OSAKA NDS Embedded Linux Cross Forum #3

R-Car H3 コンピューティングプラットフォーム向け AGLセキュア実行環境の取り組み

- R-Car H3 Computing Platform for Secure Execution Environment. –

株式会社大阪エヌデーエス
エンベデッドグループ
Linuxチーム 伊東　賢一

1人の満足から、社会の満足へ
株式会社大阪エヌデーエス

IVIの未来 - いつか来た道

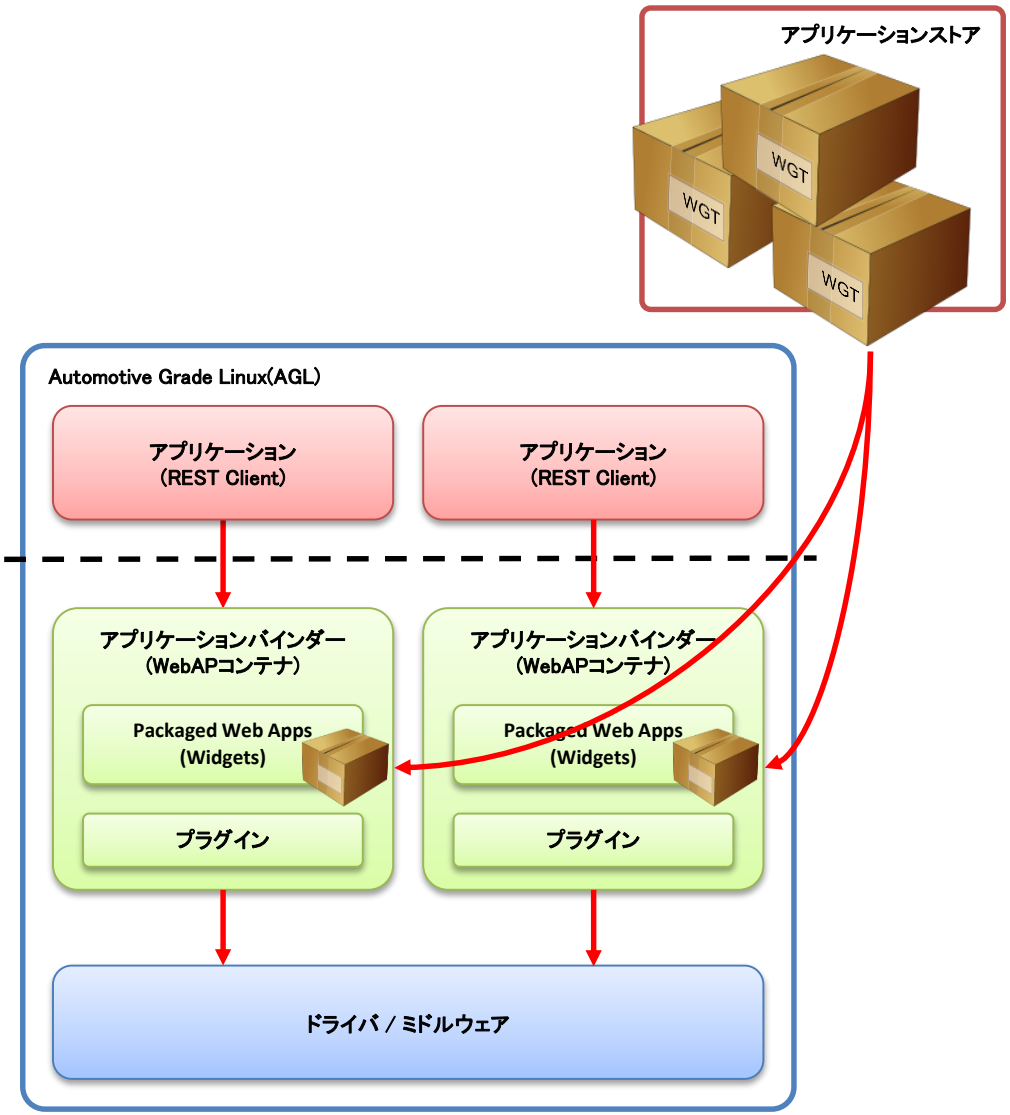
- 携帯電話で起こったこと
  - 開かれたデータネットワーク・開かれたアプリケーション実行環境が、新たなユーザー体験を提供した。
  - 新たなユーザー体験が、巨大な市場を創出した。

