車両サイバーセキュリティの未来

pwc

www.pwc.com/jp

はじめに

車両のデジタル革命によって新たなモビリティ社会が夜明けを迎えつつあることを、『Strategy&デジタル自動車レポート2018』は伝えています。利用者が求める利便性と、実用化されつつあるCASE（コネクテッド、自動化、シェアリング、電動化）技術が提供するサービス間のギャップも小さくなっており、次世代のモビリティ社会が形作られています。一方、モビリティ社会の変化は必ずしも技術の進化のみで決定されておらず、各国の政策や規制により変化の速度が決定されている面があります。その要因の一つがサイバーセキュリティへの懸念です。

近年よく言われるように、車がネットワークにつながることで利便性は向上してきました。しかし同時にサイバー攻撃の脅威にさらされるようにもなりました。このことは自動車メーカー・自動車部品サプライヤーでは課題として既に認識されており、特に車両開発の場面で、サイバーセキュリティ対策が実施されています。また、さまざまな団体から車両サイバーセキュリティに関する指針やガイドラインも公開されています。国際的な動きとして特に重要なものが、自動車基準調和世界フォーラム（WP29）ならびに本レポートの題材である国際標準規格のISO/SAE 21434です。

WP29は、国連欧州経済委員会（UN/ECE）の下部に設けられ、専門分科会にて車両サイバーセキュリティに関する検討が進められており、サイバーセキュリティ対策のRegulation（義務化）も検討されています。ISO/SAE 21434は、2020年頃に策定予定の車両サイバーセキュリティに関する国際標準規格です。ISO/SAE 21434では、路上を走行する車両および車両のシステム・部品・ソフトウェアと車両からネットワークでつながる外部デバイスまでを対象とした、サイバーセキュリティ対策の管理・実施が規定される見込みです。任意規格ですが、義務化が検討されているWP29が参照するため、業界へ大きな影響を与えます。

このようなサイバーセキュリティ対策の義務化・標準化によって、事業者には追加のセキュリティ施策の実施が求められる可能性があります。サイバーセキュリティ施策は、利用者の安全性確保の観点では必須ですが、やみくもにサイバーセキュリティ施策を実施してしまうと、車両・モビリティサービスの価格高騰やリリース遅延など、利用者への不利益も発生し得ます。そのため、国際標準規格などで求められるサイバーセキュリティ施策を正しく理解した上で、効果と効率をともに最大化し、実施を進めることが重要です。

本レポートでは、ISO/SAE 21434を題材として、今後実施が求められるサイバーセキュリティ施策をひもといていきます。

目次

1 技術革新の道しるべとなる国際標準規格（WP29 UNRとISO/SAE 21434）

本章ではまず、車両セキュリティの指針となるWP29 UNRとISO/SAE 21434について考察します。

WP29 UNR

WP29 UNRは、国連欧州経済委員会（UN/ECE）下の自動車基準調和世界フォーラム（WP29）で作成された国連規則（UNR）で、車両の開発・生産／生産後におけるサイバーセキュリティ要件が規定されています。WP29には複数の専門分科会があり、テーマごとに議論が進められています。その中の一つである自動運転専門分科会（GRVA）では日本が副議長を、さらにGRVAの会議体の一つであるサイバーセキュリティタスクフォースでは日本が英国と共同で議長を務めています。このように、日本が国際的な車両サイバーセキュリティ対策のグローバル標準化をリードする形で規則の制定を進めています。

GRVA／サイバーセキュリティタスクフォースでは、車両におけるサイバーセキュリティ要件などが検討されています。GRVA／サイバーセキュリティタスクフォースでの主要検討項目であるサイバーセキュリティ法規においては、サイバーセキュリティに関してプロセスとプロダクトの二つの観点で認証が求められています。サイバーセキュリティ法規は「国連の車両等の型式認定相互承認協定（1958年協定）」「国連の車両等の世界技術規則協定（1998年協定）」に基づく従来の車両認証制度にサイバーセキュリティの観点が追加されたものです。

プロセス面では、認証当局により車両メーカーのプロセス認証（体制や仕組みの認証と監査）が初期・3年ごとに行われる予定です。これは、従来の車両認証制度と異なり、開発した車両の品質だけでなく、車両を開発・生産する車両メーカーの、組織活動の品質が確認されることを意味しています。これにより車両メーカーでは、車両の開発・生産にかかわる全ての関連部門を含めたプロセスの構築が必要となります。プロダクト面では、上述の認証されたプロセスに従って車両が開発・生産されていることの実証が求められます。

プロセスおよびプロダクトに対するセキュリティ要件の概要は以下のとおりです。

プロセス要件
• 車両メーカーがサイバーセキュリティマネジメントシステム（CSMS）を備え「開発段階」「生産段階」「生産後の段階」にわたって導入していること
• 車両に対するリスクの特定・評価・分類・対処のプロセスが使用され、適切に管理されていることが検証されており、かつ、最新の状態に維持されていること
• 車両のセキュリティを試験すること
• 車両に対するサイバー攻撃を監視・検知・対応するプロセスが使用されていること
• サイバー脅威および脆弱性を特定し、新たに生じたものに対応するプロセスが使用されること

プロダクト要件
• 本規則で必要とされる情報をサプライチェーンを通じて収集し、検証すること
• 適切な設計および検証の情報を維持すること
• 車両およびシステムの設計において適切なセキュリティ対策を実施すること
• 車両生産後のサイバーセキュリティをサポートする手段を実施すること

ISO/SAE 21434

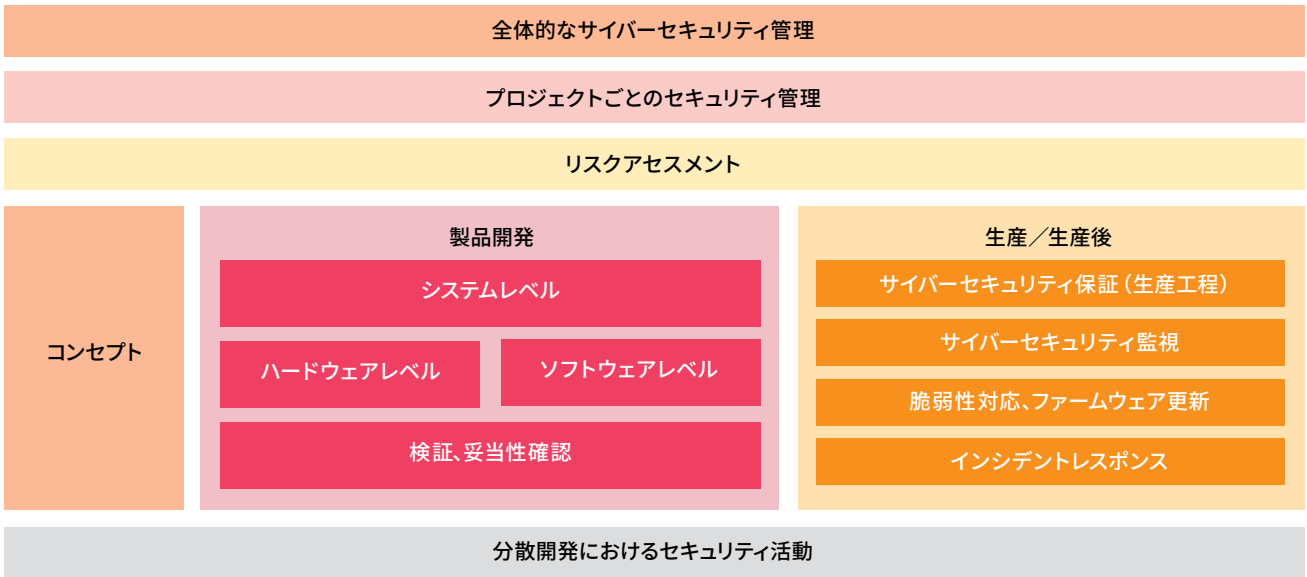
ISO/SAE 21434は、車両のライフサイクル全体を通じてサイバーセキュリティ活動に関してのプロセスを定義することを目的としています。車両のライフサイクル全体とは、車両の企画・研究から始まり、設計・実装・検証を経て、製造・出荷され、市場にて運用・廃棄されるまでの、車両の開発・運用に関する全ての活動を意味しており、その全ての活動においてサイバーセキュリティの取り組みを実施することが必要となります。このようなプロセスにより、サイバー攻撃や、攻撃による被害の発生リスクを減らすことが期待されています。

