オープンソースカンファレンス2008 Nagoya

TOMOYO Linuxのある暮らし
～Linuxの勉強からセキュリティ強化まで～

TOMOYO Linuxプロジェクト
http://tomoyo.sourceforge.jp/
武田健太郎

今日のおはなし

- TOMOYO Linuxの基本
- TOMOYO LinuxでLinuxの動きを勉強する
- TOMOYO LinuxでLinuxをセキュアにする
- LiveCDでTOMOYO Linuxを体験する

はじめまして、TOMOYO Linux

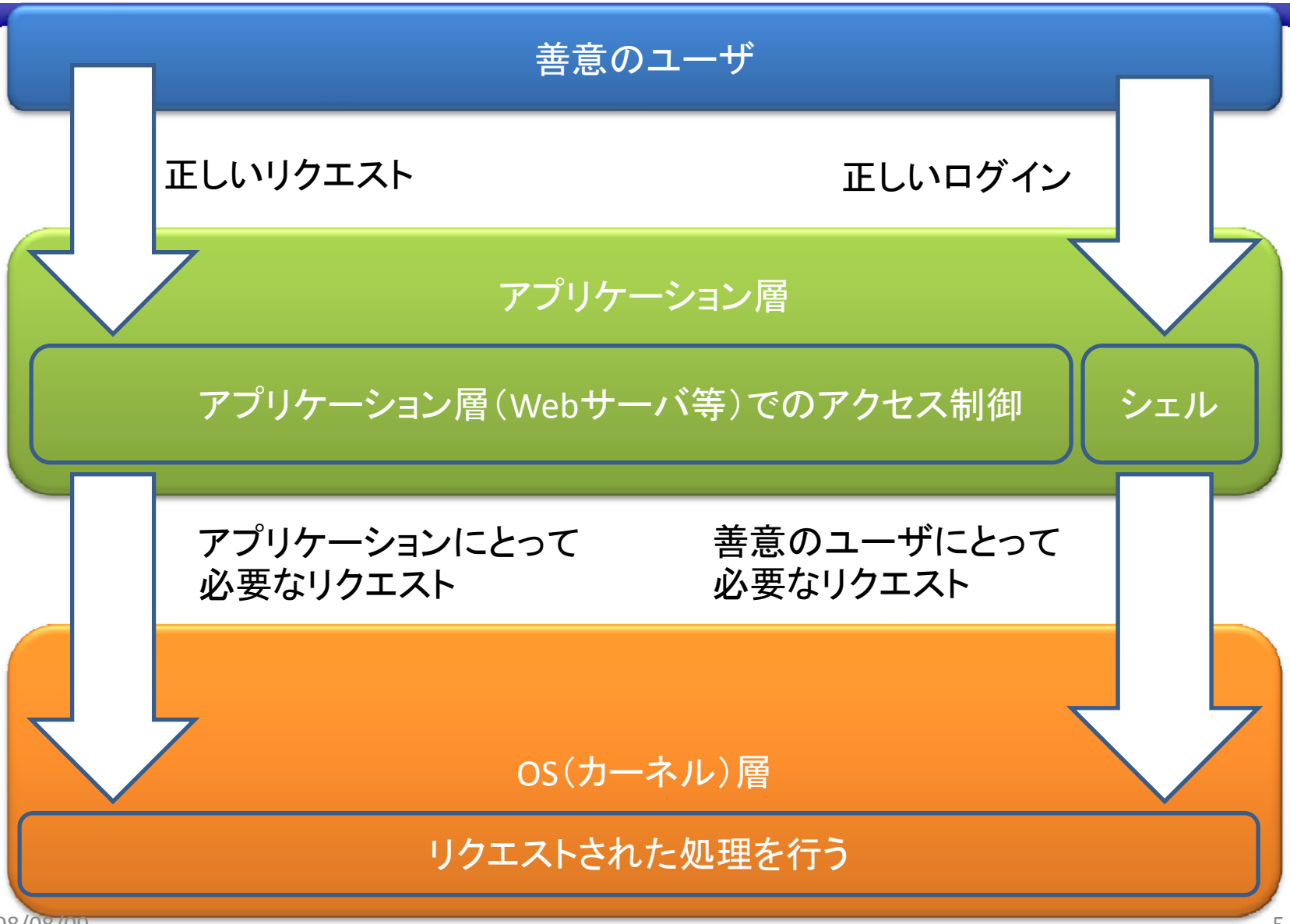
- TOMOYO LinuxはLinux向けのセキュリティ強化技術です
- カーネルレベルで「してよいこと」「わるいこと」を区別します
- 「簡単に使えて安全を保つ」工夫をしています

