

国内のSQL Slammer ワーム感染ホスト数に関する推測

1 はじめに

昨年1月に発生したSQL Slammer ワームは、Microsoft SQL サーバの持つ脆弱性「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(MS02-039)」を悪用して感染し、感染後はランダムにホストを選択し同様の脆弱性を持つホストへと拡散していく。このワーム発生時には、多くのホストが数分間という短時間に感染したため、トラフィックの急増により、一部で通信に支障をきたすなど、多大な影響をもたらした。

本レポートではワーム発生後、1年5ヶ月が経過した現在、日本国内にどの程度SQL Slammer ワームに感染しているホストが存在しているのかを、平成16年3月の検知状況をもとに推測した。その結果、日本国内において平成16年3月現在、1日当たり約160台程度のホストが、今もなおSQL Slammer ワームに感染していると推測される。

2 検知状況に見るワーム感染ホストの推測

(1) 検知状況に見るワームの特徴

平成16年3月中の国内を発信元とするSQL Slammer ワームの1観測点当たりの平均検知件数を図2-1に示す。1日当たりのアラートの平均検知件数は0.66件であった。なお、国外を含めた1観測点当たりの平均検知件数は約9.9件であった。

3月においては1観測点で1日に同一ホストから2回以上のアクセスがなかったことから、図2-1に示す検知件数は検知ホスト数と同一とみなすことができる。

図2-1では日曜日及び祭日の検知件数が他の曜日と比べ0.2件程度少なくなっており、前述の脆弱性を有したホストは、平日にインターネット接続されている場合が多いと推測される。

また、原因は不明ながら下旬に検知件数が上昇している。

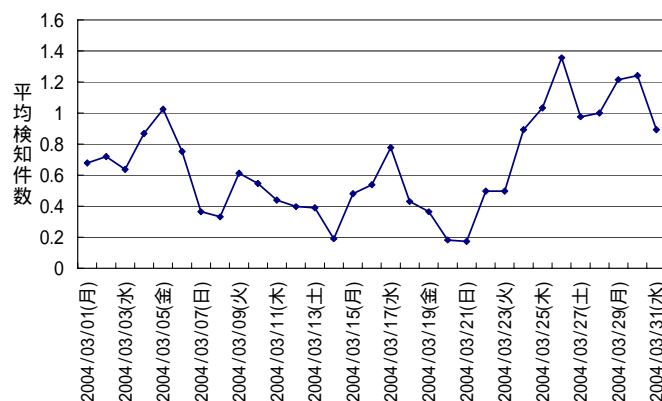


図2-1 平成16年3月における1観測点当たりの平均検知件数

図 2-2 に示すように単位時間当たりの平均検知数では夜間時間帯に比べ昼間(10時~19時)の検知件数が多く、15時がピークとなっている。

また、3月に検知したユニークなホスト数は約720ホストであった。図 2-3 にこのユニークなホストのドメイン別の内訳を示す。これらのドメインを調査したところ、ISP系ドメインの占める割合が約97%と最も多く、企業ドメインは全体の約2%、学校関連のドメインでは1%未満であった。

SQL Slammer ワームの発生から1年2ヶ月が経過したこの時期において企業等ではパッチの適用等のセキュリティ対策が講じられていると考えられ、ISPを利用したホストの感染が多くを占めている。

一方、図 2-4 に示すように全観測点における同一ホストの検知日数では1日のみが約93%を占めており、2日以上にわたる検知はわずか約7%に留まっている。

これは、感染ホストは動的に割り振られるIPアドレスでインターネットに接続していることが最大の要因と考えられる。また、常時接続環境にあるホストにおいても利用しない時間帯はコンピュータの電源を切っているものと推測される。

