講演７．国連自動車基準調和世界フォーラムにおける自動車セキュリティの議論の状況と交通安全環境研究所の取組

国際調和推進部　※新国 哲也　自動車研究部　小林 摂　河合 英直

１．はじめに

ドライバーが自動車をより安全に運転することを可能にする運転支援機能や自動運転機能の普及に伴い、自動車の制御システムや外部との情報通信におけるセキュリティの重要性が増している。国連の自動車基準調和世界フォーラム（以下、「WP29」という）の傘下の自動運転分科会（ITS/AD: Intelligent Transport Systems / Automated Driving）において取りまとめられた自動車のセキュリティガイドラインが車両構造に関する統合決議として発効した[1)]。さらに、今後 WP29 で対応すべき自動車セキュリティ上の課題を抽出するため、ITS/AD 傘下にセキュリティタスクフォース（以下、「TF」という）が新たに設置され、自動車のセキュリティに必要な国際的な技術要件について議論が進められている。

本稿では、TF における検討内容と交通安全環境研究所の活動の概要について述べる。

WP29 の ITS/AD における TF の概要は下記の通りである。

- Leading team：
  - 議長：英国（英国運輸省）
  - 日本（交通安全環境研究所）
  - 事務局：国際自動車工業連合会（OICA）
- 活動期間：1 年 (2016 年 12 月~2017 年 12 月)
- 参加国（団体）
  - 政府： 英国、日本、オランダ、ドイツ、フランス、EC、中国、他
  - 非政府組織:
    - 国際自動車工業連合会（OICA）
    - 欧州自動車部品工業会（CLEPA）
    - 国際自動車検査委員会（CITA）
    - 国際電気通信連合（ITU）
    - 国際自動車連盟（FiA）

TF は 2017 年 12 月までに WP29 での取組に関する提言をまとめ、ITS/AD へ提出することとしている。

2～5 章では TF の活動状況について、また 6 章では当研究所で実施している自動車に特化した情報セキュリティ分野への取組について説明する。

２． TF で取り扱う課題

TF では、活動を開始するにあたり ToR(Terms of Reference)として活動方針を定めた[2)]。TF の主たる課題として下記の 3 項目を設定した。

①サイバーセキュリティ対策
②ソフトウェアアップデートに関する対策
③データ保護

以下に、これらの 3 項目について TF の進捗状況を説明する。

３．サイバーセキュリティに関する議論の状況

自動車に特化したセキュリティ対策の検討は次のようなアプローチで実施している。

①どのような脅威（例えば CAN(Controller Area Network)メッセージの不正など）が起こりうるかを想定する。
②この脅威による車両安全性への影響などを最小限化する手段を検討し、その上で対策案をまとめる。

３．１．リファレンス車両モデルの概要

上記アプローチで検討を行うに当たり、サイバーセキュリティが必要とされる車両としてリファレンス車両モデルを設定し、その共通的仕様を定めた（表 1）。

また、図 1 には TF の検討対象の範囲を示した。TF において想定した検討の対象物に関する特徴は、例えばメーカなどが自動車のユーザーに対して提供するサービス用のサーバーを含んでいる点である。ITS/AD による自動車のセキュリティガイドラインが、自動運転車及び Connected vehicle といっ

た車両を対象にしているのに対し、同 TF の検討対象範囲は、自動車との通信を行う自動車メーカのサーバーや道路側との通信システムを含んだ幅広いものとなっている。

表１　リファレンス車両モデルの定義

The reference vehicle model including	
	Hardware
	Software
	Data held on the vehicle
	Internal communications
	Interfaces with
	External communication systems/ functions (e.g. V2X and emergency communications) and devices (e.g. USB, CD etc.)
	Vehicle functions/systems that use wireless communications (e.g. TPMS, keyless entry)
	Support servers which directly communicate with the vehicle
	Diagnostic/maintenance systems