と、同時にスマートホンでは悪意のあるアプリケーションや、セキュリティホールとなるアプリケーションも出現。

IVIにおいては、歴史に学び安全なネットワーク接続・アプリケーション実行環境の実装が必要。

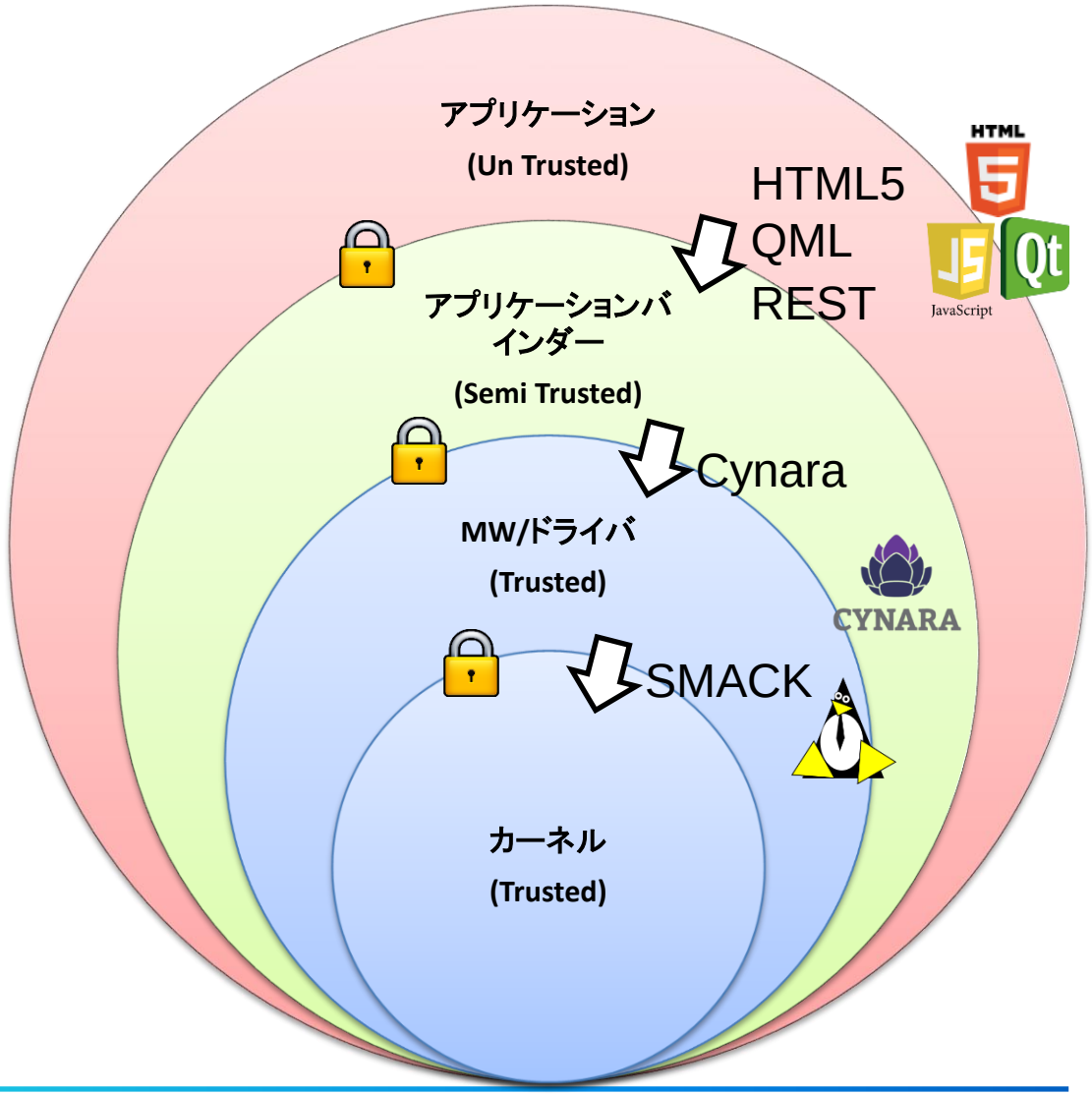
IVIの未来 - AGL Application & Security Framework

