もうSELinuxは怖くない！

～セキュアLinux徹底解説～

セキュアOSユーザ会　海外浩平 <kaigai@kaigai.gr.jp>

本日のテーマ

もうSELinuxは怖くない！～セキュアLinux徹底解説～

現在、SELinuxはRedHatやFedoraをはじめ多くのディストリビューションに搭載されており、Linuxシステムのセキュリティを考える上で、必要不可欠なコンポーネントとなっています。
本セミナーでは、Linuxのセキュリティ機能の全体像と、その中でSELinuxの果たす役割/意義/機能について、原点に立ち戻ってご紹介します。

- セキュリティを考える上での原点
  - “資産”と”脆弱性”
  - 何をすれば、セキュリティは保たれているのか？
- セキュリティの基本です
  - “基本” ですが ”初歩” ではないかもしれません。
- ☑ セキュリティの考え方とSELinux
- ☑ で、SELinuxって”アリ”なの？

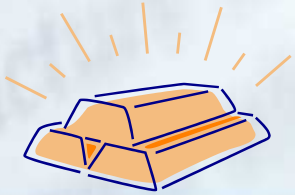
セキュリティの考え方とSELinux

セキュリティの”目的”

- なぜセキュリティは必要なのか？
  - 守るべき資産が存在する
  - 資産に対する脅威が存在する

  ⇩
  - セキュリティとは、資産を脅威から保全するための**手段**
- 別の言い方をすると…。
  - 資産が (or 脅威が) 無ければ、セキュリティは不要
  - セキュリティ対策費用が、資産価値を上回ってはナンセンス



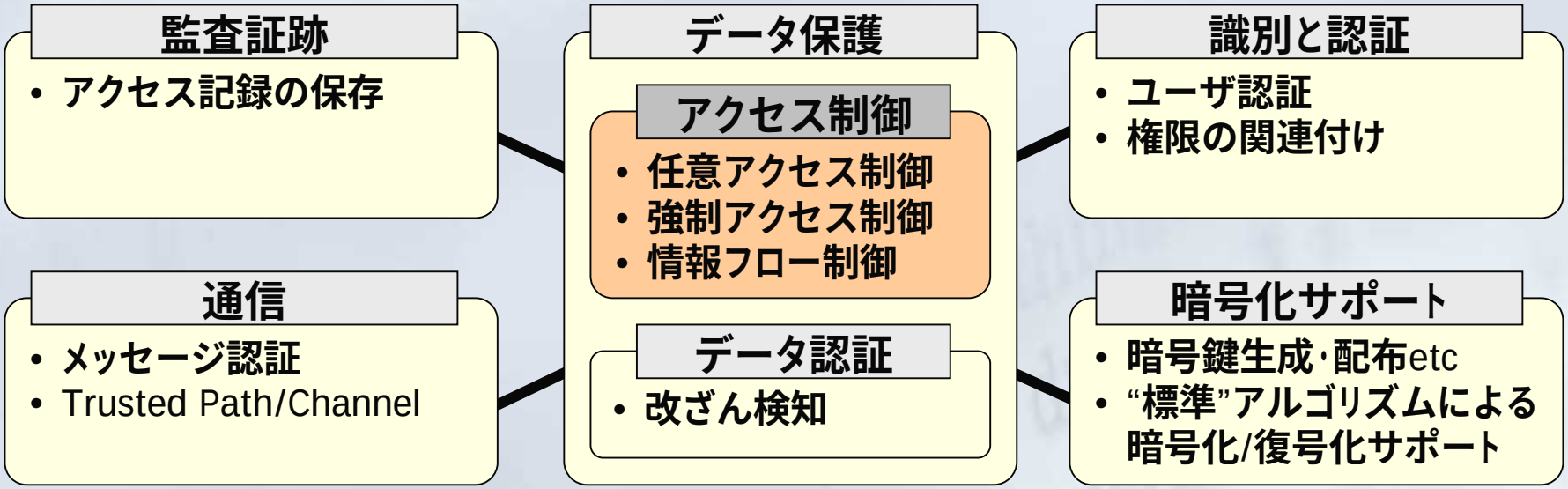


情報セキュリティ

- コンピュータの世界に話を絞ると
  - 資産：　情報システム、情報資産
  - 脅威：　"情報資産"が流出してしまう
    "情報システム"が利用できなくなってしまう
    ・・・などなど。
- そもそも、セキュリティが保たれている状態とは？
  - 機密性　…権限のない人は、情報を読み出せない
  - 完全性　…権限のない人は、情報を更新できない
  - 可用性　…必要な時に、必要な情報にアクセスできる
  - この3つが保たれている状態の事をいう
- どうやって？

セキュリティ技術の分類

- ISO/IEC15408の機能要件を元に分類
  - IT製品のセキュリティを評価・認証するための仕組み
  - SELinuxは "アクセス制御" を担当する

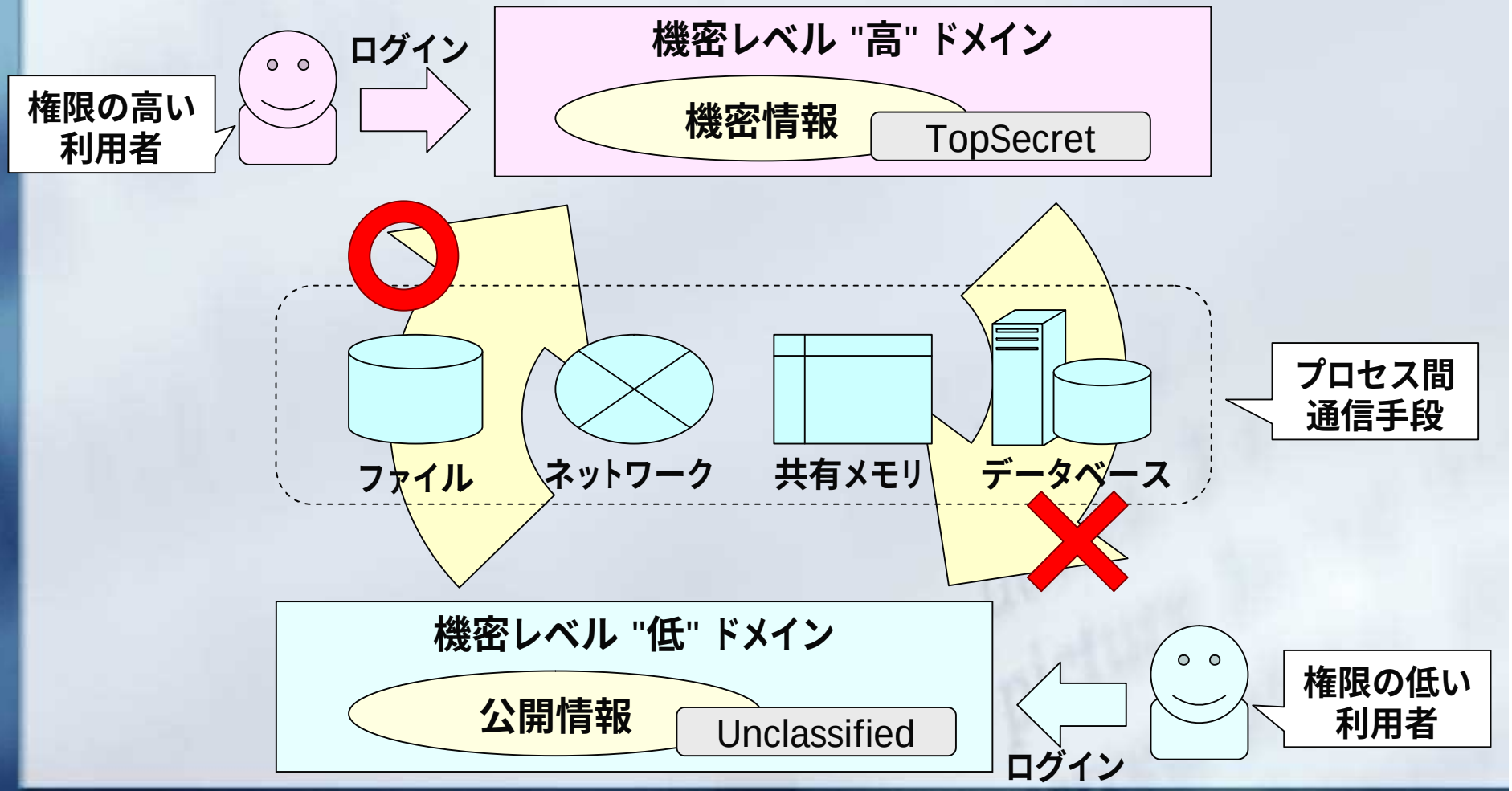


アクセス制御って…？

- 目的
  - 正当な権限のある人だけに、システム管理下の資源へのアクセスを許可する
- DAC: 任意アクセス制御
  - 伝統的なUNIXパーミッション
    - 資源のオーナーによるアクセス権の設定
    - 全知全能のroot
- MAC: 強制アクセス制御
  - SELinuxなどが提供するアクセス制御方法
    - rootも含む、全ユーザにセキュリティポリシーを適用
    - 資源のオーナーであっても、アクセス権を変更できない
  - 情報フロー制御の前提条件

