2004/06/06　12:59

MSBlaster ワームの感染先探索特性の検討 Rev.2

寺田真敏
terada@doi.ics.keio.ac.jp

慶應義塾大学 大学院 理工学研究科
〒223-8522　神奈川県横浜市港北区日吉 3-14-1

1. はじめに

本メモは、「Sasser.C ワームの感染先探索特性の検討」の追加検討であり、MSBlaster ワームを対象に実機での感染先探索特性の検証をおこなった。

MSBlaster ワーム [1] は、2003 年 8 月に発見されたネットワーク型ワームであり、CodeRed II、CodeRed3 ならびに Slammer ワームとの違いのひとつとして、感染先の探索特性を挙げることができる。

- CodeRed II ならびに CodeRed3 ワーム
  アドレスブロック探索比率を加味して常に探索 IP アドレスをランダムに選択する(アドレスブロック探索比率加味型&ランダム探索型)。

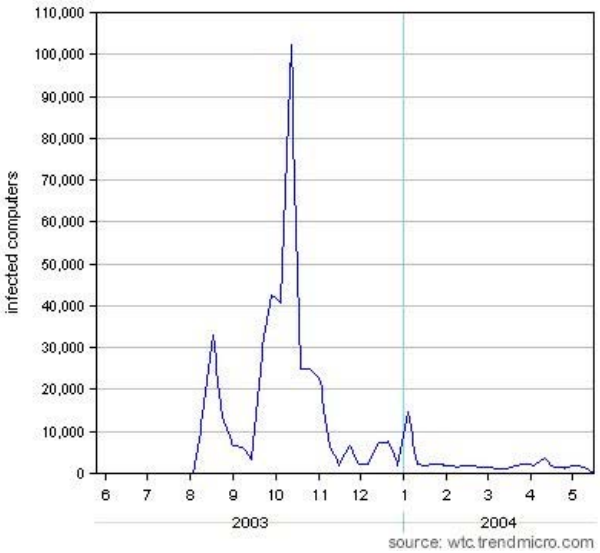


図 1.1　MSBlaster のコンピュータ感染状況
出典:トレンドマイクロ

- Slammer ワーム
  アドレスブロック探索比率を加味せず常に探索 IP アドレスをランダムに選択する(ランダム探索型)。

これに対し、MSBlaster ワームは、アドレスブロック探索比率を加味して探索開始 IP アドレスを決定した後、順次 IP アドレスを加算しながら感染活動を行う(アドレスブロック探索比率加味型&スイープ探索型)。MSBlaster ワームのコード解析に基づく感染先探索特性はいくつかのベンダから提供されている(表 1.1)。このコード解析によれば、感染先 IP アドレスの生成は次の通りである。

- 探索開始 IP アドレスの決定方法
  - 完全にランダム(異.異.異.0)：60%
  - 上位 2 オクテットが同一(同.同.異.0)：40%
    ただし、3 オクテット目の値が 20 以下の場合に上位 3 オクテットまでが同一となる。20 よりも大きい場合には上位 2 オクテットまでが同一となる。
- IP アドレスの加算方法
  上記で計算した IP アドレスの 4 オクテット目の値である 0 に 1 を加算し、その IP アドレスを探索先とする。さらに、この操作を 4 オクテット目の値が 255 に達するまで繰り返す。次に、3 オクテット目に 1 を加算し、同様の操作を続ける。

表 1.1　MSBlaster ワームの感染先探索特性

情報提供元	探索特性の情報(抜粋)
ネットワークアソシエーツ	W32/Lovsan.worm.a ワームが起動すると、TCP ポート 135 上のシステム脆弱性を探すための IP をランダムにスキャンします。

