発表９

自動車OTA Updateにおけるソフトウェアサプライチェーンセキュリティシステムの研究

納庄実菜[1,2)]，倉地亮[2)]，高田光隆[2)]，富原和幸[1)]，河合聡[1)]　1)株式会社テクノプロ，2)名古屋大学

背景

2020年6月、国際基準の策定*1により、自動車開発においてOTA Update*2対応が必須となった。昨年より車両OTA Updateの標準的なフレームワークであるUptaneの仕様について研究を行った。今回はUptane範囲外*3のソフトウェアサプライチェーン*4に着目した。

株式会社テクノプロと名古屋大学の共同研究

【Uptaneの特徴】

- 2つのOTAサーバーにより更新ファイルの完全性に対する責任を分散
- メタデータへの署名により更新ファイルの真正性を証明

Uptaneの課題と本研究の目的

課題：「Uptane範囲外の脅威」である更新データの完全性が保証されていなかった

目的：OTA Updateにおけるソフトウェアサプライチェーン全体の完全性を保証するシステムの検討及び車両にとっての有効性の検討

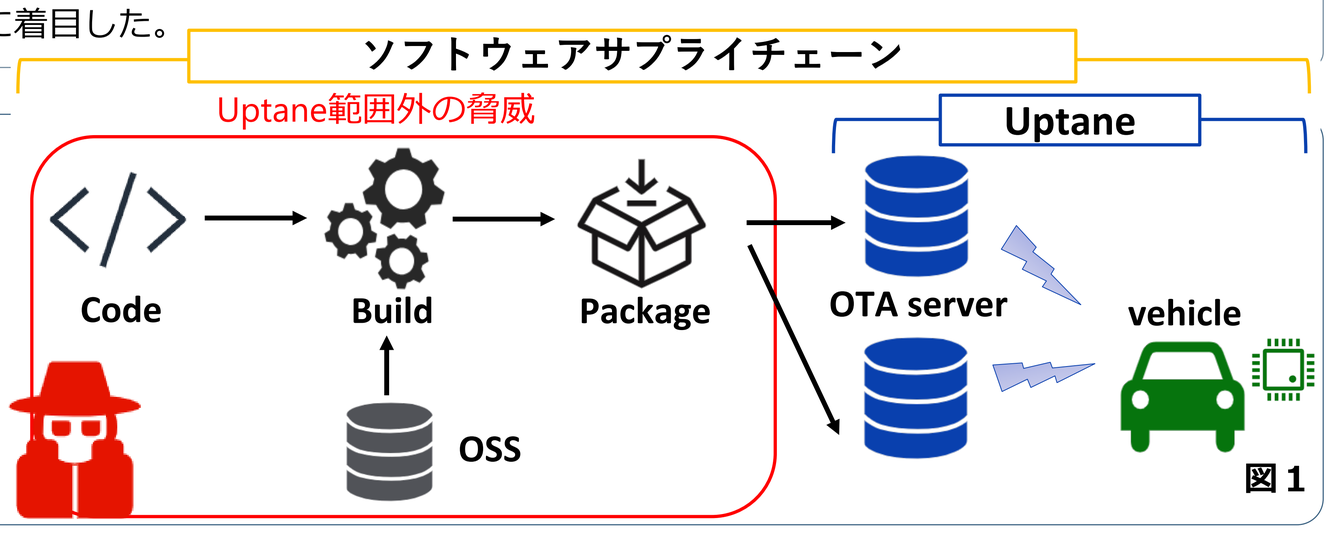

図１

調査・検討

Uptaneコミュニティ内では開発からOTAサーバーへ更新ファイルを格納するまでの工程を問題視しており、Uptaneとin-toto*5を組み合わせること（UptaneではScudoと呼ぶ）が提案されている。これを基に下記システムを設計し、想定される脅威を防ぐことができるか検討した。

