コンピュータウイルス『POSSIBLE_OTORUN2』の詳細及び対策

【始めに】現状の報告

最近農学科の研究室で感染例が増えているコンピュータウイルスがあります。「POSSIBLE_OTORUN2」という名前のウイルスで、リムーバブルドライブ内で他の不正プログラムを実行させる疑いのある "autorun.inf" ファイルを発見した際の検出名です。

実際に「POSSIBLE_OTORUN2」は現在日本、ワールドワイドいずれとも第 1 位の被害報告があがっているほど猛威を振るっているコンピュータウイルスです。

このウイルスは USB フラッシュメモリやポータブル HDD、CD、DVD などの記憶媒体の中の、Windows「自動再生」機能を実行するためのファイル(拡張子.inf)を書き換え、不正なプログラムを実行させるものです。

現段階でのウイルスの根本的な駆除方法はありません。ウイルスバスターやノートンを始めとするウイルス対策ソフトを用いても駆除することができないので注意してください。

以下に対策方法を記載します。

※ なお、この文書では Windows XP についてのみ言及しています。その他の OS をお使いの方はこの文書を参考にして対処してください。

----------◆免責事項◆----------

この設定変更によってパソコンの動作に異常をきたすことはありませんが、これはレジストリの値を書き換えるものなので、すべての作業は自己責任で行なってください。

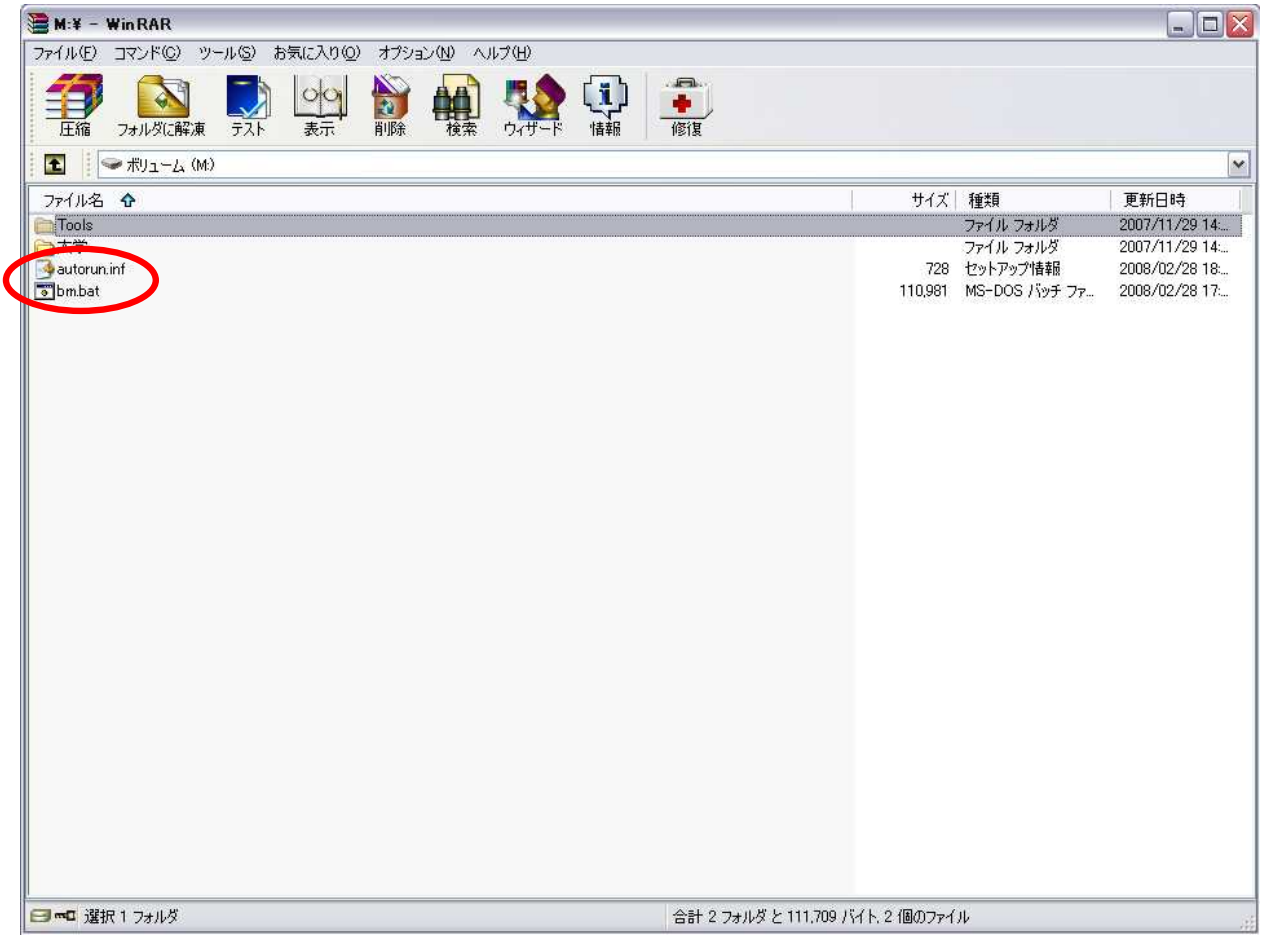
※ 操作を誤ると、Windows が正常に動作しなくなったり、起動しなくなったりしてしまいます。間違えないように注意して行ってください。

このマニュアルの説明にしたがって対処を行なって万が一トラブルがあった場合、当方は一切の責任を負いかねますのでご了承ください。

【手順 1】ファイルを消す

まず最初に誤解のないよう言及しなければなりませんが、たしかにいわゆるアンチウイルスソフトで今回話題の焦点となっている「POSSIBLE_OTORUN2」を駆除することはできません。しかし、それは検出することができないということではありません。当然然るべき部分をスキャンすれば検出自体はされるのです。

リムーバブルドライブ内部に問題のウイルスが存在しているので、まずはリムーバルドライブをスキャンし、検出したファイルを消すことから始めます。普通に開いただけではファイルが表示されることはありません。WinRAR など、ドライブ内のファイルをすべて表示するソフトを使うと問題のファイルも表示されます。



実際に自分で保存したファイル以外は一度すべて消してしまって大丈夫です。「autorun.inf」と「bm.bat」などは自動で生成されるので消えても問題ありません。

この操作を毎回行なえば基本的に他のパソコンへの感染の可能性は低くなります。メディアを挿入した段階で自動再生が実行されているので、それ以降は手動で自動再生を実行さえしなければウイルスが実行されることがないからです。ただし、一度感染したパソコンに関しては意味がありません。これはあくまで他のパソコンへの感染の拡大を防ぐ手段にすぎません。

【手順 2】レジストリを書き換える

そもそもレジストリとは何なのかを説明します。

レジストリとは、Windows 上でコンピュータに関する設定情報を管理しているデータベースのことです。 同じバージョンの Windows でも、他人のパソコンは自分のパソコンと操作方法が微妙に違っていて、使いづらいことがあるかと思います。Windows では、様々な設定を自分の好みに変更することができます。例えば、ファイルをダブルクリックの代わりにシングルクリックで開くようにしたり、小さなアイコンを表示させたりなどです。これらの情報を管理しているのがレジストリです。その他にも、ソフトウェアのインストール情報や画面やスクリーンセーバなどの情報も管理していて、壁紙を変更したりの操作をすると、レジストリも自動的に書き換えられることになります。

