自動車サイバーセキュリティー強化を求める背景とアフターマーケットへの影響

自動車サイバーセキュリティー強化が求められる背景

整備事業の視点から見ると、自動車のサイバーセキュリティー強化は、スムーズな作業の進行を妨げ、新たな設備投資を発生させるコスト要因としての側面が強調される。しかし、ここまで自動車のサイバーセキュリティーが強化されるのには、相応の理由がある。

カーメーカーなどにサイバーセキュリティーサービスを提供するUpstream Securityが発行する「グローバルモビリティサイバーセキュリティ報告書」によると、この数年で自動車に対するサイバー攻撃の数は大幅に増加（**グラフ1**）し、その影響は大規模化している。また同報告書では、悪意を持ってシステムを攻撃するハッカー（ブラックハットハッカー）の関心領域についても調査しており、その調査結果において「診断ソフトウェア」が19.3％と高い関心を集めていた。車両と接続するOBDポートや様々な操作が可能な診断ソフトは、自動車にとってセキュリティー上のリスク要因となりかねない。

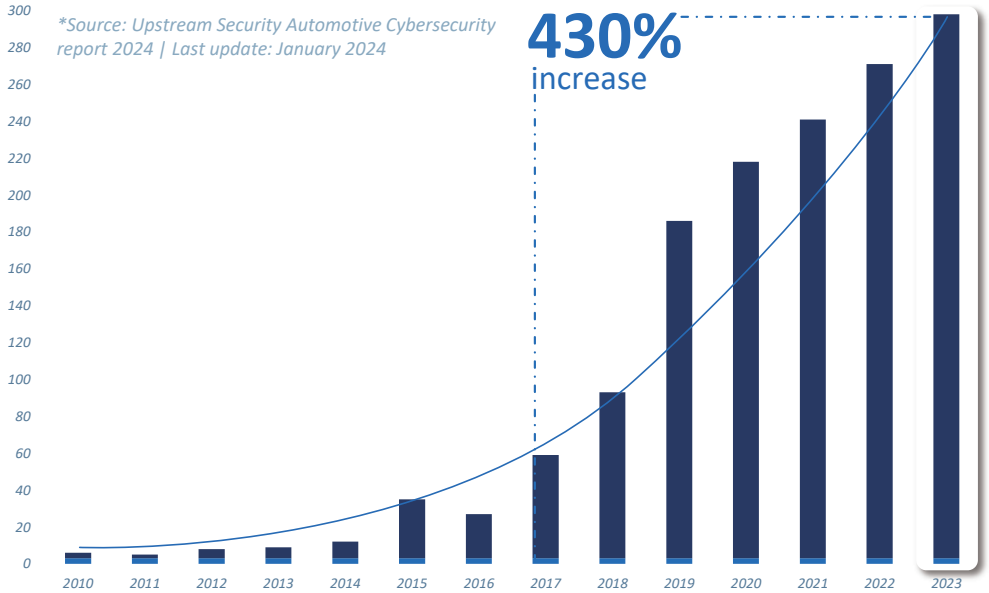
サイバーセキュリティーに関する規制では、サプライチェーン全体でのセキュリティー強化を求めており、カーメーカーは部品サプライヤーなどに対して厳密な対応を求めている。当然ながら新車販売ディーラーにおいても、セキュリティー対応が強化されている。

今後、汎用スキャンツールでサイバーセキュリティー対応車に対する各種作業が可能となったとしても、それらを所有及び使用する工場には、高いセキュリティー意識と対策が求められることになるだろう。

自動車サイバーセキュリティー強化を求める規制の内容

ネットと接続するコネクティッドカーや自動運転技術が普及したことで、サイバーセキュリティーが自動車の安全性に直結する重要な要素の一つとして考えられるようになった。サイバーセキュリティーの重要性が高まる中、自動車の安全確保を目的とした規制や規格が多数成立している。その中でも

グラフ１　車両に対するサイバー攻撃の年間発生件数の推移
出典：Upstream Security「グローバルモビリティサイバーセキュリティ報告書」



汎用スキャンツールの機能向上で整備事業者のサイバーセキュリティー対応を支援

サイバーセキュリティーに対応した自動車の登場により、
一部整備作業において影響が出始めている。
国土交通省 物流・自動車局 自動車整備課 整備事業指導官の村井章展氏に、
車両サイバーセキュリティーが強化されている背景や
整備事業者への影響、対策などについて話を聞いた。

国土交通省
物流・自動車局 自動車整備課
整備事業指導官 村井章展 氏

――車両サイバーセキュリティーが強化されている背景を教えてほしい

自動運転とOTA（Over The Air）技術の登場により、自動車に対するサイバーセキュリティー及びソフトウェアの管理が国際的な課題となった。この課題を受けて、WP29は新たな国際基準となるUN-R155とUN-R156を採択した。UN-R155がサイバーセキュリティーに関する基準、UN-R156がソフトウェアアップデートに関する基準であり、これらの基準を日本だけではなく各国が採用している。

これまでの技術基準は、自動車に対して何らかの性能要件を課していた。一方、UN-R155・156はカーメーカーに対して、サイバーセキュリティーの確保とソフトウェアの適切な配布という義務を課している。

この基準に対応するためには、カーメーカーはまず車両開発から設計、製造、使用過程に至るまで、自動車にどのようなサイバーリスクがあるかを分析する必要がある。たとえばカーメーカーや車両販売店の業務用PC、あるいは車両に搭載されたUSBポートやOBDコネクターなどあらゆるリスク要因に対し、サイバーアタックを受けた場合に車が安全であることをどのように担保しているのかが問われることになる。

また、これまでの技術基準では、たとえば自動ブレーキでは時速何km時において前方の車両に衝突しないこと、などの具体的な要件が示されていた。しかしサイバーセキュリティーの基準には、そのような具体的な要件は示されていない。具体的な要件を明示してしまうと、カーメーカーのサイバーセキュリティー対応も見えてしまい、セキュリティーリスクを高めてしまうからだ。

カーメーカーは何をリスクと考え、どのようなリスク緩和策を採用したのか審査当局に説明する必要があるが、何をすれば合格・不合格ということは決まっていない。そのためメーカーごとに対応が異なり、その対応が合理的であれば審査を通過することができる。なお同基準においては、カーメーカーの体制に対する審査と車両に対する審査があり、メーカー体制に対する審査を通過しなければ、車両に対する審査を受けることはできない。

また、今回の規則でもう一つ特徴的な点は、車両に対するサイバーセキュリティーの責任をカーメーカーに負わせていることである。これは当たり前のことだと思われるかもしれないが、開発から製造、販売、使用、整備まで、多くの人と企業が関わる自動車に対し、そのサイバーセキュリティーの全責任をカーメーカーに置いていることが、この規則のポイントと言える。

――サイバーセキュリティー強化による自動車整備業界への影響について、業界から声は上がってきているか

サイバーセキュリティーに関連する保安基準等の改正は公布が2020年、OTA対応の新型車への適用が2022年であり、この基準に適合した車両はまだそれほど多くない。そのため、実作業への影響を訴える声はまだそれほど多くないが、将来に対する懸念は耳にしている。しかし今回の基準適用を受けて、具体的にどのような作業ができなくなるのかというのは、先ほど申し上げた通りメーカーごとにサイバーセキュリティー対応が異なるため、一義的に言い切ることはできない。

もちろん国交省としても、サイバー