セキュアOS SELinux用 オープンソース設定ツール
―SELinux Policy Editor―

日立ソフトウェアエンジニアリング㈱
技術開発本部研究部
中村雄一

目次

1. SELinuxの必要性

2. SELinuxの機能紹介

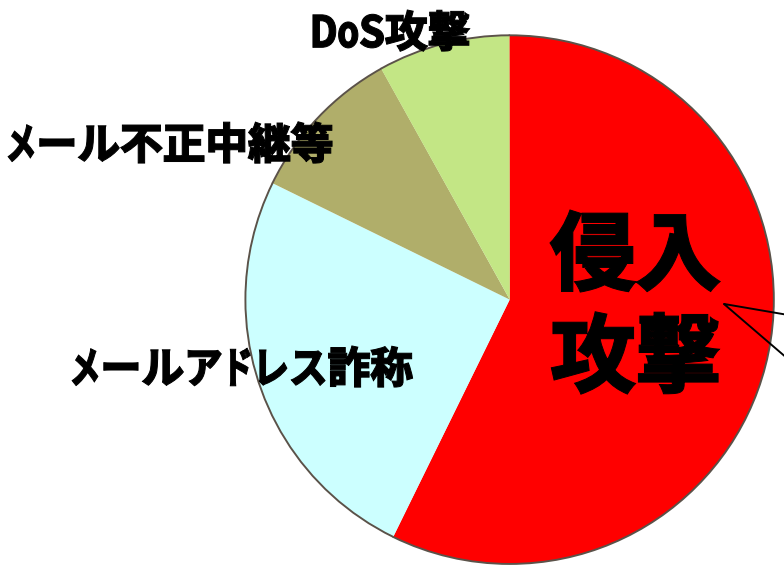
3. SELinux Policy Editorの紹介

4. 日立ソフトの取り組み

1. SELinuxの必要性

背景：侵入攻撃の脅威

不正アクセスの状況



ホームページ改ざん、
バックドア設置
システム破壊
顧客情報奪取
などやりたい放題

近年はワームによる無差別化

IPA:2002年不正アクセス届出状況のうち
未遂行為を除いたもの

**セキュアOSは侵入攻撃に
根本的に対処できる技術**

侵入攻撃の手順

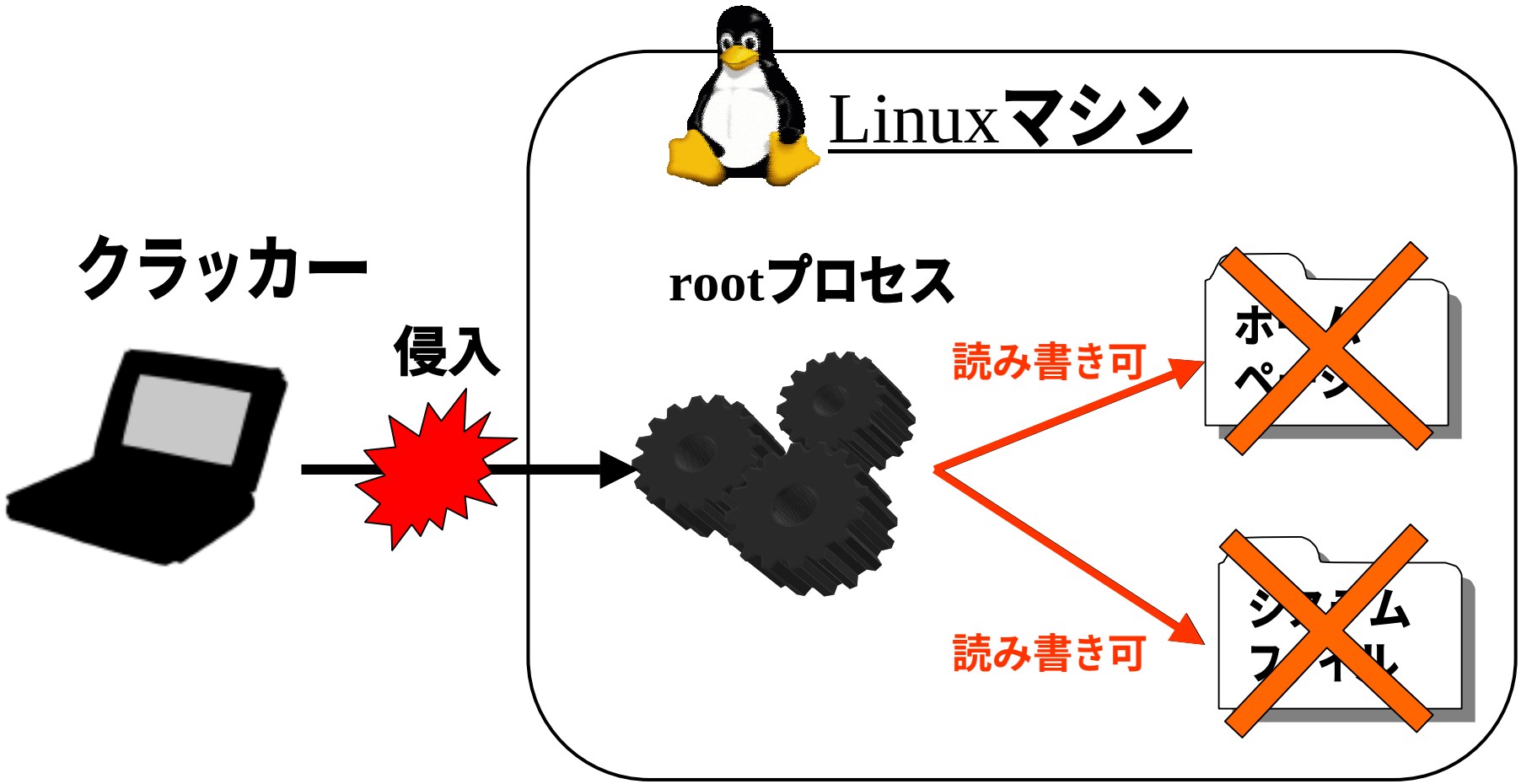
調査→侵入→root権限奪取→破壊

セキュリティホール発見
ポートスキャン
脆弱性検査ツール
など

セキュリティホールを利用
バッファオーバフロー
ヒープオーバフロー
フォーマットバグ攻撃
ＣＧＩ攻撃
など

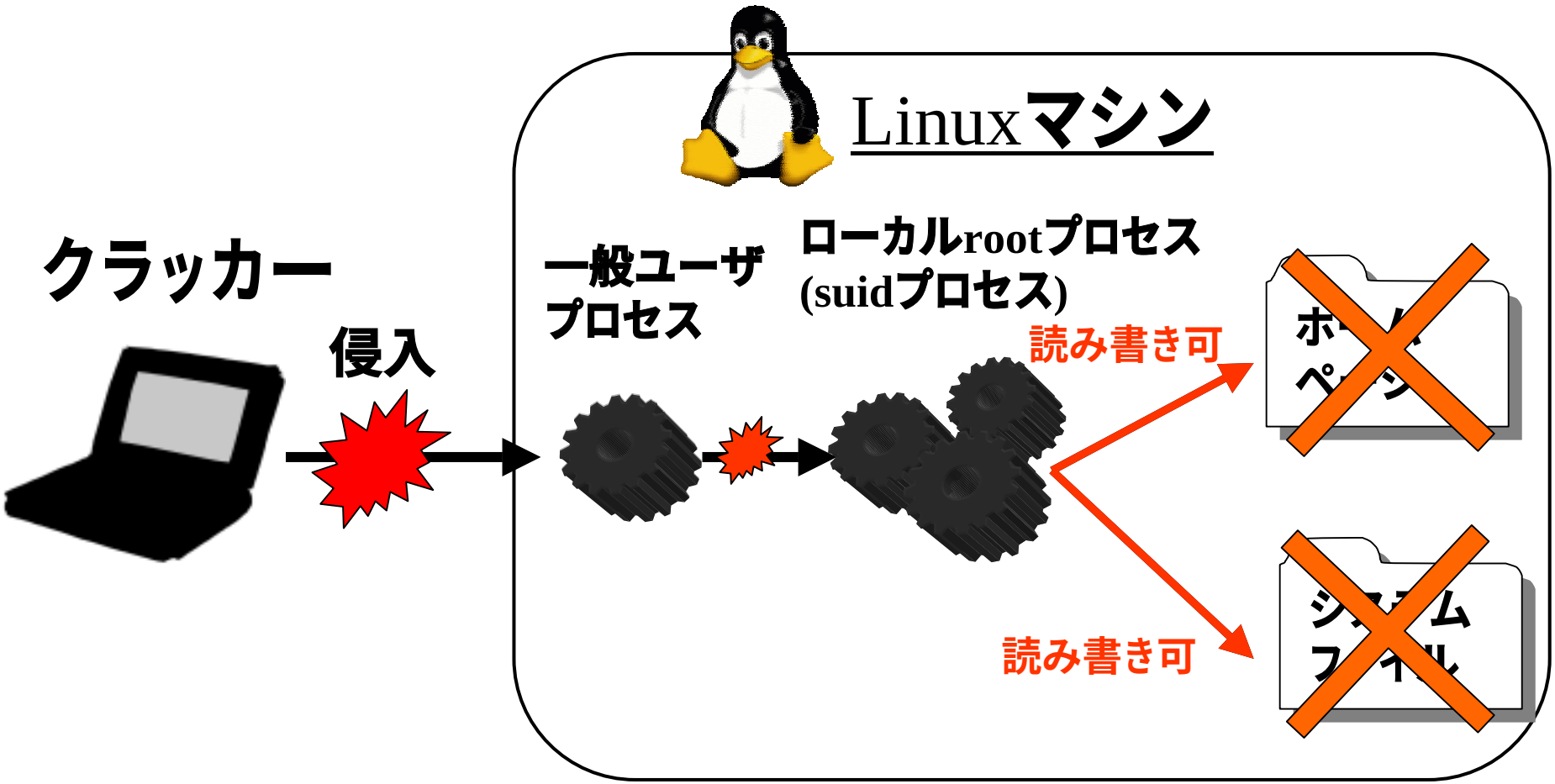
root権限を悪用
ホームページ改ざん
バックドア設置
システムファイル破壊
機密情報奪取
など

侵入攻撃例:リモートアタック



root権限を奪取するとクラッカーはやりたい放題