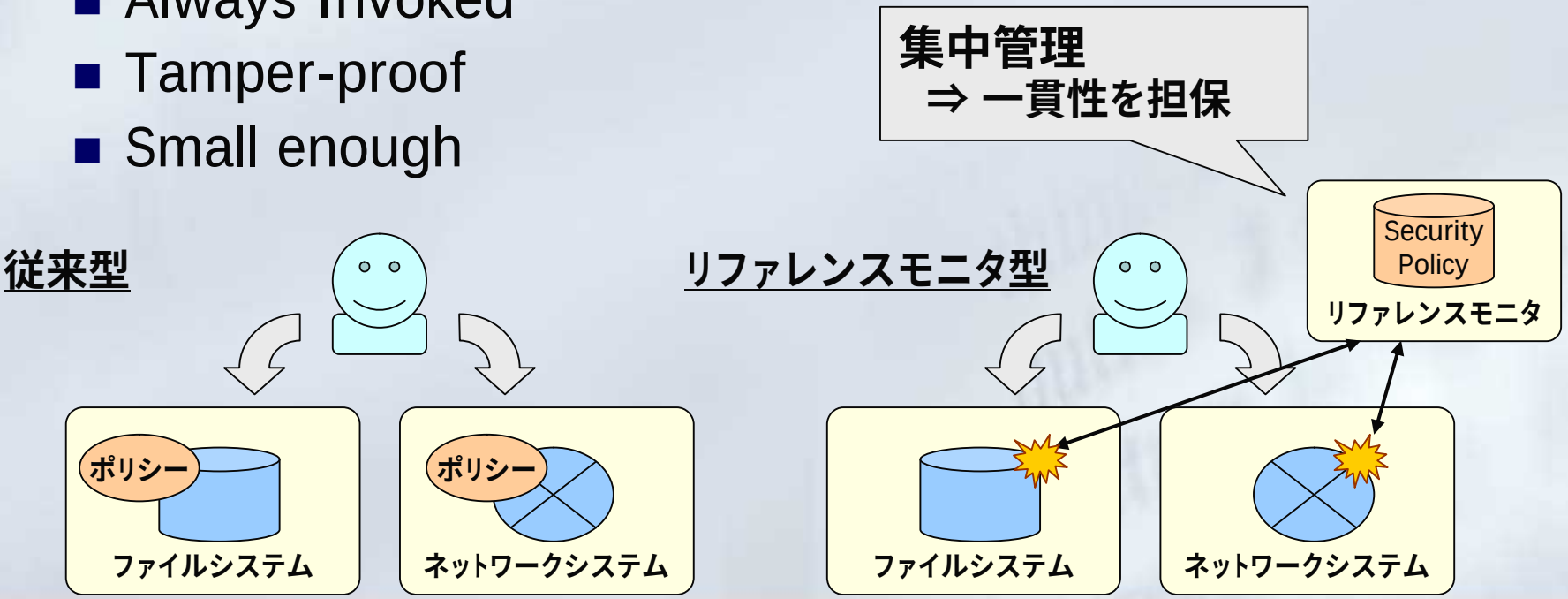
情報フロー制御

- 機密レベル “低” ⇒ “高” への情報の一方通行



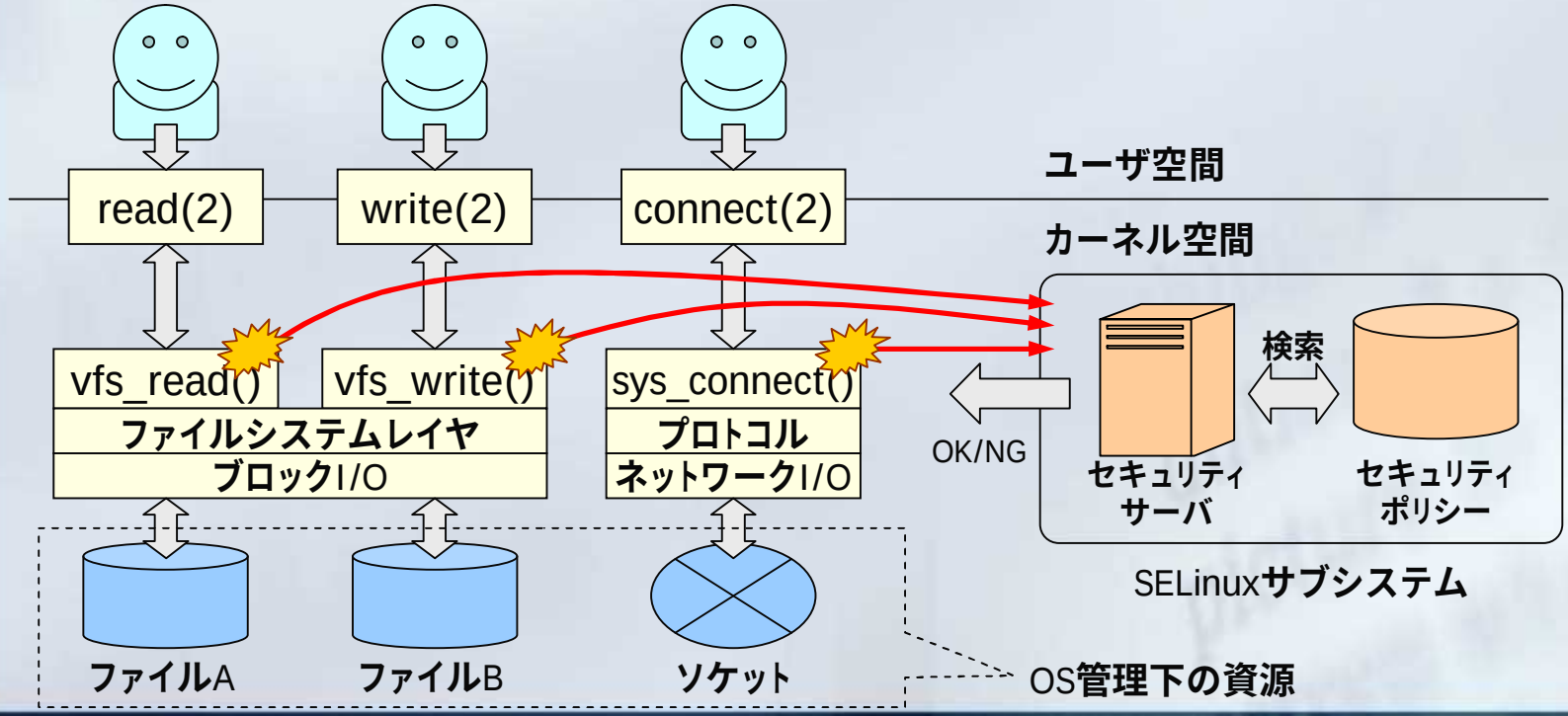
リファレンスモニタ

- 機能
  - ユーザが資源にアクセスする時に、これを”漏れなく”捕捉
  - セキュリティポリシーに従って、これを許可/禁止する
- 必要な性質
  - Always Invoked
  - Tamper-proof
  - Small enough



