# 令和 5 年度

# 安全設計・評価ガイドブック
# (RoAD to the L4)

経済産業省 製造産業局 自動車課 モビリティ DX 室
国土交通省 自動車局 技術・環境政策課 自動運転戦略室

（委託先）
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

第 1 版 (2023.8)

# 目次

# 1　はじめに

## 1.1　背景

平成 30 年 4 月に開催された高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進戦略会議にて、自動運転車の安全性に関わる「自動運転に係る制度整備大綱」が定められた。この大綱の中で、自動運転に関係する道路交通関連法制度の見直しについて政府全体の方向性がとりまとめられているが、2020 年から 2025 年頃の自動運転導入初期段階では、国際的な議論を踏まえた安全基準や安全性評価手法は制定されないことが予想される。そこで当面の間、整備が進む関係法令のほかに、安全性を適切に考慮した自動運転車の開発や実用化を促すことを目的として、

- **「自動運転車の安全技術ガイドライン 」（平成 30 年 9 月国土交通省自動車局）**
- **「ラストマイル自動運転車両システム基本設計書 」（令和 2 年 7 月国土交通省自動車局先進安全自動車推進検討会）**
- **「限定地域での無人自動運転移動サービスにおいて旅客自動車運送事業者が安全性・利便性を確保するためのガイドライン 」（令和元年 6 月国土交通省自動車局）**

等が示されており、ここで示された理念や考え方などは関係者間で共有されている。

さらに、自動運転の安全性を評価するための手法が必要であると考えられており、「自動運転の安全性評価フレームワーク Ver1.0、Ver2.0、Ver3.0」（Ver1.0 @ 2020 年 10 月、Ver2.0 @ 2021 年 12 月、Ver3.0 @ 2022 年 12 月 一般社団法人日本自動車工業会自動運転部会 AD 安全性評価分科会）が公開されている。

限定空間における自動運転移動サービスは、一般道路等で運用する場合に比べると安全性を確保しやすく、早期実現が期待される。そこで、限定空間における実用化に向けて、**「自動運転車の運行設計領域 (ODD: Operational Design Domain) において、自動運転システムが引き起こす人身事故であって、合理的に予見可能で防止可能な事故が生じないこと」**という安全目標を達成するためには、

1. 危険が予想されるケース[*1]を洗い出し、
2. 傷害度や発生頻度なども考慮してリスクの大きさを定義し、
3. 安全目標に対して許容できるレベルまでリスクを低減するための安全方策[*2]を定義・実装し、
4. 必要に応じてテストコース走行や実証実験等を通じて確認する、

必要がある。

しかしながら、自動運転移動サービスや自動運転車両・制御システムなどの開発は関係者にとって未経験の先端的な取組みであるうえに、過去の取組み事例や実績データなども乏しく、「合理的に予見可能で防止可能な事故」を論理的かつ定量的に定義すること[*3]は非常に難しいと言わざるをえない。自動運転移動サービスにとって必要な安全性が確実かつ効率よく確保されるためには、社会受容性の確立などに向けて協調領域として取り組む課題があると思われる。

将来的には高い事業意欲や優れたアイデア・技術を有するような事業者が自動運転移動サービスに新規参入することによって、社会実装が拡大・加速化することが期待されている。しかし、ADAS (Advanced Driver-Assistance System: 先進運転支援システム) など車載制御システムの開発経験豊富な自動車メーカやシステムサプライヤなどに比べると、大学や IT 系のベンチャー企業などは、たとえばノイズや故障などに対してロバストな安全性を設計で確保するノウハウや経験が浅い恐れがある。したがって、実証実験や営業運行の段階で、最悪の場合には事故が発生する懸念があり、一定の範囲は協調領域として形式知化することが望ましいといえよう。

自動運転を取り巻く上述のような現状に加えて、少子高齢化や過疎化などに起因する社会問題の拡大懸念を背景に、自動運転移動サービスの早期実用化に向けた「**自動運転レベル 4 等先進モビリティサービス研究開発社会実装プロジェクト（RoAD to the L4）**」が令和 3 年度よりスタートした。傘下のテーマ 2 事業では、「2025 年度までに、多様なエリアで、多様な車両を用いた無人自動運転サービス（レベル 4）を 50 カ所程度で実現」を目標に「無人自動運転サービスの対象エリア、車両を拡大するとともに、事業性を向上す

[*1] 歩行者脇通過や交差点通過などにおける歩行者や交差車両との衝突など。

[*2] たとえば、障害物検出性能の高度化、一旦停止や低速走行、ガードレール設置、インフラ連携・遠隔監視の活用なども含め、総合的な観点から適切な安全対策を組み合わせて安全性を確保すること。

[*3] たとえば、歩行者の飛出しや交差点での周辺車両の動きなど。

る」ことに取り組んでいる。この目標達成のためには、サービス性（利用ニーズに合致した便利なサービスの提供)、事業性（自動運転移動サービス事業を継続可能な採算性)、そして一定レベル以上の安全性が確保されたうえで、社会受容性を確立することが必要条件となる。これらのサービス性、事業性、安全性、社会受容性などは相互に深い関連がある。たとえば、サービス性を確保しようとすれば、停止や減速を少なくして速達性のあるサービスが求められるが、安全な走行環境の整備や自動運転車両の障害物認識性能の高度化などのコストは事業性を低下させる。社会受容性の観点からは、周辺の歩行者や一般車両のそれぞれが安全な行動をとることになれば、サービス性や事業性の悪化を抑えつつ安全性を確保することが期待できる。すなわち、安全性を確保するための取組みは、自動運転移動サービス事業者や自動運転車両開発者等が中心となって推進する必要はあるものの、地域住民や利用者、自治体などとも安全に関する情報を一定レベルで共有し、社会全体として安全確保に取り組むことが重要といえよう。

## 1.2　目的

この安全設計・評価ガイドブックは、自動運転移動サービスに必要な安全性を確保した設計を、確実かつ効率的に行うための一連の実施項目、実施方法、注意点、実施事例等を記載するものであり、安全設計の知見や経験が乏しい自動運転移動サービス事業者や自動運転車両開発者などが参考書・手引書として有効活用することを目指す。

その際には、実証実験や営業運行の申請が円滑に（＝確実かつ効率良く）審査・認可されることが、前記事業者にとって最も関心があり、期待することであろうことに留意すべきである。ただし、記載する項目や粒度によっては競争領域に係わるなどの懸念もあるため、審査・認可の申請にあたっては、本ガイドブックを参考にするだけでなく、自動運転移動サービス事業者および自動運転車両開発者自身で、個別状況に応じた安全性の確保に係る精査が必要である点に留意されたい。

なお、本ガイドブックは、各関係者の視点から幅広く意見や要望を聴くことで、必要に応じて内容の追加や修正を行いながら改善を続けていく。

# 2　本ガイドブックが対象とする車両・サービス

第 2 章では、安全設計・評価ガイドブックにおける対象範囲を定義する。

## 2.1　自動運転レベル

本「安全設計・評価ガイドブック」は、国土交通省の「自動運転車の安全技術ガイドライン」（平成 30 年 9 月）に準拠する内容となっている。したがって、本書における運転の自動化レベルの定義は、「自動運転車の安全技術ガイドライン」で引用する「自動運転に係る制度整備大綱」（平成 30 年 4 月）で用いる SAE International の J3016（2016 年 9 月）[*4]およびその日本語参考訳である JASO TP 180041（2018 年 2 月）の定義（表 1 参照）を採用する。

表 1　運転の自動化レベルの定義

| レベル | 名称 | 定義 | 動的運転タスク ※2 | | 動的運転タスクの作動継続が困難な場合への応答 ※3 | 限定領域 ※4 |
|---|---|---|---|---|---|---|
| | | | 持続的な横・縦の車両運動制御 | 対象物・事象の検知および応答 | | |
| 運転者が一部または全ての動的運転タスクを実行 | | | | | | |
| 0 | 運転自動化なし | 運転者が全ての動的運転タスクを実行。（予防安全システムによって支援されている場合も含む ※1） | 運転者 | 運転者 | 運転者 | 適用外 |
| 1 | 運転支援 | 運転自動化システムが動的運転タスクの縦方向または横方向のいずれかの車両運動制御のサブタスクを、特定の限定領域において持続的に実行。この際、運転者は残りの動的運転タスクを実行することが期待される。 | 運転者とシステム | 運転者 | 運転者 | 限定的 |
| 2 | 部分運転自動化 | 運転自動化システムが動的運転タスクの縦方向および横方向両方の車両運動制御のサブタスクを、特定の限定領域において持続的に実行。この際、運転者は動的運転タスクのサブタスクである対象物・事象の検知および応答することが期待される。 | システム | 運転者 | 運転者 | 限定的 |
| 自動運転システムが（作動時は）全ての動的運転タスクを実行 | | | | | | |
| 3 | 条件付き運転自動化 | 運転自動化システムが全ての動的運転タスクを限定領域において持続的に実行。この際、作動継続が困難な場合への応答準備が出来ている利用者は、自動システムが出した介入の要求を受け容れ、適切に応答することが期待される。 | システム | システム | 作動継続が困難な場合への応答準備ができている利用者（代替中運転者へ） | 限定的 |
| 4 | 高度運転自動化 | 運転自動化システムが全ての動的運転タスクおよび作動継続が困難な場合への応答を、限定領域において持続的に実行。作動継続が困難な場合、利用者が介入の要求に応答することは期待されない。 | システム | システム | システム | 限定的 |
| 5 | 完全運転自動化 | 運転自動化システムが全ての動的運転タスクおよび作動継続が困難な場合への応答を、持続的かつ無制限に実行。作動継続が困難な場合、利用者が介入の要求に応答することは期待されない。 | システム | システム | システム | 限定なし |

[*4] なお、SAE J3016 は、2018 年 6 月、2021 年 4 月に改訂されており、必要に応じて今後も見直しが行われる予定である。

表 1 に示すように、運転の自動化レベルは互いに排他的な六つのレベルで分類される。この分類の中心は、運転者または利用者および運転自動化システムそれぞれの役割にある。また、運転自動化システムの機能性が変わると、運転者または利用者の役割が変わる。

なお、表 1 中の※ 1〜※ 4 の注釈を以下に示す。

※ 1: 横滑り防止装置および衝突被害軽減ブレーキ等の予防安全システム、および車線逸脱防止支援装置等の運転支援システムは、動的タスクの一部またはすべてを持続的には実行していないので、運転自動化のレベル分類範囲から除外するものとする。これらの支援システムは、単に潜在的な状況において瞬間的な介入を提供するものであり、運転者の役割が変更されたり取り除かれたりするわけではない。

※ 2: 動的運転タスク (DDT: Dynamic Driving Task) とは、道路交通において車両を操作する際にリアルタイムで行う必要があるすべての操作上および戦術上の機能である。ただし、行程計画ならびに経由地の選択等の戦略上の機能を除く。詳細については、図 1[*5]を参照されたい。

※ 3: 動的運転タスクを実行するシステムに関連したシステム故障が発生した後、または限定領域離脱時に、動的運転タスクを実行するか、または最小リスク状態を達成するための応答を表す。

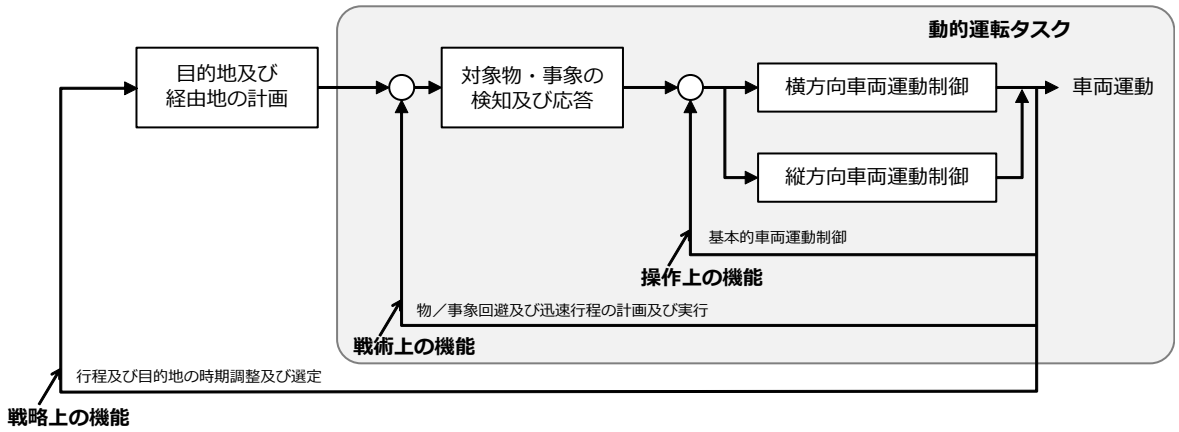



図 1　動的運転タスクの概略図（出典：JASO テクニカルペーパ「自動車用運転自動化システムのレベル分類及び定義」（JASO TP 18004:2018））

[*5] この図は制御図ではない点に注意されたい。

※ 4: 本ガイドブックにおける運行設計領域 (ODD) は、「自動運転に係る制度整備大綱」「SAE J3016」「JASO TP 180041」においては限定領域と表記されている。

## 2.2 本ガイドブックの対象範囲

本「安全設計・評価ガイドブック」の対象は、自動運転移動サービスのためのシステムとする。表 1 に示す「自動運転レベル定義」においては、赤枠内（レベル 4）が該当する。

自動運転移動サービスのためのシステムには以下が挙げられる。

- 自動走行システム
- 車内安全システム
- 遠隔監視・支援システム
- インフラ（地中に埋設した電磁誘導線、磁気マーカ等）
- 運用・保守システム
- インフラ協調システム（ブラインドモニタ、信号連携等）
- 車車間協調システム

ただし、インフラ協調システムと車車間協調システムについては、2023 年 8 月時点では対象外とする点には注意されたい。自動運転を機能させるために密接に繋がっているサブシステムを含むシステム全体が安全設計に必要な対象である。自動運転システムのサブシステム構成を図 2 に、各サブシステムの機能概要を表 2 に記載する。

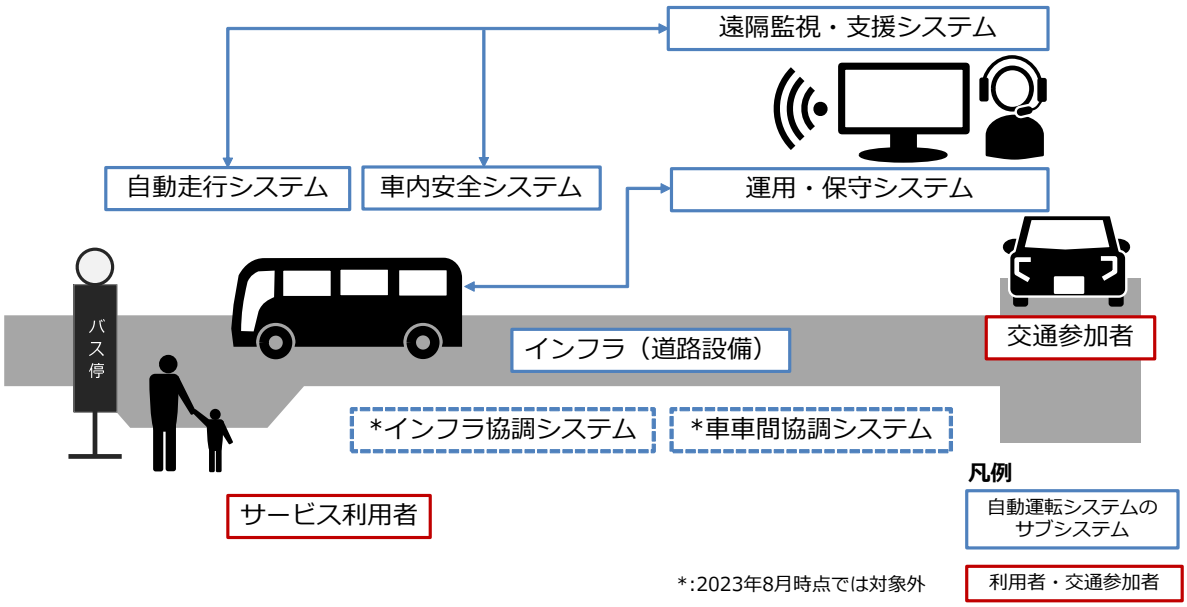



図 2　自動運転システムのサブシステム構成

表 2　自動運転システムのサブシステム構成とその機能（表内*は 2023 年 8 月時点では対象外）

| サブシステム | 機能要素 | 機能概要 |
|---|---|---|
| 自動走行システム | 走行系 | 「走る・曲がる・止まる」を実現する機能 |
| | 認識系 | 周辺環境の認識、自己位置を推定する機能 |
| | 制御系 | 認識系の情報を基に走行系を操って走行制御する機能 |
| 車内安全システム | HMI系 | 乗客・乗務員向けのヒューマンマシンインタフェース機能 |
| | 監視・記録系 | 車内状況の監視、走行の記録などの機能 |
| 遠隔監視・支援システム | 監視系 | 車両の走行状況や車内状況を監視する機能 |
| | 支援系 | 運行サービス・車内安全に関して遠隔対応する機能 |
| インフラ | 道路設備 | 磁気マーカ、バーゲートなど |
| 運用・保守システム | 点検系 | 始業点検、定期点検など |
| | 緊急時対応系 | 現場駆け付け対応、保安要員の配置など |
| *インフラ協調システム | 路車協調系 | ブラインドモニタ、信号連携等を実現するインフラセンサ・通信設備など |
| *車車間協調システム | 車車協調系 | 車車間通信設備など |

# 3　自動運転車の安全性に関する基本的な考え方

## 3.1　各種ガイドラインにおける自動運転車の安全設計に対する考え方

国土交通省自動車局が発行した「自動運転車の安全技術ガイドライン（平成 30 年度)」に示されているように、自動運転車は予見可能かつ防止可能な事故が起きないように安全対策を行うことが求められている。以下にガイドラインの文面を引用する。

> 『本ガイドラインでは、自動運転の実現において、「自動運転システムが引き起こす人身事故がゼロとなる社会の実現を目指す」ことを目標として設定し、自動運転車の開発・普及促進を行う意義を明確にする。
>
> この目標の達成に向けて、自動運転車が満たすべき車両安全の定義を、「許容不可能なリスクがないこと」、すなわち、自動運転車の運行設計領域 (ODD) において、自動運転システムが引き起こす人身事故であって合理的に予見される防止可能な事故が生じないことと定め、この定義に基づいて自動運転車が満たすべき車両安全要件を設定し、その安全性を確保する。』（自動運転車の安全技術ガイドライン（平成 30 年度)、p.3）

また、国連の自動車基準調和世界フォーラム WP29 の「自動運転フレームワークドキュメント」におけるセーフティビジョンや、「自動運転車の EU 承認免除手続きに関するガイドライン」のセーフティ要求において、双方ともに自動運転中は「合理的に予見可能かつ防止可能な傷害または死亡をもたらす交通事故を引き起こしてはならない」ことが求められている。

自動運転システムが引き起こす人身事故の種類・形態は、歩行者、自転車、人が運転する自動車などの周囲交通参加者との衝突だけでも多岐に渡ると考えられる。さらに、人を自動で輸送するサービスを提供する車両およびシステムでは、自動運転車の乗客の転倒等も含まれる。人身事故がゼロとなる社会の実現を目指すためには、合理的に予見可能かつ回避可能な危険事象に対して必要な安全対策を講じなければならない。

## 3.2 自動運転車の安全走行戦略に関する基本的な考え方

一般に、戦略は戦術の上位概念であり、「特定の目的を達成するために、大局的な視点で組織行動を計画・遂行する方策、通則」という意味を表す。安全走行戦略という単語は一般的に使われている言葉ではないが、本ガイドブックでは、「大局的な視点で、合理的に予見可能で回避可能な事故を回避するための考え方や方策」を指すものとする。すなわち、リスクの想定範囲、リスク回避の考え方や方策などが安全走行戦略となる。たとえば、ガードレールを設置するなどの走行環境整備や、急な飛出しに備えて徐行するなどの走り方の工夫など、さまざまな方策を講じてリスク低減を図ることが該当する。

具体的な場面として、一時停止線のある交差点を通過する事例について述べる。自動運転車が交差点を安全に通過するための手順として二段階停止が推奨されている。自動運転車が一時停止線で一旦停止した後、交差点周辺の安全を十分に確認しないまま、交差点内（交差車両などの進行を妨げる位置）に一気に進んでしまうと、他の車両と衝突する恐れがある。そこで、一時停止線で一旦停止した後は、交差点周辺の安全を確認しながら徐行し、交差点周辺を見通せる位置で再停止した後に交差道路に車両や歩行者が存在しないことを確認するという手順である。二段階停止は義務ではなく、またドライバに安全確認の習慣化を促すことを狙ったものと考えられるため、自動運転車が必ずしも倣う必要は無い。ただし、周辺交通参加者の行動との調和の観点などから、こうした安全運転マナー的なことに対しても、安全走行戦略の具体化検討において考慮することが望ましい。

なお、競争領域と協調領域の境界を一義的に定義することは難しいが、安全走行戦略は協調領域において定義するものであって、競争領域に及ぶことで将来の社会情勢や技術進化と齟齬が生じないことを考慮する。たとえば、自動運転車両にとって障害物となる他車両や歩行者などの存在や動きを認識する手段として、カメラや LiDAR (Light Detection And Ranging) など複数のセンサを組み合わせて使用することが知られているが、センサの選択や認識ロジックなど具体的な認識手段は、安全走行戦略には含まない。

### 3.2.1 安全走行の基本的な考え方

自動運転車両が道路交通法等の関係法令を遵守し、車両の走行機能が正常に作動することを前提としたうえで、自動運転車両が安全に走行するための基本的な考え方としては、

『防衛運転（かもしれない運転）に徹する』ことに尽きるといえよう。しかしながら、他車両による信号無視、大幅な速度超過、物陰など見えない場所からの歩行者の急な飛出しなど、遭遇頻度が低いと思われるケースに対しても網羅的に対処しようとすると、現時点では低価格で実現することが困難と思われる高度なセンシング機能、予測・判断機能、インフラ整備などが必要となったり、頻繁な徐行や一旦停止などによって周辺交通の円滑さや移動サービスとしての実用性を阻害することなどが懸念される。3.1 節で述べたように、国土交通省の自動運転車の安全技術ガイドラインでは『合理的に予見可能で回避可能な事故が生じないこと』が安全要件として示されている。リスクはゼロにはならないからこそ、社会全体で許容できるリスクのレベルを具体的に定義することが、自動運転移動サービスを実現するうえでの重要な課題の一つである。

### 3.2.2　合理的に予見可能で回避可能の定義

つぎに、『合理的に予見可能で回避可能』の定義について考える。従来の手動運転車による事故の一例として、高速道路で対向車線の車両が中央分離帯を越えて飛び込んできて衝突した事例がある。また、青信号で交差点を直進している際に、交差道路側の赤信号を見落とした車両が横から衝突した事例もある。これらは手動運転車による事故ではあるものの、実際に起きた事象という意味では予見可能な事故とみなすことが妥当である。しかしながら、これらの事象が起こる確率は極めて低く、「合理的には予見不可能」かつ「回避不可能」とみなすことが妥当である。現実の交通社会では、発生確率が無視できるほど低くない危険事象は多数発生しており、これらの事象を安易に軽視すると事故の確率は高まる。しかし、逆に必要以上に重視すると頻繁な徐行や一旦停止などによって周辺交通の円滑さや移動サービスとしての実用性を阻害することも懸念される。すなわち、レベル 4 自動運転移動サービスの実用化に際して、事業者・自動運転車両開発者・他の交通参加者すべてがこの難しい問題に取り組む必要があるといえよう。

### 3.2.3　法令違反状態の他の交通参加者への対応

自動運転車が走行する際に、他の交通参加者が信号無視する可能性を常に配慮しなければならないと仮定すると、信号交差点で青信号の場合でも、交差車両が徐行や停止することを確認できるまでは自動運転車は交差点に進入できなくなり、結果として交通流の円滑性や移動サービスの利便性に悪影響を及ぼしうる。しかしながら、通常の交通環境におい

て人間の運転者によって運行している移動サービスでは、安全確認をしているものの、完全なる安全性を保証するレベルの確認はなされてはおらず、それでいてほとんどの場合には問題は生じていない。すなわち、世間一般の声としては「そこまで過剰に心配する必要はないのではないか」と言われることも少なくないのではないかと予想される。

一方で、すべての車両が交通法規を遵守すること、すなわち制限速度を超過する車両がいないことを前提に安全走行戦略を設計した場合には、事故が発生する可能性は高くなることは自明といえよう。我が国の交通環境において、人間の運転者が制限速度を超過して走行することもあり得るということを踏まえると、世間一般の声としては「配慮が足りないのではないか」という意見が多くなることが予想される。

以上の議論から、「法令違反状態の他の交通参加者への対応はどうあるべきか」という問題に対する必要十分条件を、どのような基準や議論のプロセスで決定すれば良いのかということが、レベル 4 自動運転移動サービスの自動運転車両開発者や事業者などの関係者にとって大きな関心ごとであり、課題となるといえよう。法令違反状態の他の交通参加者の行動を考慮するかしないかを一概に定めることは困難である。しかし、レベル 4 自動運転移動サービスの実用化の過程において、何らかの根拠に基づき安全性を評価して良否を判断する必要があり、その判断基準やプロセスが評価ごとにばらつくことは社会の混乱を招く恐れがある。自動運転の倫理について国内外で議論が始まっており、その動向に期待をもって注目するところではあるが、レベル 4 自動運転車両の開発者や事業者にとっては、可能な限り具体的な安全設計の考え方が求められている。

## 3.3 安全走行戦略ワーキンググループにおける議論

第 1 章で述べたように、令和 3 年度から経済産業省が国土交通省と連携して「自動運転レベル 4 先進モビリティサービス研究開発・社会実装プロジェクト (RoAD to the L4)」を推進している。令和 4 年度からその配下に「安全走行戦略ワーキンググループ (WG)」を発足し、産官学の関係者が参画して、レベル 4 自動運転移動サービス実用化に向けた安全走行戦略の具体化に取り組んでいる。その WG において議論された内容を踏まえて、安全走行戦略の具体化に向けて議論された内容を本節でまとめる。

また、安全走行戦略の必要十分な要件は、ワーキンググループレベルだけではなく、技術や法律、社会受容性など多様な観点から検討することが必要である。理想的には、その

結論を待って安全設計に必要な安全戦略の具体化に着手すべきであるが、多くの時間を要する。そこで、安全走行戦略 WG では、レベル 4 自動運転移動サービスの実用化を目指して安全走行戦略を策定する開発実務において、すでに顕在化している、もしくはこれから顕在化が予想される潜在的な課題を広く取り上げて、今後の議論を後押しするための検討材料を提示することに取り組んでいる。そこで本節後半では、安全走行戦略 WG で議論の材料として提示した検討事例を紹介する。

### 3.3.1 代表的な危険シナリオ 1：歩行者脇通過

自動運転移動サービス車両が、走行路の左側の歩道を通行する歩行者を認識しながら、歩行者後方から追い越す場面の安全走行戦略に関する検討事例を示す。この場合の基本的な走行戦略としては、**1) 歩車分離の状況や歩行者の状態から、歩行者が走行路に飛び出してくるリスクを想定し、2) そのリスクを許容可能なレベルに低減できる速度で歩行者に接近し通過する**ことになる。

歩行者の急な飛出しによって衝突が起きる可能性を定義する要素としては、歩行者と車両との相対的な距離（前後方向と横方向)、速度、車両が停止するまでの制動距離などが挙げられる。ここで重要なことは、想定すべき歩行者の飛出し行動[*6]を関係者の協議によって定義することである。

参照すべき案件の一つに、対歩行者衝突被害軽減ブレーキの性能評価で検討されている歩行者の飛出し形態で、駐車車両の死角から歩行者が飛び出す想定の実験がある。ただし、対歩行者衝突被害軽減ブレーキは人の運転を支援する ADAS の機能であり、危険を回避する責任はドライバにある。一方で、本ガイドブックが対象とするレベル 4 自動運転では、ODD の範囲内において自動運転システムが危険を回避する責任を担うこととなり、歩行者の飛出しの想定は対歩行者衝突被害軽減ブレーキと同等で良いとは限らない。

また、参照すべき観点の一つとして、ヒューマンドライバとの比較が挙げられる。防衛運転に長けた慎重なベテランドライバの場合、ガードレールや植樹等と歩行者の位置関係などを正確に認識し、歩行者が車両の接近に気付いているかという観点から、細かい挙動や顔向きなどといった歩行者の行動を観察するなど、非常に高度かつ柔軟なリスク推定と行動選択を行っている。ただし、このような防衛運転を行っても、絶対安全を実現できる

[*6] 自動運転車両にとって、合理的に予見可能で回避可能な行動。

わけではない点には注意されたい。一方で、レベル 4 自動運転移動サービスの採算性などを考慮した実用化可能な自動運転技術では、人間と同等以上の認識・判断を行うことは容易ではなく、歩車分離の高度化や歩行者に接近する際の走行速度低減などの対策によって、飛出しに対する衝突リスクを低減する必要がある。

### 3.3.2　代表的な危険シナリオ 2：無信号交差点を直進する事例

レベル 4 自動運転移動サービス車両が、信号のない交差点において、周囲の安全を確認して交差点を直進して通過する場面の安全走行戦略に関する検討事例を示す。この場合の基本的な走行戦略は、**交差車両の位置、速度、自車両が交差点を通過するために必要な時間から、交差車両が交差点に到着する前に交差点を通過可能かを判断する**ことになるが、自車線と交差道路の優先関係によって判断は変わる。また、道路構造などの影響によって、交差道路側が優先と誤認する恐れがあることも想定しなければならない。

