

情報セキュリティ読本に記載のウイルスの特徴一覧表

ウイルス名	IPAへの 初届出年月	感染経路別分類				ウイルス感染につながる操作					ウイルスの特徴					
		メール 機能悪 用型	セキュ リティホ ール悪 用型	ネット ワーク 感染型	その他感染経路・感染場所	ファイル の実行	メールの 開封や プレ ビュー	ネット ワーク 接続	Web ページ の閲覧	その他	ファイル やHDD の破壊 や削除	ウイルス 付き メール の送信	送信者 詐称	DoS 攻撃	情報漏 えい	その他の特徴
W32/Sasser	2004年5月															再起動を繰り返す。
W32/Netsky	2004年2月				P2Pファイル交換ソフト経由											多くの亜種が出現。2004年前半で他のウイルスに比べ圧倒的に蔓延。
W32/Mydoom	2004年1月				P2Pファイル交換ソフト経由											多くの亜種が出現。亜種の中には、WordやExcelなどのファイルを削除するものがある。
W32/Bagle	2004年1月				P2Pファイル交換ソフト経由											アイコンの偽装。バックドアのインストール。ワクチンソフトの機能停止。
W32/Mimail	2003年8月															フィッシング詐欺による個人情報漏えい(亜種)
W32/Antinny	2003年8月				P2Pファイル交換ソフト (Winny) 経由											P2Pファイル交換ソフト経由の情報漏洩。 Winnyのキャッシュフォルダのファイルを削除。
W32/MSBlaster	2003年8月															再起動の繰り返し、DoS攻撃
W32/Welchia	2003年8月															MSBlasterに感染していたパソコンをみつけると、MSBlasterをそのパソコンから削除する。バックドアのインストール。
W32/Fizzer	2003年5月				共有フォルダ経由 IRC経由											バックドアのインストール。セキュリティ製品の機能停止。
Wscript/Fortnight	2003年4月															添付ファイルはない。Outlook Expressでプレビューした時にウイルスが掲載されたWebページが自動的に参照され、ウイルスが実行される。
W32/Deloder	2003年3月				共有フォルダ経由 IRC経由											パスワードクラックによるパソコンへの侵入。 バックドアをインストールし、遠隔操作を可能にする。
W32/SQLSlammer	2003年1月															大量の攻撃パケットを送信。韓国ではこのウイルスのためにインターネットが一時停止した。
W32/Bugbear	2002年10月															バックドアが仕掛けられ、キー入力情報が第三者に取得される可能性がある。セキュリティ製品の機能停止。
VBS/Redlof	2002年8月															添付ファイルはない。セキュリティホールを利用しウイルスを自動実行させる。
W32/Klez	2001年11月				共有フォルダ経由											添付ファイルによる情報漏洩、ファイル・フォルダの削除、セキュリティ製品の機能停止、毎月6日に発病し、Cドライブのファイルを削除する亜種もある。
W32/Nimda	2001年9月															公開Webサーバーが感染すると、ブラウザによっては自動的にウイルスファイルをダウンロード・実行してしまう。
W32/CodeRed	2001年7月															Webページの改竄、バックドアのインストール
W32/Sircam	2001年7月															添付ファイルによる情報漏洩、10月16日にCドライブの全てのファイルを消去。
W32/Badtrans	2001年5月															キーロガーをインストール。パスワード等を特定のメールアドレスに送信する。
W32/Hybris	2000年12月															画面上に、渦巻きを表示する亜種もある。
W32/Navidad	2000年11月															アプリケーションソフトの使用不能
W32/QAZ	2000年9月				ファイルのやり取りやダウンロード											バックドアをインストールし、遠隔操作を可能にする。
VBS/LOVELETTER	2000年5月				IRC経由											二重拡張子。拡張子が、vbs、jpg、mp3等のファイルを破壊する。ユーザのID及びパスワードの窃盗。不正プログラムの自動ダウンロード。
W32/LoveSong	2000年1月				ファイル感染型											音楽の演奏
W32/CIH	1998年8月				ファイル感染型											特定の機種種のBIOSを破壊するため、コンピュータが起動不能となる。Webサイトからダウンロードしたファイルからの感染が多い。
XM/Laroux	1997年2月				マクロ感染型											感染したExcelファイルを開くとそのExcelに感染する。以降感染したExcelで作成、編集したファイルに感染する。
Stamford	1994年2月				ブートセクタ感染型						FDからPCを起動					感染したフロッピーディスクでパソコンを起動すると、特定の条件下で画面に炎の絵を表示、HDDのブートセクターを破壊。コンピュータの起動不能。
PeterII	1993年10月				ブートセクタ感染型						FDからPCを起動					感染したディスクでマシンを起動すると、HDDを暗号化し、問題を3つ出す。全問正解するとHDDを元に戻すが、1問でも間違えるとHDDが暗号化されたままデータの復旧不能に。
Cascade	1990年12月				ファイル感染型											画面に表示されている文字を下方に落下させ、表示内容を破壊。

注1: 出現時のウイルスと亜種ではウイルスの感染経路や特徴に違いのあるものがある。この表では、亜種も含みそのウイルスに特徴的なものを記載している。

例えば、W32/Mimailは、出現当時はフィッシング詐欺を働くウイルスではなかったが、2003年11月に出現した亜種はフィッシング詐欺を働いた。

また、出現当時はメール機能を悪用のみだが、亜種ではセキュリティホールもあわせて悪用するようになったウイルスもある。(例: W32/Badtrans、W32/Bagle など)

注2: ネットワーク接続 というのは、ユーザが特別の操作を行わなくても、ネットワークに接続しているだけで感染することがあるという意味である。

注3: ウイルス付きメールの送信で の記載があるものは必ずしも大量メール一斉送信ではない。中には、数通のメールを送信するだけのものもある。

注4: バックドアをインストールするウイルスの場合、IDやパスワードの窃盗、ファイルの削除、情報漏えい等の不正アクセス行為を働かれる可能性がある。