商品名称等に関する表示
本メモ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。

情報提供元	探索特性の情報(抜粋)
シマンテック	W32.Blaster.Worm IP アドレスを生成し、そのアドレスのコンピュータに感染を試みます。IP アドレスは次のアルゴリズムに基づいて生成されます。 * 40%の確率で、 A.B.C.0 の形式のIPアドレスが生成されます。A.B.は、感染元となるコンピュータのIPアドレスの先頭 2 つの値と同じです。Cは、感染元となるシステムのIPアドレスの 3 番目の値に基づいて計算されます。ワームは、40%の確率でCの値が 20 よりも大きいかどうかを確認します。20 より大きい場合は、Cの値から 20 未満のランダムな値を差し引いた値を使用します。IPアドレスの計算が終わると、ワームは算出されたIPアドレス(A.B.C.0)に該当するコンピュータを探して感染しようとします。その後、上記で計算したIPアドレスの 0 の部分に 1 を加え、そのアドレスに該当する他のコンピュータを探して攻撃しようとします。この操作をIPアドレスの 0 の部分が 254 に達するまで繰り返し行います。 * 60%の確率で、完全にランダムなIPアドレスを使用します。
トレンドマイクロ	WORM_MSBLAST.A ワームはランダムな IP アドレスに TCP パケットを送信し、ネットワーク上のコンピュータを探します。ワームは 20 のスレッドにより TCP 接続を行います。このランダムな IP アドレス生成に以下の 2 種類の方法を用います。 * 方法 1 ワームは攻撃対象用の IP アドレス生成に感染コンピュータの IP アドレスを使用します。例えば、感染マシンの IP アドレスが A.B.C.D だった場合、A.B は固定で使用し、D を 0 に置き換えます。C の値が 20 より大きい場合、C の値より 20 引いた値から C の値までを使用します。20 以下の場合はそのままの値を使用します。 Ex. 210.23.69.101 の場合 → 210.23.[50-69].0 210.23.19.88 の場合 → 210.23.19.0 * 方法 2 0.0.0.0〜255.255.255.0 までのランダムな IP アドレスに対し、アクセスを試みます。その際に TCP1000〜5000 までの範囲で TCP ポートを開き、応答を待機します。
eEye Digital Security	Blaster Worm Analysis The worm will begin infection at an address either based off the local machine's IP address, or a completely random address, and then attempt to infect sequential IP addresses endlessly. Each time a host is infected, there is a 40% chance that it will begin at the first address of its "Class C"-size subnet (x.x.x.0), and a 60% chance that it will start at a completely random IP address with the last octet set to 0 ([1-254].[0-253].[0-253].0). If the starting address is based off of the local address, and the third octet is greater than 20, it will be reduced by a random number between 0 and 19, inclusive.

2. MSBlaster の感染先探索特性に関する動作確認

本章では、感染先探索特性の動作知見の情報収集を目的として、実験環境下での動作確認をおこなった。

2.1　確認環境

(1) 感染 PC(wormPC)とモニタ装置(monitor)

- 感染 PC(wormPC)
  VMware Workstation 4 上で稼動するMicrosoft Windows XP Professional (SP適用なし) 環境を構成し、システム時計を 2003 年 8 月 1 日に再設定した後、MSBlasterが感染時にコピーとして作成する(msblast.exe [b])を実行した。
- モニタ装置(monitor)
  Linux 上の tcpdump を使用して、MSBlaster ワームの送出するパケット(宛先ポート番号 135/tcp)をモニタリングした。

(2) ネットワーク

Sasser.C ワームの実機検証と同様に、図 2.1 に示すネットワークを構成した。

- 一番小さなサブネットワークを構成する(Netmask=255.255.255.252)。
- 感染 PC の DefaultRoute としてモニタ装置の IP アドレスを設定する。

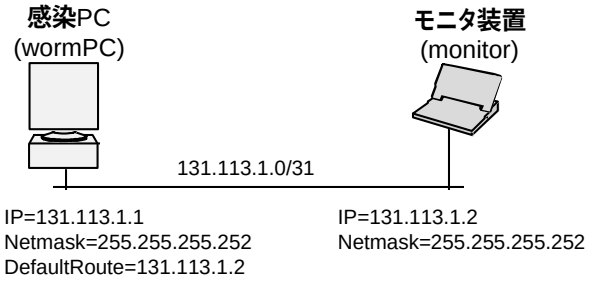


図 2.1　動作確認に使用したネットワーク構成

b) MD5=5ae700c1dffb00cef492844a4db6cd69

2.2　動作確認結果

感染 PC の IP アドレスとして、表 2.1 に示すグローバル IP アドレスを設定することで感染先探索特性を調査した。

表 2.1　IP アドレスとモニタリングパケット数

設定 IP アドレス	モニタリングパケット数(件)
プライベート=未実施	ー
グローバル=131.113.1.1 DNSによる名前解決なし[c]	7500
グローバル=131.113.1.1 DNSによる名前解決あり[d]	6993

