2025 | 自動車およびスマートモビリティの
グローバルサイバーセキュリティ報告書

Upstream

MIND THE CYBER GAP

目次

目次

CEOからの
オープニングメッセージ

2025年 Global Automotive and Smart Mobility Cybersecurity Reportをお届けできることを嬉しく思います。このレポートは、サイバー脅威が業界の対応準備を上回るペースで進化し、規制主導の対策を上回るという重要な時期に発表されました。
UNECE WP.29 R155の遵守、特に2024年のマイルストーンにより規制遵守への注目が集まりましたが、同時に誤った安心感も生み出しました。R155などのサイバーセキュリティ規制は最低限必要な基準を設定していますが、私たちのエコシステムが直面している動的で複雑な脅威に対処するには不十分です。

主要なOEMやモビリティ関係者との取り組みを通じて、私たちは安全性、ブランド評価、事業継続性、データプライバシー、および財務安定性に重大な影響を及ぼすサイバーリスクの急増を目の当たりにしてきました。
2024年には、自動車およびモビリティエコシステムに対するランサムウェア攻撃が急増し、前例のない混乱を引起こしました。Software Defined Vehicle（SDV）や自動運転車両の台頭により新たな脆弱性が生まれ、EVチャージャーやフリートシステムなどのスマートモビリティデバイスが重要インフラに統合されることで、攻撃対象領域が拡大し、リスクが増大しています。

中国の戦略的投資と政府の支援により、同国の自動車産業は、特に電気自動車（EV）分野で世界的なリーダーシップを獲得しました。しかし、この急速な成長により、サイバーセキュリティ、データプライバシーリスク、そして潜在的なスパイ行為に関する重大な懸念も浮き彫りになり、緊急対策の必要性を強調することになりました。

これらの課題に対処するには、協調的な行動が求められます。OEM、Tier-1、Tier-2サプライヤー、スマートモビリティプロバイダーは、単なる規制遵守を超えた、さらなる取り組みをしなければなりません。 ステークホルダーは、積極的なデータ駆動型の戦略を採用し、vSOC、モビリティ中心のAPIセキュリティ、脅威インテリジェンス、および脆弱性管理に一貫して投資することで、サイバーギャップを埋め、レジリエンスを強化する必要があります。サイバーセキュリティはもはや単なる技術的な課題ではなく、リーダーシップのコミットメントを必要とする戦略的必須事項です。 協力して取り組むことで、自動車およびスマートモビリティのエコシステムを強化し、顧客の信頼を守り、業界の成功を確実なものとすることができます。

Upstreamでは、2017年にUpstreamプラットフォームを初めて導入して以来、コネクテッドビークルエコシステムとモビリティ資産の保護の最前線に立ってきました。 Upstreamプラットフォームは、組織がコンプライアンスを超えて、何百万台もの車両およびモビリティ資産を積極的に監視し保護する上で、重要な役割を果たしてきました。高度なAIおよびML機能と深い業界専門知識を持つUpstreamは、今後の課題に取り組む態勢が十分に整っています。2025年以降を見据える中、私たちはコネクテッドモビリティの未来を守るために先頭に立ち続けることを約束します。

敬具

Yoav Levy

共同創業者兼CEO

概要

自動車およびスマートモビリティエコシステムは、Upstreamの継続的に更新されるサイバーセキュリティインシデントのデータベースの恩恵を受けており、サイバー脅威の一歩先を行くための重要なリソースを提供しています。

2024年だけでも、Upstreamの研究者は409件の新たなインシデントを分析し、2010年に遡るケースも含め合計1,877件の記録事例に貢献しました。 数百のディープ ウェブ フォーラムおよびダーク ウェブ フォーラムを監視することで、進化するサイバー セキュリティ環境に自信を持って対応できるよう、包括的かつ実用的なレポートを作成しました。Upstream は、自動車のサイバー インシデントのグローバルな分析を通じて、スマート モビリティ エコシステム全体が、既存の脅威と新たな脅威の両方を理解し、軽減し、防御できるように支援します。

UpstreamのAutoThreat®cyber threat intelligence プラットフォームは、先進技術、AI、自動化を活用して、Webのすべてのレイヤーを継続的にスキャンし、自動車およびスマートモビリティエコシステムに関連する新しいサイバーインシデントを検出します。 収集されたデータは、AutoThreat® プラットフォーム上でインデックス化および分析され、一元化された実用的な洞察のリポジトリを提供します。 弊社の研究者およびアナリストの専任チームは、このデータを綿密に分類して調査し、脅威アクターの動機と活動だけでなく、サイバー脅威がモビリティ資産に与える影響も明らかにしています。

各インシデントには、攻撃元の地理的位置、攻撃の影響、攻撃元の情報、その会社の種類、および攻撃者が標的に近づいているなどの追加情報が付加されます。 これにより、組織のセキュリティ体制を強化するのに役立つ、綿密かつ実用的なリポジトリが作成されます。

このレポートで分析されたインシデントは、メディア媒体を含むメディア、学術研究、バグ報奨金プログラム、政府法執行機関検証済みソーシャルメディアアカウント、Common Vulnerabilities & Exposures(CVE)データベース、およびその他の一般に入手可能なオンラインソースなど、さまざまなチャンネルから提供されました。これらに加えて、Upstreamのアナリストは、ディープウェブおよびダークウェブを積極的に監視し、自動車サイバー攻撃の舞台裏で活動する脅威アクターを追跡しています。

2024年、リスクの増大、標的となるモビリティ資産の増加、攻撃テクノロジーの進化に対処するため、弊社の調査範囲を大幅に拡大しました。この拡大された取り組みには、最も活発な脅威アクター1,133名の追跡が含まれており、その活動について第5章「ディープウェブとダークウェブからのサイバー脅威」で分析しています。注目すべきは、これらのインシデントが本レポートの各章で提示される統計やグラフに含まれていない点です。 攻撃ベクトルとその影響を分析する場合、インシデントには複数の攻撃ベクトルと潜在的な影響要素が含まれる可能性があることに注意してください。その結果、あらゆるインシデントにおいて、合計パーセンテージが100%を超える場合があります。

弊社の包括的なアプローチにもかかわらず、報告されていない、または発見されていない追加のインシデントや攻撃が存在する可能性があり、このレポートには含まれていません。

さらに詳しい情報については、AutoThreat® PROのお客様限定で詳細な分析をご覧いただけます。

エグゼクティブサマリー

2024年を通じて、自動車およびスマートモビリティのエコシステムではサイバー脅威が急増し、大規模なランサムウェア攻撃による前例のない混乱を引き起こしました。サイバーリスクが規制対応のスピードを上回る中、リスクと組織のレジリエンス（回復力）の間のギャップがますます拡大しています。

この拡大するギャップに対処するため、組織は規制対応を超えたレジリエンスの強化が必要となります。
Upstreamの「2025年グローバルモビリティサイバーセキュリティレポート」では、このサイバーセキュリティのギャップや、中国のEV市場の拡大、更には2024年にエコシステムに影響を与えた主なトレンド、脆弱性、インシデントについて詳しく分析しています。

2024年の主な動向
自動車とスマートモビリティのサイバーセキュリティリスクの規模と影響が更に拡大

2023年～24年にかけて、重大な影響を及ぼすインシデント（数千～数百万のモビリティ資産に影響）が増加し、全インシデントの

60%以上

を占めました

大規模インシデントは3倍以上に増加し、全インシデントの

19%

を占めました

92%

の攻撃がリモートで実行されました

65%

の攻撃はブラックハット（悪意のあるハッカー）によって実行されました

Source: Upstream Security

ブラックハットの脅威アクターはディープウェブやダークウェブを攻撃の起点として活用し、大規模な影響をもたらすことにますます意欲的になっている

70%

ブラックハットによる活動の70%が重大な影響を及ぼしました

76%以上

76%以上の攻撃が複数の利害関係者を標的とし、グローバルな影響を及ぼしました

Source: Upstream Security

中国は世界の自動車市場とサイバーセキュリティ環境の再構築を試みている

- 中国の戦略的投資と政府の支援により、同国は世界のEV市場におけるリーダーシップを確立しました。
- 2024年、中国はインテリジェントカー向けの新たなサイバーセキュリティ基準を導入し、グローバルな業界基準へ影響を強める計画を発表しました。
- 米国の対応と将来の課題
  サイバーセキュリティリスクの高まりを受け、2024年9月米国商務省は、中国及びロシア製の特定のハードウェア、ソフトウェアを搭載したコネクティッドカーの販売を禁止する規制案を発表しました。

サイバーセキュリティのギャップを埋めるため、AIドリブンの検知、調査機能の導入を加速し、vSOCの監視および修復機能を向上させることが求められます。

01.

自動車業界のサイバーセキュリティギャップの拡大

新たなイノベーションの波がリスクを増幅させ、規制への対応とサイバーセキュリティ対策が困難になっている。OEMはいかにサイバーセキュリティ態勢を強化し、ギャップを効果的に最小化できるのか?

自動車のイノベーションにより攻撃対象が拡大し、セキュリティ対策が困難になる中、OEMのサイバーセキュリティ態勢が脆弱化しています

ここ数年間、自動車とスマートモビリティのエコシステムにおける先進的なIoTテクノロジーの採用と相まって、革新的なソフトウェアデファインドおよび自動運転技術への規制圧力が高まっています。 自動車業界関係者は、新しい規制、規格、ガイドラインへの準備、そして新たなベストプラクティス開発の必要性という課題に直面しています。 BlackBerry QNXの調査によると、ソフトウェア開発者の75%が、納期の緊急性が機能安全を損なうことが多いことを認めており、迅速なイノベーションへの要求は自動車ソフトウェアチームに重くのしかかっています。[1] 最終的に、ソフトウェア開発チームとサイバーセキュリティチームは、迅速なイノベーションと拡大し続ける規制への準拠を迫られており、そのために継続的な対立が生じています。

2024年、多くのOEMとそのサプライヤーは、サイバーセキュリティマネジメントシステム(CSMS)に関するUNECE WP.29 R155および型式認証（2024年7月以降に生産される全ての新車に義務付けられた）、ならびにソフトウェアアップデート管理システム(SUMS)に関するR156[4]、およびISO/SAE 21434[3]の実装に引き続き重点を置きました。[2] これは、コネクティッド資産をサイバー脅威から保護するための統一されたアプローチを作り出す世界的な取り組みの一環です。

歴史的に、コンプライアンス活動に重点を置く時期には、エンドユーザーに疲労が生じることが多く、規制の有効性が損なわれることがよくあります。 サイバーセキュリティ疲れの場合、一旦コンプライアンス遵守が達成されると、セキュリティ態勢が低下し、組織はサイバーセキュリティ脅威に対して脆弱な状態になります。

このような行動は、消費者プライバシーにおけるGDPR[5]やCCPA[6]、医療におけるHIPAA[7]、決済におけるPCI DSS[7]、公益事業におけるNERC CIPなど、他の法律の採択後にも見受けられます。[9]

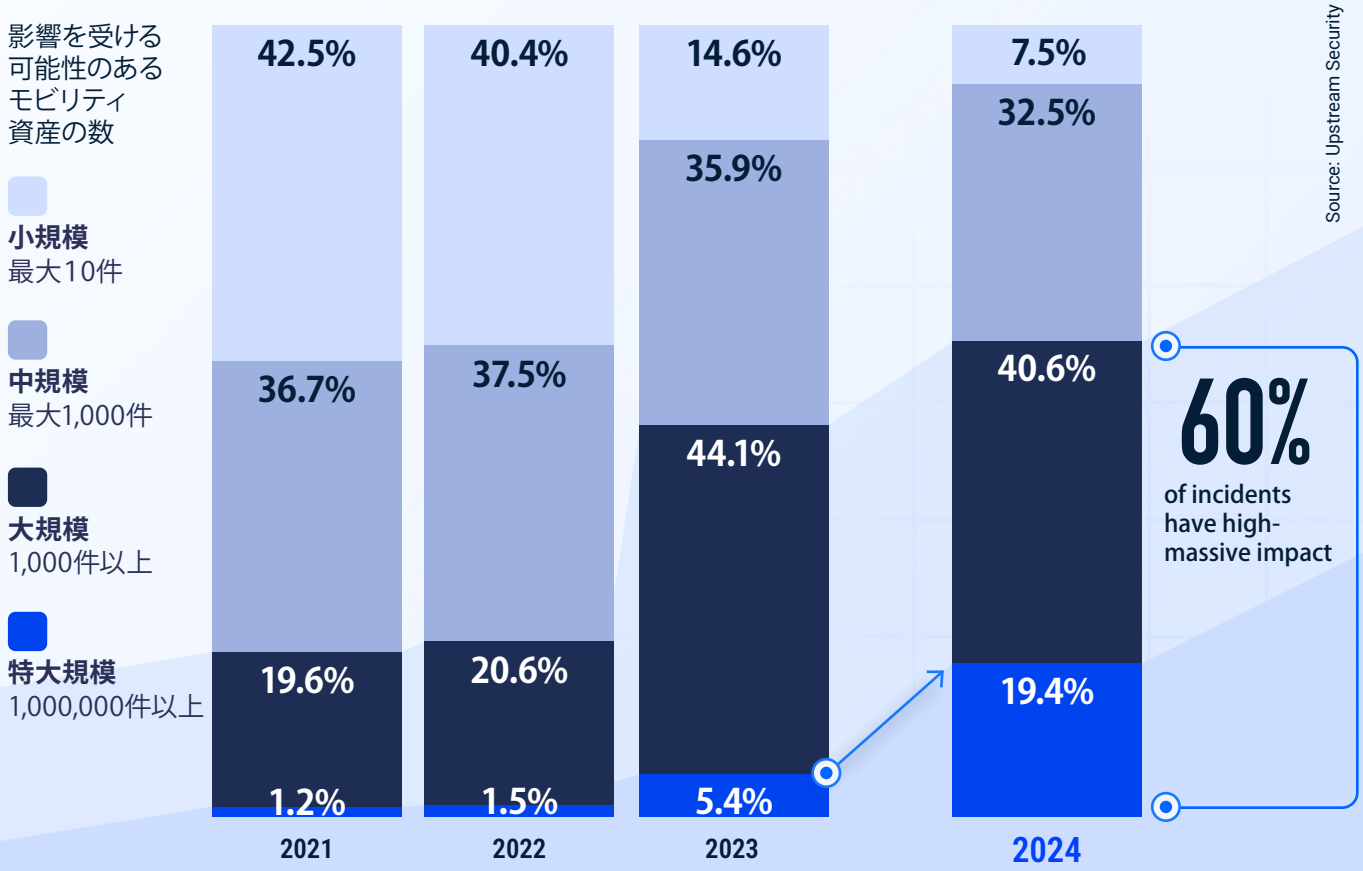
GDPR を例に挙げましょう。 施行以来6年間で、個人データ保護の権利に対する意識が高まり、データプライバシーとコンプライアンスは取締役会レベルの問題になりました。しかし同時に同意プロセスへの負担感を招き、同意メカニズムの有効性を弱め、プライバシー保護とデータ処理への信頼を損なうことにもなりました。さらに、結果よりもコンプライアンス違反と罰金の執行を優先することは、効果的な規制を示すものではありません。

自動車およびスマートモビリティのエコシステムにおいても同様で、現在コンプライアンスを重視しているという意識が、現行のサイバーセキュリティ態勢で十分だという錯覚を生み出しています。しかしサイバーインシデントのリスクや影響は増大しており、安全性や信頼性、運用の継続性、データのプライバシー、さらには財務面に深刻な影響を及ぼしています。

2024年1月、UpstreamのGlobal Automotive Cybersecurity Reportでは、2023年を自動車サイバーセキュリティの変換点と位置づけ、サイバーセキュリティのリスクが実験的なハッキングから大規模な自動車攻撃へどのように進化してきたかを検証しました。

Upstreamのデータによると、「大規模」（数千のモビリティ資産）または「特大規模」（数百万のモビリティ資産）に分類されるインシデントの割合は、2023年から2024年にかけて引き続き増加し、全インシデントの約60%を占めるようになりました。[10]

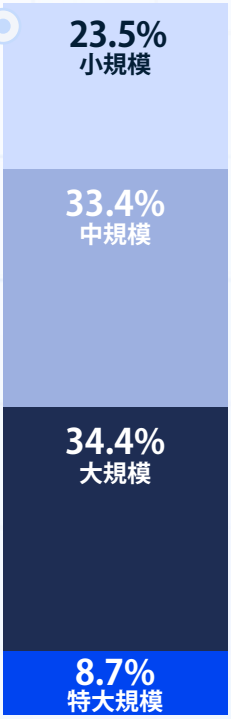
2021年から2024年までの公表されたサイバーインシデントの想定規模別内訳：



Upstreamがダークウェブとディープウェブ上で最も活発な1,133の脅威アクターを調査した結果、脅威アクターの動機が大規模な攻撃と広範な影響へとシフトしていることが判明しました：[11]

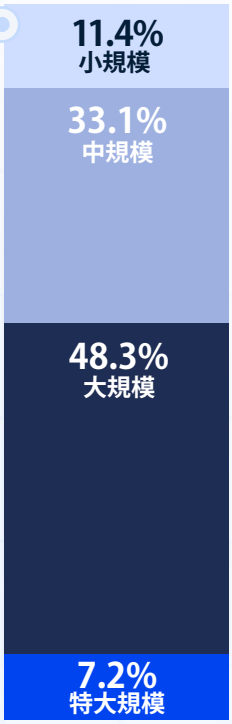
2024年には、ディープウェブおよびダークウェブ上のサイバー活動の43%が、数千から数百万のモビリティ資産に影響を及ぼす可能性があるとされました。

ディープウエブ・ダークウェブの脅威アクターの活動の規模別内訳：2024年



Source: Upstream Security

ブラックハット及び不正行為者の活動の規模別内訳：2024年



Source: Upstream Security

ブラックハットと不正行為者に焦点を当てると、56%が数千から数百万のモビリティ資産に影響を与える可能性がありました。

ブラックハットおよび不正行為者の活動対象：2024年

2024年のディープウェブやダークウェブ上のブラックハットや不正行為の55%は、OEMを標的にするか世界規模で影響を及ぼしていました。

46.7%
グローバル

8.3%
複数のOEM / ステークホルダー

45.0%
単一のOEM/ステークホルダー

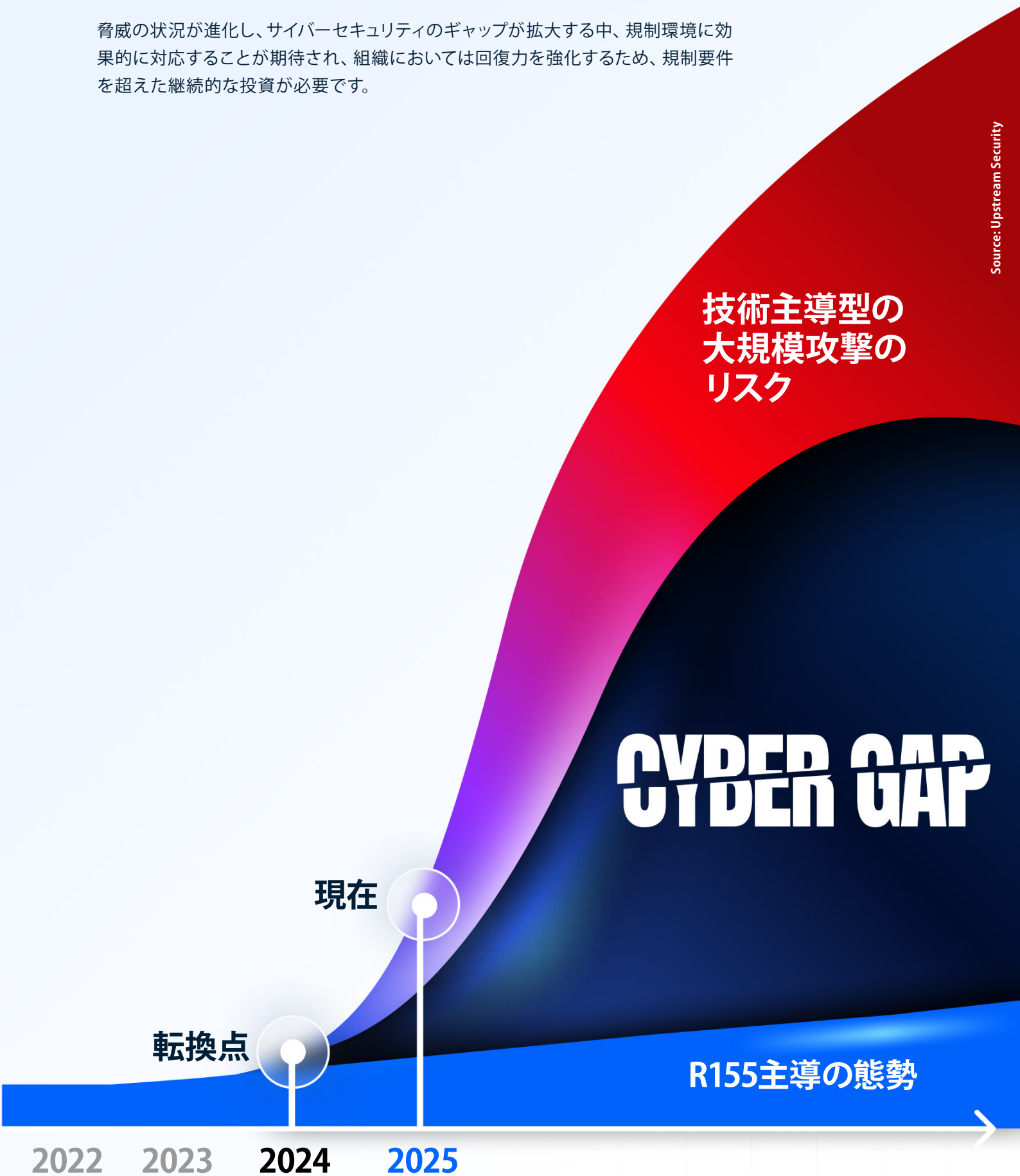
Source: Upstream Security

大規模インシデントの増加は、新たなサイバーセキュリティの脆弱性が生じていることを示しており、その背景にはいくつかの要因があります：

- 車両と複数のデバイスやアプリ（OEMコンパニオンアプリ、充電アプリ、販売店、スマートモビリティなど）間のAPI接続は、サイバー攻撃のハードルを下げ、大規模な遠隔攻撃の主要な攻撃経路となっています。
- Software Defined Vehicle（SDV）と自動運転車両技術の導入と急速な革新により、車両の主要機能への遠隔操作が可能となり、大規模な攻撃をもたらす結果となります。
- 拡大が続く攻撃対象領域、攻撃するハードルの低下、攻撃手法の多様化等により、攻撃者は幅広い範囲の攻撃を仕掛けることができます。
- AI を利用した攻撃プロセスと予備調査の自動化により、脅威アクターは迅速かつ少ないリソースで大規模な攻撃を仕掛けることが可能になります。
- ランサムウェア・アズ・ア・サービス（RaaS）やデータ抽出攻撃は実行が比較的容易で、攻撃者に即座に金銭的利益や評判の向上をもたらします。
- 規制遵守に重点を置くあまり、ITおよび製品サイバーセキュリティチームに負担が増大していることに加え、ますます複雑化するIT、OT、製品環境が、攻撃者に悪用される機会を生み出しています。

自動車のサイバーセキュリティギャップ

脅威の状況が進化し、サイバーセキュリティのギャップが拡大する中、規制環境に効果的に対応することが期待され、組織においては回復力を強化するため、規制要件を超えた継続的な投資が必要です。



ランサムウェアの年：前例のない影響をもたらした大規模なランサムウェア攻撃が席巻

自動車業界が、ソフトウェア指向アーキテクチャ、自動運転、電気自動車、アフターマーケットIoTデバイスなど先進技術を迅速に取り入れている中で、現行の規制主導のサイバーセキュリティ態勢と現実の脅威との間のミスマッチが明白になっています。

> ***企業および製品のサイバーセキュリティに対する最大の脅威のひとつはランサムウェアです。おそらく過去10年間で最も典型的なサイバー犯罪であり、毎年その脅威は増加し続けています。***

ランサムウェア攻撃は、サービスと業務の中断による収益損失、身代金の支払い、高額な復旧コスト、データとプライバシー侵害による法的・規制上のコンプライアンス問題や罰金、さらにはブランドと評判の損害等深刻な金銭的影響をもたらします。

一方、製品のサイバーセキュリティに関して、特に自動車やスマートモビリティのエコシステムでは、ランサム攻撃は安全性、稼働時間、運用の可用性と効率性に直接的な影響を与えるだけでなく、機密データに対する重大なリスクももたらします。

ランサムウェア・アズ・ア・サービス（RaaS）の採用は、クラウドコンピューティングモデル（例：IaaSやPaaS）に類似したランサムウェア配布モデルであり、ランサムウェアプロバイダーがインフラとサービスを維持し、顧客にアクセスを提供するために料金を請求するものです。このモデルの採用は、ランサムウェアの継続的な成長と成功の主な要因となっています。

2024年4月、アメリカ合衆国財務省は、イランのために悪意のあるサイバー活動に関与した2つの企業と4人の個人に制裁を課しました。これらの活動は、ランサムウェア、スピアフィッシング、マルウェア攻撃を含むサイバー作戦を通じて、10社以上のアメリカ企業および政府機関を標的にしていました。[12] またこの4人の人物は、その関与により、米国司法省から起訴されました。[13] 7月には、北朝鮮国籍の人物が、米国の病院やその他の医療機関を標的としたハッキングと恐喝の共謀に関与したとして起訴されました。[14]

2024年8月、連邦捜査局（FBI）、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）、および国防総省サイバー犯罪センター（DC3）は、共同サイバーセキュリティ勧告（CSA）を発表し、イラン拠点の脅威アクターグループが米国および海外の組織を引き続き標的にしていることを警告しました。[15]

攻撃者は2024年、ゼロデイ脆弱性の悪用技術、エッジデバイスの脆弱性を狙った攻撃、生成AI（GenAI）を活用した自動化技術といった新たな手法を駆使して攻撃を行い、大規模で高価値の組織や著名な対象を狙う「ビッグゲームハンティング」に注力しました。加えて、運用技術（OT）および接続デバイスを標的化した攻撃が増加し、特にデータ流出に重点を置く動きが見られ、自動車およびスマートモビリティエコシステムにおいてランサムウェア攻撃が拡大し、2024年のランサムウェア経済の成長を促進しました。この背景には、米国証券取引委員会（SEC）のサイバーセキュリティ事件開示ルール、さらにEUのNIS 2サイバーセキュリティ指令といった法規制の影響もあります。[17]

より厳格なサイバーセキュリティ報告要件や巨額の規制罰金により、ランサムウェアの動向が変化しました。 攻撃者はデータを暗号化し、業務を停止させることなく、財務的および評判的な損害を与える可能性があり、被害者はもはや攻撃を無視してのインシデント報告を回避することが困難となっています。

攻撃者が重要なデータを暗号化し、被害者の業務を停止させ、機密データの公開を脅迫して金銭を要求する従来の二重恐喝ランサムウェア手法の攻撃効果は低下しています。データ暗号化は多大なリソースが必要であり、また多くの組織がバックアップを活用してデータを復旧できるようになったためです。

2023年9月には、米国の大手トラックおよび車両管理ソリューション提供企業が長期にわたる二重恐喝攻撃を受け、連邦規制で義務付けられている走行時間の電子記録や輸送した在庫の追跡ができなくなる事態に陥りました。[18]

これを受けて、同企業は外部のサイバーセキュリティ専門家を雇い攻撃の調査を行い、米国連邦自動車運送安全局（FMCSA）に免除を申請して、サービスが復旧するまで、トラック運転手が紙の記録簿を使用できるようにしました。[19]

2024年11月、同企業で大規模なデータ流出が発生したと報じられました。攻撃者がダークウェブフォーラムに、同企業のシステムから70TB以上の機密データにアクセスし、流出させたことを広告しました。攻撃者は自身の主張を証明するため、盗難データの証拠とサンプルを公開しました。データのコピーは3万ドルで販売され、データの削除には10万ドルの交渉価格が提示されました。[20]

現在、攻撃者はデータ暗号化からデータ流出に焦点を移し、盗難データを最高入札者に売却するデータ流出市場を構築することで、攻撃の負担を軽減し、全体的な効率と投資収益率を向上させています。

チェックポイントの調査によると、2024年第2四半期における世界的なランサムウェア攻撃は30%増加し、過去2年間で最も高い増加率となりました。業界別の影響としては、製造業が最も大きなの影響を受けた分野であり、世界的に公表されているランサムウェア攻撃被害者の29%を占め、前年比で56%という大幅な増加を記録しました。輸送業界は40%の増加が確認されました。一方で、通信および公益事業業界では、ランサムウェアインシデントはそれぞれ177%と186%という劇的な増加が見られました。これらの業界はIoTへの依存度が高く、モビリティエコシステムと密接に関連しています。[21]

2024年、AutoThreat®の研究者たちは、108件のモビリティ特有のランサムウェア攻撃と214件のデータ漏洩を検出し、これらがモビリティエコシステムにおけるサイバーセキュリティインシデントの増加に大きく寄与しました。

特筆すべきは6月中旬、1万5000のディーラーが使用する米国の主要ディーラー管理ソフトウェアプロバイダーがランサムウェア攻撃を受け、約3週間稼働停止しました。複数の情報源を引用したCNNの報告によると、同社は復旧を急ぎ、稼働停止を終わらせるために、2500万ドルの身代金を支払った可能性が高いとされています。[22]

> ***アンダーソン・エコノミック・グループ（AEG）は、フランチャイズ型自動車ディーラーにおける直接的な総損失が10億2000万ドルに達したと推定しました。[23]***

AEGの試算では、3週間の稼働停止期間の損失が、新車販売による約5万6000台分の収益損失、中古車販売および部品・サービス収益損失、追加の人件費やITサービス費用、そして在庫にかかる追加のフロアプラン利息費用が含まれます。なお、消費者損害、ディーラーの評判損害、訴訟費用、その他損害カテゴリーは含まれていません。

2024年、AUTOTHREAT®の研究者たちは、

108件

のモビリティ特有のランサムウェア攻撃と

214件

のデータ漏洩を検出し、これらがモビリティエコシステムにおけるサイバーセキュリティインシデントの増加に大きく寄与しました。

2024年のさらなる例をいくつかご紹介します。

- 2月、日本のOEM米国部門がランサムウェア攻撃を受け、その結果、22GBの機密性の高い、車両および顧客情報が盗まれたと報じられています。[24]
- 2月、韓国のOEMが大規模なランサムウェア攻撃を受け、業務が中断されました。[25]
- 3月、中国のTier-2メーカーがランサムウェア攻撃を受け、1.2TBのデータが大量に漏洩し、中国および世界のOEMに影響を与えました。[26]
- 4月、ドイツのOEMのイタリア支社でデータ漏洩が発生し、顧客の個人情報が流出しました。[27]
- 7月、インドのOEMがランサムウェア攻撃を受け、企業データが盗まれました。[28]
- 8月、韓国の自動車部品メーカーがランサムウェア攻撃を受け、2.3TBの企業データが漏洩しました。[29]
- 9月、自動車のCANバスプロトコルソリューションを専門とする中国のTier-1メーカーがサイバー攻撃を受け、Webサイトの運営が妨害されました。[30]

サイバーセキュリティリスクはSoftware Defined Vehicle（SDV）や自動運転技術の普及により劇的に変化する可能性

CASE(コネクティッド、自動運転、シェアリング、電動化)と総称される技術の融合により、関係者は従来のハードウェア定義の構造設計からソフトウェア指向の構造設計に移行する必要に迫られ、サイバーセキュリティの課題が高まっています。

APIは車載コンポーネント、バックエンドシステム、およびアプリケーション間の接続性を向上させる上で重要な役割を果たしてきました。 APIを通じてより多くの機能が公開されるにつれ、サイバーセキュリティのリスクも劇的に増加し、一方で攻撃のコストとしきい値は低下しています。

ソフトウェアコンポーネントを制御し、脆弱性を悪用する能力は、フリート全体の制御システムのサイバーセキュリティ態勢に重大な脅威をもたらし、攻撃の規模と影響が指数関数的に拡大する原因となります。

OTA による頻繁なアップデートは、SBOMが静的ではなくなり、車両が工場から出荷されてからも長期間にわたって継続的に進化することを意味します。リスクプロファイルは絶えず変化し、常にリスクと脆弱性の分析が必要ですが、リアルタイムで修正することも可能です。

さらに、最新のSDVへの攻撃対象領域は、車載コンポーネントにとどまらず、充電ポイントやネットワーク、スマートモビリティ、OEMサービス、テレマティクスデバイス、電気自動車(EV)充電などのサードパーティアプリケーションにも及んでおり、さらに複雑さを増しています。

最後に、SDVや自動運転車両（AV）によって生成され、バックエンドシステムに保存される膨大なデータは、さらなるリスクをもたらします。バックエンドシステム（テレマティクスサーバーやアプリケーションなど）は、コネクテッドビークルの高度な機能やサービスを提供するだけでなく、車両の状態、位置、使用パターン、ドライバーの行動に関連する膨大な量の機密データを収集および管理する上で重要な役割を果たします。

ハッカーは、実際の車両をハッキングする必要さえなく、何百万人もの自動車ユーザーの個人情報を含むデータを盗むことができます。悪意のあるハッカーが制御とデータ アクセスの両面でフリート全体に影響を及ぼす可能性があるため、バックエンドサーバーに対するサイバー攻撃の脅威は特に高くなります。

ソフトウェア指向の構造設計、API、およびバックエンドシステムへの依存度が高まっているため、OEMがソフトウェアサービス、コンポーネント、およびバックエンドシステムに保存されている機密データを保護することが緊急に必要とされています。

SDV と AV が普及するにつれて、サイバー態勢のバランスが劇的に変化し、サイバーセキュリティのギャップがさらに拡大する可能性があります。

SDVおよびAV技術は、さまざまなサイバー攻撃に対して脆弱

Software Defined Vehicle（SDV）や自動運転車両は、車両のコア機能へのリモートアクセスを提供するため、ハッカーが大規模かつ効果的に攻撃できるようになります。

2024年、セキュリティ研究者たちは、SDVやAVで使用されているソフトウェアとハードウェアコンポーネントに多数の脆弱性を発見し、悪用しました。これには、LiDARセンサー、レーダー、カメラ、高精度位置決めハードウェア、OEMアプリケーション、ソフトウェア開発プラットフォームなどが含まれ、多くの場合、車両の安全性と運用信頼性に直接影響を及ぼしました。

2024年2月、デューク大学のセキュリティ研究者たちは、使用中のレーダーシステムを事前に知らなくても、AVセンサーシステムにハルシネーションを引き起こすことができました。マッドレーダーと呼ばれる攻撃のデモの中には、研究者たちがドップラーレーダーシステムでハルシネーションを誘発し、センサーから離れた車両が向きを変えて正面衝突に向かっていると誤認させるものもありました。 研究者によると、マッドレーダーはレーダーの種類を「マイクロ秒単位で」検出して学習し、瞬時かつ適切に攻撃を開始させるとのことです。 このタイプの攻撃は、レーダーを使用するアダプティブ・クルーズ・コントロール(ACC)システムを騙して、前方の車が実際には加速していないのに、加速していると誤認させ、正面衝突を引き起こす可能性があります。[31]

2024年3月、カリフォルニア大学アーバイン校と日本の慶應義塾大学のセキュリティ研究者が、市販されている第1世代および第2世代の9種類のLiDARシステムに15の脆弱性を検出しました。これらの脆弱性により、直接偽の車両や歩行者になりすましたり、AVの目の役割のセンサーから実際の車両が見えなくなることが可能になります。 LiDARセンサーに対するこれらの攻撃能力は、緊急ブレーキや前方衝突など、さまざまなAVの危険運転を直接引き起こすために使用される可能性があります。[32]

2024年5月、シンガポールのセキュリティ研究者は、カメラベースのコンピュータービジョンに依存していることを悪用して、LEDを使ってAVに干渉し道路標識を無視させることが可能であることを実証しました。セキュリティ研究者は、道路標識の外観を安定的に繰り返し歪めることができ、撮影されたすべてのフレームが歪んでいることを確認しました。 研究者チームは、中国の有名なAV開発企業で使用されているカメラを搭載した車両を使用して、実際の道路でシステムを検証しました。研究者チームは、安定化されたこの2つのバージョンの攻撃方法を開発しました。GhostStripe1は、車両へのアクセスを必要とせず、追跡システムを使用してターゲット車両のリアルタイムの位置を監視し、それに応じてLEDの点滅を動的に調整することで、標識の誤認識を引き起こします。GhostStripe2は車両へのアクセスを必要とし、カメラの電源線にトランスデューサー（エネルギーをある形態から別の形態に変換する電子装置）を設置し、フレーミングの瞬間を検出し、タイミング制御を微調整します。セキュリティ研究者は、GhostStripe1とGhostStripe2の成功率はそれぞれ94%と97%だったと断言しています。[33]

2024年5月、バッファロー大学のセキュリティ研究者が、マルチセンサーフュージョンシステムの脆弱性を発見しました。このシステムは、LiDAR、カメラ、レーダーセンサーからのデータを統合する技術で、AVで一般的に使用されています。 セキュリティ研究者は、1つの敵対的オブジェクトを使用して3種類全てのセンサーを同時に侵害できる高度な攻撃手法を導入しました。 このオブジェクトは簡単かつ安価に製作できるため、高度な隠密性と柔軟性をもって攻撃を実行することが可能です。セキュリティ研究者は、わずか2つの小さな敵対的オブジェクトを配置することで、この攻撃によって被害者のAVの認識システムからターゲット車両が効果的に見えなくなることを実証しました。[34]

マルチセンサーフュージョンは、長年にわたり適切なサイバーセキュリティ対策と考えられてきました。複数の種類のセンサーが冗長性を確保し、侵害されたセンサーを補完することができるからです。セキュリティ研究者の調査結果によると、攻撃者は複数の種類のセンサーを同時に侵害することが可能になっているため、これは、今ではもはやそうではないことを示しています。

2024年6月(2024年9月に公表)、セキュリティ研究者は韓国OEMのディーラーAPIに脆弱性を発見し、ナンバープレートのみで車両を乗っ取ることが可能だということが明らかになりました。

セキュリティ研究者は、概念実証攻撃用のUIの開発まで進めました。それは、サードパーティのAPIを使用してナンバープレートをVINに変換するVINリトリーバーツール、被害者の車両を乗っ取ったり、所有者の氏名、メール、電話番号などの個人情報を受動的に盗むために使用できるエクスプロイトモジュール、そして影響を受けた車両に命令を出したり位置を特定したりするために使用できるガレージモジュールで構成されています。[35]

研究者によると、「被害者側からは、自分の車両にアクセスされたり、アクセス権限が変更されたりしたという通知は一切ありませんでした。 攻撃者は、誰かのナンバープレートを特定し、APIを通じてそのVINを入力すれば、受動的に追跡したり、ロック解除、エンジン始動、クラクションを鳴らすなどのアクティブなコマンドを送信できる可能性があります。」ということです。[36]

研究者らはOEMに通知し、OEMは脆弱性を修正し、それが悪用されたことはないことを確認しました。 このインシデントは、APIの脆弱性が及ぼす甚大な影響を浮き彫りにし、それがSDVにどのように大きな影響を与えるかを示しています。

2024年6月、セキュリティ研究者が、インフォテインメント、ADAS、テレマティクス、自動運転などの様々な自動車部品で使用される人気の車両ソフトウェア開発プラットフォームのSGI Image Codecに、CVE-2024-35213として識別されCVSSスコア9.0（重大）が割り当てられた深刻な脆弱性を特定しました。 CVE-2024-35213が悪用されると、ソフトウェアによるシステムのクラッシュ、画像処理サービスの中断、または不正なコードの実行につながる可能性があります。[37]

2024年9月、セキュリティ研究者は、サービス拒否（DoS）攻撃、特にインターネット制御メッセージプロトコル（ICMP）フラッド攻撃が自動運転（AD）システムに与える影響についてその制御モジュールに焦点を当てて調査した研究を発表しました。 2つの実験装置が考案されました。1つ目はADソフトウェアスタックを実行しているRaspberry PiへのICMPフラッド攻撃で、2つ目は市販のAVの高精度な測位のための全地球航法衛星システムリアルタイムキネマティック（GNSS-RTK）デバイスに対する1台および2台の攻撃者によるICMPフラッド攻撃の影響を調査しました。 ADスタックはDoS攻撃に対して大きな影響はありませんでした。これは、このタイプの攻撃に対する一定の耐性を示しています。しかし、GNSS -RTKデバイスは重大な脆弱性を示しました。DoS攻撃下では、サンプルレートは1台および2台の攻撃者でそれぞれ公称レートの約50%と5%に低下しました。[38]

この研究結果は重要な意味を持っています。ADソフトウェアスタックがDoS攻撃を最小限の性能低下で対処できる一方で、GNSS-RTKデバイスのような重要な外部コンポーネントが非常に脆弱であることを示しているからです。GNSSシステムの脆弱性は、AD システムの回復力における重大な欠陥を浮き彫りにしています。特に、リアルタイムの測位ハードウェアに関して、車両の位置情報の誤りにつながる可能性があり、AVの安全性と運用上の信頼性に直接影響を与える可能性があります。

近年、地政学的紛争の影響が高まる中、UpstreamのvSOCチームは、世界中の複数のOEMで衛星測位システム（GNSS）のスプーフィング（欺瞞行為）を特定しました。[39] 偽の座標が原因で消費者が自分の車両を正しく追跡できなくなるだけでなく、特にフリート管理（車両管理）の面で業務に混乱を招く恐れがあります。さらに、GNSSスプーフィング（位置情報の欺瞞行為）により、安全上のリスクが高まります。例えば、事故の際に、救急隊などの緊急対応者が適切な支援を提供できなくなる可能性があります。[40]

「近い将来、ランサムウェアの企業のITシステムを超えて、製品、OT（運用技術）、およびスマートモビリティデバイスにまで影響を及ぼす可能性」

IoTは、デバイスとシステム間のシームレスな通信を可能にすることで、スマートモビリティの運用技術（OT）を向上させます。 例えば、車両の組立ラインでは、IoTに接続されたナットランナーが正確なトルク適用を保証し、製造工程の効率と精度を向上させます。同様に、電気自動車供給装置（EVSE）はIoTシステムと連携して充電スケジュールを管理し、エネルギー消費を最適化することで、電気自動車を効率的に充電し、電力網に過負荷をかけないようにします。

2024年1月、セキュリティの研究者たちは、自動車の生産ラインで重要な締め付け作業に使われるコードレスのハンドヘルド空気圧トルクレンチ（ナットランナー）に、25件のセキュリティの脆弱性があることを発見しました。このツールは広く普及しており、安全性の確保が求められていますこれらの脆弱性を悪用されると、認証されていない攻撃者にナットランナーを完全に操られてしまうかもしれません。

研究室での実験によると、攻撃者がランサムウェア攻撃を仕掛ける方法が明らかになりました。この攻撃では、ナットランナーを使えなくし、その内蔵画面に身代金要求メッセージを表示させます。— また、この攻撃を自動化することで、会社のすべてのナットランナーを同時にハッキングし、生産ラインに大きな混乱をもたらす恐れがあります。 別のシミュレーション攻撃のシナリオでは、攻撃者が締め付けプログラムの設定を変更します。特に、機械的な締結部品に適用される最終トルク値を変更します。このトルク値は、デバイスの全体的な設計や運用性能を確保するために計算・設計されていますが、これが変更されることで、機械の故障、保証請求の増加、そして企業価値・信用の低下を招くリスクになる場合があります。[41]

2024年2月、ロシアのハクティビスト（政治的ハッカー）グループが、リトアニアの国営電気自動車（EV）充電サービスのデータおよびアプリ制御パネルに不正アクセスを行ったとされています。攻撃を中止し、ユーザーデータを流出させないことと引き換えに、グループは身代金を要求しました。しかし、企業がこれを拒否した結果、20,000人以上の顧客データが漏洩しました。その中には、名前、メールアドレス、そしてユーザー認証用のRFIDトークンのリストが含まれていました。EVサービスのユーザーでアプリから切断され、電気自動車の充電ができなくなった人達もいました。また、リトアニアにある同社のすべての充電ポイントも接続が切断されてしまいました。 すべてのサービスの復旧には数時間かかりました。

2024年2月、カナダのオンタリオ州にある都市がランサムウェア攻撃を受け、市の電話回線やオンラインシステムがほぼ完全に停止しました。この影響は、交通システム、工学サービス、子どもケア、墓地、図書館、市の地図、公衆衛生記録、不動産税やベンダー支払いなど、多岐にわたりました。市の当局者はこの攻撃を確認し、地元当局と協議しインシデントの調査を進めていること、また、システム機能の復旧に向けてサイバーセキュリティの専門家とも相談していることを発表しました。[42]

「スマートモビリティデバイスの重要インフラへの拡大：自動車およびスマートモビリティにおけるサイバーセキュリティの次なる最前線」

スマートモビリティデバイスの成長は、テレマティクスのフリートおよび在庫管理システム、カメラ、EV充電インフラ、農業用および重機デバイスなどを含む新たな時代の到来を意味します。しかし、これに伴い大規模なサイバーセキュリティのリスクが生じています。EV充電機器やインフラ、自律システムや自動運転キット、交通制御システム、テレマティクスシステム、フリート管理ソリューション、スマート農業機器といった幅広いデバイスが攻撃に対して脆弱な状態にあるのが現状です。

スマートモビリティデバイスに対する攻撃や脆弱性は、これらのデバイスが抱える重大なサイバーリスクを浮き彫りにしています。また、車両やスマートモビリティシステムの安全性、データ、運用の可能性に直接的な影響を及ぼします。

2024年2月、英国の製品安全基準局 (OPSS) は、サイバーセキュリティ規制に違反しているとしてスペイン製EV充電器の販売を停止しました。このことは、国のエネルギーシステムに危険が及ぶ可能性があると懸念されたからです。[43] ハッカーが数千台の規制に準拠していない充電器にアクセスし、一斉に起動させる可能性があります。その結果、ピーク需要が発生し、電力網に混乱を引き起こす恐れがあります。英国で40,000台、世界で50万台以上を販売しているこの企業は、2024年6月30日まで英国での充電器の販売を継続することが許可されていました。

このインシデントは、電気自動車供給装置（EVSE）の脆弱性がどのように悪用され、EV充電システムを制御・操作する可能性があるかを示しています。その結果、地域の電力網が損傷を受けたり、サービスが中断されたり、さらには国家規模の電力網に影響を及ぼす可能性があります。

2024年3月、コロラド州立大学のセキュリティ研究者たちは、ワイヤレス接続（例：Bluetooth、WiFi）を介してELD（Electronic logging devices：電子ログ記録装置）にアクセスする方法、そしてその結果、トラックの制御を奪い、データの操作を行い、車両間でマルウェアを拡散できることを示しました。[44] 研究者たちは、ELDが相当のセキュリティリスクを伴うデフォルトのファームウェア設定で配布されていることを見いだしました。 また、ELDは、通信にCANバスを使用し、OTAアップデート用の公開APIを備え、予測可能な識別子と脆弱なパスワードを使用しています。これにより、無線範囲内にいる攻撃者が車両システムに不正に接続し、アクセスすることが容易になります。 セキュリティ研究者たちは、14秒以内でトラックのWi-Fiに接続し、ELDを再書き込みし、悪意あるCANメッセージを送信してトラックを減速させることに成功しました。

