



自動車業界における ソフトウェアデファインドビークル SDVのAPIセキュリティ リスクに対する課題



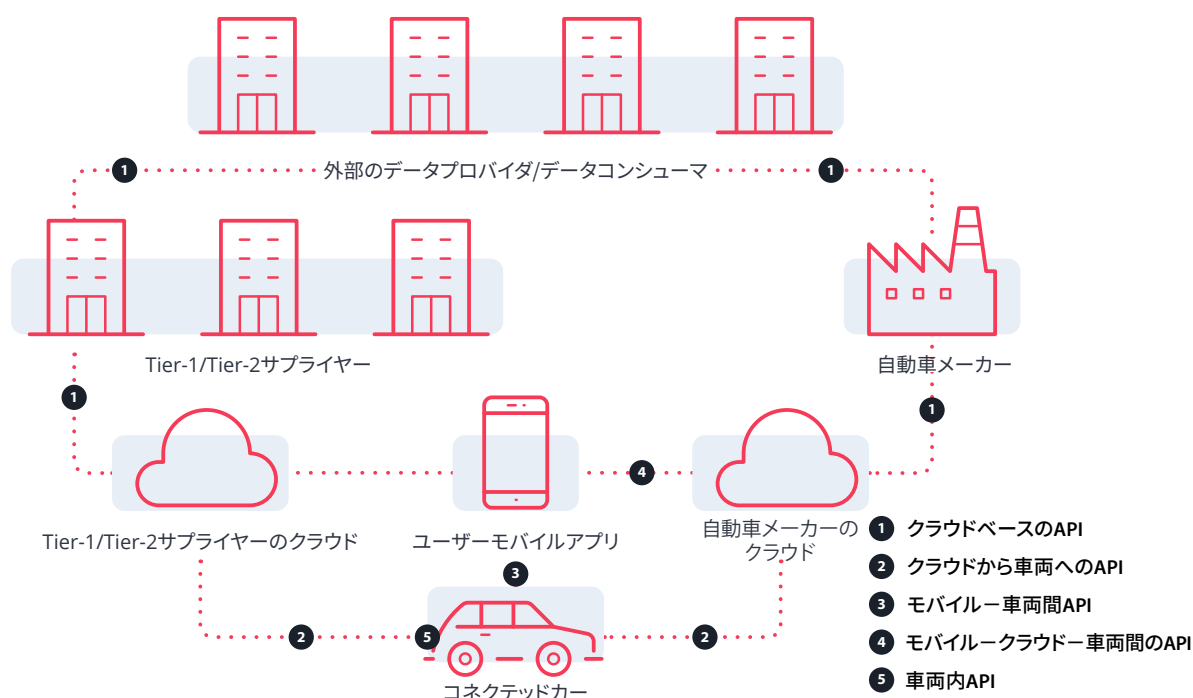
詳しくはVicOneウェブサイトをご覧ください。

(vicone.com/jpまたは右のQRコードをスキャンしてアクセス)



今日の自動車エコシステムにおいて、アプリケーション プログラミング インターフェース (API) は広く普及し、且つ不可欠なものになっています。自動車内部で多様なシステムと連携するAPIは、さまざまな用途に広く適用されています。これには、遠隔操作による車両の起動、緊急アシスタンスサービスのためのサードパーティサービスプロバイダーとの接続、そして自動車エネルギーの管理など、多くのアプリケーションが含まれます。また、自動車メーカー (OEM)とサプライヤー間のサービスクラウドも、APIを活用することでクラウドネイティブ技術を実現するソフトウェア定義ドビークル(SDV)の迅速なアップデートを実現しています。

APIはクラウドベースのAPI、クラウドから車両へのAPI、モバイルから車両へのAPI、モバイルークラウドー車両間のAPI、車載APIなど、今日の自動車エコシステム全体に広範囲で利用されています。これらの多様なAPIは、様々なシステムを繋ぎ合わせることで、自動車産業全体をよりスムーズかつ効率的に動かす極めて重要な役割を果たしています。



