VicOne

Driving Automotive Cybersecurity Forward

VicOne 2023 年自動車サイバーセキュリティ脅威動向

はじめに

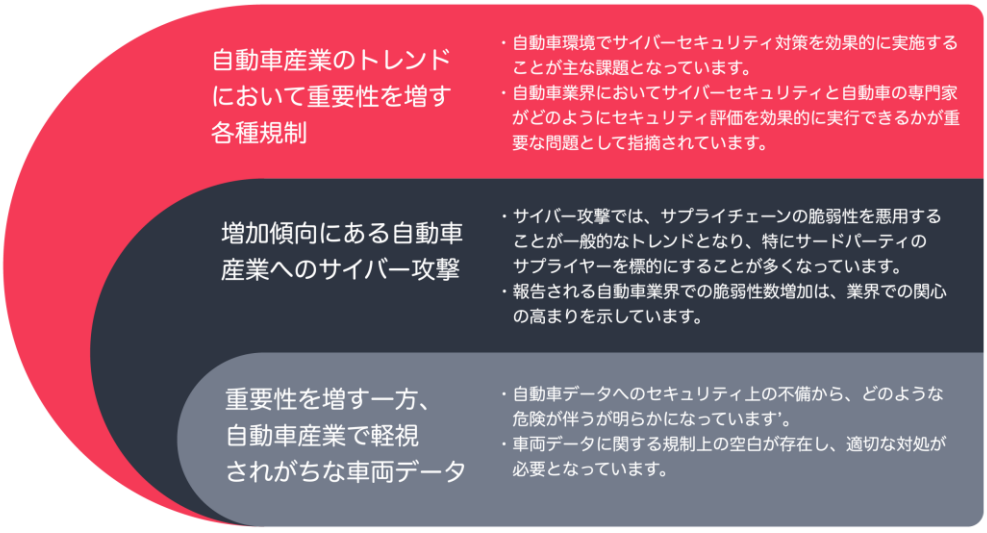
自動車業界がデジタル変革を進める中、サイバー脅威の状況も進化し広がり続けています。車両の複雑さが増し、接続性、自動化、先進運転支援システム（ADAS）の統合が進むことで、これらはサイバー攻撃や新たな脅威に対して脆弱になっています。VicOne は、自動車業界が車両の安全確保に直面する障壁を認識し、複雑な状況下でのサイバー攻撃の重大な影響を認めています。

本稿では、自動車業界に影響を与える現在のサイバーセキュリティの動向と脅威に関する包括的な概要を提供します。本稿の調査では、業界のコンプライアンスの過程を振り返り、重要なサイバーセキュリティ規制や、IT サイバーセキュリティプロセスを自動車の実践に適用する際の課題とギャップを検討します。さらに、自動車会社が直面する一般的な脆弱性とリスクを特定し、資産保護の重要性を強調します。

本稿の重要な部分として、新技術の導入に伴うリスクを強調する事例調査が含まれています。これは、革新と堅牢なセキュリティ対策のバランスの必要性を指摘します。また、最新のサイバーセキュリティ動向に関するユニークな視点を提供し、これらの進化する課題に対処する実践的な解決策を議論します。

本稿で提示する知見と推奨事項は、自動車メーカー（OEM）およびサプライヤーに対し、賢明な決断を下し、車両をサイバー攻撃から守る戦略を実施するための指針となります。その上で、このリサーチペーパーが現代の自動車サイバーセキュリティの複雑さをナビゲートするための貴重なリソースであることを目指しています。

主要ポイント



コンプライアンスの課題

2022 年 7 月から自動車メーカー（OEM）に義務付けられた国連規則 No.155（UN R155）により、様々な ISO 規格の採用が急務となっています。中でも、ISO 26262、ISO/SAE 21434、Trusted Information Security Assessment Exchange（TISAX）、および Automotive Software Process Improvement and Capability Determination（ASPICE）が重要であり、特に ISO 26262 と ISO/SAE 21434 は、OEM が直面する大きな課題となっています。

ISO 26262 は機能安全に主に焦点を当てており、OEM は、市場認証のため、多くの場合、この分野を優先します。他方、ISO/SAE 21434 は情報セキュリティへと焦点を移し、多くの OEM が見落としやすい重要な側面を扱い、自動車産業の課題に特に焦点を当て、堅牢な情報セキュリティ実践の重要性を強調しています。

加えて、2024 年 7 月までには、UN R155 により、新たに製造される車両に対する安全基準が義務化されます。これは業界にとって次なる大きな課題といえます。OEM は、過去 1 年間の重要な焦点領域を踏まえ、この期間内に新しいプロセスを導入するか、既存のプロセスを改善するかを検討する必要があります。

VicOne は数年間、自動車サイバーセキュリティの最前線で活動し、様々な OEM が ISO 規則要件を満たすための指導と支援を提供してきました。以下、VicOne が豊富な経験を生かし、クライアントがこれらの変化する各種の規制状況に対応して遵守するための方法について説明します。

規制の導入方法と業界への影響

自動車業界でのビジネスの役割によって、規制への対応が積極的か消極的かが大きく変わります。この分野は、数十年にわたり規制に従ってきた OEM やサプライヤー、そして基準の理解と実施を始めたばかりの企業などを含んでいます。

特に ISO/SAE 21434 における内部サプライチェーン管理の要求が大きな懸念事項といえます。例えば、ISO/SAE 21434 の RQ-05 は、OEM とそのサプライチェーンに対して、製品品質、サイバーセキュリティガバナンス、人員構成について継続的に報告することを義務付けています。ここでの主な課題は、これらの要件がソフトウェア供給業者や情報セキュリティプロバイダーだけでなく、ブレーキシステムやヘッドライトなどの機械部品を提供する企業にも及ぶことです。ISO/SAE 21434 は、機能安全に焦点を当てた ISO 26262 を基にしているため、要求は車両の全サプライチェーンに影響を及ぼします。

ISO ワークフローに既に慣れている下流サプライヤーにとっては、これらの変更に適応することは比較的簡単です。彼らは、既存の認証を新しい要件に合わせ、必要な文書を作成するだけです。

しかし、これまでこれらの認証を取得していない大多数のサプライヤーにとっては、課題は深刻となります。現実的には、多くの従来型サプライヤーは情報セキュリティと無関係であり、RDSEC、運用セキュリティ（OPSEC）、製品セキュリティインシデント対応チーム（PSIRT）のような専門部署を持たない可能性があります。また、特に重要なコンポーネントにおいて安定性が最優先される場合、OEM がサプライチェーンを全面的に見直すことは現実的ではありません。サプライヤーが重要な ISO 認証に追いつくことができないため、多くの OEM は代替ソリューションを模索しています。

ISO/SAE 21434 標準に準拠するための代替手段としてのペネトレーションテストと脆弱性管理

ISO/SAE 21434 は、OEM に自社の設計セキュリティを徹底的に検証することを義務付けていますが、準拠達成に向けたアプローチはさまざまです。品質管理、開発管理が確立され、整備されたサイバーセキュリティチームを持つ企業は、既存のプロセスを微調整して規制要件に対応できます。しかし、そうしたシステムを持たない他の企業にも、ISO/SAE 21434 に準拠する方法は存在します。この規制の主目的は、「設計による安全性」を証明することにあります。したがって、グループ討議やペネトレーションテスト、脆弱性管理などの第三者機関を活用することも、設計の安全性を示す有効な手段となり得ます。これは、ISO 26262 という業界の別の重要な標準とは対照的です。ISO 26262 では、危険分析とリスク評価（HARA）プロセスを厳格に遵守する必要があります。

ペネトレーションテストと脆弱性管理について再考すると、IT 業界はこれらの手法を数十年にわたり採用してきました。例えば、情報セキュリティ管理の国際標準である ISO/IEC 27001 があります。ペネトレーションテストやリスク評価などの定期的なタスクに対する大企業の受容は高まっています。ただし、IT 資産のセキュリティを強化するために設計された従来のペネトレーションテストは、道路の安全性全体を高めることを目的とする ISO/SAE 21434 の意図とは大きく異なる点に注意が必要です。

ペネトレーションテストの限界

ISO/SAE 21434 の主要な目標は、道路安全性を高めることです。ISO 基準を満たすための評価では、特に次のような問いを重視する必要があります。「ペネトレーションテストの対象が故障した場合、道路安全性にどのような影響を及ぼすか？」この観点は、多くのサイバーセキュリティプロバイダーが重視する内容とは異なります。彼らは通常、IT システムへの脅威を評価するために設計されたスコアリングシステム（例：コモン・バルネラビリティ・

スコアリング・システム、CVSS）に依存しています。車両システムにおいては、最も重要なのは常に道路安全性です。ペネトレーションテストの課題は、評価指標が IT 部門向けに設計されている点にあります。そのため、テスト報告書は重要でない結果に溢れがちで、車両の道路安全性向上や ISO 遵守プロセスの改善に役立つ情報が少ないのです。結果として、自動車メーカー（OEM）は多くのリソースを投入するものの、無関係な情報の山に直面することになります。従って、自動車のハードウェアと電子システムの両方に精通したサービスプロバイダーの存在が重要となります。

脆弱性管理の役割とその不適切な実施による影響

ペネトレーションテストと同様に、脆弱性管理に対する需要も急速に高まっています。この現象の主な要因は、国連の R155 規則と ISO/SAE 21434 です。国連の R155 規則は、サイバーセキュリティ管理システム（CSMS）の要件を 1 つの包括的なルールにまとめ、企業が車両のライフサイクル全体でサイバーセキュリティを管理することを求めています。ISO/SAE 21434 も、サイバーセキュリティ特性を持つコンポーネントは、そのライフサイクル全体で脆弱性管理を受ける必要があると規定しています。これは、ソフトウェアの材料表（SBOM）に基づく脆弱性管理サービスの普及を促しています。市場への参入を狙う伝統的な IT セキュリティベンダーの中には、急いで関連サービスを立ち上げるものもあり、OEM にとって課題を生んでいます。市場での存在感を高めようとするいくつかの SBOM スキャン製品は、数千、場合によっては数百万もの脆弱性を検出できると主張しています。しかし、フィードバックによれば、検出されたこれらの脆弱性の多くは誤検知であり、道路安全にはほとんど影響がないとされています。

ISO/SAE 21434 における TARA プロセスの課題への対応

ISO/SAE 21434 の重要な側面として、脅威分析およびリスク評価（Threat Analysis and Risk Assessment、TARA）のプロセスが挙げられます。VicOne は、2023 年に TARA に基づいたコンサルティングサービスの急増を記録しました。TARA は、OEM やサプライヤーにとって新たな大きな課題となっています。

一見すると、車両や部品をサイバー脅威から保護することは直接的な問題のように思えます。このアプローチは、ペネトレーションテストや脆弱性スキャンの目的と似ているように見えます。しかし、ISO/SAE 21434 の文書を詳しく検討すると、さらに幅広く重要な役割が明らかになります。文書には以下のように明示的に記されています[1]。

脅威シナリオの特定方法には、以下のグループディスカッションや体系的なアプローチが用いられることがあります。

- 合理的に予測可能な誤用や悪用から導かれる悪意あるユースケースの抽出
- EVITA、TVRA、PASTA、STRIDE（スプーフィング、改ざん、否認、情報漏えい、サービス拒否、特権昇格）などのフレームワークに基づく脅威モデリングのアプローチ

