自動車のサイバーセキュリティ強化技術

2022年10月31日（月）

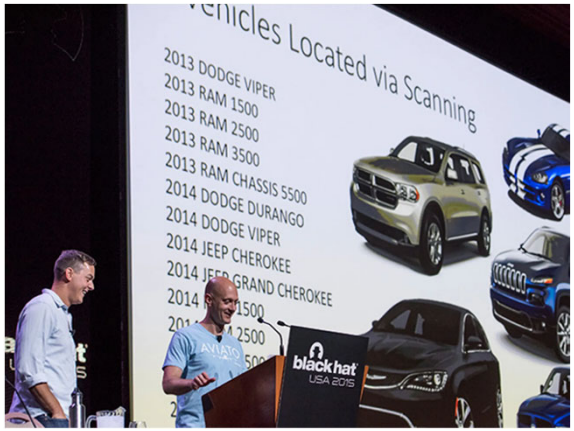
名古屋大学大学院情報学研究科
附属組込みシステム研究センター
倉地　亮
kurachi@nces.i.nagoya-u.ac.jp

アジェンダ

- 1. 背景
  - 動向，位置付け
- 2. NCESでの取り組み
  - これまでの成果
  - 現在の研究と今後の取り組み
- 3. まとめ

背景: 自動車のサイバーセキュリティ強化が要求

- 研究者らにより自動車のセキュリティ上の脅威が指摘
- 実際に販売される車両にもセキュリティ強化技術が適用されつつある
- 現在では一部車両の型式認証にサイバーセキュリティ強化が必須



https://spectrum.ieee.org/jeep-hacking-101

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

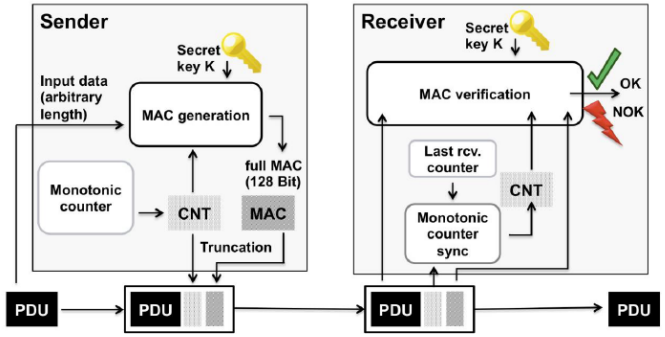
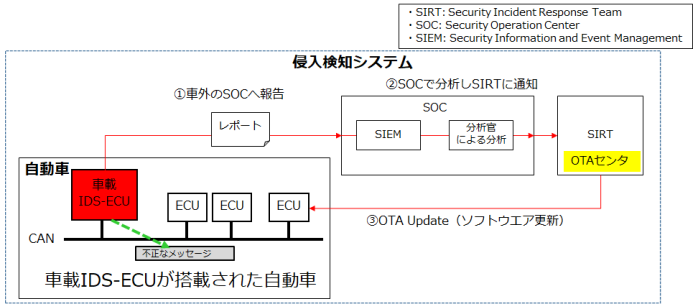


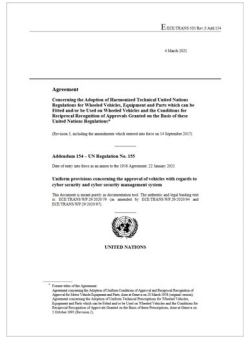
Figure 1: Message Authentication and Freshness Verification

適用されつつある技術の例1. メッセージ認証

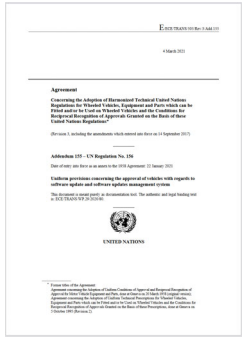
AUTOSAR version R21-11 Requirements on Module Secure Onboard Communication



