インド経済

自動車におけるサイバーセキュリティ規制の動向

2022 年 11 月

1. はじめに

2015 年、米 FCAUS（旧クライスラー）は、米国内でハッキング対策のため 140 万台をリコール（回収・無償修理）すると発表した。これは、クライスラーが使う専用無線回線「U コネクト」から車の頭脳であるコンピューターにハッカーが侵入して、外部からエンジンを切ったり、ワイパーを動かしたり、あるいは、遠隔操作でハンドルを動かしたり、加減速させたりできるリスクが発覚したためであった[1]。

ICT（情報通信技術）端末を搭載した自動車であるコネクテッドカーが普及するにつれて、利便性は高まる一方で、自動車がインターネットに常時接続されることにより、サイバー攻撃を受けるリスクも同時に高まっている。

本ニュースレターでは、世界における規制の動向を紹介した上で、その中でのインドの規制の動向について説明する。

2. コネクテッドカーの概要と現状

日本の総務省平成 27 年版情報通信白書[2]によると、コネクテッドカーとは、ICT 端末としての機能を有する自動車のことである。車両の状態や周囲の道路状況などの様々なデータをセンサーにより取得し、ネットワークを介して集積・分析することで、新たな価値を生み出すことが期待されている。具体的には、事故時に自動的に緊急通報を行うシステムや、走行実績に応じて保険料が変動するテレマティクス保険、盗難時に車両の位置を追跡するシステム等が実用化されつつある。

- 緊急通報システム

緊急通報システムとは、事故発生を検知した場合や緊急通報ボタンが押された場合に、自動的に緊急通報センターに通報する制度である。緊急通報センターのオペレーターは、運転手と会話ができる場合は、会話を通じて状況を把握し対応する。これに対して、運転手と連絡が取れない場合には、位置データや車両データを警察や消防へ送信する。欧州では 2018 年 4 月より「eCall」、ロシアでは 2017 年 1 月より「ERA-GLONASS」として、それぞれ車両への搭載が義務付けられている。このうち「eCall」の仕組みを簡単に紹介すると、「eCall」では、車両事故を検知した場合に、自動的に欧州緊急番号 112 発信が行われる。緊急電話は緊急通報センターにつながり、車両の位置情報を含む事故の詳細が送信される。車両の位置情報を把握する

---

[1] 「クライスラー、ハッキング対策で 140 万台リコール」日本経済新聞、2015 年 7 月 25 日
https://www.nikkei.com/article/DGXLASGM25H19_V20C15A7MM0000/

[2] 「平成 27 年度版情報通信白書」総務省
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h27/html/nc241210.html#:~:text=%E3%82%B3%E3%83%8D%E3%82%AF%E3%83%86%E3%83%83%E3%83%89%E3%82%AB%E3%83%BC%E3%81%A8%E3%81%AF%E3%80%81ICT,%E3%81%8C%E6%9C%9F%E5%BE%85%E3%81%95%E3%82%8C%E3%81%A6%E3%81%84%E3%82%8B%E3%80%82

ために Galileo と呼ばれる欧州の GPS が使用されている。こうした情報を受領したオペレーターにより適切な支援が行われる。

- テレマティクス保険

「テレマティクス」とは、テレコミュニケーション（通信）とインフォマティクス（情報科学）を組み合わせた造語である。テレマティクス保険では、車両の位置データや運転手の走行データ（速度、燃料使用量、走行距離、走行時間、ブレーキのかけ方、エンジンデータ）などを取得・分析し、保険会社はそこから算出された運転のリスクを保険料に反映する。その結果、安全運転をしている者の保険料は低くなり、危険な運転をしている者の保険料は高くなるという仕組みである。

- 盗難車両の追跡システム

盗難車両の追跡システムとは、車両の盗難に遭った時に自動的に車両を追跡するシステムである。例えば、トヨタ自動車は「マイカーSecurity」[3]というサービスを提供しており、ドアのこじ開けや車内侵入が起きた場合、「My TOYOTA+（携帯アプリ）」に「アラート通知」をしたり、車両を追跡して警備員を派遣したりすることが出来る。また、「リモートイモビライザー」では、クルマが盗難にあった場合にエンジンやハイブリッドシステムの始動・ステアリングロックの解除を禁止する。

