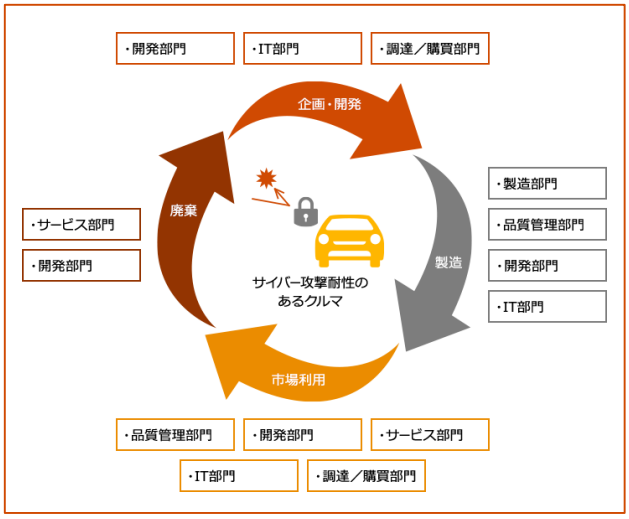
車両サイバーセキュリティの未来（2）

車両セキュリティにおける組織ガバナンスとプロセス管理

PwC コンサルティング合同会社　マネージャー
奥山　謙

組織ガバナンス

車両サイバーセキュリティ活動の目的は、車両に関するサイバーセキュリティリスクを管理（最小化）することにあります。それには、車両ライフサイクルにかかわる全ての組織が適切なセキュリティ対策を実施することが必要です。これを遂行するためにセキュリティ施策の遂行を意識した「組織」と「プロセス」を定義することで、セキュリティリスクを管理できる体制をつくります。このようなセキュリティ施策を実施するための組織とプロセスを構築する活動が「サイバーセキュリティ管理」です。第2回はサイバーセキュリティ管理について考察します。



始めに「組織」の管理について説明します。組織として、ライフサイクル全体を通じて必要十分なサイバーセキュリティ活動を実施するためには、サイバーセキュリティ活動を全体統括する組織がガバナンスを効かせることが必要です。現場由来のボトムアップのセキュリティ施策では、局所的には有効であっても、組織全体としては非効率になりがちなためです。そのため、会社経営としてサイバーセキュリティ活動を捉え、ガバナンスを推進する必要があります。

組織ガバナンスでは、組織として方針を定め、目標や戦略を定めることが必要です。サイバーセキュリティにおいても同様で、サイバーセキュリティの方針、目標、戦略立案を定めることが基本です。適切な目標・戦略を定めるためには、車両がおかれたサイバーセキュリティ環境を正確に理解することが求められます。特に、車両や車両部品に対するサイバーセキュリティ環境は近年変化が激しく、最新の攻撃手法やセキュリティ対策動向の把握は重要です。

ここで一つ注意すべき事項があります。セキュリティ分野で先行するIT・Webシステム向けセキュリティ技術の活用についてです。エンドユーザーによって使われる車両を始めとした製品分野では、出荷後の対応は容易ではないため、出荷前の品質作り込みに重点がおかれます。他方、IT・Webシステムでは運用開始後の改修も比較的容易です。このような品質への取り組み・前提条件の差から車両業界では先行するIT・Web分野の技術活用に慎重になっています。これは車両開発の視点では正しい判断である一方、IT技術の進化から取り残されるリスクにもなり得ます。そもそも車両にセキュリティ施策が必要となった理由は、車両が最新のIT技術によって進化しており、サイバーセキュリティの最新技術を適切に利用することが必要な環境へと変化していることにあります。最新のセキュリティ技術活用は難しい判断が必要なため、組織としてセキュリティ技術活用の責任所在を明確するためにもCSTO（Chief Security Technology Officer：最高セキュリティ技術責任者）などの役割も必要になるでしょう。

目標、戦略、技術責任を明確化した後は、戦略を実現するための準備が必要です。特に重要なものが、予算や人材を確保し、サイバーセキュリティ活動を始める体制を整えることです。それと同時に、規則やガイドラインといった、組織としてのサイバーセキュリティ活動に関する道しるべが必要です。これがサイバーセキュリティ管理におけるもう一つの要素である「プロセス」の管理です。

