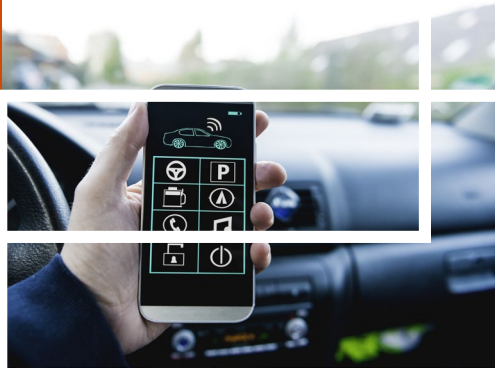
WP29への対応
自動運転車のサイバーセキュリティ(1)
UNECE WP29 GRVA(サイバーセキュリティ・ソフトウェアアップデート法規基準)とは



PwC コンサルティング合同会社　マネージャー
井上　雄介

はじめに

先ごろ発行したレポート『車両サイバーセキュリティの未来』で伝えるように、車両のデジタル化の進展によって、自動運転車の実現が近づいています。自動運転車の実用化は、ネットワークを活用した高度な自動車走行制御や、自動車に搭載されたソフトウェアのアップデート技術などによって可能となりつつあり、全世界で人の移動や物流などの大変革が迫ってきています。

自動運転機能の安全性を担保する上では、OTA(Over-The-Air)と呼ばれる無線通信を経由したデータの送受信の技術を使用して、ソフトウェアを適時にアップデートすることなどが想定されています。これは通信機能を有するがゆえに、サイバーセキュリティ対策や、ソフトウェアアップデート規格の在り方が重要となってきます。

自動車は国際的な取引によって流通する製品であり、各国基準の調和が取れない状況になってしまうと、個々の国の仕様に合わせた車両の開発が生じ、自動車OEMやサプライヤーの負担が増大することや、高い安全性能を持った自動運転車が普及しづらくなることが考えられます。

これらに対応するために、国連欧州経済委員会(United Nations Economic Commission for Europe)の「自動車基準調和世界フォーラム(WP29)」の分科会「自動運転(GRVA)」ではサイバーセキュリティ専門家会議が行われ、自動運転車の基準の策定や、国家間で認証の相互承認を行うためのサイバーセキュリティ・ソフトウェアアップデート法規基準が検討されています。日本は英国と共同で、専門家会議の議長を務めています。

本連載ではWP29 GRVAにおけるサイバーセキュリティとソフトウェアアップデート法規基準を題材として、今後、自動車OEMとサプライヤーに実施が求められる施策を紹介していきます。

第1回目はWP29 GRVAの組織の概要、同組織が策定する法規基準の全体像と押さえるべきポイントなどを把握していきます。

自動運転車のサイバーセキュリティとソフトウェアアップデート法規基準の検討について

自動運転車のサイバーセキュリティとソフトウェアアップデート法規基準の検討は前述の通り、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の分科会であるGRVAのサイバーセキュリティ専門家会議にて行われています。サイバーセキュリティ専門家会議には、日本や英国、EUなど16か国と1地域の政府代表者や、国際自動車連盟(FIA)、米国自動車技術者協会(SAE)などの業界団体、自動車関連会社が参加しています。

GRVAは自動車の装置ごとの安全や公害に関する基準の統一および相互承認の実施を目的としており、1958年にジュネーブで作成された「車両等の型式認定相互承認協定」の枠組みの中で、自動運転車のサイバーセキュリティ・ソフトウェアアップデート法規基準を検討しています。本法規基準に準じた車両の相互承認を行いたい協定締約国は、法規基準の内容をそれぞれの国の法規へ落とし込むことが求められます。

日本では2020年4月に、自動運転車に対応した改正車両法が世界に先駆けて施行されました。改正車両法では、WP29 GRVAで議論中のCS(Cyber Security)・SU(Software Update)規則が反映されており、今後CS規則とSU規則が正式に発効された際には、その差分が国内へ導入されます。

