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

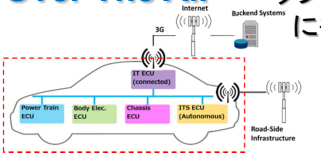
1. 研究の背景
2. 研究目的
3. 研究方法
4. 結果と考察
5. 国連（UNECE）・WP29の状況
6. まとめ

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

Over The Air　ソフトのアップデートにも通信を活用

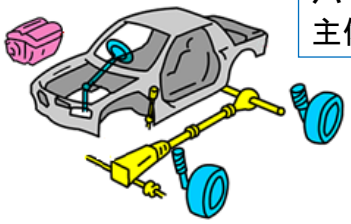


制御に係る複雑かつ大量な**情報**を記録し活用したい
（事故分析にも役立つ）

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
- …



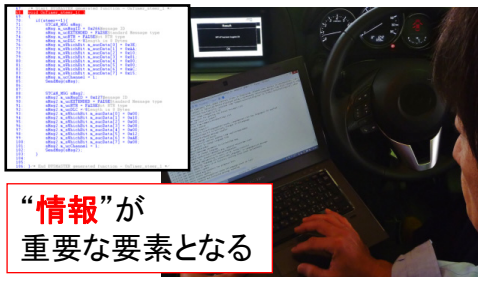
ハードウェアが主体的

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

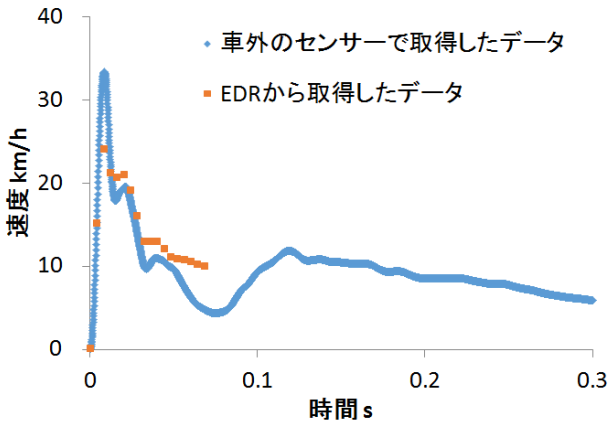
運転支援機能の制御情報に関する調査

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^2)
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

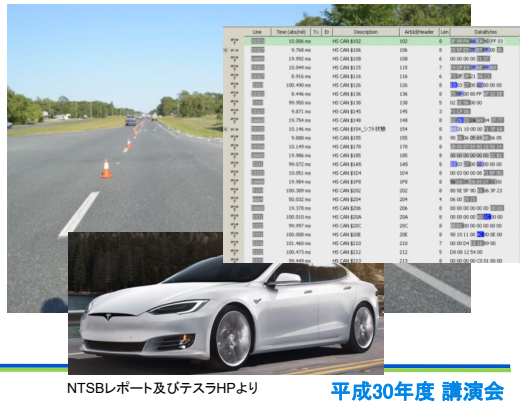
課題：車両制御の高度化に伴うデータ量の増大

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[illegible]テスラの[illegible]によるケーススタディ

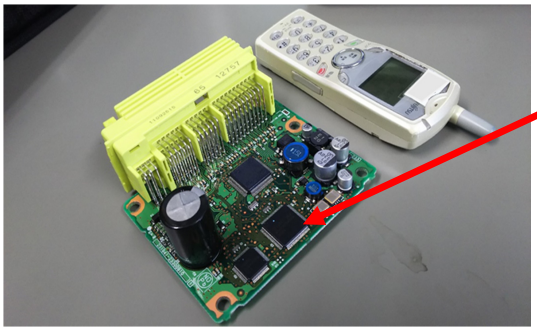
フロリダでのテスラの[illegible]で当局である
NTSB(National Transportation Safety Board)
が検証したデータ量は、**70k byte程度**
（「参考」に概要を記載）



