



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

Global IT Innovator
NTT DATA GROUP



CELF Japan Technical Jamboree 28

TOMOYO Linuxのご紹介

2009.6.12

株式会社NTTデータ

沼口大輔

numaguchid@nttdata.co.jp





- ***Part 1 : TOMOYO Linuxの概要***
- ***Part 2 : TOMOYO Linux on Android***
- **Q&A**



***TOMOYO Linux*の概要**





- 2003年に「使いこなせて安全」なLinuxを目指して開発、2005年11月にOSSとして公開
 - <http://tomoyo.sourceforge.jp/>
- ディストリビューションではありません(念のため)
 - カーネルパッチとユーティリティの2つから構成
- 2つのバージョン
 - メインライン版
 - Linux2.6.30で採用（6月10日リリース）
 - フル機能版
 - LSMを使わない独自フック版





- **Red Hat Enterprise Linux (CentOS) 3以降**

- **Ubuntu 6以降**

- **Debian 3.1以降**

- **Turbolinux 11 server**

- **Turbolinux Client 2008**

など



- 「**パス名ベース**」のアクセス制御
 - ポリシー(アクセス許可設定)の記述内容が理解しやすい
 - ポリシー編集も簡単に行える
- 「**自動学習**」機能
 - システムの起動から終了まで「**利用する機能やサービスを実行する**」だけで、必要なアクセス許可内容を自動的に収集
 - 学習結果を確認することにより、効率的に必要なポリシーを得られる
 - 管理者が**自分のシステムを理解、把握**するためのツールとしても活用可能



●被害の局所化

- ポリシー設定が適切に行われていれば、被害を限定できる

●不正アクセスの検知

- ポリシー違反の監視により検知可能

●誤操作防止

●情報漏洩の可能性を軽減

- ポリシーで許可されていない操作は失敗



- 自動学習
 - 初期設定が簡単
- リンクの区別
 - シンボリックリンクとハードリンクを区別
- ファイルシステムの制限がない
 - 純粹なパス名ベースのアクセス制御
- 省メモリー
 - **4 MB**マシンでも動作可能
- 2.4カーネルでも利用可能
 - フル機能版のみ

