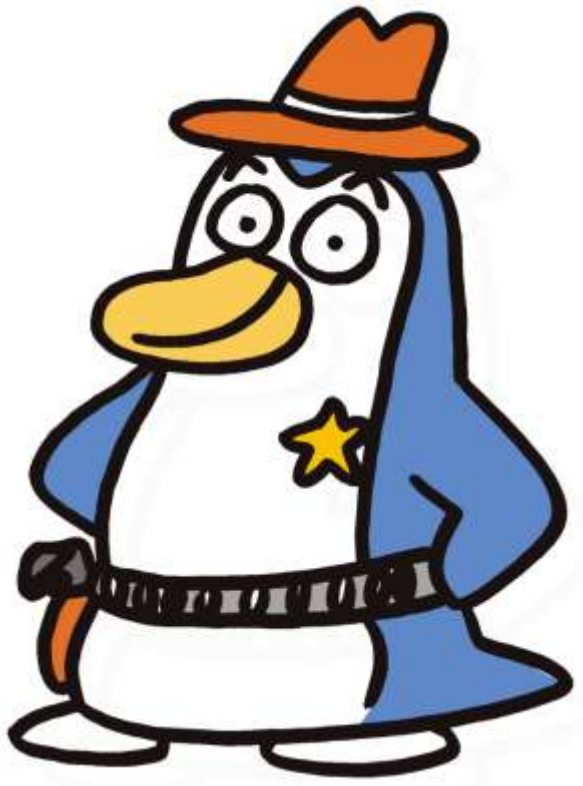
変える力を、ともに生み出す。
NTT DATAグループ

現場で使える！
TOMOYO Linux

2009.9.12
株式会社NTTデータ
沼口大輔
numaguchid@nttdata.co.jp

TOMOYO Linuxとは

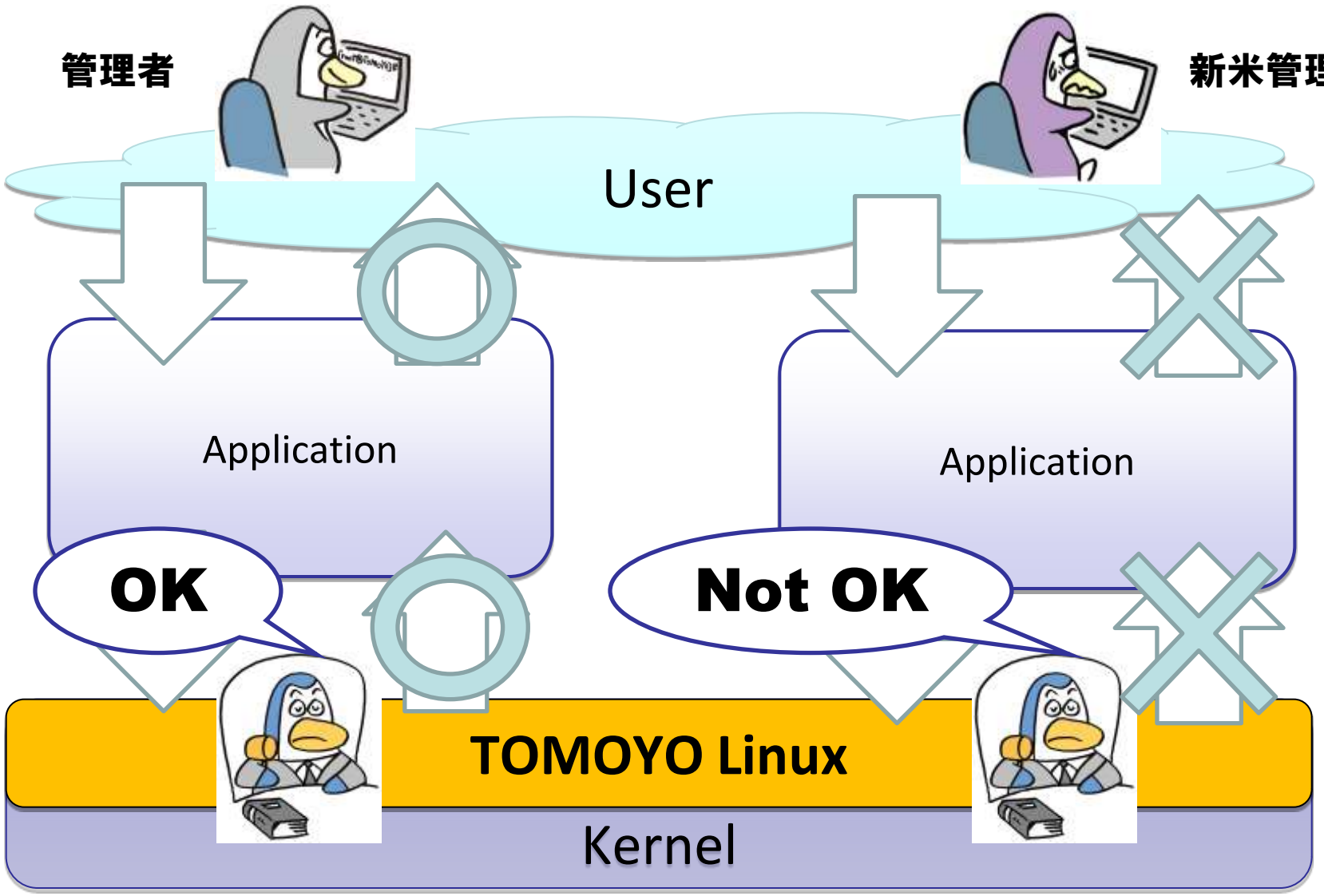
- 振る舞い志向のシステム解析及び保護ツール
  - 「使いこなせて安全」を目指して開発
  - 「セキュアOS」と言われるものの１つ
- ２つのバージョンを提供中
  - メインライン版（２系）
  - フル機能版（１系）



