

データ連携による先読み情報を活用した 遠隔支援システム

システム アーキテクチャ設計素案

目次

1. 概要	4
1.1 背景	4
1.2 本書の目的	4
1.3 対象範囲	5
1.4 前提条件・設計制約	6
1.5 文書体系	7
1.6 参考資料	7
2. システム全体像	8
2.1 システムの役割と目的	8
2.1.1 安全設計の基本方針	10
2.1.2 遠隔支援が利用不能になった場合の扱い（縮退・責任境界）	11
2.1.3 相互運用性と拡張性	11
2.2 関係構成要素	11
2.2.1 自動運転車両	12
2.2.2 データ連携基盤	12
2.2.3 遠隔監視コンソール（遠隔監視センター）	12
2.3 想定利用シナリオ	13
2.4 システム境界	13
2.5 システム要件とアーキテクチャ設計への反映方針	14
3. システムアーキテクチャ	14
3.1 構成方針	15
3.1.1 疎結合構成の原則	15
3.1.2 全国展開を前提とした構成	15
3.1.3 協調領域と競争領域の分離	15
3.1.4 安全優先設計	16
3.2 アーキテクチャ概要図	16
3.3 機能分担（協調領域/競争領域）	18

3.3.1 協調領域	18
3.3.2 競争領域	19
3.4 通信アーキテクチャ	20
3.4.2 通信の基本構成	21
3.4.3 運行管理・支援(助言)通信	22
3.4.4 リアルタイム配信系通信	22
3.4.5 データ連携系通信	23
3.4.6 運用性および拡張性への配慮	23
3.5 相互運用性の確保	23
3.5.1 基本方針	24
3.5.2 プロトコルおよびインターフェースの考え方	24
3.5.3 安全に関わる相互運用性	24
4. セキュリティ	24
4.1 セキュリティ基本方針	25
4.2 認証・認可	27
4.2.1 利用者認証 (SSO)	27
4.2.2 システム認証	28
4.2.3 認可	28
4.3 通信の保護	28
4.3.1 管理・制御系通信 (API/状態通知)	28
4.3.2 リアルタイム配信系通信 (映像・音声・イベント)	29
4.3.3 データ連携系通信 (プローブ情報・路側情報)	29
4.3.4 通信分離および障害影響の限定	29
4.4 監査ログ	29
5. 非機能要件	30
5.1 可用性・冗長化	30
5.2 性能要件	30
5.3 スケーラビリティ	33

5.4 運用・保守	33
6. 将来拡張および展開方針	34
6.1 1対N運用への対応	34
6.2 通信・セキュリティの高度化	35
6.3 標準化と競争領域の整理	35

1. 概要

1.1 背景

自動運転バスを活用した実証や商用運行が全国で拡大しており、複数拠点・複数事業者・複数車両を対象とした遠隔支援運行の需要が高まっている。また、車両・路側デバイス・データ連携基盤を組み合わせたデータ活用が進む中で、システム間の相互運用性や通信品質、データ鮮度の確保が重要な課題となっている。このため、全国規模の展開を見据え、遠隔支援に必要な構成要素の役割分担、データ流通、インターフェース、通信・認証方式等について、複数事業者・複数ベンダー間で共通的に参照可能なアーキテクチャの考え方を整理する必要がある。

1.2 本書の目的

本書は、データ連携基盤による先読み情報を活用した遠隔支援システムについて、全国規模での展開および複数事業者・複数ベンダー間での相互運用性を確保するため、共通化すべきアーキテクチャの考え方を定義することを目的とする。具体的には、既に策定済みのデータ要件（精度・鮮度・整合性、データフロー、インターフェース要件）を前提として、以下を整理する。

- ・自動運転車両、データ連携基盤、遠隔監視コンソール等の構成要素と役割分担
- ・車両状態データ、運行管理データ、路側情報、車両プローブ情報、遠隔支援データの流通構造
- ・遠隔支援リクエストおよび応答結果を連携するための基本インターフェース
- ・通信、認証・認可、セキュリティ、非機能要件に関する設計方針
- ・協調領域として共通化すべき範囲と、競争領域として各事業者に委ねる範囲

なお、本書で定義する標準アーキテクチャは、各事業者のシステム実装やUI/UX、ADS内部の判断・制御ロジックを一律に規定するものではなく、遠隔支援システム間の相互運用性を確保するために共通化すべき構成・データ流通・インターフェースの考え方を示すものである。

1.3 対象範囲

本アーキテクチャが対象とする範囲は、遠隔監視型レベル4における自動運転車両、データ連携基盤、遠隔監視コンソール間の連携構造およびデータ流通とする。(図1)