SELinuxとは

- Linuxにおけるリファレンスモニタの実装
  - ”資源”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” 呼出をフックすれば、全ての資源に対するアクセスを捕捉できる

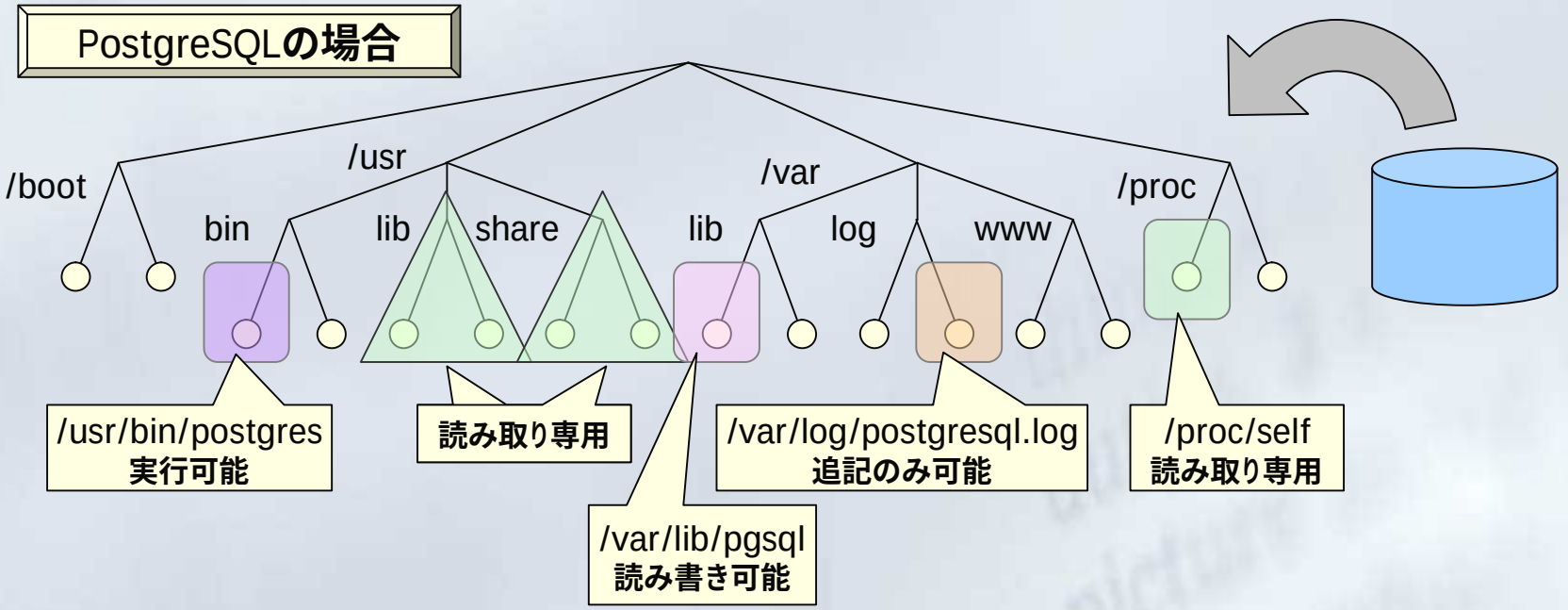


SELinuxのアクセス制御方式

- じゃあ、どうやって白黒つけるの？
- アクセス制御モデル
  - TE(Type Enforcement)
    - プログラムのアクセス可能なリソースの範囲に”枠”を作る
      - 操作対象は”枠”の内側か？外側か？
  - MLS(Multi Level Security)/MCS(Multi Category Security)
    - 上下関係を持つ”機密レベル”
    - 包含関係を持つ”機密区分”
      - この2つの制約条件を満たすか、否か？
  - RBAC(Role Based Access Control)
    - TEと密接に関連した方式で、難易度は高め。
    - 今回は説明から外します…。

Type Enforcement

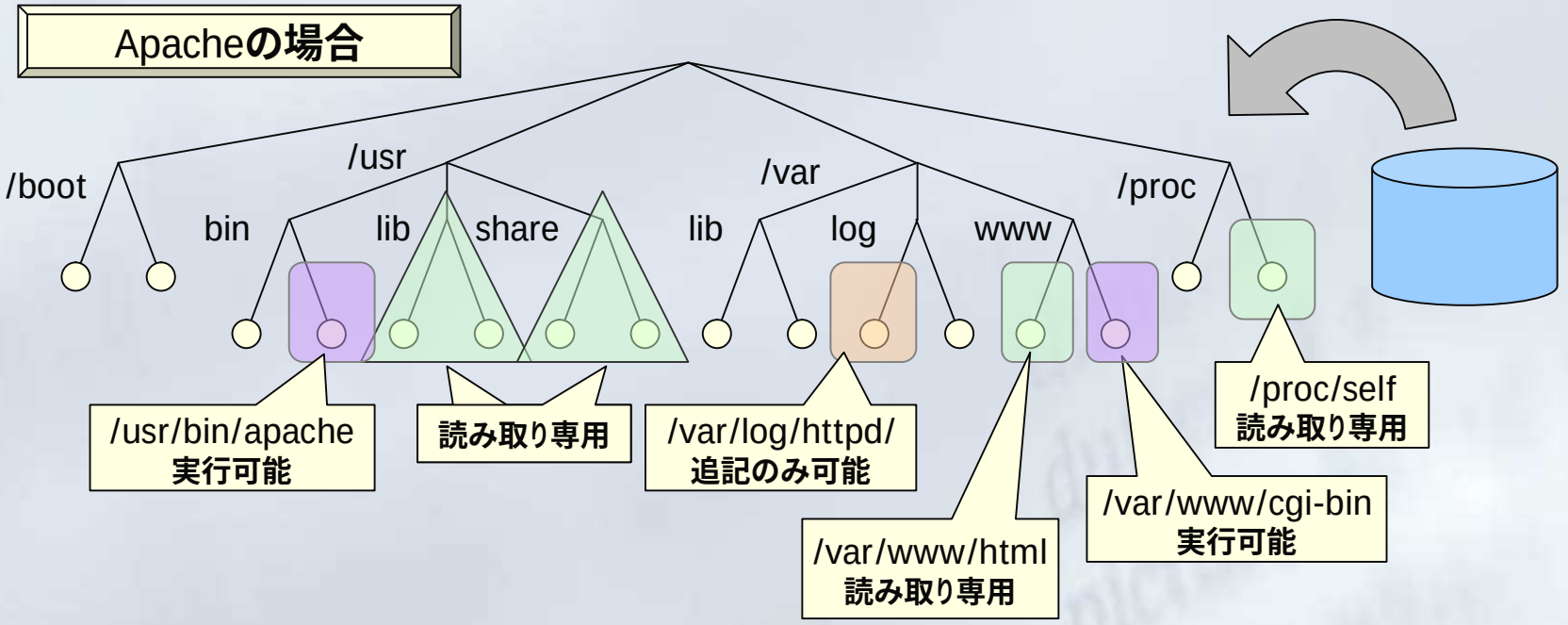
- プログラムごとに、利用可能な資源を絞り込む
  - 保有する"情報資産"を少なくする。
  - クラッカーの"攻撃手段"を少なくする。