### 3.3.3　代表的な危険シナリオ 3：信号交差点を右折する事例

レベル 4 自動運転移動サービス車両が、信号のある交差点において、周囲の安全を確認して交差点を右折して通過する場面の安全走行戦略に関する検討事例を示す。この場合の基本的な走行戦略は、**対向車線走行車両の位置、速度、横断歩行者等の状況、右折先のスペースなどに基づいて、自動運転車両が交差点を安全に右折できるか否かを判断する**ことになるが、自由流の場合と渋滞流の場合に異なると思われる。

なお、シナリオ 2 とシナリオ 3 で共通する事項として、無信号交差点を直進する際には左右の交差道路から来る車両、信号交差点を右折する際には対向車線を直進してくる車両の速度に関して、制限速度をどの程度超過してくるケースを想定するべきかが安全設計のポイントとなる。たとえば、実勢速度を参考にすることなどが考えられる。また、自動運転車両が交差点を安全に通過し終えるか否かの判断には、交差車両や対向車両の想定速度が重要となるが、（測定した）現在の速度、制限速度、実勢速度の三つの速度の視点から整理することが有効ではないかと考える。

シナリオ 2 と 3 のいずれのケースにおいても、交差点に進入してくる周辺車両の速度と位置は、自動運転車またはインフラセンサによって計測する。その計測された周辺車両の速度によって、数秒先の車速変化に対する予測が変わる可能性がある。

1) 現在車速 < 制限速度の場合　　例：上限は制限速度まで考慮するか？
2) 制限速度 < 現在車速 < 実勢速度の場合　例：上限は実勢速度まで考慮するか？
3) 実勢速度 < 現在車速の場合　　例：上限は現在車速まで考慮するか？

ただし、上記はあくまでも数秒先までの予測にすぎず、予測精度が一定程度に向上しても確実な予測にはなり得ず、予測に基づいて細かく定義するメリットはそれほど高くない。その代わりに、現地における交通実態を調査することは非常に有効であると考えられる。統計的に有効な論証となるデータを収集するには多大な労力と費用が必要となり限界があるが、先行事例や類似事例等でデータを共有し有効活用することなどが課題と考える。

## 3.4　車内安全システムに対する考え方

2.2 節で記載したように、サブシステムとして車内安全システムがある。本節では、車内安全システムにおける考え方をまとめる。レベル 4 自動運転移動サービスでは、乗客の安全は最優先課題の一つである。現在の移動サービスにおいて、とくにバスでは、乗務員（運転手）が基本的に 1 名で、運転タスクと車内安全タスクを同時に行う。運転タスクについては 3.2、3.3 節に記載した通りだが、レベル 4 自動運転移動サービスを実現するためには車内安全タスクをどのようにシステムで対応していくかを考えなければならない（図 3）。ここで言うシステムには、車内システムだけでなく、遠隔監視システムも含まれるが、運用ルールを変えず、かつ、どのシステムや乗務員でも対応しないタスクが残ってしまった場合には、自動運転移動サービスの実現が困難となる。逆に言えば、場合によっては運用等を変えて対応する必要が生じる可能性がある。一方で、レベル 4 自動運転移動サービスにおいて運転タスクをしない乗務員が車内に残る場合は、システムだけでなく乗務員が対応することで解決することも考えられるので、その場合にはシステムを簡素化できることが想定される。

道路運送法等の関係法令を遵守することを前提として、サービスを提供する事業者側の判断において、コスト等を含めたシステムの選択を行っていく必要があるといえよう。一方で、令和 4 年度時点において、レベル 4 自動運転移動サービスの認定を受けた事業者等が国内に存在しておらず、事業者としてどのような安全対策を施していくかを個社として考えていくよりも、共通の考え方としての協調領域を定めることで、効率的に議論を進め

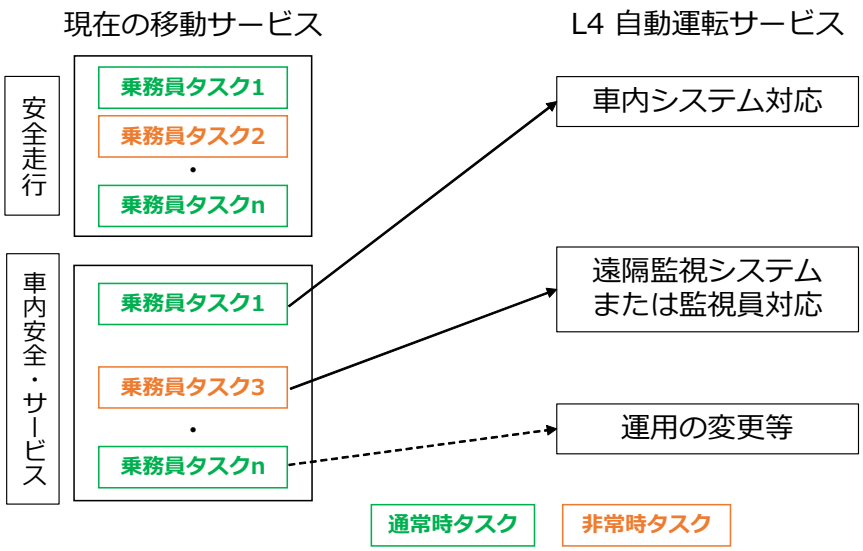



図 3　車内安全・サービスのタスクに関する考え方

ていくことが望まれる。

次節では、車内安全システムに関して、事業者における協調領域を定義するとともに、協調領域の範囲内における車内安全に関する乗務員タスクを議論する場としての会議体について説明する。

## 3.5　車内乗客安全ワーキンググループにおける議論

3.2 節と同様に、令和 4 年度から「自動運転レベル 4 先進モビリティサービス研究開発・社会実装プロジェクト (RoAD to the L4)」の配下に「車内乗客安全ワーキンググループ (WG)」（以後、車内乗客安全 WG と記す）を発足し、産官学の関係者が参画して、レベル 4 自動運転移動サービス実用化に向けて、レベル 4 自動運転車内の乗客安全に関する議論を開始している。本節では、車内乗客安全 WG において議論された内容をまとめる。車内乗客安全 WG が発足した令和 4 年度において、車内安全に関連した、国土交通省の検討会[*7]が開催されたこともあり、車内の乗客に関する安全について、どのような考え方で、どのように安全を確保していくべきかについては、上述した安全走行戦略と同様に非

[*7] 自動運転車を用いた自動車運送事業における輸送の安全確保等に関する検討会。以後、国交省の輸送の安全確保等の検討会と記す。参照 → https://www.mlit.go.jp/jidosha/jidosha_fr2_000044.html

常に重要な課題であると考えるとともに、検討会の進捗を鑑みながら車内乗客安全 WG の議論が行われている。令和 4 年度の車内乗客安全 WG においては、最初にどのようなタスクが存在するかを網羅的に列挙することとした。車内乗客の安全を確保するために必要な観点や要素が、包括的に、漏れなく網羅されるよう、バスを運行する交通事業者へのヒヤリング等も活用しながら、乗務員のタスクの流れを整理し議論を進めている。タスクは、発生頻度をもとに下記の三つに分けて議論した。

1. 通常時
2. 通常時以外
3. さまざまな乗客に対する対応

本議論の前提として、車内の安全・サービスの項目が多岐に渡り、最も難易度の高い条件として、対象車両はロボットタクシー等のいわゆるロボタクではなくバスとする。さらに、車内の条件としては着座だけでなく立ち乗りまでを想定し、走行ルートは固定ルートとして議論を進めている。サービスについては一旦議論対象外としている。

議論が進むにあたり、乗務員タスクにおける安全に対して、交通事業者間において特に競争領域としていく考え方はあまり存在せず、協調領域の範囲内であることを確認している。

令和 4 年度は現在の乗務員タスクに関する議論を行った。令和 5 年度ではレベル 4 自動運転システムへの移行の際に新たに追加されるタスクを見据えた対応方法について議論する。

# 4　自動運転車の安全性に関する要配慮事項 1：運行設計領域 (ODD) の設定

自動運転旅客移動サービスを提供する車両およびシステムは、社会に多くの利益をもたらすと同時に、公共性が高いがゆえに、確実性・透明性・費用対効果が高い要件を満たすことにより安全性を確保する必要がある。本安全設計ガイドブックは、国土交通省の「自動運転車の安全技術ガイドライン」を基本指針とするが、自動運転旅客移動サービス事業に新規参入する多様な企業や団体および役所などにも理解しやすく使いやすいように、安全性に関わる項目ごとに、

- **必要理由**：何故その要件が必要なのか
- **考え方**：どのような論理や理屈でその要件を満たすことで安全性を確保できるのか
- **具体的な事例**：代表的な自動運転旅客移動サービスのシステム構成（車載システム、遠隔監視支援システム、インフラ協調システム）で説明

を記載する。なお、サービス事業用自動運転車は、自家用自動運転車と異なり運行条件をかなり限定可能なので早期の社会実装が期待される。ただし、その限定範囲内で抜けの無い安全設計が必要である。

本章では、自動運転システムの安全設計を行うための準備として、**ユースケースの設定、運行設計領域 (ODD) の設定、シナリオの設定**を行う。また、ユースケースの設定においては、想定すべき障害物の選定も実施しておく。これらはすべて、5 章に記載する安全設計（車両レベル／抽象的レベル）において、ハザードや危険事象の洗出しを漏れなく効率的に行うための準備作業である。

なお、ビジネスモデルを含む形で、自動運転車による旅客移動サービス事業の企画構想が既に実施されており、対象地域、運行経路、自動運転車のベース車種[*8]や、車両製造者／システム提供者／事業実施者／運行管理者／乗客層などのステークホルダが既に立案されていることを前提とする。

[*8] 現状では、原則的に量産車である。

## 4.1　ユースケースの設定

自動運転車による旅客移動サービス事業の企画書などに基づいて、想定する基本的な使われ方である自動運転車のユースケース、つまり自動運転車や周辺交通参加者の振舞い、道路構造、天候や日照などさまざまな切り口で整理する。後述する安全設計や安全性評価に使うシナリオと似ているが、本ガイドブックでは、ユースケースは大括りな描写である一方、シナリオは細かくかつ動的な描写、すなわち時系列の複数シーン描写である。

スタートが同一シーン（例：潜在的なリスクあり）であっても自車の振舞いなどによっては異なるシーン（例：リスクが低い模範走行、ニアミス、事故）に至るのでシナリオは複数存在する（図 4 参照）。

### 4.1.1　必要理由

ユースケースは、開発プロセス（設計、評価）の全体において、システムの安全性を一気通貫で漏れなく検討するために必要な使用状況の整理方法である。まずは、ユースケースを粗く広く整理することで、安全設計や安全性評価の抜け漏れを防ぐ。つまり、偏った局所的な深掘り検討で終わってしまうことを回避する。

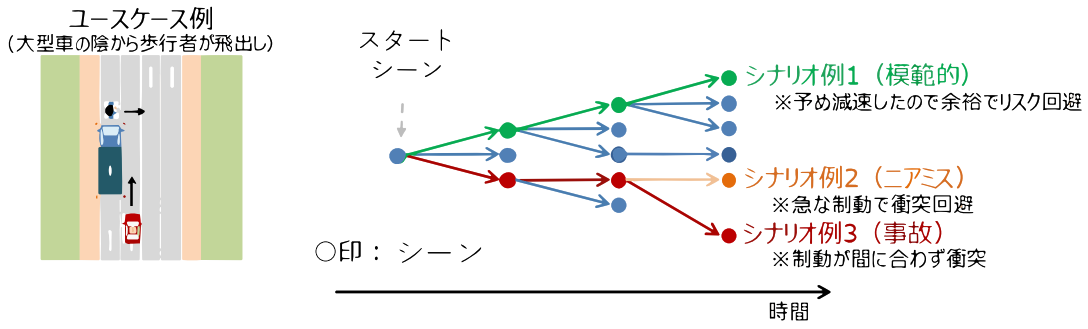



図 4　ユースケースとシナリオの関係イメージ（出典：経済産業省委託事業「平成 30 年度　高度な自動走行システムの社会実装に向けた研究開発・実証事業：自動バレーパーキングの実証及び高度な自動走行システムの実現に必要な研究開発（セーフティ）」）

### 4.1.2　考え方

本ガイドブックの対象である旅客移動サービス用レベル 4 自動運転システムに対して想定される使われ方をユースケースとして洗い出す。後述するシナリオは、ユースケースを、各種外乱要素の有無／パラメータ数値／自車の振舞いなどの各種条件で細分化したものである。ユースケースは、言い換えれば、組合せ次第で数多く存在するシナリオを分類するための棚である。棚（ユースケース）を作ってから大量の書類（シナリオ）を仕分け整理することを推奨する。

### 4.1.3　事例

BRT (Bus Rapid Transit) 事業をイメージした事例としては、自動運転システムの起動・停止、停留所での旅客乗降、停留所や退避エリアでの他自動運転車とのすれ違い、停留所での発車・停車、既定経路での自動運転、既定場所での一時停止・再発車、障害物衝突回避の停車・再発車、緊急時の縮退運転・MRM 停車、運行前後の点検やシステム調整などが挙げられる。

ユースケース例のイメージ図と車内から撮影した写真を参考に図 5 ～ 9 に示す。運行経路が決まっている場合、映像や地図情報や衛星写真なども有効活用する必要があるが、漏れ抜けを避けるために現場視察は不可欠である。

図 5　ユースケース例（専用道と歩道の並走）

図 6　ユースケース例（専用道と公道の交差 1、遮断機あり、信号機なし）

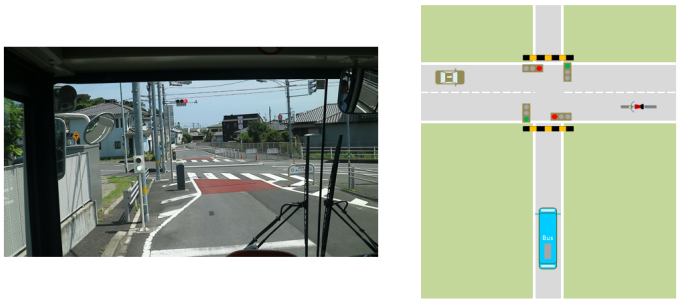


図 7　ユースケース例（専用道と公道の交差 2、遮断機あり、信号機あり）

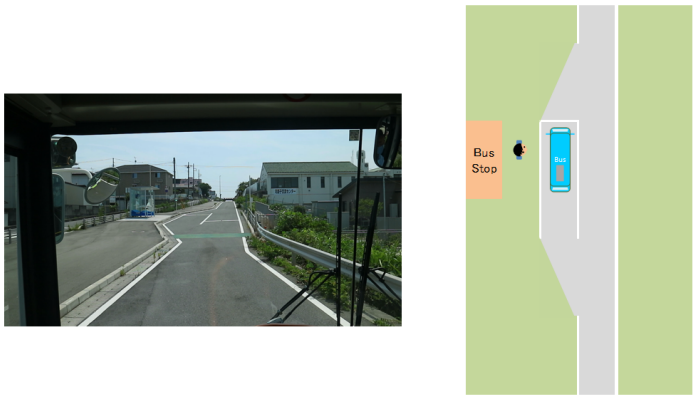



図 8　ユースケース例（停留所での旅客乗降）

## 4.2　障害物の選定

自動運転車の走行路上にあり、衝突や乗り上げといった自車の走行の妨げになる各種障害物（静止物・移動物）をリストアップしておく。さらに、自車と障害物の衝突や乗り上

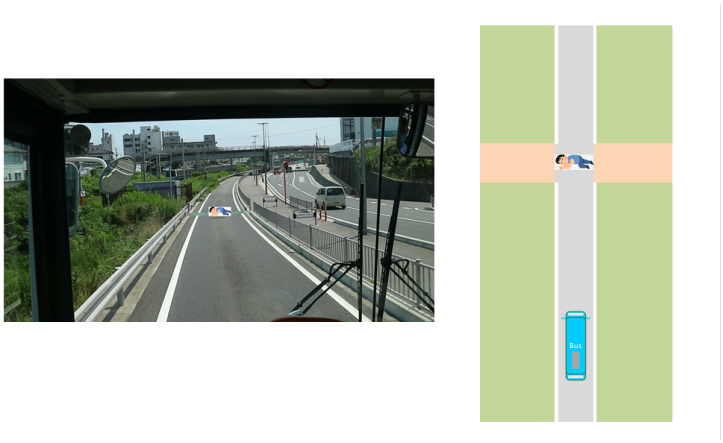



図 9　ユースケース例（横臥者との衝突回避のための停車・再発車）

げた際に予想される歩行者や乗員へ与える傷害度を衝突速度ごとに見積り、後述の安全設計の対象とすべきか否か選別しておく。つまり、検知すべき障害物の大きさの下限を合理的に決めておく。

#### 4.2.1　考え方

認知すべき障害物の大きさの下限すなわち認知性能の限界を、相対速度ごとに前もって合理的に決めておくと、後述の安全設計の対象範囲が絞られてシステム開発を効率的に行うことができる。実験やシミュレーションで、歩行者や乗客・乗員への傷害度を新たに求めるには相当なコストを要するので、ベース車両の開発製造者に可能な限りのデータ開示を依頼したい。得られた傷害度が社会的に許容されるか否かは、過去事例などを踏まえて水準を決めるべきである。

#### 4.2.2　事例

- 障害物のリスト例

  車両（乗用車・大型車）、バイク、自転車、ベビーカー、歩行者（大人・子供）、横臥者、倒木、岩やブロック片、タイヤ、パイロン、動物など
- カートがコンクリート段差に乗り上げた際の乗員傷害度例

  車両製造者への開示依頼や文献調査が必要
- 大型バスがコンクリート段差に乗り上げた際の乗員傷害度例

  車両製造者への開示依頼や文献調査が必要

- 傷害度の許容水準

  文献調査等が必要

## 4.3 ODD の設定

自動運転システムが機能する特定条件（範囲）を運行設計領域 (ODD) として設定する。特定条件（範囲）は、以下に示すように、走行環境と運行環境に大別される。なお、自動運転レベル 4 では、ODD 条件を逸脱した場合やしそうな場合には上限車速を通常より下げるなどの制限付きで自動運転を継続するフォールバック（縮退運転）を作動させ、ODD 条件を逸脱した場合には路肩など安全な場所へ自動停車するリスク最小化制御 (MRM: Minimal Risk Maneuever) を作動させて安全を確保する必要がある。これら安全設計については 5 章で詳しく記載する。

本節では、ODD 範囲の定義を主に記載するが、ODD 範囲内外の判定手段も必要である。すべての条件判定をシステムで実現することは現実的ではなく、天候条件などの ODD 内外判定は、乗員や遠隔監視員などが行う選択肢もある。

**走行環境**

- 道路条件

  専用道、優先道、一般道／単路、合流分岐路、三差路、四差路、多差路（五差路以上)、環状交差点（ラウンドアバウト）など
- 地理条件

  都市部、郊外部、山間部など
- 環境条件

  天候（降雨・降雪・霧など)、日照（西日・朝日・薄暮・夜間など）

**運行環境**

- 運行条件

  速度制限、経路限定 、信号機やガードレールなど通常インフラの要否、信号情報や死角情報などを支援するインフラ協調システムの要否、遠隔監視要員の要

否、同乗保安要員の要否など

#### 4.3.1 必要理由

どのようなシステムであっても必ず各本来機能には限界がある。旅客移動サービス用自動運転車において、認知機能などの本来機能がサービス運行中に限界に至ることを本来機能の喪失というが、その結果として不安全な車両状態、たとえば衝突による人身事故などに至ってしまうことを回避するために ODD が必要である。ODD の適切な設定と自動運転中の ODD 逸脱判定と逸脱防止の措置により、自動運転のまま本来機能が限界に至ることを回避して、自動運転システムの安全性を確保する。また、ODD 設定は、安全優先の観点より、本来機能の限界と連動させることが必須である。そのうえで、ODD 設定はコストとサービス性のトレードオフ調整の指標にもなる。

#### 4.3.2 考え方

ODD 設定／修正のプロセスを検討フロー全体図にまとめたものを図 10 に示す。ODD ／サービス／システム類型化の考え方を取り入れる。以下の二種類の CASE に対応する。

- CASE 1：
  ゼロスタート開発の場合（原型システムが無い場合）
- CASE 2：
  ODD 同類型（または ODD 別類型）の原型システムからの差分開発の場合

ODD による自動運転機能の範囲限定は、自動運転旅客移動サービスの提供価値を低減するが、自動運転システムの開発容易性や導入コストといったサービス事業の実現性を改善する。一般に関係性はトレードオフなので繰り返し検討が必要である。通常の V 字開発プロセスに沿って ODD を設定および修正する。大きな V 字を回すと手戻りが増えるので、極力、V 字左上の安全設計（車両レベル／抽象的レベル）／机上検討／シミュレーション検討といった早い段階で ODD 設定を完成に近づける必要がある。

図 10 に示す検討フロー全体図の中にある ODD 設定（本事業用仮置き）を説明する。新たな自動運転旅客移動サービス事業の企画において、以下の ODD 項目は、事業目的・時間帯ごとの乗客見込数などの顧客調査・ビジネスモデルなどから既に決定されていると

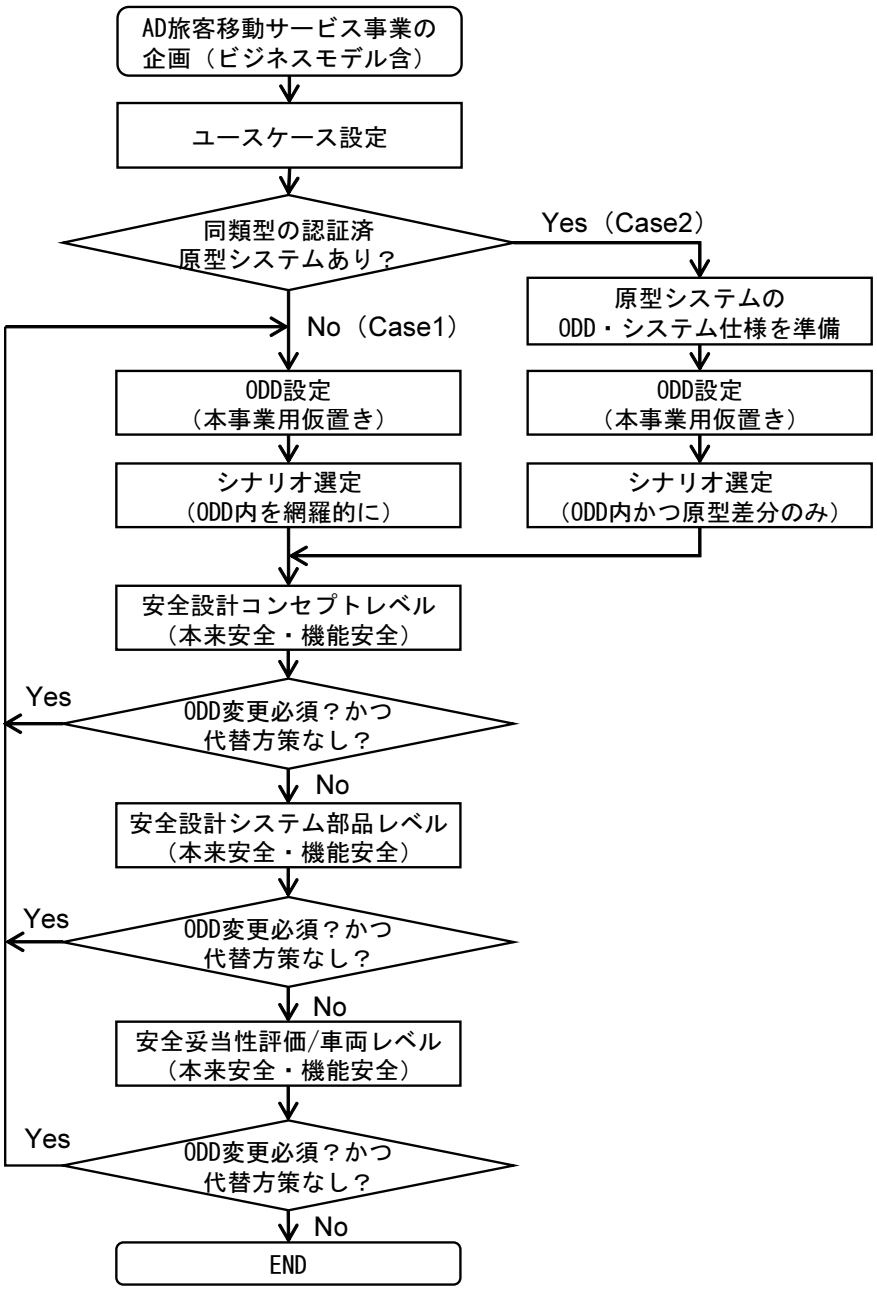



図 10　ODD 設定／修正プロセス（検討フロー全体図）

仮定する。

- 経路制限

  ターミナル 1、2 を結ぶ往復路や、特定エリアを巡る巡回路など

- 道路種類

  鉄道廃線跡地・工場・空港・観光施設等を活用した専用道、公道で交通規制を加えた優先道、公道で一般車と混走する一般道や高速道など

- 道路構造

  運行経路に沿って自動運転車両が走行する道路の構造

  – 単路、合流分岐路、N 差路、ラウンドアバウト、車線数など

- 地理条件

  特定の都市部、郊外住宅地、山間部、限定された民間地など

- 自動運転車両の車種

  カート（乗員数：少数、上限車速：徐行速度並)、小型バス・大型バス（乗員数：多数、上限車速：法定速度並）など

ODD 設定（本事業用仮置き）では、以下に記す項目を各視点から仮決めする。

- 天候条件・日照条件

  企画で設定した事業を提供する場所（地理条件)、その場所における過去の天候実績、顧客調査（時間帯ごとの乗客見込数)、ビジネスモデル（収支計画）などをもとに、環境条件（天候（降雨・降雪・霧など)、日照（西日・朝日・薄暮・夜間など）を設定する。たとえば、昼間のみの運用でも事業収益と旅客利便性が見込めるならば昼間のみの運行とすることが考えられる。つまり特定の照度以上または、日出／日没を考慮した特定の時間帯を ODD 内とする。通年でにわか雨が多く、その都度運休することになると事業収益と旅客利便性が低下するという場合には、特定の降雨量までを ODD 内として、特定の降雨量以上は運行を制限することも考えられる。また、降雪や霧などが滅多に発生しない地域で、発生した場合に運休したとしても事業収益と旅客利便性が大きく損なわれない場合には、降雪や霧の可能性が少しでもあると判断したときには ODD 外とする。

  なお、天候条件や日照条件に関する ODD は、自動運転システムのセンサ認識系の性能に強く依存するので、設定した ODD で安全設計要件[*9]を満たすセン

[*9] たとえば、周辺交通参加者との衝突回避に必要な障害物認知距離など。

サ認識系の選択が必要である。

- 運行条件（経路制限以外）

  速度制限は、企画で設定した自動運転車の車種、走行経路の道路構造（道路線形や右左折の有無など）、公道であれば交通法規などに応じて設定する。また、何かしらの阻害要因（天候・日照・死角など）でセンサ認識系の障害物認識距離が通常より劣化している場合には、速度制限を通常より下げてフォールバック（縮退運転）を作動する。

  信号機やガードレールなど通常の道路インフラは、まずは運行経路に既に存在する物を設定する。つぎに、5 章で示す安全設計（車両レベル／抽象的レベル）において、たとえば、歩行者の歩道からの急な飛出しや、交錯道路の交通量が多く交差点横断が困難な状況などに対して安全優先で設計すると徐行や一時停止の時間が増えてサービス性が著しく低下すると想定される場合には、経路の見直しやガードレールの増設などが必要となる。

  信号情報や死角情報などを支援するインフラ協調システムの要否について述べる。たとえば、自動運転車両の車載センサ認識系のみで交差点に進入して直進・左折・右折を行う場合、安全優先で設計すると徐行や一時停止の時間が増えてサービス性が著しく低下する場合がある。しかしながら、自動運転車両が交差点に進入する前から、交差点の信号情報や、交差点内の歩行者や車両、交差点に接近する車両などの情報をインフラ協調システムとの通信を介して得ることができる場合には、安全性を確保しつつ、サービス性の低下を回避できる可能性がある。

自動運転レベル 4 において、システムの故障・ODD 逸脱・性能限界などの理由で運転継続が困難と判断した場合には、MRM を作動させて路肩などに停車するなどの安全状態へ移行する。そこから自動運転再開の可否判断を行う、または手動運転によって移動するためには、同乗保安要員、遠隔監視要員、または緊急で現地に出向く管理者など人間による対応が必要である。

#### 4.3.3 事例

**走行環境**

- 道路条件
  - 専用道
  - 単路（一車線、歩道並走区間あり、曲線路・勾配路あり）、公道との交差路（信号無し・信号あり、何れも専用道側に遮断機あり）、停留所（他の自動運転車両とすれ違い可能な退避エリアあり）、横断歩道）
- 地理条件
  - 郊外住宅地
- 環境条件
  - 降雨：■■ mm 以内、降雪／積雪：全面 ODD 外、霧視程：■■ m 以上
  - 日照：■■ lx 以上、■■時■■分～■■時■■分（日中のみ）

**運行環境**

- 運行条件
  - 専用道
  - 速度制限：■■ km/h（道路曲率に対応）
  - 経路限定：あり（図 11 のイメージ参照）
  - インフラ／ガードレール：歩道並走区間の一部にあり
  - インフラ／信号機：専用道と公道（対向片側 1 車線）との交差路にあり
  - 専用道と公道（車線無し）との交差路になし
  - 車両同乗保安要員：要
  - 遠隔監視要員：要