できること

- **システムを保護する**
  - 外部からの攻撃を防ぐ
    - Webサーバの改ざん防止
  - 内部の事故を防ぐ
    - 誤操作によるシステム障害対策
- **システムの振る舞いを解析**
  - プログラムの開発
  - システムのマニュアル作成

TOMOYOの動きイメージ



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」だけシステム動作を記録
  - システムの動作に必要なアクセス許可内容を自動的に設定
  - 自分のシステムを理解、把握するためのツールとしても活用可能

TOMOYO Linuxの導入メリット

- 被害の局所化
  - ポリシーが適切に行われていれば、被害を限定できる
- 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ていない操作は失敗

２つのバージョンを提供しています

- メインライン版（２系）
  - フル機能版のサブセット
  - Linux カーネル2.6.30から利用可能
- フル機能版（１系）
  - 2005年から公開している独自版
  - Linux カーネル2.4 / 2.6でパッチ適用で利用可能
  - 多くのディストリビューションに対応
    - Red Hat Enterprise Linux 3～
    - Ubuntu 6～
    - Debian 3.1～
    - Turbolinux 11 Server （商用サポート有）

TOMOYOの主な機能

TOMOYO Linuxの機能	メインライン版（２系）	フル機能版（１系）
ファイルアクセス制御 （読み・書き・実行・作成・削除）	○	○
ファイルアクセス制御 （属性・名前空間・ioctl）	×	○
ネットワークアクセス制御	×	○
ケイパビリティの制限	×	○
パラメータ（環境変数、引数（argv）、UID、GIDなど）の制限	×	○
アクセスログ	×	○

導入に適しているところ

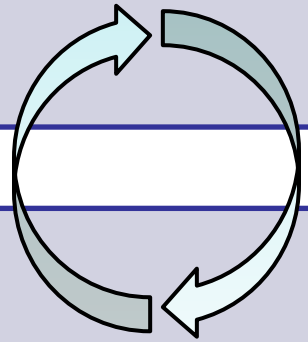
- 運用管理を委託しているところ
  - root権限は渡すけど
    必要なコマンドだけ操作させたい
  - 誤操作を防止したい

  など
- 特定の用途に特化したもの
  - サーバ
    - Webサーバ、メールサーバ、FTPサーバ…
  - 専用端末
    - メニューのオーダー端末、 ATM…

