TOMOYO Linux
タスク構造体の拡張によるセキュリティ強化Linux

平成16年6月3日
株式会社ＮＴＴデータ
技術開発本部
オープンシステムアーキテクチャグループ
原田季栄
haradats@nttdata.co.jp

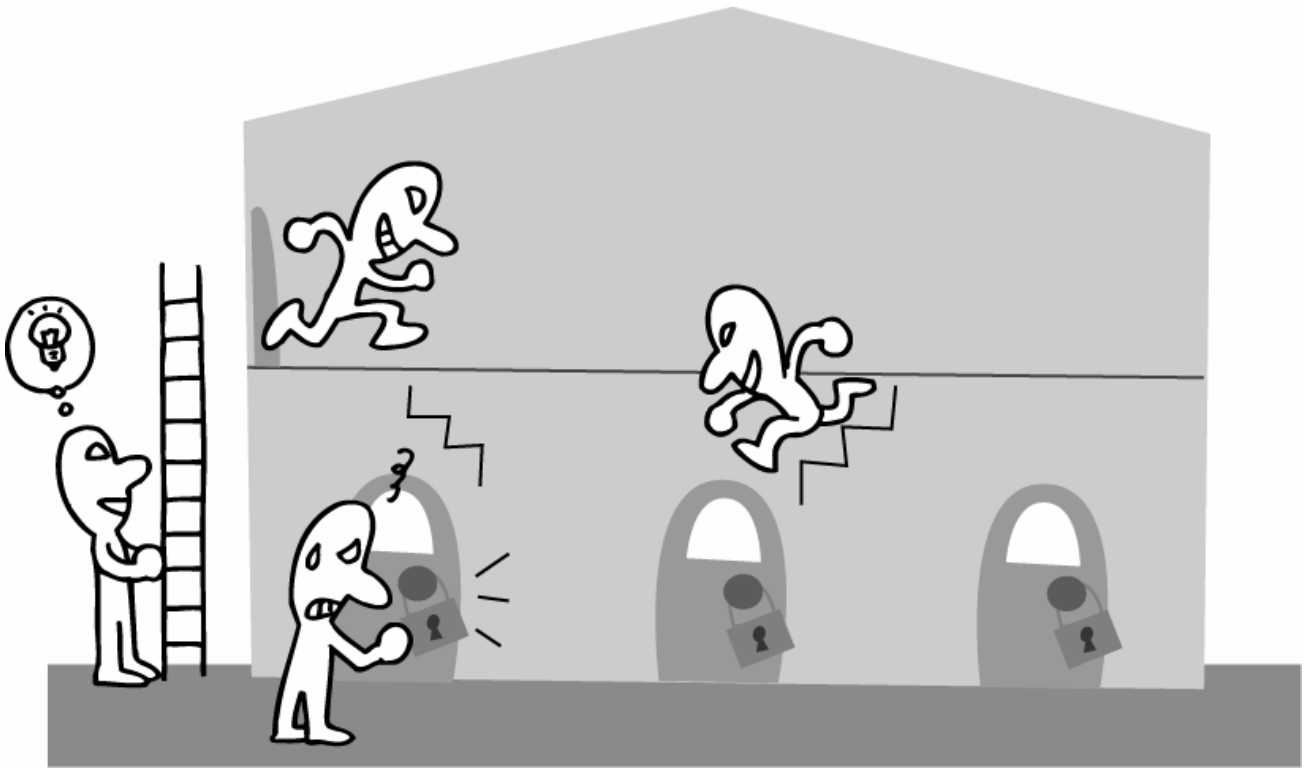
Linux セキュリティ上の課題

「所有者」による「自由裁量」のアクセス制御

粗い分類と、制御の粒度

システム管理者に対しては効力を持たない

システム管理者権限を奪われると歯止め無し



強制アクセス制御 (MAC)

- Mandatory Access Control の略
- DoDが1985年に発令したTCSECの中で、”CLASS (B1): LABELED SECURITY PROTECTION” として記述
  - アクセスの主体 (要求する側) と客体 (要求された側) について
  - 付与された重要性 (sensitivity) のラベルに基づき
  - 「強制的に例外なく」可否を判定する