ISO/SAE 21434は、大きく分けると次の7つの要素から構成されます（図表1参照）。

1. 全体的なセキュリティ管理：サイバーセキュリティに特化もしくは重点を置いた、組織としてのポリシーや戦略の策定、体制・プロセスの整備、セキュリティ文化・意識を醸成する活動の規定、品質マネジメントシステムの構築・維持、利用されるツールのセキュリティ観点の評価などの活動の規定
2. プロジェクトごとのセキュリティ管理：プロジェクトにおけるサイバーセキュリティ体制の明確化や、セキュリティ活動計画、脆弱性対応・管理、実施した施策の有効性評価などの活動の規定
3. リスクアセスメント：いわゆる一般のリスクマネジメント手法をベースとして、セキュリティリスクを分析・算定・対応するための活動の規定
4. コンセプトフェーズ：車両開発におけるコンセプトフェーズにて実施するサイバーセキュリティプロセスおよび活動の規定
5. 製品開発フェーズ：車両開発時において既存の開発プロセス・活動に対して、追加されるサイバーセキュリティプロセス活動の規定
6. 生産／生産後フェーズ：製品開発後の製造および出荷後の運用時に実施すべきサイバーセキュリティ活動の規定
7. 分散開発におけるセキュリティ活動：サプライチェーン全体の相互関係・役割分担の定義

次章以降は、上記のサイバーセキュリティ活動のうち実施時に注意を必要とする事例を取り上げて、活動の進め方について考察します。

図表1：ISO/SAE 21434の7つの要素



出典：ISO/SAE DIS 21434を引用しPwCが作成（2020年2月現在）

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

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。

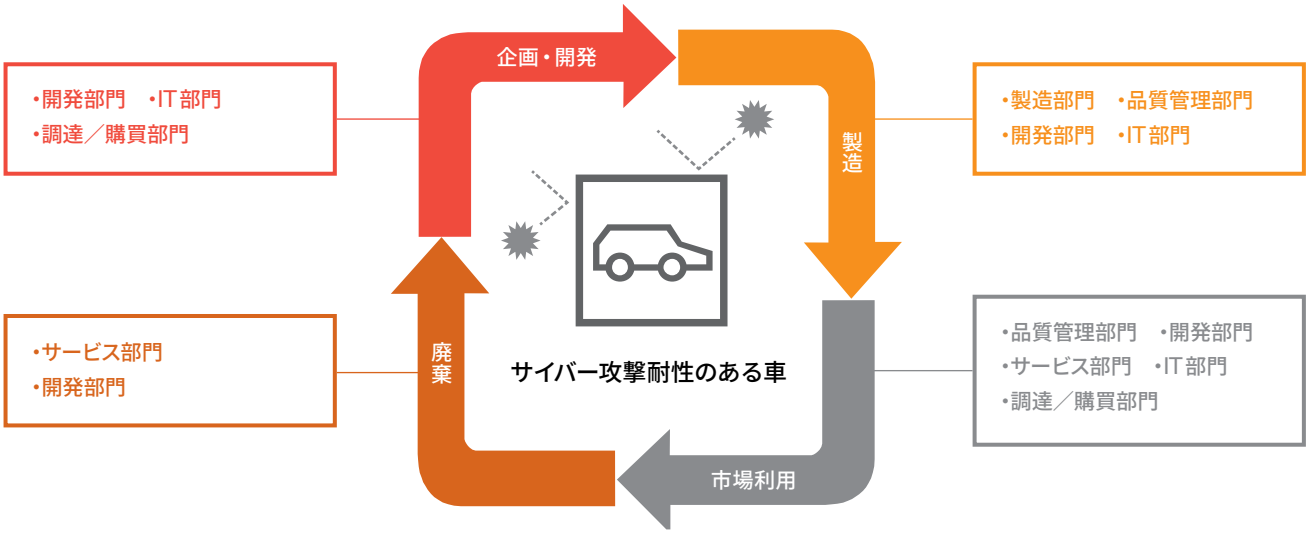
組織ガバナンス

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（図表2参照）。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、車両が置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、出荷後の対応が容易ではないため、出荷前の品質作り込みに重点が置かれます。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を要することから、組織としてセキュリティ技術活用の責任所在を明確にするためにも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。

図表2：ライフサイクル全体を通じた、サイバーセキュリティ活動のための組織管理



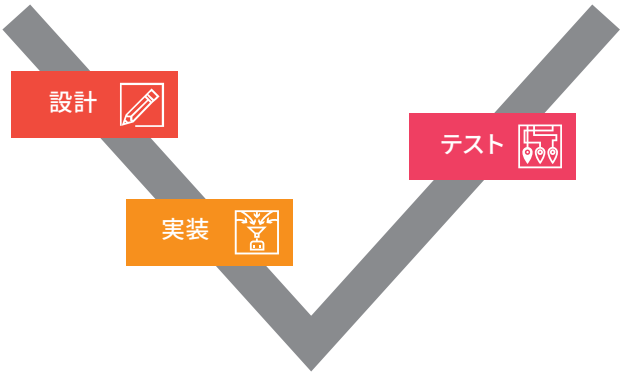
目標、戦略、技術責任を明確化した後は、戦略を実現するための準備が必要です。特に重要なのが、予算や人材を確保し、サイバーセキュリティ活動を始める体制を整えることです。それと同時に、規則やガイドラインといった、組織としてのサイバーセキュリティ活動に関する道しるべが必要です。これがサイバーセキュリティ管理におけるもう一つの要素である「プロセス」の管理です。

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の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。

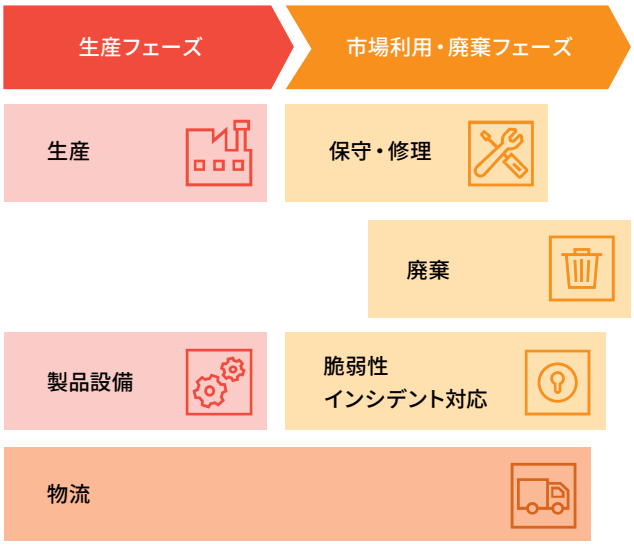
製品開発フェーズでは、企画・設計・実装・検証の各フェーズで必要となるセキュリティ施策を定義します。組織管理と同様に、車両が持つ機能や社会・利用環境などを考慮した上で、開発する車両に潜むサイバーセキュリティの脅威を識別し、開発製品のセキュリティのゴール・目標を定めることが出発点になります。製品開発フェーズ全体のセキュリティ目標が定まった後、設計・実装工程で定めたセキュリティ目標に沿って確実に開発し、検証工程で目標の達成を確認することがエッセンスです（図表3参照）。このフェーズは従来のものづくりの考え方そのものであり、自動車OEMメーカー・サプライヤーが得意とする領域です。

図表3：製品開発フェーズでのセキュリティ活動



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（図表4参照）。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。

図表4：製造・運用・メンテナンスフェーズでのセキュリティ活動



3 車両開発における脅威分析とリスクアセスメント

上述したように、車両サイバーセキュリティ確保の基本的なアプローチはリスク管理（最小化）の取り組みです。一方で全てのリスクをゼロにすることは現実的ではないため、限りあるセキュリティ対策のリソースを適切に分配し、製品ライフサイクルの各活動を通じて、十分なレベルまでリスクを低減する必要があります。そのためにはリスクを網羅的に把握した上で、各リスクの重大度に応じた対応レベルを定め、優先順位を付けて対策しなくてはなりません。本章では、製品ライフサイクル全体を通じたリスク管理活動の起点となる、コンセプトフェーズにおける「脅威分析とリスクマネジメント（TARA：Threat Analysis and Risk Assessment）」について考察します。

