セキュアOSの紹介と最新動向

～ SELinuxとTOMOYO Linuxを中心に ～

日本セキュアOSユーザ会

宍道　洋

日本セキュアOSユーザ会

Japan Secure Operating System Users Group since 2007

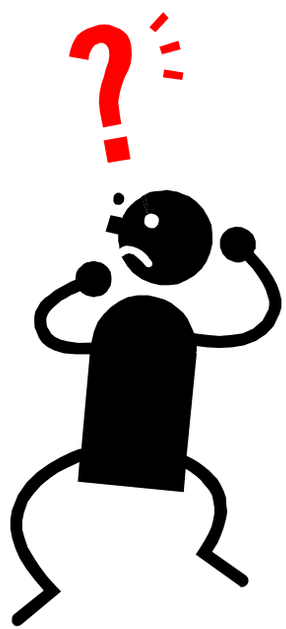
セキュアOSってなに？

- 一言で言うと「セキュリティを強化したOS」です

…？　で、何をどう強化したの？

- 最少特権化
  - プロセスを必要最小限の権限で動作
- 強制アクセス制御
  - 全ての利用者、全ての操作に例外なく
    アクセス制御を強制する

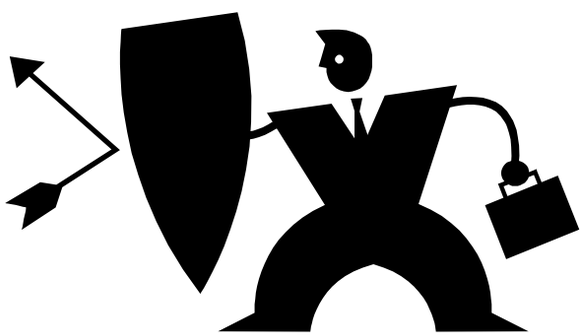
…？？



セキュアOSでなくっても…

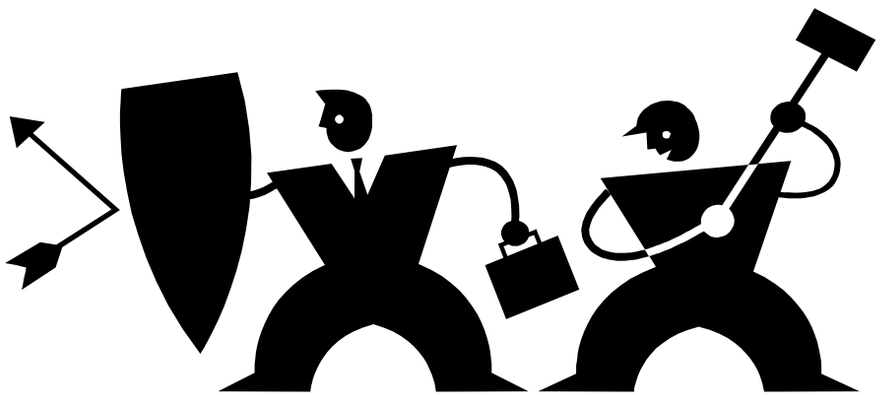
- 「基本的なセキュリティ対策で十分じゃない？」
  - 必要のないサービスを停止
  - 余計なポートをふさぐ
  - ログインパスワードの定期的な更新
  - リモートログインにはSSH＋公開鍵認証
  - こまめなソフトウェアのセキュリティパッチ適用
  - アンチウィルスソフトなどによるウィルス検知
  - IDSやF/Wなどのセキュリティ機器の導入

…などなど



でも脅威はいろいろ

- パッチ適用の不備
  - パッチ適用のために頻繁にサーバを停止できない
- 0-day攻撃
  - 0-dayの場合、パッチを当てようがない
- 内部犯行の脅威
  - 内部ネットワークに接続されたPCからの攻撃
  - 管理者権限を持つユーザの不正なアクセス



なぜそんな脅威があるの？

1. LinuxなどのUNIX系OSでは「任意アクセス制御(DAC: Discretionary Access Control)」が使われている
   - 資源（ファイルなど）の所有者が「任意」にアクセス権を変更できる
     - chmodコマンドを使ったりして
     - 機密文書が、故意または操作ミスで公開されるかも
2. 管理者はそのシステムの「神」
   - 管理者権限があると「任意アクセス制御」を無視できる
     - システム上のほとんどの権限を行使できる
     - 管理者権限を奪取できればシステムを乗っ取ることができる

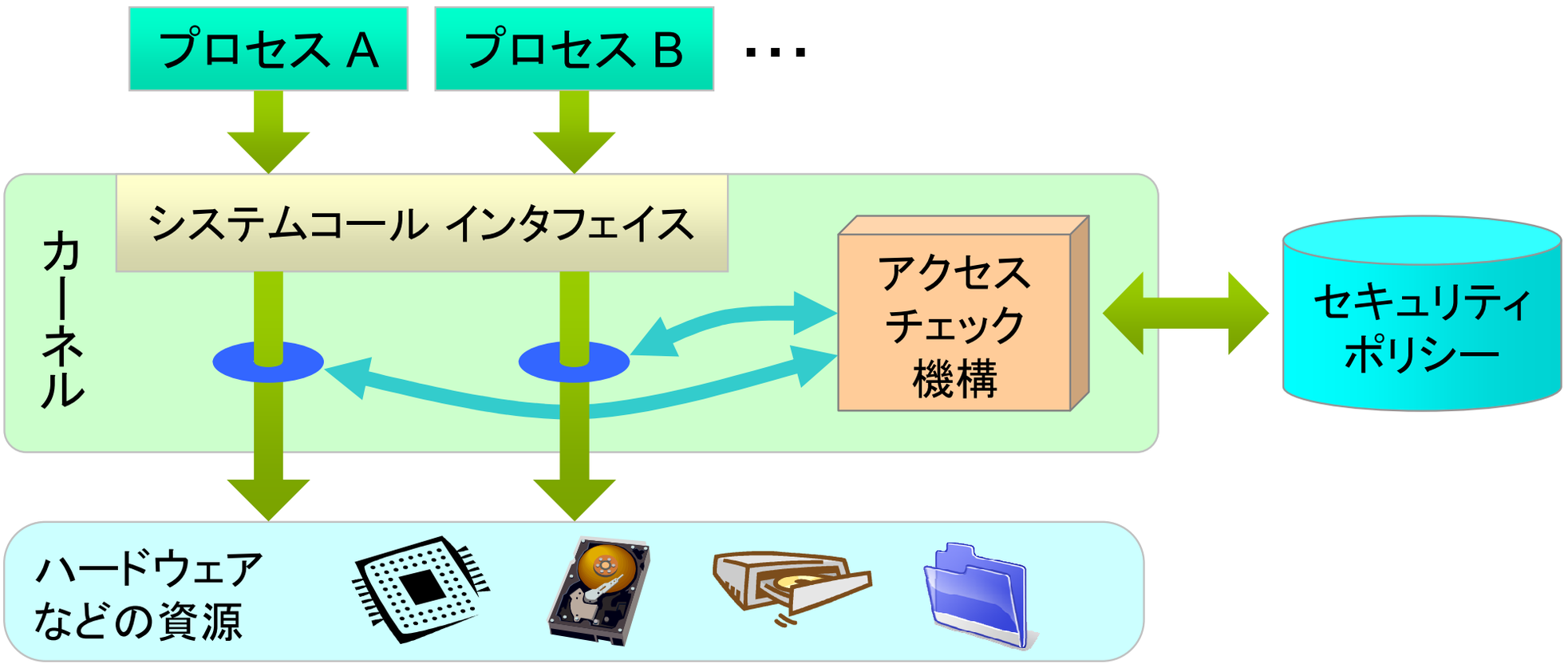
Japan Secure Operating System Users Group

セキュアOSでの対策

- セキュリティポリシーに基づく「強制アクセス制御」と「最少特権化」
  - 「セキュリティポリシー」では、「してもよいこと」や「使える特権」などを記述しておく
  - 書かれていないことは全て「禁止」
- 強制アクセス制御（MAC: Mandatory Access Control）
  - セキュリティポリシーに従ったアクセス制限を、全てのユーザやプロセスに強制させることができる仕組み
    - 資源の所有者であっても、その資源に対するアクセス権の変更ができない
    - 管理者であってもこのMACを回避できない
- 最少特権化
  - ユーザやプロセスの動作に必要最小限の特権しか割り当てない仕組み
    - 余計な特権を利用した不正な操作を不可能にする

