

W32/Sasser ワームに感染した場合の復旧方法について (Windows XP 用) Ver.1.1

2004年5月7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)

この文書は、W32/Sasser ワームに感染した Windows XP コンピュータの復旧方法を示します。これは、感染したコンピュータ以外に手近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方法です。復旧は、以下の手順を進めます。

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
2. ワームのプログラムを停止する
3. 「インターネット接続ファイアウォール」を有効にする
4. コンピュータをネットワークに接続する
5. ツールを利用してワームを駆除する
6. マイクロソフト社のセキュリティ更新プログラムを適用する
7. 今後のために

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、コンピュータがインターネット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)等の回線を利用している場合：

コンピュータの電源を入れる前に、コンピュータ本体から LAN ケーブル(イーサネットケーブル)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。



電話回線上でダイヤルアップ接続を利用している場合：

電話線をコンピュータ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. ワームのプログラムを停止する

ウイルス対策ソフトをお使いの方は、この作業を行う前にウイルス対策ソフトを無効にしてから行ってください。

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

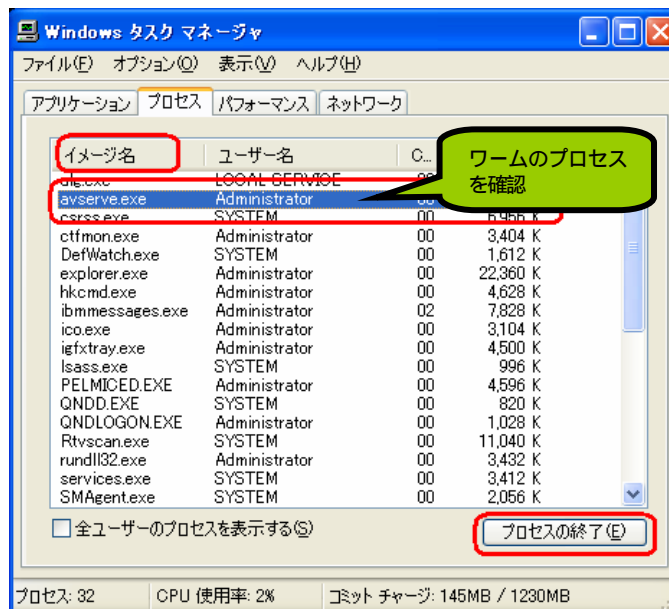
[Ctrl] + [Shift] キーを押しながら [Esc] キーを押し、タスクマネージャを実行します。

[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、次の名称のプログラムを探します。

- (1) “ avserve.exe ”
- (2) “ avserve2.exe ”
- (3) “ skynetave.exe ”
- (4) 後半に _up.exe が付き、プロセス名の前半に、4 つ、あるいは、5 つの数字が付くプロセス
(例: 54321_up.exe)



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。

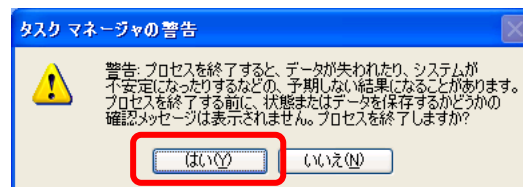
注意 1: ワームが動作していない場合 “ avserve.exe ” や “ avserve2.exe ” などのプログラムは一覧にありません。

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、「3. 「インターネット接続ファイアウォール」を有効にする」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 “ avserve.exe ” 等の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。

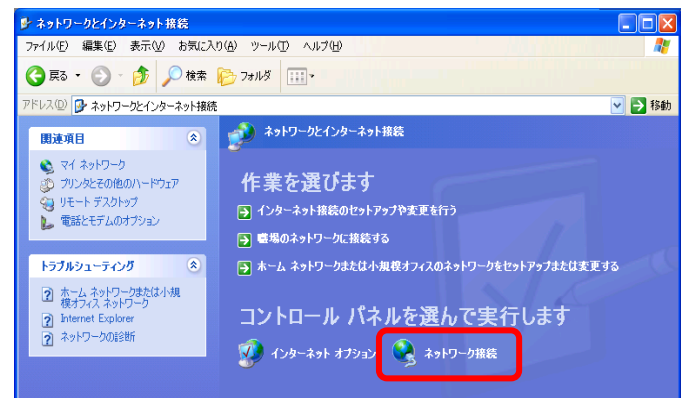
3. 「インターネット接続ファイアウォール」を有効にする

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 ...