通常、レジストリを手動で変更する必要はありません。ところが今回の悪質なウイルスは、このレジストリを書き換えて、コンピュータの情報を勝手に変更してしまいます。このようなタイプのウイルスに感染してしまった場合、レジストリを手動で元に戻さなくてはなりません。

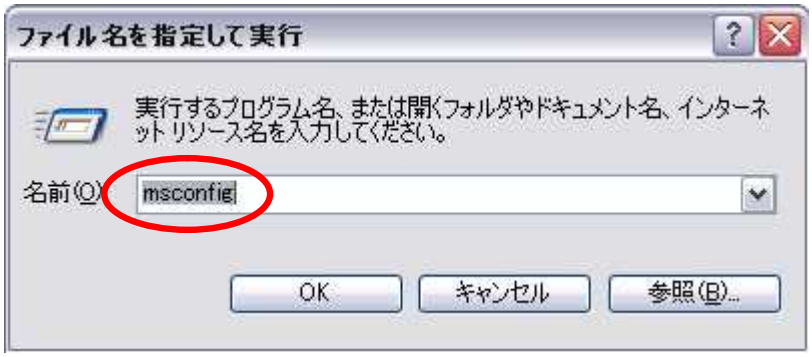
今回はレジストリを書き換えることで自動再生が機能しないようにします。ただし、レジストリを書き換えるということはパソコンのシステムファイルにアクセスするということなので、書き換えミス等、何かトラブルや不測の事態が起こった場合を考えて必ずバックアップを取るようにしてください。

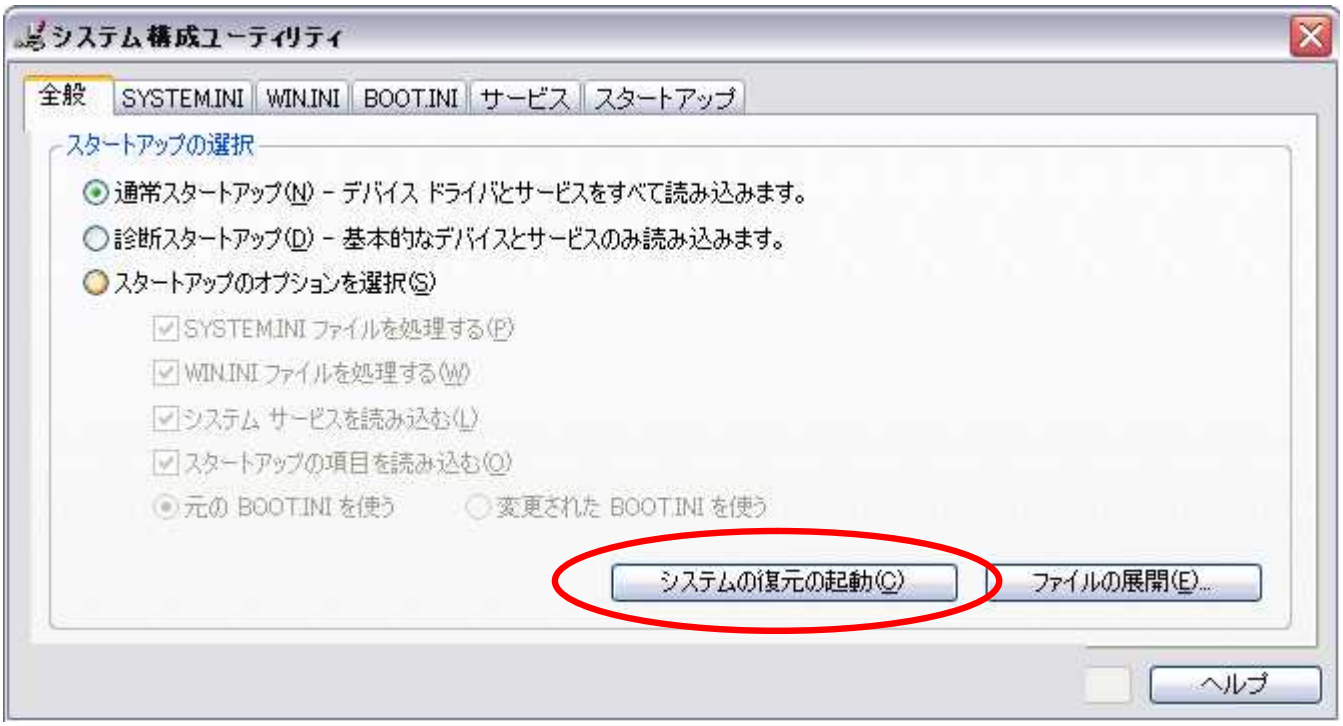
バックアップのやり方としては 2 つあります。

1. **システムを復元する。**
2. **レジストリをコピーする。**

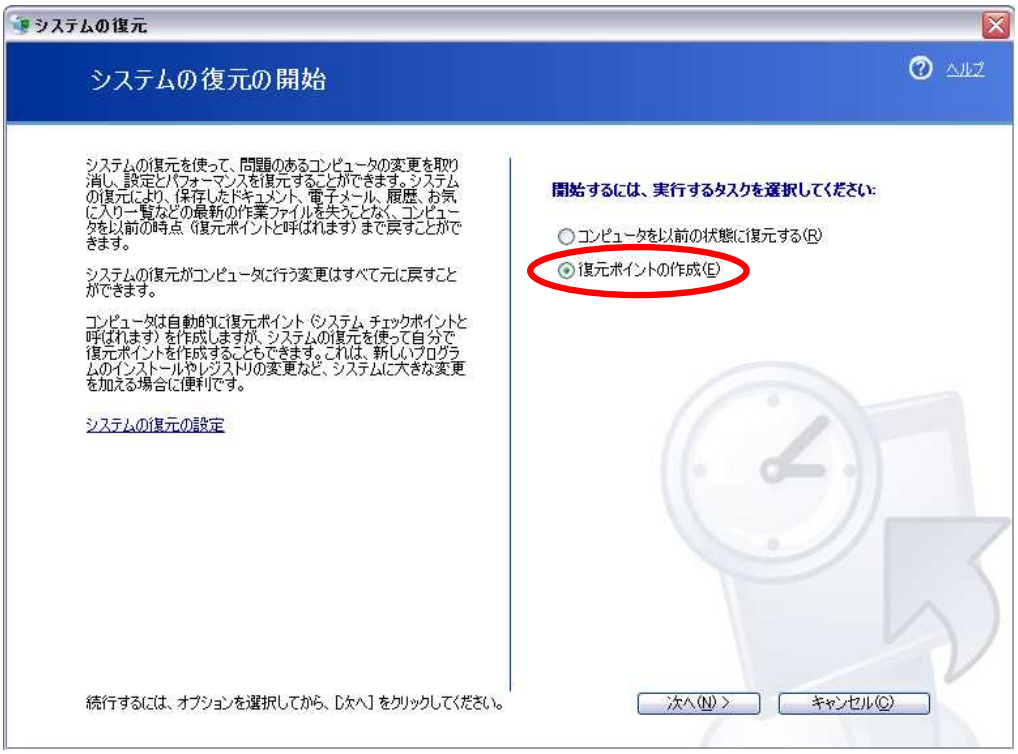
■システムを復元する。

まず[スタート] - [すべてのプログラム] - [アクセサリ] - [システムツール] - [システムの復元]、または[スタート] - [ファイル名を指定して実行] - [msconfig] - [システムの復元の起動]を実行します。

