VicOne

SDVについてのサイバーセキュリティの現状：イノベーションとリスクへの対応

詳しくはVicOneウェブサイトをご覧ください
(vicone.com/jpまたは右記QRコードをスキャンしてアクセス)

ソフトウェアデファインドビークル（SDV）への移行は、よりコネクテッドでインテリジェントかつ持続可能なモビリティの時代の到来を告げるものです。しかしこの変革は特に、サイバーセキュリティ、ソフトウェアの複雑性、規制コンプライアンスにおいて大きな課題をもたらします。SDV は、OTA（Over-the-Air）アップデート、クラウド接続、高度な車載 / 車両内システムに依存しているため、安全性、プライバシー、回復力を確保しながらリスクを管理するための強固なフレームワークが必要です。
SDV の可能性を最大限に引き出すには、自動車業界が積極的な戦略と革新的なソリューションを採用する必要があります。そのためには、自動車メーカー、サプライヤー、テクノロジープロバイダーが緊密に協力し、信頼を育み、セキュリティを優先し、イノベーションへのコミットメントを維持する必要があります。最終的に、SDV は単なる技術的進化ではなく、モビリティにおける根本的なパラダイムシフトを意味します。

SDV のサイバーセキュリティに対する重大な脅威

サイバーセキュリティリスクは、SDV が直面する最も重大な課題の一つです。ソフトウェアとコネクティビティへの依存を考えれば、これは驚くべきことではありません。これらのリスクは、統合されたシステム、外部通信チャネル、およびクラウドインフラストラクチャへの依存によって形成される攻撃対象の拡大から生じます。以下では、SDV が直面する主なサイバーセキュリティの脅威についてまとめています。

車両制御と安全性の危殆

システムが侵害されると、ブレーキ、ステアリング、加速などの重要な安全機能に直接影響し、乗客や一般道路利用者は重大な危険にさらされることになります。

- **車両のハイジャック:** 攻撃者によって SDV ソフトウェアの脆弱性が悪用されると、ステアリング、ブレーキ、加速などの重要な車両機能を遠隔操作される可能性があります。そうなった場合、乗客の安全や公道のセキュリティに対する直接的なリスクとなります。電子制御ユニット（ECU）や通信チャネルが侵害されると、システムが完全に乗っ取られる可能性があることが実証されており、このリスクの深刻さが改めて認識されました。

- **サービス妨害（DoS）攻撃：**DoS 攻撃は、車両システムを混乱させ、機能を停止させたり、重大な障害を引き起こす可能性があります。例えば、悪意を持った攻撃者が通信システムを妨害した場合、車両は重要なアップデートやリアルタイムのナビゲーション・データを受信できなくなることが想定されます。

- **仮想化のリスク：** SDV は仮想化を活用して、インフォテインメント、先進運転支援システム（ADAS）、自律走行など専門で受け持つ機能をソフトウェアにより構成された仮想マシン上で分散して処理し、共有ハードウェア上で統合します。しかし隔離対策に失敗した場合、1 つの仮想マシンで侵害が発生すると、他の機能処理にも重要な影響を及ぼす可能性があります。

- **ネットワークのリスク：**従来の CAN（Controller Area Network）バスシステムは、認証や暗号化ができないため、本質的に脆弱です。高帯域幅のイーサネット・ネットワークへの移行は改善をもたらしますが、新たなリスクをもたらします。MACsec や IPsec のような機能が実装されていない場合、攻撃者はセキュリティが不十分で攻撃に手慣れたイーサネットベースのアーキテクチャを悪用する可能性があります。

- **自律走行特有のリスク：**自律走行型 SDV は、センサーデータや機械学習モデルの操作に対して特に脆弱です。カメラ、ライダー、その他のセンサーへの不正な入力は、走行状況や周囲環境の誤認識につながり、自律走行システムを誤動作させる危険性があります。

