

## ウイルス解析報告書

<b>ウイルス名</b>	W32.Sobig.F@mm (別名: Sobig.F [F-Secure], W32/Sobig.f@MM [McAfee], WORM SOBIG.F [Trend], W32/Sobig-F [Sophos], Win32.Sobig.F [CA], I-Worm.Sobig.f [KAV])						
<b>プログラム名及び容量(添付ファイル名)</b>	プログラム名: winppr32.exe 容 量 : 約 72,000 バイト 添付ファイル名: your_document.pif、document_all.pif、thank_you.pif、your_details.pif、details.pif、document_9446.pif、application.pif、wicked_scr.scr、movie0045.pif						
<b>種 別</b>	ワーム						
<b>プログラム言語</b>	不明						
<b>発 症 環 境</b>	Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows XP						
<b>発 見 日 時</b>	2003 年 8 月 19 日						
<b>発見場所(発信地)</b>	アメリカ(最初の感染報告があった場所)						
<b>危 険 性</b>	大量にメールを送信して感染を広げるだけでなく、ネットワーク資源を調べ、アクセス可能な他のコンピュータ上に自分自身をコピーするため感染範囲が広く危険。危険度は 5 段階の 4(5 が最も危険)。						
<b>発 症 条 件</b>	このワームは、.dbx、.eml、.hlp、.htm、.html、.mht、.wab、.txt の拡張子をもつファイルに存在する全ての電子メールアドレスに自分自身を送りつける大量メール発信型、ネットワーク認識型のワーム。独自の SMTP エンジンを利用して拡散する。また、アクセス可能な共有ネットワークに自分自身のコピーを作成しようとするが、コード内のバグのためコピーに失敗する。						
<b>ウイルスの活動、影響</b>	ファイルを開いたとき、2003 年 9 月 10 日に活動を停止する。						
<b>被 害 規 模</b>	大規模に感染が報告されている						
<b>変種、亜種の有無</b>	2003 年 1 月以降 Sobig の 6 種類のが蔓延した。それぞれの簡単な比較を記す。						
	Sobig 亜種	W32.Sobig.A	W32.Sobig.B	W32.Sobig.C	W32.Sobig.D	W32.Sobig.E	W32.Sobig.F
	発見日	2003/1/9	2003/5/18	2003/5/31	2003/6/18	2003/6/25	2003/8/18
	危険度	3	3	3	3	3	4
	ウイルス実行ファイル	winmgm32.exe	msscn32.exe	msscvb32.exe	cftrb32.exe	winssk32.exe	winppr32.exe
	ファイルサイズ	65,536 バイト	52,898 バイト	約 59 キロバイト	57,856 バイト	86,528 バイト 82,195 バイト (zip)	約 72,000 バイト
	作成ファイル	winmgm32.exe dwn.dat	hnks.ini msdbr.ini	msddr.dll msddr.dat	dftm32.dat rssp32.dat	msrrf.dat	winstt32.dat
	活動の終焉	特に無し	2003/5/31	2003/6/8	2003/7/2	2003/7/14	2003/9/10
	差出人	big@boss.com	support@microsoft.com	bill@microsoft.com	admin@support.com 等	support@yahoo.com 等	admin@internet.com 等
	その他						差出人のなりすまし
	<p><b>ワームによって送信されるメールには次のような特徴がある。</b></p> <p><b>差出人:</b> 殆どの場合、差出人を詐称したアドレスを使用するが、admin@internet.com というアドレスを使用することもある。</p> <p><b>件名:</b></p> <ul style="list-style-type: none"> <li>・ Re: Details</li> <li>・ Re: Approved</li> </ul>						

**ウイルスの動作概要**

- ・ Re: Re: My details
- ・ Re: Thank you!
- ・ Re: That movie
- ・ Re: Wicked screensaver
- ・ Re: Your application
- ・ Thank you!
- ・ Your details

**本文:**

- ・ See the attached file for details
- ・ Please see the attached file for details.

