クルマをツナゲる新たなシステム･アーキテクチャに関する一考察

田中 政志[†1]　伊藤 良浩[†1]　高橋 順子[†1]　大嶋 嘉人[†1]

概要：運転支援や自動走行を筆頭に、遠隔からのリプロやメンテナンス、走行履歴等をもとにしたショップのレコメンドや保険料の割引など、情報ネットワークとの融合により多種多様な自動車向けサービスが実現され始めている。このような状況の中、外部との接続やシステム全体の大規模化、複雑化により、セキュリティ等の面で新たな問題が生じると想定される。本発表では、車を安心・安全・便利にツナゲて、新たなサービスを実現するための各種要件を整理し、通信事業者の観点からそれらに最適と考えられるシステムアーキテクチャを提案する。また、同アーキテクチャ上で特に必要となるサイバーセキュリティ対策機能とその実現に向けた課題について論じる。

キーワード：コネクテッドカー、クラウド、サイバーセキュリティ

A study of new connected car architecture

Masashi Tanaka[†1]　Yoshihiro Itoh[†1]　Junko Takahashi[†1]　Yoshihito Oshima[†1]

Abstract: Recently, new automotive services with the network and the cloud platform have been provided such as remote maintenance systems of the car and recommendations of the stores based on the driving records. Under such circumstances, there are new problems in the aspect of the cyber security caused by connecting the car through the Internet and the complexity of the connected car system. In this paper, we propose the system architectures which are suitable for the connected car from a perspective of telecommunications carrier. We analyze the requirements for the automotive service of connecting the car safely and conveniently. Moreover, we describe the cyber security countermeasures needed for the connected car architectures.

Keywords: Connected Car Architecture, Cloud System, Cyber Security

1. はじめに

近年、クルマを取り巻く環境に大きな変化が生じている。19 世紀末にガソリン自動車が開発されてからほぼ 100 年の間、車は基本的に人が操作して移動する手段として発達してきた。しかし、2000 年代に入ると利便性の向上等のために車とネットワークがつながるようになり、単なる移動手段ではなく、様々な情報を収集する動くセンサとしての側面が大きくなってきている。さらに運転支援技術が AI や ICT 技術と組み合わさって進化した自動運転の研究も盛んに行われ、徐々に「車は人が操作する」ということも自明の前提ではなくなってきている。

このような状況の中、これまで独立したシステムだった車がインターネットに接続されコネクテッドカーとなったことで、サイバーセキュリティが大きな課題となっている。これに対して既存の自動車企業（以下、OEM と記述）は、従来の車にセキュリティ機能を搭載することで対応し始めたところである。一方、Google など新規参入企業は､車というハードウェア自体は他社から調達し、AI 等の高度な技術による高機能なソフトウェアを後付で搭載することで機能追加やセキュリティの課題に対応する方向性を示している。

本論文では、はじめに我々が今後目指すべきと考える自動車サービスのイメージを示し、車を安心・安全・便利にツナゲて、この新たなサービスを実現するための各ステークホルダーの要件を整理し、通信事業者の観点からそれらに最適と考えられるシステムアーキテクチャを提案する。また同アーキテクチャ上で特に必要となるサイバーセキュリティ対策機能とその実現に向けた課題について論じる。

2. 自動車の構造に関する変化

ガソリン自動車は 1886 年にベンツ社等により開発され、その後アメリカを皮切りに世界中で大量生産による大衆化が進み、主要な移動手段として普及していく。第 2 次大戦後のアメリカでは好景気の中で大排気量の大型車が広く普及するが、1970 年代に大気汚染が社会的問題になり厳しい排ガス規制が求められるようになると小型で高性能な日本車の人気が高まり 1980 年代以降世界を席巻した[1]。

排ガス規制はその後も厳しくなり続け、これに対応し

†1 NTT セキュアプラットフォーム研究所
NTT Secure Platform Laboratories

てエンジン等を効率よく制御するための電子制御が1980 年代に本格的に導入され、さらに 1990 年代からは安全性や快適性の向上というユーザからの要求も高まり、車全体を最適に制御するため自動車内部で独立していた電子制御装置（ECU）がネットワーク化されるようになる。また 2000 年代になると、さらなる安全性や快適性向上の観点から ITS（Intelligent Transport Systems）が導入され、自動車は外部から交通情報等を取得するようになった。現在ではカーナビやインフォテイメント機器などがインターネットに接続されることにより、新たなサービスが提供されている[2]。

