車両サイバーセキュリティの未来

PwCコンサルティング合同会社　シニアマネージャー　奥山（おくやま）　謙（けん）

1. はじめに

ニュース・新聞・インターネット・テレビなど、多くの媒体が伝えるように、いま、自動運転車両の開発が進められている。CASE（コネクテッド、自動化、シェアリング、電動化）技術も進歩しており、モビリティ社会が変化しようとしている。

一方で技術の進歩は、サイバーセキュリティへの懸念にもつながっている。車がネットワークにつながることでサイバー攻撃の脅威にさらされる可能性も増えてくる。こうした動向を受けて、国連欧州経済委員会のWP29/GRVAでは、サイバーセキュリティ専門家会議が行われ、自動運転車の基準の策定等が検討されている。また、ISOでも車両サイバーセキュリティ国際標準の検討がなされている。

このような動きにより自動車関連の各社では、サイバーセキュリティ対策の実施が求められている。本稿では、WP29国連法規やISO/SAE 21434をベースとして、今後実施が求められるサイバーセキュリティ施策をひもといていく。

2. 自動運転車・コネクテッドカー

サイバーセキュリティ施策の前に、前提となる自動運転車両・コネクテッドカーやこれらが動作する環境について、おさらいをしておく。

コネクテッドカーとは、外部と通信する機能を持った車両全般のことで、WiFi機能やセルラー網とつながる機器を有した車両のことである。これにより、事故発生時などの緊急サポート機能やインターネット閲覧の機能が利用可能になる。

自動運転は、その機能によりレベル分けが5段階でなされており、ドライバーによる車両操作が前提となるLv1-3と、システム自体で車両操作をするLv4-5とに大きく分かれる。特に自動運転Lv4-5では、外部環境（ITS設備）や他の車両と通信することにより、外部環境を把握することで自動運転を実現することがあり、いわゆるコネクテッドカー同様に外部通信機能を有する。

このように、これからの自動車には外部と通信する機能が求められ、外部環境を早く正確に入手することが重要である。これにより、より安全に利便性高く様々な利用環境で自動運転車両が活動できるようになるために、高速通信や同時接続が実現できる5G（第5世代移動通信システム）などの活用も期待されている。自動車のセキュリティを検討する際には、このような最新の通信技術も理解した上で対策を検討する必要がある。

3. 自動運転車に対するサイバーセキュリティ脅威

前章で説明したとおり、自動運転車両での5Gの活用により、様々な環境で、より安全に自動運転車両が活用できるようになるなど、大きなメリットがあるが、一方で、高速で外部接続機能を有することにより、セキュリティ脅威も増えることになる。自動運転車両が外部接続できるということは、悪意ある攻撃者が自動運転車両を外部から攻撃することで、車両制御機能を奪ってしまうことも、原理的には可能になるためである。

自動運転車における、典型的なサイバーセキュリティの脅威は、車両の制御機能を奪われることである。攻撃者により、外部からアクセルやブレーキといった制御系機能を乗っ取られることで、車が故障したときのような事故を誘発されることも考えられる。

車両の制御機能を奪われる以外にも、従来のITサービスと同様な被害も考えられる。コネクテッドカーのサービスが高度になることで、車両のオーナーごとにカスタマイズされた機能も提供することとなり、そこではユーザー識別の機能が利用されることがある。そのような場合、他のユーザーに成りすますことで、不正に車内サービスを利用したり、ユーザーにひも付いた車両情報や個人情報を盗まれてしまう可能性もある。特に、シェアリングカーが普及するようになれば、ユーザー管理も重要となるので、なりすましによる、不正（無断）利用も重要な問題となることが想像される。

これからの車両では、上記のようなサイバーセキュリティ脅威を踏まえて、事故や不正利用といった問題を発生させない十分なサイバーセキュリティ対策が必要になる。

4. WP29

自動車のサイバーセキュリティ脅威が懸念される背景を受けて、国連欧州経済委員会における自動車基準調和世界フォーラムWP29の分科会であるGRVAのサイバーセキュリティ専門家会議にて2020年6月、自動車のサイバーセキュリティとソフトウェアアップデートに関する国際基準（UN規則）が成立した。