SELinux

- Security-Enhanced Linux
  - http://www.nsa.gov/selinux/
- ＮＳＡが開発、公開しているセキュリティ強化Ｌｉｎｕｘ
- 特徴
  - 強制アクセス制御をLinuxに実装
  - DTE (Domain Type Enforcement)
    - プログラムの実行状況を「ドメイン」という概念で表現
    - 「ドメイン」毎にアクセス許可を定義し、アクセスを制限する
  - RBAC (Role Based Access Control)
    - 同一ユーザでも役割により異なる権限を与える
  - LSM に対応、2.6カーネルに組み込み済み
  - 非常にきめこまかなアクセス制御を実現できる

SELinuxで問題解決？

- 「適切なポリシー」の策定と運用が現実には困難
- ラベルによるアクセス制御の問題

SELinuxの運用

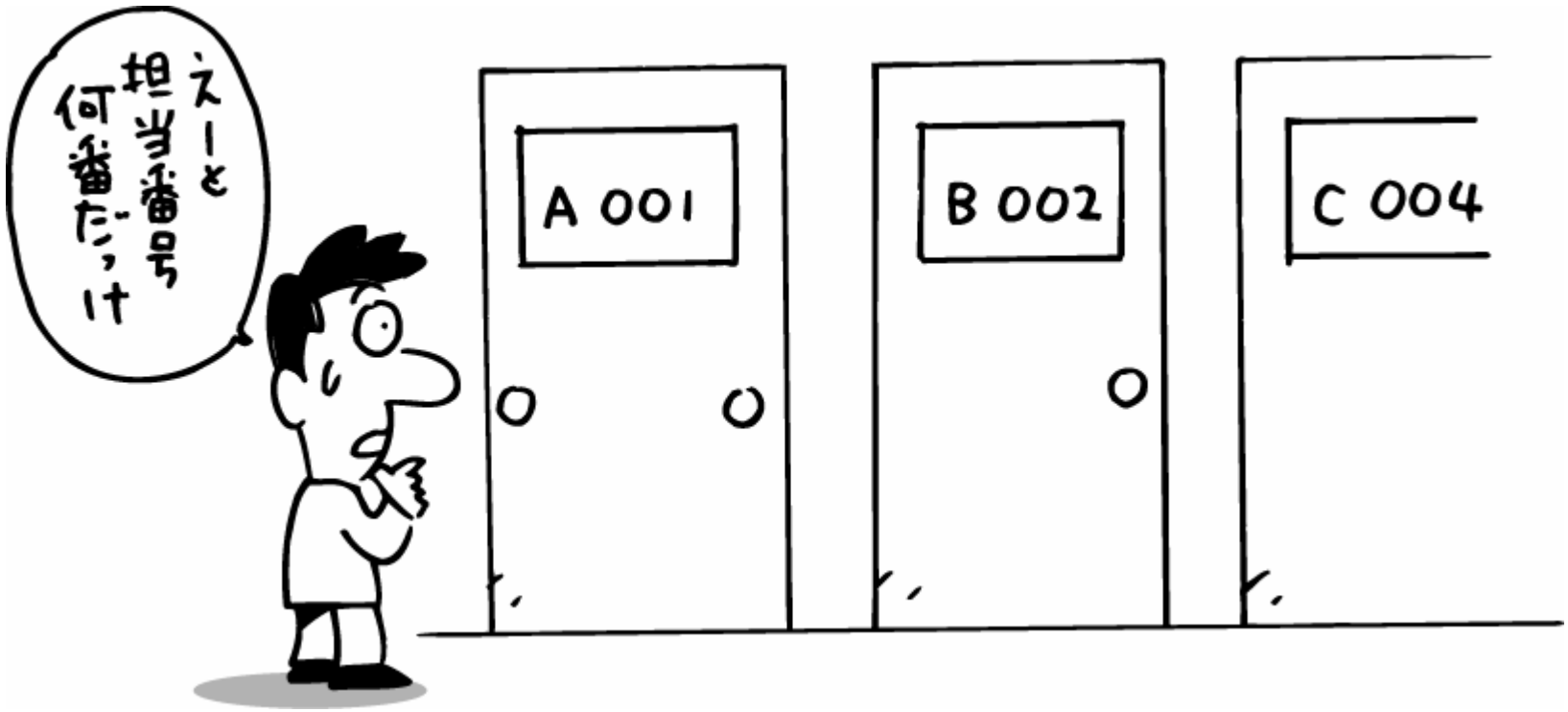
エラーログから必要なアクセス許可を割り出して
ポリシーに追加すれば動作はするのだが・・・

ポリシーを定義するということは

- ポリシーはデフォルトで全てのアクセスを禁止するようになっている。
- 管理者はアプリケーションが動作するために必要なものを全て正確に書き出さなければならない。

