ノード探索特性の可視化および定量化の提案

仲小路 博史† 寺田 真敏† 洲崎 誠一†

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，ネットワーク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，ネットワーク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．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，駆除方法など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うえで重要な情報の 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うえで重要であるが，現在，十分な情報が提供されているとはいえない．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．本論文では，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を可視化により示した後，これらの特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分類や比較を通して，提案するアプローチの有効性を示す．

Proposal for the Visualizing and Quantitative Method of Searching Characteristics of Node

Hirofumi Nakakoji,† Masato Terada† and Seiichi Susaki†

In the last few years, the trend in security threats has been shifting to botnets or phishing, and large-scale incidents caused by network worms are on decrease. However, worm infection is continuously taking place and we should not dismiss the threats still out there. 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 visualize 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.

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) からも分かるように，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，駆除方法などが主であり，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

† 株式会社日立製作所システム開発研究所
Systems Development Laboratory, Hitachi, Ltd.

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うえで重要な情報の 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うえで重要となるが，現在，十分な情報が提供されているとはいえない．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 18) のようにノード探索間隔の周期性に着目することにより，ノード探索特性を定量的に示してきた．本論文では，まず，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ノード探索特性の可視化を行うことにより，それぞれのオクテットの値の走査範囲，均一性，周期性を確認する．さらに，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，確認した特性を定量的に示す．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，コード解析結果の補完的な情報として利用したりすることで，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．

本論文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，ノード探索特性の可視化を提案する．4 章では，既知ワームのノード探索活動の可視化を通して，その特性を示す．さらに，5 章では，4 章で確認した特性の定量化と，定量化を用いたワームの分類や比較結果を示す．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み合わ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 [8] 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 [10] 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．本論文では，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．

- 走査範囲
- 均一性
- 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. ノード探索活動の可視化

ノード探索特性の 1 つである感染先ノード IP アドレスの生成規則の特性を 2 章で述べた観測軸の観点から調査するにあたり，3 種類の手法で可視化を行う．なお，可視化にあたっての特徴は，次のとおりである．

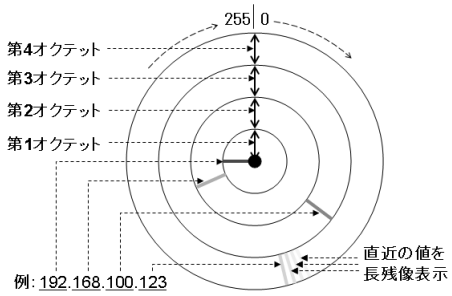

図 1 規則性の可視化
Fig. 1 Visualization of target IP address.

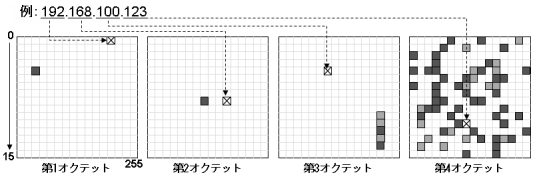

図 2 均一性および走査範囲の可視化
Fig. 2 Range and randomness of target IP addresses.

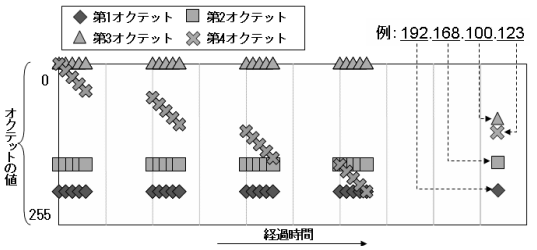

図 3 周期性の可視化
Fig. 3 Visualization of periodic patterns.

