

## 講演 1

# 車両制御における情報セキュリティに関する研究

主席研究員

新国 哲也



# 車両制御における情報セキュリティに関する研究

自動車安全研究部 主席研究員 新国 哲也

## 本日の内容

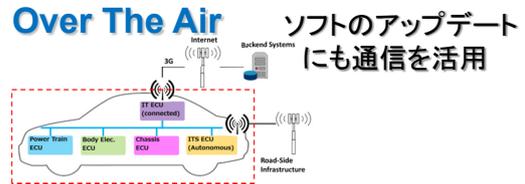
1. 研究の背景
2. 研究目的
3. 研究方法
4. 結果と考察
5. 国連(UNECE)・WP29の状況
6. まとめ

# 1. 研究の背景

➤ 自動運転技術は普及段階に入りつつある



➤ 車両のコネクティビティは高まる方向にある



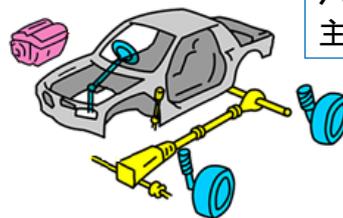
制御に係る複雑かつ大量な**情報**を記録し活用したい  
(事故分析にも役立つ)



## 自動車審査や検査も新たな対応が必要となる

これまでの審査・検査対象

- ECE R3 反射器
- ECE R6 方向指示器
- ECE R16 シートベルト
- ECE R13H ブレーキ
- ⋮

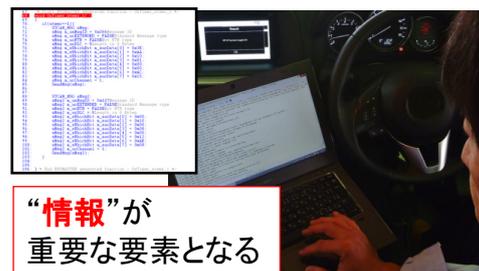


ハードウェアが  
主体的

審査・検査対象の<将来像>

従来の  
対象

- ECE R3 反射器
- ECE R6 方向指示器
- ECE R16 シートベルト
- ECE R13H ブレーキ
- ⋮



“**情報**”が  
重要な要素となる

## 2. 研究目的

自動運転技術の進展などを考慮し、  
車両制御の電子情報に関するセキュリティと  
将来的な自動車審査に係る課題を整理する

1. 実車の制御情報に関する調査  
⇒現状把握
2. 情報の管理(EDR、DSSAD)に係る要件の検討

EDR: Event Data Recorder

DSSAD: Data Storage System for Automated Driving

+ 国際基準調和への対応

## 3. 研究方法

1. 実車の制御情報に関する調査  
⇒現状把握

運転支援機能の制御情報に関する調査

実車を使い  
操舵などを中心に、  
国土交通省と協力して  
リスクに関連する調査  
を実施中

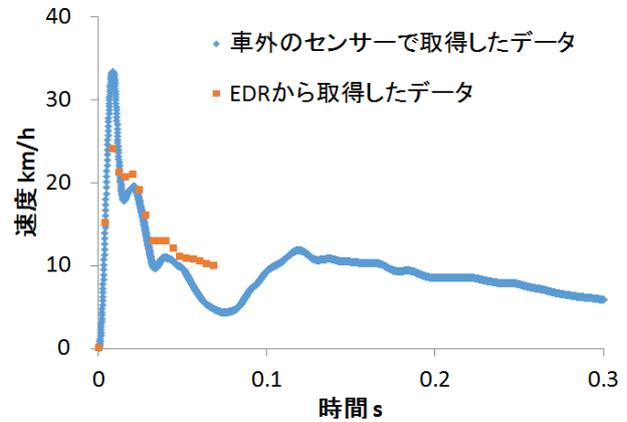


## 2. 情報の管理に係る要件の検討

衝突試験で使用した車両のエアバッグECUに記録されたEDRによるデータを取得



試験車の場合、プリクラッシュデータには  
Accelerator Pedal, Percentage of Engine Throttle (%)  
Engine RPM (RPM), Motor RPM (RPM)  
Service Brake, Brake Oil Pressure (Mpa)  
Longitudinal Acceleration, VSC Sensor (m/sec<sup>2</sup>)  
Steering Input (degrees)  
Shift Position, Sequential Shift Range  
Cruise Control Status, Drive Mode. 等が記録される



