2005－ＣＳＥＣ－30（５）
2005／7／21

検疫ネットワークを評価するための実ウイルスを用いた検証環境の考察

田中　修　　内田 勝也
情報セキュリティ大学院大学　情報セキュリティ研究科
〒221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1
E-Mail:{ mgs041503, uchida}@iisec.ac.jp

概要　2001年以降 CodeRed のようなコンピュータウイルスが短時間で大規模に感染を拡げるようになってきている。このようなコンピュータウイルスの被害は、個人や組織だけの問題だけにとどまらず、インターネットを介して様々なところに大きな影響を与えている。このような状況に対して、従来の対策方法のウイルス対策ソフトだけでの対策では対応しきれないのが現状である。このため、今後管理者が能動的にコンピュータウイルス対策を実施していくための一手法である検疫ネットワークが注目され始めている。

効果的な検疫ネットワークを構築するためには実際の検証が必要である。このため本稿では、コンピュータウイルスがネットワークにどのように拡散するかを確認するため、2003 年に猛威を振るった Slammer を感染・発症させる環境を構築して評価することで、検証環境の精度と課題について考察する。

キーワード：　ウイルス検証環境、仮想 OS、検疫ネットワーク、Slammer

Evaluation of the quarantine system using "in the wild" viruses

OsamuTanaka　Katuya Uchida
Institute of Information Security University
2-14-1 Tsuruyacho Kanagawa-ku Yokohama-City, JAPAN 221-0835
E-Mail:{ mgs041503, uchida}@iisec.ac.jp

Abustract　Computer virus such as CodeRed comes to widen infection on a large scale in a short time after 2001. The damage of such a computer virus is not confined to only an individual and a problem only for an organization and I go through Internet and give various places big influence. For such situation, it is the present conditions by measures only by anti-virus measure software of conventional measures method that cannot finish coping. On this account the quarantine inspection network which is the only thing method for a manager to carry out computer virus measures actively begins to attract attention in future. Real inspection is necessary to build an effective quarantine inspection network. On this account I consider precision and a problem of inspection environment to confirm how computer virus spreads by this report in a network by I build environment to let you develop infection, and evaluating Slammer which raged in 2003.

はじめに

ADSL を始めとする xDSL を利用した高速でしかも安価なブロードバンド通信の基盤として急速に普及し始めたため、個人でもインターネットへの常時接続が広まり、利便性を享受できる環境が整いつつある[1]。このような利便性が向上した一方で常時接続によりコンピュータウイルス（以下 ウイルス）や不正アクセスの被害が急激に増加し、どのように対応すべきかが社会全体の問題となっている。独立行政法人情報処理推進機構（以下、IPA）が発表しているウイルスや不正アクセス届出件数の資料[2][3]の図 0-1 および図 0-2 からもわかるように、ウイルスや不正アクセスに対する何らかの対策はコンピュータを利用する上でもはや無視できず、しかも必須のものとなってきている。

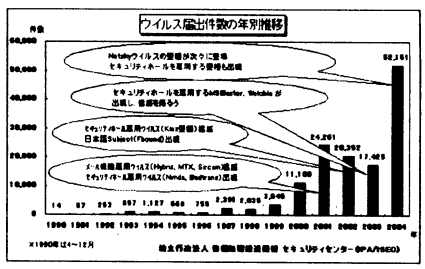

図 0-1 ウイルス届出件数の年別推移(出典 IPA)

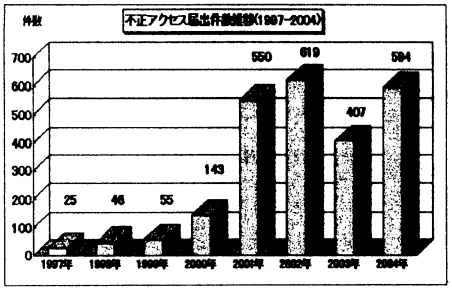

図 0-2 不正アクセス届出件数推移(出典 IPA)

