www.pwc.com/jp

# 「戦略的イノベーション創造プログラム（SIP）自動走行システム／大規模実証実験」のうち「情報セキュリティ実証実験」に係る公募

# a 脅威分析調査報告書

PwCコンサルティング合同会社

平成30年2月28日

pwc

# *Contents*

# 脅威分析調査の目的とスコープ

1

# 1-1. 脅威分析調査の目的とスコープ

目的:

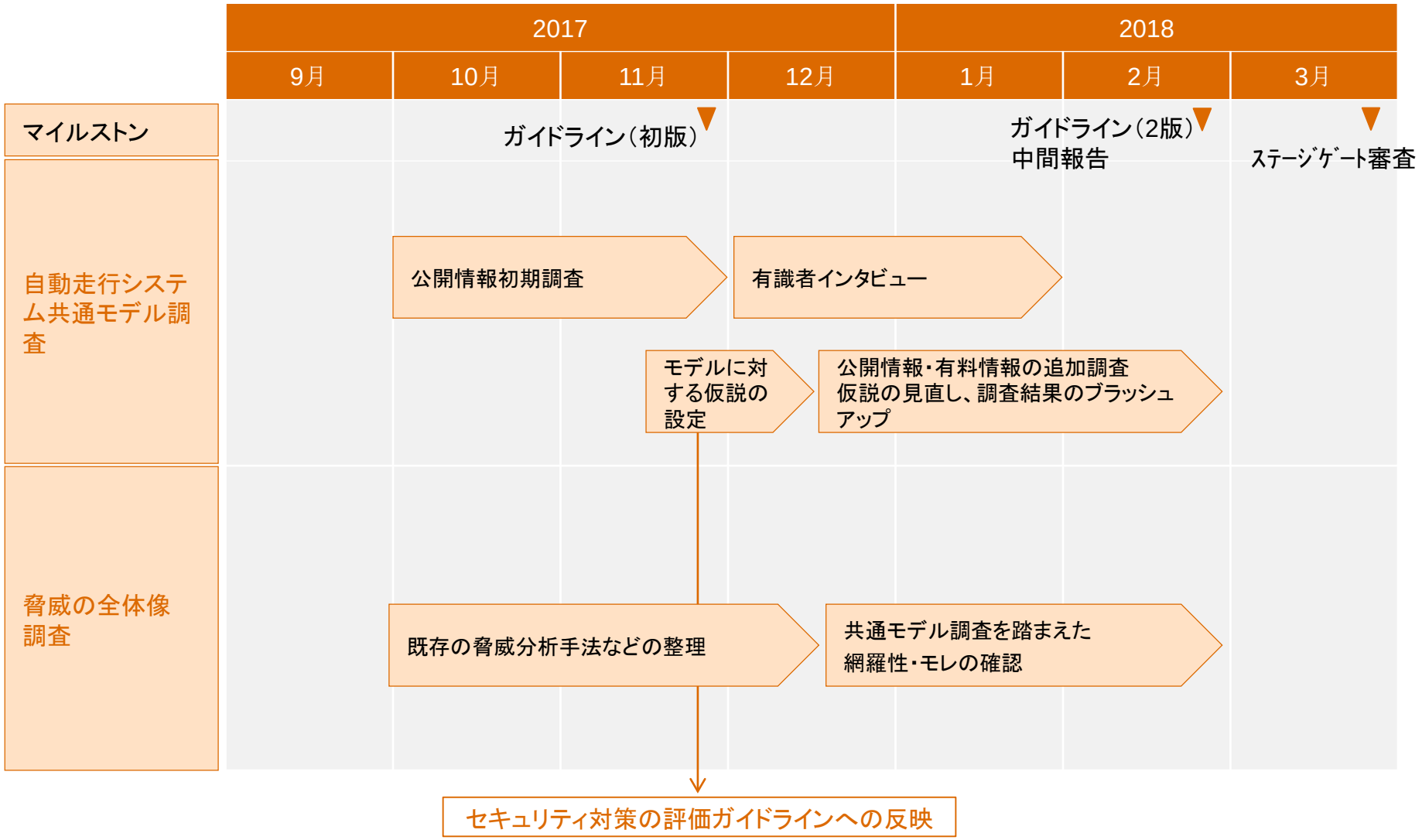
自動走行に係るV2X 等車外からの攻撃を含む脅威の全体像の整理し、自動走行車両セキュリティに関するコンセンサスの醸成を支援すること

スコープ:

脅威分析調査のスコープ

| | | |
|---|---|---|
| I. 脅威分析調査 | 自動走行システム共通モデル調査 | • 自動車メーカ、部品サプライヤ、IT企業などの自動運転・コネクテッドカーに係る取り組みをファクトベースで調査し、整理・類型化することで自動走行システム共通モデルを導出する |
| | 脅威の全体像調査 | • 自動走行システム共通モデルに係る、V2X等車外からの攻撃を含む脅威項目を抽出する<br>• 脅威項目ごとに影響度評価を実施し、特に重大な脅威については、対策状況を調査し、必要に応じて別途作成する評価ガイドラインに反映する |
| II. 情報セキュリティ評価ガイドライン策定 | | 攻撃者観点が盛り込まれた車両セキュリティの評価手法の確立とガイドライン化 |

# 1-2. 推進スケジュール


2017
2018
9月
10月
11月
12月
1月
2月
3月
マイルストン
ガイドライン（初版）
ガイドライン（2版）
中間報告
ステージゲート審査
自動走行システム共通モデル調査
公開情報初期調査
有識者インタビュー
モデルに対する仮説の設定
公開情報・有料情報の追加調査
仮説の見直し、調査結果のブラッシュアップ
脅威の全体像調査
既存の脅威分析手法などの整理
共通モデル調査を踏まえた
網羅性・モレの確認
セキュリティ対策の評価ガイドラインへの反映

# 脅威分析調査の進め方

2

# 2-1. 自動走行システム共通モデル調査フェーズ

| | |
|---|---|
| 自動走行システム共通モデル調査 | • 自動車メーカ、部品サプライヤ、IT企業などの自動運転・コネクテッドカーに係る取り組みをファクトベースで調査し、整理・類型化することで自動走行システム共通モデルを導出する |
| 脅威の全体像調査 | • 自動走行システム共通モデルに含まれる[2]等車両の攻撃を含む脅威を洗い出し、脅威の全体像の整理する<br>• 自動走行システム共通モデルに含まれる脅威に対して脅威分析を実施し、特に重大な脅威については、評価ガイドラインに対策を盛りこむ |

赤字: 本調査の主要な成果物

## 1 自動走行関連サービスと機能の一覧

- 自動車メーカ、自動車部品メーカ、およびIT企業等の公開情報を調査し、自動走行システム・コネクテッドカーに関するサービスを調査し、それを実現する機能を整理

**調査対象**

- 自動車メーカ（16社）
- 自動車部品メーカ（4社）
- IT企業（23社）

**サービス・機能の一覧**

| | サービス | 機能 |
|---|---|---|
| 1 | 運転・駐車支援 | 車間距離制御<br>車線維持制御<br>車間距離制御（V2V型）<br>隊列走行（V2V型）<br>自動運転（ITS協調型）<br>自動運転（自律型）<br>駐車周辺映像表示<br>自動駐車<br>自動駐車（スマホ連携） |
| 2 | … | … |

【インプット】
- 自動車メーカ（16社）、自動車部品メーカ（4社）、IT企業（23社）の公開情報（HPなどを参照）

【アウトプット】
- サービス・機能の一覧

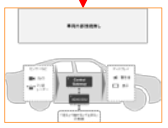
## 2 機能別のシステム構成想定

- 自動車メーカ、IT企業の公開情報をもとに調査し、機能を実現するシステム構成を検討
  ＊業界の有識者へのインタビュー結果も考慮

**機能の想定システム構成**

| | サービス | 機能 |
|---|---|---|
| 1 | 運転・駐車支援 | 車間距離制御<br>車線維持制御<br>車間距離制御（V2V型）<br>隊列走行（V2V型）<br>自動運転（ITS協調型）<br>自動運転（自律型）<br>駐車周辺映像表示<br>自動駐車<br>自動駐車（スマホ連携） |
| 2 | … | … |

HP等 → システム構成特定



車間距離制御（システム構成図）

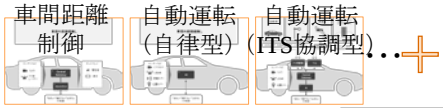
【インプット】
- サービス・機能の一覧
- 主要な自動車メーカ・IT企業が公開する機能に関する公開情報
- 有識者インタビューにおけるご意見

【アウトプット】
- 機能別の想定システム構成

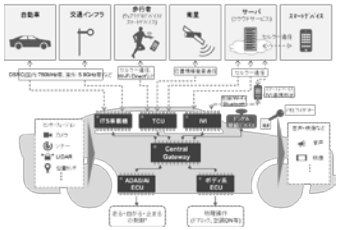
## 3 自動走行システム共通モデルの特定

- 機能別の想定システム構成をすべて勘案し本脅威分析調査における自動走行システム共通モデルを特定
  ＊業界の有識者へのインタビュー結果も考慮

**機能別の想定システム構成（40システム）**




**自動走行システム共通モデル**



【インプット】
- 機能別の想定システム構成
- 有識者インタビューにおけるご意見

【アウトプット】
- 本脅威分析調査における自動走行システム共通モデル

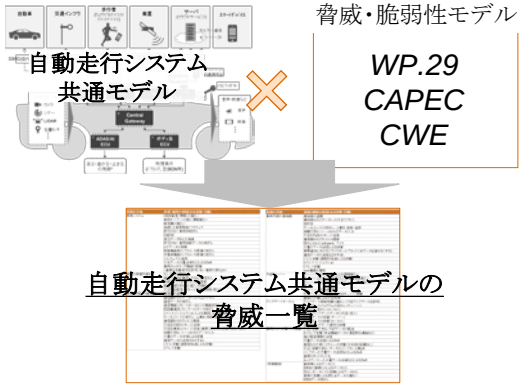
# 2-2. 脅威の全体像調査フェーズ

| | |
|---|---|
| 自動走行システム共通モデル調査 | • 自動車メーカ、部品サプライヤ、IT企業などの自動運転・コネクテッドカーに係る取り組みをファクトベースで調査し、整理・類型化することで自動走行システム共通モデルを導出する |
| 脅威の全体像調査 | • 自動走行システム共通モデルに係る、V2X等車外からの攻撃を含む脅威を洗い出し、脅威の全体像の整理する<br>• 自動走行システム共通モデルに含まれる脅威に対して脅威分析を実施し、特に重大な脅威については、評価ガイドラインに対策を盛りこむ |

赤字: 本調査の主要な成果物

## 4 自動走行システム共通モデルの脅威の一覧化

- 自動走行システム共通モデルに対して、WP.29のThreat Matrixと各種脅威・脆弱性モデルを適用することで、自動走行システム共通モデルの脅威の一覧を整理

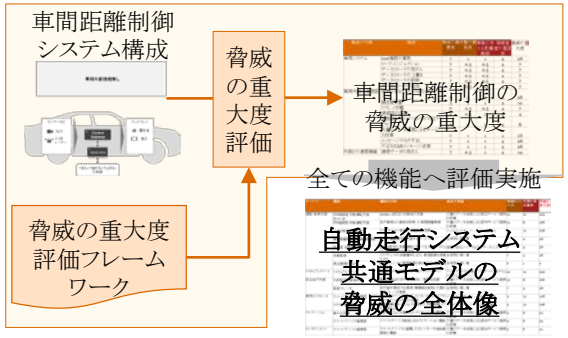



【インプット】
- 自動走行システム共通モデル
- 脅威モデル(WP.29 Threat Matrix, CAPEC)
- 脆弱性モデル(CWE)

【アウトプット】
- 自動走行システム共通モデルの脅威一覧

## 5 自動走行システム共通モデルの脅威の全体像特定

- 自動走行システム共通モデルの脅威一覧と脅威の重大度の評価指標と組み合わせ、脅威の重大度を評価するフレームワークを策定
- 機能を実現するシステムに対して、上記フレームワークを適用し、機能の脅威の重大度を評価
- 全ての機能に対してこれを実施し、自動走行システム共通モデルの重大の全体像を特定

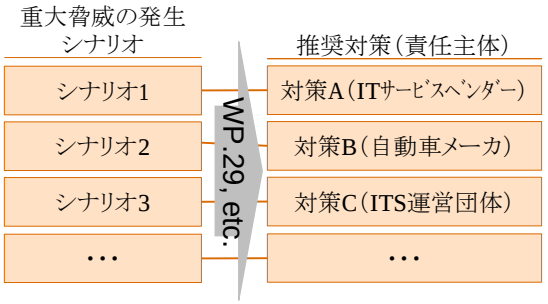



【インプット】
- 脅威の一覧
- 脅威の重大度の評価指標(WP.29, CRSS)
- 機能別の想定システム構成図

【アウトプット】
- 自動走行システム共通モデルの脅威の全体像

## 6 重大脅威に対する対策状況調査

- 自動走行システム共通モデルの重大脅威をふまえ必要な対策を特定するとともに責任主体と合わせて整理
- 加えて、別途作成する情報セキュリティ評価ガイドラインへ必要に応じて反映




【インプット】
- 自動走行システム共通モデルの脅威の全体像
- WP.29におけるセキュリティ対策(Mitigation)等の情報

【アウトプット】
- 自動走行システム共通モデルの脅威への対策状況調査結果

# 調査結果

3

# 3-1. 自動走行システム共通モデル調査

# *調査手順*

自動車メーカ、自動車部品メーカ、および自動走行車両を開発するIT企業を調査し、自動走行システムやコネクテッドカーに係るサービスとそれを実現する機能を整理

## 調査対象会社・団体

- **自動車メーカ**
  BMW, Daimler, Fiat Chrysler Automobiles, Ford, Freightliner Trucks, GM, Hyundai, Volkswagen/Audi, Volvo, Tesla,トヨタ, 日産, ホンダ, マツダ, 日野,三菱ふそう
- **自動車部品メーカ**
  Continental, Bosch, DENSO, パイオニア
- **自動走行車両を開発するIT企業**
  Alibaba, Baidu, EasyMile, Faraday Future, LeEco Group, Local Motors, NAVYA, Next Future Transportation, Otto, RDM Group, Waymo(Google), ZMP, Lyft, nuTonomy, Uber, DeNA, Aimotive, Delphi.ai, FiveAI, Innoviz Technologies, Intel, Mobileye, NVIDIA

## サービス・機能の一覧

| サービス | | 機能 | |
|---|---|---|---|
| 名称 | | 名称 | |
| 1 | 運転・駐車支援 | 1-1 | 車間距離制御 |
| | | 1-2 | 車線維持制御 |
| | | 1-3 | 車間距離制御（V2V型） |
| | | 1-4 | 隊列走行（V2V型） |
| | | 1-5 | 自動運転（ITS協調型） |
| | | 1-6 | 自動運転（自律型） |
| | | 1-7 | 駐車周辺映像表示 |
| | | 1-8 | 自動駐車 |
| | | 1-9 | 自動駐車（スマホ連携） |
| 2 | 安全走行支援 | 2-1 | 緊急ブレーキ |
| | | 2-2 | 歩行者検知（V2P型） |
| | | 2-3 | 注意喚起（ITS協調型） |
| 3 | … | … | … |

# 自動走行関連サービスと機能の一覧（1/3）

調査の結果整理した、サービスおよびサービスを実現する機能を以下に示す。

## サービス・機能の一覧

| サービス | | | 機能 | | |
|---|---|---|---|---|---|
| 名称 | | 内容 | 名称 | | 内容 |
| 1 | 運転・駐車支援 | 自動車の走行・駐車を支援するサービス | 1-1 | 車間距離制御 | ITSと協調せずに先行車両との車間距離を制御する機能 |
| | | | 1-2 | 車線維持制御 | ITSと協調せずに走行車線を維持する機能 |
| | | | 1-3 | 車間距離制御（V2V型） | ITSと協調し先行車両との車間距離を制御する機能 |
| | | | 1-4 | 隊列走行（V2V型） | 先頭車両と通信を行うことで後続車が無人で先頭車両を追従する機能（トラックなど商用車向け） |
| | | | 1-5 | 自動運転（ITS協調型） | ITSと協調することで人間に代わりあらゆる運転タスクを実施する機能 |
| | | | 1-6 | 自動運転（自律型） | ITSと協調することなく、内蔵するセンサーフュージョンを活用することで、人間に代わりあらゆる運転タスクを実施する機能 |
| | | | 1-7 | 駐車周辺映像表示 | 車両を駐車する周辺の映像を表示することで人間による車両の駐車を支援する機能 |
| | | | 1-8 | 自動駐車 | 内蔵するセンサーフュージョンを活用することで、人間に代わり車両の駐車を実施する機能 |
| | | | 1-9 | 自動駐車（スマホ連携） | スマートフォンにインストールされたアプリケーション経由で車両の操作指示を行うことで、遠隔からの車両の自動駐車を実施する機能 |
| 2 | 安全走行支援 | 自動車の安全走行を阻害する状態を検知・警告・回避するサービス | 2-1 | 緊急ブレーキ | 歩行者や接近する車両・障害物を検知した際に、音声/表示による運転者に警告、必要に応じた自動でブレーキを実施する機能 |
| | | | 2-2 | 歩行者検知（V2P型） | 歩行者の所有するスマートデバイスと連携し、車両の近くにいる歩行者を検知することで、必要に応じて車両を制御し歩行者との衝突を回避する機能 |
| | | | 2-3 | 注意喚起（ITS協調型） | 協調型ITSを活用した路車間通信システムにより、周辺環境の情報を提供することで、右折時注意・赤信号注意などの各種注意喚起を実施する機能 |
| 3 | 省燃費走行支援 | 燃費効率の良い走行を支援するために、アクセルワークを制御するサービス | 3-1 | 省燃費走行支援 | （左記の内容に同じ）（商用車向け） |

# 自動走行関連サービスと機能の一覧（2/3）

調査の結果整理した、サービスおよびサービスを実現する機能を以下に示す。

## サービス・機能の一覧

| サービス | | | 機能 | | |
|---|---|---|---|---|---|
| 名称 | | 内容 | 名称 | | 内容 |
| 4 | ｿﾌﾄｳｪｱｱｯﾌﾟﾃﾞｰﾄ | 無線通信を利用した電子制御システムのソフトウェア更新サービス | 4-1 | OTA | （左記の内容に同じ） |
| 5 | 故障検知 | 自動車に備わる自己診断機能を活用し、故障を予知・検知するサービス | 5-1 | 故障検知 | （左記の内容に同じ） |
| 6 | 緊急通報 | 緊急時に的確な支援を仰ぐために、通報を行うサービス | 6-1 | 自動衝突通知 | 車両衝突後時に、自動でセンターへの衝突通知発信を実施する機能 |
| | | | 6-2 | 車両故障時の電話サポート | 乗員の体調不良発生や車両の故障時にボタン押下することでセンターへの通知を行い、トラブル対応を支援する機能 |
| 7 | 車両状態監視 | 車両の状態を監視するサービス | 7-1 | ドア・トランク・ハザードランプなどの状態監視 | ドア、トランク、ハザードランプ、ウィンドウ等の状態をスマートデバイスなどにより遠隔監視する機能 |
| | | | 7-2 | 車両異常検知・通知 | ドアこじ開けなどの異常を検知した際に、メール等により所有者へ通知する機能 |
| | | | 7-3 | 車両位置追跡 | 車両の位置情報を取得し現在地の把握・追跡を可能とする機能 |
| 8 | 車両遠隔操作 | 遠隔地からの操作により自動車に備わる制御システムを制御するサービス | 8-1 | 遠隔からのﾄﾞｱﾛｯｸ・ｱﾝﾛｯｸ | ｽﾏｰﾄﾃﾞﾊﾞｲｽなどと連携し、遠隔地より車両のﾄﾞｱのﾛｯｸ・ｱﾝﾛｯｸを制御する機能 |
| | | | 8-2 | インテリジェントキー | イモビライザキーを活用し、車両の周辺よりドアのﾛｯｸ・ｱﾝﾛｯｸを制御する機能 |
| | | | 8-3 | 充電制御 | スマートデバイスと連携し、遠隔地より充電状況の管理（充電率の把握、充電停止等）を制御する機能 |
| | | | 8-4 | 充電制御（音声認識AI連携） | 音声認識AIエージェントと連携し、遠隔地より充電状況の管理（充電率の把握、充電停止等）を制御する機能 |
| | | | 8-5 | エアコン制御 | スマートデバイスと連携し、遠隔地よりエアコンのオン・オフを制御する機能 |
| | | | 8-6 | ｴｱｺﾝ制御（音声認識AI連携） | 音声認識AIｴｰｼﾞｪﾝﾄと連携し、遠隔地よりエアコンのオン・オフを制御する機能 |
| | | | 8-7 | エンジン再駆動・ステアリングロック解除禁止 | オーナーの要請に基づき、エンジンの再始動・ステアリングロックの解除の禁止を実施する機能 |

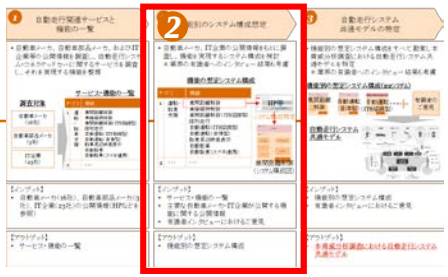
# 自動走行関連サービスと機能の一覧（3/3）

調査の結果整理した、サービスおよびサービスを実現する機能を以下に示す。

## サービス・機能の一覧

| サービス | | | 機能 | | |
|---|---|---|---|---|---|
| 名称 | | 内容 | 名称 | | 内容 |
| 9 | シェアリングサービス | 自動車のシェアリングサービス | 9-1 | カーシェアリング | （左記の内容に同じ） |
| 10 | 料金支払いサービス | 車両利用中に発生する様々な料金の支払い（高速道路・駐車場・ガソリンスタンドなど）を支援するサービス | 10-1 | 料金支払い | （左記の内容に同じ） |
| 11 | ナビゲーション | 目的地へ到着するための経路情報を提供するサービス | 11-1 | ルート検索 | 目的地へのルート検索（最短・最安ルートの検索）などを実施する機能 |
| | | | 11-2 | オペレータサービス | オペレーターがドライバーをサポートするコンシェルジュ機能（に口頭で情報検索、検索結果の配信依頼など） |
| 12 | エンタテイメント | 車内において娯楽などを提供するサービス | 12-1 | カレンダー・メール同期 | ITサービスベンダーのサービスと連携し、カレンダーやメール等の内容のIVIシステムへの表示・読み上げ等を実施する機能 |
| | | | 12-2 | SNS連携 | ITサービスベンダーのSNSと連携し、その内容をIVIシステムへ表示する機能 |
| | | | 12-3 | Wi-Fiスポット | IVIシステムをWi-Fiホットスポットとして活用することで、乗員にインターネットにアクセスを提供する機能 |
| | | | 12-4 | 各種アプリケーション利用 | 音楽再生などその他各種アプリケーションの利用 |

# 調査手順



- 車種別に自動走行システム開発で先行する企業を選定したうえで、企業が公開する情報を確認し、機能別の想定システム構成を机上調査
- 加えて、有識者インタビューを実施し想定システム構成を見直し

サービス・機能の一覧

| サービス | | 機能 | |
|---|---|---|---|
| 名称 | | 名称 | |
| 1 | 運転・駐車支援 | 1-1 | 車間距離制御 |
| | | 1-2 | 車線維持制御 |
| | | 1-3 | 車間距離制御（V2V型） |
| | | 1-4 | 隊列走行（V2V型） |
| | | 1-5 | 自動運転（ITS協調型） |
| | | 1-6 | 自動運転（自律型） |
| | | 1-7 | 駐車周辺映像表示 |
| | | 1-8 | 自動駐車 |
| | | 1-9 | 自動駐車（スマホ連携） |
| 2 | 安全走行支援 | 2-1 | 緊急ブレーキ |
| | | 2-2 | 歩行者検知（V2P型） |
| | | 2-3 | 注意喚起（ITS協調型） |
| 3 | … | … | … |

**STEP1:** 想定システム構成机上調査

調査対象会社HP等

主な調査対象会社

乗用車: トヨタ, 日産、GM、Volkswagen/Audi
商用車（トラック・バス）: 日野、三菱ふそう、Scania
商用車（シェアリング）: Waymo

＋

階層構造の車両アーキテクチャ*

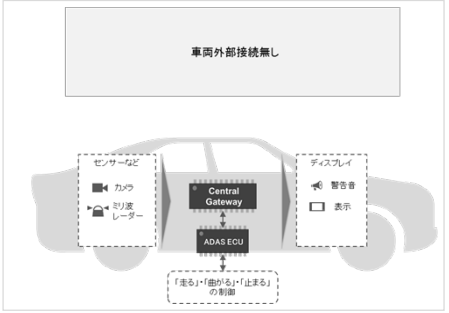
*システム構成情報が欠如している部分については、「平成27年度 戦略的イノベーション創造プログラム（自動走行システム）：V2X等車外情報の活用にかかるセキュリティ技術の研究・開発プロジェクト」報告書に掲載の階層構造のアーキテクチャを仮定

**STEP2:** 有識者インタビューをふまえた机上調査結果の見直し

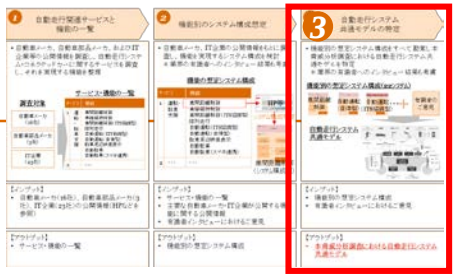

＋

有識者インタビュー

車間距離制御（想定システム構成）



# 調査手順



- 機能別の想定システム構成をすべて勘案し自動走行システム共通モデルを導出
- 加えて、有識者インタビューを実施しモデルを見直し

## 運転・駐車支援

車間距離制御
車線維持制御
車間距離制御 (V2V型)
隊列走行 (V2V型)
自動運転 (ITS協調型)
自動運転 (自律型)
周辺環境表示
自動駐車 (自律型)
自動駐車 (スマホ連携型)

## 安全走行支援

緊急ブレーキ
歩行者検知 (V2P型)
注意喚起 (ITS協調型)

## 省燃費走行支援

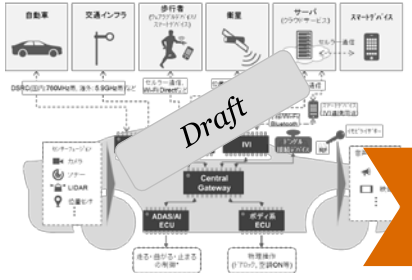
（省略）

## 車両遠隔操作

（省略）

## ・・・

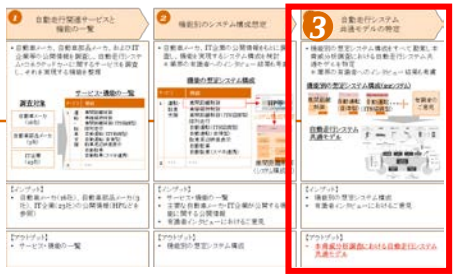
・・・

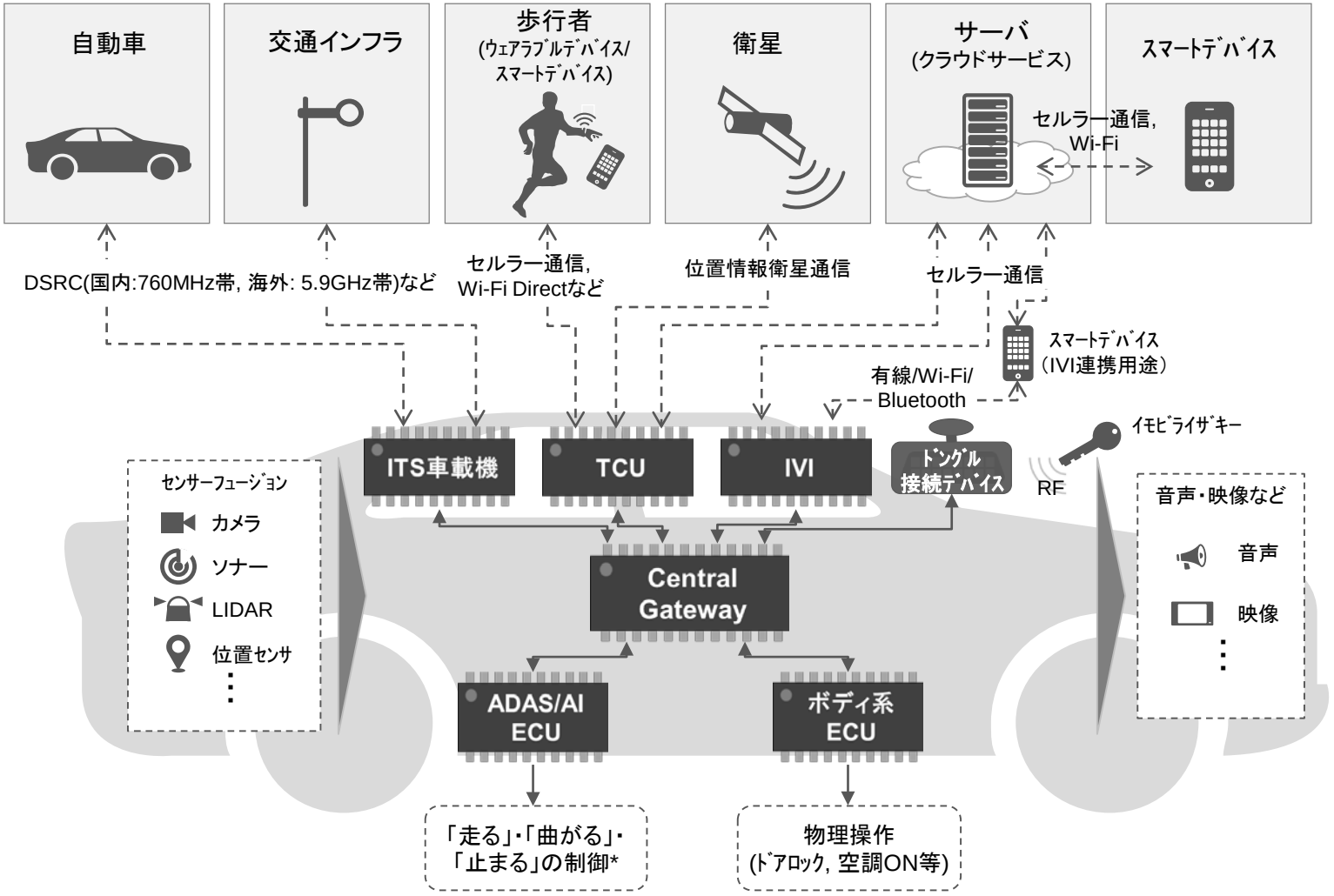



有識者インタビューを
実施し内容を見直し

# 自動走行システム共通モデル(2020年代前半)

本脅威分析調査における自動走行システム共通モデル



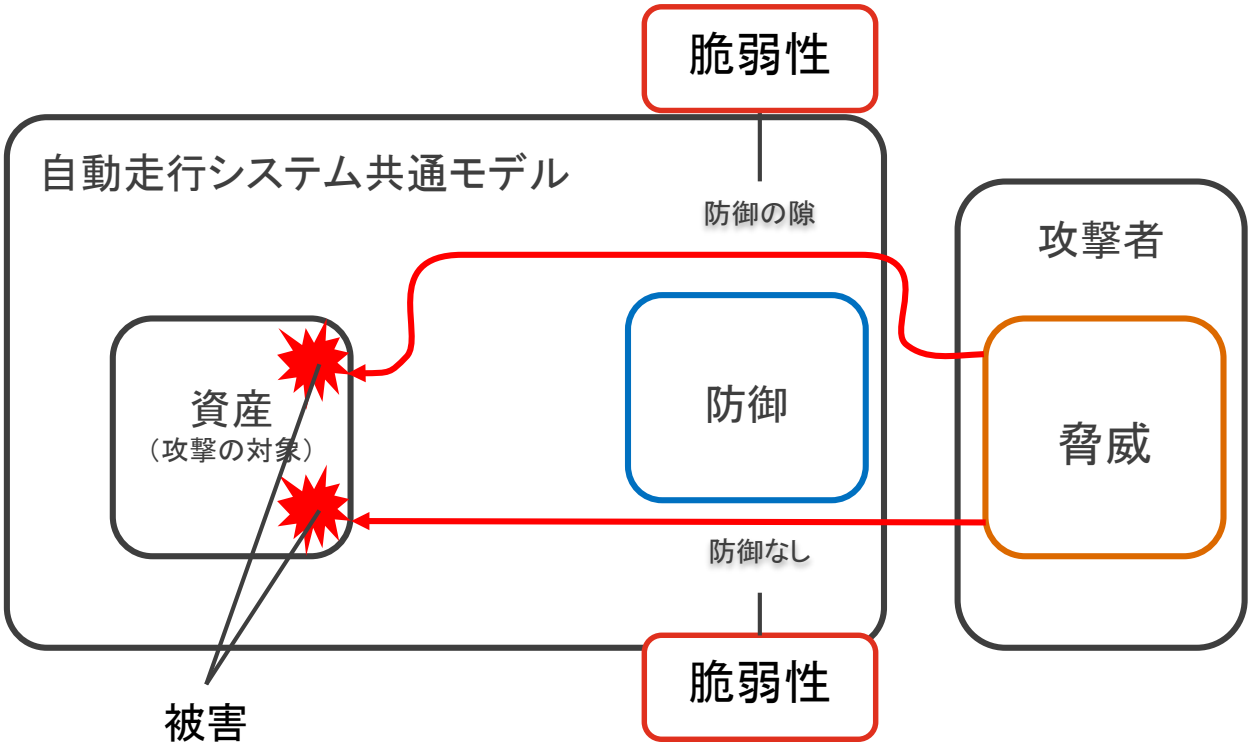



*ステアリング・ブレーキ・エンジン等に係る制御機能のトポロジーは本脅威分析結果に直接影響しないため抽象化

# 3-2. 脅威の全体像調査

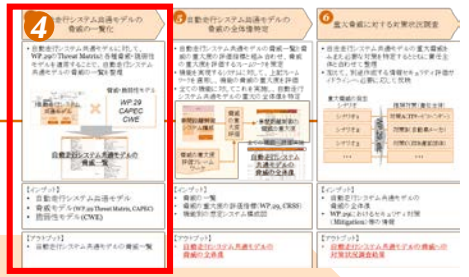
# 本調査における「脅威」の定義

本調査における脅威を、「自動走行システム共通モデルに危害(被害)を与える潜在的原因」と定義 (ISO/IEC 27000:2009 の脅威定義を本調査向けに具体化)




自動走行システム共通モデルにまつわるセキュリティ用語の関連性を示す模式図

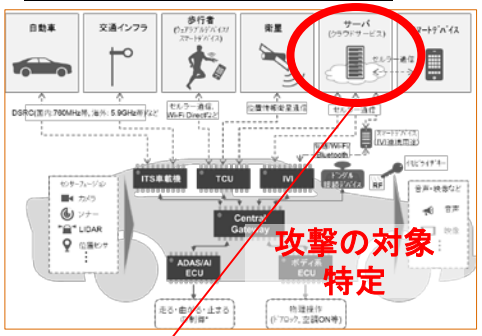
# 脅威の一覧作成手順



## STEP1

自動走行システム共通モデルとWP.29のThreat Matrix*1と比較し、共通モデルに関連するの「攻撃の対象」、および「脅威」を抽出

自動走行システム共通モデル




WP.29 Threat Matrix

| 攻撃の対象 | 脅威 |
|---|---|
| Server used to attack vehicle | Abuse of privileges by staff (**insider attack**) |
| | **Unauthorised internet access** to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means) |
| | **Unauthorised physical access** to the server (conducted by for example USB sticks or other media connecting to the server) |
| | ・・・ |
| | |
| | |

抽出

## STEP2

・CAPECを参照し、STEP1の脅威一覧を整理・詳細化
・加えて、CWE*2と比較し検算

抽出された脅威一覧

| 攻撃の対象 | 脅威 |
|---|---|
| Server used to attack vehicle | Abuse of privileges by staff (**insider attack**) |
| | **Unauthorised internet access** to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means) |
| | **Unauthorised physical access** to the server (conducted by for example USB sticks or other media connecting to the server) |
| | ・・・ |
| | |

×

CAPEC/CWE

| CAPEC-ID | Name |
|---|---|
| 112 | Brute Force |
| 114 | Authentication Abuse |
| 115 | Authentication Bypass |
| 116 | Excavation |
| 117 | Interception |
| 123 | Buffer Manipulation |
| 125 | Flooding |
| 129 | Pointer Manipulation |
| ・・・ | ・・・ |
| ・・・ | ・・・ |

整理・詳細化

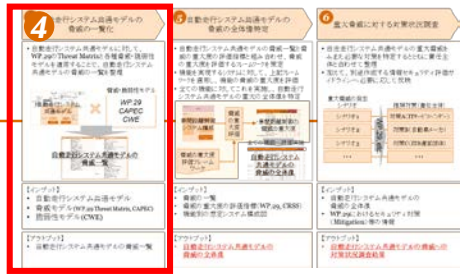
自動走行システム共通モデルの脅威一覧

| 攻撃の対象 | 脅威（被害の原因となる攻撃・欠陥） |
|---|---|
| 外部サーバー | サーバーへの不正侵入による情報漏えい |
| | サーバー上のデータ共有（ミス）による情報漏えい |
| | サーバーへの不正侵入によるサーバー乗っ取り |
| | サーバーへのDoS攻撃 |
| | サーバーへの不正侵入によるサーバー破壊 |
| | 認証の不備による不正利用 |
| ・・・ | ・・・ |

*1: WP.29 Threat Matrix: https://wiki.unece.org/download/attachments/51971917/TFCS-09-11%20%28Sec%29%20Mitigations%20table%20-%20updated%20during%20TFCS-09.xlsx?api=v2

