ハイライトレポート

2025. 7. 15

SDV世界戦　加速する世界、日本の現在地
――鍵を握るセキュリティ・コネクティビティ技術とは
Day2: SDV時代の車載セキュリティ

SDV車両に対するサイバー攻撃の危険性

昨今、自動車業界は急速に進化し、ソフトウェアによって車両の機能を制御するSDVに移行しています。その為、経済産業省と国土交通省が推進するモビリティDX戦略においても、SDVが注目されています。SDVでは、常時クラウドに接続する事で、無線によるアップデート（OTA）を通じて、最新機能の追加できるなど、利便性の向上が見込めます。一方で、インターネットへの接続が前提となる為、サイバー攻撃のリスクも飛躍的に高まります。

本ウェビナでは、SDV化に伴うサイバー攻撃によるリスクと、その対策となる基礎的なセキュリティ機能についてご紹介致します。

SDV化によって想定されるリスク

SDV化により車両をソフトウェアによって制御する事で利便性が向上します。一方で、ソフトウェアに異常が発生した場合、車両の制御に支障をきたし、人命に関わる重大な事故につながる可能性があります。また、ネットワークに常時接続されている為、侵入経路が増加し、サイバー攻撃のリスクが高まります。その為、定期的な脆弱性診断や、迅速なアップデートが必要になります。特にSDVの中核技術であるOTAによるソフトウェア更新では、更新用ファイルの偽装や改ざん、V2X通信によるデータの傍受など様々な攻撃手法が考えられます。

SDVにおけるセキュリティ対策

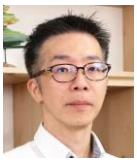
車載セキュリティにおける対策は、単一の技術では不十分であり、多層的かつ包括的なアプローチが求められます。攻撃対象領域の拡大やサプライチェーンの複雑化など、様々な要因から実現は難しいものの、車両の安全は人命に直結する為、堅牢なセキュリティシステムを構築する必要があります。守るべき対象としては、OTAアップデート中のソフトウェア、V2Xなどの通信経路における情報、車両システムそのもの、そしてユーザーデータなどが挙げられます。これらに対して、電子署名による正当性検証や、HSMによる暗号鍵の保護、TLSによる秘匿通信など様々な対策が想定されます。

OTAアップデートの対策と各種機能

OTAによるソフトウェアアップデートは、継続的に脆弱性の対策を可能にします。しかし、アップデートの過程でソフトウェアに偽装や改ざんが行われると、重大なセキュリティインシデントに繋がる為、十分な対策が必要です。具体例として、アップデート対象が正当なソフトウェアか検証する電子署名や、起動時に正当なソフトウェアかを検証するセキュアブートがあります。また、上記の検証やデータの暗号化に必要となる暗号鍵を保護するHSMも重要です。

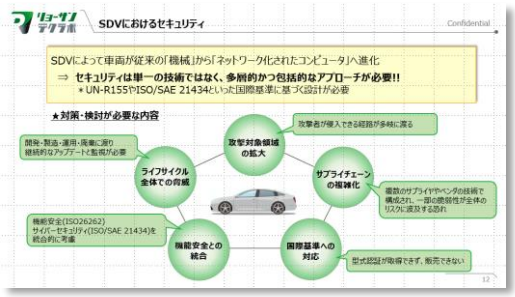
Renesas社では、HSMを搭載した車載向けSoCやMCU製品を提供しており、SDVが求めるサイバーセキュリティ要件に対応しています。製品に関するご質問がございましたら、ぜひお気軽にお問合せ下さい。

■ 本日の登壇者 ■



デバイス第一事業本部
技術支援部　第二課
澁澤 義隆

SDV化によって想定されるリスク
出所：投影資料より一部抜粋



SDVにおけるセキュリティ
出所：投影資料より一部抜粋