GRVAは自動車の装置ごとの安全や公害に関する基準の統一及び相互承認の実施を目的としており、1958年にジュネーブで作成された「車両等の型式認定相互承認協定」の枠組みの中で、自動運転車のサイバーセキュリティ・ソフトウェアアップデート法規基準を検討しており、協定締約国は、本法規基準の内容をそれぞれの国の法規へ落とし込むことが求められる。

日本では2020年4月に、自動運転車に対応した改正車両法が世界に先駆けて施行された。改正車両法では、WP29 GRVAで議論中のCS（Cyber Security）・SU（Software Update）規則が反映されており、今後正式発効されたCS規則とSU規則との差分について国内へ導入されていく見込みとなっている。

この国連基準で明記されたサイバーセキュリティ対策の特徴は以下のとおりである。

・車両ライフサイクル全般でのセキュリティ対策が必要。特に出荷後の対策も明記されている
・サプライチェーン全体での取組みが求められている（車両OEMのみが対策すればよいものではない）
・車両ライフサイクル全般を通じ、最新のリスク分析を踏まえて対応する必要がある（画一的なセキュリティ施策を実施すればよいわけでない）

以降は、これら具体的セキュリティ施策の内容について概要を説明する。

5. 企画フェーズでの取組み

車両サイバーセキュリティ施策は、前述のとおりライフサイクル全般での実施が求められている。車両ライフサイクルの一番初めは企画フェーズで、どのような車両を開発するか、企画・計画する段階である。またこのフェーズに先立って、ライフサイクル全般でのセキュリティ施策を実施管理するための組織構築も必要になる。

車両サイバーセキュリティ施策のそもそもの目的は、車両に関するサイバーセキュリティリスクを管理（最小化）することにある。それには、車両ライフサイクルに関わるすべての組織で適切なセキュリティ対策を実施することが必要だ。そのためには、セキュリティ施策を遂行する「組織」の準備が必要である。

組織として、ライフサイクル全体を通じて必要十分なサイバーセキュリティ活動を実施するためには、サイバーセキュリティ活動を全体統括する組織がガバナンスを効かせることが必要である。組織ガバナンスでは、組織として方針を定め、目標や戦略を定めることが必要だが、サイバーセキュリティにおいても同様である。サイバーセキュリティの方針、目標、戦略立案を定めることが基本となる。また、適切な目標・戦略を定めるためには、車両が置かれたサイバーセキュリティ環境を正確に理解することが求められる。特に、車両や車両部品に対するサイバーセキュリティ環境は近年変化が激しく、最新の攻撃手法やセキュリティ対策動向の把握は重要である。

企画フェーズでのサイバーセキュリティ施策は、前述の、最新の攻撃手法や対策技術を踏まえて、開発する車両のサイバーセキュリティのリスクを把握することから始まる。

リスク把握では、はじめに、開発対象の車両のユースケースや、参照可能な情報に基づいてシステム構造を整理し、守るべき情報資産・機能資産の把握をする。もちろん、企画段階では開発する車両の詳細設計は確定していないので、リスクが明確にならないこともある。このような場合では、限られた前提条件や情報に基づいて分析を進める技術も必要となってくる。

洗い出した各資産に対し、起こり得るセキュリティ上の脅威を特定する。悪意の第三者を考慮するセキュリティにおいては、実際の攻撃者（ハッカー）のアプローチや手法に関する専門性が必要になり、脅威の洗い出しに向けた構造的アプローチが各団体より提案されている。ただし、現状統一された手法は確立されていないため、各組織は製品の特性や開発現場の実情に適した手法を選択、または組み合わせて活用していく必要がある。

なお、今後のセキュリティ対策全般にいえることであるが、すべてのセキュリティリスクをゼロにすることは現実的ではなく、限りあるセキュリティ対策のリソースを適切に分配し、製品ライフサイクルの各活動を通じて、十分なレベルまでリスクを低減する必要がある。