侵入攻撃例：ローカルアタック



一般ユーザからrootへ昇格し、破壊活動可能

従来の侵入攻撃対策

- **ファイアウォール**
  通過する通信を使った攻撃は防げない

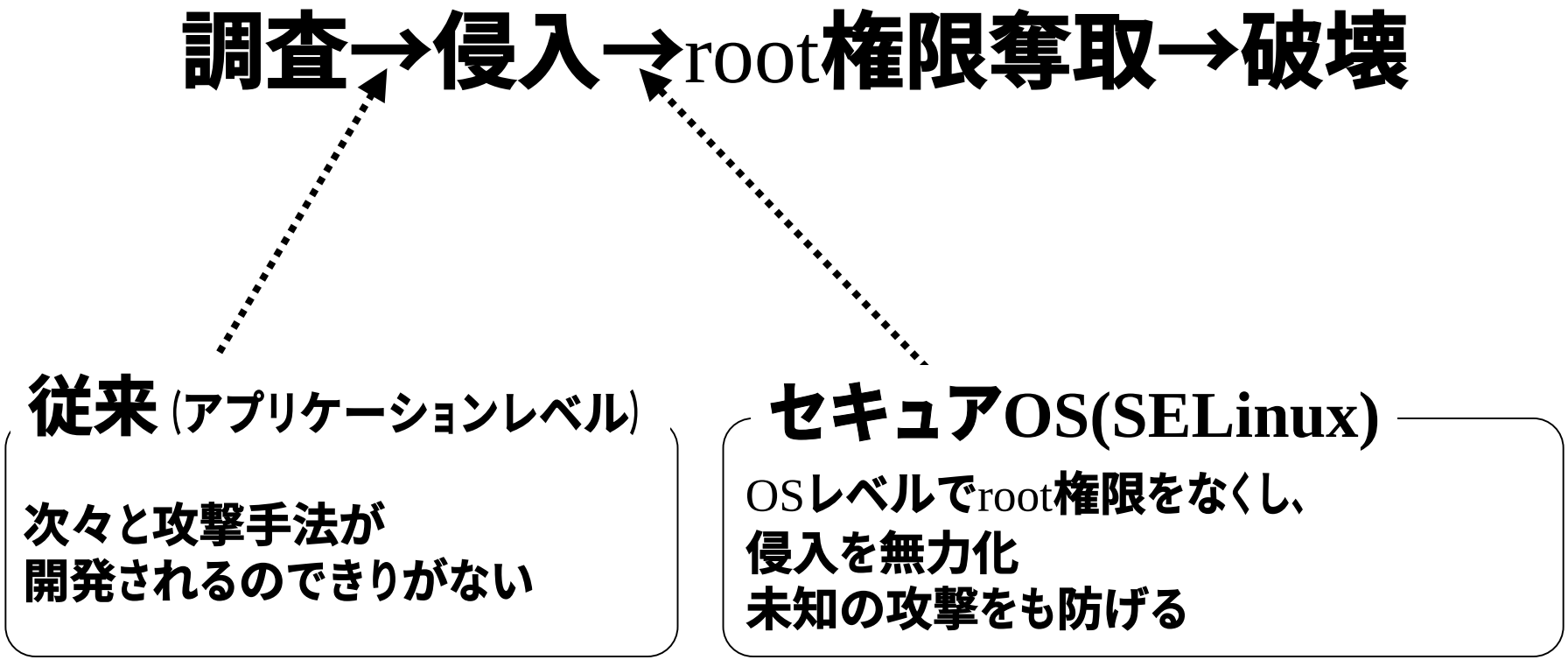
- **アプリケーションゲートウェイ（ファイアウォールの一種）**
  パケットをパターンマッチし攻撃と判定したらパケットの受付けを拒否する。
  パターンにない攻撃は防げない。

- **ＩＤＳ（侵入検知システム）**
  パケットをパターンマッチすることで侵入を検知し対策を促す。
  パターンにない攻撃は検知できない。

- **パッチ当て**
  パッチが間に合わないことがある、パッチ当てによる不安定

従来の対策は対症療法

セキュアOSの侵入攻撃対策



セキュアOSを使えば侵入攻撃を根本的に防げる

オープンソースのLinux用セキュアOS

- LIDS(Linux Intrusion Detection System)
  - Huagang Xie**氏開発**(www.lids.org)
  - **簡易なセキュア**OS**機能**
- SELinux(Security-Enhanced Linux)
  - **米国国家安全保障局**(NSA)**で開発**(www.nsa.gov/selinux/)
  - **本格的なセキュア**OS**機能**
  - **商用利用も始まっている**