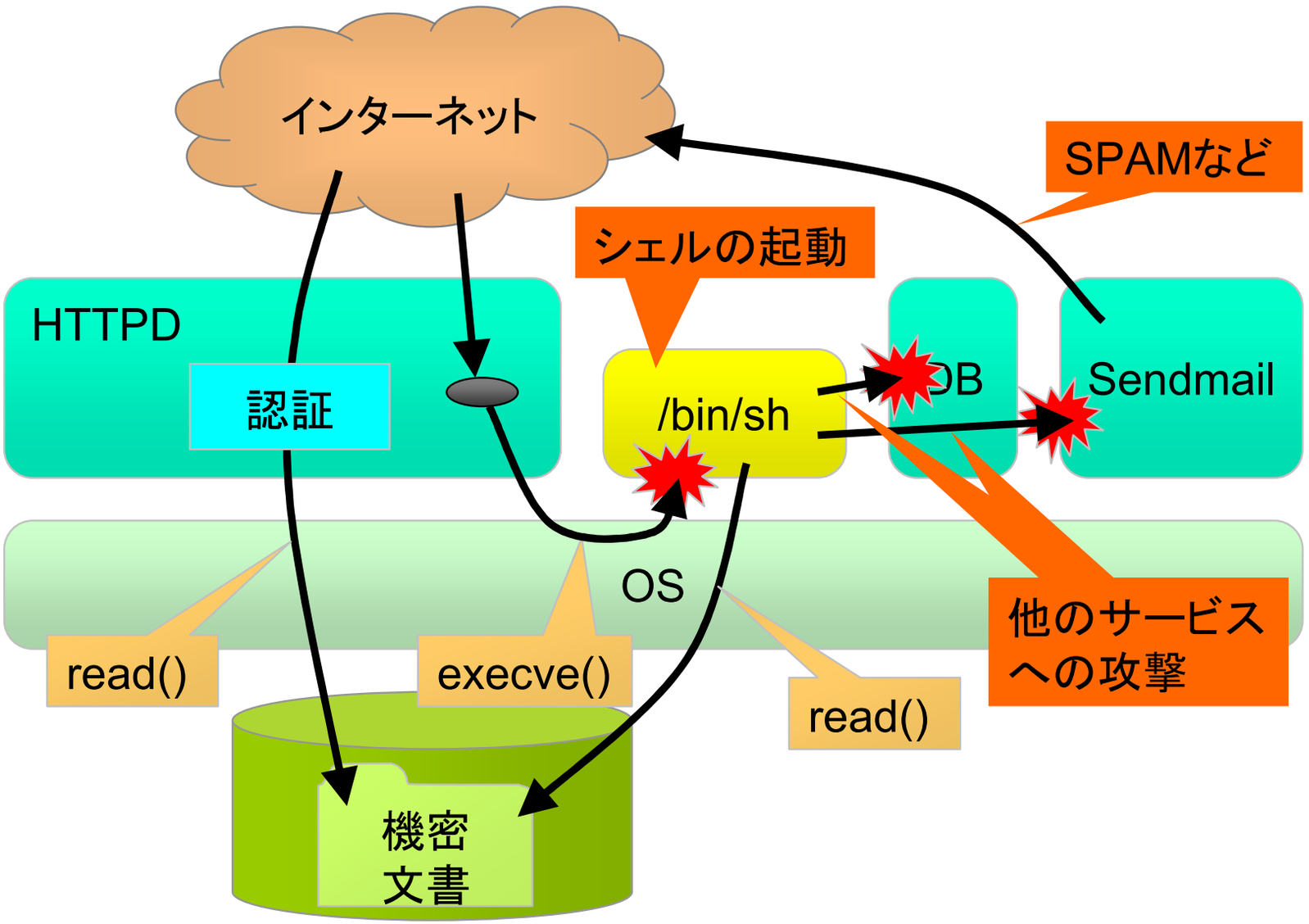
セキュアOSの仕組み

- 資源へのアクセスには、システムコール呼出が必要
  - システムコール呼出全てのフックで、アクセス全てを捕捉
    - ⇨ アクセスチェック機構によるアクセス制御が可能



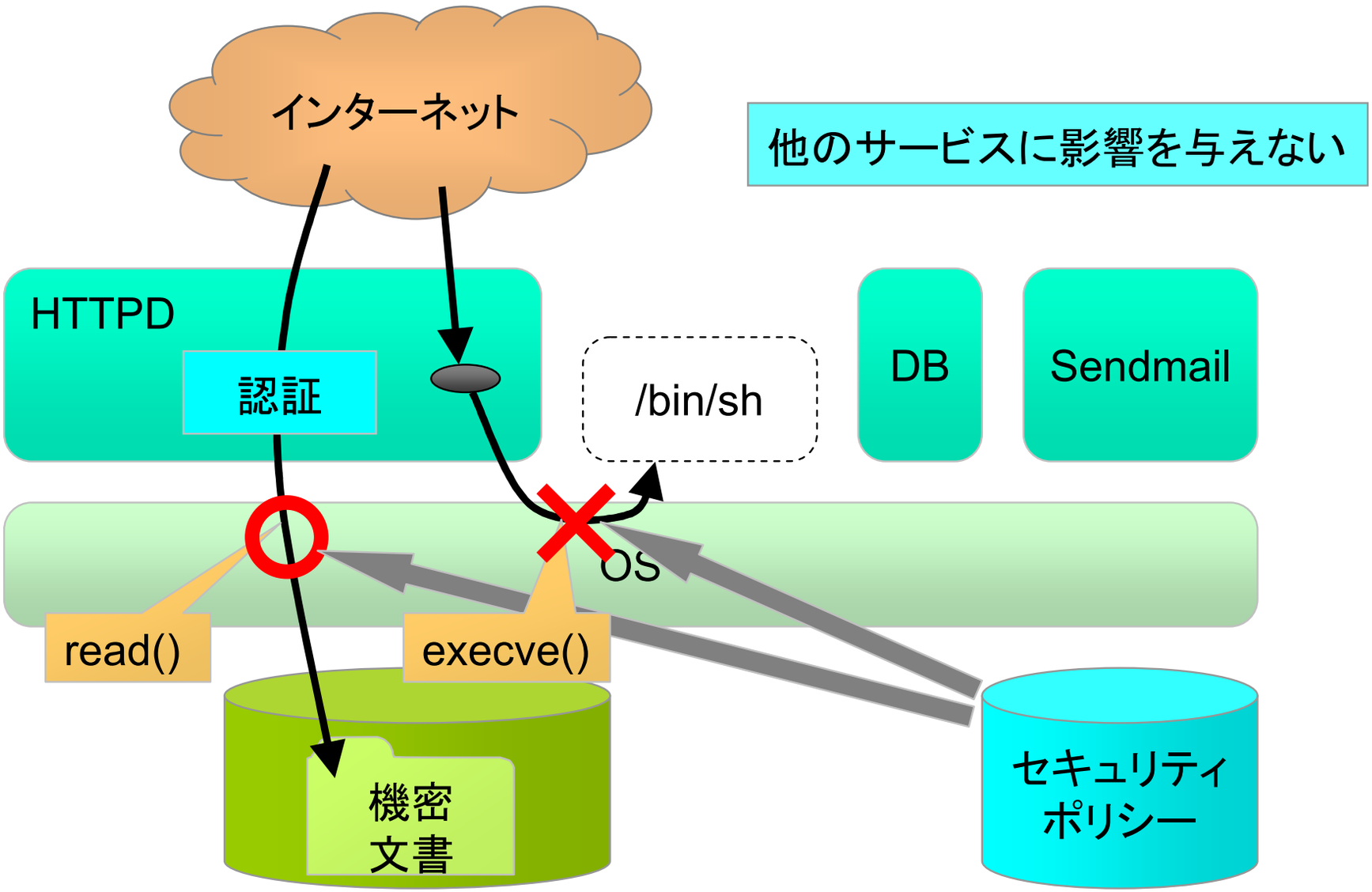
セキュアOSによる保護

- 通常のLinuxの場合



セキュアOSによる保護

- セキュアLinuxの場合



セキュアOSで守れないこともあります

- システムコールを介さない（OSが関与しない）、アプリケーションレベルの事象
  - XSSとか、SQLインジェクションとか
- DoS、DDoS攻撃
- 正規ユーザの操作ミス
  - 権限範囲内でのファイルの削除や設定ミスなど
- 正規ユーザへの成りすまし
- 攻撃を受けた脆弱アプリの動作保障
  - BOF攻撃を受けた後は、メモリ汚染のため正常な動作を期待できない

運用規定やセキュリティ機器などと組み合わせた多重防御は必要

セキュアOSの種類

- 商用のセキュアOS
  - Hizard, SecuveTOS, SHieldWare, WhiteShield
  - PitBull, HP-UX + Security Containment, AIX + Trusted AIX, CA Access Control, ...
- OSSのセキュアOS
  - TrustedBSD
  - OpenSolaris + Trusted Extensions
  - SELinux, TOMOYO Linux, Smack, LIDS, AppArmor, RSBAC, grsecurity

以降は、SELinuxとTOMOYO Linuxについて説明します。

Linuxベースのセキュア OS　その1
～ SELinux ～

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

SELinux (Security-Enhanced Linux)

- アメリカ国家安全保障局(NSA)が中心となって開発
- Linuxカーネル2.6.x および RHEL, CentOS, Fedoraで標準機能
- ラベルベースのアクセス制御方式
  - 長所: アクセス対象をラベルで抽象化し、アクセス範囲を特定できる
  - 短所: ラベル付けなどの設定が複雑化
- SELinuxのアクセス制御機能
  - TE (Type Enforcement)
  - RBAC (Role Based Access Control)
  - MLS (Multi-Level Security),
MCS (Multi-Category Security)

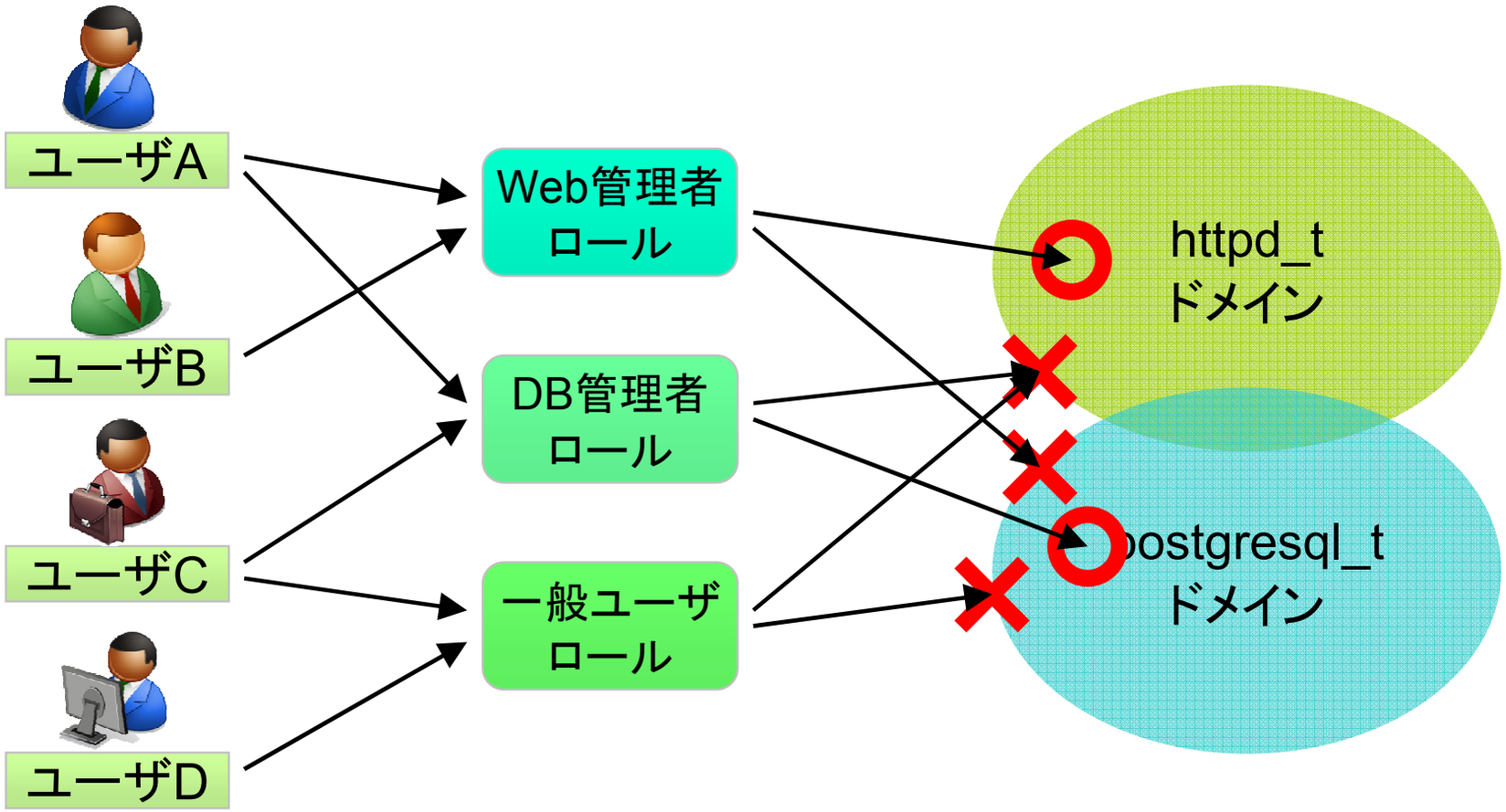
TE (Type Enforcement)