※　明示的に許可した資源だけをアクセス可能（ホワイトリスト方式）

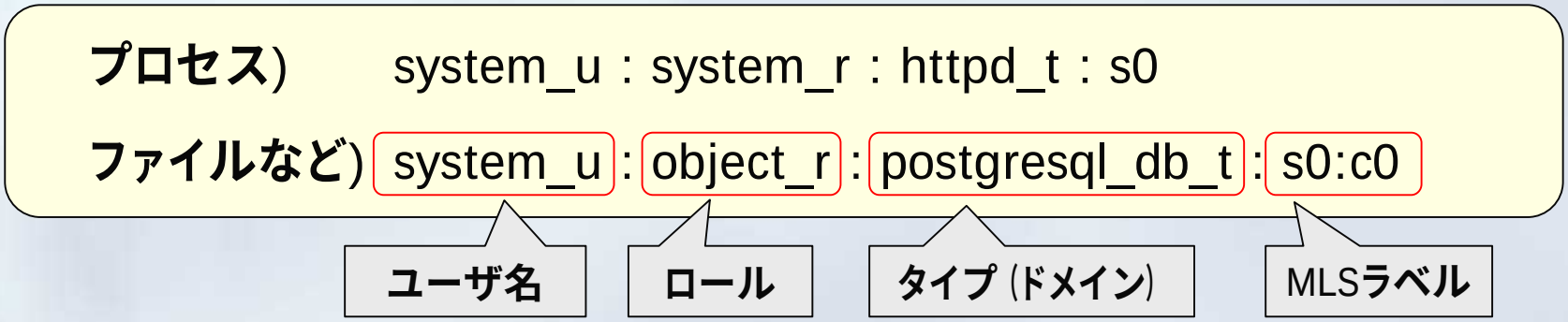
Type Enforcement

- プログラムごとに、利用可能な資源を絞り込む
  - 保有する"情報資産"を少なくする。
  - クラッカーの"攻撃手段"を少なくする。



※　明示的に許可した資源だけをアクセス可能（ホワイトリスト方式）

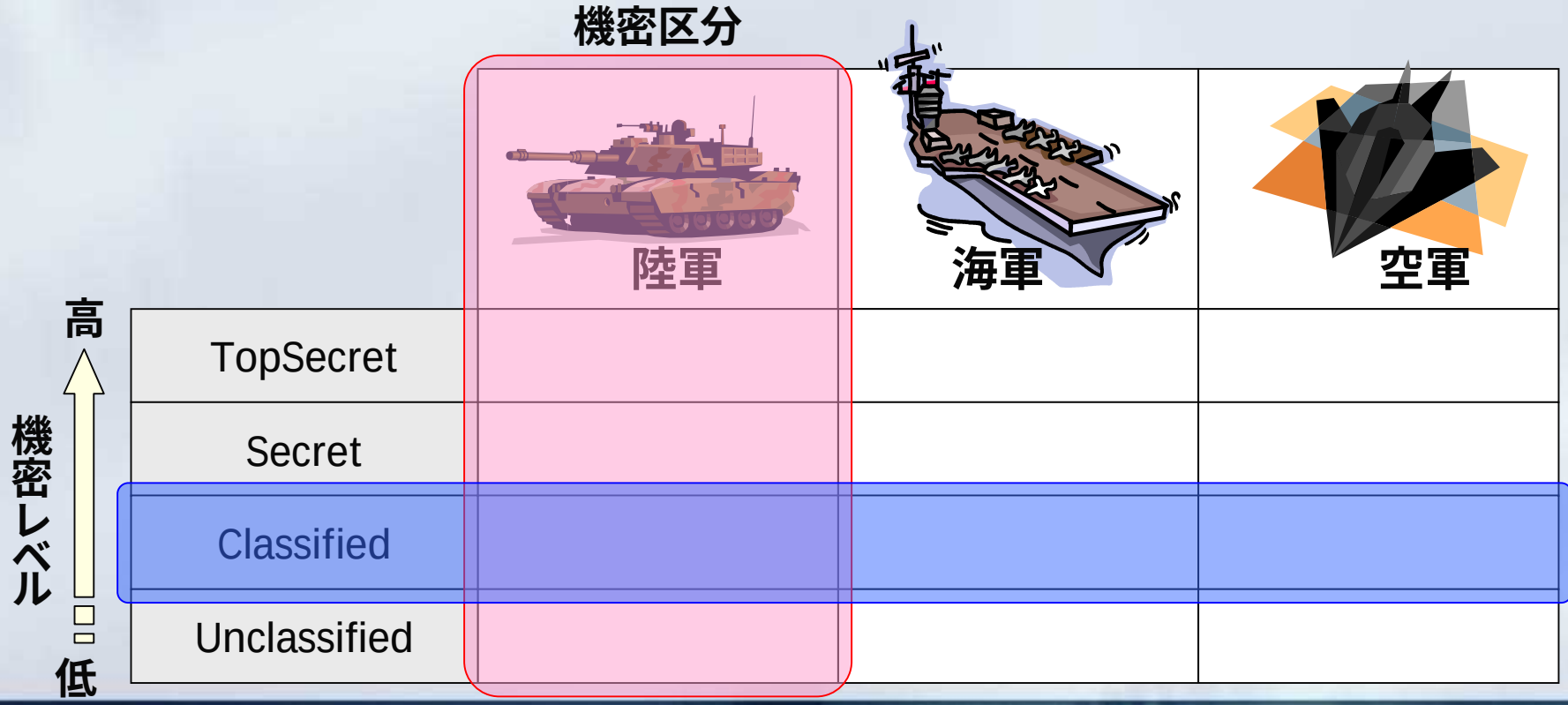
セキュリティコンテキスト



- タイプ／ドメイン
  - プロセスの場合には「ドメイン」と呼びます
  - あるドメインから見て「読み取り専用」「追記のみ可能」etc...を示す識別子
  - この辺の対応関係は、全てセキュリティポリシーで記述されている
- MLSラベル
  - 機密レベルと機密区分を示す
  - 軍用システムに由来する、最も伝統的な”強制アクセス制御”

