

令和 7 年度  
安全設計・評価プロセスガイド  
(RoAD to the L4)

令和 8 年 5 月  
国立研究開発法人 産業技術総合研究所  
一般財団法人 日本自動車研究所

# 目次

## 目次 2

|                                                 |    |
|-------------------------------------------------|----|
| 第 1 章 序章（はじめに） .....                            | 6  |
| 1.1 目的 .....                                    | 6  |
| 1.2 対象範囲.....                                   | 6  |
| 1.3 開発プロセス構築の基本方針 .....                         | 8  |
| 1.3.1 開発プロセスの構成 .....                           | 8  |
| 1.3.2 開発プロセスとプロジェクト運営の関係における留意点 .....           | 9  |
| 1.3.3 関連する標準・基準 .....                           | 10 |
| 1.3.4 リスクの評価.....                               | 11 |
| 1.3.4.1 規格が対象とするリスクの範囲と評価結果の使い道 .....           | 11 |
| 1.3.4.2 リスクの大きさの決め方（S・E・C） .....                | 11 |
| 1.3.4.3 ISO 26262 における ASIL の決定 .....           | 12 |
| 1.4 用語定義.....                                   | 13 |
| 1.4.1 法令・制度上の用語.....                            | 13 |
| 1.4.2 国際規格・技術用語 .....                           | 13 |
| 1.4.3 安全設計に関する主要用語 .....                        | 14 |
| 第 2 章 安全性を確保するための実施事項 .....                     | 15 |
| 2.1 自動運転移動サービスの定義 .....                         | 15 |
| 2.1.1 主な検討項目 .....                              | 15 |
| 2.1.2 走行ルートの選定 .....                            | 15 |
| 2.1.3 自動運転移動サービス全体構成の定義 .....                   | 17 |
| 2.1.4 安全目標の定義 .....                             | 17 |
| 2.2 走行環境条件とユースケースの定義 .....                      | 19 |
| 2.2.1 運行ルートの走行環境分析と記述方法の定義 .....                | 19 |
| 2.2.2 ユースケース（走行環境 + 自車両の進行方向で分類する走行区間）の定義 ..... | 20 |
| 2.3 基本走行戦略の策定 .....                             | 20 |
| 2.3.1 各ユースケースにおいて遵守すべき道路交通法と下位法令等の確認.....       | 21 |
| 2.3.2 各ユースケースにおける基本的な安全確認と走行方法の定義 .....         | 21 |
| 第 3 章 安全性を確保するための実施事項 2 .....                   | 23 |
| 3.1 車両機能の定義.....                                | 23 |
| 3.1.1 システム範囲 .....                              | 23 |
| 3.1.2 自動運行装置に求められる能力 .....                      | 24 |
| 3.1.3 基本機能 .....                                | 26 |
| 3.1.4 機能定義 .....                                | 27 |
| 3.2 リスクシナリオの導出.....                             | 27 |
| 3.2.1 リスクシナリオの考え方 .....                         | 28 |
| 3.2.1.1 交通関連クリティカルシナリオ .....                    | 29 |
| 3.2.1.2 認識関連クリティカルシナリオ .....                    | 31 |

|                                         |    |
|-----------------------------------------|----|
| 3.2.1.3 車両制御関連クリティカルシナリオ .....          | 34 |
| 3.2.1.4 不具合シナリオ .....                   | 35 |
| 3.2.2 シナリオ空間の定義 .....                   | 35 |
| 3.2.3 リスクシナリオの明確化 .....                 | 36 |
| 3.2.3.1 リスク要因の抽出 .....                  | 36 |
| 3.2.3.2 リスクシナリオの抽出 .....                | 37 |
| 3.2.3.3 リスクの評価 .....                    | 38 |
| 3.3 安全コンセプト .....                       | 38 |
| 3.3.1 センシング .....                       | 39 |
| 3.3.2 リスクシナリオへの対応 .....                 | 40 |
| 3.4 システムへの安全要求の導出 .....                 | 43 |
| 3.4.1 認識要求 .....                        | 44 |
| 3.4.2 予測・判断要求 .....                     | 45 |
| 3.4.3 制御要求 .....                        | 46 |
| 3.4.4 その他要求 .....                       | 46 |
| 第 4 章 実現手段の設計 アーキテクチャ設計（性能実現含む） .....   | 47 |
| 4.1 基本システム設計 .....                      | 47 |
| 4.1.1 基本方針 .....                        | 47 |
| 4.1.2 認識機能の設計 .....                     | 47 |
| 4.1.3 計算プラットフォームの設計 .....               | 48 |
| 4.1.4 車両・アクチュエータ（ACT）性能の設計（制御実現性） ..... | 48 |
| 4.1.5 運用シナリオと外部連携 .....                 | 49 |
| 4.2 SOTIF（性能限界、ミスユースに対する設計） .....       | 49 |
| 4.2.1 機能的不十分性及びトリガー条件の識別 .....          | 49 |
| 4.2.2 リスクの評価及び改善方策の適用 .....             | 49 |
| 4.3 機能安全（故障に対する設計） .....                | 49 |
| 4.3.1 システムレベルの安全設計 .....                | 50 |
| 4.3.2 ハードウェア／ソフトウェアによる実装 .....          | 50 |
| 4.4 サイバーセキュリティプロセス（ISO/SAE 21434） ..... | 51 |
| 4.4.1 コンセプトレベルの活動 .....                 | 51 |
| 4.4.2 サイバーセキュリティ仕様の定義と実装 .....          | 51 |
| 4.4.3 検証とサイバーセキュリティ妥当性確認（V&V） .....     | 51 |
| 4.4.4 継続的なサイバーセキュリティ活動 .....            | 51 |
| 第 5 章 安全性評価 .....                       | 52 |
| 5.1 安全性検証及び妥当性確認の考え方 .....              | 52 |
| 5.2 安全性検証（verification） .....           | 53 |
| 5.2.1 コンポーネント・サブシステムレベル .....           | 54 |
| 5.2.2 車両システム・自動運転移動サービスレベル .....        | 54 |
| 5.3 安全妥当性確認（validation） .....           | 54 |
| 5.3.1 コンポーネント・サブシステムレベル .....           | 54 |

|                                               |    |
|-----------------------------------------------|----|
| 5.3.2 移動サービスレベル .....                         | 55 |
| 5.4 シミュレーション、テストコースや実路走行による評価 .....           | 55 |
| 5.4.1 シミュレーション（仮想テスト）による安全性評価 .....           | 55 |
| 5.4.2 テストコースにおける模擬環境での安全性評価 .....             | 55 |
| 5.4.3 実車・実路走行による妥当性確認 .....                   | 56 |
| 5.5 先行開発・一品生産的なプロジェクトでの留意点 .....              | 56 |
| 5.5.1 要求定義や安全目標具体化の難しさ .....                  | 56 |
| 5.5.2 部品やサブシステムの性能把握の難しさ .....                | 57 |
| 5.5.3 開発体制の脆弱さに起因する難しさ .....                  | 57 |
| 5.5.4 拙速な実車・実路走行の実証によるリスク .....               | 57 |
| 第 6 章 ソフトウェアアップデート .....                      | 59 |
| 6.1 ソフトウェアアップデート機能の実装 .....                   | 59 |
| 6.2 使用中のサイバーセキュリティ確保のためのソフトウェアアップデートの実施 ..... | 59 |
| 第 7 章 巻末資料 .....                              | 61 |
| 7.1 編集委員会 構成員名簿 .....                         | 61 |

## 図目次

|                                                            |    |
|------------------------------------------------------------|----|
| 図 1 自動運転移動サービスの構成要素と周辺関係者（例） .....                         | 7  |
| 図 2 自動運転移動サービスの開発プロセス定義（事例） .....                          | 9  |
| 図 3 ルート候補案の絞り込みに当たって必要な 3 つの視点（RTL4 テーマ 4・柏の葉エリアの場合） ..... | 16 |
| 図 4 シャトルルート 1 の概要（RTL4 テーマ 4・柏の葉エリアの場合） .....              | 16 |
| 図 5 循環ルート 6 の概要（RTL4 テーマ 4・柏の葉エリアの場合） .....                | 17 |
| 図 6 走行環境の表現方法 .....                                        | 20 |
| 図 7 走行環境と交通参加者の分析事例 .....                                  | 22 |
| 図 8 自動運転移動サービスの構成要素と周辺関係者（例） - （再掲） .....                  | 24 |
| 図 9 自動運行装置が担う DDT 関連機能の概念整理 .....                          | 28 |
| 図 10 交通シナリオを整理するための主な観点 .....                              | 29 |
| 図 11 交通関連クリティカルシナリオの考え方 .....                              | 30 |
| 図 12 道路形状と自車両行動の対応関係の整理 .....                              | 30 |
| 図 13 周囲の対象物の位置と動作方向 .....                                  | 31 |
| 図 14 認識シナリオを整理するための主な観点 .....                              | 31 |
| 図 15 死角関連リスク要因の整理観点 .....                                  | 32 |
| 図 16 道路構造要素の分類 .....                                       | 33 |
| 図 17 車両運動シナリオを整理するための主な観点 .....                            | 34 |
| 図 18 シナリオ空間とリスクシナリオ .....                                  | 36 |
| 図 19 リスクシナリオ明確化の手順 .....                                   | 36 |
| 図 20 信号のある交差点右折中の操舵機能故障 .....                              | 38 |

|                                          |    |
|------------------------------------------|----|
| 図 21 システムの構成例 .....                      | 47 |
| 図 22 センサの構成例 .....                       | 48 |
| 図 23 ホットスタンバイを用いた動的冗長構成 .....            | 50 |
| 図 24 自動運転移動サービスの構成要素と周辺関係者（例） - 再掲 ..... | 53 |
| 図 25 自動運転移動サービスの開発プロセス定義（事例） - 再掲 .....  | 53 |

## 表目次

|                                                     |    |
|-----------------------------------------------------|----|
| 表 1 各構成要素の機能概要 .....                                | 7  |
| 表 2 ASIL（自動車用安全度水準） .....                           | 13 |
| 表 3 車両機能の定義からシステムへの要求導出までのプロセス .....                | 23 |
| 表 4 期待される能力と必要な機能の例 .....                           | 25 |
| 表 5 基本的な応答行動の例 .....                                | 26 |
| 表 6 DDT 機能と対応するシナリオ及び外乱 .....                       | 29 |
| 表 7 シミュレーションと、テストコース評価、実路での実車試験に関する PROS、CONS ..... | 56 |

# 第1章 序章（はじめに）

## 1.1 目的

本書は、道路交通法に基づく特定自動運行の許可及び実施を目指す事業者等を主な対象とし、その安全性の確保に係る設計、評価及び申請準備を、確実かつ効率的に進めるための開発プロセスについて解説するものである。

特定自動運行の許可取得に当たっては、関係法令、関係基準及び公的資料に基づき、自動運行装置の使用条件、走行ルート、運行体制その他の事項を具体化し、安全性を説明できるようにしておく必要がある。しかし、これらを実装（設計・評価）レベルでどのような工程と成果物に落とし込むかは、事業の内容、対象地域、車両、運行形態等に応じて整理する必要がある。従って、プロジェクト実施者自らが開発プロセスを定義し、概念設計から運用・保守までの工程を連続的に結び付け、システムの責任範囲と判断のあり方を明確にし、関連する国際規格に整合した評価手法とセーフティケースによる立証を通じて、特定自動運行に必要な安全性を説明できるようにする必要がある。本書は、関係者が開発プロセスについて理解を深めるための参考書として一連の実施項目、実施方法、注意点、実施事例などを解説する。

## 1.2 対象範囲

本書は、特定自動運行の許可取得及び実施を目指す事業において用いられる自動運行装置の安全設計・評価を対象範囲とする。

本書では、自動運行装置を主対象として安全設計・評価プロセスを解説する。必要に応じて、車内安全、遠隔監視・支援、運用・保守、インフラ連携等<sup>1</sup>、自動運転移動サービスを構成する要素についても取り上げる。参考として、主な構成要素及び周辺関係者の例を「図 1 自動運転移動サービスの構成要素と周辺関係者（例）」に、各構成要素の機能概要を「表 1 各構成要素の機能概要」に示す。

これらの構成要素全体が特定自動運行の安全に関係するが、本書では、自動運行装置を中心とした電子制御システム開発業務にフォーカスする。ただし、電子制御システムを構成する個々のコンポーネントやソフトウェア開発などの競争領域に関する記述は必要最小限に留め、電子制御システム開発において関係者が取り組むべき協調領域の技術的な専門知識を一般的に解説するものである。

なお、特定自動運行に必要な安全性の確保に当たっては、車両に備えられた自動運行装置単体によって運行の安全性を確保することを前提としつつ、信号機の設置や歩車分離など道路及び交通安全施設（交通信号機、道路標識、区画線及び道路標示等）の整備、インフラから提供される情報の活用、周囲の交通参加者の理解を促進させる取組等を合わせて検討することを基本とする。ただし、車内安全システム、遠隔監視・支援システム、インフラ（道路設備）、運用・保守システム、インフラ協調システム、車車間協調システム等については、現時点で用途や仕様の特定が難しいため、本書での解説は自動運行装置及びこれと安全上の関係が深い必要最小限の周辺要素に

---

<sup>1</sup> 技術の進展や運用形態の変化により、同一の目的に対する実装手段が変化し得るとともに、構成要素が追加・拡張され得るため、ここでは例示として「等」を付す

留める。これらの詳細については、RoAD to the L4<sup>2</sup>（以下「RTL4」という）テーマ2及びテーマ4の報告書等を参照のこと。

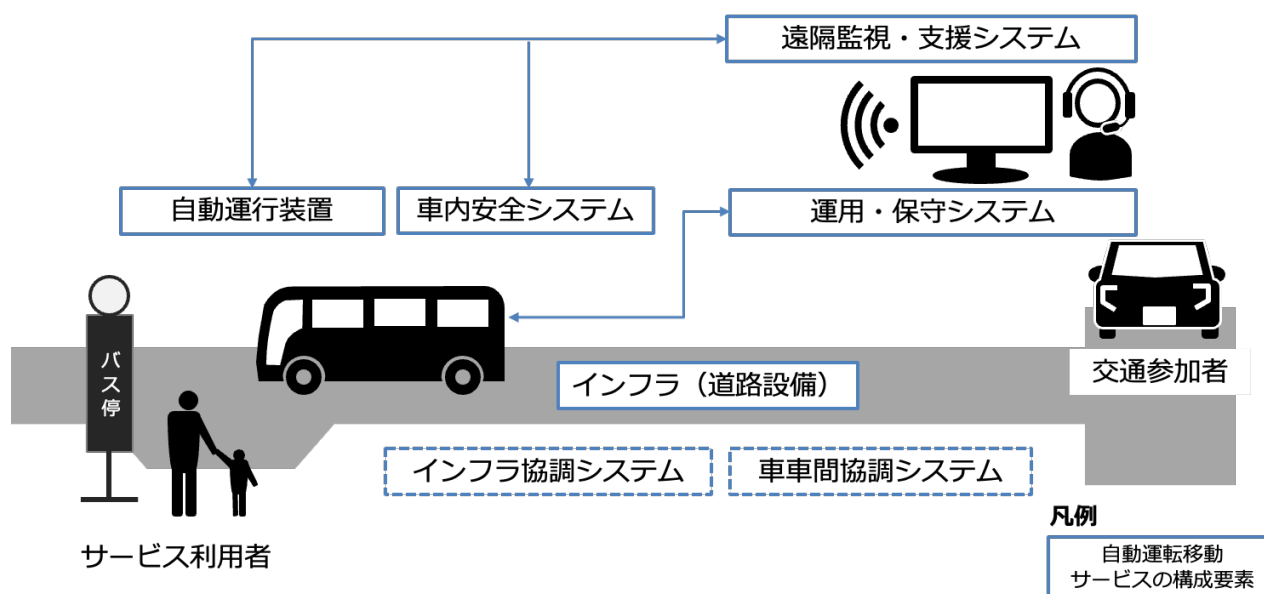


図 1 自動運転移動サービスの構成要素と周辺関係者（例）

表 1 各構成要素の機能概要

| 構成要素        | 機能概要                                                                                                                                           |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| 自動運行装置      | 定められた走行環境条件の範囲内で、周囲環境を認識し、他交通の動きを予測・判断して走行計画を立て、車両を制御（操舵・加減速・制動の指令生成及び実行）する。また、走行環境条件を満たさなくなる場合又は自動運行装置が正常に作動しないおそれがある場合には、安全を確保するために必要な制御を行う。 |
| 車内安全システム    | 乗客・乗務員向け HMI/案内、車内状況監視（転倒・取り残し等）、ドア開閉・挟み込み防止、乗降完了/安全確認（停車・発車連動）、走行/車内ログ記録を行う。                                                                  |
| 遠隔監視・支援システム | 通信を通じて車両の周囲・車内の状況等を遠隔地から監視し、必要に応じて運行の支援を行う。                                                                                                    |
| インフラ（道路設備）  | 磁気マーカ等の走行補助設備、停留所・ゲート等の設備、必要に応じた注意喚起表示など。                                                                                                      |
| 運用・保守システム   | 運行計画・運行管理、始業/定期点検・整備、インシデント対応、変更管理（ソフト更新含む）やサイバーセキュリティ管理等を実施する。                                                                                |
| インフラ協調システム  | 路側センサによって検知された車両の死角に存在する歩行者等の情報や、信号情報を通信で車両に提供する。                                                                                              |
| 車車間協調システム   | V2Vにより周辺車両の状態共有（協調認識・注意喚起等）を行う。                                                                                                                |

<sup>2</sup> <https://www.road-to-the-l4.go.jp>

### 1.3 開発プロセス構築の基本方針

自動運転車に必要な安全を確保するには、概念設計から運用・保守に至るまでの各段階を一貫して管理する開発プロセスの構築及び運用が必要である。本書が採用するプロセス構造は、エンジン、ブレーキ、ステアリング制御といった、極めて高い安全性と信頼性が要求される車載制御システム開発において一般的に採用され、確かな実績を有するものである。ISO 26262 や ISO/TS 5083 において参照モデルとして示されている「V 字型セーフティライフサイクル」の考え方にに基づき、V 字の左側に位置する定義・設計工程と、右側に位置する検証・妥当性確認工程との対応関係を明確化する。

概念設計から運用・保守までの工程を連続的に結び付け、システムの責任範囲と判断のあり方を明確にし、国際規格に整合した評価手法とセーフティケースによる立証を通じて、自動運転車が「Competent & Careful Human Driver」と同等以上の安全性の実現を目指す。

#### 1.3.1 開発プロセスの構成

開発プロセスの具体的な構成について法的な制約など特段の決まりは無いが、後述する国際標準などを参照し、プロジェクトの目標や制約などの個別事情を踏まえて関係者で定義・共有する必要がある。ここでは、RTL4 を推進する中で最終的に得られた知見や経験を基に、参考事例として「図 2 自動運転移動サービスの開発プロセス定義（事例）」に示すようにプロセスを定義し、第 2 章以降で内容を解説する。

参考までに、後述するプロセス構築の考え方や特徴について要点を述べる。

- ✓ (1)では移動サービス提供視点からの要求の具体化、(2)では走行ルートの特性の分析、(3)～(5)では安全走行に必要なシステムへの要求の具体化、(6)では上位工程からの要件を満たすシステム・コンポーネントの設計、(7)～(10)では V 字プロセス左側に対応した検証を実施する工程としている。
- ✓ 走行環境条件の定義や安全設計・評価業務管理のしやすさなどを目的に、走行ルートを走行環境（単路や交差点などの道路構造、信号やガードレール等の有無、制限速度等）に着目して同様の走行環境が続く区間ごとに分割・類型化し、また類型化した区間と自車の進行方向（直進、右折等）を組み合わせたユースケースとして類型化している。
- ✓ 安全設計・評価では、安全目標とその評価方法を定義し目標の達成を確認することが重要である。サービス、システム全体、サブシステムやコンポーネントなどそれぞれの視点から適度な抽象度の安全目標・評価方法を定義する必要があるが、「図 2 自動運転移動サービスの開発プロセス定義（事例）」では記述を省略している。

