

ICMP 利用型ワーム検出法の提案

佐島 敬真[†] 石井 啓之[‡]

† 東海大学大学院工学研究科 ‡ 東海大学電子情報学部コミュニケーション工学科

〒259-1292 神奈川県平塚市北金目1117

E-mail: †4kepm002@keyaki.cc.u-tokai.ac.jp, ‡ishii@dt.u-tokai.ac.jp

あらまし インターネットが社会基盤として広く用いられている現代社会において、ワーム等の脅威からネットワークの安全性を保つことは重要である。しかし、近年のワーム出現日数の短期化や、種類の多様化に伴い従来のワーム対策手法が有効ではないことがある。本提案では、ワームの感染が拡大する際に発生する ICMP (Internet Control Message Protocol) のトラフィック特性を用いたワーム検出法を提案している。提案システムを実際に運用されているネットワーク内に実装し、有効性を検討している。提案手法を用いることにより、従来の手法では検出が困難であった未知のワームに対する検出が低コスト、低負荷で行えることを明らかにした。

キーワード ワーム, セキュリティ, ICMP

A Proposal of Worm Detection Using ICMP

Yoshimasa SAJIMA[†] Hiroshi ISHII[‡]

† Course of Electrical Engineering, Graduate School of Tokai University

‡ Department of Communications Engineering, School of Information Technology and Electronics, Tokai University

1117 Kitakaname, Hiratsuka-shi, Kanagawa, Japan

E-mail: †4kepm002@keyaki.cc.u-tokai.ac.jp, ‡ishii@dt.u-tokai.ac.jp

Abstract With the rapid proliferation of various types of worms that create different types of threats to the network security in recent years. The conventional worms detection techniques are no longer effective in playing their roles. However, it is important for the contemporary society to protect the network, the Internet, as one of the most widely used social infrastructure nowadays. Therefore, we propose and implement that a worm detection method using the characteristics of ICMP traffic be generated during the spread of the worm's infection. From the implementation, we observe that our proposed techniques are not only low-cost and low-overhead, but also capable in detecting unknown worms as compared to the conventional methods.

Key word worm, security, ICMP

1. はじめに

インターネットによる情報通信が盛んに行われる現代社会において、継続的で安全なネットワークの運営は必要不可欠なものとなっている。しかしながら、悪意のあるユーザによってコンピュータウイルスやワーム、そして不正アクセスなどの脅威が出現しており、ネットワーク管理者は日々様々な手法を用いて対策を行っている[1]。インターネット上に存在する脅威による被害は年々増加しており、総務省の調査によると、平成16年に情報セキュリティに関するなんらかの被害を受けた企業は83.5%と多く、被害内容では「ウイルス感染」が全体の47.8%と最も多かった[2]。ウイルスやワームの感染では、対策だけではなく復旧に伴う

損害も大きくなり、ウイルス感染からの復旧処理には年間約6億円が費やされている。また、感染の拡大に伴って被害者が加害者になる可能性が高く、組織の信頼性を損なう恐れがある。

ウイルス感染による被害が拡大する原因として、ネットワークの拡大や常時接続化、そして回線速度の高速化が考えられる。ネットワークに接続される端末数が増加する近年においては、管理者の予想を超えたネットワークが作り出され、完全な管理は難しいとされる。更に、新しい脅威が短期間に出現する傾向にある現代においては、従来の手法では十分な対策が取れないこともある(表1)[3]。

本提案では、コンピュータ内のプログラムに依存せ

ず自己増殖を繰り返す不正プログラムをワームと定義し、ネットワーク内に流れるトラヒック特性からワーム感染に関する疑わしい問題箇所を早急に検出し、詳細なワーム対策に引き継ぐ手法を提案する。

表 1: パッチ配布日からワーム出現までの日数

| 名称 | パッチ配布日 | ワーム発生日 | 発生期間 |
|----------|------------|-----------|-------|
| SASSER | 2004/4/13 | 2004/4/30 | 17 日 |
| MSBLAST | 2003/7/16 | 2003/8/11 | 26 日 |
| SQLP1434 | 2002/7/24 | 2003/1/25 | 185 日 |
| NIMDA | 2000/10/17 | 2001/9/18 | 336 日 |

2. ワームの感染経路

インターネット上に存在するサービスや OS，そしてアプリケーションの多様化に伴い、ワームの感染には様々な経路が用いられている。以下に代表的なワームの感染経路を示す[3]。

