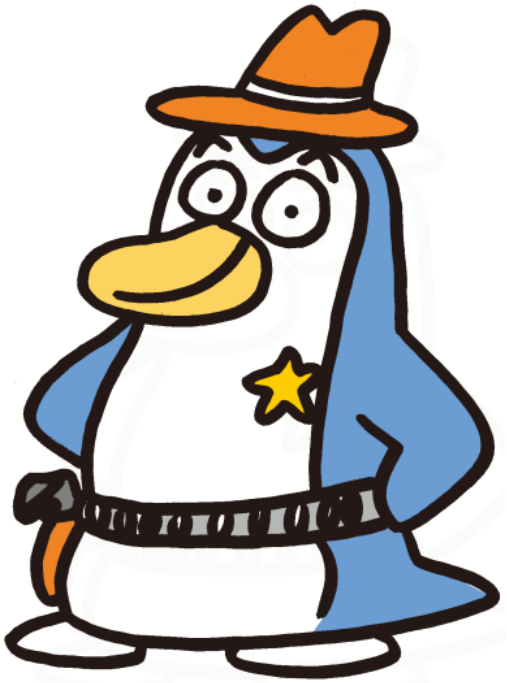
日本セキュアOSユーザ会
Japan Secure Operating System Users Group since 2007

「はじめてのTOMOYO Linux」

オープンソースカンファレンス 2009 Tokyo/Spring



2009年2月20日

沼口大輔
<numaguchid@nttdata.co.jp>

今日のお話

1.TOMOYO Linux 基礎知識

2.TOMOYO Linux の運用

3.デモ

基礎知識

セキュアOSとは

- 管理者をも「制限」できるOSのことです
- 技術的には
  - 「強制アクセス制御」(Mandatory Access Control)を実装したOSです。
- 標準機能/オプションの違いはあっても主要なOSではだいたい利用できるようになりました

セキュアOSの利点

- 不正アクセスを防ぐことができます
- 万一不正アクセスを受けても、被害を局所化できます
- 管理者の誤操作防止にも使うことができます
- 内部からの情報漏えいの可能性を軽減できます

但し、実現するには、適切な設定が重要です

TOMOYO Linuxとは

- 「使いこなせて安全」なLinuxを目指して、NTTデータが開発
- 2005年11月にOSSとして公開しました
- カーネルとユーティリティの２つから構成
- 主要なディストリビューション向けに、パッケージと導入手順書を公開しています