- ほかのLinux向けセキュリティ強化技術
  - SELinux, Smack, AppArmor, LIDS…

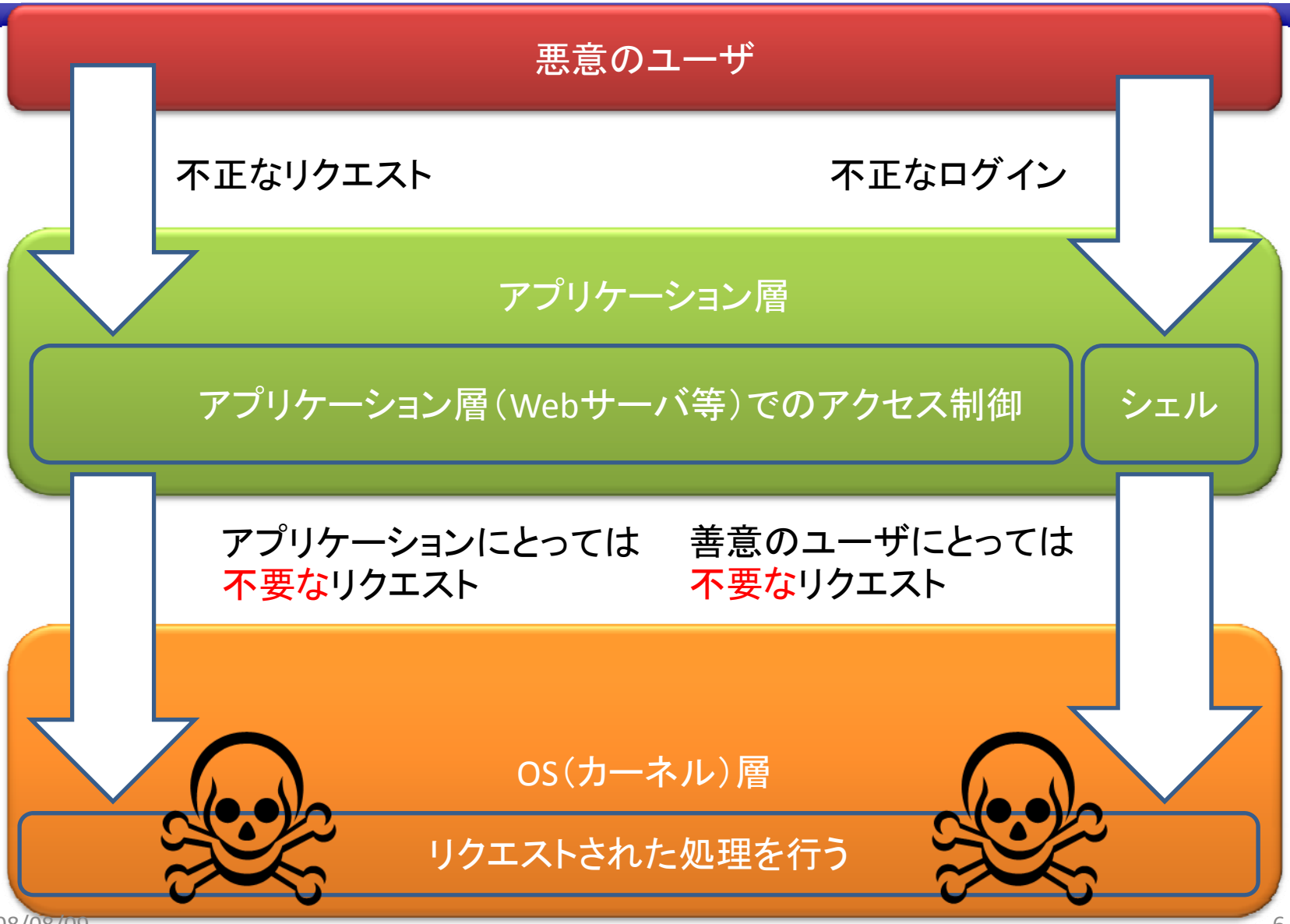
- ひとくちにセキュリティ強化っていっても、どういう風なセキュリティ強化なの？

  ➔カーネルレベルでのアクセスの可否のチェックを追加します

