



日本セキュアOSユーザ会  
Japan Secure Operating System Users Group since 2007

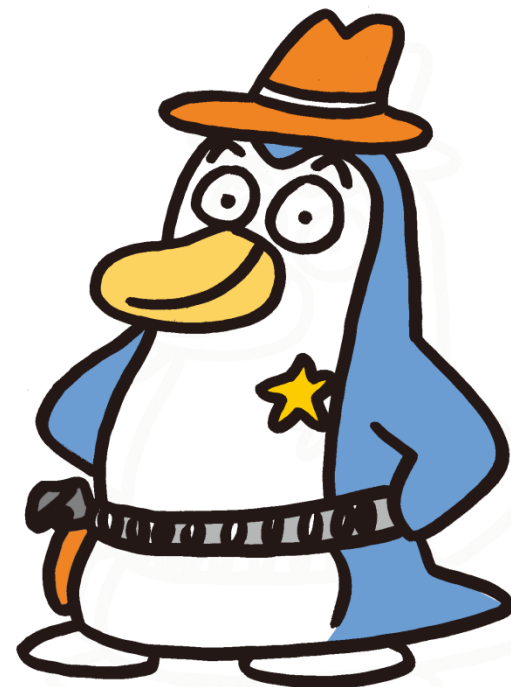
# 9.10で使える!! TOMOYO Linux

## 入門編

TOMOYO Linux Project

沼口大輔

d.numaguchi@gmail.com



# TOMOYOについて

- 2003年に「使いこなせて安全」なLinuxを目指して開発開始
- 2005年11月にOSSとして公開
  - <http://tomoyo.sourceforge.jp/>
- 2009年6月にLinuxカーネル2.6.30で採用
- 今はメインライン版(2系)とフル機能版(1系)が存在
- Ubuntu9.10以降から2系が使えるように
  - 経緯についてはThinkITの記事を  
<http://thinkit.jp/article/979/1/>

# TOMOYO Linuxの特徴

- 「**パス名ベース**」のアクセス制御
  - ポリシーの記述内容が理解しやすい
  - ポリシー編集も簡単に行える
- 「**自動学習**」機能
  - 利用する機能やサービスを実行するだけ
  - システムの起動から終了まで、必要なアクセス許可を自動的に収集
  - 自分のシステムを理解、把握するためにも活用

# TOMOYOができること

- **ファイルアクセス制御**

- プログラムがアクセスしたファイルを記録できます

- 読み込み
- 書き込み
- 実行

- 今後はネットワーク制御ができるように

- IPアドレス
- ポート番号



# 導入するメリット

- 被害の局所化
  - ポリシー設定ができていれば、被害を限定
- 不正アクセスの検知
  - ポリシー違反の監視により検知可能
- 誤操作防止
- 情報漏洩の可能性を軽減
  - ポリシーで許可されない操作は失敗

# 9.10でTOMOYO環境をつくる

## 1. カーネルパラメータ設定

- ① `/etc/default/grub`に  
「`GRUB_CMDLINE_LINUX="security=tomoyo"`」  
を追加
- ② 「`sudo update-grub`」を実行
- ③ 再起動

