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 27

TOMOYO Linuxのご紹介

2009.5.22
株式会社NTTデータ
沼口大輔
numaguchid@nttdata.co.jp

本日のメニュー

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

TOMOYO Linuxの概要

TOMOYO Linuxについて

- 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月末リリース予定）
  - フル機能版
    - LSMを使わない独自フック版

フル機能版対応ディストリビューション

- 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

TOMOYO Linuxの特徴

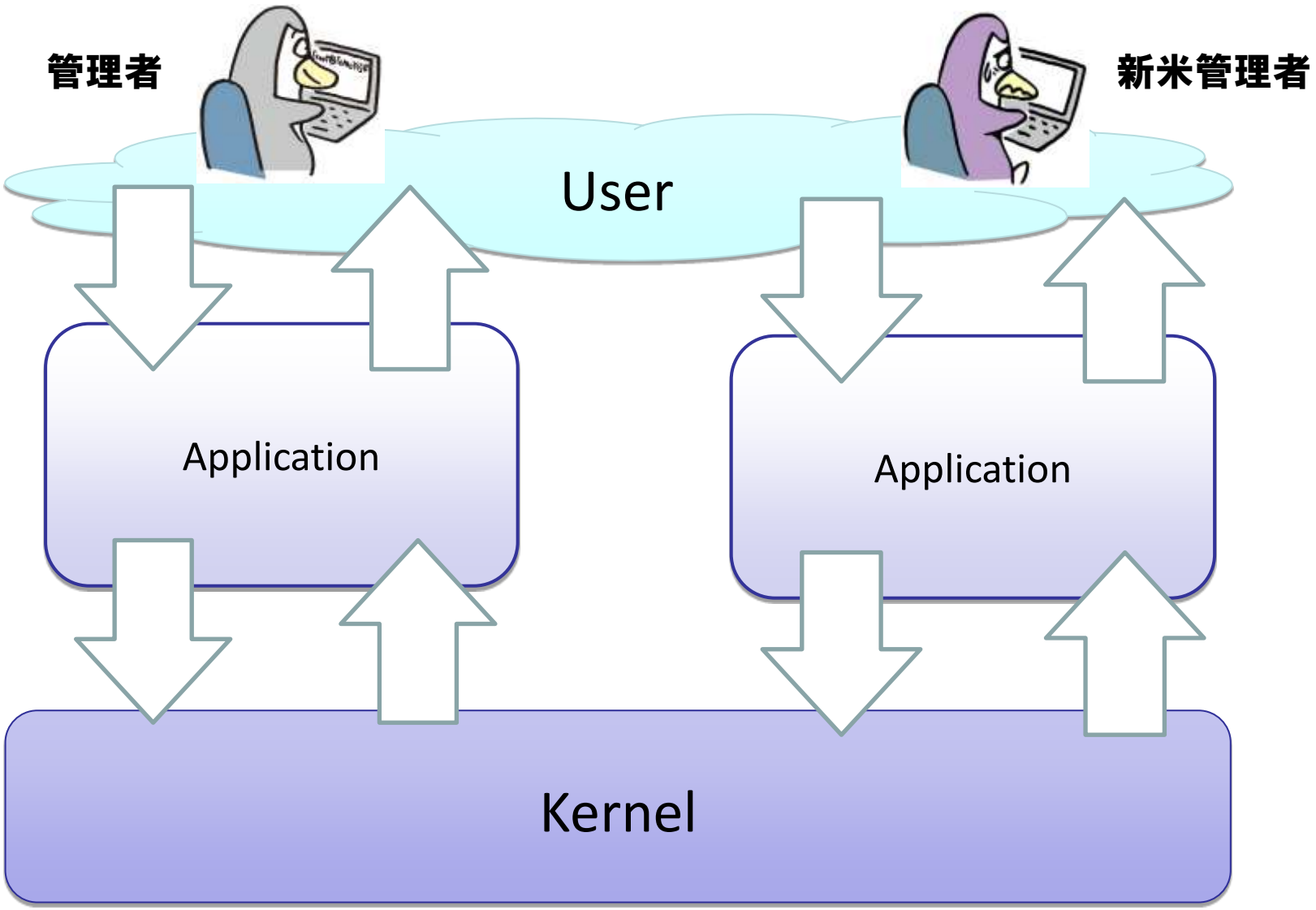
- 「パス名ベース」のアクセス制御
  - ポリシーの記述内容が理解しやすい
  - ポリシー編集も簡単に行える

