SOMPO未来研究所 主任研究員　新添 麻衣氏

デジタル時代のリスクと保険　(12)

車ハッカー事故、政府保障で

自動運転車を含めたデジタル時代の自動車「コネクテッドカー（つながる車）」の最大のリスクは何と言っても、サイバーセキュリティーだろう。実際、車内ネットワークに侵入し、遠隔操作することが可能なことが、海外での実車を使った実験などで示されている。こうした自動車へのサイバー攻撃に保険はどのように対応していけばよいのであろうか。

ハッキングにより自動運転車が正常に作動せず事故を起こした場合の取り扱いについては、国土交通省の「自動運転における損害賠償責任に関する研究会」で次のように整理されている。

ハッキングによる交通事故については、泥棒運転により生じた事故と同様に考え、既存の「政府保障事業」（自賠責保険から保険金を受けられないひき逃げなどの場合の保障制度）で被害者を保障する方針を示している。その車の運行供用者（一般には所有者）が管理責任を十分に尽くしていた状態で自動車をハッキングされた場合、現在の制度では自賠責保険の補償対象とならないのである。

本来であればハッカーを捕らえ、損害賠償をさせるべきであるが、実現するのは極めて難しいことが想定される。このような事故で被害者を救済するセーフティーネットが政府保障事業である。

ただ、この制度にも課題がある。現行の政府保障事業は自賠責保険料の一部に含まれる賦課金を主な財源として運営しており、テロのような大規模なハッキングの発生を想定していないとみられることだ。この点で、財源が十分と言えるのかどうかは将来的に論点となる可能性があるだろう。

また、政府保障事業は被害者の死亡や傷害など人身傷害のみを対象としており、保障金額も最低限のものとなっている。

このため、多くの損害保険会社は上乗せ補償として「被害者救済費用補償特約」を任意自動車保険に自動付帯で提供している。政府保障事業の額を上回る対人賠償に加え、対物賠償も補償対象となっており、ハッキング時の被害者救済にも対応している。既存の自動車保険がつながる車に対する万が一への備えにも活用できる。

なお、車両所有者が自動運転のソフトウエアの更新を怠っていたなど必要なセキュリティー対策を講じていなかった場合は、ハッカーの責任は消えない一方、運行供用者の過失も認められると考えられる。この場合は、一般的な自動車事故と同じく、自賠責保険とその上乗せ補償である任意自動車保険で被害者は救済される。

法制度面では車両メーカーのセキュリティーに関する業務プロセスの要件が強化されている。2020年４月に施行された道路運送車両の保安基準の改正に伴い、車両のリスクアセスメントや管理体制の構築、セキュリティー対策の有効性を検証する試験の実施などが型式認証の取得に必須となった。

この枠組みは、日本が共同議長を務めた国連欧州経済委員会の自動車基準調和世界フォーラム（ＷＰ29）の分科会で20年６月に新規則として採択された。自動車のサイバーセキュリティーに関連する初めての国連規則であり、今後、国内外で適用されるようになる。

高度化するサイバー攻撃に対応すべく、市場に製品を投入する際の監視と、実際の利用局面を想定した被害者救済の枠組みの両面で対処していくことが新しいテクノロジーの安全な社会実装に向けて重要である。

ハッキングによる事故時の被害者救済

	運行供用者の車両管理	
	過失なし	過失あり
国の制度	政府保障事業	自賠責保険
任意加入の自動車保険	被害者救済費用補償特約	対人・対物賠償補償

(注) 国の制度はいずれも人身傷害のみ、任意加入の自動車保険は人身・物損が対象

掲載日 2021年12月09日 日経産業新聞 012ページ