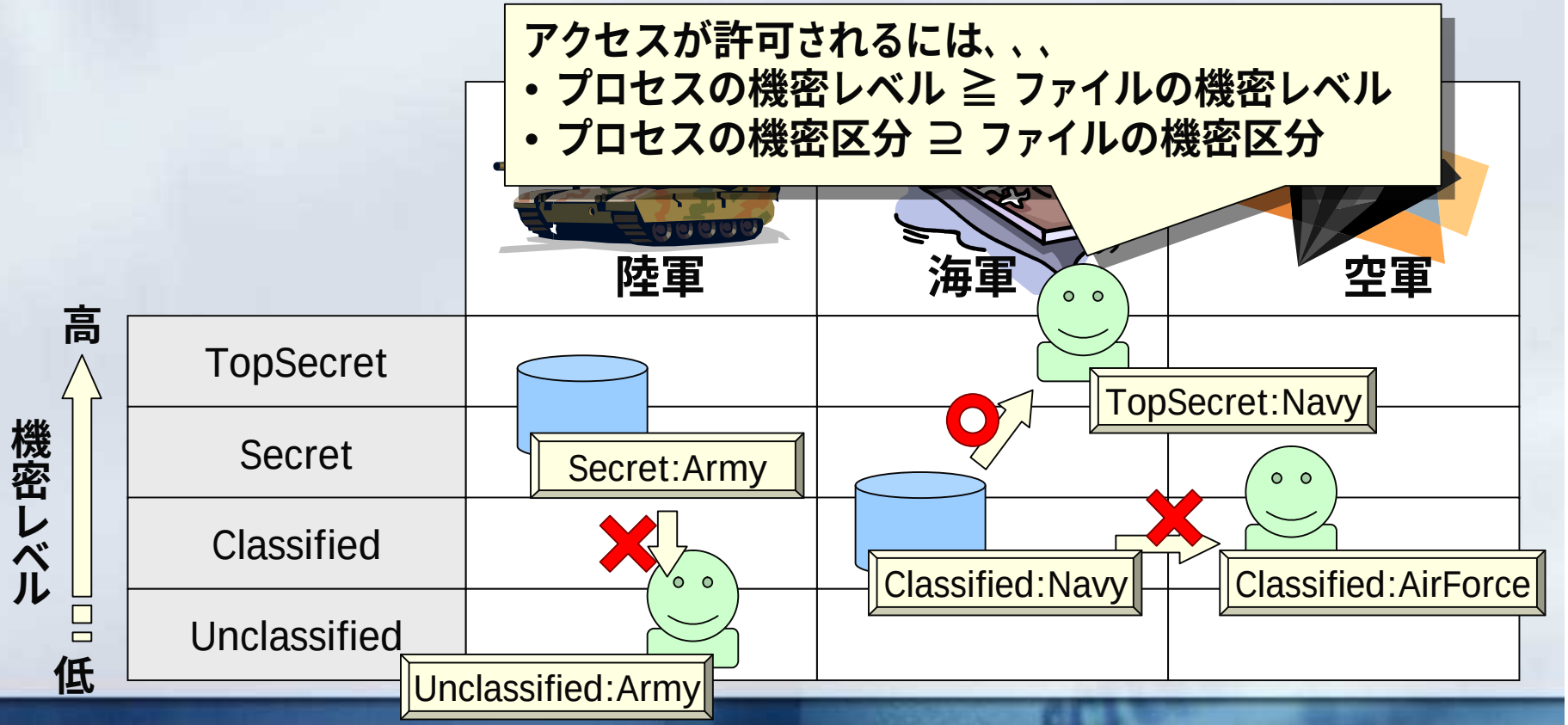
Multi Level/Category Security

- "情報の流れ"を制御する
  - 『機密レベル』の高い情報を、低い所へ流さない
  - 『機密区分』の壁を越えて情報を流さない



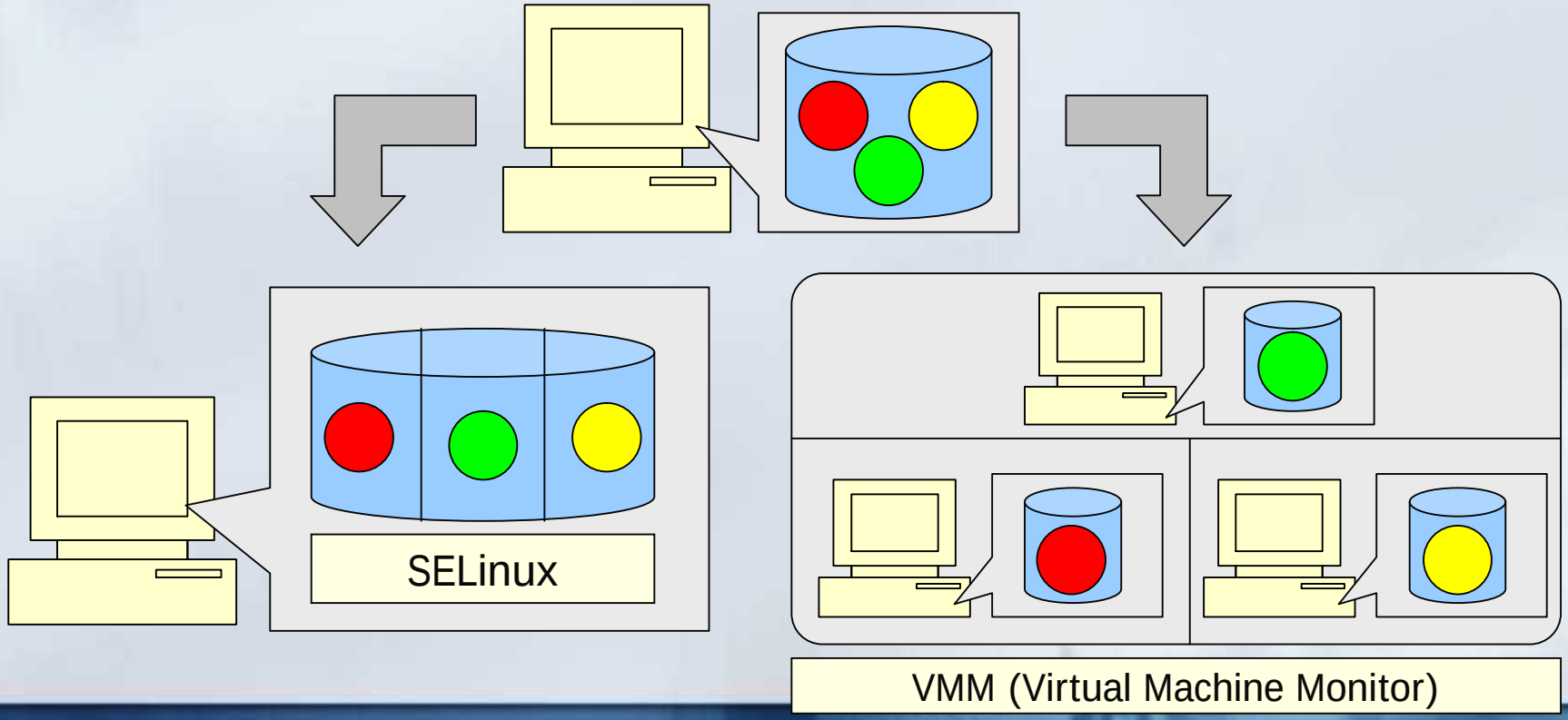
Multi Level/Category Security

- "情報の流れ"を制御する
  - 『機密レベル』の高い情報を、低い所へ流さない
  - 『機密区分』の壁を越えて情報を流さない



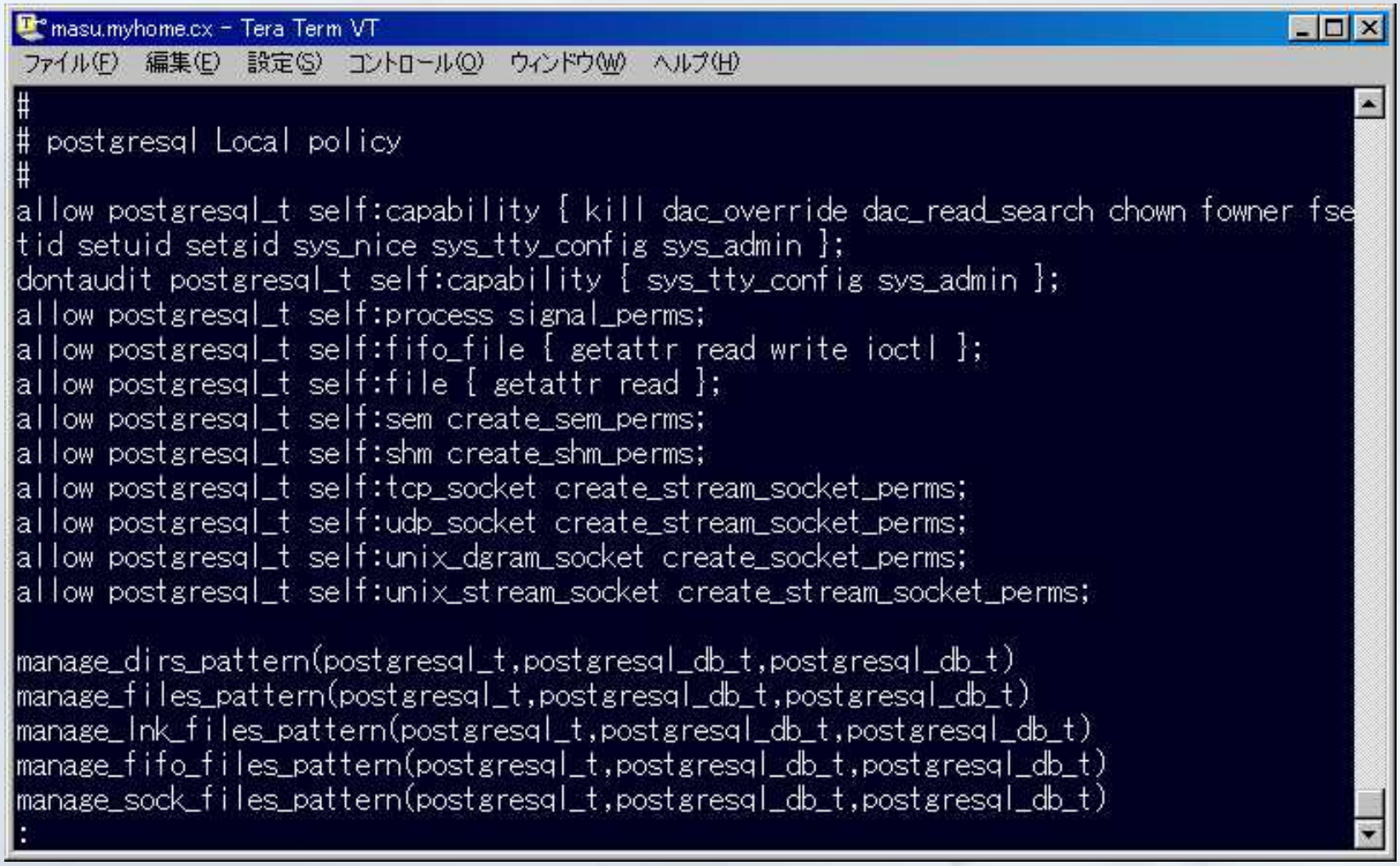
結局、どういう事？

- 同じ領域に、沢山の情報資産を置かないようにする。
  - 仮想化アプローチと発想は同じ
  - ✓ 分割の単位が細かいか、荒いかという違い
  - ✓ 従来のサーバ管理の手法を適用できるか、否かという違い