米国には1400万台近くの商用の中型・大型トラックがあり、45すべてにELDの装備が義務付けられています。したがって、多くの商用車両の安全性と可動率に深刻なセキュリティリスクをもたらします。

研究者たちは、この発見を製造業者と米国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）に報告し、広範囲にわたって混乱が生じる可能性を強調しました。

2024年5月、ドイツのある農業機械メーカーがサイバー攻撃を受け、世界中の拠点に影響が及び、会社として生産活動の停止、全ITシステムの停止、外部の専門家チームの招集を余儀なくされました。攻撃の規模は明らかではありませんが、5月29日時点で、同社はプレスリリースを行い、生産を再開できていると発表しました。しかし、会社は依然緊急事態にあり、4週間以内に100%のパフォーマンスが回復すると予想されていました。[46]

2024年5月、ヨーロッパの著名な車両追跡および車両管理機器プロバイダーがデータ侵害を受けました。[47] ダークウェブのフォーラムで公開されたデータ漏洩では、同社の内部システムの脆弱性が露呈され、GPS のIMEI（識別番号）、リアルタイムの車両追跡データ、請求の詳細、顧客アカウント情報などの機密情報が危険にさらされました。攻撃者は、40カ国以上、5000社以上に及ぶ同社の全ての内部システムにアクセスできたと表明しました。

2024年7月、あるセキュリティ研究者がノルウェーの交通管理会社で製造された交通管制機のウェブベースUI（ユーザーインターフェイス）に、CVE-2024-38944として知られる脆弱性があることを発見しました。この脆弱性により、当該の研究者は1名の交通管制官の制御を完全に獲得し、交差点の設定や交通信号の順番を変更したり、交差点を4方向点滅状態にしたりすることが可能となり、この結果、サービス拒否が引き起こされ、交通渋滞や安全上のリスクが生じました。 この問題は、機能へのアクセスを許可する前の認証が欠けていたことに起因し、高度道路交通システム通信規約（NTCIP）のセキュリティと、簡易ネットワーク管理通信規約（SNMP）のような安全性の低いネットワーク管理通信規約のリスクに関する懸念を浮き彫りにしています。[48]

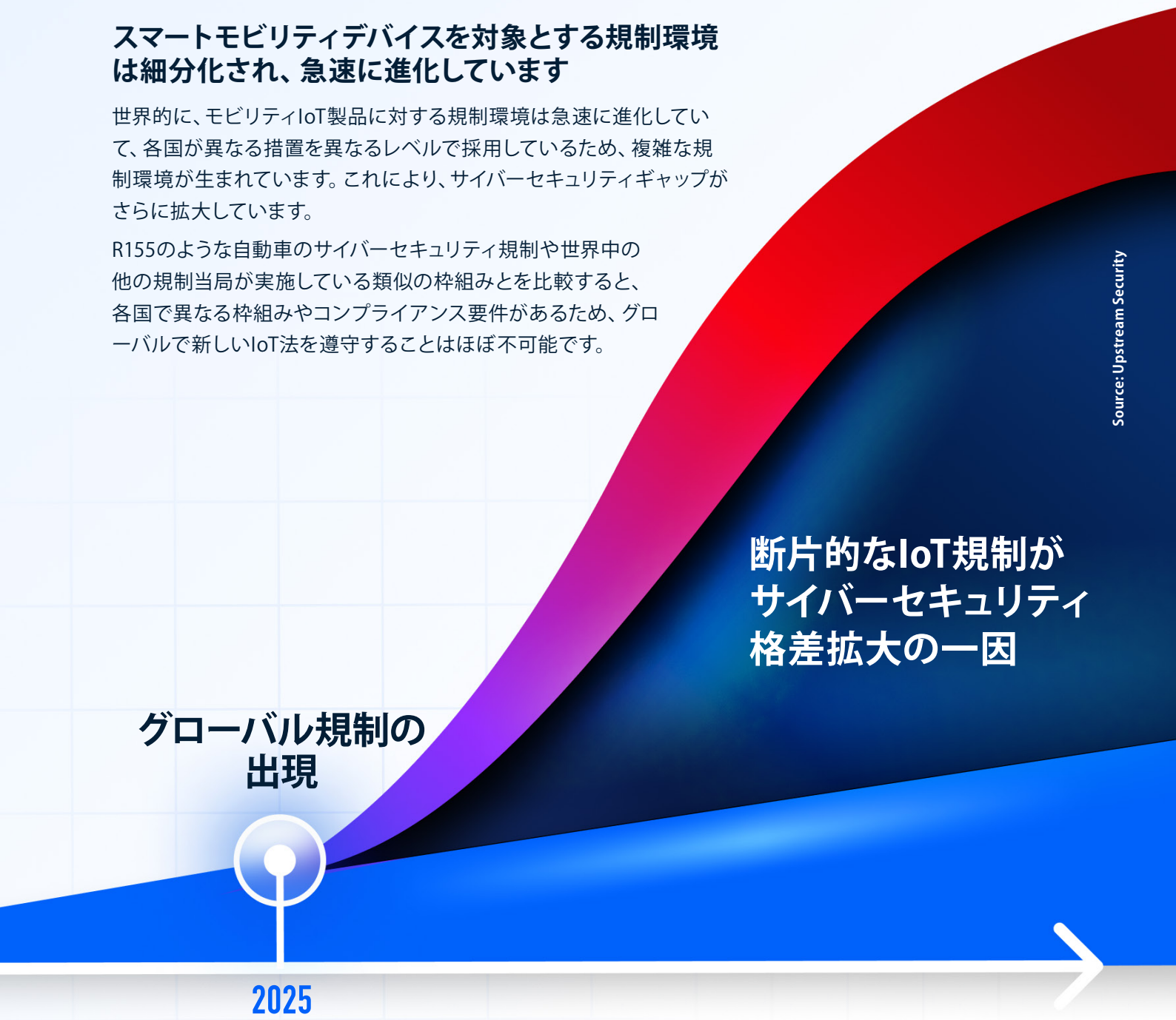
2024年11月、英国を拠点とするテレマティクス企業がサイバー攻撃を受け、多くのサービスが混乱し、多数の顧客の車両追跡機能に影響を及ぼしました。[49] 運用上の混乱だけでなく、この攻撃により会社のネットワーク内での不正な活動を許すこととなりました。 複数の配送業者が、リアルタイムの追跡に問題が生じ、配達に遅延が発生する可能性もあったことに触れ、業務に重大な影響があったと報告しました。 同社は速やかに英国情報コミッショナー事務局を含む関連当局に通報し、サイバーセキュリティの専門家と協力して調査と被害軽減に取り組んでいると発表しました。

これらの調査結果は、スマートモビリティデバイスを重要インフラとして保護する必要性と、そうしないことの意味合いを浮き彫りにしています。

スマートモビリティデバイスを対象とする規制環境は細分化され、急速に進化しています

世界的に、モビリティIoT製品に対する規制環境は急速に進化していて、各国が異なる措置を異なるレベルで採用しているため、複雑な規制環境が生まれています。これにより、サイバーセキュリティギャップがさらに拡大しています。

R155のような自動車のサイバーセキュリティ規制や世界中の他の規制当局が実施している類似の枠組みとを比較すると、各国で異なる枠組みやコンプライアンス要件があるため、グローバルで新しいIoT法を遵守することはほぼ不可能です。



EUでは、2024年10月17日にNIS2指令50が義務化され、重要インフラとエネルギー部門のサイバーセキュリティ基準とレジリエンスの確立に焦点を当てています。 NIS2指令は、EUサイバー連帯法51によってサポートされており、EU内での重大かつ大規模なサイバーセキュリティの脅威や攻撃を検知し、それらに備え、対応するための能力強化を目的としています。 これには、サイバー脅威への対応を連携して確実に行うためのSOCインフラをEU加盟国内に構築するほか、信頼性の高い資格を持つプロバイダーからのインシデント対応サービスで構成される、欧州サイバーセキュリティ予備隊の創設が含まれます。NIS2では、24時間以内の初回報告義務が追加され、併せて72時間後および30日後の報告も義務付けられています。[52]

新たなNIS2指令に従わない企業は、以下のような制裁措置とともに、巨額の行政罰金を科せられる可能性があります。:[53]

- 必須事業体（運輸、金融、エネルギー、水、宇宙、医療、行政、デジタルインフラなどの公私の事業体）ー1,000万ユーロまたは全世界の年間収益の2%のいずれか高い方を上限とする罰金
- 重要事業体（食品、デジタルプロバイダー、化学、郵便サービス、廃棄物管理、研究、製造業などの公私の事業体）ー700万ユーロまたは全世界の年間収益の1.4%のいずれか高い方の罰金
- 経営陣に対する刑事制裁（例：個人的責任）、およびサービス停止命令、遵守命令、拘束力のある指示、セキュリティ監査実施命令、脅威通知指示、厳重監督下での業務遂行などの非金銭的制裁措置。

2024年3月、欧州議会はサイバー・レジリエンス法（CRA）を承認しました。54これは、デジタルコンポーネントを持つすべての製品（ハードウェアとソフトウェアの両方）を対象とする横断的な法律です。[55] CRAは製品のライフサイクル全体をカバーし、製品の企画、設計、開発、および保守を管理するサイバーセキュリティの枠組みを提供します。 CRAはまた、製造業者に対して、積極的に悪用された脆弱性やインシデントを24時間以内に報告し、製品のサポート期間中におけるリスクを効果的に軽減することを要請しています。[56]

英国では、製品セキュリティ・電気通信インフラ法案が施行され、IoTエコシステムに対する大幅な規制変更を表しており、サイバーセキュリティを製品開発とライフサイクル管理に統合するための包括的なアプローチが求められています。[57] この法案は、サイバー脅威から消費者を保護するだけでなく、相互接続されたデバイスを悪用して重要な国家インフラを混乱させる可能性のある大規模な攻撃のリスクを軽減することを目的としています。

米国では、連邦通信委員会（FCC）が消費者向けワイヤレスIoT製品に対する自主的なサイバーセキュリティラベリングプログラムの創設を決議しました。[58]
この制度は、IoTのサイバーセキュリティとラベリングに関して、すでに進行中の官民の取り組みを基に構築されています。証券取引委員会（SEC）は、上場企業によるサイバーセキュリティリスク管理、戦略、ガバナンス、およびインシデント開示に関する規則も採択しました。[59]

2024年2月、国立標準技術研究所（NIST）は広く使用されているサイバーセキュリティフレームワーク（CSF）を更新しました。[60] この新バージョン（2.0版）は国家サイバーセキュリティ戦略の実施をサポートするもので、重要インフラの保護にとどまらず、あらゆる業界のすべての組織に適応範囲が拡大されています。 また、ガバナンスとサプライチェーンのリスク管理に新たに焦点を当て、組織がサイバーセキュリティ戦略に関する意思決定をどのように行い、実施するかを包括しています。 CSFのガバナンスコンポーネントは、サイバーセキュリティが企業リスクの主な要因であり、財務、プライバシー、サプライチェーン、風評、技術的、物理的リスクなどとともに経営陣が考慮すべきであることを強調しています。

スマートモビリティ・デバイスに影響するIoT規制の概要

規制	IoTへの影響	報告義務	発効日	適用範囲
GDPR	個人のプライバシーを保護するための包括的な法的枠組み。最大2000万ユーロまたは全世界の年間売上高の4%までの罰金。	72時間以内	2018年5月	EU加盟国
サイバーセキュリティ法	データ保護とサイバーセキュリティを重視した自主的なリスクベースの認証要件。	過度な遅滞なく、可能な限り72時間以内	2019年6月	EU加盟国
サイバーレジリエンス法	厳格なサイバーセキュリティ要件を含む包括的な法的枠組み。最大1500万ユーロまたは全世界の年間売上高の2.5%までの罰金	24時間以内	2024年10月（2027年に適用開始見込み）	EU加盟国
NIS2指令	強化されたセキュリティ対策と、より厳格な取り締まり措置。最大1000万ユーロまたは全世界の年間売上高の2%までの罰金	24時間以内、追加報告を72時間後及び30日後	2024年10月	EU加盟国
製品セキュリティ及び電気通信インフラ法	製品開発及びライフサイクル管理に対応するサイバーセキュリティ対策の包括的アプローチ	インシデントを速やかに報告	2024年4月	イギリス
NISTサイバーセキュリティフレームワーク 2.0	サイバーセキュリティリスクを管理及び軽減するための包括的フレームワーク（現在、業界範囲の拡大とサプライチェーンリスク管理の要素を含む）	なし	2024年2月	米国
サイバートラストマークラベリング	IoT機器向けの自主的なサイバーセキュリティラベリング制度	なし	2024年末	米国
SECサイバーセキュリティ報告要件	企業に対し、サイバーセキュリティリスク管理戦略に関する詳細な年次報告書提出を義務付ける（ガバナンスの最適な手法やリスク管理における取締役会の役割を含む）	重大なインシデントは4営業日以内（事案の性質、範囲、業務及び財務への影響に関する包括的な内容報告を義務付ける）	2023年12月	米国

Source: Upstream Security

重大なインシデントは4営業日以内（事案の性質、範囲、業務及び財務への影響に関する包括的な内容報告を義務付ける）

ISO/WD 24882は現在策定中の新規格であり、まだ最終承認の段階に至っていません。本規格は農業機械OEMの製造における、電気・電子システム（構成部品とインターフェースを含む）に対するサイバーセキュリティ要件の確立を目的としています。[61] この規格は、農業機械の電気・電子システム全体のライフサイクル（設計構想から廃棄）を対象とし、サイバーセキュリティリスクが適切に管理されることを求めています。

新しい規格では、デバイスの構成部品、指令・制御機能、機密データへのアクセスを保護することの重要性を強調したサイバーセキュリティ要件を規定しています。

- **リスクアセスメント：**OEMは、構想段階及び開発段階において、自社の接続システム及び構成部品に対する包括的なサイバーセキュリティリスクのアセスメントを実施しなければならない。
- **設計・開発**：サイバーセキュリティは、農業機械の設計及び開発プロセスに統合されなければならず、ハードウェア、ソフトウェア、通信インターフェースに関する具体的な要件が定められている。
- **生産・保守：**本規格では、安全な生産及び保守管理の実施を求められ、それにより農業機械のライフサイクル全体を通じてサイバーセキュリティが確実に維持されることが求められている。
- **廃棄：**デバイス寿命の終わりの時でも、OEMは機密データやシステムへの不正アクセスを防ぐため、安全な廃棄手順を検討する必要がある。

R155が幅広いグローバルな規制の枠組みを提供しているのに対し、ISO/WD 24882は農業分野特有の課題に対し、詳細な技術ガイダンスを提供しています。本規格は農業機械の運用環境や農村地域での展開に伴う脅威を考慮しており、これらの環境下では、通信接続が制限され、ソフトウェア更新の頻度が低くなるおそれがあり、不正アクセスや改ざんが深刻な影響を及ぼす可能性があります。

ISO/WD 24882はEUのCRAと整合していますが、その適用範囲をEU域外にも拡大しており、今後、車両カテゴリーT（例：農業機械）、R（例：農業用トレーラー）、S（例：交換式牽引農業機器）にまで拡大される可能性がある、R155の運用にも影響がでるものと予想されています。[62]

サイバーセキュリティの脅威が高まり続ける中、規制や規格も継続的に更新される可能性が高くなります。ISO/WD 24882を早期に採用するOEMは、将来の規制の変更に対して、サイバーセキュリティ要件をさらに強化するR155やCRAの規制改訂に対しても、対応しやすい有利な立場にあるでしょう。

サイバーギャップを埋めるため、製品セキュリティチームに求められる規制要件を超えたセキュリティレジリエンスの拡大

車両セキュリティオペレーションセンター（vSOC）は、R155およびR156の遵守に不可欠な要素であり、OEMがコネクテッドカーをリアルタイムで監視し、脅威に迅速に対応することを可能にします。

> ***2024年7月のR155の第2マイルストーンにより、vSOCが監視する車両の範囲は大幅に拡大し、生産中のすべての新車が対象となりました。これによりOEM各社には、vSOCチーム、プラットフォーム、およびプロセスの調整が求められました。***

vSOCがサイバーレジリエンスに不可欠であるにもかかわらず、そのロードマップの実施において依然として遅れをとっているOEMが多いです。

脅威の状況が絶えず進化し、大規模で影響力の大きな攻撃が主流となる中、サイバーギャップが生じ始めています。そのためサイバーセキュリティチームは規制要件を超えてvSOCを進化させ、セキュリティ態勢を継続的に維持する必要があるのです。

サイバーギャップを埋めるために必要なのは、車両、スマートモビリティデバイス、スマートモビリティシステム、APIのリアルタイム監視です。さらに人材への投資、攻撃検知能力とvSOC実行能力の向上も求められます。

vSOCの進化：コンプライアンスから大規模リスク軽減まで分けられる4つの段階

1.0 R155 & R156コンプライアンス

最初にOEM各社は、明確な枠組みと明確に定められた戦略・範囲を持つ専用のvSOCを構築することで、R155 & R156コンプライアンスを確立します。 さらに、OEMはサイバーセキュリティ管理システム（CSMS）とソフトウェア更新管理システム（SUMS）を実装し、R155に対してサイバーセキュリティフレームワークの包括的な監査を実施して認証を取得する必要があります。 このように、規制要件を満たすことは製品セキュリティチームにとって基本的な作業ですが、それだけではレジリエンスに対する誤った認識と重大なカバレッジギャップを生じる可能性があります。

2.0 修復と自動化

次に、vSOCは、応答活動を構造化し自動化するためのエンドツーエンドのプレイブックを開発・実装します。これにより、カバレッジと自動化機能を継続的に拡大します。さらに、IT サービス管理（ITSM）、セキュリティ情報イベント管理（SIEM）、拡張検知と対応（XDR）、セキュリティオーケストレーション・自動化・対応（SOAR）などの他の企業ITシステムとvSOCを統合し、組織全体の可視性と効果的な是正措置を確保します。

この段階では、vSOCはより一層データドリブン型になることに重点を置いています。vSOCチームは、検出と調査の段階で可能な限り多くのデータフィードを統合し、自動車に特化したサイバーセキュリティ分析を活用して、脅威や異常をほぼリアルタイムまたはリアルタイムで検出します。

3.0 生成AI搭載のvSOC

現代のvSOCは、複数ソースからの膨大なデータ、動的なSBOM、そしてグローバルサプライチェーンのリスクに対処しています。生成AIは、可視性の向上、調査の効率化、そして長期的なvSOCの効率性を支援する上で重要な役割を果たしています。

生成AIが搭載されたvSOCは比類のない効率性をもたらし、サイバーセキュリティチームがデータドリブン型の検出機能とvSOCの実行機能を拡張できるようにします。サイバーセキュリティチームは、大量のコネクテッドカーおよびモビリティデータの迅速な分析、パターンの検出、インシデントアラートのフィルタリング、調査の自動化、強化されたTARA（脅威分析とリスク評価）の実施により、大規模なリスクに対処することが可能となります。

4.0 スマートモビリティデバイスと自律技術

最終的に、vSOCは真に分野横断的な機能を持つようになり、自動運転車、モビリティアプリケーション、OT、およびスマートモビリティデバイスにまで範囲が拡大されます。これにより、製造後段階において車両、インフラ、および顧客を保護することができるのです。

vSOCの進化

コンプライアンスから大規模リスク軽減へ

Source: Upstream Security

製品のサイバーセキュリティギャップの評価と最小化

Upstreamは製品のサイバーセキュリティ態勢を評価し、潜在的な脆弱性を特定するための独自の方法論を開発しました。 自動車サイバーセキュリティ・クアドラントは、現在のサイバーセキュリティの状況を把握し、最適なセキュリティ成果を達成します。コネクテッドカーのデータを効果的に活用するために、改善点を特定する戦略的な仕組みです。

自動車サイバーセキュリティ・クアドラントでの組織の位置づけは、データドリブン型検出とvSOC（仮想セキュリティオペレーションセンター）実行に関する一連の基準に基づいて、評価することで決定されます。

データドリブン型検出は、顧客がコネクテッドカーから収集したデータをどれだけ効果的に使用しているかを表しています。 基準には、データのカバレッジ、多様性、品質、鮮度、豊富さが含まれます。 データドリブン型検出が高い場合、顧客はサイバーセキュリティ戦略をサポートするためにデータをより効率的に使用し、セキュリティ体制の強化や新たなビジネスチャンスの創出が可能となります。

vSOC実行は、顧客が導入しているvSOC運用とワークフローの指標です。 評価基準には、準備、予測、監視、検出、対応の各能力が含まれます。 vSOC の実行度が高いほど、車両セキュリティ オペレーション センターの機能がより包括的かつ成熟した形で示され、コネクテッドカーのサイバーセキュリティ保護が強化されている事を示しています。

4種類の組織がカテゴリーに表示されています：

データドリブン型サイバーセキュリティリーダー（右上）：このカテゴリーの組織は、データ活用とvSOCの実行の両方に優れており、vSOCの進化においてvSOC 4.0の段階まで進んでいます。 コネクテッドカーとデバイスのデータを効果的に使用し、堅牢なvSOCを展開しており、サイバーセキュリティの検出と調査が強化されています。 これらの組織は、コネクテッドカーのサイバーセキュリティに高い基準を設定する業界のリーダーとしての役割を果たしています。

データ重視型プレイヤー（左上）：このカテゴリーに属する組織は、データ活用度は高いものの、vSOCの実行が限定的（vSOC 1.0-2.0）で、スマートモビリティデバイスや自動運転システムのデータフィードまでカバーするには至っていません。コネクテッドカーから膨大なデータを取得していますが、サイバーセキュリティ保護を最大限に高めるために vSOC 機能を十分に活用していない可能性があります。 これらの組織は、vSOCの統合を強化する事で、データをより有効的に活用し、セキュリティを向上させることができます。

vSOC のパイオニア（右下）：このカテゴリーに属する組織は、データ活用度は低いものの、目的に応じたワークフローと自動化（vSOC 2.0-3.0）を導入することで、vSOCの実行を向上させ、発展を遂げています。コネクテッドカーのデータはそれほど多くないかもしれませんが、効果的なvSOCの手法とプロセスにより、基本的なレベルのサイバーセキュリティ保護を維持しています。 これらの組織は、データ活用度を高めることで、サイバーセキュリティ態勢をさらに強化することができます。

サイバーセキュリティの新たな導入者（左下）: このカテゴリーに属する組織は、コンプライアンス要件に重点を置いており、データ活用度が低く、vSOC の実行が制限されています（vSOC 1.0）。製品のサイバーセキュリティに関するベストプラクティスを導入する初期段階にあり、データ使用量を増やし、より包括的なvSOCの導入によって、サイバーセキュリティを向上させる可能性があります。これらの組織は業界のリーダーから学び、データドリブン型のサイバーセキュリティアプローチの改善に取り組むことができます。

サイバーセキュリティのギャップを埋めるために、ステークホルダーは以下を含むデータドリブン型の検出能力とvSOC実行能力を拡張する必要があります:

- モニタリングの範囲 — 車両、スマートモビリティアプリケーション、API、スマートモビリティデバイスなど、接続されているすべての資産にモニタリングを拡張します。
- 高度なML（機械学習）ベースのモジュール — 高度なAI/MLモデルを適用し、複雑な低速・長期的な攻撃を含む未知の脅威や攻撃を効果的に検出します。
- 脆弱性管理 — 単一のECUや接続デバイスから完全な車両モデルまで、製品やコンポーネントを分析します。
- 強化されたTARA — ディープウェブとダークウェブのCTIデータおよび詳細なTARAに基づいて、複雑な洞察を生成します。
- GenAIが搭載されたvSOC — vSOCの運用を変革し、比類のない効率を実現します。

02.

避けては通れない重大な議題

中国は、その膨大な製造上の優位性、新エネルギー車（NEV）技術への戦略的投資、そして広範な政府支援を活用することで、自動車エコシステムの主要な勢力となり、世界市場とサイバーセキュリティの状況を再形成しています。

中国の戦略的投資と政府支援が自動車産業を再形成

中国は、過去10年間、「中国製造2025」（MIC 2025）計画を採用し実施してきました。この計画は2015年に開始され、10年に渡る包括的な青写真となっています。MIC 2025は、中国が外国技術への依存を減らすこと、中国のハイテクメーカーが世界市場へ促進することを目的に策定されました。

この計画は、中国を先進的な製造業のリーダーに変革することを目的としており、10の戦略的産業での技術革新を目指すものでした。その分野とは、電気自動車、情報技術、通信、人工知能、先端ロボット工学、農業技術、航空宇宙工学、海事工学、バイオ医学、そして鉄道インフラです。

2020年初頭までには、MIC 2025に関連する約1,800の政府系基金（GGF）が1.5兆ドルという資本目標を登録し、そのうち6,270億ドルを調達していました。 多くの場合、GGF（政府系基金）は、資金を提供する企業の株式を取得したり取締役会の地位を得たりし、その結果、企業の意思決定に影響を与えることができます。[63]

MIC 2025は、国家の力を利用して、経済競争力に不可欠な産業において世界的に力を及ぼすようになりました。[64]

MIC 2025は、この目標を達成するために次のような段階的なプロセスを採用しました：

1. 研究開発（R&D）の地域化と国産化（例：現地で開発または取得した外国技術、知的財産、ブランド）およびグローバルサプライチェーンセグメントの管理（例：垂直統合）；
2. 戦略的な必要性として、外国技術を自国技術に置き換えること；
3. MIC 2025の産業および技術分野に至るまで、世界市場シェアの獲得をする

中国はまた、自国の法的および規制制度（例：税金、貿易制限、基準、強制的な合弁事業、知的財産権の移転、調達政策など）を利用して、MIC 2025の対象分野で、外国企業よりも国内企業を優遇しました。 この計画では、国内企業が達成すべき明確な売上成長率と市場シェアの目標を設定するところにまで踏み込んでいます。

優先的な資本へのアクセスにより、国内企業は自国の研究開発および製造能力を発展させることができました。また、新しい製造技術を進歩させ、サプライチェーンの管理と垂直統合を行いました。そして、外国の技術を取得し、競争力をを高めることができました。

> ***10年が経ち、中国は世界の自動車産業で主要な勢力となり、他国に比べて製造上の優位性を確保しています。***

OEM（相手先ブランド製造会社）は、これまでにない強力で、意欲的で、技術的に進んだ競争相手に直面している：[65]

- 2023年の生産規模は ***3,000万台*** 以上
- 2023年の生産能力は ***4,800万台*** 以上
- コストの優位性は ***25%〜30%***
- 市場投入までの時間性は ***50%*** 短縮
- 政府の補助金が ***400%〜500%*** 増加
- 世界のEVバッテリー生産の ***76%***
- **サプライチェーンの管理と垂直統合**

Source: Upstream Security

中国で操業している世界的なOEMは、中国の製造上の優位性を十分認識しています。例えば、テスラは世界の生産量の半分を上海のギガファクトリーで生産しています。[66]

中国のMIC 2025が新エネルギー車のリーダーシップを推進

中国は現在、新エネルギー車（NEV）の世界最大の市場となっています。NEVには、バッテリー電気自動車（BEV）、プラグインハイブリッド車（PHEV）、および（水素を動力源とする）燃料電池車があります。

最新の公式データによると、2024年上半期、中国のNEVの新規登録台数は、前年同期比で約40%急増し、過去最高を記録しました。

同時期にNEV（新エネルギー車）のインフラも急速に拡大し、NEV充電器の数は前年比54%増の1,020万台で、そのうち310万台は公共充電施設でした。 2024年6月時点で、中国には合計2,470万台のNEVが登録されており、総自動車保有台数の7.2%を占めています。BEV（バッテリー電気自動車）の数は1,810万台を超え、NEVの73.3%を占めています。[67]

中国の自動車ウェブサイトAutoHomeによると、2024年9月時点で、テスラのモデルYは依然として中国で最も売れている電気自動車でした。中国のNEVメーカーBYDのシーガルは僅差で2位となりました。[68]

そして2024年10月、BYDの世界四半期売上高が初めてテスラを上回り、中国のOEMメーカーの目覚ましい躍進を象徴することとなりました。[69]

MIC 2025が自動車規制の状況を一変させる

2024年1月、中国工業情報化部（MIIT）は自動車チップの規格の確立を加速させるため抜本的な計画を発表しました。 「国内自動車チップ規格策定のガイドライン」としてよく知られるこの計画には、2025年までに実施される30を超える重要な規格と、2030年までに実施される70を超える規格があります。[70] この規格は、信頼性、環境、電磁両立性、機能安全、情報セキュリティに関する基本的な要件を明確にすることに重点を置いており、国際的な競争が激化する中、重要な製品の研究開発をさらに加速させようとしています。[71]

さらに、2024年に中国の自動車規制は大きく前進し、インテリジェントネットワーク車両のための新たなサイバーセキュリティ規格、衝突に関する安全要件と試験方法が導入されました。また、世界の自動車産業の規格開発プロセスにおいて重要な役割を果たすための計画も立てられました。

2024年5月、国家標準化管理委員会（SAC）は、乗用車の追突事故時の安全要件と試験方法（GB 20072—202X）、および側面衝突時の乗員保護（GB 20071—202X）に関するガイドラインと仕様を定めた、新しいGB規格（中国国家規格）を導入しました。[72] この新しい規格は2006年版に代わるもので、2026年7月に発効する予定です。[73]

2024年6月、中国工業情報化部（MIIT）は、NEVとインテリジェントコネクテッドカーに重点を置いた、世界の自動車業界向けの新規格策定計画を発表しました。 中国は、燃料電池自動車、電磁両立性、自動車用レーダーなど、約20の国際規格の開発を主導していくことになります。 さらには、電気自動車（EV）の性能試験方法と衝突安全性の用語について少なくとも3つの新しい国際規格を開発し、1つまたは2つの国際規格作業部会を設立することを目指しています。 中国はまた、自動運転システムの世界的な技術規制の開発に重点を置き、電気自動車（EV）の最大出力測定方法と電池耐久性の第二段階に関する規制の策定を急いでいます。[74]

2024年8月、MIITは中国のインテリジェントネットワーク車両に関して、中国初となる強制的な国家規格を発表し、2026年1月1日から施行する予定です。[75]

GB 44495-2024	自動車の情報セキュリティに関する技術要件では、自動車情報セキュリティの管理システムの要件、および外部接続セキュリティ、通信セキュリティ、ソフトウェアアップグレードセキュリティ、データセキュリティなどの技術要件と試験方法を規定しています。
GB 44496-2024	自動車ソフトウェアアップグレードの一般技術要件では、自動車ソフトウェアアップグレードの管理システム要件、およびユーザー通知、バージョン番号の読み取り、安全保護、前提条件、電力保証、障害処理などの車両ソフトウェアアップグレード機能に関する技術要件と試験方法を規定しています。
GB 44497-2024	インテリジェントネットワーク車両自動運転データ記録システムでは、データ記録、データ保存と読み取り、情報セキュリティ、衝突耐性性能、環境評価などの観点から、インテリジェントネットワーク車両の自動運転データ記録システムの技術要件と試験方法を規定しています。

中国で事業を展開するグローバルOEMは、2026年の節目に備え、新しい中国の国家規格と現在の国際規格との差異を分析する必要があります。

全体的に、GB 44495-2024は、自動車サイバーセキュリティ管理システムに関する国際規格UNECE WP.29 R155およびISO/SAE 21434の要件と多くの原則を共有しています。しかし、そこには市場固有の詳細な技術要件も導入されています。[76]

さらに、GB 44495-2024 では ISO/SAE 21434 と同様に、リスク管理の重要性が強調されています。これには、新たな脅威が発生しても車両の安全性を確保するために、継続的な監視やリスク評価、および対応措置が求められています。

どちらの規格も車両のサイバーセキュリティを強化することを目的としていますが、いくつかの重要な点で異なります：

	GB 44495-2024	R155
対象範囲	M（乗用車）、N（商用車）、およびO（トレーラー、セミトレーラーを含む）の車両タイプにのみ適用されます。	L6とL7が含まれ、全てのカテゴリーL車両に拡大される予定です。
特異性	詳細な技術要件と試験方法を提供しています。	より広範な枠組みとリスクカテゴリ（別紙5参照）を提供し、製造業者に実施における柔軟性を与えています。
試験要件	メーカーが実施する必要がある 27 の具体的なサイバーセキュリティ 試験を列挙しています。これには、車両サイバーセキュリティに関するさまざまな側面が網羅されています。：外部接続、通信システム、ソフトウェアの更新、データセキュリティ、アクセス制御、サービス拒否(DoS)からの保護などです。	サイバーセキュリティ試験の必要性を強調していますが、具体的な試験方法を規定してはいません。
認証	証明書の発行や更新は不要ですが、監査は必要です。	定期的な更新と共に正式な認証プロセスが必要です。

Source: Upstream Security

中国のNEV産業の急速な成長は、サイバーセキュリティリスクの増大を伴う

急成長を遂げる中国のNEV産業において、サイバーセキュリティのリスクが高まっています。 脅威アクターは、ランサムウェアやデータ流出攻撃を用いて、中国のNEVメーカーやサプライヤーを標的とするケースが増加しています。 また、セキュリティ研究者たちは、中国のNEVに搭載されたテレマティクスシステム、インフォテインメントシステム、OEMアプリなどに重大な脆弱性も発見しています。 中国のTier-1およびTier-2サプライヤーを巻き込むサイバーインシデントが多発しており、グローバルなサプライチェーンへの懸念が高まっています。

2024年3月、中国の自動車用電子部品のTier-2サプライヤーが、データ流出と恐喝を目的とするグループの攻撃を受けました。 今回のセキュリティ侵害により1.2TBのデータが流出し、中国および世界中のOEMに影響を及ぼしました。流出したデータには、個人情報、顧客データ、ソースコード、SQLデータベース、そして添付ファイル付きの社内外の電子メールのやり取りが含まれています。[77]

2024年5月、セキュリティ研究者たちは、中国のEVメーカーのテレマティクスシステムに重大な脆弱性を発見しました。この脆弱性は、無線アクセスネットワーク(RAN)攻撃によって生じたものです。 攻撃により、GPS機能が損なわれ、さらに車両のネットワーク接続や関連するFMS(フリート管理システム)の機能にも障害が生じました。その結果、車両の追跡や位置特定が不可能となり、エンジンの始動や停止といった基本的な機能も、車両が手動で再起動されるまで操作できなくなりました。[78]

2024年6月、サーモスタットと温度センサーを専門とする中国の自動車Tier-1サプライヤーがランサムウェア攻撃を受け、その結果、300GBを超える機密データが流出しました。 このセキュリティ侵害により、同社の業務運営の信頼性が損なわれ、オンライン活動に支障が生じ、さらにウェブサイトにも直接の影響を及ぼしました。盗まれたデータには、機密文書、財務記録、そして個人情報が含まれていました。[79]

2024年8月、セキュリティ研究者たちは、保護されていないデータベースを発見しました。その中には、中国の車両所有者の75万人以上の機密情報がありました。 アメリカを拠点とするIPアドレス上でホスティングされたデータベースでは、氏名、ID番号、電話番号、住所、車両識別番号(VIN)、車種などの情報を公開しており、その結果、個人をなりすましや車両関連犯罪のリスクにさらすこととなりました。 データベースは48時間後にロックダウンされましたが、データベースの所有者は依然として不明のままです。 セキュリティ研究者たちは、組み合わせたデータが正規の組織ではなく、サイバー犯罪者によって収集された可能性があると指摘しています。[80]

2024年9月、自動車用CANバスプロトコルソリューションを専門とする中国のTier-1サプライヤーが、ハクティビストグループによる中国企業に対する作戦の一環として標的にされました。

ハクティビストグループは、同社の公式ウェブサイトのサーバーを攻撃し、停止させたと主張しています。同グループの主張について、独立した検証はなされておらず、同社も攻撃の規模についてはコメントしていません。[81]

2024年9月、中国のセキュリティ研究者たちは、プロトコルレベルでPhoneKeyシステムと車両間の情報を中継するBluetooth Low Energy(BLE)リレー攻撃を実演しました。 プロトコルベースのリレー攻撃は、被害者(車両所有者)が世界のどこにいてもよく、車両と物理的に近くにいる必要がないという利点があります。[82]

Phone-as-a-Key(PAAK、スマホキー)システムを搭載した車両の所有者は、認証済みのスマートフォンを利用して、一定の近い範囲内で車両のロック解除や各種の操作が可能ですスマホキーは、認証機構としてチャレンジ・レスポンス方式を採用しているものの、BLEリンク層でのペアリングや暗号化を有効にしていません。そのため、2017年に発表されたBLEデバイス向けの中間者攻撃および解析ツールであるGattackerにとって格好の標的となっています。研究者たちは、中国およびアメリカのEV OEMの人気モデルに対する攻撃に成功しました。標的となったのは、BLEリンク層のペアリングや暗号化が実装されていない車両でした。初期ペアリング段階でPINコードを必須入力にしていた車両には、脆弱性はありませんでした。 研究者たちは、それぞれのOEMに調査結果を報告しました。

2024年9月、あるセキュリティ研究者が、車載インフォテインメントシステムで使用されるBluetoothチップセットの脆弱性(Braktooth)を悪用した事例を示す論文を発表しました。脆弱性(Braktooth)は、多くのメーカーの様々なBluetoothチップセットに存在し、攻撃者が標的デバイスのBluetoothリソースを枯渇させることを可能にします。 攻撃者は、標的のチップセットに接続された他のBluetoothデバイスの動作を妨害したり、クラッシュさせたりすることができます。研究は、2021年の古い解析に基づいていましたが、最近のテストでは中国の人気車種の多くが、Braktooth攻撃に対して脆弱であることが明らかになりました。[83]

これらのインシデントは、中国のOEMが急速に国際市場へ進出することに伴うリスクの増大を浮き彫りにしています。アメリカやEUなど注目度の高い市場において重大な脆弱性が露呈したことで、規制当局による監視が強化され、市場での受け入れ障壁が高くなる結果となっています。

中国のNEVの成長とサイバーセキュリティへの懸念に対する国際的な対応—大幅な関税引き上げと技術使用禁止措置

中国のNEV部門の急速な成長により、国際的な技術発展に対する懸念と、コネクテッドカー、自動運転、電気自動車、バッテリー、EV充電インフラなどのサイバーセキュリティの耐性の強度に対して懸念が高まっています。

2024年2月、中国は、自国のEVメーカーに対する国際的な貿易制限を救済するために、海外サプライチェーンの構築を支援することを表明しました。これは、自国の業界の大規模なグローバル展開への取り組みの一環です。 この公約は、中国の急成長しているEVの輸出が、欧州や米国を含む一部の地域において、保護貿易主義的な反発の高まりに直面していることを受けて行われました。[84]

> ***2024年9月、米国商務省は、中国またはロシアと密接な関与がある特定のハードウェアおよびソフトウェアを搭載したコネクテッドカー、あるいはそれらの部品の個別販売または輸入を禁止する規則制定案告知を発表しました。[85]***

この規則では、車両接続システム（VCS）に搭載されているハードウェアとソフトウェア、および自動運転システム（ADS）に搭載されているソフトウェアに焦点を当てており、これらは米国の重要インフラ、国家安全保障、およびドライバーの安全面に過度のリスクをもたらすとされています。 計画されている規則においては、中国製の車両の米国市場への参入を事実上禁止するだけでなく、OEMで米国で販売される車両から中国製のソフトウェアとハードウェアを取り外すことも強制することになります。

提案された規則は、中国製の車両、ソフトウェア、および部品に対する現行の米国規制を大幅に強化するものです。 禁止措置については、ソフトウェアは2027年製モデルから、ハードウェアは2030年製モデルから、また製造年不明の製品については2029年1月1日から適用されます。[86]

米国の行動に触発され、欧州当局も中国の自動車技術がもたらすサイバーセキュリティ、スパイ活動、破壊活動などの潜在的なリスクに対する米国政府の懸念に同調しています。[87] 欧州当局では、情報通信技術（ICT）サプライチェーンツールボックス（拘束力なし）の草案を作成しています。これはEUの数か国においては、中国の通信事業者の使用禁止、使用制限、または段階的に廃止するきっかけとなった5Gセキュリティツールボックス[88]に類似した枠組みです。

EUによる中国のソフトウェアサプライヤーへの監視強化は、特に中国サプライヤーを多数抱えるOEMは経営戦略を適応させる必要があることを意味しています。 さらに、米国の禁止措置は欧州のOEMに直接影響を与え、米国で販売される車両のサプライチェーンの調整が余儀なくされるでしょう。

> ***2024年10月初旬、EUが中国製EVへの課税を今後5年間で10%から最大45%に引き上げるという劇的な発表は、中国に積極的に進出している欧州の自動車メーカーに対して中国政府の決定がどのような影響を与えるのかという疑問を提起しました。[89]***

2024年10月末までにEUの新しい関税規則が施行された場合には、中国は自国の自動車メーカーに対して、中国製の電気自動車への追加関税を支持する欧州諸国に対して行っている巨額の投資は停止するよう指示したと、ロイター通信は報じました。[90]

03.