- メールの添付ファイル
- ネットワーク接続によるシステムのセキュリティホールへの攻撃
- WEB ページ観覧
- ファイル共有

の感染では、ワームに感染した端末からメールを受信し、添付ファイルを開くことによってワームに感染する。狭義のウイルスとは異なり、他のプログラムに依存することなく独自のメールプログラムによって増殖するため、ユーザの意思とは関係なくメールが送信され、被害の拡大が早い。の感染では、ネットワークに接続された端末を検索し、OS やソフトウェアの不具合や設計ミスを利用したワーム感染方法である。この感染経路を利用したワームは、システム的设计段階からの脆弱性を利用しているため、セキュリティホールの発見からパッチの配布までに端末が無防備になる危険性がある。の感染では、セキュリティ的に脆弱なサーバ内に悪質なプログラムを仕掛け、web ページ観覧者に感染するものである。の感染では、1つのファイルを複数の端末で共有するシステムを利用してワームを拡大する感染方法である。

ワームの感染方法は、更にユーザの判断や動作を必要とするユーザ増殖型ワームと、ユーザが介入せず自動的にワームの拡散を行う自己増殖型ワームに分けられる。、の感染経路はユーザ増殖型ワームに分類されるため、ユーザの判断によってワーム感染は抑えられるが、の自己増殖型ワームでは、ユーザの意思とは関係なく増殖が行われるためワーム感染の速度が速い。

本提案では、ユーザの意思に依存せず自己増殖を繰

り返す の感染経路によるワーム感染の検出法を提案する。

3. 既存のワーム検出法と求められる機能要件

3.1. ワーム検出法

ワーム感染の拡大を防止するために様々な手法が用いられている[4]。

(a)パターンマッチング方式

パターンマッチングによるワーム検出法では、アンチウイルスソフトや IDS (Intrusion Detection System) に代表されるように、予めワームの特徴とプログラムコードを定義して検出する方法である。パターンマッチングによる検出法では、定義されているワームのパターンには確実に対処できるが、定義ファイルが最新でない場合や、未知のワームには対応できない欠点がある。

(b)ルールベース方式

ルールベース方式は、ワームの活動や特定のアプリケーションの振る舞いを分析してルール化し、ワーム感染を検知する方式である。ルールベース方式では、未知のウイルスに対応できる利点があるが、監視対象のトラヒック中のパケットを全て収集して分析することから、装置の負荷が上昇するため広帯域への適用が問題となる。また、ネットワーク状況の正常時と異常時を判定する閾値の設定に専門的知識や学習時間が必要なため、困難とされている。

(c)ARP 利用型ワーム検出法

ARP 利用型ワーム検出法[5]では、端末に感染したワームが、次感染先を検索するために送信する ARP (Address Resolution Protocol) を利用する。ARP 利用型ワーム検出法では、定義ファイルやシグニチャに非依存であり、(a)と(b)の問題点を克服している。しかし、同一サブネット内に対するワーム検出を目的としているため、同一サブネット以外に感染を広げようとするワームに関しては検出が困難である。

3.2. 求められる機能要件

ワーム感染は端末をネットワークに接続することによって行われるため、ワーム検出を行うシステムは様々なネットワーク環境に導入される必要がある。ワーム検出を行うシステムの導入が広く一般的に行われるためには、以下の機能要件が求められる[5]。

- () 低コスト
- () パターンファイルに非依存
- () 自動でワームを検出可能
- () 高精度でワームを検出可能
- () リアルタイムでワームを検出可能

本提案方式では、これらの機能要件の全てを満たすワーム検知システムを目指す。

4. 提案方式

ここでは、組織内部から外部へ対するワームの二次被害を防ぐため、LAN内に接続されている端末のワーム感染検出を目的とし、既存の手法とは異なりICMPを利用したワーム検出法を提案する。

4.1. 提案方式の原理

今回提案するワーム検出法では、ワームが感染対象とする端末を検索するために送信するICMP echo requestと、その返答であるICMP echo replyのトラフィック特性によってワームを検出する。通常では、ICMP echo requestはユーザの意思によってICMP echo replyが期待される端末に送信されるため、ICMP echo request数に対するICMP echo reply数は1対1、またはそれに近い状態になると予想される。ワームは感染を拡大する際に、ランダムなIPアドレスを生成することが知られている[6]。2005年7月の時点で世界に存在するインターネット上のホスト数は353,284,187個[7]で、IPv4アドレス空間におけるアドレス数4294,967,296個に対して8.23%に過ぎない。したがって、ワームがランダムなIPアドレスを生成し、ホストに対してICMP echo requestを送信した場合、送信先に対して到達不可能を意味するICMP Destination Unreachableが返信される確率が高い。よって、ICMPトラフィックを監視することによってワームに感染している端末の有無が判断できると思われる。