- ドメイン（プログラムの動作範囲）ごとに利用可能な資源を限定
  - たとえばApacheの場合 （httpd_tドメイン）

明示的に指定したもの以外は、全てアクセス禁止

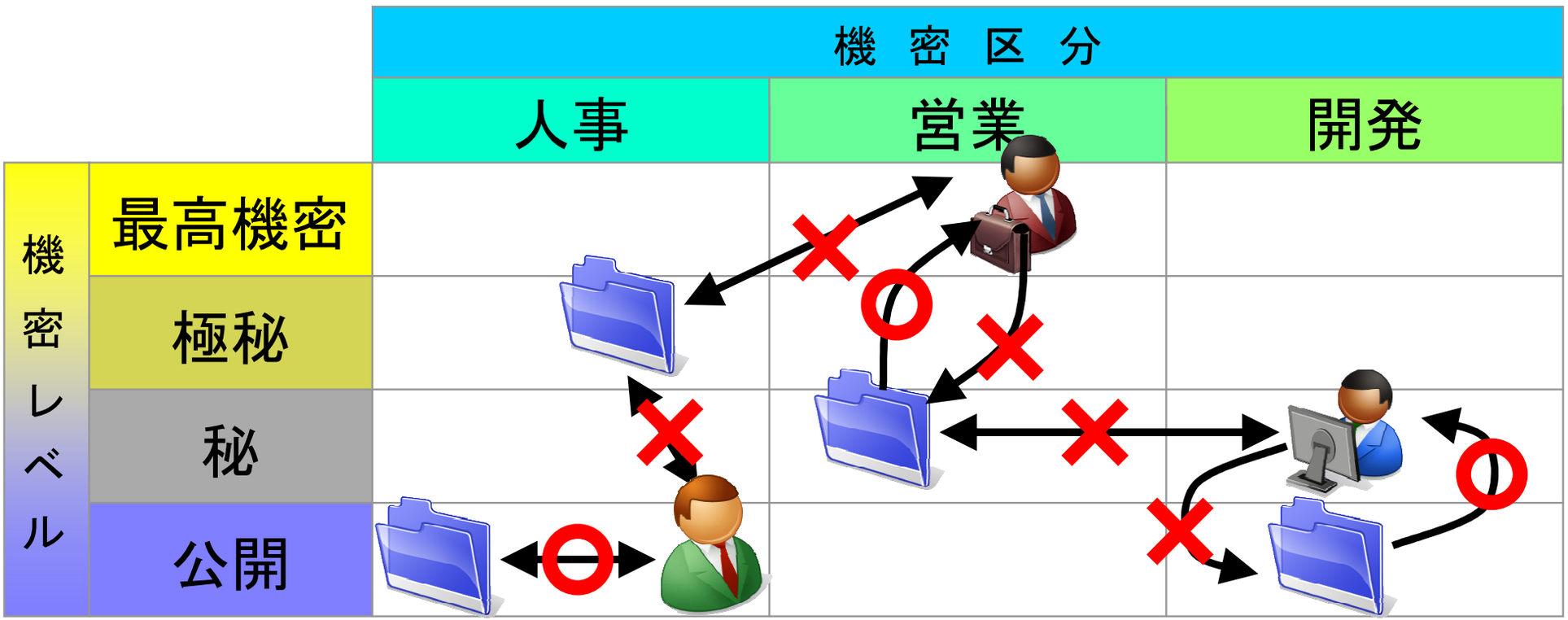
RBAC (Role Based Access Control)

- 役割(ロール)に応じたアクセス権の付与
  - 役割ごとに利用する権限を限定する



MLS, MCS (Multi-Level Security, Multi-Category Security)

- 機密レベル・機密区分に応じたアクセス制御
  - 機密区分を超えて資源を利用できない
  - 機密レベルの高い情報は低いユーザから読み出し禁止
  - 書き込みは、同じ機密レベルの資源だけ可能
    - ➡「情報の流れ（情報フロー）」を制御

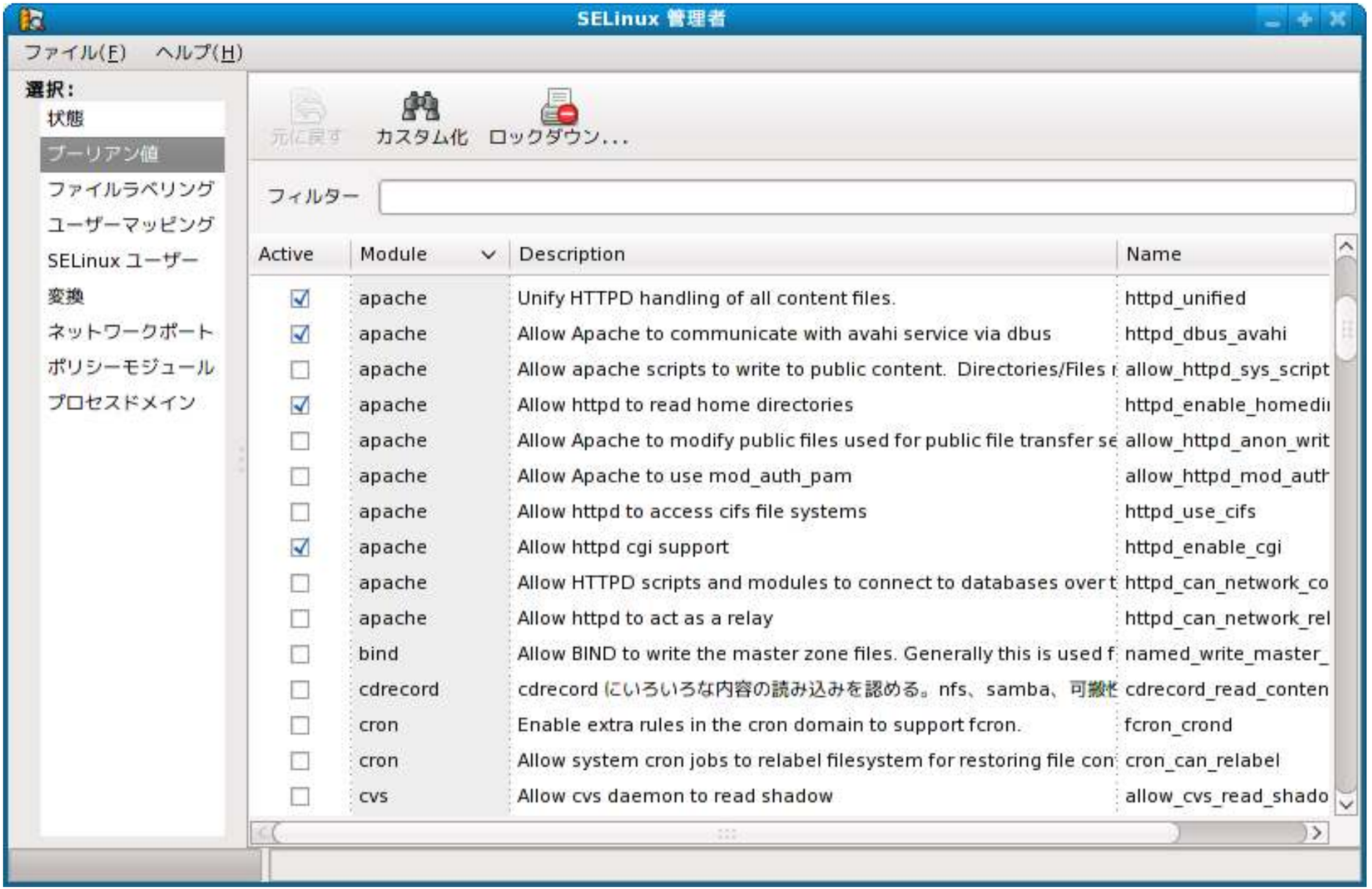


SELinuxを使うには

- FedoraやCentOS、RHELではデフォルトでインストール
  - 標準ポリシーはTargeted Policy（対象を絞ったポリシー）
    - Apacheやsyslogdなどのシステムサービスのみ保護
    - ユーザはUnconfined（非制限）ドメインで、ほぼ今までどおり
  - 管理ツールはGUIの「system-config-selinux」
    - booleanでの設定：セキュリティポリシーの一部をON/OFF
    - ファイルやディレクトリなどのタイプの設定・変更
  - setroubleshootによる問題解決
    - アクセス拒否の通知機能と、問題解決方法の提示
  - /sbin/restorecon
    - タイプの不整合の修正