自動車のサイバーセキュリティの傾向

2024年、前例のない影響を持つランサムウェア攻撃が支配的となり、SDV及び自動運転技術がサイバーセキュリティリスクを劇的に変化させ、車両システムの操作と制御に関連するインシデントが3倍以上に増加

インシデントのレビュー

2024年、サイバーセキュリティ攻撃の規模と影響が拡大し、自動車産業とスマートモビリティ産業に新たな課題をもたらしました。

2024年中、Upstreamの AutoThreat® の研究者は、自動車とスマートモビリティのサイバーセキュリティインシデント409件を分析しました。これは月平均34件に相当します。

2024年の主なインシデント：

○ ホワイトハット　● ブラックハット

1月

○ セキュリティ研究者が、ドイツのOEMサブドメインの一部にリダイレクトの脆弱性を発見しました。[91]

● 世界最大級の半導体メーカーの1つがランサムウェア攻撃を受け、ウェブサイトが停止し、5TBの機密データが流出しました。[92]

○ セキュリティ研究者が、韓国のOEMにおいて顧客の個人情報（PII）が漏洩する脆弱性を発見しました。[93]

2月

○ セキュリティ研究者が、機密データの大規模な漏洩につながったドイツのOEMクラウドの設定ミスを発見しました。[94]

● 韓国のOEMが大規模なサイバー攻撃を受け、3TBの企業データが流出しました。[95]

● リトアニアのEV充電システムに対するサイバー攻撃により、数時間にわたって業務が停止し、攻撃者は20,000人の顧客のデータを盗み出しました。[96]

3月

○ コロラド州立大学のセキュリティ研究者が、BluetoothまたはWi-Fi接続を介してELDにアクセスし、トラックを制御したり、データを操作したり、マルウェアを拡散する方法を示しました。[97]

● 中国のTier2サプライヤーがランサムウェア攻撃を受け、1.2TBのデータに重大な侵害が発生し、世界のOEMに影響を及ぼしました。[98]

○ セキュリティ研究者が、米国の電気自動車充電設備（EVSE）の50万件以上の個人情報（PII）とビジネス記録を含む、保護されていない585GBのデータベースを発見しました。[99]

4月

● 英国とアイルランドの30万人以上のタクシー乗客の個人情報（PII）が、アイルランドのスマートモビリティプロバイダーが所有する保護されていないデータベースで発見されました。[100]

● 中国のハッカーが、ドイツの大手OEMグループを標的に、技術的な知識を盗むための長期にわたるサイバースパイ活動を行いました。[101]

○ セキュリティ研究者らが、電動スクーター利用者の安全性とプライバシーを脅かす可能性のある、重大なCAN BUS注入脆弱性を発見しました。[102]

5月

○ セキュリティ研究者が、中国のOEMテレマティクスシステムに重大な脆弱性を発見し、GPS機能が危険にさらされていることが判明しました。[103]

● 欧州の著名な車両追跡および車両管理機器プロバイダーがサイバー攻撃を受け、データ侵害が発生しました。[104]

● 欧州の非営利シェアードモビリティプロバイダーが深刻なサイバー攻撃を受け、全プラットフォームでサービスが中断されました。[105]

6月

○ セキュリティ研究者が、インドのOEMの自動車管理アプリケーションに影響を与える脆弱性を発見しました。[106]

○ セキュリティ研究者が、インフォテインメント、ADAS、および自動運転システムで使用される人気の車両ソフトウェア開発プラットフォームに深刻な脆弱性があることを特定しました。[107]

● 米国の主要な自動車ディーラー管理ソフトウェアプロバイダーに対するランサムウェア攻撃により、15,000のディーラーの業務が約3週間停止し、[108] 推定10億2,000万ドルの損失が発生しました。[109]

7月

- セキュリティ研究者が、不正アクセスや運用の妨害を可能にするEV充電ステーションの脆弱性を特定しました。[110]
- セキュリティ研究者が、ノルウェーの交通制御装置にあるウェブベースのUI内に脆弱性を発見し、交通制御装置を完全に制御できるようになりました。[111]
- ドイツのOEMの香港支社が、顧客の機密個人情報（PII）を侵害するサイバー攻撃を受けたとされています。[112]

8月

- セキュリティ研究者が、大手自動車メーカーのインフォテインメントシステムに組み込まれたAndroidベースのOSに重大な脆弱性があることを特定しました。[113]
- 韓国の自動車サプライヤーがランサムウェア攻撃を受け、2.3TBのデータが侵害されました。[114]
- セキュリティ研究者が、公共交通システムで広く使用されているMIFARE技術にハードウェアバックドアを発見しました。[115]

9月

- セキュリティ研究者が、自動運転システムのインターネット制御メッセージプロトコル(ICMP)に重大な脆弱性を発見し、これによりフラッド攻撃を引き起こす可能性があることが判明しました。[116]
- セキュリティ研究者が、さまざまなOEMの複数のインフォテインメントシステムに影響を与えるクラッシュやリモートコード実行につながる可能性があるBraktoothの脆弱性を実証しました。[117]
- セキュリティ研究者が、韓国のOEMのディーラーAPIにおいて主要なAPIの脆弱性を明らかにし、これによりナンバープレートだけで車両を制御できることが判明しました。[118]

10月

- セキュリティ研究者が、オランダの交通信号プリエンプションシステムに重大な脆弱性を発見し、その結果、数千の信号機が交換されました。[119]
- ランサムウェアグループが、ドイツのOEMグループから内部文書、財務記録、個人情報を盗んだと主張しました。[120]
- セキュリティ研究者が、米国のEV OEMが使用するVCSEC ECU(イモビライザーユニット)に脆弱性があり、制御の侵害につながる可能性があることを特定しました。[121]

11月

- 英国を拠点とするテレマティクスプロバイダがサイバー攻撃を受け、業務が中断し、複数の海外のクライアントに影響を与える可能性のあるデータ盗難が発生しました。[122]
- セキュリティ研究者が、日本のOEMインフォテインメントシステムに6つの重大なゼロデイ脆弱性を検出しました。[123]
- 複数の充電ポイントオペレーター（CPO）に影響を与えたデータ侵害により、11万6千人以上の消費者の個人情報（PII）と電気自動車充電設備（EVSE）からのOCPPデータがディープウェブのハッキングフォーラムで流出しました。[124]

12月

- セキュリティ研究者が、ドイツのOEMのインフォテインメントシステムに影響を与える複数の脆弱性を検出しました。[125]
- セキュリティ研究者が、中国のOEMのインフォテインメントシステムでデータ盗難につながる可能性のある複数の脆弱性を発見しました。[126]
- サイバー攻撃により、カナダにおける世界的な自動車部品サプライヤーの事業運営が混乱させられています。[127]

ブラックハットによる攻撃は、常にホワイトハットによる攻撃を上回る

テクノロジーとサイバーセキュリティ対策が進化するにつれて、脅威アクターも進化しており、ステークホルダーは誰が攻撃を実行しているかについて、深く把握する必要があります。
ハッカーは、その意図、行動、悪意によってブラックハット、ホワイトハット、またはグレーハットに分類されます。

ブラックハット

ブラックハットハッカーは、個人的な利益、金銭的な利益、または悪意のある目的のためにシステムを攻撃します。 今日のブラックハットハッカーは、もはや単独のマルウェア開発者ではありません。彼らは組織化され、充分な資金を持つ犯罪集団の一員であることが多く、世界中に数千人のサイバー犯罪者を雇用しており、複数の組織に対して同時に協調的な攻撃を行う能力を持っています。

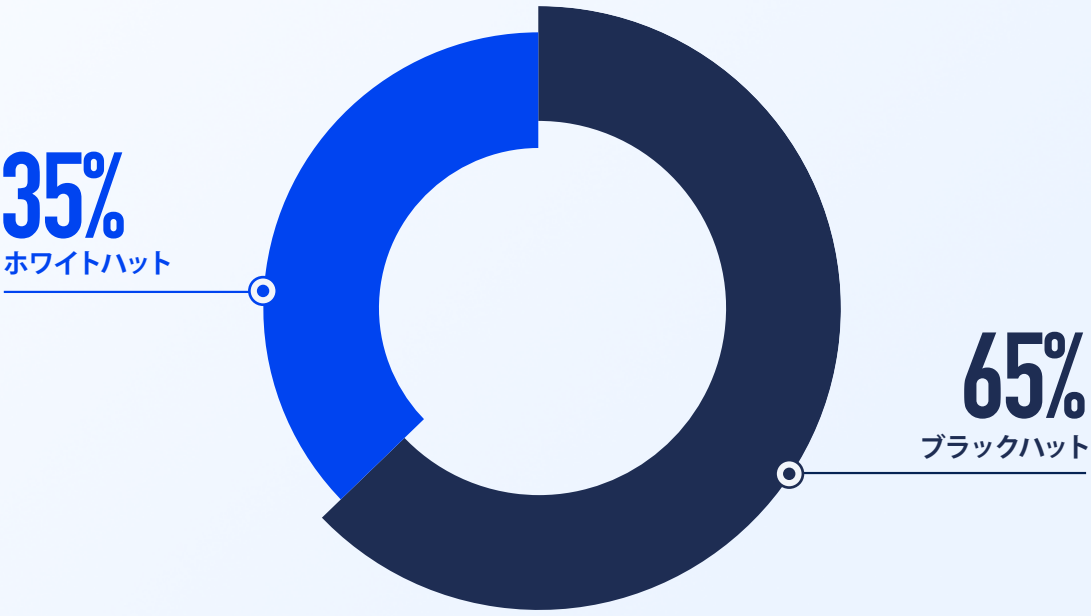
ホワイトハット

対照的に、ホワイトハットハッカーは、多くの場合、悪意のない研究者であり、セキュリティの検証や脆弱性を評価をするために、システムへの侵入や操作を試みます。 ホワイトハットハッカーは継続的に新しい、そして懸念すべき脆弱性を発見しています。 彼らは独立して活動するか、自社のサービスを利用する企業を通じてか、または責任を持って脆弱性を開示することで報酬を得る、バグ報奨金プログラムの一環として活動しています。

グレーハット

グレーハットハッカーは、一般的なホワイトハットアッタッカーグループの一部であり、倫理的な活動と悪意のある活動の境目がはっきりしない、常に変化する状況を生み出しています。 これらのハッカーは、脆弱性の発見と、場合によってはその悪用の両方に貢献しています。グレーハットハッカーは、責任ある情報開示から、金銭的報酬や評価といった利他的ではない動機まで、さまざまな目的によって行動します。また、彼らの活動は、明確な許可なしに行われる作業に関して、倫理的および法的な問題を引き起こすことがよくあります。

2024年、ブラックハットハッカーが全攻撃の65%以上を実行



Source: Upstream Security

IT業界へのブラックハット攻撃と自動車業界へのブラックハット攻撃では、その結果と影響が大きく異なります。 悪意のある自動車業界へのブラックハット攻撃は、IoTや医療、エネルギー、政府施設などの重要インフラに対するサイバー攻撃と密接に関連しており、サービスの中断や経済的損失だけでなく、潜在的な安全上のリスクや人命の喪失につながる可能性もあります。

2024年2月、韓国のOEMの欧州部門が、ランサムウェア攻撃を受け、業務に支障をきたしました。攻撃者は3TBのデータを流出させたと主張し、盗んだフォルダ画像を公開しました。OEMは攻撃を認め、当局と協力してインシデントの復旧および調査を行いました。[128]

2024年6月、15,000のディーラーが使用している、米国を拠点とする、大手ディーラーシップ管理ソフトウェアプロバイダーへのランサムウェア攻撃により、米国全土のディーラー業務が、約3週間にわたって停止しました。複数の情報源を引用したCNNの報道によると、同社は復旧を早め、停止を終わらせるために、2500万ドルの身代金を支払った可能性が高いとのことです。[129] アンダーソン・エコノミック・グループ（AEG）は、フランチャイズ自動車ディーラーへの直接的な損失総額が、10億2000万ドルに達したと推定しました。[130]

2024年11月、英国を拠点とするテレマティクス企業がサイバー攻撃を受け、重要な運用サービスと複数の国際的な車両フリートに影響を与えました。[131] この攻撃により、フリート運営者がフリート管理データにアクセスできなくなり、さまざまな業界の大手小売業者への業務の混乱と配送遅延を引き起こしました。 このインシデントを受け、同社は当局に通報し、サービスの復旧作業を開始しました。[132]

また2024年11月には、著名な脅威アクターが、複数のグローバルCPOから約116,000件の機密データを流出させました。[133] 当初はアメリカのEV OEM充電ネットワークからのデータ漏洩と主張されていたこのデータ侵害は、その後、世界中のさまざまな充電ステーションからのデータを含むことが判明し、被害はUAE、オーストラリア、メキシコ、プエルトリコ、ガイアナ、サウジアラビア、オマーン、インドにまで及びました。

これらの攻撃は、サービスの中断や経済的損失だけでなく、特に重要インフラ分野においては、潜在的な安全上のリスクや人命の喪失につながる可能性があります。ブラックハットによるこれらの多くのインシデントは、消費者は潜在的なリスクに気付かないままであり、その結果、サイバーセキュリティチームの課題水準を高めています。 これらの攻撃の巧妙化と頻度の増加は、ブラックハットハッカーによるリスクを軽減するために、堅牢なサイバーセキュリティ対策と積極的な脅威インテリジェンスが必要となります。

ほぼ全ての攻撃はリモートで実行

自動車サイバー攻撃のほとんどは、主に2つのカテゴリーに分類できます。1つは短距離攻撃 (中間者攻撃など) または遠距離攻撃 (API ベースの攻撃など) であるリモート攻撃、もう1つは車両への物理的な接続(OBD ポートなど)を必要とする物理攻撃です。

リモート攻撃はネットワーク接続(Wi-Fi、Bluetooth、3/4/5Gネットワークなど)に依存しており、多数の車両に同時に影響を与える可能性があります。

2010年以降、リモート攻撃が一貫して物理攻撃を上回っており、2010年から2024年にかけての全攻撃の88%、2024年には92%を占めています。2024年にはリモート攻撃の84%を遠距離攻撃が占めており、これは前年と一致しています。2022年にはコネクティッドカーとソフトウェア定義アーキテクチャの使用増加により30%の急増が見られました。

2024年のほぼ全てのインシデントはリモート攻撃

2024年のリモート・インシデントの大部分は遠距離攻撃

Source: Upstream Security

車両システムの操作や制御に関するインシデントが3倍以上に増加

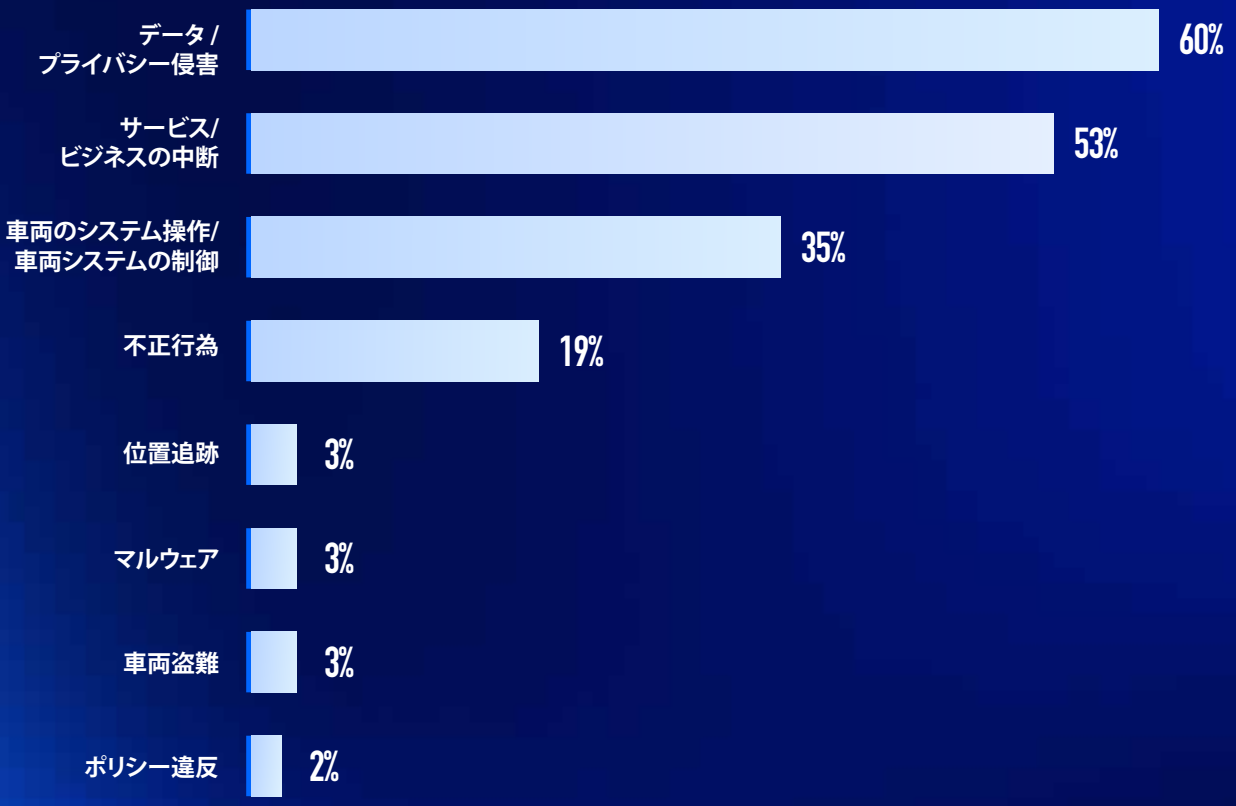
自動車とスマートモビリティのエコシステムはサイバー攻撃からますます影響を受けています。 車両への攻撃は機密データを危険にさらすことがよくありますが、さらに広範囲に及ぶ影響もあります。車両の盗難、不正行為、そしてシステムの操作や制御などが含まれ、これらは安全上のリスクをもたらす可能性もあります。

2024年のインシデントの60%が、データおよびプライバシー関連のインシデントでした。 2024年、車両システムの操作と制御に関するインシデントの割合が急激に増加し、インシデントの35%以上を占めました。

この増加にはいくつかの要因が考えられます。 この急増に大きく貢献しているのは、まず第一に、EV充電器とインフォテインメントシステムに関する研究の増加です。これは AutomotiveSecurityResearchGroup（ASRG）や、著名なホワイトハットグループがCVEを積極的に発見したプロジェクトによって証明されています。 さらに、Upstreamが自動運転車やIoTモビリティなどの分野におけるオープンソースソフトウェアの研究を強化したことも、この上昇傾向に貢献しています。これには、スマートモビリティ（例：テレマティクスシステム）、スマートシティシステム（例：交通信号システム）、EVSEなどが含まれます。

サービス/ビジネスの中断	サイバー攻撃によって引き起こされる事業の中断（例：ランサムウェアによるシステム停止やバックエンドシステムへの攻撃によるフリート運用の混乱）。
データ/プライバシー侵害	データ侵害は、脅威アクターが知的財産（IP）、企業秘密、財務情報、または個人を特定できる情報（PII）などの機密データに不正にアクセスした場合に発生します。サイバーセキュリティ・インシデントの中で、データ侵害に関するものが最も一般的で、最もコストがかかります。
不正行為	金銭的利益を目的にした脅威アクターによる車両データおよび/または車両機能を利用する違法使用。
車両盗難	脅威アクターによる遠距離、近距離、物理攻撃を伴う車両の盗難。
車両のシステム操作	脅威アクターがさまざまな車載システムを改ざんして、予想される動作を変更し、安全上のリスクを引き起こす可能性。
ポリシー違反	車両の使用、運用、管理に関して確立された規則、規制、またはポリシーに違反する脅威アクターの行為。
位置追跡	GPSナビゲーションのデータを違法に使用し、ユーザーや所有者の同意なしに車両の位置や移動を追跡すること。
車両システムの制御	脅威アクターは、コネクテッドコンポーネントを介してシステムをオーバーライドすることで、遠距離から車両の全て、または一部を制御すること。

自動車関連のサイバーインシデント409件に基づく2024年の影響内訳



Source: Upstream Security

CVESを厳重に監視

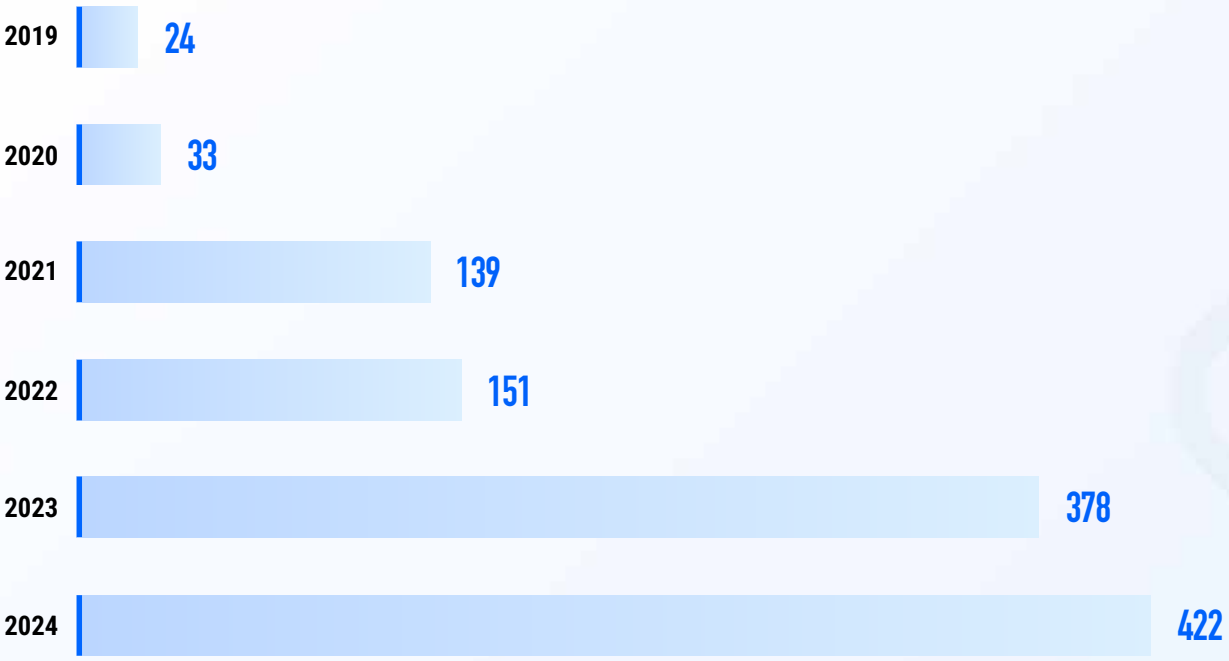
The Common Vulnerability Scoring System（CVSS）は、CVEsを評価するためのオープンで標準化された方法を提供するように設計されました。 CVSSは、脆弱性の基本的、時間的、環境特性に基づいて、組織が共同対応に優先順位を付け、調整をする援助をします。[134] また、脆弱性はCVSSスコアに基づいて「重大」「高」「中」「低」「なし」に分類されます。[135]

CVEsの分析は、自動車およびスマートモビリティのエコシステム(OEM、Tier-1、シェアードモビリティ、モビリティIoTデバイス、フリートなど)に直接影響を与えるCVEsのみに焦点を当てます。 この分析では、サプライチェーン全体で使用される可能性のある一般的なITハードウェアや、オープンソースソフトウェアコンポーネントに関連するCVEsは除外しています。

2019年から2024年に発見された自動車関連のCVEsの推移

自動車業界は2019年以来、1,147件の特定CVEsを記録しています。2023年の378件と比較して、2024年には422件のCVEsが公表されました。

CVEsが増加するのは、コネクテッドコンポーネントの普及増加、脆弱性に対するステークホルダーの認識の高まり、EV充電器とインフォテインメントシステムに関する研究イニシアチブの増加などに起因しています。



Source: Upstream Security

セキュリティチーム、開発者、研究者は、CVSS（共通脆弱性評価システム） を他の手法と併用してリスクを評価します。CVSSスコアは、製品の サプライチェーン全体 にわたって実用的に活用され、以下のような目的で使用されます。

- 脆弱性がすでに悪用されているかを判断
- 修正（パッチ適用）の優先順位を決定
- 時間とリソースの効率的な配分

さらに、CVSSはISO/SAE 21434 にも採用されており、標準のリスク評価プロセスの一環として 攻撃の実行可能性を判断する ために利用されています。

CVEsもまた、フリートマネージャーやオペレーターによって厳重に監視されなければなりません。CVEs は、フリート全体のリスク評価に影響を与えるだけでなく、フリート構成を戦略的に設計する際にも考慮することができます。

2024年のCVESの概要

CVEsは、広く認識され、カタログ化されたサイバーセキュリティリスクであり、自動車とスマートモビリティのエコシステム全体で迅速に参照できます。 これらの脅威はOEM製品によく見られますが、OEMサプライチェーン企業の製品にも出ることがあります。

OEMは、Tier-1およびTier-2サプライヤーが生産する何百ものソフトウェアおよびハードウェアモジュールから車両を組み立てます。各コンポーネントの品質と安全性は、そのコンポーネントを製造する企業に委ねられています。 したがって、サプライチェーンに関わる各企業は、自動車関連製品の品質と安全性を監視し、確保する責任があります。脆弱性は必ずしも時間どおりに対処されるわけではなく、またはまったく対処されないため、一般的に使用されているソフトウェアモジュールやコンポーネントのひとつの欠陥が、何百万台もの車両に影響を与える可能性があります。 CVEsが開示した脆弱性は、ハッカーが悪用する可能性もあります。

2024年には、米国の脆弱性データベース（NVD）における資金不足と予算削減により、CVEsの公開数に大きな影響を及ぼしました。 年初から、NVDにおいて脆弱性の公開と分析に顕著な遅延が生じ、企業のサイバーセキュリティチームはタイムリーに重要な情報が得られない状態に置かれました。4月、米国国立標準技術研究所（NIST）は、分析待ちのソフトウェアの脆弱性に関する、増え続けている未処理案件に対処するため、他の機関や産業界のパートナーと協力する計画を発表しました。[136] 年末にはCVEsの公開のペースは改善されたものの、共通脆弱性識別子（CVE）の分析の停滞に、NVDを依然として扱いかねていました。 2024年5月の報告によると、CVE提出の90%以上が未分析また脆弱性の強化が不十分であることが明らかになりました。[137] NISTは、11月までに、新たに発生するCVEsをリアルタイムで処理するために、十分なアナリストチームを設置したと報告しました。しかしながら、当局の楽観的な予測に反して、未処理案件の清算に当初の予定よりも時間を要することを認めました。[138]

公に報告された自動車関連の脆弱性の内訳（2024年）

Source: Upstream Security

2024年、Upstreamのアナリストが分析したCVSSスコアの脆弱性は、以下の通り

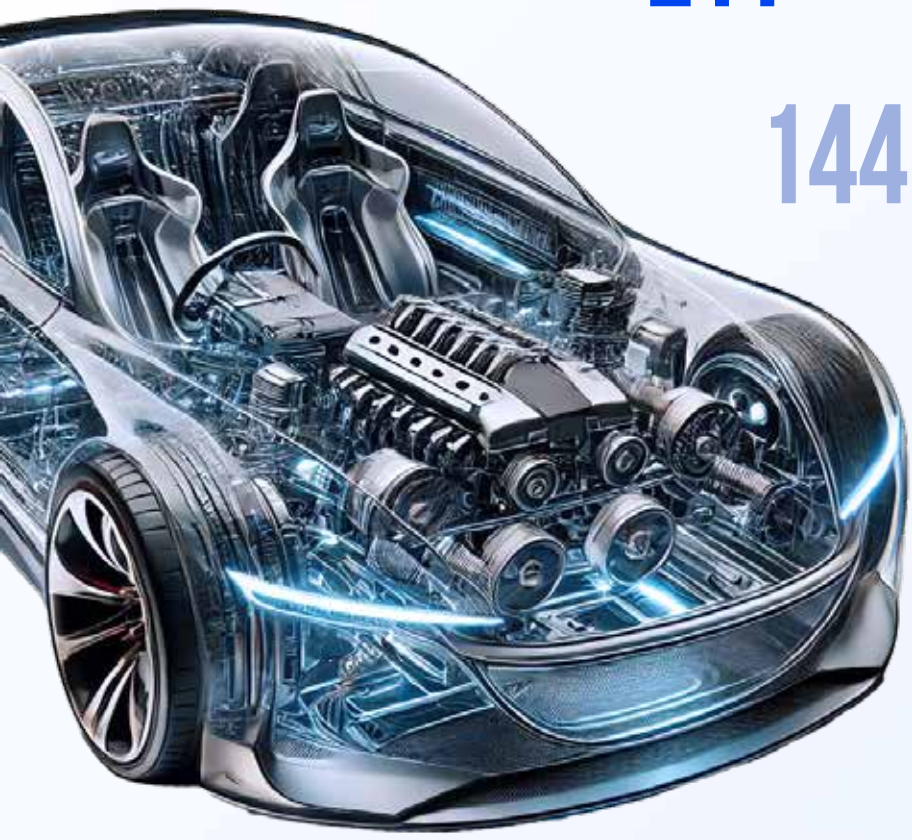
48 重大な脆弱性

211 高レベルの脆弱性

144 中レベルの脆弱性

19 低レベルの脆弱性

Source: Upstream Security



2024年の自動車関連のCVEsの増加と共に、重大な脆弱性も約41%の増加が認められました。これにより、自動車関連のCVEsが占める割合は、2023年の9%から増加し11%を超えるようになりました。この傾向は、すべての関係者が自動車特有のCVEsを注意深く監視し、積極的にエクスプロイトを検出し、さらに対策の優先順位付けを行うことの重要性を高めています。

スマートモビリティエコシステム全体に影響が及んでいます

自動車、スマートモビリティ、MaaS（Mobility-as-a-Service）のエコシステムのあらゆるセグメントで、サイバー攻撃が脅威になっています。

スマートモビリティデバイスの普及により、サイバーセキュリティリスクが大規模となる新たな時代が到来しています。EV充電設備とインフラ、自律システムと自動運転キット、交通管制システム、テレマティクスシステム、車両管理ソリューション、スマート農業機器など、さまざまなデバイスが攻撃対象となる可能性があります。

自動車およびスマートモビリティエコシステムにおけるIoTデバイスは、現在では重要なインフラとなっています。これらのデバイスへのサイバー攻撃では、他のIoTデバイスよりも高いリスクと影響をもたらすため、関係者は安全性、運用の有用性、およびデータの完全性を確保する必要があります。

重要インフラとして、自動車およびスマートモビリティを定義することで、これらのデバイスが引き起こす重大なサイバーセキュリティリスクを重要視し、それらの回復を優先する必要性を強化することに繋がります。

- OEMs
- Tier-1s
- Tier-2s
- 電気自動車
- EV充電インフラ / ローカル・グリッド
- 自動運転車
- 農業機械
- モビリティIoT
- TSP / フリートマネジメント
- カーディーラー
- 自動車、商用車、配送車両
- 公共交通機関
- 政府車両 / 緊急サービス
- カーシェアリングとバイクシェアリング
- レンタカー
- ライドシェアとヘイリング
- スマートシティ
- 保険

OEMとサプライヤー

OEMとそのコンポーネントサプライヤーにおいては、ランサムウェアの攻撃標的にされることが増えてきています。その結果、生産停止、データ損失、費用のかかるリコール、ブランドの毀損が生じています。

2024年2月、ドイツを拠点とする上場企業Tier-1の世界的なバッテリーサプライヤーがサイバー攻撃を受け、数週間にわたって生産が麻痺し、約4,000万ユーロの損害が発生しました。[139] 同社の業務は大幅に混乱し、管理、営業、財務、カスタマーサービス機能を含む業務にまで影響が及び、世界5か所の生産拠点のすべてで生産を再開するまでに1か月以上を要しました。[140] 2024年3月中旬、経営陣は会社の年次財務報告書の公表を延期することに決定しました。そして、「IT システムへのアクセスの一部は回復し、生産の大部分は再開したものの、財務報告書を完成させるために必要な財務情報やビジネス文書へのアクセスがまだできません」と述べました[141]

2024年3月、日本のOEMメーカーでは、数ヶ月前に報告されたサイバー攻撃により、業務に深刻な影響を受け、10万人以上の顧客に影響を及ぼすデータが流出したことを確認しました。流出したデータには、個人情報、財務諸表、雇用・給与情報、メディケアカード、運転免許証、パスポート、納税者番号などが含まれていました。[142] ランサムウェア集団は攻撃を行ったのは自分達であると認め、個人の従業員情報、機密保持契約書、プロジェクトデータ、パートナーや顧客に関する情報を含む100GBのデータを盗んだと主張しました。この攻撃に対応して、同社は政府当局や外部のサイバーセキュリティ専門家の支援を得て調査を行い、対応組織を立ち上げ、個人情報盗難およびクレジット・モニタリング・サービスを提供し、損害により政府発行の身分証明書の交換が必要な顧客に対しては、支払った交換費用の払い戻しを行いました。[143]

電気自動車と電気自動車充電設備

電気自動車の数が増加するにつれ、送電網のサイバーセキュリティと充電インフラの耐久性に対する懸念も高まっています。電気自動車の急速な普及により、充電インフラの開発が急速に進んだものの、サイバーセキュリティのベストプラクティスや脆弱性がしばしば見過ごされている中で、電気自動車用充電設備に特化した規制はまだまだ遅れをとっています。

充電器は、その機能を制御する物理的およびリモート操作に対して脆弱であり、EVユーザーを詐欺、データ侵害、さらには身代金攻撃にさらす可能性があります。

2024年1月、セキュリティ研究者らが米国のEVSE社の家庭用充電ステーションに複数の脆弱性を発見しました。これらの脆弱性により、攻撃者が充電器にリモートでアクセス、制御してしまう可能性があります。 このサイバーセキュリティの脆弱性には、リバースSSHトンネルの実装の欠陥、古いHTTPサーバー、既知の脆弱性を持つ非推奨のNTPクライアント、非推奨のカーネル、そして有効期限のないデバイス証明書が含まれていました。 攻撃者はEVSE社の中央サーバーに認証を行い、潜在的に独自のトンネルを作成し、接続された各充電器への不正アクセスを拡大する可能性がありました。この発見を受けて、セキュリティ研究者らは積極的に同社と協力し、脆弱性に対処しました。これはソフトウェアの更新版でアップデートされています。[144]

2024年2月、英国の製品安全基準局（OPSS）は、現行のサイバーセキュリティ規制に準拠していないとして、スペイン製EVチャージャーの販売を停止し、国家のエネルギーインフラに対する潜在的リスクへの懸念を高めました。[145] ハッカーが数千台の非準拠充電器にアクセスし、一斉にスイッチを入れることで、電力網を混乱させるピーク需要を引き起こす可能性があった為です。 この企業は英国で4万台、世界中で50万台以上を販売しており、2024年6月30日まで英国で、この充電器を販売することを許可されていました。

2024年4月、セキュリティ研究者らは、オープン充電ポイントプロトコル（OCPP）のバックエンド通信と電気自動車充電ステーション（EVCS）との間のセキュリティの脆弱性に関する技術分析PoC（概念実証）を公開しました。この分析では、16の代表的な稼働中のEV充電管理システムのうち、OCPP 1.6Jに影響を与える6つのゼロデイ脆弱性が特定されています。研究者らは、オンラインの様々なリソースからEVCS IDとOCPPバックエンドリンクを入手することに成功し、このことは中間者攻撃、サービス妨害攻撃、ファームウェア窃取、データ汚染など、様々な攻撃シナリオを示唆しています。研究者らは侵害されたEVCSを利用して、電力網に対するスイッチング攻撃を受ける可能性を実証するためのテストベッドも開発し、将来のサイバー攻撃を軽減・防止するための対策を提言しました。[146]

2024年7月、研究者らはEV充電機器にセキュリティ脆弱性を発見しました。 この脆弱性により、攻撃者は電力線通信（PLC）プロトコルを悪用して不正アクセスを行い、電気自動車（EV）の充電を妨害することができます。 なぜなら研究者たちも、充電器とEVのネットワークキーとデジタルアドレスにアクセスできたからです。[147]

2024年11月、イタリアのEV充電会社が、充電器のファームウェアにおけるセキュリティ脆弱性を修正するため、リモートアップデートをリリースしました。この脆弱性では、システムログや管理者権限への不正アクセス、そして充電器のウェブ管理インターフェースを通じた任意のコマンド実行を許していました。個人データは危険にさらされませんでしたが、攻撃者は充電システム保護機能を回避し、システム設定にアクセスし、サービス妨害攻撃を仕掛けることができる状態でした。オフラインデバイスを使用しているユーザーは、モバイルアプリを通じてパッチを更新するよう勧告されました。[148]

また、2024年11月、著名な脅威者が複数の世界的なCPOから約116,000件の機密データを流出させました。[149] 当初、アメリカのEV OEM充電ネットワークからとされていたデータ流出は、その後、世界中の様々な充電ステーションのデータを含むことが判明し、被害はUAE、オーストラリア、メキシコ、プエルトリコ、ガイアナ、サウジアラビア、オマーン、インドにまで及んでいました。

商用フリート

レンタカー会社、物流会社、配送会社などの商用フリートの運営者は、車両管理においてコネクティビティとソフトウェアへの依存度が高まるにつれ、サイバーセキュリティリスクが増大しています。

サイバーインシデントの影響は商用フリートにとって重大であり、しばしば運用効率の低下、運用コストの増加、サービスの遅延、そして極端な場合には完全なサービス中断をもたらします。

2024年3月、コロラド州立大学のセキュリティ研究者は、米国で約1400万台の中・大型商用トラックに義務付けられているELD(電子記録装置)が、BluetoothやWi-Fi接続を介してアクセスされ、トラックの制御、データの操作、車両間でのマルウェアを拡散させる可能性があることを明らかにしました。研究者は、ELDがデフォルトのファームウェア設定のまま配布されており、重大なセキュリティリスクを伴うことを発見しました。 また、通信にはCAN BUSを使用し、OTAアップデート用の公開API、予測可能な識別子と脆弱なパスワードを備えていることにより、無線範囲内の攻撃者が車両システムに不正に接続し、アクセスすることが容易になっています。 セキュリティ研究者は、14秒以内にトラックのWi-Fiに接続し、ELDを書き換え、悪意のあるメッセージを送信して、トラックを減速させることに成功しました。
研究者は、商用フリートの安全性と運用可能性に対して重大なセキュリティリスクをもたらす調査結果を、メーカーおよび米国サイバーセキュリティ・インフラセキュリティ庁（CISA）に報告し、広範囲にわたる混乱の可能性を強調しました。[150]

2024年5月、欧州の車両追跡およびフリート管理デバイスプロバイダーでデータ侵害が発生しました。 攻撃者はダークウェブのフォーラムでこれを公開し、同社のシステムの脆弱性を露呈させました。GPS IMEI番号、リアルタイムの車両追跡データ、請求詳細、顧客アカウント情報などを含む機密情報が漏洩しました。攻撃者は40カ国以上、5,000社以上にわたる企業の全ての内部システムへのアクセス権を持っていると主張しました。[151]

2024年10月、英国を拠点とする車両追跡、燃料管理、ルート最適化、およびフリート運営者向けの安全監視ソリューションのプロバイダーがサイバー攻撃に遭い、サービスの大部分に影響を受けました。その結果、刑務所の護送車や配送車両の追跡システムや緊急警報を無効化せざるを得なくなりました。 顧客データの侵害はありませんでしたが、一部の従業員データが影響を受けました。[152]

スマートモビリティIoTデバイスとサービス

スマートモビリティIoTデバイスやサービスが、普及し、利用が拡大し続けるにつれ、それらのデバイスやサービスは、スマートモビリティのエコシステム内でリスクの高いターゲットとなっています。 これらのサービスおよびデバイスには、何千人ものユニークユーザーの機密性の高い個人情報（PII）および決済データが保持されています。

スマートモビリティデバイスやサービスに対する攻撃は、車両およびスマートモビリティシステムの安全性、データ、運用可用性に直接的な影響を与えます。.

2024年4月、ドライバーにリアルタイムの天気と交通情報を提供する米国のプロバイダーがランサムウェア攻撃を受け、スタッフは直ちに全システムをシャットダウンし、即時の保護措置を講じることを余儀なくされました。このシャットダウンにより、サービスの動的情報掲示板、公式ウェブサイト、そしてリアルタイムカメラシステムにも影響が及びました。[153]

2024年9月、フィリピンを拠点とする高速道路運営会社がデータ侵害に見舞われ、顧客の機密性の高い個人情報（PII）が流出する可能性が生じました。 運営会社はサイバーセキュリティの専門家と関係当局に協力を仰ぎ、侵害範囲を徹底的に調査し、現地の規制要件への遵守を強化することで、侵害の影響を軽減する対応を取りました。[154]

2024年10月、オランダ政府は、セキュリティ研究者が緊急車両の通行を許可するための信号優先制御システムに重大なセキュリティの脆弱性があることを発見したことを受けて、数千の信号機を交換すると発表しました。 この脆弱性を悪用すると、救急車や消防車が使用する緊急無線信号に侵入し、非常時に交差点を容易に通過できるように信号を青に強制的に変えてしまいます。研究者によると、攻撃は数キロメートル離れた場所から実行され、複数の交差点に同時に影響を与える可能性があるとされています。

2030年までに数万もの信号機が、無線信号の代わりにモバイルインターネット接続を使用する新しい安全なプラットフォームに置き換えられる予定です。[155]

保険

保険会社は、サイバー脅威の状況がコネクテッドカーの保険料に直接影響することを認識し始めています。保険会社は、コネクテッドカーのデータを使用して、サイバー攻撃を受けやすい場所、車両の種類、コンポーネントを特定し、それに応じて保険料を計算することができます。

新しい行動ベースの保険モデルは、アフターマーケットデバイスを活用してテレマティクスを保険会社と共有することで、保険料と保険コストを削減することができます。しかし、脅威者はこれらのデバイスの脆弱性を悪用し、データや通信を操作して保険会社のITネットワークをハッキングすることができます。 保険会社とそのテレマティクスサプライヤーは、テレマティクスインフラの安全性を確保するために協力する必要があります。

2024年1月、あるセキュリティ研究者が、日本のOEMの保険代理店ウェブサイトに脆弱性を発見し、企業のクラウド資格情報が公開されていることが判明しました。 これにより、顧客情報、保険契約書のPDF、パスワードリセットリンク、ワンタイムパスワード、その他の情報を含む約25GBの657,000通のメールが保存されているメールアカウントにアクセスできるようになっていました。[156]

自動運転車

自動運転車（AV）のイノベーションは、OEM、スマートモビリティおよびライドシェアサービスプロバイダー、大手テクノロジー企業など、多くのステークホルダーによって急速に導入されています。 他のメーカーもそれほど遅れをとっていません。 自動運転車両は勢いを増しており、ユーザーにこれまでにない効率性と顧客体験を提供していますが、安全性への懸念や一般市民の不信感がないわけではありません。

自動運転車は、車両の中核機能へのリモートアクセスを提供しており、脅威アクターが効果的に大規模な攻撃を行うことを可能にしています。インターネットや衛星を含む複数のソースからデータや指示を受信するナビゲーターセンサー（GPS、LIDAR、カメラ、ミリ波レーダー、IMUなど）を搭載しており、これらに依存しているからです。そのため、攻撃者はセンサーによる有用なデータの取得を妨げたり、誤ったデータを取得させたり、巧妙に細工されたデータを用いてセンサーの機能を操作することが可能になります。[157]

2024年2月、デューク大学のセキュリティ研究者達は、使用中のレーダーシステムの事前知識なしに、自動運転車のセンサーシステムから実際の物体を隠す攻撃を実証しました。

MadRadarと呼ばれる攻撃のデモンストレーションでは、研究者達はドップラー・レーダー・システムに「幻の」物体を出現させ、センサーから離れて走行している車両が進行方向を変えて正面衝突すると誤認させました。研究者達によるとMadRadarは、「マイクロ秒単位」でレーダーの種類を検出・学習し、瞬時に攻撃を適応させるとのことです。このタイプの攻撃は、レーダーを使用するアダプティブクルーズコントロールシステムを欺き、前方の車が実際には加速していないのに加速していると誤認させ、正面衝突を引き起こす可能性があります。[158]

2024年3月、カリフォルニア大学アーヴァイン校と日本の慶應義塾大学のセキュリティ研究者達は、市販されている第一世代および次世代LiDARシステム9種類に15の脆弱性を発見しました。これらの脆弱性により、偽の車や歩行者を直接スプーフィングしたり、自動運転車の視界から実際の車を消失させたりすることが可能となります。 LiDARセンサーへのこれらの攻撃は、自動運転車の緊急ブレーキや正面衝突など、さまざまな危険性のある運転挙動を直接引き起こすために使用される可能性があります。[159]

2024年5月、シンガポールのセキュリティ研究者達は、カメラベースのコンピュータービジョンへの依存を利用してAVに干渉し、LEDを使用して道路標識を無視させることができることを証明しました。道路標識の外観を安定的に繰り返し歪めることができ、撮影されたすべてのフレームが歪んでいることを確認しました。研究チームは、中国の有名な自動運転車開発者が使用しているカメラを搭載した車と実際の道路を使用してシステムをテストしました。この安定した攻撃の2つのバージョンは、チームによって開発されましたGhostStripe1は、車両へのアクセスを必要とせず、追跡システムを使用して対象車両の位置をリアルタイムで監視し、それに応じてLEDの点滅を動的に調整し、標識が正しく読み取られないようにします。GhostStripe2 では車両へのアクセスが必要であり、カメラの電源線にトランスデューサーを配置してフレーミングの瞬間を検出し、タイミング制御を微調整する必要があります。研究者達は、GhostStripe1とGhostStripe2がそれぞれ94%と97%の成功率を達成したと主張しています。[160]

2024年5月、バッファロー大学のセキュリティ研究者達がマルチセンサーフュージョンシステムの脆弱性を発見しました。このシステムは、LiDAR、カメラ、レーダーセンサーからのデータを統合する技術で、自動運転車で一般的に使用されています。研究者達は、単一の敵対的オブジェクトを使用して3種類すべてのセンサータイプを同時に侵害できる、高度な攻撃手法を導入しました。このオブジェクトは、簡単かつ安価に製作でき、高度なステルス性と柔軟性をもって攻撃を実行することが可能です。 研究者達は、わずか2つの小さな敵対的オブジェクトを配置することで、標的車両を被害者側の自動運転車の認識システムから効果的に見えなくすることができることを実証しました。[161]

04.

2024年の攻撃ベクトル

自動車産業やスマートモビリティのステークホルダーは、進化する脅威とそれがサイバーセキュリティの態勢に与える影響を監視し、分析する必要があります。

ACESテクノロジーに対する脅威が攻撃環境を形作る

2024年のサイバー攻撃は、より高度化・頻発化し、車両やバックエンドシステム、さらにはスマートモビリティのプラットフォーム、デバイス、アプリケーションを標的とするようになりました。 攻撃の状況は、自動運転、コネクティビティ、電動化、シェアードモビリティ（ACES）技術に対する脅威によって形成されました。

攻撃者は、新たなゼロデイ脆弱性（未知または未対処の脆弱性を利用するサイバー攻撃の手段）を発見し、新しい手法を開発し、SDV、AV、EV、およびEV充電設備で使用されているソフトウェアやハードウェアコンポーネントの多数の脆弱性を悪用しました。

2024年、自動車およびスマートモビリティのエコシステムにおいて、テレマティクスやアプリケーションサーバーに対する攻撃が大幅に増加し、2023年の43%から2024年には66%に達しました。 この劇的な増加は、主にモビリティ部門を標的としたランサムウェア攻撃の急増によるものです。

APIは、車載コンポーネント、テレマティクス、バックエンドシステム、およびアプリケーション間の接続性を向上させるのに役立ってきました。
しかし、APIもまたサイバー脅威の主要な標的となってきました。 2022年中では、APIベースの攻撃が驚異的に380%も増加し、全インシデントの12%を占めました。それ以来、攻撃者が脆弱性を悪用して大規模な攻撃を実行するため、API関連の攻撃は着実に増加し続けてきました。 この傾向は一貫して二桁の伸びを示しており、2023年に13%増加し、 2024年にさらに10%急増して、API関連のインシデントが全攻撃の17%を占めるに至りました。

API関連への攻撃が初めてインフォテインメントシステムへの攻撃を上回り、後者は2023年の15%から2024年の14%に減少しました。

この傾向は、接続されたコンポーネントに対する攻撃者の認識と可視性の高まりに起因するものです。これは、自動車のサイバーセキュリティの脅威環境が成熟していることを示しており、脅威アクターが機密データにアクセスし、幅広いモビリティ資産を制御しようとする努力が増大していることを表しています。

テレマティクスおよびアプリケーションサーバーへの攻撃が急増

2023年は

43%

2024年は

66%

攻撃ベクトル別インシデント

Source: Upstream Security

テレマティクスとアプリケーションサーバー

コネクテッドカーは、その寿命がある限り、OEMバックエンドサーバーや車両所有者から情報を収集、送信、受信します。 これは、車両と通信するテレマティクスサーバと、車両の付属アプリケーションと連携するアプリケーションサーバの2種類のサーバを使用することで実現されます。車両と通信するテレマティクスサーバーと、車両の付属アプリケーションと連携するアプリケーションサーバーです。 さらに、一部の車両には、保険会社、フリート管理、レンタカーやリース会社、EV充電ネットワークなどの第三者と通信するバックエンドサーバーが搭載されています。

攻撃者はこれらのサーバーの脆弱性につけ込んで、機密データを流出させたり、走行中の車両に対して攻撃を仕掛けることもできます。

- 2024年1月、セキュリティ研究者が日本のOEMの保険代理店のウェブサイトに脆弱性を発見しました。企業のクラウド認証情報が露出していました。 これにより、攻撃者は約25GB、65万7000通のEメールアカウントにアクセスできました。アカウントには顧客情報、保険証書のPDF、パスワードリセットリンク、ワンタイムパスワードなどが含まれていました。[162]
- 2024年3月、米国のEV充電インフラ設置会社で約585GBのデータを含むデータ侵害が発生しました。この侵害により、作業請求書、価格提案書、電気工事許可書、調査書など、様々な業務文書が露出しました。 さらに、個人を特定できる情報（PII）、自宅の写真、充電器の詳細など、消費者情報を露呈させました。[163]
- 2024年5月、ヨーロッパの有名な車両追跡および車両管理デバイスプロバイダーがデータ侵害を受けました。データ侵害は、ダークウェブのフォーラムで攻撃者によって公開されました。
  攻撃者は会社の内部システムの脆弱性を露呈させました。これにより、GPS IMEIナンバー、リアルタイムの車両追跡データ、請求詳細、顧客アカウント情報などの機密情報が漏洩しました。 攻撃者は、40か国以上、5,000社以上にわたる企業の全ての内部システムにアクセスできたことを明らかにしました。[164]
- 2024年9月、セキュリティ研究者が、大手レンタカー会社が使用している事故報告アプリケーションに、安全ではない直接オブジェクト参照（IDOR）の脆弱性を発見しました。事故報告書の顧客PIIが露出していました。この脆弱性により、URLのレポート番号を変更することで、任意の事故報告書に不正アクセスすることが可能でした。 会社は通知を受け、速やかに第三者製アプリケーションをシャットダウンし、漏洩した情報へのアクセスを制限しました。[165]

API

コネクテッドカーやスマートモビリティデバイスやサービスでは、外部および内部のAPIが幅広く使用されており、その結果、毎月数十億件のトランザクションが発生しています。 OTAやテレマティックスサーバー、OEMモバイルアプリ、インフォテインメントシステム、モビリティIoT機器、EV充電管理、課金アプリ等はAPIに大きく依存しています。

> ***また、APIは重要かつフリート全体にわたる大規模な攻撃先となっており、機密情報（PII）の窃盗、バックエンドシステムの操作、悪意のある車両遠隔操作など、広範なサイバー攻撃につながります。***

APIハッキングは、他のシステムをハッキングするよりも費用対効果が高く、大規模な攻撃が可能です。 高度な技術や専門性はあまり必要とせず、標準的な手法で、特別なハードウェアを使わずに遠隔からの攻撃が可能です。

この3年間で、自動車業界、サプライチェーン、モビリティデバイスやサービスでは、APIベースの攻撃によるデータおよびプライバシーの侵害が大幅に増加しました。

- 2024年5月、セキュリティ研究者チームは、米国のEVSEベンダー製EV充電ステーションに複数の脆弱性を発見しました。
  同チームは、アクセス制御の不備、不十分な証明書検証、および未検証のパスワード変更といった脆弱性を突き止めました。これらの欠陥により、API認証された悪意のある攻撃者がシステムのパスワードを変更し、隣接ネットワークへ侵入する可能性が生じます。 ベンダーはこれらの脆弱性に対処するセキュリティアドバイザリを公開しました。[166]
- 2024年6月、セキュリティ研究者は韓国OEMのディーラーAPIに脆弱性があることを発見しました。この脆弱性を利用することで、ディーラーとして登録し、ナンバープレートのみで影響を受けたOEM車両を乗っ取ることが可能でした。
  研究者はボタン操作のみで被害車両を乗っ取り、氏名、メールアドレス、電話番号を含む個人情報へのアクセス、遠隔操作、追跡が可能であることを実証しました。 韓国OEMが脆弱性を修正した後の2024年9月、研究者は調査結果を発表しました。[167]
- 2024年11月、エネルギー管理とEV充電インフラを専門とする多国籍企業が情報漏洩被害に遭いました。ハッカーは、同社のプロジェクト管理システムに侵入し、REST APIの脆弱性を悪用して、従業員と顧客の記録40万件、固有メール7万5千件を含む1.5TBのデータを抽出しました。

ハッカーはダークウェブフォーラムに身代金要求文を投稿し、同社が48時間以内に情報漏洩を公表しなければ、データを公開すると脅迫しました。同社は現在調査中であり、事態の収束に努めていると発表しました。[168]

インフォテインメントシステム

車載インフォテインメントシステム（IVI）は、最も一般的な標的の1つです。インターネットに接続し、インストールされたアプリケーションや携帯電話やBluetoothデバイスとの近距離通信にさらされます。その結果、PIIにアクセスできるようになります。 さらに、IVIシステムは車両の内部ネットワークに接続することが多いため、車両に深刻なリスクをもたらします。IVIシステムは、悪意のあるソフトウェアが内部システムに侵入する際に最も抵抗の少ない経路となり得ます。