(1) 感染 PC のパフォーマンス(CPU 使用率)

msblast.exe を実行すると感染 PC のパフォーマンス(CPU 使用率)は一時的に上昇するが(図 2.1)、以降は数%の状態を維持する。

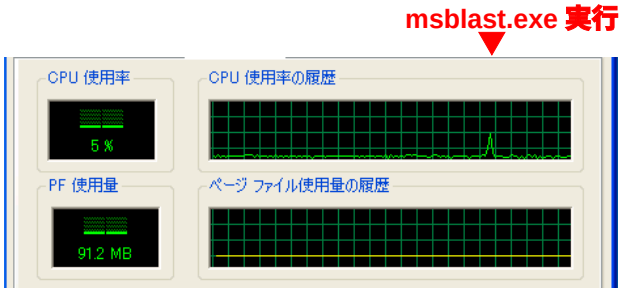


図 2.2　感染 PC のパフォーマンス(CPU 使用率)

2.2.1　経過時間毎の探索 IP アドレスの分布

(1) DNS による名前解決なし

経過時間毎の探索IPアドレスの分布(図 2.3 左上図)では、横軸に MSBlaster(msblast.exe)実行以降の経過時間、縦軸に送出されたパケットの宛先 IP アドレス範囲(0.0.0.0～255.255.255.255)を示している。

- 動作確認結果の範囲においては、探索 IP アドレスの初期値として 153.75.20.1 が選択され、以降 4 オクテット目が 1 つカウントアップされた。
- 宛先 IP アドレス範囲を探索範囲に絞った結果を図 2.3 左下図に示す。縦軸に送出されたパケットの宛先 IP アドレス範囲は、153.75.20～153.75.50 を示している。
- 感染 PC の DNS サービスに関する設定の違い(DNS による名前解決あり／なし)による探索特性の差は見られない。
- 探索開始 IP アドレスは、msblast.exe の実行とプロセス停止を繰り返したところ、3 回に 1 度くらいの割合で上位 3 オクテットが同一(同.同.同.0)となる。ただし、これ以上の精度で探索比率を得ることはできていない。

(2) DNS による名前解決あり

図 2.3 右上図に経過時間毎の探索 IP アドレスの分布を示す。また、宛先 IP アドレス範囲を探索範囲(193.92.0～193.92.30)に絞った結果を図 2.3 右下図に示す。

- 動作確認結果の範囲においては、探索 IP アドレスの初期値として 193.92.0.1 が選択され、以降 4 オクテット目が 1 つカウントアップされた。
- 探索開始 IP アドレスは、「DNS による名前解決なし」の場合と同様の結果が得られた。

2.2.2　上位 1 オクテットを対象とした探索 IP アドレスの分布

上位 1 オクテットを対象とした探索 IP アドレスの分布(図 2.4)では、横軸に探索対象となる宛先 IP アドレスの先頭から 1 オクテットの IP アドレス範囲(000～255)、縦軸に送出されたパケット数を示している。

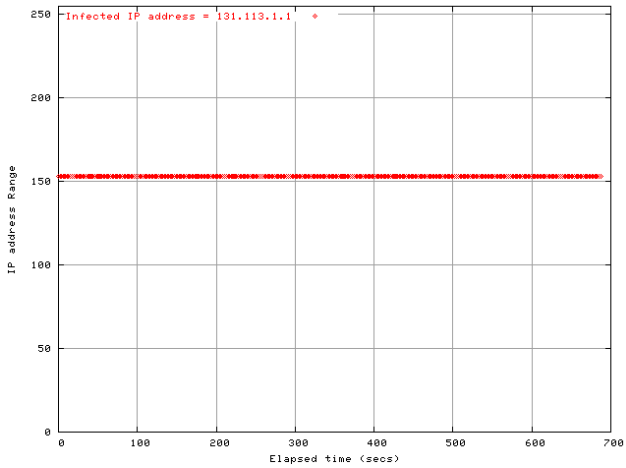
- 動作確認の範囲においては、宛先 IP アドレスとして、「DNS による名前解決なし」の場合には 153.75.20 以降の IP アドレス、「DNS による名前解決あり」の場合に 193.92.0 以降の IP アドレスが送出されている。