- パケットの送信活動の時間軸における変化を忠実に再現するために動画像を用いて表示する．
- 探索先ノードの IP アドレスの規則性を正確に表現するために，IP アドレスを 4 つのオクテットに分解し，それぞれの値を可視化する．

3.1 規則性可視化

本可視化で，ワームのノード探索活動の規則性を把握するために，ワーム感染ノードがパケットを送信している様子を**図 1** に示すように表現する．まず，オクテットの値が巡回するような（0 の次の値が 255 に，あるいは 255 の次の値が 0 にジャンプするような）現象を連続的な変化としてとらえるために，探索先ノードの IP アドレスを構成している 4 つのオクテットを，円の中心から外周に向けて放射状に配置した 4 つのラインでそれぞれ表現し，各オクテットの値を，対応する各ラインの回転角で表す．加えて各オクテットの値の推移を表現するために，一定時間の残像を表示することで，IP アドレスを構成する各オクテットの値の規則性を確認する．

3.2 均一性および走査範囲の可視化

本可視化の目的は，探索先 IP アドレスの各オクテットにおける値の均一性および走査範囲を把握することにある．**図 2** に示す本可視化手法は，各オクテットの値が生成済みか否かを直感的に確認できるようにするために，探索先ノードの IP アドレスを構成している 4 つのオクテットのそれぞれの値に基づいて，左上を 0，右下を 255 とする 16×16 のマトリクスに対応させた各矩形に彩色する．さらに，値の偏りや均一性を表現するために，値が重複した場合には，色を青系から赤系に段階的に変化させることで，アドレスブロックの走査範囲や，均一性を確認する．

3.3 周期性の可視化

本可視化の目的は，宛先 IP アドレスの各オクテットの値の生成順序に関する周期性およびノード探索タイミングを把握することにある．可視化にあたっては，探索先ノードの IP アドレスを構成している 4 つのオクテットに関して，縦軸をオクテットの値，横軸を時間とする散布グラフに表すことで（**図 3**），ノード探索活動の停止/再開，各オクテットの値の周期的/ランダムな振舞いを確認する．

4. 既知ワームのノード探索特性の可視化調査

本章では，**表 1** に示す 2001 年から 2005 年にかけて流布した代表的な 6 種類のワームを対象に，前述の可視化を通してワームのノード探索活動を示す．以降では，各ワームの概要を簡単に説明し，規則性の可視化，均一性および走査範囲の可視化，および周期性の可視化によって確認したノード探索活動にみられる特性について述べる．各図は，動画像によって示される可視化画面のスナップショットを取得した静止画像である．なお，ワームの種類によっては，一度に大量のパケットを送信する性質を持つワームや，断続的に少量のパケットを送信する性質を持つワーム，一定時間停止と送信を繰り返す性質を持つワームが存在することから，つねにワームのノード探索活動をリアルタイムに再生すると傾向の把握が困難となる場合がある．そのため，再生速度の制御を行えるようにしている☆．

4.1 データ収集環境

可視化に使用するワームのノード探索活動に関わるデータ収集環境の構成について述べる．なお，本論文

☆ 本論文で掲載している可視化画像は，静止画の視認性を向上させるために，再生速度が調整されていることに留意されたい．

表 1 主要ワーム
Table 1 List of major worms.

名称	発生時期
Nimeda.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

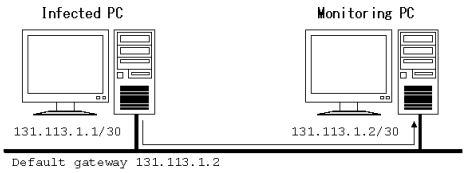

図 4 データ収集環境
Fig. 4 Data collection environment.

では，ワームの探索特性の環境として文献 5) に提示された「特殊な装置を使用する必要がない」，かつ「最小限の機器で環境を用意できる」という条件を参考に環境を構成した．

ワームの感染活動を観測するためのデータ収集環境を**図 4** に示す．ワーム感染ノード（Infected PC）には Windows2000 Server☆を，観測ノード（Monitoring PC）には Linux と tcpdump をインストールしている．ネットワークの設定に関して，サブネットマスク長に 30 bit を，ワーム感染ノードのデフォルトゲートウェイに観測ノードの IP アドレスをそれぞれ設定する．これにより，ワーム感染ノードの送信するパケットのほぼすべて（ワーム感染ノード自身を宛先としたパケット以外）が，観測ノードにおいて受信され，ログに記録される．