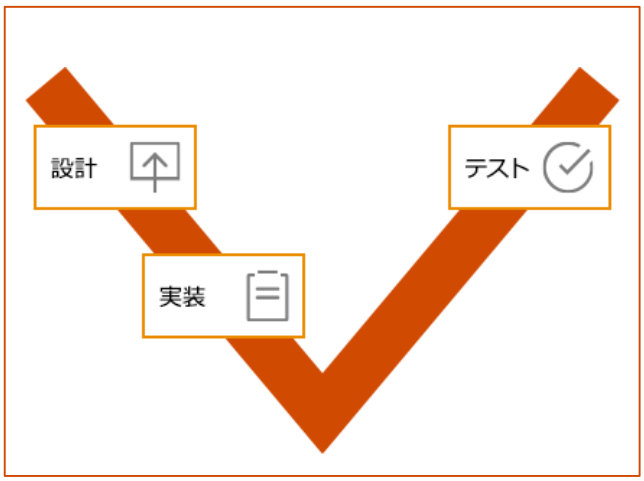
pwc

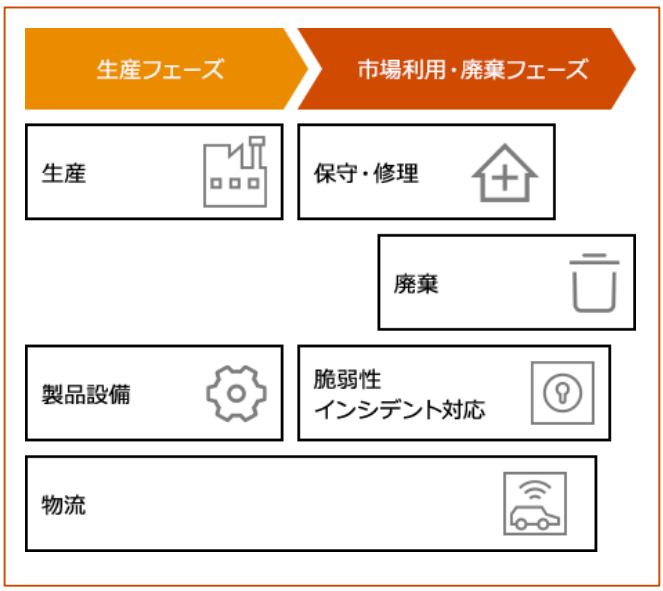
サイバー攻撃への能動的対応

車両開発のプロセスはセキュリティ観点で大きく二つに分けて考えられます。一つは製品開発フェーズ（コンセプトフェーズを含む）のプロセス、もう一つは製造・運用・メンテナンスフェーズのプロセスです。

製品開発フェーズでは、企画・設計・実装・検証の各フェーズで必要となるセキュリティ施策を定義します。組織管理と同様に、車両が持つ機能や社会・利用環境などを考慮した上で、開発する車両に潜むサイバーセキュリティの脅威を識別し、開発製品のセキュリティのゴール・目標を定めることが出発点になります。製品開発フェーズ全体のセキュリティ目標が定まった後、設計・実装工程で定めたセキュリティ目標に沿って確実に開発し、検証工程で目標の達成を確認することがエッセンスです。このフェーズは従来のものづくりの考え方そのものであり、自動車OEMメーカー・サプライヤーが得意とする領域です。

製造・運用・メンテナンスフェーズでは、セキュアに開発された車両をセキュアな状態に保つことを目的として活動を定義します。製造工程では1台1台の車両が開発時に想定したセキュリティ品質を保つ仕組みが必要です。そのため製造作業を行う環境（工場）のセキュア化を実施します。なお、近年では製造時にセキュリティ対策のため暗号鍵を埋め込むなどの施策が進んでおり、よりセキュアな環境が求められる点に留意する必要があります。運用・メンテナンス工程では、車両がサイバー攻撃を受けているか、被害が発生しているか、被害を受けやすい欠陥（脆弱性）が見つかっていないかなどの監視活動と、問題検知後の迅速な対応が必要となります。故障や経年劣化といった事故対応は以前からあるものの、能動的なサイバー攻撃への対応は自動車OEMメーカーやサプライヤーでは実施されてこなかった領域であるため、これらの活動は効率的なセキュリティ対策実施に向けて特に重要となります。





今回は、サイバーセキュリティ管理の観点からセキュリティ施策を解説しました。次回以降は今回概要を紹介した各プロセスにおけるサイバーセキュリティ活動について、具体的な活動内容を紹介しつつ、サイバーセキュリティリスクを管理する活動のあり方について考察を進めていきます。

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