



# VicOne

Driving Automotive Cybersecurity Forward




## 自動車データ

コネクテッドカーのデータ利用、収益化、  
サイバーセキュリティの脅威

Numaan Huq, Vladimir Kropotov,  
Philippe Lin, Rainer Vosseler

Trend  
**Research**   
for VicOne



主要ポイント .....	3
1. はじめに .....	5
2. 自動車データエコシステム .....	7
3. 自動車データの分析 .....	9
4. 自動車データのサイバーセキュリティリスク .....	19
5. コネクテッドカーにおけるミドルウェア API について .....	21
6. オープンな MQTT サーバーから収集された車両データ .....	23
7. 車両 API データに関する研究 .....	29
8. 結論 .....	32
付録：車両ネットワークアーキテクチャ .....	34

自動車業界における技術革新は、現代の車両をデータハブへと変貌させました。これらの車両は、大量のデータを絶えず生成し、消費し、伝送しています。この車両データの分析と使用により、車両機能の向上から新たな収益源の創出に至るまで、多くの新たな機会が生まれています。しかし、このデータ中心のエコシステムへの移行は、自動車業界に固有の一連の課題と責任ももたらしています。

本稿では、車両データとその生成、伝送、使用について詳述します。特に車両データに関連するプライバシーとセキュリティの懸念を取り上げています。しばしば、車両データはユーザーの明示的な同意や知識なしに収集され<sup>1,2</sup>データ収集の詳細が購入契約の細かい文字に隠されています<sup>3</sup>。これは、データ保護法違反を含む、データの不正使用や乱用の潜在的なリスクについて深刻な懸念を提起しています<sup>4</sup>。

さらに本稿では、車両から収集される様々な種類のデータ、このデータの活用と商業化の方法、そしてそれに伴うサイバーセキュリティのリスクについて研究しています。今回の調査で、MQTT ブローカーを通じた車両データの漏えい事例が見つかり、少量のデータでさえもドライバーやフリートを特定するのに使われる可能性があり、保護されていないデータのプライバシーとセキュリティのリスクが浮かび上がりました。なお、意外な発見としては、トレンドマイクロのテレメトリデータから車両の API 通信記録が見つかり、これらはサイバー犯罪者が利用可能な脆弱性を暴露する可能性があります。

今回の調査結果は、データ伝送の安全性と厳格な保護対策の必要性を強調しています。接続車の事業の成功がサイバー犯罪者にとっての魅力的なターゲットとなるため、強固なデータセキュリティ対策が求められています。自動車産業がデータに基づく業界へと進化するにつれ、OEM や Tier 1、Tier 2 のサプライヤーを含む業界関係者は、イノベーションとデータ保護のバランスを見つけることが重要になります。

## 主要ポイント

**データ駆動型エコシステム**：現代の車両は、データが生成・収集・配布され、革新的な方法で利用される複雑なデータハブへと進化しました。これにはプライバシーの懸念やデータの不正使用・乱用といったユニークな課題が伴います。

---

<sup>1</sup> <https://www.caa.ca/your-rights/data-privacy/>

<sup>2</sup> <https://www2.deloitte.com/ca/en/pages/consulting/articles/connectedvehiculesontario.html>

<sup>3</sup> <https://apnews.com/31c018cdbc634d42a7c97d04774954b1>

<sup>4</sup> <https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/>



**収益化とサイバーセキュリティのリスク：**車両データからの収益化機会がサイバー犯罪者を引き付けることが予想されます。初の大規模攻撃はデータに関連し、車両ハッキングやフリートの乗っ取りなど、より衝撃的な攻撃へとエスカレートする可能性があります。

**ミドルウェア API：**ミドルウェア API は、サイバー犯罪者が車両の E/E アーキテクチャや ECU に簡単に API 経由でアクセスする新たな機会を提供します。これにより、アーキテクチャに依存しないマルウェアや新しいサイバー攻撃手法が出現する可能性があります。

**車両データの漏えい：**公開された MQTT サーバー経由で共有される車両データは、サーバーのオープン性から誰でもアクセス可能です。このデータは、ドライバーやサービスのプロファイリングに利用され、その活動や運営に関する洞察を提供します。不安全な MQTT サーバーは、サブスクライバーからの書き込み命令を受け入れるため、データ汚染攻撃に対して脆弱です。

**規制のギャップ：**車両データの収集と使用に関する法的なギャップを埋める必要があります。自動車産業は規制の空白下では効果的に運営できません。適切な法規制は、明確さと安定性を提供するために不可欠です。

## 1. はじめに

技術進歩とデータ統合が自動車産業を急速に変化させています。車両はデータハブへと変貌し、絶え間なく大量のデータ<sup>5</sup>を生成、利用、送信しています。今回の調査では、自動車データの広大で見過ごされがちな領域を探求し、交通手段と社会全体の未来に対するその影響を理解することを目指しています。

今回扱った主要なデータソースの 1 つは、様々な自動車メーカー（OEM）や自動車業界のティア 1（T1）およびティア 2（T2）サプライヤーが収集したアプリケーションプログラミングインターフェース（API）のフィールド名リストでした。このデータを入手するには、オープンソースインテリジェンス（OSINT）技術を駆使する必要性がありました。なぜなら、車両によって生成・送信されるデータについての情報は、簡単には得られず、アクセスも難しかったからです。また、API フィールド名リストには、データブローカーが OEM から購入し、匿名化、集約した後、自社の API を組み込んで再販するデータも含まれていました。これにより、自動車データエコシステムにさらに貢献しています。自動車データエコシステムは、車両、メーカー、サプライヤー、データブローカー、データ利用者などがデータフローを介して結びついた巨大なネットワークです。このエコシステムの複雑さは、今回の調査での予期せぬ発見でもありました。

自動車データエコシステムにおいて、車両はデータを生成するだけでなく、データの消費者でもあります。今回の調査によると、車両は OEM やサードパーティーのクラウドからデータを受信しています。このデータ通信はモバイルアプリ経由、またはテレマティックコントロールユニット（TCU）を通じて直接行われ、TCU はゲートウェイチップや電子制御ユニット（ECU）と接続します。さらに、車両の車載インフォテインメント（IVI）システム（ヘッドユニット（HU）とも呼ばれる）の拡大するミドルウェアエコシステムについても検討しています。将来は、車両の電気・電子（E/E）システムの詳細を抽象化したアーキテクチャに依存しない開発者向け API が登場すると予想しています。

今回の調査では、トレンドマイクロのテレメトリーデータ内で車両と OEM/T1/T2 クラウド間の API 通信が確認されました。データ収集時、トレンドマイクロのテレメトリーデータを詳しく調べることで、リモートスタート/ストップ、ドアのロック/アンロック、テレマティクス収集などを行う車両 API 通信がログ内に存在していたことには驚かされました。また、公開 MQTT サーバー上での MQTT（メッセージキューイングテレメトリートランスポート）プロトコルによる車両データの漏えい事例も確認されました。これらの事例は限定的ですが、

---

<sup>5</sup> <https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car>

ドライバーの行動パターンの分析や車両の動きの追跡に十分な情報が含まれていることがありました。

今回の調査結果から、いくつかの重要な結論を導き出すことができます。車両は単なる乗り物ではなく、複雑なデータハブに変わりつつあります。OEM や T1、T2 サプライヤー、データブローカーなど、多岐にわたる関係者によって収集される車両データは統合され、新しいデータ製品の生成や、ドライバープロフィールの作成から交通データを活用したターゲット広告まで、収益化のチャンスを生み出しています。これは、車両データエコシステムが広範で複雑なものであることを示しています。しかし、車両データの普及の範囲や、データ保護のためにどのようなセキュリティ対策が必要かについては、十分に理解されていません。車両データエコシステムの探求や、データの悪用・乱用の可能性についての調査が不足しているようです。本稿では、これらの知識の欠如に取り組み、自動車データの現状と将来に関する議論を開始することを目指しています。

## 2. 自動車データエコシステム

自動車データエコシステムは、接続された車両、メーカー、サプライヤー、データブローカー、データ消費者など、データの流れによって相互に結びついているエンティティのネットワークです。

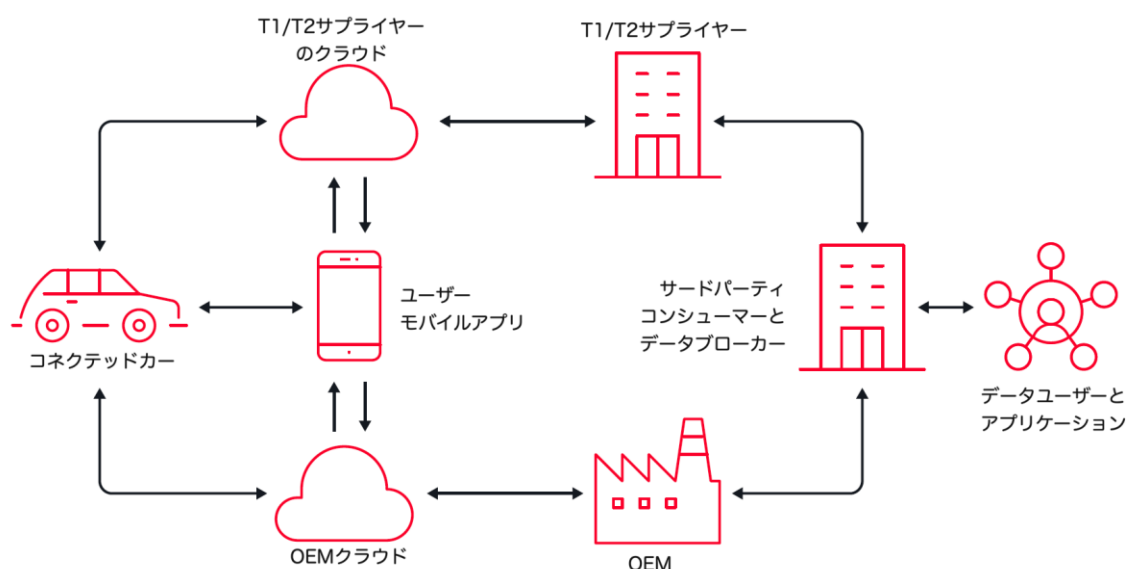


図 1：自動車データエコシステム

このエコシステムの重要な構成要素であるデータ収集は、複数のチャネルを通じて行われます。主要な方法は、TCU（テレマティクス・コントロール・ユニット）を介しており、これは 3G/4G/5G の携帯電話網を通じて OEM（元装置メーカー）や T1/T2 サプライヤーなどの信頼された第三者が所有するクラウドインフラストラクチャと通信します。TCU 以外にも、車両にリンクされたモバイルアプリケーションを通じてデータを収集することが可能で、収集できる情報の範囲と量を広げています。

車両データは貴重なリソースとなります。これにより、車両の性能、ドライバーの行動、利用パターンなどについての洞察が得られるからです。OEM や T1/T2 サプライヤーは、このデータを利用して製品の改良、機能の向上、新しい提供物の特定と創造、ユーザーエクスペリエンスの強化を行います。例えば、予測保守、ルート最適化、個人化された推奨などが、このデータから直接恩恵を受けるアプリケーションです。しかし、車両データの有用性は製造業者とそのサプライヤーに留まらず、プライバシーを保護するために適切にサニタイズされたこのデータは、データブローカーや消費者に直接売ることもできます。これにより OEM に追加の収入源が生まれるだけでなく、サービス、アプリ、製品のエコシステムの成長も促進されます。