法規の変更によって自動車OEMに求められる4つの対応

自動車に関する従来の法規とWP29 GRVAにおけるサイバーセキュリティ・ソフトウェアアップデート法規基準を比較すると、4つの大きな違いがあります。自動車OEMやサプライヤーに求められる対応を以下にまとめます。

1. 車両の型式認可に先立ち、型式認可を取得したい車両のサイバーセキュリティやソフトウェアアップデートを常に適切な状態にできるマネジメントシステムを有している組織であるか、認可を受けることが義務化されます。これをプロセス認可と呼び、認可取得後も3年に1回の更新が必要となります。
2. .従来からの車両製造タイミングで行われる型式認可に加え、開発・部品調達・生産・使用など車両のライフタイム全般において、サイバーセキュリティと適切なソフトウェアアップデートを確保することが義務付けられます。
3. サイバーセキュリティについては、各部品を製造するサプライヤー、通信関係のサービスプロバイダー、アフターマーケットまで管理する体制が求められます。
4. サイバーセキュリティのプロセス認可においては定型的な審査方法と定量的な審査基準が存在しないため、自動車OEM／サプライヤーはサイバーセキュリティ対策が網羅的に行われていることを証明することが必要になります。

これら法規の変更は、進化する攻撃者に対応し、安全な自動運転機能を提供し続けることを目的としています。

サイバーセキュリティとソフトウェアアップデートの2つのマネジメントシステム

自動車OEMが車両の型式認可に先立ち対応しなくてはならないプロセス認可においては、2つのマネジメントシステムが審査の対象となります。それがCSMS（サイバーセキュリティマネジメントシステム）とSUMS（ソフトウェアアップデートマネジメントシステム）です。

CSMS

産業用オートメーションおよび制御システムを対象としたセキュリティを管理する仕組みであり、認証にはプロセスとプロダクトの2つの観点での認証が必要となります。プロセス面では、認証当局（日本においては独立行政法人自動車技術総合機構の交通安全環境研究所が該当）により、自動車OEMのサイバーセキュリティ体制や仕組みの認証と監査が3年ごと（初期）に行われる予定です。プロダクト面では、認証されたプロセスに従って車両が開発・生産されていることの実証が求められます。これらの審査に適合することでCSMS適合証明書が得られます。

SUMS

自動車のソフトウェアアップデートを管理する仕組みであり、こちらもプロセスとプロダクトの2つの観点での認証が求められます。プロセス面では認証当局により、セキュリティを考慮したソフトウェアアップデートの仕組みやソフトウェアのバージョン管理の識別子であるRXSWINなどが求められます。プロダクト面では、認証されたプロセスに従い車両が開発・生産されていることの実証が同じく求められます。これらの審査に適合することでSUMS適合証明書が得られます。

自動車OEM／サプライヤーの認可取得における変化と影響

	主な変更内容	自動車OEM／サプライヤーへの主な影響
1	従来の型式認可に加え、サプライヤーを含むバリューチェーン全体を対象とした組織としての認可取得が求められる	自動車OEM／サプライヤーの認可取得対応工数が増大する
2	車両のライフタイム全般でCS／SU を適切に維持することが求められる	自動車OEM／サプライヤー共に、販売した後もCS環境変化への対応工数が発生する
3	自動車OEMが、サプライヤー、サービスプロバイダー、アフターマーケットの管理責任を負う	自動車OEMの管理責任と管理工数が増大する
4	認可取得にあたっての定量的な基準と定型的な審査方法が存在しなくなる	自動車OEM／サプライヤーはCS環境変化に合わせ、認可取得時の対応を進化させる必要がある

お問い合わせ

PwCコンサルティング合同会社
〒100-6921　東京都千代田区丸の内2-6-1 丸の内パークビルディング
Tel : 03-6250-1200（代表）　Mail : jp_cyber_inquiry@pwc.com