平成 29 年度成果報告書

「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
／情報セキュリティ実証実験」

平成 30 年 2 月

国立研究開発法人新エネルギー・産業技術総合開発機構

委託先　デロイト トーマツ リスクサービス株式会社

平成 30 年 2 月 28 日

国立研究開発法人新エネルギー・産業技術総合開発機構　　御中

デロイト トーマツ リスクサービス株式会社

代表取締役　　丸山　満彦

デロイト トーマツ リスクサービス株式会社（以下、「当社」という。）は、国立研究開発法人新エネルギー・産業技術総合開発機構（以下、「貴機構」という。）のご依頼に基づき、平成 29 年 9 月 28 日から平成 30 年 2 月 28 日まで、「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／情報セキュリティ実証実験における STEP1「実証前調査」」（以下、「本業務」という。）を実施し、本業務の結果を本報告書として以下のとおりまとめましたので、ご報告申し上げます。

本業務では、実証前調査として、自動走行システムにおけるセキュリティ脅威の調査及び分析によりその全体像を整理するとともに、セキュリティ評価手法・プロトコルを明確にすべく、実システム 1 台への試行調査を行い、「情報セキュリティ評価ガイドラインドラフト」作成を実施いたしました。

本報告書に記載されている事項は、本業務の実施期間中に得た情報等により確認できた事実のみに基づいています。したがって、必ずしもすべての事項を網羅したものではなく、その内容の十分性を保証するものではございません。また、本業務実施期間以降の状況の変化等を勘案したものではないことにご留意ください。

なお、本報告書は、貴機構における利用を前提として作成しています。これらの目的外で利用される場合は、お手数ですが事前に当社までご一報いただきますようお願い申し上げます。

目次

1. はじめに 3
(1) 背景 3
(2) 目的 3
2. 調査の成果 4
(1) 脅威分析調査 4
(2) 情報セキュリティ評価ガイドラインドラフトの作成 4
(3) 情報セキュリティ評価の試行調査 5
(4) 実証実験の運営準備 5

1. はじめに

(1) 背景

2020年の東京オリンピック・パラリンピックに向け、我が国の優れた最先端技術等によるイノベーションを世界に発信できるよう、自動走行システムについても実用化の加速を図ることが重要です。今回の大規模実証実験は、このような観点から、5つの技術領域（ダイナミックマップ、HMI、情報セキュリティ、歩行者事故低減、次世代都市交通）を中心に、自動車メーカー等の参加のもと、公道の実交通環境下において技術検証を行っていくものです。

また、今後の実用化に向けた技術面、運用面、制度面等での具体的課題の抽出とともに、海外メーカー等にも参加を呼び掛け、国際連携・協調の推進等も図っていくこととしています。さらに、別途、自動走行システムに対する一般の方々の正確な理解促進と社会受容性の醸成等に向けたイベントの開催なども検討することを予定しています。

(2) 目的

自動走行におけるセキュリティ脅威の調査及び分析を行い、国際標準化も見据えて車両レベル・コンポーネントレベルでのセキュリティ評価手法・プロトコルを策定し、本実証実験を通して募る参加者の車両を用いて対ハッキング性能検証のためのブラックボックステストを行うことで、以下を実現します。

- 車両への通信を用いた攻撃に対する評価手法の確立
- V2X 等車外からの攻撃を含む脅威の全体像の整理
- 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
- 我が国における自動走行車両セキュリティに関わる人材育成及びノウハウ蓄積

2. 調査の成果

(1) 脅威分析調査

① 調査要約

脅威分析調査では、自動走行システムに対するサイバー攻撃の脅威を分析するため、現在から将来にわたる自動走行システムを類型化し、構成要素の調査を行った。調査結果に基づき、サイバー攻撃の事例、将来の環境及び技術の変化動向を踏まえ、自動走行システムの脅威を分類別に洗い出し、全体像の整理を行った。

② 調査結果

脅威分析調査結果については、下記の報告書を参照。

- 脅威分析報告書
- 自動走行システム構成調査表
- 脅威シナリオ一覧

(2) 情報セキュリティ評価ガイドラインドラフトの作成

① 調査要約

ガイドラインドラフトの作成では、ITシステム分野を中心として既存のセキュリティ評価のアプローチを調査した。また、自動車分野で既知のセキュリティ問題事例及びその端緒となった脆弱性やITシステム分野における既知の脆弱性を調査し、それに対する一般的な評価項目について整理した。情報セキュリティ評価のアプローチと整理した一般的な評価項目を踏まえ、無線通信経由での車両に対するサイバー攻撃を想定した場合の、リスクベースアプローチに基づく車両向けガイドラインドラフトを作成した。

② 調査結果

ガイドラインドラフトとして、車両に対するセキュリティ評価全体のアプローチ及び一般的な評価項目を含む包括的ガイドラインの位置づけとしての本編と、技術要素ごとの攻撃手法の詳細と一般的な評価手法を含む実践手引き編を作成した。

結果については、下記を参照。

- 情報セキュリティガイドラインドラフト（本編）
- 情報セキュリティガイドラインドラフト（実践手引き）IPネットワーク編
- 情報セキュリティガイドラインドラフト（実践手引き）Wi-Fi編
- 情報セキュリティガイドラインドラフト（実践手引き）Bluetooth編

（3）情報セキュリティ評価の試行調査

① 調査要約

「（2）情報セキュリティ評価ガイドラインドラフトの作成」で作成したガイドラインドラフトの妥当性を検証するため、評価対象として車両を構成するシステムの準備を行い、ガイドラインドラフトを用いて、情報セキュリティ評価の試行調査を実施した。情報セキュリティ評価の試行調査の結果は、試行調査報告書として取りまとめた。また、試行調査の過程で判明した誤謬については修正するとともに、試行調査から得た業務遂行上のノウハウ等は加筆し、ガイドラインドラフトの品質向上を図った。

② 調査結果

情報セキュリティ評価の試行調査の結果については、下記を参照。

- 情報セキュティ評価試行調査報告書

（4）実証実験の運営準備

① 調査要約

2018年度に実施する実証実験の早期開始の実現を目的として、実証実験開始に必要な計画を立案するとともに、実証実験参加者の募集要領、申請書や規約類、契約書類（秘密保持契約、等）等の作成、及びセキュリティ管理体制の検討等、実証実験の事務局運営のための各種準備を実施した。

② 調査結果

実証実験の運営準備の結果については、下記を参照。

- 実証実験の運営準備検討結果報告書

契約管理番号	１７１０１４２８－０

脅威分析報告書

2018年2月

目次

【活動詳細】	
脅威分析の目的	**3**
目的	4
脅威分析の前提	5
脅威分析のアプローチ	7
自動走行システムのモデル化・構成調査	**8**
車両に対するサイバー攻撃の脅威	9
自動走行システムの脅威分析モデルと調査・整理手順	10
自動走行システムにおいて展開されるサービスの調査結果	11
自動走行システムの機能調査・整理アプローチ	12
自動走行システムの機能調査結果	13
無線通信および車載通信デバイス整理結果	14
脅威の分析	**15**
脅威の分析の進め方	16
分析対象車載通信デバイスの特定	17
脅威シナリオの作成	19
脅威の評価	23
脅威の全体像整理	29
脅威分析結果と対応方針	30
Appendix A 自動走行システムの構成図	31
Appendix B 通信を利用した機能の構成図	36
Appendix C 自動走行システムにおける通信情報の種別	59
Appendix D 脅威の構成要素と活用方針	61
Appendix E 脅威の分類のリファレンス	63
Appendix F STRIDEの網羅感（その他のリファレンスの比較）	67
Appendix G ガイドラインとの連携	70

脅威分析の目的

自動走行システムに対するセキュリティ脅威分析の目的

自動走行システムにおける脅威全体像を見える化し、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図る

- サイバー攻撃の対象となり得る自動走行車両、及び車両と繋がる各種サービス構成の調査を実施し、自動走行システムに対する脅威全体像の整理を行う※
- 自動走行システムに対する脅威全体像を基に、自動走行車両セキュリティの重要性に対する理解を深め、当該テーマに精通する人材育成及びノウハウの蓄積を促進する

※2018年1月時点での公開情報に基づいた調査

【脅威分析の前提】脅威の考え方

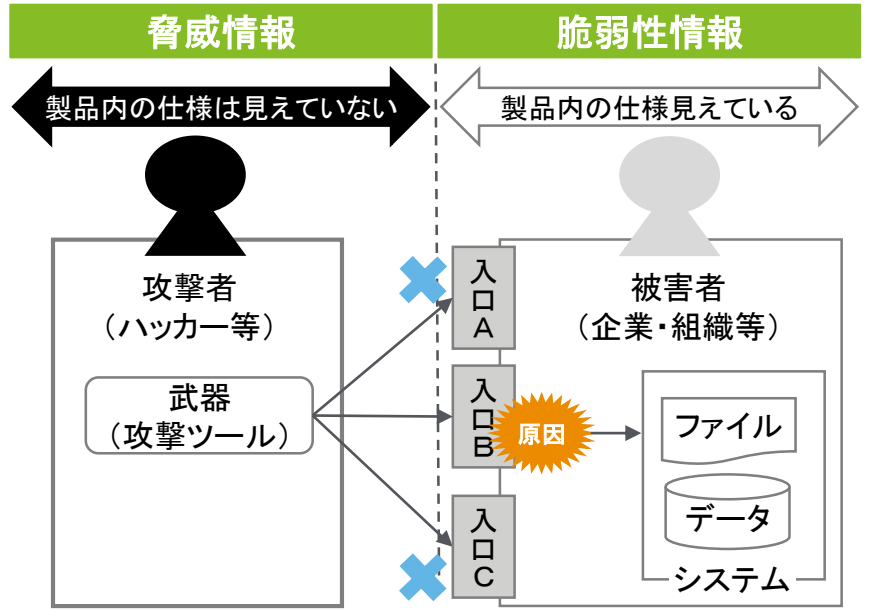
脅威を定義し、脆弱性との違いを明確にすることで分析対象の認識を共有

脅威の定義	具体例
漏えい、改ざん、破壊等の自動車及びその周辺環境に係る情報資産、および安全走行を阻害させうる潜在的な現象	■ 攻撃者のデバイスから攻撃コードを含んだパケットをBluetooth送受信装置に流し込み、リモートキーの操作なしで開錠、施錠が行われる ■ 攻撃者がWi-Fi通信上のパケットを改ざんし、地図上に存在しない経路の情報を含めることで、誤った地図情報を取得させる

脅威情報と脆弱性情報の相違点

	脅威情報	脆弱性情報
情報主体	攻撃者（ハッカー等）	被害者（企業・組織等）
視点	製品内の仕様は見えていない（ブラックボックス）	製品内の仕様が見えている（ホワイトボックス）
機密度	低い（公開情報中心）	高い（営業秘密中心）
記載観点	結果（発生事象）	原因（仕様不具合）
	影響（被害の度合い）	発生可能性（やられやすさ）

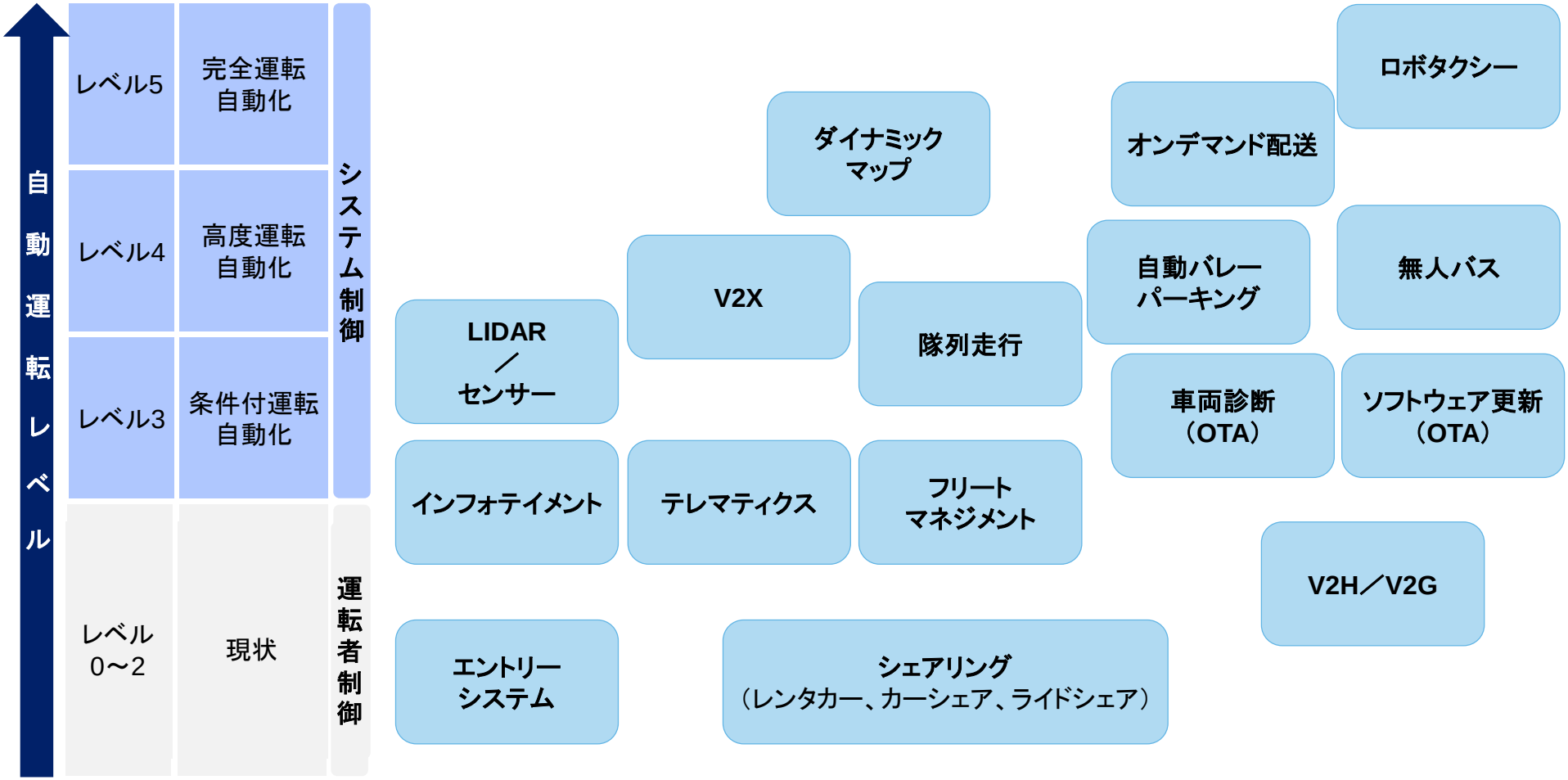
脅威情報と脆弱性情報の関係（図解）



本活動においては、上記の定義を踏まえた脅威の分析を実施

自動走行システムにおいて展開されるサービス（一部機能を含む）

自動走行システムにおけるサービスを網羅的に調査・整理することで、サイバー脅威全体像の導出を実施



SAE J3016 自動運転レベル

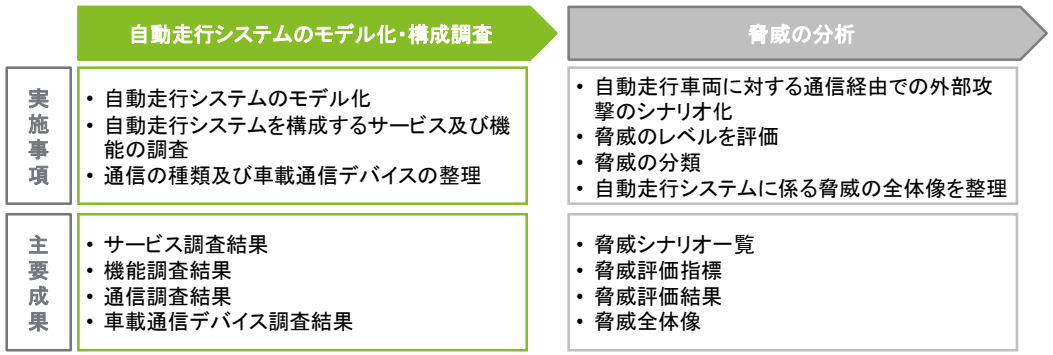
自動走行システムの進化に応じてコモディティ化するサービスや機能

プロジェクトのアプローチ

自動走行システムに対するサイバー脅威の全体像を導出するため、自動走行システムの構成要素を調査し、想定される脅威の分析を実施

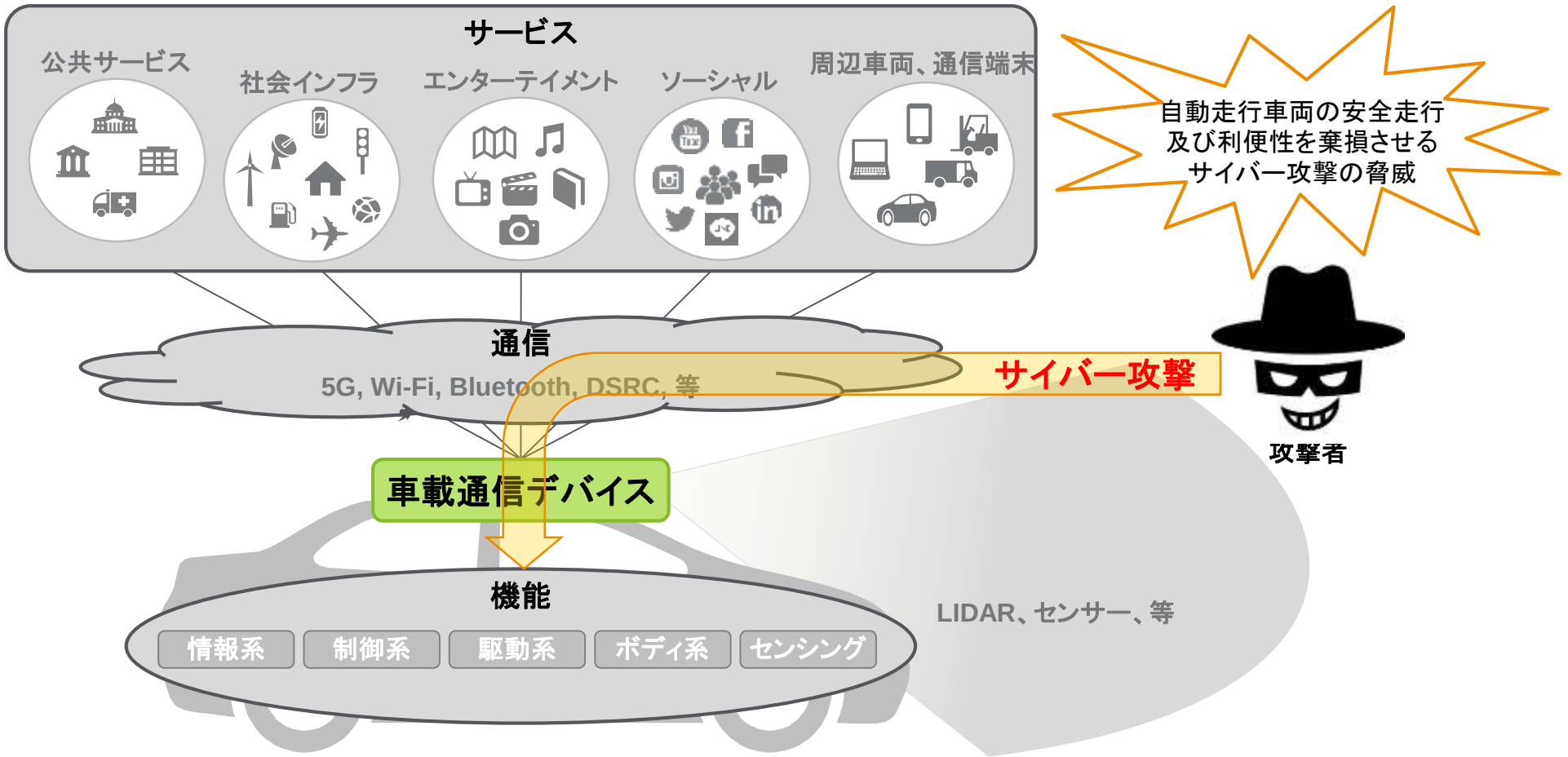
	自動走行システムのモデル化・構成調査	脅威の分析
実施事項	• 自動走行システムのモデル化 • 自動走行システムを構成するサービス及び機能の調査 • 通信の種類及び車載通信デバイスの整理	• 自動走行車両に対する通信経由での外部攻撃のシナリオ化 • 脅威のレベルを評価 • 脅威の分類 • 自動走行システムに係る脅威の全体像を整理
主要成果	• サービス調査結果 • 機能調査結果 • 通信調査結果 • 車載通信デバイス調査結果	• 脅威シナリオ一覧 • 脅威評価指標 • 脅威評価結果 • 脅威全体像

自動走行システムのモデル化・構成調査



車両に対するサイバー攻撃の脅威

車両に対するサイバー攻撃は、「通信」から「車載通信デバイス」を経由して車両に侵入するため、脅威の分析に向けた構成調査では「車載通信デバイス」に重点を置く

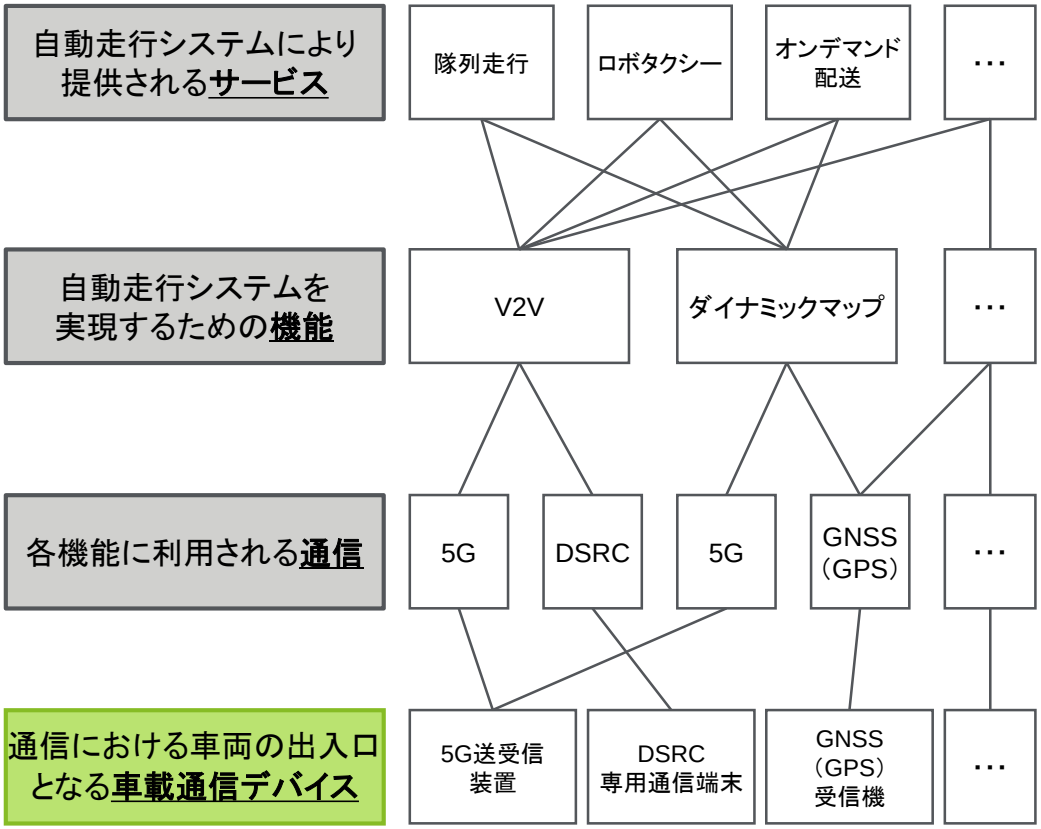


自動走行システムの構成を「脅威分析モデル」として体系化し、
サイバー攻撃の侵入口となる「車載通信デバイス」導出のために必要要素を調査

自動走行システムの脅威分析モデルと調査・整理手順

自動走行システムをモデル化し、各層の構成要素を調査・整理することで、通信における車両の出入り口となる車載通信デバイスを導出

自動走行システムの脅威分析モデルと構成要素



調査・整理手順

1 自動車メーカー・サプライヤー等の取組みや実証実験等を調査する
（スライド11）

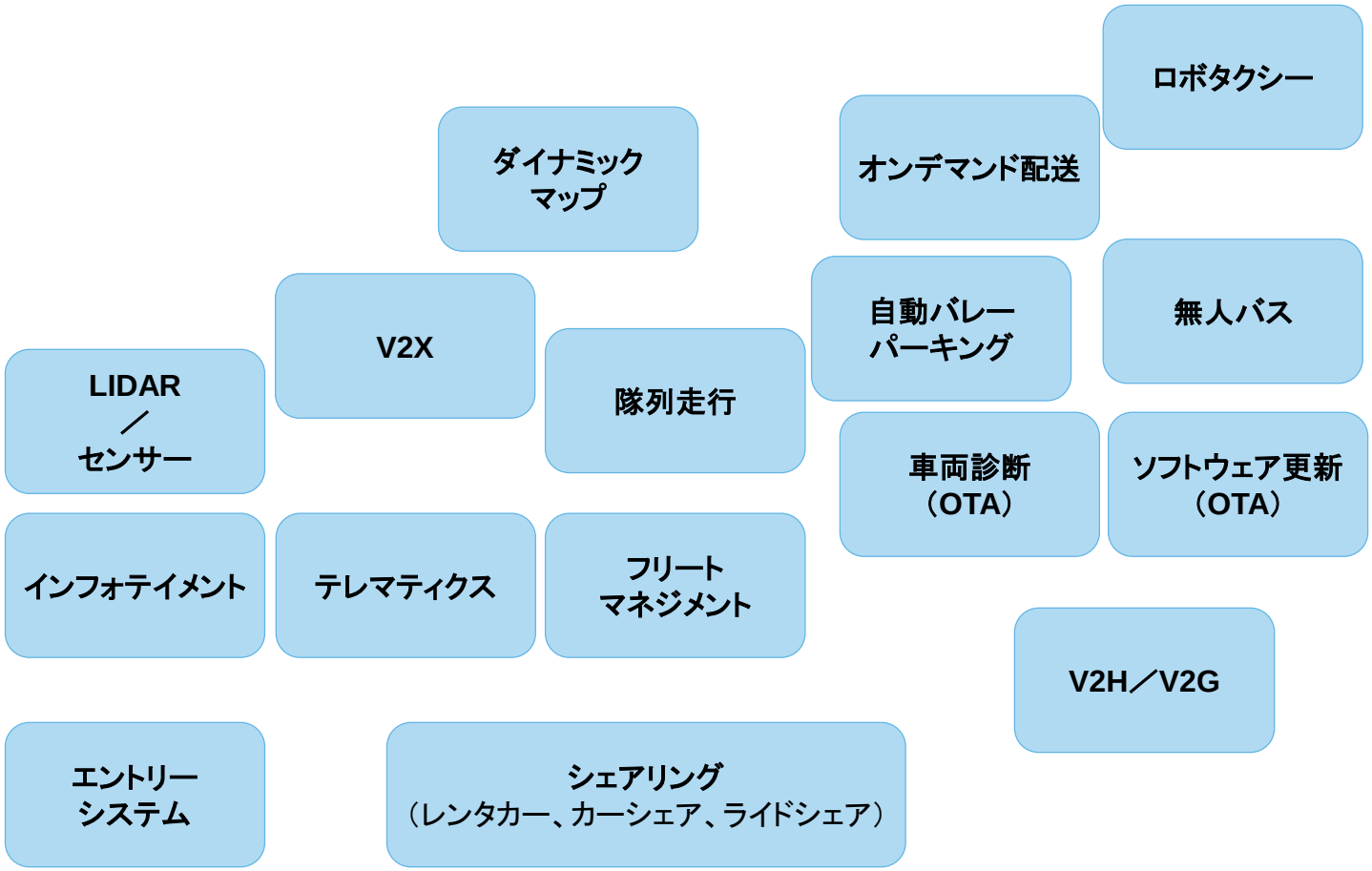
2 各サービスを構成する機能を洗い出す
（スライド13）

3 機能毎に利用される通信が異なるため、それぞれの機能で利用される通信を特定し、車載通信デバイスを整理する
（スライド14）

自動走行システムにおいて展開されるサービスの調査結果（一部機能を含む）

自動走行システムのレベルに応じて、多様なサービスが展開される

再掲



SAE J3016 自動運転レベル

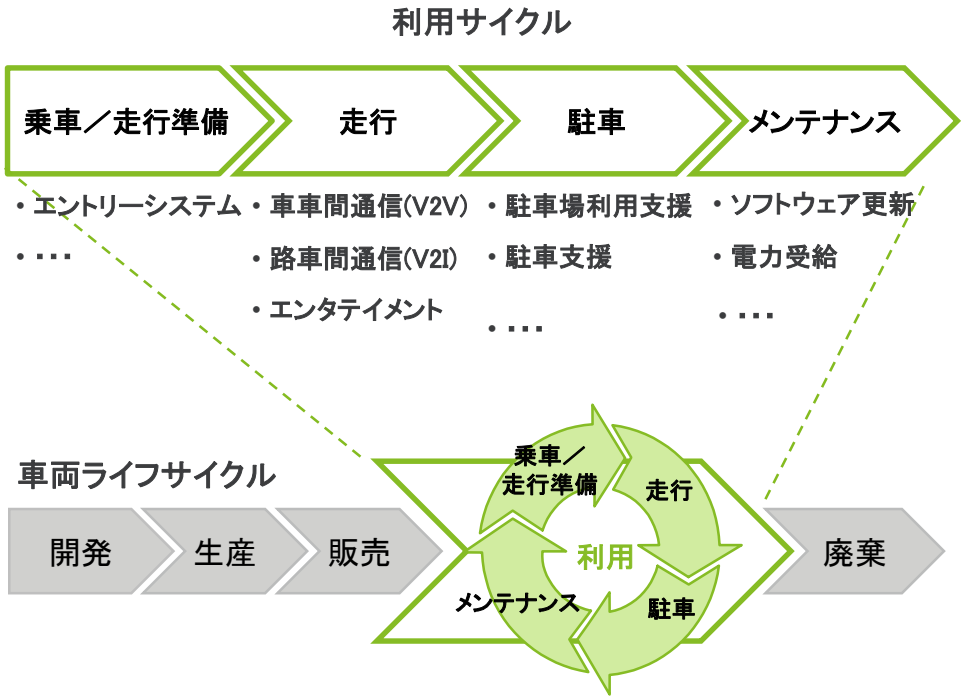
上記自動走行システムのイメージは「Appendix A」参照

自動走行システムの機能調査・整理アプローチ

自動走行システムで提供されるサービスに対応する車両側の必要機能を車両の利用サイクルから導出し、機能実現に必要となる構成要素の調査を実施

2 ①車両の「利用サイクル」毎に機能の洗い出し

機能導出のフレーム



外部からのサイバー攻撃の対象となる【利用】フェーズを対象とする

3 ②各機能毎に構成要素を整理

各機能を実現するための構成要素

通信	各機能で利用される通信
車載通信デバイス	外部との情報連携に利用される、通信上の車両への出入口となる車載通信デバイス
通信上の情報	車両外部のシステム等と連携される情報の種別

＋

通信の構成に加え、各機能が車載機能として実現化される時期、および車両との通信先になる外部システムを整理

アクセス対象	車両とつながる車両外部のデバイス、システム、サーバ、インフラ、等
実用化時期	各機能が車両に実装される時期（見込みを含む）

詳細は別紙1_自動走行システム構成調査表.xlsx」参照

自動走行システムの機能調査結果

自動走行システムに実装される機能を以下の様に集約

機能の詳細は「別紙1_自動走行システム構成調査表.xlsx」参照

自動運転レベル

	乗車／走行準備	走行	駐車	メンテナンス
システム制御		• ダイナミックマップ • V2X（周辺機器との通信） ➢ V2P（車歩行者間通信） ➢ V2I（路車間通信） ➢ V2V（車車間通信） • エンタテイメント ➢ コンシェルジュ ➢ インターネット接続 ➢ POI情報の取得、等 • 車載データの保管・送信 （走行履歴、外部環境、車両状態、等） • 周辺環境の検知 • 緊急通報 • ドライバー監視	• 駐車支援 ➢ 駐車アシスト ➢ リモコン駐車 ➢ 自動駐車 • 駐車場の利用支援 ➢ 空車情報の取得 ➢ 予約 ➢ 決済	• 配車（ロボタクシー等） • 車両管理（OTA） ➢ ソフトウェア／ファームウェア更新 ➢ 車両診断 • V2G（グリッドとの連携） • V2H （ホームシステムとの連携） ➢ 充電・給電 ➢ 家庭内IoT機器との連携 • ナビゲーション （データ更新）
運転者制御	• 目的地の設定 • 持込み機器との連携 ➢ ポータブル機器接続 • エントリーシステム ➢ ドア類の開錠・施錠 ➢ 車両の始動			

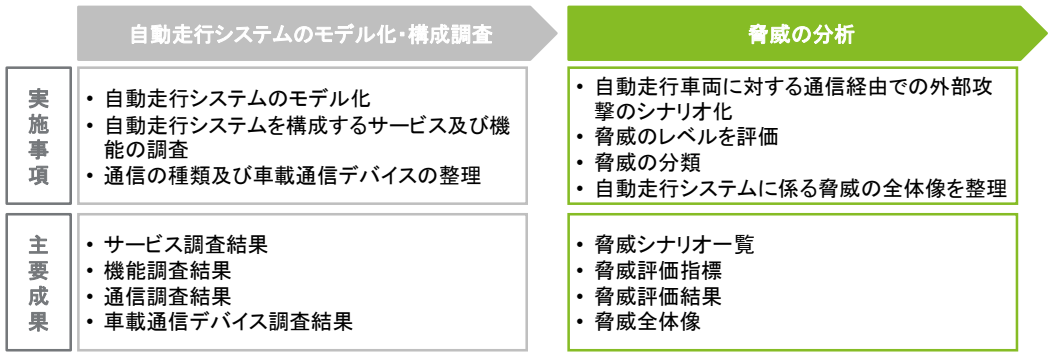
上記機能の構成イメージは「Appendix B」参照

無線通信および車載通信デバイス整理結果

自動走行システムに利用される通信および車載通信デバイスを下表の通り集約

分類	通信の種類	車載通信デバイス	車両からの接続先	主な通信情報（例）
公衆回線	5G	5G送受信装置	周辺車両、携帯事業者の基地局、サービス事業者のサーバ	走行制御情報、ダイナミックマップ情報等
	3G/4G	3G/4G送受信装置	携帯事業者の基地局、サービス事業者のサーバ	ソフトウェア更新情報、交通情報、趣味・嗜好に関する情報（インフォテイメント）
Wi-Fi	Wi-Fi	Wi-Fi送受信機	Wi-Fiアクセスポイント、サービス事業者のサーバ	ソフトウェア管理情報、車両位置情報、交通情報、趣味・嗜好に関する情報
V2X通信	Cellular V2X	Cellular V2X送受信装置	周辺車両、インフラ等	交通情報、走行制御情報等
	DSRC	DSRC通信端末（V2X）	周辺車両、インフラ等	
デバイス間連携	Bluetooth（VCK、ポータブル機器用）	Bluetooth送受信装置	スマートフォン、ポータブル機器等	エントリーシステムに用いる認証情報、ポータブル機器との連携情報等
	Bluetooth（OBD-II用）	OBD-II／ドングル	Wi-Fiアクセスポイント、サービス事業者のサーバ	ソフトウェア管理情報、診断情報
	ZigBee	ZigBee無線モジュール	社会インフラの電力網、住宅	ボディ制御情報
センシング	ミリ波レーダ(77／79GHz)	ミリ波レーダ送受信装置	周辺車両、歩行者、障害物	走行制御情報
	準ミリ波レーダ			
	LIDAR	LIDAR送受信装置		
	超音波センサー	超音波センサー送受信装置		
	生体認証センサー	生体認証センサー	搭乗者（指紋、虹彩、表情など）	生体情報
衛星通信	GNSS(GPS)	GNSS（GPS）受信機	GPS衛星	車両位置情報
情報提供（VICS等）	準マイクロ波	準マイクロ波端子	路側機（電波ビーコン）	交通情報（渋滞、事故等）
	赤外線	赤外線端子	路側機（光ビーコン）	
	DSRC	DSRC通信端末（VICS/ETC）	路側機（電波ビーコン）、周辺車両	交通情報、走行制御情報、資産情報
エントリーシステム	NFC	NFCリーダ・ライタ端末	非接触ICカード、スマートフォン	資産情報
	RF/LF (RFID)	RF/LF (RFID)リーダ・ライタ	リモートキー（キーフォブ）	ボディ制御情報

脅威の分析


自動走行システムのモデル化・構成調査
脅威の分析
実施事項
• 自動走行システムのモデル化
• 自動走行システムを構成するサービス及び機能の調査
• 通信の種類及び車載通信デバイスの整理
• 自動走行車両に対する通信経由での外部攻撃のシナリオ化
• 脅威のレベルを評価
• 脅威の分類
• 自動走行システムに係る脅威の全体像を整理
主要成果
• サービス調査結果
• 機能調査結果
• 通信調査結果
• 車載通信デバイス調査結果
• 脅威シナリオ一覧
• 脅威評価指標
• 脅威評価結果
• 脅威全体像

脅威の分析の進め方

分析対象車載 通信デバイスの特定	脅威シナリオの作成	脅威の評価	脅威の全体像整理
• 脅威分析の対象とする車載通信デバイスの優先度付け ➢ 車両外部のシステムやインフラとの通信を行う車載通信デバイスを特定 ➢ 各デバイスに利用される通信情報および実用化時期から、重要度を評価	• 重要度の高い車載通信デバイスを対象に、STRIDEを採用し脅威を整理 • 脅威シナリオを具体的に示すため「事象」と「影響」の構造でシナリオを作成	• 脅威シナリオを「顕在化率」と「影響度」の観点で評価し、脅威レベルを判定 • 評価結果をヒートマップを用いて分析	• 自動走行にかかる車載通信デバイス、およびデバイスごとの脅威の傾向（STRIDE）を鳥瞰的に把握出来るように整理
スライド 17～18	スライド 19～22	スライド 23～28	スライド 29

自動走行システムの構成調査結果を基に、脅威の分析を実施

車載通信デバイスの評価方法

車載通信デバイスの重要度を判断し、脅威分析の優先度を特定

【通信情報の種別】の詳細は「Appendix C」参照

考え方
- サイバー攻撃の対象となりうる、**通信に用いられる車載通信デバイス**を対象とする
- 機能の**実用化時期**が早く、**自動走行に必要となる情報の通信に用いられる車載通信デバイス**を重要と考える

デバイスの特定

選定条件
構造化されたルール（プロトコル）に基づく 無線通信を行う車載通信デバイス

○ → 重要度評価へ

× → 評価対象外

デバイスの重要度の評価

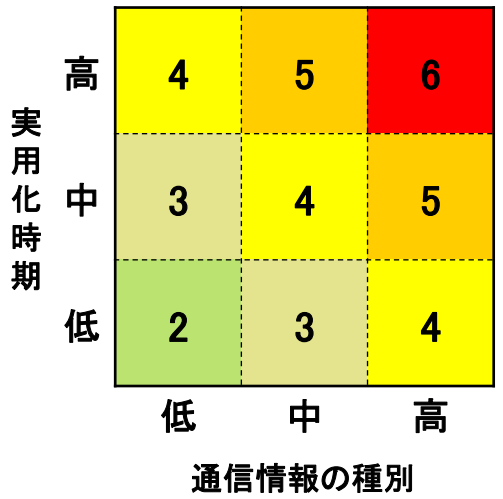
■ 自動走行に必要な機能に関する情報を取り扱うデバイスを優先する

スコア	【指標①】 通信情報の種別	
高（3）	走行制御情報	走る、曲がる、止まるに必要となる情報、およびECU等のソフトウェア管理情報
中（2）	走行サポート情報	位置情報、地図データ、等
	車両管理情報	車載データ、車載機器の消耗度、等
低（1）	周辺環境情報	個人情報および走行に影響を与えない情報

■ 実用化時期の早い機能を優先する

スコア	【指標②】 機能の実用化時期	
高（3）	実用化済	現在車両に搭載している機能
中（2）	～2020年	2020年を目途に実用化予定
低（1）	2020年以降	2020年以降に実用化予定

【指標①】と【指標②】のスコアを合計し、重要度を評価



重要度評価結果

前項の評価方法を用いて、脅威シナリオ作成の対象となるデバイスを特定

各デバイスの評価結果は
「別紙1_自動走行システム構成調査表.xlsx」参照

重要度	デバイス	主な機能
6	3G/4G送受信装置	ファームウェア／ソフトウェア更新、車両診断、地図情報の更新、等
	Wi-Fi送受信機	ファームウェア／ソフトウェア更新、等
	Bluetooth送受信装置（OBD-IIポート用）	ドア開閉、機器連携、等
5	5G送受信装置	ダイナミックマップ、等
	Cellular V2X送受信装置	周辺車両、インフラとの通信、等
	DSRC通信端末（V2X）	
	Bluetooth送受信装置（VCK、ポータブル機器用）	ドア開閉、機器連携、等
	GNSS（GPS）受信機	位置情報の取得、等
	準マイクロ波端子	道路交通情報の連携、等
	赤外線端子	
	DSRC通信端末（VICS/ETC）	信号、周辺車両との通信、ETC、等
	NFCリーダ・ライタ端末	ドア開閉、料金支払い、等
	RF/LF (RFID)リーダ・ライタ	ドア開閉、車両の始動、等

脅威分析対象とする車載通信デバイス

重要度	デバイス	主な機能
4	生体認証センサー	ドア開閉、ドライバー監視
3	ZigBee無線モジュール	充電システムとの充電状態の連携
2	該当なし	—

評価対象外

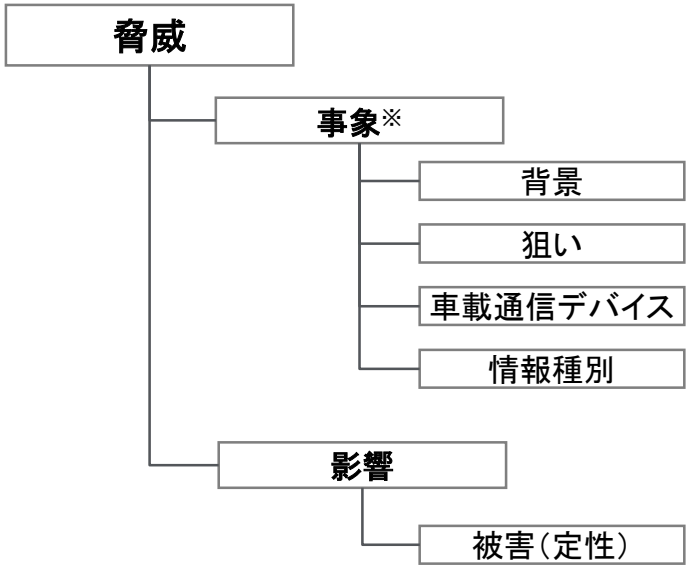
デバイス	理由
ミリ波レーダ送受信装置	前スライドの「車載通信デバイスの特定」にて除外
超音波センサー送受信装置	
LIDAR送受信装置	
充電／給電コネクタ	
近赤外線カメラ	
遠赤外線カメラ	
単眼カメラ	
ステレオカメラ	
USB	
FM多重アンテナ	
CD-R／DVD-Rドライブ	
TPMS	Bluetooth等を利用しており、外部との通信は発生しないため除外

自動走行車両への影響が考えられる、重要度「5」以上のデバイスを対象に脅威シナリオを作成し、脅威を分析

脅威シナリオの構造

わかりやすさを重視し、「事象」と「影響」の構造で脅威シナリオを整理

前提	■ 重要度評価結果に基づき、車載通信デバイス毎に脅威シナリオを作成 ■ 脅威シナリオは、解釈にバラツキが生じないように、構造上のルールを統一 ■ 以下のルールに沿って、以降の脅威シナリオの作成、評価、整理に至る一連の作業を推進



脅威シナリオの考え方

- ◆ 攻撃の背景・狙い、及び関係する情報種別等を明確にする
- ◆ 当該デバイス単位で、どのようなセキュリティ侵害（漏えい・改ざん等）が発生するかを、「事象」（何が起きて）と「影響」（どうなるか）の一連の流れのシナリオで表現する
- ◆ 専門的な表現は必要最低限に控え、多くの人がイメージできるように表現する
- ◆ 事象の結果起こり得る影響を、定性的なストーリーで整理することで、具体性を補強する

※一部の要素を抜粋、脅威の全体構成は「Appendix D」参照

脅威シナリオ例 Tampering （改ざん）	【事象】 Bluetoothを利用した車両とスマホ間で授受される認証情報（VCK：ヴァーチャル・カー・キー）をランサムウェアで暗号化される 【影響】 車両の利用が出来なくなり、金銭が要求される

脅威シナリオ作成の考え方

「既知」の脅威は公開情報を基に、「未知」の脅威は技術や環境の変化に着目し、脅威シナリオを作成

脅威シナリオ作成のポイント	
「既知」の脅威	公開された攻撃事例、研究報告等から、車両を含む自動走行システムへの応用を検討
「未知」の脅威	「現状」から「将来」への変化を実現するための技術や環境の「変化ドライバ」に着目 ※ 現状の自動車に利用されていない技術（5G, Cellular V2X等）を利用する攻撃は、「未知の脅威」とする

※ 作成する脅威シナリオは、上記のポイントを踏まえた想定であり、顕在化には一定の条件（バグ、攻撃者のスキル等）が必要

未知の脅威を導出するための着眼点

「現状」から「将来」へ移行するために必要な要素となる技術や環境の変化ドライバに注目する

周辺インフラ／環境の変化

変化ドライバ

- 次世代通信技術の実用化
  - 通信速度の向上
  - 通信データの大容量化
  - リアルタイム性の向上
  - 周辺インフラやサービス事業者との双方向通信

自動車の変化

変化ドライバ

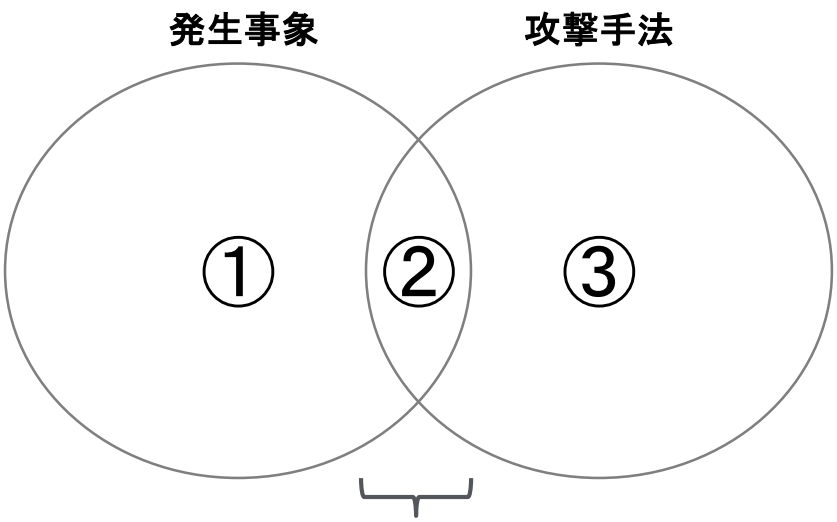
- 車載機器の機能拡張
  - データ保存容量の増加
  - ネットワーク帯域の拡大
  - 処理性能の向上
- 他業界で利用している技術の応用

脅威シナリオの分類

分析対象となる車載デバイスに対する重要な脅威の抜け漏れを防ぐため、STRIDEの軸で脅威シナリオを作成

前提	■ 車載通信デバイス毎に、STRIDEの単位で脅威シナリオを作成 ■ わかりやすさを考慮し、発生事象（何が起こるか）に着目して脅威を分類 ■ セキュリティに関する各種リファレンスを参考にし、脅威の分類の網羅性を確認

脅威の分類に言及するリファレンスは、概ね「発生事象」と「攻撃方法」の2つの視点による整理に大別される



「発生事象」と「攻撃手法」の両面をかねる

	リファレンス	脅威の分類例※
①	STRIDE	• なりすまし • 改ざん • 情報漏えい
①	ENISA	• 人的ミスによる情報の漏えい／拡散 • 第三者に起因する損害 • 機密情報の紛失
②	NIST SP800	• 機微な情報を漏らすことによって、正規の権限によらない開示および／または利用不能を引き起こす
③	CAPEC	• 既存機能の不正利用 • アクセスコントロールの悪用 • システムリソースの不正操作
③	OWASP	• タイム・ボム（潜伏型攻撃） • ウィルス • ボット

ベース

※ その他の脅威の分類は「Appendix E」参照

STRIDEをベースに、その他のリファレンスも活用し、脅威分類に漏れがないことを担保（Appendix F 参照）

STRIDE別の脅威シナリオ例

脅威のバラツキや不足等が生じないように、STRIDEを軸に「事象」と「影響」の構造で77シナリオを作成

詳細は「別紙2_脅威シナリオ一覧.xlsx 」参照

脅威分類	脅威シナリオの例示
Spoofing （なりすまし）	【事象】 車両とGNSS(GPS) 衛星の通信を妨害し、偽装した電波を流し込むことで、攻撃者がGPS衛星になりすます 【影響】 位置情報取得が利用できず、車両の目的地や経路が決定できない
Tampering （改ざん）	【事象】 遠隔から通信上のソフトウェア更新情報を改ざんし、走行制御に関するソフトウェアを異常な状態とする 【影響】 攻撃者の意図に従って走行中に異常な走行機能制限が発生し、安全走行に支障が生じる
Repudiation （否認）	【事象】 車載ETC機と料金所ETCシステム間の通信を否認し、通行料の支払いを拒否する 【影響】 詐欺行為による経済的損失が発生する
Information Disclosure （情報漏えい）	【事象】 攻撃対象の車両に接近し、ホットスポットやフリーWi-Fiを模したアクセスポイントを提供し、これに接続した車両からのWi-Fi通信上の情報を窃取する 【影響】 車両の目的地や経路、ユーザーIDやパスワード等が漏えいする
Denial of Service （サービス妨害）	【事象】 特定車両に対して大量のパケットを送信し、テレマティックスサービスを停止させる 【影響】 車両の通信機能が停止し、通信機能を用いるすべてのサービスが提供できなくなる
Elevation of Privilege （権限の昇格）	【事象】 遠隔から不正なコードや命令を流し込み、4G送受信装置の管理者権限を奪取し、これを踏み台にして車載ネットワークで接続されている他のデバイスにアクセスする 【影響】 4G送受信装置以外のデバイスや機能が攻撃者に利用されることで、攻撃者の意図に従って事故回避行動を誤作動させられ、安全走行に支障が生じる

脅威レベルの評価指標

シナリオ化した脅威を、「顕在化率」と「影響度」から脅威レベルを評価

評価の考え方	脅威が顕在化する可能性と、顕在化時の影響度を数値化し、各脅威の「脅威レベル」を評価

顕在化率

各車両の特性・構成に依らず、攻撃者から見ていかに攻撃が**成功しやすいか**を各観点別に分析し、総合的に評価

観点		評価方法
①	容易性	攻撃を成功させるための容易度
②	機器・ツール	特殊なツールや機器の必要性
③	準備期間	攻撃を行うための準備期間（潜伏等）
④	実行人数	攻撃を行うために必要となる人数
⑤	運行状態	攻撃対象車両の状態（走行中／駐停車中）

影響度

脅威が生じた車両や周辺環境への**安全面での影響**の度合いを総合的に評価

観点		評価方法
①	機能欠損の度合い	走行（走る、曲がる、止まる）に影響
②	被害の程度	乗車者に安全面での影響
③	被害の範囲	脅威が生じた車両周辺のインフラ、車両、歩行者に対する影響

各観点の具体的な評価方法は次項にて説明

「顕在化率」の判定

脅威の顕在化率を5つの観点から判定

考え方	車両の特性・構成に依らず、攻撃者から見ていかに攻撃が**成功しやすいか**を各観点別に分析し、総合的に評価

観点		評価
①	容易性	○：攻撃目的の達成に、無線ネットワークから車両内部への侵入は不要 ×：攻撃目的の達成に、無線ネットワークから車両内部への侵入が必要
②	機器・ツール	○：汎用的なPC等のデバイスを利用 ×：特殊な機器・ツールを利用
③	準備期間	○：攻撃が即時で実施可能 ×：攻撃を行うためには準備期間が必要（潜伏、乗っ取り、等）
④	実行人数	○：単独で実施可能 ×：複数人での組織的な体制が必要
⑤	運行状態	○：駐停車中の車両に対する攻撃 ×：走行中の車両に対する攻撃

○：攻撃の難易度が低い　×：攻撃の難易度が高い

判定基準

顕在化率	○がついた観点の数	評価結果 ①	②	③	④	⑤
高（3）	5	○	○	○	○	○
	4	○	○	○	○	×
		○	○	×	○	○
		・・・（省略）・・・				
中（2）	3	×	○	○	○	×
		○	×	○	○	×
		・・・（省略）・・・				
	2	×	×	○	○	×
		○	×	○	×	×
		・・・（省略）・・・				
低（1）	1	○	×	×	×	×
		×	×	×	○	×
		・・・（省略）・・・				

「影響度」の判定

脅威の影響度を3つの観点から判定

考え方	脅威が生じた**車両や周辺環境への安全面での影響の度合い**を総合的に評価 ※影響度の評価においては、被害の連鎖（二次被害、三次被害）については想定しない

観点		評価
①	機能欠損の度合い	○：走行（走る、曲がる、止まる）に影響 ×：走行への影響なし
②	被害の程度	○：乗車者の安全に影響 ×：安全面以外の影響
③	被害の範囲（周辺環境）	○：脅威が生じた車両周辺のインフラ歩行者に対する影響 ×：攻撃対象となる車両のみ影響（周辺環境の安全面に影響なし）

○：安全面での影響が高い　×：安全面での影響が低い

判定基準

影響度	○がついた観点の数	評価結果 ①	②	③
高（3）	3	○	○	○
中（2）	2	○	○	×
		○	×	○
		×	○	○
低（1）	1	○	×	×
		×	○	×
		×	×	○
	0※	×	×	×

※「該当する観点の数」が「0」になる場合、安全走行への影響は発生しないが、利便性の棄損や情報漏えい等が発生する

脅威レベルの算出

「顕在化率」と「影響度」の評価結果より、「脅威レベル」を特定

考え方	「顕在化」と「影響度」を合計し、その数値を脅威レベルとして評価

影響度＼顕在化率	1	2	3
3	4	5	6
2	3	4	5
1	2	3	4

脅威レベル	
高	6
	5
	4
	3
低	2

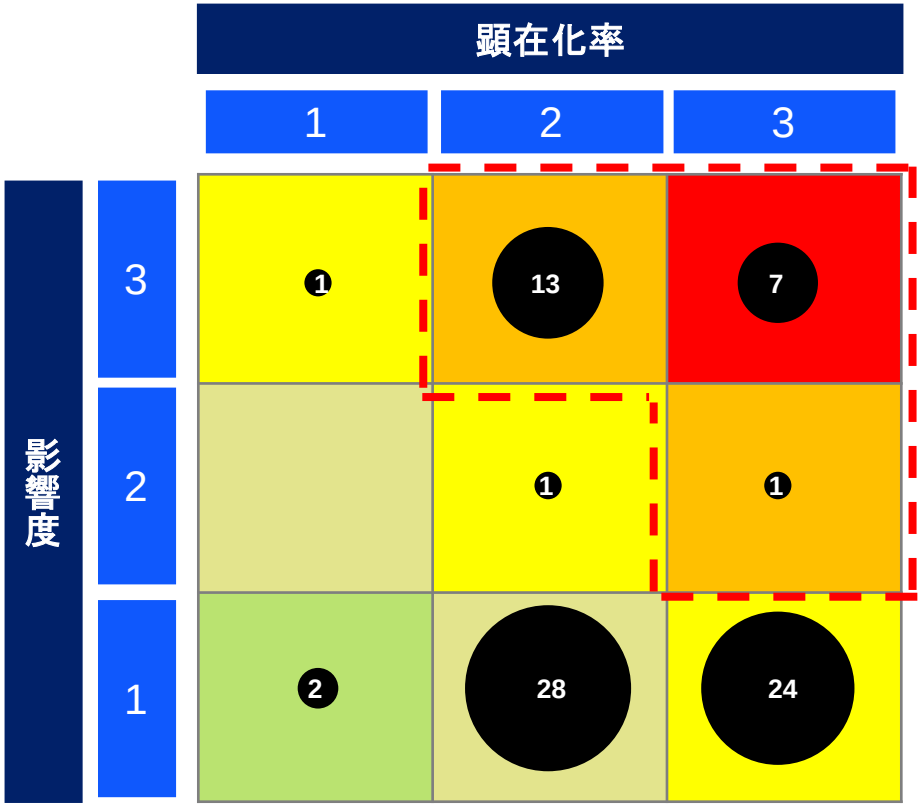
上記の評価結果に基づき、脅威の傾向を分析

脅威シナリオの評価結果

脅威シナリオに対する評価を行い、重要脅威の特徴を分析

円内の数字は該当するシナリオ数（全77シナリオ）

詳細は「別紙2_脅威シナリオ一覧.xlsx」参照



脅威レベル5, 6（枠線部分）を最重要と位置付ける

最重要の脅威の特徴

- **セキュリティの侵害からセーフティへの影響（人命に関わる被害）が発生し得る**
- **さらに、攻撃対象車両のみならず、周辺環境への影響が発生する**
  - 走行制御情報や車両管理情報に利用される通信および車載通信デバイス経由の脅威が高レベルになる傾向にある
  - 自動走行車両の通信の多くは既存のネットワークを用いるため、既存のツールの利用、遠隔からの攻撃による脅威が高まる

最重要の脅威に関しては、ペネトレーションテストを含む多面的な視点で対応を講じる必要がある

脅威シナリオ

脅威レベルが「6」となる脅威

既知の脅威

詳細は「別紙2_脅威シナリオ一覧.xlsx 」参照

No.	デバイス	情報種別	機能	狙い	脅威			
					サービスの前提、実装機能等	分類	事象	影響
1	4G 送受信装置	走行制御情報 ／ 車両管理情報	車両管理（OTA） － ソフトウェア更新（自動）	安全走行の妨害	車載機器のソフトウェア更新情報を外部システムから取得する ソフトウェア更新には走行制御に関する機能も更新される	Spoofing （なりすまし）	遠隔から外部システムになりすまし、虚偽のソフトウェア更新情報を流し込むことで、走行開始後にソフトウェアを異常な状態とする	攻撃者の意図に従って走行中に異常な走行機能制限が発生し、安全走行に支障が生じる
2	4G 送受信装置	走行制御情報 ／ 車両管理情報	車両管理（OTA） － ソフトウェア更新（自動）	安全走行の妨害	車載機器のソフトウェア更新情報を外部システムから取得する ソフトウェア更新には走行制御に関する機能も更新される	Tampering （改ざん）	遠隔から通信上のソフトウェア更新情報を改ざんし、走行制御に関するソフトウェアを異常な状態とする	攻撃者の意図に従って走行中に異常な走行機能制限が発生し、安全走行に支障が生じる
3	Wi-Fi 送受信機	走行制御情報	ダイナミックマップ － 地図情報の取得	交通事故の誘発	ダイナミックマップの利用開始時、走行開始時点の地図情報をWi-Fi通信を用いてダウンロードする	Tampering （改ざん）	遠隔から通信中のダイナミックマップ情報を改ざんし、虚偽のマップデータを流し込む	通行不可能な地帯を車道と認識させられることで危険走行を行い、事故が発生する
4	Bluetooth （OBD-II用）	走行制御情報	車両管理（OTA） －車両診断	安全走行の妨害	車両の診断やソフトウェア更新用のツールでOBD-IIポート／ドングルに接続すると、送信側が制御用のコマンドを実行できる	Spoofing （なりすまし）	通信中のOBDⅡポート／ドングルへ接続し、正規利用になりすまして不正なコードを流し込み、正規の方法以外で車両を制御する	攻撃者の意図に従って事故回避行動を誤作動させられ、安全走行に支障が生じる
5	Bluetooth （OBD-II用）	車両管理情報	車両管理（OTA） －車両診断	安全走行の妨害	車両の診断やソフトウェア更新用のツールでOBD-IIポート／ドングルに接続すると、送信側が制御用のコマンドを実行できる	Tampering （改ざん）	通信中のOBDⅡポート／ドングルへ接続し、通信中の情報を改ざんして不正なコードを流し込み、走行に用いる制御を停止する	攻撃者の意図に従って事故回避行動を誤作動させられ、安全走行に支障が生じる
6	Bluetooth （OBD-II用）	周辺環境情報	車両管理（OTA） － ソフトウェア更新	安全走行の妨害	車両の診断やソフトウェア更新用のツールでOBD-IIポート／ドングルに接続すると、送信側が制御用のコマンドを実行できる	Denial of Service （サービス妨害）	通信中のOBDⅡポート／ドングルへ接続して不正なコードを大量に流し込み、走行に用いる制御を停止する	車両内のソフトウェアに深刻なバグを残したまま走行を行うことで、事故回避行動が失敗する

未知の脅威

No.	デバイス	情報種別	機能	狙い	脅威				
					サービスの前提、実装機能等	分類	変化ドライバ	事象	影響
7	5G 送受信装置	走行制御情報	V2X（Vehicle-to-Everything） 周辺環境との通信 － 3D地図のリアルタイム・ダウンロード	安全走行の妨害	5G通信を利用し、3D地図を逐次ダウンロードして、これを自動運転に活用する	Tampering （改ざん）	【変化ドライバ】 5Gネットワークが実現し、自動運転に利用できるレベルの高信頼性、広帯域幅、充分なエリア・カバレッジが実現する － 5Gネットワークを利用した3D地図の配信が実用化された結果、自動運転に占める5G通信の重要性が拡大し、攻撃者の標的となる	車両と基地局間の通信に割り込み、位置情報や3D地図情報を改ざんして、サーバーや車両に送信する	自動運転機能や運転補助機能が正常に動作せず、当該車両および周辺車両、周辺歩行者などの安全が妨害される

脅威の全体像整理

脅威の「顕在化率」と、安全走行への「影響度」で算出した脅威の傾向

【表中のスコア】各車載通信デバイスにおけるSTRIDE別の脅威レベル平均値。脅威レベルの算出方法はスライド23～27参照　「— 」: 該当シナリオなし

通信カテゴリ	車載通信デバイス	脅威の分類					
		Spoofing（なりすまし）	Tampering（改ざん）	Repudiation（否認）	Information Disclosure（情報漏えい）	Denial of Service（サービス妨害）	Elevation of Privilege（権限の昇格）
公衆回線	5G送受信装置	5	6	4	4	5	5
	3G/4G送受信装置※	5	6	4	3	4	5
Wi-Fi	Wi-Fi送受信装置	5	4.5	—	4	4	5
V2X通信	Cellular V2X送受信装置	5	5	3	4	5	4
	DSRC通信端末（V2X）	5	5	5	3	5	3
デバイス間連携	Bluetooth送受信装置（VCK、ポータブル機器用）	4	3	4	4	4	3
	Bluetooth送受信装置（OBD-II用）	6	4.5	—	4	6	5
衛星通信	GNSS（GPS）受信機	4	4	—	—	4	—
情報提供（VICS等）	準マイクロ波端子	3.5	3	—	—	3	—
	赤外線端子	3	4	—	—	3	—
	DSRC通信端末（VICS/ETC）	3	2	2	3	3	—
エントリーシステム	NFCリーダ・ライタ端末	3	4	4	4	4	4
	RF/LF (RFID)リーダ・ライタ	4	3	—	3	3.5	—

※脅威シナリオは3G, 4Gそれぞれで作成しているため、脅威レベルの高いスコアを採用

分析の結果、安全走行に影響する情報の通信に用いられる、車載通信デバイスへの脅威が大きい傾向にある

脅威分析結果と対応方針

脅威分析結果のセキュリティガイドラインへの反映

脅威分析結果	下記の車載通信デバイスに対するサイバー攻撃が、自動走行システムに大きな影響を与える

脅威レベルの高い車載通信デバイス		セキュリティガイドラインでの評価対象
公衆回線	5G送受信装置	➢ 情報セキュリティ評価ガイドラインドラフト（実践手引き）IPネットワーク編 ➢ 情報セキュリティ評価ガイドラインドラフト（実践手引き）Wi-Fiネットワーク編 ➢ 情報セキュリティ評価ガイドラインドラフト（実践手引き）Bluetooth編
	3G/4G送受信装置	
Wi-Fi	Wi-Fi送受信装置	
デバイス間連携	Bluetooth送受信装置	
V2X通信	Cellular V2X送受信装置	V2X通信は、将来の実用化に向けた実証実験段階であり、仕様も確定していないため（2018年1月時点）、今後の検討事項とする
	DSRC専用通信端末	

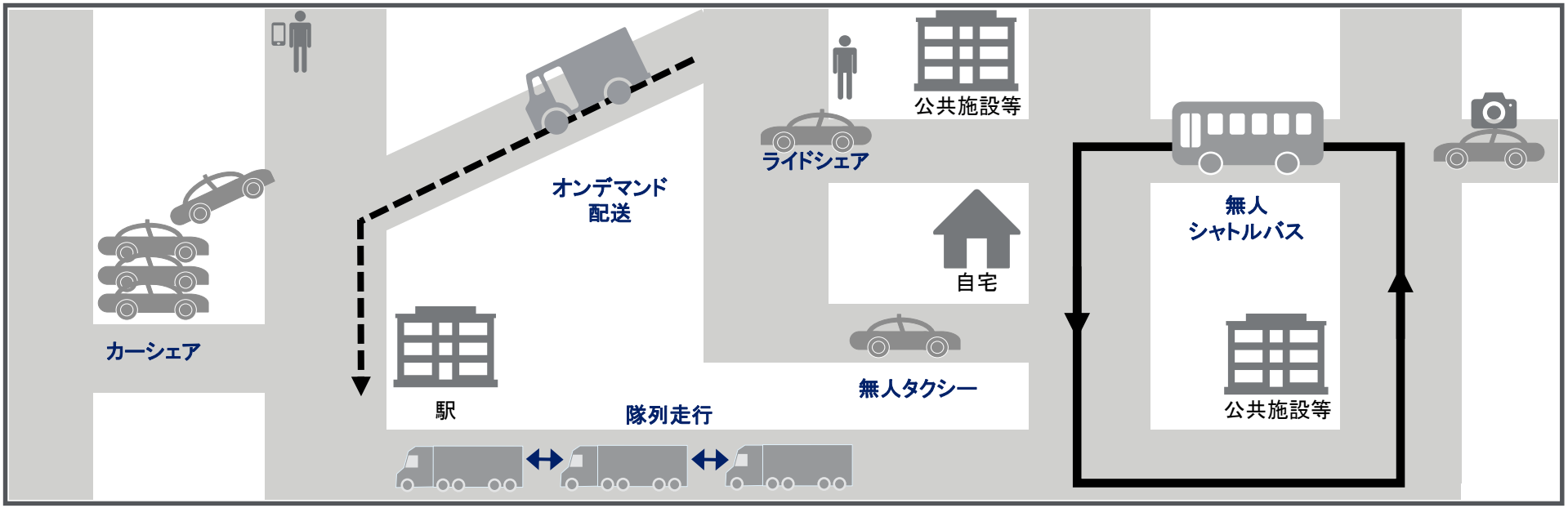
自動走行システムに対するサイバー脅威のレベルが高く、コモディティ化されているネットワークを利用する車載通信デバイスを対象にセキュリティガイドラインを策定

【Appendix A】

自動走行システムの構成図

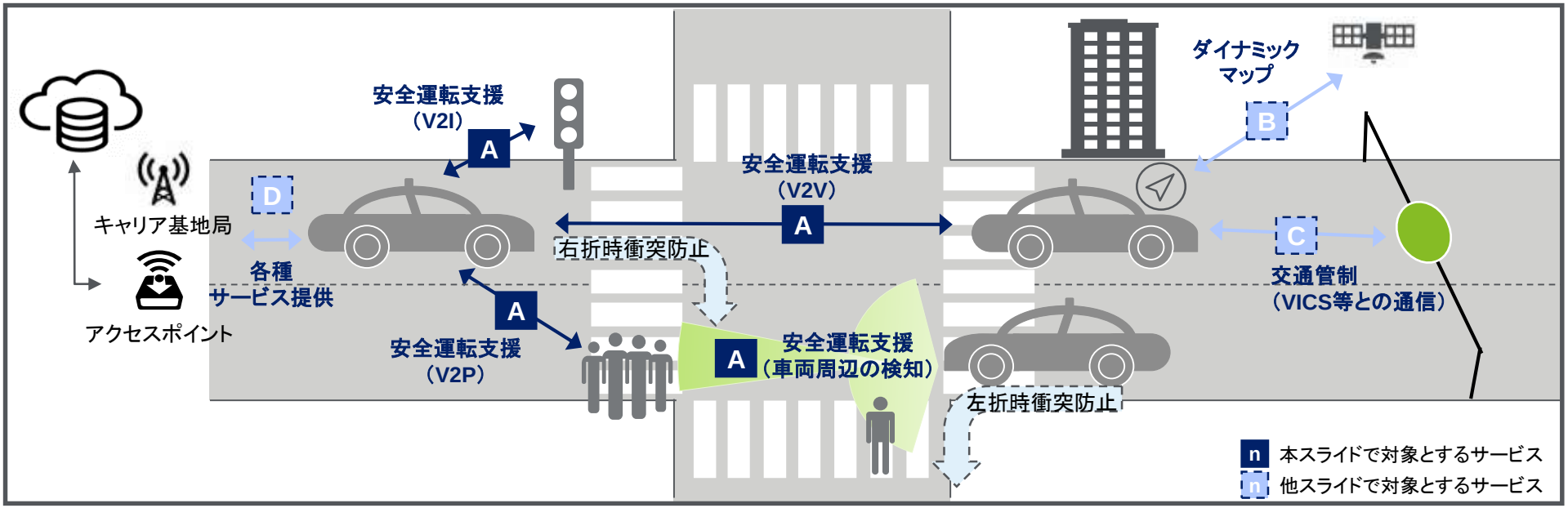
事業者等による自動走行の取組み状況 1/4
≪自動走行のサービス≫

【Appendix A】



サービス	取組み内容	実装化時期	代表的な事業者等
カーシェア	自動運転車両が指定した場所まで迎えに来て、目的地まで運ぶという自動運転型カーシェアリングを提供	サービス展開済み	レンタカー会社、アプリケーション開発事業者 自動車メーカー、ITベンチャー、等
ライドシェア	モバイルアプリ等を通じて配車を依頼することで端末のGPS機能を通じて、自動車の所有者・運転者と同乗希望者を結びつけるプラットフォームを提供		
無人タクシー・バス	自動運転車両により、利用者ニーズ等に応じたデマンド交通、巡回バスなどの交通サービスを提供	2025年以降 （一部サービスは2020年以降）	自動車メーカー、タクシー会社、 ロボットベンチャー、ITベンダー、等
オンデマンド配送	自動運転車両により、顧客が望む時間帯・場所で荷物を受け取れるオンデマンド配送サービスを提供		自動車メーカー、運送／宅配事業者、等
隊列走行	自動走行機能を持った複数の商用車等が適切な車間距離を保ちながら連続走行を行うことで、輸送効率の向上、業務交通量の低減、輸送の安全性向上を図る	高速道路： 2020年（レベル3） 2025年（レベル4）	自動車メーカー、運送／宅配事業者、 通信事業者、等