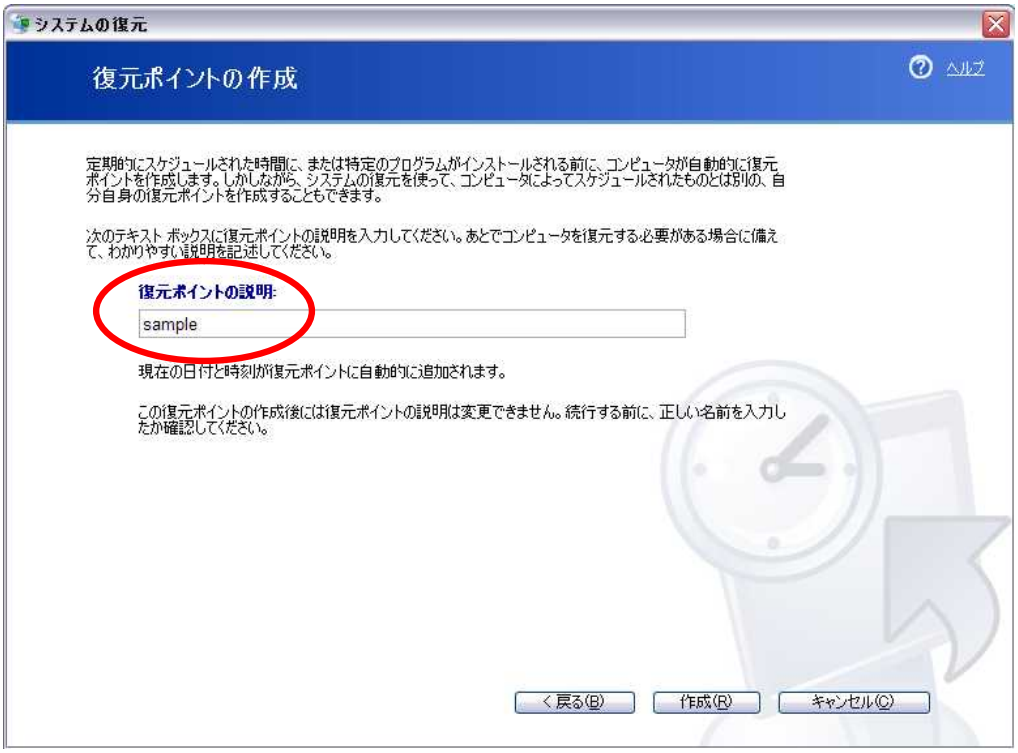




どちらの方法でも以下のような「システムの復元」の画面が表示されます。



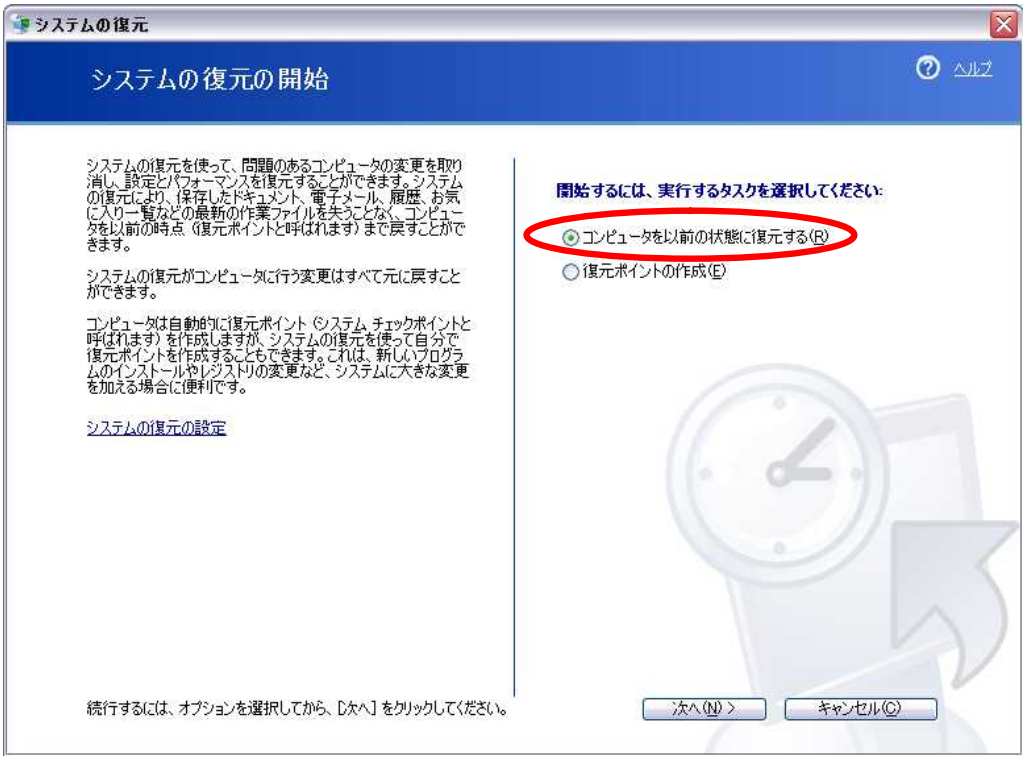
画面が開いたら上図のように「復元ポイントの作成」を選択して次の画面へ進みます。



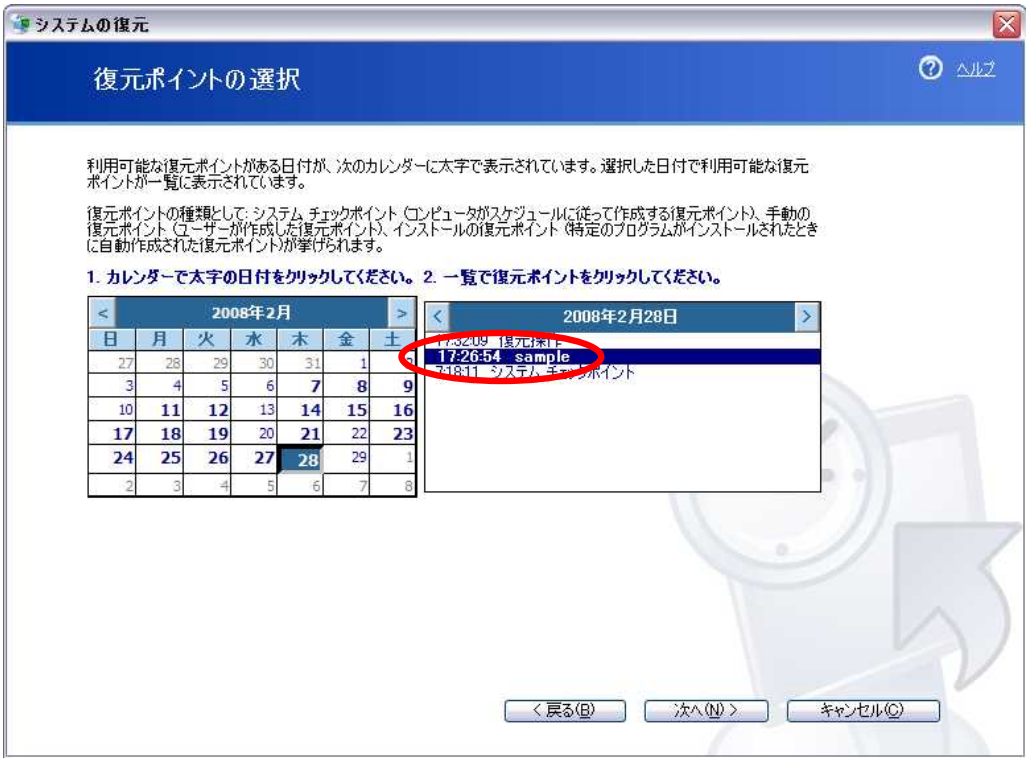
上の画面で「復元ポイントの説明」の欄に適当な名前を付けてから復元ポイントを作成します。