ISO/SAE 21434 は自動車のサイバーセキュリティ問題に対処し、それによる安全性の損失を防ぐことを目的としています。自動車の寿命が 10 年以上に及ぶことを考慮すると、この要求は合理的ですが、実装は非常に困難です。多大な人手を必要とし、どこから始めるべきか判断することさえ難しいといえます。

市場には ISO/SAE 21434 のプロセスを支援すると主張する多くの製品やサービスがありますが、これらの多くは報告書の作成や標準文書の言い換えを行うツールに過ぎません。実際の重労働は依然として OEM やサプライヤーの責任です。ISO 文書はグループディスカッションと体系的な分析の 2 つの主要な方法を概説しています。グループディスカッションはサイバーセキュリティや車両安全の専門家が関わる直接的な手法ですが、体系的アプローチの詳細はまだ不明確です。あらゆるシナリオを考慮する際、企業は推測に基づくブレインストーミングを行うことが期待されているのでしょうか。

ISO コンサルタントは、各コンポーネントの潜在的な故障シナリオを示す資産中心のアプローチから始めることを推奨します。自動車サプライチェーンの研究開発（R&D）部門のスタッフは、自社のコードが故障する可能性のあるシナリオを想定できます。一方、サイバーセキュリティ専門家は、過去のセキュリティ侵害事例を基に、コンポーネントの故障や不具合を予測することができます。理想的には、R&D 部門とセキュリティ部門の洞察を統合し、脅威の実現可能性と攻撃経路を評価する包括的なシナリオを作成します。しかし、R&D にとってはサイバー攻撃のような予測不能な出来事を予測することは難しいといえます。また、IT セキュリティの前例が自動車の安全基準に必ずしも適用されないことも、専門知識の特異性を反映しています。これら 2 つの要因が組み合わさり、潜在的な問題に対して徹底的に取り組むアプローチは大きな課題を生じます。加えて、ISO/SAE 21434 の TARA セクションには曖昧で不確定な要件が多く、多くの企業がプロセスを標準化するためには膨大な人的投資が必要です。

では、OEM とサプライヤーは TARA プロセスの課題にどう対処すべきでしょうか。VicOne は、独自の視点から、OEM の TARA 実施チームが効率的な標準運用手順（SOP）を確立する方法を考案しました。このアプローチは、現実の脅威に密接に連動する自動車の脅威情報に基づいており、不要なステップを排除します。結果として、この戦略は OEM の TARA プロセスを大幅に簡素化し、ISO コンプライアンスへの移行をスムーズに促進しています。

脅威動向について

前のセクションでは、各種規制に関する状況を確認しつつ、導入に伴う課題を理解し、誤ったアプローチを避ける方法について説明しました。このセクションでは、サイバーセキュリティの脆弱性およびサイバーインシデントの事例を集約し、自動車業界が直面する現在の問題を特定することで、ベンダーが自社システムや車両で抱える問題への対応方法について説明します。

報告された数百件脆弱性

VicOne では、自動車関連のコンポーネントやサービスに関連する共通脆弱性と公開された識別子（CVE）を監視することに常に焦点を当ててきました。2019 年以降、報告された CVE の数が大幅に増加していることが確認されています。毎年 200 件以上が報告されており（2023 年に至っては前半だけで）、近年、自動車のサイバーセキュリティに対する注目が高まっています。

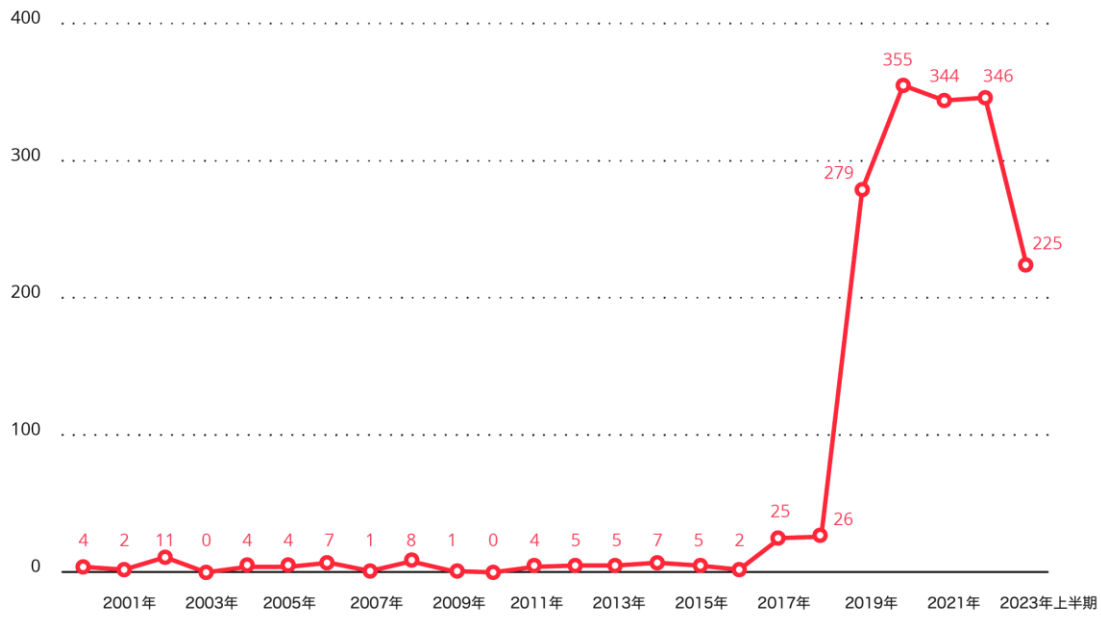


図 1：2000 年から 2023 年 上半期までの脆弱性（CVE）件数

以下の表は、CVE の中で特定した共通弱点列挙（CWE）の脆弱性の要約を示しています。データセットで最も頻繁に見られる問題は、範囲外書き込み（OOBW）、範囲外読み取り（OOBR）、バッファオーバーフロー、使用後解放、不適切な入力検証の脆弱性です。2023 年前半では、ウェブサイトやアプリケーション管理における SQL インジェクションの

脆弱性の異なるケースが見受けられます。整数オーバーフローやラップアラウンドの脆弱性の大半は、チップセットの異なるコンポーネントで発生しています。

CWE ID	名称	詳細
CWE-787 [2]	範囲外書き込み	製品は、意図したバッファの終端を超えて、または始端の前にデータを書き込みます。
CWE-416 [3]	使用後解放	解放されたメモリを参照すると、プログラムがクラッシュしたり、予期しない値を使用したり、コードを実行したりする可能性があります。
CWE-125 [4]	範囲外読み取り	製品は、意図したバッファの終端を超えて、または始端の前にデータを読み取ります。
CWE-120 [5]	入力のサイズを確認せずにバッファをコピーする（典型的なバッファオーバーフロー）	製品は、入力バッファのサイズが出力バッファのサイズより小さいかどうかを確認せずに、入力バッファを出力バッファにコピーし、バッファオーバーフローを引き起こします。
CWE-20 [6]	不適切な入力検証	製品は入力またはデータを受け取りますが、その入力がデータを安全かつ正確に処理するために必要な特性を持っているかどうかを検証しないか、誤って検証します。

表 1：自動車業界で確認された全公開公開済み脆弱性（CVE）トップ 5CWE

CWE ID	名称	詳細
CWE-125	範囲外読み取り	製品は、意図したバッファの終端を超えて、または始端の前にデータを読み取ります。
CWE-787	範囲外書き込み	製品は、意図したバッファの終端を超えて、または始端の前にデータを書き込みます。
CWE-120	入力のサイズを確認せずにバッファをコピーする（典型的なバッファオーバーフロー）	製品は、入力バッファのサイズが出力バッファのサイズより小さいかどうかを確認せずに、入力バッファを出力バッファにコピーし、バッファオーバーフローを引き起こします。
CWE-89 [7]	SQL コマンドにおける特殊要素の不適切な無	製品は、上流コンポーネントからの外部からの影響を受けた入力を使用して SQL コマンドのすべてまたは一部を構築しますが、ダウンストリームコンポーネントに送信される

CWE ID	名称	詳細
	効化（SQL インジェクション）	際に意図した SQL コマンドを変更する可能性のある特殊要素を無効化しないか、または不適切に無効化しています。
CWE-190 [8]	整数のオーバーフローまたはラップアラウンド	製品は、元の値よりも常に大きくなるというロジックを前提とした場合に、整数のオーバーフローやラップアラウンドを引き起こす可能性がある計算を行います。この計算は、リソース管理や実行制御に使用される場合、他の弱点を引き起こす可能性があります。

表 2：自動車業界で確認された全公開公開済み脆弱性（CVE）トップ 5CWE（2023 年上半期）

2023 年上半期に報告された脆弱性の大半は、チップセットまたはシステムオンチップ（SoC）に関連する問題が占めています。これに続いて、サードパーティの管理アプリケーションや車載情報娯楽（IVI）システムの脆弱性も確認されました。

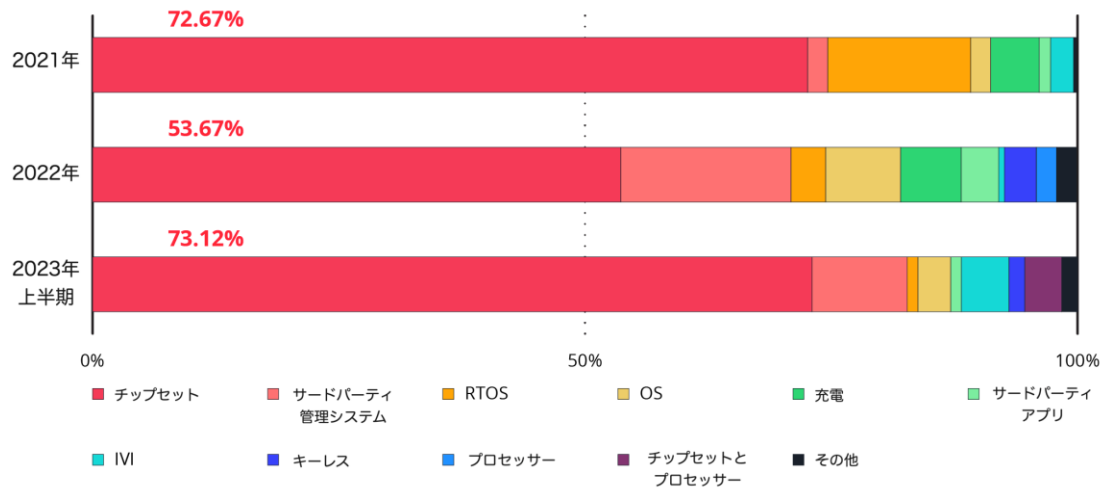


図 2：2021 年、2022 年、および 2023 年上半期におけるトップ脆弱性セキュリティ問題別の分布

サイバー攻撃とセキュリティインシデントの増加

車両やそのシステム固有の脆弱性に加え、多数の自動車関連インシデント事例を収集・分類しました。これらの事例の大半はサイバー攻撃、イモビライザーの問題、アプリケーション及びアプリケーションプログラミングインターフェース（API）に関連する問題でした。