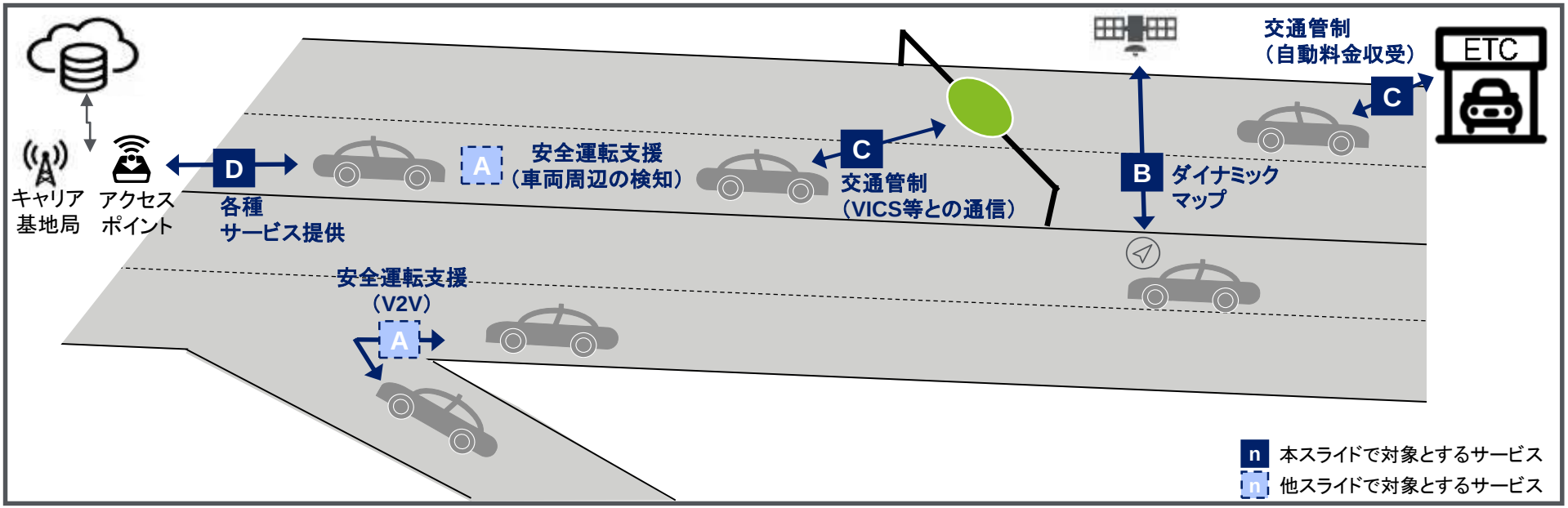
事業者等による自動走行の取組み状況 2/4 【Appendix A】
≪V2X、LIDAR等≫



機能		機能詳細	取組み内容	実装化時期	代表的な事業者等
A	安全運転支援	周辺機器との通信 （V2V、V2I、V2P）	5G等の通信技術活用を視野に入れた、双方向通信による安全運転支援技術の実装 - 交差点等にて車両車や歩行者等の状況をリアルタイムで配信・取得する技術（V2I） - 周辺車両と相互に走行状況をリアルタイムで配信・取得する技術（V2V） - 歩行者や自転車等と相互に走行状況をリアルタイムで配信・取得する技術（V2P）	2020年以降	自動車メーカー、自動車サプライヤ、電気機器メーカー、精密機器メーカー、通信事業者、ITベンダー、通信規格団体、等
		周辺環境の検知	車両周辺の状況を検知するセンサ（カメラ、レーダ、LIDAR等）を活用して、視界支援や車間警報等の認知支援を行う、自律検知型の安全運転支援技術の実装	車両に実装済み （一部機能は2020年以降）	自動車サプライヤー、電気機器メーカー、精密機器メーカー、ハイテクベンチャー、等

事業者等による自動走行の取組み状況 3/4
≪ダイナミックマップ、走行時の交通管制等≫

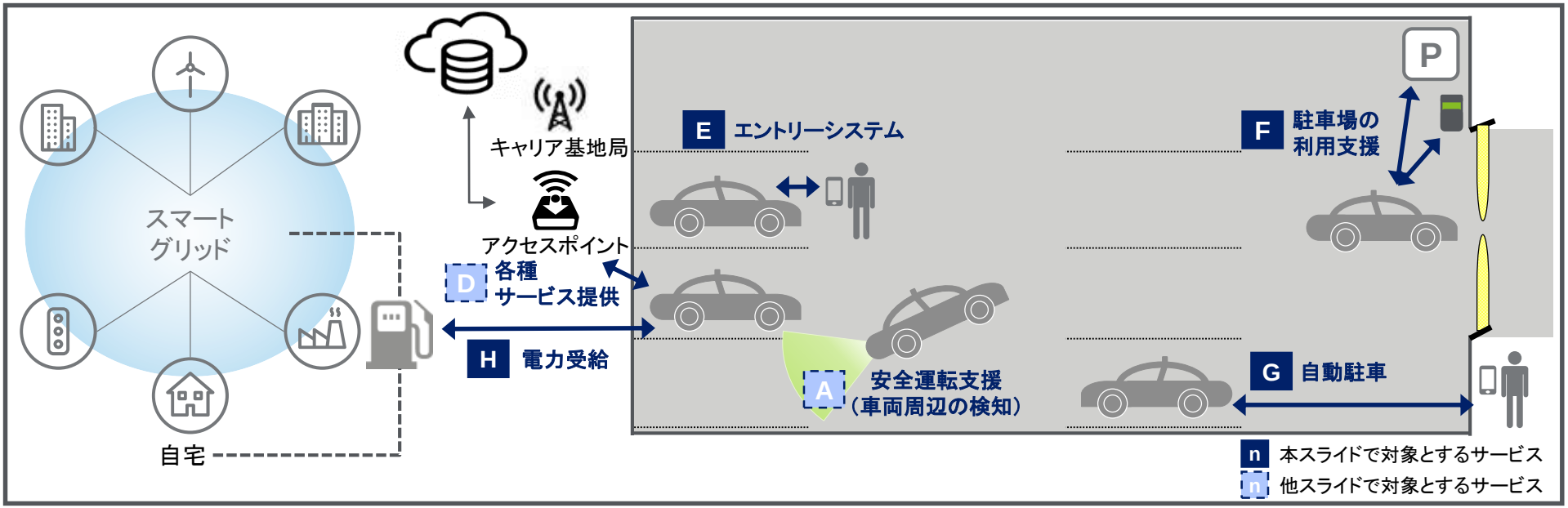
【Appendix A】



	機能	機能詳細	取組み内容	実装化時期	代表的な事業者等
B	ダイナミック マップ	位置情報の取得、 車両周辺との通信、 車両周辺の検知	静的情報に、変化する動的データ （動的、準動的、準静的情報）を重畳することで、 自車位置の正確な把握を可能にする高精度な 三次元地図を提供 - 動的情報：周辺車両、歩行者情報、等 - 準動的情報：事故、渋滞情報、等 - 準静的情報：交通規制、道路工事情報、等	2025年以降	地図製作会社、電気機器メーカー 、等
C	交通管制 （V2I）	VICS等との通信	5G等の通信技術活用を視野に入れた、プローブ データ・その他交通関連データ等のビッグデータ活 用により、円滑・快適な道路走行環境の維持を図る	2020年以降	自動車サプライヤ、電気機器メーカー、 精密機器メーカー、等
D	各種サービス 提供 （V2X、GNSS等）	広域通信（5G等）	5GやGNSS（GPS等）を活用した各種サービスを提供 例: 運行管理、エンターテインメント、コンシェルジュ サービス、テレマティクス保険管理、等	サービス展開済 （一部サービスは 2020年以降）	損害保険会社、各種サービス提供会社、等

事業者等による自動走行の取組み状況 4/4
≪駐車場における乗車、駐停≫

【Appendix A】



	機能	機能詳細	取組み内容	実装化時期	代表的な事業者等
E	エントリーシステム	ドア類の開錠・施錠、車両の始動	キーと車両の相互通信により自動でドア類の開錠・施錠、エンジン始動等を行い、利便性向上を図る	サービス展開済	自動車メーカー、自動車サプライヤ、電気機器メーカー、等
F	駐車場の利用支援	駐車場の情報取得、駐車料金の決済等	駐車場の利用前に駐車場の位置及び満車/空車情報を取得し、場内で自動的に料金の支払いを行う	2020年以降	自動車サプライヤ、電気機器メーカー、各種サービス提供会社、等
G	自動駐車	自動バレーパーキング	駐車場にて車両が自動運転で指定場所に駐車、出庫し、利便性向上や場内の事故削減を図る	2020年以降	自動車メーカー、自動車サプライヤ、電気機器メーカー、等
H	V2H／V2G（電力受給）	給電	電気自動車のエネルギーを家庭内または電力系統に連系して電力融通を行う	2020年以降	自動車メーカー、自動車サプライヤ、電気機器メーカー、電力会社、ガス会社、建設会社、等
		充電	充電器より専用の充電ケーブルを車両に接続、またはワイヤレスで車両の充電を行う	サービス展開済（ワイヤレス充電は実証実験中）	

【Appendix B】

通信を利用した機能の構成図

利用サイクル毎に整理した機能の構成要素を図式化

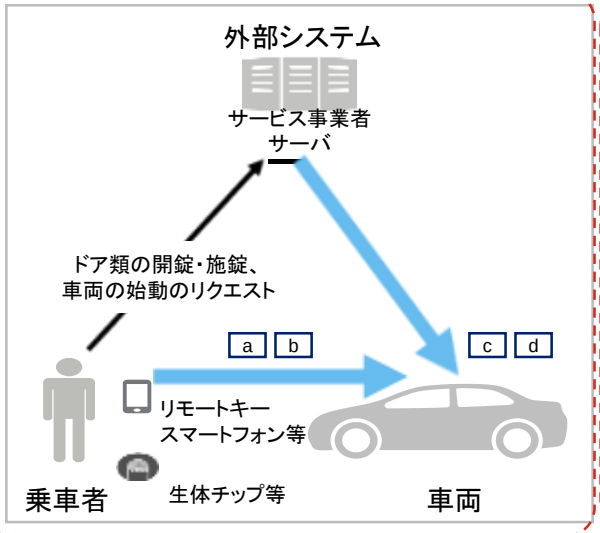
スライドの構成説明

体系図の凡例

- n　本スライドの機能に関わる具体的な技術や実施内容
- 車両と外部の通信（一方向）
- 車両と外部の通信（双方向）
- 車両が直接関わらない外部の通信

スライドタイトル
該当する利用サイクルおよび機能を記載

【乗車/走行準備】
エントリーシステム（1／2）



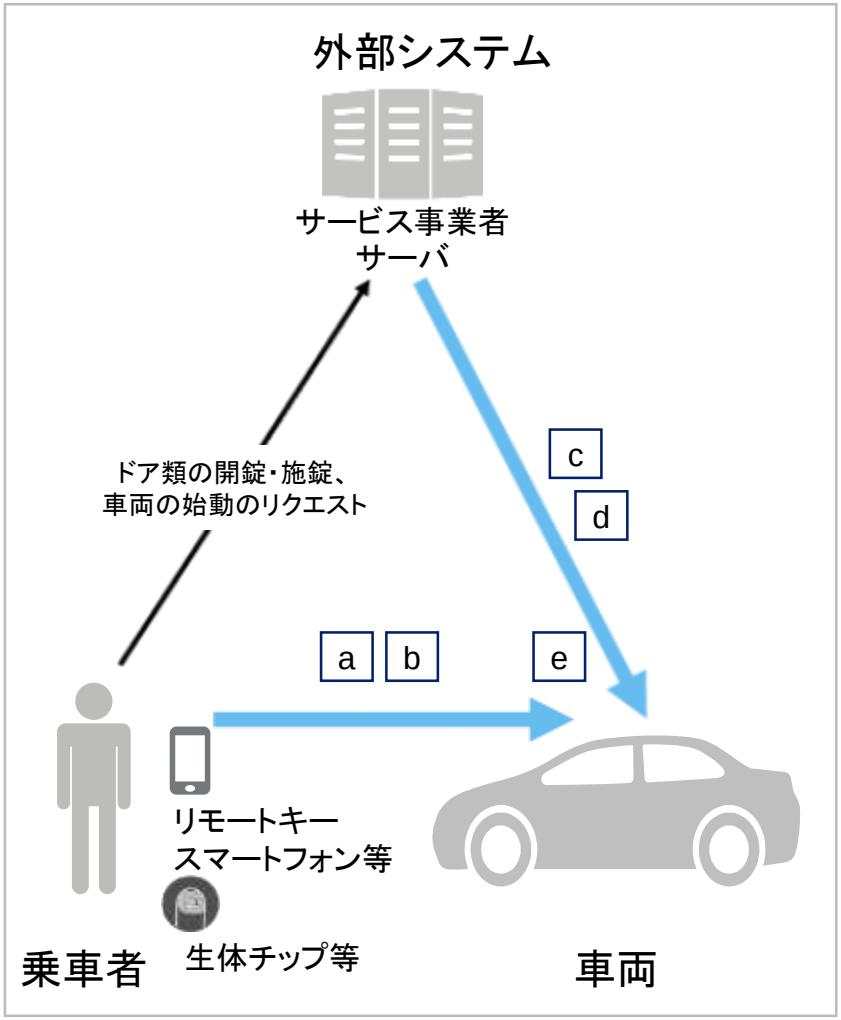
#	実用化機能	アクセス対象	通信の種類	通信デバイス
a	自家用車周辺での操作 – ドア類の開錠・施錠（ドア、トランク、ボンネット、給油口等）	リモートキー	RF/LF (RFID)	RF/LF (RFID) リーダ・ライタ
			Bluetooth	Bluetooth 送受信装置
		生体情報	センサー	生体認証センサー
		スマートフォン	Bluetooth	Bluetooth 送受信装置
		生体チップ	RF/LF (RFID)	RF/LF (RFID) リーダ・ライタ
		乗車者の指紋	生体情報	生体認証センサー
		乗車者の虹彩	センサー	生体認証センサー
		乗車者の顔	カメラ	カメラ
b	自家用車周辺での操作 – 車両の始動	a と同様		
c	自家用車の遠隔操作 – 遠隔からのドア類の開錠・施錠（ドア、トランク、ボンネット、給油口等）	サービス事業者のサーバ	携帯電話網（5G）	5G送受信装置
			携帯電話網（4G）	4G送受信装置
			Wi-Fi	Wi-Fi送受信機
d	自家用車周辺での操作 – 遠隔からの車両の始動	サービス事業者のサーバ	携帯電話網（5G）	5G送受信装置
			Wi-Fi	Wi-Fi送受信機

機能の説明
【項目】
- 実用化機能
- アクセス対象
- 通信の種類
- 車載通信デバイス

機能の体系図
当該機能および車両⇔外部間の関係性を図式化

【乗車/走行準備】

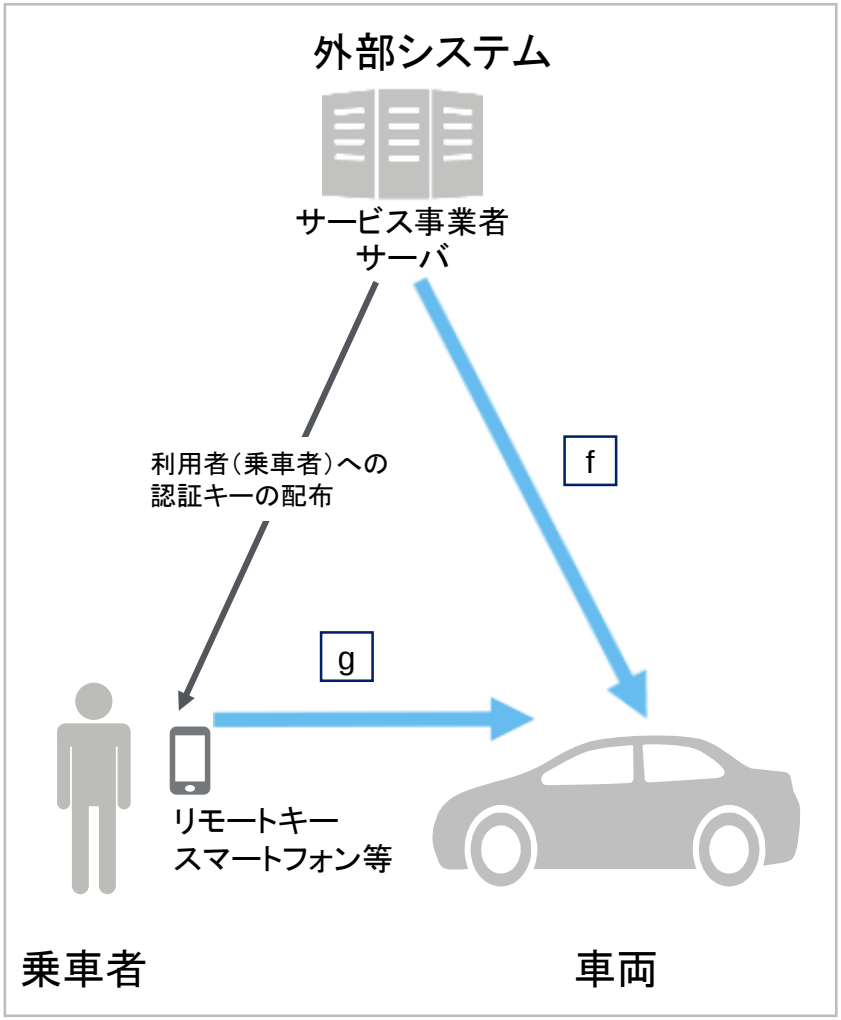
エントリーシステム（1／2）



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
a	**車両周辺での操作** - ドア類の開錠・施錠（ドア、トランク、ボンネット、給油口等）	リモートキー（キーフォブ）	RF/LF (RFID)	RF/LF (RFID) リーダ・ライタ
		スマートフォン	Bluetooth（VCK、ポータブル機器用）	Bluetooth 送受信装置
			NFC	NFCリーダライタ 端末
		乗車者の指紋	センサー	生体認証センサー
		乗車者の虹彩	センサー	生体認証センサー
		乗車者の顔	カメラ	カメラ
b	**車両周辺での操作** - 車両の始動	a と同様		
c	**車両の遠隔操作** - 遠隔からのドア類の開錠・施錠（ドア、トランク、ボンネット、給油口等）	サービス事業者サーバ	携帯電話網（5G）	5G送受信装置
			携帯電話網（4G）	4G送受信装置
			携帯電話網（3G）	3G送受信装置
			Wi-Fi	Wi-Fi送受信機
d	**車両の遠隔操作** - 遠隔からの車両の始動	サービス事業者サーバ	携帯電話網（5G）	5G送受信装置
			携帯電話網（4G）	4G送受信装置
			Wi-Fi	Wi-Fi送受信機
e	**パーソナライズ設定** （シート位置、エアコン設定、音楽プレイリスト等）	a および c と同様（車両利用時に実行）		

【乗車/走行準備】

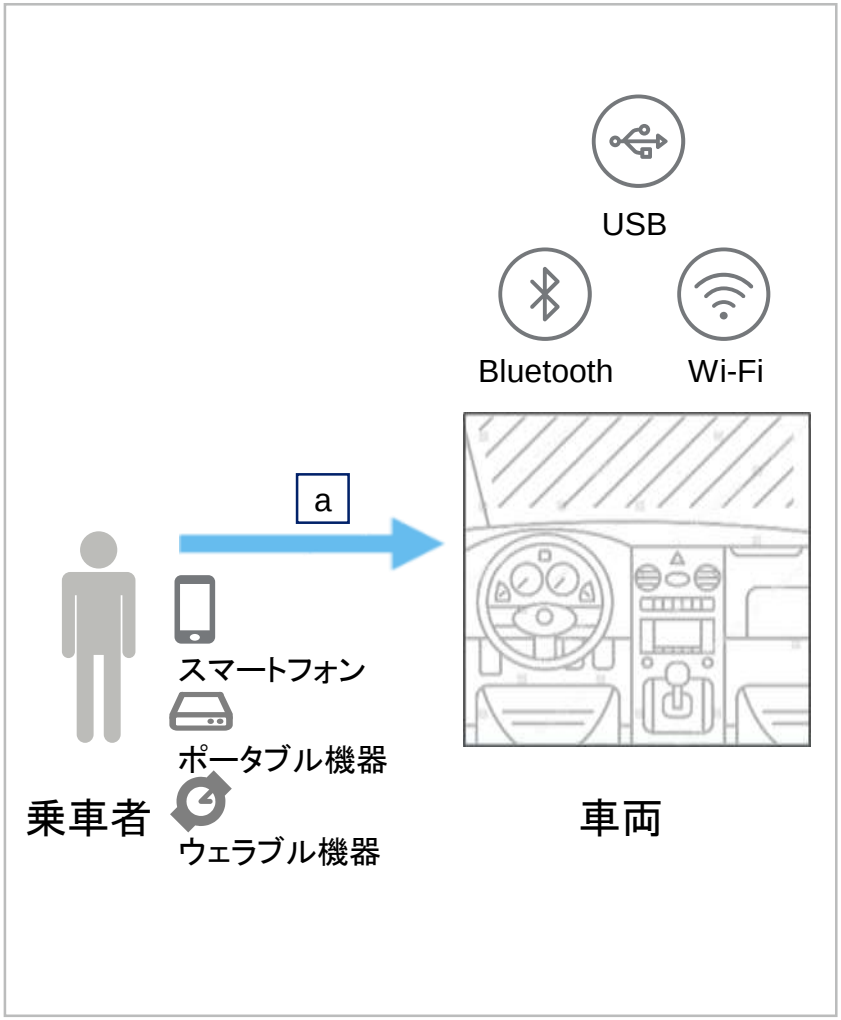
エントリーシステム（2／2）



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
f	**レンタカー、シェアリング車両周辺での操作** - 車両への認証キーの配布	サービス事業者サーバ	携帯電話網（5G）	5G送受信装置
			携帯電話網（4G）	4G送受信装置
			携帯電話網（3G）	3G送受信装置
			Wi-Fi	Wi-Fi送受信機
g	**レンタカー、シェアリング車両周辺での操作** - ドア類の開錠・施錠（ドア、トランク、ボンネット、給油口等）	リモートキー（キーフォブ）	RF/LF (RFID)	RF/LF (RFID) リーダ・ライタ
		スマートフォン	Bluetooth（VCK、ポータブル機器用）	Bluetooth 送受信装置
			NFC	NFCリーダライタ端末

【乗車/走行準備】

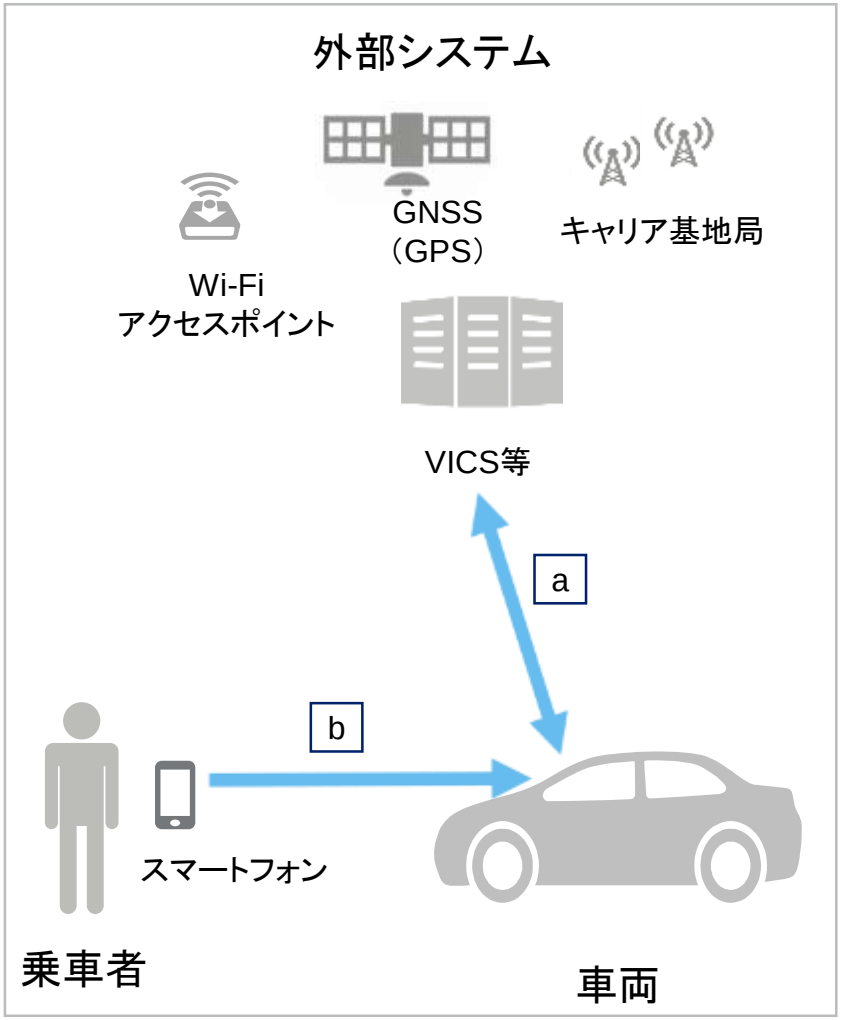
持込み機器との連携



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
a	- 各種持込み機器（ポータブル機器、ウェアラブル機器等）との連携	- スマートフォン - ポータブル機器 - ウェアラブル機器等	–	USB
			Bluetooth（VCK、ポータブル機器用）	Bluetooth 送受信装置
			Wi-Fi	Wi-Fi 送受信機

【乗車/走行準備】

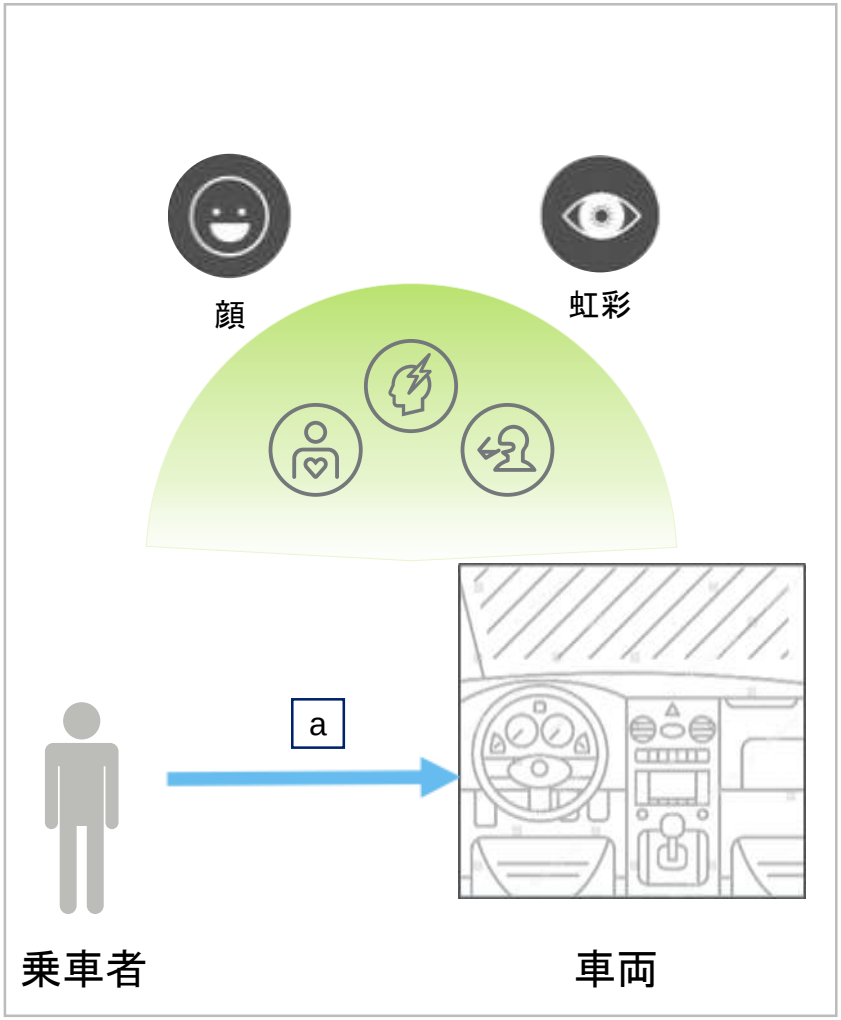
目的地の設定



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
a	**車両内での操作** - 位置情報の取得 - 交通情報（渋滞情報等）の取得	GNSS (GPS)	GNSS（GPS）	GNSS（GPS）受信機
		携帯事業者の基地局	携帯電話網（5G）	5G送受信装置
			携帯電話網（4G）	4G送受信装置
			携帯電話網（3G）	3G送受信装置
		Wi-Fi アクセスポイント	Wi-Fi	Wi-Fi送受信機
b	**遠隔操作** - 遠隔からの目的地の設定	サービス事業者サーバ	携帯電話網（5G）	5G送受信装置
			携帯電話網（4G）	4G送受信装置
			携帯電話網（3G）	3G送受信装置
			Wi-Fi	Wi-Fi送受信機

【走行】

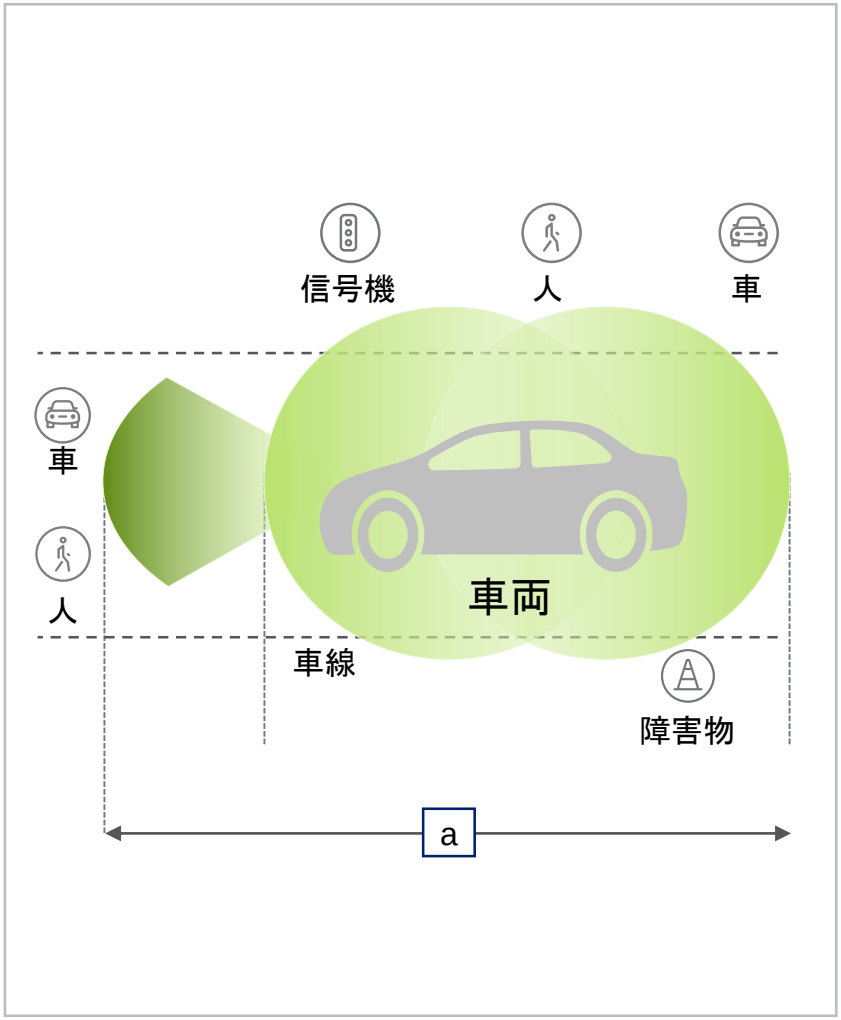
ドライバー監視



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
a	- 生体モニタリングによるドライバーの監視	乗車者の顔	カメラ	カメラ
		乗車者の生体情報（脈拍、体温、血圧、等）	センサー	生体認証センサー

【走行】

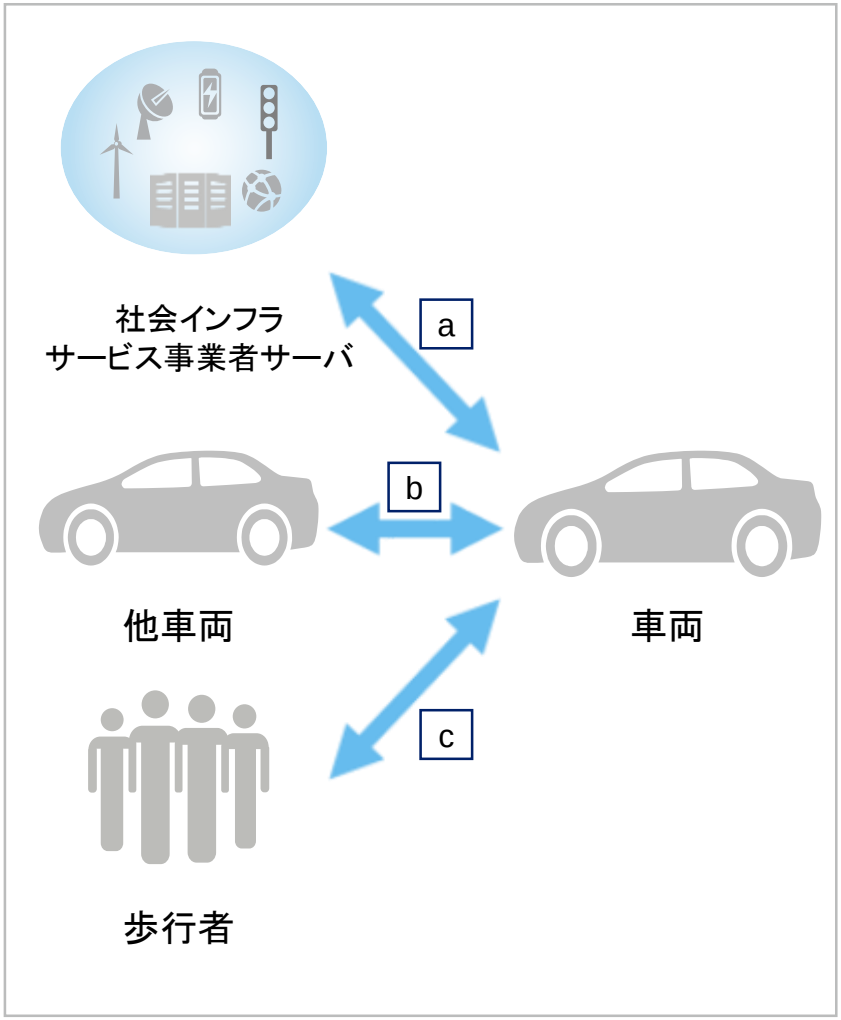
周辺環境の検知



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
a	- 車線維持支援 - 信号、交通標識等の認識 - 車両周辺の障害物等検出 - 車線変更アシスト - ヘッドライト切り替え - ナイトビジョン - 適応クルーズ・コントロール - 加速制御 - 衝突被害軽減支援 - 後方衝突警報 - 交差点進入時等の注意喚起 - 歩行者検出	- 車線 - 信号 - 交通標識 - 車両周辺の障害物 - 周辺光度 - 周辺車両 - 前方の光 - 前方車両 - 前方障害物 - 後方障害物 - 交差点内の障害物 - 歩行者	単眼カメラ	単眼カメラ
			ステレオカメラ	ステレオカメラ
			ミリ波レーダ（77GHz帯レーダー）	ミリ波レーダ送受信装置
			ミリ波レーダ（79GHz帯超広帯域レーダ）	
			LIDAR	LIDAR送受信装置
			超音波センサー	超音波センサー送受信装置
			近赤外線カメラ	近赤外線カメラ
			遠赤外線カメラ	遠赤外線カメラ

【走行】

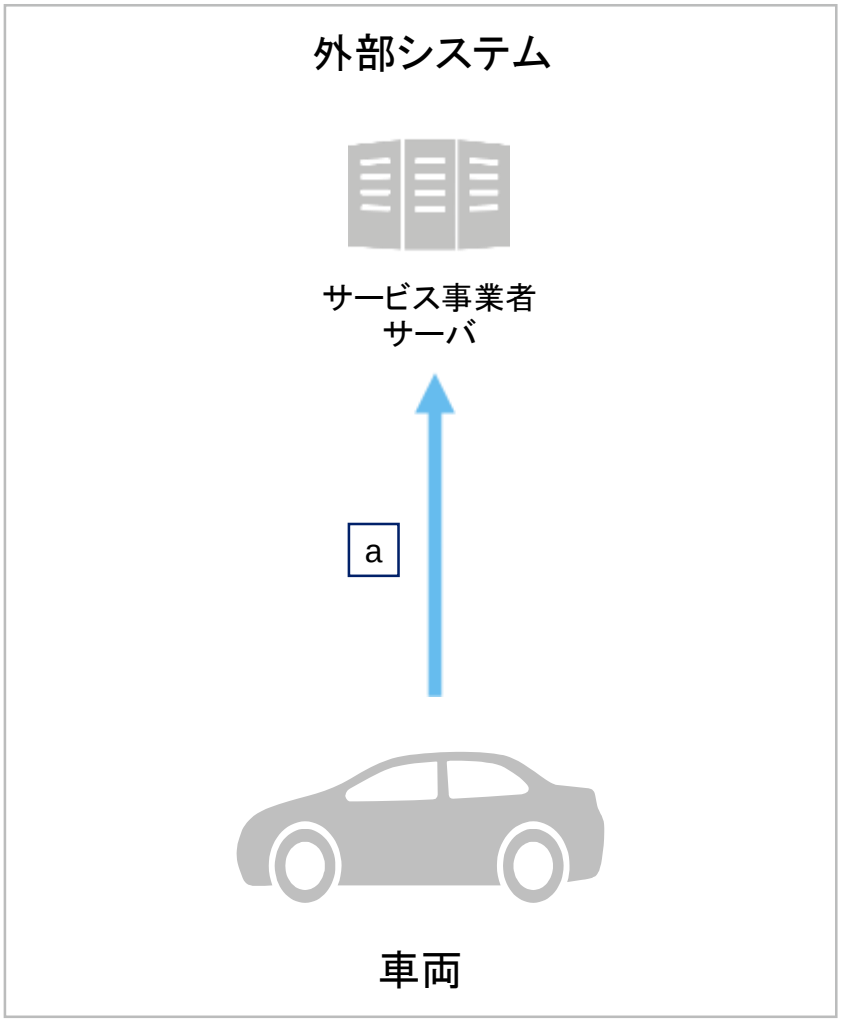
V2X（Vehicle-to-Everything）周辺機器との通信



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
a	**路車間の通信（V2I）** - 信号、交通標識等との通信 - 交差点進入時等の注意喚起 - 道路交通情報の連携、等	- 路側機 - サービス事業者サーバ等	携帯電話網（5G）	5G送受信装置
			携帯電話網（4G）	4G送受信装置
			Cellular V2X	Cellular V2X送受信装置
			DSRC	DSRC通信端末（VICS/ETC）
			準マイクロ波	準マイクロ波端子
			赤外線	赤外線端子
b	**車車間の通信（V2V）** - 適応クルーズ・コントロール - 交差点進入時の注意喚起 - 車両周辺の障害物検出、等	- 周辺車両	携帯電話網（5G）	5G送受信装置
			携帯電話網（4G）	4G送受信装置
			Cellular V2X	Cellular V2X送受信装置
			DSRC	DSRC通信端末（V2X）
c	**V2P：車歩行者通信** - 歩行者との通信	- 歩行者デバイス	携帯電話網（5G）	5G送受信装置
			携帯電話網（4G）	4G送受信装置
			Cellular V2X	Cellular V2X送受信装置
			DSRC	DSRC通信端末（V2X）

【走行】

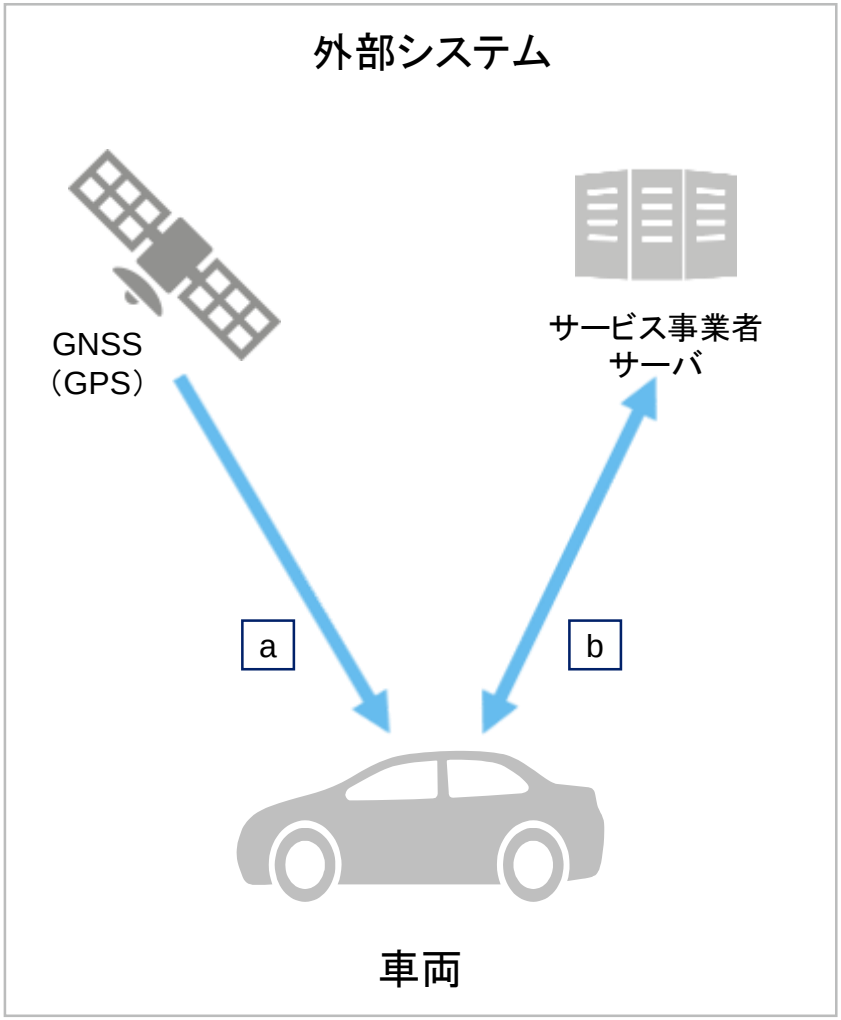
緊急通報



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
a	**外部への連絡** - 交通事故発生時の緊急通報等、外部への連絡	サービス事業者サーバ	携帯電話網（5G）	5G送受信装置
			携帯電話網（4G）	4G送受信装置
			携帯電話網（3G）	3G送受信装置
			Cellular V2X	Cellular V2X 送受信装置

【走行】

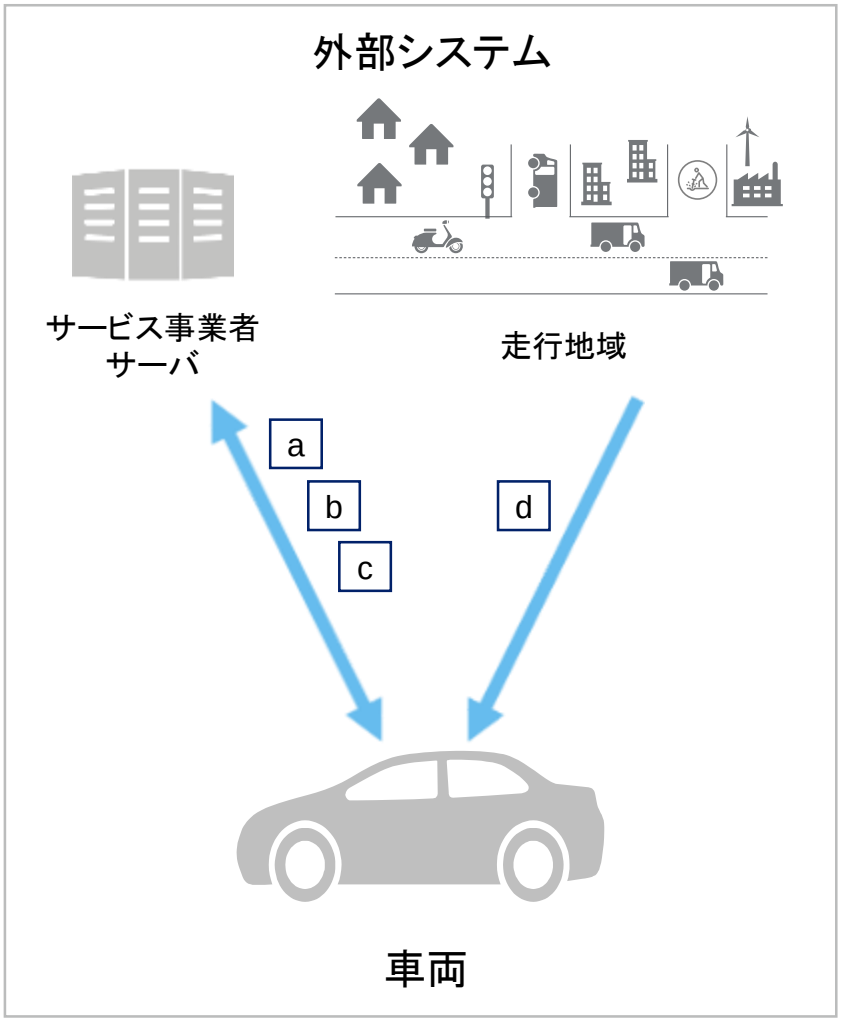
ダイナミックマップ



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
a	- 位置情報の取得	サービス事業者サーバ	GNSS（GPS）	GNSS（GPS）受信機
b	- 地図情報の取得／更新	サービス事業者サーバ	携帯電話網（5G）	5G送受信装置
			携帯電話網（4G）	4G送受信装置

【走行】

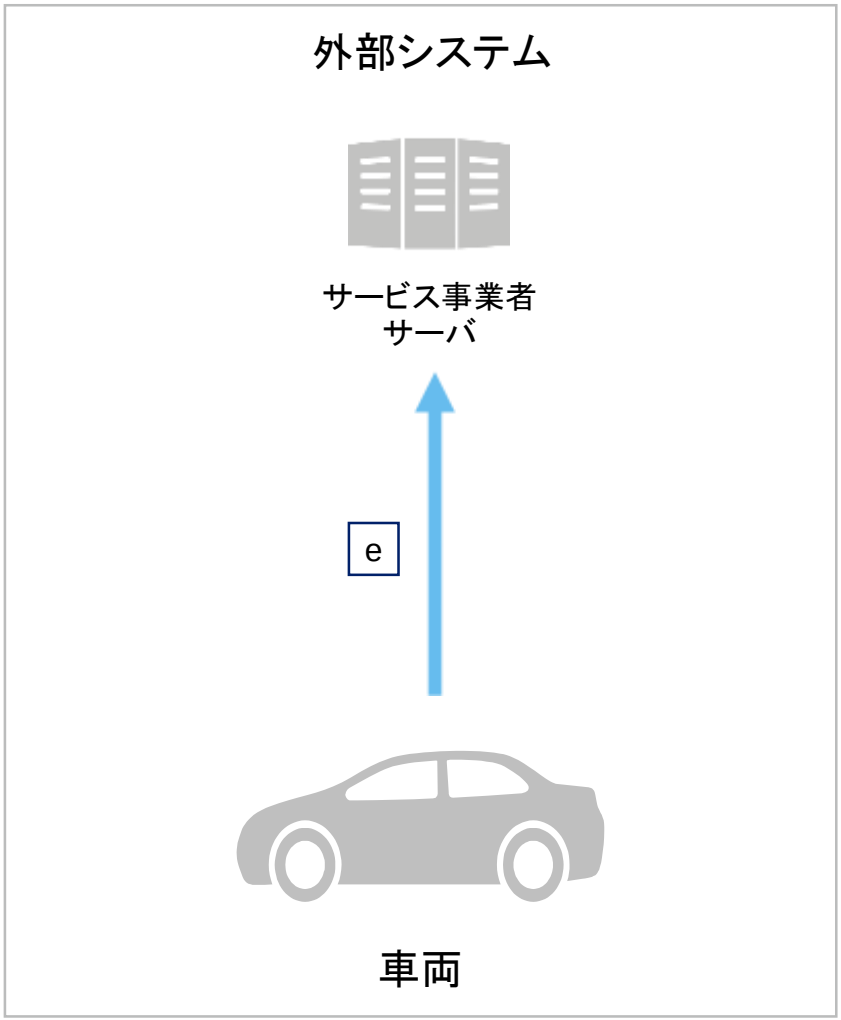
エンタテイメント（1／2）



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
a	インターネット接続（エンタメ、ニュース情報（動画、音声、画像等）の配信・受信）	サービス事業者サーバ	携帯電話網（5G）	5G送受信装置
			携帯電話網（4G）	4G送受信装置
b	IP電話		携帯電話網（3G）	3G送受信装置
c	エージェント（趣味・嗜好等に合わせた各種サービス提供）		Wi-Fi	Wi-Fi送受信機
d	周辺施設情報の取得（POI情報等の受信）	走行地域	携帯電話網（5G）	5G送受信装置
			携帯電話網（4G）	4G送受信装置
			携帯電話網（3G）	3G送受信装置
			Wi-Fi	Wi-Fi送受信機
			赤外線	赤外線端子

【走行】

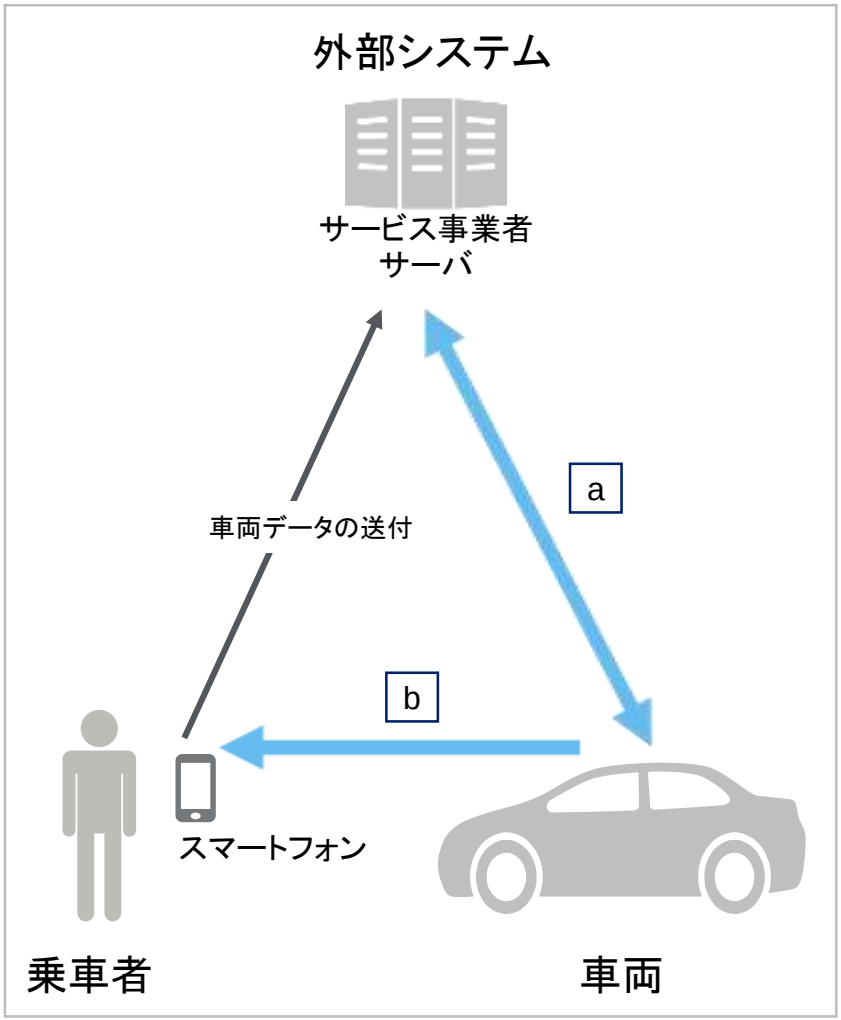
エンタテイメント（2／2）



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
e	**決済** - 利用サービスに係る料金支払い	- サービス事業者サーバ - 非接触カード - スマートフォン	携帯電話網（5G）	5G送受信装置
			携帯電話網（4G）	4G送受信装置
			携帯電話網（3G）	3G送受信装置
			Wi-Fi	Wi-Fi送受信機
			NFC	NFCリーダライタ端末

【走行】

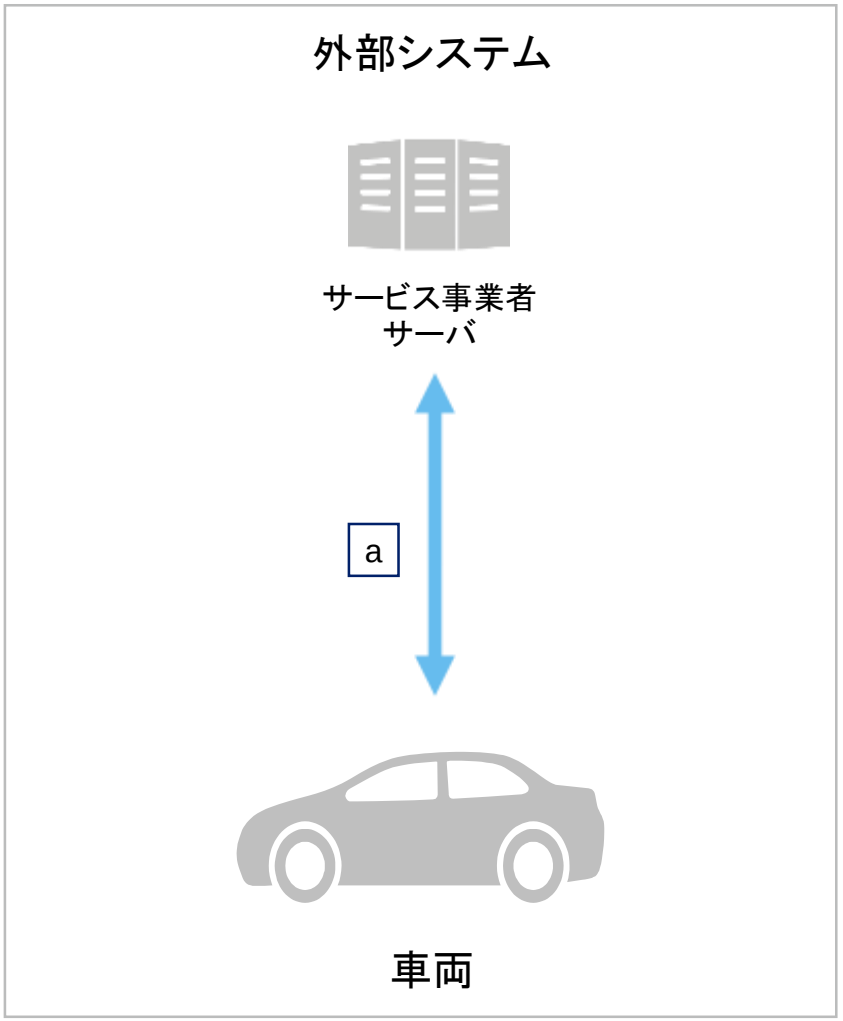
車載データの保管・送信



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
a	車載データの保管・送信（走行履歴、外部環境、車両状態、等）	サービス事業者サーバ	携帯電話網（5G）	5G送受信装置
			携帯電話網（4G）	4G送受信装置
			携帯電話網（3G）	3G送受信装置
			Wi-Fi	Wi-Fi送受信機
b		スマートフォン	Bluetooth（OBD-II用）	OBD-IIポート

【駐車】

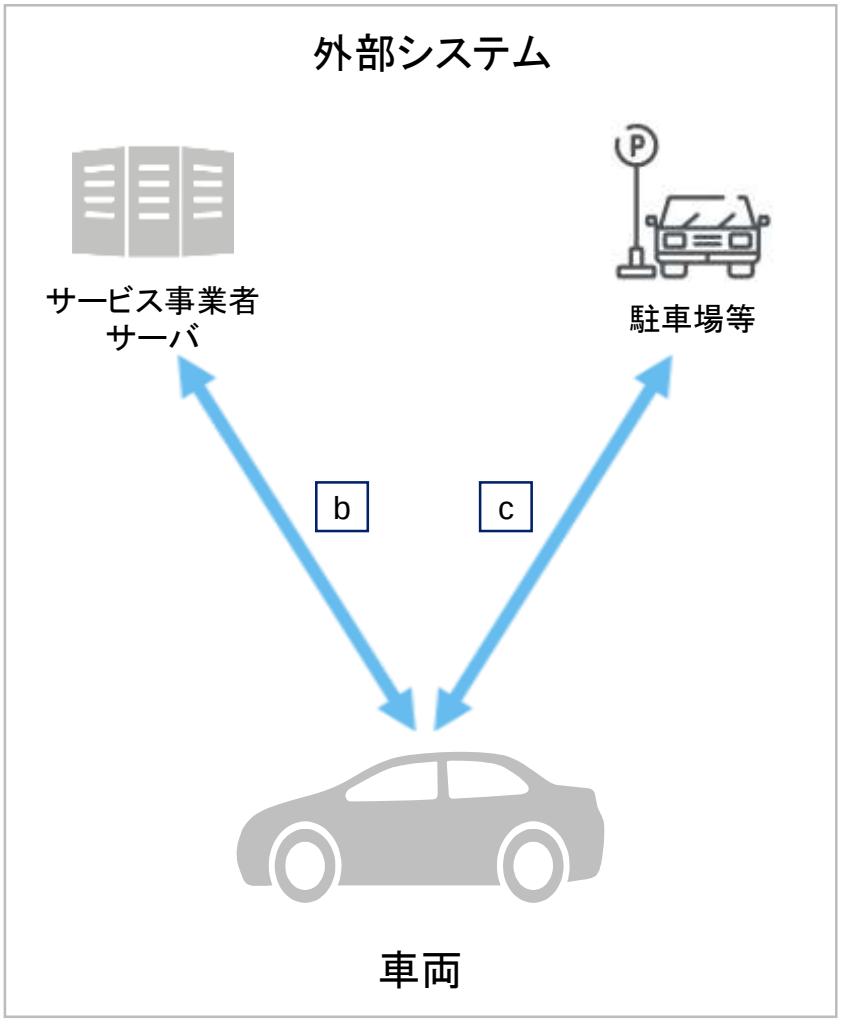
駐車場の利用支援(1／2)



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
a	**駐車場情報の取得** - 駐車場の位置及び満車/空車情報の取得	- VICS等 - サービス事業者サーバ	FM多重放送	FM多重アンテナ
			DSRC	DSRC通信端末(VICS/ETC)
			電波ビーコン(2.4GHz帯)	準マイクロ波端子(電波ビーコン受信アンテナ)
			赤外線	赤外線端子
			携帯電話網(5G)	5G送受信装置
			携帯電話網(4G)	4G送受信装置
			携帯電話網(3G)	3G送受信装置
			Wi-Fi	Wi-Fi送受信機

【駐車】

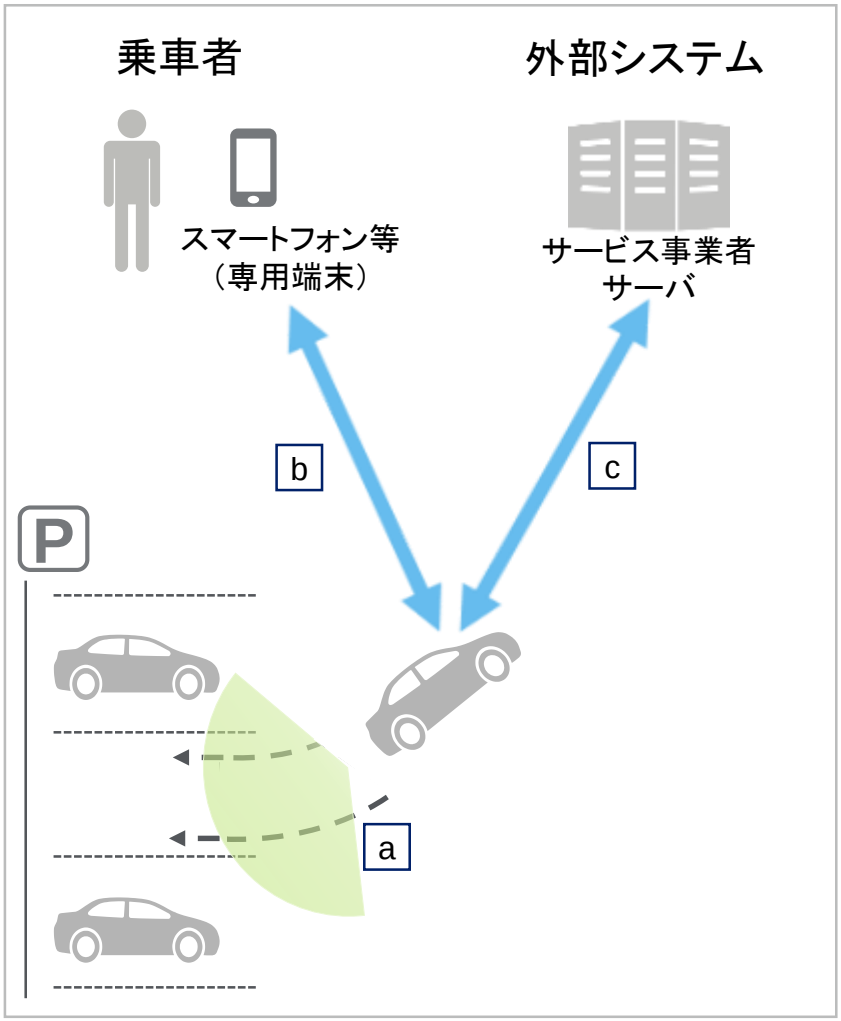
駐車場の利用支援(2／2)



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
b	**予約** - 駐車場の予約	サービス事業者サーバ	携帯電話網(5G)	5G送受信装置
			携帯電話網(4G)	4G送受信装置
			携帯電話網(3G)	3G送受信装置
			Wi-Fi	Wi-Fi送受信機
c	**決済** - 駐車料金の自動支払い	料金所の路側機器	DSRC	DSRC通信端末(VICS/ETC)

【駐車】

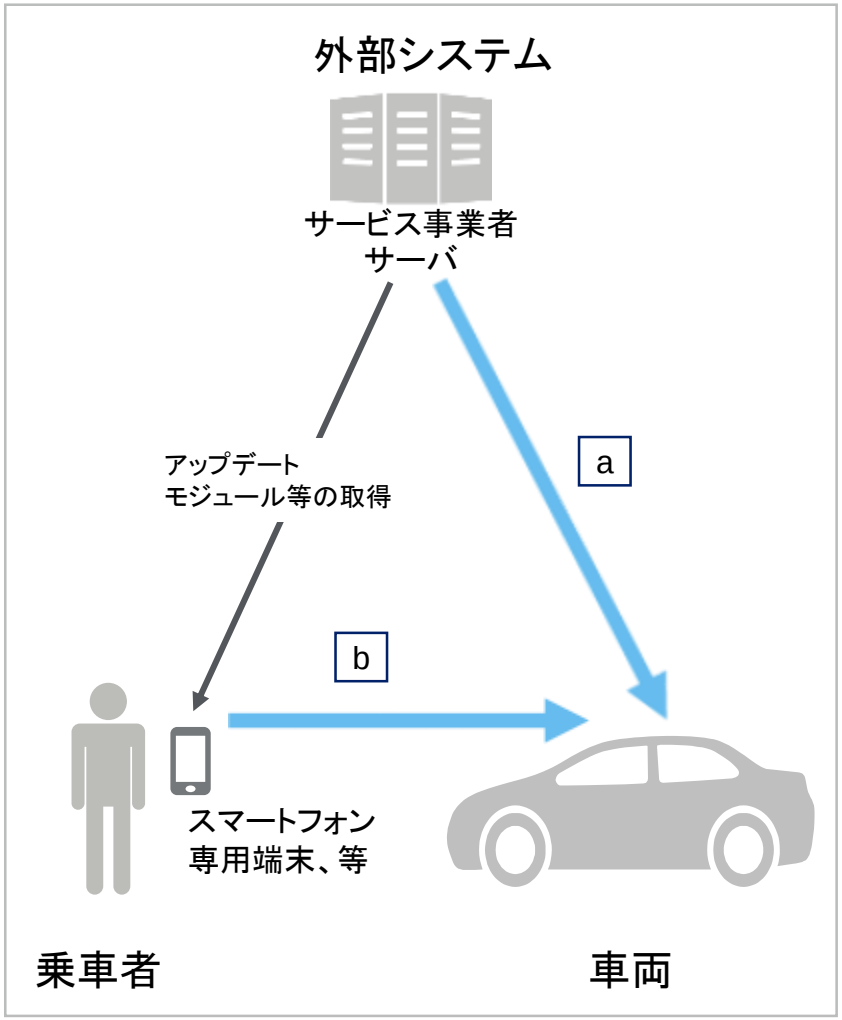
駐車支援



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
a	**駐車アシスト** - 最適な駐車経路の割り出し	車両周辺障害物情報	単眼カメラ	単眼カメラ
			ステレオカメラ	ステレオカメラ
			超音波センサー	超音波センサー送受信装置
b	**リモコン駐車** - 自動バレーパーキング	- 車両周辺障害物 - スマートフォン、専用端末	単眼カメラ	単眼カメラ
			ステレオカメラ	ステレオカメラ
			超音波センサー	超音波センサー送受信装置
			携帯電話網（5G）	5G送受信装置
			Wi-Fi	Wi-Fi送受信機
c	**自動駐車** - 自車両の状況の通知	サービス事業者サーバ	携帯電話網（5G）	5G送受信装置
			Wi-Fi	Wi-Fi送受信機

【メンテナンス】

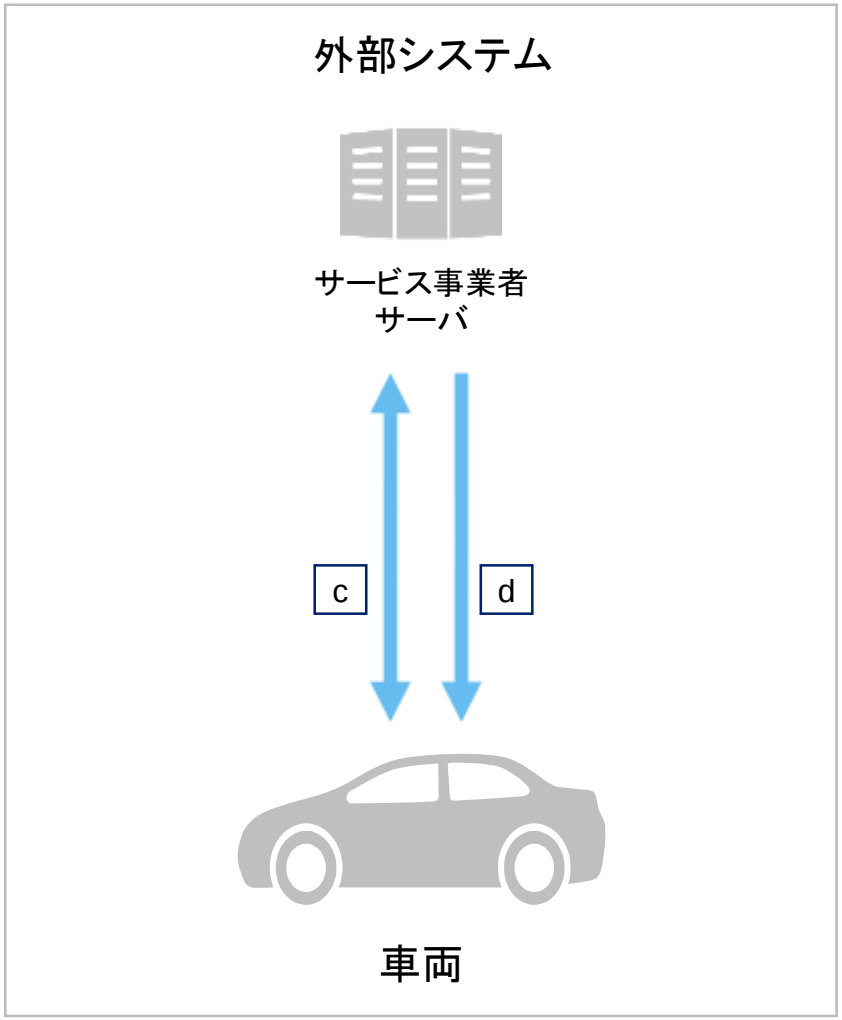
車両管理（OTA）（1／2）



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
a	**ソフトウェア／ファームウェア更新** -（自動）	サービス事業者サーバ	携帯電話網（5G）	5G送受信装置
			携帯電話網（4G）	4G送受信装置
			携帯電話網（3G）	3G送受信装置
			Wi-Fi	Wi-Fi送受信機
b	**ソフトウェア／ファームウェア更新** -（手動）	スマートフォン	Bluetooth（VCK、ポータブル機器用）	Bluetooth送受信装置
		専用端末	Bluetooth（ドングル経由）	OBD-IIポート

【メンテナンス】

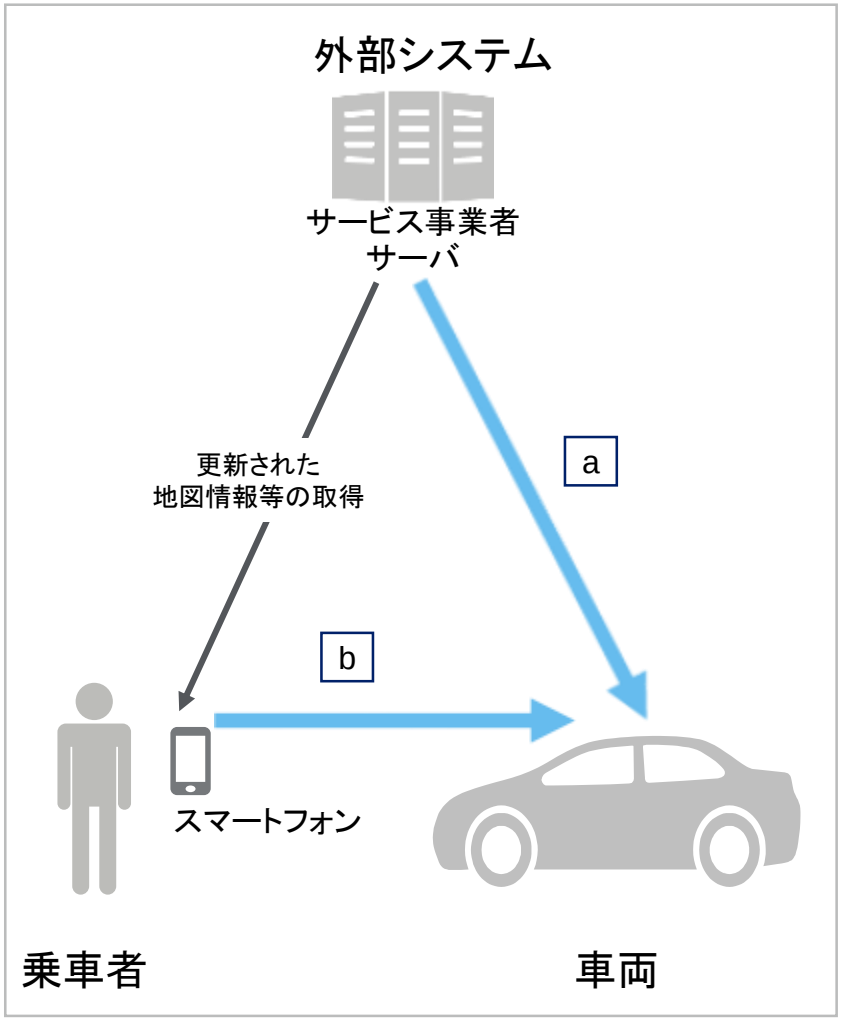
車両管理（OTA）（2／2）



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
c	**車両診断** - 車両状態の診断および通知 - タイヤの異常通知	サービス事業者サーバ	携帯電話網（5G）	5G送受信装置
			携帯電話網（4G）	4G送受信装置
			携帯電話網（3G）	3G送受信装置
			Wi-Fi	Wi-Fi送受信機
d	**マーケティング** - OEM・サプライヤ等からの広告通知	サービス事業者サーバ	携帯電話網（5G）	5G送受信装置
			携帯電話網（4G）	4G送受信装置
			携帯電話網（3G）	3G送受信装置
			Wi-Fi	Wi-Fi送受信機