これらの経緯により、近年、一部の車はインターネット経由で車両内部の制御 ECU にアクセスできるような構造になっていた。そのため、2010 年代になると学会で遠隔から運転者の意図に反した不正な車の操作ができることが発表され、車のセキュリティ確保の重要性が指摘されている[3]。現在は、上記のような不正操作を防ぐための対策の研究開発が進められている。

上記を含め、近年の自動車の構造に関する変化を以下に整理する。

(1) ネットワーク

車両情報の幅広い利活用を促す観点から、専用線等のクローズドなネットワークから、インターネットに代表されるオープンなネットワークを利用するように変化しているが、これに伴いサイバーセキュリティの問題が大きくなっている。

(2) 車載ソフトウェア

車両のコードの肥大化、複雑化に対応するため、AUTOSAR 等の標準プラットフォームやモデルベース開発など、IT 分野で実績のあるオープンな開発環境への転換が進められている。また Google Auto や Apple CarPlay 等､情報系アプリケーションを中心に IT 系企業の参入が増加している。

また、遠隔から簡易かつ安全に車両情報を送受信するために、車に専用の API（以降、ビークル API と呼ぶ）が実装され、この API を利用して車両から取得した情報の利用や車の制御ができるようになり[4][5]、W3C 等の標準化団体においてもビークル API についての検討が進められている[6]。

(3) 車両

従来の車両は各構成要素が複雑に絡み合った典型的なインテグラル型アーキテクチャと言われていたが、近年は個別化による車種の増加等に対応するため各要素が独立したモジュール型アーキテクチャの導入が進んでいる。

また、従来は OEM と系列会社による垂直統合型で、内部にノウハウを蓄積しながらそれぞれが独自に開発をおこなっていたが、開発コストの増大や技術革新のスピードに対応するため、徐々に水平分業型に変化してきている。更に、今まで自動車業界以外の企業が車両情報を活用した新たなサービスを提供し始めている。

3. 2025 年の自動車サービス

2025 年の自動車を取り巻く社会状況として以下のような予測がなされている[7][8]。

・全乗用車の約半数がコネクティドカー
・一般道で自動運転レベル 3 が実現
・交通データを含む様々な情報がオープンデータ化
・ウェアラブルデバイス等により、人やその他あらゆるモノがネットワークに常時接続し情報を提供

これらを前提に、本稿執筆時点から 10 年後にあたる 2025 年において我々が目指すべき自動車サービスのイメージを図 1 に示す。自動車サービスに関与する主なステークホルダーは、自動車の製造販売元である OEM、OEM に自動車部品等を供給するサプライヤ、OEM やサプライヤ以外で自動車サービスを提供する 3rdParty、自動車サービスを利用する利用者である。

本サービスイメージは、自動運転機能を備えたコネクテッドカーが広く普及した社会を前提としている。車と自動車サービスを提供するセンタ間では、モバイル網等を経由して制御情報や様々なデータが相互にやり取りされる。車からは位置情報やセンサ情報等の車両情報、車載部品の動作情報等がセンタ側に提供され、OEM、サプライヤ、3rdParty がこれらのデータを活用してダイナミックマップ提供サービスや車両メンテナンスサービス等を提供する。一方、車にはセンタ側から自動運転のためのダイナミックマップ情報や部品交換等のメンテナンス情報等が送信される。利用者はスマートフォン等から車両遠隔操作サービスを通じて車のエンジンやドア等の制御を行うことができる。また遠隔操作サービスは、テロ対策などのために政府やその他の機関が利用することも考えられる。

行政が提供するオープンデータや人の行動情報（店舗への訪問履歴等）も共有され安全に人や組織が活用することで、車両情報と組み合わせたレコメンドや保険等の新しい付加価値提供サービスが生み出される。また収集されたデータはマーケティングなどの様々な分野で二次利用される。