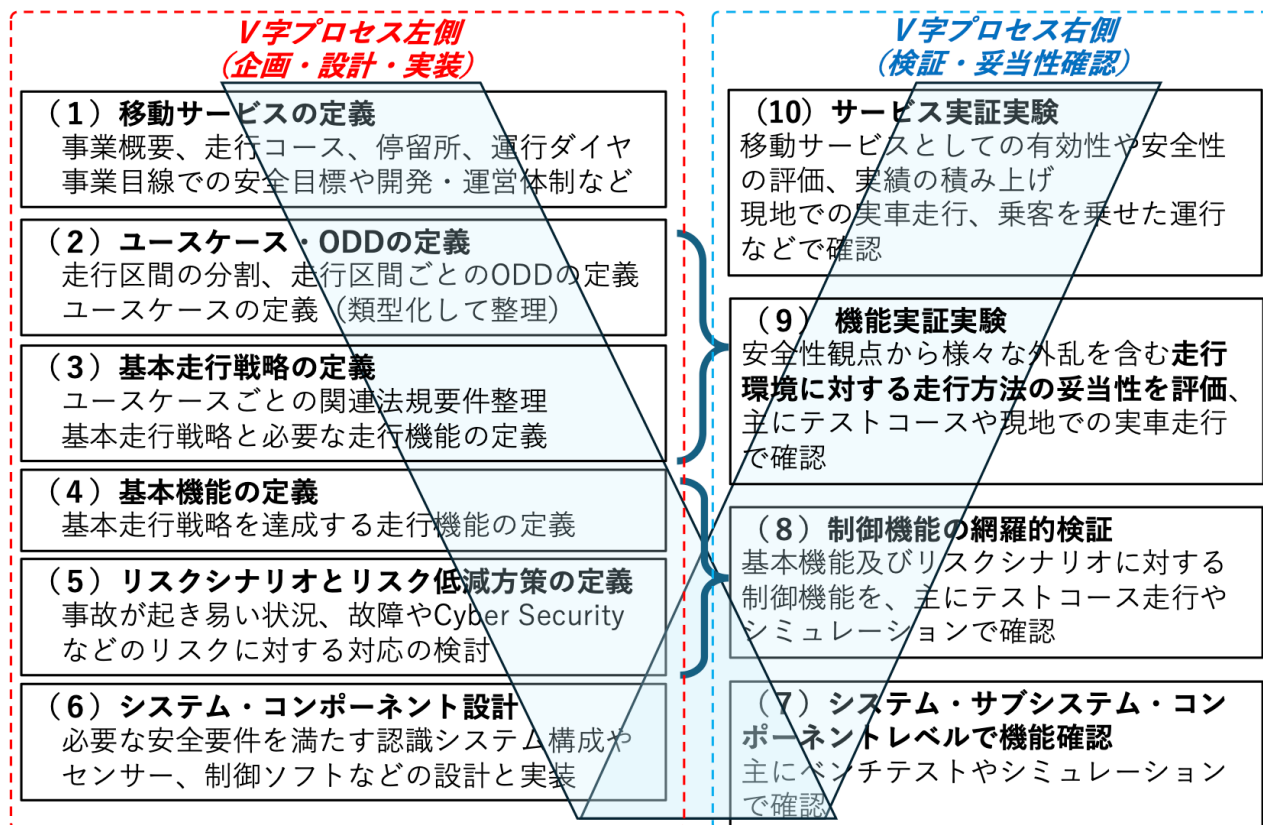


図 2 自動運転移動サービスの開発プロセス定義（事例）

### 1.3.2 開発プロセスとプロジェクト運営の関係における留意点

実際の開発プロジェクトでは、機能確認を目的としたプロトタイプ開発、プロトタイプを用いたサービスの有効性・実用性の検証、検証済みプロトタイプの量産製品化、さらには機能・性能向上や適用地域や用途の拡張を目的とした改良開発など、様々な形態が存在する。また、開発期間や体制、リソースなどの制約条件もプロジェクトごとに大きく異なる。

このため、開発プロセスは目的そのものではなく、プロジェクトの目標や制約条件に応じて最適化すべき手段であることを理解したうえで、柔軟に運用する必要がある。

一方で、基本的な開発プロセスの考え方を理解し、各工程における入力・出力（IN／OUT）や責任範囲を具体化して取り組むことは、目標及び進捗の管理、問題の早期発見に大きく寄与する。これにより、大きな手戻りを防ぎ、結果として開発目標の達成や開発効率の向上につながる点に留意すべきである。

また、前例のない先端的なプロジェクトや少人数体制のプロジェクトでは、複数の工程を同一の組織や担当者が担うケースも少なくない。しかし、そのような場合であっても（むしろそのような場合こそ）、工程を論理的に区分し、それぞれの工程として運用するという意識をプロジェクト全体で共有することが重要である。

なお、開発プロセスを上流から下流へと単純に時系列で進め、上流工程の完了を待って次の工程に着手するものと捉えることは適切ではない。上流工程から下流工程に向けて要求を段階的にブレイクダウンすることは基本かつ重要であるが、実際の開発では、下流工程での検討結果を踏まえて、上流工程で定義した要件の修正や追加が必要

となることも多い。

重要なのは、自工程完結を基本として課題解決に取り組みつつ、問題や検討結果を上下流工程と適切に共有し、プロジェクト全体として柔軟に最適解を求め最適化を図ることにある。

### 1.3.3 関連する標準・基準

自動運転車は今後、国際市場での利用や国際相互承認の枠組みが進むと想定される。このため、国内制度のみならず、国際的な法規や標準などの調和を確保した開発プロセスを構築することが重要である。

なお、ここでいう「基準」とは、国の規制を指すものであり、合致しないと製品などを販売できない規格(UN-R、PSE、PSC 等)である一方、「標準」は業界など任意団体が決めた規格をいい、基本的には義務付けされていないが、政府や地方自治体として標準への適合を義務化していたり、保険適用や調達の条件にしていたりする組織もある。なお、「規格」はその技術的規定と言える。

本書で解説する開発プロセスは、次の標準や法規を主要な参照枠として構成している。

#### 1. 標準

- 自動運転システムの全体フレーム
  - － ISO/TS 5083:2025（自動運転システムの安全）
- 安全設計プロセス
  - － ISO 26262:2018（機能安全）
  - － ISO 21448:2022（SOTIF）
  - － ISO/SAE 21434:2021（サイバーセキュリティ）
- ODD・シナリオ関連
  - － ISO 34501:2022（ADS シナリオ用語）
  - － ISO 34502:2022（シナリオベース安全性評価）
  - － ISO 34503:2023（ODD 仕様・タクソミー）
  - － ISO 34504:2024（シナリオ分類）
  - － ISO 34505:2025（シナリオ評価とテストケース生成）
- 用語体系
  - － ISO/SAE PAS 22736（レベル定義・ADS 用語）
- 安全標準
  - － UL 4600:2020/2023（自律製品の安全性評価）

#### 2. 基準（UNECE）

- － UN R155（サイバーセキュリティ）
- － UN R156（ソフトウェアアップデート）
- － UN R157（ALKS）

国内の自動運行装置の安全性審査においては、個別の国際規格への適合を申請要件として一律に求める形にはなっていないが、将来的に国際的な相互承認にも耐えうる安全論証が可能となるので、積極的に国際規格を参照して安全設計・評価プロセスを推進することが望ましい。

### 1.3.4 リスクの評価

本書で解説するリスク評価の位置付けを理解しやすくするため、ここでは関連する国際規格が想定するリスクの範囲と、評価結果を何に用いるか（何のために評価するか）を概説する。

#### 1.3.4.1 規格が対象とするリスクの範囲と評価結果の使い道

ISO 26262（機能安全）は、安全関連の電気・電子（E/E）システムの誤作動に起因して生じ得るハザードを対象とする。概念段階でハザード分析とリスク評価（HARA）を行い、シビアリティ（S）、遭遇確率（E）、コントローラビリティ（C）の3指標からASIL（Automotive Safety Integrity Level：自動車用安全度水準）（A～D 又は QM）を決定する。

ASIL は、当該ハザードに対して要求される安全要求の強度及び開発・検証の厳格度を定めるためのリスククラスである。ASIL A～D に分類された場合、リスク低減のための車両側対策が求められる。一方、品質管理プロセスで十分に管理可能と判断される場合は QM として扱い、追加の安全対策は不要とみなす。

ISO 21448（SOTIF）は、故障ではなく、意図した機能の不十分さ（性能限界、認識誤り、誤使用等）に起因する危険を対象とする。目標は不合理なリスクの不在であり、設計の見直し、検証・妥当性確認（V&V）、運用上の措置などにより残存リスクを低減する枠組みを与える。SOTIF の観点では、一般に  $S > 0$  かつ  $C > 0$  となる危険事象は重大な危害が生じ得ることを示し、リスク評価時点で想定した機能のみではリスク低減が不十分となる可能性がある。このため、当該リスクを回避又は低減するための追加対策（設計・検証・運用措置等）を検討する必要がある。

#### 1.3.4.2 リスクの大きさの決め方（S・E・C）

リスクの大きさは、コントローラビリティ（C）、シビアリティ（S）、遭遇確率（E）の3つの観点でそれぞれクラス分けした上で、各クラス及び組合せを考慮して決定する。以下に各指標の定義とクラスの考え方を示す。

##### コントローラビリティ（C）

コントローラビリティとは、危険事象が発生した際に、自動運転車両やその他関係者がその事象に対処し、危害を回避できる可能性の大きさを評価する指標である。

| クラス | C0                | C1                               | C2                                    | C3                                           |
|-----|-------------------|----------------------------------|---------------------------------------|----------------------------------------------|
| 説明  | 特別な対処不要           | 簡単に対処可能                          | 普通に対処可能                               | 対処が困難<br>又は対処不能                              |
| 例   | 通常の操作・行動で<br>問題なし | 自動運転車両又は他の交通当事者の 99% 超えが危害を回避できる | 自動運転車両又は他の交通当事者の 90% から 99% が危害を回避できる | 自動運転車両又は他の交通当事者の 90% 未満が危害を回避できる、又はなんとか回避できる |

### シビアリティ (S)

シビアリティとは、危険事象が発生した際に生じ得る人への危害の大きさを評価する指標である。

| クラス | S0                                                               | S1                                         | S2                                    | S3                       |
|-----|------------------------------------------------------------------|--------------------------------------------|---------------------------------------|--------------------------|
| 説明  | 傷害なし                                                             | 軽度及び<br>中程度の傷害                             | 重度及び生命を脅かす傷<br>害（生存の可能性あり）            | 生命を脅かす傷害（生存<br>は不確実）、致命傷 |
| 例   | AIS0 <sup>3</sup> 及び AIS 1-6 の確<br>率が 10%未満、又は安全<br>関連とは分類できない損害 | AIS 1-6 の確率が<br>10%以上（及び S2<br>又は S3 ではない） | AIS 3-6 の確率が<br>10%以上<br>（及び S3 ではない） | AIS 5-6 の確率が<br>10%以上    |

### 遭遇確率 (E)

遭遇確率とは、ある危険事象が成立し得る運転状況に、車両が直面する可能性の大きさを評価する指標である。

| クラス  | E0            | E1                                  | E2                              | E3                                | E4                              |
|------|---------------|-------------------------------------|---------------------------------|-----------------------------------|---------------------------------|
| 説明   | 極めて<br>起こりにくい | 非常に<br>低い確率                         | 低い確率                            | 中程度の確率                            | 高い確率                            |
| 時間の例 | 規定なし          | 規定なし                                | 平均動作時間の<br>1%未満                 | 平均動作時間の<br>1～10%                  | 平均動作時間の<br>10%超え                |
| 頻度の例 | 規定なし          | 多くの運転におい<br>て、年に 1 回未満し<br>か発生しない状況 | 多くの運転におい<br>て、年に数回しか発<br>生しない状況 | 平均的な運転にお<br>いて、月に 1 回以上<br>発生する状況 | 平均して、ほとんど<br>すべての運転中に発<br>生する状況 |

#### 1.3.4.3 ISO 26262 における ASIL の決定

ISO 26262 では、C/S/E の評価結果の組合せに基づき、危険事象を QM 又は ASIL A～D に分類する。  
ASIL は危険事象ごとに定められる安全要求の強度レベルであり、ASIL D が最も高い厳格度を要求する。

（ASIL の組合せ表：「表 2 ASIL（自動車用安全度水準）」を参照）

<sup>3</sup> AIS (Abbreviated Injury Scale) : 米国自動車医学振興協会(AAAM)から発表された、外傷の種類と解剖学的重症度を表すコード体系

表 2 ASIL（自動車用安全度水準）

| シビアリティ<br>クラス | 遭遇確率<br>クラス | コントロールリティクラス |    |         |
|---------------|-------------|--------------|----|---------|
|               |             | C1           | C2 | C3      |
| S1            | E1          | QM           | QM | QM      |
|               | E2          | QM           | QM | QM      |
|               | E3          | QM           | QM | A       |
|               | E4          | QM           | A  | B       |
| S2            | E1          | QM           | QM | QM      |
|               | E2          | QM           | QM | A       |
|               | E3          | QM           | A  | B       |
|               | E4          | A            | B  | C       |
| S3            | E1          | QM           | QM | A (QM*) |
|               | E2          | QM           | A  | B       |
|               | E3          | A            | B  | C       |
|               | E4          | B            | C  | D       |

\* E1 より低い遭遇確率が想定される組み合わせられた状況の場合

## 1.4 用語定義

本書における用語を、法令・制度上の用語、国際規格・技術用語、並びに安全設計に関する主要用語に区分して整理する。各用語は、それぞれの体系における位置づけに従って用い、同一の用語に対して複数の体系の定義を重ねて与えない。法令・制度上の用語は関係法令及び公的制度資料に基づき、国際規格・技術用語は当該規格において一般に用いられる意味で用いる。なお、特定の章においてのみ用いる用語については、必要に応じて当該箇所にて定義する。

### 1.4.1 法令・制度上の用語

#### 1. 自動運行装置

道路運送車両法及びこれに基づく保安基準に関係する用語であり、車両に備えられる装置をいう。本書では、自動運転移動サービスを構成する要素のうち、車両側の装置を指す用語として用いる。

#### 2. 走行環境条件

道路運送車両法に基づき、自動運行装置ごとに国土交通大臣（又は地方運輸局長）が付与する条件。本書では、自動運行装置の使用が可能な道路、環境、交通その他の条件を指す用語として用いる。

#### 3. 特定自動運行

道路交通法上の用語であり、道路において、自動運行装置をその使用条件に従って使用して自動車を運行することをいう。ただし、当該自動車の運行中の道路、交通及び当該自動車の状況に応じて当該自動車の装置を操作する者がある場合のものを除く。本書では、許可、特定自動運行計画、遠隔監視等の制度運用の文脈で用いる。

### 1.4.2 国際規格・技術用語

#### 4. ADS（Automated Driving System）

SAE J3016 において用いられる技術用語であり、動的運転タスク全体を実行する運転自動化システムをいう。本書では、国際規格又は技術の一般論を述べる場合に用いる。

## 5. ODD (Operational Design Domain)

SAE J3016 において用いられる技術用語であり、ADS 又はその機能が作動するように設計された運用条件をいう。本書では、国際規格・技術の文脈で用いる。なお、ODD は法令・制度上の走行環境条件とは区別して用いる。

### 1.4.3 安全設計に関する主要用語

## 6. ユースケース

本書では、走行環境と自車の進行方向の組合せに着目して類型化した代表的な走行場面をいう。例えば、単路直進、信号交差点右折、無信号交差点左折等がこれに当たる。なお、ユースケースは使用例又は仕様上の類型を表すものであり、その具体的な状況の展開としてのシナリオとは区別して用いる。

## 7. 基本走行戦略

本書では、ユースケースごとに、安全確認の内容、安全確認のタイミング及び確認後の走行方法を整理した基本方針をいう。停止、徐行、発進、進入判断等の原則を含む。

## 第2章 安全性を確保するための実施事項

### 2.1 自動運転移動サービスの定義

開発プロセス全体の最上位に位置する自動運転移動サービスの要件は、直接的・間接的に安全設計・評価業務に影響するので、開発工程の下流業務を担当する場合にあっても、目標を共有する意味でその内容を把握しておきたい。移動サービスが目標とする社会課題の解決に対して有効であることをはじめとして、安全性や採算性、事業の継続性など様々な観点からプロジェクトの成否を判断する指標と目標値を定義し関係者で共有することが重要である。

#### 2.1.1 主な検討項目

自動運転移動サービスでは、おおむね以下のような項目について定義する必要がある。

- ✓ 事業概要：事業の目的、実施期間、開発・運行・保守体制、採算性など
- ✓ 運行計画：走行ルートと停留所の位置、目標とする輸送量、車両台数、運行時間帯、季節や天候などの運行条件、運行回数・ダイヤなど
- ✓ 運行車両（特定されている場合）：自動運行装置を搭載するベース車両の仕様、特徴、他での使用実績など
- ✓ 運行形態：車内管理者や遠隔監視の存在と役割、乗客の定員や立席の有無など

安全性に関しては、何よりも優先的に必要基準に達するための方策を施す必要がある。その上で、自動運転車両の性能やコスト、実用性などには差異があり、あらかじめ使用する車両が特定されている場合は、走行環境と車両性能の整合や他で使用された実績などを十分に確認した上で、運行計画の策定に努めることが重要となる。

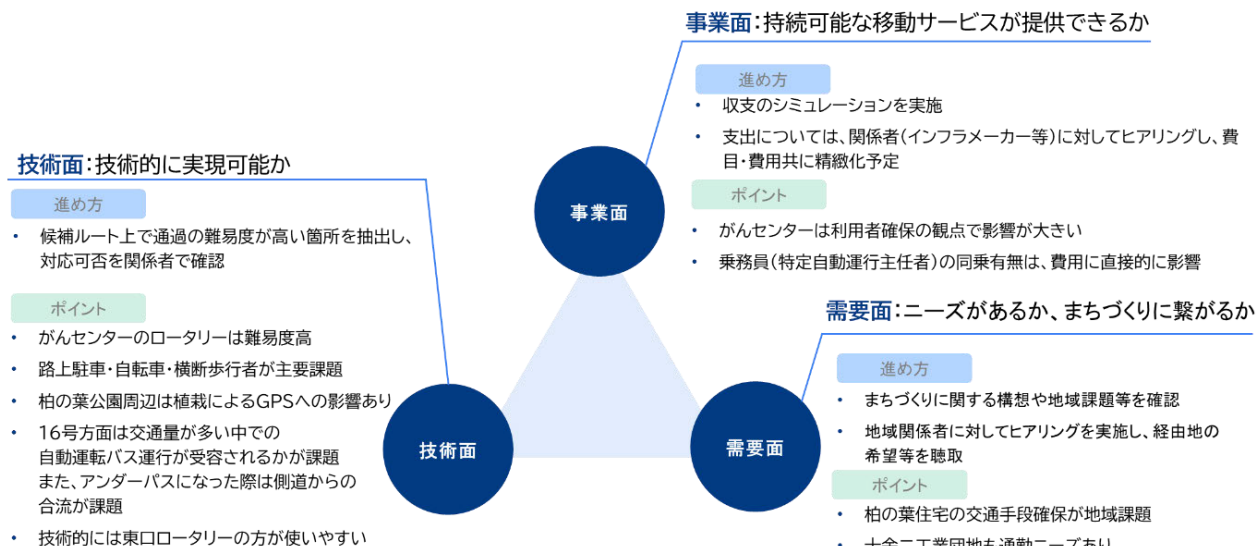
#### 2.1.2 走行ルートの選定

移動サービスの対象となる走行ルートの選定は、サービスの価値的なニーズと、発展途上の自動運転技術で必要な安全性を確保するシーズの両面から実現可能性を検討する重要な工程である。

本来、走行ルートは地域のニーズに基づいて設定されるべきものであるが、安全性は最優先事項であり、地域ニーズから導出されたルートにおいて十分な安全確保が困難な場合には、技術的に安全を確保できる範囲内でのルート設定が求められる。そのため、地域の移動ニーズを踏まえつつ、現時点の技術水準において安全な運行が可能な走行ルートを見極め、両者のバランスを取った判断を行うことが極めて重要である。

なお、走行ルートがおおむね決定した後の安全性検討作業については後述するが、走行ルート検討の初期段階では、リスクアセスメント等によりあらかじめリスクが高いと想定される場所（交差点右折や進路変更等）をリストアップし、安全対策の方向性などを関係者でできるだけ具体化しておくことで、プロジェクト全体として大きな手戻りを回避する効果がある。

参考までに、以下図 3 から図 5 までにおいて、RTL4 テーマ 4 において走行ルートに関して検討した事例を紹介する。ここでは、需要や事業性の観点から複数のルート候補案を選定し、安全確保の観点から技術的な難しさや過去の交通事故事例などについても考察している。



経済産業省令和5年掲載『令和4年度 無人自動運転等のCASE対応に向けた実証・支援事業（テーマ4）報告書』（管理番号 000454）より引用（p.190,図 150）

図3 ルート候補案の絞り込みに当たって必要な3つの視点（RTL4 テーマ4・柏の葉エリアの場合）

|                   |                                         |
|-------------------|-----------------------------------------|
| ルート全長             | ・ 2.3km(片道)                             |
| 想定ユーザー            | ・ 家族等の公園利用者、大学関係者、ホテル利用者                |
| 技術的難易度<br>(右直回数等) | ・ 右直:3回                                 |
| 過去事故件数<br>内訳      | ・ 5件<br>(高齢者:1、自転車:2、その他:2)             |
| 特徴・その他            | ・ 基本的に現状ルートから停車地を追加する形であり、技術的難易度は現在と同等。 |