利用までの流れ

導入
- カーネルのインストール（フル機能版（１系）のみ）
- ユーティリティのインストール

学習
- システムを動かして学習
- 学習結果をポリシーとして自動作成



解析
- 自動作成されたポリシーの確認
- 確認した結果をもとにポリシーを修正

運用
- TOMOYO Linuxの制御機能を有効にして運用開始

Ubuntu 9.10の場合

- 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
- ツールのインストール
  - ① 「sudo apt-get install tomoyo-ccstools」を実行
  - ② 再起動

2009/7/9にThinkITでUbuntu Japanese Team のhito さんが書かれた記事(http://thinkit.jp/article/979/1/)からの抜粋です。

動作確認

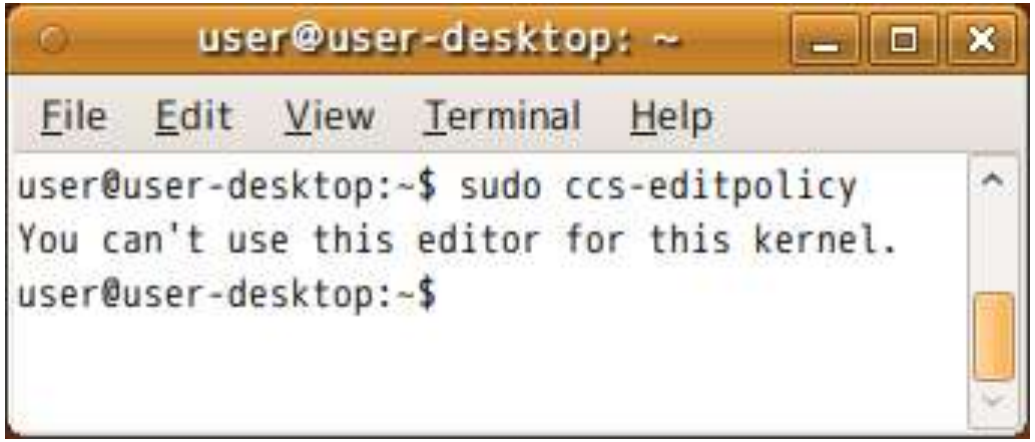
- 「**sudo ccs-editpolicy**」を実行

```
<<< Domain Transition Editor >>>      666 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/nm-dhcp-client.action
    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
   21:   0                       /bin/mkdir
```

