


学内において「DISK KNIGHT」が検出されました。


ウィルスのようにUSBメモリ、パソコンに感染し、コピーされます。

## USBメモリへの感染の有無の調査方法

USBメモリを SHIFTキーを押しながらパソコンに接続します。

(Shiftキーを押しながらUSBメモリを挿すとパソコンに感染しません)

本来なら  リムーバブル ディスク (G) と表示されるものが、

 リムーバブル ディスク (G) と表示されたら、

**「DISK KNIGHT」に感染している可能性があります。**



# 「DISK KNIGHT」の挙動

## 感染・挙動:

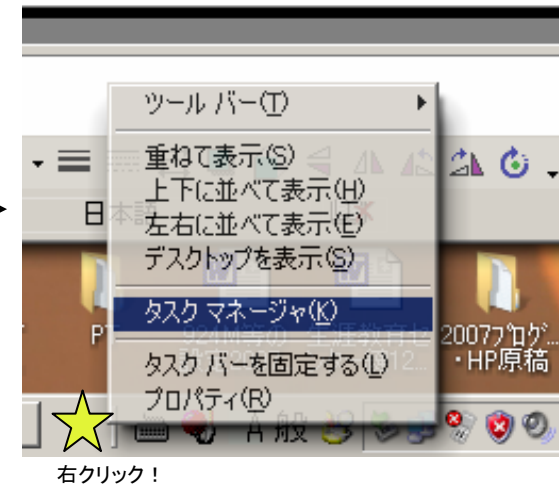
- USBメモリなどの外部メディアに感染し、パソコンに接続するとパソコンに感染します。
- 感染したパソコンに 未感染のUSBメモリを挿すとUSBメモリ内に、Knight.exe,Autorun.infを作成し感染を拡げます。
- 感染したパソコンでは「DISK KNIGHT」が、「パソコン内で動いているプログラム」を監視し、異常を検知すると確認メッセージが表示されます(かなり頻繁にメッセージが出るため、通常作業が阻害されます。)
- 感染したドライブは、Windowsセキュリティセンターと同じ形のアイコンとして表示される。
- 感染したパソコンには、C:¥windows¥knight.exe が作成され、次回のパソコン起動時に自動実行される。
- パソコン内、USBメモリ内に作成される「DISK KNIGHT」関連ファイルはシステム属性、隠し属性として作成されるため、Windowsシステムでファイル一覧を見ても現れない。
- ウィルスの様に自動複製を行うが、システムの破壊や、データファイルの改竄、情報漏洩に対する動作はしない(ウィルス対策ソフトでは検出一覧として登録されていないことが多い)。

コンピュータウィルスと同様にコピーを繰り返し、感染を広げるものの破壊活動は行わないようです。感染することでセキュリティを高める作用もあるため、「ウィルス」と認定されておらず、ウィルス対策ソフトでは認識されません。ですが、利用者の意向とは違いコピーを繰り返す動作はウィルスと認識することができます。そのため、感染した場合には削除することをお勧めします。

# DISK KNIGHT削除方法

## パソコン本体内のプログラム停止

1. タスクバーの上で(マウスの)右クリックし、メニューを出す。
2. タスクマネージャーを選択。
3. タスクマネージャーより、プロセスを選択。
4. Knight.exeを選択し
5. 「プロセスの終了」ボタンを押す。
6. プロセス一覧からKnight.exeが無くなった事を確認。



# DISK KNIGHT削除方法

## パソコン本体内のプログラム削除

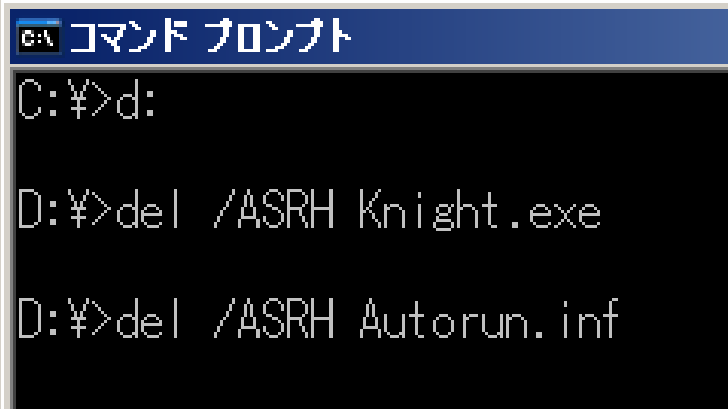
1. コマンドプロンプトを起動する(前項の1と同じ)
2. **del /ASRH c:¥windows¥Knight.exe** を入力する。

## パソコン本体内のプログラム自動起動の停止

1. [スタート]-[ファイル名を指定して実行]-[**msconfig**]  
WindowsVISTAの場合には、  
[Windowsボタン]-[全てのプログラム]-[アクセサリ]-[コマンドプロンプト]  
より msconfig
2. 「スタートアップ」タグを選択
3. Knight の名前がスタートアップ項目にあれば先頭のチェックを外す。
4. 「OK」ボタンを押す

# USBメモリ内の DISK KNIGHT削除方法

1. USBメモリをパソコンに挿す際にShiftキーを押しながら挿す  
(この作業により、感染USBメモリからはパソコン本体に感染しません)
2. マイコンピュータを開き、USBメモリのドライブの番号(EやHなどのアルファベット)を確認する。
3. **コマンドプロンプトを起動する**  
[スタート]—[ファイル名を指定して実行]—[cmd]  
WindowsVISTAの場合には、  
[Windowsボタン]-[全てのプログラム]-[アクセサリ]-[コマンドプロンプト]
4. コマンドプロンプトより以下のように入力する。
5. ドライブの移動(**USBメモリがDドライブ**の場合)  
**d:** (Enter)
6. ウィルスファイルの削除  
**del /ASRH Knight.exe** (Enter)
7. 自動起動ファイルの削除  
**del /ASRH autorun.inf** (Enter)
8. USBメモリを抜く処理を行う。



```
コマンド プロンプト
C:¥>d:
D:¥>del /ASRH Knight.exe
D:¥>del /ASRH Autorun.inf
```