- 特徴(Application)
  - REST API による UI の分離
  - Packaged Web Appsによるアプリケーションの可搬性
  - libmicrohttpd による軽量アプリケーションコンテナ
  - プラグインによる機能拡張



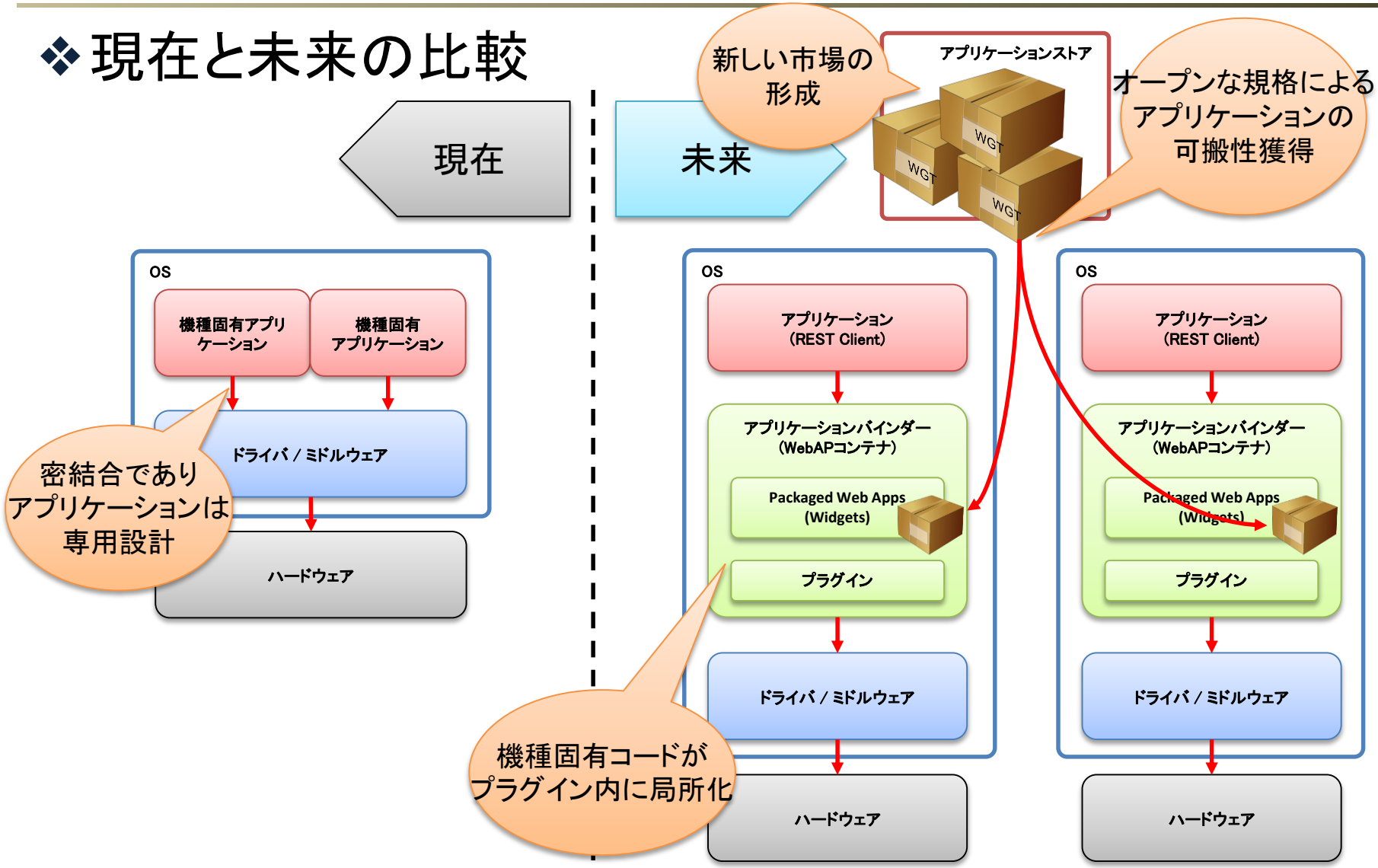
IVIの未来 - AGL Application & Security Framework

