講演１２．サイバーセキュリティ、ソフトウェアアップデート法規におけるプロセス審査の取組

自動車認証審査部　情報セキュリティ審査センター　　※小林　一樹　　榎本　恵

１．はじめに

近年、自動車制御のソフトウェア化、無線通信の高速化に伴いコネクティッドカーの普及が進んでいる。車両外との通信によるセキュリティリスクが車両の安全性を脅かす恐れがあるため、国連の自動車基準調和世界フォーラムにおいて、自動車のサイバーセキュリティ基準が検討された[1]。その結果2020年6月にUN No.155（以降、R155）サイバーセキュリティ（以降、CS）およびサイバーセキュリティマネジメントシステム（以降、CSMS）[2]、UN No.156（以降、R156）ソフトウェアアップデート（以降、SU）およびソフトウェアアップデートマネジメントシステム（以降、SUMS）[3]が採択された。

国内では令和2年（2020年）8月に自動車の特定改造等の許可に関する省令が施行され、2021年1月にR155およびR156の要件が引用された。これらの迅速な施行により、我が国は他の1958年協定加盟国（以降、58協定国）に比べ、マネジメントシステム（以降、MS）の法規適用時期が先行した。

これを受け、交通安全環境研究所は2020年7月にMS審査を担う情報セキュリティ審査センター（以降、CSTセンター）を設立した。

２．基準概要

R155、R156はMSに関する要件と車両型式に関する要件で構成されている。

CSMSに関する要件では、管理体制、リスクアセスメント・対策、セキュリティテスト、サプライヤ管理、インシデント管理といったプロセスが自動車メーカに対して要求されている。一方、車両に対し、CSMSに基づいたリスクアセスメント、セキュリティテスト、サプライヤ管理の実施などが要求されている。

SUMSでは、SU対象のソフトウェアバージョン管理、SU対象車両の特定、SUによる相互依存性・互換性などの確認、運転中のSUの安全性確認といったプロセスが要求される。また、車両要件にはSUMSに基づいて管理されたソフトウェアだけが更新され、無線通信によるSUが正しく、安全に実施される仕組みであることなどが定められている。

CSMS、SUMSともに認可後の有効期限は3年であり、自動車メーカは、要求されるプロセスが維持されていることを3年おきに審査される。

R155、R156の要件は、明確なクライテリアが存在しない。サイバー攻撃手法、ソフトウェア更新のための通信技術などは進化し続けることから、対策の正解を定めることができないためである。よって、要件適合性の評価は、各認可当局が判断することとなる。そのため、各認可当局の判断に差が出る可能性がある。そこで、インフォーマルグループで要件および要件のエビデンスの明確化を目的とした解釈文書[4,5]が作成された。さらに、R155においては、認可当局はCSMSの判定基準を国連のデータベースへアップロードすることが要求されており、58協定国間で情報共有が可能な制度となっている。

３．国内の取組

国内では、2019年6月から自動車基準認証国際化研究センターにおいて、CS/OTA国内採用ワーキングが開催され、官民においてR155、R156の要件の共通理解を図り、結果を審査マニュアルとしてまとめた。CSMS、SUMSの審査マニュアルには、要求されるプロセスに含むべき手順、アウトプットの概要、提出書面などが記載されている。

また、R156のSUMSが要求する一連のプロセスの実行結果である市場の車両へのSUは、国内において特定改造と定義し、事前許可制度を定めている。

４．CSTセンターの取組

４．１．プロセス審査への準備

CSMS、SUMSの認証審査では、自動車メーカの組織において、R155、R156が要求するプロセスが体系

的に構築され、運用されていることを確認する。一般的にプロセスとは、インプットから意図した結果を生み出す、相互に関連する一連の活動と定義され[6]、その活動とは、インプット、作業の手順とその条件、手順通り実施するための教育、アウトプットの確認、必要に応じた処置である。プロセスを適切に管理することにより、製品がニーズを満たすことをプロセス保証といい、これを有効にするためにはプロセスを分解し、プロセス保証の連鎖を実現する必要があるとしている。

これらのことから、CST センターでは、CSMS、SUMS プロセスの分解能は、自動車メーカの組織構成に依存することが想定されるため、一つの部門が実施または管理する範囲と考えた。さらに R155、R156 の解釈文書にはプロセスに含むべき事項が挙げられているため、これらを分析し、網羅されるよう要件ごとにチェック項目を定め、これを用いて申請者の提出書面から、プロセスの構築状況を確認した。

また、プロセスの実在と運用は申請者へのインタビューで確認することとした。分解されたプロセスの実際の活動と、プロセス間の関連性を質疑応答した。R155 の解釈文書には、認証機関への要件のひとつに、ISO/IEC 27001 への準拠が挙げられている。そのため、CST センターでは、2019 年にこの認証を受け、その際の経験が MS 審査の参考となった。

4．2．MS 審査を終えて

書面審査においては、申請者の書面にチェック項目が明文化されている場合は問題がないが、前後のプロセスやシステムにより手順やプロセスが暗黙知となっている場合や自動化されている場合の要件確認に時間を要した。CST センター内でのレビューを重ね、不明点を申請者に問い合わせ、理解を深めることで解決した。

審査対象となった自動車メーカの多くは、CSMS は ISO/IEC 21434、SUMS は ISO/IEC 24089 に準じ、各社の特徴をふまえたプロセスを構築していた。

4．3．これからの取組

CSMS、SUMS の初回審査では、プロセスを構築した後、そのプロセスに基づく車両開発を予定している自動車メーカも少なくなかった。よって、継続審査では、プロセスの継続的な実施の確認に重点を置く。また、MS の PDCA サイクルが回っていることを確認するため、プロセスの変化点をチェック項目に追加する予定である。

5．今後の課題

CSMS、SUMS の基準はプロセス保証の考え方をふまえ、プロセス要件を定義している。これは、車両型式に対する要件のみを定めた従前の UN 規則と大きく異なる点である。プロセスを要件としている理由として、サイバーセキュリティ、無線通信の技術は日進月歩であり、車両に搭載すべき軽減策および、SU システムが定められないからである。

同様に、車両に搭載する機能が特定できないケース、例えば、機械学習により振る舞いを決定するシステムについても、プロセスを要件とすることが妥当である。

このほか、振る舞いは有限であるものの、機能が作動する条件が多岐に渡り、全てのケースを型式認証時に確認することが非効率である場合もプロセス審査の有効性が認められる。

自動車の技術が多様化する中で UN 規則にプロセス要件が増え、車両そのものに対する認証試験だけでなく、車両が開発されるプロセスに対する審査が増えていくことが想定される。そこで、自動車認証審査部では、CSMS、SUMS におけるプロセス審査のノウハウを他分野の認証試験に生かしていけるよう教育、情報共有を進めていく。

参考文献

1) 新国 哲也, “国連自動車基準調和世界フォーラム(WP29)における自動車のサイバーセキュリティ基準の解説”, 自動車技術会論文集, Vol.52, No.1,pp. 208-212（2021）
2) ECE/TRANS/WP.29/2020/79, UNECE WP.29 181st (2020)
3) ECE/TRANS/WP.29/2020/80, UNECE WP.29 181st (2020)
4) WP.29-182-05, UNECE WP.29 182nd (2020)
5) WP.29-182-06, UNECE WP.29 182nd (2020)
6) JSQC Std 21-001:2015, “プロセス保証の指針”, 日本規格協会（2015）