USB メモリーなどから感染するウィルスの駆除方法

【概要】

USB メモリーや外付け HDD に感染し、それらを取り付けた PC に感染するウィルスは、ウィルス・チェッカーで引っかかるウィルス・ファイルを自動生成する元のウィルスを駆除（削除）しなければ完治しません。これら元ウィルスは、チェッカーやワクチンにより発見，削除できない場合もあります。

この種のウィルスはネットゲームのパスワードを盗む程度のものらしいのですが､放置すると CPU のパワーを消費し、PC の動作を遅くすることがあります。また、HDD をダブルクリックして内容を閲覧しようとすると「プログラムを選択して開く」が立ち上がり、ディレクトリを見ることができないなどの不具合が起こることもあります。

この種のウィルスは感染力が非常に強力で、一度治しても感染した HDD のウィンドウを開くことで再度感染します。

この文章情報は、この種のウィルスの削除方法を解説しています。

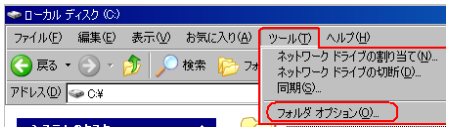
【関連ワード】

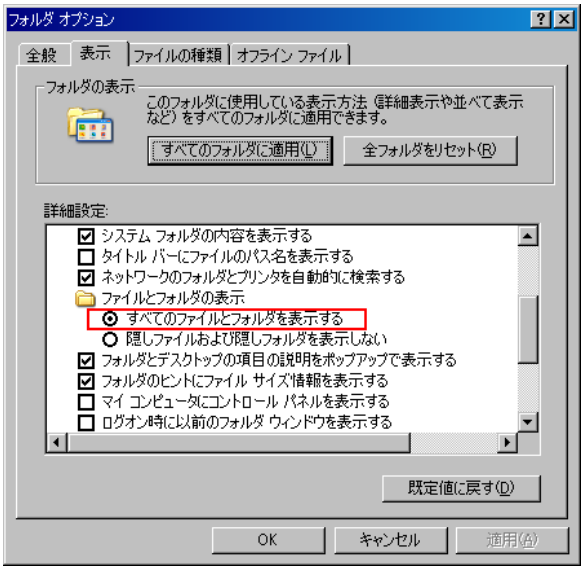
mmvo.exe, ierdfgh.exe, revo.exe, sfwypsy.exe, ksahqgbi.exe, r0so.exe, afmain0.dll, pytdfse0.dll, ssdfgh.exe, xvassdf.exe, 9swdbe.exe, autorun.inf,

【ウィルスの有無の判定方法　－(1) ファイルの確認】

これらのウィルスが感染すると、接続されているドライブのルート（最も上のディレクトリ）に「autorun.inf」という名前の隠しファイルができます。ドライブのルートを確認してください。

また、ドライブのルートに何も隠しファイルが存在しない場合、〔フォルダオプション〕（ツール→フォルダオプション）で〔すべてのファイルとフォルダを表示する〕にチェックが入っていることを確認してください。





もしこの設定がされていなければ、チェックを入れ「OK」してください。

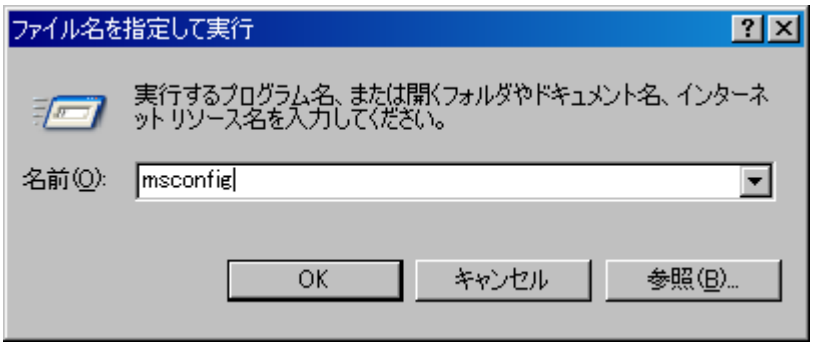
それでもルートに隠しファイルが表示されない場合、もう一度同じ箇所の設定を確認してください。

〔すべてのファイルとフォルダを表示する〕にチェックを入れたにもかかわらず、〔隠しファイルおよび隠しフォルダを表示しない〕にチェックが自動的に設定される場合、ウィルスに感染していると思われます。

