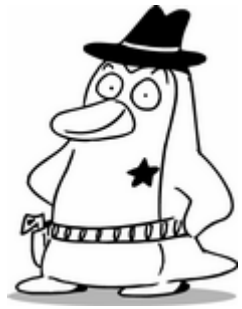
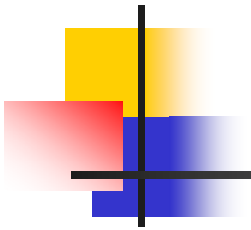
Linuxコンソーシアム 第24回セキュリティ部会

# TOMOYO Linuxの紹介



株式会社NTTデータ
基盤システム事業本部
オープンソース開発センタ

武田健太郎
takedakn@nttdata.co.jp



# TOMOYO Linux基礎知識

# TOMOYO Linuxとは

- NTTデータが開発したセキュリティ強化Linux
- 目指すところは…

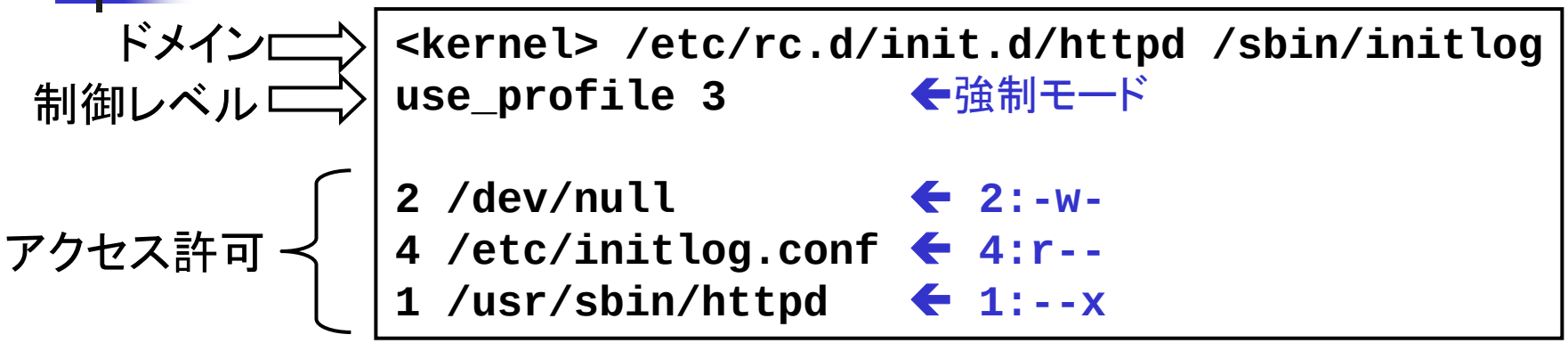
**使いこなせて安全なLinuxの実現**

- カーネルパッチ ＋ ツール群
- GPLで公開中
  - http://tomoyo.sourceforge.jp/

# TOMOYO Linuxの特徴

- パス名ベース
  - ➔ポリシーが読みやすい
- 階層構造のドメイン
  - ➔実行履歴でプロセスを区別する
- ドメインごとのアクセス制御レベル設定
  - ➔特定のデーモンの制御をON/OFFできる
- ポリシーの自動学習
  - ➔ポリシーの雛形を簡単に生成できる

