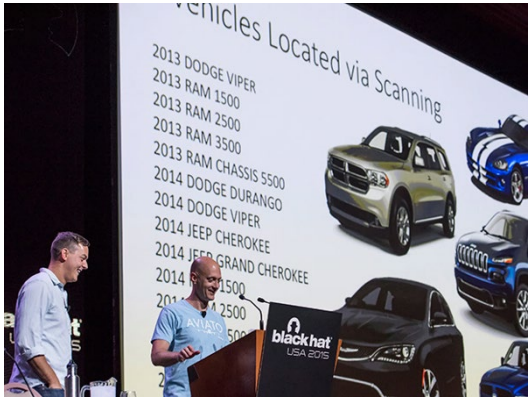
自動車のサイバーセキュリティ強化技術

2024年10月22日（火）

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

近年，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/

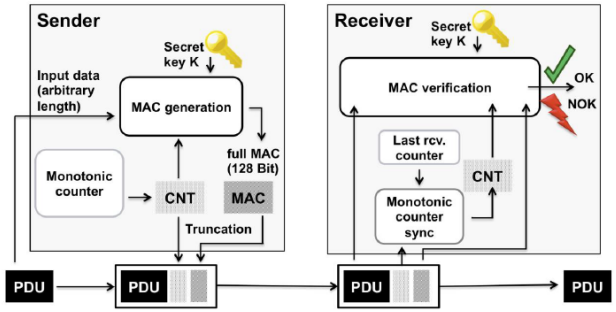
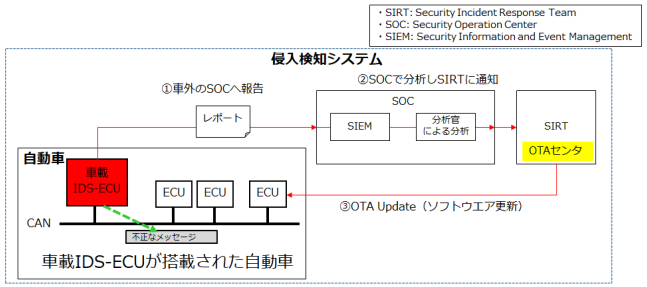


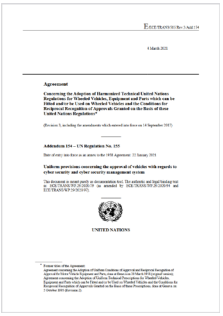
Figure 1: Message Authentication and Freshness Verification

適用されつつある技術の例1. メッセージ認証

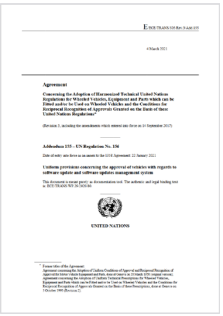
AUTOSAR version R21-11 Requirements on Module Secure Onboard Communication