SELinux**に注目が集まっている**

2．SELinuxの紹介

SELinuxの概要

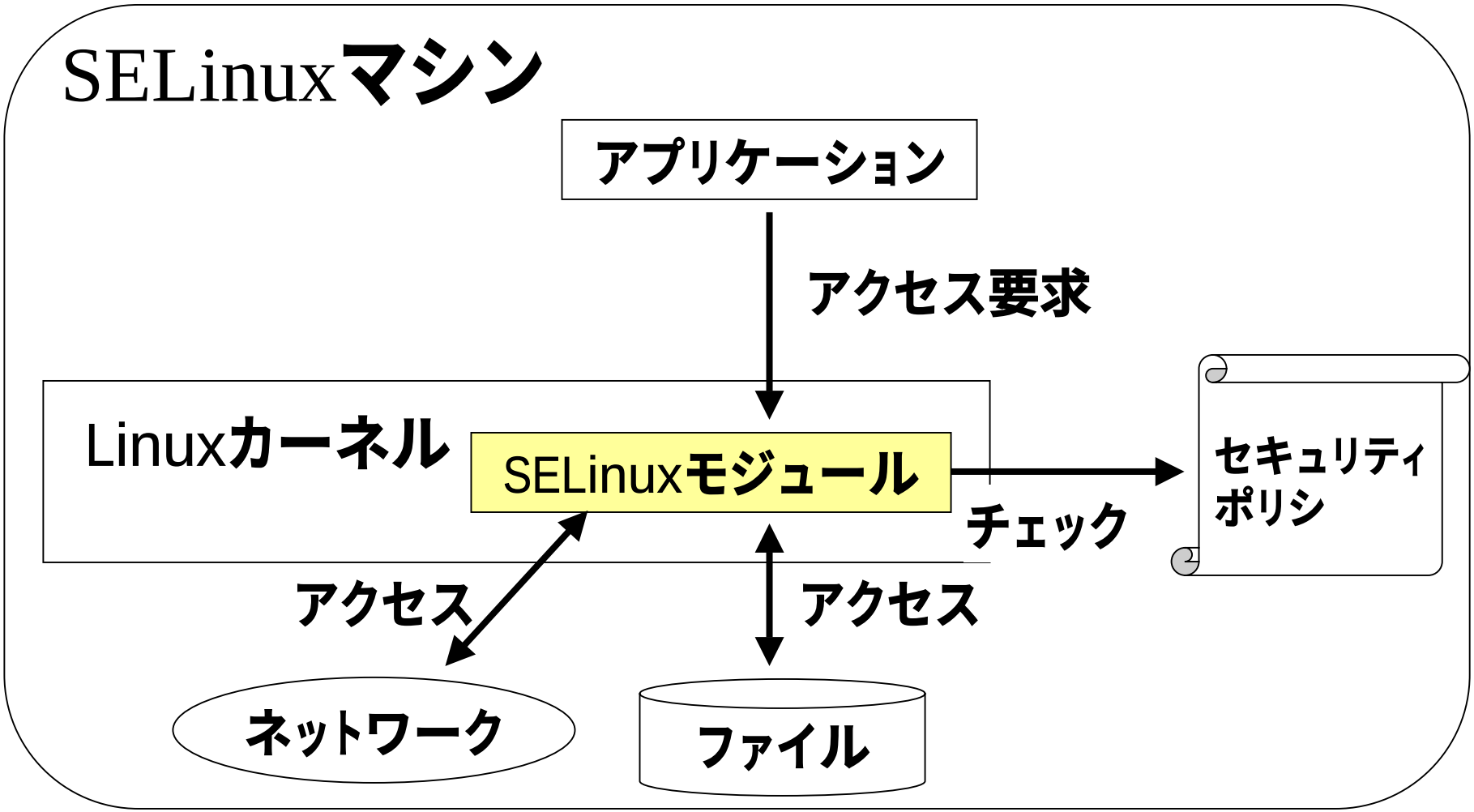
- NSA(米国国家安全保障局)で開発のセキュアOS、GPLで配布

- 高度なセキュリティ機能
  - 全てのプロセス、ユーザが必要最小限の権限
  - 監査ログの出力

  TCSEC(米国のセキュリティ評価基準。通称オレンジブック)
  C1～C2レベル相当：WindowsNT、普通のUNIX系OS
  B1レベル相当：SELinux

- 既存Linuxと高い互換性
  通常のディストリビューションに追加導入できる
  既存プログラムの改変の必要なし

SELinuxの構成



全てのリソースへのアクセスを厳しく制限

SELinuxの機能概要

- **強制アクセス制御:ＭＡＣ**(Mandatory Access Control)
  全てのプロセス、ユーザがアクセス制御を受ける

- **プロセス･ユーザ毎のアクセス制御機能:**
  TE,RBAC
  root**を排除、プロセス･ユーザが必要最小限の権限を持つ**

- **権限昇格制御機能**
  ローカルアタックを防ぐ

- **監査ログ出力機能**
  運用状況を監査

SELinuxの機能：MAC

- **普通の**Linux：**ＤＡＣ**(Discretionary Access Control)

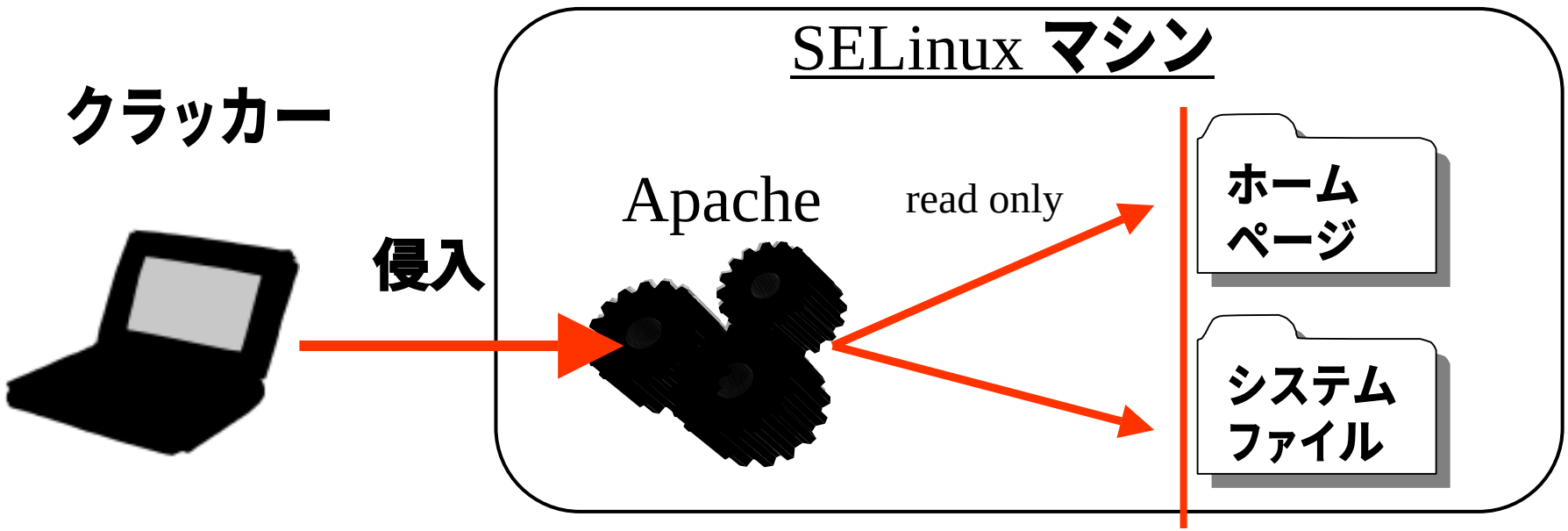
rootはセキュリティ設定を無視可能
一般ユーザでも自分のファイルに対する設定変更可
→セキュリティポリシを徹底できない

