IPA
Information-technology Promotion Agency, Japan

W32/MSBlaster（Blaster）ワームまたはW32/Welchia（Nachi）ワームに感染した場合の復旧方法について　（Windows XP用）Ver.1.4a

2004年 6月 18日
独立行政法人 情報処理推進機構
セキュリティセンター(IPA/ISEC)

本書では、W32/MSBlaster（Blaster）ワームまたはW32/Welchia（Nachi）ワームに感染したWindows XPコンピュータ以外にインターネットに接続できるコンピュータが無い場合の復旧方法をまとめています。復旧は、以下の手順で進めます。

1．コンピュータをインターネットから物理的に切り離す

まず、コンピュータがネットワークにつながらないようにして、ネットワークから攻撃を受けないようにします。再起動がかかる症状を一時的に止めます。

ADSL、CATV(ケーブルテレビ)、FTTH(光ファイバ)を利用している場合：

- **電源を入れる前に、コンピュータのLANケーブル（イーサーネットケーブル）を抜いてください。**
- **無線LANを使用している場合はルータ等の電源を切ってください。**

LANケーブル（右図）の抜き方

コンピュータの裏面にはLANケーブル（イーサーネットケーブル）の穴（ポート）があります（各PCのメーカーによって若干異なります）。
LANケーブルを抜く際は、ツメをつまんだ状態で抜きます。

ダイアルアップ接続を利用している場合：

- **電話線をパソコン本体から抜いてください。**
  ISDNをお使いの場合には、USBケーブルで接続されている場合があります。

2. 「インターネット接続ファイアウォール」を有効にする

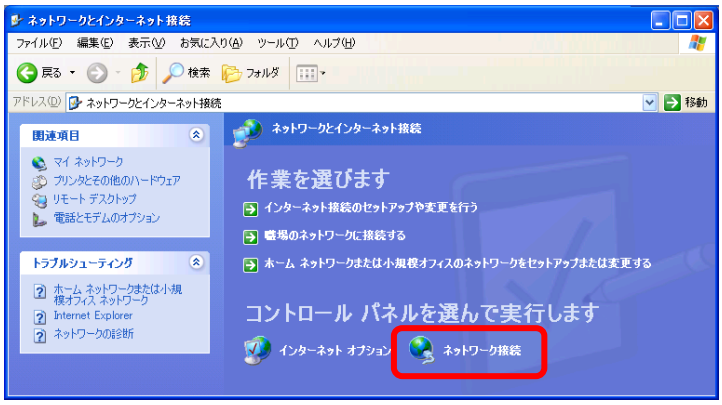
Windows XP の「インターネット接続ファイアウォール」機能を使って、復旧手順中のワームからの妨害と（再）感染を防ぎます。

● [スタート] メニューから
[コントロールパネル] を開き、
[ネットワークとインターネット接続] を
選択します。

● 続いて [ネットワーク接続] をクリックします。

※うまく表示できない場合には、以下の手順を試してください。

- [スタート]の[設定]から[ネットワーク接続]を選択
- [スタート]の[接続]から[全ての接続の表示]を選択
- [スタート]の[マイネットワーク]から、ネットワークタスク（左側）の[ネットワーク接続を表示]を選択

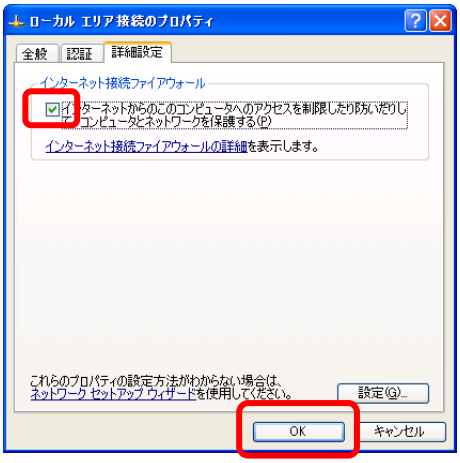


● マウスの左クリックで普段、使っている
ネットワーク接続設定を選択して、[ネットワークタスク]の [この接続の設定を変更する] をクリックします。

ADSL、CATV、FTTH 接続の方 …
　ローカルエリア接続
無線 LAN 接続の方 …
　ワイヤレスネットワーク接続
電話回線接続の方 …
　ダイアルアップ接続の下のいずれかの接続