*2: WP.29のThreat Matrixには、脅威の項目として脆弱性に近い内容を含むため、脅威の洗い出しの際にCWE（脆弱性モデル）も考慮

# 自動走行システム共通モデルの脅威一覧



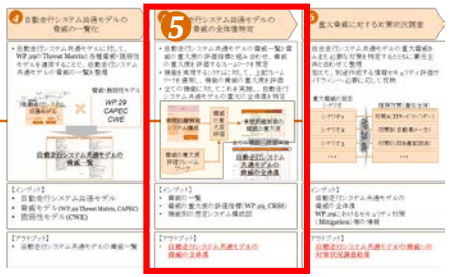
| 攻撃の対象 | 脅威（被害の原因となる攻撃・欠陥） |
|---|---|
| 車両システム | OEM資産（情報）の漏えい |
| | 車両オーナーの個人情報漏えい |
| | 暗号鍵の漏えい |
| | 偽装した車両制御ソフトウェア |
| | 許可のない車両ID改ざん |
| | ID詐称 |
| | 走行データなどの偽造 |
| | 許可のない車両診断データの改ざん |
| | ログデータの削除 |
| | 制御機能用のパラメータ数値の改ざん |
| | 充電用機能のパラメータ数値の改ざん |
| | マルウェアの追加 |
| | 不正データ大量送信などによるDoS |
| | 車両モニタリング機能の妨害 |
| | （通常は自動走行を許可しない場所で使うとか） |
| 車両の物理外部I/F | センサーの改ざん |
| | 通信データを横流しするように改ざん |
| | 外部メディアからのウイルス感染 |
| | 物理外部I/Fからの侵入（USBなど） |
| | 不正な診断用メッセージ送信（ODB-IIなど） |
| 車両（内部）の通信路 | 通信路の盗聴 |
| | 通信路からのデータへの不正アクセス |
| | 通信データの改ざん |
| | 通信機能（リモートキーなど）の機能改ざん |
| | 短距離通信/センサーのデータ改ざん |
| | コマンドインジェクションによる意図しない機能実行 |
| | データ/コードの改ざん・上書き・削除・追加 |
| | 通信路からのウイルス感染 |
| | 不正なCANメッセージ送信 |
| | 不正な専用メッセージ送信（通常OEMしか送信できないもの） |
| | 信頼できないソースからのデータ入力 |
| | 大量のデータ送信による妨害 |
| | 通信データの送信元なりすまし |
| | シビル攻撃（複数ID生成による攻撃） |
| | リプレイ攻撃 |

| 攻撃の対象 | 脅威（被害の原因となる攻撃・欠陥） |
|---|---|
| 車両外部の通信路 | 通信路の盗聴 |
| | 通信路からのデータへの不正アクセス |
| | MITM |
| | データ/コードの改ざん・上書き・削除・追加 |
| | 信頼できないソースからのデータ入力 |
| | 不正なV2Xメッセージ送信 |
| | 通信路からのウイルス感染 |
| | 改ざんされた3rd party　アプリ |
| | 大量のデータ送信による妨害 |
| | 車間通信におけるブラックホールアタック（全データを届かなくする） |
| | 通信データの送信元なりすまし |
| | シビル攻撃（複数ID生成による攻撃） |
| | コマンドインジェクション |
| | リプレイ攻撃 |
| | root権限の奪取 |
| 外部サーバー | サーバーへの不正侵入による情報漏えい |
| | サーバー上のデータ共有（ミス）による情報漏えい |
| | サーバーへの不正侵入によるサーバー乗っ取り |
| | 同上 |
| | サーバーへのDoS攻撃 |
| | サーバーへの不正侵入によるサーバー破壊 |
| | 認証の不備による不正利用 |
| アップデートサービス | アップデート用暗号鍵の漏えい（不正アップデートを許可） |
| | アップデートの妨害/アップデートプログラムの改ざん（サーバー） |
| | アップデートの妨害/アップデートプログラム改ざん（ローカル） |
| | 不正なアップデートデータの作成（混入） |
| | 正当なアップデート実行の妨害 |
| 車両からの攻撃（2次被害） | 不正/信頼できないV2Vデータの転送 |
| | タイミング攻撃（安全機能データの意図的な遅延など） |
| | 偽の緊急情報の送信 |
| | 大量データ送信によるDoS |
| | 車両からの他システムへの攻撃（※手法は記載なし） |
| | 不正/信頼できないデータのインフラへの転送 |
| | インフラへの大量データ送信などによるDoS |
| | 車両のボットネット化 |
| | ネットワークへの大量データ送信などによるDoS |
| （物理要因） | 衝突等によるデータロス |
| | DRMの管理ミスによるデータロス |
| | ITコンポーネントの故障によるデータロス |
| | 車両の売買による持ち主データの漏えい |
| | OEMデータ改ざん |

# 参考: 引用資料概要

| # | 名称 | 団体名 | 概要 |
|---|---|---|---|
| 1 | Threat matrix | 自動車基準調和世界フォーラム（WP29) | • 世界各国の自動車業界関係者およびセキュリティ専門家が協議し、作成した、車両を取り巻く環境を考慮した脅威の一覧 |
| 2 | CAPEC(Common Attack Pattern Enumeration and Classification) | MITRE | • 攻撃方法の種類を一意に識別するために攻撃方法のタイプを体系化したもの（攻撃方法タイプの一覧） |
| 3 | CWE(Common Weakness Enumeration) | MITRE | • セキュリティ上の弱点（脆弱性）の種類を識別するための共通の基準 |

# 脅威の重大度評価フレームワークの策定



WP.29およびJSAEによって策定された脅威の重大度の評価指標を組み合わせ、「脅威の大きさ」、「攻撃の発生確率」を半定量化し、「脅威の重大度」を見積もるフレームワークを策定

## 脅威の重大度評価フレームワーク

（脅威の重要度 × 攻撃の難易度）×（事象の与える影響範囲 × 情報資産の重要度）= 脅威の重大度（規格化前）

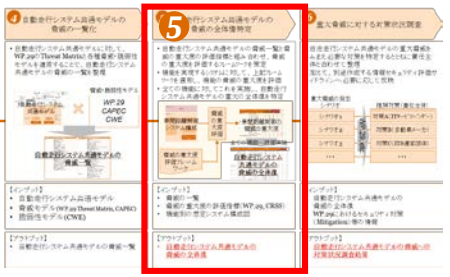
A 脅威の大きさ（インパクト）　B 攻撃の発生確率　規格化*1

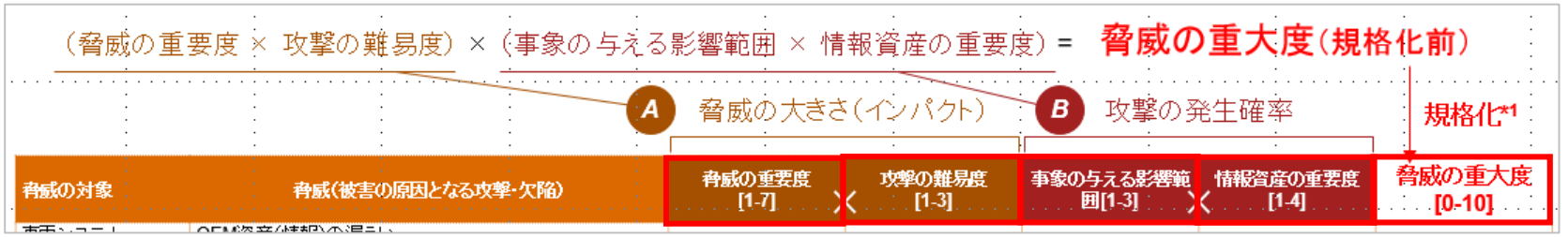
| 脅威の対象 | 脅威（被害の原因となる攻撃・欠陥） | 脅威の重要度 [1-7] × 攻撃の難易度 [1-3] | 事象の与える影響範囲[1-3] × 情報資産の重要度 [1-4] | 脅威の重大度 [0-10] |
|---|---|---|---|---|
| 車両システム | OEM資産（情報）の漏えい | | | |
| | 車両オーナーの個人情報漏えい | | | |
| | 暗号鍵の漏えい | | | |
| | 偽装した車両制御ソフトウェア | | | |
| | 許可のない車両ID改ざん | | | |
| | ID詐称 | | | |
| | 走行データなどの偽造 | | | |
| | 許可のない車両診断データの改ざん | | | |
| | ログデータの削除 | | | |
| | 制御機能用のパラメータ数値の改ざん | | | |
| | 充電用機能のパラメータ数値の改ざん | | | |
| | マルウェアの追加 | | | |
| | 不正データ大量送信などによるDoS | | | |
| | 車両モニタリング機能の妨害 | | | |
| | （通常は自動走行を許可しない場所で使うとか） | | | |
| 車両の物理外部I/F | センサーの改ざん | | | |
| | 通信データを横流しするように改ざん | | | |
| | 外部メディアからのウイルス感染 | | | |
| | 物理外部I/Fからの侵入（USBなど） | | | |
| | 不正な診断用メッセージ送信（ODB-IIなど） | | | |
| … | … | | | |

4 にて洗い出した脅威一覧　WP.29策定の指標を考慮　CRSS*2を考慮

*1:脅威の重大度スコアリングにあたっては、とり得るスコアの最大値で規格化し、0~10の値とした
*2: 車両システムに特化したセキュリティリスク分析手法（出典: JSAE, TP-15002）

# 各パラメータの定義






## 脅威の重要度

| 重要度 | 内容 | スコア |
|---|---|---|
| Lv 7 | 車両の安全性へ影響を与える | 7 |
| Lv 6 | 車両機能の動作停止 | 6 |
| Lv 5 | ソフトウェアの改ざん、パフォーマンスの変更 | 5 |
| Lv 4 | ソフトウェアの変更（ただし、操作上の影響なし） | 4 |
| Lv 3 | データの完全性侵害 | 3 |
| Lv 2 | データの機密性侵害 | 2 |
| Lv 1 | その他 | 1 |

## 攻撃の難易度

| 難易度 | 内容 | スコア |
|---|---|---|
| 高 | 権限昇格や情報収集など攻撃に至るまでに複数の条件が必要となるもの | 1 |
| 中 | 難易度がシステムに内在する脆弱性に依存する攻撃 | 2 |
| 低 | 攻撃が容易（難易度「高」に記載するような条件が不要な攻撃） | 3 |

## 事象の与える影響範囲

| 影響範囲 | 内容 | スコア |
|---|---|---|
| 大 | 不特定多数の対象に影響を及ぼす | 3 |
| 中 | 複数あるが周辺の対象のみに限定される | 2 |
| 小 | 1つの対象のみに限定される | 1 |

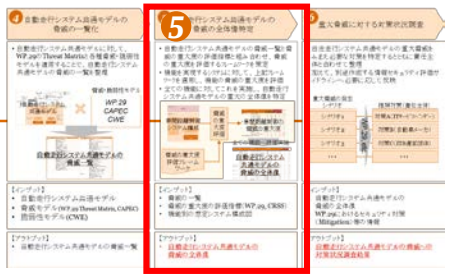
## 情報資産の重要度

| 重要度 | 内容 | スコア |
|---|---|---|
| 特高 | 制御情報 | 4 |
| 高 | 金融資産に関する情報 | 3 |
| 中 | プライバシー情報 | 2 |
| 低 | 上記以外の情報 | 1 |

## 脅威の重大度

| 脅威のレベル | スコア |
|---|---|
| レベルIII（重大） | 10.0 ~ 7.0 |
| レベルII（警告） | 6.9 ~ 4.0 |
| レベルI（注意） | 3.9 ~ 0 |

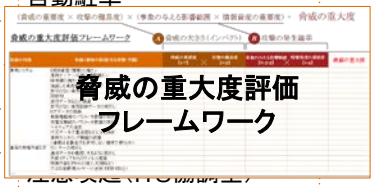
# 機能別の脅威の重大度評価



機能を実現するシステムに対して、脅威の重大度評価のためのフレームワークを適用し、機能別の脅威の重大度を評価

## 例: 車間距離維持の場合

| サービス | | 機能 | |
|---|---|---|---|
| 名称 | | 名称 | |
| 1 | 運転・駐車支援 | 1-1 | 車間距離制御 |
| | | 1-2 | 車線維持制御 |
| | | 1-3 | 車間距離制御（V2V型） |
| | | 1-4 | 隊列走行（V2V型） |
| | | 1-5 | 自動運転（ITS協調型） |
| | | 1-6 | 自動運転（自律型） |
| | | 1-7 | 駐車周辺映像表示 |
| | | 1-8 | 自動駐車 |
| | | … | |

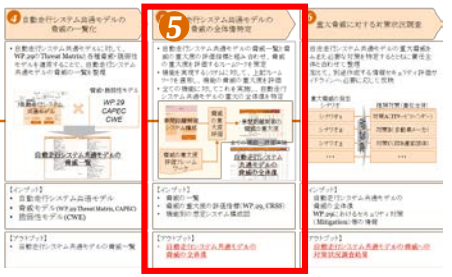

重大度評価

## 脅威の重大度評価結果（「車間距離維持」機能）

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| 通信データの送信元なりすまし | 1.39 | 0.80 | 1.11 |
| コマンドインジェクション | 1.39 | 0.80 | 1.11 |
| データ/コードの改ざん | 1.39 | 0.80 | 1.11 |
| データ/コードの上書き | 1.39 | 0.80 | 1.11 |
| データ/コードの削除 | | | 1.11 |
| データ/コードの追加 | | | 1.11 |
| 信頼できないソースからのデータ入力 | | 0.80 | 1.11 |
| MITM | | 0.80 | 0.48 |
| リプレイ攻撃 | 1.39 | 0.80 | 1.11 |
| 通信路の盗聴 | 0.40 | 0.80 | 0.32 |
| 通信路からのデータへの不正ア… | 0.40 | 0.80 | 0.32 |
| 大量のデータ送信による該当サービス提供の妨害 | 1.39 | 0.80 | 1.11 |
| root権限の奪取 | 1.39 | 0.80 | 1.11 |
| 不正なCANメッセージ送信 | 1.39 | 0.80 | 1.11 |
| 通信データの改ざん（テレマティクス） | 1.39 | 0.80 | 1.11 |

Image

# 自動走行システム共通モデルの脅威の全体像



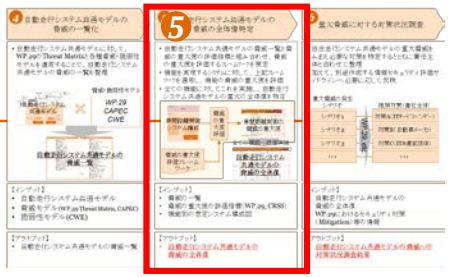
自動走行システム共通モデルに内在する脅威のうち、脅威の重大度スコアがレベルII以上のものを抽出し、以下に示す。

| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

## 自動走行システム共通モデルの脅威の全体像

| サービス | | 機能 | | | 脅威 | 脅威の大きさ | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|---|---|---|---|---|
| 名称 | | 名称 | | 内容 | | | | |
| 1 | 運転・駐車支援 | 1-3 | 車間距離制御（V2V型） | ITSと協調し先行車両との車間距離を制御する機能 | 信頼できないソースからのデータ入力 | 2.8 | 1.6 | 4.4 |
| | | | | | 大量のデータ送信による妨害 | 4.2 | 1.6 | 6.7 |
| | | 1-4 | 隊列走行（V2V型） | 先頭車両と通信を行うことで後続車が無人で先頭車両を追従する機能（トラックなど商用車向け） | 信頼できないソースからのデータ入力 | 2.8 | 1.6 | 4.4 |
| | | | | | 大量のデータ送信による妨害 | 4.2 | 1.6 | 6.7 |
| | | 1-5 | 自動運転（ITS協調型） | ITSと協調することで人間に代わりあらゆる運転タスクを実施する機能 | 信頼できないソースからのデータ入力 | 2.8 | 2.4 | 6.7 |
| | | | | | 大量のデータ送信による妨害 | 4.2 | 2.4 | 10.0 |
| | | 1-9 | 自動駐車（スマホ連携） | スマートフォンにインストールされたアプリケーション経由で車両の操作指示を行うことで、遠隔からの車両の自動駐車を実施する機能 | サーバーへの不正侵入によるサーバー乗っ取り | 1.8 | 2.4 | 4.3 |
| | | | | | 信頼できないソースからのデータ入力 | 2.8 | 2.4 | 6.7 |
| 2 | 安全走行支援 | 2-2 | 歩行者検知（V2P型） | 歩行者の所有するスマートデバイスと連携し、車両の近くにいる歩行者を検知することで、必要に応じて車両を制御し歩行者との衝突を回避する機能 | 信頼できないソースからのデータ入力 | 2.8 | 1.6 | 4.4 |
| | | | | | 大量のデータ送信による妨害 | 4.2 | 1.6 | 6.7 |
| 4 | ｿﾌﾄｳｪｱｱｯﾌﾟﾃﾞｰﾄ | 4-1 | OTA | 無線通信を利用した電子制御システムのソフトウェア更新サービス | アップデートの妨害/アップデートプログラムの改ざん（サーバー） | 4.2 | 2.4 | 10.0 |
| | | | | | 正当なアップデート実行の妨害 | 3.6 | 1.2 | 4.3 |

# 自動走行システム共通モデルの脅威の全体像



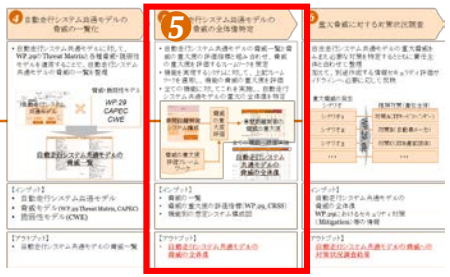
自動走行システム共通モデルに内在する脅威のうち、脅威の重大度スコアがレベルII以上のものを抽出し、以下に示す。

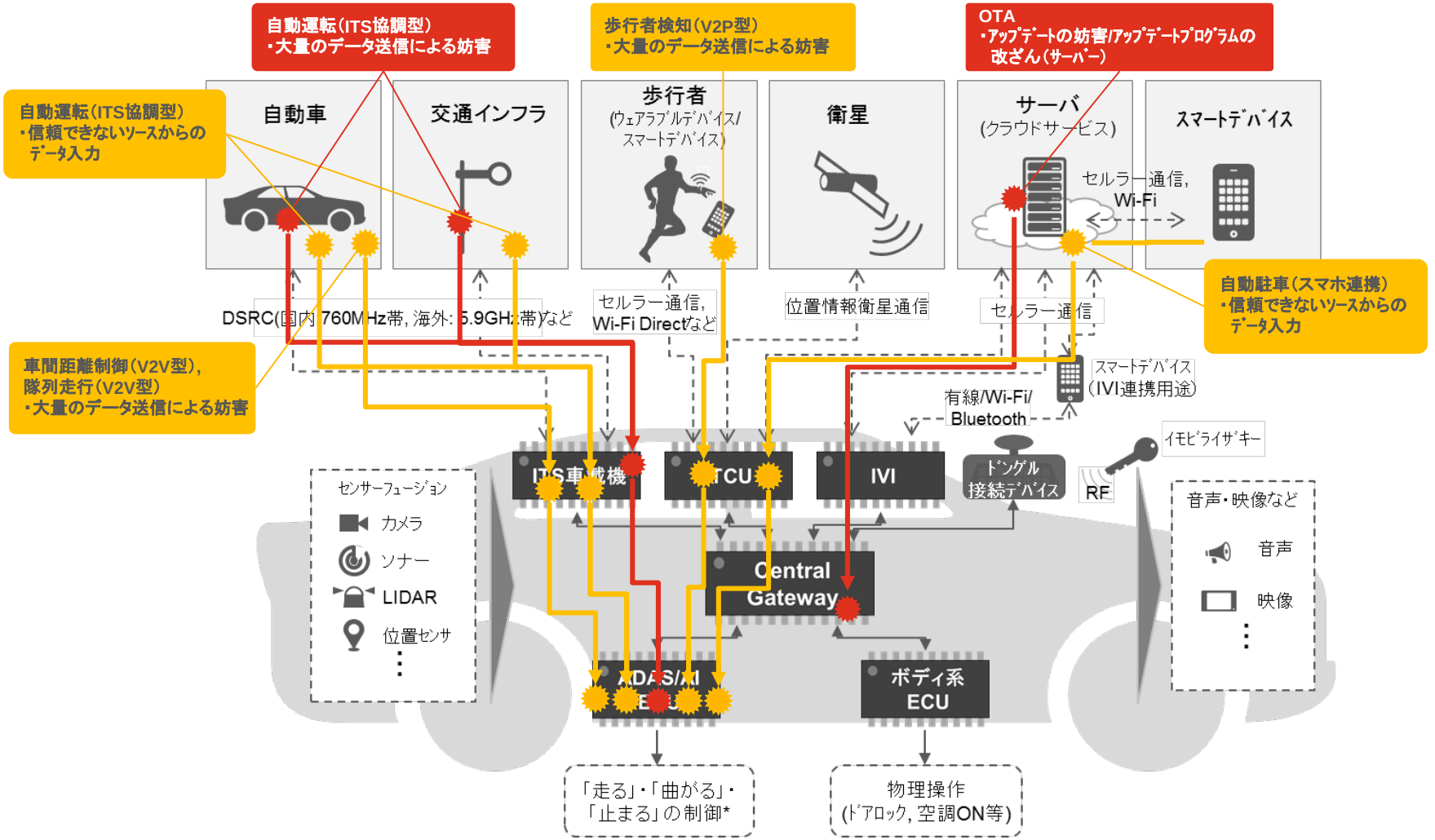
| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

## 自動走行システム共通モデルの脅威の全体像

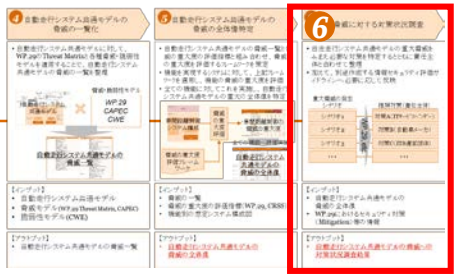
| サービス | | 機能 | | | 脅威 | 脅威の大きさ | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|---|---|---|---|---|
| 名称 | | 名称 | | 内容 | | | | |
| 5 | 故障検知 | 5-1 | 故障検知 | 自動車に備わる自己診断機能を活用し、故障を予知・検知するサービス | サーバーへの不正侵入によるサーバー乗っ取り | 1.8 | 2.4 | 4.3 |
| 8 | 車両遠隔操作 | 8-1 | 遠隔からのﾄﾞｱﾛｯｸ・ｱﾝﾛｯｸ | スマートデバイスなどと連携し、遠隔地より車両のドアのロック・アンロックを制御する機能 | サーバーへの不正侵入によるサーバー乗っ取り | 1.8 | 2.4 | 4.3 |
| | | 8-3 | 充電制御 | スマートデバイスと連携し、遠隔地より充電状況の管理（充電率の把握、充電停止等）を制御する機能 | サーバーへの不正侵入によるサーバー乗っ取り | 1.8 | 2.4 | 4.3 |
| | | 8-4 | 充電制御（音声認識AI連携） | 音声認識AIエージェントと連携し、遠隔地より充電状況の管理（充電率の把握、充電停止等）を制御する機能 | サーバーへの不正侵入によるサーバー乗っ取り | 1.8 | 2.4 | 4.3 |
| | | 8-5 | エアコン制御 | スマートデバイスと連携し、遠隔地よりエアコンのオン・オフを制御する機能 | サーバーへの不正侵入によるサーバー乗っ取り | 1.8 | 2.4 | 4.3 |
| | | 8-6 | エアコン制御（ 音声認識AI連携） | 音声認識AIエージェントと連携し、遠隔地よりエアコンのオン・オフを制御する機能 | サーバーへの不正侵入によるサーバー乗っ取り | 1.8 | 2.4 | 4.3 |
| | | 8-7 | エンジン再駆動・ステアリングロック解除禁止 | オーナーの要請に基づき、エンジンの再始動・ステアリングロックの解除の禁止を実施する機能 | サーバーへの不正侵入によるサーバー乗っ取り | 1.8 | 2.4 | 4.3 |

# 自動走行システム共通モデルの脅威の全体像
## （スコアが6以上の脅威について図示）





# 対策状況調査手順



抽出した重大脅威への対策・及び責任主体をWP.29等の推奨セキュリティ対策を踏まえ検討

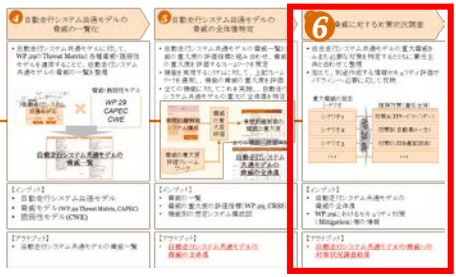
## 自動走行システム共通モデル重大脅威（一覧）

| サービス | | 機能 | | | 脅威 | 脅威の大きさ | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|---|---|---|---|---|
| 名称 | | 名称 | | 内容 | | | | |
| 1 | 運転・駐車支援 | 1-3 | 車間距離制御（V2V型） | ITSと協調し先行車両との車間距離を制御する機能 | 信頼できないソースからのデータ入力 | 2.8 | 1.6 | 4.4 |
| | | | | | 大量のデータ送信による妨害 | 4.2 | 1.6 | 6.7 |
| | | 1-4 | 隊列走行（V2V型） | 先頭車両と通信を行うことで後続車が無人で先頭車両を追従する機能（トラックなど商用車向け） | 信頼できないソースからのデータ入力 | 2.8 | 1.6 | 4.4 |
| | | | | | 大量のデータ送信による妨害 | 4.2 | 1.6 | 6.7 |
| | | 1-5 | 自動運転（ITS協調型） | ITSと協調することで人間に代わりあらゆる運転タスクを実施する機能 | 信頼できないソースからのデータ入力 | 2.8 | 2.4 | 6.7 |
| | | | | | 大量のデータ送信による妨害 | 4.2 | 2.4 | 10.0 |
| | | 1-9 | 自動駐車（スマホ連携） | スマートフォンにインストールされたアプリケーション経由で車両の操作指示を行うことで、遠隔からの車両の自動駐車を実施する機能 | サーバーへの不正侵入によるサーバー乗っ取り | 1.8 | 2.4 | 4.3 |
| | | | | | 信頼できないソースからのデータ入力 | 2.8 | 2.4 | 6.7 |

## WP.29 Security Control

| 脅威（シナリオ） | 推奨セキュリティ対策 |
|---|---|
| Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means) | - Securely configuring servers (e.g. system hardening)<br>- Protections of external internet connections, including authentication/verification of messages recieved and provision of encrypted communication channels<br>- Monitoring of server systems and communications<br>- Manage the risks and security of cloud servers (if used)<br>- Security information and event management |
| Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when stored by third-party cloud service providers | - Monitoring of server systems<br>- Managing the risks and security of cloud servers.<br>- Applying data minimisation techniques to reduce the impact should data be lost<br>- Security information and event management |
| Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner | - Timestamping messages and setting expiration time for messages<br>- Employing rate limiting measures based on context.<br>- Check size of received data<br>- Authentication of data. |
| … | 脅威シナリオに紐づくセキュリティ対策を抽出 |

どのコンポーネントにおける対策が必要か明確化し
抽出した対策の責任主体を検討



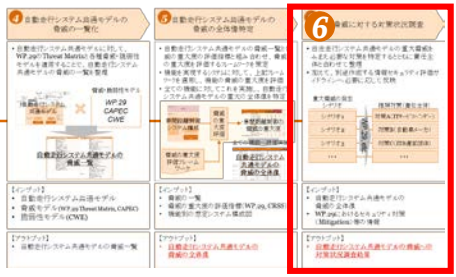
# 対策状況調査結果概要

- レベルII以上の脅威への車両側の対策は、評価ガイドへ項目を追加
- 一方で、赤字で記載した脅威への対策は、車両側だけでは不十分であるため、評価ガイドとは別に、対策の検討が必要

| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| サービス | | 機能 | | 脅威 | 脅威の重大度 | 責任主体 | | | | 評価ｶﾞｲﾄﾞにおける対応状況 | 本事業外で必要な対応 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 名称 | | 名称 | | | | 自動車メーカ | ITｻｰﾋﾞｽ事業者 | ﾃﾞﾊﾞｲｽ提供事業者 | 政府等 | | |
| 1 | 運転・駐車支援 | 1-3 | 車間距離制御（V2V型） | 信頼できないソースからのデータ入力 | 4.4 | ✔ | | | | 項目追加 | - |
| | | | | 大量のデータ送信による妨害 | 6.7 | ✔ | | | | 項目追加 | - |
| | | 1-4 | 隊列走行（V2V型） | 信頼できないソースからのデータ入力 | 4.4 | ✔ | | | | 項目追加 | - |
| | | | | 大量のデータ送信による妨害 | 6.7 | ✔ | | | | 項目追加 | - |
| | | 1-5 | 自動運転（ITS協調型） | *信頼できないソースからのデータ入力* | 6.7 | ✔ | ✔ | | ✔ | 項目追加 | *ITサービス事業者およびインフラ整備責任主体（政府等）においても、評価ガイドとは別に対策の検討が必要* |
| | | | | *大量のデータ送信による妨害* | 10.0 | ✔ | ✔ | | ✔ | 項目追加 | |
| | | 1-9 | 自動駐車（スマホ連携） | *ｻｰﾊﾞｰへの不正侵入によるｻｰﾊﾞｰ乗っ取り* | 4.3 | | ✔ | | | （ｽｺｰﾌﾟ外） | *SIP「重要インフラ等」におけるサイバーセキュリティの確保」にて検討* |
| | | | | *信頼できないソースからのデータ入力* | 6.7 | ✔ | ✔ | | | 項目追加 | |
| 2 | 安全走行支援 | 2-2 | 歩行者検知（V2P型） | *信頼できないソースからのデータ入力* | 4.4 | ✔ | | ✔ | | 項目追加 | *ヒトが利用するﾃﾞﾊﾞｲｽへの対策については、デバイス提供事業者において、評価ｶﾞｲﾄﾞとは別に、対策の検討が必要* |
| | | | | *大量のデータ送信による妨害* | 6.7 | ✔ | | ✔ | | | |
| 4 | ｿﾌﾄｳｪｱｱｯﾌﾟﾃﾞｰﾄ | 4-1 | OTA | *アップデートの妨害/アップデートプログラムの改ざん（サーバー）* | 10.0 | ✔ | ✔ | | | 項目追加 | *SIP「重要インフラ等」におけるサイバーセキュリティの確保」にて検討* |
| | | | | *正当なアップデート実行の妨害* | 4.3 | ✔ | ✔ | | | | |
| 5 | 故障検知 | 5-1 | 故障検知 | *ｻｰﾊﾞｰへの不正侵入によるｻｰﾊﾞｰ乗っ取り* | 4.3 | | ✔ | | | （ｽｺｰﾌﾟ外） | *SIP「重要インフラ等」におけるサイバーセキュリティの確保」にて検討* |
| 8 | 車両遠隔操作 | 8-1 | 遠隔からのﾄﾞｱﾛｯｸ・ｱﾝﾛｯｸ | *ｻｰﾊﾞｰへの不正侵入によるｻｰﾊﾞｰ乗っ取り* | 4.3 | | ✔ | | | （ｽｺｰﾌﾟ外） | *SIP「重要インフラ等」におけるサイバーセキュリティの確保」にて検討* |
| | | 8-3 | 充電制御 | | 4.3 | | ✔ | | | | |
| | | 8-4 | 充電制御（音声認識AI連携） | | 4.3 | | ✔ | | | | |
| | | 8-5 | エアコン制御 | | 4.3 | | ✔ | | | | |
| | | 8-6 | ｴｱｺﾝ制御（音声認識AI連携） | | 4.3 | | ✔ | | | | |
| | | 8-7 | エンジン再駆動・ステアリングロック解除禁止 | | 4.3 | | ✔ | | | | |

# 対策状況調査結果詳細(1/8)

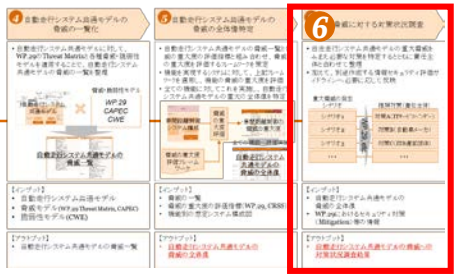


## 重大脅威に対する対策状況調査結果

| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| サービス | | 機能 | | 脅威 | 脅威の重大度 | セキュリティ対策 | 責任主体 | 評価ガイドとの対応 | 本事業外で必要な対応 |
|---|---|---|---|---|---|---|---|---|---|
| 名称 | | 名称 | | | | | | | |
| 1 | 運転・駐車支援 | 1-3 | 車間距離制御（V2V型） | 信頼できないソースからのデータ入力 | 4.4 | • 受信したすべてのメッセージのメッセージ認証<br>• 機密データを含む通信の暗号化<br>• タイムスタンプなど、リプレイ攻撃を防ぐテクニック<br>• ハッシュ、セキュリティ保護されたプロトコル、パケットフィルタリングなどの完全性チェックのためのテクニックの使用<br>• セッションハイジャックを避けるためのセッション管理ポリシー<br>• 他の車両センサー（温度、レーダーなど）を使用した整合性チェック<br>• メッセージの完全性と認証チェック<br>• 車両のファイル/データへのアクセス制御<br>• 信頼境界のネットワークセグメンテーションと実装<br>• システム監視<br>• ソフトウェアテスト<br>• アクティブメモリプロテクション<br>• ソフトウェアの完全性チェック技術<br>• オペレーティング・システムなどの脆弱性対策<br>• システムを守るための、ゲートウェイ、ファイアウォール、侵入防止/検知の組み合わせ、および監視<br>• タイムスタンプなど、リプレイ攻撃から保護するためのテクニック<br>• メッセージの内容とプロトコルの制限と監視 | 車両側:<br>自動車メーカ | 2.1.1 DrivebyDownload攻撃<br>2.1.2 ファイル添付攻撃<br>2.4.1 成りすまし攻撃<br>2.4.2 リプレイ攻撃 | - |
| | | | | 大量のデータ送信による妨害 | 6.7 | • メッセージへのタイムスタンプと有効期限の設定<br>• コンテキストを踏まえたレート制限措置<br>• 受信データのサイズの確認<br>• データの認証<br>• V2Xメッセージの承認メッセージの設定<br>• 通信を利用しないフォールバック戦略 | 車両側:<br>自動車メーカ | 2.3.3 TCU由来の攻撃<br>4.2.1 車両サービス（機能）の停止 | - |

# 対策状況調査結果詳細(2/8)

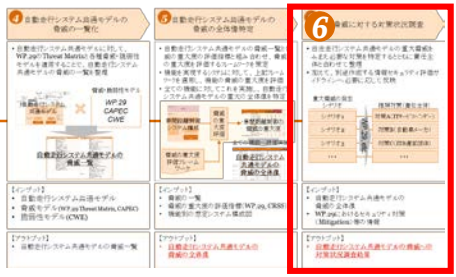


## 重大脅威に対する対策状況調査結果

| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| サービス | | 機能 | | 脅威 | 脅威の重大度 | セキュリティ対策 | 責任主体 | 評価ガイドとの対応 | 本事業外で必要な対応 |
|---|---|---|---|---|---|---|---|---|---|
| 名称 | | 名称 | | | | | | | |
| 1 | 運転・駐車支援 | 1-4 | 隊列走行(V2V型) | 信頼できないソースからのデータ入力 | 4.4 | • 受信したすべてのメッセージのメッセージ認証<br>• 機密データを含む通信の暗号化<br>• タイムスタンプなど、リプレイ攻撃を防ぐテクニック<br>• ハッシュ、セキュリティ保護されたプロトコル、パケットフィルタリングなどの完全性チェックのためのテクニックの使用<br>• セッションハイジャックを避けるためのセッション管理ポリシー<br>• 他の車両センサー(温度、レーダーなど)を使用した整合性チェック<br>• メッセージの完全性と認証チェック<br>• 車両のファイル/データへのアクセス制御<br>• 信頼境界のネットワークセグメンテーションと実装<br>• システム監視<br>• ソフトウェアテスト<br>• アクティブメモリプロテクション<br>• ソフトウェアの完全性チェック技術<br>• オペレーティング・システムなどの脆弱性対策<br>• システムを守るための、ゲートウェイ、ファイアウォール、侵入防止/検知の組み合わせ、および監視<br>• タイムスタンプなど、リプレイ攻撃から保護するためのテクニック<br>• メッセージの内容とプロトコルの制限と監視 | 車両側:<br>自動車メーカ | 2.1.1 DrivebyDownload攻撃<br>2.1.2 ファイル添付攻撃<br>2.4.1 成りすまし攻撃<br>2.4.2 リプレイ攻撃 | - |
| | | | | 大量のデータ送信による妨害 | 6.7 | • メッセージへのタイムスタンプと有効期限の設定<br>• コンテキストを踏まえたレート制限措置<br>• 受信データのサイズの確認<br>• データの認証<br>• V2Xメッセージの承認メッセージの設定<br>• 通信を利用しないフォールバック戦略 | 車両側:<br>自動車メーカ | 2.3.3 TCU由来の攻撃<br>4.2.1 車両サービス(機能)の停止 | - |

# 対策状況調査結果詳細(3/8)



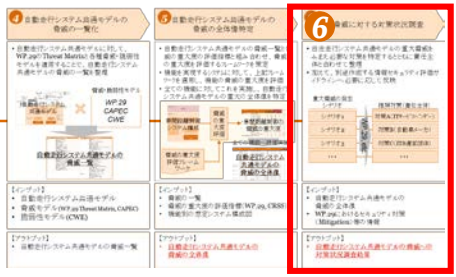
## 重大脅威に対する対策状況調査結果

| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| サービス | | 機能 | | 脅威 | 脅威の重大度 | セキュリティ対策 | 責任主体 | 評価ガイドとの対応 | 本事業外で必要な対応 |
|---|---|---|---|---|---|---|---|---|---|
| 名称 | | 名称 | | | | | | | |
| 1 | 運転・駐車支援 | 1-5 | 自動運転(ITS協調型) | 信頼できないソースからのデータ入力 | 6.7 | • 受信したすべてのメッセージのメッセージ認証<br>• 機密データを含む通信の暗号化<br>• タイムスタンプなど、リプレイ攻撃を防ぐテクニック<br>• ハッシュ、セキュリティ保護されたプロトコル、パケットフィルタリングなどの完全性チェックのためのテクニックの使用<br>• セッションハイジャックを避けるためのセッション管理ポリシー<br>• 他の車両センサー(温度、レーダーなど)を使用した整合性チェック<br>• メッセージの完全性と認証チェック<br>• 車両のファイル/データへのアクセス制御<br>• 信頼境界のネットワークセグメンテーションと実装<br>• システム監視<br>• ソフトウェアテスト<br>• アクティブメモリプロテクション<br>• ソフトウェアの完全性チェック技術<br>• オペレーティング・システムなどの脆弱性対策<br>• システムを守るための、ゲートウェイ、ファイアウォール、侵入防止/検知の組み合わせ、および監視<br>• タイムスタンプなど、リプレイ攻撃から保護するためのテクニック<br>• メッセージの内容とプロトコルの制限と監視 | 車両側:<br>自動車メーカ<br><br>インフラ側:<br>政府(道路交通分科会など)<br><br>サーバ側:<br>ITサービス事業者*1 | 2.1.1 DrivebyDownload攻撃<br>2.1.2 ファイル添付攻撃<br>2.4.1 成りすまし攻撃<br>2.4.2 リプレイ攻撃 | ITサービス事業者およびインフラ整備責任主体(政府等)においても、評価ガイドとは別に対策の検討が必要 |
| | | | | 大量のデータ送信による妨害 | 10.0 | • メッセージへのタイムスタンプと有効期限の設定<br>• コンテキストを踏まえたレート制限措置<br>• 受信データのサイズの確認<br>• データの認証<br>• V2Xメッセージの承認メッセージの設定<br>• 通信を利用しないフォールバック戦略 | 車両側:<br>自動車メーカ<br><br>インフラ側:<br>政府(道路交通分科会など)<br><br>サーバ側:<br>ITサービス事業者*1 | 2.3.3 TCU由来の攻撃<br>4.2.1 車両サービス(機能)の停止 | 同上 |