4.2 可視化結果

本節では，前述のデータ収集環境で取得したデータを用いて可視化を行った結果を示す☆☆．

4.2.1 Nimda.E

Nimda.E は，80/tcp 番ポートを利用してパッチを適用していない Web サーバ（IIS: Internet Information Service）の脆弱性（MS00-078[6]）を攻略するほか，137-139/tcp，445/tcp を利用してワームの本体を攻略先に転送する．

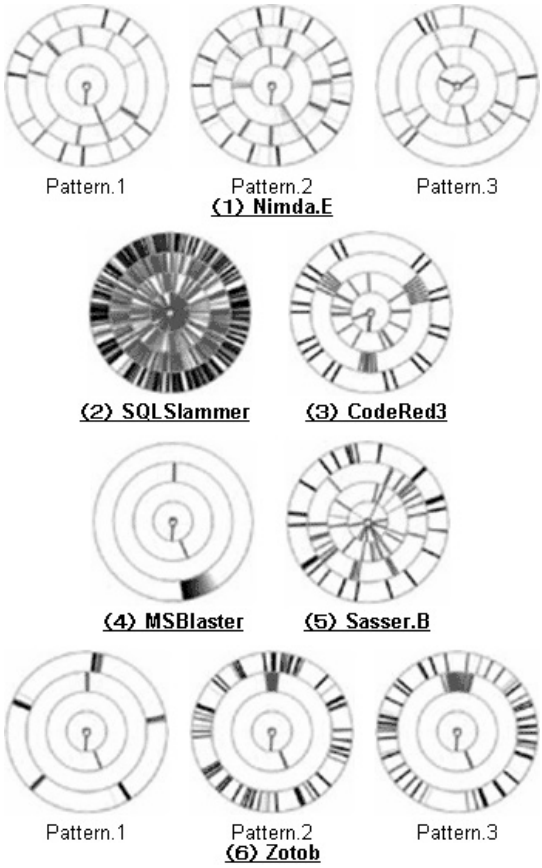

図 5 規則性の可視化結果
Fig. 5 Pattern of target IP address of major worms.

図 5 (1) から，Nimda.E が時間の経過とともにノード探索パターンを変化させていることを確認できる．パターン 1 では宛先 IP アドレスの第 1，2 オクテットを，パターン 2 では第 1 オクテットの走査範囲を 1 カ所に制限させながら，残りのオクテットの走査範囲を広くさせることで，IP アドレス空間の探索範囲を変化させている．また，値の周期性に関しては，**図 7** (1) の第 3，4 オクテットに幾何的なパターンが見られ，一定の周期で単調減少させている特徴を確認することができる．

4.2.2 SQLSlammer

SQLSlammer は，SQL Server 2000 の脆弱性（MS02-039[9]）を狙うワームで，攻略パケットを 1434/udp 番ポートに向けて送信する．

SQLSlammer は，図 5 (2) から，すべてのオクテットにおいて，走査範囲が広いこと，値の生成規則がラ

☆ 商品名称などに関する表示
本論文に記載されている会社名，製品名は，それぞれの会社の商標もしくは登録商標です．
Windows XP，Windows 2000，SQL Server は，米国 Microsoft Corporation. の米国およびその他の国における登録商標です．
Linux は，Linus Torvalds の米国およびその他の国における登録商標あるいは商標です．

☆☆ 周期性の可視化結果（図 7）については，ワームの特徴を強調させるために，ワームごとに観測期間を変化させたり，X 軸を経過時間やパケット順序に変化させたりしている．