経済産業省令和5年掲載『令和4年度 無人自動運転等のCASE対応に向けた実証・支援事業（テーマ4）報告書』（管理番号 000454）より引用（p.185,図 141）

図4 シャトルルート1の概要（RTL4 テーマ4・柏の葉エリアの場合）

[illegible]

図 5 循環ルート6の概要 (RTL4 テーマ4・柏の葉エリアの場合)

移動サービスを構成する機能（役割）や使用する車両の開発・運用・保守など、移動サービス全体を構成する要素と役割を具体化し関係者で共有する必要がある。

#### 2.1.4 安全目標の定義

**17 / 61**

を、関係者で共有する必要がある。

なお、安全目標を検討する際には、「社会受容性」という本質的に難しい課題に直面する。すなわち「どの程度の安全性が確保されていれば十分と言えるのか（How safe is safe enough?）」という問いである。いかなる技術においてもリスクを完全にゼロにすることはできず、安全の追求には終わりが無い。一方で、社会に実装する以上、どこかで「受容可能な水準」を定める必要がある。機能安全の分野では、安全とは「受け入れられないリスクが存在しない状態」、すなわち「リスクが社会的に許容可能な水準に抑えられている状態」と定義されている。しかし、その許容可能なリスク水準をどのように判断するのが明確でなければ、安全目標は定まらない。

事故の発生確率が極めて低いとしても、「事故が起こり得ることを前提とする考え方」に対して心理的な抵抗があるのは自然である。しかし、絶対安全が存在しない以上、現実的には、どの程度のリスクであれば社会として受入れ可能かを合理的に説明する枠組みが必要となる。この考え方として、本書ではリスクに基づいて安全性の妥当性を判断する risk-based approach を採用する。具体的には、以下に示す ISO 21448:2022 や ISO/TS 5083:2025 で取り上げている国際的に確立された原則などを根拠として、リスク受容の妥当性を総合的に判断する。

1. GAME 原則：対象とする自動運転移動サービス全体のリスク水準が、同等の機能を有する既存の交通システムのリスク水準を上回らないことを確認する。これは、法規・規格への適合、既存システムとの比較、体系的なリスク分析などを通じて示される。
2. ポジティブ・リスク・バランス（PoRiBa）：当該移動サービスの導入によって社会全体としての事故や被害のリスクが低減されることを確認する。評価にあたっては、人間の運転行動を含む従来の交通システムとの比較を行い、全体としてのリスク低減効果を重視する。ただし、特定の利用者層や集団に不均衡な不利益が生じる場合は、受容可能とはしない。
3. ALARP 原則：リスクが合理的に実行可能な範囲で十分に低い水準に抑えられているかを判断する。これは、追加的なリスク低減による効果と、それに要する負担やコストとの均衡を考慮し、社会通念上妥当な水準を見極めるための判断の枠組みである。
4. MEM 原則：死亡リスクに関して、当該移動サービスの導入によって交通事故に起因する死亡率が、導入前又は比較対象（同一ルート・同一走行環境条件での従来運行等）に対して統計的に有意に増加しないことを、曝露量（例：人 km、車両 km、運行時間）で正規化して定量的に評価する<sup>4</sup>。

これらの原則はいずれか一つを単独で用いるものではなく、車両性能、走行実績、運行形態、対象地域の交通状況などの個別条件を踏まえ、複数の観点を組み合わせて総合的に判断するための枠組みとして位置付ける。

なお、上述のリスク受容基準の根拠の考え方は、対象とする移動サービス又はその構成要素のライフサイクルごとに着眼点を変えて適用することが効果的と考えられるので参照のこと。

- コンセプトフェーズ：MEM / PoRiBa：社会実装可否の見通しとして検討
- 要求定義・アーキ設計フェーズ：GAME / ALARP：「悪化させない」「やるべきことをしっかりやる」を明確化する判断根拠として検討
- 詳細設計・実装フェーズ：ALARP：個別リスク低減目標を定める根拠として検討
- 検証フェーズ：GAME：実績のある事例との同等性を確認する根拠として検討
- 妥当性確認フェーズ：PoRiBa：全体的な効果を確認する根拠として検討
- 運用・改善フェーズ：PoRiBa：継続的な社会的妥当性を確認する根拠として検討

---

<sup>4</sup> MEM は本来、最小の自然死亡率を参照点にする考え方だが、ADS では人間運転の交通事故死亡率などドメイン特化の参照点を置く方が説明しやすい、という議論がある。

## 2.2 走行環境条件とユースケースの定義

走行ルートが短距離で走行環境がシンプルな場合を除き、走行ルートを走行環境（単路や交差点などの道路構造、信号やガードレール等の有無、制限速度等）に着目して特徴的な区間ごとに分けて類型化することを推奨する。そうすることによって、それぞれの区間ごとに走行環境を分かり易く具体的に定義することが容易になる。

また、走行環境と自車の進行方向（直進、右折等）の組合せに着目して、ユースケースとして類型化することを推奨する。ユースケースとして類型化することで、走行ルート全体を少ないユースケースで把握することが可能となり、関係者での議論や認識共有、プロジェクト管理などが効率化できる。また将来的に他のプロジェクトで同様のユースケースを扱う際には、従前の検討内容や実績などの情報と関連付けが可能となり、プロジェクトの企画段階から安全性検討の重要ポイントや開発の難易度、リソースなどの見積もり精度向上によって開発効率化が見込める。

走行環境条件及び基本的な走行方法の検討手順はおおむね以下のとおり。

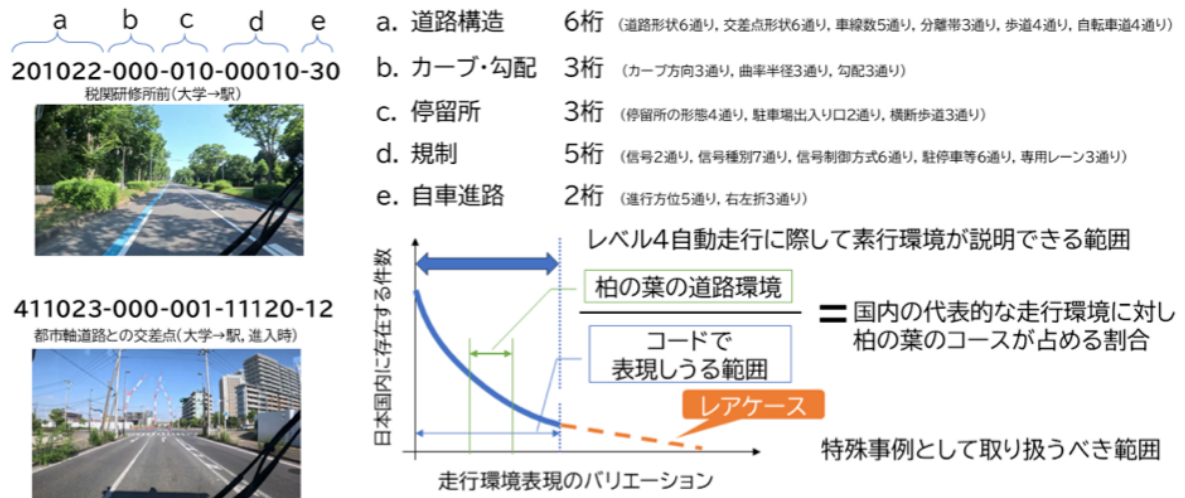
1. 運行ルートの走行環境分析と記述方法の定義
2. ユースケース（走行環境＋自車両の進行方向で分類する走行区間）の定義
3. 各ユースケースにおいて遵守すべき法規の確認
4. 各ユースケースにおける基本走行戦略（基本的な安全確認と走行方法）の定義

以下、各手順の詳細について解説する。ただし、③及び④については「2.3 基本走行戦略の策定」で後述する。

### 2.2.1 運行ルートの走行環境分析と記述方法の定義

走行環境の詳細（道路構造や道路附属物、天候等）を記述するにあたり、記述に用いる道路構造や進路に関する用語を体系的に整理し記述法を定義する必要がある。RTL4 テーマ4 では、走行環境条件設計に関する既存の研究等を参考に、走行環境の記述を独自に定義した 19 桁のコードで整理することを試行している（「図 6 走行環境の表現方法」）。

# 走行環境のコード表現



出典：霜野 慧亮 ほか（2024）「一般道混在環境下における協調型自動運転の実装に向けた Operational Design Domain の検討」自動車技術会 2024 年秋季大会 学術講演会予稿集（秋），文献番号 20246183（発表スライドより抜粋・著者提供・掲載許諾済）。

図 6 走行環境の表現方法

## 2.2.2 ユースケース（走行環境＋自車両の進行方向で分類する走行区間）の定義

先の「2.2.1 運行ルートの走行環境分析と記述方法の定義」で定義した分類に基づき、走行ルート上のユースケース（走行環境＋自車両の進行方向を組み合わせたもの）を定義する。走行ルート上には交差点や横断歩道等の様々な道路環境が存在し、進路や対応すべき交通参加者が異なるので、走行環境条件も異なる。よって、走行ルートの中で同様の走行環境が継続する区間をそれぞれユニークなユースケースとして分類することで、それぞれの区間ごとに走行環境条件を記述することができる。

## 2.3 基本走行戦略の策定

基本走行戦略は、安全確認のタイミングや内容、確認後の行動（徐行、停止、発進等）などを時系列的に整理するものである。基本走行戦略の検討は、システムがヒューマンドライバーに代わって運転操作を行う自動運転特有かつ最も重要な安全設計・評価プロセスとも言える。技術（認識性能向上や走行手順の工夫）と他（信号設置や制限速度遵守の啓蒙等）の課題の切り分けや、後述するリスクシナリオ抽出・評価・対策プロセスなどを効率化することに寄与する。

方法としては、本書で後述するレアケースや故障などを含め、リスク全体を網羅したうえで対策まで含めて走行戦略の検討に入る進め方もあり得る。しかし、実用可能なシステム性能を前提に、周囲の交通参加者を含めた道路交通法の遵守を前提とした基本的な走行方法（基本走行戦略）の成立が大前提である。したがって本書では、「2.2 走行環境条件とユースケースの定義」で類型化・整理した交差点の右左折等のユースケースごとに、まず基本走行戦略と、それを可能とするために必要な基本機能を定義し、その上でリスク対策を検討することを推奨する。

### 2.3.1 各ユースケースにおいて遵守すべき道路交通法と下位法令等の確認

自動運転レベル 4 において遵守すべき主な法規としては、道路交通法、道路運送車両法、道路法が挙げられるが、他にも関連する法規は多岐に渡る。ただしここでは、基本走行戦略に直接・深く関係する道路交通法への対応のみについて解説する。

分類した各運行区間には、優先すべき他の交通参加者（交差車両、横断歩行者等）や通行方法が道路交通法等により定められている。関連する法令の条項を整理し、各運行区間において適用される具体的な条項を明らかにすることにより、自動運行装置が対応すべき通行方法や場面理解が明確にでき、自動走行時にどの交通要因に対する考慮がなされているのかが明確になる。これは、自動運転車の安全性評価を実施する上でも重要な情報となる。

### 2.3.2 各ユースケースにおける基本的な安全確認と走行方法の定義

国土交通省のガイドラインでは、自動運転車の安全性確保について、自動運転に係る国際基準及び国際的なガイドラインにおいて自動運転車は道路交通規則を確実に遵守することが要求されていることを踏まえ、「A I 時代における自動運転車の社会的ルールの在り方検討サブワーキンググループ報告書」（令和 6 年 5 月）<sup>5</sup>に基づき、以下の基本的な考え方を示している。

1. 自動運転車は、道路交通法を遵守<sup>6</sup>する
2. 自動運転車は、他の交通参加者が道路交通法を遵守する限り、事故を発生させない
3. 自動運転車は、他の交通参加者が道路交通法を遵守しない場合であっても、できる限り事故を発生させない
4. 自動運転車は、他の交通参加者が道路交通法を遵守せず、事故が不可避な場合であっても、できる限り被害の軽減に努める

ここで扱う基本走行戦略では、自動運転車及び他の交通参加者が道路交通法を遵守する場合を想定し、様々なユースケースにおいて安全かつスムーズ（交通の円滑化を妨げない）な走行を行うために必要な、安全確認の内容や確認する位置、及び走行方法（徐行、一旦停止等）を具体化する。（他の交通参加者が道路交通法を遵守しない場合については第 3 章で解説する）

参考として、柏の葉エリアで丁字路交差点を右折するケースについて、走行環境と交通参加者の分析事例を「図 7 走行環境と交通参加者の分析事例」に示す。

---

<sup>5</sup> [https://www.cas.go.jp/jp/seisaku/digital\\_gyozaiikaikaku/kaigi6/sankou.pdf](https://www.cas.go.jp/jp/seisaku/digital_gyozaiikaikaku/kaigi6/sankou.pdf)

<sup>6</sup> 今後の国際議論等を踏まえ、関係省庁と連携した議論が必要。

なお、現在は道路交通法（下位法令を含む。以下本項において同じ。）に基づく運転操作に係る義務のうち、定型的・一般的なものについては、自動運行装置が代替して担うことが想定されており、道路交通法上の全ての義務を自動運行装置が代替して担うことが想定されているものではない。

上記の「定型的・一般的なもの」とは、信号機の信号に従う義務（道路交通法第 7 条）や最高速度に係る義務（同法第 22 条）等をいう。これに対して、同法 72 条第 1 項に基づく交通事故に係る負傷者の救護義務等、現場での個別具体的な対応が要求されるものについては、これに含まれない。

「図 7 走行環境と交通参加者の分析事例」は、信号制御された丁字路交差点において自動運転バスが右折するユースケースを例示したものである。基本走行戦略に影響し得る走行環境要因として、右折専用レーンの有無、右折矢印信号の有無、歩車分離（横断歩道の配置・信号制御）等を整理し、あわせてリスク要因となり得る交通参加者と想定行動（横断歩道へ進入する歩行者・自転車、交差道路の車両等）を抽出している。歩行者・自転車は複数方向から接近し得るため、横断歩道手前の段階で早期に認識できる視界・センサ視野の確保が重要であり、植栽や街路樹などの遮蔽物の配置も検討要素として明示しておく必要がある。

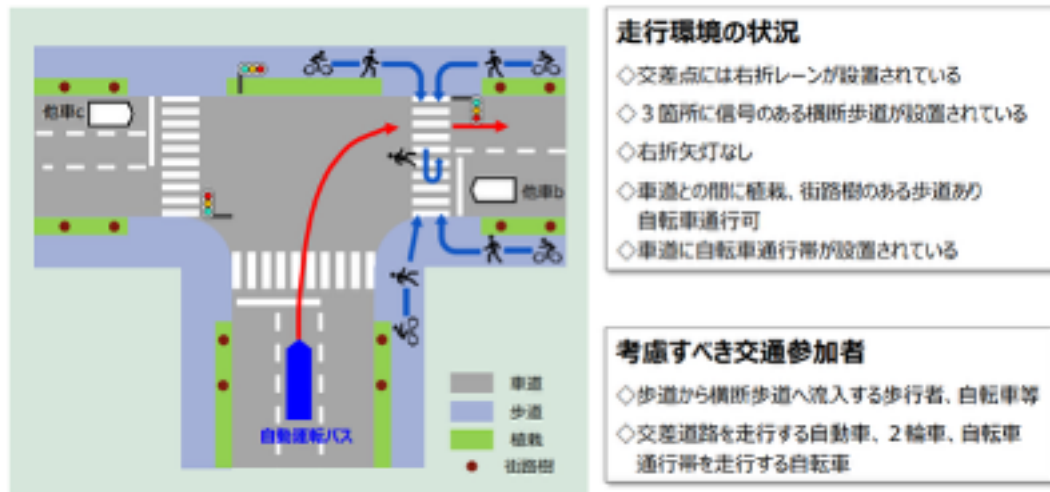


図 7 走行環境と交通参加者の分析事例

個人の思い込みや部門ごとの解釈の差によって法令不適合を招かぬよう、警察庁が令和 7 年 10 月に公表した「自動運転の開発に資する交通ルールの解釈の明確化に関する意見交換枠組みの設置」を利用し、個々の事象に応じて確認をすることも有効である。

## 第3章 安全性を確保するための実施事項 2

本章では、前章からユースケースごとの基本走行戦略を受けて、車両機能の定義からシステムへの要求導出までのプロセスを「表 3 車両機能の定義からシステムへの要求導出までのプロセス」の順に解説する。

表 3 車両機能の定義からシステムへの要求導出までのプロセス

| 実施項目          | 実施事項                                                                        | 主な入力                                   | 主な出力                        |
|---------------|-----------------------------------------------------------------------------|----------------------------------------|-----------------------------|
| 車両機能の定義       | ユースケースごとに必要な車両機能を抽出し定義する。                                                   | 走行環境条件<br>ユースケース<br>基本走行戦略             | 車両機能                        |
| リスクシナリオの導出    | リスク要因を抽出し、その要因が含まれるリスクシナリオを導出する。さらにそのシナリオのリスクの大きさを評価して、許容できないリスクシナリオを明確にする。 | 走行環境条件<br>車両機能<br>ユースケース<br>基本走行戦略     | リスク要因<br>リスクシナリオ<br>リスク評価結果 |
| 安全コンセプトの定義    | リスクに適切に対処するための考え方（安全コンセプト）を定義する。                                            | 車両機能<br>リスク要因<br>リスクシナリオ<br>リスク評価結果    | 安全コンセプト                     |
| システムへの安全要求の導出 | 安全コンセプトに従って、リスクの回避又は低減のためにシステムが実施すべきことを導出する。                                | リスク要因<br>リスクシナリオ<br>リスク評価結果<br>安全コンセプト | システムへの要求仕様                  |

### 3.1 車両機能の定義

「リスクシナリオの導出」に先立ち、自動運行装置に求められる機能を体系的に定義する。リスクシナリオを適切に導出するためには、走行環境条件のみならず、その走行環境条件内で作動する機能を明確化しておくことが必要である。ここでは、まず対象とする自動運転移動サービスの構成要素と、そのうち本章で主として扱う自動運行装置の範囲を定め、次に自動運行装置に求められる能力や基本機能を抽出したうえで、自動運行装置に求める機能を定義する。

#### 3.1.1 システム範囲

システム範囲を定めるというのは、①システム境界を明確にする、②自車両と相互作用のある外部システムを示す、③情報の流れなど外部システムとの関係を示すことである。

「図 8 自動運転移動サービスの構成要素と周辺関係者（例） - （再掲）」は、自動運転移動サービスの構成要素を示した例である。車両本体、自動運行装置、通信・管制システム、運行支援設備（停留所設備、路側装置等）、遠隔監視システム、インフラ協調システムから構成されている。

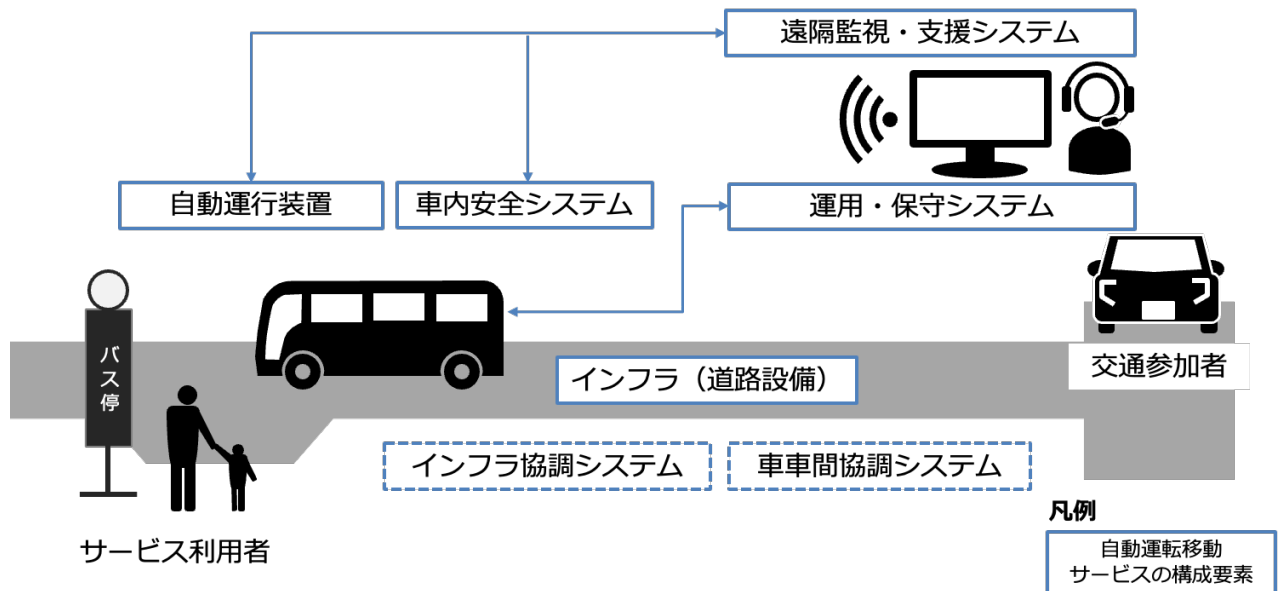


図 8 自動運転移動サービスの構成要素と周辺関係者（例） - （再掲）

この内、自動運行装置の開発では、自動運行装置にどのような動作機能を持たせるのかはもちろん、インフラ協調システムからどのような情報を受け取り、それに対して自動運行装置はどう振る舞うのかといった相互作用、遠隔監視システムと直接やり取りをするのか、通信・管制システム経由でやり取りをするのかといった自動運行装置の視点での情報の流れなどを明確にする。