自動車を標的としたAPI攻撃の現況

VicOne 2023年 自動車サーバーセキュリティ脅威動向の調査結果によると、APIは数多くのメリットをもたらす反面、2022年下半年から2023年上半年にかけて、アプリケーションとAPIに関連するインシデントは、自動車のサイバー攻撃とセキュリティインシデントの12%を占めました。

当社の自動車脅威インテリジェンスデータベースによると、2020年から2022年にかけてAPI攻撃は単一のコンポーネントを標的とする攻撃から、より広範囲なエコシステム全体を対象とした包括的な攻撃へと進化しました。この変化は、自動車エコシステム全体のセキュリティに対する新たな課題を浮き彫りにし、個々のAPIの保護だけでは不十分であることを示唆しています。

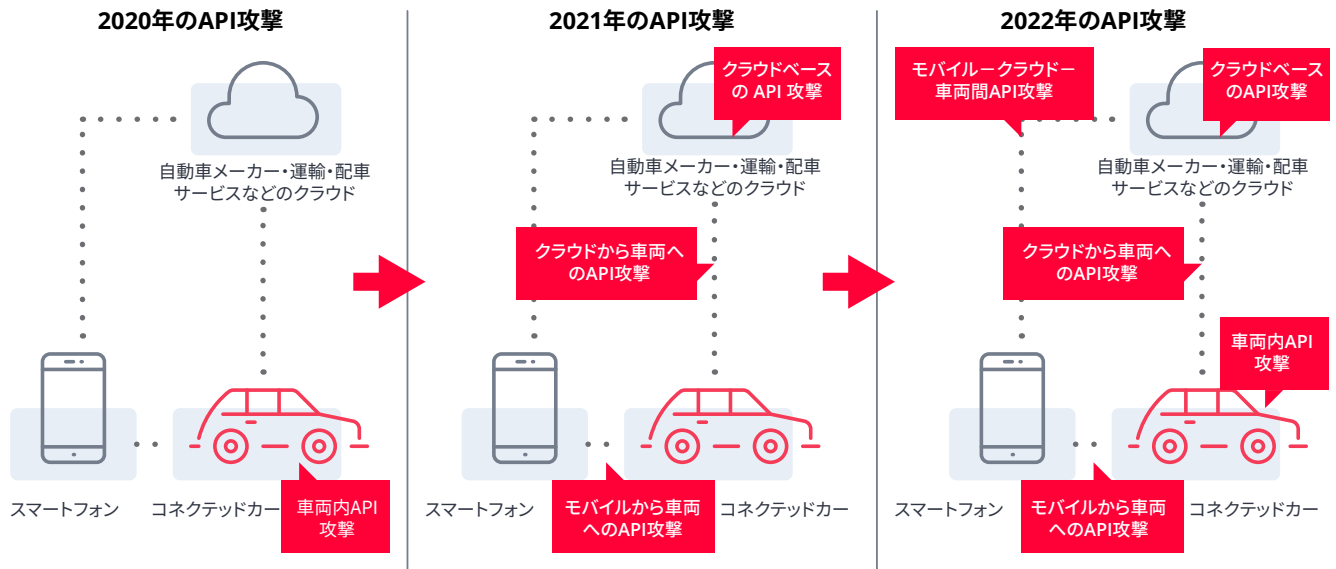


図2. 単一の標的から複数の標的へと進化するAPI攻撃

また、当社の自動車脅威インテリジェンスデータベースによると、2016年から2023年までの自動車業界におけるAPI攻撃は、主にクラウドから車両へのAPI攻撃（35%）とクラウドベースAPI攻撃（30%）が多く、次いでモバイルから車両へのAPI攻撃および車内API攻撃が続き、それぞれ13%を占めています。

