車両サイバーセキュリティの未来（9）

出荷後のセキュリティ対策の要PSIRT

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

出荷後フェーズにおけるセキュリティ活動の振り返り

前回解説したとおり、車両および車両システムのセキュリティ対策は、多くのステークホルダーと連携しつつ、車両のライフサイクル全般で取り組まなければなりません。その中で市場利用（販売後）のフェーズにおけるセキュリティ対応で中心的な役割を担う体制が、PSIRT（Product Security Incident Response Team）でした。そしてPSIRTが活躍する主な活動は、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」となります。

「脆弱性対応、ファームウェア更新」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、分析することでした。この活動で対応すべき脆弱性情報と判明した場合「脆弱性対応、ファームウェア更新」の活動を実施します。

新たに取得した脆弱性情報の内容を評価し、必要な対応を迅速に判断するために、企業は、事前に自社独自の評価基準を用意しておくことが求められます。

脆弱性情報の評価基準は、標準化団体など※1を参考に各企業が作成すべきものですが、「影響度（安全性、財務、利便性、個人情報への影響など）」「発生可能性（脆弱性悪用の難易度、所要時間など）」といったフレームに基づき、統合的に評価できる基準が必要です。

例えば「任意の不正なCAN※2メッセージを車載制御ネットワークへ送信することが可能な脆弱性」と「カーナビの操作が行えなくなる脆弱性」では、安全性への影響の大きさが異なるため、発生可能性が同じケースであれば、前者の脆弱性の深刻度が高くなると考えられます（図表1参照）。

影響度の評価を適切に実施するためには、各種ソフトウェア（オープンソースソフトウェア<OSS>、自社ソフトウェア、他社ソフトウェア）やプロトコルがどの製品のどのバージョンで利用されているかの情報を管理し、脆弱性情報の影響範囲を迅速、正確に把握できることが必要です。

図表1：脆弱性評価基準のマトリックス

脆弱性がもたらすリスクの大きさ（深刻度）＝ 影響度 × 発生可能性

		影響度				
		0	1	2	3	4
発生可能性	1	小さい	小さい	中程度	中程度	大きい
	2	小さい	小さい	中程度	大きい	大きい
	3	小さい	中程度	大きい	大きい	非常に大きい

【脆弱性評価基準のマトリックス（イメージ）】
影響度、発生可能性の評価スコアに基づき、脆弱性の深刻度（Critical／High／Medium／Low）を設定する。

脆弱性情報の評価においては、コンセプトフェーズや製品開発フェーズで実施された脅威分析との関係も重要です。外部から車両システムへの攻撃は、単一の脆弱性情報を利用する場合だけではなく、複数の脆弱性を利用することが多いです。脅威分析において、顕在化する可能性が低いと分類され、対応が先送りされた特定の脅威シナリオが、新たな脆弱性情報の出現で、顕在化可能性が高まり、優先度が高くなる場合があります。新たな脆弱性情報の出現は、既に実施済みの脅威分析への影響も確認し、適切に反映することが求められます。

「インシデントレスポンス」の活動

新たな脆弱性情報が検知されるだけでなく、既に被害が発生している状況（例えば、脆弱性悪用で自社の製品が保有する個人情報の流出、自社製品の設定情報の改ざんなど）や、今後被害が発生する可能性が極めて高い状況（例えば、自社製品を遠隔操作する手法の存在を研究者が一般公開し、自社と同構成の類似製品がハッキングされるなど）では、PSIRTを中心に社内で適切に連携しつつ、対外的な説明を行う「インシデントレスポンス」の活動が必要です。

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（インシデントトリアージ）を行います。そして優先度が高いと判断されたインシデントは、事前に決められたインシデント対応フローに基づき、適切なレベルのマネジメント層に速報を行った上で、対応を実施していくことが求められます。こうした一連の流れは、PSIRTが主体となって実施するものの、円滑な対応には、各部門の習熟が必須となるため、事前に訓練が実施されるのが望ましいです。

検知したインシデントの原因が判明し、被害を防ぐ（または最小化する）ための対策が明確となれば、多様なステークホルダーと連携し、対策を実行することが必要となります。特にユーザーが所有する車両や車両システムになんらかの変更（利用方法、設定、ソフトウェアなど）をするために、ユーザーの行動や承認が必要となる場合は、注意が必要です。

例えば「ファームウェアの脆弱性でリモートから任意のCANメッセージが実行可能なため、ファームウェアのアップデートが必要」な状況で、改修のために「正規ディーラーへの持ち込みが必要」な場合と「無線通信（OTA）で自動にアップデートが実行される」場合とでは、ユーザーの負担に差異があります。ユーザーの負担が小さく、実施しやすいのは後者だと考えられます。つまり販売後の製品を継続可能な形で円滑、迅速にアップデートできる仕組みが求められます。

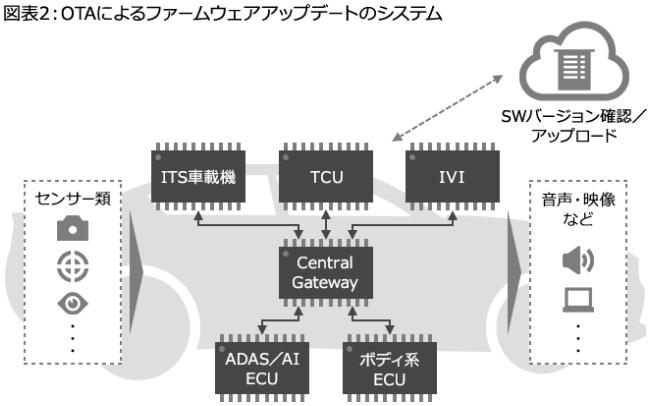
こうしたアップデートの仕組み（図表2参照）はコンセプトフェーズや製品開発フェーズで方針を検討し、実装していかなければなりませんが、PSIRTは、脆弱性やインシデント対応の経験から適切な示唆を導出し、コンセプトフェーズや製品開発フェーズのインプット情報を提示する役割も担うことが必要となります。

今回までの内容で、自動車における新たなサイバーセキュリティ活動についてフェーズごとにその内容を考察してきました。最終回となる次回は、これまで考察した取り組みを振り返り、今後の自動車開発におけるセキュリティ対策を整理し、自動車の将来について考察します。

※1：日本では、JPCERTがCVSSによる脆弱性の評価結果を公開している

※2：自動車などの内部で、電子回路や各装置を接続するための通信ネットワーク規格

図表2：OTAによるファームウェアアップデートのシステム



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