2024

Upstream

グローバルモビリティ サイバーセキュリティ報告書

自動車サイバーセキュリティの変換点、
つまりは実験的なハッキングから大規模な自動車攻撃への変換。
今回はその影響に焦点をあてていきます。

目次

目次

CEOからの
オープニングメッセージ

2024年版グローバル自動車サイバーセキュリティレポートをお届けできることを嬉しく思います。

コネクティビティとソフトウェアデファインドアーキテクチャは、過去数年にわたり、自動車とスマートモビリティのエコシステムにおける大きな変化の最前線にありましたが、更なる機能が公開されるにつれて、サイバーセキュリティのリスクは劇的に増大しています。

本レポートは、Upstreamの6回目の年次レポートとなるもので、自動車およびモビリティにおけるサイバーセキュリティリスクが、実験的ハッキングから大規模な攻撃へと進化し、業界の焦点が影響に移った経緯を分析しています。

弊社が昨年予測したように、自動車のサイバーセキュリティは変換点を迎えています。

サイバーインシデントのリスクと影響が大幅に増大しており、安全性を脅かし、運用上の影響をもたらしています。

脅威アクターの関心がモビリティ資産への大規模な影響へとシフトしているため、エコシステム全体の関係者は、サイバーセキュリティインシデントが潜在的に財務にどのような影響を及ぼす可能性があるかも評価する必要があります。

昨年、自動車およびスマート モビリティのエコシステムは新しい基準を採用し、将来の規制をどのように適応させて接続資産やソフトウェア デファインド資産の安全性を維持するかについて、世界中の規制当局と協議しました。

また、2024年7月に発効予定のUNECE WP.29 R155の第2のマイルストーンに向けた準備にも追われており、その適用範囲はすべての新車に拡大されます。

2023年は生成AI革命の年でした。

生成AIは、脅威アクターが規模や新たな攻撃手法を導入するために、ますます利用されるようになっています。

しかし、今後数か月から数年の間に、生成AIは自動車のサイバーセキュリティツールとワークフローを変革し、vSOCチームに前例のない効率化をもたらすでしょう。

この変換点は、ハッカーが依然として進化し続けていることを示すとともに、安全な自動車とスマートモビリティの体験を継続的に提供するという、業界としての弊社の取り組みを再確認するものです。

弊社は2017年にUpstreamプラットフォームを導入して以来、コネクテッドカーの安全確保に向けた取り組みを主導してきました。それにより、自動車サイバーセキュリティ技術を蓄積し、革新的かつ標準的な存在になりえるであることが証明されました。

世界をリードする自動車およびスマートモビビリティの組織、すなわちOEM、サプライヤー、モビリティIoTベンダー、フリートおよびモビリティサービスプロバイダがサイバーセキュリティ規制にを遵守し、何百万台もの車両とモビリティ資産を保護できるよう、引き続き支援していきます。

高度なサイバーセキュリティツールと知識を駆使して、2024年以降の課題に対処する体制を整えています。

ありがとうございました。

Yoav Levy
共同創設者兼CEO

方法論

自動車業界は、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を信頼しています。

Upstreamの研究者は、2010年時点のものも含め、1468件以上のインシデントを調査し、数百のディープウェブやダークウェブのフォーラムを監視していました。その上で、今後1年安全への道案内ができるよう、包括的で実用的なレポートをまとめました。

Upstreamは、世界各地で発生した自動車関連のサイバーインシデントを監視・分析し、スマートモビリティのエコシステム全体を既存・新規の脅威から守るための学習・理解・支援を行っています。

UpstreamのAutoThreat®[1]サイバーThreat Intelligenceプラットフォームでは、高度なテクノロジーと自動化ツールを使用して、自動車のエコシステムにおける新しいサイバーインシデントをネット上のサーフェイス ウェブ、ディープウェブ、ダークウェブから常に検索し、AutoThreat®プラットフォームへのインデックス化が可能です。

弊社の研究者とアナリストは、サイバー脅威、敵対者の動機と活動、およびモビリティ資産への影響をより深く理解するために、収集したデータを慎重に分類・分析しています。

各インシデントと関連するコンテキスト データ (攻撃の地理位置情報、影響、攻撃ベクトル、企業の種類、攻撃者とターゲットまでの必要な距離など) がプラットフォームに追加され、正確で実用的なリポジトリが作成されます。

本レポートで調査したインシデントは、メディア、学術研究、バグバウンティプログラム、世界中の政府法執行機関の検証済みTwitterアカウント、Common Vulnerabilities &Exposures(CVEs)データベース、およびその他の一般に公開されているオンラインソースから入手したものです。

Upstreamのアナリストは、公に報告されたサイバーインシデントに加え、ディープウェブやダークウェブを監視し、自動車を標的としたサイバー攻撃のダークウェブで活動する脅威要因について調査しています。

これらのインシデントは、本レポートの別章「ディープウェブおよびダークウェブにおける自動車およびモビリティの脅威」で取り上げており、特に明記されていない限り他の章の統計や図表からは除外しています。

自動車サイバーインシデントをすべて特定し、分析するよう努めてはいますが、公に報告されていない攻撃もある可能性があるので、本レポートに含まれていないものもあります。

公開されたインシデントの詳細については、AutoThreat® Intelligence Cyber インシデント Repository(オートスレットインテリジェンスサイバーインシデントリポジトリ)でご覧いただけます。

さらに、AutoThreat® PRO[2]をご利用のお客様には、包括的な分析結果を提供しています。

エグゼクティブサマリー

コネクティビティにより自動車とスマートモビリティのエコシステムは変化し続けており、公開される機能が増えるにつれてサイバーセキュリティリスクも高まっています。
2023年は、自動車サイバーセキュリティの新時代の幕開けとなりました。
どのサイバー攻撃も今日においては深刻さを増し、さまざまな関係者に対して世界的に財務上および業務上における影響を及ぼす可能性があります。
Upstreamの2024年版グローバルサイバーセキュリティ報告書（2024 Global Annual Cybersecurity Report）では、サイバーセキュリティリスクが試行的なハッキングから大規模なリスクへとどのように進化してきたかを検証しています。特に安全性と信頼性、業務上の可用性、データプライバシー、財務上における影響に焦点を当てています。

2023年、自動車とモビリティ関連のサイバーセキュリティにおいて、インシデントは大規模なものへと劇的に変化しました

影響が「大きい」または「非常に大きい」インシデントの割合は、2022年から2023年にかけて劇的に倍増し、全インシデントの50%近くを占めました

50%
全インシデントの50%

95%
攻撃の95%は遠隔操作によるものでした

64%
攻撃の64%はブラックハットアクターによるものでした

脅威アクターの動機も規模や影響力が非常に大きいものへと変化しています

65%
ディープウェブおよびダークウェブのサイバー活動の65%は、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。

37%
ディープウェブおよびダークウェブのサイバー活動の37%は、世界規模で多数の利害関係者に影響を与える可能性がありました。

OEMは、コネクテッドカーやソフトウェア・デファインドカー、さらにIoTおよびOT資産を保護するために多面的なアプローチを採用しています

- 頻繁なOTAアップデートにより、SBOMはもはや静的ではなく、車両が工場から出荷された後も常に進化し、リスクプロファイルは絶えず変化します。
- バックエンドシステムへの依存が高まり、OEMはソフトウェアコンポーネントと機密データの両方を緊急に保護する必要があります。
- 生成AIは、自動車のサイバーセキュリティソリューションとオペレーションを変革する可能性を秘めています。生成AIにより、迅速な調査が可能になり、vSOCのワークフローを自動化、またディープウェブやダークウェブデータと詳細なTARAに基づき複雑な洞察を生み出すこともできます。

2024年の予測

01

自動車業界における競争優位性は、今後もDXによって推進されます。そのため利害関係者はAPIを保護し、vSOCの検知範囲を拡大してAPI関連の脅威を監視する必要があります。

02

生成AIは、自動車サイバーセキュリティの利害関係者に多大な影響をもたらします。生成AIが大規模なサイバー攻撃の新たな手法に利用されることもありますが、防御側関係者も生成AIを活用し高度な検知機能、調査機能、緩和機能を利用できます。

03

UNECE WP.29 R155規制が整備され、中国を中心に世界中でも新たな規制が次々と生まれる中、規制疲れの初期兆候が見られます。

04

OEMとチャージポイントオペレーター（CPO）は、サイバーセキュリティのリスク評価を強化し続け、戦略的なEV充電インフラを保護するためのサイバーセキュリティソリューションを展開します。

01.

自動車サイバーセキュリティの変換点

実験的ハッキングから大規模な
自動車攻撃へと変化し、
焦点はその影響へと移行

2023年 自動車サイバーセキュリティの新時代が始まる

コネクティビティはここ数年、自動車とスマートモビリティのエコシステムにおける画期的な変化の最前線にありました。これにより、OTA（Over-the-Air）アップデート、ソフトウェア指向アーキテクチャ、高度なデジタル体験、多岐にわたる付加価値のあるアプリケーションとサービスが可能になりました。

最新のソフトウェア定義車両(SDV)では、コネクティビティを活用して、車両のライフサイクルを通じた改善、アップグレードを行い、幅広い機能オンデマンドサービスから収益を生み出し、革新的なデータに基づいた顧客体験を提供することで、最終的には顧客とのより深く、より長い関係を構築しています。

コネクテッドカーでは、OEMはOTAアップデートを利用して、品質と使いやすさの問題を修正し、中心となる機能、サイバーセキュリティの脆弱性を迅速でコスト効率よく修正することで、保証コストやリコールを軽減しています。

しかし、コネクティビティは、OEMとそのサプライチェーンにとってますます増加するサイバーセキュリティの課題をもたらしており、サイバー攻撃はさらに巧妙で頻繁かつ深刻になっています。
ここ数年の間に攻撃の状況が変化し、新しい攻撃手法が現れるにつれて、業界はあらゆる接続点が攻撃される可能性があることを、痛感するようになりました。

自動車サイバーセキュリティの最初の10年は、OEMやエコシステムへのサイバーインシデントや攻撃が増加した時期でした。OEMが、サイバーセキュリティ保護の向上に投資していたにもかかわらず、絶えず新しい攻撃ベクトルや手法が導入されてきました。**Upstreamの調査によれば、2019年から2023年までの期間に、クリアウェブ（メディア）で公開されたインシデントは50%以上増加し、2023年には295件に達しました。** 2023年だけを見ても、攻撃の95%は遠隔操作によるものであり、攻撃の64%はブラックハットアクターによって実行されています。[3]

アプリケーションプログラミングインターフェース（APIs）は、車両の機能をドライバーや企業アプリケーションに公開し、データに基づく体験を提供する上で重要な役割を果たしています。

> ***今年のレポートでは、自動車とモビリティのサイバーセキュリティリスクの影響に焦点を絞っています。***

エコシステムから見た外部への影響と、組織の効率やプロセスに関わる内部への影響の双方に焦点を当てています。

内部と外部の両方の影響は、関係者によってさまざまな方法で評価されます。本レポートでは、各関係者の戦略目標、ターゲット市場、関連するモビリティ資産などに合わせたカスタマイズができるフレームワークを提供します。

外部への影響は、2つの側面から客観的に評価することができます。すなわち、「規模とコスト」です。

高度なコネクティビティとソフトウェアデファインドアーキテクチャが、どのように新たなサイバーセキュリティリスクを継続的にもたらしているかを紹介します。これは、ドライバーや同乗者の安全性、大規模なデータの整合性に潜在的な影響を与え、驚異的な財務的損失につながることから、エコシステム全体にわたって経営陣の注目を集めています。

ソーシャルメディアが消費者や専門家にとって主要なプラットフォームとなる中で、脅威アクターは、ソーシャルメディアを利用して知識を共有し、数分で世界中の何百万人もの人々に情報を伝えることができます。 ソーシャルメディアは、ウイルスの拡散性から見ても、犯罪や詐欺を含む悪質な活動の主要な伝播経路の1つとなっており、外部への影響や規模を分析する際には考慮する必要があります。

車両は製造工場から出荷された後も、継続的な無線アップデート（OTA）に基づいて進化し続けています。サイバーセキュリティのリスクが、社内プロセスやリスク評価に与える内部への影響についても議論し、自動車関係者が新しいフレームワークや対策プロセスを採用するよう促します。

自動車サイバーリスクの潜在的な規模の分析

自動車のサイバーセキュリティの脅威は、非常に短い期間で急速に進化しています。2015年、チャーリー・ミラーは、1台の車の安全上重要な車載ネットワークをハッキングするために、研究から悪用まで3年間を費やしました。[4] 2023年には、セキュリティ研究者チームが、わずか数カ月で十数社以上の自動車メーカーのハッキングを行いました。チームは、テレマティック システム、自動車 API、およびそれらをサポートするインフラをハッキングしました。彼らは多数の脆弱性を発見し、遠隔操作で自動車のコマンド&コントロール(C&C)に影響を与え、OEMや消費者の機密データにアクセスすることを可能にしました。[5]

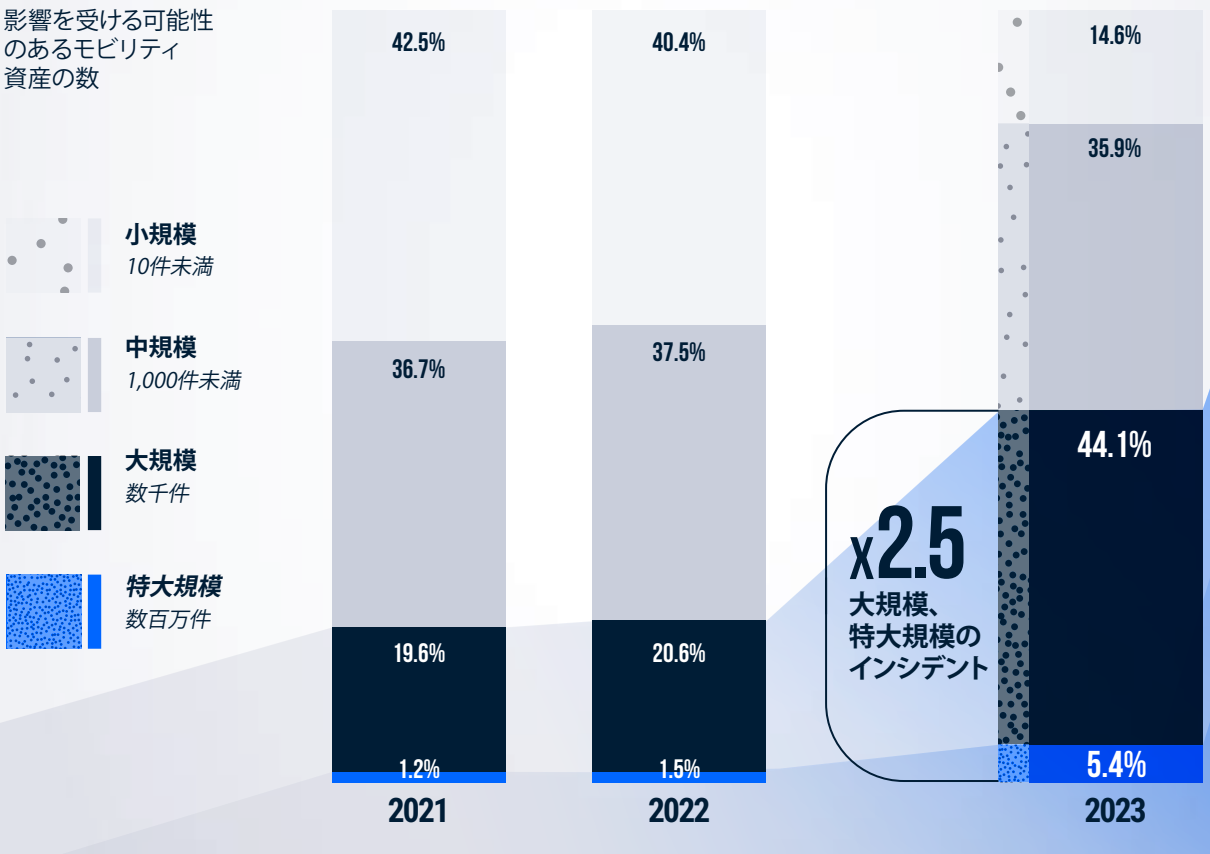
> ***2023年、自動車のサイバーセキュリティは大規模インシデントへと劇的に変化しました。***

規模を分析する際には、潜在的な影響に焦点を当てることが重要です。公に報告された情報だけでは、各インシデントの正確な影響を判断し評価することは不可能です。

Upstreamは、車両、ユーザー、モビリティ・デバイスなど、影響を受けたモビリティ資産の潜在的な規模に応じて、2021年から2023年の間に公表された、自動車関連のサイバーセキュリティ・インシデントを分析しました。Upstreamの分析では、インシデントを影響の程度に応じて4つに分類しました。10件未満の資産に影響を与える可能性のある「小規模」から、数百万件のモビリティ資産に影響を与える可能性のある「特大規模」までです。

2023年には、大規模、特大規模のインシデントの割合が 50% 近くに大幅に倍増しました。

公表されたサイバーセキュリティインシデントの潜在的規模別内訳（2021～2023年）



出典：Upstream Security

2021年と2022年においては、大規模、特大規模（数千件から数百万件のモビリティ資産に影響を与える可能性のある）のインシデントは、全体の約20%でした。しかし2023年には、大規模、特大規模の影響を及ぼすインシデントは、50%近くまで劇的に倍増しています。

全体として、最大1,000台の車両やモビリティ資産に影響を与える可能性のある中規模の攻撃件数は、過去3年間横ばい状態です。

しかし、ハッカーが知識やリソースがなくても、さらに多くの車両や資産をコントロールできる新たな攻撃ベクトルが出てきたことにより、2023年には小規模の攻撃件数は著しく減少しました。

サイバー攻撃がモビリティ・サービス・プロバイダーに与える業務妨害の影響を説明するために、2023年9月に発生した攻撃を考えてみましょう。

米国を拠点とする大手トラック輸送・車両管理ソリューション・プロバイダーは、ランサムウェア攻撃を受け、その結果、連邦規則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。[6]

これを受けて、同社は外部のサイバーセキュリティ専門家を雇って攻撃を調査し、米国連邦自動車運輸安全局に免除を申請して、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。[7]

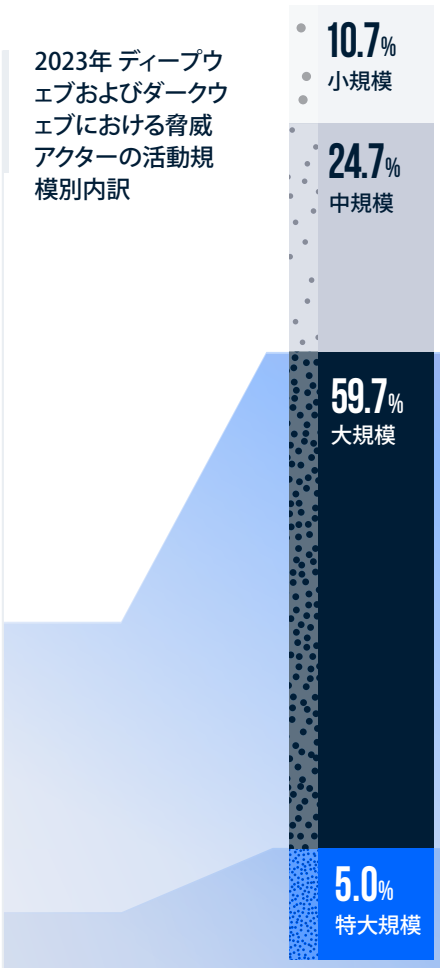
> ***同社が問題を解決するまでに、ほぼ3週間を要し、トラックドライバー、車両オペレーター、在庫管理チームなど数千人に深刻な業務上の混乱が生じました。***

脅威アクターの動機もまた、規模や影響が拡大傾向にあります

メディア（クリアウェブ）に公開されたインシデントに加えて、ディープサイバーやダークサイバー活動の影響と、脅威アクターを駆り立てる動機を評価することが重要です。Upstreamのディープウェブおよびダークウェブにおける自動車サイバーセキュリティ活動の分析によれば、最も活発な300の脅威アクターを分析した結果、活動のほぼ半分（48%）が複数のOEMや自動車サプライヤーを標的にしており、37%が世界規模で多くの関係者のモビリティ資産に影響を与える可能性がありました。

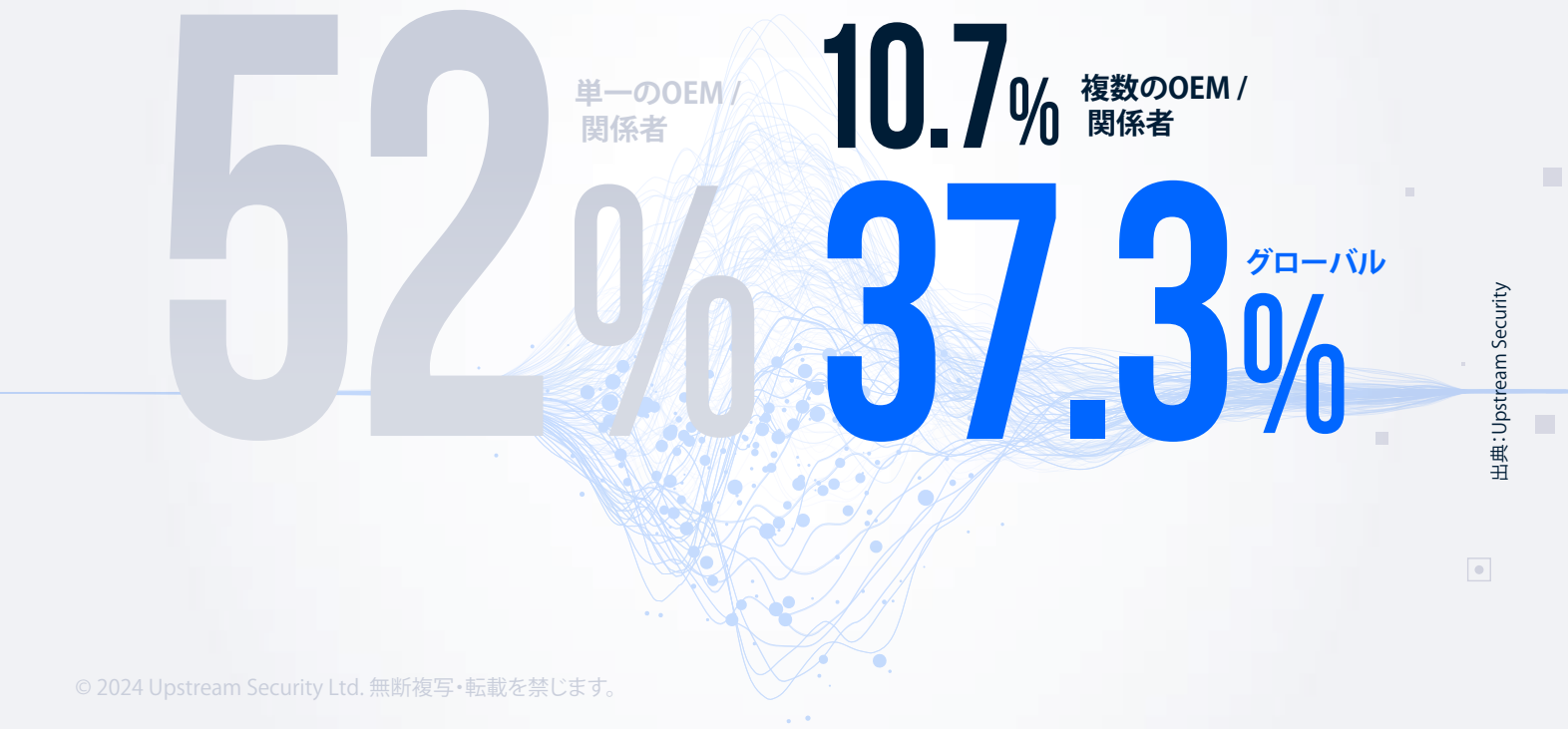
2023年には、ディープウェブとダークウェブのサイバー活動の65%近くが、数千から数百万のモビリティ資産に影響を及ぼす可能性がありました。

2023年 ディープウェブおよびダークウェブにおける脅威アクターの活動規模別内訳



出典：Upstream Security

2023年 ディープウェブおよびダークウェブにおける脅威アクターの活動規模別内訳



出典：Upstream Security

ディープウェブやダークウェブにおける**ブラックハットや不正行為**に焦点を当てると、潜在的な規模や関心領域でも、リスクが急速に高まっていることが分かります。
現在、悪意のある活動（ブラックハットや不正行為者に分類される脅威アクター）の67%が、大規模、特大規模の影響を及ぼしており（脅威アクター全体では45%）、58%の活動が複数のOEMを巻き込み、影響は世界的な広がりを見せています（脅威アクター全体では48%）。

関心領域を分析すると、ブラックハットや不正行為者の影響はますます深刻化していることが分かります。

活動の 13% は車両操作ツールに焦点を当てており、活動の 12% は機密データおよび PII へのアクセスに焦点を当てています。そしてほぼ50% は脆弱性の悪用に関連しています。[8]

2023年 ブラックハットおよび不正行為者の活動（潜在的規模別）

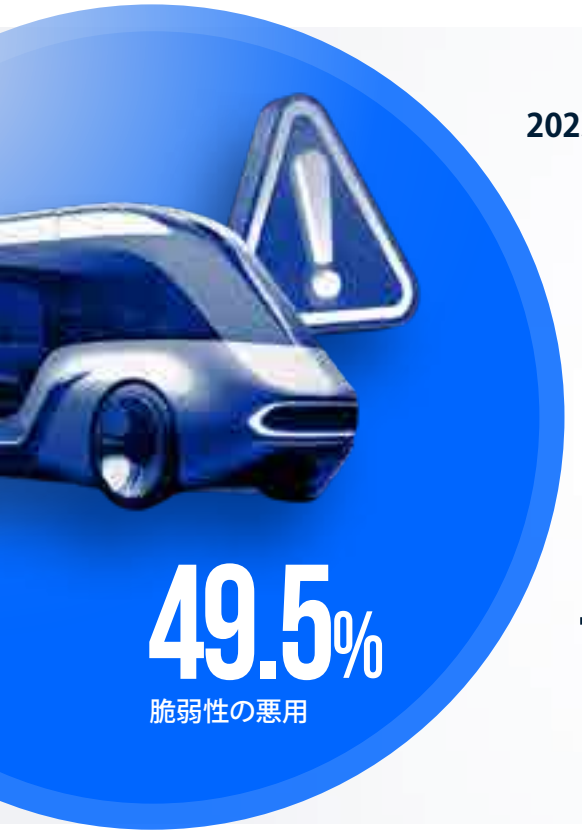
2023年 ブラックハットおよび不正行為者の活動標的

41.5% 単一のOEM / 関係者

10.4% 複数のOEM / 関係者

48.1% グローバル

出典：Upstream Security



2023年 ブラックハットおよび不正行為者の関心領域

49.5%
脆弱性の悪用

19.3%
診断ソフトウェア

12.6%
車両操作ツール

11.9%
PII
（個人情報）

6.7%
自動車
ハッキング
マニュアル

出典：Upstream Security

財務的観点

自動車およびスマートモビリティエコシステムに対するサイバー攻撃のコストの上昇

自動車やスマートモビリティへのサイバー攻撃は、リコールやOTA、生産停止、ランサムウェアの支払い、車両の盗難など、深刻な財務上の影響を及ぼします。さらに、データやプライバシーの侵害は、ブランドの評判や顧客の信頼を損ない、最終的には多額の罰金や収益の減少につながる可能性があります。

2023年におけるセキュリティインシデントの約50%が数千万のモビリティ資産に影響を与える大規模なものになる傾向があるため、車両セキュリティオペレーションセンター（vSOC）のチームは、これらのインシデントの財政的な影響を分析することは極めて重要です。[9]

2023年6月、台湾を拠点とする大手半導体メーカーは、ランサムウェアグループとそのITハードウェアサプライヤーの1社が関与するサイバーセキュリティインシデントを公開し、システムの初期設定や構成に関する情報が漏洩しました。[10]
攻撃者は機密情報を含む内部文書にアクセスしたと主張し、データの解読とオンライン公開を阻止するために7,000万ドルの身代金を要求しました。これは過去に例を見ない史上最大の身代金要求となりました。
この情報漏洩は複数の自動車関係者に影響を及ぼす可能性がありましたが、同社は、サプライヤーでのサイバーインシデントが事業運営や顧客情報には影響を与えなかったと報告しています。
同社はまた、事件発生後、このサプライヤーとのデータ交換を直ちに中止しました。

2023年11月、12のディーラーと数百人の従業員を擁するオーストラリアの大手自動車グループが同じランサムウェアグループの攻撃を受け、50GBを超える顧客や社内の機密データが盗まれました。
約91,000件以上の盗まれたファイルには、給与情報、リース契約書、支払情報、サービス見積書、請求書、クラッシュアシスタンスフォーム、CRMデータ、登録書類、従業員の運転免許証や自動車販売免許証が含まれていました。
盗まれたファイルは、身代金の期限が切れた11月末に公開されました。[11]

2023 年 6 月、あるTIER-2 が史上最大となる

7,000

万ドルの

身代金を要求されました。

サイバーセキュリティインシデントの財務的影響の分析

自動車のサイバーセキュリティインシデントの安全性、プライバシー、財務上のリスクを数値化しようとすることは、並大抵のことではありません。
自動車のサイバー脅威の潜在的な影響は重大であり、ドライバーと乗客の安全にリスクをもたらし、事業運営を混乱させ、データプライバシーを侵害し、OEMだけでなくサプライチェーン全体に経済的損失をもたらす可能性があります。

次の2つの図では、2023年に発生した2つのインシデントを分析し、公表されている情報に基づいて、財務上の影響モデルを提案します。

> ***このフレームワークの目的は、サイバーセキュリティリスクによる甚大な財務への影響を浮き彫りにすることです。***

この分析は決定的なものではなく、潜在的な財務リスクの範囲を推定するためのフレームワークです。

自動車のサイバー脅威が財務に与える主な影響

影響	内容	手法
車両の安全性、運用およびリコール	車両の通常の動作を変更し、ドライバーの安全を脅かし、リコールにつながる可能性のある遠隔操作または現地操作。 車両のソフトウェア コンポーネントにサイバーセキュリティの脆弱性がある場合、メーカーは問題を更新して解決し、影響を受ける車両の安全性と適切な動作を確保するためにリコールを発行する必要がある場合があります。	APIの悪用、リモートからのコマンド実行、悪意のあるソフトウェアアップデート、サイバーセキュリティの脆弱性
データとプライバシー侵害	顧客の PII、車両性能データ、知的財産 (IP) データなどの情報の開示により、個人や組織が危険にさらされます。	データ漏洩、 ランサムウェア、 インジェクション攻撃
車両盗難と侵入	車両のセキュリティシステムやリモートサービスの脆弱性を悪用した、車両の不正侵入や盗難。	キーレスエントリー／スタートエンジン攻撃、 リレーアタック、 信号妨害攻撃、 API攻撃
サービスおよび事業の中断	サイバーインシデントの結果、組織の運営や商品、サービスを提供する能力への影響。 この影響は、部分的なシステム停止から完全なシャットダウンにまで多岐にわたり発生し、生産性、収益、顧客の信頼の損失につながる可能性があります。	生産システムへのランサムウェアによる生産ラインの停止
法規制遵守の問題	法律、規制、または業界標準の違反につながるサイバー脅威。	訴訟、罰金
不正	個人情報の盗難、走行距離計の改ざん、アカウントのハッキングなど、個人的または金銭的な利益を目的とした悪意を持って実行される、個人または団体による不正行為。	走行距離計の改ざん、モバイルアプリ（ユーザー）の個人情報盗難
ブランド価値の低下	公的に報告されたサイバーインシデントによる財務評価 (時価総額)、信頼、認識への悪影響により、評判が損なわれます。	否定的な報道の広がりによる消費者と投資家の信頼の損失