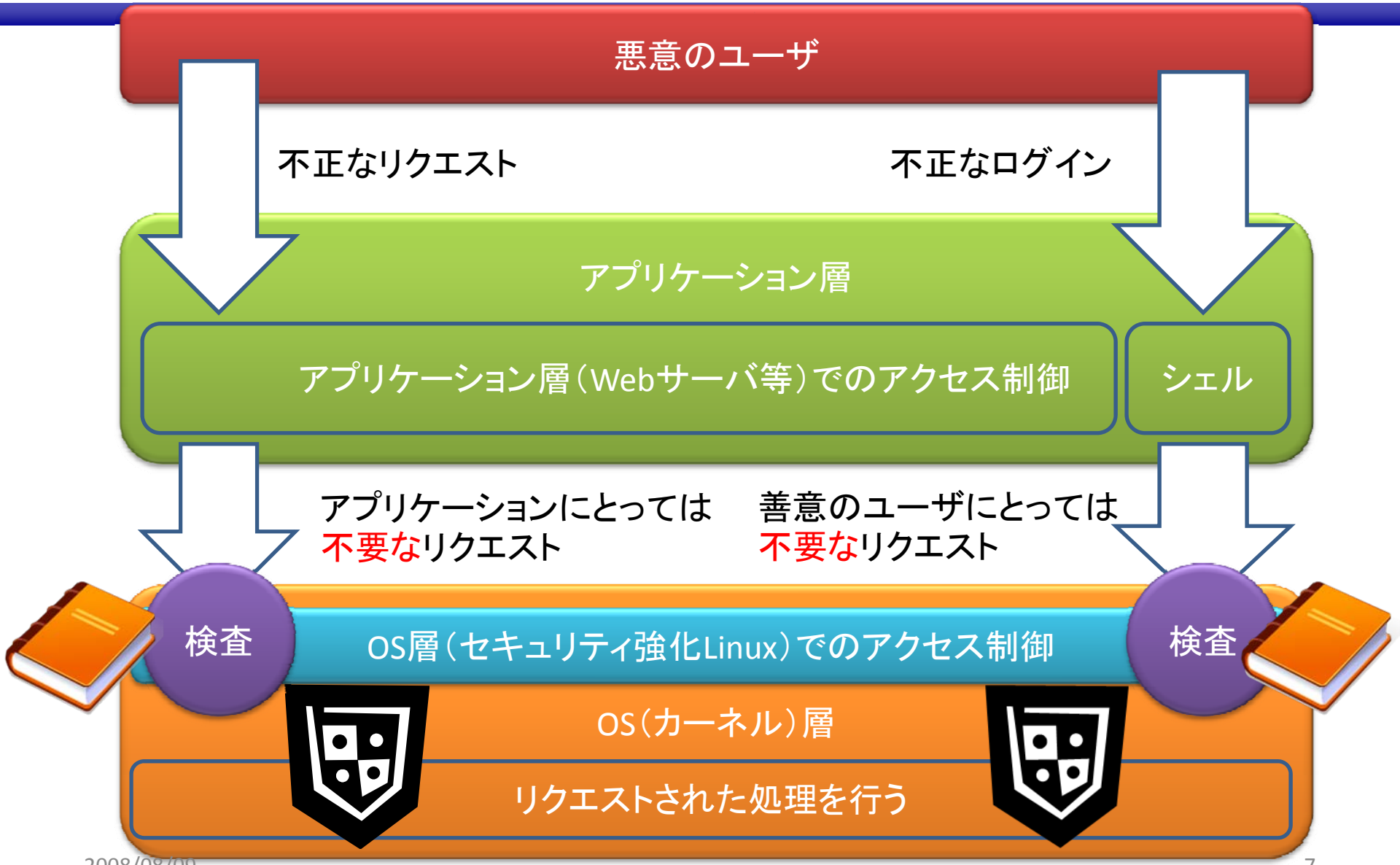
普通のLinux


善意のユーザ
正しいリクエスト
正しいログイン
アプリケーション層
アプリケーション層（Webサーバ等）でのアクセス制御
シェル
アプリケーションにとって
必要なリクエスト
善意のユーザにとって
必要なリクエスト
OS（カーネル）層
リクエストされた処理を行う

