Linux CONFERENCE 2004

Linuxカーネルの動的アクセスポリシー制御

Dynamic Access Policy Control for Linux Kernel

㈱ ＮＴＴデータ 技術開発本部

R&D Headquarters, NTT DATA Corporation

保理江 高志† 原田 季栄 田中 一男

Takashi Horie, Toshiharu Harada, Kazuo Tanaka

Agenda

- SELinuxの概要
- カーネルへのIDS･IPS機能拡張
- 運用上の課題
- フレキシビリティ改善
- 実装に関して
- LMBENCHによる性能測定
- デモンストレーション ～ FTP / Web サーバーへの適用例
- まとめ･今後の課題

はじめに

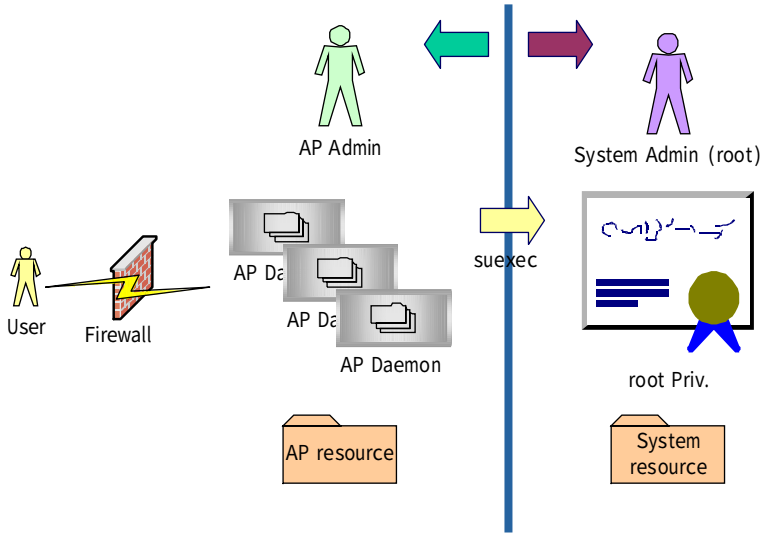
- SELinux (Security-Enhanced Linux)
  - 米NSAとSCCにより開発されたMachカーネル向けセキュリティ拡張 (DTOS)
  - Utah Univ. Flux Research Groupとの共同研究の過程で、Linuxカーネルにポート
  - 強制アクセス制御 (MAC) 機能のLinux実装
- ヒストリー
  - 2000/12　Kernel 2.2パッチとして1stリリース
  - 2001/8　LSM (Linux Security Module) 化
  - 2003/9　標準カーネルにマージ (2.6.0 ～)

SELinuxとは？

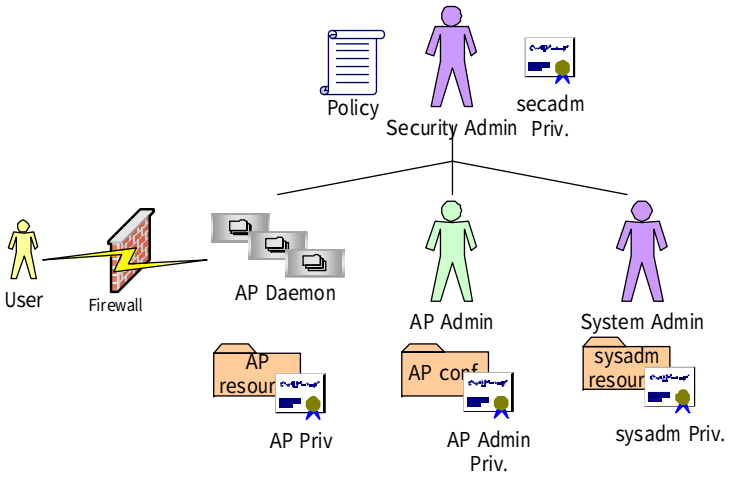
- 従来UNIX系OS
  - DAC ～ オブジェクトのアクセス権を任意に変更可能
  - 粗粒度 (Coarse Grained) のアクセス制御：
    ユーザー属性（User / Group / Other）
    × 3つのパーミッション（read / write / execute）
  - 全ての管理者権限は root に集中
- SELinux
  - MAC ～ アクセス権変更には特別な管理者権限が必要
  - 細粒度 (Fine Grained) のアクセス制御：
    ユーザー属性（任意ラベルによる管理）
    × 詳細パーミッション（read / write / execute
    / create / unlink / setattr / lock etc..）
  - アプリケーションドメイン毎に管理者権限を分割

セキュリティの基本戦略

- 従来UNIX系OS
  - 強大なroot権限を、
    いかにして “Isolate” するか



- SELinux
  - 管理者権限の分割により、
    潜在的なリスクを低減
  - 侵入されても権限を与えない



SELinuxのアクセス制御

- アクセスポリシーの定義

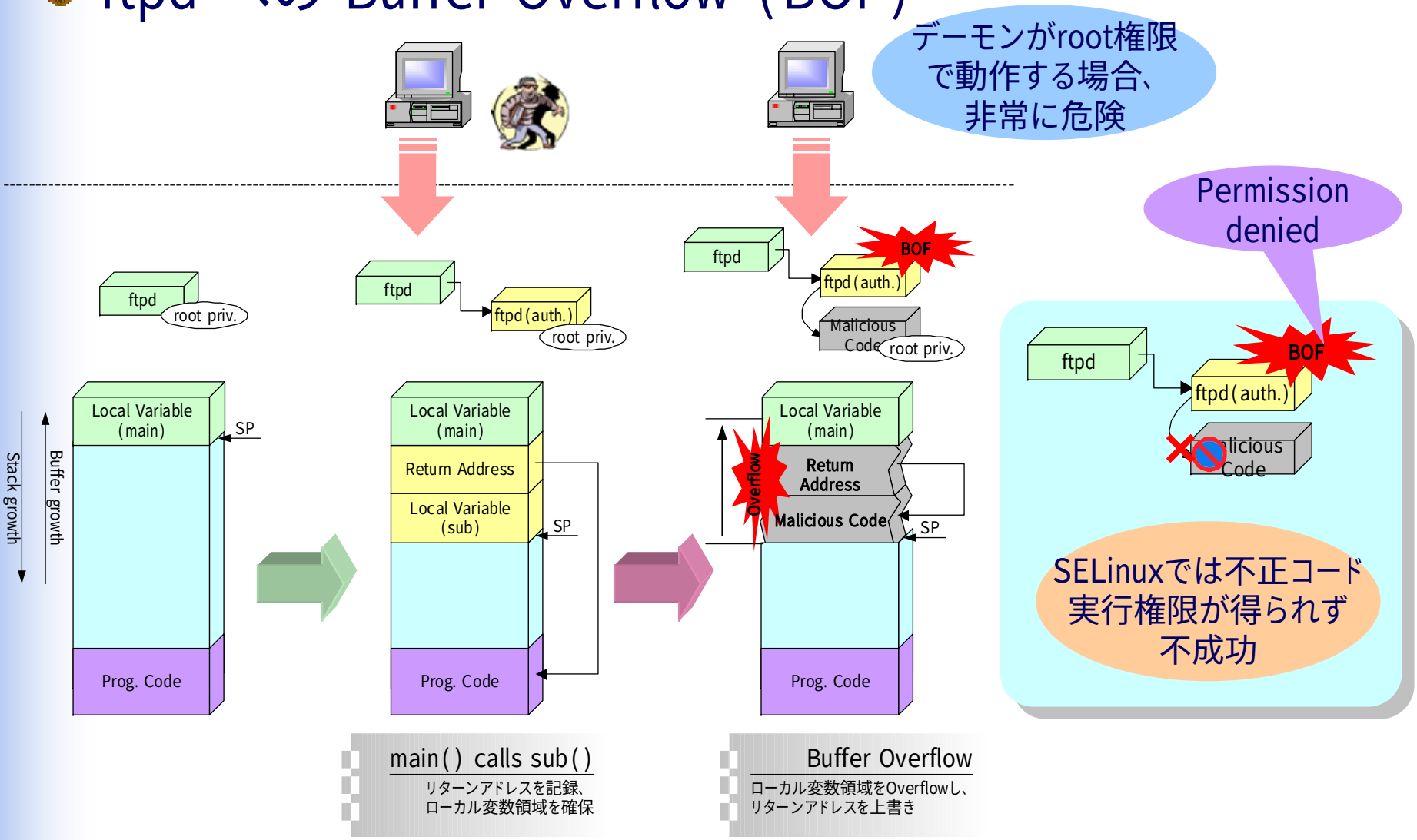
```
allow  <subject>  <object:class>  <permissions> ;

   Ex)  allow  sysadm_t  sysadm_home_t:file  {
          create execute ioctl read getattr lock write
          setattr append link unlink rename
        } ;
```