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～）**

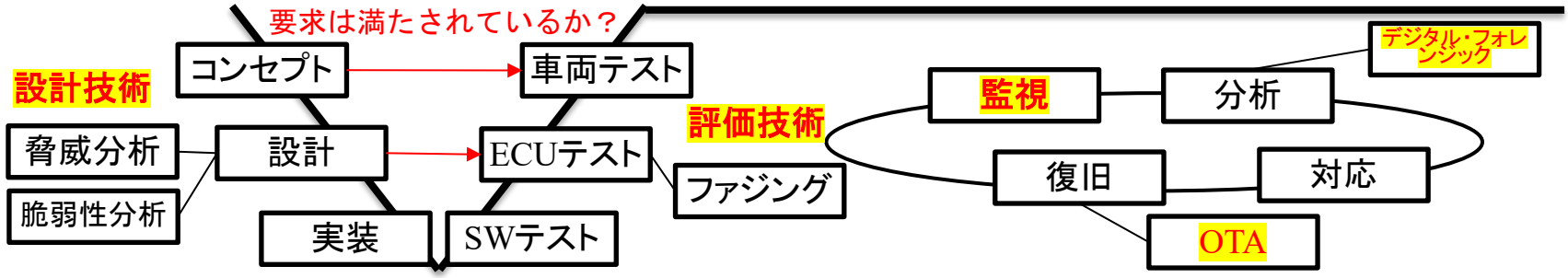
自動車の製品ライフサイクルとセキュリティ技術

- 自動車のライフサイクルは4つのプロセス(企画，開発，運用，廃棄)に分割
- 自動車のライフサイクル全体にサイバーセキュリティ強化が要求
- NCESでは，開発フェーズだけでなく，運用フェーズ（監視，OTA，フォレンジック）の研究課題にも取り組んでいる

自動車の製品ライフサイクル

企画	開発			運用（国内では平均所有年数が11年程度）	廃棄
	設計	実装	製造		

プロセス



製品（システム・サービス）


×N個

組み込む

連携

Security Operation Center (SOC)　コネクテッドサービス　WEBアプリ

複数の部品メーカ（ECU）　自動車メーカ（車両）　自動車メーカ・販売店・事業者（サービス）

設計技術，評価技術，監視，OTA，フォレンジックに関する共同研究を実施

NCESにおけるセキュリティ関連の共同研究の実施状況

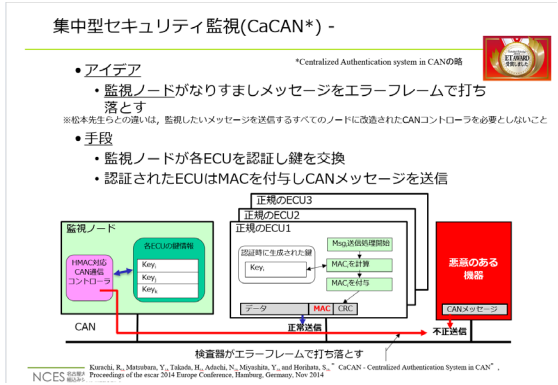
- **NCESと各企業の1対1の共同研究を複数実施**
  - セキュリティの性質上，コンソーシアム型の研究になりにくいか？
  - ただし，幾つかのテーマを繋ぎ合わせると1つの研究になりそう

- **共同研究先企業名（50音順）**
  - アイシン
  - オートネットワーク技術研究所
  - クレスコ
  - 警察大学校
  - セキュアイノベーション
  - テクノプロ（テクノプロ・デザイン社）
  - パナソニック ホールディングス
  - ミックウェア オートモーティブ　　他数社

以降では，幾つかのトピックのみをご紹介いたします

これまでの共同研究の実績

設計技術の実績 (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)

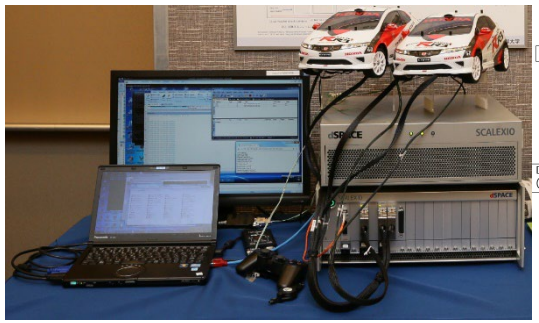


ET Award 2014
(オートネットワーク技術研究所)

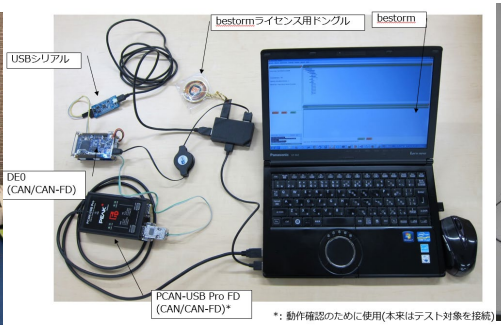
escar でのデモンストレーション
(オートネットワーク技術研究所)