図 1

EVフリート全体の脆弱性による財務への影響

2023年3月、ハッキングコンテストに参加したフランスのセキュリティ研究者チームは、EV OEMのゲートウェイエネルギー管理システムに対して、TOCTTOU（time-of-check-to-time-of-use）攻撃と呼ばれるエクスプロイトを実行し、車の走行中にリモートでアクション（フロント・トランクやドアを開けるなど）を実行できることを実証しました。[12]

OEMがこのようなことは不可能だと主張していたにもかかわらず、研究者たちは、遠隔操作で車両の制御装置にアクセスできたと主張しました。研究者たちはOEMからEVと現金10万ドルの報酬を受け取り、OEMはこの脆弱性に対するソフトウェアパッチの作成に取り組み、アップデートは間もなく自動車に適用されるだろうと報告しました。

インシデントの重大度
高い

インシデントの影響
潜在的なフリート全体への影響

脅威アクタータイプ
ホワイトハット

フリートサイズ
300万台以上の電気自動車

影響	内容	基準値	財務への影響
車両の安全性、運用およびリコール	オーロララボの車両タイプごとの OTA アップデートコスト。[13] OTAコスト算出に使用した見積もり：大型ECU5個@500MB、小型ECU10個@0.42MB。	ラインオブコード(LOC)アップデートに0.39ドル	125万ドル - 200万ドル
車両の安全性、運用およびリコール	バッテリーに永久的な損傷を受けた車両のバッテリー交換費用。[14]	0.01%～0.05%の車両に影響；1台あたり15,000ドル	525万ドル - 2,625万ドル
法規制遵守の問題	一時的なバッテリー損傷を受けた車両に関する集団訴訟の訴訟費用と和解費用。[15]	フリートへの影響額の0.5%～1%、原告1人当たり600ドル、弁護士費用50万ドル	1,100万ドル - 2,150万ドル
潜在的な財務上の影響の合計			1,750万ドル - 4,975万ドル

図 2

EV充電ネットワークのデータ流出による財務への影響

2023年6月、セキュリティ研究者が、数十万ものEV充電ステーションをつなぐ世界中のネットワークのログ数百万件（ほぼ1テラバイト）を含むオンラインデータベースを発見しました。[14]

人気のあるパブリッククラウドプラットフォームの1つにホスティングされたこの内部データベースは、アクセスにパスワードが必要なく、EV充電ネットワークを使用する顧客の機密データが含まれていました。データには、フリート顧客の名前、電子メールアドレス、電話番号、ネットワークを充電する車両を持つフリートオペレーターの名前、車両識別番号（VIN）、EVの公共および民間（住宅など）の充電ポイントの場所が含まれました。

インシデントの重大度
高い

侵害サイズ
数百万の記録を持つ1TBのデータ

脅威アクタータイプ
ブラックハット

充電ネットワークの規模の試算
30カ国以上に数十万の充電ステーションを設置

侵害の種類
意図しない開示

影響	内容	基準値	財務への影響
データとプライバシー侵害	IBMは、サイバーベースのデータ侵害のコスト見積りに関する詳細なフレームワークと、失われた記録数別の大規模な侵害（100万件以上の漏洩）の平均コストのベンチマークを提供しています。[17] このコスト分析には、データ侵害の検出、エスカレーション、通知、侵害後の対応、および事業の損失に関連する直接的および間接的なコストが含まれています。	100万～1,000万件の記録を含むデータ侵害の平均損失額は3,600万ドル	3,000万ドル - 4,000万ドル
法規制遵守の問題	GDPR 施行追跡レポートでは、運輸及びエネルギー部門の平均罰金と、情報セキュリティ確保のための技術的、組織的対策が不十分であったと報告しています。[18]	運輸部門の平均罰金（86万4,776ユーロ）と不十分な措置（134万6,050ユーロ）に基づく予想範囲	100万ドル - 200万ドル
		潜在的な財務上の影響の合計	3,100万ドル - 4,200万ドル

OEMは、コネクテッドカーやソフトウェア定義車両、およびIOT/OT資産を保護するために、多角的なアプローチを取っています。

影響力の大きいサイバーリスクの時代において、OEMは新たな社内フレームワークを採用し、コネクテッドカーやソフトウェア定義型自動車を保護するための多角的なアプローチに移行する必要がありました。
コネクテッドカーのデジタル体験とデータ駆動機能は、コネクテッドコンポーネント、遠隔操作、およびそれらをサポートするAPIによって可能になります。
継続的なOTAによって、OEMは新しい機能を展開し、バグを修正することができます。

その結果、ダイナミックなソフトウェア部品表（SBOM）が登場しました。SBOMは絶えず変化しているため、リスクと脆弱性の分析が常に必要となります。そして、OEMとサプライ チェーンのサイバーセキュリティ フレームワークとプロセスに直接影響を与えます。

内部への影響：ダイナミックSBOM

ACES（自律走行、コネクティビティ、電動化、共有モビリティ）と呼ばれる技術の収束により、関係者は従来のハードウェア定義のアーキテクチャからソフトウェア指向のアーキテクチャに移行せざるを得なくなりました。

自動車とスマートモビリティのエコシステムは、コネクテッドカーとソフトウェア定義型自動車が、競争力、顧客体験、運用効率、将来のデータを元にした収益源の鍵であることを認めています。

世界経済フォーラムがボストンコンサルティンググループ（BCG）と共同で発表した新しい調査によれば、SDVの登場により、2030年までに自動車産業に6500億ドル以上の価値が生まれ、自動車市場全体の15%から20%を占めると推定されています。SDVの成長に関するBCGの分析によると、自動車用ソフトウェアとエレクトロニクスによるOEMの収益は、現在から2030年の間に870億ドルから2480億ドルへと約3倍に増加すると予想されています。[19]

コネクティビティとSDVは大きな利点をもたらす一方で、OEMとサプライチェーン全体にとってサイバーセキュリティの課題も増大しています。

ますます多くの車載コンポーネントがソフトウェア指向のアーキテクチャによって有効化され管理されるようになり、ハードウェアとソフトウェアの製品開発の区別が曖昧になってきています。

SDVの成長に関するBCGの分析によると、自動車用ソフトウェアとエレクトロニクスによるOEMの収益は、現在から2030年の間に870億ドルから2,480億ドルへと約3倍に増加すると予想されています。

ハードウェア部品表（HBOM）は、ECU、TCU、インフォテインメントシステム、メータークラスター、CANバス、IoTコントローラーなど、車両を構築するために使用されるハードウェアコンポーネントの詳細を記した製品開発技術文書です。

SBOM は、ハードウェア コンポーネントおよび車両にインストールされるソフトウェアコンポーネント、ライブラリ、および依存関係を詳述する動的なソフトウェア開発技術文書です。HBOMとSBOMを組み合わせることで、サプライチェーンの包括的な視点を提供し、ハードウェアとソフトウェアの脆弱性に対処するための透明性とトレーサビリティを促進します。

OTAの頻繁なアップデートにより、SBOM は静的なものではなくなり、車両が工場から出荷された後もずっと進化し続け、リスクプロファイルは継続的に変化します。リアルタイムで修正することもできます。

さらに、最新のSDVのHBOMとSBOMには、車載コンポーネントのみならず、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、テレマティクス機器、電気自動車（EV）充電用のサードパーティアプリケーションも含まれており、より複雑さを増しています。

UNECE WP.29 R155およびR156、ISO/ SAE 21434、米国高速道路交通局（NHTSA）ガイドライン、中国の最近の規制など、近年の規制の取り組みにより、自動車業界でのSBOMの導入が義務付けられています。[20-24] これらの規制により、SBOM の範囲が拡大され、OEM が開発したソフトウェアだけでなく、Tier-1 および Tier-2 のコンポーネントとライブラリも含まれるようになり、OEM はソフトウェア関連の脆弱性とリスクを特定して管理できるようになります。

ソフトウェア・コンポーネントを操作して脆弱性を悪用する機能は、フリート全体の制御システムのサイバーセキュリティ体制に重大な脅威をもたらします。 SBOMに関連する脆弱性を悪用すると、ハッカーは車両全体の重要な機能や制御メカニズムに不正にアクセスできるようになります。

さらに、ソフトウェアコンポーネントによって生成され、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・サーバーなど）は、コネクテッドカー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、管理するうえで重要な役割を果たしています。

ハッカーは、実際の車両自体をハッキングすることなく、何百万もの自動車ユーザーの個人情報が含まれるこのデータを利用することができます。 バックエンドサーバーへのサイバー攻撃の脅威は、悪意のある脅威者がコントロールとデータアクセスの両面からフリート全体に影響を与えることができるため、特に高くなります。

> ***このようなバックエンドシステムへの依存度が高まっていることから、OEMにとっては、バックエンドシステムに保存されているソフトウェアコンポーネントと機密データの両方を保護することが急務であることが明らかになっています。***

このようなバックエンドシステムへの依存度が高まっていることから、OEMにとっては、バックエンドシステムに保存されているソフトウェアコンポーネントと機密データの両方を保護することが急務であることが明らかになっています。 組織上の広範な危機管理の一環であるTARAは、綿密かつ静的なプロセスとして開発された特定のフレームワークです。しかし、TARA は動的なフレームワークへと急速に進化しています。 この考え方の変化の影響は大きく、関係者は新しいツールやプラットフォームを採用し、チームが適切にトレーニングされていることを確認する必要があります。

ディープウェブ分析とダークウェブ分析を TARA フレームワークに追加する必要があるため、内部への影響は拡大します。 ディープウェブとダークウェブのモニタリングとリアルタイムの脅威インテリジェンスをSBOMのフレームワークに統合することで、OEMは次のことが可能になります：

- ソフトウェアおよびハードウェアコンポーネントの脆弱性を積極的に特定し、対処します。
- サプライチェーンのリスクを継続的に評価および管理し、車両に使用されるコンポーネントの完全性と安全性を確保します。
- サイバーセキュリティのリスクと攻撃を迅速に検知し、効果的な対応と軽減策を提供します。

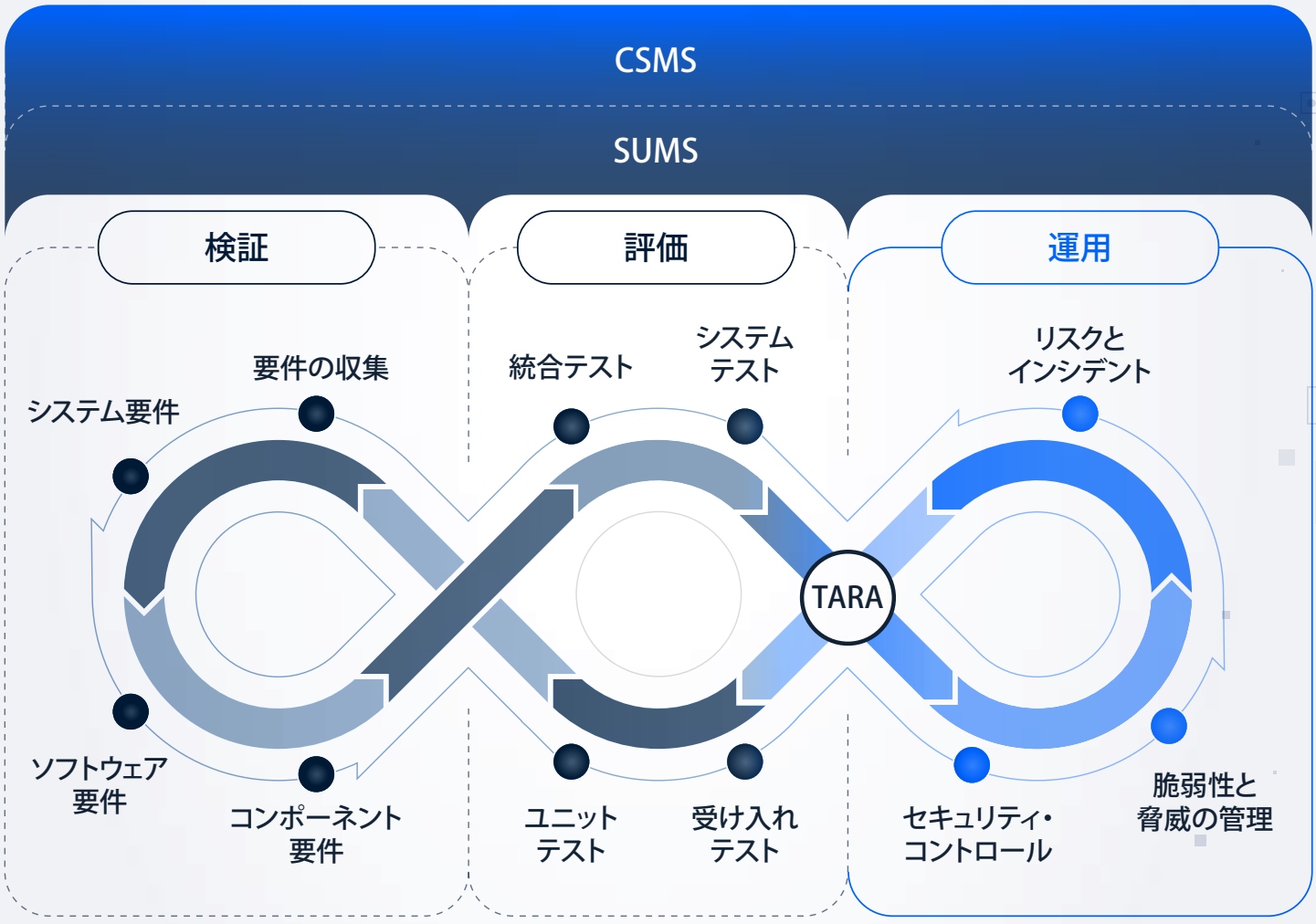
自動車の脅威インテリジェンスは現在、製品主導型 TARA の重要な要素となっており、プロアクティブなリスクの特定、優先順位付け、軽減を可能にします。

拡張された SBOM フレームワークに基づくリアルタイムの脅威インテリジェンスを備えた動的な TARA フレームワークは、OEM ソフトウェア開発チームが長期的なリスク軽減を可能にするために不可欠です。

さらに、vSOC は効果的な TARA に重要なレイヤーを追加し、実際に検出されたリスクを継続的な TARA フィードバックループに統合します。 これには、TARA、脅威インテリジェンス、およびvSOCアナリストのための対話型フレームワークを採用する必要があります。これにより、TARAが動的かつ効果的に実施されることが確認されます。

OEMはまた、多様なTARA分析に基づくSBOMの脆弱性を、企業のセキュリティ、構成、自動化、および対応（SOAR）プラットフォームと連携させ、組織横断的な可視化、タイムリーな修復、および集中的な研究開発努力による長期的なリスク軽減を確保する必要があります。

継続的なサイバーセキュリティのオーケストレーション：
ソフトウェア定義車両には、E2Eのソフトウェア、プロセス、ツールが必要



出典：Upstream Security

外部APIは大規模な攻撃における主要な攻撃ベクトルとなる

APIは自動車のデジタル変革を支えるエンジンであり、コネクテッドカーの安全性を確保する上で極めて重要な役割を果たしています。

コネクテッドカー体験をサポートし、データに基づいた機能を有効化するアプリが追加されると、サイバーセキュリティリスクも高まります。

コネクテッドカーやスマートモビリティサービスは多様なAPIに依存しており、その結果、毎月何十億もの取引が発生しています。 OEM モバイルアプリ、サードパーティアプリ、インフォテインメントシステム、社内システムOEM およびTier-1 管理システム、ディーラーシステム、アフターマーケットモビリティIoT デバイス、EV充電管理および課金アプリに至るまで、あらゆるものがコア機能を実現するためにAPIに大きく依存しています。

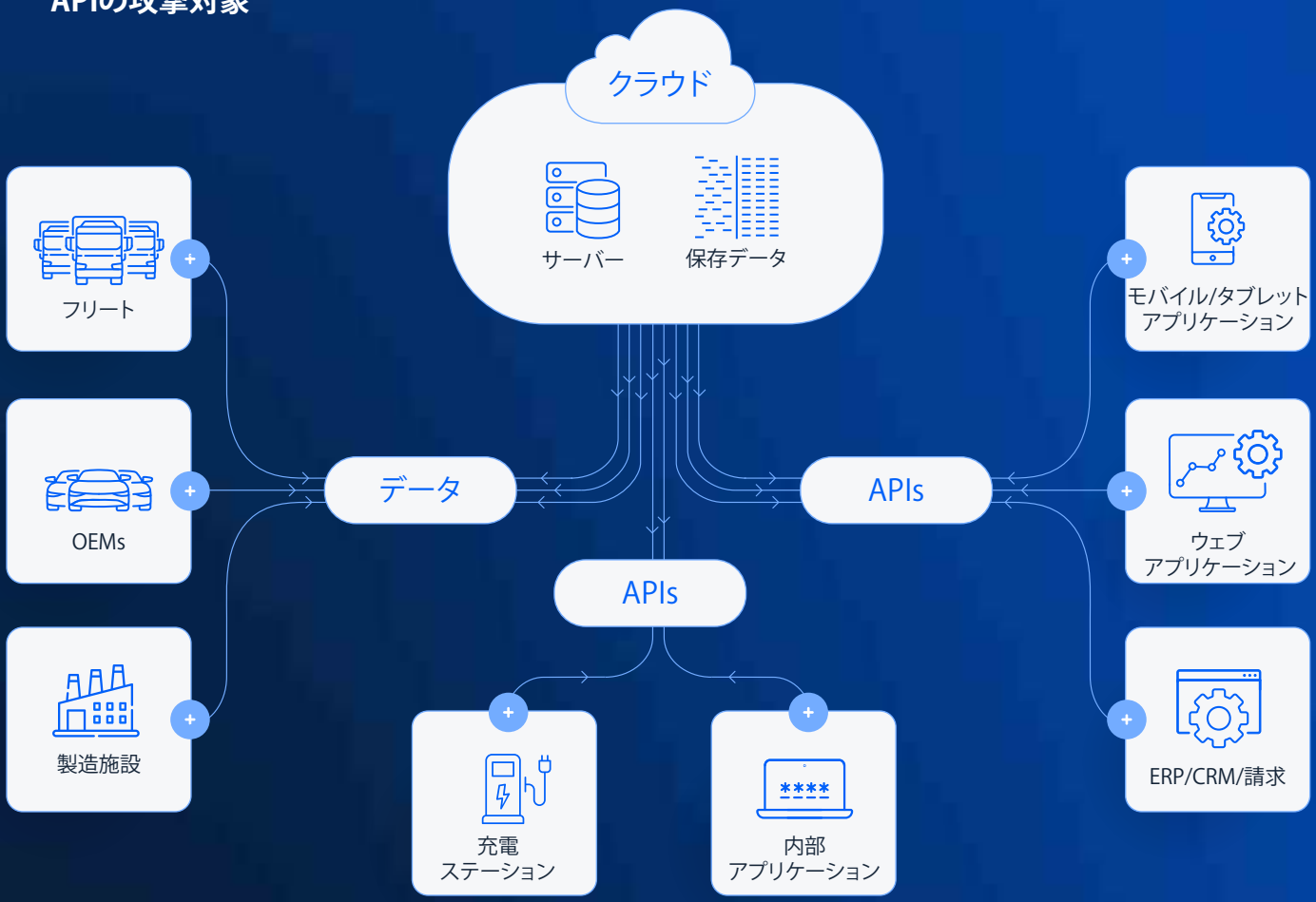
APIはまた、重要かつフリート全体の攻撃ベクトルとなり、機密情報や個人情報（PII）の盗難、悪意のある車両遠隔操作など、広範なサイバー攻撃の影響を受けやすくなります。

2023年3月、あるセキュリティ研究者が日本のOEMのCRMデータベースにアクセスしたことを明らかにしました。ハッカーは実際の運用で使用されるAPI を使用するように開発アプリを変更しましたが、この API は読み込みスピナー設定を通じて意図せず公開されました。この事件は、APIが誤って設定され、適切な認証と検証が行われなかったことが直接の原因でした。その結果、研究者は、OEM 顧客の名前、住所、電話番号、電子メール アドレス、納税者番号、車両/サービス/所有権履歴にアクセスすることができました。[25]

スマートモビリティのベンダーやフリート運営者、モビリティIoTデバイスもまた、APIを利用したサイバーリスクにさらされており、大規模な運用の混乱や機密データの漏洩につながる可能性があります。

2023年6月、パキスタンで1,000万人以上のユーザーを持つ人気のライドシェアリングサービスが、サードパーティーの通信APIが侵害され、攻撃を受けました。これにより、顧客に悪質なメッセージや通知が届きました。[26]

APIの攻撃対象



出典: Upstream Security

ソーシャルメディアは自動車サイバー活動の温床になっている

ソーシャルメディアがサイバーセキュリティに及ぼす影響は、計り知れないほど大きいものがあります。ソーシャルメディアは、その絶大な影響力によってサイバー活動の温床となっており、ポップカルチャーと悪意の境界線が曖昧になっています。かつてはディープウェブ、ダークウェブの奥深くに隠されていたものが、今では簡単に露呈し、幅広い層がアクセスできるようになっています。

自動車愛好家やハッカーが、今や自分たちの自動車ハッキングの発見を世界中の人々と簡単に共有できるようになったのも、ソーシャルメディアのおかげです。

近年、Facebook、TikTok、YouTube、Instagramは、自動車のハッキングツールやマニュアル、脱獄、ハッキングデモを共有するための人気のあるプラットフォームとなり、車両をハッキングする方法に関する論議が、ディープウェブやダークウェブの深部からオープンなインターネットへと移行しています。

自動車ハッキングが発見されたものの中には、サイバーセキュリティの専門家やホワイトハットハッカーが、人々の意識を高め、リスクへの対処を促すことを目的として作成したシステムが、共有されているものもあります。
他の自動車ハッキングの手口は、悪意をもって作成されソーシャルメディアで共有されています。

当初の意図に関係なく、ソーシャルメディアで共有された情報は、ツールや脱獄への容易なアクセスを提供し、新たな脅威アクターを助長する可能性があります。
ソーシャルメディアのウイルス的な性質により、悪用の速さと広がりが増幅され、風評被害、経済的損失、業務妨害につながる可能性があります。そのため、OEMメーカーは常に警戒を怠らず、この新しいサイバー脅威によってもたらされるリスクを軽減するために、強力なサイバーセキュリティ戦略を採用することが極めて重要です。

その典型的な例は、2022年10月に流行したいわゆる「TikTokチャレンジ」で、韓国のあるOEMが製造した数万台の車両が全国的に盗難される事態に発展しました。

その1年前、ウィスコンシン州ミルウォーキーで、ある韓国OEMの自動車盗難が急増しました。その容疑者の多くが運転する年齢には達していない若者たちでした。ソーシャルメディア上で、若者たちがこれらの車に乗り、スピード違反や急ハンドルをしたり、時には窓からぶら下がったりして楽しんでいる様子を映した動画が公開されました。窃盗犯の目的は、車からパーツをはがして売ることではなく、ソーシャルメディアで注目を浴び、閲覧数を稼ぐことでした。[27]盗難の手口を紹介する動画が広まると、翌年には韓国製OEM車の盗難が全国で急増しました。[28]

2023年1月、アメリカの2大自動車保険会社が、被害を受けた車両は盗まれやすいという理由で、特定の都市での保険契約を拒否したと報じられました。[29]

2023年2月のプレスリリースで、NHTSA（米運輸省高速道路交通安全局）はTikTokを直接非難し、「TikTokのソーシャルメディアチャレンジが全国に広がり、少なくとも14件の事故報告と8件の死者を出している」と述べました。[30]　また、韓国のOEMは830万台以上の米国の車両を対象に、リスク低減のためディーラーでの設置が必要な盗難防止ソフトウェアのアップデートを無料で提供していることを消費者に通知しました。[31]

2023年5月、韓国OEMは1件の集団訴訟に対する和解金として最大2億ドルを支払うことに合意しました。しかし、対象車両の盗難が増加し続けているため、依然として保険会社や市からの訴訟に直面しており、今後も訴訟が予想されています。

脱獄インフォテインメントシステムもまた、ソーシャルメディアのトレンドになっています。2023年9月、複数のOEMのEV のさまざまなインフォテインメントシステムに影響を与える不正なファームウェアアップデートとカスタムソフトウェアが、著名な自動車脅威アクターによって Facebook上で販売されていました。

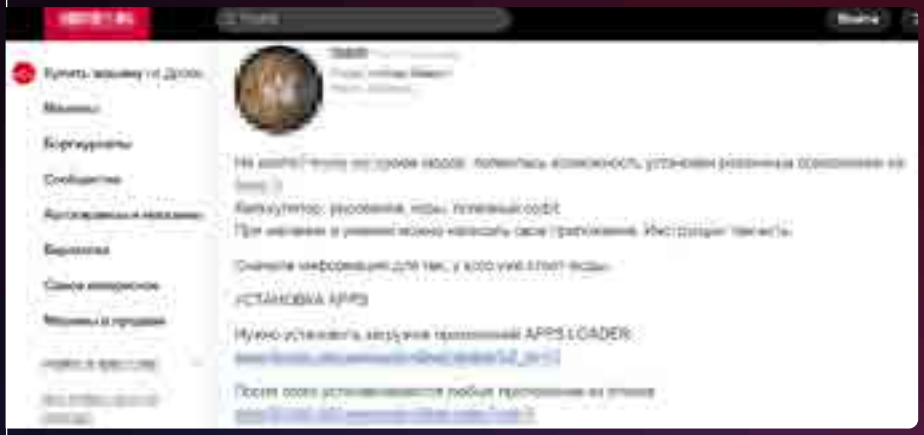
この脅威アクターは、44,000 人のフォロワーを持つ大規模な Facebook コミュニティを持っており、販売された製品が大きく露出していることを示しています。また、Youtube などの他のソーシャル メディア プラットフォームでも非常に活発に活動しており、非公式の USB ファームウェアアップデートの実行方法に関するサービスやチュートリアルを公開しています。

2023年11月、ロシアの人気自動車SNSサイトにおいて、さまざまなOEMのヘッドユニットに不正なコンテンツをインストール可能にする脱獄が公開されました。この脱獄は、ヘッドユニットに不正なアプリを追加するために必要なすべての手順が記述され、ダウンロード用のファイルも含まれていました。

脱獄インシデントはさまざまな影響をもたらす可能性があります：

- ソーシャル メディア プラットフォームで脱獄が広がるにつれ、車両のサイバーセキュリティ体制、安全性、消費者の信頼、自動車業界の評判に対する潜在的な悪影響が増大しています。
- インフォテインメントヘッドユニットを脱獄すると、安定性やパフォーマンスに問題が生じ、システム障害が発生したり、他の機能との互換性に問題が生じる可能性があります。
- 車両ソフトウェアの不正な変更はサイバーセキュリティの脆弱性を引き起こし、ハッキングの危険性を高め、盗難、データ漏洩、または車両の不正制御につながる可能性があります。
- 非公式のファームウェアアップデートは、影響を受ける OEMが提供する公式ファームウェアアップデートの価値を低下させ、テスト済みの公式ファームウェアアップデートの使用を顧客に勧めることが難しくなります。
- 許可なく車両のファームウェアをアップデートすると、保証が無効になる可能性があります。

© 2024 Upstream Security Ltd. 無断複写・転載を禁じます。



出典: Upstream Security

ロシアの人気自動車SNSサイトにヘッドユニット脱獄の実装方法を投稿

キーレスリピーター、ジャマー、OBDデバイスなどの高度な車両ハッキングツールは、ソーシャルメディア上でも広く宣伝されています。

2023年5月、脅威アクターがポーランドの自動車サイバーセキュリティとハッキングのオンラインショップを宣伝して、2008年から2023年に製造されたさまざまな自動車メーカーの車を開錠、起動できると謳うリレー攻撃型キーレスリピーターがTikTok上で販売されると、車両ハッキングツールの選択肢は大幅な広がりを見せました。[32] リレーアタックキーレスリピーターは、悪意あるアクターが物理的なキーフォブなしで車両に不正アクセスし、車両を盗むことを可能にします。

車両ハッキングツールはソーシャル メディア プラットフォームで広く注目を集めており、その結果、すでに大規模に増加しているキーレス車両盗難事件に即座に深刻な影響を及ぼし、一般市民の恐怖を増大させ、法執行機関にとってさらに大きな課題となっています。

出典: Upstream Security

販売者のTikTokページのスクリーンショット[33]

ソーシャルメディア上のサイバー活動の影響に対処するには、自動車業界、規制当局、ソーシャルメディアプラットフォームが協力して、一般の人々の意識を高め、自動車技術の安全性を確保する取り組みが必要です。

© 2024 Upstream Security Ltd. 無断複写・転載を禁じます。

自動車とスマートモビリティエコシステムは、生成AIの新時代に突入し、攻撃だけでなくサイバー防御も民主化が進んでいます。

自動車業界では生成 AI（GenAI）の時代が本格的に進行しており、OEM は顧客体験を向上させ、生産性の次の波を呼び起こそうと 生成AI 機能の導入を急いでいます。2023年、世界的なOEMは、マイクロソフト社のAzure OpenAIサービスのプライベートで安全なインスタンスを使用して、ChatGPTを活用した音声アシスタントを約90万人のベータテスターに公開しました。このサービスはOpenAIやChatGPTモデルとデータを共有しないように設定されています。[34]

生成AI 革命は、自動車のサイバーセキュリティ関係者と脅威アクターに大きな影響をもたらす

生成AIは、脅威アクターにとって、大規模な攻撃を効果的に行い、参入ハードルを下げるための重要なツールになると予想されています。
Large Language Models（LLMs）を利用することで、脅威アクターは脆弱性を迅速に特定し、その悪用方法を学習し、戦術、戦法、プロセスを標準化することができます。

> ***API は、ハッカーが 生成AI を使用して API ドキュメントを探索することができるため、特に脆弱性があります。API ドキュメントは一般に公開されている可能性があり、誤って情報が漏れたり、ダークウェブ に流出する危険性があります。***

