USB メモリなどを経由して感染するウィルスへの対策

昨年後半から全国的に猛威をふるっているのが USB メモリなどを媒体として感染を広げるウィルスです（以降、USB ワームと呼びます）。

USB ワームが広まる要因は「Autorun.inf」と呼ばれるファイルによる自動実行の仕組みにあります。Windows ではメディアの利便性を高めるため、このファイルを利用してアイコンの変更やソフトウェアの自動起動を実現しており、多くの市販ソフトウェアがこの機能を利用しています（CD-ROM を挿入すると、自動的にソフトウェアのインストールプログラムが動き出すのが代表的な例です）。

１．USB ワームに感染する流れの例

①USB ワームに感染しているパソコンに USB メモリなどを挿すと、USB ワームが自分自身のコピーとその起動を促す「Autorun.inf」ファイルを書き込みます。

②感染していないパソコンに、①で USB ワームが書き込まれた USB メモリなどを挿した場合、そのままではまだ USB ワームは実行されませんが、Windows の自動起動の機能により USB ワームが起動され、知らない間に感染します。

③感染しているパソコンに USB メモリなどを挿すと、その都度 USB ワームを媒介するメディアが増加し、瞬く間に広まります。

このような流れの媒介役には USB メモリ、USB ハードディスク、デジタルカメラ、カードリーダなど、USB などで接続するタイプでデータの書き込みが可能なものがほとんど含まれます。

２．USB ワームへの対策

OS による「Autorun.inf」の実行タイミングは以下のようになっています。

■Vista の場合

初期設定において「Autorun.inf」に実行ファイルが起動するように指定されている USB メモリなどを接続した場合、直ちに該当プログラムが起動されます。

■XP/2000 の場合

初期設定において、「Autorun.inf」に実行ファイルが起動するように指定されている USB メモリなどを接続した場合でも、直ちに該当プログラムが起動されることはありません。ただし、マイコンピュータを開き、リムーバブルメディアアイコンをダブルクリックして開くと、その時点で該当プログラムが起動されます。

以上の違いを確認した上で、使用している OS ごとに次の様な対策を行ってください。

<Step 1> 基本的な対策

最も重要なのは Windows Update などでセキュリティホールを埋めることと、信頼できるウィルス対策ソフトをインストールし、しっかりとウィルス検出用パターンファイルの更新を行う事です。

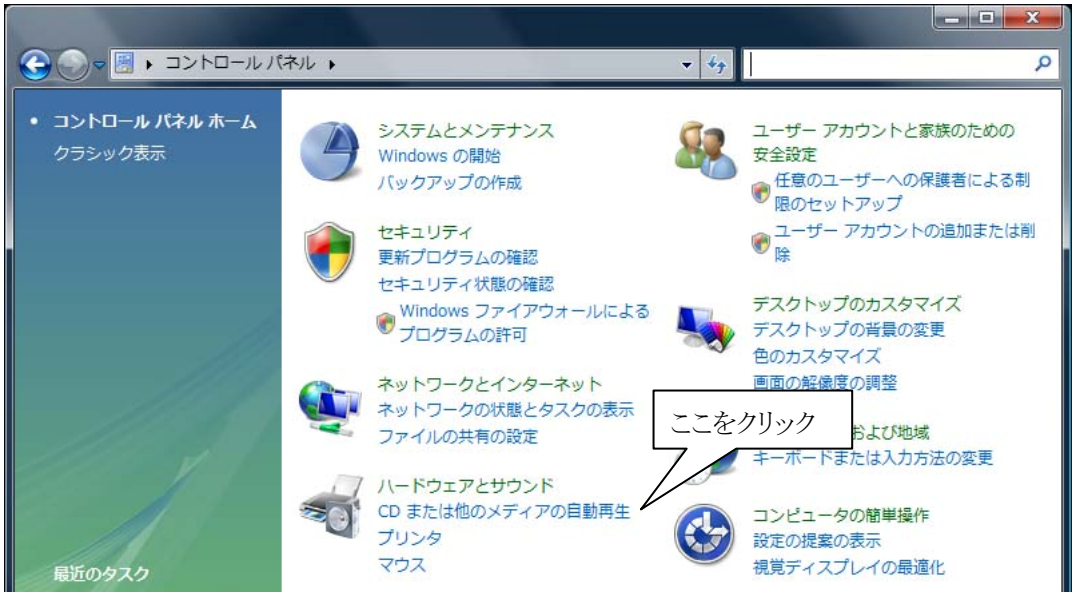
最近ではこのパターンファイルは一日に何度も更新され、新たに発生するウィルスが検出できるように工夫しています。このパターンファイルの作成・更新を的確に行ってくれるメーカーの製品を使いましょう。値段が高ければ信頼できるというわけではありませんが、どの製品でも同じようにウィルスを検出できるわけでもありません。通常、パターンファイルは定期的に自動更新されますが、時々、パターンファイルの更新状況を自分の目でチェックするくらいの注意深さが求められます。

