車両サイバーセキュリティの未来（10）

車両の進化のために

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

これまでに、ISO/SAE 21434からの示唆をもとに、車両開発・製造・出荷後に求められるセキュリティ活動について考察してきました。最終回となる第10回は、これまでのセキュリティ活動の考察全体を振り返り、個々のセキュリティ活動のつながり・連携について改めて確認します。あわせて、本連載のテーマである車両サイバーセキュリティの未来についても考察します。

ユーザー視点の意義 - 車両ライフサイクル全体を通じたセキュリティ活動 -

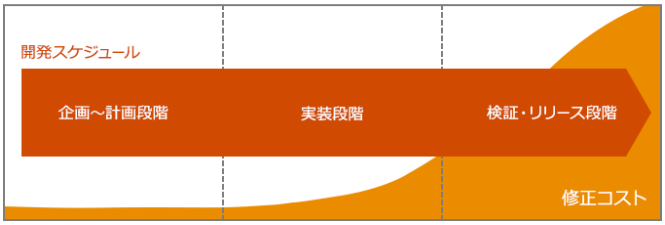
ISO/SAE 21434は、車両のライフサイクル全体を通じてサイバーセキュリティ活動に関するプロセスの定義を目的としていました。車両のライフサイクル全体とは、車両の企画・研究から始まり、設計・実装・検証を経て、製造・出荷され、市場にて運用・廃棄されるまでの、車両の開発・運用に関する全ての活動を意味します。そして、その全ての活動においてサイバーセキュリティの取り組みを実施することが求められています。

車両ライフサイクル全体の全ての工程・活動においてセキュリティ活動が求められる理由にはいくつかの要因があります。一つは、車両ライフサイクルの全ての工程に、セキュリティリスクの原因となる脆弱（ぜいじゃく）性（セキュリティ観点での欠陥）が入り込む余地があるためです。製品開発の段階でも、工場における製品の製造段階でもこのような脆弱性が入り込む可能性はあります。また、万一入り込んでしまった場合、その脆弱性を出荷後に取り除くためには、車両が市場に投入された後のセキュリティ活動も必要になります。このような脆弱性が残った状態では、車両ユーザーがセキュリティ被害に遭う可能性がぬぐい切れません。ユーザー被害を防ぐためには、車両ライフサイクル全体でセキュリティ活動を実施する必要があるのです。

メーカー視点の意義 - 車両ライフサイクル全体を通じたセキュリティ活動 -

車両ライフサイクル全体でセキュリティ活動が求められるもう一つの理由には、セキュリティ対策の効率性向上が挙げられます。脆弱性、もしくは脆弱性が入り込む要因が発生した直後でなく、別工程で対策をすると多くのコストがかかることが分かっています。（図表1参照）製品開発が後工程になるほど、作成される設計書・ソースコード・テストデータなどの成果物が増え、それらの中から問題の原因となった脆弱性を見つけ、すでに開発された別個所に影響を与えない必要十分な対策方法を検討し、実際の対応を実施する必要があるからです。ISO/SAEなどが求める車両ライフサイクル全体でのセキュリティ活動実施の要請は、単純にユーザーをセキュリティ被害から守るためだけを考えたものではなく、実は車両メーカーにとっても「効率化」というメリットのある活動の示唆でもあったのです。車両メーカーは、車両のユーザー・メーカーなど、車両を取り巻く社会全体の利益のためにも、車両ライフサイクル全体で活動することが最も良い選択であると理解することが重要になります。

図表1



ひとつなぎのセキュリティ対策

車両ライフサイクル全体での活動の意義について整理しましたが、各フェーズのセキュリティ活動のつながりについても考察を進めます。今回の連載では、コンセプトフェーズ、設計フェーズ、実装フェーズ、テストフェーズ、製造フェーズ、出荷後フェーズといったフェーズ別にセキュリティ活動を整理しました。実際の活動でも、フェーズ別に担当者が変わり、担当者（実施者）と責任者は異なることが一般的です。（図表2参照）

では、セキュリティ活動がフェーズ別に担当者と責任者で異なることは、各セキュリティ活動がそれぞれ独立した活動であることが理由なのでしょうか。実際には、各フェーズのセキュリティ活動は独立していることはなく、前後の活動が密に関係しています。例えば、コンセプトフェーズで洗い出した脅威は、セキュリティテストフェーズで追跡確認し、必要に応じてテスト項目として評価する必要があります。同じ脅威は、出荷後の監視活動でも、監視対象とすべき内容です。このように、製品ライフサイクルのフェーズ別にまとめた活動は、実際には相互に密に連携するべき活動なのです。

上述のとおり、フェーズ別にセキュリティ活動の担当者と責任者が異なることがありますが、実態は相互に連携した活動であることを理解し、各活動の担当者と責任者間で情報共有や連携を深めることが、本来目指すべきセキュリティ活動であると理解することが重要です。

車両サイバーセキュリティの未来

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す。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す。

一方で、これまで考察してきたことから分かるように、今後の自動車開発においては、製品ライフサイクル全体の全てのフェーズで、確実にサイバーセキュリティ施策を進めていくことが求められます。一カ所でもセキュリティ活動の不備不足があれば、それが原因で開発された車両やそのオーナーがセキュリティ被害に遭う可能性があります。

つまり、サイバーセキュリティ活動が正しくなければ、新しい車両のユーザーは新しい価値を得ると同時にセキュリティ脅威にさらされてしまうことになります。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、ユーザーをセキュリティ被害から守るため、車両セキュリティの活動を推進する責務があります。車両セキュリティ活動を推進することが、新しい車両の未来を創る権利が得ることを理解する必要があるのです。

図表2
開発スケジュール

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