**添付ファイル:**

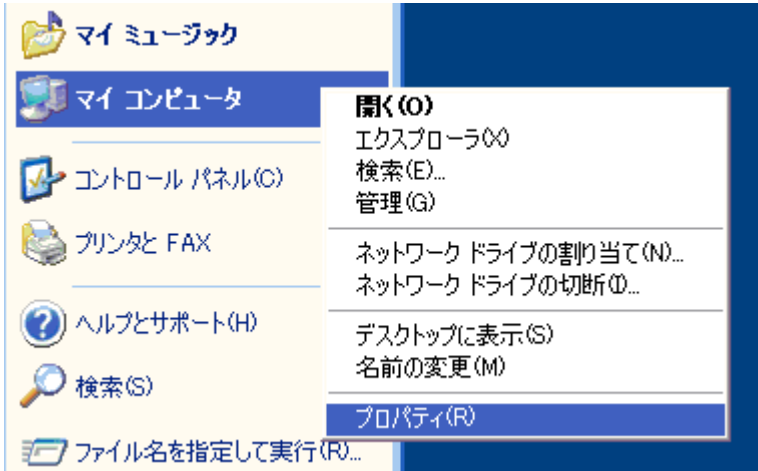
- ・ your\_document.pif
- ・ document\_all.pif
- ・ thank\_you.pif
- ・ your\_details.pif
- ・ details.pif
- ・ document\_9446.pif
- ・ application.pif
- ・ wicked\_scr.scr
- ・ movie0045.pif