- SELinux：**ＭＡＣ**(Mandatory Access Control)

誰もセキュリティ設定を無視できない。
セキュリティ設定はセキュリティ管理者だけが変えられる
→セキュリティポリシを徹底可能

プロセス毎のアクセス制御機能：TE

- root権限はなく、プロセスが必要最小限の権限を持つ
- 細かいアクセス制御が可能
  - ファイル、デバイス、UDP・TCP・ICMP・UNIXソケット共有メモリ、セマフォ、パイプ、シグナル…など２８種類のリソースの制限が可能。



侵入しても破壊活動は困難

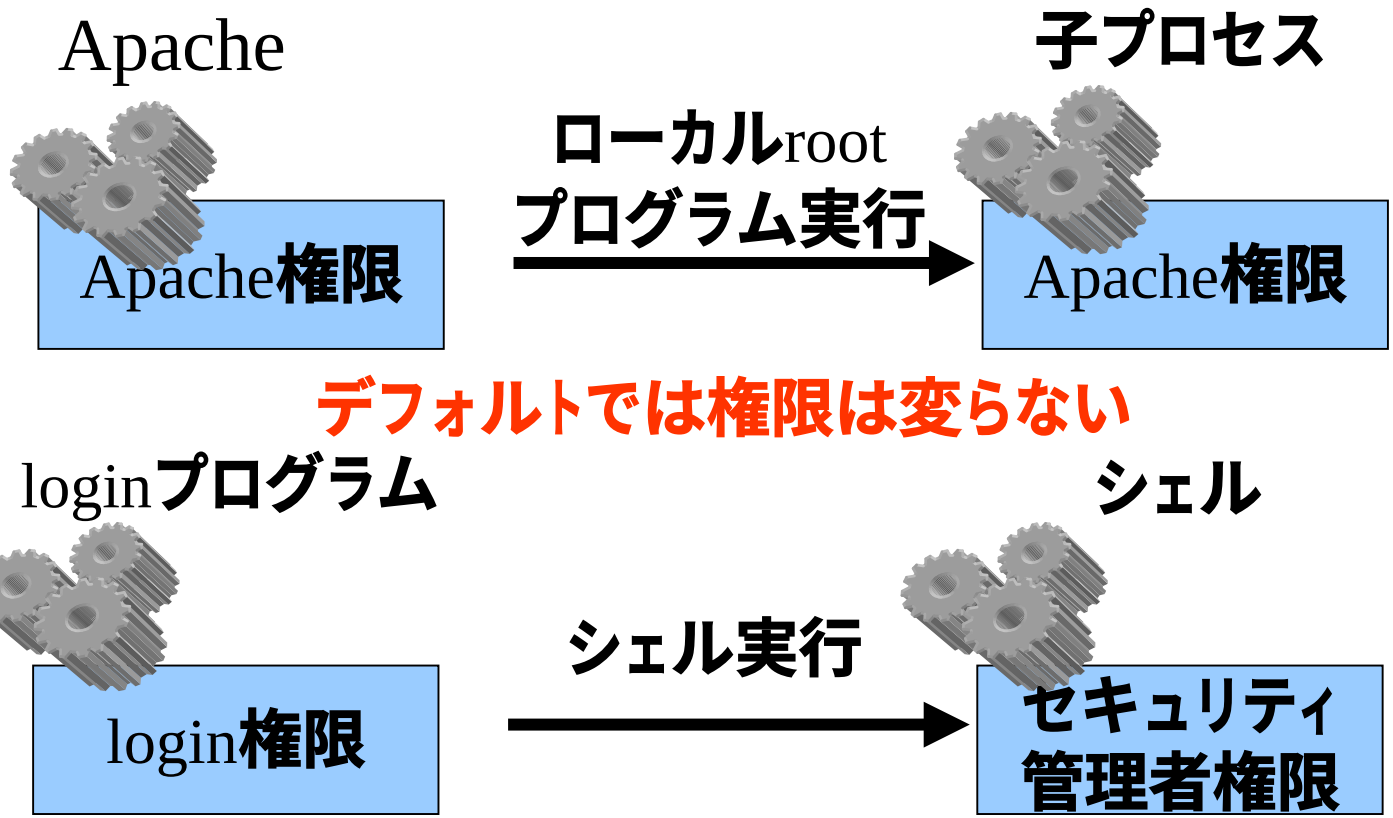
ユーザ毎のアクセス制御：ＲＢＡＣ
(Role Based Access Control)

- **従来のLinuxの管理ユーザ**
  rootユーザが全ての管理権限を持つ

- **SELinuxの管理ユーザ**
  複数の管理ユーザを設定し、管理権限を分割できる
  ネットワーク管理専用ユーザ、Web管理専用ユーザ
  などが作成可能

管理者の操作ミス、悪意ある操作の被害を最小化

権限遷移の制御



権限昇格によるローカルアタックを防げる

監査ログ機能

- **権限外の操作をしようとしたログ**

例：Apacheを乗っ取った攻撃者がシェルの起動を失敗した場合

Apr 21 13:31:15 host_xx kernel: avc: **denied { execute }** for pid=987
exe=/usr/sbin/httpd path=/bin/sh dev=08:01 ino=962840
scontext=system_u:system_r:httpd_t tcontext=system_u:object_r:shell_exec_t class=file