※　どれか分からない場合、全てについて、下記の「インターネット接続ファイアウォール」の設定を行ってください。

● [詳細設定] タブをクリックし、
[インターネットからのこのコンピュータへのアクセスを制限したり防いだりして、コンピュータとネットワークを保護する] という項目の左のチェックをつけます。



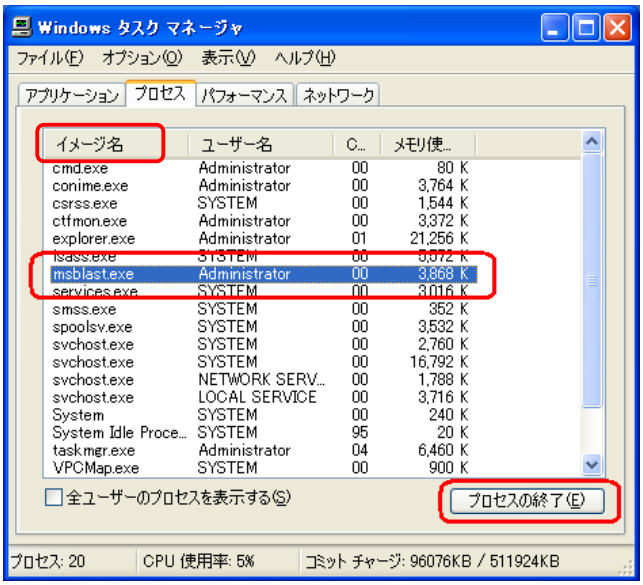
● 必ず[OK ボタン]を押して閉じます 。
その後、再起動してください。

3．ワームのプログラムを停止する

※ワクチンソフトをお使いの方は、この作業を行う前にワクチンソフトを無効にしてから行ってください。

3-1．W32/MSBlaster編

W32/MSBlaster ワーム感染時に動作しているワームのプログラム（msblast.exe）の動作を停止します。



● [Ctrl]＋[Shift] キーを押しながら[Esc]キーを押し、タスクマネージャを実行します。

● [プロセス] タブをクリックして表示します。

●「イメージ名」と書かれた欄のタイトル部分をクリックしてアルファベット順に並べ直します。

● イメージ名の欄で、“ msblast.exe ”というプログラムを探します。もしあれば、
その名前をマウスで左クリックして色を反転させ、[プロセスの終了] ボタンをクリックします。

注意１：このワームには複数の亜種が発見されています。亜種により感染時に動作しているワームプログラムが異なりますので、以下の７種類のワームプログラムについてもイメージ名の欄で、探してください。もしあれば、同様の作業を行ってください。

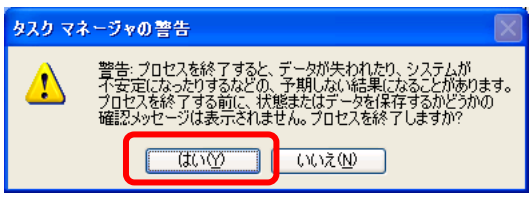
他のワームプログラム： teekids.exe 、penis32.exe 、mspatch.exe

mslaugh.exe、Enbiei.exe、mschost.exe、svchosthlp.exe

注意２：W32/Welchia ワームに感染している場合には、イメージ名に“ DLLHOST.EXE ”が存在します。この名前が見つかった場合には、「3-2．W32/Welchia 編」へ進んでください。

注意３： ワームが動作していない場合には“ msblast.exe ”や“ DLLHOST.EXE ”などのプログラムは一覧にありません。
右上の［×］ボタンをクリックしてタスクマネージャを終了してください。
その後は、「4．コンピュータをネットワークに再接続する」へ進んでください。