衝突安全班による実車試験の結果を用い、EDRデータと実測データの比較検証を行った

## 4. 結果と考察

### 課題：車両制御の高度化に伴うデータ量の増大

従来車両のエアバッグECUのEDRでは、容量は  
**1k byte程度**

**70倍以上**

フロリダでのテスラの事例に関するケーススタディ  
フロリダでのテスラの事例を調査する当局である  
NTSB(National Transportation Safety Board)  
が検証したデータ量は、**70k byte程度**  
(「参考」に概要を記載)



Line	Time (s)	Lat (°)	Lon (°)	Description	Address	Unit	Resolution
1	0.000000	30.540000	-81.300000	00-CAR EDR02	202	0	00:00:00.000000
2	0.000000	30.540000	-81.300000	00-CAR EDR03	206	0	00:00:00.000000
3	0.000000	30.540000	-81.300000	00-CAR EDR04	100	0	00:00:00.000000
4	0.000000	30.540000	-81.300000	00-CAR EDR05	118	7	00:00:00.000000
5	0.000000	30.540000	-81.300000	00-CAR EDR06	144	0	00:00:00.000000
6	0.000000	30.540000	-81.300000	00-CAR EDR07	126	0	00:00:00.000000
7	0.000000	30.540000	-81.300000	00-CAR EDR08	136	0	00:00:00.000000
8	0.000000	30.540000	-81.300000	00-CAR EDR09	138	0	00:00:00.000000
9	0.000000	30.540000	-81.300000	00-CAR EDR10	140	3	00:00:00.000000
10	0.000000	30.540000	-81.300000	00-CAR EDR11	142	0	00:00:00.000000
11	0.000000	30.540000	-81.300000	00-CAR EDR12	146	0	00:00:00.000000
12	0.000000	30.540000	-81.300000	00-CAR EDR13	154	0	00:00:00.000000
13	0.000000	30.540000	-81.300000	00-CAR EDR14	170	0	00:00:00.000000
14	0.000000	30.540000	-81.300000	00-CAR EDR15	182	0	00:00:00.000000
15	0.000000	30.540000	-81.300000	00-CAR EDR16	148	0	00:00:00.000000
16	0.000000	30.540000	-81.300000	00-CAR EDR17	154	0	00:00:00.000000
17	0.000000	30.540000	-81.300000	00-CAR EDR18	164	0	00:00:00.000000
18	0.000000	30.540000	-81.300000	00-CAR EDR19	174	0	00:00:00.000000
19	0.000000	30.540000	-81.300000	00-CAR EDR20	184	0	00:00:00.000000
20	0.000000	30.540000	-81.300000	00-CAR EDR21	194	0	00:00:00.000000
21	0.000000	30.540000	-81.300000	00-CAR EDR22	202	0	00:00:00.000000
22	0.000000	30.540000	-81.300000	00-CAR EDR23	204	0	00:00:00.000000
23	0.000000	30.540000	-81.300000	00-CAR EDR24	206	0	00:00:00.000000
24	0.000000	30.540000	-81.300000	00-CAR EDR25	208	0	00:00:00.000000
25	0.000000	30.540000	-81.300000	00-CAR EDR26	208	0	00:00:00.000000
26	0.000000	30.540000	-81.300000	00-CAR EDR27	208	0	00:00:00.000000
27	0.000000	30.540000	-81.300000	00-CAR EDR28	208	0	00:00:00.000000
28	0.000000	30.540000	-81.300000	00-CAR EDR29	210	7	00:00:00.000000
29	0.000000	30.540000	-81.300000	00-CAR EDR30	212	0	00:00:00.000000
30	0.000000	30.540000	-81.300000	00-CAR EDR31	212	0	00:00:00.000000
31	0.000000	30.540000	-81.300000	00-CAR EDR32	212	0	00:00:00.000000
32	0.000000	30.540000	-81.300000	00-CAR EDR33	212	0	00:00:00.000000
33	0.000000	30.540000	-81.300000	00-CAR EDR34	212	0	00:00:00.000000
34	0.000000	30.540000	-81.300000	00-CAR EDR35	212	0	00:00:00.000000
35	0.000000	30.540000	-81.300000	00-CAR EDR36	212	0	00:00:00.000000
36	0.000000	30.540000	-81.300000	00-CAR EDR37	212	0	00:00:00.000000
37	0.000000	30.540000	-81.300000	00-CAR EDR38	212	0	00:00:00.000000
38	0.000000	30.540000	-81.300000	00-CAR EDR39	212	0	00:00:00.000000
39	0.000000	30.540000	-81.300000	00-CAR EDR40	212	0	00:00:00.000000
40	0.000000	30.540000	-81.300000	00-CAR EDR41	212	0	00:00:00.000000
41	0.000000	30.540000	-81.300000	00-CAR EDR42	212	0	00:00:00.000000
42	0.000000	30.540000	-81.300000	00-CAR EDR43	212	0	00:00:00.000000
43	0.000000	30.540000	-81.300000	00-CAR EDR44	212	0	00:00:00.000000
44	0.000000	30.540000	-81.300000	00-CAR EDR45	212	0	00:00:00.000000
45	0.000000	30.540000	-81.300000	00-CAR EDR46	212	0	00:00:00.000000
46	0.000000	30.540000	-81.300000	00-CAR EDR47	212	0	00:00:00.000000
47	0.000000	30.540000	-81.300000	00-CAR EDR48	212	0	00:00:00.000000