コンセプトフェーズでのセキュリティ活動の概要

車両開発のコンセプトフェーズにおける主な業務は、図表5のとおりです。

図表5：コンセプトフェーズでのセキュリティ活動

具体的な活動内容については、車両の機能安全規格ISO 26262※1に沿った、現状の開発業務での経験から多くのヒントを得られますが、中でもセキュリティ特有の取り組みとなるのが「TARA」です。

脅威分析とリスクアセスメント（TARA）

TARAは、コンセプトフェーズで実施する、リスク管理のための一連の活動を指し「資産の洗い出し」「脅威の洗い出し」「リスクアセスメント」の三つの工程で実施されます。

資産の洗い出し

はじめに、開発対象のユースケースや、参照可能な情報に基づいてシステム構造を整理し、守るべき情報資産・機能資産をリストアップします。

具体的な設計検討前のコンセプトフェーズでは、資産や、資産がどこに保持されるか未定のケースも珍しくありません。例えば、車両に電子決済機能を持たせる場合、決済に必要なクレジットカード情報が車両とバックエンドサーバーのどちらに保存されるのか、またその情報がより機密度の高いカード会員データなのか、それともトークン化した情報なのかといった未確定要素については、何らかの仮定を置いて分析を進めなければなりません。

こうした点は設計上具体化すべきポイントとして明確化し、後続フェーズでフォローアップしていく必要があります。また、前提の絞り込みには前工程の「対象の定義」で十分に技術上、制度上の制約を織り込むことも有効です。

このようにコンセプトフェーズの業務では、限られた前提条件や情報に基づいて分析を進める技術が必要となってきます。

※1 ISO 26262：自動車用の機能安全規格。自動車開発における安全設計のガイドラインとして、自動車メーカーや車載機器サプライヤーなどは準拠する必要がある。

脅威の洗い出し

洗い出した各資産に対し、起こり得るセキュリティ上の脅威を特定します。その上で必要に応じて各脅威の顕在化条件についても分析、整理します。悪意の第三者を考慮するセキュリティにおいては、実際の攻撃者（ハッカー）のアプローチや手法に関する専門性が必要になります。こうした属人性の高い作業の均質性確保や、洗い出した脅威の網羅性を一定レベルで担保するための構造的アプローチとして、各団体が提案する脅威分析手法があります。ただし、現状統一された手法は確立されていないため、各組織は製品の特性や開発現場の実情に適した手法を選択、または組み合わせて活用していく必要があります。例えば、詳細設計に依存しないようにSTRIDE※2 脅威分類などを用いて脅威を洗い出し、より詳細な顕在化条件の分析には脅威の具体的な攻撃手段や可能性をツリー状に図表化するアタックツリー（後述）を用いるといったことができます。

リスクアセスメント

各脅威に対して、共通の評価基準からリスクレベルを算定し、算定結果に基づいて対策（リスク低減）の優先度を決定します。評価基準には、リスクが実現した際の影響度や発生可能性といった従来のITセキュリティの指標を活用できますが、自動車のセキュリティでは「安全（safety）」への影響にも考慮を要します。例えば、図表6に示すとおり、影響度と発生可能性のマトリックスに基づいた4段階のリスクレベルを設定しつつも「安全」を脅かすリスクについては発生可能性の値にかかわらずレベル4を与える、といった考え方です。逆にITセキュリティのみの観点では重大なリスクでも、物理的に作用する機能安全の機構により容易にリスクを回避・制御でき、実際の影響度はそれほど高くないといったケースも出てきます。このような場合は、機能安全における制御難易度（controllability）といった観点での考慮が必要になります。

さらに現在策定中のISO/SAE 21434では、製品ライフサイクル全体を通じたリスクマネジメントの単位としてCAL（Cybersecurity Assurance Level）の導入が検討されています。CALは機能安全規格ISO 26262におけるASIL（Automotive Safety Integrity Level：安全性要求レベル）に相当する分類で、セキュリティ上の達成目標を複数段階で定め、そのレベルに応じて目標達成に必要な設計、実装または運用上の対策が施されます。組織は、CALで定めた目標が製品ライフサイクルの各工程を通じて最終的に達成されるよう管理する必要があります。

図表6：リスクレベル（4段階）算定表の例

影響度（Severity）	発生可能性（Exposure）		
	低い	中程度	中程度
非常に小さい	1	1	2
小さい	1	2	3
中程度	2	3	4
大きい	3	4	4
非常に大きい（安全に影響）	4	4	4

※2 STRIDE：脅威を識別するための分類手法の一つ。Spoofing（なりすまし）、Tampering（改ざん）、Repudiation（否認）、Information Disclosure（情報漏えい）、Denial of Service（サービス拒否）、Elevation of Privilege（権限昇格）の六つの分類を用いて、脅威を洗い出す。

参考文献：

ISO/SAE International."Status of Work in Process on ISO/SAE 21434 Automotive Cybersecurity Standard" 2018,

SAE International. “SAE J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems” 2016,

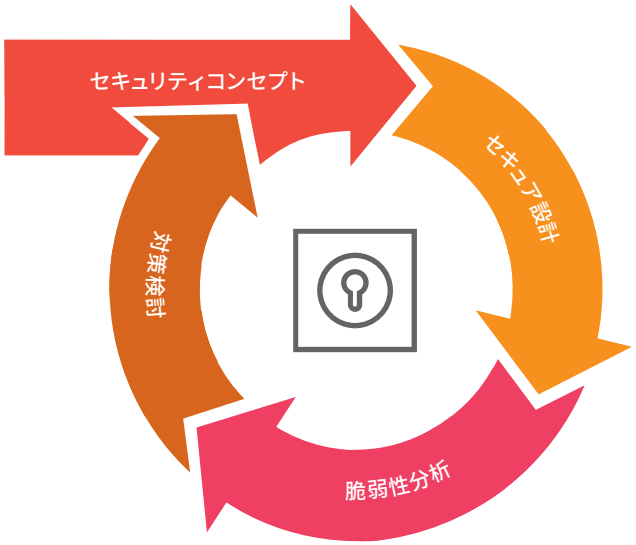
4 車両開発におけるセキュア設計と脆弱性分析

TARAの成果は、その後の製品開発フェーズにおけるリスク分析・管理の活動に引き継がれます。コンセプトフェーズにおいては、設計・実装が未定でリスクの顕在化条件や必要な対策を具体化できないケースがあります。これは、開発プロセスが進むにつれて明らかになるため、システム・ハードウェア・ソフトウェアの各開発フェーズにおいても繰り返しリスク分析を行い、リスクを管理していく必要があります。本章では、製品開発フェーズに議論を移して、システムや各コンポーネントの設計段階における活動について考察します。なお、本レポートでは設計情報も踏まえた具体的な攻撃成立条件としての「脆弱性」に係るリスク分析を、前章で解説したTARAと分けるために「脆弱性分析」と呼びます。

設計段階でのセキュリティ活動の概要

コンセプトフェーズでは、脅威の洗い出しやリスクアセスメントを行うことでサイバーセキュリティゴールが設定され、達成するための方針となるサイバーセキュリティコンセプトが定められます。製品開発フェーズでは、まずサイバーセキュリティコンセプトに従ってシステムとしての全体的な設計を行います。そして、設計のセキュリティ品質を向上するために脆弱性分析を行い、許容できない脅威の原因となる脆弱性が見つかった場合には対応方法を検討し、設計の改善を行います（図表7参照）。

