国連自動車基準調和世界フォーラム（WP.29）における自動車セキュリティ、ソフトウェアアップデートの議論の概要

UNECE
WP.29 GRVA-CSTF共同議長
交通安全環境研究所
新国（にいくに）　哲也（てつや）

自動車基準認証国際化研究センター
姫野（ひめの）　秀雄（ひでお）

1. はじめに

国際連合における自動車基準調和世界フォーラム（UNECE/WP.29）では、自動車の基準としてのセキュリティの課題を抽出するため、2016年12月にセキュリティタスクフォース（UN Task Force on Cyber security and OTA（Over-The-Air、すなわち無線によるアップデート）issues、以下、TFCS）が設置された。現在（2018年11月時点）、自動車のセキュリティやソフトウェアアップデートに関係する国際調和された基準の案について議論が進められている。議論の結果は、TFCSの親会議体であるGRVA：Working Party on Automated/Autonomous and Connected Vehiclesに対する提案文書としてまとめられた。この提案文書の内容を中心に、TFCSにおける議論の概要について述べる。

2. 自動車のサイバーセキュリティに関する提案文書

自動車のサイバーセキュリティに関しての提案文書は、大きく分けて2つの項目で構成されている。

・自動車のサイバーセキュリティに係わるガイダンス
・自動車のサイバーセキュリティを適用するための基準の案

以下には、それぞれの項目について解説する。

2.1　自動車のサイバーセキュリティに係わるガイダンス

自動車メーカに向けたガイダンスであり、車両の制御等に係わるデータや情報を不正に利用されないよう、車両の開発段階等において車両メーカが取るべき手段や行動指針を取りまとめている。車両の安全性を確保するために必要と考えられるセキュリティ対策を中心に示す内容となっている。

●サイバーセキュリティの原則

サイバーセキュリティの原則は、車両のライフサイクル（開発・設計、製造、使用など）の各段階において、自動車メーカが組織的に備えるべきサイバーセキュリティの手段が示されている。

組織的要件に係わる原則：

・組織的なセキュリティを確保するため、（意思決定ができ、組織全体に浸透させることが可能な）組織の最高階位においてセキュリティが管理され、また、推進される体制を構築すること
・組織としてサイバーセキュリティの監視を継続的に実施できる体制を構築すること
・組織には関係するサプライヤやサービスプロバイダを含み、その組織全体でセキュリティを維持する仕組みを構築すること

車両に係わる原則：

・自動車メーカは、データを保存、通信するために構築される構造（例えば車載のネットワークなど）において、その構成要素の1つが不正な操作を受けた場合に、他の要素や構造全体に影響を及ぼさないように車両設計を行うこと
・車両の寿命にわたり、ソフトウェアのセキュリティを考慮すること
・データの保存、転送に関してセキュリティを考慮すること
・自動車メーカは、試験などによりセキュリティの機能性を評価すること
・自動車メーカは、データの不正使用などに対応できるように車両を設計すること
・自動車メーカは、データの不正使用があったことを車両が検出し、対応できるように設計すること

以上の要件は指針であり、自動車メーカは可能な限りこれらの要件を反映した車両開発を行うことが求められる。

2.2　自動車のサイバーセキュリティを適用するための基準の案

本提案文書の特徴は、2.1節に示した指針に対し、同指針に示された要件がどのように自動車メーカにより守られているかを認可当局が確認する規定を提案していることである。この基準化に関する規定の案の概要を以下に示す。

基準案が想定する適用対象と範囲：

自動車ならびにその開発等に係わる活動に関するサイバー・セキュリティ・マネージメント・システム（CSMS）という概念が定義されている。CSMS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。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が含まれる。

提案された基準案の仕組み：

認可当局は、提案された基準の案に示された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。このため車両型式の承認は、CSMSの証明が確認され自動車メーカが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、自動車メーカはまず型式認証を受ける車両に対し、有効なCSMSの証明書によって証明された要件が適用されていることを認可当局に証明しなければならない。

以上、TFCSにより提案されたサイバーセキュリティの基準の案を含む提案文書について、概要を解説した。この提案文書の特徴は、指針に示された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によって要件が遵守されているかについて認可当局が確認する規定を基準の案として提案している点にある。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、攻撃の対象を公にさらすこともない。

3. 自動車のソフトウェアアップデートに関する提案文書

自動車のサイバーセキュリティに関する提案文書と同様に、ソフトウェアアップデートに関する提案文書も2つの項目で構成されている。

・自動車のソフトウェアアップデートに係わるガイダンス
・自動車のソフトウェアアップデートを実施するための基準の案

以下には、それぞれの項目について解説する。

3.1　自動車のソフトウェアアップデートに係わるガイダンス

主に車両の安全性に関して下記の要件を提案している。

○ソフトウェアの移送が（通信の失敗などにより）中断した場合、移送前の状態でシステムを立ち上げることが可能であること。

○移送されたソフトウェアの実行前には、アップデートの内容がドライバに通知されること。

○アップデートを実行する際に、その実行プロセスによって当該ソフトウェアの制御する機能の作動が制限される場合、特に車両の安全性に係わるような機能がこの制限を受けるような場合には、実行プロセスの間、作動不可の状態にすること。

○自動車メーカは、ユーザに対してアップデートの成否について確実に知らせること。また、アップデートにより変更された機能について、その内容をユーザに確実に知らせるとともに取扱説明書にも反映すること（この反映の方法は、本案では特に規定していない）。

OTAアップデート（いわゆる無線通信を使ったアップデート）について：

OTAアップデートについては、下記の要件を遵守することが求められる。

○ユーザによる追加的な作業（例えば運転操作以外の操作を必要とする作業）が発生するアップデートについては、運転中のOTAアップデートの実行を禁止すること。

○OTAアップデートを完了するために（一般的な車両ユーザが有さない）専門的な知識を有する技術者による何らかの作業が必要な場合は、自動車メーカは適切な技術者によりOTAアップデートを完了する措置を取らなければならない。

3.2　自動車のソフトウェアアップデートを実施するための基準の案

「自動車のサイバーセキュリティの基準案」と同様に、自動車そのものの要件だけではなく、自動車メーカによるソフトウェアアップデートの組織的な実施プロセスに関して、当局が確認できる仕組みを提案している。この基準化に関する規定の案の概要を示す。

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）という概念が定義された。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、3.1節に示された指針が自動車メーカによって設定されるSUMSによってどのように実践されるかについて、証明することが求められる。TFCSが提案する基準の案において、車両型式の認可にはSUMSの証明が必須となる。

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、自動車メーカはまず型式認証を受ける車両に対し、有効なSUMSの証明書によって証明された要件が適用されていることを認可当局に証明しなければならない。ここでは、特に型式認証を受ける車両が当該車両メーカのSUMSの上で開発・設計され、生産され、また使用段階においてもその適合性を維持できるであろうことを当局に示すことが求められる。

4. 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TFCSにより検討された。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する番号を定義する概念として考案された。なお、RxSWINを使ったアップデート対象となる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。

5. おわりに

国際連合の自動車基準調和世界フォーラム（UNECE/WP.29）における自動車のセキュリティやソフトウェアアップデート（OTAを含む）に関する基準の案について、概要を紹介した。2018年10月現在においてGRVAの参加国によりこの案のレビューが行われており、2019年1月に開催予定のGRVAの第2回会議において、内容が審議される予定である。