)	DFT (s_k)	Serial (p_k)
1	93.36	69.56	0.09	1.00
2	98.05	74.55	0.05	0.89
3	97.66	73.95	0.05	0.84
4	96.48	74.87	0.06	0.27

表 4.4 CodeRed3 の探索特性

k	網羅範囲 (R_k)	分散 (V_k)	DFT (s_k)	Serial (p_k)
1	17.58	23.15	0.00	0.00
2	64.84	58.84	0.01	0.00
3	82.42	73.25	0.05	0.31
4	82.42	73.04	0.06	0.13

4.4. MSBlaster

表 4.5 に示すように、MSBlaster の R_4 が 100.00 を示していることから、第 4 オクテットにおいて 0~255 の範囲を全て走査していることがわかる。また、 p_4 が 1.00 を示していることから、均一に値を生成していることがわかる。第 1, 2 オクテットに関しては、 R_1, R_2 が低い値を示していることから、値がほとんど変化していないことがわかる。

4.5. Sasser.B

表 4.6 に示すように、Sasser.B[12] の第 1 オクテットの走査範囲に関する R_1, V_1 が他のオクテットと比較して低いことから、第 1 オクテットの走査範囲に若干の制限があることがわかる。また、第 1,2 オクテットに関する p_1, p_2 が低い値になっていることから、これらのオクテットにおいては均一的ではなく、値の出現頻度に偏りがあることがわかる。

4.6. Zotob

表 4.7 に示す Zotob[13] の第 1,2 オクテットの走査範囲に関する R_1, R_2 及び V_1, V_2 の低い値は、当該オクテットの走査範囲が非常に狭いことを示している。

これまでの定量的結果では、走査範囲を示す網羅範囲 R_k と分散 V_k の二要素は同じ増減傾向を示していたが、Zotob の第 3 オクテットの走査範囲を示す R_3, V_3 においては逆の傾向を示している。これは、第 3 オクテットの生成時に、取りうる値のパリエーションの少なさが網羅範囲 R_3 の低さに影響し、生成した値が 3,2,1,0,255 といったように 0 で巡回している特性が分散 V_3 に大きく影響したものと考えられる。

表 4.5 MSBlaster の探索特性

k	網羅範囲 (R_k)	分散 (V_k)	DFT (s_k)	Serial (p_k)
1	0.39	0.00	0.00	0.00
2	0.39	0.00	0.01	0.00
3	1.56	1.07	0.02	0.00
4	100.00	72.58	0.02	1.00

表 4.6 Sasser.B の探索特性

k	網羅範囲 (R_k)	分散 (V_k)	DFT (s_k)	Serial (p_k)
1	49.22	46.17	0.01	0.00
2	68.75	63.41	0.04	0.00
3	78.52	72.89	0.05	0.12
4	75.78	73.20	0.06	0.71

表 4.7 Zotob の探索特性

k	網羅範囲 (R_k)	分散 (V_k)	DFT (s_k)	Serial (p_k)
1	0.39	0.00	0.00	0.00
2	0.78	0.48	0.00	0.00
3	3.91	121.50	0.13	0.00
4	87.50	73.56	0.03	0.03

5. 定量結果の検証

本章では、2章で提示した観測軸に基づいて定量化した各ワームの結果と、文献[5]において同観測軸に基づいて可視化して得られた知見とから、本稿で提案した定量化の妥当性について検証する。さらに、各ワーム間のノード探索特性の相関性を算出し、一般的に特性が類似していると言われているワームの亜種同士の類似性を定量結果に基づき検証する。

5.1. ノード探索特性の可視化との比較検証

文献[5]において SQLSlammer の第1オクテットに見られた走査範囲の制限及び、均一性の高さは、それぞれ表4.3に示した R_1, V_1 の相対的な低さと、 p_1 の高さに表れている。また、CodeRed3 の規則性の可視化にみられる第3, 4オクテットの生成順序の規則性は、表4.4に示した s_3, s_4 の高さに表れており、第1オクテットの走査範囲の相対的な狭さは、 R_1, V_1 の低い値によって表わされている。さらに、図5.1に示したような MSBlaster の第4オクテットに見られたスイープしながらの探索特性は、表4.5に示した R_4, V_4 の高い値に、そして偏りなく走査する特性が p_4 の高い値にそれぞれ表れている。