### 3.1.2 自動運行装置に求められる能力

走行環境条件内で自動運行装置が安全かつ円滑に運行するために必要な能力を整理する。その上で、それらの能力を実現するために必要な機能を抽出する。

「表 4 期待される能力と必要な機能の例」は、自動運行装置に期待される能力と対応する必要な機能の例である。設計段階では、これらの機能をさらに詳細化していく。

表 4 期待される能力と必要な機能の例

| 期待される能力                   | 必要な機能   |
|---------------------------|---------|
| 静的・動的対象物の認識能力             | センシング   |
| 周辺対象の挙動予測能力               | 予測      |
| 走行可能領域の識別能力               | 識別／判断   |
| 自己位置推定能力                  | 自己位置推定  |
| 安全かつ法規適合な走行計画生成能力         | 走行計画    |
| 走行計画実行能力                  | 計画実行    |
| 自動運行装置の安全な作動能力            | 作動／停止   |
| 自動運行装置運用時の安全確保能力          | 運転状態監視  |
| 運転状態認識能力                  |         |
| 要求性能逸脱検出能力                |         |
| 運転モード遷移能力                 | 運転状態遷移  |
| 最小リスク状態への移行能力             | MRM     |
| ユーザ介入・解除対応能力              | ユーザ指示受入 |
| 周囲交通参加者への意思表示能力           | HMI     |
| 自動運行装置搭載車両への接近・乗降時の安全確保能力 |         |
| 乗員の外部連携支援能力               | 外部通信    |

(出典：ISO/TS 5083:2025, Annex E.2.3 を参考に整理)

また、自動運行装置は、安全に関わる物体や事象を正しく検知し、それに対して適切な応答を実行しなければならない (Object and Event Detection and Response: OEDR)。この応答は、衝突の危険がある周囲の障害物から安全な距離を維持しつつ、安定した制御操作又は回避行動を実現しなければならない。「表 5 基本的な応答行動の例」は、そのような要求を満たす基本的な応答行動の例を示している。これらの視点からも必要な機能を抽出する。

表 5 基本的な応答行動の例

| 応答行動         | 説明                                                                   |
|--------------|----------------------------------------------------------------------|
| 先行車追従        | 先行車両との間に十分な安全距離を維持するため、縦方向及び必要に応じて横方向の制御を行い、現在走行している車線内で追従走行を継続する挙動。 |
| 加速           | 周囲状況及び交通規則を踏まえ、必要かつ適切な範囲で車両速度を高めるための縦方向制御挙動。                         |
| 減速           | 前方状況や安全確保の必要性に応じて、車両速度を低下させるための縦方向制御挙動。                              |
| 停止           | 安全性と車両挙動の安定性を確保しながら、車両を完全停止状態に導くための縦方向制御挙動。                          |
| 優先権譲与        | 交差点等において他の道路利用者を優先させるため、自車の進行を抑制し、通行優先権を譲る挙動。                        |
| 車線変更         | 安全性及び交通状況を考慮しつつ、隣接する車線へ移動するために縦方向及び横方向の制御を組み合わせて行う挙動。                |
| 車線変更中止       | 開始又は準備中の車線変更を取りやめ、元の走行車線内に留まる、又は復帰するための制御挙動。                         |
| 追い越し         | 前方車両を追い越す目的で、隣接車線への移動と速度調整を組み合わせて行う挙動。                               |
| 追い越し中止       | 追い越しを目的とした車線移動又は加速動作を中断し、元の走行状態に戻るための制御挙動。                           |
| 右左折（進路転換）    | 現在走行している道路又は車線から接続する道路又は車線へ移行するために、縦方向及び横方向の制御を行う挙動。                 |
| 車線内位置調整      | 車線境界を越えることなく、車線内の位置を調整するために横方向及び必要に応じた縦方向制御を行う挙動。                    |
| 車線外逸脱（回避的移動） | 安全確保を目的として、車線境界を一部又は全部越えて車両を移動させる制御挙動。                               |
| 走行レーン離脱・停車   | 走行中のレーンから完全に離脱し、路肩や駐車帯等の非走行領域に移動した上で停止する挙動。                          |
| MRC 移行       | 人による介入を前提とせず、システム自身が縦方向及び横方向の制御を行い、最小リスク状態に到達するための挙動。                |

（出典：NHTSA, A Framework for Automated Driving System Testable Cases and Scenarios (2018), Chapter 4 を参考に整理）

### 3.1.3 基本機能

衝突回避の緊急時を除いて<sup>7</sup>、車両を公道で運行する際には道路交通法で定められた交通方法を遵守しなければならない。なお、道路交通法の個別・具体的な解釈については、当局に直接確認することが望ましい。したがって、自動運行装置が道路交通法を遵守して運行するために必要な基本機能を整理する。速度遵守、信号遵守、優

<sup>7</sup> 「緊急時を除いて」については、保安基準の細目告示第 72 条の 2 の 1 号に「自動運行装置の作動中、他の交通の安全を妨げるおそれがないものであり、かつ、乗車人員の安全を確保できるものであること。この場合において、交通上のリスクの最小化を図るための制御（以下「リスク最小化制御」という。）の作動中であつては、この規定は適用しない。」とある。ただし、リスク最小化制御は衝突回避と同等ではなく、リスク最小化制御の中に衝突回避が含まれることがあるという関係になる。

先権の適切な判断、歩行者・自転車の保護、駐停車規定の遵守など、本書の整理として法令に基づく最低限の走行機能を明確にする。

### 3.1.4 機能定義

システム範囲設定、能力要件、基本的な応答行動、法令遵守の観点を踏まえて、自動運行装置に備えなければならない機能を本書として総合的に示す。

以下は、車両レベルの機能の例を示している。ただし、これらの例は、あくまで一般的に考えられる基本的な項目の一部であり、構想しているシステムに応じて、項目を細分化・追加・拡張することが必要となる。

#### 1. 自動運転モード管理機能

開始／終了／再開可能条件の認知・判断、など

#### 2. 認識機能

車両周辺物体認識、信号・標識認識、路面状態認識、自己位置推定、など

#### 3. 予測機能

他車挙動予測、歩行者・自転車挙動予測、路面状態変化予測、信号状態予測、走行経路上の潜在リスク予測など

#### 4. 判断・計画機能

リスク評価・意思決定、経路計画、行動計画、運転モード選択判断、冗長系選択判断など

#### 5. 走行動作機能

先行車追従、加速、減速、停止、優先権譲与、車線変更、追い越し、右左折、車線内位置調整、車線外逸脱、走行レーン離脱・停車、MRC 移行、など

#### 6. 安全運転機能

障害物／衝突回避、緊急停止、車間距離維持、車線逸脱防止、など

#### 7. 乗員・乗客関連機能

乗降制御、乗員状態監視、など

#### 8. 通信機能

衛星通信、V2X 通信、遠隔監視通信、など

#### 9. 自己診断・冗長管理機能

センサ・コントローラ・アクチュエータ自己診断、冗長系切替、など

### 3.2 リスクシナリオの導出

動的運転タスク（Dynamic Driving Task: DDT）は、自動運行装置がリアルタイムで車両を操作し、周囲の状況に適切に対応する能力を評価・設計するための枠組みである（「図 9 自動運行装置が担う DDT 関連機能の概念整理」）。この観点において、自動運行装置の中心的機能は DDT に位置付けられる。したがって、システムの安全性を論証するためには、DDT の性能が対象とする走行環境条件内のあらゆる状況下において安全に機能することを示す必要がある。

DDT の安全性を主張する方法や手段は複数考えられるが、本書では DDT を認識、予測・判断、制御の 3 つの要素に分解して考える。

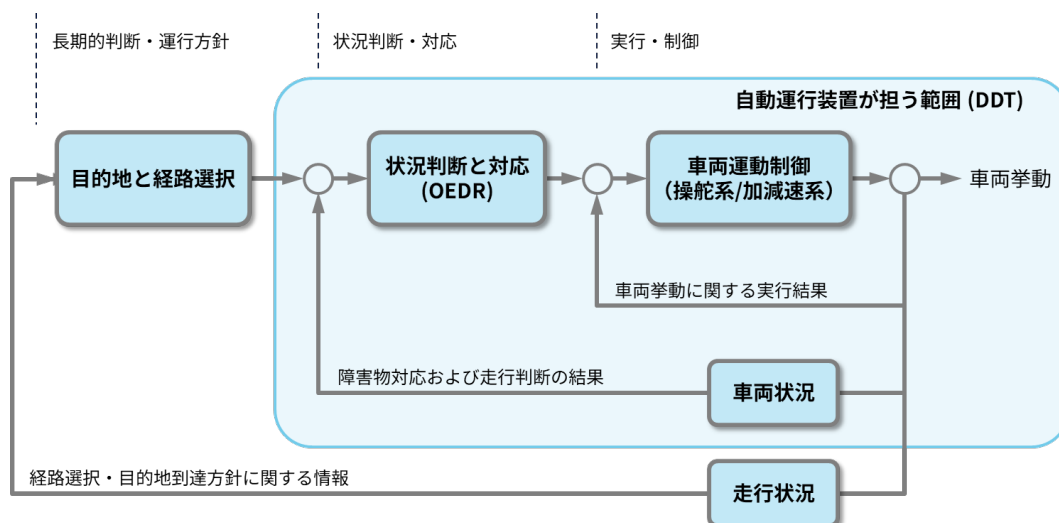


図 9 自動運行装置が担う DDT 関連機能の概念整理

(参考：ISO/SAE PAS 22736:2021 に示される DDT の考え方)

### 3.2.1 リスクシナリオの考え方

各ユースケースにおけるリスクシナリオを抽出する際には、走行環境条件の風景要素だけでなく、天候や照度、路面状態などの環境状態、さらに歩行者や他車両などの動的要素も含めて、走行路上に潜む危険を予測する危険予知 (KY) の観点からあらゆるシナリオを検討する必要がある。しかし、こうしたシナリオをフラットに考えると、理論的には無限に広がってしまい、網羅的な評価は困難となる。

この問題に対処するため、運転における DDT を、認識 (perception)、予測 (prediction)・判断 (judgement)、制御 (control) の 3 つの機能に分解する考え方がある。認識はセンサや通信によって外界を正しく把握する機能、予測・判断は周囲交通参加者の動きや状況を基に自車の走行計画を立てる機能、制御は計画された走行を実現するために車両を操作する機能である。

シナリオは、これら DDT の 3 つの機能に対応させて以下のように構造化することができる。

- 認識シナリオ：DDT の認識機能に対応
- 交通シナリオ：DDT の予測・判断機能に対応
- 車両制御シナリオ：DDT の制御機能に対応

次に、これらのシナリオにおいて考慮すべきリスク要因として、各シナリオに対応する外乱や故障を整理する。

- 認識外乱：センサの取付け状態や汚れ、周辺車両による死角、環境条件（霧・逆光・光量不足等）によって正しい認識が妨げられる要因
- 交通外乱：合流部や割込み、周辺車両の挙動など、交通環境に起因する要因
- 車両制御外乱：路面の凹凸や横風、車両重量や荷重分布など、計画どおりに車両が操作できなくなる要因

- 故障：センサ・アクチュエータ・ソフトウェアなど、システム自体の異常。その要因としてサイバー攻撃も含む。

このように、シナリオごとに対応する外乱や故障の要因を整理することで、膨大なシナリオ群を効率的に分類・体系化でき、網羅性を確保しつつ、特に人への危害に至る可能性のあるリスクシナリオを抽出できる。

**表 6 DDT 機能と対応するシナリオ及び外乱**

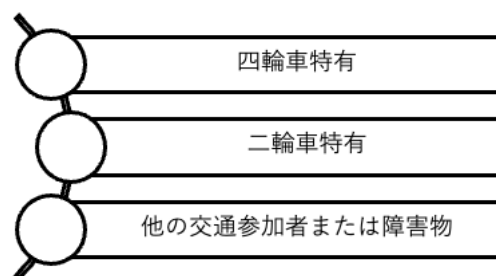
| DDT 機能 | 処理結果                                        | シナリオ     | 外乱     | 外乱の物理原則                                                                        |
|--------|---------------------------------------------|----------|--------|--------------------------------------------------------------------------------|
| 認識     | 周囲交通環境の物体位置（距離、方向、相対速度等）<br>自己状態（位置、方向、速度等） | 認識シナリオ   | 認識外乱   | センサメカニズムに応じた<br>原理的な外乱<br><br>例：<br>カメラ：可視光<br>ミリ波：電波<br>LiDAR：赤外光<br>加速度センサ：G |
| 予測/判断  | 周囲交通環境の物体移動位置<br>経路、速度目標                    | 交通シナリオ   | 交通外乱   | 幾何的観点（周辺交通環境＋交通参加者との位置関係等）<br>交通参加者の動作                                         |
| 制御     | 駆動指示<br>操舵指示<br>制動指示                        | 車両制御シナリオ | 車両制御外乱 | 路面、外界からタイヤ及びボディに入力される力学的な外乱                                                    |

（参考：日本自動車工業会「自動運転の安全性評価フレームワーク Ver3.0」に示される外乱の考え方）

### 3.2.1.1 交通関連クリティカルシナリオ

交通環境に関わるリスク要因を整理する際には、対象となる主体の違いに着目して整理すると理解しやすい。

例えば、交通に関わるシナリオは、四輪車を中心とした一般車両に特有のもの、二輪車に特有のもの、及び車両以外の交通参加者や道路上の障害物に関わるもの、といった観点で整理することができる。



**図 10 交通シナリオを整理するための主な観点**

交通に関わるシナリオは、道路形状、自車両の行動、及び周囲の対象物（四輪車、二輪車、その他交通参加者又は障害物）の位置や動きといった複数の要素を組み合わせることで、網羅的に把握することができる。



図 11 交通関連クリティカルシナリオの考え方

### 道路形状と自車両行動

一般道における道路形状は、説明の便宜上、交差なし（単路）、合流、分岐、交差といった代表的な形態に整理できる。

自車両は、これらの道路形状に応じて、車線内を直進（車線維持）する行動や、車線変更を行う。また、交差路では、車線変更ではなく右左折という行動が生じる。

そのため、自車両の行動は、直進（車線維持）、車線変更、右左折といった観点で整理でき、これらは道路形状との対応関係として捉えることができる。

| 道路形状     | 自車両行動         |
|----------|---------------|
| 交差なし（単路） | 直進（車線維持）、車線変更 |
| 合流       | 直進（車線維持）、車線変更 |
| 分岐       | 直進（車線維持）、車線変更 |
| 交差       | 直進（車線維持）、右左折  |

図 12 道路形状と自車両行動の対応関係の整理

### 周囲対象物の位置と動作

考慮すべき自車両周囲の対象物の位置及び動作は、自車両の走行軌跡に侵入する可能性がある位置として整理する。具体的には、自車両周辺の 6 方向の位置（周辺①～周辺⑥）、交差路から進入する左右 2 方向の位置（進入①、進入②）、対向方向として 3 方向の位置（対向①～対向③）、さらに二輪車・自転車・歩行者を主な対象として考えた場合の自車両近接の 2 箇所（近接①、近接②）である。これらを合わせ、合計 13 の位置として定義できる（「図 13 周囲の対象物の位置と動作方向」）。

障害物としては、コーンや道路工事用フェンスなどの静止障害物のほか、ボールなどの動的障害物が考えられる。また、対象物の形状や寸法などの特性についても考慮する。



図 13 周囲の対象物の位置と動作方向

各ユースケースにおいては、これらの位置及び対象物特性の組合せを考慮し、該当するシナリオを網羅的に洗い出す。

その際、信号無視や突然の飛び出しなど、他の交通参加者による容易に想定できる交通規則違反についても考慮に入れる。

### 3.2.1.2 認識関連クリティカルシナリオ

認識に起因するリスクは、その性質に応じていくつかの観点から整理できる。具体的には、センサや認識処理の性能に起因する認識限界、物理的・環境的要因によって対象物が検知できない死角、及び外部との情報連携が成立しない、又は制限されることによる通信制限の観点である。

各ユースケースにおいては、これらの観点を踏まえ、認識に関わるリスクを体系的に洗い出し、該当する認識シナリオを整理する。



図 14 認識シナリオを整理するための主な観点

## 認識限界

認識限界に関連するクリティカルシナリオは、システムの物理特性に係る複数の認識関連リスク要因の組合せとして整理できる。認識に影響を与える要因は数多く存在するが、これらをセンサに関わる物理的な原理の観点から整理することで、シナリオ検討において考慮すべき要因を効率的に絞り込むことができる。

センサの種類を具体的に選定する前段階の車両レベルの分析においては、一般に用いられている既存センサが有する特性上の弱点を踏まえ、想定されるリスク要因を抽出することが有効である。

## 死角

交通関連シナリオの検討では、通常、周囲の車両や対象物が自車両によって検出されていることを前提とする。しかし実際の交通環境では、他の車両や道路構造物によって視界が遮られ、自車両から認識できない領域、いわゆる死角が生じる。このような死角の存在により、安全上重要となるシナリオが発生し得るため、死角に起因するシナリオを考慮する必要がある。

死角に関する要因は、大きく以下の3つの観点から整理できる。

- ① 周辺車両による死角
- ② 道路構造要素による死角
- ③ 道路形状に起因する死角

これらの観点に基づき、死角に関連するシナリオを体系的に整理する（「図 15 死角関連リスク要因の整理観点」）。

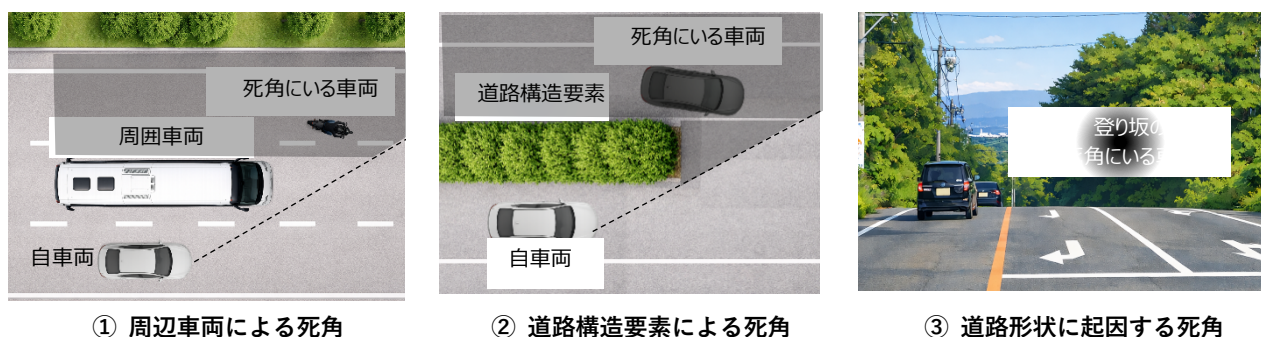


図 15 死角関連リスク要因の整理観点

### ① 周辺車両による死角

周辺車両による死角では、直前を走行する車両だけでなく、他の周辺車両によっても視界が遮られる可能性がある。特にカーブ区間では、自車両及び周辺車両の位置関係が時間とともに変化するため、死角となる領域も動的に変化する。このような特性を踏まえ、周辺車両の配置や動きに応じた死角シナリオを検討することが重要である。

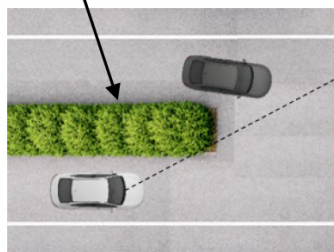
### ② 道路構造要素による死角

道路構造要素による死角シナリオは、遮蔽を生じさせる構造物の位置と、自車両と遮蔽された車両との相

対的な動きの係に目して整理できる。遮蔽要素は道路構造の一部として存在する場合があります、その種類や配置によって死角の発生状況は異なる。

これらの道路構造要素は、位置関係の違いにより、「内側に配置された構造物によるもの」と「外側に配置された構造物によるもの」に分けて考えることができる（「図 16 道路構造要素の分類」）。それぞれについて、自車両の進行方向や周辺車両の動きとの組合せを考慮し、該当するシナリオを整理する。