● タスクマネージャの警告が表示されますが、[はい] をクリックします。

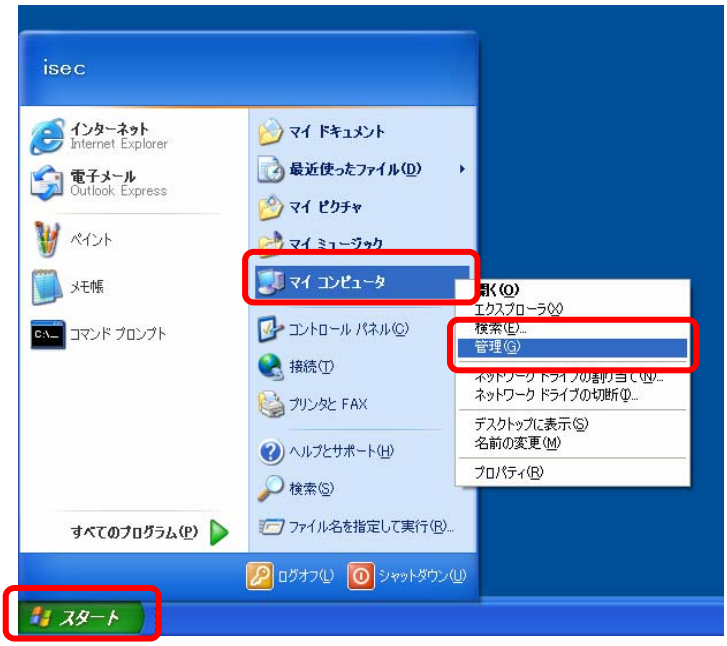


● タスクマネージャを見て“ msblast.exe ”プログラムがプロセスから消えたことを確認します。

● タスクマネージャの右上の［×］ボタンをクリックして終了します。

3-2 W32/Welchia編

W32/Welchia ワーム感染時に動作しているワームのプログラムの動作を停止します。

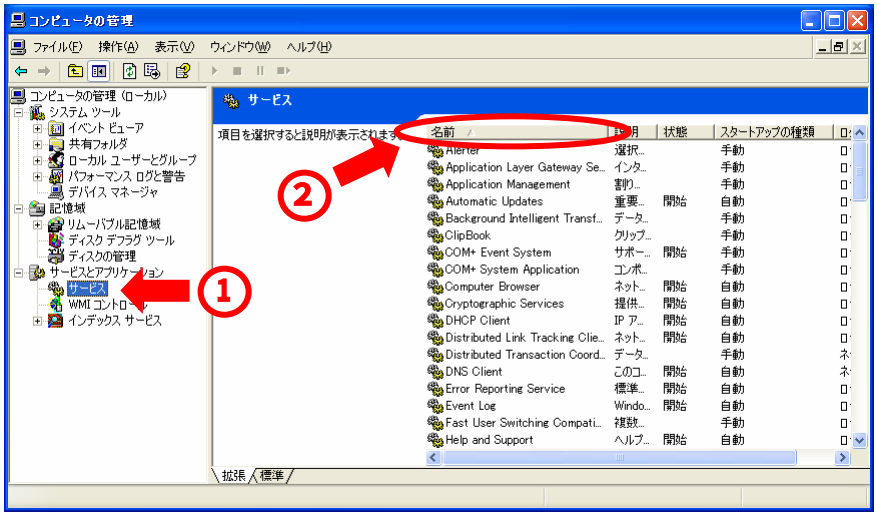


● [スタート] ボタンをクリックしてメニューを開きます。

● メニューの[マイコンピュータ] を右クリックします。

● 開いたメニューの中の [管理]を左クリックして選択します。

● ウィンドウの右側で [サービスとアプリケーション] をダブルクリックします。



● [サービス] (右図①) をクリックします。

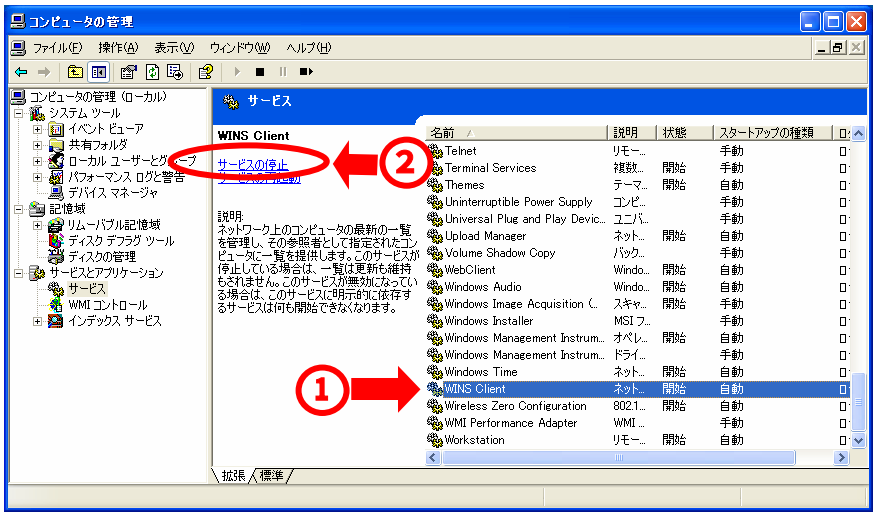
アルファベット順に並んでいない場合は [名前] (右図②) と書かれた欄のタイトル部分をクリックすると並べ直すことができます。