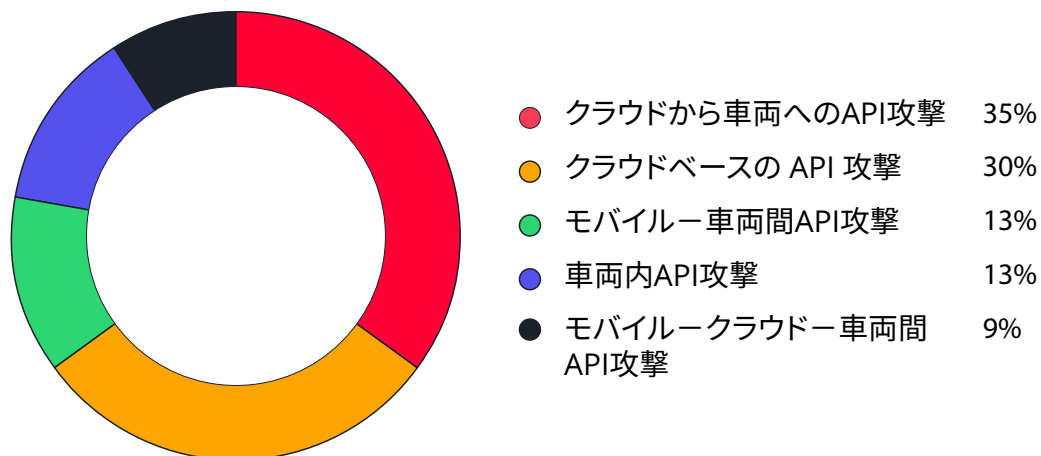


図3. 2016年から2023年までのAPI攻撃カテゴリの傾向

これらの分析結果から、以下の3つの結論を導き出すことができます：

- ・ クラウドから車両へのAPI攻撃が最も一般的な攻撃手法である
- ・ WebAPIの保護は不可欠だが、それだけでは自動車セキュリティの確保には不十分
- ・ モバイルデバイスの保護は自動車セキュリティをさらに強化する重要な要素となる

注意すべきは、SDVはその本質からAPIへの依存度が非常に高いという点です。このため、今後も攻撃対象が拡大しSOTA(Software Over-the-Air) テクノロジーによる頻繁なアップデートに起因するリスクが生まれます。攻撃者がOTAサーバーに侵入し正当なSOTAアップデートに見せかけ、不正なAPIを介して悪意のあるソフトウェアを車両に送り込む事も可能です。これまでOTAアップデートは四半期ごとに行われ攻撃チャンスは年に4-5回しかありませんでしたが、今後年間12-14回へと大幅に増加する可能性がありリスクも高まります。OTAアップデート頻度の増加は、攻撃者に多くの機会を提供し、攻撃の成功確率を大幅に高めてしまいます。これらのことから、自動車 API セキュリティがこれまで以上に重要となっていると言えるでしょう。