2001 年の CodeRed[4]以来、ウイルスが大きな社会問題になり始め、SQL Slammer(以下 Slammer)[5]発生時には、韓国のインターネットのバックボーンに影響をあたえ、米国でもインターネットを使った予約システムや ATM が利用できなくなるなど、単に感染した組織にとどまらず、インターネットのネットワーク基盤に大きな影響を与えた。Slammer のような短時間でしかも大規模に感染する可能性がある“Warhol Worms”[6]の発生は考えられてはいたが、対応策が十分考慮されていない状況で実際に発生したことで、対応が急務であると認識された。こうした状況から、現在企業や個人が行なう対策として大きく 2 つの方法が普及してきた。1 つは利用しているコンピュータに対してウイルス対策ソフト（以下 ワクチン）を導入し、常に最新の状態を保つ方法であり、もう 1 つはインターネットと利用している LAN[1]との境界にあたるゲートウェイ部分にウイルス対策のシステムを導入する方法である。しかし残念ながらウイルス対策として考えられる方法を行なっているにもかかわらず、ウイルスに感染してしまう事故が後を絶たない現状がある[7]。

第 1 章 最近のウイルスの現状

1.1 ウイルスの概要

ウイルスは、第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、「自己伝染機能」、「潜伏機能」、「発症機能」の 1 つ以上の機能を有するものと定義されている[8]。従来は感染方法や自己増殖の有無により「ウイルス」、「ワーム」、「トロイの木馬」などに分類していた。しかし、最近のウイルスは様々な機能を有しているために明確な分類をすることができなくなってきている。このため、本稿ではこれらの有害プログラム[9]の総称をウイルスとして扱う。

1.2 ウイルス感染経路

ウイルスが感染を拡げていく方法として、COM/EXE/SYS などの拡張子を持つファイルに感染し EXE や COM 等の実行時に感染を拡げていくファイル感染型、マイクロソフト社の Office 製品のマクロ機能を利用して感染を拡げるマクロウイルス型、実行することでウイルスに感染するファイルを電子メール(以下 メール)に添付して感染を拡げていくメール添付型、利用者の心理を狙って感染を拡げようとするソーシャルエンジニアリング型やプログラムに存在する不具合を利用してウイルスの感染を拡げるセキュリティホール型などがある。

CodeRed のようなウイルスが発見される 2001 年頃までは、フロッピーや CD-ROM 等のメディアやメールを介してウイルスに感染していた。しかし最近では、それぞれの機能を併せ持った複合型ウイルスが主流になってきおり、ネットワークを介して短時間でより多くのコンピュータに感染するようになってきている。

1.3 ウイルス感染理由

コンピュータがウイルスに感染する主な理由は、以下が考えられる。

① 利用者がウイルス感染に対して脅威を感じていないためにウイルス対策を実施しないため。
② 通常ワクチンのほとんどがウイルス定義ファイル(以下 パターンファイル)と呼ばれるウイルス情報と比較してウイルスに感染しているか判断している。この方法は、既知ウイルスは検出できるが、未知ウイルスは検出できない。このため日々発生する新種のウイルスへの対応が遅れてしまうため。
③ 最近のウイルスは OS やアプリケーションに存在するセキュリティホールと呼ばれる脆弱性を利用して感染を拡大している。従来はセキュリティホールが発見されてからウイルスの攻撃に利用されるまで、数ヶ月以上の期間があったが、最近はセキュリティホール発見後すぐにウイルスの攻撃に利用される、いわゆる「ゼロデイアタック」が多くなってきたため。

さらに、最近発見されるウイルスはネットワークを介して短時間で多くのコンピュータに感染する仕組みを備えているため、上記の点に配慮しながら管理、運用しなければウイルスに感染してし

[1] Local Area Network：ここでは、規模にかかわらずインターネットに直接接続していない内部のネットワークとする

まう可能性がある。

1.4 ウイルスの対応方法

一般的なウイルス対策の方法として、利用するコンピュータにワクチンを導入し、常に最新の状態にしておくことである。ワクチンを導入しておくことで、常にウイルスに感染していないかのチェックができる。さらに企業等で多くのコンピュータを利用している場合には、リスク管理の一つとしてウイルス対策があり、確実に管理するために、通知・駆除・削除・管理・設定・パターンファイルの自動更新等の機能が必要になってきており、実際の企業用の製品においてはこれらの機能が一般化している。

