「サイバーセキュリティの搭載は、車両の型式認証のための前提条件となりつつあります」

Moritz Minzlaff 博士に聞く、戦略的課題としての車載セキュリティ

車両のセキュリティ要件の増加に伴い、新たな規格と法規が必要になってきています。このインタビューでは、自動車業界が対応すべき問題について、ESCRYPT のベルリンオフィスでシニアマネージャを務める Moritz Minzlaff 博士に説明いただきました。

Minzlaff 博士、車載セキュリティ分野で拘束力のある規格と法規を作成する取り組みが現在本格化していますが、ここでは特にどのような開発分野が注目されていますか？

現在、誰もが注目している 2 つの取り組みがあります。その 1 つは、プロセスレベルでの基準を設定する ISO/SAE 21434 であり、もう 1 つは、サイバーセキュリティを車両の型式認証の前提条件にしようとする動きである UNECE WP.29 です。UNECE の規定と ISO の仕様はどちらも、今後 3 年以内に施行される予定です。つまり、準備のための時間はあまり残されていません。

それでは、近い将来、車両の型式認証に一定の IT セキュリティが求められるようになるということですね。

その通りです。将来的に、OEM メーカーは UNECE 仕様に従って適切なリスク処理を行える体制を整えなければ、EU や日本などの市場で車両型式の認証ができなくなります。ISO/SAE 21434 は、このハードルを越えるための鍵となる動きであり、自動車産業に共通のセキュリティ規格を提供することを目的としています。また、これ以外にも多くの規制や法律が地域レベルで絶えず進展しているということにも留意しなければなりません。

自動車メーカーやサプライヤが直面している特有の課題には、どのようなものがありますか？

大きな課題として挙げられるのは、セキュリティが将来的にはサプライチェーンとライフサイクル全体にわたって総合的にアプローチしなければならないものとして捉えられていることです。もはや、セキュリティ機能を備えた 2 ～ 3 個の中央 ECU を車両に搭載するだけでは不十分なのです。車両メーカーは、プラットフォーム全体を通じてクリティカルな要素を特定し、フェーズアウトまでのすべての段階において安全を保証する必要があります。つまり、ライフサイクル管理が今後、非常に重要な問題になるということであり、どうすれば、ネットワーク接続を備えた車両の生産を開始した後でもリスクベースの保護をしっかりと確立できるかということです。出荷された車はその後何年にもわたって絶えず変化する脅威のランドスケープにさらされるのですから。

OEM メーカーやサプライヤが、車両保護を企業活動における永続的な取り組みとして定着させるために今すべきことは何でしょうか？

それには 2 つの側面からアプローチする必要がありますが、まずは製品のセキュリティ要件を特定することが必要です。車両やコンポーネントには多様な接続形態があり、搭載される機能や安全関連度、自動運転レベルなどもさまざまですが、それぞれに専用の保護が必要となります。これらを識別して必要なセキュリティレベルを特定し、それを実装するには、開発、生産、品質保証、販売、カスタマーコミュニケーションといったすべての関係者が連携して作業する必要があります。また、責任や役割は、社内だけでなくサプライチェーン全体で明確に定義しなければなりません。

また、「棚卸し」、つまり監査やアセスメントを標準的な手順で実施することも必要でしょう。自社のどの領域が基準を満たし、どの領域がそうでないか。将来的な規制要件のどの側面に既に対応できているか。どのような既存のプロセスをベースにすれば、将来のプロセスを構築できるか。このようにしてギャップ分析を行えば、今後の開発においてセキュリティのどの分野に投資すれば最も効果的かを明らかにすることができます。

ESCRYPT のようなセキュリティ専門企業と提携することは有効でしょうか？

もちろんです。なぜなら、当社の独立した視点と業界全体にわたるグローバルなノウハウを活用すれば、お客様の専門知識を理想的に補完できるからです。ネットワーク接続を備えた車両を継続的に保護するための唯一の方法は、関係者が連携して包括的なアプローチを取ることです。そのため、ESCRYPT では、標準的なコーポレート IT セキュリティと組み込み型セキュリティを統合したソリューションを提供しています。将来のサイバーセキュリティに対応するための唯一の方法は、車両やアプリからクラウドに至るまで、すべての領域を対象にした対策を取ることです。

Moritz Minzlaff 博士
ESCRYPT シニアマネージャ

当社では、さまざまなメーカーやサプライヤと連携してすべての主要マーケットで広範なプロジェクトを遂行してきた経験を基に、ベンチマークを提供することも可能です。また、お客様が現在実施しているセキュリティ対策をさまざまな側面から検証し、さらなる開発が必要な部分を正しく特定することで、サイバーセキュリティの確立に向けて投資すべき対象を見つけるお手伝いをすることができます。残された時間は短いですが、UNECE 仕様に準拠した型式認証を達成できないことのリスクは膨大であり、また達成するにしても期限に間に合わないことや多大なコストがかかるといったことは避けなければなりません。ESCRYPT には深いエンジニアリング経験があります。当社のノウハウをご活用いただければ、お客様は量産段階での車載セキュリティを適切に構築し、今後の課題の解決への道を切り拓くことができます。■

「ネットワーク接続を備えた車両を継続的に保護するための唯一の方法は、関係者が連携して包括的なアプローチを取ることです。」