SELinuxと日立ソフトの取り組みのご紹介

日立ソフトウェアエンジニアリング (株)
2007年6月14日

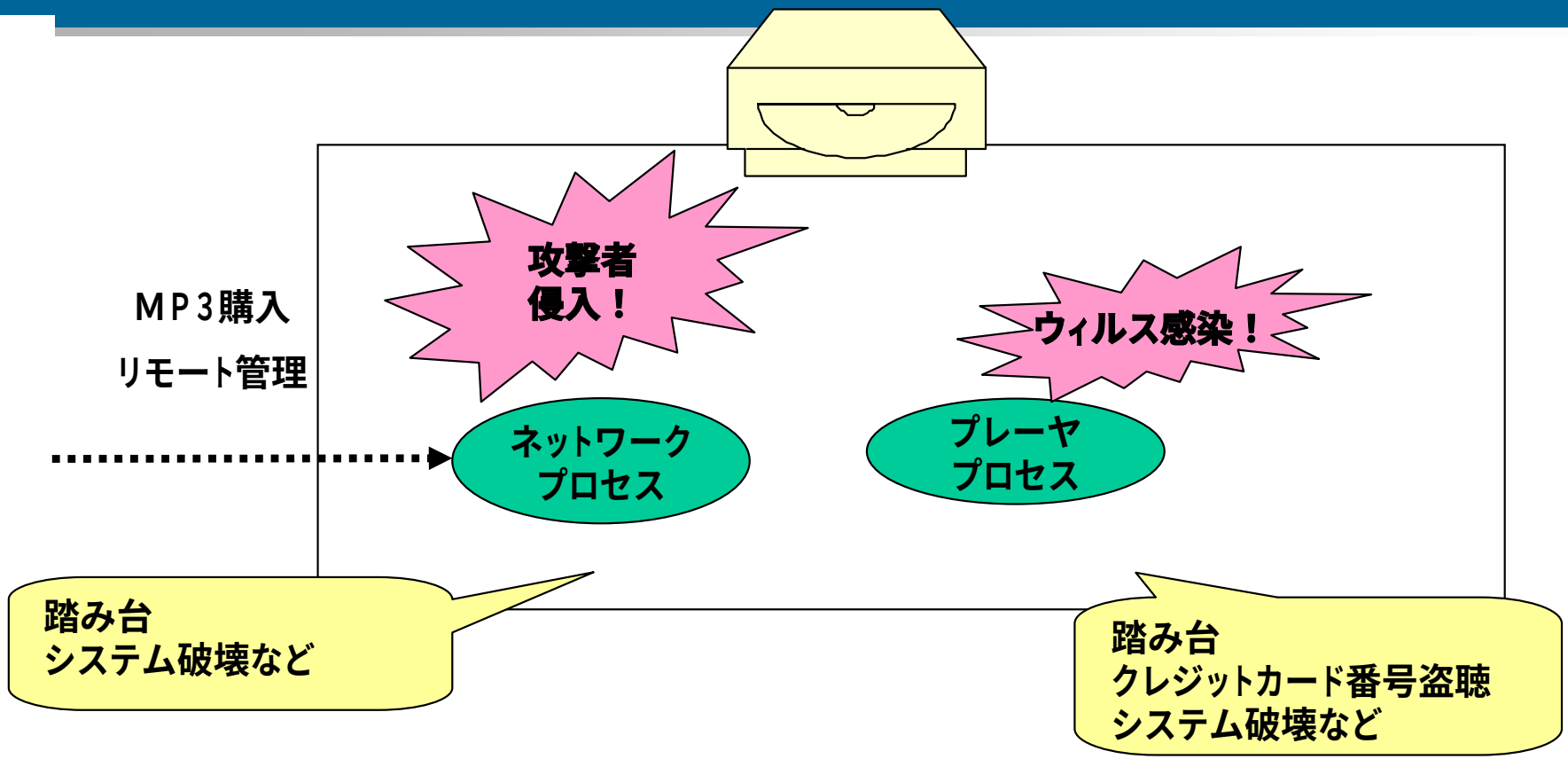
お問い合わせ：技術開発本部 研究部　中村雄一
ynakam@hitachisoft.jp

HitachiSoft
創る、支える、拓く

背景：組込み機器とセキュリティ

- 最近の組込み機器
  - ネットワーク接続、PC化
  - Linux適用の拡大
  - アップデート困難
  - 攻撃者にとって好都合に
- 業界のセキュリティ意識は高くない
  - 全部root、認証無しなど
  - Windows95時代を彷彿
- ＰＣで起こったことが組込み機器でも
  - ハッキング、ワーム、ウィルス、踏み台化
  - 攻撃も始まりつつある
    - 携帯電話ウィルス感染
    - ATM, POS端末，プリンタウィルス感染
    - ルータ、NICの攻略
    - DVDレコーダ踏み台化