【メンテナンス】

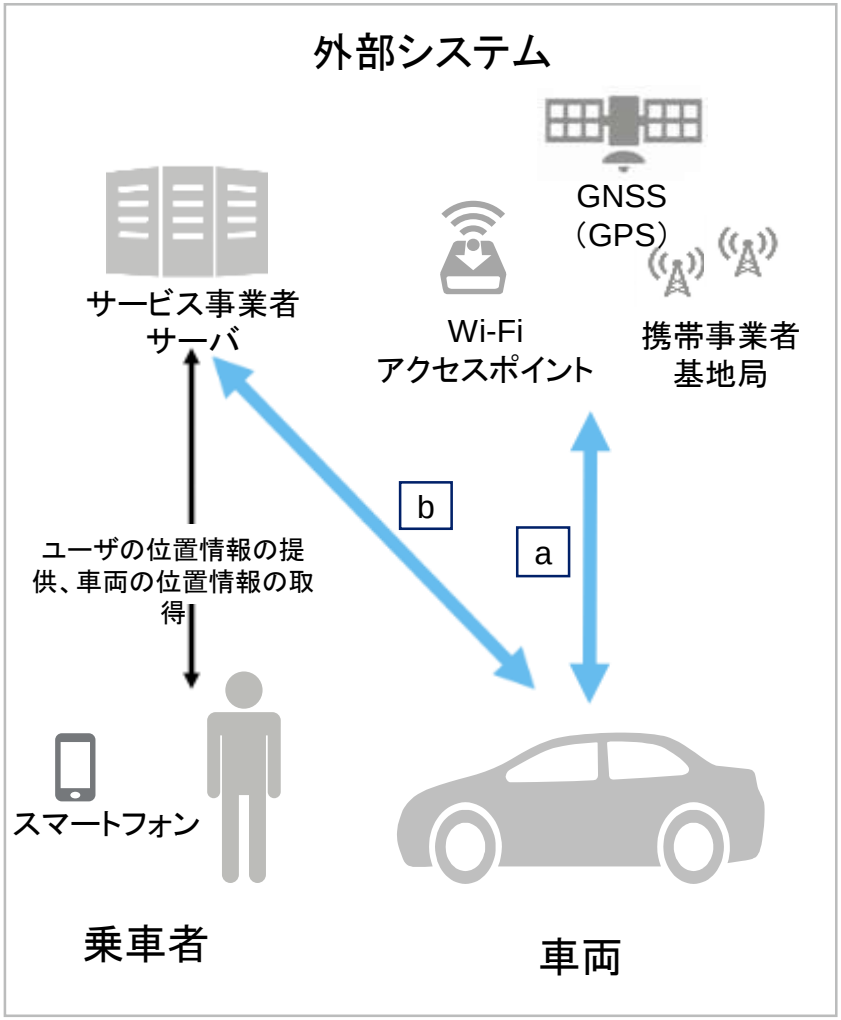
ナビゲーション



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
a	**地図情報の更新** -（自動）	サービス事業者サーバ	携帯電話網（5G）	5G送受信装置
			携帯電話網（4G）	4G送受信装置
			携帯電話網（3G）	3G送受信装置
			Wi-Fi	Wi-Fi送受信機
b	**地図情報の更新** -（手動）	スマートフォン	Bluetooth（VCK、ポータブル機器用）	Bluetooth送受信装置
		CD-Rドライブ、DVD-Rドライブ等	–	CD-Rドライブ、DVD-Rドライブ等

【メンテナンス】

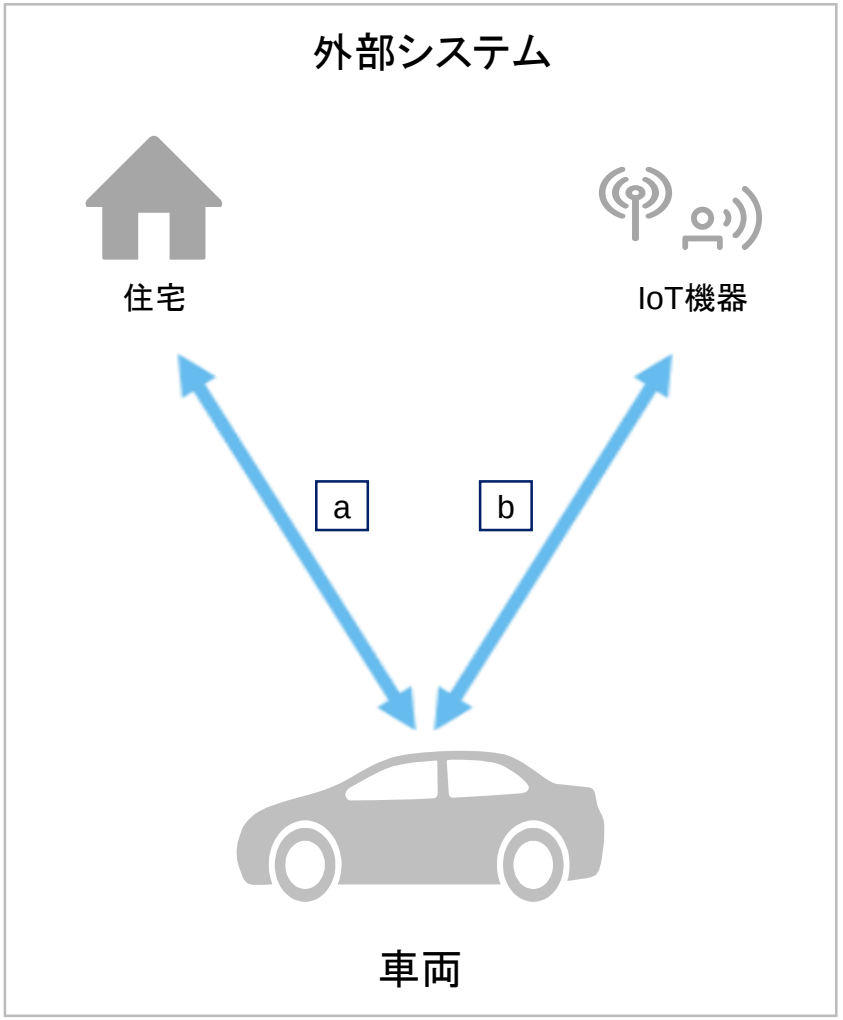
配車手配



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
a	- 配車に伴う位置情報の取得	GNSS(GPS)	GNSS(GPS)	GNSS(GPS)受信機
		携帯事業者の基地局	携帯電話網(5G)	5G送受信装置
			携帯電話網(4G)	4G送受信装置
			携帯電話網(3G)	3G送受信装置
		Wi-Fiアクセスポイント	Wi-Fi	Wi-Fi送受信機
b	- 配車に伴う位置情報の連携	サービス事業者サーバ	携帯電話網(5G)	5G送受信装置
			携帯電話網(4G)	4G送受信装置
			携帯電話網(3G)	3G送受信装置
			Wi-Fi	Wi-Fi送受信機

【メンテナンス】

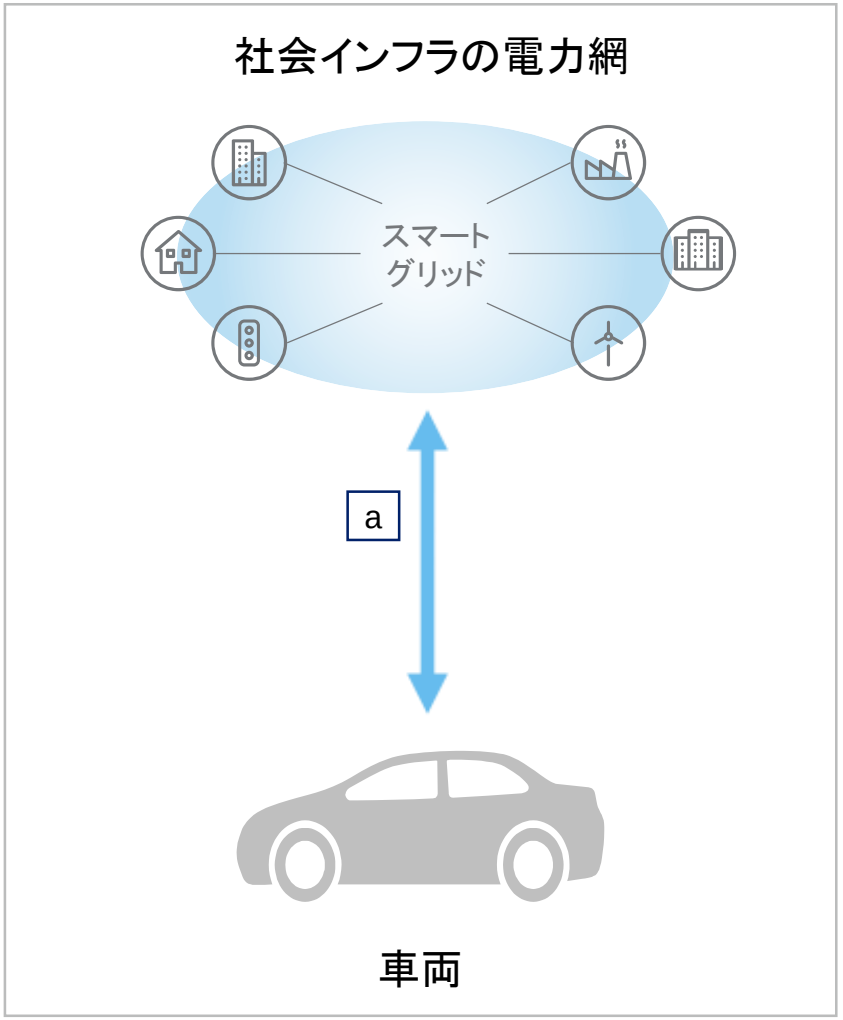
V2H：ホームシステムとの連携（Vehicle-to-Home）



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
a	**電力充電、給電** - 家庭での電力の受給電	住宅	CHAdeMO	充電/給電コネクタ
			ZigBee	ZigBee無線モジュール
			Wi-Fi	Wi-Fi送受信機
b	**家庭内のIoT機器との連携** - IoT機器との連携	IoT機器	携帯電話網（5G）	5G送受信装置
			携帯電話網（4G）	4G送受信装置
			携帯電話網（3G）	3G送受信装置
			Wi-Fi	Wi-Fi送受信機

【メンテナンス】

V2G :グリッドとの連携（Vehicle-to-Grid）



#	実用化機能	アクセス対象	通信の種類	車載通信デバイス
a	**電力充電、給電** - グリッド（電力網）との電力の受給電	社会インフラの電力網	CHAdeMO	充電/給電コネクタ
			ZigBee	ZigBee無線モジュール
			Wi-Fi	Wi-Fi送受信機

【Appendix C】

自動走行システムにおける通信情報の種別

通信情報の種別と重要度

自動走行システムにおける通信情報の種別

詳細は「別紙1_自動走行システム構成調査表.xlsx」参照

カテゴリ	情報の種別	重要度（評価指標）	情報の具体例	
車両情報	走行制御情報	高（3）	走行制御情報	車線、信号、周辺車両、障害物の位置や距離、等
			ソフトウェア管理情報	ソフトウェア更新、機能制限、等
	走行サポート情報	中（2）	交通情報	渋滞、工事、道路状況、等
			地図情報※1	地図情報、ダイナミックマップ、等
			車両位置情報※1	目的地、自車位置情報、等
	車両管理情報		車載データ※1	運転履歴、走行履歴、利用事象の発生時刻、等
			診断情報	故障、部品消耗度に関する情報、等
			車両属性情報※1	車両識別番号、車種、走行距離、等
			ボディ制御情報	充電管理、認証情報、等
個人情報	乗車者情報	低（1）	生体情報	指紋、虹彩、等
			資産情報	クレジットカード、ETC、等
			趣味・嗜好に関する情報	動画・音楽配信、等
			アプリケーション管理※1	サービスID、利用履歴、等
周辺環境情報※2			POI／周辺環境情報	気象情報、駐車場、近隣飲食店等の情報、等

一部の通信情報は、複数の種別に該当することに留意する

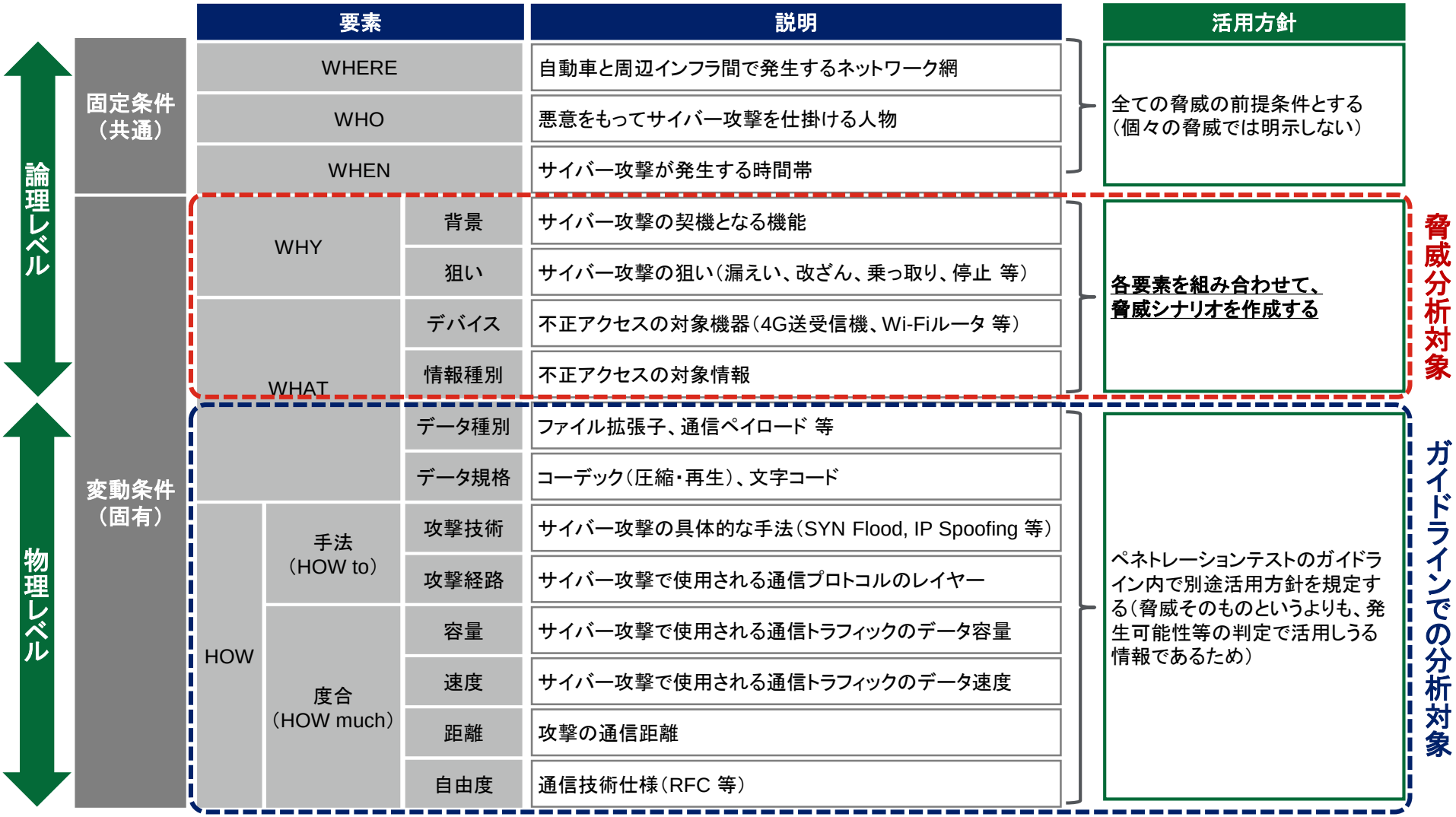
※1他の情報と組み合わせることで、個人情報となる可能性のある情報
※2走行には影響しない周辺地域・施設等の情報

【Appendix D】

脅威の構成要素と活用方針

脅威の構成要素と活用方針

5W1Hを踏まえた脅威の全体構造



【Appendix E】

脅威の分類のリファレンス

脅威の分類のリファレンス 1/3

主要リファレンスにおける脅威の分類の考え方

STRIDE

発生事象の特性に応じた分類		
1	Spoofing	なりすまし
2	Tampering	改ざん
3	Repudiation	否認
4	Information Disclosure	情報漏えい
5	Denial of Service	サービス妨害
6	Elevation of Privilege	権限の昇格

ENISA
(Threat Taxonomy)

資産（情報・物理）の紛失を分類		
1	Information leakage/sharing due to human error	人的ミスによる情報の漏えい/拡散
2	Erroneous use or administration of devices and systems	デバイス／システムの管理権限の誤用
3	Using information from an unreliable source	信頼性の低い情報源からの情報の利用
4	Unintentional change of data in an information system	情報システムにおける意図しないデータ変更
5	Inadequate design and planning or improperly adaptation	不適切な設計および計画、または不適当な適応
6	Damage caused by a third party	第三者に起因する損害
7	Damages resulting from penetration testing	ペネトレーション・テストによる損害
8	Loss of information in the cloud	クラウド内の情報喪失
9	Loss of (integrity of) sensitive information	機密情報の（完全性の）喪失
10	Loss of devices, storage media and documents	デバイス、ストレージメディア、ドキュメントの紛失
11	Destruction of records	レコードの破壊

脅威の分類のリファレンス 2/3

主要リファレンスにおける分類の考え方

NIST SP 800-30
(Threat Events Achieve Results)

攻撃手法および発生事象で分類		
1	Obtain sensitive information through network sniffing of external networks.	外部ネットワークのネットワークスニッフィングを介して、機微な情報を取得する
2	Obtain sensitive information via exfiltration.	機微な情報を取り出して、取得する
3	Cause degradation or denial of attacker-selected services or capabilities.	アタッカーが選択したサービスまたは機能の低下または提供拒否を引き起こす
4	Cause deterioration/destruction of critical information system components and functions.	基幹業務に関わる情報システムコンポーネントおよび機能の低下／破壊を引き起こす
5	Cause integrity loss by creating, deleting, and/or modifying data on publicly accessible information systems (e.g., web defacement).	公的にアクセス可能な情報システム上にデータを作成したり、システム上のデータを削除したり、あるいはデータを変更することによって、完全性の喪失を引き起こす
6	Cause integrity loss by polluting or corrupting critical data.	極めて重要なデータを汚染する、あるいは改ざんすることによって、完全性の喪失を引き起こす
7	Cause integrity loss by injecting false but believable data into organizational information systems.	もっともらしいが偽のデータを組織の情報システムに挿入することによって、完全性の喪失を引き起こす
8	Cause disclosure of critical and/or sensitive information by authorized users.	アクセス権限のあるユーザによる、極めて重要な情報および／または機微な情報の開示を引き起こす
9	Cause unauthorized disclosure and/or unavailability by spilling sensitive information.	機微な情報を漏らすことによって、正規の権限によらない開示および／または利用不能を引き起こす
10	Obtain information by externally located interception of wireless network traffic.	外部に設置された傍受用デバイスを使用して、無線ネットワークトラフィックを傍受し、情報を取得する
11	Obtain unauthorized access.	不正なアクセスを行う
12	Obtain sensitive data/information from publicly accessible information systems.	公的にアクセス可能な情報システムから、機微なデータ／情報を取得する
13	Obtain information by opportunistically stealing or scavenging information systems/components.	機会を伺って情報システム／コンポーネントを盗んだり、あさることによって、情報を取得する

脅威の分類のリファレンス 3/3

主要リファレンスにおける分類の考え方

CAPEC

攻撃手法に応じた分類		
1	Collect and Analyze Information	情報の収集および分析
2	Inject Unexpected Items	予期しない項目を挿入（変数・命令文、等）
3	Engage in Deceptive Interactions	虚偽のやりとり（なりすまし、等）
4	Manipulate Timing and State	タイミングと状態の悪用
5	Abuse Existing Functionality	既存機能の不正利用
6	Employ Probabilistic Techniques	確率的技法の利用
7	Subvert Access Control	アクセスコントロールの悪用（認証・承認）
8	Manipulate Data Structures	データ構造の不正操作
9	Manipulate System Resources	システムリソースの不正操作

OWASP
(Category: Threat)

Webシステムの脅威を分類		
1	REVERSE TROJAN (Server-to-Client)	リバース・トロイ（遠隔操作型トロイの木馬）
2	TIME BOMB	タイム・ボム（潜伏型攻撃）
3	BOTS	ボット
4	LOGIC BOMB	ロジック・ボム（悪意ある開発者が仕込んだ潜伏型コード）
5	KEY LOGGERS	キーロガー
6	SNIFFERS	スニッファ
7	BACKDOORS	バックドア
8	ROOTKITS	ルートキット（権限奪取用ツール）
9	VIRUS	ウィルス
10	WORM	ワーム
11	SPYWARE	スパイウェア
12	TROJAN HORSE	トロイの木馬

【Appendix F】

STRIDEの網羅感（その他のリファレンスの比較）

STRIDEの網羅感 1/2

他リファレンスとのマッピング

※OWASPについては、具体的な攻撃手段の記載のため、STRIDEとのマッピングは行わない

STRIDE		CAPEC		ENISA (Threat Taxonomy)	
No	項目	No	項目	No	項目
1	なりすまし (Spoofing)	3	虚偽のやりとり（なりすまし、等）	3	信頼性の低い情報源からの情報の利用
		6	確率的技法の利用		
2	改ざん (Tampering)	8	データ構造の不正操作	4	情報システムにおける意図しないデータ変更
		9	システムリソースの不正操作	9	機密情報の（完全性の）喪失
3	否認 (Repudiation)	-	-	-	-
4	情報漏えい (Information	1	情報の収集および分析	1	人的ミスによる情報の漏えい／拡散
5	サービス妨害 (Denial of Service)	5	既存機能の不正利用	6	第三者に起因する損害
				7	ペネトレーションテストによる損害
				8	クラウド内の情報喪失
				10	デバイス、ストレージメディア、ドキュメントの紛失
				11	レコードの破壊
6	権限の昇格 (Elevation of Privilege)	2	予期しない項目を挿入（変数・命令文、等）	2	デバイス／システムの管理権限の誤用
		4	タイミングと状態の悪用	5	不適切な設計および計画、または不適当な適応
		7	アクセスコントロールの悪用（認証・承認）		

STRIDEの網羅感 2/2

他リファレンスとのマッピング

STRIDE		NIST SP 800-30 (Threat Events Achieve Results)	
No	項目	No	項目
1	なりすまし (Spoofing)	9	機微な情報を漏らすことによって、正規の権限によらない開示および／または利用不能を引き起こす
2	改ざん (Tampering)	5	公的にアクセス可能な情報システム上にデータを作成したり、システム上のデータを削除したり、あるいはデータを変更することによって、完全性の喪失を引き起こす
		6	極めて重要なデータを汚染する、あるいは改ざんすることによって、完全性の喪失を引き起こす
		7	もっともらしいが偽のデータを組織の情報システムに挿入することによって、完全性の喪失を引き起こす
3	否認 (Repudiation)		-
4	情報漏えい (Information	1	外部ネットワークのネットワークスニッフィングを介して、機微な情報を取得する
		2	機微な情報を取り出して、取得する
		8	アクセス権限のあるユーザによる、極めて重要な情報および／または機微な情報の開示を引き起こす
		10	外部に設置された傍受用デバイスを使用して、無線ネットワークトラフィックを傍受し、情報を取得する
		12	公的にアクセス可能な情報システムから、機微なデータ／情報を取得する
		13	機会を伺って情報システム／コンポーネントを盗んだり、あさることによって、情報を取得する
5	サービス妨害 (Denial of Service)	3	アタッカーが選択したサービスまたは機能の低下または提供拒否を引き起こす
		4	基幹業務に関わる情報システムコンポーネントおよび機能の低下／破壊を引き起こす
6	権限の昇格 (Elevation of	11	不正なアクセスを行う

【Appendix G】

ガイドラインとの連携

脅威分析とガイドラインのつながり

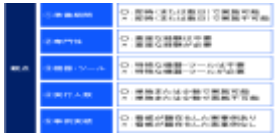
脅威分析の結果は、ガイドラインのインプットとして連携

脅威分析

デバイス	論理レベルでの脅威シナリオ（例）	脅威の分類
3G/4G 送受信装置	遠隔から外部システムになりすまし、虚偽のソフトウェア更新情報を流し込み、異常な走行機能制限を発生させる	Spoofing（なりすまし）
	遠隔から通信上のソフトウェア更新情報を改ざんし、走行制御に関するソフトウェアを書き換える	Tampering（改ざん）
	…	
	…	Repudiation（否認）
DSRC専用 通信端末	攻撃対象の車両に接近し、ホットスポットやフリーWi-Fiを模したアクセスポイントを提供し、これに接続した車両からのWi-Fi通信上の情報を窃取する	
	…	Information Disclosure（情報漏えい）
	…	
Bluetooth	…	Denial of Service（サービス妨害）
	…	
…	…	Elevation of Privilege（権限の昇格）