*1: サーバ運営事業者が運営受託業者の場合は委託元が責任主体

# 対策状況調査結果詳細(4/8)



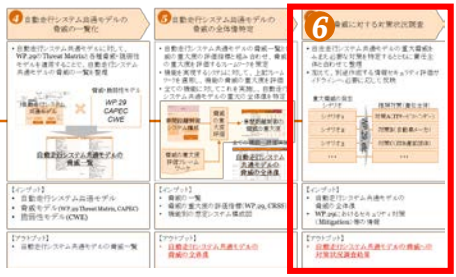
## 重大脅威に対する対策状況調査結果

| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| サービス | | 機能 | | 脅威 | 脅威の重大度 | セキュリティ対策 | 責任主体 | 評価ガイドとの対応 | 本事業外で必要な対応 |
|---|---|---|---|---|---|---|---|---|---|
| 名称 | | 名称 | | | | | | | |
| 1 | 運転・駐車支援 | 1-9 | 自動駐車(スマホ連携) | サーバーへの不正侵入によるサーバー乗っ取り | 4.3 | • セキュアなサーバ設定(システムの脆弱性対策など)<br>• 外部インターネット接続の保護(受信したメッセージの認証/検証、暗号化された通信経路の提供などの)<br>• サーバシステムと通信の監視<br>• クラウドサーバーのリスクとセキュリティの管理(使用されている場合)<br>• セキュリティ情報とセキュリティベントの管理 | サーバ側:<br>ITサービス事業者*1 | (記載なし) | 4.2.4 自動車セキュリティの分析整理と技術課題の今後の方向性*2 |
| | | | | 信頼できないソースからのデータ入力 | 6.7 | • 受信したすべてのメッセージのメッセージ認証<br>• 機密データを含む通信の暗号化<br>• タイムスタンプなど、リプレイ攻撃を防ぐテクニック<br>• ハッシュ、セキュリティ保護されたプロトコル、パケットフィルタリングなどの完全性チェックのためのテクニックの使用<br>• セッションハイジャックを避けるためのセッション管理ポリシー<br>• 他の車両センサー(温度、レーダーなど)を使用した整合性チェック<br>• メッセージの完全性と認証チェック<br>• 車両のファイル/データへのアクセス制御<br>• 信頼境界のネットワークセグメンテーションと実装<br>• システム監視<br>• ソフトウェアテスト<br>• アクティブメモリプロテクション<br>• ソフトウェアの完全性チェック技術<br>• オペレーティング・システムなどの脆弱性対策<br>• システムを守るための、ゲートウェイ、ファイアウォール、侵入防止/検知の組み合わせ、および監視<br>• タイムスタンプなど、リプレイ攻撃から保護するためのテクニック<br>• メッセージの内容とプロトコルの制限と監視 | 車両側:<br>自動車メーカ<br><br>サーバ側:<br>ITサービス事業者*1 | 2.1.1 DrivebyDownload攻撃<br>2.1.2 ファイル添付攻撃<br>2.4.1 成りすまし攻撃<br>2.4.2 リプレイ攻撃 | 同上 |

*1: サーバ運営事業者が運営受託業者の場合は委託元が責任主体
*2: SIP「重要インフラ等におけるサイバーセキュリティの確保」にて検討

# 対策状況調査結果詳細(5/8)

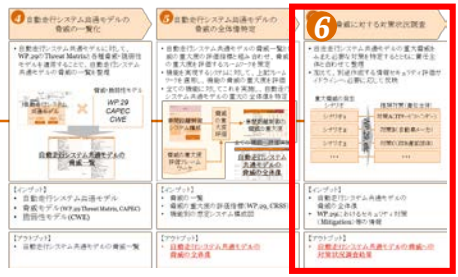


## 重大脅威に対する対策状況調査結果

| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| サービス | | 機能 | | 脅威 | 脅威の重大度 | セキュリティ対策 | 責任主体 | 評価ガイドとの対応 | 本事業外で必要な対応 |
|---|---|---|---|---|---|---|---|---|---|
| 名称 | | 名称 | | | | | | | |
| 2 | 安全走行支援 | 2-2 | 歩行者検知(V2P型) | 信頼できないソースからのデータ入力 | 4.4 | • 受信したすべてのメッセージのメッセージ認証<br>• 機密データを含む通信の暗号化<br>• タイムスタンプなど、リプレイ攻撃を防ぐテクニック<br>• ハッシュ、セキュリティ保護されたプロトコル、パケットフィルタリングなどの完全性チェックのためのテクニックの使用<br>• セッションハイジャックを避けるためのセッション管理ポリシー<br>• 他の車両センサー(温度、レーダーなど)を使用した整合性チェック<br>• メッセージの完全性と認証チェック<br>• 車両のファイル/データへのアクセス制御<br>• 信頼境界のネットワークセグメンテーションと実装<br>• システム監視<br>• ソフトウェアテスト<br>• アクティブメモリプロテクション<br>• ソフトウェアの完全性チェック技術<br>• オペレーティング・システムなどの脆弱性対策<br>• システムを守るための、ゲートウェイ、ファイアウォール、侵入防止/検知の組み合わせ、および監視<br>• タイムスタンプなど、リプレイ攻撃から保護するためのテクニック<br>• メッセージの内容とプロトコルの制限と監視 | デバイス側:<br>デバイス提供事業者<br><br>車両側:<br>自動車メーカ | 2.1.1 DrivebyDownload攻撃<br>2.1.2 ファイル添付攻撃<br>2.4.1 成りすまし攻撃<br>2.4.2 リプレイ攻撃 | ヒトが利用するデバイス側における対策については、評価ガイドの対象外であり、今後検討が必要 |
| | | | | 大量のデータ送信による妨害 | 6.7 | • メッセージへのタイムスタンプと有効期限の設定<br>• コンテキストを踏まえたレート制限措置<br>• 受信データのサイズの確認<br>• データの認証<br>• V2Xメッセージの承認メッセージの設定<br>• 通信を利用しないフォールバック戦略 | デバイス側:<br>デバイス提供事業者<br><br>車両側:<br>自動車メーカ | 2.3.3 TCU由来の攻撃<br>4.2.1 車両サービス(機能)の停止 | 同上 |

# 対策状況調査結果詳細(6/8)



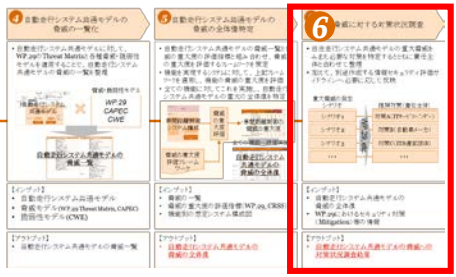
## 重大脅威に対する対策状況調査結果

| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| サービス | | 機能 | | 脅威 | 脅威の重大度 | セキュリティ対策 | 責任主体 | 評価ガイドとの対応 | 本事業外で必要な対応 |
|---|---|---|---|---|---|---|---|---|---|
| 名称 | | 名称 | | | | | | | |
| 4 | ｿﾌﾄｳｪｱｱｯﾌﾟﾃﾞｰﾄ | 4-1 | OTA | アップデートの妨害/アップデートプログラムの改ざん(サーバー) | 10.0 | • ソフトウェア更新における暗号化保護と署名の実装<br>• 専用線の利用等によるアップデートに使用される通信のセキュリティ確保<br>• アップデートの正確の保証<br>• テンプレートとポリシーの設定を含むセキュアな手順の確立<br>• 構成管理を確実にし、ｱｯﾌﾟﾃﾞｰﾄのﾛｰﾙﾊﾞｯｸが可能であること<br>• 使用される暗号の有効な鍵管理と保護<br>• アップデートに関するバージョンとタイムスタンプとロギング | 車両側:<br>自動車ﾒｰｶ<br><br>サーバ側:<br>ITｻｰﾋﾞｽ事業者*1 | 4.3.1 制御系ファームウェアの改ざん<br><br>4.4.1 情報系アプリケーションの改ざん | 4.2.4 自動車セキュリティの分析整理と技術課題の今後の方向性*2 |
| | | | | 正当なアップデート実行の妨害. | 4.3 | • 許可されていない物理的アクセスを最小化し、防止するための対策<br>• 釣り合いのとれた物理的保護とモニタリング<br>• 従業員の役割に基づくアクセス制御<br>• データ消失時の影響を低減するためのデータ最小化技術 | 車両側:<br>自動車ﾒｰｶ<br><br>サーバ側:<br>ITｻｰﾋﾞｽ事業者*1 | 2.3.3 TCU由来の攻撃<br>4.2.1 車両サービス(機能)の停止 | 同上 |

*1: サーバ運営事業者が運営受託業者の場合は委託元が責任主体
*2: SIP「重要インフラ等におけるサイバーセキュリティの確保」にて検討

# 対策状況調査結果詳細(7/8)



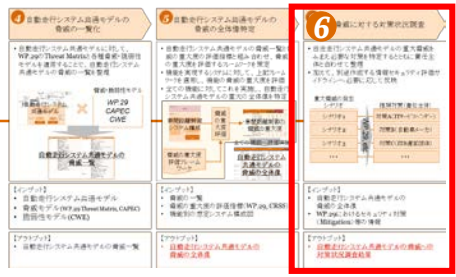
## 重大脅威に対する対策状況調査結果

| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| サービス | | 機能 | | 脅威 | 脅威の重大度 | セキュリティ対策 | 責任主体 | 評価ガイドとの対応 | 本事業外で必要な対応 |
|---|---|---|---|---|---|---|---|---|---|
| 名称 | | 名称 | | | | | | | |
| 5 | 故障検知 | 5-1 | 故障検知 | サーバーへの不正侵入によるサーバー乗っ取り | 4.3 | • セキュアなサーバ設定(システムの脆弱性対策など)<br>• 外部インターネット接続の保護(受信したメッセージの認証/検証、暗号化された通信経路の提供などの)<br>• サーバシステムと通信の監視<br>• クラウドサーバーのリスクとセキュリティの管理(使用されている場合)<br>• セキュリティ情報とセキュリティベントの管理 | サーバ側:ITサービス事業者*1 | (記載なし) | 4.2.4 自動車セキュリティの分析整理と技術課題の今後の方向性*2 |
| 8 | 車両遠隔操作 | 8-1 | 遠隔からのドアロック・アンロック | サーバーへの不正侵入によるサーバー乗っ取り | 4.3 | • セキュアなサーバ設定(システムの脆弱性対策など)<br>• 外部インターネット接続の保護(受信したメッセージの認証/検証、暗号化された通信経路の提供などの)<br>• サーバシステムと通信の監視<br>• クラウドサーバーのリスクとセキュリティの管理(使用されている場合)<br>• セキュリティ情報とセキュリティベントの管理 | サーバ側:ITサービス事業者*1 | (記載なし) | 同上 |
| | | 8-3 | 充電制御 | サーバーへの不正侵入によるサーバー乗っ取り | 4.3 | • セキュアなサーバ設定(システムの脆弱性対策など)<br>• 外部インターネット接続の保護(受信したメッセージの認証/検証、暗号化された通信経路の提供などの)<br>• サーバシステムと通信の監視<br>• クラウドサーバーのリスクとセキュリティの管理(使用されている場合)<br>• セキュリティ情報とセキュリティベントの管理 | サーバ側:ITサービス事業者*1 | (記載なし) | 同上 |
| | | 8-4 | 充電制御(音声認識AI連携) | サーバーへの不正侵入によるサーバー乗っ取り | 4.3 | • セキュアなサーバ設定(システムの脆弱性対策など)<br>• 外部インターネット接続の保護(受信したメッセージの認証/検証、暗号化された通信経路の提供などの)<br>• サーバシステムと通信の監視<br>• クラウドサーバーのリスクとセキュリティの管理(使用されている場合)<br>• セキュリティ情報とセキュリティベントの管理 | サーバ側:ITサービス事業者*1 | (記載なし) | 同上 |

*1: サーバ運営事業者が運営受託業者の場合は委託元が責任主体
*2: SIP「重要インフラ等におけるサイバーセキュリティの確保」にて検討

# 対策状況調査結果詳細(8/8)

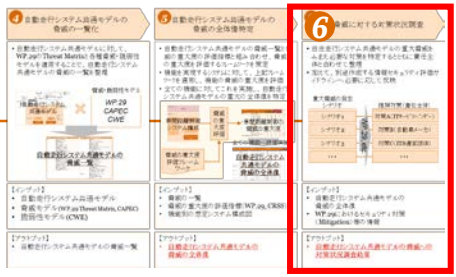


## 重大脅威に対する対策状況調査結果

| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

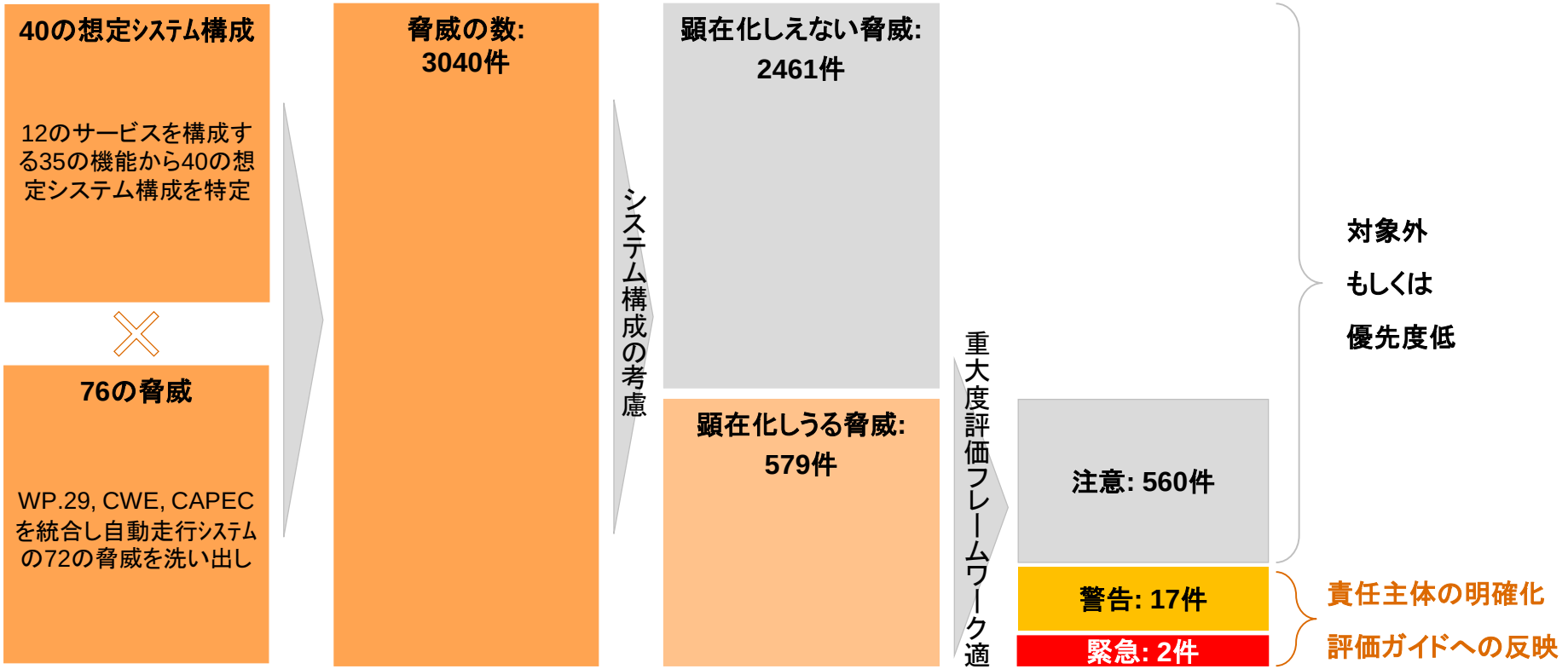
| サービス | | 機能 | | 脅威 | 脅威の重大度 | セキュリティ対策 | 責任主体 | 評価ガイドとの対応 | 本事業外で必要な対応 |
|---|---|---|---|---|---|---|---|---|---|
| 名称 | | 名称 | | | | | | | |
| 8 | 車両遠隔操作 | 8-5 | エアコン制御 | サーバーへの不正侵入によるサーバー乗っ取り | 4.3 | • セキュアなサーバ設定(システムの脆弱性対策など)<br>• 外部インターネット接続の保護(受信したメッセージの認証/検証、暗号化された通信経路の提供などの)<br>• サーバシステムと通信の監視<br>• クラウドサーバーのリスクとセキュリティの管理(使用されている場合)<br>• セキュリティ情報とセキュリティベントの管理 | サーバ側:ITサービス事業者*1 | (記載なし) | 4.2.4 自動車セキュリティの分析整理と技術課題の今後の方向性*2 |
| | | 8-6 | エアコン制御(音声認識AI連携) | サーバーへの不正侵入によるサーバー乗っ取り | 4.3 | • セキュアなサーバ設定(システムの脆弱性対策など)<br>• 外部インターネット接続の保護(受信したメッセージの認証/検証、暗号化された通信経路の提供などの)<br>• サーバシステムと通信の監視<br>• クラウドサーバーのリスクとセキュリティの管理(使用されている場合)<br>• セキュリティ情報とセキュリティベントの管理 | サーバ側:ITサービス事業者*1 | (記載なし) | 同上 |
| | | 8-7 | エンジン再駆動・ステアリングロック解除禁止 | サーバーへの不正侵入によるサーバー乗っ取り | 4.3 | • セキュアなサーバ設定(システムの脆弱性対策など)<br>• 外部インターネット接続の保護(受信したメッセージの認証/検証、暗号化された通信経路の提供などの)<br>• サーバシステムと通信の監視<br>• クラウドサーバーのリスクとセキュリティの管理(使用されている場合)<br>• セキュリティ情報とセキュリティベントの管理 | サーバ側:ITサービス事業者*1 | (記載なし) | 同上 |

*1: サーバ運営事業者が運営受託業者の場合は委託元が責任主体
*2: SIP「重要インフラ等におけるサイバーセキュリティの確保」にて検討

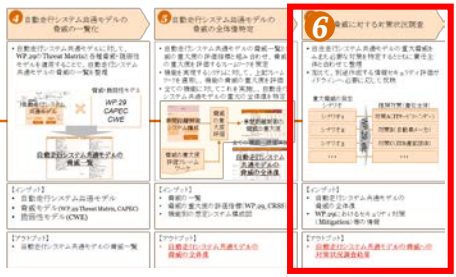


# 脅威の全体像調査のアプローチ（まとめ）

- 自動走行システムに係るすべてのシステム構成を踏まえ顕在化しうる脅威を抽出し、重大度評価フレームワークを適用することで優先して対応すべき脅威を特定
- 特定した脅威に対して、対策の責任主体を明確化するとともに、車両側での対策が必要な脅威は、評価ガイドへ反映



# ステークホルダーが危惧すべき脅威と対策の提言



## 01 自動車メーカ

- 自動車メーカは、ITS 協調型の自動運転機能に対する「大量データ送信による妨害」などの脅威への対策が必要である
- 自動車メーカが主体的に対策すべき重大脅威については評価ガイドラインへ項目を追加しており、今後これらに基づき評価することで対策がなされることを期待している

## 02 ITサービス事業者

- ITサービス事業者は、OTA機能に対する「アップデート妨害」などの脅威への対策が必要である
- これらは主にサーバ等の情報システムにおける対策が必要であり、本プロジェクトの検討範囲外である
- 一方で、SIP「重要インフラ等のけるサイバーセキュリティの確保」にて対応検討中であり、今後は協力した取り組みが重要となる

## 03 政府等

- 政府等は、自動車と協調する交通インフラに対する「大量データ送信による妨害」などの脅威への対策が必要である
- これらに対する自動走行システムと協調したセキュリティ対策は現状未検討の状態であり、今後の普及に向けて本格的なセキュリティ対策の検討が必要である

## 04 デバイス提供事業者

- デバイス提供事業者は、V2P 用途のウェアラブルデバイスやスマートデバイスに対する「信頼できないソースからのデータの入力」などの脅威への対策が必要である
- これらに対する自動走行システムと協調したセキュリティ対策は現状未検討の状態であり、今後の普及に向けて本格的なセキュリティ対策の検討が必要である

# 別紙1：機能別の想定システム構成

# 1-1. 車間距離制御

## 1. 機能概要

ITSと協調することなしに、先行車両との車間距離を制御する機能。状況に応じた、警告の音声による通知とディスプレイへの表示も行う。以下のようなセンサー等を活用する。

- カメラ
- ミリ波レーダーなど

## 2. 実装状況

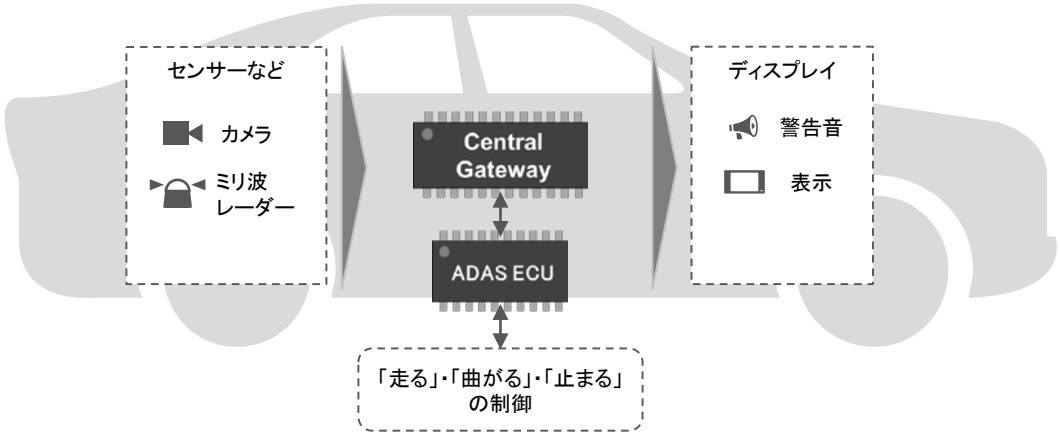
| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

| 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|

## 4. 想定システム構成

車両外部接続無し



# 1-2. 車線維持制御

## 1. 機能概要

ITSと協調することなしに、走行車線の維持を制御する機能。状況に応じた、警告の音声による通知とディスプレイへの表示も行う。搭載されたカメラより収集したデータを活用し制御する。

## 2. 実装状況

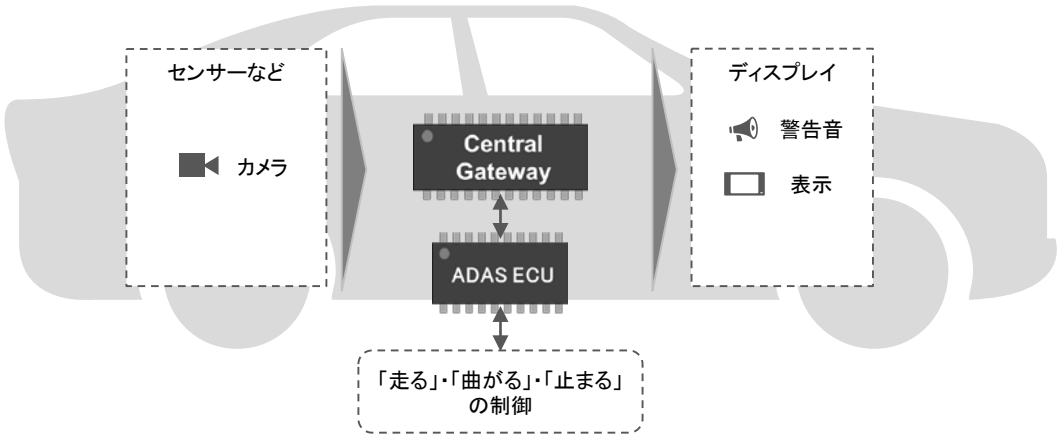
| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

| 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|

## 4. 想定システム構成

車両外部接続無し



# 1-3. 車間距離制御(V2V型)

## 1. 機能概要

ITSと協調することで、先行車両との車間距離を制御する機能。状況に応じた、警告の音声による通知とディスプレイへの表示も行う。以下のようなセンサー等を活用する。

- カメラ
- ミリ波レーダーなど

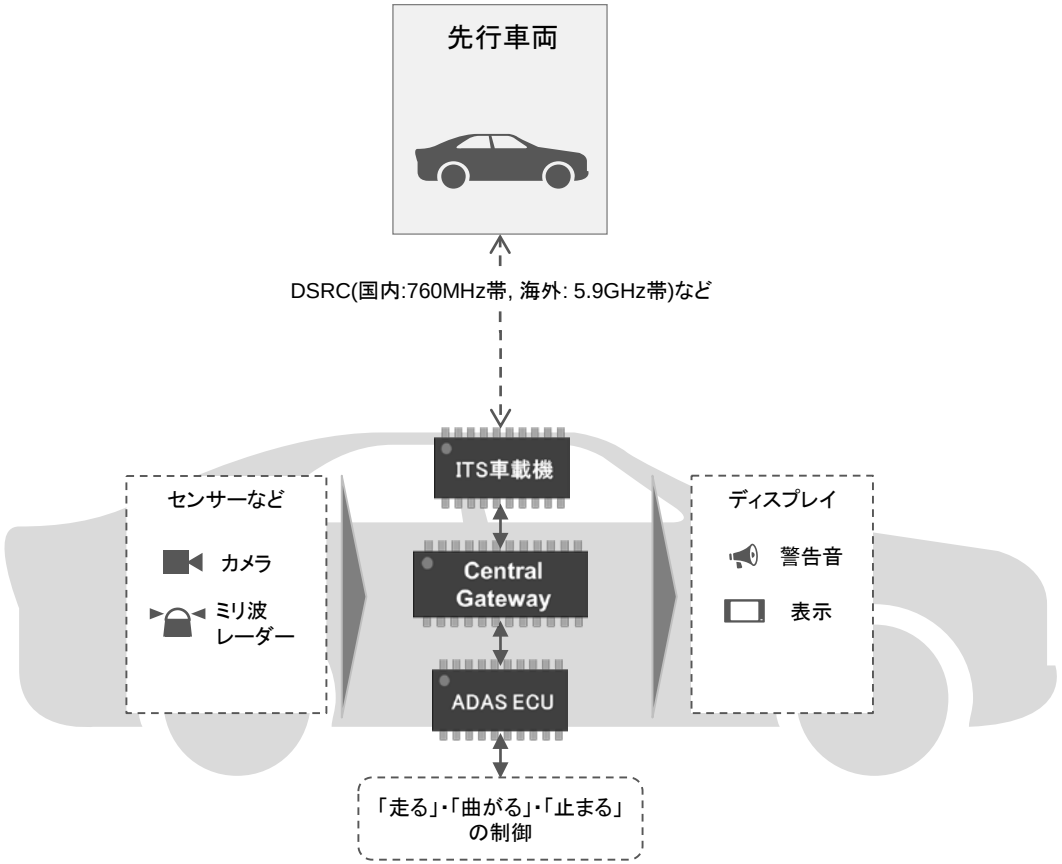
## 2. 実装状況

| 実装済み*1*2 | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

| 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|

## 4. 想定システム構成




*1: 2018年2月現在、日本国内の特定の自動車メーカが製造する特定の車両において実装されている
*2: 日本では760MHz帯の周波数を活用しているが、米国・欧州は5.9GHzなどの高周波帯で整備検討中

# 1-4. 隊列走行（V2V型）

## 1. 機能概要

先頭車両と通信を行うことで、後続車両が無人で先頭車両を追随することを可能とする機能。トラックなどの商用車向けの機能。以下のようなセンサー等を活用する。

- カメラ
- LiDAR
- ミリ波レーダーなど

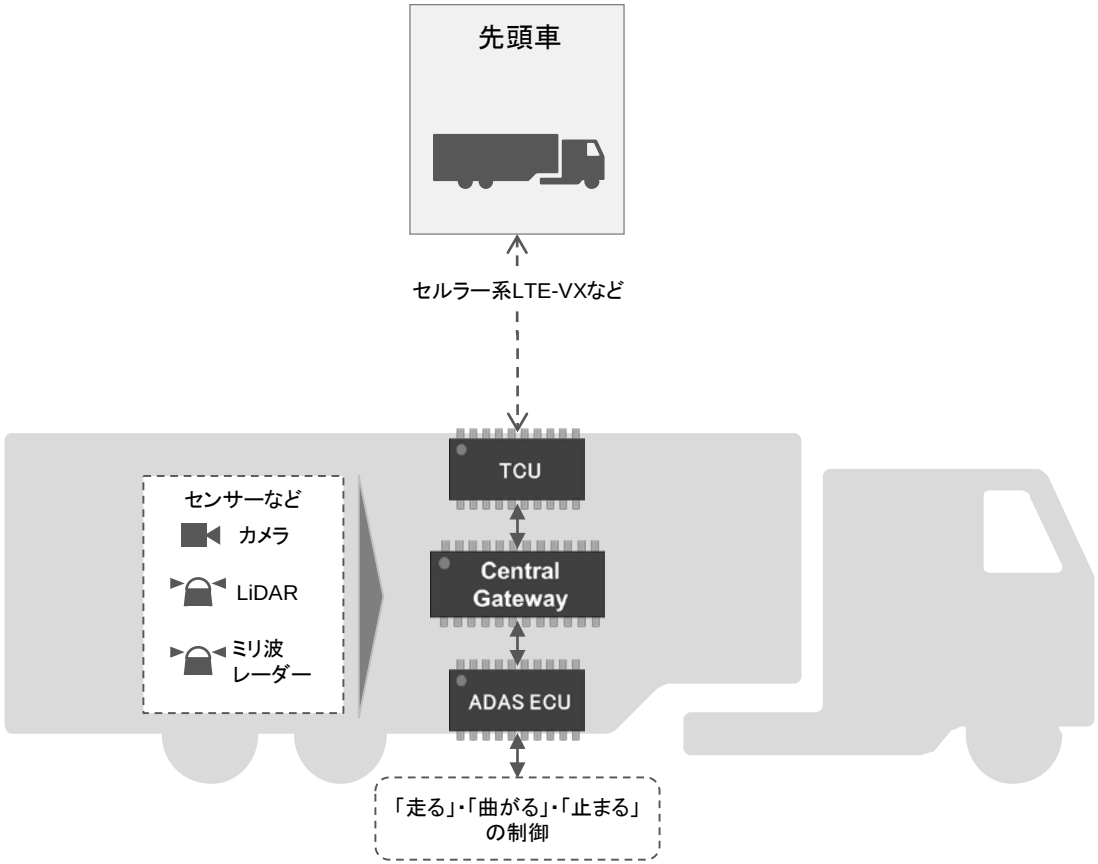
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

| 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|

## 4. 想定システム構成



# 1-5. 自動運転(ITS協調型)

## 1. 機能概要

車両に搭載した各種センサー等に加え、以下に示すようなITSを中心とした車両外部システムと協調することで、人間に代わりあらゆる運転タスクを実施することを可能とする機能。

- 交通インフラ
- 自動車
- 位置情報衛星
- ダイナミックマップシステムなど

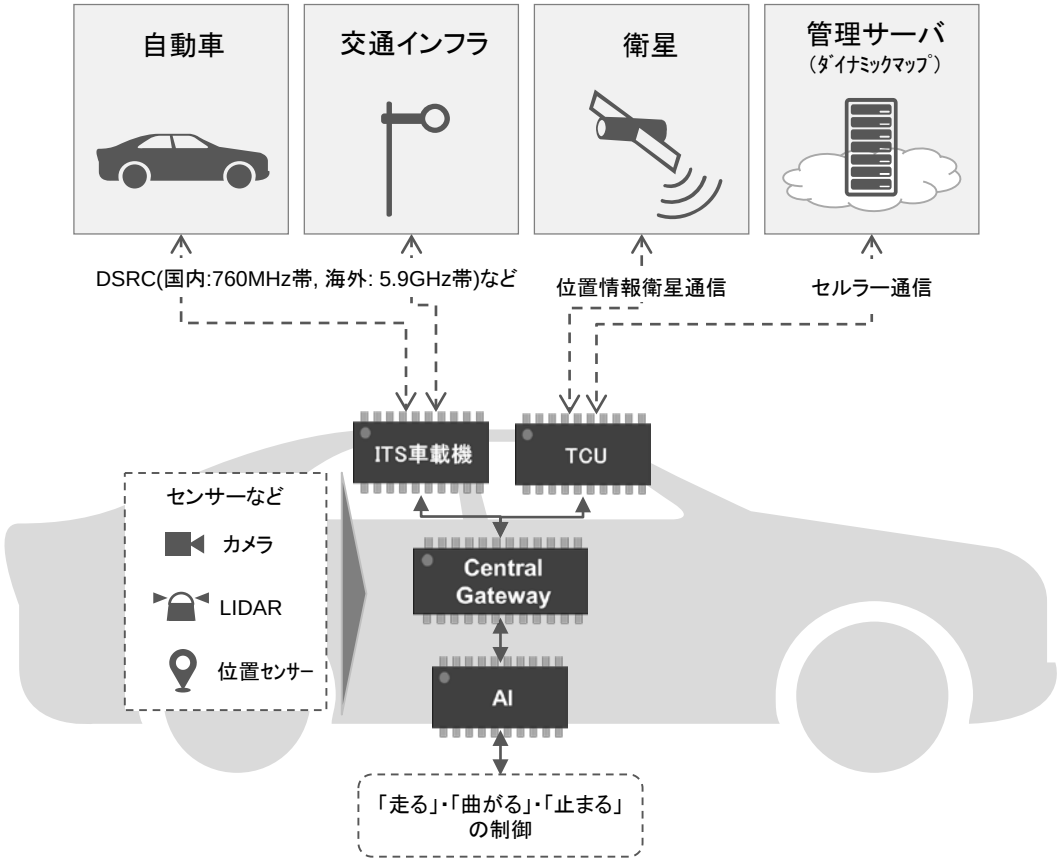
## 2. 実装状況

| 実装済み | 開発中*1*2 |
|---|---|

## 3. 自動走行レベル (SAE)

| 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|

## 4. 想定システム構成




*1: 2020年代前半の実用化に向けて自動車OEMにて開発中
*2: 日本では760MHz帯の周波数を活用し、米国・欧州は5.9GHzなどの高周波帯を活用し整備検討中

# 1-6. 自動運転（自律型）

## 1. 機能概要

ITSなどの車両外部システムと協調することなく、車両に搭載する以下のようなセンサー類を活用することで、人間に代わりあらゆる運転タスクを実施する機能。

- ビデオカメラ
- LiDAR
- 距離センサー
- 位置センサーなど

## 2. 実装状況

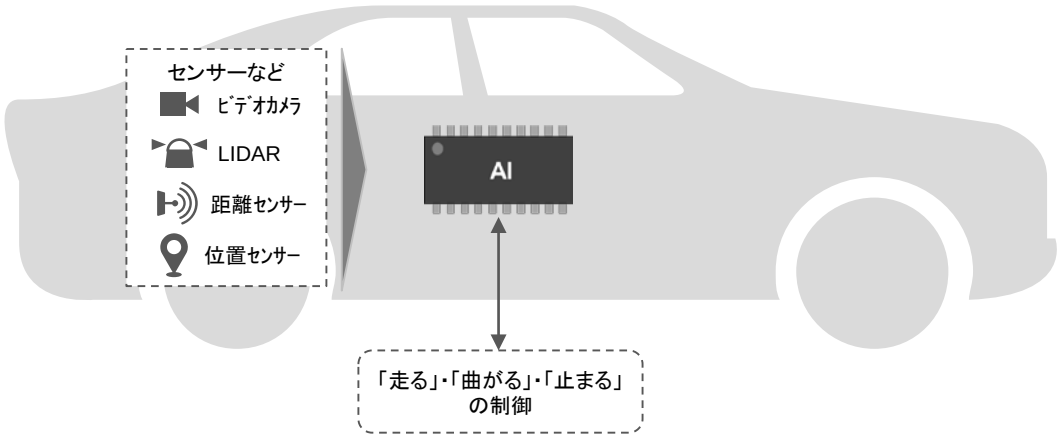
| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

| 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|

## 4. 想定システム構成

車両外部接続無し



# 1-7. 駐車周辺映像表示

## 1. 機能概要

駐車スペースの周辺の映像を360°カメラなどの映像として内蔵ディスプレイに表示するなどし、運転者による車両の駐車を支援する機能。

## 2. 実装状況

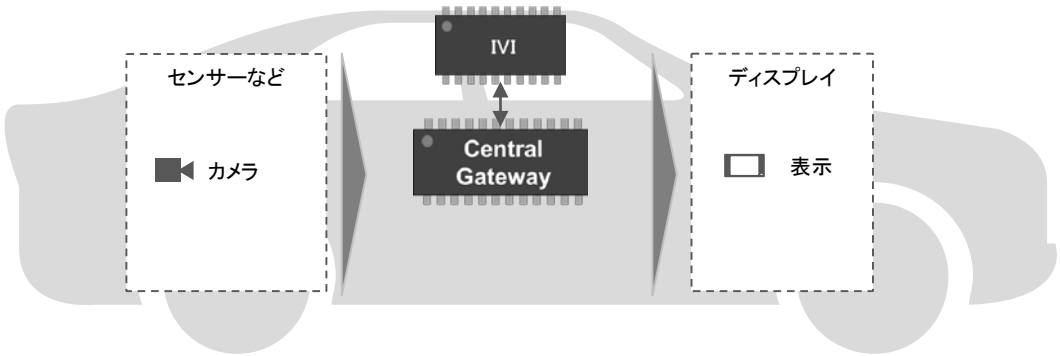
| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成