適用されつつある技術の例2. 侵入検知システム



国際基準　UN-R155
（サイバーセキュリティ）



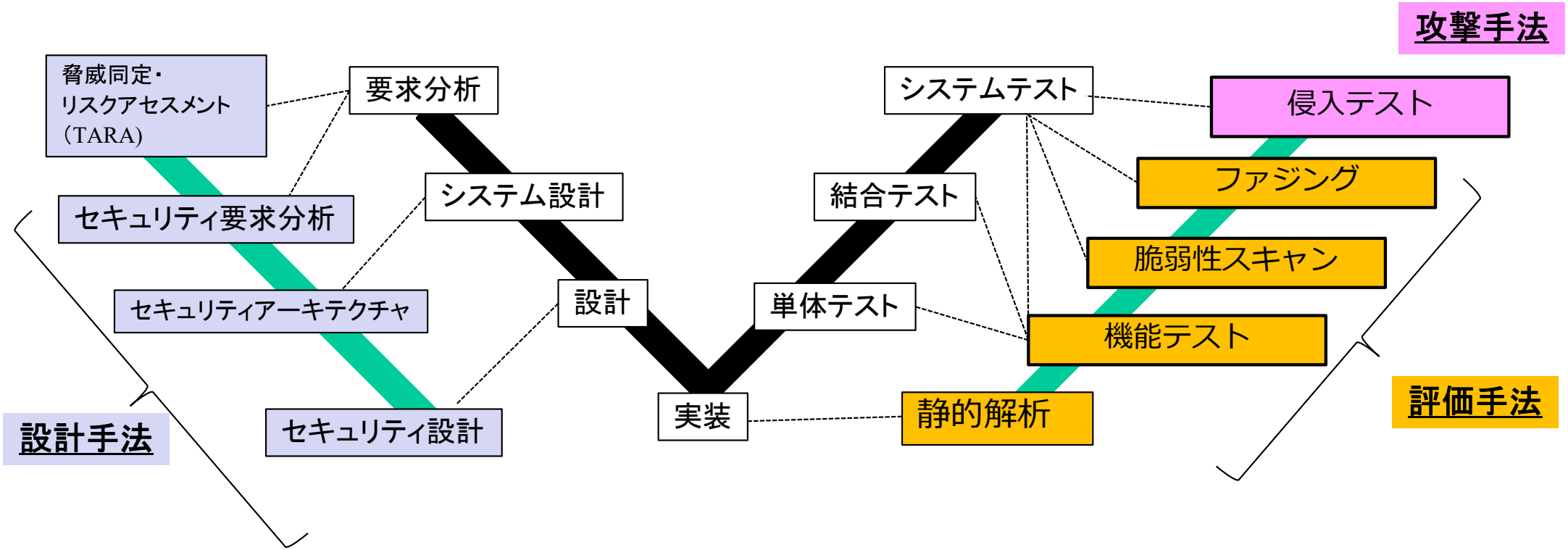
国際基準　UN-R156
（ソフトウェアップデート）

脅威事例（2010～） → **セキュリティ強化 (2019～)** → **国際基準と法制度化（2022～）**

セキュリティ強化技術の位置付け

- 国際基準では，自動車のライフサイクルに合わせたプロセス全体のサイバーセキュリティ活動が要求
- 開発の上流工程では，導出されたリスクが十分に低減できていることの論証が必要
- テスト工程では，要求が確かに実装され，論証が不十分な点が検証されていること

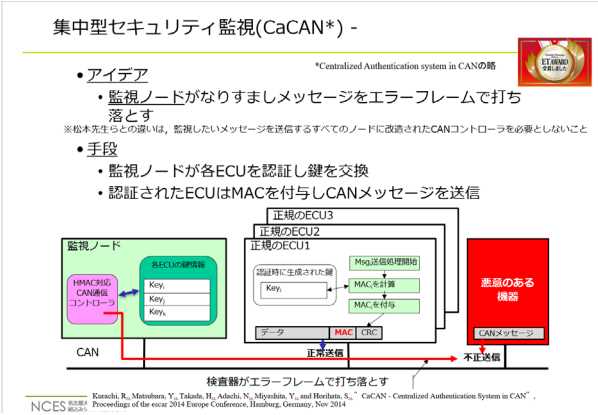
➡ セキュリティ強化技術として，攻撃手法，設計手法，評価手法等が要求



NCESでは，攻撃手法，設計手法，評価手法等に関する研究を実施

自動車のセキュリティ強化技術に関する実績

強化手法の実績 (1) ET Award (2014年)
(2) SIP自動走行システム事業の大規模実証実験(2017年度)