<Step 2>「Autorun.inf」による自動起動を止める

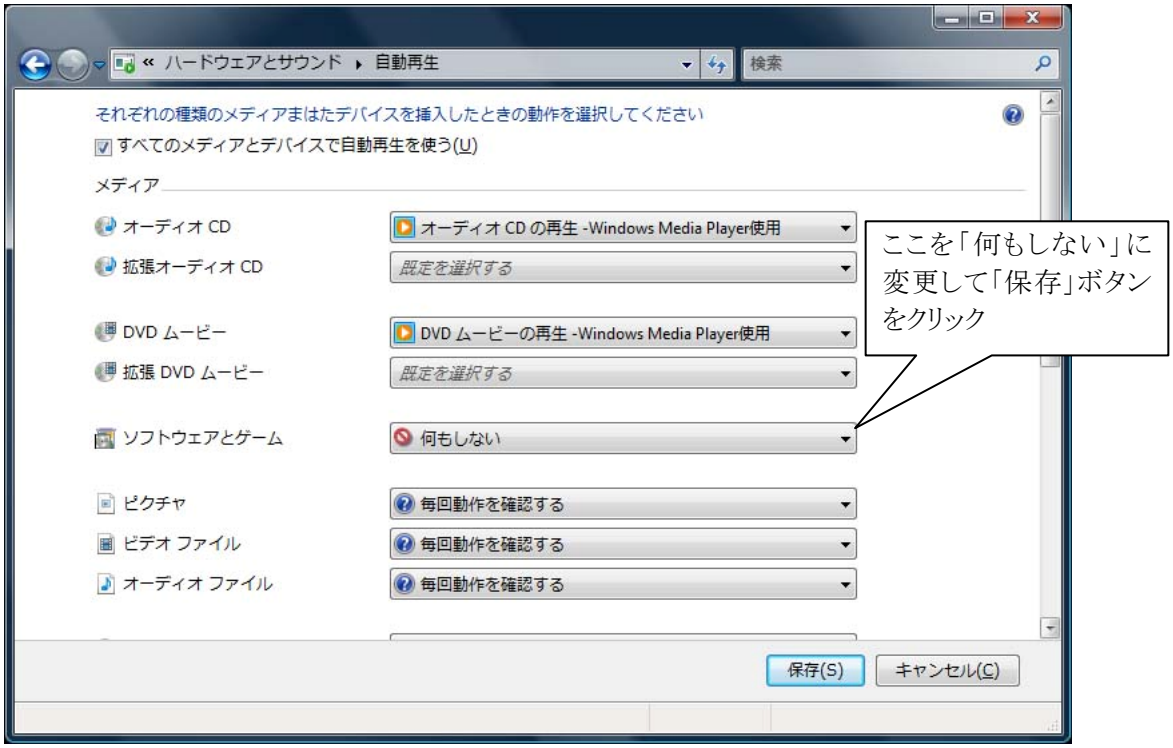
■Windows Vista の場合

Vista では USB メモリなどを挿しただけで「Autorun.inf」が実行される危険性があります。必ず以下の手順で自動起動の設定を変更してください。

①スタートメニューから「コントロールパネル」を開き、「ハードウェアとサウンド」の「CD または他のメディアの自動再生」をクリックします。



②「ソフトウェアとゲーム」欄の設定を「プログラムのインストール／実行」から「何もしない」に変更して「保存」します。これで、CD や DVD の自動再生は有効のまま、USB メモリなどの自動再生は無効になります。