生成AI を利用すると、エンドポイントのマッピング、API のターゲット設定、潜在的な脆弱性が特定できるほか、それらの脆弱性を悪用するための段階的なガイダンスの入手が可能になります。
LLMs は、公開された脆弱性データベースやサイバーセキュリティ研究から情報を取り込み、悪意のあるコードやスクリプトを生成するためにも利用できます。

> ***脅威アクターは、生成AI をツールとして利用して、複雑なフィッシング攻撃を実行し、自動化することができます。また、本物だと思わせる偽コンテンツ（ソーシャル エンジニアリング）を生成し、検出システムを適応して回避するマルウェアを作成することも可能です。***

その適応力と効率性により、従来のサイバーセキュリティ対策を回避できる大規模攻撃が可能となります。

サイバーセキュリティ権威インテリジェンスデータで訓練された LLMs は、攻撃戦略をエスカレートさせ、自動化されたプロセスと大規模で高度な攻撃を実行できます。 脆弱性と攻撃パターンを分析することで、自己進化するマルウェアの系統を生成し、既存のセキュリティ対策では検出できない独自のテクニック、ペイロード、ポリモーフィックコードで特定の標的を攻撃するバリエーションを作り出すことができます。

例えば、脅威アクターは 、LLMs を利用して脆弱性の発見を自動化することで効率を高め、脆弱性を特定するのではなく、脆弱性を不正利用するためにリソースを活用します。. 生成AIはまた、ハッカーが膨大な量のデータを迅速に選別し、最も攻撃しやすい場所を特定することも可能にします。このアプローチは、人間の分析では見落とされる可能性のある弱点を AI モデルが正確に特定できるため、攻撃プロセスを高速化するだけでなく、その有効性も高めます。

さらに、生成AI はさまざまな攻撃シナリオをシミュレートできるため、ハッカーは戦略を洗練させ、戦術の改良に利用できます。**生成AIを使用して攻撃環境をシミュレートすることで、サイバーセキュリティはさらなる課題に直面します。これは、予測不可能で高度な攻撃が増加し、**これらの攻撃を検知することが困難になるためです。

BAIN & COMPANY の調査によると、ダークウェブ上での 生成AIに関する 記述は 2023 年に桁違いに急増しました。[35]

BAIN & COMPANY の調査によると、ダークウェブ上での生成AI に関する記述は、 2023年に桁違いに急増しました。

自動車サイバーセキュリティのリーダーは、生成AIの革新的な機能の活用が必須

防御面では、生成AI は自動車のサイバーセキュリティ対策と運用を変革する可能性を秘めており、迅速な調査から vSOC ワークフローの自動化、ディープウェブやダークウェブのデータ、詳細なTARAに基づく複雑な洞察の生成に至るまで、幅広い活用を可能にします。

生成AI がもたらす比類のない効率性で、サイバーセキュリティチームは複数のソースから大量のコネクテッドカーとモビリティデータを迅速に分析し、パターンを検出し、インシデントアラートをフィルタリングして、調査を自動化することも可能になります。

> ***ガートナー社の最新レポートによれば、2023 年には 5% 未満にとどまっていた生成 AI の API やモデルの導入が、2026 年までには企業の 80% 以上が導入し、プロダクション環境でも 生成AI 対応アプリケーションが展開されると予想しています。***[36]

2023 年に、Upstream は独自の 生成AI 対応アプリケーション（アルファ版）を立ち上げました。このアプリケーションは、自動車関係者が調査の改善、自動化、データの洞察、および詳細な分析を通じて、vSOC の変革を成し遂げる助けとなります。現代のvSOCは複数のソースから大量のデータを取り込んでいるため、生成AIは簡単なNLPの質問でデータを照会し、分析を出してくれます。Upstream の 生成AI を活用した対策は、継続的に傾向を監視し、影響の背景と分析を提供します。

02

自動車のサイバーセキュリティの傾向

サイバーセキュリティ攻撃の規模と影響が拡大するにつれて、自動車とスマートモビリティの関係者は、新たな課題に直面しています。

インシデント

2023 年は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。

2023 年、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 295 件を分析しました。これは月平均25件に相当します。

2023 年の主なインシデント:

1月

- 研究者は、主要な世界的 OEM の車両を遠隔操作し、消費者の個人情報(PII)へアクセスできる重大な脆弱性を発見しました。[37]
- 韓国の OEM 車両数台に搭載されたヘッドユニットが不正アクセスされました。[38]

2月

- 日本の OEM が、グローバルサプライヤー準備情報システムのデータ侵害の影響を受けました。[39]
- 世界の OEM 各社は、自動車の盗難急増を引き起こした、ハッカーに活発に悪用されている脆弱性に対する緊急パッチをリリースしました。[40]
- CANバス操作を使用した、革新的な自動車盗難方法が増加していると報告されました。[41]

3月

- ハッキングコンテストに参加した研究者が、2 分以内に米国の OEM 車両をハッキングしました。[42]
- セキュリティ研究者が日本の OEM の顧客関係管理（CRM）システムをハッキングしました。[43]
- VoIP ソフトウェアベンダーに対するサプライチェーン攻撃の一環として、ドイツ、韓国、日本の OEM が、標的にされました。[44]

4月

- 研究者らは、車両に接近した攻撃者が日本の OEM 車両を盗むことを可能にする重大な CAN バスの脆弱性を報告しました。[45]
- セキュリティ研究者が、韓国の OEM に車載されているインフォテインメントシステムが影響を受ける重大な脆弱性を発見しました。[46]

5月

- 日本の OEM への攻撃で、車両の位置情報を含む 10 年分の顧客データが流出しました。[47]
- スイスの多国籍自動車部品サプライヤーが大規模なランサムウェア攻撃を受け、業務運営に影響がでました。[48]
- ドイツの自動車サービスプロバイダーがサイバー攻撃を受け、複数のシステムの利用に影響がでました。[49]

6月

- セキュリティ研究者が、人気のあるネットワークメッセージングプロトコルに、フリート全体のテレメトリーデータの操作を可能にする複数の脆弱性を発見しました。[50]
- 韓国の OEM のインフォテインメントユニットがセキュリティ修正後にもかかわらずハッキングされました。[51]
- 米国の EV 充電ステーションネットワークからの大規模なデータ漏洩で、企業の機密データや顧客の個人情報 (PII) が流出しました。[52]

7月

- 米EV充電会社の充電器がハッキングされ、不正なコンテンツや画像が表示されました。[53]
- ランサムウェア攻撃により日本の港湾業務に支障が生じ、日本の主要OEM自動車部品の入手に影響が出ました。[54]
- ドイツのOEM企業のウェブサイトにAPIの脆弱性があり、悪意のあるデータ流出が可能になりました。[55]

8月

- セキュリティ研究者が米国のEV OEMのインフォテインメントシステムをジェイルブレイクしました。[56]
- セキュリティ研究者が、人気の高いモビリティプロバイダーの脆弱性を発見し、アカウントの乗っ取りや違法な金融取引を可能にしました。[57]
- 米国のEV OEMのデータが漏洩し、75,000人以上の従業員が影響を受けました。[58]

9月

- 米国のトラック運送・車両管理ソリューションプロバイダーは、ランサムウェア攻撃を受け、顧客は走行時間の電子記録や輸送在庫の追跡ができなくなりました。[59]
- ドイツの大量輸送会社がサービスプロバイダーへのサイバー攻撃を受け影響が出ました。[60]
- 英国最大の物流グループのひとつが、ランサムウェア攻撃を受けて破産を宣言しました。[61]

10月

- 米国の大手引越し・保管レンタル会社がサイバー攻撃を受け、13GBの従業員データと業務データが流出したと言われています。[62]
- ドイツのOEMのブラジル販売代理店がランサムウェア攻撃を受けました。[63]

11月

- 米国の大手自動車部品販売会社のデータ漏洩により、18万人以上の従業員と顧客が影響を受けました。[64]
- 世界的OEMを顧客に持つ、中国の大手自動車部品サプライヤーがランサムウェア攻撃の影響を受けました。[65]
- 米国の州交通局がサイバー攻撃の影響を受け、サービスに大きな混乱が生じました。[66]

12月

- 研究者らが複数の車両フリートに影響を与えるフリート管理ソフトウェアに重大な脆弱性を発見しました。[67]
- 日本のOEMがオーストラリアとニュージーランドでサイバー攻撃を受け、顧客の個人情報漏洩につながりました。[68]

2023年の大半の攻撃は ブラックハットアクターによって実行された

テクノロジーとサイバーセキュリティ対策が進歩するに伴い、ハッカーも進化しています。そのため関係者は誰が攻撃を行っているかをより詳細に知る必要があります。

ハッカーは、その意図、行動、悪意に応じてブラックハット、ホワイトハット、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をもってシステムを攻撃します。
現在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、十分なリソースを備えており、世界中で何千人ものサイバー犯罪者を雇用しており、複数の企業に対する同時攻撃を行うことができます。

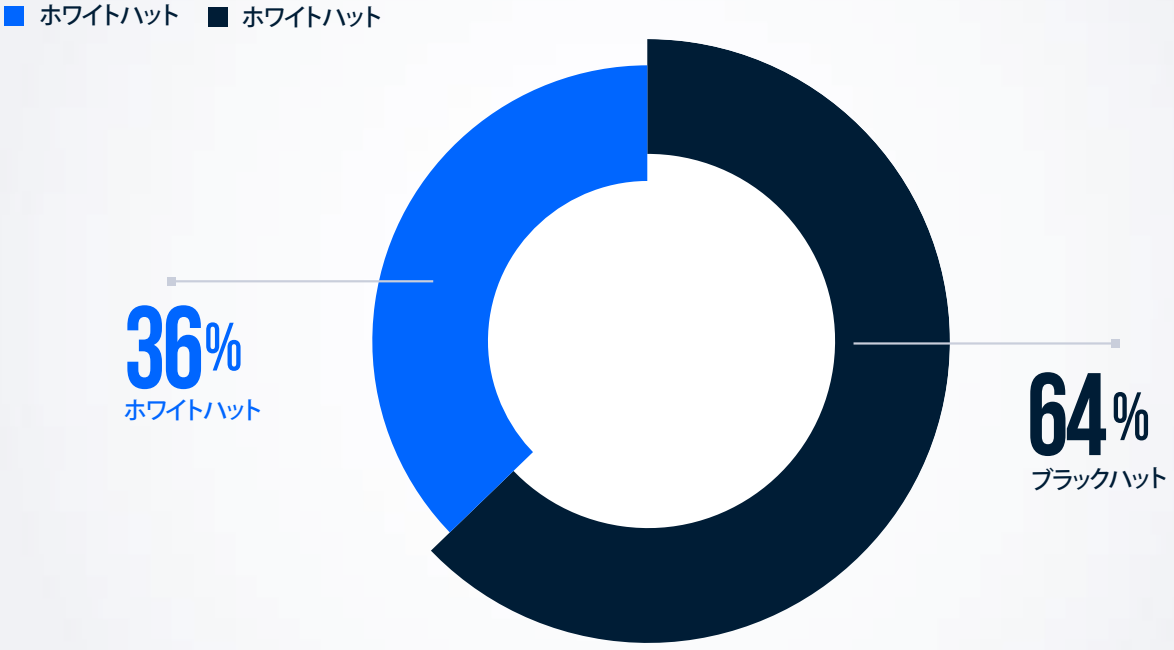
ホワイトハット

対照的に、ホワイトハットハッカーは、悪意のない研究者であることが多く、セキュリティの検証や脆弱性の評価を行うためにシステムに侵入し、操作します。
ホワイトハットハッカーは、常に新しい、あるいは不穏な脆弱性を発見しています。
彼らは、サービスを活用する企業を通じて、またはバグ報奨金プログラムの一環として、独立して運営されており、脆弱性を責任を持って開示することでで報酬を得ています。

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ハ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界線が曖昧になる、動的な状況を提示しています。
これらのハッカーは、脆弱性の発見に貢献する一方、場合によっては脆弱性を悪用することもあります。
グレーハットハッカーの動機は、名誉ある情報開示から、金銭的報酬や知名度といった利他的ではないものに至るまで様々です。
また、彼らの活動は明確な許可を得ずに行われるため、倫理的、または法的な問題を引き起こすことがよくあります。

2023年の攻撃のほとんど（インシデントの64%）はブラックハットアクターによって実行されました。



出典：Upstream Security

自動車のブラックハット攻撃とITのブラックハット攻撃の大きな違いは、攻撃の結果とその影響にあります。
自動車のブラックハットによる攻撃は、医療、エネルギー、政府施設などの重要なOTインフラに対するサイバー攻撃と密接に関連しており、サービスの中断や金銭的損失だけでなく、安全上や人命にかかわる危機につながる可能性があります。

2023年9月、米国を拠点とする大手トラック運送業およびフリート管理ソリューションの主要プロバイダーがランサムウェア攻撃を受けました。この結果、顧客は連邦規制で義務付けされている走行時間を電子ログに記録したり、輸送された在庫を追跡したりできなくなりました。[69]これを受け、同社は外部のサイバーセキュリティ専門家を雇って調査を行い、米国連邦自動車運送安全局に免責を申請して、サービスが復旧するまでトラック運転手が用紙による記録を使用できるようにしました。[70]

2023年6月、韓国のあるOEMの車載インフォテインメントシステムが、セキュリティのアップデートを発行した後にハッキングされました。[71]
過去に起きた攻撃では、同じハッカーがエンジニアリングメニューとファームウェアイメージの操作を通じてLinuxベースのシステムへのルートアクセスを獲得し、カスタムアプリケーションを実行できるようにしました。
OEMは新しいファームウェアイメージをリリースし、古いファームウェアイメージを削除することで対応しました。OEMのエンジニアは当初、ファームウェアイメージに署名するために秘密鍵を使用していましたが、アップデータが常に署名の検証を保証していなかったため、攻撃者はルートアクセスを獲得し、再び署名されていないコードをインストールすることができました。[72]

2023年12月、研究者は、ある車両管理ソフトウェアベンダーが、2023年4月に報告されたテレマティクスゲートウェイの危険な脆弱性を無視していたことを報告しました。ハッカーがバックエンドインフラストラクチャを標的にしてフリート全体を操作およびシャットダウンし、数万台の車両に影響を与える可能性があるため、この脆弱性は重大なリスクをもたらします。これらのゲートウェイがどの程度使用されたかは不明ですが、このベンダーは49カ国以上で11万9000台以上の車両を追跡しています。この脆弱性の悪用は確認されていません。[73]

OEMがコネクテッドサービスやソフトウェア対応機能のために、車載サブスクリプションを利用するようになっていることを受け、グレーハットハッカーは、セキュリティ対策を回避して独自のアプリケーションをインストールしたり、有料サービスに無料でアクセスしたりする方法を常に探しています。さらに、彼らが暴露し、ディープウェブやダークウェブ上のフォーラムでしばしば議論される脆弱性は、ブラックハットハッカーらによって悪用される可能性があります。

大半の攻撃はリモートで実行される

自動車サイバー攻撃のほとんどは、近距離攻撃 (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と、車両への物理的な接続（例：OBD ポート）が必要な物理的攻撃の2つのカテゴリーに分類されます。

> ***リモート攻撃はネットワーク接続（Wi-Fi、ブルートゥース、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的攻撃数を上回っており、2010年から2023年は全攻撃の89%を占め、2023年には95%に達するなど、増加の一途をたどっています。2023年のリモート攻撃の大半は遠距離からの攻撃でした（85%）。
接続性とソフトウェアデファインドアーキテクチャの採用の結果、遠距離攻撃の割合は増加し、2022 年の 70% から上昇しました。

2023年の大半のインシデントはリモート攻撃

2023年に発生したリモートでのインシデントの大半は遠距離攻撃

出典元：Upstream Security

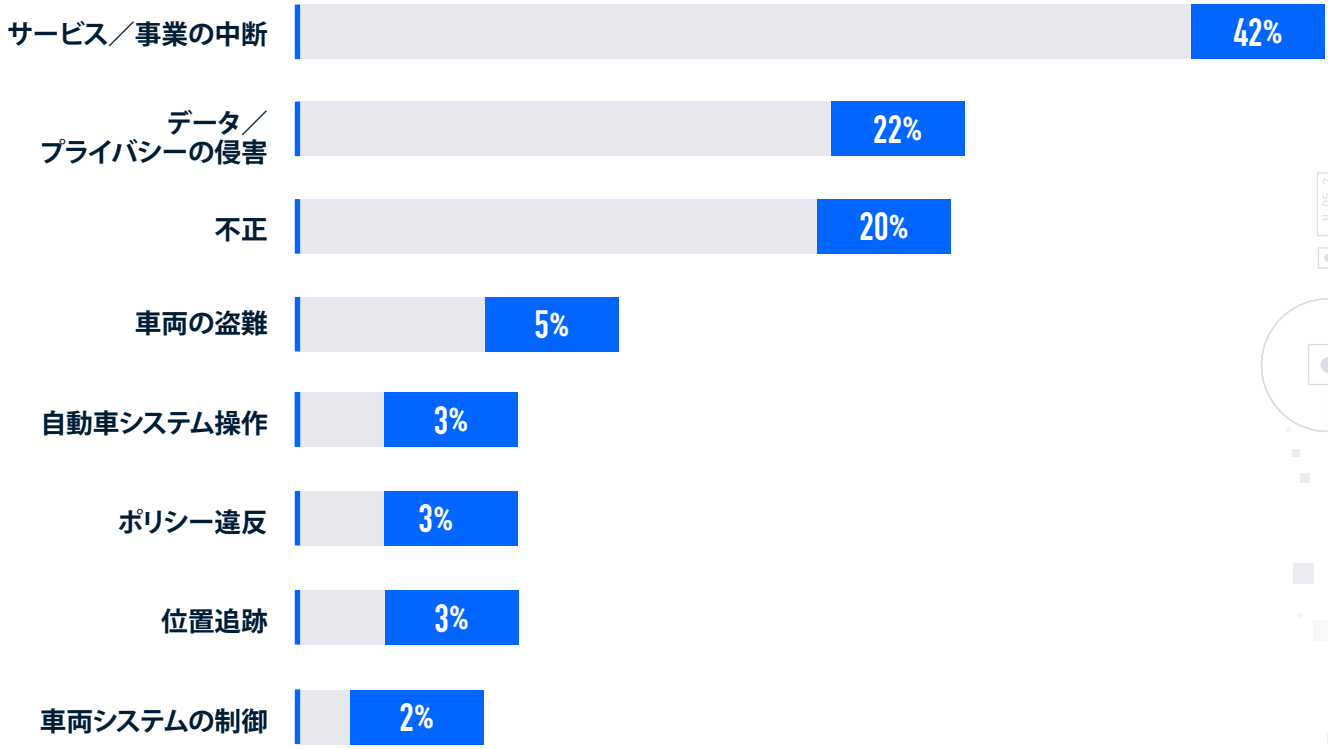
より強力になる攻撃

自動車とスマートモビリティエコシステムは、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、安全上の危険、ビジネスの中断、車両の盗難、システム操作、詐欺などの広範囲にわたる影響をもたらす可能性もあります。

運用サービスやビジネスの中断は増加の一途をたどりインシデントの42%を占めており、2022年の40%から増加しています。
また、詐欺関連の事件も劇的に増加しており、2023 年のインシデントの 20% を占め、2022 年の 4% から増加しました。

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、生産の遅延や停止などの通常業務の混乱（例：OEMやTier-1サプライヤーのランサムウェア攻撃、システムや機器へのサイバー攻撃によって引き起こされるオペレーションフリートの混乱）。
データ／プライバシー侵害	データ侵害は、脅威行為者が知的財産（IP）、企業秘密、財務情報、個人を特定できる情報（PII）などの専有機密データに不正アクセスした場合に発生します。 データ漏洩を伴うサイバーセキュリティに関するインシデントは、最も一般的で最も高額な費用が掛かります。
詐欺	金銭的利益を目的とした、脅威アクターによる車両データおよび/または車両消費者データの違法使用。
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盗難。
車のシステム操作	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、接続された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ができます。

自動車関連のサイバーインシデント295件に基づく2023年の影響内訳



出典元：Upstream Security

CVESを厳重に監視

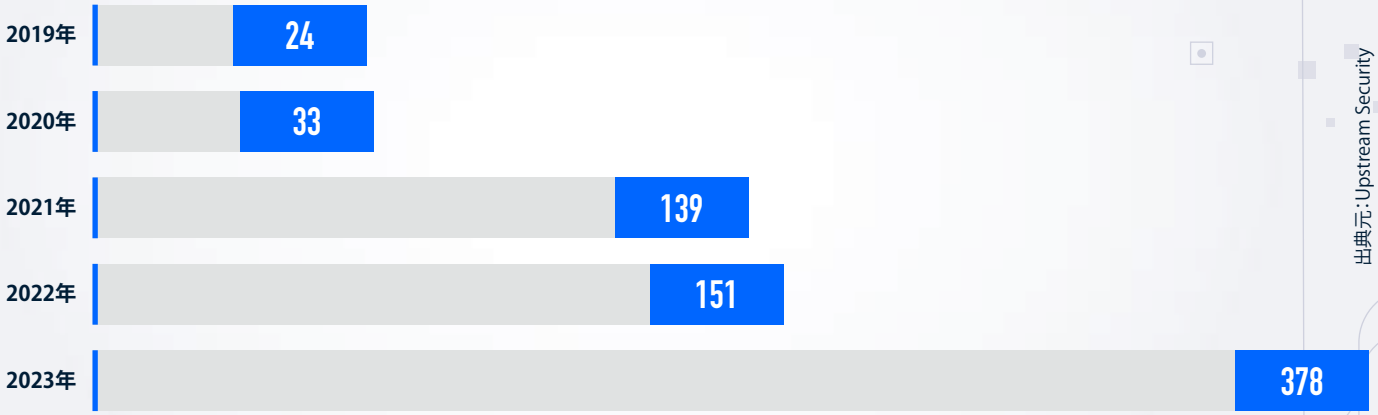
Common Vulnerability Scoring System (CVSS) は、CVEs を評価するためのオープンで標準化された方法を提供するように設計されました脆弱性スコアリングシステムです。CVSSは、脆弱性の基本的、時間的、環境特性に基づいて、組織が共同対応に優先順位を付け、調整をする援助をします。
また、脆弱性はCVSS スコアに基づいて「重大」「高」「中」「低」「なし」に分類されます。[75]

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。

自動車業界は2019年以降、725件の特定CVEsを記録しています。2022年の151件と比較して、2023年には378件のCVEsが公表されました。

2023年にCVEsが150%増加するのは、コネクテッドコンポーネントの継続的な普及と、脆弱性を積極的に特定しようという関係者の意識の高まりに起因します。

2019年から2023年に発見された自動車関連のCVEsの推移



出典：Upstream Security

セキュリティチーム、開発者、研究者は、リスクを評価するために、CVSSを他のいくつかの方法とともに使用します。CVSSスコアには、脆弱性がすでに悪用されているかどうかの判断やパッチ適用の優先順位付け、時間とリソースの効率的な割り当てなど、製品のサプライチェーン全体で実用的なアプリケーションがあります。CVSS は、攻撃の実現可能性を判断するための規格のリスク評価プロセスの一部として、ISO/SAE 21434 でも使用されます。

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注意深く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ときに考慮することもできます。

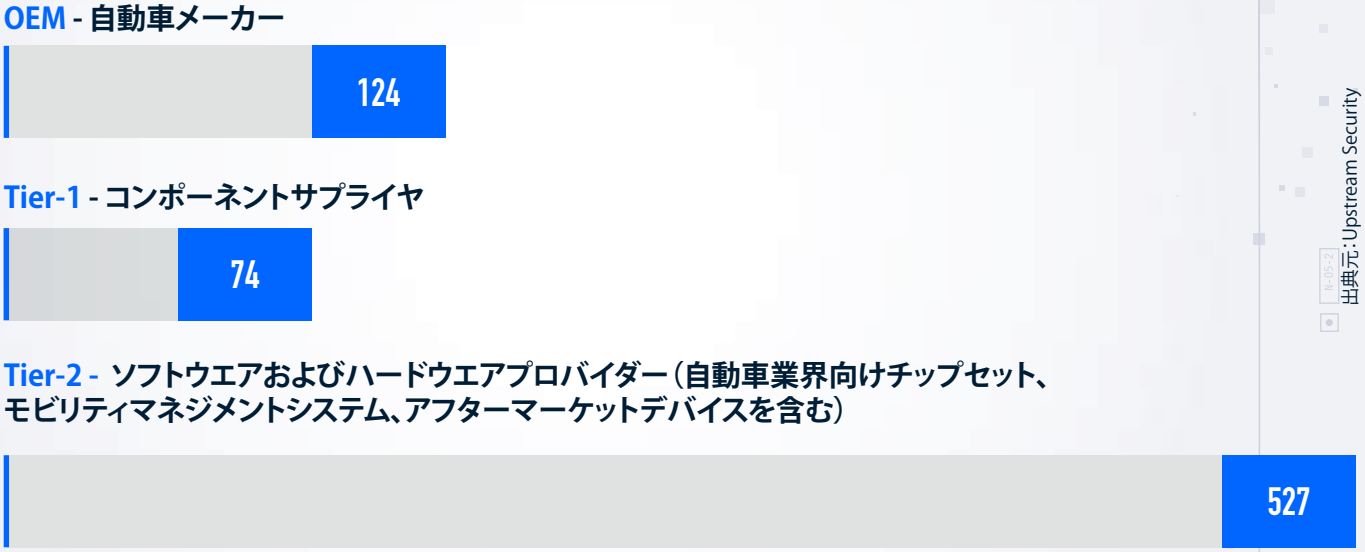
2023年CVSの概要

CVEsは、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る、認知されカタログ化されたサイバーセキュリティリスクです。これらの脅威ははOEM製品に見られるのが一般的ですが、OEMサプライチェーン企業の製品にも確認されることがあります。

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かかっています。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督し、確保する責任があります。
脆弱性は常に期限内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たったひとつの欠陥が、何百万台もの車両に影響を与える可能性があります。

CVEsは重要な脆弱性を開示していますが、ハッカーに悪用される可能性もあります。

公に報告された自動車関連の脆弱性の内訳（2019〜2023年）



出典元：Upstream Security

CVEs

2023年、アップストリーム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

34 重大な脆弱性

266 高い脆弱性

66 中度の脆弱性

12 低い脆弱性

出典：Upstream Security

2023年に自動車関連のCVEsが急増したのに伴い、深刻度も上昇しました。2023年には、重大かつ高度の脆弱性がCVEs全体の80%近くを占め、2022年の71%から上昇しました。

この傾向は、すべての利害関係者による自動車固有のCVEsを綿密に監視し、悪用を積極的に検出し、緩和を優先することの重要性を増幅させます。

その影響はスマートモビリティのエコシステム全体に及ぶ

サイバー攻撃は自動車、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を脅かしています。

- 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、宅配便
- 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
- ライドシェアリングとヘーリング
- スマートシティ
- 保険

出典元：Upstream Security

EV 充電、フリート管理、モビリティ共有アプリケーションなど、デジタル フットプリントを拡大している分野がますます増えており、ランサムウェア攻撃だけでなく、インフラストラクチャや公共の安全を標的とした攻撃にも直面しています。

OEMとサプライヤーによる責任の共有

費用のかかるリコール、ブランドの毀損、データの損失に加えて、OEMとそのコンポーネントサプライヤーに対するサイバー攻撃は、生産停止を引き起こしました。2023年6月、米国を拠点とする自動車産業向け高性能合金のTier-1サプライヤーに、サイバーセキュリティインシデントを示すネットワーク障害が出始めました。[76]その後11日間、管理、販売、財務、顧客サービスなど、同社の生産の多くの側面が大幅に中断されました。同社は、生産時間の損失が純収益に約1,800万から2,000万ドル、希薄化後の1株当たり利益に約0.40から0.45ドルの影響を与えたと報告しました。[77]

OEMはサプライヤーに大きく依存しているため、サイバー攻撃のリスクはさらに高まっています。ハッカーは、Tier-1または2のコンポーネントサプライヤーの脆弱性を悪用して、車両自体に直接アクセスする可能性があります。

2023年8月、オランダのTier-1電磁石サプライヤーがランサムウェア攻撃を受け、ランサムウェアグループが同社のビジネスシステムに不正アクセスし、開発部門と販売部門に障害が発生しました。このランサムウェアグループは、二重恐喝、初期アクセスブローカーのアフィリエイト、ハッカーフォーラムでの広告といったモデルを展開することで知られています。これに対応するため、同社は第三者の有力なサイバーセキュリティ専門家を雇用し、事業継続計画を含む対応手順を有効にしました。[78]

急速に拡大するEV充電エコシステム

EVの普及に伴い、送電網のサイバーセキュリティや充電インフラに対する懸念が高まっています。EVの急速な普及により、充電インフラの開発・展開が比較的早く進み、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見落とされることが多くなりました。

充電器は、その機能を操作する物理的およびリモート操作に対して脆弱であり、EVユーザーを詐欺被害、データ漏洩、さらにはランサムウェア攻撃にさらす可能性があります。また、車両から充電ネットワーク、送電網から車両、および送電網からフリートなど、さまざまな充電攻撃ベクトルに関連した新たな脅威も存在します。2023年1月、あるセキュリティ研究者が、有名な画面共有プログラムを悪用して、米国のEV充電会社の新しい350kW充電器の基盤となるオペレーティングシステム（OS）にアクセスしました。
研究者は、充電器アプリをバックグラウンドで実行したまま、OSメニューにアクセスし、ウェブブラウザを開き、競合他社のウェブサイトに移動することができたのです。[79]

以前にも、別のハッカーが充電器の重要な設定にアクセスし、過熱保護などの機能を閲覧するというインシデントが発生しています。[80]

2023年7月、セキュリティ研究者は、スイスを拠点とするプロバイダーの充電ステーション管理システム（CSMS）のAPIインターフェースに見つかった3つの重大な脆弱性に焦点を当てた詳細なレポートを発表しました。この脆弱性により、敵対者は他のユーザーがアップロードしたファイルにアクセスしたり、必要なプロビジョニングPINコード（認証）をバイパスしたり、充電器のOCPP接続を乗っ取ったりすることが可能になります。[81]

研究者は、ドライバーのデータを公開し、ベンダーのプロビジョニングプロセス、管理、充電ステーションの運用に関するサービスの可用性に影響を与える攻撃ベクトルを実証しました。[82]

2023年5月、セキュリティ研究者は、米国のEV OEMの所有者が使用する一般的なサードパーティ製アプリケーションに、CVE- 2023-29857として知られる脆弱性を報告しました。[83]
この脆弱性により、攻撃者はアプリケーションのリンクに直接アクセスすることで、機密情報を入手することが可能になります。[84]

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事業者は、車両管理のために接続性とソフトウェアへの依存度が高まるにつれ、そのサイバーセキュリティリスクは倍増しています。

2023年9月、米国を拠点とする大手トラック輸送および車両管理ソリューションプロバイダーがランサムウェア攻撃を受け、顧客は連邦規則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りました。[85]
これを受け、同社は外部のサイバーセキュリティ専門家を雇って調査を行い、米国連邦自動車運送安全局に免除を申請して、サービスが復旧するまでトラック運転手が紙のログを使用できるようにしました。[86]

