車載制御ネットワークに対する集中型セキュリティ監視システム（15654360）

研究代表者

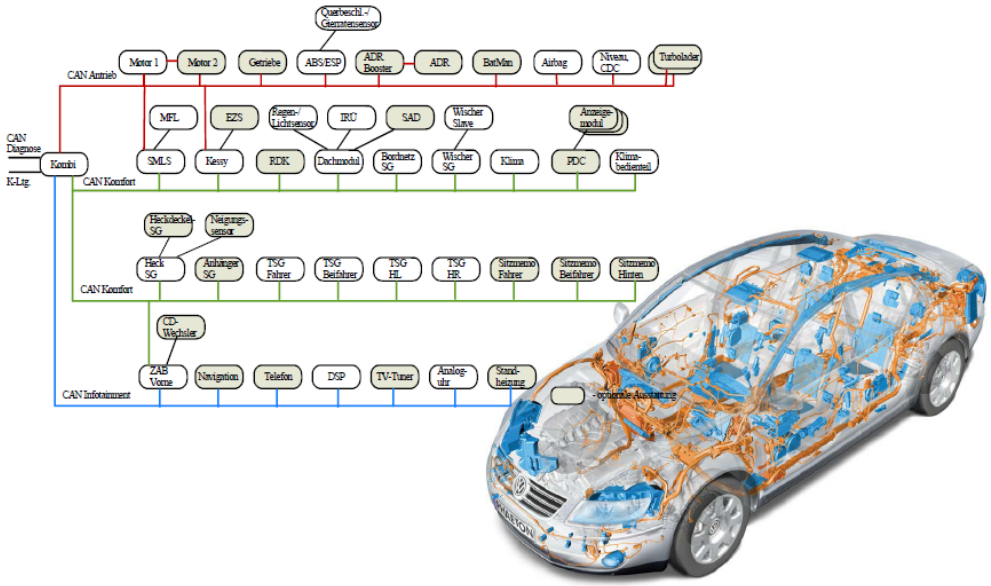
倉地　亮

名古屋大学大学院情報学研究科
附属組込みシステム研究センター

最終更新日: 2018年9月5日

車載電子制御システム

- 多くの機器（センサやアクチュエータ）を制御することで走行機能を実現
- 機器によって定まる時間制約をもつリアルタイムシステム
- 時間制約を満たせない場合には重大な事態となりうる
  - 例えばブレーキを踏んでも作動しない/遅延する場合重大な過失となる



（例）VW Phaeton(2004):