NTSBレポート及びテスラHPより

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**

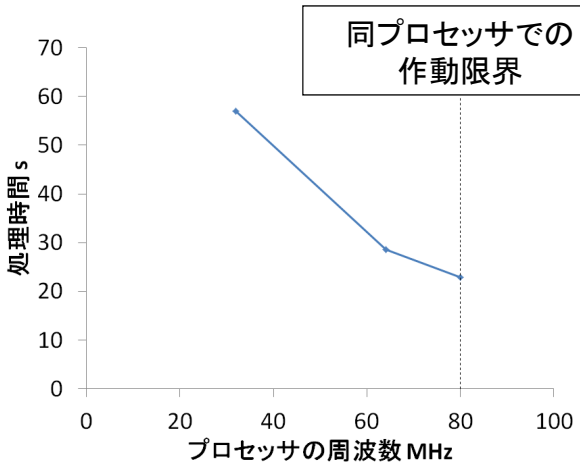
Intel Core i7の冷却装置の例

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

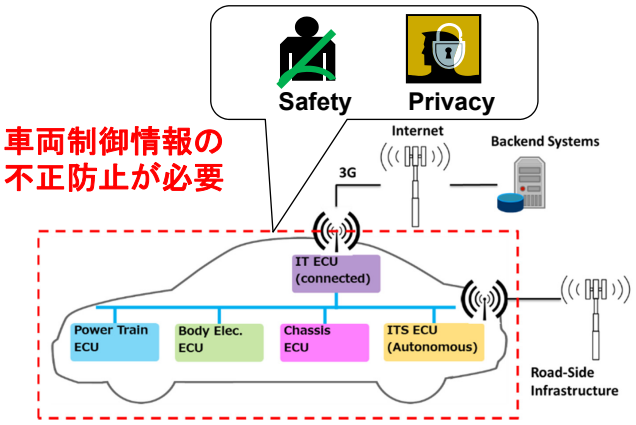
国連（UNECE）・WP29における自動車セキュリティ関連の
活動状況について

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

国際連合（UN）

欧州経済委員会（ECE）

自動車基準調和世界フォーラム（WP29）

ITS-AD
自動運転分科会

セキュリティ
タスクフォース

GRPE
排出ガス・エネルギー

GRE
灯火器

GRB
騒音

GRRF
ブレーキと走行装置

GRSP
衝突安全

GRSG
安全一般

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)

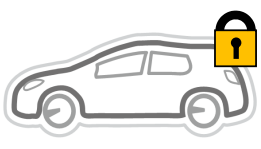
参加者: 協定加盟国(EC、ドイツ、オランダ、フランス、韓国、
中国、米国など)
非政府組織(国際電気通信連合、国際自動車工業
連合会、欧州自動車部品工業会など)

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

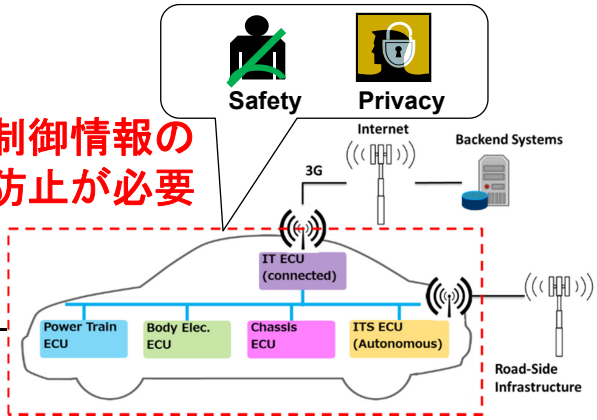


セキュリティ・タスクフォース 議論のポイント

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, v 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 m 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 veh manufacturer or by their duly accredited representative.
3.2. It shall be accompanied by the technical information necessary for the purposes of the checks ref Annex 1 to this Regulation.
3.3. In cases where such information is shown to be covered by intellectual property rights or k stitute know-how of the manufacturer or of their suppliers, the manufacturer or their suppliers shall supply suffi 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 m the information document set out in Annex 2 to this Regulation, when submitting an application for type approval.
4. **Approval regarding cyber security**

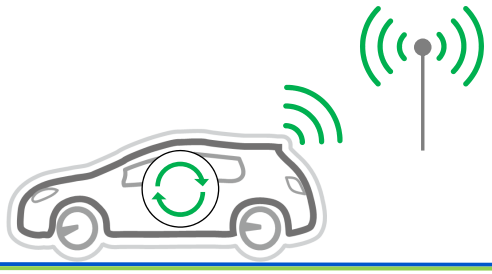
メーカはSecurity Principleを守ること

メーカ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

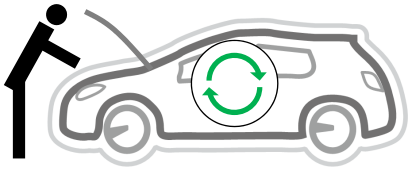
⇒サービスキャンペーンやリコールの実施率が上がると期待される

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

参考 フロリダでのテスラの事故によるケーススタディについて

- 出典：NTSB(National Transportation Safety Board)による “TECHNICAL RECONSTRUCTION GROUP CHAIRMAN’S FACTUAL REPORT”/ Williston, FL / NTSB Number: HWY16FH018
- 同レポートに言及のあった、当該車両のパラメータとサンプリング時間、記録時間は下記の通り

1. ACCの車速設定値
2. 車速
3. ステアリング角度
4. エアバッグ作動ステータス
5. ブレーキランプスイッチ
6. フォルト・コード
7. モータトルクデマンド
8. ブレーキ指示値

サンプリング時間：100ms
記録時間：2分程度

- 以上の情報と、下記の仮定の条件から、同レポートで調査対象となったデータの必要記録容量を試算した

	パラメータ	仮定した必要 byte （タイムスタンプとの合計値）
1	ACCの車速設定値	2 (9)
2	車速	2 (9)
3	ステアリング角度	2 (9)
4	エアバッグ作動ステータス	1 (8)
5	ブレーキランプスイッチ	1 (8)
6	フォルト・コード	1 (8)
7	モータトルクデマンド	2 (9)
8	ブレーキ指示値	2 (9)

- タイムスタンプは、当該ECUが発行し、各パラメータと1対1で対応する
- タイムスタンプは、年（西暦下2桁）、月、日、時、分、秒、1/100秒のデータで構成し、7byteとする
- サンプル数は1パラメータ当たり1000個で試算する

必要記録容量の試算値は
69 byte ×1000 個 ≒ 70k byte