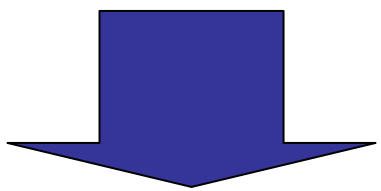
ラベルによるアクセス判定

ユーザが意識するファイル名やディレクトリ名ではなく、それらにつけられた符号（ラベル）によりアクセス可否が判断される。



TOMOYO以前の取り組み

- アクセスポリシー自動生成支援システム
  - JNSA Network Security Forum 2003で発表
    - http://www.jnsa.org/award/2003/result.html
  - 特殊なカーネルにより、
    - プロセス起動履歴と、履歴毎のアクセス要求を記憶
    - 記憶したアクセス要求をファイルに抽出
    - Windows上でGUIエディタを用いて確認、編集
  - 特徴
    - もれがなく、正確なポリシーの策定が可能



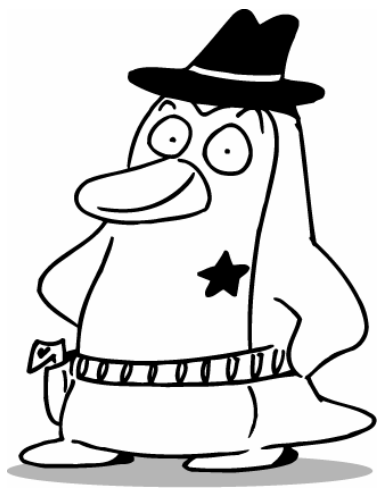
これに強制アクセス制御機能を加えたものが TOMOYO Linux

TOMOYO以前の取り組み

- SAKURA Linux（物理的な改ざん防止）

SAKURAの限界

- 改ざん防止策にはなるが、情報漏洩防止策にはならない
- かといって複雑なポリシーの管理運用はしたくない
- そんなときこそTOMOYOの出番



TOMOYO Linux

- ラベルによらないアクセス許可の付与
  - ファイル名、ディレクトリ名そのままでポリシーを確認、編集
- アクセスポリシーの自動定義機能

- アクセスポリシーに基づく強制アクセス制御
- アクセスポリシーによらない自発的アクセス制御

ラベルによらないアクセス許可

普段意識しているファイル名やディレクトリ名をそのまま使えるから直感的でわかりやすく、間違えない。

ポリシーの自動定義

管理者の手をわずらわせることなく、
必要十分なポリシーが得られる

SAKURAとTOMOYO

「改ざん防止のSAKURA」＋「アクセス制御のTOMOYO」で
簡単ながら強固なセキュリティを実現可能

タスク構造体について

- 今回の強制アクセス制御の実装ではタスク構造体を利用しています。
  - 全てのプロセスが持っている。(プロセスの「名札」として使える)
  - 好きな情報を何でも記録することができる。(「名札」には名前以外も書き込める)
  - 「複製」と「更新」により引き継がれていく。(Linuxのプロセス生成の仕組みを活用できる)

デモ

- **アクセスポリシー自動定義**
- **自動定義された内容に基づく強制アクセス制御**

デモ

- **アクセスポリシーに拠らない自発的アクセス制御**

デモ

- **サーバー機能**

参考文献

- 日経システム構築 2004年4月号 no.132「解説」
  - 「セキュアなシステムを作る（3つの原則に従いOSの機能を強化）」
- 読み込み専用メディア上でのLinuxサーバの運用について
  - 「読み込み専用マウントによる改ざん防止Linuxサーバの構築」
    Linux Conference 2003
    http://lc.linux.or.jp/lc2003/30.html
    原田季栄、保理江高志、田中一男
- 強制アクセス制御のポリシー定義の自動化について
  - 「プロセス実行履歴に基づくアクセスポリシー自動生成システム」
    Network Security Forum 2003
    http://www.jnsa.org/award/2003/result.html
    原田季栄、保理江高志、田中一男
- http://www11.plala.or.jp/tsh/
  - 本資料掲載内容のフォローアップ情報を公開します

special thanks to

- 本資料作成にあたりお世話になった方々に感謝致します。

ＮＴＴデータカスタマサービス　半田哲夫様

NTTデータ経営研究所
NTT Data Institute of Management Consulting, Inc.

CREATION podna クリエイション パドル

AKIRA IGARASHI (illustration)