自動車データは、多様な用途で活用されています。これにはエンターテインメント、個人に合わせた推薦、運転行動に基づく保険商品、さらにスマートシティソリューションなどが含まれます。自動車データのエコシステムは、OEM や T1/T2 サプライヤーだけではなく、消費者、サードパーティサービスプロバイダー、新しいアプリケーションや製品も含めた幅広い範囲に及びます。総じて、自動車データエコシステムは自動車業界内で進化し続けるダイナミックな分野です。車両データを利用して新しい洞察と革新的なビジネスモデルを創出する一方で、様々な業界向けのデータ駆動型製品やサービスの市場も形成しています。



### 3. 自動車データの分析

自動車は、データを生成し消費する複雑なハブとして機能しています。私たちはすでに、自動車データエコシステムが、コネクテッドカー、OEM、サプライヤー、データブローカー、データ利用者を含むエンティティのネットワークであることを理解しています。これらは全て、データフローによって互いに繋がっています。自動車がデータを生成し送信することは以前から知られていますが<sup>6,7</sup>、どのようなデータが OEM や T1、T2 のクラウドに送られているのかはほとんど明らかにされていません。これにより、データのプライバシー、セキュリティ、そして利用に関する重要な疑問が生じ、ドライバーの日常のデジタル足跡についての不明点が生じています。

#### 3.1 データソースについて

今回の調査における主要なデータソースは、様々な OEM およびサプライヤーが収集した API フィールド名でした。これらの API フィールド名や車両の生データへのアクセスは、実際には困難を伴いました。車両データのアクセスを求め、OEM 各社にリクエストを提出しましたが、完全に拒否されることもあれば、プライバシーの観点から特定の地理的位置からのデータアクセスがサポートされていないと通知されることもありました。また、ある2つのケースでは、詳細な議論が行われましたが、解決には至らず、依然として車両データへのアクセスができないこともありました。また、車両データをどう使用する予定かについて詳細な説明書を提出するよう求められた場合もありました。ただし、**データ取得時の困難にもかかわらず、こうした厳格なアクセス制御は、OEM が適切な監督を行い、データアクセスを無差別に提供しないことを示す、良い兆候とも言えます。**

ライブ車両のデータフィードは価値があるものですが、今回の調査では、主にどの API データフィールドが生成されて収集されるのか、そしていくつかのサンプルデータを確認することが必要でした。さらには、異なる OEM、T1/T2 サプライヤー、データブローカーから API フィールド名を収集するために OSINT も利用しました。アプリや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、データを GitHub やブログで公開している車好きのコミュニティも存在していました。OEM や T1/T2 サプライヤーが自ら API フィールド名を公表している場合もあり、こうした透明性には感謝しかありません。こうして、BMW<sup>8,9,10</sup>、

---

<sup>6</sup> <https://www.theglobeandmail.com/drive/technology/article-what-kind-of-data-is-my-new-car-collecting-about-me-nearly-everything/>

<sup>7</sup> <https://www.washingtonpost.com/technology/2019/12/17/what-does-your-car-know-about-you-we-hacked-chevy-find-out/>

<sup>8</sup> [https://github.com/bimmerconnected/bimmer\\_connected](https://github.com/bimmerconnected/bimmer_connected)

<sup>9</sup> <https://bmw-cardata.bmwgroup.com/thirdparty/public/car-data/technical-configuration/api-documentation>

<sup>10</sup> <https://bmwcardata.bmwna.com/telematicKeys/EN/BMWCarDataTelematicsDataGlossary.pdf>

Rolls-Royce<sup>11</sup>、Geotab 経由の Ford<sup>12</sup>、OnStar 経由の General Motors (GM)<sup>13, 14</sup>、Geotab 経由の GM<sup>15, 16</sup>、Mercedes-Benz<sup>17, 18, 19</sup>、Tesla<sup>20, 21, 22</sup>、Audi<sup>23</sup>、Caruso<sup>24</sup>、Samsara<sup>25</sup>、Otonomo<sup>26, 27</sup>、Smartcar<sup>28</sup>、High Mobility<sup>29, 30</sup>、GeoTab 経由の Navistar<sup>31</sup>、Open Vehicles Monitoring System<sup>32</sup>、GeoTab<sup>33, 34</sup>、AutoPi<sup>35</sup>、Invers<sup>36</sup>、Viper<sup>37</sup>から API フィールド名を収集しました。個別のデータソースはある程度不完全でしたが、多くのソースからデータを集めて照合することで、車両が生成し OEM や T1/T2 のクラウドに送り返すことができるデータフィールドの種類についてかなり包括的な理解を得ることができました。

また、公開されている MQTT サーバーを介した車両データの流出も確認しました。生の車両データを探し求める過程で、世界中の MQTT サーバーを見つけ出すことができました。今回の調査では、主に車両データがどこで見つかるかを特定するため、多様なソースからデータを収集することを目指しました。また、トレンドマイクロのテレメトリーデータも調査し、予期せぬ車両と OEM や T1/T2 クラウドとの API コールのログも確認することができました。

---

<sup>11</sup> [https://www.rolls-roycemotorcars.com/content/dam/rrmc/marketUK/rollsroycemotorcars\\_com/downloads/Rolls-Royce\\_CarData\\_Data\\_Catalogue.pdf](https://www.rolls-roycemotorcars.com/content/dam/rrmc/marketUK/rollsroycemotorcars_com/downloads/Rolls-Royce_CarData_Data_Catalogue.pdf)

<sup>12</sup> <https://support.geotab.com/pl-PL/oem-integration/mygeotab/doc/ford-data-set>

<sup>13</sup> <https://developer.gm.com/>

<sup>14</sup> <https://flespi.com/protocols/general-motors-onstar#parameters>

<sup>15</sup> <https://support.geotab.com/oem-integration/mygeotab/doc/gm-data-set>

<sup>16</sup> [https://docs.google.com/document/d/100MkJ0qn--pErAidaoSrQxW22NYj3E4dW\\_9Pf6DBCu/edit#heading=h.jloxp6otbxnm](https://docs.google.com/document/d/100MkJ0qn--pErAidaoSrQxW22NYj3E4dW_9Pf6DBCu/edit#heading=h.jloxp6otbxnm)

<sup>17</sup> <https://developer.mercedes-benz.com/products?vt=cars&vt=vans&vt=smart>

<sup>18</sup> <https://www.postman.com/mbdevelopers/workspace/mercedes-benz/overview>

<sup>19</sup> <https://www.scip.ch/en/?labs.20180405>

<sup>20</sup> <https://www.zimlon.com/b/comprehensive-list-of-data-tesla-collects-from-their-customers-cm529/>

<sup>21</sup> <https://tesla-api.timdorr.com/>

<sup>22</sup> [https://github.com/timdorr/tesla-api/blob/master/ownerapi\\_endpoints.json](https://github.com/timdorr/tesla-api/blob/master/ownerapi_endpoints.json)

<sup>23</sup> [https://github.com/arjenvrh/audi\\_connect\\_ha](https://github.com/arjenvrh/audi_connect_ha)

<sup>24</sup> <https://dev.caruso-dataplace.com/api/consumer/page/data-catalog/>

<sup>25</sup> <https://developers.samsara.com/reference/overview>

<sup>26</sup> <https://otonomo.io/data/>

<sup>27</sup> <https://docs.otonomo.io/reference/service-access-token>

<sup>28</sup> <https://smartcar.com/docs/api-reference/intro>

<sup>29</sup> <https://www.high-mobility.com/car-api>

<sup>30</sup> <https://airtable.com/appnqv8fdIWYRB0D4/shry3EDO6LiBunTm/tblCBBV23F1zBOnhl>

<sup>31</sup> <https://support.geotab.com/oem-integration/doc/truck-data>

<sup>32</sup> <https://docs.openvehicles.com/en/latest/index.html>

<sup>33</sup> <https://geotab.github.io/sdk/software/api/reference/>

<sup>34</sup> <https://support.geotab.com/mygeotab/mygeotab-add-ins/doc/analytics-api>

<sup>35</sup> <https://api.autopi.io/>

<sup>36</sup> <https://developers.invers.com/api-reference/>

<sup>37</sup> [https://github.com/fiquett/Viper\\_SmartStart\\_Control](https://github.com/fiquett/Viper_SmartStart_Control)

## 3.2 データ分類について

OEM、T1/T2 サプライヤー、ブローカーから集めた API フィールド名は構造が整っていないことが多く、同じタイプのデータに複数の名称が存在し、データの理解と活用を複雑にしています。今回の調査での主要な任務の1つは、車両データを大きなカテゴリーに分類することです。

表1に示されているカテゴリーは上位レベルのもので、それぞれに細分化されたサブカテゴリーがあります。今回の調査では、具体例にわかりやすい短い名称を提供し、OEM や T1/T2 ブローカー固有の API フィールド名の使用は控えています。

データカテゴリー	説明	データフィールドの例
車両情報	車両の識別と詳細に関する情報	車体番号、メーカー、モデル、年式、車両クラス
運転挙動	車両の運転挙動	速度、激しい加速、激しいブレーキング、コーナリング
燃料システム	車両の燃料システムに関するデータ	燃料レベル、燃料消費量、航続距離、近くの給油所
位置情報	地名を含む車両の地理的位置情報	緯度、経度、ジオハッシュ、都市、国
トリップ情報	車両の走行に関する詳細	走行時間、走行距離、停車駅
車両の安全性	安全関連データ	衝突イベント、シートベルト着用、スピード違反、衝突写真
サービスとメンテナンス	車両のサービスおよびメンテナンスに関するデータ	サービスイベント、サービス時間、サービスポイント、サービスリマインダー
休憩エリア	休憩所に関する情報	近隣の休憩エリア、休憩エリアの距離
故障診断コード (DTC)	車両で検出された DTC (コード、説明、ステータスを含む)	DTC、DTC 説明、DTC ステータス
バッテリー	車両のバッテリーに関する情報	バッテリー電圧、バッテリー残量、バッテリー温度
エンジン	エンジン性能データ	エンジン温度、回転数、エンジン状態
タイヤ空気圧モニタリング (TPM)	タイヤに関する情報	TPM ステータス、圧力フロント/リア/左/右

車両ステータス	車両の全体的な状態	車両の健康状態、エンジンクーラントレベル、燃料レベル
テレマティクス	テレマティクスと TCU に関するデータ	テレマチックポジション更新、テレサービス状況
クライメートコントロール	車両の気候制御システム	キャビン温度、AC オン/オフ、デフロスト
充電	電気自動車またはハイブリッド車の充電システムに関するデータ	充電パワー、充電ステータス、充電プラグステータス
ドアと窓	車両のドアと窓の状態と制御	ドアステータス、ウィンドウステータス、トランクロックステータス、ウィンドウ開閉
照明システム	車両の照明システムの状態と制御	ライトの状態、ヘッドライトの状態、室内灯の状態、オン/オフ
インフォテインメント・システム	車両のインフォテインメント・システムに関するデータ	ラジオ局、音量、メディアソース
車両セキュリティ	セキュリティ関連データ	アラームステータス、盗難防止ステータス、車両ロック
ナビゲーション・システム	車両のナビゲーションシステムに関するデータ	GPS ロケーション、ナビゲーションルート、目的地
オーディオ & エンターテインメント	車両の IVI 機能に関するデータフィールド	スピーカータイプ、オーディオソース、イコライザー設定
コネクティビティ	車両の接続オプション	Bluetooth 接続、Wi-Fi 接続、遅延、強度
ユーザー・プリファレンス	車両に保存されているユーザー設定	シート調整、空調設定、言語
ドライブトレインとパフォーマンス	車両のドライブトレイン・コンポーネントおよび性能に関するデータ	車速、エンジン回転数、トランスミッションギア