- 意味
  - sysadm_t (System Admin.ロールの管理者) による
  - sysadm_home_t (System Admin. ホーム配下のfile) への
  - 以下のパーミッションを許可 { create execute ... }

BOFによる不正アクセス被害

- ftpd への Buffer Overflow（BOF）



SELinuxと不正アクセス

不正アクセスの痕跡情報

【SELinuxのアクセス制御情報】

May 19 17:05:46 kids kernel: avc: denied { execute } for pid=2801 exe=/usr/sbin/in.ftpd name=sh dev=sda2 ino=831854 scontext=system_u:system_r:ftpd_t tcontext=system_u:object_r:shell_exec_t tclass=file

翻訳すると・・・ BOFそのもの

「ftpd が shell の execute を試みたので拒否しました。」

不正アクセス検知への適用

- アクセス制御ログの他のログレコード(アクセス拒否等)とは区別して扱える必要がある。

Linuxカーネルベース IDSの概念

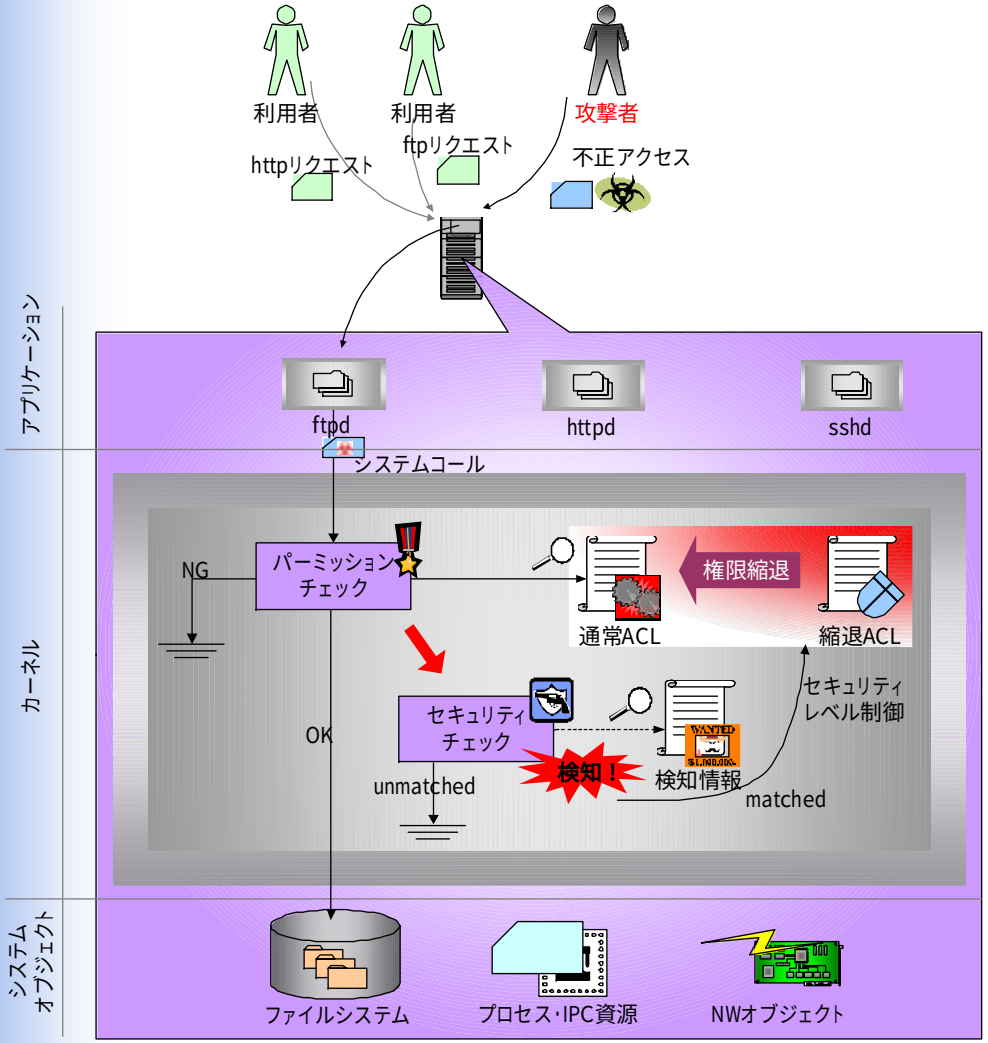
- IDS機能拡張 ～ OSアクセス制御レベルでの不正アクセス検知
  - 検知対象：不正行為に付随して発生するアクセス
    - 危険度の高いアクセスポリシー違反の検知
  - パーミッションとは別の観点のセキュリティチェック（極めて重大なポリシー違反チェック）を実施

連携

両者の連携を
OS機能として実現

- IPS機能拡張 ～ 管理者権限の縮退による防御
  - 対応手段：アクセスポリシーの動的変更
    - 攻撃者の最終的なターゲットは管理者権限の奪取
    - 管理者権限を縮退し、攻撃を受けているシステム資源を実質的に「ロック」することで、権限取得・改ざん・破壊・漏えい行為への万全の対策となる。

Linuxカーネルベース IDSのアーキテクチャ



- アクセスポリシーを動的に制御

トリガ

- 重大なポリシー違反の監視

ポリシーの記法拡張 I

- 検知対象の定義 ～ ftpd への BOF 検知

```
strict  <subject>  <object:class>  <permissions> ;
    Ex)  strict  ftpd_t  shell_exec_t:file  { execute }  ;
```

- 定義対象

【侵入・権限取得】
  - 権限の無いプロセスからの shell 等の起動 (BOF)
  - 権限奪取・権限拡大の試み

【改ざん・破壊行為】
  - バイナリ・設定・ログファイルの改ざん・消去

【情報漏えい行為】
  - 機密ファイルへの不正な参照

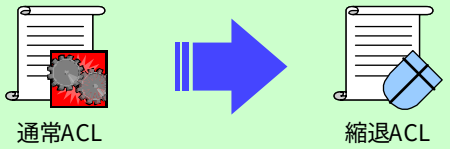
ポリシーの記法拡張 II

- ステート毎のアクセスポリシーの定義 ～ ftpd_t 縮退

```
allow   <subject>   <object:class>
                                  <permissions> <state> ;

   Ex)   allow   ftpd_t   user_home_t:file   {
            create ioctl read getattr lock write setattr
            append link unlink rename }   1 ; /* 通常時 */
   Ex)   allow   ftpd_t   user_home_t:file   {
            read getattr lock ioctl }   3 ;        /* 縮退時 */
```