図表7：設計段階でのセキュリティ活動



セキュア設計

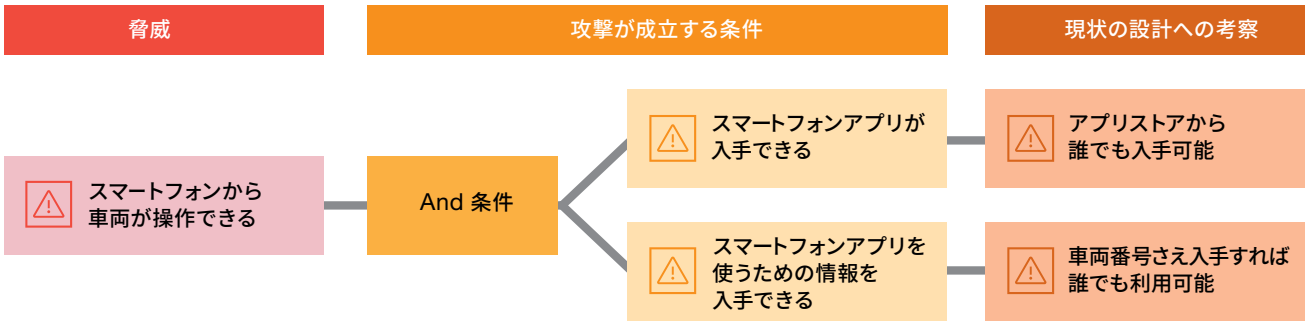
はじめに、セキュリティコンセプトに基づいて、システム全体の設計を行います。設計段階でのセキュリティ品質は、製品開発全体におけるセキュリティ品質のベースとなるためとても重要です。例えば、使用する主要ハードウェアやOSといったシステムのベースとなる要素は、システム設計のような早い段階で決定することが多くあります。ソフトウェア設計のような後の段階でOSなどシステムの根幹にかかわる部分に脆弱性が見つかり変更が必要となった場合、設計の変更が広範囲に及びます。また、実装やテストの段階のように、後の工程で脆弱性が見つかった場合は、前の工程に戻ってやり直す「手戻り」も多くなります。このように、設計段階で組み込まれてしまった脆弱性は、製品開発全体のコストや期間に大きなインパクトを与えることになります。設計段階でのセキュリティ品質を向上させることは、後の工程で発見される脆弱性を減らし、手戻りが少ない効率的な開発につながります。こうした効率的な開発をするために、設計について脆弱性分析を行い、対策を設計に反映させるというサイクルを回すことでセキュリティ品質を向上させます（図表7参照）。

脆弱性分析

脆弱性分析とは、攻撃のために悪用可能な脆弱性が設計上に存在しているかを確認する活動です。これにはアタックツリーなどの手法が用いられます（図表8参照）。

まずコンセプトフェーズで洗い出した脅威に対して、どのような条件で攻撃が成立してしまうかを考えます。そして、現状の設計として攻撃が成立する可能性があるかを考察することで、脆弱性が存在しているかを判断します。スマートフォンやサーバーと通信するようなコネクテッドサービスの分析では、車両そのものの分析だけではなく、関連するシステムも含めて分析する必要があります（図表8参照）。

図表8：アタックツリーを用いた脆弱性分析の例



対応方法の検討と設計への反映

脆弱性分析によって製品に脆弱性が存在すると判断された場合は、コンセプトフェーズで実施したリスクアセスメントの結果と照らし合わせ、許容できない脆弱性であるかを判断し、対応方法を検討します。対応方法は攻撃が成立しないように設計を変更する以外に、システムを監視し、検知・対応および復旧ができる機能を追加するアプローチも含めることができます。このアプローチは、攻撃が発生したとしてもすぐに危険な状態にはつながらないような緊急度が低い脅威に対して適用することが可能です。このように複数ある選択肢の中から、リスクや開発コスト、日程などを総合的に判断し、対応方法を決定していきます。

このような脆弱性分析、対応方法の検討、設計への反映というサイクルを、脆弱性が存在しなくなる、もしくはリスクが許容できるレベルに低減できるまで繰り返し行います。その際には、設計の変更によって別の脆弱性が新たに発生するケースについても考慮する必要があります。また、システム全体の設計時だけではなく、ハードウェア設計やソフトウェア設計のように、より具体的な設計を行う際にも、これらの活動を行うことでセキュリティ品質を担保します。

設計段階で発生する脆弱性と実装段階で発生する脆弱性

セキュア設計だけでは全ての脆弱性について対応できないことにも注意する必要があります。図表9では設計段階と実装段階で発生する脆弱性の例を示しています。

図表9：設計段階と実装段階で発生する脆弱性の例

設計段階で発生する脆弱性	実装段階で発生する脆弱性
■ 認証機能の不備 ■ 脆弱性のあるサードパーティ製ソフトの使用 ■ 重要データの耐タンパ性※1が低いストレージへの保管	■ バッファオーバーフロー※2 ■ SQLインジェクション※3 ■ ディレクトリトラバーサル※4

図表9で示したバッファオーバーフローやSQLインジェクションのような実装段階のコーディングに起因する脆弱性は設計段階で見つけることはできません。設計段階で発見ができない脆弱性については、実装段階での対策が必要となります。

※1 耐タンパ性：外部から重要データを盗み出そうとする行為に対する耐性度合い。

※2 バッファオーバーフロー：プログラムによって確保されたメモリ領域を超えるデータが送り込まれることにより誤動作が生じること。

※3 SQLインジェクション：セキュリティ上の不備を利用して攻撃者が任意のSQL文（データベースへの命令文）を実行させてデータベースを不正に操作すること。

※4 ディレクトリトラバーサル：ディレクトリをさかのぼることなどにより、本来はアクセスが禁止されているディレクトリやファイルに不正アクセスする手法。

5 車両開発における セキュアコーディング実施のポイント

コンセプトフェーズにおける脅威分析とリスクアセスメント、開発フェーズにおけるセキュア設計、脆弱性分析と対策実施の活動の結果によって作成される設計書に従い、ソフトウェアを実装するフェーズで行うべき「セキュアコーディング」について考察します。

セキュアコーディングとは「サイバー攻撃に耐えられる堅牢なプログラムを書くこと」です。第4章の最後で「設計段階で発生する脆弱性」と「実装段階で発生する脆弱性」について解説しましたが、セキュアコーディングは「実装段階で発生する脆弱性」に対する施策となります。

第1章の図表1に示したISO/SAE 21434の7つの要素の一つである「製品開発フェーズ」に含まれる「ソフトウェアレベル」の中の最も詳細なレベルの活動です。

セキュアコーディングの重要性

セキュアコーディングが重要である理由は「設計段階で発生する脆弱性」に対して施策を講じていても、セキュアコーディングの不備による「実装段階で発生する脆弱性」があった場合、深刻な被害につながる可能性があるためです。例えば「実装段階で発生する脆弱性」の代表事例であるバッファオーバーフローやSQLインジェクションなどの脆弱性により、第三者に意図しないコードを実行されてしまう可能性があります。

さらに、ソフトウェア全体の脆弱性としては「設計段階で発生する脆弱性」に比べて「実装段階で発生する脆弱性」が多く報告されており、脆弱性の「数」の観点でも重要と考えられます。

セキュアコーディングの具体的な作業

図表10に、セキュアコーディングのための具体的な作業を挙げます。コーディング作業に先立ち、プロジェクトの特性（製品が扱う情報や機能の重要度、コスト、納期など）に応じて全体計画を策定する必要があります。

図表10：セキュアコーディングの具体的な作業

作業項目	概要
セキュアコーディング全体計画の策定	セキュアコーディングの全体計画を策定します。ソースコードレベルでのプログラムの堅牢性を確認する方法（静的コード解析ツール利用、ピアレビュー※1など）についても検討します。
セキュアコーディング教育	セキュアコーディングの概要や、違反した場合に起こる問題について学びます。
コーディングルールの策定	自動車業界で一般的に利用されるCERT-C/C++※2やMISRA-C/C++※3などのコーディングスタンダードをベースとし、必要に応じて自社のルールを追加して策定します。
静的解析ツールの利用計画策定（静的解析ツール利用時）	ソースコードレベルでのプログラムの堅牢性を確認するための静的解析ツールの選定や、静的解析ツール実行／対応計画の策定などを行います。
コーディング	コーディングを行います。開発ツールの警告メッセージを利用することで、プログラムの堅牢性をある程度、担保することができます。
ソースコードレベルでのプログラムの堅牢性の確認	ツール利用による静的解析や、ソースコードレビューをして、ソースコードレベルでのプログラムの堅牢性を確認します。ここで問題が検出された場合は、ソースコードの修正と確認作業を繰り返します。