ソフトウェアとアップデートの悪用

OTA アップデートとサードパーティソフトウェアへの依存は、SDV の完全性とセキュリティを維持する上で大きな課題となります。

- **OTA アップデートの悪用：**OTA アップデートは SDV にとって不可欠ですが、安全でないメカニズムがリスクをもたらす可能性があります。たとえば、攻撃者が悪意のあるアップデートを配信したり、機能を無効にしたり、バックドアを挿入したりして、車両の機能やユーザーデータを危険にさらす可能性があります。

- **サプライチェーンの脆弱性:**サードパーティのソフトウェアやハードウェアは、製造段階でセキュリティリスクを導入してしまう可能性があります。攻撃者は、パッチが適用されていない脆弱性を悪用して、複数の車種で使用されているコンポーネントに悪意のあるコードを挿入する可能性があります。

- **レガシーシステムのリスク：**車両は何十年にもわたって稼働し続ける可能性があるため、旧式のシステムの安全確保が課題となります。アップデートを受けなくなったレガシーシステムは、新たな脅威に対して特に脆弱です。

データ漏洩とプライバシー侵害

SDV は膨大な量のデータを生成・処理するため、サイバー攻撃の格好の標的となっています。このデータを保護することは、ユーザーのプライバシーを確保し、信頼を維持するために不可欠です。

- **クラウドとバックエンドの脆弱性：**SDV は、データの処理、機能の展開、リアルタイム分析の実施において、クラウドプラットフォームに大きく依存しています。クラウドインフラストラクチャが侵害されると、攻撃者は複数の車両に同時にアクセスできるようになり、車両を標的とした大規模な攻撃やランサムウェアが可能になります。ナビゲーションのルートや OTA アップデートの設定など、操作されたデータは、自律走行システムを誤誘導したり、重要なアップデートを遅らせたり、誤報を誘発したりする可能性があり、安全上の懸念や運用の混乱につながります。

- **データ盗難とプライバシー侵害：**SDV は、位置情報の履歴、運転パターン、生体認証、個人的な好みなど、膨大な顧客データを生成し、保存します。車両や関連するクラウドプラットフォームへのサイバー攻撃は、データの盗難、、個人情報・機密情報の悪用につながる可能性があります。

- **サードパーティとの統合リスク：**SDV は多くの場面で、スマートホーム、充電ネットワーク、車両管理プラットフォームなど、サードパーティのアプリケーションや外部システムと統合されることがよくあります。サードパーティ製の API（アプリケーション•プログラム•インターフェース）やシステムの脆弱性は、攻撃者が車両を侵害したり、データを盗んだり、業務を妨害したりするための侵入口となる可能性があります。

財務および経営の混乱

SDV へのサイバー攻撃による財務上および業務上の打撃は相当なものです。ランサムウェアから特定運行業務（フリート）の攻撃に至るまで、これらのインシデントはビジネスを混乱させ、ユーザーの信頼を損ないます。

- **ランサムウェアと恐喝：**SDV を標的としたランサムウェア攻撃は、身代金が支払われるまでユーザーを車両から締め出したり、重要なシステムを無効にしたりする可能性があります。特定運行業務への攻撃は、ロジスティクス、ライドシェアリングサービス、その他のオペレーションを混乱させる可能性があります。
- **フリート特有の攻撃：**車両管理システムは特に魅力的な標的です。攻撃者は、経路を操作したり、車両を使用不能にしたり、機密性の高い業務データにアクセスしたりして、業務の遅延や経済的損失を引き起こす可能性があります。

一般的な SDV のサイバーセキュリティ脅威

表 1 では、2014 年から 2024 年までの 10 年間に公表された関連する脆弱性の数に基づく SDV のサイバーセキュリティ脅威の上位を紹介しています。

脅威	カテゴリー	カウント
サプライチェーンの脆弱性	ソフトウェアとアップデートの搾取	1,564
サードパーティの統合リスク	データ漏洩とプライバシー侵害	308
車両のハイジャック	車両制御と安全性の危殆	295
特定運行業務への攻撃	財務および経営上の混乱	44
クラウドとバックエンドの脆弱性	データ漏洩とプライバシー侵害	30
ネットワークリスク	車両制御と安全性の危殆	27
仮想化リスク	車両制御と安全性の危殆	3