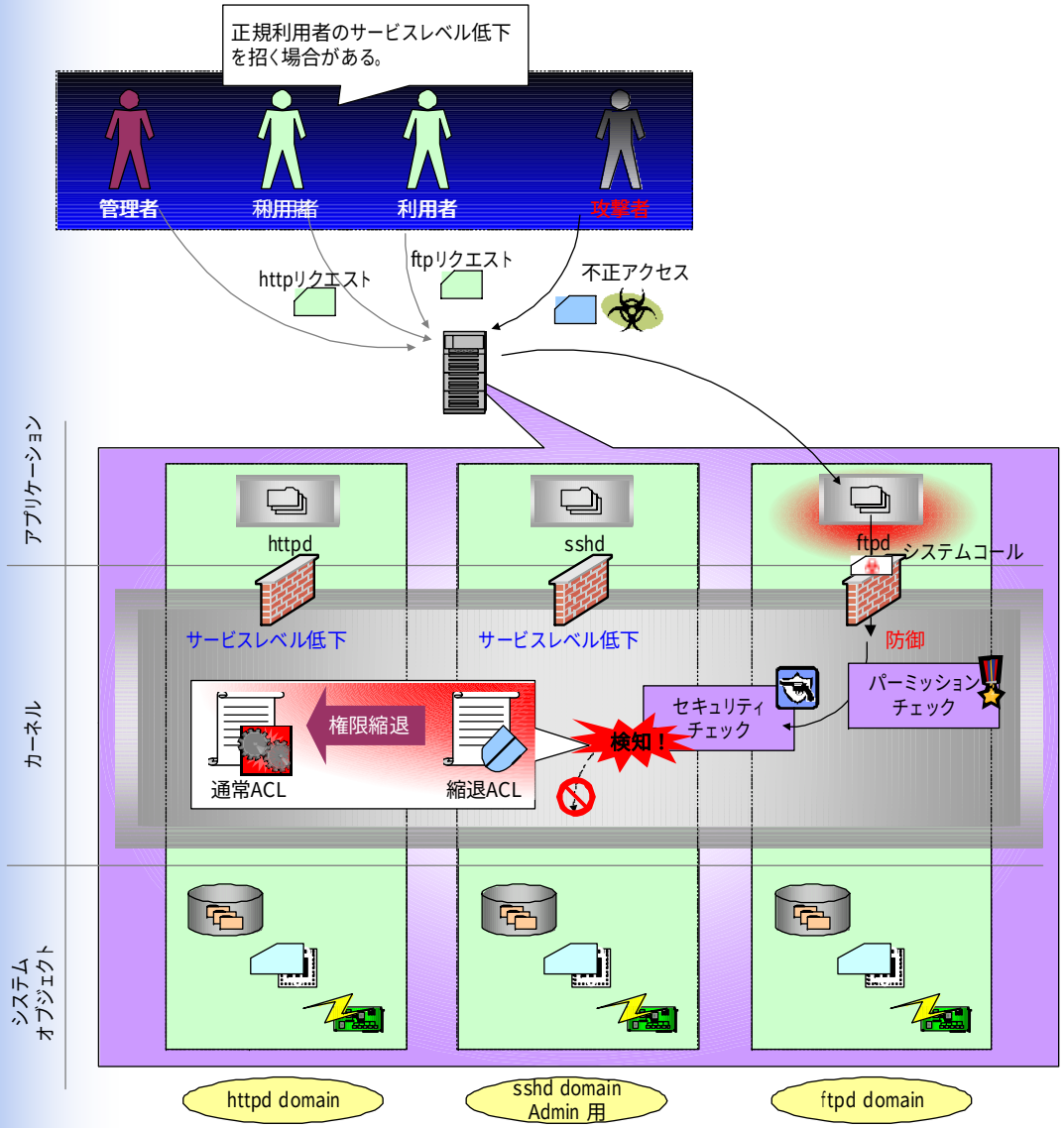
- 意味 ～ ftpdの権限縮退
  - 状態変更 (1 → 3) で
    create/write/setattr/append/link/unlink/renameを
    権限縮退 → FTPアップロードの禁止



効果について

- 以下のメリットが得られる。
  - リアルタイム性 ： 検知～防御をOSレイヤで連携
    ネットワーク型IDSでの検知 → 防御にはタイムラグを伴う
    - 検知はしたものの、被害を招いてしまうケースがある。
  - 一般性・汎用性 ： 亜種攻撃への耐性
    例) ftpdへのBOF攻撃 ・・・ 以下に依存せず検知可能
    - ftpd及び脆弱性・攻撃ツールの種別
    - ローカル攻撃 or リモート攻撃の別
  - ポリシーファイルの「封印」～ 改ざんリスク回避
    SELinuxはアクセスポリシー設定が要
    - セキュリティ管理者 (secadm) の権限を「運用中」は無効化
    - ポリシーファイルへの変更権限を誰も持たない、と言う状況を
      実現可能 → アクセスポリシー改ざん行為からの完全な保護