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

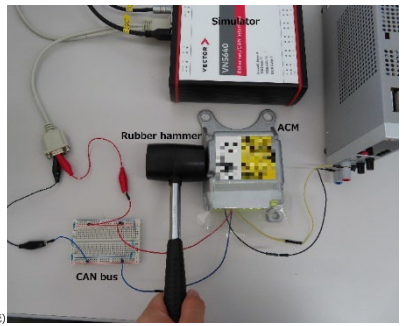
評価技術の実績 (1) 仮想環境上の評価 (2) ECUの評価 (3) 実車両の評価



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)

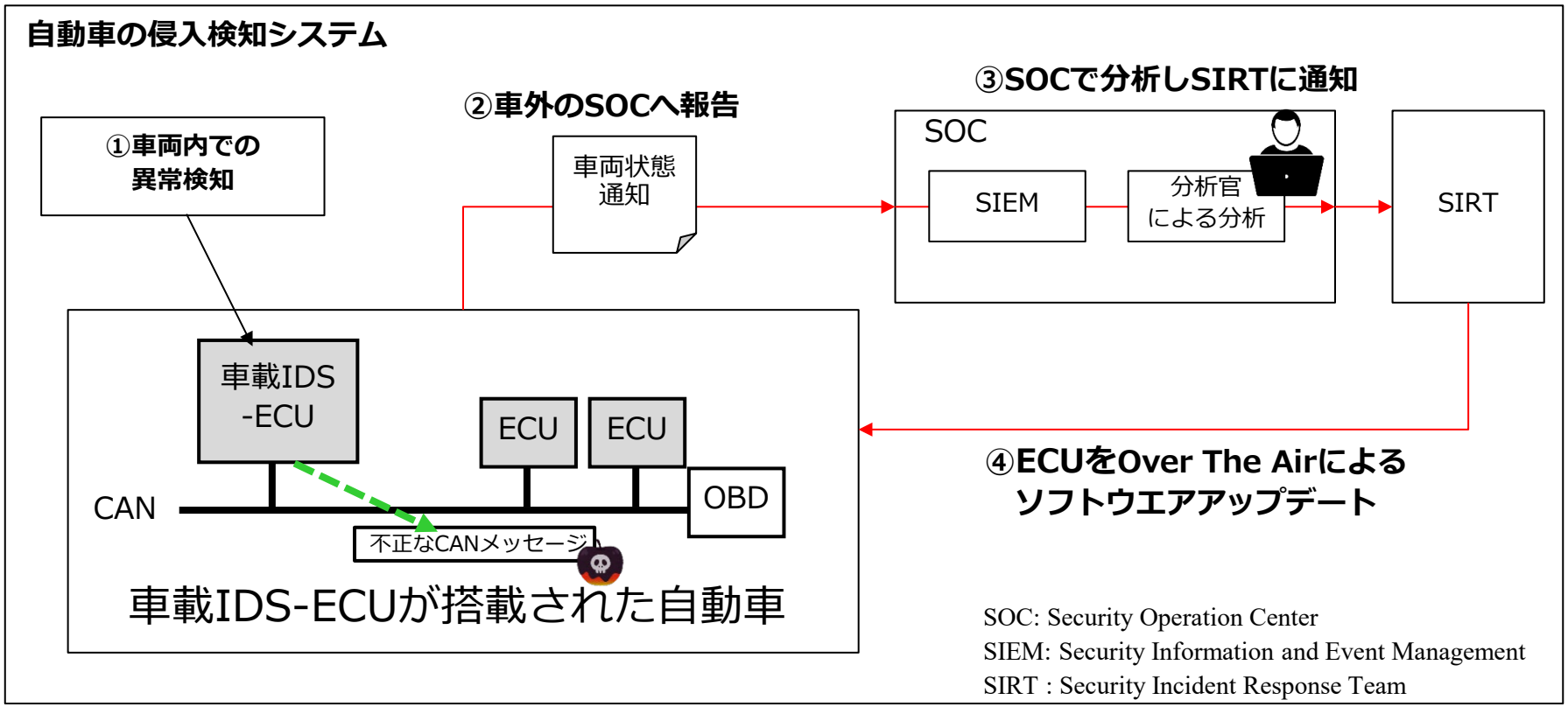


実ECUの評価
(警察大学校とパナソニック)