※1 ピアレビュー：立場や職種が同じ（または近い）者によって、成果物を検証して改善を図る品質保証の手法。

※2 CERT-C/C++：セキュアなソフトウェアをつくるためのコーディングガイドライン。約300項目のルールが規定されている。

※3 MISTRA-C/C++：自動車の機能安全を目的として作成されたC/C++言語用のコーディングガイドライン。2016年にセキュリティに関するルールも発行された。

セキュアコーディング時の課題と解決方法

多くの組織は何らかの静的解析ツールを利用してソースコードレベルでのプログラムの堅牢性を確認していますが、この時の大きな課題として「検出される問題が多すぎて対応しきれない」「ツールの誤検知かどうかの判断だけでも大変」ということが挙げられます。

この課題を解決するために、一般的なソフトウェアの開発では、静的解析ツールが示す重要度（Critical/High や Moderate/Low など）に応じた対応をする場合が多くあります。例えば、Critical/High の問題について、修正あるいはリスクを分析したのち可能な場合はリスクを受容し、Moderate/Low の問題については、誤検知かどうかの判定もしない方針とするケースなどもあり得ます。

一方、自動車業界では、静的解析ツールで検出された問題を修正しなかった場合、静的解析ツールが重要度を Low と判定した問題でも人命にかかわる被害が発生する可能性があるため、静的解析ツールが示す重要度などにより自動的に対応を決定することは難しいのが実情です。

では、自動車のソフトウェア開発においては、どのような解決策があるのでしょうか。

PwC としてクライアントにアドバイスしている解決策は「ツールが検出した問題は全て対応する」、そのために「全ての問題に対応するための施策を考える」ということです。ここで「対応する」とは「誤検知と判定する」または「修正する」ことを指します。

ポイントは「そもそも脆弱なコードを可能な限り入れない」ことと「ツールが検出した問題に計画的に対応する」ことです。

そのための具体的な施策として、以下が挙げられます。

- セキュアコーディング教育を実施する
- 開発フェーズの早い段階から静的解析ツールを実行する
- CI ツール※4に静的解析ツールを組み込むなど、静的解析ツールの実行を自動化する

※4 CI（Continuous Integration）ツール：ソースコードのビルド（実行可能ファイルや配布パッケージを作成する処理）やテストを継続的に実施するためのツール。静的解析ツールを Jenkins などの自動ビルド機能を備えたツールと連携することで、自動ビルドのタイミングで静的解析を実行できる。

6 車両開発における セキュリティテスト

本章では、実装された車両／車載製品に対するテスト段階における施策である「セキュリティテスト」について紹介します。

目的別のセキュリティテスト分類

セキュリティテストは、大きく脆弱性診断とペネトレーションテストの二つの概念を含みます。

脆弱性診断

前章までに紹介したとおり、セキュリティに関する取り組みは、コンセプトフェーズ、開発フェーズ、実装フェーズごとに行われ、各フェーズにおいて脅威分析の実施とその結果に基づいたセキュア設計、セキュアコーディングなどが行われます。このように、上流工程において想定された脅威への対策が想定どおり適切に実施されているか否かを確認するテストが、脆弱性診断になります。このような性質上、脆弱性診断では事前に想定脅威とその対策が明確であるためチェックリストなどを作成することが可能であり、その網羅性についても一定の説明ができます。

ペネトレーションテスト

一方、ペネトレーションテストは攻撃による達成目標を定め、その目標を達成するために攻撃（評価）を行うテストになります。ペネトレーションテストは網羅性を求めるものではなく、例えば「特定のECU（Electronic Control Unit）上で任意コードを実行する」などの目的を達成できるか、できない場合はどこまで目標に迫れたか、目標を達成できない理由・原因は何かを明らかにすることが目的となります。ペネトレーションテストは上流工程でのさまざまな取り組みを考慮せずに実施するため、上流工程で想定していなかった脅威、すなわち上流工程での検討漏れを明らかにする効果が期待できます。別の言い方をすると、ペネトレーションテストで実施する各テスト項目は、脆弱性診断に含まれる項目である可能性もあります。

これは、世の中の攻撃者が製造企業のセキュリティ対策とは無関係に、目標達成に向けてあらゆる手段を講じてくる状況と同一であり、攻撃者目線で評価を行うことを意味します。

図表11に示すように脆弱性診断とペネトレーションテストではその思想が異なり、一方が他方を包含するというものではありません。全ての製品に対して全てのセキュリティテストを実施することはコスト的に現実的ではないため、実施に当たっては、製品モデル、類似モデルとの機能差分などに基づいて対象を選定することが重要です。

図表11：脆弱性診断とペネトレーションテストの概要

	目的	メリット	デメリット
脆弱性診断	上流工程で想定した脅威に関する対策の充足状況を確認する。	一定の網羅性を説明することができる。	上流工程で想定していなかった脅威、対策を検討してなかった脅威への対策状況を評価できない。
ペネトレーションテスト	達成目標を設定し、目標が達成できるかどうか、できない場合はその理由・原因を明らかにする。	上流工程で想定していなかった脅威に対する評価を行うことができる。上流工程での検討結果自体の評価を行うことができる。	網羅性を説明することは難しい。各テスト項目は、脆弱性診断と重複する可能性がある。

テスト対象別のセキュリティテスト観点

脆弱性診断、ペネトレーションテストともに、テスト対象へのアプローチとして、HW（ハードウェア）に対するテストとSW（ソフトウェア）に対するテストが考えられます。

HW（ハードウェア）を対象としたセキュリティテスト

HWに対するテストはいくつかのレベルがあり、一つには製品が提供している標準的な外部インターフェースに対するテストが考えられます。例えば、イーサネットポート（LANポート）、Wi-Fi、Bluetoothなどのネットワークの接続インターフェース、USBポートなどの外部デバイスの接続インターフェース、CD/DVDなどのメディア入力、筐体（きょうたい）に設置されているボタンなどが想定されます。こうしたインターフェースは、利用者が標準的に利用できるものであり、また、マニュアルなどに利用方法が記載されているため最もテストがしやすい一方、内部仕様が分からない場合は無意味なテストを行ってしまう可能性もあり、効果的なテストが難しい領域です。

次に考えられる項目としては、筐体の分解などを行い、内部のプリント基板などを対象とした調査・分析が考えられます。例えば、利用している各種チップの種類・用途、シルク印刷の有無・内容、デバッグポートの有無、出荷前におけるピン利用の痕跡の調査・分析などが挙げられます。

こうした調査・分析は製品仕様の推定を行う上で有益であり、また、デバッグポートなどを発見・特定できた場合、それ自体が大きなリスクであると同時に開発者向けの内部情報にアクセスできるため、後続のテストを行う上でも有益であるといえます。また、こうした分析の結果、通信機能を有するファームが格納されたチップを特定できた場合、当該チップからファームウェアの抽出ができるか、抽出したファームウェアの分析ができるか、というテストも考えられます。

SW（ソフトウェア）を対象としたセキュリティテスト

SWに対するテストもHWに対するテストと同様にいくつかのレベルがあります。最も基本的なテストとしては、利用者に提供されているユーザーインターフェース（UI）を操作し、セキュリティ機能のバイパスやセキュリティ上問題のある操作ができないか確認することが挙げられます。また、ネットワークへの接続インターフェースが提供されていた場合、不要なサービスが起動していないか、実行されているソフトウェアに既知の脆弱性が存在しないかを確認し、脆弱性が存在していれば実際に攻撃を行い、攻略可能か確認するといった内容が考えられます。

こうしたテストに関しても内部仕様を把握せずに外部からテストする場合、やみくもなテストとなり、効果的なテストが難しくなる可能性があります。そのため、HWに対するテストにおいて抽出したファームウェアを分析し、内部仕様を明らかにした上でSWのテストを行うなどの方法も想定されます。図表12にHWテストとSWテストの内容例をまとめています。

