資料28-1-2-3

情報セキュリティ
平成28年度成果と今後の課題

平成29年3月28日

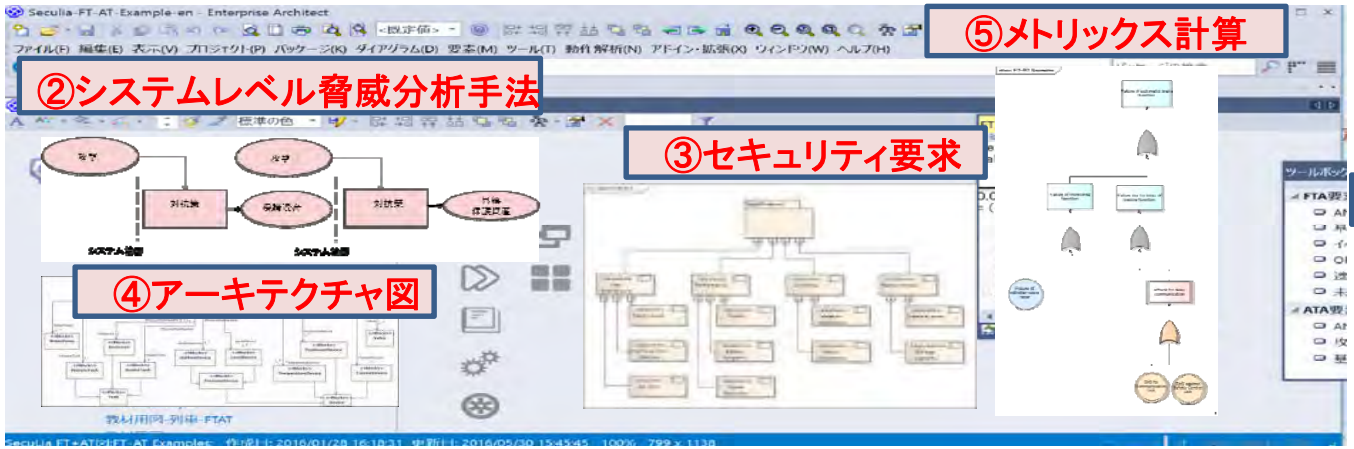
第28回 SIP自動走行システム推進委員会

情報セキュリティに係る成果報告

H28年度までの成果

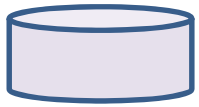
- 脅威分析：JasParと連携し脅威解析手法を開発。ツール仕様を決定
- 評価手法：車両ブラックボックス評価、車内LAN/部品評価手法を開発
- V2X署名検証：優先度付き検証方式を開発し、1,000/s目途付け完了