実車両を評価
(パナソニック)

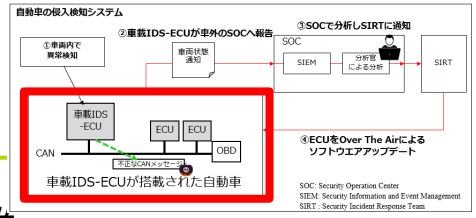
自動車の侵入検知システム

- 自動車には車載IDS-ECUが配置され，車両内の異常や攻撃を検出
- 車載IDS-ECUが車外にあるSOCに車両状態通知を転送
- Over The Air (OTA)によるソフトウェアアップデートで保守

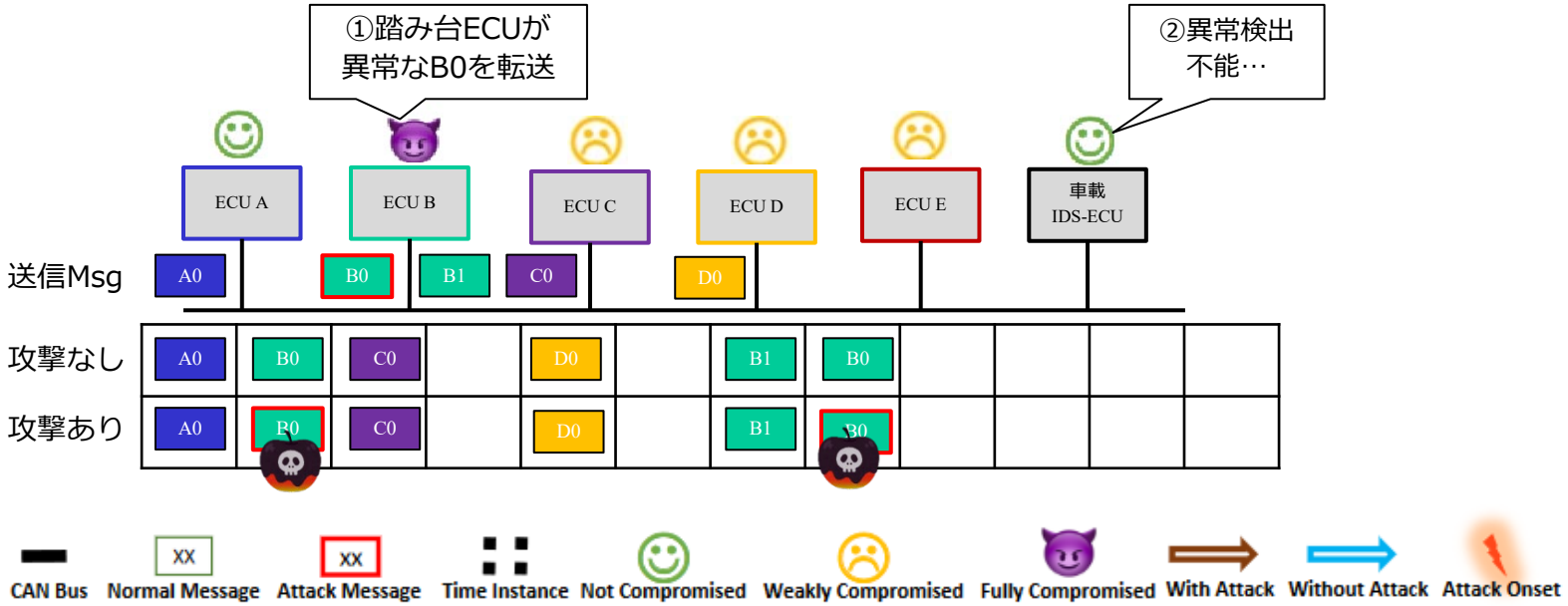


現在，幾つかの共同研究プロジェクトは①～④に関するテーマを実施

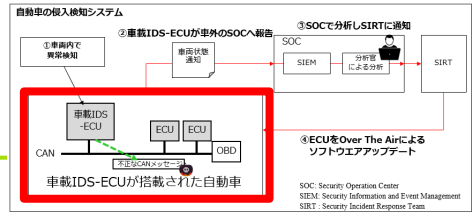