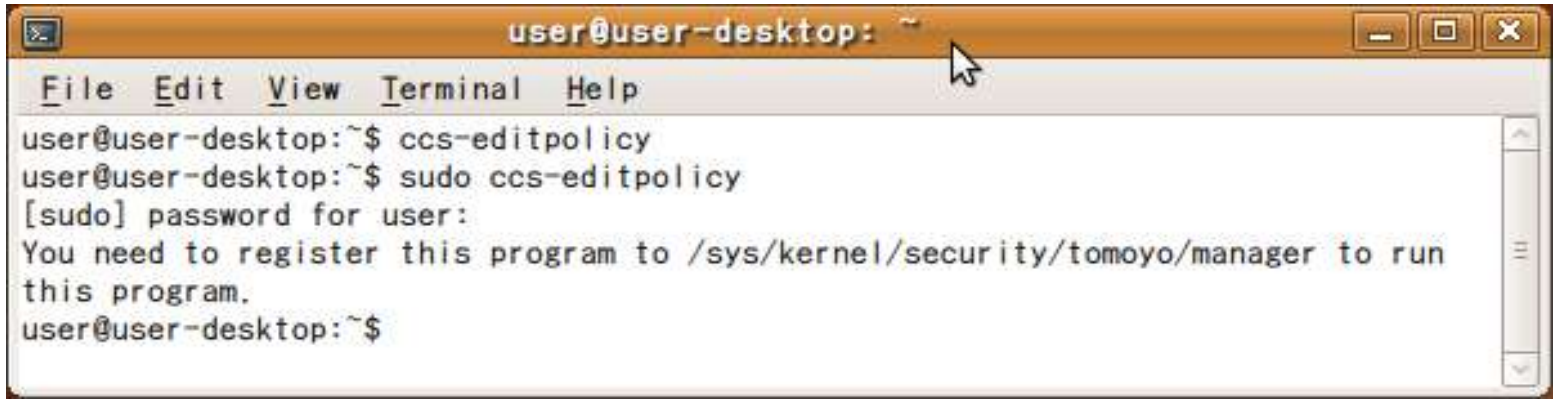
画面が表示されれば成功

エラーが表示された1

- 

  - You can’t use this editor for this kernel.
- GRUB設定を確認！！
  - /etc/default/grub
  - 「sudo update-grub」を実行

エラーが表示された2

- 

  - **You need to register this program to /sys/kernel/security/tomoyo/manager to run this program.**
- **/etc/tomoyoを確認**

/etc/tomoyoの確認

- /etc/ccsディレクトリだけがある場合
  - 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
    「sudo /usr/lib/ccs/tomoyo_init_policy.sh」
    を実行
  - カーネル起動時のオプションを確認

ポリシー（設定）について

- ４種類のテキストファイルで定義
- /etc/tomoyoに格納される

構成要素	概要	定義ファイル
ドメインポリシー	システムの振る舞い(アクセス許可)を定義	domain_policy.conf
例外ポリシー	ドメインポリシーの例外を定義	exception_policy.conf
プロファイル	制御レベルを定義	profile.conf
マネージャポリシー	ポリシー管理ができるプログラムを定義	manager.conf

システム稼働中のポリシー

- /sys/kernel/security/tomoyo/ ディレクトリに格納

構成要素	定義ファイル
ドメインポリシー	domain_policy
例外ポリシー	exception_policy
プロファイル	profile
マネージャポリシー	manager

ポリシーの管理

- 「ccs-editpolicy」を使う
  - /sys/kernel/security/tomoyo/にあるポリシーを編集
  - リモートマシンのポリシー管理も対応
    - SSHから操作可能
- 管理対象
  - ポリシーの修正
  - 動作モード設定
  - メモリーの上限設定

ドメインについて

- ドメインとは
  - 全てのプロセスが、それぞれ1つのドメインに属する
  - 同じプログラムでも呼び出し元が異なれば別ドメイン
  - 例
    - /sbin/getty → /bin/login → /bin/bash