【脅威分析ツール全体の概要（完成予想図）】

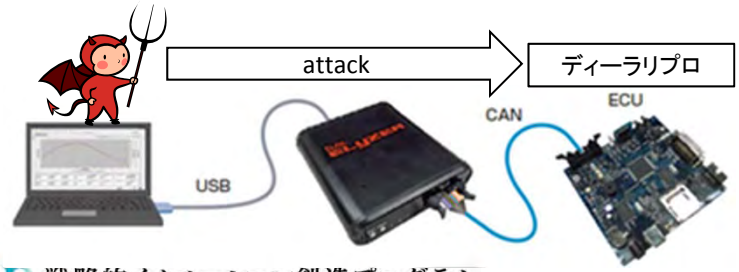


【脅威分析】
JasPar仕様に対し
多重防御戦略追加

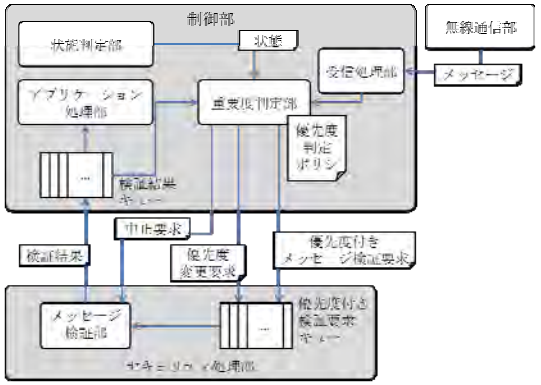
①ユースケース DB



【評価手法】
車内LAN評価シミュレータ開発完了
リプログラミング時脅威の評価手法を開発
CAN侵入時のふるまい検知評価を開発



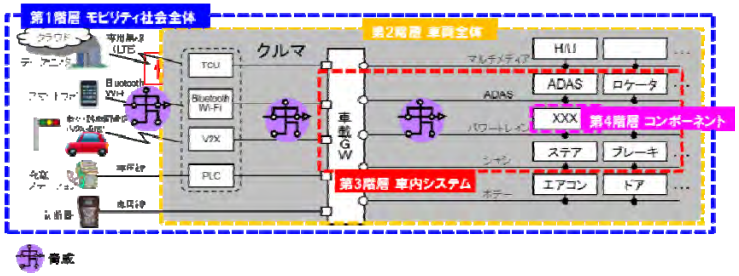
【V2X署名検証】
優先度付きメッセージ検証プロトコル開発完了



情報セキュリティに係る成果報告（評価手法）

第2階層　車両全体

(1)車両ブラックボックス評価手法開発
WiFi、テレマティクスを攻撃口として
耐性及び、機能安全を確認



a) 通信盗聴
b) ポートスキャン
c) ファジング
d) ペネトレーション
e) ジャミング

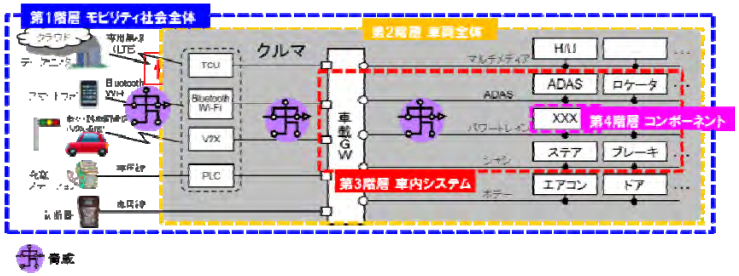
H29以降の大規模実証実験
業界の標準的評価法への反映
Auto-ISAC連携

情報セキュリティに係る成果報告（評価手法）

第3階層　車内システム

(2)車内通信（CAN bus)に対する評価手法開発

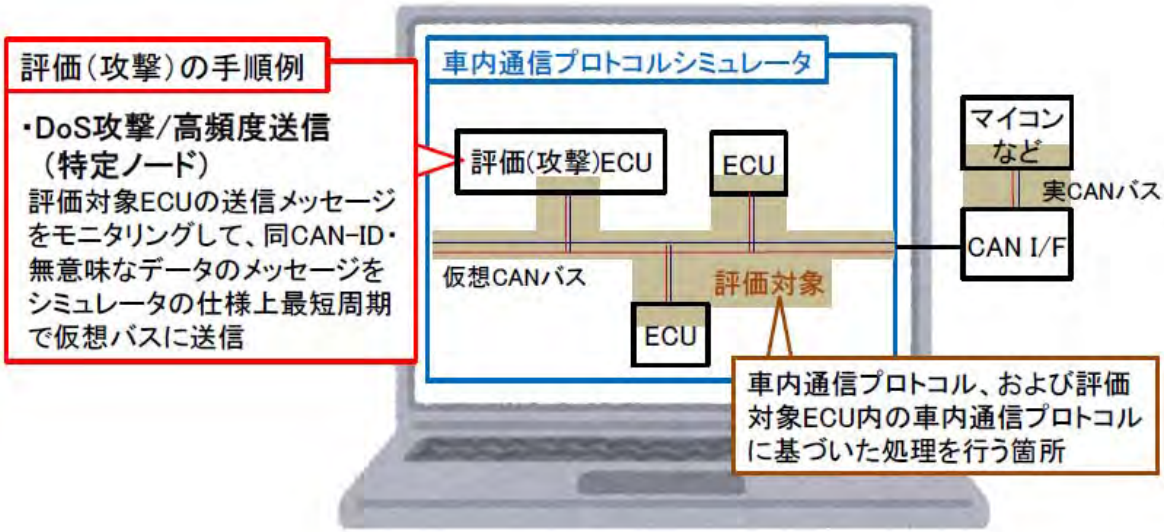
①車内通信シミュレータを用いて、
- 想定される攻撃手法
- その場合の通信挙動を確認



《評価データベースとして活用予定》

a) DoS攻撃
- 1)高頻度送信
- 2)メッセージ衝突
- 3)異常メッセージ送信

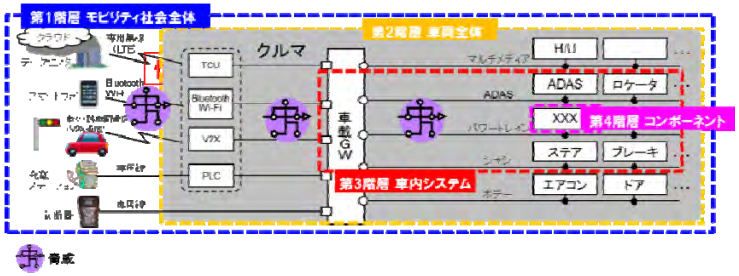
b) なりすまし攻撃
- 1)メッセージリプレイ
- 2)メッセージ改竄
- 3)送信頻度改竄