- **重要リソースのアクセスが許可されたログ**

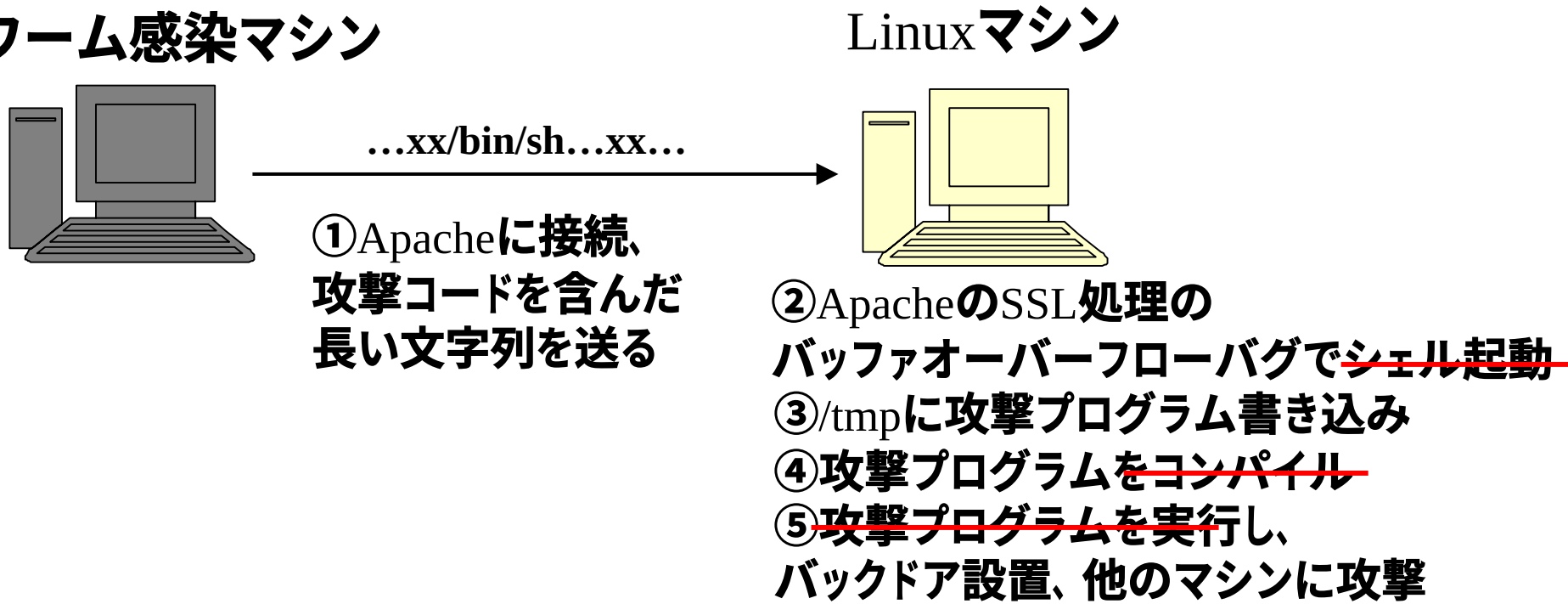
例：webmasterユーザがホームページの更新をした場合

Apr 21 13:31:15 host_xx kernel: avc: **granted { write }** for pid=987 exe=/bin/vi
path=/var/www/html/index.html dev=08:01 ino=962840
scontext=**webmaster**:webmaster_r:webmaster_t
tcontext=system_u:object_r:web_contents_t tclass=file

攻撃者・管理者の行動を細かく監査可

SELinuxへの攻撃例：Slapperワーム

Slapperワーム：OpenSSLの脆弱性を利用しApacheに感染するワーム



SELinuxの場合、Apacheはシェル、コンパイラ、攻撃プログラムの実行権限を持たないので、Slapperワームの被害を受けない

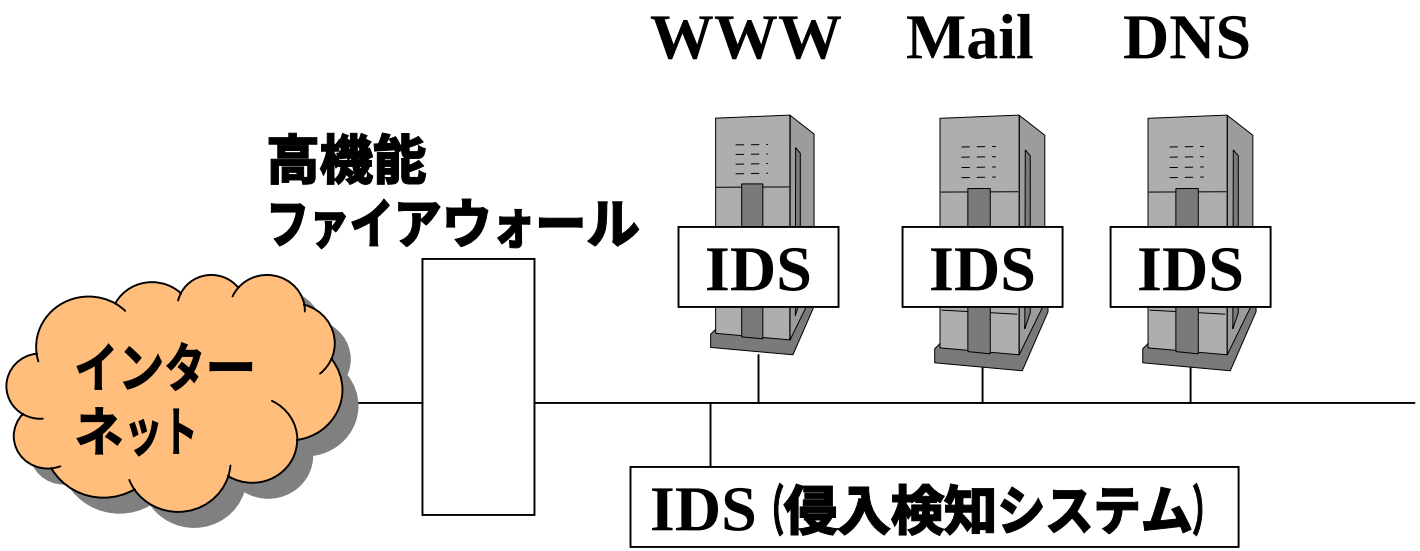
SELinuxのパフォーマンス

- セキュリティチェックのオーバヘッド
  - 全般的に数パーセント～10%程度
- 例：Apache
  - 静的ページ転送速度はほとんど性能差なし
- 例：PostgreSQL
  - 処理できるトランザクション数が2%程度低下

SELinuxによるオーバヘッドは実用上問題ない

SELinux導入のメリット

従来のセキュアサーバシステム

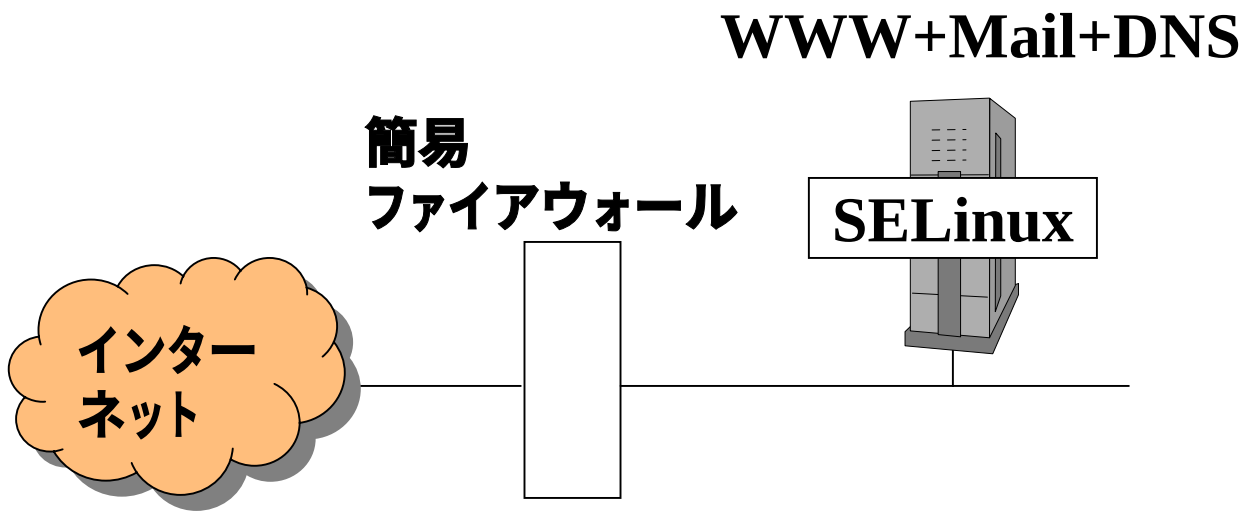


・複数台サーバを設置
・高価なセキュリティ機器を複数導入
・常時ログ監視、パッチ適用

ここまでやっても未知の攻撃には対処不可

SELinux導入のメリット

SELinuxを適用したセキュアサーバシステム



- サーバの統合が可能（侵入の影響が局所化されるので）
- 高価なセキュリティ機器は不要
- パッチ適用はリアルタイムである必要はない
- 未知の攻撃にも対処可能