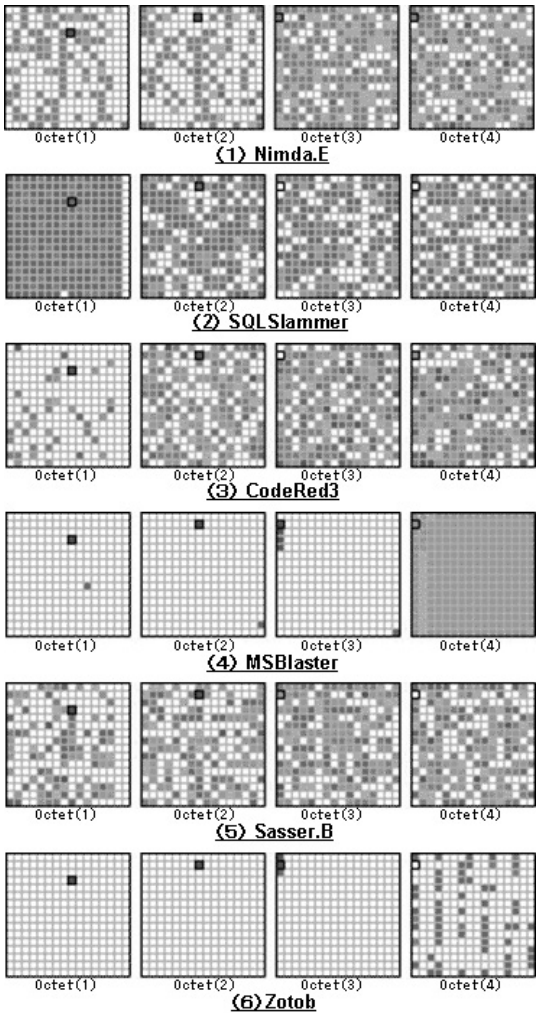

図 6 均一性および走査範囲の可視化結果
Fig. 6 Range and randomness of target IP addresses of major worms.

ンダムであることが分かる．また，**図 6** (2) により，第 1 オクテットには，均一に値を生成する特性も確認できる．さらに，同オクテットでは値が 0 から 239 の範囲に制限されている．これは Multicast アドレスの上限まででアドレス生成を止めるという，実用的な判断に基づく設計に起因するものと考えることができる．

4.2.3 CodeRed3

CodeRed3 は，80/tcp 番ポートを利用して Web サーバ（IIS）の脆弱性（MS01-033 [7]）を攻略するパケットを送信する．

CodeRed3 は，図 5 (3) および図 6 (3) から，宛先 IP アドレスの第 1 オクテットの走査範囲が狭く，第 2〜第 4 オクテットの走査範囲が広いことが分かる．また，図 5 (3) からは，第 3，4 オクテットを，等間隔に並んだ複数のブロックに分けて規則正しく変化させて探索していることが確認できる．このことから，CodeRed3 は第 3，4 オクテットの値の生成規則に周期性を持つと考えることができる．

4.2.4 MSBlaster

MSBlaster は，Windows の脆弱性（MS03-026 [11]）を攻略するパケットをランダムな IP アドレスの 135/tcp 番ポートに向けて送信する性質を持つ．

MSBlaster は，図 5 (4) および図 6 (4) から，宛先 IP アドレスの第 1 から第 3 オクテットの走査範囲を 1 カ所に制限させながら，第 4 オクテットだけを規則正しく単調増加（スイープ）させて走査範囲を広くしていることが分かる．また，図 7 (4) により，一定時間ごとに，一定範囲を分割して探索していることから，MSBlaster は，第 4 オクテットの値の生成規則に周期性があると考えることができる．

4.2.5 Sasser.B

Sasser.B [12] はランダムな IP アドレスに対して，445/tcp 番ポートを利用した LSASS（Local Security Authority Subsystem Service）の脆弱性（MS04-011 [13]）スキャンを行う．

Sasser.B は，図 6 (5) から，すべてのオクテットにおいて走査範囲が広い傾向にあるものの，第 1 オクテットにおいては，一部の値（右側 2 列）が欠けていることから走査範囲に若干の制限を持っていることが分かる．また，すべてのオクテットにおいてランダムな特性が見られるものの，図 7 (5) の第 1，2 オクテットの縦軸中央付近に点が集中して見られることから，第 1，2 オクテットの均一性は低いことが分かる．