復元ポイントの作成が完了すると下図のように表示されます。これで何かトラブルが起こったときに作成した時点まで復元することができます。

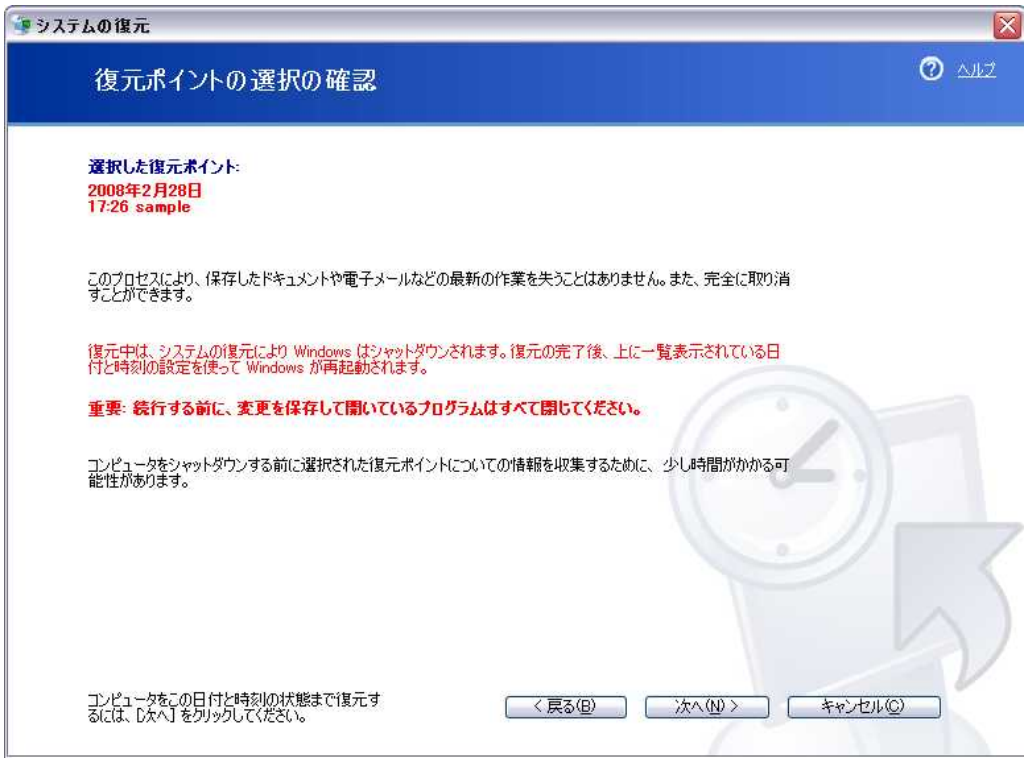
では実際に何かしらのトラブルが発生し復元する必要が生じた場合のやり方を紹介します。
このときも復元ポイントを作成するときと同じよう、「システムの復元」を起動します。



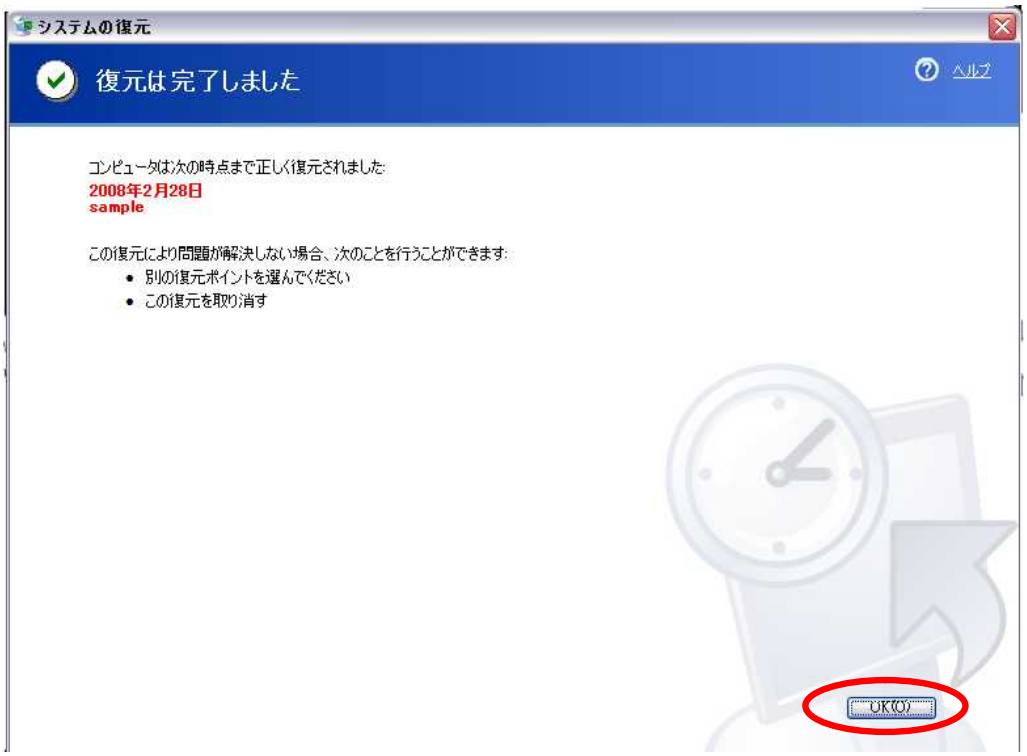
今度は「コンピュータを以前の状態に復元する」を選択して次の画面へ進みます。



すると上図のようなカレンダーが表示されます。「1.カレンダーで太字の日付をクリックしてください。」の中で復元ポイントを作成した日時を選択します。選択すると「2.一覧で復元ポイントをクリックしてください。」の中に作成した復元ポイントが表示されます。そこを選択して次の画面へ進みます。