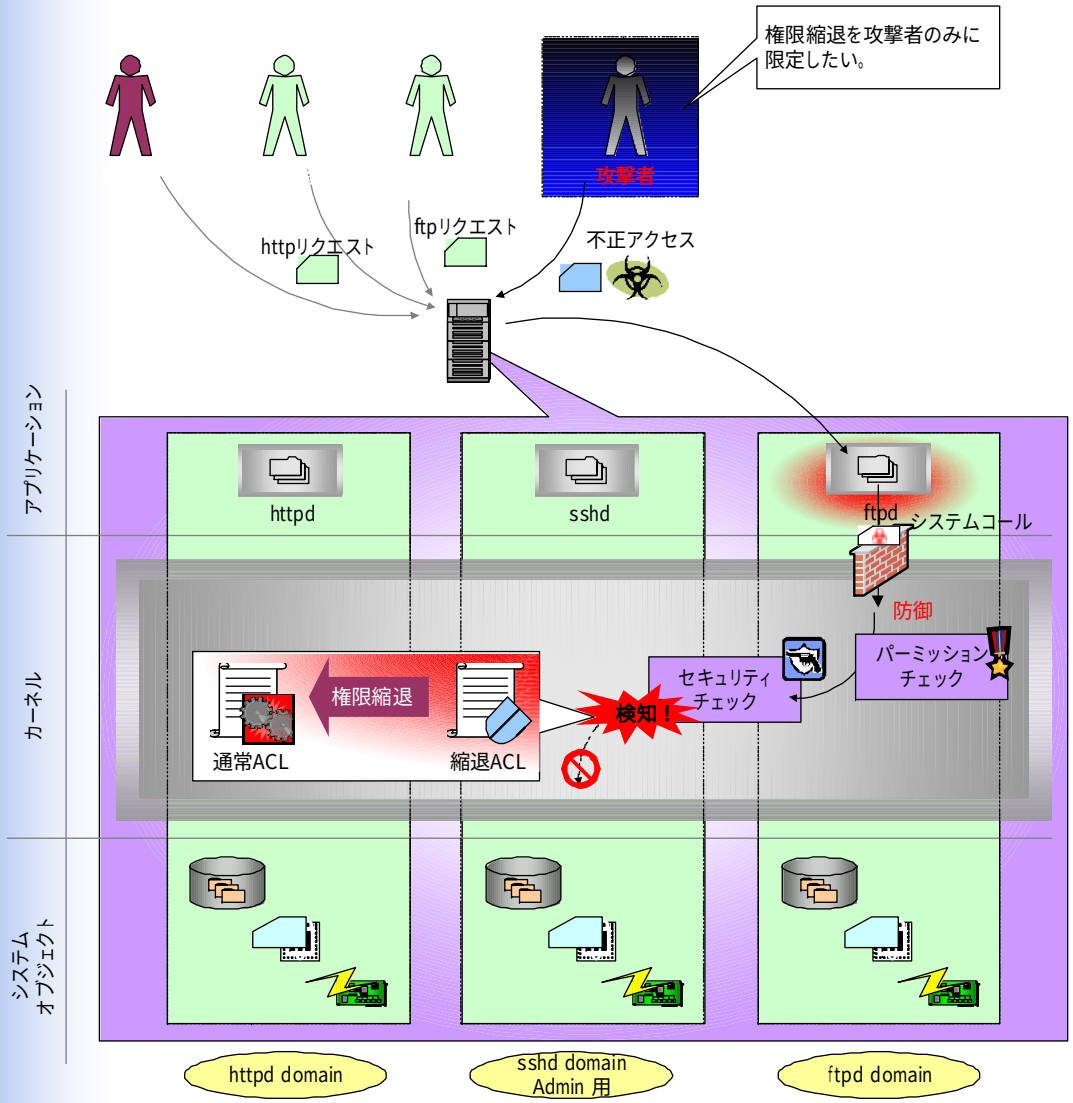
初期プロトタイプでの問題点



- 重大なポリシー違反の検知
- カーネル全体としての防御が機能
- サービスレベル低下を招いてしまう。

制御に柔軟性が欠ける。

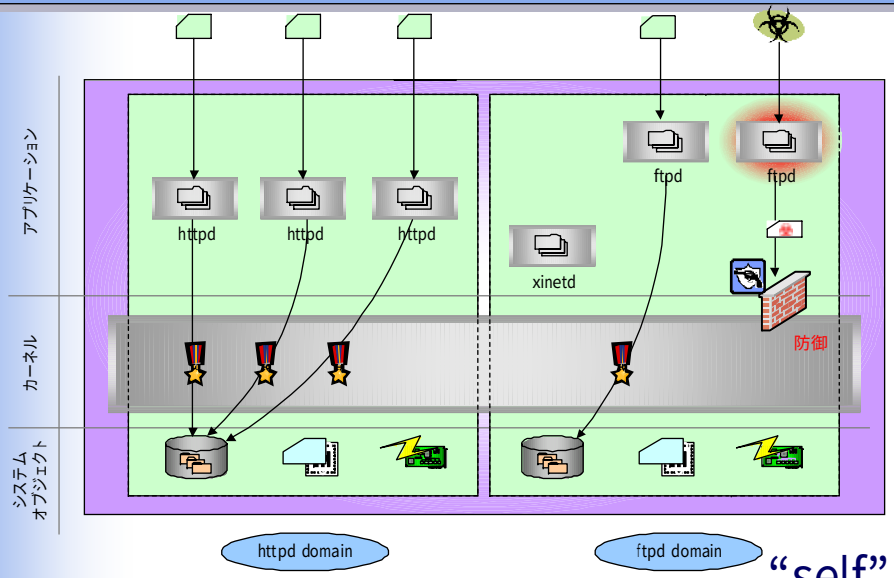
機能改善① ～プロセス単位のセキュリティレベル制御



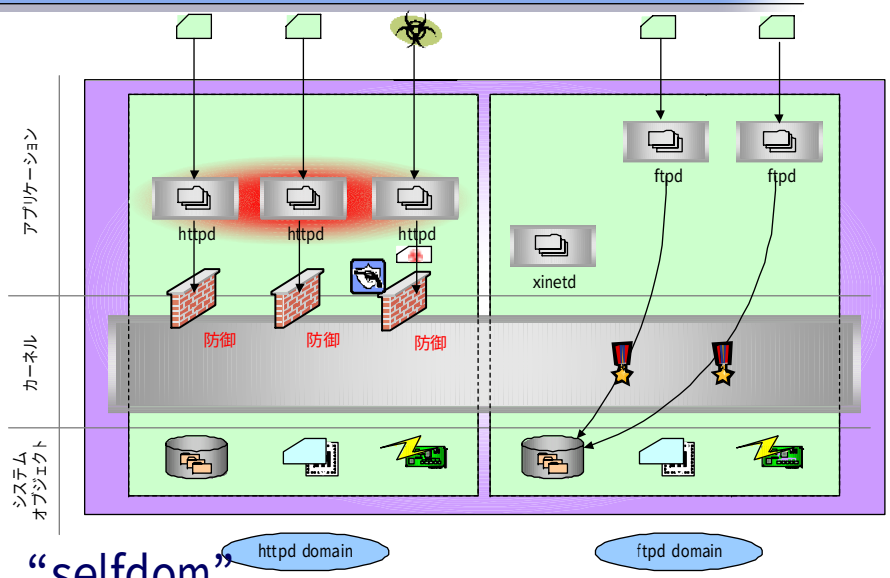
- 「カーネルのセキュリティレベル」
- 「プロセス毎のセキュリティレベル」

ただし、発生する事象・アプリケーション種別により権限制御すべき範囲は異なる

セキュリティレベルの制御範囲



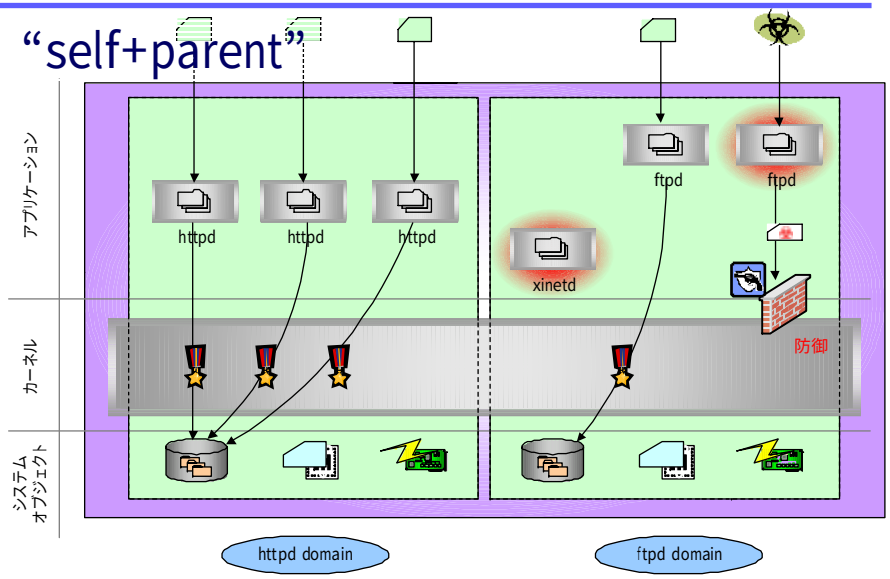
“self”



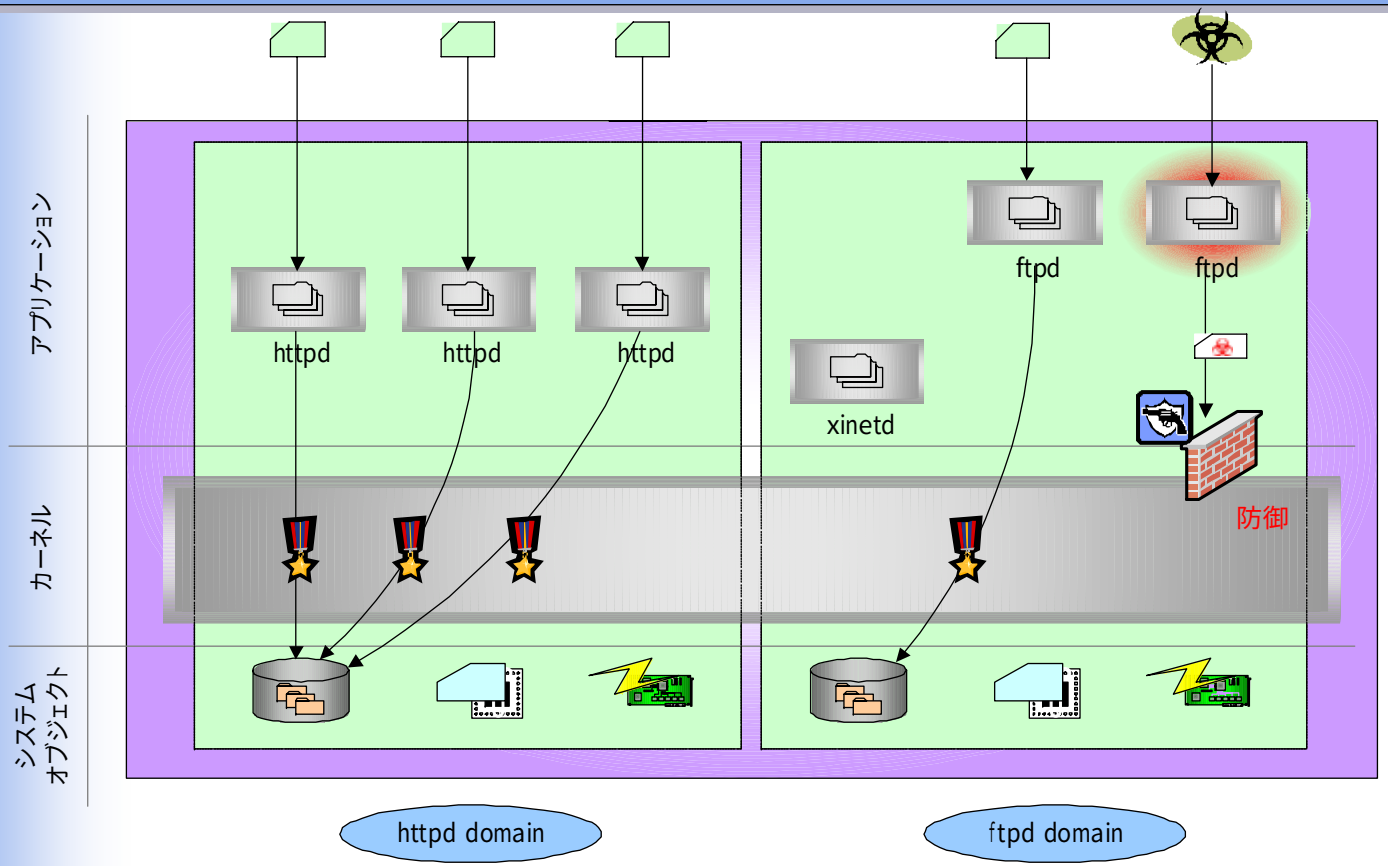
“selfdom”