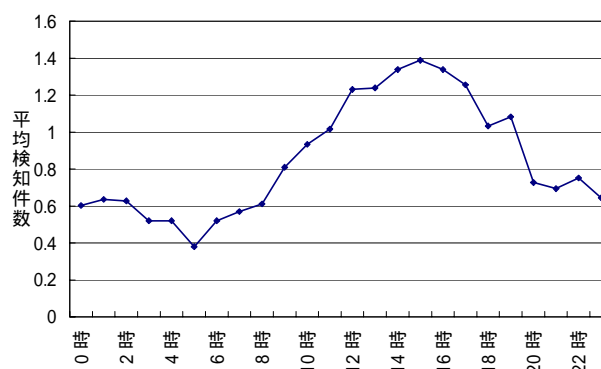


図 2-2 1 観測点当たりの時間帯別平均検知件数

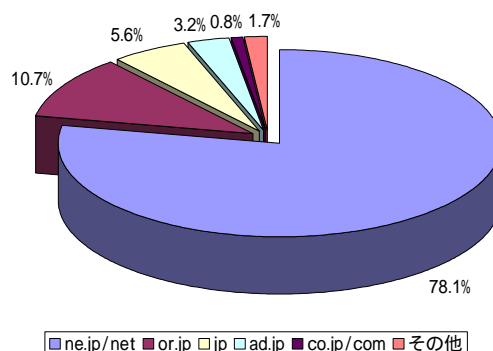


図 2-3 検知ホストのドメイン別内訳

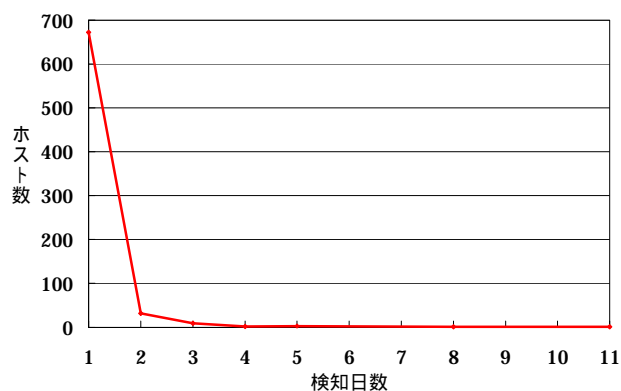
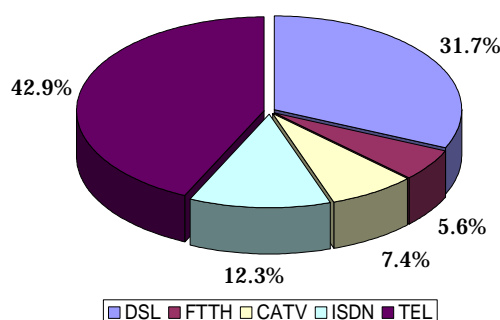


図 2-4 同一ホストの検知日数 (全観測点)

(2) インターネット利用実態

ここで、インターネット利用実態について考えてみる。総務省が平成 15 年度に行った「通信利用動向調査」の結果によれば、インターネット利用において人口普及率が 60% を超え、個人のインターネットの利用頻度・利用時間は毎日少なくとも 1 回利用するが 42.9% と最も多く、利用時間も 10~30 分未満が 23.4% を占めている。また、企業¹の約 80% がホームページを開設しており、インターネットを利用している事業所²の接続回線にはブロードバンド回線が 42.7% を占めているなど利用実態が報告されている。

一方、国内全般のインターネット接続回線では、総務省の「インターネット接続サービスの利用者数等の推移【平成 16 年 2 月末現在】(速報)」によれば図 2-5 に示すように 2004 年 2 月現在で DSL サービス利用者は約 31.7%、FTTH サービス利用者は約 5.6%、CATV サービス利用者は約 7.4% であり、電話回線利用者は全体の 55.2% の比率となっている。また、電話回線利用者のうち約 38.2% を ISDN 回線利用者が占めていると考えられる。