表 1：位レベルのデータカテゴリとそれに対応する説明、データフィールドの例

OEM、T1/T2、ブローカーからの API フィールド名のデータを大カテゴリーに分類することで、データの出所と利用方法の理解が深まりました。この上位レベルの概観は、車両データの複雑さを簡略化し、データをよりアクセスしやすく、理解しやすいものになっています。

### 3.3 新たなデータの推測

データは、新たな知見を得られる際、その真価を発揮します。このアプローチを実現する 1 つの方法は、異なるデータフィールドを組み合わせることで新たなデータの推測を試みることです。推測されたデータは、燃料の効率、ドライバーのパフォーマンス、地域の気象条件、道路の表面状態など、重要な知見を提供する可能性があります。これらの知見の品質と正確性は、統合されているデータポイントの品質、頻度、関連性に大きく依存する点に注意する必要があります。

- **燃料効率 = GPS + エンジン + 燃料消費量** — GPS データ（ルートや速度の情報を含む）をエンジン性能と燃料消費データと組み合わせることで、車両の燃料効率を計算することができます。これにより、運転習慣の改善や車両のメンテナンススケジュールの改善、さらには将来の車両設計に影響を与えることができます。
- **排出物分析 = エンジン + 燃料 + 運転者の行動** — エンジン、燃料システム、運転者の行動からのデータを統合することで、車両の排出物についての洞察を得ることができます。これにより、環境に優しい運転戦略の策定や排出物削減技術の開発に寄与することができます。
- **最適なルーティング = GPS + エンジン** — GPS データとエンジン性能の指標を相関させることで、最適なルーティング戦略を開発できます。これにより、移動時間の短縮、燃料効率の改善、車両の摩耗の最小化に役立ちます。
- **予知保全 = エンジン + GPS + DTC** — エンジンデータ、GPS データ（運転パターンを含む）、診断トラブルコード（DTC）を組み合わせることで、予知保全を実現できます。これにより、潜在的な問題を予測し、サービスのスケジュールを組むことができ、車両の寿命を延ばし、最適な性能を保つことができます。
- **運転者のパフォーマンス = GPS + エンジン + 燃料 + ブレーキ** — GPS データ（ルート、速度）、エンジン性能、燃料効率、ブレーキングパターンを統合することで、運転者のパフォーマンスの総合的な概観を提供します。これにより、運転者のトレーニングや保険の評価が助けられ、車両の安全性が向上します。
- **EV の航続距離 = バッテリー + GPS + 運転者の行動** — 電気自動車（EV）において、車両の航続距離を推定するには、バッテリーデータ（充電状態や放電率など）、GPS データ（ルートや速度など）、運転者の行動を統合する必要があります。これは、充電スケジュールの管理、ルート計画、そして未来の EV の設計に役立ちます。
- **タイヤの健康状態 = タイヤの圧力 + TPM 警告** — タイヤの圧力データとタイヤ圧力モニタリング（TPM）の警告を組み合わせることで、タイヤの健康状態を正確に評価できます。これにより、タイムリーなメンテナンスが可能となり、道路安全と車両性能を最適に保つことができます。
- **マイクロウェザー = ワイパー + ブレーキ + 外部温度** — ワイパーの使用状況、ブレーキの状態、外部温度センサーからのデータを収集することで、リアルタイムの地元の天候評価が可能になります。これはルート計画の改善に役立ち、より正確な天気予報のために気象機関と共有されることがあります。



- **駐車分析 = 車両の状態 + GPS** — 車両の状態データ（アイドル時間、速度、エンジンの状態など）と GPS を組み合わせることで、洞察に富んだ駐車分析が得られます。これは都市計画、より良い駐車解決策の設計、運転者へのリアルタイム駐車支援に役立ちます。
- **交通予測 = 車両性能 + GPS** — 車両性能データと GPS データを組み合わせることで、予測交通モデリングが可能になります。これはルーティングの改善、渋滞の最小化、交通管理戦略の支援に役立ちます。
- **車両のセキュリティ状態 = ドア + トランク + 窓 + GPS** — 車両のドア、窓、トランクの状態データと GPS 情報を統合することで、車両のセキュリティ状態を把握できます。これは侵入の迅速な検出と対応、車両セキュリティの強化に役立ちます。

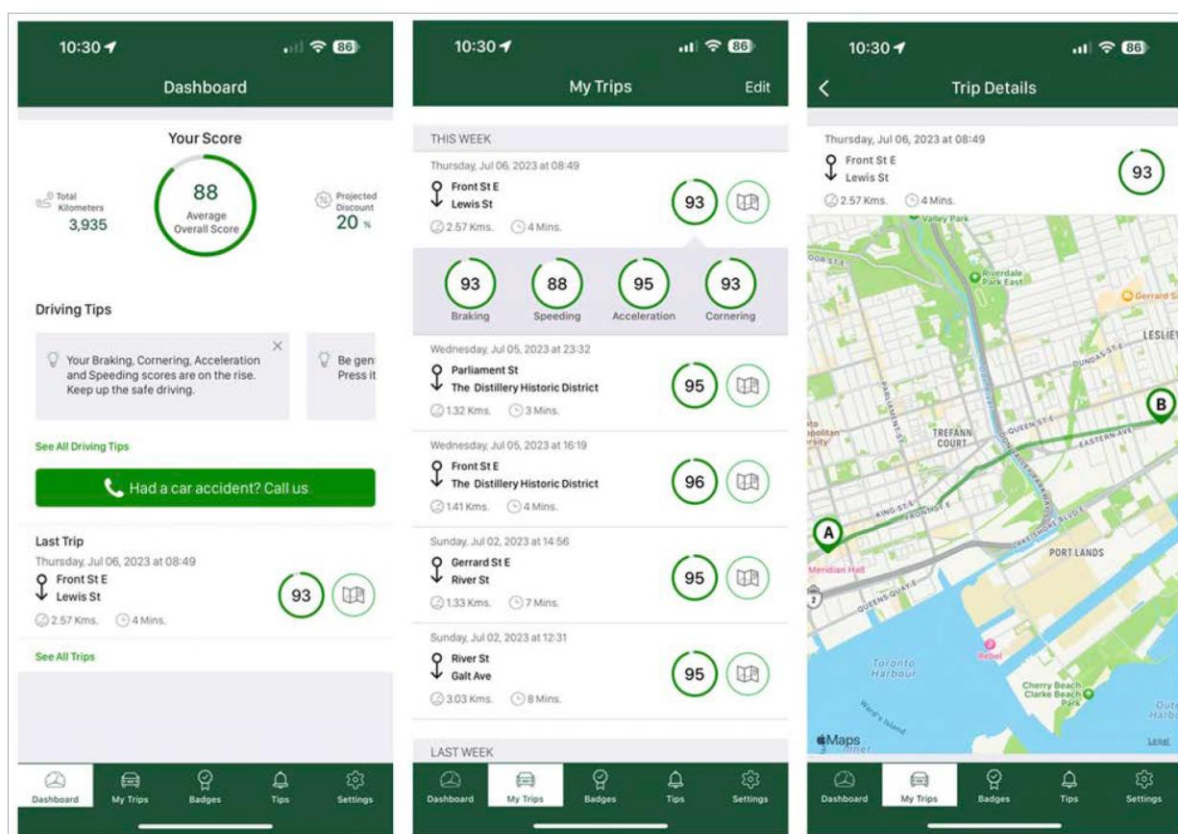


図 2：ブレーキ、加速、速度超過、コーナリング、GPS データを組み合わせる動的な保険料率と示しています。データはスマートフォンのジャイロスコープや GPS からの読み取り、または車両の診断用ポートに接続された小型のデバイスを通じて収集されます。この小型デバイス（ dongle ）はスマートフォンを介してインターネットに接続し、運転データを転送します。また、このデータは自動車メーカーによってテレマティクスコントロールユニット（TCU）を使用して収集することもあります。

このようにデータを分析して新しい知識を引き出すことは、洞察を深めるだけでなく、車両の性能を高め、安全性を向上させ、メンテナンスを容易にし、環境への影響も低減できます。車両が生成する大量のデータを効果的に組み合わせることで、これらのデータが本来持つ潜在的な価値を最大限に引き出すことが可能です。

### 3.4 データの収益化

OEM は、将来の優れた車の製造に役立つフィードバック、運転者や乗客の体験の向上、新しい運転技術の開発のために、主に車両データを収集しています。収集したデータの一部のみが販売され、大部分は研究用途に残されます。しかし、車両データには、新たな収益源を生み出す可能性もあります。テレマティクスデータは、車両の性能理解に寄与するだけでなく、パーソナライズされたサービスや革新的なビジネスモデルの開発にも利用可能です。この節では、OEM と第三者が車両データをどのようにして収益化できるかを探ります。

車両データの収益化方法について、今回の調査でも、実現可能な戦略についてブレインストーミングしました。これらの戦略には、既に実用化されているもの、新たに出現しているもの、そして将来的な方法が含まれます。

- **使用ベースの保険**：運転パターンや車両の健康状態などのデータ分析により、パーソナライズされた保険ポリシーを作成します。
- **車両管理サービス**：車両の利用、メンテナンス、ルート選定を最適化します。
- **車両メンテナンス・修理サービス**：テレマティクスデータを活用して車両の問題を理解し、診断することで、先見の明を持ったメンテナンスサービスを提供します。
- **位置情報ベースのサービスと広告**：運転パターンや位置情報に基づいた広告を通じて、ドライバーにターゲットを絞り、ビジネス収益を生み出します。
- **付加価値サービス**：テレマティクスデータに基づくサービスを開発し、サブスクリプションや一度きりの購入から収益を得ます。
- **サービス提供者とのパートナーシップ**：保険会社や修理工場、車両管理会社などと提携し、テレマティクスデータから得られる収益を分け合います。
- **データ集約と分析**：テレマティクスデータを集約し、分析することで得られる貴重な洞察やトレンドを研究機関、政府、自動車業界の関係者に提供します。

The screenshot displays the BMW Cardata website interface for 'Pay As You Drive Insurance'. It includes a 'Price overview' table, a 'Volume based discount' table, and various service features like 'Retrieve odometer information remotely' and 'What data or features do I have access to?'. The 'Price overview' table lists individual and monthly rates. The 'Volume based discount' table shows discounts based on the number of vehicles collected. The 'What data or features do I have access to?' section lists 'odometer', 'Retrieve km values remotely without the necessity of a single', 'Verify odometer information for fleet contracts', and 'Offer customized insurance products'.