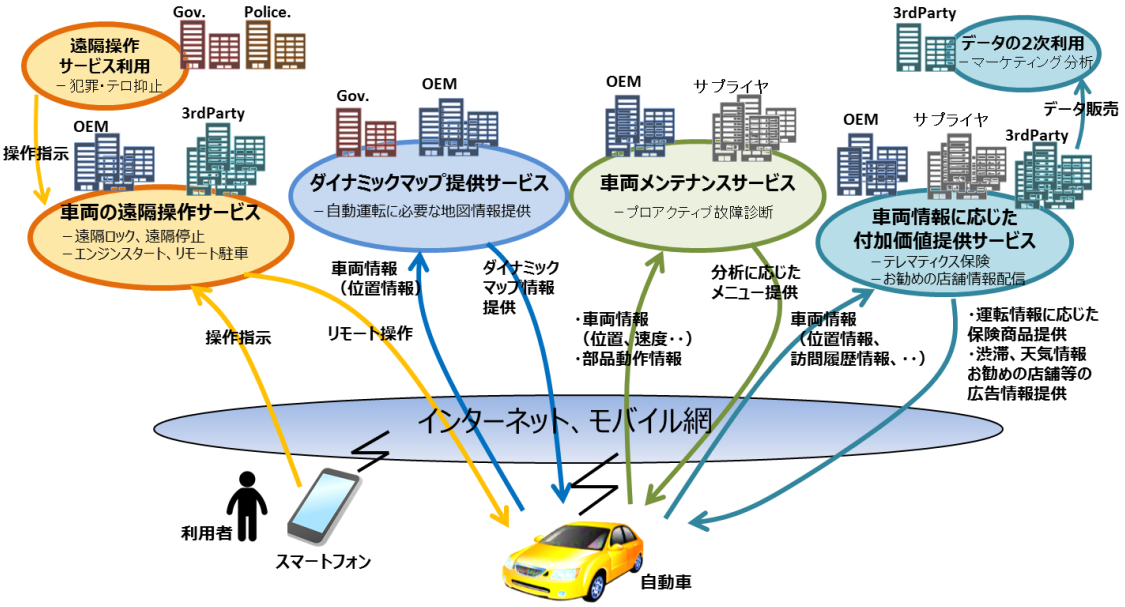


図 1 2025 年の自動車サービスイメージ

このように我々は、車両情報がより自由に活用され様々な人や組織から多種多様なサービスが生み出されることで、車が単なる移動手段ではなく、様々なインフラと融合した快適な動く生活空間となる社会を目指すべきと考える。

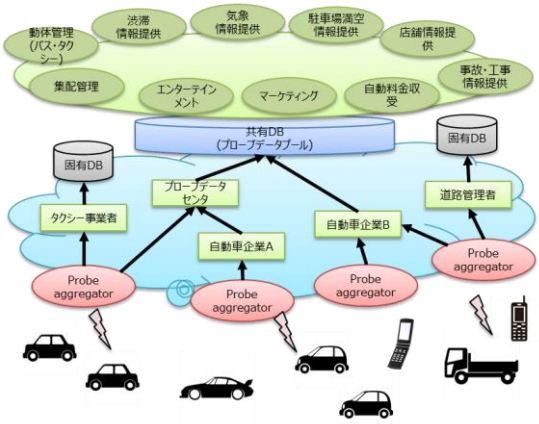
4. 既存研究

本章では、本研究の対象である車両情報を活用したサービスのシステムアーキテクチャに関する既存研究[9][10]を紹介する。

(1) 自動車情報基盤アーキテクチャ

文献[9]では、自動車を「動くセンサ」として捉え、自動車がセンシングする実空間データを活用し、様々なプローブ情報システムを横断的に構築することを実現するデジタル情報基盤（図 2）が提案されている。自動車と様々なサービスシステムを情報通信技術でつなぎ、自動車情報を社会共通の基盤として活用することを目的としている。インターネット経由で自動車企業などが集めた自動車に関するデータは、車種等に依存しない共通のデータ形式に変換されて共通 DB（プローブデータプール）に蓄積される。この共通 DB に集められたデータは標準化された手順で外部から利用することができ、このデータを使ってプローブデータを活用したマーケティングや、走行履歴を基にした運転者向けのレコメンドなど様々なサービスを企業が提供できるようになっている。

本研究は、プローブデータの収集・活用を目的としているため、車からデータを取得し、それを自動運転等に利用することはスコープ外である。



（文献[9] 佐藤(2008)p12 を参考に作成）

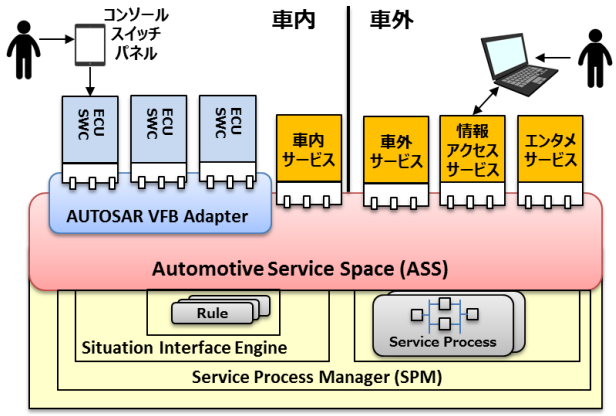
図 2 自動車情報基盤アーキテクチャ

(2) ASPF アーキテクチャ[

文献[10]では、自動車分野のサービス統合システムの課題として、リアルタイム性の保証、安全性・信頼性の保証、車外情報システムの短期製品サイクルへの追従を挙げ、これを解決するために、従来の制御系プラットフォームと情報系プラットフォームにサービスレイヤを追加した新しい車載向けサービスプラットフォーム(ASPF プラットフォーム：図 3)が提案されている。基本コンセプトとして、車外の情報システムのライフサイクルや利用者のニーズに合わせてクルマ内部の機能が拡張できることを目指している。また SOA（Service Oriented Architecture）をレファレンスとすることにより、車内外のサービスを連携・統合して付加価値の高いサービスが安全に提供できるとしている。