選択すると上図のように確認の画面が表示されます。特に問題がなければ次へ進みます。するとコンピュータが再起動され、システムの復元が開始されます。



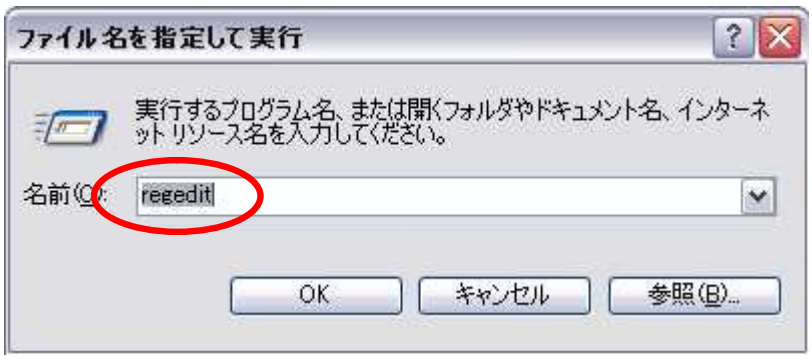
再起動が完了し、システムの復元が正常に行なわれると上のように完了の確認画面が表示されます。OK を押すとコンピュータが正常に起動します。

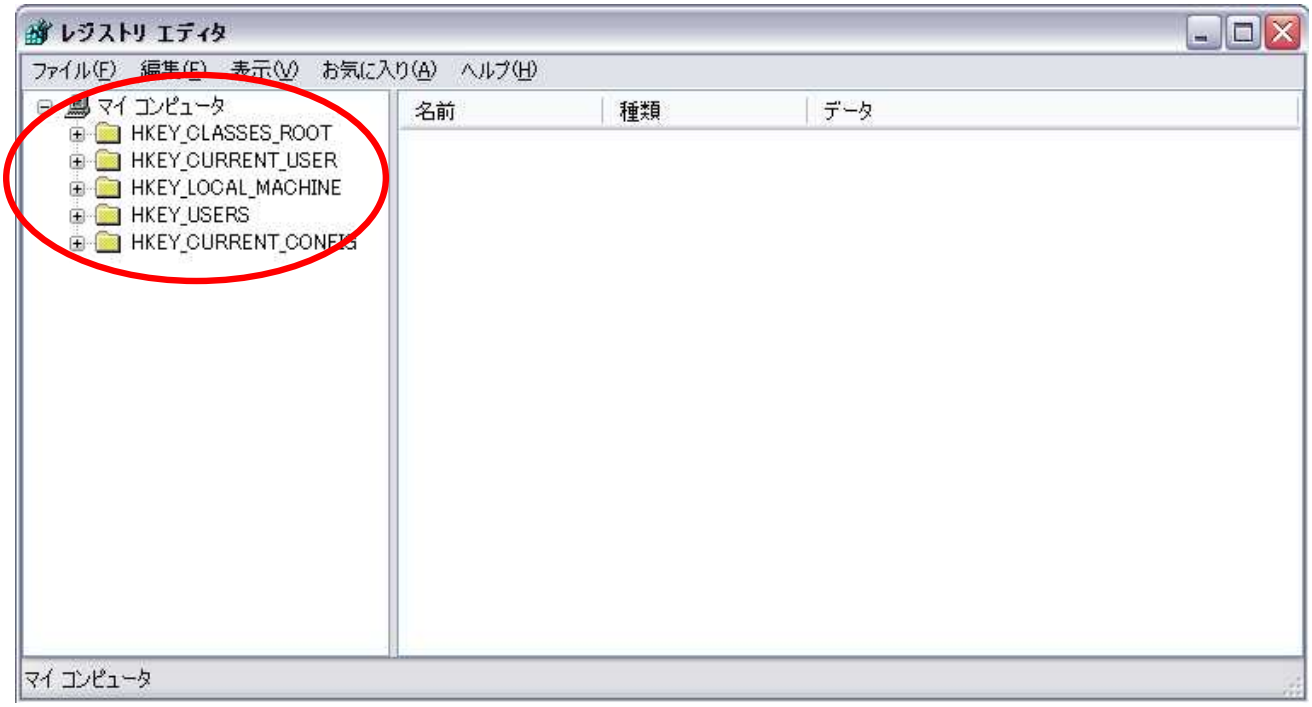
これでシステムを復元することができます。

※ 基本的にコンピュータには 90 日までシステムのバックアップが取ってあるので、復元ポイントの作成を忘れてしまっても復元することはできます。しかし復元できるポイントが不定なので、システムファイルを操作するときは必ず直前に復元ポイントを作成するようにしてください。

■レジストリをコピーする。

[スタート] - [ファイル名を指定して実行] - [regedit] - [レジストリ エディタ]を実行します。





エディタが起動するとマイドキュメントなど、エクスプローラのように扱うことができます。左の窓で必要なフォルダを選択すると右の窓にレジストリファイルが表示されます。

バックアップを取る際には[ファイル] – [エクスポート]から必要なファイルを出力するようにしてください。

反対に、何かトラブルがあったりなどしてレジストリを元の状態に戻したいときはエクスポートしたファイルをダブルクリックすれば完了します。または[ファイル] – [インポート]からバックアップしてあったレジストリファイルを入力することもできます。

【手順 3】自動再生機能を停止させる

それでは実際に Windows の自動再生機能を停止させていきます。
ここで Windows XP には Home edition と Professional edition とがありますが、Professional edition には「グループ ポリシー」という便利な機能があるので、レジストリを直接操作しなくても自動再生機能をオフにすることができます。