2.2.3　特定の上位 2 オクテットを対象とした探索 IP アドレスの分布

特定の上位 2 オクテットを対象とした IP アドレスの分布(図 2.5)では、横軸に探索対象となる宛先 IP アドレスの先頭から 3 オクテット目の IP アドレス範囲(153.75.000～172.75.255 ならびに 193.92.000～193.92.255)、縦軸に送出されたパケット数を示している。

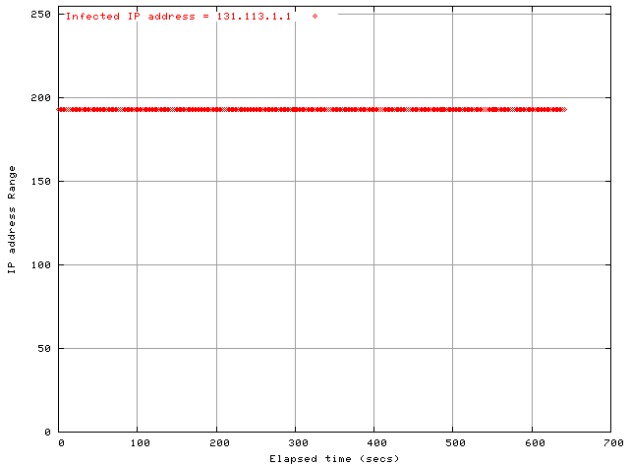
c) 感染PCのIPアドレスをDNSに登録していない。感染PCには利用可能なDNSサーバを設定していない。
d) 感染PCのIPアドレスをDNSに登録している。感染PCには利用可能なDNSサーバを設定している。

感染 PC に設定した IP アドレス=131.113.1.1
DNS **による名前解決なし**

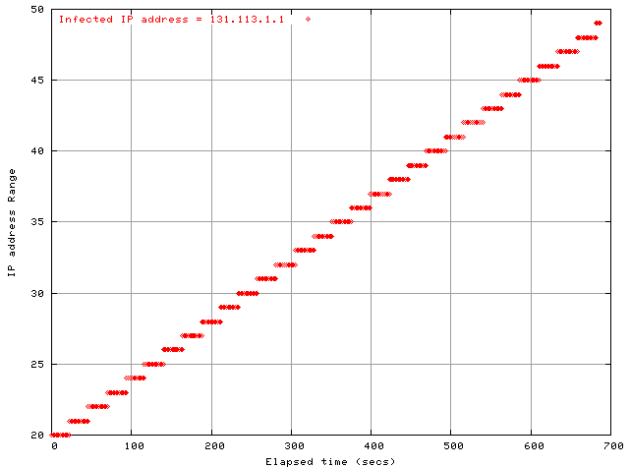


153.75.50

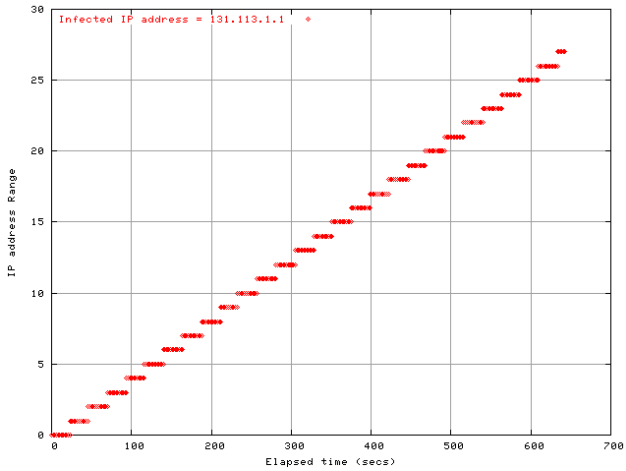
感染 PC に設定した IP アドレス=131.113.1.1
DNS **による名前解決あり**