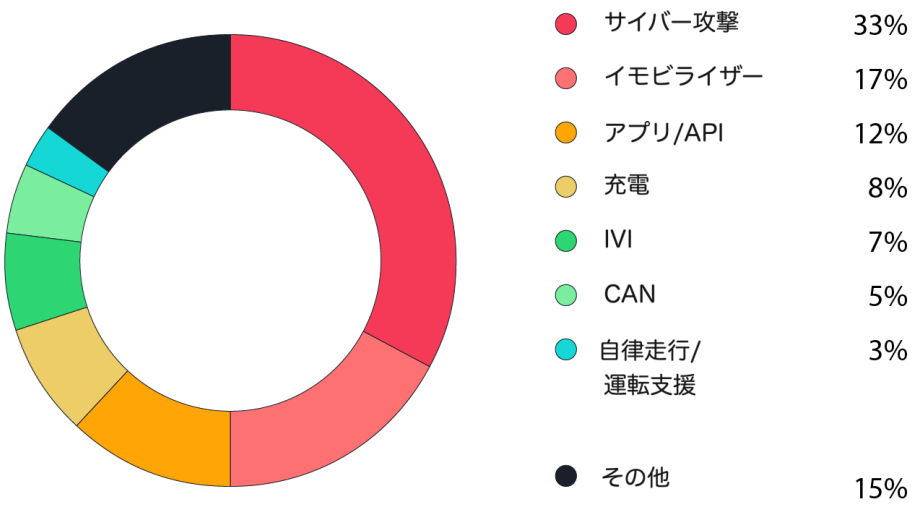


図 3：2022 年後半から 2023 年前半にかけてのセキュリティインシデント事例のカテゴリ別分布

サイバー攻撃インシデントを詳しく調べると、多くの事例がサービスや診断を提供するサードパーティ業者や自動車部品供給者に起因していることがわかります。これらには製造会社、物流プロバイダー、サービス提供者、部品やアクセサリーを生産する企業が含まれます。

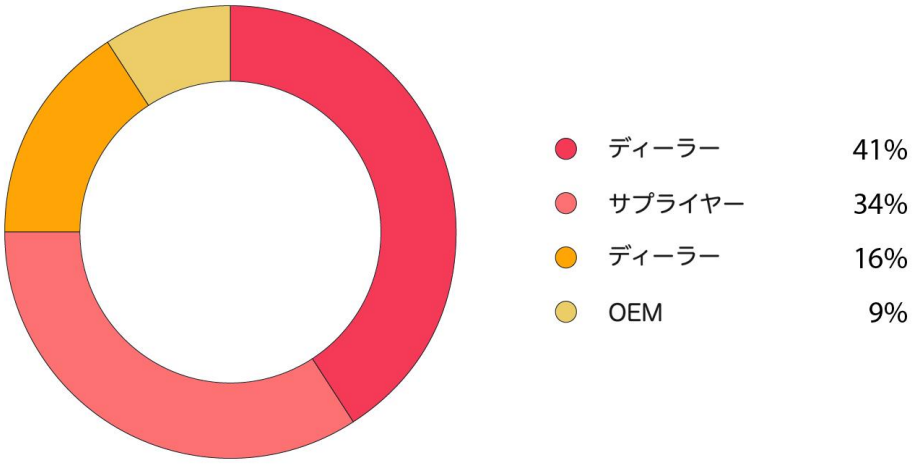


図 4：2022 年後半から 2023 年前半にかけてのサイバー攻撃事例のカテゴリ別分布

また、2021 年から 2023 年に発生したサイバー攻撃インシデントの財務的影響を推定する計算を行いました。影響とコストはランサムウェア攻撃による被害、漏えいしたデータや個人識別情報（PII）の露出、システム停止期間に伴う損失に関連しています。これらの費用は技術や運用に関連する実質的なコストを含み、ブランディング、パブリックリレーションズ、セールス、マーケティング費用などの無形コストは考慮されていません。

費用	2021 年	2022 年	2023 年上半期
ランサムウェアによる損害	US$74,755,025	US$142,003,000	US$209,675,448
情報漏えい／個人情報の露出	US$13,795,000	US$4,000,000	US$9,574,700,000
システムダウンタイムのコスト	US$1,300,385,123	US$802,432,329	US$1,998,351,233
総損害費用	US$1,388,935,148	US$948,435,329	US$11,782,726,681

表 3：2021 年から 2023 年上半期にかけてのサイバー攻撃被害コスト推定

この推定によれば、自動車業界を狙ったサイバー攻撃が増えており、被害コストも上昇傾向にあることが示されています。

地域別データ

2023 年上半期に報告されたサイバー攻撃の大部分は北米とヨーロッパからで、2022 年に見られた傾向が続いています。しかし、一般的なセキュリティインシデントでは、特に 2023 年上半期にアジア太平洋地域からの報告が顕著です。

北米	43%
欧州	30%
アジア太平洋	20%
グローバル	6%
アフリカ	1%

表 4：2022 年における自動車産業のセキュリティインシデントの地域分布

北米	31%
グローバル	28%
アジア太平洋	23%
欧州	13%
南米	5%

表 5：2023 年上半期における自動車産業のセキュリティインシデントの地域分布

北米	45%
欧州	32%
アジア太平洋	21%
南米	1%
グローバル	1%

表 6：2022 年に報告された自動車産業におけるセキュリティインシデントからのサイバー攻撃の地域分布

欧州	41%
北米	41%
アジア太平洋	13%
南米	3%
アフリカ	1%
アラブ諸国	1%

表 7：2023 年上半期に報告された自動車産業セキュリティインシデントからのサイバー攻撃の地域分布

地域	国	
アジア太平洋	オーストラリア	フィリピン
	中国	シンガポール
	インドネシア	韓国
	日本	台湾
	マレーシア	
欧州	フランス	スペイン
	ドイツ	スイス
	イタリア	トルコ
	オランダ	イギリス
北米	カナダ	米国
南米	メキシコ	

表 8：2022 年に報告された自動車サイバー攻撃の国別一覧

地域	国	
アフリカ	モーリシャス	
アラブ諸国	モロッコ	
アジア太平洋	オーストラリア	韓国
	インド	台湾
	日本	タイ
	シンガポール	
欧州	ベルギー	ポーランド
	チェコ共和国	ポルトガル
	デンマーク	ロシア
	フランス	スペイン
	ドイツ	スウェーデン
	ギリシャ	スイス
	イタリア	トルコ
	オランダ	イギリス
	ノルウェー	
北米	カナダ	米国
南米	ブラジル	ペルー
	メキシコ	

表 9：2023 年上半期に報告された自動車サイバー攻撃の国別一覧

ケーススタディ

現在の脅威動向の概要に続いて、さらなる重要事項を強調するため、実際のインシデント事例 3 件を詳細に検証します。これらの事例には、CPU、CAN インジェクション、アプリ/API に関連する顕著な脆弱性が含まれています。

これらのケーススタディは、現在の脆弱性と車両エコシステムへの新技術導入が、アタックサーフェスを拡大し、新たなリスクを生み出す状況を示しています。さらに、これらの事例は、攻撃者が車両の制御を得るだけでなく、機密情報を盗んだり妨害したりする可能性も示唆しています。

Zenbleed

2023 年 7 月、Google のセキュリティリサーチャーTavis Ormandy 氏は、AMD 社製の Zen 2 マイクロアーキテクチャ [9] に重大な脆弱性が存在することを明らかにしました。この脆弱性は、Zenbleed と呼ばれ、コアあたり秒速 30kb で機密データが漏洩する可能性があるという顕著な脅威をもたらします。

これまで CPU は自動車と直接的な機能的な関連性を持ちませんでした。しかし、ソフトウェア定義車（SDV）の登場によって、この状況が一変しました。現在では、多くの車両に機能を強化するための強力な CPU が搭載されています。運転支援や自動運転などの先進機能が普及するにつれて、これらの機能を支える複雑な計算を処理するために、強力な CPU や GPU への依存が増しています。

こうした業界のニーズに応えるべく、AMD 社は自動車用デジタルコックピットソリューションを導入しました。しかし、AMD 社製 Zen CPU をコアプロセッサとして使用する車両は、脆弱性 Zenbleed という重大なセキュリティリスクに晒されています。この脆弱性は、パスワードやトークンなどの機密情報の流出を引き起こす可能性があり、車両及びその乗員のセキュリティとプライバシーを危険にさらすことになります。

軽減策

脆弱性 Zenbleed への対応は、影響を受けるシステムのセキュリティを保護する上で重要です。CPU ハードウェアは回路の変更による修正パッチが不可能なため、代替解決策が必要となります。この脆弱性は AMD 社に報告され、同社はファームウェアのマイクロコードアップデートをリリースして問題に対処しました。影響を受けた AMD 社製 CPU を搭載する OEM の車両では、車両のアップデート機構に応じて、OTA アップデートや製品リコールを通じてマイクロコードアップデートを適用できます。マイクロコードアップデートの適用が不可能な場合は、ソフトウェアの回避策が存在します。DE_CFG の「チキンビット」を設定

することでも脆弱性を軽減できますが、この方法には欠点があります。ソフトウェアの脆弱性修正を適用すると、脆弱性の起源がパフォーマンス最適化技術にあるため、パフォーマンスが低下する可能性があるからです。

脅威の観点から見ると、ハードウェアの脆弱性は珍しく、発生する可能性も低い問題です。しかし、発生した際には重大な問題を引き起こすことがあります。特にハードウェアの脆弱性、中でも CPU の脆弱性は修復が非常に難しいものです。ベンダーが CPU を交換することはほとんど不可能で、一部の欠陥はマイクロコードのアップデートで修正できますが、ソフトウェア修正が CPU の動作を遅くすることもあります。一つの問題を解決すると新たな問題が生じることもあり、CPU の脆弱性の軽減は特定の問題により異なり、多くの場合は修正不可能です。規制要件を考慮すると、脆弱性の軽減は非常に重要です。潜在的な被害シナリオを特定し、実際の被害が発生する前に対処する必要があります。ハードウェアの脆弱性、特に CPU に関連するものは完全に解決することはほぼ不可能ですが、こうした中でも、OTA アップデート、デバッグインターフェースの無効化、物理的保護などの他の対策も、解決策の一環として重要と言えます。

CAN バスインジェクション

1980 年代に導入されたコントローラーエリアネットワーク（CAN）バスは、自動車用途専用に設計された通信プロトコルです。CAN バスが登場する前、自動車メーカーは多数の点対点接続に頼っていましたが、それは複雑でかさばる配線システムを必要としていました。現在、CAN バスは自動車業界で広く採用された標準となり、ほとんどの現代車に使用されています。CAN バスは派手な技術ではないものの、自動車業界で堅牢かつ確立されたシステムとして存在しています。バスオフ攻撃[10]、CANCAN[11]、weepingCAN[12]などのいくつかの既知の問題がありますが、それでも車両通信技術としてはトップクラスです。

CAN バスに新たに登場した課題は、「CAN バスインジェクション」という攻撃手法で、これは Ian Tabor 氏と Ken Tindell 氏によって発見されました[13]。この手法を使うと、潜在的な攻撃者が車両を盗みやすくなり、2023 年に入って犯罪者たちに頻繁に使用されています。多くの人にはあまり知られていないかもしれませんが、2023 年上半期に報告された主要な脅威の 1 つとなっています．この問題は、CAN バスおよびイモビライザーに関連する 2 つの種類の脅威と言えます。こうした脅威が車の設計に大きな影響を与える問題であることは確かであり、想定される攻撃シナリオは以下の通りです：