● 「名前」の欄に

“Network Connections Sharing”

“WINS Client”

があれば、
左クリックで選択し (右図①)、[サービス停止] (右図②) をクリックします。小さなウィンドウが開いて、削除中の表示になり、元の画面に戻ります。

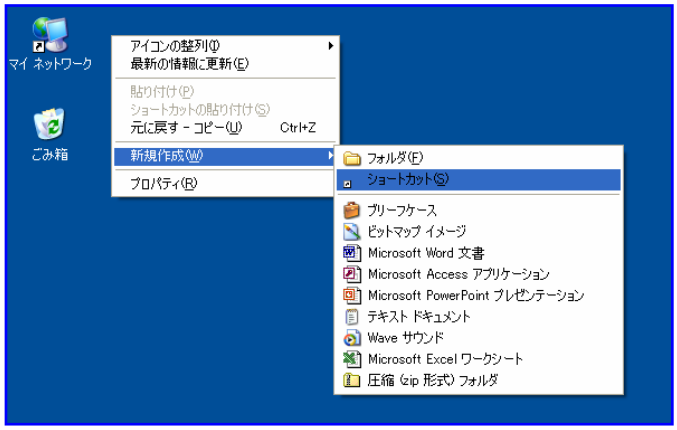


● この操作を繰り返して、2 つのサービスを停止します。

注意： ワームが動作していない場合には“Network Connections Sharing”や“WINS Client”は、一覧にありません。右上の [×] ボタンをクリックして終了し、「4. コンピュータをネットワークに再接続する」へ進んでください。また、“Network Connections Sharing”で[サービス停止]がなければ、そのまま次の手順へ進んでください。

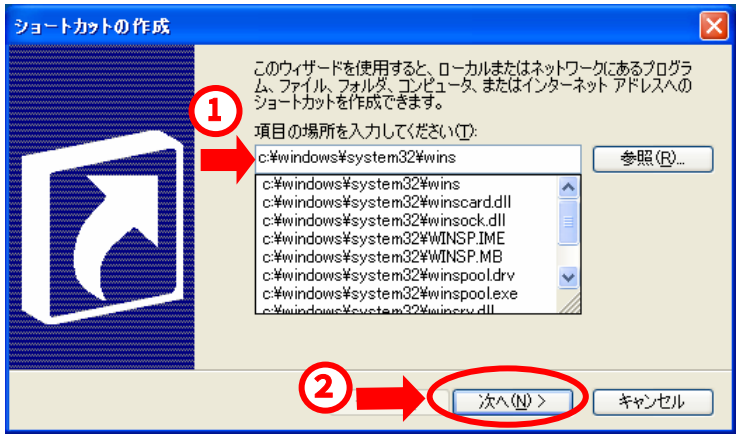
● 「コンピュータの管理」のウィンドウの
右上の［×］ボタンをクリックして画面を
閉じてください。