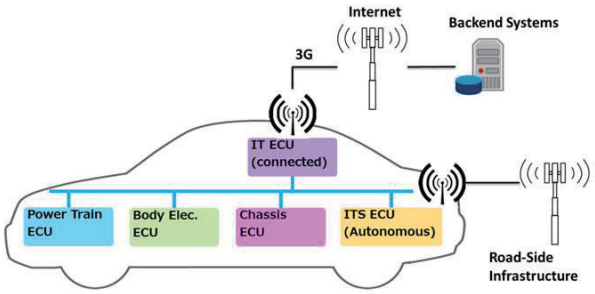

図１　脅威分析の検討対象範囲

想定した脅威のカテゴリは下記の通りである。

1. Compromise of back-end server
（サービス用のサーバーへの不正接続）
2. Internal communication channels used to attack a vehicle（内部通信手段を利用した攻撃）
3. Update process used to attack a vehicle
（アップデートを利用した攻撃）
4. Human factor and social engineering
（人的要素に関する脅威）
5. Compromise of external connectivity
（外部接続手段の不正接続）
6. Target of an attack on a vehicle（特定車両への攻撃）
7. System design exploits（設計仕様の悪用）
8. Data loss / "data leakage" from vehicle
（情報漏えい）
9. Physical manipulation of systems to enable an attack （システムの物理的な改ざん）
10. Vehicle used as a means to propagate an attack
（他への攻撃起点とする車の悪用）
11. Communication loss to/from vehicle
（通信のロス）
12. Non-cyber security vehicle threats
（その他の物理的な脅威）

３．２．脅威分析及びその対策の検討例

以上に説明してきたアプローチにより、TF で実施した脅威分析とその対策の例を紹介する。議論の結果の取りまとめには、例えば車両メーカの開発などに活かせるように脅威の例に対する対応策および手段を示すこととしている。なお、紙面の関係上サーバーといった WP29 においては直接的な基準化の対象にならないものに関しては説明を割愛し、車両に関連する脅威分析とその対策についての検討例を紹介する。

①脅威の例：Spoofing of messages by impersonation
（なりすましによるメッセージの不正）

②対応策　：Online Services should have a strong mutual authentication of messages and assure secure communication (confidential and integrity protected) between the involved entities.
（オンラインサービスでは、送受信とも強固な認証手段を設ける）

手段の例：

- ✓ Message authentication for all messages received.（メッセージに認証を持たせる）
- ✓ Encryption for communications containing sensitive data.（重要データに暗号を用いる）
- ✓ Techniques to prevent replay attacks, such as timestamping and use of freshness values（時刻情報や常時更新する値を利用する）など

4．ソフトウェアアップデートについて

TF におけるソフトウェアアップデートに関する議論の状況について説明する。ソフトウェアアップデートに関するセキュリティについては前章の「サイバーセキュリティに関する議論の状況」においてカバーされているので、ここでは制度上の課題とその対策の議論の状況について説明する。

TF は、車両の登録後も含め OTA (Over-The-Air updates)すなわち無線通信を使ったソフトウェアアップデートの可用性なども考慮し、メーカ以外の当局など必ずしもソフトウェアの詳細な記載内容を把握していない者が必要に応じてソフトウェアアップデートの概要（アップデート対象の機能や型式認証への影響など）や履歴を把握する方法について検討している。現在案として挙げているのは、型式認証の対象となる機能単位で 1 つのソフトウェア同定番号（SWIN ：SoftWare Identification Number）を与え、このソフトウェア同定番号にソフトウェアアップデートの情報を関連付けて管理する方法である。

この提案のポイントは、自動車が基準適合の審査を経て、市販・登録されユーザーに使用される段階までを含めたソフトウェアアップデートの取り扱いを透明化することにある。例えば、欧州においては車両の登録情報についてメンバー国間の電子化による情報共有化を進めているが、このシステムと WP29 において検討中である審査情報の電子化（DETA : Database for the Exchange of Type Approvals）を組み合わせれば、SWIN の方法を適用し自動車の審査から使用までのソフトウェアアップデートを一括管理できる可能性がある。一方で、日本のように自動車審査と登録の仕組みが分かれている場合には、必ずしも有効ではない。TF では、各国事情にも配慮しながら、各国の制度に役立つ提案ができるよう議論を進めている。

5．データ保護について

先述の通り、ITS/AD において自動車のセキュリティガイドラインが取りまとめられ、車両構造に関する統合決議として発効した。このガイドラインはドイツ及び日本からの原案を統合し修正を加えた構成となっており、ガイドラインに取り上げられた個人情報を含むデータ保護については主にドイツの原案を反映している。この背景から TF においても引き続きデータ保護を主課題の 1 つと捉え議論を進めている。現状では、データ保護の手段としてのセキュリティ上の課題は、先の 3 章に示した「サイバーセキュリティに関する議論の状況」に含まれる課題として議論されている。なお、データ保護のポリシーについては、これからの議論となっている。