そのために、リスクは洗い出すだけでなく、重要度や発生可能性を踏まえて、リスクの高低を評価し、適切に管理することが求められる。

6. 開発フェーズ：サプライチェーンの取組み

企画フェーズの後は、設計・実装といった開発を行うフェーズとなる。ここでは、企画フェーズで洗いだしたリスクへの詳細化や具体的な対応の立案実施をすることになる。

前述のとおり、企画フェーズでのリスク分析は、まだ設計内容が定まっていない段階のものであるため、いくつかの前提条件を置いたものとなっている。そのため、車両開発が進み、設計内容が詳細化・決定していく都度、洗い出したリスクが顕在化する条件を再度整理することが必要である。また、セキュリティ対策を設計内容に取り込むことで、洗い出したリスクの評価を見直す場合もある。十分なセキュリティ対策を設計に取り込むことができるのであれば、リスクは低減されたとみなすことができる一方、設計上の制約で十分なセキュリティ対策が施せない場合は、リスクが高まったと考え、追加のセキュリティ対策の検討や、時には、当該機能の実装を取りやめるなど、リスク回避の施策も必要になるかもしれない。

一般に、車両開発フェーズは、車両OEMのみで実施されることはなく、サプライヤと呼ばれる車両部品開発の委託先も関わって実施される。そのため、セキュリティ対策の実施も、委託先で実施されるよう車両OEMから要件を出す必要がある。要件には、企画フェーズで実施したリスク分析結果を基にしたセキュリティ対策検討を含む必要がある。委託先では受けとったリスク分析結果を踏まえて、前述のリスク分析の詳細化作業を実施することが必要となる。

また、ソフトウェア開発の実装フェーズに入ると、リスク分析を考慮した対策のみならず、ソフトウェアをセキュアに実装する基本的な取組みも必要となる。一般に、セキュアコーディングと呼ばれる取組みのことで、すべてのエンジニアがサイバーセキュリティ上の欠陥＝脆弱性の無い安全なプログラムを開発できる仕組みが必要である。昨今の車両開発では、ソフトウェアの大規模化が進んでおり、ソフトウェア開発に関わるプログラマーの数が増えてきている。また、大量のプログラマーのうち、1人でもミスをしてしまうと、車両もしくは車両部品に欠陥が入り込み、セキュリティ被害を発生させてしまう点が難しい問題である。

このような大量のプログラマーが関わる実態を踏まえると、セキュアコーディングの施策を人手で管理実施することは現実的でなくなってくる。そこで、セキュアコーディングの実施管理にツールを使うことが一般的となっている。静的解析ツールと呼ばれる、実装されたプログラムの品質をチェックするツールを使うことで、機械の力でセキュアコーディングを運営するやり方となる。これに加え、開発者のセキュアコーディング理解向上を目的とした教育を実施することで、組織としてセキュリティ施策を実施することが求められる。

また、開発フェーズでの最終段階として、セキュリティを考慮した、製品テストの実施が必要となる。セキュリティを考慮したテストでは、大きく2つの観点での実施が必要である。1つは、前段で洗い出したリスク評価を踏まえたテストで、洗い出したリスクが十分に対応されているかを確認するものである。もう1つは、最新の攻撃技術動向を踏まえて攻撃者目線でセキュリティ品質が十分であるかを確認するものである。後者のテストは、リスク分析結果を基にするというより、攻撃者目線で実際の攻撃を仕掛けることで、リスク評価結果は妥当であったかを再確認する観点に重きが置かれる。このようなテストを適切に使い分けて実施することで、開発した車両を出荷しても問題ない安全なものとなっているかを確認することが求められる。

7. 製造フェーズでの取組み

開発フェーズの後は、工場において製品を製造・生産するフェーズとなる。製造・生産フェーズにも、セキュリティ脅威は存在し、セキュリティ施策の実施が必要となる。

製造での主なセキュリティリスクは、自動運転車のリスクが高まってきたのと同様に、製造工場でもIoT化・スマートファクトリー化が進み、ネットワークにつながるようになってきたことが要因となっている。また、システム自体に汎用的なOSやアプリケーションが用いられることも増えており、このような環境の変化によって、マルウェアのターゲットとなるなどセキュリティリスクがより高まっている。