      ⇒　「/sbin/getty /bin/login /bin/bash」ドメイン

    - /usr/bin/ssh → /bin/login → /bin/bash

      ⇒　「/usr/bin/ssh /bin/login /bin/bash」ドメイン

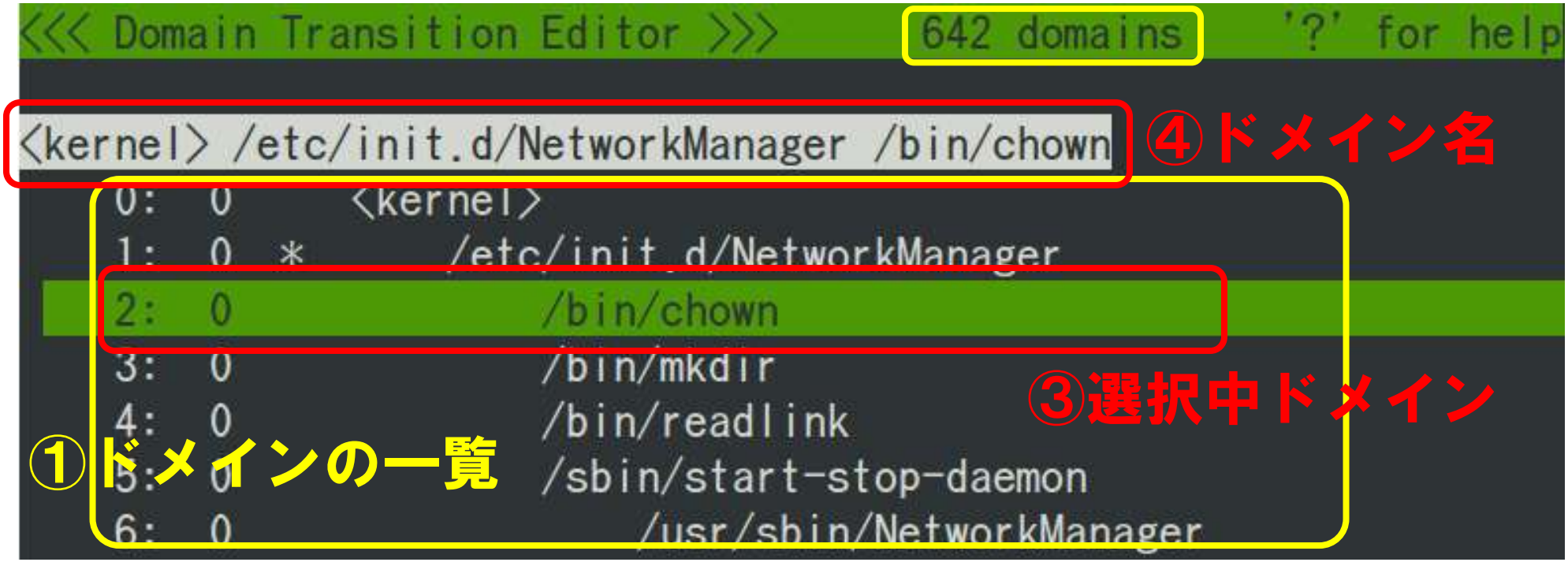
ドメインについて

- ドメイン遷移とは
  - プログラムを実行するたびに、異なるドメインへ遷移
  - 例
    - /sbin/getty → /bin/login → /bin/bash で実行すると
      - /sbin/gettyを実行中
        - »「/sbin/getty」ドメイン
      - /sbin/getty が /bin/login を実行
        - »「/sbin/getty /bin/login」ドメインに遷移
      - /bin/login が /bin/bash を実行
        - »「 /sbin/getty /bin/login /bin/bash」ドメインに遷移

