

# Linux LiveCD を使った外部メディア専用ウイルスチェック方法

-自動感染機能のみのチェック-

2009/10/21 一般 PC 版 京都大学東南アジア研究所 情報処理室

注意：このシステムでウイルスらしきものを発見したからといって、すべてがウイルスとは限りません。なぜなら、製品 CD/DVD や一部の製品 USB メモリには、自動再生機能を導入しているケースがあるからです。

## 1. 利用準備

(ア)Linux Live CD を作成してください

### ① ISO イメージのダウンロード

<http://www.rcis.aist.go.jp/project/knoppix/> より

「KNOPPIX6.0.1CD 日本語版(LGAT 対応) 600MB」

をダウンロードしてください。

### ② ISO イメージから CD 作成

お手持ちの CD 作成ソフトを使って ISO イメージ書き込みを行って下さい。

必要でしたらお渡しします。

### ③ CD/DVD ドライブがない場合

比較的新しい端末であれば、USB メモリからの起動も可能です。

1GB の空き容量のある USB メモリをお持ち下されば、Linux LiveUSB を作成いたします。

(イ)CD/DVD ドライブに Linux LiveCD を挿入し、電源を入れ、CD から起動してください。

### ① システム起動場所を選択できるなら、CD 起動を選択してください、

DELL 社 PC は、起動時に「F12」をなにか押していると、システム起動場所選択画面が出てきます。

Eee PC のネットブックならば、「Tab」キーとなっています。

### ② もし、システム起動場所の選択が分からなければ、BIOS メニューを出し、Boot の順番としてハードディスクよりも CD を優先にしてください。


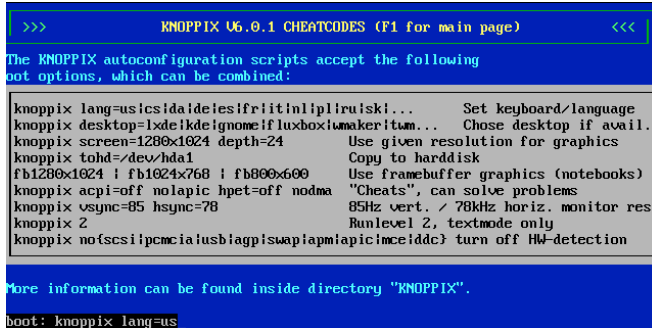
BIOS 設定については、各 PC 付随のマニュアルをお読み下さい。たとえば、DELL 社 PC は、起動時に「F2」キーを何度かおしていると、BIOS 画面が現れます。

# Linux LiveCD を使った外部メディア専用ウイルスチェック方法

-自動感染機能のみのチェック-

2009/10/21 一般 PC 版 京都大学東南アジア研究所 情報処理室

- 起動用 CD-ROM あるいは USB メモリをパソコンに差してから、パソコンを起動します。
- 下図のように boot: が出てきたら、必要に応じて下記の文字を追加してください。

|  |   |
|--|---|
|  <p><b>Knoppix 6</b><br/>CD/USB-Version - Release Information: <a href="http://knopper.net/knoppix/">http://knopper.net/knoppix/</a><br/>KNOPPIX U6.0.1 <a href="http://www.knoppix.de/">http://www.knoppix.de/</a> RELEASE: 2009-02-06 (2009-02-25 J)<br/>boot: _</p>  | <p>a) モニタ解像度の標準が 1024x768 を越える場合 (1280x1024 の場合)<br/>boot: screen=1280x1024</p> <p>b) 表示言語が日本語以外の場合 (英語にしたければ)<br/>boot: lang=us</p> <p>※a), b) 両方なら、<br/>「boot: lang=us screen=1280x1024」<br/>となる。</p> |
|  <pre>&gt;&gt;&gt; KNOPPIX U6.0.1 CHEATCODES (F1 for main page) &lt;&lt;&lt; The KNOPPIX autoconfiguration scripts accept the following boot options, which can be combined:  knoppix lang=us cs da de es fr it nl pl ru sk ... Set keyboard/language knoppix desktop=lxde kde gnome fluxbox umakeritum... Chose desktop if avail. knoppix screen=1280x1024 depth=24 Use given resolution for graphics knoppix tohd=/dev/hda1 Copy to harddisk fb1280x1024   fb1024x768   fb800x600 Use framebuffer graphics (notebooks) knoppix acpi=off nolapic hpet=off nodma "Cheats", can solve problems knoppix vsync=85 hsync=78 85Hz vert. / 78kHz horiz. monitor res knoppix 2 Runlevel 2, textmode only knoppix noscsi pcmcia usb agp swapi apic mc ddc) turn off HW-detection  More information can be found inside directory "KNOPPIX". boot: knoppix lang=us_</pre> | <p>F3 を押せば詳細オプションが表示されます。</p> <p>また日本語キーボードなどの場合、「=」の位置が本来の位置では出てこない場合があります。</p> <p>その場合には「へ(^)」を押してみてください。</p>   |