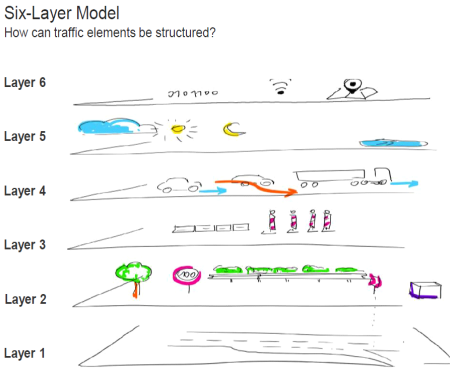
## 4.4 シナリオの設定

先に整理／設定したユースケースと ODD をもとに、安全設計・評価用シナリオを抽出する。


図 11　既定経路の例

### 4.4.1　必要理由

シナリオは、開発プロセス（安全設計、安全性評価）全体を通して、システムの安全性を一気通貫で漏れなく検討するために必要であり、使用状況を特定化して再現する共通台本である。前述の大括りな描写であるユースケースと異なり、シナリオは細かくかつ動的な描写すなわち時系列の複数シーン描写である。5 章の「安全設計（車両ベース／抽象的レベル）」におけるハザードや危険事象の抽出、10 章の安全性評価に繋がる共通の準備作業としてシナリオを設定する。




| Layer | シナリオ構造 | 例 |
|---|---|---|
| Layer 6 | デジタル情報<br>(Digital information) | ・V2X<br>・地図データなど |
| Layer 5 | 環境条件<br>(Environmental condition) | ・光条件<br>・天候<br>・気温 など |
| Layer 4 | 移動物体<br>(Moving object) | ・車<br>・歩行者 など |
| Layer 3 | 一次的な規制とイベント<br>(Temporal modifications and events) | ・道路建造物<br>・落ち荷物<br>・倒れた木 など |
| Layer 2 | 道路構造物とルール<br>(Road furniture and Rules) | ・交通標識<br>・レーンマーカ<br>・ボッツドッツ など |
| Layer 1 | 道路<br>(Road Layer) | ・道路線形<br>・道路の凹凸など |

図 12　PEGASUS プロジェクトの 6 Layer Model によるシナリオ表現

| プロセス | 処理結果 | 外乱 | 物理原則 |
|---|---|---|---|
| 認知 | 周辺交通環境の位置情報、自己位置。交通情報 | 認識外乱 | センサメカニズムに応じた原理的な外乱(例)カメラ:可視光、ミリ波:電波、LiDAR:赤外光 |
| 判断 | 軌跡、車速目標指示 | 交通外乱 | 道路構造＋交通参加者との位置関係といった幾何的観点と、交通参加者の動作 |
| 操作 | 軌跡、車速目標指示を達成するための各ACTへの運動指示分配 | 車両運動外乱 | 路面、外界からタイヤおよびボディに入力される力学的な外乱 |

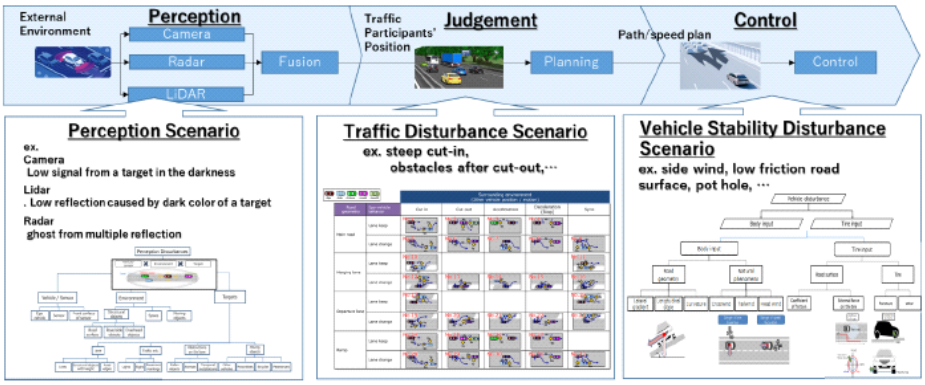



図 13　物理原則に基づくシナリオ構造

### 4.4.2　考え方

自家用車の自動運転安全性評価のために網羅的かつ階層的にシナリオを体系化した事例としては、ドイツの PEGASUS プロジェクト[*10]における 6 Layer Model シナリオ（図

[*10] http://www.pegasus-projekt.info/files/tmpl/pdf/1st_European_CCAD_Side_Event_Folien.pdf

12)[*11][*12]や、一般社団法人日本自動車工業会の「自動運転の安全性評価フレームワーク／物理原理に基づくシナリオ構造」（図 13）などがある。前者は、道路構造、自然環境、交通流などを組み合わせたもの、後者は、自動運転の動的運転タスクを実行するために必要な機能プロセスを、物理原則の異なる「認知：認識外乱、判断：交通外乱、操作：車両外乱」に分けて、各機能プロセスへ影響を及ぼす（阻害する）要因や物理原則で体系化したものである。後者は経済産業省から一般財団法人日本自動車研究所が受託する SAKURA プロジェクト[*13]でも活用されている。

自家用自動運転車の場合、制限条件は少なくシナリオの数はかなり多くなる。一方、旅客移動サービス用自動運転車の場合、運行地域・運行経路・運行時間帯などが一般的に限定されるのでシナリオ数をかなり絞ることが可能と思われる。したがって、前述のように設定した ODD を、網羅的に体系化されたシナリオの各階層項目（道路構造、道路種類、自車の位置と挙動、周辺交通参加者の位置と挙動、天候や日照、インフラなど）に当てはめて制約することで安全設計・評価用シナリオを設定する。

ODD 設定によるシナリオの限定（経路や道路構造の限定、天候・日照の限定、速度制限、周辺交通参加者の限定等）や、ODD 類型化（走行環境やサービス環境の観点で事業を大きく分類）による同類原型との差分を抽出するような考え方により、安全設計・評価用シナリオの数は、漏れなく重複なく整理することで効率的に設定する。

旅客移動サービス用自動運転車の乗客・周辺車の乗員・歩行者などに人的危害を与える可能性が差し迫ったクリティカルなシナリオを漏れなく抽出する。さらに、そのような人的危害を与える可能性が予見されるプレクリティカルなシナリオ、すなわち先読み対応が必要なシナリオについても可能な限り抽出する。

#### 4.4.3 事例

**運行経路に沿った個別シナリオの事例（5 章で参照）**

専用道を主に走行しつつも、一部の区間で歩道との並走や公道と交差するような運行経路を有する仮想の自動運転旅客移動サービス事業を想定した。運行経路に沿ったリスクシ

[*11] https://www.pegasusprojekt.de/files/tmpl/Pegasus-Abschlussveranstaltung/15_Scenario-Database.pdf

[*12] https://www.meti.go.jp/meti_lib/report/H30FY/000351.pdf

[*13] https://www.sakura-prj.jp/project_info/

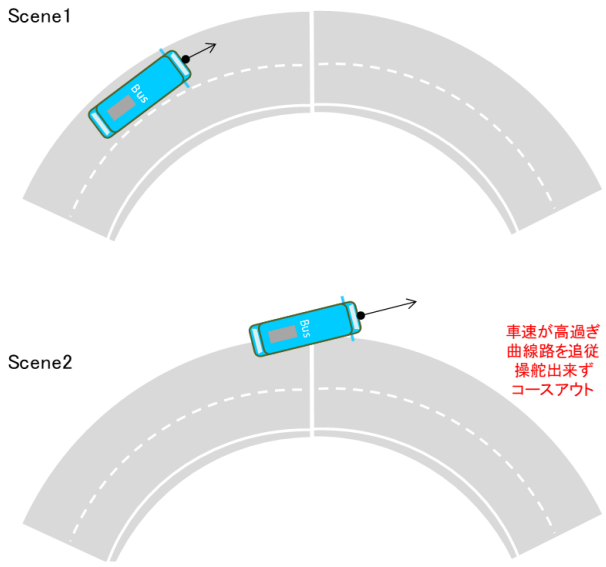



図 14　シナリオ例 1：急な曲線路での車線追従走行（通常走行／外乱なし）

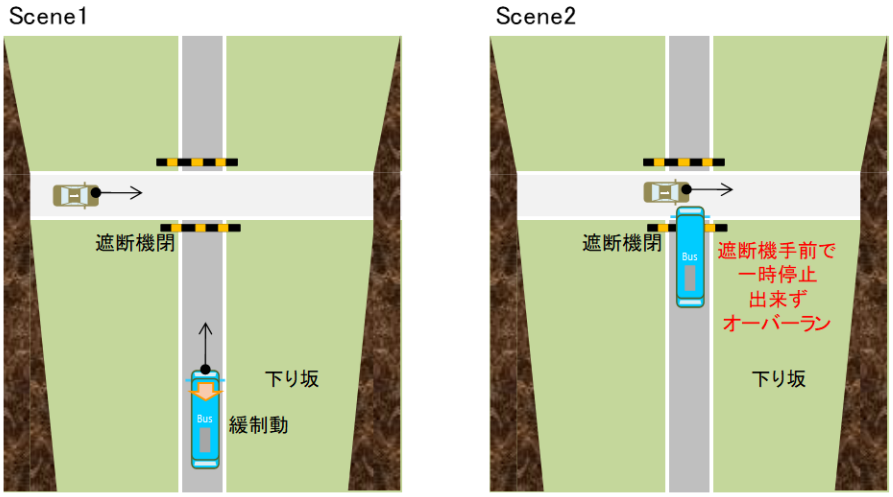



図 15　シナリオ例 2：下り坂での減速・一時停止（通常走行／外乱なし）

ナリオ事例を図 14～ 図 26 に示す。

　各シナリオは、「始まりのシーン 1：人的危害を伴う事故へ至る潜在的リスクあり」と「終わりのシーン 2：適切な安全方策なく人的危害を伴う事故へ至ってしまう状況」のイメージ図を使って、安全設計（車両レベル／抽象的レベル）で実施するハザードや危険事象の洗出しにて活用しやすい表記とした。


図 16　シナリオ例 3：上り坂での発進・加速（通常走行／外乱なし）

図 14 は、急な曲線路を車線に沿って走行することができずコースアウトするシナリオである。

図 15 は、下り坂途中にある自動運転車専用道と公道の交差路（遮断機あり・信号機なし）の前で一時停止するために減速制動するが所定位置で止まり切れずにオーバーランするシナリオである。

図 16 は、上り坂途中にある自動運転車専用道と公道の交差路（遮断機あり・信号なし）で、意図した発進加速ができず速やかに交差路を横断できないシナリオである。

図 17 は、自動運転車専用道と公道の交差路（遮断機あり・信号なし）を一時停止後に発進するが、交差路接近車両の挙動予測を間違えて衝突回避できないシナリオである。

図 18 は、自動運転車専用道と並走する歩道を酩酊状態で歩く歩行者が、車道に急に転倒または飛び出してきたので急制動するが、衝突を回避できないシナリオである。

図 19 は自車が走行する路面上に認知できないほど高さが低い障害物（倒れた木の枝・小石・地割れなど）があり自動運転車両が乗り上げてしまうシナリオである。

図 20 は橋梁上を走行する際に強い横風を受けて、車線維持操舵しきれずにコースアウトするシナリオである。

図 21 は停留所に停車するために減速制動および操舵するが、周辺路面が凍結しているために、コースアウトやオーバーランするシナリオである。

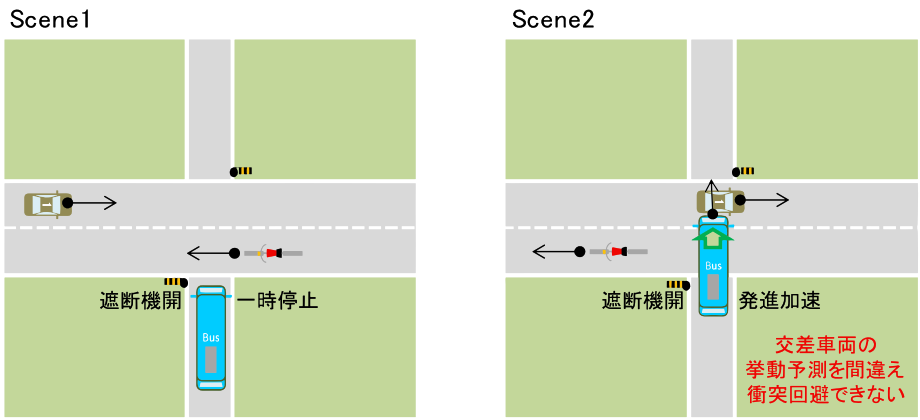



図 17　シナリオ例 4：一般公道と自動運転車専用道の交差路を横断（交通外乱）

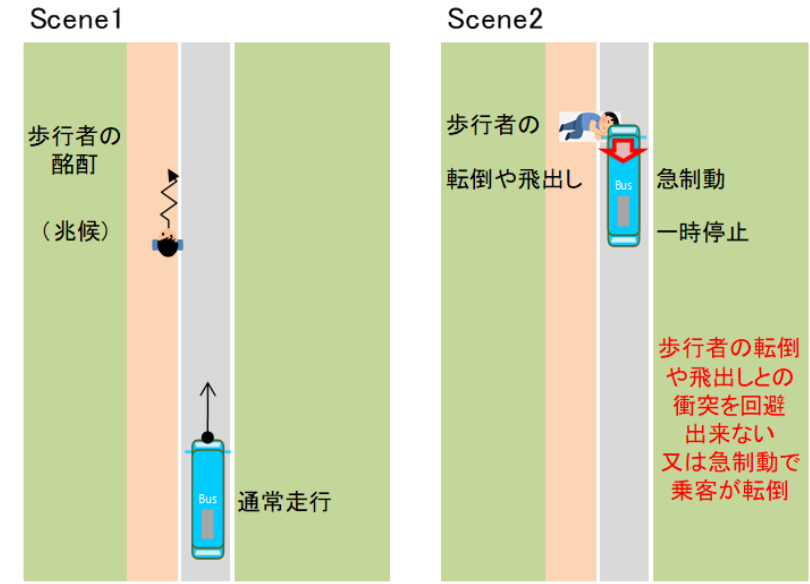



図 18　シナリオ例 5：歩道歩行者の転倒または飛出し（交通外乱）

図 22 は停留所から発車するために発進加速および操舵するが、周辺路面が凍結しているために、コースアウトするシナリオである。

図 23 は自動走行中に急な豪雨があり、前方障害物（横断歩道を横断する歩行者）を車速に見合った適切な距離で認知できず、歩行者との衝突を回避できない、または、かなり接近してからの急制動によって乗客が転倒するシナリオである。

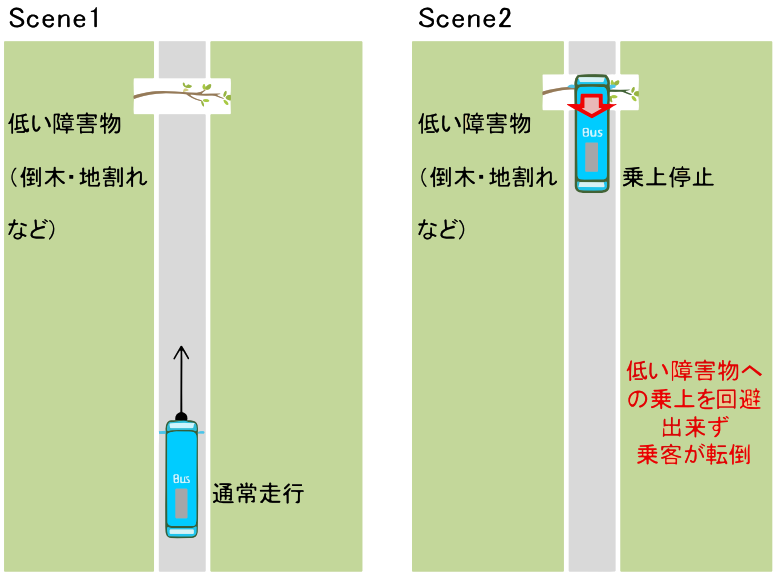



図 19　シナリオ例 6：路面高が低い障害物（倒れた木の枝・小石・地割れなど）（交通外乱）

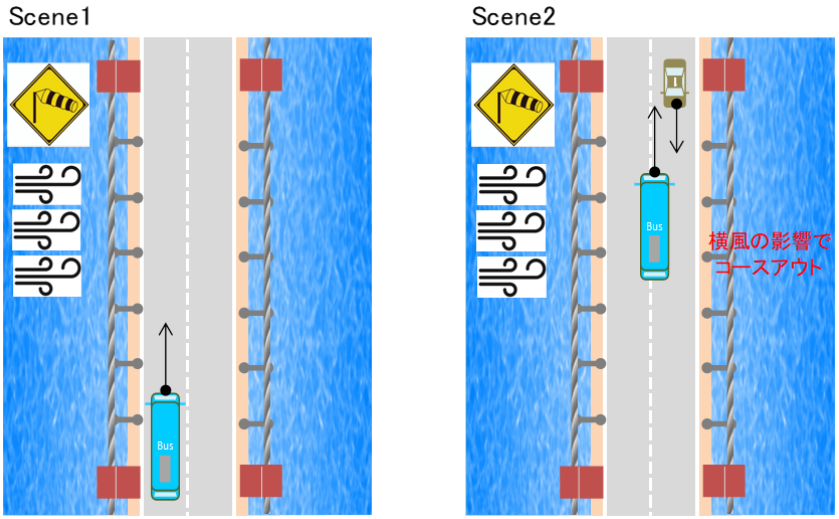



図 20　シナリオ例 7：強い横風下での車線維持走行（車両外乱）

図 24 は自動走行中に進行方向に朝日や西日があり、前方障害物（横断歩道を横断する歩行者）を車速に見合った適切な距離で認知できず、歩行者との衝突を回避できない、または、かなり接近してからの急制動によって乗客が転倒するシナリオである。

図 25 は自動運転車専用道と交差する歩道を移動して接近する障害物（歩行者・自転車）が、交差路角にある家屋壁などで隠蔽されるため、自動運転車前方に急に現れて衝突を回

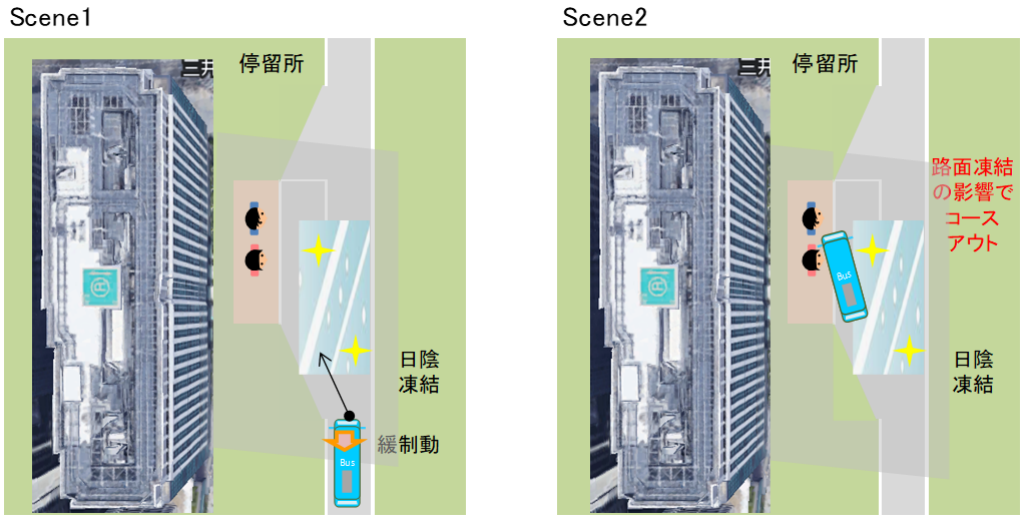



図 21　シナリオ例 8：低 $\mu$ 路面での制動・停車（車両外乱）

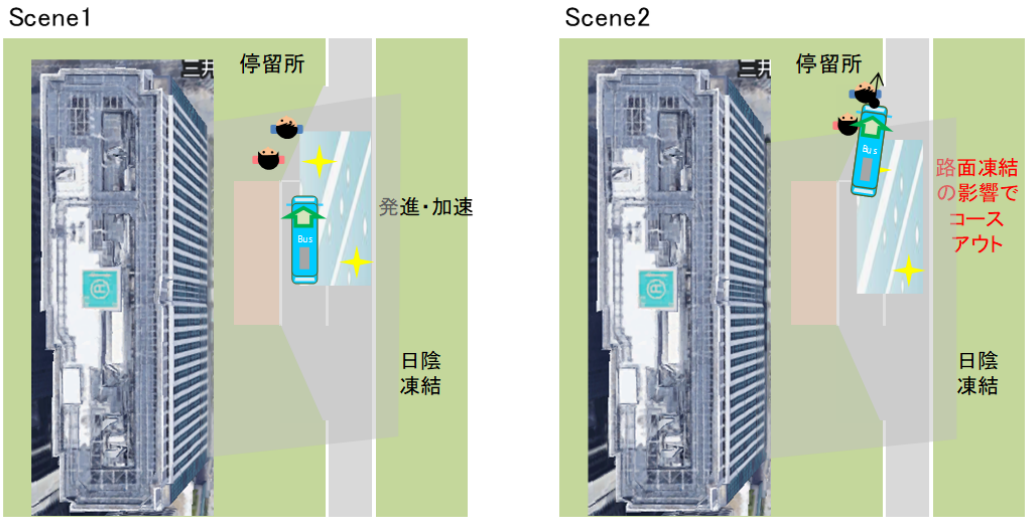



図 22　シナリオ例 9：低 $\mu$ 路面での発進・加速（車両外乱）

避できない、または、かなり接近してからの急制動によって乗客が転倒するシナリオである。

図 26 は停留所で停車して乗客が降車する際に、最後に降車した乗客のショルダーバックが扉に挟まれるが、自動運転車両乗降扉外近傍の状況がカメラの死角となっており、

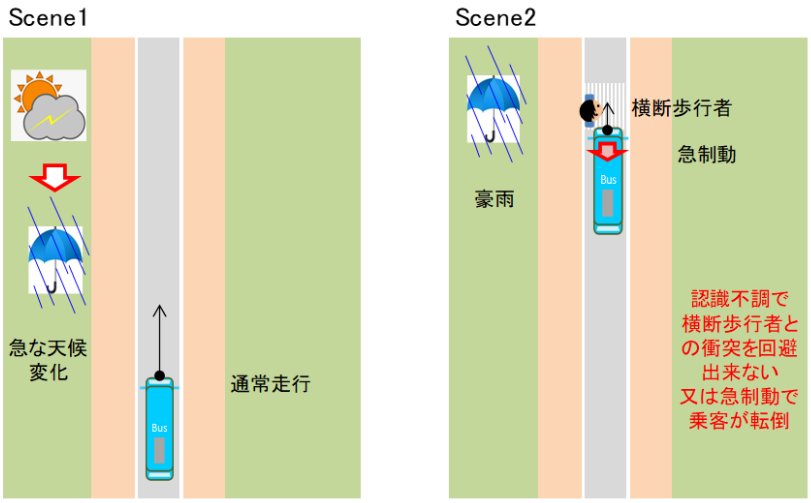



図 23　シナリオ例 10：急な豪雨／歩行者横断（認識外乱）

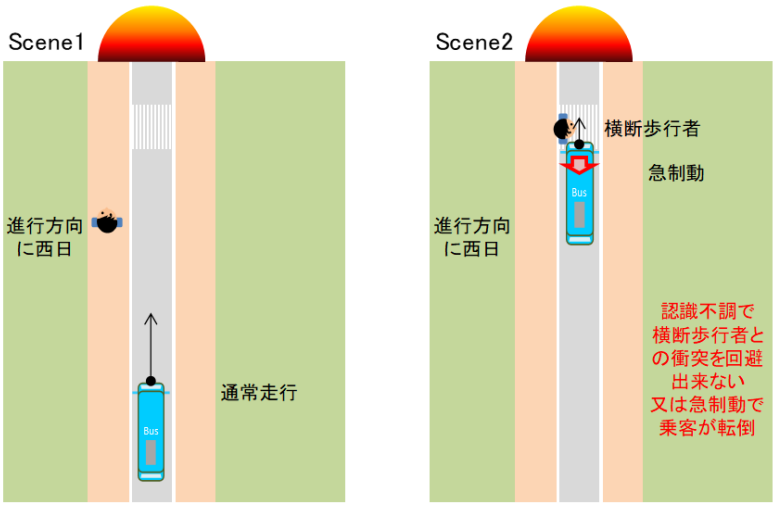



図 24　シナリオ例 11：西日など逆光／歩行者横断（認識外乱）

自動運転システムも遠隔監視員も気づかずに発車して降車客が引きずられるシナリオである。

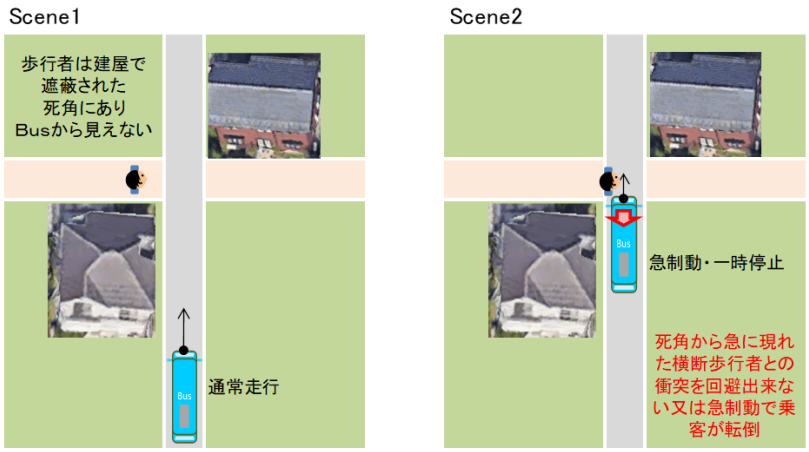



図 25　シナリオ例 12：死角からの歩行者飛出し（死角シナリオ）

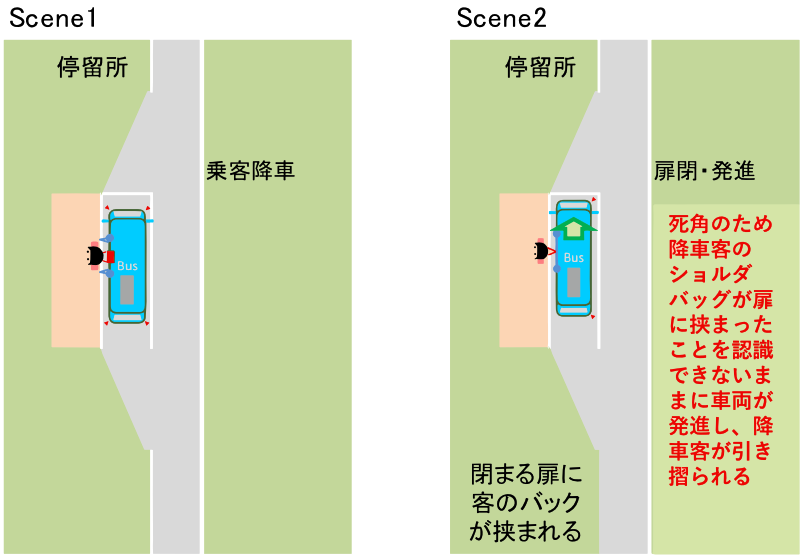



図 26　シナリオ例 13：停留所の死角にて降車客のバックが扉に挟み込む事例（死角シナリオ）

# 5　自動運転車の安全性に関する要配慮事項 2：安全設計コンセプト検討

4 章で設定した ODD、シナリオをもとに、本来機能（係る性能や仕様）の不十分性に対する安全性と、ハードウエアの故障やソフトウエアのバグなどの機能失陥に対する安全性

を、車両レベルや抽象的レベルで検討して、安全を確保するための方針を決定する。前者は国際規格 ISO 21448 (SOTIF) の範疇であり、後者は国際規格 ISO 26262（機能安全）の範疇である。また、本来機能（係る性能や仕様）の不十分性についての安全設計は、外乱なし・交通外乱あり・車両外乱あり・認識外乱あり（性能限界）・ミスユース（誤操作・誤使用）にシナリオを分類して安全設計を実施する。この物理原則に基づいた三種の外乱については、国際規格 ISO 34502（自動運転システムにおけるシナリオベース安全性評価フレームワーク）で導入されており、本ガイドブックでもシナリオの分類方法を踏襲する。

本章では、合理的に予見される人身事故を、合理的な安全方策で回避するように安全設計を実施する。本ガイドブックは、一般的なシステム開発 V 字プロセスにおいて上流工程である車両レベルや抽象的レベルの安全設計を記載する。

最初に、5.1 節では、本章で扱う安全設計の対象として車両レベルの機能定義を行う。具体的には、機能レベルアーキテクチャ（機能ブロック全体図）を明確にする。その後、本来機能の不十分性に対する安全設計（5.2 節：外乱なし、5.3 節：交通外乱／車両外乱、5.4 節：性能限界（認識外乱)、5.5 節：ミスユース等）と故障やバグに対する機能安全設計（5.6 節：故障やバグへの対処）に分けて説明する。

なお、5.2 節〜5.5 節に記載する本来安全と 5.6 節の機能安全では、以下の共通手順に沿って安全設計（車両レベル／抽象的レベル）を行う。

**安全設計手順**

- Step 1: ハザード分析

  ODD や機能ブロック図を参考にしながら、本来あってはならない危険なシナリオを想定してハザード[*14]と危険事象[*15]を抽出する。
- Step 2: リスクアセスメント

