
このページはあくまで2009年5月の内容です。

2010年1月現在話題となっている亜種には対応していません。

ご注意ください。

対策

- [Adobe Readerを最新にする](#)
- [Adobe Flash Playerを最新にする](#)
- [該当IPアドレスへの接続を遮断](#)
- [Adobe ReaderのJavascriptを切る](#)
- 掲示板などに貼られている怪しいリンクをむやみに開かない
- ウイルス定義ファイルを更新する
- [WindowsUpdate](#)

感染しているか確認

どうやら感染するとC:\WINDOWS\system32\sqliodbc.chmが上書きされる様子
これのハッシュ値を確認してみるといいかも
ファイルサイズが大きく違うのでよくわかんなかったらそっちでどうぞ
作成日時や更新日時は環境によってバラバラなのでとりあえず無視してもOK

正常なsqliodbc.chm

ファイルサイズ：50,727バイト

CRC32：B61C7A80

MD5：F639AFDE02547603A3D3930EE4BF8C12

SHA-1：FBDD32ED13D27E4102621E1067FDF3634F33B2C3

上書きされたsqliodbc.chmの例（あくまで例でありこの限りではない）

ファイルサイズ：1,323 バイト

CRC32：7585CBB6

MD5：BF7209B9589AD09A25740F6D47D0ADEA

SHA-1：D695F957AA9DEB0E4D92F4546DB3A883B1909008

他にもこんな症状が出る

- コマンドプロンプトを実行中ではないのにcmd.exeが起動している
- cmdやregeditが起動しない（Explorerが落ちる）
- 特定のサイトに接続できなくなる
- ブラウジングがまともにできない
- Adobeが5分に1回のペースで更新を要求してくる
- CPUの稼働率が何も作業していないのに50%近くに上がる(CPUのコア数によって違う)

とにかく怪しいと思ったら確認してみよう

<関連>[Windows XPで感染を確認する方法](#)

[Windows 2000で感染を確認する方法](#)

[Windows vistaで感染を確認する方法](#)

駆除方法

一部のウイルス対策ソフトで検出できるようだが基本的にリカバリ（OSのクリーンインストール）
いろいろファイルが改ざんされているという話なのでやはり現状ではリカバリ推奨
個人情報が出たりウイルス拡散する可能性もあるから気づいたらできるだけ早く行うこと

GENOに書いてあるキャッシュ削除では何の対処にもなっていないので注意