● デスクトップ（画面上の何も無いところ）で
右クリックしてメニューを開きます。（右図）



● メニューから
［新規作成］－［ショートカット］を
選択してクリックします。

● ショートカットの作成が開きます。
入力する部分（右図①）に、次のとおりに
キーボードから入力します。



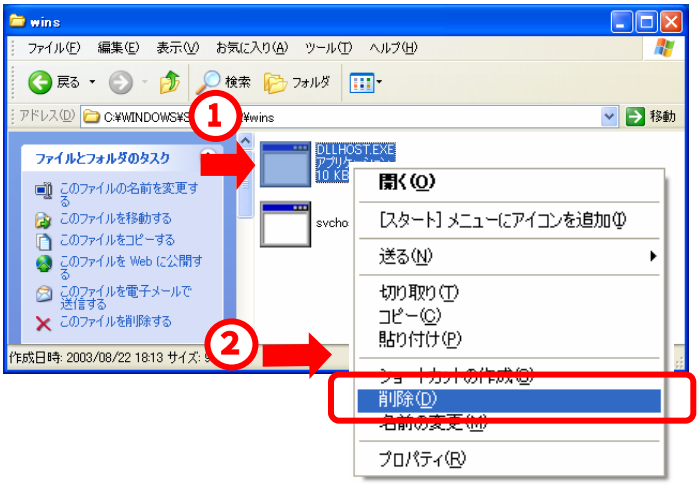
C:\windows\system32\wins

　正しく入力すると、すぐ下の枠内にも同じ
文字列が表示されます。
　表示されない場合は、入力が間違っていま
すので、良く確認して再度入力してください。

● ［次へ］をクリックします。［完了］をクリックします。ウィンドウが閉じます。

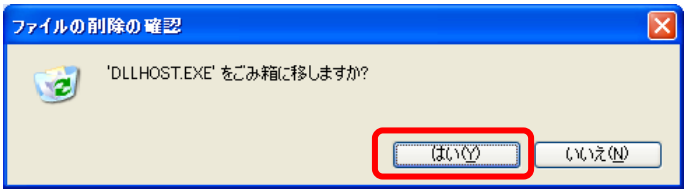
● デスクトップに新しくできたアイコン“ wins ”（右図参照）を
ダブルクリックします。

● 開いたウィンドウの右側に、
“ svchost.exe ”、“ DLLHOST.EXE ”
のアイコンが表示されたら、以下の方法で、
これら２つのファイルを削除してください。



● アイコン（右図①）を右クリックして
メニューを開き、「削除」を選んで
クリックします。（右図②）

● 確認メッセージ（右図）が出たら
「はい」を選択します。
読み取り専用の場合も「はい」を押して
削除してください。



● ２つのファイルを削除したら「4．コンピュータをネットワークに再接続する」に進みます。

4．コンピュータをネットワークに再接続する

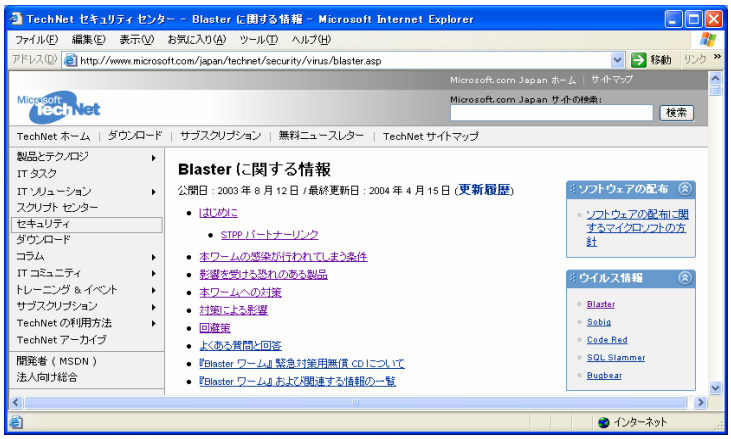
● 外しておいた LAN ケーブル（イーサーネットケーブル）、電話線を再度つなぎます。