車両外部接続無し



# 1-8. 自動駐車(自律型)

## 1. 機能概要

ITSなどの車両外部システムと協調することなく、車両に搭載する以下のようなセンサー類を活用することで、人間に代わり車両の駐車を実施する機能。

- 高解像度カメラ
- 超音波ソナーなど

## 2. 実装状況

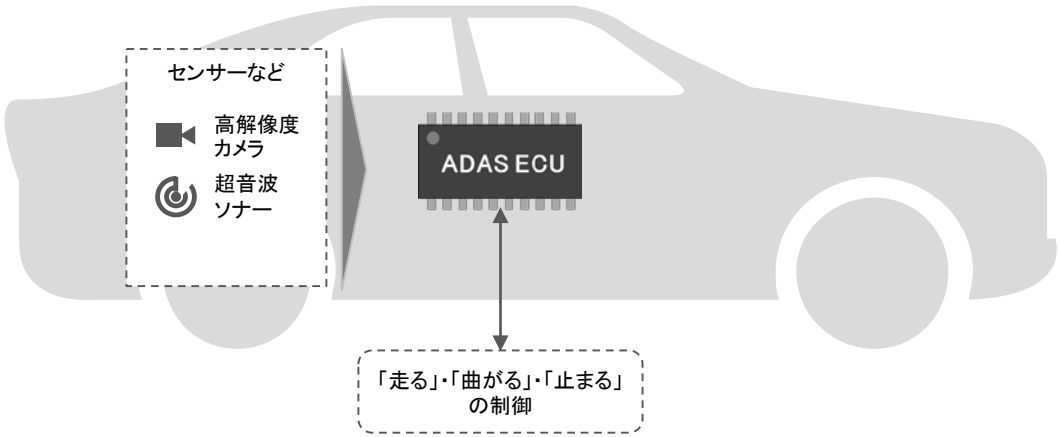
| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

| 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|

## 4. 想定システム構成

車両外部接続無し

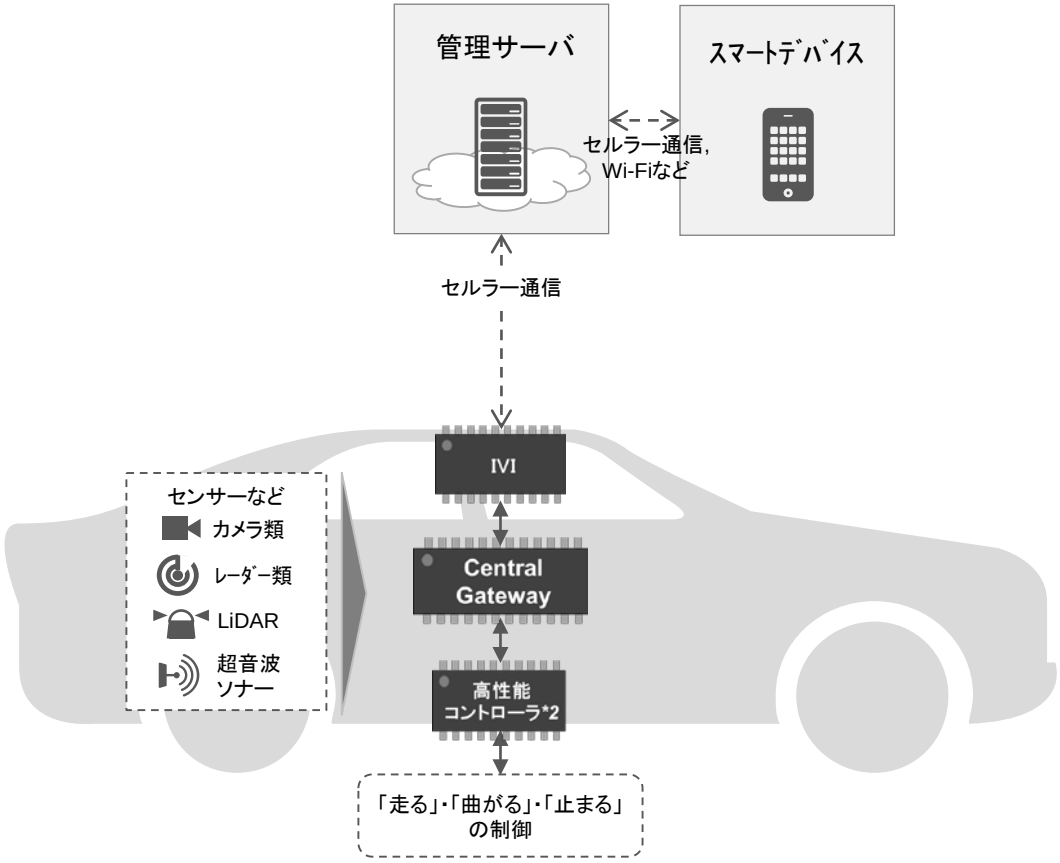


# 1-9. 自動駐車（スマホ連携）

## 1. 機能概要

スマートフォンにインストールされたアプリケーション経由で車両の駐車に関する操作指示を行い、遠隔から人間に代わり車両の駐車を実施する機能。以下のようなセンサー等を活用する。

- フロント/360°カメラ
- 赤外線カメラ
- ミッドレンジ/ロングレンジレーダー
- LiDAR
- 超音波ソナーなど




## 2. 実装状況

| 実装済み | 開発中*1 |
|---|---|

## 3. 自動走行レベル (SAE)

| 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|

*1: 欧州の一部の自動車メーカが、特定の高級車モデルにおいてし、2018年に販売予定
*2: 制御コントローラとして演算性能の高いSoC(System-on-a-chip)が利用される

# 2-1. 緊急ブレーキ

## 1. 機能概要

歩行者や関する車両・障害物を検知した際に、音声/表示により運転者に警告・必要に応じた自動ブレーキを実施する機能。以下のようなセンサー等を活用する。

- カメラ
- レーダー
- 超音波ソナー

## 2. 実装状況

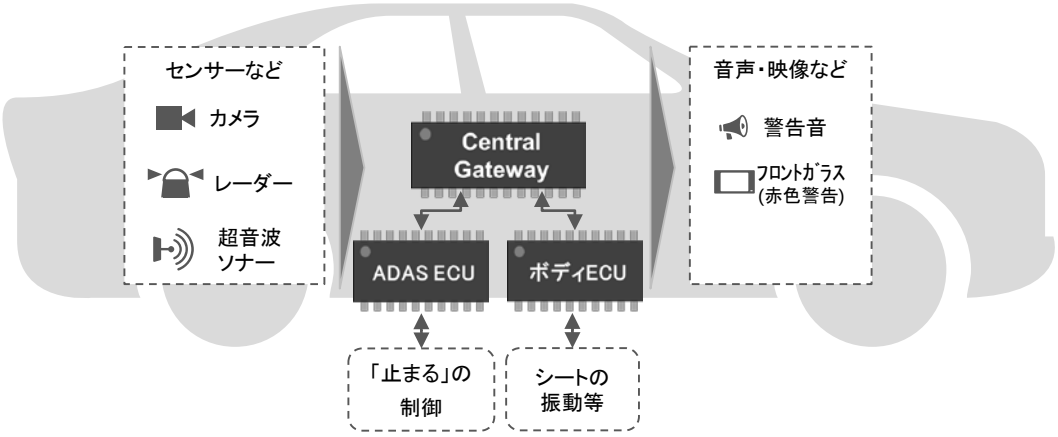
| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成

車両外部接続無し



# 2-2. 歩行者検知(V2P型)

## 1. 機能概要

歩行者の所有するスマートデバイスと連携し、車両の近くにいる歩行者を検知することで、必要に応じて車両を制御し歩行者との衝突を回避する機能。

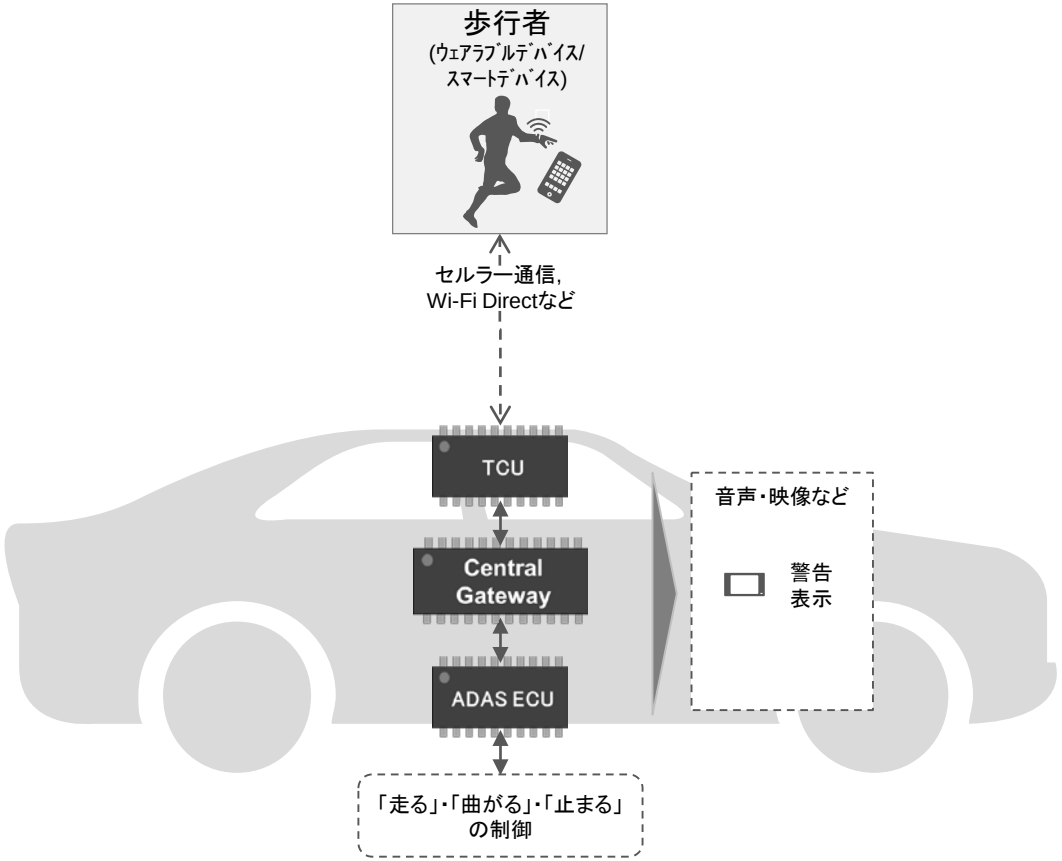
## 2. 実装状況

| 実装済み | 開発中*1*2 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成




*1: 米国の自動車メーカなどで実用に向けて開発中

*2: 現時点では通信インターフェースはWi-Fi Direct、セルラー通信など複数乱立している状況

# 2-3. 注意喚起(ITS協調型)

## 1. 機能概要

協調型ITSを活用した路車間通信システムにより、周辺環境の情報を提供することで、以下に示すような機能を提供。

- 右折時注意喚起
- 赤信号注意喚起
- 信号待ち発信準備案内
- 緊急車両存在通知など

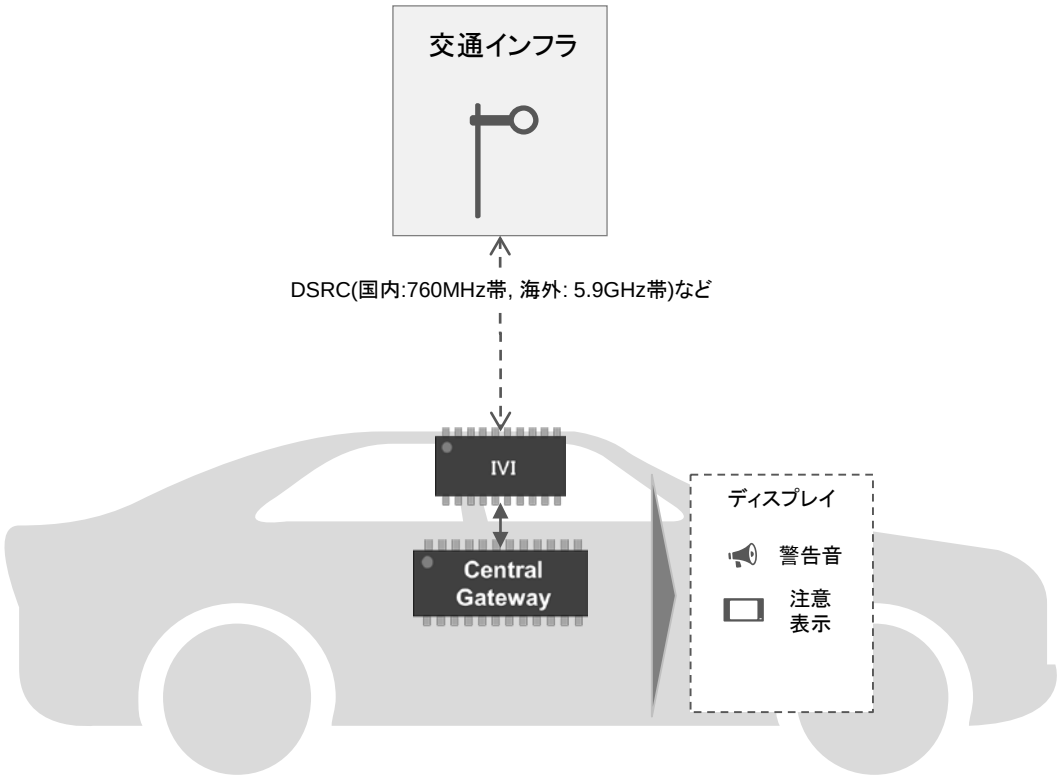
## 2. 実装状況

| 実装済み*1*2 | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成




*1: 車両とITSの両方で対応が必要であり普及率はまだ低い(日本国内の一部車両、大都市圏の一部の交差点のみで整備済み)
*2: 日本では760MHz帯の周波数を活用しているが、米国・欧州は5.9GHzなどの高周波帯で整備検討中

# 3-1. 省燃費走行支援

## 1. 機能概要

燃費効率の良い走行を支援するために、アクセルワークを制御する機能。主にトラックなどの商用車で利用される。

## 2. 実装状況

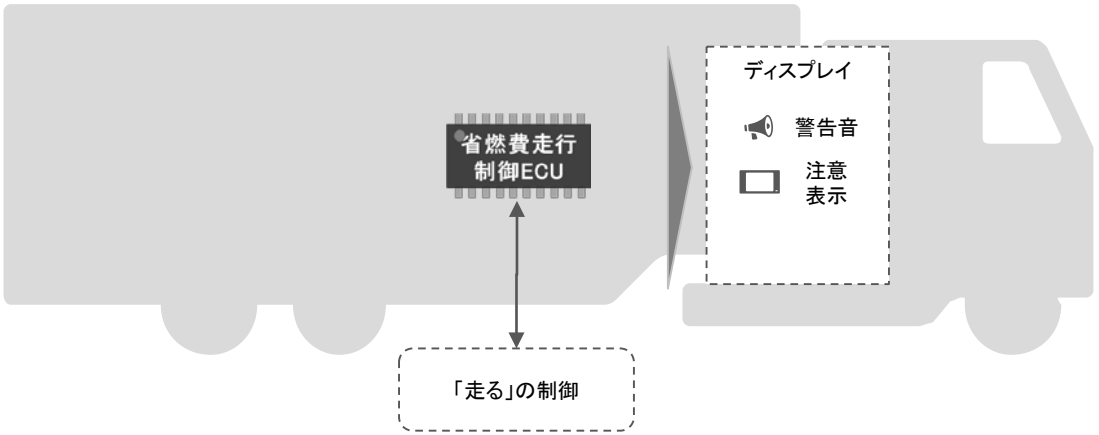
| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成

車両外部接続無し



# 4-1. OTA

## 1. 機能概要

無線通信を利用することで、遠隔地より電子制御システムのソフトウェアのアップデートを行う機能。

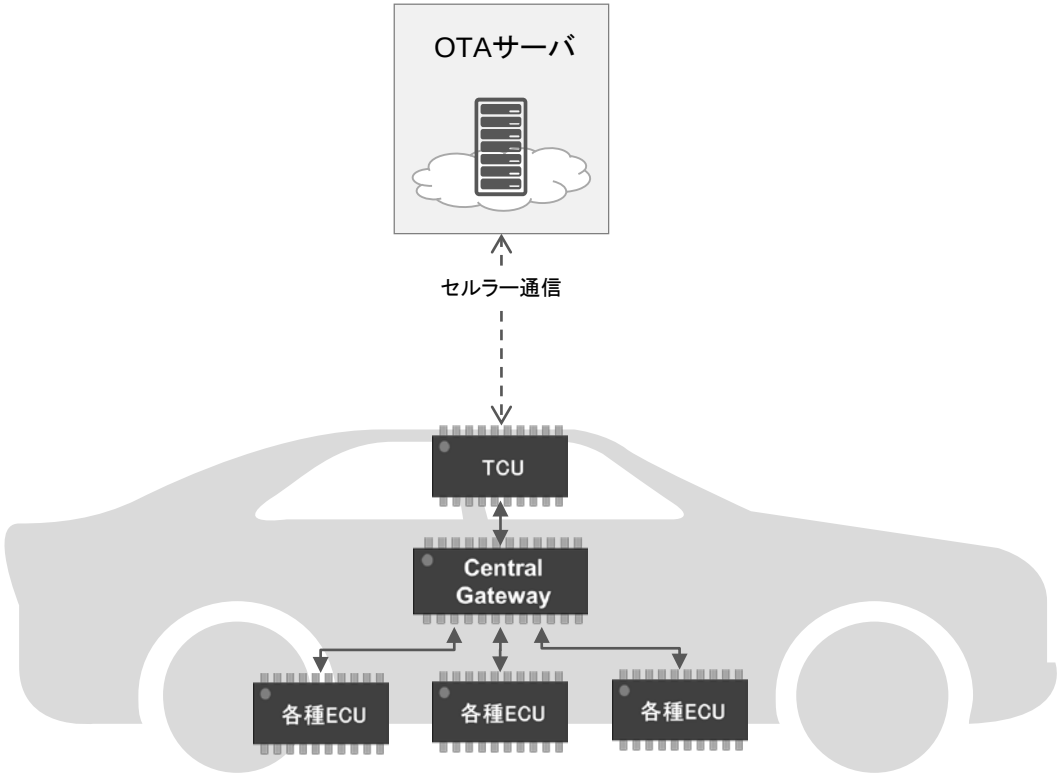
## 2. 実装状況

| 実装済み*1 | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成




*1: 今後急速に普及が進むことが想定されるが、現在は、一部の自動車メーカにおいて実装されている状況

# 5-1. 故障検知

## 1. 機能概要

自動車に備わる自己診断機能を活用し、車両を構成するコンポーネントの故障を予知・検知する機能。

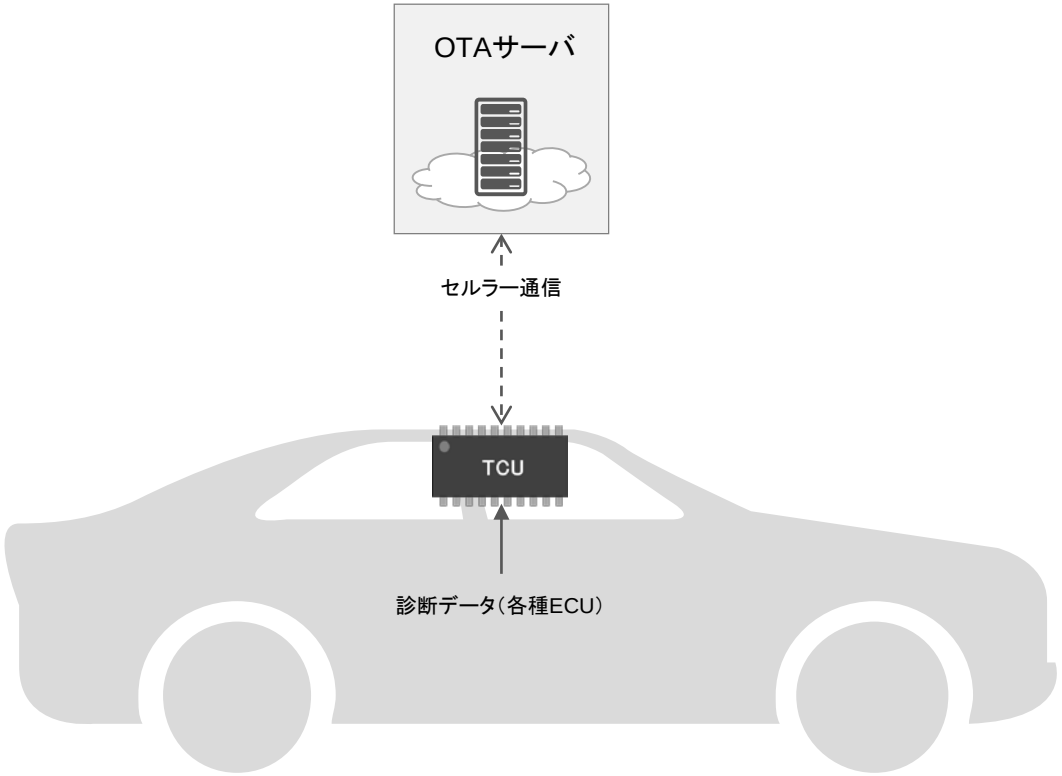
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成



# 6-1. 自動衝突通知

## 1. 機能概要

事項発生時などの車両衝突後時に、自動でセンターへの衝突通知発信を実施する機能。日本ではHELPNET、欧州ではeCallと呼ばれるサービスが利用可能。

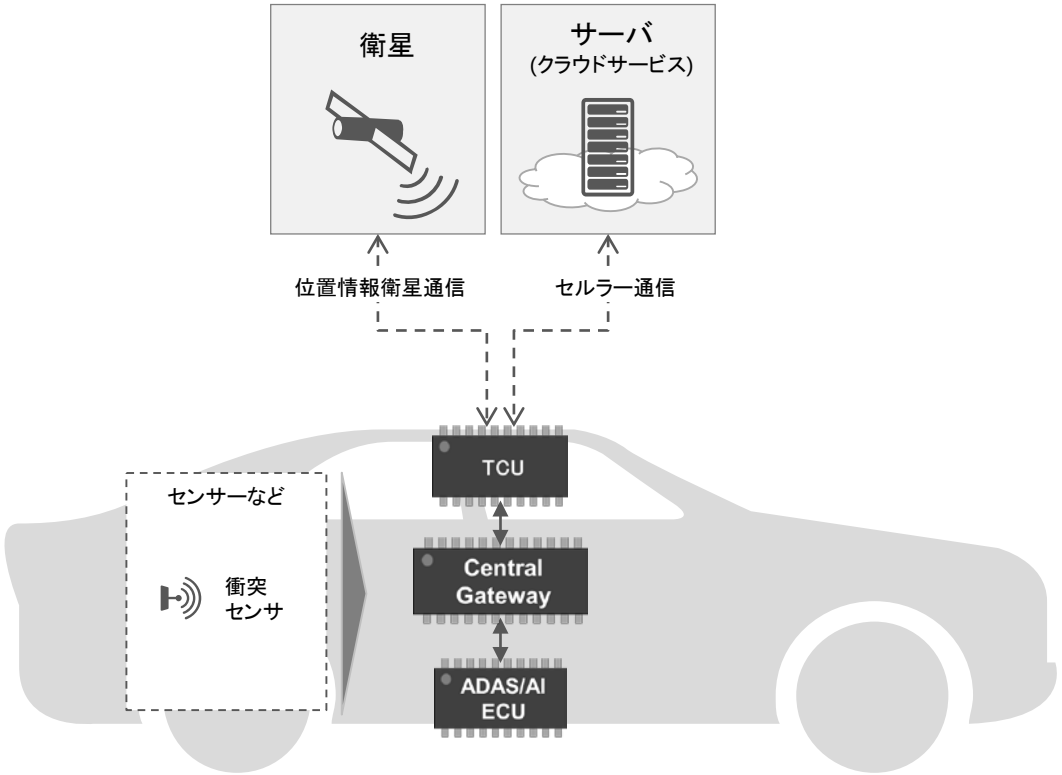
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

| 対象外 |
|---|

## 4. 想定システム構成



# 6-2. 車両故障時の電話サポート

## 1. 機能概要

乗員の体調不良発生や車両の故障時にボタン押下することでセンターへの通知を行い、通話により、発生しているトラブルへの対応を支援する機能。日本ではHELPNET、欧州ではeCallと呼ばれるサービスが利用可能。

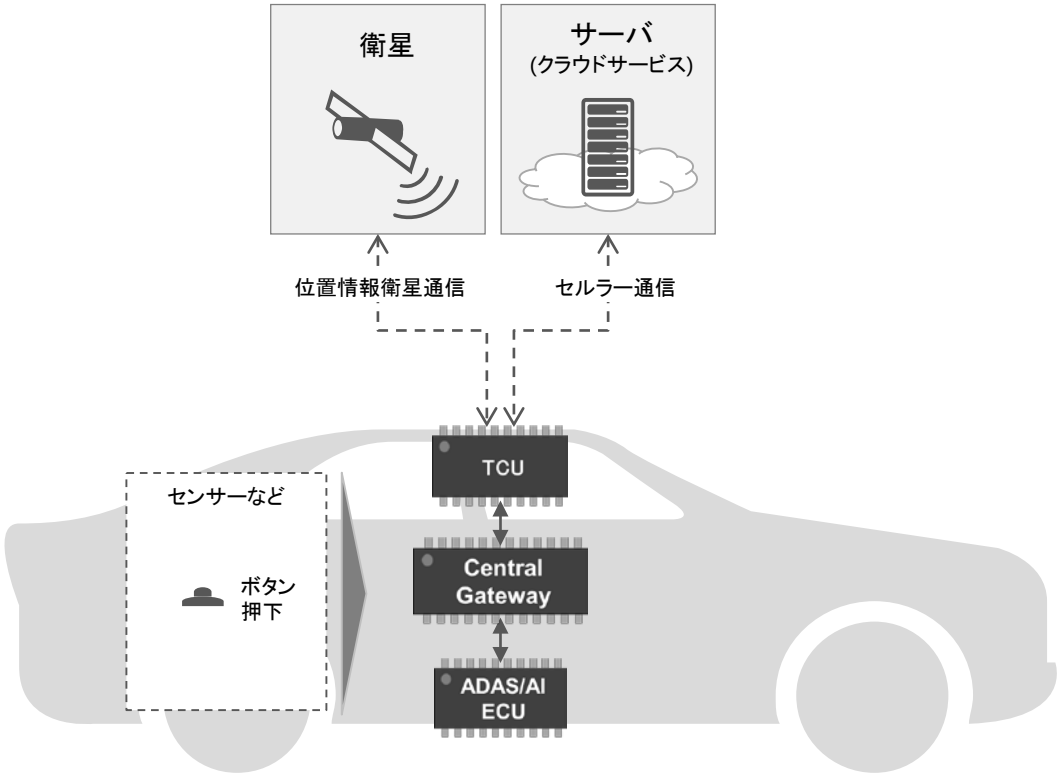
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

| 対象外 |
|---|

## 4. 想定システム構成



# 7-1. ドア・トランク・ハザードランプなどの状態監視

## 1. 機能概要

スマートデバイスなどにより以下の状態を遠隔監視する機能。

- ドア
- トランク
- ハザードランプ
- ウィンドウなど

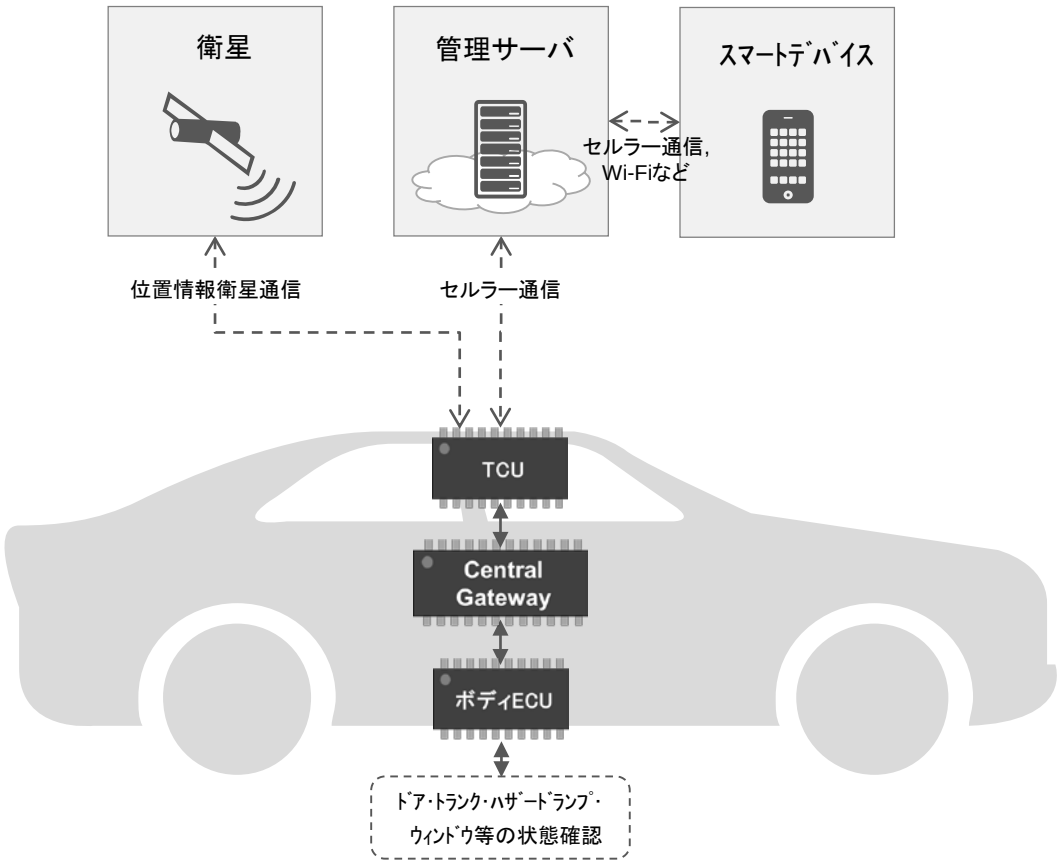
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

| 対象外 |
|---|

## 4. 想定システム構成



# 7-2. 車両異常検知/通報

## 1. 機能概要

車両ドアのこじ開けなどの異常を検知した際に、メール等により所有者へ通知する機能。

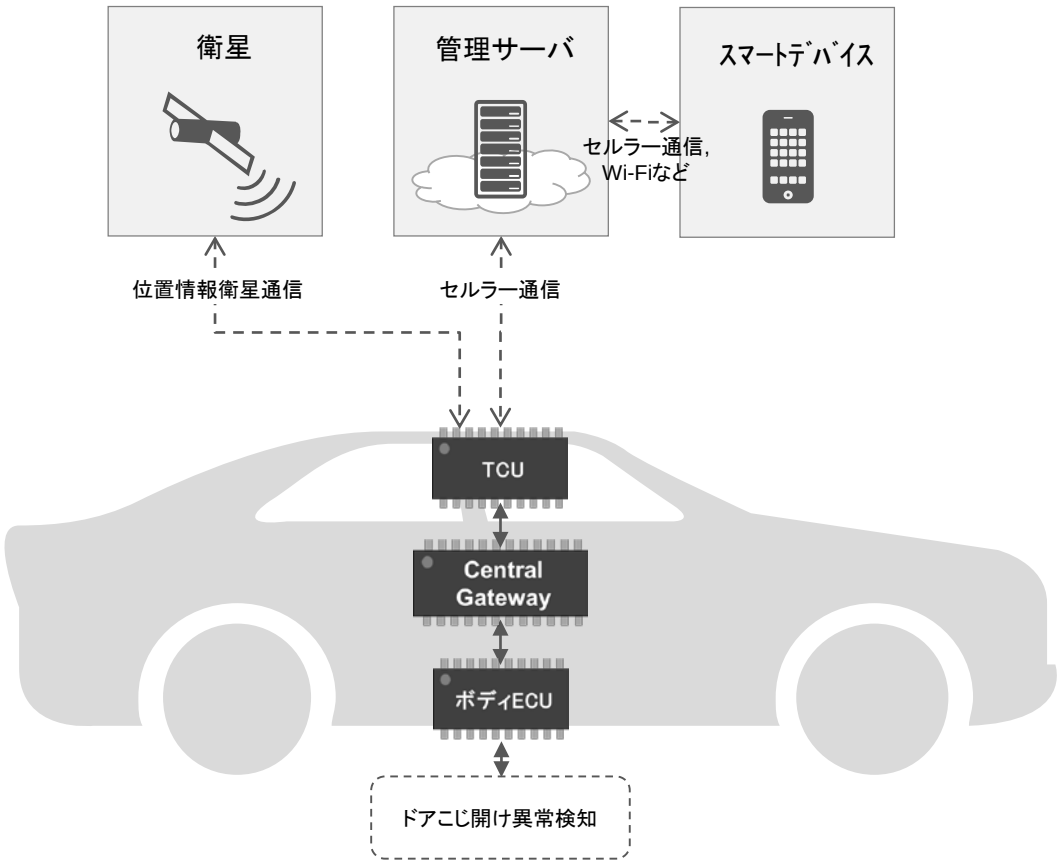
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成



# 7-3. 車両位置追跡

## 1. 機能概要

車両の位置情報を取得し現在地の把握・追跡を可能とする機能。

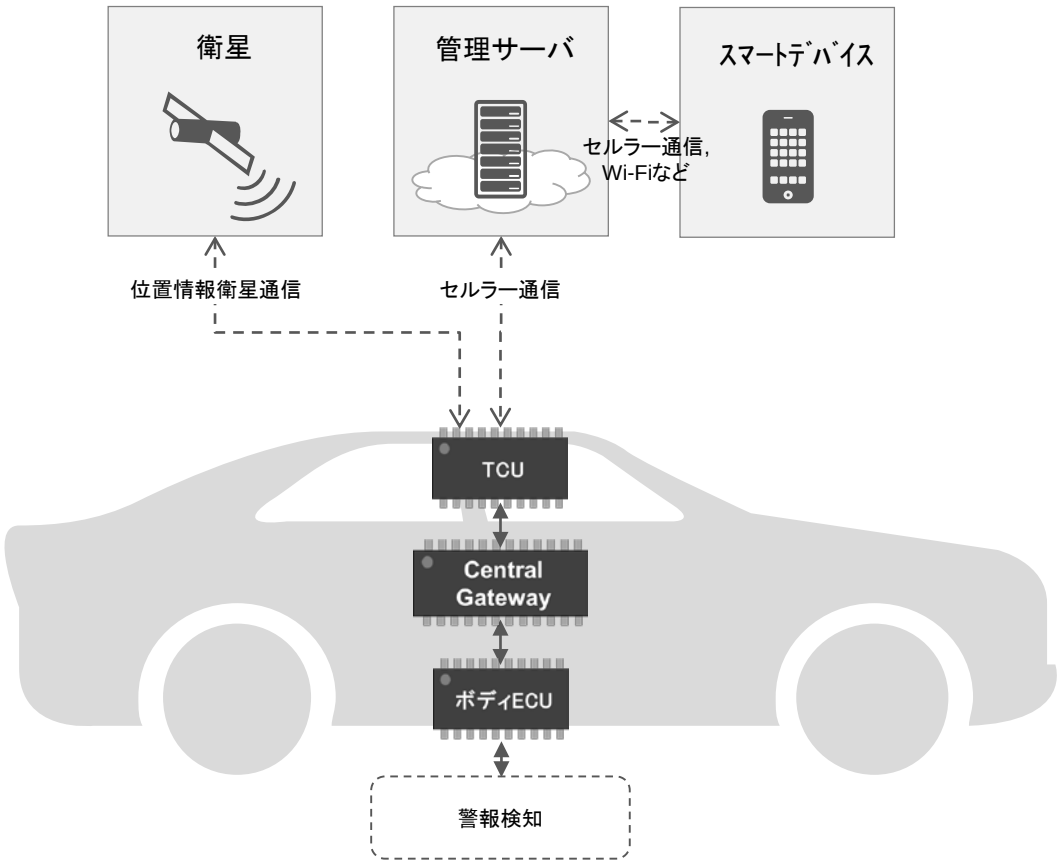
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成



# 7-3. 車両位置追跡(デバイス接続型)

## 1. 機能概要

OBDIIコネクタに接続したデバイス経由で車両の位置情報を取得し現在地の把握・追跡を可能とする機能。

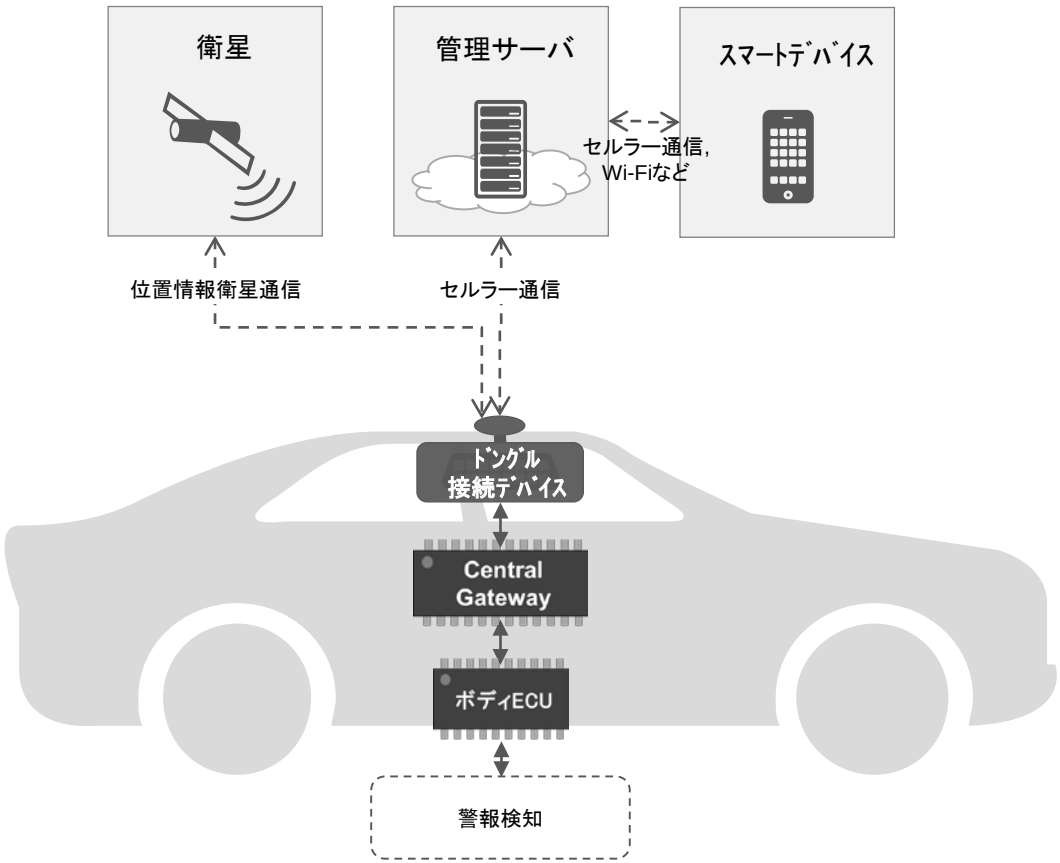
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

| 対象外 |
|---|

## 4. 想定システム構成



# 8-1. 遠隔からのドアロック・アンロック

## 1. 機能概要

スマートデバイスなどと連携し、遠隔地より車両のドアのロック・アンロックを制御する機能。

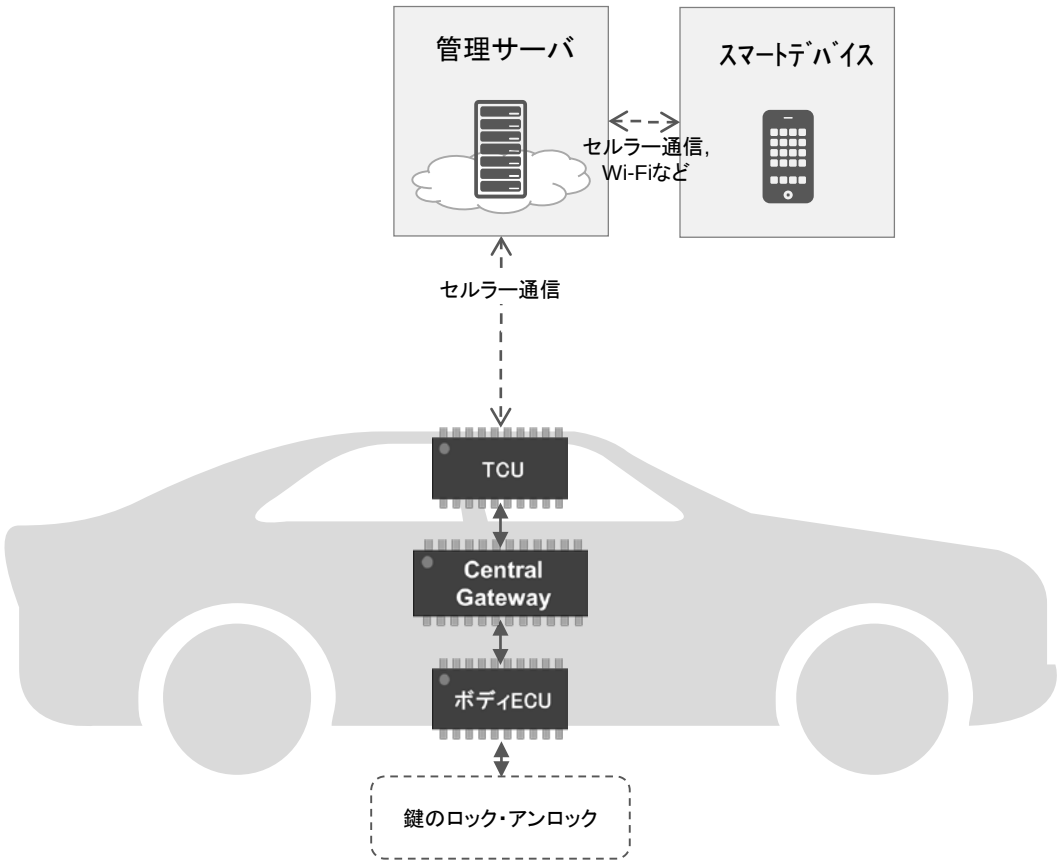
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成