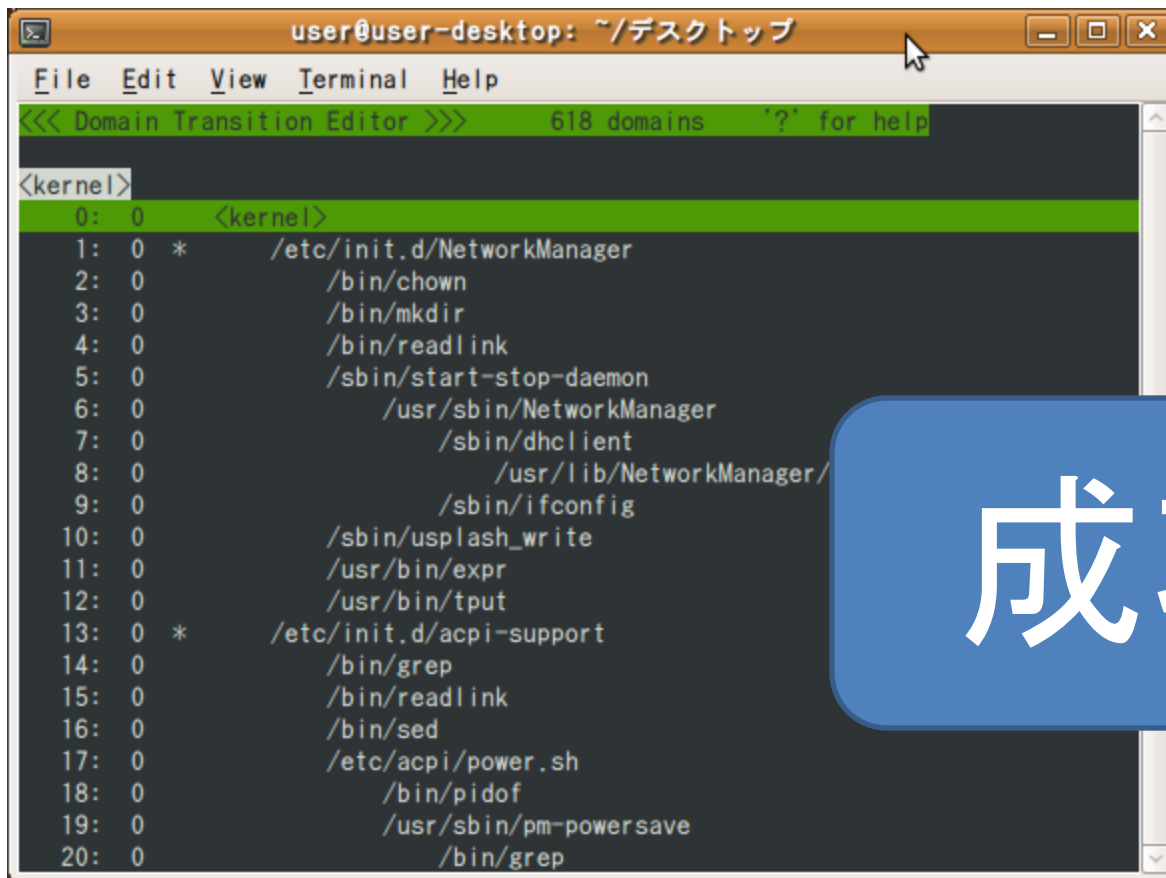
## 2. ツールインストール

- ① 「`sudo apt-get install tomoyo-ccstools`」を実行

ThinkITでhitoさんが書かれた記事(<http://thinkit.jp/article/979/1/>)の抜粋です。

# 確認

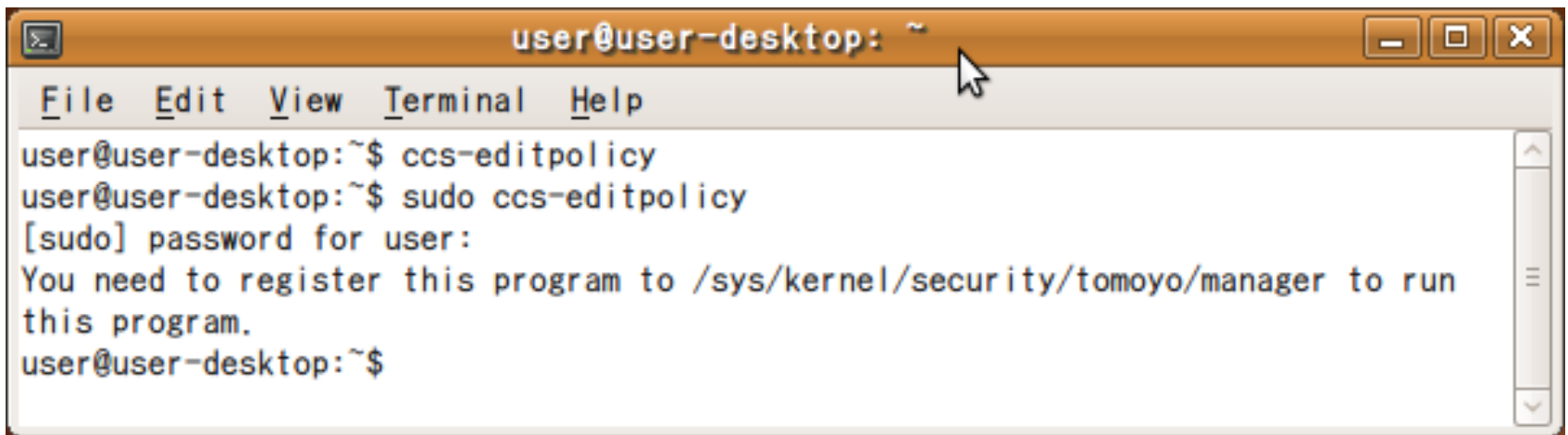
- 「sudo ccs-editpolicy」を実行



```
user@user-desktop: ~/デスクトップ
File Edit View Terminal Help
<<< Domain Transition Editor >>> 618 domains '?' for help
<kernel>
0: 0 <kernel>
1: 0 * /etc/init.d/NetworkManager
2: 0 /bin/chown
3: 0 /bin/mkdir
4: 0 /bin/readlink
5: 0 /sbin/start-stop-daemon
6: 0 /usr/sbin/NetworkManager
7: 0 /sbin/dhclient
8: 0 /usr/lib/NetworkManager/
9: 0 /sbin/ifconfig
10: 0 /sbin/usplash_write
11: 0 /usr/bin/expr
12: 0 /usr/bin/tput
13: 0 * /etc/init.d/acpi-support
14: 0 /bin/grep
15: 0 /bin/readlink
16: 0 /bin/sed
17: 0 /etc/acpi/power.sh
18: 0 /bin/pidof
19: 0 /usr/sbin/pm-powersave
20: 0 /bin/grep
```

# 確認

- エラーメッセージ↓が表示された



```
user@user-desktop: ~  