- 特徴(Security)
  - レイヤーベースのセキュリティアーキテクチャ
  - HTML5/QML+REST API によりUIレイヤーを分離
  - SMACK/Cynaraを活用したアクセス制御
  - 署名による認証と完全性の保障



IVIの未来 - AGL Application & Security Framework

❖現在と未来の比較

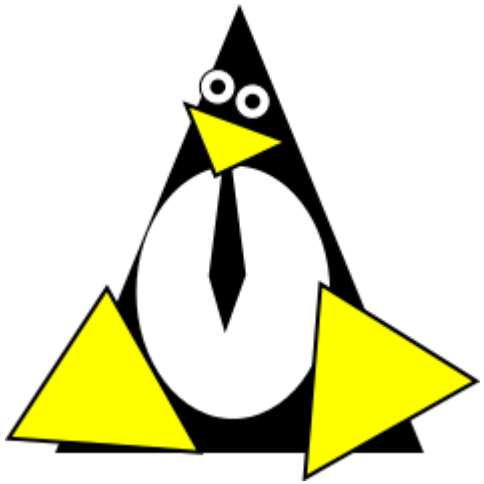


AGL App Framework - Packaged Web Apps

- W3C Packaged Web Apps に準拠。
- Webアプリを間単に導入するための仕組み。
- 導入から実行までJS多用。
- アプリケーションストアなど配布元による署名。
- セキュリティ情報(権限、ハッシュなど)を同梱。
- ZIPによるアーカイブ。