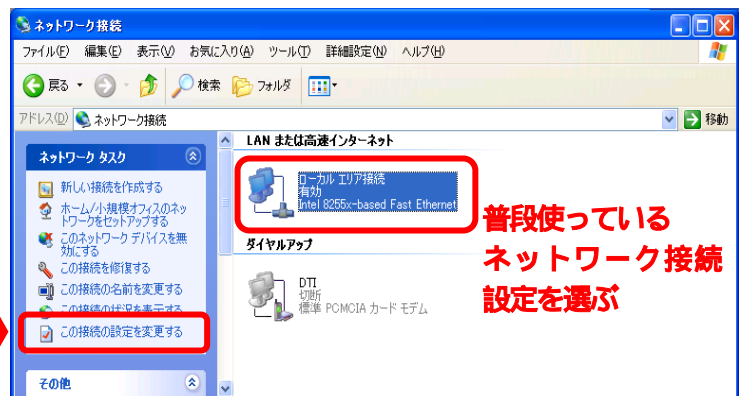
ローカルエリア接続

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 ...

ダイヤルアップ接続の下のいずれかの接続

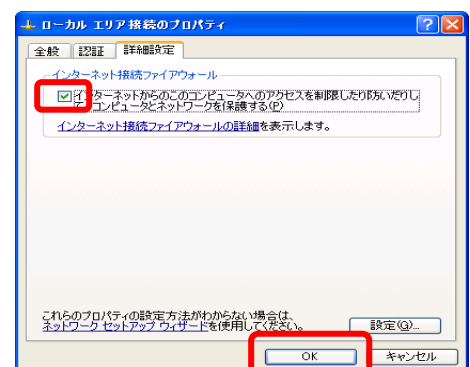


どの接続方法が分からない場合、全てについて、下記の「インターネット接続ファイアウォール」の設定を行ってください。

[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 にチェックをつけます。

必ず [OK ボタン] を押して閉じます。

アイコンの横に「ファイアウォール」と表示されていることを確認します。



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（イーサネットケーブル）、電話線を再度つなぎます。

5. 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、確実に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。Microsoft Internet Explorer（ホームページを見るプログラム）を使って、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確認してください。

株式会社シマンテック 提供

<http://www.symantec.com/region/jp/sarcj/data/w/w32.sasser.removal.tool.html>

トレンドマイクロ株式会社 提供

<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

<http://www.nai.com/japan/security/stinger.asp>

6. マイクロソフト社のセキュリティ更新プログラムを適用する

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

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

Windows Update を次の手順で実施します。

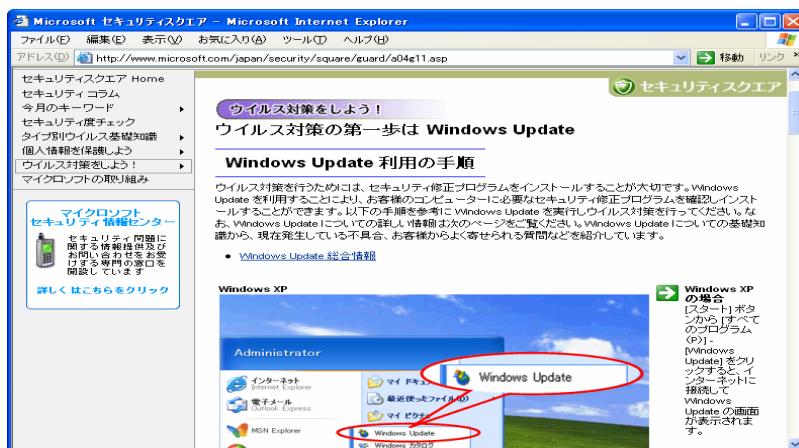
Microsoft Internet Explorer（ホームページを見るプログラム）を使って、マイクロソフト社の Web サイトにアクセスします。

