車両サイバーセキュリティの未来（1）

国際標準規格「ISO/SAE21434」からの示唆

PwC コンサルティング合同会社　マネージャー
奥山 謙

はじめに

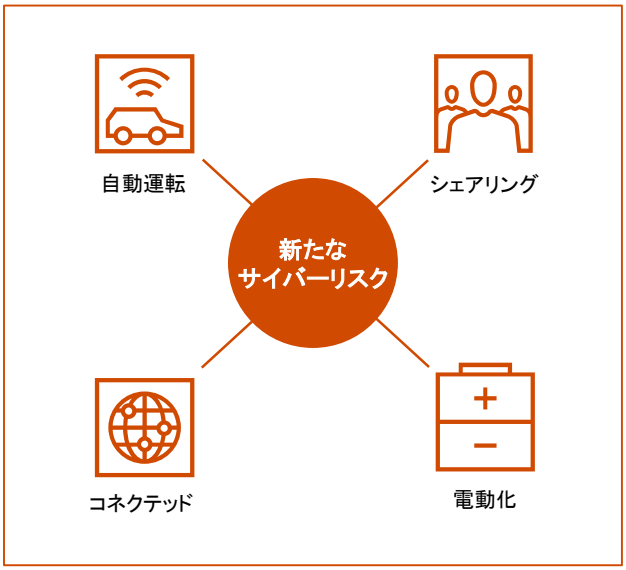
Strategy&デジタル自動車レポート2018が伝えるように、車両のデジタル革命によって、新たなモビリティ社会が夜明けを迎えつつあります。利用者が求める利便性と、実用化されつつあるCASE（コネクテッド、自動化、シェアリング、電動化）技術が提供するサービスとの間のギャップも小さくなっており、次世代のモビリティ社会が形作られています。一方、モビリティ社会の変化は必ずしも技術の進化のみで決定されておらず、各国の政策や規制により変化の速度が決定されている面があります。その要因の一つがサイバーセキュリティへの懸念です。

近年よく言われるように、車がネットワークにつながることで利便性が向上してきましたが、同時にサイバー攻撃の脅威にさらされるようにもなりました。このことは自動車メーカー・自動車部品サプライヤーでは課題として既に認識されており、特に車両開発の場面で、サイバーセキュリティ対策活動が実施されています。また、 さまざまな団体から車両サイバーセキュリティに関する指針やガイドラインも公開されています。国際的な動きとして特に重要なものが、自動車基準調和世界フォーラム（WP29）と、本連載の題材である国際標準規格のISO/SAE 21434です。

WP29は、国連欧州経済委員会（UN/ECE）の下にあり、専門分科会にて車両サイバーセキュリティに関する検討が進められており、サイバーセキュリティ対策のRegulation（義務化）も検討されています。ISO/SAE 21434では、路上を走行する車両および車両のシステム・部品・ソフトウエアと車両からネットワークでつながる外部デバイスまでを対象とした、サイバーセキュリティ対策の 管理・実施が規定される見込みです。任意規格ですが、 義務化が検討されているWP29に参照されるため、業界へ大きな影響を与えます。

このようなサイバーセキュリティ対策の義務化・標準化によって、事業者には追加のセキュリティ施策の実施が求められる可能性があります。サイバーセキュリティ施策は、利用者の安全性確保の観点では必須ですが、やみくもにサイバーセキュリティ施策を実施してしまうと、車両・モビリティサービスの価格高騰やリリース遅延など、利用者への不利益も発生し得ます。そのため、 国際標準規格などで求められるサイバーセキュリティ施策を正しく理解した上で、効果と効率をともに最大化し、実施を進めることが重要です。

本連載では、ISO/SAE 21434を題材として、今後実施が求められるサイバーセキュリティ施策をひもといていきます。第1回はISO/SAE 21434が規定するサイバーセキュリティ活動の全体像を把握していきます。