「①車両内での異常検知」の課題



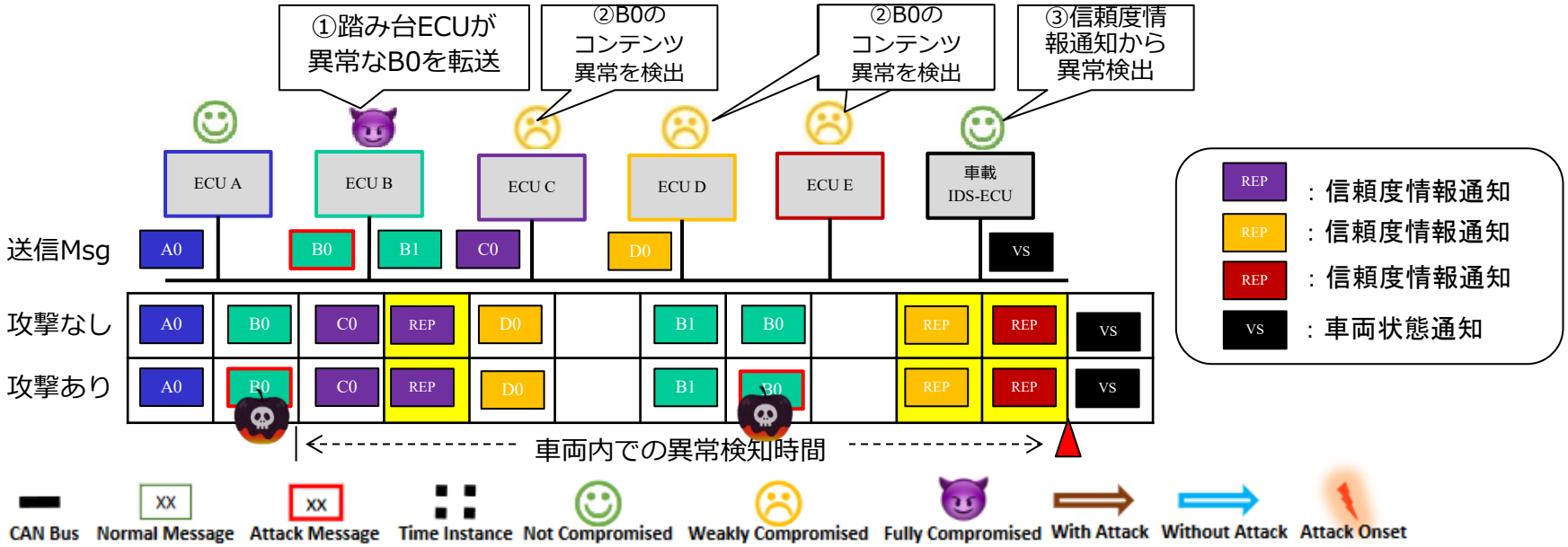
- プログラムが改ざんされたECU（踏み台ECU）の検知が困難
  - 最も強力な攻撃のひとつだが，既存研究がほとんどない
  - 下図の例. ECU Bのプログラムを改ざんし乗っ取り，異常なメッセージB0を転送
- 踏み台ECUの検知の難しさ　…　既存手法が役に立たない
  - 例1. メッセージ認証コード(MAC)：攻撃者に悪用され無力
  - 例2. 転送頻度監視：B0の転送頻度は変化なく検知できない
  - 例3. 信号波形監視：ECU Bから転送されるB0メッセージのため検知できない