6．当研究所の取組について

ここまで TF における 3 つの主課題について議論の状況を説明した。1 章でも述べたが、TF としては 2017 年 12 月までにこれらの課題に対する対応策をまとめる予定である。この対応策への日本の意見の反映はもちろんであるが、さらにセキュリティに関する将来的な WP29 レベルの活動（例えば自動車のセキュリティに関する国際的な共通ルールの検討など）に関わっていくために、日本として対応するための組織が必要となった。そこで、自動車基準認証国際化研究センター（JASIC: Japan Automobile Standards Internationalization Center）に設置されている、官民からなる連携組織「自動運転基準化研究所」の傘下に、今年、通信・セキュリティタスクフォース（主査：自動車工業会）が設置され（図 2）活動を開始した。

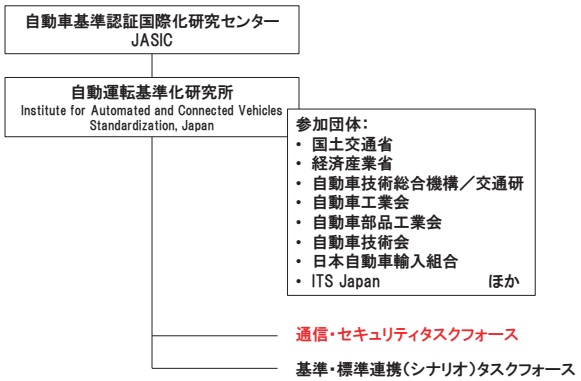

図 2　WP29 でのセキュリティの議論に対応する国内の体制

自動運転基準化研究所の通信・セキュリティタスクフォースでは、ITS/AD の TF にリンクしながら国内の専門家による脅威分析結果を基に ITS/AD の TF に提言を行うとともに、通信やセキュリティ分野の基準化を考慮した将来課題の検討のために独自の調査活動を行っている。本調査活動は当研究所

が主体となり実施しており、下記にその概要を説明する。

６．１．セキュリティに関する調査の目的

自動運転基準化研究所では、発足初年度である 2016 年度からセキュリティに関する調査を実施している。2016 年度の主な調査目的は、基準化の観点での自動車独自のセキュリティについて考え方を整理することであった。調査では次のような知見が得られた。自動車では、例えば鉄道や飛行機といった他の輸送機器で通常行われている物理的なセキュリティ（例えば、情報管理区域の設定やセキュリティ教育など）を設定することが難しい。従って、物理的なセキュリティを期待しない設計思想により自動車のセキュリティ対策を施すことが必要となる。一方で、最終的な車両の安全性確保（非常停止など）について配慮することも重要である。

今年度の調査では、最終的な車両の安全性確保のため、不正等による制御異常を考慮した非常停止機能について市販車両の調査の実施や、共通的な非常停止機能について調査・検討を行うこととなった。

６．２．市販車両の非常停止機能に関する調査

非常停止機能を備える車両を用い、非常停止機能の作動条件・方法及び非常停止後の車両の状態等について調査を行っている。以下には非常停止機能の作動条件に関する調査結果の概要を示す。

市販車両の非常停止機能の作動条件として、手動での作動手順について調査した。国内メーカを対象に、取扱説明書で非常停止機能の装備の記載がある車種を対象に作動方法を調査した。対象の 5 社の車両は「START」ボタンが付いており、このボタンを長押しするか連打することで非常停止機能が作動する。

一方で一部の輸入車両では非常停止機能の作動条件が異なっている。例えば図 3 の車両では、「START」ボタンが無く、車両の起動は運転席への着座がトリガとなっている。この車両では、シフトレバーの P レンジを長押しすることで非常停止機能が作動する。

図 3　「START」ボタンが無くディスプレイでの操作設定が主体の車種

このように、手動での非常停止機能の作動条件は異なっており、仮にドライバーが制御異常を把握しても非常停止に戸惑う可能性が考えられる。そのため、非常停止機能の作動条件が統一化される必要がある。

７．まとめ

WP29 において自動運転に関する議論を行う ITS/AD に新たに設置されたセキュリティに関する TF の活動状況と、これに対応する日本国内の動向について説明した。

今後は、TF の議論の取りまとめ（2017 年 12 月をめどに活動）に向け、日本の意見を反映しつつ、セキュリティに関して WP29 で扱うべき将来的な課題の明確化を進め、WP29 内の議論に反映していく。

参考文献

1） United Nations/Economic and Social Council, http://www.unece.org/fileadmin/DAM/trans/main/wp29/wp29resolutions/ECE-TRANS-WP.29-78r6e.pdf, 2017

2） United Nations/Economic and Social Council/WP29/ITS/AD/Cyber Security Task Force,https://wiki.unece.org/download/attachments/42041673/TFCS-03-04e Updated ToR clean.pdf, 2017