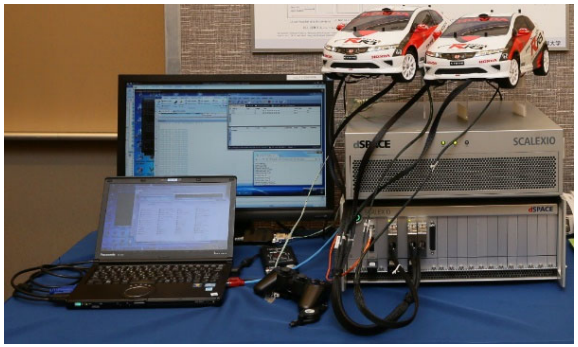


ET Award 2014
(オートネットワーク技術研究所)

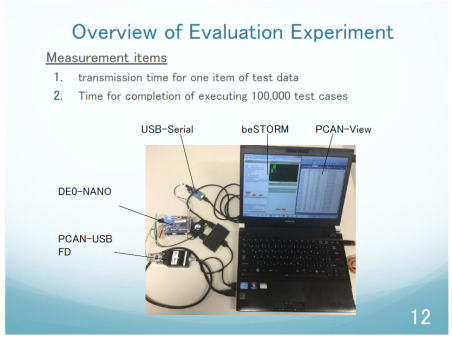
escar でのデモンストレーション
(オートネットワーク技術研究所)

SIP自動走行システム事業のうち大規模実証実験
https://www.synopsys.com/ja-jp/japan/press-releases/2017-11-27.html

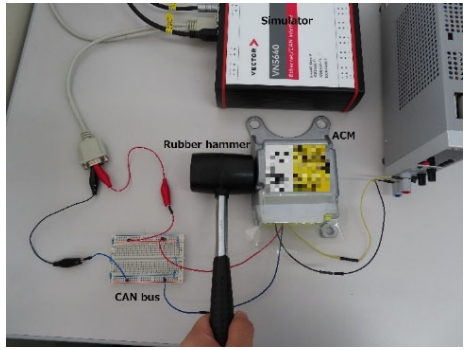
評価手法の実績 (1) 仮想環境上の評価 (2) ECUの評価 (3) 実車両の評価



仮想環境(HILS)上の評価
(dSPACE社とシノプシス)



実ECUの評価
(beyond Security社)



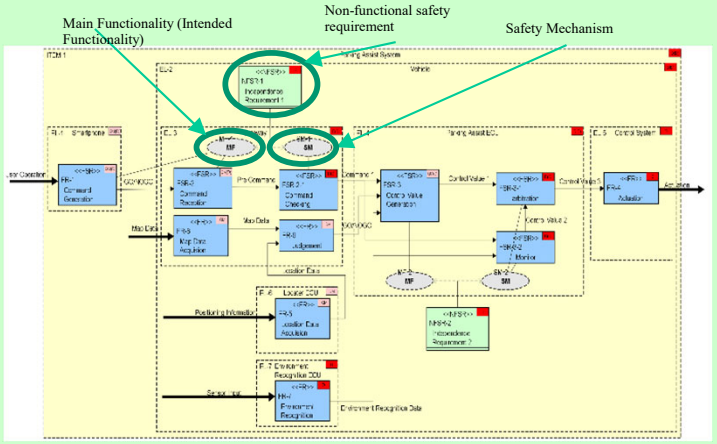
実ECUの評価
(警察大学校とパナソニック)

実車両を評価
(パナソニック)