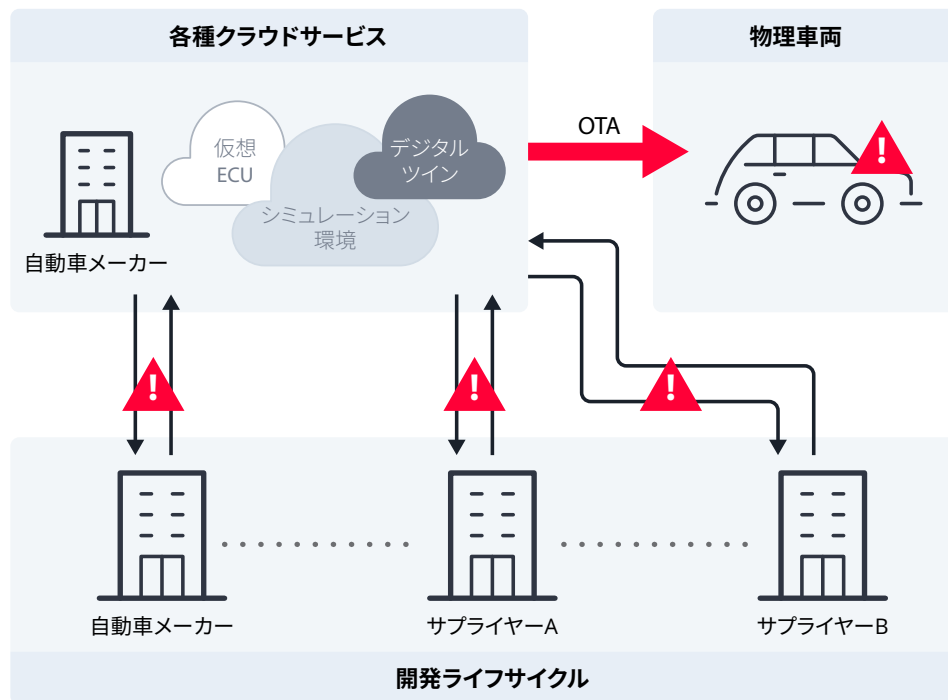


図4. SDVエコシステムにおけるリスク

自動車メーカーや運輸、配車サービス管理者にとってのリスク

そこで、過去3年間に報告されたAPI関連のセキュリティインシデントをいくつか検証し、自動車APIのセキュリティリスクについて理解を深めたいと思います。

車両の遠隔ハイジャック：地球の裏側からのAPI攻撃

[VicOne自動車セキュリティ研究者の調査](#)によると、攻撃者は漏洩したアカウント認証情報を悪用して、地球の裏側にある車両であってもリモート攻撃を実行することができると言われています。この認証情報を使って攻撃者は車両のAPIにアクセスし、車両のドアの状態を取得したり、リモートで車両を始動させたりと遠隔操作でさまざまなコマンドを実行できるようになります。攻撃者はフィッシングやサイバー攻撃によって不正に認証情報を入手することができます。残念ながら、このような認証情報には車両フリートに関する高い金銭的価値とプライバシーリスクがあるにもかかわらず、一般資産と同様に管理されているケースが少なくありません。

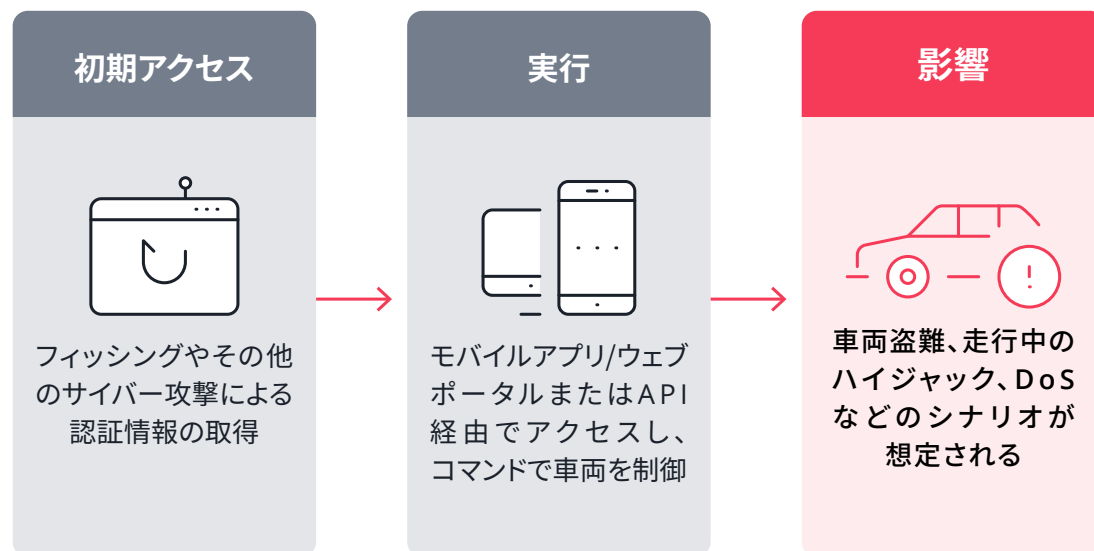


図5. APIアクセスによるリモートカーハイジャックの攻撃経路

遠隔からの完全乗っ取り：侵害された自動車クラウドサービスAPI

2023年1月に公開されたブログ記事で、ウェブアプリケーションのセキュリティ研究者であるSam Curry氏と彼のチームは、テレマティクスシステムとAPIの脆弱性を悪用してさまざまな自動車メーカーのバックエンドのクラウドインフラストラクチャにアクセスする方法をデモンストレーションしました。彼らは一般にアクセス可能な自動車修理工場のウェブサイトからある有名自動車ブランドの従業員用LDAP (Lightweight Directory Access Protocol) データベースに書き込みができることを発見しました。このウェブサイトに登録することで、従業員用アプリケーションへの限定的なアクセス権を取得し、それを利用して、このメーカーが利用しているGitHubを含む機密性の高い社内アプリケーションへのアクセス権をも取得することに成功しました。