  前述のハザードごとに、曝露率 E、傷害度 S、制御可能性 C からリスクの大きさを評価する。リスクの大小から、対策実施の有無や優先度を決定する。
- Step 3: 安全目標設定

  ハザード分析とリスクアセスメントの結果を受けて、安全目標を設定する。

[*14] 潜在的な危害を与える要因

[*15] ハザードと運用状況の組合せ

- Step 4: 安全方策検討

  安全目標を達成できるように安全方策（対処方針）を決定する。

- Step 5: 機能レベル検証

  安全方策が想定仕様どおり機能して、安全目標が達成できるか、安全分析（演繹的分析／ FTA 等、帰納的分析／ FMEA 等)、シミュレーションテスト、実車テストなどで検証する。

図 27 に示すように、シナリオは危険でないシナリオと危険なシナリオ、また、既知のシナリオと未知のシナリオに分類される。5.2 節 ～ 5.5 節に記載する本来機能（係る性能や仕様）の不十分性に対する安全性では、上述の安全設計手順すなわちリスク低減活動を繰り返して実施することで、既知の危険でないシナリオ（エリア 1）を拡大する必要がある。

## 5.1 車両レベルの機能定義（既存システム）

4 章で設定した ODD とシナリオをもとに、自動運転旅客移動サービスを実現する自動運転システムの機能レベル基本アーキテクチャ（機能ブロック全体図）を作成して、安全

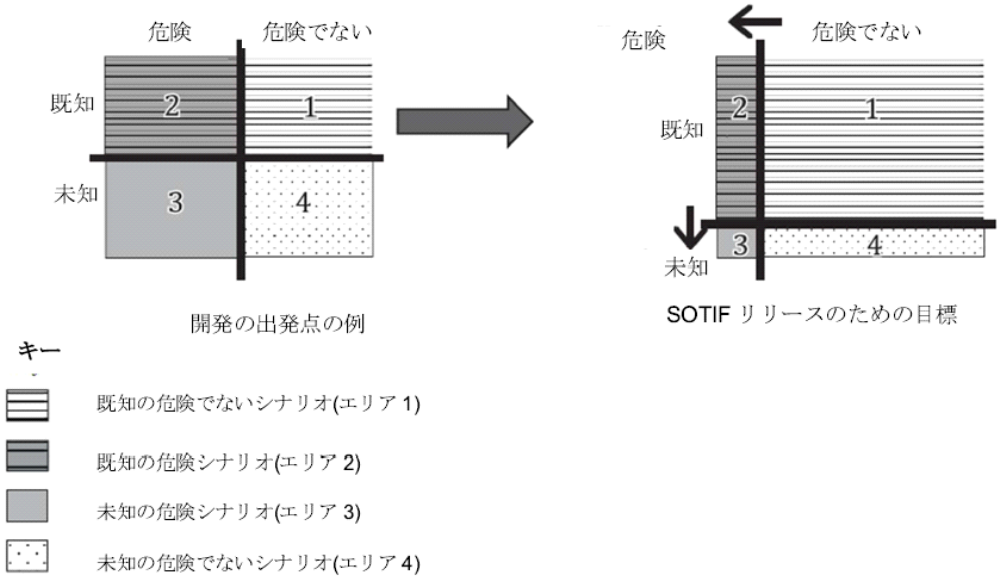



図 27　ISO21448 の活動として生じるシナリオカテゴリ別の進化（出典：ISO 21448/SOTIF 意図した機能の安全性）

設計（車両レベル／抽象的レベル）の対象となる機能範囲を明確にする。なお、この段階では、後述の安全設計で付加される各種の安全方策が未だ施されていない状態である。

### 5.1.1 必要理由

既に設定した ODD、シナリオをもとに、本来機能の安全性と、故障やバグなどの機能失陥に対する安全性を検討するための共通対象を、まずは機能レベルで明確にする必要がある。安全設計（車両レベル／抽象的レベル）では、ODD ／シナリオで特定化された「運用状況」と機能レベル基本アーキテクチャ（機能ブロック全体図）で特定化された「システム仕様」の両方が揃うことで、ハザード（危害の潜在的要因）や危険事象の洗出しなどが可能となる。

### 5.1.2 考え方

自動運転システムの機能が複数のサブシステムに跨るのであれば、それらサブシステムのすべてが対象である。たとえば、自動運転車載システムの他、遠隔監視支援システム、インフラ（地中に埋設した電磁誘導線、磁気マーカ、白線、信号機、踏切など）、インフラ協調システム（死角情報支援システム、信号情報提供システムなど）などである。

自動運転システムに期待する機能（機能要件）を、前述の ODD、シナリオをもとに洗い出す。さらに、それら機能処理の入出力情報をもとに各機能ブロックを繋ぐことで、機能レベル基本アーキテクチャ（機能ブロック全体図）を作成する。なお、後述する本来安全設計、機能安全設計ともに必要な共通作業である。

また、既にベースとなる原型システムとその機能ブロック図が存在するのであれば、前述の ODD、シナリオから導かれる機能レベルに抽象度合いを揃えたい。また、安全設計（車両レベル／抽象的レベル）の機能レベル基本アーキテクチャ（機能ブロック全体図）には、細かいハードウェアの区分け情報（コントローラボックス、電子基板など）は必要ないが、車載システム・遠隔監視支援システム・インフラ協調システムなど、物理的に距離があり無線などで情報を共有するシステムの区分け程度は必要である。

### 5.1.3　事例

レベル 4 自動運転移動サービスの自動運転システム*16を想定した機能レベル基本アーキテクチャ（機能ブロック全体図）の例を図 28 に示す。

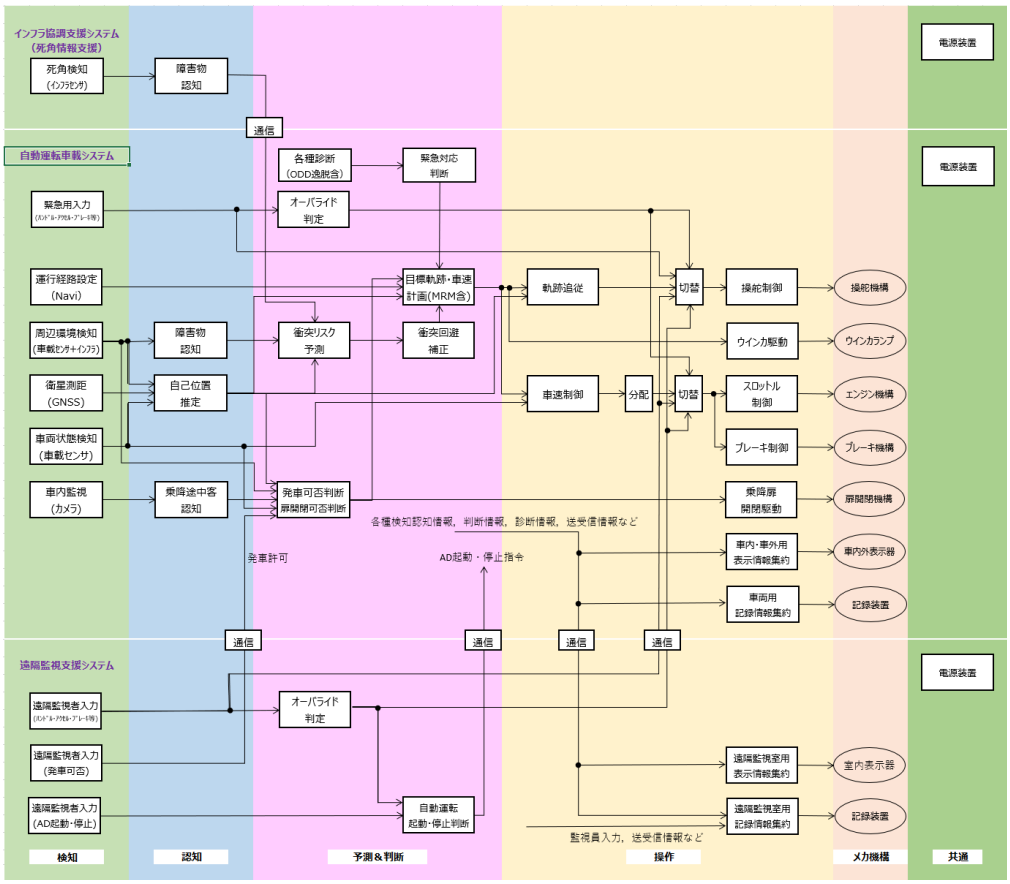



図 28　機能レベル基本アーキテクチャ（機能ブロック全体図）の例（旅客移動サービス用自動運転システム（レベル 4）を想定）

*16 自動運転車載システム・遠隔監視支援システム・インフラ協調システム（死角情報支援システム）で構成される。

## 5.2　本来安全 1：本来設計（外乱なし）

ODD 内で交通環境[*17]や自然環境[*18]から干渉されない状況を想定した安全設計の手順を説明する。

### 5.2.1　必要理由

交通環境や自然環境から干渉されない状況においても、自動運転車両システムを構成する機能の性能不足や仕様不備により、静止物・移動物などの障害物と衝突する、すなわち人身事故に至る可能性がある。これを避けるための要件を明確にする必要がある。

### 5.2.2　考え方

本来あってはならない安全設計・評価用シナリオ（以下、シナリオと表記する）を洗い出し、それぞれのシナリオにおける要因をハザード分析で明らかにしたうえで、リスクアセスメント、安全目標、安全方策、機能レベル検証の順に、車両レベル／抽象的レベルでの安全設計を行う。

### 5.2.3　ハザード分析

本来あってはならないシナリオの発生要因を機能ブロック図から特定し、ハザードと危険事象を抽出する。

**シナリオ例 1：急な曲線路での定速走行（通常走行　外乱なし）**

自動運転車両が急な曲線路に近づき、曲線路を低速で通過するように制動を開始したが、減速が不十分でコースアウトした。機能ブロック図（図 28）を用いてこのシナリオを説明すると以下のようになる。

目標軌跡・車速計画は自己位置推定で得られた曲線路入口までの距離に基づいて、その手前で曲線路を通過する車速になるように車速計画を作成した。この車速計画の目標車速と実車速が一致するように、ブレーキ制御はブレーキ機構への入力を調整した。しかしながら、曲線路手前での減速が不十分で、車速が高いまま曲線路に進入し、曲線路をコース

[*17] 交通参加者・落下物・交通規制など
[*18] 天候・日照・横風・路面 $\mu$ 変化など

アウトした。

**シナリオ例 1 の発生要因となる機能の例 1：自己位置推定**

あらかじめ用意された地図に対し、自動運転車両がどの位置にいるかを推定することを自己位置推定と呼ぶ。自己位置推定には多くの方式が存在するが、いずれの方式も何らかの理由により推定誤差が大きくなる場合がある。自動運転車両が曲線路の入口に近づく過程で自己位置を実際よりも進行方向手前に推定すると、車速制御による減速が遅れることになる。その推定誤差が大きいほど、遅れも大きくなり、車両がコースアウトする可能性が高まる。

- ハザード：自己位置推定の推定誤差の拡大（進行方向手前への誤推定）
- 危険事象：コースアウト

**（自己位置推定の補足）**

自動運転車の多くは、各種センサ情報をもとに自車位置（以下、自己位置と呼ぶ）を特定することで、自律的に走行することができる。センサの代表的なものとしては、GPS をはじめとする GNSS（Global Navigation Satellite System：全球測位衛星システム）や、非常に短い波長の電磁波であるレーザの反射光情報を元に対象までの距離や形状を計測する LiDAR (Light Detection And Ranging) などがある。

GNSS を用いた自己位置特定において、GNSS 受信機を二つ以上使う RTK などの相対測位による高精度位置測位や、タイヤの回転数を計測し走行距離を推定する DMI (Distance Measuring Instrument)、ジャイロや加速度センサが角度および速度の変化を計測し自己位置特定を支援する IMU (Inertial Measurement Unit) などの GNSS 補完機能もあるが、基本的な GNSS 受信機の測位精度は ±2∼3m であり、車線内の走行が基本である自動運転車両にとって GNSS の単独測位での自己位置特定は難しい。とくに、周辺に高層の建物がある場合、地下、高架下、トンネルを通過する場合などは通信が弱くなったり、失ってしまうこともある。しかし、受信状態が良いときであれば、RTK を用いた場合には誤差 2cm 程度の性能を発揮することもある。

また、自動運転車両の自己位置推定の手法として SLAM (Simultaneous Localization and Mapping) が知られている。SLAM による自己位置推定では、LiDAR 等で得られた物体の位置と、あらかじめ準備された地図上の静止物体（ランドマーク）の位置との照合

を行う。その際、LiDAR 等で検出した移動物体をランドマークと取り違えると自己位置推定に誤差が発生する。

磁気マーカを用いた自己位置推定では、車載する磁気センサが路面に埋め込まれた磁気マーカが発生する磁力を検出する。雨や雪などに影響されることもなく、距離の短いコースではインフラ整備の費用も抑えられるため有効な手法と考えられる。磁気マーカは上面を S 極や N 極にする自由度があり、規則に則って配置することにより、進行方向の位置を車両に伝えることができる。磁気センサは検知範囲が比較的狭く、目標軌跡の追従中に発生する蛇行により、磁気マーカを検出できないことが起こり得る。一般に、センシングの信号遅れや操舵機構の動作遅れは目標軌跡追従時の蛇行を助長する方向に働くため、それらの遅れが少なくなるように機材を選定するか、蛇行してもその幅が小さく済むように、自動運転の運行速度を低く設定する必要がある。

誘導ケーブルによる自己位置推定では路面に埋め込まれた誘導ケーブルに電流を流し、それが発する磁力を車載の磁気センサが検出する。磁気マーカと同じように雨や雪などに影響されることもなく、距離の短いコースではインフラ整備の費用も抑えられるため有効な手法と考えられる。磁気マーカ方式と同じく、センサの検知範囲が比較的狭く、その対策が必要である。

マップマッチングによる自己位置推定では、車両の走行時に記録された軌跡（所定時間前から現在までに車両が辿ってきた軌跡）にマッチングする道路ネットワークを探索する。GNSS などの自己位置推定を補う手法として用いられることが多い。道路ネットワークの情報や記録された軌跡の精度によっては自己位置推定に誤差を生じる場合も考えられる。

以上のように、自己位置を推定する手法は多数存在する。実際の走行環境を勘案の上、手法を選択することが重要である。選択する際には ODD を考慮することも考えられる。

自己位置推定がなんらかの理由で不良と判断された場合、自動運転車両はコース逸脱を防止すべくただちに停止する必要がある。自動運転中は多少の蛇行が発生していると考えられ、目標軌跡の接線方向と自動運転車両進行方向のなす角度はゼロを中心に所定の範囲内を変動している。角度が範囲の上限・下限値となった瞬間に自己位置不良に陥ると、最も早い逸脱（＝最悪ケースの逸脱）が発生する。この最悪ケースと停止距離を考慮し、走行コースの横方向に余裕を持たせる必要がある。走行コースが決まっており、余裕をあまり確保できない場合には、自動運転の運行速度を低くして停止距離を短くすることが考え

られる。また、曲率半径が小さいほど、逸脱が速くなる。そのことも勘案し、運行速度を決定する。

自動運転移動サービスでは走行コースが決められているため、自己位置推定に必要な地図はコースをカバーする小規模のものとなる。

自己位置推定に高さの推定を含むことも考えられる。一般道の上に高速道路が存在する地点で自動運転車両が一般道を走行しているか、それとも高速道路を走行しているかを判別するためには、自動運転車両の高さの推定が必要となる。自動運転移動サービスでは走行コースは固定であり、高さは 2 次元平面での自己位置推定と地図情報により推定できる。

**シナリオ例 1 の発生要因となる機能の例 2：緊急対応判断**

自己位置推定の誤差が大きい場合、緊急対応判断は自動運転を停止することができる。この閾値が大きいほど判断は遅れることになる。判断が遅れた場合に減速・停止が遅れ、コースアウトする。

- ハザード：緊急事態の判断遅れ
- 危険事象：コースアウト

**シナリオ例 1 の発生要因となる機能の例 3：目標軌跡・車速計画**

曲線路入口の直前で減速を完了する、安全余裕の小さい車速計画では、自己位置推定の進行方向の誤差によっては入口までの減速が完了できず、コースアウトする。

- ハザード：目標軌跡・車速計画の安全余裕の不足
- 危険事象：コースアウト

**シナリオ例 2：下り坂での減速・一時停止（通常走行／外乱なし）**

自動運転車両は遮断機の手前で停止するように制動を開始したが、下り坂で制動の遅れもしくは不足が発生してオーバーランした。機能ブロック図（図 28）を用いて説明すると以下のようになる。

自己位置推定で得られた車両の遮断器までの距離に基づいて、その手前で停止するように車速計画を作成した。この車速計画すなわち目標車速の時系列に実車速が一致するよう

に、ブレーキ制御はブレーキ機構への入力を調整したが、ブレーキ機構の発生する制動が遅れるか制動力が不足して遮断機手前で一時停止できず、オーバーランした。

**シナリオ例 2 の発生要因となる機能の例 1：自己位置推定**

シナリオ例 1 の場合と同じく、車両進行方向の推定誤差（進行方向手前への誤推定）により制動が遅れることが考えられる。

- ハザード：自己位置推定の推定誤差の拡大（進行方向手前への誤推定）
- 危険事象：遮断機のオーバーラン

**シナリオ例 2 の発生要因となる機能の例 2：ブレーキ制御**

ブレーキ制御の例として、道路勾配情報を用いたフィードフォワード制御と、目標車速と実車速の偏差に基づくフィードバック制御を挙げることができる。フィードフォワード制御は応答遅れがない長所を持つものの、たとえば車重変化などの制御対象の特性変化に対応できず[*19]、それに対応できるフィードバック制御と併用される。しかしながら、このような制御の構成を用いたとしても、その設計によっては車重変化に十分には対応した制動力が発揮できず、実車速が目標車速通りには下がらずに、すなわち実車速と目標車速の偏差が大きくなってオーバーランすることが考えられる。

- ハザード：ブレーキ制御の車重変化に対する適応性能不足
- 危険事象：遮断機のオーバーラン

**シナリオ例 2 の発生要因となる機能の例 3：ブレーキ機構**

ブレーキ機構が発生し得る最大制動力は機材により異なる。少なくとも乗客満載時でも余裕を持って停止できるような機材を選定しなければならない。逆に言えば、適切に選定されていない場合には制動力が不足することが考えられる。

- ハザード：ブレーキ機構の性能不足（最大制動力不足）
- 危険事象：遮断機のオーバーラン

[*19] 車重変化を推定してフィードフォワード制御と組み合わせることにより車重変化に対応することも考えられる。

**シナリオ例 2 の発生要因となる機能の例 4：目標軌跡・車速計画**

最大制動力や乗車満載の考慮が足りない車速計画では、ブレーキ機構の性能不足や乗客満載により、実際には発揮できない減速を行う車速計画が行われ、オーバーランが発生することが考えられる。

遮断機の直前で停止するような余裕のない車速計画では、自己位置推定の進行方向の誤差によってはオーバーランが発生することが考えられる。

- ハザード：目標軌跡・車速計画の安全余裕の不足
- 危険事象：遮断機のオーバーラン

**シナリオ例 3：上り坂での発進・加速（通常走行／外乱なし）**

交差車両が存在するときに遮断機が開き、交差点での発進が OK となり、目標軌跡・車速計画は車両が発進するように車速計画を作成した。この車速計画（目標車速）に実車速が一致するようにスロットル制御はエンジン機構への入力を調整した[*20]。しかしながら、上り坂の影響でエンジン機構の発生する駆動力が不足して、交錯する車両との接触が発生した。

**シナリオ例 3 の発生要因となる機能の例 1：スロットル制御**

スロットル制御の例として、道路勾配情報を用いたフィードフォワード制御と、目標車速と実車速の偏差に基づくフィードバック制御を挙げることができる。フィードフォワード制御は応答遅れがない長所があるものの、車重変化などの制御対象の特性変化に対応できず[*21]、それに対応できるフィードバック制御と併用される。しかしながら、このような制御の構成を用いたとしても、その設計によっては車重変化に十分には対応した駆動力が発揮できず、実車速が目標車速通りには上がらずに、すなわち目標車速と実車速の偏差が大きくなって意図した発進加速ができない可能性がある。

- ハザード：スロットル制御の車重変化に対する適応性能不足

---

[*20] ここでは従来のエンジン機構を有する車両を例として取り上げているが、EV 車であればモーターとその制御機構となる。ただし、本ガイドブックの以下の説明ではエンジン機構を例として説明する点に留意されたい。

[*21] 車重変化を推定してフィードフォワード制御と組み合わせることにより車重変化に対応することも考えられる。

- 交錯する車両との衝突

**シナリオ例 3 の発生要因となる機能の例 2：エンジン機構**

エンジン機構が発生できる駆動力が小さく、かつ、乗客満載などにより車重が大きい場合、発進不能となることが考えられる。

- ハザード：エンジン機構の性能不足（最大駆動力不足）
- 交錯する車両との衝突

### 5.2.4 リスクアセスメント

前述のシナリオごとに、曝露率 E、傷害度 S、制御可能性 C からリスクの大きさを評価する。リスクの大小から、対策実施の有無や優先度を決定する。国際機能安全規格 ISO 26262-3 の付属書 B に分類例が掲載されているので活用すると良い。表 3、4、5 を参照さ

表 3　曝露率の尺度（付属書 B より冒頭のみ抜粋）

**表 B.2　動作状況の期間に関する曝露の確率のクラス**

| | | 動作状況での曝露の確率のクラス（表2参照） | | | |
|---|---|---|---|---|---|
| | | **E1** | **E2** | **E3** | **E4** |
| 期間（平均動作時間の%） | | 規定なし | 平均動作時間の1%未満 | 平均動作時間の1～10% | 平均動作時間の10%超 |
| 例 | 道路レイアウト | – | • 安全でない急勾配な山岳路通過<br>• 田舎道の交差点<br>• ハイウェイ入口ランプ<br>• ハイウェイ出口ランプ | • 一方通行（市街地） | • ハイウェイ<br>• セカンダリーロード<br>• カントリーロード |
| | 路面 | | • 雪道または氷盤路 | • 濡れた道路 | |

**表 B.3　動作状況の頻度に関する曝露の確率のクラス**

| | | 動作状況での曝露の確率のクラス（表2参照） | | | |
|---|---|---|---|---|---|
| | | **E1** | **E2** | **E3** | **E4** |
| 状況の頻度 | | 大多数のドライバーにとっては、年に1回未満しか発生しない状況 | 大多数のドライバーにとっては、年に数回しか発生しない状況 | 平均的なドライバーにとっては、月に1回以上発生する状況 | 平均して、ほとんどすべての運転中に発生する状況 |
| 例 | 道路レイアウト | – | • 安全でない急勾配な山岳路通過 | – | – |
| | 路面 | | • 雪道または氷盤路 | • 濡れた道路 | |
| | 付近のエレメント | | | • トンネル内 | |

表 4　傷害度の尺度（付属書 B より冒頭のみ抜粋）

表 B.1 シビアリティの分類例

| | シビアリティのクラス(表1参照) | | | |
|---|---|---|---|---|
| | **S0** | **S1** | **S2** | **S3** |
| 単一傷害に対する参考（AIS尺度より） | • AIS 0 および AIS 1-6 の確率が10%未満<br>• 安全関連とは分類できない損害 | • AIS 1-6 の確率が10%以上（および、S2 または S3 ではない） | • AIS 3-6 の確率が10%以上（および、S3ではない） | • AIS 5-6 の確率が10%以上 |
| 例 | • 路側インフラストラクチャへの衝突<br>• 路側のポスト、フェンス、等の突き倒し | • 極低速での小幅な静止物への側面衝突。例えば、木への衝突（パッセンジャーセルへの衝突） | • 低速での小幅な静止物への側面衝突。例えば、木への衝突（パッセンジャーセルへの衝突） | • 中速での小幅な静止物への側面衝突。例えば、木への衝突（パッセンジャーセルへの衝突） |

表 5　制御可能性の尺度（付属書 B より冒頭のみ抜粋）

表B. 4　ドライバー又は潜在的リスクのある人によるコントロール可能な危険事象の例

| | 運転ファクタ及びシナリオ | コントローラビリティのクラス（表3参照） | | | |
|---|---|---|---|---|---|
| | | C0 | C1 | C2 | C3 |
| | | 大抵はコントロール可能 | すべてのドライバまたは他の交通当事者の99%以上が，通常，危害を回避できる。 | すべてのドライバまたは他の交通当事者の90%以上が通常，危害を回避できる。 | すべてのドライバまたは他の交通当事者の90%未満が，通常，危害を回避できる。又は，なんとか回避できる。 |
| 例 | 気を散らすと考えられる状況（気が散る状況） | 意図した運転経路を維持 | – | – | – |
| | 予想できないラジオの音量増加 | 意図した運転経路を維持 | – | – | – |
| | 警告メッセージ燃料低下 | 意図した運転経路を維持 | – | – | – |

れたい。

### 5.2.5　安全目標

車両レベルのハザード分析とリスクアセスメントの結果を受けて、安全目標を設定する。以下にその例を示す。なお、SG は Safety Goal の略である。

ただし、以下はあくまで考え方の例示であって、自動運転車の安全要件を定めたものではないことに留意されたい。

**シナリオ例 1 に関する安全目標の例**

SG1：（車重変化、天候条件、道路曲率等の）ODD 範囲内においてコースアウトが無いこと。

**シナリオ例 2 に関する安全目標の例**

SG2：（車重変化、天候条件、路面勾配等の）ODD 範囲内において一時停止時にオー

バーランが無いこと。また、停止時の自動運転車両と遮断機の距離が所定値以上であること。

**シナリオ例 3 に関する安全目標の例**

SG3：（車重変化、天候条件、路面勾配等の）ODD 範囲内において目標加速度と実加速度の差が所定値以下であること。

### 5.2.6 安全方策

シナリオごとに複数の方策が考えられる。方策をセットで実施することにより、各方策に課される条件を緩和でき、より現実的な解が得られる。

**シナリオ例 1 に関する安全方策の例**

- 自己位置推定

  誤差が想定する範囲[*22]に収まるように、アルゴリズム（ソフトウェア）を改良するのはもちろんのこと、自己位置推定の観測対象である道路周辺のインフラを整備することも考えられる。たとえば SLAM 方式による自己位置推定では、走行コース周辺の静止立体物（ランドマーク）を用いて自己位置推定を行う。ランドマークが多いほど、推定誤差が小さくなることが期待できるため、もしも、ランドマークが少ない場所が走行コース上にあれば、そこに位置情報表示施設を設置することも考えられる。

- 緊急対応判断

  緊急事態の判断閾値[*23]を適切に設定する。緊急事態の判断直後に緊急停止を開始してコースアウトがないように、すなわち緊急事態の判断が遅れないように判断指標を設定する。

---

[*22] コースアウトが無いことを実現できる誤差の範囲。緊急対応判断や目標軌跡・車速計画などの他の方策も行うことを前提としても良い。以降、範囲や閾値などの条件が説明されるが、ここでの内容と同様、他の方策とのセットを前提としても良い。

[*23] たとえば、GNSS 方式と SLAM 方式の自己位置を備えた自動運転システムにおいては、両者の推定値の偏差に対する許容値を指す。なお、この許容値を小さく設定すると緊急事態の判断の遅れは防げるが、選択した自己位置推定の手法によっては頻繁に緊急事態判断がなされることも考えられる。すなわち、許容値を小さくして判断の遅れを小さくするには限界がある。その場合には目標軌跡・車速計画などの安全方策とセットで行う必要がある。

- 目標軌跡・車速計画

  自己位置推定の推定誤差がある程度生じることを前提として、その上限となる誤差が発生しても曲線路入口で減速が完了するような車速計画を行う。すなわち、入口のかなり手前で目標車速が曲線路通過時に要求される目標車速となるような車速計画を行う。

**シナリオ例 2 に関する安全方策の例**

- 緊急対応判断

  緊急事態の判断指標を適切に設定する。シナリオ例 1 の安全方策で記載した内容と同じである。

- ブレーキ制御

  ODD 範囲内において目標速度と実速度の差が所定値以下（小さい値）となるようにブレーキ制御を設計する。

- ブレーキ機構

  急な下り坂、定員満載状態でも想定する減速度が発揮できるようにブレーキ機構を設計する。もしくは、ブレーキ機構を構成する機材を選定する。

- 目標軌跡・車速計画

  自己位置推定の推定誤差や、ブレーキ制御による目標車速と実車速の偏差をあらかじめ考慮した車速計画を行う。たとえば、停止位置と遮断器の距離に余裕を持たせた車速計画を行う。

**シナリオ例 3 に関する安全方策の例**

- スロットル制御

  ODD 範囲内において目標速度と実速度の差が所定値以下（小さい値）となるようにスロットル制御を設計する。

- エンジン機構

  定員満載状態でも想定する加速度が発揮できるようにエンジン機構を設計する。もしくは、エンジン機構を構成する機材を選定する。

### 5.2.7 機能レベル検証

安全方策の各項目を検証する。安全目標が達成できない場合には安全方策を見直す。安全目標が達成された後、自動運転移動サービスの事業者はその検証内容を文書化して保管する。ODD 範囲内において膨大な量の検証が必要な場合はシミュレーションの活用が有効と考えられる。ただし、複数の条件で実車実験も並行して行い、シミュレーションの妥当性を確認しておく必要がある。