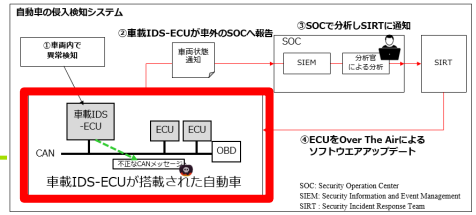
「①車両内での異常検知」のアイデア



- 群衆の知恵
  - 各ECUが相互に信頼／非信頼を評価し合う
- 提案手法の概要
  - メッセージB0の受信ノード(ECU C, D, E）が異常を検出
  - ECU C, D, Eは信頼度情報通知を転送しECU Bを非信頼と評価
  - 車載IDS-ECUは信頼度情報通知内の情報からECU Bの異常を検出



提案手法で用いる信頼度計算モデル



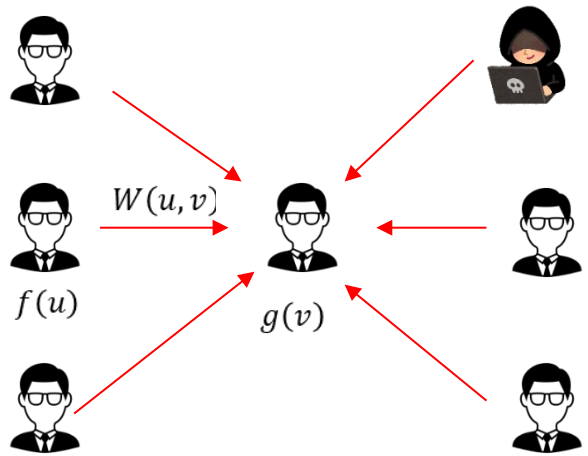
- Kumarの計算モデル
  - 公平性(Fairness)と善良性(Goodness)による信頼できないユーザの検出モデル
  - 例えば，SNSやショッピングサイト上の詐欺師や嘘つきを見つける手法

- **公平性**
  - **自身が他のユーザをどう評価（$W(u, v) \in [-1,1]$ ）するかに影響**
  - **他のユーザに正しい評価を与える場合，公平とみなす**
  - $f(u) \in [0,1]$

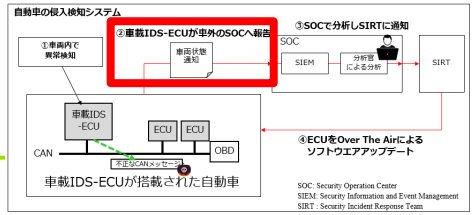
$$f(u) = 1 - \frac{1}{out(u)} \sum_{u \in out(u)} \frac{|W(u,v) - g(v)|}{R} \qquad (2)$$

- **善良性**
  - **他のユーザーによる自身の評価に影響**
  - 公正なユーザから高い評価を得られれば，善良なユーザとみなされる
  - Goodness $g(v) \in [-1, 1]$

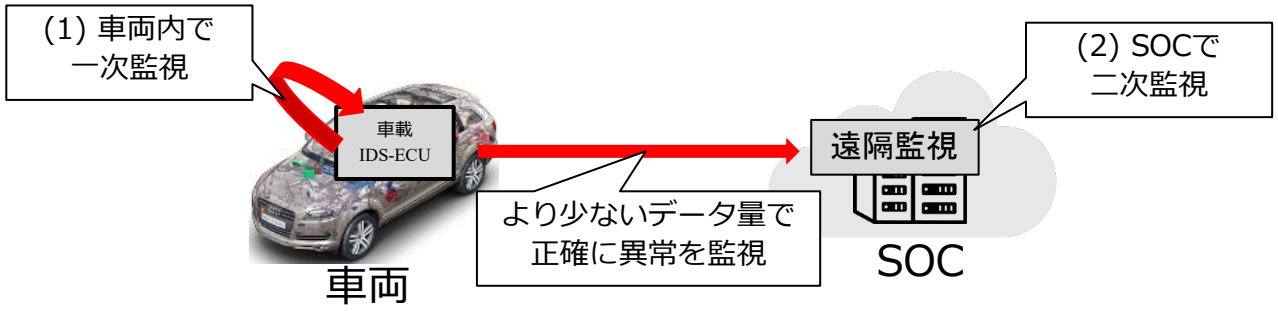
$$g(v) = \frac{1}{in(v)} \sum_{u \in in(v)} f(u) \times W(u,v) \qquad (1)$$