道路内側に配置された構造物



道路外側に配置された構造物

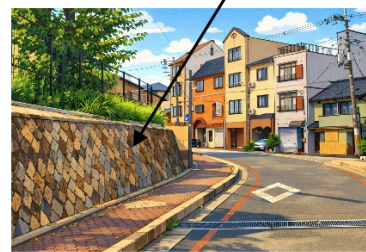


図 16 道路構造要素の分類

### ③ 道路形状に起因する死角

道路形状に起因する死角シナリオは、道路の形状的特徴と、車両同士の遮蔽関係に基づいて定義できる。この種の死角は、同一路上において高低差が生じる道路形状によって発生することが多く、代表的な例として縦曲線や並行する斜面などが挙げられる。

既に定義されている車両位置の整理方法を応用することで、道路形状に起因する死角シナリオについても、他の死角要因と同様に整理することが可能である。

## 通信制限

通信を利用した機能は、位置推定、経路案内、周囲状況の把握など、自動運行装置の能力を補完・拡張する重要な役割を担っている。一方で、通信には通信方式や利用環境に固有の制約があり、通信状態の悪化や情報の欠落が安全上重要なシナリオにつながる場合がある。このため、通信の限界に起因するシナリオについても、体系的に整理し、検討対象に含める必要がある。

通信制限に起因するシナリオは、通信に関わる要因の性質に着目し、以下の 3 つの観点から整理できる。

- ① センサに起因する通信制限
- ② 環境に起因する通信制限
- ③ 送信機に起因する通信制限

これらの観点に基づき、通信制限に関連するシナリオを整理する。

### ① センサに起因する通信制限

センサに起因する通信制限は、主にデジタルマップに関する要因と、V2X に関する要因に分けて考えることができる。

デジタルマップは、車両の位置推定や経路案内を支援するために用いられ、認識センサと組み合わせることで認識結果の信頼性向上にも寄与する。しかし、デジタルマップは、データ収集や生成アルゴリズムの不備、あるいは更新の遅れにより、実際の道路状況と不整合を生じる可能性がある。例えば、一時的な車線規制や道路形状の変更が反映されていない場合、誤った判断につながるおそれがある。

V2X は、他車両、道路インフラ、歩行者、サーバなどの通信を通じて、自車両周辺の状況を事前に把握する手段を提供する。特に悪天候時や複雑な交通環境において有効である一方、通信品質の低下や情報の欠落が生じる場合がある。また、デジタルマップ、V2X、他のセンサから得られる情報が一致しない場合には、情報融合の挙動が通信制限シナリオに影響を与える点にも留意が必要である。

## ② 環境に起因する通信制限

環境に起因する通信制限は、通信信号や測位信号に影響を及ぼす周囲環境の特性に着目し、静的要素、空間要素、動的要素の 3 つの観点から整理できる。

静的要素には、建物、樹木、トンネル、立体交差といった道路沿い・上空・地下の構造物が含まれる。これらは通信信号の遮蔽や反射を引き起こし、通信品質の低下や測位精度の悪化につながる場合がある。

空間要素としては、電波干渉、降雨や霧による減衰など、車両周囲の空間的な条件が挙げられる。これらの要因は、通信や測位の安定性を低下させ、結果として通信制限に起因するシナリオを生じさせる可能性がある。

動的要素には、周囲を走行する車両、二輪車、歩行者などが含まれる。これらの移動体は、通信経路を一時的に遮断したり、通信環境を変化させたりすることで、通信状態に影響を与える。

## ③ 送信機に起因する通信制限

送信機に起因する通信制限は、通信や測位に関与する送信源の種類に着目して整理できる。具体的には、他の車両、道路インフラ、歩行者が携帯する端末、サーバ、遠隔制御装置、衛星などが対象となる。

これらの送信機において、故障や設定不良、通信負荷の増大などが生じた場合、送信されるメッセージが利用できなくなったり、信頼性が低下したりする可能性がある。また、衛星に起因する通信制限では、測位信号の欠落や不安定化が発生し、位置推定に影響を与える場合がある。

このように、送信機側の要因についても考慮し、通信制限に起因するシナリオを整理することが重要である。

### 3.2.1.3 車両制御関連クリティカルシナリオ

車両制御に関連するクリティカルシナリオは、車両運動に直接影響を与える力の入力に着目して整理できる。これらの力は、主に車体に作用するものと、タイヤを介して作用するものに分けて考えることができる。車両制御関連シナリオは、こうした入力特性の違いに基づき、体系的に整理する（「図 17 車両運動シナリオを整理するための主な観点」）。

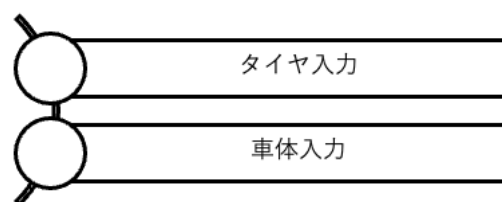


図 17 車両運動シナリオを整理するための主な観点

#### タイヤ入力

タイヤ入力に起因する車両制御関連のリスク要因は、路面状態とタイヤの状態の二つの観点から整理できる。

路面状態とは、タイヤが受ける力に影響を与える路面の特性や変化を指す。例えば、路面とタイヤの間の摩擦係数は、雨、雪、凍結、不均一な路面などによって変化し、タイヤのグリップ低下を引き起こす場合がある。このような摩擦特性の変化は、車両の安定性や制御性に影響を与える。

タイヤの状態とは、パンクやバーストのような突発的な変化、あるいは摩耗や空気圧低下といった時間をかけて進行する変化を指す。これらの変化によりタイヤに発生する力が変わり、車両の挙動が乱れることで、制御困難な状況に至る可能性がある。

### **車体入力**

車体入力に起因する車両制御関連のリスク要因は、道路の形状と自然現象の二つの観点から整理できる。

道路の形状には、曲線半径、縦方向の勾配、横方向の勾配などが含まれる。これらの要素により、車両に作用する慣性力や重力の方向・大きさが変化し、車線逸脱や速度変動など、車両制御に影響を及ぼす場合がある。

自然現象には、横風、追い風、向かい風など、車両のボディに直接作用する風が含まれる。特に強風や突風は、車両の進行方向や速度に変動を生じさせ、周辺車両との干渉や走行安定性の低下につながるおそれがある。

#### **3.2.1.4 不具合シナリオ**

これまで述べてきた、DDT 機能（認識、予測・判断、制御）に対応する、認識関連クリティカルシナリオ、交通関連クリティカルシナリオ、車両制御関連クリティカルシナリオは、タイヤのパンクなど一部の例外を除き、自動運行装置が正常に機能している状態において発生するシナリオである。

これに対し、不具合シナリオは、自動運行装置に何らかの異常が発生し、DDT 機能が正常に動作できなくなる状態を伴うシナリオを指す。

認識関連、交通関連、車両制御関連の各クリティカルシナリオにおけるリスク要因は、同一のシステム及び同等の走行環境条件下ではシステムに作用し、他の走行環境条件下では作用しないという特徴を持つ。したがって、個々のリスク要因については、該当するシナリオを対象として対処を検討することになる。

一方、不具合は、故障（物理的な損傷や劣化）やサイバー攻撃によって発生することが考えられる。故障はさらされる環境や経年の影響を受けるものの、運転シナリオとは独立して、ある確率で発生する性質を持つ。サイバー攻撃についても、攻撃のタイミングや仕組まれた手段に依存して発生するものであり、運転シナリオとは無関係に生じる。

したがって、特定のシステム要素の故障や、サイバー攻撃による特定機能への悪影響については、あらゆる走行シナリオにおいて発生する可能性を考慮する必要がある。

#### **3.2.2 シナリオ空間の定義**

自動運転車両のシナリオ設計においては、まず考慮すべきシナリオ空間を明確に規定する必要がある。シナリオ空間とは、走行環境条件と自動運行装置の振る舞いを踏まえ、想定されるすべての走行シナリオを包含する範囲を指す。地理的な観点では、まず走行ルート及びその周辺の道路環境をシナリオ空間の対象範囲として定義する。その上で、当該範囲に含まれる道路形状、信号や標識などの静的要素、ならびに他車両や歩行者といった動的要素を考慮することで、想定すべきシナリオ空間が具体化される。

シナリオ空間には、通常シナリオ、リスクが顕在化するクリティカルシナリオ、ならびに自動運行装置の不具合状態を伴うシナリオを含む。

ユースケースごとにシナリオ空間を定義することで、各ユースケースにおける自動運行装置の振る舞いやリスク要因を個別に検討でき、走行ルート全体の安全性や機能性を体系的に評価することが可能となる。

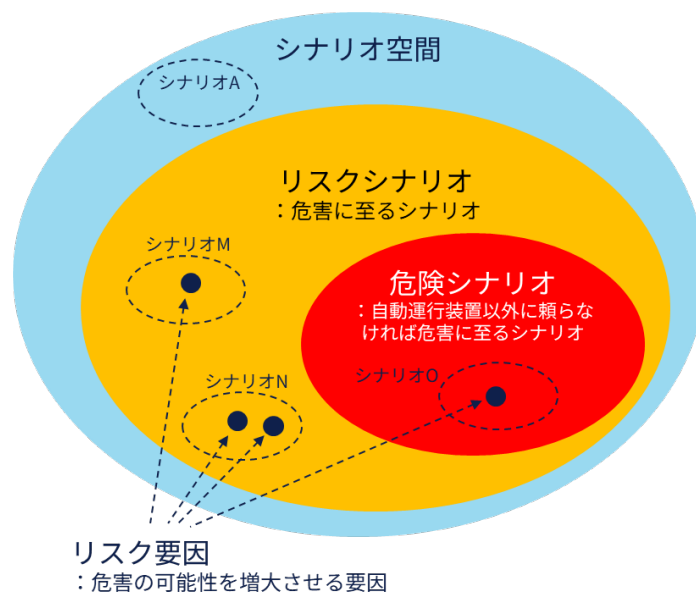


図 18 シナリオ空間とリスクシナリオ

### 3.2.3 リスクシナリオの明確化

自動運行装置の安全性を検証するためには、潜在的なリスク要因を体系的に把握し、それらを基盤としてリスクシナリオを導出することが重要である。リスク分析のプロセスは大きく3つの流れに分けて考えることができる。すなわち、①リスク要因を抽出し、②そのリスク要因が含まれるシナリオ、つまりリスクシナリオを抽出し、③最後にそのリスクシナリオが人への危害の観点でどの程度の大きさのリスクを抱えているかを見積もるリスクの評価、という一連の流れである。

リスクの大きさを評価した結果、許容できないリスクシナリオを明確にし、以降、それらのシナリオに対するリスクの回避又は低減方法を検討していく。

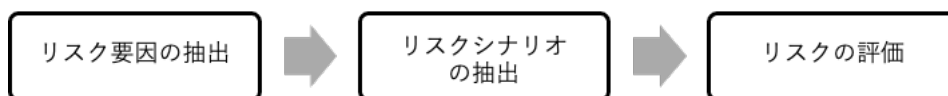


図 19 リスクシナリオ明確化の手順

#### 3.2.3.1 リスク要因の抽出

リスクシナリオを抽出する前段階として、まずリスク要因を明確にする。リスク要因とは、人への危害や事故の可能性を高める要素である。

リスクシナリオには、自動運行装置が正常に機能している状態でリスクが顕在化するクリティカルシナリオと、自動運行装置の故障や異常状態を伴う不具合シナリオの双方が含まれる。そのため、リスク要因の抽出にあたっては、走行

環境条件に起因する要因だけでなく、システム内部の不具合に起因する要因についても考慮する必要がある。

リスク要因を抽出する際には、ユースケースを対象に、走行環境条件に基づいて自動運転車両の視点から状況を詳細に観察する。ユースケースごとに、「どのような危険が潜んでいるか」を注意深く洗い出すことが、後続のリスクシナリオの網羅性と妥当性を確保する上で重要である。

観察にあたっては、交通関連、認識関連、車両制御関連の各クリティカルシナリオの分類を利用して、体系的かつ網羅的にリスク要因を抽出する。

その際、不具合関連のリスク要因については、DDT を構成する機能ごとに、不具合が発生した場合の影響を網羅的に考慮する。

以下に、具体的なリスク要因の例を示す。

十字路交差点をバスが右折する状況において、

**例 1：死角（周辺車両による視界制約）**

進行方向の先が見えない

具体例 1：対抗右折車両が交差点内に存在し、その先に存在する他の車両や歩行者が見えない、また相手からもバスが見えない。

**例 2：交通状況（道路形状＋自車両位置＋対象物の位置・動作）**

予期せぬ周辺交通参加者の動き

具体例 2：バスが右折する先の横断歩道近くに歩行者が存在（静止）。

**例 3：不具合発生**

操舵機能が故障

具体例 3：操舵トルクが出力できなくなる。

### 3.2.3.2 リスクシナリオの抽出

抽出したリスク要因に基づいて、クリティカルシナリオ及び不具合シナリオを抽出する。

クリティカルシナリオは、「3.2.1 リスクシナリオの考え方」で取り上げた「交通関連クリティカルシナリオ」「認識関連クリティカルシナリオ」「車両制御関連クリティカルシナリオ」の観点を基礎とし、さらに他の道路利用者や物体の動的な振る舞いを考慮することに加え、潜在的に危険を生じ得る相互作用を体系的に抽出する。

また、リスク要因として抽出した不具合を起点として、それが通常シナリオやクリティカルシナリオの状況下で発生した場合を不具合シナリオとして体系化する。

以下に、具体的なリスクシナリオの例を示す。

十字路交差点をバスが右折する状況において

### **例 1：死角（周辺車両による視界制約）**

進行方向の先が見えない

具体例 1：死角を作っている車両の背後から、二輪車がバスの進路に進入して衝突する。

### **例 2：交通状況（道路形状＋自車両位置＋対象物の位置・動作）**

予期せぬ対向車両の動き

具体例 2：バスが右折開始直後に、停止していた歩行者が横断を始めたためバスは減速、バスの減速に気付くのが遅れた対向直進車が衝突する。

### **例 3：不具合発生**

操舵機能が故障

具体例 6：バスは走行すべき軌道から外れ、交差点外側の歩道に乗り上げる。（青矢印）

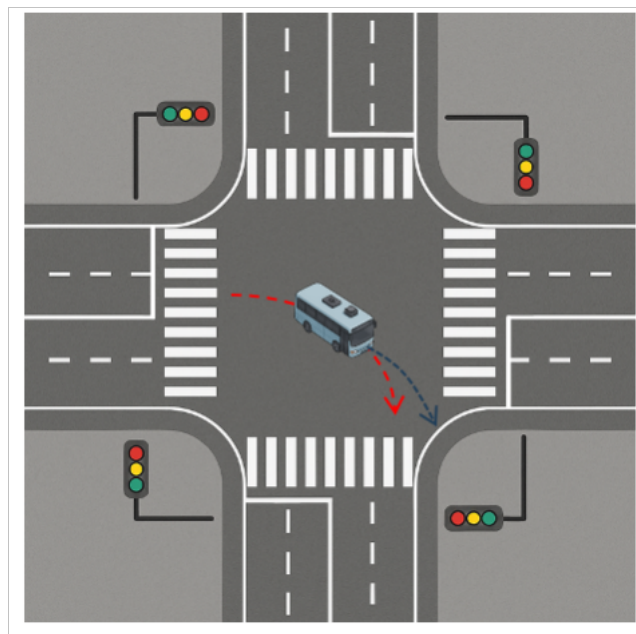


図 20 信号のある交差点右折中の操舵機能故障

#### **3.2.3.3 リスクの評価**

抽出したそれぞれのリスクシナリオにおけるリスクの大きさを評価する。リスク評価の考え方は、「1.3.4 リスクの評価」を参照のこと。

### **3.3 安全コンセプト**

安全コンセプトとは、走行環境条件下のすべての運転条件において、通常時及び不具合時を問わず乗員や他の道路利用者に不当な安全上のリスクを与えないようにするための、車両レベルでの基本的な安全確保の考え方を示すものである。

安全コンセプトは、車両に対する安全要求を導出する前段階において、安全確保の原則、リスク対応、フェールセ

ーフ方針、といった考え方を体系的に整理するものであり、後続の安全要求定義やシステム設計、さらには安全性を論証するセーフティケースにおける重要な基盤として位置付けられる。

したがって、妥当なリスク分析や論理的な考え方に基づき、一貫性をもって策定することが極めて重要である。

以下では、車両レベルの安全確保の中核をなす、センシング及びリスクシナリオへの対応について、明確化しておくべき内容を示す。

### 3.3.1 センシング

車両が安全に走行するためには、周囲環境や他の交通参加者を正確に把握するとともに、自車位置や車両自身の状態を高い信頼性で把握することが極めて重要である。安全コンセプトにおけるセンシングの基本方針として、まず、車両が取得すべき情報と、その情報を基に安全を確保するための考え方を体系的に整理しておく必要がある。具体的には、主に、①物標認識（周囲の対象物の検出・認識）、②自己位置推定（地図上の正確な位置・姿勢の推定）、③車両状態情報（速度、加速度、ヨーレート、操舵角等）がある。

#### ①物標認識

物標認識については、走行環境条件に応じて安全に関わるすべての対象物を網羅的に抽出し、認識すべき対象物を明確化しておく必要がある。対象物には、歩行者、自転車、他の車両に加え、標識や道路標示、信号機、路側帯構造物、落下物や工事資材等の障害物が含まれる。こうした対象物を明確化しておくことで、車両が安全に走行するために必要な認識要件が整理され、その後の安全確保の方針の基礎となる。

加えて、物標認識のセンシング戦略としては、認識すべき対象物を安全影響度やリスク度合いに応じて優先順位付けし、重要な対象物を重点的に監視する方針を整理しておくことが考えられる。例えば、歩行者や自転車などリスクの高い対象物は最優先で把握し、事故リスクや被害の大きさに直結する情報を確実に取得できるように整理しておくことで、変化する走行環境の中でも安全性を一貫して確保することが可能となる。

#### ②自己位置推定

自己位置推定については、位置情報、速度・加速度情報、地図情報などによる相互照合により、自車の位置・姿勢・走行軌跡を一定の精度で確保する必要がある。特に自動運転バスでは、歩道・車道境界の位置や停留所への正着制御など、位置推定誤差が安全性やサービス品質に直接影響するため、環境条件（高架下、ビル街、トンネル等）による位置推定の悪化を想定し、複数情報源の冗長性とフェールセーフ動作の方針を整理しておくことが必要である。

加えて、走行環境や運行条件に応じて自己位置推定の重要性や必要精度を調整する、いわゆる走行環境条件の変化への適応戦略を検討しておくことも考えられる。

#### ③車両状態情報

車両の状態を正しく把握するためには、速度、加速度、ヨーレート、操舵角などの車両状態情報を高い信頼性で取得することが重要である。安全で安定した車両挙動を実現するためには、現在の車両状態を正確に認識していることが前提となるため、これらの情報を適切に把握することが、走行中の安全確保につながる。

このような車両状態情報を適切に活用するためには、走行環境条件や想定する走行シナリオに基づき、何を対象として、どの範囲を、どの程度の精度及び分解能でセンシングすべきかという基本的な考え方を整理しておく必要がある。

加えて、速度や運行状況に応じて情報の取得頻度や監視の重要度を調整する動的更新戦略を検討しておくことも考えられる。また、安全に直接影響する情報を重点的に監視する優先順位付けや、走行環境条件の変化に応じて注視すべき情報を調整する適応的な方針も整理しておくことが考えられる。

これにより、変化する走行環境や運行条件の中でも、車両状態情報に基づく安全確保の原則を一貫して示すことが可能となる。

#### ④不具合対応

センシング全体の基本方針として、センサ及び推定アルゴリズムの冗長性を確保しておくことが重要である。冗長性とは、単一のセンサや推定系の障害、一時的な機能低下、計測誤差の増大が発生した場合でも、車両全体として必要な情報を維持できるよう複数のセンサ・推定手法を組み合わせる考え方である。また、物標認識や位置推定、車両状態計測のいずれかで不確かさが急激に増加した場合には、安全側行動を取る基本方針（速度制限による減速、走行継続の可否判断、MRM への移行等）を明確に定義しておく必要がある。

