

とりあえず感染してるか確認する手順 (Vistaユーザー)

【2009/5/17 10:00時点の情報です】

1. ウィンドウズキー (Windowsのマークのあるキー) を押し、でてきたメニューの「検索の開始」に「ファイル名を指定して実行」と入力、でてきたプログラムをクリック

2. 「ファイル名を指定して実行」という画面が出てくるので、入力欄に「cmd.exe」(全部半角で)と入力して「OK」ボタンを押す
背景が黒いウィンドウが開いた場合、そのまま閉じて3へ
起動しない場合：**感染疑い濃厚** [感染してしまった時の対処方法へ](#)

3. もう一度1. を実行

4. 「ファイル名を指定して実行」という画面が出てくるので、入力欄に「regedit.exe」(全部半角で)と入力して「OK」ボタンを押す
(「続行するにはあなたの許可が必要です」というダイアログが出た場合は、「続行(C)」ボタンを押す)

「レジストリエディタ」というウィンドウが開いた場合すぐに閉じて5へ
起動しない場合：**感染疑い濃厚** [感染してしまった時の対処方法へ](#)

5. C:\Windows\Help\mui」以下のディレクトリにsqlsodbc.chmがあります
わからなければ「エクスプローラ」でCドライブから
Windows Help muiフォルダの中を探してください
muiディレクトリ内に「0411」「0409」などのディレクトリが存在する
場合がある(このディレクトリ自体は無害なので気にしなくて良い)ので、
その場合は「0411」「0409」内から「sqlsodbc.chm」ファイルを探すこと

見つからない場合、コントロールパネルのフォルダオプションの
「表示の登録されている拡張子は表示しない」のチェックが外れているか
確認してください

外していないと「sqlsodbc」ってファイルしか見つからず
「sqlsodbc.chm」で検索しても見つかりません

sqlsodbc.chm を右クリック プロパティでボリュームを確認

1個のファイル 50,727バイト と表示されればOK

49.5kbyteと表示された場合、右クリック、プロパティで50,727byteかどうか見る
それ以外の数値の場合は **感染の疑い濃厚**

念のためMD5値の確認も推奨

・ HashTab Shell Extension

<http://www.forest.impress.co.jp/lib/sys/file/fileuty/hashtabshlex.html>

を使い、CRC32,MD5,SHA1の情報を取得する。

正常なsqlsodbc.chmは

ファイルサイズ： 50,727バイト

CRC32： B61C7A80

MD5： F639AFDE02547603A3D3930EE4BF8C12

SHA-1： FBDD32ED13D27E4102621E1067FDF3634F33B2C3

6. 以下のウイルス対策ソフトを導入するか、オンラインスキャンする

・ Kaspersky

・ avast!

・ ウイルスバスタ2009

・ニフティオンラインスキャン

<http://www.nifty.com/security/vcheck/?mid=601287&lid=20>

使用したアンチウイルスソフトによって、検出された場合のウィルス名称に差異があります。

例：avast! での検出名 JS:Redirector-H* (*は数字)
など

現在上記検索にもひっかからない亜種が出てきているため、絶対とは限りません
また、SymantecでもKasperskyでも、オンラインスキャンでは感染していることが
わからないようだ、という報告も出ています。【2009/5/17 23:29】