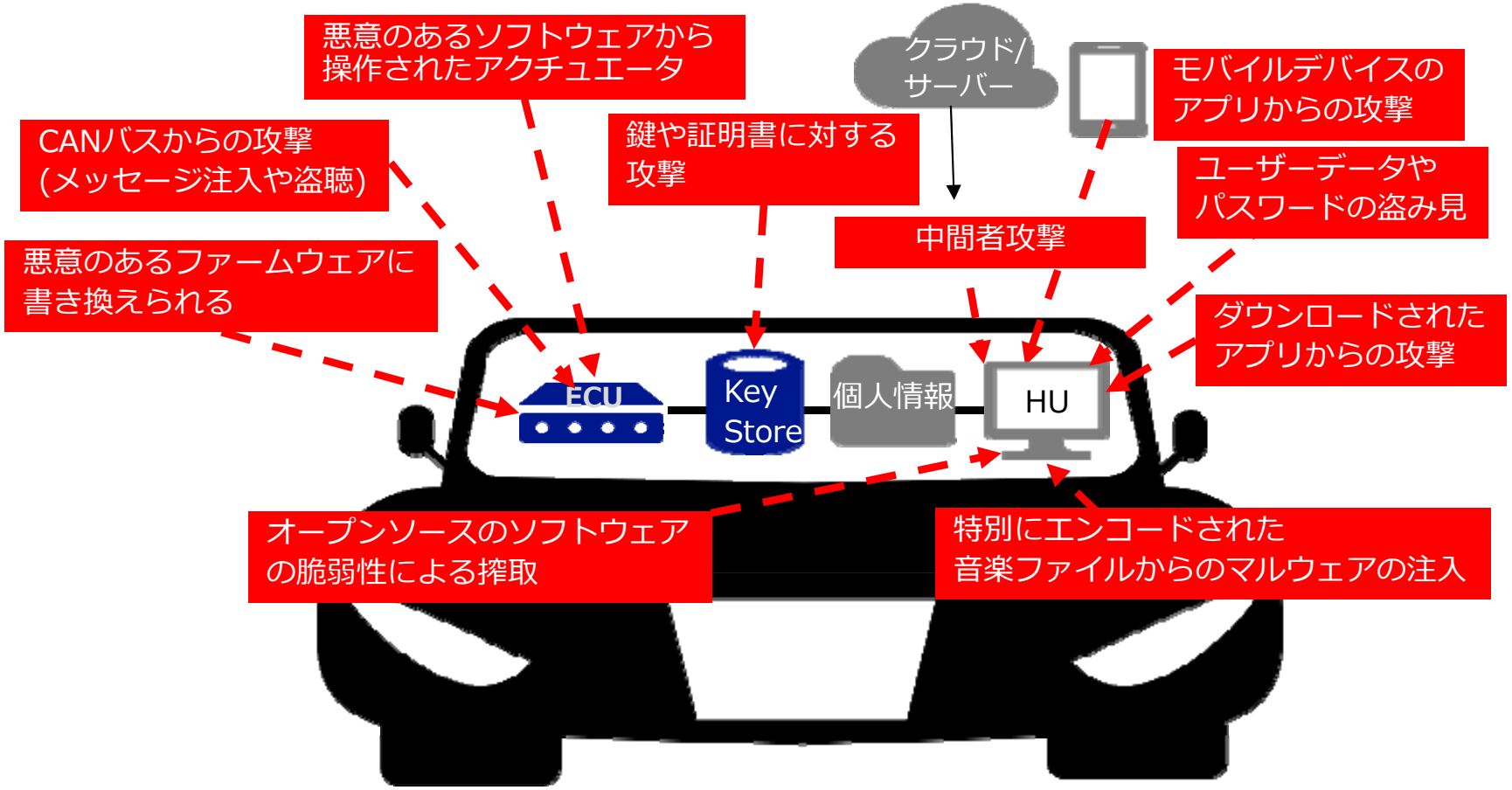
- 11,136個の電子部品が搭載
- 通信
  - 61個のECUが搭載
  - 外部からの診断のために31個のECUがシリアル通信
  - 35個のECUが4つのCANバスに接続
- 通信データ
  - 2500個のシグナル
  - 250個のCANメッセージを使用

http://www.iestcfa.org/presentations/wfcs04/keynote_leohold.pdf

大規模な分散制御システムとして構成される

自動車のセキュリティ脅威

- 自動車の制御システムを乗っ取る脅威事例が増加しており，今後も増加が予想されている．セキュリティ機能の追加はコストに直結するため，コスト効率の高い手法が望まれている



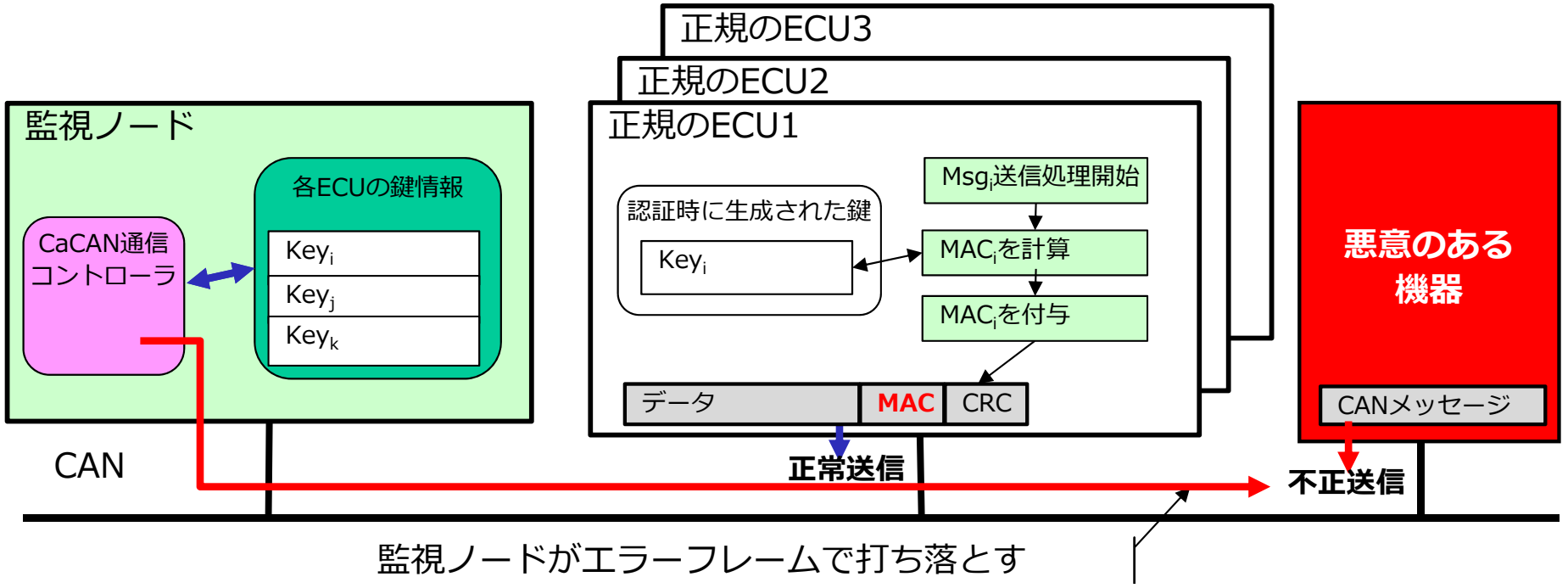
http://qz.com/461576/here-are-all-the-ways-a-hacker-can-take-control-of-your-car/ より一部改変し出典