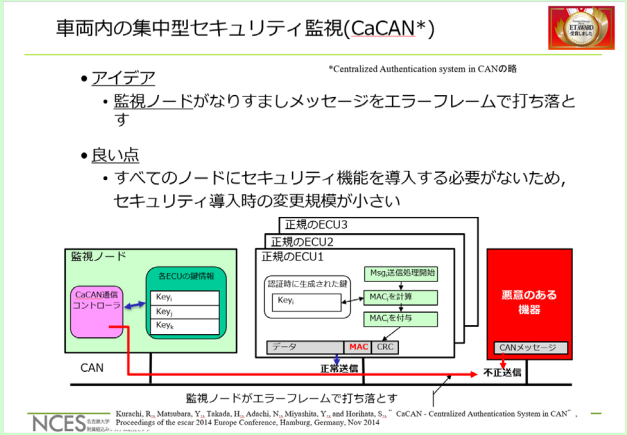
NCESでの取り組み

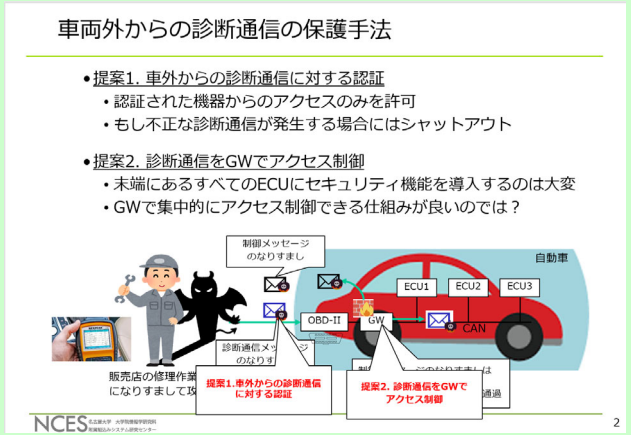
- 複数の自動車のサイバーセキュリティ強化に関する研究プロジェクトを実施
  - 設計手法(aとb)，評価手法(c)と デジタルフォレンジック(d)など
- 将来の車載電子制御システムに関する強化手法なども実施