Debian, Ubuntu, GentooなどでもSELinuxが使えます

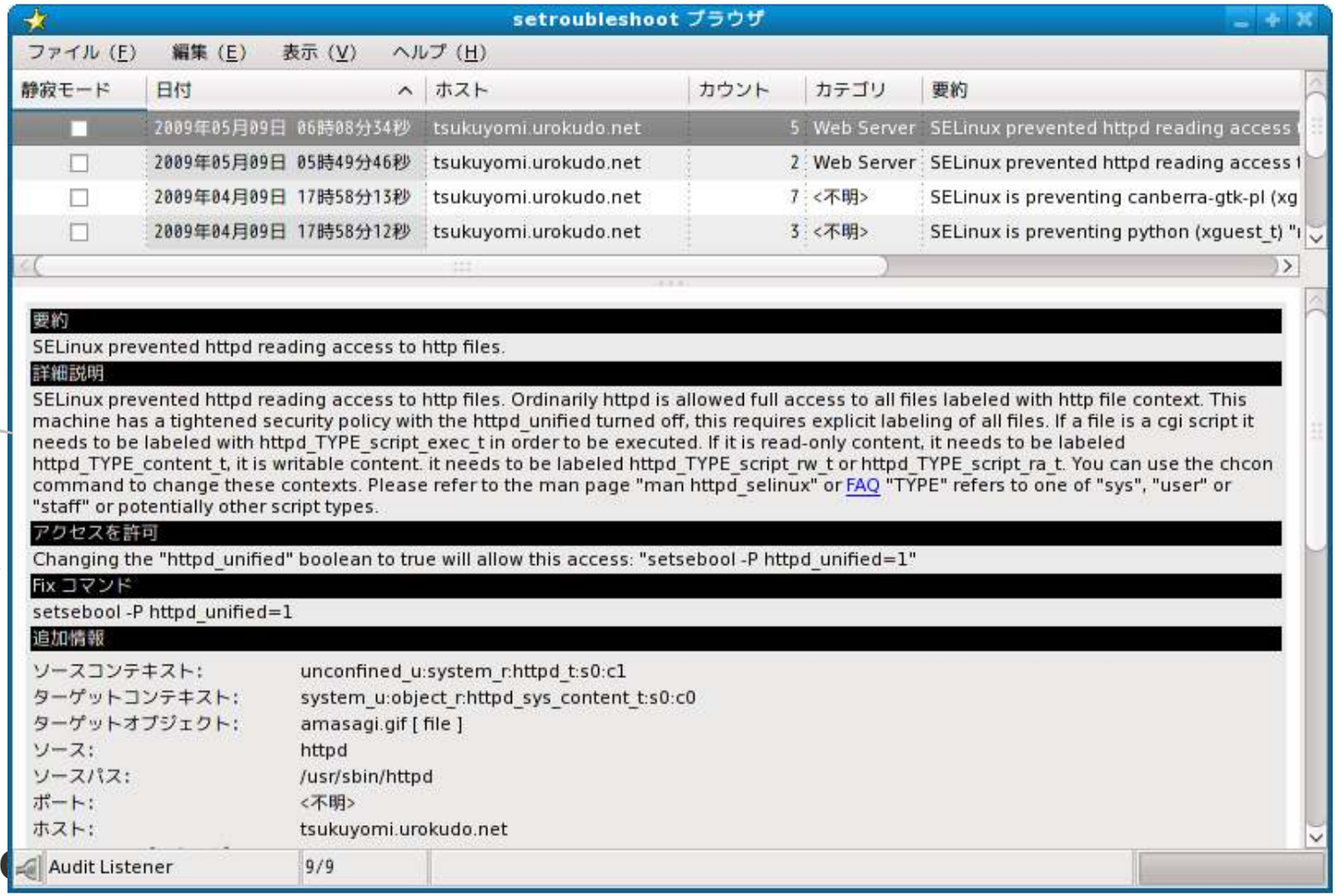
system-config-selinux



Japan
Secure Operating System
Users Group

setroubleshoot

警告の表示



原因

解決方法の提案

Linuxベースのセキュア OS その2
～ TOMOYO Linux ～

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

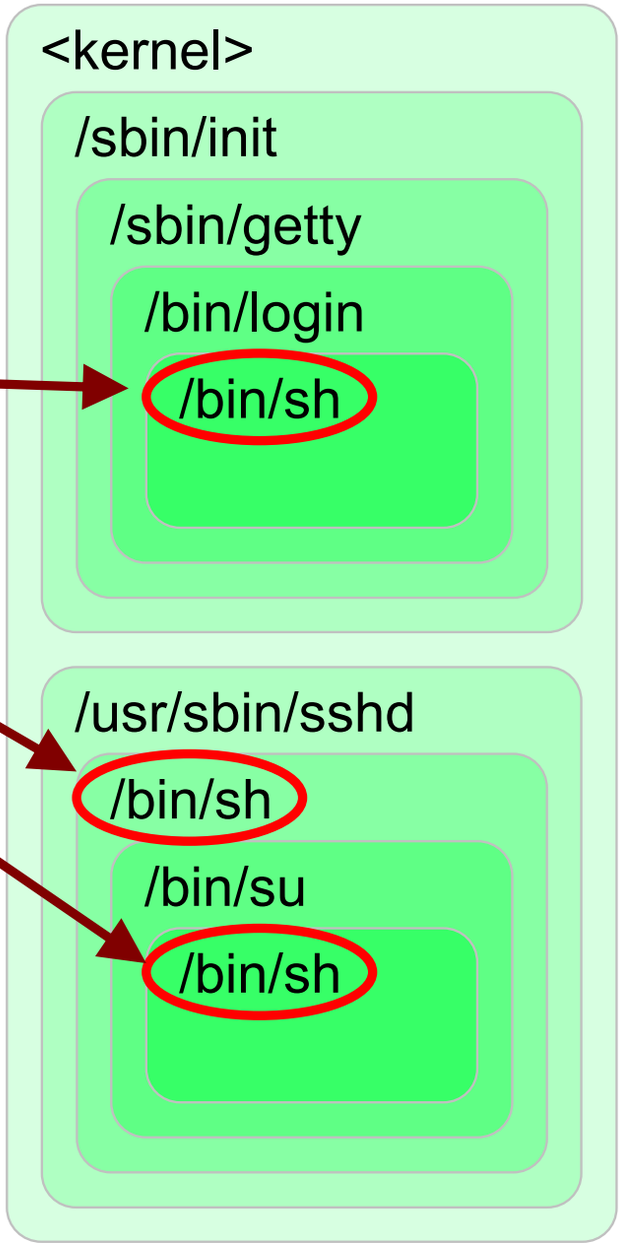
Japan Secure Operating System Users Group

TOMOYO Linuxとは？

- NTTデータで開発され、2005年にOSSとして公開
- TOMOYO Linuxの主な機能
  - パス名ベースのアクセス制御
    - SELinuxの場合は、TEによるラベルベースのアクセス制御
  - プロセスの呼び出し履歴に基づくドメイン
  - ポリシーの自動学習機能
    - プロセスの動作を監視して記録する
      - 読み書きするファイルや、呼び出す別プロセスなど
    - 運用時には、学習したポリシーを強制できる
      - 運用時でも一部をアクセス制御対象外や学習モードにすることも可能

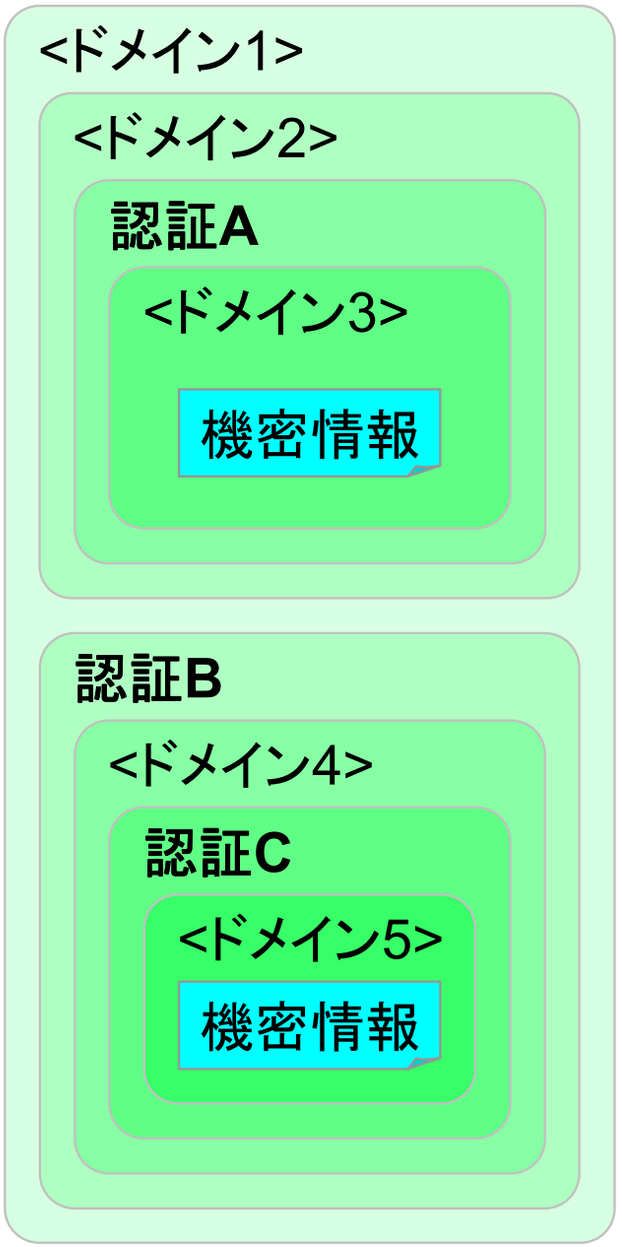
TOMOYO Linuxのドメイン

- プロセスの呼び出し履歴に基づく階層的ドメイン
  - 呼び出し順が異なれば別ドメイン
    - コンソールでログインしたsh
    - SSH経由でログインしたsh
    - さらにsuを実行した後のsh
  - それぞれで異なるポリシーを設定可能