図. 自動車におけるPotential threat vectors

提案手法: 集中型セキュリティ監視(CaCAN*)

*Centralized Authentication system in CANの略

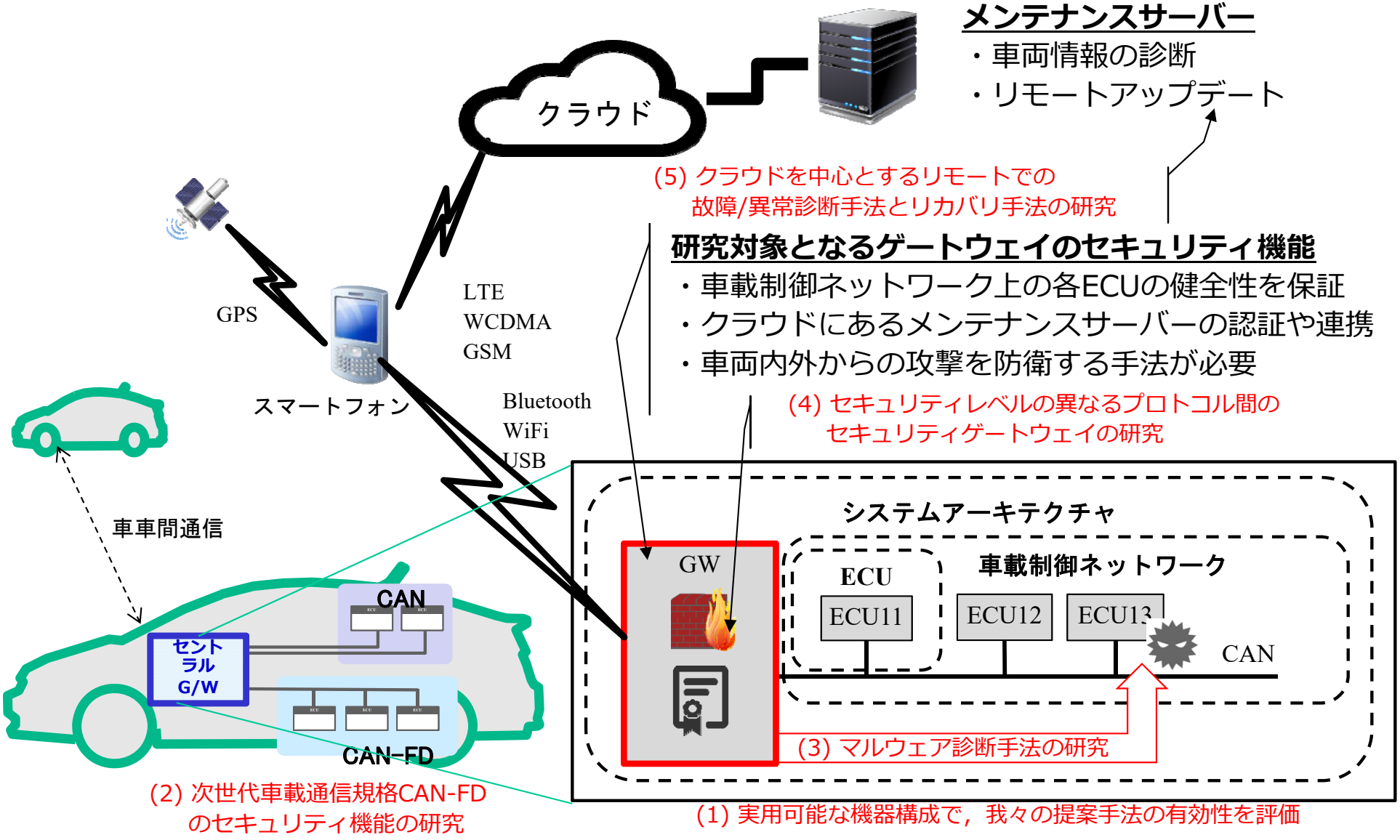
- アイデア
  - 監視ノードがなりすましメッセージをエラーフレームで打ち落とす
- 良い点
  - すべてのノードにセキュリティ機能を導入する必要がないため，セキュリティ導入時の変更規模が小さい



