FCA（旧クライスラー）は、140 万台のリコールをこの 7 月に発表した。遠隔操作による自動車のハッキング実験によって、危険性が明らかになったからである。また、今年 3 月には、カリフォルニア州ではコネクテッドカーへの集団訴訟が起きている。これらの事件は、IoT（モノのインターネット）時代の主役として期待されてきたコネクテッドカーの開発が、大きな転機を迎えたことを意味している。今回は、これらの事件の経緯について、紹介することにしたい。

自動車メーカーのハッキング対策が始動

ウォール・ストリート・ジャーナル、ニューズウィーク、NHK をはじめ日米のマスコミ各社は、2015 年 7 月 23 日より一斉に、FCA 社（フィアット・クライスラー・オートモービルズ、旧クラスイラー社）による 140 万台のリコールを報じたのである。

FCA 社によるリコールは、セキュリティ専門家であるチャーリー・ミラーミとクリス・バラセックによる同社に対する警告と、彼らによる実験結果による。遠隔操作によりハッキングされる実験の模様は、7 月 21 日に、米専門誌「ワイアード」より、動画で公開されている。

この動画は、ノートパソコンで、自動車の制御システムに簡単に侵入し、エアコンやワイパーを勝手に操作したり、最後にはエンジンを停止させ、アクセルがきかない状態にした様子を紹介している。関心のある人は、この動画を閲覧することをお勧めする。

このハッキング実験を行った専門家は、FCA に搭載されている同様のシステムであればどの車でも遠隔操作が可能だとし、自動車各メーカーによる対策の必要性を訴えている。

自動車のハッキングへの恐れは、数年前から内外で指摘されてきたが、自動車メーカーの取り組みは、十分とは言えなかった。自動停止ブレーキ、コネクテッドカー、電気自動車など、業界での生き残りを賭けた技術革新競争を、自動車メーカーは最優先させてきたからである。

実際のリコールは、今回が始めてである。実際のハッキング被害が生起する前の対策と

して、注目すべきものである。このような自動車メーカーがハッキング対策に本格的に取り組まざるを得なくなった背景には、次に紹介するように、欧米でコネクテッドカーが政治問題化し始めているからである。

もっと大きな社会的背景として、家電製品、医療機器、建物の照明・空調・エレベータ機器、POS や ATM 端末まで、ハッキング被害の話題が世界各地で表面化してきている実態がある。これが、もし自分の愛車がハッキングされたらどうなるという不安を、社会に広めており、政治問題化するのは時間の問題であったといってよい。

政治問題化した自動車のハッキング問題

自動車のハッキングを政治問題として取り上げ注目された最初は、米上院議員であるエド・マーキー（Ed Markey）による報告書である（「車がハッキングされる危険性、米上院議員が報告書で警告」《Nick Statt（CNET News）2015/02/10 》を参照）

この報告書は、2015 年 2 月 9 日に発表され、インターネットに常時接続されているコネクテッドカー（Connected Car）の大半が危険であると指摘している。同調査は、マーキー事務所によって 1 年以上前に開始され、自動車メーカー20 社にアンケートを送付し、16 社から回答を得ている。

同報告書は、「ハッキング攻撃をリアルタイムで回避するシステムを運用していると答えたメーカーはわずか 2 社で、ハッカーに乗っ取られた車を遠隔から減速または停止させることができると認めたメーカーも 2 社にとどまった」と報告している。

報告書は、最後に「業界のセキュリティおよびプライバシープラクティスが驚くほどまちまちで不完全な状態にあることから（中略）、米国家道路交通安全局は、プライバシー問題について米連邦取引委員会（FTC）と協議し、自動車のコネクテッド化が進む現代においてドライバーのデータ、セキュリティ、プライバシーを保護する新基準を公布することが必要になっている」と結論づけている（出所は、上記の参照資料）。

次に、注目すべきは、カルフォルニア州で集団訴訟となった事件である。2015 年 3 月に、 Stanley 法律事務所が、トヨタ、Ford、GM の 3 社に対して、コネクテッドカーのハッキング問題について正確な情報を消費者に伝えていないとして、集団訴訟を起こしている（出所、「自動車メーカーとハッキング可能車両に対する訴訟提起」、SBC、14. July 2015、http://www.sbdjapan.co.jp/lawsuit_seeks_damages_against/）。

この集団訴訟が注目されるは、「これら 3 社の車両メーカーが、ハッキングによる車両のリモート操作が可能である事を認識しながらもコネクテッドカーを販売し、消費者を危険に晒し、コンピュータを利用したカーシステムの危険性を意図的に消費者に知らせず、またそれに伴う安全性対策を怠った」という点（下線は筆者による）にある。

根本的なハッキング対策としては、車載ネットワーク CAN（Controller Area Network）へのハッキングされないようにするだけでは不十分である。中野技術士事務所の指摘（http://nakano-pe.jp/blog/archives/3582）にあるように、仮に CAN がハッキングされても、それとは別にエンジンとブレーキが作動できる仕組みを用意することが必要である。

自動車メーカー各社による、今後のハッキング対策に注目していきたい。

（TadaakiNEMOTO）