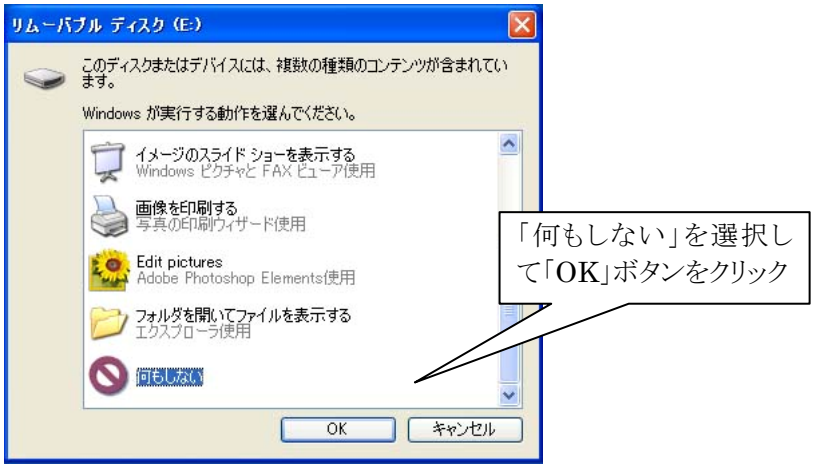


③上記により自動起動が無効となりますが、USB メモリなどを挿したら、ウィルス対策ソフトの「ウィルス検索」機能を利用してウィルスが含まれていないことを確認してから利用してください。

■Windows XP、2000 の場合

WindowsXP や Windows2000 では USB メモリなどを挿しただけでは「Autorun.inf」は実行されません。以下の手順で取り扱ってください。

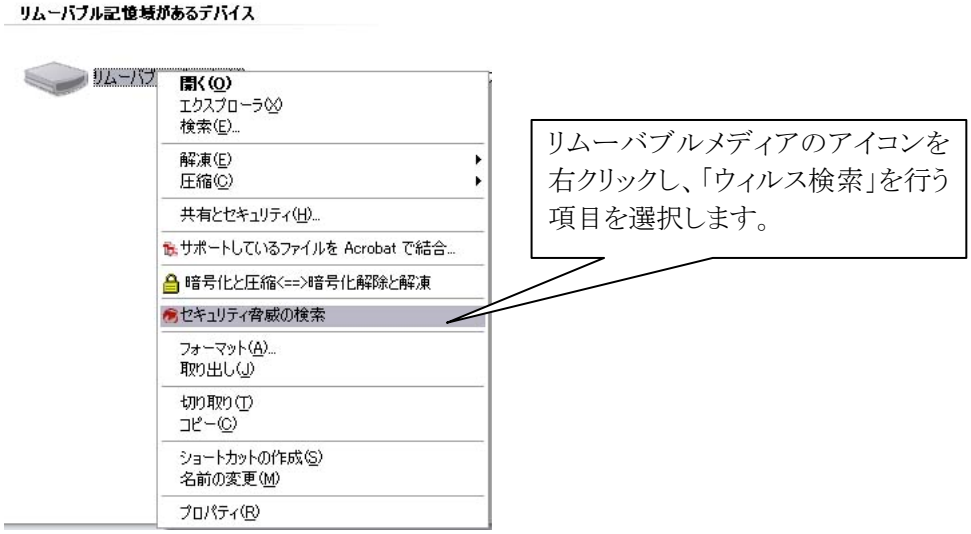
①USB メモリなどを挿した場合に、以下のようなダイアログが表示されたら、「何もしない」を選択して「OK」をクリックします。このダイアログが表示されない場合もあります。