4.2. 提案方式の有効性

ICMPのタイプ別によるトラフィック特性を利用したワーム検出法では、従来の方法で必要であったパターンファイルが不要なため、未知のワームに対して有効である。また、ネットワーク内を流れるトラフィックから特定のトラフィックのみを監視対象とするため、監視装置に高負荷を与えずデータファイルが記憶デバイスの容量を圧迫することなく長期観測が可能である。

4.3. 提案方式の実装

提案方式を導入したシステムをネットワーク内に実装し、評価を行った。今回のICMPトラフィック特性の測定では、クラスCのプライベートネットワークを利用し、図1のように組織内部と外部がやりとりするトラフィックを全て収集できる位置にICMP監視サーバを設置し、測定を行った。ICMP監視サーバにはFedora Core1がインストールされた端末(メモリ 256MB, CPU733MHz)を使用し、10月1日から1週間、11月1日から1週間、12月1日から1週間の3期間においてICMPトラフィックの測定を実施した。また、ICMP監視サーバ内ではPerlスクリプトによって、ネットワ

ーク内を流れるデータから自動でワーム検知に必要なデータを分析、識別し、LANからWANへ対するICMP echo request数と、WANからLANへ返信されるICMP echo reply数、ICMP Destination Unreachable数から組織外部に対するICMP echo requestに対するICMP成功率を算出する。以上の流れを図2に示す。このように算出された結果は定期的に更新されるため、リアルタイム性を有すると考えられる。

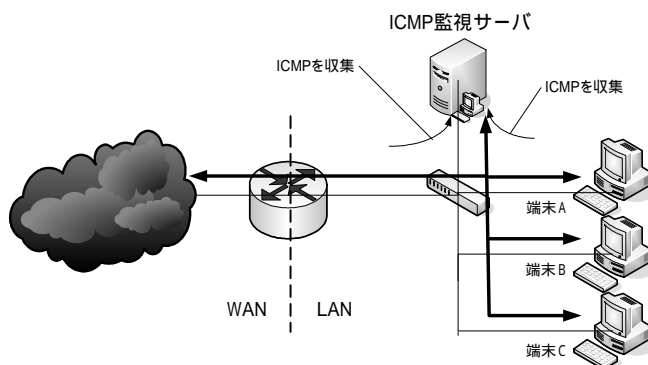


図1: 実験ネットワーク構成図

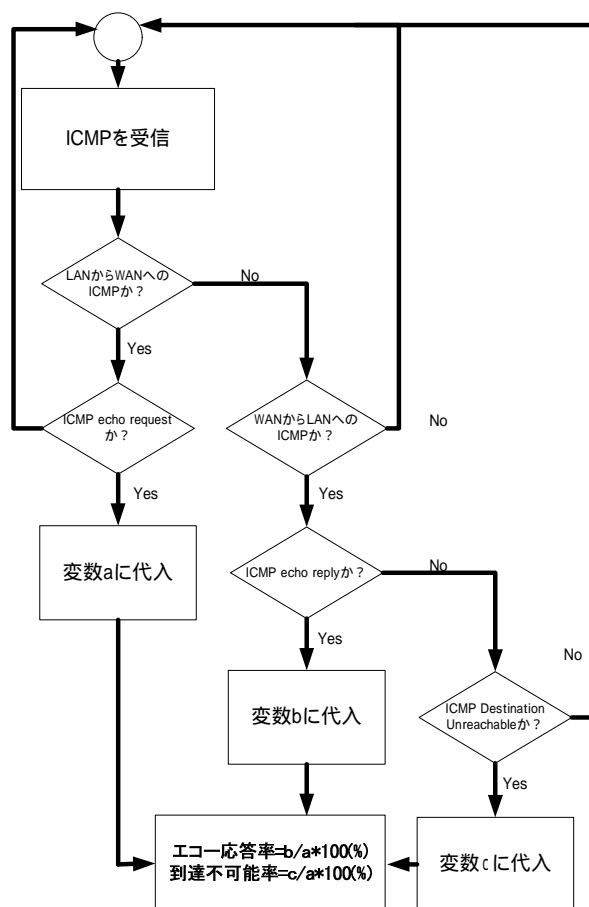


図2: データ処理フローチャート

5. 評価

本提案では、従来のワーム検出法との比較に加え、3.2 で述べたワーム検出に求められる機能要件について評価を行い、本提案方式がワーム検出に対して有効であるかを考察する。