一般化してきた理由としては、パターンファイルの更新頻度について考えてみると、図 1-1 に示すように最近ではほぼ毎日パターンファイルが更新されている。これは利用者各自がパターンファイルを更新し、管理者がそれぞれのコンピュータの実施状況を確認することは、両者への負担が大きくなり実用的でないことから当然の流れといえる。

年	更新回数	平均更新間隔	備考
2001 年	87 回	4.20 日	
2002 年	116 回	3.15 日	
2003 年	142 回	2.57 日	
2004 年	215 回	1.70 日	
2005 年	177 回	0.93 日	2005/06/14 まで

図 1-1 トレンドマイクロ社のウイルス対策製品のパターンファイル更新状況（[10]より作成）

しかし、最近では脆弱性を利用して感染を拡大させるものが増加してきた。脆弱性を利用したウイルスは、メモリ上で実行され感染を拡大するものがあり、この場合ワクチンでは発見ができないという問題がある。2003 年に多くの企業で被害にあった Slammer や MSBlast[11]はまさに、この点を狙ったものであった。

脆弱性を利用したウイルスは、実行メモリ上でウイルス活動を行なうため、現在のワクチン機能では発見できないことが多い。この様なウイルスへの有効な対策は、脆弱性に対するソフトウェアベンダが推奨する更新を適用し、脆弱性を修復することである。しかし、現在利用しているアプリケーションに不具合が発生し支障をきたすといった懸念やベンダが推奨する更新する作業の手間を理由に一部の利用者が行なわないことがある。また、最近では、可搬型コンピュータに普及により、管理の徹底ができていないコンピュータの存在があげられる。

このようにウイルスや利用環境の変化に伴って、LAN のネットワーク機器側で、利用者からの LAN の利用制限を行なう検疫ネットワークの考え方が出てきた。しかし検疫ネットワークは新しい技術であるため、提供している会社によって検疫方法が異なるなど必要要件の定義がなく、構築にあたっては有効な設定をどのように行なうかの一般的な方法がない状態である。このため検疫ネットワークを構築して、有効に機能しているかを確認するためには、実証実験が必須な状況である。

第 2 章 ウイルスの発症検証環境

実ウイルスを用いて、感染・発症する際の考慮点として、1 つはオペレーティングシステム（OS）やアプリケーションプログラムのバージョンやセキュリティパッチの適用状態によって感染・発症の状態が変化してしまう点、もう 1 つはウイルスの挙動を確認するために、繰り返し検証を行なうために感染・発症するコンピュータの条件を毎回合致させることが必要な点がある。

検証環境において、特に OS の挙動が一定ではなく実行するたびにその挙動が変化してしまうような環境では、検証結果が異なってしまう。このため同一環境を用意した上で、同じでテストできる環境は必須である。しかしここで同一環境をどのように用意するかが問題になる。ツール等を利用しなかった場合には、同じ環境を用意するために、毎回 OS の導入・パッチの適用や詳細な設定を毎回行なうことになる。この場合、通常 OS のインストールから詳細な設定までに数時間かかってしまう。さらに詳細設定においては、手動で行なう部分が多数あるため注意を払っていても設定ミスを起こす可能性がある。仮にこのような条件を解決できたとしても、繰り返し検証を行なう場合には、環境構築に多くの時間をとられることになり、検証において実用的でないと判断した。別の方法としては、バックアップソフトを利用してバックアップ/リストアする方法がある。同一環境に復元することができるが、複数の手順を行なわなければならない点や使用するバックアップソフトによって復元の時間がかかり、実用的でないと判断した。別の方法として、ハードディスク(以下 HDD)のクローニングを行なう方法がある。同一環境（HDD のクローニングの状態を作成した時点）に復元するには、1 つの手順で戻すことが可能であり、今回検証を行なう環境を復元するための所要時間は、10 数分で復元ができ、検証において実用的と判断でした。 このた