4.2.6 Zotob

Zotob [14] は，445/tcp 番ポートを利用して Windows のプラグアンドプレイの脆弱性（MS05-039 [15]）を攻略するパケットを送信する性質を持つ．

図 5 (6) から，Zotob は，宛先 IP アドレスの第 1〜第 3 オクテットの走査範囲を狭い範囲に制限していることが分かる．また，第 4 オクテットを表す最外周に 5 方向のラインが見られ，5 つのブロックに分けて周期的に値を減少させて探索していることが分かる．Zotob は，図 5 (6) のパターン 1 から 3 に見られるように，時間の経過とともに，第 3 オクテットの走査範囲を徐々に広げていくことで，探索範囲を拡大している．

4.3 可視化のまとめ

本章では，6 種類のワームについて可視化を行った．まず，図 5 に示す規則性の可視化は，Nimda.E や Zotob のように，時間の経過とともに探索パターン

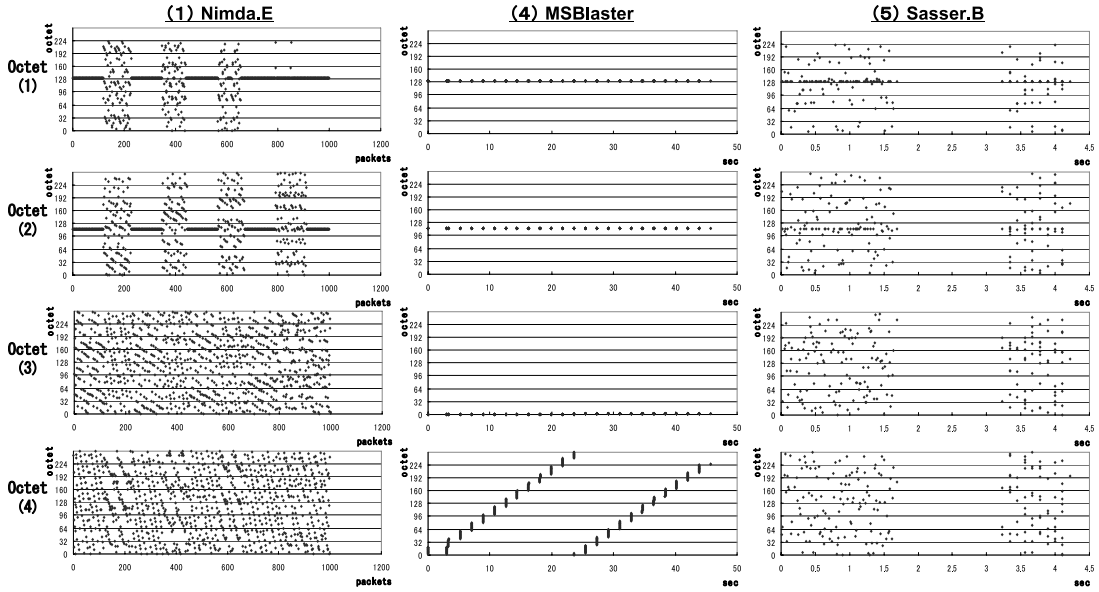

図 7 周期性の可視化結果
Fig. 7 Periodic pattern of major worms.