TOMOYO Linuxのドメイン

- 階層的ドメインと認証プログラムの組み合わせ
  - 別のドメインへ移行する際に認証プログラムをおくことができる
    - ログイン時の一回だけでなく、任意の回数の認証を通すことが可能
    - 認証方法は自由
      - パスワード方式
      - 特定ファイルの有無
      - 環境変数の値
      - キー入力タイミング　　などなど
    - 認証をクリアしないと目的のドメインに到達しない



ポリシーの自動学習機能

- プロセスの動作を監視し、記録する
  - ファイルなど資源へのアクセス（読み書き、作成、変更など）
  - ネットワークアクセス
  - 使用する環境変数や権限、シグナルなど
- 基本はゼロからのポリシー作成
  - SELinuxのように用意されたポリシーはない
  - 学習モードで作成し、必要に応じて調整し、適用する
- ポリシー作成のほかに、プロセスのアクセス解析として利用可能
  - 複雑なプログラムや商用アプリのアクセス解析
  - 組込み機器でのファイルシステム最適化（不要なファイルの削除など）

ポリシーの自動学習機能

- 学習例
  - /sbin/gettyの場合

```
<kernel> /sbin/init /sbin/getty
use_profile 1

allow_read/write /tmp/utmp
allow_create /tmp/utmp
allow_write /tmp/wtmp
allow_create /tmp/wtmp
allow_execute /bin/login
allow_read /etc/issue
allow_read /lib/ld-uClibc-0.9.30.1.so
allow_read /lib/libuClibc-0.9.30.1.so
allow_read/write /dev/null
allow_read/write /dev/ttyS0
```

ドメイン

学習モード

/tmp/utmpの生成と読み書き

/tmp/wtmpの生成と書き込み

loginコマンドの実行

使用するライブラリの読み込み

仮想デバイスファイルの読み書き

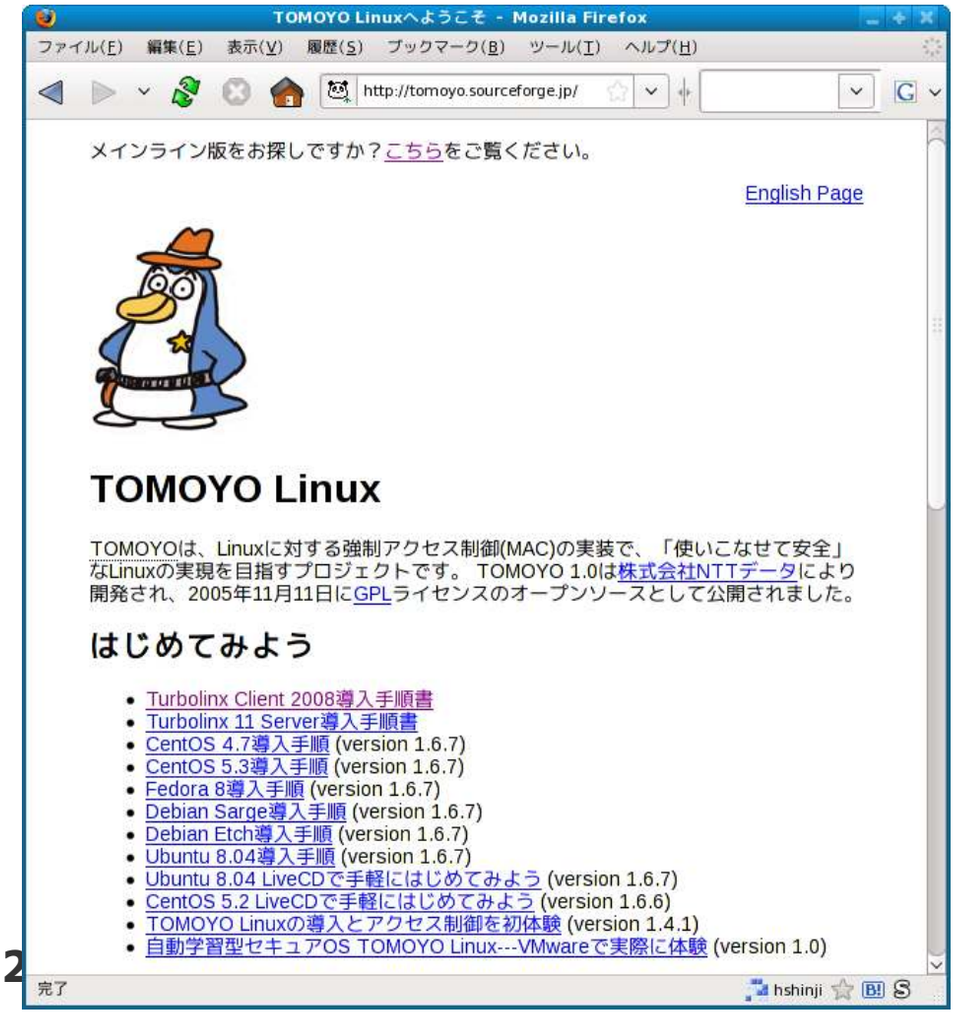
ポリシーの編集ツール

```
shinji@teruzuki-x86:~
<<< Domain Transition Editor >>>      57 domains    '?' for help

<kernel> /etc/init.d/S50dropbear /sbin/start-stop-daemon /usr/sbin/dropbear
   10:  3                  /bin/sh
   11:  3                      /bin/ip
   12:  3                      /bin/run-parts
   13:  3              /sbin/ifup
   14:  3                  /bin/sh
   15:  3                      /bin/ip
   16:  3                      /bin/run-parts
   17:  3  *       /etc/init.d/S49ntpd
   18:  3              /bin/pidof
   19:  3              /usr/sbin/ntpd
   20:  3  *       /etc/init.d/S50dropbear
   21:  3              /sbin/start-stop-daemon
   22:  3                  /usr/sbin/dropbear
   23:  3                      /bin/sh
   24:  3                          /bin/hostname
   25:  3                          /bin/su
   26:  0 #                            /bin/sh
   27:  3                          /usr/bin/id
   28:  3                          /usr/bin/scp
   29:  3  *       /etc/init.d/S90crond
   30:  3              /sbin/start-stop-daemon
```

```
shinji@teruzuki-x86:~
<<< Domain Policy Editor >>>      31 entries    '?' for help

<kernel> /etc/init.d/S50dropbear /sbin/start-stop-daemon /usr/sbin/dropbear
    0: allow_execute    /bin/sh
    1: allow_read/write /dev/null
    2: allow_read/write /dev/ptmx
    3: allow_read/write /dev/pts/\$
    4: allow_read/write /dev/tty
    5: allow_read       /dev/urandom
    6: allow_read       /etc/TZ
    7: allow_read       /etc/dropbear/dropbear_dss_host_key
    8: allow_read       /etc/dropbear/dropbear_rsa_host_key
    9: allow_read       /etc/group
   10: allow_read       /etc/hosts
   11: allow_read       /etc/passwd
   12: allow_read       /etc/resolv.conf
   13: allow_read       /home/shinji/.ssh/authorized_keys
   14: allow_read       /lib/ld-uClibc-0.9.30.1.so
   15: allow_read       /lib/libcrypt-0.9.30.1.so
   16: allow_read       /lib/libgcc_s.so.1
   17: allow_read       /lib/libuClibc-0.9.30.1.so
   18: allow_read       /lib/libutil-0.9.30.1.so
   19: allow_read/write /mnt/lastlog
   20: allow_write      /mnt/wtmp
```

TOMOYO Linuxを使うには

- Turbolinux, Fedora, CentOS, Debian, Ubuntu, Mandriva などで利用可能
  - http://tomoyo.sourceforge.jp/ （オフィシャルサイト）
    - 導入手順書
    - 講演資料
  - UbuntuやCentOSによる Live CDもあります



SELinuxとTOMOYO Linuxの最近の動向
～ SELinux ～

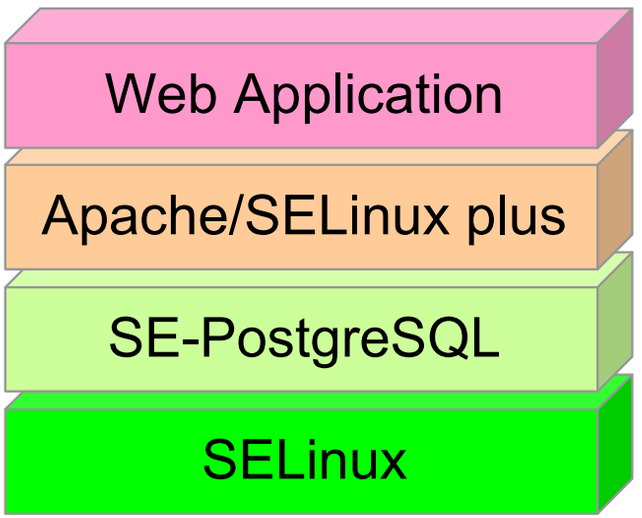
日本セキュアOSユーザ会
Japan Secure Operating System Users Group since 2007

LAPP/SELinux

- SELinuxを使ってLAPPスタック全体を保護
  - LAPPスタック
    - Linux + Apache + PostgreSQL + PHP
      - ➡それぞれに異なるセキュリティ機能があり、一貫性が無い