情報セキュリティに係る成果報告（評価手法）

第3階層　車内システム

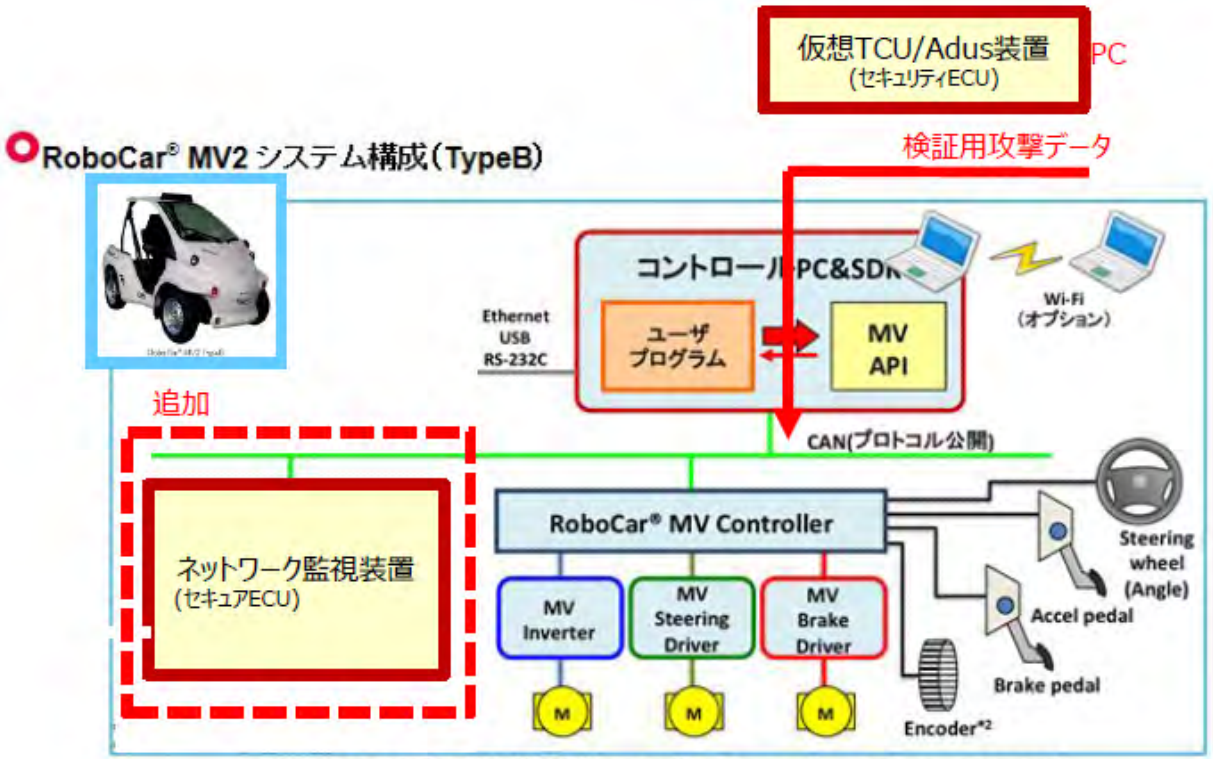
(2)車内通信（CAN bus)に対する評価手法開発



②侵入検知ガイドライン

・CANメッセージの周期乱れ

・CANメッセージの抜け　　etc.



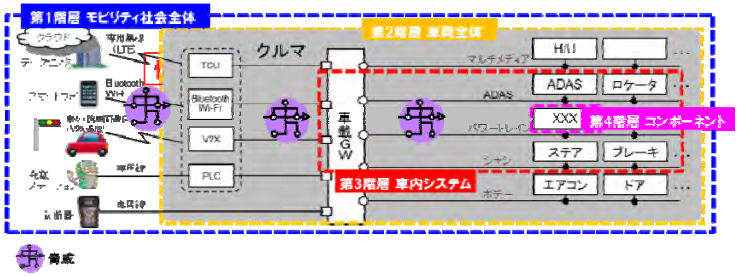
RoboCar® MV2システム構成例（TypeBプラットフォーム＋コントロールPC&SDK）