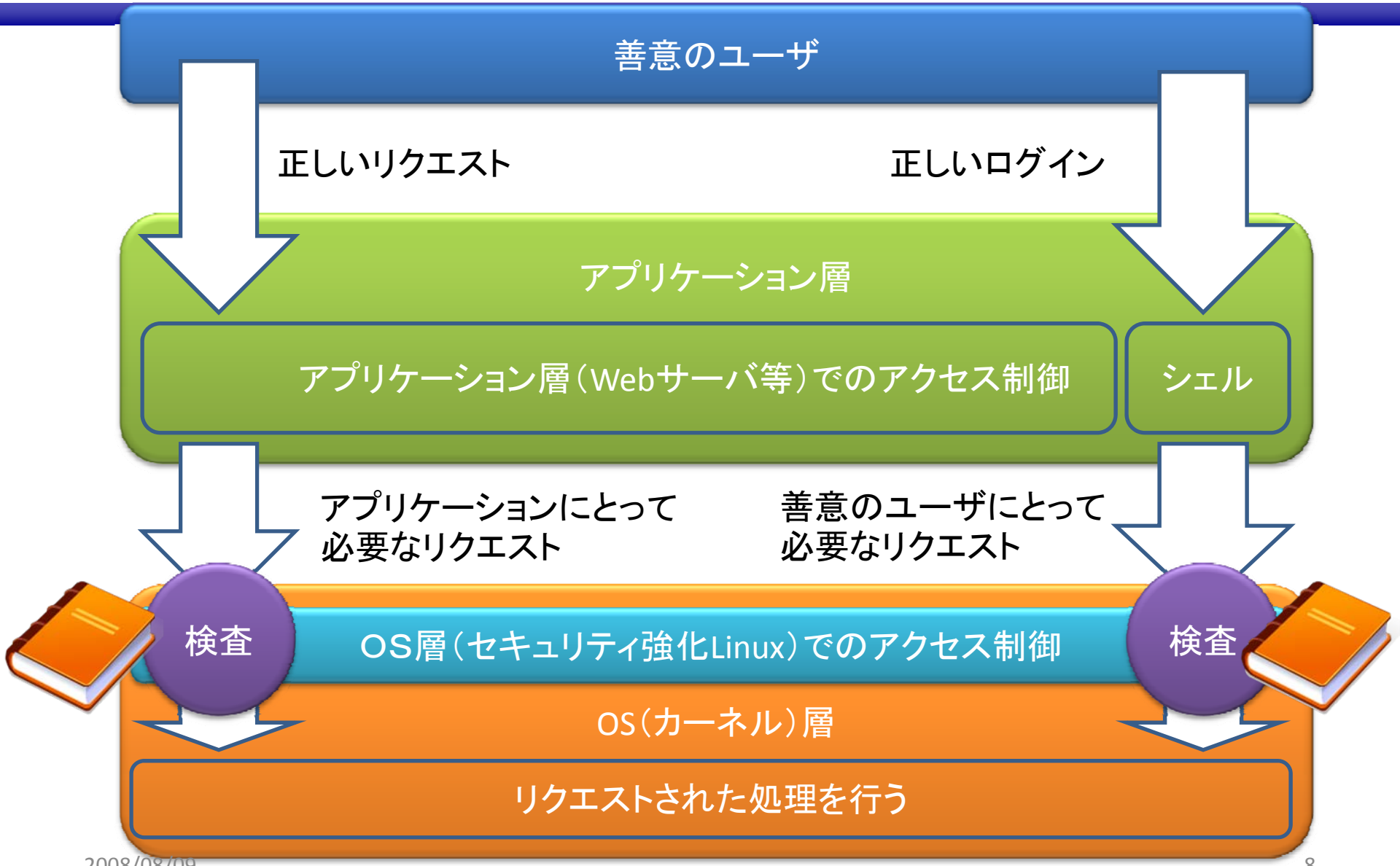
悪い人が来たら…


悪意のユーザ
不正なリクエスト
不正なログイン
アプリケーション層
アプリケーション層（Webサーバ等）でのアクセス制御
シェル
アプリケーションにとっては
不要なリクエスト
善意のユーザにとっては
不要なリクエスト
OS（カーネル）層
リクエストされた処理を行う

セキュリティ強化Linux



セキュリティ強化Linux



セキュリティ強化設定

- ポリシー
  - セキュリティ強化OSの設定のこと
  - 多くの場合「ホワイトリスト方式」
  - カーネルの視点で「やってよいこと」をすべて記述する必要がある