め、通常の利用環境と同じこの環境を本稿では、実環境として扱う。

さらに、検証を実施するに当たり実環境だけで不足がでてきてしまう。この点を補うため、仮想マシンを作成するツールを利用して検証する方法を利用することとした。この方法は、1台のコンピュータ上に複数のOSを実行するもので、仮想マシンとして導入したOSは、1つのファイルとなり、このファイルをバックアップ/リストアすることで、同一の環境を復元できるメリットがある。ただし、1台のコンピュータ上に複数のOSを導入するため、パフォーマンスの劣化が避けられないという欠点がある。

上記の内容を踏まえた上で本稿では、感染させるコンピュータのHDD全体の内容をイメージファイルとしてバックアップをとる方式、感染させるコンピュータを仮想OSとして1ファイルにしてしまう方式の2種類の方式を用いて検証することにした。なお、2種類の方式を実現するためのツールとして、実環境では、Symantec社のLiveState Recovery Desktop 3.0[12]、仮想環境では、VirtualPC2004[13]及びVMware 5.0 Workstation[14]を利用した。

2.1 検証環境のシステム構成

図 2-1 に示した検証環境を構築し、実際にSlammerの感染状況の確認を行なった。

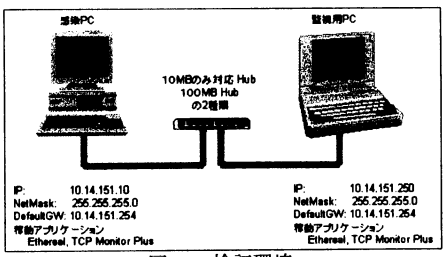

図 2-1 検証環境

(1) 感染PC (Windows 2000)

ウイルスの実行稼動環境として、SP4適用の日本語版 Windows2000 Professional(以下 実環境と言う)、SP4適用の日本語版Windows2000 Professional上のVirtualPC2004にSP4適用の日本語版Windows2000 Professional環境(以下 仮想環境-VPCと言う)、SP4適用の日本語版Windows2000 Professional上のVMWareWorkStation5にSP4適用の日本語版Windows2000 Professional環境(以下 仮想環境-VMWと言う)の3種類の環境を準備した。

(2) モニタ装置 (Windows XP)

ネットワークの負荷状況を確認するために、Ethereal、TCP Monitor Plusを利用した。[2]

2.2 実環境の構築

実環境は、検証で得られる結果がそのまま結果となる点でわかりやすいものである。環境構築においては上記でも述べたとおり、毎回同一の条件で検証環境を利用するため、検証する機器のHDD全体をイメージファイルとしてバックアップし、復元できる環境を構築した。

環境構築にあたり、イメージファイルの作成は、10数分程度で完了でき、復元も検証実施時と同一環境を10数分程度で構築(復元)できた。

2.3 仮想環境の構築

仮想環境は、検証で得られる結果と実環境で得られる結果との差異を比較した上で判断しなければいけない点がある。環境構築においては上記でも述べたとおり、毎回同一の条件で検証環境を利用するため、検証するコンピュータ上に仮想マシンを構築して、仮想OSを1つのファイルとして、バックアップし、復元できる環境を構築した。

環境構築にあたり、イメージファイルの作成は、10数分程度で完了でき、復元も検証実施時と同一環境を10数分程度で構築(復元)できた。

第3章 Slammerの検証結果

2003年に猛威を振るったSlammerを用いて実際に脆弱性を利用したウイルスがネットワークにどのような負荷を与えながら拡散するかの挙動を確認するため、以下の条件で検証を行なった。