48	0.000000	30.540000	-81.300000	00-CAR EDR49	212	0	00:00:00.000000
49	0.000000	30.540000	-81.300000	00-CAR EDR50	212	0	00:00:00.000000
50	0.000000	30.540000	-81.300000	00-CAR EDR51	212	0	00:00:00.000000
51	0.000000	30.540000	-81.300000	00-CAR EDR52	212	0	00:00:00.000000
52	0.000000	30.540000	-81.300000	00-CAR EDR53	212	0	00:00:00.000000
53	0.000000	30.540000	-81.300000	00-CAR EDR54	212	0	00:00:00.000000
54	0.000000	30.540000	-81.300000	00-CAR EDR55	212	0	00:00:00.000000
55	0.000000	30.540000	-81.300000	00-CAR EDR56	212	0	00:00:00.000000
56	0.000000	30.540000	-81.300000	00-CAR EDR57	212	0	00:00:00.000000
57	0.000000	30.540000	-81.300000	00-CAR EDR58	212	0	00:00:00.000000
58	0.000000	30.540000	-81.300000	00-CAR EDR59	212	0	00:00:00.000000
59	0.000000	30.540000	-81.300000	00-CAR EDR60	212	0	00:00:00.000000
60	0.000000	30.540000	-81.300000	00-CAR EDR61	212	0	00:00:00.000000
61	0.000000	30.540000	-81.300000	00-CAR EDR62	212	0	00:00:00.000000
62	0.000000	30.540000	-81.300000	00-CAR EDR63	212	0	00:00:00.000000
63	0.000000	30.540000	-81.300000	00-CAR EDR64	212	0	00:00:00.000000
64	0.000000	30.540000	-81.300000	00-CAR EDR65	212	0	00:00:00.000000
65	0.000000	30.540000	-81.300000	00-CAR EDR66	212	0	00:00:00.000000
66	0.000000	30.540000	-81.300000	00-CAR EDR67	212	0	00:00:00.000000
67	0.000000	30.540000	-81.300000	00-CAR EDR68	212	0	00:00:00.000000
68	0.000000	30.540000	-81.300000	00-CAR EDR69	212	0	00:00:00.000000
69	0.000000	30.540000	-81.300000	00-CAR EDR70	212	0	00:00:00.000000
70	0.000000	30.540000	-81.300000	00-CAR EDR71	212	0	00:00:00.000000
71	0.000000	30.540000	-81.300000	00-CAR EDR72	212	0	00:00:00.000000
72	0.000000	30.540000	-81.300000	00-CAR EDR73	212	0	00:00:00.000000
73	0.000000	30.540000	-81.300000	00-CAR EDR74	212	0	00:00:00.000000
74	0.000000	30.540000	-81.300000	00-CAR EDR75	212	0	00:00:00.000000
75	0.000000	30.540000	-81.300000	00-CAR EDR76	212	0	00:00:00.000000
76	0.000000	30.540000	-81.300000	00-CAR EDR77	212	0	00:00:00.000000
77	0.000000	30.540000	-81.300000	00-CAR EDR78	212	0	00:00:00.000000
78	0.000000	30.540000	-81.300000	00-CAR EDR79	212	0	00:00:00.000000
79	0.000000	30.540000	-81.300000	00-CAR EDR80	212	0	00:00:00.000000
80	0.000000	30.540000	-81.300000	00-CAR EDR81	212	0	00:00:00.000000
81	0.000000	30.540000	-81.300000	00-CAR EDR82	212	0	00:00:00.000000
82	0.000000	30.540000	-81.300000	00-CAR EDR83	212	0	00:00:00.000000
83	0.000000	30.540000	-81.300000	00-CAR EDR84	212	0	00:00:00.000000
84	0.000000	30.540000	-81.300000	00-CAR EDR85	212	0	00:00:00.000000
85	0.000000	30.540000	-81.300000	00-CAR EDR86	212	0	00:00:00.000000
86	0.000000	30.540000	-81.300000	00-CAR EDR87	212	0	00:00:00.000000
87	0.000000	30.540000	-81.300000	00-CAR EDR88	212	0	00:00:00.000000
88	0.000000	30.540000	-81.300000	00-CAR EDR89	212	0	00:00:00.000000
89	0.000000	30.540000	-81.300000	00-CAR EDR90	212	0	00:00:00.000000
90	0.000000	30.540000	-81.300000	00-CAR EDR91	212	0	00:00:00.000000
91	0.000000	30.540000	-81.300000	00-CAR EDR92	212	0	00:00:00.000000
92	0.000000	30.540000	-81.300000	00-CAR EDR93	212	0	00:00:00.000000
93	0.000000	30.540000	-81.300000	00-CAR EDR94	212	0	00:00:00.000000
94	0.000000	30.540000	-81.300000	00-CAR EDR95	212	0	00:00:00.000000
95	0.000000	30.540000	-81.300000	00-CAR EDR96	212	0	00:00:00.000000
96	0.000000	30.540000	-81.300000	00-CAR EDR97	212	0	00:00:00.000000
97	0.000000	30.540000	-81.300000	00-CAR EDR98	212	0	00:00:00.000000
98	0.000000	30.540000	-81.300000	00-CAR EDR99	212	0	00:00:00.000000
99	0.000000	30.540000	-81.300000	00-CAR EDR100	212	0	00:00:00.000000

