⑪ 自動運転車両における情報・セキュリティ分野の基準に関する活動報告

自動車安全研究部　　新国 哲也

1．はじめに

国連欧州経済委員会における自動車基準調和世界フォーラム（WP29）では、自動運転及び関連する技術について基準案の策定を進めている。優先課題として、表 1 に示す項目が掲げられている。これらの課題は、自動運転に関する専門家分科会として 2018 年に発足した自動運転技術分科会 GRVA(Working Party on Automated / Autonomous and Connected Vehicles)において検討が進められている。

表 1　WP29 における自動運転の優先課題 [1)]

課題名	概要
Functional Requirements for automated / autonomous vehicles	自動運転に関する機能要件を検討する。車両制御のみならず、安全性に対するリスク低減方策、ヒューマンマシンインターフェース等をカバーする。
New assessment / Test method	自動運転のための新しいアセスメント及び試験方法を検討する。
Cyber security and (Over-the-Air) Software updates	サイバーセキュリティ及びソフトウェアアップデートに関する基準案を策定する。
Data Storage System for Automated Driving vehicles (DSSAD：Data Storage System for Automated Driving)	自動運転に関するデータ記録装置の要件を検討する。なお、衝突による衝撃をイベントとした車両情報記録装置（EDR: Event Data Recorder）の検討も同時に進める。

本報告では、著者が議長として関わっているサイバーセキュリティ、ソフトウェアアップデート及び自動運転に関するデータ記録装置（DSSAD）について、活動の状況を概説する。

2．サイバーセキュリティに関する基準案について

専門家会議により検討されている基準案の特徴は次の通りである。

① 車両のセキュリティを確保するため、自動車メーカが取るべき組織的なルールを設定することと、そのルールが自動車メーカの組織により守られていることを認可当局が確認すること。

② 自動車メーカの組織的なルールの下に、セキュリティ方策が車両型式に適切に反映されていることを認可当局が確認すること。

・基準案が想定する適用対象と範囲：

自動車の開発やサービス等について、セキュリティを担当する組織的な主体として、サイバー・セキュリティ・マネージメント・システム（CSMS）という概念を定義している。CSMS には、製造されるプロダクツ（車両や部品・システム）そのものではなく、自動車メーカを中心とする組織が取るべき行動等に関する規定やそれを運用する仕組みが含まれる。CSMS の対象になる組織には、自動車メーカのみならず、関連するサプライチェーンなどの組織も含まれる。

・提案された基準の仕組み：

認可当局は、サイバーセキュリティに関する要件が、当該自動車メーカの組織により確実に実施されていることを確認の上、認可を行う。さらに車両型式の認可は、自動車メーカが CSMS の有効な証明書を有する状態でのみ与えられる。

・車両型式の認証について：

型式認証を受けようとする際には、自動車メーカがその時点で有効な CSMS の証明書を有することが必要となる。その上で、審査の対象になる型式の車両に適切なセキュリティ対策がなされていることを認可当局が確認する（例えば、CSMS により実施された脅威分析に基づき各装置のセキュリティ機能が設計されていることを確認する）。これにより型式が審査される。

以上、サイバーセキュリティの基準案を解説した。この基準案の特徴は、セキュリティに関する技術的要件そのものが基準とされているのではなく、自動車メーカの組織が取るべき行動に関して、基準の要件が定められている点にある。このために、進歩の早い情報技術に合わせ基準を頻繁に変更する必要はない。また、基準として個別の技術（例えば特定の暗号化技術

など）を指定することもないため、攻撃の対象が公にさらされることもない。

3．ソフトウェアアップデートの基準案について

２．で説明したサイバーセキュリティに関する基準案の特徴と同様に、ソフトウェアアップデートに関する基準案においても次の２つの段階を有するアプローチが提案されている。

①車両安全を確保するためのソフトウェアアップデートプロセス（後に説明する）を組織的なルールとして設定することと、そのルールが自動車メーカの組織により守られていることを認可当局が確認すること。

②自動車メーカの組織的なルールの下に、適切にソフトウェアアップデートが実施されるための仕組みが型式を取得する車両に備わっていることを認可当局が確認すること。

・基準案が想定する適用対象と範囲：

自動車のためのソフトウェアアップデートの仕組みに関して、ソフトウェア・アップデート・マネージメント・システム（SUMS）という概念を定義している。SUMS とは、製造されるプロダクツ（車両や部品・システム）そのものではなく、自動車メーカを中心とする組織がソフトウェアアップデートのために適用する行動等に関する規定や、それを運用する仕組みを表す。SUMS の対象になる組織には、自動車メーカのみならず、関連するサプライチェーンなどの組織が含まれる。自動車メーカは、SUMS によってどのように安全性が確保されるかについて、証明することが求められる。さらに車両型式の認可は、自動車メーカが SUMS の有効な証明書を有する状態でのみ与えられる。

・車両型式の認証について：

型式認証を受けようとする際には、自動車メーカがその時点で有効な SUMS の証明書を有することが必要となる。その上で、審査の対象になる型式の車両に適切な対策がなされていることを認可当局が確認する（例えば、安全性を確保するため、車両制御に係わるアップデートを走行中に実施できないようにする仕組みが、設計通り機能するかを確認する）。これにより型式が審査される。

・ソフトウェア照合番号の定義について

ソフトウェアアップデートのプロセスの透明化を図るため、車両に搭載されたソフトウェアと認可当局の承認内容とを照合する方法が検討された。この検討において RxSWIN（Regulation x に対する Software Identification Number）は、型式認証を受けた車載のシステムにインストールされたソフトウェア（複数のユニットにより構成されるシステムであれば、それぞれのユニットに存在する複数のソフトウェア）のバージョン情報を集約し、管理する概念として考案された。なお、ソフトウェアのバージョン管理などの運用ルールは、自動車メーカがそれぞれのシステムに応じて設定することができるとしている。

4．データ記録装置に関する基準について

DSSAD については、WP29 の GRSG(Working Party on General Safety、一般安全)専門家会議の議題であった EDR(Event Data Recorder、車両衝突をトリガとした、車両状態に関するデータの記録装置)とともに、新たに発足したインフォーマルワーキンググループ（Informal Working Group on Event Data Recorder（EDR）and Data Storage System for Automated Driving（DSSAD）、以下 IWG EDR/DSSAD とする）において、基準化の議論が開始された。

IWG EDR/DSSAD の活動方針は次の通りである。

① EDR と DSSAD の違いを明確化する

② WP29 の指示である同一車線内の自動運転機能（ALKS: Automated Lane Keeping System）に対応する DSSAD の要件を検討する

③ さらに高度な自動運転機能に対応するデータ記録要件を整理し、基準案をまとめる

①及び②の課題は、2020 年 3 月をめどに基準案をまとめるよう取り組んでいる。

5．まとめ

GRVA において、優先的に取り組まれている課題の中から、サイバーセキュリティ、ソフトウェアアップデート及び DSSAD の基準化に関する活動状況を概説した。今後も、交通安全環境研究所として積極的に WP29 の議論に参画し、基準の公平性を確保しつつ国内導入の円滑化を図っていく。

参考文献

1) United Nations/Economic and Social Council, ECE/TRANS/WP.29/2019/34”Framework document on automated/autonomous vehicles”（2019）