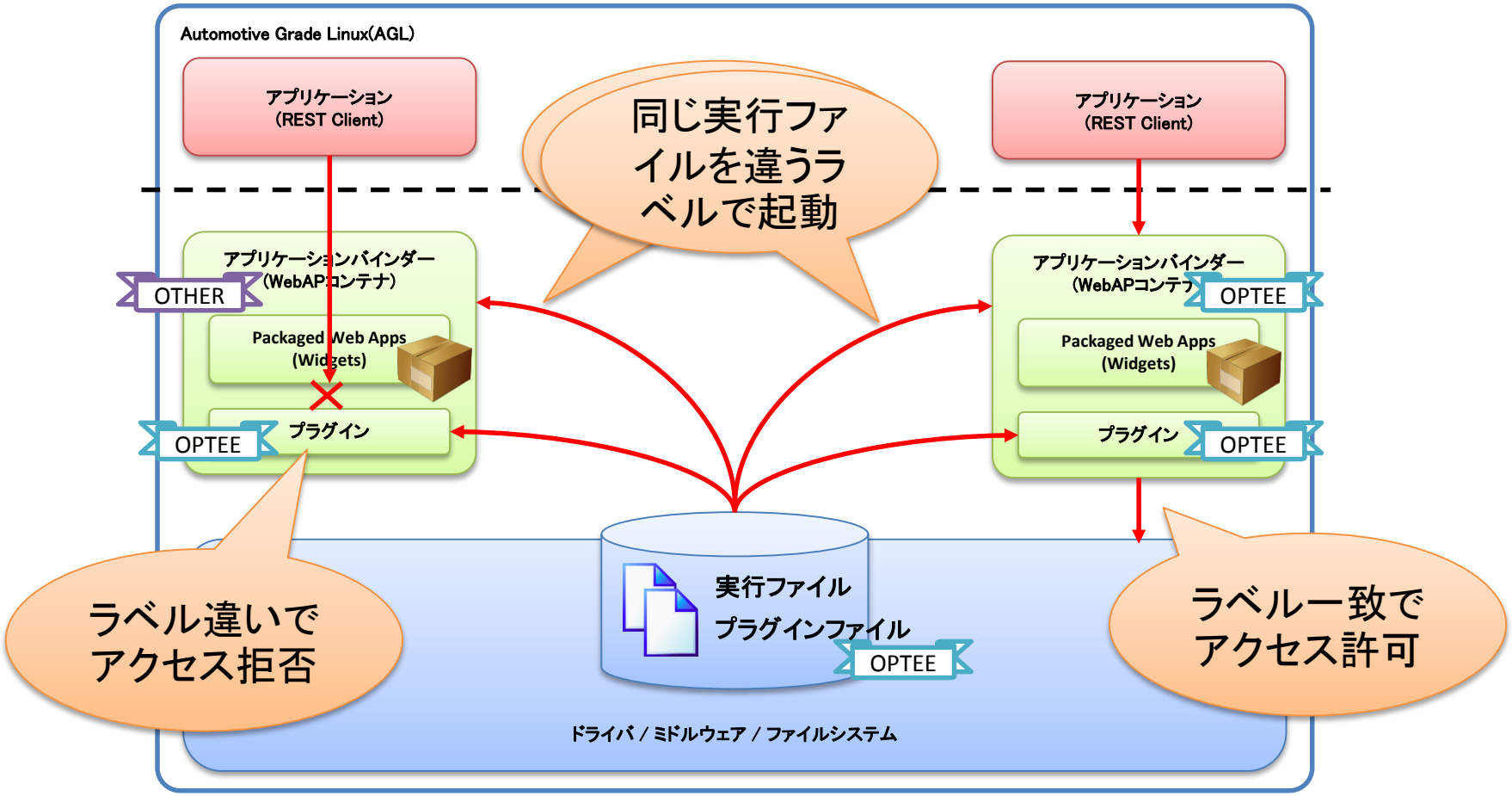
AGL Security Framework - SMACK

- LSM(Linux Security Module)によるラベルを利用したセキュリティ機能
- システムコール内にてラベルをルールに照らして評価し、許可されないアクセスは拒否(MAC(Mandatory Access Control))
- プロセス、ファイル、ネットワーク(IP Address)などにラベルを設定できる
- Linuxカーネル 2.6.25 から利用可能