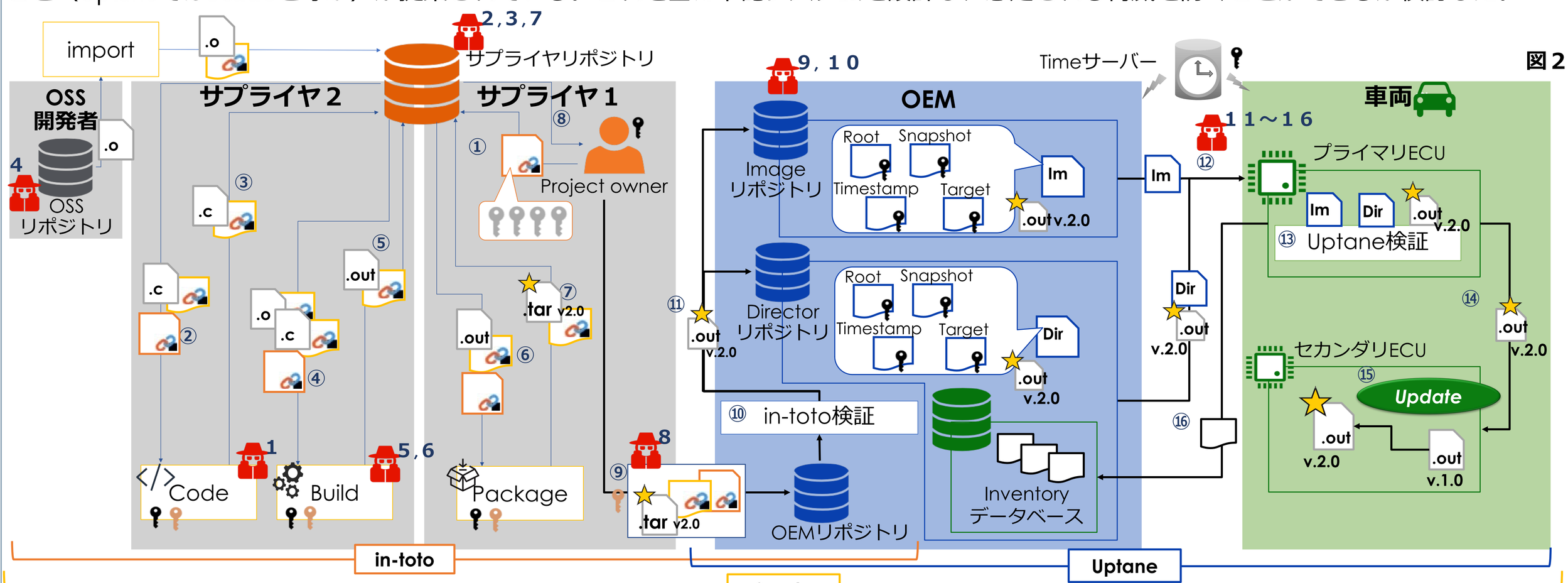

図２

Layout file	ファイル名	Im Image metadata files
Link metadata	• .c：ソースコード	Dir Director metadata files
署名生成鍵	• .o：オブジェクトファイル	metadata file
署名検証鍵（Project owner）	• .out：実行ファイル	Vehicle version manifest（更新結果情報）
署名検証鍵（Functionary）	• .tar：アーカイブ	攻撃
新規作成するファイル	更新ファイル	

ソフトウェアサプライチェーンにおいて想定される脅威を挙げ、それぞれの機能で想定した脅威を防ぐことが可能かの検討を行った。

検討結果として表1の通り、想定される脅威に対し全てに対応することが可能と考える。

No	想定される脅威	検出の可否 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	任意のソフトウェア攻撃	-	○**
10	ミックスアンドマッチ攻撃	-	○**
11	中間者攻撃	-	○**
12	リプレイ攻撃	-	○**
13	ロールバック攻撃	-	○**
14	部分的なバンドルインストール攻撃	-	○**
15	フリーズ攻撃	-	○**
16	ファストフォワード攻撃	-	○**

内部犯（インサイダー）：鍵を持っている／利用できる
外部犯：鍵を持っていない／利用できない
*： 内部犯（インサイダー）の場合、鍵を持っているため防ぐことはできない
**：内部犯（インサイダー）の場合でも、両方のリポジトリの鍵が漏洩しない限り防げる

表１

*1) UN-R155（サイバーセキュリティ）, UN-R156（ソフトウェアアップデート）, *2) Over The Air Update , *3) 図1参照, *4) 今回のOTA Updateにおいて更新ファイルの開発から車両側ソフトウェア更新までの工程と定義, *5) 開発からインストールまでの開発手順の完全性/真正性を保証するオープンソースフレームワーク。

結論

- **今回検討したシステム構成により、OTA Updateにおけるソフトウェアサプライチェーン全体に渡り、想定される脅威に対して完全性を保証するシステム設計ができた。**
- **将来的に都度機能拡張を想定された自動車が流通することを考えた場合、有用なシステムであると考える。**

今後の方針

Scudo （in-toto＋Uptane）のテストベッドを作成し、実際に脅威に対して有効かを検証し、新たな問題があれば改良案や対策を提案する。

NCESシンポジウム2024　@名古屋大学　2024年10月22日