#### ⑤ロバスト性

走行環境条件によってセンシング性能が低下する場合の安全方針も整理しておく必要がある。雨、雪、霧、夜間、逆光、路面状態の変化、電波環境の悪化などにより、物標認識・位置推定・状態計測のいずれの精度も低下し得ることを想定し、その際に車両が安全を確保するための基本原則として、速度制限による減速や MRM への移行を定めておく。これにより、変化する走行環境に応じた一貫した安全確保の考え方が提示できる。

こうしたセンシング戦略の整理により、変化する走行環境や運行条件の中でも、車両が安全に走行するための基本的な方針を一貫して示すことができる。

### 3.3.2 リスクシナリオへの対応

リスクシナリオに対する適切な対応方針を定める。「3.2.3 リスクシナリオの明確化」において対応が必要と判断したリスクシナリオについては、その発生を抑制する観点からの「リスク低減戦略」と、発生又は予期される状況において、交通参加者（他車両・歩行者等）及び乗員の安全を確保するために求められる行動の考え方としての「リスク対応戦略」を体系的に整理する。

すなわち、リスクシナリオの発生をどのような考え方で抑制すべきか、また想定外の状況が生じた場合にどのような応答行動が求められるかを明確にすることで、後続の設計・実装フェーズにおいて一貫した安全方針を与える。

#### 1) リスク低減戦略

リスクシナリオは、システムの誤作動、機能の不十分性、あるいは想定外の運用状況によって発生する可能性がある。これらのリスクを抑制又は発生時の影響を低減するためには、各リスク要因に応じた対応の方向性をあらかじめ整理しておくことが重要である。

ここでは、個別の設計戦略を定める前段階として、車両システム全体としてリスクにどのような考え方で向き合うべきかを明らかにし、対応の一貫性を確保するための基本的な方針を策定する。これにより、後続の設計プロセスにおいて、安全性に関する判断や対策が統一された枠組みのもとで進められるようにする。また、設計上の配慮に加え、運転挙動に関する慎重な判断もリスク低減方針に含まれる。

リスク低減方針として、①危険な振る舞いを発生させない（機能の不十分性・直接的ミスユースへの対応）、②コントロールビリティやシビアリティに悪影響を与えない（間接的ミスユースへの対応）、③機能不全による影響を最小限に抑える（不具合対応）、さらに④運転挙動においてリスクを予測し、慎重な判断を行うこと（予測行動）が挙げられる。

### ①機能の不十分性・直接的ミスユースへの対応

センサ認識、位置推定、経路判断、制御出力など、自動運行装置を構成する各機能が意図どおりの性能を発揮できないことは、リスクの主要な発生要因となる。したがって、環境条件や運用条件に応じた個々の機能の精度・応答性・安定性を確保することが重要である。このような必要性能に対して、例えば、どの程度のマージンをもたせるかなどの方針を策定する。

例えば、自動運行装置では認知・対応が難しい残存リスクが存在し、想定外の緊急時には乗員又は乗客が自動運転を停止できる機能を備える場合がある。ただし、誤った操作によって自動運転を意図せず停止させるシナリオも想定され、突然の停止で適切な制御が失われ衝突に至る危険性があり、こうしたときは直接的ミスユースに該当する。したがって、この例では、誤操作によって自動運転が停止できないようにする仕組み、又は必ず安全に制御が移行する仕組みをどのような方針で備えるかを策定する。

ちなみに、実装事例としては、緊急停止ボタンを「停止要求」として自動運行装置が検知し、MRM への移行によって安全に停止する方法が実用化されている。

### ②間接的ミスユースへの対応

車いすで乗車する場合、車いす固定用ベルトを正しく装着していないことは間接的ミスユースに該当する。これは、走行中に前後方向や横方向に力が加わった際、車いすが意図せず移動し、車内で他の構造物や乗客に衝突する危険があるためである。したがって、この例では、車いす固定用ベルトが正しく装着されていない場合には発進を許可しない、あるいは警告を発するなど、発進前や走行中にどのような仕組みで対応するかの方針を策定する。

### ③不具合対応

自動運行装置においては、センサ、アクチュエータ、通信、電源などの構成要素に不具合が生じた場合でも、車両全体が直ちに機能不全に陥ることなく、安全性を維持できるようにしなければならない。特に、走行に関わる基本的な機能（走る・曲がる・止まる）については、不具合発生時にも一定の機能を継続できるような考え方が重要となる。そのための手段としては、例えばフェールオペレーショナルな冗長化の考え方や、許容できないずれを検出して安全側に制御を移行するような安全機構の考え方などが挙げられる。また、システム不具合の原因となり得るサイバー攻撃についても、外部からの情報の入口を制限する、高度な暗号化技術で対応するなど、どのような対処を採るべきかの方針を策定する。

### ④予測行動

運転挙動において将来生じ得るリスクをあらかじめ想定し、安全側に余裕を持たせた行動を取ることが重要であ

る。例えば、信号機のある交差点で右折する場合、信号が青になったからといって即座に進入するのではなく、先行車が右折を完了するまで待機することで、信号が赤に変わった後に交差点内で立ち往生するリスク（道路交通法第五十条第一項相当）を低減できる。また、不測の事態に備えて、常時フリースペースを把握しながら走行することや、人通りの多い道路を走行する際には、歩行者や自転車の予期しない行動を想定して、あらかじめ余裕をもって停止可能な速度で走行するなど、どのような状況を想定し、どの程度の余裕を確保して走行するかについての方針を策定する。

また、周辺車両や道路構造物、道路形状等によって生じる死角については、その要因が固定物由来か移動物由来かを問わず、死角内に歩行者や他車両が存在する可能性を常に考慮した上で運転挙動を計画する必要がある。特に、死角内に存在する可能性のある対象については、その有無や状態を直接把握できないことを前提に、自車両の走路へ進入し衝突に至る可能性を想定し、安全側に余裕を持った判断や挙動を選択する必要がある。固定物に起因する死角については、事前に把握できるという特性を踏まえ、リスクの低減と交通の円滑化の両立を意図した走行戦略の方針を整理する。

このように危険を未然に低減する方針を整理しておくことで、車両が遭遇し得るリスクに体系的に備えることが可能になる。

## 2) リスク対応戦略

リスクに対する未然防止策や予測的な対応を講じたとしても、すべてのリスクを排除することは困難である。そのため、リスクが顕在化し、リスクシナリオが現実化した場合においても、実際の走行状況や環境条件に応じて、他の交通参加者及び乗員の安全を確保するためのリスク対応戦略を策定しておく必要がある。

自動運転車両は、平坦路、交差点、降雨・降雪時など、様々な走行環境条件下で運行する。そのため、リスクの顕在化後に車両がとるべき基本的な対応行動として、①障害回避（反応的）、②緊急操作、及び③MRM への移行といった行動について、走行環境条件に応じた実施方針を体系的に整理しておくことが望ましい。

### ① 障害回避（反応的）

障害回避（反応的）とは、走行中に視認・検知された路面上又は進路近傍の障害に対し、一定の時間的・空間的余裕が残されている状況下で、車両の安定性及び周囲の安全を確保するために、制動や操舵を組み合わせる回避を行う行動を指す。これは、予測的な安全運転とは区別され、また限界的な制御を伴う緊急操作には至らない範囲の反応的な対応である。この行動は、危険を検知した後、可能な限り早い段階で回避操作を行うことを原則とする。例えば、前方の路面上に水たまりや小さな落下物が確認され、そのまま進入した場合に、車両挙動の不安定化や、障害物の跳ね上げ・飛散による周囲への影響といったリスクが顕在化するおそれのある状況が考えられる。このような場合に、走行路外に回避可能なフリースペースが存在し、一定の時間的・空間的余裕が残されているときには、周囲の交通状況を踏まえつつ、緩やかな減速と操舵を組み合わせる進路を調整するなど、車両の安定性及び他の交通参加者の安全を確保するための方針を示す。

### ② 緊急操作

緊急操作とは、想定外のリスクの顕在化やシステム不具合が発生した際に、衝突や車線逸脱などの重大な結果

に至るリスクを回避するために行う突発的な操作を指す。この行動は、周辺環境に配慮しつつ、車両が有する最大限の制御能力を発揮して、迅速かつ確実に対応することを原則とする。例えば、直進中に車両周囲に回避可能なフリースペースがなく、衝突回避のため制動力に頼らざるを得ない場合には、車内アナウンスを行いつつ保舵制御で直進を維持し、最大制動力を積極的に出力して安全に停止するなど、迅速かつ確実に安全を確保するための方針を示す。

### ③MRM

MRM（Minimal Risk Maneuver）とは、走行環境条件を満たさなくなる前に停止できない場合、又は自動運行装置が正常に作動しないおそれがある場合に、車両を MRC（Minimal Risk Condition）に導くための一連の動作を指す。MRC とは、車両が周囲への影響を最小化した形で安全に停止している状態である。この行動は、車両の残存機能を最大限に活用し、確実かつ速やかに MRC へ到達することを原則とする。例えば、路肩に駐車スペースがある場合には路肩に停車する、路肩が狭い道路では減速して駐車可能な箇所まで進み、他車や歩行者に影響を与えない形で停車する、降雪や路面凍結などで制動距離が長くなる状況では、周囲の障害物や道路構造を考慮し、必要に応じて車線上で減速停止する、といった対応が挙げられる。

このように、障害回避・緊急操作・MRM の各行動を走行環境条件ごとに整理しておくことで、環境に応じた一貫性のあるリスク対応方針を構築できる。これにより、リスク対応戦略を具体的な運行条件に即して実効性のあるシステム要求に展開させることができる。

## 3.4 システムへの安全要求の導出

安全コンセプトに基づき、リスクを低減・回避するためにシステムが満たすべき要求を導出する。この要求定義は、システムに「こうしてほしい」と期待する振る舞いや性能を明確に示すものであり、実際の部品仕様や制御ロジックに直接踏み込むものではない。既存の知見や常識に基づいて定義することも可能であるが、過度に設計を制約しないよう注意する。

導出する要求は、通常シナリオ、クリティカルシナリオ、不具合シナリオすべてに対応できるよう整理しなければならない。これにより、各シナリオにおいて自動運行装置が安全に走行するための条件が明確化される。要求には、通常運行の機能だけでなく、性能、異常時の挙動、サイバーセキュリティ、冗長化など、システム全体の安全性を担保するための包括的な条件を含める。さらに、要求は定量化可能なものは数値として整理し、類型化・集約化することで、後続の設計・検証活動にスムーズに展開できる状態にしておく。複数の要求の関連性や優先度も整理する。

加えて、安全コンセプトで示された車両が安全に走行するための基本的な考え方や、それに基づくリスク対応方針が変更された場合でも、要求内容を適切に見直せるよう、その背景や理由をあわせて記録しておく必要がある。

システムへの安全要求は、車両が周囲環境を正しく把握し、適切に判断し、安全な行動を実行するために、DDT の構成要素である「認識」「予測・判断」「制御」の 3 つの観点から体系的に整理することが有効である。

以下に、それぞれの観点において留意すべき事項と、要求定義の方向性を示す。

なお、これら 3 つの観点は説明上は「認識 → 予測・判断 → 制御」の順に述べるものの、要求の厳しさや許容

誤差は必ずしもこの順で一方向に決まるわけではない。例えば、走行軌跡生成における絶対位置精度や進路予測に伴う不確かさの許容誤差といった「予測・判断側の要求」がまず定まり、それに応じて、物標の位置認識精度や自己位置推定精度などの「認識側の要求」が導かれる場合もある。このように、各要求は相互に関連し合うため、個々の要求は、制御側で求められる成立条件を考慮しつつ、整合的に設定する必要がある。

### 3.4.1 認識要求

認識機能は、安全走行の前提となるものであり、自車位置、周辺車両、歩行者、障害物、信号、標識、道路線形、路面状態などの走行環境を正確に把握することを目的としている。したがって、認識要求は、システム全体の安全性を確保するために、車両が走行環境条件下で対象物を正しく認識できることを保証するために定義する。

具体的には、まず、車両として必要な性能要求を明確化する。

#### 物標認識

物標認識としては、走行環境条件下におけるセンシングの対象、検知範囲（距離及び上下左右方向）、静止物体の認識精度（認識率）、認識条件、動的移動物体の認識精度（認識率）、認識条件、分類精度、認識時間などが挙げられる。また、誤認識や誤検知（偽陰性／偽陽性を含む）に関する観点も認識精度として整理し、必要に応じて分類精度や識別精度として区別して定義する。

#### 位置推定

位置推定としては、絶対位置精度、分解能、推定遅延時間、位置情報の更新周期などが挙げられる。

#### 車両状態情報

車両状態情報としては、車速、加速度、ヨーレートなどがあり、これらの精度、分解能、取得遅延許容時間、相互の同期ずれ許容時間などが挙げられる。

#### 不具合対応

認識機能が部分的に失われた場合でも、システム全体として安全を確保するための情報を維持するために、センシング異常の検出及び処置要求を定義する。具体的には、センシングの故障や性能低下を検出する機能や冗長化などのセンシング構成、冗長センサへの切り替え、認識結果の信頼性低下のシステムへの通知、異常時のアルゴリズム補正や認識機能制限などによる最低限取得可能な情報の維持などが含まれる。この場合も、異常検出時間や処置時間など、安全な制御を行うために必要な定量値を指示する必要がある。

#### ロバスト性

環境変化や条件の違いに応じても安定的に認識精度を保つロバスト性要求を定義する。例えば、物標認識では、天候や照度など、急激に変化する環境条件においても、対象物を適切に安定的に検知できる変化への追従性や許容可能な認識低下時間などが挙げられる。

これらの要求により、車両レベルの認識機能が安全コンセプトに沿った形で確実に実現されることを保証する。

### 3.4.2 予測・判断要求

予測・判断機能は、認識結果に基づき、周囲の交通参加者の将来挙動を予測し、自車の安全行動を決定するものである。この機能は、通常シナリオ、クリティカルシナリオ、不具合シナリオにおける車両行動と密接に関連しており、これらのシナリオで車両がどのような行動をとるべきかが、予測・判断機能への要求となる。したがって、予測・判断要求は、システム全体が一貫して安全側の行動を選択できることを保証するために定義する。

#### シナリオ対応

シナリオに応じて車両がとるべき行動を明確化する。例えば、クリティカルシナリオとして、車両直前に歩行者が飛び出す状況が想定される場合、回避可能距離がある場合は制動と操舵を組み合わせることで衝突を避け、緊急操作が必要な場合には直進保舵の状態で最大限の制動力を発揮して停止する、といった操作や行動を定義する。この際、対象物から確保すべき距離や速度低減の目標値など、具体的な定量値も設定し、経路計画に基づく行動が安全に実行されることを保証する。潜在的リスクを先読みして回避可能な計画作成を可能とするために、他車両や歩行者の進路、速度、横断や車線変更などの意図など、時間的に予測すべき対象や方法についても定義する。

#### 性能

車両として必要な性能要求を明確化する。計画した経路については、経路の精度を定義する。計画経路と車両が実際に走行すべき経路との許容誤差を明確化し、位置推定や車両運動の要求精度を考慮した上で安全で許容される範囲内に走行可能であることを保証する。また、前方車両の急停止や予期せぬ障害物の出現など、クリティカルシナリオに該当する状況でも、判断処理が遅延せず、誤判断や不安定な挙動を生じないように、判断時間の制約や経路変更時間などに関する要求を定義する。

#### 不具合対応

予測・判断機能が部分的に失われたり誤作動したりした場合でも、システム全体として安全を維持するために、異常の検出及び処置に関する要求も定義する。その際、前段の認識機能の不具合も含めて考える。具体的には、判断アルゴリズムの出力異常や処理遅延を検出する機能、異常時に安全側の行動（減速、停止、MRM への移行等）に速やかに切り替える手段、判断結果の信頼度のシステムへの通知、異常時における行動範囲や選択肢の制限による最低限の安全確保の方法、などが含まれる。この場合も、異常検出時間や処置時間など、安全な制御を行うために必要な定量値を指示する必要がある。

#### ロバスト性

予測・判断機能が処理負荷の変動や計算負荷の増大により更新周期が乱れる場合でも、安全側の行動選択が維持されることを保証するためのロバスト性要求も定義する。具体的には、交通状況が複雑になった場合や多数の対象物が存在する場合でも、判断や経路更新が要求時間内で実施されること、計算遅延や一時的な入力欠損が発生しても危険な経路計画や不安定な行動が生成されないこと、などが含まれる。

これらにより、予測・判断機能は車両全体の安全性を損なうことなく、通常シナリオからクリティカルシナリオ、不具合シナリオまで一貫して安全側の行動を選択できることを保証する。

### 3.4.3 制御要求

制御機能は、予測・判断機能により決定された安全側の行動を車両運動として具体的に実現し、安全かつ安定した走行状態を維持するものである。したがって、制御要求は、計画された安全行動を正確かつ確実に車両レベルで実行できることを保証するために定義する。

#### 駆動・操舵・制動

具体的には、駆動、操舵、制動の各制御系が、車両ダイナミクスや路面状態に応じて安定かつ滑らかに動作し、急な進路変更や緊急制動が必要な場合でも、乗員の安全性と快適性を両立した制御が行えることを要求する。また、計画経路に沿った車両運動を正確に実現するため、制御系の応答精度や車両挙動の追従精度を明確に定義し、経路生成で算出された位置、速度、加速度、操舵量が安全かつ正確に実現されることを保証する。

#### 不具合対応

制御系に異常が発生した場合でも、システム全体として安全性を維持できるよう、異常検出及び処置に関する要求を定義する。具体的には、制御系の故障や性能低下を検出する機能、冗長構成や代替制御手段の確保、異常時に安全側の挙動（減速、停止、MRM への移行等）へ速やかに切り替える処置、制御逸脱や限界状態を監視して安全側に遷移する仕組みなどが含まれる。この場合も、異常検出時間や処置時間など、制御行動の安全性を担保するために必要な定量値を指示する。

#### ロバスト性

制御機能が外乱や環境変化に対して安定して動作することを保証するために、ロバスト性に関する要求を定義する。例えば、路面摩擦や荷重の変化、風や勾配などの外乱に対しても、車両挙動が許容範囲内で安定的に維持されること、また制御負荷の変動により制御周期や応答が乱れる場合でも、計画経路への追従精度が損なわれないことなどが含まれる。

これらの要求により、制御機能が安全コンセプトに沿った形で確実に実現され、通常走行から緊急時まで、一貫して安定かつ安全な車両挙動を維持できることを保証する。

### 3.4.4 その他要求

上記の 3 分類に加え、システム全体の安全性を支える要素として、以下の要求も併せて定義する必要がある。

- ✓ HMI（Human-Machine Interface）：乗員／乗客、メンテナンス作業など、人との相互作用に関する情報提示及び操作要求。誤操作防止、緊急時の適切な情報伝達などを含む。
- ✓ 通信・連携（Connectivity / Cooperation）：他車・インフラ・運行管理システムとの情報交換に関する要求。通信途絶時の安全性維持も含む。
- ✓ サイバーセキュリティ（Cybersecurity）：外部からの不正アクセスや改ざんに対して、システムの安全機能を確実に保護するための要求。

これらを総合的に整理し、通常シナリオ、クリティカルシナリオ、不具合シナリオのすべてに対して有効に機能する要求体系として構築する。

## 第4章 実現手段の設計 アーキテクチャ設計（性能実現含む）

### 4.1 基本システム設計

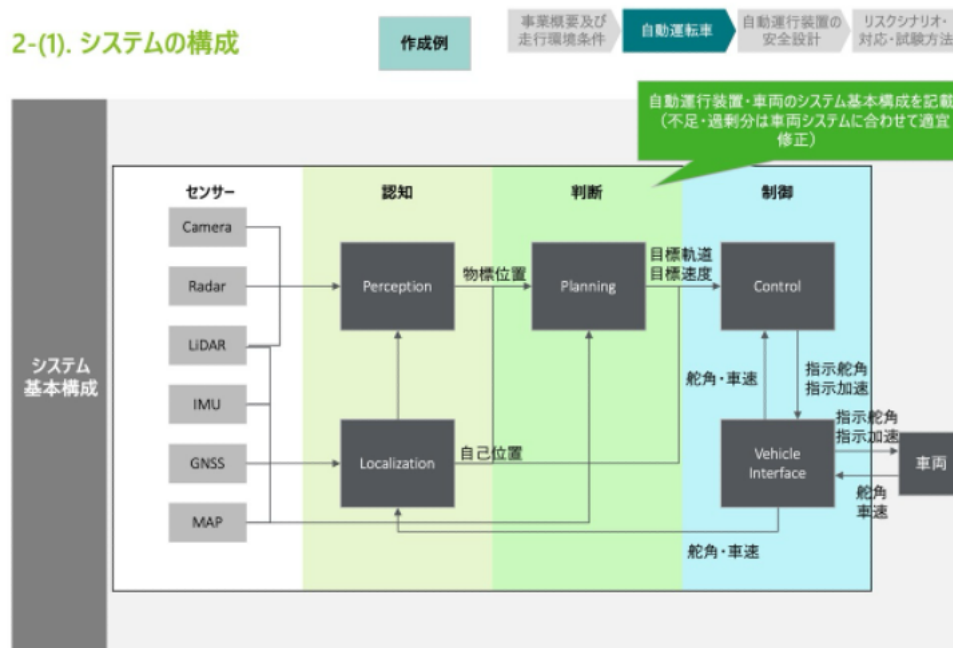
基本システム設計では、第2章で策定した安全走行戦略と、第3章で導出したリスクシナリオ及び安全目標を前提として、車載装置及び周辺運用・支援系の構成を具体化する。

