サイバーセキュリティ協力を進める日本の自動車業界

※本資料は 2020 年 7 月 7 日にオンライン誌の Lawfare が公開したオリジナルの記事を日本語訳されたものです。

オリジナル記事:

「The Japanese Automobile Industry Is Taking Next Steps for Cybersecurity Collaboration」
https://www.lawfareblog.com/japanese-automobile-industry-taking-next-steps-cybersecurity-collaboration

著者:
NTT チーフ・サイバーセキュリティ・ストラテジスト　松原実穂子

本文:

サイバーセキュリティリスクを巡る議論は、えてして重要な産業である自動車業界を見落としがちだ。独自のサイバーセキュリティの課題を抱えながらも、問題を解決すべく日本の自動車業界は努力を続けており、成功を収めつつある。

日本の自動車業界に対する一連のサイバー攻撃後、同業界におけるサイバーセキュリティ強化への取り組みが本格化した。まず、2017 年にワナクライのため、日産の英国工場の生産に障害が出た。その後も日本の自動車業界へのサイバー攻撃は続き、2019 年にはトヨタの販売子会社がサイバー攻撃を受け、310 万人の顧客の個人情報が流出した恐れがある。2020 年 6 月にはホンダがサイバー攻撃を受け、イタリア、日本、北米、トルコ、英国の業務が一時停止する事態に陥った。こうした事件を受け、サイバーセキュリティは、自動車メーカーやそのサプライヤーの業務継続にとっても不可欠であることを改めて自動車業界は痛感することとなった。

自動車業界のサイバーセキュリティのリスクは、他業界と比べてそれほど深刻なものではないと考えている人も中にはいるかもしれない。しかし、自動車メーカーが恐れる悪夢のシナリオとは、サイバー攻撃により日々の企業活動が停止し、顧客の情報資産や企業の知的財産が窃取されることだ。自動車業界へのサイバー攻撃によって、提供している製品やサービスに悪影響が発生するだけでなく、顧客の安全・安心も損なわれてしまいかねないのである。

自動車のサイバーセキュリティは、一筋縄ではいかない。自動車そのもの、自動車メーカーやサプライヤー（電子機器やソフトウェアのサプライヤー含む）、サービス事業者（ディーラーやカーシェアリングなど）という 3 つの層で構成されているためである。

自動車そのもののサイバーセキュリティは、自動車の各部品のセキュリティに依存するところが大きい。例えば、電子化された制御システム、コネクテッドカーサービス、製造システムなどが挙げられる。自動車メーカーは日々の業務を行うため、大量の IT システムやコンピュータ、サーバーを使用している。こうしたシステムでサイバーセキュリティが確保されなければ、自動車メーカーは製造のあらゆる課程で部品のセキュリティを確保し、自動車関連のコンピュータプログラムを安全に作れなくなってしまう。また、自動車メーカーと技術のサプライヤーは知的財産情報の一部を共有し、自動車が適切に設計・製造されるようにする必要がある。そのため、データ・セキュリティは全関係者が責任持って対応しない限り実現できない。

サプライチェーンリスク管理も複雑だ。通常、自動車は 4 万の部品からできている上、近年は搭載されるソフトウェアが飛躍的に増えている。自動車がますますインターネット接続されるようになってきたため、自動車メーカーは IT 企業や自動運転センサー、光学センサーカメラの会社など新たなサプライヤーとも協力するようになり、サプライチェーンはさらに拡大している。ディーラーやコネクテッドカーサービス事業者は、顧客の名前や住所、GPS の履歴、銀行口座から与信情報に至るまで膨大な顧客の個人情報を扱う。

現在、自動車に特化したグローバル共通のサプライチェーンに関するサイバーセキュリティ基準や標準は存在しない。各自動車メーカーは、ISO/IEC 27001 などの国際セキュリティ標準、アメリカ政府 NIST の「サイバーサプライチェーンリスクマネジメント」などの国別のガイドラインや規制を取り入れて対応してきた。自動車メーカーが参照している NIST の文書には、SP800-161、SP800-171、SP800-58 などがある。相互認証など、二国間、多国間でも個別のイニシアチブを調和させるための努力が続けられている。一方、国連の WP.29 は、サイバーセキュリティのタスクフォースを作り、日本が議長を務め、54 カ国が自動車自身へのサイバー攻撃対策に関する指針を議論してきたが、2020 年 6 月に採択された。2021 年 1 月から施行される。

それでは、今後進めていくために最善の方法は何であろうか？　日本のサイバーセキュリティ部会が、自動車のサイバーセキュリティ改善に向けて具体的な提言をしている。

2019 年 4 月、一般社団法人日本自動車工業会（JAMA）は、WP.29.など様々なステークホルダーとサイバーセキュリティ課題について話し合うとともに、サプライチェーンリスク管理のためのサイバーセキュリティ・ガイドラインを作るため、電子情報委員会の下にサイバーセキュリティ部会を設立した。日本の自動車メーカー14 社全てがこの部会に参加しており、業界全体のサイバーセキュリティのレベル向上を目指している。その 2～3 カ月後、一般社団法人日本自動車部品工業会（JAPIA）もサイバーセキュリティのワーキンググループを設立した。2019 年夏からは両ワーキンググループが協力し、ガイドラインについて議論を始めた。

国内外に共有できるガイドラインの作成という共通の目標があったとは言え、各社がどのようなサイバーセキュリティの取り組みを進めているのか、ポリシーを持っているのかを最初から競合同士で率直に話し合うのが容易だった訳ではない。月に 2～3 回、会合を行ってきた（新型コロナウイルスの感染拡大に伴い、新たな課題が浮上した。オンラインで会合を開くようになり、機微な文書をオンライン上で共有することへの懸念にどう対処するか検討しなければならなくなったからだ）。

