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

2007－DPS－130 (47)
2007－CSEC－ 36 (47)
2007／3／2

ワームのノード探索特性の可視化に関する提案

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．伝播特性のうち，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．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を可視化により示した後，これらの特性を基に，実ワームの分類を試みる．

Proposal for the visualizing method of searching characteristics of node

Hirofumi Nakakoji† Masato Terada† 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. 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 based on the quantified target-search 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，ワームが感染活動を行う際にネットワーク上で示す感染先ノード探索活動や，攻略パケットの送信活動の特徴を表した「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．

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]のようにノード探索間隔の周期性に着目することにより，ワームのノード探索特性に関わる特徴を定義してきた．本稿では，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周期性，走査範囲，均一性を

確認する．さらに，実際のワームについて，可視化により得られたノード探索特性に基づくワームの分類を行い，分布傾向を示す．

本稿の構成について述べる．まず，2章でワームの感染活動の概要を述べた後，3章では，ノード探索特性の可視化を提案する．4章では，可視化を通して既知ワームのノード探索活動の特性を示し，傾向に基づいた分類を試みる．5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原因は，感染拡大活動によるものである．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調査した．本稿では，特に（2）に示した感染先ノードIPアドレスの生成規則の可視化に着目する．

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，探索先ノードの特定の難易度を表す．

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，次の通りである．

- パケットの送信活動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概要を把握するために，ワーム感染ノードがパケットを送信している様子を図3.1に示すように表現し，そこに見られる規則性を把握する．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捉えるために，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に置き換えて表す．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．

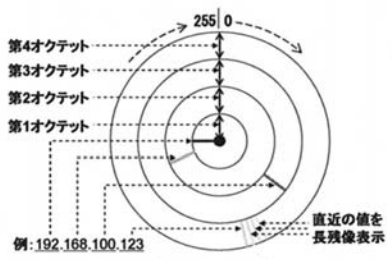

図3.1 規則性の可視化

3.2. 均一性及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及び走査範囲を把握することにある．図 3.2 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，色を寒色系から暖色系に段階的に変化させることで，各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及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 3.3)，ノード探索活動の停止／再開，各オクテットの値の周期的／ランダムな振る舞いを確認する．

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 4.1 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，各ワームの概要を簡単に説明し，規則性の可視化，均一性及び走査範囲の可視化，及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．

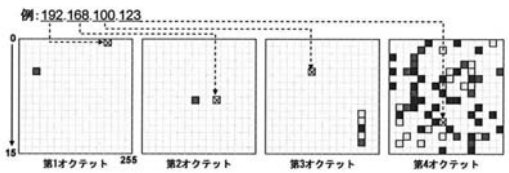

図 3.2 均一性及び走査範囲の可視化

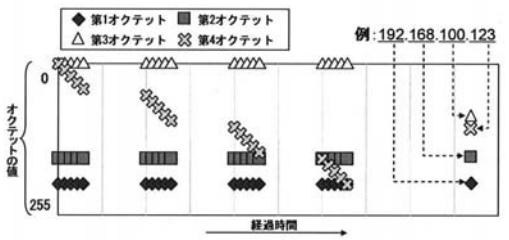

図 3.3 周期性の可視化

表 4.1 主要ワーム

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

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，常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[1]．

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，本稿では，ワームの探索特性の環境として文献[8]に提示された「特殊な装置を使用する必要がない」且つ「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 4.1 に示す．ワーム感染ノード（Infected PC）には Windows2000[2] 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 30bit，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，

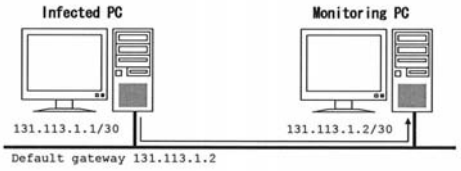

図 4.1 データ収集環境

[1]本稿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．

[2]商品名称等に関する表示

本稿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.の米国及びその他の国における登録商標です．

Linux は，Linus Torvalds の米国及びその他の国における登録商標あるいは商標です．

ワーム感染ノードの送信するパケットのほぼ全て（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[9]）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 4.2 から，Nimda.E が時間の経過と共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一箇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，値の均一性に関しては，図 4.3 の第 1,2 オクテットを表すマトリックスの中央付近に連続的な矩形（縦に並んだ矩形群）を構成しており，オクテットの値の分布に一部偏りが表れている．