193.92.30



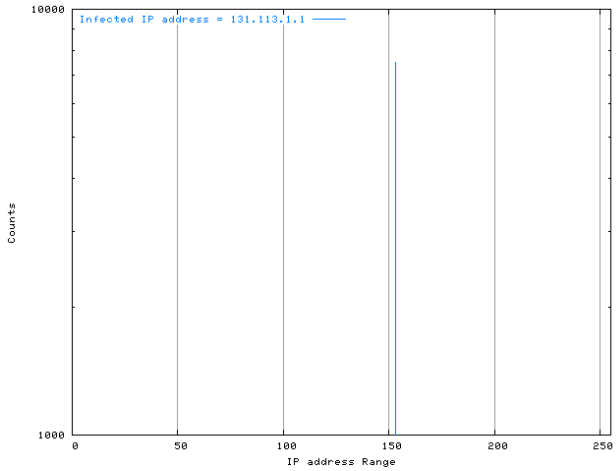
153.75.20



193.92.0

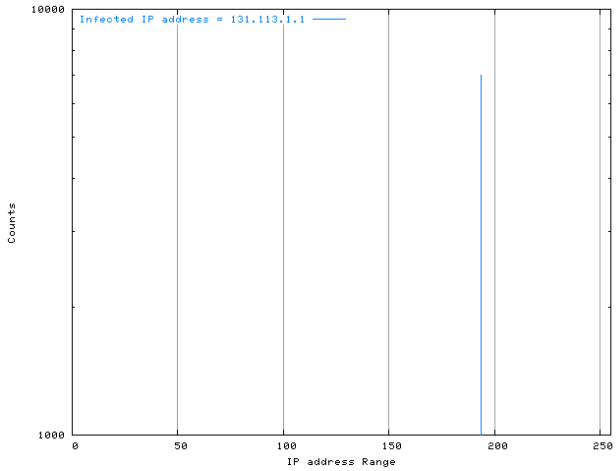
図 2.3　経過時間毎の探索 IP アドレスの分布

感染 PC に設定した IP アドレス=131.113.1.1
DNS **による名前解決はなし**



000　　255

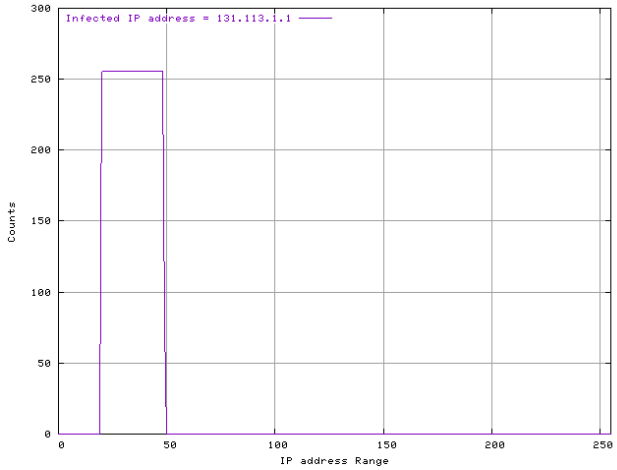
感染 PC に設定した IP アドレス=131.113.1.1
DNS **による名前解決あり**