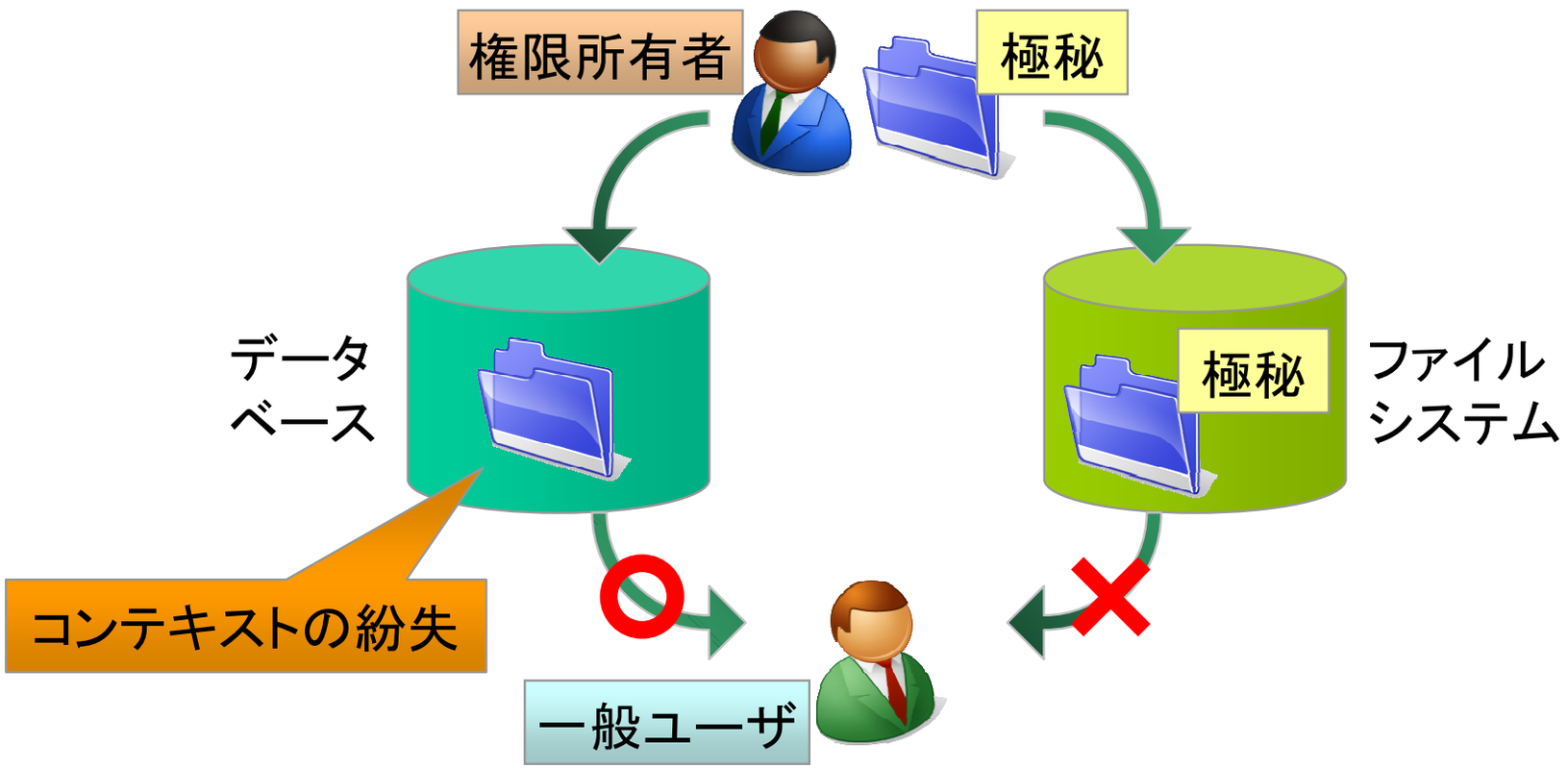
⬇

  - SELinux + Apache/SElinux plus + SE-PostgreSQL + PHP
    - NECの海外浩平氏が開発
    - SELinuxの提供するAPIを使って、セキュリティ機能を拡張
    - 共通のセキュリティコンテキスト（セキュリティ属性）を利用して、LAPPスタック全体で一貫性のあるアクセス制御を行う



SE-PostgreSQL

- SELinux上でのPostgreSQLの問題点
  - 同じセキュリティコンテキストの情報をファイルシステムとDBに格納
    - ➡DB上の情報からセキュリティコンテキストが紛失