Price overview	Price
Individual rate (per km without VAT)	0.2047*
Individual rate (per km with VAT)	0.2397*

Volume based discount	Discount
1 - 1,000	0%
1,001 - 2,000	5%
2,001 - 5,000	10%

図 3：データおよびデータ製品を販売する OEM の例 <sup>38, 39</sup>

<sup>38</sup> <https://bmw-cardata.bmwgroup.com/thirdparty/public/car-data/pricing>

<sup>39</sup> [https://developer.mercedes-benz.com/products/pay\\_as\\_you\\_drive\\_insurance](https://developer.mercedes-benz.com/products/pay_as_you_drive_insurance)

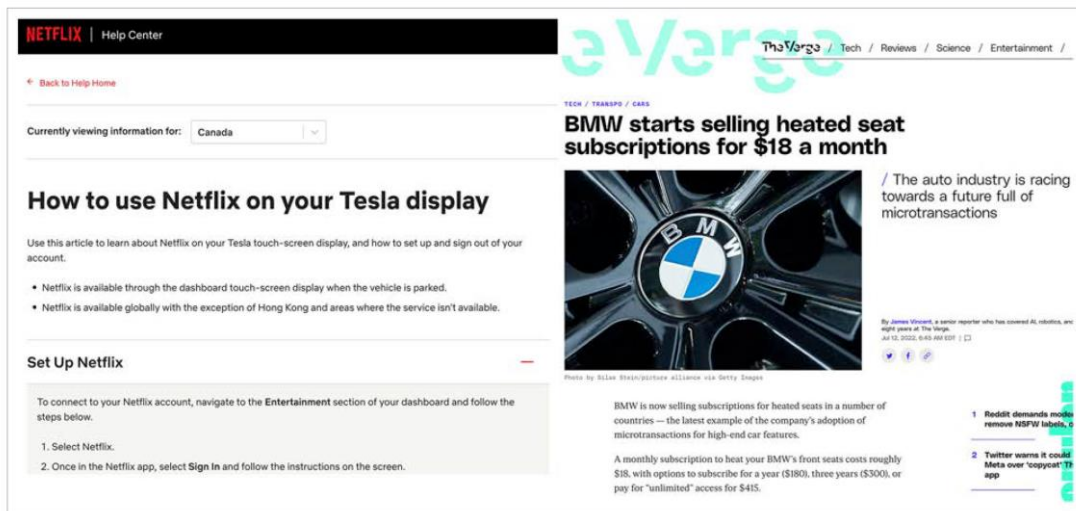


図 4：車両で利用可能なサブスクリプションサービスの例<sup>40, 41</sup>

自動車データは、自動車産業だけでなく、多岐にわたる業界にとっても貴重です。表 2 では、3 つの組織を例に挙げ、彼らが日常業務において自動車データをどう活用可能かを探ります。

ここで紹介する例には、特に銀行の場合、個人や集団をプロファイリングする必要があるものが含まれます。プライバシー侵害に思えるかもしれませんが、銀行がローンを確認する際には、既に借り手の財務状況を深く調べるデータポイントを利用しています。車両データはこの評価にさらに深みを加え、銀行は既に確立したプライバシー保護の仕組みを有しています。多くのデータポイントを組み合わせるプロファイリングの方法がなければ、完全に匿名化されたデータはあまり価値がありません。車両データの収益化においてプロファイリングが重要な要素であるため、関係者はデータの責任ある扱い、ユーザーのプライバシー保護、データの不正使用や濫用の防止を確実にするための先手を打つことが不可欠です。

<sup>40</sup> <https://help.netflix.com/en/node/112323/ca>

<sup>41</sup> <https://www.theverge.com/2022/7/12/23204950/bmw-subscriptions-microtransactions-heated-seats-feature>

業界・組織	日常業務における自動車データの利用例
銀行	<p>銀行は潜在的なクライアントや顧客に関連する財務習慣、信頼性、リスクについてのデータの取得と利用に関心を持つことがあります。銀行が使用できるデータには以下のものが含まれます：</p> <ul style="list-style-type: none"> <li>● <b>運転行動</b>：これには、運転者の習慣、運転ルート、旅行の頻度、道路での過ごす時間が含まれます。このデータは人のライフスタイルに関する洞察を提供し、クレジットスコアリングやリスクプロファイリングに利用できます。</li> <li>● <b>車両使用状況</b>：車両がどれほど頻繁に使用されるか、通常どこを運転するか、メンテナンス状況などの情報です。定期的な長距離の旅行は、車両ローンや保険商品の必要性を示唆することがあります。</li> <li>● <b>車両のメンテナンスと修理</b>：車両の定期的なメンテナンスとケアは、個人の財政的信頼性の指標となり、クレジットやローンの判断に役立ちます。</li> <li>● <b>位置情報</b>：訪れる場所は、その人のライフスタイル、消費習慣、財政能力を示すことがあります。例えば、高級ショッピング地区への定期的な訪問は、一定の収入水準を示すかもしれません。</li> <li>● <b>燃料効率</b>：車両の使用とメンテナンスの良さを示す指標です。高い燃料効率は、責任ある使用と財政的に責任ある個人であることを示す可能性があります。</li> </ul> <p>銀行はこのデータを利用して収益を生み出すことができます：</p> <ul style="list-style-type: none"> <li>● <b>パーソナライズされたローン提供</b>：車両の世話をする能力、運転習慣、購入予定の車種に基づいたパーソナライズされた車両ローンを提供します。</li> <li>● <b>クレジットスコアリングとリスクプロファイリング</b>：顧客の習慣をより深く理解し、クレジットスコアとリスク評価を行います。</li> <li>● <b>クロスセリングとアップセリング</b>：自動車保険、車両ローン、自動車購入報酬を含むクレジットカードなどの金融商品を推奨します。</li> <li>● <b>マーケティングと広告</b>：位置情報を利用したターゲット広告を行い、顧客が自動車購入を検討している際にオファーを提供します。</li> <li>● <b>パートナーシップ構築</b>：自動車小売業者や修理工場との特別オファーによる新しい収益源を生み出します。</li> </ul>
配送	<p>配送会社は、以下の車両データのサブセットを利用できます：</p> <ul style="list-style-type: none"> <li>● <b>GPS</b>：GPS データにより配送ドライバーのルートが最適化され、配送が迅速化し、燃料消費も削減されます。正確な GPS 履歴によって、交通量の多い地域と時間帯を把握し、配送スケジュールを改善できます。</li> <li>● <b>エンジンと燃料消費</b>：燃料効率に関する情報から、コスト削減につながる効率的な運転実践を促進できます。また、配送車両のメンテナンスタイミングを見極めるのにも役立ちます。</li> <li>● <b>ドライバーの行動</b>：加速、制動、速度などのドライバーの行動を監視することで、安全運転実践の遵守を確認できます。</li> <li>● <b>車両の状態</b>：車両の健康状態を監視し、予防保守を計画することで、停止時間の削減と予期せぬ修理コストを抑えられます。</li> <li>● <b>DTC (故障診断コード)</b>：車両の潜在的な問題を示すコードにより、予防保守を実施し、配送中の車両故障リスクを減少させます。</li> </ul> <p>収益を増やすために、このデータを活用することで運用効率が向上し、コストが削減され、顧客満足度が改善されます。例えば、GPS データを用いた効率的なルーティングや、エンジンや DTC データを用いた車両メンテナンスにより運用コストが最小限に抑えられます。ドライバー行動データを用いたドライバー性能の向上は安全性を高め、事故や損害に関連するコストを節約できます。データを基にした洞察は、高需要地域におけるサービスの戦略的拡大に利用され、ビジネス成長を推進します。</p>

<p>レッカー車 業界</p>	<p>レッカー会社は、車両データの複数のサブセットから恩恵を受けることが可能です。これらのデータは、収益の増加とサービスの充実に寄与します：</p> <ul style="list-style-type: none"> <li>● <b>故障データ</b>：エンジンの状態、故障診断コード（DTC）、燃料レベル、バッテリー状態に関連するデータは、車両の潜在的な故障を予測するのに役立ちます。これらの洞察を基に、レッカー会社は援助を積極的に派遣したり、予防措置を講じたりすることができます。</li> <li>● <b>GPS 位置情報</b>：リアルタイムの位置情報により、故障や立ち往生した車両の正確な位置を特定し、より迅速に対応できます。また、事故や故障の GPS データを利用してレッカー車を適切な場所に配置し、素早い対応を可能にします。</li> <li>● <b>車両の状態</b>：車両が停車中か、アイドル状態か、移動中かを把握することで、故障や不具合により立ち往生している車両を特定しやすくなります。</li> </ul> <p>このデータを活用して収益を上げる方法はいくつかあります：</p> <ul style="list-style-type: none"> <li>● <b>予防的サービス</b>：故障データの分析を通じて、共通の問題を防ぐために設計されたサービスを開発し、これを定額制のサブスクリプションとして提供し、安定した収益を確保します。</li> <li>● <b>ターゲット支援</b>：リアルタイムの GPS データを利用して立ち往生した車両の対応時間を短縮することで、顧客の経験を向上させ、顧客の忠誠心を築きます。</li> <li>● <b>パートナーシップ</b>：予測保守に関する洞察を車両メンテナンスサービスと共有し、紹介料を受け取ります。</li> <li>● <b>会員プログラム</b>：故障の予測データを基に、特定エリア内での定額レッカーサービスを提供する会員プログラムを導入します。</li> </ul>
---------------------	---

表 2：日常業務における自動車データの利用例



## 4. 自動車データのサイバーセキュリティリスク

自動車データは、自動車業界だけでなく様々な産業にとっても非常に価値があります。異なるデータ領域を組み合わせることで、新たな洞察を得たり、斬新なデータ製品を創出したり、革新的な製品やサービスを提供することが可能です。前節では、OEM やサードパーティが車両データを利用し、どのようにして収益化するかを探りました。そして実際に、車両向けのデータモネタイズやサブスクリプションサービスが提供されている例をすでに見てきました。収益化の機会が増え、大きな収益を生むようになれば、それは蜜を求めるミツバチのように、サイバー犯罪者を引き寄せることになるでしょう。

トレンドマイクロが VicOne 向けに行ったサイバー犯罪アンダーグラウンドへの調査<sup>42</sup>で、現在の脅威はカーモディンクに関わるものが主であることが明らかになりました。車好きが車両の機能を改変し、走行距離データを操作する例がこれに当たります。将来的な脅威には、サイバー犯罪者が車両のユーザーアカウントに無断でアクセスし、車を特定、侵入、盗むことが考えられます。盗難車は海外へ運ばれたり、部品として売られたり、他の犯罪に使用される恐れがあります。コネクテッドカーのサイバー犯罪市場は未成熟ですが、第三者が車両データを積極的に使用し始めるにつれて成長すると見込まれています。コネクテッドカーに対する最初の大規模な攻撃がデータを目標にし、それが車のハッキングや車両群の乗っ取りといったより劇的な攻撃へと発展する可能性が予想されます。

車両データが不適切に利用または悪用されるさまざまな方法についてブレインストーミングを実施してその可能性を検討しました。

- **車両のリアルタイム追跡**：リアルタイムの位置情報を取得することで、特定の車両が追跡され、これにより運転者や乗客のプライバシーや安全が危険にさらされる可能性があります。例えば、車両の現在地や通常のルートが把握されていれば、犯罪者はその車の下に不正品を隠して運ぶことができ、車両を運搬ツールとして利用することができます。リアルタイムでの車両追跡は、高いプロファイルを持つ個人やその資産の監視に利用されることもあります。
- **運転者のプロファイリング**：運転のパターンから、個人の習慣やライフスタイル、通常の訪れる場所が分析され、プライバシーの侵害やデータの不正利用の懸念が生じます。
- **データの漏えい**：個人を特定する情報、メンテナンスデータ、燃料消費量、その他の運用データが漏れることにより、プライバシーが侵害され、敏感な情報が露呈する恐れがあります。
- **データ操作**：車両に偽の警告を生成したり、性能データを改ざんすることで、誤った診断や危険な運転設定を引き起こす可能性があります。
- **データを人質に身代金要求**：攻撃者が OEM や T1/T2/ブローカーのクラウドに保存されている車両データへのアクセスを暗号化またはロックし、アクセスの復元に身代金を要求するこ

