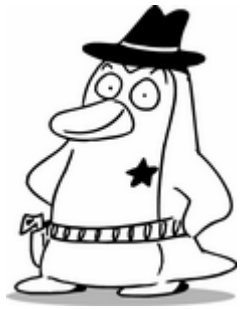
YLUG 第72回 カーネル読書会
TOMOYO Linux Night

TOMOYO Linux
機能紹介＆デモ

TOMOYO Linux Project

武田健太郎



TOMOYO Linuxって？

- NTTデータが開発したセキュリティ強化Linux
  - 「使いこなせて安全なLinux」の実現
- カーネルパッチ ＋ ツール群
  - メジャーなディストロには対応
  - 非LSM (Linux Security Module)
    - この話は後ほど…
- 2005/11/11よりGPLで公開中
  - http://tomoyo.sourceforge.jp/
  - 最新バージョンは1.3.1

TOMOYO Linuxの特徴は？

- パス名ベースのポリシー
  - プログラムやアクセス対象のファイルを絶対パスで表記するため読みやすい
- ポリシーの自動学習
  - 「学習モード」にして操作することで、自動的にポリシーを生成
- 階層的なドメイン
  - プログラムの実行のたびにドメイン遷移
  - プロセスツリーがドメイン遷移構造に対応する

ポリシーって？ ドメインって？

- ポリシー＝（ドメイン＋制御モード＋アクセス許可）×N
  - すべてのプロセスはいずれか1つのドメインに属する
  - アクセス許可に記述されていないアクセスは、制御モードに応じて許可or学習or拒否される

ドメイン
```
<kernel> /etc/rc.d/init.d/httpd /sbin/initlog
```
制御モード
```
use_profile 3          ← 強制モード
```
アクセス許可
```
2 /dev/null            ← 2:-w-
4 /etc/initlog.conf    ← 4:r--
1 /usr/sbin/httpd      ← 1:--x
```

読み下すと…

/etc/rc.d/init.d/httpdから起動された**/sbin/initlog**には
- **/dev/null**への書き込み
- **/etc/initlog.conf**の読み込み
- **/usr/sbin/httpd**の実行

のみを許可し、それ以外のアクセスは拒否する

どうやってる？

- execve(2)をフック
  - execveのたびにドメイン遷移
  - 各プロセスの持つ自ドメインの情報を更新
    - sched.hのtask_structにドメイン情報を付加してある
- open(2)をフック
  - 「ファイルを開いてよいか」をポリシーからチェック
    - アクセス拒否なら-EPERMを返す

open(2)の他にも、ケイパビリティやネットワーク関連のシステムコールもフックしており、アクセス制御できます

実際にTOMOYO Linuxの動きをお見せしましょう

デモ1:ログイン後の操作の学習と強制

- rootでSSHログイン後、学習モードにして以下の操作を学習させる
  - id
  - date
  - head -3 /etc/passwd
  - zsh
    - tail -3 /etc/passwd
    - exit
- 強制モードにすると、学習モードで行った操作以外が拒否されます

デモ1:ポイント

- 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
```

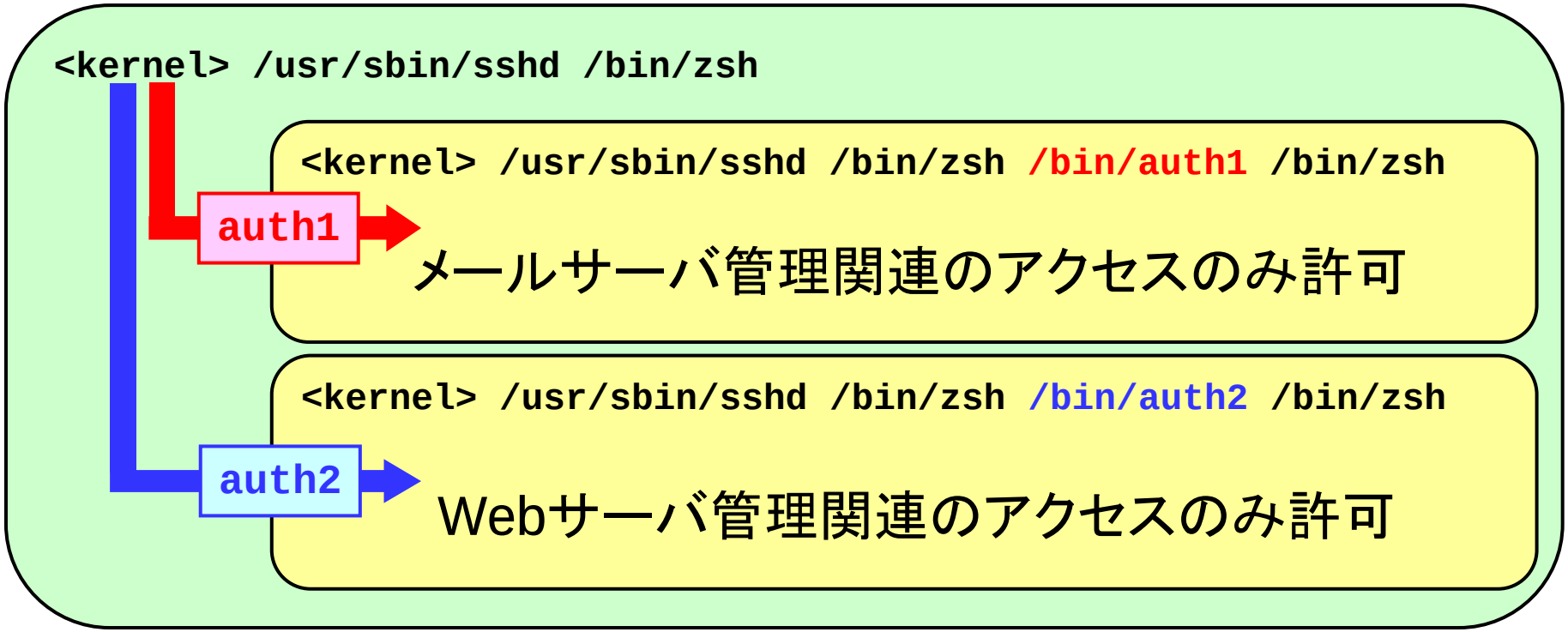
```
<kernel> /usr/sbin/sshd /bin/zsh /bin/zsh
1 /usr/bin/tail
```

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

デモ2:ドメインの階層構造を利用した権限分割

- 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:権限分割を実現するポリシー（1/2）



デモ2:権限分割を実現するポリシー（2/2）

```
<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
```
← Postfixの起動スクリプト

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

1 /usr/bin/vi
1 /etc/init.d/apache2
```
← Apacheの起動スクリプト

おわりに

- TOMOYO Linux 1.3.2 まもなくリリース予定
  - パス名をグループ化するマクロ機能
  - ドメイン遷移をさらに詳細に制御する機能
- TOMOYO Linuxの実装レベルの解説
  - ネットワークセキュリティExpert 5
    「TOMOYO Linuxの秘密」
- TOMOYO Linuxの使用方法の解説
  - SoftwareDesign 2007年1月号～
    「TOMOYO Linuxの世界」
- TOMOYO Linux Wiki
  - http://tomoyo.sourceforge.jp/wiki/
- メーリングリスト
  - http://lists.sourceforge.jp/mailman/listinfo/tomoyo-users
  - http://lists.sourceforge.jp/mailman/listinfo/tomoyo-dev