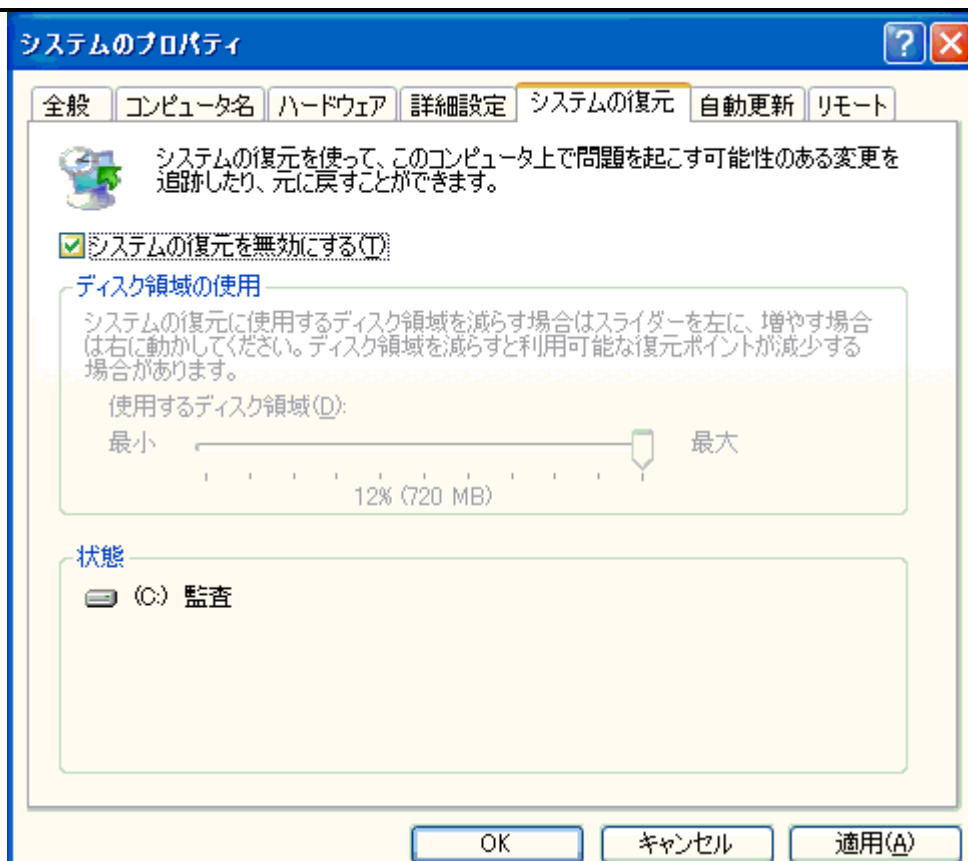
**ワームが実行されると次のような動作を行う。**

1. Windows インストール先フォルダ%Windir% (標準ではC:\WindowsまたはC:\WINNT) に自分自身である winpr32.exe をコピーする。
2. Windows インストール先フォルダに%Windir%\winstt32.dat. を作成する。
3. Windows の起動時に必ずワームが実行されるようにするために、レジストリを操作する。
  - ・ 対象レジストリキー  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run  
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run
  - ・ 追加する値  
"TrayX"="Windows フォルダ%\winpr32.exe /sinc"
4. 次の拡張子を持つファイルからメールアドレスを収集し、発見したメールアドレスに対し独自のSMTPエンジンを使用し自分自身を送付する。
  - ・ .dbx
  - ・ .eml
  - ・ .hlp
  - ・ .htm
  - ・ .html
  - ・ .mht
  - ・ .web
  - ・ .txt

送信されるメールの差出人については、感染したコンピュータから収集されたメールアドレスからランダムに選択されるため、実際には感染していないコンピュータから感染メールが送信されたように詐称される。

5. 書込み権限のある共有ネットワークに、自分自身をコピーしようとする。ワームは、標準の Windows API を利用して、この動作を試みる。しかし、コード内のバグにより、共有ネットワークへのコピーは、実際には行われない。
6. 感染したコンピュータに任意のファイルをダウンロードさせ実行する機能がある。感染したコンピュータは、ワームの作者からシステム情報を盗まれたり、スパムリレーサーバなどの目的で使用されることがある。
- また、ワームのセルフ・アップデート機能として利用されることがある。ワームは、正しい条件の下において、ワーム作者のコントロールするマスタサーバのリストの 1 つと接触しようとする。ファイルを取得するための URL を探し、取得した URL から、悪意あるファイルをダウンロードし実行する。
- ダウンロードを試みる条件は以下の通りである。
- ・ UTC 時間で、金曜日あるいは日曜日
  - ・ UTC 時間で、上記曜日の 19:00-22:00 の間
- また、マスタサーバに関する IP アドレスが含まれるリストは以下の通りである。
- ・ 12.232.104.221
  - ・ 12.158.102.205
  - ・ 24.33.66.38
  - ・ 24.197.143.132
  - ・ 24.206.75.137
  - ・ 24.202.91.43
  - ・ 24.210.182.156
  - ・ 61.38.187.59
  - ・ 63.250.82.87
  - ・ 65.92.80.218
  - ・ 65.92.186.145
  - ・ 65.95.193.138
  - ・ 65.93.81.59
  - ・ 65.177.240.194
  - ・ 66.131.207.81
  - ・ 67.9.241.67
  - ・ 67.73.21.6
  - ・ 68.38.159.161
  - ・ 68.50.208.96
  - ・ 218.147.164.29
7. ポート 123/udp(NTP ポート)にアクセス可能な幾つかのサーバのうちの 1 つに接続し、NTP プロトコルを利用して UTC 時間を得る。
8. マスタサーバの 8998/udp ポートに probe(調査依頼)を送信することで、ダウンロードの開始を試みる。要求を受けたマスタサーバは、ワームが悪意のあるファイルをダウンロードできる URL を返す。
9. 次のポートを開く。これらのポート上で、あらゆる UDP ダイアグラムを待機し、入ってきたダイアグラムは分析され、特有のシグネチャを伴ったダイアグラムを受取り次第ワームのマスタサーバリストが更新される。
- ・ 995/udp
  - ・ 996/udp
  - ・ 997/udp