情報セキュリティに係る成果報告（評価手法）

第４階層　コンポーネント

(3)鍵配布、リプログラム認証評価手法開発

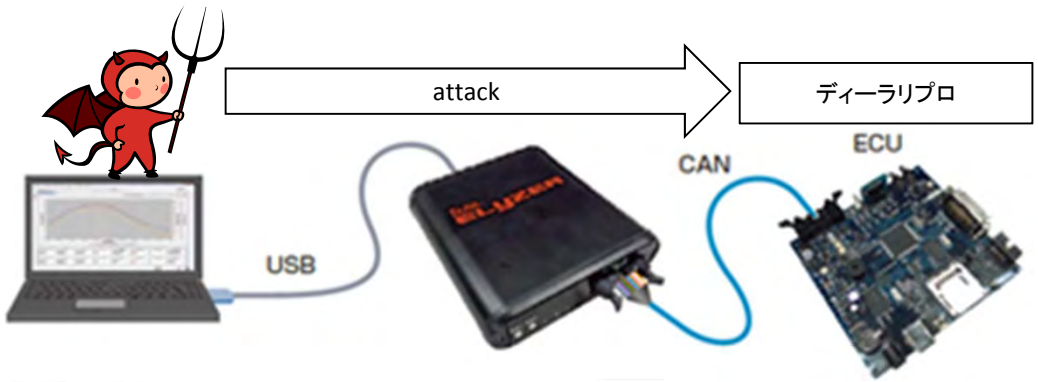
車載コンピュータ（ECU）のセキュリティリスクレベルに応じて、リプログラム時に必要な標準的目標レベルを検討



・暗号アルゴリズム
・乱数Bit数、エントロピー

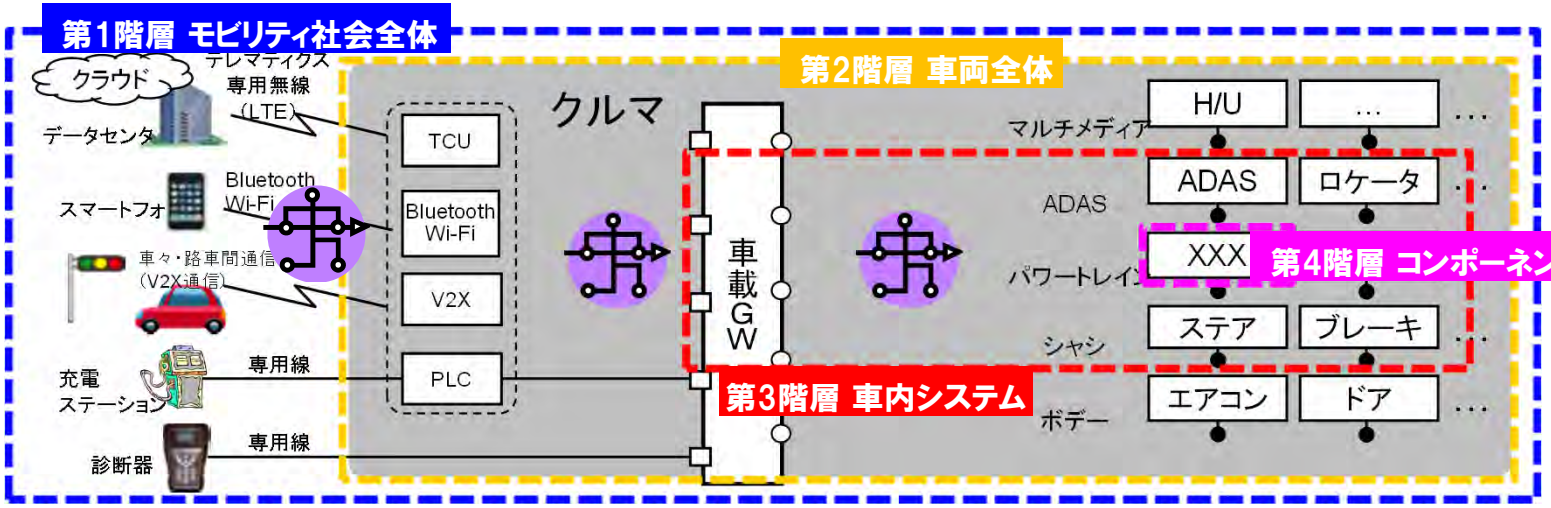
《評価方法》

①評価ボードによる実機攻撃評価
②他業界(※)の鍵管理調査　(※)銀行ATM、カード決済端末、スマートメータ



情報セキュリティに係る今後の課題

最終目標	**車両評価手法の確立**
今後の課題	■ FOT車両のブラックボックス評価 ■ 車両ブラックボックス評価手法の進化と、SIP後の体制構築 ■ 車両外部（通信、サーバ）も含めた統合的脅威分析



・第１階層を含む統合的脅威分析の検討及び、評価環境の構築
・車両ブラックボックス評価の進化