<sup>42</sup> <https://vicone.com/blog/what-lies-in-store-for-connected-cars-in-the-cybercriminal-underground>

とがあります。これは、排出ガス計算などの政府規制に関連してリアルタイムの車両データが必要な場合に特に深刻な損害をもたらします。

- **ソーシャルエンジニアリング**：収集したデータを使用して、悪意ある目的でデータを利用するターゲットを絞ったソーシャルエンジニアリング攻撃を仕掛ける可能性があります。
- **インフラの攪乱**：救急車や公共サービス車両などの重要インフラ車両を特定し、必要不可欠なサービスに影響を与えかねない攪乱攻撃を計画・実行することができます。
- **産業スパイ**：自動車データは、企業や産業のスパイ活動に利用され、ビジネス運営や戦略、競争上の優位性に関する貴重な洞察を提供する可能性があります。
- **故障診断コードとメンテナンス**：故障診断コード（DTC）やメンテナンスデータにアクセスすることで、車両の脆弱性を特定し、それをサイバー攻撃で悪用することができます。
- **車両の接続性**：車両の接続性に関する情報は、車両システムや関連インフラに対する標的型サイバー攻撃を行うために悪用されうる。例として、車の Wi-Fi 接続がリモートでの車両ハッキングに使われることがあります<sup>43</sup>。
- **脅迫行為**：攻撃者がドライバープロフィールを作成し、位置情報やその他の機密データを公開することをちらつかせて脅迫することができます。未申告の事故や車両の不具合についての情報を公開すると脅して、人を脅迫することができます。
- **保険詐欺**：急ブレーキや急加速、過度のスピードといった運転習慣に関するデータを操作し、ドライバーを低リスクとして示して保険料を不正に低くすることができます。

これらは、コネクテッドカーにおけるサイバー脅威のデータ中心の範囲を絞ったリストとなります。なお、トレンドマイクロのリサーチペーパー「Identifying Cybersecurity Focus Areas in Connected Cars Based on WP.29 UN-R155 Attack Vectors and Beyond」<sup>44</sup>では、さらにサイバーセキュリティのリスク評価のフレームワークである DREAD 脅威モデリング評価を含み、サイバー脅威の網羅的なリストを提供しています<sup>45</sup>。

自動車データの収益化と使用が拡大するにつれ、サイバー犯罪者による悪用のリスクも増大しています。車両の追跡から保険詐欺まで、多岐にわたる脅威は、自動車業界及びデータ中心の関連企業に対する堅固なサイバーセキュリティ対策の急務を浮き彫りにしています。同時に、規制当局は運転者と乗客を守るためのデータプライバシーと保護の法律を策定し、施行する必要があります。この変化する環境を操縦するには、革新を促進し、セキュリティとプライバシーを保証するバランスの取れた取り組みが、コネクテッド車の将来を形作る上で必要です。

---

<sup>43</sup> <https://keenlab.tencent.com/en/2020/01/02/exploiting-wifi-stack-on-tesla-model-s/>

<sup>44</sup> [https://documents.trendmicro.com/assets/white\\_papers/wp-a-roadmap-to-secure-connected-cars.pdf](https://documents.trendmicro.com/assets/white_papers/wp-a-roadmap-to-secure-connected-cars.pdf)

<sup>45</sup> <https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/dread-threat-modeling-intro/>

## 5. コネクテッドカーにおけるミドルウェア API について

現代のコネクテッドカーは、車輪のある巨大なスマートフォンに変わりつつあります。ここでは、第三者によるクラウド接続アプリが運転手や乗客の体験にとって重要な役割を担っています。この動きは、物理的なボタンを廃止し、完全デジタル化されたコックピットへの切り替えを行う高級車メーカーから始まりました。デジタル、またはスマートコックピットは、現在では中価格帯の車両にも普及しています。これらは、気候制御、ラジオ、ハザードライトといった通常の車の機能を管理するアプリケーションの実行に加え、地図、インターネットラジオ、ウェブブラウザ、動画ストリーミング、ソーシャルメディア、メッセージング、仮想アシスタントといった第三者アプリケーションも実行できます<sup>46, 47</sup>。

図5では、私たちが考えるクラウドコネクテッドカーのエコシステムを示しています。ヘッドユニットではアプリケーションの実行がサポートされ、E/Eの詳細を抽象化し、開発者が車載アプリを容易に構築できるミドルウェア層が存在します。このミドルウェアはゲートウェイ ECU と通信し、ECU へのメッセージを送る必要があるアプリケーションへの API アクセスを提供します。バススイッチは、パケットを目的の ECU にルーティングします。アプリケーションは、携帯電話からのテザリングされたセルラー接続、あるいは TCU 内蔵の eSIM を通じて、OEM クラウドや Netflix、Google といった第三者クラウドと通信することが可能です。車の E/E アーキテクチャによっては、ゲートウェイ ECU が直接クラウドサービスと通信することもあります。車がより多く接続され、賢くなるにつれて、車専用のアプリが開発されるようになります。そして、OEM および T1/T2 サプライヤーによるアプリ開発者が登場することでしょう。OEM アプリはミドルウェアを介さずにゲートウェイ ECU へアクセスすることが多いですし、バススイッチと直接通信することもあります。

ミドルウェア API はスマートコックピットを搭載した自動車の豊かなエコシステムを創出しますが、同時に車の電気・電子 (E/E) アーキテクチャや電子制御ユニット (ECU) への API アクセスを通じて、サイバー犯罪者に新たな機会を提供することにもなります。これは、アーキテクチャに依存しないリモートアクセストロイの木馬 (RAT)、ランサムウェア、フィッシング攻撃を通じてインストールされるボットネットマルウェアなど、多種多様なマルウェアの出現につながりかねません。さらに、脱獄した携帯電話を車に接続し、車内にマルウェアをインストールする攻撃方法も考えられます。反面、OEM のクラウドへの攻撃は車の機能を無効にし、個人情報漏洩、走行中の制御喪失、収益の減少など、様々な問題を引き起こす可能性があります。クラウド API は車の特定、解錠、始動、盗難、または車内の貴重品の盗難に利用される可能性があります。

<sup>46</sup> <https://www.volvocars.com/intl/v/connectivity/infotainment-page>

<sup>47</sup> <https://www.amazon.com/alexa-auto/b?ie=UTF8&node=17744356011>

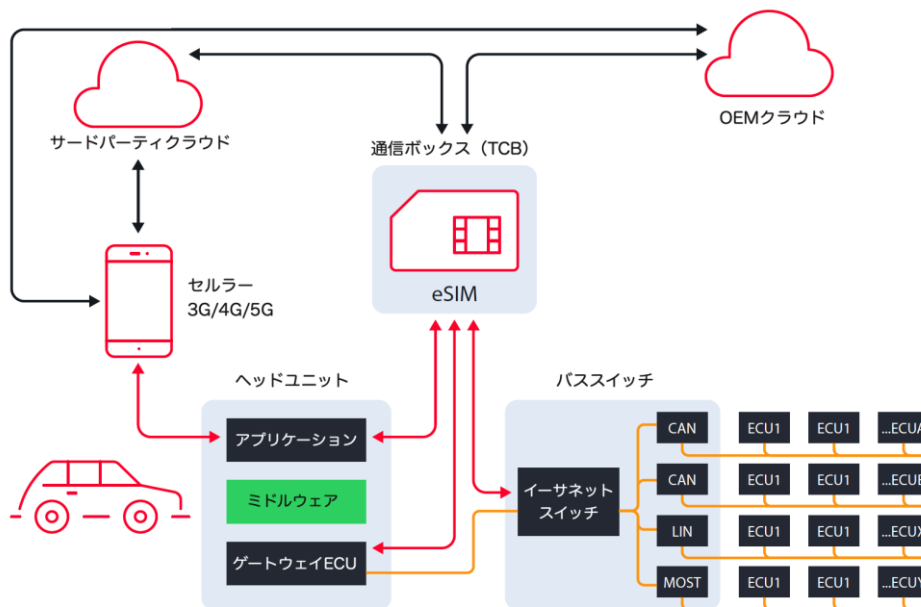


図5：クラウドコネクテッドカーのアーキテクチャ

2023年1月に公開されたブログ記事で、ウェブアプリケーションセキュリティリサーチャーである Sam Curry 氏は、OEM のテレマティクスシステムと API の脆弱性を悪用して、様々な OEM のバックエンドクラウドインフラにアクセスした方法を示しました。特に Mercedes-Benz では、公開されているウェブサイトが車の修理工場向けに作られており、社員の LDAP（軽量ディレクトリアクセスプロトコル）システムと同じデータベースに書き込むことが判明しました。このサイトに登録することで、同氏は、従業員用アプリケーションへの限定的なアクセスを獲得し、その後、Mercedes-Benz の GitHub に含まれる顧客車両と通信するためのアプリケーション構築の詳細な指示を含む、敏感な内部アプリケーションへのさらなるアクセスを得ました<sup>48</sup>。

自動車業界は従来、安全性をセキュリティより優先してきました。セキュリティ対策は、規制要件によってのみ実施されることが多くなります。包括的なセキュリティ対策が不足していると、接続された車両がサイバー脅威にさらされるリスクがあります。特に、ミドルウェア API が普及すると、自動車の E/E システムや ECU への容易なアクセスを通じて、サイバー犯罪者の主要な攻撃手段となる可能性が高まります。多様な既存のマルウェアやサイバー攻撃方法を使用して、車を侵害することが容易になります。したがって、自動車業界はこれらのセキュリティのギャップに積極的に取り組み、規制の遵守を超えたサイバーセキュリティフレームワークの開発が求められます。

<sup>48</sup> <https://samcurry.net/web-hackers-vs-the-auto-industry/>

## 6. オープンな MQTT サーバーから収集された車両データ

MQTT は、マシン同士の通信（M2M）に特化した軽量なパブリッシュ・サブスクライブ型のメッセージングプロトコルです。これにより、帯域幅や電力が限られた不安定なネットワーク環境下でも、デバイス間のメッセージのやり取りが可能になります。これまでも、産業用インターネット・オブ・シングス（IoT）環境における MQTT のセキュリティ問題を調査したトレンドマイクロ社の研究論文<sup>49</sup>を含め、暴露された MQTT ブローカーに関する広範な先行研究があります。

今回の調査で MQTT を通じて漏洩した車両データを追跡したところ、いくつかのオープンブローカーを発見され、これらは認証やパスワード保護を欠いており、接続された車両から利用されていました。これらのブローカーは世界中に分散しており、転送されていたデータには車両の GPS 情報、エンジン監視、車両追跡システム、OBD データなどが含まれていました。

当初、OEM から直接車両データへのアクセスを希望していましたが、残念ながらそのアクセスは許可されませんでした。データ分析実験には、OEM の提供するものほどではないにせよ、実際の車両データが必要でした。そこで、公に共有されているオープンな MQTT サーバーから車両データを探し、それを購読して収集する方法を模索しました。はじめは見込みが薄いと思っていましたが、予想外にも多数のオープンな MQTT サーバーがリアルタイムの車両データを放送しており、これらは今回の調査におけるデータ分析実験に適していることがわかりました。