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の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存されています。

2023年7月、ポーランドの都市交通局のサーバーがサイバー攻撃を受け、スマート交通システムが停止しました。この攻撃は、市内の公共交通機関の発券システム、信号機の管理、公共交通機関の停留所の電子案内板に影響を与え、市内全域に交通渋滞を引き起こしました。[87]

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活用して、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。

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やライドシェアサービスのプロバイダー、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。

2023年10月、サンフランシスコで歩行者が人間の運転する車にはねられ、さらにロボタクシーに轢かれるという事故が発生したため、カリフォルニア州は米国OEMのAVに対し、無人自動車を州道から撤去するよう命じました。[88]2023年11月、同OEMは米国で保有する950台のドライバーレスカーをすべてリコールしましたが、現在、安全性への懸念と社会的信頼の欠如を克服するため、徐々に運行を再開する計画を立てています。[89]

それにもかかわらず、他のAV企業は、技術の準備が整う前に急激に拡張しすぎた結果、上記のような問題が生じたと認識し、独自の展開と試行を進めています。[90]

このことは、2023年に行われた多くの発表によって実証されました。:

- 2023年7月、Waymoの共同最高経営責任者（CEO）は、配車サービスの分野で目覚ましい勢いと大きな商業的機会が見られていることから、トラック輸送に関する技術的、商業的、運用的な取り組みを先送りし、配車サービスへの取り組みと投資に集中することを決定したと発表しました。[91]

- 2023年8月、Axiosは、ダラスフォートワース地域でテストを実施している複数の自動運転トラック運送会社について報告しました。その中には、今後数年以内に自動運転トラックの展開を予定しているAurora、Gatic、Torc Robotics、Kodiak Roboticsなどが含まれます。[92]

- 2023年10月、WaymoはUberとの提携を発表し、Waymoが現在運営しているメトロフェニックスの225平方マイル以上のエリアで、完全自動運転、全電気式のWaymoライドを提供することを発表しました。[93]

- 2023年11月、トヨタとBMWが支援するMay Mobilityは、アリゾナ州、ミシガン州、ミネソタ州、テキサス州の少数の都市でオンデマンドの無人輸送シャトルを拡大するため、1億500万ドルの新たな資金調達ラウンドを発表しました。[94]

- 2023 年 11 月、AV 開発会社の Motional とHyundaiは、シンガポールで IONIQ 5 ロボタクシーを共同開発し、2024 年にラスベガスやその他の米国の都市に展開する計画を発表しました。[95]

- 2023年12月、日本はレベル4の自動運転車専用帯域の割り当てを決定しました。[96]

技術面では、新しいセンサーの種類、ソフトウェアやハードウェアの機能、サービス、通信の種類によって潜在的な脆弱性が露呈し、将来の攻撃の可能性が高まりつつあります。自動運転車は、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ます。

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阻止したり、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。[97]

農業用車両に対する修理権の影響

米国の農業用車両の修理権をめぐる論争は、2023年も引き続き大きな話題となりました。

特に農業用車両のオーナーは、所持している車両を自らハッキングしてメーカーの独自修理制限を潜り抜けて自分で車両修理ができるようにしたり、最新トラクター内に閉じ込められる事故を防止することに力を注いでいます。

一部の農家は、海賊版ファームウェアをインストールすることで、OEMの制限を回避しています。これにより、マルウェア、スパイウェア、ランサムウェアにさらされる可能性があります。さらに、正規ディーラーに頼らずに機器を自己修理しようとしている農家は、オンラインフォーラム上で、ソフトウェアのバグ、トラクターシステムの操作方法、コードとデータの交換方法について情報交換する可能性もあります。自己修理のために不正なソフトウェアやハッキング機器を使用すると、マルウェア、スパイウェア、ランサムウェアが意図せずインストールされ、メーカー保証が無効になる可能性があります。

修理権の動きに呼応して、全米でいくつかの法案が提出されています。彼らの目標は、農家や独立した技術者が自分で機器を修理できるように、機器メーカーにソフトウェア、コード、ツールを提供するよう要求することです。

- 2023年4月、コロラド州は米国で初めて農家のための「修理権」を認める法律を可決しました。これは2024年の初めに施行されます。[98]

- 2023年6月、アメリカファームビューロー連合(AFBF)はCLAAS of Americaと了解覚書（MOU）を締結し、さらに多くの農家や牧場主に対して自分の農機具を修理する権利を提供することになりました。[99] 2023年、AFBFはJohn Deere、CNH Industrial Brands(Case IH、New Hollandを含む)、AGCO、クボタと同様のMOUを締結しました。5つの了解覚書を合わせると、米国で販売されている農業機械のほぼ4分の3をカバーしています。

- 2023年11月、米国の裁判官はDeere社による統合訴訟棄却の取り組みを却下し、Deere社は、「農業機械メーカーがメンテナンスと修理のサービスを制限するために違法に共謀した」という作物農場と農民からの請求に直面しなければならないと述べました。[100]

世界中の規制当局は、修理権法によって引き起こされるサイバーリスクの増大が「転換点」に達する前に、そのリスクに焦点を移しています。2023年6月、NHTSAは、マサチューセッツ州の修理権法に起因する安全上の懸念について、数十社のOEMに通知しました。[101] NHTSAは、メーカーは連邦政府の安全要求事項をすべて遵守しなければならないと改めて強調しました。これらの最近の動向とNHTSAによる明確な指摘は、OEMにとって重要なガイドラインとなり、この対立を将来的に解決する道筋を示しています。

03

2023年における サイバー攻撃の現状

スマートモビリティおよび自動車業界関係者が認識すべき、新たな脅威と、それらがもたらすサイバーレジリエンスへの影響

巧妙化する攻撃がエコシステム全体に大規模な影響を及ぼす可能性

2023年、サイバー攻撃はより巧妙かつ頻繁になり、さまざまな車両システムやコンポーネント、スマートモビリティプラットフォーム、IoTデバイス、アプリケーションを標的にするようになりました。
新たな攻撃手法により、あらゆるコネクティビティが攻撃に対して脆弱であるということが業界内で強く認識されるようになっています。

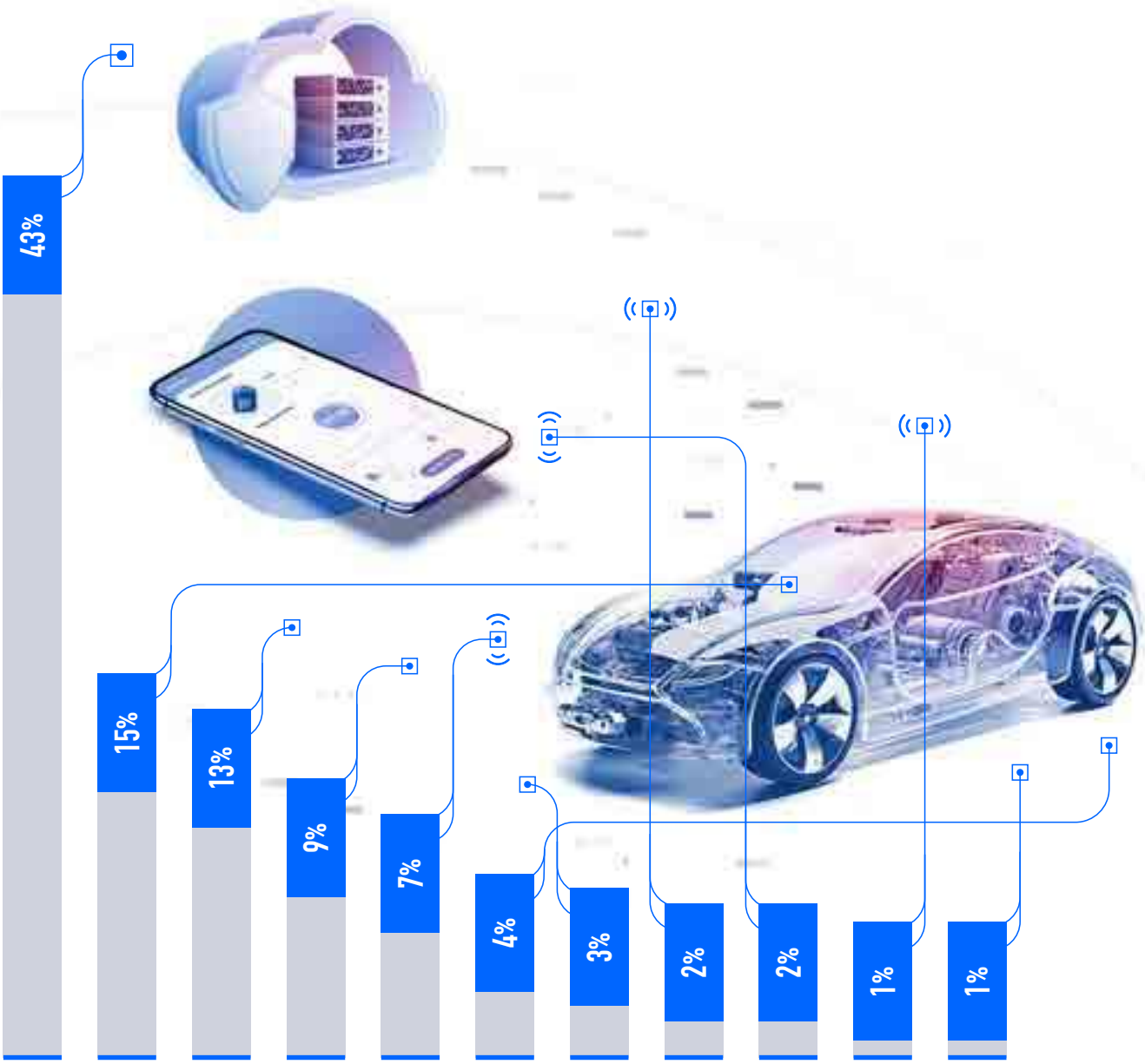
2022年にスマートモビリティのエコシステムの中核となる2つの領域が標的となってから攻撃は増加し続けている状況です。この2つの領域の1つは、モビリティアプリケーションおよびサービスのためのAPI、そしてもう1つは、今後10年でガソリンスタンドなどの燃料供給インフラに取って代わると予想されるEV充電インフラです。

なお、APIベースの攻撃は2022年に劇的に増加し、インシデント全体の12%を占め、380%という驚異的な増加を示しました。今後、さまざまな脅威アクターがAPIの脆弱性を利用して大規模な攻撃を仕掛けてくるため、APIベースの攻撃は徐々に拡大していくと予想されます。
実際、2023年にはAPIがインシデント全体の13%を占めるようになりました。

2023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、バックエンドサーバー（テレマティクス、アプリケーションなど）や インフォテインメントシステムをターゲットとするインシデントが急増しました。サーバー関連のインシデントは2022年の35%から2023年には43%に増加し、インフォテインメント関連のインシデントは2022年の8%から2023年には15%とほぼ倍増しました。

この傾向は、コネクテッドコンポーネント(サーバー、インフォテインメントシステム)への認識と可視性の高まりに直接関係しています。また、自動車のサイバーセキュリティ環境が確立したことや、脅威アクターが大規模なモビリティ資産全体にわたって機密データや車両制御へのアクセスを得ようとしていることも要因になっています。

標的別インシデント



出典：Upstream Security

テレマティクスおよびアプリケーションサーバー

コネクテッドカーは、車両のライフサイクルを通じて、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。これを実現するために、2種類のサーバーを使用します。1つは車両と通信するテレマティクスサーバー、もう1つは車両のコンパニオンアプリと通信するアプリケーションサーバーです。

さらに、保険会社、フリート、レンタカーおよびリース会社、EV充電ネットワークなどのサードパーティと通信するバックエンドサーバーを搭載する車両もあります。

ブラックハットアクターは、バックエンドサーバーの脆弱性を狙うことで、走行中の車両を攻撃することもできます。

- 2023年6月、Automotive Security Research Group(ASRG)のセキュリティ研究者は、コネクテッドカーで広く採用されているネットワークメッセージングプロトコルであるMQTTに複数の脆弱性を発見しました。これにより、攻撃者は一般的なテレマティクスユニットを使用してフリート車両全体のテレメトリデータにアクセスし、さらには操作できるようになります。[102]

CVE-2023-3028[103]と総称される一連の脆弱性が特定されました:

- MQTTバックエンドは認証が不要なため、攻撃者の不正アクセスが可能になります。
- 車両のテレメトリデータ(GPSの位置、速度、走行距離計、燃料など)がパブリックトピックのメッセージとして公開されてしまいます。バックエンドは、パブリックトピックの MQTT 投稿としてコマンドも車両に送信します。その結果、攻撃者はフリート全体の機密データにアクセスできてしまいます。
- 車両またはバックエンドから送信されるMQTTメッセージは、暗号化も認証もされていません。攻撃者は、車両やバックエンドになりすましてメッセージを作成し、投稿することができます。攻撃者は、例えば、車両の位置について誤った情報をバックエンドに送信することもできます。
- バックエンドサーバーは、パブリックトピックで特定のMQTTメッセージを送信することで、車両のCANバスにデータを注入できます。これらのメッセージは認証も暗号化もされていないため、攻撃者はバックエンドになりすまして、偽のメッセージを作成し、バックエンドが管理する車両にCANデータを注入することもできます。

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、自動車の盗難や車上荒らしが増加の一途をたどっている現状では、このリモートキーレスエントリー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操作により、ブラックハットアクターは自由に攻撃を実行できます。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、こうした攻撃が一般的になっています。

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。キーフォブと車両間の通信は、無線信号を傍受して中継、再生、または妨害できる装置を利用して操作できます。

キーフォブのメカニズムと車両間の通信は、いくつかの方法で攻撃される可能性があります：

「ライブ」信号によるリレーアタック

リレーアタックでは、キーフォブの信号が圏外であっても、ハッカーは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、車の近くに設置された送信機や中継器を使用して無線信号を増幅させることができます。そして、メッセージを増幅し中継して車両エンジンのロックを解除して始動させます。窃盗犯は、車両所有者の自宅内にあるキーフォブからの信号を傍受するために、このタイプの攻撃をすることが多くなっています。

蓄積された信号を使ったリプレイ攻撃

別のタイプのリレー攻撃では、ハッカーはキーフォブと車両間で送信されるメッセージを傍受し、後で使用するために保存します。関連するメッセージを取得した後、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。

キーフォブのリプログラミング

より高度で高価な装置を使用してキーフォブシステムを再プログラムすることで、元のキーを使えなくすることができます。再プログラミング装置は、オンラインで合法的に入手でき、公認の整備士やサービスセンターで使用されています。OBDポートに接続するため、自動車窃盗犯が車両を完全にコントロールすることが比較的容易になります。

キーフォブと車両間の通信妨害

また、自動車窃盗犯はキーフォブと車両間の通信を遮断する信号妨害装置を使って、車上荒らしに入ることも可能です。この装置により、所有者が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インジェクションによるワイヤレスキーフォブECUの偽装

ハッカーが好む新しい攻撃方法として、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ケーブルに接続してワイヤレスキーフォブECUになりすますCANインジェクターデバイスを使用し、リモートキーレスエントリーシステム全体をバイパスすることが可能です。

- 2023年1月、セキュリティ研究者が、フランスのOEM車種のリモートキーレスシステムに影響を与える脆弱性（CVE-2022-38766に記載）を発見しました。この脆弱性は、ローリングコードセットに基づいています。ローリングコードセットはリプレイ攻撃を防止するための一連の変更コードです。このケースでは、システムが、新しいローリングコードセットを生成する代わりに、ドアの開放要求毎に同じローリングコードセットを使用していることを研究者は発見しました。
この脆弱性により、攻撃者は専用のデバイスを用いて信号を傍受・再生し、キーレスシステムを操作することが可能となります。[104]

- 2023年2月、スコットランドのグラスゴーの警察は、前月に市内で28台の車両が盗難されたことを受け、キーレス車両の盗難が増加しているとして警告を発しました。[105] 同日、英国サフォーク州警察は、英国OEMの高級SUV 5台が1ヶ月間で盗難に遭い、キーレス車両の盗難が急増していると市民に警告しました。[106]
2023年3月から5月にかけて、ベルギーのワーテルロー地方警察[107]、英国のウスターシャー警察[108]、ドイツのフランコニア警察[109]が同様の発表をしました。
2023年8月、英国政府は、前年比25%増と急増している車両盗難に対処するため、キーレス車両のハッキング装置を禁止する計画を発表しました[110]

- 2023年4月、サイバーセキュリティー研究者が、CANインジェクタデバイスを用いてスマートキーシステム全体をバイパスするCANインジェクションと呼ばれる新たな攻撃手法を公開しました。[111]
このデバイスをヘッドライトコネクター、テールライトコネクターからコントロールCANバスに接続するか、パネルに穴を開けてツイストペアのCANケーブルを通してコントロールCANバスに接続すると、スマートキーECUになりすますことが可能です。この研究者は、2022年7月に発生した日本のOEM車の盗難事件について、長期にわたりデジタル・フォレンジックによる調査をおこない、2回の失敗を経て、この手法を発見しました。[112]

ECUs

エンジン、ステアリング、ブレーキ、ウインドウ、キーレスエントリーなど、さまざまな重要システムを司る電子制御ユニット（ECU）は、干渉を受けたり操作されたりすることがあります。ハッカーは、複数の高度なシステムを同時に作動させることで、ECUを操作し、その機能を制御しようとします。

- 2023年2月、米運輸省道路交通安全局（NHTSA）は、2019年11月から2021年6月までに製造された約1万7000台の日本製OEM SUVのリコールを命じました。ハイブリッドバッテリー出力の計算に使用されるハイブリッド車両制御ECUのソフトウェアは、必要に応じてバッテリー出力を制限せず、特定の条件下でハイブリッドシステムが完全にシャットダウンする場合があります。[113]
  この問題の理由は不明ですが、重大なサイバーリスクに発展する可能性があることは確かです。

- 2023年11月、ハッカーがマイクロコントローラーを搭載したデバイスを使用して、日本のOEM車のCANバスを読み取り、エンジンがオフになっても車両のACC（アクセサリー）リレーに通電し続け、ステレオとインフォテインメントシステムへの電力を維持できるようにしました。[114]
  この種の攻撃は、プライバシー侵害や他の車両システムの不正利用につながる可能性があります。

APIs

コネクテッドカーやスマートモビリティのIoT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必要ない標準的な手法で、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2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。

- 2023年1月、セキュリティ研究者のグループが、テレマティックスシステム、自動車API、およびそれらをサポートするインフラのセキュリティについて数か月にわたり調査した詳細な研究記事を発表しました。同グループは、世界の主要な19のOEMとサプライヤーで複数の脆弱性を発見し、車両を遠隔操作し、OEMと消費者の機密データにアクセスできるようにしました。[115]

- 2023 年 3 月、セキュリティ研究者は、開発アプリを変更して実稼働するAPI を使用することで、日本の OEMのCRM データベースにアクセスできるようになったと明らかにしました。この API は、読み込みスピナー設定によって意図せず公開されていました。APIの設定ミスや適切な認証・検証がなされていなかったことにより、研究者はOEMの顧客の氏名、住所、電話番号、メールアドレス、納税ID、車両・サービス・所有履歴等にアクセスできました。[116]

- 2023年7月、スイスを拠点とするプロバイダーのCSMS(Charging Station Management System)プラットフォームのAPIインターフェースに3つの重大な脆弱性が発見されたとセキュリティ研究者が報告しました。[117]　この脆弱性により、攻撃者は他のユーザーがアップロードしたファイルにアクセスしたり、必要なプロビジョニングPINコード(認証)をバイパスしたり、充電器のOCPPを乗っ取ったりすることができます。

- 2023年11月、ASRGのセキュリティ研究者は、ドイツのOEM車両に搭載された特定のECUを攻撃者がクラッシュさせ、REST APIコールを介して音量を最大レベルに不可逆的に変更することを可能にする脆弱性(CVE-2023-6073118に記載)を開示しました。[119]

- 同月、ビットマスクAPIの処理中に発生し、予期しない動作を引き起こし、システムをクラッシュさせるマルチモードコールプロセッサのメモリ破損の脆弱性(CVE-2023-22388[120])を、一般的な車載プラットフォームチップのTier-2サプライヤーが公開しました。[121]

モバイルアプリケーション

コネクテッドカーやソフトウェアデファインドカーの増加により、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を提供できるようになります。また、車両所有者はスマートフォンやデバイスを使って重要な機能を便利にコントロールできるようになります。モバイルアプリケーションを使用することで、ユーザーは車両の位置を追跡したり、ドアを開けたり、エンジンを始動させたり、補助装置の電源をオンにしたりすることができます。

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。

- 2023年5月、セキュリティ研究者は、米国のEV OEM所有者が使用する一般的なサードパーティ製アプリケーションの脆弱性（CVE-2023-29857[122]）を報告しました。この脆弱性により、攻撃者はアプリケーションのリンクに直接アクセスして、機密情報を入手することができます。[123]

- 2023年6月、パキスタンで1,000万人以上のユーザーを持つ人気の配車サービスがハッキングされ、その結果、消費者が嫌がらせのメッセージや通知を受信する事態が発生しました。同社によると、サードパーティの通信APIが侵害されていたのが原因でした。[124]

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。

- 2023年5月、自動車業界におけるオープンソース実装の提唱者であるハッカーが、オンラインで販売されているツールを使って日本の自動車OEMのインフォテインメント・システムのハッキングに成功し、不正利用の証拠をGitHubに投稿しました。このハッカーは、USBドライブを介して複数のアプリケーションを伝送制御プロトコル経由でインストールすることに成功しました。その中には、ファイルマネージャーやサードパーティ製アプリも含まれていました。[125]

- 2023年8月には、ドイツの研究者が、チップメーカーのプロセッサーに電圧フォールト注入攻撃を用いて米国のEV OEMのIVIシステムのジェイルブレイクに成功し、ほぼ取り消し不能のルートアクセスを得ました。この攻撃により、研究者はインフォテインメントシステム上で任意のソフトウェアを実行し、加速の高速化やシートヒーターなどの有料機能のロックを解除することができました。さらに、このエクスプロイトにより、OEMの社内サービス・ネットワークで認証と認可に使用する車両固有の鍵（暗号システムの公開鍵）の抽出が容易になりました。このエクスプロイトによって取得したルート権限で、悪意のあるアクターがプライベートユーザーのデータにアクセスし、暗号化されたNVMe(Non-Volatile Memory Express)ストレージを復号化し、自動車のIDを改ざんする可能性があります。[126]

EV充電インフラ

電気自動車の普及を加速させるためには、信頼性と安全性の高い充電インフラの提供が不可欠です。しかし今日では、多くの充電器、充電インフラ・コンポーネント、関連アプリは、物理的な操作や遠隔操作に対して脆弱なので、信頼性のある動作を妨げたり、EVユーザーを詐欺や身代金攻撃にさらしたり、充電ネットワーク、地域の電力網、あるいは法人車両にも広範な影響を及ぼす可能性があります。

- 2023年1月、ハッカーが人気の画面共有プログラムを悪用し、米国のEV充電会社の新しい350kW充電器の基本オペレーティング・システム（OS）にアクセスしました。ハッカーは、充電器アプリがバックグラウンドで実行されている間に、OSメニューにアクセスし、Webブラウザを開き、競合他社のWebサイトに移動することができました。[127] 以前にも、別のハッカーが充電器の重要な設定にアクセスし、過熱保護などを閲覧することができたというインシデントが起きています。[128] どちらのケースも、電気自動車の充電セキュリティに関する意識を高めることを目的としたインシデントでした。

- 2023年6月、セキュリティ研究者は、最も人気のあるパブリッククラウドプラットフォームの1つで、パスワードなしでホストされている内部データベースを発見しました。このデータベースには、世界中に数十万のEV充電ステーションのネットワークを持つ世界的なEV充電サービスプロバイダーの数百万のログ（約1テラバイト）のロギングデータが含まれていました。また、EV充電ネットワークを利用する顧客に関する機密情報（顧客名、Eメールアドレス、フリート顧客の電話番号、ネットワークに充電する車両を持つフリート事業者の名前、車両識別番号（VIN）、EV公共充電ポイントおよび家庭用充電ポイントの位置など）も含まれていました。[129]

ブルートゥース

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。

2023年3月、ハッキングコンテストに参加したフランスのセキュリティ研究者チームが、エクスプロイトを使って米国のEV OEMのIVIに侵入することを実証しました。このエクスプロイトには、ヒープオーバーフローの脆弱性とBluetoothチップセットの範囲外の書き込みエラーが含まれていたために、研究者は他のサブシステムのルートアクセスを得ました。[130]
このエクスプロイトは、非常に影響力のある脆弱性とエクスプロイトに対してのみ贈られる、長年続いたコンテストで初のTier-2賞を受賞し、25万ドルの賞金も獲得しました。[131]

OTAアップデート

OTA（Over-the-Air）プログラミングは、遠隔ソフトウェア管理方法の1つで、新しいソフトウェア、ファームウェア、または構成設定を、中央からネットワークを通じてすべてのデバイスに無線配信することを可能にするものです。ソフトウェアデファインドアーキテクチャの拡張により、OTAを利用して、OEMとそのTier-1およびTier-2サプライヤーはSBOMを継続的に更新し、車両の品質、安全性、機能性を向上させ、新機能を導入できるようになります。

しかし、リモート・アップデートは物理的なアップデートよりもリスクが高くなります。ワイヤレス通信は多くのサイバー攻撃に機会を与え、複数の車両、さらには全フリート車に一度に影響を及ぼす可能性があるからです。

さらに、アップデートは車両の機能性にとって極めて重要になる可能性があります。OTAアップデートの失敗は、2023年11月に米国を拠点とするEV用OEMが起こしたように、深刻な車両の不具合を引き起こす可能性があります。OEMは、特定機能のバグ修正と改善を提供するOTAアップデートをリリースした後、突然キャンセルしました。アップデートに失敗した結果、2つの車種のインフォテインメント・システム（重要な車両機能を作動させるために使用される）が機能しなくなりました。OEMは、この問題は人為的なミス（誤ったセキュリティ証明書とともに誤ったビルドが送信された）によるものであり、OTAアップデートを利用して問題を修正し、完全な機能を回復できると述べました。[132]

OTAがより頻繁に使用され、ますます多くのOEMによって活用されるようになるにつれ、Upstream社のAutoThreat®研究者は、ディープウェブとダークウェブにおけるOTA関連の活動を継続的に監視しています。当社の研究者は、OTAのアップデートを乱用してサイバー攻撃を実行しようとすることへの関心が高まっていることを確認しました。

V2X攻撃はまだ初期段階にありますが、今後数年でさらに増加すると予想されます

テレマティクス、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。
車両接続には、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。

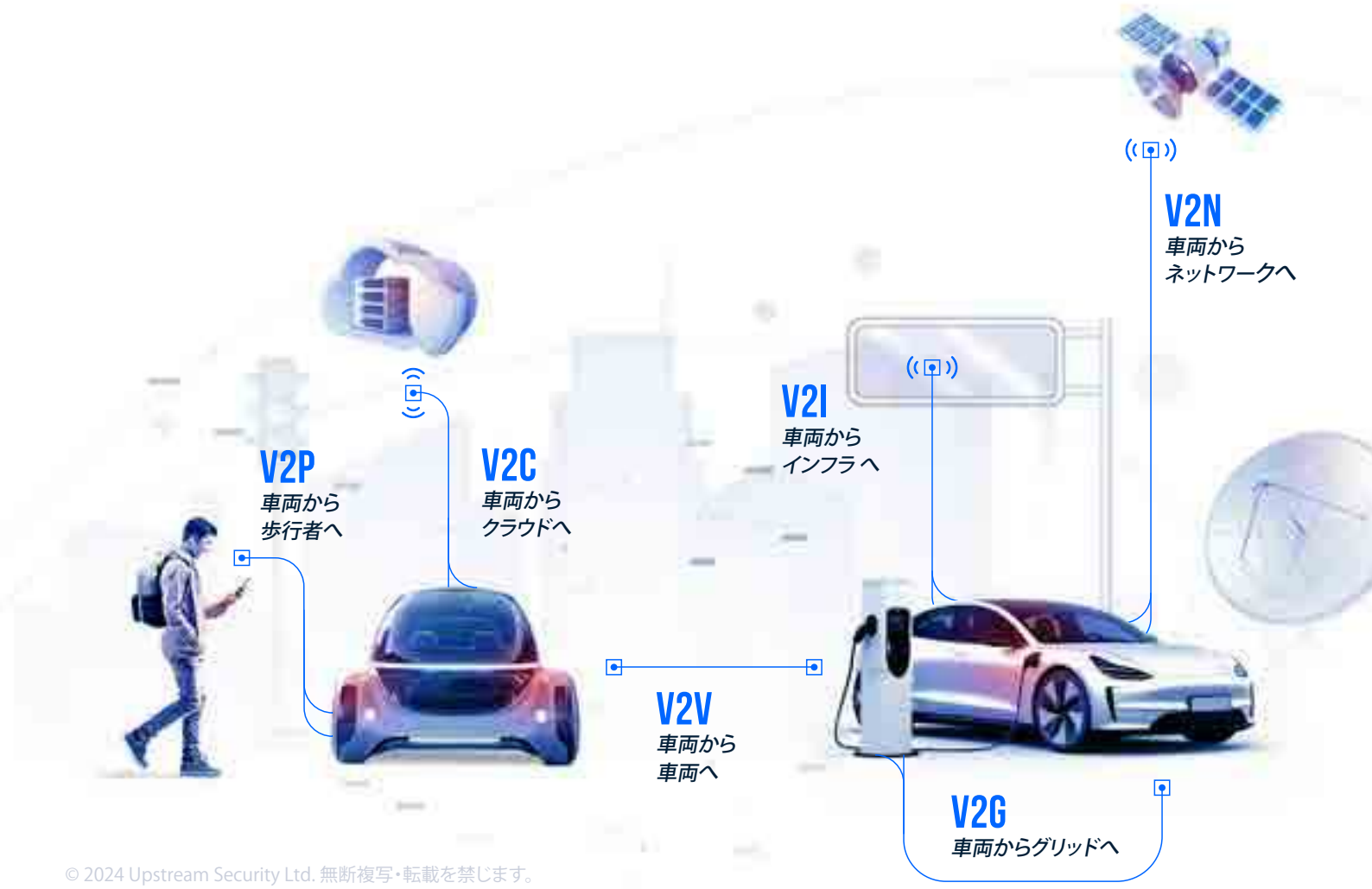
最も重要な追加機能は、車両が道路上の他の車両やデバイスと通信し、EV充電器や道路インフラなどの外部ソースからデータを受信する機能です。

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かかっています。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。[133]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[134]

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。[135]

この命令はC-V2Xの普及に向けた重要な一歩ですが、現在のFCC規則はDSRC標準に基づいており、C-V2X標準とは互換性がないため、最終規則までにはまだ多くの課題を解決する必要があります。