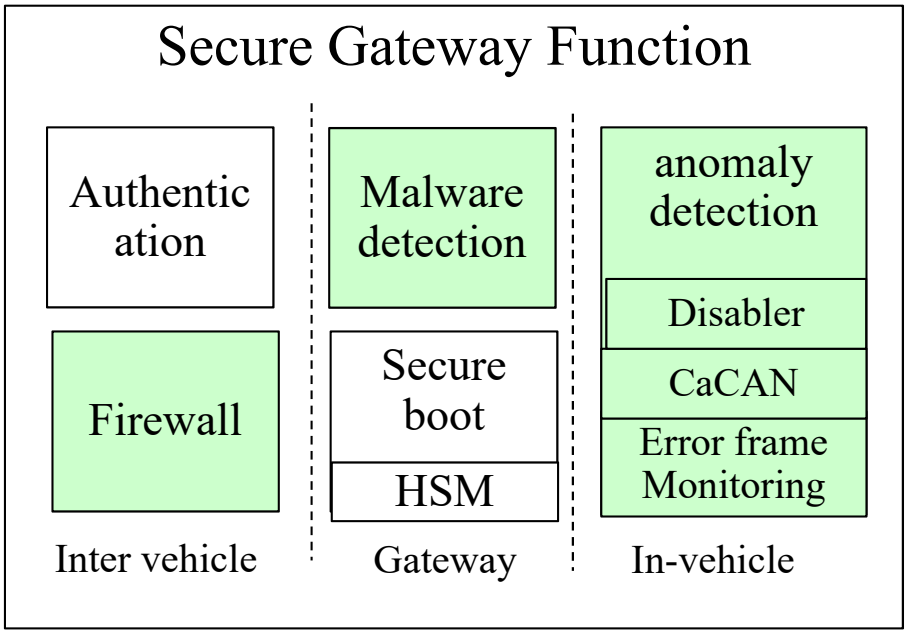
Kurachi, R., Matsubara, Y., Takada, H., Adachi, N., Miyashita, Y., and Horihata, S., ”CaCAN - Centralized Authentication System in CAN”, Proceedings of the escar 2014 Europe Conference, Hamburg, Germany, Nov 2014

