Blasterワームの概要とその対策

笠原, 義晃
九州大学情報基盤センター

https://doi.org/10.15017/1470667

出版情報：九州大学情報基盤センター広報 : 学内共同利用版. 3 (3), pp.107-114, 2003-11. 九州大学情報基盤センター
バージョン：
権利関係：

Blasterワームの概要とその対策

笠原 義晃*

1 はじめに

今Windows PCを使っている人で,「Blasterワーム」「Windows Update」といった言葉に心当りの無い人は,3章「対策」を先に読んで,書いてある処置をしてください.

日本時間で2003年8月12日午前2時頃から,Blasterワーム(マイクロソフト社による呼称[1])と呼ばれるウィルスの一種がインターネット上で流行しはじめました.このワームはWindows OSを感染対象としており,インターネットに接続した未対策のWindows PCに容易に感染して被害を広げます.九州大学の学内ネットワークも例外ではなく,13日に複数のPCに感染が認められ,その後1ヶ月以上が経過した現在も新規感染が終息していません.また,このワームには複数の亜種(Blasterワームのプログラムを元に作成されたと考えられる類似したワーム)が発見されており,またBlasterと関連の深いより問題のある活動をするワームも発見され,問題となっています(詳細は2.4節).

本稿では,このBlasterワーム(亜種含む)の概略と,対策方法について述べます.なお,この文書は読者として一般利用者を想定しているため,技術的に曖昧な記述が含まれています.より詳細な情報については,脚注や末尾の参考URL等を参照してください.

2 Blasterワームの概要

この章ではBlasterワームの概略について述べます.より詳しい情報について知りたい場合は,脚注や末尾の参考URLを参照してください.

2.1 感染対象

Blasterワームが感染する可能性のあるWindow OSの種類は以下の通りです.

- Microsoft Windows NT 4.0
- Microsoft Windows 2000

*九州大学情報基盤センター
E-mail : kasahara@nc.kyushu-u.ac.jp

[1]MS BLAST, WORM_MSBLAST.A, W32.Blaster.Worm, W32/Lovsan.worm等の別名がありますが,本稿ではBlasterに統一します

- Microsoft Windows XP
- Microsoft Windows Server 2003

影響を受けない種類は以下の通りです.

- Microsoft Windows 98
- Microsoft Windows 98 Second Edition (SE)
- Microsoft Windows Millenium Edition (Me)

感染する可能性のある Windows OS において,「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[2](823980[3])」のセキュリティ修正を適用していない場合に, Blaster ワームによる攻撃を受けると感染します. 大雑把に言うと, 影響を受ける種類の Windows を PC にインストールしてインターネットに接続すると, それだけで感染する可能性があります. **利用者の操作は一切必要なく**, メールを読んだり, ウェブを見たりする必要もありません. **完全に自動的に感染します.**

Blaster ワームは TCP ポート 135 番を利用して通信するため, これをファイアウォールなどで遮断していて攻撃が PC に届かなかった場合は感染しません. もちろん, ファイアウォールで保護された中のネットワークに感染している PC がある場合はファイアウォールは意味がありません. 九州大学では, Blaster ワーム発生の数日後に学外からの 135 番ポートアクセスを閉鎖しましたが, 既に感染しているホストが学内に多数残っていたため内部から内部への感染が続いています. また, 外部に持ち出したノート PC が感染し, それを内部に持ち込んだために内部での感染が拡大している事例も発生しています.

2.2 感染時の症状

Blaster ワームは感染の拡大を目的として作成されており, Windows OS の書き換えやデータの破壊といった活動をしません. このため, 利用者は自分の PC が感染していても気づかない場合があります. また, 感染活動にともなって OS が異常終了したり再起動したりする事があります. また, 攻撃のために多数の相手にデータを送出するため, ネットワークの性能が劣化する場合があります.

このワームは感染した PC の TCP ポート 4444 番に遠隔から PC を操作可能な裏口を設置します. このため, 感染した PC をそのままの状態で放置すると PC を外部から不正に利用され, 二次的な被害を受けたり, 別の PC に対する加害者になる危険性があります.