04

規制の現状

規制の拡大に備え、コネクテッド
モビリティ資産を安全に保つための
新しい基準を採用

生成AIは自動車とスマートモビリティのエコシステムを再構築していますが、規制は依然として進化の途上にあります。

生成AIは、自動車業界を再構築し、完全にカスタマイズ可能なドライブ体験とパーソナライズされたデータ駆動型の機能を提供しています。継続的な学習により、個々の運転パターンに適応することで安全性を高めます。自動車産業における生成AIの世界市場は、2022年には3億1200万ドルと評価され、2030年には17億ドルに達する見通しです。[136]

しかし、生成AIの影響力が増大したことで、関連するリスクと規制上の障害が明らかになりました。生成AIによる出力結果が間違っていたり、害を及ぼす可能性を懸念する声が上がっており、重大な問題になっています。AI機能の使用は、安全性、責任、法的責任に関する複雑な問題を提起します。生成AIを採用する競争圧力により、統合がより広範になるにつれて、組織はリスク管理のための戦略を積極的に策定する必要があります。生成AI技術の急速な進化に伴う多面的な課題に対処するためには、新たなサイバーセキュリティリスクの導入を含め、包括的なアプローチが必要です。[137]

生成AIの規制やガイドラインの状況は、金融業界を筆頭に多くの業界で進化しています。2023年11月、シンガポール金融管理局（MAS）は金融機関向けの生成AIリスク管理フレームワークとガイドラインを発表しました。これらのガイドラインは、複数の銀行や大手テクノロジーベンダーと共同で作成されました。[138]　2023年12月、欧州議会もまた、人工知能法に関する暫定合意に達したことを発表しました。[139]　この規制は、基本的権利が確実に保護されることに重点を置き、リスクと影響に基づいたAIの使用義務を定めています。また、この規制の取り組みは、欧州市場全体でAIベースのテクノロジーを急速に普及させることも目的としています。

自動車業界でも同様の傾向を予測し、他の懸念事項の中でも特に安全性とプライバシーの確保に焦点を当てた、特定の生成AIガイドラインとリスク管理フレームワークの開発が見込まれています。

自動車産業における生成AIの世界市場は、2022年には3億1200万ドルと評価され、2030年には17億ドルに達する見通しです。

サイバーセキュリティの世界的規制強化

世界的な規制強化は、技術の進歩に適応し、安全性を促進し、環境問題に対処しようとする、政府と規制当局の協調的な取り組みを反映しています。この規制強化は、自動車産業界の未来を形作るという世界的な取り組みを示しています。

中国

中国は最近、さまざまな規制やガイドラインを導入し、自動車とスマートモビリティのエコシステムに関連したリスク管理フレームワークを確立するため、幅広い取り組みを行っています。

2023年12月、中国運輸省はロボタクシーや自動運転トラック、ロボバスなど、自動運転車(AV)サービスの試行ガイドラインを発表しました。

16カ月にわたる世論調査を経て策定された全国的なガイドラインでは、自動運転車の安全性を確保するため、ルールの標準化や総合的な監視体制の構築を進めています。
例えば、AVは自動化レベルに関係なく、指定されたエリアでしか運行できません。

- 自動運転バスは「閉鎖された道路、または比較的条件が単純な道路」に限定されます。
- ロボタクシーは「管理された安全な交通状況下」で許可されます。
- ロボトラックには明確な制約があり、「ポイントツーポイントの高速道路または良好な交通状況」に限定されています。

運営者は、公共交通機関の許可と関連するライセンスを取得しなければならず、AVには道路での注意喚起のための明確なラベルを付ける必要があります。

さらに、このガイドラインではソフトウェアについても言及しており、無線 (OTA)アップグレードは産業情報省の安全規制に従わなければならないと強調しています。[140]

中国工業情報化部は、自動車情報セキュリティの技術要件や完成車の情報セキュリティ技術要件など、4つの必須国家基準について一般からの意見を募集しました。これらの基準は、2023年7月5日まで意見を募集していました。

> ***UNECE WP.29 R155とほぼ一致していますが、規格の開発、策定、および有効期間を担当する機関、車両のセキュリティ要件、試験方法、車種の変更などの分野で違いがあります。***

中国政府は審査に向けて初版の完成を目指しており、2024年半ばに規格をリリースする予定です。導入はリリースから 12 か月後の 2025 年半ばに予定されています。[141]

2023年6月、中国国務院は規制枠組みに関する通知を発表し、中国で高品質の充電インフラシステムを推進する必要性を強調しました。この枠組みは、標準化の欠如、施工不良、アンバランスな設計など、急速に成長する中国の充電インフラが直面する課題に対処するための戦略的対応です。この枠組みはまた、2030年に向けて設定されたより広範な戦略目標にも対応しています。これには、広範なカバレッジ、適度な規模、合理的な構造、完全な機能を備えた質の高い充電インフラシステムの構築も含まれます。[142]

日本とEU

日本とEUでは、国連規則（UN-R157-01シリーズ）により、2023年1月時点で、高速道路での制限速度が130km/hで、車線変更が可能なレベル3の自動運転装置の承認が下りています。
今後の規制は、レベル4と5の無人車両に焦点を当てます。[143]

インド

2023年4月、インドは乗用車の実走行排出ガス（RDE）規制を実施し、路上走行時の排出ガス規制の遵守を義務付けました。
この規制は、テスト条件と実走行時の間に生まれる排出ガス量の差に対処するものです。RDEは、欧州での規制強化を受けて、多様な走行条件をカバーし、実環境に合わせて排出基準を調整する適合係数への依存度を低減します。この提案は、インドの政策立案者が、適合要素を段階的に廃止するスケジュールを設定するためのものです。特に欧州は、2025年までに、RDE試験で測定された小型車のすべての路上排出ガスが、RDE基準の境界条件に基づく実験室試験の限界値を超えないように提案しています。[144]

RDEを実施するには、路上を走行中の車両からリアルタイムのデータを収集、分析する必要があります。このデータには、排出ガス、エンジン性能、運転パターンに関する情報が含まれる場合があります。このような機密データを不正アクセスや潜在的なデータの悪用から守るためには、サイバーセキュリティ対策が必要です。

2023年11月、インドは世界標準に従い、自動車メーカーに対し、「サイバーシールド」と呼ばれる必須セキュリティフレームワークを提案しました。道路交通大臣が支持するこの計画は、サイバー脆弱性から車両システムを強化し、電気自動車の充電ステーションまで保護を拡大することを目的としています。このイニシアティブは、乗用車と商用車の両方を対象としており、相互接続が進む自動車業界において、先制的なサイバーセキュリティ対策の重要性を認識しています。草案は国会承認前に専門家による精査が行われることになっています。[145]

米国

2023年8月、カリフォルニア州プライバシー保護局（CPPA）は、内蔵アプリ、センサー、カメラを通じてコネクテッドカーが収集する膨大なデータを調査するための執行措置を開始しました。この動きは、自動車業界におけるプライバシーへの関心の高まりを反映しています。CPPA は、OEM の透明性を確保し、収集されるデータの把握、その拡散の防止、削除の要求など、消費者データの権利を遵守することをことを目的としています。
このイニシアティブは、データ管理に関する懸念を浮き彫りにしており、サプライチェーン、物流、建設など、自動車以外の業界にも影響を与える可能性があります。[146]

UNECE WP.29 R155および ISO/SAE 21434の拡大

2023 年、多くの自動車 OEM とそのサプライヤーは、サイバー セキュリティ管理システム (CSMS) と型式承認用に R155[147]、ソフトウェア 更新管理システム (SUMS) 用に WP.29 R156 (148) の実施を継続しました。[148] R155の第2マイルストーンに基づき、2024年7月から生産されるすべての新車に適用、義務化されます。過去数か月の間に、OEMの一部は、予想されるR155への適合が難しいことと、今後の第2マイルストーンに基づき、特定モデルの生産を中止しました。[149]

これらの規制は、ISO/SAE 21434[150]とともに、サイバー脅威からの保護を目的に、統一したアプローチを構築するための世界的な取り組みの一環です。

規制の変更、業界標準の発展、および研究での知見により、米国運輸省道路交通安全局 (NHTSA)[151]、欧州連合サイバーセキュリティ機関(ENISA) (152) 、加盟業界団体Auto-ISAC[153] など、ガイドラインとベストプラクティスを更新した組織もありました

R155とISO/SAE 21434はどちらも、特定の解決策や正確なプロセスの概要を示すのではなく、サイバーセキュリティ分析を高い基準で実施することの重要性を強調しています。このガイドラインでは、プロセスの概要を説明し、リスク分析および対応目標を定め、開発、生産、生産後の段階で、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く示されています。

UNECE WP.29 概要

規則WP.29の主なコンポーネント

R155 CSMS

サイバーセキュリティ管理システム

車両の設計段階から製造完了後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
L6	重量350kg（～770lb）以下の四輪車で、エンジンが50立方cmを超えず、最高速度が45km/h（～28mph）に設計されているもの	R155（レベル3以上の機能を装備する場合）
L7	重量が400kg（～880ポンド）未満の四輪車で、連続定格出力が15kWを超えないもの	R155（レベル3以上の機能を装備する場合）
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

出典：UNECE

車両は、カテゴリー分類に応じて、R155(154)、R156(155)、またはその両方で規制されます。

自動車産業への規制の影響

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ける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、維持する必要があります。車両がよりソフトウェアで定義されるようになり、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 を実行する複雑さは劇的に変化しました。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証明することが求められるため、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カ国で事業を行うOEMに適用されます。

R155により、OEMやサプライヤーは、新規および新興の車両アーキテクチャ、モビリティサービス、コネクテッドビークルエコシステムに関連するセキュリティリスクを特定し、対応できるようになります。これには以下のような脅威が含まれます。

- 生産中の車両に関連するバックエンドサーバー
- 車両とつながる通信チャネル
- 車両のシステム更新
- サイバー対策が不十分な車両
- 車両の外部接続に関する事項
- 車両データ/コード

R155規制は、自動車のサイバーセキュリティにおいて、具体的な脅威事例や緩和策を提示するなど、実践的なアプローチをとっている点が特徴です。しかし、それは包括的なアプローチにも基づいており、プロセスとガバナンス、およびIT、製品、OT、IoTの観点をカバーしています。

この規制では、「プロセス」という用語が明確に強調されており、低レベルの技術仕様を義務付けることなく、サイバーセキュリティ構造に関するガイダンスを提供する意図があります。今日の自動車サイバー環境は、多様かつダイナミックであり、厳格な技術的対策は逆効果です。この規制は、意図的に技術に中立的な形で草案されており、OEMが自動車のサイバーセキュリティをどのように確保するかについて、ある程度の柔軟性を持たせています。

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月に予定されている拡張により、すべての新車は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。[156]

ISO/SAE 21434による長期的な信頼の確立

ISO/SAE 21434 基準の主な違いとして、ISO/SAEの基準は、 OEMとそのサプライヤーに資産リスクを計算する包括的なプロセスを提供し、そのスコアの計算方法と脆弱性に対する緊急度に応じて優先順位付けを提案することです。

この基準は、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、コンセプト段階から廃車までの車両のライフサイクルを通じて、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基準とR155 CSMSの要件に従うため、OEMは、自動車が組立ラインを離れてから10年以上にわたって継続的に監視を実施するためにvSOC(仮想セキュリティオペレーション)を維持することが推奨されています。

> ***2023年には新たに378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たことで、関係者は、既存および将来的な脆弱性と、将来発生する可能性のある未発見の脆弱性の両方から製品を保護するために、危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。***

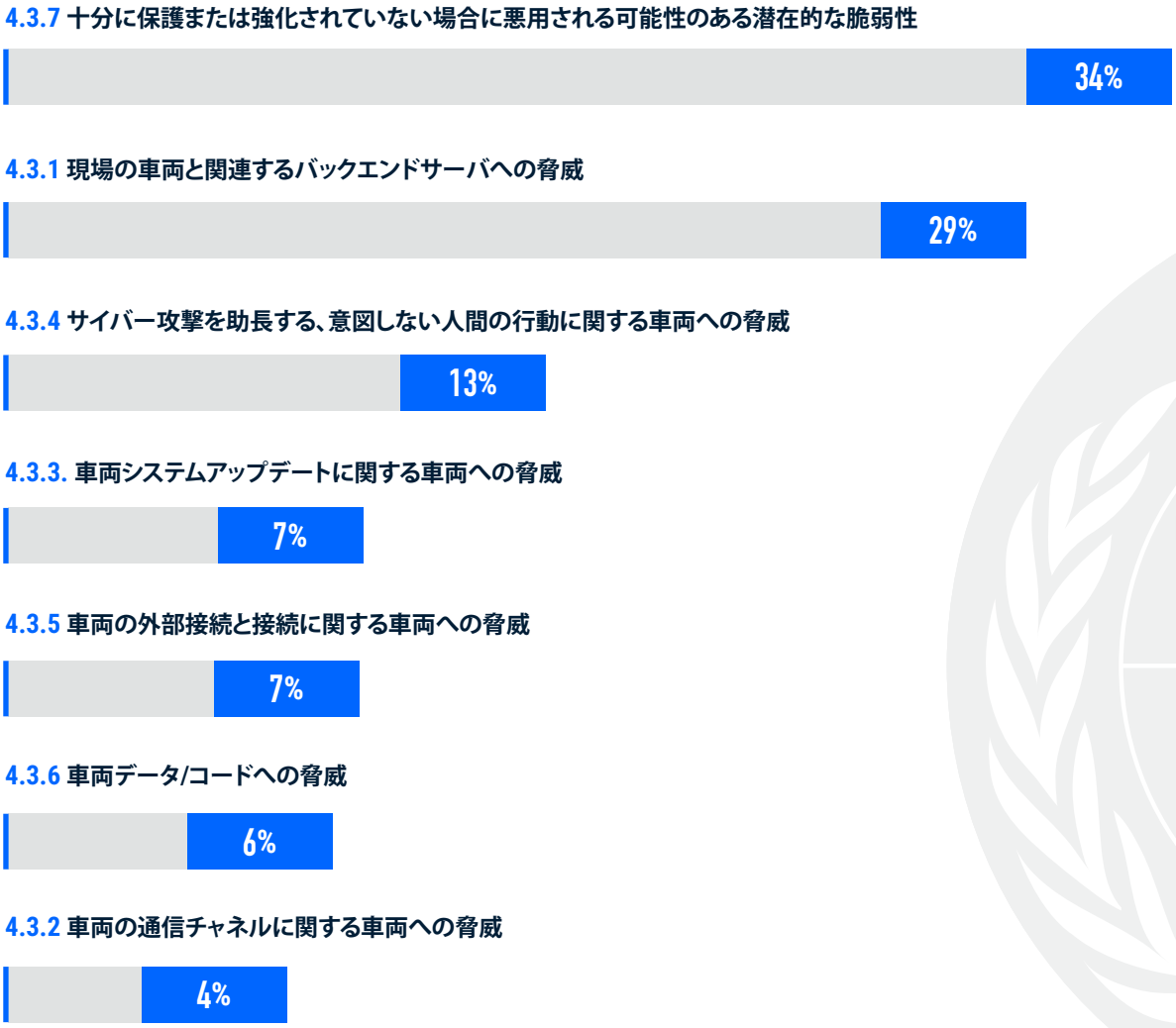
ISO/SAE 21434 と WP.29 が連携し、世界規模で車両をサイバー攻撃から保護

ISO/SAE 21434	R155	R155	R155	R156
設計によるセキュリティ	**サイバーセキュリティ管理システム**	**脅威分析とリスク評価**	**モニタリング**	**ソフトウェア更新管理システム**
製品開発の各ステップにおける技術要件	車両のライフサイクル全体を通じたサイバーセキュリティのモニタリング	脆弱性のリスク評価とリスクスコア	車両ログに基づく早期発見とインシデントへの迅速な対応	車両のライフサイクル全体にわたる継続的な安全性の更新

R155 は既存の脅威に対応しているのか?

Upstreamの調査チームは、2023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つの脅威カテゴリに関連付けました。

R155の脅威と脆弱性に分類される2023年のサイバーインシデント



出典：Upstream Security

成熟し続ける規制状況

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、政策当局は規制の在り方を常に考えています。
2024 年 7 月時点で、すべての新車にスコアを拡大するという 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。

R155の対象は二輪車や農業機械に拡大する見込み

現代の二輪・三輪車は、コネクテッド化が一層進み、複数のソフトウェアコンポーネント、センサー、電子部品、高度なインフォテインメントシステムを含むように設計されているため、これらすべてがサイバーリスクを大幅に増大させています。二輪車の安全確保は、自動車エコシステムの安全性と信頼性を深めるための世界的な取り組みの一環です。実際、2023年7月に、UNECEはR155の適用範囲を拡大し、L6およびL7.を含む現在の適用範囲を超えて、すべてのカテゴリーL車両を対象とする提案を提出しました。[157] CLEAPが主導するこの提案が承認されれば、2029年7月から発効し、二輪車OEMにCSMSの導入が義務付けられることになります。

UNECEはまた、カテゴリーTの車両や農業機械、関連するカテゴリーR（農業用トレーラー）およびカテゴリーS（交換可能な牽引式農業または林業用機器）にも、R155の適用を追加するオプションについて議論しています。[158] この拡大に関しては、合意が得られていない中、2024年中に決定が予定されています。

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

2023年 12月にアップデートされたEUサイバーレジリエンス法 (CRA) は、デジタルコンポーネント (ハードウェアとソフトウェアの両方) を備えたすべての製品を対象とする水平的な法律です。[159] CRAの焦点は消費者であり、スマートウォッチから自動車まで、最新のコネクテッドデバイスの利用を保護することです。

CRAは製品のライフサイクル全体をカバーし、製品の計画、設計、開発、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、メーカーに対して、悪用された脆弱性やインシデントを積極的に報告し、製品のサポート期間を通じて効果的にリスクを軽減することを求めています。[160]

CRA は 2024年5月に発効予定で、製造メーカーは36か月以内に準拠する義務があります。[161]

CRAの適用範囲を決定することは、OEMやその他のモビリティ関係者にとって重要です。CRAでは特に、R155も含む一般安全規則（EU）2019/2144 [162]の対象となる製品は除きます。したがって、カテゴリーM、N、およびOの一部の車両には、R155が適用されます。その他の車両はCRAの対象となります。[163] R155 がその適用範囲を拡大するにつれて、CRAに準拠するための要件にも直接影響を与えることになります。

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」[164] 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。[165] 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：[166]

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、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。

ISO15118 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。

SEC、サイバーセキュリティインシデントへの関心の高まりに同調

2023年7月、米国証券取引委員会 (SEC) は上場企業のサイバーセキュリティに関する情報開示の最終規則を採択しました。[167]

2023年12月15日に発効した最終規則には 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（Form 8-Kを使用して）開示すること、そして、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 (Form 10- Kを使用して) 毎年開示することです。[168]

新しい規則によれば、SECの規制下で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、そのインシデントの性質、範囲、発生時期等の重要な側面に加え、そのインシデントが企業に与える重要な影響または合理的に予測される重要な影響について、財務状態や業績の結果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による影響が重大な部分に焦点を当てています。

この規則では、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、司法長官からの書面通知がある場合に報告を遅らせることが認められています。また、小規模企業に対しては180日の延長も認められています。[169]

2023 年11月、ランサムウェアグループは発効日を知らず、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。[170] 攻撃が疑われた時点では、新しいSECはまだ発効しておらず、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。

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。これらの事象は現在、確立された重要性基準に基づき、重要事象として株主やSECに報告する必要があります。

SECの新たなサイバーセキュリティ規制により、サイバーセキュリティ攻撃への対応に追われる自動車およびモビリティ関係者による申告が相次ぐと予想されます。

NHTSA サイバーセキュリティのベストプラクティスを更新

NHTSA(米運輸省道路交通安全局)は、2023年に新車向けの最新のサイバーセキュリティベストプラクティスを発表しました。[171] これらのガイドラインは法的な拘束力を持ちませんが、進化する攻撃手法とエコシステム全体におけるサイバーセキュリティリスクの軽減に対して緊急性を持たせることを目的としています。

R155などの自動車業界全体のサイバーセキュリティ慣行の標準化や、NHTSAの最新車両に関するサイバーセキュリティーベストプラクティス[172] の発表を見ると、世界中の政府機関や規制当局が、さらに脆弱化している車両のハッキングからの保護を重要視していることが分かります。

初版の最終稿は、新しい業界基準や研究を考慮し、実際のインシデントや2016年および2021年の草案で提出されたコメントから得た知識を組み込んでいます。NHTSAは、自動車とそのサイバーセキュリティの進化に合わせて、サイバーセキュリティのリスク評価とベストプラクティスの更新を続けていきます。

NHTSA は、米国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、保護、検出、対応、復旧」に基づく階層化されたサイバーセキュリティのアプローチを推奨しています。

- 安全上重要な車両制御システムと機密情報の保護をリスクベースで優先順位付けをする
- 潜在的な脅威やインシデントをタイムリーに検知し迅速な対応をとる
- 攻撃発生時の迅速な復旧
- 効果的な情報共有を含む、業界全体で学んだ教訓の浸透を加速させる方法

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の結びつきが強調されており、自動車業界の結びつきが強まりつつある中で、安全技術者やセキュリティ関係者も、ハッカーのシグナル操作能力を考慮すべきであるという点を明確にしています。

NHTSAの最新の推奨は、サイバー対策の構成とプロセスはISO/SAE21434の遵守であり、リモート攻撃からの保護に関してはR155の遵守も挙げられています。

NHTSAのガイドラインでは、セキュリティーと安全性を確保するため、連携の重要性が強調されており、業界全体での効果的な情報共有の手段としてAuto-ISACへの参加が提案されています。 Upstreamはこれを推進しており、コミュニティの共同メンバーとして、Upstream AutoThreat®Intelligence Cyber Incident Repository[173] を維持し、毎年発行しているサイバーセキュリティ年次報告書で知見を共有しています。Upstream は、Auto-ISAC[174] および ASRG[175] のメンバーでもあり、業界の知識の共有が行われ、サイバーセキュリティのベストプラクティス形成に尽力しています。

ADS と ADAS に対する最新のアプローチ

自動運転は常に進化しており、NHTSA は自動運転システム (ADS) と先進運転支援システム (ADAS) に関する規制を策定しています。2023年4月、NHTSAは第2次改正SGO 2021-01 「自動運転システムおよびレベル2先進運転支援システムのインシデント報告」を発行しました。[176]

更新されたSGOは、2023年5月15日から3年間施行され、2021年に発行された当初のSGOで定められた報告要件の更新が含まれています。 これにより、NHTSAは、ADSおよびレベル2のADAS搭載車両に関する実際の事故について、標準化された、適時かつ透明性の高いデータを受け取ることができます。これは、急速に進化し、公道でテストされている自動化技術の潜在的な安全上の懸念を特定するために不可欠です。

2023年7月、NHTSAは、この分野に内部リソースを集中させるため、NHTSAの既存の規則策定室の下に、自動化安全室と自動化除外部門を設置しました。[177]

NHTSAは修理権より安全性とサイバーセキュリティを重視

修理権とは、車両の所有者や個人修理工場が、車両の診断、整備、修理に必要な情報、ツール、ソフトウェアにアクセスできる権利のことを指します。高度な技術や複雑なシステムを備えた現代の車両背景において、修理権は重要な問題となっています。2023年には大きな話題となりました。

> ***2023年6月、劇的な動きとして、NHTSAは、マサチューセッツ州の修理権法[178]に関する安全上の懸念を記した書簡を数十社のOEMに送りました。この書簡では、サイバーセキュリティの懸念から同法を無視するよう警告しています。***

NHTSAはさらに、自動車メーカーが連邦政府の安全義務を完全に遵守することを期待すると明言しました。

2023年のNHTSAの最新情報

2023年8月、NHTSAは、シートベルトの着用を増やすために、OEMに対し、右助手席と後部座席にシートベルト着用警告システムの装備を義務付ける規則案を発表しました。当該規制案は、乗用車、トラック、バス、重量1万ポンド未満の多目的乗用車に適用されます。[179]

2023年 9月、NHTSA は、後部衝撃ガードと発光可変 (ADB) ヘッドランプに関して、国家運輸安全委員会 (NTSB) が発行した速度に基づく交通死亡事故の削減に関する安全勧告に対応しました。[180]

どちらの取り組みも、安全機能を無効にして車両システムを操作するサイバー主導の方法を探している不正行為者の注意を引く可能性があります。これらの操作は、ディープウェブまたはダークウェブのフォーラムやマーケットプレイスで公開されると、他の悪意のあるアクターによっても使用される可能性があります。こうした潜在的な操作は、動機に関係なく、安全性を損なうだけでなく、保証も無効になる可能性があります。

EV充電インフラのサイバーセキュリティ規制は拡大し続ける

現在、EVは世界の新車販売台数の約15%を占めており(181)、 2040年までに新車販売台数の過半数を占めると予想されています。[182] 電気自動車充電ステーション (EVCS) の数が急速に増加する中、世界中で EVCS を侵害し操作しようとする脅威アクターによって、市場は挑戦を強いられています。

EVCSは、複数のベンダーのコンポーネントを搭載したコネクテッドIoTデバイスであり、市場の要求に応じて迅速に設置されます。
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。

- 充電ポイントオペレーター (CPO) は充電エコシステムでは必須段階ですが、バックエンドのコマンドアンドコントロール (C&C) サーバーをハッキングすることで広範囲に攻撃される可能性があります。CPOは、複数の充電ステーションを標的にしたり、広範な充電需要を作り出すことで遠隔攻撃され、広範囲でサービス拒否を引き起こす可能性があります。さらに攻撃者は、個人情報(PII)や課金パターンなどのプライベートな消費者データに不正にアクセスする可能性があります。

- APIを利用した攻撃は、比較的簡単なサイバースキルや技術スキルでも実行できる可能性があります。この攻撃手法は、シンプルでありながらも十分な攻撃範囲を持ち、フリート全体に影響を与える可能性があります。API攻撃はバックエンドサーバーを標的にして影響を与え、その結果、データの盗難やサービス妨害が発生する可能性があります。API攻撃は、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、通信するエコシステム内のあらゆるエンティティから発生する可能性があり、その逆も同様です。

EVの普及が進むにつれ、EV充電器と充電インフラに焦点を当てた新しい規格が登場しています。

> ***EVの充電基準は、電力網における電力需要の増加を管理するとともに、安全で信頼性が高く、利用しやすい充電器を提供することに重点を置いています。***

EVCSを保護する規制は大きく2つに分けられます：

01

運用基準

EVCSがバックエンドサーバーや車両、CSMSと安全に通信し、データの保存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、そして現在開発中の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の製造元および車両OEM によって作成されています。

02

地域規制の理論的フレームワーク

規制は国または地域レベルで州によって施行されます。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（スマート充電ポイント）規制などが含まれます（本レポートでさらに説明）。

世界の規制当局は、サイバーリスクに対するEVCSの安全確保に焦点を当てた、様々な種類の規制を推進することに注力しています。

EVCSのサイバーセキュリティ規制の最新事例

地域 / 国	規制	焦点	実施日	実施状況
米国	NIST IR 8473	EVCS		任意
	国家電気自動車インフラ基準および要件	EVCS	April 2023	必須
EU	ETSI EN 303 645	IoT	2025年8月	
	NIS2指令	重要インフラ	2024年10月	必須
	EUサイバーレジリエンス法	IoT	2024年初頭予定	必須、3年間の移行期間あり
英国	英国規格協会 (BSI) のエネルギースマート家電 (ESA) の規格	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
日本	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セキュリティおよび安全フレームワーク	IoT	2020年11月	必須

米国

2023 年 3 月に、米国連邦道路局 (FHWA) による国家電気自動車インフラ基準と要件が発効しました。[183] 本新規則は、国家電気自動車インフラ (NEVI) フォーミュラプログラムの下で資金提供されるプロジェクト、および特定の法定当局の下での公的にアクセス可能なEV充電器の建設プロジェクト (連邦補助高速道路上のプロジェクトとして扱われる、連邦資金提供によるEV充電インフラプロジェクトを含む) に関する要件と最低基準を定めるものです。

基本的に、FHWAはISO 15118の原則を採用し、連邦官報における最終規則の公表日から1年後までに充電ステーションがISO 15118に適合し、プラグアンドチャージ機能を備えることを要求しています。現在、市場に出回っている多くの充電器がISO 15118を採用していませんが、この法律はコンプライアンスのために国家規格を採用することの意義を強調しています。[184]

また、充電ステーションの設置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超高速充電インフラ向け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超高速充電インフラのサイバーセキュリティリスクを管理するためのガイダンスを最終決定しました。[185]
EV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、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ーの運用
- 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。[186]

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。

EU

IoT機器に関するETSI EN 303 645の規制が欧州電気通信標準化機構によって発行されました。ETSI EN 303 645は、スマートコネクテッドデバイスにおけるデータ保護と整合性を確保するために特別に設計されました。同規制は現在検討中であり、最終要件案は2025年8月1日に提示される予定です。[187]

NIS2指令は、重要インフラとエネルギー分野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おり、EVCSも規制対象に含まれます。また、IoT機器のサイバーセキュリティ保護に言及しているEUサイバー連帯法も対象としています。[188] 本イニシアティブは、サイバーリスクと脆弱性の検知、予防及び対応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、加盟国内でのSOC（セキュリティオペレーションセンター）インフラの形成が含まれます。[189] この枠組みは2024年10月17日に義務化されます。

EUサイバーレジリエンス法は、IoT機器を含むデジタル接続機器を対象としています。同法は2024年初めまでに施行される予定です。[190]

また、ISO 15118の一部および任意認証を「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実施しています。EU全域の著名なOEM及びEVCSオペレーターには受け入れられていますが、EUにおける本格的な導入については未定です。[191] [192]
関連規制は2024年から2025年の間に施行される予定で、同地域はすでにISO 15118の自主的な受け入れが始まっています。

英国

2021年12月に、スマートエネルギー搭載スマート家電（ESA）に対する英国規格協会（BSI）の規制対象にEVCSを含める提案がなされました。[193]

英国は EVCS 規制の最前線にあり、2021 年電気自動車 (スマート充電ポイント) 規制を導入しています。この規制は 2022 年 6 月に発効し、民間充電ポイント (家庭用または職場用) に適用されます。[194]

英国の規制では、「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」「電気供給者との相互運用性」「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計測システム」「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無作為化遅延」「コンプライアンス保証のためのコンプライアンス声明」「10年間の販売登録」などの要件を満たすことが求められています。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。[195] 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。

2022年2月に公表され、直近では2023年6月に更新されたEVCSの販売者および運営者向けのガイダンスレターでは、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が提案されています。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。[196]

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 月に 経済産業省（METI）から公表された「 IoT安心・安全フレームワーク 」[197] や 2019年6月の総務省（MIC) による「 IoT 5G 総合セキュリティ対策」[198] など、IoT 機器を対象とする規制に基づいています。