本アーキテクチャでは、Web サービスで使われる技術

を活用して車内外のサービスをシームレスに連携するため、情報セキュリティの仕組みが不可欠である。しかし、本研究ではファイアウォールの必要性が述べられている程度で、セキュリティ要件に関する検討等は行われていない。



（文献[10] 岩田(2013)p175 を参考に作成）
図 3 ASPF アーキテクチャ

5. 機能要件とシステムアーキテクチャ

本章では、3 章で提示した 2025 年の自動車サービスに対するステークホルダーの要求について考察し、同サービスを実現するシステム（以降、自動車サービスシステムと呼ぶ）の機能要件をまとめ、自動車サービス向け機能の大部分をネットワーク上のプラットフォームに配置する新しいシステムアーキテクチャを提案する。

5.1 ステークホルダーの要求

各ステークホルダーは自動車サービスに対して次のような要求を持つと考えられる。

OEM は、車に対して最終的な製造責任を持つため、コネクテッドカーや自動運転技術が進んだとしても完成品である自動車の品質や安全性を担保しなくてはならない。そのため車への操作制限等の管理権限は OEM が持つべきと考えるだろう。また、品質向上等の手段として車両情報を活用したプロアクティブな故障診断や製品改善や、車両販売後に車の機能を組みなおすことで新たなサービスを実現する機能を追加できるようにしたいと考えるだろう。また、複雑化する車両のセキュリティ管理に関しては負担を軽減したいと考えるだろう。

サプライヤは、複数の OEM に製品供給するようになってきているため、OEM に依存せずに直接自社のシステムや部品の情報を活用してプロアクティブな故障診断や製品の改善を行いたいと考えるだろう。更に、ユーザーインターフェースを持つ製品の場合、利用者に対して直接的にサービスを提供することによる新たなビジネスモデルを開拓したいと考えるかもしれない。

3rd Party は、幅広い利用者に継続的にサービスを利用してもらうため、車の機能や車種の違い等を意識せずに簡易にサービスアプリケーション開発を行い、サービスのトレンドに合わせてタイムリーにアプリケーションを提供したいと考えるだろう。

利用者は、前述の通り、車を単なる移動手段ではなく、快適な動く生活空間として捉えるようになる。様々なサービス提供者から多種多様なサービスが提供され、それらの中から利便性や経済性の観点で最適なものを取捨選択して利用したいと考えるだろう。また、車を乗り換えても同じサービスを利用できることや、逆に、車を乗り換えることなく新しいサービスを利用できることを望むだろう。

5.2 自動車サービスの機能要件

5.1 節で示した各ステークホルダーの要求に基づき、自動車サービスシステムに求められる機能要件に関して述べる。

(1) 自動車に関する要件
- A) ネットワークが遮断された際にも車の基本機能（走る、曲がる、止まる）を実行できる。
- B) 車の外部から車の情報を参照することができる。
- C) 車の外部から車の制御機能にアクセスできる。
- D) 販売後、車の機能の向上や追加が簡単にできる。

(2) サービス用アプリケーション開発に関する要件
- A) アプリケーションの開発、改造を OEM やサービス提供者が容易にできる。
- B) 同じアプリケーションで複数の車種にサービス提供できる。

(3) サービス提供に関する要件
- A) 開発したサービスをサービス開発者が迅速に提供、改善できる。
- B) 車の長いライフサイクルを通じて、新しいサービスの追加、変更ができる。
- C) 利用者が車を乗り換えても同じサービス（過去の走行履歴、各種設定等）を継続して利用できる。

(4) 情報セキュリティに関する要件
- A) 自動車サービスシステムの更新や管理ポリシの設定・施行を OEM やサービス提供者が容易にできる。

5.3 システムアーキテクチャの提案

本節では自動車サービスシステムのアーキテクチャの

提案を行う。まず、5.2 節で検討した機能要件に基づき、機能配置の方針について述べる。

(1)　自動車の基本機能

車載制御システムはリアルタイム性が求められるシステムであり、特に車の基本機能（走る、曲がる、止まる）は事前に定められた時間内に処理され、実行されなければならない。さもなくば、人命に関わるような被害をもたらす可能性がある。このため、ネットワークが遮断された際にも車の走行に影響を及ぼさないように、車の基本機能に関しては車両内に配備する。

