

## ウイルス解析報告書

ウイルス名	W32/CIH.1106 (W95/CIH.1106)
プログラム名及び容量 (添付ファイル名)	1106バイト (ファイル名不定・被感染ファイルはサイズが変化しない)
種別	32ビットWindows(PE)ファイル感染型ウイルス
プログラム言語	アセンブラ
発症環境	Windows95/98/ME (WindowsNT/2000/XPでは感染も発病もしない)
発見日時	2002年11月28日
発見場所(発信地)	不詳
危険性	ハードディスク内容の喪失、BIOSROM内容の消去によるPCの破壊
発症条件	毎月2日
ウイルスの活動、影響	<p>このウイルスは、Windows95/98/ME環境で動作し、Windows NT/2000/XPでは感染も発病もしない。</p> <p>ウイルスはメモリーに常駐し、他のプログラムが実行されるたびにそのファイルに感染するウイルスである。実際にはプログラム実行だけではなく、ファイルを開く時に感染するので、ファイル検索などでも感染する。感染は宿主ファイルの空白部分に埋め込まれる形で行われるため、被感染ファイルのファイルサイズは1バイトも増加しないという、きわめて特殊な方法がとられている。</p> <p>このウイルスは毎月2日に発病し、ハードディスクをフォーマットする(完全復旧は困難)。また一部機種種のフラッシュROM BIOS内容を破壊し、起動できないようにする。BIOSが破壊された場合、メーカーなどの修理が必要である。</p> <p>Win Zipの自己展開ファイルには感染しない。</p>
被害の規模	被害報告はない(2002年12月6日現在)
亜種、変種の有無	このウイルスはW32/CIH.10xxの亜種である。その内容の違いは発病日の違いだけであり、プログラムサイズの違いはアSEMBル時のオプションが、速度に対して最適化するためである。つまり、プログラム随所にアライメント調整のためのNOPコードが埋め込まれたために100バイトほど長くなっているのである。
ウイルス動作概要	<p>&lt;感染プログラムからシステムへの感染&gt;</p> <p>感染したプログラムが起動するとウイルスはIDTのアドレスを取得し、INT 03hのジャンプ先アドレスをウイルスプログラム内部のアドレスに書き換える。その後INT 03hを行い、ウイルスプログラムの特権レベルで実行させる。</p> <p>デバックレジスタdr1の内容が0または-1の場合、ウイルスプログラムが常駐していないと判断し、システムメモリを確保してウイルスプログラムをこのメモリに転送し、ファイルシステムをフックする。dr0には直前のファイルシステムのフックアドレスが格納される。</p> <p>宿主のプログラムの実行開始アドレスにジャンプして感染処理を終了する。</p> <p>&lt;感染システムから実行プログラムへの感染&gt;</p> <p>メモリに常駐したウイルスはファイルシステムをフックしており、IFSFN.OPEN(ファイルを開く/プログラムの実行を含む)が行われた時にioreq構造体のパス名を元にして実行ファイルに感染する。</p> <p>まず、拡張子がEXEであるか判別し、EXEの時にはそのファイルが存在するかを確認する。ファイルの属性を保存してファイルを読み書き可能で開き、PEヘッタのシグネチャとその1バイト前が0であることを確認する(PEの1バイト前が非0ならば既感染なので処理を中断する)。</p> <p>さらにEXEファイルの隙間のバイト数を計算し、十分な大きさがある場合、隙間にウイルスプログラムを書き込む。この時、隙間が分断されている場合には、ウイルスプログラムを分割して書き込む。WinZipの自己展開ファイルかどうかを判別してWinZipの自己展開ファイルに感染しない。</p> <p>またPEヘッタのシグネチャの1バイト前に55hを書き込み、PEヘッタのセクションテーブルの内容を書き換えて分割されたウイルスプログラムを結合できるようにする。PEヘッタのエントリーポイントもウイルスプログラムの先頭アドレスに書き換える。</p>

	<p>最後にファイルの属性とファイルのタイムスタンプを感染前の状態に戻す。</p> <p>I/Oポートから日付を読み出し、日にちが2日のときには発病する。 発病はBIOSの破壊から行われ、書き換え可能なBIOSを上書きする。 BIOSの種類によってはこの発病ルーチンは正しく動作せず、BIOSは破壊されない。</p> <p>その後、1台目のハードディスクのはじめのデータから順に上書きする。 ハードディスクが複数ある場合には、 1台目のハードディスクはじめのデータ 2台目のハードディスクはじめのデータ ⋮ n台目のハードディスクはじめのデータ 1台目のハードディスク次のデータ 2台目のハードディスク次のデータ ⋮ という順番で行われ全てのハードディスクが直ちに破壊される。 そのため全てのハードディスクの先頭部分(FATなどの重要なデータがある部分)が すばやく破壊される。</p>
感染・発症防止方法	<p>OSやアプリケーションは出所の確かなCDからインストールを行う。 オンラインでソフトウェアを入手する場合は公式サイトから一次配布のものをダウンロードして利用する。 感染が疑われるパソコンでは、システム時計が2日にならぬよう、前もって進めるか遅らせる。(暫定的な方法であるが)</p>
ウイルスの駆除方法	<p>&lt; 確認 &gt; 被感染ファイルと思われるファイルをフロッピーディスクなどに書き出し、感染のおそれのないオリジナルファイルとファイル比較、またはサムチェック比較を行う。これを複数のファイルに対して行い、同じバージョンの同じファイルであるにもかかわらず、比較結果が異なる場合は感染のおそれがある。</p> <p>&lt; 駆除 &gt; データファイルのみをCD-RやMOなどにバックアップしたうえで、オリジナルのCDからOSとアプリケーションを再インストールして復旧する。 決して感染パソコンの実行ファイルを再利用してはならない。</p>
その他	<p>報告書作成 : 2002年12月9日現在</p>

W32/CIH.1106 システム感染フローチャート



