

## 認証取得の糸口に、競合他社との差別化に、ぜひお役立てください！

近年、自動車サイバーセキュリティに関しては、UN-R155やISO/SAE2143などの国際的な法令・規格の発効が続き、存在感が増す一方で、実務的には「車載OEMから具体的な要求が出てこない」「規格でも設計要件等は具体化されていない」など、手の付け所にお悩みの方も多いようです。

本ウェビナでは3名のエキスパートをお招きし、自動車サイバーセキュリティの概要を始め、ISO/SAE21434の要点と認証プロセス、実践的な内容としてハードウェア部品選定のポイント・生産工程における暗号鍵書込みの重要性をご説明します。

## 自動車セキュリティの転機

自動車制御にネットワークが組み込まれるようになって日は長いですが、これまで車載ネットワークはクローズドされた環境という事もあり、遠隔からのサイバー攻撃は、現実的な脅威として捉えられていませんでした。

**第1の転機**は、大学研究者によって報告された車載ネットワークを介した車両操作の実証です。これを受けて、各国で対策技術の開発や、ガイドライン発行等が進められました。何をどの程度実施すればよいか不明瞭な状況が続きました。

そうした中で**第2の転機**となったのが、2015年のJeepのハッキング報告です。Jeepが遠隔操作できることを実証しました。事前通告を受けたChrysler社は該当の140万台をリコールするに至りました。脆弱性の一つはセルラーネットワーク側の設定ミスでしたが、**業界に与えた影響は甚大**でした。

ここから自動車サイバーセキュリティにおける活動が各方面において一斉に動き出すことになりました。

## 法規制と規格

第2の転機以降、国際規格の策定、国連規則の制定が始まりました。国連協定規則UN-R155は2021年1月に発効になりました。国際規格ISO/SAE 21434も同じ年に発行されました。ISO/SAE 21434で規定する要件は、UNR155の解釈文書から多く参照されています。

UN-R155は日本においてもいち早く国内法規へ反映され、今はOEMの、3年毎の適合証明更新の時期に差し掛かっています。今後、サプライヤに対しては、より厳密な対応が求められることが想定されます。

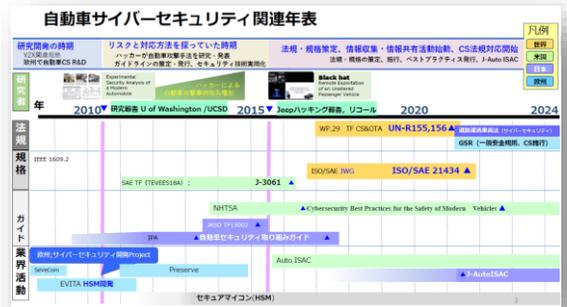
また、日欧等の58協定国以外では、世界各国でセキュリティ要求は異なり、その点についても解説しました。

### ■ 本日の登壇者 ■



一般財団法人 日本自動車研究所  
伊藤 寛 氏

新モビリティ研究部



自動車サイバーセキュリティ関連年表

出所：投影資料より一部抜粋

[他のウェビナはこちらから](#)

リョーサンウェブサイト