**シナリオ例 1 に関する機能レベル検証の例**

- 自己位置推定

  ODD 範囲内において自己位置推定の誤差が想定する範囲に収まっていることを確認する。たとえば、自己位置推定が最も劣化する条件を洗い出し、その条件下でも機能が安全目標を満たしていることを確認する。
- 緊急対応判断

  シナリオ例 1 と同じような曲線路に接近する過程で、自己位置推定に誤推定を発生（緊急事態の判断閾値を超える誤推定を発生）させて緊急対応判断が非常停止を行った結果、コースアウトが無いことを確認する。
- 目標軌跡・車速計画

  自己位置推定の推定誤差をあらかじめ考慮した車速計画を作成することによって、ODD 範囲内においてコースアウトが無いことを確認する。

**シナリオ例 2 に関する機能レベル検証の例**

- 自己位置推定

  ODD 範囲内において自己位置推定の誤差が想定する範囲に収まっていることを確認する。
- ブレーキ制御

  ブレーキ制御による目標速度と実速度の差が ODD 範囲内において所定値以下（小さい値）となることを検証する。
- ブレーキ機構

（車重変化、天候条件、路面勾配等の）ODD 範囲内において目標とする減速度が発揮できることを検証する。

- 目標軌跡・車速計画

  自己位置推定の推定誤差（進行方向誤差）をあらかじめ考慮したうえで車速計画を作成することで、ODD 範囲内において一時停止時にオーバーランが無いこと、また、停止時の自動運転車両と遮断機の距離は所定値以上であることを検証する。

**シナリオ例 3 に関する機能レベル検証の例**

- スロットル制御

  スロットル制御による目標速度と実速度の差が ODD 範囲内において所定値以下となることを検証する。

- エンジン機構

  ODD 範囲内において目標とする加速度が発揮できることを検証する。

## 5.3 本来安全 2：本来設計（外乱あり／センサ認識系除く）

ODD 範囲内、かつ交通環境[*24]や自然環境[*25]から干渉される状況において、自動運転車両が静止物や移動物などの周囲の障害物と衝突することがなく、すなわち人身事故が発生することなく、安全に自動運転するための要件を明確にする。

### 5.3.1 必要理由

交通環境や自然環境から干渉される状況においても、自動運転車両システムを構成する機能の性能不足や仕様不備により、静止物や移動物などの障害物と衝突する、すなわち人身事故に至る可能性がある。これを避けるための要件を明確にする必要がある。

### 5.3.2 考え方

認識外乱が強まって、センサ認識系が性能限界に至る場合は性能限界の項で記載する。ここでは交通外乱と車両外乱への対処だけを示す。本来あってはならない安全設計・評価用シナリオを洗い出し、それぞれのシナリオにおける要因をハザード分析で明らかにしたうえで、リスクアセスメント、安全目標、安全方策、機能レベル検証の順に車両レベル／抽象的レベルの安全設計を行うことは本来設計（外乱なし）と同じである。

### 5.3.3 ハザード分析

本来あってはならないシナリオの発生要因を機能ブロック図（図 28）から特定し、ハザードと危険事象を抽出する。

**シナリオ例 4：一般公道と自動運転専用道の交差路を横断（交通外乱）**

交差車両の接近状態から衝突は発生しないと判断して、自動運転車両が発進した。その後、交差車両が加速など、発進判断時の予想と異なる行動を行い、自動運転車両に衝突した。このシナリオを機能ブロック図（図 28）を用いて説明すると以下のようになる。

周辺環境検知は左方から接近中の物体を検出し、障害物認知はそれを自動車と判断した。衝突リスク予測は自動車と判断した交差車両の位置、速度および自動運転車両の位置

[*24] 交通参加者・落下物・交通規制など。
[*25] 天候・日照・横風・路面 $\mu$ 変化など。

から衝突リスクがゼロであると予測した。目標軌跡・車速計画が発進のための車速計画を作成した。この車速計画（目標車速）に実車速が一致するように、スロットル制御はエンジン機構への入力を調整して自動運転車両は発進した。その後、交差車両が速度を上げて、自動運転車両に衝突した。

**シナリオ例 4 の発生要因となる機能の例：衝突リスク予測**

交差車両の速度や位置を用いた衝突リスク予測に、どの程度不確定要素（加速度等）を考慮するかによっては予測結果に差が生じることが考えられる。

- ハザード：衝突リスク予測の衝突予測の遅れ
- 危険事象：衝突

**シナリオ例 5：歩道歩行者の転倒または飛出し（交通外乱）**

自動運転車両の前方を移動中の歩行者が転倒もしくは飛び出して、コースに進入した。自動運転車両は急制動を行ったが、歩行者と衝突した。また、急制動によって乗客が転倒して負傷した。このシナリオを機能ブロック図（図 28）を用いて説明すると以下のようになる。

周辺環境検知は前方を移動中の物体を検出し、障害物認知はそれを歩行者と判断した。衝突リスク予測は歩行者の位置および自己位置推定から衝突リスクが高いと予測した。衝突回避補正は衝突を避けるための指令を目標軌跡・車速計画に出力した。目標軌跡・車速計画は衝突回避もしくは衝突時の衝撃低減のための車速計画を作成した。このとき、減速度が許容値以下となるように車速計画が作成される。この車速計画、すなわち目標車速に実車速が一致するように、ブレーキ制御はブレーキ機構への入力を調整した。しかしながら、衝突を回避するために必要な減速度が許容値を超過しており、自動運転車両は歩行者に衝突した。また、許容できる最大の減速度が発生し、自動運転車両内の乗客が転倒した。なお、操舵による衝突回避も考えられるが、ここでの記載は省略した。

**シナリオ例 5 の発生要因となる機能の例 1：衝突リスク予測**

衝突リスク予測では、歩行者の自動運転車両に対する位置や速度、その他、ガードレールの有無や白線の存在などの周囲の交通環境に関する情報を用いて衝突リスクを予測する。予測の遅れにより衝突が発生することが考えられる。

- ハザード：衝突リスク予測の衝突予測の遅れ
- 危険事象：衝突

**シナリオ例 5 の発生要因となる機能の例 2：目標軌跡・車速計画**

通常の走行状態（定速走行）の車速が高い場合、停止までの時間がかかり衝突が発生することが考えられる。

- ハザード：通常の走行状態（定速走行）での高い車速
- 危険事象：衝突

**シナリオ例 6：小さな障害物（倒木・岩等）や地割れなど（交通外乱）**

自動運転車両のコース前方に小さな障害物（低い障害物）もしくは地割れなどがあり、その検出ができず、障害物への乗上げもしくは地割れを通過した。乗上げ時または地割れ通過時の上下加速度や前後加速度により乗客が転倒した。このシナリオを機能ブロック図（図 28）を用いて説明すると以下のようになる。

周辺環境検知は小さな障害物（低い障害物）もしくは地割れを検出できず、障害物認知は何も認知しない状態で、衝突リスク予測はリスクがないと判断した状態で、自動運転車両は走行を継続した。衝突回避補正は回避補正の指令を出力せず、目標軌跡・車速計画は通常の走行状態（定速走行）が維持されるように車速計画を作成した。その結果、通常の走行状態で自動運転車両は障害物に乗り上げた、もしくは地割れを通過した。乗上げ、もしくは地割れ通過に伴う上下加速度や前後加速度が発生し、自動運転車両の乗客が転倒した。

**シナリオ例 6 の発生要因となる機能の例 1：周辺環境検知**

検知できない障害物のサイズの範囲が広いほど（たとえば、高さが高いほど)、障害物を乗り上げたときの上下加速度や前後加速度の最大値は大きくなる。同様に、検知できない地割れのサイズの範囲が広いほど、上下加速度や前後加速度の最大値は大きくなると考えられる。

- ハザード：乗り上げてはいけない小さい物体が検知できないこと。通過してはいけない大きさの地割れが検知できないこと。

- 危険事象：乗客の転倒、車両の転覆

**シナリオ例 7：強い横風下での車線維持走行（車両外乱）**

横風の影響でコースアウトした。このシナリオを機能ブロック図（図 28）を用いて説明すると以下のようになる。

自己位置推定による自動運転車両の位置と目標軌跡に基づき、軌跡追従は目標操舵角を算出した。横風に対する目標操舵角の補正が十分ではなく、自動運転車両がコースから逸脱した。

**シナリオ例 7 の発生要因となる機能の例 1：軌跡追従**

軌跡追従は自動運転車両の位置に関するフィードバック制御となっており、横風などの外乱にはある程度は対応できる。しかしながら、このような制御構成を用いたとしても、制御器の設計次第では外乱に十分には対応できず、自動運転車両がコースから逸脱することが考えられる。

- ハザード：軌跡追従制御の性能不足
- 危険事象：コースアウト

**シナリオ例 8：低 $\mu$ 路面での制動・停車（車両外乱）**

停留所に停車しようと減速したが、路面凍結の影響でコースアウトした。このシナリオを機能ブロック図（図 28）を用いて説明すると以下のようになる。

目標軌跡・車速計画は停留所に停車するように軌跡・車速計画を作成した。車速制御は車速計画（目標車速）に実車速が追従するようにブレーキ制御への入力を調整した。また、軌跡追従は自動運転車両を目標軌跡に追従するように目標操舵角を調整した。操舵制御は目標操舵角に実操舵角が追従するように操舵機構の入力を調整した。その結果、操舵や速度調整（制動）が行われたものの、路面の摩擦係数 $\mu$ が低く、車両挙動が軌跡追従で想定する挙動から外れて、コースアウトした。

**シナリオ例 8 の発生要因となる機能の例 1：目標軌跡・車速計画**

路面摩擦係数 $\mu$ が低い状態では達成困難な車速計画を目標軌跡・車速計画が作成することによってタイヤスリップが発生し、自動運転車両がコースから逸脱することが考えら

れる。

- ハザード：目標軌跡・車速計画の路面 $\mu$ 変化に対する対応性能不足
- 危険事象：コースアウト

**シナリオ例 8 の発生要因となる機能の例 2：ブレーキ機構**

ここではタイヤもブレーキ機構を構成する要素とする。路面摩擦係数 $\mu$ が低い冬場ではタイヤが発揮できる制動力の範囲が狭くなる。その結果、ブレーキ制御によって実車速を目標車速に追従させることができず、タイヤスリップが発生し、自動運転車両がコースから逸脱することが考えられる。

- ハザード：ブレーキ機構（タイヤ）の性能不足（制動力）
- 危険事象：コースアウト

**シナリオ例 8 の発生要因となる機能の例 3：操舵機構**

ここではタイヤも操舵機構を構成する要素とする。路面摩擦係数 $\mu$ が低い冬場ではタイヤが発揮できる横力の範囲が狭くなる。その結果、軌跡追従によって自動運転車両を目標軌跡に追従させることができなくなることが考えられる。

- ハザード：操舵機構（タイヤ）の性能不足（横力）
- 危険事象：コースアウト

**シナリオ例 9：低 $\mu$ 路面での発進・加速（車両外乱）**

停留所から発進しようと加速したが、路面凍結の影響でコースアウトした。このシナリオを機能ブロック図（図 28）を用いて説明すると以下のようになる。

目標軌跡・車速計画は停留所から発進するようにも軌跡・車速計画を作成した。車速制御は車速計画（目標車速）に実車速が追従するようにスロットル制御への入力を調整した。また、軌跡追従は自動運転車両を目標軌跡に追従するように目標操舵角を調整した。操舵制御は目標操舵角に実操舵角が追従するように操舵機構の入力を調整した。その結果、操舵や車速調整（制動）が行われたが、タイヤスリップが発生して車両の挙動が軌跡追従で想定する挙動から外れて、コースアウトした。

**シナリオ例 9 の発生要因となる機能の例 1：目標軌跡・車速計画**

路面摩擦係数 $\mu$ が低い状態では達成困難な車速計画を目標軌跡・車速計画が作成することによってタイヤスリップが発生し、自動運転車両がコースから逸脱することが考えられる。

- ハザード：目標軌跡・車速計画の路面 $\mu$ 変化に対する対応性能不足
- 危険事象：コースアウト

**シナリオ例 9 の発生要因となる機能の例 2：エンジン機構**

ここではタイヤも駆動力を発生するための要素としてエンジン機構に含まれるものとする。路面摩擦係数 $\mu$ が低い冬場ではタイヤが発揮できる駆動力が小さくなる。その結果、スロットル制御によって実車速を目標車速に追従させることができず、タイヤスリップが発生し、自動運転車両がコースから逸脱することが考えられる。

- ハザード：エンジン機構（タイヤ）の性能不足（駆動力）
- 危険事象：コースアウト

**シナリオ例 9 の発生要因となる機能の例 3：操舵機構**

ここではタイヤやチェーンも操舵機構を構成する要素とする。路面摩擦係数 $\mu$ が低い冬場ではタイヤが発揮できる横力が小さくなる。その結果、軌跡追従によって自動運転車両を目標軌跡に追従させることができず、タイヤスリップが発生し、自動運転車両がコースから逸脱することが考えられる。

- ハザード：操舵機構（タイヤ）の性能不足（横力）
- 危険事象：コースアウト

### 5.3.4 リスクアセスメント

危険事象ごとに曝露率 E、傷害度 S、制御可能性 C からリスクの大きさを評価する。リスクの大小から、対策実施の有無や優先度を決定する。国際機能安全規格 ISO 26262-3 の付属書 B に分類例が掲載されているので活用すると良い。表 3、4、5 を参照されたい。

### 5.3.5　安全目標

ハザード分析とリスクアセスメントの結果を受けて、安全目標を設定する。以下にその例を示す。

**シナリオ例 4 に関する安全目標**

SG4：ODD 範囲内で、自動運転車両にとって合理的に予見可能で回避可能な行動を交差車両が行ったとしても、衝突が無いこと。

**シナリオ例 5 に関する安全目標**

SG5：ODD 範囲内で、自動運転車両にとって合理的に予見可能で回避可能な行動を歩行者が行ったとしても、乗客の転倒が無いこと。

**シナリオ例 6 に関する安全目標**

SG6：ODD 範囲内において乗客の転倒が無いこと。

**シナリオ例 7 に関する安全目標**

SG7：ODD 範囲内においてコースアウトが無いこと。

**シナリオ例 8 に関する安全目標**

SG8：ODD 範囲内においてコースアウトが無いこと。

**シナリオ例 9 に関する安全目標**

SG9：ODD 範囲内においてコースアウトが無いこと。

### 5.3.6　安全方策

安全目標の項目ごとに安全方策を立案する。以下にその例を示す。

**シナリオ例 4 に関する安全方策**

- 衝突リスク予測

  安全サイド側に立って交差車両との衝突のリスク予測を行う。

**シナリオ例 5 に関する安全方策**

- 衝突リスク予測

  安全サイド側に立って歩行者との衝突のリスク予測を行う。

- 目標軌跡・車速計画

  歩行者との衝突を避けるべく急停車が発生した場合、その減速加速度が乗員転倒につながらないよう、通常の走行状態（定速走行）での車速を低速側に設定する。

**シナリオ例 6 に関する安全方策**

- 周辺環境検知

  周辺環境検知の検知できる障害物・地割れの範囲を広くする。すなわち、より低い障害物を検知できるように、また、より小さい地割れを検知できるようにする。

- 目標軌跡・車速計画

  目標軌跡・車速計画は通過車速を低速側に設定する。その結果、乗上げ時や地割れ通過時の上下加速度や前後加速度を許容値以下とする。

**シナリオ例 7 に関する安全方策**

- 軌跡追従

  ODD の範囲内で想定されるいかなる横風が発生したとしても自動運転車両がコースから逸脱しないように、軌跡追従の制御を設計する。

- 周辺環境検知

  横風の強さを監視する仕組み（インフラセンサによる横風検出部）を導入する。目標軌跡の追従が可能な横風の許容値をあらかじめ調べておき、機能ブロックの各種診断が横風検出部から許容値以上の横風を受けているとの情報を受け次第、緊急対応判断は軌跡追従や車速制御を介して自動運転車両を停止させる。乗員・遠隔監視者による異常対応を行う。たとえば、強風による運転停止の状況や運転再開見込みなどを、乗員もしくは遠隔監視者が乗客へアナウンスする。

  監視する仕組みはコースの要所に設置されたインフラセンサも考えられる。ま

た、横風を推定することで監視を代用することも考えられる。

**シナリオ例 8 に関する安全方策**

- 目標軌跡・車速計画

  目標軌跡・車速計画は路面摩擦係数 $\mu$ が低い状態でも達成可能な車速計画を作成する。$\mu$ が推定できる場合にはその推定値に応じて車速計画を変更することも考えられる。ただし、$\mu$ は急変することもあるので、車速計画は安全サイドに設定する。たとえば、冬場では瞬間的に $\mu$ の推定値が高くなったとしても $\mu$ が低いことを想定した車速計画を継続する。

- ブレーキ機構

  自動運転車両のタイヤとして、季節に応じて適切なタイヤを選定する。たとえば、冬場はスノータイヤを使用する。

- 操舵機構

  自動運転車両のタイヤとして、季節に応じて適切なタイヤを選定する。たとえば、冬場はスノータイヤを使用する。冬場にスノータイヤを使用することで、操舵機構のタイヤ能力を軌跡追従制御が想定する範囲に収める。

**シナリオ例 9 に関する安全方策**

- 目標軌跡・車速計画

  目標軌跡・車速計画は路面摩擦係数 $\mu$ が低い状態でも達成可能な車速計画を作成する。$\mu$ が推定できる場合にはその推定値に応じて車速計画を変更することも考えられる。ただし、$\mu$ は急変することもあるので、車速計画は安全サイドに設定する。たとえば、冬場では瞬間的に $\mu$ の推定値が高くなったとしても $\mu$ が低いことを想定した車速計画を継続する。

- エンジン機構

  自動運転車両のタイヤとして、季節に応じて適切なタイヤを選定する。たとえば、冬場はスノータイヤを使用する。

- 操舵機構

  自動運転車両のタイヤとして、季節に応じて適切なタイヤを選定する。たとえ

ば、冬場はスノータイヤを使用する。冬場にスノータイヤを使用することで、操舵機構のタイヤ能力を軌跡追従制御が想定する範囲に収める。

### 5.3.7 機能レベル検証

安全方策の各項目を検証する。安全目標が達成できない場合には安全方策を見直す。安全目標が達成された後、自動運転移動サービスの事業者はその検証内容を文書化して保管する。ODD 範囲内において膨大な量の検証が必要な場合は、シミュレーションを活用することが考えられる。ただし、複数の条件で実車実験も並行して行い、シミュレーションの妥当性を確認しておく。これは本来設計（外乱なし）と同じである。

#### シナリオ例 4 に関する安全検証

- 衝突リスク予測

  交差車両が想定されるいかなる挙動を行ったとしても、衝突リスク予測機能がリスクを適切に予測し衝突が発生しないことを検証する。

#### シナリオ例 5 に関する安全検証

- 衝突リスク予測

  歩行者が想定されるいかなる挙動を行ったとしても、衝突リスク予測機能がリスクを適切に予測し衝突が発生しないことを検証する。
- 目標軌跡・車速計画

  歩行者が想定されるいかなる挙動を行ったとしても、目標軌跡・車速計画が定常走行の車速を低速側に設定していたことにより衝突が発生しないことを検証する。

#### シナリオ例 6 に関する安全検証

- 周辺環境検知

  周辺環境検知の検出範囲が意図通りに広がったことを検証する。
- 目標軌跡・車速計画

障害物や地割れの通過車速が低速となり、乗上げ時や地割れ通過時の上下加速度や前後加速度が許容値以下となることを検証する。

### シナリオ例 7 に関する安全検証

- 軌跡追従

  想定されるあらゆる横風に対して、自動運転車両の目標軌跡からの逸脱量が許容できる範囲内に収まることを検証する。

- 周辺環境検知

  許容値よりも強い横風が発生したとき、横風検出部の検出結果を受けて緊急対応判断が自動運転車両を停止させることを検証する。

### シナリオ例 8 に関する安全検証

- 目標軌跡・車速計画

  路面摩擦係数 $\mu$ に応じて目標軌跡・車速計画が適切な車速計画を作成し、実車速と目標車速の偏差が所定値以内であることを検証する。

- ブレーキ機構

  自動運転車両のタイヤとして、季節に応じた適切なタイヤを選定することにより、実車速と目標車速の偏差が所定値以内であることを、実車実験を通じて検証する。

- 操舵機構

  自動運転車両のタイヤとして、季節に応じた適切なタイヤを選定することにより、実軌跡と目標軌跡の偏差が所定値以内であることを、実車実験を通じて検証する。

### シナリオ例 9 に関する安全検証

- 目標軌跡・車速計画

  路面摩擦係数 $\mu$ に応じて目標軌跡・車速計画が適切な車速計画を作成し、実車速と目標車速の偏差が所定値以内であることを検証する。

- エンジン機構

  自動運転車両のタイヤとして、季節に応じた適切なタイヤを選定することにより、実車速と目標車速の偏差が所定値以内であることを、実車実験を通じて確認する。

- 操舵機構

  自動運転車両のタイヤとして、季節に応じた適切なタイヤを選定することにより、実軌跡と目標軌跡の偏差が所定値以内であることを、実車実験を通じて確認する。

## 5.4 本来安全 3：性能限界（センサ認識系）

ODD（経路限定など）内で自動運転旅客移動サービスを提供するレベル 4 自動運転システムにおいて、その一部の機能が性能限界に至って本来機能を喪失したとしても、自動運転車両が静止物や移動物などの周囲の障害物と衝突する（人身事故を起こす）ことなく、安全に走行するための要件を明確にする。

なお、本ガイドブックでは、センサ認識（認知）機能の性能限界のみを説明することに注意されたい。操作機能の性能限界に対する安全設計は、路面タイヤ間の摩擦円特性など従来のドライバ運転車と同じである。また、予測判断機能の性能限界に対する安全設計は、トロッコ問題（リスク回避の優先付）のような倫理的な側面も有しており、今後の政府等の取組みや検討に注視されたい。

### 5.4.1 必要理由

センサ認識系の性能限界は、電子部品の偶発故障などと異なり、走行環境（天候や日照、死角など）によっては高い頻度で性能限界に至り、本来機能を喪失して静止物や移動物などの周囲の障害物と衝突する（人身事故に至る）可能性がある。

したがって、以下の三つのケースを考える必要がある。

- CASE 1

  ODD 内であってセンサ認識系が性能限界に至らず、自動運転旅客移動サービス車が周囲と衝突することがない場合、安全に自動運転を継続するための要件を明確にする必要がある。

- CASE 2

  自動運転中に走行環境などが悪化して ODD を逸脱することでセンサ認識系が性能限界に至る場合、自動運転旅客移動サービス車両が周囲と衝突することがなく、安全な車両状態へ移行するための要件を明確にする必要がある。

- CASE 3

  ODD 内であってもセンサ認識系が性能限界に至る場合、障害物との衝突やタイヤ踏み越え時の衝撃による乗客や乗員への傷害を回避するための要件を明確にする必要がある。障害物の最大検知距離や最低検知高などが該当する。

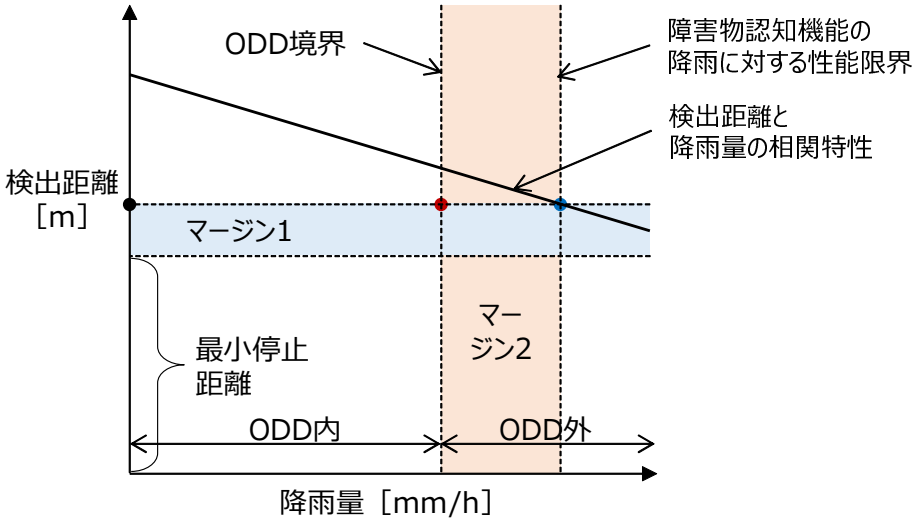



図 29　ODD と性能限界の関係（イメージ）（降雨量に対するセンサ認識性能の例）

CASE3 は本来機能の基本設計であり本節での説明は割愛する。

### 5.4.2　考え方

ODD と性能限界を考慮したセンサ認識系の安全設計方針を図 29 を使って示す。

- Step 1

  センサ認識系の本来機能を阻害する要因が無い場合、動的運転タスク[*26]の実現が必要な交通外乱シナリオにおいて、検出距離などのセンサ認識性能に特定の余裕度（マージン 1：センサ認識性能のバラツキ対応）を伴って衝突を回避できる必要がある。（例：図 29 中の黒点以上の検出距離が必要）

- Step 2

  センサ認識系の阻害要因の度合が ODD 境界以内にある場合、動的運転タスクの実現が必要な交通外乱シナリオにおいて、検出距離などのセンサ認識性能に特定の余裕度（マージン 1：センサ認識性能のバラツキ対応）を伴って衝突を回避できる必要がある。（例：図 29 中の赤点以上の検出距離が必要）

- Step 3:

[*26] たとえば、乗客転倒防止のために所定減速度以下という制約付きで、障害物との衝突回避など。

センサ認識系の阻害要因の度合が増して性能限界に至るまでの間に、検出距離などのセンサ認識性能に特定の余裕度（マージン 2：ODD 境界判定のバラツキ対応）が必要である。（例：図 29 中の青点以上の検出距離が必要）

以上、ODD とセンサ認識系の性能限界における静的な関係について説明した。これは、5.4.1 節に示した CASE 1 に相当する。一方、自動運転中に走行環境などが悪化して、最終的に ODD から逸脱する CASE 2 について説明する。降雨量などセンサ認識系の性能阻害要因が ODD 境界に近づいた際には縮退運転モード[*27]で自動運転を継続し、ODD 境界を超えたことを検知した際には MRM を起動させて路肩などへの自動停車などの最小リスク状態へ移行して自動運転を停止する。

上述の考え方で安全設計を行って適切なセンサ認識系を選択するために、以下の検討が必要である。

認識外乱、すなわちセンサ認識系の各種阻害要因[*28]に対する認知性能[*29]の相関特性（センサ認識系単体）を、センサ認識系の開発製造者から情報入手するか、環境試験施設を使って新たに計測実験を行い入手しなければならない。さらに、センサの車両設置情報[*30]を加えて、車両設置された状態での各種阻害要因に対する認知性能の相関特性を見積っておく必要がある。

上述の考え方に基づいて、ハザード分析、リスクアセスメント、安全目標、安全方策、機能レベル検証の順に安全設計（車両レベル／抽象的レベル）を行う。

### 5.4.3 ハザード分析

前述の ODD（経路限定など）で限定された安全設計・評価用シナリオと機能レベル基本アーキテクチャをもとに、センサ認識系の本来機能が大きく阻害されたり性能限界に至って破綻するハザード（潜在的な危害を与える要因）と危険事象（ハザードと運用状況の組合せ）を漏れなく抽出する。HAZOP (HAZard and OPerability studies)、STAMP/STPA (Systems Theoretic Accident Model and Processes/System Theoretic Process Analysis) などの手法を活用することを推奨する。HZ は HaZardous event の略

[*27] 通常の自動運転モードよりも上限車速を下げた自動運転モードなど。
[*28] 降雨、降雪、霧、西日、薄暮、センサや対象物の汚れ、マルチパスなど。
[*29] 最大検知距離、最小検知距離、検知方位、精度、分解能、属性認識率など。
[*30] 設置高、設置方位（水平角・俯角）、センサ種と数など

である。

事例による説明を以下に示すにあたり、4.4 節のシナリオ設定で事例として挙げたいくつかのクリティカルまたはプレクリティカルなシナリオ例を参照する。

図 23 のシナリオ例 10：急な豪雨、図 24 のシナリオ例 11：西日など逆光は、認識外乱と交通外乱（歩行者横断）を組み合わせたシナリオ事例である。図 25 のシナリオ例 12：交差路の死角は、認識外乱（死角）と交通外乱（交差路で歩行者横断）を組み合わせたシナリオ事例である。図 26 のシナリオ例 13：乗降用扉前後の死角は、認識外乱（死角）と交通外乱（停留所降車客の自動扉挟み込み）を組み合わせた具体的なシナリオ事例である。以下の例 1 はシナリオ例 10 に、例 2 はシナリオ例 11 に、例 3 はシナリオ例 12 に、例 4 はシナリオ例 13 に相当する。

**例 1：（原理）計測用電磁波の伝搬減衰による不検知**

HZ1：ODD（経路制限など）内を自動運転する際、自然環境の悪化（雨、雪、霧など）、障害物の低反射特性（黒色、ステルス形状など）、車両の整備不良（センサ汚れなど）によって、センサ認識系が性能低下や性能限界に陥り、障害物などの不検知が生じて（ハザード）、周辺障害物（静止物・移動物）との衝突回避に必要な減速などがなされない状態（危険事象）に至る。

**例 2：（原理）対象物と背景のコントラスト不足や過度な特性乖離による不検知**

HZ2：ODD（経路制限など）内を自動運転する際、周辺障害物と背景のコントラスト不足（背景同色など）や、過度な特性乖離（朝日・西日などに起因する逆光など）によって、センサ認識系が性能阻害や性能限界に陥り、障害物などの不検知が生じて（ハザード）、周辺障害物（静止物・移動物）との衝突回避に必要な減速などがなされない状態（危険事象）に至る。