を変化させるワームや，MSBlaster のようにオクテットの値を巡回させて走査するようなワームの特性の把握に有用である．次に，SQLSlammer のように値がランダムに生成されているように見えていても，実際には第 1 オクテットに限り値を均一に生成する特性があることを，図 6 に示す均一性および走査範囲の可視化から示した．さらに，図 5 および周期性を表す図 7 により，Nimda.E の第 3，4 オクテット，MSBlaster の第 4 オクテットに等幅間隔の規則性，つまり周期性の存在を示した．

5. ノード探索特性の定量化

4 章では，可視化によってノード探索特性の調査を行った．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．

5.1 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．

5.1.1 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_k 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 $X_k = \{x_{ki}\}_{i=1,2,\ldots,n}$ とし，系列 X_k に含まれるユニークな値の総数，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．

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

また，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．

5.1.2 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_k 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 $X_k = \{x_{ki}\}_{i=1,2,\ldots,n}$ とすると，V_k は式 (2) で求められる．

$$V_k = \sigma_k^2 = \frac{\sum_{i=1}^{n} (\overline{x_k} - x_{ki})^2}{n}, k = (1, 2, 3, 4) \tag{2}$$

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．

5.2 周期性および均一性の定量化

周期性およ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[16),17)]（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および均一性の評価に上記の 2 つの検定手法を適用した．

5.2.1 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．本論文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 $X_k = \{x_{ki}\}_{i=1,2,\ldots,n}$ 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，特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．本論文においては，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．

5.2.2 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．本論文ではオクテット（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 $X_k = \{x_{ki}\}_{i=1,2,\ldots,n}$ 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．

5.3 既知ワームのノード探索特性の定量化

5.1 節および 5.2 節で述べた 4 つの定量化手法を用いて，表 1 に示した 6 種類のワームのノード探索 IP アドレスを，走査範囲およびランダム性の観点から評価した．本論文では，各ワームが送信した 1,024 個のパケットの宛先 IP アドレスの第 k オクテットについて，それぞれ系列 $X_k = \{x_{ki}\}_{i=1,2,\ldots,1024}$ を作成し，定量化した結果を**表 2**，**表 3**，**表 4**，**表 5**，**表 6**，**表 7** に示す．

5.3.1 Nimda.E

Nimda.E に見られた第 3，4 オクテットの広範囲で規則的な振舞いは，網羅範囲 (R_3, R_4) および DFT 検定 (s_3, s_4) に現れており，2 つのオクテットの特性がほぼ同様であること示している．また，第 3，4 オクテットに見られた周期性は s_3，s_4 に比較的高い値として現れている．

5.3.2 SQLSlammer

SQLSlammer は，文献 8) 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[19)] 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おり，また，IP アドレスの均一性および走査範囲の可視化（図 6 (2)）結果から，第 1 オクテットに均一性を確認した．この特性は p_1 に現れており，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，オクテット値が 0 から 239 の範囲に制限されて生成される特性は，R_1 の相対的な低さに現れている．これは Multicast アドレスを考慮して設計がなされた結果であり，制限にはあたらないともいえる．本論文では，こういった設計の相違もワームの特性の 1 つであると考え，IP アドレスの最大範囲（0 から 255）を対象に評価するという方法を選択している．なお，静止画像（図 6 (2)）からは確認することは難しいが，均一性および走査範囲の可視化の動画像においては，第 1 オクテットの生成順序に規則性を確認でき，その特性は s_1 に現れている．ただし，その他のオクテットは，ランダムな系列をなしている．

5.3.3 CodeRed3

CodeRed3 の規則性の可視化に見られる第 3，4 オクテットの生成順序の規則性は，s_3，s_4 に現れている．また，均一性および走査範囲の可視化に見られる第 1 オクテットの走査範囲の相対的な狭さは，R_1 の相対的な低さに現れている．

5.3.4 MSBlaster

MSBlaster に見られた第 4 オクテットをスイープさせながら全範囲を探索する特性が R_4 および V_4 に，

偏りなく走査する特性が p_4 にそれぞれ現れている．一方で，規則正しく値が生成されていることから，周期性を表す s_4 に高い値が見られることを想定していたが，期待するほど高い値は得られなかった．

5.3.5 Sasser.B

Sasser.B に見られた第 1 オクテットの走査範囲の制限は，R_1 の相対的な低さに現れている．第 3，4 オクテットの広範囲に及ぶランダムな振舞いは V_3，p_3，V_4，p_4 によりそれぞれ確認できる．4.2 節の可視化結果からは第 3 オクテットと第 4 オクテットとのランダム性の違いを確認することはできなかったが，定量化により，値の均一性 (p_3, p_4) に大きな違いがあることが分かった．