情報記録容量の大幅な増大  
が必要

## 課題：自動車用マイクロプロセッサチップのハードウェア的制約



自動車用チップ  
クロック周波数 32 MHz

自動車では、様々な制約からチップのみを特別に手当てするような冷却装置は用いられていない  
PCに比べ非常に過酷な環境でチップが使用されている

自動車の使用環境での耐性や信頼性を考慮して、**車載チップの計算能力は相当制限されたものになっている**

Intel Core i7の冷却装置の例

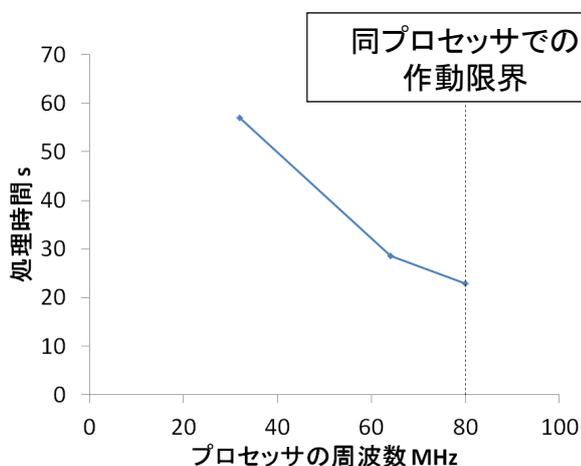
クロック周波数 1GHz以上



“COOLING MASTERについて” - TITANホームページより

## 車載レベルのプロセッサの計算能力に関する調査結果

RSA暗号(鍵の長さ256 byte)\*を70k byteのデータに対し実施した際の処理時間を計測した



- ✓ 60 MHz以上では周波数に対して処理時間の短縮が鈍くなる(頭打ち)
- ✓ 処理時間の大幅な短縮にはハードウェア自体を変更する必要がある

\*RSA暗号は総務省及び経済産業省により示された「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」の「守秘」のための暗号に指定されている

## 自動運転技術の進展などを考慮し、 車両制御の電子情報に関するセキュリティと 将来的な自動車審査に係る課題を整理した

- ◆ 自動運転に係る情報の管理には、現状の車両に比べ高い容量や処理速度が要求される  
(EDRのケースでは、レベル2でも現状に対し70倍程度以上の情報量)
- ◆ セキュリティなどの要点整理が必要  
⇒WP29でも議論が開始された
- ◆ ハードウェア上の制約も考慮する必要がある