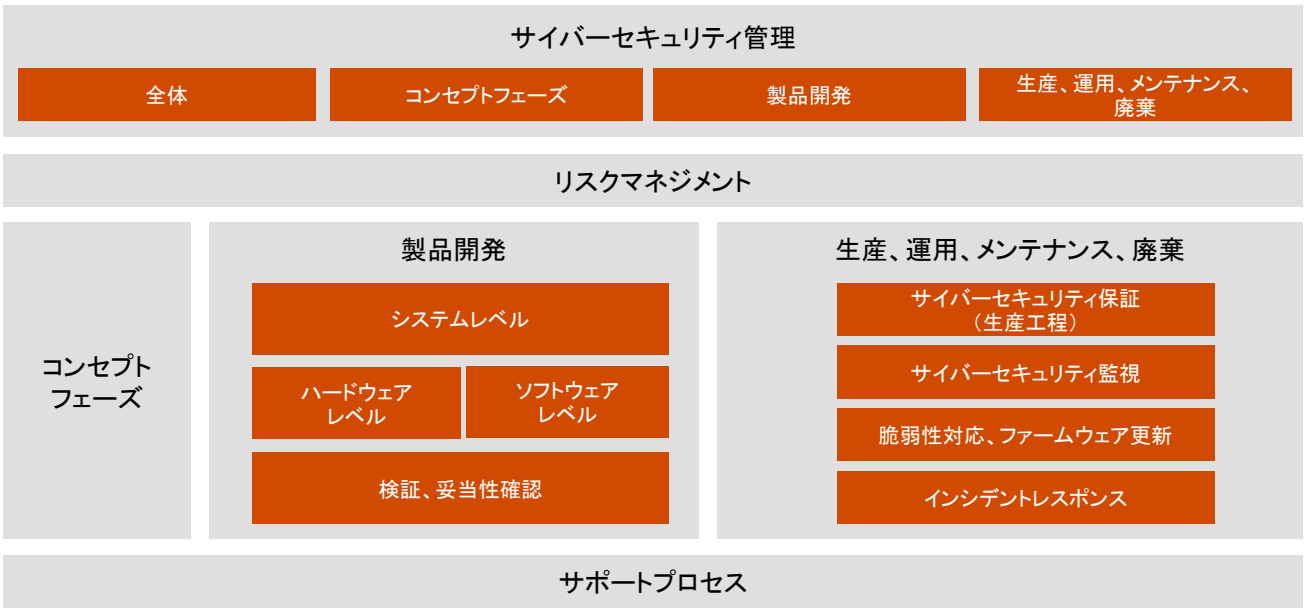


規格が技術革新の道しるべに

ISO/SAE 21434は、車両のライフサイクル全体を通じてサイバーセキュリティ活動に関するプロセスを定義することを目的としています。車両のライフサイクル全体とは、車両の企画・研究から始まり、設計・実装・検証を経て、製造・ 出荷され、市場にて運用・廃棄されるまでの、車両の開発・ 運用に関する全ての活動を意味しており、その全ての活動においてサイバーセキュリティの取り組みを実施することが必要となります。このようなプロセスにより、サイバー攻撃や、攻撃による被害の発生リスクを減らすことが期待されています。ISO/SAE 21434は、大きく分けると次の6つの要素から構成されます。

1. Management of Cybersecurity（サイバーセキュリティ管理）：サイバーセキュリティに特化もしくは重点を置いた、ライフサイクル全体を通じたセキュリティ対策の実施を確かなものとする管理活動の規定
2. Risk Management（リスクマネジメント）：いわゆる一般のリスクマネジメント手法をベースとして、セキュリティリスクを分析・算定・対応するための活動の規定
3. Concept Phase（コンセプトフェーズ）：車両開発におけるコンセンプトフェーズにて実施するサイバーセキュリティプロセスおよび活動の規定
4. Product Development（製品開発）：車両開発時において既存の開発プロセス・活動に対して、追加される サイバーセキュリティプロセス・活動の規定
5. Production, Operation, Maintenance, Decommissioning（生産、運用、メンテナンス、廃棄）：製品開発後の製造および、出荷後の運用時に実施 すべきサイバーセキュリティ活動の規定
6. Supporting Process（サポートプロセス）：その他の一般的なサイバーセキュリティ活動の規定

次回以降は、上記のサイバーセキュリティ活動のうち実施時に注意を必要とする事例を取り上げて、活動の進め方について考察します。



出所：以下資料より引用し、PwCにて翻訳（2019年4月時点）
Status of Work in Process on ISO/SAE 21434 Automotive Cybersecurity Standard <https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1525889601.pdf>

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