5.3.6 Zotob

第 1，2 オクテットの走査範囲が制限されている Zotob の特性は，R_1，R_2 に現れている．一方，それほど大きな変化が見られなかった第 3 オクテットの走査範囲の一要素を示す分散 V_3 が非常に高くなっている．これは，第 3 オクテットの生成時に 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値に大きく影響したものと考えられる．

5.3.7 定量化のまとめ

2 観測軸 4 種類の検定手法を用いて探索先ノードの IP アドレスを評価した結果は 4 章で得られた可視化による直感的な結果と，ほぼ一致する．また，Sasser.B で得られた定量値から，可視化による直感的な把握が難しかったノード探索特性を見出すことができる．

定量化からワームの種類によって異なった組合せの定量値を得ることができ，これらの値を，ワームを特徴付ける新たなプロパティとして定義することで，ワームの分類に応用できる可能性がある．一方で，網羅範囲が高い値，すなわち広い範囲を走査した場合には，均一性も比較的高くなる傾向を示すなど，定量値間の相関関係が見られた．これは，ランダム性が高いほど広い範囲で，かつ均等の出現確率で値が生成されることに起因していると考えることができる．

5.4 相関性の検証

本節では，本論文で扱った挙動の異なる 6 種類のワーム，および類似の特性を有する 2 つのワームを対象に，前節において付与したプロパティを利用してノード探索特性の類似性を検証する．ここでは，同系のワームとして，Sasser.B の亜種ワームである Sasser.C（**表 8**）を新たに検証対象に加え，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 $x = \{x_i\}, y = \{y_i\}$ $(i = 1, 2, \ldots, n)$ が与えられたときに，相関係数 c は式 (3) で求められる．

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

表 2 Nimda.E の探索特性
Table 2 Characteristics of Nimda.E.

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 3 SQLSlammer の探索特性
Table 3 Characteristics of SQLSlammer.

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 CodeRed3 の探索特性
Table 4 Characteristics of CodeRed3.

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

表 5 MSBlaster の探索特性
Table 5 Characteristics of MSBlaster.

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 6 Sasser.B の探索特性
Table 6 Characteristics of Sasser.B.

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 7 Zotob の探索特性
Table 7 Characteristics of Zotob.

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

表 9 ノード探索特性の相関性
Table 9 Correlation among target-searching characteristics.

	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

表 8 Sasser.C の探索特性
Table 8 Characteristics of Sasser.C.

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

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している．

いま，2 つの系列 $x = \{x_i\}, y = \{y_i\}$（$i = 1, 2, \ldots, n$）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．同様にして，V_k，s_k，p_k についても c_V，c_s，c_p を求める．Sasser.C を含むすべてのワーム間の相関係数を**表 9** 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☆．検証を行った結果，Sasser.B と Sasser.C との間で，すべての定量値（c_R, c_V, c_s, c_p）において高い相関性がある．文献 20) 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現れており，本論文で得られたノード探索特性の定量値によっても裏付けることができる．

☆ Nimda.E の DFT 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．

6. おわりに

本論文では，過去に発生したワームに感染したノードによる感染先ノード探索活動の可視化，および定量化を行い，個々のワームに走査範囲，均一性，周期性の観測軸において差異が現れることを確認した．走査範囲の観測軸から，近隣ノードを重点的に探索する Nimda.E や Zotob，MSBlaster などのタイプと，IP アドレス空間を網羅的に探索する SQLSlammer や CodeRed3，Sasser.B などのタイプに分類できる．また，均一性や周期性の観測軸から，SQLSlammer 以外のワームについては，上位オクテットにランダム性が高い傾向を確認できる．さらに，これらの観測軸の定量化を用いたワームの分類から，観測軸がワームのノード探索特性を表現するプロパティとして利用できることを示した．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，たとえば，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，対策の立案や，優先度の決定に活用することができる．

