車両サイバーセキュリティの未来（8）

出荷後のセキュリティ対策 ～ サイバーセキュリティ監視

PwC コンサルティング合同会社　シニアマネージャー　奥山 謙
PwC コンサルティング合同会社　マネージャー　安井 智広

前回は、製造フェーズにおけるセキュリティ活動について考察しました。第8回は、自動車を出荷した後に必要となるセキュリティ活動の在り方について考察します。

出荷後もセキュリティ活動が必要

従来の自動車開発において、製品の品質を高める活動は、出荷前の開発や製造フェーズで実施するものでした。セキュリティ活動と同様に、出荷前のセキュリティ対策が重要であることは、本シリーズでも前回までに紹介したとおりです。ただし、セキュリティの観点では、いくつかの理由で、出荷後であってもセキュリティ対策を実施する必要があります。背景には、製品を能動的に攻撃する攻撃者の存在があります。

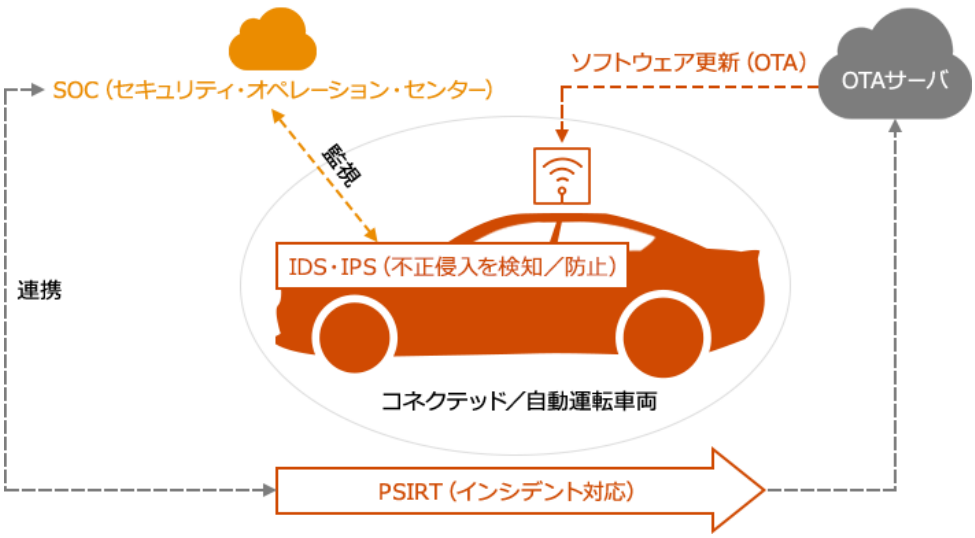
攻撃者は新しい攻撃手法を発見するなど、新たなやり方を試してくることがあります。製品出荷前のある段階では十分な対策であったとしても、新たな攻撃手法が見つかることで、防ぐことのできないものが登場するかもしれません。攻撃を進化させる能動的な攻撃者に対処するためには、製品出荷後のセキュリティ環境の変化に追従するためのセキュリティ対策が必要になってくるのです。

出荷後フェーズにおけるセキュリティ活動の全体像

出荷後に実施すべきセキュリティ対策は、ISO/SAE 21434における「サイバーセキュリティ監視」「脆弱性対応、ファームウェア更新」「インシデントレスポンス」といった活動です（図表1参照）。サイバーセキュリティ監視は車両などを監視し、自動車への攻撃を検知する活動です。脆弱性対応、ファームウェア更新は、出荷後に脆弱性が発見された際に、修正したファームウェアを用意し、車両を安全な状態に更新するもの。インシデントレスポンスは、攻撃を検知した後に、その内容を踏まえて被害の発生を防ぐことを目的としています。

これまでもIT業界では、類似の活動が実施されてきました。IT業界での活動内容やノウハウを、いかに自動車に適用するかを検討することが重要な観点です。

図表1：出荷後のセキュリティ活動の概要



サイバーセキュリティ監視の活動

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、分析することです。サイバーセキュリティ情報には、政府系組織やセキュリティベンダーが提供する外部の情報と、社内のアセスメントで発覚した脆弱性情報といった企業内部の情報という2つに大別されます。

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ります。2019年現在、自動車へ攻撃やインシデント情報が報告される数は多くありません。他方、製品に搭載される脆弱性情報は多く報告されています。これらの情報を確実に入手し、報告された情報が自社に関係するのか、どの程度の影響を及ぼすのかを正しく判断する運用体制の構築が必要になります。

社内活動の場合、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ります。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ります。詳細は、次回の「脆弱性対応、ファームウェア更新」で解説します。

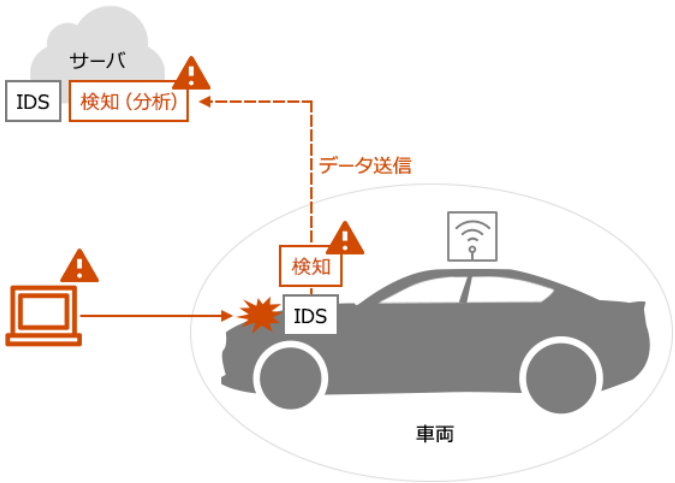
また、社内活動で攻撃情報を入手するための施策として、車載IDS（侵入検知システム：Intrusion Detection System）やSoC（Security Operation Center）／SIEM（Security Information and Event Management）の導入が進められています。外部からの情報だけに頼らない、自社製品に対する攻撃を検知することが導入の狙いです。

攻撃情報収集に役立つ車載IDS、車両向けSoC

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す。車載IDSはネットワーク型とホスト型などの種別があり、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・検知します。攻撃者の攻撃に対応するためには、まずは攻撃の発生を特定できなければ活動を開始することができませんので、先に説明した攻撃者の存在を踏まえれば、今後特に重要になる技術と言えます。

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ます。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ません。そのため、車載IDSでは簡易な分析にとどめ、クラウド環境などに用意したSoCに必要なデータを送信し、複雑な分析などを任せる構成をとります。SoCは、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役割を担います。また、SoCで特定車両に対する攻撃が発見した場合に備え、SoC側から当該車両に指示を送り、通信遮断などの対処を開始する機能も合わせて構築することで、将来のサイバー攻撃に備えます。（図表2参照）

図表2：リアルタイムで車両への攻撃を検知・対応



お問い合わせ

PwCコンサルティング合同会社
〒100-6921　東京都千代田区丸の内2-6-1 丸の内パークビルディング
Tel：03-6250-1200（代表）　Mail：jp_cyber_inquiry@pwc.com