表 1. 2014 年から 2024 年までに報告された脆弱性の数に基づく SDV のサイバーセキュリティ脅威上位

従来の IT サイバー攻撃や公表されている脆弱性の数から推測できるように、自動車サプライチェーンは多数のサプライヤーに依存しているため、依然として格好の標的であり、堅牢で包括的なサイバーセキュリティ確保することが永遠の課題となっています。自動車関連の脆弱性に関する VicOne の分析ではこのような問題が浮き彫りになっており**サプライチェーンの脆弱性**は 1,564 件と脅威のトップにランクされています。

これは、サプライヤーやサードパーティが相互に接続されたネットワークを保護することの複雑さを露呈しています。

サードパーティの統合リスクは 308 件で、2 番目に多い脅威となっています。これは、充電ネットワーク、スマートホーム連携、車両管理プラットフォームなど、外部エコシステムへの依存度が高まっていることが主な原因です。これらの API やシステム内の弱点は攻撃者の侵入口となり、車両を侵害したり、データを盗んだり、業務を妨害したりする可能性があります。電気自動車（EV）の急速な普及により、これらのリスクは拡大し、充電ネットワークの脆弱性により、その対策が急務となっています。

車両のハイジャックは車両の制御と安全性に影響を与える重大な懸念事項で、295 件の脆弱性が文書化されています。攻撃者は SDV ソフトウェアの脆弱性を悪用して、ステアリング、ブレーキ、加速などの重要な車両機能をリモートですることができ、乗客の安全や公道のセキュリティに対する直接的な脅威となります。侵害された ECU や通信チャネルがシステムの完全な乗っ取りにつながるインシデントのデモンストレーションは、この脅威の深刻さを示しています。

これらのリスクだけでなく、広帯域イーサネットなどの高度なネットワーキングアーキテクチャへの移行は、さらなる課題をもたらします。例えば、MACsec や IPsec などの認証メカニズムの実装を怠ると、ネットワークシステムに侵入されやすくなります。車両イーサネットへの侵入を足掛かりに攻撃者がセンサーデータや機械学習モデルを操作し、そのデータの歪みによって自律走行車が周囲の状況を誤って判断する可能性があります。

SDV サイバーセキュリティの解読：脅威に対する 4 つの領域からのアプローチ

SDV のセキュリティリスクをよりよく理解するために、SDV を 4 つの重要なドメインに分類しました。これらのドメインは、SDV が直面する独自のサイバーセキュリティ上の課題に対処するためのフレームワークを提供します：

- **オンボード（車載 / 車両内ソフトウェアおよびハードウェア・アーキテクチャ）：**ECU、IVI（車載インフォテインメントシステム）、ADAS テクノロジーなど、車載 / 車両内のすべてのシステムとコンポーネントを指します。
- **オフボード（車両外のサポートとツール）：**SDV のエコシステムを開発・維持するために使用される、車外ツールやシステムを指します。
- **クラウド（クラウド駆動型車両サービス）：**リアルタイム分析、OTA アップデート、リモート管理機能など、車両をサポートするクラウドベースのインフラとサービスが含まれます。
- **開発（開発ツールとプロセス）：**SDV ソフトウェアを構築・維持する際の、開発ツール、ワークフロー、方法論など、開発基盤を指します。

図 1 に示すように、年別およびドメイン別の脆弱性の内訳は、SDV におけるセキュリティリスクに関する重要な傾向の変遷を示しています。このデータを調査することで、トレンドを特定し、重点分野を特定し、ドメイン全体にわたって変化する脅威の状況をよりよく理解することができます。