今後の課題としては，複数の特徴をあわせ持つマルウェア間の相関性の検証や，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ている「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

成果であり，関係各位に深く感謝いたします．

参 考 文 献

1) W32.Nimda.E@mm. http://www.symantec.com/region/jp/sarcj/data/w/w32.nimda.e@mm.html
2) CodeRed. http://www.symantec.com/region/jp/avcenter/venc/data/codered_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) 寺田真敏，高田眞吾，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).
6)「Web サーバーフォルダへの侵入」の脆弱性に対する対策（MS00-078）. http://www.microsoft.com/japan/technet/security/bulletin/MS00-078.mspx
7) Index Server ISAPI エクステンションの未チェックのバッファにより Web サーバーが攻撃される（MS01-033）. http://www.microsoft.com/japan/technet/security/bulletin/MS01-033.mspx
8) W32.SQLExp.Worm. http://www.symantec.com/region/jp/sarcj/data/w/w32.sqlexp.worm.html
9) SQL Server 2000 解決サービスのバッファのオーバーランにより，コードが実行される（323875）（MS02-039）. http://www.microsoft.com/japan/technet/security/bulletin/MS02-039.mspx
10) W32.Blaster.Worm. http://www.symantec.com/region/jp/sarcj/data/w/w32.blaster.worm.html
11) RPC インターフェイスのバッファオーバーランによりコードが実行される（823980）（MS03-026）. http://www.microsoft.com/japan/technet/security/bulletin/MS03-026.mspx
12) W32.Sasser.B.Worm. http://www.symantec.com/region/jp/sarcj/data/w/w32.sasser.b.worm.html
13) Microsoft Windows のセキュリティ修正プログラム（835732）（MS04-011）. http://www.microsoft.com/japan/technet/security/bulletin/MS04-011.mspx
14) W32.Zotob.A. http://www.symantec.com/region/jp/avcenter/venc/data/jp-w32.zotob.a.html
15) プラグアンドプレイの脆弱性により，リモートでコードが実行され，特権の昇格が行なわれる（899588）（MS05-039）. http://www.microsoft.com/japan/technet/security/bulletin/ms05-039.mspx
16) A STATIISTIICAL TEST SUIITE FOR RANDOM AND PSEUDORANDOM NUMBER GENERATORS FOR CRYPTOGRAPHIIC APPLIICATIIONS. http://csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501.pdf
17) 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).
18) 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).
19) 寺田真敏：Slammer ワームの感染先探索特定の検討 Rev.1. http://www.doi.ics.keio.ac.jp/~terada/slammer040514.pdf
20) 日立製作所システム開発研究所：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/

(平成 18 年 12 月 6 日受付)
(平成 19 年 6 月 5 日採録)

仲小路博史

2001 年東京理科大学大学院理工学研究科情報科学科修士課程修了．同年（株）日立製作所システム開発研究所入所．PKI ならびに X.509 属性証明書の研究開発に従事．現在はネットワークセキュリティ技術に関する研究開発に従事．

寺田 真敏（正会員）

1986 年千葉大学大学院工学研究科写真工学専攻修士課程修了．同年（株）日立製作所入社．博士（工学）．現在，システム開発研究所にてネットワークセキュリティの研究に従事．2004 年 4 月から JPCERT コーディネーションセンター専門委員，2004 年 4 月から中央大学研究開発機構客員研究員，2004 年 8 月から情報処理推進機構セキュリティセンター研究員を兼務．

洲崎 誠一（正会員）

1991 年 3 月横浜国立大学電子情報工学科卒業．同年 4 月（株）日立製作所システム開発研究所に入所．以来，情報セキュリティ技術の研究開発に従事．日立製作所システム開発研究所第 7 部（セキュリティシステム研究部）主任研究員．博士（工学）．1996 年情報処理学会第 52 回全国大会優秀賞，平成 12 年度山下記念研究賞受賞．