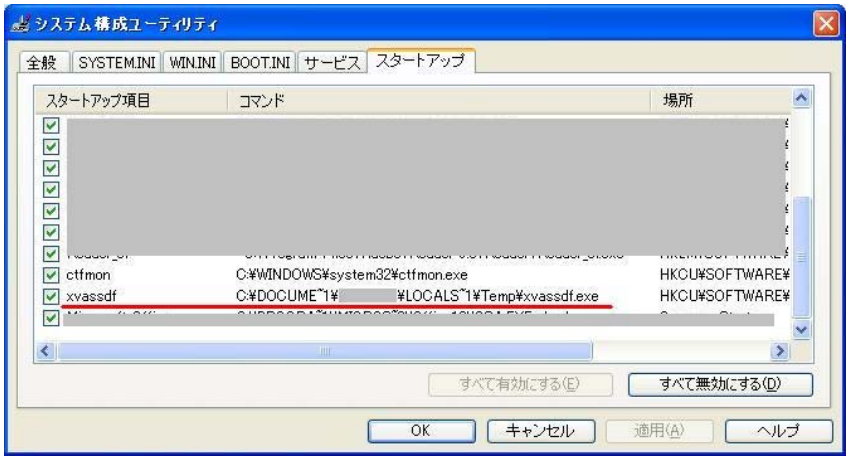
以下の方法でさらに確認してください。

【ウィルスの有無の判定方法　－(2) 実行ファイルの確認】

1. 〔スタート〕メニュー→〔ファイル名を指定して実行(R)〕を選択します。
2. 〔名前(O)〕に「msconfig」と入力し、〔OK〕をクリックします。



3. 〔スタートアップ〕のタブを表示させ、下図のように「xvassdf」や「mmvo.exe」、「revo.exe」があればウィルスに感染しています。これらのファイルを見つけたら、〔スタートアップ項目〕のチェックを外してください。



〔コマンド〕の部分には、起動時に実行されるウィルスの場所も表示されています。後ほど削除しなければならないファイルですので、ディレクトリをしっかりと記録してください。

4. 「OK」をクリックし、ウィンドウを閉じると再起動を求められます。他の HDD のルートを見る前に、すぐに再起動してください。次回の起動ではウィルスは起動しなくなります。念のためもう一度同様の方法（「msconfig」→「スタートアップ」タブ）で確認し、これらのファイルが起動していないことを確認してください。

【ウィルスファイルの削除】

順序として、

A.　システムの復元を無効にする。

B.　隠しファイルを見えるようにする。

C.　ウィルスファイル及び関連ファイル特定する。

D.　各 HDD のウィルスファイル及び関連ファイルを削除する。

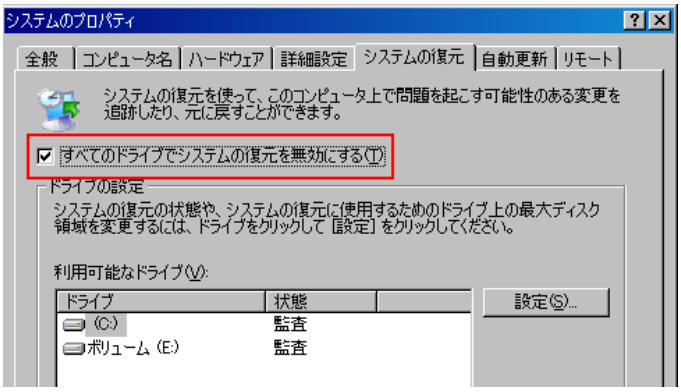
E.　システムの復元を有効にする。

という手順を踏みます。

注意：PC のレジストリを変更する作業が含まれます。操作に自信の無い方は作業を行わないで下さい。

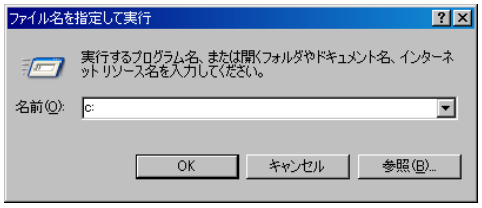
A.　システムの復元を無効にする

〔スタート〕→〔マイコンピュータ〕右クリック→〔プロパティ〕→〔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、〔OK〕します。



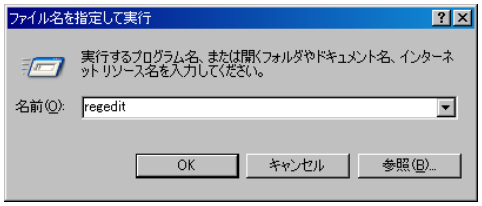
B.　隠しファイルを見えるようにする

1. 〔スタート〕→〔ファイル名を指定して実行〕を開き、「c:」と入力して〔OK〕をクリックします。



注意：これで C ドライブが開きます。アイコンをクリックするとウィルスが起動しますので、必ずこの方法を使ってドライブのルートディレクトリを表示させてください。

2. 〔スタート〕→〔ファイル名を指定して実行〕を開き、「regedit」と入力して〔OK〕をクリックします。



これでレジストリエディタが起動します。

注意：以下の操作に自信の無い方は、操作を行わないで下さい。

3. レジストリを変更する

以下のレジストリを変更します。変更箇所は 3 箇所あります。変更後、隠しファイルが見えるようになります。

3-1 CheckedValue

HKEY_LOCAL_MACHINE
SOFTWARE
Microsoft
Windows
CurrentVersion
Explorer
Advanced
Folder
Hidden
SHOWALL
"CheckedValue"を 1 に変更します。