3. 自動車に関する世界的なサイバー攻撃の現状

世界で走るコネクテッドカーの台数は、2021 年に 1 億 1,940 万台であったのに対して、2023 年には 3 億 5,200 万台に増加すると予測されている[4]。また、生成されるデータ量は、コネクテッドカーは 2025 年までに 1 時間あたり約 25GB と予想されるのに対し、完全自動運転車は 1 時間あたり 500GB のデータを生成する可能性が高い。現在、最新の自動車は約 1 億本のコードを使用しており、自動運転や車車間通信の登場により 2030 年には使用コード量は 3 倍に増加する可能性がある。このように、モビリティの新しい波によって取り扱われるデータ等の量は急増し、その結果、サイバーセキュリティツールへの依存度もその分高まることが予想される。

自動車に対するサイバー攻撃の数は、2018 年から 2021 年にかけて 225%増加したとされている[5]。また、84.5%を超える自動車関連の事件がリモートで実行されている。例えば、2021 年 7 月に英国にて、住居の外に駐車していたメルセデスベンツ GLC 250 がハッキングされ、盗難されるという事件が起きた。その件では、ハッカーが駐車場でスキャンデバイスを用いてキーレス型の車のドアロックを解除し、エンジンをかけ、車を盗難した。

2021 年のサイバー攻撃による被害件数トップ 3 は、順に、データ/プライバシーの侵害（38%）、自動車の盗難（27%）、制御システム（20%）である[6]。例えば、車には 100 個以上の ECU（電子制御装置）が搭載されており、エンジン・ドア・トランスミッション・車線維持システム・車間距離制御システムなどをソフトウエアで電子制御しているが、ECU の通信経路に外部から侵入があった場合、これらが不正に制御されるリスクがある。また、4G／LTE などの通信モジュールから無線

---

[3] 「マイカーSecurity」トヨタ自動車
https://toyota.jp/tconnectservice/service/mycarsecurity.html?padid=from_tconnectservice_service_dispatch_raize
[4] 「CONNECTED VEHICLE TREND RADAR 2」Capgemini/invent, 2020
https://www.capgemini.com/wp-content/uploads/2020/09/ConnectedVehicleTrendRadar_2_Report.pdf
[5] “Upstream's 2022 Global Automotive Cybersecurity Report”, Upstream, January 2022
https://upstream.auto/2022report/
[6] 脚注 5 に同じ

LAN（Wi-Fi）、Bluetooth などの無線通信インターフェースを通じて不正侵入される可能性も生じている。

4. 世界的なサイバーセキュリティに関する規制

自動車に対するサイバー攻撃のリスクが高まる中、サイバーセキュリティに関する国際標準の構築が求められてきた。そうした中、国連欧州経済委員会（UNECE）が自動車のサイバーセキュリティ及びソフトウエアアップデートに関する国連標準である UNR155、UNR156 を採択し、また、ISO（国際標準化機構）と SAE International（米国自動車技術者協会）が共同でサイバーセキュリティに関する国際規格 ISO/SAE 21434 を策定した。

- UNR155 及び UNR156

  2020 年 6 月、国連欧州経済委員会（UNECE）の自動車基準調和世界フォーラム（WP29）において、自動車のサイバーセキュリティ及びソフトウエアアップデートに関する国連標準である UNR155、UNR156 が採択された。これらの規制は、乗用車、バン、トラックおよびバスに適用される。UNR155 は、サイバーセキュリティおよびサイバーセキュリティマネジメントシステム（CSMS）、UNR156 は、ソフトウェアアップデートおよびソフトウェアアップデート管理システム（SUMS）に関する規制である。本規制の具体的な実施要件として、ISO/SAE 21434 を参照することとなっている。UNR155 及び UNR156 の主な内容は以下の通りである[7]。

  - サイバーセキュリティ及びソフトウェアアップデートの適切さを担保するための業務管理システムを確保すること。
  - サイバーセキュリティに関して、車両のリスクアセスメント（リスクの特定・分析・評価）及びリスクへの適切な対処・管理を行うとともに、セキュリティ対策の有効性を検証するための適切かつ十分な試験を実施すること。
  - 危険・無効なソフトウェアアップデートの防止や、ソフトウェアアップデートが可能であることの事前確認等、ソフトウェアアップデートの適切な実施を確保すること。

  EU（欧州連合）では既に UNR155 及び UNR156 を適用している。

- ISO/SAE 21434

  2021 年 8 月 31 日に発行された ISO/SAE 21434 は、ISO（国際標準化機構）と SAE International（米国自動車技術者協会）が共同で策定したサイバーセキュリティに関する国際規格であり、サプライヤーとメーカーが、車の設計から廃車までの自動車のライフサイクルを通したサイバーセキュリティ対策を講じることを要求している。

