

---

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。

## GENOウイルスとは

最初に感染が確認されたのが通販サイトのGENOだったためそう呼ばれる。  
Adobe ReaderやAdobe Flash Playerの脆弱性を突いた新種のウイルスである。

- (1)感染したWebページをひらく
- (2)感染したjsが、94.247.2.195の改変jquery.jsを実行
- (3)IP/UAで振り分け処理(Vistaは大丈夫そう?)
- (4)PDF/Flash起動。各種ウイルス本体をInternetTempに展開
- (5)bufferOverrunでウイルス本体の起動を試行

感染した場合

パスワードなどの個人情報が抜かれている可能性あり

いつものバックドア系ウイルスなんだけど、今回なんか変だな

- ・ PDFファイルとかシステムファイルがなぜか増殖する
- ・ メモリを馬鹿食いする
- ・ 再起動時にブルースクリーン

とりあえず、駆除せずに再起動したら帰ってこれないかもしれないな

## GENO感染時の症状

- ・ sqlsodbc.chmを改変
- ・ cmd.exe、regedit.exeが起動不能
- ・ 一部のアンチウイルスソフトが更新不能
- ・ 特定サイトにアクセス不能(Windows Update、アンチウイルスソフト関連サイト)
- ・ ネットワークのトラフィックを監視、ユーザー名やパスワード等の情報を収集
- ・ Googleの検索結果を改竄(リンクを弄る)
- ・ explorer.exeや一部のブラウザが異常終了
- ・ Acrobatが勝手に起動
- ・ PDFファイルやシステムファイルが増殖
- ・ CPU、メモリ使用率がUP
- ・ 再起動時にBSOD