[2] http://www.microsoft.com/japan/security/security_bulletins/ms03-026e.asp
[3] http://support.microsoft.com/?kbid=823980

このワームはマイクロソフト社 Windows Update のウェブサイトにサービス妨害攻撃をかけるように作成されています．しかし，マイクロソフト社側の対策によりこの攻撃は失敗しました．

2.3 亜種について

Blaster ワームの「亜種」と呼ばれるワームがいくつか見つかっています．これらの亜種は，元の Blaster ワームを一部改変し，感染時に作成するファイルやサービス妨害攻撃対象サイトを変更した物です．このような変更が加わったことにより，元の Blaster ワームを検出するように作成された対策ツールでは亜種を検出できない場合があります．このような亜種の情報は随時追加されて行きますので，ウィルス検査ツールや Blaster ワーム対策ツールを利用する場合は最新の物を利用する必要があります．

2.4 Welchia ワームについて

Welchia ワーム[4]は，Blaster ワームと同じ手法を使って感染を広げる新種のワームです．このワームは，感染した PC が既に Blaster ワームに感染していると，Blaster ワームの活動を停止させ，Blaster ワームの作成したファイルを削除します．また，マイクロソフト社のウェブサイトから修正パッチをダウンロードし，Blaster が感染しないように OS を修正してしまいます．

これだけ聞くとこのワームはよいワームに聞こえるかもしれません．しかし，このワームは，Blaster 対策されている PC にも感染していけるように Microsoft IIS ウェブサーバにも攻撃をかけ，感染するように作られています．また，感染する相手を探すために大量の PING パケットを送出し，ネットワークにより大きな負荷をかけます．これらのことから，(作者の意図は不明ですが) 結果的には元の Blaster ワームよりはるかに高い負荷をネットワークにかける，より悪質なワームになっていました．

九州大学でも，この Welchia ワームに感染したホストが多数発生したためにコアスイッチの性能が低下するという事態が発生しています．現在，感染ホストを積極的にネットワークから切り離す事で，ワーム対策をうながしていますが，今だに制圧できていません．

3 対策

Blaster ワーム (亜種・Welchia 含む) を学内から一掃し，安全なネットワークを取り戻すには，Windows 利用者一人一人による対策が必須です． この章では Blaster

[4]Nachi，MSBLAST.D，Lovsan.D などの別名があります

ワームに感染しないための対策及び感染した場合の対処方法について述べます.

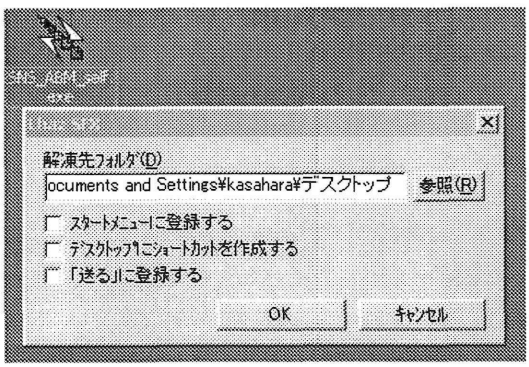
3.1　応急処置

Windows PC を使っていて，Blaster ワームについて何も知らない，またはウィルスなどについて何も対策した覚えがないという人の PC は高い確率で既に感染しています．インターネットに蔓延しているワーム・ウィルスは他にも多数ありますが，Blaster ワームは**PC をインターネットにつないだけで自動的に感染し，他の PC に感染を広げる**ため，事態は非常に深刻です．Windows PC をインターネットに接続する場合には，**Blaster ワーム対策は必須**です.

Blaster ワーム対応には,「駆除」と再感染を防ぐための「対策」が必要です．難しそうに思うかもしれませんが，既に自動対策ツールがいくつか公開されており，これを利用すると簡単です．株式会社 LAC[5]から,「駆除」と「対策」の両方を半自動で処理するツールが公開されていますので，これを利用するのがよいでしょう．Blaster ワームに感染しているかどうかよくわからない場合も含めて，必ず一度はこのツールを使って確認し，対策を実施してください．以下，利用法について説明します[6].

まず `http://www.lac.co.jp/security/jsoc/tool/download/download.htm` から「exe 自己解凍版」をダウンロードし，デスクトップなどに保存します．もし自分の PC が頻繁に再起動するなどの不具合があってダウンロードできないようであれば，他の人に頼むなどして別の PC からダウンロードしてもらい，それをフロッピーディスクなどでコピーしてください．このファイルを入手できたら，以下の作業中に再度感染してしまうのを防ぐために，**PC のネットワークケーブルをはずしてください.** 頻繁な再起動で作業ができない場合は，Windows.FAQ の情報[7]が参考になります.