**注：なお、オープンな MQTT ブローカーにデータを送信することはありませんでした。**多くのオープンまたはセキュリティが不十分な MQTT サーバーは、任意の購読者からの書き込み指令を許可していますが、これはデータ汚染の攻撃によるリスクをもたらします。私たちは慎重に行動し、車両データをリスニングしていたオープンな MQTT ブローカーに一切のデータを送信しないようにしました。収集したデータのかなりの部分は公共交通機関に取り付けられた GPS ユニットからのもので、12 の国際都市での公共交通機関を追跡することができました。公共交通のデータは公開情報であるため、リアルタイムに近い GPS 座標、進行方向の角度、タイムスタンプ、高度、速度を含む情報を見つけることは予想されていました。これらのデータポイントを活用して、ドイツ・ケルンの市バスのルートをアニメーションで表現することができました。また、公共交通データは政府の公式ウェブサイトでも提供されており、私たちはこれを使用して結果を確認しました。

---

<sup>49</sup> [https://documents.trendmicro.com/assets/white\\_papers/wp-the-fragility-of-industrial-IoTs-data-backbone.pdf](https://documents.trendmicro.com/assets/white_papers/wp-the-fragility-of-industrial-IoTs-data-backbone.pdf)



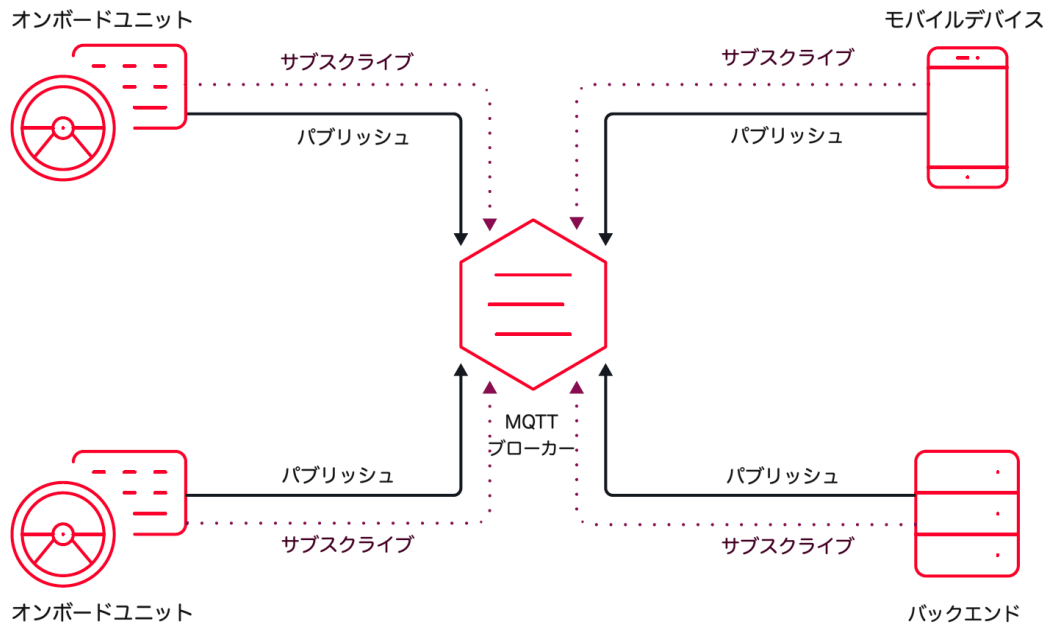


図 6：MQTT ブローカーが車載ユニット（OBU）や購読者のモバイルデバイスと交信する様子を示した機能図

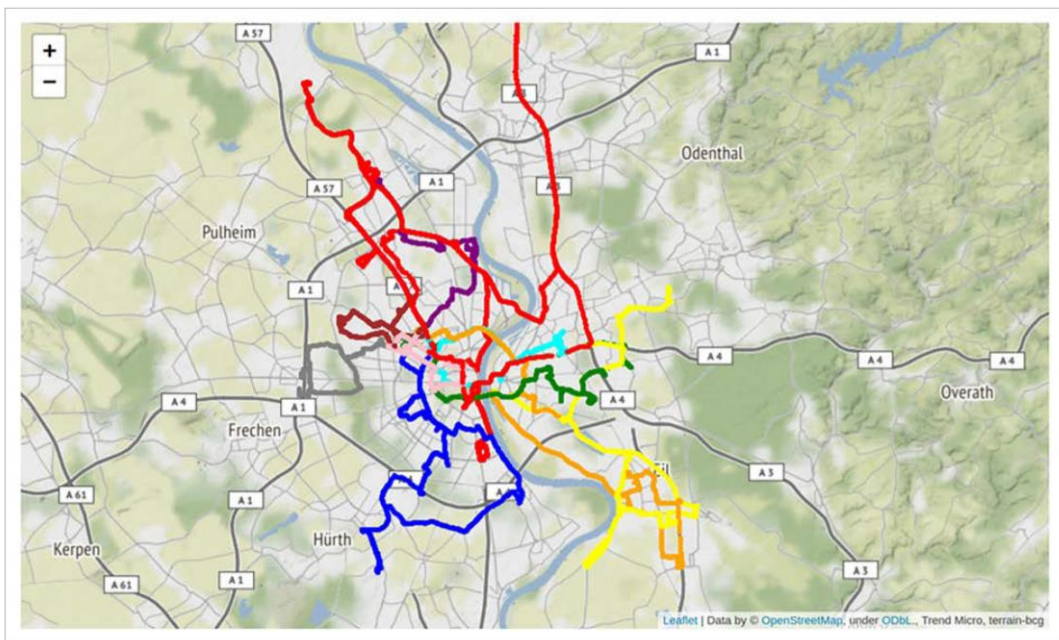


図 7：オープンな MQTT ブローカーから収集したデータに基づいて描かれたドイツ・ケルンの公共交通路線

Vehicle ID	Company ID	Speed (km/h)	Latitude	Longitude	Altitude (m)	Odometer	Fuel Level (%)	Inside Passenger Temp (°C)	People Onboard	Remaining Range (km)	State Of Charge (%)	Total People In Onboard	Total People Out Onboard
3350-377419	7	15.27	60.504899974912405	5.056600011885166	59.0	1330198	11	-	0	-	-	0	0
3350-453003	45	0.0	60.35521217621863	5.367395952343941	83.0	29360	100	21	-2	-	100	21	23
3350-377413	7	0.0	60.44610000215471	5.170960016548634	48.0	792925	97	-	-1	-	-	3	4
3350-453146	45	0.36	60.4024419374764	5.320996334776282	4.0	785640	-	21	7	288532	87.2	16	9
3350-453102	45	0.0	60.37250856868823	5.35939316265285	58.0	32590539	-	22	15	335284	87.2	18	3
3350-387155	35	0.02	60.28810003772378	5.261810040101409	51.0	994855	48	-	0	-	-	1	1
3350-377311	7	0.39	60.38730002939701	5.345899965673685	42.0	1328877	89	-	7	-	-	7	0
3350-453155	45	0.0	60.34969512373209	5.287786312401295	46.0	1470766	100	21	0	264129	93.2	0	0
3350-135621	31	19.97	60.379347279667854	5.344253098592162	2.0	617032	-	-	1	-	-	3	2
3350-377445	7	17.04	60.35550001077354	5.104899974539676	26.0	1935529	98	-	10	-	-	10	0
3350-387051	35	0.0	60.3887999650538	5.318940002471209	17.0	1343661	100	-	0	-	-	9	9
3350-453113	45	0.0	60.37190314382315	5.358281973749399	57.0	1050854	100	21	0	334932	98.8	0	0
3350-387082	35	0.0	60.20410004071891	5.445380005985498	67.0	686932	100	-	-1	-	-	4	5
3350-135743	31	0.0	60.37350856868823	5.35939316265285	58.0	32590539	-	22	15	335284	87.2	18	3
3350-387155	35	0.02	60.28810003772378	5.261810040101409	51.0	994855	48	-	0	-	-	1	1
3350-377311	7	0.39	60.38730002939701	5.345899965673685	42.0	1328877	89	-	7	-	-	7	0
3350-453155	45	0.0	60.34969512373209	5.287786312401295	46.0	1470766	100	21	0	264129	93.2	0	0
3350-135621	31	19.97	60.379347279667854	5.344253098592162	2.0	617032	-	-	1	-	-	3	2
3350-377445	7	17.04	60.35550001077354	5.104899974539676	26.0	1935529	98	-	10	-	-	10	0

図 8：MQTT を通じてノルウェーの公共バスから収集されたデータの例。乗車している乗客数が含まれる

MQTT を通じて収集された車両データの分析から、いくつかの興味深いデータポイントが明らかになりました：

- **デバイスコード**：これらはオンボードユニット（OBU）で使用されるデバイス識別のための内部コードです。
- **ドライバーの身元**：実名は開示されていませんが、「company-035-driver」のような識別子を通じて、複数のドライバーを特定することができました。これらは彼らの雇用主を示唆しています。
- **ナンバープレート**：ほとんどが Base64 で暗号化されエンコードされていましたが、12 枚以上のプレートが平文であることが判明しました。
- **住所**：いくつかのデータセットでリアルタイムのおおよその住所情報が利用可能でした。

## 6.1 ドライバーのプロファイリング

MQTT データを用いた調査で、私たちは以下の質問をしました：どのようにしてドライバーをプロファイル化できるのか？また、何をプロファイル化するのか？

- **ドライバーの行動分析**：加速、ブレーキ、速度超過、運転スタイルなど。
- **ドライバーの効率分析**：最終トリップの燃料消費量、走行距離、電気自動車のバッテリー利用によるエネルギー消費など。
- **ドライバーの利用状況**：エンジンの総稼働時間、累積走行距離、平均走行距離などの指標。
- **安全性分析**：事故地点、事故の重大さ、インジケーター灯の状態、ブレーキや速度超過、加速の統計データなど。
- **ルート最適化**：地理位置情報と車速を分析して、各ドライバーの走行ルートを把握。
- **時間管理**：車両の時間状態、トリップの概要、最後のトリップ情報などを用い、ドライバーが運転に費やす時間と休憩時間をモニタリング。

MQTT データは公にブロードキャストされており、私たちはデータを購入していなかったため、細かく制御することができませんでした。これらの制約のもとでドライバーのプロファイル作成を試みたところ、興味深い結果が得られました。