出典元：総務省の「インターネット接続サービスの利用者数等の推移【平成 16 年 2 月末現在】(速報)」

図 2-5 インターネットの利用比率

(3) ワーム感染ホストの推測

3 月における国内からの SQL Slammer ワームの検知状況は、下記のとおりである。

- (ア) 国内の感染ホストの検知状況は曜日及び時間帯によって差異が生じており、週日かつ 10 時~19 時の昼間に多く検知している。
- (イ) ドメイン別の検知状況では、ISP 系のドメインがそのほとんどを占めている。
- (ウ) 同一 IP アドレスから複数日にわたる検知状況では 1 日間で最も多く約 97% である。

¹企業とは、常用雇用者規模 100 人以上の企業（農業、林業、漁業及び鉱業を除く）

²事業所とは、常用雇用者規模 5 人以上の事業所（郵便、電気通信業を除く）

総務省 平成 15 年「通信利用動向調査」の結果より

一方、SQL Slammer ワームは「SQL Server2000」のみでなく「MSDE2000」もその感染対象となり得る。「MSDE2000」はデータベースエンジンであり、会計ソフトウェアをはじめとする幅広い分野のソフトウェアに組み込まれているものである。

以上のことから、co.jp ドメインを取得しておらず、インターネット接続に一般の ISP を利用している事業所又は SOHO(Small Office Home Office)等のような場所において当該脆弱性を有したコンピュータが今もなお数多く存在している可能性が高いと推測される。

セキュリティ対策が施されていない「SQL Server2000」や「MSDE2000」が組み込まれたコンピュータをインターネットに接続するとワームに感染するが、一般に就業時間外は電源が切られているホストが多いことから同一 IP アドレスによる複数日の検知が少ない結果となっているものと推察される。また、国内からのワームの検知件数が減少しない要因の一つには、利用者自身も当該脆弱性を有したソフトウェアであることに気が付かず、適切な措置を講じないまま利用し続けているとも考えられる。

3 SQL Slammer ワーム感染ホスト数の推測

(1) SQL Slammer ワームの検証

ワームに感染したホストが送出する UDP パケットは、CPU の性能や接続回線によって大きく異なるため、代表的な環境においてどのような違いが生じるか検証を行った。

表 3-1 SQL-Slammer ワーム感染端末諸元

機種	CPU	メモリ	OS	アプリケーション
DOS/V互換機	Pentium (1000MHz)	512Mbytes	Windows XP Professional	SQL Server 2000 Personal Edition

検証環境には、表 3-1 に示す端末及び図 3-1 に示す 100Mbps、10Mbps の LAN 及び ADSL 回線(上り 512kbps) の 3 種類のネットワーク環境を使用した。

本検証はそれぞれのネットワーク環境において、検証用端末にワームを感染させ、感染したホストから 1 秒間にどの程度 UDP パケットを送出しているか、ネットワークアナライザ(Ethereal V0.10.3)により検証を行った。

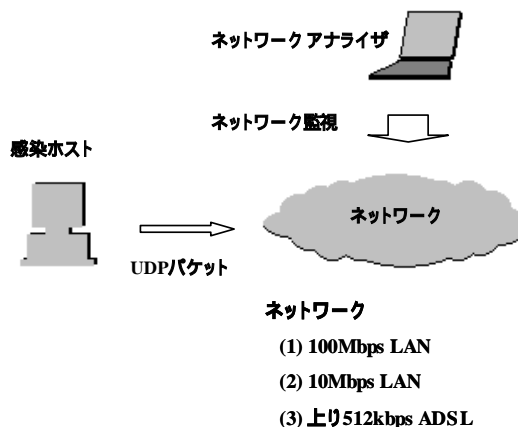


図 3-1 SQL-Slammer ワーム検証環境

図 3-2 に検証結果を示す。本検証環境では、各ネットワークにおける UDP パケットの 1 秒間当たりの送出数は 100Mbps の LAN 環境で平均 24,304.94 個、10Mbps の LAN 環境で平均 2,819.16 個、上り 512kbps の ADSL 環境で平均 112.54 個であり、UDP パケット送出数と伝送速度とはほぼ比例関係にあった。UDP パケット送出数と伝送速度との関係は次の近似式で表される。