「Windows Update 利用の手順」（マイクロソフト社）

<http://www.microsoft.com/japan/security/square/guard/a04g11.asp>

「Windows Update 利用の手順」のページが出ます。（右図）

ページの手順にしたがって Windows Update を実行してください。



電話回線上でダイヤルアップ接続を利用している場合：

Microsoft Internet Explorer (ホームページを見るプログラム) を使って、個別の修正プログラム (MS04-011) を次の URL からダウンロードしてください。

<http://download.microsoft.com/download/5/7/b/57bc7cca-10f7-4afb-9220-231c26ee6f03/WindowsXP-KB835732-x86-JPN.EXE>

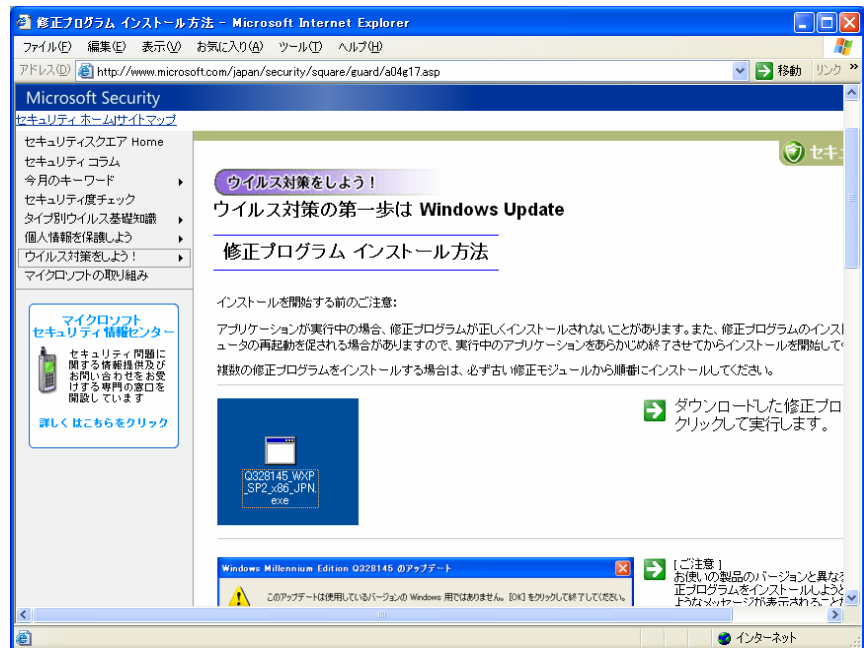
上記プログラムのインストール手順は、次のマイクロソフト社の Web サイトにアクセスします。

「修正プログラム インストール方法」(マイクロソフト社)

<http://www.microsoft.com/japan/security/square/guard/a04g17.asp>

「修正プログラム インストール方法」のページが出ます。(右図)

ページの手順にしたがって修正プログラムをインストールしてください。



7. 今後のために

以上で Sasser ワームに関する対策は完了です。

Windows に対する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。

手順は、「6. マイクロソフト社のセキュリティ更新プログラムを適用する」を参照してください。

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：

Sasser ワームについてのお知らせ

<http://www.microsoft.com/japan/security/incident/sasser.msp>

ホームユーザー向け - Sasser ウイルスに関する情報 Windows XP 編

http://www.microsoft.com/japan/security/incident/sasser_xp.msp

ホームユーザー向け - Sasser ウイルスに関する情報 Windows 2000 編

http://www.microsoft.com/japan/security/incident/sasser_2k.msp

その他：W32/Sasser に関する情報

シマンテック：

<http://www.symantec.com/region/jp/sarcj/data/w/w32.sasser.worm.html>

トレンドマイクロ：

http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM_SASSER.A

日本エフセキュア：

<http://www.f-secure.co.jp/v-descs/v-descs3/sasser.htm>

日本ネットワークアソシエイツ：

<http://www.nai.com/japan/security/virus.asp?v=W32/Sasser.worm>

アンラボ：

<http://japan.ahnlab.com/virusinfo/view.asp?seq=856>

アラジンジャパン：

http://www.aladdin.co.jp/esafe/virus/v_all/Win32_Sasser.html

ソフォス：

<http://www.sophos.co.jp/virusinfo/analyses/w32sassera.html>

コンピュータアソシエイツ：

http://www.caj.co.jp/virusinfo/2004/win32_sasser_a.htm

新種ワーム「W32/Sasser」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/sasser.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/>