図 1: 展開

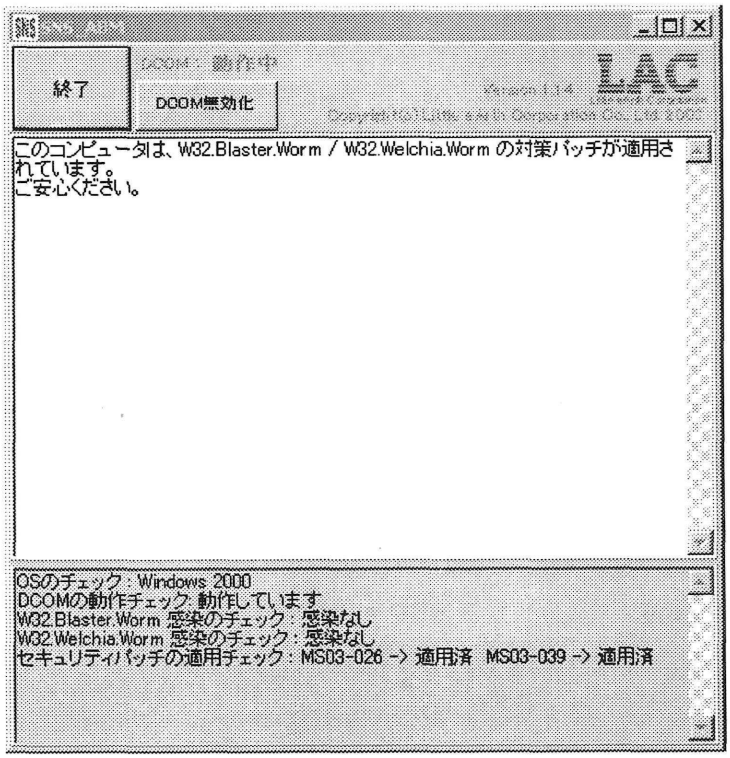


[5] `http://www.lac.co.jp/`
[6] 付属ドキュメントの説明を若干アレンジしています
[7] `http://homepage2.nifty.com/winfaq/blaster.html`

ダウンロードしてきたSNS_ABM_self.exeをダブルクリックします．Lhaz SFXのウィンドウが出ますので，そのままOKをクリックします(図1)．SNS_ABMフォルダができますので，これをダブルクリックで開き，中のSNS_ABM.exe(対策ツール本体)をダブルクリックして実行します．

画面下の「感染のチェック」で感染なしと出ており，また「パッチの適用チェック」で「適用済み」が出ている場合，Blasterワームには感染しておらず，また感染の危険性もありません(図2)．

図2: ツール実行画面



どちらかに感染している場合,「駆除」ボタンを押すことにより駆除できます.「駆除」が完了したら,「DCOM無効化[8]」ボタンを押します．確認画面で「はい」を押してDCOMを停止させます．ここでPCを再起動し，ネットワークケーブルを接続してください[9]．

再度対策ツールを実行し，ワーム感染が無いことを再確認してください．確認したら終了を押します．パッチの適用がされていない場合，Windows Update[10]を実行す

[8]DCOMはBlasterワームが感染に利用するWindowsの機能です
[9]DCOMを無効化していないと，接続した時点で再感染する恐れがあります
[10]ネットワーク経由でWindows OSの不具合を修正する仕組み(後述)

るか聞いてくるので,「はい」をクリックし実行してください．Windows Updateにより，Blasterの根本的な対策が適用されます．終了したら，再度対策ツールを実行し，「対策パッチが適用されています」の表示が出ることを確認してください．確認したら「DCOM有効化」ボタンを押し，DCOMを有効に戻して再起動してください[11]．

これで応急処置は終了です．

3.2　亜種の駆除

3.1節で紹介したLAC社提供のツールは，一部のBlaster亜種に対応していません．このため，このツールだけではワームを駆除できていない可能性があります．Windows Updateにより不具合を修正していれば再感染の心配はありませんが，亜種に感染していないかどうかも確認しておいた方がよいでしょう．

複数のウィルス対策ソフトベンダーからBlasterワームに対応した無料駆除ツールが公開されていますが，今の所以下の物が多数の亜種に対応しているようです (他にもあるかもしれません)．

- シマンテック W32.Blaster.Worm 駆除ツール
  `http://www.symantec.co.jp/region/jp/sarcj/data/w/w32.blaster.worm.removal.tool.html`
- トレンドマイクロ ダメージクリーンナップサービス
  `http://www.trendmicro.co.jp/esolution/solutionDetail.asp?solutionId=4700`

トレンドマイクロの駆除ツールはBlasterワーム以外にも一部の有名 (?) なウィルス・ワームに対応しています．今までウィルス対策に無頓着だった場合，知らないうちに他のウィルス等に感染している可能性があり，このツールを利用して駆除できるかもしれません．一般的なウィルス・ワームに関してより完全な駆除・対策を施すには，市販のウィルス駆除ソフトを導入する必要があるでしょう．

4　今後に向けての対策

4.1　欠陥と修正

Blasterワームが利用したWindowsの欠陥 (セキュリティホール) は，Blasterワームが出現する約一ヶ月前に発見され，修正された物でした．その時点でWindows OSに修正パッチを適用していれば，感染するはずはなかった物です．それにもかかわら