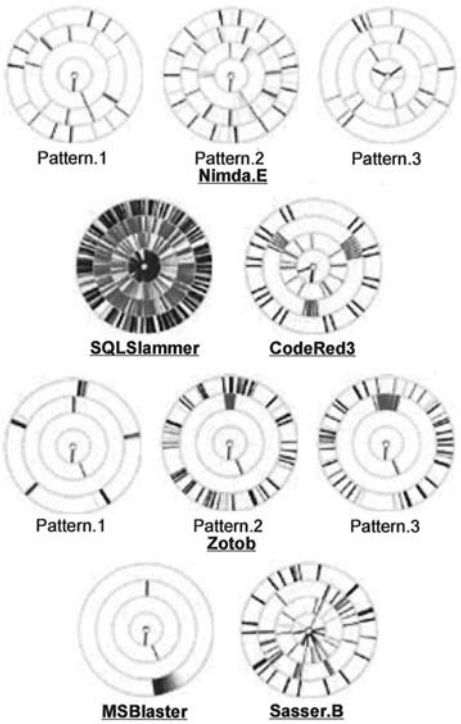

図 4.2 規則性の可視化結果

4.2.2. SQLSlammer

SQLSlammer は，SQL Server 2000 の脆弱性（MS02-039[10]）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 4.2 及び図 4.4 から，全てのオクテットにおいて，走査範囲が広いこと，値の生成規則がランダムであることがわかる．また，図 4.3 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．

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[11])を攻略するパケットを送信する．

CodeRed3 は，図 4.2 及び図 4.3 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わかる．また，図 4.2 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