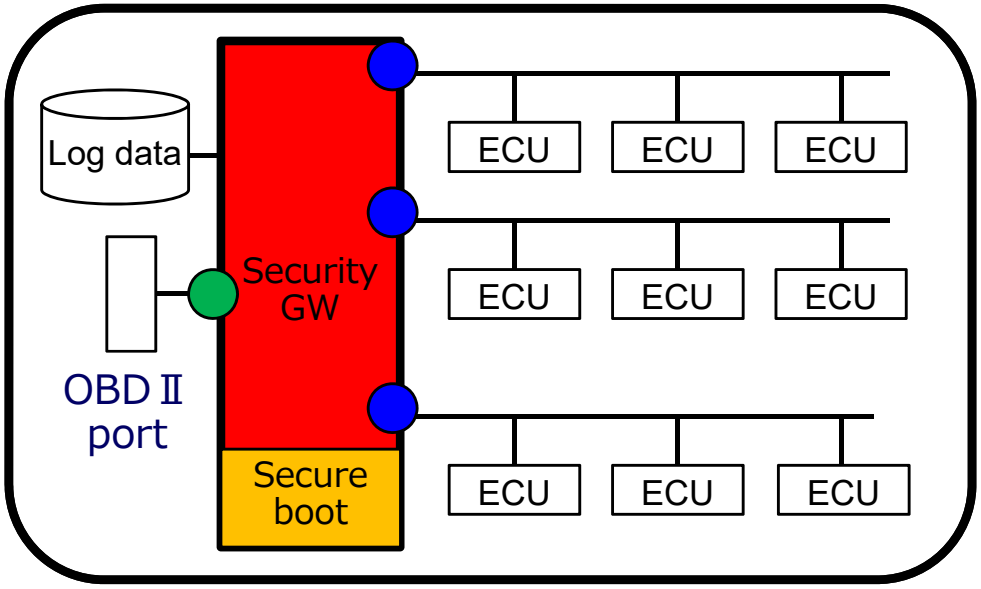
研究開発概要

- 5つの研究課題に分類し，各**セキュリティ強化手法**と**評価手法**を開発



成果物の導入シナリオ1: セキュリティゲートウェイ



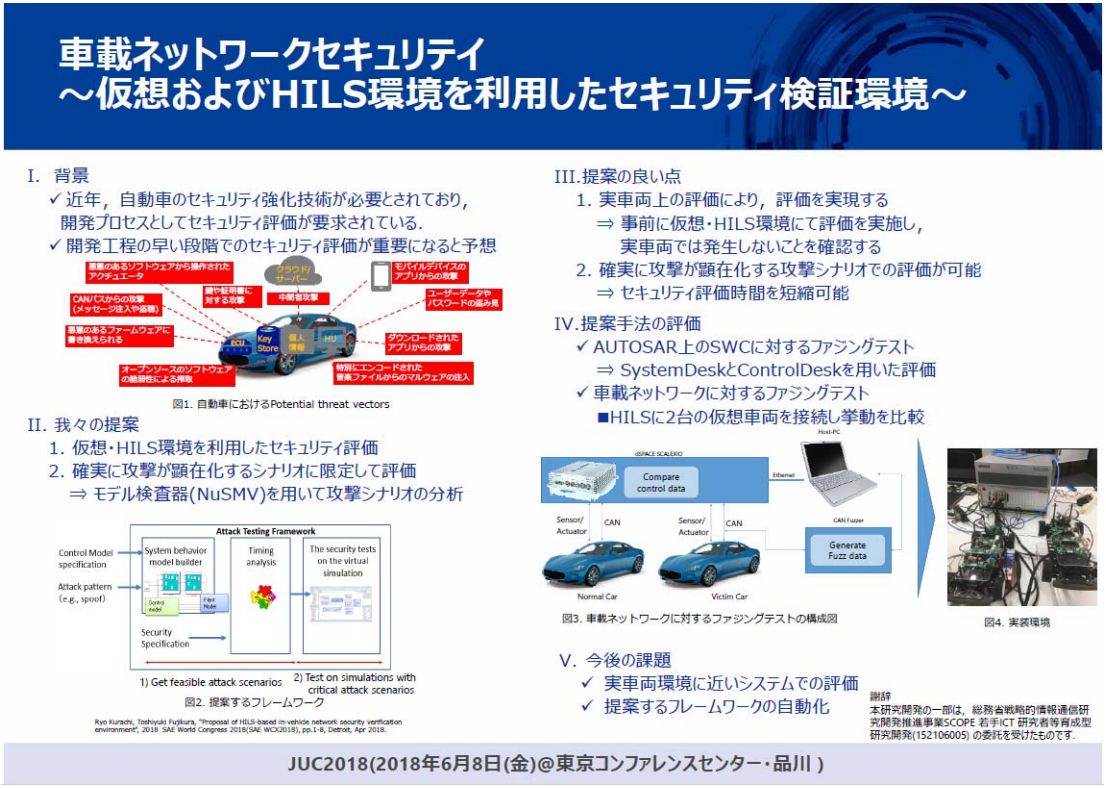


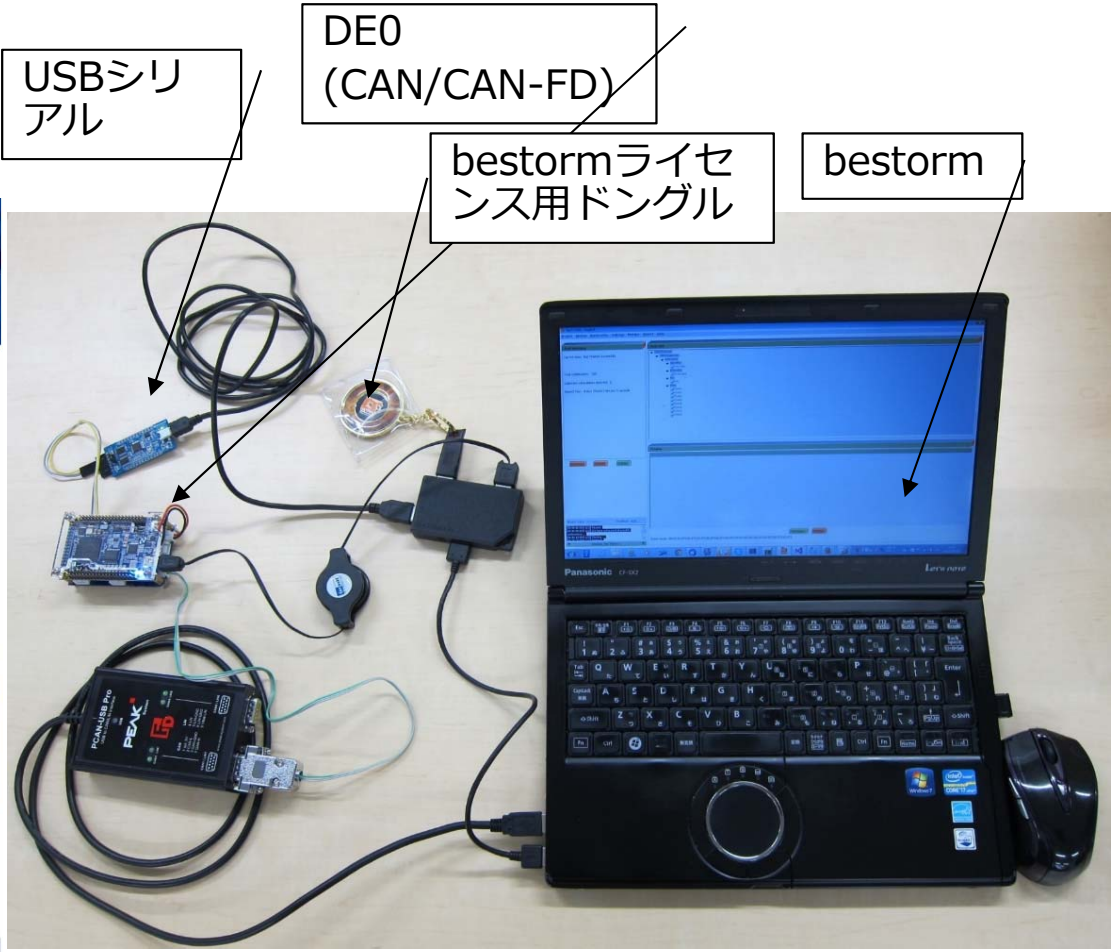
	Features	Add HW	Add SW
Firewall	中継フレーム監視機構	Yes	No
Malware detection	ハードウェアによる中継監視	Yes	No
Anomaly detection	**CaCAN**	Yes	No
〃	**エラーフレーム監視機構**	Yes	No
〃	**CAN Disabler(不正送信防止機構)**	Yes	No

Kurachi, R., Takada, H., Mizutani, T., Ueda, H., and Horihata, S.,” SecGW – Secure In-vehicle Gateway”, Proceedings of the escar 2015 Europe Conference, Cologne, Germany, Nov 2015

成果物の導入シナリオ2: 提案する評価手法

- 研究開発した評価手法は，現在市販される自動車のセキュリティ評価にも容易に導入可能である





提案1) HILSを用いた評価手法

提案2) IT系ツールを用いた評価手法

まとめと今後の予定

- まとめ
  - SCOPEの研究課題では，自動車のセキュリティを強化するためのセキュリティ強化技術やセキュリティ評価手法に関する研究開発を行った
  - この結果，様々な有益な技術開発を行うことができた

- 今後の予定
  - 実用化に向け，GWサプライヤ，ツールベンダーなどと連携を進める
  - 本研究で開発された技術をベースに，自動運転技術に関するセキュリティ強化技術や評価技術に注力していく