図表12：HWテストとSWテストの内容例

HWテストの内容例	SWテストの内容例
・外部インターフェースに対する操作、異常入力の挿入 ・筐体の分解、プリント基板上の情報の分析 （使用チップ・用途、シルク印刷、デバッグポートなど） ・チップの取り外し、ファームウェアの抽出、など	・ユーザーインターフェース（UI）の操作 ・ネットワーク経由でのスキャン、脆弱性診断 ・ファームウェア解析 ・脆弱性に対する攻撃の実施

セキュア開発ライフサイクル全体におけるセキュリティテストの位置付け

こうしたさまざまなテスト内容が脆弱性診断として実施すべき項目か、ペネトレーションテストとして実施すべき項目かは、上流工程でどこまで、どのような脅威を想定し、その対策をどの程度、どのように組み込んだかに依存します。言い換えれば、上流工程で想定された脅威への、対策の充足状況を確認するために行うのが脆弱性診断であり、そもそもの想定の充足性・妥当性を確認するために行うのがペネトレーションテストといえます。

このようにセキュリティテストは、テストフェーズのみで実施方針、内容を検討するのではなく、開発プロセス全体の取り組みを踏まえて策定することが重要です。

7 製造フェーズにおけるセキュリティ対策

ここまでは、設計、実装、テストと製品開発におけるセキュリティ活動にフォーカスし、考察を行ってきました。本章では製品そのもののセキュリティから離れ、製品を完成させる際に不可欠な製造フェーズにおいて必要となるセキュリティ活動について考察します。

製造フェーズにおけるセキュリティ活動の必要性

これまで、製造工場では独自のネットワークや制御系システムの設備が用いられていたものの、それでもマルウェアなどによるセキュリティ被害は発生していました。さらに近年では、スマートファクトリーのようなIoT化が進み、さまざまな機器が製造工場のネットワークに接続しています。また、システム自体に汎用的なOSやアプリケーションが用いられることが増えています。このような環境の変化により、マルウェアのターゲットとなるといったセキュリティリスクがより高まっているといえます。

また、車両がネットワークに接続されたことで、通信の暗号化やメッセージ認証のような暗号技術の利用が広がりました。その影響で、暗号技術において重要な役割を果たす暗号鍵を、内部に保管しなければならないECU（Electronic Control Unit）が増えてきました。この暗号鍵は製造工場で厳重に管理し、漏えいや改ざんがないことを常に保証する必要があります。

さらに、国際規格であるISO/SAE 21434とともに重要であり、今後の法律化が見込まれている“Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA”においても、製造フェーズを含む開発のライフサイクル全体でCSMS※1の実施が求められており、今後は法律・国際規格の上でも製造工場におけるセキュリティ活動が必須になると考えられます。

このように、工場のIoT化・車両機能の進化・法律・国際規格といったさまざまな面から製造フェーズにおけるセキュリティ活動の必要性が高まっています。

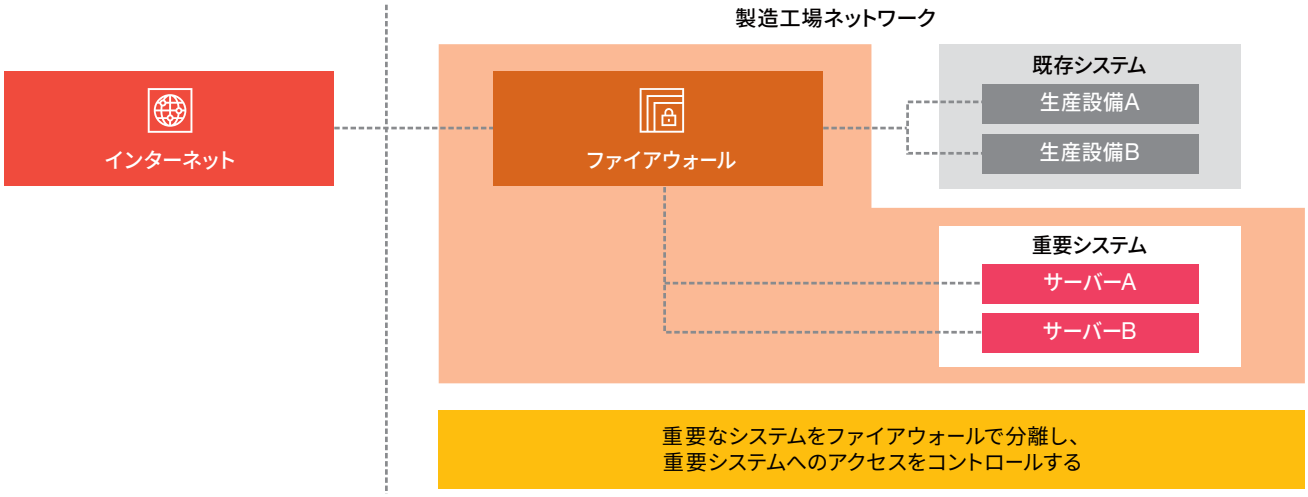
製造工場の各設備で必要なセキュリティ対策とは

これまで工場の生産設備は外部のネットワークにつながることが少なく、セキュリティ対策が十分に実施されていないケースもあると考えられます。そのような設備をそのまま外部のネットワークにつないでしまうと、セキュリティ強度の弱い生産設備が攻撃の対象となってしまいます。ネットワーク全体がセキュリティ上の危険にさらされるため、各生産設備やネットワークへのセキュリティ対策が必要です。

しかし、全ての設備を同じレベルでセキュアにすると、作業量やコストが膨大になってしまいます。そこで、ネットワークを分離し、ネットワーク同士の接続にはファイアウォールなどでアクセスを制御、各設備にそれぞれ必要なセキュリティ対策を施すことで、効率的なセキュリティ管理を実現します（図表13参照）。

※1 CSMS（Cyber Security Management System）：産業用オートメーションおよび制御システムを対象としたセキュリティを管理する仕組み。

図表13：重要システムへのアクセスコントロール例



より強固な対策が必要な暗号鍵管理システム

通信の暗号化やメッセージ認証などには暗号鍵と呼ばれるデータを用います（図表14参照）。この暗号鍵は、攻撃者に不正に入手されると、暗号化通信の解読や車両のなりすましにつながるため、生産設備や車両内で安全に保管するなど厳重に管理する必要があります。

暗号鍵は車種や車両1台ごとに別の鍵を使うことが想定されるため、その際には暗号鍵と車両やデバイスをひも付けて管理し、デバイス内に暗号鍵を書き込むための管理システムが必要となります。前述のとおり、この暗号鍵は漏えいすると車両に対して大きなインパクトを与えてしまうため、暗号鍵を取り扱うシステムは、通常の生産設備よりも高いレベルでのセキュリティ強度を確保することが必要です。

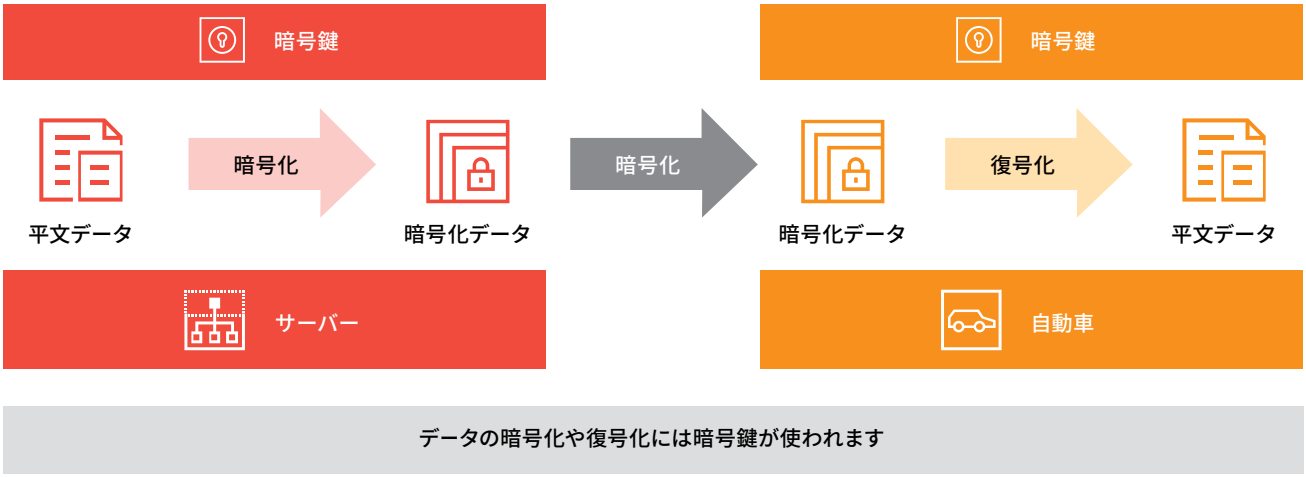
鍵管理システムのセキュリティ対策例

- サーバールームへの入室管理などの物理セキュリティ強化
- 多要素認証などを用いたシステムへのアクセス制御強化
- HSM※2による暗号鍵の管理
- 鍵管理に関連するシステムのログ監視強化