[11] DCOMを無効化したままだとWindowsの機能が一部制限されます

ず，Blasterは世界中に蔓延し，また九州大学の内部でも1000台に及ぶPCが感染しました．テレビや新聞でもかなり取り上げられたにもかかわらず，今だに対策されていないPCが多数あります．

Blasterワームは「幸いにして」破壊活動をしないワームでした．しかし，Blasterワームと同じ手法を使い，PCを再起不能にするのは非常に簡単なのです．ウィルスやワームに感染するのを予防する手間と，感染し破壊された物を復旧する手間では，はるかに後者の方が大きいものです．

また，みなさんがお使いのソフトウェア(Windowsに限らず)には常に欠陥(バグ)がつきものであることを理解してください．ソフトウェアの公開前に，全ての欠陥を発見するのは不可能です(無限の時間が必要)．ソフトウェアというのは，ある程度の完成度に達した時点で公開・発売され，その後利用者の報告などにより改善されていく物です．テレビや電話のように，買ってきたらそのまま使えばいいという物ではなく，定期的に修正していかなければならない物なのです．

幸いにして，Windows製品にはネットワークを通じて簡単に修正を適用する仕組み「Windows Update」が提供されています．Blasterワーム発生後も，また別の欠陥が発見され，修正パッチが公開されています．これを放置すれば，ほどなくBlasterよりもっと悪質なワームが作成され，あなたのPCを襲うのは間違いありません．

4.2 Windows Updateについて

Windows Updateはインターネットに接続されているWindowsなら簡単に利用できます．スタートメニューに「Windows Update」が用意されていますので[12]，それをクリックしてください．インターネットエクスプローラーが起動し，Windows Updateページが表示されます．あとは画面の指示に従って「重要な更新とService Pack」を適用してください[13]．Windows Updateを使うのはこれが初めてというようなPCの場合，同時に導入できない修正があるため，一回の操作では全部の修正が終わりません．このため，再起動を含めて何回かWindows Updateを繰り返す必要があります．**重要な更新とService Packの一覧が空になるまで**全ての修正を適用しなければなりませんので注意してください．

また，Windows XPには，マイクロソフト社から「重要な更新」が公開された時にこれを利用者に通知したり，自動的にダウンロード・適用する「自動更新」という機能があります．Windows 2000などでもWindows Updateでこの機能を追加する事ができます．「重要な更新」の公開を検知すると，タスクバーにアイコンと共に通知が表示されます．時々，これが表示されているのに放置している人がいるようですが，これではマイクロソフト社が「重要な更新」を作成し公開しても意味がありません．「重

[12]Windows XPでは「すべてのプログラム」の中にあります
[13]http://www.microsoft.com/japan/security/square/guard/a04g11.aspに図解があります

要な更新」を適用するとPCを再起動する必要がある場合がほとんどですので，作業中には適用できないかもしれませんが，できるだけはやく適用しましょう．

5　おわりに

本稿では，Blasterワームの概要と対策について紹介し，また同様の被害を受けないようにするための基本的な方法としてWindows Updateを紹介しました．Blasterワームは九大内でも今だに制圧できておらず，このため**新しくインストールしたWindows PCをネットワークに接続するとすぐに感染する危険性がある**という状況です．少なくとも感染ホストを全て対策し，学内ネットワークにBlasterワームによる攻撃が流れていない状態にする必要があります．このためには利用者一人一人の協力が必須です．また，Windowsマシンを新規に購入したり，OSを再インストールしたりした場合には，ネットワークに接続する前に対策する必要があります．マイクロソフト社のページ「パソコンを守るための3つの手順[14]」を是非読んでください．

3章「対策」では，なるべく技術的な知識の必要ない自動ツールを紹介しています．最低でもここに書いた内容はやっておいて欲しいと思います．しかし，これだけではBlasterの対策はできても，今後現れてくる新手のワーム・ウィルスの対策にはなりません．4章で述べたように，Windows UpdateによってOSを常に最新の状態にしておけば，今後新種のワームが登場した時にも，自分が感染して管理者や回りの利用者に迷惑をかける危険性はかなり小さくなるでしょう[15]．

6　参考URL

- Microsoft セキュリティ(一般ユーザ向け)
  `http://www.microsoft.com/japan/security/`
- Microsoft TechNet セキュリティセンター (より高度な情報)
  `http://www.microsoft.com/japan/technet/security/`
- Blasterに関する情報 (他社からの情報へのリンクが多数あります)
  `http://www.microsoft.com/japan/technet/security/virus/blaster.asp`
- Windows Update
  `http://windowsupdate.microsoft.com/`

[14] `http://www.microsoft.com/japan/security/protect/default.asp`
[15] マイクロソフト社の修正よりワームが先に流行したらどうしようもありませんが…