②ウィルス対策ソフトの「ウィルス検索」機能を利用してウィルスが含まれていないことを確認してから利用してください。

〈Step 3〉 ウィルス対策ソフトでUSBメモリなどのウィルスチェックを実行する（各OS共通）

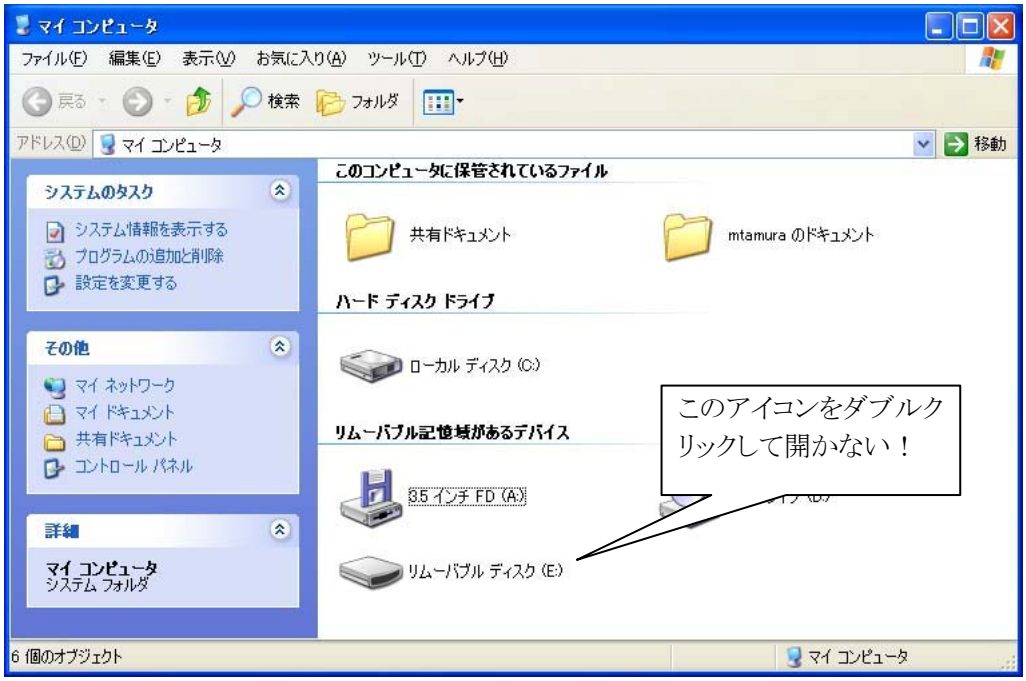
①「マイコンピュータ」を右クリックして「エクスプローラ」を選択するなどしてエクスプローラを起動し、USB メモリなどのリムーバブルメディアのアイコンを右クリックし、メニューから「ウィルス検索」（←使用しているウィルス対策ソフトによって表現が異なります）を選択します。



②上記のチェックでウィルスが検出されなければ、安全に使用できます。ただし、ウィルス対策ソフトのパターンファイルが最新のものに更新されていない場合、正しく検出されないこともありますので、注意してください。

〈Step 4〉 USBメモリなどのファイルを使用する場合の注意（各OS共通）

①ウィルスチェックが済んでいないUSBメモリなどを挿したとき、マイコンピュータを開いて**リムーバブルメディアのアイコンをダブルクリックすることは厳禁**です。この操作によって「Autorun.inf」が実行され、USBワームに感染する可能性が高くなります。



②ウィルスチェックが済んでいる場合でも、もしかしたら検出できなかったウィルスが潜んでいるかもしれません。中のファイルを確認したい場合は、マイコンピュータから開いていくのではなく、エクスプローラを使用してフォルダビューから展開していくようにしてください。