Driver Name	Plate Number	Vehicles' Addresses	Speed (in units)	Latitude	Longitude	Captured Time	Angles	Height
10	10		0, 0			09:05:07, 09:01:11	297, 0	16, 39
36	36		13.202908, 0, 0, 13.869628, 0, 13.888108			10:52:16, 10:05:51, 10:13:00, 10:21:00, 10:25:40, 10:25:40	153, 216, 37, 343, 37, 160	22, 12, 22, 21, 19, 16
68	68		0, 0			10:40:19, 10:25:40	265, 36	26, 22
79	79		15.277148, 0			10:51:06, 12:11:46	238, 344	6, 24
82	82		0, 13.888108, 0, 10, 0, 12.332468			10:39:30, 10:25:40, 10:11:11, 10:21:00, 10:21:00, 12:11:46	349, 36, 120, 151, 148, 161	20, 19, 18, 15, 28, 24
99	100		11.147188, 6.480748			10:52:16, 10:21:00	258, 259	20, 19
105	105		0, 0, 0			10:51:16, 10:11:46, 11:21:00	151, 149, 149	23, 15, 29
125	125		11.591688, 0, 0			10:25:35, 10:25:40, 10:21:00	251, 256, 77	1, 18, 23
200	200		0, 0, 0, 13.369588			10:39:30, 10:52:16, 10:21:00, 10:11:46	176, 176, 0, 77	22, 22, 19, 23
208	208		0, 10.091548, 0, 0			10:51:16, 10:21:00, 10:11:46, 10:11:46	131, 149, 151, 78	40, 27, 27, 26
332	332		0, 0			10:25:40, 09:01:11	146, 0	16, 39
335	335		12.017628, 0, 0, 0, 0			10:40:21, 10:05:56, 10:11:11, 10:21:00, 10:11		

図 9：MQTT データを用いたドライバープロファイリング。プライバシー保護のため、識別子を伏せている

重要な事実の 1 つがすぐに明らかになりました：より多くのデータがあれば、それだけプロファイリングは改善されます。車両データを並べ替えて分析した後、1 日分の GPS データを KML ファイル (Keyhole Markup Language) にエクスポートし、Google Earth に読み込みました。その結果、その日におけるドライバーの活動全体を示す画像が得られました。

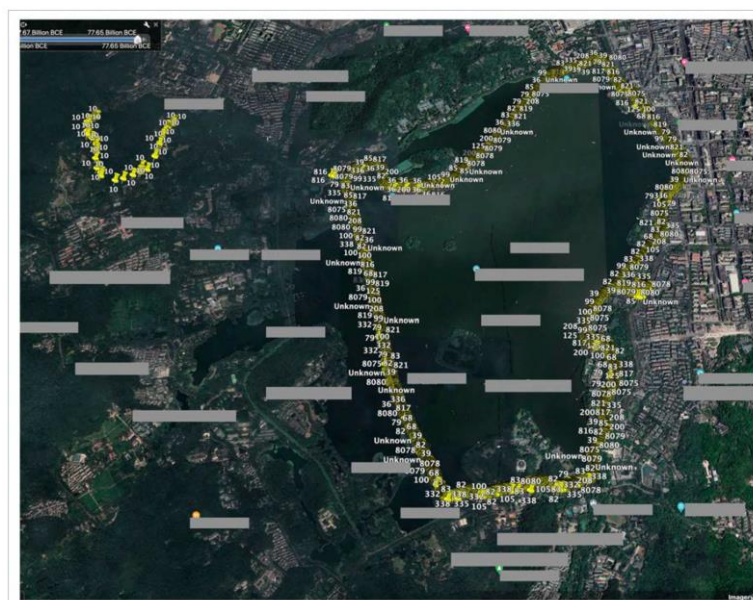


図 10：MQTT を介して収集された例示データ。これを用いてドライバーのプロファイリングと、Google Earth でのルートマッピングを行なった。プライバシー保護のため、地名は伏せている

地図上の画像は、専門的な配達サービスのもので一致しています。もし一般的な配達サービスであれば、都市中にデータポイントが散見されるはずですが、MQTT データからは、各ドライバーの正確な配達先住所も把握できました。これらのデータを長期間にわたって分析することで、各住所の配達パターンやドライバー個々の定期的なルートを特定することができます。地図上のラベルはプライバシー保護のために伏せられていますが、ビジネス名は Google マップ上で確認できました。この可視性により、我々は漏えいした車両データを使って顧客のビジネスもプロファイリングすることが可能です。

## 6.2 その他の確認事項

医療車両向けの GPS プラットフォームからのデータも検証しました。このデータは本来公開されるべきものですが、分析を進めた結果、これらの車両に搭載されている OBU ユニットの具体的なモデルと、各ユニットに紐づけられた電話番号を特定することができました。この事実は、これらの電話番号を介してリモートでの脆弱性が引き起こされるリスクを浮き彫りにしています。

今回の調査では、MQTT ブローカーが非公開のデータを共有している事実を発見しました。そのデータには以下のような情報が含まれています：

- SIM カードに記録された ICCID（集積回路カード識別番号）
- GSM の信号強度
- 温度センサーの情報
- エアコンの作動状態
- 曇り止め装置の状態
- 再生中のラジオ局の情報
- IMEI（国際モバイル機器識別番号）を用いた OBD データ
- ABS（アンチロックブレーキシステム）、エアバッグ、ブレーキ、クリアライト、クラッチ、フォグライト、ヒーター、ハイビームライト、ホーン、左方向指示器、ロービームライト、減速装置、リバースギア、右方向指示器、ドアセンサー、衝突警報、危険警報、緊急警報、疲労警報、オイル警報、盗難警報、車両転倒警報などのリアルタイム状態
- 電気自動車のバッテリー管理システム（BMS）の状態とバッテリー電圧情報

今回の調査では、空港のサービス車両のデータも発見しました。これにはトラクター、除氷トラック、軽トラック、中型トラック、電動乗客バス、廃水トラック、はしご車などが含まれており、それぞれのナンバープレート番号も記録されていました。空港の滑走路側で使用されるサービス車両には、安全確保と追跡のために ADS-B（自動従属監視放送）送信機が装備されており、Flightradar24<sup>50</sup>などのフライト追跡サイトで追跡できますが、ナンバープ

---

<sup>50</sup> <https://www.flightradar24.com/>



レート番号付きでオープンな MQTT サーバー上にこのデータが存在するのは注目に値します。

公開された MQTT サーバーを通じて、意図的にもそうでなくても送信される車両データは、サーバーの開かれた性質上、誰でもアクセス可能です。今回の分析で示されたように、このデータはドライバーやサービスの詳細なプロフィールを作成し、その活動や運営に関する洞察を提供するために使用することができます。これは、データの不正使用や悪用がドライバー、乗客、そして車両群の安全とプライバシーを危険にさらすというセキュリティ上の懸念を引き起こします。さらに、運用上の敏感なデータが不適切な者の手に渡れば、サービスが混乱する可能性もあります。多くのオープンまたはセキュリティが不十分な MQTT サーバーは、任意の購読者からの書き込み命令を受け入れており、これがデータ汚染攻撃のリスクを高めています。そのため、車両データが適切に保護され、安全かつ認証されたチャンネルを通じた伝送を確実にすることが不可欠です。



## 7. 車両 API データに関する研究

今回の調査では、車両データをさまざまなソースから収集し、それらがどのような場所で見つけられるかを特定することを主目的としています。この方法で、前節で話したように、MQTT を通じて共有されている車両データを発見しました。また、適切な調査を行うため、トレンドマイクロのテレメトリデータも調べ、私たちのログ内で車両と OEM/T1/T2 クラウド間の API 通信を確認しました。複数の車両 API リクエストの 카테고リーを識別し、その中から一部を例示データとともにここに提示します。プライバシーを守るため、一部のデータフィールドは非表示にしています。

### Telematics

```
1 [REDACTED].com,/here-fleet-telematics/v2/calculateroute.json?x-api-key=[REDACTED]&ff&mode=fastest;bus;traffic:disabled;&language=de-DE&height=400cm&instructionFormat=text&routeAttributes=sh,bb&legAttributes=mm&maneuverAttributes=direction,action&speedFcCat=85,75,60,45,,,,;85,75,60,45,,,,;85,75,60,45,,,,;85,75,60,45,,,,;85,75,60,45,,,,;85,75,60,45,,,,&departure=2023-03-15T20:00:00&restTimes=EU&waypoint0=[REDACTED]&waypoint1=[REDACTED]
```

**テレマティクス：**この API コールは、OEM のフリートテレマティクス API に対するルート計算リクエストのようです。これは、高さ 400 センチメートルのバスに対して、交通状態を無効にして最速ルートを計算します。リクエストにはルート、レグ、マニューバー属性が含まれ、テキスト形式で指示が提供されます。出発時刻が設定されており、EU のドライバー休息時間も考慮されています。ルートは、緯度と経度で指定された始点から終点まで計算されます。

### Doors

```
US""":80""":[REDACTED].com""":4""GET""/experimental/connectedvehicle/v1/vehicles/YOUR_VEHICLE_ID/doors""443""com:443/""67""200""81""HTTPS""2023-03-23 15:50:50.000""""""web""2023-03-23-15"
```

**ドア：**この API コールは、特定の車両のドアの状態（施錠・解錠、開閉）を取得するもののようです。車両は「YOUR\_VEHICLE\_ID」という仮の ID で識別され、実際のリクエストでは本物の車両 ID に置き換えられることになります。

### Remote Start

```
CA,T, [REDACTED]:443,-,-, [REDACTED].GET,443,90,200,71,HTTPS,2023-03-27 12:13:45.000,, [REDACTED],https:// [REDACTED]/remote/start, [REDACTED] Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36""web,2023-03-27-12
```

**リモートスタート：**この API コールは、車両を遠隔でスタートするための OEM の API に対する POST リクエストです。

### Climatization

```
"DE""PT"" [REDACTED]""US"" [REDACTED]"" [REDACTED]"" [REDACTED]""/vehicle/v1/vehicles/[REDACTED]/climatization/stop""443""90""200""71""2023-03-01 06:50:40.000""TRE"" [REDACTED]""web""2023-03-01-06"
```



イバー攻撃に脆弱であることは周知の事実であり、侵害されるとボットネットマルウェアのような悪質なソフトウェアがインストールされる恐れがあります<sup>51</sup>。ボットネットマルウェアはネットワークトラフィックを傍受し、機密データを抜き取ることができます<sup>52</sup>。トレンドマイクロは、ルーターが侵害された際のデータ流出方法について調査したリサーチペーパーを発表しています。自宅のルーターが攻撃を受けマルウェアに感染すると、車両アプリとOEM/T1/T2 クラウドバックエンド間の安全でない API 通信が傍受されることがあり、これが車両データのセキュリティとプライバシーにとって脅威となります。その結果、機密性の高い車両データの不正アクセス、車両機能の改ざん、または車両の位置追跡など、車の所有者のプライバシーと安全に対する重大なリスクが生じる可能性があります。

---

<sup>51</sup> <https://www.trendmicro.com/vinfo/us/security/news/home-router>

<sup>52</sup> <https://documents.trendmicro.com/assets/wp/wp-securing-your-home-routers.pdf>

## 8. 結論

現代の車両は、複雑なデータの集積点へと進化しました。車両データを中心としたエコシステムが発展し、データは収集され、分配され、革新的な方法で利用されています。しかし、このようなデータ中心のエコシステムには、独自の課題が伴います。特に、ドライバーはデータの生成、転送、共有についての認識や制御が不足している状況です<sup>53, 54, 55, 56</sup>。これは彼らの日々のデジタル足跡に不確実性をもたらし、データプライバシーに関する深刻な懸念や、データの悪用、乱用への恐れ、そして車両メーカーへの信頼問題を引き起こしています。

車両データは、API やアプリケーションなど、多くの経路を通じてアクセス可能です。その使用は大きな潜在力を秘めており、自動車産業の主要な収益源となるでしょう。しかし、車両データの匿名性を深く掘り下げると、懸念が生じます。完全に匿名化された車両データは、プロファイリングが困難になるため価値を失い、プロファイリング（個人的なものであれ集団的なものであれ）がなければ、収益化を実現するのは難しい課題となります。従って、本当に完全に匿名化された車両データは存在しないと考えられます。収益化が進み強力な収益を生み出すことは、避けられずサイバー犯罪者を惹きつけるでしょう。リスクは明白であり、接続された車両に対する最初の大規模攻撃はデータを対象とすると予想され、それは車両のハッキングやフリートの乗っ取りといったより顕著な攻撃へと発展する可能性があります。したがって、車両データの保護が極めて重要になっています。