脅威レベルの評価

顕在化率



＋

影響度

脅威レベルの決定

脅威レベルの高い車載通信デバイスの評価を実施

脅威の分類に応じたガイドラインへの反映

情報セキュリティ評価ガイドライン
ドラフト（本編）
ver.2.0
2018年MM月DD日発行

該当箇所

第2章
車両を取り巻く脅威の全体像

付録1
想定される一般的な脅威一覧

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

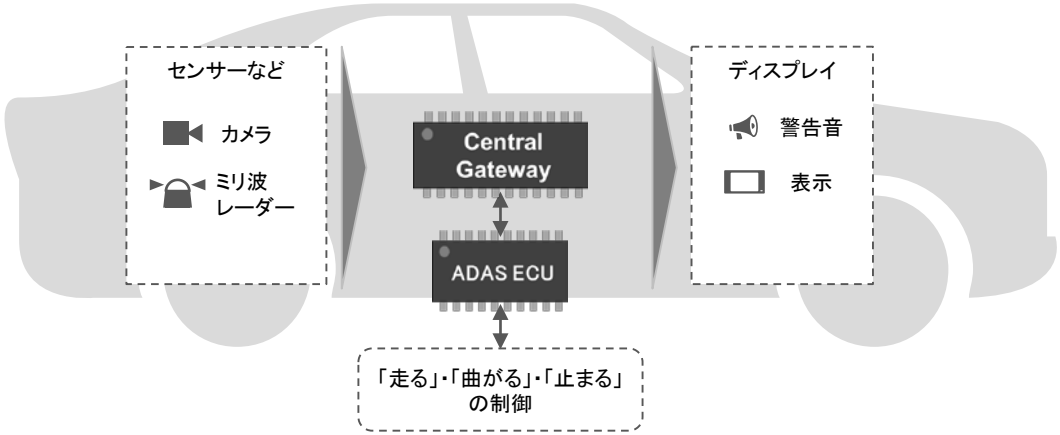
実装済み	開発中

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

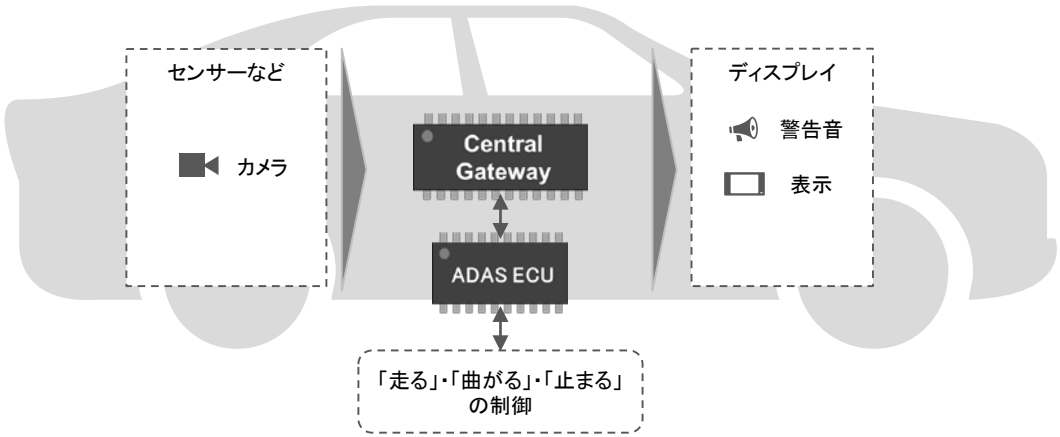
実装済み	開発中

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

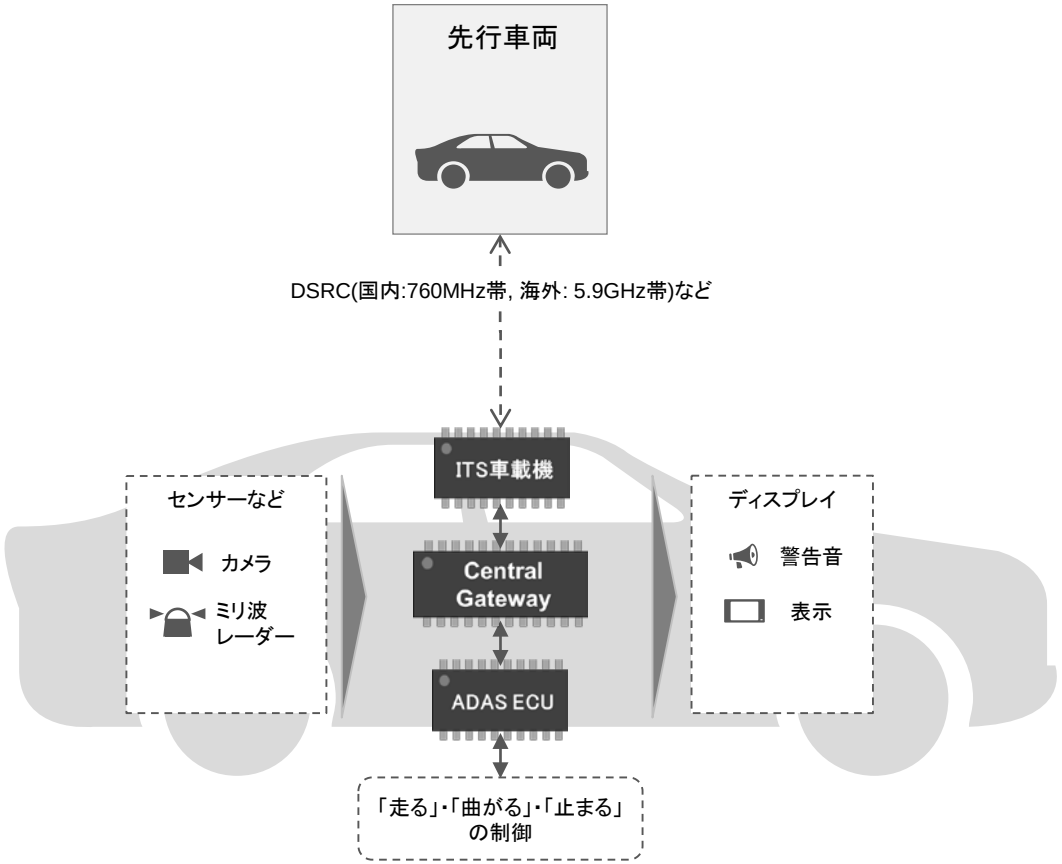
2. 実装状況

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

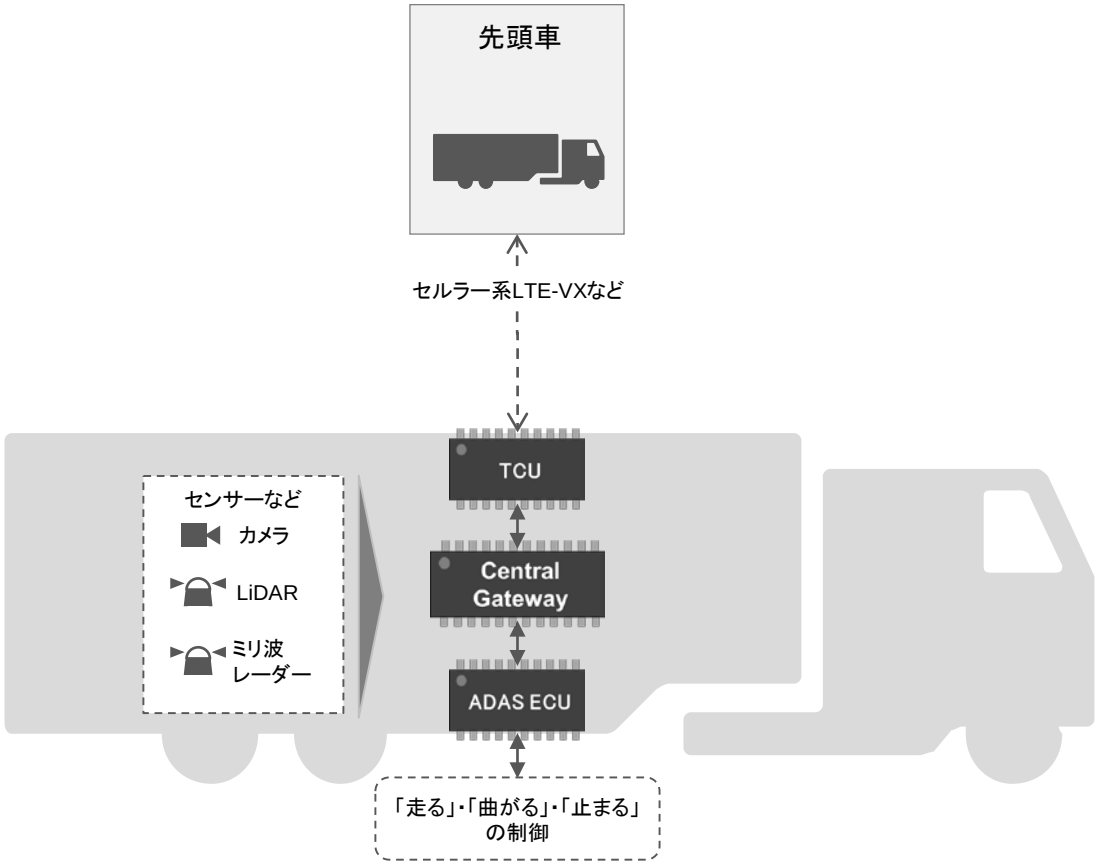
2. 実装状況

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

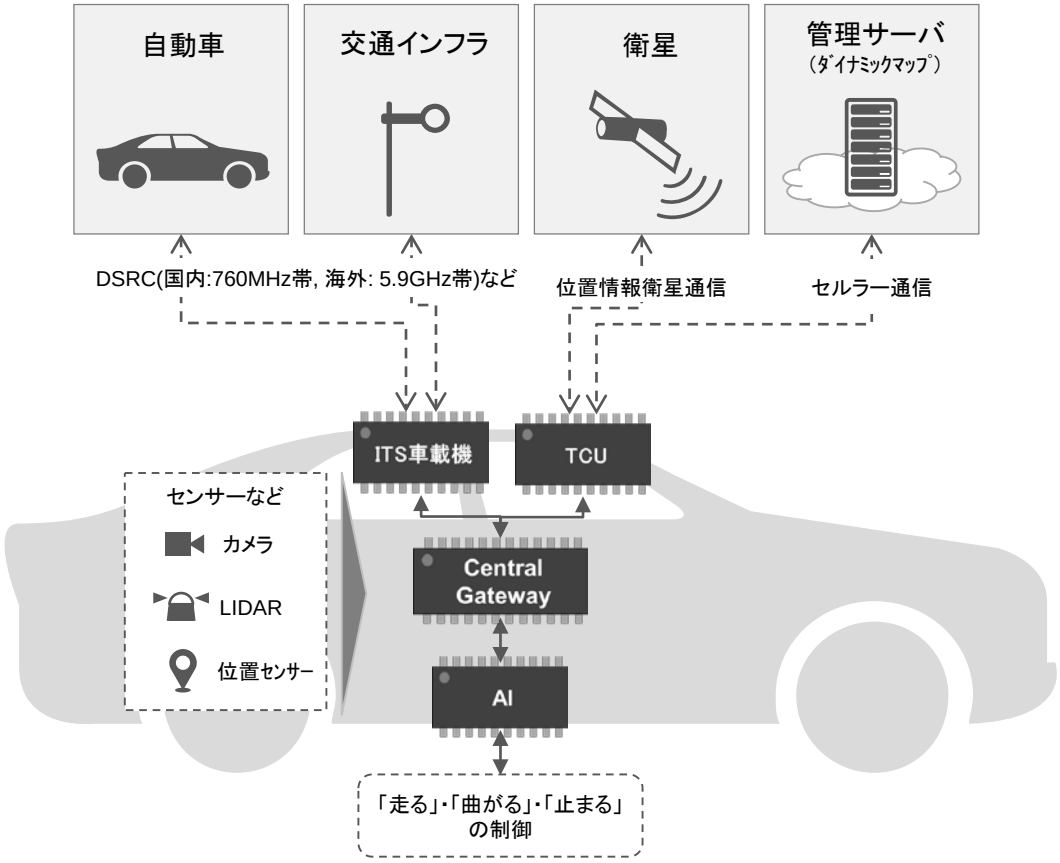
2. 実装状況

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

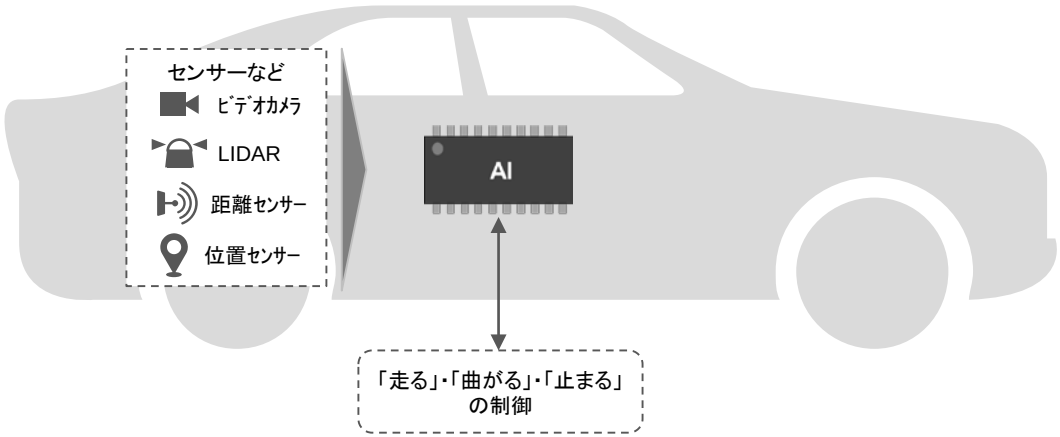
実装済み	開発中

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

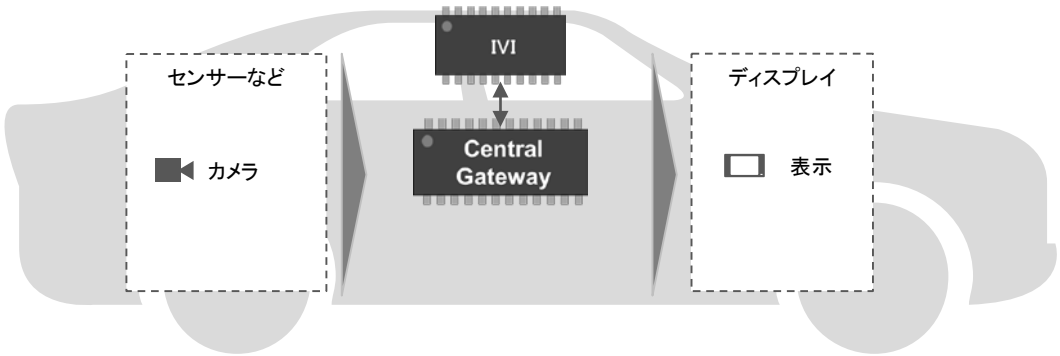
実装済み	開発中

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

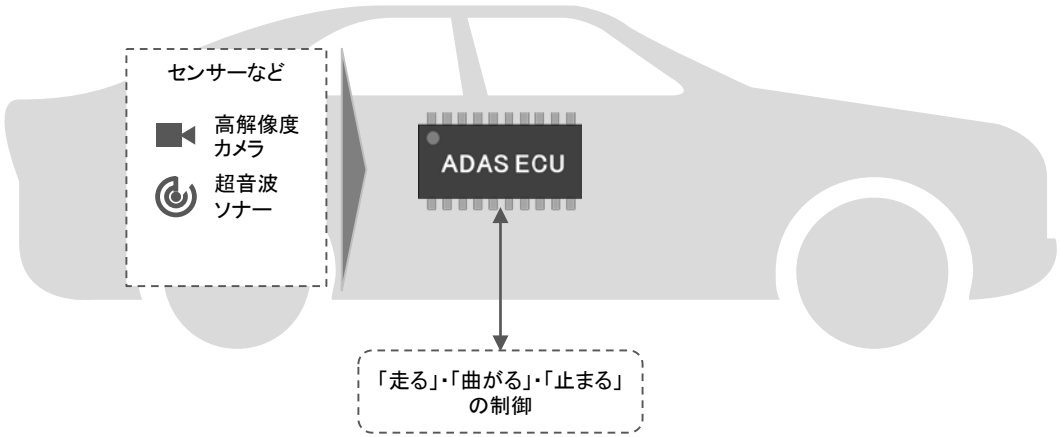
実装済み	開発中

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

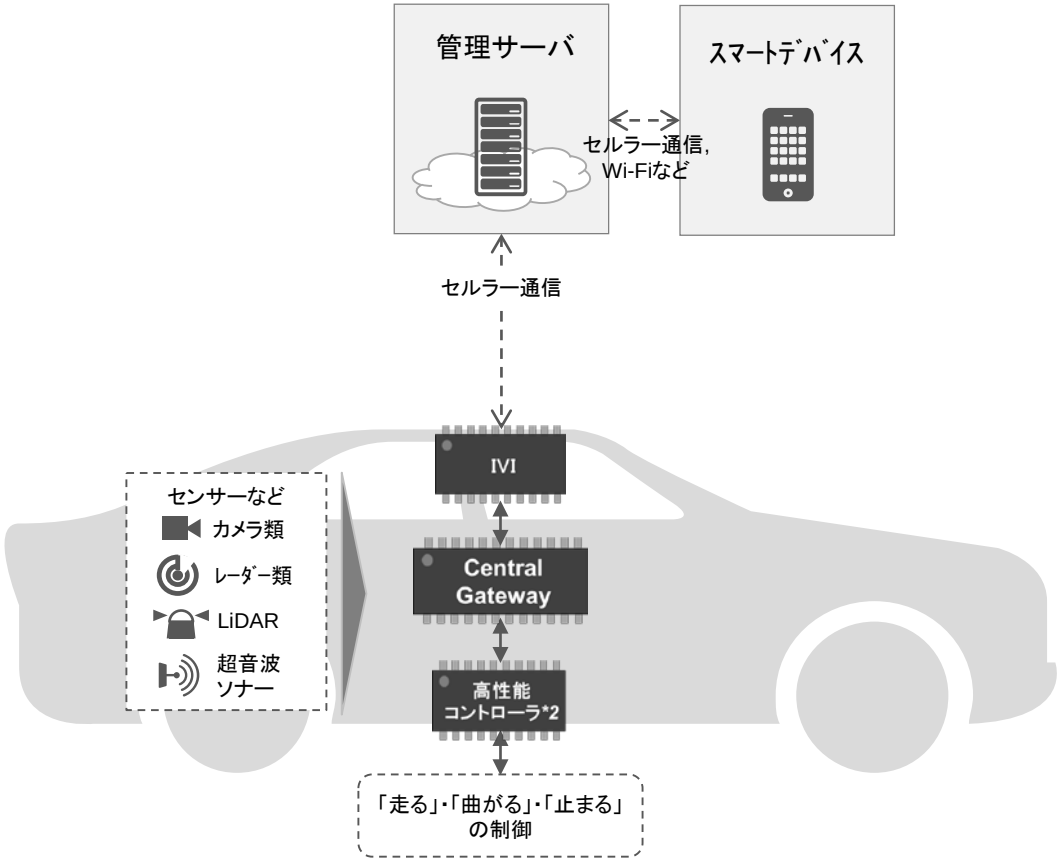


1-9. 自動駐車（スマホ連携）

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

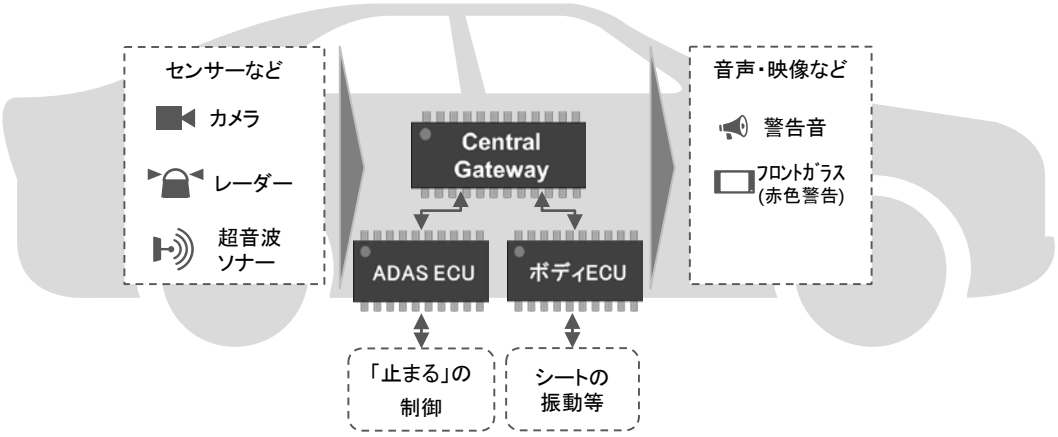
実装済み	開発中

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。

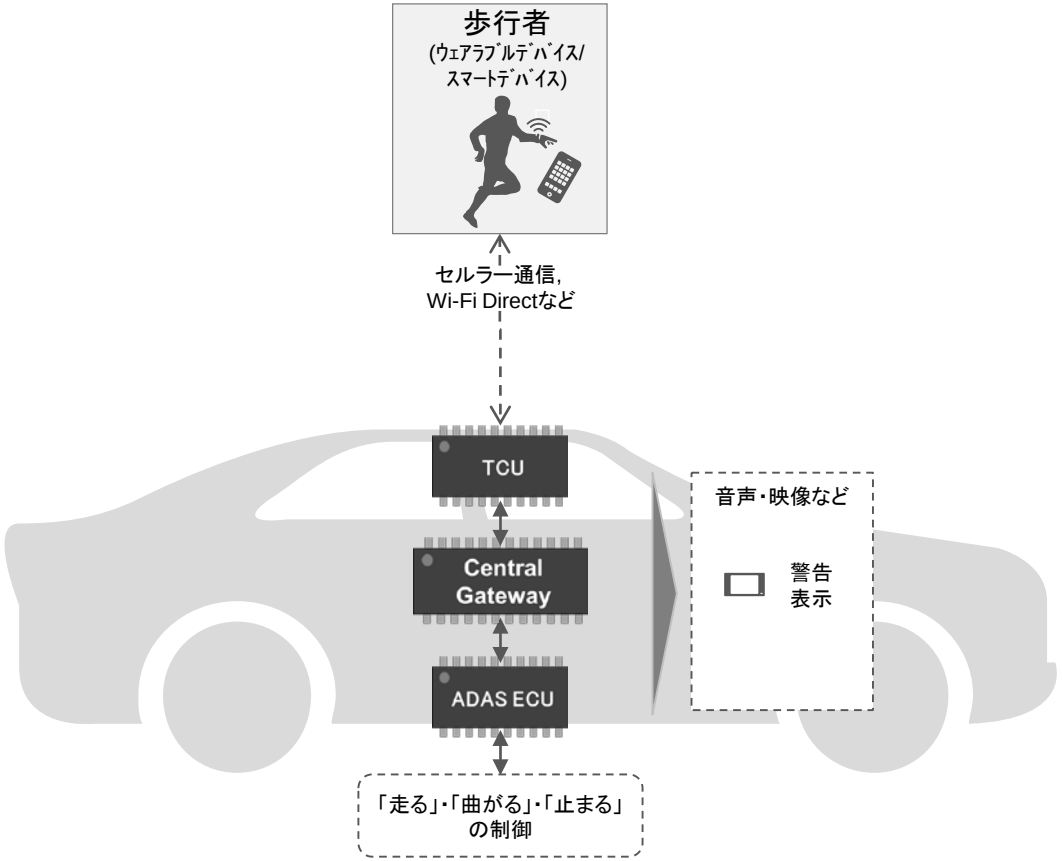
2. 実装状況

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

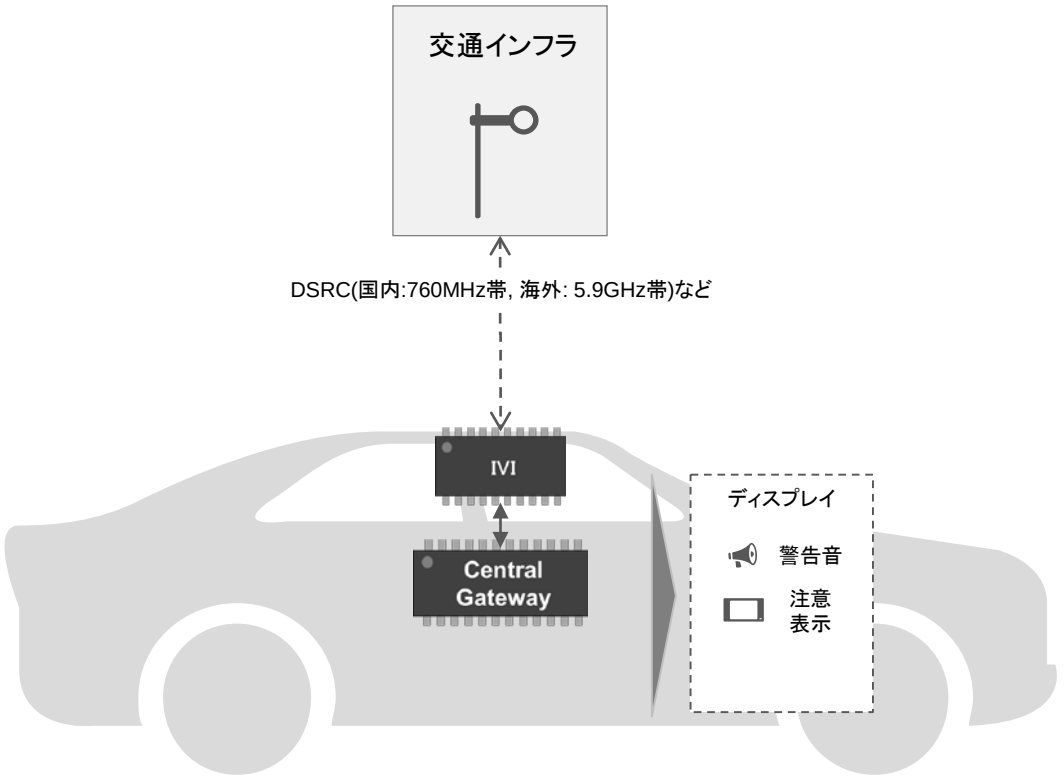
2. 実装状況

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

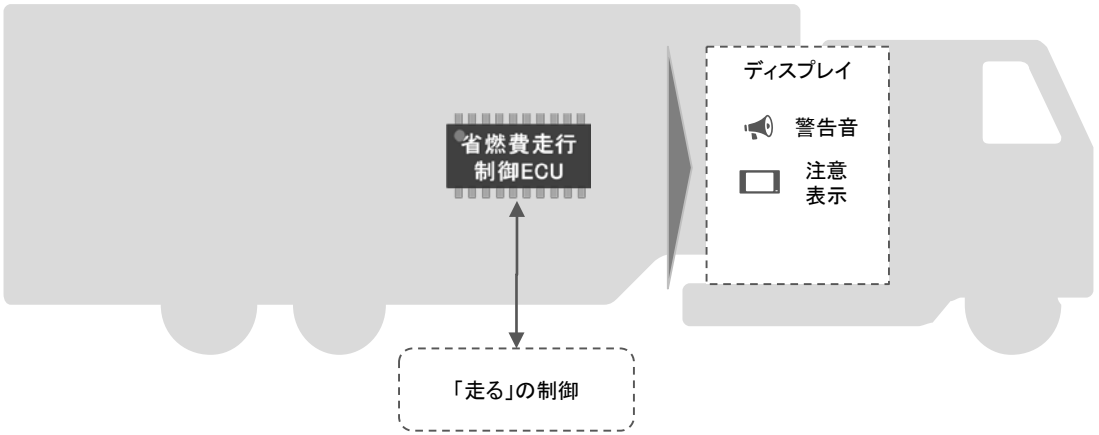
実装済み	開発中

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。

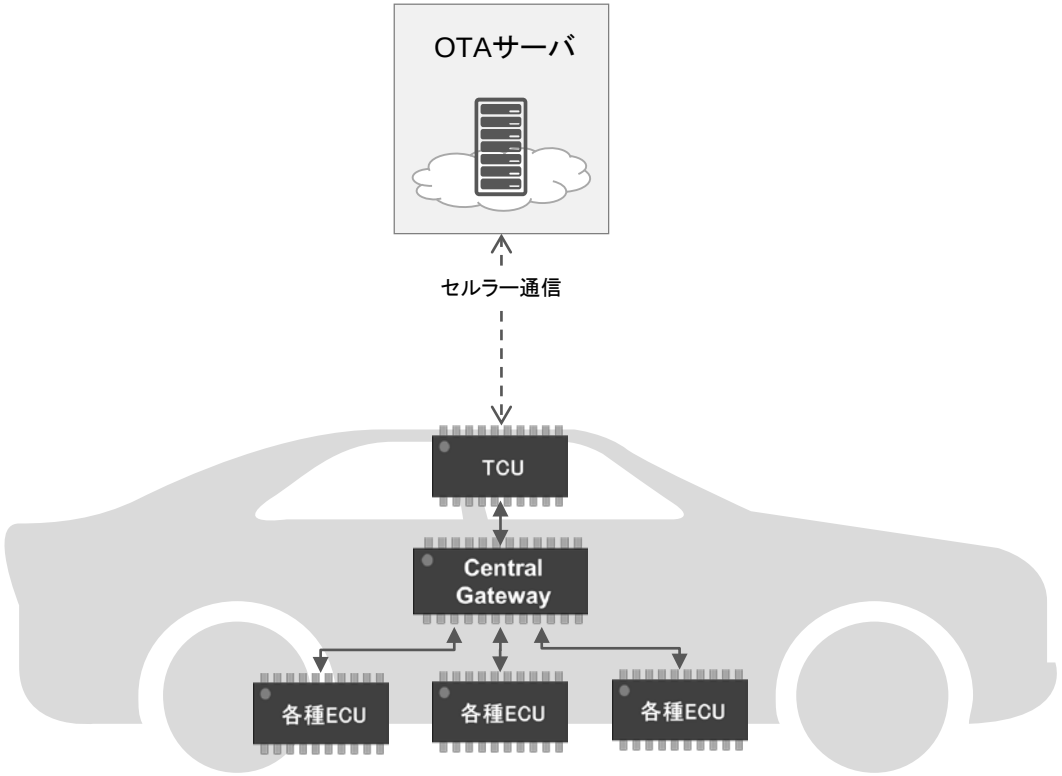
2. 実装状況

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。

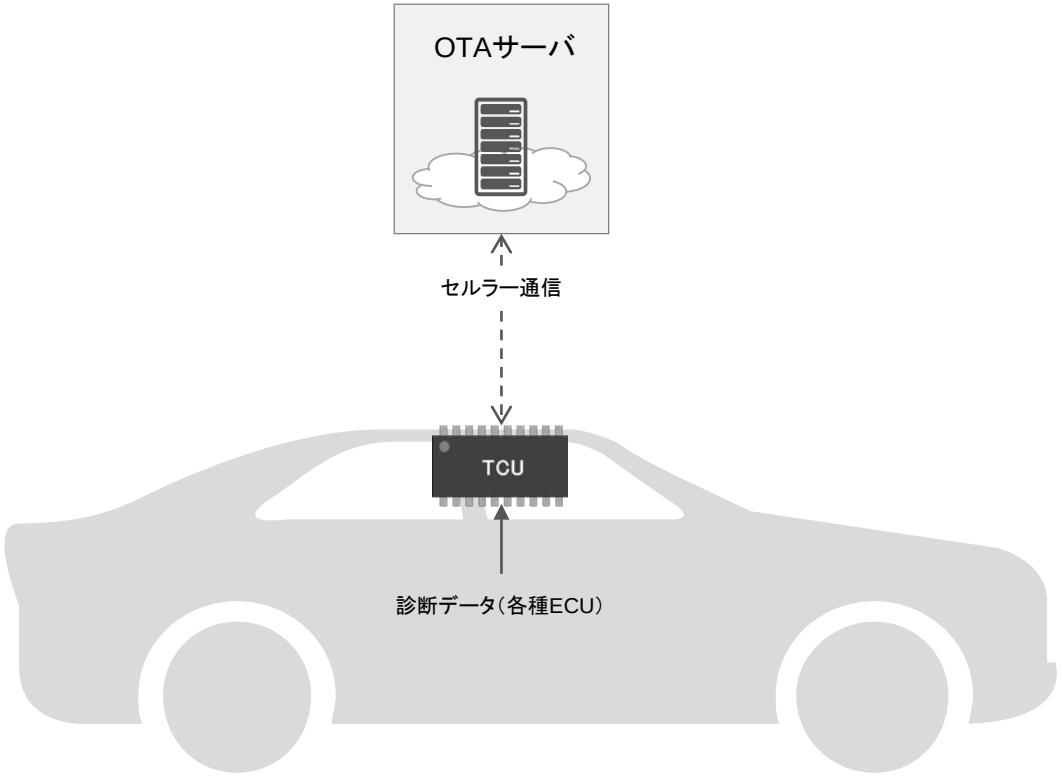
2. 実装状況

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。

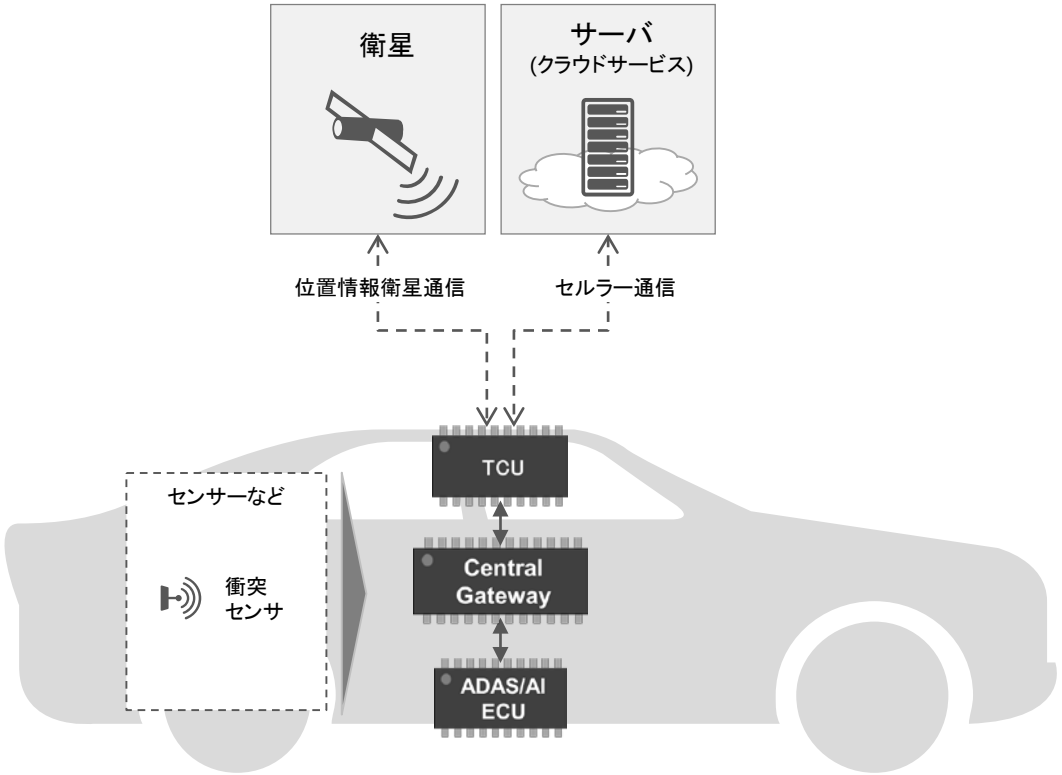
2. 実装状況

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。

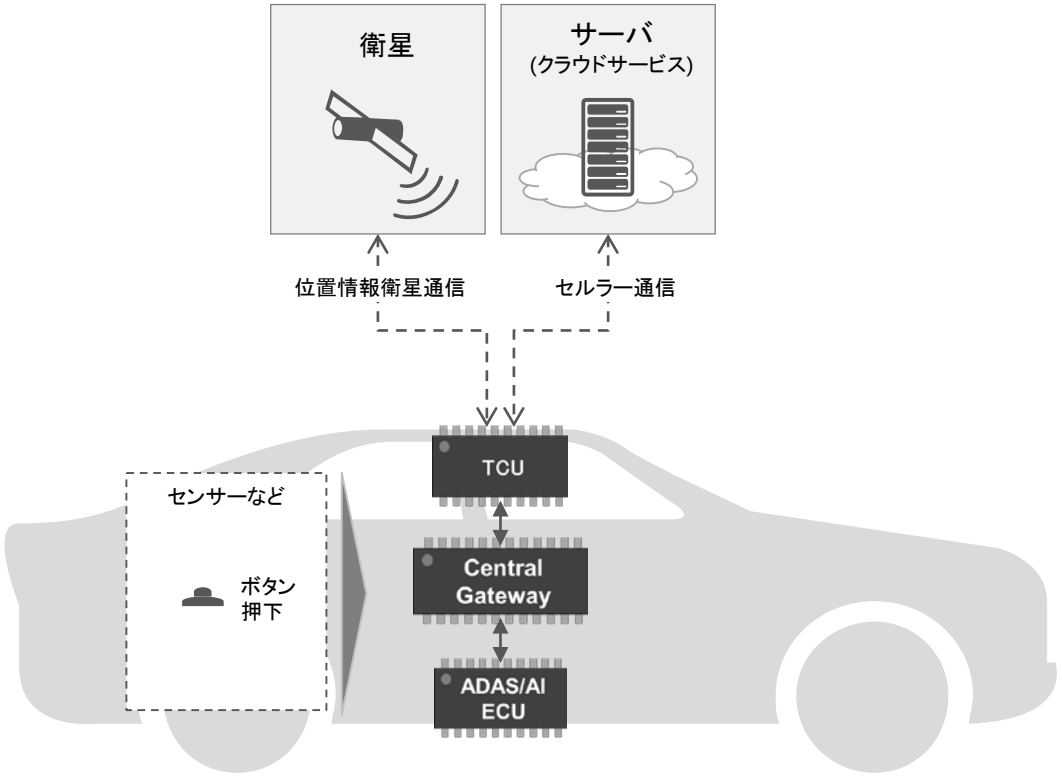
2. 実装状況

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

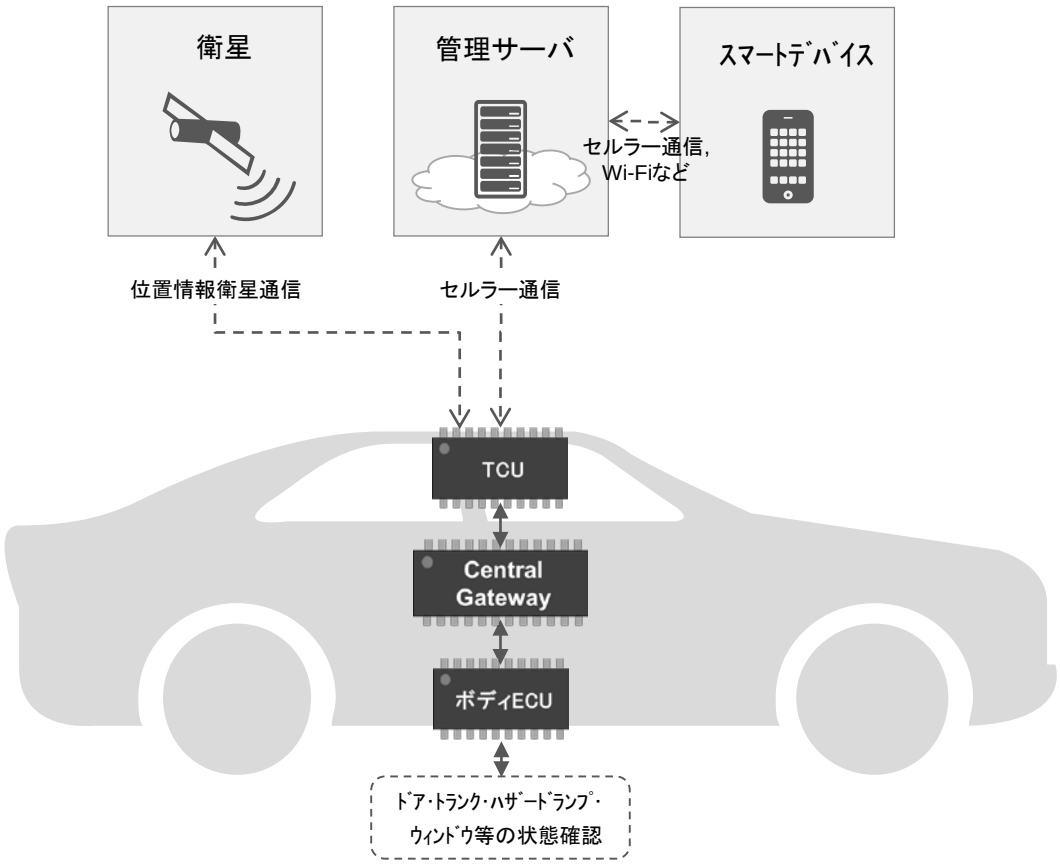
2. 実装状況

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。

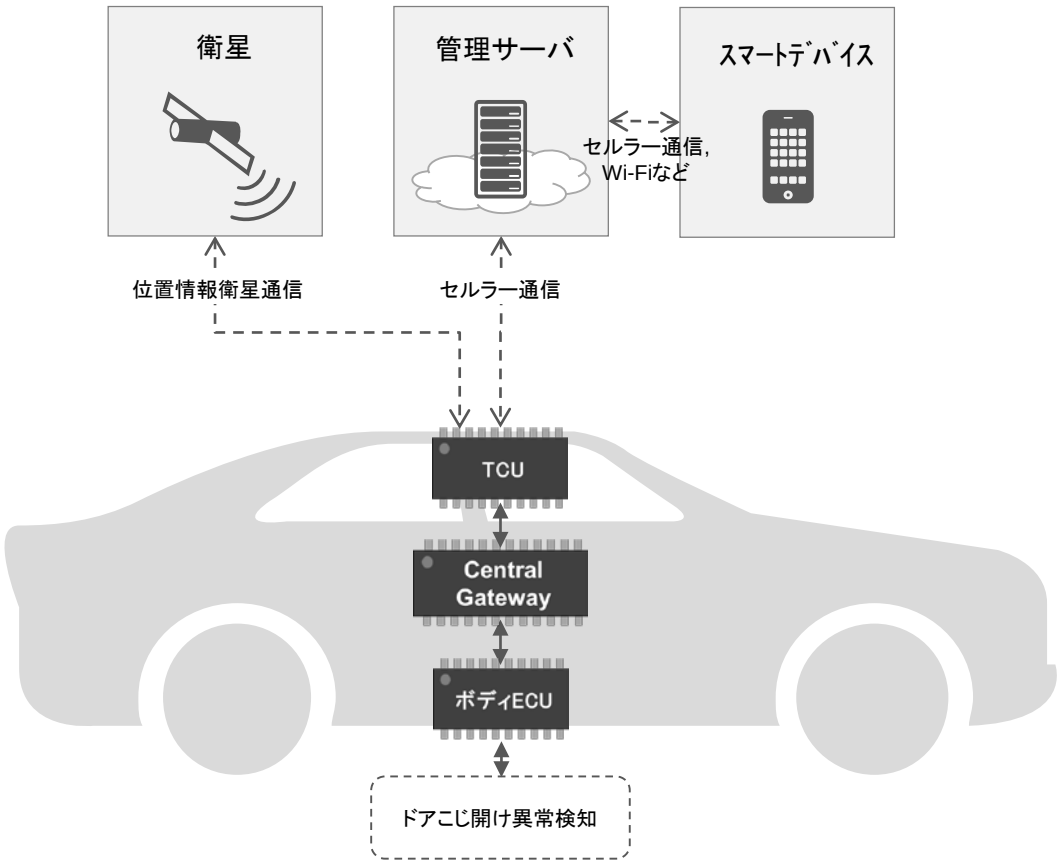
2. 実装状況

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。

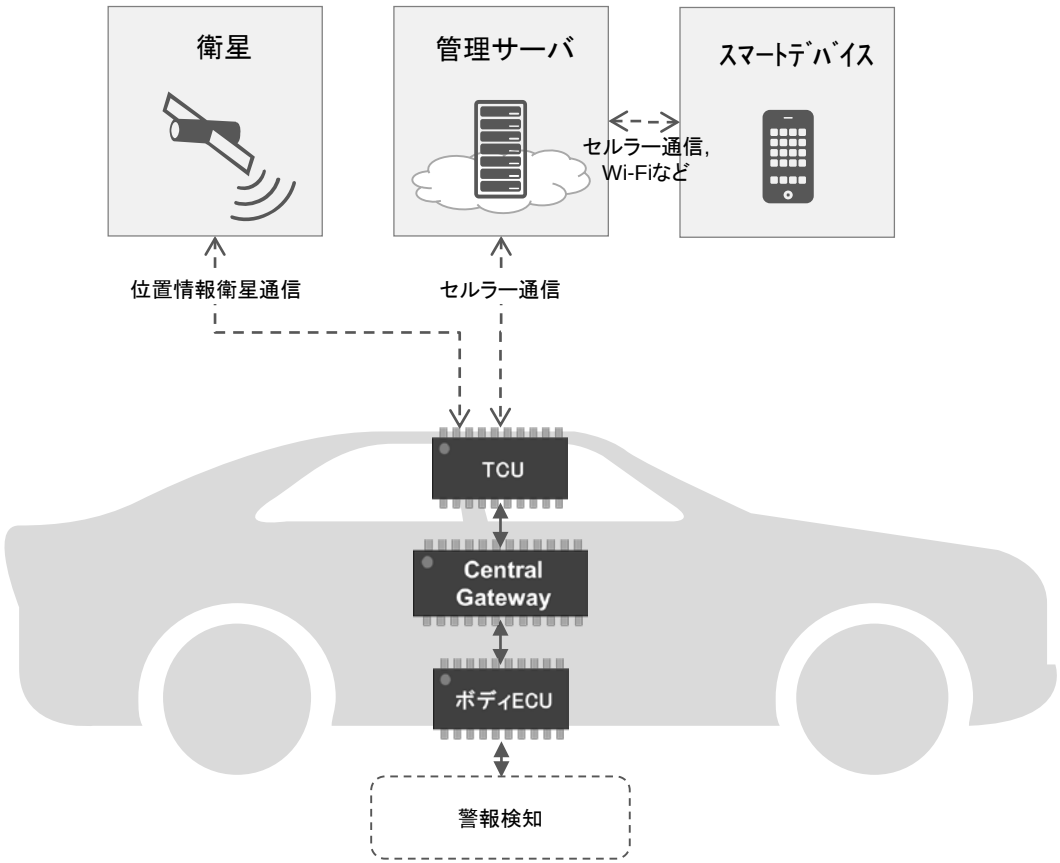
2. 実装状況

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。

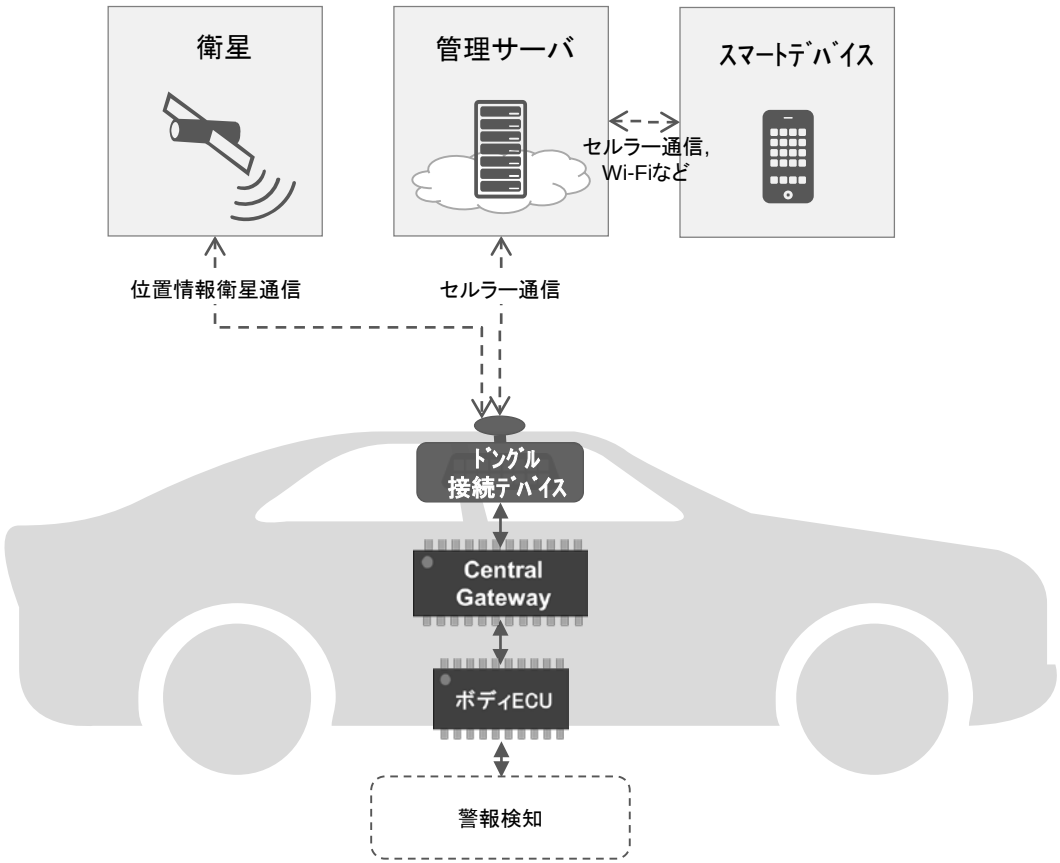
2. 実装状況

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。

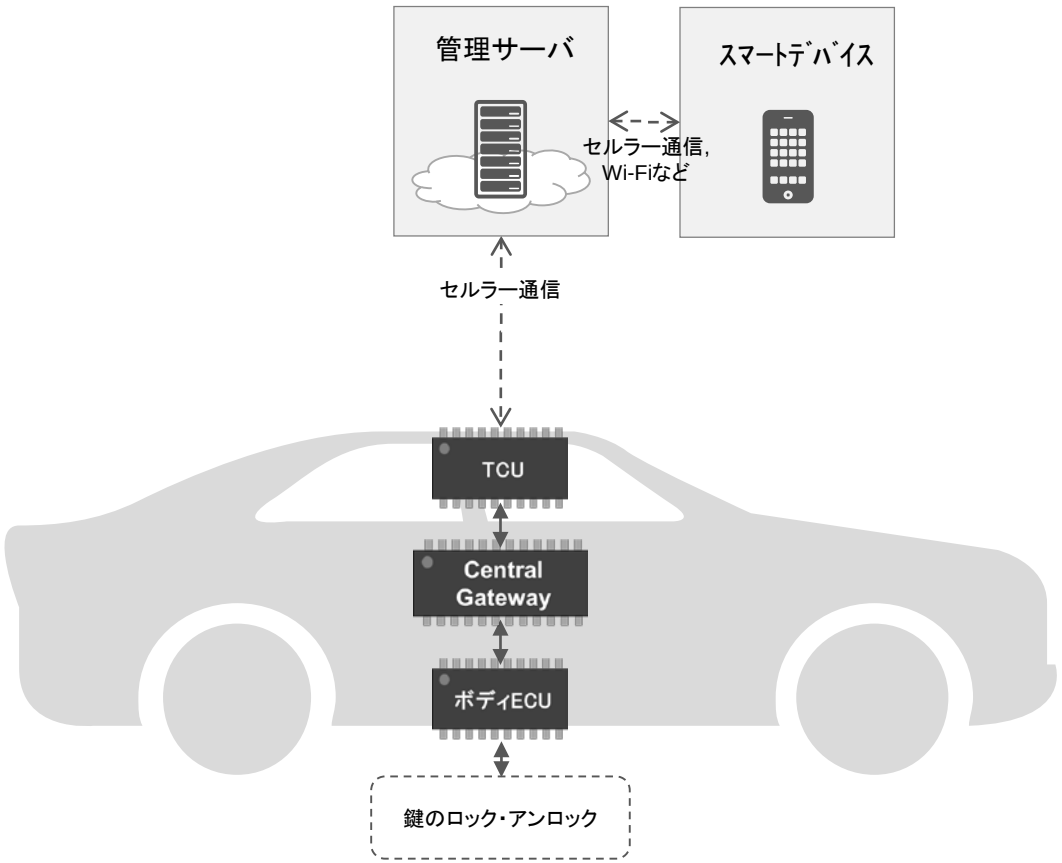
2. 実装状況

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。

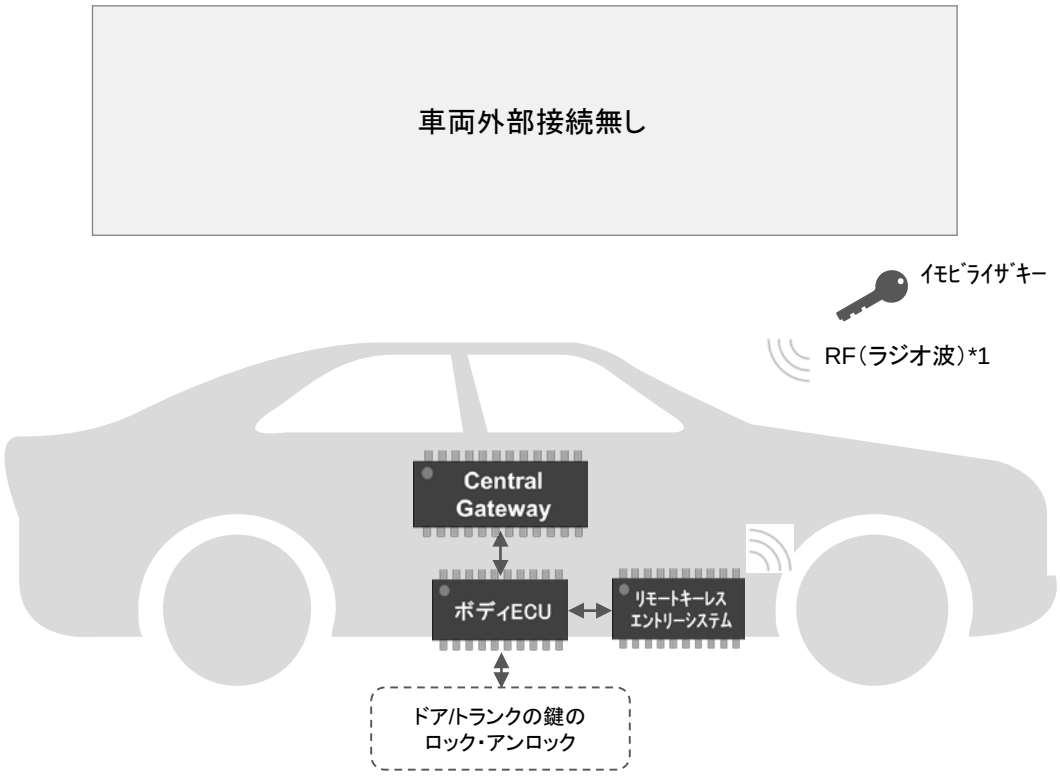
2. 実装状況

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。

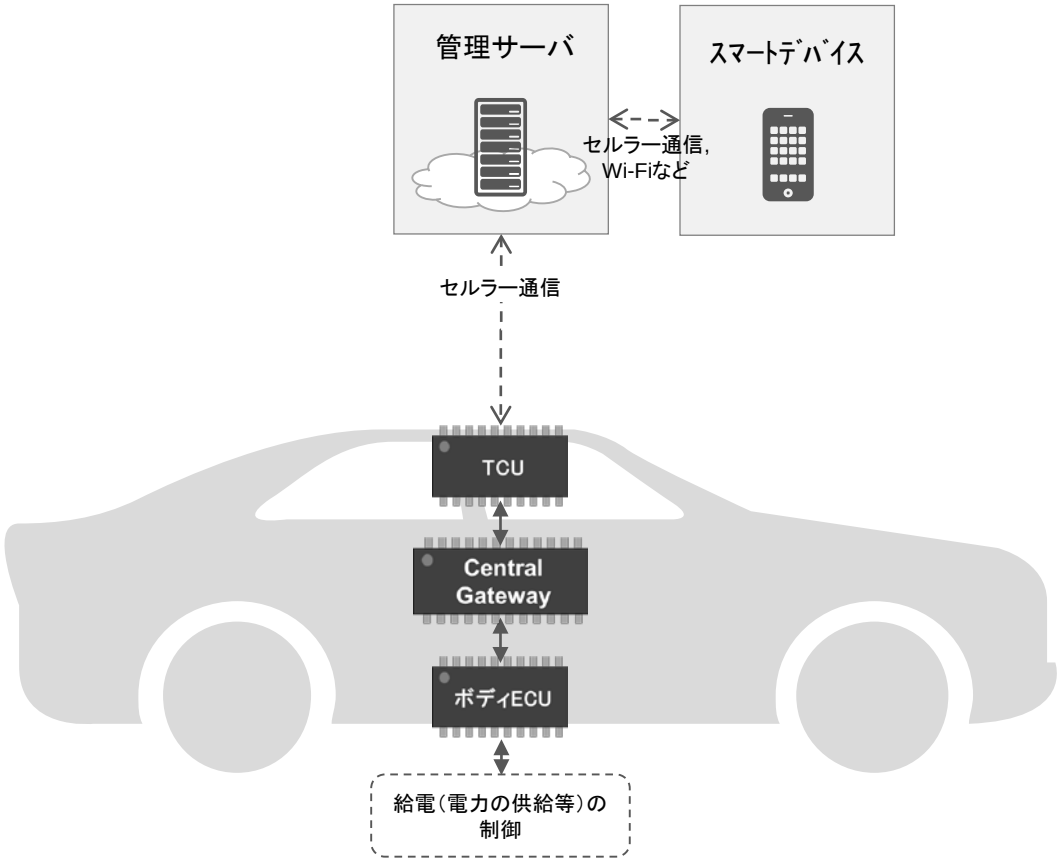
2. 実装状況

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。

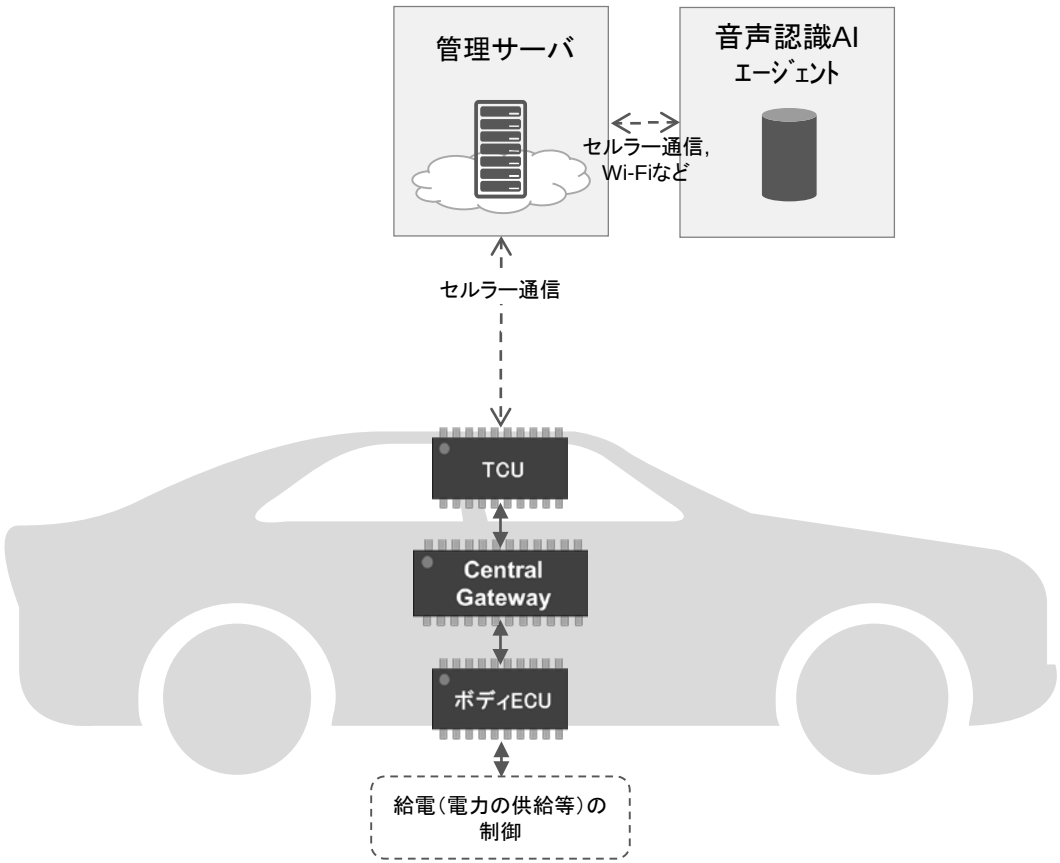
2. 実装状況

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。

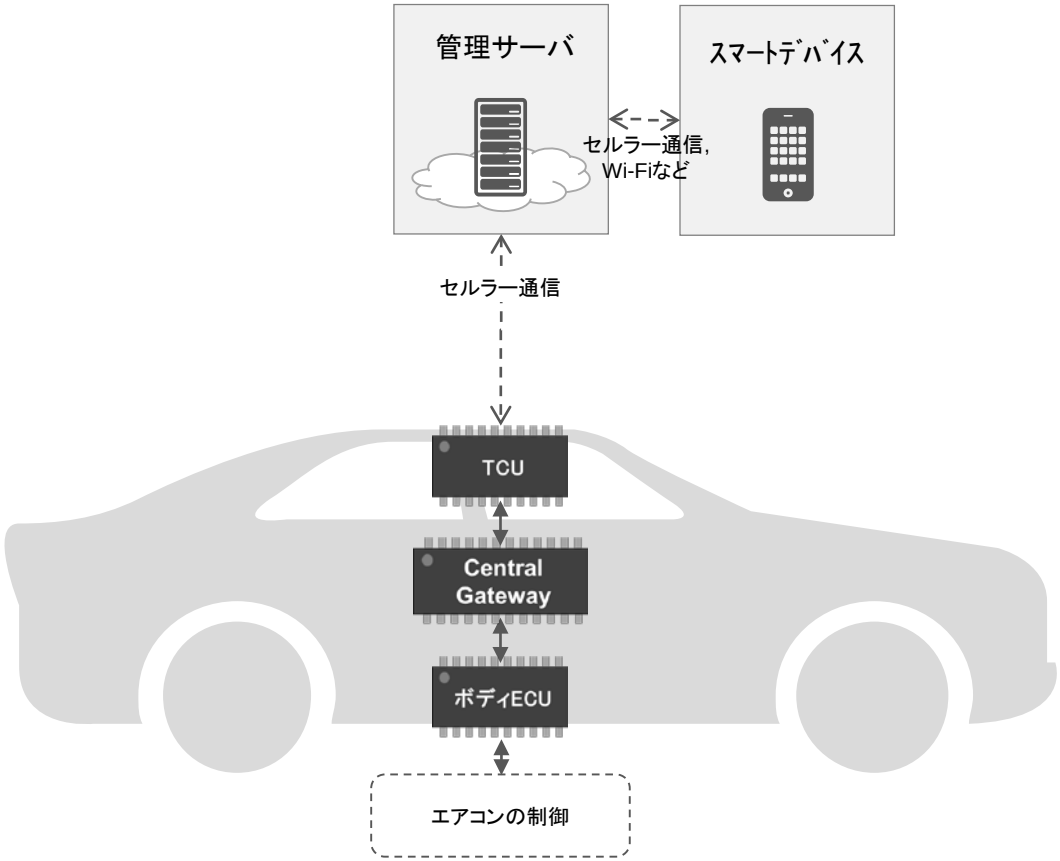
2. 実装状況

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。

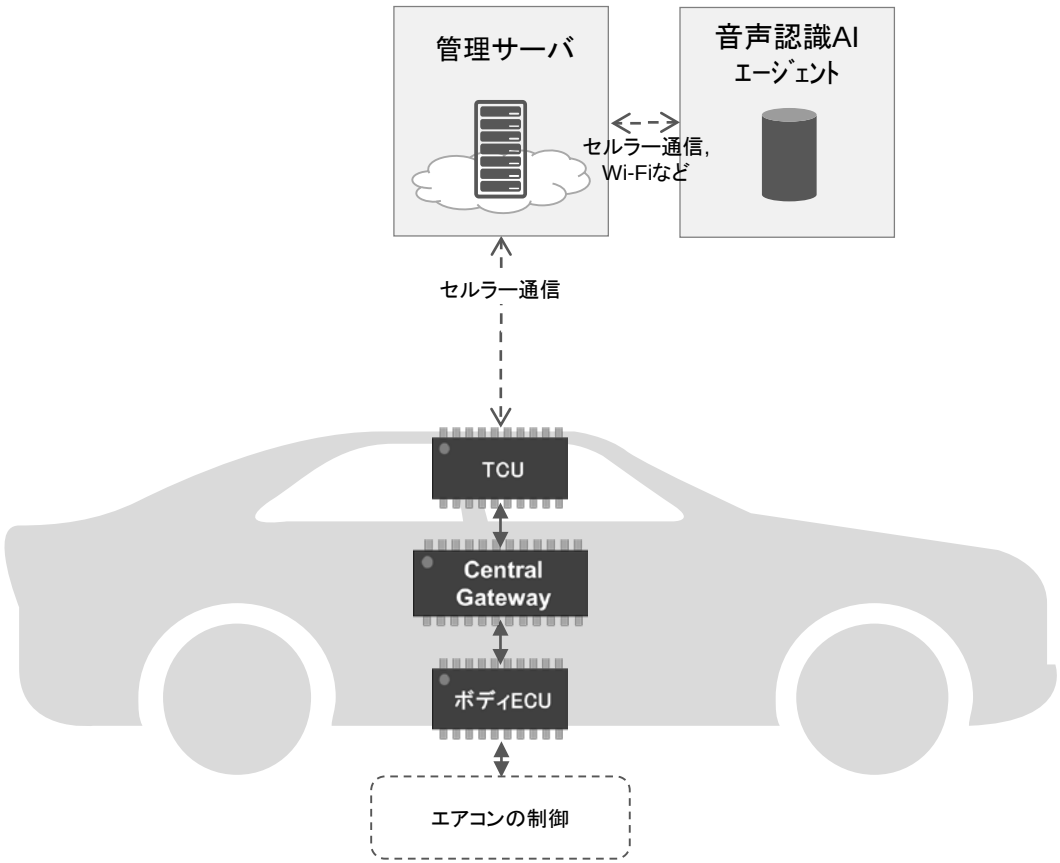
2. 実装状況

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。

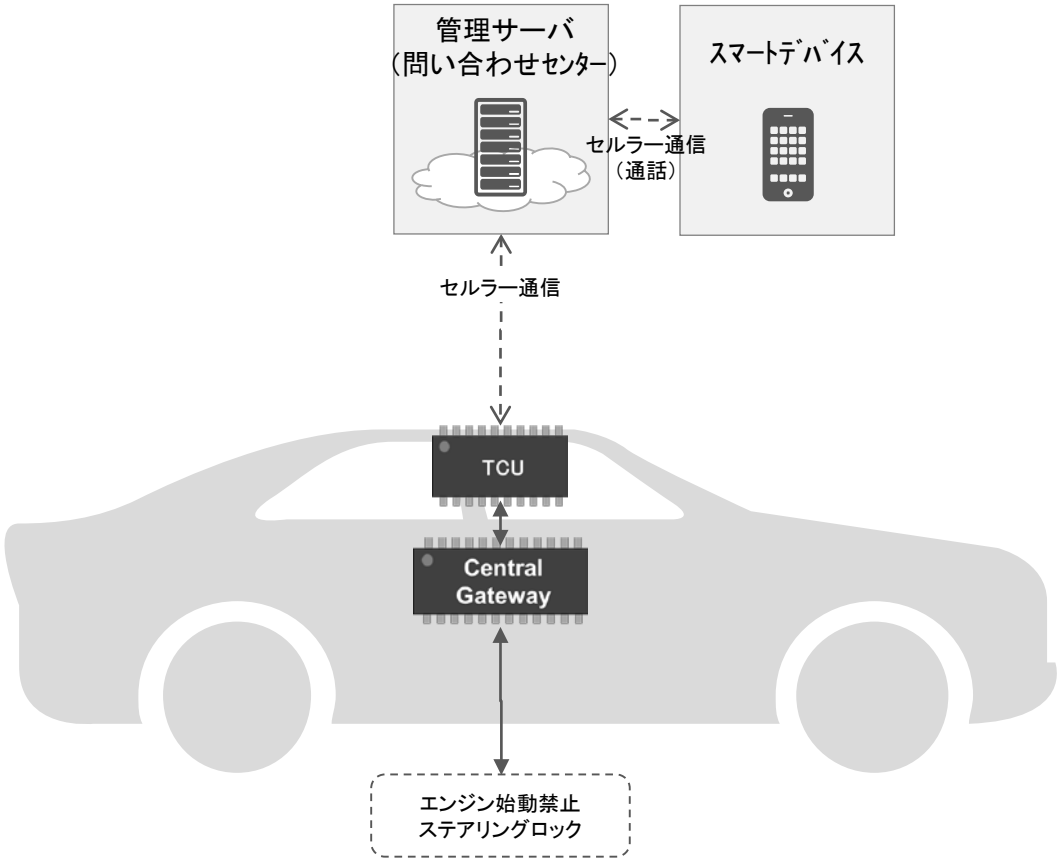
2. 実装状況

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。

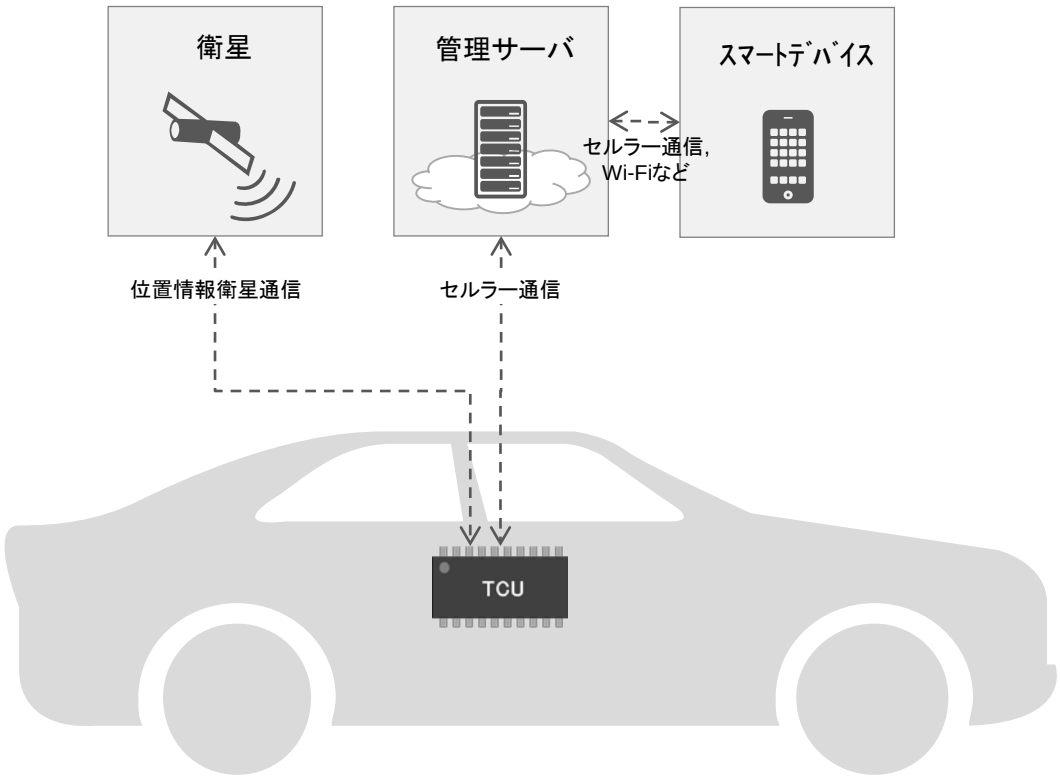
2. 実装状況

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。

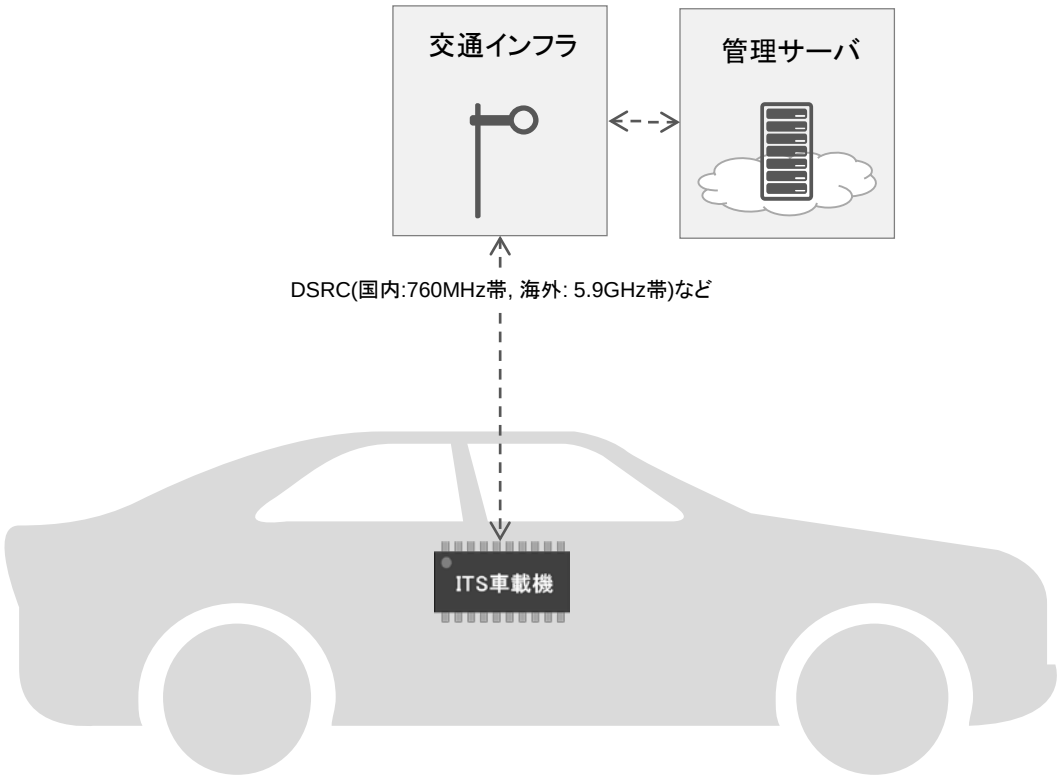
2. 実装状況

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。

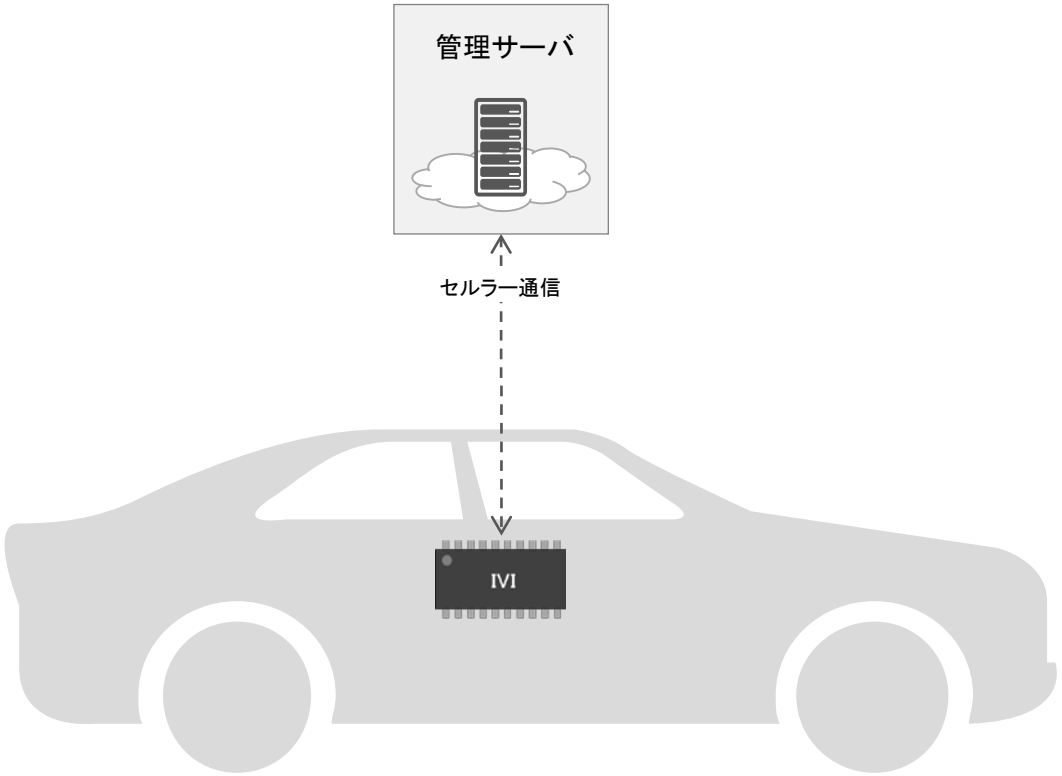
2. 実装状況

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。

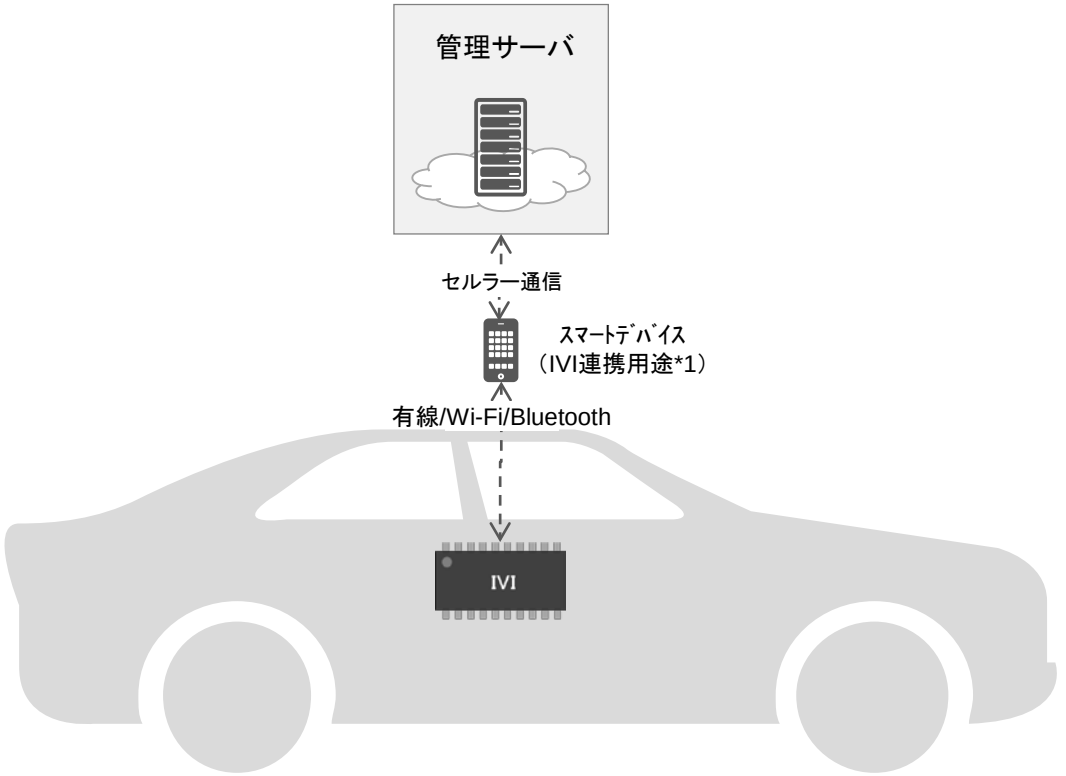
2. 実装状況

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。

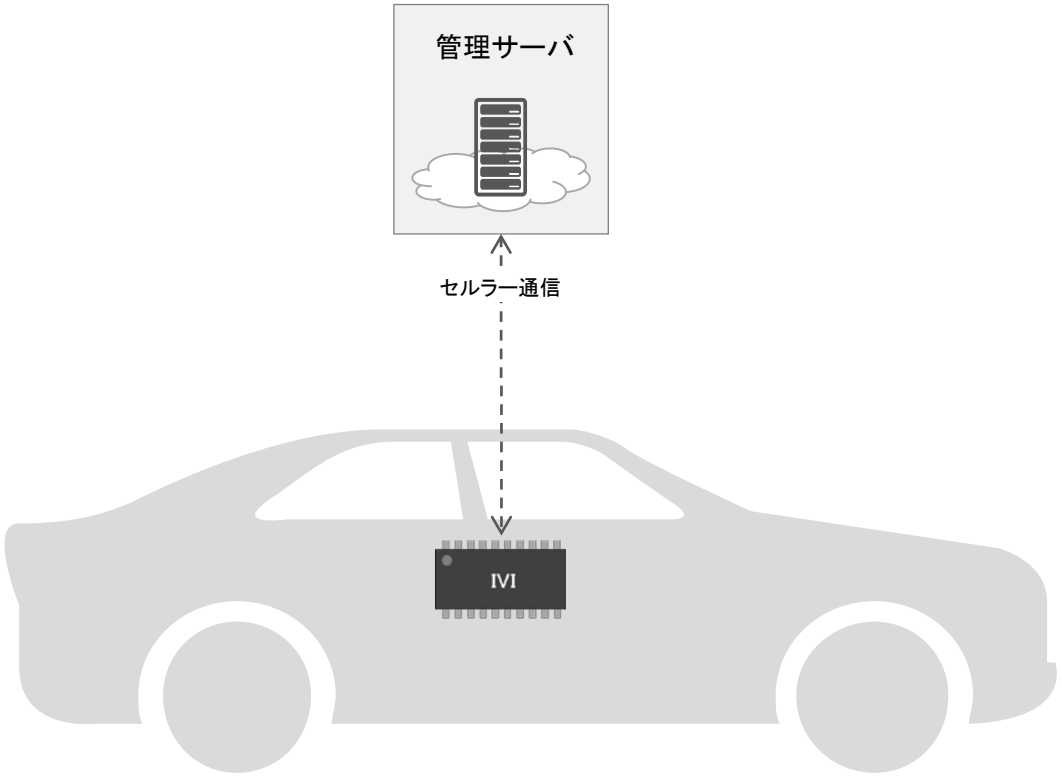
2. 実装状況

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。

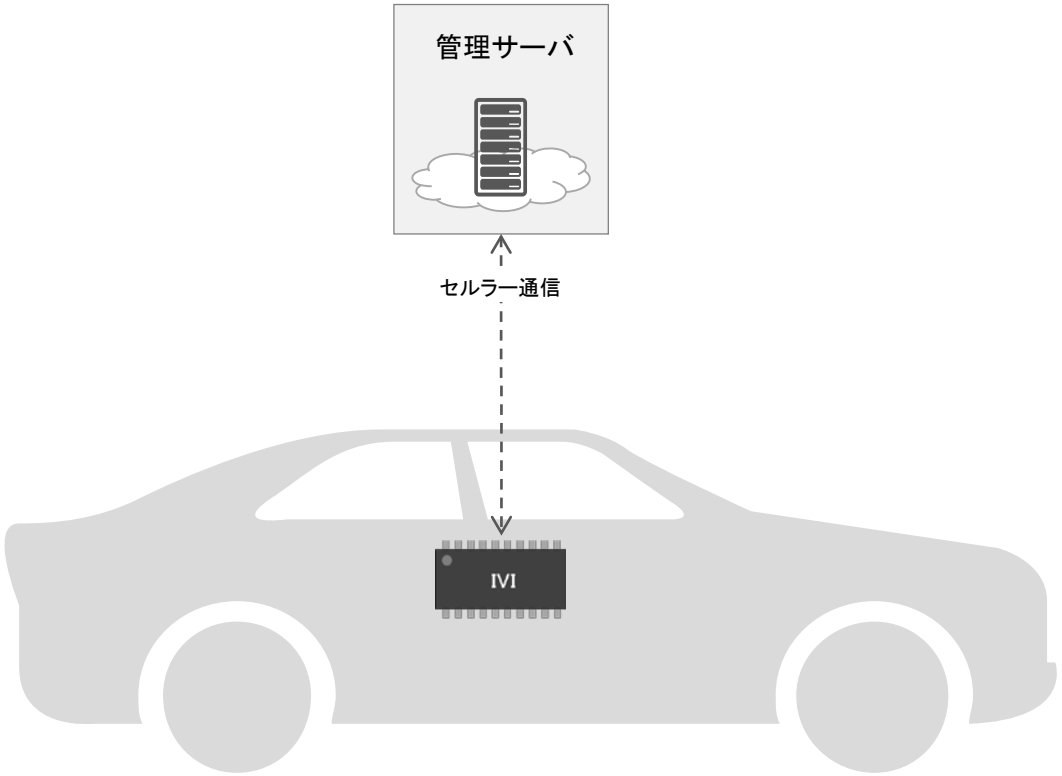
2. 実装状況

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。

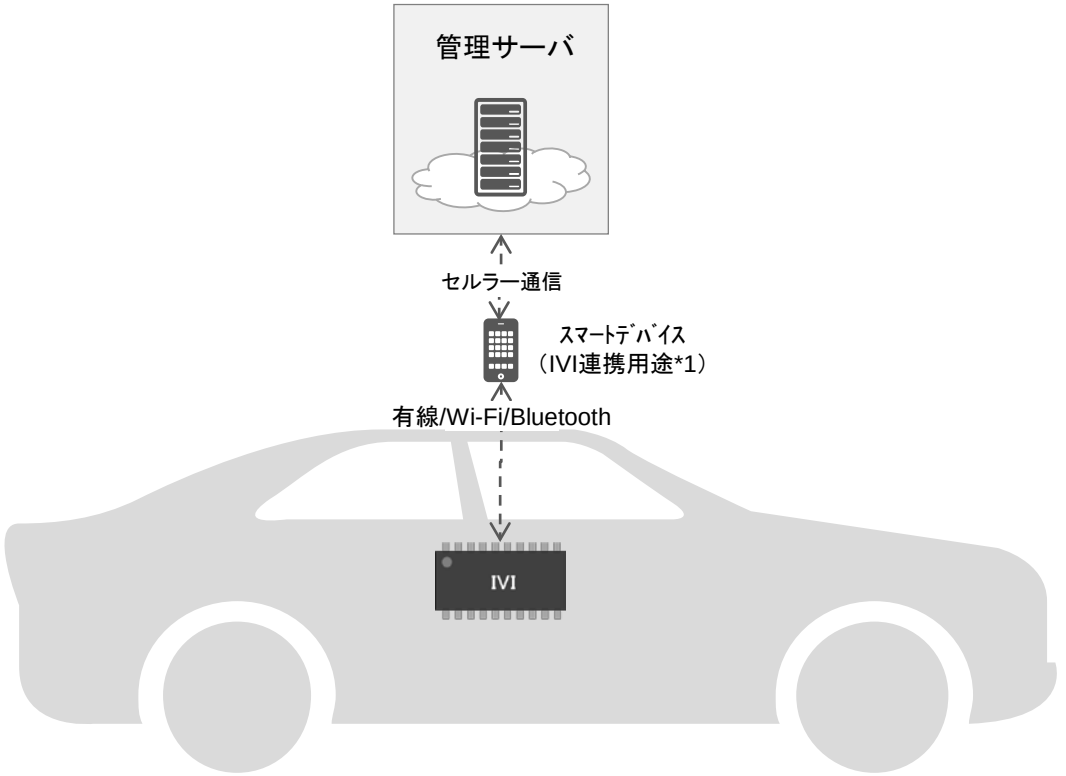
2. 実装状況

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。

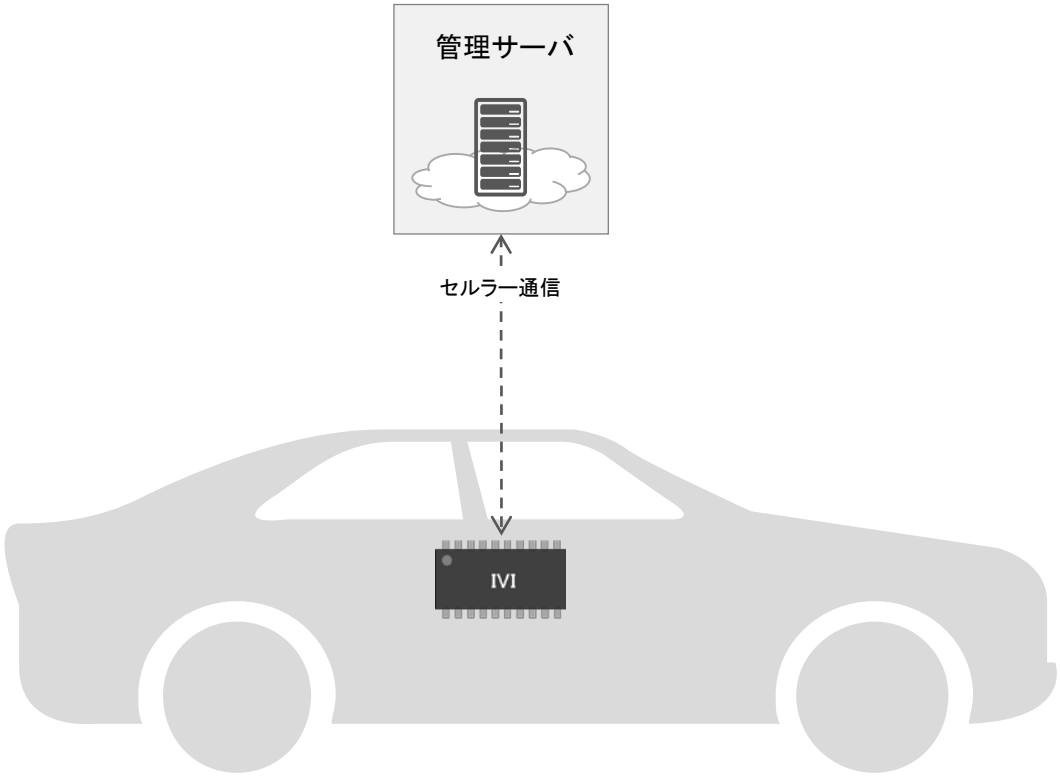
2. 実装状況

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。

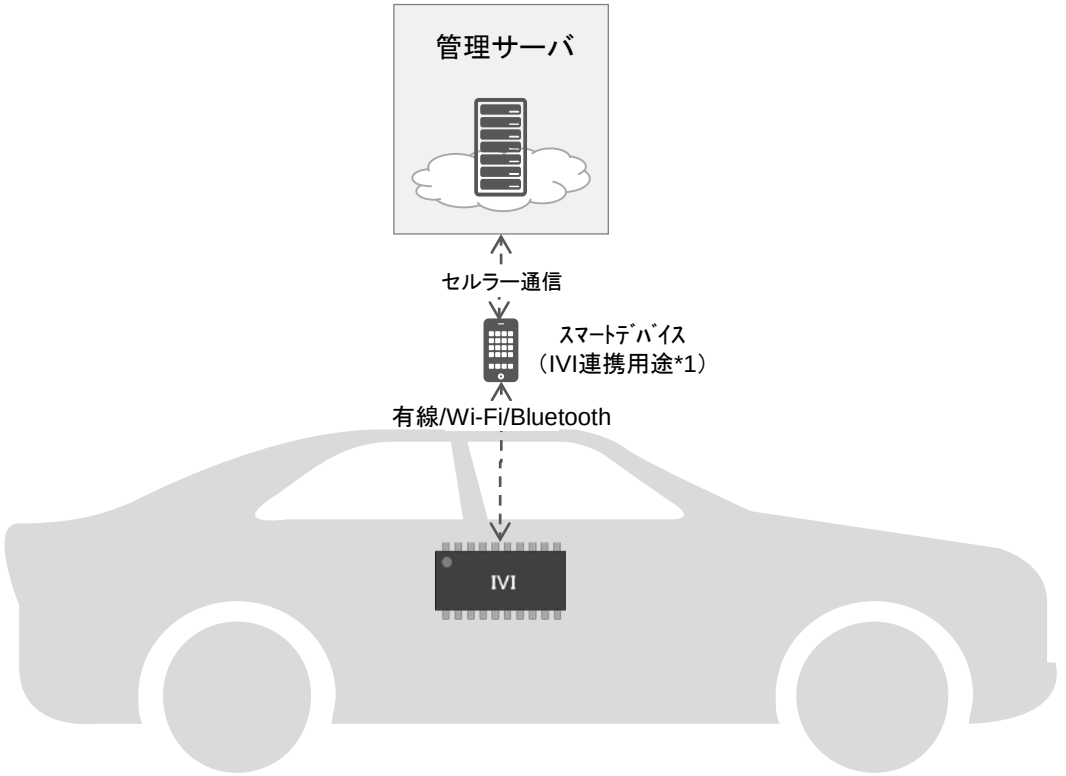
2. 実装状況

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。

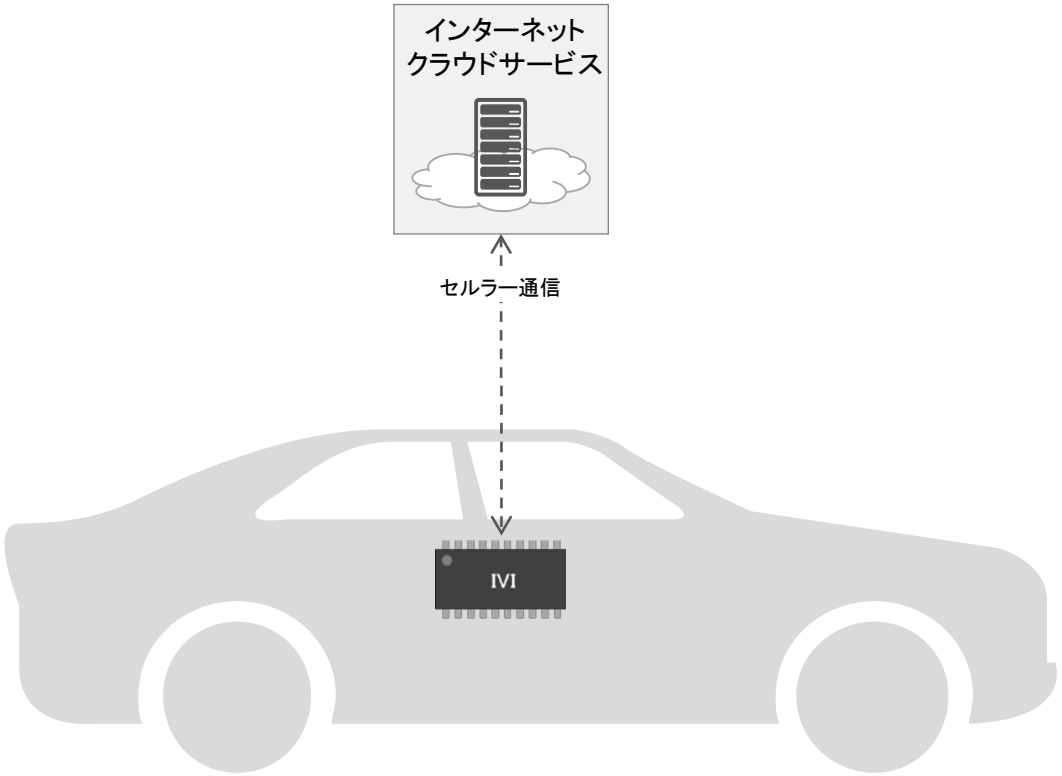
2. 実装状況

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。

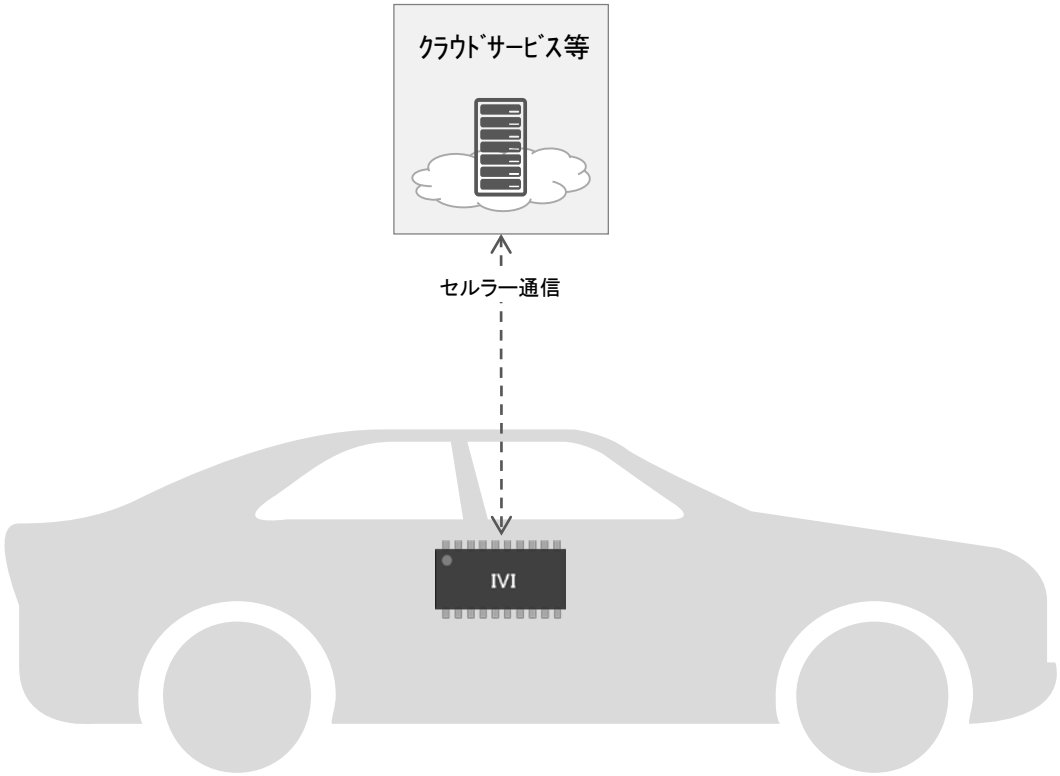
2. 実装状況

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。

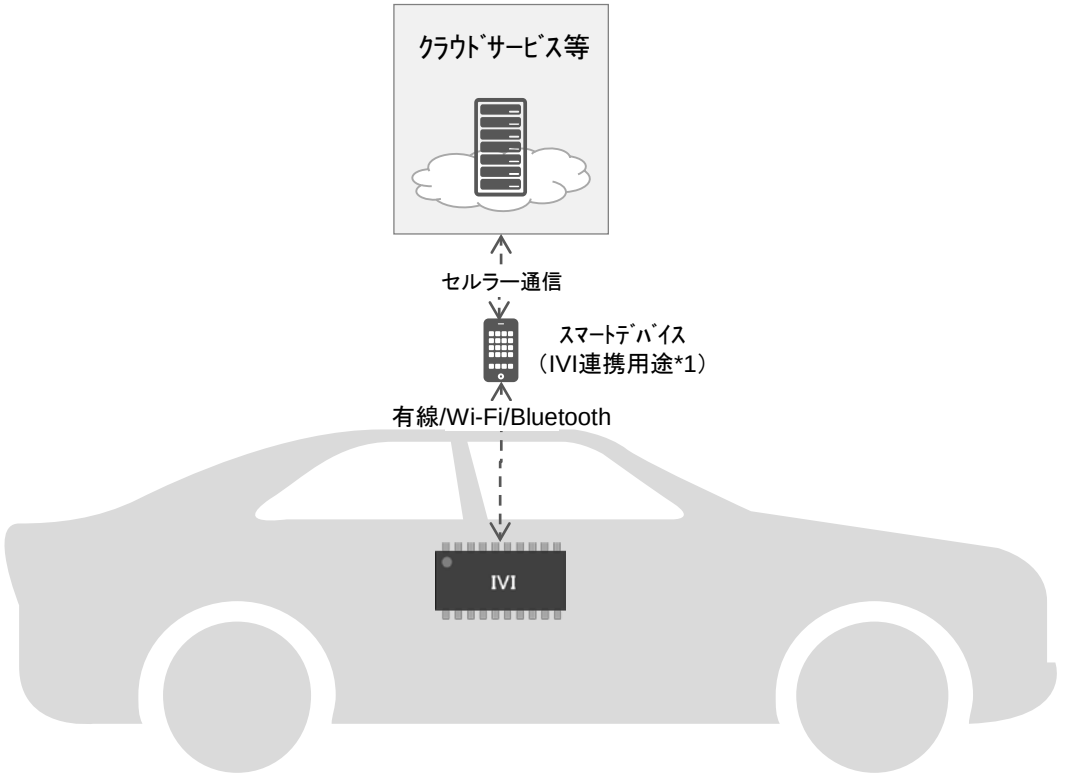
2. 実装状況

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



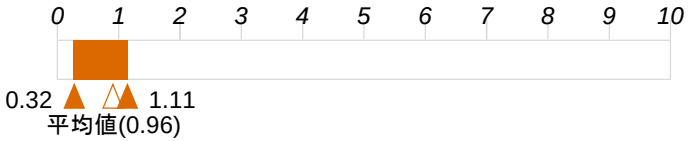
*1: 図に示したスマートデバイスは、乗員が車載のIVIシステムに接続し、ナビゲーションやエンタテイメント機器として利用するスマートデバイスのことを指す

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

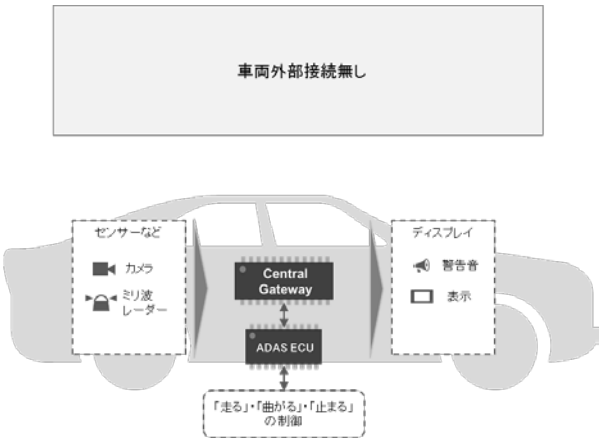
1-1. 脅威の重大度（スコア）の分布



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

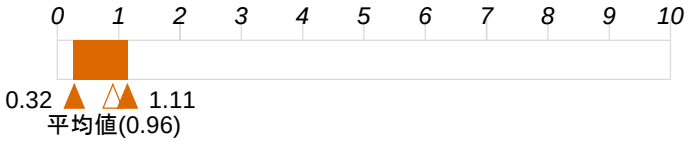
脅威のレベル	レベルI（注意）	レベルII（警告）	レベルIII（重大）
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

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

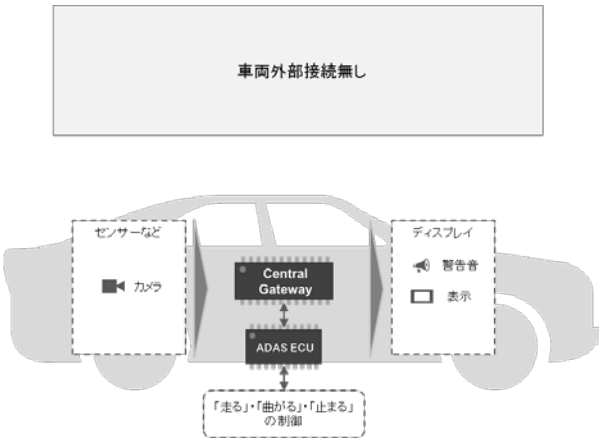
1-1. 脅威の重大度（スコア）の分布



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

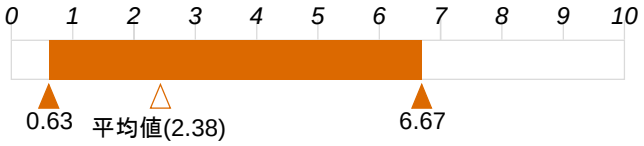
脅威のレベル	レベルI（注意）	レベルII（警告）	レベルIII（重大）
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

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

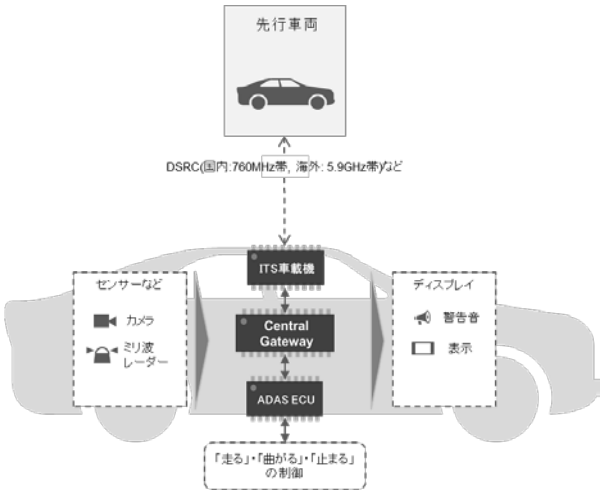
1-1. 脅威の重大度(スコア)の分布



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

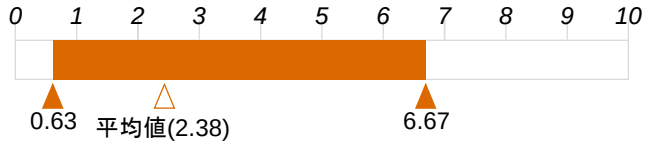
脅威のレベル	レベルI(注意)	レベルII(警告)	レベルIII(重大)
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

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

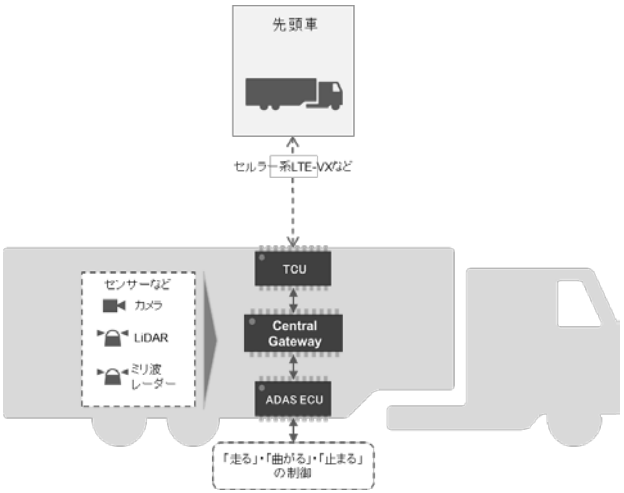
1-1. 脅威の重大度(スコア)の分布



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

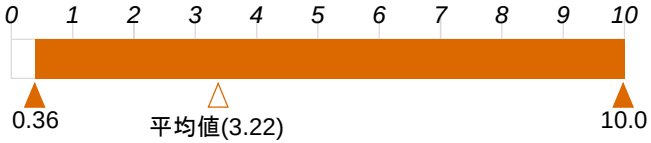
脅威のレベル	レベルI(注意)	レベルII(警告)	レベルIII(重大)
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

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

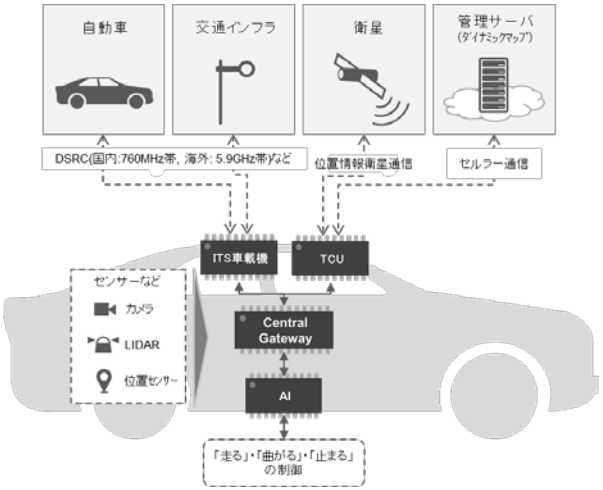
1-1. 脅威の重大度(スコア)の分布



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

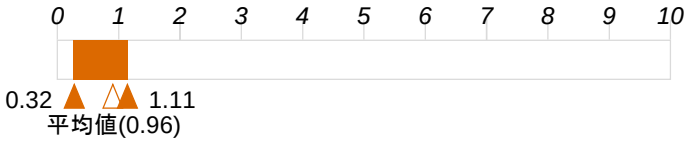
脅威のレベル	レベルI(注意)	レベルII(警告)	レベルIII(重大)
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

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

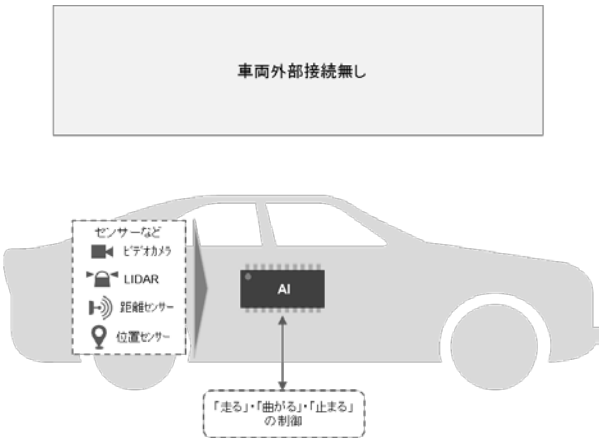
1-1. 脅威の重大度(スコア)の分布



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

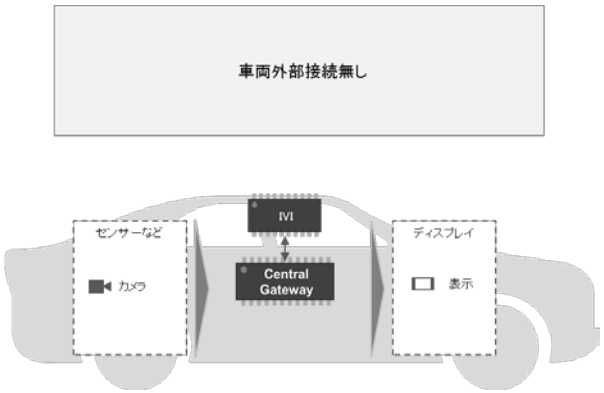
1. 評価結果

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

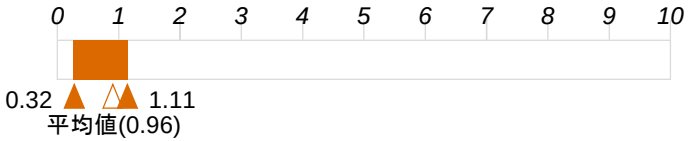
脅威のレベル	レベルI（注意）	レベルII（警告）	レベルIII（重大）
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

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

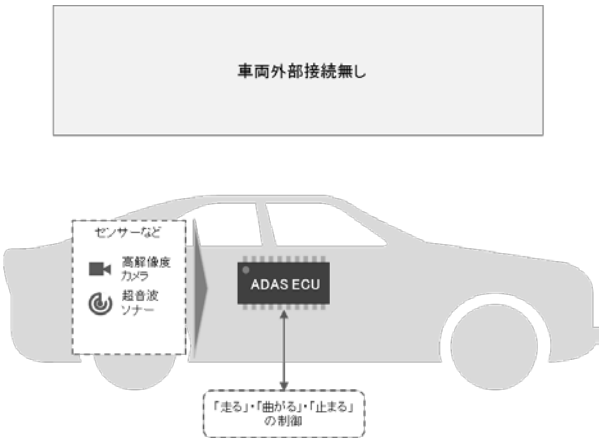
1-1. 脅威の重大度(スコア)の分布



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

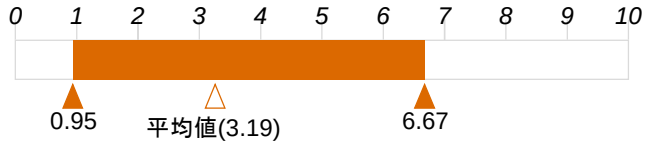
脅威のレベル	レベルI(注意)	レベルII(警告)	レベルIII(重大)
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

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

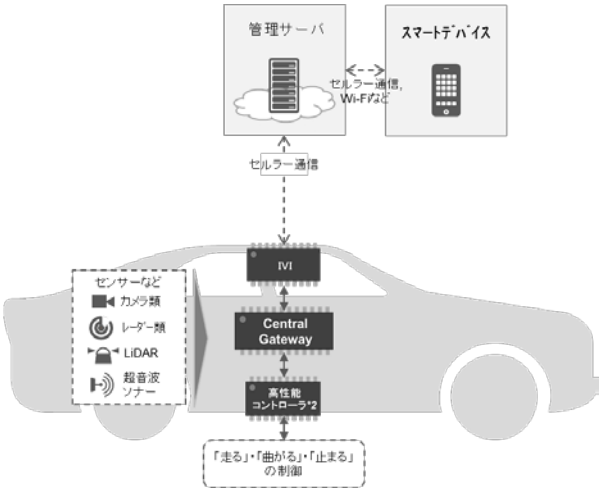
1-1. 脅威の重大度（スコア）の分布



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

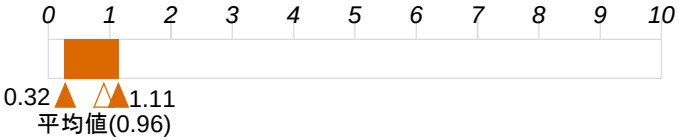
脅威のレベル	レベルI（注意）	レベルII（警告）	レベルIII（重大）
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

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

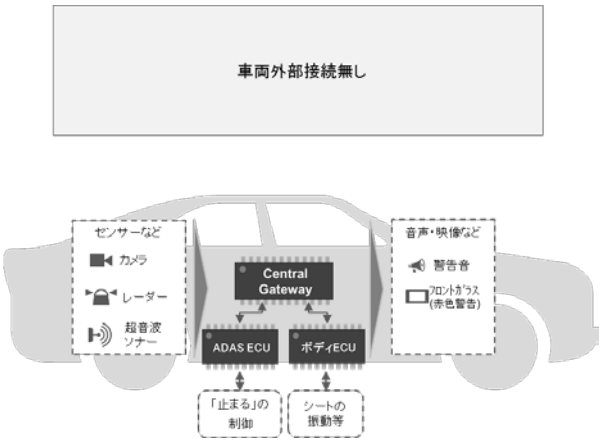
1-1. 脅威の重大度（スコア）の分布



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

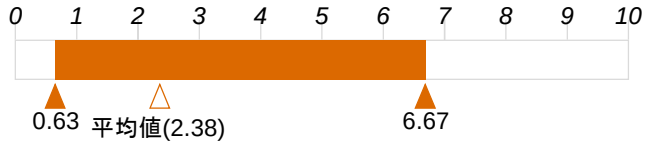
脅威のレベル	レベルI（注意）	レベルII（警告）	レベルIII（重大）
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

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

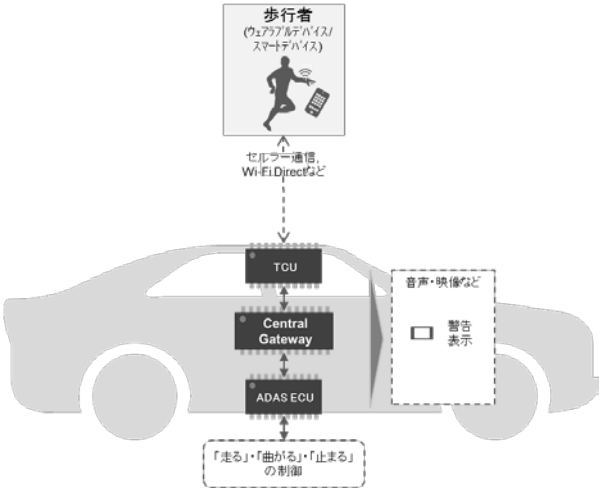
1-1. 脅威の重大度(スコア)の分布



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)

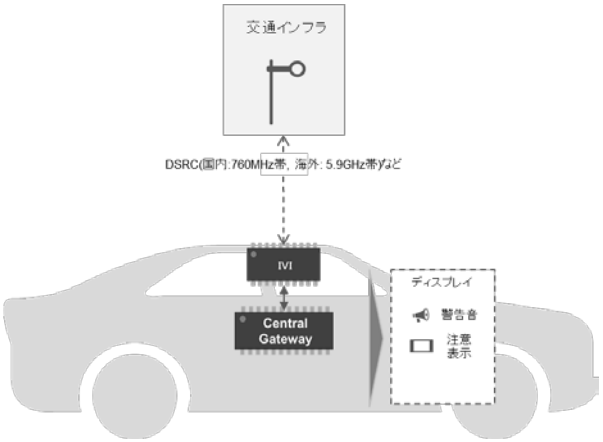
1. 評価結果

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

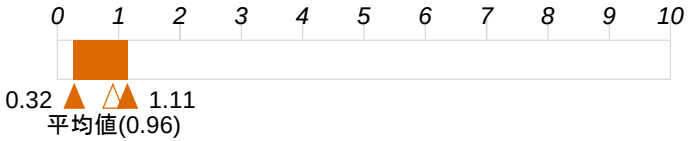
脅威のレベル	レベルI(注意)	レベルII(警告)	レベルIII(重大)
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

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

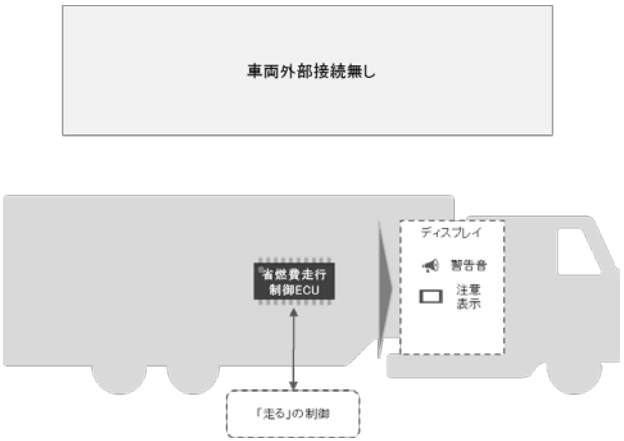
1-1. 脅威の重大度（スコア）の分布



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

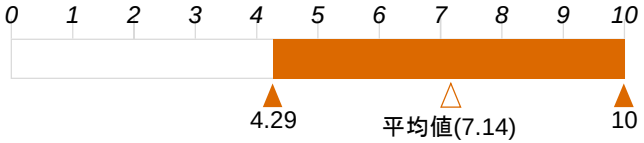
脅威のレベル	レベルI（注意）	レベルII（警告）	レベルIII（重大）
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