AGL Security Framework - SMACK

❖ラベルによるアクセス制御の例



セキュリティ - 脅威と課題

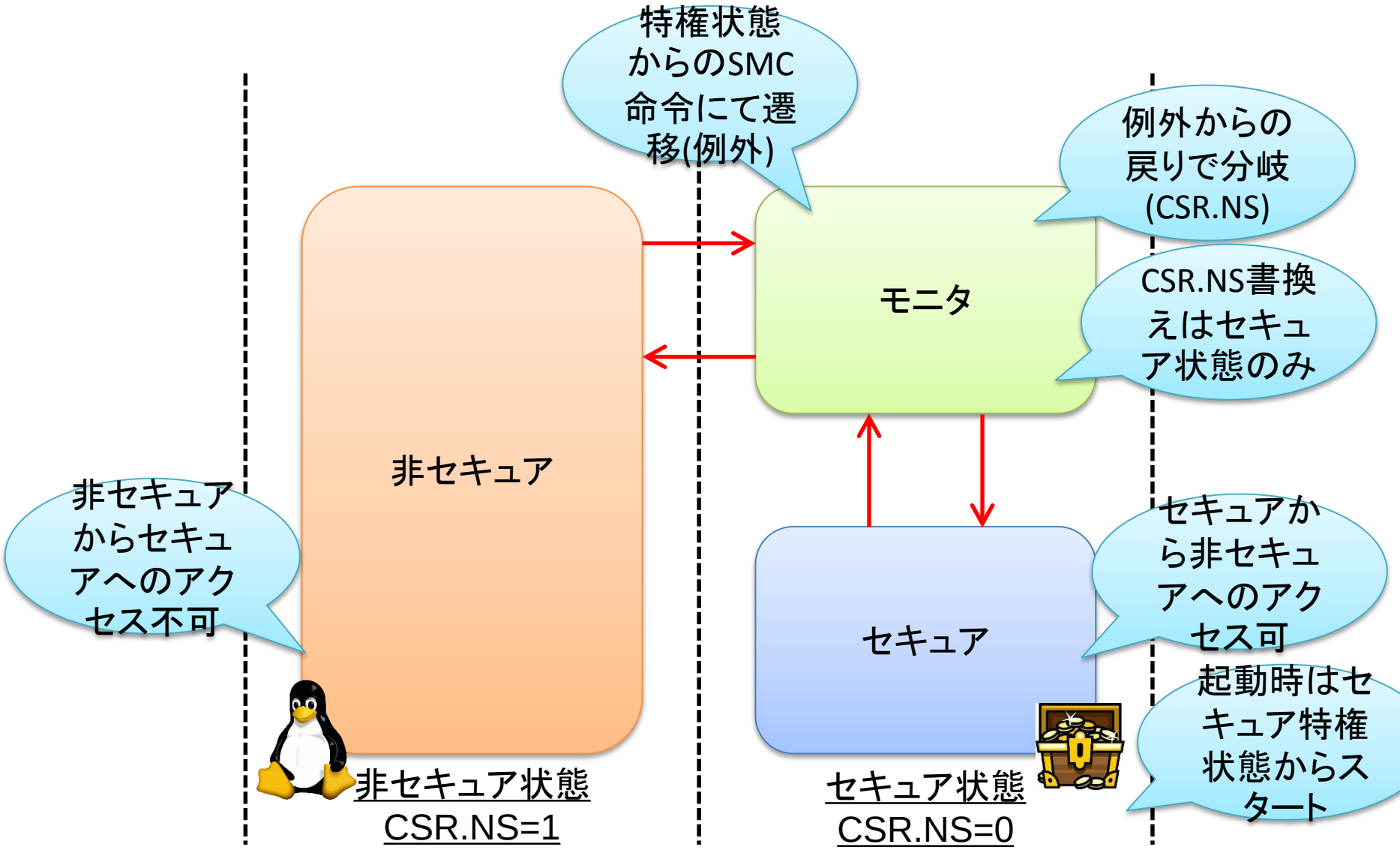
- 不正FW書込みによる脅威
  - セキュリティ機能の回避
  - 無制限・自由な不正アクセス
- 汚染されたシステムの脅威
  - 汚染されたシステムからの重要な情報の流出
- 未知の脆弱性による脅威
  - 脆弱性を介した不正アクセスや情報の流出

→Trust Zone を用いることで脅威に対抗

セキュリティ - TrustZone – 特徴

- ARMセキュリティ拡張
- CPUの動作モードのひとつ
  - プログラム実行の根幹に与えられた拡張機能
- セキュア / 非セキュア(ノーマル)のモード
  - 非セキュアモードからセキュアモード資源(メモリ等)へのアクセス禁止
- セキュアモードから起動
  - 信頼の鎖によるセキュアブート(署名確認の連鎖)を実現可能(不正FWによるセキュリティ機能回避の防止)