運転手が自分のデータを共有することで報酬を受け取る新ビジネスモデルの出現は、プライバシー保護と技術進歩を両立させる潜在力を持っています。これは、データ共有が都市生活をスムーズにするスマートシティ構想とも一致しています。しかし、車両データの収集と使用における法的な不備にも取り組む必要があります。自動車業界は、規制の空白地帯で効率的に機能することはできません。適切な法律は、明確性と安定性を確保するために不可欠です。関係者はこの問題の重要性を認識し、解決策を模索することが急務です。

自動車と技術の収束は膨大な機会をもたらしますが、慎重な舵取りが求められます。OEM、T1、T2 サプライヤー、そしてデータブローカーは、車両データエコシステムにおける重要な役割を担っています。彼らの行動と決断は、運転者の安全、プライバシー、そして総合的な体験に大きく影響を及ぼします。だからこそ、これらの関係者が先手を打ち、責任を持っ

---

<sup>53</sup> <https://www.newsnationnow.com/business/tech/car-data-collection-protect-yourself/>

<sup>54</sup> <https://mashable.com/article/privacy-please-what-data-do-modern-cars-collect>

<sup>55</sup> <https://www.consumerreports.org/automotive-technology/who-owns-the-data-your-car-collects/>

<sup>56</sup> <https://www.wired.com/story/car-data-privacy-toyota-honda-ford/>

てデータを取り扱い、その悪用や乱用を防ぐことが極めて重要です<sup>57</sup>。これと並行して、車両データの収集と利用における規制のギャップを埋めることも必要です。

自動車データのサイバーセキュリティを向上させるための5つの提言は以下のとおりです：

1. **強力なデータ保護策の導入**：車両が多くデータを生成し、さらに接続されるようになるため、データ保護の強化が不可欠です。これには、データの暗号化、安全な API、セキュアなクラウドストレージが含まれます。セキュリティ監査や侵入テストを定期的実施し、脆弱性を特定し修正することが重要です。
2. **ユーザーへの情報提供**：多くのドライバーは、自分の車がどれほどのデータを収集し、それがどのように利用されているのかについて、理解が不足しています。OEM や他の関係者は、データ収集の方法、リスク、データ保護の方法についてユーザーに情報を提供すべきです。これには、わかりやすいプライバシーポリシーやデータ収集設定の調整方法、完全にオフアウトする方法の案内が含まれるべきです。
3. **車両 API のセキュリティ強化**：API はサイバー犯罪者のアクセスポイントとなることがよくあります。したがって、車両 API のセキュリティを強化することが優先事項です。これには、強固な認証手段、アクセス制限、API 活動の監視と記録を通じて不審な活動を検出し対応することなどが含まれます。
4. **データ収集と使用の規制**：車両データの収集、保管、利用を規制する明確なルールが必要です。これには、データへのアクセス権、保管期間、利用目的などが明確に定められるべきです。規制機関は、ドライバーを守るデータプライバシーと保護の法律を策定し、施行する必要があります。
5. **セキュアなミドルウェア API の開発**：接続された車両のミドルウェア API は、車両の E/E アーキテクチャや ECU へのアクセスをサイバー犯罪者に提供するリスクがあります。このため、これらの API はセキュリティを考慮して設計され、強力な認証と暗号化を含むべきです。

自動車業界がスマート車両とデータ経済に進むにあたり、革新を促進しつつプライバシーとセキュリティを維持するバランスを見つけることが重要です。

---

<sup>57</sup> <https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/>



## 付録：車両ネットワークアーキテクチャ

接続車両は主に無線で通信しますが、電気自動車（EV）が電源に繋がれている際に電力線を通じてグリッドや他のバックエンドインフラと通信するなど、例外も存在します<sup>58</sup>。現代の接続車両には、その多様性が車の種類に匹敵するほど様々な内部ネットワークアーキテクチャがあります。コンポーネントは標準化されたプロトコルを用いて通信しますが、全く同一のネットワークアーキテクチャは存在しません。これは、同じメーカーの異なる車種やモデルでさえも異なることがあります。車内でデータがどのように生成され、どのように利用されるのかを理解するために、ネットワークアーキテクチャの高度な理解が必要です。

車内部品との機能と相互作用を解析するために、今回の調査では、一般的な車両ネットワークアーキテクチャを作成しました。これは実際の生産車両のアーキテクチャではなく、車両内部ネットワークのネットワークトポロジと主要コンポーネントを理論的に視覚化したものです。

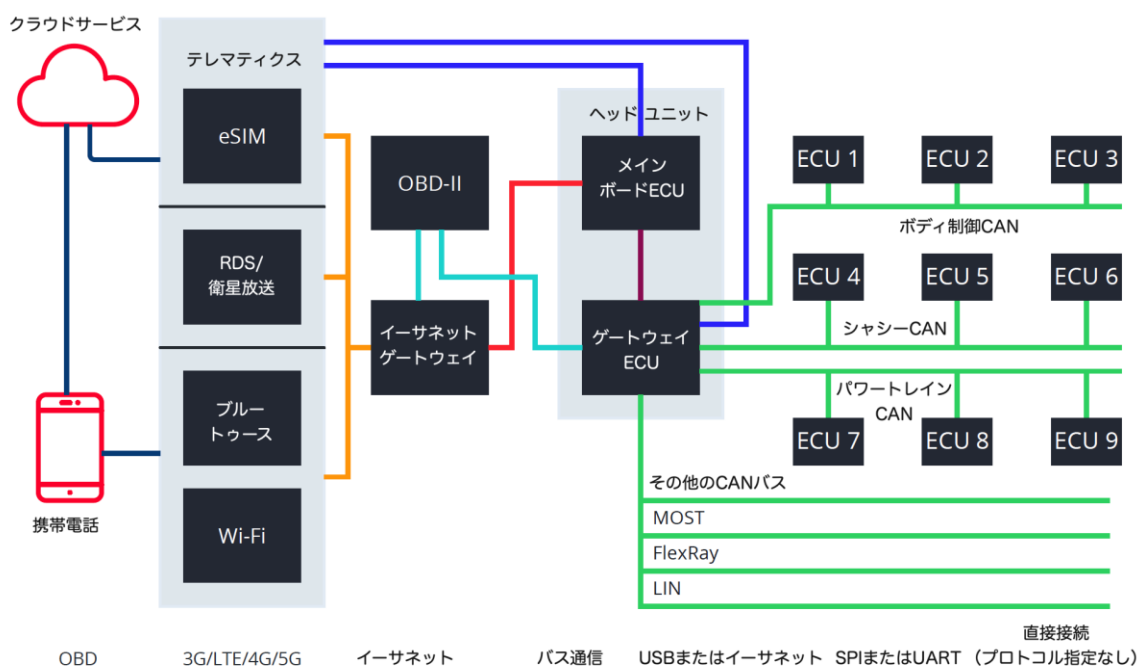


図 11：現代の接続車両の典型的なネットワークアーキテクチャ

今回の調査で作成した一般的な車両ネットワークアーキテクチャでは、主要なコンポーネントとそれらの相互作用は次のようになります：

- **テレマティクス制御ユニット（TCU）**には、車が3G/4G/5Gネットワークに接続するための電子SIM（eSIM）が含まれています。TCUはテレマティクスデータの送信、クラウドバツ

<sup>58</sup> <https://ieeexplore.ieee.org/document/5075439>

クエンドサーバーとの通信、リアルタイムデータの受信、インターネットアクセスの提供などを可能にします。

- **RDS/衛星ユニット**は、FM 放送と衛星放送からデジタル情報を受け取ります。RDS-TMC（ラジオデータシステム - トラフィックメッセージチャンネル）を用いて、車はリアルタイムの交通情報を受信し、**ヘッドユニット**に表示することができます。衛星コンポーネントは、データ通信用のセルラー・衛星接続を実現し、サブスクリプションに基づく交通情報と警告を提供します。
- **Bluetooth** と **Wi-Fi** の接続は、現代の車で一般的です。携帯電話は Bluetooth を介してヘッドユニットに接続され、車両は Wi-Fi ホットスポットを作成して乗客にインターネット接続を提供することができます。また、自宅の Wi-Fi ネットワークに接続して OTA（Over-The-Air）ソフトウェア更新をダウンロードすることもあります。Bluetooth および/または Wi-Fi 経由で車両に接続された携帯電話は、そのセルラーネットワークを通じて車両にインターネットアクセスを提供するためにテザリングを行うことができます。
- **OBD-II** は車のオンボード自己診断システムです。OBD-II ポートはヘッドユニットと通信することができるだけでなく、CAN バスに直接接続して CAN メッセージやコマンドの送受信を行います。
- **イーサネットゲートウェイ**は、無線周波数（RF）モジュールとヘッドユニット間のデータのやり取りを管理します。車両ネットワークによっては、イーサネットゲートウェイがゲートウェイ ECU と直接通信する場合がありますが、今回使用した模範的なアーキテクチャではヘッドユニットを介して通信を行います。
- **メインボードの電子制御ユニット（ECU）**は、ヘッドユニットの中核プロセッサとして機能し、ナビゲーション、ディスプレイ、ラジオの再生、ネットワーク接続の管理、気候制御などを担います。このアーキテクチャでは、SPI（シリアル周辺機器インターフェース）または UART（ユニバーサル非同期受信機-送信機）プロトコルを使用してゲートウェイ ECU と通信し、CAN メッセージやコマンドを送受信します。
- **ゲートウェイ ECU** は、CAN（コントローラーエリアネットワーク）、LIN（ローカルインターコネクトネットワーク）、MOST（メディア指向システムトランスポート）、FlexRay などの異なるバスシステムとの通信を管理します。これらは最も一般的に見られるバスプロトコルですが、他にも存在します。ゲートウェイはアプリケーションがバスに直接通信するのを防ぎ、メッセージを目的のバスに正しく振り分けます。また、メッセージが規格を満たしていることを検証する役割も果たします。
- 車内の各 **ECU** は接続されたバスを通じて通信し、エンジン制御、トラクション制御、ドアロック、気候制御、バッテリー管理、ハイブリッドパワートレイン、エアバッグ、レーダーなどの機能を担当します。



VicOne は、未来の自動車を守るというビジョンを持ち、自動車産業向けに幅広いサイバーセキュリティソフトウェアやサービスを提供しています。自動車メーカーの厳しい要求に応えるために開発された VicOne の各ソリューションは、現代の車両が必要とする高度なセキュリティニーズにマッチし、セキュリティを確保、スケーリングするように設計されています。VicOne は、トレンドマイクロの子会社であり、トレンドマイクロが 30 年以上にわたって培ってきたサイバーセキュリティ技術をベースにしています。これにより、類まれな自動車の保護と深いセキュリティへの洞察を提供し、お客様が安全でスマートな車両を開発できるよう支援しています。

詳しくは VicOne 公式サイト  
[www.vicone.com/jp](http://www.vicone.com/jp) をご確認ください。  
こちらの QR コード  
からもアクセスできます。



IN COLLABORATION WITH