- 2024年1月、セキュリティ研究者はヨーロッパのOEM車両とインフォテインメントシステムに7つの脆弱性を発見しました。CVE-2023-28895からCVE-2023-28901に分類されたこれらの脆弱性は、複数のセキュリティ上の弱点を明らかにしました。パワーコントローラーチップ（車両の電気機能を管理する重要なコンポーネント）への不正制御を可能にするハードコード化されたパスワード、CAN BUSネットワーク経由での車両診断情報の傍受と読み取りを可能にする脆弱性、データ過負荷によるエンターテインメントおよびナビゲーションシステムのクラッシュリスク、そして車両識別番号を悪用して、走行履歴や車両統計などの機密ユーザーデータを漏洩させる可能性があるオンライン車両サービスを管理するクラウドサービスの欠陥などです。[169]
- また2024年1月、セキュリティ研究者は、日本のOEMが広く使用しているすべてのバージョンのヘッドユニットに影響を与える脆弱性を発見しました。 この脆弱性はCVE-2024-39339として特定され、設定ミスが原因で発生し、機密情報（診断ログトレース、システムログ、ヘッドユニットのパスワード、PIIなど）が意図せず開示される可能性があります。[170]
- 2024年7月、車載インフォテインメントおよびテレマティクスシステムで使用されているチップセットに、CVE-2024-21462として知られる脆弱性が発見されました。この脆弱性は、バッファオーバーリードの脆弱性が原因で、悪用されると一時的なサービス拒否（DoS）攻撃を受ける可能性があります。[171]
- 2024年10月、日本のOEMインフォテインメントシステムにおいて、CVE-2024-6245として識別されたデフォルト認証情報の脆弱性が発見されました。 Linuxに関連する脆弱性により、攻撃者は既知のユーザー名とパスワードを使用して不正アクセスし、システムの完全性と可用性に影響を与えました。[172]

EV充電インフラ

信頼性が高く安全な充電インフラを提供することは、EVの普及を促進させるために不可欠です。 しかし今日、多くの充電器、充電インフラ部品、および関連アプリは、直接的な操作またはリモートによる操作に対して脆弱であり、それによって正常に機能しなくなる可能性があります。また、EVユーザーの個人情報の流出、詐欺、ランサム攻撃の危険にさらされるだけでなく、充電ネットワークや車両群、さらには地域の電力網にまで広範囲に影響が及ぶおそれがあります。

- 2024年1月、セキュリティ研究者たちが米国のEVSE（電気自動車充電設備）の家庭用充電ステーションに脆弱性が複数あることを見つけ出しました。これにより、攻撃者が充電器にリモートでアクセスし、コントロールできる可能性がありました。セキュリティ脆弱性には、リバースSSHトンネルの実装の欠陥、古いHTTPサーバー、既に脆弱性を持つことがわかっている非推奨のNTPクライアント、非推奨のカーネル、そして無期限の有効期限を持つデバイス証明書が含まれていました。 ハッカーがEVSEの中央サーバーで認証されてしまうと、不正なトンネルが作成され、接続された各充電器まで不正アクセスが拡大されるおそれがありました。 この発見後、セキュリティ研究者たちは積極的に企業と協力し、脆弱性に対処しました。その結果、ソフトウェアのリリースによりアップデートが行われたのです。[173]

- 2024年2月、英国の製品安全基準局（OPSS）は、現行のサイバーセキュリティ規制に準拠していないとしてスペイン製EV充電器の販売を停止しました。これにより国家のエネルギーインフラに対する潜在的なリスクへの懸念が高まりました。[174] ハッカーが数千もの非準拠充電器にアクセスし、一斉にスイッチを入れてしまうと、電力網が混乱するピーク需要が引き起こされる可能性があります。

- 2024年4月にセキュリティ研究者達が技術分析のPoC（概念実証）を発表しました。EV充電ステーション（EVCS）とOCPP（Open Charge Point Protocol）のバックエンド通信の脆弱性を指摘 したものです。その中で、16の代表的な稼働中のEV充電管理システムにおいて6つのゼロデイ脆弱性が確認されたことを明らかにしました。 研究者たちは、様々なオンラインリソースからEVCS IDとOCPPバックエンドリンクを入手することに成功しました。これによると、中間者攻撃、サービス妨害、ファームウェア盗難、データ汚染など、さまざまな攻撃シナリオが引き起こされていたことがわかりました。 さらに、侵害されたEV充電ステーション（EVCS）を使用して、電力網に対するスイッチング攻撃を行う可能性を実証するためのテストベッドを開発し 将来のサイバー攻撃を軽減、防止するための対策を推奨しました。[175]

- 2024年5月、ベルギーに拠点を置くEV充電器メーカーが、ハッカー集団の標的になりました。彼らは充電ステーションのQRコードを悪用して、ユーザーを偽の支払いページに誘導していたのです。

EU規制の下では、充電ステーションではQRコードなどのアドホックな支払い方法が必要とされています。同社は、機器上に複数の偽造QRコードが発見されたことを確認しました。これらのQRコードにより、ハッカー集団の金銭的窃盗が可能になったとしています。[176]

- 2024年8月、セキュリティ研究者らは、Open Charge Point Protocol (OCPP)を介してEV充電ステーションを管理するオープンソースプラットフォームに重大な脆弱性（CVE-2024-21550）があることを確認しました。この脆弱性は、クロスサイトスクリプティング（XSS）脆弱性の一種で、攻撃者がWebSocketsを介して悪意のあるHTMLやJavaScriptコードをプラットフォームの管理インターフェースに入れ込む事ができるというものです。 このセキュリティー侵害により、不正なユーザーがインターフェースを操作したり、機密情報にアクセスできるようになります。[177]
- 2024年11月、複数の世界的な充電ポイント事業者（CPO）に影響を及ぼすデータ侵害が発生し、UAE、オーストラリア、メキシコ、プエルトリコ、ガイアナ、サウジアラビア、オマーン、インドを含む複数の国の顧客の個人識別情報（PII）とOCPPが流出しました。 これらのCPOに共通する要素の1つは、インドのEV充電およびエネルギー管理ソフトウェアプロバイダーが開発したEV充電アプリを使用していることです。 このデータ侵害により、約116,000件の消費者の個人識別情報（PII）および機密データが漏洩しました。これには、消費者の名前、充電ステーションの所在地、車両情報（VINナンバーなど）、暗号鍵、および認証トークンが含まれていました。 自動車業界を標的にしていることで最近知られるハッカーが、このデータをディープウェブのハッキングフォーラムに公開しました。 ハッカーは米国の充電ステーションから得たデータだと主張しましたが、分析の結果、複数のOEMによって使用されている世界中の充電ステーションからの情報が含まれていることが明らかになりました。[178]

GPS/GNSS ナビゲーションシステム

GPS/GNSSナビゲーションシステムは、車両の正確な位置追跡と効率的な経路案内に不可欠です。 しかし、これらのシステムは、信号のなりすましや妨害などの直接的な操作やリモートでの攻撃に対してますます脆弱になっています。これらの攻撃によって、ナビゲーションの精度が乱され、ユーザーのプライバシーが脅かされ、さらには自動運転車や接続された車両の安全性にも危険が及ぶ可能性があります。 これらの脆弱性が原因で、交通ネットワーク、車両群の運用、さらにはナビゲーション技術に対するユーザーの信頼が大きく損なわれかねません。

- 2024年5月、フランス製の企業用ジェット機がポーランドからイギリスへ向かう途中にサイバー攻撃の被害に遭いました。 パイロット達の報告によると、GPSや他のナビゲーションや通信信号が30分間遮断されたそうです。 当局は、この事件を地域の通信およびシグナルインフラを妨害することを目的とした一連の大規模なサイバー攻撃と関連付けました。 このサイバー攻撃によって、航空機、船舶、およびその地域で運行するあらゆる形態の輸送機関にリスクが生じました。[179]
- 2024年5月、あるセキュリティ研究者が、利用者数の多いGPS車両追跡アプリに重大な脆弱性を発見し、世界中の13万台以上の車両に影響を及ぼしました。GPSのブランド名は明らかにされませんでしたが、アプリのデモモードのセキュリティが脆弱だったため、車両のリアルタイムの位置情報へ不正アクセスが可能になるという欠陥でした。デモモードのURLとクッキーの設定を変更することで、別の地域の車の位置を確認することができたのです。
  研究者は、その問題を会社に報告しました。[180]
- 2024年8月、オープンソースのGPS追跡システムに2つの脆弱性（CVE-2024-31214とCVE-2024-24809）が見つかりました。特定のバージョンで導入されたデバイスイメージファイルのアップロード機能の欠陥に起因した脆弱性です。このモジュールはパストラバーサルと危険なファイルタイプの無制限アップロードに対して脆弱です。これらの脆弱性が悪用された場合、認証回避やリモートコード実行につながる可能性があります。[181]

サードパーティサービス

サードパーティサービスは、車両の接続性とユーザー体験向上させるために、リモート診断、インフォテインメント（情報・娯楽システム）、車両管理などの機能が含まれます。しかし、これらのサービスは直接的および遠隔的な操作の両方に対して脆弱であり、データ漏洩、不正アクセス、サービス中断などの影響を受ける可能性があります。 このような脆弱性により、ユーザーは詐欺、プライバシー侵害、ランサムウェア攻撃にさらされるおそれがあります。これは車両エコシステム全体に影響を与え、安全性を損ない、コネクテッドカー技術への信頼を損ないかねないものです。

- 2024年3月、インドのOEMがサードパーティプロバイダーを通じてデータ侵害を受け、その結果、企業データと顧客の個人情報が流出しました。OEMまたはマーケティングプロバイダーが侵害に関する調査を開始したか、法執行機関に報告したかどうかは不明のままです。[182]

- 2024年5月、米国の電気自動車運転者向けに設計された、運転状況、充電状況、その他の車両関連の指標に関する詳細な洞察を提供するサードパーティ製アプリケーションの脆弱性が、セキュリティ研究者により発見されました。 この脆弱性には、パスワードのプレーンテキスト保存と認証情報の検証不備が含まれており、脅威アクターがシステムを完全に制御する可能性がありました。 研究者からこの問題の報告を受けたソフトウェア開発者は、その脆弱性を認めましたが、適切な解決策を見つけるためにテスト中であると回答しました。[183]
- 2024年9月、ディーラーのスケジューリングとコミュニケーション自動化のためのAI活用ソリューションを専門とする米国の企業がサイバー攻撃を受け、機密データが漏洩しました。脅威アクターにより、約24万件の消費者個人情報（PII）が漏洩しました。これには、VIN（車両識別番号）や走行距離、修理オーダー、価格、文書などの車両データが含まれていました。企業が、この侵害に関して調査を開始したか、関係当局に通知したかどうかは、未だ不明です。[184]

ECU

電子制御ユニット (ECU) は、エンジン、ハンドル操作、ブレーキ、窓、キーレスエントリーを含め、さまざまな重要なシステムを制御しており、妨害や操作される可能性があります。 攻撃者は、高度なシステムを複数同時に実行することで、ECUを操作し、その機能を制御しようとします。

- 2024年4月、自動車業界で使用されているマイクロコントローラー(MCU)に対する電圧グリッチ攻撃が、セキュリティ研究者らにより実証されました。 この脆弱性により、攻撃者は電源を操作することで読み出し保護（RDP）機能を回避でき、保護されたファームウェアにアクセスし、これらのMCUを使用しているシステムのセキュリティを侵害しました。研究者たちにより脆弱性を開示された製造元はそれを修正しました。[185]
- 2024年5月、さまざまな自動車のボディコントロールモジュール（BCM）に組み込まれた、パワーウィンドウや電動式ドアミラー、イモビライザーシステム、集中ドアロックなどを制御するMCUに対する電圧グリッチ攻撃を、セキュリティの研究者グループが実証しました。 この脆弱性を悪用し、16バイトのIDコード認証を回避することで、不正にファームウェアの抽出ができました。 攻撃者は、シークレットキーや車両制御機能などの機密情報にアクセスする可能性がありました。脆弱性は製造元に開示され、修正されました。[186]

- 2024年9月、200台を超える車両の走行距離計を不正に操作し、走行距離を合計で1,400万マイル以上減らした罪で、米国のカーディーラーが起訴されました。ツールを使用して、走行距離計の ECU 読み取り値を変更し、実際より少ない走行距離を登録書類に記載していました。各車両の走行距離は平均で65,000マイル減少されており、購入者を欺いていました。地元当局はこの詐欺を非難し、消費者や中古車市場への信頼に対する悪影響を強調しました。[187]

スマートモビリティデバイスとインテリジェント交通システム

渋滞の軽減、交通管理の改善、リアルタイムでの道路交通状況や気象データの共有、全体的な輸送効率の向上において、スマートモビリティデバイスとインテリジェント交通システムは不可欠です。 しかし、これらはスマートモビリティエコシステム内では、高リスクのターゲットとなっています。何百万人ものユーザーに関するリアルタイムでの位置情報、個人識別情報（PII）、支払い情報が含まれており、システムが攻撃されると安全性、データ、および運用の可用性が直接影響を受けます。
公共交通システム、電子ログ装置、信号や制御システムは、ランサムウェア攻撃、データ操作、物理的および遠隔操作に対して脆弱です。これらの脆弱性が悪用されると、交通の流れが妨害され、公共の安全が損なわれ、交通ネットワークが詐欺や妨害行為にさらされ、インフラや移動システムに対する国民の信頼が損なわれてしまいます。

- 2024年3月、ELD（電子ログ装置）がBluetoothやWi-Fi接続を介してアクセスされ、トラックが制御されたり、データが操作されたり、車両間でマルウェアが拡散されたりする可能性が、コロラド州立大学のセキュリティ研究者によって示されました。[188]
- 2024年4月、道路やハイウェイを走行中の運転者にリアルタイムで天候と交通状況を提供する米国のプロバイダーがランサムウェア攻撃を受け、スタッフはすべてのシステムをシャットダウンするという即座の保護措置を取ることを余儀なくされました。 この停止により、動的情報掲示板によるサービスの表示、公式ウェブサイト、およびリアルタイムカメラシステムが影響を受けました。[189]
- 2024年7月、宇宙線による自動運転システムや電気自動車への潜在的な脆弱性が、研究により、明らかにされました。宇宙線により、マイクロプロセッサやセンサーなどの重要な電子システムに混乱が生じ、誤動作が引き起こされる可能性があります。 このことで、車両の信頼性と安全性に重大なリスクがもたらされました。この問題を軽減するために、1つのコンポーネントが故障した場合でも機能を確保するためのモジュラー冗長性と、宇宙線による故障に対する耐性を高めるための検出および修正システムを研究者らは推奨しています。[190]

- 2024年9月、交通機関のチケットおよびパスサービスを専門とするコロンビアの企業が大規模なデータ侵害を受け、機密性の高い個人情報や車両データを含む80万件の文書が流出しました。 セキュリティ研究者は、同社の決済アプリデータを保存していたクラウドストレージの安全性の低さが原因で侵害が発生したことを明らかにしました。[191]
- 2024年9月、フィリピンを拠点とする高速道路運営会社がデータ侵害を受け、顧客の機密性の高い個人情報が露出した可能性がありました。運営会社は、サイバーセキュリティの専門家と関連当局と協力して、侵害の範囲を徹底的に調査し、現地の規制要件の遵守を強化し、侵害の影響を軽減するための対策を講じました。[192]
- 2024年10月、セキュリティ研究者がオランダで使用されている交通信号優先システムに重大なセキュリティ脆弱性を発見し、その結果オランダ政府は数千の信号機を、従来の短距離無線信号より安全なモバイルインターネット接続を使用するプラットフォームに置き換えました。[193]

モバイルアプリケーション

コネクティッドカーやSoftware Defined Vehicle（SDV）の増加により、OEMは車両コンパニオンアプリやサードパーティアプリを通じてリモートサービスや機能を提供できるようになっています。モバイルアプリケーションにより、ユーザーは車両の位置を追跡し、ドアを開け、エンジンを始動し、補助装置をオンにし、プレミアム機能に加入するなど、さまざまなことができます。

ドライバーにデジタル体験を提供する同じアプリもハッカーが悪用して、車両やバックエンドサーバーにアクセスされる可能性があります。 また、コンパニオンアプリケーションには、オープンソースの脆弱性、ハードコードされた認証情報、API/バックエンドサーバの脆弱性など、一般的なソフトウェアの脆弱性が存在する可能性があります。

OEMコンパニオンやスマートモビリティアプリも、個人情報の窃盗に使われる可能性があります。 ブラックハットアクターは、モバイルデバイスやアプリケーションサーバーの脆弱性を悪用して、認証情報を入手し、大規模に個人情報を侵害することができます。

- 2024年4月、セキュリティ研究者が、インドのオートバイメーカーのコンパニオンアプリに2つの脆弱性（CVE-2024-33308およびCVE-2024-33309）を発見しました。 これらの脆弱性により、リモート攻撃者が緊急連絡先機能を介して権限を得て、不十分に保護されたAPIエンドポイントを通じて機密情報を取得することが可能となっていました。[194]

- 2024年6月、日本のOEMの子会社でサイバーインシデントが発生し、OEMのコンパニオンアプリケーションのデータ漏洩につながりました。OEMは、人為的ミスにより消費者の個人識別情報（PII）が不正に開示されたと発表し、法執行機関による調査が開始されました。[195]
- 2024年6月、セキュリティ研究者は、同じインドのオートバイメーカーのコンパニオンアプリに別の脆弱性を発見しました。これはCVE-2024-35537として知られています。 研究者らは、このアプリがRSA鍵ペアを安全に処理していなかったため、攻撃者が復号化によって機密情報にアクセスできたことを発見しました。[196]

車両センサー

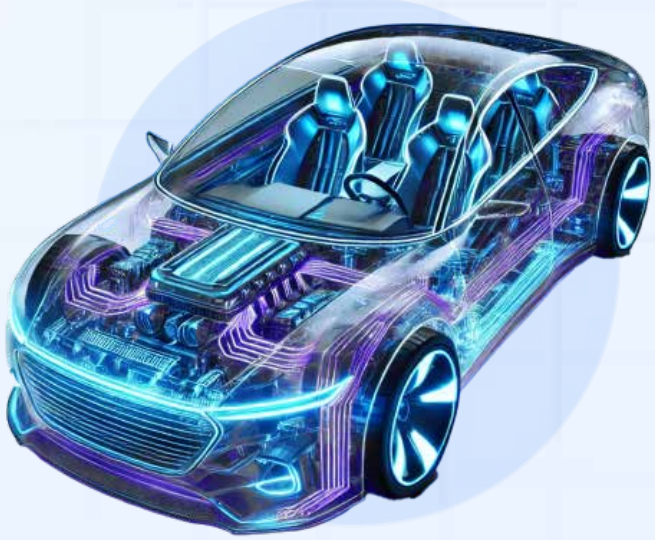
センサーは現代の車両において重要な役割を果たしており、物体検知、衝突回避、自動運転システムのためのリアルタイムデータ収集など、重要な機能を可能にしています。 ただし、センサーは、スプーフィング、ジャミング、データ干渉など、物理的およびリモート操作の両方に対して脆弱です。 これらの脆弱性は、データの誤った解釈、車両の安全性の低下、重要機能の混乱を引き起こし、コネクテッドカーや自動運転車の全体的な信頼性に影響を及ぼす可能性があります。

- 2024年2月、デューク大学のセキュリティ研究者は、使用中のレーダーシステムに関する事前知識なしに、自動運転車のセンサーシステムに幻覚を引き起こすことに成功しました。 MadRadarと呼ばれる攻撃のデモンストレーションの1つでは、研究者たちがドップラーレーダーシステムに幻覚を引き起こし、センサーから離れていく車両が方向を変え、正面衝突の危険がある方向に向かっていると誤って認識させました。[197]
- 2024年9月、バッファロー大学のセキュリティ研究者は、自動運転車のAIシステムに脆弱性を特定しました。特にミリ波レーダー、LiDAR、カメラに関するものでした。 彼らは、3Dプリントされたオブジェクトや金属箔、いわゆる「ブリックマスク」がレーダー検知を誤らせ、車両を見えなくする可能性があることを明らかにしました。 この研究は、自動運転車のセキュリティにおいて、より強力な防御が必要であることを浮き彫りにしました。[198]
- 2024年10月、CVE-2024-39081と名付けられた脆弱性がタイヤ空気圧モニタリングシステムで発見されました。この欠陥により、攻撃者はBluetoothを介して中間者攻撃を実行し、TPMSデータを操作して、アプリを通じてユーザーに偽のアラームを送信することが可能になります。タイヤの状態について誤った情報をユーザーに与え、車両の安全監視システムを妨害する可能性のある脆弱性は、重大な安全上の懸念を引き起こします。[199]

CANバス

CANバスは、現代の車両のさまざまな電子部品間の通信に不可欠であり、エンジン制御、ブレーキ、安全システムなどの機能のためのリアルタイムのデータ交換を可能にします。 しかし、CANバスは物理的および遠隔的な操作に対して脆弱であり、不正なメッセージの注入、盗聴、なりすまし攻撃などの脅威にさらされています。 これらの脆弱性は、車両の運転を妨げ、安全性を損ない、重要なシステムの不正な制御につながる可能性があり、コネクテッドカーの全体的なセキュリティと信頼性に影響を与えます。

- 2024年3月、研究者が日本の人気スポーツ用多目的車（SUV）のSecOCシステム（ECU200間のPDU通信の信頼性とフレッシュネスを確認するために必要な機能を提供する）をリバースエンジニアリングし、[200] 車両通信を保護する暗号鍵を抽出しました。さらに、パワーステアリングECUのデバッグポートをバイパスしてファームウェアを取得し、脆弱性を特定してRAM内の暗号鍵を見つけ出したのです。 これにより、レーンキープアシスト（LKA）やアダプティブクルーズコントロール（ACC）といったドライブバイワイヤ機能の制御が可能になりました。研究者は、自動車システムにおける強力な暗号化プロトコルと安全な鍵管理の重要性を強調しました。[201]
- 同じく2024年3月、英国の何千人もの車両所有者が車両盗難の増加をめぐり、日本の自動車OEMを相手取って訴訟を起こす資格を得ましたこの訴訟では、窃盗犯がCANバス内の特定のコンポーネントによってセキュリティを回避し、車に損傷を与えることなく盗むことができると主張しています。 12万台以上の車両が危険にさらされているとされ、訴訟では契約違反と消費者の権利侵害に対する損害賠償が求められています。[202]
- 同年4月には、研究者が、インドの複数の電動スクーターメーカーに影響を与えるサイバーセキュリティの脆弱性を発見しました。このセキュリティ研究では、リモートCANバスインジェクション攻撃を使用して、攻撃者がリモートで電動スクーターを停止できるようにしました。 セキュリティ研究者はサイバーセキュリティリスクを軽減するため、インドのOEMと当局に情報を提供しました。[203]



リモートキーレスエントリーシステム

現代の車両には、盗難防止として非常に強力な暗号とイモビライザーを備えたスマートキーフォブを含むリモートキーレスエントリーシステムが使用されています。しかし、車両の盗難や車上荒らしが増加の一途を辿っている現状では、このシステムが裏目に出ている可能性があります。

ワイヤレスキーフォブの操作により、ブラックハットアタッカーは自由に攻撃を仕掛けてきます。 一般に公開されているハッキングのチュートリアルや登録なしでオンライン販売されているデバイスにより、こうした攻撃が広く普及しているのです。

短距離無線送信機を搭載したワイヤレスキーフォブが車両に近づくと、暗号化された無線信号が受信ユニットに送信されます。無線信号を傍受して中継、再生、または妨害できるデバイスを利用して、キーフォブと車両間の通信は操作可能となります。

キーフォブのメカニズムと車両間の通信は、以下の手段で攻撃される恐れがあります：

「ライブ信号」を使用したリレー攻撃

リレー攻撃では、ハッカーはキーフォブの信号が圏外であっても、キーフォブと車両間の正常な通信を傍受します。 ハッカーは、車両の近くに設置された送信機やリピーターを使用して無線信号を増幅させることができます。そうすることで、メッセージを増幅して中継し、車両のロックを解除しエンジンを始動させます。 窃盗犯は、車両所有者の自宅内にあるキーフォブから発信される信号を傍受するために、このタイプの攻撃が増加傾向にあります。

保存された信号を用いたリプレイ攻撃

別のタイプのリレー攻撃では、ハッカーがキーフォブと車両間で送信される情報や通信を傍受し、後で使用するために保存します。関連する情報を取得した後、ハッカーはいつでも車のドアのロックを解除したり、エンジンを始動したりできます。

キーフォブの再プログラミング

一般的なデバイスと比較して、より高度で高価なデバイスは、キーフォブシステムを再プログラムすることができ、元のキーフォブを無効にします。その再プログラミング装置は、オンラインで合法的に入手可能であり、公認の整備士やサービスセンターで使用されています。一方で、この装置はOBDポートに接続できるため、自動車窃盗犯が比較的容易に車両をコントロールすることができるという懸念もあります。

キーフォブと車両間の通信妨害

自動車窃盗犯は、キーフォブと車両の通信を妨害する信号ジャマーという装置を使って、車両に侵入することができます。 この装置の影響で、所有者は車両をロックできなくなり、窃盗犯は自由に出入りできるようになります。

CAN インジェクションを使用したワイヤレスキーフォブ ECU 偽装

ハッカーが好む新たな攻撃手法として、CAN インジェクションがあり、窃盗犯が車両を盗むために広く使用されています。攻撃者は、CANワイヤに接続し、ワイヤレスキーフォブ ECU になりますCANインジェクターデバイスを使って、リモートキーレスエントリーシステム全体を回避することが可能です。

スマートフォンをデジタルキーにする Phone-as-a- Key（PaaK）

Phone-as-a- Key（PaaK）機能は、Bluetooth Low Energy（BLE）、近距離無線通信（NFC）、超広帯域無線通信（UWB）などの技術によって、スマートフォンをデジタルキーに変換します。 PaaK によって従来のキーフォブの必要はなくなり、利便性が高まる一方で、新たなサイバーセキュリティの脆弱性も生じます。具体的には、信号暗号化の脆弱性や、車両専用アプリの欠陥、スマートフォンのオペレーティングシステムの脆弱性などが挙げられ、車両への不正アクセスにつながる可能性があります。

リモートキーレスエントリーシステムに対する攻撃は2024年も注目を集め、車両盗難が増加し続けました。

- 2024年5月、米国の自動車 OEM（オリジナル・エクイップメント・メーカー）が、最新のスポーツカーモデルのキーフォブに欠陥があるとして提訴されました。この車両に関する盗難の増加は、キーフォブのセキュリティを破る方法を、ソーシャルメディア上の動画やオンラインガイドが指南していたことが原因と考えられています。 訴訟では、キーフォブが安全でない商用無線周波数で使用しているため、傍受されやすく、車両盗難を容易にしていると指摘されています。[204]
- 2024年5月、中国の研究グループが米国のEVの超広帯域（UWB）技術に脆弱性があることを発見し、それが原因でリレー攻撃を受けやすくなっていることが明らかになりました。 研究の結果、車両の超広帯域（UWB）システムの信号が、傍受、捕捉、そして操作される可能性を高めていることを発見しました。 この研究では、攻撃者は車両をだまして、キーフォブが近くにあると誤認識させ、さらに遠隔で車両のロックを解除し、エンジンを始動させることが可能であることを実証しました。 OEM は問題があることを認め、脆弱性について調査中であり、UWBのセキュリティを強化する対策に取り組んでいると報告しました。[205]
- 2024年7月、韓国のOEM電気自動車のキーレスシステムにおける既知の脆弱性を悪用する手法がソーシャルメディアで話題になり始めました。 あるソーシャルメディアアカウントは、エミュレーター装置と呼ばれる高度なツールを紹介しました。この装置は、無線通信を組み合わせて、車両のキーと車両自身の間の通信を傍受し、複製することができます。 この装置があることで、ハッカーは1分もかからずに車両のキーから発信される信号を模倣し、本物のキーを使うかのように車両のロックを解除し、エンジンを始動することが可能になります[206]
- 2024年9月、中国のセキュリティ研究者は、PhoneKeyシステムと車両との間の情報をプロトコルレベルで中継するBluetooth Low Energy（BLE）リレー攻撃を実演しました。 プロトコルベースのリレー攻撃は、攻撃者が世界中のどこにいても可能で、車両との物理的な近接を必要としないという利点があります。[207]
- 2024年11月、セキュリティ研究者らは、アジアの OEM 数社のリモートキーレスエントリー（RKE）システムに脆弱性があることを明らかにしました。 調査では、当該ブランドのRKEシステムは、安全性の低いローリングコード（通信の都度更新されるコード）の実装を悪用して不正アクセスを行う攻撃に対して、依然として脆弱であることが確認されました。脆弱性は、安全ではない暗号方式、古い暗号アルゴリズム、および不十分な対策が原因で生じています。[208]

Bluetooth

Bluetoothは、無線周波数を使って機器を接続し、データを共有する無線通信技術です。 Bluetooth Low Energy（BLE）は、デバイス間のデータ共有に使用される標準プロトコルで、ベンダーは数百万台の車両、住宅用スマートロック、商業ビルの入退室管理システム、スマートフォン、スマートウォッチ、ノートパソコンなどのロックを解除するための近接通信に採用されています。

- 2024年5月、スイスの電気自動車充電器にCVE-2023-0863およびCVE-2023-0864と識別される2つの脆弱性が発見されました。これらの脆弱性は、Bluetooth Low Energy（BLE）を介して悪用される可能性があり、不適切な認証や機密情報のクリアテキストでの送信が含まれます。その結果、充電ステーションの制御が奪取されるだけでなく、通信の盗聴や設定の変更が行われるリスクも生じました。[209]
- 2024年8月、セキュリティ研究者が主要OEMが使用するインフォテインメントシステムに重大な脆弱性を発見しました。 これらの脆弱性により、インターネット接続がなくてもAndroid Automotive OSを搭載した車両からGPS座標などの機密データを抽出することが可能であることが判明しました。
  また、これらの脆弱性により、悪意のあるUSBデバイスや、ブルースナーフィングを介してマルウェアが拡散することも可能になります。ここで、ブルースナーフィングとは、攻撃者がBluetoothを経由して、ペアリングされたデバイスに侵入するハッキング手法です。[210]
- さらに2024年9月、セキュリティ研究者が車両のスマートフォンキーシステムに対するBLE（Bluetooth Low Energy）リレー攻撃を実施し、物理的な近接をせずにリモートで解錠できることを実証しました。研究者はGattackerツールを使用し、暗号化や適切なペアリングメカニズムが欠如していた米国および中国の電気自動車（EV） BLEシステムの脆弱性を悪用しました。ただし、ペアリングPINを使用している車両は影響を受けませんでした。 調査結果は製造業者に報告されましたが、複数のサプライヤーへの依存関係のため、問題の修正には困難が伴うとされました。[211]

WI-FI

Wi-Fiは現代の車両においてシームレスな接続に不可欠であり、リアルタイムのデータ交換、インフォテインメント、無線によるアップデートを可能にします。しかし、車載Wi-Fiネットワークは、不正アクセス、データ漏洩、サービス拒否（DoS）攻撃などを含む、物理的および遠隔操作による脆弱性があります。 これらの脆弱性により、ユーザーはプライバシーリスク、不正行為、および車両運用に影響を与える可能性のある脅威にさらされる可能性があり、コネクテッドカーと広範な交通エコシステムのセキュリティと信頼性に影響を及ぼします。

- 2024年3月、セキュリティ研究者がアメリカのOEM 電気自動車に対して中間者(MiTM)フィッシング攻撃を実施しました。彼らは偽の「OEMゲスト」Wi-Fiネットワークを構築し、ユーザーを騙して偽のOEMページにログインさせました。これにより研究者は認証情報を取得し、二要素認証をすり抜けて、所有者に知られることなく新しいスマートキーを追加し、車両のロックを解除することができました。 研究者たちはセキュリティ強化のために物理的なカードキーの使用を提案しましたが、OEMは、このプロセスは意図的なものであり、セキュリティの欠陥ではないと主張しました。[212]
- 2024年8月、国際空港を含む主要な交通拠点を管理する米国の主要空港がサイバー攻撃を受けました。この攻撃により多数のシステムが混乱し、チェックインプロセスに深刻な遅延が生じ、フライト情報に不可欠なWi-Fiやディスプレイシステムが無効化されました。 港湾当局は連邦当局と共に攻撃を調査していますが、乗客データが漏洩したかどうかはまだ確認されていません。[213]

V2X攻撃は劇的に増加すると予想される

テレマティク、スマートモビリティ、車載/モビリティIoT、その他のサービスでは、コネクテッドカーがサーバー、アプリ、さまざまな車両コンポーネントとデータを共有する必要があります。
コネクテッドビークル・ツー・エブリシング（V2X）とは、既存のセルラーネットワークのインフラを活用して、車両、インフラ、その他のアクティブな道路利用者が常時通信できるようにする技術の総称です。 車両の接続には次の7つの主要なモードがあります。

V2I	**車両から インフラへ**	車両と道路インフラ間で無線データ交換し、事故、工事、駐車場などの情報を取得します。
V2V	**車両から 車両へ**	渋滞や事故を避けるために、車両間で位置情報を含むデータを共有します。
V2N	**車両から ネットワークへ**	車両、信号機、車線区分線、その他の道路インフラネットワークの間の通信。
V2C	**車両から クラウドへ**	車両とクラウドベースのバックエンドシステム間の通信により、車両はサービスやアプリケーション間で送信される情報やコマンドを処理できます。
V2P	**車両から 歩行者へ**	車両、インフラ、個人向けモバイル機器間の通信により、歩行者環境に関する情報を提供し、安全性、モビリティ、環境の向上を実現します。
V2D	**車両から デバイスへ**	車両とそれに直接接続する電気機器との間でデータや情報を交換します。
V2G	**車両から グリッドへ**	車両と送電網の間で双方向の電力フローが発生するため、悪用されれば都市や国の送電網全体に大きな問題を引き起こす可能性があります。

> ***数年以内に、車両はAPI、センサー、カメラ、レーダー、モビリティIoTモジュールなどを通じて常に周囲と通信し、情報交換するようになり、環境からのさまざまな入力を処理することで車両の運転を向上させるようになります。***

最も重要な追加機能は、車両が道路上の他の車両やデバイスと通信し、EV充電器や道路インフラなどの外部ソースからデータを受信する機能です。

車両は、車線に進入してくる可能性のある歩行者や自転車、前方の交通状況、交差点の交通照明や制御システムからのデータなどを考慮し、周囲の環境全体と情報交換することが期待されます。

V2X技術の一部の要素は、現在すでに使用されています。V2Xは、先進運転支援システムの重要な構成要素であり、高速道路交通システムとセンサーを使用して自律走行とスマートシティを強化します。OEMも、V2X技術を使用して、車両にリアルタイムの道路情報を提供することで交通渋滞を軽減しています。V2Xのおかげで、ドライバーはより安全に運転でき、詳しい情報に基づいた決定を行うことができます。 また、車両は速度や位置などのデータをリアルタイムで共有することが可能になり、ドライバーに潜在的な事故を警告することで道路の安全性が向上します。 さらに、Vehicle-to-Home（V2H）などのV2X EV充電技術により、EVは需要が高い時間帯に放電し、低需要・安価の時間帯に充電することで電気料金を削減できます。

V2Xの未来は、DSRCやセルラーV2X(C-V2X)など、過去数年間にわたってテストされてきた新しい無線通信技術に依存することになります。C-V2Xは、3GPP標準の4G LTEまたは5Gモバイルセルラー接続を使用して、車両、歩行者、信号機などの路側交通管制装置間でメッセージを交換します。[214] DSRCとC-V2Xの両方がV2Xの未来を可能にしますが、C-V2XのLTE（Long-Term Evolution）の使用はコネクテッドカーのエコシステムを大きく変える可能性があると考えられています。 既存のセルラーインフラを利用できるため、普及を加速させるために必要な労力が軽減されると同時に、高密度な場所での高速通信が保証されることになります。[215]

2023年4月、FCCは、高速道路交通システム(ITS)規則の最終的な国家規定に先立ち、コネクテッドカー向けのC-V2X技術を承認しました。 FCCの公安・国土安全保障局、エンジニアリング・技術局、無線通信局は、5.895~5.925GHz帯の周波数帯の上位30MHz帯におけるC-V2X技術の展開を許可するため、いくつかのFCC規則の全国的な適用免除を求める自動車メーカー、機器メーカー、州運輸省から提出された共同申請を受け入れました。[216]

FCCは、州運輸局を含む組織に対して、2023年4月に14件、2023年8月に17件、2023年11月に8件、2024年4月に11件の適用免除申請を承認しました。 2024年4月の時点で、合計50件の適用免除が認められています。[217]

過去5年間、米国運輸省（DOT）は、FHWAターナー・フェアバンク高速道路研究プログラムを通じて、V2X技術の研究と開発に6,150万ドルを投資しました。さらに、2024会計年度に予算化された後続研究プロジェクトに1,250万ドルを投資しました。[218]

2023年11月、米国運輸省は、すべての新型軽自動車に専用狭域通信（DSRC)-V2V通信技術の搭載を義務付けるという以前の提案を、正式に撤回すると発表しました。これは、C-V2X規格と互換性のないDSRCが、移行期間後に5.9 GHz帯での使用を許可されなくなるためです[219]

2024年8月、米国運輸省は全国的にV2X技術を展開するためのフレームワークを立ち上げ、正式に全国V2X展開計画を発表しました。[220]

この計画は、米国運輸省のビジョン、魅力的な目標、マイルストーンを設定し、あらゆるレベルの政府、公共機関、民間部門を含む業界関係者に行動を呼びかけています。 魅力的な目標やターゲットは、法的、規制的義務や、特定の連邦政府の資金を意味するものではありません。要するに、この計画は、連邦政府のリーダーシップを示し、政府と産業界が協働できる道筋を提供します。

この計画に加えて、米国運輸省の連邦道路管理局（FHWA）は、接続性と相互運用性のある車両技術を推進するために、「コネクティビティで命を守る:V2X展開の加速」プログラムの下で6,000万ドルの助成金を交付すると発表しました。これらの助成金は、アリゾナ州、テキサス州、ユタ州、コロラド州、ワイオミング州を含むいくつかの州での大規模展開を実施するV2X技術の資金として使用され、V2X技術の新たな展開を加速・促進するための全国的なモデルとしての役割を果たします。

05.

ディープウェブと ダークウェブからの サイバー脅威

サイバー脅威インテリジェンスは、ディープウェブとダークウェブのリスクを明らかにし、自動車およびスマートモビリティの関係者が、増大するサイバーリスクを積極的に軽減できるよう支援します。

ディープウェブとダークウェブとは何なのか?

インターネットには複数の層があり、インデックス化されていないものもあります。 インターネットには クリアウェブ、ディープウェブ、ダークウェブの3つの主要な層があります。 各層へのアクセスには、異なるノウハウとツールが必要です。例えば、ダークウェブのフォーラムでは、ユーザーは固有のリソースロケーションアドレスを知っている必要があります（ダークウェブにはドメイン名が存在しないため）。そのため、特別なブラウザを使用し、多くの場合、サイト管理者に特定のトピックに精通していることを示さなければ、アクセス権を得ることができません。

インターネットの第1層はクリアウェブ、あるいはサーフェスウェブです。インターネットの中で最も小さく、かつ最も身近な層であり、アクセスに必要なのはウェブブラウザのみです。[221] この層のウェブでは、誰もが知る一般的な検索エンジンによって情報がインデックス化され、非常にアクセスしやすく、人々に信頼され毎日利用されています。.

クリアウェブ

- *自動車およびサイバー関連の公共メディア報道とニュース*
- *検証済み研究者の公開ブログとレポート*
- *学術論文や研究論文*
- *自動車愛好家とフォーラム*
- *ソーシャルメディア*
- *コード共有サイト*

インターネットの第2層はディープウェブで、インターネット上の全ウェブページの96%を占めています。[222] この層のウェブデータは検索エンジンによってインデックス化されていません。これは、ログインが必要であるか（例えば ペイウォールなど）、または所有者がウェブクローラーによるインデックス化をブロックしているためです。 一般の人にとってのディープウェブには、有料コンテンツ、サブスクリプションウェブサイト、非公開グループ、および企業の非公開ウェブサイトが含まれます。 ハッカーにとってのディープウェブには、匿名かつ挑発的な、違法性が疑われるコンテンツを掲載する画像掲示板も含まれています。

ディープウェブ

- *プライベートSNSグループ*
- *プライベートメッセージアプリ*
- *貼り付けサイト*
- *非公開の自動車チューニングやハッキングフォーラム*

インターネットの最後の層である第3層はダークウェブで、悪意のある活動や犯罪に利用され、盗まれたデータが流通している非常に隠蔽性の高いウェブ層です。 ダークウェブのフォーラムにアクセスするには、ユーザーは特殊なブラウザ（Torなど）を使用し、サイトのURLを知っている必要があります（ダークウェブには通常のドメイン名が存在しないため）。また、多くの場合、サイト管理者に特定のトピックに精通していることを示さなければ、アクセス権を得ることができません。 フォーラムやページはモデレーターによって管理されていることが多く、ユーザー間の透明性の欠如や、フォーラム内の情報の種類が故に、常に高い疑惑の目が向けられています。

ダークウェブ

- *悪意のある貼り付けサイト*
- *違法なマーケットプレイス*
- *画像掲示板*
- *非公開のハッキングフォーラム*
- *違法な依頼サービス*
- *悪意のある行為者が利用する正規のプラットフォーム（Tor、Telegramなど）*

ダークウェブのハッカーは、匿名性を維持するために、多くの場合、プロキシサーバーとTorブラウザを使用します。プロキシチェーンと呼ばれるツールを使用して、複数（通常は3〜5台）のプロキシサーバーをチェーン接続します。 その結果、攻撃者のパケットは複数のプロキシサーバーを経由して送信されることになります。 ハッカーは、意図的に競合国のプロキシサーバーを使用し、セキュリティ情報（プロキシログなど）の共有を阻止することで、自分たちの特定をより困難にしています。

2024年、UpstreamのAutoThreat®チームは、ディープウェブおよびダークウェブの脅威アクターのマッピングと分析の範囲を大幅に拡大し、2023年に300件だったアクティブな脅威アクターを1,133件まで含むようになりました。

調査結果は、OEM、Tier-1サプライヤーおよびTier-2サプライヤー、EV充電のステークホルダー、さらにスマートモバイルIoTデバイスとプラットフォームを対象としていました。 このデータと、2024年のディープウェブおよびダークウェブ上のサイバー活動の43%以上が、数千から数百万のモビリティ資産に影響を与える可能性があったという事実を併せると、自動車とモビリティのステークホルダーは、サイバー脅威インテリジェンスに関する深い可視性と洞察にアクセスし、積極的に自身を守る必要があります。

2024

2024年のディープウェブおよびダークウェブ上のサイバー活動の

43%

が、数千から数百万のモビリティ資産に影響を与える可能性がありました

表面下の世界：ディープウェブおよびダークウェブ上のサイバーリスクの解明

一部の推計によると、インターネットの大部分は非公開であり、ディープウェブおよびダークウェブがその95〜99%を占めています。[223] ディープウェブおよびダークウェブのフォーラム、マーケットプレイス、モバイルメッセージングアプリケーション、ペーストサイトなどで、自動車関連のさまざまなコンテンツを見つけることができます。

消費者はウェブフォーラムを利用して、OEMが共有したがらない情報を見つけ出しています。具体的には、車両の違法改造や不正なシステム操作に役立つ情報などです。さらに、マーケットプレイスでは、メーカーの規約や契約に違反して、自動車部品、コンポーネント、チップ、ソフトウェア、その他のアイテムが販売されています。 非常に複雑な自動車技術を改ざんする危険性を認識せずに、こうした行為に及ぶ車両所有者は多く存在します。

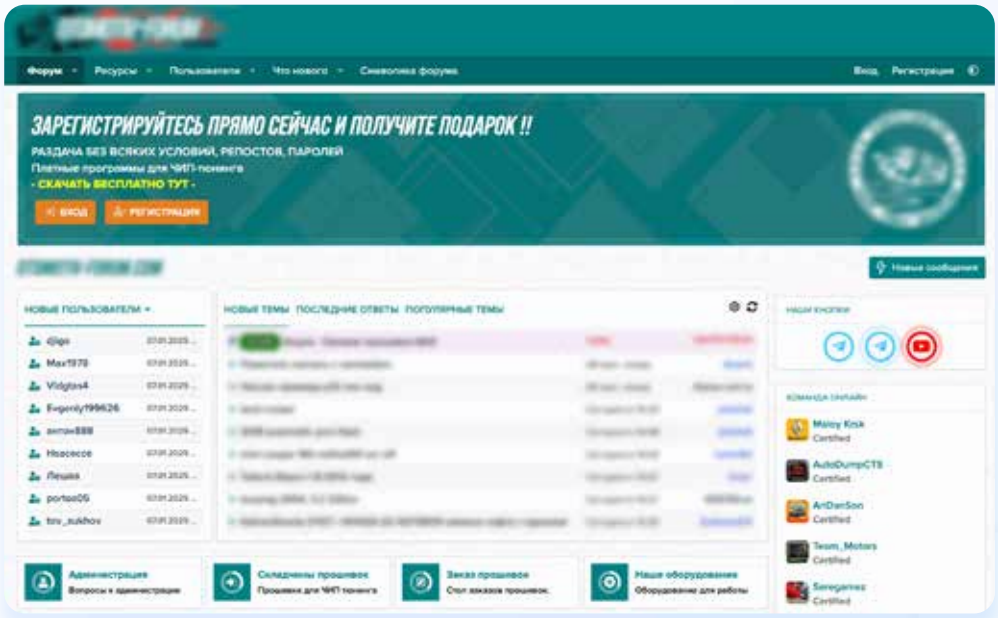
こうした行為は、自動車関連のステークホルダーや保険会社に影響を与える可能性があります。 不正改造された車両は、あたかも正当であるかのように虚偽の情報を報告する恐れがあります。極端なケースでは、脅威アクターは、車両認証に使用されるデータをリバースエンジニアリングすることで、OEMや保険会社のサーバーにアクセスすることもできます。

フォーラム

ディープウェブおよびダークウェブ上には、自動車関連のフォーラムが存在します。そこでは、自動車ソフトウェアの共有や販売、チップやエンジンのチューニング、インフォテインメントのクラッキング、診断機器のクラッキング、リバースエンジニアリング、キーフォブの改造、イモビライザーのハッキングなどを扱っています。

プレミアム機能へのアクセスや修理権の主張など、さまざまな理由から、車両のセルフプログラミングについて質問する人は珍しくありません。さらに、ECUのリマッピングレッスン、ガイド、ソフトウェア、およびチューニング済みファイルのデモがすぐに利用可能となっています。

2024年8月、Upstreamの AutoThreat® PROチームは、ある脅威アクターを発見しました。このアクターは、人気のあるディープウェブ上の自動車関連フォーラムで、クラックされた診断ソフトウェアや診断ツールへの不正アクセスを提供していました。これらのツールを使用すると、通常は認定ユーザーやサービスセンターに限定されている高度な診断、ファームウェアの更新、カスタム設定などを、一般ユーザーが実行できるようになります。この不正ソフトウェアは標準的なセキュリティプロトコルを回避し、車両システムや重要な機能への広範囲なアクセスを可能にします。