- 潜在的な攻撃者は、スマートキー受信機の電子制御ユニット（ECU）が接続されているヘッドライトを通じて、車両の CAN バス配線にアクセスします。

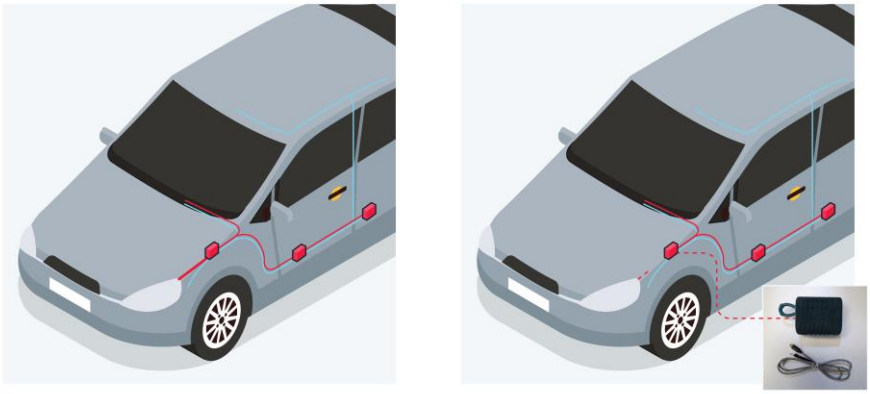


図 5：左図ではヘッドライトが車両の CAN バスに接続されたままとなっている。右図では、それが CAN インジェクターに置き換えられている

- CAN インジェクターが起動すると、潜在的な攻撃者はデバイスが応答を受信するまで、CAN バスを繰り返し起動するための起動フレームを送信することができます。
- 応答を受け取った後、CAN インジェクターは以前述べた仲裁メカニズムによって生じる支配的オーバーライド回路を活用します。この回路は、他のデバイスが CAN バスで通信するのを阻止し、CAN バスプロトコルのエラーメカニズムを無効化します。これにより、他の ECU が CAN インジェクターを停止することや、一部のセキュリティハードウェアを迂回することが防がれます。
- この時点で CAN インジェクターは、スマートキーECU に偽装して、「キー認証済み、イモビライザーを解除」という偽のメッセージを車両のゲートウェイ ECU に連続して送信します。
- ゲートウェイ ECU はこの偽のメッセージを別の CAN バスに転送します。

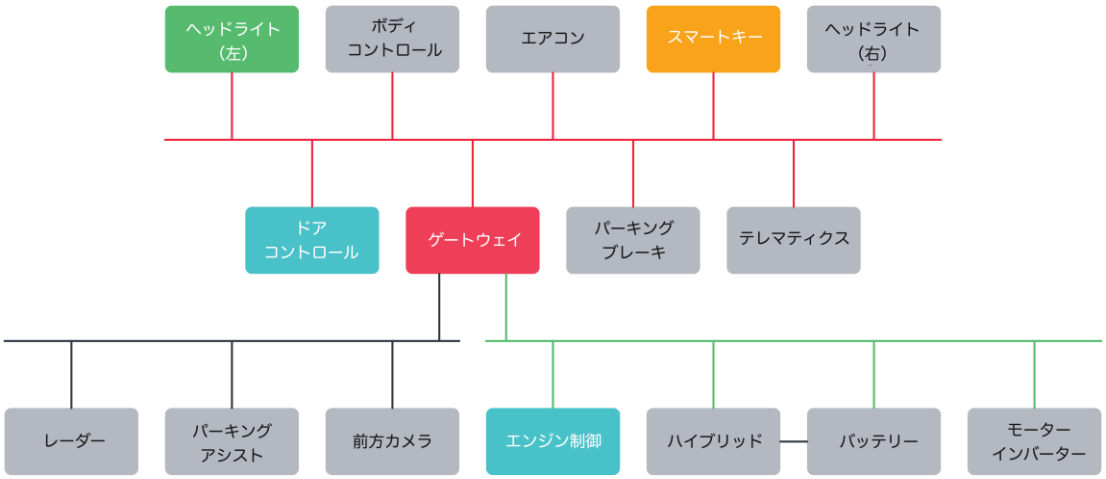


図 6：盗難車両の簡略化された CAN バス図（Ken Tindell のオリジナル画像に基づく）[14]

- エンジン制御システムは偽のメッセージを受け入れ、イモビライザー機能を解除します。
- CAN インジェクターは、「キー認証済み、ドアを解除」という別の偽の CAN メッセージをドア ECU に連続して送信し、車両のドアを解錠します。

図 7：アンロッカーツールセット。赤で囲まれているのは、車両の CAN バスに接続するためのケーブルの 2 本のピン、CAN ハイと CAN ローです（Ken Tindell のオリジナル画像に基づく）[15]

インターネットアーカイブの初期データによると、このツールセットは 2022 年 6 月 18 日から Keyless Go Repeater のウェブサイトで販売され始めました[16]。アーカイブを確認したところ、1 台あたりの価格は 3,500 ユーロ（約 3,700 米ドル）でした。初回リリース時もこの価格であったかは不明ですが、2022 年から利用可能であることは確認されています。さらに、簡単な調査で、このツールセットの価格が通常 1,500 ユーロ（約 1,600 米ドル）から 5,000 ユーロ（約 5,300 米ドル）の範囲であることが多くのウェブサイトで確認されました。ツールセットは通常、小さな箱の形をしており、一部のバージョンは JBL の Bluetooth スピーカーや Nokia 3310 の携帯電話のように見えるデザインになっています。この擬装により、デバイスが見つかっても、法執行機関がそれが何であるかを識別するのが難しくなります。

ベンダー	価格
Keyless Go Repeater [17]	€4,500 (around US$4,700)
Shop-Auto-PODOLSK [18]	US$4,000
AutoDecoders [19]	€1,500 (around US$1,600)
Agent Grabber [20]	€4,500 (around US$4,800)
UnlockCars Grabber [21]	€3,500 (around US$3,700)
Kodgrabber [22]	US$5,000

表 10：2023 年 8 月時点でのさまざまなウェブサイトにおけるアンロックツールの価格

緩和策

Tindell 氏によると、攻撃を防ぐ方法としては、一時的なものと恒久的なものの 2 つが提示されています。

一時的な対策としては、ゲートウェイ ECU を再プログラムする方法が効果的です。特定の時間内にエラーが検出されない場合にのみメッセージを転送することで、CAN バスに故障を引き起こすインジェクターや、スマートキーCAN フレームを送信できる事実を回避します。この方法は、CAN インジェクターがメッセージをフィルタリングする機能に依存しています。しかし、攻撃者は容易に適応し、類似の攻撃を考案する可能性が高いとは言えます。

恒久的な解決策としては、ゼロトラストアプローチを採用し、CAN デバイスが他の ECU からのメッセージをデフォルトで信頼しないようにすることです。代わりに、ECU の真正性を確認するための追加の検証手段を CAN フレームに実装することができます。これを実現するには、ECU に秘密鍵を提供し、特定の車両とペアリングする必要があります。

これらの緩和策は、工学的な観点から導かれています。しかし、規制の観点から見ると、さらに多くの緩和策が考えられます。例えば、ゲートウェイ ECU に対する OTA アップデートを可能にし、リアルタイムでの対応を実現することや、テレメトリーメッセージを改善して早期に脅威を検出することが有効です。さらに、物理的保護を強化することで、追加の防御層を設けることができます。これらの追加対策は、損害シナリオに組み込まれ、潜在的な攻撃者に対するより強固な障壁を形成すべきだと言えるでしょう。

自動車クラウドサービスの侵害

接続された車両の主な特長は、インターネットへの接続能力です。この車両はネットワークリソースにアクセスし、同時にテレメトリーデータを送信することができます。この能力によって、車両は単なる移動手段から、価値ある情報を提供し、さまざまな機能を実行できるデバイスへと変化します。以下の図は、VicOne によるビジョンを示しています。これは、クラウドに接続された車両エコシステムで、現代の接続された車両が車輪付きの巨大なスマートフォンに変わり、サードパーティが提供するクラウド接続アプリケーションが運転手や乗客の体験に重要な役割を果たす様子を描いています。

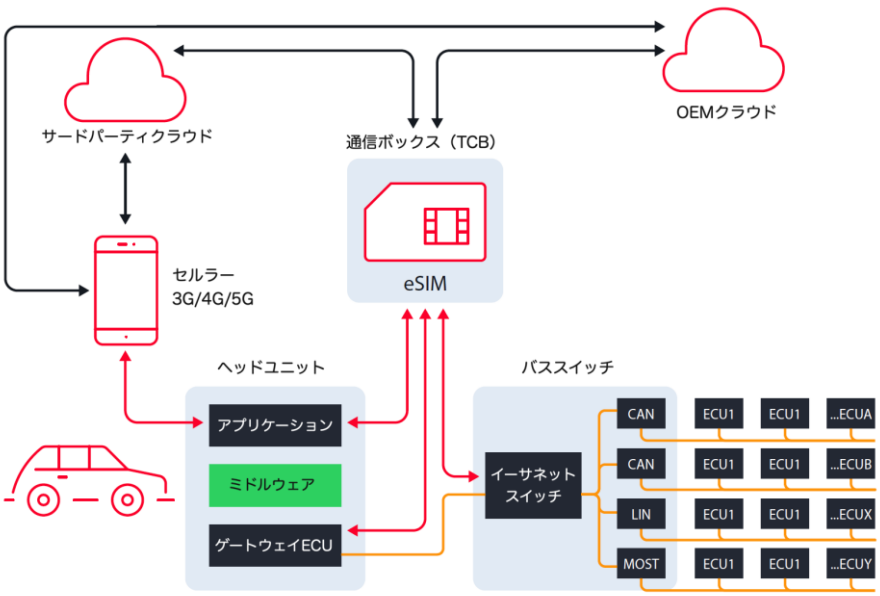


図 8：ラウドに接続された車両のアーキテクチャ [23]

ほとんどのコネクテッドカーは、サービスやデータへのアクセスのために OEM またはサードパーティのクラウドサービスに接続しています。この設計アーキテクチャは理にかなっており必要不可欠に見えますが、新たな課題も生じさせています。

2023 年 1 月に公開されたブログ記事で、Web アプリケーションセキュリティリサーチャーの Sam Curry 氏および同氏のチームは、テレマティクスシステムと API の脆弱性を突いて、異なる OEM のバックエンドクラウドインフラにアクセスする方法を示しました。特に Mercedes-Benz の事例において、車両修理工場用に作られた公開ウェブサイトを発見しました。このウェブサイトは、企業の核となる従業員向け LDAP（Lightweight Directory Access Protocol）システムと同じデータベースへ書き込まれていました。このサイトに登録することで、彼は従業員用アプリケーションへの限定的なアクセスを得て、その後、Mercedes-Benz の GitHub を含む機密性の高い内部アプリケーションへさらにアクセスを拡大しました。そこでは、顧客の車両と通信するアプリケーションを構築するための詳細な指示が見つかりました [24]。