# 8-2. インテリジェントキー

## 1. 機能概要

イモビライザキーを活用し、車両の付近から遠隔でドアの鍵のロック・アンロックを制御する機能。
キーを身につけている状態であれば、ドアに付いた、リクエストスイッチ等を押すことで、ドアやトランクロックの開閉も可能な場合もある。
また、鍵穴にキーを差し込むことなくエンジンの始動が可能な場合もある。

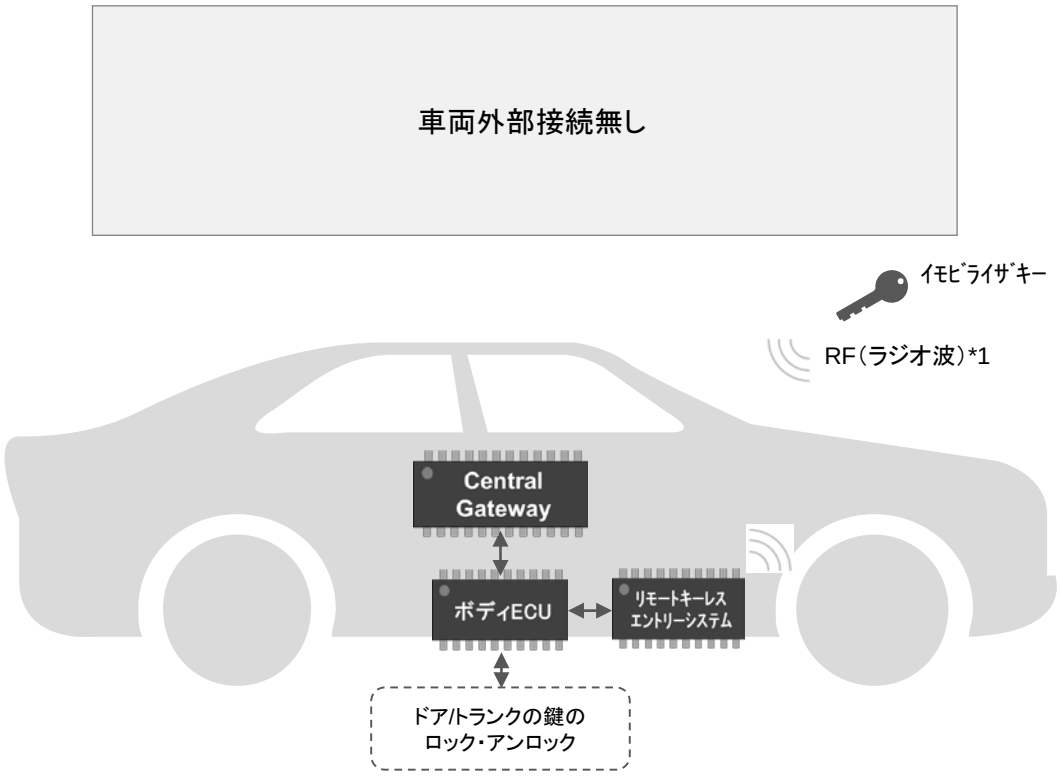
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成




*1: 車両の周辺の限られたエリアからの遠隔操作

# 8-3. 充電制御

## 1. 機能概要

スマートデバイスと連携し、遠隔地より充電状況の管理（充電率の把握、車両への電力給電の停止等）を制御する機能。

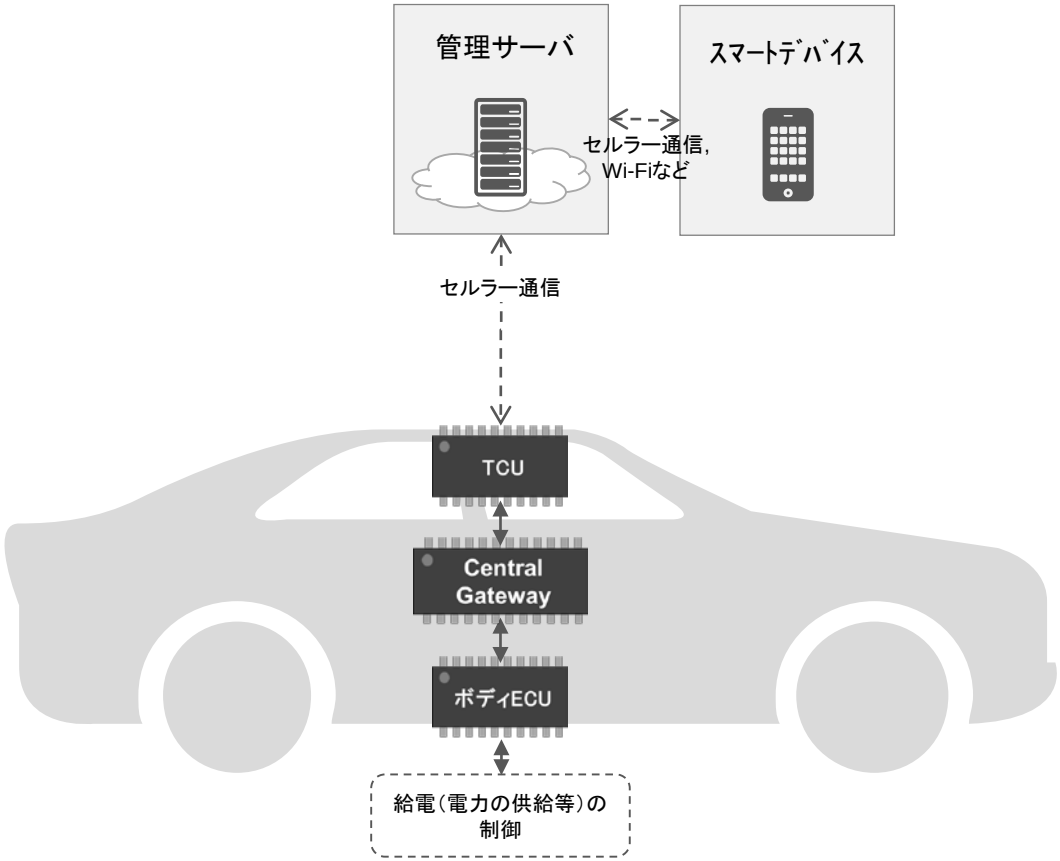
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成



# 8-4. 充電制御(音声認識AI連携)

## 1. 機能概要

ITベンダーの提供する音声認識AIエージェントと連携し、遠隔地より充電状況の管理(充電率の把握、車両への電力給電の停止等)を制御する機能。

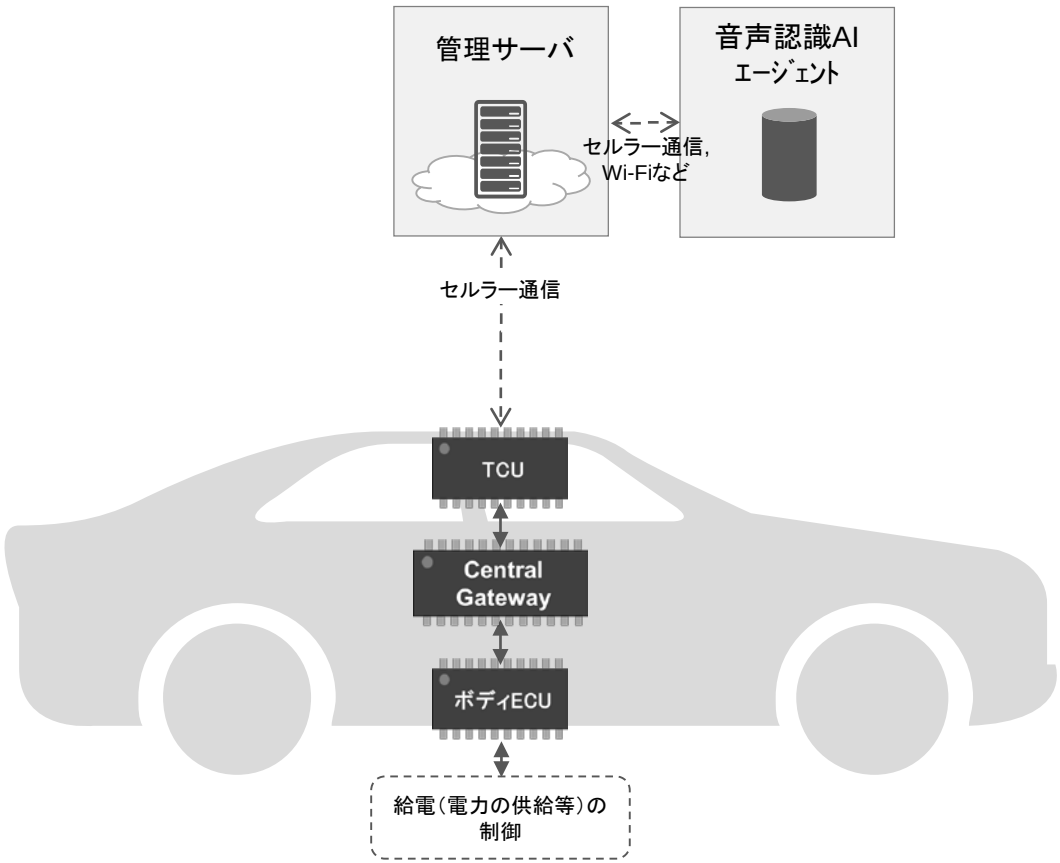
## 2. 実装状況

| 実装済み*1 | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成




*1: 米国・日本の一部の自動車メーカの一部のモデルにおいて実装済み

# 8-5. エアコン制御

## 1. 機能概要

スマートデバイスと連携し、遠隔地よりエアコンのオン・オフ、温度設定等を制御する機能。

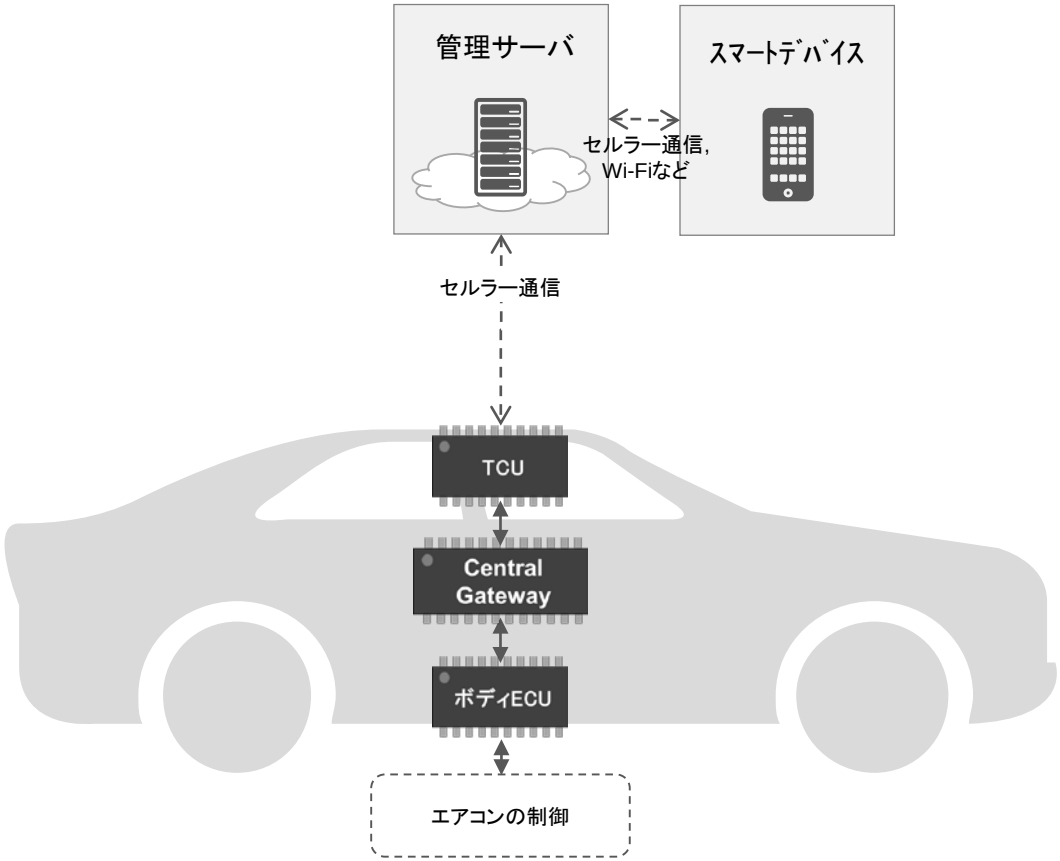
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成




*1: 脚注を入力

# 8-6. エアコン制御（音声認識AI連携）

## 1. 機能概要

ITベンダーの提供する音声認識AIエージェントと連携し、遠隔地よりエアコンのオン・オフ、温度設定等を制御する機能。

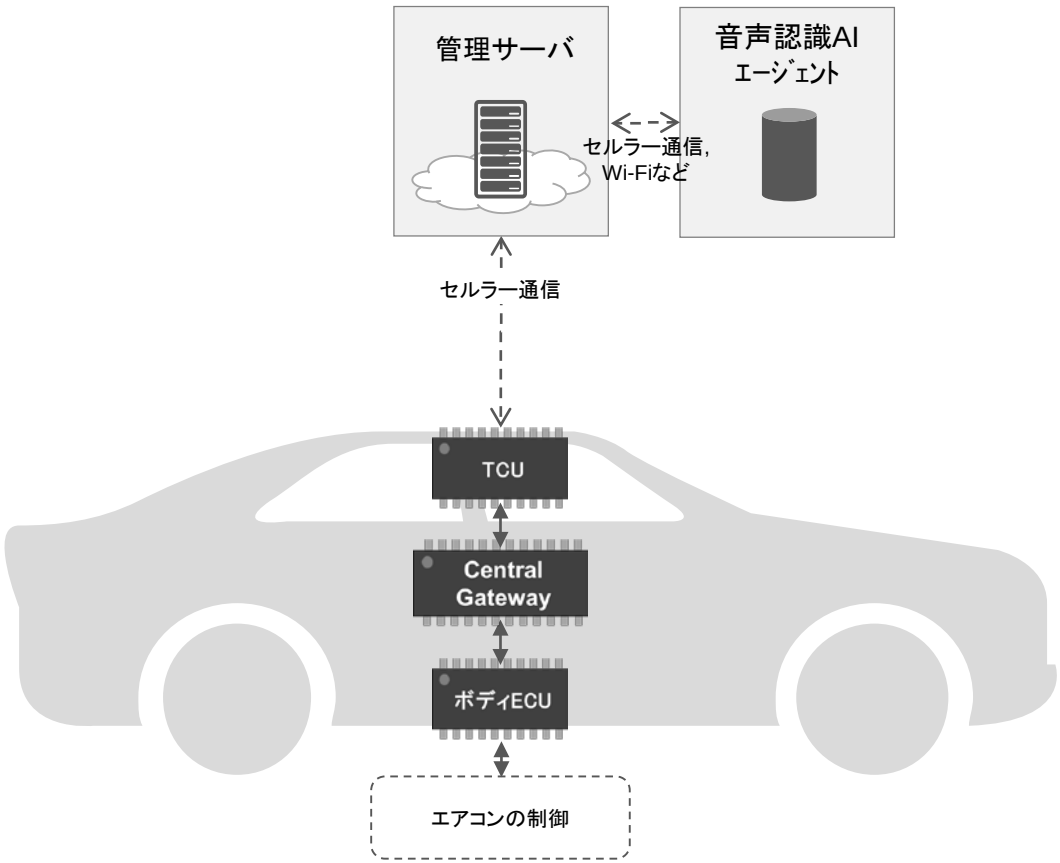
## 2. 実装状況

| 実装済み*1 | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

| 対象外 |
|---|

## 4. 想定システム構成




*1: 米国・日本の一部の自動車メーカの一部のモデルにおいて実装済み

# 8-7. エンジン再駆動・ステアリングロック解除禁止

## 1. 機能概要

車両の盗難被害等の発生の際に、オーナーの要請に基づき、エンジンの再始動・ステアリングロックの解除の禁止を実施する機能。

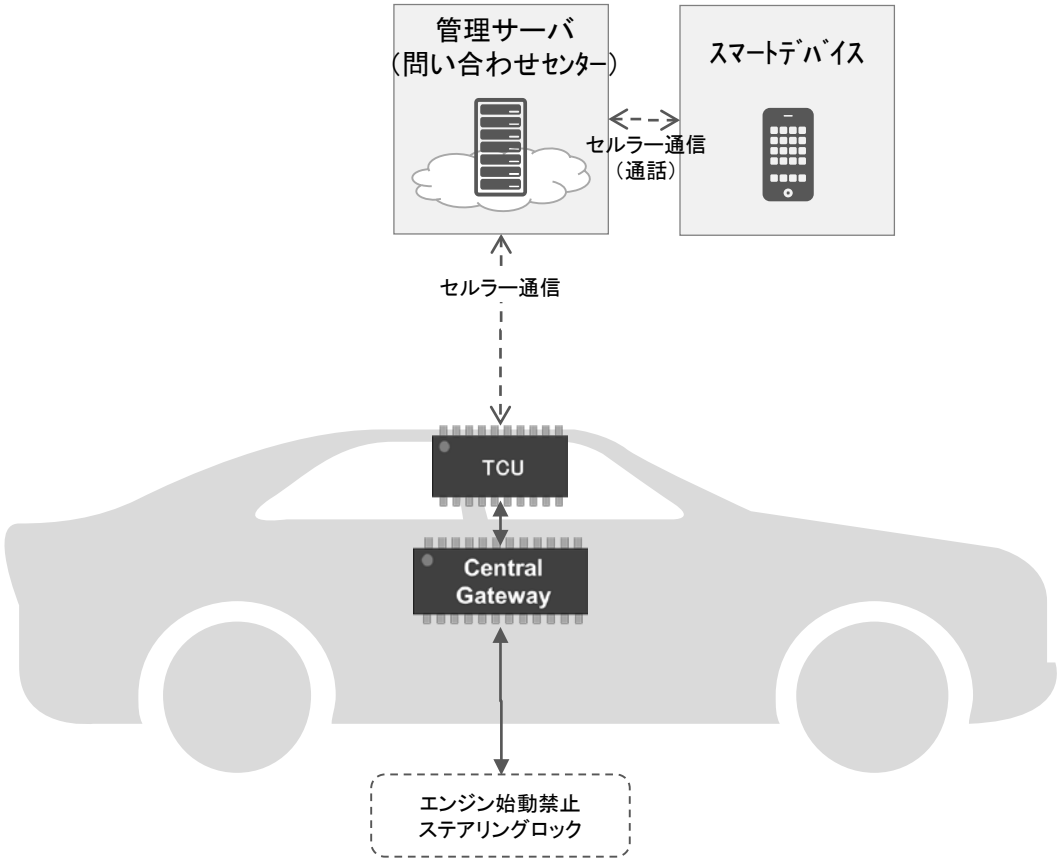
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成



# 9-1. カーシェアリング

## 1. 機能概要

スマートデバイス等を活用し、シェアリング用途の自動車の配車を可能とする機能。

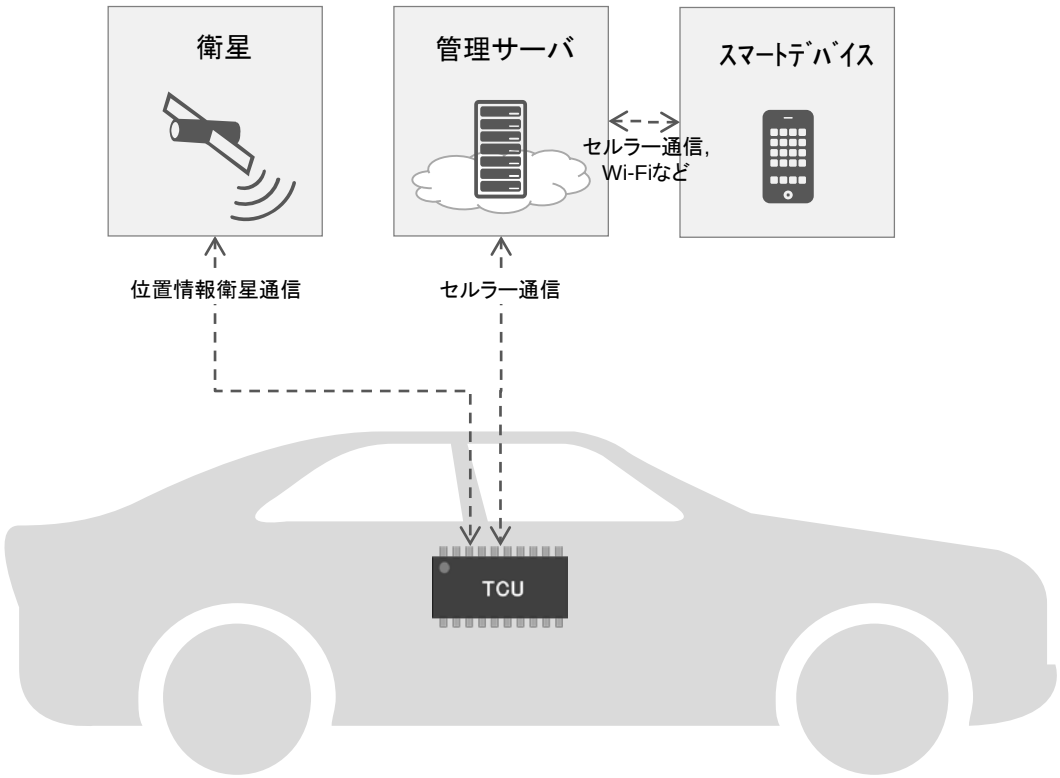
## 2. 実装状況

| 実装済み*1 | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成




*1: 普及率は低いものの、欧米のサービス提供企業が自動車関連企業と共同でサービスを提供

# 10-1. 料金支払い

## 1. 機能概要

車両利用中に発生する様々な料金の支払い（高速道路・駐車場・ガソリンスタンドなど）を支援する機能。日本国内では普及が進められているETC2.0等で料金の支払いが可能でありされており、車両との通信としてはDSRCが用いられている。

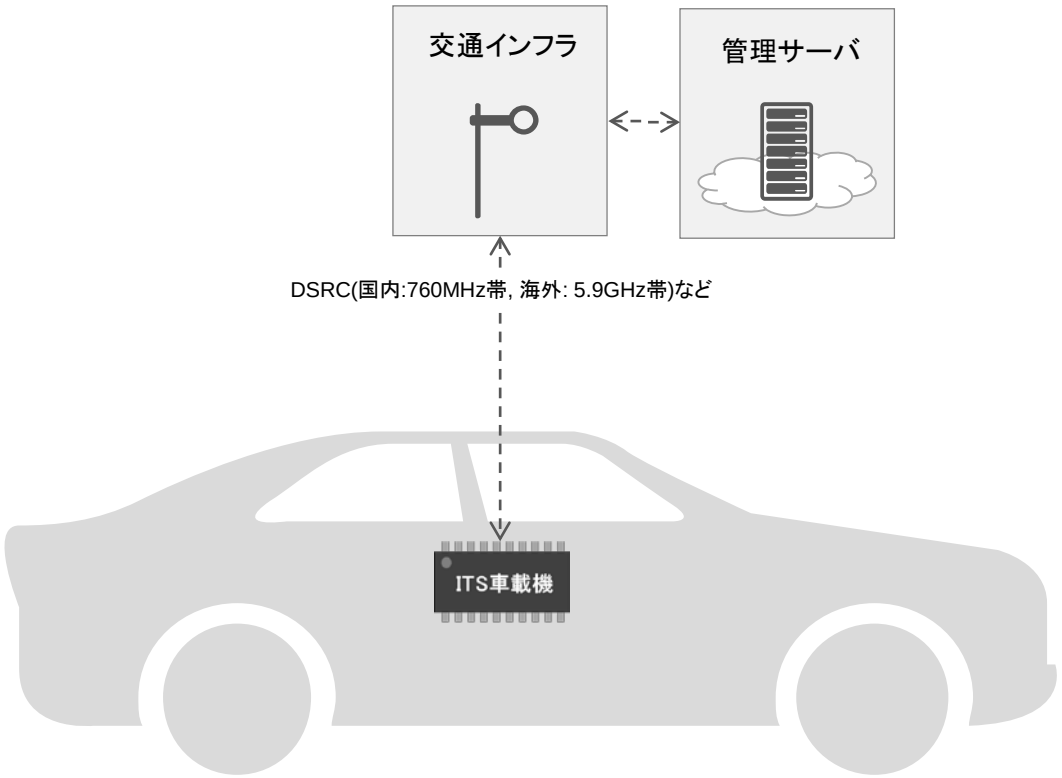
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

| 対象外 |
|---|

## 4. 想定システム構成



# 11-1. ルート検索(組込み型)

## 1. 機能概要

目的地までのルート検索(最速のルート、立ち寄り場所を考慮した目的地までのルート等の検索)を支援する機能。

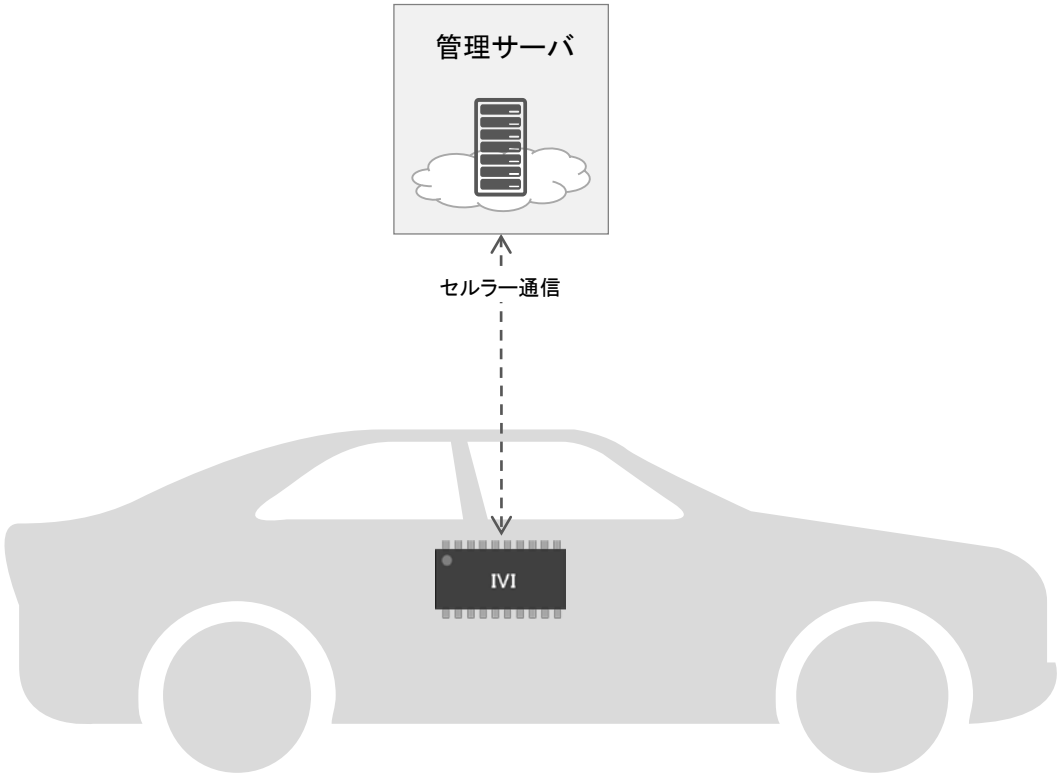
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成



# 11-1. ルート検索（スマホ連携型）

## 1. 機能概要

目的地までのルート検索（最速のルート、立ち寄り場所を考慮した目的地までのルート等の検索）を支援する機能。Android AutoやApple CarPlay等のオペレーティングシステムと連携した機能。

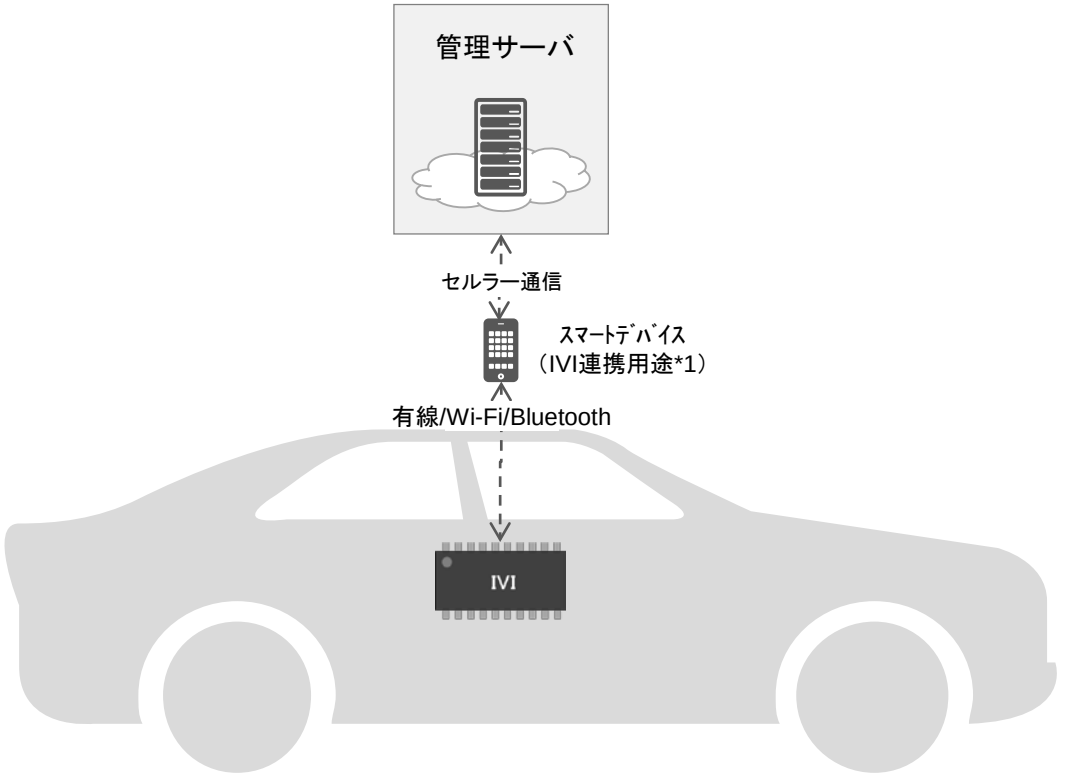
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成




*1: 図に示したスマートデバイスは、乗員が車載のIVIシステムに接続し、ナビゲーションやエンタテイメント機器として利用するスマートデバイスのことを指す

# 11-2. オペレータサービス(組込み型)

## 1. 機能概要

オペレーターのガイドにより、目的地や周辺のスポットの検索などの各種ナビゲーションを支援する機能。

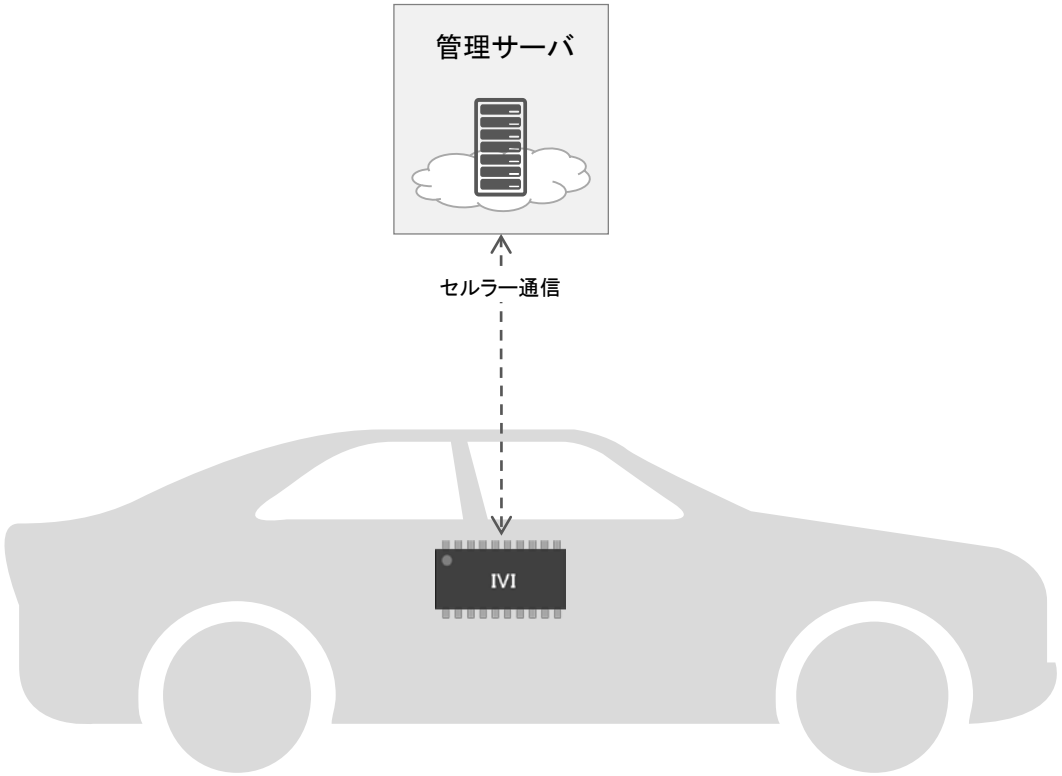
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

| 対象外 |
|---|

## 4. 想定システム構成



# 12-1. カレンダー・メール同期(組込み型)

## 1. 機能概要

パソコンやスマートデバイスで利用するカレンダーやメールなどの情報を車載側のシステムに同期することで、車に居ながらスケジュールなどの情報を確認することができる機能。

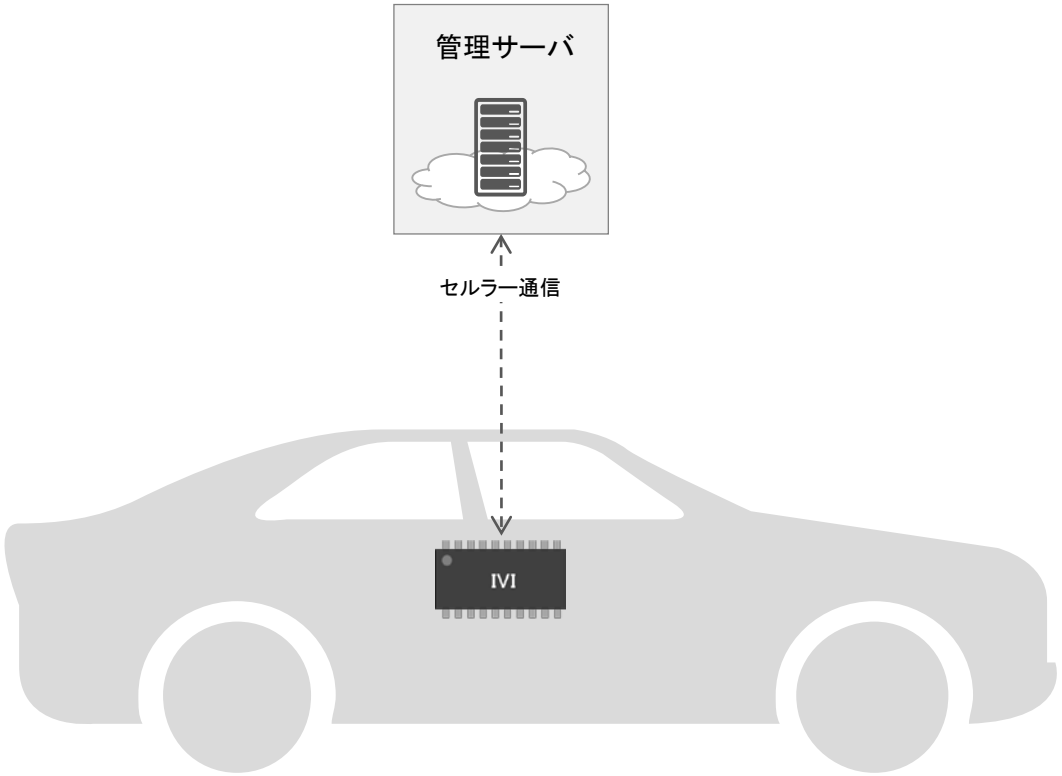
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成



# 12-1. カレンダー・メール同期（スマホ連携型）

## 1. 機能概要

パソコンやスマートデバイスで利用するカレンダーやメールなどの情報を車載側のシステムに同期することで、車に居ながらスケジュールなどの情報を確認することができる機能。Android AutoやApple CarPlay等のオペレーティングシステムと連携した機能。

