自動車サイバーセキュリティ対応における直近の課題について

2024 年 7 月から、日本においても型式認証の際、サイバーセキュリティ審査が全ての新型車両（OTA 対応/非対応問わず）で必須となりました。この審査では個別の車両のセキュリティに加えて、サプライチェーン全体のサイバーセキュリティ管理の仕組みも問われることとなります。2024 年は、国内だけでなく、各国・地域で法規化および適用、ガイドライン発行が行われており、自動車メーカーおよび車載システムサプライヤーは、その影響を受けているのではないでしょうか。本メルマガでは、昨年の各国・地域における自動車サイバーセキュリティに関する動きと、そこから見える直近の課題について触れます。

欧州では、UNECE WP.29 のサイバーセキュリティ規則（UN-R155、UN-R156）が、2022 年 7 月以降、新型車両に適用され、2024 年 7 月に適用範囲が「継続生産車両」に拡大されました。これにより、自動車メーカーは新型車だけでなく、すでに販売されている車種にもサイバーセキュリティ対策を適用する必要があります。

昨年、欧州の自動車メーカー（OEM）によるサプライヤー選定時に実施されたポテンシャル分析結果を見る機会がありました。その中で、「サイバーセキュリティの運用」の側面で、インシデント対応や脆弱性管理の中核を担う PSIRT 体制（組織内部、顧客とのインタフェースなど）、PSIRT 活動フローに関する評価項目が含まれていました。そのことから、サプライヤー選定時に、エンジニアリング能力だけでなく、製品ライフサイクルにわたるサイバーセキュリティ管理の能力が評価されていることがうかがえます。少なくともインシデント対応や脆弱性管理を実行できる仕組みが準備、展開できていることが求められていると考えられます。

続いて、米国の動きについて触れます。NHTSA（米国国家道路交通安全局）は、2024 年 12 月にサイバーセキュリティガイドラインを更新しました。このガイドラインは、リモート攻撃の増加、OTA（Over-the-Air）更新の安全性、サプライチェーンの脆弱性を考慮して、過去に発行した「Cybersecurity Best Practices for the Safety of Modern Vehicles（2016 年初版、2022 年更新版）」を基に更新されています。具体的には、以下の 3 つのポイントに焦点を当てています。

- OTA アップデートのセキュリティ強化：ソフトウェア更新前認証の義務付け、デジタル署名の導入、更新中のデータ暗号化と改ざん防止策の強化
- OEM のサイバー攻撃対応義務：自社製品のサイバーセキュリティ管理システム（Cybersecurity Management System：CSMS）策定の義務化、インシデント発生時の対応手順の明確化（PSIRT）と迅速な報告義務
- サプライチェーンのセキュリティ監査の強化：主要サプライヤーやソフトウェア開発企業へのセキュリティ要件の適用、企業間での情報共有強化によるサプライヤーチェーン全体のリスク管理の徹底

最後に、自動車業界にとって重要な国の一つである中国の動きについて触れます。2024 年 9 月に 3 つの法規「GB 44495-2024 自動車完成車情報セキュリティ技術要件」、「GB 44496-2024 自動車用ソフトウェアアップデートの一般技術要件」、「GB 44497-2024 インテリジェント・コネクテッド・ビークル自動運転データ記録システム」が発行されました。GB 44495-2024 と GB 44496-2024 は、2026 年 1 月以降に型式申請した車両から適用されます。

その中でも、GB 44495-2024 は、UN-R155 および ISO/SAE 21434 への準拠が前提になりますが、適合性評価（OEM やサプライヤーが準拠すべき認証プロセス）と試験要件（脆弱性テスト、ペネトレーションテストの実施義務）が具体的に規定されているのが特徴です。

また、自動車業界およびサイバーセキュリティ団体（Auto-ISAC、J-Auto-ISAC、JASPAR など）の活動に着目すると、この 2 年位の期間で、業界共通の課題として取り組んでいる「SBOM の標準化」活動が報告されています。例えば、1 月 17 日に Auto-ISAC の SBOM ワーキンググループから発行された「Auto-ISAC Software Bill of Materials (SBOM) Informational Report」では、CSMS の一要素である PSIRT における脆弱性管理、インシデント対応、ソフトウェアアップデートの仕組み、サプライヤーチェーンのリスク管理への適用と課題が報告されています。

前述の各国・地域の動き、サイバーセキュリティ団体の活動から、今年は OEM、サプライヤーの各社にとって、CSMS およびソフトウェアアップデート管理システムの確立と維持、サプライヤーチェーンにおけるセキュリティ対応がより優先度の高い課題になると考えられます。各社で課題に対応する中で、業界活動の成果（標準化）を参考にする、または取り入れることがポイントになります。今後は、当社の経験に基づいた具体的な課題解決のヒントをメルマガやセミナーで紹介していきます。

2025/2/20 小西 晃輔

【関連セミナー】
「サイバーセキュリティセミナーシリーズ　～各国の動きと課題～」
日時：2 月 28 日(金) 8 時 30 分～9 時（30 分）
URL：https://biz3.co.jp/publictraining/7012