## 5. 国連(UNECE)・WP29の状況

---

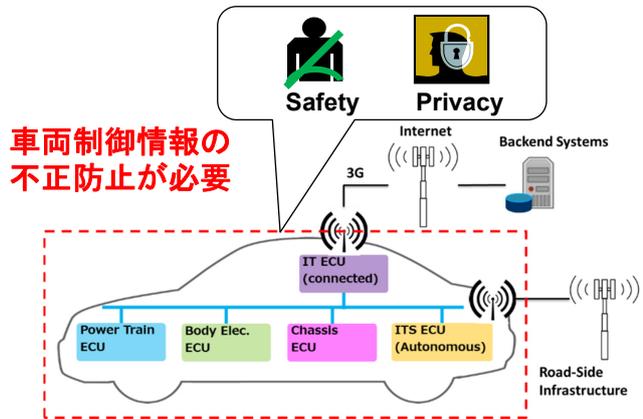
国連(UNECE)・WP29における自動車セキュリティ関連の  
活動状況について

# WP29-ITS/ADのセキュリティ・タスクフォースについて

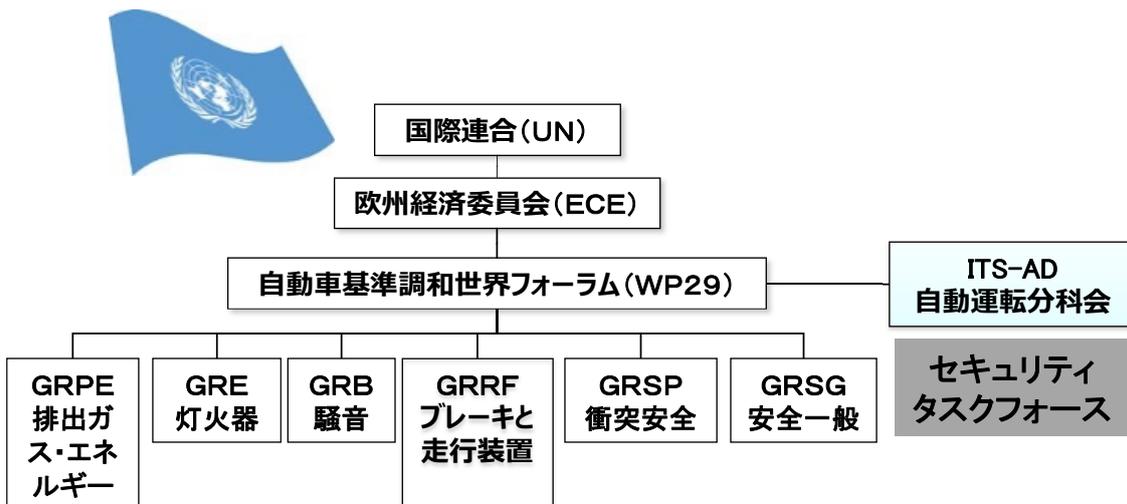
設立の背景:

自動車の車両制御等に係る重要情報を不正利用されないようにすることが重要であり、グローバル化が進む自動車において**国際的な対応が不可欠**である

ITS/AD(自動運転分科会)に、新たにTask Force on Cyber security and OTA(Over The Air) が設立され、2016年12月より活動を開始した



# WP29におけるセキュリティタスクフォース



## WP29-ITS/ADのセキュリティ・タスクフォースについて

### タスクフォースの構成

活動期間: 2016年12月  
~2018年6月

共同議長: ダーレン・ハンドレー氏  
(英国運輸省)  
新国哲也 (交通研)

セクレタリ: ジェンス・  
シェンケンバーガー氏(OICA/Hyundai)

参加者: 協定加盟国(EC、ドイツ、オランダ、フランス、韓国、  
中国、米国など)  
非政府組織(国際電気通信連合、国際自動車工業  
連合会、欧州自動車部品工業会など)



National Traffic Safety and Environment Laboratory

15

## セキュリティ・タスクフォースの課題

セキュリティ・タスクフォースの主課題は下記の2点

1. Vehicle Security
2. Software Update(OTAを含む)

これらに関して、WP29で対応すべき方策(基準化案)を  
まとめ、  
ITS/ADに提案文書を提出する



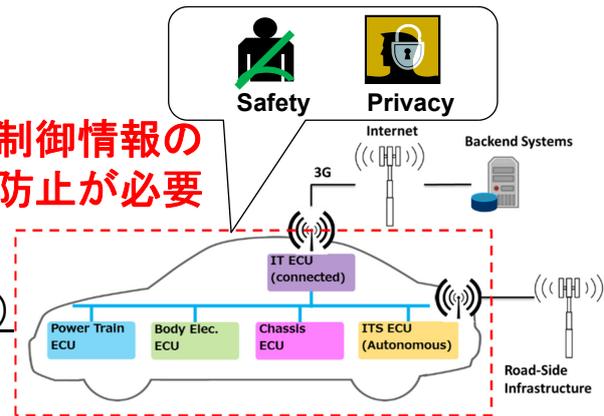
# セキュリティ・タスクフォース 議論のポイント

## Vehicle Security 技術的な対応策の検討

狙い:

想定される脅威に対し  
車両システムへの影響を低減  
するための緩和策 (mitigation)  
をWP29において共有する

車両制御情報の  
不正防止が必要



方策:

1. セキュアな車両システム構築するための原則(Principle)と緩和策 (mitigation)をまとめ、共有する
2. 実効性のある、横断的な**セキュリティ基準化案**を示す

# セキュリティ・タスクフォースの提案内容 (抜粋)

## Annex A Draft proposal to introduce a regulation on cyber security

1. Scope .
- 1.1 This Regulation applies to vehicles of the categories L, M, N, O, R, S and T...
2. Definitions .
- 2.1 "Vehicle type" means vehicles of a particular category which do not differ in at least the following essential respects:..
  - (a) The manufacturer;..
  - (b) The manufacturer's type designation;..
  - (c) The manufacturer's cyber security management system .
  - (d) Essential aspects of vehicle design with respect to cyber security.
- 2.2 Lifetime – the period from registration of a vehicle until it is scrapped .
- 2.3 Cyber security– The use of technologies, processes and practices designed to protect vehicles, systems, networks, devices and services – and their information, data and functionality– from attack or unauthorized access .
- 2.4 Cyber security management system .
- 2.5 "Competent Authority" means an entity, e.g. a Technical Service or another existing body, notified by a Contracting Party to carry out preliminary assessment of the manufacturer and to issue a certificate of compliance, in accordance with the prescriptions of this Regulation. The Type Approval Authority must ensure that the competent authority provided its competence in this field is properly documented .
3. Application for approval regarding cyber security .
- 3.1 The application for approval of a vehicle type with regard to cyber security shall be submitted by the manufacturer or by their duly accredited representative .
- 3.2 It shall be accompanied by the technical information necessary for the purposes of the checks referred to in Annex 1 to this Regulation .
- 3.3 In cases where such information is shown to be covered by intellectual property rights or by confidential know-how of the manufacturer or of their suppliers, the manufacturer or their suppliers shall supply sufficient information to enable those checks to be made properly .
- 3.4 With regard to cyber security, the Competent Authority shall ensure that the manufacturer uses the information document set out in Annex 2 to this Regulation, when submitting an application for type approval .
4. Approval regarding cyber security .

メーカーはSecurity Principleを守ること

メーカーは自社のシステムに関するリスクを分析し対策を取ること

リスク分析や対策に関して文書化すること

当局は、同文書によりメーカーが適切な対策を実施していることを確認すること

# Software Updates OTA(Over The Air)について



## Software Update(OTA)について

無線によるSoftware Updateが可能になると…

従来は、ユーザーがディーラーなどに車を持ち込んでupdateを実施していたが、無線を使えばその必要はなくなる

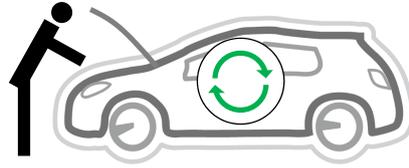
⇒サービスキャンペーンやリコールの実施率が上がると期待される

一方で、安全性に影響するなどの課題はないのか？

⇒過去のサービスキャンペーンやリコールを調査  
Software Updateが実施されたケースで  
**技術者による手作業**が必要であったケースを抽出した

## Software Update(OTA)について

いくつかのケースでは、ソフトウェアだけでなく**ハードウェアの点検・交換や、アクチュエータの学習作業**などを行っている。



自動車では、スマートフォンなどとは異なり、**OTAの利用が適さない場合がある**

⇒提案文書に反映済み

## 6. まとめ

- 車両の制御に係る情報の管理は、将来的な自動車審査・検査に係る課題であり、調査・研究を実施している
- セキュリティは WP29において重要なアイテムとして位置づけられ、議論が行われている
- WP29において国際的な連携が図れるよう提案内容のまとめに貢献する