このように、鍵管理システムではより強固なセキュリティ対策が必要となります。既存のシステムと鍵管理システムが同一ネットワーク上で混在している環境では、それら全てを同じレベルのセキュリティ強度にしなければ、最もセキュリティ強度が低いシステムに対して攻撃が行われ、同一ネットワーク上の鍵管理システムが危険にさらされることになります。そのため、前述したようなネットワークの分離とアクセスコントロールを行い、それぞれのシステムにおいて必要十分なセキュリティ構成にすることが重要となります。

※2 HSM（Hardware Security Module）：データセンターなどにおいて暗号鍵のような重要なデータを保管するためのセキュアなハードウェア。

図表14：暗号化処理の概要



8 出荷後のセキュリティ対策 ——サイバーセキュリティ監視

本章では、自動車を出荷した後に必要となるセキュリティ活動の在り方について考察します。

出荷後もセキュリティ活動が必要

従来の自動車開発において、製品の品質を高める活動は、出荷前の開発や製造フェーズで実施するものでした。製品の品質を高めるセキュリティ活動と同様に、出荷前のセキュリティ対策が重要であることは、前章までに紹介したとおりです。ただし、セキュリティの観点では、いくつかの理由で、出荷後であっても対策を実施する必要があります。背景には、製品を能動的に攻撃する攻撃者の存在があります。

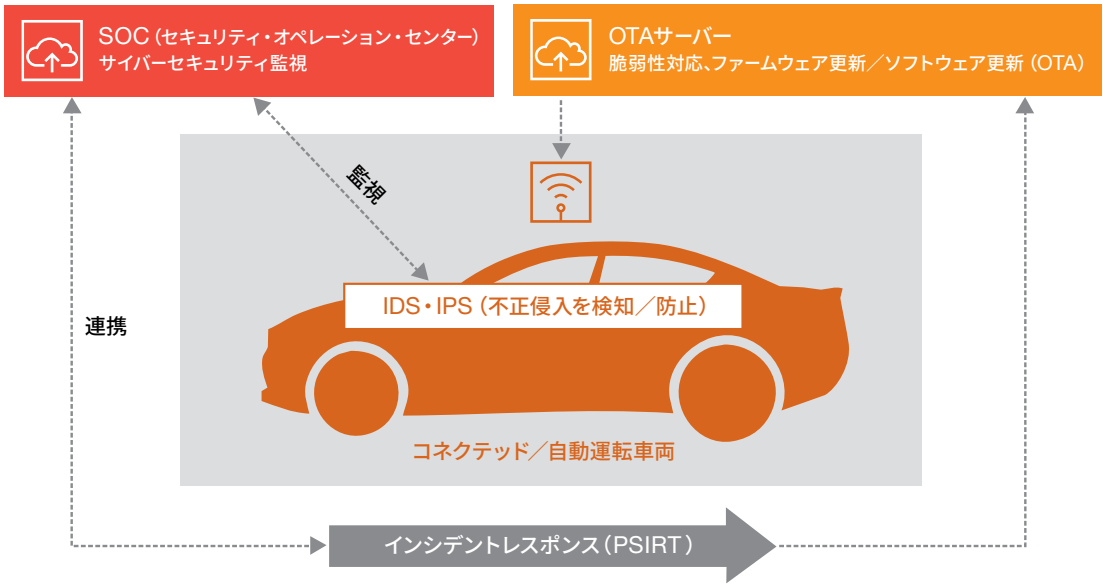
攻撃者は新しい攻撃手法を発見するなど、新たなやり方を試してくることがあります。製品出荷前のある段階では十分な対策であったとしても、新たに見つかった攻撃手法に対しては防ぐ手立てがないといったことが起こるかもしれません。攻撃を進化させる能動的な攻撃者に対処するには、製品出荷後のセキュリティ環境の変化に追従するためのセキュリティ対策が必要になってくるのです。

出荷後フェーズにおけるセキュリティ活動の全体像

出荷後に実施すべきセキュリティ対策は、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」といった活動です（図表15参照）。サイバーセキュリティ監視は車両などを監視し、自動車への攻撃を検知する活動です。脆弱性対応、ファームウェア更新は、出荷後に脆弱性が発見された際に、修正したファームウェアを用意し、車両を安全な状態に更新するもの。インシデントレスポンスは、攻撃を検知した後に、その内容を踏まえて被害の発生を防ぐことを目的としています。ここで中心的な役割を担う体制がPSIRT（Product Security Incident Response Team）です。

これまでもIT業界では、類似の活動が実施されてきました。IT業界での活動内容やノウハウを、いかに自動車に適用するかを検討することが重要な観点です。

図表15：出荷後のセキュリティ活動の全体像



「サイバーセキュリティ監視」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、分析することです。サイバーセキュリティ情報には、政府系組織やセキュリティベンダーが提供する外部の情報と、社内のアセスメントで発覚した脆弱性情報といった企業内部の情報という二つに大別されます。

外部から情報を入手する場合、有償または無償で取得できる多様な情報源の中から適切に選択し、継続的かつタイムリーに収集する必要があります。2019年現在、自動車への攻撃やインシデント情報が報告される数は多くありません。他方、車両に搭載される製品の脆弱性情報は多く報告されています。これらの情報を確実に入手し、報告された情報が自社に関係するのか、どの程度の影響を及ぼすのかを正しく判断する運用体制の構築が必要になります。

社内で得られる情報の一つには、社内のアセスメントやセキュリティテスト活動において見つかる脆弱性情報があります。これが見つかった場合、必要な改修作業と製品への展開を実施する必要があります。詳細は、次章の「脆弱性対応、ファームウェア更新」で解説します。

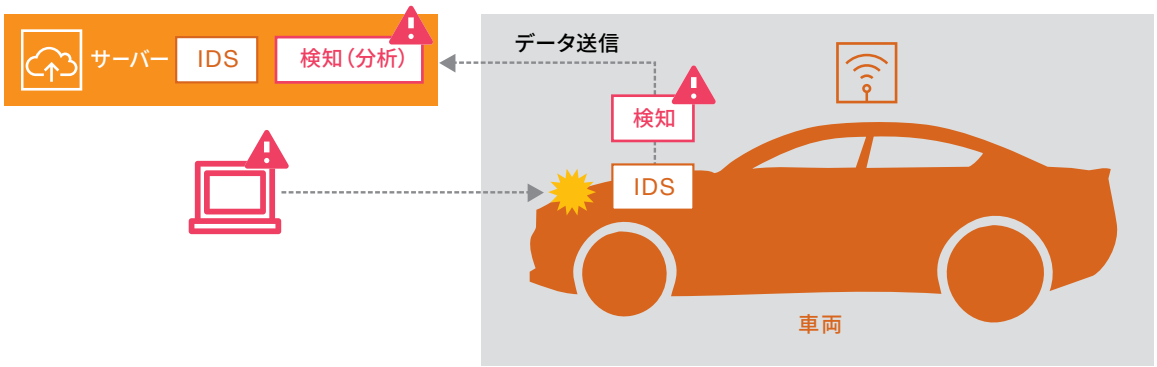
また、社内で攻撃情報を入手するための施策として、車載IDS（侵入検知システム：Intrusion Detection System）やSoC（Security Operation Center）/SIEM（Security Information and Event Management）の導入が進められています。外部からの情報だけに頼らない、自社製品に対する攻撃を検知することが導入の狙いです。