ディープウェブの
自動車フォーラムの例

Source: Upstream Security

ディープウェブおよびダークウェブのフォーラム上でクラックされた診断ソフトウェアやツールの増加は、重大なリスクをもたらします。OEMのセキュリティ対策が脆弱化し、複数のプラットフォームにわたるコネクテッドカーシステムが危険にさらされます。

マーケットプレイス

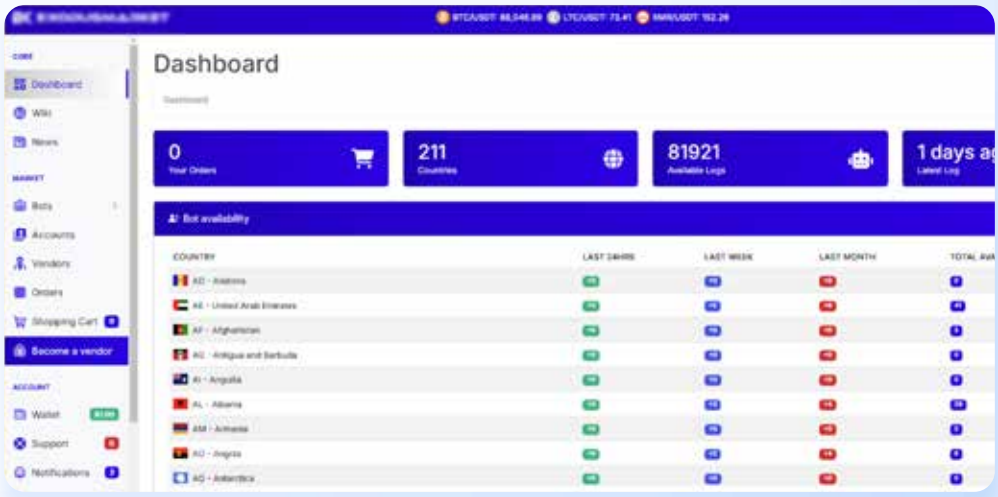
ダークウェブのマーケットプレイスは、Torや I2Pなどの特殊なブラウザと、アクセスするための登録が必要な商用ウェブサイトです。 これらは主に闇市場として機能しており、薬物、武器、サイバー兵器、盗難データ、偽造文書、その他の違法な商品に関わる取引を仲介しています。[224]

自動車関連のダークウェブマーケットプレイスのリストには、車両関連の「製品」やサービスを提供するものもあります。例えば、偽造文書や自動車アプリケーション、スマートモビリティサービスのユーザー認証情報など（例：OEMのコネクテッドカーサービス、シェアモビリティサービス）です。

ダークウェブのマーケットプレイスでは、自動車関連の議論や商品が数多く見られます。

- インフォテインメントのハッキング、CAN バスのリバースエンジニアリング、チップチューニング、ソフトウェアのハッキングや違法アップグレードに関する説明書やガイド
- データ侵害で盗まれたOEM関連情報や認証情報の売買・公開
- 車両盗難や改造用ツールの情報や売買（キー信号グラバー、キーフォブプログラマー、GPSジャマー、レーダー探知機など）
- カーシェアリングやライドシェアリングのアカウントに関連するハッキングや不正行為
- 偽造運転免許証や自動車保険の売買

2024年6月、Upstreamはブラックハットの脅威アクターが提供するダークウェブのマーケットプレイスで、複数のOEMやディーラーから流出した認証情報を発見しました。[225]



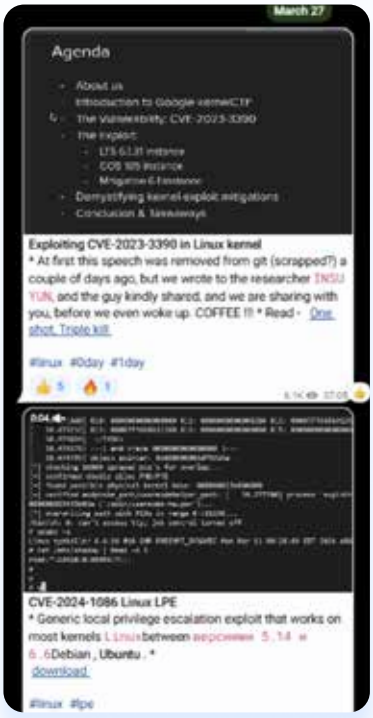
ディーラーの認証情報が流出したダークウェブマーケットプレイスの例

Source: Upstream Security

メッセージングアプリケーション

モバイル メッセージング アプリケーションは、違法行為に使用されることがますます増えています。Telegram、Discord、Signal、WhatsAppのような人気のあるメッセージングアプリケーションは、ハッキング手法の共有、盗まれたクレジットカード、アカウント認証情報、脆弱性の悪用、漏洩したソースコード、マルウェアの取引に積極的に利用されています。このようなアプリケーションは、秘匿性が高くアクセスしにくいダークウェブのフォーラムに取って代わりました。

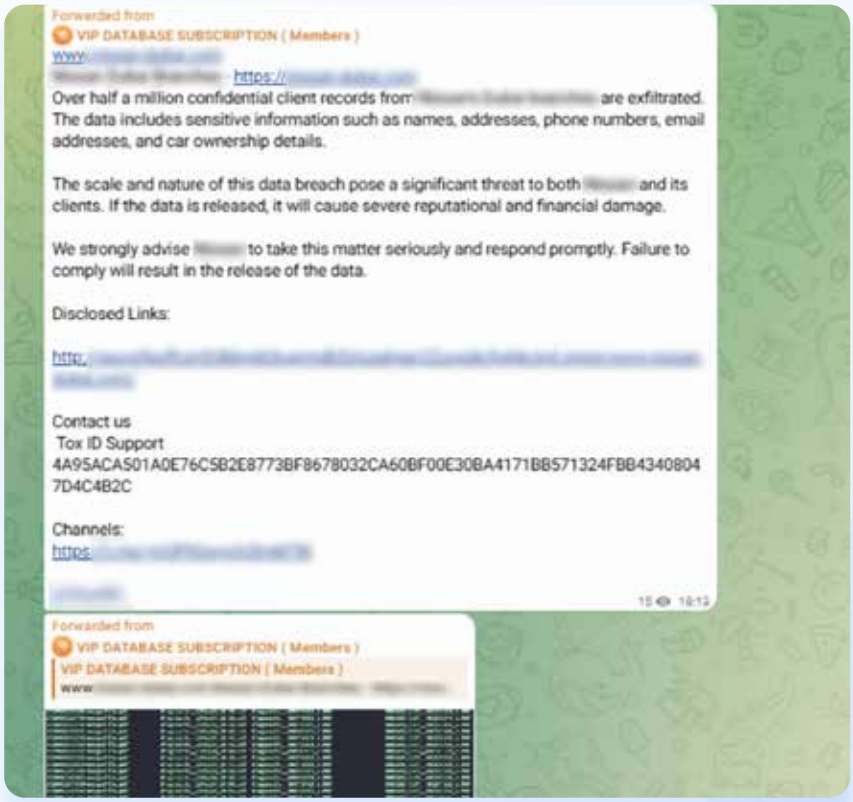
2024年3月、Upstreamは1万6000人以上のメンバーを持つサイバー犯罪のTelegramチャンネルを特定しました。このチャンネルには、多くの大手OEMに影響を与えるLinuxカーネルの脆弱性を突いた不正に関する情報が公開されていました。[226]



Source: Upstream Security

サイバー犯罪Telegramチャンネルで発見されたエクスプロイト(脆弱性を利用した不正プログラム)

2024年10月、Upstreamは、ランサムウェアのTelegramチャンネルで、日本のOEMを標的にしたランサムウェア攻撃の結果を紹介する投稿を発見しました。盗まれたデータには、氏名、住所、電話番号、メールアドレス、車両所有情報など、機密性の高い顧客個人識別情報（PII）が含まれていました。[227]



Source: Upstream Security

OEMから盗まれたデータに関連するTelegramメッセージの例

ディープウェブとダークウェブの脅威アクター

ホワイトハット（セキュリティ研究者）

サイバーセキュリティ研究者は、技術的専門知識を活用して、組織内および業界全体の脆弱性を明らかにします。 効果を持続するためには、最新の攻撃手法、新たなトレンド、および実現技術の進歩について常に情報を更新し続ける必要があります。

多くの研究者は、脆弱性の悪用や特殊な車両ツールキットなどの研究成果をGitHub のようなプラットフォームで公開しています。 この公開性は協力と技術革新を促進する反面、意図せずに悪意のある者たちにこれらの洞察へのアクセスを提供し、サイバーセキュリティのリスクを増幅させる可能性があります。

2024年12月、あるセキュリティ研究者はLinuxカーネルの脆弱性を標的とするエクスプロイトを公開しました。これにより、影響を受けるシステムで特権昇格と不正な制御が可能になりました。[228] その後まもなく、この脆弱性は数万人のメンバーを有する悪意のあるTelegramチャンネルで共有されましたが、その多くが悪意を持ったブラックハットの攻撃者でした。[229] このエクスプロイトがチャンネルを通じて広く拡散されたことで、特に様々なOEMが使用しているLinuxベースのインフォテインメントシステムに対する攻撃に利用される危険性が大幅に高まっています。このような攻撃は、不正アクセス、データ漏洩、または重要な車両機能の停止につながる可能性があります。

ブラックハット

ブラックハットハッカーは悪意を持ってサイバーセキュリティを侵害し、ダークウェブのフォーラムやマーケットプレイスで幅広い活動に参加しています。 ブラックハットハッカーが、ディープウェブやダークウェブのフォーラムで、遠距離の脆弱性に対するエクスプロイトを公開すると、他の多くの脅威アクターに対し、車両を衝突させたり、制御することができるエクスプロイトを開示することになります。そして、それは、大規模な深刻な安全上のリスクを引き起こす可能性があります。

2024年8月、Upstreamは、ブラックハットハッカーがサイバー犯罪フォーラム上で、複数のOEMに影響を及ぼす可能性のあるOpenSSHの脆弱性を悪用するエクスプロイトを公開したことを突き止めました。 この脆弱性により、コード実行、サービス拒否、特権昇格が可能となり、特に複数のOEM製インフォテインメントシステムが影響を受ける可能性があります。 さらに、このエクスプロイトにより、攻撃者は影響を受けるシステムに対してリモートでコマンドを実行できる可能性があります。

グレーハットは、ブラックハットとホワイトハットの境界線を曖昧にする

伝統的に、「ブラックハット」という用語は脆弱性を悪用しようとする悪意のある行為者を表し、一方「ホワイトハット」という用語は防御を改善するために働くサイバーセキュリティ研究者を表します。 しかしながら、自動車業界では、よりコネクテッド化とソフトウェア定義化が進むにつれて、この区別が徐々に薄れてきている。これにより、車両を改造したりコンポーネントをジェイルブレイクしたりする消費者も含む「グレーハット」の関与が増加しています。

2024年3月、Upstreamは車載インフォテインメント（IVI）システムのジェルブレイク方法に関するガイドラインがディープウェブのプラットフォーム230で公開されたことを明らかにしました。[230]

その指示書には、OTAアップデートをブロックする方法、ユーザーが未承認のサードパーティアプリをサイドロードする方法、ハンズフリー車線中央維持機能などの一部の非対応機能を保持する方法、そして将来のアップデートで導入される可能性のあるソフトウェア制限を防ぐ方法が概説されていました。 2つの方法が説明されました。1つはIVIブラウザから直接インストールされたアプリマネージャーを使用する方法、もう1つはUSB経由でファイルをサイドローディングする方法です。 両方のアプローチは、システムの制限を回避して隠された機能のロックを解除しました。

影響を受けたインフォテインメントシステムでOTAアップデートをブロックする手順中に表示される警告プロンプト

Source: Upstream Security

詐欺師

詐欺師は通常、診断ツール、ソフトウェア、チップチューニングサービス、走行距離修正サービスなどの売買にディープウェブを利用しています。詐欺師は、金銭的利益から競争的または悪意のある目的でシステムの脆弱性を悪用することまで、さまざまな動機に駆り立てられています。これらの犯罪者は、しばしば自動車ローン詐欺、保証金詐欺、偽造部品の流通など、高額な機会を標的にします。彼らはコネクテッドカーシステムやサプライチェーンプロセスの弱点を利用します。 コネクテッドカーやソフトウェア定義車の台頭に伴い、プレミアム機能へのアクセスを得るためにデジタルプラットフォームを利用する機会が増えています。 彼らの行為は、金銭的な損失をもたらすだけでなく、消費者の信用を損ない、安全性と運用の信頼性を危うくします。

2024年3月、ディープウェブの有名な脅威アクターが、特定の車両用の診断ソフトウェア、電子部品カタログ、修理マニュアルへの不正アクセスを提供し、TeamViewerを介したリモートインストールを行っていました。この詐欺師は、自動車フォーラムでの活発な関与で知られ、OEMの利用規約、ポリシー、安全対策231を回避しながら、さまざまな不正サービスを提供していました。[231]

The fraud operators' website

Source: Upstream Security

車愛好家

多くの車好き—車両とその動作に情熱を持つ人々—がディープウェブ上の様々な自動車フォーラムで活動しています。 彼らはアドバイスを提供し、質問をし、自分の車で見つかった問題やバグについて議論し、さらには自動車関連ファイルや非公式のソフトウェアアップデートへのリンクを共有します。

車愛好者がフォーラムに投稿する情報は、2つの懸念点があります。第一の懸念は、悪意のある脅威アクターがしばしばこれらのフォーラムを監視し、報告されたバグや脆弱性を自身の利益のために悪用することです。第二の懸念点は、これらのプラットフォームで共有されたファイルやリンクはしばしば信頼性がなく、マルウェア、スパイウェア、ランサムウェアが含まれている可能性があり、セキュリティを脅かしたり、保証を無効にする恐れがあるということです。

2024年6月、ある車愛好家がディープウェブのプラットフォームでジェイルブレイクを公開し、広く使用されている自動車のインフォテインメントシステムにサードパーティアプリをインストールできるようにしました。この活発な愛好家は、豊富な技術知識と経験を持ち、フォーラムで公式アプリのインストール制限を回避するための技術ガイドや方法を共有しています。この問題は、自動車システムを不正な改造から保護することの課題が増大していることを浮き彫りにしています。不正改造は、コネクテッドビークルプラットフォームに潜在的な脆弱性をもたらす可能性があります。

新しい自動車とスマートモビリティの収益モデルが危険にさらされています。

脅威アクターらの、セキュリティの回避やジェイルブレイクによるプレミアム機能の不正利用がますます増えています。車両やデバイスのサイバーセキュリティや、データを活用した収益化にも多大なリスクをもたらしています。

2024年5月、有名な脅威アクターが、一部の電気自動車向けのファームウェアの改変など、許可されていないリモートおよび非リモートサービスを提供しました。[232] この脅威アクターによって提供されたリモートサービスには、特定の車両モデルに対するルートアクセス機能が含まれており、隠れた機能の有効化や有料サブスクリプションを免れることを可能にしました。追加サービスには、地域固有の設定調整、エアバッグなどの安全システムの無効化、診断ソフトウェアへの不正アクセスの提供などが含まれていました。

2024年9月、Upstreamは、人気の脅威アクターが、LANアクセスのロック解除とSSHベースのルート権限を持つ改造されたインフォテインメント・モジュールを販売しているのを追跡しました。[233] 脅威アクターによると、これらの改造ユニットは複数の国に出荷可能で、OEMが制限をしている機能に対する高度なアクセスも可能になるとのことです。

> ***こうした行為は、自動車業界が直面している大きな課題を浮き彫りにしています。それは、コネクテッドカーシステムを、不正な改造や、ファームウェアの変更、診断アクセスの拡大といった脅威から守る事です。***
> ***また、これは、OEM各社のプラットフォームにおける現在のサイバーセキュリティ対策の堅牢性についても、重要な課題を投げかけています。***

脅威アクターが特定のIVI、ECU、TCUに関する専門知識を獲得するにつれ、自動車業界はOEMとサプライチェーンにとってのディープウェブとダークウェブの脅威状況を把握し、それらに対する防御を強化するためのセキュリティプロトコルを確立することが極めて重要になります。

ランサムウェア攻撃者が自動車関連企業を標的に、ディープウェブとダークウェブを利用

悪意のある攻撃者は、自動車およびモビリティ関連の利害関係者（OEM、サプライヤー、さらにはEV充電インフラを含む）をランサムウェア攻撃の標的にするケースが増えています。 サプライチェーンのどの要素が狙われても、OEMやサービスプロバイダー、スマートモビリティのデバイスやアプリケーションにリスクをもたらす可能性があります。

> ***ランサム攻撃を受けると、運用や生産に深刻な影響がでるだけでなく、顧客の機密情報やシステムの認証情報などを流出する危険性もあります。***

恐喝して金銭を要求するために、攻撃者は通常ダークウェブ上に「リークサイト」を保有しています。 ここでは盗まれたデータが公開され、攻撃や被害者に関する情報が共有されます。

2024年、ランサムウェア攻撃とデータ流出サイトが大きなニュースとなりました。以下にいくつかの注目すべき攻撃を挙げます：

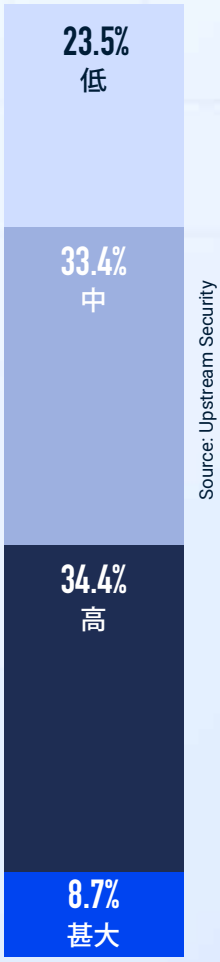
- 2024年7月、二輪車および商用車の大手メーカーがランサムウェア攻撃の標的となりました。 脅威アクターは、個人情報や機密保持契約書を含む機密性の高い企業データを流出させたと主張しました。身代金の期限が切れた後、グループはダークウェブのプラットフォームに盗んだデータを公開しました。[234]
- 2024年10月、有名なディーラーがロシアを拠点とするランサムウェアグループの被害に遭いました。 攻撃者は二重恐喝戦術を用い、請求書、会計記録、個人情報、雇用契約書、証明書、内部文書などの機密性の高い企業データを流出させました。 身代金支払いの期限が過ぎると、グループは攻撃を激化させ、盗んだデータをダークウェブのプラットフォームで公開しました。[235]

脅威アクターは依然として大規模な攻撃とその影響に重点を置いています

ディープウェブとダークウェブにおける脅威アクターの動向を分析し、そのサイバー活動がもたらす影響を評価することは不可欠です。Upstream社は2023年にはディープウェブとダークウェブ上で最も活発な300の脅威アクターを対象とした調査を開始しましたこの調査により、大規模なサイバーインシデントへの移行が明らかになりました。2023年のインシデントの約65%が数千から数百万のモビリティ資産に影響を与え、48%が複数のOEMや自動車サプライヤーを標的にしていました。[236]

2024年に当社の調査範囲は大幅に拡大しました。リスクの増大、標的となるモビリティ資産の追加、そして技術の進化を背景に、1,133の活動中の脅威アクターを調査対象に含めるようになりましたこの多様なアクターには、ブラックハット、ホワイトハット、不正行為者、自動車関連の不正行為者、そして自動車愛好家が含まれていました。この広範な分析によると、ダークウェブのサイバー活動の43%以上が数千から数百万のモビリティ資産に潜在的な影響を与える可能性があり、50%が複数のステークホルダーを標的にしていることが示されました。

2024年のディープウェブとダークウェブ活動の規模別内訳



Source: Upstream Security

2024年のディープウェブとダークウェブの脅威アクターの標的内訳

50.0%
単一のOEM/ステークホルダー

10.8%
複数のOEM/ステークホルダー

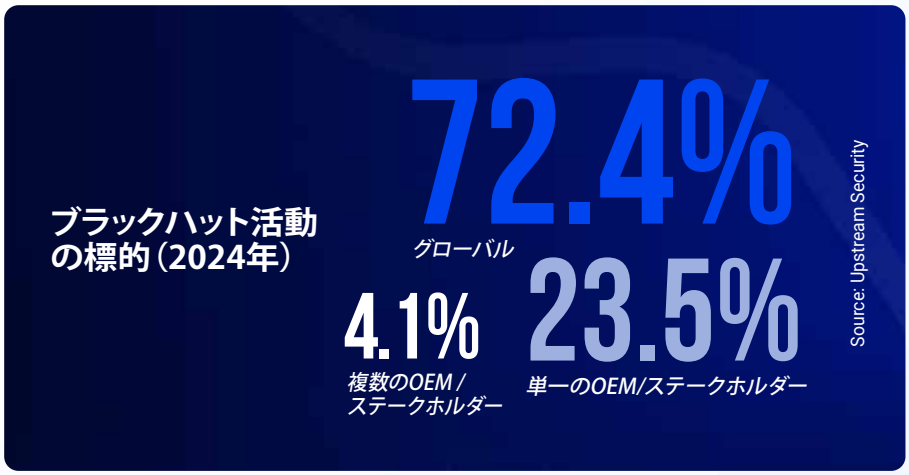
39.2%
グローバル

Source: Upstream Security

ディープウェブとダークウェブにおけるブラックハット活動に迫る

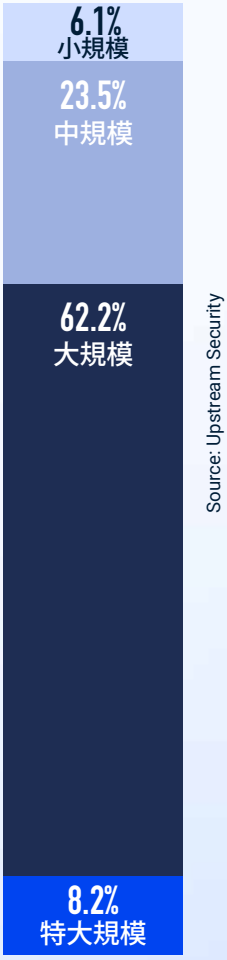
ディープウェブとダークウェブにおけるブラックハット活動を詳しく調べると、リスクが急速に高まりつつあることが分かります。

2024年には、ブラックハット活動の70%以上が大規模、又は特大規模の影響を及ぼし、76%以上が世界規模で複数のステークホルダーを巻き込んでいます。[237]

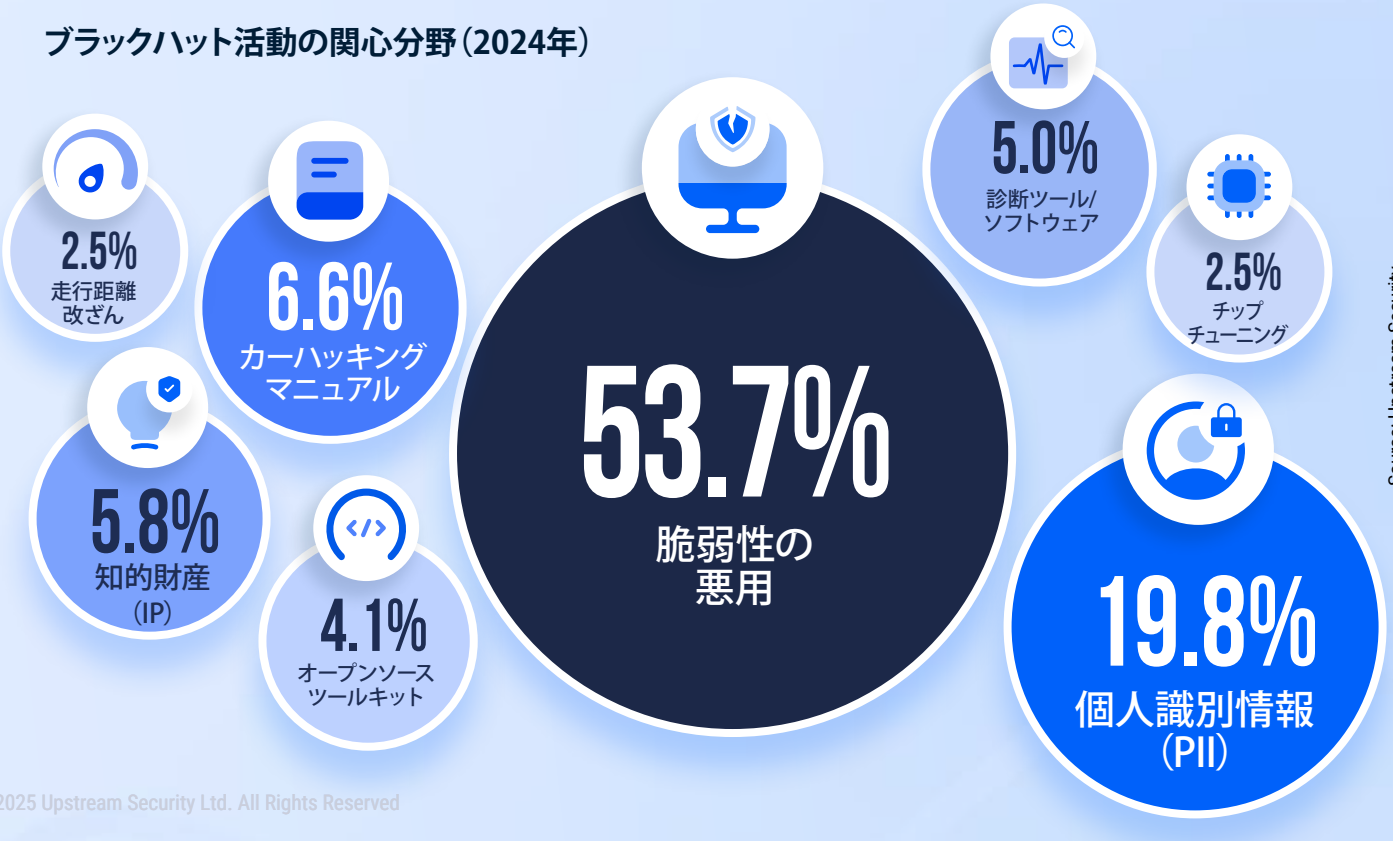


ブラックハットの関心領域を分析すると、その活動範囲と影響力を拡大し続けているのが分かります。活動の約54%が脆弱性の悪用関連、20%が機密性の高い個人情報へのアクセス取得、6%が知的財産の盗用、残りの20%が車両操作関連（例：車両ハッキングマニュアル、診断ツール/ソフトウェア、オープンソースツールキット、走行距離の改ざん、チップチューニング）となっています。[238]

潜在規模別に見たブラックハット活動（2024年）

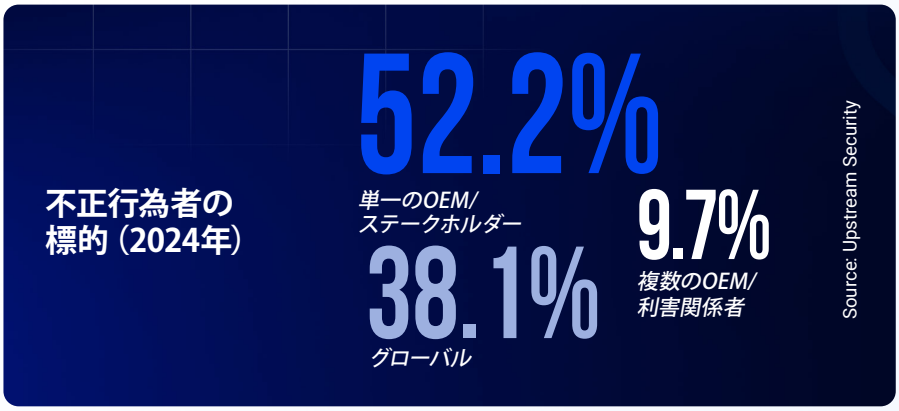


ブラックハット活動の関心分野（2024年）



深刻かつ大規模な影響を及ぼす不正行為者

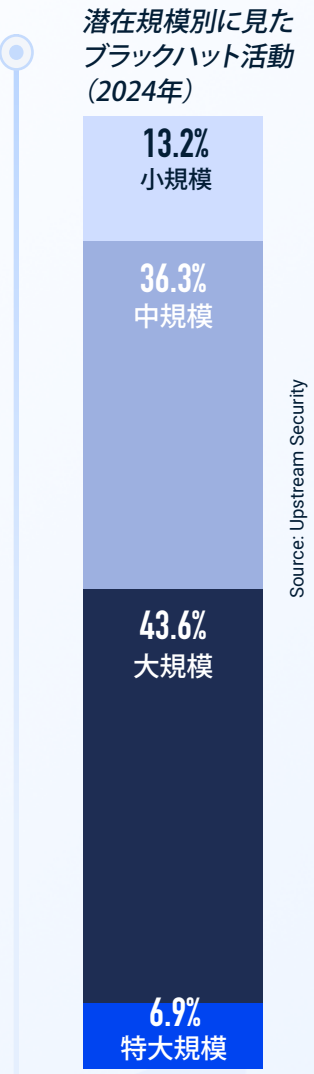
ディープウェブ及びダークダークウェブの不正行為者も、深刻かつ増大する脅威となっています。2024年には、不正行為者の活動の50%以上が大～特大規模の影響を及ぼし、48%が複数のOEMに関与、あるいは世界的範囲に及んでいました。[239]



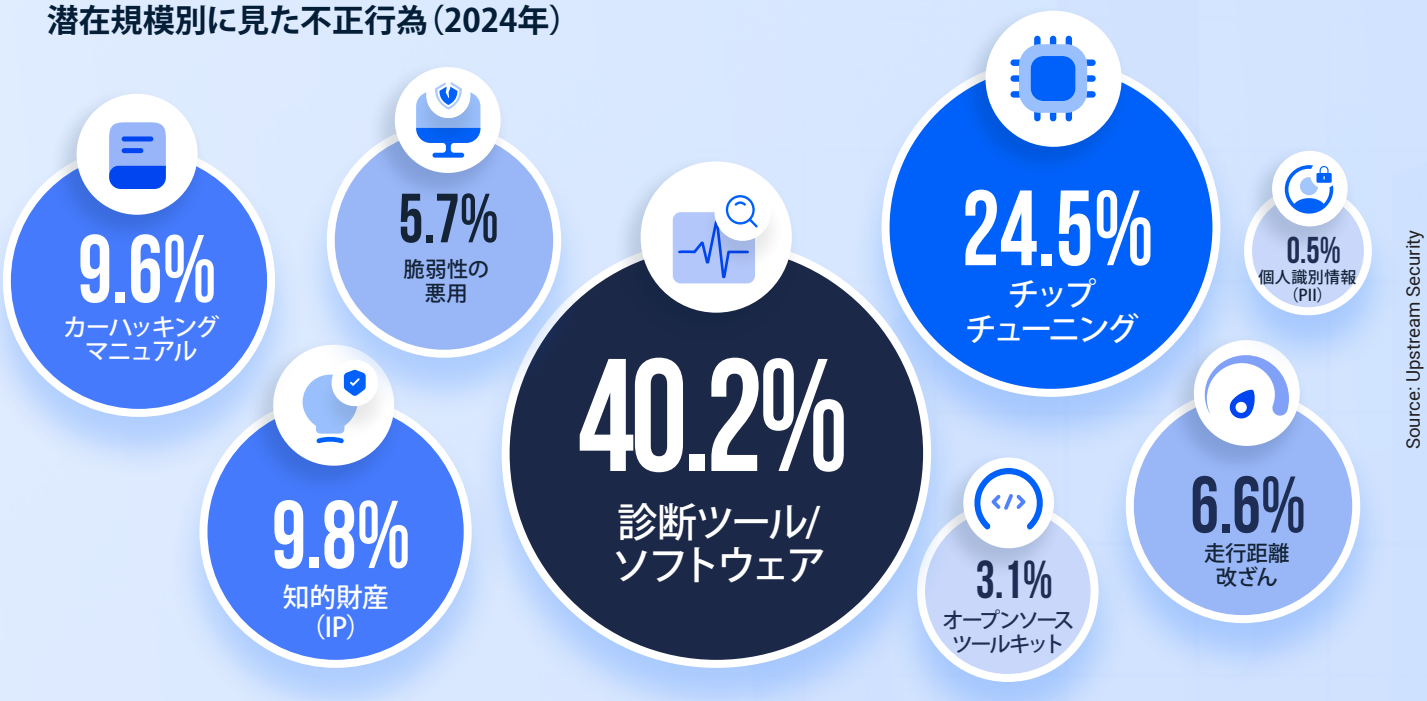
不正行為者の関心領域を分析すると、車両操作が彼らの活動の約72%を占めているのが分かります。このカテゴリは、主に次の 3 つの関心領域で構成されています。

1. 活動の40%を占める診断ツール
2. 活動の25%を占めるソフトウェアとチップチューニング
3. 活動の7%を占める走行距離の改ざん

不正行為者は、カーハッキングマニュアル（10%）やオープンソースツールキット（3%）にも関与しています。[240] 加えて、その活動のうち10%弱が知的財産（IP）に関与し、6%が脆弱性の悪用、1%未満が機密性の高い個人識別情報（PII）を標的にするものでした。[241]



潜在規模別に見た不正行為（2024年）



ディープウェブとダークウェブのリスクへの積極的アプローチ

2024年には、ディープウェブおよびダークウェブ上でのデータ共有が飛躍的に増加しました。これらのプラットフォームでは、自動車関連セキュリティの脆弱性やデータ漏洩、その他のサイバー脅威が定期的に公開され、活発に議論されています。UpstreamのAutoThreat® PROのアナリストは、ディープウェブやダークウェブのサイトで自動車関連の情報を大量に検出しました。自動車関係者は、ディープウェブおよびダークウェブを監視し、サイバーセキュリティ体制に重大な欠陥が生じないように備えることが不可欠です。効果的なサイバーセキュリティ対策には、企業や組織が、公開情報・非公開情報のいずれにおいても、自らがいつ、どのような文脈で言及されたり標的にされたりしているかを把握していることが求められます。UNECE WP.29 R155とISO/SAE 21434、NHTSAガイドラインおよび中国の規制などの規則では、サイバー脅威 インテリジェンスと脆弱性の監視が義務付けられています。ディープウェブとダークウェブは、このような要件を遵守する上で不可欠な要素です。

> ***継続的にディープウェブやダークウェブを監視することで、検出力が向上します。また、脆弱性やセキュリティ侵害が発見されてからその情報が広まるまでの対応時間を短縮することも可能です。***

その際、ソフトウェアパッチの導入、設定の変更、または漏洩した認証情報の置換などの予防措置が極めて重要です。加えて重要なのは、犯罪者による侵害データへのアクセスおよび不正取引の機会を最小限にすること、また、潜在的悪用の可能性をステークホルダー、従業員、主要幹部役、顧客に警告することです。

従来のIT脅威インテリジェンスサービスは、コネクテッドカー分野の専門知識を十分に備えていないことが多く、OEM、Tier-1、Tier-2をはじめとするモビリティ関係者にとって課題となっています。

UpstreamのAuto Threat® PROソリューションは、このような課題を克服すべく開発され、自動車およびスマートモビリティエコシステムに特化したサイバー脅威インテリジェンスを収集、分析、公開しています。サプライチェーン全体を対象に、様々な自動車セグメントに合わせてカスタマイズされています。例えば、自動車メーカー、Tier-1およびTier-2サプライヤー、スマートモビリティデバイスとアプリケーション、コネクテッドカーサービスプロバイダー、保険会社やその他の自動車関係者などが対象です。Upstreamは、ディープウェブやダークウェブを積極的に監視し、自動車関連の新たなサイバートレンドや脅威アクターをいち早く発見します。脆弱性、悪用、不正行為といった新たな脅威を、公になる前に特定し、迅速に対応します。適切なサイバー脅威インテリジェンスを活用することで、自動車およびモビリティ関係者は、必要なサイバーセキュリティ対策を積極的に講じ、次なるサイバーインシデントを防ぐことができるのです。

06.

規制の実態

サイバーセキュリティの回復力、安全性、データ保護への強い重視が、車両、EV充電インフラ、AIシステムの規制フレームワークの進化を推進している

注：本章では、自動車およびスマートモビリティのサイバーセキュリティ規制に関する最新の更新事項と傾向の概要を提供します。包括的な規制評価について、追加の資料を参照し、詳細な分析を行うことをお勧めします。

EU AI法は、自動車におけるAIシステムに厳格なルールを適用することで、自動車業界に大きな影響を与えるでしょう

AIは自動車業界に変革をもたらすとされています。設計や研究開発から個別化されたドライバー体験や車両品質まで、広範囲にわたり変革をもたらす可能性があります。

自動車およびスマートモビリティのエコシステムには、大きな投資と強い期待が寄せられています。ステークホルダーはAIをゲームチェンジャー、すなわち大きな変革をもたらすものと考えており、すでに相当な資金投入と広範囲にわたるパイロットプロジェクトが進行中です。

マッキンゼーによると、75%の企業が少なくとも1つの生成AIアプリケーションを試験的に導入しています。 40%以上の企業が最大500万ユーロを投資し、一部企業においては2000万ユーロを超える投資を行っています。[242] 実際、2024年5月にトヨタは、AIに重点を置くことを強調し、AI、EV、その他に130億ドルを投資すると発表しました。.[243] トヨタは自動運転、安全性、生成AIを含むさまざまな分野でAI関連の投資を拡大する計画を立てていました。

しかし、広く普及するには依然として課題が残っています。 これらには、熟練した人材の不足、倫理的懸念、個人情報の保護、サイバーセキュリティのリスク、そして規制に関する不確実性などが含まれます

> ***2024年8月、EUの人工知能法（AI法）が施行され、3年間にわたって段階的に導入、ほとんどの規定は24ヶ月後に適用されます。[244]***

この規制は、EUの27の加盟国が国内法を必要とせずに直接実施できるもので、基本的権利の保護を確保し、リスクと影響に基づいてAIを使用するための義務を確立することに重点を置いています。

この目標を達成するために、EUのAI法はAIシステムをリスクレベルに基づいて4つのカテゴリに分類しています：許容できないリスク、高リスク、限定リスク、そして最小リスクです。EUAI法は、特に高リスクのAIシステムに関する、サイバーセキュリティのリスクに取り組んでいます。第15条は、これらのシステムが適切な精度、堅牢性、およびサイバーセキュリティのレベルを確保し、ライフサイクル全体を通じて一貫したパフォーマンスを維持するように設計・開発することを義務付けています。[245]

75%

の企業が、少なくとも1つの生成AIアプリケーションを試験的に導入している。

40%

以上の企業が最大500万ユーロを投資し、一部企業においては2000万ユーロを超える投資を行っている。

この規制に取り組むことによって、欧州市場全体でAIを基盤とした技術の急速な成長を可能にすることも目指しています。 AI法違反に対する罰則は、最大で3500万ユーロ、または企業の年間世界総売上高の7%のいずれか高い方を課せられる可能性があります。コンプライアンス違反は、製品のリコールや市場での販売禁止につながる可能性もあります。 EU AI法は、AIの安全基準に対する世界的な協調を促進し、他の地域が追随する前例となる可能性があります。

EU AI法におけるリスクベースアプローチでは、ほとんどの自律運転システムが高リスクに分類され、厳格なコンプライアンス対策が求められています。
EU域外の企業も、欧州経済領域内で事業を展開する場合はEU AI法を遵守する必要があります。

AI法は、既存の自動車および一般製品の安全規制を認識しています。これらの法律は、既にAIのいくつかの側面に対応していますが、AI法の高リスク要件を具体的に組み込むように改正され、自動車AI向けの業界固有の枠組みが作成されます。 EU AI法における高リスクAIと低リスクAIの規定は、業界が直面すると予想される規制上の要求をいち早く示しています。

AIは自律運転のイノベーションを推進し、実現する主要な要因の1つです。AI法は車両には直接適用されませんが、 OEMや、特にAIを大きく活用する可能性が高い自律運転技術は、改正型式承認枠組み規制（TAFR）基準が利用可能になった場合、それに関連する新たなコンプライアンス義務に直面する可能性があります。 AV（自律走行車両）にとってAIの重要性を考えると、これは自動車業界とAVの開発に大きな影響を与える可能性があります。[246]

EU 内外の自動車業界の関係者は、コンプライアンスを確保するために、新しい要件を理解し、適応する必要があります。 現行の自動車規制と新しいEU AI法との兼ね合いにより、規制環境の複雑さが増し、関係者はさまざまな規制の枠組みを慎重に検討する必要があります。 長期的なAI主導の戦略を練る際に、スキル開発、倫理的配慮、データプライバシー、および規制のコンプライアンスをバランスよく調整することが求められます。

UNECE WP.29 R155および ISO/SAE 21434の拡張

2024年、多くの自動車OEMとそのメーカーは、サイバーセキュリティ管理システム（CSMS）と型式承認に関するR155、[247] そしてソフトウェア更新管理システム（SUMS）に関するR156を引き続き実施しました[248]

2024年7月、R155の第２段階の施行により、対象車両の範囲が大幅に拡大し、生産中のすべての新車が対象となりました。

これらの規制は、ISO/SAE 21434とともに、[248] 自動車およびスマートモビリティのサイバー脅威に対する統一された対策を作成するための、世界的な取り組みの一環です。

R155およびISO/SAE 21434のどちらも、具体的な解決策や正確なプロセスの概要が示されていないことに注意することが重要です。その代わりに、高度なサイバーセキュリティ基準の重要性が強調されています。ガイドラインでは、プロセスの概要が示され、リスク分析と対応目標が明記されています。さらに、開発、製造および製造後の各段階において、生涯にわたるサイバーセキュリティの脅威と脆弱性を考慮する必要性が強調されています。

R155は2022年に発効して以来、継続的に拡張されてきています。2024年6月、国連は自動車基準調和世界フォーラムにおいて、R155をカテゴリーLの車両（例：オートバイとスクーター）[251]にも適用を拡大する提案[250]を採択しました。2029年7月までに、カテゴリーLのOEMは、CSMS（サイバーセキュリティ管理システム）252の監査に合格したことを示す証拠として、適合証明書を取得する必要があります。[252] さらに2024年7月には、R155の第２段階が施行され、生産中のすべての新車にサイバーセキュリティ法が適用されるようになりました。

UNECE WP.29 の概要

規則WP.29の主要構成要素

R155 CSMS

サイバーセキュリティ管理システム

構想段階からポストプロダクションまでのサイバーセキュリティ管理

R156 SUMS

ソフトウェア更新管理システム

車両のライフサイクル全体を通じて安全なソフトウェアの更新を確保するためのサイバーセキュリティ対策

WP.29で規制される車両

車両カテゴリー	定義	適用規制
L (すべて)	四輪未満の車両（例：オートバイやスクーター）	R155
M	四輪車以上で乗客を運搬することを目的としたもの	R155 および R156
N	四輪車以上で物品を運搬することを目的としたもの	R155 および R156
O	ECUを一つ以上搭載しているトレーラー	R155 および R156
R	農業用トレーラー	R156
S	交換可能な牽引式農業機械または林業機械	R156
T	2つの車軸を持ち、時速6km(~3.5mph)以上で走行する電動式、車輪式、または留め金式農機具	R156

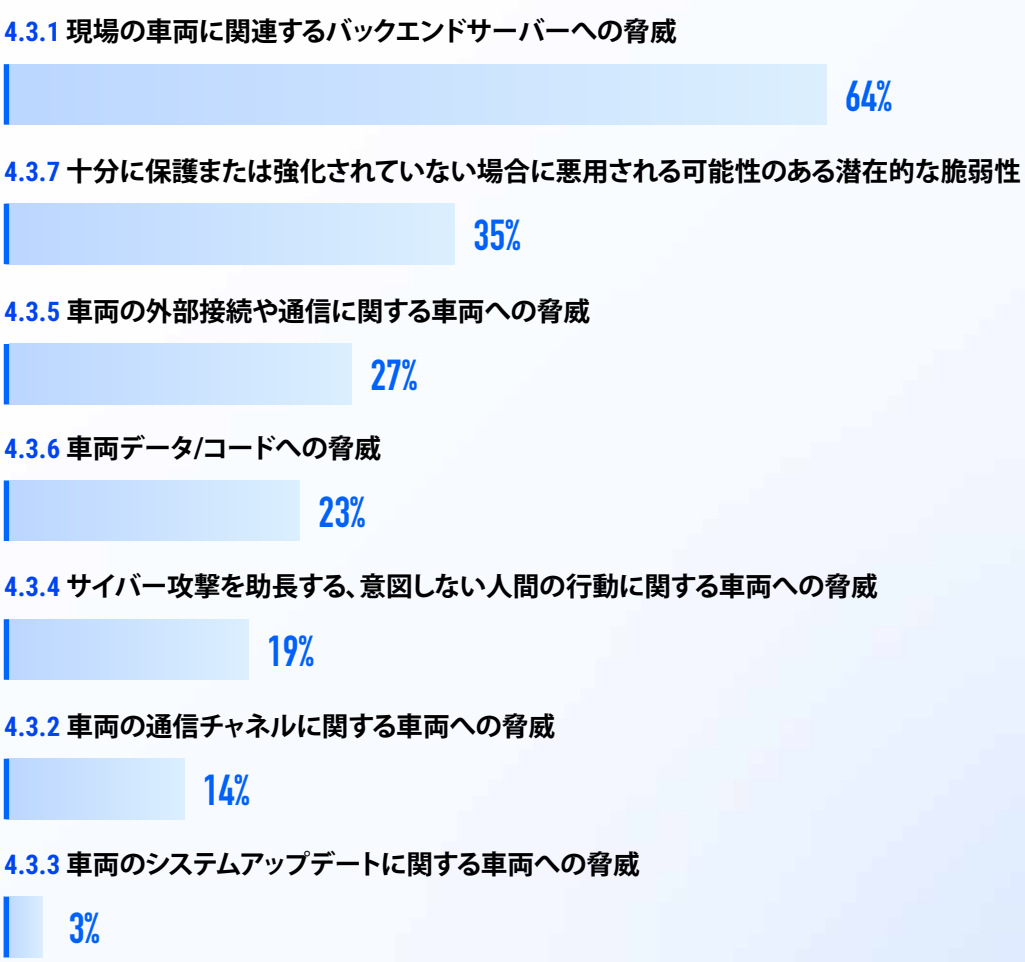
Source: Upstream Security

車両は、カテゴリー分類に応じて、R155(253)、R156(254)、またはその両方で規制されます。

R155 は脅威に対応しているのか?