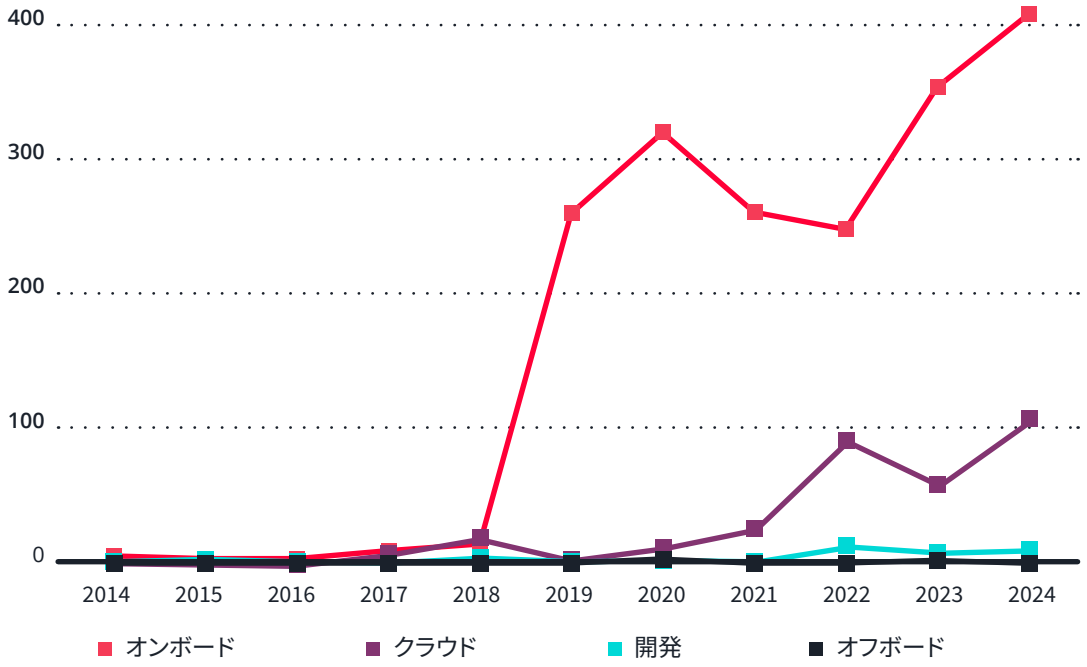

図 1.2014 年から 2024 年までに公表された SDV ドメインごとの脆弱性の比較

ECU、通信ネットワーク、オペレーティングシステム（OS）プラットフォームなど、車載システムの複雑化に伴い、過去 10 年間に公表された脆弱性のほとんど（83%）がオンボードドメインに集中しています。このことは、OTA アップデートや内部通信プロトコルなど、重要な車両機能に対するセキュリティの確保が急務である事を浮き彫りにしています。

クラウドドメインでは近年、リアルタイムデータ処理、機能展開、EV 充電ネットワークなど、クラウドベースのサービスへの依存度が高まっていることを反映して、脆弱性が大幅に増加しています。この傾向は、クラウドインフラと信頼性の高い V2C（ビークル・トゥ・クラウド）通信を保護することの重要性を強調しています。

開発ドメインは、全体的な脆弱性の割合としては小さいものの、この領域におけるリスクは特に懸念すべきものです。開発プロセスやツールの欠陥は SDV エコシステム全体に広がる可能性があり、安全なコーディングの実践と強固なサプライチェーンセキュリティの必要性が強調されています。

最後に、報告された脆弱性の数が最も少ない**オフボードドメイン**は、比較的安全なままですが、それでも診断ツールやキャリブレーションインターフェースの保護には依然として注意が必要です。

このような傾向を踏まえ、VicOne のゼロデイ脆弱性の分析では、特定のシステムおよびデバイスレベルの脅威について、より深い洞察を得ることができます。

表 2 では、各脆弱性に関連する脆弱なシステムまたはデバイス、脅威、SDV ドメインを示します。注目すべきは、1 つを除くすべてがオンボード領域で安全制御、通信プロトコル、ヘッドユニットなどの重要なシステムが特に脆弱であることです。サードパーティ統合の脆弱性や車載／車両内ハイジャックなどのリスクは、これらのシステムを効果的に保護するために、サードパーティコンポーネントの厳格なテストと安全な統合が必要であることを強調しています。