安価でセキュアなシステムを実現可

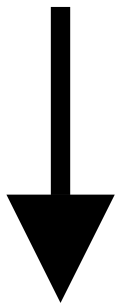
SELinuxを導入する際の留意点

- SELinuxのセキュリティは設定次第
  - 設定を間違えるとどうにもならない
- 遠隔保守には気をつける
  - パスワードの管理、通信路の暗号化、接続元の限定
- 侵入以外の脅威には別途対策が必要
  - DoS攻撃、メール不正中継など
- 大きな権限をもつプロセスの公開に気をつける
  - 特に遠隔管理用デーモンには要注意
    ※従来よりは侵入に強い

まとめ：SELinux

SELinux

- アクセス制御が例外なく強制（ＭＡＣ）
- 全てのプロセス、ユーザが最小限の権限を持つ（ＴＥ，ＲＢＡＣ）
- 権限の遷移が厳しく制限
- 監査ログ出力

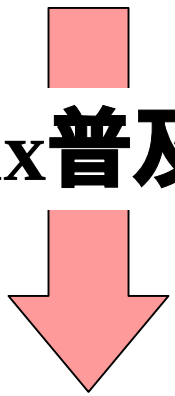


- SELinuxは侵入攻撃全般に耐性
- 安価でセキュアシステムが構築可能

3. SELinux Policy Editor

設定ツールの必要性

SELinuxのセキュリティ機能は設定次第
→しかし、設定は大変複雑



SELinux普及の妨げ

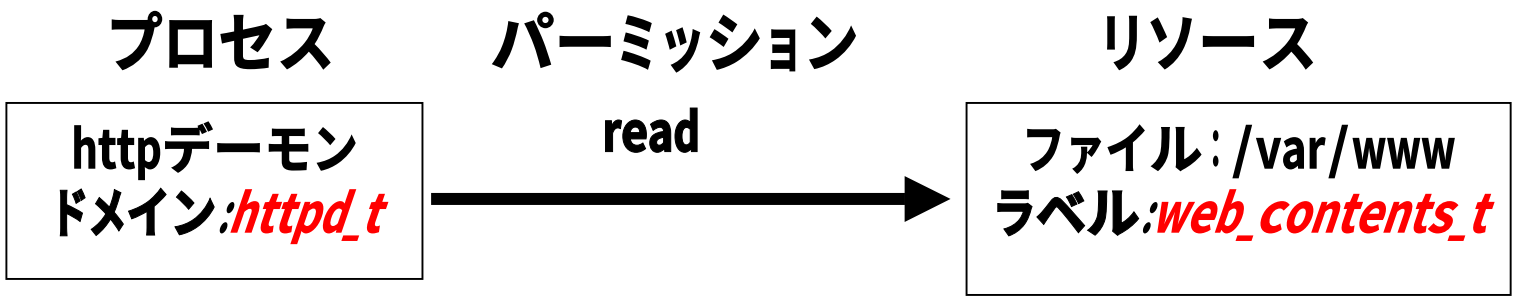
日立ソフトでSELinux設定ツール
「SELinux Policy Editor」を開発

SELinuxの設定の基本

ドメインとラベルの間に許可するパーミッションを記述して設定

ドメイン：プロセスに付与する権限名
ラベル：リソースに付与する識別名

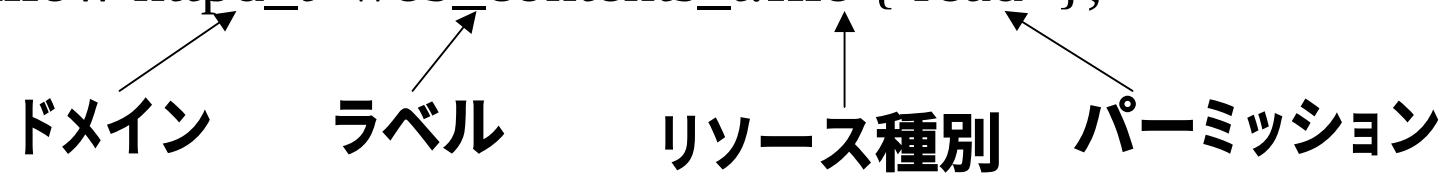
例：httpデーモンに対してホームページのアクセス許可を与える場合



SELinux設定言語

- allow文：ドメインにラベルへのパーミッション付与

例：**allow** httpd_t web_contents_t:file { read };



- マクロ

例：can_network(httpd_t)

```
…
allow httpd_t:port_t tcp_socket name_bind;
allow httpd_t:port_t udp_socket name_bind;
…
```