Upstreamの調査チームは、2024年に発生した公表済みの自動車サイバーインシデントを分析し、R155Annex5(規制付録5)に示された7つの脅威カテゴリと関連付けました。

R155の脅威と脆弱性に分類される2024年のサイバーインシデント



Source: Upstream Security

WP.29が自動車産業に与える影響

新しい規制、規格、ガイドラインは、高レベルのサイバーセキュリティを確保するように設計されています。その結果、顧客の安全性とセキュリティが向上すると同時に、業界全体で統一された用語、ガイドライン、目標、適用範囲が確立されています。 製造業者は、革新的なサイバーセキュリティのアプローチを導入し、継続的な改善を行うために、このような柔軟な対応が求められています。

ISO/SAE 21434は、ISO 26262 道路車両-機能安全規格に基づき、自動車OEMおよびサプライヤーに、車両のライフサイクル全体を通してサイバーセキュリティを実装するよう要求しています。これは、「グループ全体でのセキュリティ」の考え方を採用し、製品開発と生産の各段階、および生産後の段階においても、エンジニアリング要件を確立することに重点を置いています。

R155では、OEMに対し、車両のライフサイクル全体を通じて、脅威分析とリスク評価 (TARA)を実施し、維持することを求めています。
車両のソフトウェア定義化が進み、ソフトウェアコンポーネントが車両のライフサイクル全体にわたって継続的に更新されることで、効果的なTARAの実施がますます複雑化しています。 OEMはまた、Tier-1およびTier-2サプライヤーとともに、将来の攻撃に対処し、軽減するためのプロセスを構築する必要があります。 この規制はOEMに適用されますが、CSMSがバリューチェーン全体を含むことを示す必要があるため、R155の影響範囲もサプライヤーにまで拡大します。R155は、1958年のUNECE輸送協定および条約に参加する54カ国で事業を展開するOEMに適用されます。

UNECE規制とISO / SAE 21434規格はクリティカルマス(普及率が一気に跳ね上がる分岐点)に達しており、世界中のオペレーションを変化させています。2024年7月に発効した第2マイルストーンでは、すべての新車がR155に準拠することになります。

OEMは、サプライヤーやサイバーセキュリティ企業と緊密に連携し、業界全体のコンプライアンスや認証の取り組みを支援し、強固なサイバーセキュリティのガバナンス構造(管理体制)とテストプロセスを確立しています。

OEMとサプライヤーの連携を強化するため、欧州自動車工業会(ACEA)と欧州自動車サプライヤー協会(CLEPA)は2022年10月にAuto-ISACと提携し、自動車のサイバーセキュリティに関する情報共有のための欧州中央拠点を設立しました。[255]

ISO/SAE 21434に基づく長期的な信頼の確立

ISO/SAE 21434とR155の主な違いは、ISO/SAE規格がOEMとそのサプライヤーに資産リスクを算出するための包括的なプロセスを提供し、そのスコアの計算方法や脆弱性の優先度を決定する方法を提案していることです。

この規格は、構造化されたサイバーセキュリティフレームワークを提供し、車両のライフサイクル全体において、コンセプト段階から廃棄に至るまで、サイバーセキュリティをエンジニアリングの不可欠な要素として確立しています。

さらに、ISO/SAE 21434規格およびR155 CSMS要件に従うため、OEMは車両が組立ラインを離れた後も10年以上にわたり、継続的な監視を実施するためにvSOC(車両セキュリティオペレーションセンター)を維持することが推奨されています。

2024年には新たに422件のCVEが発見されており、ディープウェブおよびダークウェブの活動が急激に増加していることを踏まえ、関係者は既存および将来的な脆弱性、さらには将来発生する可能性のある未発見の脆弱性から製品を保護するために、脆弱性を軽減する技術を継続的に見直し、実施することが必須となります。

ISO/SAE 21434 と WP.29 が連携し、世界規模で車両をサイバー攻撃から保護

ISO/SAE 21434
設計上のセキュリティ
製品開発の各段階における技術要件

R155
サイバーセキュリティ管理システム
車両ライフサイクル全体にわたるサイバーセキュリティ監視

R155
脅威分析とリスク評価
脆弱性のリスク評価、およびリスクスコア

R155
モニタリング
車両ログに基づく早期検知と、インシデントへの迅速な対応

R156
ソフトウェア更新管理システム
車両ライフサイクル全体にわたる継続的な安全性の更新

自動車サイバーセキュリティ基準に準拠するには、RF関連のサイバーリスクへの対処が不可欠。

RF規制（周波数割り当てや干渉防止など）は、ITUやFCCなどの地域、または国際的な電気通信当局によって管理されています。そのサイバーセキュリティの影響は、R155とISO/SAE 21434が義務付けるリスク管理、およびセキュリティ管理の範囲内に含まれます。 RF関連の脅威への対処は、これらの自動車サイバーセキュリティ基準に準拠するために極めて重要です。実際、RF規制はR155とR156の両方の型式認証において、不可欠な要素として認識されることがよくあります。

CSMSとの関連性（R155）

V2X、Bluetooth、Wi-Fi、キーレスエントリーなどのRFに基づいた通信システムは、重要な攻撃対象領域と見なされています。 OEMはCSMSの一環として、包括的な脅威モデリングを通じてRF関連の脅威と脆弱性を評価することが求められます。さらに、OEMはこれらの脆弱性を軽減するためのリスク管理措置を実施し、R155要件への準拠を確保する必要があります。

ISO/SAE 21434との関連性

ISO/SAE 21434は、ジャミング、スプーフィング、不正アクセスなどのRF通信の脅威を含む、詳細な脅威分析とリスク評価（TARA）を義務付けています。

さらに、ISO/SAE 21434は、安全な通信プロトコルの使用やデータの整合性と機密性を保護するための高度な暗号化技術の採用など、無線通信のための強固なサイバーセキュリティ制御の実装を重視しています。

自動車及びスマートモビリティエコシステムに関連するRF（無線周波数）重点規制の要約：

	規制 / 基準	影響
国際規制、および地域規制	ITU無線通信規則（国際電気通信連合）[256]	2024年8月に更新。この国際規制は、V2Xや緊急通報システムなどの自動車アプリケーションを含む無線周波数の使用を規定している。
	FCC パート15（米国）[257]	ライセンス不要のRFデバイス（自動車のキーフォブ、Bluetooth、Wi-Fi、その他の短距離通信システムを含む）を規制しています。
	ETSI EN 302 571 (EU)[258]	この規制は、V2X通信に焦点を当て、EUにおけるインテリジェント交通システム（ITS）に割り当てられた5,855 MHz～5,925 MHz周波数帯で動作する無線送信機と受信機の技術仕様、および測定方法を概説しています。.
	指令2014/53/EU RED - 無線機器指令（EU）[259]	EUで販売されているRF機器（無線通信機能搭載車を含む）の適合性を対象としています。
自動車特有の規格	ISO 15118（路上車両 - 車両からグリッドへの通信インターフェース）[260]	EV（安全な無線通信プロトコルを含む）と充電ステーション間の通信を定義します。
	IEEE 802.11p、車載無線アクセスとして知られている（WAVE）[261]	V2X通信向けに調整された規格。車両間（V2V）、および車両とインフラ間（V2I）のリアルタイムな無線通信を可能にします。
サイバーセキュリティ関連規格	SAE J3105[262]	EVの安全な無線充電通信を対象としています。
	SAE J2945/1[263]	小型車両用の車載V2V安全通信システムのシステム要件を規定しています（セキュリティと効率性のためのRF管理を含む）。
	ETSI EN 303 645[264]	センサーやインフォテインメントプラットフォームなどの RFに基づいた自動車用IoTシステムに特化したIoTデバイスのサイバーセキュリティに重点を置いています。

Source: Upstream Security

アップデートされる規制の動向

自動車とスマートモビリティのエコシステムが進化し、新しいアプリケーション、デバイス、サービスが導入されるにつれて、政策当局は法律の在り方を常に見直しています。2024年7月時点で、すべての新車に適応範囲を拡大するというR155の重要なマイルストーンに加え、世界中の立法者は、車両やインフラ、消費者のプライバシーに対するサイバーセキュリティのリスクを一層強く認識するようになっています。これらのリスクに対処するために、自動運転車を含む新しい法律が起草されつつあります。

EUサイバーレジリエンス法は、サイバーセキュリティのレジリエンス拡大を促進

2024年10月に正式に採択されたEUサイバーレジリエンス法（CRA）は、ハードウェアとソフトウェアの両方を含むデジタルコンポーネントを備えたすべての製品を対象とする水平的な法律として機能します。消費者保護を重視し、CRAはウェアラブル技術から車両に至るまで、幅広い最新の接続機器におけるサイバーセキュリティの向上を目指しています。[265]

CRAは、企画、設計から開発、保守に至るまで、製品のライフサイクル全体にわたる包括的なサイバーセキュリティの枠組みを確立します。 また、メーカーに対して、積極的に悪用された脆弱性やインシデントを報告し、製品のサポート期間を通じてタイムリーなリスク軽減を実施することを求めています。[266]

メーカーは2027年10月までに本法に準拠しなければなりませんが、一部の規定はそれ以前に適用される可能性があります。OEMやモビリティの関係者は、CRAの適用範囲を慎重に検討する必要があります。R155によるサイバーセキュリティ管理の対象カテゴリーであるM、N、および特定のO車両を含む、一般安全規則（EU）2019/2144の規制対象製品は、CRAの適用範囲外となります。しかし、それ以外の車両はCRAの適用対象となります。 R155や同様の規制が拡大するにつれ、OEMはCRAとR155の両方の要件に適合する必要が出てきます。これにより、適用対象となるすべての車両およびデジタル製品に対し、強固なサイバーセキュリティ体制が確保されます。[267]

ISO15118は車両からグリッドへの通信（V2G）を保護

ISO 15118は、「道路車両 - 車両からグリッドへの通信インターフェース」[268]の主要な通信規格で、サイバーセキュリティの機能と要件も含まれています。また、電気自動車（EV）と電気自動車供給設備（EVSE）の間で暗号化された安全な通信を保証します。[269]

これはカテゴリーMおよびNの車両に適用されますが、他のOEMにもそのフレームワークを採用するよう奨励しています。 また、EVを充電するためのコンバインド充電システム（CCS）規格の高水準通信プロトコル（HLC）の基盤としても機能します。

EVの充電プロセスで信頼を確立する必要から、この規格は電力網を保護し、電力網の過負荷を防ぎながら、一度に複数の車両の充電をサポートするように設計されました。

ISO 15118規格は、次の3つの基本段階を含む「プラグアンドチャージ」操作を規定しています。[270]

01

機密保持

トランスポートレイヤーセキュリティ（TLS v1.2）プロトコルは、楕円曲線ディフィー・ヘルマン（ECDH）鍵合意プロトコルを使用し、1回の充電セッションに有効な共有キーを用いて、暗号化された通信セッションを確立するために使用されます。

02

データの整合性

すべてのメッセージは、対称TLSセッション キーを使用して、充電セッション中に暗号化および復号化されます。.

03

信頼性

送信者の信頼性とメッセージの整合性は、楕円曲線デジタル署名アルゴリズム（ECDSA）を使って検証されます。

ISO 15118は、EVSEメーカー、EV OEM、充電ポイント運営会社（CPO）を含む、充電プロセスに関与するすべての事業体に適用されます。例として、クラウドサービスプロバイダー(CSP、エッジコンピューティングやデータストレージなど)、および電力網（ユーティリティ、ビル管理システムなど）です。

カリフォルニア州エネルギー委員会（CEC）は、ISO 15118を積極的に推進しています。2024年5月には、EV充電におけるISO 15118規格の実施に関する業界の最新情報を議論する技術ワークショップを開催しました。 このワークショップでは、CECのスタッフや業界の代表者によるプレゼンテーションが行われ、EV充電インフラにおける安全で標準化された通信プロトコルの重要性が強調されました。[271]

2024年10月、国際標準化機構（ISO）は、ISO 15118-20:2022の改正案として、ISO 15118-20:2022/DAmd 1を発表しました。この改正案では、新たに発生するサイバーセキュリティの脅威に対処するため、セキュリティプロトコルの改善を含む強化策を導入し、V2G通信の整合性と機密性を確保します。[272]

ランサムウェア攻撃により、米国上場企業のSECサイバーセキュリティ開示要件の不備が明らかに

2023年7月、米国証券取引委員会(SEC)は、上場企業に対するサイバーセキュリティ開示の最終規則を採択しました。[273]

2023年12月に発効した最終規則は、次の2つの要件があります。上場企業がサイバーセキュリティの重大なインシデントがあると判断した場合、それを判断してから4営業日以内に（フォーム8-Kを使用）開示すること、もう1つは、サイバーセキュリティのリスク管理、戦略、およびガバナンスに関する情報を（フォーム10-Kを使用）毎年開示することです。[274]

新しい規則によれば、SECの規則に基づいて取引される上場企業は、重大なサイバーセキュリティインシデントの発生を開示し、その性質、範囲、発生期等の重要な側面、ならびにそのインシデントが企業に与える重大な影響または起こりうる重大な影響を財務状況や業績を含めて説明しなければなりません。この開示は、重大なサイバーセキュリティインシデントが企業に与える重要な影響に焦点を当てています。

またこれらの規則では、国家安全保障または公共の安全に重大なリスクをもたらすサイバーセキュリティインシデントについて、司法長官による書面通知を条件として、報告の遅延が認められています。また、小規模企業に対しては、最大180日間の延長も認められています。[275]

これらの規則により、SECはサイバーセキュリティインシデントやデータ漏洩における透明性と説明責任の重要性を強調しています。これらの事象は、確立された重要性基準に基づき、重要な事象として株主やSECに報告する必要があります。SECによるこの新しい規制により、サイバーセキュリティ攻撃の課題に直面する自動車およびモビリティ関連企業からの申請が相次ぐと予想されます。

2023年11月、あるランサムウェアグループは発効日を知らずに、自ら攻撃した上場企業をSECに提訴しようとしました。この攻撃は、金融機関向けのローン発行システムおよびデジタル融資プラットフォームを提供する企業に対して行われました。 攻撃者は、被害者である上場企業が新しい規則に基づいて侵害を開示しなかったと訴えました。[276] 攻撃が疑われた時点では、SECの新しい規則はまだ施行されておらず、標的となった企業は、脅威を軽減するために発見後即座に行動したと報告しています。

2024年6月、1万5,000の販売店が利用する販売店管理ソフトウェアの米国大手プロバイダーがランサムウェアの攻撃を受け、販売店の業務がほぼ3週間停止し、SECの開示規則が試されることになりました。[277]

影響を受けた複数の販売店は、攻撃がビジネスに悪影響を及ぼしたとして、SECに開示書類を提出しました。しかし、ランサム攻撃を受けた販売店管理ソフトウェアプロバイダーの上場親会社は、この事件が自社の業務に「重大な影響を与えるものではない」と述べ、開示の必要はないとしました。[278]

この矛盾で、SECのサイバーセキュリティに関する事例の開示規則に不備があることが浮き彫りになり、企業は独自の対応戦略と透明性のレベルを選択できるようになっています。このことで、時としてインシデントの深刻さが軽視される可能性があります。

サイバーインシデントの報告に関する重要性の基準に関して、企業にとって、より明確な境界線を確立するには、SECの法執行措置と判例法が必要になるかもしれないと専門家は述べています。 現在のSEC開示規則は曖昧であるため、サイバーインシデントのタイムリーかつ透明性のある報告を確保するためには、見直しと改善が必要です。

現代の車両の安全のための NHTSAサイバーセキュリティの最善策

2022年9月、米国運輸省道路交通安全局（NHTSA）は、最新式車両向けのサイバーセキュリティの最善策の更新版を発表しました[279] これらのガイドラインに拘束力はありませんが、進化する攻撃方法と、エコシステム全体にわたるサイバーセキュリティのリスクを軽減させる緊急性を反映させることが目的です。

R155のような、自動車業界全体におけるサイバーセキュリティ対策の標準化や、NHTSAが発表した現代の車両の安全のためのNHTSAサイバーセキュリティの最善策を見ると、世界中の政府機関や規制当局が、ハッキングに対してより脆弱になっている車両の保護を重要視していることが分かります。[280]

このイテレーションの最終版では、業界の新しい標準と研究が考慮され、実際のインシデントから得られた知識や、2016年と2021年の草案に対して提出されたコメントが取り入れられています。

NHTSAは、米国立標準技術研究所（NIST）のサイバーセキュリティフレームワークの5つの主要機能である「識別」「防御」「検知」「対応」「復旧」に基づいた、階層化されたサイバーセキュリティへの取り組みを推奨しています。これには以下が含まれます。

- 安全上重要な車両制御システムおよび機密情報の保護に関するリスクベースの優先順位付け
- 潜在的な脅威やインシデントのタイムリーな検出と迅速な対応
- 攻撃が発生した際の迅速な復旧
- 効果的な情報共有を含む、業界全体で得られた教訓の採用を加速させる方法

更新されたガイドラインでは、サイバーセキュリティと安全性の関連が強調され、自動車業界のつながりが強化されるにつれ、安全管理技術者とセキュリティの関係者は、敵対者が信号を操作する能力も考慮する必要があることが明確にされました。

NHTSAからの最新推奨事項は、構造とプロセス面にISO/SAE 21434からの影響を受けていますが、リモート攻撃からの保護が含まれているためR155の影響も受けています。

NHTSAのガイドラインでは、セキュリティと安全性を確保するために連携の重要性が強調されており、業界全体で効果的な情報共有を行う手段としてAuto-ISACへの参加が提案されました。 Upstreamはこれを支持しており、協力的なコミュニティメンバーとして、Upstream AutoThreat® Intelligence サイバーインシデントリポジトリ281を管理し、年次報告書で洞察を共有しています。
さらにUpstreamは、Auto-ISAC[282] および ASRG[283] の誇り高きパートナーおよびスポンサーでもあり、業界の知識共有と、サイバーセキュリティの最善策が具体化が行われています。

NHTSAは、車両の安全性を向上させ、新たなADSの課題に対処するための対策を実施

2024年4月、NHTSAは5年以内に全ての新型乗用車両に自動緊急ブレーキシステムを装備することを義務付ける規則を導入しました。
この義務付けは、車両が低視界条件下であっても、歩行者との衝突を含む起こり得る衝突を検知し、対応できるようにすることで、交通事故による死傷者数を減少させることを目的としています。 この措置により年間約362人の命が救われ、2万4,000件の負傷者の発生が防げると予測しています。[284]

2024年5月、NHTSAの欠陥調査室（ODI）は、アメリカの自動運転技術企業の自動運転システム（ADS）の性能を調査するために予備評価を開始しました。 同社の第5世代ADSに関して、ADSを搭載した車両が衝突事故の唯一の当事者となった、あるいは交通安全法に違反した可能性のある運転動作を行ったと示したインシデントの報告が22件ありました。調査では、ADSの交通管制装置を検知し対応する能力、および静止・半静止状態の物体や車両との衝突を回避する能力を評価することに焦点が当てられました。[285]

2024年10月、NHTSAは自動運転および半自動運転車両技術に対する監視を強化しました。 同局は、死亡事故を含む複数の衝突事故を受けて、米国のEV OEMの完全自動運転（FSD）ソフトウェアに関する調査を開始しました。 この調査は、約240万台の車両を対象に、低視界条件下おけるFSDの性能を検証するものです。[286]

Auto-ISAC、自動車脅威マトリックス（ATM）を導入

2024年3月、Auto-ISACは「Automotive Threat Matrix（ATM）」を導入しました。これは、自動車業界全体におけるサイバー脅威インテリジェンスの分類と共有を強化するとともに、自動車の脅威やリスクの評価を大きく前進させる革新的な取り組みです。ATMは、MITRE ATT&CKフレームワークを基にしており、[287] 自動車特有のサイバー攻撃の戦術と技術に特化した、精密に調整した標準分類法を提供しています。[288]

ATMにより、コネクテッドカーおよびソフトウェア定義型車両に対するサイバー脅威を特定、評価、軽減するための体系的リソースを活用できます。 ATMは、業界横断的な共通言語を使用しているので、自動車業界全体の協力体制が強化されます。これにより、利害関係者やセキュリティ専門家が連携し、進化する敵の脅威に対するセキュリティの強靭性を高めることが可能になります。

ATMフレームワークの導入は、自動車業界におけるリスク管理の包括的なアプローチに向けた重要な一歩となります。ATMには13に及ぶ戦術の下に技術が70以上組み込まれており、様々な攻撃経路や影響を受けたコンポーネントに対処する構造になっています。 このフレームワークにより、脆弱性管理、脅威評価とリスク分析（TARA）、サイバー脅威インテリジェンスなど、リスク管理の重要側面が強化されます。こうして、自動車セクター特有のサイバーセキュリティ関連イベントへの対応に関する業界基準が確立されます。

車両データとプライバシー規制の導入

コネクテッドカーは特有のデータプライバシーおよびサイバーセキュリティの課題をもたらし、OEMはこれに対処しなければなりません。世界中の規制当局がこれに注目し、消費者中心の車両データのプライバシーとセキュリティ基準を策定しています。

2024年6月、EUは正式にデータ法[289] を採択し、車両を含むコネクテッドデバイスが収集したデータに対するユーザーの管理権を増強しました。 この法案は、OEMに対し、アフターマーケットサービス向けに第三者が車両データへアクセスできる環境の整備を促すものです。これにより、消費者のデータ権利を保障しながら、市場競争が促進されます。2024年8月、EUはAI法も最終決定しました。[290] この法案は、自動運転などのAI駆動機能に関する要件を定め、車両データに影響を与えます。データ保護と安全基準の遵守を確保するため、データの透明性とリアルタイム監視を義務付けています。

I2024年5月、データプライバシーを管轄する規制機関である米国連邦取引委員会（FTC）は、車両によって収集されたデータに関する懸念を強調しました。特に位置情報やその他の機密情報に関して、強力なプライバシーおよびセキュリティ対策の必要性が強調されました。[291]

これは、複数の上院議員からの書簡を受けて、FTCに対して自動車メーカーの慣行、特に位置情報を法執行機関と共有することについて調査を求めたものです。[292] さらに、2024年6月、連邦通信委員会（FCC）は、消費者データの悪用の可能性があるとして、自動車メーカーの接続慣行を精査する意向を発表しました。[293]

州レベルでの規制の進展も引き続き拡大しています。以下はその例です。：

- **ニュージャージー州：**自動車販売店に対し、販売または下取り車両から、消費者の個人情報を削除することを義務付ける法律を制定。[294]
- **テネシー州**：自動車会社によるデータ収集を拒否できるドライバー登録簿を作成する法案を提出。[295]
- **ニューヨーク州:**保険法を更新する法案を提案。自動車保険会社に対し、料率計算におけるテレマティクスデータの使用方法の開示を義務付ける。[296]
- **カリフォルニア州:**自動車メーカーに対し、車載カメラの存在を開示することを義務付ける法律を可決。[297]
- **カリフォルニア州：**家庭内暴力の被害者や生存者を保護するため、コネクテッドカーに対するセキュリティ対策の追加を検討中。[298]

車両から生成されるデータの多くは個人データとみなされる可能性があり、消費者のほとんどは、データ保護のための法律の必要性を感じています。[299]

今後数年間、自律型テクノロジーの台頭に伴い、米国およびEU市場向けの新規制が引き続き増加すると予想されます。これらの新規制では、消費者がデータ利用に「同意する」または少なくとも「同意しない」など、消費者の意向が必要となります。
規制の整備が進む中、OEMは、自社のデータプライバシーとセキュリティポリシーに関して、戦略的に意思決定を行う必要があります。これは、相互信頼の構築、コンプライアンスの徹底、消費者保護の最大化が実現します。

自動車サイバーセキュリティ規制に関するグローバルな視点

世界中で進化し続ける規制は、政府や規制当局が技術発展に適応し、安全性を促進し、セキュリティ問題に対処するための協調的な取り組みを反映しており、自動車産業の未来を形作る世界的な取り組みを示しています。

EU

2024年7月、EUの一般安全規制の一環として、車両の安全性と自動運転モビリティに関する新しい規則が施工されました。 現在EUで販売される車両には、ドライバーを支援し、EU全域の乗員、歩行者、自転車利用者をより良く保護するための一連の新しい安全機能を搭載する必要があります。[300]

この規制は主に物理的な安全対策に焦点を当てていますが、製品ライフサイクル全体を通じてサイバーセキュリティを確保する能力を実証するために、サイバーセキュリティ管理システムの認証も義務付けています。 さらに、メーカーが車両の型式認証を取得するために満たさなければならない要件の包括的な枠組みを確立しています。

EU一般安全規制 - 車両の安全性と自動運転に関する新規則

	すべての道路車両	乗用車とバン	バスとトラック
2024年7月以降、すべての新車に必須となる新安全機能 **これらの対策は2022年7月以降のすべての新型車両に適用されています*	● インテリジェントスピードアシスタンス ● カメラまたはセンサーによる後退検知 ● ドライバーの眠気に対する注意喚起 ● 緊急停止信号 ● サイバーセキュリティ対策	● レーンキープアシスト ● 緊急ブレーキ車、歩行者、自転車の検出 ● イベントデータレコーダー	● 歩行者や自転車との衝突を防ぐための検知と警告 ● タイヤ空気圧モニタリングシステム
2024年7月から2029年1月にかけて段階的に導入される対策	● 高度なドライバーの注意散漫警告 ● 安全で長持ちするタイヤ性能 **これらの対策の適用対象：2024年7月以降の新型車両；2026年7月以降の新型車両*	● 安全ガラス **これらの対策の適用対象：2024年7月以降の新型車両；2026年7月以降の新型車両*	● 自転車利用者や歩行者をより良く見えるように改善された直視機能 ● イベントデータレコーダー **これらの対策の適用対象：2026年1月以降の新型車両；2029年1月以降の新型車両*

2024年10月、EUはNIS2指令を施行し、重要部門全体のサイバーセキュリティを強化しました。これは、コネクテッドカー、EV充電インフラ、適応型交通信号機やスマートハイウェイなどのインテリジェント交通システム（ITS）を含む、スマートモビリティのエコシステム全体に影響を与えました。[301] この更新は、当初のNIS指令を拡大し、「重要」および「重要性の高い」事業体の両方に、リスク管理、インシデント対応、サイバーインシデントの詳細な報告など、包括的なサイバーセキュリティ対策の採用を求めています。EV充電事業者およびITSプロバイダーは、不正アクセスやデータ侵害に対する強力な防御を実施する必要があります。これはEUの持続可能なモビリティ目標を確保する上で不可欠です。 NIS2の下で、企業はサイバーセキュリティに関する上級管理職の役割を指定する義務があります。上級管理職は説明責任を果たし、サイバーセキュリティを組織の戦略に統合することが義務付けられています。 この指令は、コンプライアンス違反に対する高額な罰則を定めています。増大するサイバー脅威から相互接続されたモビリティネットワークの完全性を保護することを目的として、セキュリティ運用と回復力への積極的な投資をしています。[302]

2024年10月、EUは「サイバーレジリエンス法」を正式に採択しました。これは、コネクテッドカーやEV充電インフラなど、デジタル要素を持つ製品のサイバーセキュリティを強化することを目的とした画期的な法律です。この法律は、ハードウェアおよびソフトウェア製品の設計、開発、製造、マーケティングに関するEU全域のサイバーセキュリティ要件を導入し、市場に出る前に製品の安全性を確保するものです。

この法律は、医療機器や自動車など、既存のEU規則ですでに対象となっている製品を除き、別のデバイスやネットワークに直接または間接的に接続されるすべての製品に適用されます。 2027年までに、製造業者は自社製品がEU市場に適合していることを確認する必要があります。[303]

サイバーセキュリティ体制に直接影響を与えるものではありませんが、2024年に欧州連合は電気自動車供給装置（EVSE）の展開と標準化を強化するために、いくつかの規制を実施しました。

- 2024年に発効した代替燃料インフラ規則（AFIR）は、欧州横断運輸ネットワーク（TEN-T）に沿って60キロメートルごとに公共の急速充電器の設置を義務付けています。この規制は、登録されたバッテリー電気自動車（BEV）1台につき1.3 kW、プラグインハイブリッド車（PHEV）1台につき0.8 kWの公共利用可能な充電器を確実に利用できるようにすることを目的としています。[304]
- ユーロ7排出ガス基準（規制（EU）2024/1257)が採択され、自動車とエンジンの型式認証に関する厳格な要件が導入されました。この基準は排出ガスとバッテリーの耐久性に重点を置いています。これは、これまでの規制を組み合わせて、EU全体で排出ガス型式認証の統一システムを構築するものです。[305]

- ネットゼロ産業法（規制(EU) 2024/1735）は、EVSEの生産と展開を含む、欧州のネットゼロ技術製造エコシステムを強化することを目指しています。これは、ネットゼロ技術分野におけるEUのレジリエンスと供給の安全性を向上させるための措置の枠組みを設定しています。[306]

米国

2024年、米国は自動車部門のサイバーセキュリティを向上させるために、いくつかの重要な措置を導入しました。

2024年3月、米国商務省は、パブリックコメントを求める規則制定案の事前通知を公表しました。それは主に中国とロシアにおける自動車産業のサプライチェーンリスクに関する問題と質問についてのコメントです。[307]

> ***2024年9月、米国商務省は規則制定案の通知を公表しました。中国またはロシアと関連を持つ特定のハードウェアやソフトウェアを組み込んだコネクテッドカー、あるいはそれらの部品の個別販売や輸入を禁止する方針を示しました。[308]***

この規則は、車両接続システム（VCS）に統合されたハードウェアとソフトウェア、および自動運転システム（ADS）に統合されたソフトウェアに焦点を当てています。これらが米国の重要インフラ、国家安全保障、および運転者の安全に対して過度のリスクをもたらす場合を対象としています。 計画されている規制は、事実上、中国車を米国市場から締め出すことになります。それと同時に、OEMメーカーに対して米国で販売される車両から中国製のソフトウェアやハードウェアを取り除くよう義務付けることにもなります。

この提案された規則は、中国の車両、ソフトウェア、および部品に対する米国の現行の規制を大幅に強化するものです。 ソフトウェアの禁止は2027年モデルから、ハードウェアの禁止は2030年モデルから適用されます。モデル年が明記されていない製品については2029年1月1日から適用されます。[309]

2024 年 9 月の提案を受けて、OEM、Tier 1 サプライヤー、政府を含む業界関係者は、提案された規制を実施する際の課題について懸念を表明しています。 コメントでは、新しい要件が既存のサプライチェーンを混乱させ、運用の複雑さを増し、生産コストの増加につながる可能性があることを強調しています。 さらに、国際貿易協定との潜在的な対立や、コンプライアンスがもたらす経済的影響についての懸念もあります。

ステークホルダーは、産業活動や貿易への混乱を最小限に抑えつつ、サイバーセキュリティを強化するバランスの取れたアプローチを求めています。[310]

2024年11月、運輸保安庁（TSA）は、国家のサイバーセキュリティ耐性を強化するため、地上交通機関（貨物・旅客鉄道、大量輸送ネットワーク、高速道路を基盤とする物流、場合によってはEV充電インフラも対象となる可能性がある）や、天然ガス、石油、危険物などのエネルギー製品を輸送するパイプライン事業者に対し、サイバーリスク管理プログラムを義務付ける規則制定案を公示しました。[311] 提案された規則では、パイプライン、旅客鉄道、貨物鉄道、および特定の長距離バス事業者など、高リスクの事業者に対し、NIST サイバーセキュリティフレームワークに沿った包括的なサイバーセキュリティリスク管理プロトコルの確立を義務付けています。[312] これらの事業者は、サイバーセキュリティインシデントをサイバーセキュリティ・インフラセキュリティ庁（CISA）に報告し、物理的セキュリティリスクをTSAに通知する必要があります。この提案は、TSAが業界および連邦政府のパートナーと継続的に協力して、重要インフラを標的とする国家主体によるサイバー脅威の高まりに対応することを強調しています。[313]

中国

2024年、中国は自動車およびスマートモビリティのエコシステムに関連する一連の規制や政策を導入し、リスク管理の枠組みの確立と、これらの分野におけるインテリジェントな変革と高度化を推進するための幅広い取り組みを示しました。

2024年6月、工業情報化部（MIIT）は、NEVやインテリジェントコネクテッドカーに焦点を当てた、世界の自動車産業向けの新しい基準を策定する計画を発表しました。 中国は、燃料電池車、電磁両立性、自動車用レーダーなどを含む、約20の国際規格の開発をリードする予定です。 さらに、中国は電気自動車（EV）の性能試験方法および衝突安全性用語に関する少なくとも3つの新しい国際標準を開発し、1つまたは2つの国際標準化ワーキンググループを設立することを目指しています。 中国はまた、自動運転システムのグローバルな技術規制の開発に注力し、EVの最大出力測定方法と動力用バッテリーの耐久性の第二段階に関する規制の策定を促進させます。[314]

2024年8月、MIITは、コネクテッドカーのアクセス、リコール、オンラインアップグレード管理の強化に関する30日間のパブリックコンサルテーションを開始しました。この協議では、インテリジェントコネクテッドカー、特に運転支援システムと無線(OTA)アップグレードを組み合わせた車両の管理を改善するための意見を求めています。システム障害の必須報告、リコール手続きの強化、および自動車メーカー向けの詳細なOTA更新手続きの提出などの対策が示されています。[315]

2024年8月、MIITは中国におけるインテリジェントネットワーク車両の最初の強制国家標準を発表し、2026年1月1日から施行される予定です。[316]

GB 44495-2024

自動車の情報セキュリティに関する技術要件は、自動車情報セキュリティ管理システムの要件、および外部接続セキュリティ、通信セキュリティ、ソフトウェアアップグレードセキュリティ、データセキュリティなどの技術要件とテスト方法を規定しています。[317]

GB 44496-2024

自動車ソフトウェアアップグレードの一般技術要件では、自動車ソフトウェアアップグレードの管理システム要件、およびユーザー通知、バージョン番号の読み取り、安全保護、前提条件、電源保証、障害処理などの車両ソフトウェアアップグレード機能に関する技術要件とテスト方法が規定されています。[318]

GB 44497-2024

インテリジェントネットワーク車両自動運転データ記録システムでは、データ記録、データ保存と読み取り、情報セキュリティ、衝突耐性能、環境評価などの観点から、インテリジェントネットワーク車両自動運転データ記録システムの技術要件とテスト方法が規定されています。[319]

中国で事業を展開する世界的なOEMは、2026年の節目に向けて準備し、新しい中国の国家基準と現行の国際基準との間のギャップを分析する必要があります。

全体として、GB 44495-2024ではサイバーセキュリティ管理システムに関するR155およびISO/SAE 21434の要件と多くの共通原則を共有しています。 しかしながら、これは市場固有の詳細な技術要件が導入されています。[320]

さらに、GB 44495-2024では、ISO/SAE21434のようなリスク管理の重要性を強調しており、これには継続的な監視、リスク評価、新たな脅威が発生しても車両の安全性を確保するための対応措置が含まれています。

どちらの規格も車両のサイバーセキュリティを強化することを目的としていますが、いくつか重要な点で違いがあります。：

	GB 44495-2024	R155
適用範囲	M（乗用車）、N（商用車）、およびO（セミトレーラーを含むトレーラー）車両カテゴリのみ適用。	L6およびL7を含み、カテゴリLの全車両へ拡大される見込み。
特徴	具体的な技術要件およびテスト方法を規定。	包括的な枠組みとリスクカテゴリ（附則5）を提示し、メーカーが柔軟に実施できる環境を提供。
テスト要件	メーカーが実施しなければならないサイバーセキュリティテスト27項目を明示。外部接続、通信システム、ソフトウェアアップデート、データセキュリティ、アクセス制御、サービス拒否（DoS）保護など、車両のサイバーセキュリティの様々な側面に及ぶ。	サイバーセキュリティテストの必要性を強調するも、具体的なテスト方法は規定せず。
認証	証明書の発行・更新不要、監査の実施が必須。	定期的な更新を伴う正式な認証プロセスを要求。

Source: Upstream Security

2024年10月、中国国家標準化管理委員会により、スマートモビリティ分野の新しい国家安全規格3件の策定が承認されました。[321]

- **インテリジェントコネクテッドビークルデータセキュリティ管理システム仕様：** 本規格は、自動車関連企業内のデータセキュリティに焦点を当て、研究開発、設計、生産を通じてデータを保護する、ライフサイクルアプローチを重視しています。企業が堅牢なデータセキュリティ管理体制を構築できるよう、指針となることを目的としています。
- **自動車セキュリティ脆弱性の分類と評価：** 本規格は、車両のセキュリティ脆弱性を、重大度と潜在的な危害に基づいて分類および評価するための枠組みを定めています。脆弱性管理を強化し、自動車のサイバーセキュリティ基準の向上を図ります。
- **自動車デジタルキーシステムの技術仕様：** 本規は、NFC、UWB、Bluetooth技術を用いたデジタルキーの機能およびセキュリティ要件を定めています。また、車両との安全な連携を支援し、デジタルキーを安心して使用できるようにします。

MIIT（工業情報化部）の指導の下、全国自動車標準化技術委員会は、これらの規格の起草と検証プロセスを主導し、承認と採用を迅速に進めます。そして、スマートモビリティエコシステムの主要な技術開発を支援します。

インド

2024年、インドは規格や規制の策定および実施を通じて、自動車サイバーセキュリティの強化で大きな進展を遂げました。

自動車サイバーセキュリティを向上させ、ISO 21434やR155/R156などの世界的な規制の枠組みと足並みを揃えるために独自の標準を開発しています。

インドは、2027年までにAIS 189（Cyber Security Management System322）およびAIS 190（Software Update and Software Updates Management System323）を実施する予定です。これにより、国内で販売されるすべてのコネクテッドカーにサイバーセキュリティ機能の搭載が義務付けられることになります。[324]

2024年6月、インド標準規格局（BIS）は、EVの安全性と品質を確保するための新規格、IS 18590: 2024[325] と 18606: 2024.[326]を導入しました。両規格は、L、M、N車両カテゴリの電動パワートレインとバッテリーの安全性および性能に焦点を当てています。 厳格な要件を設定することで、重要なシステムの信頼性と安全性を確保しています。 これは消費者の信頼を高め、EVの普及を加速させる上で極めて重要です。 BISは現在、電気自動車および充電システムなどの関連機器に関して、インド規格を30件設定しています。[327]

シンガポール

2024年5月、シンガポールはサイバーセキュリティ（改正）法2024を制定しました。これは、進化するサイバー脅威と技術進歩に対処するために、当初のサイバーセキュリティ法2018の適用範囲を拡大したものです。[328]

本改正は、深刻化するサイバーセキュリティの課題への対応を目的としています。これは、接続性の向上やクラウドプラットフォームの普及、および現代のサプライチェーンの複雑化により、攻撃対象領域が大幅に拡大していることを受けたものです。 また、本改正により、シンガポールサイバーセキュリティ庁（CSA）の権限が強化され、サイバーインシデントをより効果的に調査し、組織に重要情報の提供を義務付けることが可能となっています。 法令違反に対する罰則は、組織の年間収益の最大10%または50万シンガポールドルのいずれか高い方が科される可能性があります。[329]

この法律は、特に自動車やモビリティ分野を対象としてはいないものの、重要サービスを提供する、あるいは重要情報インフラを扱う企業は全て、強化サイバーセキュリティ基準を遵守しなければならないと強調しています。

本法は、エネルギー、水、銀行や金融、病院や医療、陸・海・空の輸送、情報通信、テレビや新聞などのメディア、警察や消防などの緊急サービス、そして政府に関する分野に重点を置いています。[330] そのため、自動車関連業界、スマートモビリティサービス提供者、およびEV（電気自動車）充電に関わる関係者は、更新されたサイバーセキュリティ規制を遵守する必要があります。

EV市場の拡大に伴い、充電インフラ規制の枠組みが進化を続ける

2024年第3四半期のEV販売に関する最近のPWC報告書によると、世界中で電気自動車（EV）のシェアが増えていることがわかりました。 2023年の第1四半期では、調査対象となった市場で販売された車両のうち28%が電気自動車でした。 2024年第3四半期までに、この数字は41%に上昇しました。[331]

電気自動車の市場シェア拡大の要因には、中国におけるプラグインハイブリッド車（PHEV）市場の急速な拡大や、中国からのPHEV輸出の急増が含まれています。ヨーロッパの主要5市場で、電気自動車（EV）の販売が大幅に増加しました。現在では、全ての新車登録のうち、56%をEVが占めています。 アメリカでは、電気自動車の市場シェアが初めて20%を超えました。[332]

2024年の第3四半期までに販売された車の41%が電気自動車

41%

電気自動車の充電ステーション（EVCS）の数が急速に増加する中で、サイバー攻撃などの悪意ある行動を通じて、世界中でEVCSを操作しようとする脅威アクターが市場に課題をもたらしています。

EVCSは、複数のメーカーが提供する部品を含むインターネットに接続されたIoTデバイスです。市場の需要に応えるため迅速に設置されています。これにより、複数の攻撃ベクトルにさらされることになります。

- 充電ポイント運営者（CPO）は充電エコシステムにおいて重要な役割を担っていますが、バックエンドの指令制御（C&C）サーバーがハッキングされると大規模な攻撃を受ける可能性があります。CPOは、遠隔から攻撃を受ける可能性があります。その方法には、複数の充電ステーションを同時に狙うことや、非常に大きな充電需要を意図的に作り出すことが含まれます。このような攻撃によって、充電システムが広範囲で使えなくなる「サービス拒否（DoS）」の状態が引き起こされることがあります。 さらに、攻撃者は個人情報（PII）や充電パターンを含む消費者の個人データに不正にアクセスする可能性があります。

- APIベースの攻撃では、サイバースキルや技術的スキルの要求水準が低くなることがよくあります。 この攻撃ベクトルは、より単純でありながら十分な攻撃面を生み出し、潜在的に全車両に影響を及ぼす可能性があります。 API攻撃ではバックエンドサーバーを標的にし、影響を与え、データ窃取やサービス拒否につながる可能性があります。APIへの攻撃は、エコシステムのあらゆる要素から発生する可能性があります。これには、車両自体、充電ステーション、モバイルアプリ、サードパーティアプリケーションなど、APIと通信を行うすべての要素が含まれます。

EVの数が増え続けるにつれて、EVの充電器や充電インフラに焦点を当てた新しい基準が登場しています。

> ***EV充電規格では、安全で信頼性が高く、アクセスしやすい充電器の提供に焦点を当てると共に、電力網における電力需要の増加を管理することに重点を置くことになるでしょう。***

EVCSを保護する規制は、大きく2つのカテゴリーに分けられます：

- **運用基準**

  EVCS がバックエンドサーバー、車両、CSMS と安全に通信する方法、データの保存方法や暗号化方法などに関するガイドライン。これには、ISO 15118、OCCP（現在1.6から2.0.1への移行中）、CHAdeMO、および現在開発中の IEC 63110 が含まれます。 これらの運用基準は、データの整合性を確保するために、EVCSメーカー自身と車両OEMによって作成されています。

- **地域法の理論的枠組み**

  EVCSオペレーターが実際に行うべき行動と満たすべき前提条件、およびその作成につながった理論的枠組みで構成されています。法律は国または地域レベルで施行されます。これには、米国のNIST IR 8473、EUのNIS2指令、サイバーレジリエンス法およびサイバー連帯法、英国の電気自動車（スマートチャージポイント）規制などが含まれます（本報告書でさらに詳しく説明）。

EVCSのサイバーセキュリティは、世界的に規制の重要な焦点となってきています。

最近のEVCSサイバーセキュリティ規制の例

地域 / 国	規制	焦点	実施日	施行状況
	ETSI EN 303 645	IoT	2025年8月	
	NIS2指令	重要インフラ	2024年10月	義務
	EUサイバーレジリエンス法	IoT	2024年10月	36ヶ月以内に義務化、一部の規定はそれ以前に適用
	NIST IR 8473	EVCS	2023年10月	任意
	国家電気自動車インフラ基準および要件	EVCS	2023年4月	必須
	GB/T サイバーセキュリティ規格	IoT、 EVCS	2022年5月	任意
	GB/T 18487.1-2023	EVCS	2024年4月	必須
	GB/T 27930-2023	EVCS	2024年4月	必須
	GB/T 34658-2017	EVCS情報システム	2017年12月	任意
	エネルギースマート家電（ESA）に関する英国規格協会（BSI）規格	スマート家電	2021年12月	任意
	2021年電気自動車（スマート充電ポイント）規制への準拠	EVCS	2022年12月	必須
	総務省 IoT 5G 総合セキュリティ対策	IoT	2019年6月	必須
	経済産業省 IoTセキュリティ・セーフティ・フレームワーク	IoT	2020年11月	必須

Source: Upstream Security

EU

欧州電気通信標準化機構(ETSI)が、IoTデバイス向けのETSI EN 303 645規格を公表しました。2024年9月、ETSIはサイバーセキュリティとデータ保護に関する懸念の高まりに対応して、消費者向けIoTデバイスの高レベルのセキュリティ規定を概説した包括的な文書の更新版、ETSI EN 303 645 V3.1.3(2024-09)を発表しました。[333]

この文書には、すべての消費者向けIoTデバイスに適用される基本的なセキュリティ要件を定めた基本規定、適用のためのガイダンス、組織に対して規定の適用方法について明確な例と説明文を提供すること、GDPRの遵守、個人データを処理するIoTデバイスがGDPR基準に準拠し適合するようにすることが含まれています。そして将来の改訂により現在の推奨事項が必須条項に移行することを見越して、将来に備えていますこの基準は、基本的なセキュリティレベルを確保しながらも、成果を重要と考え、過度な規制を行わないイノベーションのための柔軟な枠組みを提供していきます。 これにより、組織は特定の製品に合わせたセキュリティソリューションをカスタマイズすることができます。[334]

NIS2指令[335] は2024年10月に義務化され、重要インフラとエネルギー部門のサイバーセキュリティ基準とレジリエンスの確立に重点を置いています。 NIS2指令は、EUサイバー連帯法[336] によって裏付けられています。この法律は、重大かつ大規模なサイバーセキュリティの脅威や攻撃を検知し、それに備え、対応するためのEUの能力を強化することを目的としています。 これには、サイバー脅威への協調的な対応を確保するためにEU加盟国内にSOC（セキュリティオペレーションセンター）インフラを構築することや、信頼できる資格のあるプロバイダーによるインシデント対応サービスで構成される欧州サイバーセキュリティ予備部隊を創設することが含まれます。 NIS2はまた、24時間以内の報告義務を課し、さらに72時間後と30日後の追加報告を要求しています。[337]

2024年10月、欧州委員会はEU内の重要機関やネットワークに関するNIS2指令の実施に向けた最初の規則を制定しました。 これらの規則は、サイバーセキュリティのリスク管理対策を概説し、重大なインシデントを国家機関に報告するための基準を定めています。主要な措置には、サイバーセキュリティのリスク管理、インシデント報告、監督および執行措置、サプライチェーンセキュリティ、および強化された制裁を伴う合理化された報告が含まれます。[338]

2024年10月、欧州議会は公式にサイバー・レジリエンス法（CRA）を採択しました。これはデジタル要素（ハードウェアとソフトウェアの両方）を持つすべての製品を対象とする横断的な法律です。[340] CRAは製品のライフサイクル全体をカバーし、製品の企画、設計、開発、および保守を管理するサイバーセキュリティの枠組みを提供します。

規制措置には、製造業者、輸入業者、および販売業者に対する強制的な義務のほか、製品の分類とセキュリティ対策、そして監視と執行が含まれます。CRAはまた、製造業者に対し、悪用される頻度が高い脆弱性やインシデントを24時間以内に報告し、製品のサポート期間を通じてリスクを効果的に軽減することを求めています。[341]

ISO 15118は、ヨーロッパで「プラグアンドチャージヨーロッパ」というプロジェクト名で、部分的かつ自主的に導入されています。 EU全域の著名なOEMやEVCS事業者にはこれが受け入れられていますが、EUでの本格的な導入については未定です。関連規制は2025年までに施行される予定であり、この地域ではすでにISO 15118を自主的な受け入れが始まっています。

また、ISO 15118は、「プラグアンドチャージヨーロッパ」というプロジェクト名で欧州において部分的かつ自主的に導入されています。[342] EU全域の著名なOEMやEVCS事業者には受け入れられていますが、EUでの本格的な導入については未定です。

米国

2023年3月、米国連邦道路管理局(FHWA)による国家電気自動車インフラ基準および要件が発効しました。[343] この新しい規則は、国家電気自動車インフラ (NEVI) フォーミュラ・プログラムで資金供給されるプロジェクトや、特定の法令下で公衆がアクセス可能なEV充電器の建設プロジェクトに関連する要件と最低基準を定めています。これには、連邦資金で資金提供され、連邦補助道路上のプロジェクトとして扱われる任意のEV充電インフラプロジェクトが含まれます。

基本的に、FHWAはISO 15118の原則を採用し、充電ステーションに対して1年以内にISO 15118とプラグ&チャージ規格に準拠することを要求しています。 この法案は、現在市場の多くの充電器がISO 15118を使用していないにもかかわらず、コンプライアンスのための全国的な基準を採用することの価値を強調しています。[344]

この規則は、充電ステーションの場所に関する適切な物理的戦略と、消費者データを保護し、充電インフラと電力網の安全性を確保するサイバーセキュリティ戦略の実施を義務付けています。.