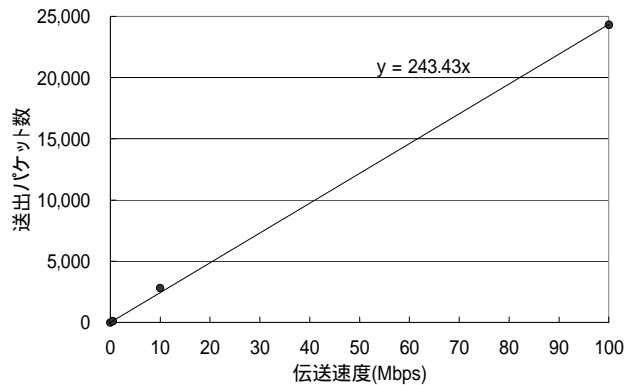


図 3-2 SQL-Slammer ワーム検証結果

$$y = 243.43x \quad \dots (1)$$

また、感染時の CPU 使用率を図 3-3 に示す。100Mbps の LAN 環境では、CPU 使用率は約 100% であったが、10Mbps の LAN 環境及び ADSL 環境下では単位時間当たりに送出できるパケット数が少ないため 10 数%程度の CPU 使用率となっている。

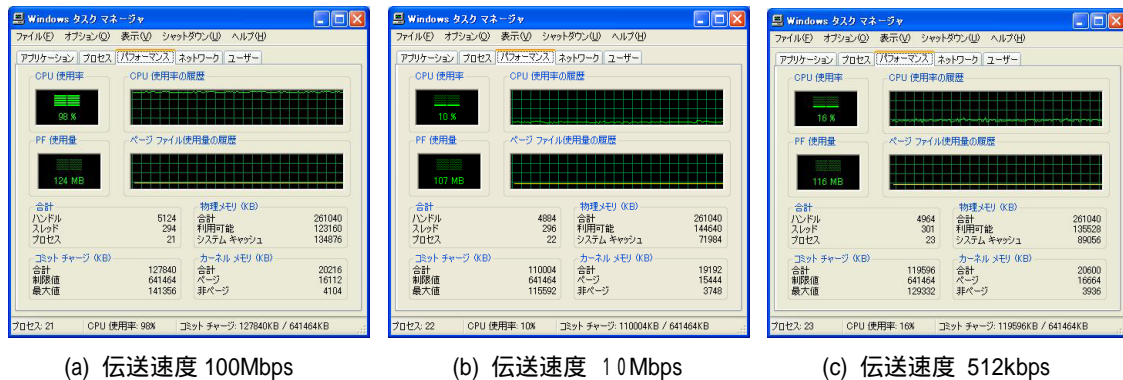


図 3-3 ワーム感染時の CPU 使用率

したがって、ワームが送出する UDP パケット数は感染端末の CPU 性能ではなく、ネットワーク環境に大きく依存していると言える。

(2) SQL Slammer ワーム感染ホスト数の推測

前述の検知状況及びワームの感染の特徴から、以下の前提条件を設定し国内におけるワーム感染ホスト数を推測する。

【前提条件】

- (ア) 感染ホストは ISP を利用したコンピュータで、インターネット接続後直ちにワームに感染する。
- (イ) 利用者は少なくとも毎日 1 回はインターネットを利用する。
- (ウ) インターネットへの接続時間は就業時間である 9 時間を想定し、時間外はコンピュータの電源を切っている。
- (エ) 当該脆弱性を有するコンピュータは、インターネットの利用環境やセキュリティ対策による偏りがなく、一様に存在する。

SQL Slammer ワームに感染したコンピュータが 1 観測点の IP アドレスを選択する確率を求める。IP アドレスの総数は 2^{32} 個存在するため、任意の 1 つの IP アドレスを選択する確率 P_0 は、約 2.33×10^{-10} ($P_0 = 1/2^{32}$) である。