これらの発見からは明確なメッセージが確認できます。自動車業界も、IT 業界のクラウドサービスが直面している問題から免れているわけではありません。しかし、比較すると、自動車業界はこれらの問題に対処するための準備が十分ではないことが明らかです。

脆弱性の分析

Curry 氏の発見を基に、影響を受けたクラウドサービスのウェブサイトで発生している共通の脆弱性（CWE）のリストをまとめることができます。これにより、シンプルな現実が浮

き彫りになりました。これらの問題は IT 業界で何千回も発生していますが、自動車業界は十分に周知されているとは言えません。

ここで指摘されているのは 2 種類のクラウド関連問題です。1 つ目は認証と認可に関わる問題、2 つ目は入力パラメータの適切なサニタイズ（消毒）に関わる問題です。認証に関しては、API が適切なアクセス制御を欠いており、事前認証の問題や個人情報（PII）へのアクセスが起こり得ます。認可については、API がユーザー権限を十分にチェックせず、ユーザーのリクエストをそのまま信用してしまうことがあります。2 つ目の問題、入力パラメータの適切なサニタイズに関しては、解決策は「ユーザーを決して信用しない」というシンプルな原則に従うことです。これは、「入力の検証とサニタイズは常に重要である」という言葉に示されています。入力検証は、適切な形式のデータのみがソフトウェアシステムのコンポーネントに入ることを保証するプログラミング技術です [25] 。この概念は広く知られているプログラミングの原則ではありますが、適切なコーディングスタイルガイドや継続的インテグレーション／継続的デプロイメント（CI/CD）環境がないと、実装は依然として困難であると言えます。

CWE ID	名称	詳細
CWE-20	不適切な入力検証	この脆弱性が悪用されると、ソフトウェアが入力を検証しないか、または不適切に検証することで発生し、制御フローやデータフローを変更する可能性があります。
CWE-287	不適切な認証	この脆弱性が悪用されると、システムがユーザーの身元を正しく確立できない弱点であり、攻撃者が正当なユーザーになりすます可能性があります。
CWE-284	不適切なアクセス制御	この脆弱性が悪用されると、ソフトウェアがユーザーやプロセスが特定のアクションを実行するために必要な権限を持っているかどうかを検証しない場合に存在し、権限のないアクセスやデータの変更につながる可能性があります。
CWE-639	安全でない直接オブジェクト参照（IDOR）	この脆弱性が悪用されると、アプリケーションが内部実装のオブジェクト（例えばデータベースの記録）を公開し、攻撃者がデータへの不正アクセスを得るために操作できる場合に発生します。
CWE-89	SQL インジェクション	これは、不正な SQL 文をエントリーフィールドに挿入して実行することでデータを破壊または削除できるコード注入の手法です。通常、ユーザー入力が不適切にフィルタリングされたりエスケープされたりしないことから生じます。
CWE-798	ハードコーディングされた認証情報の使用	この脆弱性が悪用されると、ソースコード内に明示的な資格情報（ユーザー名やパスワードなど）を含めることを指し、攻撃者が不正アクセスに利用する可能性があります。

表 11：Sam Curry 氏の調査に基づく脆弱性（CWE）の一覧

緩和策

理想的には、これらの問題は設計段階で特定されるか、製品化する前にペネトレーションテスターを雇用して早期に発見されるべきです。しかし、伝統的に自動車業界の開発プロセスは安全性に重点を置いており、サイバーセキュリティの側面への注意が不足していました。これが、現在の規制でサイバーセキュリティに対するより多くの注意が求められる理由です。幸いなことに、IT 業界の成熟した実践方法を取り入れることで解決策を見つけることができます。以下の表には、IT で一般的に使用されている実践方法が示されており、これらは自動車産業にも適用可能です。

方法	方法の論拠	活動	活動の詳細
教育と訓練	安全なコーディング慣行に関する定期的な訓練を行うことで、開発者は一般的な落とし穴を避けることができます。	ワークショップ	開発者がセキュリティ問題を扱う実践的な経験を得られるワークショップを開催します。
セキュアコーディング	一般的な脆弱性を防ぐために、セキュアコーディング基準に従います。		
ソフトウェア開発ライフサイクル（SDLC）	ソフトウェア開発ライフサイクルの各段階で、特に最後ではなく、セキュリティを組み込むことで、早期に脆弱性を特定し、軽減することができます。	セキュアバイデザイン	最初からセキュリティを念頭に置いてシステムを設計します。
コードレビュー	同僚によるコードレビューは、脆弱性になる前に潜在的な問題を発見するのに役立ちます。		
静的アプリケーションセキュリティテスト（SAST）および動的アプリケーションセキュリティテス（DAST）	これらはコード内の特定のタイプの脆弱性を自動的に検出することができます。		
外部監査	外部の専門家による定期的なセキュリティ監査は、脆弱性を特定し、アプリケーションのセキュリティについて独立した評価を提供するのに役立ちます。	ペネトレーションテスト	システムに対する攻撃を模倣するプロセスで、潜在的な脆弱性を特定します。
バグ報奨金	特にセキュリティ脆弱性に関するソフトウェアのバグを報告するための報奨金プログラム。		

表 12：IT 業界で一般的に使用され、自動車産業に応用可能なベストプラクティス

セキュリティ強化の最も重要な要素は、企業の上級経営陣からの支援です。セキュリティを向上させることで新たな懸念事項が生じ、プロジェクトの遅延が発生する可能性があります。これには相当な労力と財政的投資が必要で、その成果はすぐには見えないかもしれません。しかし、長期的には、これらの取り組みは非常に価値があることが証明されます。これらは規制上の観点から効果的な軽減戦略であり、問題が生じる前にリスクを積極的に減らすこともできます。

自動車業界の動向

ここ数年を経て最近の様々な動向に伴い、自動車業界は自身のニーズをより明確に理解するようになりました。これらの動向のほとんどは、すべて自動車ベンダーにコンプライアンスが求められるものであり、各種の基準や規制によって推進されています。今日、いかなるベンダーも最高の機能を有するだけでは不十分となっています。各ベンダーは市場に参入し、車両を販売する許可を得るために、規制遵守を示さなければなりません。このセクションでは、これら最近の動向を見ていきます。

規制コンプライアンス

前述の通り、現代の自動車産業において規制コンプライアンスは極めて重要です。そうした規制プロセスは多くの要求を含んでおり、これらの要求に応えるためには TARA やペネトレーションテストのようなツールが重要な役割を果たします。

TARA について

2021 年 3 月、国際連合欧州経済委員会（UNECE）は UN R155[26] を公表しました。その後の 2021 年 8 月には、ISO/SAE 21434 規格が発表され、道路上の車両の電気および電子（E/E）システムのサイバーセキュリティが注目されました。これら双方に関する文書は、車両のライフサイクル全体を通じて TARA 活動（Threat Assessment and Remediation Analysis の略で脅威評価と軽減分析を意味する）の重要性を強調しています。

TARA の主要な目的は、脅威の特定、リスク評価、リスクの優先順位付け、軽減策の提案の 4 つです。前述のように、OEM は、多くの場合、脅威シナリオや攻撃経路の分析に直面します。TARA で示された側面を理解することで、こうした一連の課題に対応することができます。このプロセスは、宝物を探して混沌としたジャングルをナビゲートすることに例えられ、目的地にたどり着くためには地図が不可欠であるのと同様、TARA は、その地図上で最適なコースを示す役割を果たします。

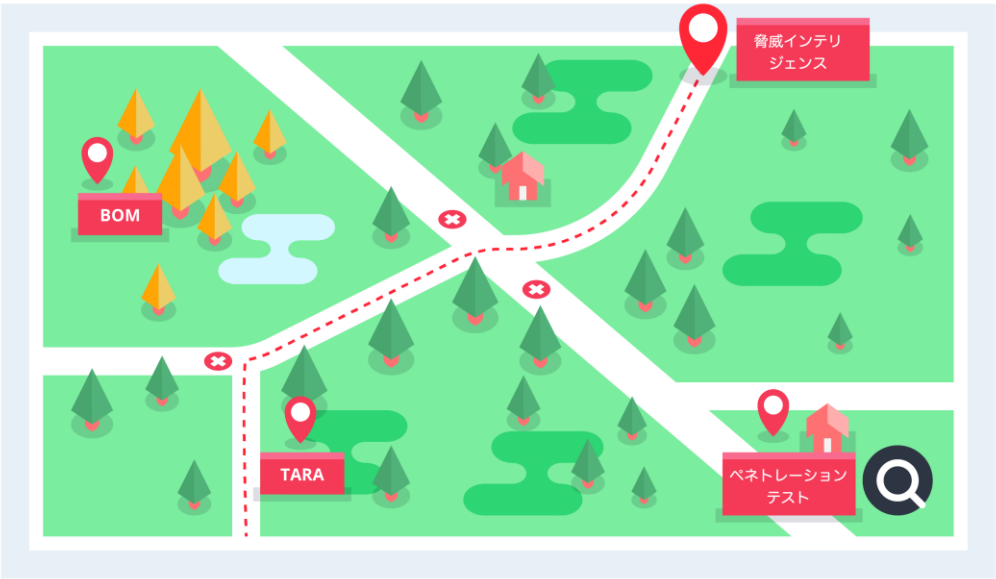


図 9：TARA やその他の重要ツールを使用して、潜在的な問題をマッピングする

規制遵守のために、企業や組織は以下のような重要項目のためのツールが不可欠となります。これらは先に示した図にも描かれています：

- 包括的な部品表（BOM）は、ソフトウェア BOM（SBOM）とハードウェア BOM（HBOM）が含まれ、地形に関する詳細な情報を提供します。
- 高品質な脅威情報は、宝の位置を正確に特定するのに役立ちます。
- TARA（脅威評価およびリスク分析）は、目標に到達するための最適なルートを計画するのに有効です。
- 目標が地図上で明確でない場合は、ペネトレーションテストを用いて、より詳細な調査を行うことができます。

各項目は、いずれも重要であり、どれか 1 つが欠けても、セキュリティ向上や緊急のセキュリティ問題に対処する目標達成が難しくなります。

全体のプロセスの中では、TARA が中心的な役割を果たし、いわば行動計画の背景にある設計図のように機能します。他の項目や情報も重要であり、例えば、不十分な脅威情報は時間の無駄になる可能性があり、間違った場所へ導かれることから、情報の質は極めて重要であると言えます。同様にペネトレーションテストは「宝」、つまり脆弱性の所在を特定する上で不可欠です。

TARA の活動は、単発の任務ではなく、継続することで、車両の設計方法を示し、潜在的な損害を未然に防ぐ戦略を提供します。

ペネトレーションテスト

自動車産業におけるペネトレーションテストのほぼ 100%は、ISO/SAE 21434 のサイバーセキュリティ目標を満たしているかを検証することを目的としていると言えます。ペネトレーションテストは、規制に合格する確実な方法ではありませんが、OEM にとって自社製品やシステムを予期せぬ方法で検査するための手段として有効です。