000　　255

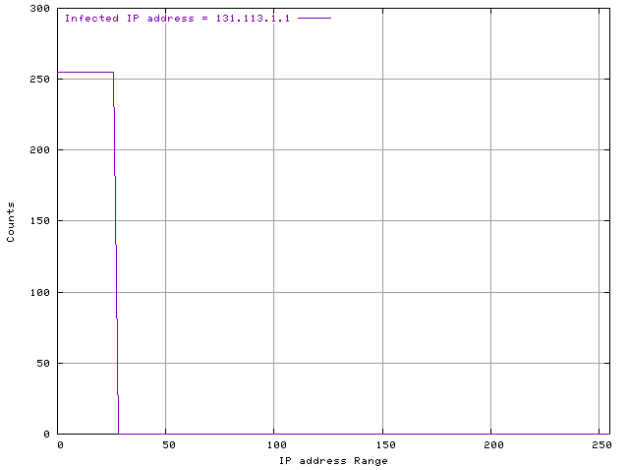
図 2.4　上位 1 オクテットを対象とした探索 IP アドレスの分布

感染 PC に設定した IP アドレス=131.113.1.1
DNS による名前解決なし



153.75.000　　153.75.255

感染 PC に設定した IP アドレス=131.113.1.1
DNS による名前解決あり



193.92.000　　193.92.255

図 2.5　特定の上位 2 オクテット(152.75,193.92)を対象とした探索 IP アドレスの分布

- 動作確認の範囲においては、宛先 IP アドレスとして、153.75.20 ならびに 193.92.0 以降の IP アドレスのみが送出されている。

2.3　TCP 再送処理に関する考察

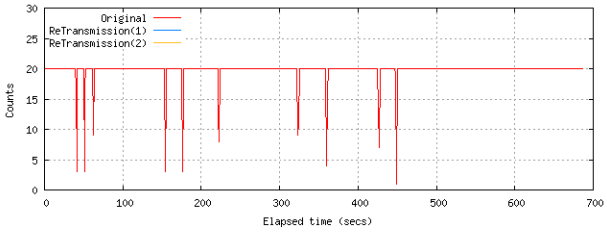
本実験構成において、モニタ装置(monitor)は、受信したパケットを次のように処理するため、感染 PC では TCP パケット(SYN の設定された TCP パケット) の再送処理が発生することになる。

- 宛先 IP アドレスがモニタ装置(monitor)の IP アドレスに一致した場合：”icmp: tcp port 135 unreachable”を感染 PC に返送する。
- 上記以外：受信パケットを廃棄する。

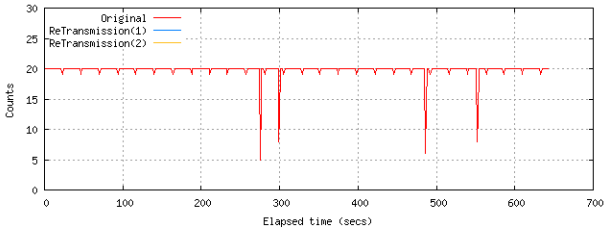
(1) TCP 再送に関する動作確認結果

TCP パケット(SYN の設定された TCP パケット) の再送処理に関連した動作確認を行ったところ、次の結果が得られた。

- 探索 IP アドレスの上位 1 オクテットが感染 PC と異なる場合、TCP の再送パケットは送出されていない(図 2.6)。
  ⇒ ICMP パケット(tcp port 135 unreachable)を受信しない場合には再送処理をおこなわない。
- 探索 IP アドレスの上位 3 オクテットが感染 PC と同じ場合、18 個(131.113.1.2, 131.113.1.4～131.113.1.20)の TCP パケット再送が発生した(図 2.7、図 2.8)。なお、再送回数は 1 回のみであった。
  ⇒ ICMP パケット(tcp port 135 unreachable)を受信した場合には再送処理をおこなう。



(a) DNS による名前解決なし



(b) DNS による名前解決あり

—：オリジナル　—：1 回目の再送　—：2 回目の再送

図 2.6　経過時間毎の TCP 再送パケットの分布
(上位 1 オクテットが感染 PC と異なる場合)