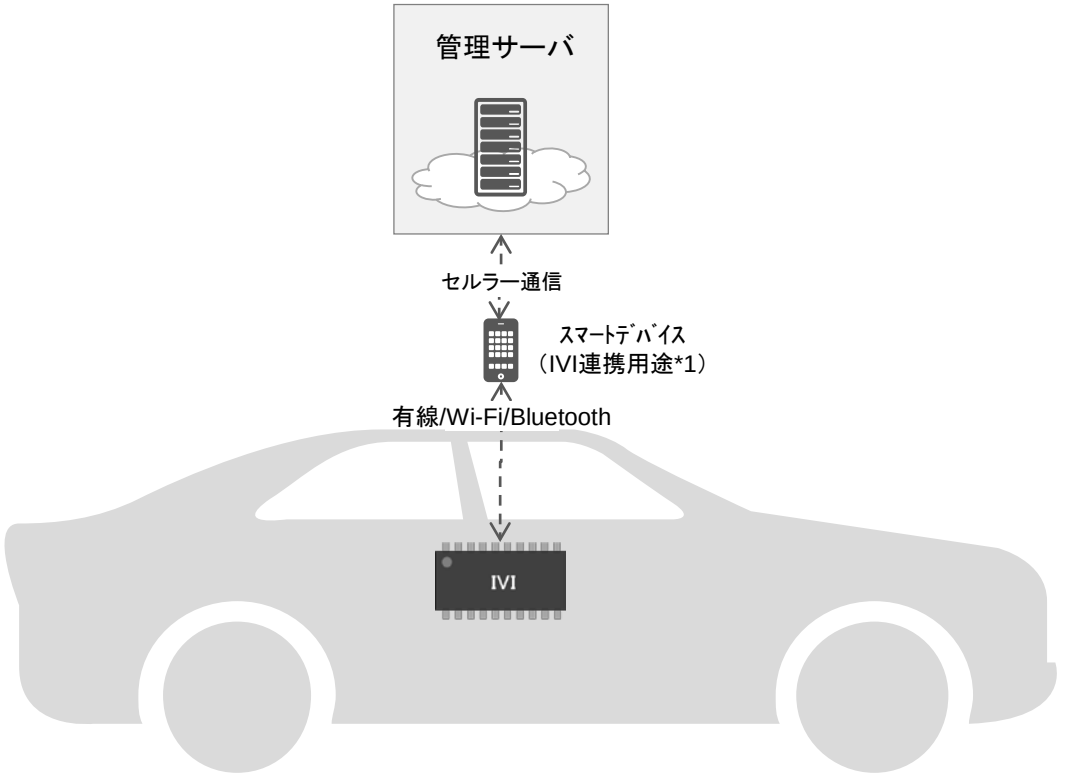
## 2. 実装状況

| 実装済み*1 | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成




*1: 図に示したスマートデバイスは、乗員が車載のIVIシステムに接続し、ナビゲーションやエンタテイメント機器として利用するスマートデバイスのことを指す

# 12-2. SNS連携(組込み型)

## 1. 機能概要

パソコンやスマートデバイスで利用するSNSの情報を車載側のシステムに同期することで、車に居ながらこれを確認することができる機能。

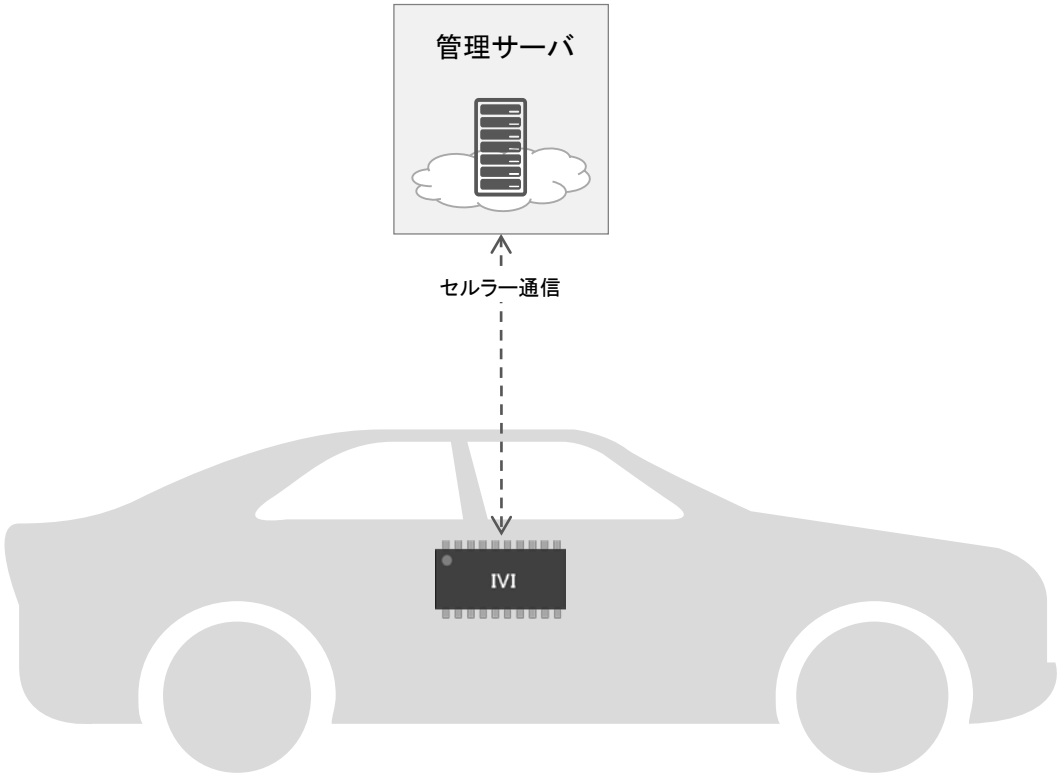
## 2. 実装状況

実装済み | 開発中

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成



# 12-2. SNS連携（スマホ連携型）

## 1. 機能概要

パソコンやスマートデバイスで利用するSNSの情報を車載側のシステムに同期することで、車に居ながらこれを確認することができる機能。Android AutoやApple CarPlay等のオペレーティングシステムと連携した機能。

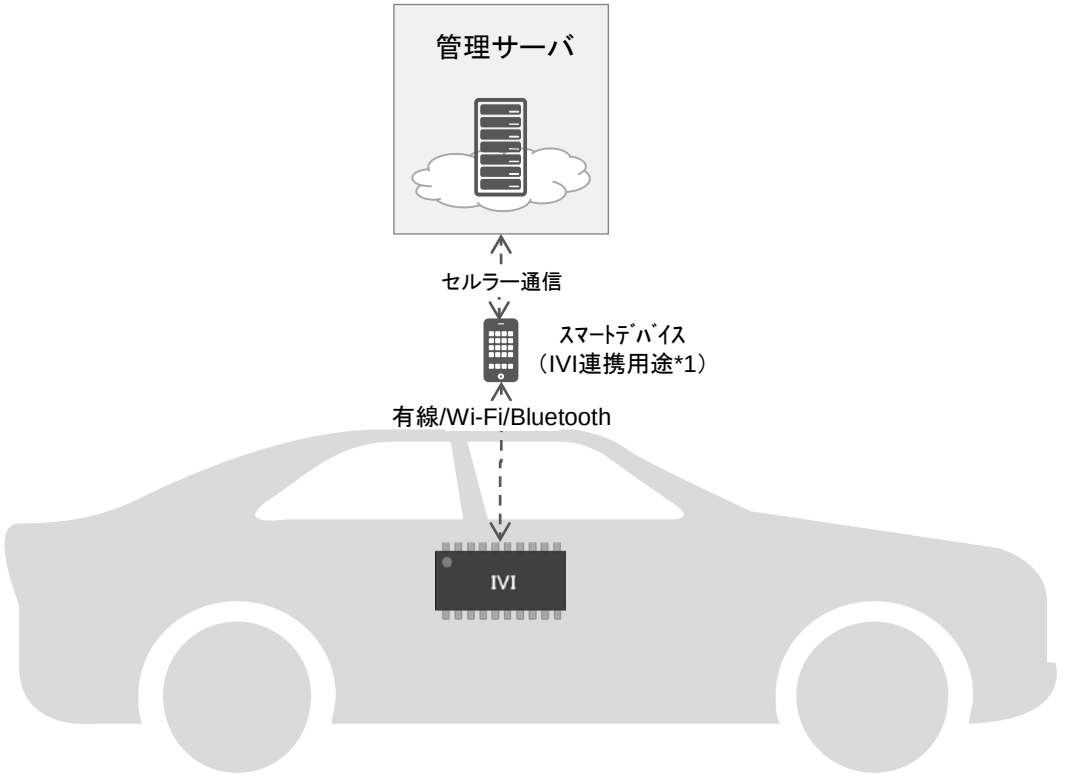
## 2. 実装状況

| 実装済み*1 | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成




*1: 図に示したスマートデバイスは、乗員が車載のIVIシステムに接続し、ナビゲーションやエンタテイメント機器として利用するスマートデバイスのことを指す

# 12-3. Wi-Fiスポット(組込み型)

## 1. 機能概要

車両に搭載されたIVI等のシステムをWi-Fiスポットとして利用する機能。これにより、車両の乗員が利用するスマートデバイスは、Wi-Fiスポットを介して、インターネットやクラウドサービスにアクセスすることが可能となる。

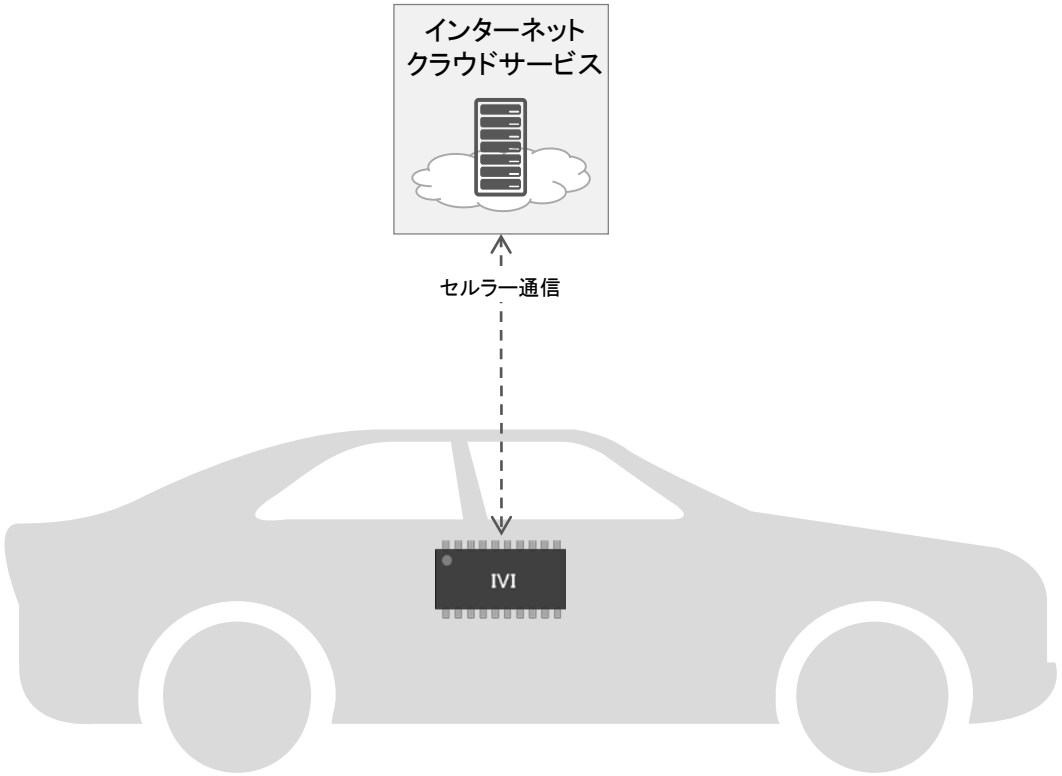
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

| 対象外 |
|---|

## 4. 想定システム構成



# 12-4. 各種アプリケーション利用(組込み型)

## 1. 機能概要

その他、音楽再生、ラジオ、通話など、IVIシステムにインストールされた(もしくは、システムを提供する自動車メーカが提供する)アプリケーション。

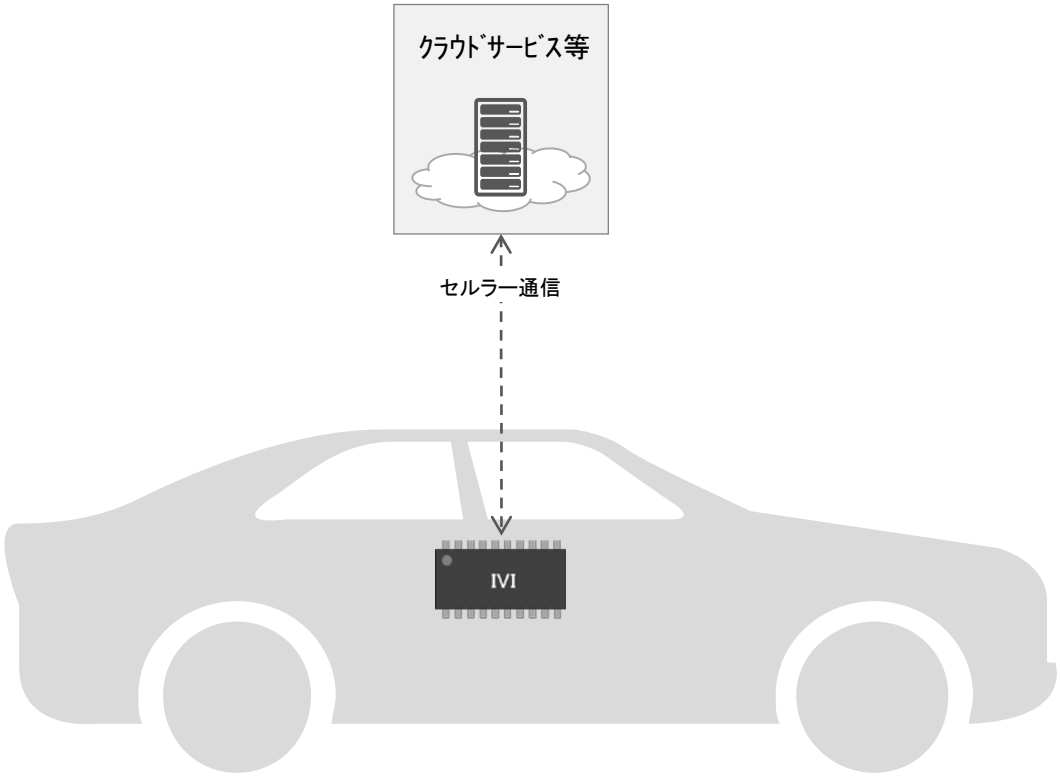
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

対象外

## 4. 想定システム構成




*1: 脚注を入力

# 12-4. 各種アプリケーション利用（スマホ連携型）

## 1. 機能概要

その他、音楽再生、ラジオ、通話など、Android AutoやApple CarPlay等のオペレーティングシステム上にインストールされたアプリケーション。

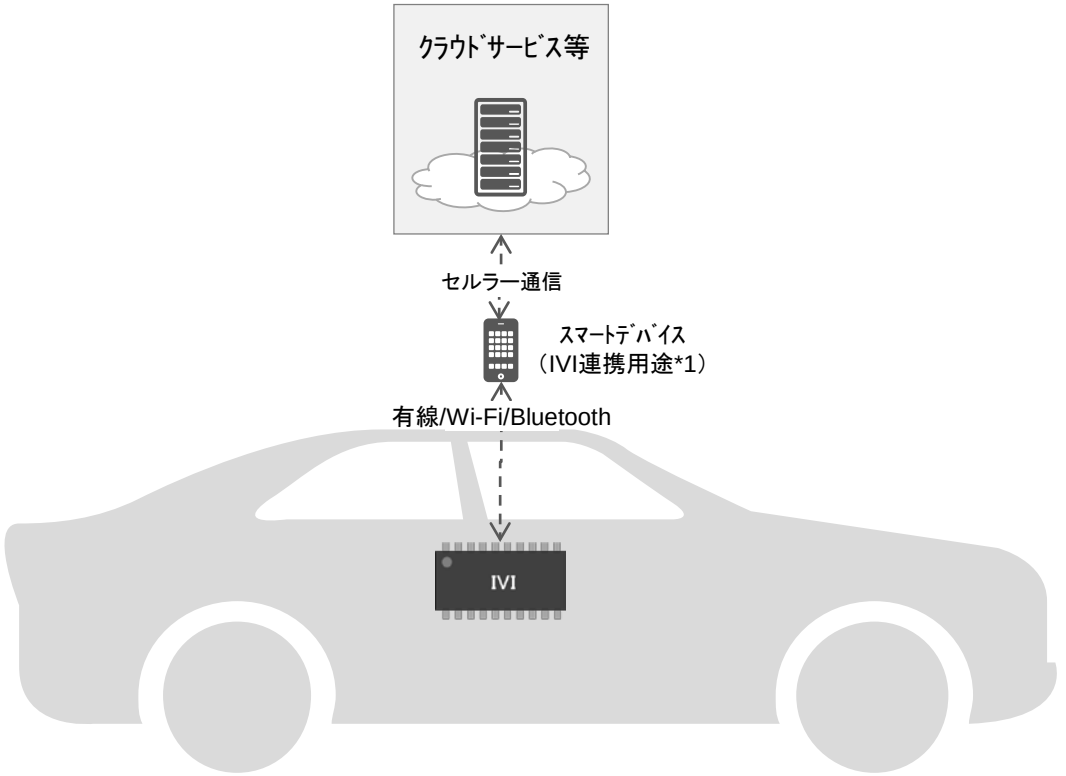
## 2. 実装状況

| 実装済み | 開発中 |
|---|---|

## 3. 自動走行レベル (SAE)

| 対象外 |
|---|

## 4. 想定システム構成



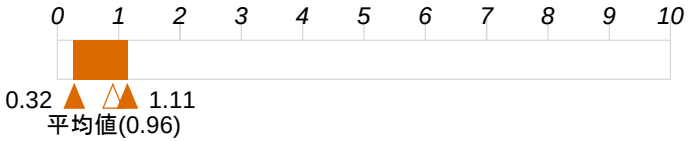

*1: 図に示したスマートデバイスは、乗員が車載のIVIシステムに接続し、ナビゲーションやエンタテイメント機器として利用するスマートデバイスのことを指す

# 別紙2：機能別の影響度評価結果

# 1-1. 車間距離制御

## 1. 評価結果

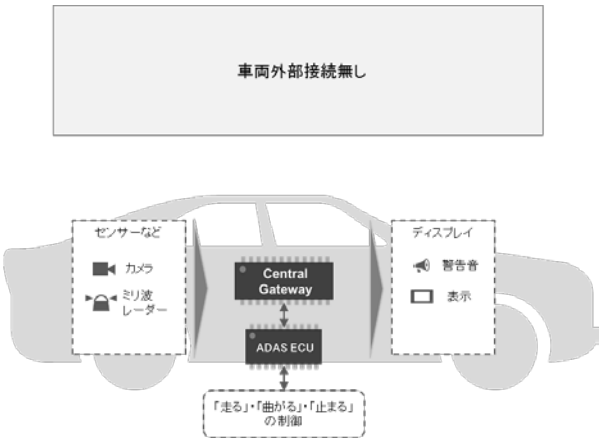
### 1-1. 脅威の重大度（スコア）の分布




### 1-2. 最も重大な脅威

- 通信データの送信元なりすまし
- コマンドインジェクションなど

## 2. 想定システム構成




## 3. 脅威の重大度

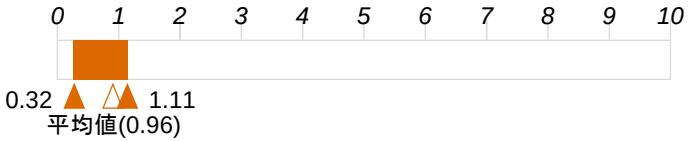
| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| 通信データの送信元なりすまし | 1.39 | 0.80 | 1.11 |
| コマンドインジェクション | 1.39 | 0.80 | 1.11 |
| データ/コードの改ざん | 1.39 | 0.80 | 1.11 |
| データ/コードの上書き | 1.39 | 0.80 | 1.11 |
| データ/コードの削除 | 1.39 | 0.80 | 1.11 |
| データ/コードの追加 | 1.39 | 0.80 | 1.11 |
| 信頼できないソースからのデータ入力 | 1.39 | 0.80 | 1.11 |
| MITM | 0.60 | 0.80 | 0.48 |
| リプレイ攻撃 | 1.39 | 0.80 | 1.11 |
| 通信路の盗聴 | 0.40 | 0.80 | 0.32 |
| 通信路からのデータへの不正アクセス | 0.40 | 0.80 | 0.32 |
| 大量のデータ送信による該当サービス提供の妨害 | 1.39 | 0.80 | 1.11 |
| root権限の奪取 | 1.39 | 0.80 | 1.11 |
| 不正なCANメッセージ送信 | 1.39 | 0.80 | 1.11 |
| 通信データの改ざん（テレマティクス） | 1.39 | 0.80 | 1.11 |

# 1-2. 車線維持制御

## 1. 評価結果

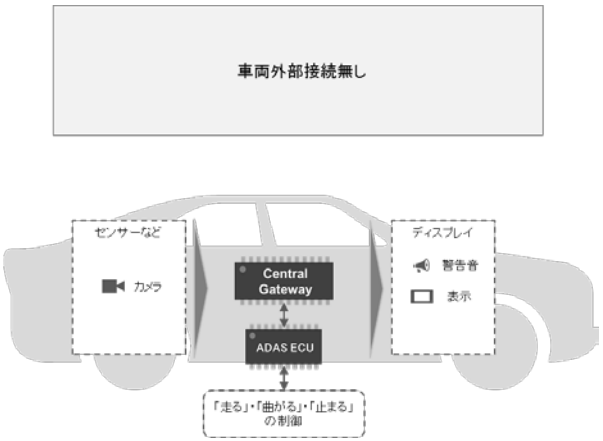
### 1-1. 脅威の重大度（スコア）の分布




### 1-2. 最も重大な脅威

- 通信データの送信元なりすまし
- コマンドインジェクションなど

## 2. 想定システム構成




## 3. 脅威の重大度

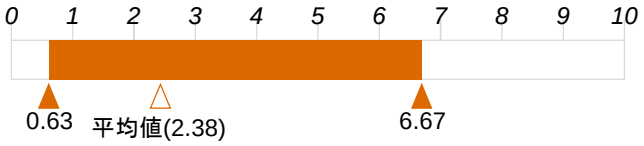
| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| 通信データの送信元なりすまし | 1.39 | 0.80 | 1.11 |
| コマンドインジェクション | 1.39 | 0.80 | 1.11 |
| データ/コードの改ざん | 1.39 | 0.80 | 1.11 |
| データ/コードの上書き | 1.39 | 0.80 | 1.11 |
| データ/コードの削除 | 1.39 | 0.80 | 1.11 |
| データ/コードの追加 | 1.39 | 0.80 | 1.11 |
| 信頼できないソースからのデータ入力 | 1.39 | 0.80 | 1.11 |
| MITM | 0.60 | 0.80 | 0.48 |
| リプレイ攻撃 | 1.39 | 0.80 | 1.11 |
| 通信路の盗聴 | 0.40 | 0.80 | 0.32 |
| 通信路からのデータへの不正アクセス | 0.40 | 0.80 | 0.32 |
| 大量のデータ送信による該当サービス提供の妨害 | 1.39 | 0.80 | 1.11 |
| root権限の奪取 | 1.39 | 0.80 | 1.11 |
| 不正なCANメッセージ送信 | 1.39 | 0.80 | 1.11 |
| 通信データの改ざん（テレマティクス） | 1.39 | 0.80 | 1.11 |

# 1-3. 車間距離制御(V2V型)

## 1. 評価結果

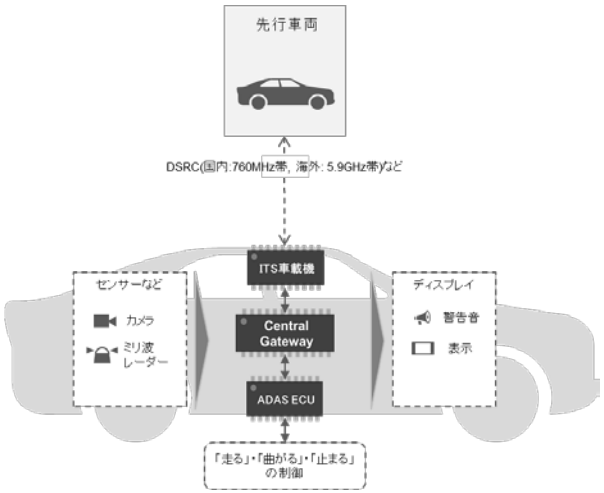
### 1-1. 脅威の重大度(スコア)の分布




### 1-2. 最も重大な脅威

- 大量データ送信による該当サービス提供の妨害
- 信頼できないソースからのデータ入力

## 2. 想定システム構成




## 3. 脅威の重大度

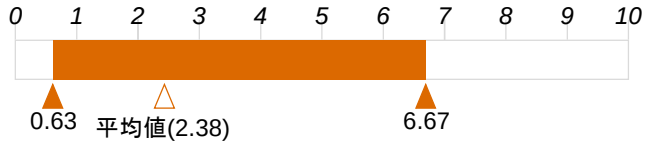
| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ(インパクト) | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| 通信データの送信元なりすまし | 1.39 | 1.59 | 2.22 |
| コマンドインジェクション | 1.39 | 1.59 | 2.22 |
| データ/コードの改ざん | 1.39 | 1.59 | 2.22 |
| データ/コードの上書き | 1.39 | 1.59 | 2.22 |
| データ/コードの削除 | 1.39 | 1.59 | 2.22 |
| データ/コードの追加 | 1.39 | 1.59 | 2.22 |
| 信頼できないソースからのデータ入力 | 2.79 | 1.59 | 4.44 |
| MITM | 0.60 | 1.59 | 0.95 |
| リプレイ攻撃 | 1.39 | 1.59 | 2.22 |
| 通信路の盗聴 | 0.40 | 1.59 | 0.63 |
| 通信路からのデータへの不正アクセス | 0.40 | 1.59 | 0.63 |
| 大量のデータ送信による該当サービス提供の妨害 | 4.18 | 1.59 | 6.67 |
| root権限の奪取 | 1.39 | 1.59 | 2.22 |
| 不正なV2Xメッセージ送信 | 1.39 | 1.59 | 2.22 |

# 1-4. 隊列走行(V2V型)

## 1. 評価結果

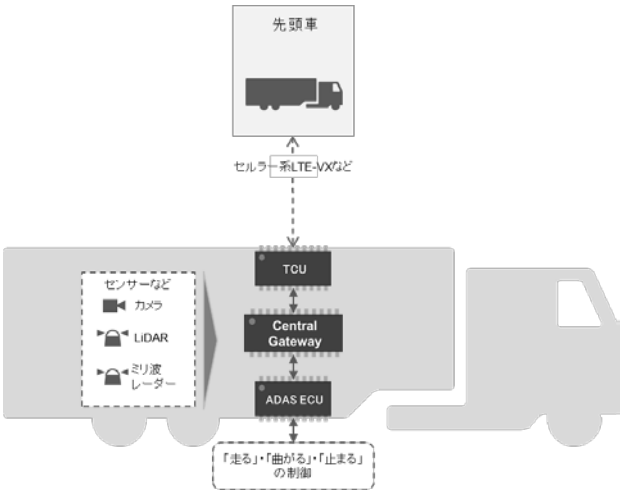
### 1-1. 脅威の重大度(スコア)の分布




### 1-2. 最も重大な脅威

- 大量データ送信による該当サービス提供の妨害
- 信頼できないソースからのデータ入力

## 2. 想定システム構成




## 3. 脅威の重大度

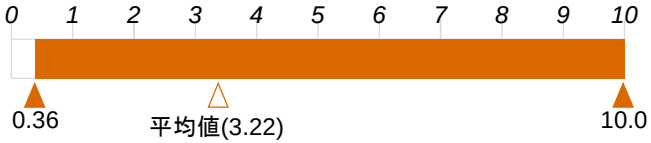
| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ(インパクト) | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| 通信データの送信元なりすまし | 1.39 | 1.59 | 2.22 |
| コマンドインジェクション | 1.39 | 1.59 | 2.22 |
| データ/コードの改ざん | 1.39 | 1.59 | 2.22 |
| データ/コードの上書き | 1.39 | 1.59 | 2.22 |
| データ/コードの削除 | 1.39 | 1.59 | 2.22 |
| データ/コードの追加 | 1.39 | 1.59 | 2.22 |
| 信頼できないソースからのデータ入力 | 2.79 | 1.59 | 4.44 |
| MITM | 0.60 | 1.59 | 0.95 |
| リプレイ攻撃 | 1.39 | 1.59 | 2.22 |
| 通信路の盗聴 | 0.40 | 1.59 | 0.63 |
| 通信路からのデータへの不正アクセス | 0.40 | 1.59 | 0.63 |
| 大量のデータ送信による該当サービス提供の妨害 | 4.18 | 1.59 | 6.67 |
| root権限の奪取 | 1.39 | 1.59 | 2.22 |
| 不正なV2Xメッセージ送信 | 1.39 | 1.59 | 2.22 |

# 1-5. 自動運転(ITS協調型)

## 1. 評価結果

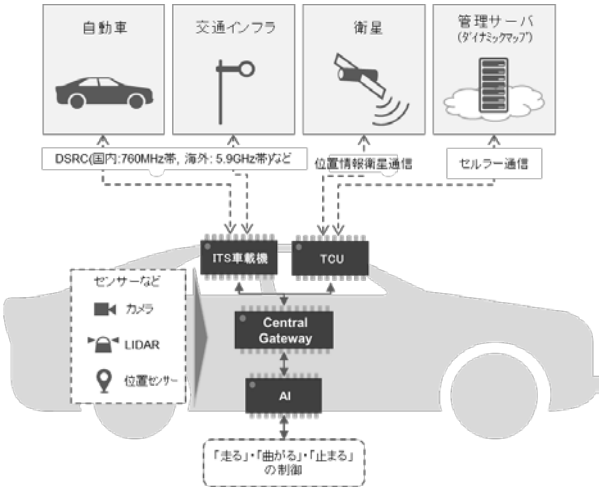
### 1-1. 脅威の重大度(スコア)の分布




### 1-2. 最も重大な脅威

- 大量データ送信による該当サービス提供の妨害
- 信頼できないソースからのデータ入力

## 2. 想定システム構成




## 3. 脅威の重大度

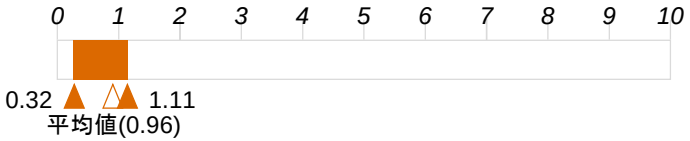
| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ(インパクト) | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 1.79 | 0.60 | 1.07 |
| サーバーへのDoS攻撃 | 0.60 | 0.60 | 0.36 |
| 通信データの送信元なりすまし | 1.39 | 2.39 | 3.33 |
| コマンドインジェクション | 1.39 | 2.39 | 3.33 |
| データ/コードの改ざん | 1.39 | 2.39 | 3.33 |
| データ/コードの上書き | 1.39 | 2.39 | 3.33 |
| データ/コードの削除 | 1.39 | 2.39 | 3.33 |
| データ/コードの追加 | 1.39 | 2.39 | 3.33 |
| 信頼できないソースからのデータ入力 | 2.79 | 2.39 | 6.67 |
| MITM | 0.60 | 2.39 | 1.43 |
| リプレイ攻撃 | 1.39 | 2.39 | 3.33 |
| 通信路の盗聴 | 0.40 | 2.39 | 0.95 |
| 通信路からのデータへの不正アクセス | 0.40 | 2.39 | 0.95 |
| 大量のデータ送信による該当サービス提供の妨害 | 4.18 | 2.39 | 10.00 |
| root権限の奪取 | 1.39 | 2.39 | 3.33 |
| 不正なCANメッセージ送信 | 1.39 | 2.39 | 3.33 |
| 通信データの改ざん(テレマティクス) | 1.39 | 2.39 | 3.33 |

# 1-6. 自動運転(自律型)

## 1. 評価結果

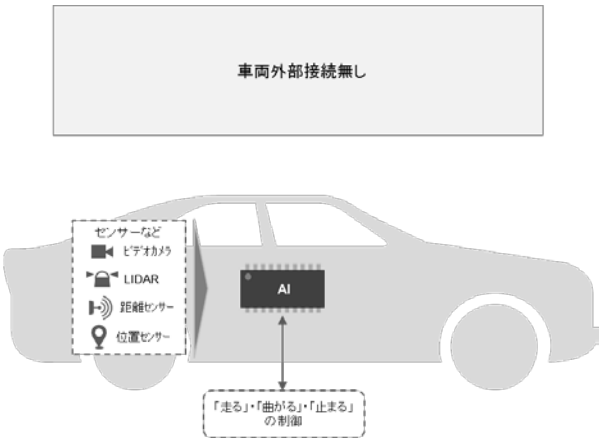
### 1-1. 脅威の重大度(スコア)の分布




### 1-2. 最も重大な脅威

- 通信データの送信元なりすまし
- コマンドインジェクションなど

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ(インパクト) | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| 通信データの送信元なりすまし | 1.39 | 0.80 | 1.11 |
| コマンドインジェクション | 1.39 | 0.80 | 1.11 |
| データ/コードの改ざん | 1.39 | 0.80 | 1.11 |
| データ/コードの上書き | 1.39 | 0.80 | 1.11 |
| データ/コードの削除 | 1.39 | 0.80 | 1.11 |
| データ/コードの追加 | 1.39 | 0.80 | 1.11 |
| 信頼できないソースからのデータ入力 | 1.39 | 0.80 | 1.11 |
| MITM | 0.60 | 0.80 | 0.48 |
| リプレイ攻撃 | 1.39 | 0.80 | 1.11 |
| 通信路の盗聴 | 0.40 | 0.80 | 0.32 |
| 通信路からのデータへの不正アクセス | 0.40 | 0.80 | 0.32 |
| 大量のデータ送信による該当サービス提供の妨害 | 1.39 | 0.80 | 1.11 |
| root権限の奪取 | 1.39 | 0.80 | 1.11 |
| 不正なCANメッセージ送信 | 1.39 | 0.80 | 1.11 |
| 通信データの改ざん(テレマティクス) | 1.39 | 0.80 | 1.11 |

# 1-7. 駐車周辺映像表示

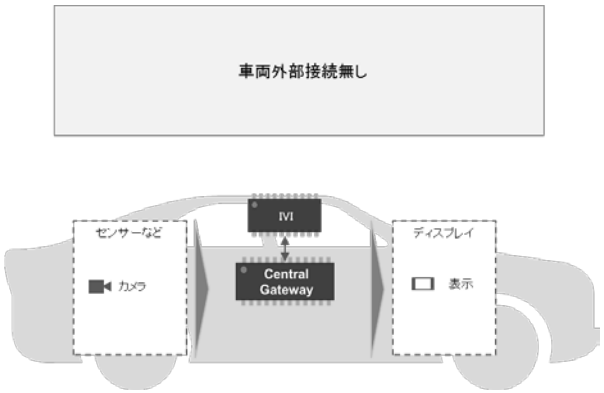
## 1. 評価結果

### 1-1. 脅威の重大度（スコア）の分布


### 1-2. 最も重大な脅威

- コマンドインジェクション
- データ/コードの改ざんなど

## 2. 想定システム構成




## 3. 脅威の重大度

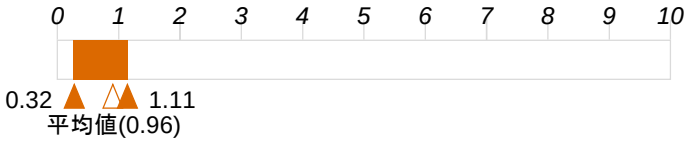
| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| 通信データの送信元なりすまし | 0.20 | 0.20 | 0.04 |
| コマンドインジェクション | 0.80 | 0.20 | 0.16 |
| データ/コードの改ざん | 0.80 | 0.20 | 0.16 |
| データ/コードの上書き | 0.80 | 0.20 | 0.16 |
| データ/コードの削除 | 0.80 | 0.20 | 0.16 |
| データ/コードの追加 | 0.80 | 0.20 | 0.16 |
| 信頼できないソースからのデータ入力 | 0.80 | 0.20 | 0.16 |
| MITM | 0.60 | 0.20 | 0.12 |
| リプレイ攻撃 | 0.80 | 0.20 | 0.16 |
| 通信路の盗聴 | 0.40 | 0.20 | 0.08 |
| 通信路からのデータへの不正アクセス | 0.40 | 0.20 | 0.08 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.20 | 0.20 | 0.04 |
| root権限の奪取 | 0.80 | 0.20 | 0.16 |
| 不正なCANメッセージ送信 | 0.20 | 0.20 | 0.04 |
| 通信データの改ざん（テレマティクス） | 0.80 | 0.20 | 0.16 |

# 1-8. 自動駐車(自律型)

## 1. 評価結果

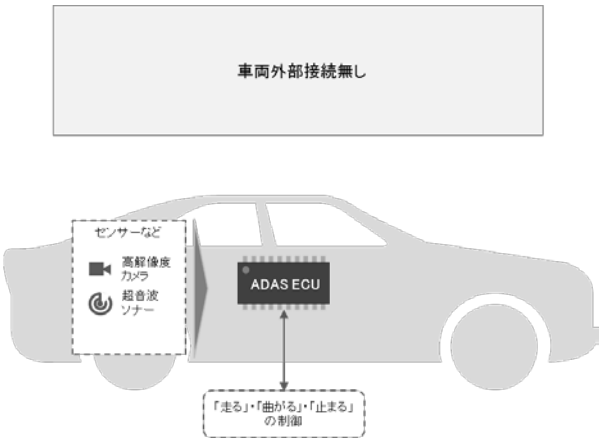
### 1-1. 脅威の重大度(スコア)の分布




### 1-2. 最も重大な脅威

- 通信データの送信元なりすまし
- コマンドインジェクションなど

## 2. 想定システム構成




## 3. 脅威の重大度

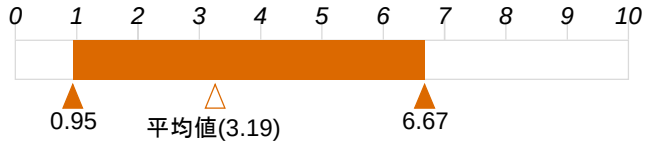
| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ(インパクト) | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| 通信データの送信元なりすまし | 1.39 | 0.80 | 1.11 |
| コマンドインジェクション | 1.39 | 0.80 | 1.11 |
| データ/コードの改ざん | 1.39 | 0.80 | 1.11 |
| データ/コードの上書き | 1.39 | 0.80 | 1.11 |
| データ/コードの削除 | 1.39 | 0.80 | 1.11 |
| データ/コードの追加 | 1.39 | 0.80 | 1.11 |
| 信頼できないソースからのデータ入力 | 1.39 | 0.80 | 1.11 |
| MITM | 0.60 | 0.80 | 0.48 |
| リプレイ攻撃 | 1.39 | 0.80 | 1.11 |
| 通信路の盗聴 | 0.40 | 0.80 | 0.32 |
| 通信路からのデータへの不正アクセス | 0.40 | 0.80 | 0.32 |
| 大量のデータ送信による該当サービス提供の妨害 | 1.39 | 0.80 | 1.11 |
| root権限の奪取 | 1.39 | 0.80 | 1.11 |
| 不正なCANメッセージ送信 | 1.39 | 0.80 | 1.11 |
| 通信データの改ざん(テレマティクス) | 1.39 | 0.80 | 1.11 |