その結果、影響を受けるクラウドサービスのウェブサイトで発生する共通脆弱性タイプ一覧 (CWE) のリストが作成されると同時に、このようなセキュリティ対策に対する自動車業界の意識の欠如が明らかになりました。クラウド環境における主な問題点として、認証および権限管理の不備と、入力パラメータに対する適切なサニタイズ処理の不備が挙げられます。前者は事前認証の脆弱性や個人を特定できる情報 (PII) への不正アクセスにつながるといったリスクを孕み、後者はインジェクション攻撃に脆弱性を曝す可能性があります。

これらの調査結果は、自動車業界がIT業界と同等のセキュリティ課題に直面しているにもかかわらず、それらに効果的に対処するための十分な対策が講じられていないことを浮き彫りにしています。例えば、適切な入力検証とサニタイズ処理は、**セキュリティリスクの緩和**において極めて重要ですが、コーディングスタイルガイドやCI/CD (継続的インテグレーションと継続的デリバリー) 環境が整備されていなければ、依然として適切な対策としては不十分です。

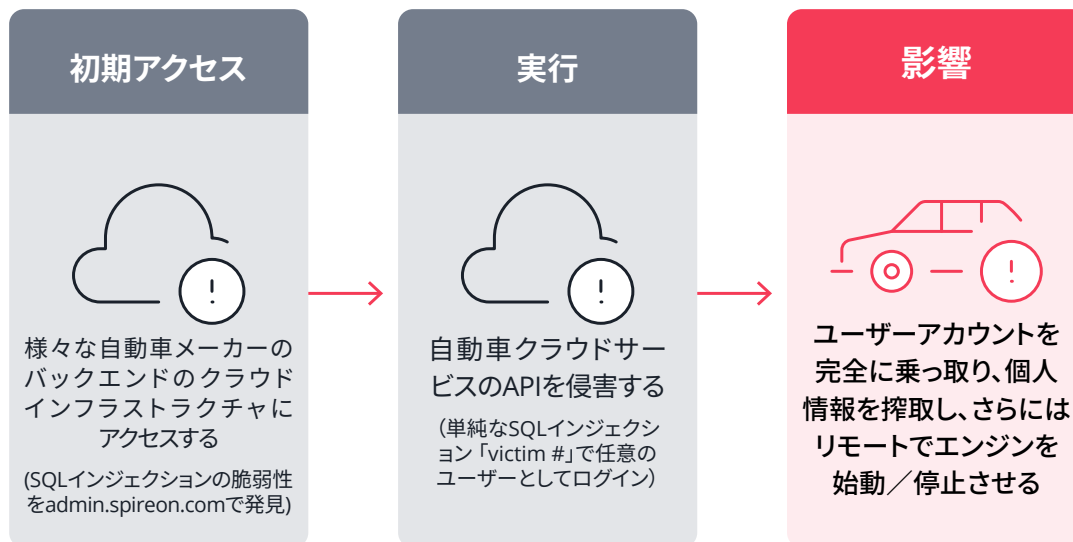


図6. 侵害された車両クラウドサービスAPIを介した車両のリモート完全乗っ取り攻撃経路

遠隔からの完全乗っ取り：タクシーアプリAPIの悪用

2022年9月、ハッカーによるロシアの人気タクシーアプリのAPIの脆弱性の悪用により、モスクワで深刻な交通渋滞が発生しました。攻撃者はAPIを操作してシステムに偽のタクシーを大量に送信し、サービスを麻痺させ、市街地の渋滞を引き起こしました。この事件はAPIのセキュリティ脆弱性がもたらす潜在的なリスクと、高度なサイバー攻撃に対する強固な防御策の必要性を浮き彫りにしました。重要なインフラを保護し、市民生活の安全と都市交通へのサイバー攻撃の被害を最小限におさえるため、積極的なセキュリティ対策を講じることの重要性を改めて示しています。