このような可視化結果と定量化結果の傾向の一致は、上記で述べたワーム以外のノード探索特性にも表れている。これらの結果により、可視化によって得られた特性の定量化の有効性を示すことができた。

5.2. 相関性の検証

4章において算出した各種定量値に基づき、表4.1に挙げた6種類のワーム間の類似性を検証する。さらに、同系のワームとして、Sasser.B の亜種ワームである Sasser.C[14]を新たに検証対象(表5.1)に加え、計7種類のワームの相互相関性の分析を行った。

相関性の分析にあたってはピアソンの積率相関係数を用いる。2つの系列 $x = \{x_i\}_{i=1,2,\dots,n}$, $y = \{y_i\}_{i=1,2,\dots,n}$ が与えられたときに、相関係数 c は式(3)で求められる。

$$c = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2} \sqrt{\sum_{i=1}^n (y_i - \bar{y})^2}} \quad (3)$$

相関係数 c は、2つの系列間の相関性が高いほど1.00に近づき、相関性が低い場合には0.00に近づく。また、-1.00に近づくほど逆の相関性が高いことを示す。

表 5.1 Sasser.C の探索特性

k	網羅範囲(R_k)	分散(V_k)	DFT(s_k)	Serial(p_k)
1	47.66	46.06	0.00	0.00
2	66.41	63.37	0.02	0.00
3	75.39	72.41	0.03	0.10
4	71.48	73.19	0.04	0.37

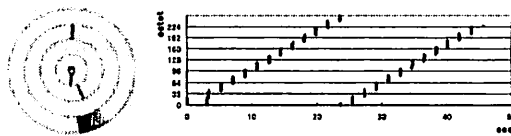


図 5.1 MSBlaster の第4オクテットの可視化結果

いま、2つの系列 $x = \{x_i\}_{i=1,2,\dots,n}$, $y = \{y_i\}_{i=1,2,\dots,n}$ を、検証対象とする2つのワームの各オクテットの定量値系列 $R = \{R_k\}_{k=1,2,3,4}$ として、相関係数 C_R を求める。同様に、 V, s, p についても C_V, C_s, C_p を求める。Sasser.C を含む全てのワーム間の相関係数を表5.2に示す。なお、 μ は、4つの相関係数の平均値を求めた値である¹⁾。

検証を行った結果、Sasser.B と Sasser.C との間で、全ての定量値 (C_R, C_V, C_s, C_p) において高い相関性がある。また、文献[15]によると、Nimda, CodeRed, Sasser のノード探索特性は同じタイプとして分類されている。この分類も相関係数に表れており、本稿で求めたノード探索特性の定量値によって裏付けることができる。

6. まとめ

本稿では、ワームのノード探索特性の定量化について提案し、過去に発生した6種類のワームの定量化を行った。これまでに提示してきた走査範囲、均一性、および周期性の観測軸に基づいた定量化により、可視化で得られた知見を定量的に示すことができるとともに、ワーム間の相関性の定量評価にも活用できることを確認できた。これらの検証結果から、本稿で提案した4つの定量値は、ワームのノード探索特性に関する定量的なプロパティとして利用できると考える。

ネットワーク管理者はこれらの情報を把握することにより、例えば、内部で発生したワームによる外部への影響力や、外部で発生したワームによる内部への影響力を推定することができたり、ネットワークを流れるトラフィックからワームの種別を推定したりすることが可能となる。

今後の課題としては、ノード探索特性に基づくシステムとの連携方式の検討ならびにワームの同定などがあげられる。

謝辞

本研究は独立行政法人情報通信研究機構から委託を受け実施した「ネットワーク環境の脆弱性レベルをリアルタイムで定量評価し、情報流通をセキュアに運用するための意思決定システムの研究開発」の成果の一部である。

表 5.2 ノード探索特性の相関性

	SQLSlammer					CodeRed3				
	C_R	C_V	C_S	C_P	μ	C_R	C_V	C_S	C_P	μ
Nimda.E	0.62	0.86	-0.44	-	0.35	0.86	0.98	0.99	-	0.94
SQLSlammer						0.86	0.94	-0.52	-0.22	0.26