#### 4.1.1 基本方針

自動運行装置は一般に「認識、予測・判断、制御」という階層に分けて整理されることが多く、外部環境を認識し、走行計画を立て、それを車両制御に落とし込むという一連の処理を繰り返す構造をとる。

このとき、センサ、計算プラットフォーム、アクチュエータといった要素技術を、3階層の機能構成と整合するように選定し、配置する必要がある。

#### 2-(1). システムの構成



引用元：「走行環境条件付与手続きに先立ち作成する検討資料」<sup>8</sup>

図 21 システムの構成例

#### 4.1.2 認識機能の設計

認識に関しては、天候、昼夜、対象物の距離や大きさ、道路形状といった条件を踏まえ、カメラ、LiDAR、レーダなどのセンサ種類と必要性能を定める。単一センサではカバーできない場面が存在する場合には、異種センサのフュージョンにより相補的な認識性能を確保する設計とする。センサの搭載位置や視野角は、死角と検知可能範囲に直結するため、走行環境条件を踏まえて最適化することが重要である。

<sup>8</sup> [https://www.mlit.go.jp/jidosha/jidosha\\_tk7\\_000043.html](https://www.mlit.go.jp/jidosha/jidosha_tk7_000043.html) [走行環境条件付与手続きに先立ち作成する検討資料]-[本資料]より。図中の項番は引用元資料の表記であり、本書の章番号ではない。

## 2-(1). システムの構成

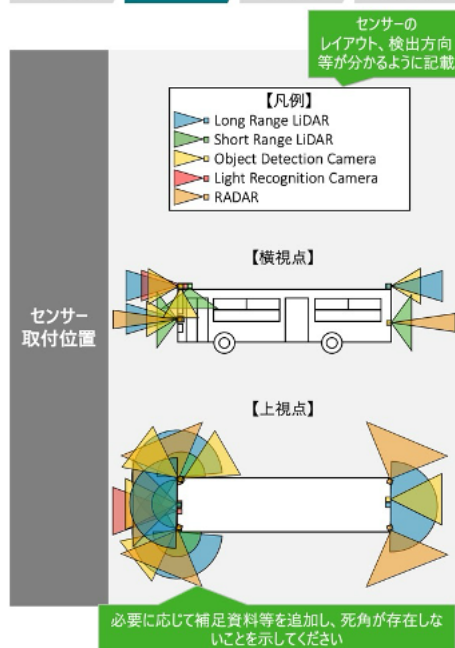
作成例

事業概要及び  
走行環境条件

自動運転車

自動運行装置の  
安全設計

リスクシナリオ・  
対応・試験方法



引用元：「走行環境条件付与手続きに先立ち作成する検討資料」<sup>9</sup>

図 22 センサの構成例

### 4.1.3 計算プラットフォームの設計

計算プラットフォームについては、認識、予測・判断、制御の各機能ブロックに必要な計算量及びレイテンシを見積もり、処理余裕度を持たせたコントローラ構成を検討する。リアルタイム性が不足すると安全走行戦略そのものが実現できなくなるため、安全性要求を満たし得る処理性能と、フェールオーバーや冗長構成を含めた可用性設計が求められる。さらに、ソフトウェア更新やサイバーセキュリティ対策を前提に、セキュアなアップデート機能やアクセス制御を計算プラットフォーム側の仕様として組み込むことが望ましい。

### 4.1.4 車両・アクチュエータ（ACT）性能の設計（制御実現性）

車両・アクチュエータ性能の観点では、最大加減速度、操舵角速度、ブレーキ制動力などを、安全目標と走行戦略から逆算して定義する。通常時の制御性能だけでなく、路面  $\mu$  の低下や突発的な外乱に対しても安全に制御できるよう、制御性能を定義することが必要である。加えて、性能余裕を持たせることが必要である。これは ISO 26262 における技術安全コンセプトとも整合する考え方であり、車両の物理的限界と制御アルゴリズムの設計を一体で扱うことが重要である。

<sup>9</sup> [https://www.mlit.go.jp/jidosha/jidosha\\_tk7\\_000043.html](https://www.mlit.go.jp/jidosha/jidosha_tk7_000043.html) [走行環境条件付与手続きに先立ち作成する検討資料]-[本資料]より。図中の項番は引用元資料の表記であり、本書の章番号ではない。

#### 4.1.5 運用シナリオと外部連携

運用シナリオと外部連携については、車両システムの起動から停止に至る一連のシーケンスと、ODD 内で想定される運行モードを整理し、遠隔監視・インフラ協調・管制システムとの連携方法を設計する。大雨や視界不良など車両単独では検知・判断が難しい状況に対しては、インフラ情報や遠隔監視からの入力と役割分担を明確にし、運行制限や経路変更など運用側の制御も含めたアーキテクチャとして定義する。こうした設計により、車両単体の性能限界だけに依存せず、安全を確保できるシステム全体構成を実現する。

### 4.2 SOTIF（性能限界、ミスユースに対する設計）

SOTIF（Safety of the Intended Functionality）は、ISO 21448 で定義される概念であり、「意図した機能の不十分さ」や「合理的に予見可能なミスユース」によって生じる危険を対象とする。これは、故障を原因とするリスクを扱う機能安全（ISO 26262）とは異なり、ソフトウェアやアルゴリズムの性能限界、環境認識の誤り、運転者や利用者による想定内／想定外の使い方などに起因するリスクを対象とするものである。自動運行装置では、AI やセンサフュージョンなどの高度な機能が多用されるため、SOTIF の観点からの設計・検証が不可欠である。

#### 4.2.1 機能的な不十分性及びトリガー条件の識別

本工程は、SOTIF におけるリスク源を特定するための極めて重要なフェーズである。単なる経験則に頼るのではなく FTA（Fault Tree Analysis）や STPA（System-Theoretic Process Analysis）などの体系的な解析手法により仕様や性能が不十分であることによって危険な挙動が生じる箇所を洗い出す。これが「機能的な不十分性」である。併せて、合理的に予見可能なミスユースや、特定の環境条件（雨天、逆光、反射、地物等）が重なった場合に危険な挙動を引き起こす「トリガー条件」を識別する。例えば、センサのダイナミックレンジ不足により、橋の欄干からの反射を車両や障害物と誤認し、不要な急制動を行うケースは、機能的な不十分性とトリガー条件が組み合わさった典型例である。こうした組み合わせを漏れなく、かつ体系的に抽出し、SOTIF のリスク源を明確化することが後続の SOTIF リスク評価及び改善方策の妥当性を担保する基盤となる。

#### 4.2.2 リスクの評価及び改善方策の適用

識別された危険な挙動について、発生頻度や結果の重大性などを踏まえ、リスクの大きさを評価する。評価の結果、リスクが許容範囲内に収まらない場合には、機能の性能向上、アルゴリズムの改善、構成部品の追加、冗長化、運用条件（ODD）の制約など、様々な改善方策を検討し設計を見直す必要がある。自車単独での対応が難しい場合には、インフラ協調や遠隔監視の活用、あるいはサービスとしての運用ルール（速度制限・経路制限）の変更も含めて検討することが望ましい。このプロセスは一度で完了するものではなく、危険事象の理解が深まるごとに対策を見直し、リスクが受容可能な水準に達するまで反復的に適用していくことが重要である。

### 4.3 機能安全（故障に対する設計）

機能安全は、ISO 26262 で定義される考え方であり、E/E システムの「故障」を原因とする危険を対象とする。自動運行装置においても、故障に起因する危険事象を許容レベルまで低減することが必須であり、第 3 章で実施し

た HARA（Hazard Analysis and Risk Assessment）と安全目標の設定を出発点に、安全コンセプトを具体的なシステム設計へ落とし込むことになる。

#### 4.3.1 システムレベルの安全設計

システムレベルの安全設計では、車両レベルで定義された安全コンセプトを基に、安全目標を実現するための技術的な対策方針（技術安全コンセプト）を策定し、想定する基本システム構成に反映させる。設計時には故障モード影響解析（FMEA）やフォールトツリー解析（FTA）などの手法を用い、各要素の故障がシステム全体や車両挙動に与える影響解析を実施する。このプロセスは安全設計の妥当性を客観的に立証するための重要な解析活動と位置付けられる。解析の結果を基に故障検知、影響緩和、警告などの手段を仕様として定義する。故障時に安全目標を達成できないことが判明した場合は、直ちに設計へのフィードバックを行い構成部品の追加や冗長構成の導入など抜本的な見直しによりシステム構成自体を見直す必要がある。冗長構成とする際には、CCF（Common Cause Failure）のリスクを低減するため、物理的・論理的な独立性を確保したアーキテクチャとすることが重要である。レベル 4 自動運転バスのような可用性要求の高いシステムでは、例えば「図 23 ホットスタンバイを用いた動的冗長構成」に示すような待機系を持つ動的冗長構成やホットスタンバイ構成などが有効な手段となりうる。

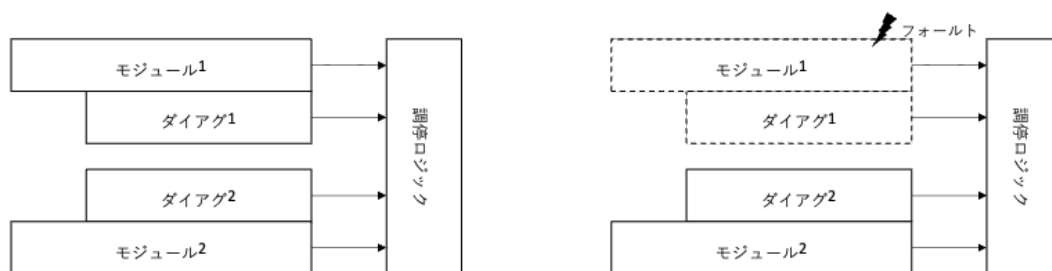


図 23 ホットスタンバイを用いた動的冗長構成

制御モジュール 1 のフォールトをダイアグ 1 により検出したら、モジュール 2 に制御を切り替えることによりフォールトトランスを達成することができる。待機するモジュール 2 は、切替時の機能空白の最小化や制御の継続性を確保するために、稼働状態で待機する、いわゆるホットスタンバイが望ましい。システムが最初のフォールトに対する反応を行った後は冗長性のない動作モードになるので、2 番目のフォールトのリスクを低減するために、この車両動作状態に留まる許容時間を制限する必要がある点には注意を要する。

#### 4.3.2 ハードウェア／ソフトウェアによる実装

システムレベルで定義した安全要求を、ハードウェア及びソフトウェアに具体的な設計として落とし込む。ハードウェア設計では、個々のデバイスの故障率や診断カバレッジを考慮してシステム全体の故障確率を評価し、ISO 26262 で定められる ASIL レベルに応じた安全メカニズム（ECC、パリティチェック、ロックステップ CPU 等）を適用する。ソフトウェア設計では、ASIL に応じた開発プロセスや設計原則（モジュール化、疎結合、明確なインターフェース等）を採用し、システムチックフォールト（設計・実装上のバグ）を低減することが求められる。これは、障害時のフォールトト

レランス設計と密接に関連し、ハードウェアとソフトウェアの協調により安全目標を達成する仕組みを構築する作業である。

## 4.4 サイバーセキュリティプロセス（ISO/SAE 21434）

近年、自動運転車両では、車両機能が多くの外部機器やネットワークと連携するようになり、それに伴いサイバー攻撃リスクも急速に拡大している。とりわけレベル 4 の自動運転バスなどの輸送サービス車両では、運行やサービスの継続性、乗員及び第三者の安全、社会的信頼を確保することが不可欠である。

ISO/SAE 21434 は、こうした車両 E/E システムのライフサイクル全体（構想 → 開発 → 量産・運用 → 廃止）を対象に、サイバーセキュリティを体系的に管理するためのプロセスを示している。本節では、同規格で求められている考え方を参考に、開発から運用まで継続的にリスクを低減し、安全性を確保するための活動を整理する。

### 4.4.1 コンセプトレベルの活動

開発初期段階では、まずアイテム（車両 + E/E システム + 接続サービス）及びその運用環境を明確に定義することが重要である。続いて、資産、攻撃経路、実現可能性などを含む脅威分析・リスク評価（TARA：Threat Analysis & Risk Assessment）を行い、安全性や運行継続性に影響し得るシナリオを特定することが望ましい。

TARA の結果に基づき、サイバーセキュリティ目標を設定し、暗号・鍵管理・認証・セキュア診断・ログ・時刻同期・障害時の安全動作など、技術的又は運用的な対策方針を整理して「サイバーセキュリティコンセプト」としてまとめる。この段階で定義したコンセプトは、以降の設計と検証の基礎となる。

### 4.4.2 サイバーセキュリティ仕様の定義と実装

サイバーセキュリティコンセプトを実現するため、具体的な仕様策定とアーキテクチャ設計を行う。ここでは、ネットワーク分割や境界防御、最小権限、セキュアブート、ランタイム保護、侵入検知・ログ機構などを設計原則として検討することが求められている。

これらの対策方針をハードウェア・ソフトウェアの両面から具体化し、システム／サブシステム／コンポーネント単位へ段階的に展開していく。設計段階では、脆弱性分析を繰り返し行い、十分な堅牢性を確保できるようアーキテクチャを精緻化していくことが推奨される。

### 4.4.3 検証とサイバーセキュリティ妥当性確認（v&v）

実装されたサイバーセキュリティ対策が定義したセキュリティ仕様に適合しているかを確認するため、テストや分析を用いて検証（Verification）を行う。検証では、個々のコンポーネントや統合されたシステムが、設計段階で定めた要求どおりに動作しているかを確かめ、実装と仕様との整合性を評価する。

その後、妥当性確認（Validation）として、システム全体がサイバーセキュリティ目標を達成し、対策が実際の運用環境下で有効に機能しているかを評価する。妥当性確認では、残存する未知の弱点や脆弱性が最小限に抑えられていることを確認するため、脆弱性スキャン、ファジングテスト、ペネトレーションテストなどの手法を活用する。これらの結果を踏まえて、必要に応じて設計や対策方針を見直し、改善を行う。

### 4.4.4 継続的なサイバーセキュリティ活動

量産や運用段階においてもサイバーセキュリティ活動は継続される。運用時の監視によってセキュリティ関連情報を収集し、検知したイベントに対して脆弱性分析や影響評価を行うことが望ましい。必要に応じて、OTA（Over-the-Air）更新などによる是正措置を実施し、対策の適用を継続的に改善していく。

また、サプライチェーン構成や外部環境の変化、部品やソフトウェアの脆弱性発見などに応じて、サイバーセキュリティ体制を定期的に見直すことも重要である。こうした継続的な改善が、ISO/SAE 21434 で求められている「ライフサイクル全体を通じたリスク低減」の考え方につながる。

## 第5章 安全性評価

車両側（自動運行装置を含む車両システム）および自動運転移動サービス（運用・遠隔監視等を含むサービス全体）においては、道路交通法に基づく特定自動運行の許可を受ける主体（特定自動運行実施者等）が、関係ガイドラインや関連法規等との整合の観点から、安全目標、安全走行戦略、リスクシナリオの網羅性や残存リスクなどの妥当性（社会受容性を含む）を説明可能な形で提示する必要がある。

これを支えるため、自動運行装置、自動運転車両、関連するインフラ等を含めた自動運転移動サービスの開発関係者は、担当範囲において、設計した機能が要求どおりに正しく機能していること（verification）及び必要な安全性が確保されていること（validation）の根拠を整備し、特定自動運行実施者等が説明に用いられる形で取りまとめる必要がある。

### 5.1 安全性検証及び妥当性確認の考え方

安全性評価は、V字プロセス左側の設計活動で設計した機能が確実に実装され正しく機能していることを検証（verification）するとともに、最終的に自動運転移動サービスに必要な（妥当）な安全性が確保されていることを確認・証明（validation）する活動である。

安全性を評価する方法としては、仮想環境を用いたシミュレーションやベンチでの模擬テスト、テストコースや走行ルートでの実車走行などを、それぞれの得失などを踏まえた上で適切に組み合わせて、組織的かつ計画的に行う必要がある。

ここで重要なことは、V字プロセスの左側で要求機能や仕様を定義することと並行して、右側で要求が満たされていることを検証する方法を具体的に定義することである。さらに、V字プロセスの左側と右側の活動を一体で進めることである。

言い換えると、V字プロセス左側での要求・目標を定義する作業を進め、コンポーネントやシステムの出来上がりを待って右側の検証作業方法を下から順番に具体化を検討するような方法で仕事を進めると、最終的な目標未達や大きな手戻りが発生しプロジェクトが破綻するおそれがあるため、注意が必要である。

また、自動運行装置及び周辺運用・支援系を含む複雑・大規模なシステム開発においては、V字プロセスの左側よりも右側の検証活動の方が沢山のリソース（人、物（検証マシンパワー、評価テストベンチ）、時間、資金等）を要することが一般的である。したがって、評価、妥当性確認のしやすさを考慮し、V字プロセス左側の設計段階からテストビリティ（テストしやすい機能の実装）を織り込みつつ、V字プロセス右側で考え方、方針に基づき、テスト設計を進め、下位から上位まで段階的・体系的に評価、妥当性確認を行うことが不可欠である。

以下の解説に関連して「図 24 自動運転移動サービスの構成要素と周辺関係者（例） - 再掲」、ならびに「図 25 自動運転移動サービスの開発プロセス定義（事例） - 再掲」を再掲する。