3-2 Hidden

HKEY_CURRENT_USER
SOFTWARE
Microsoft
Windows
CurrentVersion
Explorer

Advanced

"Hidden"を１に変更します。

3-3　ShowSuperHidden

HKEY_CURRENT_USER

SOFTWARE

Microsoft

Windows

CurrentVersion

Explorer

Advanced

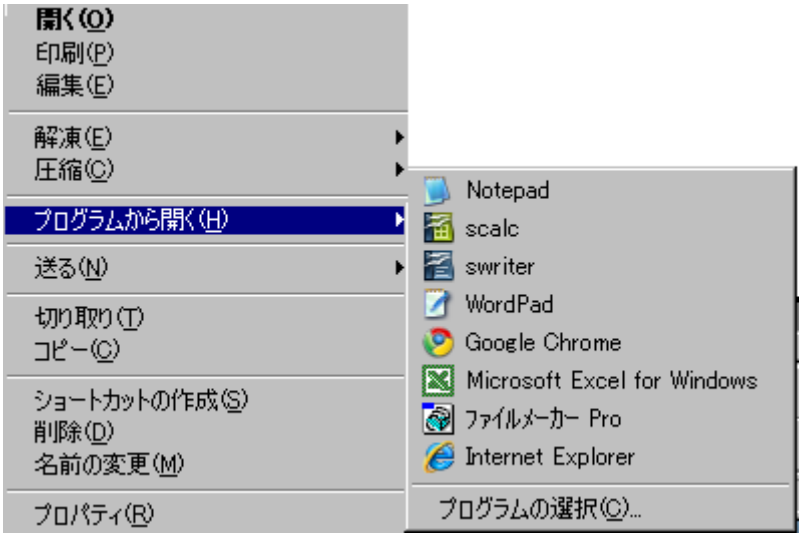
"ShowSuperHidden"を１に変更します。

以上の変更により隠しファイルが強制的に見えるようになります。

4.　レジストリエディタを閉じる

C.　ウィルスファイル及び関連ファイル特定する

前の作業により「autorun.inf」という隠しファイルが見えるようになったはずです。このファイルを右クリックし〔プログラムから開く〕→〔Notepad〕を選択します。



Notepad で開くと、

open=△△△△.exe

shell¥open¥Command=△△△△.exe

などのように実行ファイルが指定されています。

exe ではなく、com や bat の場合もあります。これらのファイルがウィルス本体です。これらは同じルートディレクトリにある場合があります。

例：mmvo.exe, ierdfgh.exe, revo.exe, sfwypsy.exe, ksahqgbi.exe, r0so.exe, ssdfgh.exe, xvassdf.exe, 9swdbe.exe, ksahqgbi.exe, s1.com f1.exe など。

D. 各 HDD のウィルスファイル及び関連ファイルを削除する

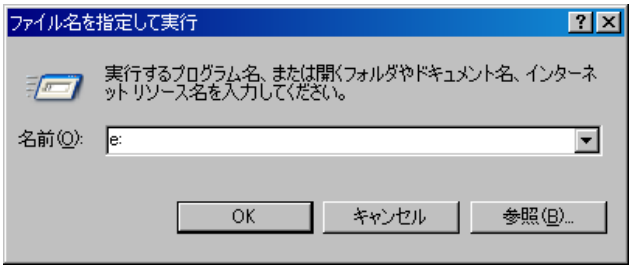
注意： 削除は単純に Delete キーではなく、「〔Shift〕キー＋〔Delete〕キー」を使用し、ゴミ箱に入れないで削除してください。

1. 前項で見つけた以下のファイルを削除します。
   - autorun.inf
   - 実行ファイル

さらに、接続されている各 HDD のルートディレクトリにも同様のファイルがあるはずなので、見つけて削除します。

注意：HDD のアイコンをダブルクリックしてはいけません！必ず〔スタート〕→〔ファイル名を指定して実行〕を開き、ディスクレターと「:」を入力し、〔OK〕で開いてください。

例：



2. 【ウィルスの有無の判定方法 －(2) 実行ファイルの確認】の〔3〕で調べた、起動時に実行されるウィルスを削除する。

例：

C:¥WINDOWS¥system32 の中に mmvo.exe, revo.exe, ierdfgh.exe, xvassdf.exe

や

C:¥Documents and Settings¥〔ユーザー名〕¥Local Settings¥Temp の中に xvassdf.exe

があれば、削除してください。

E.　システムの復元を有効にする

以下の通り、前述 A 項と逆の作業を行いシステムの復元を有効にします。

〔スタート〕→〔マイコンピュータ〕右クリック→〔プロパティ〕→〔すべてのドライブでシステムの復元を無効にする〕のチェックを外し、〔OK〕します。

以上でウィルスの駆除は完了です。

【予備知識】

〔Autorun.inf〕について

〔Autorun.inf〕は本来、CD などを入れたときに自動的に指定したプログラムをスタートさせるためのプログラムです。このファイル自体が常にウィルスに関係する悪いファイルではありません。