世界のEV充電標準規格

ISO 15118

ISO 15518は、充電中のEVと充電ステーション(EVSE/EVCS)間の暗号化された安全な通信を保証する世界的なサイバーセキュリティ規格であり(199)、複合充電システム(CCS)のセキュリティ規格として機能する高水準の通信プロトコルと考えられています。[200]

ISO 15118規格は、3つの基本的なステップを含む「プラグアンドチャージ」の運用を規定しています。

01

秘密保持
メッセージはTLSプロトコルで暗号化されます。

02

データの整合性
メッセージは、秘密キーと公開キーのペアを使用して、改ざんされないように保持されます。

03

信頼性
送受信されるメッセージは、楕円曲線デジタル署名アルゴリズム(ECDSA)を用いて保証されます。[201]

ISO 15118 は、ビークルツーグリッド (V2G) サイバーセキュリティの側面をカバーしており、充電プロセスに関与するすべてのエンティティに適用されます。

- EVs
- CPOs
- データ処理および保存を担うクラウドオペレーター
- 電力網(ユーティリティ・ビル管理システムとも呼ばれます)

コンボ充電システム (CCS)

世界各国の複数のOEMがサポートする、世界有数の充電プロトコルのひとつCCSのサイバーセキュリティ対策はISO 15118.202の対象です。[202]

DIN SPEC 70121

DIN SPEC 70121は、ISO 15118の前身となるドイツ版であり、ISO 15118の早期未発表版の理論的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の更新機能は含まれていません。

CHAdeMO(チャデモ)

日産、三菱、トヨタなどのOEMが開発した日本の規格(Charge de Moveの略)。CHAdeMOは2009年に初めて導入され、ISO 15118規格に代わる規格を提供することを目的としています。[203] ISO 15118と同様に、CHAdeMOはV2Gのセキュリティ面をカバーしています。充電プロセスは、IPv6セキュリティ対策と契約キーの暗号化とともに、ユーザーの車両識別番号（VIN）を照合することで可能になります。

CHAdeMOは2023年9月に「外部充電設計ガイドラインver.2.0.1」を公表し、CHAdeMO充電器/V2X機器、EV、プラグインハイブリッドEV（PHEV）に自動接続デバイス-アンダーボディ（ACD-U）充電システムを安全に統合または後付けするための技術的および運用的要件を追加しました。[204]

OCPP 2.0.1

オープンチャージアライアンスによって策定されたオープンチャージポイントプロトコル（OCPP）は、2013年に導入され、現在バージョン1.6から2.0.1に移行中です。OCPPは、EVCSおよびCSMS用の著名なオープンソースのセキュア通信規格です。この規格は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への注目すべき改善点には、デバイス管理の合理化とトランザクション処理の改善（マルチベンダーの充電ポイントを管理するオペレータ向け）機能、安全なアップデートや認証（安全なTLS暗号化を使用）によるセキュリティの強化、ISO 15118対応などが挙げられます。[205]

ISO 15118 は車両と充電ステーション間の通信を保護しますが、OCCP は充電ステーション自体とバックエンド サーバー間のセキュリティ面を扱います。OCCPにはCPO、電気通信、および電力管理が含まれます。[206]

避けられない車両データと プライバシー保護に関する法規制

コネクテッドカーは、OEMや規制当局が対処しなければならない独自のデータプライバシーとサイバーセキュリティの問題を提起しています。自動車から得られるデータの多くは個人データと考えられ、多くの消費者がデータ保護に関する法制化の必要性を感じています。[207] 世界中の規制当局が注目し、消費者中心の自動車データのプライバシーとセキュリティに関する基準を策定しています。

2023年9月、モジラ・ファウンデーションはプライバシーとセキュリティに関して主要なOEM25社を評価しましたが、全体的に芳しくない結果に終わりました。[208]

- 個人情報の過剰な収集
- 個人情報の共有または販売
- 個人情報に対する消費者の制御不可
- 政府および法執行機関との情報共有の意向
- 乏しいサイバーセキュリティの実績

現在米国では、データプライバシーを管理する規制当局である連邦取引委員会(FTC)と国家道路交通安全局（NHTSA）が業界の自主規制を提唱していますが[209]、各州で異なる取り組みがなされており、多くの州が全く着手していません。これまでのところ、コネクテッドカーに特化したデータプライバシー法を制定したのは全米でもほんの一握りの州だけですが、議会ではさらに数州が審議中です。加えて、各州は包括的なプライバシー保護法案を介してコネクテッドカーのデータを取り扱う選択ができます。カリフォルニア州消費者プライバシー法（CPRA）Prop24はその代表例です。[210] CPRAは、自動車メーカーや保険会社が消費者の許可なく正確な位置情報を利用することを禁止しています。

EUでは、規制当局がデータ及び人工知能に関する新たな規制枠組みを開発しており、自動車業界に大きな影響を与えています。[211]

2023年6月に合意されたEUデータ法では、データアクセス、ユーザーの権利、公正な契約条件、公共部門のデータアクセス、クラウドサービスプロバイダーの柔軟性に関する原則を定めています。これらの法整備は、進化するAIとデータ駆動型の自動車産業における規制とイノベーションのバランスを取ることを目的としています。[212]

「データ法」により、コネクテッドデバイスのユーザーが自身のデータにアクセスし、そのデータを第三者と共有してアフターマーケットやその他のデータ駆動型イノベーションサービスの提供が可能になることで、デジタル環境の公平性が確保され、競合するデータ市場を刺激し、データに基づいたイノベーションの機会が生まれます。[213]

2023年11月にEU理事会はデータ法を採択しました。[214] 広範な法制化であるにもかかわらず、車両データへのアクセスやデータ修正などの問題がある自動車業界を含め、分野別での法制化が進められています。

車両に人工知能（AI）を使用することは、特にソフトウェアのアップデートや車載データへのアクセスに関して、立法者の課題となっています。

2023 年 12 月、欧州の機関である 欧州委員会、理事会、議会は、AI に関する世界初の包括的な法律である新 AI 法について、暫定的な政治合意に達しました。これは、自動運転車に間接的に影響を与える広範な規制の枠組みを構築することを目的としています。

現在、草案の精緻化に向けた作業が進められており、2024年の初めには議会と理事会で正式に採択される予定です。[215] また、UNECE（国際連合欧州経済委員会）はAI関連ソフトウェアのアップデートに関するガイドラインを提案し、インパクトのあるアップデートに向けた承認機関の関与を推奨しています。

自動運転車やコネクテッドカーのデータとプライバシー法の制定は不可欠です。2024年から2025年にかけて、消費者のオプトインまたは最小限のオプトアウトの同意を必要とする新たな規制が、米国およびEU市場に導入されることが予想されます。規制が進化し続ける中、OEMは、相互の信頼、コンプライアンス、消費者保護を最大限に高めるために、自社のデータプライバシーとセキュリティポリシーについて戦略的な決定を行う必要があります。

05

ディープウェブと
ダークウェブからの脅威

サイバー脅威インテリジェンスは、
サイバーリスクの影響が拡大する中、
自動車およびスマートモビリティの
関係者に実用的かつ積極的な
リスク軽減策を提供します。

ディープウェブとダークウェブとは何なのか?

インターネットは、異なる機能や役割を持つ多層レイヤーからなり、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大きく分けて、クリア、ディープ、ダークの3つの層があります。それぞれのレイヤーにアクセスするには、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、サイト管理者に特定のトピックに精通していることを証明しなければなりません。

インターネットの第1層は、クリアウェブあるいは表面ウェブと呼ばれるもので、インターネットの最も小さく、かつ最も身近な部分で、アクセスに必要なのはウェブブラウザのみです。[216] この層のウェブは、誰もが知る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、一般の人々に信頼され毎日利用されています。

クリアウェブ

- *自動車とサイバー公共メディアの報道とニュース*
- *検証済みの研究者の公開ブログとレポート*
- *学術・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*
- *ファイル共有サイト*

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。[217] 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ません。理由は、サインインの背後（例えばペイウォール）にあるか、その所有者がウェブクローラーによるインデックス作成をブロックしているかのいずれかになります。一般の人にとってのディープウェブとは、有料コンテンツ、サブスクリプションサイト、非公開の私的なグループ、民間企業のウェブサイトなどが含まれます。ハッカーにとってのディープウェブには、匿名かつ挑発的で違法性の高いコンテンツを所有する画像掲示板などが挙げられます。

ディープウェブ

- *私的な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フォーラム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、悪質な行動や犯罪が行われ、盗用データが利用される非常に隠蔽性の高いウェブ層です。ダークウェブ・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）を使い、サイトのURLを知っていなければなりません（ダークウェブにはドメイン名がないため）。また、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すことも多くあります。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、ユーザー間における透明性の欠如していることやフォーラム内の情報の種類が故に、常に疑惑の目が向けられています。

ダークウェブ

- *悪質な貼り付けサイト*
- *違法なマーケットプレイス*
- *画像掲示板*
- *非公開ハッキングフォーラム*
- *違法な雇用サービス*
- *悪質なアクターが参加しう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Torブラウザとプロキシサーバを使用することがほとんどで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。この場合、攻撃者から送信されるパケットは複数のプロキシサーバーを経由します。プロキシサーバーは、競合国間においてセキュリティ情報（プロキシログなど）を共有できないように意図的に使用されているため、ハッカーの特定がより困難になっています。

2023年、UpstreamのAutoThreat®研究者がディープウェブおよびダークウェブ上で検知した脅威は、2022年に比較して156%増加しました。対象となった標的は、OEM、自動車Tier-1サプライヤーおよびTier-2サプライヤー、モビリティIoT デバイス、プラットフォームでした。

このデータは、2023年にディープウェブおよびダークウェブ上でのサイバー活動の約65%が、数千から数百万のモビリティ資産に影響を与える可能性があったという事実を示しています。[218] 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対し深層で接近し可視化することで、自らを積極的に守る必要があります。

2023年10月、UPSTREAMは、車載インフォテインメント（IVI）システムを違法にカスタマイズするための手順や方法が、

156%

ディープウェブの自動車フォーラムで公開されていることを発見しました。

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グレーハット

従来、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ある行為者を表し、ホワイトハットという用語は、防御強化に取り組むサイバーセキュリティの専門家を表します。しかしながら、自動車がインターネットに接続され、ソフトウェア中心のアプローチ転換が進んでいる自動車業界ではその区別は徐々に薄れつつあり、現在では「グレーハット」という存在が関与するようになりました。グレーハットはカスタマイズ目的で自動車を改造したりジェイルブレイクを行うような消費者が含まれます。

2023年10月、Upstreamは、車載インフォテインメント（IVI）システムを違法にカスタマイズするための手順や方法が、ディープウェブの自動車フォーラムで公開されていることを発見しました。フォーラムでは、ハッキングによる不正なサードパーティ製アプリケーションのインストール、隠し機能のロック解除、システムの安全制限を解除した運転中のビデオ視聴などが行なわれていました。IVIをジェイルブレイクし不正アプリケーションをインストールすると、消費者はサイバーセキュリティの脆弱性にさらされ、保証が無効になる可能性があります。信頼性の低いソフトウェアには、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るほか、システムの安定性に問題が発生し、クラッシュ、障害、非互換性を引き起こすこともあります。

ディープウェブとダークウェブで何が起こっているのか?

ディープウェブやダークウェブは、インターネットの96〜99%を占めていると推定されており、そのほとんどが非公開となっています。[219] 自動車に関連する幅広いコンテンツは、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、ユーザーがテキストやコードを貼り付けて共有するペーストサイトなどで見つけることができます。

多くの場合、消費者は、OEMが共有したがらない情報を見つけるためにウェブフォーラムを利用します。特に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は、自動車部品、コンポーネント、チップ、ソフトウェア、その他アイテムが、メーカーの規約や契約に違反して売買されていることで知られています。最先端の自動車技術に手を加えることの危険性を認識せずに、こうした行為に及ぶ自動車所有者は多くいます。

こうした行為は、保険会社だけではなく、自動車関係者にも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可能性があります。極端な場合、脅威アクターは、車両の認証にすでに使用されているデータをリバースエンジニアリングし、OEMや保険会社のサーバーに侵入することもできます。

ディープウェブとダークウェブに関する最も一般的な議論

出典: Upstream Security

自動車とモビリティの新たなIOT収益源へ損害をもたらす脅威アクター

脅威アクターらの、システムの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、データを利用したサービスに多大なリスクをもたらしています。

Upstreamは、38,000人以上のフォロワーを持つ、ソーシャルメディア上で人気の中東の脅威アクターを追跡しています。様々なOEMのIVIシステム向けにジェイルブレイクサービスやカスタムソフトウェアを公然と提供しており、その中にはApple CarPlay、Android Auto、診断サービス、ファームウェアのアップグレードなどの機能が含まれています。この脅威アクターによれば、従来の不正取引では利用できなかった独自の機能を提供しているとのことです。

> ***このことは、コネクテッドカーの不正改造、ファームウェアの更新、診断アクセスの安全確保に関連する課題が増大していることを浮き彫りにしています。また、既存のセキュリティー対策の有効性についても疑問を投げかけています。***

脅威アクターが特定のIVI、ECU、TCUに精通するにつれ、OEMとサプライチェーンは、ディープウェブやダークウェブの脅威の状況を可視化し、セキュリティプロトコルを強化して脅威から保護することが重要になります。

2023年9月、ある名の知られた東欧の脅威アクターが、ディープウェブの自動車フォーラムで、欧州の各種OEM向け診断ソフトウェアへの不正リモートアクセスサービスを販売し始めました。このようなソフトウェアへの不正アクセスサービスの提供は、OEMの利用規約に違反するものであり、また、OEM側においてはユーザーのプレミアム機能への評価確認が制限され、収益が失われる可能性があります。

別の例では、2023年10月、Upstreamはある南欧の脅威アクターを特定しました。このアクターは、ディープウェブフォーラムで、様々なOEMのIVIシステム全体に対して変更や制御を行える、ルートアクセスの売買を行なっていました。この脅威アクターは、ヘッドユニットのジェイルブレイクによって非公式なファイルや変更の受け取りができるようになるとし、また、ユーザーのフォルダ閲覧、アプリのインストール、運転中のビデオを再生、ナビゲーションシステムの改ざんさえ可能になると示唆しました。

フォーラム

ディープウェブやダークウェブには 、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、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、自動車ソフトウェアなどを扱う自動車関連のフォーラムがありますが、一般的なハッキングフォーラムにも自動車関連のハッキング情報が含まれています。

このようなフォーラムでは、情報、見識、ハッキング、不正なソフトウェア操作などが常に取引されています。ECUのチューニングは一般的な話題であり、インフォテインメントシステムのジェイルブレイク、ソースコード、データ侵害、車のハッキングツールやチュートリアルと共に話題となります。

修理費の節約、あるいは修理権の主張など、さまざまな理由から、車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。

2023年9月、UpstreamのAutoThreat® PROチームは、ディープウェブの人気自動車フォーラムで活動する、ある脅威アクターを発見しました。このアクターは、欧州OEMのIVIシステム向けにリモートのジェイルブレイクソリューションを販売していました。このジェイルブレイクはCANパッチで構成され、Android Auto、Androidスクリーンミラーリング、Apple CarPlay、ボイスコントロール、運転中のビデオ、ファームウェアとマップのアップデートなど、サブスクリプションベースのものを除くすべての機能を有効にします。

ディープウェブの自動車フォーラムの例

マーケットプレイス

ダークウェブマーケットプレイスは、TorやI2Pのような特殊なブラウザとアクセス登録が必要な商用ウェブサイトです。主に闇市場として機能しており、麻薬、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。[220]

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、自動車関連の「製品」やサービスを提供するものもあります。例えば、偽造文書やユーザー認証情報などの自動車アプリケーションやスマートモビリティサービス（OEMのコネクテッドカーサービス、シェアードモビリティサービスなど）に関するものです。

ディープウェブやダークウェブのマーケットプレイスには、自動車に関連する議論や商品が数多く存在しています。

- 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関連情報および認証情報の売買・公開
- キーシグナルグラバー、キーフォブプログラマー、GPS妨害装置、レーダー探知機など、車両の盗難・改造用ツールの情報及び売買
- カーシェアリングやライドシェア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

2023年10月、Upstreamはダークウェブのマーケットプレイスで、複数のOEMの顧客データベースを販売している脅威アクターを発見しました。

ダークウェブマーケットプレイスで売買されている顧客データベースの例

2023年には、Upstreamはダークウェブの人気マーケットプレイスで、グローバルOEMの従業員やディーラーのログイン情報を販売している脅威アクターも発見しています。

メッセージングアプリケーション

オンライン上でのやり取りがモバイルデバイスに移行するにつれ、モバイルメッセージングアプリケーションを利用した違法行為がますます増加しています。

Telegram、Discord、Signal、WhatsAppといった人気のメッセージングアプリケーションは、ハッキング方法の共有や、また、盗んだクレジットカード、アカウントのログイン情報、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頻繁に使用されています。

こうしたアプリケーションは、内密で誘導が難しいダークウェブのフォーラムに取って変わりました。

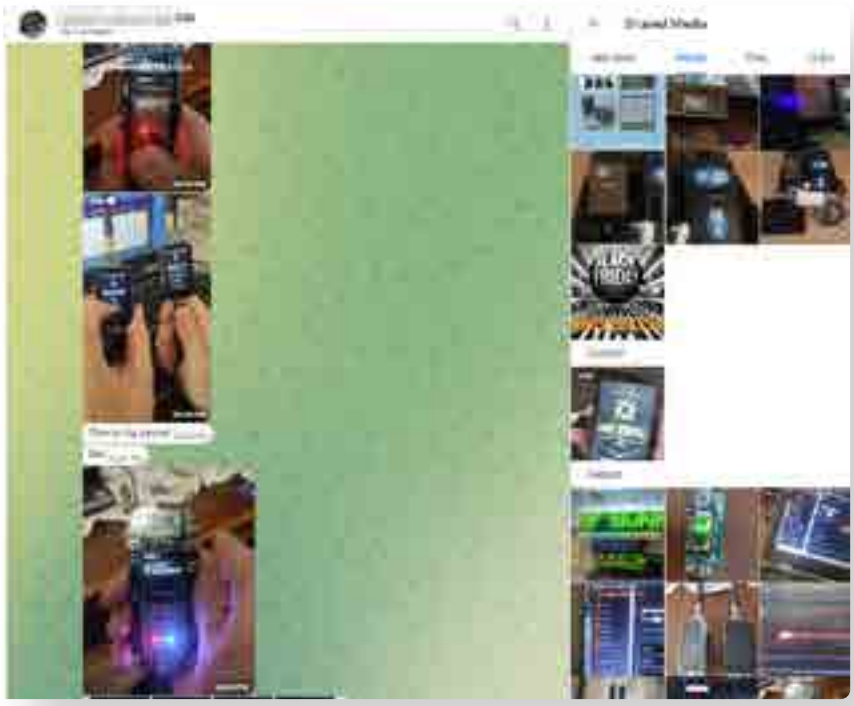
2023年6月、Upstreamはランサムウェアのチャンネルで、日本のOEMから重要な顧客PIIを含むデータが盗まれたことを示唆する投稿を発見しました。

盗難されたOEMデータに関するTelegramのメッセージの例

2023年8月、Upstreamは、多くの大手OEMに影響を与えるLinuxカーネルの不正に関する情報を発見しました。脆弱性はCVE-2023-3269で知られ、1万人のメンバーを擁するサイバー犯罪Telegramチャンネルで投稿されていました。

サイバー犯罪Telegramチャンネルで発見された不正

2023年12月、Upstreamは、人気のTelegramチャンネルで活動する東ヨーロッパの脅威アクターを追跡し、このアクターがリレーアタック・キーレスリピーターを売買していることを突き止めました。これは、複数のOEM車両のロックを解除し起動できるものです。売り手は非常に活動的かつ機敏であり、不正な車両アクセスツールの販売を長年にわたり続けています。



Telegramで売買されているリレーアタック・キーレスリピーター

ディープウェブとダークウェブにおける脅威アクター

セキュリティ研究者

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サイバーセキュリティの脆弱性を特定します。効果的なセキュリティのために、研究者は最新の攻撃手法、トレンド、新しい有効な技術について把握する必要があります。 多くのセキュリティ研究者は、脆弱性の悪用や車両ツールキットなどの調査結果を、GitHubのようなコードデータベースのホスティングサービスで公開しています。セキュリティ研究者が共有する知識は通常公開されており、悪意のある脅威者を含む誰もがアクセスできます。2023年1月、あるセキュリティ研究者が韓国のOEM車両モデルのヘッドユニットをハッキングしました。この研究者は、ヘッドユニットのファームウェアをリバースエンジニアリングすることで、ユニットをルート化し、機能の追加や削除を可能にしました。ファームウェアは、さまざまな車両モデルで使用されており、多くのヘッドユニットにリスクを及ぼします。[221]

2023年10月、あるセキュリティ研究者は、アメリカの電気自動車OEMの顧客が使用する、サードパーティ製のセルフホスト型データロガーでの設定ミスによるリスクを公開しました。[222] オープンソースインテリジェンス技術（OSINT）を使用して、この研究者は認証なしで設定されたデータロガーを見つけ、そのダッシュボードにアクセスすることができました。これにより、リアルタイムで位置の追跡、ドライバーが車内にいるかどうかの確認、車のオフライン化（スリープモードなど）、車のトランクが開いているかどうかの確認が可能になりました。研究者は、身体的な危害の可能性を含めた潜在的なリスクを強調し、車のオーナーが自分自身を守るための手順を説明しました。そして、この情報の開示と提案に対するOEMの反応について共有しました。

不正行為者

通常、不正行為者は、診断ツール、ソフトウェア、チップチューニングサービス、走行距離改ざんサービスなどの売買のためにディープウェブを利用します。

ディープウェブで非常に人気の高い不正サービスの一つに走行距離の改ざん、いわゆる走行距離計詐欺があります。これは、車の走行距離計の接続を外し、リセットあるいは改変して走行距離数を変更するというものです。

NHTSA（米国運輸省道路交通安全局）によると、毎年45万台以上の車両が虚偽の走行距離表示で販売され、アメリカの車購入者に10億ドル以上の損失をもたらしています。[223]

2023年9月、Upstreamは、走行距離ブロッカーと走行距離計プログラミングツール（走行距離の修正等に使用するものなど）を売買する脅威アクターを発見しました。これらは、西ヨーロッパのOEMが製造した特定の車両向けで、ディープウェブの自動車マーケットプレイスで売買されていました。

不正行為者のウェブサイト

ブラックハットハッカー

ブラックハットハッカーは、ディープウェブやダークウェブのさまざまなフォーラムやマーケットプレイスで活動しており、悪意を持ってサイバーセキュリティを侵害し、幅広い活動に関与しています。ブラックハットハッカーの中には、近距離のハッキングを専門とする者もおり、リモートエントリーシステムをハッキングして車を盗むなどします。一方で、遠距離のハッキングを専門とするブラックハッカーは、主に脆弱性を突いた不正行為を行います。

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、遠距離での脆弱性に対する不正プログラムを公開すると、他の多くの脅威アクターの不正行為を誘引することがあり、車両を衝突させたり制御したりなどの安全上の重大な危険を大規模に引き起こす可能性があります。

l2023年1月、Upstreamは、ブラックハットハッカーが複数のOEMに影響を及ぼすLinuxの脆弱性に対する不正プログラムを、サイバー犯罪フォーラムで公開していたことを発見しました。

このプログラムを不正に悪用すると、影響を受けた車両でサービスの利用拒否が引き起こされ、システムがクラッシュする可能性があります。さらには、この脆弱性を悪用し、攻撃者が対象車両にリモートでコマンドを実行することができます。

自動車愛好家

ディープウェブのさまざまな自動車フォーラムには、自動車愛好家、つまり車とその動作に情熱を注ぐ人々が大勢活動しています。

こうした自動車愛好家らは、アドバイスを求めたり質問をし合い、自分の車で見つけた問題やバグについて話し合ったりします。さらには自動車用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たりしています。

車好きがフォーラムに投稿する情報には、2つの問題点があります。第1の問題は、悪意のある脅威者がこうしたフォーラムに潜んでいることが多く、報告されたバグや問題を利用することです。第2の問題は、投稿されたファイルやリンクに信頼性がなく、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、被害が生じても保証対象にならない場合があります。

2023年6月、Upstreamは、主要OEMのIVIシステムのジェイルブレイクが、ドイツの自動車愛好家のブログでダウンロード可能となっていることを発見しました。ブログには、IVIシステムをハックキングするための詳細なガイドライン、手順、ビデオチュートリアルのほか、ジェイルブレイク後に可能な変更例が含まれていました。

自動車サプライヤーを標的にするランサムウェアアクターの増加

悪意あるアクターは、OEM、サプライヤー、さらにはEV充電のインフラなど、自動車およびモビリティのさまざまな関係者に、ランサムウェア攻撃を行う傾向がますます増えています。サプライチェーンのいかなる部分も、OEM、サービスプロバイダー、またはモビリティIoTデバイスにリスクをもたらす可能性があります。自動車サプライヤーは専門性が高いため、他のサプライヤーに切り替えようとしても非常にコストがかかり、簡単ではありません。

ランサム攻撃によって、サプライチェーン全体にわたる稼働率と生産性に深刻な影響を与える可能性があります。

攻撃者は、金銭を要求する目的でダークウェブ上に「リークサイト」を保持しています。そこでは、盗難したデータや組織の機密情報の公開、ターゲットになった被害者の情報を投稿しています。2023年、ランサムウェア攻撃やリークサイトの話題がたびたび注目を浴びました。そのいくつかを紹介します。

2023年6月、TIER-2に対する史上最大7000万ドルの身代金要求が発生しました。

2023年6月、台湾の大手半導体メーカーは、あるサイバーセキュリティインシデントについて公表しました。このインシデントは、ランサムウェアグループとITハードウェアサプライヤーの1社が関与したもので、サーバーの初期設定と構成に関する情報が漏洩しました。[224]
攻撃者は、機密情報を含む内部文書にアクセスしていると主張し、データを復号化し、オンラインでの公開を防ぐためには、7000万ドルの身代金が必要であるとしました。これは史上最大の身代金要求です。このデータ侵害は複数の自動車利害関係者に影響する可能性がありますが、同社は自身のビジネス運営や顧客情報には影響を受けなかったと報告しています。同社はこのインシデントの後、このプロバイダーとの情報共有を直ちに終了しました。

2023年8月、オランダのTier-1電磁石サプライヤーでは、ランサムウェアグループによるシステムへの不正アクセスによって、開発部門と販売部門が機能停止に陥りました。

これに対応するため、同社はサードパーティの有力なサイバーセキュリティ専門家を起用し、業務継続計画を含む対応手順を強化しました。[225]

同じく2023年8月、ドイツのOEMと提携しているタイのバッテリーメーカーが、ランサムウェア攻撃を受け、データが盗難されました。

ランサムウェアグループは、このメーカーのプロジェクトと情報についての5つの文書を盗難し、要求額が支払われなければ、それらを公開すると脅迫しました。[226]

ランサム攻撃は、車両、テレマティクスシステム、IoTデバイスに重大なリスクをもたらします。 2023年9月、アメリカの大手トラック運送および車両管理ソリューションプロバイダーがランサムウェア攻撃を受け、連邦規則で義務付けられている走行時間の電子記録や輸送在庫の追跡ができなくなりました。[227]

また9月には、英国最大の物流グループのひとつが、ランサムウェア攻撃を受けて破産を宣言しました。[228]

ディープウェブおよびダークウェブの活動増加で求められる、自動車・モビリティエコシステムの迅速な対応

ディープウェブおよびダークウェブでのデータ共有は、2023年に飛躍的に増加しました。自動車関連セキュリティの脆弱性、機密情報の漏洩、その他のサイバー脅威が定期的に公開され議論されています。 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領域で自動車関連の情報を大量に発見しました。こうした領域で活動する攻撃者の一歩先を行くには、リスクを定期的に監視し軽減することが必要です。そのためには、製品情報と自動車の専門知識が欠かせません。

業界関係者は、ディープウェブおよびダークウェブを監視し、セキュリティ体制に深刻なギャップが生じないようにしなくてはなりません。効果的なサイバーセキュリティ保護を実現するには、企業や製品が公式、非公式にかかわらず、どのように言及されているのかを把握することが重要です。 UNECE WP.29 R155規制とISO/SAE 21434規格、さらにNHTSAのガイドラインと中国の規制では、サイバー脅威インテリジェンスと脆弱性の監視が必要とされています。ディープウェブおよびダークウェブ は、これらの要件に不可欠な要素と考える必要があります。

企業が継続的にディープウェブやダークウェブを監視すると、検出の向上が図られます。また、脆弱性やセキュリティ侵害が発見された場合、その情報が広く世間に知られるまでの緩和時間を短縮することができます。また、企業は脆弱性の修正を行うソフトウェアパッチの導入や、関連する設定の変更といった予防措置も講じることができます。重要なのは、犯罪者が行う侵害されたデータのコピーおよび売買の機会を最小限にすること、また、不正の可能性を、自動車関係者、従業員、幹部役員、顧客に早い段階で警告することです。

> ***従来のIT脅威インテリジェンスでは、コネクテッドカーに関する専門知識が不足しており、OEM、Tier-1、Tier-2、他のモビリティ関係者に多くの課題が生じています。***

UpstreamのAuto Threat® PROソリューションは、このような課題を克服するために開発されたもので、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の収集、分析、公開を行います。このソリューションは、サプライチェーン全体を対象としており、さまざまな自動車のセグメントに向けて開発されています。OEM、Tier-1およびTier-2サプライヤー、モビリティIoT、コネクテッドカーのサービスプロバイダー、保険会社、その他のモビリティ関係者などを対象としています。

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の発見に努めています。これにより、Upstreamは、ディープウェブやダークウェブで脆弱性、不正、詐欺行為といった新たな脅威が広がる前の特定と軽減が可能です。

適切なサイバー脅威インテリジェンスを備えることで、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ます。

06

自動車サイバーセキュリティソリューション

増大するサイバーセキュリティの
脅威の影響と規模を効果的に
軽減するために必要なツールと
洞察をvSOCに提供

進化し続ける
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、自動車のサイバーセキュリティソリューションは進化しています。サイバー脅威が高度化、頻発化、大規模化する中、サイバーセキュリティソリューションは、膨大なモビリティ資産と絶えず変化するSBOMに対して、効果的かつ迅速な修復を提供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と車両セキュリティオペレーションセンター（vSOCs）は、車両への直接的な攻撃にとどまらず、企業が商用で保有する車両、コンパニオンアプリケーション、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する必要があります。

現代の車両の接続性の向上により、サイバー攻撃の規模と影響は飛躍的に拡大し、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、および運用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関係者、OEM、Tier-1およびTier-2は、新たな基準や規制が採用されるたびに、サイバーセキュリティに高い優先順位を置き続けます。コネクテッドカーやモビリティサービスを将来にわたって保護し続けるためには、多層的なサイバーセキュリティアプローチが不可欠です。