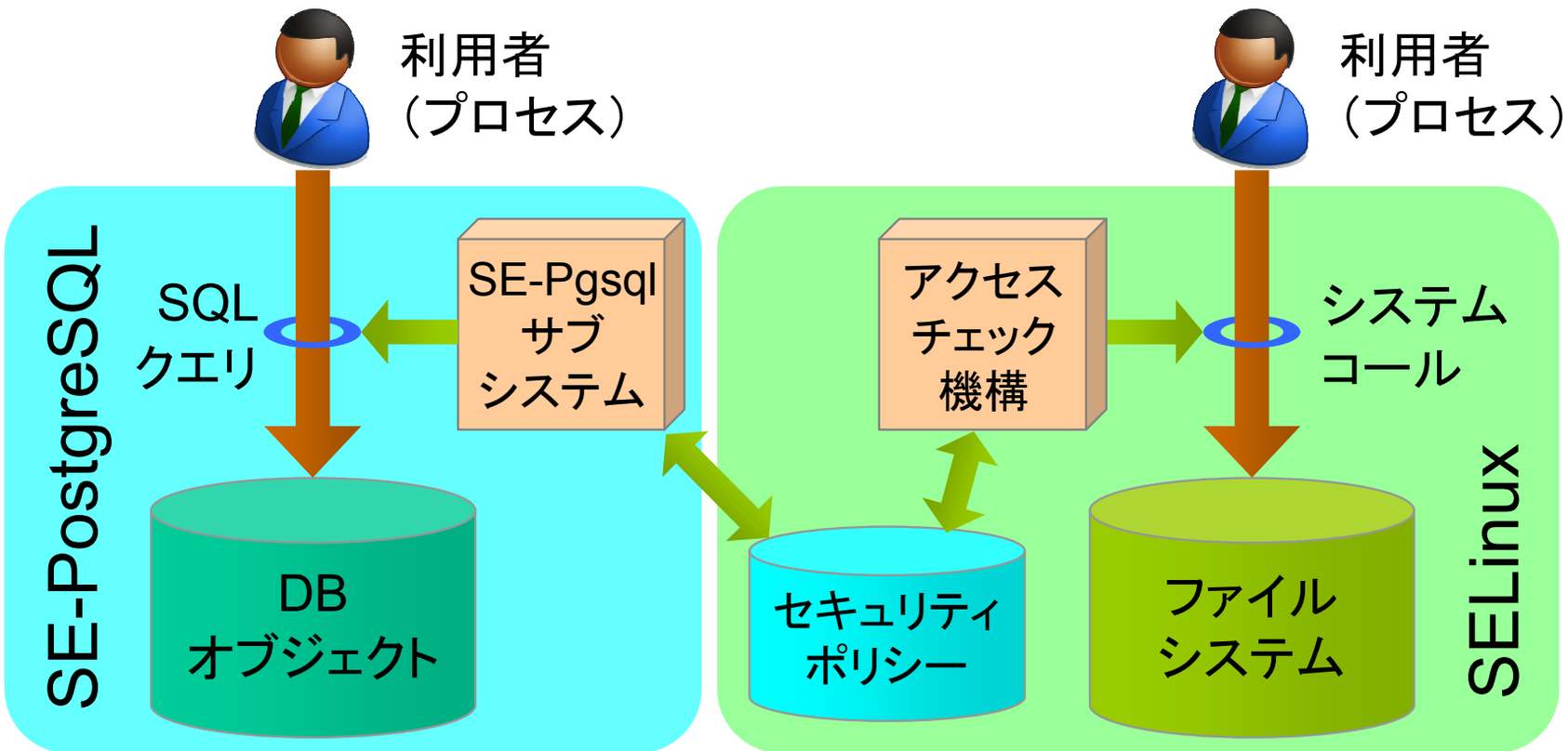


SE-PostgreSQL

- SE-PostgreSQL
  - DBへのアクセス時にSELinuxのポリシーを適用

SELinux　　：プロセス ➡ システムコール ➡ ファイルシステム

SE-PostgreSQL ：プロセス ➡ SQLクエリ ➡ DBオブジェクト

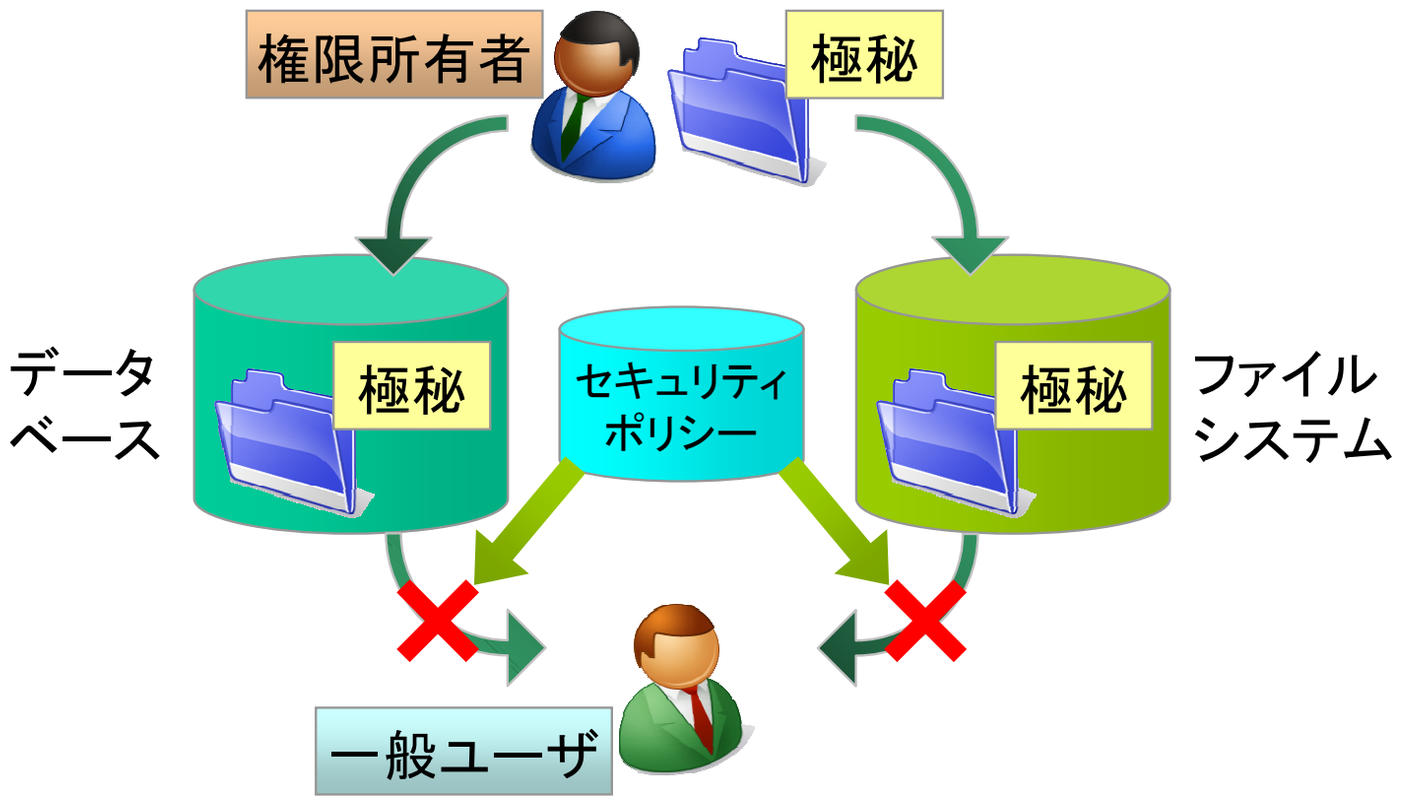


SE-PostgreSQL

- SE-PostgreSQL
  - DBへのアクセス時にSELinuxのポリシーを適用

SELinux　　：プロセス ➡ システムコール ➡ ファイルシステム

SE-PostgreSQL ：プロセス ➡ SQLクエリ ➡ DBオブジェクト



Apache/SELinux plus

- SELinux上でのWebアプリケーションの問題点
  - Webサーバプロセスが全てのWebアプリを実行
    ➡ OSやDBからは利用者の区別が不可能

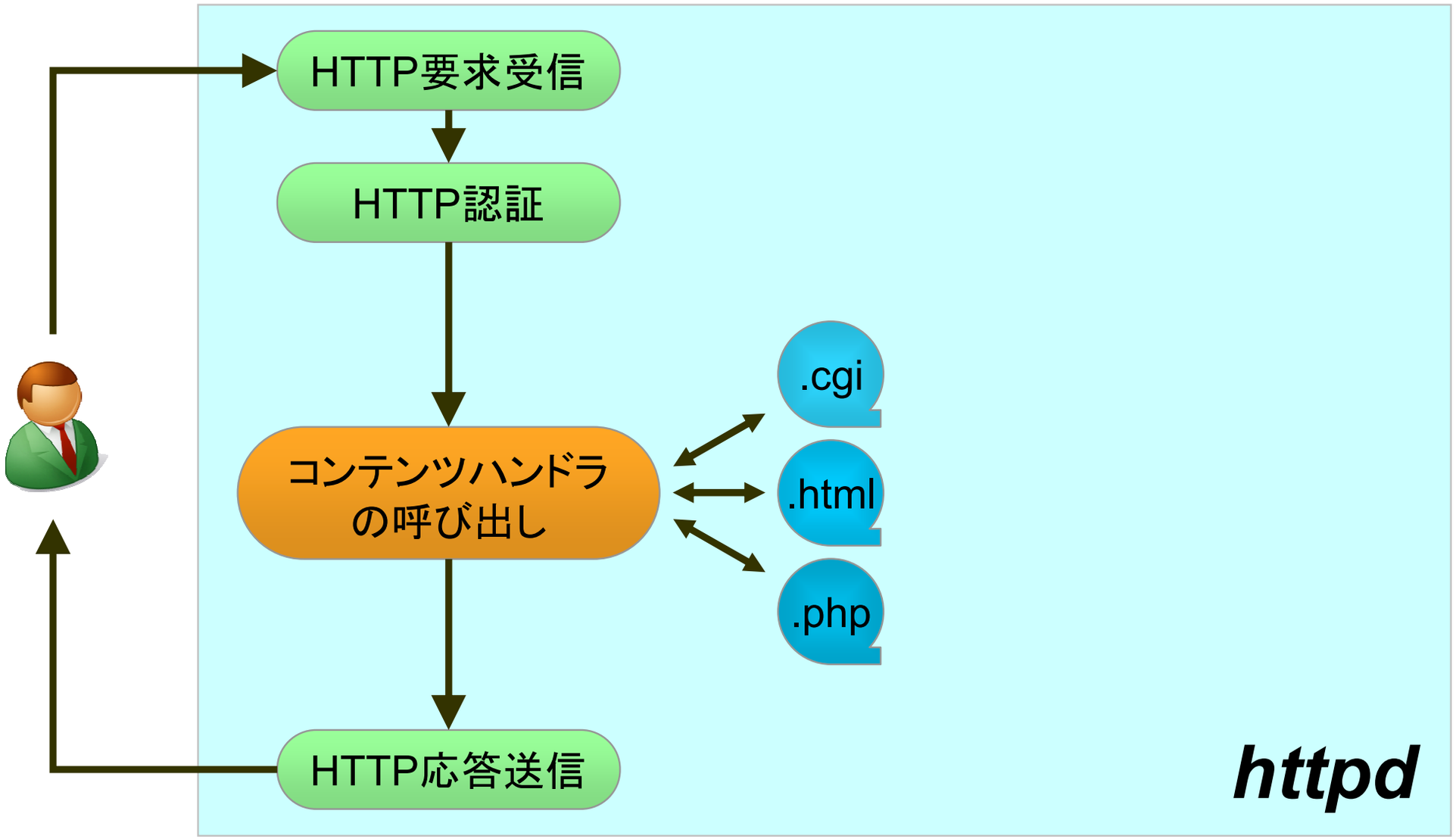
リクエスト実行前に、利用者に応じた権限の割り当てが必要

- スレッド単位で権限を割り当てられるようになった（Linuxカーネル2.6.28以降）
  - WebアプリはWebサーバプロセスのスレッドとして動作
  - 親プロセスの権限を越えない範囲でスレッドの権限を設定可能
  - これも海外氏の開発