ドメインメイン遷移画面

ドメインメイン遷移画面

②ドメインの数



④ドメイン名

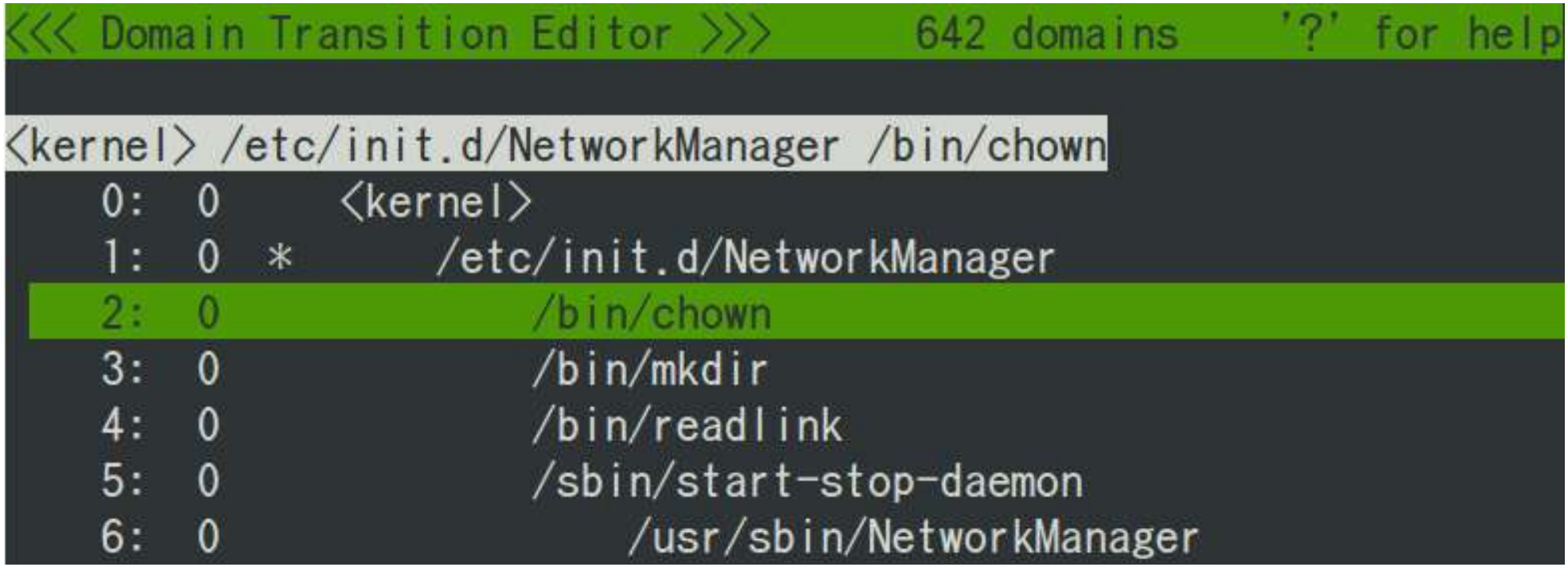
③選択中ドメイン

①ドメインの一覧

ドメイン遷移画面の読み方

- <kernel>
  - 全てのドメインの基点でカーネルが属するドメイン
- /bin/chownドメイン
  - 正しくは
    <kernel> /etc/init.d/NetworkManager /bin/chown
    というドメイン
  - /bin/chownは、カーネルから起動された
    /etc/init.d/NetworkManagerが起動したもの
- ドメイン遷移を見ることで、どんな順番でプログラムが実行されたかが確認できる

ドメインポリシーを見る



カーソルをポリシーを
見たいドメインに合わせて [Enter]

ドメインポリシー

- ドメイン単位でアクセス許可設定を定義

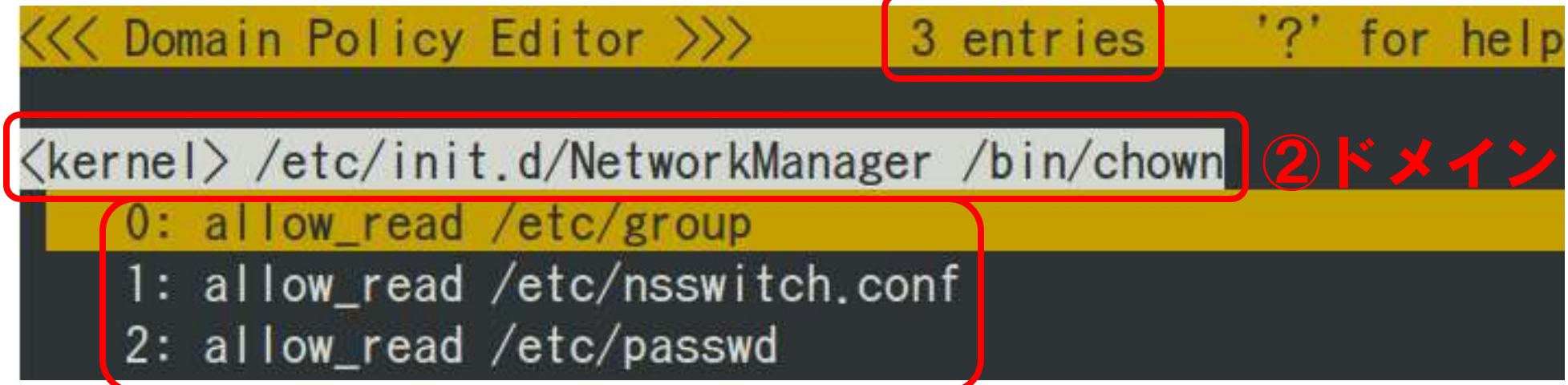
```
<<< Domain Policy Editor >>>      3 entries    '?' for help

<kernel> /etc/init.d/NetworkManager /bin/chown
    0: allow_read /etc/group
    1: allow_read /etc/nsswitch.conf
    2: allow_read /etc/passwd
```