また、車両がネットワークに接続されたことで、通信の暗号化やメッセージ認証のような暗号技術の利用が広がった。その影響で、暗号技術において重要な役割を果たす暗号鍵を、内部に保管しなければならない車両部品が増えている。この暗号鍵は製造フェーズで、製品に書き込む必要がある。そのため、工場では、暗号鍵自体及び暗号鍵を書き込む製造システムのリスク対策を厳重に実施・管理し、暗号鍵の漏えいや改ざんがないことを常に保証する必要がある。

さらには、開発フェーズと同様に上述の施策は、委託先と協調して実施する必要がある。暗号鍵を書き込む必要のある車両部品は委託先で製造されていることもあるためで

ある。このようなケースでは、車両OEMと委託先のシステムをネットワークで接続し、安全に暗号鍵を受け渡す仕組み・運用を構築する必要がある。対象が車両そのものではないが、車両のセキュリティ品質を確保するために、車両を製造するための環境・システムのセキュリティ施策が必要となっている。

8. 市場利用・廃棄フェーズでの取組み

車両が製造され、市場で利用されている段階でも、セキュリティ施策の実施が必要である。ここでは市場利用・廃棄フェーズでのセキュリティ施策について説明する。

WP29国連法規では、セキュリティ施策の1つとして、サイバーセキュリティ監視を求めている。サイバーセキュリティ監視とは、サイバーセキュリティインシデント事例、脅威情報、脆弱性情報などの自社製品に関連するサイバーセキュリティ情報を取得し、分析することである。外部から情報を入手する場合、有償または無償で取得できる多様な情報源の中から適切に選択し、継続的かつタイムリーに収集する必要がある。また、社内活動で情報を集める場合の情報の1つには、社内のアセスメントやセキュリティテスト活動で見つかる脆弱性情報がある。これが見つかった場合、必要な改修作業と製品への展開を実施する必要がある。

また監視活動の1つとして、車載IDS（侵入検知システム：Intrusion Detection System）やSOC（Security Operation Center）／SIEM（Security Information and Event Management）の導入が進められている。車載IDSとは、車両に搭載される部品もしくはソフトウェアであり、車両や車載部品が攻撃を受けていることをリアルタイムに検知するための機器である。車載IDSは、車両ネットワークを流れるデータ、部品への通信データ、部品上で動くソフトウェアのふるまいなどを分析し、車両への被害を発生し得る攻撃、もしくはその可能性を分析・検知する。また車載IDSとの組み合わせで、車両向けのSOC運用も利用検討が進められている。車載IDSは車両内にあり、限られたリソースで動作することから、複雑かつ大量なデータを分析することには向いていない。そのため、SOCを構築することで、複数の車両から送られた大量のデータを分析し、攻撃の兆候を捉える。このような施策で総合的にセキュリティ監視することで、セキュリティリスクの顕在化に備える。

また、実際にセキュリティリスクが顕在化した後のPSIRTと呼ばれる組織・活動も重要である。新たな脆弱性情報が検知された、セキュリティ被害が発生している、今後被害が発生する可能性が極めて高い、といった状況では、インシデントレスポンス活動が必要だ。インシデントレスポンスにおいてPSIRTは、製品開発部門、品質管理部門、IT部門などの社内ステークホルダーと連携し、被害の規模、追加被害の可能性や規模などを加味し、インシデントの緊急度に基づく優先度付けをする。そして優先度が高いと判断されたインシデントは、事前に決めたインシデント対応フローに基づき、適切な対応をしていくことが求められる。

9. おわりに

車両のコネクテッド化や自動運転の実現など、車両の未来は社会が求める新しい価値である。このような新しい価値をもたらす車両の登場が、人の生活や社会をより良いものにすることは明確な事実である。一方で、これまで説明したとおり、今後の自動車開発においては、ライフサイクル全般にわたって、サイバーセキュリティ施策の実施が求められる。

次世代モビリティ社会を構築する、つまり、車両の未来をつくるメンバーには、ユーザーへの価値提供と同じように、車両セキュリティ活動を推進することが必要であることを理解することが重要となる。