5．マイクロソフト社の修正プログラム（MS04-012）を適用する

ワームが悪用する脆弱性について、セキュリティ修正プログラムをダウンロードして適用します。

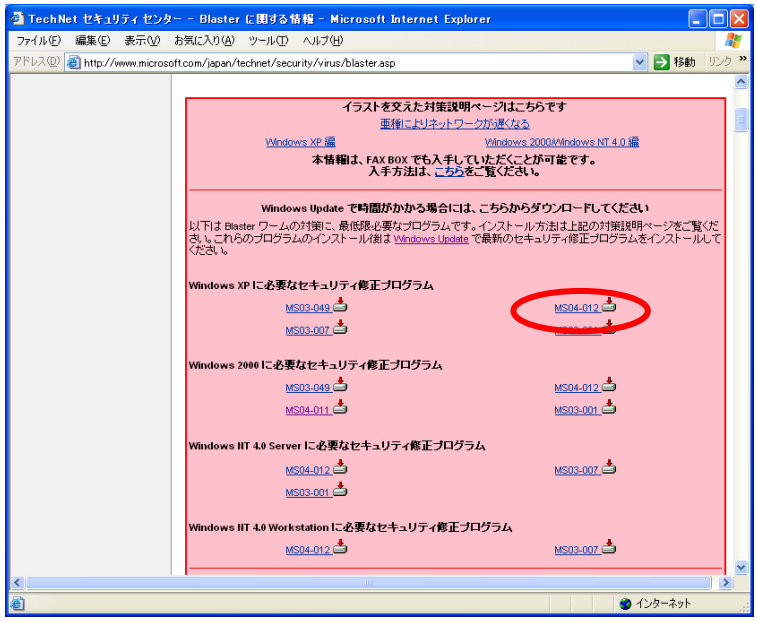
● Microsoft Internet Explorer（ホームページを見るプログラム）を使って、マイクロソフトの Web サイト（右図）にアクセスします。

http://www.microsoft.com/japan/technet/security/virus/blaster.asp



● 「Blaster に関する情報」のページが出ます。

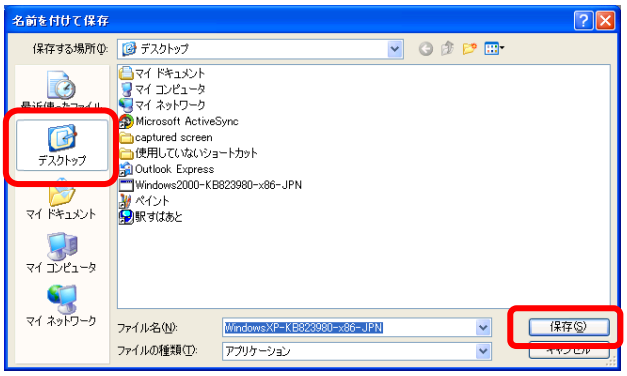
● スクロールしてページの少し下を見てください。



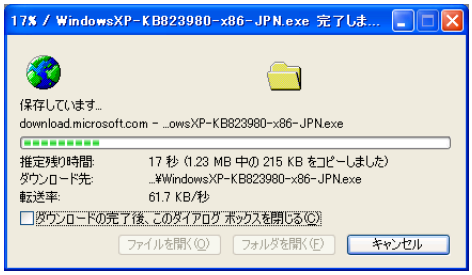
● ピンクの四角の中の「Windows Update で時間がかかる場合にはこちらからダウンロードしてください」の項目から「Windows XP に必要なセキュリティ修正プログラム」の下の「MS04-012」をクリックします。