2023年10月、米国商務省の国立標準技術研究所(NIST)は、NIST IR 8473「EV超急速充電インフラのサイバーセキュリティフレームワークプロファイル」により、EV超急速充電インフラのサイバーセキュリティリスク管理に関するガイダンスを最終決定しました。[345]

EVの充電ステーションと充電インフラは、複雑なインフラ、相互接続性、および複数のデータネットワークに依存しているため、さまざまなサイバーセキュリティの脅威に対して脆弱です。NIST IR 8473は、EV充電環境全体をカバーする包括的な枠組みを提供します。ガイドラインには以下の項目が含まれます。

- 電気自動車
- 超高速充電（XFC）
- XFCクラウドまたはサードパーティの運用
- ユーティリティおよびビルネットワーク

さらに、NIST IR 8473には、ISO 21434規格に基づくデータ保護に関するセクションが確立されています。[346]

NISTが提案する枠組みは任意ですが、EV充電関係者がリスク管理プロセスの一環として、サイバーセキュリティ態勢を理解、評価、伝達するための具体的なプロセスを開発できるように設計されています。

2024年8月、米国政府はクリーンエネルギーシステムのサイバーセキュリティを強化するための包括的な計画を発表し、特に国家の電力網およびEV充電インフラの保護に重点を置きました。 クリーンエネルギーにおける相互接続されたスマートテクノロジーへの依存度が高まっていることを認識し、この取り組みは、サイバー攻撃によって悪用される可能性のある脆弱性を軽減することを目指しています。 この計画では、電力網の防御の近代化、EV充電ネットワークへの堅牢なセキュリティ対策の実施、および進行中のクリーンエネルギーへの移行を支援するためのこれらの重要システムの回復力の確保を優先しています。[347]

英国

英国はEVCS規制の最前線に立っています。 2021年12月、英国規格協会（BSI）のスマートエネルギー搭載スマート家電（ESA）の規制対象にEVCSを含める提案がなされました。[348]

2022年6月、電気自動車（スマート充電ポイント）規制2021が施行され、民間充電ポイント（家庭用および職場用）に適用されました。[349]

英国の規制では、充電器は以下の要件を満たすことが求められています。:「デマンドサイド・レスポンス・サービス等のスマートな機能」、「電力供給業者との相互運用性」、「通信ネットワークにアクセス不能でも充電可能」、「安全性の向上」、「充電統計の透明性を高める測定システム」、「オフピーク時のデフォルト充電スケジュール」、「需要の急増から保護するためのランダム化された遅延」、「コンプライアンス保証のための遵守声明」、「10年間の販売登録」新たなサイバーセキュリティ要件については、2022年12月に発効した規則の附則1にも概説されています。[350] 充電器にはこれらの設定が予めされていますが、所有者の好みに合わせて調整することができます。

EV充電システム（EVCS）の販売者および運営者向けガイダンスレターは2022年2月に発行され、直近では2023年6月に更新されました。この中で、EVCSのサイバーセキュリティ要件を欧州ETSI EN 303 645規格に合わせることを推奨しています。
ETSI EN 303 645は、提案されたベンチマークと測定可能な目標に基づいて選択されました。[351]

2024年10月、英国運輸省は、「公共充電ポイント規制2023」（The Public Charge Point Regulations 2023）の理解を深めるため、一般に利用可能なEV充電ポイントの運営者向けに最新のガイダンスを発行しました。[352] これらの規制は2023年11月に公布、施行され、2024年11月以降に設置される公共充電ポイントに対して多くの要件が義務化されています。[353] また、この規制は、決済方法、価格の透明性、信頼性、データアクセシビリティーなどの分野に焦点を当てています。具体的なサイバーセキュリティ・プロトコルについては詳述されていませんが、コンプライアンスの遵守には、データ、決済システム、充電ポイントの運用の完全性を保護するための強力なサイバーセキュリティ対策を実施する必要があります。

日本

日本におけるEVCSのサイバーセキュリティ保護対策は、2020年11月の経済産業省（METI）の「IoT セキュリティ・セーフティ・フレームワーク」[354] 、2019年6月の総務省（MIC）による「IoT 5G総合セキュリティ対策」[355] など、IoT機器を対象とする規制に基づいています。

世界中で使えるEV（電気自動車）充電の規格

ISO 15118

ISO 15118は、電気自動車（EV）と充電ステーション（EVSE/EVCS）間での通信を暗号化し、安全に行うための世界的なサイバーセキュリティ規格です。これにより、充電中の通信を保護します。また、この規格は高レベルな通信プロトコルとされ、[356] コンバインド・チャージング・システム（CCS）のセキュリティ規格として機能しています。[357]

ISO 15118規格は、「Plug and Charge（プラグ＆チャージ）」という便利な仕組みを管理しています。この仕組みには、次の3つの大事なステップがあります。

01

機密性

メッセージはTLSプロトコルを使用して暗号化されます。

02

データの整合性

メッセージは、秘密鍵（プライベートキー）と公開鍵（パブリックキー）のペアを使って、壊れたり改ざんされたりしないように保存されます。

03

真正性

送信者の身元および送信されたメッセージの信頼性は楕円曲線デジタル署名アルゴリズム（ECDSA）により保証されます。[358]

ISO 15118は、電気自動車（EV）が電力を充電したり、余った電気を電力会社に送り返したりする（これをV2G技術と呼びます）時のサイバーセキュリティについての規格です。この規格は、EV、充電器、電力会社、そしてサービスを提供する会社など、充電に関わる全ての人や仕組みに適用されます。

- 電気自動車（EV）
- 充電ステーションとCPO（充電ポイント運営者）
- データ処理と保存を担当するクラウドオペレーター
- 電力網（ユーティリティ/ビルディング管理システムとも呼ばれます）

コンバインド・チャージング・システム（CCS）

CCSは世界中の多くの自動車メーカー（OEM）によってサポートされている、最も重要な充電規格の1つです。CCSのサイバーセキュリティ対策はISO 15118に準拠しています。[359]

DIN SPEC 70121

DIN SPEC 70121はISO 15118のドイツ版の前身であり、ISO 15118の初期の未公開版の理論的な原則に基づいて構築されました。 DIN SPEC 70121には、スマート充電やセキュアTLS通信など、ISO 15118により更新された機能は含まれていません。

CHAdeMO

CHAdeMO（チャデモ）は日産、三菱、トヨタなどの自動車メーカーによって作られた日本発の電気自動車の急速充電規格です。（「Charge de Move」の略）CHAdeMO（チャデモ）は2009年に初めて導入され、ISO 15118標準に代わる選択肢を提供することを目指しています。[360] ISO 15118と同様に、CHAdeMOもV2G通信におけるセキュリティ対策を含んでいます。 充電プロセスは、ユーザーのVIN（車両識別番号）を確認し、IPv6のセキュリティ対策と契約鍵暗号化を組み合わせることで可能になります。

2023年9月に、CHAdeMOは「外部充電設計ガイドライン ver.2.0.1」を発表しました。このガイドラインでは、ACD-U（車両下部自動接続装置）充電システムをCHAdeMO充電器やV2X機器、電気自動車（EV）、プラグインハイブリッド車（PHEV）に安全に統合または後付けするための技術的および運用上の要件が追加されています。[361]

OCPP 2.0.1

オープン・チャージ・ポイント・プロトコル（OCPP）は、オープン・チャージ・アライアンスによってつくられ、2013年に初めて導入されました。現在、バージョン1.6から2.0.1に移行中です。OCPP（Open Charge Point Protocol）は、EVCS（電気自動車充電ステーション）とCSMS（充電管理システム）の間で安全な通信を行うための代表的なオープンソース規格です。この規格（OCPP）は、ISO 15118と並行して運用されています。

バージョン1.6から2.0.1への主な改良点には、次の機能が含まれています：複数のメーカーの充電ポイントを管理するオペレーター向けのデバイス管理の効率化と取引処理の改善、安全なTLS暗号化を使用した認証および安全な更新によるセキュリティの向上、そしてISO 15118のサポート。[362]

2024年11月に、OCPP 2.0.1（エディション3）のアップデートがリリースされました。このアップデートでは、プロトコルの機能性と信頼性を向上させるためのさまざまな修正と内容の分かりやすい説明が追加されました。[363]

ISO 15118は車両と充電ステーション間の通信を保護するのに対し、OCPP（Open Charge Point Protocol）は、充電ステーションとバックエンドサーバー（管理システム）間のセキュリティの側面をカバーしています。これには、CPO（充電サービスプロバイダー）、通信、そして電力管理も含まれています。[364]

07.

自動車サイバーセキュリティソリューション

ステークホルダーは、サイバーセキュリティリスクの増大と新たに生じるギャップに効果的に対処するためにAIを活用したサイバーセキュリティツールの導入を検討すべきです

進化を続けるサイバーセキュリティソリューション

自動車業界のデジタル化が進む中、自動車サイバーセキュリティソリューションも進化しています。 サイバー脅威がますます巧妙化、大規模化し、頻発する中、サイバーセキュリティソリューションは、膨大な数のモビリティ資産と絶えず変化するSBOM（ソフトウェア部品表）に対して、効果的かつ迅速に対処しなければなりません。 車両サイバーセキュリティチームおよび車両セキュリティオペレーションセンター（vSOC）は、車両への直接的な攻撃にとどまらず、車両フリート、コンパニオンアプリ、モビリティサービス、モビリティIoTデバイス、EV充電インフラなどを標的とした脅威についても調査しなければなりません。

現代の車両におけるネットワーク接続が向上したことにより、サイバー攻撃の規模と影響を飛躍的に拡大させる要因となりました。OEMとそのサプライチェーンにとってサイバーセキュリティの課題が増大し、信頼性、安全性、運用上の可用性が危険にさらされています。

スマートモビリティのステークホルダー、OEM、Tier-1、Tier-2は、新しい基準や規制が採用される中で、引き続きサイバーセキュリティを重要な優先事項として位置づけています。

> ***今後もコネクテッドカーとモビリティサービスの安全性を確保し、サイバーセキュリティのギャップを最小限に抑えるためには、多層的なサイバーセキュリティアプローチの採用が不可欠です。***

複雑なサプライチェーンと変化するSBOMの中で、ライフサイクル全体にわたって車両を保護

車両の耐用年数は通常、乗用車は12年、商用トラックは20年、農業用車両は30年です。 そのためOEMは、数十年前の技術による製品を確保するための長期的な戦略を開発しなければなりません。 UNECE.29 R155およびISO/SAE 21434は、開発から生産、そして生産後の車両のライフサイクル全体を網羅して、サイバーセキュリティの脅威と脆弱性を考慮する必要性があるとしています。

2022年に初めて、OEMとそのサプライヤーが正式な規制と標準化の対象となりました。 2024年までに、UNECE規制とISO/SAE 21434規格の適用が一定の水準を超え、業界標準として確立されたことで、グローバルオペレーションを根本的に変革します。 重要な節目は2024年7月で、R155の2番目のマイルストーンが発効した際、新たに製造されるすべての車両のモニタリングが義務付けられました。 この透明性により、サプライチェーンのボトルネックを乗り越え、生産の混乱に関する長年の懸念に対処することができました。 OEMは、サプライヤーに厳格なサイバーセキュリティプロトコルの遵守を求めることで、サードパーティベンダーによってもたらされる脆弱性のリスクを軽減しました。

R155は、OEMに対し、車両のライフサイクルの全段階を通じて脅威分析とリスク評価（TARA）を実施し、維持することを義務付けています。また、OEMはTier-1およびTier-2サプライヤーと共に、将来の攻撃に対処し軽減するためのプロセスを作成しなければなりません。ISO/SAE 21434は、サプライヤーと共にR155の要件を実施する方法のガイダンスとして活用できます。

01

サイバー対応能力の記録

OEMは、サプライヤーのサイバー履歴を確認し、サプライヤーが関連コンポーネント全部に対して継続的にリスクと脆弱性の管理を行うことを確認する責任があります。

02

共有責任の明確化

サイバーセキュリティの責任は、サイバーセキュリティインターフェース協定（CIA）を使用して共有および文書化されます。これにより、責任分担の不明確さによって見落とされることがないようにします。そして実行責任者、承認者、支援者、報告を受ける人、助言者（RASIC）などの確立されたプロジェクト管理手法を活用して進めることが出来ます。

OEMとサプライヤーがどのような分担方法に合意したとしても、OEMはR155およびR156を遵守し、ISO/SAE 21434の要件に従った取り組みを実施する責任を負います。

設計段階からのセキュリティ

車両のサイバーセキュリティに関するR155の規制で明確に指定されている4つの対策のうちの1つは、バリューチェーン全体におけるリスクを軽減するために「設計段階から」車両の安全を確保することです。 設計段階からのセキュリティでは、開発段階の早い時期にコンポーネントまたはソフトウェアのサイバーセキュリティリスクを評価する必要があります。 この手法は、すべての車両コンポーネントとサブシステムがサイバーセキュリティの脆弱性に対して設計、開発、テストされ、発見された適用可能なリスクが効果的に軽減されることを確認することで実現されます。 OEMが、車両のセキュリティの最終的な責任を負いますが、サプライチェーン内のサプライヤー全員も、設計段階からのセキュリティの実践を採用する必要があります。

多層的なサイバーセキュリティスタック

製造後の段階では、コネクテッドカー、スマートモビリティアプリケーション、およびデバイスは、強固で多層的なサイバーセキュリティ対策が求められます。 この取り組みは、ITや企業のサイバーセキュリティの標準として長い間確立されてきています。現在ますます巧妙化する脅威や新たな脆弱性に対抗するため、自動車業界やスマートモビリティのステークホルダーにも採用されています。

企業は、エンドポイントソリューション、ネットワークセキュリティソリューション、クラウドセキュリティ、APIセキュリティ、内部セグメンテーション技術など、複数のセキュリティソリューションを活用しています。

2019年、ガートナー社はセキュリティオペレーションセンター(SOC)可視化トライアドというネットワーク中心の概念を導入し、標準化しました。[365]

ガートナー社の調査によると、最新のSOCは、脅威の可視化、検知、対応、調査、修復を強化するために、よく知られた3つの主要なセキュリティ要素を駆使する必要があるとされています。

01

セキュリティ情報およびイベント管理（SIEM）

ITインフラ、アプリケーション、その他のセキュリティツールから生成されるイベントログやセキュリティアラートを収集し、分析します。

02

ネットワーク中心の検知および対応

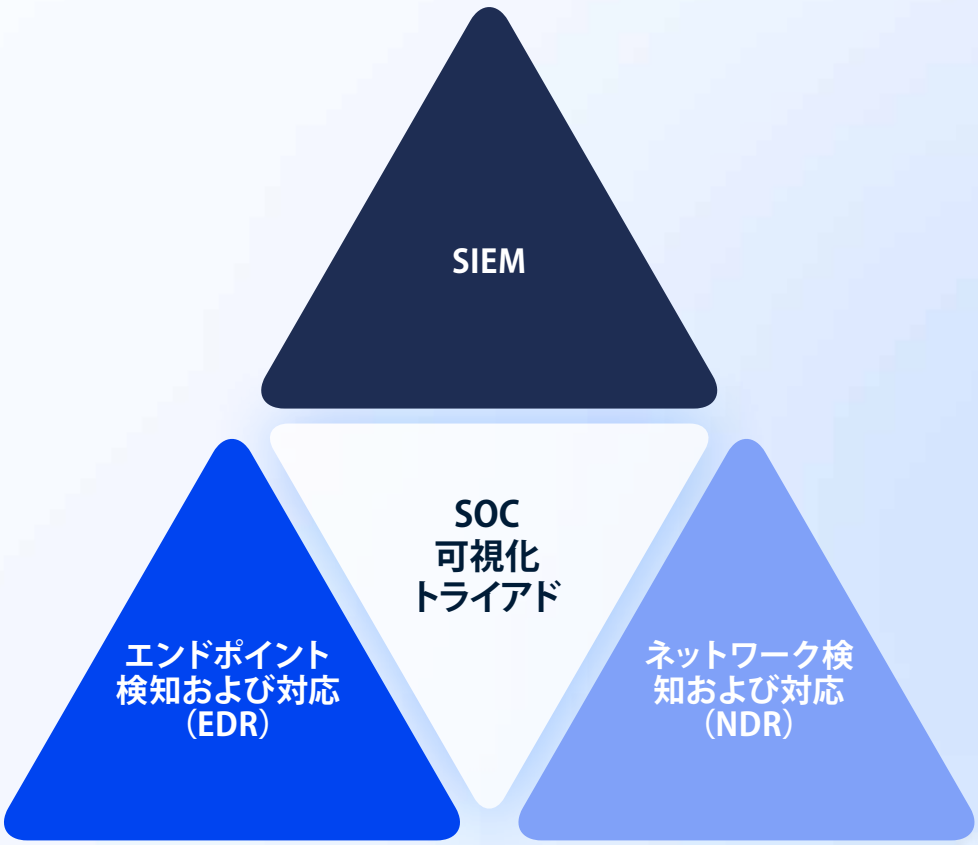
ネットワークトラフィックを監視し、検出された脅威とネットワークアクティビティを関連付けます。AI（人工知能）とML（機械学習）は、既知及び未知のリスクの検出に効果を発揮する必須の技術です。

03

エンドポイント検知および対応

エンドポイント（サーバー、デスクトップ、ラップトップ）の操作を監視することで、迅速に攻撃の兆候を特定します。

SOC可視化トライアド



Source: Upstream Security

ガートナー社のSOC可視化トライアドに基づくマルチレイヤーSOCアプローチの視覚的表現[366]

自動車産業がスマートモビリティエコシステムに進出したことによって、サイバーチームの課題であるモビリティー資産は自動車そのものだけではなくなりました。 SOCのアプローチをvSOCに適用することで、OEM、Tier-1、テレマティクス・サービス・プロバイダー（TSP）、およびエコシステム内のその他のステークホルダー間に、より安全なレイヤーが構築され、脅威を最小限に抑えて、攻撃を防ぐことができます。OEMサーバーやITバックエンドインフラをサイバー攻撃から守るITネットワークセキュリティに加えて、vSOCでは車両検出と応答（V-XDR）に焦点を当てた新しい保護レイヤーが追加されます。

自動車サイバーセキュリティにおけるの3つのレイヤー

APIセキュリティ

vSOCに新たに追加されたこの機能は、vSOCとIT SOC間の機能横断的な取り組みであり、APIベースのアプリケーション、サービス、機能の保護に重点を置いています。 APIセキュリティでは、車両へのアクセスやさまざまな機能にAPIが不可欠であるため、車両の保護対策も講じています。

自動車クラウドセキュリティ

自動車クラウドを活用し、監視することで、車両テレマティクス、OTAアップデート、リモートコマンド、診断など、幅広いモビリティ資産及びサイバー脅威の検知を強化します。また、車両、アプリケーション、その他のコネクテッドサービスにわたるセキュリティを車両群全体で把握し、複数の車両にまたがる攻撃を特定します。

車両セキュリティ

ECU、診断データストリーム、ホストセキュリティ情報、CAN / イーサネットイベントなどの車両内部コンポーネントを監視および保護します。

Source: Upstream Security

自動車インフラの各レイヤーには、サイバーセキュリティに関する固有の課題があります。これらの課題は、V-XDRと専用vSOCを含む多層的なアプローチで対処することができます。

効果的なAIドリブンでのVSOCの開発

多くの大企業では、ITシステム、インフラ、資産の監視にSOCが日常的に利用されています。 しかし、OEMが直接管理するITインフラとは異なり車両は常に動いており、直接の管理下には置かれません。そして、車両は外部のシステムやアプリケーションと1分間に何千回ものやりとりを行います。

OEMは、vSOCの確立と社内での位置づけに継続的に取り組んでいます。OEMは、vSOCのスコープの定義づけを行っており、組織構造のどこに組み入れるかを決定し、ソーシング（社内、ハイブリッド、マネージドvSOCなど）や運用モデル（ワングローバルvSOC、複数の地域での展開など）について評価しています。 OEMはR155に準拠するためにできるだけ早くvSOCを確立する必要があります。
vSOCの導入には選択肢がいくつかあります。

- 既存のSOCから独立したvSOC構築
- 生産後のコネクテッドカーに特化し、規制要件と法令順守を重視
- CISOを報告先として管理するが、時にはアフターセールスやグローバルオペレーション部が管理する
- 場合によっては、コネクテッドカーのインフラであるIT面(自動車クラウド)にも焦点を当てる

しかしながら、一部のOEMではすでにvSOCの成熟度はより高いレベルに達しています。 規模が拡大し、vSOCのプロセスと知識が成熟していることへの対応として、2つの新しいタイプのvSOCが登場しています：

フュージョンvSOC

基本的なvSOC機能とOTAヘルスモニタリング、DTCモニタリング、サイバーなどを組み合わせたクロスファンクショナルなアプローチを取り入れています。フュージョンvSOCは、スマートモビリティエコシステム全体にわたるデータドリブン型サービスとアプリケーションを保護するため、IT SOCとの緊密な連携が必要です。これは、複雑な攻撃ベクトルを検出し効果的に軽減するために重要です。

IT-OT vSOC

IT SOC、OT SOC、vSOC を統合し、広範なセキュリティ運用センターを一元管理します。設計から製造（車両生産の OT 監視など）まで、車両のライフサイクル全体のセキュリティ要素を網羅します。 また多くのOEMは、IT-OT vSOCのスコープを拡大しています。そうすることで、車両関連APIに加えてエンタープライズAPIも含めた組織全体のAPIセキュリティリスクの監視が可能になります。 中には、EV充電ステーションや関連インフラを含めた拡大を検討している企業もあります。

コネクテッドカーの運用データの大部分は、OEMが所有・管理しています。 将来的には、多くのステークホルダーがコネクテッドカーのデータやAIツール、機能へのアクセスが必要となり、劇的に移行していくと考えられます。

フリートの所有者やオペレーター、モビリティサービスプロバイダー、州政府、地方自治体などのスマートモビリティ関係者は、OEMが運営するものとはまったく異なるビジネス目標を持つ、独自の独立したvSOCを確立する必要があるかもしれません。

車両、モビリティアプリケーション、OTおよびIoTモビリティデバイスを標的とするサイバー攻撃の数と巧妙さが増す中、OEMは 「モビリティSOC」または「自動車SOC」とも呼ばれる 統合 vSOC を開発し、製造後の段階で車両、インフラ、顧客を保護する必要があります。 AIおよびML技術は、新たなサイバーセキュリティリスクの影響に対抗する上で重要な要素です。

効果的な vSOC は適切に実施されれば、明確なフレームワークを携えます。それは、能力、構成要素、運用モデルを詳細に示し、また、ビジョン、ミッション、運営方針を含んで、明確に定義付けた戦略と範囲も示します。 高度なAIモデルは、多くのvSOC機能において重要な要素となります：

- 24時間365日稼働
- 自動車に関するさまざまなフィードからデータを取り込み、各フィード間の相関を分析
- ガバナンスの概要と運営方針、基準、手順、プロセスの指針
- SIEMやSOARプラットフォームと統合し、組織を横断的に可視化し効果的な修復を実現

- 自動車に特化したサイバーセキュリティ分析により、脅威と異常をほぼリアルタイムで検出
- アラートの効果的なトリアージと調査
- パープルチーム、脅威モデル、脅威インテリジェンス融合を活用し、出現前にその脅威を予測
- 積極的な脅威ハンティングの実施
- エンドツーエンド（E2E）のプレイブックの構築・導入し、インシデント対応を構造化・自動化

必要な機能を確実に提供するために、vSOCは以下の3つの方法で構築することができます：

01

統合

既存のエンタープライズSOCはモビリティ資産を含むように拡張可能ですが、OTの専門知識や特定のプラットフォームの追加、運用手順の変更が必要になります。

02

新規構築

新規に自動車向け専用のvSOCを設立することで、洗練されたチーム、プロセス、およびプレイブックを構築します。

03

委託

vSOC は、IT と自動車関連のサイバーセキュリティの両方に対応できるマネージド・セキュリティ・サービス・プロバイダー（MSSP）に委託することができます。

2024年の間は、多くのOEM企業は、vSOCの導入に注力し、その運用をR155に整合するよう努めました。 2024年7月に施行されたR155の2番目のマイルストーンでは、生産中のすべての新車およびカテゴリーL車両[367] に適用範囲が拡大され、自動車業界全体のサイバーセキュリティ基準を調和させる上で重要な一歩となりました。R155の適用範囲の拡大に伴い、より徹底した規制への取り組みと、より厳格なコンプライアンス措置の重要性が増しています。

OEM企業やスマートモビリティの関係者には、OWASP Top 10を超えた、状況に応じたAPIセキュリティアプローチが求められています。

実際のところ、エントリーレベルのAPIハッキングは比較的標準化されており、高度な技術的専門知識を必要とせず、特別なハードウェアなしでリモートで行うことができるため、他のタイプのシステムに比べて費用対効果の高い攻撃方法となっています。The Open Web Application Security Project (OWASP)におけるAPI セキュリティ Top 10[368] は、開発者とセキュリティチームがAPIのリスクを理解する際のIT業界の基準であり、脅威の進化に応じて更新されます。

2023年に更新されたトップ10リストには、次の通りです。

01 **オブジェクトレベルの認可不備**

02 **認証の不備**

03 **オブジェクトプロパティレベルの認可の不備**

04 **無制限のリソース消費**

05 **機能レベルの認可の不備**

06 **重要な業務フローへの無制限アクセス**

07 **サーバーサイドリクエストフォージェリ**

08 **セキュリティの設定ミス**

09 **不適切な資産管理**

10 **APIの安全でない使用**

更新されたOWASP API Top 10のリスク一覧では、進化する脅威の状況について触れ、十分な警戒とプロアクティブなサイバーセキュリティ対策が不可欠であると強調されています。 APIを利用した攻撃の影響は、サービスの中断、車両とドライバーの安全性、データ漏洩とプライバシーの侵害、サブスクリプションや機能制限の回避を狙った不正行為、さらにはブランドの評判にまで及びます。

しかし、自動車とスマートモビリティのエコシステムでは、OWASPのようなITベースのAPIセキュリティだけでは不十分です。ITベースのセキュリティソリューションは、主にトランザクション、パーミッション、ボリューム、バリュー、ペイロードの正確性に重点を置いています。しかし、多くの場合、モビリティ資産が置かれた状況や道路上での物理的な動作、安全性への影響を無視しています。拡張検出では、 APIトラフィックに加えて、テレマティクスデータなどの追加のデータソースも考慮する必要があります。これら2つの情報源を組み合わせることで、組織は潜在的な脅威と脆弱性についてより深く理解することができます。APIセキュリティには、車両、アプリケーション、消費者の状況を反映させるために、運用データとAPIトラフィックをコンテキスト化する包括的な視点が必要です。

APIトラフィックやドキュメントに加えて様々なデータソースを活用することで、運用システムへの脅威を示す異常を特定することができます。

- 車両、ユーザー、およびデバイスの位置
- ユーザーおよび車両識別番号
- 車両テレマティクス
- 課金およびログイン履歴
- 充電ステーションのプロトコル

モビリティのステークホルダーは、APIベースのサイバーセキュリティリスクの監視や検出に関連する責任を見極めています。 このようなリスクは、エンタープライズSOC、vSOC、もしくは新しいIT-OT SOCで分析可能です。

自動車専用の脅威インテリジェンスを活用した予防的なリスク管理

多層的アプローチには、サイバー脅威インテリジェンスの監視など、脅威検出能力を強化するための予防的な対策も含める必要があります。OEM企業やモビリティ関連の関係者は、コンプライアンスを維持しながら、製品の脆弱性を事前に特定し、軽減することが求められます。 業界特有の目的に特化した脅威フィードを利用することで、関係者はサーフェスウェブ、ディープウェブ、ダークウェブの調査結果に基づく新たな脅威についての最新情報を継続的に把握できます。

コネクテッドビークルのエコシステムが進化するにつれて、大規模なサイバーリスクがもたらされ、自動車に対する脅威インテリジェンスの重要性がますます高まっています。 サイバーの脆弱性と攻撃は、サプライチェーン全体に影響を及ぼし、信頼と安全性が危険にさらされます。 そのため、すべての関係者がリスクの分析、脅威の監視、サイバー攻撃への迅速な対応を積極的に行う必要があります。

OEM企業がコネクテッド機能の向上を目指す中、脅威アクター（攻撃者）は車載通信システムやその他の車両のクラウドデータを標的にする傾向が強まっています。 自動車専用の脅威インテリジェンス製品のみが、車両の状況を把握し、異常を瞬時に特定し、システムの精度を低下させる恐れのある誤検知を除去することが可能です。

自動車サイバーセキュリティに対するUpstreamのAIドリブンおよびクラウドベースのアプローチ

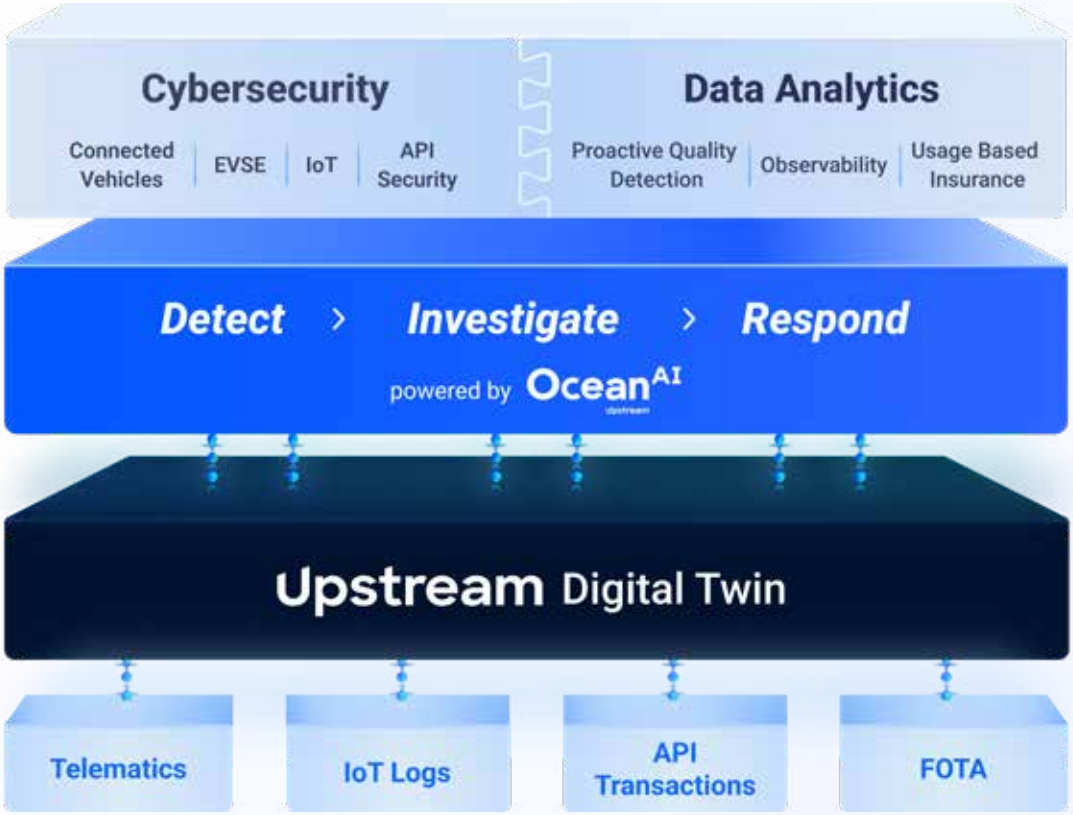
Upstreamにより、コネクテッドカー、IoT、スマートモビリティ向けに特別に設計された、世界初のクラウドベースのデータ管理プラットフォームは、自動車およびスマートモビリティのサイバーセキュリティに、根本的かつ革新的な変革をもたらしました。 他のサイバーセキュリティ保護アプローチが、各領域を個別に対応するのとは異なり、Upstreamは車載コンポーネント、IoTデバイス、テレマティクス、診断、消費者向けアプリケーション、OTAアップデート、EVチャージャーなど、スマートモビリティエコシステム全体にわたる、サイバー攻撃の領域を監視する独自のアプローチを開発しました。

Upstream Platform[369] はエージェントレスで、車両やデバイスにハードウェアやソフトウェアをインストールする必要がなく、比類のないサイバーセキュリティの検出と対応を提供します。

> ***Upstreamの高度なAI機能であるOcean AIを搭載したプラットフォームにより、ステークホルダーが多岐にわたるサイバーセキュリティ攻撃を効果的に検出、調査、自動化、および軽減することができます。***

Upstreamプラットフォームは、断片化された分散型モビリティデータを、集中化、構造化、文脈化したデータレイクに変換し、そのデータの可能性を最大限に引き出します。 このデータを活用することで、サイバーセキュリティの検出と対応（XDR）、不正防止、予防的な車両品質管理、可観測性、使用量ベースの保険など、さまざまなユースケースにわたって、高度なAIドリブン型アプリケーションを顧客に提供します。

2024年初頭、Upstreamは検出、調査、および対応プロセスに変革をもたらすように設計された、最先端のAIおよびML機能スイートであるOcean AI[369] を発表しました。Ocean AIは、データ効率、検出、実用的な洞察に重点を置いた高度なプラットフォーム機能と堅牢なMLベースの検出に加えて、生成AI(GenAI)機能を組み込んで、コネクテッドカーデータのROIを最大化します。 これらの機能により、組織はサイバー調査の実施と結果の最適化において、格段の柔軟性を得ることができます。

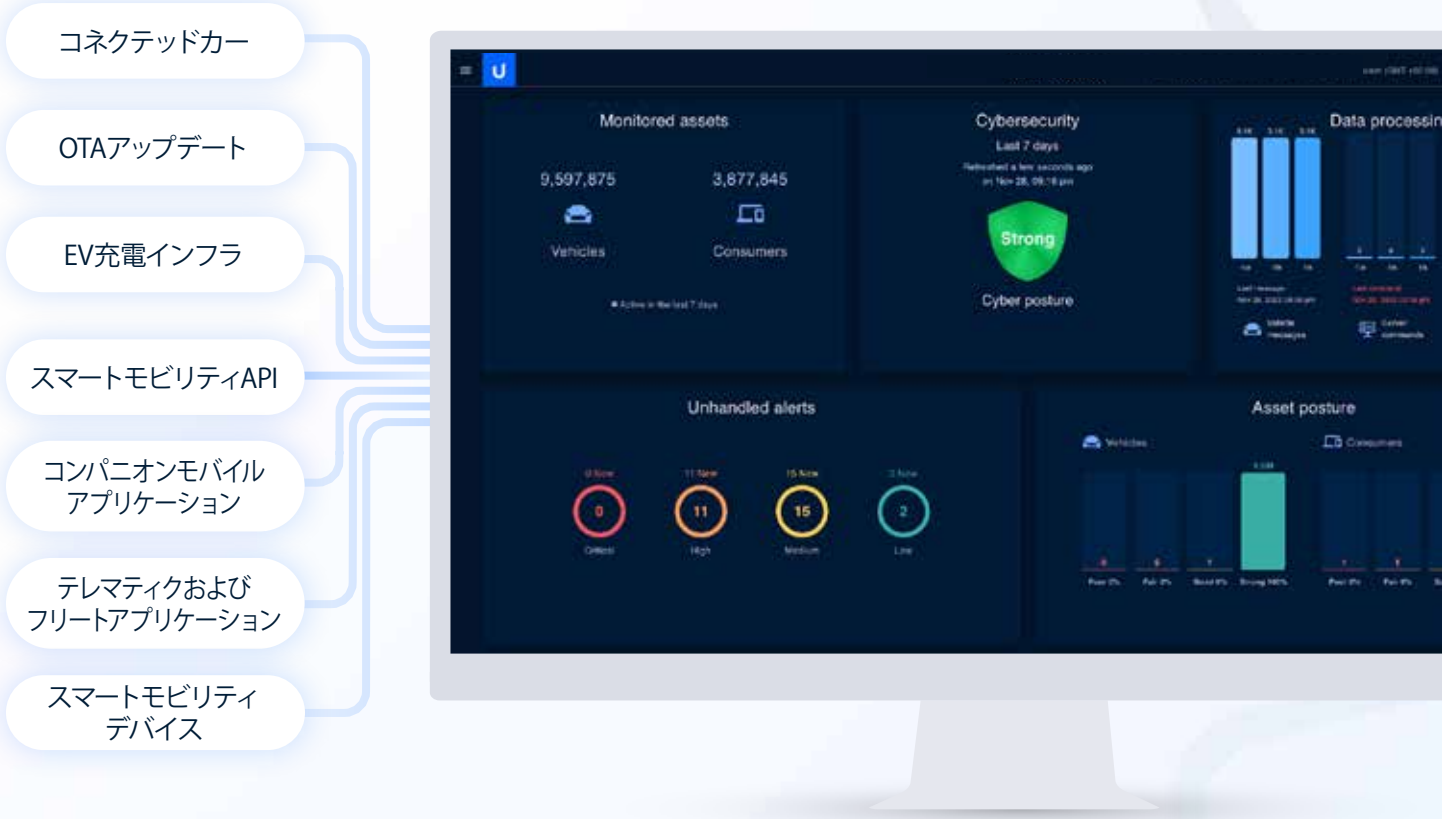


Source: Upstream Security

目的特化型の検出と対応プラットフォーム（XDR）

IT、OT、IoT、およびコネクテッドカーのデータを使用するように設計されたUpstream Platformは、高度な機械学習とAIモデル、そして既知および未知のモビリティ関連のサイバーセキュリティリスクに対応する何百もの検出器を含む、堅牢なサイバーセキュリティ検出、および対応プラットフォーム（XDR）[371] へと大幅に進化しました。

現在、世界中で何千万台もの車両、スマートモビリティデバイス、充電ステーションがUpstream Platformによって監視され、世界最大手のOEMやスマートモビリティ企業の一部に対して、検出や対応の取り組み、およびvSOC（仮想セキュリティオペレーションセンター）を支援しています。さらに、このプラットフォームは毎月数十億件の API トランザクションを監視しており、EV 充電インフラストラクチャ[372] やモビリティ IoT [373] を含むようにその範囲を拡大しています。これらはすべて、自動車とスマート モビリティのデジタルトランスフォーメーションの中核を成すものです。



Source: Upstream Security

Upstreamプラットフォームは、データの正規化とクレンジング、ライブデジタルツインプロファイリング、モビリティインテリジェンス、AIおよびMLを活用した検出、さらに独自の生成AI機能を活用してモビリティデータの異常を特定します。そして、モビリティ特化型アプリケーションを通じて、他に類を見ないデータドリブン型の実用的な洞察を提供します。

Upstream は多数のデータ ストリームを処理し、高度なデータドリブン型アプリケーションを開発できることから、自動車業界やスマート モビリティ業界の関係者にサイバー セキュリティの枠を超えた Upstream の利用拡大を促しています。

サイバーセキュリティXDR	サイバーセキュリティ関連の攻撃、脅威、リスク、脆弱性を監視、検出、調査します。
EV充電	EV充電ステーションおよびインフラを監視し、車両や電力網に影響を及ぼすリスクに加え、EV充電の運用可用性、安全性、データを標的としたサイバー攻撃を検出し、軽減します。
スマートモビリティデバイス	モビリティおよび輸送のエコシステムにおけるコネクテッドデバイスの安全性を確保し、監視することで、運用上の混乱を軽減し、機密データを保護します。
APIセキュリティ	スマートモビリティのAPI ベースのアプリケーション、デバイス、サービスを監視・保護し、継続的な運用可能性を確保し、データも保護します。
プロアクティブな品質異常検知	コンポーネントの故障をより早期に監視し、規模および重大性を予測し、根本原因分析(RCA)によってアフターセールス品質エンジニアを支援することで、最終的に保証およびリコールにかかるコストを削減します。
不正検出	走行距離の改ざん、車両盗難などの不正行為に関連するシナリオを特定します。

自動車およびスマートモビリティのデータストリーム用に設計されたデータエンジニアリング

自動車、モビリティ、輸送の各業界固有の多様なデータセットに対応するため、Upstreamはデータ正規化のための統一辞書を活用しています。その結果、プラットフォームは複数のデータフィード、ソース、およびテレマティクスサービスを効率的に一元化・標準化します。

ライブデジタルツイン

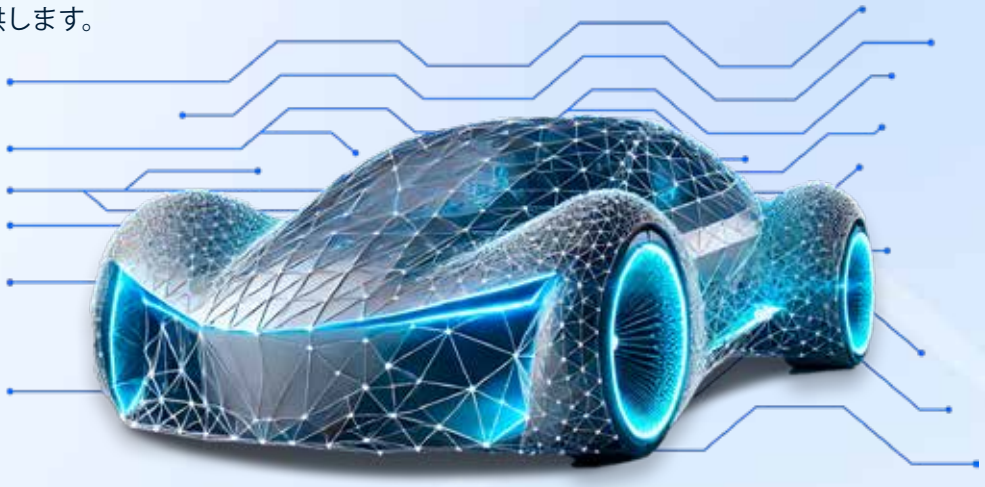
デジタルツインは、Upstreamプラットフォームのコア要素です。 クラウドに保存され、継続的に強化されることで、デジタルツインは、車両、スマートモビリティデバイス、EV充電ステーション、およびインフラ、アプリケーション利用者などあらゆる資産をデジタルで表現します。デジタルツインは多数のソースからデータを収集し、監視対象資産のライフサイクル全体にわたるリアルタイムのスナップショットを提供します。データ内のイベントおよび異常を統合することで、潜在的な攻撃を効果的に検出し、脅威を的確に特定します。

AIおよびMLを活用した検出と調査

Upstreamプラットフォームは、ドメインの専門知識およびMLを活用した異常検出機能を用いて、既知および未知の脅威を特定します。 AIおよびMLを活用した異常検出は、識別が難しい攻撃の発見に優れています。 このプラットフォームは、独自のモデルを使用して、個々の車両、消費者、およびフリート全体の動向を監視します。プラットフォームは、単一のエンドポイントに限定された異常な挙動、またはフリート全体にわたる異常な挙動を特定します。 Upstreamは、生成AIを活用した調査、自動化された修復および対応、そして自動車サイバーセキュリティ分野の専門知識や実績のあるプレイブックを駆使することで、迅速かつ効果的な脅威の軽減とSOCの最適化を実現します。

APIドリブンによるリスクを軽減するための検出および対応の拡張

API ベースのサイバー攻撃および脆弱性の急増に伴い、スマートモビリティの関係者は、毎月数十億件もの API トランザクションを監視するという課題に直面しています。UpstreamのAPIセキュリティレイヤー374は、APIトランザクションおよびUpstreamプラットフォームの堅牢なデジタルツインを関連付け、消費者向けアプリケーションからIoTデバイス、車両に至るまで、影響を受けるすべての資産について、状況的かつ包括的な視点を提供します。



UpstreamのAPIセキュリティソリューションにより、モビリティのステークホルダーは以下のメリットを得られます。

01

APIディスカバリー

文書化された、または文書化されていないAPI、および非推奨ながら稼働中のAPIすべてについて、リアルタイムのトラフィックデータ付きの完全なカタログを得られます。これには、サードパーティや内部サービスで使用されるAPIも含まれます。

02

APIモニタリング

静的および動的トラフィック ソースを検出しながら適合分析を継続的に実施し、API 環境における潜在的な脆弱性を特定します。

03

高度な検出

高度なAIおよびMLモデルを適用して、複雑な低負荷・低速攻撃を含む、未知の脅威や攻撃を効果的に検出します。

ノーコードの検出機能

カスタマイズと柔軟な検出を確保することは、長期的な俊敏性を維持するうえで非常に重要です。Upstreamプラットフォームは、Upstream独自のデジタルツインを活用したノーコードの検出機能ビルダーを提供しており、検出機能のカスタマイズや新たな検出機能の追加が容易に実現できます。これらの機能により、お客様はコーディングや開発リソースを必要とせずに、新たなユースケースに対応し、新しいビジネスロジックをサポートすることが可能になります。

プロアクティブなサイバー脅威インテリジェンス

UpstreamのAutoThreat® PROと緊密に連携することで、セキュリティチームは、各資産に特化した実用的なインテリジェンスを活用し、モビリティの脅威状況を前例のないレベルで可視化することができます。

AutoThreat® PROは、脆弱性インテリジェンスと自動車特有のエクスプロイト研究を組み合わせています。 それは、数百ものディープウェブ、ダークウェブ、クリアウェブの情報源を活用し、脆弱性やエクスプロイトを発見するとともに、脅威アクターの特定と対策を行います。. その範囲は、車載システムと車外システムの両方に及びます。車載インテリジェンスでは、IVIのジェイルブレイクやTCUのルート化など、車両内部で接続された機器の改ざんを検出します。一方、車外インテリジェンスは、外部や他社製品の脆弱性まで対象を広げ、　診断ツールやモバイルアプリの改ざんを通じた車両データや制御システムへの不正アクセスを含みます。

厳選されたインテリジェンス(HUMINT)により、ステークホルダーはUpstreamの堅牢なインテリジェンス収集インフラを活用して、カバレッジを拡大し、ディープウェブやダークウェブで安全かつ匿名で交流することができます。 Upstreamの専門サイバー脅威インテリジェンスアナリストは、自動車およびスマートモビリティのエコシステムに精通しており、脅威アクターの動機や効果的な緩和策について独自の洞察を提供することができます。

Source: Upstream Security

2024年3月、Auto-ISACは自動車業界のサイバー脅威の評価と共有を改善するための重要な取り組みである自動車脅威マトリックス（ATM）を導入しました。Upstreamは最近、自動車関係者が効果的にATMを運用できるよう支援するため、ATMをAutoThreat® PROに統合しました。[376]

AutoThreat® PROは、ATMの戦術と技術を活用し、影響を受けたコンポーネント、ベクター、および潜在的な影響に基づいて攻撃を整理します。これにより、サイバーセキュリティチームは脆弱性をより正確に特定でき、攻撃をMITRE ATT&CKフレームワークに関連付けることで、包括的な視野を得ることができます。

Upstream プラットフォームは、ディープウェブやダークウェブからの発見事項を関連するATM技術と自動的にリンクさせ、現在の脅威の包括的な視点を提供します。また、これらの発見を規則第155条附則5などの規制要件と整合させ、実行可能な洞察を提供し、コンプライアンスを加速させます。

AutoThreat®PROは、脅威アクターのインテリジェンスをATMにマッピングすることで、脅威アクターの活動と動機について独自の視点を提供します。これにより、サイバーセキュリティチームはリスクの優先順位付けを行い、積極的なリスク管理戦略を実施することができます。

Source: Upstream Security

UpstreamのAutoThreat® プラットフォームと AutoThreat®PRO

車両管理サービスおよびモビリティSOC

世界中の数百万台の車両とモビリティ端末を保護する最先端の車両管理サービスおよびモビリティSOCを活用し、包括的なサービスを通じてOEMのサイバーレジリエンスを強化しています。 UpstreamのSOC[377] で、コネクテッドカー、デバイス、およびそれらのコンポーネントを標的としているサイバー脅威を積極的に監視します。トップクラスの世界的な乗用車、商用車、農業用車両、EVのOEMとの経験を活かし、UpstreamのSOCはモビリティデータのソースを統合して多機能的な対応能力を構築します。

UpstreamのマネージドSOCは速やかに展開され、既存の企業プロセスとプラットフォームに統合されます。 ビルド-オペレート-トランスファー（BOT）モデルは、ベンダーロックインを回避した柔軟性を提供し、セキュリティチームがいつでも運用を引き継ぐことを可能にします。 各顧客の組織と作業方法に合わせてカスタマイズされたカスタム プレイブックと自動化されたワークフローにより、対応プロトコルが特定の顧客のニーズに適合し、脅威に迅速に対処できるようになります。 プレイブックには、不審なIPアドレスのブロック、車両所有者へのフィッシング試行の警告、OTAサーバーの制御など、自動化されたワークフローが含まれています。

包括的な脅威の検出と対応

UpstreamのマネージドSOCは、コネクテッドカーおよびデバイスのデータをほぼリアルタイムで監視し、APIセキュリティリスク、新たに出現するIoTの脅威、EV充電の操作、車両関連の不正行為、および車両全体に影響を与える脆弱性など、幅広いサイバー脅威から保護しています。 Upstreamプラットフォームを搭載したSOCは、AIとMLベースの検出を適用してデータをコンテキスト化し、既知および未知のサイバーリスクを特定します。

AIを活用した高度な調査と軽減措置

UpstreamのAI機能である、Ocean AIを搭載したマネージドSOCによって、アラート処理の最適化、ユニークなパターンの特定、迅速な対応を加速することで、前例のない効率性と緩和能力を実現します。 Ocean AIでは、Upstreamの充実したデータ、ライブデジタルツイン、および検出機能を活用して、深い洞察力を提供し、高度な調査を支援しています。また、脅威インテリジェンスを統合することで、リスク評価を強化します。

安全でコンプライアンスに準拠した運用

UpstreamのマネージドSOCは、フォロー・ザ・サンモデルを採用して、最先端の安全な施設によって運営されています。 GDPRなどの国際的なデータ保護規制に準拠し、ロールベースのアクセス制御（RBAC）を採用してデータのプライバシーを保護しています。 SOCはまた、運用全体にわたって高いセキュリティ基準を維持するために、リモート監査機能も提供しています。

モビリティおよび IoTの サイバー対策サービス

Upstreamは、自動車およびスマートモビリティエコシステム向けに特化した包括的なツールとシミュレーションスイートを用いて、製品セキュリティインシデント対応チーム（PSIRT）を支援するため、サイバーセキュリティサービスポートフォリオを拡大しました：[378]

- **インシデント対応トレーニング：**綿密なシミュレーションを通じた実践的な訓練により、準備態勢と運用準備を向上させます。
- **成熟度評価**：業界標準に対するサイバーセキュリティの現状評価を行い、強みと改善すべき領域を特定します。
- **ステークホルダー教育：**業界のベストプラクティスと進化する脅威に合わせて、チームの能力を調整するためのカスタマイズされたトレーニングプログラムです。

UpstreamのvSOC

08.

