◆InternetSecurity　Knowledge（インターネットセキュリティ　ナレッジ）　TREND MICRO

http://is702.jp/special/331/partner/12_t/

◆TREND MICRO　USBメモリで広まるウイルスへの対策（記事より抜粋）

http://jp.trendmicro.com/jp/threat/solutions/usb/?WT.ac=JPclusty_Threat_USBvirus

現在、USBメモリを介したウイルス（USBワーム）が複数発見され、被害が広まっています。
ウイルスに感染したUSBメモリを使用することで、コンピュータに感染します。
コンピュータの設定や操作によってはウイルスが自動的に起動、USBメモリをコンピュータに挿した瞬間に感染します。

■USBワーム（オートラン）に感染すると？マイコミジャーナル（ハウツー）より引用

http://journal.mycom.co.jp/articles/2009/01/19/Autorun/001.html

・レジストリ情報等、Windowsのシステム改変を行う。

・オンラインゲームのIDやパスワードが盗み出される別のウイルスをダウンロードさせられる。

・接続されている別のハードディスクおよびリムーバブルドライブに自分自身をコピーする。

・パソコンに格納されている特定の情報を外部に送信する。

※注）　レジストリ　：　Windows が1つの場所で、全アプリケーションの設定を集中的に管理するようなシステムのこと

■USBワームへの対策　TREND MICRO　USBメモリで広まるウイルスへの対策より引用

http://jp.trendmicro.com/jp/threat/solutions/usb/?WT.ac=JPclusty_Threat_USBvirus#020

1. 出所不明のUSBメモリを使用しない

USBメモリは、信頼のできるコンピュータでのみ使われているものを使用しましょう。

2. 信頼できないコンピュータではUSBメモリを使用しない

USBメモリを使用するコンピュータは、ウイルス対策ソフトを常に最新の状態で使用し、ウイルスが存在しないようにしておきましょう。公共のパソコンやネットカフェなど、セキュリティ対策が不明なコンピュータでUSBメモリを使用するのはやめましょう。

3. USBメモリの自動実行をさせない

マイ コンピュータからUSBメモリに該当するドライブをクリックすることで、「autorun.inf」ファイルが実行される可能性があります。マイ コンピュータではなく、エクスプローラで、必要なファイルのみを使用するようにしましょう。そして、ファイルを開く前には、必ずウイルスチェックをするようにしてください。
また、USBメモリのルートフォルダに「autorun.inf」という名前のフォルダを先に作成しておくことで、USBワームによる不正な「autorun.inf」ファイルを作成させないという方法もあります。

■Autorun.inf について　　キャノンITソリューションより引用

http://canon-its.jp/product/nd/virusinfo/vr_inf_autorun.html

通常、Autorun.inf 自身は悪意のあるアーカイブではありません。このファイルの役目は、主にリムーバブルデバイスおよびメディア(例: USBメモリ、USB接続外付けハードディスク、CD、DVDなど)に対して、コンピュータに接続もしくは新しいメディアが挿入されると、自動的にプログラムが実行できるようにするため役割を持ちます。一般的には、ソフトウェアのインストールの際にCDを挿入すると、自動的にインストーラが起動するのは、CDに含まれているインストーラを起動させるファイルが、Autorun.infに情報としてテキストデータで書かれているためです。つまり、Autorun.inf 自身はプログラムを持ち合わせているわけではなく、他のプログラムを実行させるための情報を持っているだけに過ぎません。
※Autorun.inf は、どのメディアでもルートディレクトリに置かれています。

◎「SHIFT」キーを押しながら、USBメモリをパソコンに接続する