Apache用モジュール「mod_selinux」
利用者ごとの権限でWebアプリを実行可能に

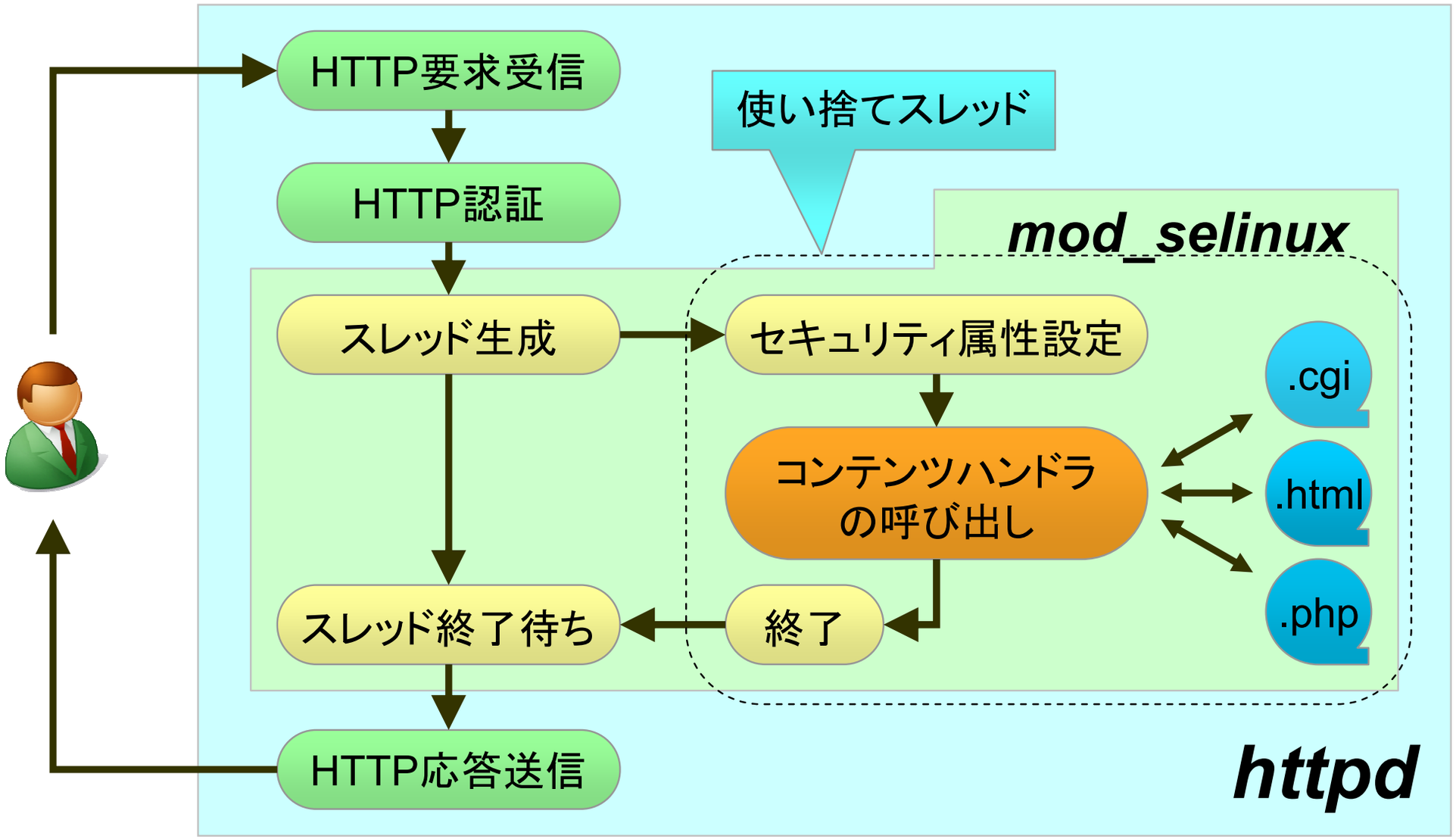
Apache/SELinux plus

- 通常のApache

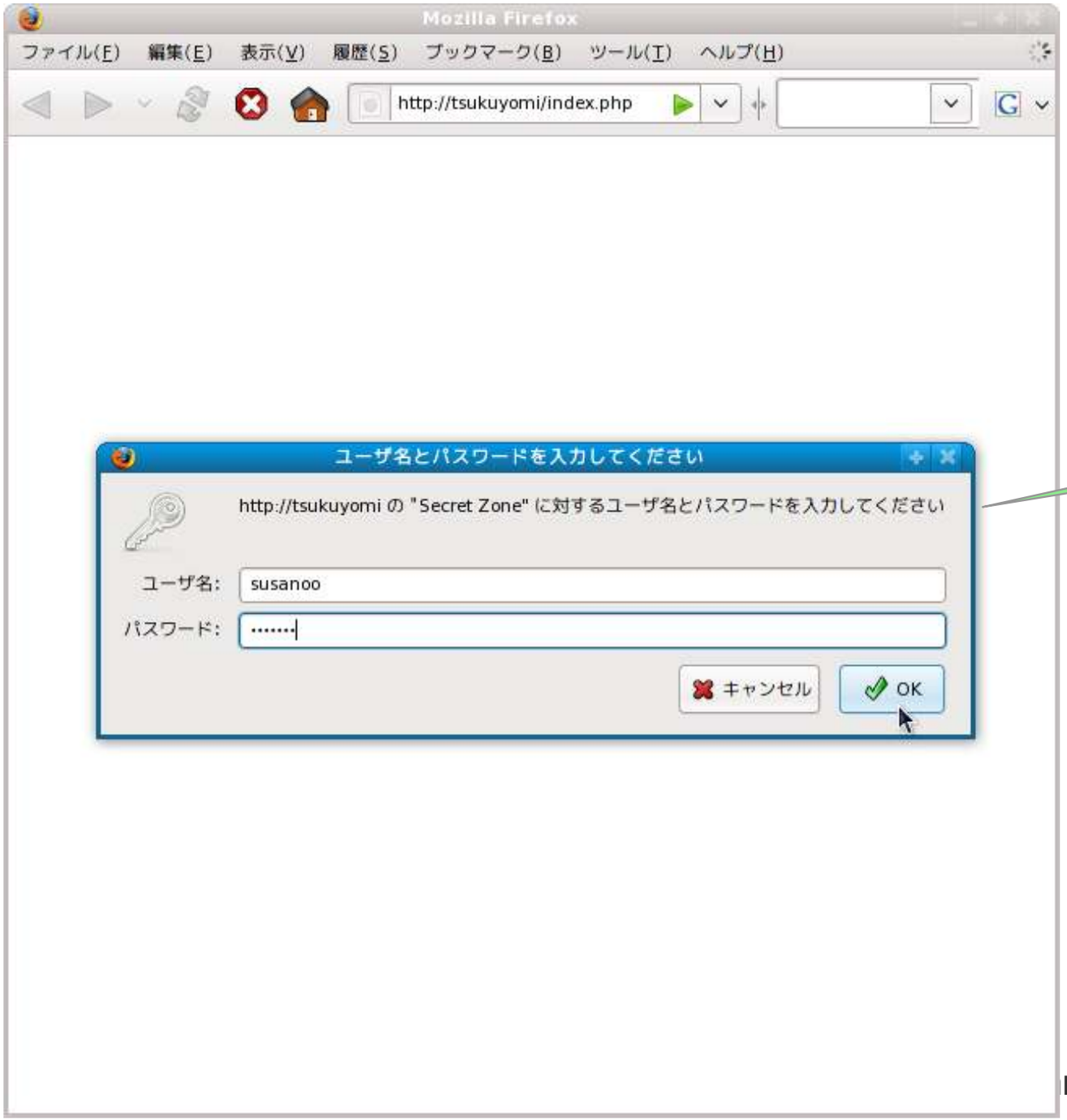


Apache/SELinux plus

- Apache/SELinux plus



LAPP/SELinuxの動作例



ユーザの認証

LAPP/SELinuxの動作例

SELinux awared Apache example - Mozilla Firefox

ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

http://tsukuyomi/index.php

HTTP Authenticated user: **susanoo**
Security Context: **system_u:system_r:httpd_t:s0:c0.c2**

The result of:

SELECT security_context, * FROM food

security_context	id	name	price
unconfined_u:object_r:sepgsql_fixed_table_t:s0	1	shijimi	300
unconfined_u:object_r:sepgsql_fixed_table_t:s0	2	shirauo	400
unconfined_u:object_r:sepgsql_fixed_table_t:s0:c0	3	moroge-ebi	350
unconfined_u:object_r:sepgsql_fixed_table_t:s0:c0	4	amasagi	400
unconfined_u:object_r:sepgsql_fixed_table_t:s0:c1	5	unagi	550
unconfined_u:object_r:sepgsql_fixed_table_t:s0:c1	6	koi	600
unconfined_u:object_r:sepgsql_fixed_table_t:s0:c2	7	suzuki	600

SELECT security_context, * FROM f

Static Contents with Category

- "shijimi" labeled as s0
- "shirauo" labeled as s0
- "moroge-ebi" labeled as s0:c0
- "amasagi" labeled as s0:c0
- "unagi" labeled as s0:c1
- "koi" labeled as s0:c1
- "suzuki" labeled as s0:c2

カテゴリが **c0 ～ c2** のユーザ

カテゴリ **c0, c1, c2** の DBのデータが表示される

カテゴリ **c0** の画像

カテゴリ **c1** の画像

LAPP/SELinuxの動作例

SELinux awared Apache example - Mozilla Firefox

ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

http://tsukuyomi/index.php

HTTP Authenticated user: **ookuninushi**
Security Context: **system_u:system_r:httpd_t:s0:c0**

The result of:

SELECT security_context, * FROM food

security_context	id	name	price
unconfined_u:object_r:sepgsql_fixed_table_t:s0	1	shijimi	300
unconfined_u:object_r:sepgsql_fixed_table_t:s0	2	shirauo	400
unconfined_u:object_r:sepgsql_fixed_table_t:s0:c0	3	moroge-ebi	350
unconfined_u:object_r:sepgsql_fixed_table_t:s0:c0	4	amasagi	400

SELECT security_context, * FROM food

Static Contents with Category

- "shijimi" labeled as s0
- "shirauo" labeled as s0
- "moroge-ebi" labeled as s0:c0
- "amasagi" labeled as s0:c0
- "unagi" labeled as s0:c1
- "koi" labeled as s0:c1
- "suzuki" labeled as s0:c2

カテゴリが **c0** のみのユーザ

カテゴリ **c0** のみのDBのデータが表示される

カテゴリ **c0** の画像

カテゴリ **c1** の画像

SELinuxとTOMOYO Linuxの最近の動向
～ TOMOYO Linux ～

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

TOMOYO Linux

- Linuxカーネルのメインラインへ
- NTTデータのTOMOYOチームの活動
  - 2007年からメインライン化への活動が始まる
  - LKMLへ15回の提案を行ったほか、海外での多数の講演により、Linuxコミュニティで認知される
  - 2009年2月、James Morrisのツリー、およびLinux-nextにマージされる
  - 2009年3月、Linus Torvaldsのツリーにマージされる
  - 2009年4月、Linux-2.6.30-rc1としてリリース
- Linux-2.6.30のリリースは、2009年6月末の予定

Japan Secure Operating System Users Group

TOMOYO Linux

- メインライン版 (LSM対応版: バージョン2.2.x)
  - ファイルに対するアクセス制御・学習のみ（今後拡充予定）
  - 2.6.30カーネルに搭載予定
- フル機能版 (独自フック版: バージョン1.6.x)
  - 2.4系カーネルにも対応
  - SELinuxとの共存が可能
  - JNSAのWebサーバで稼働中
    - JNSA: NPO 日本ネットワークセキュリティ協会　http://www.jnsa.org/

さいごに

日本セキュアOSユーザ会

Japan Secure Operating System Users Group since 2007

Japan
Secure Operating System
Users Group

まとめ

- セキュアOSの基本
  - ポリシーに基づく「強制アクセス制御」と「最少特権」
- インストールなど利用しやすさや情報量などから、最初は SELinux や TOMOYO Linuxがお勧め
  - 多くのディストリビューションで採用されている SELinux
    - LAPP/SELinuxにより、セキュアOSの守備範囲が広がりました
  - 日本発で、日本語での情報・サポートのあるTOMOYO Linux
    - メインライン化すると、今よりさらに気楽に利用できるでしょう

これを機会にセキュアOSを使ってみてください

Japan Secure Operating System Users Group

参考

- 日本セキュアOSユーザ会　http://www.secureos.jp/
- SELinux
  - NSA（アメリカ国家安全保障局）のSELinuxサイト
    http://www.nsa.gov/research/selinux/
  - Fedora SELinux User Guide
    http://docs.fedoraproject.org/selinux-user-guide/
- TOMOYO Linux
  - オフィシャルサイト　http://tomoyo.sourceforge.jp/
  - はてなキーワード
    http://d.hatena.ne.jp/keyword/TOMOYO Linux
  - 2ch「【本家まで】TOMOYO Linux 0.0.3【もう一息】」スレ
    http://pc11.2ch.net/test/read.cgi/linux/1239030346/

日本セキュアOSユーザ会

- about us
  - セキュアOS技術を中心としたセキュリティ技術全般に関心のある人々による、情報交換・交流・議論のためのコミュニティ
    - Web site : http://www.secureos.jp/
    - Mailing List : users-ml@secureos.jp
  - セキュアOS塾
    - 3～4ヶ月に一回程度の勉強会
    - 平日夜/東京都内 + 懇親会
    - 次回　セキュアOS塾 - 03
      - 2009年5月28日（木）
      - ライトニングトーク 3本
      - SELinuxを使ってみる入門BoF

セキュアOS塾 – 01 の様子
(2008/10/29)

ありがとうございました

日本セキュアOSユーザ会

Japan Secure Operating System Users Group since 2007