ペネトレーションテストには、1972 年に James P. Anderson 氏が初めて実施して以降、長い歴史があり、現在のペネトレーションテストプロセスに不可欠となった脆弱性発見の手順を提案しました [27]。現代では、ペネトレーションテストは外部攻撃者を模倣し、潜在的なサイバー脅威を評価するために使用されます。IT 業界においては、ペネトレーションテストの実践とプロセスは年々成熟化しています。ペネトレーションテストが品質保証（QA）と混同されることがありますが、これらはまったく異なるものです。QA テストはプロセスに注目するのに対し、ペネトレーションテストはコーディング構造の欠陥を明らかにすることに重点を置いています。

自動車業界におけるペネトレーションテストは IT 業界とは異なる特徴を持っています。IT では、主に見落とされがちな脆弱性を見つけて正しく修正することに焦点を当てています。例えば、ある API で特定の脆弱性が見つかった場合、同じ開発チームが類似のパターンを多くの場所で繰り返す可能性が高いため、関連する各 API の全体的なレビューが必要です。将来の被害を減らすためには、包括的なチェックが望ましいです。時には、問題がコードの脆弱性ではなく論理的またはアーキテクチャ的な脆弱性であることもあります。これらの問題は QA プロセスではほとんど検出できないため、ペネトレーションテストが有効です。

自動車業界では、ペネトレーションテストは IT 業界よりも複雑です。問題を特定するだけでなく、ハードウェアとソフトウェアの問題を同時に識別する必要があります。このプロセスは TARA（脅威分析およびリスク評価）と密接に統合され、通常 V モデルプロセスの右側で行われます。自動車の問題が生命に関わるため、ベンダーは可能な被害を最小限に抑えるために徹底的な検査が必要です。

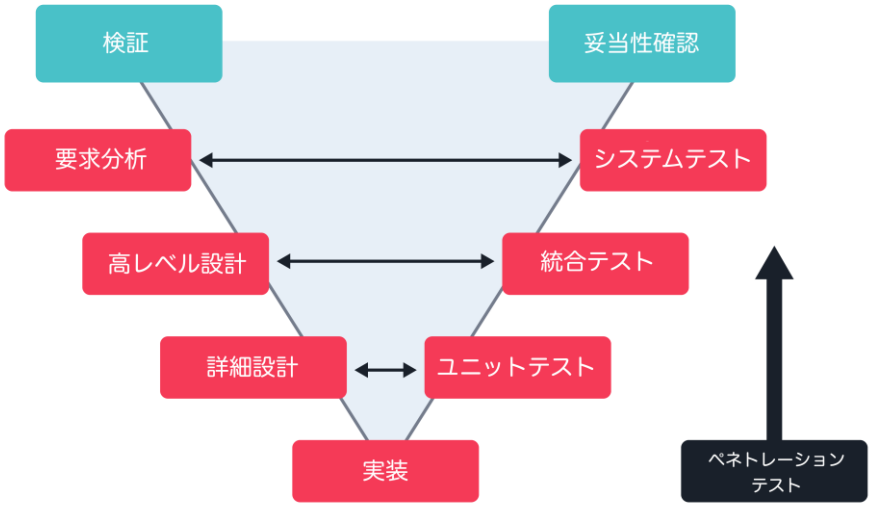


図 10：自動車ソフトウェア開発の V モデル

リスクマネジメント

自動車産業におけるリスクマネジメントは、サプライチェーン、製造、規制、市場、財務、技術など、多岐にわたる複雑な問題です。その範囲は最初に想像されるよりもずっと広くなっています。自動車産業は通常、リスクの特定と評価に多くの時間を費やし、それらを軽減する戦略を開発します。このプロセスには、継続的なモニタリングも含まれています。これらの取り組みはすべて、常に変化する環境における長期的な成功と安全を確保することを目的としています。

安全性は自動車産業において最も重要です。伝統的な製造業者は、多くの場合、機能安全のリスクに注目しがちですが、サイバーセキュリティのリスクにはそれほど重点を置いていません。しかし、車両がソフトウェア定義型モデルへと進化し、ほぼすべての機能がソフトウェアとハードウェアの連携を必要とするようになると、サイバーセキュリティリスクは、新しくかつ重要な懸念として浮上してきます。これは多くの伝統的な自動車メーカーにとって新しい分野であり、技術統合が車両の機能性とセキュリティにますます根ざしていく変化する環境を反映しています。適切なリスクマネジメントは、法的要件への適合を容易にする TARA 活動の処理にも役立つでしょう。

サイバーセキュリティリスク

サイバーセキュリティリスクとは、システム内で被害や不正アクセスを引き起こす可能性のある弱点や脆弱性を指します。車両の文脈では、これらの脆弱性はハードウェアに限らずソフトウェアにも及びます。これらは車両の様々な部品のレベルで発生する可能性があります。例えば、車の Wi-Fi 接続マネージャーのソフトウェア脆弱性が攻撃の侵害経路になることが

あります。同様に、ラジオ周波数のソフトウェア定義ラジオ（SDR）を使用してラジオ信号を記録・再生するといった簡単な脆弱性が、認証なしに車のドアを開ける可能性をもたらすこともあります。これらのリスクは、自動車産業におけるサイバーセキュリティの複雑さと多面性を示しており、ハードウェアとソフトウェアの両方を保護し、潜在的な脅威に対抗する必要があります。

特に自動車産業における外部サイバーセキュリティリスク管理の主な課題は、脆弱性を実行可能で価値のある対策に転換してリスクを軽減することです。近年導入されたいくつかのアプローチには、SBOM や HBOM があります。SBOM はソフトウェアサプライチェーンのリスクを、HBOM はハードウェアサプライチェーンのリスクを管理するために設計されています。SBOM や HBOM に記載されたアイテムに脆弱性が見つかると、迅速な対応と適切な対策が可能になります。しかし、これらのプロセスを実装することは簡単ではありません。理論上は完璧に思える SBOM や HBOM も、現実世界で包括的かつ完全なものを構築するのは大変な作業です。これは、現代車両に存在する多様なコンポーネントや依存関係の広範囲にわたり、ソフトウェアとハードウェアの両方に関連するすべての潜在的リスクを追跡する難しさから生じる複雑さによるものです。

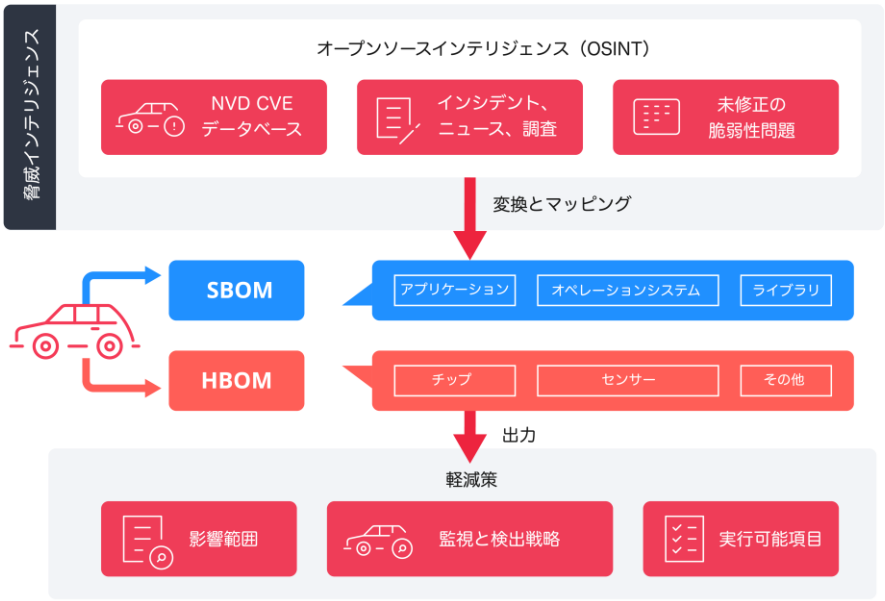


図 11：外部サイバーセキュリティリスクの取り扱いプロセス

既知の脆弱性以外にも、特にベンダーの視点からリスク管理において課題をもたらす、隠れたていたり目立たなかったりする脆弱性が、多くの場合、存在します。これらには、研究論文などで言及される SSL ライブラリの潜在的脆弱性や、タイヤ空気圧監視システム（TPMS）の信号を偽造するツールの使用などが含まれます。このような隠れたリスクを管理すること

は特に困難となります。これらの脆弱性は容易に検出や理解ができないことがあるためです。ベンダーは、これらの脆弱性が悪用されたり、詳細な研究が行われるまで気づかないこともあり、複雑な現代の自動車技術、特にソフトウェアとハードウェアの入り組んだ相互作用は、これらの隠れた脆弱性の特定と対処をより複雑にしています。

インシデント対応

IT業界では、「インシデント対応」（IR）とは、セキュリティ侵害やサイバー攻撃の影響をどのように扱うかを指します。しかし、自動車業界ではこの用語の意味が少し異なります。ここでは、外部のサイバーセキュリティリスクと内部のセキュリティインシデントの両方がどのように同時に対処されるかを示します。例えば、自動車会社がセキュリティ侵害やサイバー攻撃に直面した場合、IT 業界の原則を活用して影響を軽減することができます。ビジネスネットワーク内であっても、公共クラウドサービスであっても、アプローチは同じです。しかし、問題が車両に関係する場合は、異なる対処法が必要になります。

IT 分野では、事態はもっと単純です。例えば、サイバーセキュリティ・インフラストラクチャ・セキュリティ庁（CISA）が警告を発すると、企業や組織はすぐにその助言に基づいて行動を起こすことができます。具体的な対処法が示されていなくても、業界標準のセキュリティ分析ツール YARA、事前定義されたプレイブックガイド、IT 業界で周知された脅威項目分類の MITRE フレームワークなどが対策の伝達と特定を支援しているため、セキュリティベンダーは迅速に対応できます。

一方、自動車業界では状況は異なります。あるブランドの車両に特定の脆弱性が、事例や調査によって明らかになった場合、他の車両メーカーはその発見の意味を把握せず、同じ脆弱性が自社の車両にも影響を及ぼす可能性があるとは気づかないかもしれず、適切にチェックするためのシステムが存在していません。こうした中、彼らは次のような疑問を抱くかもしれません。

役割	質問	アクション
製品セキュリティインシデント対応チーム（PSIRT）	この脆弱性は私たちの車両に影響を与えますか？	影響範囲を把握する必要があります。
車両セキュリティ運用センター（VSOC）	脆弱性が発生しているかどうかをどうやって知ることができますか？	テレメトリが必要で、それを検出する方法を考え出す必要があります。

表 13：インシデント対応における質問

現在の自動車産業では、以下の 2 つの質問に対処することが難しい状況にあります。これは、統一された標準が存在しないためです。また、各状況も車両メーカーによって異なります。SBOM と HBOM を完全にコントロールすることができれば、問題解決は容易になるかもし

れませんが、全ての場合に当てはまるわけではありません。自動車産業には、IT 産業で用いられている技術と同様の手法を取り入れ、これらの問題に迅速に対処し解決する必要があることは明らかです。

自動車データのエコシステム

自動車業界や車両エコシステムには、業界の進展に対応して規制自体を更新する必要がある分野が存在します。その中でも特に顕著なのが、急速に拡大しているものの見過ごされがちな車両データの世界です。トレンドマイクロのリサーチチームが VicOne 向けに執筆したリサーチペーパー「自動車データ：コネクテッドカーのデータ利用、収益化、サイバーセキュリティの脅威」[28] では、このエコシステムがカバーする広大な規模が主要な発見とされています。