脆弱なシステム/デバイス	脅威カテゴリー	SDVドメイン
安全制御システム	サードパーティの統合リスク	オンボード
自動車用ブートシステム	サプライチェーンの脆弱性	オンボード
ドングル	サードパーティの統合リスク	オンボード
USBインターフェース付きドングル	サードパーティの統合リスク	オンボード
Wi-Fiインターフェース付きドングル	サードパーティの統合リスク	オンボード
通信プロトコル	サードパーティの統合リスク	オンボード
ヘッドユニット	車両のハイジャック	オンボード
自動車用CPU	サプライチェーンの脆弱性	オフボード
自律システム	サプライチェーンの脆弱性	オフボード

表 2.2024 年に VicOne が発見した 9 件のゼロデイ脆弱性の概要
（各脆弱性に関連する脆弱なシステムまたはデバイス、脅威、SDV ドメインを示す）。

全体として、SDV の複雑化とコネクテッド化は、4 つの領域すべてにわたるセキュリティへの総合的なアプローチを求めており、本レポートは、さらなる注意が必要な領域や新たなリスクを軽減するための積極的な対策に関する指針として役立ちます。

SDV の将来性：今年の予測

過去 10 年間のデータと VicOne の 2024 年サイバーセキュリティ脅威分析からの考察に基づき 2025 年に予想される主要なサイバーセキュリティ事象を概説し、SDV の将来について以下の予測を提示します。

サプライチェーンの時限爆弾：SDV を麻痺させる隠れた脆弱性

サプライチェーンの脆弱性は、過去 10 年間で最も重大な脅威として特定され、1,564 件の弱点が文書化され、そのうち 279 件は 2024 年に公表されました。過去の事件から、ECU などの重要なコンポーネントの脆弱性が車両の安全性を完全に損なう可能性があることが示されており、SDV のセキュリティにおけるサプライチェーンの極めて重要な役割が浮き彫りになっています。

2025 年脅威予測

サプライチェーン攻撃は、SDV に統合されたサードパーティのハードウェアおよびソフトウェアコンポーネントの脆弱性をサイバー犯罪者が巧みに悪用することで、今後も増加し続けるでしょう。

- 攻撃者は、サードパーティコンポーネントのパッチ未適用の脆弱性を利用して、大規模なデータ侵害を企てるでしょう。
- 製造時に埋め込まれた悪意のあるコードは、将来的なリモートからの悪用を可能にするバックドアとして機能することになります。

OTA アップデートで壊れる車両

OTA アップデートは SDV にとって不可欠ですが、適切に保護されなければ、依然として重要な攻撃ベクトルであり続けます。過去の傾向から、不正または悪意のあるアップデートは車両の機能を停止させ、ユーザーの安全を脅かす可能性があります。

2025 年脅威予測

OTA メカニズムに脆弱性があると、攻撃者は悪意のあるソフトウェアアップデートを配信したり、重要なアップデートプロセスを妨害したりすることが可能になります。

- 不正な OTA アップデートは、マルウェアを導入し、車載 / 車両内を操作不能にします。
- 攻撃者は、悪意のあるアップデートを使用して重要な安全機能を無効にし、ユーザーの安全性に重大なリスクをもたらします。

包囲されるクラウド：狙われる SDV バックエンドシステム

過去 10 年間で、クラウドインフラストラクチャに関連する脆弱性の文書化された事例が 30 件確認されており、そのうち 2024 年には 2 件が確認されています。

クラウドへのセキュリティ侵害により車両サービスが中断され、機密データが流出し、V2C（ビークル・トゥ・クラウド）通信が妨害される事象が想定されます。

2025 年脅威予測

SDV がリアルタイムのデータ処理とソフトウェア展開のためにクラウドプラットフォームへの依存を強めているため、クラウドベースのシステムはサイバー攻撃の格好の標的になるでしょう。

- 攻撃者はバックエンドのクラウドプラットフォームをコントロールし、複数の車両に同時に影響を与えます。
- クラウドシステムからのデータ漏洩は、機密性の高いユーザーデータを大規模に暴露することになります。

サードパーティ製アプリがサイバー脅威への扉を開けてしまう

過去 10 年間に文書化された 308 件の脆弱性のうち 103 件が昨年発表されたばかりであるため、サードパーティ統合リスクは 2024 年に 2 番目に重大な脅威としてランク付けされました。サードパーティシステムを介した侵害は、車両管理業務を中断させ、より厳格な統合プロトコルの必要性を強調しています。