  http://tomoyo.sourceforge.jp/ja/1.6.x/analysis.html

普通のLinux

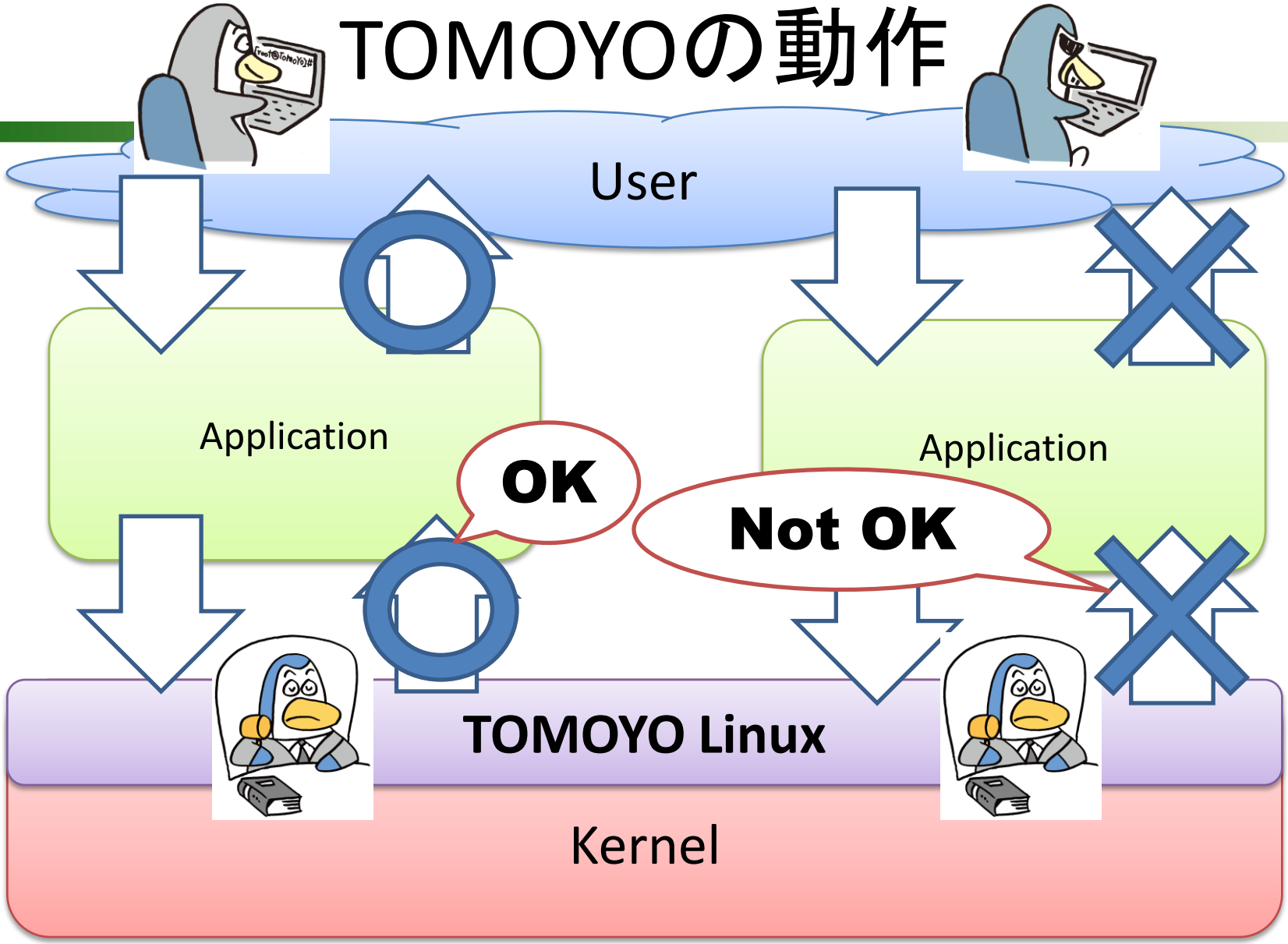
User

Application

Application

Kernel

TOMOYOの動作



ポリシーについて

- 「いい」、「わるい」を判断する設定をポリシーと呼びます
- TOMOYO Linuxのポリシー
  - 「ホワイトリスト方式」を採用
    - 必要なものを列挙します（それ以外は実行できません）
  - 「パス名」を使用
    - ファイル名やディレクトリ名をそのまま使います
  - テキストファイル
    - Emacs, viなどのエディタで編集できます

