



自動車サイバーセキュリティの現状



VicOne 2025年 自動車サイバーセキュリティレポート ハイライト

自動車ソフトウェア中心の高度なマシンへと進化するにつれて、**サイバーセキュリティの重要性はかつてないほど高まっています**。新しいコードが行き書かれ、先進的な機能が一つ追加されるたびに、これまでにないサイバーセキュリティリスクが出現し、コネクテッドカーのセキュリティ確保競争は激化しています。

このレポートでは、VicOne がリスクとチャンスに満ちた状況から見てきた主要なトレンドと洞察を検証し、新たなAI セキュリティリスクから将来の課題予測まで

常に変化し続ける
自動車サイバーセキュリティの状況を
映し出します

AI

モビリティに革命を 起こし、 リスクを再定義する

車両へのAI統合は、変革的な機能を実現する一方、
重大なリスクももたらします。

自動車セキュリティにおける AIの主なリスク

車両内のAIシステムは、アクセスとデータの両面で脆弱性を生み出し、サイバー脅威に対する新たな攻撃経路を開く可能性があります。



音声アシスタントシステム： 新たなフロンティア、 新たなリスク

音声アシスタントは、ハンズフリー機能によって車両操作に革命をもたらしました。しかし、音声認識への依存は、プロンプトインジェクション攻撃のような新しい脅威を生み出します。



オンボードAIの展開と 攻撃対象領域の拡大

AIモデルを車載ハードウェアに直接展開することで、重要な機能の低遅延と応答性が保証されます。しかし、チップベースのAIアクセラレータは、車両をハードウェア特有の脆弱性にさらす可能性があります。

SDV

が直面する重要な サイバーセキュリティ課題

車両がよりスマートに、よりコネクテッドになる時代において、SDV（ソフトウェア・デファインド・ビークル）は進化し続ける複雑なサイバーセキュリティ課題に直面しています。過去10年間の脆弱性データは、安全な自動車の未来のために取り組むべき最も重要な領域と脅威を浮き彫りにしています。

83%

最も脆弱な領域

オンボードシステム

ECU（電子制御ユニット）からインフォテインメントシステム、ADAS（先進運転支援システム）に至るまで、オンボードシステムは最も大きく、最も露出している領域です

15%

クラウドインフラ

データ処理と接続性のためにクラウドベースのサービスへの依存度が高まるにつれて、この領域の脆弱性が増加し、車両が大規模な攻撃にさらされる可能性が高まっています。

主要なセキュリティ懸念事項*



1,564件 サプライチェーンの脆弱性

サプライヤーやサードパーティが車両エコシステムに深く組み込まれているため、この複雑なネットワークのすべてのリンクにわたってセキュリティを確保することは、非常に困難な課題です。



308件 サードパーティ連携

車両が外部サービスへの依存度を高めるにつれて、サードパーティ技術の統合により攻撃対象領域が拡大し、予期せぬリスクをもたらしています。



295件 車両ハイジャック

SDVソフトウェアを標的とする 익스プロイト（脆弱性攻撃）は、攻撃者に重要な車両システムの遠隔制御を可能にし、安全性とセキュリティの両方を危険にさらす可能性があります。

*2014年から2024年に公開された
SDV関連の脆弱性合計2,271件に基づく

増加傾向にある 自動車の脆弱性



2024 年だけで、

530 件の自動車関連の脆弱性が特定され、

車両関連のセキュリティリスクが大幅に増加していることを示しています。



特に2019年以降に見られるこの大幅な増加は、現代の自動車システムの複雑化が進んでいることを示しています。車両がよりコネクテッドになり、ソフトウェアへの依存度が高まるにつれて、攻撃対象領域は拡大し続けています。この進化は、ますます高度化するこれらのシステムを悪用から守るための包括的なセキュリティ戦略の緊急の必要性を強調しています。

サイバー攻撃による コストの高騰



2024年の第4四半期におけるサイバー攻撃の急増は、コスト急騰の大きな要因となりました。いくつかの著名な自動車会社が標的となり大規模なデータ侵害が発生したことで、高度なサイバーセキュリティ対策の重要性が浮き彫りになりました。

VicOneは、報告されたサイバー攻撃が自動車業界に与える経済的影響を3つの重点分野に焦点を当てて推定しました。

被害内容



データ漏洩



システム
ダウンタイム



ランサムウェア
被害

2022

2023

2024

\$400万

\$97億

\$200億

\$8億

\$25億

\$19億

\$2.4 億

\$5.2億

\$5.3億

合計被害額

(単位: 米国ドル)

