自動車のサイバーセキュリティ認証にかかわる支援サービス

CSMS/SUMS認証およびCS/SU (OTA)車両型式認証にかかわる支援
UN-R155/R156とISO/SAE 21434に対応

コネクテッドカーとセキュリティリスク

高度自動運転支援など先端技術の導入に伴い、自動車はますますデジタル化され、多くの電子機器やソフトウェアが搭載されています。車載マイクロコントローラの数は最大150に達し、ソフトウェアは1億ステップが実装されています。2030年までにソフトウェアは、3億ステップに達すると予測されており、急激な発展が見込まれています。

出典：ウェブサイトUNECE Press Release, published on 25 June 2020

自動車に搭載されたワイヤレス機器と外部環境を接続するIoTの普及により、自動車産業においてもサイバーセキュリティの確保は重要な課題であり、システムの管理と構築を運用することが非常に重要となります。

自動車のサイバーセキュリティ国際標準の全体像

こうした高度化された自動車のセキュリティ確保に向けて、自動車のサイバーセキュリティ国連規則 UN-R155 / R156 が2020年6月にUNECE WP29で合意されました。
EUでは、2022年7月以降の新型車両型式は、UN-R155「車両のサイバーセキュリティとサイバーセキュリティ管理システム（CSMS）」およびUN-R156「車両のソフトウェアアップデートとソフトウェアアップデート管理システム」に適合することが要求されます。また、2024年7月からは全ての新車両に適用されます。

自動車のサイバーセキュリティ認証にかかわる支援サービス

テュフ ラインランド ジャパンは、認証取得を目標にした技術支援サポートをはじめ、認証継続取得のためのゴール設定や各国市場への適合支援など、さまざまなサービスを提供します。また、テュフ ラインランドはEUの各当局よりテクニカルサービスとして指定を受けているため、この知識と経験を生かした支援を一貫した体制で提供することが可能です。

■ サイバーセキュリティ適合ギャップ分析

- UN-R155/R156および ISO/SAE 21434 に対応した、車両の開発段階から開発完了後の段階までを網羅したサイバーセキュリティライフサイクルのギャップ分析を実施し、認証取得に向けた問題点を明確にします。

■ 支援サービス

- 検証（verification）、監査、アセスメントの実施。
  UN-R155/R156のCSMS/SUMS認証取得に必要な開発初期から生産終了後の市場監視プロセスに対して行います。
- 各種技術的な対策の適合評価（UN-R155 附則5のリスク軽減策の評価など）。
- サイバーセキュリティ作業成果物の評価。
  ISO/SAE 21434に対応した、車両のライフサイクル全般の作業成果物を確認します。
- CSMS/SUMS認証につながる事前審査など。
- 要求事項の当局解釈についての確認および説明。

■ トレーニング

- CSトレーニング～基礎編、CSワークショップ、CSエンジニア認定コース（2021年3月以降開始予定）。

公平性の確保
テュフ ラインランドは、第三者認証機関としての公平性、客観性については、管理策に基づき対応します。

www.tuv.com

TÜVRheinland®
Precisely Right.

UN-R155について

UN-R155は、試験方法や合否基準等が規定されておらず、サイバーセキュリティへのリスク回避や低減を確実にすることが困難です。技術が進歩するなかでも、最善策を適用していることを証明することが、製造業に求められます。
UN-R155規則は、大きく以下の2つの要件から構成されていて、これらの要件について型式認証として認可当局またはテュフ ラインランドのようなテクニカルサービスによる確認が要求されます。

1. 車両型式要件

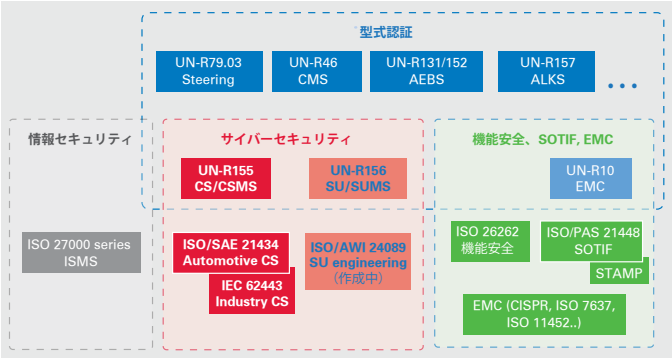
- 文書監査と車両テスト（サプライチェーン含む）
- 車両製造者への要求

2. サイバーセキュリティ管理システム（CSMS）およびソフトウェアアップデート管理システム（SUMS)の要件

CSMSの認証を取得するためには、主に以下のポイントに対応することが重要です。

- ライフサイクル全般を網羅するCSMS
- リスク低減策を考慮したプロセスの構築
- 脅威や脆弱性について時間内に軽減できるプロセスの構築
- 継続的な監視プロセスの構築
- サプライチェーンでの管理プロセスの構築

サイバーセキュリティの法規制と標準の関係



ISO/SAE 21434について（適合の必要性、背景など）

ISO/SAE DIS 21434「車両のサーバセキュリティエンジニアリング」は、自動車のサイバーセキュリティ国際規格として、2020年2月に発行されました。ISO/SAE 21434は、CSMSのプロセス構築に有効であり、ライフサイクル全体での適合やサプライチェーンでのセキュリティ対策が規定されています。
また、車両のリスク評価としてUN-R155の附則5にあるリスク低減策に対しても有効なガイダンスとして活用できます*。

*ISO/SAE 21434 ではカバーされていない、車両外部のリスク低減などについては別途対応が必要です。

ISO/SAE DIS 21434版の主な項目

1. サイバーセキィリティ管理
2. 継続的なサイバーセキュリティ活動
3. リスクアセスメント手法
4. コンセプトフェーズ
5. 製品開発フェーズ
6. 開発完了後フェーズ
7. 分散サイバーセキュリティ活動

ISO/SAE 21434に準拠したプロセスのアウトプット（作業成果物）は、市場でサイバーセキュリティのインシデントが発生した場合に、最善を尽くした証拠として必要になります。さらに生産中および生産終了後のフェーズにおいても、サイバーセキュリティに関連するインシデントを監視し、適切に対応するプロセスを構築することも要求されています。
例：PSIRT: Product Security Incident Response Team

お問い合わせ
テュフ ラインランド ジャパン株式会社
モビリティ事業部　営業 柏木貴志
Tel: 045-470-1860
takashi.kashiwagi@tuv.com
www.tuv.com

TÜVRheinland®
Precisely Right.