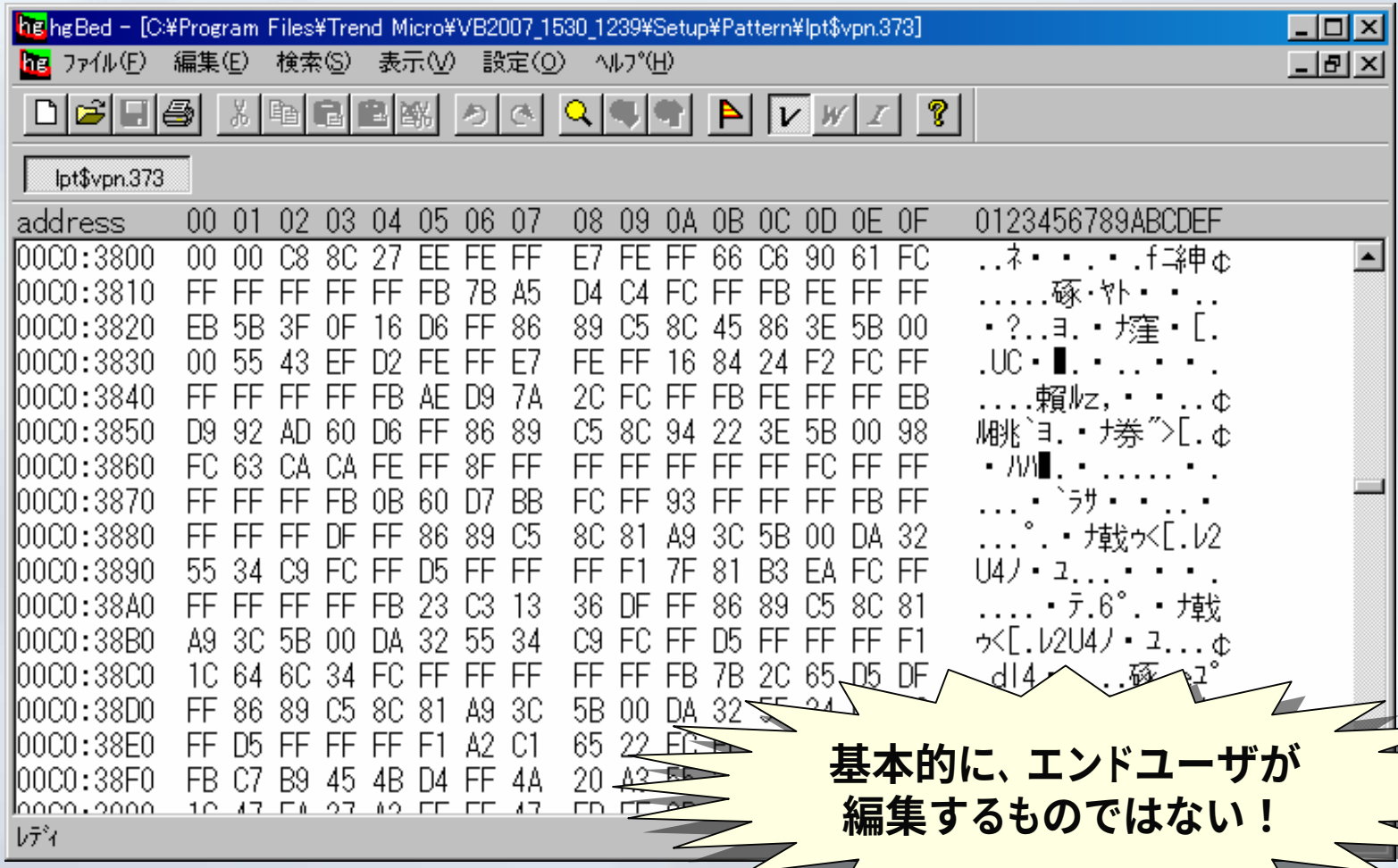
で、SELinuxは”アリ”なのか？

ポリシーの作成が難しい…？



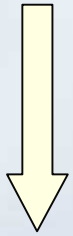
ポリシーの作成が難しい…？

- ↓某社アンチウイルスソフトのパターンファイル



SELinuxポリシー体系

- **3種の異なるポリシー**
  - Targeted Policy
  - Strict Policy
  - MLS Policy



ぬるい

厳しい

- Targeted Policy
  - FedoraやRedHatEL、CentOSでの標準ポリシー
  - ユーザのシェルなどは今まで通り
    - 全部許可する = unconfinedドメイン
  - 特定のサーバプロセスだけを保護
    - 対象を絞っている = Targeted

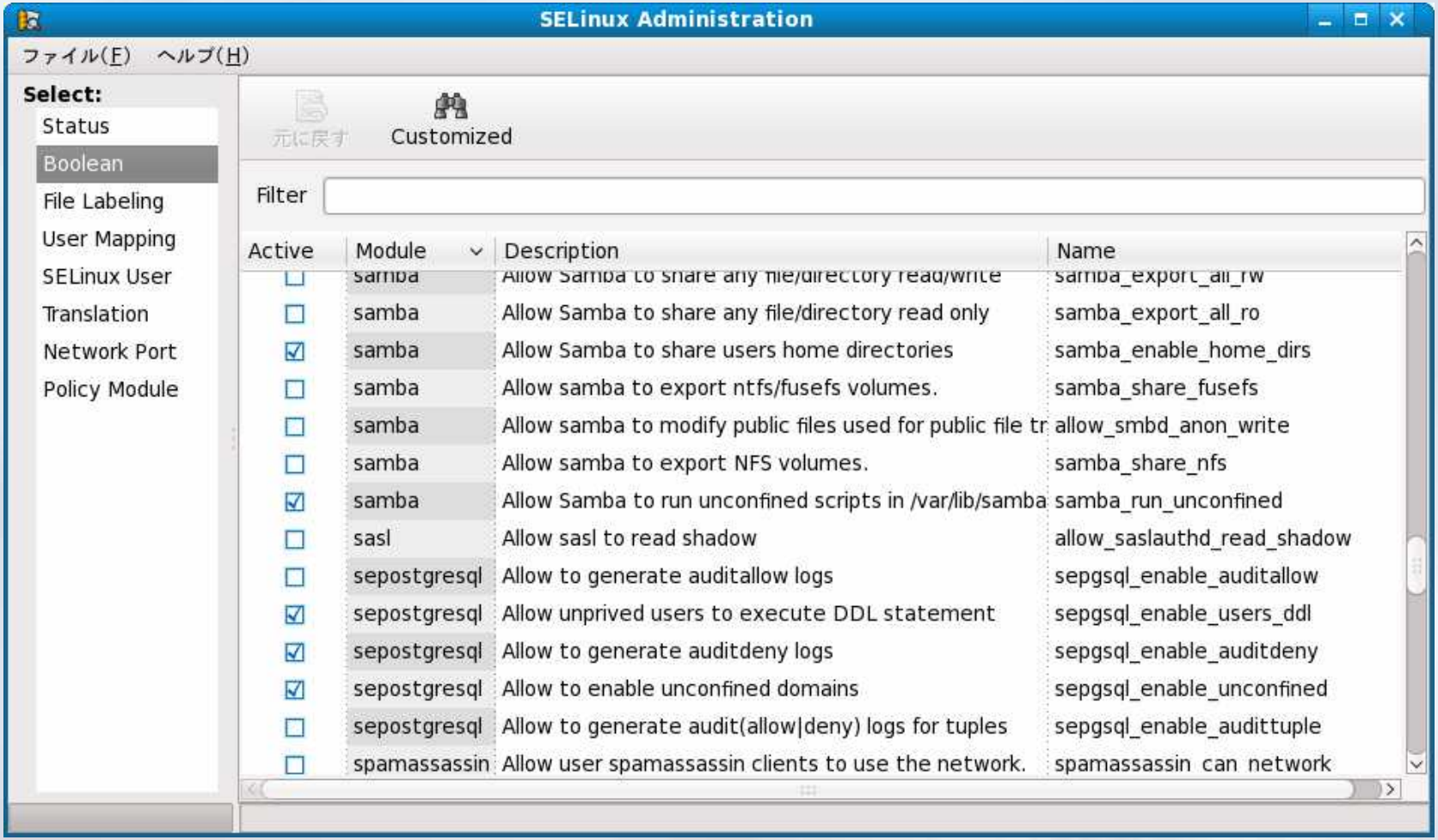
SELinuxの"カスタマイズ"