攻撃情報収集に役立つ車載IDS、車両向けSoC

車載IDSとは、車両に搭載される部品もしくはソフトウェアであり、車両や車載部品が攻撃を受けていることをリアルタイムに検知するための機器です。車載IDSはネットワーク型、ホスト型などの種別があり、車両ネットワークを流れるデータ、部品への通信データ、部品上で動くソフトウェアのふるまいなどを分析し、車両への被害を発生し得る攻撃、もしくはその可能性を検知します。攻撃者の攻撃に対応するためには、まずは攻撃の発生を特定できなければ活動を開始することができませんので、先に述べたような能動的な攻撃者の存在を踏まえれば、今後特に重要になる技術といえます。

また車載IDSとの組み合わせで、車両向けのSoC運用も利用検討が進められています。車載IDSは車両内にあり、限られたリソースで動作することから、複雑かつ大量なデータを分析することには向いていません。そのため、車載IDSでは簡易な分析にとどめ、クラウド環境などに用意したSoCに必要なデータを送信し、複雑な分析などを任せる構成をとります（図表16参照）。SoCは、複数の車両から送られた大量のデータを分析し、攻撃の兆候を捉える役割を担います。また、SoCで特定車両に対する攻撃が発見された場合に備え、SoC側から当該車両に指示を送り、通信遮断などの対処を開始する機能も合わせて構築することで、将来のサイバー攻撃に備えます。

図表16：リアルタイムで車両への攻撃を検知・対応



9 出荷後のセキュリティ対策の要 ――PSIRT

出荷後のセキュリティ活動のうち、PSIRT活動の主体である「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」について考察します。

出荷後フェーズにおけるセキュリティ活動の振り返り

第8章で解説したとおり、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）です。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によって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、分析した上で、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、標準化団体などによる評価※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、個人情報などへの影響）」「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17参照）。

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。

※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 CAN（Controller Area Network）：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17：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、単一ではなく複数の脆弱性情報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によって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。新たな脆弱性情報が出現した際には、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、脆弱性悪用による自社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。

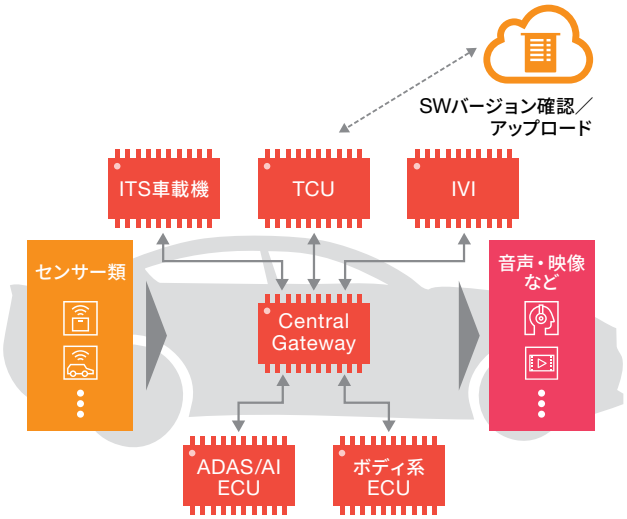
インシデントレスポンスにおいてPSIRTは、製品開発部門、品質管理部門、IT部門などの社内ステークホルダーと連携し、被害の規模、追加被害の可能性や規模などを加味し、インシデントの緊急度に基づく優先度付け（インシデントトリアージ）を行います。そして優先度が高いと判断されたインシデントは、事前に決められたインシデント対応フローに基づき、適切なレベルのマネジメント層に速報を行った上で、対応を実施していくことが求められます。こうした一連の流れは、PSIRTが主体となって実施するものの、円滑な対応には各部門の習熟が必須となるため、事前に訓練を実施しておくのが望ましいです。

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何らか（利用方法、設定、ソフトウェアなど）の変更をするために、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18参照）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へ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。

図表18：OTAによるファームウェアアップデートのシステム



10 車両の進化のために

ここまでの章では、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。本章では、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や連携について改めて確認します。あわせて、本レポート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。

車両ライフサイクル全体を通じたセキュリティ活動 ――ユーザー視点の意義

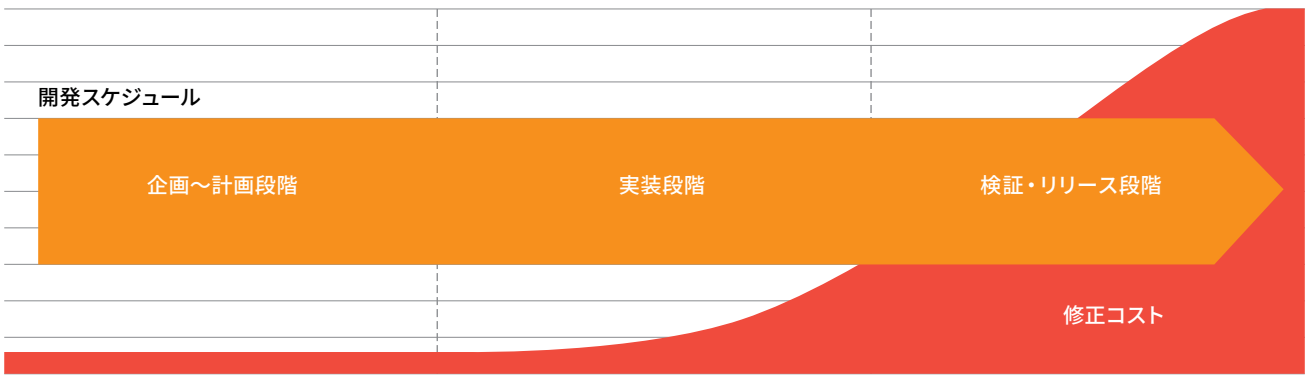
ISO/SAE 21434は、車両のライフサイクル全体を通じたサイバーセキュリティ活動に関するプロセスの定義を目的としていました。車両のライフサイクル全体とは、車両の企画・研究から始まり、設計・実装・検証を経て、製造・出荷され、市場にて運用・廃棄されるまでの、車両の開発・運用に関する全ての活動を意味します。そして、その全ての活動においてサイバーセキュリティの取り組みを実施することが求められています。

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。車両に脆弱性が残った状態では、ユーザーがセキュリティ被害に遭う可能性が拭い切れません。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。

車両ライフサイクル全体を通じたセキュリティ活動 ――メーカー視点の意義

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19参照）。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、既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 21434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、ユーザーをセキュリティ被害から守ることだけを考えたものではなく、実は車両メーカーにとって「効率化」というメリットが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・メーカーを含め、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19：開発工程が進むにつれて上昇する修正コスト



ひとつながり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。本レポートでは、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。実際の活動では、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。

では、セキュリティ活動の担当者と責任者がフェーズ別に異なるのは、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。さらには、出荷後の監視活動でも監視対象としなければなりません。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。

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っていても、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いえます。

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であり明白です。

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。

従って、サイバーセキュリティ活動を正しく行わなければ、新しい車両のユーザーは新しい価値を得られたとしても、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、車両の未来を創るメンバーには、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してこそ、新しい車両の未来を創る権利を得られることになるのです。

お問い合わせ先

PwC Japanグループ
https://www.pwc.com/jp/ja/contact.html

PwC Japan Group Contacts

【執筆者】
奥山 謙
PwCコンサルティング合同会社 シニアマネージャー

【監修】
林 和洋
PwCコンサルティング合同会社 パートナー

村上 純一
PwCコンサルティング合同会社 ディレクター

納富 央
PwCコンサルティング合同会社 マネージャー

安井 智広
PwCコンサルティング合同会社 マネージャー

澤 謙太
PwCコンサルティング合同会社 シニアアソシエイト

吉田 万里子
PwCコンサルティング合同会社 シニアアソシエイト

亀井 啓
PwCコンサルティング合同会社 シニアアソシエイト

www.pwc.com/jp

電子版はこちらからダウンロードできます。www.pwc.com/jp/ja/knowledge/thoughtleadership.html
発刊年月：2020年2月　管理番号：I201910-4