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

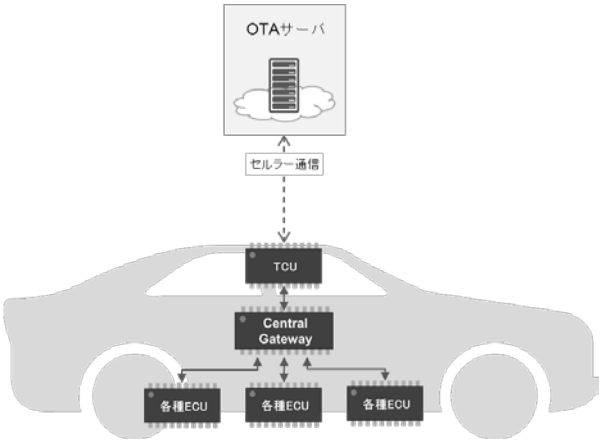
1-1. 脅威の重大度（スコア）の分布



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

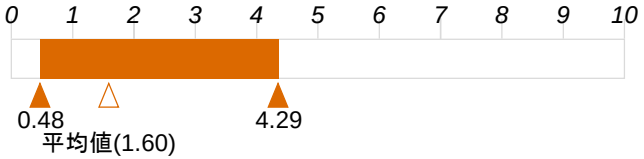
脅威のレベル	レベルI（注意）	レベルII（警告）	レベルIII（重大）
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

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

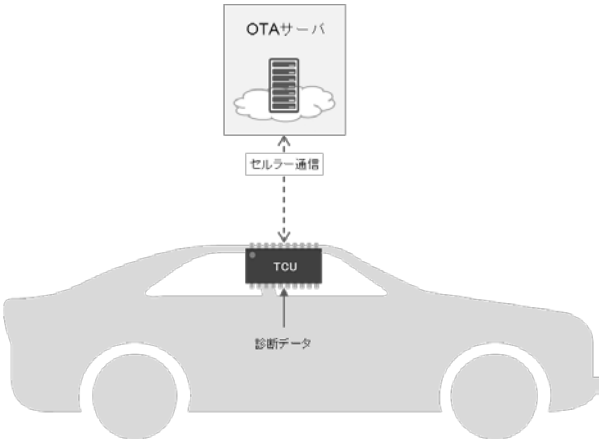
1-1. 脅威の重大度（スコア）の分布



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

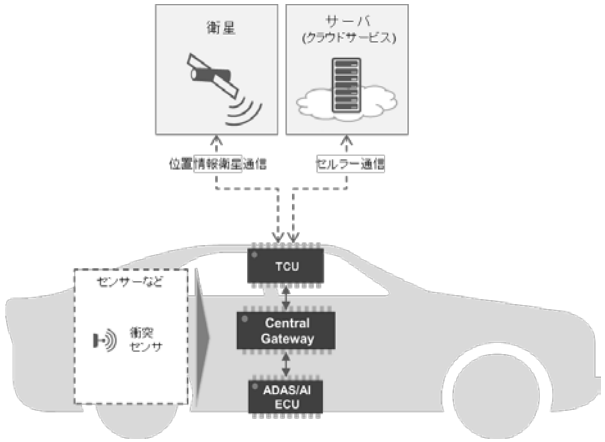
1. 評価結果

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

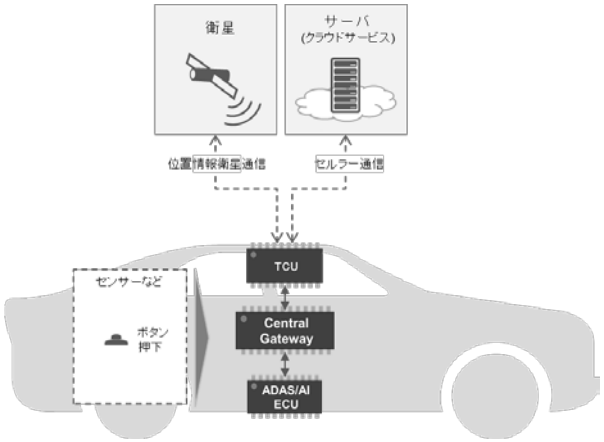
1. 評価結果

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

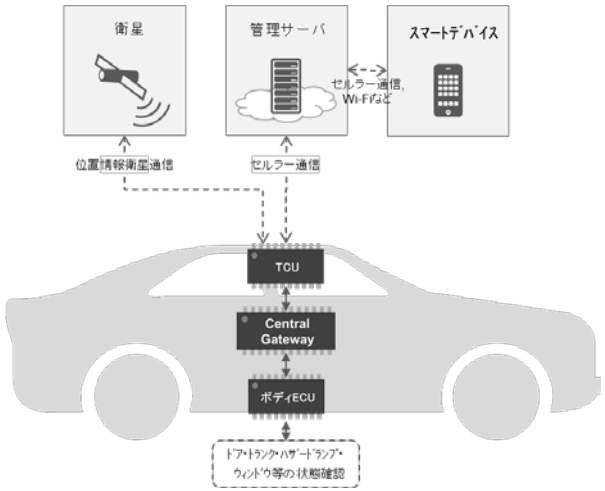
1. 評価結果

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

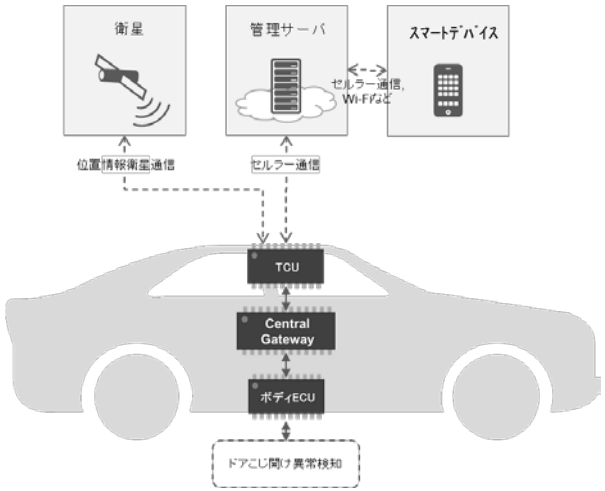
1. 評価結果

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

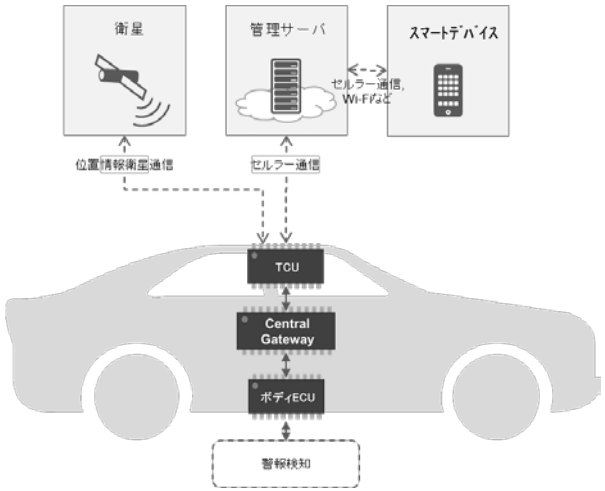
1. 評価結果

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)

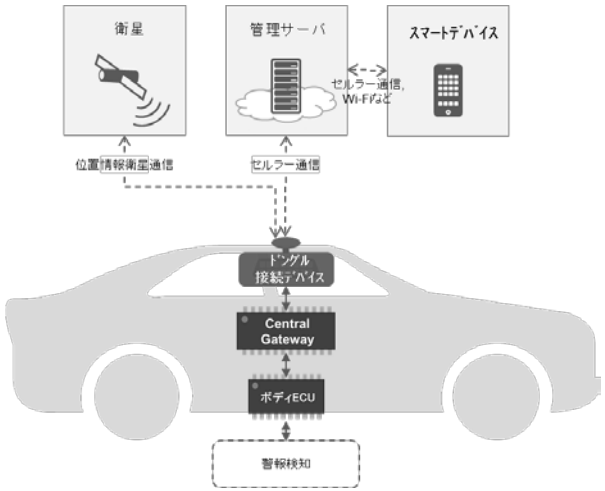
1. 評価結果

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

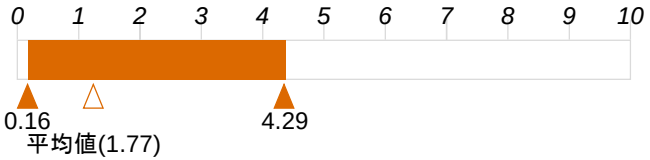
脅威のレベル	レベルI(注意)	レベルII(警告)	レベルIII(重大)
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

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

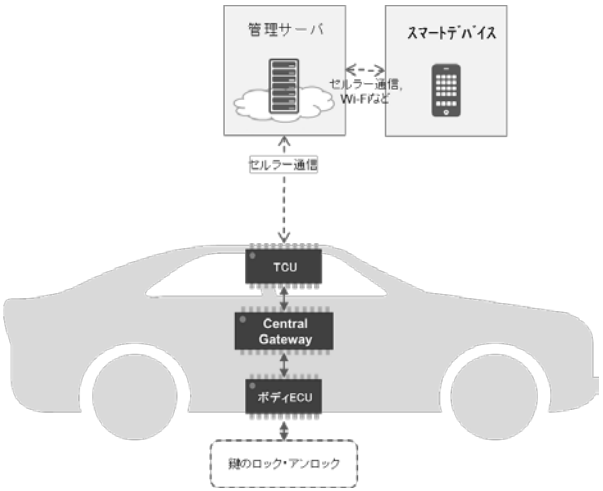
1-1. 脅威の重大度（スコア）の分布



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

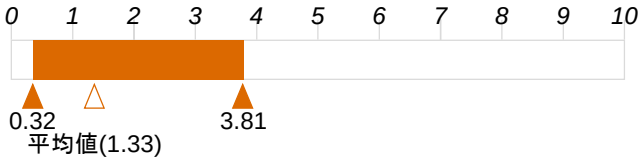
脅威のレベル	レベルI（注意）	レベルII（警告）	レベルIII（重大）
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

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

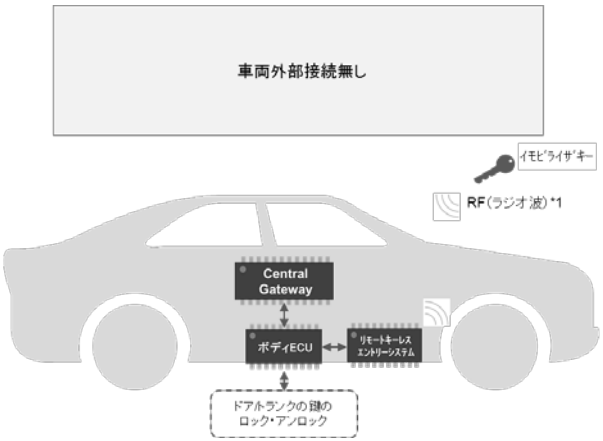
1-1. 脅威の重大度（スコア）の分布



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

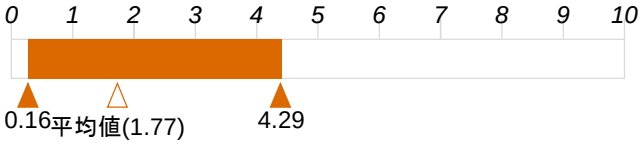
脅威のレベル	レベルI（注意）	レベルII（警告）	レベルIII（重大）
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

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

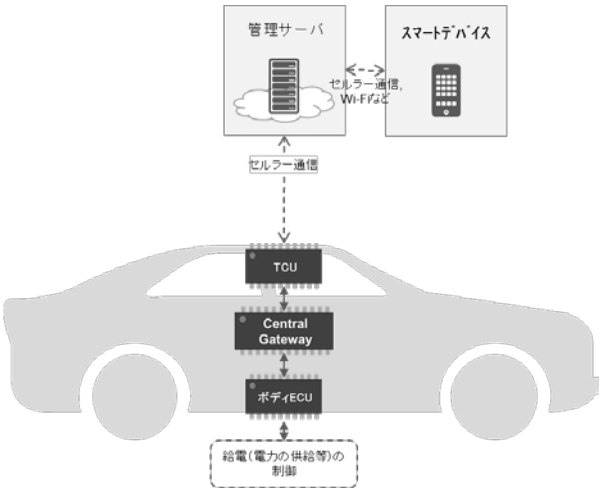
1-1. 脅威の重大度（スコア）の分布



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

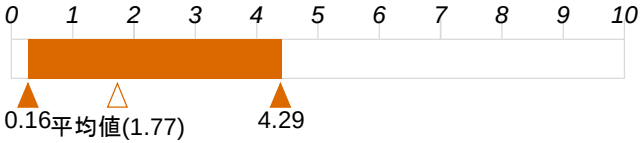
脅威のレベル	レベルI（注意）	レベルII（警告）	レベルIII（重大）
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

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

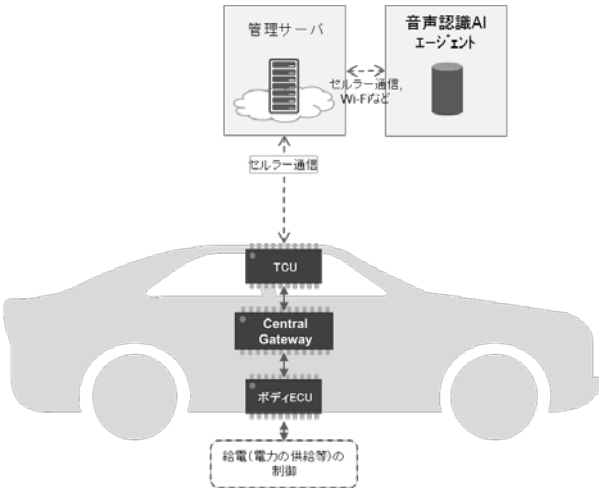
1-1. 脅威の重大度（スコア）の分布



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

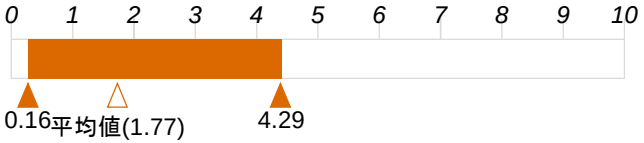
脅威のレベル	レベルI（注意）	レベルII（警告）	レベルIII（重大）
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

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

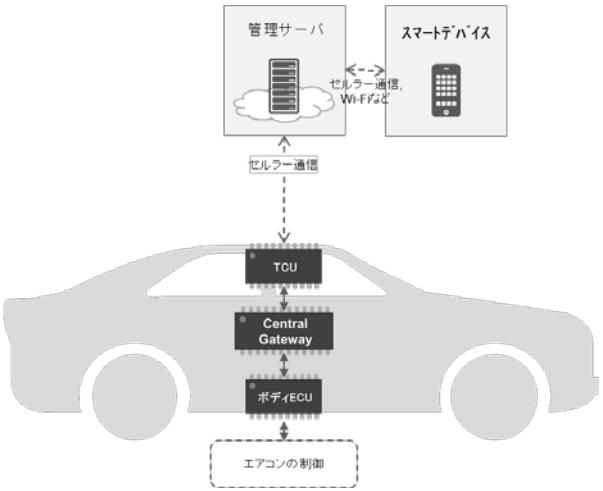
1-1. 脅威の重大度（スコア）の分布



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

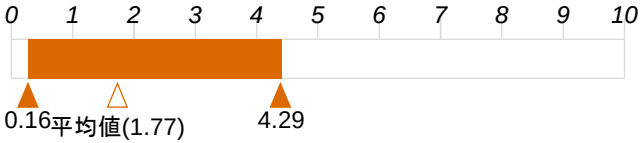
脅威のレベル	レベルI（注意）	レベルII（警告）	レベルIII（重大）
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

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

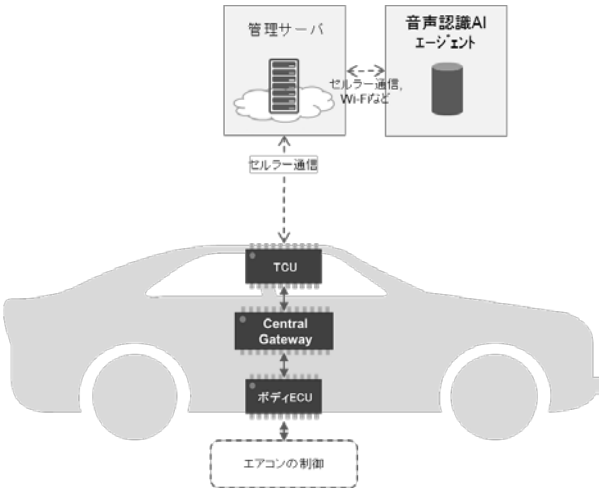
1-1. 脅威の重大度（スコア）の分布



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

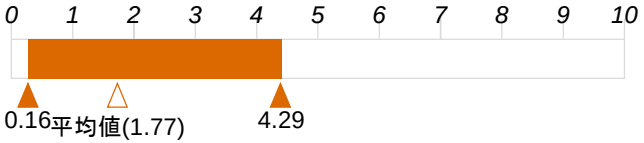
脅威のレベル	レベルI（注意）	レベルII（警告）	レベルIII（重大）
スコア	0 ~ 3.9	4.0 ~ 6.9	7.0 ~ 10.0

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

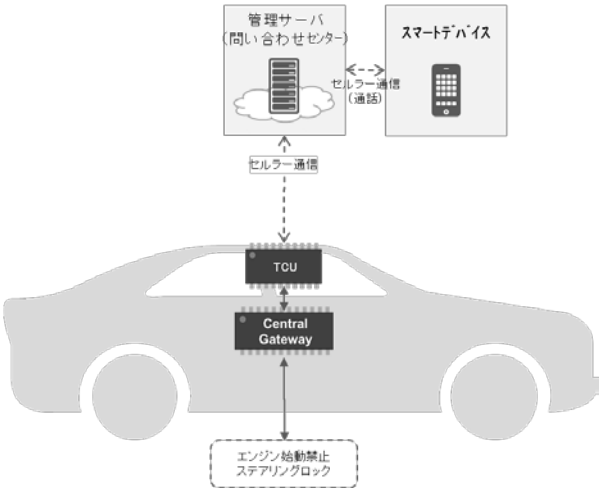
1-1. 脅威の重大度（スコア）の分布



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

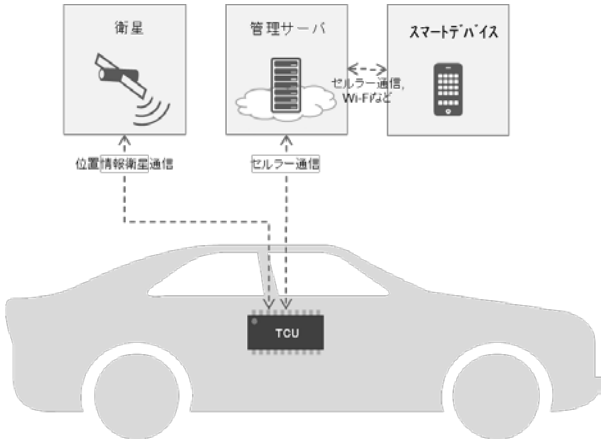
1. 評価結果

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

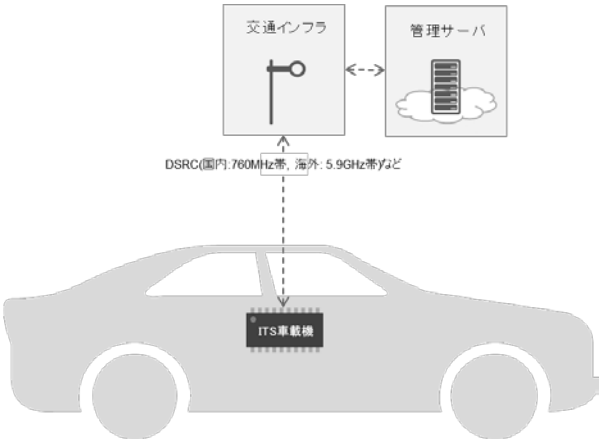
1. 評価結果

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)

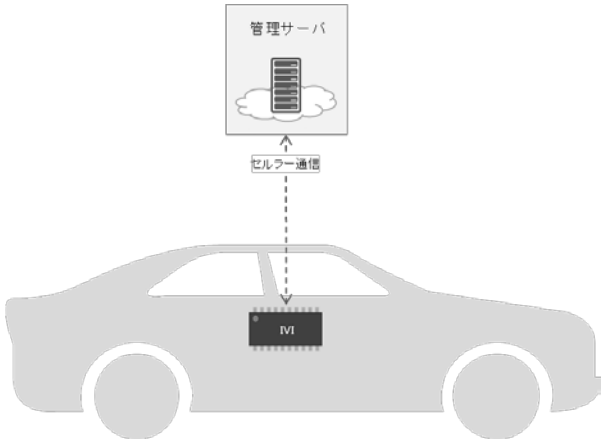
1. 評価結果

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）

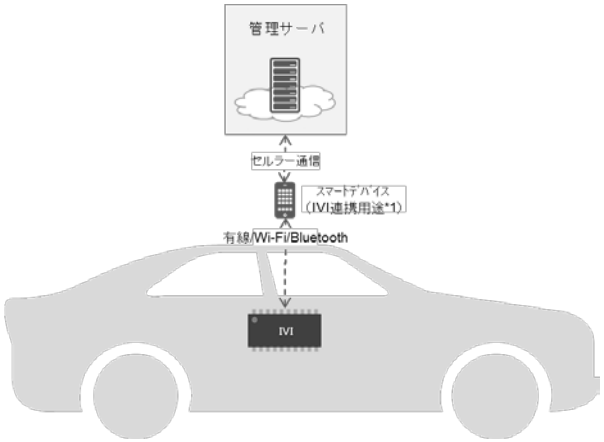
1. 評価結果

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)

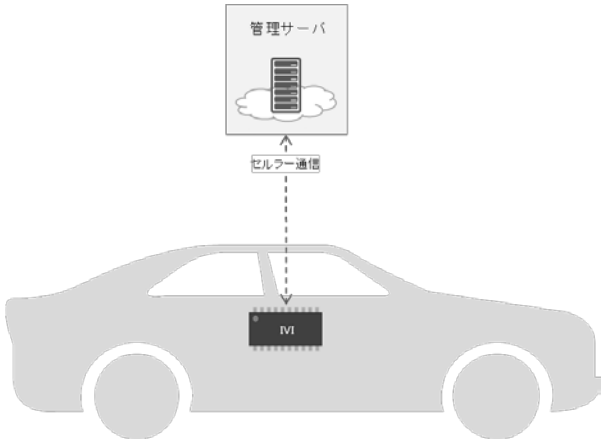
1. 評価結果

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)

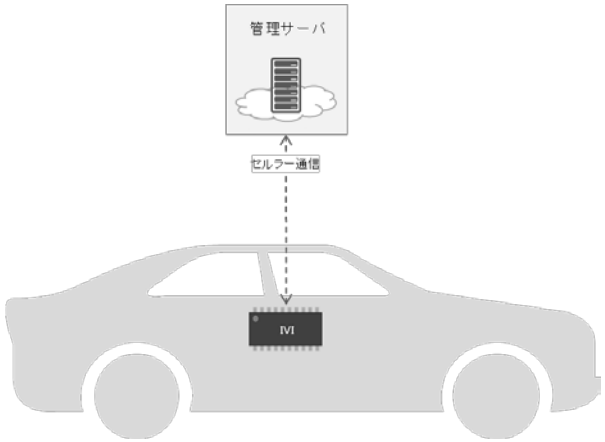
1. 評価結果

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)

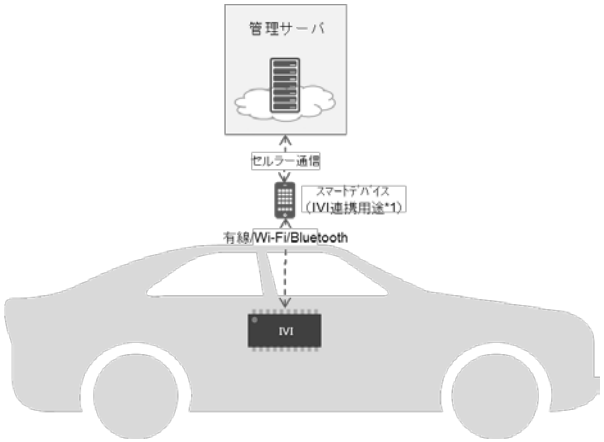
1. 評価結果

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)

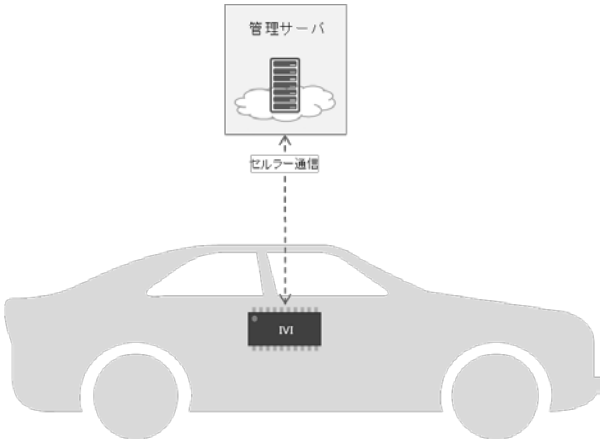
1. 評価結果

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）

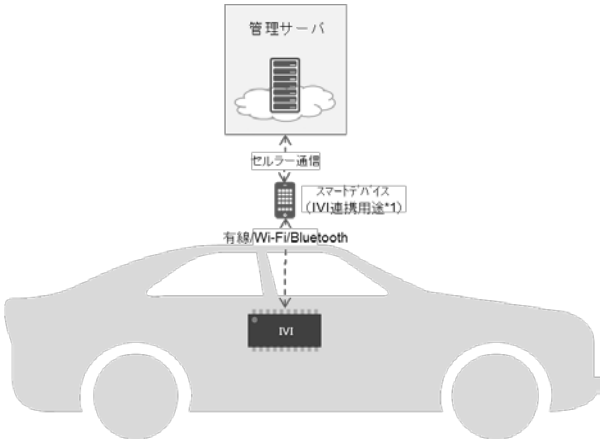
1. 評価結果

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)

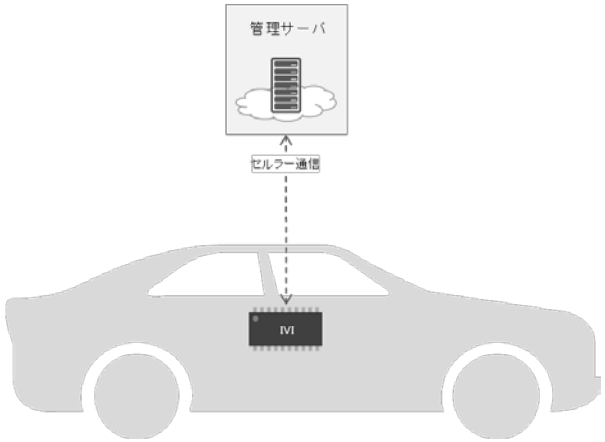
1. 評価結果

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)

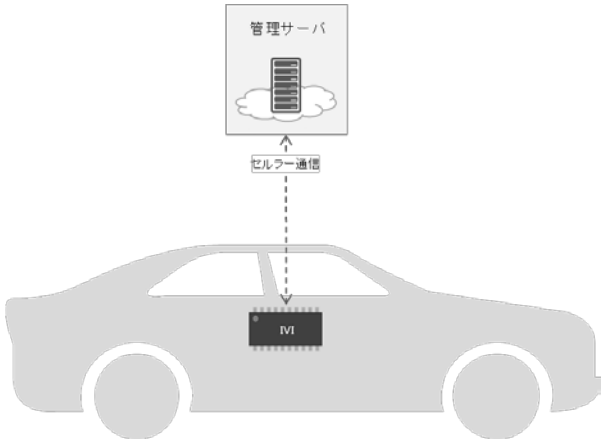
1. 評価結果

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）

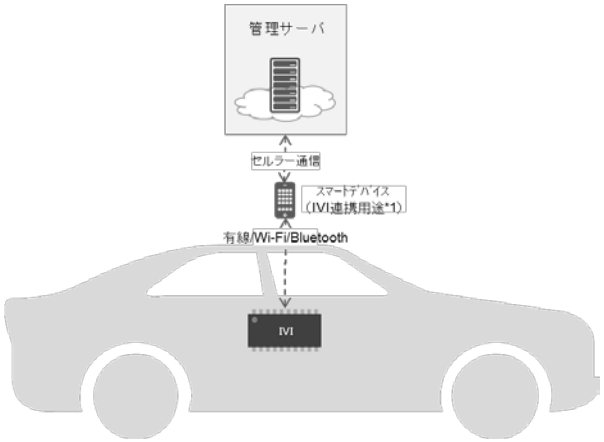
1. 評価結果

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

情報セキュリティ評価ガイドライン
ドラフト（本編）
【成果報告書版】

2018年2月28日発行

【本書の位置づけ】
本書は、「情報セキュリティ評価ガイドラインドラフト（本編） ver.3.2」をもとに、成果報告書版として作成したものである

目次

1. はじめに 1

1.1. 背景と目的 1
1.2. 本書の構成 2
1.3. 適用範囲 3
1.4. 前提事項 4
1.5. 用語の定義 4
1.6. 参考文献 5

2. 車両を取り巻く脅威の全体像 6

2.1. 車両を取り巻く脅威の全体像 6

3. 評価プロセス 7

3.1. 事前調整 8
3.2. 想定される攻撃者の整理 9
3.2.1. 攻撃者の推定 9
3.2.2. 攻撃者のプロファイル 9
3.3. 攻撃対象コンポーネントの特定 10
3.3.1. 機能の洗い出し 10
3.3.2. コンポーネントの洗い出し 10
3.3.3. 機能とコンポーネントのマッピング 10
3.3.4. 攻撃者が興味を示す機能の特定 11
3.3.5. 攻撃者が興味を示すコンポーネントの特定 11
3.4. 車両個別のリスク分析 12
3.4.1. 攻撃者ファクターの導出 13
3.4.2. 脆弱性ファクターの導出 15
3.4.3. 発生可能性の計算 15
3.4.4. 影響度ファクターの導出 15
3.4.5. 影響度の見積 16
3.4.6. コンポーネントリスクの評価 16
3.5. 評価計画の立案 18
3.5.1. テストスコープの決定 18
3.5.2. 技術的分析 18
3.5.3. 評価計画の作成 20
3.6. テストの実施 23
3.6.1. テスト実施前の対応事項 23
3.6.2. テスト実施中および実施後の対応事項 23
3.7. リスクマッピング 24

3.7.1. コンポーネントレベルリスク評価 24
3.7.2. 車両レベルリスク評価 25
3.7.3. フリートレベルリスク評価 25
3.7.4. トータルリスク評価 25
3.7.5. リスク評価例 26
3.8. 改善案および残存リスクの整理 27
3.8.1. 発見事項に対する改善案の検討 27
3.8.2. 残存リスクの整理 27
4. 評価結果の報告 28
4.1. レポートの作成 28
4.1.1. 発見事項の整理 28
4.1.2. 評価結果の整理 28
4.1.3. レポートの評価 28
付録 1. 想定される一般的な脅威一覧 29
付録 2. 一般的な評価項目一覧 29
付録 2.1. 自動車における既知の脆弱性に対する一般的な評価項目 29
付録 2.2. IT システム分野における既知の脆弱性に対する一般的な評価項目 29

1. はじめに

1.1. 背景と目的

自動車のコネクテッド化が進み、ネットワークを経由して車内外の様々なデータのやり取りが行われている。これにより自動車の快適性が向上し、また、クラウドとつながることで様々なサービスを受けられるようになっている。その一方で、無線通信等のネットワークを経由した車外サービスの利用増により、車外からの遠隔操作等によるセキュリティ攻撃等のリスクが高まり、無線経由の通信に対するセキュリティ確保の必要性が増している。

また、今後、市場に登場するとみられる自動走行車両の場合、車両を市場へリリースした後の運用時においても、OTA（Over The Air）によるソフトウェア更新に伴う車両の仕様変更や、車外サービスの仕様変更に伴う車両への影響等の考慮が必要となることが考えられる。これらのことから無線経由の通信に対するセキュリティ確保の観点において、開発車に対するセキュリティ評価に加え、市販車に対するセキュリティ評価の必要性も増している。

開発車や市販車におけるセキュリティ評価においては、セキュリティ機能が要求通りに実現できているかという観点に加えて、車外からの実際の攻撃に対する耐ハッキング性能という観点がより重要となる。そこで、IT システム分野で採用されているペネトレーションテストを、自動車にも適用する動きが高まっている。

ペネトレーションテストは、攻撃者視点によるセキュリティ評価であり、車両の脆弱性を利用して実際に外部から攻撃が可能かを検証する。これはツールによる脆弱性診断やファジングテストといった他のセキュリティ評価とは異なる性質をもつ。ペネトレーションテストでは、攻撃者視点による評価という性質上、評価対象をブラックボックスとして扱う場合も多く、一般的に評価に用いる情報は制限されることから、情報収集に多くの労力を費やす。また、実車両を必要とすることから、開発の終盤に評価が実施される場合が多く、評価期間やリソースについて制約も受ける場合もある。このように、情報や評価期間、リソース等の制約を大きく受けるペネトレーションテストに対しては、リスクアプローチにより対象を絞った上で効率よく評価を行うことが望ましい。更に、発見された脆弱性に対してそのリスクを評価し優先度をつけた上で、必要な対応を実施しリスクを許容可能なレベルまで低減することが望まれる。

上記を踏まえ、本ガイドラインでは以下の 3 つを目的とする。

1. 開発車および市販車に対して、無線通信経由での車外から車両の車外ゲートウェイ（GW）までの攻撃を想定したセキュリティ評価を行うこと
2. 攻撃者視点で評価項目を作成し、脆弱性の有無を効率よく評価すること
3. 発見された脆弱性に対するリスク評価を行い、許容可能なレベルまで低減すること

1.2. 本書の構成

本ガイドラインは、情報セキュリティ評価ガイドラインドラフト（本編）と、情報セキュリティ評価ガイドラインドラフト（実践手引き）の 2 段構成としている。情報セキュリティ評価ガイドラインドラフト（本編）では、車両に対する情報セキュリティ評価の概要や評価プロセスの詳細を記載し、評価実施者のみならず、評価責任者や評価依頼者が理解しておくべき内容が記載されている。

一方、情報セキュリティ評価ガイドラインドラフト（実践手引き）は、Wi-Fi 編、Bluetooth 編等の各通信プロトコルに応じた別冊となっており、主として評価実施者が理解しておくべき具体的な評価手法が記載されている。このため、実際の評価における詳細な手法については、各通信プロトコルの実践手引きを参照されたい。また、実際の情報セキュリティ評価においては、ペネトレーションテストの目的に則り、評価実施者は実践手引きに記載された内容以外の評価手法についても臨機応変に組み込んでいく必要がある点を留意が必要である。

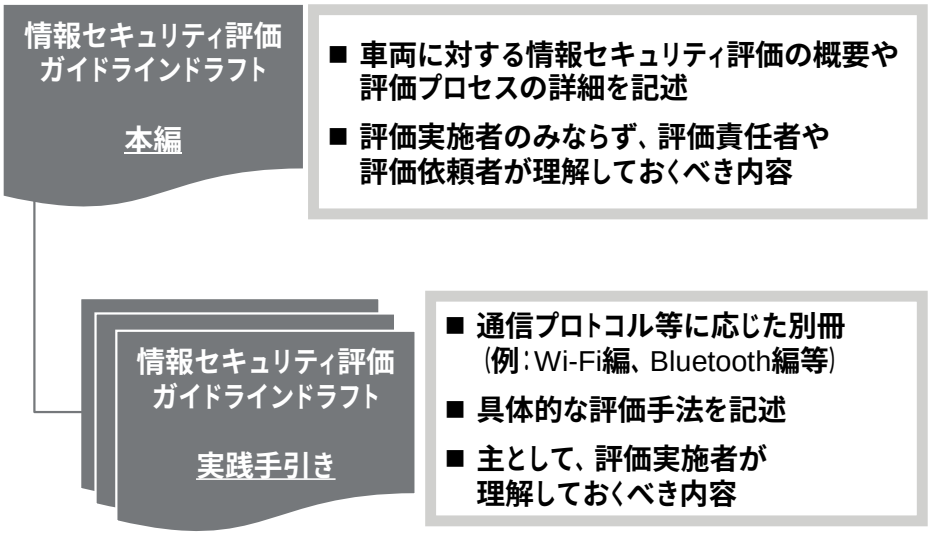


図 1.1 情報セキュリティ評価ガイドラインドラフトの構成

情報セキュリティ評価ガイドラインドラフト（本編）は、以下の構成となっている。

第 1 章は、本書の目的や、適用範囲、前提事項について述べる。

第 2 章は、脅威分析に基づき、現在および将来の自動走行車両および自動走行システムにおける共通モデルに関する脅威の全体像を整理する。

第 3 章は、本ガイドラインにおける評価プロセスの詳細について説明する。具体的には、テスト前に実施する事前調整やリスク分析、テスト後に実施するリスク評価、改善案および残存リスクの整理について説明する。

第 4 章は、情報セキュリティ評価の結果および改善案に関する評価結果レポートの作成について説明する。また、作成した評価結果レポートに対する、記載事項の網羅性、評価内容の適切性に関するチェックリストを含む。

付録 1 は、車両個別の脅威分析を実施する上で参考として利用可能な、一般的に想定される脅威の一覧を記載する。

付録 2 は、過去に顕在化した自動車に関するインシデント事例を含む一般的な脆弱性に対して、予防等の対処となる評価方法を記載する。

1.3. 適用範囲

一般にセキュリティでは多層防御の考え方があり、複数の層における防御策によりセキュリティを維持している。本ガイドラインでは車内を「外部接続」、「車載 GW」、「車載ネットワーク」、「ECU」の 4 つのレイヤーに分けて考える。その上で、車外との通信と、車内のネットワークを分離すると、車内 GW より内部の車載ネットワークや ECU は車内ドメインでの保護対象となる。一方、車外との通信の入口となる車外 GW までは、無線経路から直接攻撃が及ぶ領域ととらえ、本ガイドラインでは、主に、3G／LTE 等のセルラー通信や Wi-Fi／Bluetooth 等の無線経路による攻撃を想定し、車外から車外 GW までのセキュリティ評価を対象とする。図 1.2 の点線枠内に本ガイドラインの適用範囲を示す。

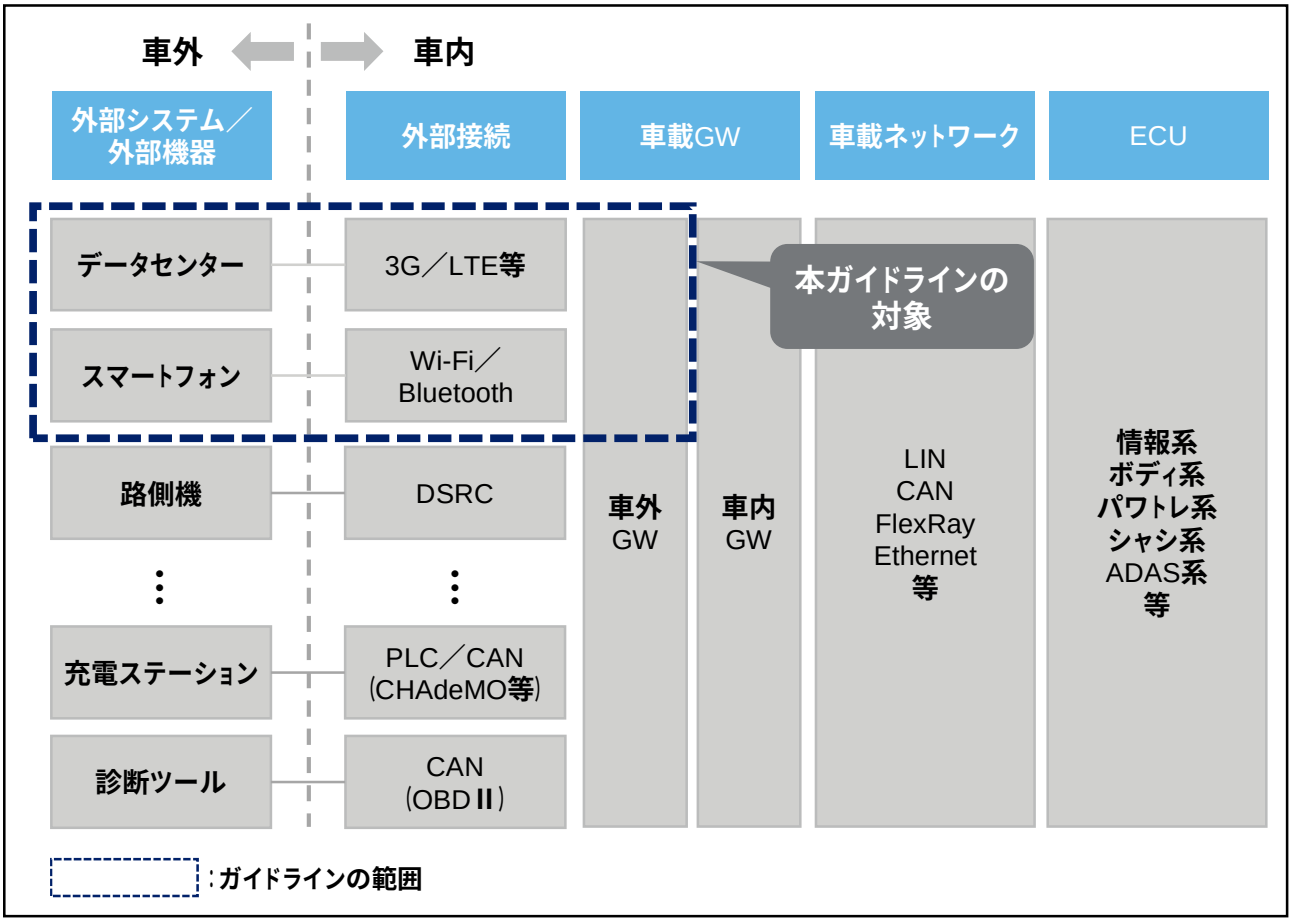


図 1.2 本ガイドラインの適用範囲

1.4. 前提事項

本ガイドラインのＶ字プロセスにおける位置付けを図 1.3 に示す。本ガイドラインは、①車両総合評価、②市販車評価、③－1 システム設計、③－2 H/W-S/W 統合評価の大きく 4 つの工程での活用を前提とする。

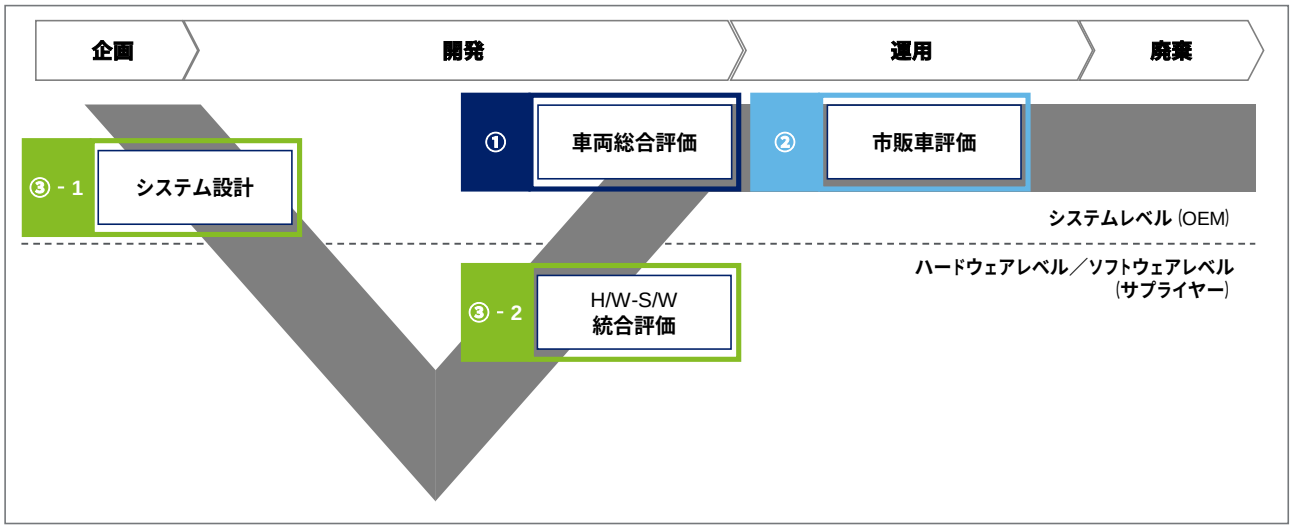


図 1.3 本ガイドラインのＶ字プロセスにおける位置付け

なお、上記の評価において高度なスキルが求められる場合や評価に対する客観性が強く求められる場合は、外部専門家を活用することも考えられる。

1.5. 用語の定義

本ガイドラインで利用する用語とその定義を表 1-1 に示す。

表 1-1 （公開資料のため、記載内容を削除）

また、本ガイドラインで利用する略語の定義について表 1-2 に示す。

表 1-2 （公開資料のため、記載内容を削除）

1.6. 参考文献

- SAE International（2016 年）「SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems」
- Open Web Application Security Project（OWASP）（2016 年）「OWASP Risk Rating Methodology」, <https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology>, 2017 年 11 月 28 日アクセス
- 独立行政法人 情報処理推進機構（IPA）（2015 年）「共通脆弱性評価システム CVSS v3 概説」, <https://www.ipa.go.jp/security/vuln/CVSSv3.html>, 2017 年 11 月 28 日アクセス
- MITRE Corporation, （2006-2017 年）「Common Weakness Enumeration, A Community Developed List of Software Weakness Types」, <http://cwe.mitre.org/>, 2017 年 11 月 28 日アクセス
- MITRE Corporation, （2017-2017）「Common Attack Pattern Enumeration and Classification, A Community Resource for Identifying and Understanding Attacks」, < https://capec.mitre.org/>, 2018 年 1 月 26 日アクセス
- McAfee,（2015 年）「Automotive Security - Best Practices, Recommendations for security and privacy in the era of the next-generation car」,<https://www.mcafee.com/hk/resources/white-papers/wp-automotive-security.pdf>, 2018 年 1 月 9 日アクセス
- Cyber Security Academy,（2017 年）「Multi actor roadmap to improve cyber security of consumer used connected cars」,<https://www.csacademy.nl/csa-scripties/februari-2017/85-multi-actor-roadmap-to-improve-cyber-security-of-consumer-used-connected-cars>, 2018 年 1 月 9 日アクセス

2. 車両を取り巻く脅威の全体像

2.1. 車両を取り巻く脅威の全体像

車両と外部との通信は、乗車、走行準備、走行、駐停車、サービス・メンテナンスといった様々な利用シーンにおいて、利便性や快適性また安全性の向上等を目的としたサービス提供に利用されはじめている。図 2.1 にそれらのサービス事例を示す。これらサービスの多くは 2020 年頃から実装される見込みであり、サービス実現のために自動車メーカーだけでなく、サプライヤー、電気機器メーカー、IT ベンダー、地図製作会社、電力会社、保険会社等、多くの事業者が参画するものと見られる。

図 2.1 （公開資料のため、記載内容を削除）

「1.1 背景と目的」でも触れたように、無線通信等のネットワークを経由した車外サービスの利用増により、自動車のコネクテッド化が進むことで、車外からの遠隔操作等によるセキュリティ攻撃等のリスクが高まっている。またそれに伴い、無線経由の通信に対するセキュリティを確保する必要性が増している。自動車のセキュリティ確保のためには、それぞれのサービスおよび通信経路においてどのような脅威が存在するかを把握することが重要となる。なお、「脅威」とは、漏えい、改ざんまたは破壊等の自動車およびその周辺環境に係る情報資産および安全走行を侵害させ得る潜在的な現象を指す。

脅威を把握する上で、様々な脅威分析の手法を用いることができるが、本ガイドラインでは具体的な脅威分析手法については対象に含めていない。また、既に自組織の設計プロセスで脅威分析を実施している場合は、その結果を用いることができる。

本ガイドラインの評価プロセスでは「3.2 想定される攻撃者の整理」において、攻撃者プロファイルを作成するが、その際に攻撃者のスキル、能力や動機等を検討するため、評価対象となる車両ごとにどのような脅威が存在し得るのかについて検討しておくことが望ましい。

本ガイドラインでは脅威分析に活用可能な情報として、付録 1 に一般的な脅威を列挙している。

3. 評価プロセス

本評価プロセスは、図 3.1 のとおり「攻撃者中心アプローチ」と「リスクアプローチ」を基本的な考え方としている。

2つの基本的な考え方	① 攻撃者中心アプローチ	攻撃者が入手し得る情報、攻撃者の標的となり得る機能（情報）に着目し、攻撃者視点で評価を行うプロセスとする
	② リスクアプローチ	ペネトレーションテストに費やすことができるリソース（ヒト、モノ、カネ、時間）は有限であり、評価実施における制約であることからリスク見合いの評価が実施できるプロセスとする

図 3.1 情報セキュリティ評価プロセスの基本的な考え方

また、本評価プロセスは「テスト実施前の評価プロセス」、「テスト実施」、「テスト実施後の評価プロセス」に大別できる。それぞれの評価プロセスのステップと主な実施内容は図 3.2 のとおりである。

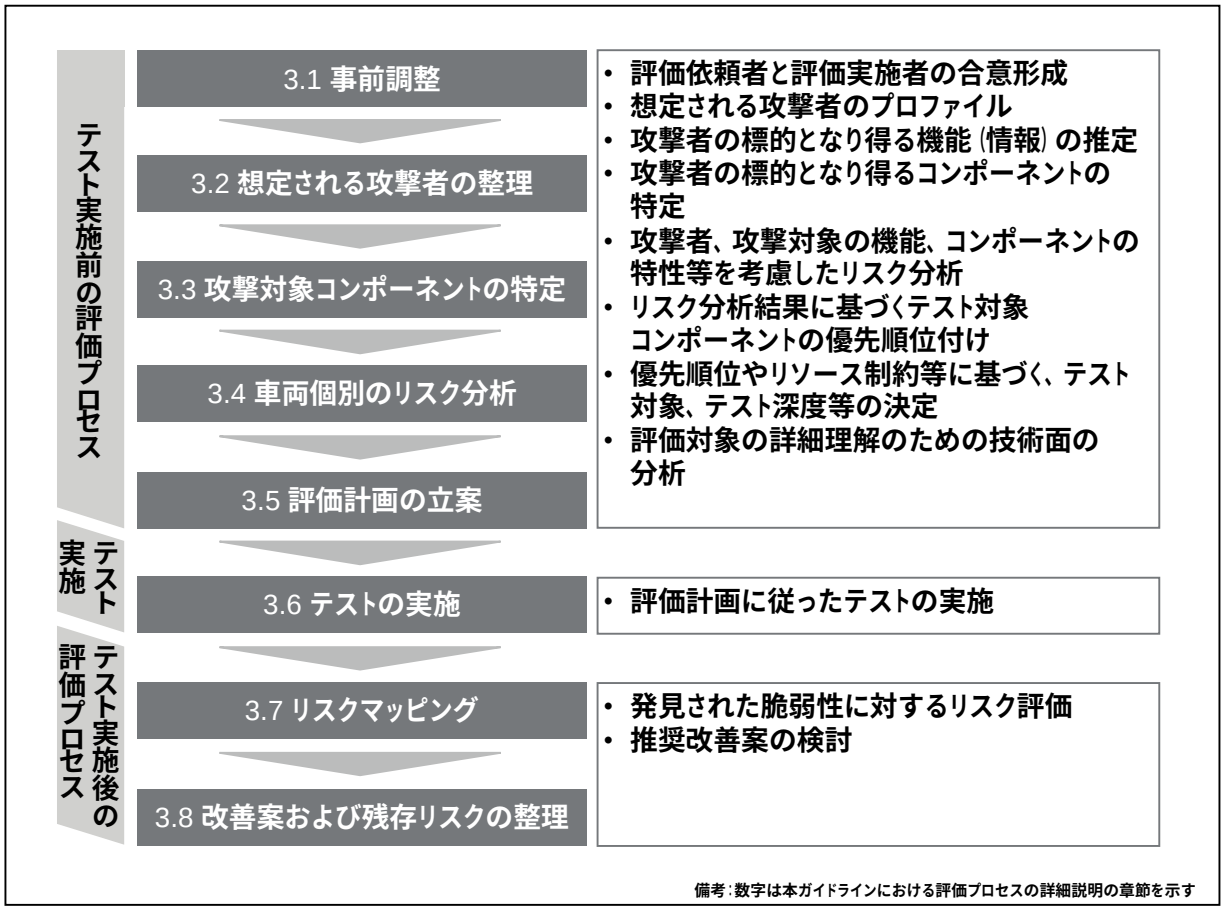


図 3.2 評価プロセスの全体像

テスト実施前の評価プロセスは、テスト実施に向けた評価計画の立案のために、評価対象のコンポーネントを選定するためのリスク分析を行うプロセスである。

テストの実施は、計画に従ってテストを実施するプロセスである。

テスト実施後の評価プロセスは、テストの実施により発見された脆弱性に対するリスク評価および改善案の検討を行うプロセスである。

3.1. 事前調整

情報セキュリティ評価の最初のステップ「3.1 事前調整」では、主として以下を実施する。

- 評価依頼者と評価実施者との間で情報セキュリティ評価の実施前に各種取り決め事項についての調整

事前調整では、表 3-1 に例示する事項等について評価依頼者と評価実施者の双方で協議し、合意する。

表 3-1 （公開資料のため、記載内容を削除）

本ガイドラインで提示する情報セキュリティ評価のプロセスは、評価の実施に割り当て可能なリソース（ヒト、モノ、カネ、時間）は有限であり、網羅的に評価を実施することは現実的に不可能であるという前提のもと、攻撃者中心アプローチ、リスクアプローチを採用している。このため、評価実施前に評価期間、評価範囲や評価体制・人数等の割り当て可能なリソースを明確にするための情報について、評価依頼者と評価実施者双方で協議し、合意する。特に評価対象については、テスト専用の車両やコンポーネントおよびサーバ環境を準備する等により実運用環境とは異なる場合がある。このため、評価実施前にはテスト環境と実運用環境との差分について十分把握しておく必要がある。また、接続先サーバの設定等、テストのために実運用環境とテスト環境の切り換えが必要となる場合においては、切り換えが正常に行われたかの確認方法や問題が発生した際の対処プロセス等について、評価依頼者と評価実施者で合意しておくことが望ましい。

また、攻撃者中心アプローチ、リスクアプローチとして、後のステップにおいて、攻撃者の標的となり得る機能（情報）に着目し、当該機能を構成するコンポーネントを特定することになるが、どのような情報を利用し、当該ステップを実施するかを明確にしておくため、一般に公開されている情報に加え、評価依頼者から詳細な設計情報等が提供され得るのかどうかについても合意しておく。一般に入手可能な情報として、OEM 各社より市販されているサービスマニュアル等のドキュメントがあるが、これらの入手には時間を要する場合があることを鑑みて、評価で利用する情報について評価依頼者と確認しておくことが望ましい。

なお、一般に公開されている情報のみにより評価を行う場合は、評価対象に関する事前の情報は提供されないことになるためブラックボックステストとなる。一方、評価依頼者から詳細な設計情報等が提供される場合は、車両に係る情報を考慮した評価となるため、グレーボックステストまたはホワイトボックステストとなる。また、評価依頼者から詳細な設計情報等が提供される場合、攻撃者の標的となり得る機能（情報）を構成するコンポーネントの特定を効果的に実施することができ、かつ攻撃者が仕掛ける可能性が最も高いワーストケースの攻撃を模擬することができる。

3.2. 想定される攻撃者の整理

2 番目のステップ「3.2 想定される攻撃者の整理」では、主として以下を実施する。

- 評価対象を攻撃する可能性のある攻撃者の推定
- 攻撃者のプロファイル

当該ステップで実施する事項の流れを図示すると図 3.3 のとおりである。
次項より、各サブステップを順に説明する。

図 3.3 (公開資料のため、記載内容を削除)

3.2.1. 攻撃者の推定

当該サブステップでは、どのような攻撃者が存在し得るかを推定し、整理する。攻撃者の推定は、各社で保有している脅威分析の結果、2.1 節や付録 1 で例示している脅威の情報、一般に公開されているベストプラクティスや専門家による論文や出版物等に基づき実施する。
攻撃者の推定結果は図 3.4 のとおり整理する。

図 3.4 (公開資料のため、記載内容を削除)

3.2.2. 攻撃者のプロファイル

当該サブステップでは、表 3-2 に例示するような定性的な観点から攻撃者を評価し、それぞれの攻撃者像を明確化する。

表 3-2 (公開資料のため、記載内容を削除)

攻撃者のプロファイル結果は図 3.5 のとおり整理する。

図 3.5 (公開資料のため、記載内容を削除)

3.3. 攻撃対象コンポーネントの特定

3 番目のステップ「3.3 攻撃対象コンポーネントの特定」では、主として以下を実施する。

- 攻撃者の標的となり得る機能（情報）の特定
- 上記で特定した機能を構成するコンポーネントとのマッピング
- 上記マッピング結果から、攻撃者の標的となり得るコンポーネントの特定

当該ステップで実施する事項は多岐に及ぶため、流れを図示すると図 3.6 のとおりである。
次項より、各サブステップを順に説明する。

図 3.6 (公開資料のため、記載内容を削除)

3.3.1. 機能の洗い出し

Web カタログ、ユーザーマニュアル等の一般に公開されている情報や、評価依頼者との協議の結果提供された情報に基づき、評価対象が有する機能を一覧としてリストアップする。リストアップにおいては、電気および電子制御に係る機能を対象とし、機械や装飾に係る機能については対象外とする。また、事前に評価対象のコンポーネントリスト等が提供されている場合は、それらコンポーネントに明らかに該当しないと想定される機能については対象外とすることができる。ここでの目的は攻撃者の標的となり得るコンポーネントの特定であるので、機能の粒度については、当該機能を実現するコンポーネントの粒度を意識し、必要以上に詳細化しないように留意する。また、評価対象における機能が網羅的に洗い出されていることが必要となるため、評価依頼者と評価実施者が機能の網羅性について確認を行いながら進める必要がある。

なお、機能のリストアップ結果は図 3.7 のとおり整理する。

図 3.7 (公開資料のため、記載内容を削除)

3.3.2. コンポーネントの洗い出し

サービスマニュアル等の一般に公開されている技術的情報や、評価依頼者との協議の結果提供された情報に基づき、評価対象が有するコンポーネントを一覧としてリストアップする。なお、ハーネス等を含む全てのコンポーネントについてリスト化することが望ましい。そのためにはコンポーネントやそれらの配線情報が必要になるが、これらの情報入手のためにサービスマニュアル（整備書、修理書等）の入手が強く推奨される。

コンポーネントのリストアップ結果は図 3.8 のとおり整理する。

図 3.8 (公開資料のため、記載内容を削除)

3.3.3. 機能とコンポーネントのマッピング

「3.3.1 機能の洗い出し」においてリストアップした機能と、「3.3.2 コンポーネントの洗い出し」においてリストアップしたコンポーネントとのマッピングを行い、それぞれの機能がどのコンポーネントから構成されているかの紐付けを行う。

なお、マッピングにおいては、同一のコンポーネントが、複数の機能を構成していることも想定される。

機能とコンポーネントのマッピング結果は図 3.9 のとおり整理する。

図 3.9 (公開資料のため、記載内容を削除)

3.3.4. 攻撃者が興味を示す機能の特定

「3.3.1 機能の洗い出し」においてリストアップした各機能について、「3.2 想定される攻撃者の整理」で推定した攻撃者が興味を示す機能、つまり攻撃の標的となり得る機能をマッピングする。

なお、マッピングにおいては、1 つの機能に対し、複数の攻撃者が該当することも想定される。複数の攻撃者の標的となり得る機能は、攻撃に晒される可能性の高い機能であるため、優先度が高いものとして認識されるべきである。

攻撃者の標的となり得る機能のマッピング結果は、図 3.10 のとおり整理する。

図 3.10 (公開資料のため、記載内容を削除)

3.3.5. 攻撃者が興味を示すコンポーネントの特定

攻撃者の標的となり得るコンポーネントを特定するために、「3.3.4 攻撃者が興味を示す機能の特定」において攻撃者の標的となり得るとして特定した機能を構成するコンポーネントを、「3.3.3 機能とコンポーネントのマッピング」の結果を利用して特定する。

図 3.10 に示すように、「3.3.3 機能とコンポーネントのマッピング」において、機能とコンポーネントとがマッピングされている。また、「3.3.4 攻撃者が興味を示す機能の特定」において、攻撃者の標的となり得る機能が特定されているので、当該機能のみに絞り込んだマッピングを導出することができる。以上より、攻撃者の標的となり得るコンポーネントを特定することができる。

図 3.11 (公開資料のため、記載内容を削除)

攻撃者の標的となり得るコンポーネントの特定結果は図 3.12 のとおり整理する。

図 3.12 (公開資料のため、記載内容を削除)

3.4. 車両個別のリスク分析

4 番目のステップ「3.4 車両個別のリスク分析」では、主として以下を実施する。

- 攻撃者の特性から攻撃者ファクターの導出
- コンポーネントの特性から脆弱性ファクターの導出
- 上記 2 つのファクターから発生可能性の見積
- 「安全性」・「財務上の損失」・「プライバシー」・「性能・品質」の観点から影響度ファクターを導出し、影響度を見積
- 発生可能性と影響度からコンポーネントリスクを評価

本ガイドラインでは、リスク分析手法として、IT システム分野における標準的なリスク分析手法である OWASP（The Open Web Application Security Project）の OWASP Risk Rating Methodology をベースとした手法を適用する（図 3.13 参照）。

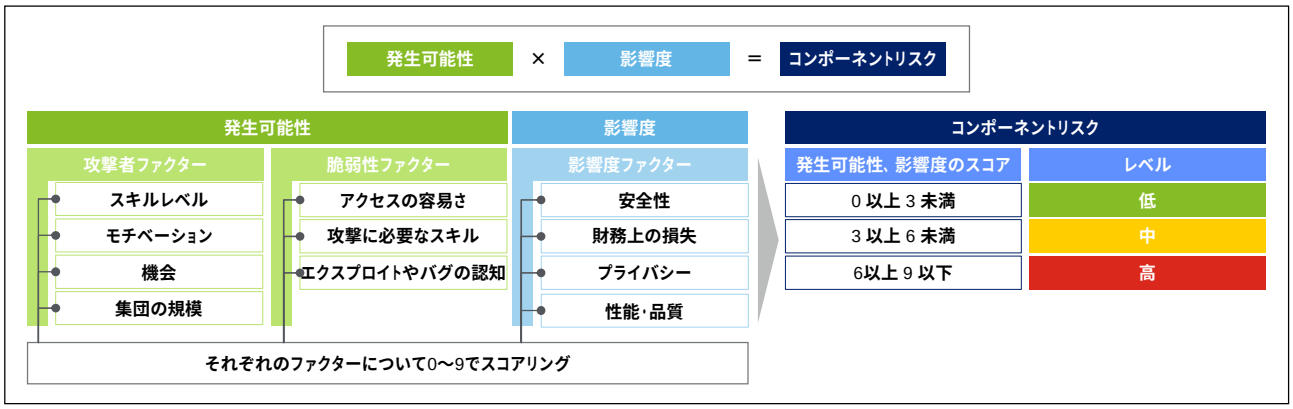


図 3.13 リスク分析手法の考え方

本節では、「3.3.5 攻撃者が興味を示すコンポーネントの特定」で特定した攻撃者の標的となり得るコンポーネントごとにコンポーネントリスクを評価する方法を説明する。

なお、コンポーネントリスクは、発生可能性と影響度それぞれのスコアに応じて、高、中、低のレベルを導出することで評価する。また、発生可能性は攻撃者ファクターと脆弱性ファクターからなり、影響度は影響度ファクターからなる。

コンポーネントリスクを構成するそれぞれの要素の説明は表 3-3 のとおりである。

表 3-3 コンポーネントリスクを構成する要素

（カッコ内は OWASP Risk Rating Methodology で使用される用語を表す）

コンポーネントリスクの構成要素		内容
発生可能性（Likelihood）		脆弱性が攻撃者によって発見され、悪用される可能性の尺度
	攻撃者ファクター（Threat Agent Factors）	攻撃者による攻撃が成功する可能性の尺度
	脆弱性ファクター（Vulnerability Factors）	当該コンポーネントで脆弱性が発見され、悪用される可能性の尺度

コンポーネントリスクの構成要素		内容
影響度（Impact）		攻撃が成功した場合の影響の尺度
	影響度ファクター（Impact Factors）	脆弱性が悪用される場合のシステムへの影響の尺度

当該ステップで実施する事項は多岐に及ぶため、流れを図示すると図 3.14 のとおりである。
次項より、各サブステップを順に説明する。

図 3.14 (公開資料のため、記載内容を削除)

3.4.1. 攻撃者ファクターの導出

攻撃者ファクターは、特定の脆弱性が、攻撃者によって発見され、悪用される可能性の尺度であり、攻撃者の「スキルレベル」、「モチベーション」、「機会」、「集団の規模」の 4 つの要素からなる。「スキルレベル」、「機会」、「集団の規模」は攻撃者ごとにスコアリングを行い、「モチベーション」は攻撃者と機能の組み合わせごとにスコアリングを行う。それぞれの要素は、0～9 の尺度でスコアリングし、攻撃者ファクターは 4 つの要素の尺度の平均値で計算する。
攻撃者ファクターの 4 つの要素は表 3-4 のとおりである。

表 3-4 攻撃者ファクターの構成要素

攻撃者ファクターの構成要素	内容
スキルレベル	攻撃者はどの程度熟練しているか
モチベーション	攻撃者が標的とする機能に関して、どの程度モチベーションがあるか
機会	攻撃者がコンポーネントを攻撃するのにどの程度のツール類（HW および SW）や情報を必要としているか
集団の規模	攻撃者の規模はどの程度か

攻撃者ファクターの導出は図 3.15 の手順で実施する。

図 3.15 (公開資料のため、記載内容を削除)

3.4.1.1. 攻撃者ごとのスコアリング

「3.2.2 攻撃者のプロファイル」で実施した攻撃者ごとの定性評価の結果に基づき、攻撃者の「スキルレベル」、「モチベーション」、「機会」、「集団の規模」の 4 つの要素についてそれぞれスコアリングする。スコアリング結果は図 3.16 のとおり整理する。

なお、「スキルレベル」、「機会」、「集団の規模」は、攻撃者ごとにスコアリングを行うのに対し、「モチベーション」は、攻撃者と機能の組み合わせごとにスコアリングを行うため、「モチベーション」のスコアリング結果は下図の枠内に整理することとなる。ただし、スコアリングを行う対象となる機能は、「3.3.4 攻撃者が興味を示す機能の特定」において、複数の攻撃者が興味を示すとされた機能に限定される。

図 3.16 (公開資料のため、記載内容を削除)

3.4.1.2. 機能ごとの攻撃者ファクターの導出

「3.3.4 攻撃者が興味を示す機能の特定」において、どの攻撃者がどの機能を標的とし得るかが特定されているため、それぞれの機能に対し、「3.4.1.1 攻撃者ごとのスコアリング」の結果に基づき、攻撃者の「スキルレベル」、「モチベーション」、「機会」、「集団の規模」の 4 つの要素のスコアを導出し、その平均値を求めることで、機能ごとの攻撃者ファクターを導出する。

なお、機能ごとに、4 つの要素について異なるスコアを持つ複数の攻撃者の標的となり得ると想定される。この場合は、各要素について、ワーストケース(最高値となるスコア)を使用する。

図 3.17 に示す機能ごとの攻撃者ファクターの導出の考え方に従い、「3.3.4 攻撃者が興味を示す機能の特定」において特定した機能ごとに攻撃者ファクターを導出する。

図 3.17 (公開資料のため、記載内容を削除)

なお、機能ごとの攻撃者ファクターの導出結果は図 3.18 のとおり整理する。

図 3.18 (公開資料のため、記載内容を削除)

3.4.1.3. コンポーネントごとの攻撃者ファクターの導出

「3.3.5 攻撃者が興味を示すコンポーネントの特定」において、攻撃者の標的となり得る機能を構成するコンポーネントが特定されているため、それぞれのコンポーネントに対し、「3.4.1.2 機能ごとの攻撃者ファクターの導出」の結果に基づき、当該機能を構成するコンポーネントごとの攻撃者ファクターを導出する。

なお、同一のコンポーネントが、複数の機能を構成していることも想定される。この場合は、ワーストケース(最高値)の攻撃者ファクターを使用する。

図 3.19 (公開資料のため、記載内容を削除)

なお、コンポーネントごとの攻撃者ファクターの導出結果は図 3.20 のとおり整理する。

図 3.20 (公開資料のため、記載内容を削除)

3.4.2. 脆弱性ファクターの導出

脆弱性ファクターは、コンポーネントで脆弱性が発見され、悪用される可能性の尺度であり、「アクセスの容易さ」、「コンポーネントの攻撃に必要な情報やツール」、「エクスプロイトやバグの認知」の 3 つの要素からなり、コンポーネントごとにスコアリングを行う。スコアリングの際には、当該コンポーネントがどの機能で使用されているかという観点は考慮せずに、あくまでもコンポーネント単体に対して評価する。

それぞれの要素は、0～9 の尺度でスコアリングし、脆弱性ファクターは 3 つの要素の尺度の平均値で計算する。

脆弱性ファクターの 3 つの要素は表 3-5 のとおりである。

表 3-5 脆弱性ファクターの構成要素

脆弱性ファクターの構成要素	内容
アクセスの容易さ	攻撃者が当該コンポーネントにどの程度容易にアクセスできるか
コンポーネントの攻撃に必要な情報やツール	攻撃者が当該コンポーネントの脆弱性をどの程度容易に悪用できるか
エクスプロイトやバグの認知	当該コンポーネントの脆弱性はどの程度知られているか

「3.3.5 攻撃者が興味を示すコンポーネントの特定」において、攻撃者の標的となり得る機能を構成するコンポーネントが特定されているため、それぞれのコンポーネントに対し、「アクセスの容易さ」、「コンポーネントの攻撃に必要な情報やツール」、「エクスプロイトやバグの認知」の 3 つの要素についてスコアリングを行い、その平均値を求めることで、脆弱性ファクターを導出する。

脆弱性ファクターの導出結果は図 3.21 のとおり整理する。

図 3.21 (公開資料のため、記載内容を削除)

3.4.3. 発生可能性の計算

発生可能性は、脆弱性が攻撃者によって発見され、悪用される可能性の尺度であり、「3.4.1 攻撃者ファクターの導出」で求めた攻撃者ファクターと「3.4.2 脆弱性ファクターの導出」で求めた脆弱性ファクターから、コンポーネントごとに計算する。なお、発生可能性は攻撃者ファクターと脆弱性ファクターの平均値である。

発生可能性の計算結果は図 3.22 のとおり整理する。

図 3.22 (公開資料のため、記載内容を削除)

3.4.4. 影響度ファクターの導出

影響度ファクターは、脆弱性が悪用される場合のシステムへの影響の尺度であり、「安全性」、「財務上の損失」、「プライバシー」、「性能・品質」の 4 つの要素からなり、コンポーネントごとにスコアリングを行う。それぞれの要素は、0～9 の尺度でスコアリングし、影響度ファクターは 4 つの要素の