    - たとえば、「このファイルを読み込んでよい」
    - たとえば、「このIPアドレス・ポート番号でbindしてよい」
  - ポリシーに書いていないことはできない

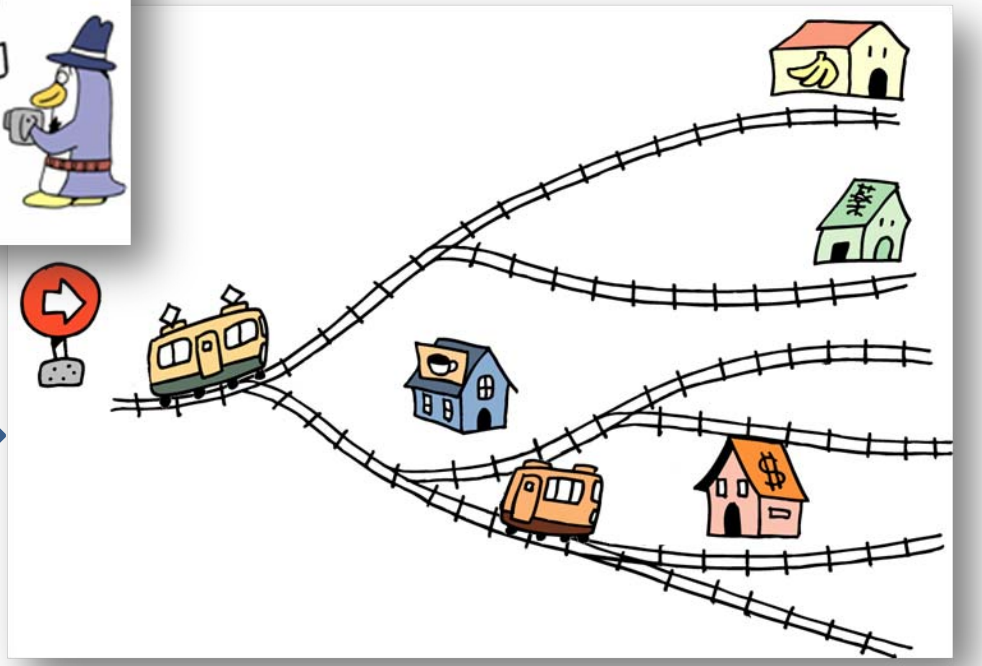
TOMOYO Linuxの特徴

- ポリシーの可読性に優れ、自動学習機能を搭載している
- 自動学習機能の使い方：
  - TOMOYO Linuxを学習モードに設定
    - アプリケーションを動作させる
    - TOMOYO Linuxが動作を学習して自動的にポリシーを作成する
  - TOMOYO Linuxを強制モードに設定
    - 学習させた動作しかおこなえなくなる