検証項目

・コンピュータのネットワークカードのリンクスピードを10MB/100MBのそれぞれの設定によって、感染速度に変化があらわれるのか

・コンピュータの搭載メモリの容量を256MB/512MB/1GBによって感染速度に変化があらわれるのか

・仮想環境-VPC、仮想環境-VMWのそれぞれの仮想環境上のOSで、実環境と同じ条件で検証した場合に、感染速度に変化があらわれるのか

の各項目ごとに検証を行ない、実環境での検証結果は 表 3-1 実環境での計測結果、仮想環境-VPC検証環境での計測結果は 表 3-2 仮想環境

[2]本稿で記載している会社名・製品名は、それぞれの会社の商標もしくは登録商標

-VPC 検証環境での計測結果、仮想環境-VMW での検証結果は表 3-3 仮想環境-VMW 検証環境での計測結果にそれぞれまとめた。

実環境

NICのLinkSpeed設定　10MB Half

	搭載メモリ		
	256MB	512MB	1GB
1秒当りの送出パケット	29.41	30.95	31.1

NICのLinkSpeed設定　100MB Half

	搭載メモリ		
	256MB	512MB	1GB
1秒当りの送出パケット	7971.45	7223.48	7452.32

表 3-1 実環境での計測結果

仮想環境 - VirtualPC2004

HostOSのNICのLinkSpeed設定　10MB Half
GuestOSのNICの設定:LinkSpeed設定　Auto

	搭載メモリ		
	128M	256MB	512MB
1秒当りの送出パケット	34.48	33.22	33.41

HostOSのNICのLinkSpeed設定　100MB Half
GuestOSのNICの設定:LinkSpeed設定　Auto

	搭載メモリ		
	128M	256MB	512MB
1秒当りの送出パケット	752.04	752.96	722.18

表 3-2 仮想環境-VPC 検証環境での計測結果

仮想環境 - VMWare

HostOSのNICのLinkSpeed設定　10MB Half
GuestOSのNICの設定:LinkSpeed設定　Auto

	搭載メモリ		
	128M	256MB	512MB
1秒当りの送出パケット	2807.3	2812.4	2829.08

HostOSのNICの設定:LinkSpeed設定　100MB Half
GuestOSのNICの設定:LinkSpeed設定　Auto

	搭載メモリ		
	128M	256MB	512MB
1秒当りの送出パケット	4826.02	5034.28	5127.07

表 3-3 仮想環境-VMW 検証環境での計測結果

さらに実環境において、感染したコンピュータからの通信パケットの送出状況の結果を、ネットワーク伝送速度 10MB の場合は図 3-1、ネットワーク伝送速度 100MB の場合は図 3-2 に示す。

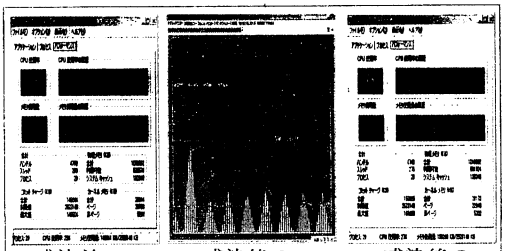

図 3-1 ネットワーク伝送速度 10MB の場合

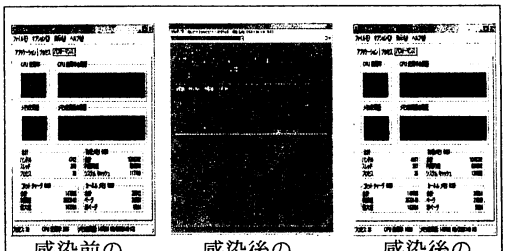

図 3-2 ネットワーク伝送速度 100MB の場合

検証の結果、実環境の Slammer に感染したコンピュータが 1 秒間に送出する UDP パケットは、10Mbps の LAN 環境で感染 PC の CPU 使用率は 25%で、平均で約 33 個、100Mbps の LAN 環境で感染 PC の CPU 使用率は 100%の高負荷状態を維持したまま 1 秒あたり約 7,600 個のパケットが送出された。実環境において Slammer は約 400 バイトのパケットを送出することから、100Mbps の LAN 環境で、転送効率を考えない理論値の場合で、一秒あたり最大 31,250 パケットの送出が可能である。このことを踏まえて収集したデータの有効性について検討すると、この理論値に近い結果を警察庁が公開[15]している。

警察庁の調査では、Slammer に感染したコンピュータが 1 秒間に送出する UDP パケットは、100Mbps の LAN 環境で平均約 24,305 個、10Mbps の LAN 環境では平均約 2,819 個が送出されており、本調査と比較すると大きな開きが出ている。さらに、また仮想環境においては、VMWare を利用しての Slammer に感染したコンピュータが 1 秒間に送出する UDP パケットは、200 個が送出されているとの報告[16]がある。