● 「保存」をクリックします。

● 「デスクトップ」をクリックして、
「保存」をクリックします。



● 修正プログラムがダウンロードされます
（ダウンロード終了後にウィンドウが残ったら消してください）。
ダウンロード時間の目安：
ダイアルアップ経由 約 3 分
ブロードバンド経由 約 1 分



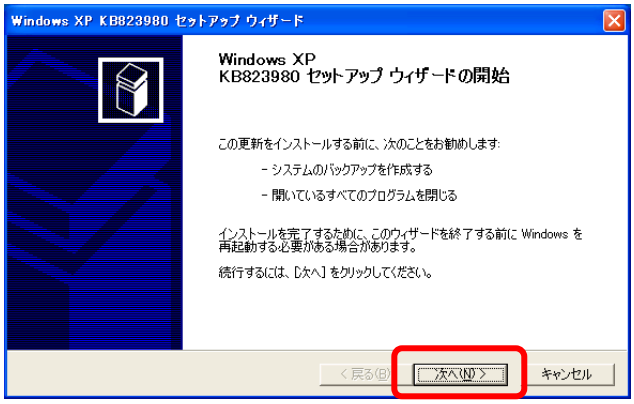
● デスクトップ上に修正プログラム（WindowsXP-KB828741-x86-JPN.exe）が保存されます。
（右図のアイコン）

● 修正プログラムをダブルクリックして実行します。
（修正プログラムのインストールが完了したら、このファイルは削除しても構いません。）

※ 画面に右のようなアイコンが出ない場合は、画面上の何も表示されていないところで右クリックし、
「最新の情報に更新」を選択してください。

● セットアップウィザードが起動します。
[次へ] をクリックし、
[同意します]をクリックし、
[次へ] をクリックします。
修正プログラムがインストールされます。

● [完了] をクリックすると自動的に再起動がはじまります。
※再起動を要求されたら、再起動を実行します。



6. 必要な場合 もう一度ワームのプログラムを停止する

修正プログラムインストール後の再起動の後に、W32/MSBlaster ワームが再度起動されることがあります。

● 「3-1. W32/MSBlaster 編」に従って、タスクマネージャを実行し、このワームのプログラム（msblast.exe 等）が動いているかどうかを確認してください。

● ワームのプログラム“msblast.exe”等が動いていた場合には、「3-1. W32/MSBlaster 編」に従って、もう一度停止してください。

7．ツールを利用してワームを駆除する

ウイルス対策ソフトウェアベンダー等各社より提供されている駆除ツールを入手し、駆除を行います。手動で削除するよりも、確実で安全に駆除をすることができます。

● 以下に駆除ツールの掲載先を記載します。こちらからダウンロードしてください。
● ツールの使用方法については、各社のページをよくご確認ください。

株式会社シマンテック 提供　（上：W32/MSBlaster 用、下：W32/Welchia 用）
http://www.symantec.com/region/jp/sarcj/data/w/w32.blaster.worm.removal.tool.html
http://www.symantec.com/region/jp/sarcj/data/w/w32.welchia.worm.removal.tool.html

トレンドマイクロ株式会社 提供　（W32/MSBlaster、W32/Welchia 兼用）
http://www.trendmicro.co.jp/esolution/solutionDetail.asp?solutionId=4700

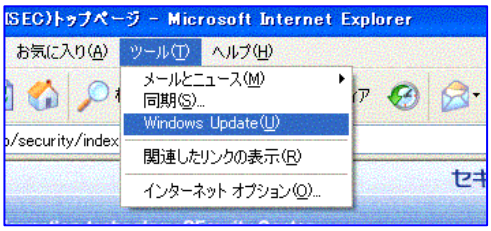
日本ネットワークアソシエイツ株式会社 提供　（W32/MSBlaster、W32/Welchia 兼用）
http://www.nai.com/japan/security/stinger.asp