File Edit View Terminal Help  
user@user-desktop:~$ ccs-editpolicy  
user@user-desktop:~$ sudo ccs-editpolicy  
[sudo] password for user:  
You need to register this program to /sys/kernel/security/tomoyo/manager to run  
this program.  
user@user-desktop:~$
```

- /etc/tomoyoがあるか確認します



# /etc/tomoyoの確認

- /etc/tomoyoがディレクトリが存在しない場合
  - ① 「`sudo mv /etc/ccs /etc/tomoyo`」を実行
  - ② または  
「`sudo /usr/lib/ccs/tomoyo_init_policy.sh`」実行
  - ③ 再起動
- /etc/tomoyoがディレクトリが存在する場合
  - /etc/tomoyo以下にconfファイルあることを確認
  - カーネル起動時のオプションを確認

# デモ

- 9.10のTOMOYOで、どんなことができるか実際に確認していきましょう。
- Gnome Terminalの動作をチェック



# TOMOYOの情報

- TOMOYOの使い方
  - ホームページ
    - <http://tomoyo.sourceforge.jp>
  - TOMOYO Linuxの世界(参考)
    - 技術評論社Software Design誌での連載を掲載
    - <http://tomoyo.sourceforge.jp/wiki/?WorldOfTomoyoLinux>
- イベント情報
  - はてなキーワード
    - <http://d.hatena.ne.jp/keyword/TOMOYO%20Linux>
- 質問など
  - メーリングリスト
  - 掲示板

ありがとう  
ございました