表記	範囲
self	・攻撃対象となったプロセス自身
parent	・攻撃対象プロセスの生成元
pparent	・上記parentの生成元
selfdom	・上記selfと同一ドメインのプロセス
pdom	・攻撃対象プロセスの遷移元ドメイン
ppdom	・上記pdomの遷移元ドメイン
proc	・全てのプロセス
kernel	・暗黙的セキュリティレベル

“self+parent”

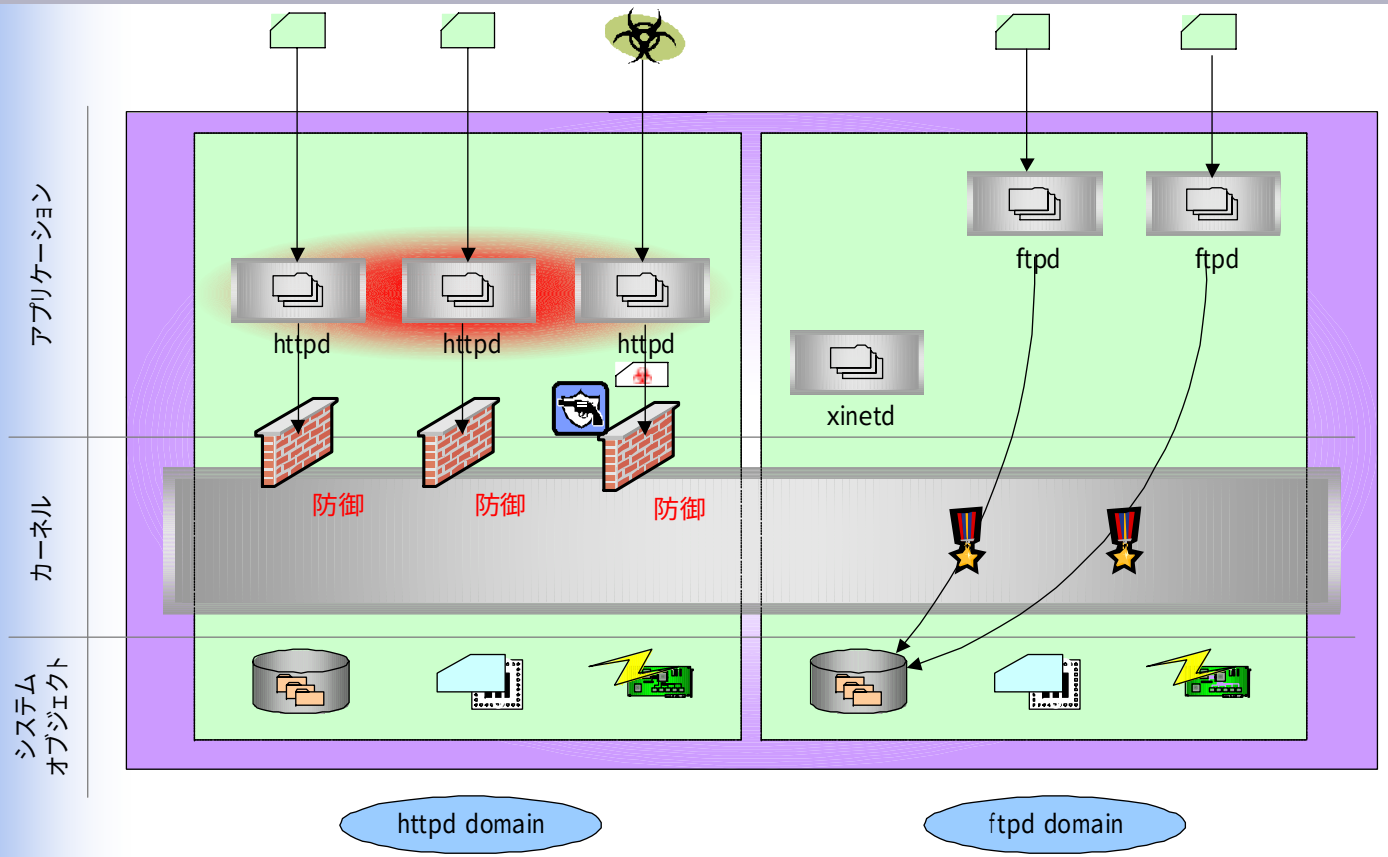


セキュリティレベルの制御範囲(self)



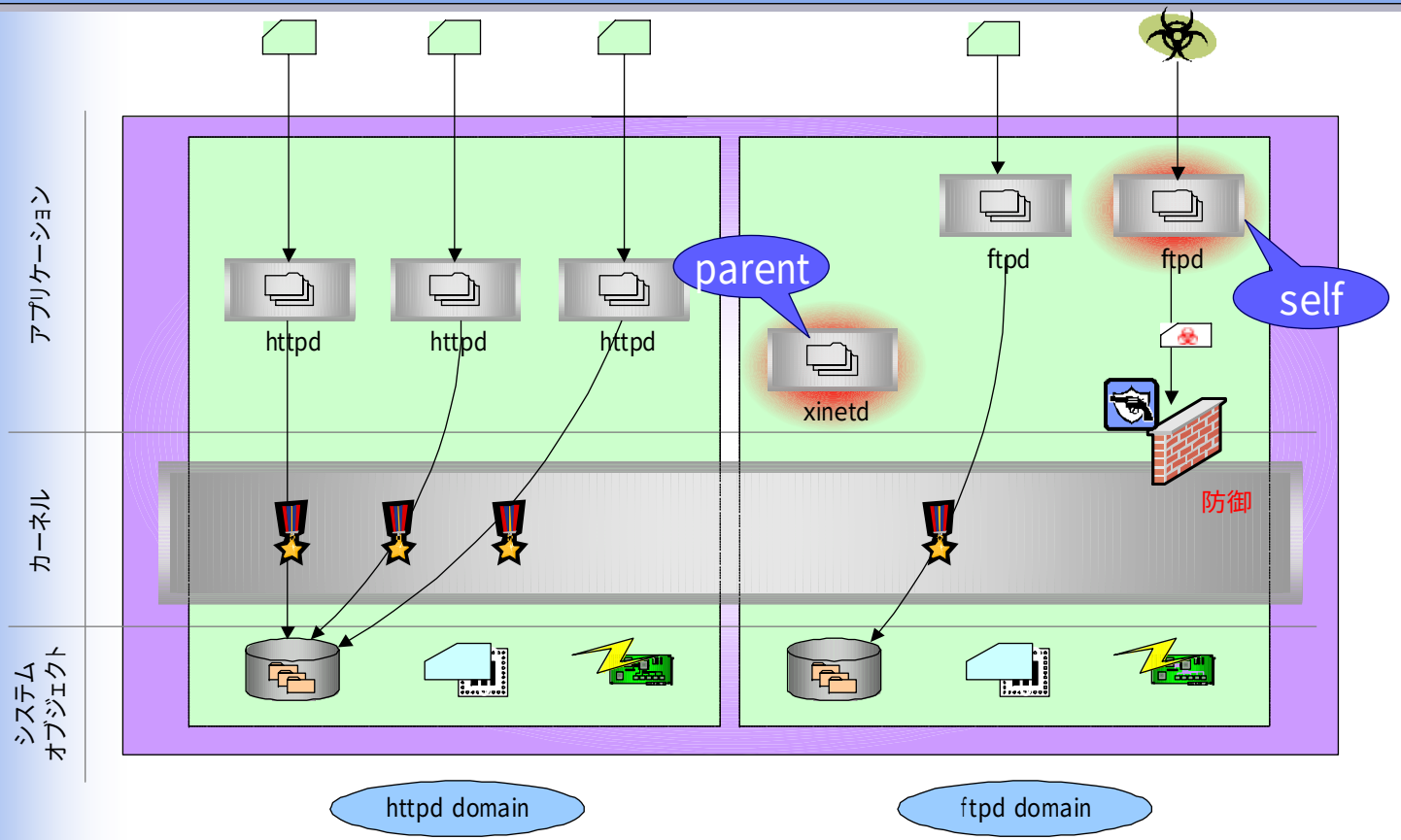
- self
  攻撃対象プロセスの権限縮退
  - 低危険度の攻撃
  - プロセスのライフタイムが短い