これらの相違については、実環境においては、送出されるパケットの傾向として CPU やメモリ

といったものより、ネットワーク環境に大きく依存することが確認できた [15] 。このため、ネットワークがより高速になると、被害はさらに大きくなる可能性があると推測できる。さらに、ウイルスが利用するプロトコルとして、TCP プロトコルを利用するウイルスは、プロトコル仕様としてコネクションを確立する必要があるため、コネクションが確立できない場合、TCP タイムアウトを待つ必要がある。一方、UDP プロトコルを利用するウイルスではコネクションを確立する必要がないため、タイムアウトが発生せず、CPU や回線帯域といった物理的な範囲内では最速で感染する。このため、ネットワークがより高速なものになり、UDP プロトコルを利用し、しかも MSBlast のように利用されている台数の多いものに着目したウイルスが発生すると、Slammer での被害よりもはるかに大規模な被害になることが容易に推測できる。

第 4 章 課題

検証に対する今後の課題として、ネットワーク環境を再度検証するとともに、今回視覚化目的のソフトを利用せず、送出パケットの取得方法等を変更しながら、実験を繰り返して検証の精度を高めたい。

上記の実験から、ウイルスに感染する速度が数分から数時間の間に速まってきており、ワクチンの対応ではパターンファイルの更新・配布が間に合わず、また脆弱性対策では、修正プログラムの配布・適用が間に合わず感染が広がり、LAN が利用できなくなる可能性があることが確認できた。このため、従来の対策を補完しながらも被害を最小限に抑制するための一手法としての検疫ネットワークを実際に構築し、今回の検証結果を利用して検疫ネットワーク導入の効果を評価していきたい。

参考文献

[1]総務省, 平成 16 年版情報通信白書
http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h16/index.html
[2] 独立行政法人 情報処理推進機構, 2004 年ウイルス届出状況
http://www.ipa.go.jp/security/txt/2005/documents/2004all-vir.pdf
[3] 独立行政法人 情報処理推進機構, 2004 年不正アクセス届出状況
http://www.ipa.go.jp/security/txt/2005/documents/2004all-cra.pdf
[4] トレンドマイクロ社, ウイルスデータベース (CodeRed)
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=CODERED.A
[5] トレンドマイクロ社, ウイルスデータベース (Slammer)
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_SQLP1434.A
[6] Nicholas C Weaver, Warhol Worms: The Potential for Very Fast Internet Plagues
http://www.cs.berkeley.edu/~nweaver/warhol.html
[7] 独立行政法人 情報処理推進機構,「国内におけるコンピュータウイルス被害状況調査 報告書」
http://www.ipa.go.jp/security/fy15/reports/virus-survey/documents/2003_virus_domestic.pdf
[8] 独立行政法人 情報処理推進機構, コンピュータウイルス対策基準
http://www.ipa.go.jp/security/antivirus/kijun952.html
[9] 内田勝也・高橋正和, 有害プログラム
共立出版, 2004/07
[10] トレンドマイクロ社,パターンファイル情報
http://www.trendmicro.co.jp/support/pattern.asp
[11] トレンドマイクロ社, ウイルスデータベース(MSBlast)
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.A
[12] シマンテック社 ,Symantec LiveState Recovery Desktop 3.0
http://www.netjapan.co.jp/P_Symantec/LSR/
[13] マイクロソフト社,VirtualPC2004 の概要
http://www.microsoft.com/japan/windows/virtualpc/evaluation/overview2004.mspx
[14] ネットワールド社, VMWare Workstation 5.0
http://www.networld.co.jp/vmware/workstation/outline.htm
[15] 警察庁, 国内の SQL Slammer ワーム感染ホスト数に関する推測
http://www.cyberpolice.go.jp/detect/pdf/20040625_slammer.pdf
[16] 寺田真敏・高田真吾・土居範久, ネットワークの感染先探索特性の検討
CSS2004