a.セキュリティ要求分析

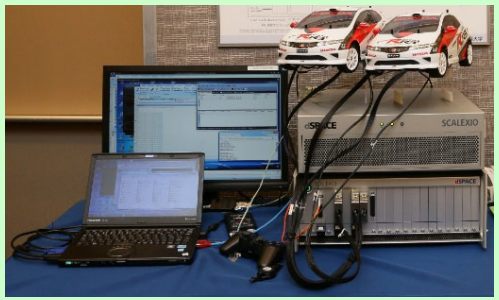


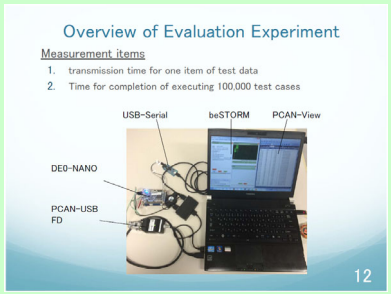
b. 強化手法

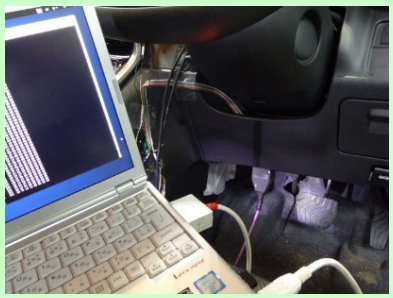




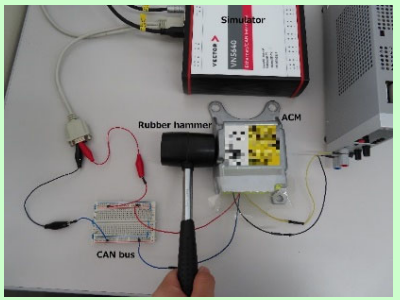
c. 評価手法と攻撃手法



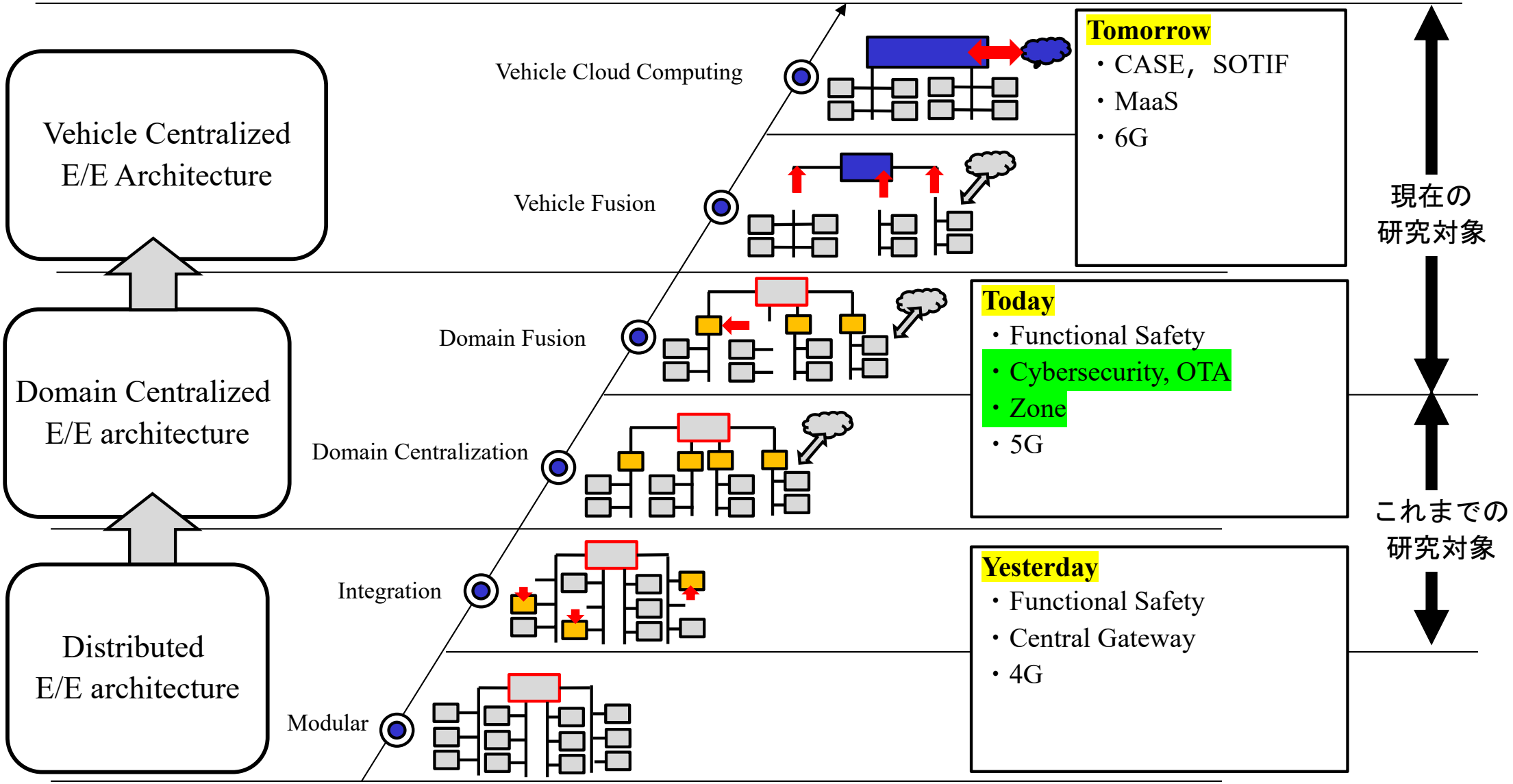




d. デジタルフォレンジック