[Enter] を押すとドメイン遷移画面に戻る

ドメインポリシー

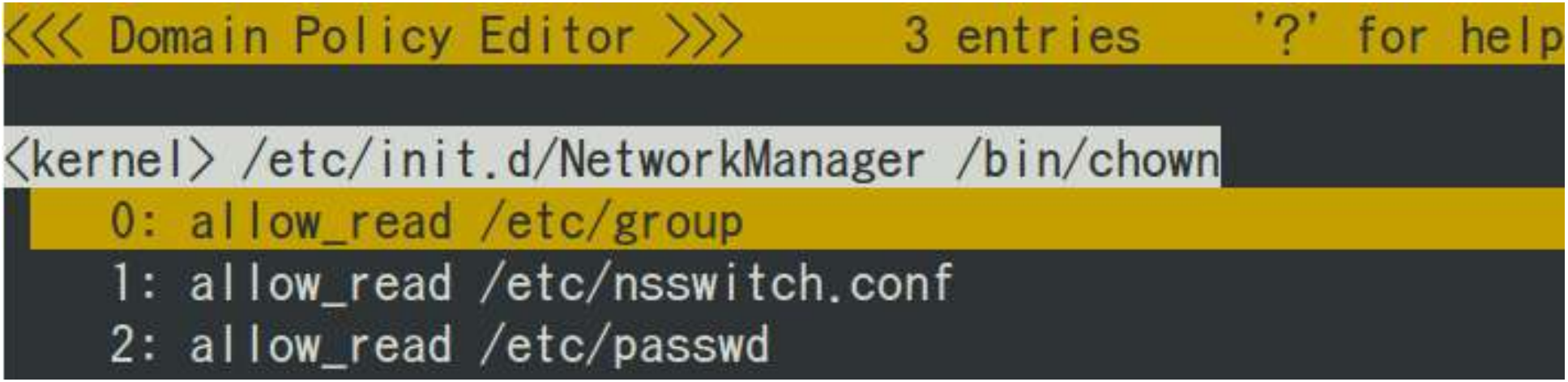
①許可リストの数



②ドメイン

③アクセス許可リスト

ドメインポリシーの読み方



- **<kernel> /etc/init.d/NetworkManager /bin/chownが、**
  - **/etc/group**
  - **/etc/nsswitch.conf**
  - **/etc/passwd**
- **ファイルを読込むのを許可**

設定できるアクセス許可

- ファイルの作成、読み書き、実行、切り詰めなど
  - allow_execute
  - allow_read
  - allow_write
  - allow_read/write
  - allow_create
  - allow_unlink
  - allow_mkdir
  - allow_rmdir
- 詳細は
  - http://tomoyo.sourceforge.jp/2.2/policy-reference.html#Policy_Files を参照