# 1-9. 自動駐車（スマホ連携）

## 1. 評価結果

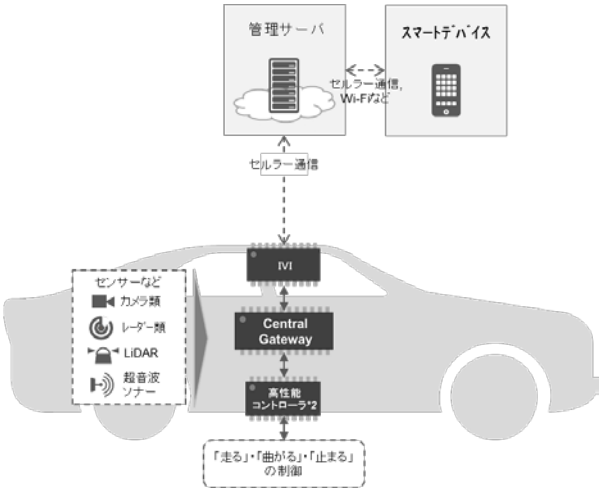
### 1-1. 脅威の重大度（スコア）の分布




### 1-2. 最も重大な脅威

- 信頼できないソースからのデータ入力
- サーバーへの不正侵入による車両への攻撃

## 2. 想定システム構成




## 3. 脅威の重大度

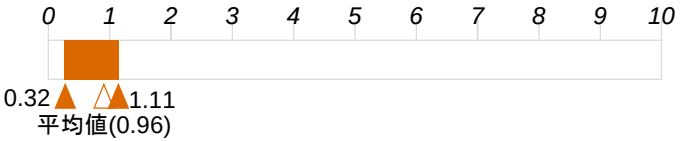
| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 1.79 | 2.39 | 4.29 |
| サーバーへのDoS攻撃 | 1.39 | 2.39 | 3.33 |
| 通信データの送信元なりすまし | 1.39 | 2.39 | 3.33 |
| コマンドインジェクション | 1.39 | 2.39 | 3.33 |
| データ/コードの改ざん | 1.39 | 2.39 | 3.33 |
| データ/コードの上書き | 1.39 | 2.39 | 3.33 |
| データ/コードの削除 | 1.39 | 2.39 | 3.33 |
| データ/コードの追加 | 1.39 | 2.39 | 3.33 |
| 信頼できないソースからのデータ入力 | 2.79 | 2.39 | 6.67 |
| MITM | 0.60 | 2.39 | 1.43 |
| リプレイ攻撃 | 1.39 | 2.39 | 3.33 |
| 通信路の盗聴 | 0.40 | 2.39 | 0.95 |
| 通信路からのデータへの不正アクセス | 0.40 | 2.39 | 0.95 |
| 大量のデータ送信による該当サービス提供の妨害 | 1.39 | 2.39 | 3.33 |
| root権限の奪取 | 1.39 | 2.39 | 3.33 |
| 不正なCANメッセージ送信 | 1.39 | 2.39 | 3.33 |
| 通信データの改ざん（テレマティクス） | 1.39 | 2.39 | 3.33 |

# 2-1. 緊急ブレーキ

## 1. 評価結果

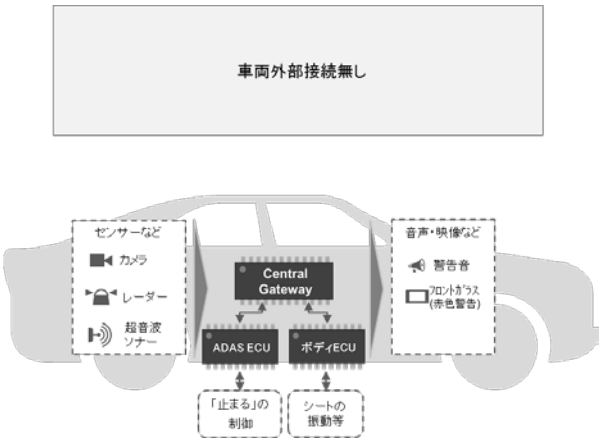
### 1-1. 脅威の重大度（スコア）の分布




### 1-2. 最も重大な脅威

- 通信データの送信元なりすまし
- コマンドインジェクションなど

## 2. 想定システム構成




## 3. 脅威の重大度

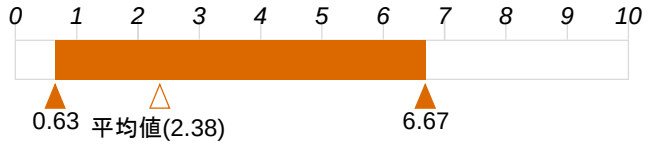
| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| 通信データの送信元なりすまし | 1.39 | 0.80 | 1.11 |
| コマンドインジェクション | 1.39 | 0.80 | 1.11 |
| データ/コードの改ざん | 1.39 | 0.80 | 1.11 |
| データ/コードの上書き | 1.39 | 0.80 | 1.11 |
| データ/コードの削除 | 1.39 | 0.80 | 1.11 |
| データ/コードの追加 | 1.39 | 0.80 | 1.11 |
| 信頼できないソースからのデータ入力 | 1.39 | 0.80 | 1.11 |
| MITM | 0.60 | 0.80 | 0.48 |
| リプレイ攻撃 | 1.39 | 0.80 | 1.11 |
| 通信路の盗聴 | 0.20 | 0.80 | 0.16 |
| 通信路からのデータへの不正アクセス | 0.20 | 0.80 | 0.16 |
| 大量のデータ送信による該当サービス提供の妨害 | 1.39 | 0.80 | 1.11 |
| root権限の奪取 | 1.39 | 0.80 | 1.11 |
| 不正なCANメッセージ送信 | 1.39 | 0.80 | 1.11 |
| 通信データの改ざん（テレマティクス） | 1.39 | 0.80 | 1.11 |

# 2-2. 歩行者検知(V2P型)

## 1. 評価結果

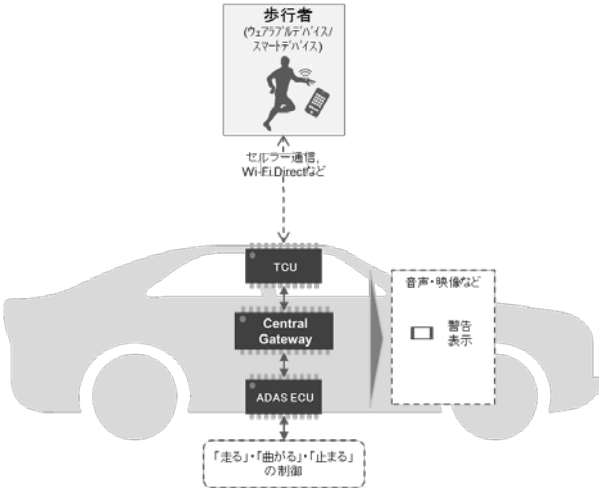
### 1-1. 脅威の重大度(スコア)の分布




### 1-2. 最も重大な脅威

- 大量のデータ送信による該当サービス提供の妨害
- 信頼できないソースからのデータ入力

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ(インパクト) | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| 通信データの送信元なりすまし | 1.39 | 1.59 | 2.22 |
| コマンドインジェクション | 1.39 | 1.59 | 2.22 |
| データ/コードの改ざん | 1.39 | 1.59 | 2.22 |
| データ/コードの上書き | 1.39 | 1.59 | 2.22 |
| データ/コードの削除 | 1.39 | 1.59 | 2.22 |
| データ/コードの追加 | 1.39 | 1.59 | 2.22 |
| 信頼できないソースからのデータ入力 | 2.79 | 1.59 | 4.44 |
| MITM | 0.60 | 1.59 | 0.95 |
| リプレイ攻撃 | 1.39 | 1.59 | 2.22 |
| 通信路の盗聴 | 0.40 | 1.59 | 0.63 |
| 通信路からのデータへの不正アクセス | 0.40 | 1.59 | 0.63 |
| 大量のデータ送信による該当サービス提供の妨害 | 4.18 | 1.59 | 6.67 |
| root権限の奪取 | 1.39 | 1.59 | 2.22 |
| 不正なV2Xメッセージ送信 | 1.39 | 1.59 | 2.22 |

# 2-3. 注意喚起(ITS協調型)

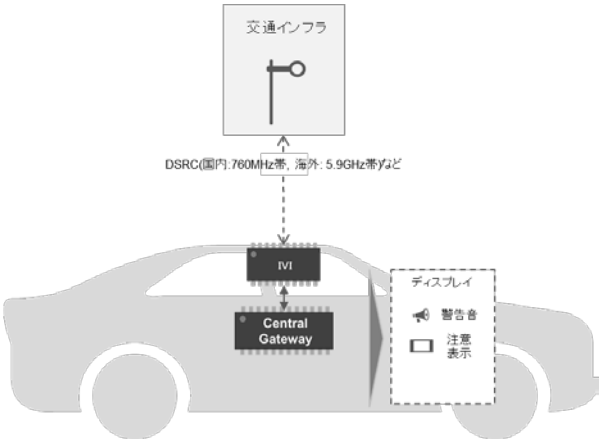
## 1. 評価結果

### 1-1. 脅威の重大度(スコア)の分布


### 1-2. 最も重大な脅威

- 信頼できないソースからのデータ入力
- コマンドインジェクションなど

## 2. 想定システム構成




## 3. 脅威の重大度

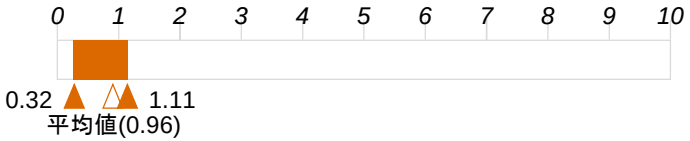
| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ(インパクト) | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| 通信データの送信元なりすまし | 0.20 | 1.59 | 0.32 |
| コマンドインジェクション | 0.80 | 1.59 | 1.27 |
| データ/コードの改ざん | 0.80 | 1.59 | 1.27 |
| データ/コードの上書き | 0.80 | 1.59 | 1.27 |
| データ/コードの削除 | 0.80 | 1.59 | 1.27 |
| データ/コードの追加 | 0.80 | 1.59 | 1.27 |
| 信頼できないソースからのデータ入力 | 1.59 | 1.59 | 2.54 |
| MITM | 0.60 | 1.59 | 0.95 |
| リプレイ攻撃 | 0.80 | 1.59 | 1.27 |
| 通信路の盗聴 | 0.40 | 1.59 | 0.63 |
| 通信路からのデータへの不正アクセス | 0.40 | 1.59 | 0.63 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 1.59 | 0.95 |
| root権限の奪取 | 0.80 | 1.59 | 1.27 |
| 不正なV2Xメッセージ送信 | 0.80 | 1.59 | 1.27 |

# 3-1. 省燃費走行支援

## 1. 評価結果

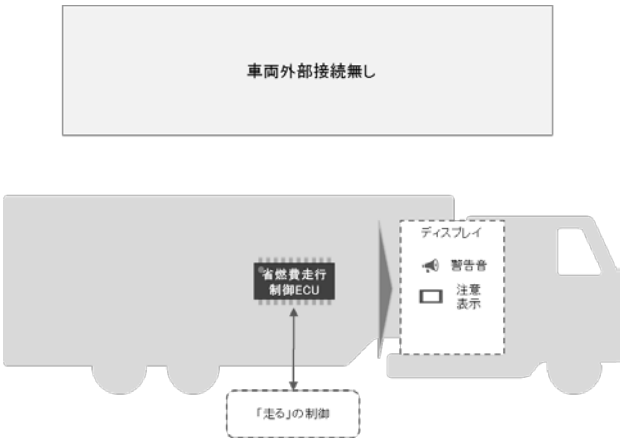
### 1-1. 脅威の重大度（スコア）の分布




### 1-2. 最も重大な脅威

- 通信データの送信元なりすまし
- コマンドインジェクションなど

## 2. 想定システム構成




## 3. 脅威の重大度

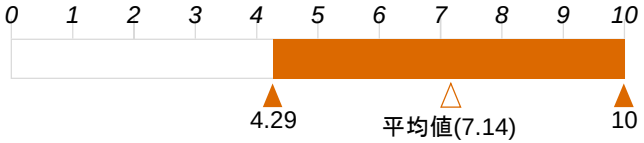
| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| 通信データの送信元なりすまし | 1.39 | 0.80 | 1.11 |
| コマンドインジェクション | 1.39 | 0.80 | 1.11 |
| データ/コードの改ざん | 1.39 | 0.80 | 1.11 |
| データ/コードの上書き | 1.39 | 0.80 | 1.11 |
| データ/コードの削除 | 1.39 | 0.80 | 1.11 |
| データ/コードの追加 | 1.39 | 0.80 | 1.11 |
| 信頼できないソースからのデータ入力 | 1.39 | 0.80 | 1.11 |
| MITM | 0.60 | 0.80 | 0.48 |
| リプレイ攻撃 | 1.39 | 0.80 | 1.11 |
| 通信路の盗聴 | 0.40 | 0.80 | 0.32 |
| 通信路からのデータへの不正アクセス | 0.40 | 0.80 | 0.32 |
| 大量のデータ送信による該当サービス提供の妨害 | 1.39 | 0.80 | 1.11 |
| root権限の奪取 | 1.39 | 0.80 | 1.11 |
| 不正なCANメッセージ送信 | 1.39 | 0.80 | 1.11 |
| 通信データの改ざん（テレマティクス） | 1.39 | 0.80 | 1.11 |

# 4-1. OTA

## 1. 評価結果

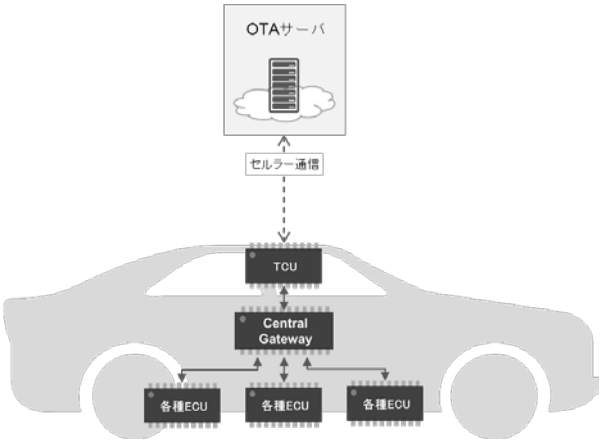
### 1-1. 脅威の重大度（スコア）の分布




### 1-2. 最も重大な脅威

- アップデートの妨害/アップデートプログラムの改ざん（サーバー）
- 正当なアップデート実行の妨害

## 2. 想定システム構成




## 3. 脅威の重大度

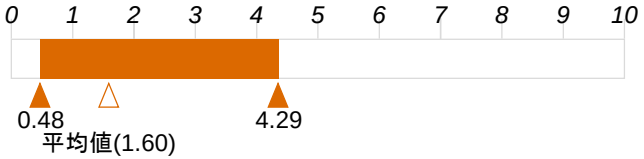
| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| アップデートの妨害/アップデートプログラムの改ざん（サーバー） | 4.18 | 2.39 | 10.00 |
| 正当なアップデート実行の妨害 | 3.59 | 1.20 | 4.29 |

# 5-1. 故障検知

## 1. 評価結果

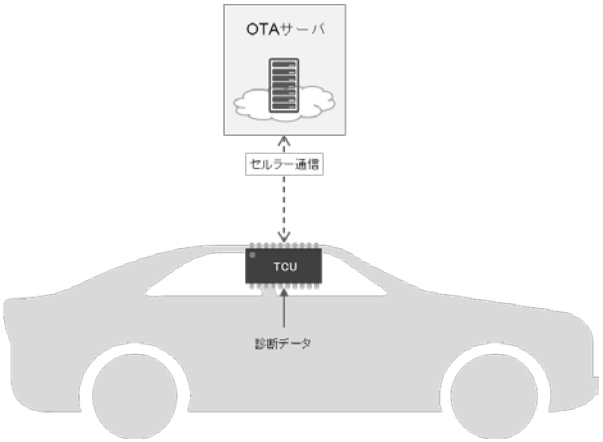
### 1-1. 脅威の重大度（スコア）の分布




### 1-2. 最も重大な脅威

- サーバーへの不正侵入による車両への攻撃
- データ/コードの改ざん

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 1.79 | 2.39 | 4.29 |
| サーバーへのDoS攻撃 | 0.60 | 2.39 | 1.43 |
| 通信データの送信元なりすまし | 0.20 | 2.39 | 0.48 |
| コマンドインジェクション | 0.20 | 2.39 | 0.48 |
| データ/コードの改ざん | 0.80 | 2.39 | 1.90 |
| データ/コードの上書き | 0.80 | 2.39 | 1.90 |
| データ/コードの削除 | 0.80 | 2.39 | 1.90 |
| データ/コードの追加 | 0.80 | 2.39 | 1.90 |
| 信頼できないソースからのデータ入力 | 0.80 | 2.39 | 1.90 |
| MITM | 0.60 | 2.39 | 1.43 |
| リプレイ攻撃 | 0.80 | 2.39 | 1.90 |
| 通信路の盗聴 | 0.40 | 2.39 | 0.95 |
| 通信路からのデータへの不正アクセス | 0.40 | 2.39 | 0.95 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 2.39 | 1.43 |
| root権限の奪取 | 0.80 | 2.39 | 1.90 |
| 不正なCANメッセージ送信 | 0.20 | 2.39 | 0.48 |
| 通信データの改ざん（テレマティクス） | 0.80 | 2.39 | 1.90 |

# 6-1. 自動衝突通知

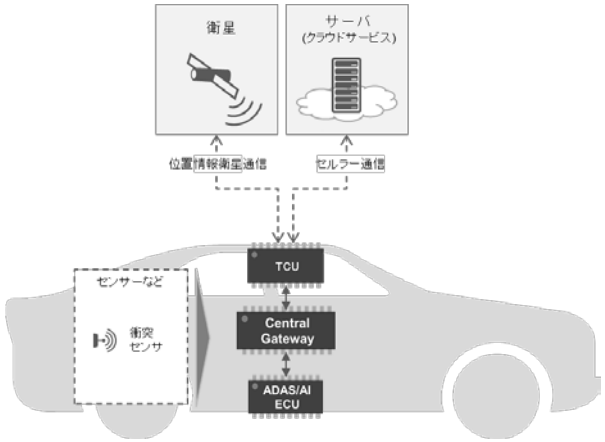
## 1. 評価結果

### 1-1. 脅威の重大度（スコア）の分布


### 1-2. 最も重大な脅威

- コマンドインジェクション
- データ/コードの改ざんなど

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| 通信データの送信元なりすまし | 0.20 | 0.40 | 0.08 |
| コマンドインジェクション | 0.80 | 0.40 | 0.32 |
| データ/コードの改ざん | 0.80 | 0.40 | 0.32 |
| データ/コードの上書き | 0.80 | 0.40 | 0.32 |
| データ/コードの削除 | 0.80 | 0.40 | 0.32 |
| データ/コードの追加 | 0.80 | 0.40 | 0.32 |
| 信頼できないソースからのデータ入力 | 0.80 | 0.40 | 0.32 |
| MITM | 0.60 | 0.40 | 0.24 |
| リプレイ攻撃 | 0.80 | 0.40 | 0.32 |
| 通信路の盗聴 | 0.40 | 0.40 | 0.16 |
| 通信路からのデータへの不正アクセス | 0.40 | 0.40 | 0.16 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.20 | 0.40 | 0.08 |
| root権限の奪取 | 0.80 | 0.40 | 0.32 |

# 6-2. 車両故障時の電話サポート

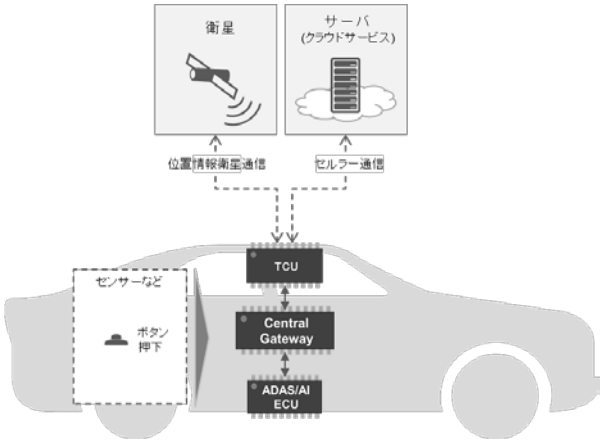
## 1. 評価結果

### 1-1. 脅威の重大度（スコア）の分布


### 1-2. 最も重大な脅威

- コマンドインジェクション
- データ/コードの改ざんなど

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| 通信データの送信元なりすまし | 0.20 | 0.40 | 0.08 |
| コマンドインジェクション | 0.80 | 0.40 | 0.32 |
| データ/コードの改ざん | 0.80 | 0.40 | 0.32 |
| データ/コードの上書き | 0.80 | 0.40 | 0.32 |
| データ/コードの削除 | 0.80 | 0.40 | 0.32 |
| データ/コードの追加 | 0.80 | 0.40 | 0.32 |
| 信頼できないソースからのデータ入力 | 0.80 | 0.40 | 0.32 |
| MITM | 0.60 | 0.40 | 0.24 |
| リプレイ攻撃 | 0.80 | 0.40 | 0.32 |
| 通信路の盗聴 | 0.40 | 0.40 | 0.16 |
| 通信路からのデータへの不正アクセス | 0.40 | 0.40 | 0.16 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.20 | 0.40 | 0.08 |
| root権限の奪取 | 0.80 | 0.40 | 0.32 |

# 7-1. ドア・トランク・ハザードランプなどの状態監視

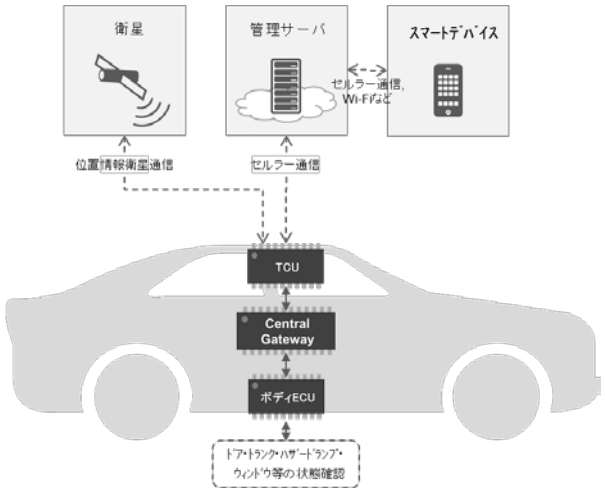
## 1. 評価結果

### 1-1. 脅威の重大度（スコア）の分布


### 1-2. 最も重大な脅威

- サーバーへの不正侵入による車両への攻撃
- サーバーへのDoS攻撃など

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 2.39 | 1.20 | 2.86 |
| サーバーへのDoS攻撃 | 2.39 | 1.20 | 2.86 |
| 通信データの送信元なりすまし | 0.80 | 1.20 | 0.95 |
| コマンドインジェクション | 0.80 | 1.20 | 0.95 |
| データ/コードの改ざん | 0.80 | 1.20 | 0.95 |
| データ/コードの上書き | 0.80 | 1.20 | 0.95 |
| データ/コードの削除 | 0.80 | 1.20 | 0.95 |
| データ/コードの追加 | 0.80 | 1.20 | 0.95 |
| 信頼できないソースからのデータ入力 | 1.59 | 1.20 | 1.90 |
| MITM | 0.80 | 1.20 | 0.95 |
| リプレイ攻撃 | 0.80 | 1.20 | 0.95 |
| 通信路の盗聴 | 0.80 | 1.20 | 0.95 |
| 通信路からのデータへの不正アクセス | 0.80 | 1.20 | 0.95 |
| 大量のデータ送信による該当サービス提供の妨害 | 2.39 | 1.20 | 2.86 |
| root権限の奪取 | 0.80 | 1.20 | 0.95 |
| 不正なCANメッセージ送信 | 0.80 | 1.20 | 0.95 |
| 通信データの改ざん（テレマティクス） | 0.80 | 1.20 | 0.95 |

# 7-2. 車両異常検知/通報

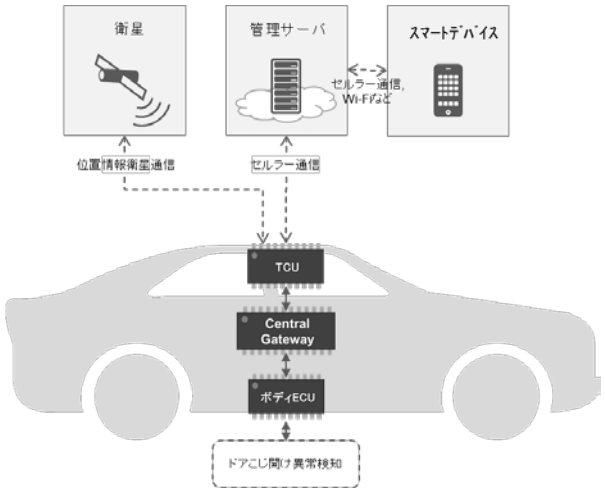
## 1. 評価結果

### 1-1. 脅威の重大度（スコア）の分布


### 1-2. 最も重大な脅威

- サーバーへの不正侵入による車両への攻撃
- サーバーへのDoS攻撃など

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 2.39 | 1.20 | 2.86 |
| サーバーへのDoS攻撃 | 2.39 | 1.20 | 2.86 |
| 通信データの送信元なりすまし | 0.80 | 1.20 | 0.95 |
| コマンドインジェクション | 0.80 | 1.20 | 0.95 |
| データ/コードの改ざん | 0.80 | 1.20 | 0.95 |
| データ/コードの上書き | 0.80 | 1.20 | 0.95 |
| データ/コードの削除 | 0.80 | 1.20 | 0.95 |
| データ/コードの追加 | 0.80 | 1.20 | 0.95 |
| 信頼できないソースからのデータ入力 | 1.59 | 1.20 | 1.90 |
| MITM | 0.80 | 1.20 | 0.95 |
| リプレイ攻撃 | 0.80 | 1.20 | 0.95 |
| 通信路の盗聴 | 0.80 | 1.20 | 0.95 |
| 通信路からのデータへの不正アクセス | 0.80 | 1.20 | 0.95 |
| 大量のデータ送信による該当サービス提供の妨害 | 2.39 | 1.20 | 2.86 |
| root権限の奪取 | 0.80 | 1.20 | 0.95 |
| 不正なCANメッセージ送信 | 0.80 | 1.20 | 0.95 |
| 通信データの改ざん（テレマティクス） | 0.80 | 1.20 | 0.95 |

# 7-3. 車両位置追跡

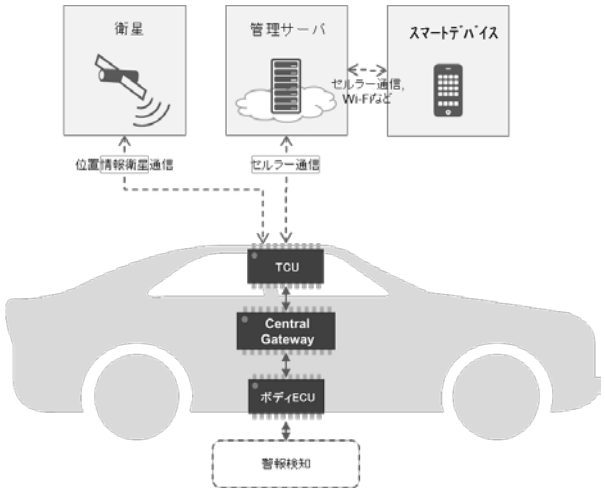
## 1. 評価結果

### 1-1. 脅威の重大度（スコア）の分布


### 1-2. 最も重大な脅威

- サーバーへの不正侵入による車両への攻撃
- サーバーへのDoS攻撃など

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 2.39 | 1.20 | 2.86 |
| サーバーへのDoS攻撃 | 2.39 | 1.20 | 2.86 |
| 通信データの送信元なりすまし | 0.80 | 1.20 | 0.95 |
| コマンドインジェクション | 0.80 | 1.20 | 0.95 |
| データ/コードの改ざん | 0.80 | 1.20 | 0.95 |
| データ/コードの上書き | 0.80 | 1.20 | 0.95 |
| データ/コードの削除 | 0.80 | 1.20 | 0.95 |
| データ/コードの追加 | 0.80 | 1.20 | 0.95 |
| 信頼できないソースからのデータ入力 | 1.59 | 1.20 | 1.90 |
| MITM | 0.80 | 1.20 | 0.95 |
| リプレイ攻撃 | 0.80 | 1.20 | 0.95 |
| 通信路の盗聴 | 0.80 | 1.20 | 0.95 |
| 通信路からのデータへの不正アクセス | 0.80 | 1.20 | 0.95 |
| 大量のデータ送信による該当サービス提供の妨害 | 2.39 | 1.20 | 2.86 |
| root権限の奪取 | 0.80 | 1.20 | 0.95 |
| 不正なCANメッセージ送信 | 0.80 | 1.20 | 0.95 |
| 通信データの改ざん（テレマティクス） | 0.80 | 1.20 | 0.95 |

# 7-3. 車両位置追跡(デバイス接続型)

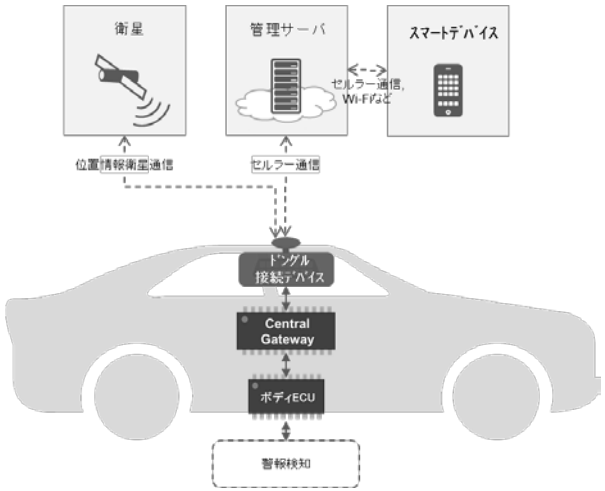
## 1. 評価結果

### 1-1. 脅威の重大度(スコア)の分布


### 1-2. 最も重大な脅威

- サーバーへの不正侵入による車両への攻撃
- サーバーへのDoS攻撃など

## 2. 想定システム構成




## 3. 脅威の重大度

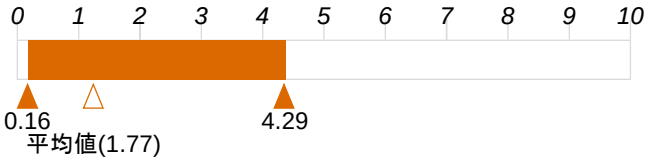
| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ(インパクト) | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 2.39 | 1.20 | 2.86 |
| サーバーへのDoS攻撃 | 2.39 | 1.20 | 2.86 |
| 通信データの送信元なりすまし | 0.80 | 1.20 | 0.95 |
| コマンドインジェクション | 0.80 | 1.20 | 0.95 |
| データ/コードの改ざん | 0.80 | 1.20 | 0.95 |
| データ/コードの上書き | 0.80 | 1.20 | 0.95 |
| データ/コードの削除 | 0.80 | 1.20 | 0.95 |
| データ/コードの追加 | 0.80 | 1.20 | 0.95 |
| 信頼できないソースからのデータ入力 | 1.59 | 1.20 | 1.90 |
| MITM | 0.80 | 1.20 | 0.95 |
| リプレイ攻撃 | 0.80 | 1.20 | 0.95 |
| 通信路の盗聴 | 0.80 | 1.20 | 0.95 |
| 通信路からのデータへの不正アクセス | 0.80 | 1.20 | 0.95 |
| 大量のデータ送信による該当サービス提供の妨害 | 2.39 | 1.20 | 2.86 |
| root権限の奪取 | 0.80 | 1.20 | 0.95 |
| 不正なCANメッセージ送信 | 0.80 | 1.20 | 0.95 |
| 通信データの改ざん(テレマティクス) | 0.80 | 1.20 | 0.95 |

# 8-1. 遠隔からのドアロック・アンロック

## 1. 評価結果

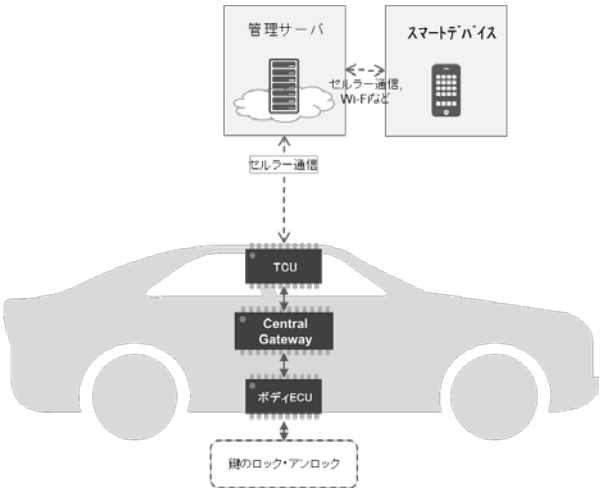
### 1-1. 脅威の重大度（スコア）の分布




### 1-2. 最も重大な脅威

- サーバーへの不正侵入による車両への攻撃
- 信頼できないソースからのデータ入力

## 2. 想定システム構成




## 3. 脅威の重大度

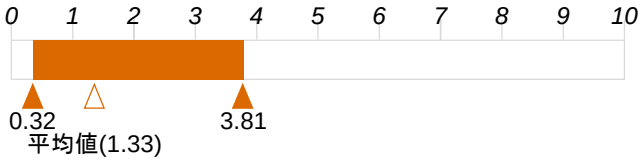
| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 1.79 | 2.39 | 4.29 |
| サーバーへのDoS攻撃 | 0.60 | 2.39 | 1.43 |
| 通信データの送信元なりすまし | 0.20 | 0.80 | 0.16 |
| コマンドインジェクション | 0.80 | 2.39 | 1.90 |
| データ/コードの改ざん | 0.80 | 2.39 | 1.90 |
| データ/コードの上書き | 0.80 | 2.39 | 1.90 |
| データ/コードの削除 | 0.80 | 2.39 | 1.90 |
| データ/コードの追加 | 0.80 | 2.39 | 1.90 |
| 信頼できないソースからのデータ入力 | 1.59 | 2.39 | 3.81 |
| MITM | 0.60 | 2.39 | 1.43 |
| リプレイ攻撃 | 0.80 | 2.39 | 1.90 |
| 通信路の盗聴 | 0.40 | 2.39 | 0.95 |
| 通信路からのデータへの不正アクセス | 0.40 | 2.39 | 0.95 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 2.39 | 1.43 |
| root権限の奪取 | 0.80 | 2.39 | 1.90 |
| 不正なCANメッセージ送信 | 0.20 | 2.39 | 0.48 |
| 通信データの改ざん（テレマティクス） | 0.80 | 2.39 | 1.90 |

# 8-2. インテリジェントキー

## 1. 評価結果

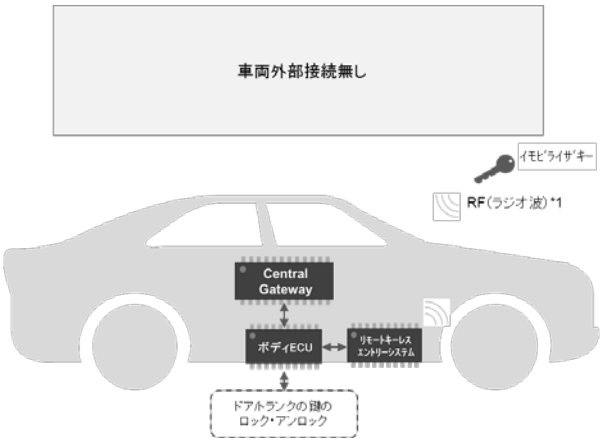
### 1-1. 脅威の重大度（スコア）の分布




### 1-2. 最も重大な脅威

- 短距離通信/センサーの改ざん
- 信頼できないソースからのデータ入力

## 2. 想定システム構成




## 3. 脅威の重大度

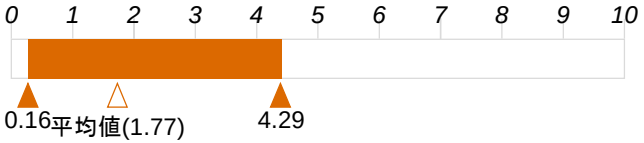
| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| 通信データの送信元なりすまし | 0.20 | 1.59 | 0.32 |
| コマンドインジェクション | 0.80 | 1.59 | 1.27 |
| データ/コードの改ざん | 0.80 | 1.59 | 1.27 |
| データ/コードの上書き | 0.80 | 1.59 | 1.27 |
| データ/コードの削除 | 0.80 | 1.59 | 1.27 |
| データ/コードの追加 | 0.80 | 1.59 | 1.27 |
| 信頼できないソースからのデータ入力 | 1.59 | 1.59 | 2.54 |
| MITM | 0.60 | 1.59 | 0.95 |
| リプレイ攻撃 | 0.80 | 1.59 | 1.27 |
| 通信路の盗聴 | 0.40 | 1.59 | 0.63 |
| 通信路からのデータへの不正アクセス | 0.40 | 1.59 | 0.63 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 1.59 | 0.95 |
| root権限の奪取 | 0.80 | 1.59 | 1.27 |
| 通信機能（リモートキーなど）の機能改ざん | 0.80 | 1.59 | 1.27 |
| 短距離通信/センサーの改ざん | 2.39 | 1.59 | 3.81 |

# 8-3. 充電制御

## 1. 評価結果

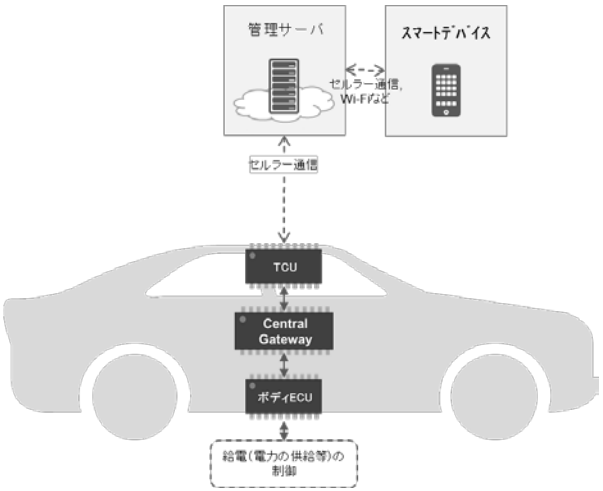
### 1-1. 脅威の重大度（スコア）の分布




### 1-2. 最も重大な脅威

- サーバーへの不正侵入による車両への攻撃
- 信頼できないソースからのデータ入力

## 2. 想定システム構成




## 3. 脅威の重大度

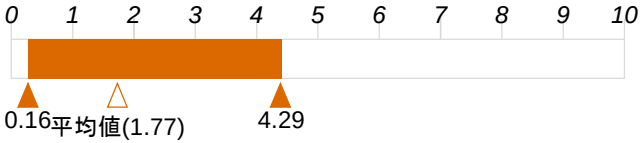
| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 1.79 | 2.39 | 4.29 |
| サーバーへのDoS攻撃 | 0.60 | 2.39 | 1.43 |
| 通信データの送信元なりすまし | 0.20 | 0.80 | 0.16 |
| コマンドインジェクション | 0.80 | 2.39 | 1.90 |
| データ/コードの改ざん | 0.80 | 2.39 | 1.90 |
| データ/コードの上書き | 0.80 | 2.39 | 1.90 |
| データ/コードの削除 | 0.80 | 2.39 | 1.90 |
| データ/コードの追加 | 0.80 | 2.39 | 1.90 |
| 信頼できないソースからのデータ入力 | 1.59 | 2.39 | 3.81 |
| MITM | 0.60 | 2.39 | 1.43 |
| リプレイ攻撃 | 0.80 | 2.39 | 1.90 |
| 通信路の盗聴 | 0.40 | 2.39 | 0.95 |
| 通信路からのデータへの不正アクセス | 0.40 | 2.39 | 0.95 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 2.39 | 1.43 |
| root権限の奪取 | 0.80 | 2.39 | 1.90 |
| 不正なCANメッセージ送信 | 0.20 | 2.39 | 0.48 |
| 通信データの改ざん（テレマティクス） | 0.80 | 2.39 | 1.90 |