セキュリティレベルの制御範囲(selfdom)



- selfdom
  攻撃対象プロセスドメイン
  - 同一ラベルを持つプロセス群
  - セッションスティッキーでない場合

セキュリティレベルの制御範囲(parent)

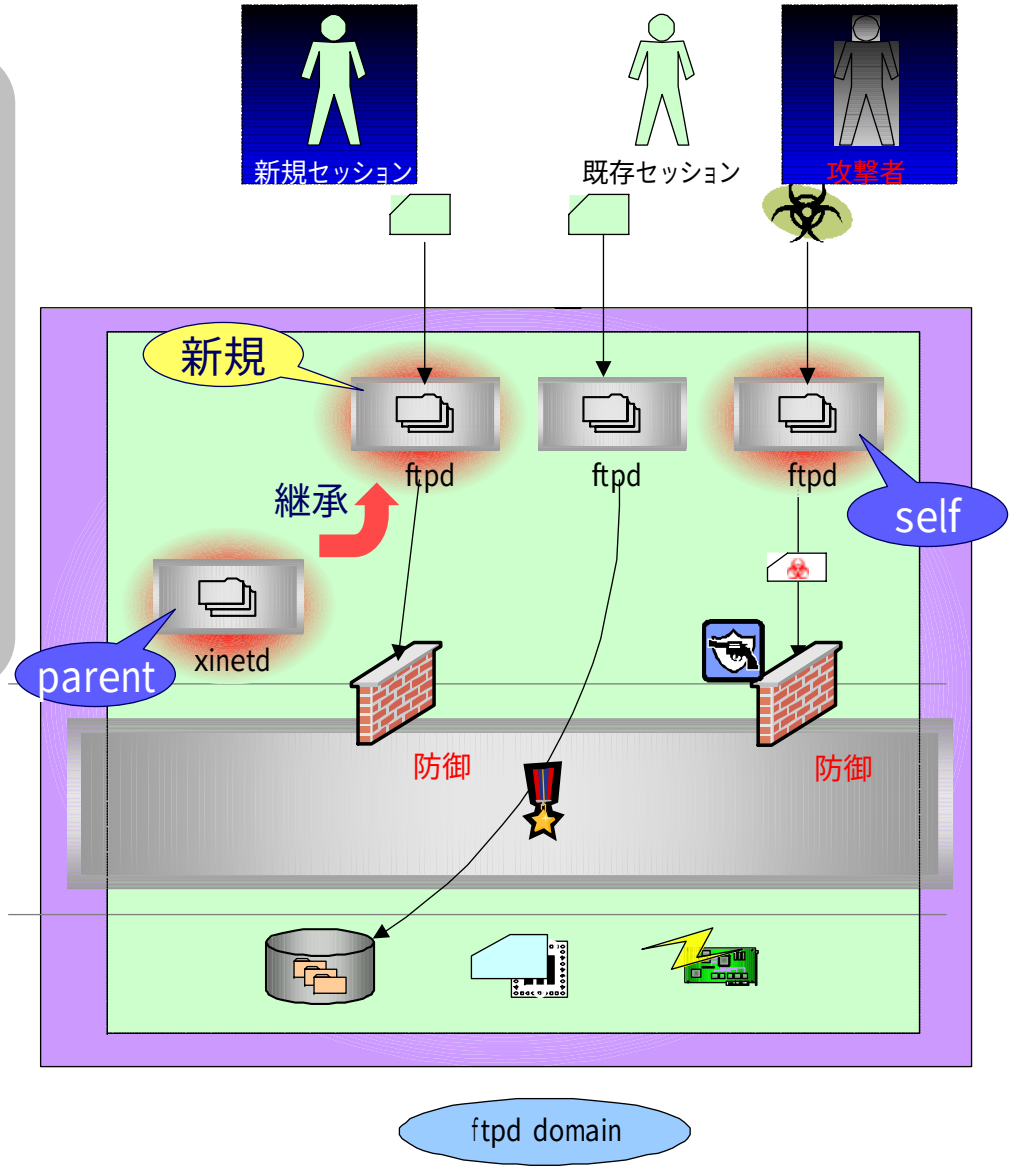


- parent
  攻撃対象プロセスの生成元
  - セキュリティレベル継承
  - 以後も継続的に権限縮退を図る

セキュリティレベル継承

- 新規プロセスは生成元プロセスのセキュリティレベルを継承
- 既存セッションのサービス維持と新規セッションの権限縮退が両立

parent
起動元のshellやxinetdへの指定が有効

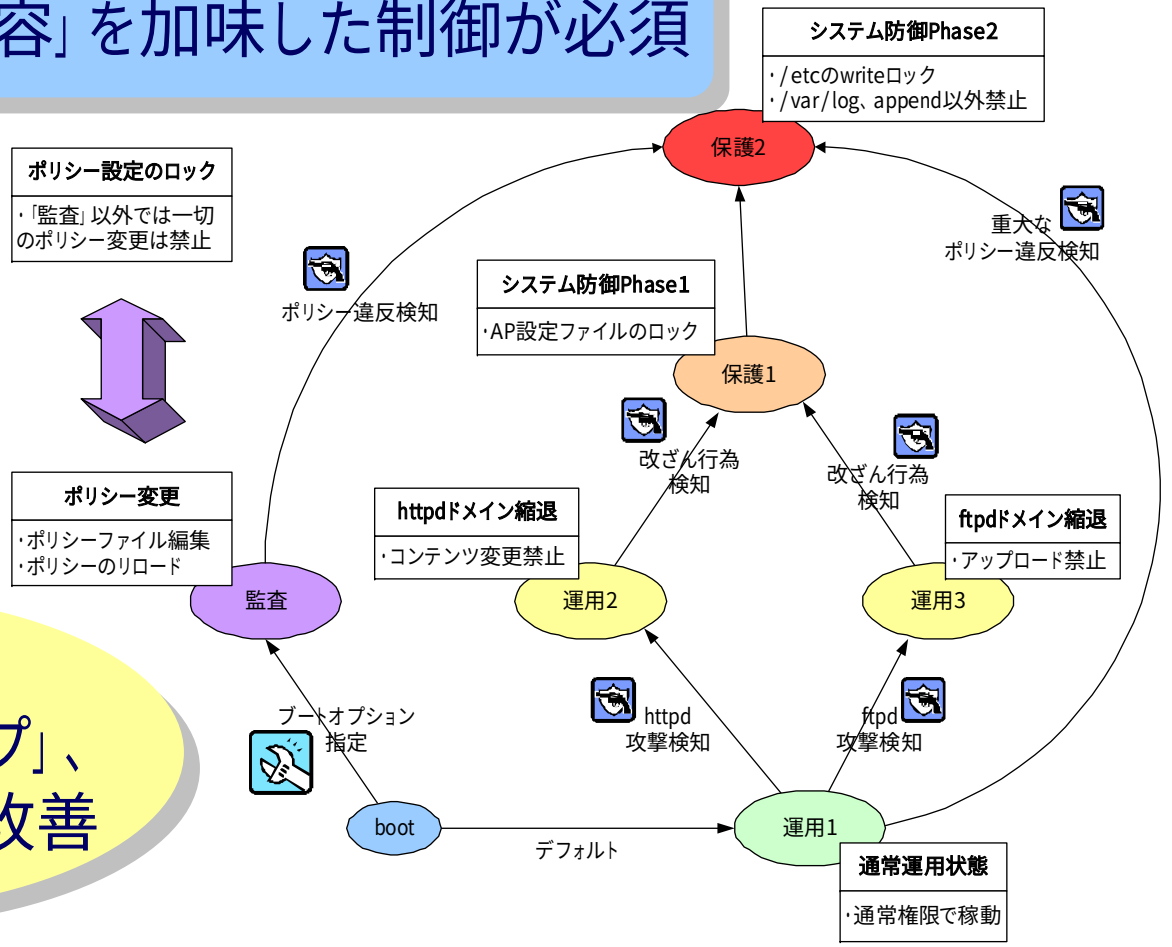


機能改善② ～ 状態遷移の文脈性

- 適切な「防御」の実現
- 「状況」と「攻撃内容」を加味した制御が必須

ポリシーファイル封印
ポリシー変更権限を
他状態から隔離
(ポリシー改ざん不可能)

遷移パス
「分岐」・「スキップ」、
フレキシビリティ改善



ポリシーの記法拡張III

- 最終的な検知対象定義

```
strict  <subject>  <object:class>  <permissions>
                   <goto N>  <scope>  <state> ;

   Ex)  strict  user_t  etc_t:file  { write unlink }
                   goto 3  { self parent } 1  ;
```

- 意味
  - 状態1において
  - user_t（一般ユーザー）による
  - etc_t（/etc 配下のfile）への
  - 以下のパーミッションリクエストを監視 { write unlink }
  - 検知した際には、{ self parent }を状態3に遷移

SELinuxへの実装に関して

- 拡張対象

対象	機能拡張
パーミッション構造体 (Access Vector)	・検知対象定義用メンバ追加
	・制御範囲／遷移先定義用メンバ追加
	・動的制御情報の定義 (パーミッション情報の配列化)