デモ

デモの内容

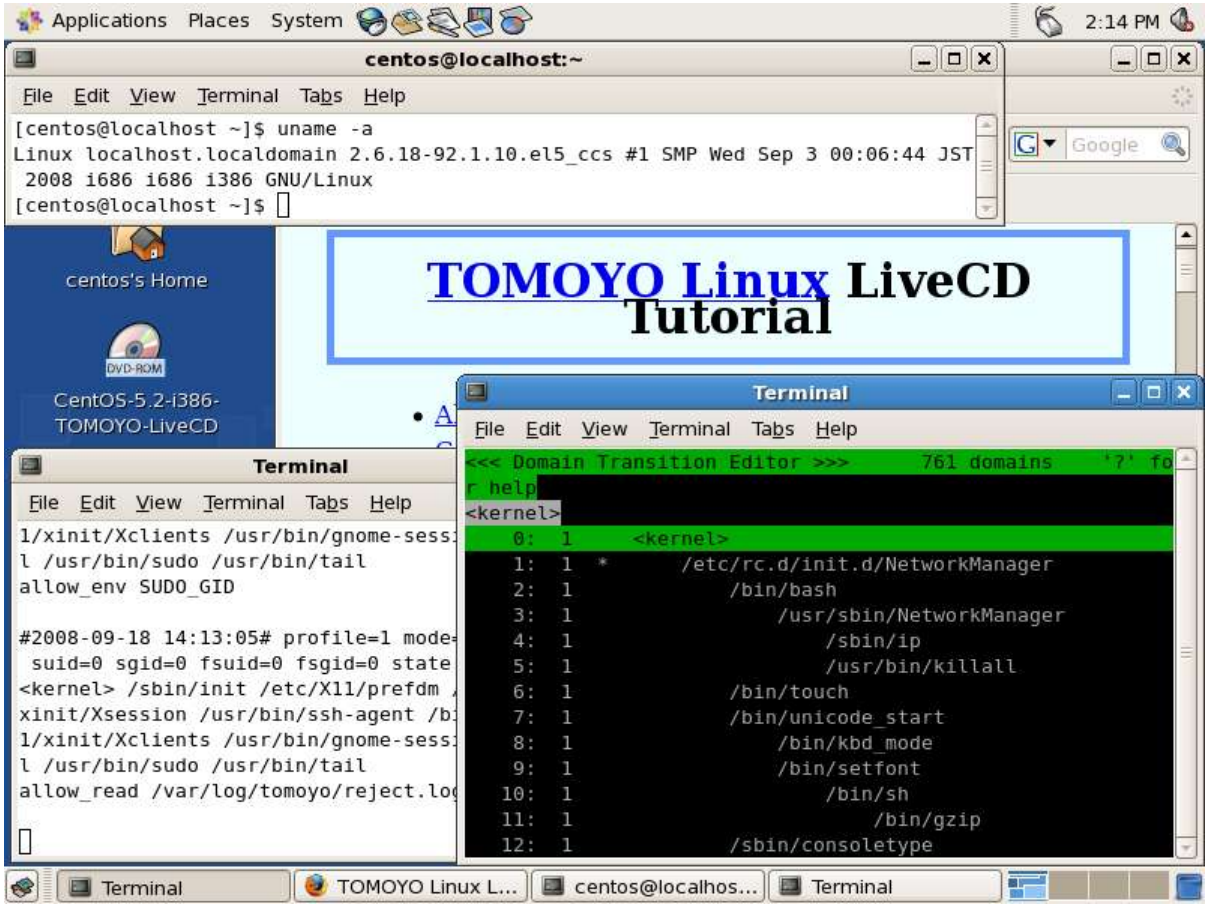
- SSHの動作制御
  - 学習させたコマンドだけ実行できる
    - リモートマシンにログインしコマンドを学習
    - TOMOYOの制御を有効にして、管理者ログイン
    - 学習したコマンドと学習しなかったコマンド実行
- 管理者の操作をWebサーバ管理操作に限定
  - SSHでのリモート管理で
    - サービスの起動
    - ログの確認

物足りない人へ・・・

フル機能版をどうぞ

フル機能版がLive CDで体験できます

- CentOSとUbuntuを使った
  フル機能版TOMOYO Linux Live CDを公開中
  - http://tomoyo.sourceforge.jp/wiki/?TomoyoLive



導入実績

■NPO日本ネットワークセキュリティ協会のWebサーバで稼働中

- 詳細な報告書が公開されています
- http://www.jnsa.org/result/2007/tech/secos/

■商用システム導入事例について資料を公開

- 日経BP主催Open Source Revolution!の講演資料です
- http://sourceforge.jp/projects/tomoyo/docs/osr20060515.pdf

TOMOYO Linuxの情報

- TOMOYO Linuxの導入、管理方法について
  - ホームページ
    - http://tomoyo.sourceforge.jp/
  - TOMOYO Linuxの世界（フル機能版（１系））
    - 技術評論社Software Design誌での連載記事を掲載
    - http://tomoyo.sourceforge.jp/wiki/?WorldOfTomoyoLinux
- イベント情報について
  - はてなキーワード
    - http://d.hatena.ne.jp/keyword/TOMOYO%20Linux

TOMOYO導入のお手伝いします

- 商用システムへの検証、ポリシー作成、運用など、お手伝いします。
  tomoyo-sale@kits.nttdata.co.jp
  まで、お問い合わせください。
- TOMOYOの技術的なご質問なども
  お気軽にお問い合わせください。

変える力を、ともに生み出す。

NTT DATAグループ