- booleanの変更
  - boolen
    =セキュリティポリシーの一部を有効化/無効化するためのスイッチ
  - 意味のあるまとまりを単位としてポリシーを修正できる
- ファイルの”タイプ”を変更する
  - 標準のインストールパスを変更
  - 『読み込み専用』→『読み書き可能』へ属性を変更
- MCSを利用する
  - 独自の”機密区分”を設定する事ができる
  - 人に読みやすい"別名"を付ける事ができる

- system-config-selinuxで設定できるんです。

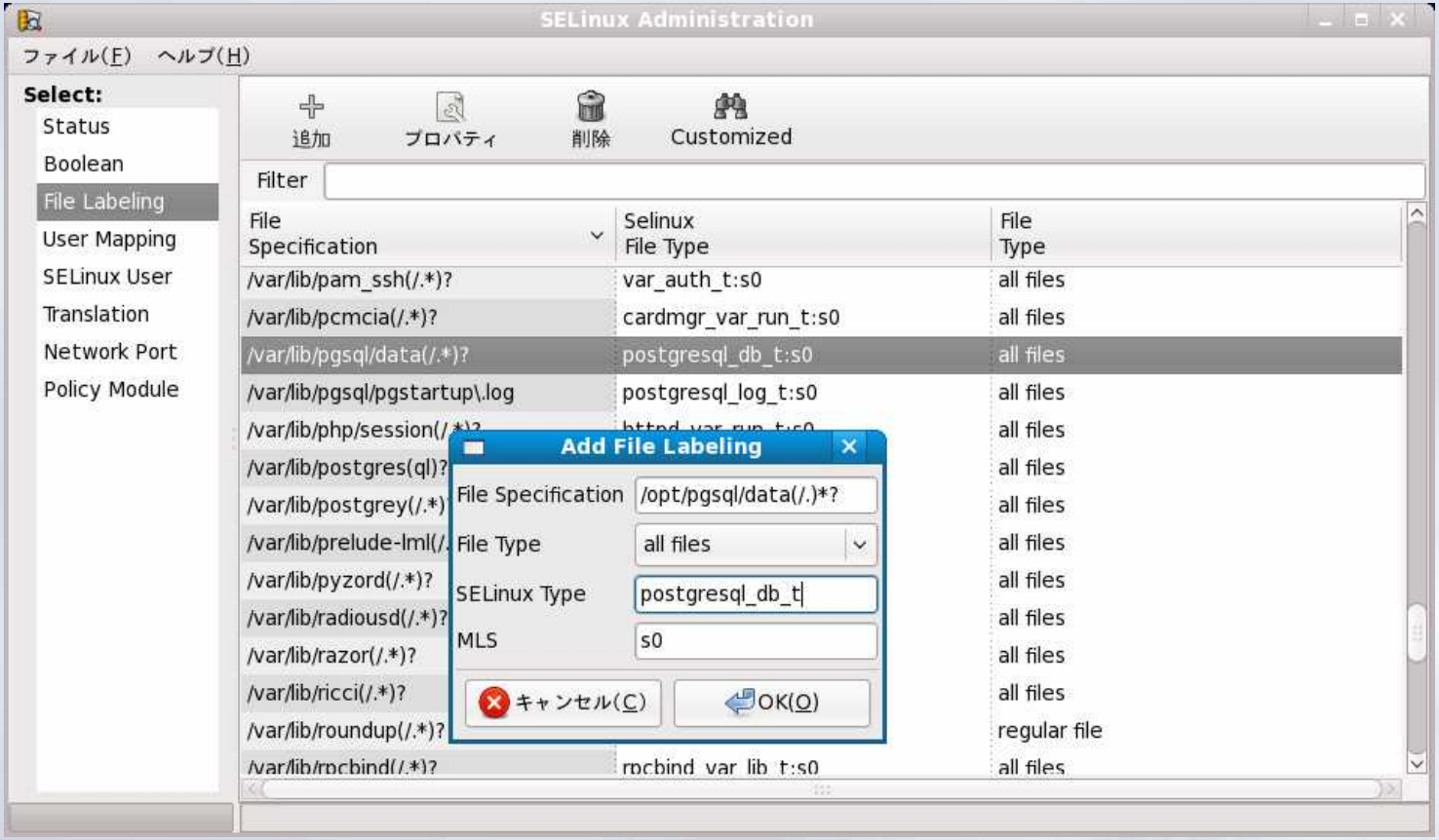
system-config-selinux

- GUIでbooleanのカスタマイズが可能



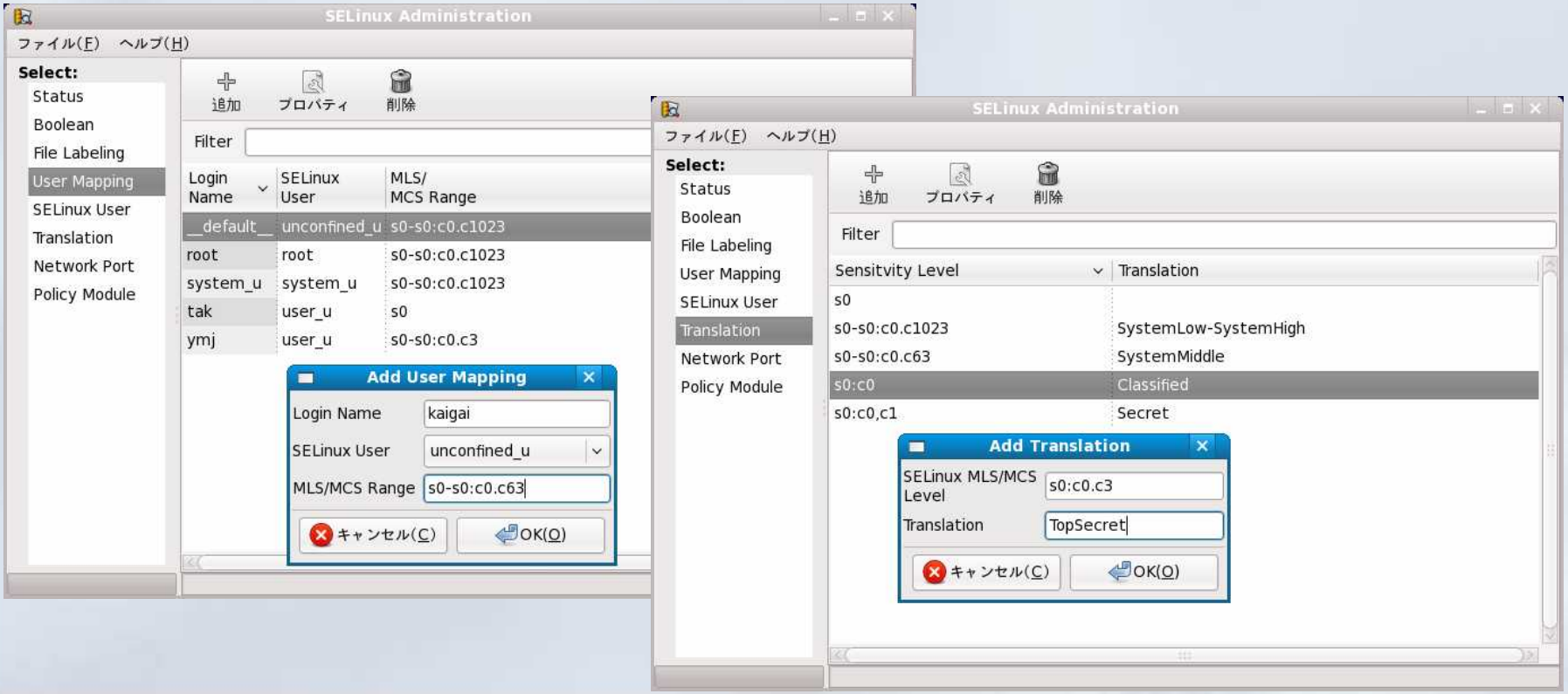
system-config-selinux

- ファイル/ディレクトリの"タイプ"を変更することができる
  - 標準のインストールパスを変更する
  - 『読み込み専用』→『読み書き可能』なタイプに変更する



system-config-selinux

- 各ユーザの"機密区分"を指定できる
- "機密区分"に、読みやすい名前を付けることも可能
  - 『s0:c0.c3』なら『TopSecret』という具合



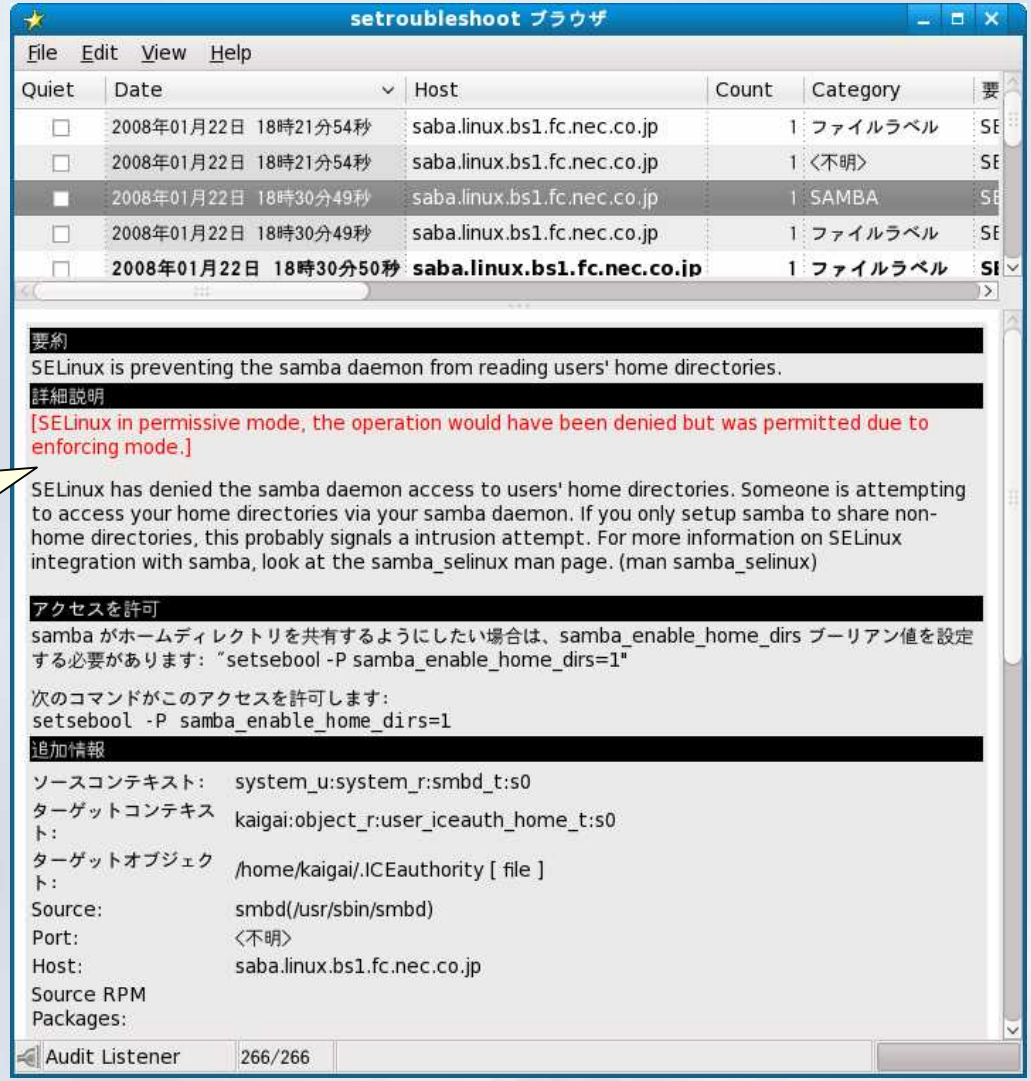
SELinuxでトラブルに遭ったら？

- setroubleshoot
  - ログを解析して、トラブル解決のためのヒントを提示
- **ポリシーモジュールの自動生成**
  - **“最終手段”、ポリシーの修正。**
- **詳しい人に聞いてみよう**
  - **ユーザコミュニティのご紹介**

setroubleshoot

既知の問題点であれば、DBの中から予想される対処方法を検索し、ユーザに提示する。

何かSELinuxが"アクセス拒否"をした場合、ポップアップで通知



ポリシーモジュールの自動生成

(警告) これは最終手段です

cat /var/log/audit/audit.log | **audit2allow** -m hoge -o hoge.te

Auditログから、SELinuxアクセス拒否を抽出
⇒ 拒否されたパターンを"全て許可"するポリシーを自動生成