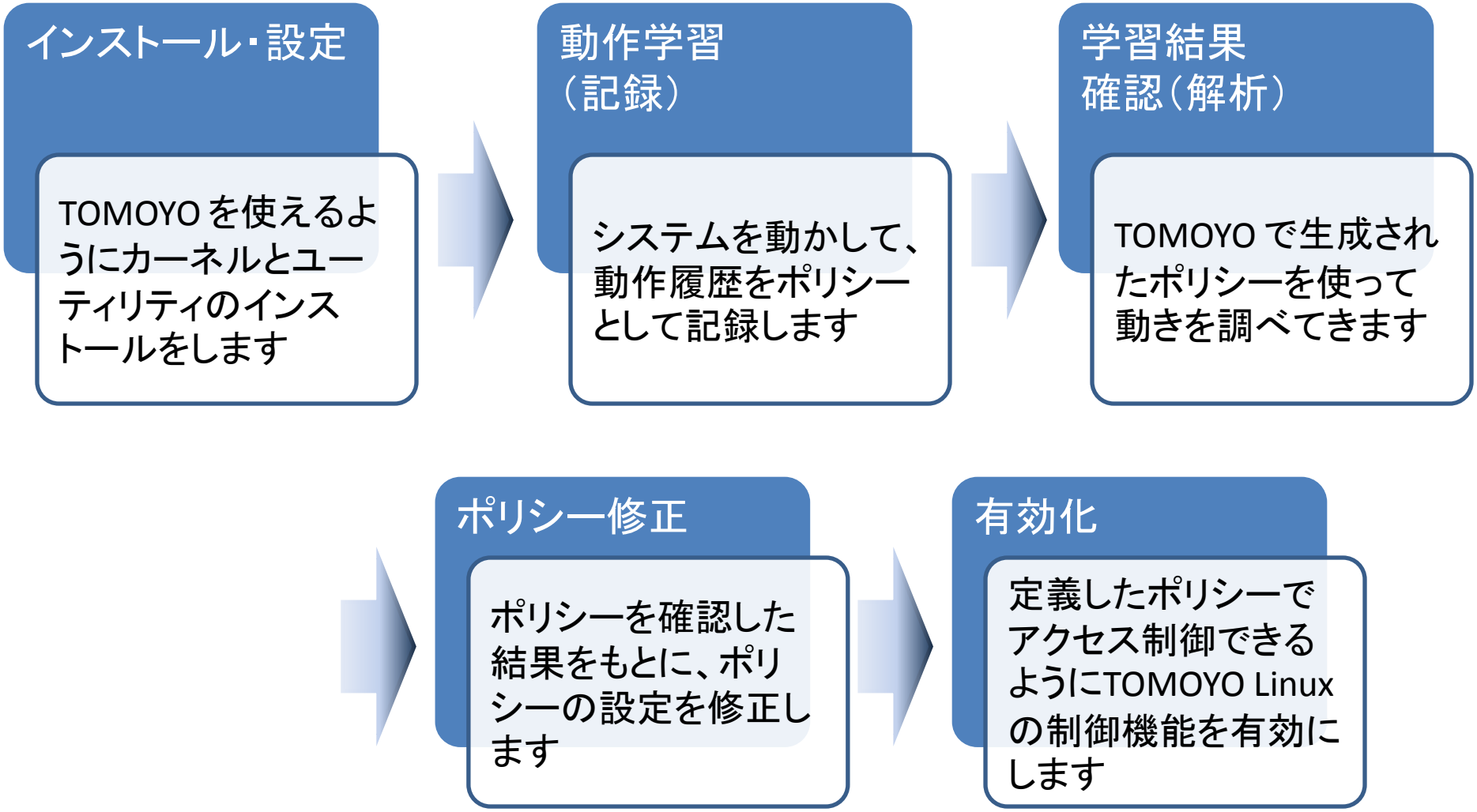
学習機能について

- ポリシーの作成に学習機能が使えます
  - 初期ポリシーを自動で作成
    - ポリシーをゼロから作る必要はありません
    - 自動学習機能が備わっており、プログラムを実行すると、その結果に基づいてポリシーが作成されます

学習する内容

- プロセスの起動履歴
  - プロセスを呼び出した親プロセス、親の親プロセス、さらにその親、・・・、をさかのぼって記録しています
- プロセスの振る舞い
  - 起動履歴ごとにプロセスがどんなファイルを読み出したのか、実行したのかなどの情報を学習しています

導入から運用までの流れ



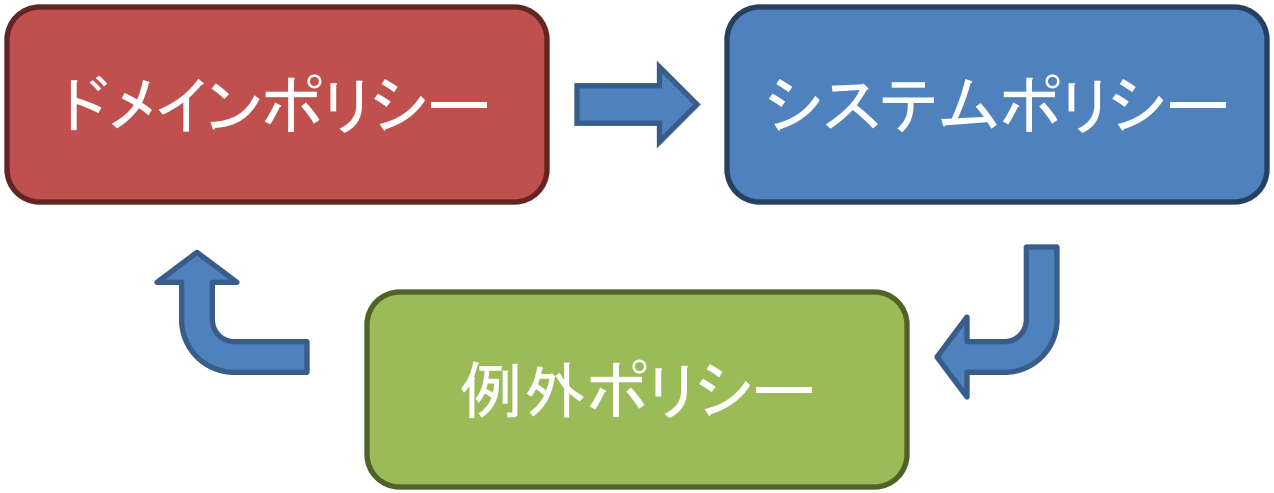
運用方法

ポリシーの管理方法

- ポリシーエディタを使います
- 主な機能
  - ポリシーの確認、変更
    - TOMOYOで使われる3種類のポリシーを扱います
      - » ドメインポリシー
      - » システムポリシー
      - » 例外ポリシー
  - 動作モードの切り替え
    - プログラム単位で、学習、強制の動作モードを設定します