アクセス制御関数	・セキュリティチェック ロジック追加
	・パーミッション動的管理対応
状態遷移関数	・検知に基づく状態遷移制御 ロジック追加
	・状態遷移先指定の制御 ロジック追加
ツール	・ポリシーパーザの拡張、入出力関数の変更
制御インタフェース	・セキュリティレベル参照インタフェース
task_security_struct 構造体	・セキュリティレベル管理用メンバ追加

ベンチマークについて

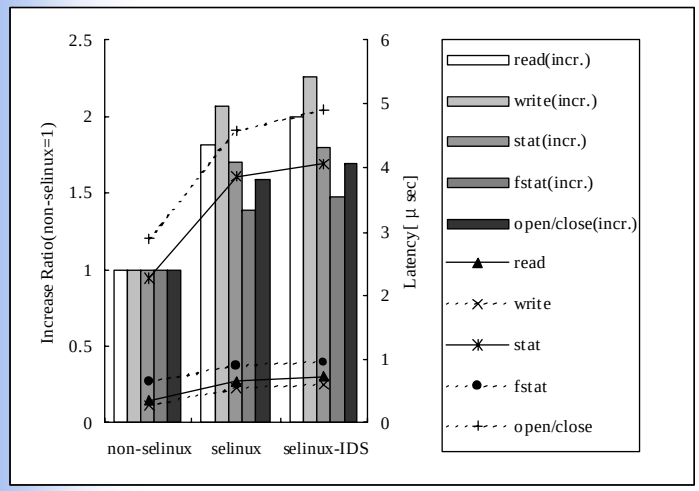
- 性能比較
  - Kernel 2.6.3 (non-SELinux)
  - Kernel 2.6.3 (SELinux)
  - Kernel 2.6.3 (SELinux-IDS)
- 測定項目 ～ LMBENCH
  - lat_syscall：read/write/open/close etc..
  - lat_proc：fork/execve
  - lat_http：httpリクエスト処理時間
- 実験条件

CPU	Pentium III 933MHz
Memory	2GB, (512MBx4 SDRAM 133MHz)
Disk	18GB SCSI Disk, (18 GByte, Ultra160)

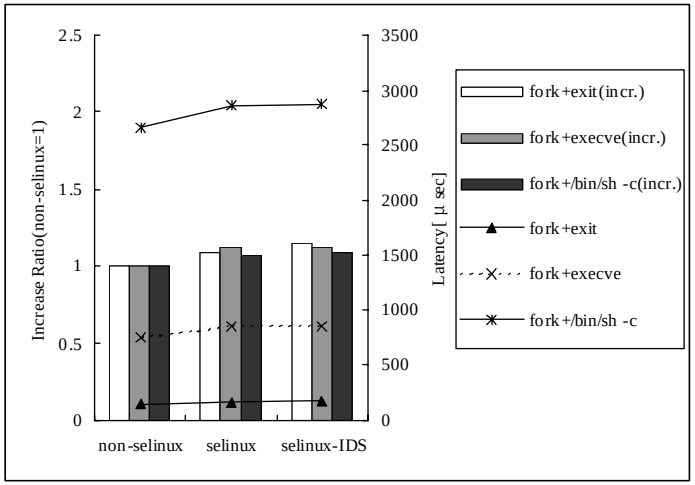
ベンチマーク結果

		non-selinux	selinux	selinux-IDS
lat_syscall [μsec]	read	0.35	0.64	0.71
	write	0.27	0.55	0.61
	stat	2.27	3.85	4.07
	fstat	0.65	0.90	0.95
	open/close	2.90	4.58	4.89
lat_proc [μsec]	fork+exit	148	161	168
	fork+execve	755	847	847
	fork+/bin/sh	2658	2863	2872
lat_http [msec]		1.67	1.96	1.98

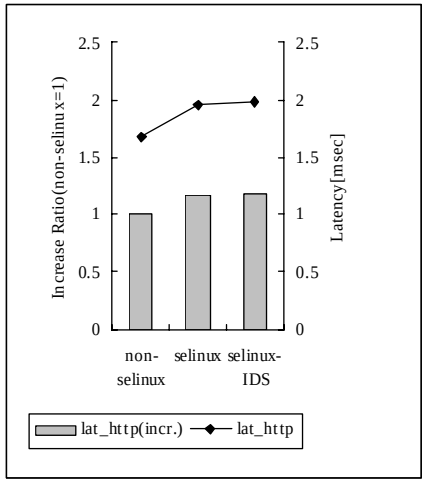
- レイテンシ伸び率 最大10%
- アプリケーション性能への影響微少（httpリクエスト処理）



