

OTA Updateに関する研究の活動紹介

南宮イク^{1,2)}, 倉地亮²⁾, 高田光隆²⁾, 大林茂雄¹⁾, 河合聡¹⁾ 1)株式会社テクノプロ, 2)名古屋大学

これまでの研究

- Uptaneの調査（仮想環境でのテストベッド作成と評価）
- Uptaneの課題とその解決法の調査
- サプライチェーン全体への完全性を保証するシステムの検討

新たな進展の報告

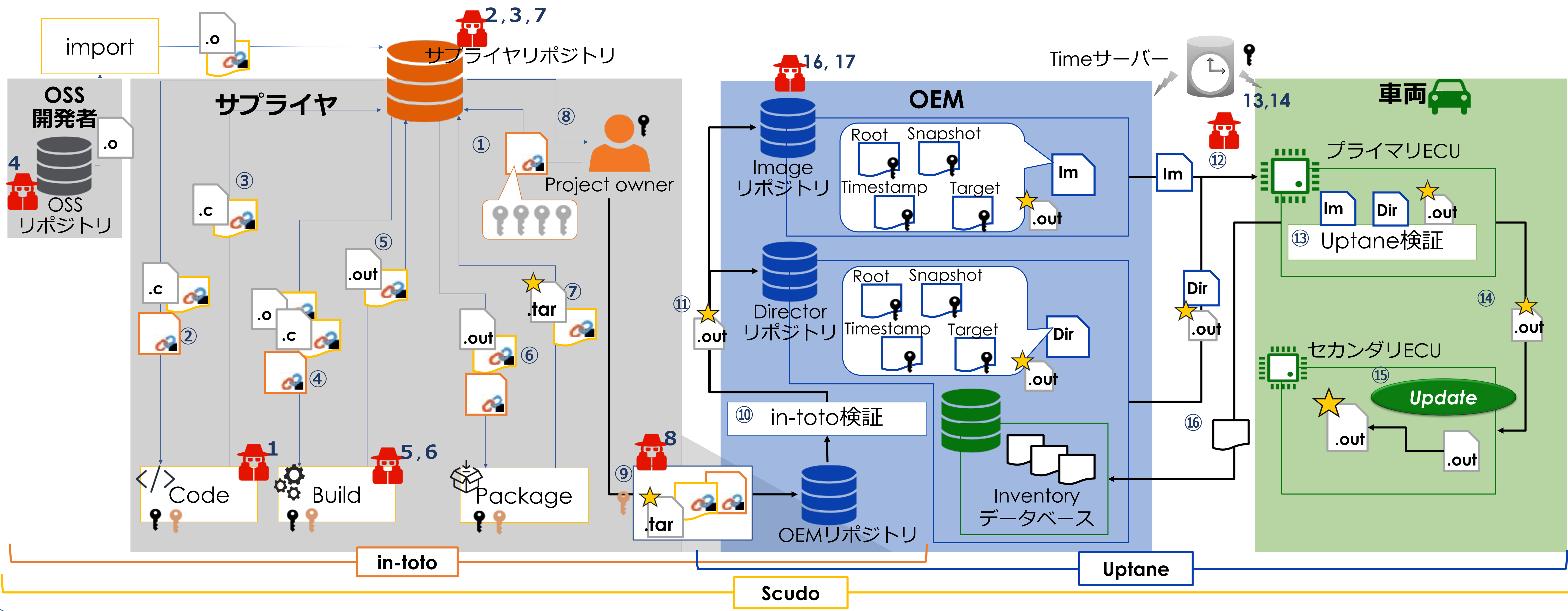
- Scudo (Uptane + in-toto) 用に仮想環境テストベッドの改良
- テストベッドを用いた検知できる脅威の明確化

テストベッドの構成

◆ 4つのコンポーネントからなる。

- サプライヤ : Code / Build / Package の工程(Step)を担当
- OEM : in-toto最終検証, Director/Imageリポジトリ
- 車両 : Primary ECU + Secondary ECU
- Attacker : 各工程への攻撃を実施

◆ 図中の丸数字順に処理が実施される。(①～⑬)



テストベッドを用いたScudoの検証結果

ソフトウェアサプライチェーンにおいて、検出可能な脅威が拡大し、防御力の向上を確認できた。
※下記表のNo.は前述図のAttacker番号に紐づく

No	想定される脅威	テスト実施結果	
		in-toto	Uptane
1	不正なコードをソースリポジトリに送信	○	-
2	ソースリポジトリの侵害	○	-
3	変更されたソースからビルド（ソースリポジトリと一致しない）	○	-
4	悪意ある依存関係の使用	△	-
5	ビルドプラットフォームの侵害	△	-
6	CI/CDでビルドされていないartifactsのアップロード	○	-
7	パッケージリポジトリの侵害	○	-
8	悪意あるパッケージの使用	○	-
9	Eavesdrop attack (盗聴攻撃)	-	×
10	Drop-request attack (ドロップリクエスト攻撃)	-	×
11	Slow retrieval attack (遅延攻撃)	-	×
12	Freeze attack (フリーズ攻撃)	-	×
13	Partial bundle installation attack (部分的バンドルインストール攻撃)	-	○
14	Rollback attack (ロールバック攻撃)	-	○
15	Endless data attack (エンドレスデータ攻撃)	-	×
16	Mix-and-match attack (ミックスアンドマッチ攻撃)	-	○
17	Arbitrary software attack (任意のソフトウェアへの攻撃)	-	○