ネットワーク利用許可の13個のallow文に展開

- リソースとラベルの関連付け

例：/var/www(|/.*)　system_u:object_r:web_contents_t

設定言語の問題概要

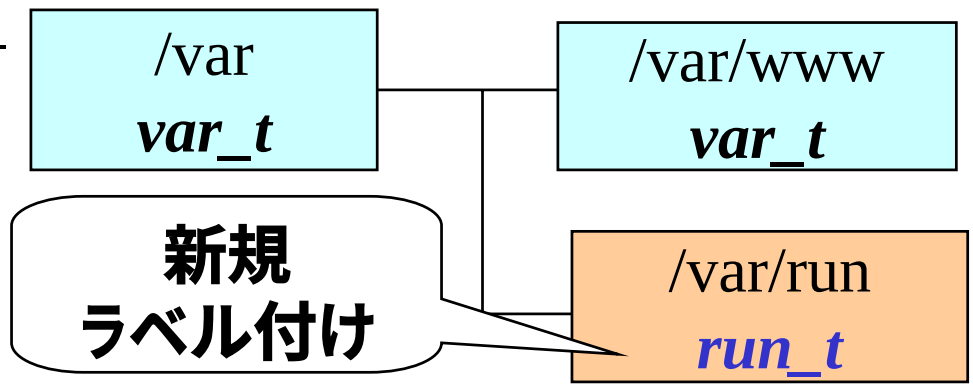
- リソースのラベル付けが煩雑
- 設定項目が膨大
- 設定の確認が困難

問題1

- リソースのラベル付けが煩雑
  - ラベル付けの競合
  - ラベル名の重複

ラベル付けの競合の例：

・ファイル・ラベルの対応



・some_tは/var以下をread可：**allow** *some_t var_t*:file {*read*}

新規ラベル付けしたファイルにsome_t**はアクセス不可になり設定の追加が必要**

問題2、3

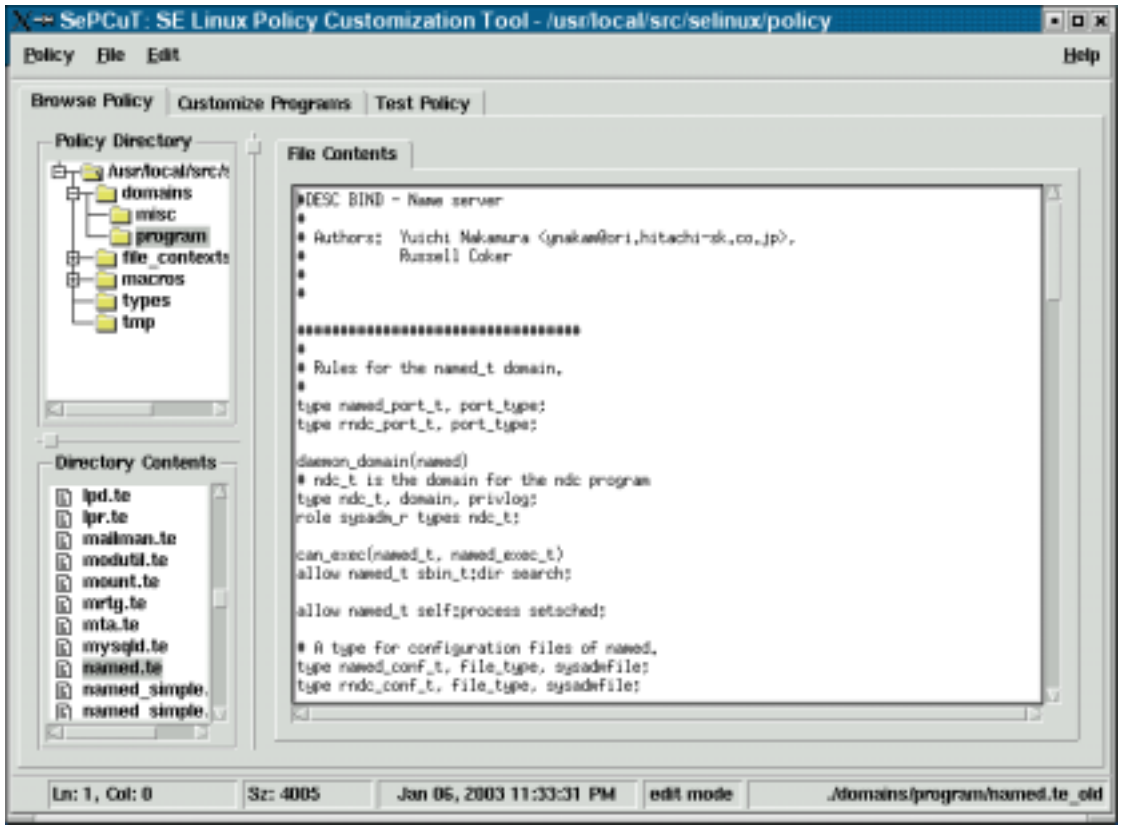
- 設定項目が膨大
  - リソース種別、パーミッション、マクロが膨大

  例：ファイル種別7種、ファイルパーミッション17種
  　　マクロ１５０個以上
  →設定ファイル数200以上、行数10000行以上に

- 設定の確認が困難
  - テキストベース
  - リソースにアクセス可能なドメインが分からない

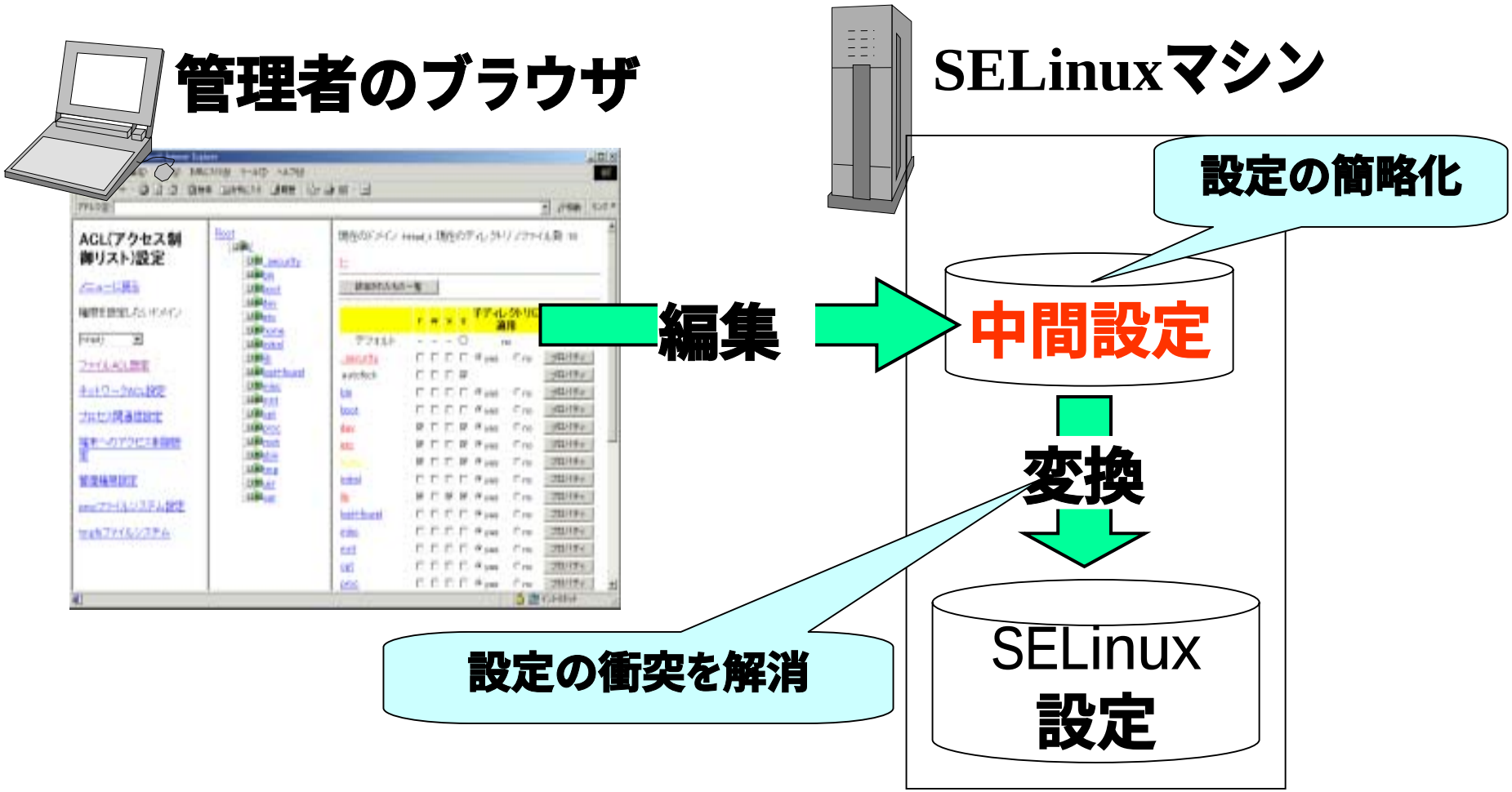
設定状況の把握・設定の編集が困難

従来の設定ツール：setools



ソースコードブラウザ
設定方法自体は簡単にならない

SELinux Policy Editor



中間設定

- リソースを直接指定

例：

```
domain httpd_t;
allow /etc/httpd r;
allownet -tcp -port 80;
```

httpd_tドメインは
/etc/httpdを読み込み可
TCP80番ポートを使用可

- 設定項目の絞込み

ーリソース種別とパーミッションのうち使用頻度の低いものを統合

例：

従来の設定言語	中間設定
7種類のファイル種別 file dir lnk_file chr_file blk_file sock_file fifo_file	「ファイル」に統合
4種類のパーミッション read getattr ioctl lock	「r（読み込み）」に統合