2025 年脅威予測

スマートホームの統合や充電ネットワークなど、サードパーティのアプリケーションへの依存は、今後も重大なサイバーセキュリティリスクをもたらすでしょう。

- サードパーティの API に脆弱性があると、攻撃者が車両システムに不正アクセスできるようになります。
- 外部アプリケーションが侵害されると、ユーザーの財務情報や個人情報が漏えいします。

自動運転への攻撃：自動運転の未来を左右する

VicOne の 2024 年分析と過去のデータで強調されているように、自律システムは依然としてセンサーデータの改ざんに対して非常に脆弱です。攻撃者はセンサー入力を歪める能力を実証しており、自動運転の意思決定プロセスにおける重大な判断ミスにつながっています。

2025 年脅威予測

攻撃者はカメラ、ライダー、その他の自律走行センサーからのデータを改ざんし、車両の意思決定プロセスを欺くでしょう。

- 偽造された道路標識や操作されたセンサー入力によって、車両は誤った方向に誘導されます。
- 悪意のある行為者はセンサーデータを改ざんし、システムの重大な誤動作を引き起こします。

自動車にもランサムウェアの脅威が及ぶ：支払うか、締め出されるか

過去の事例から、ランサムウェアが個人所有の車や車両管理システムの両方に対して強力な脅威をもたらすことが明らかになっています。相互接続されたシステムに依存する集中型の車両運行管理は、特に大規模なランサムウェア攻撃に対して脆弱です。

2025 年脅威予測

SDV とバックエンド管理システムを標的としたランサムウェア攻撃は、頻度と巧妙さの両方で増加するでしょう。

- 攻撃者は車両や重要なシステムをロックし、その復旧のために身代金を要求します。
- 商用サービスを狙ったフリートワイドのランサムウェア攻撃は物流とライドシェアサービスを混乱させるでしょう。

ネットワークの乗っ取り：車載イーサネットシステムのサイレント妨害工作

過去 10 年間で、車載ネットワークプロトコルに関連する 27 件の脆弱性が記録されており、その多くは高帯域幅のイーサネットアーキテクチャに起因しています。SDV にイーサネットベースの通信が採用されるようになったことで、特に MACsec や IPsec などの暗号化プロトコルの実装が不十分であることによる新たなリスクが生じています。

2025 年脅威予測

SDV がイーサネットベースのアーキテクチャに移行するにつれ、暗号化プロトコルの実装が不十分な場合、システムは不正利用の危険にさらされることになります。

- 攻撃者は中間者（MITM）攻撃を行い、通信データの傍受や操作を行います。
- ネットワークへの侵入により、車両の重要な制御機能が遮断され停止する危険性があります。

SDV の未来を守る

自動車業界における複雑化、コネクテッド化、先端技術への依存の高まりを反映して、SDV のサイバーセキュリティ環境は急速に進化しています。本レポートで詳述したように、サプライチェーン、サードパーティの統合、クラウドシステム、および自律的な運用における脆弱性は、メーカー、サプライヤー、および開発者が対処しなければならない多様かつ重大なリスクを示しています。SDV のセキュリティには、堅牢な暗号化、安全な OTA 機構、より厳格な統合プロトコルに焦点を当てた包括的なアプローチが不可欠です。これらの課題を積極的に管理することによってのみ、自動車業界は潜在的な混乱から保護し、ユーザーの信頼を維持することができます。

VicOne の 2025 年予測では、技術革新、協力、警戒を通じてこれらの脆弱性に対処することの緊急性を強調しています。広帯域イーサネットシステムの安全確保からランサムウェアやセンサー操作のリスク軽減に至るまで、関係者間の協調的な取り組みが不可欠です。本レポートは、SDV の強靭で安全な未来を構築するために重要な分野を特定し、必要な協力関係を促進するためのガイドとなります。

SDVについてのサイバーセキュリティの現状：
イノベーションとリスクへの対応 2025.1

詳しくはVicOneウェブサイトをご覧ください
(vicone.com/jpまたは右記QRコードをスキャンしてアクセス)