5.1. 測定結果

表 2 において、3 測定期間中における組織内部の ICMP トラヒックの測定値を示す。

表 2：各測定期間中における ICMP パケット量

| 測定期間 (2005 年) | 10/1-10/7 | 11/1-11/7 | 12/1-12/7 |
|--------------------------------|-----------|-----------|-----------|
| 稼働端末数 ¹ | 33 | 34 | 53 |
| ICMP echo request 数 | 120960 | 54 | 13 |
| ICMP echo reply 数 | 10 | 54 | 12 |
| ICMP Destination unreachable 数 | 120950 | 0 | 1 |
| ICMP 返答率 (%) | 0.008 | 100 | 92.3 |

(¹ 稼働端末数の計測では、測定期間内にネットワーク内に流れる ARP を収集し、分析することによって求めた)

表 2 の 10 月 1 日から 7 日までの測定期間においては、他の期間に比べて ICMP 返答率が極端に少ないことがわかる。調査の結果、組織内ネットワークに接続された 1 台の端末から、定期的に外部の特定ホストに対して ICMP echo request を送信したためであることがわかった。端末を検査したところ、この端末にワーム感染は認められなかったが、通常の業務では使用することがないソフトウェアが稼働していることが判明した。結果的にはワーム感染によるワーム拡大の動作ではなかったが、外部のホストに対して不必要な接続を試みていたことは事実である。ICMP echo request を外部に大量送信していた端末から、不必要なソフトウェアを除去した後の測定結果では、ICMP echo request に対してほぼ 100% の ICMP echo reply が確認された。これらの ICMP echo request は、端末所有者から組織外部に対するネットワークの疎通を調べるため意図的に出されたものであったため、異常な ICMP トラヒックでないと見える。また、ICMP 返答率は組織内部の端末数に関係なく 1 対 1 かそれに近い値であることから、本提案方式は端末数の増減に依存することなく異常トラヒックの検出が可能である。この結果から、4.2 で述べた通り ICMP echo request 数と ICMP echo reply の関係

は、通常のネットワーク運営において 1 対 1 の関係が成り立つことがわかった。

表 3：ネットワーク内 ICMP トラヒック量

| 測定期間 | 2005/12/1-12/7 |
|----------------------|----------------|
| ネットワーク全体トラヒック量 | 658MB |
| ICMP 総パケット量 | 13.02MB |
| 監視対象 ICMP echo パケット量 | 12.58KB |

表 3 では、組織内ネットワークでやり取りされている全体のトラヒック量と、ICMP のみに注目した場合の監視トラヒック量の違いについて示している。3 つの測定期間の中で最も稼働端末数が多かった 12 月 1 日から 7 日において、組織内部と組織外部でやり取りされるすべてのトラヒック量を監視したところ 658MB となった。また、組織ネットワーク内外でやり取りされるすべての ICMP タイプを監視したところ 13.02MB となり、長期の監視を行う場合には従来のルールベースのようにトラヒック中の対象パケットを全て収集してから分析を行う手法には不向きであるといえる。しかし、提案方式では予め収集するトラヒックの種類を組織ネットワーク内から外部へ対して発生する ICMP echo request と、それに応答する ICMP echo reply に限定しているため、全てのトラヒックを収集する場合に比べて約 0.002% という極めて少ないデータ量で測定が可能であることがわかる。

5.2. 求められる機能要件に対する考察

今回の ICMP トラヒックの測定結果を基に、3.2 で述べたワーム検出に求められる機能要件について考察する。

() 低コスト

今回の実装結果表 3 より、本提案システムでは特定のトラヒックのみを測定対象とするため、データの記憶装置は極めて小さな容量で目的を達成できることが確認できた。また、ICMP はほぼ全てのネットワーク機器が対応しているため、新たな対応機器を揃えることなく低コストで本システムを稼働開始することができる。

() パターンファイルに非依存

本提案方式では ICMP を用いたワーム検出法を提案した。項目 1. で述べたように、ネットワークを通じてワーム感染を広げることはワーム感染拡大の特徴のひとつである。感染候補を検索するために送信される ICMP をワーム検出対象とすることによって、ワームの種類に関係なく検出が可能であるため、従来のような定義ファイルを事前に準備し、定義ファイルを最新

に保つ必要があり、未知のワームに対しても有効である。

() 自動でワームを検出可能

図 2 の測定手順より、ICMP 監視サーバによって収集されたデータは自動で ICMP のタイプを識別し、ICMP echo request 数に対する ICMP echo reply 数の割合を算出する。したがって、ネットワーク管理者が直接収集されたデータを基に判断を行わないので、自動検出が可能である。