中間設定からSELinuxへの変換

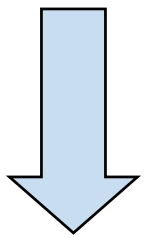
1. リソース名からラベルを生成

2. SELinux設定言語の出力
   - allow文の出力
   - リソースとラベルの関連付けを出力

変換例

変換前

```
domain one_t;      domain two_t;
allow /var r;      allow /var/www r;
```



/var以下：var_t
/var/www以下：var_www_t
というラベル生成

変換後

```
allow one_t var_t:file r_file_perms;
allow one_t var_www_t:file r_file_perms;
allow two_t var_www_t:file r_dir_perms;
…その他6つのファイル種別にも同じallow文
/var(/.*) system_u:object_r:var_t
/var/www(/.*) system_u:object_r:var_www_t
```

子ディレクトリに対するラベルのallow文も出力、ラベルの競合解消

GUIの画面

設定状況を視覚的･多角的に表示

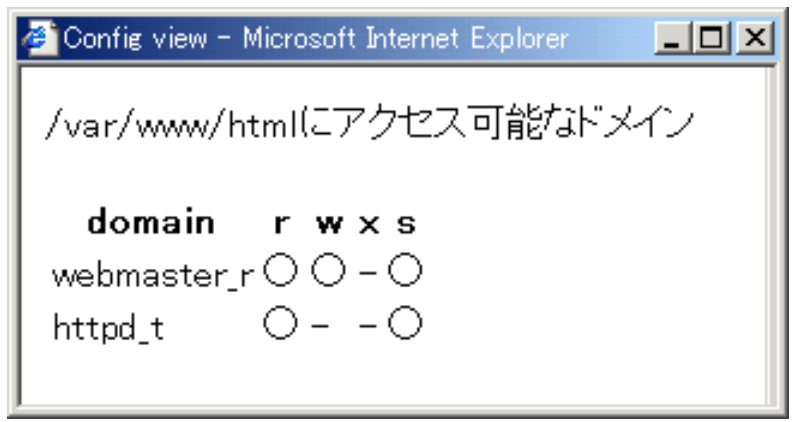
ドメインから見た権限

現在のドメイン :httpd_t :現在のディレクトリ :/var/www

	r	w	x	s	子ディレクトリに適用	
cgi-bin	☑	☐	☑	☑	○ no	◉ yes
html	☑	☐	☐	☑	○ no	◉ yes
icons	☑	☐	☐	☑	○ no	◉ yes

適用

リソースから見た権限



まとめ：SELinux Policy Editor

- SELinux Policy Editor **によって設定方法自体が簡単になった**
  - **リソースを直接指定（中間設定）**
  - **設定項目の絞込み（中間設定）**
  - **設定を視覚的・多角的に確認（GUI）**
- http://www.selinux.hitachi-sk.co.jp/ **にて**
  オープンソースで公開
  - 2003**年**1**月：α版**
  - 2003**年**5**月：β版**

4．日立ソフトの取り組み

日立ソフトのSELinuxに対する取り組み

当社のSELinuxに対する取り組みの経緯

2001年　SELinuxに関する調査を開始
2001/08　IPA殿公募採択(オペレーティングシステムのセキュリティ機能拡張の調査)
2001/10　LinuxWorldにてSELinuxを初出展
2002/05　LinuxWorldにてSELinuxのセキュア遠隔管理ツール発表、ワークショップ講演
2002/10　IPA殿公募採択(セキュアなインターネットサーバー構築に関する調査)
2003/01　ポータルサイト公開による情報提供(http://www.selinux.hitachi-sk.co.jp/)
2003/01　SELinux Policy Editor α版　GPLで公開
2003/02　net&com2003にてポリシー設定ツール公開・展示。
2003/04　日経Linux5月号「特集１　究極のセキュアOSを簡単導入」執筆
2003/05　SELinux Policy Editor β版　GPLで公開

- ツール類の整備
- SELinuxの普及活動
- SELinuxシステム構築サービスの提供

ツール類の整備

- **構築･運用ツール**
  - セキュア遠隔管理ツール「Secure Webmin」の開発
    LinuxWorld Expo/Tokyo 2002にて発表
  - SELinux設定ツール「SELinux Policy Editor」の開発
    net&com2003にて発表、GPLで公開
- **監査ツール**
  - ログ監査ツール
  - 設定脆弱性監査ツール

SELinuxの普及活動

- IPA受託調査によるSELinux関連ドキュメント作成
  - 「オペレーティングシステムのセキュリティ機能拡張の調査」
    http://www.ipa.go.jp/security/fy13/report/secure_os/secure_os.html
  - 「セキュアなインターネットサーバー構築に関する調査」
    http://www.ipa.go.jp/security/fy14/contents/trusted-os/guide.html
- ポータルサイト開設による情報提供
  - http://www.selinux.hitachi-sk.co.jp/
- SELinux Policy Editorのオープンソースでの公開
- 展示会での講演、雑誌記事の執筆
  - Linux World Expo/Tokyo 2002ワークショップ講演
  - 日経Linux 5月号　特集1執筆

SELinuxシステム構築サービス

- コンサルテーションサービス
  - 標準コンサルテーション
  - アプリケーションのセキュリティポリシー設計
  - 管理者ユーザ権限の提案
- システム構築サービス
  - SELinuxインストール･基本設定
  - アプリケーションのセキュリティポリシー設定
  - 運用マニュアル作成
- サポートサービス
  - ヘルプデスクサービス
  - メンテナンスサービス
  - オンサイトサポートサービス

参考文献

- セキュアOSやSELinuxの概要
  - 日立ソフトのSELinuxページ

    http://www.selinux.hitachi-sk.co.jp/

    SELinux関連のドキュメント、SELinux Policy Editorのドキュメント
  - 日経Linux 5月号　特集1

    セキュアOSの概要、SELinuxの設定方法の概要
- セキュアOSやSELinuxの詳細
  - 「オペレーティングシステムのセキュリティ機能拡張の調査」

    http://www.ipa.go.jp/security/fy13/report/secure_os/secure_os.html

    様々なセキュアOSの概要と、SELinuxについて
  - 「セキュアなインターネットサーバー構築に関する調査」

    http://www.ipa.go.jp/security/fy14/contents/trusted-os/guide.html

    SELinuxの設定方法の詳細
  - SELinux配布サイト

    http://www.nsa.gov/selinux/

DIGITAL & GLOBAL
日立ソフト

お問い合わせは
日立ソフトウェアエンジニアリング (株)
プラットフォーム設計部
e-mail: linux@kam.hitachi-sk.co.jp
URL:http://www.selinux.hitachi-sk.co.jp/
まで