**例 3：（原理）死角による不検知**

HZ3：ODD（経路制限など）内を自動運転（非優先道を交差横断）する際、周辺障害物（非優先道の車両や歩行者など）を、交差点周辺建屋で生じる死角によって、センサ認識系が性能阻害や性能限界に陥り、障害物などの不検知が生じて（ハザード）、周辺障害物との衝突回避に必要な減速が接近直前（死角解消）までなされない状態（危険事象）に至る。

**例 4：（原理）死角や認識処理不良による不検知**

HZ4：ODD（経路制限など）内を自動運転（停留所で再発車）する際、乗降客やその荷物や服等が自動開閉扉に挟まれたことを、センサ視界（FOV）の不足や認識処理の不良により、センサ認識系や遠隔監視者が認知できず（ハザード）、再発車して客が引きずられるような状態（危険事象）が生じる。

**例 5：（原理）マルチパスによる誤検知**

HZ5：ODD（経路制限など）内を自動運転する際、周辺構造物（道路インフラ、建物、路面など）で乱反射した計測用電磁波（ミリ波）をセンサ（ミリ波レーダ）が受信することで、実際には存在しない物体の誤検知が生じて（ハザード）、乗客の転倒や後続車の追突を招く不必要なブレーキ制動がなされる状態（危険事象）に至る。

### 5.4.4 リスクアセスメント

前述のシナリオごとに、曝露率 E、傷害度 S、制御可能性 C からリスクの大きさを評価する。リスクの大小から、対策実施の有無や優先度を決定する。機能安全国際規格 ISO 26262-3 の付属書 B に分類例が掲載されているので活用すると良い。表 3、4 を参照されたい。

### 5.4.5 安全目標

車両レベルのハザード分析とリスクアセスメントの結果を受けて、不合理なリスクと判断されるハザードに対して安全目標を設定する。

**例 1：（原理）計測用電磁波の伝搬減衰による不検知**

SG1：ODD（経路制限等）内を自動走行する際、周辺障害物（静止物・移動物）との衝突回避に必要な減速がなされない状態（危険事象）に至るものであり、自然環境の悪化（雨、雪、霧など）、障害物の低反射特性（黒色、ステルス形状など）、車両の整備不良（センサ汚れなど）などによって、センサ認識系が性能低下や性能限界に陥り、障害物などの不検知が生じること（ハザード）を防止する。

**例 2：（原理）対象物と背景のコントラスト不足や過度な特性乖離による不検知**

SG2：ODD（経路制限等）内を自動走行する際、周辺障害物（静止物・移動物）との衝

突回避に必要な減速がなされない状態（危険事象）に至るものであり、周辺障害物と背景のコントラスト不足（背景同色など）や、過度な特性乖離（朝日・西日など逆光など）などによって、センサ認識系が性能阻害や性能限界に陥り、障害物などの不検知が生じること（ハザード）を防止する。

**例 3：（原理）死角による不検知**

SG3：ODD（経路制限等）内を自動運転（非優先道を交差横断）する際、周辺障害物（非優先道の車両や歩行者など）との衝突回避に必要な減速が接近直前（死角解消）まで実施されない状態（危険事象）に至るものであり、周辺障害物を、交差点周辺建屋で生じる死角によって、センサ認識系が性能阻害や性能限界に陥り、障害物などの不検知が生じること（ハザード）を防止する。

**例 4：（原理）死角や認識処理不良による不検知**

SG4：ODD（経路制限など）内を自動走行（停留所で再発車）する際、再発車して客が引きずられるような状態（危険事象）に至るものであり、乗降客やその荷物や服等が自動開閉扉に挟まれたことを、センサ視界（FOV）の不足や認識処理の不良により、センサ認識系や遠隔監視者が認知できないこと（ハザード）を防止する。

**例 5：（原理）マルチパスによる誤検知**

SG5：ODD（経路制限等）内を自動走行する際、乗客の転倒や後続車の追突を招く不必要なブレーキ制動がなされる状態（危険事象）に至るものであり、周辺構造物（道路インフラ、建物、路面など）で乱反射した計測用電磁波（ミリ波）をセンサ（ミリ波レーダ）が受信することで、実際には存在しない物体の誤検知が生じること（ハザード）を防止する。

### 5.4.6　安全方策

前述の 5.4.2 節で示したように、性能限界に至る手前に適切な余裕度を持った ODD 境界線を設けて ODD 逸脱を検出する。検出時は、上限車速を下げたり、軌跡を対象物から遠ざけ迂回させて衝突回避の余裕度を増すなどの縮退運転で自動運転を継続、または、MRM を起動させて最小リスク状態（路肩停車など）へ移行して自動運転を停止する。

**異種センサ冗長構成の活用（例）**

- 例 1：（原理）計測用電磁波の伝搬減衰による不検知
- 例 2：（原理）対象物と背景のコントラスト不足や過度な特性乖離による不検知

原理（性能限界）が異なる異種センサを使った異種冗長構成で ODD 逸脱を検出する。たとえば、二種（カメラ／ LiDAR）のセンサや、三種（カメラ／ LiDAR ／ミリ波レーダ）のセンサなどを備えることが考えられる。耐自然環境性能は一般に、カメラ＜ LiDAR ＜ミリ波レーダである。同じ障害物に対する異種センサ認識系出力を比較してその差異により限界に至ったセンサ認識系を判定する。ただし、たとえば、天候の急変により、複数種のセンサが極めて短い時間差で性能限界へ至った場合に、各センサ認識出力に差異が生じず判定できないケースがあり得る。

また、性能限界に至った場合の走行戦略については、冗長構成に応じて検討する。たとえば、二種冗長構成であれば、一種が限界に至った段階で ODD 境界を逸脱したと判断して、MRM を起動させて最小リスク状態（路肩停車など）へ移行して自動運転を停止する。

三種冗長であれば、一種が限界に至った段階で先ず縮退運転へ移行する。さらに、二種が限界に至った段階で ODD 境界を逸脱したと判断して、MRM を起動させて最小リスク状態（路肩停車など）へ移行して自動運転を停止する。

ただし、動的運転タスク、つまり障害物への衝突回避や自己位置推定などに必要な認知エリアが、異種センサで重複してカバーされている事が前提である。異種センサで、異なる認知エリアを単に分担しているだけであれば、上述の異種冗長構成に該当しない。

**インフラ協調システムの活用（例）**

- 例 3：（原理）死角による不検知

ODD（経路制限等）内を自動運転（非優先道を交差横断）する際、周辺障害物（非優先道の車両や歩行者など）が交差点周辺建屋などで生じる死角によって車載センサでは検知できない場合がある。このように見通しが悪い交差点に接近する場合は、通常は、縮退運転（通常運転時よりも上限車速を下げたリスク回避モード）へ移行したり、自車が走行する道路が優先であっても交差点進入前で一時停止する必要がある。しかし、頻繁に車速を下げるとサービス性を損なうので、インフラ協調システム（死角情報支援システム）を活用する選択肢もある。見通しが悪い交差点に固定カメラなど設置して交差点に接近する他車両や歩行者などの交通情報を自動運転車へ事前に通信で送り、車載センサ認識系と併せ

て自動運転判断処理に利用する。サービス性とコスト（通信の信頼性確保に必要な対策費も含む）は背反するので選択には注意が必要である。

**遠隔監視支援システム・インフラ協調システムの活用（例）**

- 例 4：（原理）死角や認識処理不良による不検知

乗客の乗降確認をシステム／遠隔監視者／乗員の誰が行うにせよ、まずは乗降客モニタに死角を作らないことが必要である。車内側カメラだけでなく車外カメラ（乗降口上、停留所側などに設置）の映像を、システム／遠隔監視者／乗員などで共有して乗降客の異常を検知する。

AI を使ったシステム認識処理を行う場合は、深層学習など機械学習をベースにしたもの（ブラックボックス的で後検証不可、認識性能が一般に高い）とルールベースのもの（ホワイトボックス的で後検証可能、認識性能が一般に低い）があり、両者の組合せも可能である。いずれのアルゴリズムにせよ正解率 100% には至らない。

なお、車外カメラ（停留所側）は、図 28 の機能レベル基本アーキテクチャ例におけるインフラ協調システム（死角情報支援システム）の活用例に相当する。同種カメラでも別場所や別アングルのカメラを追加設置することで死角を減らすことは可能である。

**位置情報表示施設の活用（例）**

- 例 1：（原理）計測用電磁波の伝搬減衰による不検知

あらかじめ位置情報表示施設を既知の場所（危険事象を抽出した場所など）に設置して、センサ認識性能の ODD 逸脱を検出する。運行経路が既知な場合、特定の場所を走行または一時停止などした際に、どのような方位、距離に、どの様な信号強度でセンサ信号が反射して戻って来るかあらかじめわかる。したがって、何かしらの阻害要因により受信信号の強度が弱まっている場合、その信号強度の減衰程度からあらかじめ決めた ODD 境界を逸脱した否かを判定する。

**誤検知履歴と地図情報の活用（例）**

- 例 5：（原理）マルチパスによる誤検知

ODD で設定された運行経路において、障害物の誤検知が生じやすい場所の履歴情報を、運行経路設定機能（ナビ地図含）にあらかじめ記録しておく。運行経路を自動運転で走行中に、自己位置推定機能と運行経路設定機能（ナビ地図含む）の出力情報から、障害物の誤検知履歴がある地点に接近中と判断した場合は、あらかじめ早めに速度を下げて走行（縮退運転）したうえで、障害物の正しい認識結果が確定してから衝突回避行動（ブレーキ制御やハンドル制御など）を行う。つまり、誤検知による不必要な急制動や急操舵を回避する。

### 5.4.7　機能レベル検証

センサ認識系の基本性能仕様[*31]は、運行経路に沿ったシナリオをもとに危険事象に繋がるような破綻がないか検証が必要である。シナリオをコマ送りのように机上検証するのはかなり労力が必要であり、見落としも生じる可能性があるので、安全設計（車両レベル／抽象的レベル）のフェーズであっても、シミュレーションによって安全方策の有効性を確認することを推奨する。

ただし、このフェーズで行うシミュレーションモデルは、上記の基本性能を設定した比較的に簡易で演算負荷が低いセンサ認識系モデルでも対応可能である。センサ認識系の各種阻害要因（または阻害原理）に対する基本性能の阻害程度をあらかじめ収集準備しておき、簡易なセンサモデルに反映させて使い分けるとよい。実際のセンサ物理現象を再現するような詳細なセンサモデルは、阻害程度も予測可能なモデルであるが演算負荷が高い。したがって、詳細なセンサモデルを使う検証は、設計仕様がかなり固まった段階、たとえば開発プロセスの最終段階などでの利用を推奨する。

[*31] FOV（最大距離、最小距離、方位）、分解能、精度、認知レート、認知遅れ、属性認識率など。

## 5.5 本来安全 4：ミスユース等

ODD（経路限定など）内で自動運転旅客移動サービスを提供するレベル 4 自動運転システムにおいて、乗客、乗員、遠隔監視者、運行管理者などがミスユース[*32]を行っても、周辺車両の運転者、歩行者などが誤った振舞いを自動運転車に行っても、自動運転車が静止物や移動物などの周囲障害物と衝突する（人身事故を起こす）ことなく、安全に走行するための要件を明確にする。

### 5.5.1 必要理由

本ガイドブックではレベル 4 自動運転を対象としており自動運転旅客移動サービス車両の運転席に運転者はいない。しかし、自動運転車載システムのみならず、遠隔監視支援システムやインフラ協調システム（死角情報支援システム）など、自動運転に関わるシステム全体（図 28 の機能レベル基本アーキテクチャ参照）に対して何らかの関わりを有する人間（乗客、乗員、遠隔監視者、運行管理者など）のミスユースや、周辺車両の運転者、歩行者などの自動運転車への誤った振舞い[*33]により、周辺障害物との衝突などの不安全な状況に至る可能性がないか漏れなく洗い出し、不合理なリスクがある場合には、不合理なリスクがなくなるまで安全対策を施す必要がある。

なお、検討範囲を先入観で限定すべきではない点に注意されたい。システムの起動・停止や再発車における人間による操作、運行走行前後の点検や調整における人間による操作、乗客などの干渉行為（いたずらや悪意も含む）、また、周辺車の運転者や歩行者との意思疎通の不調（いたずらや悪意も含む）なども対象として検討すべきである。

SOTIF 規格 (ISO 21448) では、乱用（いたずら行為や悪意ある行為）はミスユースの対象外である。しかし、本ガイドブックでは、乱用もシステムと人間の相互関係に関わるものであり、ミスユースの検討過程において除外せず厚めに対処することを推奨する。

[*32] 誤操作：本人が意図しない操作、誤使用：開発者の意図に反した使用。
[*33] 故意による危険行動など。

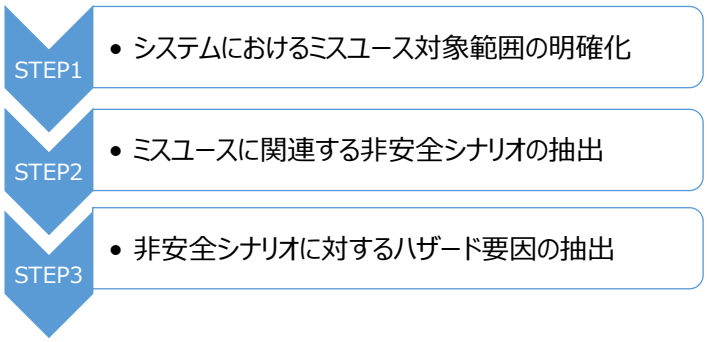



図 30　ミスユースハザード抽出までのプロセス（STAMP ／ STPA を活用）

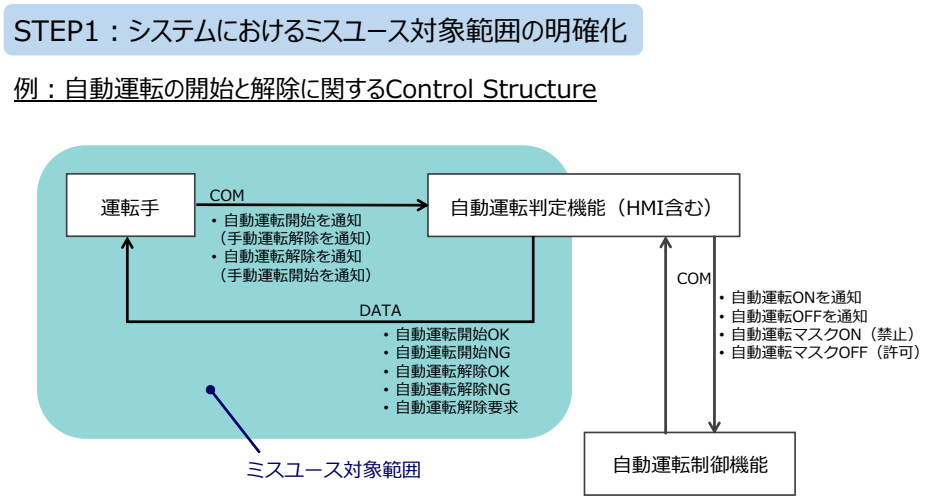



図 31　ミスユース対象範囲の明確化イメージ

### 5.5.2　考え方

4.3 節で設定した ODD、4.4 節で設定したシナリオ、5.1 節で定義した機能レベル基本アーキテクチャ（機能ブロック全体図）をもとに、自動運転車両の走行や運行に係るさまざまな人間と自動運転システムの相互関係を図示化して、人間が引き起こすミスユースに関するハザードを漏れなく抽出することがまず重要である。

STAMP ／ STPA を用いた事例を図 30 ～ 図 33 に示す。図 30 はハザード抽出までのプロセス、図 31 はミスユース対象範囲の明確化イメージ[*34]、図 32 はミスユースに関連

[*34] 前述の機能レベル基本アーキテクチャ例をもとに、ミスユースに関わる機能部分を選択して抽象化したも

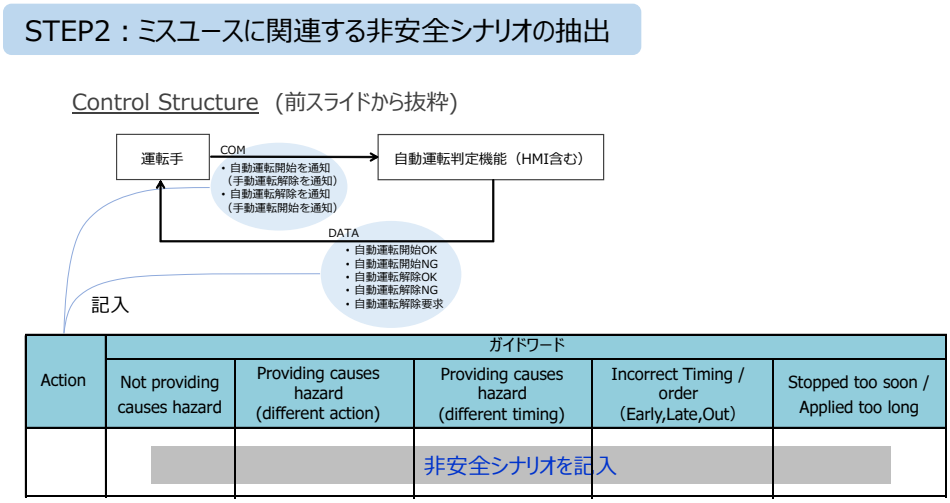



図 32　ミスユースに関連する非安全シナリオの抽出イメージ

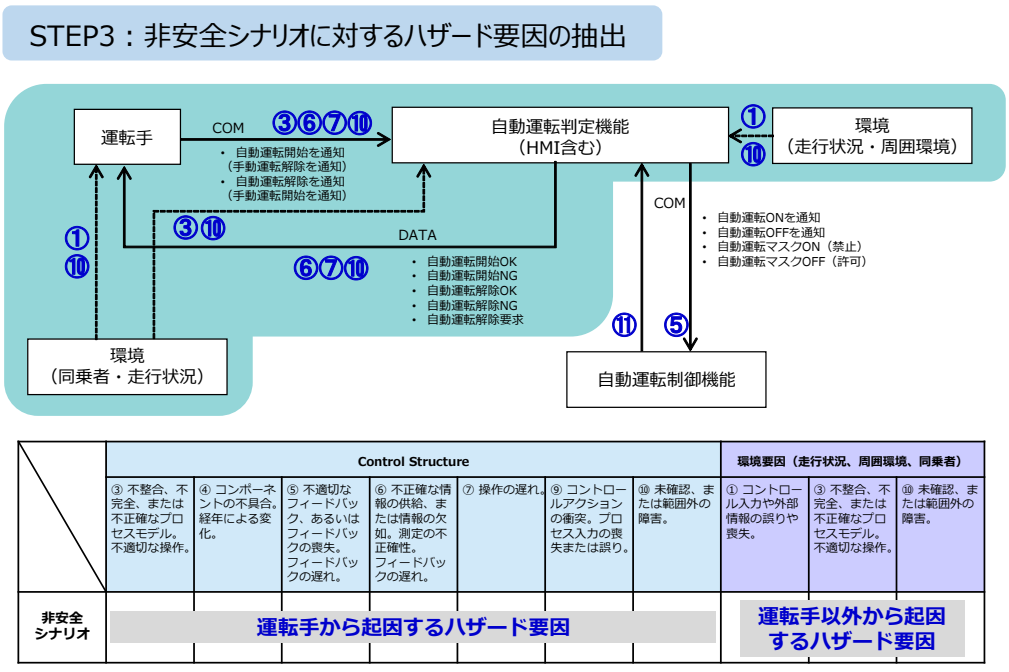



図 33　非安全シナリオに対するハザード要因の抽出イメージ

する非安全シナリオの抽出イメージ、図 33 は非安全シナリオに対するハザード要因の抽出イメージである。なお、図 30 ～ 図 33 は、経済産業省委託事業「平成 28 年度スマート

の。

モビリティシステム研究開発・実証事業：自動バレーパーキングの実証及び高度な自動運転システムの実現に必要な研究開発（安全設計）」から引用した。

### 5.5.3 ハザード分析

ODD、シナリオ、機能ブロック図をもとに、乗客、乗員、遠隔監視者、運行管理者、周辺車両の運転者、歩行者などの自動運転システムに対するミスユース（誤操作・誤使用）に関するハザードと危険事象を抽出する。

**例 1：誤操作**

HZ1：ODD（経路制限など）内で自動運転中（レベル 4）、遠隔監視者（遠隔運転可能な者）が意図せず間違って、または、乗客や乗員が意図や悪意の有無に関わらず、ハンドルやブレーキペダルなどに触れる。その結果、遠隔監視者や乗客や乗員の意図的なオーバーライドとシステムが誤判断して、操作入力を運転へ反映するとともに自動運転を解除するが、遠隔監視者や乗客や乗員は自動運転の解除に気づかず（ハザード）、静止物・移動物などの周辺障害物との衝突回避に必要な減速などがなされない状態（危険事象）に至る。

**例 2：誤使用**

HZ2：停留所で自動運転システムを起動する際、遠隔監視者（遠隔運転可能な者）や乗員が、自己位置推定機能[*35]の初期化手順を間違えたため自己位置推定誤差が極めて大きいまま自動運転を開始する（ハザード）。適切な自動操舵と加速で停留所から発車することができずにコースアウトして静止物・移動物などの周辺障害物と衝突する状態（危険事象）に至る。

**例 3：交通参加者の悪意**

HZ3：乗客が転倒しないように所定減速度以下で制動する制約がある自動運転旅客移動サービス車が、一般車や歩行者と混在する公道を走行する際、一般車が急な加減速やカットイン、横断歩行者が急な飛出しや U ターンなどで、自動運転車の性能を試すような悪意ある振舞いを行うこと（ハザード）で、静止物・移動物などの周辺障害物と衝突する状態

[*35] 自己位置推定機能の具現化には各種方法があるが、ここでは、加速度センサとジャイロを利用した慣性航法とマップマッチングを組み合わせたものを想定した。自動走行中は、積分的に溜まる誤差を定期的にマップマッチングでリセットする。自動運転システムを停止後、手動運転で車両移動して再度起動する場合には自己位置推定値のリセットが必要である。

（危険事象）に至る。

### 5.5.4　リスクアセスメント

前述の危険事象ごとに、曝露率 E、傷害度 S、制御可能性 C からリスクの大きさを評価する。リスクの大小から、対策実施の有無や優先度を決定する。国際機能安全規格 ISO 26262-3 の付属書 B に分類例が掲載されているので活用すると良い。表 3、4、5 を参照されたい。

### 5.5.5　安全目標

車両レベルのハザード分析とリスクアセスメントの結果を受けて、安全目標を設定する。

**例 1：誤操作**

SG1：ODD（経路制限等）内で自動運転中（レベル 4)、静止物・移動物などの周辺障害物との衝突回避に必要な減速などがなされない状態（危険事象）に至るものであり、遠隔監視者が意図せず間違って、または乗客が意図や悪意の有無に関わらず、ハンドルやブレーキペダルなどに触れた結果、遠隔監視者や乗客や乗員の意図的なオーバーライドとシステムは誤判断して、操作入力を運転へ反映するとともに自動運転を解除するが、遠隔監視者や乗客は自動運転の解除に気づかないこと（ハザード）を防止する。

**例 2：誤使用**

SG2：停留所で自動運転システムを起動する際、適切な自動操舵と加速で停留所から発車することができずにコースアウトして静止物・移動物などの周辺障害物と衝突する状態（危険事象）に至るものであり、遠隔監視者（遠隔運転可能な者）や乗員が、自己位置推定機能の初期化手順を間違えたため自己位置推定誤差が極めて大きいまま自動運転を開始してしまうことを（ハザード）を防止する。

**例 3：交通参加者の悪意**

SG3：自動運転旅客移動サービス車（乗客が転倒しないように所定減速度以下で制動する制約あり）が、一般車や歩行者と混在する公道を走行する際、静止物・移動物などの周辺障害物と衝突する状態（危険事象）に至るものであり、一般車が急な加減速やカットイン、横断歩行者が急な飛出しや U ターンなどで、自動運転車の性能を試すような悪意ある

振舞を行うこと（ハザード）を防止する。

### 5.5.6　安全方策

誤操作（本人が意図しない操作）に対しては、人間とシステムの間で正しく意思疎通ができるように、ヒューマン・マシン・インタフェース（HMI）を適切に設計する。つまり、システムから人間へのシステム状態表示機能の改善、人間からシステムへの入力操作機能の改善などを行う。

誤使用（開発者の意図に反した使用）に対しては、警告ラベル表示・教育マニュアルの改善などが必要である。

**例 1：誤操作**

自動運転システムは、運転者の認知・予測・判断・操作の全機能を代替えするものであり、ハンドル操作・アクセル操作・ブレーキ操作のいずれかに介入があった時点で自動運転は解除され手動運転へ戻る必要がある。介入意思を持たずに誤って、ハンドル・アクセル・ブレーキなどに触れた場合に、自動運転が誤って解除されないための方策としては、たとえば、ハンドル操作力・アクセル操作量・ブレーキ操作量が各々所定値を超えた場合に限定するなどの条件を付ける方策がある。また、自動運転が解除された場合に、音声や警告音などで注意喚起することも、解除されたことに気づかない危険な状態を回避する方策となる。

**【補足】**　オーバーライド（意図した運転介入と自動運転解除）のしやすさと間違った介入判定防止は一般的に背反の関係にある。航空機のオートパイロット装置においても同種の課題があり、製造メーカごとの設計ポリシーで対策方法は大きく異なることが有名である。旅客航空機の場合、機種ごとのライセンス取得がパイロットに義務化されている。

**例 2：誤使用**

自動運転システムを起動する際に必ず正しい手順で実施するように、起動操作を行う遠隔監視者や乗員に周知徹底する。具体的には、警告ラベル表示・教育マニュアルの改善などが必要である。また、ヒューマンエラーへの対策として、GNSS 情報も利用して、自己位置推定値が極めて大きな誤差を持っていないか（適切なリセット処理が定期的に実施さ

れているか）セルフチェック機能をシステムに加えることを推奨する。

**例 3：交通参加者の悪意**

自動運転旅客移動サービス事業が社会にもたらすメリット、安全性、特徴（自動運転車の特有の振舞いなど）を十分社会へ告知することで社会受容性を醸成する必要がある。また、自動運転車が自動走行する際に周辺車両の運転者や歩行者へ、自動運転中であることや運転意思表示（お先にどうぞ、など）を行うことである程度の効果が期待される。さらに、悪意ある者に対しては、自動運転車の周辺映像を常に撮影記録している旨を周辺に告知することも抑止力となる。

なお、保安基準において、一定の灯火を除き、自動車が右左折、進路の変更、加速、減速、停止その他の動作を行うとする旨を他の交通に対し指示することを目的としたものを備えてはならないこととなっているので、その旨を留意する必要がある。

### 5.5.7 機能レベル検証

ミスユース課題の検証にはドライビングシミュレータ（以下、DS という）の活用が有効である。評価プロセスで使用するような大掛かりな DS（車両挙動と体感 G のリアルな再現）ではなく、遠隔監視システムに近い規模のシミュレータでも有効である。ただし、操作系や表示系など HMI に関する部分は実際に想定する物に近いものを準備する必要がある。

図 34　ミスユース課題を検証するための簡易型ドライビングシミュレータ例（出典：経済産業省委託事業「平成 30 年度　高度な自動走行システムの社会実装に向けた研究開発・実証事業：自動バレーパーキングの実証及び高度な自動走行システムの実現に必要な研究開発（セーフティ）」）

## 5.6　機能安全

本節では、ODD 範囲内において、自動運転車両の電気／電子システムの機能失陥時に自動運転車両が道路インフラなどの周辺静止物と衝突することがなく、すなわち人身事故を発生させることなく安全に自動運転するために求められる要件を明確にする。

### 5.6.1　ハザード分析

ODD、シナリオ、機能ブロック図を元に、自動運転車両に搭載された電気／電子システムが周囲や環境から外乱がない状態での運用中に機能失陥を起こした場合のハザードおよび危険事象を抽出する。

**ハザード分析の進め方**

ここでのハザードとは、自動運転車両の基本制御（軌跡追従、車速制御）を行う電気／電子システムの機能失陥により引き起こされる、危害になり得る潜在的な原因を指す。操

舵失陥（曲がる）や制動失陥（止まる）、急加速（走る）などの、車両レベルの異常な振舞いとしてハザードを識別する。ハザードの分析には、FMEA や HAZOP 等の安全分析の手法を用いることができる。ハザード分析の際はインフラによる外部監視等の安全方策の有無についても考慮する。ハザード識別後は、ハザード発生時に危害となり得る状況を想定して危険事象を特定する。

**危険事象の例 (1)**

ODD 範囲内（既定経路の道路線形に応じた上限車速、最大乗員、通常時に想定する最低路面 $\mu$ など）を自動運転する際に、自動運転車両制御システムの操舵機能失陥により、既定の走行軌跡を逸脱し、結果として、白線、縁石、ガードレールなどを踏み越してコースアウトする。

**危険事象の例 (2)**

ODD 範囲内を自動運転する際に、自動運転車両制御システムの制動機能失陥により、既定の停車位置をオーバーランし、結果として交差点や横断歩道に進入する。

### 5.6.2 リスクアセスメント

前述の危険事象ごとに、たとえば上限車速を制限することで傷害度 S が低下する、および制御可能性 C が向上するなどの自動運転観点で、曝露率 E、傷害度 S、制御可能性 C からリスクの大きさを車両レベルのリスクアセスメントにより評価する。リスクの大小から、対策実施の可否や優先度を決定する。