尺度の平均値で計算する。

影響度ファクターの 4 つの要素は表 3-6 のとおりである。

表 3-6 影響度ファクターの構成要素

影響度ファクターの構成要素	内容
安全性	当該コンポーネントが攻撃されセキュリティが侵害された場合、安全性に係る影響はどの程度あるか
財務上の損失	当該コンポーネントが攻撃されセキュリティが侵害された場合、OEM または車両オーナーに対する財務上の損失はどの程度あるか
プライバシー	当該コンポーネントが攻撃されセキュリティが侵害された場合、プライバシーや機密性の損失はどの程度あるか
性能・品質	当該コンポーネントが攻撃されセキュリティが侵害された場合、車両性能や品質に係る影響はどの程度あるか

「3.3.5 攻撃者が興味を示すコンポーネントの特定」において、攻撃者の標的となり得る機能を構成するコンポーネントが特定されているため、それぞれのコンポーネントに対し、「安全性」、「財務上の損失」、「プライバシー」、「性能・品質」の 4 つの要素についてスコアリングを行い、その平均値を求めることで、影響度ファクターを導出する。

影響度ファクターの導出結果は図 3.23 のとおり整理する。

図 3.23 （公開資料のため、記載内容を削除）

3.4.5. 影響度の見積

影響度は、攻撃が成功した場合の影響の尺度であり、「3.4.4 影響度ファクターの導出」で求めた影響度ファクターと同値である。

影響度の見積結果は図 3.24 のとおり整理する。

図 3.24 （公開資料のため、記載内容を削除）

3.4.6. コンポーネントリスクの評価

攻撃者の標的となり得るコンポーネント全てに対し、表 3-7 に従い、発生可能性と影響度のスコアに応じてそのレベルを「高」、「中」、「低」で評価する。

表 3-7 発生可能性と影響度のスコアとそれに応じたレベル

スコア	レベル
0 以上 3 未満	低
3 以上 6 未満	中
6 以上 9 以下	高

また、発生可能性と影響度の積を計算し、コンポーネントリスクを評価する。なお、コンポーネントリスクの評価結果は図 3.25 のとおり整理する。

図 3.25 (公開資料のため、記載内容を削除)

また、リスク分析の結果を視覚的に捉える上で、発生可能性と影響度のレベルに従い、リスクヒートマップにマッピングすることが望ましい。

図 3.26 (公開資料のため、記載内容を削除)

3.5. 評価計画の立案

5 番目のステップ「3.5 評価計画の立案」では、主として以下を実施する。

- テスト実施に向けたテスト対象範囲の決定
- テスト対象のコンポーネントを対象とした詳細な技術的な分析
- テスト実施に向けた評価計画の作成

当該ステップで実施する事項の流れを図示すると図 3.27 のとおりである。
次項より、各サブステップを順に説明する。

図 3.27 （公開資料のため、記載内容を削除）

3.5.1. テストスコープの決定

「3.1 事前調整」において、評価依頼者と評価実施者との間であらかじめ合意した評価期間や評価範囲等に基づき、テストを実施する際のスコープについて協議し、最終的に合意する。

当該ステップにおいて、テスト対象とするコンポーネントを選定することになるが、「3.4.6 コンポーネントリスクの評価」において、リスクヒートマップにより、それぞれのコンポーネントごとに発生可能性と影響度のレベルがマッピングされているため、当該マップを活用し、どのコンポーネントをテスト対象とするかを双方の協議の上で決定する。

また、テストに割り当て可能なリソース（ヒト、モノ、カネ、時間）は有限であることから、テスト対象のコンポーネント数が多ければ、1 つのコンポーネントに対し実施できるテストは少なくなり、逆にテスト対象のコンポーネントが少なければ、1 つのコンポーネントに対し深度あるテストを行うことができる。このため、テスト対象のコンポーネントの決定に加え、どの程度までテストを行うか（テスト深度）についても合意が必要となる。テスト深度の決定に際しては、評価対象の各コンポーネントにおける大まかなテスト項目数を見積る必要がある。その上で、テスト期間やテスト体制・人数等を鑑みて、テスト深度を決定する。

テストを実施する上で評価依頼者と評価実施者の間で合意すべき事項を表 3-8 示す。これらの内容は、評価計画書にも記載する。

表 3-8 （公開資料のため、記載内容を削除）

3.5.2. 技術的分析

技術的分析では、対象のコンポーネントに対して「3.5.1 テストスコープの決定」より定義されたテストの範囲と深度に基づきテスト項目を検討するために技術的な詳細分析を行う。具体的には、コンポーネント間の接続関係や、通信プロトコルを明らかにする。

3.5.2.1. 関連情報の収集

技術的分析の準備として、必要な関連情報の収集を行う。技術的分析を行うためには、「3.3 攻撃対象コンポーネントの特定」で選別した対象コンポーネントの接続関係や、接続に用いられている通信プ

ロトコル等が分かる情報を収集する必要がある。情報収集においては、評価のアプローチ（ブラックボックス／グレーボックス／ホワイトボックス）によってその対応が異なる。

ブラックボックステストの場合は、開発部門からの情報提供はなく、ユーザーマニュアルやサービスマニュアル等の一般に入手可能な情報から収集する必要がある。なお、これらドキュメントの入手については、時間を要する場合もある点について留意する。また、一般に入手可能な情報について、適宜インターネット（特定のユーザーのみに限定されておらず、一般に公開されており、検索サイトで検索可能な Web サイト）からの情報も活用することが望ましい。更に、情報が十分でない場合は、必要に応じてリバースエンジニアリングによる情報収集を実施することが望ましい。

グレーボックスまたはホワイトボックステストの場合は、開発部門から詳細な設計情報等の一部または全てが提供されるので、必要に応じて情報収集を行う。

一般的に入手可能な情報の例を表 3-9 に示す。

表 3-9 (公開資料のため、記載内容を削除)

3.5.2.2. 車両のセキュリティに関する理論的検討

リスク分析で実施した各機能とコンポーネントのマッピングでは、コンポーネントがどのように接続されているかまでは明らかにしていない。ここでは、収集した情報を用いて可能な範囲でシステムにおけるコンポーネント間のつながりを明確にする。具体的には、ECU、センサー、アクチュエータおよびそれらを接続するワイヤーハーネス等のコンポーネント間の接続を収集した情報から推定し、システムブロック図等を作成する。また、コンポーネント間の結線情報として、その接続方式と、通信を行っている場合はプロトコルを明確にする。システムブロック図によりコンポーネント間の接続および通信プロトコルを明確にした後、有線／無線インターフェースでの侵入経路を検討する。例えば、どのような信号を受信するか、どのようなセンサーが搭載されているか、どのようなオーディオ入力があるか（Bluetooth 等）を考慮し検討を行う。検討に際して表 3-10 の要素についても考慮に入れるとよい。

表 3-10 (公開資料のため、記載内容を削除)

有線／無線インターフェースにおける侵入経路を明確にした後、テスト項目を検討する。テスト項目の検討においては、通信プロトコルごとに一般的に実施されるテスト項目、過去のインシデント事例における攻撃者の目標および既に実装されているセキュリティ対策の回避策の観点について検討する。一般的なテスト項目の検討に際しては、付録 2 に記載されている一般的な評価項目を参照されたい。なお、付録 2 は「付録 2.1 自動車における既知の脆弱性に対する一般的な評価項目」と「付録 2.2 IT システム分野における既知の脆弱性に対する一般的な評価項目」のように、自動車分野および IT システム分野に分けて記載してあるので、その点に留意して参照するとよい。

ここまでの作業は、限られた情報による可能な範囲での分析であるため、前提を明確にした上で推測を含んでいても構わない。但し、その前提や、導出されたテスト項目については、評価依頼者と評価実施者の間で認識を合わせるために合意しておくことが重要である。

3.5.3. 評価計画の作成

「3.5.1 テストスコープの決定」でテスト依頼者とテスト実施者との間で合意した事項を盛り込んだ評価計画を作成する。

評価計画の目次の例を図 3.28 に示す。

図 3.28 （公開資料のため、記載内容を削除）

評価項目の作成については、基本的には評価責任者が既知の脆弱性情報等をもとに都度作成する必要がある。なお、本ガイドラインの付録 2 では一般的な評価項目を例示しており、図 3.29 に示す手順を参考に評価項目を作成することもできる。

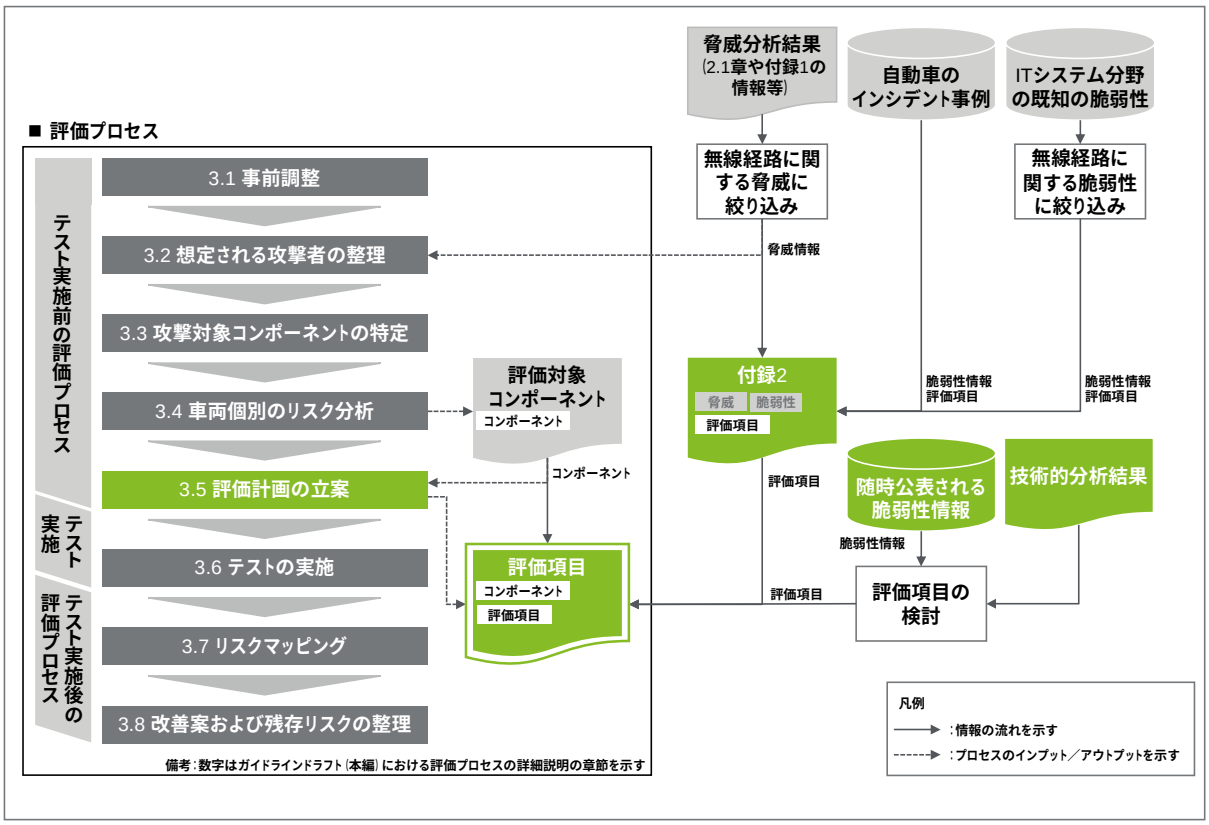


図 3.29 評価項目の作成に至るプロセスと情報の関連性

付録 2 に例示した評価項目に含まれる内容の概要について図 3.30 に示す。

<table>
<tr><th colspan="2">脆弱性の分類</th><th>付録2で考慮する脆弱性の内容</th></tr>
<tr><td colspan="2">自動車分野で既知</td><td>■ 自動車分野における過去のインシデント事例
・ 米国A社におけるIVIの脆弱性
・ 欧州B社におけるコネクテッドサービスの脆弱性
・ 米国C社の無線LAN脆弱性
・ 日本D社のモバイルアプリ脆弱性 等</td></tr>
<tr><td rowspan="2">自動車分野で未知</td><td>ITシステム分野で既知</td><td>■ ITシステム分野における既知の脆弱性のうち、自動車に適用可能なもの
・ コネクテッドサーバー側の脆弱性
・ Webアプリの脆弱性 など</td></tr>
<tr><td>上記以外</td><td>■ 対象外
※自動車およびITシステム分野で公表される情報を踏まえ、適時アップデートが必要</td></tr>
</table>

図 3.30 付録 2 に含まれる脆弱性内容概要

付録 2.1 では自動車分野で既知の脆弱性として、セキュリティ研究者によって発見され海外のカンファレンスやインターネット等で公表済である主なインシデント事例を記載している。また、自動車分野で未知の脆弱性であっても、IT システム分野においては既知の脆弱性は考慮しており、その中でも特に自動車に適用可能な脆弱性について付録 2.2 にて記載している。

IT システム分野の脆弱性は、CWE List Version 3.0（共通脆弱性タイプ一覧）を基本として参照している。CWE List Version 3.0 では 700 種類を超える脆弱性が公表されているため、一般に本リストを活用する場合にどこから着手すればよいか判断するだけでも大変な作業となる。限られたリソースを有効に活用し最大限の効果を得るためには、個別の脆弱性に逐一対応するのではなく、全般的な根本原因を基に開発者が実際に犯しやすいプログラミングエラーや設定ミス等をより重点的に対策する必要がある。そこで付録 2.2 において一般的な評価項目とするために、2011 CWE/SANS Top 25 および OWASP Top Ten（2013）のリストを基に、より重要度の高い脆弱性に対して抽出している。

2011 CWE/SANS Top 25 は、セキュリティ分野で権威ある専門家が、セキュリティバグの原因となり得る、サイバー攻撃につながる恐れのある最も危険なプログラミングエラー25 項目のコンセンサスリストとして共同発表したものである。また、OWASP Top Ten（2013）は、コンサルティング会社 4 社、ツール/SaaS ベンダー3 社を含む、アプリケーションセキュリティ専門の 7 社から提供された情報を用い、悪用難易度、検出難易度および影響についての統計データに基づいて選択・順位付けされた脆弱性のリストである。このような専門家の判断による項目の優先付けは、特にリソースの制限されるペネトレーションテストにおいては有用とされる。

優先付けされた脆弱性から、付録 2.2 における一般的な評価項目を導出するために CWE（Common Weakness Enumeration）に割り当てられた CAPEC（Common Attack Pattern Enumeration and Classification）を利用している。これにより重要度の高い脆弱性に対する評価項目において、攻撃パターンの十分性を確保している。また、ポートスキャン等、脆弱性に紐づかない攻撃パターンについては CAPEC から必要な評価項目を整理し追加している。

但し、付録 2.2 においては、脆弱性に優先的に取り組むべき脆弱性に絞っていることから、あくまで一般的な評価項目の一覧とし、評価項目を網羅的に列挙したものではないことには留意が必要である。

そのために、安全性に係るコンポーネントや機密性の高い情報を扱うコンポーネント等は必要に応じて、自動車分野および IT システム分野において随時更新される脆弱性情報も合わせて確認する必要がある。このように幅広く網羅的な脆弱性調査が必要となる場合は、外部の専門家に依頼することも視野に入れ検討するとよい。

付録 2 および随時公表される脆弱性情報から評価項目を抽出する際は、「3.4 車両個別のリスク分析」にて評価対象として特定されたコンポーネントにおいて、「3.5.2 技術的分析」の結果として明らかになった有線／無線インターフェースについての評価項目を抽出する。なお、付録 2 には、関連する技術列を付与してあるため、評価項目の抽出においては当該情報を参考にできる。

評価項目の検討結果は、表 3-11 に示すとおり、評価項目の一覧として取りまとめる。また、テストを実施した結果についても記載ができるようにしておく。

作成した評価計画および評価項目については、最終的に評価依頼者と評価実施者の間で合意する。

表 3-11 (公開資料のため、記載内容を削除)

3.6. テストの実施

6 番目のステップ「3.6 テストの実施」では主として、以下を実施する。

・　評価計画に従ったテストの実施

3.6.1. テスト実施前の対応事項

テストの実施に際しては、事前準備の段階で合意したセキュリティや安全の確保された場所やテスト環境を準備する必要がある。

また、テスト固有のツールを要する場合があり、使用するツールについてテスト前に検討および判断をする必要がある。テストに必要なツールについては、各通信プロトコルの実践手引きの付録を参照されたい。

テストにおいて、評価対象に対して事前の情報収集のために分解等の物理的な操作を行う場合がある。このような場合は、分解を行う前に評価対象（コンポーネント）について写真等で記録することが重要である。記録の際には、対象となるコンポーネント毎に ID 等を付与し、識別可能な状態にしておくことが望ましい。

3.6.2. テスト実施中および実施後の対応事項

評価計画の立案で作成した評価項目に従ってテストを実施する。テストにおける詳細な手順については、各通信プロトコルの実践手引きを参照されたい。

テスト実施中は、各評価項目の実行コマンドや、その実行結果について、評価 PC 画面のキャプチャ等により記録することが重要となる。これによりテストの再現性向上に役立つだけでなく、評価レポート作成を効率的に進めることができる。

発見事項および評価結果についてはそれぞれ後述する表 4-2、表 4-3 に記載する項目について記録する。

また、テストにて発見された脆弱性については、「3.7 リスクマッピング」および「3.8 改善案および残存リスクの整理」に従い、脆弱性のリスク評価およびリスク低減策の検討を実施する。

3.7. リスクマッピング

7 番目のステップ「3.7 リスクマッピング」では主として、以下を実施する。

・　テストによって発見された脆弱性に対するリスク評価

当該ステップで実施する事項の流れを図示すると図 3.31 のとおりである。

図 3.31 （公開資料のため、記載内容を削除）

リスク評価には CVSS（Common Vulnerability Scoring System）の基本評価基準（Base Metrics）に基づいた評価基準を用いており、自動車に固有な要件を考慮し、以下の 4 つのレイヤーでリスク評価手法を定義する。

① CVSS v3.0 の標準的なメトリクスを用いたコンポーネントレベルリスク評価
② CVSS v3.0 の標準的なメトリクスを用いた車両レベルリスク評価
③ 低、中、高、緊急の 4 つの定性的な基準を用いたフリートレベルリスク評価
④ 上記①～③の加重平均によるトータルリスク

テストにより発見された脆弱性ごとに、コンポーネントレベルリスク、車両レベルリスク、フリートレベルリスクをそれぞれ算出した上で、それらの加重平均を行い、トータルリスクを算出する。そのトータルリスクを最終的な指標として、発見された脆弱性の評価を行う。

以下に、各リスクの評価基準および算出方法について説明する。

3.7.1. コンポーネントレベルリスク評価

3.7.1.1. コンポーネントレベルリスクの評価基準

CVSS の基本評価基準における脆弱性評価の構成要素は、攻撃元区分（AV）、攻撃条件の複雑さ（AC）、必要な特権レベル（PR）、ユーザー関与レベル（UI）、スコープ（S）、機密性への影響（C）、完全性への影響（I）、可用性への影響（A）の 8 つがある。それぞれの構成要素について、定性的な評価およびそれに紐付く定量的な評価（スコア）が定義されている。

コンポーネントレベルリスクは、対象となるコンポーネント単体でのリスクを意味する。CVSS v3.0 に基づいたコンポーネントレベルでのリスクに対する構成要素を表 3-12 に示す。リスクの構成要素ごとに尺度を選択し、その際に選択した理由を具体的に記録することが重要である。なお、既存の脆弱性であれば、JPCERT/CC 等で公表している脆弱性分析結果を参考にしながら、評価してもよい。

表 3-12 （公開資料のため、記載内容を削除）

3.7.1.2. コンポーネントレベルリスクの計算方法

基本評価基準の基本値としてコンポーネントレベルリスクを計算する。計算に際して、まず影響度と攻撃容易性の 2 つのパラメータについて値を求める。影響度と攻撃容易性については、それぞれ以下に示す CVSS v3.0 に準拠した式で計算する。なお、車両レベルリスクについても本計算方法と同一である。

3.7.2. 車両レベルリスク評価

3.7.2.1. 車両レベルリスクの評価基準

車両レベルリスクは、コンポーネント同士が接続されることにより構成された車両単体におけるリスクを意味する。CVSS v3.0 に基づく車両レベルリスクの構成要素を表 3-13 に示す。コンポーネントレベルリスクの評価と同様に、リスクの構成要素ごとに尺度を選択し、その際に選択した理由を具体的に記録する。

表 3-13 （公開資料のため、記載内容を削除）

3.7.2.2. 車両レベルリスクの計算方法

3.7.1.2 コンポーネントレベルリスクの計算方法と同様に、車両レベルリスクを計算する。

3.7.3. フリートレベルリスク評価

フリートレベルリスクは、1 つの脆弱性が一台の車両のみならず、複数の車両に影響を与える場合を考慮したリスクである。フリートレベルリスクは、表 3-14 に示す CVSS v3.0 の深刻度評価尺度のスコアを参照している。

表 3-14 CVSS v3.0 の深刻度評価尺度

深刻度	スコア
無	0
低	0.1－3.9
中	4.0－6.9
高	7.0－8.9
緊急	9.0－10.0

表 3-15 にフリートレベルリスクの評価尺度を示す。

表 3-15 （公開資料のため、記載内容を削除）

3.7.4. トータルリスク評価

トータルリスクは、コンポーネントレベルリスク、車両レベルリスク、フリートレベルリスクの加重平均により求める。一般に、それぞれのリスクの大小関係は、1 つの脆弱性の影響が及ぶ範囲に比例するため「フリートレベルリスク」＞「車両レベルリスク」＞「コンポーネントレベルリスク」と考えることができる。本ガイドラインにおける、それぞれのリスクに対する重み付けを表 3-16 に示す。

表 3-16 （公開資料のため、記載内容を削除）

最終的に、トータルリスクのスコアを、表 3-16 に照らし合わせ、脆弱性における深刻度の評価を行う。

3.7.5. リスク評価例

「3.6 テストの実施」において、表 3-17 の脆弱性が見つかったと仮定し、実際に実施したリスク評価のサンプルを図 3.32 に示す。

表 3-17 (公開資料のため、記載内容を削除)

図 3.32 (公開資料のため、記載内容を削除)

3.8. 改善案および残存リスクの整理

8 番目のステップ「3.8 改善案および残存リスクの整理」では主として、以下を実施する。

- リスク評価の結果から、リスクに対する対処の明確化
- 対処実施後における残存リスクの整理

当該ステップで実施する事項を図 3.33 に示す。

図 3.33 （公開資料のため、記載内容を削除）

3.8.1. 発見事項に対する改善案の検討

リスク評価により深刻度が評価されたリスクに対して、どのような対処を実施するかを検討する。対処の方法には、リスクの低減、リスクの回避、リスクの移転、リスクの保有の大きく 4 つがある。

表 3-18 リスクの対処の方法

対処の観点	内容
リスクの低減	脆弱性に対して情報セキュリティ対策を施すことにより、脅威発生の可能性を下げること
リスクの回避	脅威発生の要因を停止または全く別の方法に変更することにより、リスクが発生する可能性を取り去ること
リスクの移転	リスクを他社等に移すこと。リスクが発生した場合に備え保険に入り、損失補償を準備する等が考えられる
リスクの保有	特にリスクを低減するためのセキュリティ対策を行わず、許容範囲内として受容することである。この対処は、当該リスクの発生頻度や影響が小さいことが前提となる

これらの観点を参考にして、個々のリスクにおける改善案を検討する。また、それぞれの改善案には、短期的、中期的、長期的といった時間軸の観点を含める。時間軸については表 3-19 の観点を考慮する。

表 3-19 改善案検討における時間軸

対処	考慮すべき観点
短期的対策	全体の設計に対する影響がなく、対策に要するコストが低い
中期的対策	コンポーネントレベルでの対策に労力を要するが、設計変更は限定的である
長期的対策	コンポーネントレベルでの対策に労力を要し、また大幅な設計変更を伴う

3.8.2. 残存リスクの整理

改善案を実施後に、残存するリスクについて明確にし、評価レポートに記載する。1 つの脆弱性に対して短期的、中期的、長期的と複数の改善案がある場合は、それぞれの改善案について残存するリスクを明確にし、評価レポートに記載する。

評価依頼者は、評価レポートに記載の残存リスクを鑑みて、実施する改善案について判断する。

4. 評価結果の報告

4.1. レポートの作成

テストで発見した脆弱性のリスク評価およびその改善案をレポートとして作成する。事前調整事項で合意した評価期間、体制等の情報や、「3.5 評価計画の立案」で決定した内容も記載する。

記載する項目例を表 4-1 に示す。

表 4-1 （公開資料のため、記載内容を削除）

4.1.1. 発見事項の整理

発見事項については、「3.7 リスクマッピング」にあるリスク評価手法を用いて、発見事項毎にコンポーネントレベルリスク、車両レベルリスク、フリートレベルリスク、トータルリスクに対するスコアおよび評価尺度の評価を行う。また、個別の発見事項毎に表 4-2 にある項目についてまとめる。

表 4-2 （公開資料のため、記載内容を削除）

4.1.2. 評価結果の整理

個別評価結果詳細については、表 4-3 にある項目についてまとめる。

表 4-3 （公開資料のため、記載内容を削除）

4.1.3. レポートの評価

前節で作成したレポートに対して、評価実施者が、表 4-4 に示すチェックリストを用いてレポートの評価を行うことが望ましい。各項目の記載の有無と記載ページを示すことで、評価依頼者によるレポート品質の確認が可能となる。チェック項目がレポートに含まれていない場合は、備考欄にその理由を記載する。

表 4-4 （公開資料のため、記載内容を削除）

付録1.想定される一般的な脅威一覧

（公開資料のため、記載内容を削除）

付録2.一般的な評価項目一覧

付録2.1. 自動車における既知の脆弱性に対する一般的な評価項目

（公開資料のため、記載内容を削除）

付録2.2. IT システム分野における既知の脆弱性に対する一般的な評価項目

（公開資料のため、記載内容を削除）

情報セキュリティ評価ガイドライン
ドラフト（実践手引き）Wi-Fi編
【成果報告書版】

2018年2月28日発行

【本書の位置づけ】
本書は、「情報セキュリティ評価ガイドラインドラフト（実践手引き）Wi-Fi 編 ver.3.2」をもとに、成果報告書版として作成したものである

目次

1. はじめに 1

1.1. **背景と目的** 1
1.2. **適用範囲** 2
1.3. **前提事項** 3
1.4. **用語の定義** 3
1.5. **本書の構成** 4
1.6. **参考文献** 4

2. プロトコル概要 5

2.1. IEEE 802.11 5
2.2. Wi-Fi 6
2.3. **無線** LAN **における通信モード** 6
2.4. **無線** LAN **の** MAC **フレーム** 6
2.4.1. **フレームフォーマット** 6
2.5. **無線** LAN **における暗号化技術** 7
2.5.1. WEP 7
2.6. WPS **による無線** LAN **ネットワークの確立** 8

3. 一般的な攻撃手法 9

3.1. **一般的な攻撃アプローチ** 9
3.1.1. Wi-Fi **に対する一般的な攻撃アプローチ** 10
3.2. **評価に必要なデバイスと評価端末の準備** 10
3.2.1. **評価に必要なデバイス等の準備** 10
3.3. **個別の攻撃手法の説明** 10

付録 1. 使用するツールの紹介 11

付録 2. 一般的な評価手法 11

1. はじめに

1.1. 背景と目的

自動車のコネクテッド化が進んでおり、ネットワークを経由して車内外の様々なデータのやり取りが可能となっている。これにより自動車の快適性および安全性が向上し、また、クラウドとつながることで様々なサービスを受けられるようになっている。その一方で、無線通信等のネットワークを経由した車外サービスの利用増により、車外からによる遠隔操作等のセキュリティ攻撃等のリスクが高まり、無線経由の通信に対してセキュリティを確保する必要性が高まっている。

また、今後、市場に登場するとみられる自動走行車両の場合、車両を市場へリリースした後の運用時においても、OTA（Over The Air）によるソフトウェア更新に伴う車両の仕様変更や、車外サービスの仕様変更に伴う車両への影響等の考慮が必要となることが考えられる。これらのことから無線経由の通信に対するセキュリティ確保の観点において、開発車に対するセキュリティ評価に加え、市販車に対するセキュリティ評価の必要性も高まっている。

開発車や市販車におけるセキュリティ評価においては、セキュリティ機能が要求通りに実現できているかという観点に加えて、車外からの実際の攻撃に対する耐ハッキング性能という観点がより重要となる。そこで、IT 業界で採用されているペネトレーションテストを、自動車にも適用する動きが高まっている。

ペネトレーションテストは、攻撃者視点によるセキュリティ評価であり、車両の脆弱性を利用して実際に外部から攻撃が可能かを検証する。これは他の、ツールによる脆弱性診断やファジングテスト等のセキュリティ評価とは異なる性質をもつ。ペネトレーションテストでは、攻撃者視点による評価という性質上、評価対象をブラックボックスとして扱う場合も多く、一般的に評価に用いる情報は制限されることから、情報収集に多くの労力を使う。また、実車両を必要とすることから、開発の終盤に評価が実施される場合が多く、評価期間やリソースについて制約も受ける場合もある。このように、情報や評価期間、リソース等の制約を大きく受けるペネトレーションテストに対しては、リスクアプローチにより攻撃対象を絞った上で効率よく評価を行うことが望まれる。

本ガイドラインは、情報セキュリティ評価ガイドライン(本編)に従い作成された評価計画に従い実際に評価を行うために必要となる、具体的な評価手法を検討する際に参照されることを想定したガイドラインである。そのため、情報セキュリティ評価ガイドライン(実践手引き)は要素技術毎にまとめられており、各実践手引きにおいては車両に対して一般的に実施されるペネトレーションテストの評価手法を含めている。ただし、実際の情報セキュリティ評価においては、ペネトレーションテストの目的にのっとり、本ガイドラインに記載された内容以外の評価手法についても臨機応変に組み込んでいく必要がある点には留意いただきたい。

1.2. 適用範囲

本ガイドラインでは、車両が有するインターフェースのうち、Wi-Fi を攻撃対象とした実践手引きを対象としている。具体的には、図 1-1 に示すとおり、攻撃者が車両の有する Wi-Fi により構成される無線 LAN ネットワークに対して接続を試みる、もしくは無線 LAN ネットワークまでのアプローチを範囲としており、無線 LAN ネットワークに接続後のアプローチ(例えば、IP ネットワークに対する攻撃等)については別の実践手引きにて説明する。

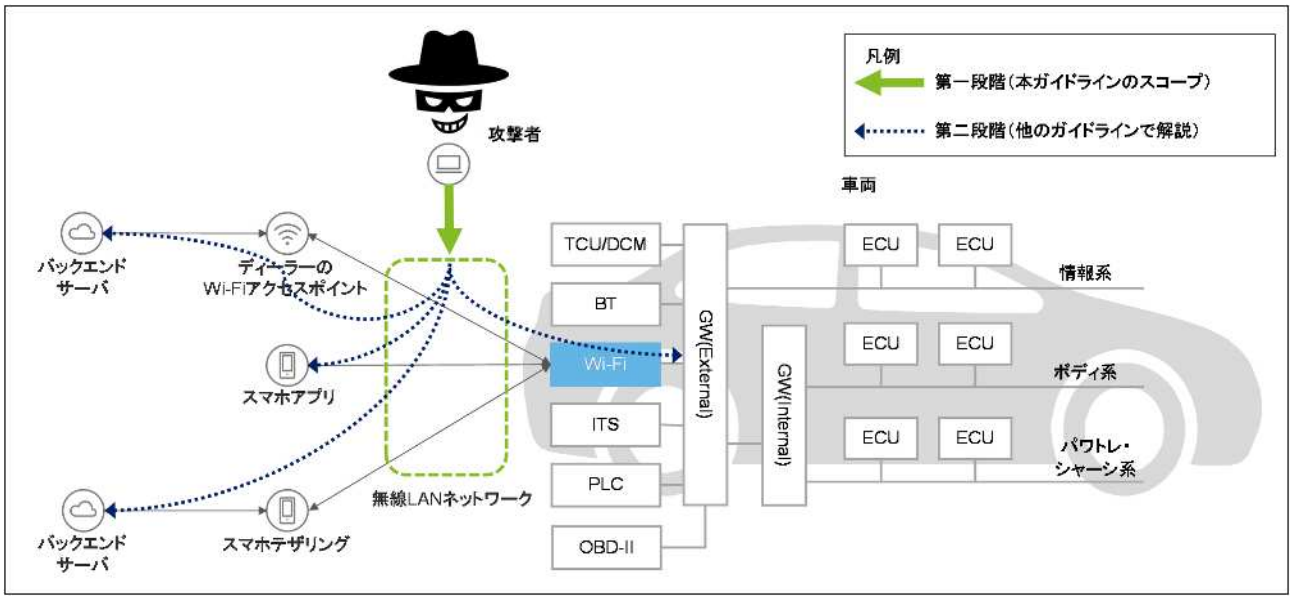


図 1-1 本ガイドラインの適用範囲

1.3. 前提事項

本ガイドラインは、情報セキュリティ評価ガイドライン(本編)に従い作成された評価項目のうち Wi-Fi に関連した評価項目に対する具体的な評価手法を検討する際に参照されることを目的としたガイドラインとなっており、活用される場面については、情報セキュリティ評価ガイドライン(本編)でも述べているように、図 1-2 に示す V 字プロセスにおける①車両総合評価、②市販車評価、③－1 システム設計、③－2 H/W-S/W 統合評価の 4 つのフェーズでの活用を想定している。

各フェーズでのガイドライン利用にあたる前提事項の詳細については、情報セキュリティ評価ガイドライン(本編)を参照のこと。

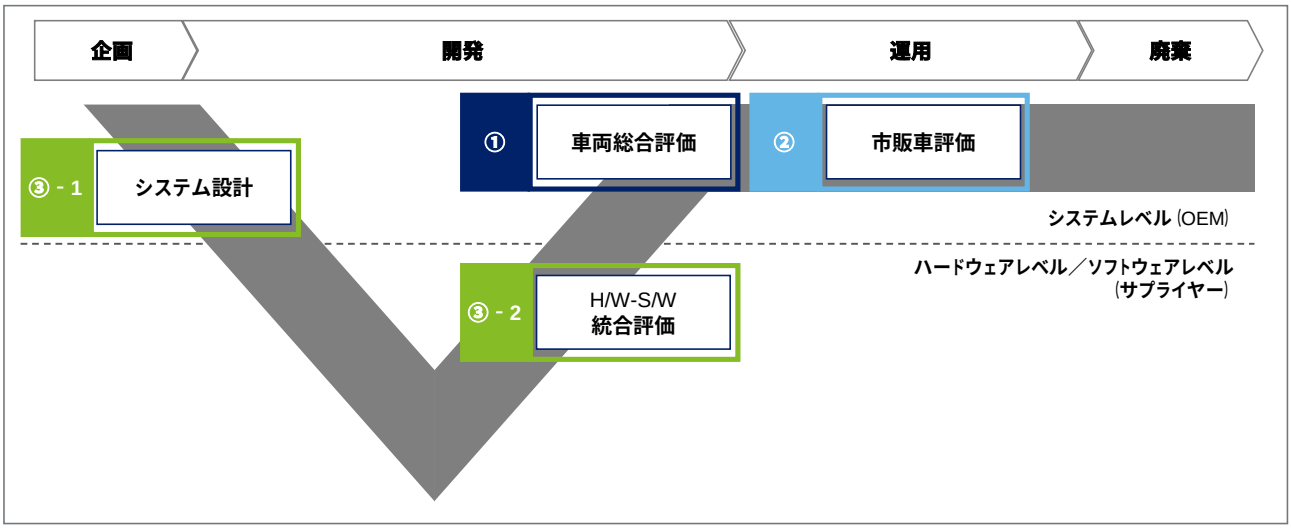


図 1-2　本ガイドラインの V 字プロセスにおける位置付け

1.4. 用語の定義

本ガイドラインで利用する用語とその定義を表 1-1 に示す。

表 1-1　（公開資料のため、記載内容を削除）

また、本ガイドラインで利用する略語の定義について表 1-2 に示す。

表 1-2　（公開資料のため、記載内容を削除）

1.5. 本書の構成

情報セキュリティ評価ガイドラインドラフト(Wi-Fi 編)は、以下の構成となっている。

第 1 章は、本書の目的、適用範囲や前提事項について述べる。

第 2 章は、Wi-Fi に関するプロトコルのうちペネトレーションテストを実施する上で必要となる内容について述べる。

第 3 章は、Wi-Fi に対する具体的な攻撃手法について記載する。ガイドラインにおける評価プロセスの詳細について説明する。

付録 1 は、Wi-Fi に対するペネトレーションテストを実施する上で必要となる代表的なツールを紹介する。

付録 2 は、Wi-Fi に対する一般的な評価手法について紹介する。

1.6. 参考文献

- インプレス R&D、改訂三版 802.11 高速無線 LAN 教科書、守倉 正博、久保田 周治[監修]
- 共立出版株式会社、無線 LAN セキュリティ-次世代技術 IEEE 802.11i と WPA の実際、Jon Edney、William A. Arbaugh[著]、加藤 聰彦[監訳]
- オライリー・ジャパン、802.11 無線ネットワーク管理 第 2 版、Matthew Gas[著]、渡辺　尚、小野　良司[監訳]、林　秀幸[訳]
- リックテレコム、パケットキャプチャ無線 LAN 編、竹下　恵 [著]
- Mc Graw Hill、Hacking Exposed Wireless-Third Edition: Wireless Security Secrets & Soutions、Joshua Wright[著]、Johnny Cache[著]

2. プロトコル概要

2.1. IEEE 802.11

無線 LAN を規定しているプロトコルは IEEE 802.11 である。IEEE 802.11 は図 2-1 に示すとおり、複数のプロトコルによって定義されており、主に論理的な制御を定義している 1 つの MAC (Media Access Control)層と、物理的に異なる通信方法を定義した複数の物理層(PHY)のプロトコルから構成されている。

無線 LAN がリリースされた当初は図 2-1 に示される 802.11 MAC と 802.11 PHY を IEEE 802.11 としてリリースし、その後も様々な異なる物理層(802.11b、802.11a 等)の規格や、セキュリティ機能の拡張(802.11i)を追加しており、これらを総称して IEEE 802.11 と呼んでいる。そのため、当初リリースされた IEEE 802.11(802.11 MAC と 802.11 PHY)はこれと比して、オリジナル IEEE 802.11 と呼ぶ場合もある。

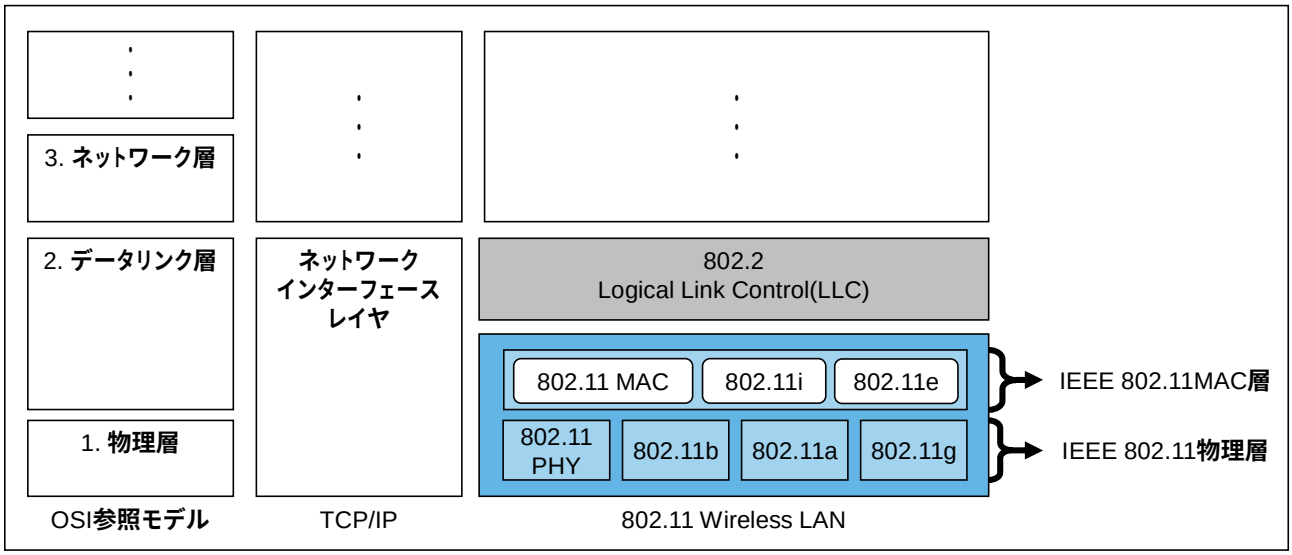


図 2-1 IEEE 802.11 プロトコルスタック

IEEE 802.11 には、MAC 層、物理層でそれぞれ様々なプロトコルが定義されている。その代表的な規格については表 2-1 に示すとおりである。

表 2-1 IEEE 802.11 関連の主な規格

規格	概要
IEEE 802.11	オリジナルの無線 LAN プロトコル。2.4GHz 帯および赤外線による 1Mbps、2Mbps の通信規格
IEEE 802.11a	5GHz 帯を利用した 54Mbps の通信規格
IEEE 802.11b	5.5Mbps、11Mbps の通信速度をサポートした 802.11 の拡張規格
IEEE 802.11g	2.4GHz 帯を利用した 54Mbps の通信規格
IEEE 802.11i	セキュリティ機能の拡張規格
IEEE 802.11n	MIMO (Multiple Input Multiple Output)を利用した高速通信規格
IEEE 802.11ac	5GHz 帯を利用した高速通信規格

（公開資料のため、記載内容を削除）

2.2. Wi-Fi

無線 LAN の名称として Wi-Fi もよく利用されている。無線 LAN 規格がリリースされた当初は、IEEE 802.11 の実装に関する詳細パラメータは各ベンダーにおいて独自で規定していたこともあり、相互接続に問題が生じる場合があった。そこで、WECA (Wireless Ethernet Compatibility Alliance、現在は Wi-Fi Alliance と呼ぶ)と呼ばれる民間団体において、無線 LAN 機器の相互接続の検証が行われるようになり、検証をパスしたデバイスには Wi-Fi ロゴが付与されるようになった。

それゆえ、無線 LAN のことを Wi-Fi と呼ぶケースも多いため本ガイドラインにおいても特に断りなく Wi-Fi と表現している箇所は無線 LAN と同義の扱いとする。

2.3. 無線 LAN における通信モード

無線 LAN においては、物理層レベルでは IEEE 802.11 に始まり、IEEE 802.11b、IEEE 802.11a 等、通信速度の異なる様々な通信規格が定義されているが、どの通信速度においても MAC 層レベルは共通であり基本的には以下の 2 つの通信モードのいずれかで動作している。

- インフラストラクチャモード
- アドホックモード

いずれのモードにおいても SSID (Service Set Identifier)と呼ばれる識別子を用いてどの無線 LAN に属する通信であるかを識別している。インフラストラクチャモードでは AP (Access Point、親機)が、アドホックモードでは STA が SSID を設定することとなっている。

（公開資料のため、記載内容を削除）

2.4. 無線 LAN の MAC フレーム

2.4.1. フレームフォーマット

無線 LAN の MAC フレームは図 2-2 に示すとおり、30 バイトのヘッダーとデータ、FCS (Frame Check Sequence)から構成される。フレーム本体については無線 LAN が持つ暗号機能(WEP、WPA、WPA2 等)を利用した場合は、暗号化されたデータとなる。

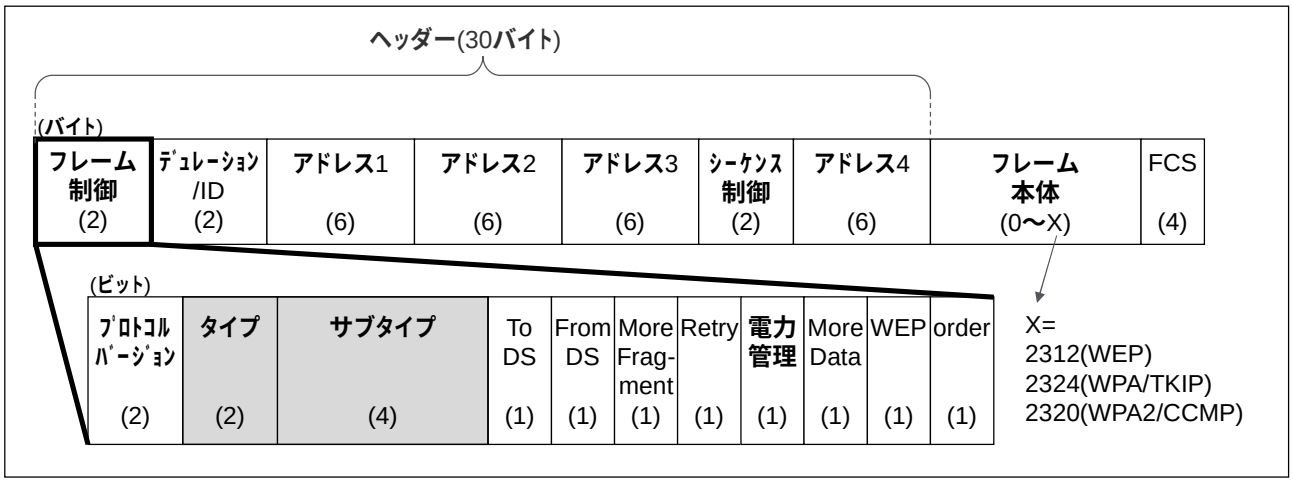


図 2-2 IEEE 802.11 MAC フレーム

（公開資料のため、記載内容を削除）

2.5. 無線 LAN における暗号化技術

2.5.1. WEP

WEP による暗号化のイメージを図 2-3 に示す。WEP においてはデータ送信時、事前に共有している WEP キーと呼ばれる共有鍵(40bit または 104bit)に加え、データ送信時に作成される IV (Initial Vector、24bit)を組み合わせた鍵(64bit または 128bit)が送信データの暗号化に利用される。

受信側は同じく事前に共有している WEP キーに加え、受信した無線 LAN フレームにある IV を取り出し、鍵を生成してデータを復号する。IV については平文として送信されていることおよび IV 自体が 24bit 長と比較的短いことや、単に共有鍵と IV を組み合わせたものから RC4 を利用して暗号化していることもあり、様々な欠陥が指摘されている。

その結果、WEP キーの解析ツールが公開され、基本的には一定量の無線 LAN フレームを収集できれば、鍵長に関わらず WEP キーを解析することが可能な状況となっている。

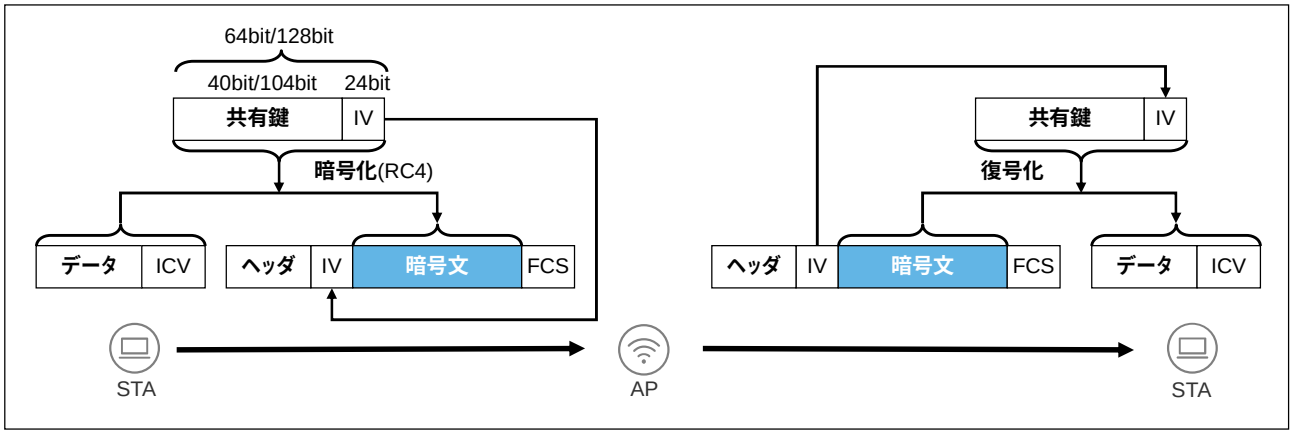


図 2-3 WEP による暗号化

（公開資料のため、記載内容を削除）

2.6. WPS による無線 LAN ネットワークの確立

Wi-Fi Protected Setup (WPS)とは、無線 LAN 機器の接続を容易に行うための規格であり、Wi-Fi Alliance が 2007 年 1 月頃から対応機器の認定を開始している。

WPS における代表的な接続方式は図 2-4 に示すとおり PBC (Push Button Configuration)方式と PIN (Personal Identification Number)方式がある。PBC 方式では無線 LAN の AP および STA に搭載された WPS ボタンを押下することで、接続が完了する。PIN コード方式では、STA にあらかじめ割り振られた 4 桁もしくは 8 桁の数字を AP へ登録する。近年は NFC (Near-field communication)や USB デバイスを利用した方式も利用されている。

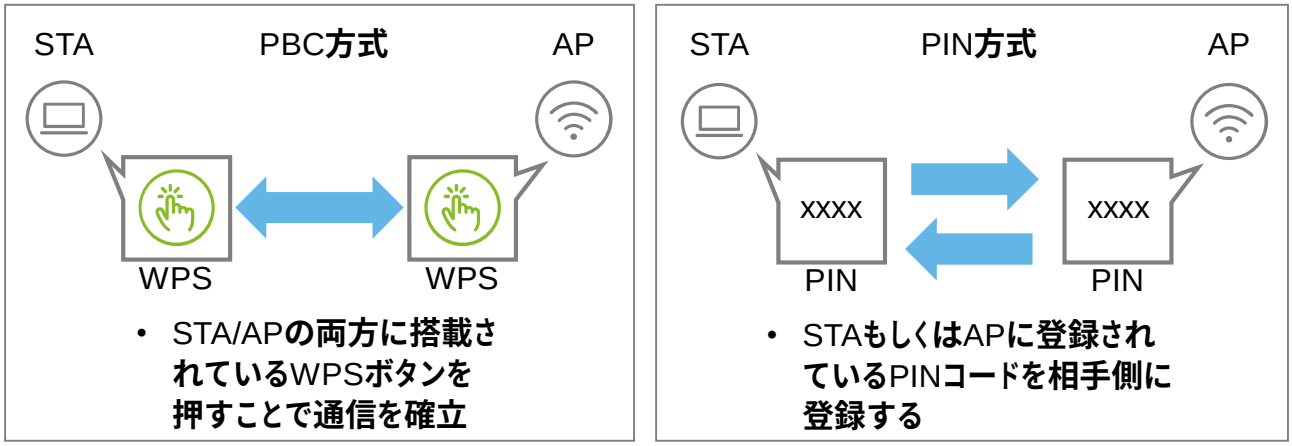


図 2-4 WPS における接続方式

3. 一般的な攻撃手法

3.1. 一般的な攻撃アプローチ

攻撃者が車両に対して攻撃を仕掛けようとした場合、最も魅力的に映る機能の 1 つが、車両とバックエンドサーバー、モバイルアプリ等を結ぶネットワークである。車両が有するネットワークインターフェースは TCU を始め、Wi-Fi や Bluetooth 等多岐にわたり、攻撃者はこれらが接続されたネットワークを介し、IVI(In-Vehicle Infotainment)、バックエンドサーバー、モバイルアプリ等への侵入を最初の目標とすることが想定される。

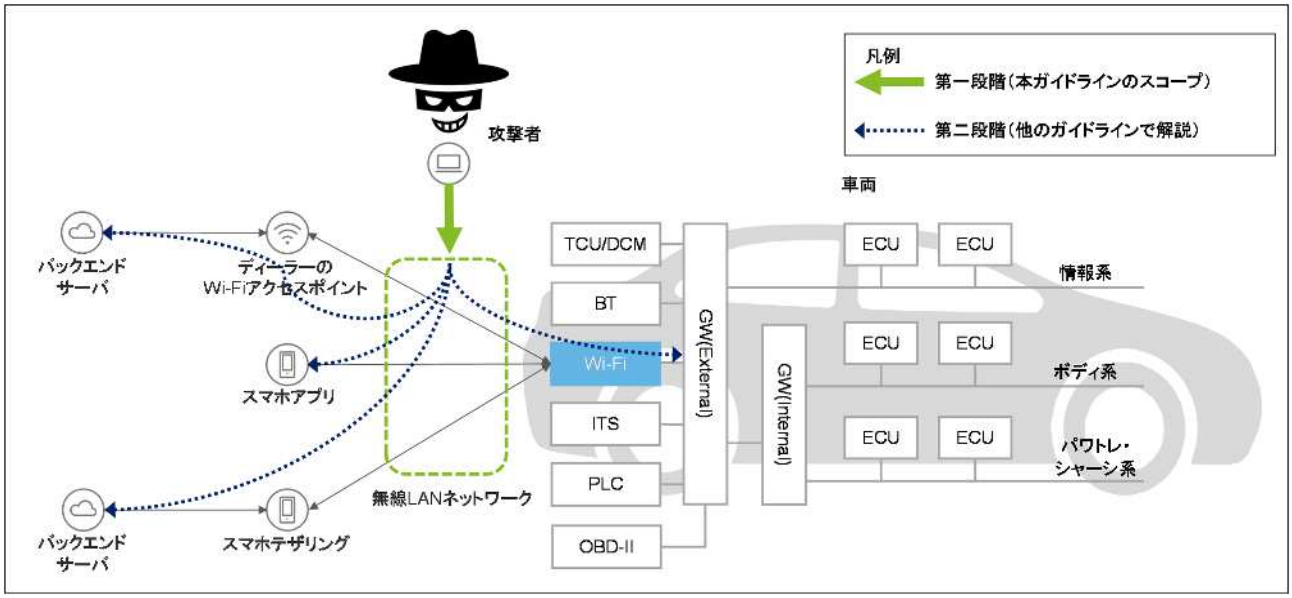


図 3-1 攻撃者による無線 LAN ネットワークに対する攻撃アプローチ

IVI 等への攻撃のアプローチは大きく二段階に分けることができる。第一段階目は、各種ネットワークに対して攻撃を実施し、IVI 等が属するネットワークへ接続することで IVI 等と通信できるようになることを目標とした攻撃であり、第二段階目は、IT 業界でもよく利用される攻撃手法を利用し、IVI 等への攻撃を試みることが目標となっている。

本ガイドラインでは図 3-1 に示すとおり、第一段階目の攻撃対象であるネットワークインターフェースのうち、Wi-Fi に対する攻撃アプローチを整理し、攻撃者が IVI 等と IP 層レベルで通信可能となる状態までを解説する。それ以外のネットワークインターフェースへの攻撃手法については他の実践手引き(例えば Bluetooth 編)にて別途解説する。

また、第二段階目の攻撃アプローチについても、他の実践手引き(例えば IP ネットワーク編)にて解説する。

3.1.1. Wi-Fi に対する一般的な攻撃アプローチ

前述のとおり、攻撃の目標は対象となる無線ネットワークへの接続となる。これは有線ネットワークで置き換えるならば、攻撃対象となるネットワークに接続されているスイッチの空ポートに物理的に LAN ケーブルを挿すところまでを意味している。

無線ネットワークに対する攻撃アプローチ全体像は図 3-2 のとおりである。

攻撃のフェーズは大きく分けると 2 つあり、無線 LAN ネットワーク接続前に行われる攻撃と、無線 LAN ネットワーク接続後に行われる攻撃に整理される。

無線 LAN ネットワーク接続前に行われる攻撃は、無線 LAN のプロトコルの仕組みや特徴を利用したパスワードを解析するアプローチ、無線 LAN のプロトコルや無線 LAN のハードウェアチップが有する脆弱性を利用した攻撃アプローチおよび単に無線 LAN ネットワークを利用不可能にすることを目的とした DoS 攻撃が想定される。1 つ目はプロトコルの特徴を利用しているため、パッチ等で修正できる類のものではなく、適切なプロトコルの利用やセキュリティの設定が求められ、2 つ目についてはパッチやファームウェアの更新等の対応が必要となるものである。3 つ目の DoS 攻撃については無線 LAN の仕組み上、防ぐことは困難である。

また、無線 LAN ネットワーク接続後に行われる攻撃は、流れているデータのスニフィングおよびスニフィングから得られた情報を踏まえたうえで、無線 LAN ネットワーク上で動作している IP ネットワークに対する攻撃が行われることが想定される。なお、IP ネットワーク層における攻撃手法については別の実践手引き(IP ネットワーク編)にて詳説する。

図 3-2 （公開資料のため、記載内容を削除）

3.2. 評価に必要なデバイスと評価端末の準備

3.2.1. 評価に必要なデバイス等の準備

Wi-Fi に対する情報セキュリティ評価を実施するにあたり必要となる主なデバイスは表 3-1 のとおりである。この中でも特に考慮すべきデバイスとしては、情報セキュリティ評価で利用する OS および無線 LAN クライアントデバイスが挙げられる。

表 3-1 （公開資料のため、記載内容を削除）

（公開資料のため、記載内容を削除）

3.3. 個別の攻撃手法の説明

（公開資料のため、記載内容を削除）

付録1. 使用するツールの紹介

（公開資料のため、記載内容を削除）

付録2. 一般的な評価手法

（公開資料のため、記載内容を削除）

情報セキュリティ評価ガイドライン
ドラフト（実践手引き）IPネットワーク編
【成果報告書版】

2018年2月28日発行

【本書の位置づけ】
本書は、「情報セキュリティ評価ガイドラインドラフト（実践手引き）IP ネットワーク編 ver.2.2」をもとに、成果報告書版として作成したものである

目次

1. はじめに 1

1.1. **背景と目的** 1
1.2. **適用範囲** 2
1.3. **前提事項** 3
1.4. **用語の定義** 3
1.5. **本書の構成** 4
1.6. **参考文献** 4

2. プロトコル概要 5

2.1. **プロトコルの階層モデル** 5
2.1.1. OSI **参照モデル** 5
2.1.2. TCP/IP **の階層モデル** 5
2.2. **データリンク層** 6
2.2.1. **データリンク層の概要** 6
2.3. **インターネット層** 7
2.3.1. IP **の概要** 7
2.4. **トランスポート層** 7
2.4.1. **トランスポート層の概要** 7
2.5. **アプリケーション層** 8
2.5.1. **アプリケーション層の概要** 8

3. 一般的な攻撃手法 9

3.1. **一般的な攻撃アプローチ** 9
3.1.1. IP **ネットワークに対する攻撃アプローチ** 9
3.2. **評価に必要なデバイスと評価端末の準備** 10
3.2.1. **評価に必要なデバイス等の準備** 10
3.3. **個別の攻撃手法の説明** 10

付録 1. 使用するツールの紹介 11

付録 2. 一般的な評価手法 11

1. はじめに

1.1. 背景と目的

自動車のコネクテッド化が進んでおり、ネットワークを経由して車内外の様々なデータのやり取りが可能となっている。これにより自動車の快適性および安全性が向上し、また、クラウドとつながることで様々なサービスを受けられるようになっている。その一方で、無線通信等のネットワークを経由した車外サービスの利用増により、車両外部からによる遠隔操作等のセキュリティ攻撃等のリスクが高まり、無線経由の通信に対してセキュリティを確保する必要性が高まっている。

また、今後、市場に登場するとみられる自動走行車両の場合、車両を市場へリリースした後の運用時においても、OTA（Over The Air）によるソフトウェア更新に伴う車両の仕様変更や、車外サービスの仕様変更に伴う車両への影響等の考慮が必要となることが考えられる。これらのことから無線経由の通信に対するセキュリティ確保の観点において、開発車に対するセキュリティ評価に加え、市販車に対するセキュリティ評価の必要性も高まっている。

開発車や市販車におけるセキュリティ評価においては、セキュリティ機能が要求通りに実現できているかという観点に加えて、車外からの実際の攻撃に対する耐ハッキング性能という観点がより重要となる。そこで、IT 業界で採用されているペネトレーションテストを、自動車にも適用する動きが高まっている。

ペネトレーションテストは、攻撃者視点によるセキュリティ評価であり、車両の脆弱性を利用して実際に外部から攻撃が可能かを検証する。これは他の、ツールによる脆弱性診断やファジングテスト等のセキュリティ評価とは異なる性質をもつ。ペネトレーションテストでは、攻撃者視点による評価という性質上、評価対象をブラックボックスとして扱う場合も多く、一般的に評価に用いる情報は制限されることから、情報収集に多くの労力を使う。また、実車両を必要とすることから、開発の終盤に評価が実施される場合が多く、評価期間やリソースについて制約も受ける場合もある。このように、情報や評価期間、リソース等の制約を大きく受けるペネトレーションテストに対しては、リスクアプローチにより攻撃対象を絞った上で効率よく評価を行うことが望まれる。

本ガイドラインは、情報セキュリティ評価ガイドライン（本編）に従い作成された評価計画に従い実際に評価を行うために必要となる、具体的な評価手法を検討する際に参照されることを想定したガイドラインである。そのため、情報セキュリティ評価ガイドライン（実践手引き）は要素技術毎にまとめられており、各実践手引きにおいては車両に対して一般的に実施されるペネトレーションテストの評価手法を含めている。ただし、実際の情報セキュリティ評価においては、ペネトレーションテストの目的にのっとり、本ガイドラインに記載された内容以外の評価手法についても臨機応変に組み込んでいく必要がある点には留意いただきたい。

1.2. 適用範囲

本ガイドラインは、車両が有するインターフェースのうち、Wi-Fi 等に接続した後の通信で利用される IP ネットワークを攻撃対象とした実践手引きである。具体的には、図 1-1 に示すとおり、攻撃者が車両の有する Wi-Fi 等により構成される無線 LAN ネットワークに接続後の IP ネットワークを範囲としている。

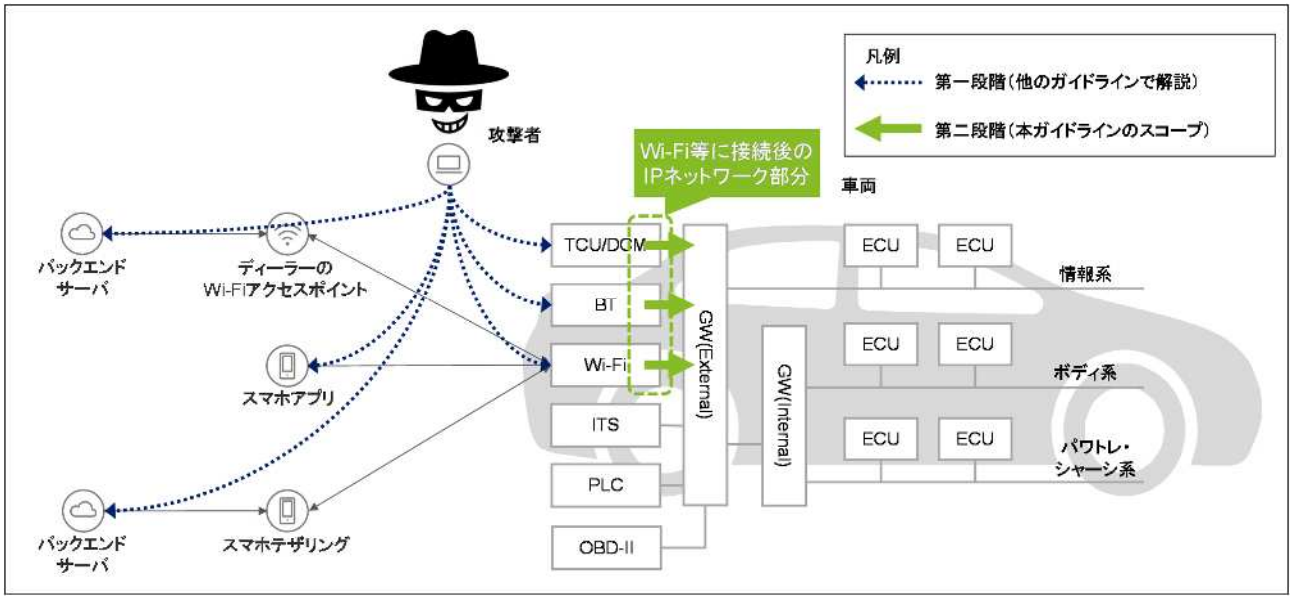


図 1-1 本ガイドラインの適用範囲

なお、バックエンドサーバー等で稼働する Web アプリケーションや、スマホアプリ等は本書の対象外であるが、以下に参考となる情報を記載する。

- 独立行政法人 情報処理推進機構（IPA）（2017年）「安全なウェブサイトの作り方」，<https://www.ipa.go.jp/security/vuln/websecurity.html> , 2018年2月19日アクセス
- 独立行政法人 情報処理推進機構（IPA）（2016年）「IPAテクニカルウォッチ「ウェブサイトにおける脆弱性検査手法（ウェブアプリケーション検査編）」」，<https://www.ipa.go.jp/security/technicalwatch/20160928-2.html> , 2018年2月19日アクセス
- 独立行政法人 情報処理推進機構（IPA）（2014年）「IPAテクニカルウォッチ「ウェブサイトにおける脆弱性検査手法の紹介（ソースコード検査編）」」，<https://www.ipa.go.jp/security/technicalwatch/20140306.html> , 2018年2月19日アクセス
- Open Web Application Security Project（OWASP）（2014 年）「OWASP Testing Guide v4」，<https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents> , 2018 年 2 月 19 日アクセス
- Open Web Application Security Project（OWASP）「OWASP Zed Attack Proxy Project」，<https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project> , 2018 年 2 月 19 日アクセス

1.3. 前提事項

本ガイドラインは、情報セキュリティ評価ガイドライン（本編）に従い作成された評価項目のうち IP ネットワークに関連した評価項目に対する具体的な評価手法を検討する際に参照されることを目的としたガイドラインとなっており、活用される場面については、情報セキュリティ評価ガイドライン（本編）でも述べているように、図 1-2 に示す V 字プロセスにおける①車両総合評価、②市販車評価、③－1 システム設計、③－2 H/W-S/W 統合評価の 4 つのフェーズでの活用を想定している。

各フェーズでのガイドライン利用にあたる前提事項の詳細については、情報セキュリティ評価ガイドライン（本編）を参照のこと。

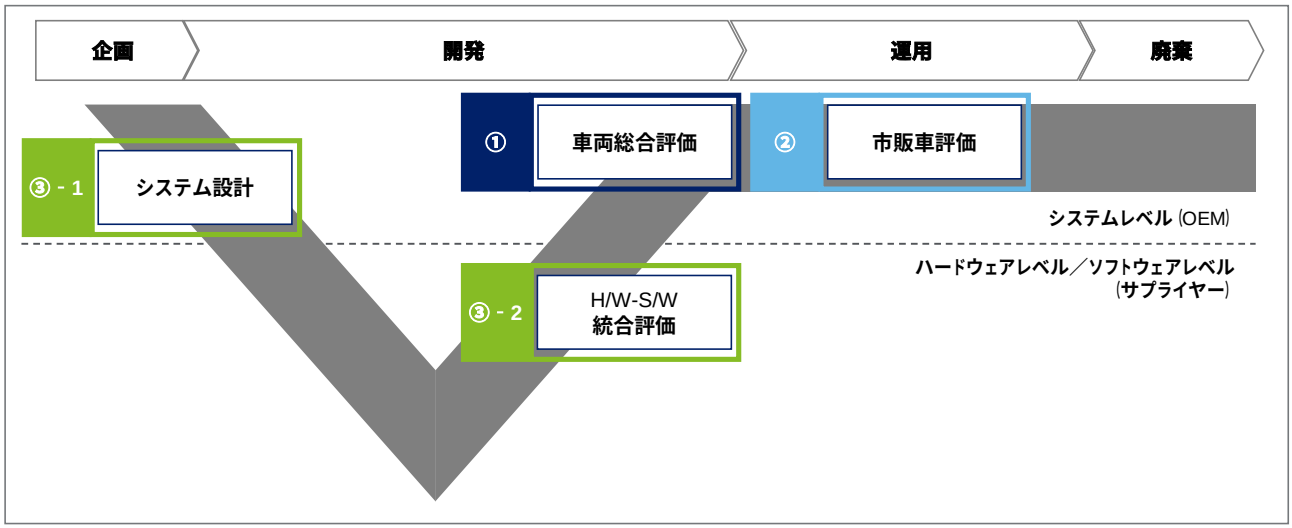


図 1-2　本ガイドラインの V 字プロセスにおける位置付け

1.4. 用語の定義

本ガイドラインで利用する用語とその定義を表 1-1 に示す。

表 1-1　（公開資料のため、記載内容を削除）

また、本ガイドラインで利用する略語の定義について表 1-2 に示す。

表 1-2　（公開資料のため、記載内容を削除）

1.5. 本書の構成

情報セキュリティ評価ガイドラインドラフト（IP ネットワーク編）は、以下の構成となっている。

第 1 章は、本書の目的、適用範囲や前提事項について述べる。

第 2 章は、IP ネットワークに関するプロトコルのうちペネトレーションテストを実施する上で必要となる内容について述べる。

第 3 章は、IP ネットワークに対する具体的な攻撃手法について記載する。

付録 1 は、IP ネットワークに対するペネトレーションテストを実施する上で必要となる代表的なツールを紹介する。

付録 2 は、IP ネットワークに対する一般的な評価手法について紹介する。

1.6. 参考文献

- 株式会社オーム社、マスタリング TCP/IP 入門編 第 5 版、竹下隆史、村山公保、荒井透、苅田幸雄[著]
- 株式会社オーム社、マスタリング TCP/IP 情報セキュリティ編、齋藤孝道[著]
- 株式会社オーム社、マスタリング TCP/IP SSL/TLS 編、Eric Rescorla[著]、齋藤孝道、鬼頭利之、古森貞[監訳]
- ソフトバンククリエイティブ株式会社、情報システムセキュリティの実践的監査手法 ペネトレーションテスト入門、古川泰弘、吉成大知[著]
- 株式会社マイナビ出版、サイバーセキュリティ完全ガイド Kali Linux によるペネトレーションテスト、Peter Kim[著]、保要隆明、前田優人、美濃圭佑、八木橋優[監訳]、株式会社クイーブ[訳]
- 株式会社オライリー・ジャパン、実践 Metasploit ―ペネトレーションテストによる脆弱性評価、David Kennedy、Jim O'Gorman、Devon Kearns、Mati Aharoni[著]、青木一史、秋山満昭、岩村誠、川古谷 裕平、川島 祐樹、辻 伸弘、宮本久二男[監訳]、岡真由美[訳]
- 株式会社リックテレコム、パケットキャプチャ入門 第 3 版 LAN アナライザ Wireshark 活用術、竹下恵 [著]

2. プロトコル概要

2.1. プロトコルの階層モデル

2.1.1. OSI 参照モデル

ネットワークプロトコルについて議論する際によく引き合いに出されるのが OSI 参照モデルである。国際標準化機構（ISO）により策定された当モデルは、コンピューター等の機器が持つべき通信機能を 7 つの階層構造に分け、機能を分割することで、複雑になりがちなネットワークプロトコルを単純化している。

OSI 参照モデルにおける各層の役割を図 2-1 に示す。

第7層	アプリケーション層	・ 個別のアプリケーションのプロトコルを規定
第6層	プレゼンテーション層	・ データ表現形式（フォーマット）の変換
第5層	セッション層	・ 通信の開始から終了までの通信の管理 （コネクション（論理的な通信路）の確立／切断等）
第4層	トランスポート層	・ ネットワークの両端のノード（*）におけるデータ転送管理 （エラー訂正、再送制御等）
第3層	ネットワーク層	・ アドレスの管理 ・ ネットワークの経路選択（ルーティング）
第2層	データリンク層	・ 物理層で直接接続された機器間の信号の受け渡し
第1層	物理層	・ コネクタのピン数、形状やケーブル等の規定 ・ ビット列（0と1）と電気信号等の変換