自動学習？

学習モード

強制モード



自動学習

- 動作を学習するということは、
  - プロセス（主体）の資源（客体）へのアクセスを
  - 監視し
  - 記録する
- 一種のアクセス解析機能
- アクセス解析の結果＝ポリシー
- ポリシーを読むことで、「Linuxの中で何が起こっているのか？」を理解できる

- 具体的にどんな風に学習するの？
  ➔TOMOYO Linuxで学習したポリシーの例をお見せします

プロセスの実行履歴のトレース

```
<kernel>
  /sbin/init
    /sbin/mingetty
      /bin/login
        /bin/bash
          /bin/ls
```

- この/bin/lsは…
  - /sbin/initから実行された、
  - /sbin/mingettyから実行された、
  - /bin/loginから実行された、
  - /bin/bashから実行されました

Bashのポリシー

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

--x /bin/egrep                          r-- /etc/profile.d/less.sh
--x /bin/grep                           r-- /etc/profile.d/which-2.sh
--x /bin/hostname                       r-- /etc/sysconfig/i18n
-w- /dev/null                           r-- /etc/termcap
rw- /dev/tty                            rw- /root/.bash_history
r-- /etc/bashrc                         r-- /root/.bash_logout
r-- /etc/inputrc                        r-- /root/.bash_profile
r-- /etc/nsswitch.conf                  r-- /root/.bashrc
r-- /etc/passwd                         --x /sbin/consoletype
r-- /etc/profile                        --x /usr/bin/clear
r-- /etc/profile.d/colorls.sh           --x /usr/bin/dircolors
r-- /etc/profile.d/cvs.sh               --x /usr/bin/id
r-- /etc/profile.d/glib2.sh             --x /usr/sbin/ccs-editpolicy
r-- /etc/profile.d/krb5-devel.sh        allow_capability SYS_IOCTL
r-- /etc/profile.d/lang.sh
```

- 具体的にどんな風に学習した結果を使おう？
  - ➔TOMOYO Linuxを使ったreadaheadの設定ファイルの作り方を紹介します

readahead

- ファイルを先読みしてメモリキャッシュに乗せて高速化を図る仕組み
- /etc/readahead/bootに列挙されたファイルがシステム起動の初期フェーズにメモリに乗る

- システムが起動するまで読み込まれるファイルを記載する
- この設定ファイルをTOMOYO Linuxを使って作ってみませう

readaheadの設定

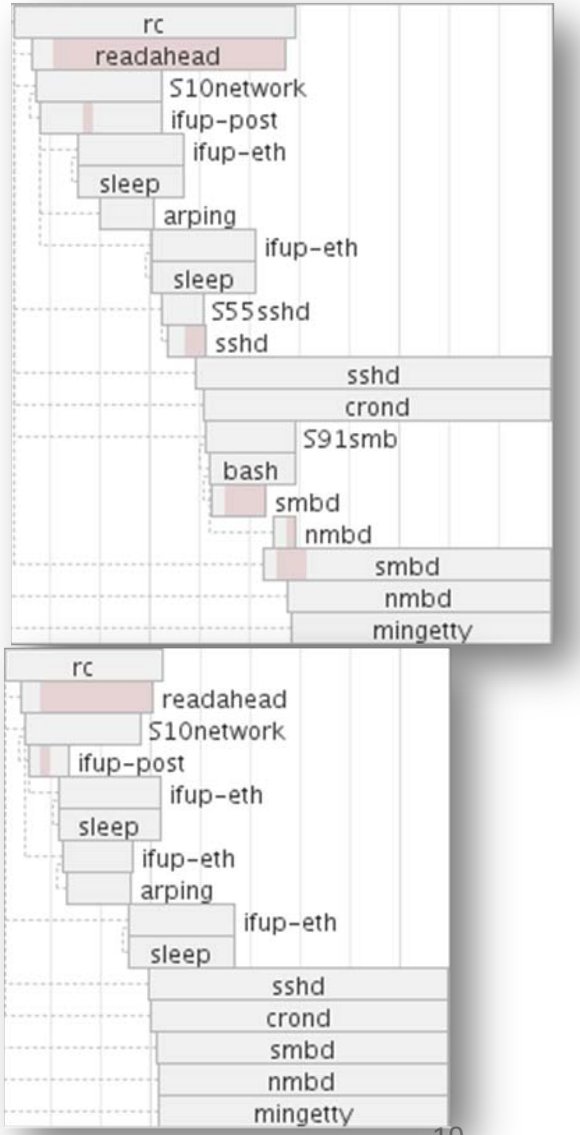
- システムの起動時に使用するファイルを含むべき
- システムの起動時に使用しないファイルは含まないべき

- TOMOYO Linuxでのつくり方
  - ライブラリファイルなどの読み込みを無条件に許可するallow_readエントリをポリシーから削除
  - TOMOYO Linuxを学習モードに設定してシステムを起動
  - ポリシーからシステム起動時に読み込んだファイルを抽出！