最後に Enter を押すこと。

- すると下図のように OS の起動が始まります。

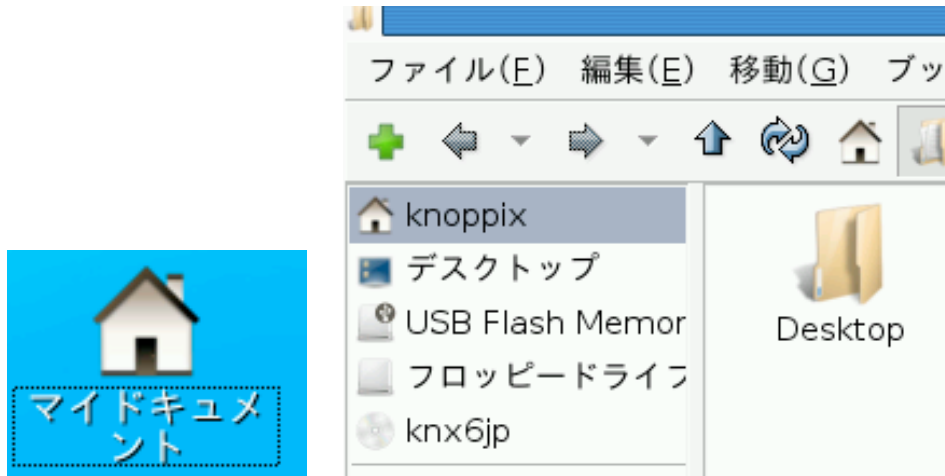


- しばらく待っているとデスクトップ画面が出てきますので、USB メモリや USB HDD をパソコンに差し込みます。
- そして下図のような「マイドキュメント」をクリックしてください。すると下記の右図のような画面が出てきます。たとえば USB メモリを差し込んだ場合、「USB Flash Memory」が出ているはずですが、それをクリックしてください。

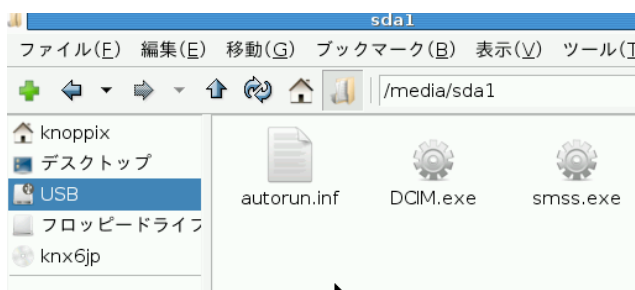
# Linux LiveCD を使った外部メディア専用ウイルスチェック方法

-自動感染機能のみのチェック-

2009/10/21 一般 PC 版 京都大学東南アジア研究所 情報処理室



7. すると、「USB Flash Memory」が USB メモリに付けた名前（今回は USB）に変更された上、下図の画面が出てくるはずです。



8. リスト表示するために、下図の矢印部分を参考にリストアイコンをクリックしてください。ここで「Autorun. inf」があればウイルスが仕込まれている可能性が非常に高くなります。

至急、情報処理室にご連絡下さい。 情報処理室は侵入経路の特定、再発防止策を練るためにウイルスの捕獲を常に望んでおります。連絡が取れない場合には次に進んでください。（下記の例では、捕獲したウイルスを例に挙げています。Smss.exe がウイルスの本体、DCIM.exe はデジカメ画像データをウイルスによって覆い隠している例です）

Autorun が見つけられなければ、右上の×を押して「10」に進んでください。



- (ア) Autorun. inf があれば、右クリックして「削除」が選択できるかどうか見て下さい。選択できれば次へ進んでください。 下図のように選択できなければ「プロパ

