IT時事ネタキーワード「これが気になる！」（第82回）

つながる車、サイバー攻撃に対抗措置

2021.09.17

「コネクテッドカー」（つながるクルマ）とは、ICT端末としての機能を備えた自動車のことだ。車両の状態や周囲の道路状況などのデータをセンサーで取得し、ネットワークを介して集積・分析する。総務省の情報通信白書によれば、事故時に自動的に緊急通報を行うシステムや、盗難時に車両の位置を追跡するシステムが実用化されつつある。

私たちが日常持つスマホのように、車が常にインターネットにつながり、ネット上のクラウドサーバーとやり取りして便利な機能を提供するには、5Gによるモバイルネットワークの高速・大容量化や、IoT、ビッグデータ、AIなどの進展が欠かせない。未来に向けた総務省のコネクテッドカー構想については、平成29年の「Connected Car社会の実現に向けて」が詳しい。

ICTなどの最新技術により、自動運転や安全制御装置、盗難防止、事故やトラブル時の対応、快適な車内環境のコントロールなど、よりラクに安全に利用できるのはうれしいことだ。ただし、サイバー攻撃が高度化し被害が急増する世の中では、便利さに潜むリスクを気にせずにはいられないのも真実だ。

2015年、米国でジープ・チェロキーをWi-Fi経由でハッキングし、遠隔地から走行中の車両のエンジンを止める、ブレーキを操作する、ワイパーを作動させる、情報ディスプレーやオーディオシステムを乗っ取る操作実験が成功し、140万台のリコールに発展した。この事件をきっかけに、自動車におけるセキュリティ対策の必要性が問われるようになった。

コネクテッドカーの実現で、車のセキュリティ問題はネットワーク全体に広がった。コネクテッドカーのサーバーをハッキングすれば、そこにつながるすべての車を人質に取れる。車1台からネットワークに侵入され、サーバーやシステムにアクセスされる可能性もある。

防御のため自動車メーカーやIT企業90社が連携

もし今どきのハッカーがコネクテッドカー・システムへの攻撃を計画したらと想像してみた。ハンドル制御やアクセル制御を乗っ取って自動車を暴走させれば、事故を引き起こせる。安全装置や救助システムを停止させて、メーカーの信用を落とすこともできる。流通システムの車をかく乱し、流通を止めることもできる。集められた走行データを人質に、身代金要求もできるだろう。ハッカーにとって金の鉱脈となる可能性は少なくない。

一般的なコンピューター端末なら、セキュリティ装置やセキュリティソフトの導入がある程度浸透しているが、車や家にあるAI搭載のエアコンや電子レンジに使用者自らセキュリティ対策を行うのは考えにくい。

コネクテッドカーの技術は進歩しているものの、セキュリティ対策は追い付いていないといわれる。そんな現状に対し、日本の自動車業界が2021年2月11日、トヨタ自動車をはじめとする車メーカー14社が車部品メーカー7社と共同で、「つながるクルマ」のサイバー攻撃対策のための新団体、一般社団法人「Japan Automotive ISAC（J-Auto-ISAC）」を設立。8月30日には、会員企業が92社になった。

活動方針には脅威・脆弱性情報の収集および解析、関連情報の共有、管理施策やシステム施策の紹介、方針やガイドラ

インの策定、SIRTの構築および強化、外部連携、人材の育成などが挙げられている。

そもそもコネクテッドカーとは… 続きを読む