＊ノードとはネットワーク接続されているコンピューター等の機器を指す

図 2-1 OSI 参照モデル

なお、ネットワークに接続されたコンピューター等の機器は、OSI 参照モデルではノードと呼ばれる一方で、TCP/IP においてはホストと呼ばれる。

2.1.2. TCP/IP の階層モデル

TCP/IP は、ネットワークにおいて最も標準的に利用されているプロトコルの一つであり、インターネット関連技術の標準化団体である IETF（Internet Engineering Task Force）が規定している。これらは RFC（Request for Comments）と呼ばれる公式文書としてまとめられ、インターネット上で公開されている。

TCP/IP のデータ通信モデルは、階層の一式と見なすことができ、4 つの階層で構成される。図 2-2 に TCP/IP の階層モデルと、各階層における代表的なプロトコルを示す。

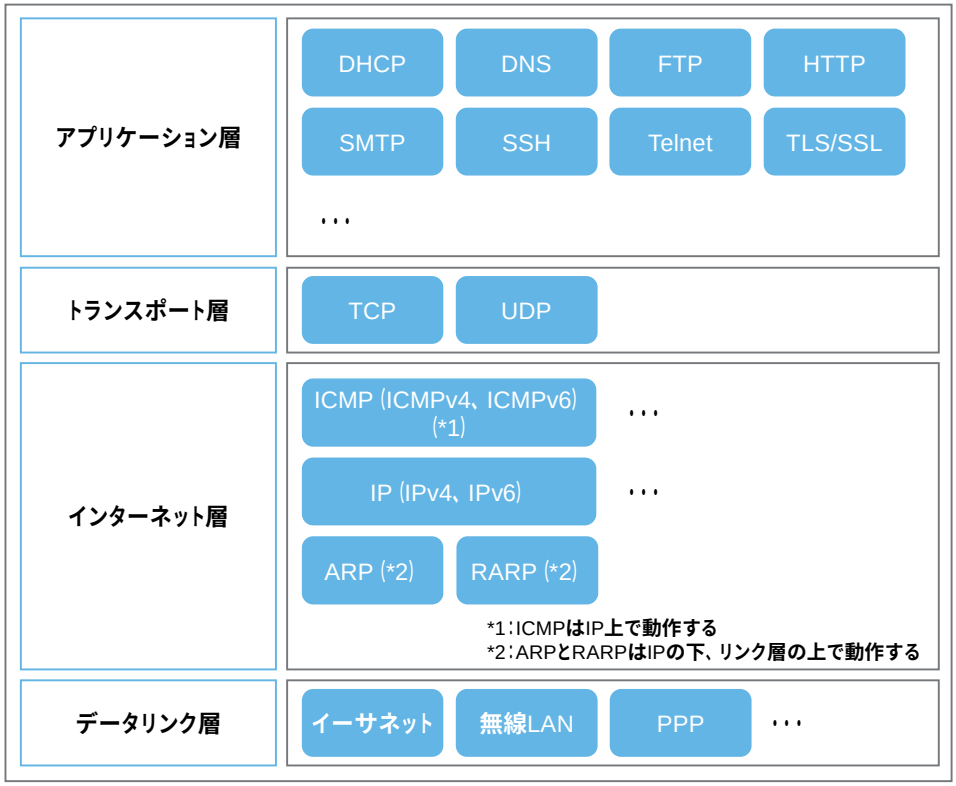


図 2-2　TCP/IP の階層モデルと代表的なプロトコル

（公開資料のため、記載内容を削除）

2.2. データリンク層

2.2.1. データリンク層の概要

データリンク層のプロトコルでは、直接通信媒体で接続された機器間で通信を行うための仕様を規定している。通信媒体としては、ツイストペアケーブル（より対線）、同軸ケーブル、光ファイバー、無線等がある。また、機器間をスイッチ、ブリッジやリピーター等の機器で中継する場合もある。

実際に機器間で通信を行うには、物理層とデータリンク層が必要となる。

2 進数の「0」と「1」で表現されるコンピューターの情報は、通信媒体でやりとりされる際には、電気信号等に変換されることになるが、物理層が 2 進数の「0」および「1」と、電気信号等との変換を担う。

一方、データリンク層は、単なる 2 進数の「0」と「1」の列としてではなく、「フレーム」という単位にまとめて送信先の機器に伝える役割を担う。

本節では、データリンク層に関連する技術である MAC（Media Access Control）アドレスや、具体的な通信手段であるイーサネット等について説明する。

（公開資料のため、記載内容を削除）

2.3. インターネット層

2.3.1. IP の概要

インターネット層は TCP/IP の核とも言え、主として、IP（Internet Protocol）と、ICMP（Internet Control Message Protocol）の 2 つのプロトコルで構成される。本節では、まず IP について説明した後に、IP に関連するプロトコルについて説明する。

IP は OSI 参照モデルにおける第 3 層であるネットワーク層に位置付けられる。ネットワーク層は終点ノード間（エンド・ツー・エンド（起点から終点まで））のパケット配送に対する責任を持つ。ネットワーク層の下位の階層であるデータリンク層は、同一のデータリンクで接続されているノード間のパケット配送を行うため、データリンクを超えた通信を行うためにはネットワーク層が必要となる。ネットワーク層は、通信経路上、異なるデータリンクであったとしても、その間の連携を取りながらパケットを配送することで別のデータリンクに接続されているノードとの通信を可能とする。

IP の役割は大きく 3 つあり、IP アドレス、終点ホストまでのパケット配送（ルーティング）、IP パケットの分割と再構築処理である。

（公開資料のため、記載内容を削除）

2.4. トランスポート層

2.4.1. トランスポート層の概要

「2.3 インターネット層」で説明したとおり、IP ヘッダーのプロトコルフィールドでは、上位の階層のどのプロトコルにデータを渡すかが番号で示されている。この番号により、IP が運んでいるデータが TCP（Transmission Control Protocol）なのか UDP（User Datagram Protocol）なのかを識別する。同様にトランスポート層の代表的なプロトコルである TCP や UDP においても、次にどのプログラムにデータを渡せば良いかを識別するための番号が定義されている。この番号はポート番号と呼ばれ、トランスポート層の上位の階層であるアプリケーション層の処理を行うプログラムを識別する。

TCP と UDP は目的によって使い分けられ、TCP は信頼性のある通信を提供するために「順序制御」や「再送制御」を行う。また、「フロー制御（流量制御）」や「輻輳制御」といったネットワークの利用効率を向上させる機能等を備えている。一方で、UDP は、パケットが宛先のホストまで到達する保証はされていないため、必要に応じてプログラムが再送処理を行わなければならず、高速性やリアルタイム性を重視する通信や同報通信等に使用される。

（公開資料のため、記載内容を削除）

2.5. アプリケーション層

2.5.1. アプリケーション層の概要

ネットワークを利用するアプリケーションには、ブラウザ、電子メールソフト、ファイル転送ツール等があり、アプリケーションそれぞれの通信処理が必要となる。それぞれのアプリケーションの通信処理を行うのがアプリケーションプロトコルである。IP、TCP や UDP 等の下位の階層のプロトコルは、アプリケーションによらず使用できるように設計された汎用性の高いプロトコルであるのに対し、アプリケーションプロトコルは、個々のアプリケーションの実行を実現するために作られたプロトコルである。

（公開資料のため、記載内容を削除）

3. 一般的な攻撃手法

3.1. 一般的な攻撃アプローチ

攻撃者が車両に対して攻撃を仕掛けようとした場合、最も魅力的に映る機能の一つが、車両とバックエンドサーバー、モバイルアプリ等を結ぶネットワークである。車両が有するネットワークインターフェースは TCU（Telematics Communication Unit）を始め、Wi-Fi や Bluetooth 等多岐にわたり、攻撃者はこれらが接続されたネットワークを介し、IVI（In-Vehicle Infotainment）への侵入を最初の目標とし、続いてそれらが通信を行うであろうバックエンドサーバーやモバイルアプリ等を次なる目標とすることが想定される。

IVI 等への攻撃のアプローチは大きく二段階に分けることができる。第一段階目は、各種ネットワークに対して攻撃を実施し、IVI 等が属するネットワークへ接続することで IVI 等と通信できるようになることを目標とした攻撃である。第二段階目は、IVI 等への攻撃を試みることが目標であり、IT 業界でもよく利用される攻撃手法が利用される。

本ガイドラインでは、図 1-1 に示すとおり、第二段階目の攻撃アプローチを解説する。

なお、第一段階目の攻撃対象であるネットワークインターフェースのうち、Wi-Fi 等に対する攻撃アプローチについては、他の実践手引き（例えば Wi-Fi 編等それぞれのプロトコルに応じた編）にて別途解説している。

3.1.1. IP ネットワークに対する攻撃アプローチ

第一段階目の攻撃が成功すると、第二段階目の攻撃として、IP ネットワークを介した IVI 等への攻撃を試みることになる。IP ネットワークに接続した後の攻撃アプローチは大きく分けると 4 つある。

1 つ目のステップは、第一段階目の攻撃が成功し、ネットワークに接続した後、当該ネットワークに接続している他の攻撃対象の IP アドレスを特定するステップである。

2 つ目のステップは、1 つ目のステップで特定した IP アドレス上で稼働するサービスや OS を特定するステップである。

3 つ目のステップは、2 つ目のステップで特定したサービスや OS 等に、脆弱性につながるような潜在的な設定ミスやソフトウェアのバージョンが古いこと等による脆弱性の有無を識別するステップである。

4 つ目のステップは、識別した脆弱性を利用して攻撃対象の乗っ取りや侵入を試みるステップである。

（公開資料のため、記載内容を削除）

3.2. 評価に必要なデバイスと評価端末の準備

3.2.1. 評価に必要なデバイス等の準備

IP ネットワークに対する情報セキュリティ評価を実施するにあたり必要となる主なデバイスは表 3-1 のとおりである。

表 3-1 （公開資料のため、記載内容を削除）

（公開資料のため、記載内容を削除）

3.3. 個別の攻撃手法の説明

（公開資料のため、記載内容を削除）

付録1. 使用するツールの紹介

（公開資料のため、記載内容を削除）

付録2. 一般的な評価手法

（公開資料のため、記載内容を削除）

情報セキュリティ評価ガイドライン
ドラフト（実践手引き）Bluetooth編
【成果報告書版】

2018年2月28日発行

【本書の位置づけ】
本書は、「情報セキュリティ評価ガイドラインドラフト（実践手引き）Bluetooth 編 ver.2.2」をもとに、成果報告書版として作成したものである

目次

1. はじめに 1

1.1. **背景と目的** 1
1.2. **適用範囲** 2
1.3. **前提事項** 3
1.4. **用語の定義** 3
1.5. **本書の構成** 4
1.6. **参考文献** 4

2. プロトコル概要 5

2.1. Bluetooth **概要** 5

3. 一般的な攻撃手法 7

3.1. **一般的な攻撃アプローチ** 7
3.1.1. Bluetooth **に対する一般的な攻撃アプローチ** 7
3.2. **評価に必要なデバイスと評価端末の準備** 8
3.2.1. **評価に必要なデバイス等の準備** 8
3.3. **個別の攻撃手法の説明** 8

付録 1. 使用するツールの紹介 9

付録 2. 一般的な評価手法 9

1. はじめに

1.1. 背景と目的

自動車のコネクテッド化が進んでおり、ネットワークを経由して車内外の様々なデータのやり取りが可能となっている。これにより自動車の快適性および安全性が向上し、また、クラウドとつながることで様々なサービスを受けられるようになっている。その一方で、無線通信等のネットワークを経由した車外サービスの利用増により、車両外部からによる遠隔操作等のセキュリティ攻撃等のリスクが高まり、無線経由の通信に対してセキュリティを確保する必要性が高まっている。

また、今後、市場に登場するとみられる自動走行車両の場合、車両を市場へリリースした後の運用時においても、OTA（Over The Air）によるソフトウェア更新に伴う車両の仕様変更や、車外サービスの仕様変更に伴う車両への影響等の考慮が必要となることが考えられる。これらのことから無線経由の通信に対するセキュリティ確保の観点において、開発車に対するセキュリティ評価に加え、市販車に対するセキュリティ評価の必要性も高まっている。

開発車や市販車におけるセキュリティ評価においては、セキュリティ機能が要求通りに実現できているかという観点に加えて、車外からの実際の攻撃に対する耐ハッキング性能という観点がより重要となる。そこで、IT 業界で採用されているペネトレーションテストを、自動車にも適用する動きが高まっている。

ペネトレーションテストは、攻撃者視点によるセキュリティ評価であり、車両の脆弱性を利用して実際に外部から攻撃が可能かを検証する。これは他の、ツールによる脆弱性診断やファジングテスト等のセキュリティ評価とは異なる性質をもつ。ペネトレーションテストでは、攻撃者視点による評価という性質上、評価対象をブラックボックスとして扱う場合も多く、一般的に評価に用いる情報は制限されることから、情報収集に多くの労力を使う。また、実車両を必要とすることから、開発の終盤に評価が実施される場合が多く、評価期間やリソースについて制約も受ける場合もある。このように、情報や評価期間、リソース等の制約を大きく受けるペネトレーションテストに対しては、リスクアプローチにより攻撃対象を絞った上で効率よく評価を行うことが望まれる。

本ガイドラインは、情報セキュリティ評価ガイドライン（本編）に従い作成された評価計画に従い実際に評価を行うために必要となる、具体的な評価手法を検討する際に参照されることを想定したガイドラインである。そのため、情報セキュリティ評価ガイドライン（実践手引き）は要素技術毎にまとめられており、各実践手引きにおいては車両に対して一般的に実施されるペネトレーションテストの評価手法を含めている。ただし、実際の情報セキュリティ評価においては、ペネトレーションテストの目的にのっとり、本ガイドラインに記載された内容以外の評価手法についても臨機応変に組み込んでいく必要がある点には留意いただきたい。

1.2. 適用範囲

本ガイドラインでは、車両が有するインターフェースのうち、Bluetooth を攻撃対象とした実践手引きを対象としている。図 1-1 に示すとおり、Bluetooth では様々なサービスが提供されている。攻撃者による攻撃の第一段階は、まず Bluetooth によって提供されるサービスを理解し、提供されるサービスを利用した攻撃が想定される。そのため、IVI（In-Vehicle Infotainment）によって提供される Bluetooth 上のサービスの理解、Bluetooth 上で提供されるサービスを利用した攻撃に関する情報セキュリティ評価手法についてを本ガイドラインの適用範囲とする。

一方、Bluetooth 上で提供されるサービスによっては、IVI と IP を利用した通信が可能となる場合がある。このようなサービスが提供されている場合、攻撃者は Bluetooth 経由で IP ネットワークへ接続後、IP ネットワークに対する一般的な攻撃手法を利用して攻撃をすることが想定される。この攻撃については第二段階の攻撃として想定しており、別の実践手引きにて説明する。

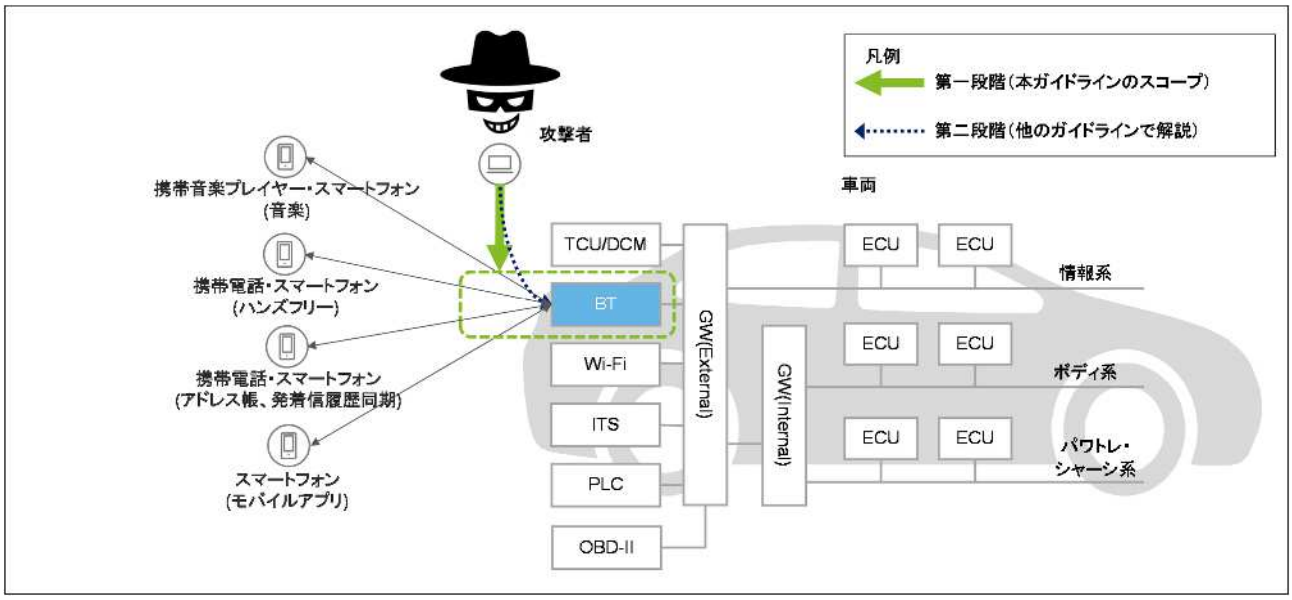


図 1-1 本ガイドラインの適用範囲

1.3. 前提事項

本ガイドラインは、情報セキュリティ評価ガイドライン（本編）に従い作成された評価項目のうち Bluetooth に関連した評価項目に対する具体的な評価手法を検討する際に参照されることを目的としたガイドラインとなっており、活用される場面については、情報セキュリティ評価ガイドライン（本編）でも述べているように、図 1-2 に示す V 字プロセスにおける①車両総合評価、②市販車評価、③－1 システム設計、③－2 H/W-S/W 統合評価の 4 つのフェーズでの活用を想定している。

各フェーズでのガイドライン利用にあたる前提事項の詳細については、情報セキュリティ評価ガイドライン（本編）を参照のこと。

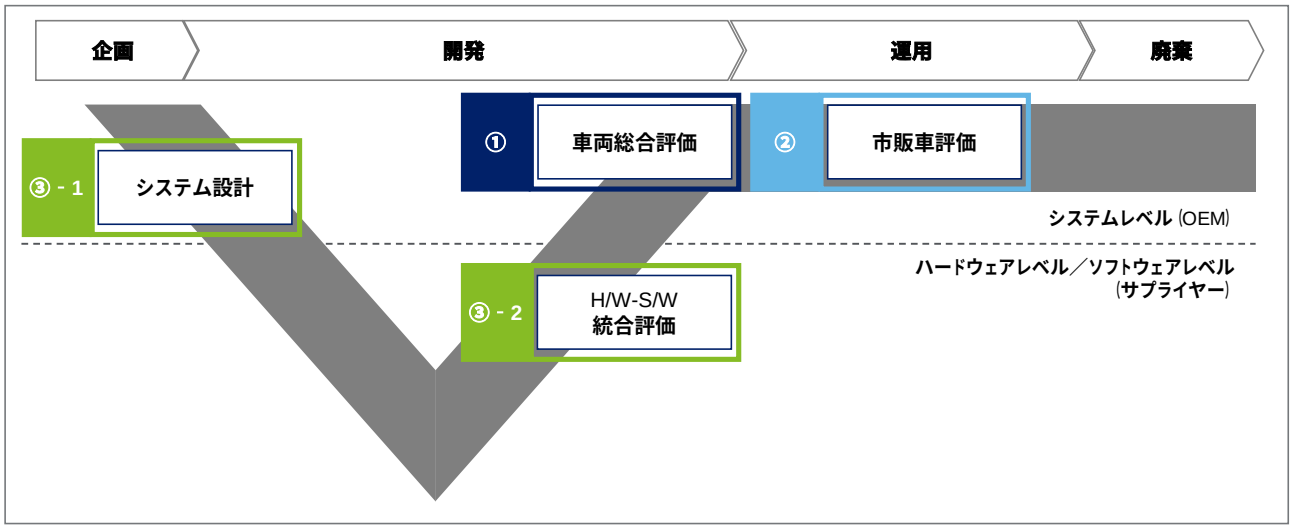


図 1-2　本ガイドラインの V 字プロセスにおける位置付け

1.4. 用語の定義

本ガイドラインで利用する用語とその定義を表 1-1 に示す。

表 1-1　（公開資料のため、記載内容を削除）

また、本ガイドラインで利用する略語の定義について表 1-2 に示す。

表 1-2　（公開資料のため、記載内容を削除）

1.5. 本書の構成

情報セキュリティ評価ガイドラインドラフト（Bluetooth 編）は、以下の構成となっている。

第 1 章は、本書の目的、適用範囲や前提事項について述べる。

第 2 章は、Bluetooth に関するプロトコルのうちペネトレーションテストを実施する上で必要となる内容について述べる。

第 3 章は、Bluetooth に対する具体的な攻撃手法について記載する。

付録 1 は、Bluetooth に対するペネトレーションテストを実施する上で必要となる代表的なツールを紹介する。

付録 2 は、Bluetooth に対する一般的な評価手法について紹介する。

1.6. 参考文献

- 日刊工業新聞社、Bluetooth ガイドブック―ワイヤレス通信の新技術、宮津 和弘[著]
- ピアソンエデュケーション、Bluetooth テクノロジーへの招待―使用開発者による近距離無線通信技術の手引き、ブレント・ミラー[著]、チャトシック・ビスディキアン[著]、清野 幹雄[監訳]
- リックテレコム、Bluetooth 技術解説ガイド(テクノロジー解体新書)、宮津 和弘[著]、日本エリクソン[監修]
- オライリー・ジャパン、Bluetooth Low Energy をはじめよう、Kevin Townsend[著]、Carles Cufi[著]、Akiba[著]、Robert Davidson[著]、水原 文[訳]
- Mc Graw Hill、Hacking Exposed Wireless-Third Edition: Wireless Security Secrets & Soutions、Joshua Wright[著]、Johnny Cache[著]
- National Institution of Standards and Technology、Draft NIST Special Publication 800-121 Revision 2 Guide to Bluetooth Security、John Padgetee[著]、John Bahr[著]、Mayank Batra[著]、Marcel Holtmann[著]、Rhonda Smithbey[著]、Lily Chen[著]、Karen Scarfone[著]

2. プロトコル概要

2.1. Bluetooth 概要

Bluetooth とは、「小型」「軽量」「低消費電力」を主眼においた、数 m～数十 m 程度の近距離間通信をターゲットとした 2.4GHz 帯の周波数を利用した通信を行う通信プロトコルである。1999 年 1 月に Bluetooth 1.0 として規格化され、2002 年 3 月には Bluetooth 1.1 が IEEE 802.15.1 として規格化された。それ以降も進化を続け、現在は Bluetooth 5.0 までリリースされている。

現在 Bluetooth には BR(Basic Rate)/EDR(Enhanced Data Rate)と LE(Low Energy)という 2 つの異なる規格が存在しており、BR/EDR と LE については物理層レベルで異なるプロトコルとして定義されているため、この 2 つの間に互換性はない。なお、Bluetooth BR/EDR については Bluetooth Classic とも呼ばれている。

表 2-1 Bluetooth のバージョンと機能の遷移

バージョン	リリース時期	概要
1.0b	1999 年 7 月	最初のバージョン
1.1	2002 年 3 月	普及バージョン
1.2	2003 年 11 月	無線 LAN(IEEE 802.11b/g)との干渉対策が盛り込まれた
2.0	2004 年 11 月	最大通信速度が 3Mbps となる Enhanced Data Rate (EDR)がオプションで利用可能となった
2.1	2007 年 3 月	ペアリングが簡略化された
3.0	2009 年 4 月	無線 LAN 規格 802.11 の MAC/PHY 層が利用可能となり、最大通信速度が 24Mbps となる High Speed(HS)がオプションとして利用可能となった
4.0	2009 年 12 月	Bluetooth LE を追加
4.1	2013 年 12 月	モバイル端末向け通信サービスとの電波干渉を抑える技術、データ転送の効率化、自動の再接続機能等々の機能追加
4.2	2014 年 12 月	Bluetooth LE の通信速度が Data Packet Length Extension の導入により 260Kbps から 650Kbps に高速化。また、IPv6/6LoWPAN でインターネット接続が可能となった
5.0	2016 年 6 月	Bluetooth LE のデータレートが 2Mbps、1Mbps、125Kbps となり 125Kbps 通信についてはその通信距離が 400m となった

Bluetooth BR/EDR は、P2P(Point to Point)ネットワークトポロジーによる継続的な無線接続を実現することを目的としており、主に無線スピーカーやハンズフリーシステムなどに利用されることが多い。

一方、Bluetooth LE は、P2P 接続以外に 1 対多のブロードキャスト接続や多対多のメッシュ構成による通信接続も視野に入れており、低電力を生かしたビーコンソリューションやセンサーネットワークなどに利用されることが多い。

最新の Bluetooth のコントローラーでは上記の 2 つのプロトコルを利用することができるようデュアルスタックのチップセットが利用されているケースがほとんどである。表 2-2 に示すとおり、各製品がどの規格をサポートしているかについては、外観的にはその製品に付与された Bluetooth ロゴから確認

することができる。

表 2-2 Bluetooth のロゴの表記とサポートしている規格

ロゴの表記	サポートしている規格
Bluetooth	Bluetooth BR/EDR
Bluetooth Smart	Bluetooth LE
Bluetooth Smart Ready	Bluetooth BR/EDR と Bluetooth LE のデュアルスタック

Bluetooth BR/EDR と Bluetooth LE に関する主な特徴は以下のとおりである。

表 2-3 Bluetooth BR/EDR 及び LE の主な特徴

<table>
<tr><th rowspan="2">特徴</th><th colspan="2">Bluetooth BR/EDR</th><th colspan="2">Bluetooth LE</th></tr>
<tr><th>4.1 より前</th><th>4.1 以降</th><th>4.2 より前</th><th>4.2 以降</th></tr>
<tr><td>無線チャネル数</td><td colspan="2">全 79 チャネル、チャネルあたり 1MHz</td><td colspan="2">全 40 チャネル、チャネルあたり 2MHz</td></tr>
<tr><td>検索/接続</td><td colspan="2">問い合わせ (Inquery) /
ペアリング(Pairing)</td><td colspan="2">アドバタイジング(Advertising)</td></tr>
<tr><td>ピコネット内の
スレーブ数</td><td colspan="2">最大 7(アクティブ)/255(トータル)</td><td colspan="2">制限なし</td></tr>
<tr><td>H/W アドレスの
プライバシー保護</td><td colspan="2">機能なし</td><td colspan="2">プライベートアドレス機能あり</td></tr>
<tr><td>最大転送速度</td><td colspan="2">1～3Mbps</td><td colspan="2">1Mbps (GFSK 変調方式利用時)</td></tr>
<tr><td rowspan="2">ペアリング
アルゴリズム</td><td>2.1 より前
E21/E22/SAFER+</td><td rowspan="2">P-256 楕円曲線暗号化方式 / HMAC-SHA-256</td><td>AES-128</td><td rowspan="2">P-256 楕円曲線暗号化方式 / AES-CMAC</td></tr>
<tr><td>2.1-4.0
P-192 楕円曲線暗号化方式/
HMAC-SHA-256</td><td></td></tr>
<tr><td>デバイス認証
アルゴリズム</td><td>E1/SAFER</td><td>HMAC-SHA-256</td><td colspan="2">AES-CCM</td></tr>
<tr><td>暗号化
アルゴリズム</td><td>E0/SAFER+</td><td>AES-CCM</td><td colspan="2">AES-CCM</td></tr>
<tr><td>標準通信距離</td><td colspan="2">30m</td><td colspan="2">50m</td></tr>
<tr><td>最大出力</td><td colspan="2">100mW (20dBm)</td><td colspan="2">10mW (10dBm)</td></tr>
</table>

（公開資料のため、記載内容を削除）

3. 一般的な攻撃手法

3.1. 一般的な攻撃アプローチ

3.1.1. Bluetooth に対する一般的な攻撃アプローチ

IVI における Bluetooth 機能の搭載は増加傾向にあり、攻撃者によって魅力的に映る機能の一つとなっている。Bluetooth 機能によって提供されるサービスは様々であり、音楽の再生やハンズフリーでの電話利用、スマートフォン等に保存されているアドレス帳等の同期、また、モバイルアプリケーション等との接続によるサービスの利用等が想定される。

そのため、図 3-1 に示すとおり、攻撃の第一段階として想定されるアクションとして、まずは攻撃者による IVI の Bluetooth インターフェースに関する情報収集とその Bluetooth によって提供されるサービスの理解、また提供されているサービスの特徴を利用した攻撃が行われるものと考えられる。更に、Bluetooth によって IVI と IP ネットワークによる通信が提供されていた場合は、攻撃の第二段階として IP ネットワーク上で利用される攻撃手法を通して IVI への攻撃が行われる可能性がある。また、識別された Bluetooth 上で提供されるサービスの実装上の脆弱性を利用したエクスプロイトの開発が行われ、攻撃に利用されることが想定される。

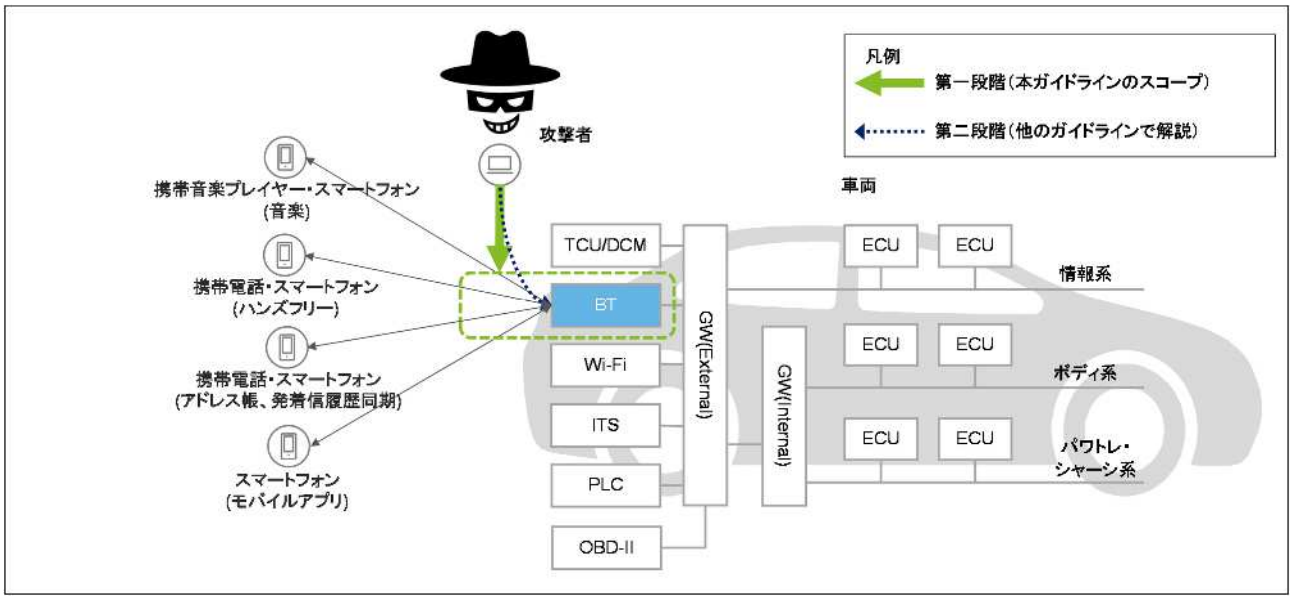


図 3-1 攻撃者による Bluetooth に対する攻撃アプローチ

本ガイドラインでは攻撃の第一段階の部分にフォーカスした攻撃アプローチを整理し、情報セキュリティ評価手法として解説する。

第二段階目の攻撃アプローチについては、他の実践手引き(例えば IP ネットワーク編)にて解説する。

3.2. 評価に必要なデバイスと評価端末の準備

3.2.1. 評価に必要なデバイス等の準備

Bluetooth に対する情報セキュリティ評価を実施するにあたり必要となる主なデバイスは表 3-1 のとおりである。

表 3-1 （公開資料のため、記載内容を削除）

（公開資料のため、記載内容を削除）

3.3. 個別の攻撃手法の説明

（公開資料のため、記載内容を削除）

付録1. 使用するツールの紹介

（公開資料のため、記載内容を削除）

付録2. 一般的な評価手法

（公開資料のため、記載内容を削除）

情報セキュリティ評価
試行調査報告書
【成果報告書版】

2018年2月28日発行

目次

1. 全体要約 2

1.1. 評価の目的 2
1.2. 評価対象 2
1.2.1. 評価対象システムおよびコンポーネント 2
1.2.2. 評価対象インターフェース 3
1.3. 評価の実施 4
1.3.1. 評価実施概要 4
1.3.2. 評価項目概要 4
1.4. 発見事項に対するリスク評価 5
1.5. 主な発見事項 5
1.6. 総括 5

2. 評価詳細説明 6

2.1. 評価条件 6
2.1.1. 評価環境 6
2.1.2. 前提情報 6
2.2. 評価体制 6
2.3. 評価方法 7
2.3.1. 事前調整 8
2.3.2. 想定される攻撃者の整理 8
2.3.3. 攻撃対象コンポーネントの特定 8
2.3.4. 車両個別のリスク分析 9
2.3.5. 評価計画の立案 13

3. 評価結果 16

3.1. ペネトレーションテストによって発見された脆弱性に対するリスク評価（リスクマッピング） 16
3.1.1. コンポーネントレベルリスク評価 16
3.1.2. 車両レベルリスク評価 16
3.1.3. フリートレベルリスク評価 16
3.1.4. トータルリスク評価 17
3.2. 個別発見事項 17
3.3. 個別評価結果 17
3.4. 情報セキュリティ評価ガイドラインドラフトの妥当性 17

別紙 A. ハードウェアハッキングとリバースエンジニアリング 18

別紙 B. 個別評価結果詳細 18

1. 全体要約

1.1. 評価の目的

本評価は、国立研究開発法人新エネルギー・産業技術総合開発機構（以下「NEDO」という。）が実施する、「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」プロジェクトの一環として行われたものである。本評価の目的は、大きく以下の 2 つとする。

（1）情報セキュリティ評価ガイドラインドラフトの妥当性検証

本プロジェクトで作成した情報セキュリティ評価ガイドラインドラフト（以下「ガイドラインドラフト」）を用いて、実際の車両を構成するシステムに対して評価を行い、ガイドラインドラフトの妥当性の検証を行うとともに、必要に応じてガイドラインドラフトの修正を行う。

（2）評価対象システムにおける脆弱性評価

（1）の評価によって、評価対象システムを構成するコンポーネントにおける脆弱性の有無を確認する。更に、発見された脆弱性に対するリスク評価を行い、その改善策を提案する。

1.2. 評価対象

1.2.1. 評価対象システムおよびコンポーネント

評価対象システムは、インフォテイメントシステムである。

本評価においては、有限な評価リソース（ヒト、モノ、カネ、時間）を有効に活用するために、リスクベースアプローチを採用している。まず、想定される攻撃者を整理した上で、攻撃者が興味を示す機能を洗い出し、更にそれら機能と関連するコンポーネントを紐づけることで、コンポーネント一覧から攻撃者が興味を示す（攻撃対象となる）コンポーネントを特定した。

次に、攻撃者が興味を示すコンポーネントに対してリスク分析を行い、リスクの発生可能性や影響度からコンポーネントリスクを見積った。

今回の評価では、発生可能性と影響度の組合せが（低、低）、（低、中）、（中、低）となるコンポーネントはコンポーネントリスクが低いと判断し評価対象外とした。そして、それ以外のリスクにマッピングされたコンポーネントを評価対象とした。

1.2.2. 評価対象インターフェース

本プロジェクトで作成したガイドラインドラフトは、図 1.1 に示すように無線通信経由での車外から車両の車外ゲートウェイ（GW）までの攻撃を想定したセキュリティ評価を対象としたガイドラインとなっている。この点を踏まえて評価対象のコンポーネントにおける無線経由でのインターフェースを調査した。その結果、Wi-Fi、Bluetooth、LTE の 3 つのインターフェースが搭載されていることが明らかとなった。

また、上記に加え、評価対象のコンポーネントのうち、アクセス容易性が高い USB ジャックについては、USB のネットワークデバイスを挿入すれば無線アクセスが可能となることもあるので、本評価においては USB についても評価対象インターフェースの 1 つと解釈することとした。

本評価では、Wi-Fi、Bluetooth、LTE、USB の 4 つのインターフェースをアタックサーフェスとした攻撃を対象としてペネトレーションテストを実施した。

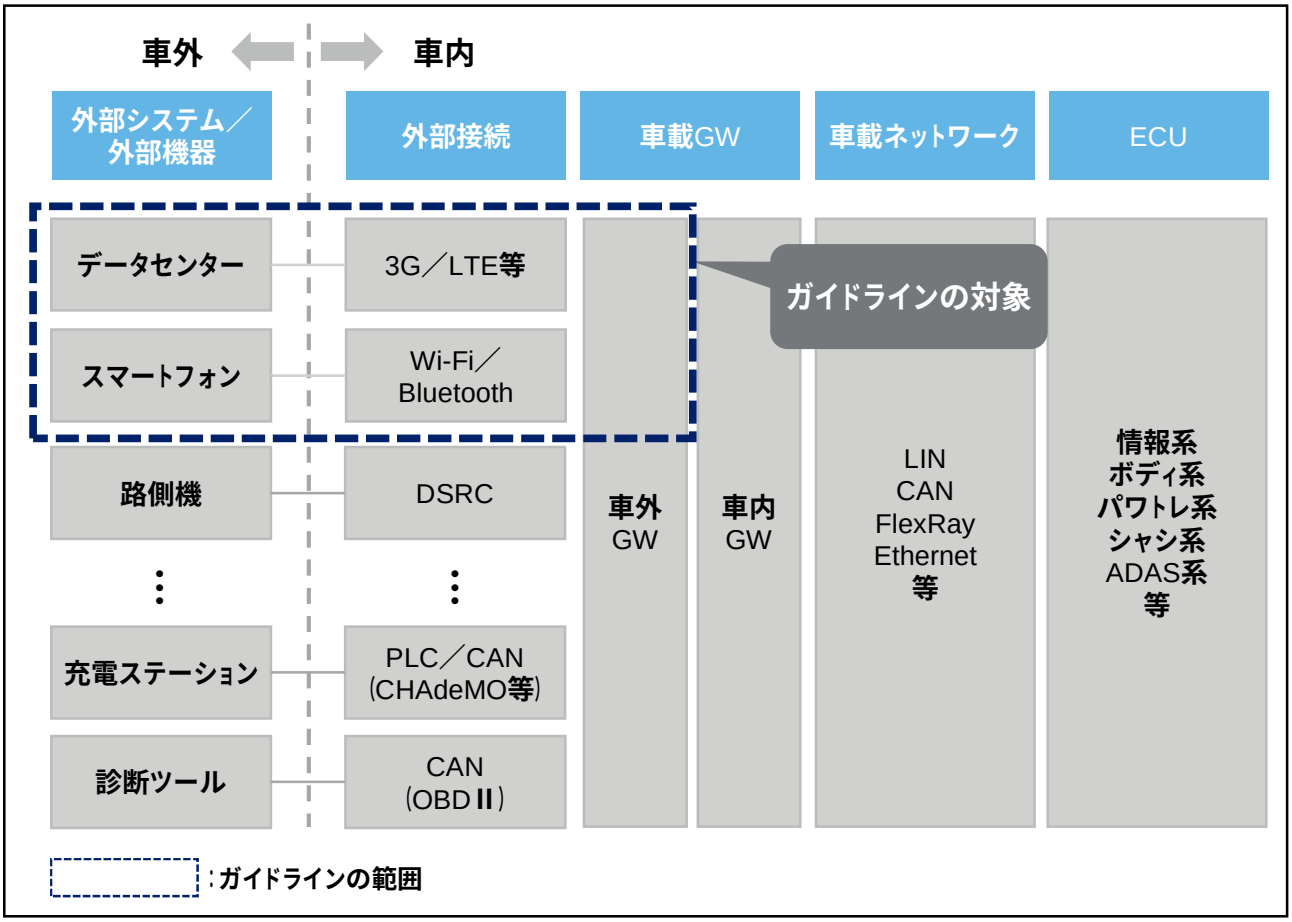


図 1.1 ガイドラインドラフトの適用範囲

1.3. 評価の実施

1.3.1. 評価実施概要

本評価は、デロイトトーマツリスクサービス株式会社が NEDO より受託した、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」の一環として実施した。表 1-1 に、評価実施概要を示す。

表 1-1 評価実施概要

項目	内容
評価期間	• テスト実施前の評価プロセス：2017 年 10 月 1 日～2018 年 1 月 19 日 ➢ 事前調整 ➢ 想定される攻撃者の整理 ➢ 攻撃対象コンポーネントの特定 ➢ 車両個別のリスク分析 ➢ 評価計画の立案 • テスト実施：2017 年 12 月 18 日～2018 年 2 月 16 日 ➢ ペネトレーションテストの実施（Wi-Fi、Bluetooth、LTE、USB） • テスト実施後の評価プロセス：2018 年 1 月 15 日～2018 年 2 月 16 日 ➢ リスクマッピング ➢ 改善策および残存リスクの整理 • 報告：2018 年 2 月 1 日～2018 年 2 月 16 日 ➢ 試行調査報告書の作成

1.3.2. 評価項目概要

評価システムにおける Wi-Fi、Bluetooth、LTE、USB に対するペネトレーションテストの評価項目作成にあたり、以下 3 つの情報を参照している。

（1） ガイドラインドラフト（本編）の「付録 2 一般的な評価項目一覧」
（2） 随時公表される脆弱性情報
（3） 技術的分析結果

ガイドラインドラフト（本編）の「付録 2 一般的な評価項目一覧」において、Web アプリケーションに係る評価項目を除いた上で、ガイドラインドラフト（実践手引き）の IP ネットワーク編、Wi-Fi 編、Bluetooth 編と紐づく評価項目を抽出した。この評価項目を基にして、随時公表される脆弱性情報や技術的分析結果の情報も活用し評価項目の検討を行った。

随時公表される脆弱性情報としては、Wi-Fi の WPA2 に対する深刻な脆弱性である KRACK（Key Reinstallation Attacks）や、Bluetooth の実装における脆弱性である BlueBorne を考慮している。また、技術的分析結果として、ストレージデバイスに対するハードウェアハッキングおよびリバースエンジニアリングにより収集したシステム情報を評価項目検討に活用している。

1.4. 発見事項に対するリスク評価

本評価で発見された脆弱性に対しては、各々にリスク評価を行った。リスク評価には CVSS（Common Vulnerability Scoring System）の基本評価基準（Base Metrics）に基づいた評価基準を用いており、自動車に固有な要件を考慮し、以下の 4 つのレイヤーでリスク評価手法を定義している。

① CVSS v3.0 の標準的なメトリクスを用いたコンポーネントレベルリスク評価
- 対象となるコンポーネント単体でのリスクを評価

② CVSS v3.0 の標準的なメトリクスを用いた車両レベルリスク評価
- コンポーネント同士が接続されることにより構成された車両単体におけるリスクを評価

③ 低、中、高、緊急の 4 つの定性的な基準を用いたフリートレベルリスク評価
- 1 つの脆弱性が一台の車両のみならず、複数の車両に影響を与える場合を考慮したリスクを評価

④ 上記①～③の加重平均によるトータルリスク

1.5. 主な発見事項

（省略）

1.6. 総括

（1）情報セキュリティ評価ガイドラインドラフトの妥当性検証

（省略）

（2）評価対象システムにおける脆弱性評価

（省略）

2. 評価詳細説明

2.1. 評価条件

2.1.1. 評価環境

（省略）

2.1.2. 前提情報

（省略）

2.2. 評価体制

評価体制図を図 2.1 に示す。

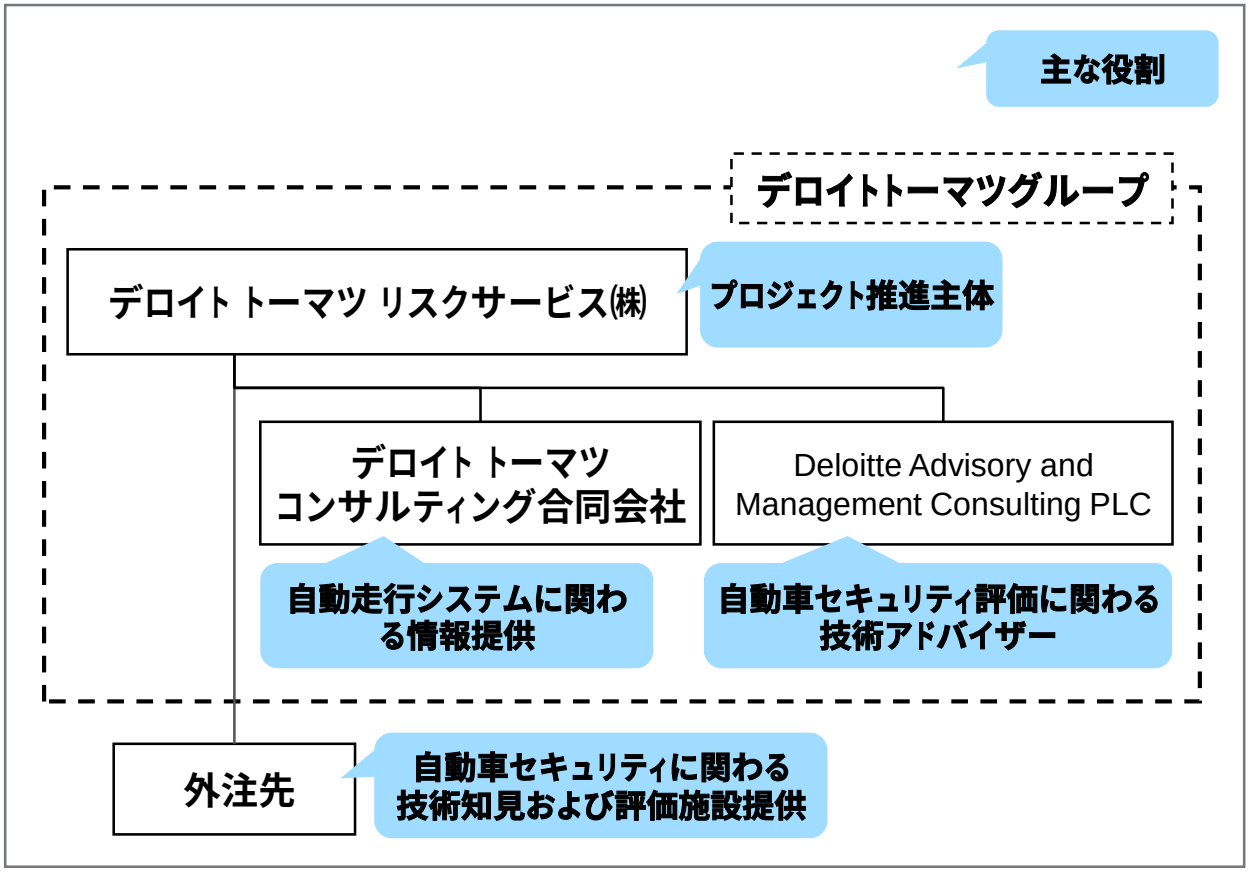


図 2.1 評価体制図

2.3. 評価方法

本評価ではガイドラインドラフトの情報セキュリティ評価プロセスを用いており、そのプロセスでは評価の実施に割り当て可能なリソース（ヒト、モノ、カネ、時間）は有限であり、網羅的に評価を実施することは現実的に不可能であるという前提のもと、攻撃者中心アプローチ、リスクアプローチを採用している。「攻撃者中心アプローチ」と「リスクアプローチ」を基本的な考え方を図 2.2 に示す。

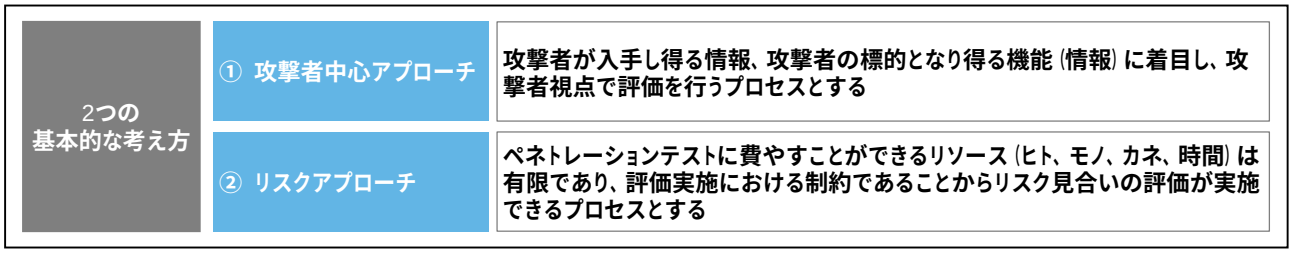


図 2.2 情報セキュリティ評価プロセスの基本的な考え方

また、当評価プロセスは「テスト実施前の評価プロセス」、「テスト実施」、「テスト実施後の評価プロセス」に大別できる。それぞれの評価プロセスのステップと主な実施内容は図 2.3 のとおりである。

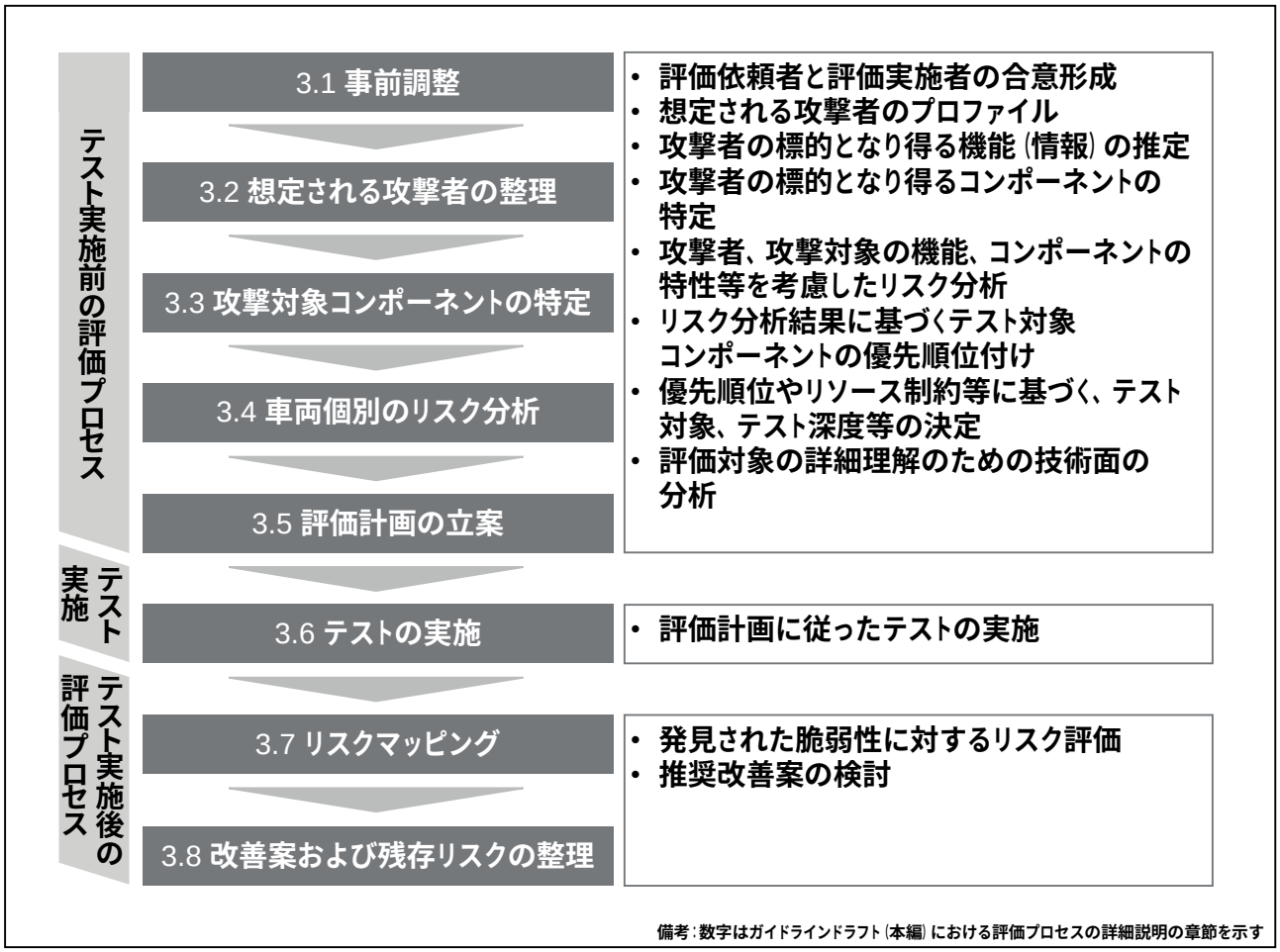


図 2.3 評価プロセス概要

各工程の数字は、ガイドラインドラフト（本編）における評価プロセスの詳細説明の章節を示す。テスト実施前の評価プロセスは、テスト実施に向けた評価計画の立案のために、評価対象のコンポーネン

トを選定するためのリスク分析を行うプロセスである。テストの実施は、計画に従ってテストを実施するプロセスである。テスト実施後の評価プロセスは、テストの実施により発見された脆弱性に対するリスク評価および改善案の検討を行うプロセスである。

以降、それぞれのプロセス内容の説明と本評価で実施した結果について述べる。

2.3.1. 事前調整

実際の情報セキュリティ評価においては評価の実施前に、評価依頼者と評価実施者との間で、目的、評価対象、評価範囲、評価で利用する情報、評価環境等の各種取り決め事項についての調整を行う。

本評価は、作成したガイドラインドラフトの妥当性検証を目的とした試行調査であるので、事前調整は実施していない。

2.3.2. 想定される攻撃者の整理

本評価に用いる攻撃者プロファイルは、ガイドラインドラフトに記載のある攻撃者プロファイルを活用した。以降、本攻撃者プロファイルを用いて、攻撃者が興味を示す機能やコンポーネントについて特定を行った。

2.3.3. 攻撃対象コンポーネントの特定

攻撃対象コンポーネントを特定するために、以下のステップを踏んでいる。

① 評価対象システムにおける機能およびコンポーネントの洗い出し
② 機能とコンポーネントのマッピング
③ 攻撃者が興味を示す機能の特定
④ 攻撃者が興味を示すコンポーネントの特定

2.3.3.1. 評価対象システムにおける機能およびコンポーネントの洗い出し

本評価においては、事前にコンポーネント情報について提供されていたため、コンポーネントの洗い出しについて特に追加となる調査は行っていない。

次に、評価対象システムにおける機能の洗い出しを行った。機能の調査には主に評価対象車両の主要装備一覧表の Web サイトを参照した。

2.3.3.2. 機能とコンポーネントのマッピング

「2.3.3.1 評価対象システムにおける機能およびコンポーネントの洗い出し」においてリストアップした機能とコンポーネントに対して、それぞれの機能が具体的にどのコンポーネントから構成されているかという紐付けを行った。

2.3.3.3. 攻撃者が興味を示す機能の特定

リストアップした各機能について、攻撃の標的となり得る機能をマッピングした。各機能に対する攻撃者の動機を想定してマッピングを行っている。

複数の攻撃者の標的となり得る機能は、攻撃に晒される可能性の高い機能であるため、優先度が高いものとして認識されるべきである。本評価においては、2 つ以上の攻撃者がマッピングされた機能を優先度が高いものと判断し、攻撃者が興味を示す機能として扱っている。

2.3.3.4. 攻撃者が興味を示すコンポーネントの特定

攻撃者が興味を示すコンポーネントを特定した。

2.3.3.5. 評価対象外となる機能およびコンポーネント

攻撃者が興味を示すかどうかの観点で優先度が低いとされた機能については以降の評価において評価対象外となる。

2.3.4. 車両個別のリスク分析

ここからは、攻撃者が興味を示すコンポーネントに対してリスク分析を行い、コンポーネント毎に対する評価の優先度付けを行う。ガイドラインドラフトではリスク分析手法として、IT システム分野における標準的なリスク分析手法である OWASP（The Open Web Application Security Project）の OWASP Risk Rating Methodology をベースとした手法を適用している。（図 2.4 参照）

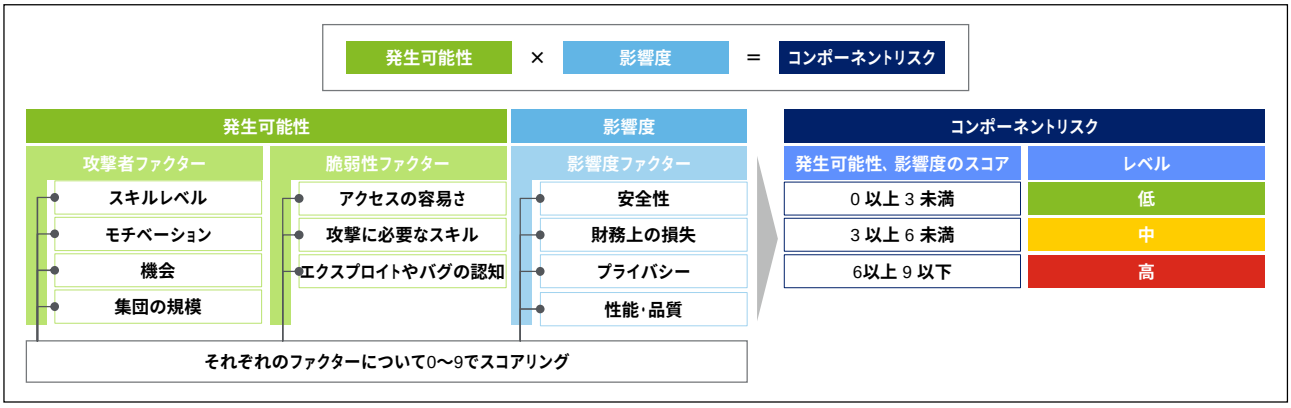


図 2.4 リスク分析手法の考え方

リスク分析では、発生可能性と影響度からコンポーネントリスクを求め評価を行う。コンポーネントリスクを構成する要素を表 2-1 に示す。

表 2-1 コンポーネントリスクを構成する要素

コンポーネントリスクの構成要素	内容
発生可能性（Likelihood）	脆弱性が攻撃者によって発見され、悪用される可能性の尺度

コンポーネントリスクの構成要素		内容
	攻撃者ファクター（Threat Agent Factors）	攻撃者による攻撃が成功する可能性の尺度
	脆弱性ファクター（Vulnerability Factors）	当該コンポーネントで脆弱性が発見され、悪用される可能性の尺度
影響度（Impact）		攻撃が成功した場合の影響の尺度
	影響度ファクター（Impact Factors）	脆弱性が悪用される場合のシステムへの影響の尺度

リスク分析の手順として、以下のステップを踏んでいる。

① 攻撃者ファクターの導出
② 脆弱性ファクターの導出
③ 発生可能性の計算
④ 影響度の見積（影響度ファクターの導出）
⑤ コンポーネントリスクの評価

2.3.4.1. 攻撃者ファクターの導出

2.3.4.1.1. 攻撃者ファクターの説明

攻撃者ファクターは、特定の脆弱性が、攻撃者によって発見され、悪用される可能性の尺度であり、攻撃者の「スキルレベル」、「モチベーション」、「機会」、「集団の規模」の 4 つの要素からなる。「スキルレベル」、「機会」、「集団の規模」は攻撃者ごとにスコアリングを行い、「モチベーション」は攻撃者および機能ごとにスコアリングを行った。それぞれの要素は、0～9 の尺度でスコアリングし、攻撃者ファクターは 4 つの要素の尺度の平均値で計算している。

攻撃者ファクターの 4 つの要素は表 2-2 のとおりである。

表 2-2 攻撃者ファクターの構成要素

攻撃者ファクターの構成要素	内容
スキルレベル	攻撃者はどの程度熟練しているか
モチベーション	攻撃者が標的とする機能に関して、どの程度モチベーションがあるか
機会	攻撃者がコンポーネントを攻撃するのにどの程度のツール類（HW および SW）や情報を必要としているか
集団の規模	攻撃者の規模はどの程度か

2.3.4.1.2. 機能ごとおよびコンポーネントごとの攻撃者ファクターの導出

コンポーネントの攻撃者ファクターを導出するためには、まず機能ごとに攻撃者ファクターを求め、その結果を基に、当該機能を構成するコンポーネントごとの攻撃者ファクターを導出した。

2.3.4.2. 脆弱性ファクターの導出

脆弱性ファクターは、コンポーネントで脆弱性が発見され、悪用される可能性の尺度であり、「アクセスの容易さ」、「コンポーネントの攻撃に必要な情報やツール」、「エクスプロイトやバグの認知」の 3 つの要素からなり、コンポーネントごとにスコアリングを行った。

それぞれの要素は、0～9 の尺度でスコアリングし、脆弱性ファクターは 3 つの要素の尺度の平均値で計算している。

脆弱性ファクターの 3 つの要素は表 2-3 のとおりである。

表 2-3　脆弱性ファクターの構成要素

脆弱性ファクターの構成要素	内容
アクセスの容易さ	攻撃者が当該コンポーネントにどの程度容易にアクセスできるか
コンポーネントの攻撃に必要な情報やツール	攻撃者が当該コンポーネントの脆弱性をどの程度容易に悪用できるか
エクスプロイトやバグの認知	当該コンポーネントの脆弱性はどの程度知られているか

2.3.4.3. 発生可能性の計算

発生可能性は、脆弱性が攻撃者によって発見され、悪用される可能性の尺度であり、コンポーネントごとに計算した。なお、発生可能性は攻撃者ファクターと脆弱性ファクターの平均値としている。

2.3.4.4. 影響度の見積 (影響度ファクターの導出)

影響度は、攻撃が成功した場合の影響の尺度であり、影響度ファクターと同値である。

影響度ファクターは、脆弱性が悪用される場合のシステムへの影響の尺度であり、「安全性」、「財務上の損失」、「プライバシー」、「性能・品質」の 4 つの要素からなり、コンポーネントごとにスコアリングを行った。それぞれの要素は、0～9 の尺度でスコアリングし、影響度ファクターは 4 つの要素の尺度の平均値で計算している。

影響度ファクターの 4 つの要素は表 2-4 のとおりである。

表 2-4　影響度ファクターの構成要素

影響度ファクターの構成要素	内容
安全性	当該コンポーネントが攻撃されセキュリティが侵害された場合、安全性に係る影響はどの程度あるか
財務上の損失	当該コンポーネントが攻撃されセキュリティが侵害された場合、OEM または車両オーナーに対する財務上の損失はどの程度あるか
プライバシー	当該コンポーネントが攻撃されセキュリティが侵害された場合、プライバシーや機密性の損失はどの程度あるか
性能・品質	当該コンポーネントが攻撃されセキュリティが侵害された場合、車両性能や品質に係る影響はどの程度あるか

「2.3.3.4 攻撃者が興味を示すコンポーネントの特定」において、攻撃者の標的となり得る機能を構成するコンポーネントが特定されているため、それぞれのコンポーネントに対し、「安全性」、「財務上の損失」、「プライバシー」、「性能・品質」の 4 つの要素についてスコアリングを行い、その平均値を求めることで、影響度ファクターを導出した。

2.3.4.5. コンポーネントリスクの評価

攻撃者の標的となり得るコンポーネント全てに対し、発生可能性と影響度の積をとることでコンポーネントリスクを計算した。

また、表 2-5 に従い発生可能性と影響度に対して、スコアに応じてそのレベルを「高」、「中」、「低」で評価した。

表 2-5　発生可能性と影響度のスコアとそれに応じたレベル

スコア	レベル
0 以上 3 未満	低
3 以上 6 未満	中
6 以上 9 以下	高

また、発生可能性と影響度の評価軸において、コンポーネントリスクをヒートマップとして表現した。

今回の評価では、発生可能性と影響度の組合せが（低、低）、（低、中）、（中、低）となるコンポーネントはコンポーネントリスクが低いと判断し評価対象外とした。そして、それ以外のリスクにマッピングされたコンポーネントを評価対象とした。

2.3.5. 評価計画の立案

2.3.5.1. 技術的分析

2.3.5.1.1. コンポーネント間接続および無線インターフェースの明確化

システムブロック図より明らかになった各コンポーネントがつながるバスおよび無線インターフェースをまとめる。無線インターフェースにおいて、評価環境にアンテナが実装されていない機能については評価対象外とする。

また、評価対象のコンポーネントのうち、アクセス容易性が高い USB ジャックについては、USB のネットワークデバイスを挿入すれば無線アクセスが可能となり得るので、本評価においては USB についても評価対象インターフェースの 1 つと解釈することとした。

本調査結果より、評価対象インターフェースとして、Wi-Fi、Bluetooth、LTE、USB とした。

2.3.5.1.2. ハードウェアハッキングおよびリバースエンジニアリングによる情報収集

（省略）

2.3.5.2. 評価項目の作成

評価項目作成のインプットとなる情報として大きく以下の 3 つがある。

（1） ガイドラインドラフト（本編）の「付録 2 一般的な評価項目一覧」
（2） 随時公表される脆弱性情報
（3） 技術的分析結果

これらの情報についての概要を説明するとともに、本評価における活用方法について説明する。

（1）ガイドラインドラフト（本編）の「付録 2 一般的な評価項目一覧」

ガイドラインドラフト（本編）の「付録 2 一般的な評価項目一覧」（以下「付録 2」）は、主に自動車分野における過去のインシデント事例と、IT システム分野の既知の脆弱性情報から作成されている。自動車分野で既知あるいは未知の脆弱性で場合分けを行い、自動車分野で未知の脆弱性については、IT システム分野における脆弱性を考慮しており、その中でも自動車に適用可能な脆弱性について考慮している。付録 2 に含まれる脆弱性内容の概要を図 2.5 に示す。付録 2 にはこれら脆弱性を発見するための評価項目を一覧としてまとめている。

本評価においては、付録 2 の評価項目のうち Web アプリケーションに係る評価項目を対象外とした。更に、ガイドラインドラフト（実践手引き）の IP ネットワーク編、Wi-Fi 編、Bluetooth 編と紐づく評価項目を抽出した。

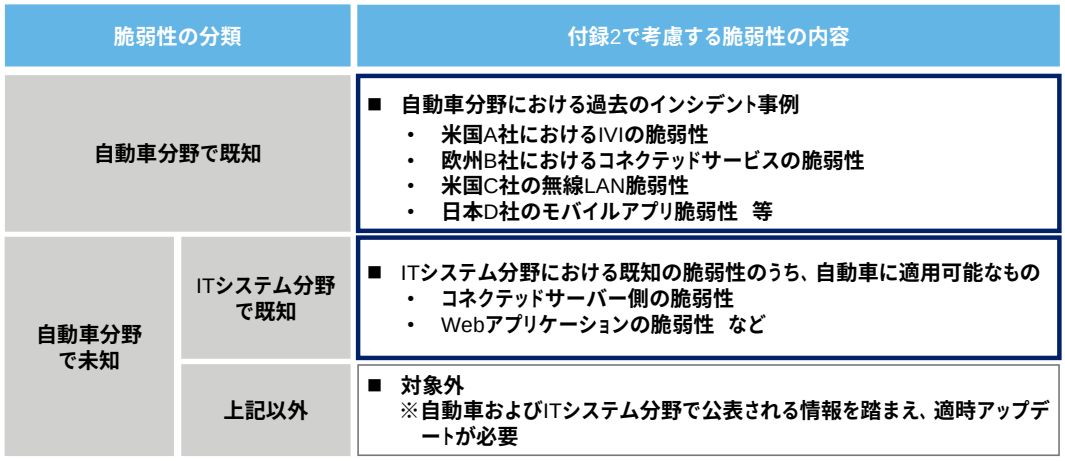


図 2.5 付録 2 に含まれる脆弱性内容概要

（2）随時公表される脆弱性情報

随時公表される脆弱性情報としては、Wi-Fi の WPA2 に対する深刻な脆弱性である KRACK*1（Key Reinstallation Attacks）および Bluetooth の実装における脆弱性である BlueBorne*2 を考慮した。

*1：CVE-2017-13077、CVE-2017-13078、CVE-2017-13079、CVE-2017-13080、CVE-2017-13081、CVE-2017-13082、CVE-2017-13084、CVE-2017-13086、CVE-2017-13087、CVE-2017-13088

*2：CVE-2017-0781、CVE-2017-0782、CVE-2017-0783、CVE-2017-0785、CVE-2017-1000250、CVE-2017-1000251、CVE-2017-14315、CVE-2017-8628

（3）技術的分析結果

技術的分析結果として、ストレージデバイスに対するハードウェアハッキングおよびリバースエンジニアリングにより収集した情報として活用した。

2.3.5.3. 評価項目一覧

2.3.5.3.1. Wi-Fi の評価項目

（省略）

2.3.5.3.1. Bluetooth の評価項目

（省略）

2.3.5.3.1. LTE の評価項目

（省略）

2.3.5.3.2. USB の評価項目

（省略）

3. 評価結果

3.1. ペネトレーションテストによって発見された脆弱性に対するリスク評価（リスクマッピング）

リスク評価には CVSS の基本評価基準（Base Metrics）に基づいた評価基準を用いており、自動車に固有な要件を考慮し、以下の 4 つのレイヤーでリスク評価手法を定義している。

① CVSS v3.0 の標準的なメトリクスを用いたコンポーネントレベルリスク評価
② CVSS v3.0 の標準的なメトリクスを用いた車両レベルリスク評価
③ 低、中、高、緊急の 4 つの定性的な基準を用いたフリートレベルリスク評価
④ 上記①～③の加重平均によるトータルリスク

テストにより発見された脆弱性ごとに、コンポーネントレベルリスク、車両レベルリスク、フリートレベルリスクをそれぞれ算出した上で、それらの加重平均を行い、トータルリスクを算出した。そのトータルリスクを最終的な指標として、発見された脆弱性の評価を行った。

以下に、各リスクの評価基準および算出方法について説明する。

3.1.1. コンポーネントレベルリスク評価

CVSS の基本評価基準における脆弱性評価の構成要素は、攻撃元区分（AV）、攻撃条件の複雑さ（AC）、必要な特権レベル（PR）、ユーザー関与レベル（UI）、スコープ（S）、機密性への影響（C）、完全性への影響（I）、可用性への影響（A）の 8 つがある。それぞれの構成要素について、定性的な評価およびそれに紐付く定量的な評価（スコア）が定義されている。

コンポーネントレベルリスクは、対象となるコンポーネント単体でのリスクを意味する。CVSS v3.0 に基づいたコンポーネントレベルでのリスクに対する構成要素を表 3-1 に示す。

表 3-1 （省略）

3.1.2. 車両レベルリスク評価

車両レベルリスクは、コンポーネント同士が接続されることにより構成された車両単体におけるリスクを意味する。CVSS v3.0 に基づく車両レベルリスクの構成要素を表 3-2 に示す。

表 3-2 （省略）

3.1.3. フリートレベルリスク評価

フリートレベルリスクは、1 つの脆弱性が一台の車両のみならず、複数の車両に影響を与える場合を考慮したリスクである。フリートレベルリスクは、表 3-3 に示す CVSS v3.0 の深刻度評価尺度のスコアを参照している。

表 3-3 CVSS v3.0 の深刻度評価尺度

深刻度	スコア
無	0
低	0.1－3.9

深刻度	スコア
中	4.0－6.9
高	7.0－8.9
緊急	9.0－10.0

表 3-4 にフリートレベルリスクの評価尺度を示す。

表 3-4 （省略）

3.1.4. トータルリスク評価

トータルリスクは、コンポーネントレベルリスク、車両レベルリスク、フリートレベルリスクの加重平均により求める。一般に、それぞれのリスクの大小関係は、1 つの脆弱性の影響が及ぶ範囲に比例するため「フリートレベルリスク」＞「車両レベルリスク」＞「コンポーネントレベルリスク」と考えることができる。最終的に、トータルリスクのスコアを、「表 3-3　CVSS v3.0 の深刻度評価尺度」に照らし合わせ、脆弱性における深刻度の評価を行う。