**リスクアセスメントの進め方**

E、C、S は、ISO 26262-3 の付属書に記載される表の値などを参照して評価しても良い。ただし、C に関して従来は人間ドライバの制御可能性、すなわち危害を回避する可能性を評価しているが、レベル 4 以上ではシステムが運転に責任を持つため、C については議論中である。E に関しては交差点、歩行者の有無など ODD を考慮する。評価の際は、ハザード、状況、結果を含むシナリオを想定し、結果として事故に至る場合の傷害のレベルで S を見積もる。

**シナリオの例 (1)**

走行路を車両が定速で走行中 (E) に、操舵失陥が発生し車線を逸脱して (C)、路肩に衝

突し、乗員が傷害を負う (S)。

**シナリオの例 (2)**

走行路を車両が定速で走行中 (E) に、制動失陥が発生し停止線で停車できず (C)、バーゲートなど障害物に衝突し、乗員が傷害を負う (S)。

### 5.6.3 安全目標

ハザード分析およびリスクアセスメントの結果を受けて、機能失陥時のハザードへの対処を要求する安全目標 (Safety Goal) および安全目標達成時のシスムの状態を示す安全状態 (Safe State) を定義する。

**安全目標および安全状態の内容**

安全目標は、技術的な解決策ではなく機能レベルの最上位の要求として定義する。安全状態は、機能の停止、機能の縮退、機能の継続の三つが一般的だが、自動運転車両の場合は、システムの各要素を冗長化して機能を継続する、または MRM により減速して車両を停車するなどの状態が考えられる。

**安全目標および安全状態の例 (1)**

**安全目標：** 既定経路の道路線形に応じた上限車速、最大乗員、通常時に想定する最低路面 $\mu$ などの ODD 範囲内を自動運転する際に、自動運転車両制御システムの操舵失陥による車線逸脱を防止すること。

**安全状態：** 自動運転車両の操舵システム失陥によるハザードを回避する間、操舵機能を継続する。

**安全目標および安全状態の例 (2)**

**安全目標：** 既定経路の道路線形に応じた上限車速、最大乗員、通常時に想定する最低路面 $\mu$ などの ODD 範囲内を自動運転する際に、自動運転車両制御システムの制動失陥による障害物への衝突を防止すること。

**安全状態：** 自動運転車両の制動制御システムの失陥よるハザードを回避する間、制動機能を継続する。

### 5.6.4　安全方策

定義した安全目標および安全状態を達成するための安全方策を、危険事象の防止に求められる時間的な制約や、ただちに安全状態に移行できない場合の緊急時動作等を考慮して仕様化し、適用する。

**安全方策の例 (1)**

自動運転車両の操舵制御機能失陥時に車線を逸脱しないように、操舵制御機能を冗長化し、片方が故障しても、もう一方で操舵制御機能を継続するような安全設計を行う。

**安全方策の例 (2)**

自動運転車両の駆動制御機能失陥時に MRM を行い、緩減速した後に、安全な場所に停車するような設計を行う。

**安全方策の例 (3)**

遠隔監視システム等のインフラによる監視または強制停止等を適用する。あわせて、インフラ情報の確度等について当事者間でコミュニケーションをとり、安全方策の適切性を確認する。

### 5.6.5　機能レベル検証

適用した安全方策が車両レベルで有効に機能し安全目標を達成していることを、実車による再現可能なテスト、分析、長期試験等により評価する。

**機能レベル検証の進め方**

検証手法としては、実車両での再現可能なテスト、FTA や FMEA 等による分析、シミュレーション、長期テスト、実使用状況でのユースケースを考慮したパネルテスト、レビューなどが適用できる。最終的な評価は実際の走行環境で実車評価を行う必要がある。

**機能レベル検証の例 (1)**

「操舵失陥による車線逸脱を防止する」という安全目標に対して、車両テストで故障を発生させたときに、安全方策によって車線が逸脱しないことを確認する。

**機能レベル検証の例 (2)**

「制動失陥による障害物への衝突を防止する」という安全目標に対して、車両テストで前方に障害物を置いた条件で、車両テストで故障を発生させたときに、安全方策によって車両が障害物に衝突しないことを確認する。

**機能レベル検証の例 (3)**

故障率の目標値を設定し、部品レベルの分析により目標値の達成を確認する。

**機能レベル検証の例 (4)**

実使用条件下で、安全を考慮したうえで、複数台の試験車両を用いて行う長期のフリートテストにて最終確認を行う。

**機能レベル検証の例 (5)**

遠隔システムによる監視等の外部による安全方策を適用した場合には、想定したインフラシステムとの相互作用も含めて評価を行う。

# 6　自動運転車の安全性に関する要配慮事項 3：保安基準の遵守

国土交通省自動車局発行「自動運転車の安全技術ガイドライン」では、以下が規定されている。

(1) 自動運転に係る装置・機能のうち、道路運送車両の保安基準が定められているものについては、当該基準に適合するものであること
(2) (1) 以外の自動運転に係る装置・機能については、今後早期に国連規則が成立することが見込まれる装置・機能の要件や、関係する ISO 等の国際標準や業界標準に適合することを推奨する
(3) 自動運転に係る装置・機能以外の車両の構造・装置については、道路運送車両の保安基準の規定に適合するものであること

上記ガイドラインでは記述がないが、自動運転車は手動運転の一般車両と同様に、法令を遵守する必要がある。本章では法令の中で自動運転車に関連する項目への主な対応について記述する。

## 6.1　自動運転車の設計・評価において配慮すべき事項

自動運転に関連する法令のうち、道路交通法、道路運送車両法、道路法、旅客自動車運送事業運輸規則の 4 法令において、自動運転車の設計・評価時に配慮すべき事項が記載されている[*36]。

- 道路交通法（第四章の三 特定自動運行の許可等）[*37]

  レベル 4 に相当する、運転者がいない状態での自動運転である特定自動運行の許可制度が定められており、遵守する必要がある。[*38]

[*36] ただし、車両改造の内容次第では、上記 4 法令以外を確認する必要がある点に注意されたい。
[*37] https://www.npa.go.jp/bureau/traffic/selfdriving/L4-summary.pdf
[*38] https://elaws.e-gov.go.jp/document?lawid=335AC0000000105_20250426_504AC0000000032

- 道路運送車両法（保安基準第 48 条–自動運行装置）[*39]

  運転者に代わって「認知」・「予測」・「判断」・「操作」を行うレベル 3・4 の自動運転システムが、「自動運行装置」として保安基準の対象装置に追加されており、遵守する必要がある。

- 道路法（第 2 条 2-五 自動運行補助施設）

  交通事故防止を図るために必要な道路附属物として、自動運行補助施設が新たに位置づけられており、遵守する必要がある。

- 旅客自動車運送事業運輸規則[*40]

  自動車運送事業者等が自動運転車を用いて事業を行う場合に講ずるべき輸送の安全確保に関する措置が定められており、遵守する必要がある。

## 6.2 改正道路交通法

2022 年 4 月、道路交通法の一部を改正する法律が成立した。自動運転関係の規定については、2023 年 4 月から施行された。

## 6.3 最新動向資料

最新動向を知るための資料の一つとして、下記を参照されたい。

- 高速道路等における運行時に車両を車線内に保持する機能を有する自動運行装置に係る基準 (UN-R157)[*41]

[*39] https://www.mlit.go.jp/common/001346762.pdf
[*40] https://www.mlit.go.jp/jidosha/content/001603471.pdf
[*41] https://www.mlit.go.jp/common/001373650.pdf

# 7　自動運転車の安全性に関する要配慮事項 4：ヒューマン・マシン・インタフェース

本章ではヒューマン・マシン・インタフェース（以下、HMI という）について記述する。
国土交通省の「自動運転車の安全技術ガイドライン」では以下が規定されている。
レベル 4 の自動運転車は、次の機能を有する HMI を備える。

- 自動運転システムの作動状況を運転者（又は運行管理者）又は乗員が容易かつ確実に認知することができる機能[*42]
- 自動運転の継続が困難であるとシステムが判断し、車両を自動で停止させることをあらかじめ 運転者又は乗員（および運行管理センタにおいて遠隔監視される車両では運行管理者）に知らせることができる機能

なお、上記のガイドラインには記述されていないが、乗員や遠隔監視者による緊急停止（意図した運転介入と自動運転の解除）を正しくシステムが判断できる HMI を備える必要がある。

**参考文書**

- ISO/TC22 SC39/WG8 TR21959
- SIP-adus ヒューマンファクタ[*43]
- HMI の課題[*44]
- 周囲参加者への HMI[*45]

**乗務員対象の HMI の例**

乗務員（または遠隔監視を行う運転管理者）がハンドルやブレーキペダルなどに触れてしまい、意図せず自動運転モードが解除されてしまうことで危険事象に繋がる可能性があ

[*42] レベル 3 とレベル 4 の両方の自動運転モードを有する自動運転車については、運転者がレベル 3 の自動運転モードであるか、レベル 4 の自動運転モードであるかを区別して認知できること。
[*43] https://www.sip-adus.go.jp/file/its/evt_2019_its_forum13_06.pdf
[*44] https://home.jeita.or.jp/device/lirec/symposium/fpd/pdf/2018_1a.pdf
[*45] 同上

る。したがって、自動運転の作動中／非作動について、明確な表示やアナウンスが必要である。複数アクションによる緊急停止判定機能や自動運転開始判定機能を備えることも、意図しない緊急停止や自動運転開始を回避するための選択肢である。

**乗客対象の HMI の例**

乗客が着座した状態での走行が前提となる場合、乗客が着座する前に自動運転車両が停留所前を発進すること、または停留所前に停車完了する前に乗客が立ち上がることで、転倒して怪我するリスクがある。このリスクを回避するためには、自動運転車両制御モード状態の車内乗客に対する表示やアナウンスをわかりやすいものとする必要がある。

**車外の歩行者や周辺車両対象の HMI の例**

歩行者や周辺車両のドライバと自動運転車両のミスコミュニケーションに起因する、歩行者との譲り合い接触事故や、急制動による乗客の転倒などを回避するために、自動運転車両制御モード状態の車外への表示やアナウンスをわかりやすいものとする必要がある。

# 8　自動運転車の安全性に関する要配慮事項 5：データ記録装置の搭載

本章ではデータ記録装置の搭載について記述する。

事故発生後には、自動運転システムの作動状況ならびに運転者の状況を分析して、事故発生原因を特定できることが望ましい。そこで自動運転車は、システムの状態、異常・機能低下・失陥の発生などに関連する必要なデータを収集し、記録する機能を有する必要がある。国土交通省自動車局が「自動運転車の安全技術ガイドライン」を発行した 2018 年 9 月時点では、記録すべきデータについて今後検討されると記されており、データ記録装置という一般的な言葉が使われている。データ記録装置として求められる情報は今後変化すると考えられ、常に最新の要件や情報に対して自動運転システムの設計を行うことが必要であることを踏まえて以下に説明する。

2020 年 4 月の道路運送車両法の改正により、「自動運行装置」について定義されるとともに、保安基準において、自動運行装置に備える作動状態記録装置の技術基準が定義された。同時に、道路交通法の改正で「自動運行装置を使用した運転（いわゆるレベル 3 自動運転）」に関する規定が整備されるとともに、自動運行装置を備えている自動車を運転する場合には作動状態記録装置による記録等が義務付けられた。さらに、2023 年 4 月の道路交通法の改正で「特定自動運行（いわゆるレベル 4 自動運転）」の定義が追加された。これら自動運行装置に備える作動状態記録装置の技術基準[*46]を満足するよう設計しなければならない。

当該技術基準で定めている作動状況記録装置で記録すべき情報は以下の通りである。前述の通り本内容は今後変わる可能性があり、最新の技術基準で確認される必要がある。また、2020 年に発出されている「自動運行装置に備える作動状態記録装置に記録する情報について（依頼）」にも留意する必要がある。

- 自動運行装置の作動状況が別の状況に変化した時刻
- 自動運行装置による引継ぎ要求が発せられた時刻

[*46] 国土交通省 道路運送車両の保安基準 第 48 条 自動運行装置 別添 123 「作動状態記録装置の技術基準」 https://www.mlit.go.jp/common/001346769.pdf

- 自動運行装置がリスク最小化制御を開始した時刻
- 自動運行装置の作動中に運転者が、かじ取装置又は制動装置若しくは加速装置の操作装置への操作によりオーバーライドした時刻
- 運転者が対応可能でない状態となった時刻
- 自動運行装置が故障のおそれのある状態となった時刻

# 9　自動運転車の安全性に関する要配慮事項 6：サイバーセキュリティ

本章では自動運転車両が開発、製造、および、実際に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。国土交通省の「自動運転車の安全技術ガイドライン」では 4 章 (6) 項において以下のように要件を規定している。

> 『自動車製作者等又は自動運転車を用いた移動サービスのシステム提供者は、サイバーセキュリティに関する国連 (WP29) 等の最新の要件を踏まえ、自動運転車のハッキング対策等のサイバーセキュリティを考慮した車両の設計・開発を行うこと。』

この要件の具体例として、

1. 自動運転車の接続および通信の安全確保
2. 車外のネットワークから車内の制御系ネットワークが影響を受けないこと
3. システムの機能不全時のセーフモードを備えること
4. 不正操作を検知したときは、運転者に警告の上、車両を安全にコントロールすること

といったことが挙げられている。

また、12km/h 以下のラストマイル自動運転については、国土交通省が令和 2 年 7 月 17 日に公開した「ラストマイル自動運転車両システムのガイドライン」において、『サイバーセキュリティシステムについて代替の安全確保策が講じられることを前提に基準緩和認定制度の活用を可能とすること』とされている。

国際的には、WP29 において定められた基準である UN-R155 が、関連する標準である ISO/SAE 21434 とともに成立しており、国内では、UN-R155 に対応して「道路運送車両の保安基準」が改正され、第 17 条の 2（電気装置）第 3 項に「サイバーセキュリティを確保できるものとして、性能に関し告示で定める基準に適合するものでなければならない。」とされている。型式認定では、車両の技術的要件に加えて、開発段階から製造、

運用、廃棄に至るライフサイクルでのサイバーセキュリティに対応する体制、いわゆるCSMS (Cyber Security Management System) の構築も求められており、自動車メーカを中心としてその対応が進められ、セキュリティ対策を実装した自動車も出てきている。

一方で、ラストマイルの移動手段として用いられるモビリティは、オーナーカーや電動カートをベースに、遠隔操作や自動運転が可能となるように改造したものも多く、改造したものの場合のセキュリティをどう扱うか、自動運転システム開発者、自動車メーカ、車両・運行管理を行う事業者等の関係者における役割・責任分担を取り決めておくことが重要となる。通常のオーナーカーの場合における分散開発では、自動車メーカとサプライヤの間で依存関係を明確にするために、DIA（Development Interface Agreement：開発協働契約書）を取り交わすなどが行われているが、これと同等の契約を関係者間で取り交わすことも考えられる。

ラストマイルの自動運転の場合には、遠隔監視や遠隔操作を行うことがほとんどとなると考えられることから、通信機能の活用は必須ともいえる。インターネットとも繋がることになるため、通信機能の実装といった面からもサイバーセキュリティ対策を行うことが必要となるが、事業者によって車両・運行管理や遠隔監視・遠隔操作が行われることで、通常のオーナーカーにおける対応とは異なることが考えられる。

## 9.1 車両製作者・自動運転移動サービスのシステム提供者・車両使用者の役割

自動運転移動サービス向けの車両を製作する際には、自動車メーカがサービスシステムまで含めて提供する場合もあれば、自動運転システムの開発者が市販車を購入して改造する場合もある。自動車メーカがシステムまで提供する場合には、自動運転車両が型式認定を受けるケースも想定される。

一方、自動運転システムの開発者が改造する場合には、車両本体のセキュリティ対策そのものは自動車メーカから提供されるが、それをどう車両に反映するのか、それぞれの役割を明確にする必要がある。一般的には、自動運転システムとの整合性確認を行うことも考えると、自動車メーカから受け取ったセキュリティ対策も含め、自動運転システム開発者が製造後の運用段階におけるセキュリティ管理の主体となると考えられる。

また、運用段階において、新たな脆弱性が発見されたり、インシデントの発生などが起こ

り得るため、そうした情報の収集とセキュリティパッチの提供などの対応が求められる。自動車メーカの場合には、AUTO-ISAC (Automotive Information Sharing & Analysis Center) へ参加するなど、情報収集にも取り組んでいるが、自動運転システムの開発者の場合には、どのように情報収集を行うかも課題である。

車両使用者については、後述するソフトウェアアップデートの実施作業を行うことのほか、セキュリティ侵害が起きていないかといった日常的な点検を行うことが求められると考えられる。

## 9.2 開発・製造段階でのサイバーセキュリティの確保

「自動運転車の安全技術ガイドライン」の 4 章 (6) 項において、「ネットワークに接続したコネクテッドカーである自動運転車の安全確保の観点から、サイバー攻撃に対するセキュリティ対策を講じることが不可欠である。」とされているように、ラストマイル向けの車両においても、ネットワークに接続されることによるサイバーセキュリティのリスクを考慮することが必要である。

オーナーカー等を利用して自動運転移動サービス車両を開発する場合、ベースとなる市販車にセキュリティ対策が実装されていれば、改造に伴って新たに生じる攻撃対象領域 (Attack Surface) と脅威に対して、オーナーカーに実装されているセキュリティ対策に追加で必要となる対応を行うことが求められる。一般的には、改造に伴って変化する部分に対して、脅威分析を実施し、脅威を低減するためのセキュリティ対策を検討することが考えられる。

想定される脅威としては、たとえば、UN-R155 の Annex 5 には脆弱性と脅威に関する説明が記載されており、これらの情報は既知として対応することが求められるものと考えられる。

## 9.3 運用段階でのサイバーセキュリティの確保

サイバーセキュリティの一番難しい点は、開発した時点では問題がなくても、後になって、未知の脆弱性が見付かり、その脆弱性を悪用した攻撃が仕掛けられるといったことが起こりえるため、開発して終わりではないということである。

システムに脆弱性が見付かった場合や、サイバー攻撃によるインシデントが発生した場

合には、セキュリティパッチの提供やサイバー攻撃への対応や復旧などが必要となる。まずは、脆弱性やセキュリティインシデントの情報収集、情報管理を行う体制を構築することに加え、セキュリティパッチ等の対応は、該当部分を開発した企業等が対応することが望ましいため、こうしたサプライヤを含めたサプライチェーンのマネージメントも必要になる。

オーナーカー等を利用して自動運転移動サービス車両とした場合、ベースとなった車両に関する情報収集等は自動車メーカが行うことが想定されるが、改造した部分に関する脆弱性等の情報収集をどのように行うかを検討する必要がある。

# 10　自動運転車の安全性に関する要配慮事項 7：安全性評価

自動運転車両開発者または自動運転移動サービスのシステム提供者は、テストコースや実路での実車テストと仮想テストを適切に組み合わせて安全性評価を行う。

## 10.1　実車テスト

安全設計コンセプト検討における安全方策の立案では、不良や危険を検出する方式・閾値、ODD や運行条件が仮決めされる。実車テストではそれらが安全を確保できるかを評価する。もしも、確保されていないと評価された場合には、閾値を見直すが、場合によっては方式に遡っての見直しも考えられる。安全が確保されると判断されるまで、見直しを繰り返す。

**例 1：自己位置の誤推定**

急な曲線路を通過中に自己位置の誤推定が発生した場合、最悪の状況では自動運転車両のコース逸脱距離が大きくなることが考えられる。この逸脱距離が許容値以下であることを実車テストで確認する。たとえば、テストコースに急な曲線路を再現して自動運転車両を走行させ、動作不良を疑似的に発生させる。自動運転車両が停止した地点でコースからの逸脱距離を計測する。許容値以下とならない場合には、自己位置の誤推定を判断する方式・閾値の見直しを行う。逸脱距離は運行速度や停止までの減速度にも影響されるので、これらも見直すことが考えられる。ただし、減速度の設定は乗客・乗員の転倒や怪我が無いことを条件にあらかじめ設定する。

上述の許容値がどのような観点から決定されるすべきかは今後の議論の対象となり得る。

**例 2：路上の小物体の乗り越し**

テストコースに小物体を設置し、自動運転車両がそれを乗り越す実験を行う。発生する上下加速度や前後加速度と通過速度の関係を調査する。乗客の転倒や怪我が起きないために推奨される上下加速度や前後加速度の知見が利用できる場合には、その知見と実験結果に基づいて運行速度を決定する。

## 10.2　仮想テスト

最悪の状況が特定できない、すなわち、想定すべき状況が多数考えられる場合は、仮想テストを用いて評価を行うことも考えられる。また、実車でテストするのが困難あるいは危険なケースのテストも可能である。

**例：自動運転の経路の近くを移動する歩行者**

シミュレータ上に以下の判断や動作を行う自動運転車両を再現する。

衝突リスク予測が衝突リスクが高いと判断した直後に、目標車速計画によって運行速度を低下させる。歩行者が転倒したことを検出次第、緊急対応判断は軌跡追従や車速制御を介して自動運転を停止させる。図 28 に示した機能ブロック図を参照されたい。経路に進入する歩行者や自動運転車両の軌跡の経路や車速の候補を、実際の運用で想定されるすべての事例を網羅するように準備する。

上述の候補から一つを選び、歩行者が走行コースに進入して自動運転車両が自動運転を停止するシナリオをシミュレータ上に再現する。このシミュレーションで、衝突リスク予測が「衝突リスクが高い」と判断した直後に目標車速計画が運行速度を低下させること、および、歩行者が転倒したことを検出してただちに緊急対応判断が軌跡追従や車速制御を介して自動運転を停止させることを確認する。この確認を軌跡の候補すべてに対して実行する。

このように、想定する事例が多数考えられる場合でも、シミュレーションを用いて安全性の評価を行うことができる。この場合、シミュレーションが実車の振舞いを高精度に再現する必要がある。シミュレーション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の有効性を確認しておくことも必要である。

## 10.3　実環境試験の事例

自動運転車両に関する評価事例としては、たとえば以下のような試験を行うことなどが考えられる。

(1) 目的

カメラシステムの認識性能が目標に達しているかを確認する。

(2) 評価概要

実機カメラの画像から対象物の認識率を算出し、標準環境時の認識性能と外乱時の認識性能を比較し、外乱が与える影響を評価する。

- 認識性能の評価指標

  認識率は、評価対象フレーム数に対する認識対象物の認識成功フレーム数の割合とし、評価シーンごとに算出する。認識の成否判定は、評価画像の正解値とカメラシステムが出力する結果との比較を行い、それらの一致率によって成否を判定する。

- 外乱
  - 照度：対象物周辺の照度
  - 降雨：対象物周辺の雨量

(3) テスト環境

照度条件および降雨条件を設定可能で評価対象物を設置できる施設を使用し、以下の環境を再現する。

- 照度：施設照明全灯 (1600lx) から消灯 (0lx) までの 5 段階とする。
- 降雨：施設における雨量設定として 30/50/80 mm/h の 3 段階の雨量レベルを施設内全域において降雨させる。

(4) 結果例

- 照度

  照度が低下するほど認識性能が低下した。

- 降雨

  降雨によりレンズに水滴が付着すると認識性能が低下した。

(5) 対策案

- 目標認識率以下の照度条件は ODD 外に設定する。
- 目標認識率以下になると想定される降雨条件は ODD 外に設定する。また、降雨による水滴付着の影響を低減するために、1) 車室内にカメラを設置し、ワイパによる視界遮断時はソフトにより認識フレームから除外する、2) レンズの撥水処理と空気吹付による水滴除去を実施する。
- 認識性能低下条件での学習を追加する。

# 11　自動運転車の安全性に関する要配慮事項 8：使用過程の安全確保

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。国土交通省の「自動運転車の安全技術ガイドライン」では 4 章 (9) 項において以下を規定している。

(1) 自動運転車に搭載されるソフトウェア等について、使用過程においてサイバーセキュリティを確保するために必要なアップデート等に係る措置を講じること。（ソフトウェアアップデート機能の実装）
(2) サイバーセキュリティを確保するために必要となるソフトウェアのアップデート等の必要な措置に係る作業を実施すること。（使用中の車のサイバーセキュリティを確保するために必要なソフトウェアアップデートの実施）

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う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、乗員の安全を確保するために不可欠である。また同ガイドラインは 4 章 (3) 項において「自動運転車は、既に定められた自動運転に係る道路運送車両の保安基準を満たすこと」と規定している。サイバーセキュリティ／ソフトウェアアップデートは道路運送車両法の保安基準第 17 条の 2 第 3 項、第 4 項に該当規則があり、また車両法第 99 条の 3 の特定改造許可制度にも該当する場合がある。法規適合への対応の参考となる ISO 標準として ISO/SAE 21434、ISO 24089 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。

## 11.1 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、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[*47]という）は、現在オーナーカーを中心に採用が進んでいる機能である。したがって、サービス事業者による日常の車両メンテナンスで更新作業対応が可能な場合が多いと思われるので、自動運転移動サービスに用いられることが想定される車両においては、OTA の採用はまだ先になることが想定される。そのため、サービス事業者および／あるいは車両の使用者が OTA を用いてソフトウェアアップデートを行いたい場合には、車載機と通信インフラ双方の開発と実装が必要となる。また、これら機能の実装とともに、ソフトウェアアップデート実施の際の確実性およ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。

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

レベル 4 自動運転移動サービス車両では、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必要なソフトウェアアップデートを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 9 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。

(1) 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。たとえば、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

[*47] Over The Air の略。

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使用者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、一般の使用者を想定した情報提供も必要となる。

(2) 上記のソフトウェアアップデートの実施に当たり、前述の通り自動車メーカ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が、使用者はその指示にしたが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、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、11.1 節に示したような管理体制の構築も必要である。

# 12　自動運転車の安全性に関する要配慮事項 9：自動運転車の使用者への情報提供

国土交通省から発行されている「自動運転車両の安全技術ガイドライン」では、自動運転車が安全を確保するための「(10) 自動運転車の使用者への情報提供」として、「自動車製作者等（ディーラーを含む）又は自動運転車を用いた移動サービスのシステム提供者は、自動運転車の使用者に対し、平易な資料等を用いて次の点を周知し、使用者が理解することができる措置を講じること」に関する具体的な要件を示している。

したがって、自動車製作者など（ディーラーを含む）または自動運転車を用いた移動サービスのシステム提供者は、国土交通省の安全技術ガイドラインが示す要件を満たすことを含めて、自動運転レベル 4 に関して今後も整備が進む道路運送車両法などの関連法規を遵守することが必要となる。

また、自動運転移動サービスの社会実装と普及を進めるうえで、必要な安全性を確実かつ効率良く確保するためには、上記のとおり使用者への情報提供とあわせて、社会受容性の確立に向けた情報発信や新たにサービス導入を検討する団体や企業などへの情報発信が有効であり、積極的に取り組むことが望ましい。

## 12.1　利用者や地域住民、社会に向けた情報提供の必要性

自動運転移動サービスの社会実装においては、サービス性・採算性・安全性などのバランスを取ることが必要で、利用者や地域住民、行政機関などの理解や協力を得て社会受容性を確立することが重要課題となる。

自動運転システムは、計画した動作を確実に繰り返すことでは優れている。他方、自動運転移動サービスで当面実用化可能な自動運転技術は限定的であり、ヒューマンドライバが五感や経験などを踏まえて行うような高度な危険予測は容易ではない。必要な安全性を確保することは大前提となるが、たとえば法令違反状態にある交通参加者に対して、自動運転システムの機能だけでさまざまな危険を回避しようとすれば、徐行や一旦停止などの機会が増加しサービス性の低下が懸念される。また、ガードレールなどのコスト負担は事業採算性に影響する。したがって、自動運転システムの弱点を補う方策を検討するにあた

り、乗客や周辺交通参加者、関係する行政機関などの理解や協力を得るために、必要な情報を発信することが重要な課題となる。

**必要と思われる情報の事例**

1. 移動サービス社会実装プロジェクトの概要に関する情報

   プロジェクトの背景・目的 (why)、事業主体や開発体制 (who)、場所 (where)、移動サービス提供時期や開発日程 (when)、主要課題と解決方策 (how) など。実証実験や試乗会、説明会などに関する情報。

2. 自動運転システムの全体像に関する情報

   自動運転移動サービスに係るシステム全体概要、遠隔監視システム、運行管理体制、インフラやインフラ協調システムなど走行環境やルール整備の考え方や方策の全体概要など。

3. 自動走行車両に関する詳細情報

   車種（バス、乗用車、カートなど)、外観・内観、車両製造者、自動走行システム開発者、障害物検知システムの概要（センサ構成、主要な障害物の検出機能(距離や方位、精度など)、ODD、運用速度など。

4. サービス内容に関する情報

   サービス提供者、運行事業者、運行形態、サービス提供区間、路線図、運行ダイヤ、利用料金、料金収受方法、車内乗客安全に係る注意事項など。

5. 安全性に関連する情報提供

   走行実績、事故歴、セーフティドライバや乗務員の有無と役割、遠隔監視者の有無と役割、主な危険なシーンにおける自動走行車両の振舞い、サイバーセキュリティ対策、自動運行記録装置など。

6. その他

   問合せ先、開発者側からの情報、利用者や試乗体験者からの意見など

## 12.2 自動運転移動サービス導入検討中の事業者／地方自治体などに向けた情報発信

自動運転移動サービスの導入をこれから検討しようとする自治体や団体・企業などに対しては、必要な安全性を確保するための取組みが確実かつ効率良く実施されるように、自動運転移動サービス導入までのプロセスや検討内容、事業モデル、導入メリットなどの項目について情報提供する必要がある。以下に、有用と考えられる項目を示す。