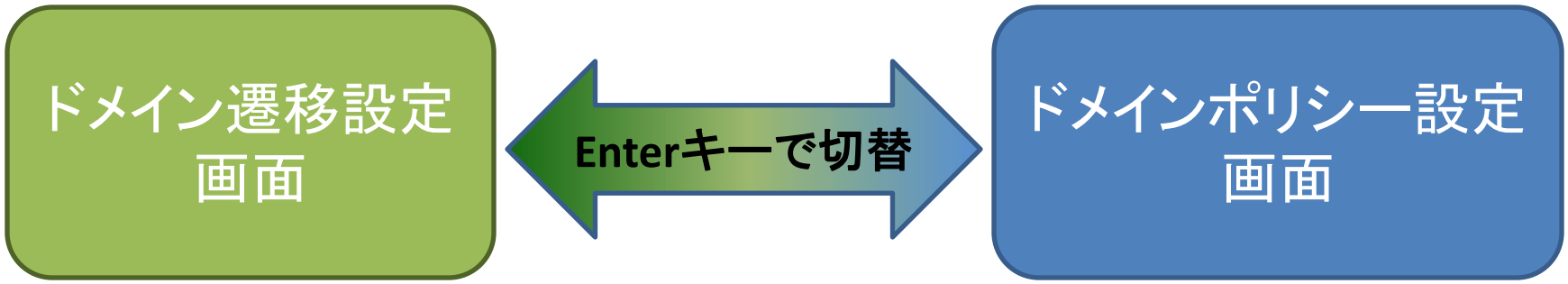
ポリシーエディタの使い方1

- ポリシーエディタ(ccs-editpolicy)では、ドメインポリシー、システムポリシー、例外ポリシーを設定・確認ができます。
- 各ポリシーへの切り替えは、[Tab]キーを使います。



ポリシーエディタの使い方2

- 次にプログラムの動きを見るときは、ドメイン遷移画面とドメインポリシー画面を切り替えて使います。
- ドメイン遷移画面でドメインを選択して、[Enter]キーを押すとポリシー設定画面に切り替わります。



ドメイン遷移画面の読み方

プロファイル
(動作モード)
0 : 無効
1 : 学習
2 : 確認
3 : 強制
※今回の設定です

```
0:  1     <kernel>
1:  1  *      /etc/rc.d/init.d/acpid    ドメイン
2:  1            /bin/bash
                       /usr/sbin/acpid ( -> 706 )
3:  1            /bin/touch
4:  1            /sbin/consoletype
```

読み下すと…

1. /etc/rc.d/init.d/acpidが実行され、
2. /etc/rc.d/init.d/acpidから/bin/bashが実行され、
3. /bin/bashから/usr/sbin/acpidが実行されている
4. /etc/rc.d/init.d/acpidから/bin/touchが実行されている。
5. /etc/rc.d/init.d/acpidからsbin/consoletypeが実行されている。

ドメインポリシー画面の読み方

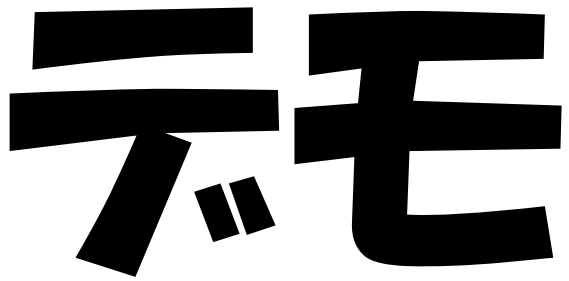
ドメイン

アクセス許可リスト

```
<kernel> /etc/rc.d/init.d/acpid
    0: allow_execute     /bin/bash
    1: allow_read        /bin/bash
    2: allow_execute     /bin/touch
    3: allow_read/write /dev/pts/¥$
    4: allow_read/write /dev/tty
    ...
```

読み下すと...

- **/etc/rc.d/init.d/acpid**には、以下のアクセスのみを許可する
  - /bin/bash、/bin/touchの実行
  - /bin/bashの読み込み
  - /dev/pts/¥$、/dev/ttyの読み書き
  - **...**



デモ

- ファイルアクセス、ネットワークアクセスについて、以下を実演します。
  1. 学習機能により初期ポリシーを作成する
  2. 初期ポリシーの内容を確認する
  3. 「強制」モードに切り替える
- デモ内容
  1. gcc（がどんなファイルにアクセスするか）
  2. ssh（がどんな通信をしているか）

TOMOYO Linuxの制御機能

- 今日ご紹介介したファイルアクセスやネットワークアクセス以外にも下記の制御が可能です
  1. ケイパビリティの利用
  2. シグナルの利用
  3. マウント機能
  4. chroot の利用

  など

詳細は下記を参照
http://tomoyo.sourceforge.jp/ja/1.6.x/policy-reference.html#profile

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
    - 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
- その他
  - 2ちゃんねる
    - http://pc11.2ch.net/test/read.cgi/linux/1212502041/

Q&A

- 質問があればご遠慮なく
- 展示ブースへもぜひお越しください

TOMOYOを使ってみてください

ありがとう
ございました