効率的なサイバーセキュリティ対応に向けたポイント

（大野）

昨年末 12 月 25 日に国土交通省より、自動車サイバーセキュリティに関する重要な方針が示されました。具体的には、これまで自動運転機能を備えた自動車に限定してきた自動車サイバーセキュリティ関連レギュレーション（UN-R155，156）の適用範囲を、国内で登録される全ての車両に拡大するというものです。適用拡大のタイミングは無線ソフトウェアアップデート機能の有無によって異なり、下表のタイミングでそれぞれレギュレーションへの適合が必須となります。サイバーセキュリティに対する自動車業界の関心は近年急速な高まりを見せていましたが、今回の発表をもっていよいよ、日本においても「まったなし」の状況になったと言えます。

	新型車	継続生産車
無線 SU 対応車	2022 年 7 月以降	2024 年 7 月以降
無線 SU 非対応車	2024 年 1 月以降	2026 年 5 月以降

さて、国際レギュレーション UN-R155, 156 への適合を目指す場合、各レギュレーションに対応した国際標準をガイドラインとして活用するのが早道です。今回は UN-R155 の参照先である ISO/SAE 21434 に対応したサイバーセキュリティ管理システムの効率的な構築に向けて気をつけて欲しいポイントについてお話したいと思います。

レギュレーション適合の期限が目前に迫ったこの状況で最も避けなければならないことは、要求の本質、全体像を把握しないまま、規格に記載された個別の要求事項を局所的、表面的に満足しようとすることです。このような取り組み方は現場に不要な混乱を招いたり、開発の効率を大きく低下させたりする場合があります。ISO/SAE 21434 は、例えば PSIRT のような新しい取り組みを要求する一方で、品質管理や機能安全など組織によっては既に整備されているか改善が進行している領域に関係する要求も多く含んでいます。

例えば、ISO/SAE 21434 Clause.5「全体的なサイバーセキュリティ管理」および Clause.6「プロジェクト依存のサイバーセキュリティ管理」の要求を満足しようとする場合、IEC 62443 や ISO/IEC 27001 に従った情報セキュリティ管理システムは新たに整備しなければならない場合がありますが、ISO 9001 および IATF 16949 に準拠して整備した品質管理システムが既にあれば、要求の多くがこの品質管理システムによって満たされます。また、組織標準プロセスの整備という観点でも、組織標準プロセスそのものが ISO/SAE 21434 に準拠したものになっているかを独立的に監査する仕組みは新たに構築しなければならない部分ですが、過去に ISO 26262 への対応として Automotive SPICE のプロセスモデルを活用して整備した組織標準プロセスがあれば、その枠組みはサイバーセキュリティ対応プロセスの整備に大いに役立ちます。こうした領域においては既存の仕組みを最大限活用したり、効果的に連携したりすることが、スムーズなサイバーセキュリティ対応のカギとなります。

弊社では、2021 年 2 月 26 日に「サイバーセキュリティ概論トレーニング」の開催を予定しています。ISO/SAE 21434 の個別の要求事項の詳細について掘り下げる前に自動車サイバーセキュリティの全体像や、関連規格との関係をつかんでおくには最適なトレーニングとなっておりますので、ぜひ参加ご検討いただければと思います。

2021/2/8 大野 貴正