3.2. 個別発見事項

（省略）

3.3. 個別評価結果

（省略）

3.4. 情報セキュリティ評価ガイドラインドラフトの妥当性

（省略）

以上

別紙A. ハードウェアハッキングとリバースエンジニアリング

（省略）

別紙B. 個別評価結果詳細

（省略）

「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／情報セキュリティ実証実験」

実証実験の運営準備検討結果報告書

平成３０年２月

目次

１．検討概要 3

２．検討結果 4

(1) **計画立案** 4

(2) **実証実験参加者の募集要領、申請書、規約類の策定** 4

(3) **契約書類に関する検討** 4

(4) **セキュリティ管理体制・方法の確立** 5

１．検討概要

2018 年度に実施する実証実験の早期開始の実現を目的として、実証実験開始に必要な計画を立案するとともに、実証実験参加者の募集要領、申請書や規約類、契約書類（秘密保持契約、等）等の作成等、実証実験の事務局運営のための各種準備を実施した。

（1）計画立案

次年度の実証実験環境の場所、参加者車両又はシステム・必要機材等の借用や購入に関する計画の検討、及び必要に応じて各種事前手続、申請、契約締結等の検討を実施した。

（2）実証実験参加者の募集要領、申請書、規約類の策定

実証実験の円滑な推進のために参加者に周知及び合意するべき事項等を明らかにし、参加者募集要領や規約類を検討のうえ、文書案を作成した。

（3）契約書類に関する検討

機密保持条件等を含む契約案策定のために国立研究開発法人新エネルギー・産業技術総合開発機構（以下、貴機構という）と協議の上で想定参加者等から要求や条件を収集し、締結に向けた課題を明らかにしたうえで整理し、契約書案を作成した。

（4）セキュリティ管理体制・方法の確立

機密として扱うべき評価結果情報等について、必要なセキュリティ管理を実施するための管理体制及び方法を検討した。

２．検討結果

(1)　計画立案

次年度の実証実験環境の場所、参加者車両又はシステム・必要機材等の借用や購入に関する計画検討、及び各種事前手続、申請、契約締結等の必要性及び必要な場合の事前準備の検討を実施した。

・次年度実証実験計画については、「H30 年度実施計画書案」を参照のこと
・各種事前手続、申請、契約締結等については、次項(2)及び(3)を参照のこと

(2) 実証実験参加者の募集要領、申請書、規約類の策定

実証実験の円滑な推進のために参加者に周知及び合意するべき事項をリストアップし、参加者募集要領や規約類を検討のうえ、文書案を作成した。

実証実験参加にあたっての規約類については、各参加企業への依頼事項として募集要領の中でその主な事項を提示するとともに、各参加企業と締結する契約書類に含めることとしている。（後者については次項(3)を参照のこと）

・参加者募集要領については、別紙 1「実証実験参加企業募集要領」を参照のこと

また、上記参加者募集要領に基づき、参加企業募集のための説明資料を作成した。資料作成にあたっては、第 2 回技術委員会（2018 年 2 月 2 日開催）及び第 3 回技術委員会（2018 年 2 月 20 日開催）にて説明資料案を提示し、参加企業の候補となる自動車メーカー様等のご意見・ご要望を集め、それらを反映し作成した。

・参加企業募集のための説明資料については、別紙 2「実証実験計画及び実施要領などについて」（実証実験への参加企業募集にあたって）を参照のこと

なお、実証実験参加募集にあたっては、貴機構より提示の候補企業リストを元に、各社への個別打診にて行う（オープンな募集は行わない）旨の指示を受けており、上記参加企業募集のための説明資料を用いた個別の依頼及び参加エントリーの回答を頂くことを想定して、募集のための依頼文書や申請書の事前準備は不要と判断した。

(3) 契約書類に関する検討

機密保持条件等を含む契約案策定のために貴機構と協議の上で想定参加者等から要求や条件を収集し、締結に向けた課題を明らかにしたうえで整理し、契約書案を作成した。

・秘密保持契約書 雛型

参加企業個社ごとに締結するもので、車両評価実施にあたって参加企業から提供頂く各種機密情報（車両の仕様等に関わる情報、等）及び評価結果に関わる情報の機密管理のために、開示範囲等を明記します。
秘密保持契約 雛型案については、別紙 3「秘密保持契約（NDA）_雛型案」を参照のこと

・評価車両提供に関わる覚書 雛型
参加企業個社ごとに締結するもので、評価実施のための提供車両の要件や提供期間、等の取り決め事項について明記します。
車両提供に関わる覚書 雛型案については、別紙 4「覚書_雛型案」を参照のこと

その他、実証実験にあたって各参加企業又は評価実施に必要なサービスを提供する企業と取り交わしが必要になる契約書類として、今期実証前調査の結果を踏まえて、下記の書類を想定した。これらについては、実証実験における評価対象や評価環境、具体的な評価項目等によって変わってくるため、事前の準備は不要と判断した。

- ✓ テレマティクス関連サービスの契約書類 … 評価実施にあたって必要となる、テレマティクスサービス等（インフォテイメント関連を含む）の契約のための申請手続きに関わる書類
  例．通信サービス利用申込書
- ✓ 確認書 … 評価実施の対象とするサービスやアプリケーション、サーバーに関わる情報（IP アドレス、等）や評価実施内容、事前の準備や依頼事項、等を明記した書類で、評価実施に先立って関連サービス提供者と取り交わすもの

(4) セキュリティ管理体制・方法の確立
機密として扱うべき評価結果情報等について、必要なセキュリティ管理を実施するための管理体制及び方法を検討した。

・セキュリティ管理体制及び方法については、別紙 1「実証実験参加企業募集要領」の「５．補足（情報管理について）」を参照のこと

以 上

別紙 1

「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／情報セキュリティ実証実験」

実証実験
参加募集要領

平成３０年４月

目　次

１．募集趣旨 3

２．実証実験概要 3

３．募集手続き 5

４．参加条件 6

５．補足（情報管理について） 7

６．問い合わせ先 8

１．募集趣旨

2020 年の東京オリンピック・パラリンピックに向けて、自動走行システムの実用化の加速を図ることが重要となっています。それにあたり、5 つの技術領域（ダイナミックマップ、HMI、情報セキュリティ、歩行者事故低減、次世代都市交通）を中心に、自動車メーカー等の参加のもと大規模実証実験を行い、今後の実用化に向けた、技術面、運用面、制度面等での具体的課題抽出を行うべく、各種取り組みが進められています。

その情報セキュリティ領域における取り組みとして、車両レベル・コンポーネントレベルでのセキュリティ評価手法・プロトコルをガイドラインとして策定し、対ハッキング性能検証のためのブラックボックステストを行うことで、車両への通信を用いた攻撃に対する評価手法を確立することを目的として、実証実験を行うものです。

実証実験にあたっては、参加企業を募り、車両または車両ベンチ（部品システム）をご提供頂き、当該車両または車両ベンチ（部品システム）に対するブラックボックステストを行うことで検証作業を実施します。

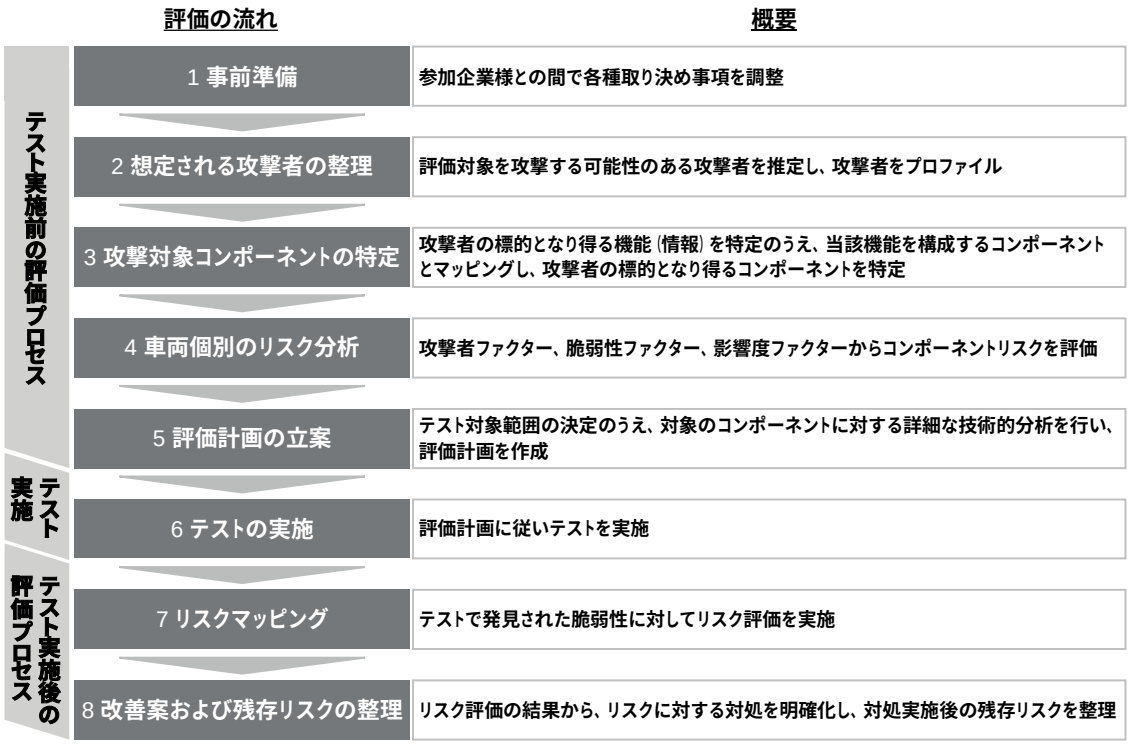
２．実証実験概要

本実証実験では、下表の通り 2017 年 2 月末までに、Step1（実証前調査）として情報セキュリティ評価ガイドラインドラフト（以下「ガイドラインドラフト」という）の作成を行っており、本募集ではその後続の Step2（実証実験）にてその検証のための車両評価に使用する車両または車両ベンチ（部品システム）を提供頂く参加企業を募るものです。

【実証実験の全体像】

実証実験における車両評価では、ガイドラインドラフトで用いられている車両評価の流れ（下図）に従い、参加企業から提供頂く車両または車両ベンチ（部品システム）の評価を行います。

【車両評価の流れ】



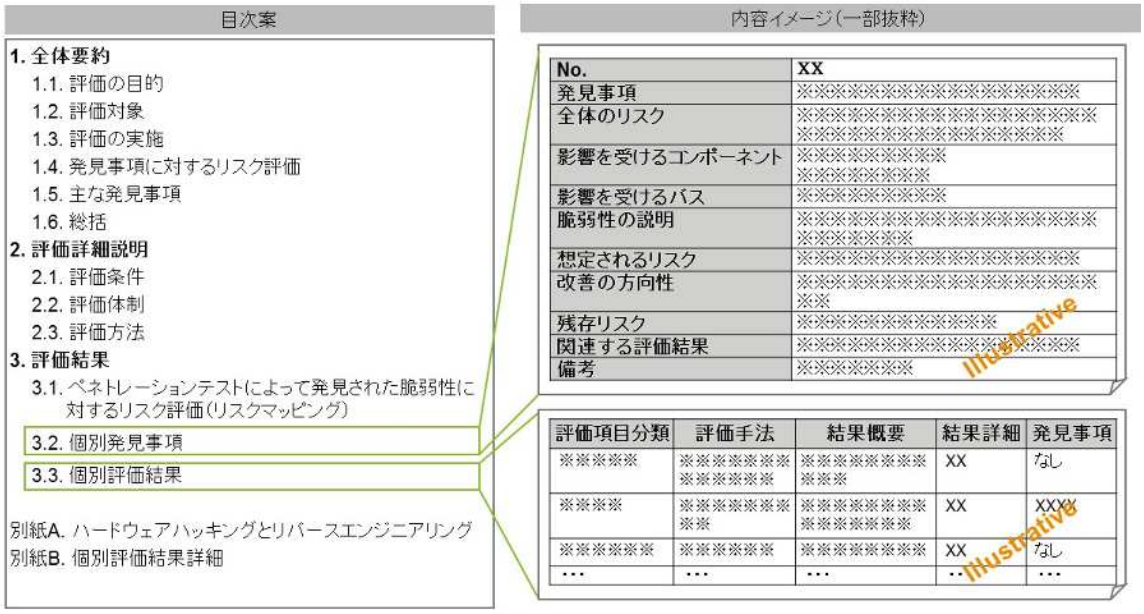
なお、参加企業からご提供いただく車両または車両ベンチ（部品システム）は専用の施設に搬入し、セキュリティや安全の確保された場所にて評価を実施します。

【評価作業実施場所の例】

施設名称	設備内容
拠点A	● 車両3台が入庫可能で隔離された**本実証実験専用の車両秘匿管理施設**を用意（排気設備完備） ● 3か所の出入り口について、**IDカードによる入退室管理**で物理セキュリティを確保 ● 必要に応じて、隣接する電波暗室のシャーシダイナモを用いた評価実施も可能

また、本車両評価において発見された手続き等に関わる問題点や気付きをもとに、ガイドラインドラフトを更新するとともに、評価した結果、発見された脆弱性については、車両または車両ベンチ（部品システム）を提供頂いた企業毎に個別に評価レポート（下記イメージ）を提出のうえその内容をご報告します。

【評価レポートイメージ】

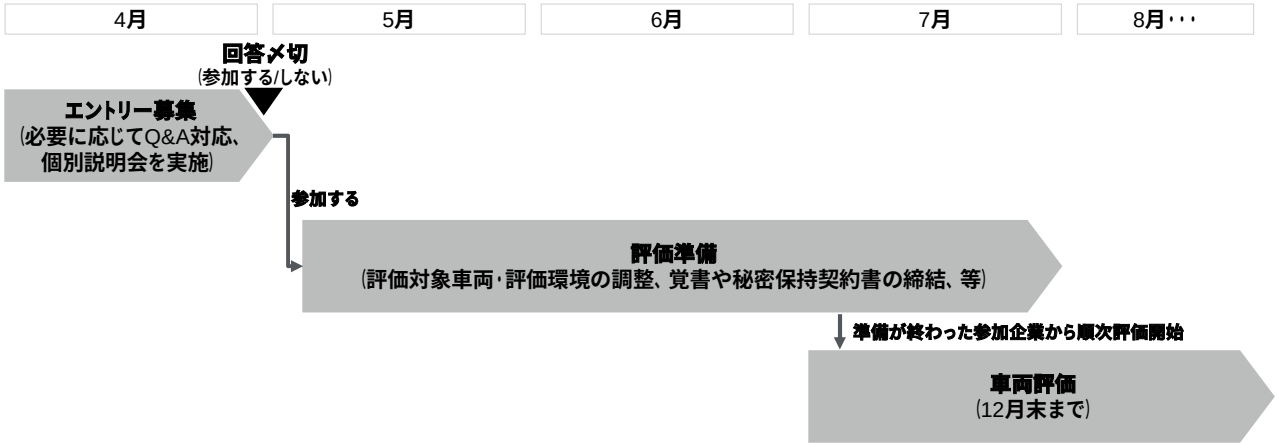


３．募集手続き

参加企業の募集は、別途提示される候補企業（国内自動車 OEM）の各社に個別打診により実施します。4 月上旬に、各社に参加エントリーの依頼の連絡を行い、4 月末までにエントリーする/しないの回答を受けます。

エントリーする参加企業は、評価対象車両や評価環境の調整・準備、評価車両提供に関わる覚書や秘密保持契約書の締結等の車両評価に向けた準備を行い、準備が整った参加企業から順次車両評価を開始します（7 月の車両評価開始を目指します）。

【募集開始から車両評価開始まで】



４．参加条件

参加にあたっては、原則、下記参加規約に同意頂くことを条件とします。（評価準備の際に覚書等の書面にて取り交わします）

【実証実験 参加規約】

（1）車両の要件

参加企業は、少なくとも以下のうちいずれかの外部通信機能を持つ車両を、実証実験の評価車両として提供します。

- Wi-Fi
- Bluetooth
- 3G/4G/LTE

（2）車両の種別

提供する車両の種別は、開発車または市販車とします。

（3）車両の提供形態

車両そのものの提供が難しい場合は、車両ベンチ（部品システム）でも可とします。ただし、「（1）車両の要件」を満たし、無線区間のテストができるシステムであることが必要です。

（4）提供期間

車両提供の期間は 6 ヶ月間とします。
ただし、6 ヶ月間の提供がどうしても困難な場合は、個別の調整を可とします。

（5）予備部品の準備

参加企業は、評価対象車両 1 台に加えて、当該車両に関わる予備部品（評価に必要となるヘッドユニット等を含む部品システム）を少なくとも 1 台*を予め用意しておきます。

* より深い評価を行う場合は 2 台以上を用意

（6）保守サポート

参加企業は、評価環境構築時および評価実施中の評価車両に関する問題発生時のサポート体制（担当窓口および必要な部品サプライヤーとの連携体制）を設置します。

（7）車両提供に係る費用

車両提供に係る費用（車両そのものおよび運送費、予備部品を想定）は、参加企業の負担とします。
なお、マニュアル等のその他関連費用については、評価実施者が負担します。

（8）外部通信環境

参加企業は、評価車両とともにテレマティクスで必要になる通信サービスおよびサーバー側のテスト環境（検証用サーバー、等）を提供します。テスト用アカウント等、

評価に必要事項も併せて用意します。また、参加企業は、車両出荷前に予め提供する車両との開通テストを実施しておきます。

（9）車両の返却

参加企業は、提供する車両について、その返却時に評価により破損している恐れがあることを了承します。

（１０）情報提供

参加企業は、車両に関する一般ユーザーが手に入る範囲の情報として、ユーザーマニュアルやサービスマニュアルを用意し、評価に必要となる情報を提供します。
（費用は評価者の負担とします）

（１１）評価に関わる承諾

参加企業は、覚書または秘密保持契約書、確認書等の取り交わしを通じて、車両評価において車両およびサーバーにサイバー攻撃を実施することを承諾します。

（１２）個別調整

参加企業は、エントリー後に、前項までの規約を含め、より具体的な内容について評価者と協議のうえ調整を行います。

５．補足（情報管理について）

（1）情報セキュリティ管理体制

実証実験において取り扱う情報に大変機微なものが含まれることを踏まえ、その機密管理を徹底します。

① 海外法人との連携時の情報の海外流出を防ぐ機密管理

海外メンバーからの機密情報の流出を防ぐべく、配慮を行います。

■ 海外のチームメンバーが知りうる情報の最小限化

下記にて、海外メンバーが本プロジェクトで知りうる情報は最小限に抑えます。

- 評価は日本国内でのみ実施する
- 海外メンバーは、アドバイザーとしての関与であり、評価作業を直接実施しない
  （海外メンバーへは、ノウハウや知見の提供に必要な情報のみを提供）

■ 契約により海外のチームメンバーからの対外情報流出を防止

海外メンバーが本プロジェクトで知り得た機密情報は、日本と当該海外法人との契約における秘密保持条項により、機密保持を担保します。

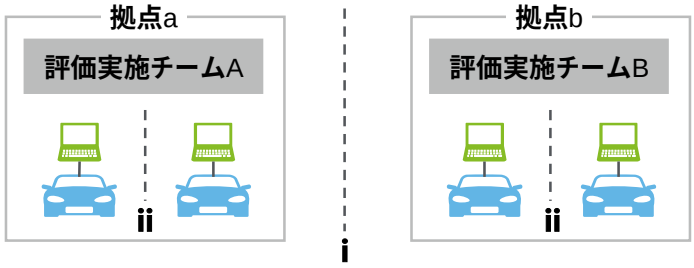
② 参加企業間の評価に関わる情報のセキュリティ確保

評価環境を物理的に分けることでセキュリティを確保します。

■ 評価拠点による物理的隔離（ｉ）

評価実施は 2 つの拠点（それぞれの別の評価実施チームが評価を実施する体制）とし、かつ拠点間の評価車両の移動は行わないことにより、拠点間でのセキュリティを確保します。

■ テスト実施環境の物理的隔離（ⅱ）
同一拠点で複数の評価車両を評価する場合において、テスト実施環境（評価で使用する PC 等）を物理的に分けることでセキュリティを確保します。



（２）評価結果の開示範囲
車両固有の評価結果については、参加企業や実証実験事務局と締結する秘密保持契約に基づき各参加企業に限定して開示します。

凡例 ○ ： 開示する
× ： 開示しない

情報分類		開示範囲		
		評価車両の提供者（各参加企業）	実証実験事務局 (NEDO様)	公表（ガイドライン等に記載）
1	車両毎の評価結果	○	×	×
2	車両毎の評価項目/手順	○	△*2	×
3	統計化*1した評価結果	○	○	○
4	汎用化した評価項目/手順	○	○	○

*1「統計化」とは、 複数の車両の評価データをその性質や傾向を数量的に把握するために整理することを言い、「統計化」によって作られたデータからは参加企業様が特定できなくなります。
*2 参加企業様からの許諾を頂いた範囲内での開示とします。

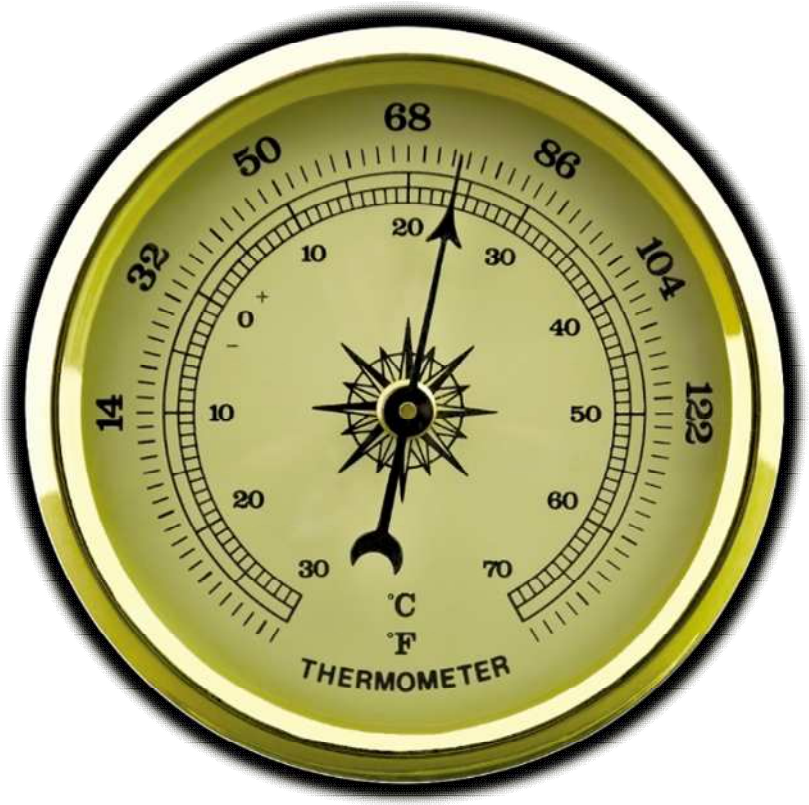
６．問い合わせ先

本事業委託先　：XXXXXXXXXXX
担当　：○○ ○○、○○ ○○
電話番号　：XX-XXXX-XXXX
Fax　：XX-XXXX-XXXX
E-mail　：XXXX@xxx.xxxx.xxx

以 上

別紙2

「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／情報セキュリティ実証実験」



実証実験への参加企業募集にあたって

（実証実験計画および実施要領などについて）

2018年2月

アジェンダ

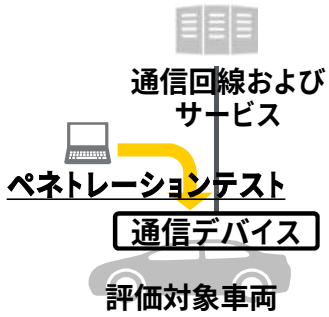
実証実験の概要	3
参加企業募集に向けたご依頼事項	8
実証実験における車両評価について	14
情報の機密管理について	18

実証実験の概要

車両への通信を用いた攻撃に対する評価手法確立のために実証実験を行います

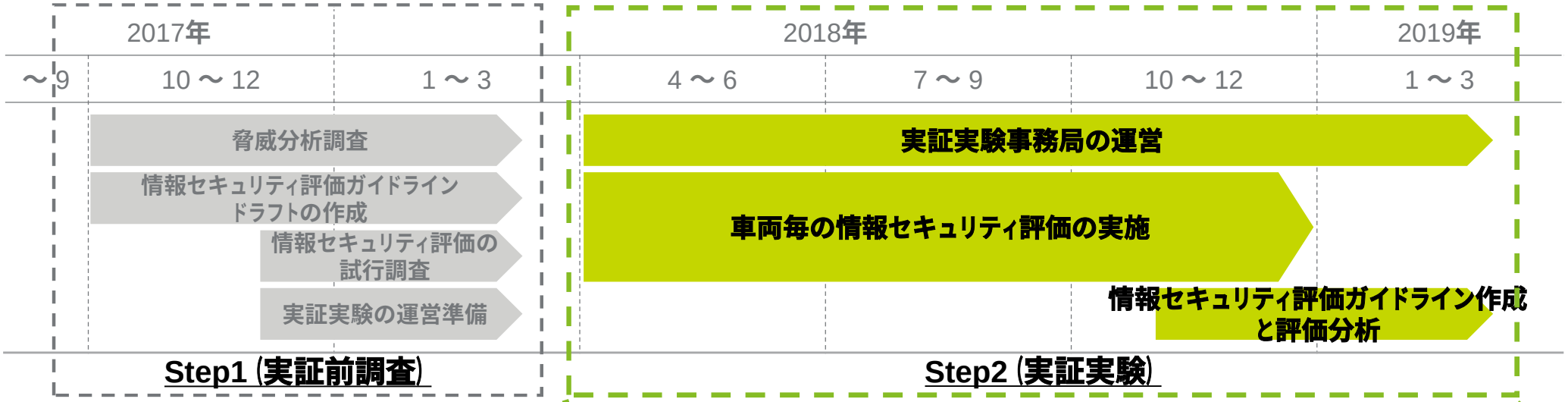
実証実験の背景と目的

背景	■ 2020年の東京オリンピック・パラリンピックに向けて、自動走行システムの実用化の加速を図ることが重要となっています ■ 5つの技術領域（ダイナミックマップ、HMI、情報セキュリティ、歩行者事故低減、次世代都市交通）を中心に、自動車メーカー等の参加のもと大規模実証実験を行い、今後の実用化に向けた、技術面、運用面、制度面等での具体的課題抽出が必要です
目的	■ 車両レベル・コンポーネントレベルでのセキュリティ評価手法・プロトコルをガイドラインとして策定し、本実証実験を通して募る参加者の車両を用いて対ハッキング性能検証のためのブラックボックステストを行うことで、**車両への通信を用いた攻撃に対する評価手法**を確立します

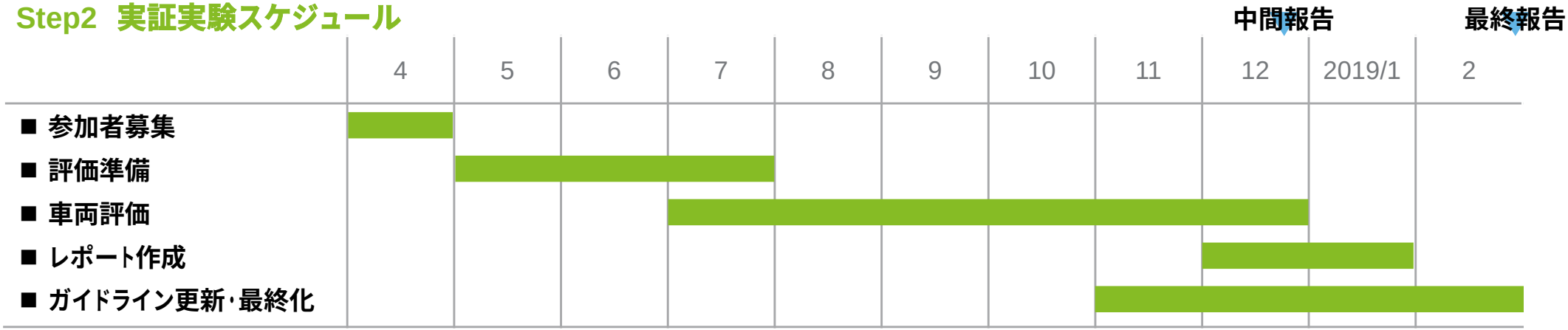


2017年度作成した評価ガイドラインに基づき、年内に実証実験の各評価を完了し、2019年2月末までにその結果を整理します

全体スケジュール



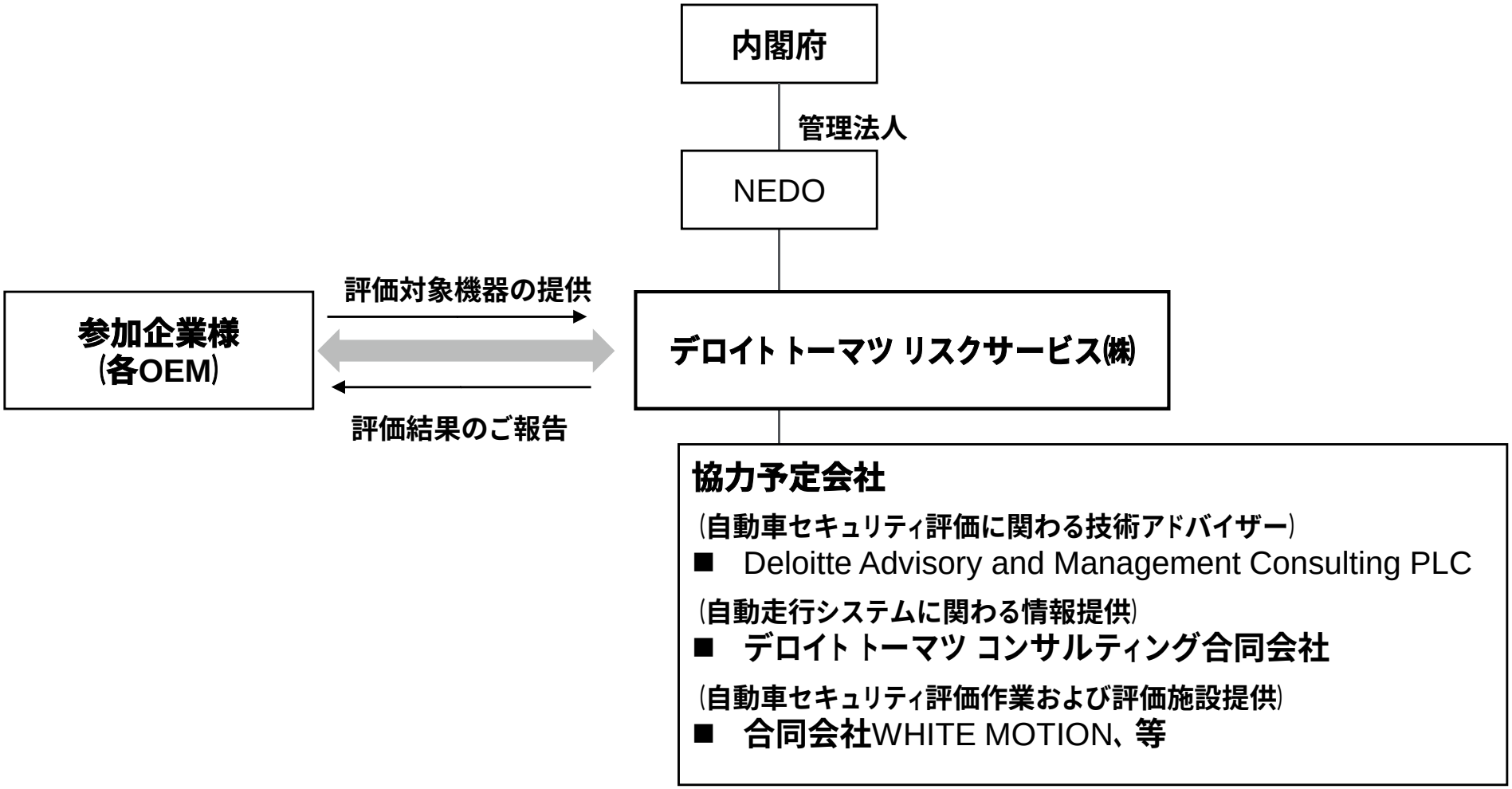
Step2　実証実験スケジュール



実証実験の進め方は9ページ参照

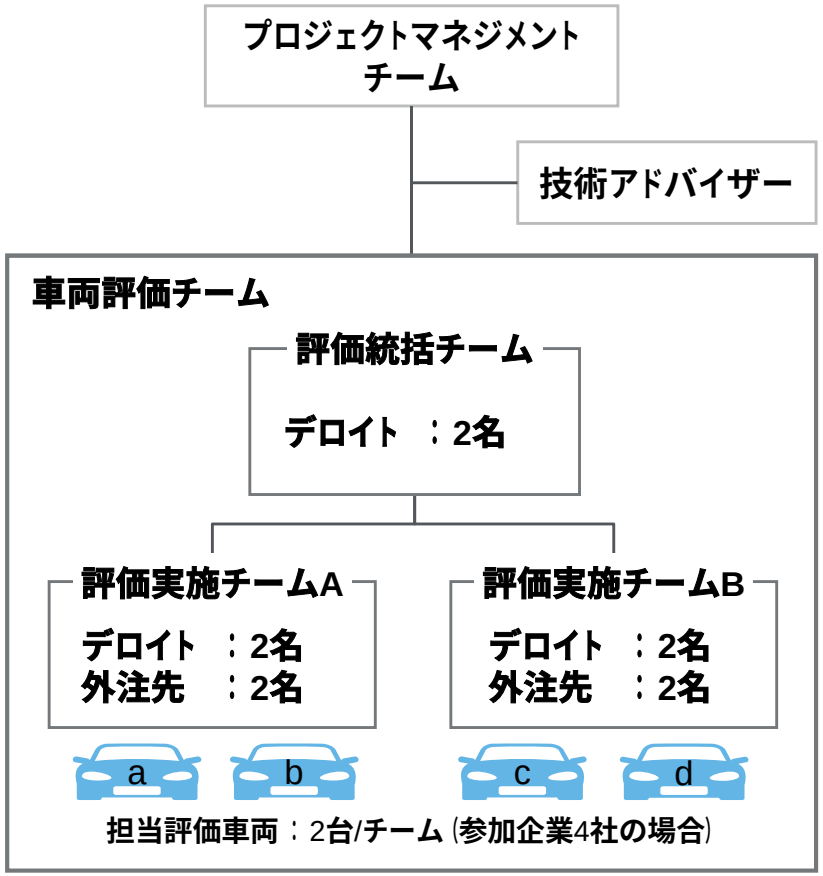
各協力会社と連携のうえ、実証実験を推進します

実証実験の推進体制



Step1（実証前調査）での情報セキュリティ評価の試行調査を担当していたメンバーを中心に、情報セキュリティ評価の経験者により車両評価チームを組成します

実証実験における車両評価チーム体制（イメージ）



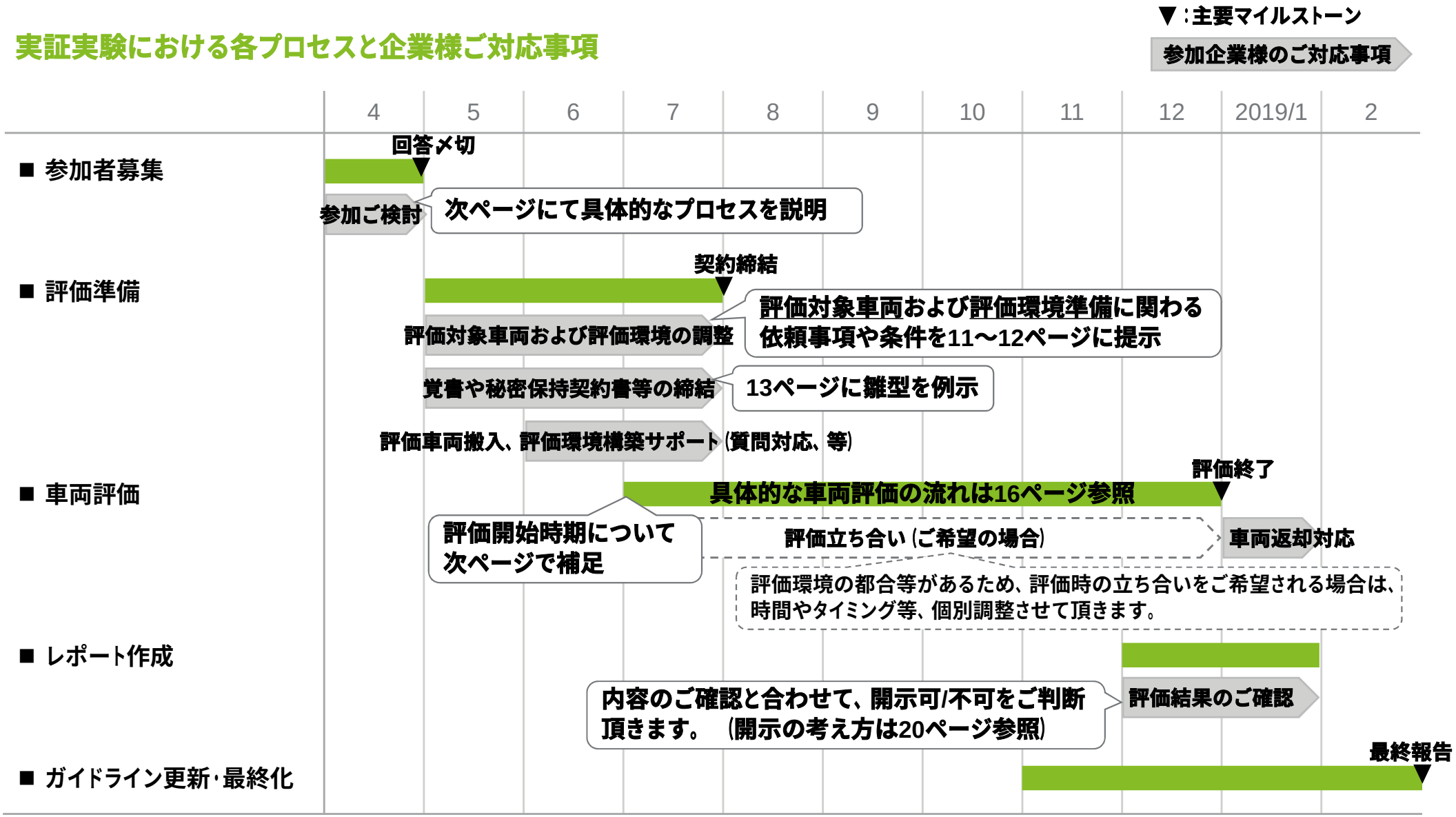
■ 主要メンバーの関連実績（抜粋）

XXXXXXX （統括チーム）	・**脆弱性診断**、**Webアプリケーション/モバイルアプリケーションテスト**、機器設定値レビュー ・**自動車セキュリティ脆弱性評価**のガイドライン作成及び評価実施 ・企業や組織向け情報セキュリティポリシー、スタンダード、プロシージャ、セキュリティ設定ベースラインの作成 ・**ペネトレーションテスター技術者育成研修**の講師及び研修資料の作成
YYYYYYY （チームA）	・**脆弱性診断**、**Webアプリケーションテスト**、機器設定値レビュー ・**自動車セキュリティ脆弱性評価**のガイドライン作成及び評価実施 ・企業向け情報セキュリティポリシー、スタンダード、プロシージャ、セキュリティ設定ベースラインの作成
ZZZZZZZ （チームB）	・車載マイコンにおける**セキュリティ回路の設計および検証** ・**自動車セキュリティ脆弱性評価**の方法論開発およびガイドライン作成 ・**自動車セキュリティ脆弱性評価**におけるリスク分析およびリスク評価

参加企業募集に向けた依頼事項

4月末に参加表明を頂き、7月末までに契約締結のうえ、評価を開始しますので、ご協力をお願い致します

実証実験における各プロセスと企業様ご対応事項



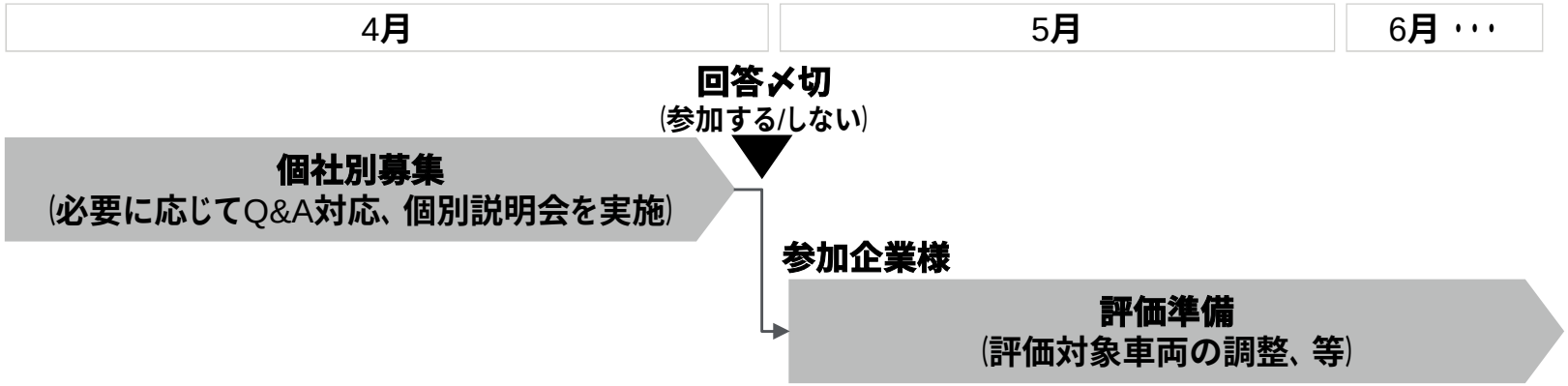
※ 上記は最も効率的な進捗を想定したスケジュールであり、実際には個別に調整のうえ、各対応を進めさせて頂きます。

エントリー頂いた参加企業から順次契約手続き等の準備を行い、評価を開始します

参加企業募集プロセスおよび評価開始時期

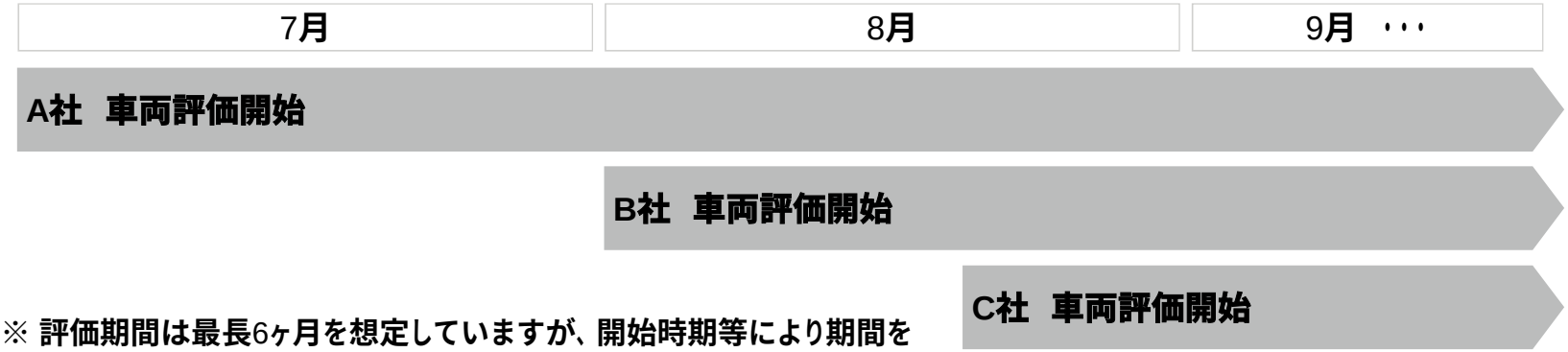
参加者募集プロセス

■ 4月上旬に各社に個別に参加エントリーの依頼の連絡を行い、4月末までにエントリーのご回答を頂きます。



評価開始時期

■ 評価準備 (詳細は後述) が終った参加企業様から順次車両評価を開始します。



※ 評価期間は最長6ヶ月を想定していますが、開始時期等により期間を短くする必要がある場合は、評価対象の数を調整することで対応します

評価対象車両のご提供および評価環境の準備にあたり、以下をお願い致します

評価対象車両および評価環境に関わる依頼事項 (1/2)

以下は現時点の想定であり、具体的な内容は各社エントリー後に個別に調整させて頂きますのでよろしくお願い致します

■ 評価対象車両のご提供に関して

車両の要件	少なくとも以下のうちいずれかの外部通信機能を持つシステムをご準備ください。 Wi-Fi、 Bluetooth、 3G/4G/LTE
車両の種別	評価対象車両は**開発車または市販車**を想定しています。
車両の提供形態	**車両そのもの**の提供が難しい場合は、**車両ベンチ (部品システム)** でも構いません。 ただし、上記「車両の要件」を満たし、無線区間のテストができるシステムである必要があります。
提供期間	**6ヶ月間**を想定しています。 (評価作業そのものは評価対象1台あたり2～3か月程度を見込んでおりますが、複数の評価対象車両を並行して評価を進めるため、余裕を見て6ヶ月間ご提供頂きたく考えております。より短期間のご提供をご希望する場合は、個別にご調整させて頂きます。)
予備部品	評価対象車両1台に加え、当該車両に関わる**予備部品 (評価に必要となるヘッドユニット等を含む部品システム) ***のご用意をお願い致します。 * 少なくとも1台のご用意をお願いします。2台以上ご用意頂けるとより深い評価が可能になります。

評価対象車両のご提供および評価環境の準備にあたり、以下をお願い致します

評価対象車両および評価環境に関わる依頼事項 (2/2)

以下は現時点の想定であり、具体的な内容は各社エントリー後に個別に調整させて頂きますのでよろしくお願い致します

■ 評価対象車両のご提供に関して (続き)

保守サポート	評価環境構築時および評価実施中の評価車両に関する**問題発生時のサポート体制**をご準備願います (具体的には担当窓口の設置と、必要な部品サプライヤーとの連携、等を想定)。
車両提供に係る費用	**車両提供に係る費用 (車両そのものおよび運送費、予備部品を想定) は各参加企業様に負担して頂きます**。 その他関連費用 (マニュアル、等) については当社が負担致します。
車両返却時の状態	車両返却時には、評価により破損している恐れがありますのでご了承願います。

■ 評価環境の準備に関して

外部通信環境	テレマティクスで必要になる**通信サービスおよびサーバー側**のご用意をお願いします。 サーバーは検証用サーバー等の**テスト環境**でお願いします。(併せてテスト用アカウントをご用意願います) また、車両出荷前に車両との開通テストを済ませておいて頂けると助かります。
情報提供	車両に関する一般ユーザーが手に入る範囲の情報として、**ユーザーマニュアルやサービスマニュアル**もご用意頂けると助かります (費用は当社負担とします)。
承諾	覚書または秘密保持契約書、確認書等 (後述) の取り交わしを通じて、車両およびサーバーにサイバー攻撃による評価を実施することについてご承諾を頂きます。

車両評価の開始までに、必要な契約書類を取り交わします

実証実験参加に必要な契約書類（抜粋）

■ 秘密保持契約

- 秘密情報の厳密に管理することに加え、開示範囲等を明記します。
- 評価結果および評価項目の開示範囲については、20ページを参照ください。

秘密保持契約 雛型案（イメージ）

（秘密保持）
秘密情報（結果等）の第三者への開示・漏洩の禁止、目的以外の使用禁止、諒解の下に第三者に開示する場合の条件、再開示先等

（情報の利用および開示）
適法に利用/開示できる権利を保障すること　等

（期間）
契約期間、秘密情報の返却・破棄の条件、滅失または毀損時の対応　等

（協議）
契約外の事項等について協議すること　等
・・・

■ 評価車両提供にあたっての覚書

- 評価車両をご提供頂くにあたって、車両の要件や提供期間、等の取り決め事項について明記します。

車両提供に関わる覚書 雛型案（イメージ）

（目的と提供期間、場所）
車両提供の目的と期間、車両を使用する場所、等

（貸与車両）
提供頂く車両の要件（外部通信機能、車両の種別や提供形態等）、予備部品、評価に必要な通信サービス　等

（貸与車両の引き渡し）
車両提供の時期、仕方（輸送）、提供場所　等

（貸与車両の返却）
車両返却の時期、仕方（輸送）、返却時の車両の状態　等

（禁止事項）
評価車両の第三者提供の禁止、所定の使用場所以外での使用等
・・・

※ 各契約書類の雛型は予め用意しますが、参加企業様でお持ちの雛型を活用することも可能です。具体的な内容は締結時に個別に調整させて頂きます。
※ 上記の他、必要に応じて通信サービス契約等の締結を予定しています。

実証実験における車両評価について

実行性および利便性の高いアプローチを採用した評価ガイドラインに基づき、車両評価を行い、その内容を検証します

情報セキュリティ評価ガイドラインドラフトのポイント

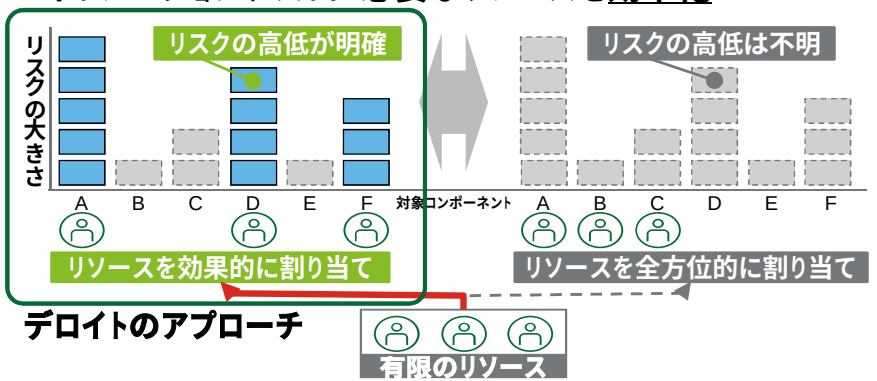
実行性が高いガイドライン

■ **各種ベストプラクティスに準拠しています**

1. ペネトレーションテストが浸透するITシステム分野において実質的な業界標準として扱われているガイドラインや方法論を考慮
   - NIST (Technical Guide to Information Security Testing and Assessment)
   - PCI Security Standards Council (Penetration Testing Guidance)
   - OWASP (Risk Rating Methodology)
2. 自動車のペネトレーションテストに係るデロイトの方法論を活用
   - OEMでの採用実績もあり、セキュリティ評価における各種課題が実証済み

■ **攻撃者視点によるリスクアプローチを採用しています**

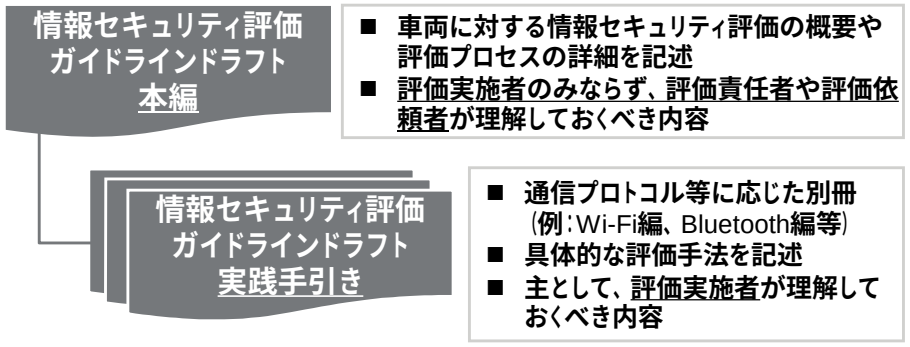
1. 攻撃者の目線でリスクの高いコンポーネントに絞り込むことで、ペネトレーションテストに必要なリソースを効率化



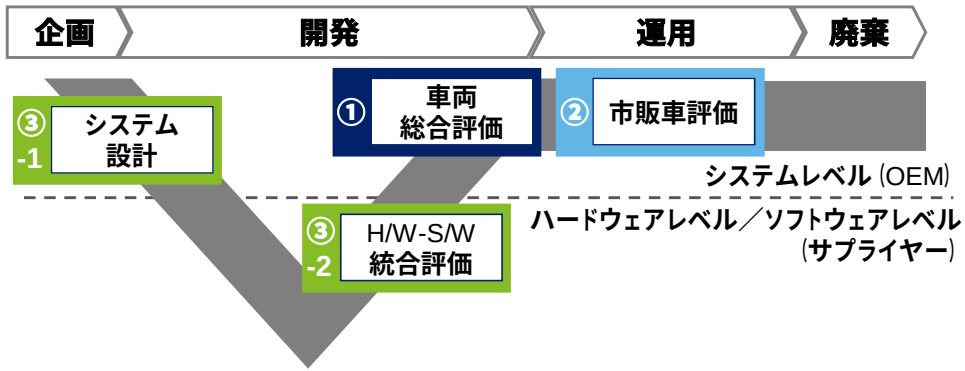
利便性が高いガイドライン

■ **システム全体視点の構成としています**

1. 開発車や市販車単体に加え、これらに繋がるシステム全体の最終責任者が考慮すべき視点を含むべく、「本編」と「実践手引き」の2階層で構成



2. V字プロセスにおける各工程での活用が期待可



想定される攻撃者、攻撃対象コンポーネントを整理してからテストを行います

車両評価の流れ（評価ガイドラインドラフトより）

※吹き出しは参加企業様のご対応事項

	評価の流れ	概要	
テスト実施前の評価プロセス	1 事前準備	参加企業様との間で各種取り決め事項を調整	評価車両のご提供および評価環境の準備のご協力（詳細は前述）
	2 想定される攻撃者の整理	評価対象を攻撃する可能性のある攻撃者を推定し、攻撃者をプロファイル	■ 机上分析にて、評価対象のスコープを明確化 ■ ここで評価対象を調整することで評価期間を短縮可能
	3 攻撃対象コンポーネントの特定	攻撃者の標的となり得る機能（情報）を特定のうえ、当該機能を構成するコンポーネントとマッピングし、攻撃者の標的となり得るコンポーネントを特定	
	4 車両個別のリスク分析	攻撃者ファクター、脆弱性ファクター、影響度ファクターからコンポーネントリスクを評価	
	5 評価計画の立案	テスト対象範囲の決定のうえ、対象のコンポーネントに対する詳細な技術的分析を行い、評価計画を作成	
テスト実施	6 テストの実施	評価計画に従いテストを実施	立ち合い（ご希望の場合に別途調整）
テスト実施後の評価プロセス	7 リスクマッピング	テストで発見された脆弱性に対してリスク評価を実施	■ 発見事項をリスク評価により重み付け
	8 改善案および残存リスクの整理	リスク評価の結果から、リスクに対する対処を明確化し、対処実施後の残存リスクを整理	評価結果のご確認と開示可否の判断

テストによって発見された事項、想定されるリスク等を整理し、改善の方向性や残存リスクを記載した評価レポートを作成します

評価レポートのイメージ

目次案

1. 全体要約
- 1.1. 評価の目的
- 1.2. 評価対象
- 1.3. 評価の実施
- 1.4. 発見事項に対するリスク評価
- 1.5. 主な発見事項
- 1.6. 総括

2. 評価詳細説明
- 2.1. 評価条件
- 2.2. 評価体制
- 2.3. 評価方法

3. 評価結果
- 3.1. ペネトレーションテストによって発見された脆弱性に対するリスク評価（リスクマッピング）
- 3.2. 個別発見事項
- 3.3. 個別評価結果

別紙A. ハードウェアハッキングとリバースエンジニアリング
別紙B. 個別評価結果詳細

内容イメージ（一部抜粋）

No.	XX
発見事項	※※※※※※※※※※※※※※※※※※※※
全体のリスク	※※※※※※※※※※※※※※※※※※※※ ※※※※※※※※※※※※※※※※※※※※
影響を受けるコンポーネント	※※※※※※※※※ ※※※※※※※※※
影響を受けるバス	※※※※※※※※※※
脆弱性の説明	※※※※※※※※※※※※※※※※※※※※ ※※※※※※※※
想定されるリスク	※※※※※※※※※※※※※※※※※※※※
改善の方向性	※※※※※※※※※※※※※※※※※※※※ ※※
残存リスク	※※※※※※※※※※※※※※
関連する評価結果	※※※※※※※※※※※※※※※※※※※※
備考	※※※※※※※※

Illustrative

評価項目分類	評価手法	結果概要	結果詳細	発見事項
※※※※※	※※※※※※※※ ※※※※※※※	※※※※※※※※ ※※※	XX	なし
※※※※※	※※※※※※※※ ※※	※※※※※※※※ ※※※※※※※※	XX	XXXX
※※※※※※※	※※※※※※※	※※※※※※※※※	XX	なし
・・・	・・・	・・・	・・・	・・・

Illustrative

情報の機密管理について

実証実験において取り扱う情報に大変機微なものが含まれることを踏まえ、その機密管理を徹底します

情報セキュリティ管理体制について

海外法人との連携時の情報の海外流出を防ぐ機密管理

下記により、海外メンバーからの機密情報の流出を防ぎます。

①海外のチームメンバーが知りうる情報の最小限化

下記にて、海外メンバーが本プロジェクトで知りうる情報は最小限に抑えます。

- 評価は日本国内でのみ実施する
- 海外メンバーは、アドバイザーとしての関与であり、評価作業を直接実施しない
  （海外メンバーへは、ノウハウや知見の提供に必要な情報のみを提供）

そのうえで

②契約により海外のチームメンバーからの対外情報流出を防止

海外メンバーが本プロジェクトで知り得た機密情報は、日本と当該海外法人との契約における秘密保持条項により、機密保持を担保します。

参加企業間の評価に関わる情報のセキュリティ確保

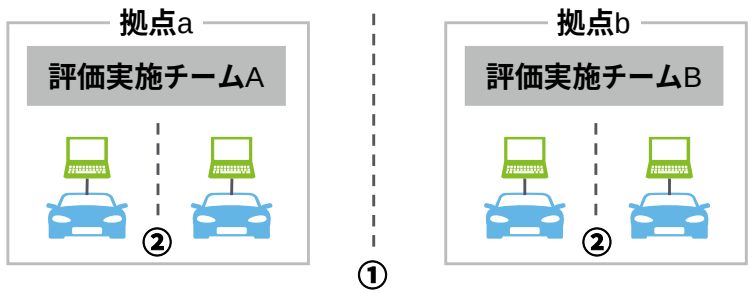
評価環境を物理的に分けることでセキュリティを確保します。

①評価拠点による物理的隔離

評価実施は2つの拠点（それぞれの別の評価実施チームが評価を実施する体制）とし、かつ拠点間の評価車両の移動は行わないことにより、拠点間でのセキュリティを確保

②テスト実施環境の物理的隔離

同一拠点で複数の評価車両を評価する場合において、テスト実施環境（評価で使用するPC等）を物理的に分けることでセキュリティを確保



上記に加え、当社では情報セキュリティ管理に関わる国際標準であるISO/IEC27001の認証を取得したうえで、当基準に則った情報管理を徹底しており（21ページ参照）、本プロジェクトにおいても十分な機密管理を行います。

車両毎の評価結果および評価項目/手順の開示は、各参加企業様個社に限定します

評価結果の開示範囲

■ 車両固有の評価結果については、各参加企業様やNEDO様と締結する秘密保持契約に基づき各参加企業様に限定して開示します。

凡例 ○ ： 開示する
× ： 開示しない

情報分類		開示範囲		
		評価車両の提供者 (各参加企業様)	実証実験事務局 (NEDO様)	公表 (ガイドライン等に記載)
1	車両毎の評価結果	○	×	×
2	車両毎の評価項目/手順	○	△*2	×
3	統計化*1した評価結果	○	○	○
4	汎用化した評価項目/手順	○	○	○

*1 「統計化」とは、複数の車両の評価データをその性質や傾向を数量的に把握するために整理することを言い、「統計化」によって作られたデータからは参加企業様が特定できないものとなります。

*2 参加企業様からの許諾を頂いた範囲内での開示となります。

評価結果等の機密情報は、ISO/IEC27001に則り厳重に管理、運用します

情報セキュリティ管理体制について

- 機密として扱うべき評価結果情報等について、必要なセキュリティ管理を実施するため、責任者を明確にした管理体制及び方法（各作業の情報取り扱いフロー/ルールなど）を確立します。
- なお、デロイトではデロイト トーマツグループ全体でISO/IEC27001の認証を取得しており、これにより、情報セキュリティ管理体制がISO/IEC27001に適合したものであると対外的に認められております。（下記URLの案内参照）

  https://www2.deloitte.com/jp/ja/pages/about-deloitte/articles/about-deloitte-japan/ISO27001.html
- デロイトでは、取扱う情報の重要性を十分に認識したうえで、上記に基づき構築した、情報セキュリティに関連する社内規程の整備・運用、教育、物理的セキュリティ対策の強化、情報テクノロジーによるセキュリティ強化及び、それら施策に対する内部監査の実施といった情報セキュリティ管理体制により、本業務を推進します。

別紙 3

秘密保持契約　雛型（案）

XXX（以下、甲という。）と YYY（以下、乙という。）とは、両者間で「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」の実施検討及び情報交換（以下、本件検討という。）を行うにあたり、次のとおり契約を締結する。

第 1 条　（秘密保持）

第1項　甲および乙は、相手方から本件検討のために、秘密である旨を表示した文書もしくはその他の有形の媒体によって開示された情報（甲から乙に貸与される貸与試作品を含む。）および口頭もしくは視覚的手段などによる開示後 30 日以内にその内容を文書に取りまとめ秘密である旨を表示して通知された情報（総称して、以下、秘密情報という。）を、相手方の事前の文書による了解を得ない限り、第三者に開示・漏洩してはならず、本件検討以外の目的に使用してはならない。

第2項　前項の規定は、次の情報には適用しない。

（ア）　相手方から開示を受けた時すでに公知であった情報

（イ）　相手方から開示を受けた後に自らの責によらず公知となった情報

（ウ）　相手方から開示を受けた時すでに自ら所有していたことを証明できる情報

（エ）　第三者から秘密保持義務を負うことなく適法に取得したことを証明できる情報

（オ）　相手方から開示された情報によることなく独自に開発・取得したことを証明できる情報

第3項　甲および乙は、本件検討の存在・内容・結果（乙から甲に提供される評価結果を含む。）を、相手方の事前の文書による了解を得ない限り、第三者に開示・漏洩してはならない。

第4項　甲および乙は、本条第１項に基づく相手方の了解下で相手方の秘密情報を第三者に開示する場合には、自らの責任で、自らがこの契約で負担する全ての義務と同等の義務を当該第三者に負担させなければならない。

第5項　甲は、乙が、会社 A（住所 A）、会社 B（住所 B）および会社 C（住所 C）（以下、総称して再開示先という。）に対して、本件検討に必要な範囲に限り、甲の秘密情報および本件検討の存在・内容・結果を開示することを了解する。但し、乙は、自らの責任で自らがこの契約で負担する全ての義務と同等の義務を再開示先に負担させなければならない。

第 2 条　（情報の利用および開示）

第1項　甲および乙は、本件検討において自ら利用しまたは相手方に開示する情報について、当該情報を不正競争防止法等に照らし適法に利用しまたは開示できる正当な権利があることを相手方に保証する。

第 3 条　（期間）

第1項　この契約は、2018 年 MM 月 DD 日から 201Y 年 MM 月 DD 日まで有効とする。なお、本件検討の結果、甲乙共同にて開発等を行うことで合意した場合、速やかに適切な契約を別途締結するものとする。

第2項　甲および乙は、相手方から要求がある場合には、相手方の指示に従い速やかに相手方から受領した秘密情報をその写しも含め、返却または廃棄するものとする。ただし、乙から甲に提供される評価結果の取扱いについては、甲乙間で別途協議し決定するものとする。なお、本項は、乙の法令遵守および業務管理上必要とされる保管を妨げない。

第3項　乙は、試作貸与品を滅失または毀損等した場合には、ただちに甲に報告するとともに、代替品の貸与を含めその後の取り扱いについて甲乙間で協議し決定する。なお、乙は、甲の責に帰すべき事由による場合を除き、当該滅失または毀損等により甲に生じた損害を賠償するものとする。

第4項　本条第１項の規定にもかかわらず、第１条の規定はこの契約終了後も 10 年間有効とする。但し、甲乙間で別途協議の上その取り扱いを定めた情報については、その定めに従う。

第 4 条　（協議）

第1項　甲および乙は、この契約に定めない事項およびこの契約の各条項に関する疑義については、誠意をもって協議して解決する。

この契約締結の証として本書 2 通を作成し、両当事者記名・捺印のうえ各 1 通を保有する。

2018 年 MM 月 DD 日

甲：　住所
　　社名
　　部門　役職
　　氏名

乙：　住所
　　社名
　　部門　役職
　　氏名

別紙 4

覚書　雛型（案）

XXX（以下、「甲」という。）と YYY（以下、「乙」という。）とは、両者間で「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」における車両システム侵入テストに参加するにあたり、評価対象車両の提供及び評価環境について以下のとおり合意する。

第 1 条　（覚書の目的）

第1項　甲は、車両システム侵入テストに参加するにあたり、使用する評価対象車両（以下「車両」という）を乙に無償にて貸与し、乙はこれを借り受ける。

第2項　本覚書の貸与期間（以下「貸与期間」という）は、2018 年 MM 月 DD 日より 201Y 年 MM 月 DD 日までとする。

第 2 条　（貸与車両）

第1項　甲が貸与する車両は少なくとも下記各号のいずれかの外部通信機能を持つシステムを備えている。

（1号）　Wi-Fi

（2号）　Bluetooth

（3号）　3G/4G/LTE

第2項　甲が貸与する車両は開発車または市販車とする。ただし、車両の貸与が出来ない場合は、車両ベンチ（部品システム）をもって代替することとするが、前項を満たさなければならない。

第3項　甲は、車両 1 台に加え、車両に関わる予備部品（評価に必要となるヘッドユニット等を含む部品システム）を提供する。

第4項　甲は、評価環境構築時及び評価実施中の車両に関して、問題発生時のサポート体制（担当窓口の設置、部品サプライヤーとの連携等）を整備する。

第5項　甲は、車両の提供に係る費用（車両、予備部品、往復の運送費、等）を負担する。その他関連費用（ユーザマニュアル、サービスマニュアル等）は乙が負担する。

第6項　車両システム侵入テストに起因し、車両または車両ベンチが故障または破損した場合の修繕のための費用は、甲の負担とする。

第7項　甲は、テレマティクスで必要になる車両の通信サービスを開通し、乙に引き渡すものとする。甲は、車両の引き渡し時に、通信が可能な状態とし、テレマティクスサービスに必要となる情報（ユーザ ID、パスワード等）を提供する。

第8項　車両の通信先となるサーバーは、本番環境と同等のテスト環境とする。

第9項　車両システム侵入テストに起因し、サーバーに不具合が生じた場合、乙は復旧、

修繕及びそれらに掛かる費用負担の責は負わないものとする。

第 3 条　（車両の引渡し）

第1項　甲は、第 1 条、第 2 項に規定する貸与開始時期までに車両を後記表示の使用場所で乙に引き渡すものとする。

第 4 条　（使用目的）

第1項　乙は、車両を「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」における車両システム侵入テストのため（以下「本目的」という）にのみ使用し、本目的以外のために車両を使用しない。

第 5 条　（善管注意義務）

第1項　乙は、車両を善良なる管理者の注意義務をもって管理するものとする。

第 6 条　（点検義務）

第1項　乙は、車両の引渡し後直ちに及び貸与期間中、定期的に車両の点検を行うものとする。

第2項　乙は、貸与期間中に車両の瑕疵を発見した場合は直ちに甲に書面にて通知するものとする。

第3項　乙が本条、第 1 項の点検及び前項の通知を行わなかった場合、車両の瑕疵により乙または第三者に損害が生じても、甲は賠償の責を負わない。

第 7 条　（表示等）

第1項　乙は、自己の物との混同を避けるため、車両を、自己の所有物ではないことがわかるように明確に表示して使用する。

第2項　乙は、甲の要求があるときはいつにても車両に甲の指定するタグ、プレート等を貼付するものとする。

第 8 条　（禁止事項）

第1項　乙は、下記各号に規定する行為を行ってはならない。

（1号）　車両の第三者に対する譲渡、賃貸、または担保供与

（2号）　後記表示の使用場所以外での車両の使用

第 9 条　（転貸借）

第1項　乙は、甲の書面による承諾を得たうえで第三者に貸与した場合においても、貸

借人としての責務を免れない。

第 10 条　（報告義務）

第1項　甲は、車両の使用状況について、いつにても乙に書面その他の方法による報告を求めることができる。

第2項　乙は、本覚書第 1 条、第 2 項に規定する貸与期間中に第三者より車両の所有権または占有権を主張された場合には速やかに甲に通知するものとする。

第 11 条　（返還）

第1項　貸与期間の満了または合意の解除により本覚書が終了した場合、乙は直ちに車両を返還する。

第 12 条　（合意解除）

第1項　甲乙の一方が下記各号の一つに該当するときは、その相手方は当該当事者に対し、何等通知催告を要することなく本覚書での合意の全部又は一部を解除することができるものとする。

（1号）　本覚書の条項の一つでも違反したとき

（2号）　差押、仮差押、仮処分、租税滞納処分等を受け、または破産、民事再生、会社更生、特別清算等の申立をなし、またはこれを受けたとき、もしくは競売の申立を受けたとき

（3号）　監督官庁より営業停止または営業免許もしくは営業登録の取消の処分を受けたとき

（4号）　資本減少、営業の廃止または合併によらず解散の決議をしたとき

（5号）　支払停止、支払不能もしくは自ら振出し、または引受けた手形、小切手につき不渡りとなったとき

（6号）　その他財産状態が悪化しまたはそのおそれがあると認められたとき

（7号）　暴力団、暴力団員、暴力団に関係する団体・個人、その他の反社会的勢力（以下総称して「反社会的勢力」という）に該当し、主たる出資者もしくは役職員が反社会的勢力と取引その他の関係を有し、または暴力・威力・詐欺的手段を用いて信用の毀損、業務の妨害、もしくは不当な要求をしたとき

第2項　前項により本覚書に規定する合意の解除をした当事者は、これにより生じた損害がある場合には相手方に対し、その賠償の請求をすることができるものとする。

第3項　第１項各号に規定する事由以外の貸与期間中の解除は不可とする。

第4項　前項の規定に拘らず、乙の責めに帰することができない事由により、「情報セキュリティ実証実験」が延期または中止となった場合、乙は、本覚書を解除することができる。

第 13 条　（合意管轄）

第1項　本覚書又はその他の諸契約より生ずる権利義務に関する争訟については、東京地方裁判所をもって第一審の専属管轄裁判所とする。

第 14 条　（協議）

第1項　本覚書に規定のない事項または本覚書の各条項に疑義が生じた場合、甲乙誠意をもって協議のうえ解決する。

第 15 条　（覚書の変更）

第1項　本覚書の変更はすべて文書をもって行うものとし、甲乙双方の署名または記名押印を必要とするものとする。

第 16 条　（不可抗力）

第1項　本覚書は、天災、地変その他甲乙双方の責に帰することができない事由により、車両が毀損、滅失し、これにより本覚書での合意事項を継続することが不可能又は困難となった場合、本覚書は当然に消滅する。この場合、甲及び乙は、相手方に生じた損害につき責任を負わないものとする。

以上の合意を証するため、本覚書を 2 通作成し、甲乙記名捺印のうえ各 1 通を保有する。

2018 年 MM 月 DD 日

甲　住所
会社名
役職　氏名

乙　住所
会社名
役職　氏名

記

＜貸与目録＞

車両 XXXX　1 **台**

＜納品・使用場所＞

XXXXXXXXXXX