# Linux LiveCD を使った外部メディア専用ウイルスチェック方法

-自動感染機能のみのチェック-

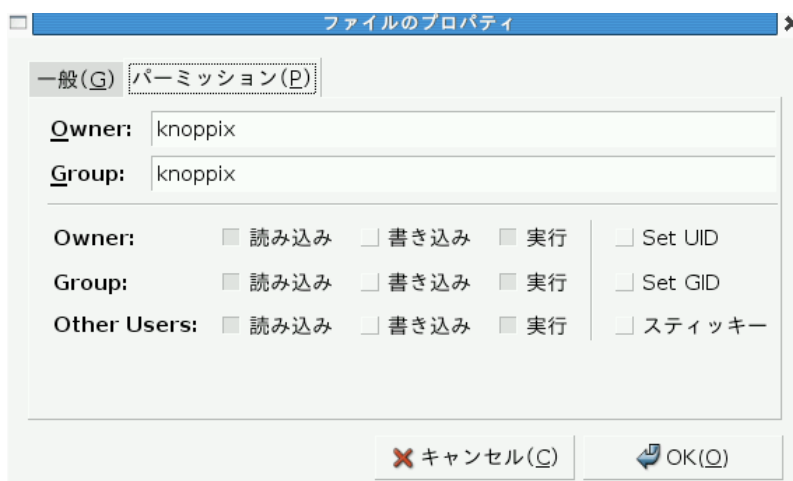
2009/10/21 一般 PC 版 京都大学東南アジア研究所 情報処理室

ティ」を選んで、サブ項目「書き込みの有効化」へ進んでください。

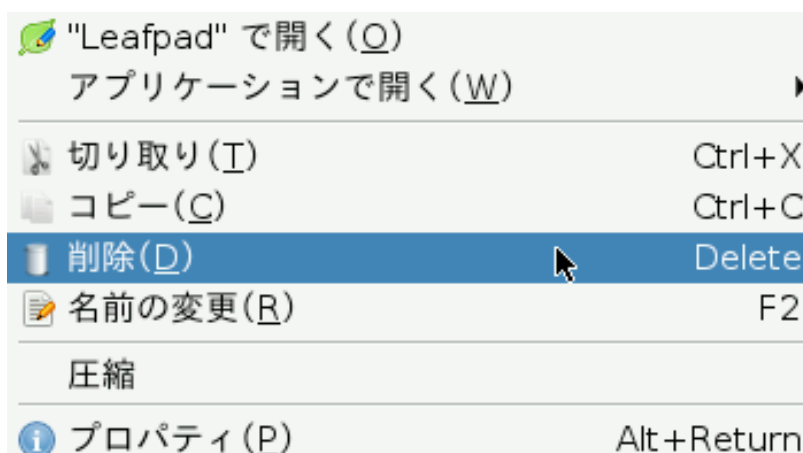


## ① 「書き込みの有効化」

プロパティを選んで、上部の「パーミッション」をクリックしてください。そして下図の「書き込み」の選択ボタン「」のチェックをすべてつけてください。



(イ) 下図のように削除を選択できれば、選択してください。

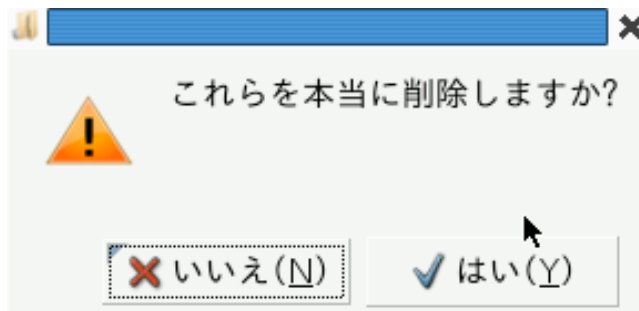


(ウ) 下図のように、「削除して本当にいいのか？」と出てくるので「はい」のボタンをクリックしてください。

# Linux LiveCD を使った外部メディア専用ウイルスチェック方法

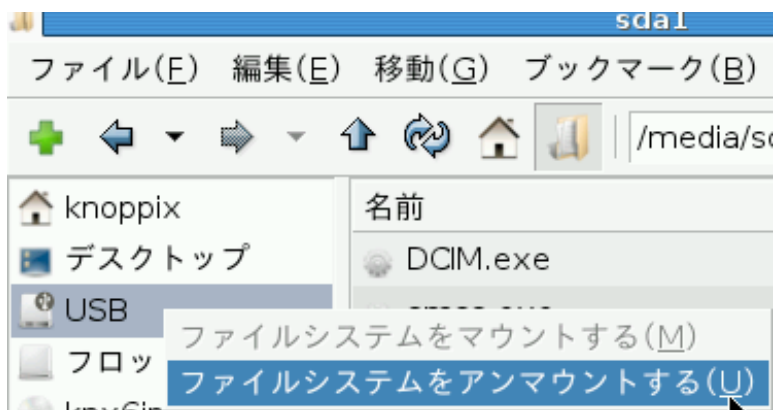
-自動感染機能のみのチェック-

2009/10/21 一般 PC 版 京都大学東南アジア研究所 情報処理室

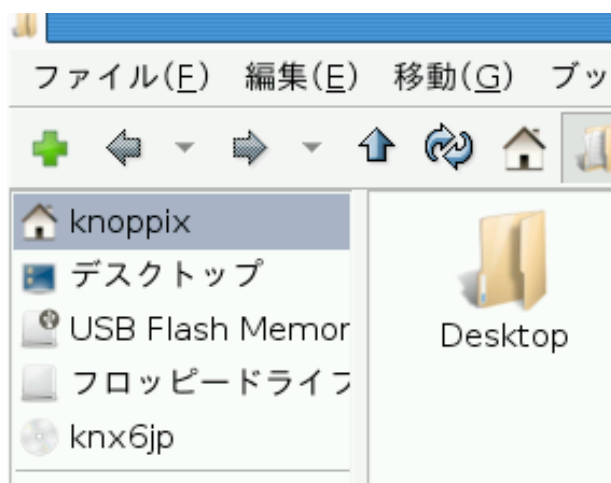


(エ)そして Autorun.inf が消えたことを確認してください。なお smss.exe など意図しないデータがあった場合にも、削除されることをお勧めします。