インターネット接続の各回線種別における上り回線の平均速度を調査したところ³、ADSL では約 783.8 kbps、FTTH では約 34.0 Mbps、CATV では約 869.6 kbps であった。電話回線の場合、ISDN 回線を約 64 kbps、アナログ回線を約 28.8 kbps として回線種別毎の packets 送出回数を求める。

式(1)から 1 秒間における各回線種別における packets 送出回数を算出し、インターネット接続時間が 9 時間の場合の各回線種別における packets 送出回数 ($N_1 \sim N_5$) 及び任意の 1IP アドレスを選択する確率 ($P_1 \sim P_5$) を求めた。その結果を表 3-2 に示す。

表 3-2 各回線種別における packets 送出回数及び 1IP アドレス選択確率

回線種別	平均速度(上り)	packets 送出回数(N_n)	1IP 選択確率(P_n)
FTTH	34.0 Mbps	268,100,000	6.24E-02
DSL	783.8 kbps	6,180,000	1.44E-03
CATV	869.6 kbps	6,850,000	1.59E-03
ISDN	64 kbps	504,000	1.17E-04
アナログ回線	28.8 kbps	220,000	5.12E-05

³ 出典：RBB TODAY (ブロードバンド情報サイト) <http://www.rbbtoday.com/rbbcorp/> 利用者の声

よって、国内における感染ホストが 24 時間以内に少なくとも 1 回は特定の 1 ホストを選択する確率 P は

$$P = P_1 \times 0.056 + P_2 \times 0.317 + P_3 \times 0.074 + P_4 \times 0.123 + P_5 \times 0.429$$
$$4.11 \times 10^{-3}$$

となる。

また、サイバーフォースセンターにおいて 1 観測点における国内からの 1 日当たりの平均検知ホスト数は 0.66 ホスト、標準偏差は約 0.32 である。95%信頼区間における国内の平均検知ホスト数 μ は次式で表される。

$$\bar{x} - 1.96 \frac{\sigma}{\sqrt{n}} < \mu < \bar{x} + 1.96 \frac{\sigma}{\sqrt{n}} \quad \dots \dots (2)$$

\bar{x} : 標本平均値
 σ : 標本標準偏差
n: 標本数

式(2)より、国内における平均検知ホスト数 μ は、 $0.55 < \mu < 0.77$ の範囲内となり、国内における 1 日あたりの SQL Slammer ワームに感染するホスト数 N は、

$$134 < N < 188$$

の範囲内であると推測される。

4 まとめ

検知状況を分析した結果、国内における SQL Slammer ワームが減少しない一つの要因には co.jp ドメインを取得しておらずインターネット接続に一般の ISP を利用している事業所又は SOHO(Small Office Home Office)等において、当該脆弱性を有したコンピュータが今もなお数多く存在しているためと考えられる。

この分析結果を踏まえ平成 16 年 3 月における 1 日当たりの国内の感染ホスト数を推測したところ、134 ~ 188 台の範囲内であった。

SQL Slammer ワームに関しては、マイクロソフト社から当該脆弱性を有する「SQL Server2000」、「MSDE2000」が存在するか確認する SQL Scan ツール (<http://www.microsoft.com/japan/sql/downloads/securitytools.asp>) が提供されている。

日々、新しい脆弱性やウイルス/ワーム等が報告されている現状において、今一度使用しているコンピュータのセキュリティについて再確認し、適切な対応をとる必要がある。

参考文献

- (1) インターネット接続サービスの利用者数等の推移【平成 16 年 2 月末現在】(速報)
http://www.soumu.go.jp/s-news/2004/040331_5.html
- (2) 平成 15 年通信利用動向調査の結果
http://www.soumu.go.jp/s-news/2004/pdf/040414_1_a.pdf
- (3) 「SQL Server および MSDE を標的とした SQL Slammer ワームに関する情報」
<http://www.microsoft.com/japan/technet/treeview/default.asp?url=/japan/technet/security/virus/sqlslamuprcd.asp>