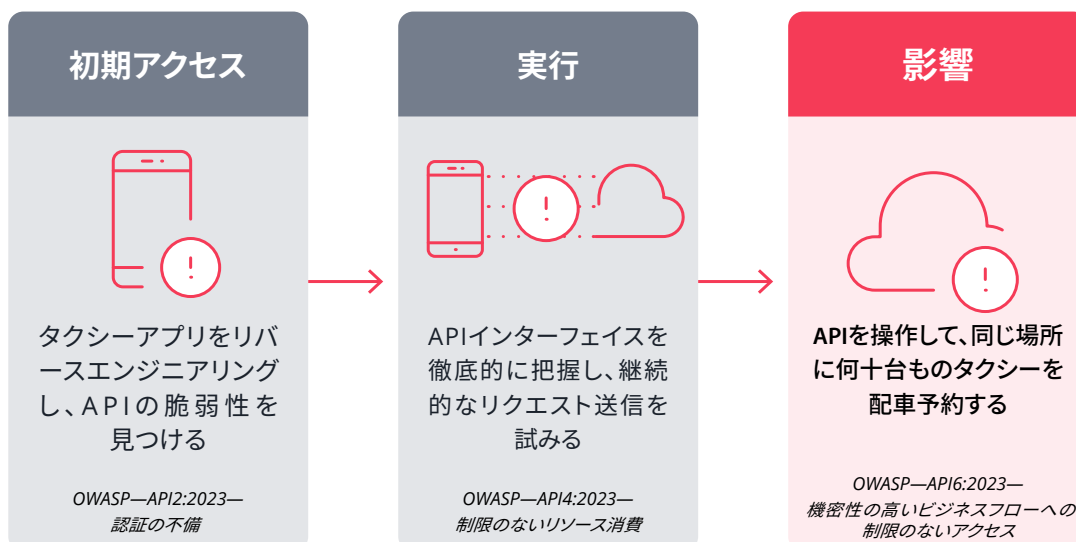


図7. タクシーアプリのAPIを悪用して車両をリモートで乗っ取る攻撃経路

まとめると、APIの脆弱性に起因する脅威とリスクは以下の通りです：

- ・ OTAスプーフィング：非正規のAPIコールが、正規のOTAアップデート要求を模倣
- ・ サイバー攻撃／ランサムウェアインシデント：攻撃者がシステムに侵入し、ランサムウェア感染の起点となる
- ・ 車両侵入／イモビライザーシステム：APIの欠陥による、車両制御システムへの不正アクセス

設計から実走行まで、SDVのAPIとセキュリティリスクをワンプラットフォームで完全に可視化

広大な自動車エコシステムにおけるAPIセキュリティリスクを効果的に軽減するには、体系的なアプローチを実施することが不可欠です。すべてのコンポーネントが潜在的な攻撃対象となるため、包括的な戦略が必要となります。“Innovation Insight for API Protection”と題された Gartner® のレポートによると、『API 保護製品は、ディスカバリ、ポスチャーマネジメント、ランタイムプロテクション』という主要な3つの機能が鍵となります。*これらの原則に基づき、VicOne と 42Crunch は共同で自動車のライフサイクルにおける自動車サプライチェーンの API セキュリティリスクに対処するため、継続的な発見（検出）、動態（状態）管理、ランタイム保護を可能にする統合ソリューションを提供しています。