2025年の予測

マーティン・アレンド

BMWグループ 自動車セキュリティ部門
ゼネラルマネージャー

2025年を見据えると、自動車のエコシステムにおける脅威は増加傾向にあり、その背景にはAIの進化が大きく影響しています。 これらの脅威は、車両本体、その基幹システム、または車両と連携するモバイルアプリを攻撃対象とする可能性があります。

BMWグループでは、迅速かつ包括的に対応をするため、現場対策の有効性に重点を置くことを優先します。これらの課題に対処するため、当社は検知システムの信頼性と拡張性を優先し、サイバーセキュリティ戦略の基盤とします。

カリン・ショーペン

シスコセキュリティ タロスインテリジェンスグループ
プロダクトマネジメント担当VP

コネクテッド自動運転車（CAV）は、輸送手段に革命をもたらす革新的な技術です。 しかし、他の新しい技術と同様に、サイバー攻撃のリスクを伴います。これは、企業の経済活動を妨げ、一般の人々の安全を脅かす可能性があります。

車両接続性の向上、複雑なサプライチェーン、およびメーカーのデータ収益化の取り組みにより、CAVの攻撃対象領域は広範囲に及びます。CAVとそのエコシステムに対する全サイクルセキュリティ対策を開発し実行することの重要性と緊急性が高まっています。

ウルフ・シュラハター

DXB マネジメント
アドバイザリー部門CEO

EV充電インフラに対するハッキングのリスクは、重要なITシステムやインフラと相互接続していることから、緊急の課題となっています。 充電ネットワークの相互接続性が高まることにより、サイバー犯罪者が悪用する新たな脆弱性が生じています。不正アクセスされた充電ステーションは、より広範囲な攻撃の入り口となり、電力網や基幹ネットワークなどの重要なインフラを脅かす恐れがあります。

ハイブリッド戦争をめぐる最近の議論において、充電インフラのデジタル化と相互接続性の拡大は、サイバー攻撃の標的としての魅力を高めています。 これらのリスクを軽減するために、EV充電事業者とメーカーは、強固なサイバーセキュリティ基準を導入し、進化する脅威から安全を確保するために定期的な更新を徹底する必要があります。

オズグル・トフムク

AWS 自動車および製造部門
ゼネラルマネージャー

2025年には、高度なSDVモジュールとECU仮想化の導入がさらに進み、エンドツーエンドのE/Eアーキテクチャへの移行が加速するでしょう。仮想化されたECUとツールは車両ソフトウェア開発を効率化し、一方で生成AIはワークフローを加速化、サイバーセキュリティテストを強化、コード修正支援のための自動推論を可能にします。 OEMは、生成AIを活用してセキュリティ運用、検出、脆弱性管理、およびインシデント対応能力を強化します。

AIの急速な普及により、OEMは責任あるAIの実践を採用し、自動車における生成AIエッジアプリのセキュリティ上の課題に対処することが求められます。 主な検討事項としては、エッジでのコンテンツの管理、OTAモデル更新のセキュリティ対策、および物理的な攻撃による基盤モデルの窃取からサイバーフィジカルシステムを防御することです。 AIを活用したサイバーセキュリティに多額の投資が行われていますが、OEMは進化する脅威に対して強固な防御体制を構築するために、IDとアクセス管理、データ保護、脅威モデリングなどの基本的なセキュリティ対策を継続的に優先する必要があります。

マーティン・ホフマン

Terra Quantum AG
チーフビジネスオフィサー

UNECE WP.29やサイバーレジリエンス法といった国際的な規制の影響力が高まり、自動車メーカーは製品のライフサイクルとサプライチェーン全体にわたって、強固なサイバーセキュリティ対策を導入することを迫られています。

しかし、業界が電動化やAI、自動運転技術を推進するにつれて、サイバーセキュリティは単なるコンプライアンス上の必要性から、戦略的な競争上の優位性へと発展しました。

これらの変革的な技術には、広範囲に影響を与える可能性のあるサイバー攻撃を特定し対処するために、積極的で柔軟に対応できるアプローチが必要です。

広範な影響を及ぼすサイバー攻撃への対処

ヴィノッド・デソウザ

Google Cloud CISOオフィス
マニュファクチャリング&インダストリー責任者

2025年には、地政学的緊張と国家が支援するサイバー攻撃が自動車メーカーに対するリスクを増大させ、重要インフラや知的財産を標的とするでしょう。 ITとOTシステムの融合や相互接続されたテクノロジーへの依存度の高まりにより、攻撃対象が拡大し、新たな脆弱性を露呈する可能性があります。 ランサムウェアは生産ラインやサプライチェーンを標的とすることで、さらに破壊的になると予想されています。また、AIによる攻撃は、防御を突破するために、自動化と機械学習を活用し、より高度化するでしょう。

防御側によるAIの継続的な導入により、2025年には攻撃者に対して優位に立てるでしょう。しかし、ライフサイクルとサプライチェーン全体のリスクを効果的に軽減するためには、サイバーセキュリティにおける協調的なアプローチが必要です。 安全なクラウドプラットフォームの採用と情報共有の促進は、相互接続された環境におけるサプライチェーンのセキュリティ強化と回復力向上のための重要な戦略となります。

ティム・ガイガー

フォード・モーター・カンパニー
コネクテッド・サイバーセキュリティ
シニアディレクター

コネクテッドカーの普及が進むにつれ、自動車メーカーはますますサイバーセキュリティの課題に直面しています。 APIは、車両システム、外部デバイス、クラウドサービス間の通信を可能にする上で重要な役割を果たしています。 同時に、攻撃者はAPIの弱点を悪用する方法をどんどん賢く巧妙なものにしています。

自動車APIを保護することは、コネクテッドカーの安全性、プライバシー、信頼性を確保するために重要です。今日の積極的な対策が、将来の重大なインシデントを防ぐことにつながります。

Mike Lexa

CNHインダストリアル社
最高情報セキュリティ責任者(CISO)兼ITインフラ担当VP

2025年には、自動車業界のCISO（最高情報セキュリティ責任者）は、コネクテッドカー、自動運転車、電気自動車の普及によって、ますますサイバーセキュリティの課題に直面することになるでしょう。 これらのイノベーションは、攻撃対象領域を拡大することになりえます。例えば、無線での更新や、インフォテインメントシステム、車両同士が通信を行うこと（V2X）などの分野に弱点を生じさせます。 これらのリスクをさらに悪化させているのは、厳しくなる規制、複雑なサプライチェーン、そしてサイバー攻撃と防御の両方に使われるAIの二重利用です。

この進化する状況を乗り切るためには、CISO（最高情報セキュリティ責任者）は強力なサイバーセキュリティのフレームワークを導入し、厳密な第三者評価を実施し、積極的な脅威検出戦略を実行する必要があります。 規制への対応を最優先し、AIを活用したサイバーセキュリティソリューションを活用、従業員のトレーニングに投資することが、進化する脅威から守るために不可欠です。

ヨアヴ・レヴィ

Upstream Security
CEO(最高経営責任者)兼共同創業者

2025年に向けて、自動車業界におけるサイバーセキュリティの状況は、かつてないほど複雑になると予想されます。 脅威アクターはすでに、大規模で巧妙な攻撃手法に移行しており、車両だけでなく、EV充電インフラ、APIを利用した関連アプリ、販売店ネットワークといった相互接続されたシステムを標的にしています。 この拡大する攻撃対象領域には、サイバーセキュリティに対する変革的かつ積極的なアプローチが必要になります。

AIは、これらのリスクに対処する上で中心的な役割を果たすようになるでしょう。 すでに初期投資を行っている自動車メーカー（OEM）が多いですが、2025年にはAIの導入が加速し、検出、調査、そして緩和プロセス全体にわたって統合されるようになるでしょう。 リアルタイムのデータ処理により、異常をより早く検出し、脅威をより正確に特定し、自動化された迅速な対応が可能になります。これにより、モビリティエコシステムにおける保護のための新たな基準が確立されるでしょう。この進化する状況を乗り切るためには、高度なXDR（拡張型検出と対応）と強力なAPIセキュリティを組み合わせた未来を見据えた戦略が不可欠です。

参考文献

1. https://www.blackberry.com/us/en/company/newsroom/press-releases/2024/blackberry-qnx-research-reveals-rising-pressure-on-software-engineers-leads-to-critical-trade-offs-in-safety-and-security
2. https://unece.org/sites/default/files/2021-03/R155e.pdf
3. https://unece.org/sites/default/files/2021-03/R156e.pdf
4. https://www.iso.org/standard/70918.html
5. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504
6. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
7. https://www.govinfo.gov/app/details/CRPT-104hrpt736/CRPT-104hrpt736
8. https://www.pcisecuritystandards.org
9. https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx
10. Upstream's 2024 Global Automotive Cybersecurity Report
11. Upstream's 2024 Global Automotive Cybersecurity Report
12. https://home.treasury.gov/news/press-releases/jy2292
13. https://www.justice.gov/opa/pr/justice-department-charges-four-iranian-nationals-multi-year-cyber-campaign-targeting-us
14. https://www.justice.gov/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals
15. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a
16. https://www.sec.gov/newsroom/press-releases/2023-139
17. https://eur-lex.europa.eu/eli/dir/2022/2555
18. https://therecord.media/orbcomm-trucking-software-ransomware
19. https://www.bleepingcomputer.com/news/security/orbcomm-ransomware-attack-causes-trucking-fleet-management-outage/
20. https://cyberpress.org/orbcomm-data-breach-exposes-70-tb-of-data/
21. https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/
22. https://edition.cnn.com/2024/07/11/business/cdk-hack-ransom-tweny-five-million-dollars/index.html
23. https://www.andersoneconomicgroup.com/dealer-losses-due-to-cdk-cyberattack-reach-1-02-billion/
24. https://www.cyberdaily.au/security/10245-who-is-mogilevich-the-newest-ransomware-gang-on-the-darknet
25. https://www.bleepingcomputer.com/news/security/hyundai-motor-europe-hit-by-black-basta-ransomware-attack/
26. https://hackmanac.com/news/hacks-of-today-14-03-2024
27. https://www.quattroruote.it/news/industria-finanza/2024/04/15/mercedes_benz_rilevato_attacco_hacker_possibili_violazioni_ai_dati_dei_clienti.html
28. https://x.com/H4ckManac/status/1808912853526794442
29. https://x.com/FalconFeedsio/status/1822544253882614181
30. https://dailydarkweb.net/cybervolk-group-claims-cyber-attacks-against-chinese-companies/
31. https://www.hackster.io/news/madradar-triggers-hallucinations-in-autonomous-vehicle-sensor-systems-researchers-say-b56b87763cbd
32. https://www.techexplorist.com/study-finds-security-flaws-first-next-gen-lidar-systems/81641/
33. https://www.theregister.com/2024/05/10/baidu_apollo_hack
34. https://dl.acm.org/doi/10.1145/3636534.3649372
35. https://samcurry.net/hacking-kia
36. https://samcurry.net/hacking-kia
37. https://securityonline.info/cve-2024-35213-critical-vulnerability-discovered-in-blackberry-qnx-sdp/
38. https://arxiv.org/html/2409.01324v1
39. Source: Upstream Security
40. https://www.iata.org/contentassets/c8e90fe690ce4047a8edfa97f4824890/iata_safety_risk_assessment_gnss_interference.pdf
41. https://www.securityweek.com/bosch-nutrunner-vulnerabilities-could-aid-hacker-attacks-against-automotive-production-lines/
42. https://www.cbc.ca/news/canada/hamilton/ransomware-attack-1.7133457
43. https://www.telegraph.co.uk/news/2024/02/21/car-charger-withdrawn-hackers-could-attack-national-grid/
44. https://www.ndss-symposium.org/wp-content/uploads/vehiclesec2024-47-paper.pdf
45. https://www.trucking.org/economics-and-industry-data
46. https://lemken.com/de-de/lemken-aktuelles/landtechnik-news/detail/lemken-von-cyberattacke-betroffen
47. https://thecyberexpress.com/alleged-frotcom-data-breach/
48. https://www.redthreatsec.com/blog/greenlightspart1
49. https://www.fleetnews.co.uk/news/telematics-giant-microlise-suffers-cyber-attack
50. https://eur-lex.europa.eu/eli/dir/2022/2555

参考文献

51. https://data.consilium.europa.eu/doc/document/ST-12041-2023-INIT/en/pdf
52. https://www.consilium.europa.eu/media/69093/st16996-en23.pdf
53. https://www.cnbc.com/2024/09/20/eu-nis-2-what-tough-new-cyber-regulations-mean-for-big-business.html
54. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
55. https://www.europarl.europa.eu/news/en/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products
56. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet
57. https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime
58. https://docs.fcc.gov/public/attachments/DOC-401201A1.pdf
59. https://www.sec.gov/news/press-release/2023-139
60. https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework
61. https://www.iso.org/standard/88353.html
62. https://upstream.auto/blog/agricultural-oems-new-safety-and-availability-standards/
63. https://sgp.fas.org/crs/row/IF10964.pdf
64. https://www.uschamber.com/assets/archived/images/final_made_in_china_2025_report_full.pdf
65. https://newsletter.dunneinsights.com/p/surrender-to-china-or-punch-back
66. https://insideevs.com/news/715427/tesla-ev-production-shanghai-vs-global/
67. https://www.globaltimes.cn/page/202408/1317819.shtml
68. https://www.autohome.com.cn/rank/1
69. https://www.cnbc.com/2024/10/31/chinese-ev-maker-byds-quarterly-sales-overtook-teslas-for-the-first-time.html
70. https://www.globaltimes.cn/page/202401/1305028.shtml
71. https://english.www.gov.cn/news/202401/09/content_WS659ced27c6d0868f4e8e2e3b.html
72. https://www.sac.gov.cn/
73. https://igarr.com/2024/05/06/china-new-collision-safety-standards-for-passenger-vehicles/
74. https://english.www.gov.cn/news/202406/22/content_WS6676229dc6d0868f4e8e8708.html
75. https://wap.miit.gov.cn/jgsj/zbys/qcgy/art/2024/art_e1bb0d211dbf40a2949b28deb8a96d19.html
76. https://dissec.to/general/chinas-new-vehicle-cybersecurity-standard-gb-44495-2024/
77. https://ransomwareattacks.halcyon.ai/attacks/bianlian-attacks-keboda-technology
78. https://www.linkedin.com/posts/arun-mane-272456166_cybersecurity-iso21434-r155regulation-activity-7191932471561617409-MUPA/
79. https://ransomwareattacks.halcyon.ai/attacks/lockbit-ransomware-strikes-qufu-temb-auto-parts-in-china
80. https://www.techradar.com/pro/security/mystery-database-containing-sensitive-info-on-762-000-car-owners-discovered-by-researchers
81. https://dailydarkweb.net/cybervolk-group-claims-cyber-attacks-against-chinese-companies/
82. https://kevin2600-cmd.github.io/2024/09/13/Grand-Theft-Auto-A-peek-of-BLE-relay-attack.html
83. https://kevin2600-cmd.github.io/2024/09/13/Braktooth-Hunting-in-the-Car-Hacker%27s-Wonderland.html
84. https://edition.cnn.com/2024/02/07/cars/china-ev-global-push-intl-hnk/index.html
85. https://www.bis.gov/press-release/commerce-announces-proposed-rule-secure-connected-vehicle-supply-chains-foreign
86. https://www.reuters.com/business/autos-transportation/us-propose-barring-chinese-software-hardware-connected-vehicles-sources-say-2024-09-21/
87. https://www.politico.eu/article/europe-looks-to-follow-on-tackling-risk-of-chinese-car-software/
88. https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security
89. https://www.bbc.com/news/articles/cly20n4d0g9o
90. https://www.reuters.com/business/autos-transportation/china-tells-carmakers-pause-investment-eu-countries-backing-ev-tariffs-sources-2024-10-30/
91. https://securityaffairs.com/156843/reports/bmw-affected-by-redirect-vulnerability.html
92. https://therecord.media/foxsemicon-ransomware-attack-taiwan
93. https://techcrunch.com/2024/01/11/hyundai-motor-india-data-exposed/
94. https://techcrunch.com/2024/02/14/bmw-security-lapse-exposed-sensitive-company-information-researcher-finds
95. https://www.bleepingcomputer.com/news/security/hyundai-motor-europe-hit-by-black-basta-ransomware-attack/
96. https://www.delfi.lt/en/business/data-of-20-000-ignitis-on-clients-leaked-in-cyber-incident-95857777
97. https://www-theregister-com.cdn.ampproject.org/c/s/www.theregister.com/AMP/2024/03/22/boffins_tucktotruck_worm/
98. https://ransomwareattacks.halcyon.ai/attacks/bianlian-attacks-keboda-technology
99. https://hackread.com/ev-charging-firm-spills-trove-of-customer-info
100. https://www.techradar.com/pro/security/taxi-software-firm-breach-exposes-details-of-over-300000-passengers

参考文献

101. https://www.manager-magazin.de/unternehmen/autoindustrie/volkswagen-chinesische-hacker-sollen-vw-ueber-lange-zeit-ausspioniert-haben-a-2936f896-4d41-4ee3-8ccd-8abafc6b016d
102. https://www.youtube.com/watch?v=qWmiyprxziw
103. https://www.youtube.com/watch?v=B0yzk0Oi6mE
104. https://thecyberexpress.com/alleged-frotcom-data-breach/
105. https://www.standaard.be/cnt/dmf20240523_94739718
106. https://nvd.nist.gov/vuln/detail/CVE-2024-35537
107. https://securityonline.info/cve-2024-35213-critical-vulnerability-discovered-in-blackberry-qnx-sdp/
108. https://en.as.com/latest_news/cdk-global-and-their-car-dealership-software-what-we-know-about-the-ransomware-attack-n/
109. https://www.andersoneconomicgroup.com/dealer-losses-due-to-cdk-cyberattack-reach-1-02-billion/
110. https://blog.ret2.io/2024/07/17/pwn2own-auto-2024-charx-bugs/
111. https://cybersecuritynews.com/traffic-light-controller-authentication-bypass-vulnerability/
112. https://www.redhotcyber.com/post/il-threat-actors-888-rivendicata-una-compromissione-ai-danni-dei-clienti-bmw/
113. https://cybernews.com/security/android-head-units-drivers-data-safety/
114. https://www.businesskorea.co.kr/news/articleView.html?idxno=223166
115. https://innovationorigins.com/en/chip-hacking-poses-threat-to-public-transport-security/
116. https://arxiv.org/html/2409.01324v1
117. https://kevin2600-cmd.github.io/2024/09/13/Braktooth-Hunting-in-the-Car-Hacker's-Wonderland.html
118. https://samcurry.net/hacking-kia
119. https://cybernews.com/news/dutch-government-will-replace-hackable-traffic-lights/
120. https://cyberinsider.com/volkswagen-says-its-monitoring-the-situation-following-8base-ransomware-claims/
121. https://www.synacktiv.com/sites/default/files/2024-10/hexacon_0_click_rce_on_tesla_model_3_through_tpms_sensors_light.pdf
122. https://www.fleetnews.co.uk/news/telematics-giant-microlise-suffers-cyber-attack
123. https://cyberinsider.com/zero-day-flaws-in-mazdas-infotainment-expose-cars-to-takeover-attacks/
124. https://www.cyberdaily.au/security/11395-tesla-data-breach-falsely-claimed-by-intelbroker-third-party-ev-charging-firm-actually-breached
125. https://techcrunch.com/2024/12/12/researchers-find-security-flaws-in-skoda-cars-that-may-let-hackers-remotely-track-them/
126. https://github.com/zgsnj123/BYD_headunit_vuls/tree/main
127. https://www.bleepingcomputer.com/news/security/auto-parts-giant-lkq-says-cyberattack-disrupted-canadian-business-unit
128. https://www.bleepingcomputer.com/news/security/hyundai-motor-europe-hit-by-black-basta-ransomware-attack/
129. https://edition.cnn.com/2024/07/11/business/cdk-hack-ransom-tweny-five-million-dollars/index.html
130. https://www.andersoneconomicgroup.com/dealer-losses-due-to-cdk-cyberattack-reach-1-02-billion/
131. https://www.fleetnews.co.uk/news/telematics-giant-microlise-suffers-cyber-attack
132. https://theloadstar.com/cyber-attack-on-tech-provider-blacks-out-live-tracking-for-uk-retail-deliveries/
133. https://www.redhotcyber.com/en/post/intelbroker-claims-tesla-charging-database-breach/
134. https://www.cvedetails.com/cvss-score-distribution.php
135. https://nvd.nist.gov/vuln-metrics/cvss
136. https://www.thestack.technology/nvd-crisis-vulnerabilities-data-update/
137. https://therecord.media/nist-database-backlog-growing-vulncheck
138. https://www.nist.gov/itl/nvd
139. https://medium.com/@ravi8383soni/varta-shares-in-focus-looming-insolvency-and-cyber-attack-e1ae429e7bb3
140. https://www.varta-ag.com/en/about-varta/news-press/details/varta-makes-good-progress-in-solving-the-cyberattack
141. https://www.varta-ag.com/fileadmin/varta_ag/publications/ad-hoc_announcements/240315_VARTA_AG_Ad_hoc_Postponement_of_financial_reports_EN_final.pdf
142. https://www.nissan.com.au/website-update.html
143. https://www.bleepingcomputer.com/news/security/nissan-confirms-ransomware-attack-exposed-data-of-100-000-people/
144. https://www.eenewseurope.com/en/vulnerability-found-in-chargepoint-home-ev-chargers/
145. https://www.telegraph.co.uk/news/2024/02/21/car-charger-withdrawn-hackers-could-attack-national-grid/
146. https://www.researchgate.net/publication/377183224_Uncovering_Covert_Attacks_on_EV_Charging_Infrastructure_How_OCPP_Backend_Vulnerabilities_Could_Compromise_Your_System
147. https://www.greencarcongress.com/2024/07/20240717-swri.html
148. https://support-emobility.enelx.com/content/dam/enelxmobility/italia/documenti/manuali-schede-tecniche/Waybox-3-Security-Bulletin-06-2024-V1.pdf

参考文献

149. https://www.redhotcyber.com/en/post/intelbroker-claims-tesla-charging-database-breach/
150. https://www.ndss-symposium.org/wp-content/uploads/vehiclesec2024-47-paper.pdf
151. https://thecyberexpress.com/alleged-frotcom-data-breach/
152. https://www.securityweek.com/cyberattack-on-microlise-disables-tracking-in-prison-vans-courier-vehicles/
153. https://statescoop.com/kansas-city-traffic-system-still-down-after-cyberattack/
154. https://www.zigwheels.ph/car-news/mptc-encounters-data-breach
155. https://cybernews.com/news/dutch-government-will-replace-hackable-traffic-lights/
156. https://eaton-works.com/2024/01/17/ttibi-email-hack/
157. https://drivingpress.com/the-risks-of-autonomous-vehicles/
158. https://www.hackster.io/news/madradar-triggers-hallucinations-in-autonomous-vehicle-sensor-systems-researchers-say-b56b87763cbd
159. https://www.techexplorist.com/study-finds-security-flaws-first-next-gen-lidar-systems/81641/
160. https://www.theregister.com/2024/05/10/baidu_apollo_hack
161. https://dl.acm.org/doi/10.1145/3636534.3649372
162. https://eaton-works.com/2024/01/17/ttibi-email-hack/
163. https://hackread.com/ev-charging-firm-spills-trove-of-customer-info/
164. https://thecyberexpress.com/alleged-frotcom-data-breach/
165. https://cybernews.com/security/hertz-vulnerability-reveals-customers-data/
166. https://community.ui.com/releases/Security-Advisory-bulletin-039-039/44e24007-2c2c-4ac0-bebf-3f19b9b24f09
167. https://samcurry.net/hacking-kia
168. https://www.it-daily.net/en/shortnews-en/hacker-demands-125000-dollars-in-baguettes-from-schneider-electric
169. https://nvd.nist.gov/vuln/detail/CVE-2023-28895, https://nvd.nist.gov/vuln/detail/CVE-2023-28896, https://nvd.nist.gov/vuln/detail/CVE-2023-28897, https://nvd.nist.gov/vuln/detail/CVE-2023-28898, https://nvd.nist.gov/vuln/detail/CVE-2023-28899, https://nvd.nist.gov/vuln/detail/CVE-2023-28900, https://nvd.nist.gov/vuln/detail/CVE-2023-28901
170. https://nvd.nist.gov/vuln/detail/CVE-2024-39339
171. https://nvd.nist.gov/vuln/detail/CVE-2024-21462
172. https://nvd.nist.gov/vuln/detail/CVE-2024-6245
173. https://www.eenewseurope.com/en/vulnerability-found-in-chargepoint-home-ev-chargers/
174. https://www.telegraph.co.uk/news/2024/02/21/car-charger-withdrawn-hackers-could-attack-national-grid/
175. https://www.researchgate.net/publication/377183224_Uncovering_Covert_Attacks_on_EV_Charging_Infrastructure_How_OCPP_Backend_Vulnerabilities_Could_Compromise_Your_System
176. https://www.bright.nl/nieuws/1198728/phishing-met-valse-qr-codes-op-laadpalen-ontdekt-in-brussel.html
177. https://nvd.nist.gov/vuln/detail/CVE-2024-21550
178. https://www.redhotcyber.com/en/post/intelbroker-claims-tesla-charging-database-breach/
179. https://securityaffairs.com/160499/cyber-warfare-2/electronic-warfare-hit-defence-secretary-jet.html
180. https://ahmadmansourr.medium.com/hacking-more-than-130-000-car-worldwide-in-5-minutes-766e76003c67
181. https://cybersecuritynews.com/traccar-gps-system-vulnerability/
182. https://cybernews.com/security/gamooga-data-leak/
183. https://infosecwriteups.com/hacking-into-30-tesla-cars-around-the-world-using-a-third-party-software-00957ac68c92?gi=ce897b36be4a
184. https://darkwebinformer.com/888-allegedly-has-leaked-the-data-of-blink-ai-automotive/
185. https://jerinsunny.github.io/stm32_vglitch/
186. https://jerinsunny.github.io/blogs/2024/02/14/rh850-voltage-glitching.html
187. https://www.carscoops.com/2024/09/indiana-car-dealer-sued-for-rolling-back-odometers-14-million-miles/
188. https://www-theregister-com.cdn.ampproject.org/c/s/www.theregister.com/AMP/2024/03/22/boffins_tucktotruck_worm/
189. https://statescoop.com/kansas-city-traffic-system-still-down-after-cyberattack/
190. https://www.automotiveworld.com/articles/research-tackles-cosmic-ray-threat-to-avs-and-evs/
191. https://cybernews.com/security/gopass-colombia-data-leak/
192. https://www.zigwheels.ph/car-news/mptc-encounters-data-breach
193. https://cybernews.com/news/dutch-government-will-replace-hackable-traffic-lights/
194. https://nvd.nist.gov/vuln/detail/CVE-2024-33308, https://nvd.nist.gov/vuln/detail/CVE-2024-33309
195. https://www.autoindustriya.com/auto-industry-news/toyota-ph-reports-mytoyota-app-data-breach-some-customer-data-compromised.html
196. https://nvd.nist.gov/vuln/detail/CVE-2024-35537
197. https://www.hackster.io/news/madradar-triggers-hallucinations-in-autonomous-vehicle-sensor-systems-researchers-say-b56b87763cbd

参考文献

198. https://www.buffalo.edu/provost/messages.host.html/content/shared/university/news/news-center-releases/2024/08/self-driving-cars-attackers.detail.html
199. https://nvd.nist.gov/vuln/detail/CVE-2024-39081
200. https://www.autosar.org/fileadmin/standards/R20-11/FO/AUTOSAR_PRS_SecOcProtocol.pdf
201. https://icanhack.nl/blog/secoc-key-extraction/
202. https://www.gbnews.com/lifestyle/cars/toyota-lexus-drivers-compensation-keyless-car-theft
203. https://www.youtube.com/watch?v=qWmiyprxziw&ab_channel=AmynasecLabs
204. https://www.carscoops.com/2024/05/general-motors-faces-class-action-lawsuit-over-camaro-key-fob-security/
205. https://thecyberexpress.com/tesla-ultra-wideband-vulnerable-relay-attacks/
206. https://www.thestreet.com/electric-vehicles/forget-the-kia-boyz-a-new-exploit-leaves-kias-and-hyundais-vulnerable
207. https://kevin2600-cmd.github.io/2024/09/13/Grand-Theft-Auto-A-peek-of-BLE-relay-attack.html
208. https://eprint.iacr.org/2024/1816
209. https://nvd.nist.gov/vuln/detail/CVE-2023-0863, https://nvd.nist.gov/vuln/detail/CVE-2023-0864
210. https://cybernews.com/security/android-head-units-drivers-data-safety/#comments-reply
211. https://kevin2600-cmd.github.io/2024/09/13/Grand-Theft-Auto-A-peek-of-BLE-relay-attack.html
212. https://www.bleepingcomputer.com/news/security/mitm-phishing-attack-can-let-attackers-unlock-and-steal-a-tesla/amp/
213. https://www.infosecurity-magazine.com/news/cyber-attack-travel-chaos-seattle/
214. https://en.wikipedia.org/wiki/Cellular_V2X
215. https://gttwireless.com/dsrc-vs-c-v2x-comparing-the-connected-vehicles-technologies/
216. https://www.dwt.com/blogs/broadband-advisor/2023/05/fcc-connected-vehicles-c-v2x
217. https://www.its.dot.gov/research_areas/emerging_tech/pdf/Accelerate_V2X_Deployment_final.pdf
218. https://www.its.dot.gov/research_areas/emerging_tech/pdf/Accelerate_V2X_Deployment_final.pdf
219. https://www.its.dot.gov/research_areas/emerging_tech/pdf/Accelerate_V2X_Deployment_final.pdf
220. https://www.its.dot.gov/research_areas/emerging_tech/pdf/Accelerate_V2X_Deployment_final.pdf
221. https://www.cyberghostvpn.com/en_US/privacyhub/dark-web-vs-deep-web/
222. https://www.cyberghostvpn.com/en_US/privacyhub/dark-web-vs-deep-web/
223. https://forestvpn.com/blog/cybersecurity/how-much-of-the-internet-is-the-dark-web/
224. https://en.wikipedia.org/wiki/Darknet_market
225. Upstream Security
226. Upstream Security
227. Upstream Security
228. https://github.com/google/security-research/security/advisories/GHSA-c45w-xwww-rfgg
229. Upstream Security
230. Upstream Security
231. Upstream Security
232. Upstream Security
233. Upstream Security
234. Upstream Security
235. Upstream Security
236. Upstream Security
237. Upstream Security
238. Upstream Security
239. Upstream Security
240. Upstream Security
241. Upstream Security
242. https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/automotive-r-and-d-transformation-optimizing-gen-ais-potential-value
243. https://asia.nikkei.com/Business/Automobiles/Toyota-to-invest-13bn-in-EVs-AI-and-supply-chain
244. https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en
245. https://artificialintelligenceact.eu/article/15
246. https://www.twobirds.com/en/insights/2023/global/impact-of-the-eus-ai-act-proposal-on-automated-and-autonomous-vehicles
247. https://unece.org/sites/default/files/2021-03/R155e.pdf
248. https://unece.org/sites/default/files/2021-03/R156e.pdf

参考文献

249. https://www.iso.org/standard/70918.html
250. https://unece.org/sites/default/files/2024-05/ECE_TRANS_WP.29_2024_40e.pdf
251. https://unece.org/sites/default/files/2024-11/ECE-TRANS-WP.29-1179e.pdf
252. https://www.cyres-consulting.com/un-regulation-no-155-now-also-applies-to-motorcycles/
253. https://unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf
254. https://unece.org/fileadmin/DAM/trans/doc/2020/wp29/ECE-TRANS-WP29-2020-080e.pdf
255. https://clepa.eu/mediaroom/clepa-and-acea-join-with-auto-isac-on-motor-vehicle-cybersecurity/
256. https://www.itu.int/en/mediacentre/Pages/PR-2024-07-04-ITU-Radio-Regulations.aspx
257. https://www.ecfr.gov/current/title-47/chapter-I/subchapter-A/part-15
258. https://www.etsi.org/deliver/etsi_en/302500_302599/302571/02.01.01_60/en_302571v020101p.pdf
259. https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en
260. https://www.iso.org/standard/77845.html
261. https://standards.ieee.org/ieee/802.11p/3953/
262. https://www.sae.org/standards/content/j3105_202305/
263. https://www.sae.org/standards/content/j2945/1_202004/
264. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf
265. https://www.consilium.europa.eu/en/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts-new-law-on-security-requirements-for-digital-products/
266. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
267. https://unece.org/sites/default/files/2023-05/GRVA-16-26e.pdf
268. https://www.iso.org/standard/69113.html
269. https://www.switch-ev.com/blog/what-is-iso-15118
270. https://www.switch-ev.com/blog/basics-of-plug-and-charge
271. https://www.energy.ca.gov/event/workshop/2024-05/iso-15118-implementation-updates-workshop
272. https://genorma.com/en/standards/iso-15118-20-2022-awi-amd-1
273. https://www.sec.gov/news/press-release/2023-139
274. https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214
275. https://www.sec.gov/education/smallbusiness/goingpublic/SRC
276. https://www.databreaches.net/alphv-files-an-sec-complaint-against-meridianlink-for-not-disclosing-a-breach-to-the-sec/
277. https://edition.cnn.com/2024/07/11/business/cdk-hack-ransom-tweny-five-million-dollars/index.html
278. https://cyberscoop.com/cdk-ransomware-attack-sec-disclosure-material-impact/
279. https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf
280. https://www.govinfo.gov/content/pkg/FR-2022-09-09/pdf/2022-19507.pdf
281. https://upstream.auto/research/automotive-cybersecurity/
282. https://automotiveisac.com/press-news/auto-isac-partners-with-upstream-security-to-enhance-automotive-threat-landscape-visibility
283. https://www.telematicswire.net/asrg-partners-with-upstream-to-enhance-automotive-cyber-threat-intelligence/
284. https://apnews.com/article/automatic-emergency-braking-requirement-stop-standards-366abf6958eaf4e48e7ca4737075071b
285. https://static.nhtsa.gov/odi/inv/2024/INOA-PE24016-12382.pdf
286. https://nypost.com/2024/10/18/business/nhtsa-to-investigate-elon-musks-tesla-after-several-full-self-driving-crashes/
287. https://attack.mitre.org
288. https://automotiveisac.com/press-news/the-auto-isac-launches-automotive-threat-matrix-atm-tool-to-enhance-vehicle-cybersecurity-governance
289. https://eur-lex.europa.eu/EN/legal-content/summary/the-european-data-act.html
290. https://artificialintelligenceact.eu/
291. https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/05/cars-consumer-data-unlawful-collection-use
292. https://www.wyden.senate.gov/news/press-releases/wyden-investigation-reveals-new-details-about-automakers-sharing-of-driver-information-with-data-brokers-wyden-and-markey-urge-ftc-to-crack-down-on-disclosures-of-americans-data-without-drivers-consent
293. https://www.lexology.com/library/detail.aspx?g=c6ed5413-e6d1-4883-b164-d343fa199a83
294. https://complyauto.com/2024/03/05/wiping-in-vehicle-data-nj-dealers-now-required-to-offer-to-delete-certain-information/
295. https://news.bloomberglaw.com/privacy-and-data-security/internet-connected-car-privacy-questions-prompt-states-to-act
296. https://www.lexisnexis.com/community/insights/legal/capitol-journal/b/state-net/posts/states-beginning-to-regulate-popular-usage-based-car-insurance

参考文献

297. https://trustcassie.com/resources/blog/californias-new-car-privacy-law-sb-286/
298. https://www.reuters.com/business/autos-transportation/california-enacts-car-data-privacy-law-curb-domestic-violence-2024-09-30/
299. https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf
300. https://single-market-economy.ec.europa.eu/document/download/cd243af9-c877-401e-9f69-d7d4ab6a90c6_en
301. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
302. https://upstream.auto/blog/nis2-directives-impact-on-the-smart-mobility-ecosystem/
303. https://www.consilium.europa.eu/en/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts-new-law-on-security-requirements-for-digital-products/
304. https://alternative-fuels-observatory.ec.europa.eu/general-information/news/questions-and-answers-regulation-deployment-alternative-fuels
305. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401257
306. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1735
307. https://www.federalregister.gov/documents/2024/03/01/2024-04382/securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles
308. https://www.bis.gov/press-release/commerce-announces-proposed-rule-secure-connected-vehicle-supply-chains-foreign
309. https://www.reuters.com/business/autos-transportation/us-propose-barring-chinese-software-hardware-connected-vehicles-sources-say-2024-09-21/
310. https://www.regulations.gov/document/BIS-2024-0005-0059/comment
311. https://www.federalregister.gov/documents/2024/11/07/2024-24704/enhancing-surface-cyber-risk-management
312. https://www.nist.gov/cyberframework
313. https://www.cybersecuritydive.com/news/tsa-cyber-risk-management/732257/
314. https://english.www.gov.cn/news/202406/22/content_WS6676229dc6d0868f4e8e8708.html
315. https://digitalpolicyalert.org/event/21880-closed-consultation-on-miit-notice-on-further-strengthening-the-access-recall-and-online-upgrade-management-of-intelligent-connected-vehicles
316. https://wap.miit.gov.cn/jgsj/zbys/qcgy/art/2024/art_e1bb0d211dbf40a2949b28deb8a96d19.html
317. https://dissec.to/general/chinas-new-vehicle-cybersecurity-standard-gb-44495-2024/
318. https://www.codeofchina.com/standard/GB44496-2024.html
319. https://www.chinesestandard.net/Related.aspx/GB44497-2024
320. https://dissec.to/general/chinas-new-vehicle-cybersecurity-standard-gb-44495-2024/
321. https://www.eet-china.com/mp/a358838.html
322. https://morth.nic.in/sites/default/files/ASI/12_Draft_AIS_189_CSMS_DF.pdf
323. https://morth.nic.in/sites/default/files/ASI/13_Draft_AIS_190_SUMS_DF.pdf
324. https://bwsecurityworld.com/technology/cybersecurity-standards-for-connected-vehicles-to-be-mandatory-by-2027-in-india-report/
325. https://www.services.bis.gov.in/php/BIS_2.0/bisconnect/standard_review/Standard_review/Isdetails?ID=MzA2MDY%3D
326. https://www.services.bis.gov.in/php/BIS_2.0/bisconnect/standard_review/Standard_review/Isdetails?ID=MzA2MDU%3D
327. https://www.theweek.in/news/biz-tech/2024/06/23/what-are-is-18590-2024-is-18606-2024-bis-introduces-two-standards-ev-safety-quality.html
328. https://sso.agc.gov.sg/Acts-Supp/19-2024/Published/20240704?DocDate=20240704
329. https://www.herbertsmithfreehills.com/notes/cybersecurity/2024-06/singapore-expands-the-scope-of-the-cybersecurity-act-?
330. https://www.herbertsmithfreehills.com/notes/cybersecurity/2024-06/singapore-expands-the-scope-of-the-cybersecurity-act-?
331. https://www.strategyand.pwc.com/de/en/industries/automotive/electric-vehicle-sales-review-2024-q3.html
332. https://www.strategyand.pwc.com/de/en/industries/automotive/electric-vehicle-sales-review-2024-q3.html
333. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf
334. https://www.etsi.org/newsroom/press-releases/2457-etsi-releases-new-guidelines-to-enhance-cyber-security-for-consumer-iot-devices
335. https://eur-lex.europa.eu/eli/dir/2022/2555
336. https://data.consilium.europa.eu/doc/document/ST-12041-2023-INIT/en/pdf
337. https://www.consilium.europa.eu/media/69093/st16996-en23.pdf
338. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_5342, https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks
339. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
340. https://www.europarl.europa.eu/news/en/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products
341. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet
342. https://www.charin.global/technology/plug-charge

参考文献

343. https://www.federalregister.gov/documents/2023/02/28/2023-03500/national-electric-vehicle-infrastructure-standards-and-requirements
344. https://www.foley.com/insights/publications/2023/04/us-dot-finalizes-ev-charging-infrastructure-rules/
345. https://www.nccoe.nist.gov/projects/cybersecurity-framework-profile-electric-vehicle-extreme-fast-charging-infrastructure
346. https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8473.ipd.pdf
347. https://www.theverge.com/2024/8/9/24216329/cybersecurity-clean-energy-biden-administration-priorities
348. https://www.gov.uk/government/consultations/electric-vehicle-smart-charging/public-feedback/electric-vehicle-smart-charging-consultation-summary-of-responses
349. https://www.legislation.gov.uk/uksi/2021/1467/made
350. https://www.legislation.gov.uk/uksi/2021/1467/made
351. https://assets.publishing.service.gov.uk/media/628ce214e90e071f653a494a/Guide-to-evscp-regulations-2021-V2.1.pdf
352. https://www.gov.uk/government/publications/the-public-charge-point-regulations-2023-guidance/public-charge-point-regulations-2023-guidance#background
353. https://www.legislation.gov.uk/uksi/2023/1168/contents/made
354. https://www.meti.go.jp/press/2020/11/20201105003/20201105003-1.pdf, https://www.dataguidance.com/news/japan-meti-releases-iot-security-and-safety-framework
355. https://www.dataguidance.com/news/japan-mic-announces-publication-iot-5g-security, https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00036.html
356. https://www.switch-ev.com/blog/what-is-iso-15118
357. https://en.wikipedia.org/wiki/Combined_Charging_System
358. https://www.switch-ev.com/blog/basics-of-plug-and-charge
359. https://www.charin.global/technology/iso15118/
360. https://www.cinch.co.uk/guides/electric-cars/what-is-chademo-ev-charging
361. https://www.chademo.com/design-guideline-for-external-charging-updated
362. https://www.openchargealliance.org/protocols/ocpp-201/
363. https://openchargealliance.org/my-oca/ocpp/
364. https://www.linkedin.com/pulse/how-does-ocpp-201-iso-11518-work-together-why-do-matter-beckmann/
365. https://www.gartner.com/en/documents/3904768
366. https://www.gartner.com/en/documents/3904768
367. https://unece.org/media/press/387828
368. https://owasp.org/API-Security/editions/2023/en/0x11-t10/
369. https://upstream.auto/platform/
370. https://upstream.auto/press-releases/upstream-unveils-ocean-ai/
371. https://upstream.auto/platform/cybersecurity/
372. https://upstream.auto/solutions/sector/electric-vehicle-charging/
373. https://upstream.auto/solutions/sector/sim-enabled-mobility-iot/
374. https://upstream.auto/platform/api-security/
375. https://upstream.auto/autothreat-intelligence/
376. https://upstream.auto/blog/deep-dark-web-intelligence-proactive-automotive-cybersecurity/
377. https://upstream.auto/solutions/vehicle-security-operations-center/
378. https://upstream.auto/solutions/cyber-readiness-services/

UPSTREAMセキュリティについて

Upstreamは、クラウドベースのAIを活用したデータ管理およびサイバーセキュリティプラットフォームを提供します。それはコネクテッドカー、スマートモビリティ、IoTエコシステムに特化して設計されています。 Upstreamプラットフォームは、断片化され分散したモビリティデータを一つにまとめ、分かりやすく整理して保存する仕組みです。それにより、そのデータを最大限に活用できるようにします。 このデータを活用することで、Upstreamはサイバーセキュリティ対策（XDR）や詐欺防止、システムの監視、車両の品質管理の改善、使用状況に基づいた保険設計など、さまざまな分野でAIを活用した便利なアプリケーションを提供しています。

Upstreamは、Alliance Ventures（ルノー、日産、三菱）、ボルボグループ、BMW、ヒュンダイ、MSI保険、ナショナルワイド保険、セールスフォースベンチャーズ、シスコインベストメンツ、CRV、グリロットキャピタルパートナーズ、マニヴモビリティの各企業からの民間資金によって運営されています。

詳しくは

以下をご覧ください

www.upstream.auto

Contact us:

hello@upstream.auto

フォローしてください