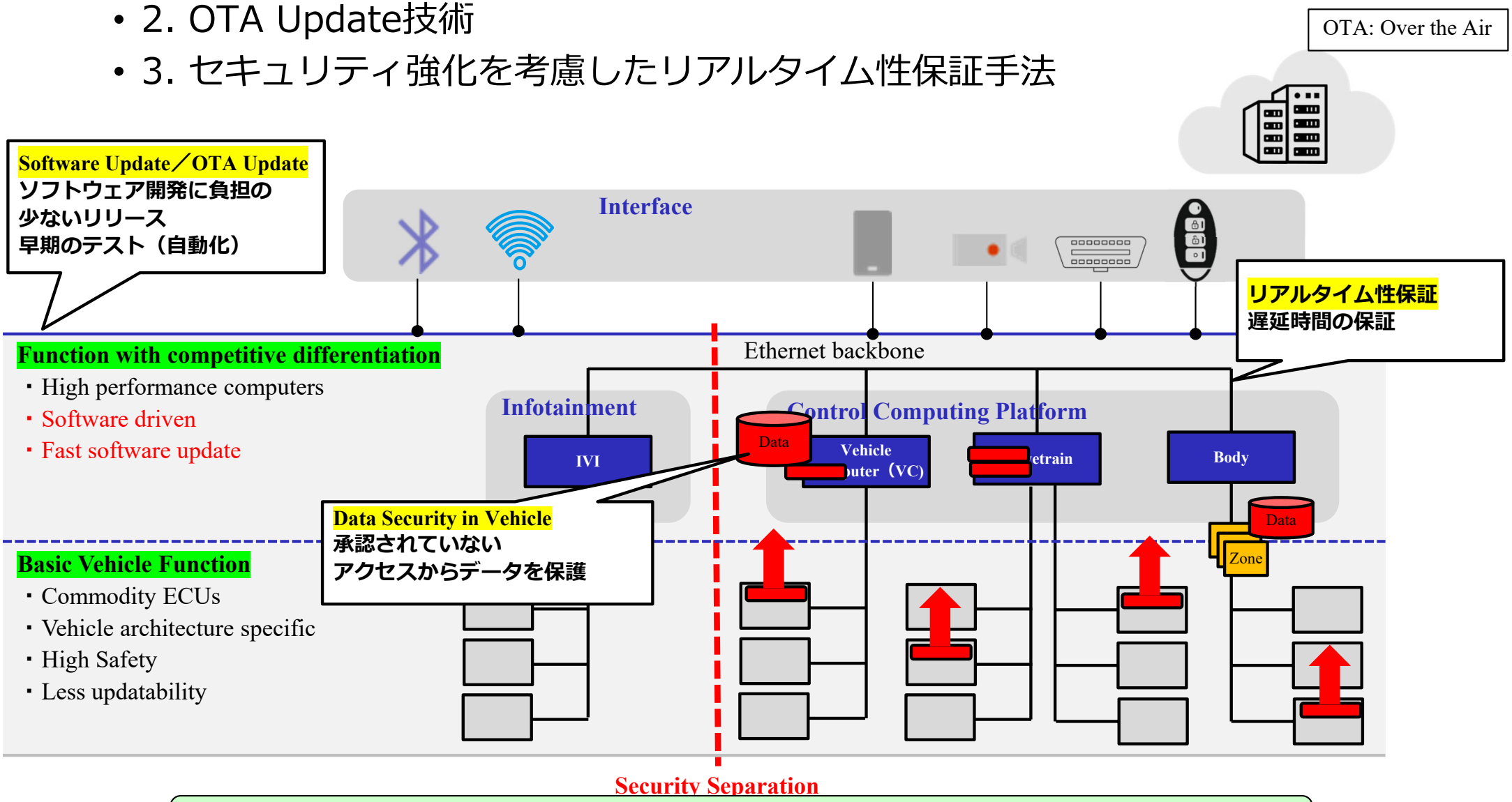
自動車の電子制御システムのロードマップ



将来システムを対象としたセキュリティ強化技術が対象になりつつある

現在の研究と今後の取り組み

- 1. 車載ECUのアクセス制御やデータセキュリティ（強化手法と評価手法）
- 2. OTA Update技術
- 3. セキュリティ強化を考慮したリアルタイム性保証手法



詳しくはポスターにお越しください

まとめ

- NCESでは自動車のサイバーセキュリティ強化技術の研究を多数の企業や公的資金で実施
- 今後はより将来のシステムにおけるセキュリティ強化技術の研究開発を実施していく