セキュリティ - TrustZone – 動作



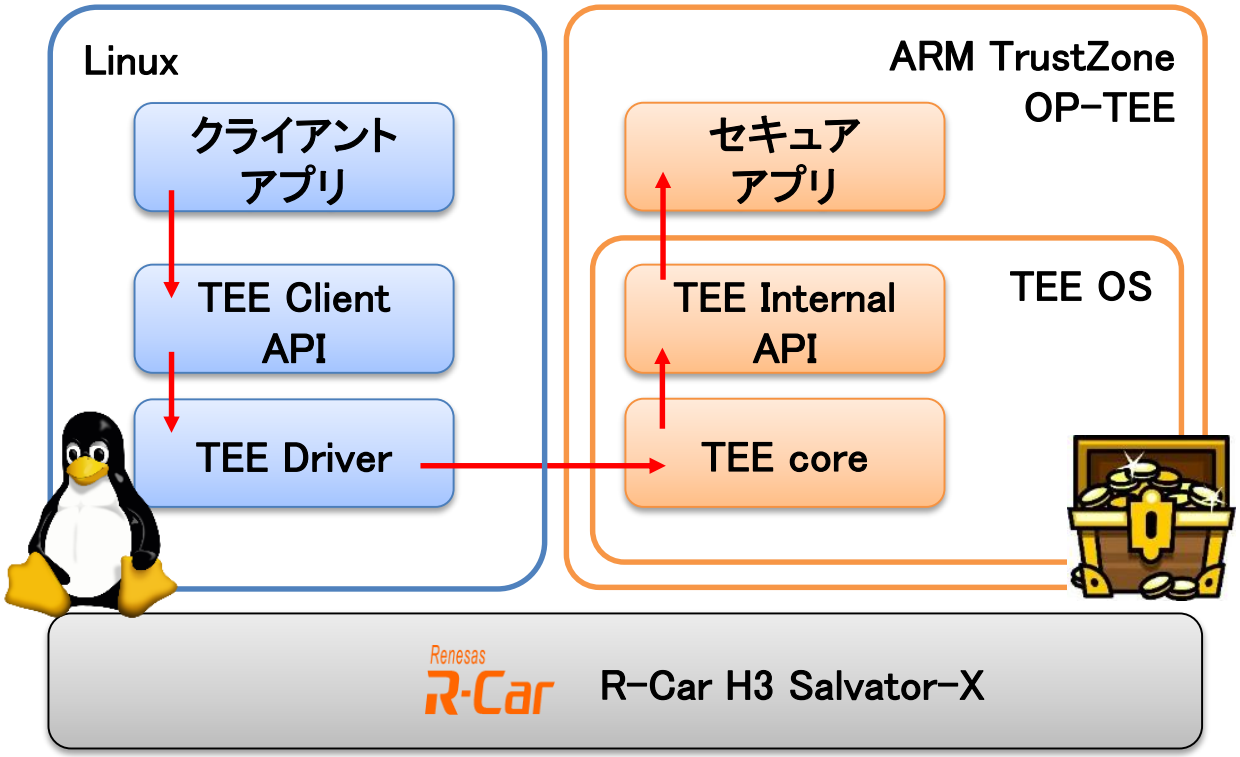
セキュリティ - OP-TEE

- GlobalPlatform
  - ICカードに関連する業界標準化団体
  - サービス（クレジット）、ハード（半導体、RW機器）、ソフトウェア（SI）、通信(〃)関連各社が参加
  - TEE(Trusted Execution Environment)を定義
    - 汎用HWでのセキュアな実行環境を定義
- OP-TEE
  - TEEの実装
  - オープンソースプロジェクト

    https://github.com/OP-TEE
  - 二条項または三条項BSDライセンス

セキュリティ - OP-TEE - セキュアアプリ - 実装

❖実際の実行経路



取り組み – デモのご紹介–デモ構成

❖デモの構成