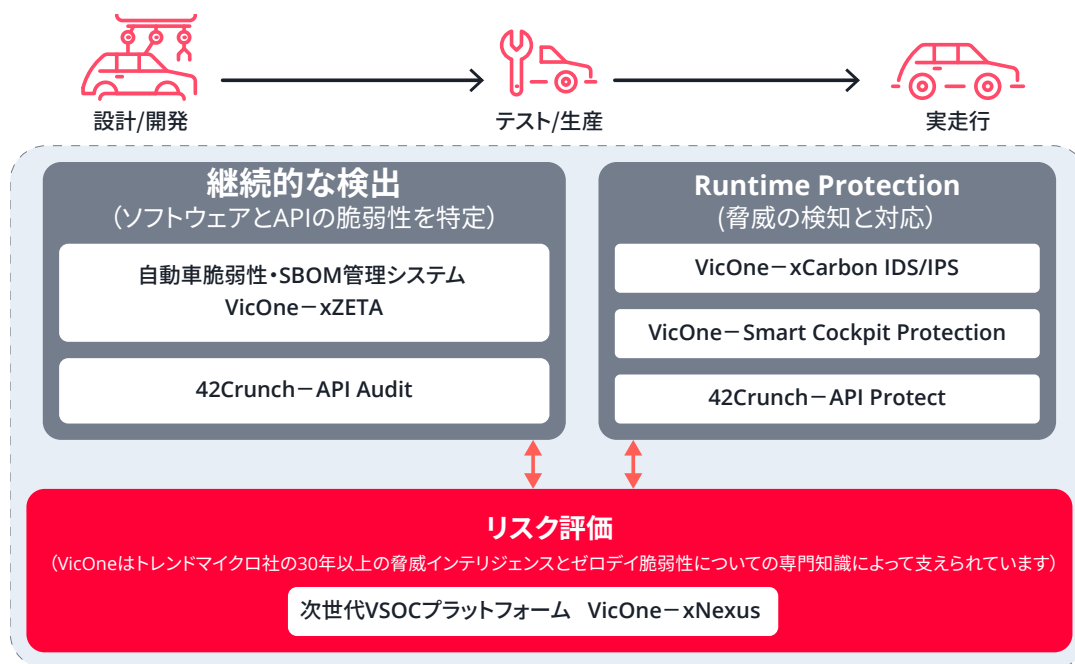


図8. 自動車のライフサイクルを通して VicOne と 42Crunch が提供する包括的で実用的なソリューション

設計やテストの段階において重要なのは、攻撃者に見つかる前にソフトウェアやAPIの脆弱性を継続的に特定することです。42Crunch のAPI Auditを使えば、API の設定ミスやAPI の脆弱性を特定できます。例えば、危殆化した自動車クラウドサービスのAPIを含むケースに関して、SQLインジェクションの脆弱性を設計段階で特定することができ、最新のOWASP (Open Worldwide Application Security Project) のAPIセキュリティ脆弱性トップ10を開発段階で排除することで、将来システムが運用される際に深刻な脅威となることを防ぎ、シフトレフト（セキュリティ対策やテストの前倒し）をさせることができます。

VicOneの自動車脆弱性・SBOM管理システムxZETAでは、SBOMの生成を自動化し、継続的な脅威検知を強化することでゼロデイ脆弱性、未公開脆弱性、既知の脆弱性、マルウェア、ランサムウェア、高度な持続的脅威といった様々な脅威をバイナリやファームウェアから早期に発見することができます。これにより、API とファームウェアの両方の脆弱性を、システム稼動前に事前に緩和し深刻なセキュリティインシデントを未然に防ぐことができます。

実走行中の車両において42CrunchのAPI Protectは、APIに対して直接ランタイム保護を実施し、悪意のある攻撃から各APIを保護します。一方、VicOneの侵入検知・防御システム (IDS/IPS) xCarbonとSmart Cockpit Protectionは、悪意のあるCAN (コントローラエリアネットワーク) メッセージ、DoS (サービス拒否) 攻撃、異常なAPIトランザクションなどの異常を検知できます。これらにより、脅威の検出と対応をリアルタイムで行うことができます。

完全な可視化は、車両内とバックエンドの両方のインフラストラクチャにおける問題と課題を共通理解するために不可欠です。VicOneの次世代車両セキュリティオペレーションセンター (VSOC) プラットフォーム xNexus は、設計段階から実走行時の検出まですべての脆弱性とセキュリティイベントを統合し可視化することでリスクを包括的に把握できます。また人工知能(AI)と大規模言語モデリング(LLM)を活用することで、これらの脆弱性とセキュリティイベントをコンテキスト化された攻撃経路に関連付けることができ、自動車メーカーとサプライヤーはより正確かつ実用的な脅威に関する洞察により自動車のサプライチェーン全体にわたる継続的かつ動的なリスク評価が容易になります。