提案手法の利点

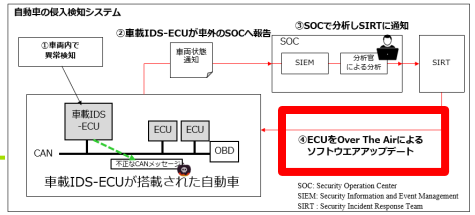


- **遠隔からの車両監視時に必要なデータ量を低減可能**
- **遠隔監視に関する既存研究の課題**
  - すべてのCANメッセージを車両外のSOCへ転送し遠隔監視を実現
  - ある車両1台あたり1時間に生成される**CANのデータ量は約1.8GB**
  - 100万台単位の遠隔監視は困難では？
- **我々の提案手法**
  - 車両に搭載されるN個のECUの公平性と善良性のみをSOCで監視
  - 10個のECUを100ms周期で監視しても，1秒あたり800Bのデータ
  - 1時間に**2.8MB程度のデータ量**と試算



②車外のSOCへ報告に必要なデータ量を削減し，③遠隔での監視アルゴリズムを検討中

④ Over The Airによるソフトウエアアップデート



- オンライン参加の皆様には大変申し訳ありませんが,
  ポスター発表**P09**, **P10**(赤枠)にてご紹介いただく予定です.
- 現地参加の皆様は是非お立ち寄りください.