◆Professional edition のみ

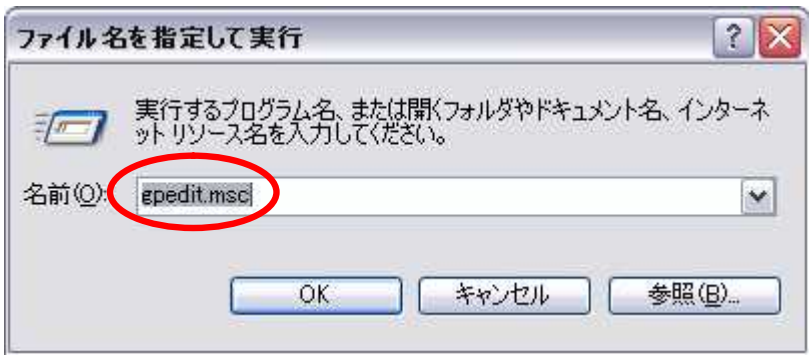
1. 「グループ ポリシー」を利用する。

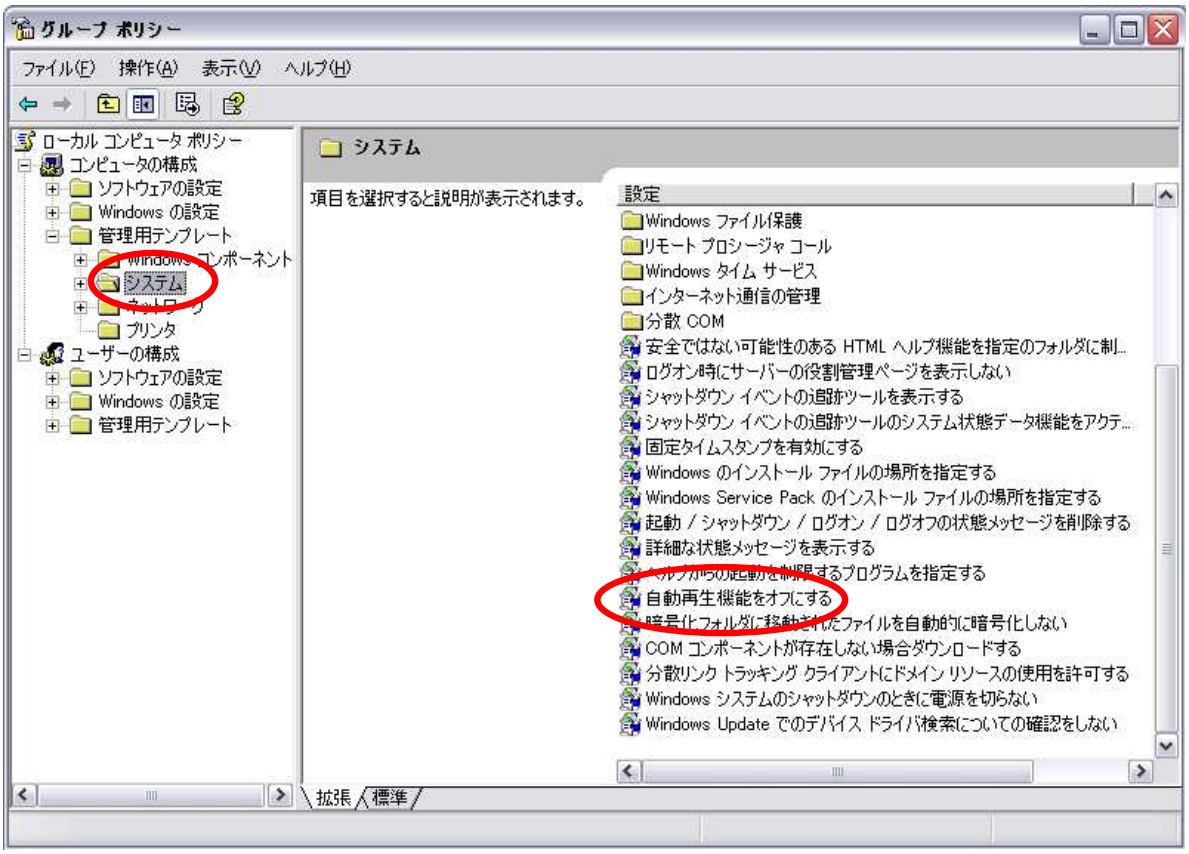
◆Home edition 及び Professional edition でグループ ポリシーを利用しない場合

2. Windows の設定を変更するソフトウェア「TweakUI」を利用する。
3. レジストリを書き換える。

■「グループ ポリシー」を利用する。

[スタート] - [ファイル名を指定して実行] - [gpedit.msc] - [グループ ポリシー]を実行します。





グループ ポリシーが開いたら[コンピュータの構成] - [管理用テンプレート] - [システム]を開きます。上図のように右の窓に「自動再生機能をオフにする」という項目があるので、それを開きます。

「開くと自動再生機能をオフにするのプロパティ」を設定します。

上図のように設定を有効にし、「すべてのドライブ」を選択して適用します。

グループ ポリシーを利用した設定はこれで完了です。

■Windows の設定を変更するソフトウェア「TweakUI」を利用する。

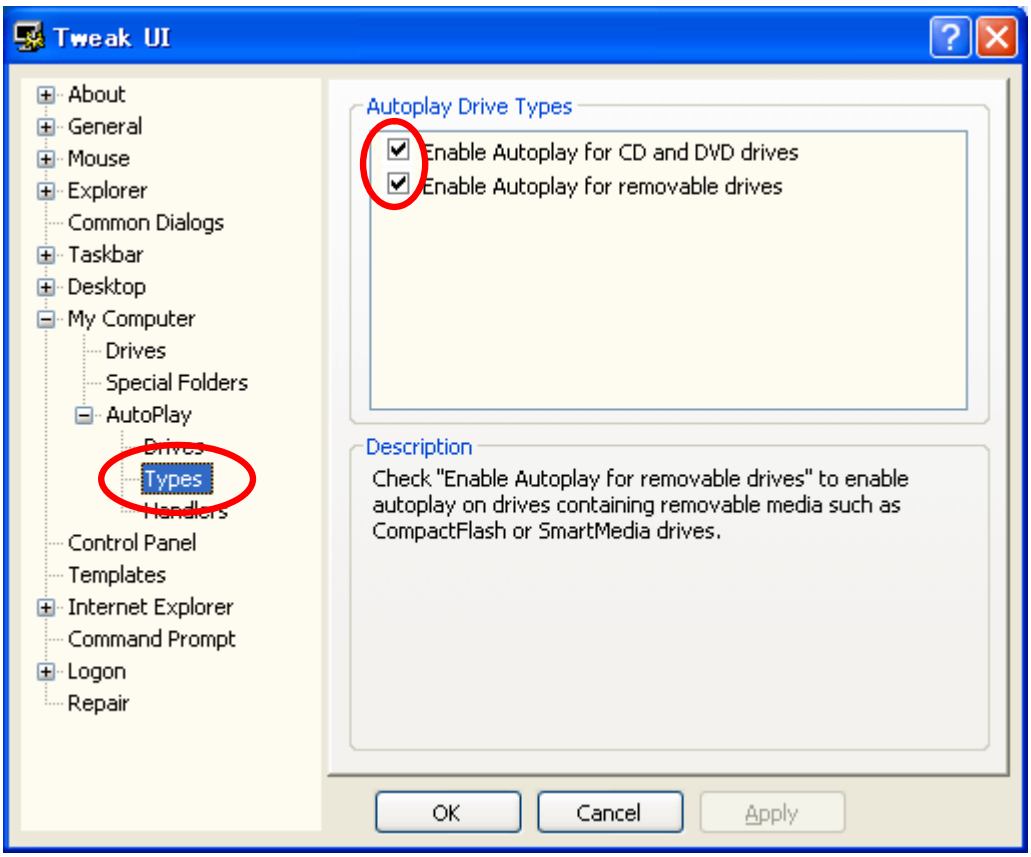
TweakUI はマイクロソフト社から無保証で提供されているユーティリティ「Powertoys」の一部です。Powertoys は Microsoft 社が開発したものですが、Windows 製品の一部としてではなく、自力でトラブルを解決できるパワーユーザー向けに、無保証のツールとして配布されています。このツールの使用に関しては、Microsoft のテクニカルサポートを受けることは一切できません。

と言っても今回は簡単な設定をするだけですし、このマニュアル通り設定すれば特に問題はないかと思います。ただし、万が一トラブルがあった場合、当方は一切の責任を負いかねますのでご了承ください。