5. インドにおけるサイバーセキュリティ対策

インド政府は、現在、WP29 にて採択された UNR155 及び UNR156 を採用はしていない。一方で、個人情報保護の観点から、2000 年情報技術法（IT 法）、2011 年情報技術（合理的なセキュリティ実務・手続き及びセンシティブな個人データ・情報）細則が導入されており、その中にはサイバーセキュリティに関連する規定も存在している。例えば、IT 法第 43A 条では、センシティブな

[7] 「道路運送車両の保安基準等の一部を改正する省令及び道路運送車両の保安基準の細目を定める告示等の一部を改正する告示について」国土交通省、https://www.mlit.go.jp/report/press/content/001379922.pdf

個人情報を扱う企業が、合理的なセキュリティ実務・手続きを導入しておらず、その結果、ある者が損害を被った場合、企業は損害を被った者に対して補償しなければならないとしている。

加えて、2022 年 9 月 25 日付で 2000 年 IT 法に基づく通達が施行されており、そこでは、対象事業者はインド国内に過去 180 日分のログを保存すること、サイバー事件が生じた場合 6 時間以内に当局 CERT-In（India Computer Emergency Response Team）に報告すること、インド国内の連絡先を CERT-In に通知すること等が義務づけられた。

インド国内の企業は、以上に加えて、個人情報保護・情報セキュリティに関する信頼性を高めるため、ISO 27001 や ISO 27701 の認証取得を検討するべきと考えられる。まず、ISO 27001 は情報セキュリティマネジメントシステムに関する国際規格であり、情報の機密性・完全性・可用性の観点からリスクを適切に管理することを求めている。また、ISO 27701 は、ISO 27001 を拡張した規格であり、個人情報の処理によって影響を受けかねないプライバシーを保護するための要求事項とガイドラインを規定している。

インドにおけるコネクテッドカー市場は、未だ黎明期というべき状況であるが、インド大手自動車メーカー各社がコネクテッドカーを開発するなど、今後需要の増加が期待されおり、国際標準に合わせた自動車のサイバーセキュリティ対策を講じる必要性が高まるのは時間の問題である。そのため、インドにおいても製品開発から販売・メンテナンスまでの自動車バリューチェーンの中にサイバーセキュリティを組み込む検討を始める必要がある。

6. 終わりに

世界の自動車産業がサイバー攻撃によって被る損害は、2024 年までに 5,050 億米ドルに及ぶと予測されている[8]。インドにおいてもコネクテッドカーの利用者増加に伴い、サイバー攻撃による損害が高まることが予想されるため、インド自動車産業は、産業全体として、サイバー攻撃やサイバー犯罪者の特定・防止に積極的かつ適切に取り組む必要がある。そのためにも、インド自動車 OEM 及びサプライヤーは、サイバーセキュリティに関するインド IT 法及び国際標準である UNR155/UNR156、ISO/SAE 21434、それら規格を導入するための要件及び認証手順を理解することが強く推奨される。

[8] 脚注 5 に同じ

執筆
荒木　基晃（あらき　もとあき）
MBA、USCPA
2018 年、太陽有限責任監査法人よりグラントソントン・インディアに出向、ジャパンデスクを担当。
愛知県田原市出身。
Motoaki.araki@in.gt.com

グラントソントン・インディア
グラントソントン・インターナショナル加盟事務所。監査・保証業務、税務業務、アドバイザリー業務のフルライン専門サービスを提供。金融・自動車・メディア・ヘルスケア・不動産・消費財に強みを持つ。インド国内 13 都市 15 事務所、約 5,600 名の専門家を有する。
URL：https://www.grantthornton.in/ja/services/growth/global-expansion/india-japan/

◆◇　発行情報　　◇◆
インド愛知デスク

■発行元
2022 年度インド愛知デスク運営業務受託者： 松田綜合法律事務所（担当：弁護士 久保達弘）
〒100-0004 東京都千代田区大手町二丁目 1 番 1 号 大手町野村ビル 10 階
TEL: 03-3272-0101（代表） FAX: 03-3272-0102
URL: www.jmatsuda-law.com

■配信停止またはご送付先アドレスの変更・お名前の変更は下記アドレスにご連絡下さい。
aichidesk@jmatsuda-law.com