9. 外部メディアを取り出します。「マイドキュメント」の左サイドニューにある「USB メモリ」アイコンで「右クリック」して「ファイルシステムをアンマウントする」を選択します。



すると、下図のように「USB Flash Memory」という表示に変わっているはずです。これでメディアを抜くことができます。



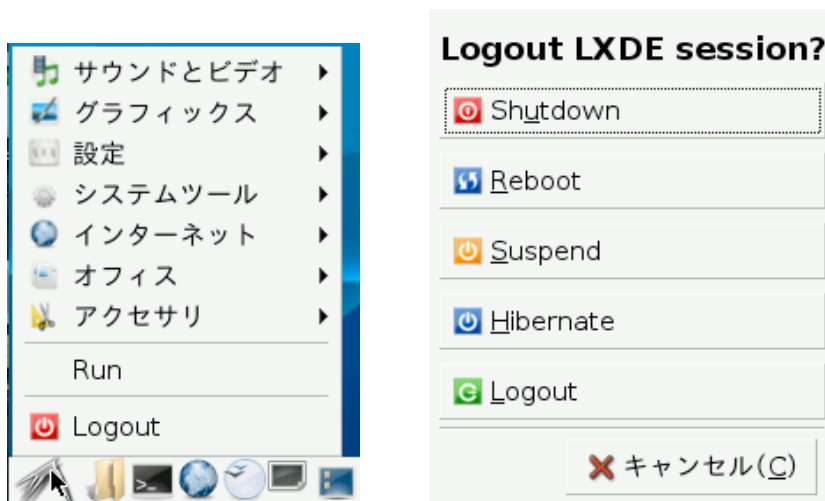
※必要に応じて、他の外部メディアを接続して「ステップ4～8」を繰り返してください。

# Linux LiveCD を使った外部メディア専用ウイルスチェック方法

-自動感染機能のみのチェック-

2009/10/21 一般 PC 版 京都大学東南アジア研究所 情報処理室

10. 最後に終了します。下図の左のアイコンをクリックして、「Logout」を選択し、「Shutdown」を選択してください。



11. 下図がでたら、CD を取り出して Enter を押してください。パソコンが終了します。

```
Shutdown complete.  
[ 1123.143750] SysRq : Emergency Sync  
[ 1124.153464] SysRq : Emergency Remount R/O  
Please remove CD, close cdrom drive and hit return [2 minutes].
```