(2)　自動車向けサービス機能

車はライフサイクルが長期間に渡る製品である。一方で、情報サービスや情報システムはライフサイクルが車と比較して非常に短い。車が情報システムと融合しつつある現状では、情報サービスや情報システムのライフサイクルが短いことによって発生するシステムの脆弱性によって、車自体の安全性が損なわれる可能性がある。また、続々と新たに提供される情報サービスが古い車種では対応できないことは利用者やサービス提供者にとって不利益となる可能性がある。このため、車に手を加えず新しいサービスの提供やシステム更新、セキュリティ管理ができるように、自動車向けサービス機能は可能な限り車の外部、すなわち、ネットワーク上に配備する。

(3)　車や外部サービスの機能を呼び出すための API

従来の自動車向けサービスアプリケーション開発には、車載制御システムに関する専門的で広範な知識やノウハウが必要であった。今後、多種多様な自動車サービスが様々な組織から提供される社会を実現するためには、IT 業界における WEB やスマートフォン向けサービスの事例のように、幅広いサービス提供者が車の機能を用いたサービスアプリケーション開発を容易に行い、迅速にサービス提供できなくてはならない。このため、車の機能を呼び出す API や車から外部のサービスを利用するための API を整備し、アプリケーションから利用できるようにする。

上記の方針に従い、車の基本機能を除く、自動車向けサービス機能の大部分をネットワーク側に配置するシステムアーキテクチャを提案する。ここで、ネットワーク上に配置される機能群を自動車サービスプラットフォーム（以下、プラットフォーム）と呼ぶ。図 4 に提案するシステムアーキテクチャを示す。

プラットフォームは下記機能から構成される。

- 車の制御機能や車両情報にアクセスするためのビークル API、ならびに、外部システムのサービスにアクセスするためのサービス API。ビークル API はアプリケーション開発時に車種の違いを意識せずに利用できるよう抽象化を図る。
- 画面の look & feel など利用者ごとのアプリケーションの設定データやサービスの利用履歴等を管理するサービス管理機能。
- 車両の遠隔監視やレコメンドのための分析に必要となる位置情報や車両の状態など、車に関するデータを一定間隔で収集し、蓄積・管理するための車両データ管理機能。
- サービス提供者等の保有する外部システムと接続し通信を行う外部接続インターフェース（外部システム）機能、ならびに、車と接続し通信を行う外部接続インターフェース（車）機能。標準化された通信プロトコルを採用することにより、様々な外部システムや車種との接続性を担保する。

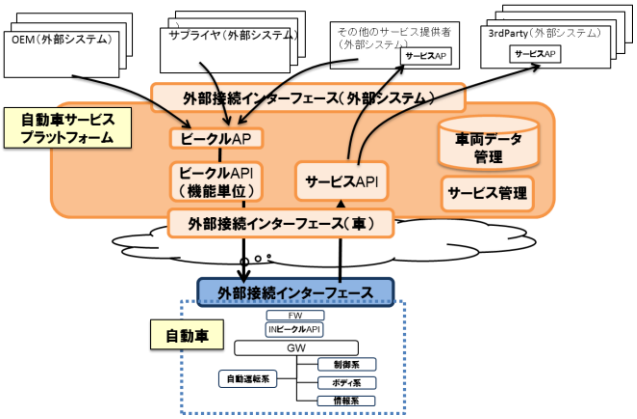


図 4　提案アーキテクチャ

また、車側の機能構成を図 5 に示す。車側には、自動車サービス向け機能を可能な限り配置せずに、プラットフォームと連携する機能と、車の基本機能だけを残す構成としている。

車の外部接続インターフェースはプラットフォームのみと通信を行う機能を有し、プラットフォーム上のサービス API、およびビークル API と通信を行う。

プラットフォームからの要求は、車側の外部接続インターフェース、および FW を経由し車両内のビークル API（以降、インビークル API と呼ぶ）に送られる。インビークル API は、要求を車両制御用メッセージ（CAN メッセージ等）に変換し、車内の通信ネットワークを仲介する GW を通じて ECU に送信する。また、車内のヘッドユニット等の情報系システムからの要求は、外部接続インターフェースを通じてプラットフォーム上のサービス API に送られる。呼び出されたサービス API に基づき外部システムにて処理された結果は車内の情報系システム