# 8-4. 充電制御（音声認識AI連携）

## 1. 評価結果

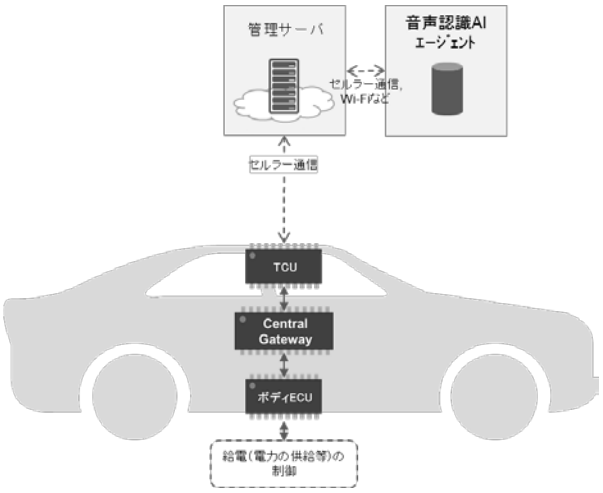
### 1-1. 脅威の重大度（スコア）の分布




### 1-2. 最も重大な脅威

- サーバーへの不正侵入による車両への攻撃
- 信頼できないソースからのデータ入力

## 2. 想定システム構成




## 3. 脅威の重大度

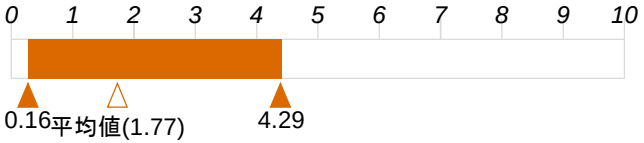
| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 1.79 | 2.39 | 4.29 |
| サーバーへのDoS攻撃 | 0.60 | 2.39 | 1.43 |
| 通信データの送信元なりすまし | 0.20 | 0.80 | 0.16 |
| コマンドインジェクション | 0.80 | 2.39 | 1.90 |
| データ/コードの改ざん | 0.80 | 2.39 | 1.90 |
| データ/コードの上書き | 0.80 | 2.39 | 1.90 |
| データ/コードの削除 | 0.80 | 2.39 | 1.90 |
| データ/コードの追加 | 0.80 | 2.39 | 1.90 |
| 信頼できないソースからのデータ入力 | 1.59 | 2.39 | 3.81 |
| MITM | 0.60 | 2.39 | 1.43 |
| リプレイ攻撃 | 0.80 | 2.39 | 1.90 |
| 通信路の盗聴 | 0.40 | 2.39 | 0.95 |
| 通信路からのデータへの不正アクセス | 0.40 | 2.39 | 0.95 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 2.39 | 1.43 |
| root権限の奪取 | 0.80 | 2.39 | 1.90 |
| 不正なCANメッセージ送信 | 0.20 | 2.39 | 0.48 |
| 通信データの改ざん（テレマティクス） | 0.80 | 2.39 | 1.90 |

# 8-5. エアコン制御

## 1. 評価結果

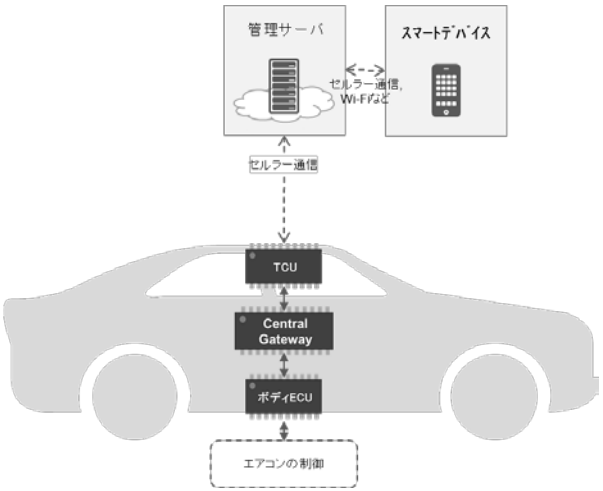
### 1-1. 脅威の重大度（スコア）の分布




### 1-2. 最も重大な脅威

- サーバーへの不正侵入による車両への攻撃
- 信頼できないソースからのデータ入力

## 2. 想定システム構成




## 3. 脅威の重大度

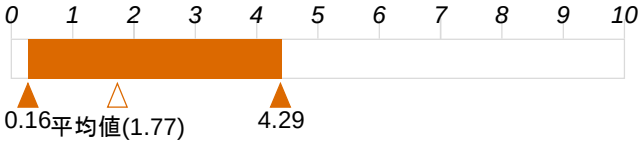
| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 1.79 | 2.39 | 4.29 |
| サーバーへのDoS攻撃 | 0.60 | 2.39 | 1.43 |
| 通信データの送信元なりすまし | 0.20 | 0.80 | 0.16 |
| コマンドインジェクション | 0.80 | 2.39 | 1.90 |
| データ/コードの改ざん | 0.80 | 2.39 | 1.90 |
| データ/コードの上書き | 0.80 | 2.39 | 1.90 |
| データ/コードの削除 | 0.80 | 2.39 | 1.90 |
| データ/コードの追加 | 0.80 | 2.39 | 1.90 |
| 信頼できないソースからのデータ入力 | 1.59 | 2.39 | 3.81 |
| MITM | 0.60 | 2.39 | 1.43 |
| リプレイ攻撃 | 0.80 | 2.39 | 1.90 |
| 通信路の盗聴 | 0.40 | 2.39 | 0.95 |
| 通信路からのデータへの不正アクセス | 0.40 | 2.39 | 0.95 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 2.39 | 1.43 |
| root権限の奪取 | 0.80 | 2.39 | 1.90 |
| 不正なCANメッセージ送信 | 0.20 | 2.39 | 0.48 |
| 通信データの改ざん（テレマティクス） | 0.80 | 2.39 | 1.90 |

# 8-6. エアコン制御（音声認識AI連携）

## 1. 評価結果

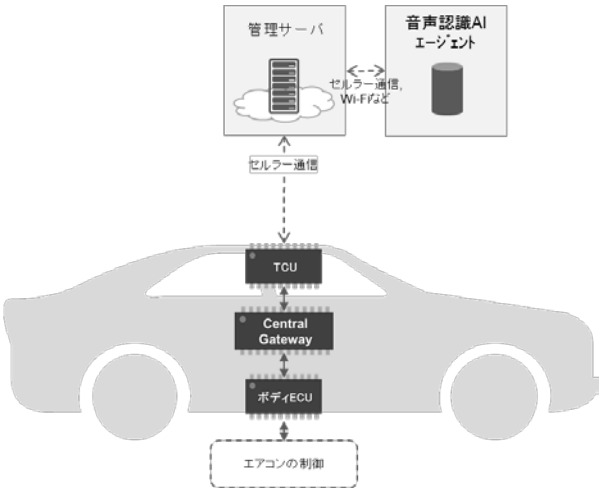
### 1-1. 脅威の重大度（スコア）の分布




### 1-2. 最も重大な脅威

- サーバーへの不正侵入による車両への攻撃
- 信頼できないソースからのデータ入力

## 2. 想定システム構成




## 3. 脅威の重大度

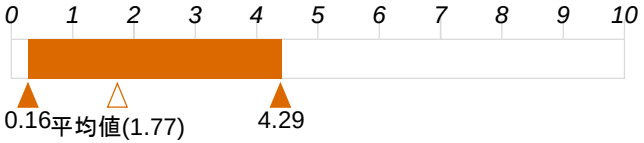
| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 1.79 | 2.39 | 4.29 |
| サーバーへのDoS攻撃 | 0.60 | 2.39 | 1.43 |
| 通信データの送信元なりすまし | 0.20 | 0.80 | 0.16 |
| コマンドインジェクション | 0.80 | 2.39 | 1.90 |
| データ/コードの改ざん | 0.80 | 2.39 | 1.90 |
| データ/コードの上書き | 0.80 | 2.39 | 1.90 |
| データ/コードの削除 | 0.80 | 2.39 | 1.90 |
| データ/コードの追加 | 0.80 | 2.39 | 1.90 |
| 信頼できないソースからのデータ入力 | 1.59 | 2.39 | 3.81 |
| MITM | 0.60 | 2.39 | 1.43 |
| リプレイ攻撃 | 0.80 | 2.39 | 1.90 |
| 通信路の盗聴 | 0.40 | 2.39 | 0.95 |
| 通信路からのデータへの不正アクセス | 0.40 | 2.39 | 0.95 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 2.39 | 1.43 |
| root権限の奪取 | 0.80 | 2.39 | 1.90 |
| 不正なCANメッセージ送信 | 0.20 | 2.39 | 0.48 |
| 通信データの改ざん（テレマティクス） | 0.80 | 2.39 | 1.90 |

# 8-7. エンジン再駆動・ステアリングロック解除禁止

## 1. 評価結果

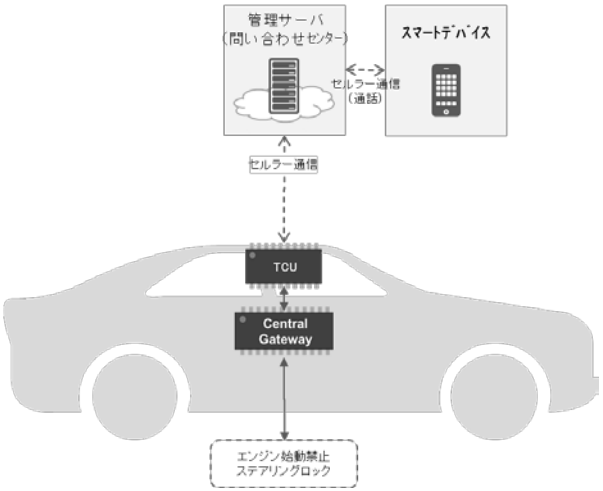
### 1-1. 脅威の重大度（スコア）の分布




### 1-2. 最も重大な脅威

- サーバーへの不正侵入による車両への攻撃
- 信頼できないソースからのデータ入力

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 1.79 | 2.39 | 4.29 |
| サーバーへのDoS攻撃 | 0.60 | 2.39 | 1.43 |
| 通信データの送信元なりすまし | 0.20 | 0.80 | 0.16 |
| コマンドインジェクション | 0.80 | 2.39 | 1.90 |
| データ/コードの改ざん | 0.80 | 2.39 | 1.90 |
| データ/コードの上書き | 0.80 | 2.39 | 1.90 |
| データ/コードの削除 | 0.80 | 2.39 | 1.90 |
| データ/コードの追加 | 0.80 | 2.39 | 1.90 |
| 信頼できないソースからのデータ入力 | 1.59 | 2.39 | 3.81 |
| MITM | 0.60 | 2.39 | 1.43 |
| リプレイ攻撃 | 0.80 | 2.39 | 1.90 |
| 通信路の盗聴 | 0.40 | 2.39 | 0.95 |
| 通信路からのデータへの不正アクセス | 0.40 | 2.39 | 0.95 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 2.39 | 1.43 |
| root権限の奪取 | 0.80 | 2.39 | 1.90 |
| 不正なCANメッセージ送信 | 0.20 | 2.39 | 0.48 |
| 通信データの改ざん（テレマティクス） | 0.80 | 2.39 | 1.90 |

# 9-1. カーシェアリング

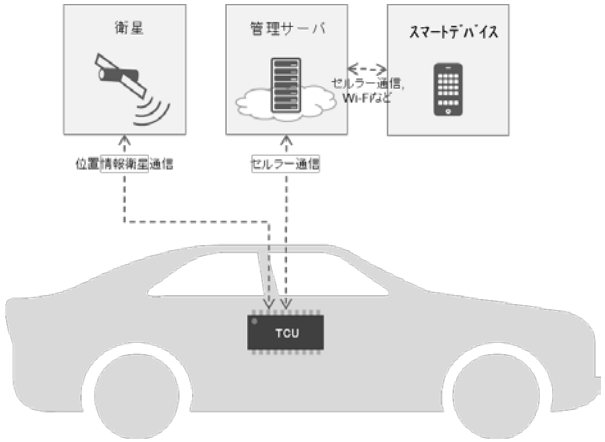
## 1. 評価結果

### 1-1. 脅威の重大度（スコア）の分布


### 1-2. 最も重大な脅威

- サーバーへの不正侵入による車両への攻撃
- 信頼できないソースからのデータ入力

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 1.79 | 1.20 | 2.14 |
| サーバーへのDoS攻撃 | 0.60 | 1.20 | 0.71 |
| 通信データの送信元なりすまし | 0.20 | 1.20 | 0.24 |
| コマンドインジェクション | 0.80 | 1.20 | 0.95 |
| データ/コードの改ざん | 0.80 | 1.20 | 0.95 |
| データ/コードの上書き | 0.80 | 1.20 | 0.95 |
| データ/コードの削除 | 0.80 | 1.20 | 0.95 |
| データ/コードの追加 | 0.80 | 1.20 | 0.95 |
| 信頼できないソースからのデータ入力 | 1.59 | 1.20 | 1.90 |
| MITM | 0.60 | 1.20 | 0.71 |
| リプレイ攻撃 | 0.80 | 1.20 | 0.95 |
| 通信路の盗聴 | 0.40 | 1.20 | 0.48 |
| 通信路からのデータへの不正アクセス | 0.40 | 1.20 | 0.48 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 1.20 | 0.71 |
| root権限の奪取 | 0.80 | 1.20 | 0.95 |
| 不正なCANメッセージ送信 | 0.20 | 1.20 | 0.24 |
| 通信データの改ざん（テレマティクス） | 0.80 | 1.20 | 0.95 |

# 10-1. 料金支払い

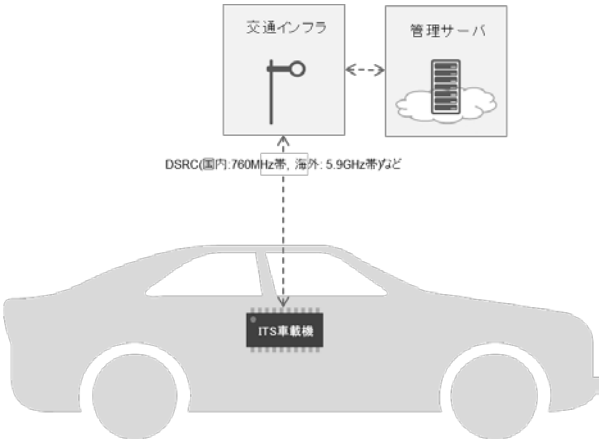
## 1. 評価結果

### 1-1. 脅威の重大度（スコア）の分布


### 1-2. 最も重大な脅威

- サーバーへの不正侵入による車両への攻撃
- 信頼できないソースからのデータ入力

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 1.79 | 1.79 | 3.21 |
| サーバーへのDoS攻撃 | 0.60 | 1.79 | 1.07 |
| 通信データの送信元なりすまし | 0.20 | 1.79 | 0.36 |
| コマンドインジェクション | 0.80 | 1.79 | 1.43 |
| データ/コードの改ざん | 0.80 | 1.79 | 1.43 |
| データ/コードの上書き | 0.80 | 1.79 | 1.43 |
| データ/コードの削除 | 0.80 | 1.79 | 1.43 |
| データ/コードの追加 | 0.80 | 1.79 | 1.43 |
| 信頼できないソースからのデータ入力 | 1.59 | 1.79 | 2.86 |
| MITM | 0.60 | 1.79 | 1.07 |
| リプレイ攻撃 | 0.80 | 1.79 | 1.43 |
| 通信路の盗聴 | 0.40 | 1.79 | 0.71 |
| 通信路からのデータへの不正アクセス | 0.40 | 1.79 | 0.71 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 1.79 | 1.07 |
| root権限の奪取 | 0.80 | 1.79 | 1.43 |
| 不正なCANメッセージ送信 | 0.20 | 1.79 | 0.36 |
| 通信データの改ざん（テレマティクス） | 0.80 | 1.79 | 1.43 |

# 11-1. ルート検索(組込み型)

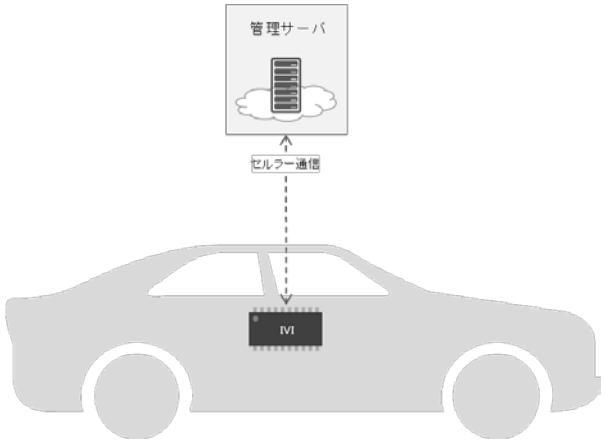
## 1. 評価結果

### 1-1. 脅威の重大度(スコア)の分布


### 1-2. 最も重大な脅威

- サーバーへの不正侵入による車両への攻撃
- 信頼できないソースからのデータ入力

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ(インパクト) | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 1.79 | 1.20 | 2.14 |
| サーバーへのDoS攻撃 | 0.60 | 1.20 | 0.71 |
| 通信データの送信元なりすまし | 0.20 | 0.40 | 0.08 |
| コマンドインジェクション | 0.80 | 0.40 | 0.32 |
| データ/コードの改ざん | 0.80 | 1.20 | 0.95 |
| データ/コードの上書き | 0.80 | 1.20 | 0.95 |
| データ/コードの削除 | 0.80 | 1.20 | 0.95 |
| データ/コードの追加 | 0.80 | 1.20 | 0.95 |
| 信頼できないソースからのデータ入力 | 1.59 | 1.20 | 1.90 |
| MITM | 0.60 | 1.20 | 0.71 |
| リプレイ攻撃 | 0.80 | 1.20 | 0.95 |
| 通信路の盗聴 | 0.40 | 1.20 | 0.48 |
| 通信路からのデータへの不正アクセス | 0.40 | 1.20 | 0.48 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 1.20 | 0.71 |
| root権限の奪取 | 0.80 | 1.20 | 0.95 |
| 不正なCANメッセージ送信 | 0.20 | 1.20 | 0.24 |

# 11-1. ルート検索（スマホ連携型）

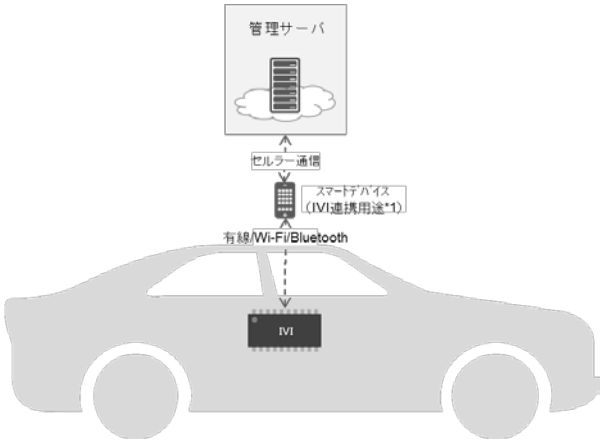
## 1. 評価結果

### 1-1. 脅威の重大度（スコア）の分布


### 1-2. 最も重大な脅威

- 信頼できないソースからのデータ入力
- コマンドインジェクションなど

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| 通信データの送信元なりすまし | 0.20 | 1.20 | 0.24 |
| コマンドインジェクション | 0.80 | 1.20 | 0.95 |
| データ/コードの改ざん | 0.80 | 1.20 | 0.95 |
| データ/コードの上書き | 0.80 | 1.20 | 0.95 |
| データ/コードの削除 | 0.80 | 1.20 | 0.95 |
| データ/コードの追加 | 0.80 | 1.20 | 0.95 |
| 信頼できないソースからのデータ入力 | 1.59 | 1.20 | 1.90 |
| MITM | 0.60 | 1.20 | 0.71 |
| リプレイ攻撃 | 0.80 | 1.20 | 0.95 |
| 通信路の盗聴 | 0.40 | 1.20 | 0.48 |
| 通信路からのデータへの不正アクセス | 0.40 | 1.20 | 0.48 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 1.20 | 0.71 |
| root権限の奪取 | 0.80 | 1.20 | 0.95 |

# 11-2. オペレータサービス(組込み型)

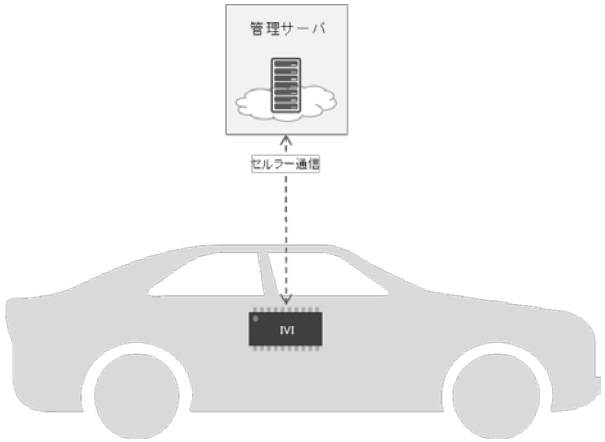
## 1. 評価結果

### 1-1. 脅威の重大度(スコア)の分布


### 1-2. 最も重大な脅威

- サーバーへの不正侵入による車両への攻撃
- 信頼できないソースからのデータ入力

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ(インパクト) | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 1.79 | 1.20 | 2.14 |
| サーバーへのDoS攻撃 | 0.60 | 1.20 | 0.71 |
| 通信データの送信元なりすまし | 0.20 | 0.40 | 0.08 |
| コマンドインジェクション | 0.80 | 0.40 | 0.32 |
| データ/コードの改ざん | 0.80 | 1.20 | 0.95 |
| データ/コードの上書き | 0.80 | 1.20 | 0.95 |
| データ/コードの削除 | 0.80 | 1.20 | 0.95 |
| データ/コードの追加 | 0.80 | 1.20 | 0.95 |
| 信頼できないソースからのデータ入力 | 1.59 | 1.20 | 1.90 |
| MITM | 0.60 | 1.20 | 0.71 |
| リプレイ攻撃 | 0.80 | 1.20 | 0.95 |
| 通信路の盗聴 | 0.40 | 1.20 | 0.48 |
| 通信路からのデータへの不正アクセス | 0.40 | 1.20 | 0.48 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 1.20 | 0.71 |
| root権限の奪取 | 0.80 | 1.20 | 0.95 |
| 不正なCANメッセージ送信 | 0.20 | 1.20 | 0.24 |

# 12-1. カレンダー・メール同期(組込み型)

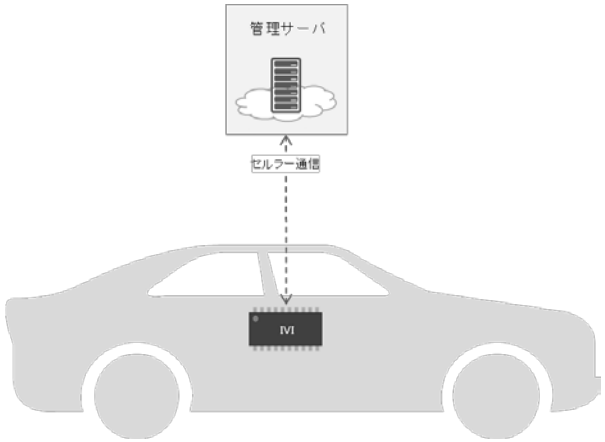
## 1. 評価結果

### 1-1. 脅威の重大度(スコア)の分布


### 1-2. 最も重大な脅威

- サーバーへの不正侵入による車両への攻撃
- 信頼できないソースからのデータ入力

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ(インパクト) | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 1.79 | 1.20 | 2.14 |
| サーバーへのDoS攻撃 | 0.60 | 1.20 | 0.71 |
| 通信データの送信元なりすまし | 0.20 | 0.40 | 0.08 |
| コマンドインジェクション | 0.80 | 0.40 | 0.32 |
| データ/コードの改ざん | 0.80 | 1.20 | 0.95 |
| データ/コードの上書き | 0.80 | 1.20 | 0.95 |
| データ/コードの削除 | 0.80 | 1.20 | 0.95 |
| データ/コードの追加 | 0.80 | 1.20 | 0.95 |
| 信頼できないソースからのデータ入力 | 1.59 | 1.20 | 1.90 |
| MITM | 0.60 | 1.20 | 0.71 |
| リプレイ攻撃 | 0.80 | 1.20 | 0.95 |
| 通信路の盗聴 | 0.40 | 1.20 | 0.48 |
| 通信路からのデータへの不正アクセス | 0.40 | 1.20 | 0.48 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 1.20 | 0.71 |
| root権限の奪取 | 0.80 | 1.20 | 0.95 |
| 不正なCANメッセージ送信 | 0.20 | 1.20 | 0.24 |

# 12-1. カレンダー・メール同期(スマホ連携型)

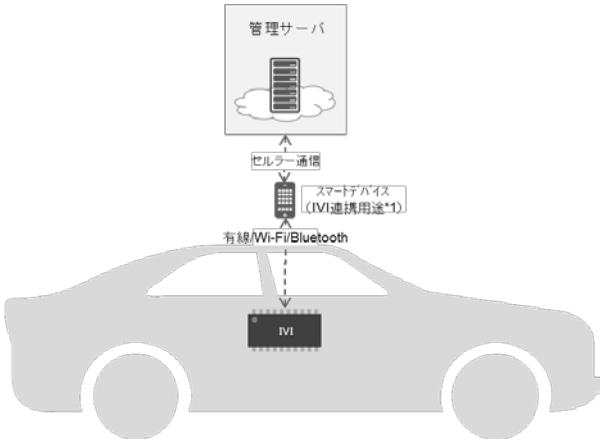
## 1. 評価結果

### 1-1. 脅威の重大度(スコア)の分布


### 1-2. 最も重大な脅威

- 信頼できないソースからのデータ入力
- コマンドインジェクションなど

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ(インパクト) | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| 通信データの送信元なりすまし | 0.20 | 1.20 | 0.24 |
| コマンドインジェクション | 0.80 | 1.20 | 0.95 |
| データ/コードの改ざん | 0.80 | 1.20 | 0.95 |
| データ/コードの上書き | 0.80 | 1.20 | 0.95 |
| データ/コードの削除 | 0.80 | 1.20 | 0.95 |
| データ/コードの追加 | 0.80 | 1.20 | 0.95 |
| 信頼できないソースからのデータ入力 | 1.59 | 1.20 | 1.90 |
| MITM | 0.60 | 1.20 | 0.71 |
| リプレイ攻撃 | 0.80 | 1.20 | 0.95 |
| 通信路の盗聴 | 0.40 | 1.20 | 0.48 |
| 通信路からのデータへの不正アクセス | 0.40 | 1.20 | 0.48 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 1.20 | 0.71 |
| root権限の奪取 | 0.80 | 1.20 | 0.95 |

# 12-2. SNS連携(組込み型)

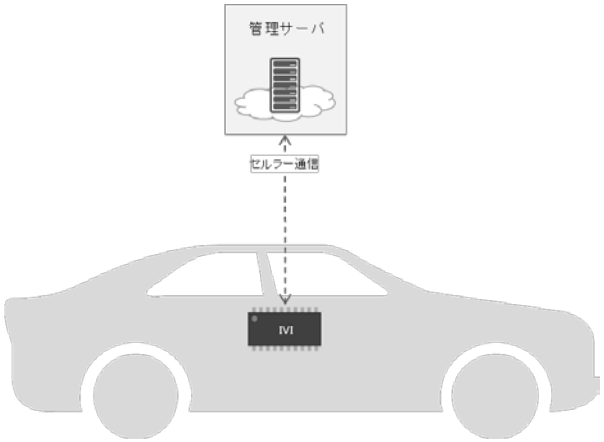
## 1. 評価結果

### 1-1. 脅威の重大度(スコア)の分布


### 1-2. 最も重大な脅威

- サーバーへの不正侵入による車両への攻撃
- 信頼できないソースからのデータ入力

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ(インパクト) | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 1.79 | 1.20 | 2.14 |
| サーバーへのDoS攻撃 | 0.60 | 1.20 | 0.71 |
| 通信データの送信元なりすまし | 0.20 | 0.40 | 0.08 |
| コマンドインジェクション | 0.80 | 0.40 | 0.32 |
| データ/コードの改ざん | 0.80 | 1.20 | 0.95 |
| データ/コードの上書き | 0.80 | 1.20 | 0.95 |
| データ/コードの削除 | 0.80 | 1.20 | 0.95 |
| データ/コードの追加 | 0.80 | 1.20 | 0.95 |
| 信頼できないソースからのデータ入力 | 1.59 | 1.20 | 1.90 |
| MITM | 0.60 | 1.20 | 0.71 |
| リプレイ攻撃 | 0.80 | 1.20 | 0.95 |
| 通信路の盗聴 | 0.40 | 1.20 | 0.48 |
| 通信路からのデータへの不正アクセス | 0.40 | 1.20 | 0.48 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 1.20 | 0.71 |
| root権限の奪取 | 0.80 | 1.20 | 0.95 |
| 不正なCANメッセージ送信 | 0.20 | 1.20 | 0.24 |

# 12-2. SNS連携（スマホ連携型）

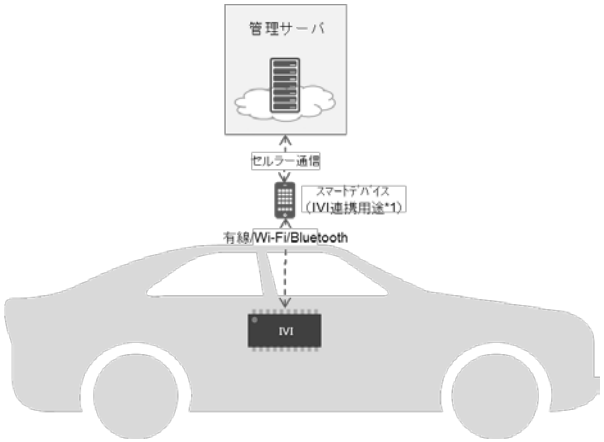
## 1. 評価結果

### 1-1. 脅威の重大度（スコア）の分布


### 1-2. 最も重大な脅威

- 信頼できないソースからのデータ入力
- コマンドインジェクションなど

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| 通信データの送信元なりすまし | 0.20 | 1.20 | 0.24 |
| コマンドインジェクション | 0.80 | 1.20 | 0.95 |
| データ/コードの改ざん | 0.80 | 1.20 | 0.95 |
| データ/コードの上書き | 0.80 | 1.20 | 0.95 |
| データ/コードの削除 | 0.80 | 1.20 | 0.95 |
| データ/コードの追加 | 0.80 | 1.20 | 0.95 |
| 信頼できないソースからのデータ入力 | 1.59 | 1.20 | 1.90 |
| MITM | 0.60 | 1.20 | 0.71 |
| リプレイ攻撃 | 0.80 | 1.20 | 0.95 |
| 通信路の盗聴 | 0.40 | 1.20 | 0.48 |
| 通信路からのデータへの不正アクセス | 0.40 | 1.20 | 0.48 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 1.20 | 0.71 |
| root権限の奪取 | 0.80 | 1.20 | 0.95 |

# 12-3. Wi-Fiスポット(組込み型)

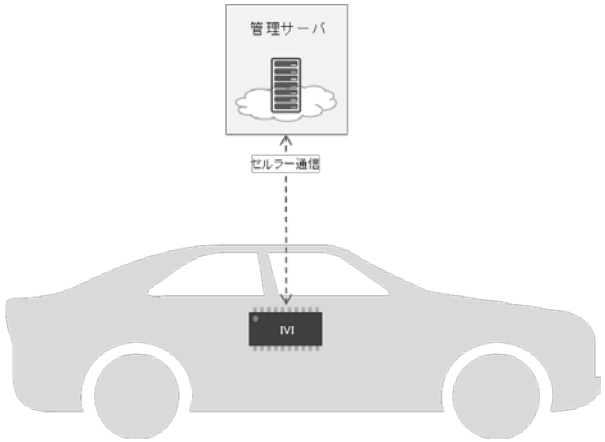
## 1. 評価結果

### 1-1. 脅威の重大度(スコア)の分布


### 1-2. 最も重大な脅威

- サーバーへの不正侵入による車両への攻撃
- 信頼できないソースからのデータ入力

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ(インパクト) | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 1.79 | 1.20 | 2.14 |
| サーバーへのDoS攻撃 | 0.60 | 1.20 | 0.71 |
| 通信データの送信元なりすまし | 0.20 | 0.40 | 0.08 |
| コマンドインジェクション | 0.80 | 0.40 | 0.32 |
| データ/コードの改ざん | 0.80 | 1.20 | 0.95 |
| データ/コードの上書き | 0.80 | 1.20 | 0.95 |
| データ/コードの削除 | 0.80 | 1.20 | 0.95 |
| データ/コードの追加 | 0.80 | 1.20 | 0.95 |
| 信頼できないソースからのデータ入力 | 1.59 | 1.20 | 1.90 |
| MITM | 0.60 | 1.20 | 0.71 |
| リプレイ攻撃 | 0.80 | 1.20 | 0.95 |
| 通信路の盗聴 | 0.40 | 1.20 | 0.48 |
| 通信路からのデータへの不正アクセス | 0.40 | 1.20 | 0.48 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 1.20 | 0.71 |
| root権限の奪取 | 0.80 | 1.20 | 0.95 |
| 不正なCANメッセージ送信 | 0.20 | 1.20 | 0.24 |

# 12-4. 各種アプリケーション利用(組込み型)

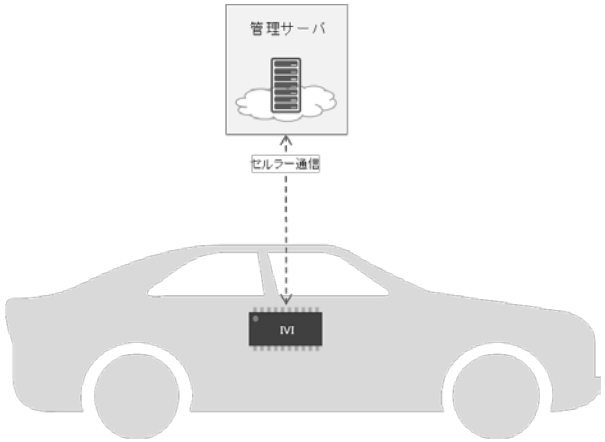
## 1. 評価結果

### 1-1. 脅威の重大度(スコア)の分布


### 1-2. 最も重大な脅威

- サーバーへの不正侵入による車両への攻撃
- 信頼できないソースからのデータ入力

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI(注意) | レベルII(警告) | レベルIII(重大) |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ(インパクト) | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| サーバーへの不正侵入による車両への攻撃 | 1.79 | 1.20 | 2.14 |
| サーバーへのDoS攻撃 | 0.60 | 1.20 | 0.71 |
| 通信データの送信元なりすまし | 0.20 | 0.40 | 0.08 |
| コマンドインジェクション | 0.80 | 0.40 | 0.32 |
| データ/コードの改ざん | 0.80 | 1.20 | 0.95 |
| データ/コードの上書き | 0.80 | 1.20 | 0.95 |
| データ/コードの削除 | 0.80 | 1.20 | 0.95 |
| データ/コードの追加 | 0.80 | 1.20 | 0.95 |
| 信頼できないソースからのデータ入力 | 1.59 | 1.20 | 1.90 |
| MITM | 0.60 | 1.20 | 0.71 |
| リプレイ攻撃 | 0.80 | 1.20 | 0.95 |
| 通信路の盗聴 | 0.40 | 1.20 | 0.48 |
| 通信路からのデータへの不正アクセス | 0.40 | 1.20 | 0.48 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 1.20 | 0.71 |
| root権限の奪取 | 0.80 | 1.20 | 0.95 |
| 不正なCANメッセージ送信 | 0.20 | 1.20 | 0.24 |

# 12-4. 各種アプリケーション利用（スマホ連携型）

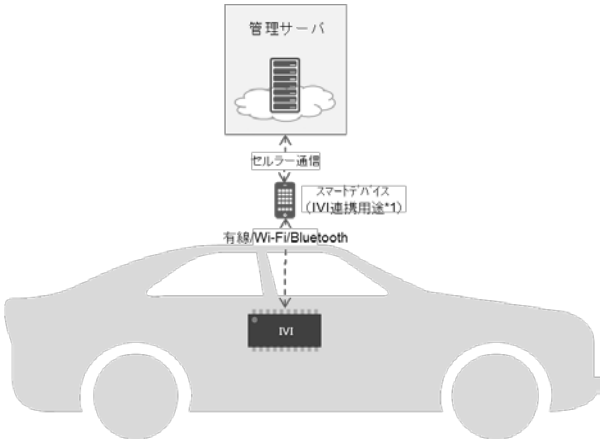
## 1. 評価結果

### 1-1. 脅威の重大度（スコア）の分布


### 1-2. 最も重大な脅威

- 信頼できないソースからのデータ入力
- コマンドインジェクションなど

## 2. 想定システム構成




## 3. 脅威の重大度

| 脅威のレベル | レベルI（注意） | レベルII（警告） | レベルIII（重大） |
|---|---|---|---|
| スコア | 0 ~ 3.9 | 4.0 ~ 6.9 | 7.0 ~ 10.0 |

| 脅威 | 脅威の大きさ（インパクト） | 攻撃の発生確率 | 脅威の重大度 |
|---|---|---|---|
| 通信データの送信元なりすまし | 0.20 | 1.20 | 0.24 |
| コマンドインジェクション | 0.80 | 1.20 | 0.95 |
| データ/コードの改ざん | 0.80 | 1.20 | 0.95 |
| データ/コードの上書き | 0.80 | 1.20 | 0.95 |
| データ/コードの削除 | 0.80 | 1.20 | 0.95 |
| データ/コードの追加 | 0.80 | 1.20 | 0.95 |
| 信頼できないソースからのデータ入力 | 1.59 | 1.20 | 1.90 |
| MITM | 0.60 | 1.20 | 0.71 |
| リプレイ攻撃 | 0.80 | 1.20 | 0.95 |
| 通信路の盗聴 | 0.40 | 1.20 | 0.48 |
| 通信路からのデータへの不正アクセス | 0.40 | 1.20 | 0.48 |
| 大量のデータ送信による該当サービス提供の妨害 | 0.60 | 1.20 | 0.71 |
| root権限の奪取 | 0.80 | 1.20 | 0.95 |