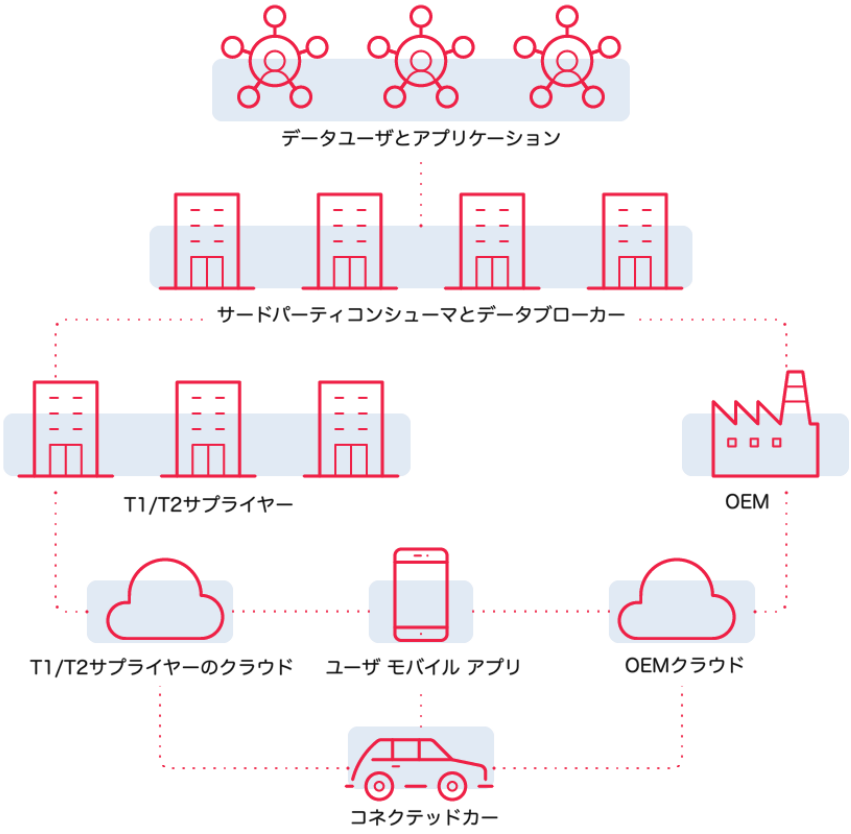


図 12：自動車データのエコシステム

現代の車両がデータを生成し活用していることは一般的に認識されていますが、現在の自動車データエコシステムの深さと複雑さについては、十分な認識がないようです。これは、現在業界が扱っている大量のデータを適切に管理するための規制基準が不足していることにも現れています。

自動車業界でのデータ収益化の進展は収益成長に寄与する可能性がありますが、同時にサイバー犯罪を助長する可能性もあります。このデータの収益化が今後も増加するならば、コネクテッドカーに対する最初の大規模攻撃はデータ関連のものになると予想されます。こうしたデータがサイバー犯罪者の手に渡った場合、それによりもたらされる深刻なリスクは容易に想像できます。自動車業界がサイバーセキュリティ規制にどう取り組んでいるかについては議論されていますが、自動車データのエコシステムは、業界の進展が現在の規制の不備を浮き彫りにしています。車両データの収集と利用に関する法的な不備は解決される必要があります。この成長分野を適切に管理するためには、適切な立法への取り組みが不可欠です。

自動車サイバー犯罪のアンダーグラウンド市場

自動車業界の現在のトレンドがサイバー犯罪活動にどのように影響を及ぼしているかを理解する別の方法は、サイバー犯罪のアンダーグラウンド市場を調査することです。トレンドマイクロのリサーチチームは、VicOne 向けに現在及び将来にわたるコネクテッドカーに対するサイバー犯罪を調査しています[29]。

アンダーグラウンド市場のフォーラムで議論されているコネクテッドカーに関わるサイバー攻撃として最も近い事例は、カーモディファイ（別名：カーモッディング）です。カーモッディングは通常、車両の特徴を解除し、走行距離数を操作するために愛好家たちによって行われます。彼らは車載機能をハックして、例えば車のシートヒーターのような機能を有効にします。これは通常、OEM が有料でアップグレードとして提供する機能です。また、走行距離数を減らすためにソフトウェアを調整することもあります。このような操作は OEM の利益に影響を与えますが、コネクテッドカーの利用者を直接的に標的にしているわけではないため、カーモッディング活動がサイバー攻撃として分類されるべきかどうかは疑問です。

現在、地下フォーラムで広く議論されている攻撃	将来、地下フォーラムで流行する可能性のある攻撃
カー改造（マニュアルカーハッキング）による： • カーシートヒーターのようなプレミアム機能の有効化 • 走行距離の操作	悪意のある者にコネクテッド車両のユーザーアカウントを売却し、以下のことが可能になる： • フィッシング、キーロギング、その他のマルウェアを使用してユーザーになりすます • 遠隔地から車のドアを開けたり、エンジンやモーターを起動する • 車を開け、中の貴重品を盗む • 車にアクセスし、一度限りの犯罪を行う • 車を持ち去り、部品として売る • 車の位置を特定し、車の持ち主の自宅を知り、持ち主が不在であることを突く

表 14：アンダーグラウンド市場のフォーラムで広く議論されている現在の攻撃と、将来流行しそうな攻撃

自動車産業にとっての大きな懸念の 1 つは、OEM への攻撃です。実際、ネットワーク侵害や、ダークウェブ上での仮想プライベートネットワーク（VPN）アクセス販売の事例を確認しています。しかし、フォーラムでの議論は、今のところ、IT 資産を収益化する一般的な方法に限られています。これは、サイバー犯罪者たちがコネクテッドカーのデータの価値をまだ認識していないか、またはそのような情報に対する市場の需要を明確に感じていないことを示唆しています。

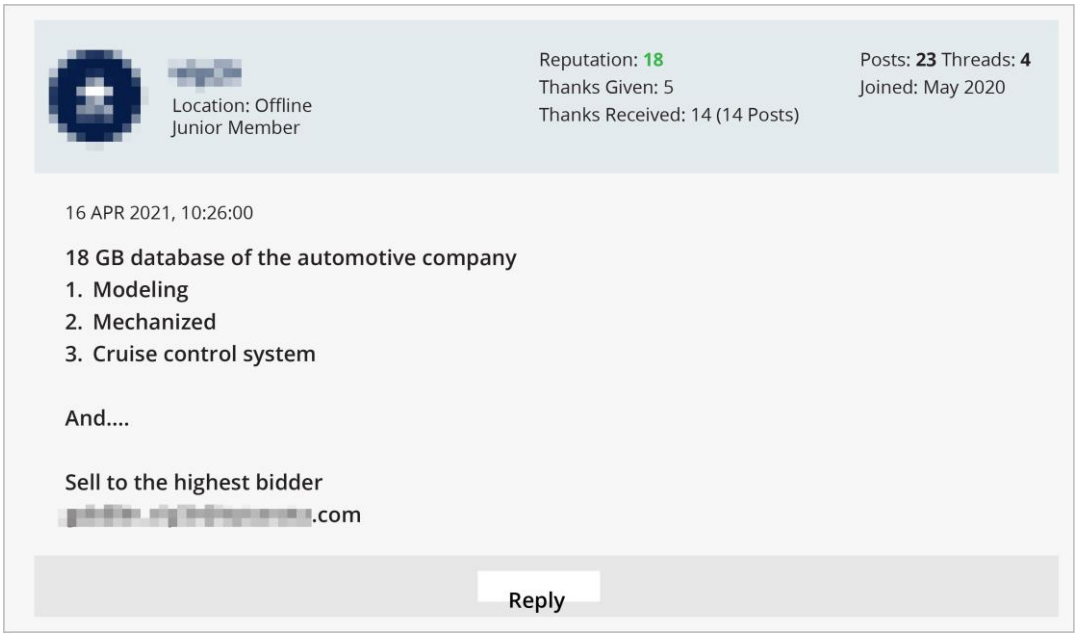


図 13：OEM からのデータダンプを提供するユーザーによるサイバー犯罪アンダーグラウンド市場のフォーラムにおける投稿（元の投稿は削除されたため、再現されたもの）

これらの調査結果から、サイバー犯罪アンダーグラウンドでのコネクテッドカー関連データの市場はまだ初期段階にあることが分かります。しかし、VicOne では、この状況が長く続かないと予測しています。すでに述べた通り、サードパーティの事業者が車両データを広範囲に活用し始めると、コネクテッドカー関連データの価値は大幅に上昇するでしょう。サイバー犯罪者たちは、この状況を迅速に理解し、車両データを窃取する最初の試みがすぐに現れると考えられます。

自動運転車の未来展望：イノベーションと潜在的な懸念のバランスを考える

自動運転車（SDV）の登場は、自動車技術における重要な進歩を示しています。このような時代状況においては、ハードウェアよりもソフトウェアが車両の能力、特徴や運転体験全体が重視されます。この新しい技術は、革新とカスタマイズに大きな可能性をもたらしますが、同時に安全性、サイバーセキュリティ、データプライバシーに関して多くの懸念も引き起こしています。車両がソフトウェアにますます依存し、接続されるにつれて、サイバー脅威や

情報漏えいのリスクが増し、利用者の機密情報の保護や車両システムの完全性についての疑問が浮かび上がっています。

- 高度運転支援システム（ADAS）：これらのシステムは、自動ブレーキ、レーンキープアシスト、アダプティブクルーズコントロールなどの機能を通じて車両の安全性を向上させます。しかし、ソフトウェアとセンサーへの依存が、サイバー攻撃の標的になり、安全機能が危険にさらされる可能性があります。
- 自動運転：自動運転車は、道路の安全性と効率の向上を約束する未来を提示しています。しかし、自動運転システムの複雑さは、ソフトウェアの不具合やハッキングによる脆弱性を生じさせ、乗客の安全とデータセキュリティにリスクをもたらします。
- AI 搭載スマートコックピット：スマートコックピットは AI を使用して運転体験をパーソナライズし、ドライバーの行動や好みに基づいて設定を調整します。これにより快適さと利便性が向上しますが、個人データの収集と取り扱いに関する懸念や、強固なデータ保護措置の必要性が生じます。
- サブスクリプション機能：車両は現在、強化されたナビゲーションやパフォーマンスアップグレードなど、ソフトウェアベースの機能をサブスクリプションベースで提供できます。このビジネスモデルは、車両とメーカー間の連続的なデータ交換を必要とし、安全なデータ伝送プロトコルとより透明なデータ収集の必要性を強調します。
- 使用量ベースの保険（UBI）：UBI は、車両ソフトウェアを介して監視される運転行動に基づいて保険料を調整します。このアプローチは詳細な運転データの収集に大きく依存しており、データのプライバシーとセキュリティが前面に出てきます。なぜなら、このデータの誤用や不正アクセスは重大なプライバシーへの影響を及ぼす可能性があるからです。

このように、自動運転車（SDV）は魅力的な機会を提供する一方で、これらの応用における安全性、サイバーセキュリティ、データプライバシーとの関連において、技術の安全性や倫理的な展開を保証するために、総合的かつ警戒心を持ったアプローチが必要となっています。