● ポスターセッション＆休憩　16:15-- 17:00

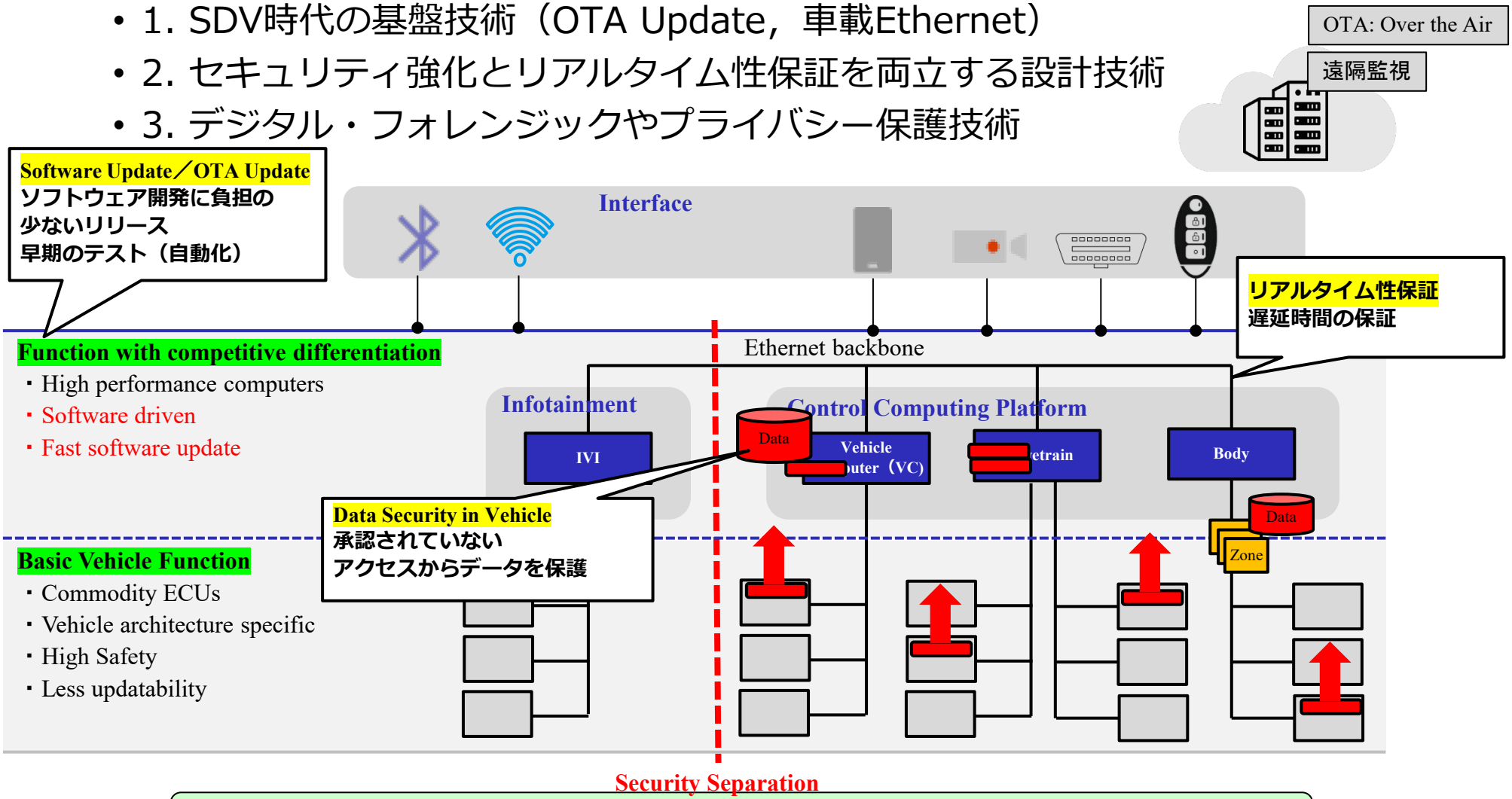
◇ポスター展示（FUJIホールエントランス）

協力企業、団体、NCESのプロジェクトのポスター展示を行います。

ポスターNO.	タイトル	発表者
P01	自動車のサイバーセキュリティ強化技術[資料]	倉地 亮（附属組込みシステム研究センター 特任准教授）
P02	AUTOSAR Adaptive Platform(A 2 P)コンソの活動紹介[資料]	笹本 晃司（附属組込みシステム研究センター 研究員）
P03	enPiT-Reskill Embの紹介 ～学部レベルの教材を活用した社会人ソフトウェア学習の始め方～[資料]	福島 泰子（附属組込みシステム研究センター 研究員）
P04	Open SDV Initiativeの活動紹介[資料]	高田 広章（附属組込みシステム研究センター長）
P05	衛星搭載ソフトウェアの構築技術[資料]	高田 光隆（附属組込みシステム研究センター 研究員）
P06	リアルタイムLinux関連の研究活動[資料]	李 奕驍（附属組込みシステム研究センター 特任助教）
P07	あなたの会社の人材育成にNCESを活用しませんか[資料]	山本 雅基（附属組込みシステム研究センター　特任教授）
P08	先進モビリティサービスのための情報通信プラットフォームに関するコンソーシアム[資料]	渡辺 陽介（未来社会創造機構モビリティ社会研究所 特任准教授）
P09	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[資料]	納庄 実菜（株式会社テクノプロ　テクノプロ・デザイン社）
P10	車載向けOTA更新における差分アルゴリズムの比較評価	川崎 雄也（株式会社クレスコ）
P11	LiDARを用いた物体認識性能の向上と活用事例	岸田 宏翼（キヤノンITソリューションズ株式会社）

今後の取り組みの方向性

- **次世代の自動車に必要なセキュリティ技術の研究開発を進める**
- 1. SDV時代の基盤技術（OTA Update，車載Ethernet）
- 2. セキュリティ強化とリアルタイム性保証を両立する設計技術
- 3. デジタル・フォレンジックやプライバシー保護技術



詳しくはポスターP01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に関する共同研究を複数実施
- 今後は次世代の自動車に必要な技術の研究開発に注力予定