

2026 年 9 月 10 日

パナソニック オートモーティブシステムズが AI 時代の SDV における新たなサイバーセキュリティ課題を提起 ～ISC2^{※1} SECURE Japan 2026 で講演～

パナソニック オートモーティブシステムズ株式会社（代表取締役社長：永易正史、本社：神奈川県横浜市）は、2026 年 9 月 1 日に東京コンファレンスセンター・品川で開催された「ISC2 SECURE Japan 2026^{※2}」において、セキュリティ開発部 プリンシパルエキスパート 安齋潤が「境界が消える AI 時代の SDV（Software-Defined Vehicle）をどう守るか」をテーマに講演したことをお知らせします。

本講演は、AI と車両、クラウドが高度に連携し、従来のシステム境界が曖昧になる SDV 環境において顕在化が想定される新たなサイバーセキュリティ課題に着目し、その問題提起と対策の方向性について提言したものです。今回、将来の SDV 環境におけるセキュリティ確保の重要性を示す内容として、ISC2 SECURE Japan 2026 の講演プログラムに採択されました。



ISC2 はサイバーセキュリティ分野の国際的な非営利会員団体で、27 万人以上のセキュリティ専門家で構成されており、安全で安心なサイバー世界の実現に向けて活動しています。このたび開催された ISC2 SECURE Japan 2026 では、セキュリティ専門家が集い、最新のサイバーセキュリティ動向や技術について講演や展示を通じて議論・共有しました。

■ 講演概要

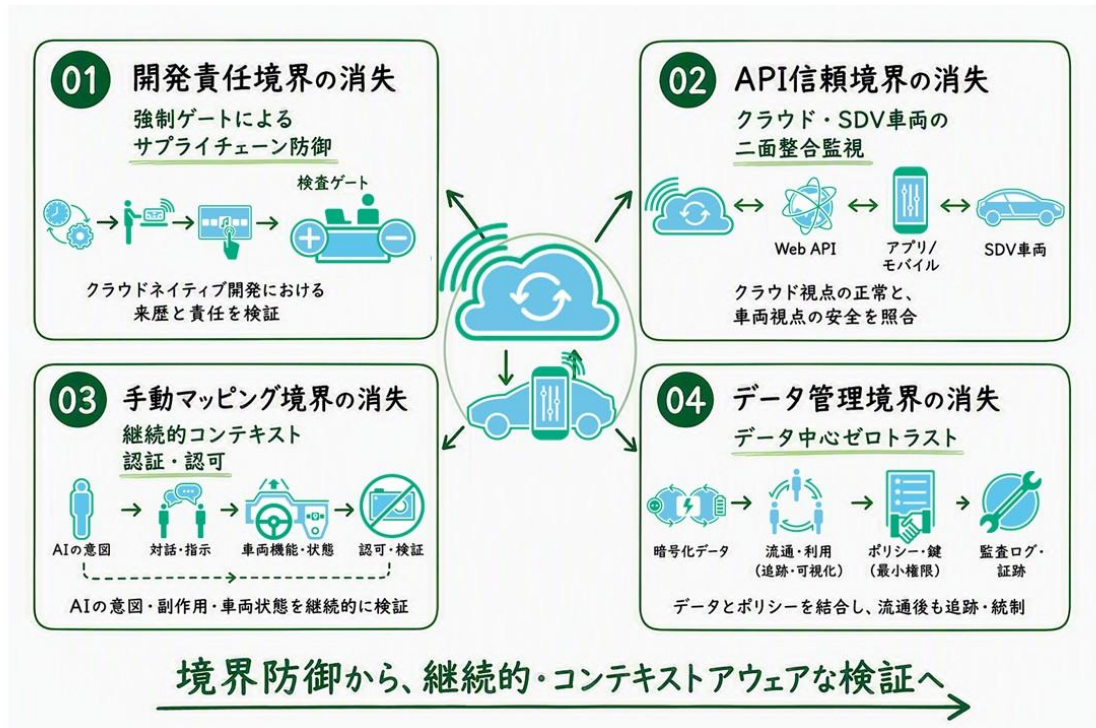
SDV の普及に伴い、自動車はクラウド、AI、外部サービスとの連携を前提としたシステムへと進化しています。一方、車載ソフトウェアの開発は OSS 活用拡大による脆弱性リスクの増加や生成 AI を活用した攻撃の高度化など、新たなサイバーセキュリティ上の課題への対応が求められています。

また近年は、生成 AI の活用によりソフトウェア開発の自動化や、クラウドサービス間の連携の高度化が進んでいます。今

後、AI エージェントが開発・運用、車両機能の制御に関与するようになると、誰が開発責任を負うのか、どのシステム同士がどのような関係で接続されているのかといった従来明確だった境界が複雑化し、把握が難しくなることが想定されます。しかし、こうした将来の SDV 環境におけるセキュリティ課題については、業界全体での議論や対策の検討が十分に成熟しておらず、今後さらなる議論と取り組みの深化が求められています。