- 「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

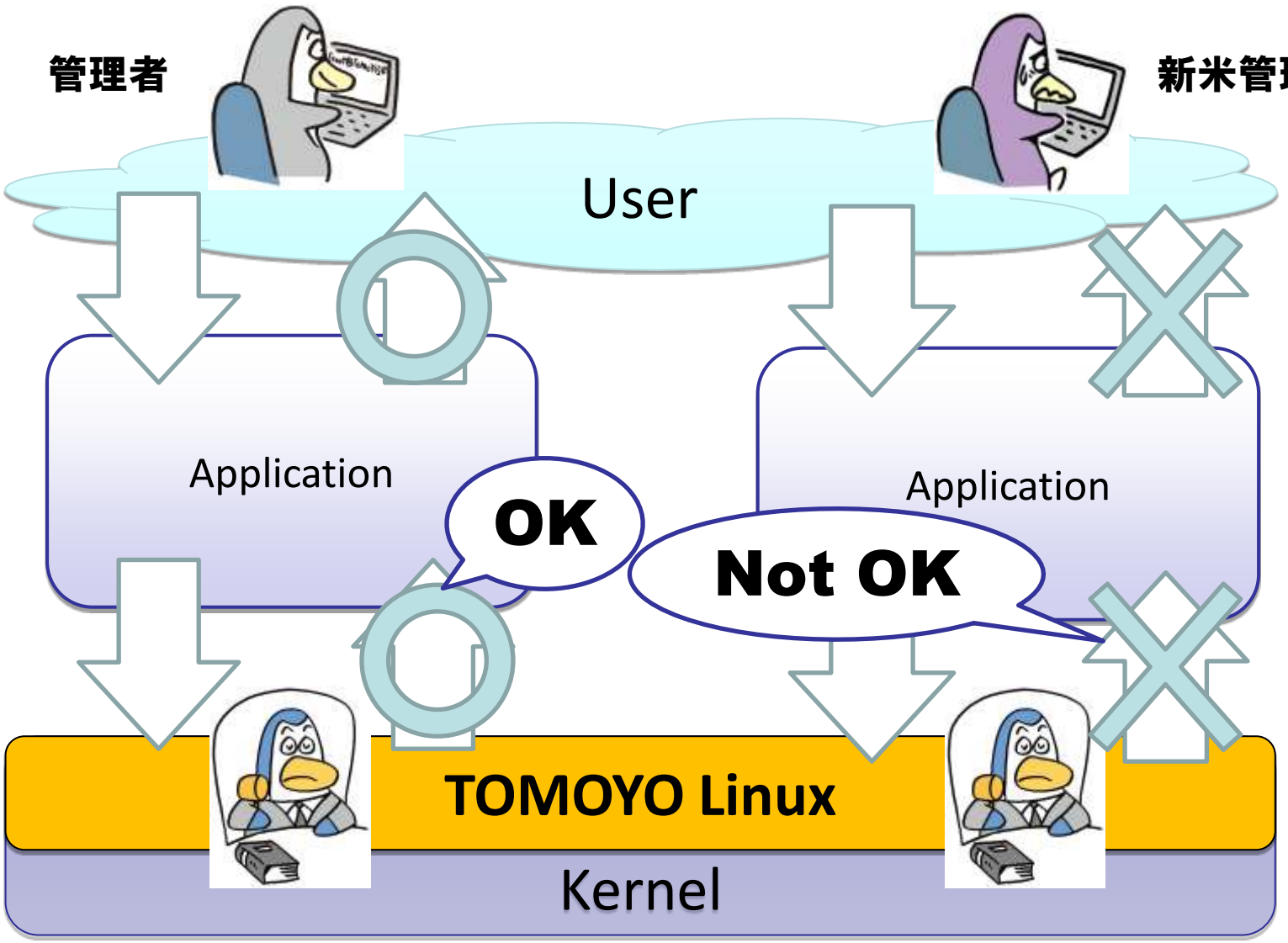
TOMOYO Linuxの導入メリット

- ポリシー（良い悪いの定義）が適切に行われていれば、不正アクセスを受けた場合でも**被害を限定（局所化）**できる
- ポリシー違反の監視により**不正アクセスの検知**が可能
- 管理者の**誤操作防止**
- 内部からの**情報漏洩の可能性を軽減**
  （管理者であろうが内部関係者であろうがポリシーで許可されていない操作は失敗）

普通のOS



TOMOYOの場合



例えば

- Webサーバ
  - Webコンテンツを読込むだけ
    - クラックされても改ざんされない
  - 運用でログのチェック
    - 見るだけで、ログ削除はできない（故意でも、過失でも）

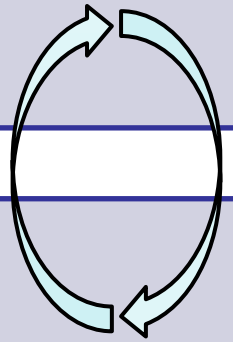
TOMOYOが制御できること

- 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

利用までの流れ

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

ディストリ毎に導入手順を公開

- Red Hat系
  - http://sourceforge.jp/projects/tomoyo/wiki/HowToRedHat
- Debian
  - http://sourceforge.jp/projects/tomoyo/wiki/HowToDebian
- Ubuntu
  - http://tomoyo.sourceforge.jp/ja/1.6.x/1st-step/ubuntu8.04-live
- Turbolinux
  - http://www.turbolinux.co.jp/products/server/11s/user_guide

組込み機器とTOMOYO Linux

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

SELinuxとの比較

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

デモ

デモでやること

- 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の情報

- 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/

お知らせ

メインライン化記念パーティ開催します

- ●概要
  - 日時：2009年7月3日（金）19:00開場
  - 場所：銀座ライオン　アトレ恵比寿店
  - 形式：立食パーティ
  - 参加費：未定
- ◆http://sourceforge.jp/projects/tomoyo/wiki/ThankYou
- ●パーティの前に勉強会を計画中

Global IT Innovator

NTT DATA GROUP