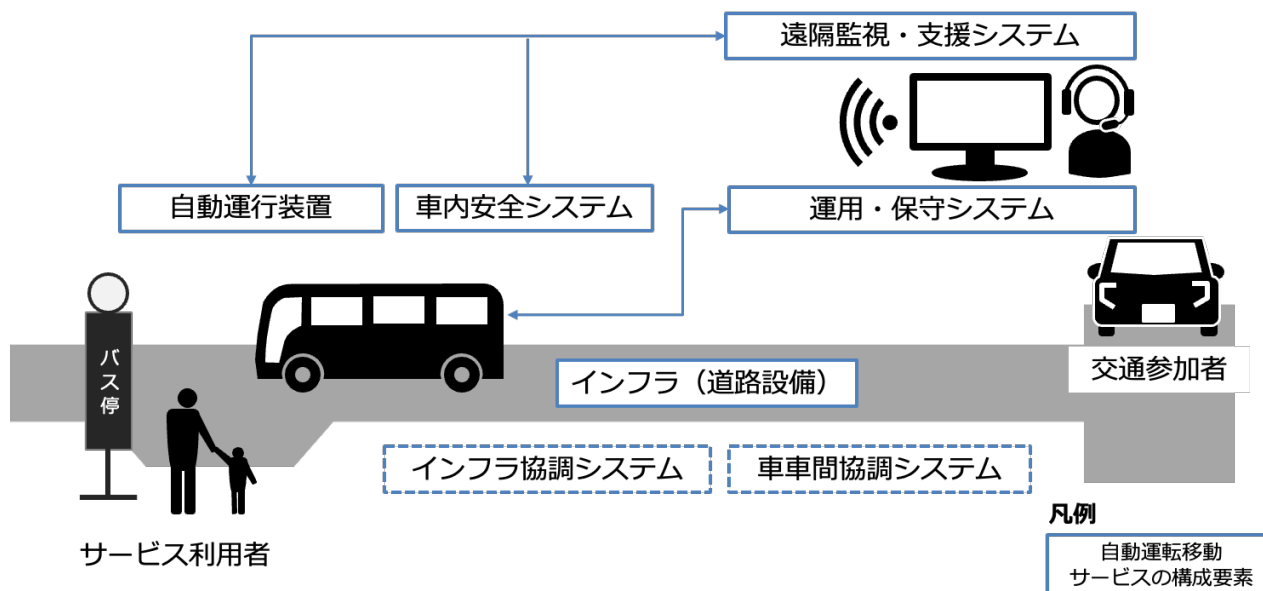


図 24 自動運転移動サービスの構成要素と周辺関係者（例） - 再掲

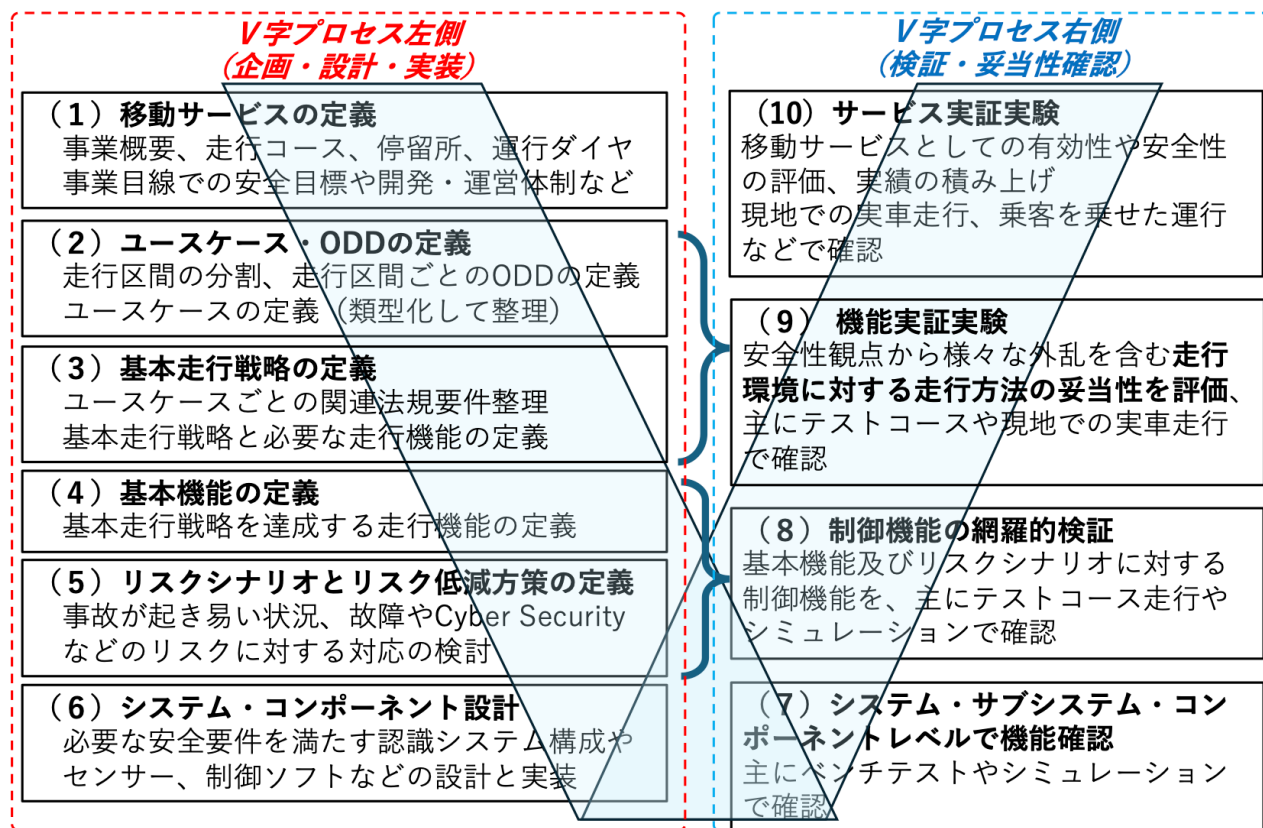


図 25 自動運転移動サービスの開発プロセス定義（事例） - 再掲

## 5.2 安全性検証（verification）

安全性検証は、センサや ECU などコンポーネントレベルから、自動運転車両及びインフラや運行・支援システムなどを含む自動運転移動サービス全体レベルまで、それぞれのレベルにおいて、V 字左側で定義した安全要件や仕様と

実装した対象の機能や性能との一致性を検証する活動である。

### 5.2.1 コンポーネント・サブシステムレベル

ECU やソフトウェアは、試験の自動化や条件の組合せにより検証範囲を拡大しやすい一方、ハードウェアを含むシステムは、個体差やノイズ、温度などの環境条件まで含めて実機で網羅的に確認することは一般に困難である。カタログなど関連情報を確認することに加えて、簡易なモデルを作成して仮想的に影響レベルを把握し V 字プロセス左側にフィードバックするような活動を推奨する。

また、それぞれのコンポーネントに対して V 字プロセス左側で定義した安全目標や要求仕様が正しく定義されていることは、複数のコンポーネントを統合して構成される一段上位のシステムレベルの評価において、システムレベルの要件を満たしていることによって証明される。理想的には、V 字プロセス左側で定義するシステム要求を、下流工程でシステムを構成する複数のコンポーネントごとに要件を分解して割り当てる段階で、外乱やバラツキなども考慮して必要な要件を全てコンポーネントへの要件として具体化出来ていれば、コンポーネントを組み合わせたシステムレベルの評価で問題は生じない。しかしながら、自動運転のような複雑・大規模かつ高い性能を要求されるシステムでは難しい。

対策としては、V 字プロセス左側で「一定の安全マージン」を加えてロバスト性の高い設計に配慮することが必要である。また、安全上の重要機能については、必要十分な安全マージンを定義することが難しい場合もあるので、対象機能をブラックボックスとして扱い、機能失陥時のリスクに対して冗長性を持たせたり、出力値に一定のガードをかけて急激な変化を抑制するなどの対応を検討する必要がある。

### 5.2.2 車両システム・自動運転移動サービスレベル

車両システム（自動運行装置を含む車両側）および自動運転移動サービス（運用・遠隔監視等を含むサービス全体）を対象として安全設計・評価を行う場合、V 字プロセスの左側で安全目標を定義する際に、同時にテストビリティ（検証可能性）を確保することが重要である。すなわち、目標が達成されたことを確認するための評価指標、評価条件、評価方法を具体的に定義し、V 字プロセスの右側で実施可能な検証計画へ接続する必要がある。例えば、「[距離] km、[回数] 回、[日数] 日の走行において操作介入が[上限回数] 回以下」といった運行実績に基づく指標、または「[人数] 人の試乗者へのアンケート結果から、『安心できる』との回答が N %以上」といった必要性評価の指標が考えられる。V 字プロセスの左側（目標定義）と右側（確認方法）を一体として設計しない場合、目標を定義しても達成状況を客観的に確認できないおそれがあることに留意すること。

## 5.3 安全妥当性確認（validation）

安全妥当性の確認は、V 字プロセス左側で定義した安全目標や要求仕様が定量的・論理的かつ社会的な観点からも妥当であることを証明するための活動である。

### 5.3.1 コンポーネント・サブシステムレベル

コンポーネント・サブシステムレベルでは、移動サービスや車載装置及び周辺運用・支援系など上位レイヤからの要求を満たすように設計することに尽きるので、このレベルでの「安全妥当性の確認」を目的とした特段の活動を行う必

要はない。

### 5.3.2 移動サービスレベル

自動運転移動サービスレベルにおいては、関連法規などとの整合性の観点から、安全目標、安全走行戦略、リスクシナリオの網羅性や残存リスクなどの妥当性（社会受容性を含む）を説明可能な形で示す必要がある。

そのための主要な材料として、5.4 で述べるシミュレーション、テストコース、実路走行等の評価結果（ログ、事象分析、再現試験結果を含む）に加え、社会受容性に関する利用者・関係者のフィードバック（アンケート、ヒアリング等）である。

実路での実証はレアケースへの遭遇確率が低く、データ収集・解析にも手間と費用を要するため、プロジェクト企画の初期段階から、テスト条件を作り込み、試験結果から条件成立や期待どおりの挙動を判断できるようにする度合い（テストビリティ）を設計に織り込む必要がある。具体的には、運行・制御・認識の状態や判断根拠を追跡できるログ／診断出力（モニタリング、記録・保存、可視化、イベントタグ等）、及び同一事象の再現と切り分けを可能にする仕組み（入力ログの再生[リプレイ]、テストモード、故障注入／通信遅延・センサ欠落等の条件付与）をあらかじめ実装する観点で検討を進めることが重要である。

また、アンケート情報を有効活用するためには、あらかじめ仮説を定義し、結果が仮説検証に結びつく設計（設問、対象者、評価観点）とするなど、専門知識の獲得や実施例の参照など事前の取組が重要な点に留意することが重要である。

## 5.4 シミュレーション、テストコースや実路走行による評価

安全性評価、安全妥当性確認の手段である、シミュレーション、テストコースや実路走行の得失について述べる。

### 5.4.1 シミュレーション（仮想テスト）による安全性評価

シミュレーションが実車の振る舞いを高精度に再現することによって、実機では確認が難しい特殊なシナリオも含めた網羅性の高い検証が可能となる。一方で、精密モデルの開発に要する初期投資の負担が大きいため、再利用や機能更新などライフサイクルを考慮した導入計画の策定が重要である。また、シミュレーションで検証するシナリオの一部を実車テストでも実施し、両者の比較を通じてシミュレーション結果の妥当性と有効性を確認する必要がある。

【具体的な活用例】

- ✓ 夜や雨・霧などの天候変化に対するカメラシステムの障害物認識性能の評価
- ✓ 死角からの歩行者飛び出しに対する車両挙動（制動や衝突回避などの制御ロジック）の評価

### 5.4.2 テストコースにおける模擬環境での安全性評価

走行コース（公道）では難しい危険なシナリオにおける実車動作の検証や、雨や明るさなど定量的な条件で繰り返し評価が可能である。一方、場所（試験設備）や実験車両の仕立てなど仕掛けが大がかりで時間と費用が嵩む、走行コースとの整合証明が必要である。

#### 【具体的な活用例】

- ✓ Euro NCAP のテストプロトコル等に基づく衝突回避（AEB 等）及び車線維持支援（LSS）のシナリオ試験・性能評価
- ✓ 悪環境試験設備を使用した、実車の障害物や信号認識性能評価

### 5.4.3 実車・実路走行による妥当性確認

実車・実路走行では、安全妥当性の証明に有効なデータが得られる。一方、レアケース・危険シナリオの確認は難しく、また、獲得できるデータ量は限られる。

#### 【具体的な活用例】

- ✓ 公道実証実験による、自動運行装置の誤作動やヒヤリハット、操作介入の頻度評価など
- ✓ 一般乗客を対象とした試乗会による、ユーザ体験のコメント収集など

「表 7 シミュレーションと、テストコース評価、実路での実車試験に関する PROS、CONS」に、シミュレーション、テストコースや実路での実車試験に関する利点（PROS）と課題（CONS）を記す。

表 7 シミュレーションと、テストコース評価、実路での実車試験に関する PROS、CONS

| 評価手法     | Q（品質）                                              | C（コスト）                                               | D（納期）                                             |
|----------|----------------------------------------------------|------------------------------------------------------|---------------------------------------------------|
| シミュレーション | PROS：多様なシナリオを網羅的に繰り返し検証可能<br>CONS：実環境との乖離、モデル精度に依存 | PROS：実車不要で低コスト<br>CONS：高精度モデルやツール導入の初期投資負担が大きい       | PROS：環境構築後は短期間に大量の試験が可能<br>CONS：モデル構築や検証に時間がかかる   |
| テストコース評価 | PROS：公道では難しい評価が可能<br>CONS：模擬環境なので評価条件は限定的          | PROS：比較的安価に実施できる<br>CONS：車両準備や設備使用コストが負担             | PROS：比較的早期に集中して実施できる<br>CONS：準備や日程調整等に手間がかかる      |
| 実路での実車試験 | PROS：安全妥当性証明に有効なデータを獲得できる<br>CONS：外的要因に左右され再現性が低い  | PROS：試験のための準備は比較的少ない<br>CONS：長期走行やデータ収集に必要なコスト負担が大きい | PROS：比較的早期に実施可能<br>CONS：必要な数のデータを獲得するために長期間の試験が必要 |

## 5.5 先行開発・一品生産的なプロジェクトでの留意点

OEM で実施する乗用車の量産開発のように、従前の技術やノウハウの蓄積と実績、階層的なサプライチェーンのような役割分担の仕組みと十分なリソース、採算に裏打ちされた開発費用が確保されるプロジェクトとは違って、自動運転のような先行開発・一品生産的なプロジェクトで生じやすい問題・課題への配慮について述べる。

### 5.5.1 要求定義や安全目標具体化の難しさ

法規を守らない周辺交通参加者に対しても出来る限りリスクを回避するために、必要な安全性を確保（How

safe is safe enough?) する命題に対して、実装設計レベルの要求値や仕様を定義することは非常に難しい。また、後述するように実現手段の目途が無いまま、実現困難な目標や達成可能な安易な目標を定義してプロジェクトを進めると後に大きな手戻りが生じるリスクもある。

留意点としては、上流工程では、様々な前提条件や考え方を示した上で仮の目標を定義し、下流工程との対話を重ねながら「擦り合わせ」的に作業を進め、プロジェクト全体マネジメントの仕組みの下に、必要に応じて目標の見直しも行いながら柔軟に進める必要がある。

### 5.5.2 部品やサブシステムの性能把握の難しさ

先行開発・一品生産的な開発では、専用部品やサブシステムなどを調達することは難しく、既存で類似のものを流用する必要がある。その際、調達先から使用目的に関する性能データの提供や部分的改造をお願いすることが難しく、必要な性能が確保できる確証なく車両に搭載し実装しながら性能評価するしかないケースもある。

留意点としては、第一にできるだけ実績のあるものを調達すること、やむなく独自の要素技術開発に着手する際は、必要なリソースを確保し失敗するリスクも踏まえた開発計画を関係者で共有すること。また、「分からないことには対応できない」では先に進めないので、許容可能な範囲で安全マージン（例えば、カタログよりもN%性能低下・応答遅れ等）を足して設計すること。また前述のように、機能失陥時のリスクに対して冗長性を持たせたり、出力値に一定のガードをかけて急激な変化を抑制するなどの対応を検討する必要がある。

### 5.5.3 開発体制の脆弱さに起因する難しさ

一般的に、V字プロセスの上流と下流では、下流ほど、また設計よりも評価に沢山のリソースを必要とする。しかしながら、先行開発・一品生産的なプロジェクトにおいては十分なリソースを確保することは難しい。V字プロセス左側の設計工程を不十分なまま実装作業を進めると、かろうじて実車・実路走行を開始できても安全性検証作業で多くの不具合が発生し、不具合の解析や対策が進まず先に進めなくなるリスクがある。

留意点としては、最終目標：社会実装（営業運行等）までのマイルストーンを具体化し、プロジェクト計画の策定や推進においては、仮の目標値や要求を定義して上流から下流まで降ろして下流からのフィードバックを上流に返して修正するサイクルを短期間で繰り返し、目標値や要求の具体化・適正化を進めること。また、データ管理やノウハウの形式知化などの優先度が下がり作業が滞った中で要員の病気や交代などが発生すると致命的なリスクとなるので、開発環境の充実にリソースを割くなどの対策を講じること。

### 5.5.4 拙速な実車・実路走行の実証によるリスク

自動運転移動サービスの黎明期等においては、プロジェクトの成果を関係者に示し易いことから「実車・実路走行」の早期実施が過度に重視されることがある。

その結果、安全を設計工程で作こむために重要な要求定義や検証方法（評価指標・条件・手順）等の具体化が不十分なままに、車両製作や制御システム実装を進めてしまい、実証走行（車両及び自動運転サービスの安全妥当性確認）において重大な不具合が顕在化し、事故が発生したり、手戻りが増大したり等、社会実装が難しくなるリスクがある。

このため、安全性・妥当性を確認する方法として、仮想環境を用いたシミュレーション、テストベンチでの模擬テスト、テストコースまたは走行ルートでの実車走行を、作業工程ごとに適切に組み合わせ、組織的かつ計画的に実施することが重要である。

## 第6章 ソフトウェアアップデート

本章では、自動運転車両が開発、製造された後の市場で使用されている状況において、安全確保のために車両制作者・自動運転移動サービスのシステム提供者・車両使用者が実施すべき内容を述べる。

ソフトウェアアップデートは市場で使用中の車に機能を追加したり、仕様変更やサイバーセキュリティ対策等を行ったりするのに適した技術である。一方で、ソフトウェアアップデートの際には正しい更新用ソフトウェアが配布され、インストールされて意図通りの更新が行われること、更新の実施中に更新行為が車両機能に影響を及ぼすかどうかを確認し、必要な対策を講じることは、車両と乗員の安全を確保するために不可欠である。サイバーセキュリティ／ソフトウェアアップデートに関する要件は「道路運送車両の保安基準」第 17 条の 2 第 3 項及び同第 4 項に規定され、詳細は告示で定められる。また、電気通信回線等を用いて車両のプログラム等を提供し改変を行わせる場合など、内容によっては道路運送車両法第 99 条の 3 に基づく特定改造許可制度の対象となり得る。法規適合への対応の参考となる ISO 標準として ISO/SAE 21434、ISO24089 も存在している。2022 年 7 月以降に認可を取得する自動車は、基本的に上述の基準に適合していることが必要となる。自動車メーカーが上記規則への適合を前提に開発製造した車両をそのまま自動運転移動サービスに使用するのであれば問題はないと考えられるが、サービス事業者が独自に車両を開発し、使用する場合には注意が必要である。以下に主な留意点を述べる。

### 6.1 ソフトウェアアップデート機能の実装

ソフトウェアアップデートを実施するためには、自動車製作者・システム提供者が車両とソフトウェアアップデートを実施するツール双方にアップデートを実行するための機能を実装することが必要である。専用ツールを用いて有線で車両に接続し、ソフトウェアアップデートを実施する機能は、すでにほとんどの車両において実装されている。一方で、現在オーナーカーを中心に採用が進んでいる機能として、無線通信を用いてソフトウェアアップデートを実施する機能（以下、OTA という）がある。これは、無線通信を行うことから、車載機と通信インフラ双方の開発と実装が必要になる機能である。移動サービスに用いられる車両においては、サービス事業者により日常の車両メンテナンスでソフトウェアアップデート対応が可能な場合が多いことから、OTA の採用は先の話になると予想されている。OTA の実装には、ソフトウェアアップデート実施の際の確実性及び整合性を確保するためのプロセスを組織として有している必要がある。これには不正な改ざんの防止、対象車両の特定、ハードウェアとソフトウェアの構成情報、変更履歴の把握、使用者への必要な情報提供などが含まれる。

### 6.2 使用中のサイバーセキュリティ確保のためのソフトウェアアップデートの実施

自動運転移動サービスの構成要素のうち、更新対象となる車載装置及び周辺運用・支援系では、通常の保守点検に加え、サイバーセキュリティを確保するために自動運転車両のソフトウェアアップデートを適切に実施する必要がある。確保されるべきサイバーセキュリティの要件、対応方法については第 4 章にて記載されているため、ここではサイバーセキュリティ対応に限定せず、ソフトウェアアップデート実施時の主な留意点を記載する。

- ✓ ソフトウェアアップデートを実施する際に、安全に実施できる環境が整っているかを確認する。例えば、ソフトウェアアップデートの実施中には関連機能を停止させる必要がある場合がある。その場合、アップデートの実施者は当該機能が作動しなくても車両の安全に影響を及ぼさない状態であることを確認してから実施する

必要がある。例として、ブレーキ関連の機能が停止する場合、駆動輪がエンジン動力から完全に切り離され、車両が完全に停止している状態であることが挙げられる。また、ソフトウェアアップデートを OTA により実施する場合には、訓練された整備士ではない一般のユーザーがアップデート作業を実施するケースが想定される。その場合、必要な電源を確保する方法等、一般のユーザーを想定した情報提供も必要となる。

- ✓ 上記のソフトウェアアップデートの実施にあたり、前述のとおり自動車メーカーが製造した量産車両をそのまま使っているのであれば、メーカーの責任において必要なソフトウェアアップデートの抽出、対象車両の特定、使用者への通知等が行われることが想定される。この場合、使用者はその指示に従ってソフトウェアアップデートを実施すればよいため、特に大きな課題はないと考えられる。一方で、自動運転移動サービス実現のためにサービス事業者が遠隔監視／遠隔操作システムの搭載等の改造を車両に行っていた場合には、その部分はサービス事業者が責任を負って実施することになり、管理体制の構築も必要である。

## 7.1 編集委員会 構成員名簿

谷川 浩 一般財団法人 日本自動車研究所 研究主幹

|        |                                       |       |
|--------|---------------------------------------|-------|
| 田中 伸一郎 | 元) RTL4 安全走行戦略 WG 委員 (ウーブン・バイ・トヨタ)    |       |
| 平野 薫   | DNV ビジネス・アシュアランス・ジャパン株式会社 テクニカルエキスパート |       |
| 星野 正喜  | 株式会社 クリスタライト                          | フェロー  |
| 福田 和良  | 一般財団法人 日本自動車研究所                       | 主席研究員 |
| 深澤 竜三  | 一般財団法人 日本自動車研究所                       | 主任研究員 |

平野 清美      株式会社 キーノ コンサルティング

以上