凡例 ○ : 検出可能 △ : 条件つきで検出可能
 - : 守備範囲外 x : 検出不可

ネットワーク上のデータの監視、妨害は防げない

株式会社テクノプロと名古屋大学の共同研究

用語説明

Scudo : 自動車向けOTA Updateのオープンソースフレームワーク。

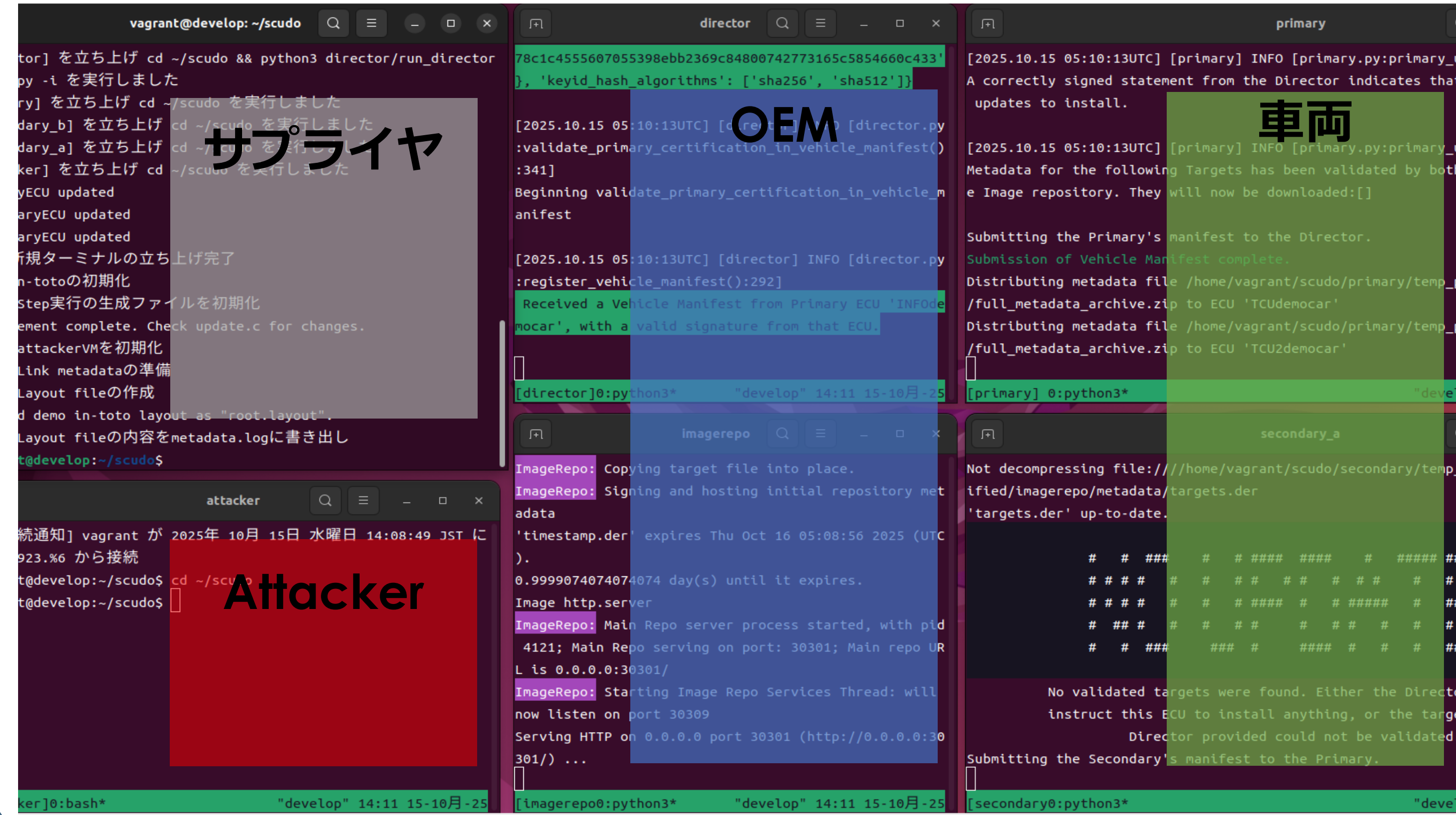
Uptaneにin-totoを組み合わせ、ソフトウェア生成から車両適用までの完全性および真正性を確保することを目的とする。

in-toto : ソフトウェア開発～Repositoryへの格納までの工程で、更新プログラムが正しい手順で作られたことを検証するフレームワーク。

Uptane : 車両への配信～車両で適用するまでの工程で、更新プログラムが正しく車両に届けられたことを検証するフレームワーク。

テストベッド画面

Virtual Box上に4つのコンポーネントを構築し評価した。
(Uptane demoコードをベースに作成し、ubuntuで動作)



今後の方針

実機ベースのテストベッドを構築し、引き続き有用性や改善案の模索を行う。