() 高精度でワームを検出可能

表 2 より、ネットワーク内において、通常は ICMP の echo の要求と返答は 1 対 1 であるため、従来のシステムで必要であったトラフィック特徴の学習期間や閾値設定が不必要であることがわかる。しかし、正常なネットワーク運営においても ICMP echo request に対する返答が無い場合も十分考え得ることであるため、ワームによる異常トラフィックであると判断する時間的区間と計測数の閾値に関する検証が必要である。

() リアルタイムでワームを検出可能

本提案のワーム検出法の測定手順では、刻々と変化する ICMP トラフィックの特性を常時観測し、リアルタイムで ICMP echo request に対する ICMP echo reply と ICMP Destination Unreachable の割合を算出しているため、リアルタイムにワームを検出可能であるといえる。

5.3. 提案方式の応用

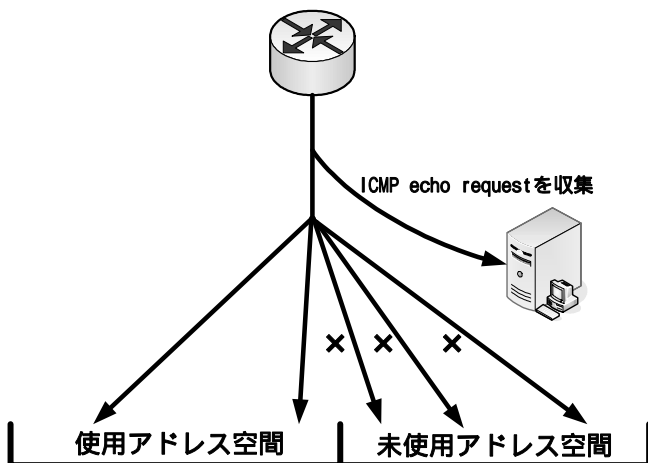


図 3：組織内部に対するワーム検知

今回の実装では、組織内部ネットワークでワーム感染した端末から、組織外部に対する二次的被害の拡大を想定したワーム対策システムを提案した。しかし、今回のシステムを応用することによって、組織外部から内部に対するワーム感染も検知することが可能であると考えられる。通常、ネットワークを運用する際は、ネットワーク管理の都合上管理者によって組織内で使用される IP アドレスの範囲が限定されることが多い。

そのようなネットワーク運用をする場合、管理者がユーザに割り当てた IP アドレス以外に対する ICMP echo request を監視することによって外部から組織内部に対するワーム感染を試みているかを判断することができると思われる(図 3)。

6. まとめ

本提案では、正常な通信の結果生じた ICMP のトラフィックとは異なり、ワームの感染から引き起こされるトラフィック特性に着目し、ICMP を利用したワーム検出法を提案した。提案システムの実装を通じ、その有効性を明らかにすると共に、システムの応用例を示した。本提案方式では、3.2 で示したワーム検知システムに求められる機能要件を全て満たすことを目標とした。しかし、高精度の検出に関しては正常な ICMP パケットと、異常 ICMP パケットの判別には更なる検討が必要である。今後の課題として、ICMP 測定時における時間的区間を設定し、正常時と異常時を識別する新たな閾値の決定を行う必要がある。通常、ICMP を用いた通信の確認は特定のホストに対して一定時間内に終了する。したがって、閾値の決定では通信の疎通確認に支障が起らない時間的区間を設定することによって実現できると考えられる。

文 献

- [1] IPA (情報処理推進機構) “国内・海外におけるコンピュータウイルス被害状況調査”
http://www.ipa.go.jp/security/fy16/reports/virus-survey/documents/2004_virus_domestic.pdf
- [2] 総務省 “情報通信白書平成 17 年度版”
<http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h17/pdf/index.html>
- [3] 情報セキュリティ対策講座
<http://itpro.nikkeibp.co.jp/as/tm/solution18/index.html/>
- [4]トレンドマイクロ社 “ウイルス検出技術”
<http://www.trendmicro.com/jp/security/general/tech/overview.htm/>
- [5] 波戸邦夫 “ワーム検出方法 Worm Sonar の提案” 信学技報 IN2004-31, pp.25-30, July, 2004
- [6] Internet System Consortium “Internet Domain Survey”
<http://www.isc.org/index.pl/?ops/ds/>
- [7] IT pro “新種ワームが感染を拡大中(2003 年 8 月 23 日)”
http://itpro.nikkeibp.co.jp/free/ITPro/NEWS/20030820/1/?ST=itpro_print/
- [8] 藤井聖, 中村豊, 藤川和利, 砂原秀樹 “通信先ホスト数の変化に注目した異常トラフィック自動検出法の提案と評価” 電子情報通信学会論文誌 B, Vol. J88-B No.10, pp.1922-1933, Oct, 2005
- [9] RFC792 “Internet Control Message Protocol”