に返却され、表示や再生が行われる。

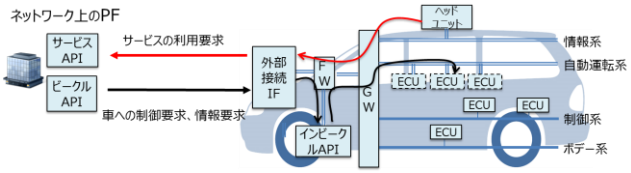


図 5　車側のシステム構成

以上のように機能を配置することによるメリットは以下のとおりである。

まず、プラットフォームに車の基本機能以外の自動車サービス向け機能を集約することで、機能の多くを車に配置する場合に比べて、アクセス制御やシステム更新等のセキュリティに関するポリシ設定や更新を一元的に管理でき、脆弱性への対応もし易くなる。一方、車の走行に関わる基本機能は車のみで実行可能であり、利用者はたとえネットワークと接続できない場合でも車の走行機能に関して操作することができる。また、車の外部との接続点を外部接続インターフェースのみにすることで、車への外部からの侵入口を最小化し、セキュリティ上、監視すべき箇所を絞り込むことが可能となる。

次に、ビークル API を整備することで、サービス提供者は車側の構造や車種毎の細かい違いを意識せずにサービス開発を行うことが可能となる。ビークル API を組み合わせることで、新たな自動車サービスに必要な機能追加、変更も可能となる。また、サービス API を統一することで車から外部サービスへのアクセスが容易になる。

更に、サービス管理機能によりプラットフォーム上で利用されるサービスの設定や利用状況を管理することで、利用者が車を乗り換えたとしても、同じサービスを継続して利用することが可能となる。

また、車両データ管理機能により車両情報を収集・管理することで、データ分析による付加価値サービスの創出や、遠隔からの車両状態の監視といったことが可能となる。

最後に、本アーキテクチャを介することで OEM、サプライヤ、3rdParty の連携、協業がしやすくなり、そのエコシステムが形成され、自動車サービス市場の活性化が期待できる。

表 1 にプラットフォームの機能と 5.2 節で示した自動車サービスの機能要件との対応について示す。

表 1　プラットフォームの機能と対応する機能要件

プラットフォームの機能	機能概要	対応する機能要件
API（ビークルAPI、サービスAPI）	プラットフォーム上に車の機能をサービス化して利用できるビークルAPI、および外部サービスを利用できるサービスAPIを設置	5.2 (1) C) 5.2 (1) D) 5.2 (2) A) 5.2 (3) A) 5.2 (3) B)
API（ビークルAPI）	ビークルAPIで車種などの違いを吸収	5.2 (2) B)
車両データ管理	車両情報をプラットフォームで収集・蓄積・管理	5.2 (1) B)
サービス管理	利用サービスをプラットフォーム側で管理	5.2 (3) C)
外部接続インターフェース（車）	プラットフォームと車の接続は単一の外部接続IFからのみ行う	5.2 (4) A)

6.　セキュリティ要件と対策

本章では、5 章で提案したシステムアーキテクチャにおけるセキュリティ要件とその対策としてのセキュリティ機能について述べる。

6.1　システムに求められるセキュリティ要件

提案アーキテクチャの中核となるプラットフォームには種々の機能が集中し、また、数多くのステークホルダーにアクセスを許容する必要がある。よって、本プラットフォームはサイバー攻撃の脅威に晒される可能性が高く、それらを検知、防御、対応するためのセキュリティ対策が極めて重要である。

情報セキュリティの 3 要素である機密性、完全性、可用性の観点から本プラットフォームにおけるに求められるセキュリティ要件を以下に整理する。

- 機密性：許可されたステークホルダーのみが、プラットフォームにアクセスし、許可された機能やサービスのみを利用できること。また、プラットフォームに収集された情報を利用する際に、機微な情報やプライバシーに関わる情報が外部に漏れないこと。

- 完全性：プラットフォームで提供される車の制御に関する機能や自動車サービスに関連する機能が、その機能の提供者の意図したとおりに正確に動作すること。また、プラットフォームに格納される車や自動車サービスに関する情報が改ざんされないこと。

- 可用性：プラットフォームが備える車の制御に関する機能や自動車サービスに関連する機能が、必要なタイミングで利用できること。また、プラットフォームに格納される車や自動車サービスに関する情報が消失しないこと。