ネットMP3プレーヤの脅威例



攻撃者はやりたい放題！

組込み機器で脆弱性が発見されると

アップデート困難なので、回収、店頭での対策などが必要

→対策費用も膨大に（あるケースでは120億円）（※IPA「組込みソフトウェアを用いた機器におけるセキュリティ」より）

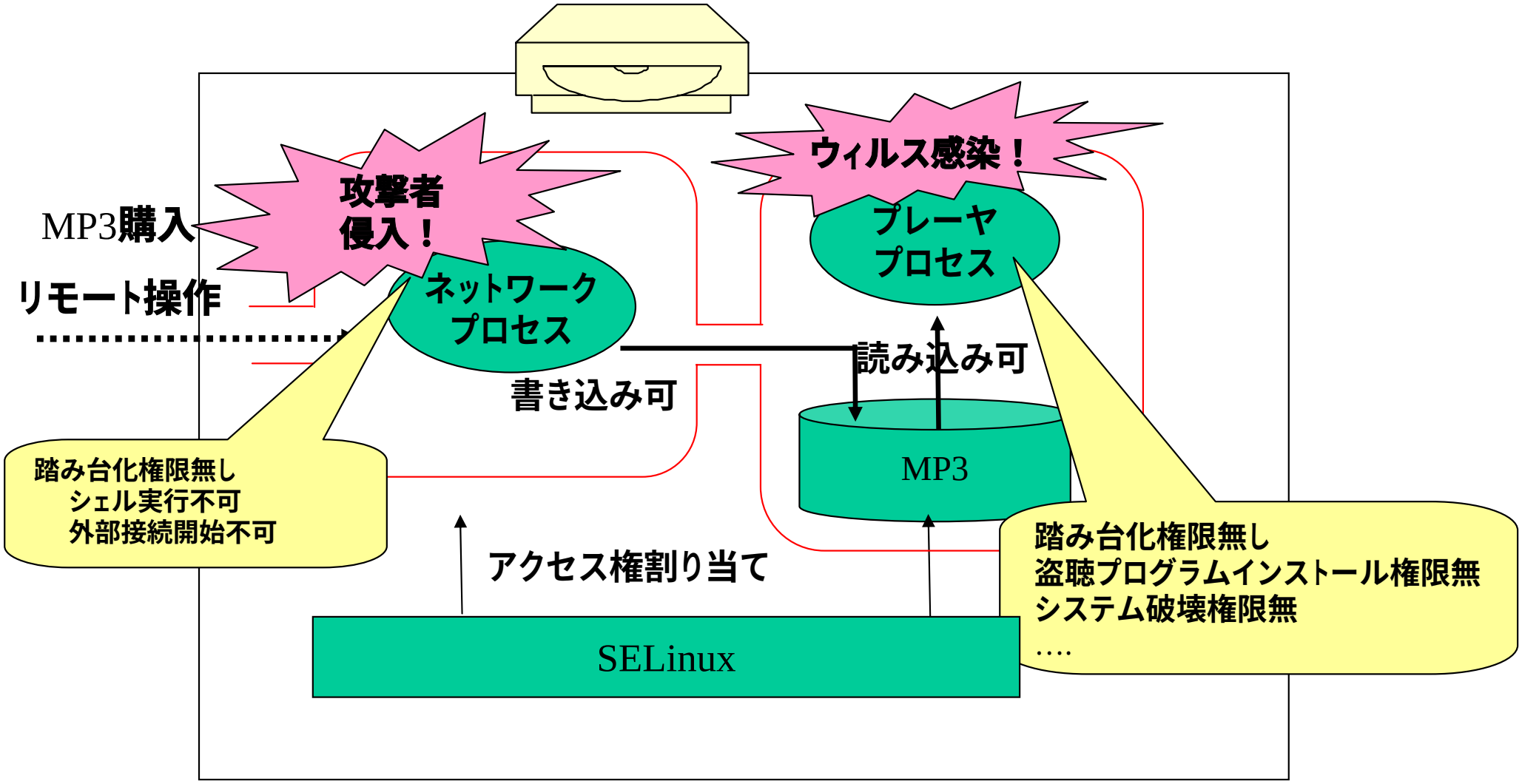
SELinuxとは

- セキュアＯＳ技術
  - プロセス毎に必要最小限の権限を割り当て
  - rootでさえ回避できない
  - 攻撃者が持てる権限も最小化

- Linuxカーネル2.6標準オプション

- 組込みに適
  - 軽い対策
  - アップデート無しでも耐性あり
  - アーキテクチャ非依存

SELinuxの効果



攻撃者、ウィルスの動作を封じ込める
アップデート無しでも耐性

日立ソフトのSELinuxに対する取り組み

- SELinuxリリース直後より取り組み(2001)～
- 普及活動の主導
  - Linuxコンソーシアム www.linuxcons.gr.jp (理事)
  - SELinuxユーザ会 www.selinux.gr.jp(代表)
  - 多数の執筆、講演：SELinux書籍, 日経Linux, ITMedia,@ITなど
- 技術開発
  - ツール類の開発
    - SELinux Policy Editor, SELinux/Aid
  - SELinux Symposium 2005,2006@ワシントンDC での発表
- サーバ向けソリューション開発
  - セキュアLinuxソリューション http://hitachisoft.jp/product/secure-linux/
  - DMZ向けサーバ、シングルサインオンサーバ等に実績