checkmodule -m -M -o hoge.mod hoge.te

生成されたポリシーを、モジュールとしてビルド(-m)
-MでMLS/MCSを有効化

semodule_package -o hoge.pp -m hoge.mod

ビルドされたポリシーを、Policy Package形式に変換

semodule -i hoge.pp

Policy Packageをインストール

一番手っ取り早い方法

- 詳しい人に聞く。
- selinux-users@selinux.gr.jp には、
  詳しい人が沢山居ます。

- 質問するときのヒント
  - よく分からないけど動かない！→ ×
  - こんな情報を付けてくれると嬉しいです。
    - ディストリビューションの種類
    - /var/log/audit/audit.log の内容
    - selinux-policy のバージョン
    - sestatus –a、getsebool –a、semodule -l の出力結果

まとめ

- セキュリティの考え方
  - “脆弱性” と ”情報資産”
  - SELinuxは ”アクセス制御” を強化するための機能
  - OSの中に壁を作ることで、
    - 区画（ドメイン）の持つ”情報資産”を減らします
    - 攻撃に使える道具を縛ることで”脆弱性”を減らします
  - そのためのモデルが、TEやMLS/MCS、RBAC
- SELinuxってどうよ？
  - 発想を転換しよう
    - ポリシーを書くのは難しい？ ⇒ 自分で書くから難しい
  - カスタマイズ　　... system-config-selinux
  - トラブルの手助け ... setroubleshoot、audit2allow
  - 最後に頼りになるのは？
    - 日本語で質問できるユーザコミュニティ

質問タイム

Any Question?

業務連絡

- セキュアOSユーザ会ブース (4F) で展示中
  - 組込みSELinux／評価ボード
  - SE-PostgreSQL 8.3対応版
  - SELinuxによるキオスクパソコン

- 引き続き、この教室で下記セミナーが開催されます

「TOMOYO LinuxでLinuxの動きを学びませう」

14:00〜14:45　by 武田健太郎 (NTTデータ)