複雑なサプライチェーンとダイナミックなSBOMの中で、ライフサイクル全体にわたって車両を保護

乗用車の寿命は通常12年、商用トラックは20年、農業用車両は30年です。従って、OEMは、数十年前の技術で稼働する製品を確保するための長期的な戦略を策定する必要があります。

UNECE WP.29 R155とISO/SAE 21434は、車両のライフサイクルの開発、生産、生産後の各段階において、生涯続くサイバーセキュリティの脅威と脆弱性を考慮する要件を定めています。OEMとそのサプライヤーは、2022年に初めて規制と標準化の対象となりました。

2023年、OEMは引き続き2つの主要分野に注力しました。ひとつは、2024年の2番目のマイルストーンであるR155で予想されるモニター車両の範囲拡大に備えること、もうひとつはダイナミックなSBOMで複雑なサプライチェーンにまたがるコネクテッドカーを確保することでした。2023年は、OEMがTier-1およびTier-2サプライヤーに対してサイバーセキュリティの実践状況の開示を求めた2年目となり、サプライチェーンのボトルネックにとどまらない生産中断への懸念が緩和されました。

そうすることで、サイバーセキュリティの脆弱性をサードパーティベンダーから直接自社車両に持ち込むリスクを低減し、偽造部品が正規の施設に入り込み、耐摩耗性の低下や安全制限の無効化など安全性を脅かされるのを防ぐことができました。

R155では、OEMに対して、自動車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、維持することが求められています。また、Tier-1、Tier-2のサプライヤーとともに、将来の攻撃への対処と緩和のためのプロセスを構築する必要があります。

IISO/SAE21434は、サプライヤーとともにR155要求事項を実施する方法のガイダンスとして使用することができます。

01

サイバーレコードの能力

OEMは、サプライヤーのサイバー履歴をチェックし、サプライヤーがすべての関連部品について継続的なリスク管理と脆弱性管理を実施している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範疇を共有し、サイバーセキュリティインターフェイス契約（CIA）を用いて文書化されることで、責任範疇の共通認識を持ち、抜け漏れがないようにします。これは、RASIC（Responsible Approving Supporting Informed Consulting）などの確立されたプロジェクト管理手法を用いて行うことができます。

OEMとサプライヤー間で合意した方法のあるなしに関わらず、OEMはR155とR156を遵守し、ISO/SAE 21434の要件事項に従った方法を実施する責任を負うことになります。

設計上のセキュリティ

車両サイバーセキュリティに関するR155規則で明確に規定された対策には4つあり、その中の1つは、バリューチェーン全体のリスクを軽減するために「設計上」で車両の保護をすることです。

設計上のセキュリティは、開発フェーズの早い段階、コンポーネントや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。これは、すべての車両部品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、発見されたリスクが効果的に軽減されていることを確認することで実現されます。

自動車セキュリティの最終責任はOEMにありますが、サプライチェーンに関わるすべてのサプライヤーも同様に設計上のセキュリティ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

ITや企業のサイバーセキュリティにおいて、多層的なセキュリティはすでに標準なものとなっています。高度化する脅威や新たな脆弱性は絶えず出現しており、セキュリティの強化と複数のデータソースを活用した効果的な対策が求められています。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使用しています。

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) の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。[229] 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つのコア・セキュリティ要素に依存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出と応答

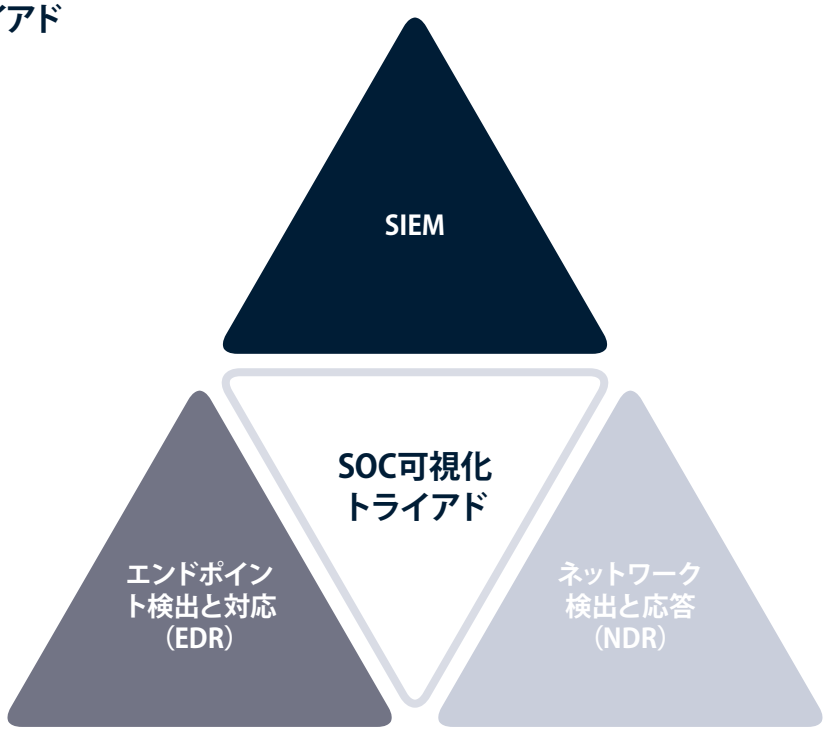
ネットワークトラフィックを監視し、検出された脅威とネットワークアクティビティを関連付けます。

03

エンドポイントの検出と対応

エンドポイント（サーバー、デスクトップ、ラップトップ）の操作をキャプチャし、攻撃の兆候を早期に特定します。

SOC可視化トライアド



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 [29]

自動車業界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の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では車両の検出と応答（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。

自動車クラウドセキュリティ

自動車クラウドを活用し、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とサイバー脅威への検知を拡大。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全体で把握し、複数の車両による攻撃を特定します。

車両セキュリティ

車両内部のコンポーネント（ECU、診断、DTCデータストリーム、OSログ、CANイベントなどを含む）の監視および保護をします。

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。これらの課題には、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。

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。

効果的なvSOCは、コネクテッドカーやスマートモビリティエコシステムのセキュリティに不可欠なものです。それにより、OEMはインフラ全体と車両をリアルタイムで監視し、検知された脅威に迅速に応答することができます。

一方で、スマートモビリティエコシステムの絶え間ない拡大とデジタルトランスフォーメーションに伴い、これまでより多くのステークホルダーがvSOCを必要とすると予想されています。モビリティIoTベンダー、フリートシステム、その他のスマートモビリティサービスプロバイダーは、vSOCによる資産の監視と保護に移行するでしょう。

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、憲章を含んで、明確に定義付けた戦略と範囲も示します。

効果的なvSOCはまた、次のようなものでなければなりません。

- 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
- 自動車に特化したサイバーセキュリティ分析により、脅威や異常をほぼリアルタイムで検出
- アラートのトリアージと調査
- 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
- ガバナンスの概要と運営方針、基準、手順、プロセスの指針
- エンドツーエンド（E2E）のプレイブックの構築・導入し、応答活動を構造化・自動化
- 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

vSOCは次の3つの方法で構築できます。

01 自社編成

既存のエンタープライズSOCをモビリティ資産に拡張するには、OTの専門知識、特定のプラットフォームの導入、運用手順の変更が必要になります。

02 新規設立

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、プレイブックを構築します。

03 他社外注

vSOCは、ITと自動車関連の両方のサイバーセキュリティ能力を持つマネージド・セキュリティ・サービス・プロバイダー（MSSP）に外注することが可能です。

vSOCが効果的なリスク低減とサイバー対策に不可欠であると理解した多くのOEMは、2023年中も、vSOCの導入に注力し続けました。規制対象となる監視車両の範囲は、2024年7月、2番目のマイルストーンであるR155に伴い大幅に拡大すると予想されます。OEMは、vSOCチーム、プラットフォーム、プロセスを適切に調整する必要があります。

次世代のvSOC

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ではvSOCのスコープの定義づけを行なっており、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）と運用モデル（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。

Fusion vSOC

コネクテッド・ビークル・オペレーション・センターの一部であり、vSOCの基本機能と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部門横断型なアプローチを含みます。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駆動型サービスとアプリケーションの保護のため、IT SOCと緊密に連携することが必要です。これは、複雑な攻撃ベクトルを検知し効果的に軽減するために重要です。

IT-OT vSOC

IT SOCとvSOCを統合し、広範なセキュリティ運用センターを管理します。設計から製造（車両製造の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ています。

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へのアクセスが必要となり、劇的に移行していくと考えています。

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。

自動車に特化した脅威インテリジェンスでリスクに対するプロアクティブなアプローチを提供

多層的なアプローチには、サイバー脅威インテリジェンスの監視など、脅威検知能力を強化するためにプロアクティブな要素も必要です。

OEMやモビリティのステークホルダーは、コンプライアンスを遵守しながら、自社製品の脆弱性を積極的に特定し低減する必要があります。業界に特化した専用の脅威フィードを使用することで、ステークホルダーは、サーフェイスウェブ、ディープウェブ、ダークウェブのそれぞれの調査結果に基づく新たな脅威を継続的に更新し続けることができます。

コネクテッドカーのエコシステムが複雑化し、大規模なサイバーリスクが発生する中、自動車に特化した脅威インテリジェンス製品の重要性は高まっています。サイバーセキュリティの脆弱性やサイバー攻撃は、サプライチェーン全体に影響を及ぼし信頼と安全を脅かします。すべてのステークホルダーは、リスク分析、脅威モニタリング、サイバー攻撃への効果的な対応に積極的に取り組む必要があります。

OEMsにとってのメリット

- モビリティ資産に対するサイバー脅威の早期検出
- 綿密な脅威インテリジェンスを必要とする自動車規格や規制に対応
- 脅威、脆弱性、ハッキングが公になる前に風評リスクを管理
- 保証違反やポリシー違反を早期に発見し、将来の保証問題を回避
- サイバー脅威に対する意識向上によって顧客との信頼関係を構築
- 自動車サプライチェーンに対する直接的な脅威への監視と管理
- 現在の脅威の状況を評価し、同業他社や競合他社に対するベンチマークを実施s

Tier-1、Tier-2サプライヤーのメリット

- より詳細なコンポーネントの脅威監視によりOEMの信頼を獲得
- 保証違反やポリシー違反を早期発見し、将来の保証コストを削減
- 有名なコンポーネントハッキングフォーラムやチャットを監視することにより、コンポーネントの脆弱性を特定し修正
- 脅威フィードを監視し、脆弱性を軽減することで規制要求に対応

CISOsにとってのメリット

- 組織データや個人情報の漏えいを監視し、組織を危険にさらす可能性のある潜在的な侵害を検出
- ITおよびOTのセキュリティを向上させ、クラウドサービスや企業ネットワークに適切なサイバーセキュリティ対策を導入するための手順を開発
- 他組織に対する攻撃を監視・分析し、自社の資産やアプリケーションに対する同様の脅威への防御方法を開発s
- サイバー脅威の状況についてよりよく理解し、サイバーリスクの効果的な評価、アクションの優先順位付け、リソースのより効率的な割り当てが可能
- 企業ネットワークへのアクセス方法を販売するダークウェブ上のアクターの発見
- 組織内の脅威を発見
- 製品の部品表などの知的財産の流出を監視

VSOC アナリストにとってのメリット

- フォーラム上でのチャットのやり取りを監視し、新たな脅威をいち早く検知
- 新たな不正の手口、トレンド、脅威アクターを特定
- 一般的な海賊版の特徴や違法修正の認識と監視
- 自動車の顧客の個人情報に関わるデータ侵害の検知、警告、および対応策の提示
- 組織のネットワーク、リソース、ビジネスを混乱させる新たな脅威の発見
- アンダーグラウンドマーケットで売買される新たな脆弱性や不正サービスを常に把握
- 車両関連のソフトウェアセキュリティを監視し、必要なOTAアップデートを発行
- 侵害されたアカウントの無効化と所有者への通知により、将来のコネクテッドカーへのサイバー攻撃を未然に防止
- 自動車関連のゼロデイ脆弱性とエクスプロイトキットの追跡

保険エコシステムへのメリット

- 自動車への不正侵害やハッキングの主な原因、場所、方法を特定することで、保険数理士の実質的なリスク測定と保険コストの評価が可能
- コネクテッドカーに設置されたドライブレコーダー操作など一般的な保険詐欺の手口を検出
- 走行距離計操作などの保証違反や保険契約違反の特定と防止
- ローカル市場と資産サブセットの地理的なリスク領域を理解s

スマートモビリティアプリケーションやサービスに対するメリット

- 成りすまし犯罪に関する不正の特定
- 不正なカーシェアリングや配車サービスの利用売買およびドライバーのアカウント売買を検出
- カーシェアリングや配車サービスの利用者データおよびレンタルの利用者データを販売する悪質な業者の発見
- ハッキングフォーラム上での共有されたモビリティ資産の窃盗や不正行為の方法を監視

脅威アクターはテレマティクスやその他のコネクテッドカーのデータを標的とするようになってきています。なぜならOEMが自動車のコネクティビティ強化に努めているためです。自動車の構造や仕組みを熟知した、Threat Intelligence製品だけが、車両の背景を理解して異常を迅速に特定し、サイバーセキュリティ対策チームの感度を鈍らせる可能性のある誤報アラームを排除できます。製品のサイバーセキュリティ担当役員やCISOは、拡大する自動車ハッキングの脅威に対して、組織のニーズに合った独自のアプローチで対処することが求められています。

OEMやスマートモビリティアプリケーションで求められるフュージョン検出の拡張ーOWASP TOP10の範囲以上の補償

現実の問題として、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、技術的な専門知識は少なくて済み、特別なハードウェアがなくてもリモートで行うことができるため、他のシステムに比べて費用対効果が高くなります。

Open Web Application Security Project（OWASP）におけるAPI Security Top 10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。（参照230）

2023年に更新されたトップ10のリストには以下のものが含まれています。

01 **オブジェクトレベルの認可の不備**

02 **認証の不備**

03 **破損したオブジェクトのプロパティレベルの許可**

04 **破損したオブジェクトのプロパティレベルの許可**

05 **機能レベルの認可の不備**

06 **機密性の高いビジネスフローへの無制限のアクセス**

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 **安全でないAPIの消費**

更新されたOWASPのAPI Top10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ベースの攻撃の影響は、サービスの中断、車両とドライバーの安全性、データ漏洩、プライバシー、サブスクリプションや機能制限の回避を目的とした不正行為、さらにはブランドの評判にまで及びます。

しかし、自動車やスマートモビリティのエコシステムの背景においては、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、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、道路上での物理的動作、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データソースも考慮する必要があります。このような2つの情報源の組み合わせによって、組織は潜在的な脅威と脆弱性をより深く理解することができます。

APIセキュリティには全体的な視点が必要です。運用データとAPIトラフィックの状況から車両、アプリケーション、消費者の状態を反映します。様々なデータソースをAPIトラフィックやドキュメントと並行して活用することで、運用システムに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、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
- 課金とログイン履歴
- 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と検出に関する責任を見きわめています。このようなリスクはエンタープライズSOCやvSOC、あるいは新たなIT-OT SOCで分析可能です。

UPSTREAMの自動車サイバーセキュリティへのクラウドアプローチ

Upstreamは、コネクテッドカー向けに構築されたクラウドベースのサイバーセキュリティおよびデータ管理プラットフォームを提供し、他社にはない自動車サイバーセキュリティの検出と対応、データ駆動型アプリケーションを実現します。

Upstreamのエージェントレスソリューションは、モビリティIoTデバイス、アプリケーション、コネクテッドカーの迅速な保護が可能です。また、フリート全体の分析および巧妙な異常や攻撃を検知する総合的なアプローチを提供します。

Upstream Platformは、車両データの価値を引き出し、高度に分散した車両データを集中化、構造化、コンテキスト化されたデータレイクに変換することで、お客様のコネクテッドカーとモビリティアプリケーションの構築を支援します。CUpstreamは、モビリティサイバーセキュリティにおける最初の脅威インテリジェンスソリューションであるAutoThreat ® PROと組み合わせることによって、業界をリードするサイバー脅威プロテクションおよび実用的なインサイトを提供し、お客様の環境やvSOCにシームレスに統合します。

攻撃対象が拡大し、ハッカーたちがコネクテッドビークルを制御するための複雑な手法を開発する中、Upstream PlatformとAutoThreat® PROの強力な組み合わせは、自動車産業のサイバーセキュリティ対策に不可欠なものとなっています。

AutoThreat®チームが収集・分析したデータは、現場で見られる脆弱性や欠陥に対する検出器や解決策を生み出すために継続的に利用されています。

これによりUpstreamは、まだ業界に知られていない将来の脅威を先取りすることができるのです。

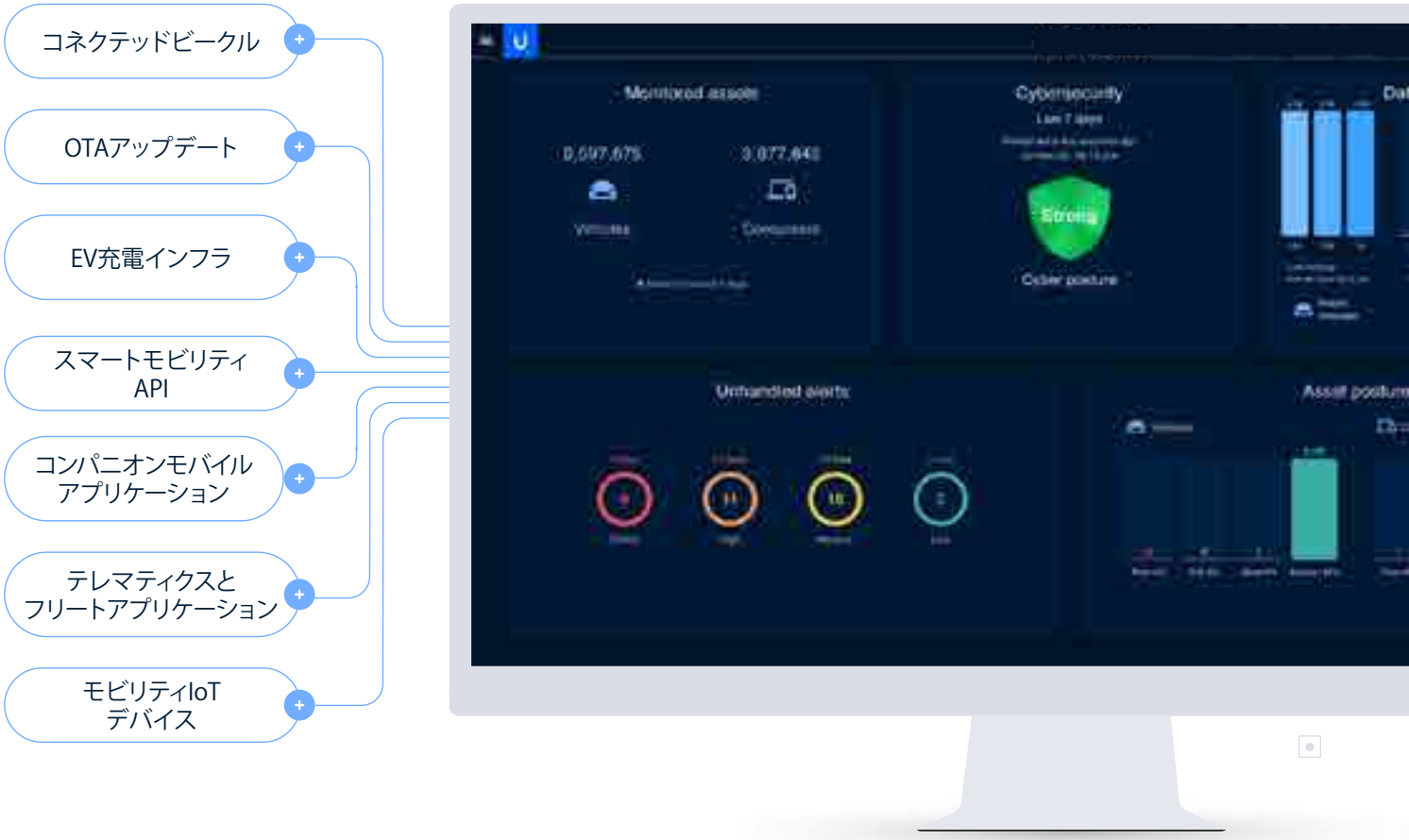
UPSTREAMプラットフォーム

2017年、Upstreamは、コネクテッドビークルのエコシステムを保護する抜本的かつ革新的な方向性を示しました。それは、コネクテッドビークルとスマートモビリティのために構築された初のクラウドベースのサイバーセキュリティおよびデータ管理プラットフォームによって、もたらされました。

Upstream Platformは、堅牢なサイバーセキュリティ検出・対応プラットフォーム（V-XDR）へと大きく進化しました。このプラットフォームは、高度な機械学習モデルや効果的な調査のための生成AIレイヤーを備え、数百の検出器によって幅広いスマートモビリティステークホルダーのためのサイバーセキュリティおよびモビリティに関する事例に対応します。

現在、Upstream Platformは世界中で何百万台の車両を監視し、検出・対応活動を支援するとともに、世界最大級のOEMやモビリティプレーヤーのvSOCをサポートしています。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の充電インフラとモビリティIoTにも範囲を広げています。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変革の中核をなすものです。

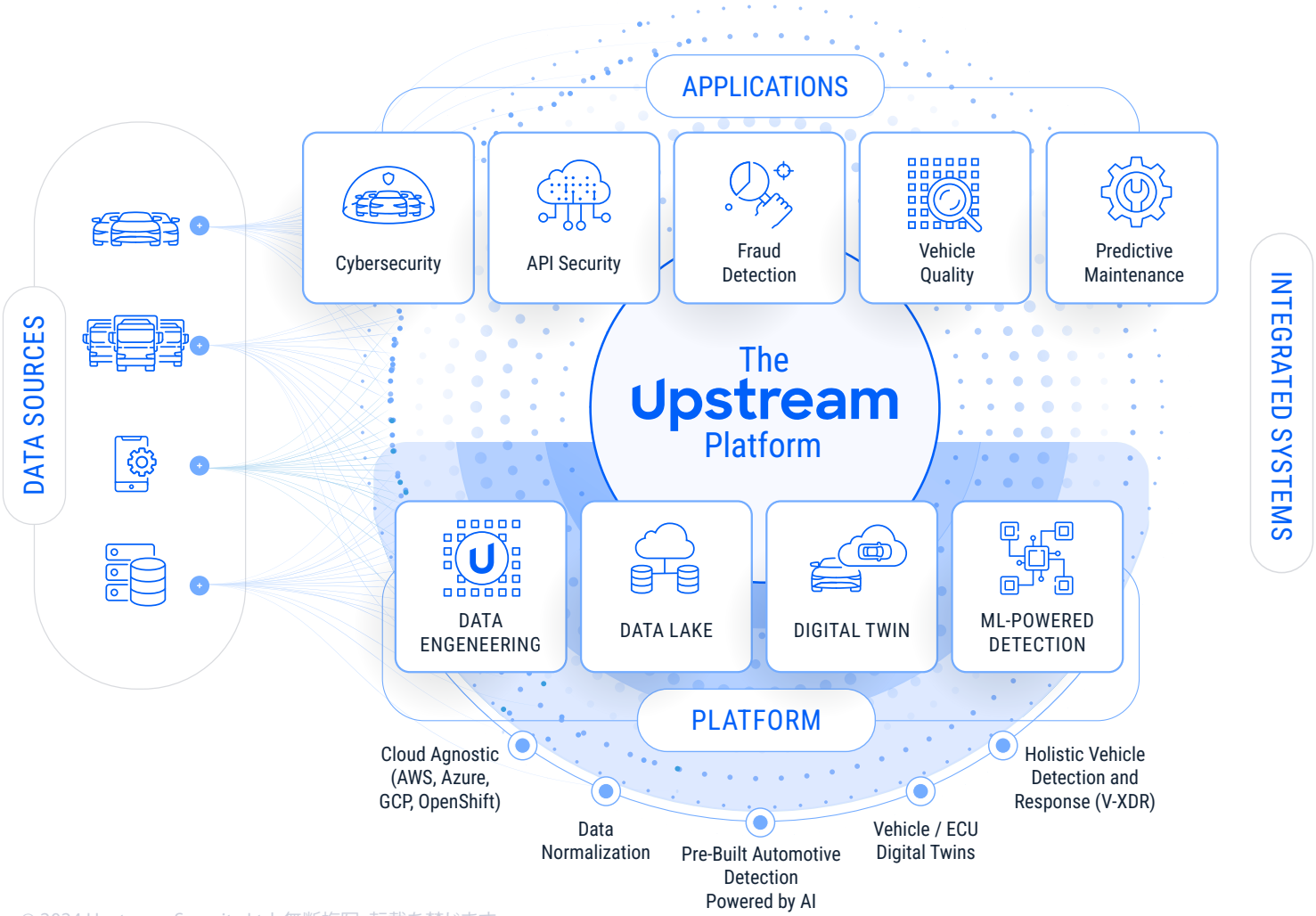
Upstreamは、スマートモビリティのエコシステム全体でサイバーセキュリティの脅威を検出する、即時導入可能なソリューションを提供しています。（下図参照）



Upstreamは、多数のデータストリームを処理し、高度なデータ分析やMLアプリケーションを開発できます。それにより、OEMはサイバーセキュリティのみならず、不正検知、予測分析、車両品質、保険、その他のデータ駆動型の事例にもUpstreamが活用できます。

今般Upstreamのプラットフォームが拡張され、幅広い事例に活用できるようになりました。

サイバーセキュリティ	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・検知
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、継続的な運用可用性確保とデータ保護を実現.
不正検知	走行距離計の巻き戻し、車両盗難など、不正に関連するシナリオを特定.
車両品質	コネクテッドカーの品質を監視し、リコールやメンテナンスコストを削減.
予知保全	重要な機器の劣化を予測することで、運用可用性と安全性を確保しメンテナンスコストを削減.



進化するスマートモビリティのサイバーリスクに対応する検出と応答の拡大

スマートモビリティAPIのセキュリティ

APIベースのサイバー攻撃や脆弱性が急増する中、スマートモビリティのステークホルダーは現在、毎月何十億もの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セキュリティソリューションは、APIトランザクションと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ます。それにより、コンシューマー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対し、コンテキストに基づいた包括的なビューを提供します。

UpstreamのAPIセキュリティソリューションによって、モビリティステークホルダーは以下のようなメリットが得られます。

APIディスカバリー

リアルタイムのトラフィックデータを持つ全ドキュメントを完全にカタログ化します。ドキュメント化された、もしくはされていないAPIや、推奨されていないAPIなど、サードパーティや内部サービスで使用されているAPIも含みます。

APIモニタリング

継続的に、静的および動的なトラフィックソース検出によるコンフォーマンス分析を実施します。更新によって導入されたAPIランドスケープの潜在的な脆弱性を特定します。

フュージョン検出

高度なAI/MLモデルを適用し、複雑で低速な攻撃を含む未知の脅威・攻撃を効果的に検出します。

ノーコード検出器の構築

簡単に検出器をカスタマイズし、新しい検出機能の追加が可能です。コーディングや開発リソースなしで新しい事例やビジネスロジックに対応します。

vSOCのアナリストは、ほぼリアルタイムでAPIのサイバー脅威を監視および検出します。そして、脅威を効果的に低減するための必要な情報を見つけ、運用を中断することなく、アラートに応答したワークフローを駆動できます。

車載セキュリティデータストリームの統合

Upstreamでは、車載セキュリティインシデントを検出するためのデータ収集プログラムが組み込まれており、侵入検知防御システム（IDPS）が作動してアラートが表示されるようになっています。アラートは、車載用サイバーセキュリティソリューションの多くにみられる誤検知を軽減するように設計されています。Upstreamは、IDPSのデータフローを他のコネクテッドカーのデータソースと組み合わせ、vSOCアナリストに追加情報を提供し、問題を迅速に解決できるようにします。

車載データソース統合には、侵入検知システムマネージャー（IDSM）、各種セキュアロガー、セントラルゲートウェイとテレマティクスコントロールユニット（TCU）の両方をサポートするIDPSデータソースなどがあります。

脅威ハンティング機能搭載

UpstreamのAutoThreat® PROと密接に連携することで、vSOCチームは脅威ハンティングを活用し、コネクテッドカーの過去のデータと事例を調査します。それにより、アナリストによる異常パターンや潜在的な悪質行動の特定が可能となっています。

Upstreamが提供するvSOCサービス

Upstream Platformを活用し、Upstream独自のManaged vSOCサービスを提供します。このサービスは、単一のECUから個々の車両やデバイス、そしてフリート全体の視点に至るまで、深く高度な検出、調査、軽減機能を提供します。このような全方位的な視点を持つことで、OEMやスマートモビリティベンダーは、既知および未知のサイバーセキュリティの脅威を軽減することができ、車両、アプリケーション、サービス、充電インフラ、IoTデバイス、フリート全体にわたる脅威に対応できます。

Upstream Managed vSOCサービスは、Upstreamの堅牢なテクノロジースタックとAutoThreat® PROを活用し、最大限の効果をもたらします。世界中で何百万台もの車両をモニタリングしてきた豊富な経験と実証された方法をもとに、Upstreamは最小限の導入時間でターンキーソリューションを提供します。Upstream Managed vSOCサービスは、OEMの既存プロセスやワークフローとシームレスに統合し、カスタムメイドのプレイブックを提供します。さらに、このサービスはグローバルMSSPパートナー各社と連携し、世界中の車両、デバイス、アプリケーションを保護しています。

サイバーセキュリティ、モビリティとIoTプロトコル、規制とコンプライアンス、不正、そして運用に深い専門知識を持つ経験豊富なアナリストや研究者チームが、自動車エコシステムに関する独自の視点を提供し、多角的なvSOCを実現しています。

Upstreamを利用することで、OEMとモビリティ関係者は、脅威の検知と対応に定評のある手法を適用した完全運用型のvSOCサービスを活用でき、必要に応じて運用範囲を地理的に拡大し、スケールアップすることが可能です。

OEMは実績のあるBOT（Build-Operate-Transfer）モデルを活用することで、柔軟性を高め、ロックインを回避することができます。UpstreamのvSOCサービスには、OEMチームへの導入モデルや方法論、プレイブックのトレーニングが含まれるため、必要に応じてスムーズな引継ぎが可能です。

OEMは実績のあるBOT（Build-Operate-Transfer）モデルを活用することで、柔軟性を高め、ロックインを回避することができます。

UpstreamのvSOCサービスには、OEMチームへの導入モデルや方法論、プレイブックのトレーニングが含まれるため、必要に応じてスムーズな引継ぎが可能です。

UpstreamのvSOC

UpstreamのvSOC

2023年には、Upstreamは以下にご紹介する複数の主要領域において、vSOCの可視性を拡張し、検知と調査の性能を高めました。また、多数の車載データストリームをUpstreamプラットフォームに直接統合し、エンドポイント管理に近い機能を提供しました。