\$10億

\$128億

\$225億

これらの要因は、自動車業界に対するサイバー攻撃の経済的影響がエスカレートしていることを示しています。

EV充電

における課題とリスク

電気自動車 (EV) の普及が急速に進むにつれて、充電インフラの信頼性とセキュリティは、自動車サイバーセキュリティの中心的な課題となっています。EVの利用が拡大するにつれて、そのエコシステムに関連する課題とリスクも増大しています。



主な課題

進化する 充電ニーズと ユーザー行動

EVの普及が進むにつれて、ユーザーは高速で信頼性が高く、安全な充電ソリューションを期待するようになり、新たな要求が生まれています。

複雑な エコシステム

EV 充電ネットワークは、サービスプロバイダー、充電事業者、eローミングプラットフォーム、電力網事業者など相互依存するプレイヤーからなる複雑な網の目構造になっています。

独自の セキュリティ 標準

OCPP (Open Charge Point Protocol) のような広く採用されているプロトコルでさえ、依然として包括的なセキュリティ対策が不足しており、システムが脆弱なままになっています。



脅威は、**不正なポートアクセス**のような基本的な攻撃から、無線周波数を介して**通信を妨害**する高度なエクスプロイトまで多岐にわたります。



現実世界のリスクには、**電力網の不安定化**や充電ステーションを介した**データ盗難**などが含まれます。



研究者たちは、V2G Evilなどのツールを使用してプロトコルの欠陥を発見し、ハッカーが充電システムやより広範な電力網インフラを操作できる方法を実証しています。

アンダーグラウンド からの洞察

VicOneは、ダークウェブやディープウェブ上のアンダーグラウンドフォーラムにおける自動車関連の議論を継続的に監視し、インテリジェンスを収集して新たな脅威を予測しています。これらのフォーラムのスクリーンショットから、攻撃者が現代の車両の脆弱性を悪用するために**常に進化させている戦術**が明らかになります。実際、自動車盗難は施錠された車両に侵入するための従来の機械的なツールを超えて進化しています。



車両の 익스프로イトと脆弱性

익스프로イトは、盗難、破壊工作、または不正な制御を可能にする可能性があります。



ハッキングツールとチュートリアル

これらは攻撃者の参入障壁を下げ、悪用のリスクを高めます。



コネクテッドカーとIoTデバイスの 익스프로イト

IoTデバイスやアプリの脆弱なセキュリティは、車両をリモート攻撃にさらす可能性があります。



企業スパイとインサイダー脅威

インサイダー脅威は、従来のセキュリティ対策を回避します。



漏洩した企業の認証情報とアクセスデータ

不正アクセスは業務を妨害し、機密データを盗む可能性があります。



盗まれた知的財産と機密データ

盗まれたデータ市場は、偽造部品、侵害されたソフトウェア、競争上の優位性の喪失のリスクを高める可能性があります。



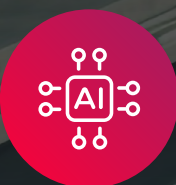
データ侵害

データ侵害は信頼を損ない、規制上の罰則につながる可能性があります。

自動車サイバーセキュリティの 未来

2025年 の主要予測

自動車業界がAI、自動運転、クラウド接続などの技術で進歩するにつれて、サイバーセキュリティの課題はますます緊急かつ複雑になっています。



AIの統合は、不正なコマンド、データ侵害、その他のサイバー攻撃の新たなリスクをもたらします。

AIは車両機能を強化しますが、サードパーティ連携を介したサイバー攻撃の経路も開くことになります。



プラットフォームの標準化は、何百万台もの車両をシステム全体の脆弱性にさらすことになります。

相互接続されたサプライチェーンにより、エコシステム全体で何百万ものデバイスや車両に影響を与える脆弱性に関する事例の発生件数が増える可能性があります。



EV充電インフラが、サイバー脅威のホットスポットとして浮上するでしょう。

EV充電ネットワークは、データ盗難、システムハイジャック、その他サイバー攻撃の標的となり、重大なセキュリティ課題を引き起こす可能性があります。



自動運転車は、センサー操作のリスクに直面するでしょう。

攻撃者が意思決定システムを欺くことで、事故の発生や、交通の流れの妨害、重要なフリートを無効化・迂回させるリスクが懸念されます。



Shifting Gears

VicOne 2025年 自動車サイバーセキュリティレポート

本レポートは、自動車サイバーセキュリティにおける重要なトレンド、詳細な分析、そして専門家による具体的な提言などを深く掘り下げています。変化し続ける自動車業界を取り巻くこの状況を乗り切るためにお役立てください。

レポート本編をダウンロード