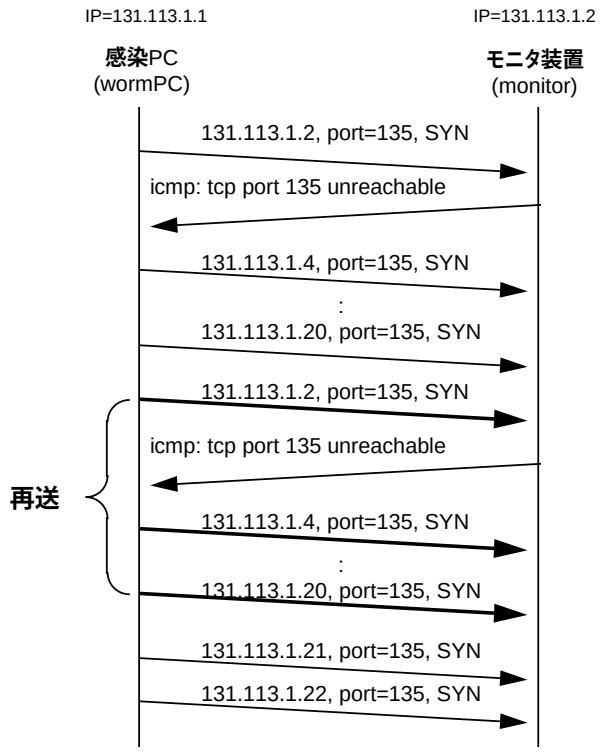
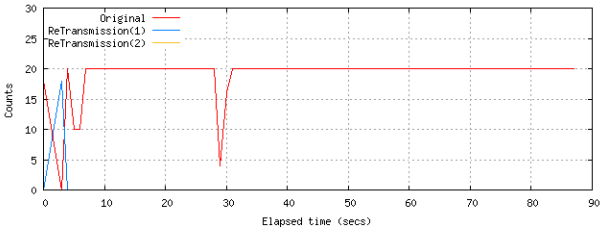
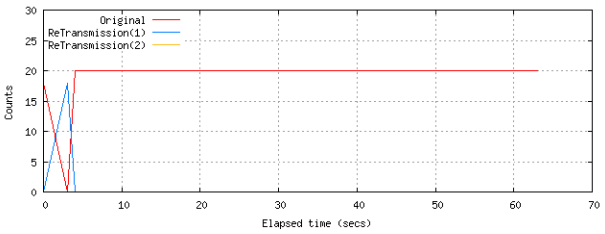


図 2.7　TCP パケット再送処理のシーケンス



(a) DNS による名前解決なし

「システムのシャットダウン」ダイアログ



(b) DNS による名前解決あり

—：オリジナル　—：1 回目の再送　—：2 回目の再送

図 2.8　経過時間毎の TCP 再送パケットの分布
(上位 3 オクテットが感染 PC と同じ場合)

- 探索 IP アドレスの上位 3 オクテットが感染 PC と同じであり、かつ、DNS 名前解決ありの場合、「システムのシャットダウン」を示す警告ダイアログ図 2.9 を挙げた後、システムシャットダウン処理に入りパケットの送出が停止した。この事象には再現性がある。また、ダイアログを挙げる前後に、TCP パケット(135/tcp) ならびに ICMP パケット(tcp port 135 unreachable) 以外のパケットは送出されていない。

探索IPアドレスの上位 3 オクテットが感染PCと同じ場合に発生するTCPパケットの再送処理については、「MSBlasterワームは、20 のスレッドを使用する動作[e]」にも関連すると思われる。

また、DNS 名前解決ありの場合の「システムのシャットダウン」については、パケット停止時刻から逆算して、パケット送出開始 5 秒後(図 2.8)にダイアログが挙がったと考えられる。この時刻は TCP パケットの再送処理完了にほぼ合致していることから、TCP パケット再送処理と DNS の設定に起因した障害であると類推される。

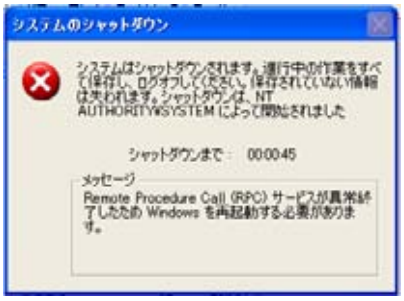


図 2.9　「システムのシャットダウン」ダイアログ

(2) MSBlaster における TCP 再送処理

Windows における TCP 再送処理については、Microsoft Knowledge Base Article – 224829：「Windows 2000 と Windows XP の TCP 機能の説明」[2]に記載されている。

> **再転送タイムアウト**(RTO)**は、**RFC 793 **に記載されている** SRTT (Smoothed Round Trip Time)**計算を使用して、接続の特性に合わせて動的に調整されます。セグメントのタイマは、そのセグメントが再転送されるたびに** 2 **倍になります。**TCP **では、このアルゴリズムを使用して、接続の通常の遅延に応じたセルフ チューニングを行います。**

e)出典元トレンドマイクロ「ワームはランダムなIPアドレスにTCPパケットを送信し、ネットワーク上のコンピュータを探します。ワームは 20 のスレッドによりTCP接続を行います。」