lat_syscall



lat_proc

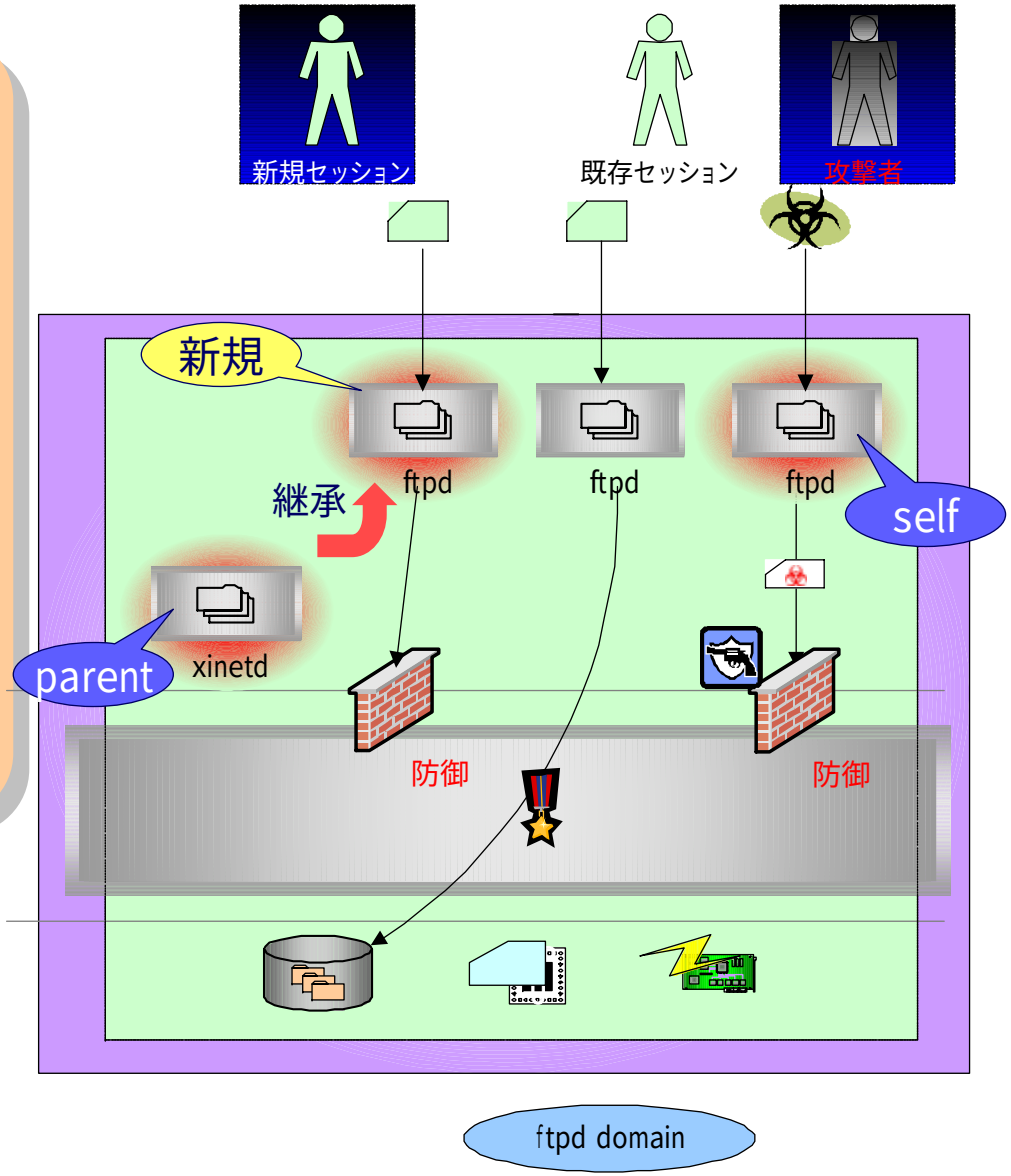


lat_http

デモのご紹介

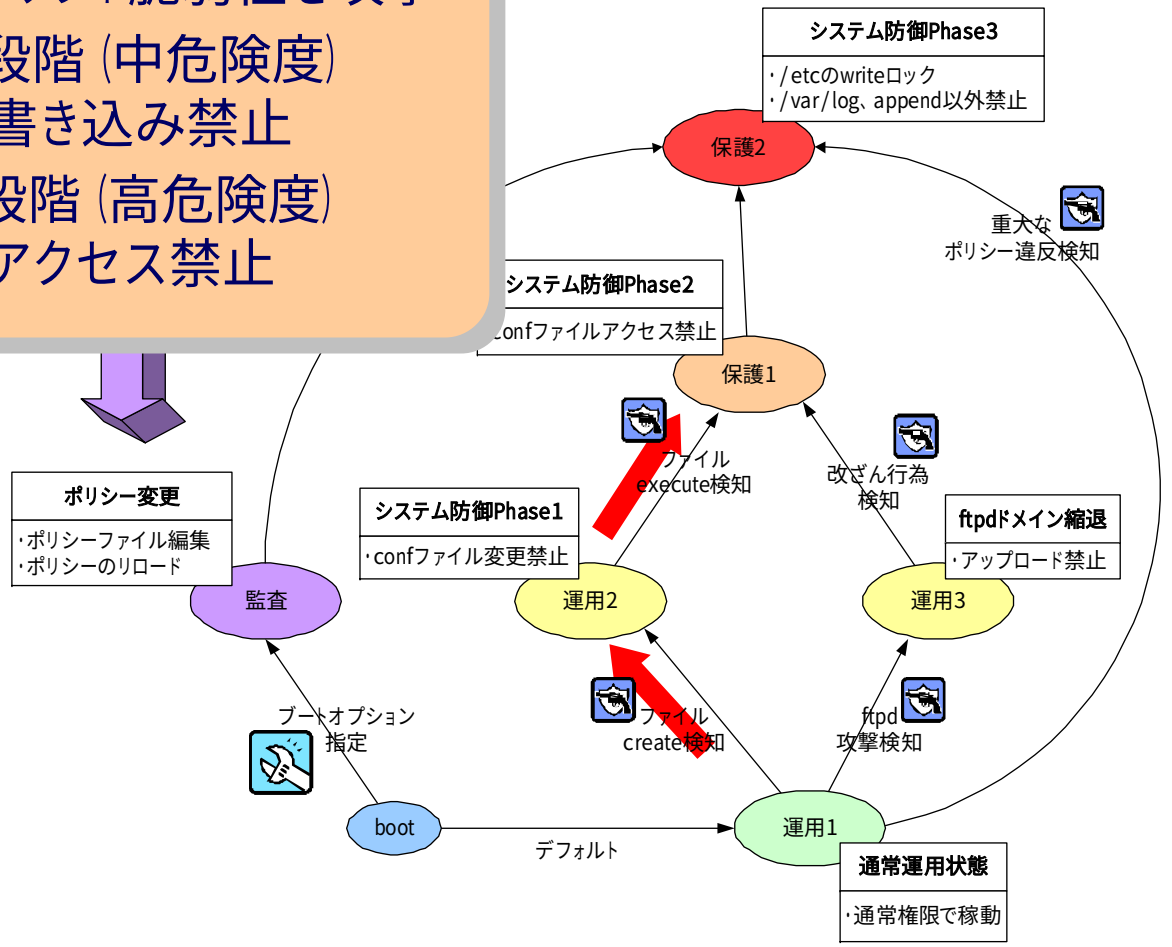
デモ１：対BOF防御

- wu-ftpdへのBOF攻撃を検知
  xinetdのセキュリティレベルUP
- 権限縮退
  以後起動されるftpセッションはupload禁止
- 既存セッションの維持
  既存ftpセッションはupload許可のまま維持



デモのご紹介

- デモ２：遷移パス制御
  - リモートからのＣＧＩスクリプト脆弱性を攻撃
  - /tmpへのツール設置段階（中危険度）
    → AP Confファイル書き込み禁止
  - /tmpでのツール実行段階（高危険度）
    → AP Confファイルアクセス禁止



まとめ

- SELinuxの不正アクセス検知への適用
  - OSカーネルレイヤでの検知･防御機構の実現
  - 検知対象定義“strict” ～ セキュリティチェック
  - 動的アクセスポリシー制御 ～ 権限縮退
- フレキシブルな状態制御
  - グローバルな権限縮退によるサービスレベル低下への対処
  - 制御範囲の指定、セキュリティレベル継承
  - 状態遷移の文脈性 ～ アクセスポリシーの「封印」

今後の課題・ロードマップ

- セキュリティツールとの連携
  - 他の IDS による検知情報を、動的アクセスポリシー制御の際のトリガとして利用
  - 本カーネルの検知機構を他の IPS のセンサとして利用
- 成果物の公開
  - GPL等のライセンスに基づく公開準備を現在、進めている。

「Linuxカーネルの動的アクセスポリシー制御」

ご清聴、ありがとうございました。

Please contact us for more information..

㈱ NTTデータ 技術開発本部
保理江 (mailto:horietk@nttdata.co.jp)

※ LinuxWorld .org Pavilion 内 JLA ブースにて
展示を行っています。