株式会社ラック 提供　（W32/MSBlaster、W32/Welchia 兼用）
http://www.lac.co.jp/security/jsoc/tool/download/download.htm

※IPA セキュリティセンター（http://www.ipa.go.jp/security/）のページに設けたリンクから辿ることもできます。

8．今後のために

● 以上で MSBlaster、Welchia ワームに関する対策は完了です。



● Windows Update を使用して、その他のセキュリティ修正プログラムをインストールすることをお勧めします。他のウイルス/ワームや不正アクセスへの予防となります。

※ Windows Update を開始する前に、作業中の内容を保存して、すべてのプログラムを閉じてください。

(1) Windows Update を使うためには、Internet Explorer から、「お気に入り(A)」の右隣にある「ツール(T)」をクリックしてメニューを開き、「Windows Update」を選択してください。
(2) [更新をスキャンする] をクリックしてください。
(3) 「重要な更新と Service Pack」の数が 0 ならば、作業完了です。0 以外なら次に進んでください。
(4) [更新の確認とインストール] をクリックし、[今すぐインストールをする] をクリックしてください。許諾の確認後、ダウンロードとインストールが始まります。
(5) 更新によっては、コンピュータの再起動が必要になる場合があります。必要ならば再起動してください。再起動後は、もう一度 Windows Update を使い、この手順の(1)から作業を再開してください。

● 新しい修正が追加されることがありますので、定期的に Windows Update を使うことをお勧めします。

【参考】

修復方法等を掲載したマイクロソフト社のホームページ：

Blaster に関する情報

http://www.microsoft.com/japan/technet/security/virus/blaster.asp

Blaster ワームへの対策 - Windows XP 編

http://www.microsoft.com/japan/technet/security/virus/blasterE_xp.asp

Blaster ワームへの対策 - Windows 2000/Windows NT 4.0 編

http://www.microsoft.com/japan/technet/security/virus/blasterE_nt4w2k.asp

その他：W32/MSBlaster に関する情報

シマンテック：

http://www.symantec.com/region/jp/sarcj/data/w/w32.blaster.worm.html

トレンドマイクロ：

http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.A&VSect=T

日本エフセキュア：

http://www.f-secure.co.jp/v-descs/v-descs3/lovsan.htm

日本ネットワークアソシエイツ：

http://www.nai.com/japan/security/virL.asp?v=W32/Lovsan.worm.a

アンラボ：

http://ahnlab.co.jp/virusinfo/view.asp?seq=732

アラジンジャパン：

http://www.aladdin.co.jp/esafe/virus/v_all/Win32_Blaster.html

ソフォス：

http://www.sophos.co.jp/virusinfo/analyses/w32blastera.html

株式会社ラック

http://www.lac.co.jp/security/jsoc/tool/download/download.htm

「W32/MSBlaster」ワームに関する情報（IPA セキュリティセンター）：

http://www.ipa.go.jp/security/topics/newvirus/msblaster.html

その他：W32/Welchia に関する情報

シマンテック：(W32.Welchia.Worm)

http://www.symantec.com/region/jp/sarcj/data/w/w32.welchia.worm.html

トレンドマイクロ：(WORM_MSBLAST.D)

http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.D

日本エフセキュア：(Welchi)

http://www.f-secure.co.jp/v-descs/v-descs3/welchi.htm

日本ネットワークアソシエイツ：(W32/Nachi.worm)

http://www.nai.com/japan/security/virN.asp?v=W32/Nachi.worm

アンラボ：(Win32/Welchia.worm. 10240)

http://ahnlab.co.jp/virusinfo/view.asp?seq=736

ソフォス：(W32/Nachi-A)

http://www.sophos.co.jp/virusinfo/analyses/w32nachia.html

「W32/Welchia」ワームに関する情報（IPA セキュリティセンター）：

http://www.ipa.go.jp/security/topics/newvirus/welchi.html

この手順書は、IPA セキュリティセンターのホームページにも掲載しています。

アドレス　　http://www.ipa.go.jp/security/