日本自動車工業会のサイバーセキュリティ部会は、ガイドラインを作成する上で 4 つのステップを取った。第 1 に、サイバーセキュリティやサプライチェーンリスク管理を扱っている「サイバー・フィジカル・セキュリティ対策フレームワーク」という 2019 年 4 月に経済産業省が作った文書を参照した。この文書は、他国のサイバーセキュリティのガイドラインや規制も参照しており、様々な政策を調和させる上で役立つと考えたためである。

第 2 に、部会のメンバーは、各社のサイバーセキュリティ・ポリシーの抜粋を比較検討し、各社がサイバー・フィジカル・セキュリティ対策フレームワークの主な項目にどのように取り組んでいるかを理解した。サイバーセキュリティのリスク管理についてメンバーごとに異なる段階にあり、各社独自の企業文化を反映し、それぞれ使う用語も異なるため、同フレームワークと各社の現状を比較するのに 2～3 カ月を要した。

第 3 に、日本自動車工業会と日本自動車部品工業会は、サイバー・フィジカル・セキュリティ・フレームワークに含まれる 129 の項目のうち、中小企業も実践すべき最低限の基準として 50 項目のみを使うことにした。日本自動車工業会と日本自動車部品工業会のメンバーは大手の自動車メーカーや部品メーカーだが、下請けや孫請け企業は中小企業が多い。最低限の基準を示したことで、企業が取るべきサイバーセキュリティ対策の強固な土台ができた。最低限の基準には、例えば、サイバーセキュリティのポリシーの策定やサイバーセキュリティの責任者の任命が盛り込まれている。基準について合意に至るまでに 2 カ月かかった。

第 4 に、部会は 3 カ月かけて、サイバーセキュリティ・サプライチェーンリスクマネジメントに関するガイドラインを作成した。最初のバージョンは 2020 年 5 月に発表され、今後英語版も出ることになっている。対象となるのは、自動車メーカー、部品メーカー、技術サプライヤーである。3 カ月間のトライアル期間中に、数社にガイドラインを使ってもらい、フィードバックを得た上で、再度見直し、修正する。

また、自動車工業会は、ガイドラインを拡充し、より高度なサイバーセキュリティ能力を持った企業や、自動車メーカーやサプライヤーだけでなく工場やディーラーも対象にしたいと考えて

いる。日本の自動車業界としては、2020 年 5 月のガイドラインと今後の改訂版が業界全体のサイバーセキュリティの底上げに役立つと期待している。各自動車メーカーは、かつては、グループ企業内ではポリシーを実践できても、サプライヤーには強制できなかった。しかし、このガイドラインがあれば、自動車のサプライチェーンに入っている全ての日本企業がサイバーセキュリティの取り組みで足並みをそろえられるようになる。次に取るべきステップは、他国との相互認証の合意取り付けとなる。

日本の自動車メーカーやサプライヤーは、グローバルな自動車のサイバーセキュリティに貢献したいと強く願っている。米国に市場を持っている日本の自動車メーカーは、米国の Auto-ISAC に参加しており、日本のサイバーセキュリティやサイバー攻撃に関する知見を共有している。Auto-ISAC は、2015 年に設立され、サイバーセキュリティのベストプラクティスやサイバー脅威インテリジェンスの共有を行う。メンバーには、自動車メーカーだけでなく、IT 企業や AT&T などテレコム企業も含まれる。ホンダやトヨタは、2019 年の Auto-ISAC の会合でプレゼンしたこともある。また、日本自動車工業会は 2017 年に J-Auto-ISAC を立ち上げ、日本国内でのサイバー脅威インテリジェンスの共有にも力を入れている。

日本の自動車メーカーやサプライヤーがサプライチェーンリスク管理に関するガイドラインの拡充を国内で進める中、今後日本は、相互認証のため他国と協力する必要があり、日本の自動車業界としてもベストプラクティスを共有したいと思っている。ドイツ、イギリス、アメリカもそれぞれサイバーセキュリティ規制に取り組んでいるところだ。例えば、アメリカの運輸省道路交通安全局は、2016 年に Cybersecurity Best Practices for Modern Vehicles を出している。自動車業界のサイバーセキュリティに関する世界標準があれば、日本と他国との間の協力が一層強化できるだろう。

新型コロナウイルスは世界経済に大打撃を与えた。サイバー攻撃者は、テレワークへの急激な移行や新型コロナウイルスの最新情報への人々の関心を悪用し、新型コロナウイルスがらみのなりすましメールを送り、偽の接触追跡アプリや VPN を作っている。サイバー脅威が高まっているにもかかわらず、バラクーダネットワークスの 2020 年 5 月の調査結果によると、世界の 4 割の組織がコストカットの一環でサイバーセキュリティ予算を削減した。この未曾有の危機において、国境を問わず仕掛けられてくるサイバー攻撃と戦うには、企業間・国家間のサイバーセキュリティ協力の重要性が今まで以上に高まっている。

サイバーセキュリティは、自動車に関わる全ての企業にとって、イノベーションを維持し、顧客を守る上で共通の課題であり、チャンスでもある。電子化された制御システムのサプライヤーは世界でもそれほど数は多くない。ディーラーは複数の自動車メーカーと取引することが多い。そのため、業界が一丸となってサイバーセキュリティに取り組むことが必要不可欠であ

る。国レベルや国際レベルでのガイドライン作りについての議論は進んでいる。グローバルでの安全を確保するには、今こそ、二国間でベストプラクティスを共有し、ウィンウィンの関係を獲得すべきだ。日本の準備はできている。次に手を挙げるのは誰か？

以上