6.2 セキュリティ機能

6.1 節のセキュリティ要件を満たすために､プラットフォームが備えるべきセキュリティ機能について述べる。

(1) ID 管理機能

プラットフォームにアクセスするステークホルダー、すなわち､サービス利用者（運転者､データ利用者など）やサービス提供者（OEM やサプライヤ､3rd Party など）、あるいは、サービス利用者が用いる車やスマートフォンなどのデバイスなど、多様な種別、役割のアイデンティティを管理する。外部の機関やサービスにおいて管理されるアイデンティティとの連携、紐付けも行う。

(2) 認証機能

上記のアイデンティティがプラットフォームへアクセスする際、その種別やアクセスの内容に応じて、適切な認証方式、レベルで確認する。

利用者の認証においては、一般の IT システムと同様、強固さと簡便さの両立が肝要である。運転者の認証用デバイスとしては、広く普及し、かつ、携帯性を有するスマートフォンが好適であるが、所有しない運転者のための方策の検討が必要である。

また、車そのものの認証の実現も課題である。モバイル通信用の SIM を用いる案があるが､SIM は取り外して他の車で利用することができてしまう。他方、車載部品の殆どが付替えられた場合に、それを以前と同一の車と見做すのか？といった疑問もある。よって、車のアイデンティティとは何か、何を持って同一視をすべきか、から検討する必要があるだろう。

(3) 認可機能

API や情報へのアクセスが有った際に、それが車の安全性や利用者／提供者の経済性を損なう不正なアクセスではないかを事前に確認し、防止する。

前述の通り、プラットフォームには多様な種別、役割を持ったアイデンティティが存在するため、それに適した複雑な認可ポリシを扱える機構が必要である。これには認可ポリシの設定、更新が適切に簡便に行えることも含まれる。

また、車の API、特に、制御に関わる機能の呼び出しは、現実世界に直接的に影響を与えるため、車両や利用者の状況に応じて許可／不許可の判断を変えなくてはならないケースもある。このように、その時々の状況を的確に把握し、それらを踏まえた的確な判断をリアルタイムに実現する技術の確立が必要である。

(4) アプリケーション正当性確認機能

従来は車載システムに関する専門的で広範な知識を有する OEM やサプライヤが、車種を限定した専用のアプリケーションを作成しており、その処理ロジックの正当性が厳密に確認され、リリースされてきた。OEM 以外多数のステークホルダーがより早いサイクルでアプリケーションを開発し、提供できるようにするためには、開発されるアプリケーションが、車やサービス利用者、サービス提供者に悪影響を及ぼすものではないことを短時間で確認する機能が必要である。

多種多様なアプリケーションの処理ロジックから、ステークホルダーに害をもたらす不適切なコード（例えば、プライバシーポリシに違反するもの等）を機械的に抽出することは現時点では困難であり、今後の課題である。なお、故意ではない作り込みを抑制するためには、アプリケーションの開発ガイドラインの作成や、それに準じた開発環境の提供等のアプローチで対応していくことも考えられる。

(5) 攻撃検知機能

プラットフォームには車の制御に関連する機能をはじめ重要な機能や情報が集中して存在するため、様々なサイバー攻撃が行われると考えられる。前述の認証や認可､あるいはアプリケーション正当性確認機能によって、サイバー攻撃を事前に防止する対策に加えて、プラットフォームや車に対して攻撃が試行されていないか、万が一にも攻撃が成功し、被害が発生していないかを検知する機能が必要である。

同機能は、一般 IT システム向けのセキュリティログ・トラヒック分析技術（例えば、文献[11]など）をベースに実現できると考えられるが、高速で移動する多数の車との間で送受される大量の通信の中からサイバー攻撃、特に未知の攻撃をリアルタイムに特定するためには、更なる検討が必要である。

(6) パーソナルデータ保護機能

i. データ分析時の保護

プラットフォームには車の挙動や運転者に関する様々なデータが蓄積されている。自動車サービスではこれらのデータをパーソナルデータとして有効に利活用することが想定されるが、パーソナルデータの取り扱いについては、プライバシーの観点から国外、国内で盛んな議論が行われている。[12]

プラットフォームに収集されたパーソナルデータが、適切にプライバシー保護されない形で各種サービスで利活用されたり、外部に販売されたりしないように、パーソナルデータを保護する機能が必要である。また、データの二次利用において、外部のデータとの相関分析を、両方のデータのプライバシーを保護しながら行うことも求められる。

データの匿名化や、分散された状態のまま統計処理を行う等のアプローチで対応していくことが必要であると考えられるが、車から取得され、増え続ける大量のデータに対して必要なレベルの匿名性を担保しながらいかに効率的に分析し、その結果を利活用できるようにするかは今後の課題である。

ii.　データ蓄積時の保護

プラットフォームに蓄積される車の挙動に関するデータについては、自動車サービスにおいて利活用されるだけではなく、ドライブレコーダーのデータのように事故が起きた際の証拠として、あるいは、事故の発生時に製品の機能として問題なく動作したことを証明するデータとして利用されることも考えられる。このため、データを改ざんや滅失から長期に渡って保護する機能が必要となる。