応答面では、Upstreamはプレイブックや横断的なコラボレーションなどの文書化を含むエンドツーエンドの応答プロセスを構築することで、システムの能力拡大に注力してきました。2023年、UpstreamのvSOCは、SIEMやSOARパートナーとの連携を強化することで、組織全体の可視性を高め、シフトレフトを効果的に実行し、横断的な影響力を高めました。

生成AIを活用したVSOC調査の強化

2023年、Upstreamは高度な生成AIを搭載したクエリレイヤーをUpstreamV-XDRプラットフォームに導入しました。これらの新機能により、vSOCチームは「枠にとらわれない」思考が可能となるほか、複数のソースから大量のデータを効果的に分析し、パターンを検出することが可能となります。また、インシデントアラートをフィルタリングし、調査を自動化することも可能です。

大規模なリスクへの対応が課題となっている今日のvSOCにおいて、生成AIは自然言語処理（NLP）により簡単な質問でデータの照会ができるため、インサイトを引き出すのに役立ちます。

生成AIはvSOCの調査と運用を変革し、以下のようなさまざまなユースケースを実現します。

データ分析

特定期間における週間サイバーセキュリティアラート数など、関連する履歴データを特定・分析し、パターンや異常を自動で特定する。

アラートフィルタリング

アラートの重大度を追跡し、深刻度の高いアラートの傾向や突発的なスパイクを特定する。これは、セキュリティ対応の優先順位をつけるのに重要である。

アラート分析

不正なOTAソフトウェアアップデートに関するアラートなど、特定の種類のアラートについて徹底的に見抜き、セキュリティリスクを把握する。

調査と自動化

会話型チャットを使用し、調査の改善とvSOC ワークフローの自動化を行い、時間とリソースを節約する。

強化されたTARA

ディープウェブとダークウェブのデータ、徹底した脅威分析とリスク評価（TARA）に基づき、多角的なインサイトを生成する。

UPSTREAM AUTOTHREAT® PRO CYBER THREAT INTELLIGENCE

UpstreamのAutoThreat® PROは、自動車とスマートモビリティエコシステムに特化した、世界初で唯一のCyberThreat Intelligence(CTI)ソリューションです。カスタマイズされたCTI、ディープウェブ、ダークウェブの調査を提供し、クライアント専用の資産（SBOMなど）、自動車およびモビリティのサイバー攻撃者、自動車特有のサイバーリスクを分析します。UpstreamのCTIは、自動車やモビリティのサイバー脅威エコシステムにおける脆弱性、悪用、不正行為、偽造品を特定するために、特別設計されています。

Upstreamは自動車のCTIにおいて独自の視点を持ち、サイバーセキュリティパズルの未知の部分を明らかにすることに重点を置いています。モビリティ関係者は、単一のECUから完全な車両モデルやコネクテッドデバイスに至るまで、製品やコンポーネントを分析することで、脆弱性管理、脅威認識、製品インテリジェンスを強化し、規制の順守を確保できます。

UpstreamのAutoThreat®チームには、自動車やモビリティに関する深い専門知識に加え、製品への豊富な経験を持つサイバーセキュリティ研究者やアナリストが所属しています。このサービスは、CTIディープウェブとダークウェブの調査レポートを定期的かつ緊急時に発行し、カスタマイズされたクエリも含まれています。また、AutoThreat® PROは、使いやすいオンラインプラットフォームを提供し、クリアウェブのサイバーインシデントポータルへのアクセス、Upstreamの自動CVEフィードによる脆弱性管理、自動車サイバー攻撃者専用のリポジトリを提供します。

07

2024年の予測

生成AIのような新技術に加え、
APIやIoTデバイスへの依存が
高まることによって、
新たなチャンスがもたらされる
一方、課題も生じて来るでしょう。

2024年に向けて、当社の主な予想は以下の通りです。

01 自動車のDXは、大規模な攻撃の標的を継続的に導く

競争の優位性を確保するために、モビリティ・アプリケーション、車載サブスクリプション、データ駆動型サービスなどの迅速な導入を始めとして、自動車業界のDXが継続されていくでしょう。車両がさらにソフトウェア重視になり、重要な車両機能へのリモートアクセスが可能になるにつれて、APIの安全確保とAPI関連の脅威を監視する車両セキュリティセンターの適用範囲の拡大に注意を向けなければなりません。

02 生成AIは諸刃の剣

生成AIを使って新たな大規模攻撃手法を導入することで、自動車やスマートモビリティの関係者に深刻な影響を与えるでしょう。生成AIは脅威アクターにとって重要なツールになると予想され、脆弱性を素早く特定し、それを悪用する方法を学習し、戦術、方法、作業手順を標準化し、いわば艦隊規模の攻撃を実行できます。

一方で、生成AIは関係者に自動車のサイバーセキュリティを変革する能力を提供し、迅速な調査に基づく車両セキュリティセンターの作業手順の自動化、さらにはディープウェブやダークウェブのデータ、綿密なTARAに基づく複雑な洞察まで、さまざまな場面で活用できます。

03 自動車のサイバーセキュリティ規制は圧倒的に複雑化

コンプライアンスの期限が迫り、新しい基準が次々と導入される中、自動車業界は疲弊し始めています。UNECE WP.29 R155の第２の節目（マイルストーン）が間近に迫る中、二輪車や三輪車、農業用車両に関する新規制、中国やその他の国における新規制の可能性など、関係者は極めて複雑な規制変更の状況に直面しています。

04 電気自動車の急速な普及がサイバーリスクを拡大し、新たな規制を促進

OEMと電気自動車充電スタンド事業者（CPO）は、サイバーセキュリティのリスクアセスメントをさらに深化させ、IoTプロトコル、標準、規制にも対応できるようにプロセスを拡大しています。また、戦略的な電気自動車充電インフラを保護するための専用の解決策を評価・採用することも極めて重要です。米国と英国で、電気自動車充電設備（EVSE）に関する新たな規制が制定されました。中国でも、EVSE、AVおよび自動車の情報セキュリティに関する規制を制定しています。

REFERENCES

1. https://upstream.auto/research/automotive-cybersecurity/
2. https://upstream.auto/autothreat-intelligence/
3. Upstream Security
4. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
5. https://samcurry.net/web-hackers-vs-the-auto-industry/
6. https://therecord.media/orbcomm-trucking-software-ransomware, https://www.bleepingcomputer.com/news/security/orbcomm-ransomware-attack-causes-trucking-fleet-management-outage/ , https://www.marketscreener.com/quote/stock/HAYNES-INTERNATIONAL-INC-46351/news/Haynes-International-Inc-Begins-Network-Outlet-of-Cybersecurity-Incident-44109194/
7. https://www.bleepingcomputer.com/news/security/orbcomm-ransomware-attack-causes-trucking-fleet-management-outage/
8. Upstream Security
9. Upstream Security
10. https://voonze.com/tsmc-supplier-suffers-ransomware-attack-and-has-data-leaked-by-hacker-group/ , https://finance.yahoo.com/news/chipmaker-tsmc-confirms-data-leak-151811628.html
11. https://www.cyberdaily.au/security/9879-lockbit-ransomware-gang-claims-hack-on-queensland-based-q-automotive-group
12. https://techcrunch.com/2023/03/28/hackers-could-remotely-turn-off-lights-honk-mess-with-teslas-infotainment-system/, https://insideevs.com/news/659185/tesla-model-3-compromised-in-under-two-minutes-at-hacking-contest/
13. https://www.auroralabs.com/ota-ccg-lp-1/
14. https://www.reuters.com/legal/tesla-owners-sue-over-impact-software-update-ev-batteries-2023-05-12/
15. https://www.reuters.com/legal/tesla-owners-sue-over-impact-software-update-ev-batteries-2023-05-12/
16. https://techcrunch.com/2023/06/09/shell-recharge-security-lapse-exposed-drivers-data/
17. https://www.ibm.com/reports/data-breach
18. https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/numbers-and-figures
19. https://www.bcg.com/publications/2023/rewriting-rules-of-software-defined-vehicles
20. https://unece.org/sites/default/files/2021-03/R155e.pdf
21. https://unece.org/sites/default/files/2021-03/R156e.pdf
22. https://www.iso.org/standard/70918.html
23. https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf
24. https://www.asiafinancial.com/china-plans-rules-to-regulate-data-flows-from-smart-cars
25. https://eaton-works.com/2023/03/06/toyota-c360-hack/
26. https://www.latestly.com/socially/world/bykea-app-hacked-pakistans-ride-hailing-application-gets-hacked-users-receive-abusive-messages-see-pics-5197926.html
27. https://www.thedrive.com/news/43454/why-milwaukee-might-sue-hyundai-kia-over-stolen-car-epidemic
28. https://urbanmilwaukee.com/2022/08/17/kia-hyundai-thefts-now-national-problem/
29. https://edition.cnn.com/2023/01/27/business/progressive-state-farm-hyundai-kia/index.html
30. https://www.nhtsa.gov/press-releases/hyundai-kia-campaign-prevent-vehicle-theft
31. https://www.techradar.com/news/hyundai-and-kia-cars-could-be-stolen-with-just-a-usb-cable, https://www.malwarebytes.com/blog/news/2023/02/tiktok-car-theft-challenge-hyundai-kia-fix-flaw
32. https://hackingtoolscar.pl/shop/
33. https://www.tiktok.com/@keyless_go
34. https://www.mckinsey.com/features/mckinsey-center-for-future-mobility/our-insights/drivers-of-disruption/gen-ai-in-high-gear-mercedes-benz-leverages-the-power-of-chatgpt
35. https://www.bain.com/insights/generative-ai-and-cybersecurity-strengthening-both-defenses-and-threats-tech-report-2023
36. https://www.gartner.com/en/newsroom/press-releases/2023-10-11-gartner-says-more-than-80-percent-of-enterprises-will-have-used-generative-ai-apis-or-deployed-generative-ai-enabled-applications-by-2026
37. https://samcurry.net/web-hackers-vs-the-auto-industry/
38. https://xakcop.com/post/hyundai-hack-2/
39. https://www.bleepingcomputer.com/news/security/researcher-breaches-toyota-supplier-portal-with-info-on-14-000-partners/amp/
40. https://www.malwarebytes.com/blog/news/2023/02/tiktok-car-theft-challenge-hyundai-kia-fix-flaw
41. https://www.motor1.com/news/654686/car-thieves-destructive-can-bus-hack-steal/
42. https://insideevs.com/news/659185/tesla-model-3-compromised-in-under-two-minutes-at-hacking-contest/

REFERENCES

43. https://eaton-works.com/2023/03/06/toyota-c360-hack/
44. https://www.bleepingcomputer.com/news/security/hackers-compromise-3cx-desktop-app-in-a-supply-chain-attack/
45. https://nvd.nist.gov/vuln/detail/CVE-2023-29389
46. https://nvd.nist.gov/vuln/detail/CVE-2023-26244
47. https://www.cybersecurityconnect.com.au/industry/9052-toyota-data-breach-exposes-10-years-worth-of-data-for-over-2m-customers
48. https://www.bleepingcomputer.com/news/security/multinational-tech-firm-abb-hit-by-black-basta-ransomware-attack/
49. https://www.stern.de/gesellschaft/regional/bayern/internet--einschraenkungen-bei-werkstattkette-atu-nach-cyberangriff-33482946.html
50. https://garage.asrg.io/cve-2023-3028-improper-backend-communications-allow-access-and-manipulation-of-the-telemetry-data/
51. https://hackaday.com/2023/06/08/hacking-a-hyundai-ioniqs-infotainment-system-again-after-security-fixes/
52. https://www.globalvillagespace.com/tech/shell-recharge-data-breach-exposes-ev-drivers-information/
53. https://grist.org/technology/hackers-already-infiltrate-ev-chargers-it-could-only-get-worse/
54. https://therecord.media/major-japanese-port-suspends-operations-following-lockbit-attack
55. https://thehackernews.com/2023/07/a-data-exfiltration-attack-scenario.html
56. https://www.blackhat.com/us-23/briefings/schedule/index.html#jailbreaking-an-electric-vehicle-in--or-what-it-means-to-hotwire-teslas-x-based-seat-heater-33049; https://www.darkreading.com/application-security/tesla-jailbreak-unlocks-theft-in-car-paid-features
57. https://therecord.media/moovit-vulnerabilities-allow-free-subway-rides
58. https://www.foxbusiness.com/technology/tesla-data-breach-affects-75735-people-state-attorney-general-announces
59. https://therecord.media/orbcomm-trucking-software-ransomware; https://www.bleepingcomputer.com/news/security/orbcomm-ransomware-attack-causes-trucking-fleet-management-outage/
60. https://www.nw.de/lokal/bielefeld/mitte/23661084_Mobiel-nach-dem-Cyberangriff-Displays-konnten-Pendlern-keine-korrekten-Zeiten-anzeigen.html; https://www.radiobielefeld.de/nachrichten/lokalnachrichten/detailansicht/cyberangriff-bei-mobiel-partner-keine-aktuellen-fahrplan-anzeigen-in-bielefeld.html
61. https://therecord.media/knp-logistics-ransomware-insolvency-uk
62. https://restoreprivacy.com/threat-actor-claims-data-breach-on-american-moving-firm-u-haul/
63. https://thecyberexpress.com/cyberattack-on-bmw-munique-motors/
64. https://www.bleepingcomputer.com/news/security/auto-parts-giant-autozone-warns-of-moveit-data-breach/
65. https://www.bleepingcomputer.com/news/security/qilin-ransomware-claims-attack-on-automotive-giant-yanfeng/
66. https://www.seattletimes.com/seattle-news/transportation/cyberattack-shuts-down-wa-transportation-website-causing-havoc-for-ferry-passengers-others/
67. https://cyberscoop.com/fleet-management-vulnerability-digitial-communications-technologies/
68. https://www.bleepingcomputer.com/news/security/nissan-is-investigating-cyberattack-and-potential-data-breach/amp/
69. https://www.bleepingcomputer.com/news/security/orbcomm-ransomware-attack-causes-trucking-fleet-management-outage/
70. https://www.bleepingcomputer.com/news/security/orbcomm-ransomware-attack-causes-trucking-fleet-management-outage/
71. https://hackaday.com/2023/06/08/hacking-a-hyundai-ioniqs-infotainment-system-again-after-security-fixes/
72. https://hackaday.com/2023/06/08/hacking-a-hyundai-ioniqs-infotainment-system-again-after-security-fixes/
73. https://cyberscoop.com/fleet-management-vulnerability-digitial-communications-technologies/
74. https://www.cvedetails.com/cvss-score-distribution.php
75. https://nvd.nist.gov/vuln-metrics/cvss
76. https://www.wjhl.com/business/press-releases/globenewswire/8856072/haynes-international-announces-network-outage/
77. https://www.globenewswire.com/en/news-release/2023/07/19/2707585/9124/en/Haynes-International-Provides-Cybersecurity-Update-and-Estimated-Third-Quarter-Financial-Impact.html
78. https://www.kendrion.com/en/news-events/news/news-detail/kendrion-experiences-cyber-security-incident
79. https://www.autoevolution.com/news/new-electrify-america-charger-gets-hacked-displays-tesla-s-supercharging-network-209367.html
80. https://twitter.com/MichaelMuni/status/1617272328626360321
81. https://c2a-sec.com/a-case-study-on-the-importance-of-security-validation-done-right-abb-chargersync-platform/
82. https://c2a-sec.com/a-case-study-on-the-importance-of-security-validation-done-right-abb-chargersync-platform/
83. https://nvd.nist.gov/vuln/detail/CVE-2023-29857
84. https://nvd.nist.gov/vuln/detail/CVE-2023-29857
85. https://therecord.media/orbcomm-trucking-software-ransomware
86. https://www.bleepingcomputer.com/news/security/orbcomm-ransomware-attack-causes-trucking-fleet-management-outage/

REFERENCES

87. https://www.rmf24.pl/regiony/olsztyn/news-atak-hakerski-sparalizowal-olsztyn-ustalenia-rmf-fm,nId,6866990#crp_state=1; https://cyberdefence24.pl/cyberbezpieczenstwo/atak-hakerski-w-olsztynie-sparalizowal-miasto
88. https://www.reuters.com/business/autos-transportation/california-suspends-gm-cruises-driverless-autonomous-vehicle-permits-2023-10-24/
89. https://www.reuters.com/business/autos-transportation/gms-cruise-recall-950-driverless-cars-after-accident-involving-pedestrian-2023-11-08/
90. https://www.axios.com/2023/11/27/self-driving-cars-robotaxis-trust
91. https://waymo.com/blog/2023/07/doubling-down-on-waymo-one.html
92. https://www.axios.com/2023/08/07/dallas-autonomous-trucks
93. https://waymo.com/blog/2023/10/the-waymo-driver-now-available-on-uber.html
94. https://www.prnewswire.com/news-releases/may-mobility-announces-105-million-series-d-investment-round-led-by-ntt-to-scale-autonomous-transit-services-301979363.html
95. https://www.hyundai.com/worldwide/en/company/newsroom/detail/motional-ioniq-5-robotaxi-to-be-manufactured-at-new-hyundai-motor-group-innovation-center-singapore-0000000360
96. https://asia.nikkei.com/Business/Technology/Japan-to-assign-bandwidth-for-Level-4-self-driving-vehicles
97. https://drivingpress.com/the-risks-of-autonomous-vehicles/
98. https://apnews.com/article/colorado-right-to-repair-farming-equipment-1da00ea957fd1057bf522cb4725e62d4
99. https://www.fb.org/news-release/farm-bureau-continues-to-advance-farmers-right-to-repair
100. https://www.reuters.com/legal/litigation/deere-must-face-us-farmers-right-to-repair-lawsuits-judge-rules-2023-11-27/
101. https://www.vice.com/en/article/m7bbkv/biden-administration-tells-car-companies-to-ignore-right-to-repair-law-people-overwhelmingly-voted-for
102. https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-3028
103. https://nvd.nist.gov/vuln/detail/CVE-2023-3028
104. https://nvd.nist.gov/vuln/detail/CVE-2022-38766
105. https://news.stv.tv/west-central/surge-in-keyless-car-thefts-sees-28-vehicles-stolen-in-glasgow-in-january-2023
106. https://www.suffolk.police.uk/news/latest-news/vehicle-owners-urged-be-vigilant-following-number-thefts
107. https://kitchener.ctvnews.ca/police-say-relay-and-reprogramming-thefts-are-on-the-rise-in-waterloo-region-here-are-the-most-targeted-vehicles-1.6308378
108. https://www.worcesternews.co.uk/news/23493583.keyless-theft-land-rovers-rise-warn-police/
109. https://www.infranken.de/lk/forchheim/blaulicht/heroldsbach-erneuter-autodiebstahl-wegen-keyless-go-funktion-taeter-stoeren-schluessel-signal-art-5691576
110. https://www.telegraph.co.uk/news/2023/08/29/keyless-car-hacking-equipment-ban-to-cut-car-thefts/
111. https://nvd.nist.gov/vuln/detail/CVE-2023-29389, https://kentindell.github.io/2023/04/03/can-injection/
112. https://kentindell.github.io/2023/04/03/can-injection/
113. https://www.carscoops.com/2023/02/toyota-rav4-prime-ecu-software-could-shut-down-the-hybrid-system/
114. https://hackaday.com/2023/11/22/keeping-a-mazdas-radio-on-after-the-engine-shuts-off/
115. https://samcurry.net/web-hackers-vs-the-auto-industry/
116. https://eaton-works.com/2023/03/06/toyota-c360-hack/
117. https://c2a-sec.com/a-case-study-on-the-importance-of-security-validation-done-right-abb-chargersync-platform/
118. https://nvd.nist.gov/vuln/detail/CVE-2023-6073
119. https://nvd.nist.gov/vuln/detail/CVE-2023-6073
120. https://nvd.nist.gov/vuln/detail/CVE-2023-22388
121. https://nvd.nist.gov/vuln/detail/CVE-2023-22388
122. https://nvd.nist.gov/vuln/detail/CVE-2023-29857
123. https://nvd.nist.gov/vuln/detail/CVE-2023-29857
124. https://www.latestly.com/socially/world/bykea-app-hacked-pakistans-ride-hailing-application-gets-hacked-users-receive-abusive-messages-see-pics-5197926.html
125. \https://juniperspring.xyz/posts/honda-reverse-engineering/
126. https://www.blackhat.com/us-23/briefings/schedule/index.html#jailbreaking-an-electric-vehicle-in--or-what-it-means-to-hotwire-teslas-x-based-seat-heater-33049 , https://www.darkreading.com/application-security/tesla-jailbreak-unlocks-theft-in-car-paid-features
127. https://www.autoevolution.com/news/new-electrify-america-charger-gets-hacked-displays-tesla-s-supercharging-network-209367.html
128. https://twitter.com/MichaelMuni/status/1617272328626360321
129. https://www.globalvillagespace.com/tech/shell-recharge-data-breach-exposes-ev-drivers-information/

REFERENCES

130. https://insideevs.com/news/659185/tesla-model-3-compromised-in-under-two-minutes-at-hacking-contest/
131. https://insideevs.com/news/659185/tesla-model-3-compromised-in-under-two-minutes-at-hacking-contest/
132. https://techcrunch.com/2023/11/14/a-software-update-bricked-rivian-infotainment-systems/
133. https://en.wikipedia.org/wiki/Cellular_V2X
134. https://gttwireless.com/dsrc-vs-c-v2x-comparing-the-connected-vehicles-technologies/
135. https://www.dwt.com/blogs/broadband-advisor/2023/05/fcc-connected-vehicles-c-v2x
136. https://www.leewayhertz.com/generative-ai-in-automotive-industry/
137. https://hbr.org/2023/11/navigating-the-new-risks-and-regulatory-challenges-of-genai
138. https://www.thebanker.com/The-world-s-first-GenAI-guidelines-for-banks-1702900543
139. https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai
140. https://techcrunch.com/2023/12/13/china-autonomous-vehicle-driving-regulation/ , https://xxgk.mot.gov.cn/2020/jigou/ysfws/202312/t20231205_3962490.html
141. https://www.miit.gov.cn/jgsj/zbys/qcgy/art/2023/art_439d600cba254bd5b426d4dadc6d82b5.html; https://unece.org/sites/default/files/2021-03/R155e.pdf; https://en.wikipedia.org/wiki/World_Forum_for_Harmonization_of_Vehicle_Regulations
142. https://www.gov.cn/zhengce/zhengceku/202306/content_6887168.htm
143. https://www.marklines.com/en/report/rep2457_202303
144. https://theicct.org/pv-india-rde-testing-apr23/
145. https://www.cybersecurity-insiders.com/india-to-make-cybershield-mandatory-for-vehicles/; https://timesofindia.indiatimes.com/business/dontgetscammed/news/cybershield-mandate-for-vehicles-govt-takes-preemptive-action-against-cyber-threats-to-cars-trucks/articleshow/105208966.cms
146. https://www.jdsupra.com/legalnews/california-takes-the-wheel-a-closer-9580097/
147. https://unece.org/sites/default/files/2021-03/R155e.pdf
148. https://unece.org/sites/default/files/2021-03/R156e.pdf
149. https://www.linkedin.com/pulse/automotive-cybersecurity-2023-horizontal-europe-sight-tschersich-hesre/?utm_source=share&utm_medium=member_ios&utm_campaign=share_via
150. https://www.iso.org/standard/70918.html
151. https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf
152. https://www.enisa.europa.eu/publications/smart-cars, https://www.enisa.europa.eu/publications/recommendations-for-the-security-of-cam/
153. https://automotiveisac.com/best-practices
154. https://unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf
155. https://unece.org/fileadmin/DAM/trans/doc/2020/wp29/ECE-TRANS-WP29-2020-080e.pdf
156. https://clepa.eu/mediaroom/clepa-and-acea-join-with-auto-isac-on-motor-vehicle-cybersecurity/
157. https://unece.org/sites/default/files/2023-07/ECE-TRANS-WP.29-GRVA-16e.pdf
158. https://www.linkedin.com/pulse/automotive-cybersecurity-2023-horizontal-europe-sight-tschersich-hesre/?utm_source=share&utm_medium=member_ios&utm_campaign=share_via
159. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act#:~:text=Less%20apparent%20to%20many%20users,software%20with%20a%20digital%20component
160. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet
161. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet
162. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32019R2144
163. https://www.linkedin.com/pulse/automotive-cybersecurity-2023-horizontal-europe-sight-tschersich-hesre/?utm_source=share&utm_medium=member_ios&utm_campaign=share_via
164. https://www.iso.org/standard/69113.html
165. https://www.switch-ev.com/blog/what-is-iso-15118
166. https://www.switch-ev.com/blog/basics-of-plug-and-charge
167. https://www.sec.gov/news/press-release/2023-139
168. https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214
169. https://www.sec.gov/education/smallbusiness/goingpublic/SRC
170. https://www.databreaches.net/alphv-files-an-sec-complaint-against-meridianlink-for-not-disclosing-a-breach-to-the-sec/
171. https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf

REFERENCES

172. https://www.govinfo.gov/content/pkg/FR-2022-09-09/pdf/2022-19507.pdf
173. https://upstream.auto/research/automotive-cybersecurity/
174. https://automotiveisac.com/press-news/auto-isac-partners-with-upstream-security-to-enhance-automotive-threat-landscape-visibility
175. https://www.telematicswire.net/asrg-partners-with-upstream-to-enhance-automotive-cyber-threat-intelligence/
176. https://www.nhtsa.gov/laws-regulations/standing-general-order-crash-reporting
177. https://www.nhtsa.gov/speeches-presentations/automated-road-transportation-symposium-arts23-keynote-address
178. https://www.vice.com/en/article/m7bbkv/biden-administration-tells-car-companies-to-ignore-right-to-repair-law-people-overwhelmingly-voted-for
179. https://www.nhtsa.gov/press-releases/nhtsa-proposes-seat-belt-warning-system-expansion
180. https://www.nhtsa.gov/sites/nhtsa.gov/files/2023-09/NTSB-Response_September-2023_Speeding_Rear-Impact-Guards_ADB-Headlamps-v2.pdf
181. https://www.iea.org/reports/global-ev-outlook-2023/executive-summary
182. https://www.progressive.com/lifelanes/on-the-road/future-of-electric-cars
183. https://www.federalregister.gov/documents/2023/02/28/2023-03500/national-electric-vehicle-infrastructure-standards-and-requirements
184. https://www.foley.com/insights/publications/2023/04/us-dot-finalizes-ev-charging-infrastructure-rules/
185. https://www.nccoe.nist.gov/projects/cybersecurity-framework-profile-electric-vehicle-extreme-fast-charging-infrastructure
186. https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8473.ipd.pdf
187. https://www.nemko.com/blog/cybersecurity-requirements-ce-marking-postponed-till-1-august-2025
188. https://data.consilium.europa.eu/doc/document/ST-12041-2023-INIT/en/pdf
189. https://www.consilium.europa.eu/media/69093/st16996-en23.pdf
190. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
191. https://www.electrive.com/2021/04/21/partners-pledge-to-implement-plugcharge-across-europe/
192. https://www.charin.global/technology/plug-charge
193. https://www.gov.uk/government/consultations/electric-vehicle-smart-charging/public-feedback/electric-vehicle-smart-charging-consultation-summary-of-responses
194. https://www.legislation.gov.uk/uksi/2021/1467/made
195. https://www.legislation.gov.uk/uksi/2021/1467/made
196. https://assets.publishing.service.gov.uk/media/628ce214e90e071f653a494a/Guide-to-evscp-regulations-2021-V2.1.pdf
197. 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
198. 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
199. https://www.switch-ev.com/blog/what-is-iso-15118
200. https://en.wikipedia.org/wiki/Combined_Charging_System
201. https://www.switch-ev.com/blog/basics-of-plug-and-charge
202. https://www.charin.global/technology/iso15118/
203. https://www.cinch.co.uk/guides/electric-cars/what-is-chademo-ev-charging
204. https://www.chademo.com/design-guideline-for-external-charging-updated
205. https://www.openchargealliance.org/protocols/ocpp-201/
206. https://www.linkedin.com/pulse/how-does-ocpp-201-iso-11518-work-together-why-do-matter-beckmann/
207. https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf
208. https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/
209. https://www.nhtsa.gov/technology-innovation/vehicle-data-privacy
210. https://www.forbes.com/sites/stevetengler/2022/05/17/privacy-battle-over-connected-cars-takes-an-interesting-turn-in-california/
211. https://europe.autonews.com/guest-columnist/connected-cars-evolving-eu-regulatory-landscape
212. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3491, https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai
213. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113
214. https://www.consilium.europa.eu/en/press/press-releases/2023/11/27/data-act-council-adopts-new-law-on-fair-access-to-and-use-of-data/
215. https://www.dentons.com/en/insights/articles/2023/december/14/the-new-eu-ai-act-the-10-key-things-you-need-to-know-now
216. https://www.cyberghostvpn.com/en_US/privacyhub/dark-web-vs-deep-web/
217. https://www.cyberghostvpn.com/en_US/privacyhub/dark-web-vs-deep-web/

REFERENCES

218. For more details, see Chapter 1
219. https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html
220. https://en.wikipedia.org/wiki/Darknet_market
221. https://xakcop.com/post/hyundai-hack-2/
222. https://infosecwriteups.com/how-i-hacked-1000-tesla-cars-using-osint-4cd837b8c530; https://www.ctfiot.com/142013.html
223. https://www.nhtsa.gov/equipment/odometer-fraud
224. https://voonze.com/tsmc-supplier-suffers-ransomware-attack-and-has-data-leaked-by-hacker-group/
225. https://www.kendrion.com/en/news-events/news/news-detail/kendrion-experiences-cyber-security-incident
226. https://thecyberexpress.com/qilin-leaks-data-from-the-tesm-cyber-attack/
227. https://therecord.media/orbcomm-trucking-software-ransomware
228. https://therecord.media/knp-logistics-ransomware-insolvency-uk
229. https://www.gartner.com/en/documents/3904768
230. https://owasp.org/API-Security/editions/2023/en/0x11-t10/

UPSTREAMについて

Upstream Securityは、コネクテッドカーとスマートモビリティサービス専用に構築されたクラウドベースのモビリティサイバーセキュリティおよびデータ管理プラットフォームを提供しています。Upstreamのプラットフォームは、機械学習、データ正規化、デジタルツインプロファイリング技術を融合して、既存の自動車データフィードを使用してリアルタイムで異常を検出します。Upstreamは、業界で初めて自動車のサイバーセキュリティに特化したThreat Intelligenceフィードである AutoThreat®Intelligenceと組み合わせ、これまでにない、サイバーセキュリティとデータに基づいたインサイトをお客様の環境に応じてシームレス提供します。

Upstreamは、同盟ベンチャーズ企業（ルノー、日産、三菱）、ボルボグループ、BMW、ヒュンダイ、三井住友海上保険株式会社、ネイションワイド・インシュアランス、セールスフォースベンチャーズ、CRV、グリロット・キャピタル・パートナーズおよびマニブ・モビリティから資金提供されています。

詳しくは、こちらから

ホームページ：
www.upstream.auto

お問い合わせ：
hello@upstream.auto

フォロー：

Upstream