組込みSELinuxへの取り組み事項

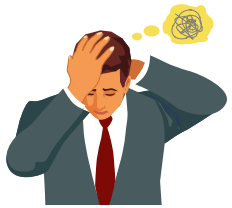
- 移植、評価、チューニング
- 設定支援ツール
- コミュニティとの共同作業

SELinuxの移植、評価、チューニング

- Zaurusに移植、評価
  - 移植作業
    - BusyBoxの対応、ライブラリ等を移植
      - BusyBox: 組み込みLinuxで標準的に使われるツール
    - 測定
      - パフォーマンス、メモリ消費量、ストレージ増加サイズ
  - チューニング
    - 例：ストレージ容量数M→数百K
- 移植にはノウハウが必要
  - 様々なパッチが必要
  - 特に設定作業

設定支援ツール (SELinux Policy Editor)

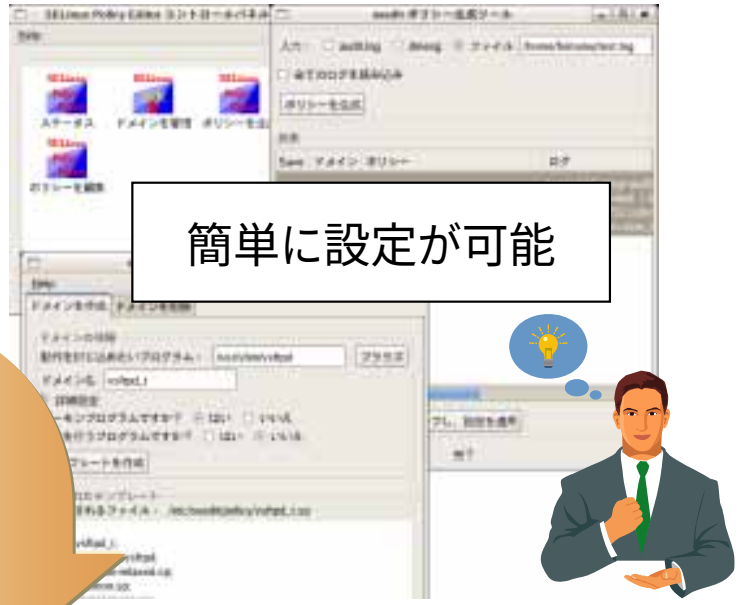
SELinuxのポリシーの設定は複雑で難しい・・・。



当社開発の設定支援ツール

「SELinux Policy Editor」

※ OSSで公開 ⇒ http://seedit.sourceforge.net/



従来の設定書式(Apacheの設定)

```
policy_module(apache,1.3.16)
attribute httpdcontent;
attribute httpd_exec_scripts;
attribute httpd_script_exec_type;
type httpd_t;
type httpd_e
init_daemon_
role system_
....
ifdef(`target

')
optional_policy(
                prelink_object_file(httpd_modules_t)
')
...
allow httpd_t httpd_sys_content_t:dir r_dir_perms;
allow httpd_t httpd_sys_content_t:file r_file_perms;
allow httpd_t httpd_sys_content_t:lnk_file r_file_perms;
...
corenet_non_ipsec_sendrecv(httpd_t)
corenet_tcp_sendrecv_all_if(httpd_t)
corenet_udp_sendrecv_all_if(httpd_t)
corenet_tcp_sendrecv_all_nodes(httpd_t)
corenet_udp_sendrecv_all_nodes(httpd_t)
corenet_tcp_sendrecv_all_ports(httpd_t)
corenet_udp_sendrecv_all_ports(httpd_t)
corenet_tcp_bind_all_nodes(httpd_t)
corenet_tcp_bind_http_port(httpd_t)
corenet_tcp_bind_http_cache_port(httpd_t)
corenet_sendrecv_http_server_packets(httpd_t)
....
/var/www(/.*)  --  gen_context(system_u:object_r:httpd_sys_content_t, s0)
```

「誰が」「何に」「どんなアクセスができるか」を細かく設定

- ルール数が数万～数十万
- 複雑な書式

SELinux Policy Editorの設定書式

```
domain httpd_t;
program /usr/sbin/httpd;
allow /var/www/** r;
allownet –protocol tcp –port 80 server;
```

コミュニティとの協調

- 基盤部分は、コミュニティと協調
  - オープンソースのサポートには、コミュニティと渡り合う力が必要
- BusyBoxのSELinux対応
  - SELinux管理コマンドをBusyBoxに移植
  - BusyBox Projectに提案、マージ
- SELinuxのサイズ削減パッチ
  - SELinuxコミュニティに提案、マージ
- CELinux Forumでの発表

組込みLinuxセキュリティ強化サービス

- SELinuxのポーティング
  - Linux2.6には標準装備。実装にはノウハウが必要。
  - 実装を日立ソフトがコンサル、請け負い・支援します

- Linuxセキュリティのサポートサービス
  - SELinuxを中心にしたセキュリティ全般のサポートサービス
    - ドライブ暗号、バッファオーバーフロー防止技術など評価中