まずは TweakUI をダウンロードします。以下の URL にアクセスするとダウンロードが始まります。

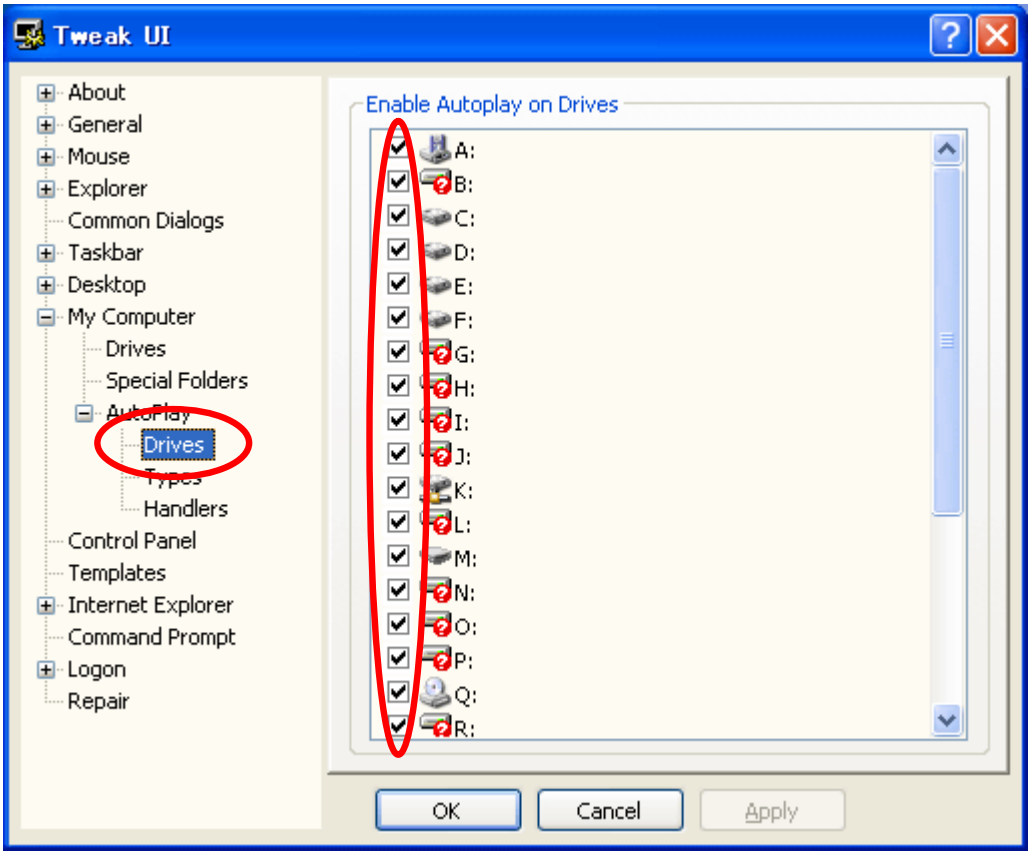
http://download.microsoft.com/download/f/c/a/fca6767b-9ed9-45a6-b352-839afb2a2679/TweakUiPowertoySetup.exe

ダウンロードが完了したらインストールをし、ソフトを実行してください。



左の窓で[My Computer] - [AutoPlay] - [Types]を選択すると右の窓が上図のように表示されます。デフォルトではどっちもチェックされて有効に設定されているので、右の窓のチェックボックスを両方外して無効にします。

次に左の窓で[My Computer] - [AutoPlay] - [Drives]を選択すると右の窓が下図のように表示されます。



右の窓はやはりすべてデフォルトでチェックされて有効に設定されているので、リムーバルドライブの対応するチェックボックスを外して無効にします。「Types」と「Drives」の設定は当然重複していますが、どちらか片方でも無効に設定されていれば自動再生も無効になるようです。

※ このとき、A、B、C のチェックは絶対に外さないようにしてください。パソコンの起動に関するプログラムが含まれているので、無効にしてしまうと起動ができなくなってしまいます。本体に D などのハードディスクがあるパソコンでは、D のチェックボックスも外さないで下さい(CD やメモリーカードのリーダー、リムーバブルドライブが割り当てられるアルファベットのチェックボックスをオフにしてください)。

※ またネットワーク HDD など、共有フォルダをお持ちの方は、Z や Y など、共有フォルダが割り当てられているアルファベットにチェックを入れないでください。再設定が必要になります。

TweakUI を利用した設定はこれで完了です。

■レジストリを書き換える。

◆レジストリを書き換える準備をする。

レジストリを書き換える際には Windows をセーフモードで起動して行なってください。

セーフモードとは、「Windows の起動に必要な最小限のファイルだけを読み込んで起動すること」という認識で良いと思います。 必要最小限の起動とは、普段と何が違うのでしょうか。

1. インターネットへの接続ができない。
2. ディスプレイドライバも標準の VGA 用のもので起動されるため、普段 SVGA や XGA などの解像度でパソコンを使っている場合はデスクトップのアイコンが大きく表示される。
3. モニタに表示できる色が通常の High Color(16 ビット)や True Color(24 ビット)に設定している場合でも 16 色に減る。このため色表示も通常と比べてかなりおかしくなる。
4. ドライバなどを必要とするような周辺機器(プリンタなど)は使用できない。

つまり、パソコンの起動に最低限必要なもの以外は読み込まないモードで起動するということです。アイコンが大きくなっても、表示される色数が減っても、周辺機器が使えなくても、パソコン自体は動作できます。これがセーフモードです。

なぜセーフモードで起動した状態でレジストリの書き換えを行なわなければならないかというと、ウイルスが活動に使うファイルの中には通常の起動では起動時に読み込まれてしまい、起動後は「使用中」になって変更も削除もできないファイルが数多くあります。しかしこれらのファイルの中にはセーフモードで起動すれば起動時に読み込まれずに変更や削除が可能になる場合があり、これを利用するためセーフモードでの起動が必要になるのです。

◆セーフモードで起動する手順

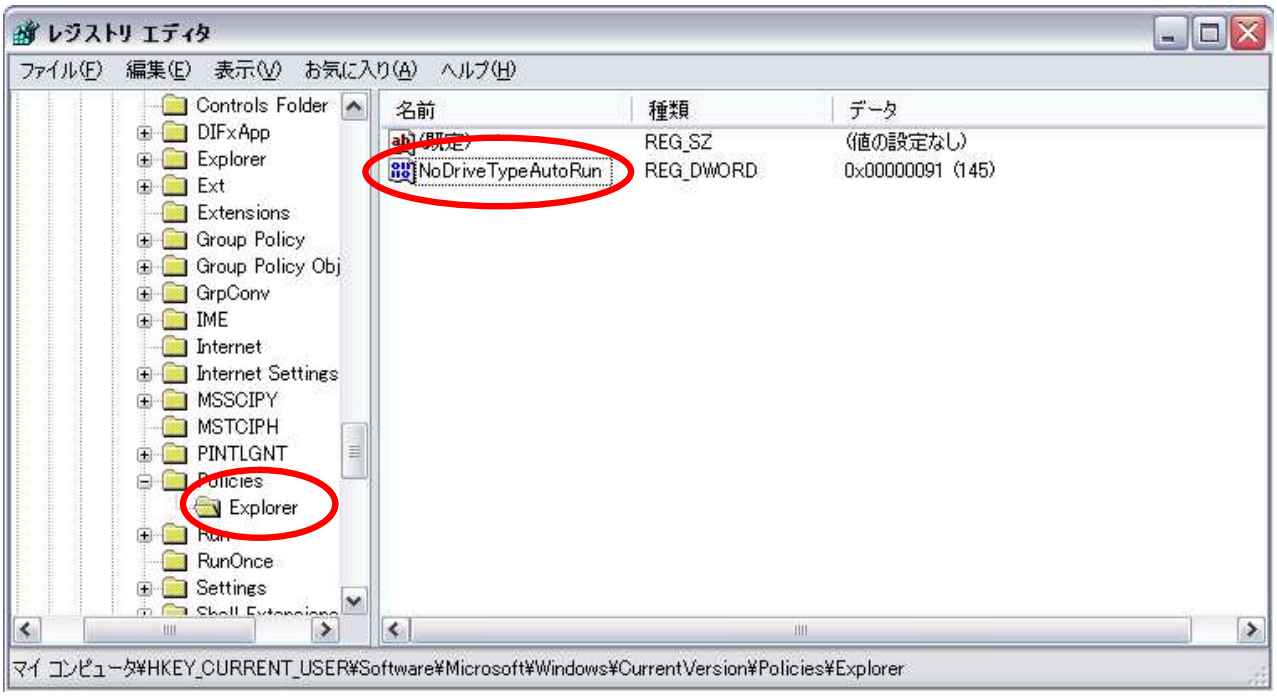
1. コンピュータを起動させる。
2. 「Windows XP を起動しています…」のメッセージが表示されている間に[F8]を押す。
3. 「Windows 拡張オプションメニュー」が表示されるので、[↓][↑］キーを使って[セーフモード]を選択し、[Enter]を押す。