結論

本稿では、規制環境を詳しく検討し、ISO/SAE 21434 と UN R155 が非常に重要であることを指摘しました。さらに自動車業界がコンプライアンスを達成する際に直面する様々な課題をまとめました。OEM やサプライヤーがコンプライアンスを実現するためのアプローチは、その規制状況や規制手続きに関する経験によって異なります。しかし、製造プロセス全体を通じて最も重要な原則は「セキュア・バイ・デザイン」です。規制は、問題が壊滅的な状況になる前に、全てのプロセスでセキュリティを保証することを目指しています。

脅威動向を分析した結果、2023 年上半期のサイバー攻撃による損失が 11 億ドルを超え、過去 2 年間と比べて前例のない増加を記録したことが分かりました。詳細に調べると、これらの攻撃は主に自動車関連のサプライヤーを対象としており、この傾向は増加しています。特に注目すべきは、これらの攻撃の 90%以上が OEM 自体ではなく、サプライチェーン内の他の企業を狙っていたことです。攻撃者は保護がしっかりしている企業に侵入するのが難しいため、警戒が緩い企業を狙うことが多い傾向があります。しかし、サプライチェーンが混乱されることにより、OEM も影響を受けます。結果として、サイバー攻撃からシステムを守ることは、個々の企業や組織だけでなく、サプライチェーン全体を強化すべきことを意味します。

本稿で扱ったケーススタディは、事例の特徴を理解した上で、どのような技術的な手法や規制的なアプローチを用いて根本的な問題を解決しているかを明らかにしました。これらの事例は、個々のコンポーネントから統合システムに至るまで、すべてのレベルで検証がいかに重要かを示しています。これは、UN R155 や ISO/SAE 21434 の TARA プロセスを含む規制の推奨が、検証プロセスを実装する最適なワークフローを定義する上で非常に重要である理由も示しています。

自動運転車（SDV）の領域に進出するベンダーにとって、この技術革新は自動車エコシステムを根本的に変革し、車両の使用方法を拡大するでしょう。しかし、こうした進展は、車両の安全性を確保するために、さらなるセキュリティ対策を必要とします。一例として、車両データと拡大する自動車データのエコシステムがあり、自動車業界のこの側面を安全に取り扱うための明確なガイドラインと規制の不足が浮き彫りになりました。新機能の導入は、多くの場合、車両の潜在的なアッタクサーフェスを拡大させてしまいます。特に自動車産業においては、さらなる革新も強固なセキュリティ対策と並行して進めることが求められています。

参照

[1] ISO. (2021). ISO. “ISO/SAE 21434:2021 Road vehicles Cybersecurity engineering.” Accessed on Nov. 17, 2023, at https://www.iso.org/standard/70918.html.

[2] The MITRE Corporation. (April 25, 2009). CWE. “CWE-787: Out-of-bounds Write.” Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/787.html.

[3] The MITRE Corporation. (July 19, 2006). Common Weakness Enumeration. “CWE-416: Use After Free.” Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/416.html.

[4] The MITRE Corporation. (July 19, 2006). Common Weakness Enumeration. “CWE-125: Out-of-bounds Read.” Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/125.html.

[5] The MITRE Corporation. (July 19, 2006). Common Weakness Enumeration. “CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow').” Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/120.html.

[6] The MITRE Corporation. (July 19, 2006). Common Weakness Enumeration. “CWE-20: Improper Input Validation.” Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/20.html.

[7] The MITRE Corporation. (July 19, 2006). Common Weakness Enumeration. “CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').” Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/89.html.

[8] The MITRE Corporation. (July 19, 2006). Common Weakness Enumeration. “CWE-190: Integer Overflow or Wraparound.” Accessed on Nov. 10, 2023, at https://cwe.mitre.org/data/definitions/190.html.

[9] Tavis Ormandy. (July 2023). cmpxchg8b. “Zenbleed.” Accessed on Nov. 10, 2023, at https://lock.cmpxchg8b.com/zenbleed.html.

[10] Masaru Takada, Yuki Osada, and Masakatu Morii. (2019). IEEE Xplore. “Counter Attack Against the Bus-Off Attack on CAN.” Accessed on Nov. 10, 2023, at https://ieeexplore.ieee.org/document/8827010.

[11] Matan Ziv. (June 2022). Cymotive. “CANCAN: Encapsulation of CAN-FD Messages for Circumvention of Security Measures.” Accessed on Nov. 10, 2023, at https://www.cymotive.com/wp-content/uploads/2022/06/CANCAN-Research-paper_-Matan-Ziv-Principal-Cybersecurity-Researcher-1.pdf.

[12] Gedare Bloom. (Jan. 1, 2021). NDSS. “WeepingCAN: A Stealthy CAN Bus-off Attack.” Accessed on Nov. 10, 2023, at https://www.ndss-symposium.org/ndss-paper/auto-draft-102/.

[13] Omar Yang. (May 5, 2023). VicOne. “How to Get Away With Car Theft: Unveiling the Dark Side of the CAN Bus.” Accessed on Nov. 10, 2023, at https://vicone.com/blog/how-to-get-away-with-car-theft-unveiling-the-dark-side-of-the-can-bus.

[14] Ken Tindell. (April 3, 2023). Canis Automotive Labs. “CAN Injection: keyless car theft.” Accessed on Nov. 10, 2023, at https://kentindell.github.io/2023/04/03/can-injection/.

[15] Ken Tindell. (April 3, 2023). Canis Automotive Labs. “CAN Injection: keyless car theft.” Accessed on Nov. 10, 2023, at https://kentindell.github.io/2023/04/03/can-injection/.

[16] KeylessGoRepeater. (May 18, 2022). WayBackMachine. “Unlocker, opener for Toyota-Lexus 2017+.” Accessed on Nov. 10, 2023, at https://web.archive.org/web/20220518024120/https://keylessgorepeater.com/products/unlocker-opener-for-toyota-lexus-2017/ .

[17] KeylessGoRepeater. (May 18, 2022). WayBackMachine. “Unlocker, opener for Toyota-Lexus 2017+.” Accessed on Nov. 10, 2023, at https://web.archive.org/web/20220518024120/https://keylessgorepeater.com/products/unlocker-opener-for-toyota-lexus-2017/.

[18] Shop-Auto-PODOLSK . (n.d.). Shop-Auto-PODOLSK . “AST PRO UNLOCKER for Toyota/Lexus (2017+).” Accessed on Nov. 10, 2023, at https://shop-auto-podolsk.com/ast-pro-unlocker-for-toyotalexus-2017/.

[19] AutoDecoders. (n.d.). AutoDecoders. “AST PRO UNLOCKER for Toyota / Lexus 2017+.” Accessed on Nov. 10, 2023, at https://autodecoders.com/product/ast-pro-unlocker-for-toyota-lexus-2017/.

[20]Agent Grabber. (n.d.). Agent Grabber. “Unlocker, opener for Toyota-Lexus 2015+.” Accessed on Nov. 10, 2023, at https://agentgrabber.com/en/product/unlocer-toyota-lexus-2020/.

[21] Unlocks Cars Grabber. (n.d.). Unlocks Cars Grabber. “AST Unlock PRO: JBL Car Unlocking + Emergency Start for Toyota/Lexus.” Accessed on Nov. 10, 2023, at https://unlockcarsgrabber.com/product/ast-unlock-pro-jbl-car-unlocking-emergency-start-for-toyota-lexus/.

[22] KodGrabber. (n.d.). KodGrabber. “(UST v1.0) Unlocker & Emergency start Toyota Lexus 2022.” Accessed on Nov. 10, 2023, at https://kodgrabber.club/keyprog/ust-v-10.

[23] Numaan Huq, Craig Gibson, Vladimir Kropotov, and Rainer Vosseler. (Feb. 16, 2021). Trend Micro. “Cybersecurity for Connected Cars: Exploring Risks in 5G, Cloud, and Other Connected Technologies.” Accessed on Nov. 10, 2023, at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/in-transit-interconnected-at-risk-cybersecurity-risks-of-connected-cars.

[24] Samwyco. (Jan. 3, 2023). Sam Curry. “Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More.” Accessed on Nov. 10, 2023, at https://samcurry.net/web-hackers-vs-the-auto-industry/.

[25] Jaroslav Lobacevski. (March 21, 2022). GitHub. “Validate all the things: improve your security with input validation!” Accessed on Nov. 10, 2023, at https://github.blog/2022-03-21-validate-all-things-input-validation/.

[26] United Nations. (June 24, 2020). UNECE. “WP.29 - Introduction.” Accessed on Nov. 17, 2023, at https://unece.org/wp29-introduction.

[27] Ben Ben-Aderet. (Feb. 17, 2023). Forbes. “The Five Important Moments In History That Shaped The Modern Cybersecurity Landscape.” Accessed on Nov. 10, 2023, at https://www.forbes.com/sites/forbestechcouncil/2023/02/17/the-5-important-moments-in-history-that-shaped-the-modern-cybersecurity-landscape/.

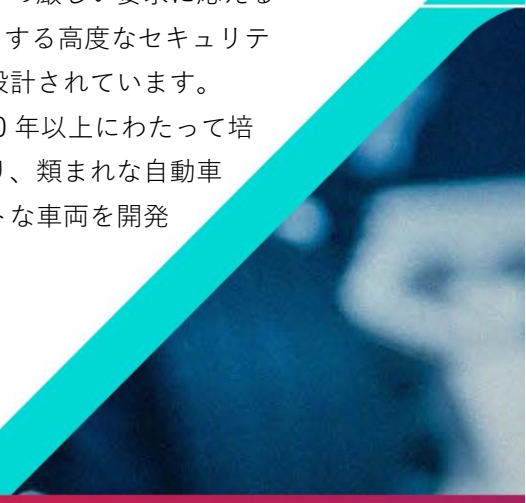
[28] Numaan Huq, Vladimir Kropotov, Philippe Lin, and Rainer Vosseler. (Nov. 15, 2023). VicOne. “Automotive Data: Opportunities, Monetization, and Cybersecurity Threats in the Connected Vehicle Landscape.” Accessed on Nov. 15, 2023, at https://vicone.com/research/the-road-ahead-is-paved-with-risky-data.

[29] Numaan Huq, Vladimir Kropotov, and David Sancho. (May 23, 2023). VicOne. “What Lies in Store for Connected Cars in the Cybercriminal Underground?” Accessed on Nov. 10, 2023, at https://vicone.com/blog/what-lies-in-store-for-connected-cars-in-the-cybercriminal-underground.

VicOne

Driving Automotive Cybersecurity Forward

VicOne は、未来の自動車を守るというビジョンを持ち、自動車産業向けに幅広いサイバーセキュリティソフトウェアやサービスを提供しています。自動車メーカーの厳しい要求に応えるために開発された VicOne の各ソリューションは、現代の車両が必要とする高度なセキュリティニーズにマッチし、セキュリティを確保、スケーリングするように設計されています。VicOne は、トレンドマイクロの子会社であり、トレンドマイクロが 30 年以上にわたって培ってきたサイバーセキュリティ技術をベースにしています。これにより、類まれな自動車の保護と深いセキュリティへの洞察を提供し、お客様が安全でスマートな車両を開発できるよう支援しています。



詳しくは VicOne 公式サイト www.vicone.com/jp をご確認ください。こちらの QR コードからもアクセスできます。

IN COLLABORATION WITH

TREND MICRO™ Trend Research