講演では、これらの課題を「開発責任境界」「API 信頼境界」「手動マッピング境界」「データ管理境界」の 4 つの境界の消失だと定義し、その対応の方向性を提言しました。

	概要	対応の方向性の提案
開発責任境界	多数の企業と AI がクラウドネイティブに協働して車載ソフトウェアを開発する時代には、「何を、誰が、どこで生み出したか」という来歴（プロビナンス）の追跡が困難となり、開発責任の所在が曖昧となる。	強制ゲートによるサプライチェーン防御：ソフトウェアの来歴・供給元・製造環境などの検証ステップを SBOM 作成前に組み込み、開発責任の所在が明確なソフトウェアのみを車両へ採り入れることで開発責任の所在を明確化できる。
API 信頼境界	車両が外部サービスと Web API で常時連携する場合は、認証という一つのゲートが突破されると、車両はクラウドからの指令が不正であっても「正当な指示」として遂行してしまうリスクがある。	二面整合監視：クラウドと車両の双方から静的・動的な挙動の整合性を照合し、両者の視点の齟齬（走行中のエンジン停止指示等）を捉えて未然に不正動作を防止する。
手動マッピング境界	従来は設計者が定めた対応表（手動マッピング）に沿って車両が動作していたが、マッピングを AI エージェントに任せただけの場合、自ら操作を選択し実行するため、意図しない操作や権限の肥大化を招きかねない。	継続的コンテキスト認証認可：AI の操作がその時々々の文脈（コンテキスト）に照らして妥当かつ安全であるかを都度検証し、必要最小限の一時権限を付与して逸脱を抑止する。
データ管理境界	SDV 車両における AI の活用などが進み、個人情報や蓄積量が増加するとともに、従来は車内に閉じていた個人情報や操作ログ、車内外カメラの映像データなどの車外での活用が拡大。その結果、データの所在や利用状況を継続的に把握することが難しくなり、情報漏えいや目的外利用のリスクが高まる。	データ中心ゼロトラスト：車外へ転送される個人情報や操作ログなどのデータそのものに利用ポリシーを暗号技術で紐づけ、サービス提供事業者などへデータが移動しても当該ポリシーを強制することで、利用証跡を記録・監査しながらアクセス制御を行う。



■ 課題に対する対応

当社は、今回課題提起した「開発責任境界」「API 信頼境界」「手動マッピング境界」「データ管理境界」への対策として、複数の技術の特許出願を進めています。将来的には、自動車サイバーセキュリティソリューション「VERZEUSE[®]※3」シリーズとして提供することを目指しています。

VERZEUSE[®]シリーズは 2023 年に初のソリューションを発表して以降、自動車業界が直面するサイバーセキュリティ課題に対応するため継続的にソリューションの拡充を進め、2025 年には「EdgeTech+ AWARD 2025」を受賞しました。近年は、AI 技術の急速な発展に伴い、サイバーセキュリティのリスクは一層高度化・複雑化しており、セキュリティ対策の重要性は益々高まっています。今回の発表で課題提起した新たな脅威も踏まえて「AI による攻撃から車両を守る」「車載 AI を守る」「AI で車両を守る」という 3 つの観点で VERZEUSE[®]シリーズの刷新を進めていきます。

今後も当社は、安全で信頼性の高いモビリティ社会の実現に貢献していきます。

※1 International Information System Security Certification Consortium, Inc.

※2 <https://web.cvent.com/event/061e8b17-0965-49f5-9097-58f0b69a305d/summary>

※3 VERZEUSE[®]は、パナソニック オートモーティブシステムズ株式会社または関連会社の日本国における登録商標です。スペイン語で「見る」を意味する「Ver」と、「神」を意味する「Zeus」を組み合わせた造語です。空または上空から神のごとく、社会の安全を見守るという意味を込めています。

パナソニック オートモーティブシステムズ株式会社について

パナソニック オートモーティブシステムズ株式会社は、日本を本社とし、海外 8 カ国に傘下子会社を有するグローバル企業です。Tier 1 として、国内外の自動車メーカーに、インフォテインメントシステムをはじめとする当社ならではの先進技術を提供し、快適で安心・安全なクルマづくりに貢献しています。企業ビジョンに、世界一の「移ごこちデザイン」

カンパニーを掲げ、人に寄り添う技術で世界のお客様のご期待にお応えします。
なお当社は、2027 年 4 月 1 日より社名を「モビテラ株式会社」に変更いたします。

<https://automotive.panasonic.com/>

報道関係者様 お問い合わせ先

パナソニック オートモーティブシステムズ株式会社 経営企画センター コーポレートコミュニケーション室

e-mail: press-pas@ml.jp.panasonic.com