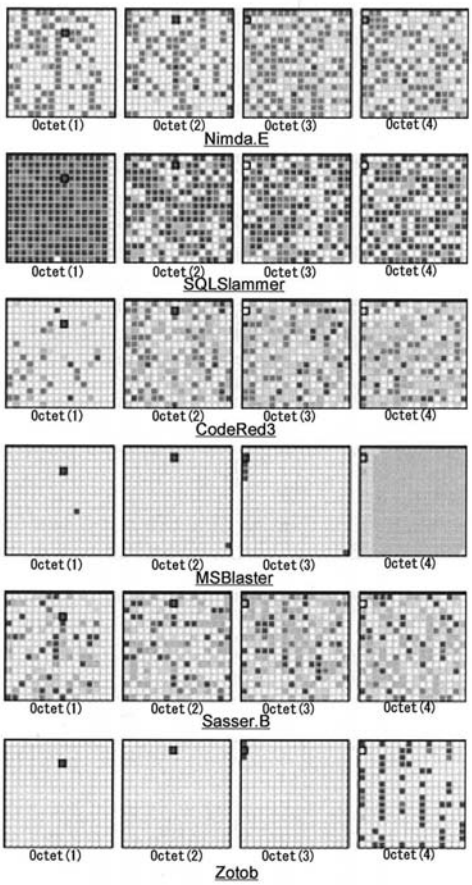

図 4.3 均一性及び走査範囲の可視化結果

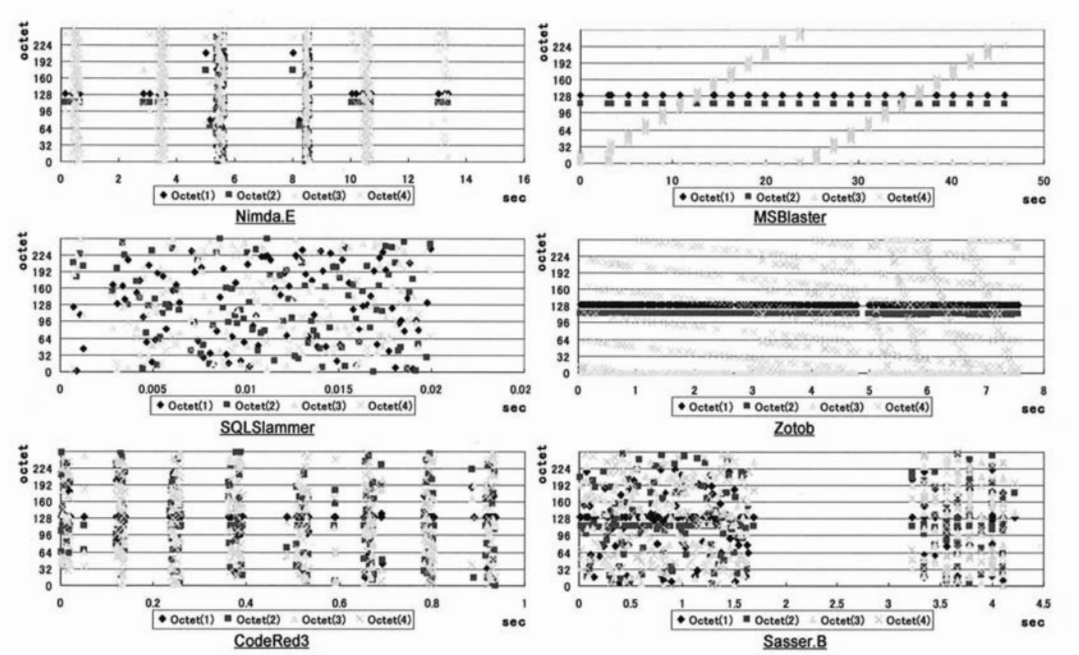

図 4.4 周期性の可視化結果

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[12]）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 4.2 及び図 4.3 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一箇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わかる．また，図 4.4 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[13]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[14]）スキャンを行う．

Sasser.B は，図 4.3 から，全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もっていることがわかる．また，全オクテットにおいてランダムな特性がみられるが，図 4.3 の第 1,2 オクテットに赤（濃）い矩形が 1 点見られること，そして図 4.4 から縦軸中央付近に第 1,2 オクテットを表す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ということがわかる．

4.2.6. Zotob

Zotob[15]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[16]）を攻略するパケットを送信する性質を持つ．

図 4.2 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わかる．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わかる．

Zotob は，図 4.2 のパターン 1 から 3 に見られるように，時間の経過と共に，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. ノード探索特性に基づくワームの分類

これまでの調査により確認したワームの観測軸におけるノード探索の特徴に基づいて，各ワームを2章で述べたランダム性（周期性，均一性）及び走査範囲を軸に定性的に分類した（図 4.5）．

文献[17]では，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．図 4.5 からも同様の傾向を確認できることから，ワームの分類にこれらの可視化は有効であると考えることができる．

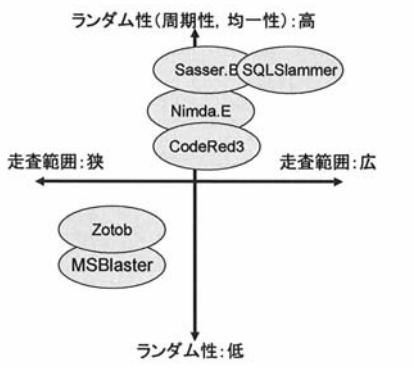

図 4.5 ワームの分類

5. まとめ

本稿では，ワームのノード探索特性の可視化について提案し，6 種類のワームの可視化を行った．まず，図 4.2 に示す規則性の可視化は，Nimda.E や Zotob のように，時間の経過と共に探索パターン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った．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，実際には生成される値に均一性がみられることを，図 4.3 に示す均一性及び走査範囲の可視化から示した．さらに，図 4.2 及び周期性を表す図 4.4 により，Nimda.E の第 3,4 オクテット，MSBlaster の第 4 オクテット，CodeRed3 の第 3,4 オクテット，Zotob のパターン 1 の第 4 オクテットの値に等幅間隔の規則性，つまり周期性の存在を示した．

今後は，本稿で扱った走査範囲，均一性，周期性の各観測軸にみられる特性の定量化を行い，複数のワーム間における類似性の比較や，ノード探索特性を用いた検知技術への適用を行いたい．

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」の成果の一部である．

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 Worm,
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] 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).
[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] 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).
[9] 「Web サーバーフォルダへの侵入」 の脆弱性に対する対策,
http://www.microsoft.com/japan/technet/security/bulletin/MS00-078.mspx
[10] 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,
http://www.microsoft.com/japan/technet/security/bulletin/MS02-039.mspx
[11] 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,
http://www.microsoft.com/japan/technet/security/bulletin/MS01-033.mspx
[12] 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,
http://www.microsoft.com/japan/technet/security/bulletin/MS03-026.mspx
[13] W32.Sasser.B.Worm,
http://www.symantec.com/region/jp/sarcj/data/w/w32.sasser.b.worm.html
[14] Microsoft Windows のセキュリティ修正プログラム,
http://www.microsoft.com/japan/technet/security/bulletin/MS04-011.mspx
[15] W32.Zotob.A,
http://www.symantec.com/region/jp/avcenter/venc/data/jp-w32.zotob.a.html
[16] 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,
http://www.microsoft.com/japan/technet/security/bulletin/ms05-039.mspx
[17]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/