改ざんからの保護には長期署名方式などが考えられるが、極めて膨大な量のデータをいかに効率的、経済的に保管しつづけるかが大きな課題となるだろう。

以上述べたセキュリティ機能の提案アーキテクチャへのマッピングを図 6 に示す。

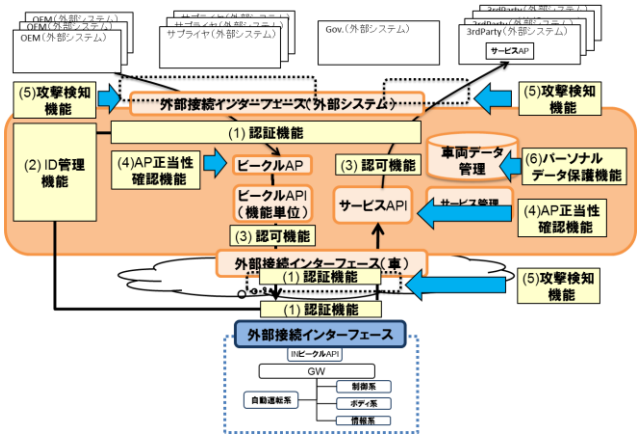


図 6 システムアーキテクチャ上のセキュリティ機能

7. おわりに

本論文では、執筆時点から 10 年後の 2025 年頃における自動車サービスを想定し、同サービスを実現する機能の大部分を車ではなくネットワーク上のプラットフォームに配置するシステムアーキテクチャを提案した。これは、多数のステークホルダーが参画するエコシステムの形成に大いに寄与するものである。また、提案アーキテクチャの実現に向けたキーとなるセキュリティ機能として ID 管理、認証・認可、アプリケーションの正当性確認、攻撃検知、パーソナルデータ保護を取り上げ、それらを実現する上での今後の課題を述べた。

提案アーキテクチャのように車とネットワーク上のプラットフォームとの間で密接な機能連携を行うことは、現時点での周囲の環境を前提とすると実現困難であるかもしれないが、次世代の通信ネットワークインフラである 5G やエッジコンピューティングなどの分散処理機構が普及することで、十分可能になると考えられる。

今後は実用化に向け、プラットフォームと車との間の通信の遅延や信頼性、車載システムの処理能力なども加味しつつ、各機能の実装方法の検討を進める。また、セキュリティ機能を実現する上での技術課題についても検討を進める。

参考文献

[1] “よく分かる自動車歴史館”. https://gazoo.com/car/history/Pages/car_history_001.aspx, (参照 2016-08-01).

[2] デンソーカーエレクトロニクス研究会. 図解 カーエレクトロニクス [上]システム編. 日経 BP 社, 2014, 13p.

[3] Chris Valasek, Charlie Miller, Remote Exploitation of an Unaltered Passenger Vehicle. Technical report, Blackhat 2015.

[4] “Tesla Model S JSON API”. http://docs.timdorr.apiary.io/#, (参照 2016-08-01)

[5] “Hacking a Tesla Model S: What we found and what we learned”. https://blog.lookout.com/blog/2015/08/07/hacking-a-tesla/, (参照 2016-08-01).

[6] “W3C Automotive and Web Platform BG”. https://www.w3.org/community/autowebplatform/, (参照 2016-08-01)

[7] “自動運転を視野に入れたコネクテッドカー関連の世界市場を調査“. https://www.fuji-keizai.co.jp/market/16002.html, (参照 2016-08-01).

[8] 総務省. 平成 27 年情報通信白書. 第 4 章第 1 節.

[9] 佐藤雅明. インターネット上での自動車情報基盤の構築. 慶応義塾大学大学院 政策・メディア研究科 博士論文, 2009.p. 10-12.

[10] 岩井 明史. 車載向けサービスプラットフォームの構築と評価. デンソーテクニカルレビュー vol.18 2013 p.172.

[11] Zhong, Y. et al.. Detecting Malicious Inputs of Web Application Parameters using Character Class Sequences. The 39th Annual International Computers, Software & Applications Conference (COMPSAC). 2015.

[12] 総務省.改正個人情報保護法等を踏まえたプライバシー保護検討タスクフォース（第一回）.資料 5. “コネクテッドカーにおけるプライバシー保護について”,(参照 2016-08-01).