例えば、タクシーアプリのAPIが悪用された事件では、当社の統合ソリューションにより、APIにおける認証の不備やトークンの異常を最初のアクセスから検出することができます。攻撃者がテストを開始すると過剰なリソース消費と異常なAPIトランザクションを検出できます。

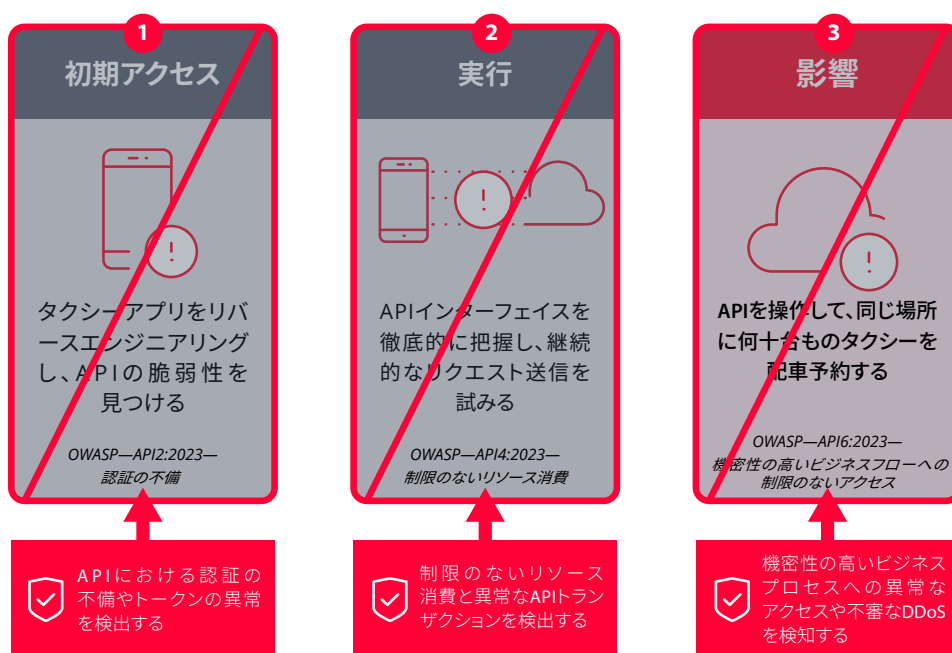


図9. VicOne x 42Crunchのソリューションによる対策

行き届いた検出力で安心・安全を確保: SDVのリスクを回避

当社の統合ソリューションにより、自動車メーカーとサプライヤーはエコシステム（車両、モバイル、Web）内の API セキュリティ問題を評価し、見つかった問題に迅速に対処することができます。継続的なディスカバリ、ポスチャーマネジメント、ランタイムプロテクションにより、自動車サプライチェーンの API セキュリティリスクを効果的に管理し、以下のようなメリットを実現します。：

- ・ 網羅的なリスク可視性：自動車エコシステム全体の API セキュリティや自動車関連リスクを網羅的に可視化
- ・ リソース配分の最適化：API セキュリティイベントを他の車両データやセキュリティイベントと統合することで、リアルタイムに変化するリスク評価を改善
- ・ 脅威の精確な検出：最新の OWASP トップ 10 の API セキュリティ脆弱性をより迅速かつ精確に検出
- ・ コンテキスト化されたリスクの可視化：エコシステム全体のセキュリティイベントとデータを相関させることで、具体的な対策策定に繋がる、コンテキスト化された脅威に関する洞察を得ることができる
- ・ 長期的なセキュリティ対策：シームレスな段階的実装と、車載システムのエージェント有無に合わせた柔軟な拡張性により、自動車のライフサイクルの変化に対応しながら長期的なセキュリティ対策が可能に

SDV の API セキュリティリスク回避ソリューションの詳細については弊社までお問い合わせください

*Gartner, [Innovation Insight for API Protection](#), Dionisio Zumerle, Jeremy D'Hoinne, et al, 2 February 2024. (For Gartner Subscribers only) GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

自動車業界におけるSDVのAPIセキュリティ
リスクに対する課題_2024.8
Copyright © 2024 VicOne Corp.
All Rights Reserved.

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)