実機(Windows 2000、Window XP)において TCP 再送処理の確認をおこなったところ、再転送タイムアウト(RTO)は、1 回目が約 3 秒であり、2 回目はその倍の約 6 秒となっている。一方、eEye Digital Security 社が解析した "Blaster Worm assembly code [3]" によれば、MSBlaster は 20 個の TCP コネクションの確立操作後、1.8 秒間 sleep した時点でソケットの状態確認をおこなう。このとき TCP コネクションが利用できない場合には、TCP コネクションの解放操作に入る。

①	20 **個のノンブロッキングの** TCP/IP **ソケットを作成する**(.text:004017B2～)。
②	20 **個の連続した** IP **アドレスのポート番号** TCP/135 **に対して** TCP **コネクションの確立を試みる**(.text:004017E6～)。
③	sleep(1.8 **秒)する**(.text:0040184B)。
④	select **を利用してソケットの状態を確認し、失敗している場合にはソケットを閉じる**(.text:00401852～)

すなわち、MSBlaster は、Windows の再転送タイムアウト(RTO)よりも短い間隔で TCP コネクション確立状態の確認ならびに解放をおこなうことで、TCP パケット(SYN の設定された TCP パケット) の再送動作を抑止していることになる。

3. まとめ

本メモでは、MSBlaster ワームの流布特性について実機での検証をおこなった。

(1) MSBlaster ワームの感染先探索特性

- アドレスブロック探索比率を加味して探索開始 IP アドレスを決定した後、IP アドレス加算により総探査する(アドレスブロック探索比率加味型&スイープ探索型)タイプに属する(図 3.1)。
- 感染 PC の DNS サービスに関する設定の違い(DNS による名前解決あり／なし)による探索特性の差は見られない。
- 探索開始 IP アドレスは、3 回に 1 度くらいの割合で上位 3 オクテットが同一(同.同.同.0)となる。ただし、これ以上の精度で探索比率を得ることはできていない。
- TCP コネクション確立時の TCP 再送処理を抑止する実装となっている。

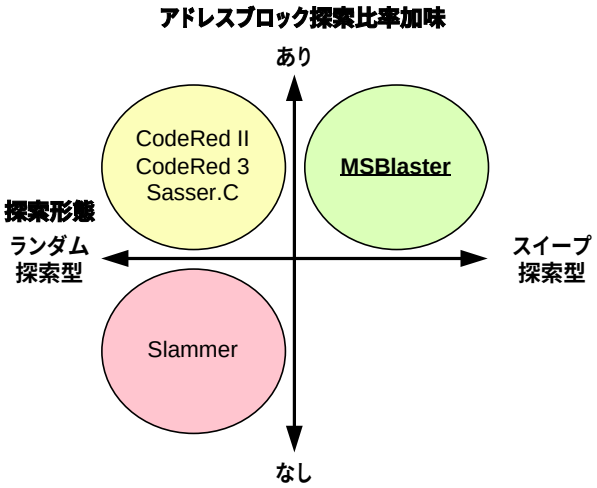


図 3.1　感染先探索特性の分類

参考文献

1) MSBlaster
ネットワークアソシエーツ：W32/Sasser.worm
http://www.nai.com/japan/security/virL.asp?v=W32/Lovsan.worm.a
シマンテック：W32.Sasser.Worm
http://www.symantec.com/region/jp/sarcj/data/w/w32.blaster.worm.html
トレンドマイクロ：WORM_SASSER.A
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.A
eEye Digital Security：Blaster Worm Analysis
http://www.eeye.com/html/Research/Advisories/AL20030811.html
2) Microsoft Knowledge Base Article - 224829
Windows 2000 と Windows XP の TCP 機能の説明
http://support.microsoft.com/default.aspx?scid=kb;ja;224829
3) eEye Digital Security：
MSBlaster worm disassembly by eEye Digital Security, Inc., August 12, 2003.
http://www.eeye.com/html/Research/Advisories/Blaster_Analysis.txt

更新履歴

日付	更新内容
2004-05-14	Rev.0：初版
2004-05-30	ネットワーク構成を追記した。
2004-06-02	Rev.1：実験環境依存に関する検討項目として、TCP 再送処理を記載した。
2004-06-06	Rev.2：TCP パケット再送処理のシーケンスに SYN を追記した。TCP 再送処理を改訂した。