◆レジストリの書き換えを実行する。

TweakUI は大変有用なツールですが、一回設定してしまえば終わりのソフトウェアなので、パソコンの軽量化を気にするのであればあまり無駄なインストールは避けたいという方もいるかもしれません。そこで実際に TweakUI によって無効化した結果のレジストリ設定を調べてみました。

結局 TweakUI もレジストリの書き換えをソフトを利用して簡単にしただけなので、レジストリを書き換えることでインストールしなくても同様の設定を行なうことができます。

自動再生に関するレジストリは[HKEY_CURRENT_USER] - [Software] - [Microsoft] - [Windows] - [CurrentVersion] - [Policies] - [Explorer]に含めれています。



TweakUI の「Types」によるレジストリの設定は以下のように設定します。

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Policies¥Explorer]
"NoDriveTypeAutoRun"=dword:000000b5
```

「NoDriveTypeAutoRun」の設定値によって動作が変わります。具体的な設定値は以下のようになります。

設定値	CD-ROM ドライブ	リムーバブルドライブ
dword:00000091	有効	有効
dword:00000095	有効	無効
dword:000000b1	無効	有効
dword:000000b5	無効	無効

TweakUI の「Drives」によるレジストリの設定は以下のように設定します。

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Policies¥Explorer]
"NoDriveAutoRun"=hex:FF,FF,FF,FF
```

これですべての文字に対応するドライブが無効となります。こちらも「NoDriveAutoRun」の設定値によって動作が変わります。

こちらの設定はやや複雑なのですが、このレジストリ値は REG_BINARY 型のバイナリ値で、各ドライブは下位ビットから順に対応しているようです。つまり最初の 1 byte(8bit)が、下位ビットから A：～H：ドライブに対応し、次の 1 byte が I：～P：に対応といった具合です。

「hex」というのは 16 進法を表わしています。ドライブは A～Z の英字に対応するのですが、それを横に並べて、その並びに 2 進法で有効を 1、無効を 2 として表現します。

少し専門性の強い話になってしまいましたが、簡単に図解すると以下のようになります。

対応ドライブ	HGFEDCBA	PONMLKJI	XWVUTSRQ	ZY------
2 進法	11111111	11111111	11111111	11111111
16 進法	FF	FF	FF	FF

これがすべての文字に対応するドライブの自動再生を無効にした場合の表となります。ちなみに最後の 6 文字分はドライブに対応する文字はありませんので 0 でも 1 でもまったく同じ結果が得られます。

例えば、無効にするドライブを A、E、F、K、M、Q とすると、対応する表は以下のようになる。

対応ドライブ	HGFEDCBA	PONMLKJI	XWVUTSRQ	ZY------
2 進法	00110001	00010100	00000001	00000000
16 進法	31	14	01	00

したがって、レジストリは以下のようになります。

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Policies¥Explorer]
"NoDriveAutoRun"=hex:31,14,01,00
```

※ 上記の例はあくまで例です。TweakUI に関する章でも明記しましたが、A、B、C を無効にしてしまうとパソコンの起動ができなくなります。絶対にやめてください。

【手順 4】設定を確認する

最後に設定の変更が有効かどうかの確認を行なってください。

と言っても作業自体はごく簡単なものです。実際に USB フラッシュメモリや CD、DVD といった類のリムーバルの記憶媒体をパソコンに挿入するだけです。挿入した際に見慣れた以下の図のような窓が出てこなかったら設定成功です。

【おまけ】TweakUI を日本語化する

必要ないと思いますが、インストールしたソフトを日本語化したいという人のために TweakUI の日本語化ツールのダウンロード先を記載します。

http://stereo.jpn.org/muttyan/file/twi133jb.lzh

こちらもインストールしてから万が一トラブルがあった場合、当方は一切の責任を負いかねますのでご了承ください。

【最後に】このマニュアルの利用に関して

このマニュアルの最初にも言及している通り、今回話題の焦点となっているコンピュータウイルス「POSSIBLE_OTORUN2」は、現存するアンチウイルスソフトでは駆除することはできません。しかし、これだけ世界的に猛威を振るっているウイルスを各社が放っておくことはありませんので、近いうちに「POSSIBLE_OTORUN2」を駆除することができるウイルス定義が配布されていくでしょう。駆除することが可能になれば今回の設定を元に戻しても問題はありません。このマニュアルで紹介した対処方法はあくまで緊急対処法であり、ウイルスの動作元を強引に抑えているだけにすぎません。つまり、**コンピュータはウイルスに感染したまま**ということです。そこは忘れないようにしてください。

またデジタル化が進む中、それに伴って利用する人々が深めるべきデジタル機器に対する知識は相当な遅れをとっていると言わざるを得ません。現段階で消えてしまってもさほど問題のあるデータを取り扱っている方はあまりいないかと思いますが、それでも卒業論文関連のデータであったり単位に関係のあるレポートであったり、それなりに大事なデータも増えてきているでしょう。自身のパソコンを操作する時も基本的には保存は 2 ヶ所、**それぞれが独立した HDD に保存したりしてバックアップを取る**ことを心がけてください。USB フラッシュメモリも外部の記憶媒体なので、文書などのバックアップ専用のものを用意してもいいかもしれません。

そして USB フラッシュメモリや CD、DVD など、リムーバルメディア上でのファイルの操作も避けるようにしてください。リムーバルメディア上で操作すると、パソコンが保存先にアクセスする度に内部の HDD にアクセスするのとは違い負荷がかかり、ファイルやメディアが壊れる原因となります。特に上書きができる USB フラッシュメモリなどでは、保存されている文書をそのまま開き操作を行なう人が少なくありません。**必ず一度デスクトップなど、HDD 上にコピーしそのファイルで作業をし、最後に保存したファイルをリムーバルメディアにコピーし直す**ようにしてください。

【情報ソース】
今回のマニュアルを作成する際に様々な情報を参考にさせていただきました。この場を借りてお礼申し上げます。
・トレンドマイクロ株式会社
・Lenovo Japan
・@IT(アットマーク・アイティ)
・BBBN Support Page
・ANGIE WORKSHOP
・Vector