**有用と思われる情報の事例**

1. 事業導入の背景、狙い、課題など
2. 事業モデル

   サービス提供者、サービス内容、提供価値、想定利用者、主な費用や収入など。
3. 導入までのプロセスなど

   導入関係者（地方自治体・運用事業者・自動運転車両開発者など）が取り組んだ導入プロセス、実証実験や実用化などに係る許認可当局からの指導内容や対応など。

# 13　無人自動運転移動サービスに用いられる車両の安全性（追加事項）

本章では、レベル 4 の無人自動運転移動サービスに用いられる車両の安全性向上や、そこで用いられる自動運転車の安全性に関わるリモートサービスについて、背景、考え方、設計上の配慮事項、および安全方策の例について記す。

## 13.1　背景

レベル 4 の無人自動運転移動サービスの場合、人間のドライバが車内にいる場合と同等の安全性を確保するため、自動運転車内または遠隔監視を行う場所に特定自動運行主任者を配置することが必要である。

## 13.2　自動運転車の安全技術ガイドライン（国土交通省自動車局）

レベル 4 の無人自動運転移動サービスに用いられる自動運転車に関しては、「自動運転車の安全技術ガイドライン（平成 30 年 9 月、国土交通省自動車局）」記載の「4 章．自動運転車の安全性に関する要件（7）無人自動運転移動サービスに用いられる車両の安全性（追加要件）」を参考に、取組みを進めることが望ましい。

つぎに、「自動運転車の安全技術ガイドライン（平成 30 年 9 月、国土交通省自動車局）」に記載された配慮事項を以下に引用する。

(1) 設定された ODD の範囲外となった場合や自動運転車に障害が発生した場合等、自動運転の継続が困難であるとシステムが判断した場合において、路肩等の安全な場所に車両を自動で移動し停止させる MRM を設定すること（移動サービスにあっては、乗客が安全に外部へ降車できる必要があることから、路肩等の安全な場所に車両を自動で移動し停止させる MRM を備えることを要件とした。）。
(2) 運行管理センタから車室内の状況が監視できるカメラ、音声通信設備を設置すること。
(3) 車室内の乗員が容易に押せる位置に非常停止ボタンを設置すること。

(4) 非常停止時（MRM 作動や事故による停止を含む。以下同じ。）に、運行管理センタに自動通報する機能を有すること。

(5) 非常停止時における運行管理センタとの連絡状況等、非常時の対応状況についてHMI により乗員にわかりやすく伝える機能を有すること。

## 13.3 ODD 外通過

無人自動運転移動サービス（レベル 4）に用いられる自動運転車に関しては、ODD の外を通過しなければいけない場合、自動運転システムが機能しないことを考慮した遠隔監視・支援を運行管理センタで実施することが必要である。

遠隔監視・支援においては、「遠隔型自動運転システムを搭載した自動車の基準緩和認定制度[*48] （平成 30 年 3 月、国土交通省自動車局）」の別紙 2「2. 代替の安全確保措置」を考慮する必要がある。

## 13.4 遠隔監視・支援

### 13.4.1 遠隔監視

遠隔監視とは、遠隔側にいる人間による遠隔監視システムの通信状態と、通信を介した自動運転車の運転環境、車両運転状態、自動運転システム状態、乗客および貨物状態の監視のことを示す。遠隔監視の目的は、遠隔側にいる人間による当該自動運転車の状態や周辺環境の把握である。

**遠隔監視に関する安全方策の例 (1)**

監視項目は、遠隔監視を行うために遠隔側の人員構成に合わせた必要最小限のものを選定すべきである。監視項目が多すぎると遠隔監視を行う側の負荷が増え安全性が損なわれる恐れがある。

**遠隔監視に関する安全方策の例 (2)**

監視項目は、通常時の監視項目と危険事象発生時の監視項目の表示を分けて示すべきである。後者はより目立つ位置に表示させ、監視者がすぐに気づくよう音や音声による通知

[*48] https://www.mlit.go.jp/report/press/jidosha07_hh_000271.html

も利用するのが望ましい。

### 13.4.2 遠隔支援

遠隔支援とは、自動運転システムが対処できない状況に遭遇した場合に、運用の継続を容易にするために、遠隔側にいる人間によって運転操作に該当しない範囲で自動運転システムへの入力情報やインストラクション（指示）を提供することである。

**遠隔支援の例**

レベル 4 の自動運転システムが対処できない状況に遭遇した場合に、遠隔側より通信を介して遠隔側にいる人間が自動運転車に情報を提供したり、指示を行って安全な運行を継続する。

**遠隔支援に関する安全方策の例**

情報提供や指示の遅延は、対象とする事象に対処するために、余裕のある時間内に収める必要がある。

## 13.5 旅客自動車運送事業運輸規則

特定自動運行保安員が特定自動運行事業用自動車に乗務しない場合においては、次に掲げる措置を講じる必要がある。

- 営業所その他の適切な業務場所に特定自動運行保安員を配置し、当該特定自動運行保安員に遠隔監視装置等を用いて遠隔から運行の安全の確保に関する業務を行わせること。
- 緊急を要する場合において旅客が特定自動運行保安員に連絡することができる装置及び特定自動運行事業用自動車を停止させることができる装置を当該特定自動運行事業用自動車に備えること。

詳細については、令和 5 年 3 月 31 日に公布した改正「旅客自動車運送事業運輸規則」[*49]を参照されたい。

[*49] https://www.mlit.go.jp/jidosha/content/001603471.pdf

## 13.6　自動運転の公道実証実験に係る道路使用許可基準

警察庁では、遠隔型自動運転システムおよび特別装置自動車の公道実証実験について、「自動運転の公道実証実験に係る道路使用許可基準（令和５年４月）」を公表し、許可に係る審査の基準や指導事項などを示している。

# 14　車内乗客安全に関する要配慮事項

本章では、レベル 4 自動運転移動サービスの実現に向け、車内無人を想定した場合において、車内乗客安全の要配慮事項について説明する。なお、すでに第 3 章において、大方の考え方や付随して立ち上がっている車内乗客安全 WG について記述をしているため、本章は重複する箇所があることに留意いただきたい。令和 4 年度の車内乗客安全 WG での議論の結果を用いて本章は作成されている。

## 14.1　車内乗客安全における考え方

3.2 節で述べたように、車内乗客安全については非常に重要であるという認識がある一方で、令和 4 年の日本においてレベル 4 無人自動運転移動サービスは存在しない。今後は、レベル 4 の自動運転が広く認められていく過程とその結果も参考にしつつ、かつ、自動運転レベル 4 先進モビリティサービス研究開発・社会実装プロジェクトの進捗に応じて、本ガイドブックにおいても適宜必要なアップデートを今後行いつつ、考え方を整理していく予定である。

令和 4 年度においては、まずは、車内乗客安全において車内乗客の安全を確保するために必要な観点や要素が、包括的かつ漏れなく網羅されるように、通常走行時／通常走行時以外の乗務員のタスクの流れの整理から始めた。そのため、現時点の本ガイドブックにおいても車内乗客安全に向けて考慮すべきタスクの議論に留める。

なお、3.2 節で述べたように、最終的には事業者の責任や判断を持ってシステムが構築されるので、本章はあくまでもその選択や開発の参考となるものである。

## 14.2　車内乗客安全の前提

### 14.2.1　本検討の前提条件

受容性や技術の熟成等の理由により、各社の方針において現状では車内無人を想定しない場合もある。しかし、本項では、将来を見据えて車内無人化を可能とするために必要な事項を整理共有する。ただし、ガイドブックという性質上、協調領域における議論のみを記載する。

本ガイドブックにおける車内乗客安全の想定条件は、車内の安全・サービスの項目が多岐に渡るうえで、最も難易度の高い条件として、対象車両はロボットタクシー等のいわゆるロボタクではなくバスとする。さらに、車内の条件としては着座だけでなく立ち乗りまでを想定し、走行ルートは固定ルートとする。サービスについては一旦議論対象外としており、運賃収受や運賃収受に関連するタスク等は含まれていない。一方、今後の議論や流れによっては、サービスの一部を車内乗客安全 WG の議題に含める可能性があり、その場合は本節の条件を変更する。

### 14.2.2　運行環境イメージ

車内乗客安全において考慮すべき想定される運行環境のイメージを図 35 に記す。運行環境は、車両環境と道路環境に分別されると考えられる。走行する場面場所によって道路環境は大きく変化し、運行経路においてこれらは一様ではなく、さまざまなパターンとその組合せがあるため多岐にわたる。さらに、車両環境は、図左下に示すように運行中に変わらない車両・車内環境と、図右下に示すように運行中に変化する車両・車内環境の 2 種


図 35　運行環境イメージ

類に分別される。これらは、車内安全を考えるうえで十分に考慮しなければならない要因となる。

## 14.3　車内乗客安全を実現するために考えられるタスク（通常時）

第 3 章で述べた通り、車内乗客安全 WG において、交通事業者の委員の協力を得て乗務員タスクを列挙した。乗務員タスクは、通常時、通常時以外、さまざまな乗客対応に分けてタスクの整理を行った。なお、乗務員タスクにおいては、「バス停でバスが停車している」時点から「次のバス停で停車する」時点までを一連の動作として定義する。

### 14.3.1　通常走行における乗務員タスクの流れ

基本的にトラブル対応がない場合に、乗務員が確実に行うタスクについて列挙する。具体的なタスクを図 36 に示す。本タスクは、通常時のタスクとして列挙しており、乗務員が常時行っているタスクと考える[*50]。通常時のタスクとして、乗降時、車内の乗客へのサービス、発車時、走行時、停車時、定常走行時、乗降確認、常時に分けてタスクを洗い出した。下記に場面ごとの詳細タスクを記す。

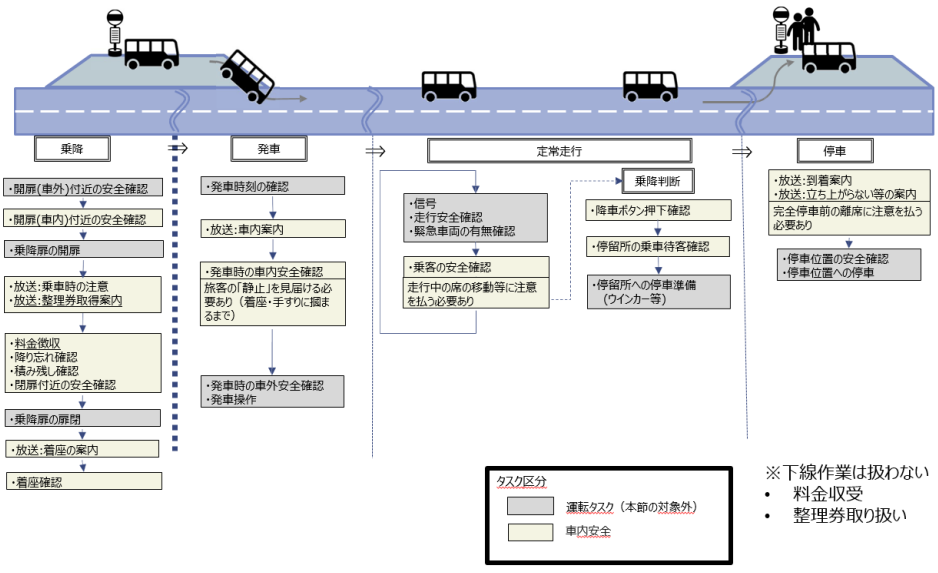



図 36　通常走行時における乗務員タスクの流れ

[*50] ただし、乗客が存在する場合を想定する。

- 乗降時
  - 開扉（車内）付近の安全確認
- 車内の乗客へのサービス
  - 放送：乗車時の注意
  - （放送：整理券取得案内）（サービスタスクとして議論の対象外とした）
  - （料金徴収）（サービスタスクとして議論の対象外とした）
  - 降り忘れ確認
  - 積み残し確認
  - 閉扉付近の安全確認
  - 放送：着座の案内
  - 着座確認
- 走行時
  - 車内安全確認

    走行中の席の移動などに注意を払う必要あり
- 発車時
  - 放送：出発の案内
  - 車内安全確認

    旅客の静止を見届ける必要あり（着座・手すりに摑まるまで）
- 停車時
  - 放送：到着案内
  - 放送：立ち上がらないなどの案内

    完全停車前の離席に注意を払う必要あり
- 定常走行時
  - 乗客の安全確認（異常時、緊急時以外）
- 乗降確認
  - 降車ボタン押下確認
  - 停留所の乗車待客確認
- 常時
  - さまざまな乗客対応

なお、運転タスクとサービスに関するタスクは今回の対象としては除外する。

### 14.3.2　さまざまな乗客への対応

14.2.2 節で説明したように車両の中の環境は常に大きく変化する。とくに、レベル 4 自動運転移動サービスにおいては、さまざまな乗客を安全に目的地まで運ぶことが最重要となる。乗客は、場所や環境によって、割合は異なるもののさまざまな場合が想定される。そのため、あらゆる乗客の利用を想定した対応を考えておく必要がある。下記にさまざまな乗客への対応方法について記述する。まず、障碍を持たれている方への対応としては、交通事業者への現状の対応方法についてヒアリングを行うとともに、WEB 等で公開されている対応についての調査を行った。

現状の乗務員は、身体障碍者、知的障碍者、精神障碍者、発達障碍者、車いす利用者への対応について、介助者がいる場合においては、基本的に介助者に依頼することが多い。一方、介助者がいない場合は、乗務員が個別対応を行っている。また、事前連絡があり、一人の乗務員での対応が困難であると判断した場合には、増員による対応も行っているのが現状である。レベル 4 自動運転移動サービスの普及等についての社会的な認知が十分に進んでいないことから、令和 4 年度の車内乗客 WG においては、想定される対応例や個別の具体的な対応方法についての議論は行わなかったが、今後も継続的な議論が必要であると考えられる。

また、障碍者ではなくても、ベビーカーを利用している乗客や、大きな荷物（特に転がる可能性のあるキャスターバッグ）、高齢者用の補助器具、杖や松葉杖などを利用している乗客もいることを踏まえて、とくにカーブや発進・停止時に、乗務員は乗客の安全確認を行っている。

### 14.3.3　運行前後の乗務員タスク（参考情報）

第 3 章で紹介した車内乗客安全 WG において、自動運転サービスを考えるうえでは乗務員の仕事について（とくに運行の前後も含めて）網羅的に考える必要があるという意見が出ている[*51]。そこで本節では、運行前後の乗務員タスクを整理する。公開されている情報を参考にしながら、交通事業者へのヒアリングも交えて作成した図を図 37 に示す。

[*51] ただし、令和 4 年度段階では深い議論が十分には進んでいない。

図の中央が運行におけるタスクになっており、詳細は図 36 を参照されたい。運行の前提として、運行準備のための運行管理タスクが存在する。運行前には、運行準備、始業点呼、出庫準備、回送タスクが存在し、それぞれの項目において行うべき詳細タスクが存在する。また、運行後においては、終点到着、回送時のタスクが存在し、その後再度運行に戻る場合と運行終了に分けられ、運行終了の場合は、帰庫に関するタスクとして、到着点呼、終業点検、終業点呼のタスクがある。下記にそれぞれの詳細タスクを記す。

- 事前準備
  - 運行管理
    - 車両の交番（作業）表の作成（ダイヤ改正に伴い年数回程度）
    - 点呼簿の作成、車両の交番（作業）表への割当
- 運行前
  - 運行準備

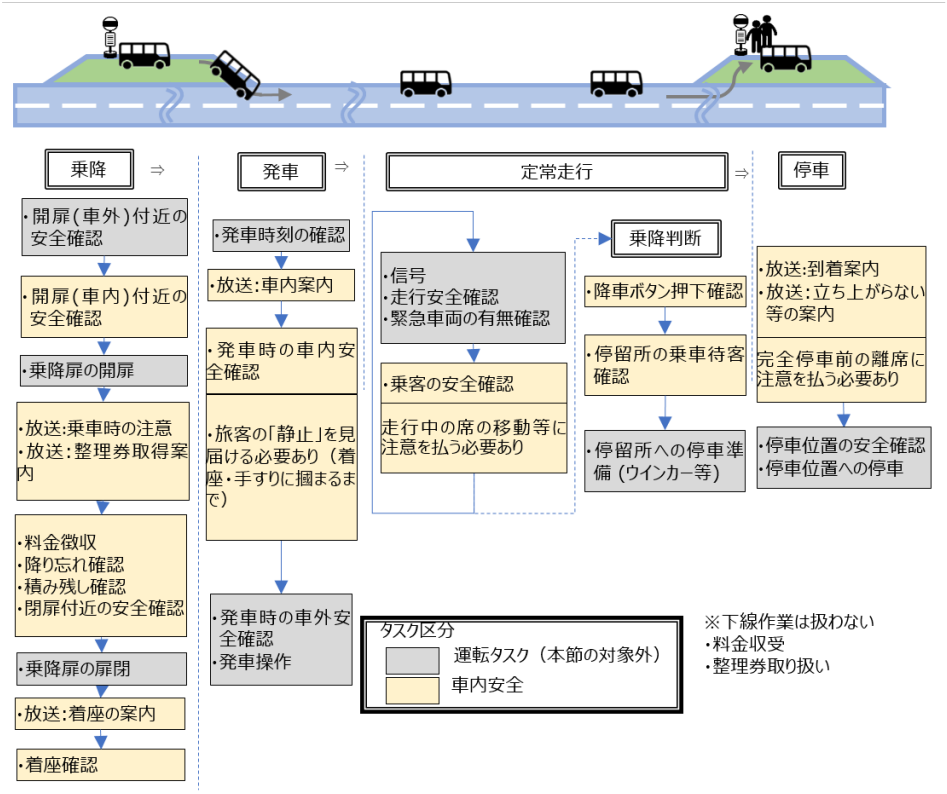



図 37　運行前後のタスク

        - 運転車両の割り当て確認
        - 点呼準備（アルコール、体温測定、免許証確認）
        - 車両点検（タイヤ、ワンマン機器、エンジンルーム）
        - 運賃箱のセッティング
        - 点検記録の作成
    - 始業点呼
        - 対面点呼（運行管理者 $\Leftrightarrow$ 乗務員）
    - 出庫準備
        - デジタコ・ドラレコの設定（立ち上げ）
        - 系統番号の一括設定＝交番番号の設定
        - 方向幕の行先表示の確認
    - 始発停留所への移動
        - 営業所から待機場までの車両移動（手動運転）
        - 系統設定および確認（行先表示、車内放送、運賃表示、出発時間）
        - 車両の乗り場への移動（回送）
- 運行後（回送）
    - 終点到着
        - 車内降ろし忘れの確認
    - 回送
        - 回送時間の確認（運行指示書の確認）
        - バス停 $\rightarrow$ 車庫までの回送移動（輪止め）
        - 車内の忘れ物確認
        - 車内の簡易清掃（アルコール拭き取りなど）
- 帰庫
    - 到着点呼
        - 帰庫を報告
    - 終業点検
        - 燃料補給（電気自動車であれば充電）
        - 保管場所へ車両移動（輪止め）
        - デジタコ・ドラレコの設定（終了操作）

    - 車内点検（遺失物・異常部位の点検）
    - 車内清掃・車両洗浄
  - 終業点呼
    - 売上を精算し、「乗務記録簿」を記入
    - アルコール・体調確認・異常の有無報告
    - 終業点呼（乗務日報の確認・記載）

運行前後の詳細タスクの実施方法については、各社や運行環境で異なる箇所もあると考えられるが、項目としてはおおよそ網羅されていると考えている。なお、運行前後の車内乗客安全に関する乗務員タスクについては、特段これ以上の深化は考えておらず、あくまでも参考情報としての活用を想定している点に注意されたい。

## 14.4　車内乗客安全を実現するために考えられるタスク（通常時以外）

14.3 節で通常時タスクについて説明した。本節では、乗客や自然災害など何かに起因して起こりうる対応についてのタスクについて説明する。その中で、主に乗客に対して緊急で対応しなければいけないタスクと、車両トラブルの車両故障等に対応すべきタスクの二つに分けてタスクを列挙している。

### 14.4.1　緊急時

ここでは図 38 に示す緊急時のタスクについて説明する。こちらも通常時と同様に、事業者へのヒアリングを中心としてタスクを網羅的に記述した。図 38 に示すように、通常時と同様、運転タスクと車内安全タスクに分けるが、緊急時の運転タスクについては本節では対象外とした。緊急時は基本的に通常時と異なって、常に発生する事象でないうえにいつ起こるかもわからない突発的な事象となる。緊急時の事象としては、バス関係、車内トラブル対応、車両火災、犯罪対応などの対応タスクが挙げられる。それぞれのタスクにおける詳細タスクについて下記に記す。

- バス関係
  - 前ドア挟み
  - 後ドア挟み

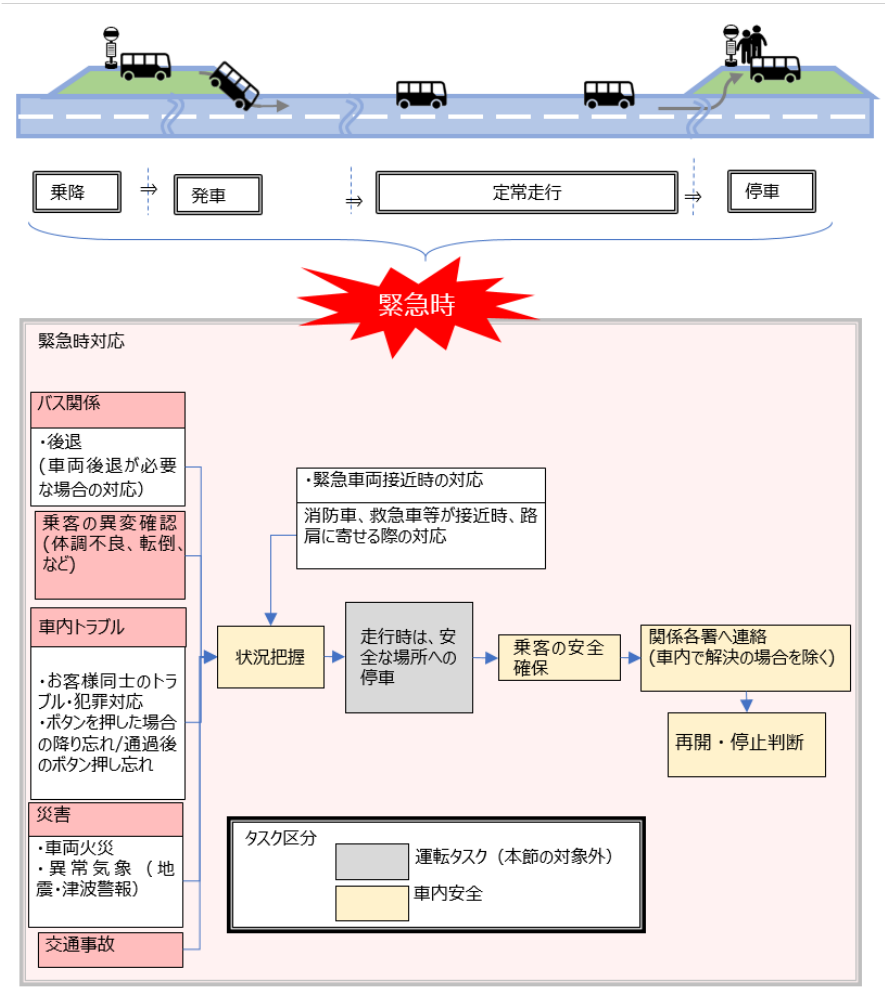



図 38　緊急時の乗務員タスク

  - 走行時の乗客転倒
  - 停車時の乗客転倒
- 車内トラブル対応
  - 病気
  - ボタンを押した場合の降り忘れ
  - 通過後のボタン押し忘れ
  - 忘れ物
  - 掃除
- 車両火災

- 犯罪対応
  - バスジャック
  - スリ
  - 痴漢
  - 危険物
  - 異臭

これらは、それぞれ個別の状況判断から、その後の対応まですべて乗務員が行いつつ、乗務員から運行管理者（責任者等も含む）にも適宜相談しつつ対応する。とくに、乗客への対応が迅速に求められるものも多く、確認するタスクに加えて、対応するタスクについても非常に重要となる。

#### 14.4.2 異常時

ここでは図 39 に示す異常時のタスクについて説明する。こちらも通常時、緊急時と同様に、事業者へのヒアリングを中心としてタスクを網羅的に記述した。図 39 に示すように、通常時や緊急時と同様に、運転タスクと車内安全タスクに分けるが、異常時の運転タスクについては本節では対象外とした。異常時についても、緊急時と同様に、常に発生する事象でないことに加えていつ起こるかもわからない突発的な事象である。異常時の事象は故障トラブルの起因事象となりうる、車両ドア装置故障、運賃収受システム故障、案内表示システム故障、LED 行先表示器故障、降車信号装置故障、空調システム故障などがあり、それぞれで想定される詳細を下記に記す。

- 車両ドア装置故障
  - ドア開閉スイッチ不具合
- 運賃収受システム故障
  - 運賃箱故障
  - IC カードリーダ（乗車 or 降車）故障
  - 整理券発行機故障
- 案内表示（運賃表示）システム故障
  - 表示板 LED 球切れ
  - 表示不具合

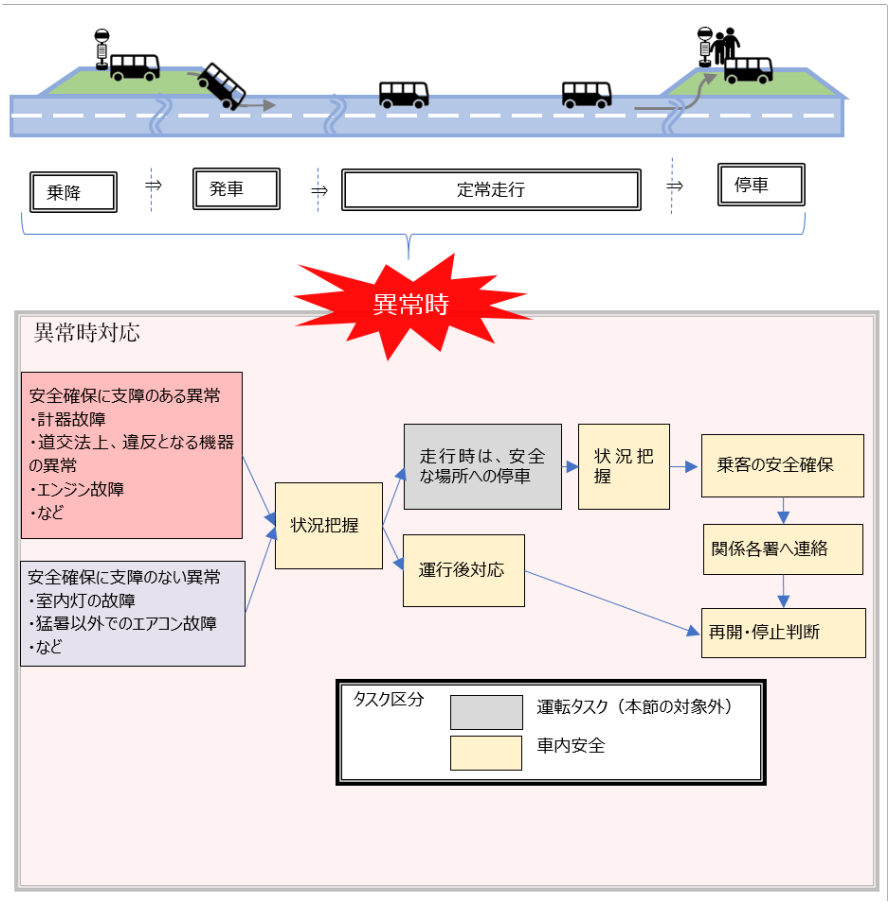



図 39　異常時の乗務員タスク

- LED 行先表示器（横断幕）故障（車内からではなく、周囲の利用者からの指摘）
  - 前方横断幕故障
  - 側方横断幕故障
  - 後方横断幕故障
- 降車信号装置（押しボタン）故障
- 空調システム故障（真夏日 or コロナ）[*52]

これらも緊急時と同様に、それぞれ個別の状況判断から、その後の対応まですべて乗務員が行いつつ、乗務員から運行管理者（責任者等も含む）にも適宜相談して対応する。異常

[*52] この故障が発生すると、真夏日の場合には熱中症対策のため車内冷却が不足する。または、新型コロナウィルス感染防止のための換気能力が不足する。

時の上記タスクにおいて安全確保に関わるものについては、安全走行との連携を強く求められるものがあるため、本タスクについては令和 5 年度以降に更なる深化した内容について報告するものとし、2023 年 8 月時点では現状の記載に留める。

## 14.5　まとめ

令和 4 年度は、車内乗客の安全を確保するために必要な観点や要素が、包括的に漏れなく網羅されるよう通常走行時／通常走行時以外の乗務員のタスクの流れを整理した。これらは、複数の交通事業者の意見を経て構築されたものであり、特殊環境や個別事例などにおける例外はある可能性はあるが、レベル 4 自動運転移動サービスにおいて考慮すべきタスクであるといえる。

令和 5 年度以降では、これらの議論に対する対応策を具体化し、自動運転システムへの移行の際に新たに追加されるタスクを見据えていく。また、レベル 3、レベル 4 自動運転システム（保安要員あり／なし）の各々で異なるタスクを考慮して記載するとともに、個別事例の深化を記す予定であり、個人情報やノウハウ等を除いてガイドブックにおける本章の更新を行う。その際に、国土交通省が令和 5 年 1 月にとりまとめた輸送の安全確保等の検討会の報告書との整合性には十分に留意するものとする。