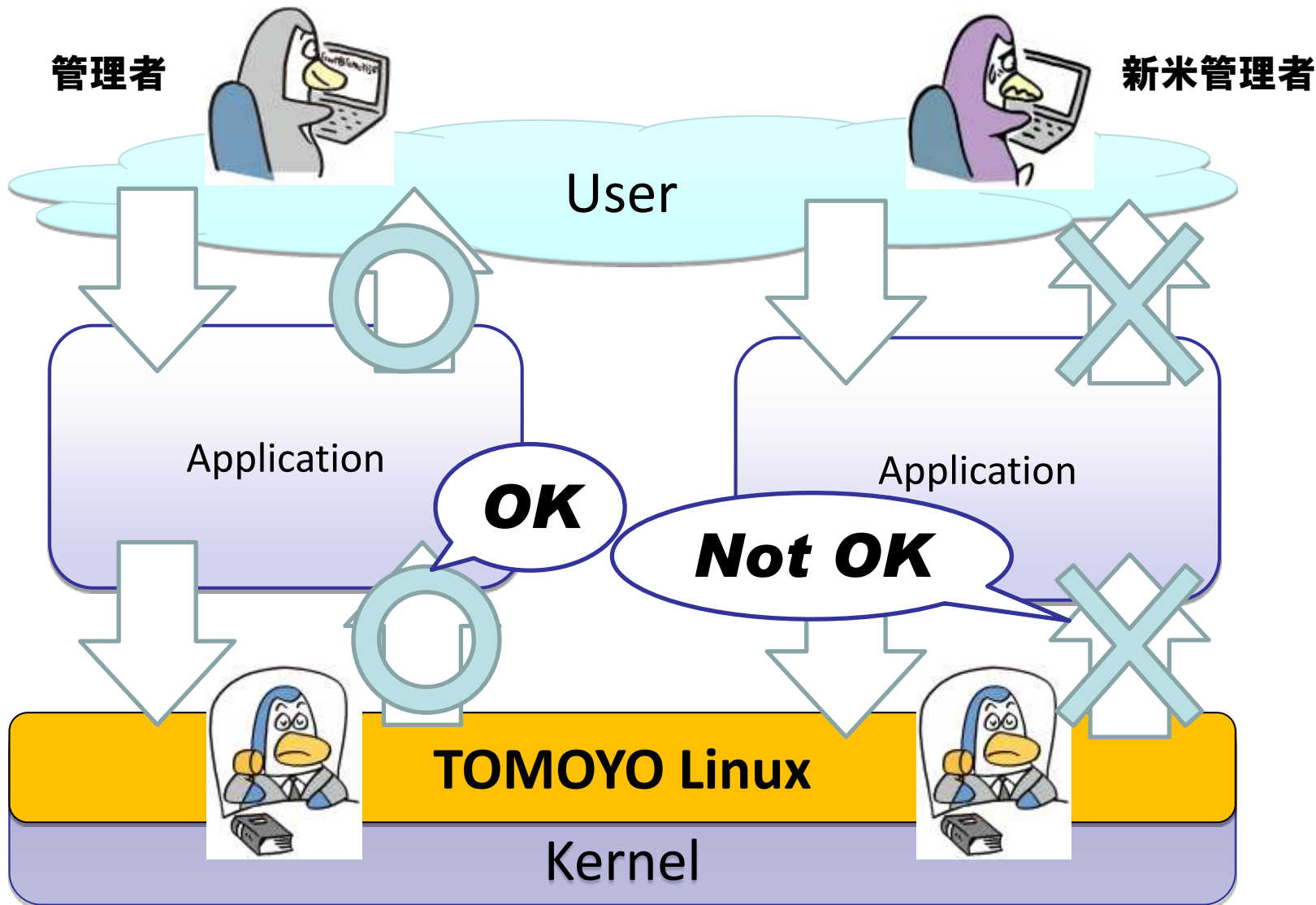


SELinuxとの比較



	SELinux	TOMOYO Linux
方式	ラベル	パス名
対応カーネル	2.6	2.6, 2.4(フル機能版)
アクセス制御		
RBAC	○	△
MCS / MLS	○	×
ファイルシステム制約	xattr必要	なし
ポリシー管理		
自動学習	—	○
編集	Booleanでon/off	直接
分割管理	モジュール利用	しない

TOMOYOの動作





● **Webサーバ**

– **Webコンテンツを読込むだけ**

• **クリックされても改ざんされない**

– **運用でログのチェック**

• **見るだけポリシーにしておく**

– **故意でも過失でもログ削除はできない**



- ファイル

- 読み書き実行

- 名前空間操作 (*mount, chroot*など)

- ネットワーク

- IPアドレス、ポート番号(*UDP/TCP*)

- ケイパビリティ

- その他パラメータ

- 環境変数、引数(*argv*)、*UID*など



導入

- ・ カーネルのインストール(通常はパッケージを利用)
- ・ ユーティリティのインストール

学習

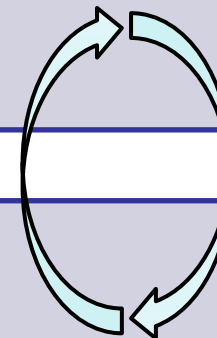
- ・ システムを動かして学習
- ・ 学習結果をポリシーとして自動作成

解析

- ・ 自動作成されたポリシーの確認
- ・ 確認した結果をもとにポリシーを修正

運用

- ・ TOMOYO Linuxの制御機能を有効にして運用開始





■ ドメイン + 制御モード + アクセス許可

● アクセス許可

- ホワイトリスト方式

● ドメイン

- すべてのプロセスは何れか1個のドメインに所属
- プログラムを実行するたびに、異なるドメインへ

● 制御モード

- *enforcing*
- *permissive*
- *learning (policy generation)*
- *disabled*



ポリシー例



<kernel> lsbinlinit

← ドメイン

use_profile 1

← 制御モード

allow_env HOME

アクセス許可

allow_env TERM



allow_read /etc/selinux/config

allow_capability SYS_MOUNT

allow_read /proc/cmdline

allow_read /selinux/enforce

allow_read /selinux/policyvers

allow_read

/etc/selinux/targeted/policy/policy.21

allow_read/write /selinux/load



デモ





● **SSHの動作制御**

- **学習させたコマンドだけ実行できる**

- **管理者ユーザでログインし、
コマンド操作を学習**
- **TOMOYOの制御を有効にして
再度管理者がログイン**
- **学習したコマンド、
学習しなかったコマンドを実行**



- **TOMOYO Linux の導入、管理方法について**
 - ホームページ
 - <http://tomoyo.sourceforge.jp/>
 - **TOMOYO Linuxの世界**
 - 技術評論社**Software Design**誌の連載記事を掲載
 - <http://tomoyo.sourceforge.jp/wiki/?WorldOfTomoyoLinux>
- **イベント情報について**
 - はてなキーワード
 - <http://d.hatena.ne.jp/keyword/TOMOYO%20Linux>
- **最新情報 & 匿名で質問**
 - 2ちゃんねる
 - <http://pc11.2ch.net/test/read.cgi/linux/1239030346/>
 - <http://tomoyo.sourceforge.jp/2ch/>



●勉強会

- 日時：2009年7月3日（金）16:00～
- 場所：日本SGI株式会社 SGIホール

●懇親会

- 日時：2009年7月3日（金）19:00～
- 場所：銀座ライオン アトレ恵比寿店

◆ <http://sourceforge.jp/projects/to moyo/wiki/ThankYou>

Global IT Innovator

NTT DATA GROUP



TOMOYOは株式会社NTTデータの登録商標です。
LinuxはLinus Torvalds氏の日本およびその他の国における登録商標または商標です。
その他の商品名、会社名、団体名は、各社の商標または登録商標です。