```
egrep '^allow_read|^allow_execute' /proc/ccs/domain_policy | ¥
  awk '{ print $2; }' | ¥
  sort | uniq | ¥
  egrep '^/bin/|^/etc/|^/lib/|^/sbin/|^/usr/|^/var/' ¥
    > /etc/readahead.d/default.early
```

結果

- デフォルトの設定では
  - 827個のファイルを先読み
  - 起動時間は23秒
- 学習結果からつくった設定では
  - 236個のファイルを先読み
  - 起動時間は21秒

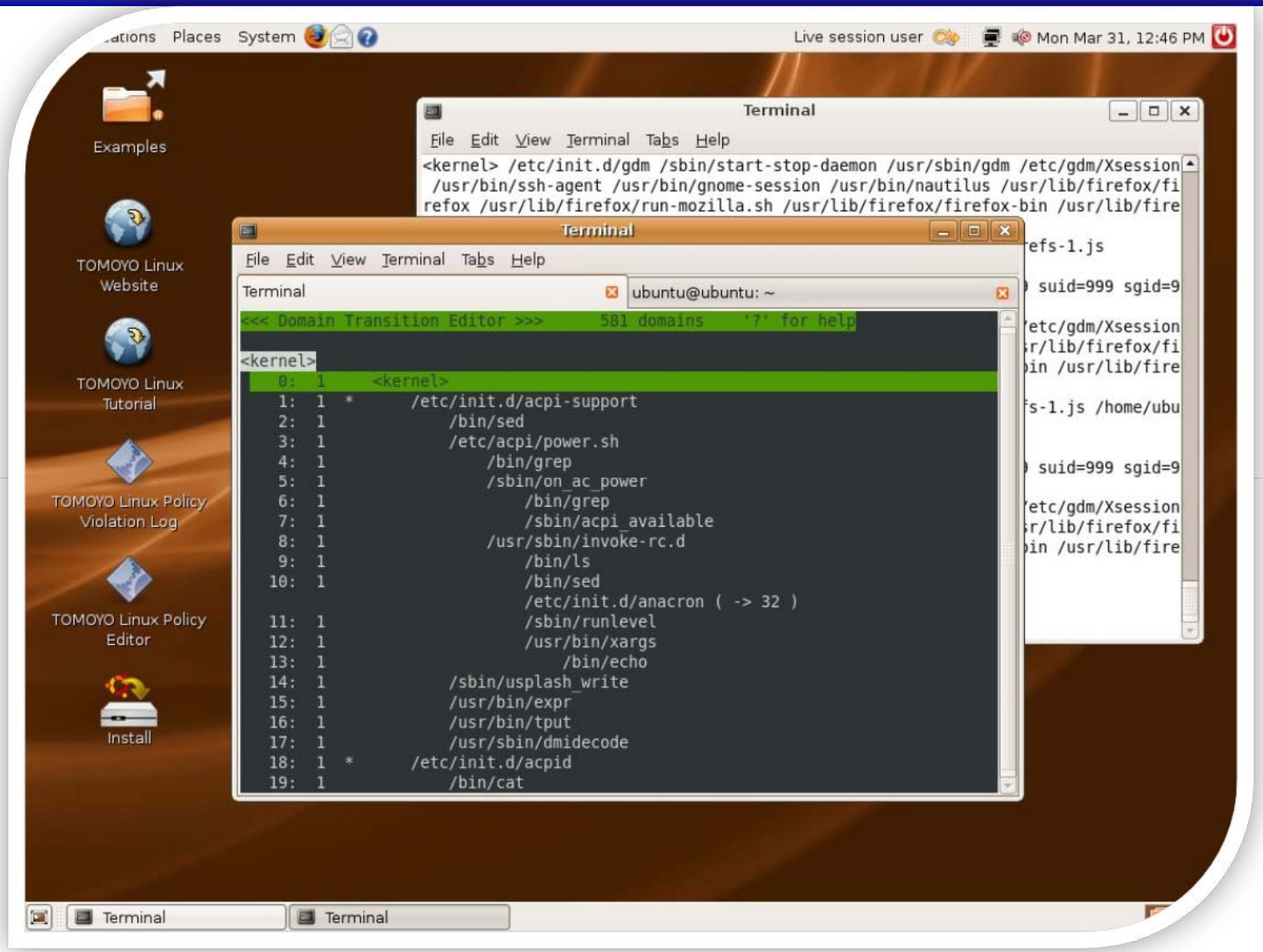


これ以外にも…

- シェルの設定ファイルって何が読まれるんだっけ？
  - .profile .bash_profile .bash_login .bashrc …
  - …どれがどれだか覚えきれませんorz
- make install時にどんなファイルが配置されるのか知りたいなぁ

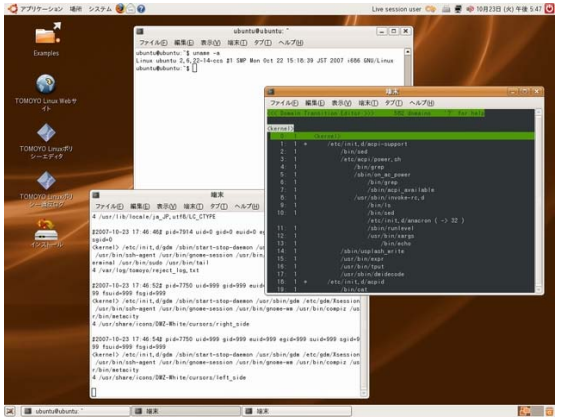
- どちらの場合も、TOMOYO Linuxでbashやmakeの動作を学習させれば一発です
  - 実際にTOMOYO GUIの開発や、無線LANドライバをtarballに固めたりする時に大活躍

そしてセキュリティ強化へ…



TOMOYO Linux Live!

- LiveCD：
  - CDからOSが起動するように作られたシロモノ
- TOMOYO Linux Live!
  - Ubuntu 8.04.1にTOMOYO Linux 1.6.3を導入済
  - いきなり学習モードで起動する
  - システム全体のポリシー（＝アクセス解析結果）がブラウズ可能
  - Linuxの学習に最適！



試してみる人へのお願い

- TOMOYO Linuxの学習機能は、それぞれのLinuxにオーダーメードのポリシーを提供します
  - 「デフォルトのポリシー」はありません
  - これをネックに感じる人が多い
- ユーザが事例を出してくれることが支えです
  - 「こんなポリシーを書いてみたよ」
    - Apache, MySQL, PostgreSQL, OpenSSH… etc.
  - あなたの使い方をぜひお寄せください

参考リンク

- TOMOYO Linuxオフィシャル
  - http://tomoyo.sourceforge.jp/
- メーリングリスト
  - http://lists.sourceforge.jp/mailman/archives/tomoyo-users/
- はてなダイアリーキーワード
  - http://d.hatena.ne.jp/keywords/TOMOYO%20Linux
  - イベントが時系列に並んでいます
- 2ch
  - http://pc11.2ch.net/test/read.cgi/linux/1212502041/
  - 中の人随時降臨中