	<ul style="list-style-type: none"> <li>・ 998/udp</li> <li>・ 999/udp</li> </ul>
<p><b>感染・発症防止方法</b></p>	<ol style="list-style-type: none"> <li>1. 「ウイルスの動作概要」記述した内容のメールが届いた場合には、安易にメールを開封しない。</li> <li>2. 特に次のファイルが添付されているメールには注意する。 your_document.pif、document_all.pif、thank_you.pif、your_details.pif、details.pif、document_9446.pif、application.pif、wicked_scr.scr、movie0045.pif</li> <li>3. 予期せぬメールが届いた場合には、添付ファイルを絶対に開かない。</li> <li>4. ネットワーク管理者は、次のことを実行する。             <ul style="list-style-type: none"> <li>・ ポート 99x/udp 上でインバウンドのトラフィックをブロックする。</li> <li>・ ポート 8998/udp 上でアウトバウンドのトラフィックをブロックする。</li> <li>・ 感染したコンピュータからの要求である可能性があるため、NTP リクエスト(ポート 123/udp)を監視する(このようなチェックは、1時間に1回の頻度で行う)。</li> </ul> </li> </ol>
<p><b>ウイルスの駆除方法</b></p>	<p><b>手動による修復を行う場合、コンピュータに関する高度な知識が必要とされ、間違えるとコンピュータが正常に起動しなくなる場合がある。</b></p> <ol style="list-style-type: none"> <li>1. 被害拡大防止のため、接続されているネットワークから切り離す。</li> <li>2. システムの復元オプションを無効にする。  <b>Windows Me システムの復元機能を無効にする手順</b> <ol style="list-style-type: none"> <li>1. 実行中のプログラムを全て停止させる。</li> <li>2. デスクトップ上の[マイコンピュータ]アイコンを右クリックし、[プロパティ]を選択する。</li> <li>3. [パフォーマンス]タブを選択し、[ファイルシステム]ボタンをクリックする。</li> <li>4. [トラブルシューティング]タブを選択し、[システムを復元しない]にチェックを入れる。</li> <li>5. [OK]ボタンをクリックする。</li> <li>6. [閉じる]ボタンをクリックし、コンピュータを再起動する。 再起動時に _RESTORE フォルダ内のバックアップファイルが削除される。</li> </ol> <b>Windows XP システムの復元機能を無効にする手順</b> <ol style="list-style-type: none"> <li>1. [スタート] ボタンをクリックする。</li> <li>2. 表示されたメニューの中から [マイ コンピュータ] を右クリックし、[プロパティ] を選択する。</li> </ol>  <ol style="list-style-type: none"> <li>3. [システムの復元] タブをクリックする。</li> <li>4. [システムの復元を無効にする]、または [すべてのドライブでシステムの復元を無効にする] にチェックを入れる。</li> </ol> </li> </ol>



5. [適用] ボタンをクリックして設定を保存する。
6. [OK] ボタンをクリックしてウィンドウを閉じる。

詳細については、Windows のマニュアル等を参照のこと。

3. セーフモードで再起動する / 動作中のプロセスを終了させる  
セーフモードの詳細については、W32.HLLW.Fizzer@mm を参照のこと

#### Windows 95/98/Me

コンピュータをセーフモードで再起動する。Windows NT 以外のすべての Windows 32-ビット OS はセーフモードで起動することができる。

#### Windows NT/2000/XP

ワームのプロセスを停止するには

1. Ctrl+Alt+Delete キーを同時に押す。
2. [タスクマネージャ]をクリックする。
3. [プロセス]タブをクリックする。
4. リスト最上部のイメージ名をダブルクリックしてプロセスをアルファベット順に並べ替える。
5. リストをスクロールして、Winpr32.exe を探す。
6. 該当するファイルを発見したら、それをクリックして[プロセスの終了]をクリックする。
7. タスクマネージャを閉じる。

4. 感染ファイルを削除する。

Windows エクスプローラを開き、次のファイルを探して削除する。

- ・ winpr32.exe

5. レジストリから値を削除する。

1. [スタート]ボタンを押し、[ファイル名を指定して実行]をクリックする。( [ファイル名を指定し

	<p>て実行]ダイアログボックスが表示される。)</p> <ol style="list-style-type: none"><li>2. regedit と入力する。 [OK]をクリックする。(レジストリ エディタが開く。)</li><li>3. 次のレジストリキーを選択する。 HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run</li><li>4. 画面右側で、次の値を削除する。 "TrayX"="%Windir%¥winppr32.exe /sinc"</li><li>5. 次のレジストリキーを選択する。 HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Run</li><li>6. 画面右側で、次の値を削除する。 "TrayX"="%Windir%¥winppr32.exe /sinc"</li><li>7. レジストリエディタを終了する。</li></ol> <p><b>無償修復ツールがワクチンベンダーから配布されているので、使用上の注意をよく読み自己責任において使用すること。</b></p>
<b>その他</b>	なし