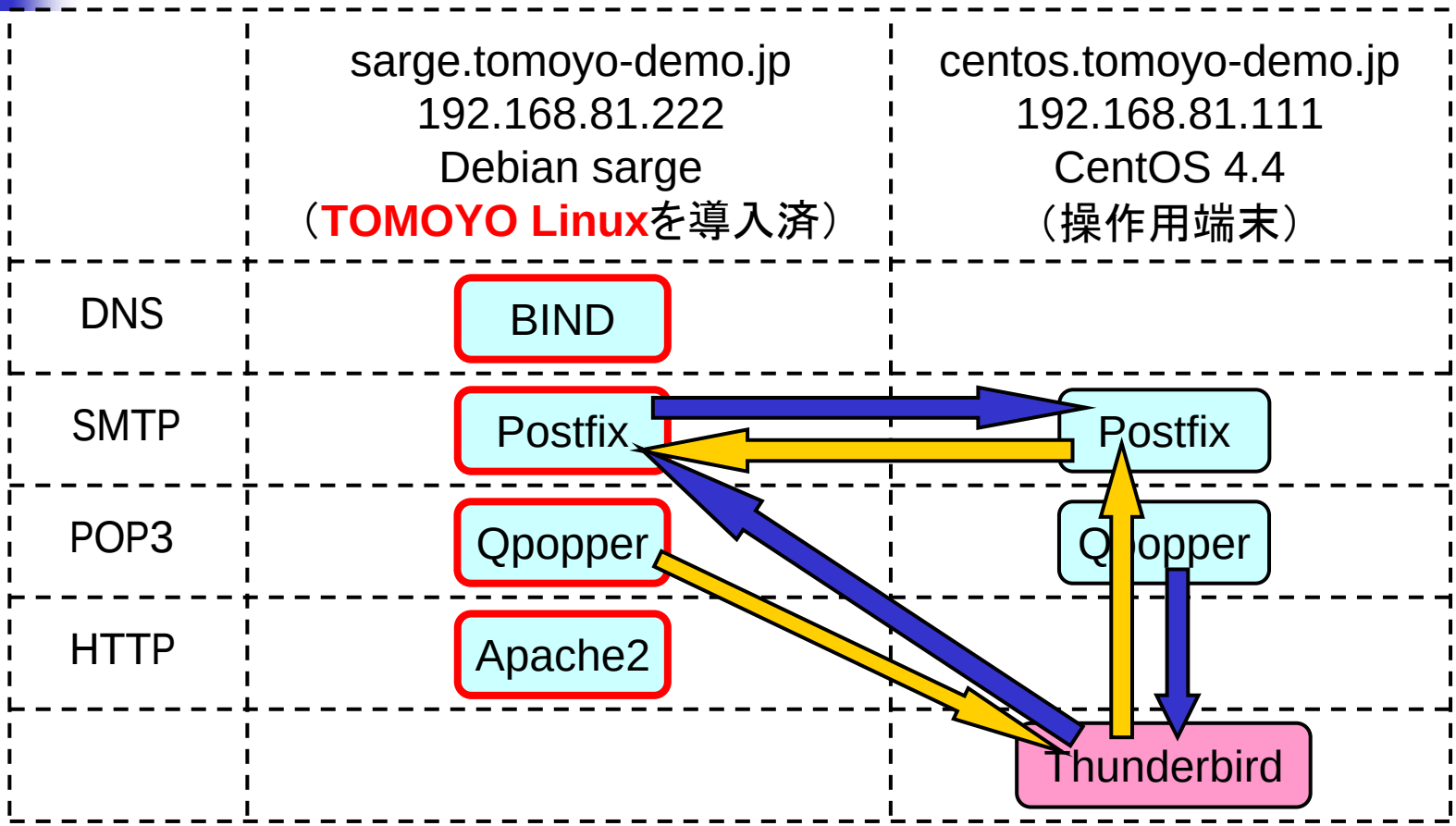
# TOMOYO Linuxのポリシーの例

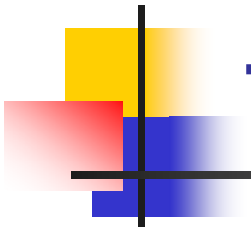



- /etc/rc.d/init.d/httpd から起動された /sbin/initlog には、以下のアクセスのみを許可する
  - /dev/null への書き込み
  - /etc/initlog.conf の読み込み
  - /usr/sbin/httpd の実行（=次のドメインへの遷移）

# デモ

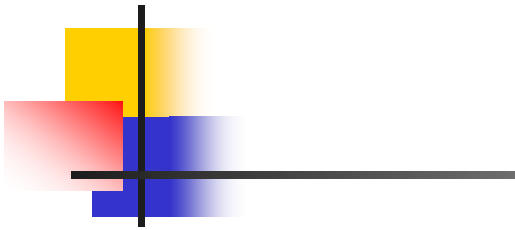
# 動作確認環境





# デモの内容

- デモ1: ログイン後の操作の学習と強制
  - 自動学習を実演し、ポリシーが簡単に生成できることを示す
- デモ2: TOMOYO Linuxで権限分割
  - 階層構造になっているポリシーを利用して、権限分割を実現できることを示す



# デモ1（TOMOYO Linuxの基本）
# ログイン後の操作の学習と強制

# デモ1
# ログイン後の操作の学習

- rootでログインし、学習モードに設定、以下の操作を学習させる
  - id
  - date
  - head -3 /etc/passwd
  - zsh
    - tail -3 /etc/passwd
    - exit
- 強制モードにして操作する
  - 学習した操作以外は拒否される

# デモ1のポイント
# ポリシーの自動学習

- 実際に行った操作に沿ってポリシーが自動生成される
- ログインシェルのzshと起動したzshはドメインが異なる

```
<kernel> /usr/sbin/sshd /bin/zsh
1 /usr/bin/id
1 /bin/date
1 /usr/bin/head
1 /usr/bin/zsh
```

```
<kernel> /usr/sbin/sshd /bin/zsh /bin/zsh
1 /usr/bin/tail
```

```
<kernel> /usr/sbin/sshd /bin/zsh /bin/zsh /usr/bin/tail
4 /etc/passwd
```

# デモ2（応用例）
# 管理者の権限分割

# デモ2
# 管理者の権限分割

- 管理者の役割を以下の2つに分割
  - メールサーバの管理者
    - Postfixの設定ファイルの編集
    - Postfixの再起動
  - Webサーバの管理者
    - Apacheの設定ファイルの編集
    - Webコンテンツの編集
    - Apacheの再起動
- rootとしてログイン後、異なる追加認証を抜けることで異なる役割に遷移

## デモ2のポイント (1/2)

# ドメイン階層を利用した権限分割

# デモ2のポイント (2/2)
# 権限分割を実現するポリシー

```
<kernel> /usr/sbin/sshd /bin/zsh

1 /bin/auth1
1 /bin/auth2
```

```
<kernel> /usr/sbin/sshd /bin/zsh /bin/auth1 /bin/zsh

1 /usr/bin/vi
1 /etc/init.d/postfix
```

```
<kernel> /usr/sbin/sshd /bin/zsh /bin/auth2 /bin/zsh

1 /usr/bin/vi
1 /etc/init.d/apache2
```

# おわりに

- TOMOYO Linuxを使ってみたい
  - ➔Software Design 2007年1月号～
    今日から使えるセキュアOS
    「TOMOYO Linuxの世界」
- TOMOYO Linuxの実装に興味がある
  - ➔技術評論社「ネットワークセキュリティExpert 5」
    「TOMOYO Linuxの秘密」

- TOMOYO Linux Wiki
  - http://tomoyo.sourceforge.jp/wiki/
- メーリングリスト
  - http://lists.sourceforge.jp/mailman/listinfo/tomoyo-users