	MSBlaster					Sasser.B				
	C_R	C_V	C_S	C_P	μ	C_R	C_V	C_S	C_P	μ
Nimda.E	0.04	0.53	0.98	-	0.51	0.86	0.99	0.68	-	0.84
SQLSlammer	0.04	0.45	-0.63	-0.98	-0.28	0.86	0.91	-0.92	-0.99	-0.03
CodeRed3	0.46	0.46	0.98	0.07	0.49	1.00	1.00	0.77	0.23	0.75
MSBlaster						0.40	0.50	0.82	0.99	0.67

	Zotob					Sasser.C				
	C_R	C_V	C_S	C_P	μ	C_R	C_V	C_S	C_P	μ
Nimda.E	0.05	0.85	0.71	-	0.53	0.88	0.99	0.87	-	0.91
SQLSlammer	0.05	0.47	-0.40	-0.98	-0.21	0.88	0.92	-0.70	-0.98	0.03
CodeRed3	0.47	0.75	0.61	0.07	0.48	0.99	1.00	0.94	0.34	0.82
MSBlaster	1.00	0.29	0.71	1.00	0.75	0.35	0.51	0.93	0.96	0.69
Sasser.B	0.42	0.78	0.37	0.99	0.64	1.00	1.00	0.92	0.99	0.98
Zotob						0.37	0.78	0.42	0.96	0.63

文 献

- [1] W32.Nimda.E@mm,
<http://www.symantec.com/region/jp/sarcj/data/w/w32.nimda.e@mm.html>
- [2] CodeRed Worm,
http://www.symantec.com/region/jp/avcenter/venc/data/colored_worm.html
- [3] @police, 我が国におけるインターネット治安情勢について, 警察庁, 平成 18 年 11 月,
<http://www.cyberpolice.go.jp/detect/pdf/20061110.pdf>
- [4] IPA (独立行政法人 情報通信推進機構),
<http://www.ipa.go.jp/>
- [5] 仲小路博史, 寺田真敏, 洲崎誠一, ワームのノード探索特性の可視化に関する提案, Computer Security Symposium 2007, Vol.2007 No.16, pp.273--278.
- [6] W32.SQLEXP.Worm,
<http://www.symantec.com/region/jp/sarcj/data/w/w32.sqlexp.worm.html>
- [7] TRENDMICRO, WORM_MSBLAST.A,
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.A
- [8] 仲小路博史, 寺田真敏, 周波数分析に基づくインシデント傾向検知手法に関する検討, Computer Security Symposium 2005, ISEC-193, SITE-192, pp.83--88 (2005).
- [9] A STATISTICAL TEST SUITE FOR RANDOM AND PSEUDORANDOM NUMBER GENERATORS FOR CRYPTOGRAPHIC APPLICATIONS,
<http://csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501.pdf>
- [10] 独立行政法人情報通信研究機構, 独立行政法人情報処理推進機構, CRYPTREC Report 2005 - 擬似乱数検定のための CRYPTREC ミニマムセット仕様書, pp.283--303(2006)

- [11] 寺田真敏, 高田真吾, 土居範久, ネットワークワームの感染先探索特性の検討, Computer Security Symposium 2004, pp.487--492 (2004).

- [12] W32.Sasser.B.Worm,
<http://www.symantec.com/region/jp/sarcj/data/w/w32.sasser.b.worm.html>

- [13] W32.Zotob.A,
<http://www.symantec.com/region/jp/avcenter/venc/data/jp-w32.zotob.a.html>

- [14] W32.Sasser.C.Worm,
<http://www.symantec.com/region/jp/sarcj/data/w/w32.sasser.c.worm.html>

- [15] 日立製作所, 17th Annual FIRST Conference ネットワークワームの動作検証システム,
<http://www.sdl.hitachi.co.jp/japanese/news/2005/first/>

ⁱ Nimda.E の Serial 検定結果が $\{p_k\}_{k=1,2,3,4} = 0$ であるため, 相関係数 C_p は計算できない. この場合は, 母数を 3 として平均値 μ を求めている.