具体的には、以下の構成要素とそれらの間でやり取りされるデータを対象とする。

- 自動運転車両(自動運転システム)
自動運転を実現する主体であり、遠隔支援の必要性を判定する。また、遠隔支援リクエストの生成及び送信を行うとともに、遠隔支援に必要な車両状態データや映像・音声情報を送信する。
- データ連携基盤
複数の外部情報源から取得したデータを統合・標準化し、遠隔支援システムへ連携する。以下のシステムを含む。
 - 環境情報連携システム¹⁾
路側デバイス等から取得される交通環境情報（路側情報）を提供する。
 - 車両情報連携システム²⁾
複数車両から収集した車両プローブ情報を集約し、提供する。
- 遠隔監視コンソール
人が介在し、運行監視および遠隔支援判断を行う領域とする。以下のシステムから構成される。
 - 自動運転車両管理システム：複数車両の運行状況を統合的に管理し、運行全体の最適化および異常検知を行う。
 - 遠隔支援システム：車両状態および外部情報(先読み情報)を統合表示し、遠隔監視者による判断支援および指示操作を可能とする。
 - 映像・音声システム：遠隔監視に必要な映像・音声情報を提供する

本アーキテクチャでは、上記構成要素間におけるデータフロー（アップリンク／ダウンリンク）およびインターフェースの設計を対象とする。

なお、自動運転技術そのものや詳細な車両制御ロジックについては、本アーキテクチャの対象外とする。

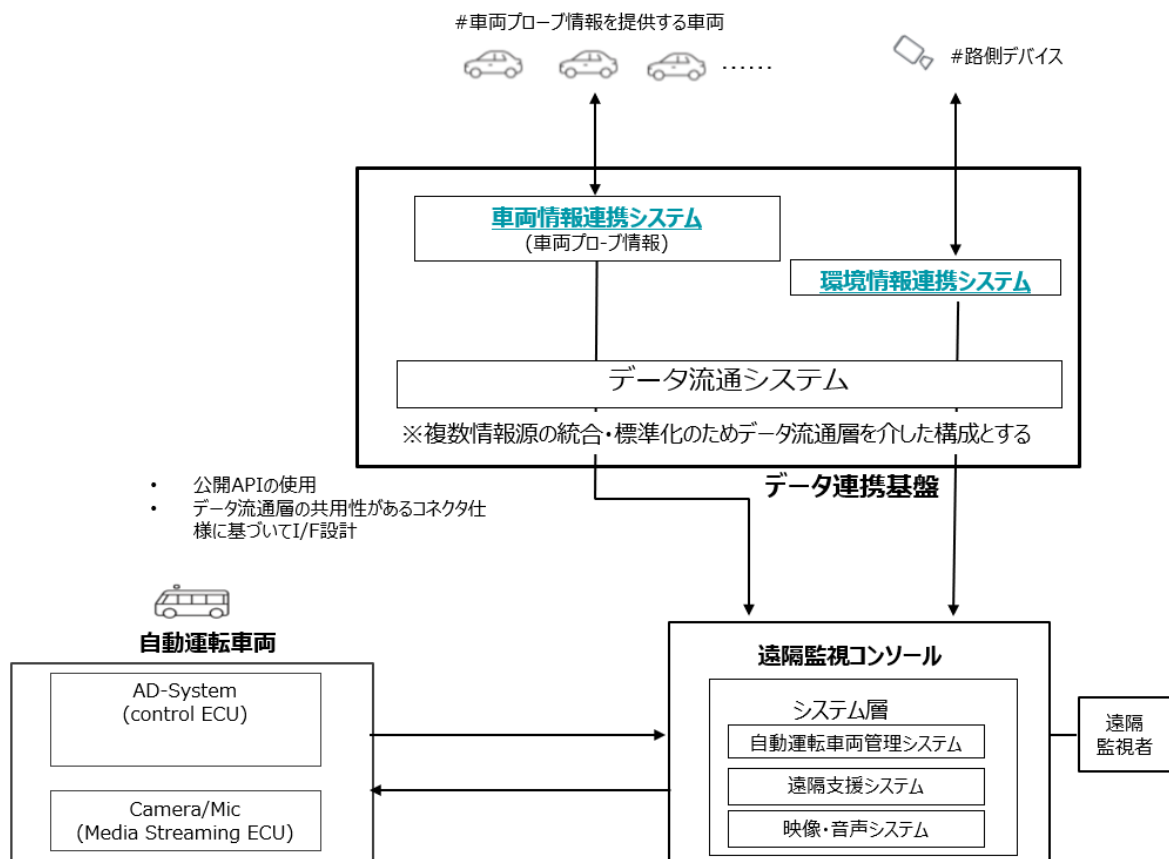


図1: アーキテクチャ構成概要図

- 1) 24年度「産業DXのためのデジタルインフラ整備事業」の成果物
- 2) 25年度「デジタルライフライン整備事業」のC-2にて開発中

1.4 前提条件・設計制約

- 全国規模での運用を前提とし、1対N運用に耐える拡張性・可用性を確保すること
- 遠隔支援に用いる各システムの機能・インターフェース仕様を踏まえ、段階的な導入・早期実装を可能とすること
- 通信品質（遅延・冗長性）、セキュリティ基盤（認証・認可等）を満たすこと
- データの精度・鮮度・整合性を維持できるよう、基盤側の処理方式を適切に設計すること

1.5 文書体系

発行予定の関連文書一覧と各文書の対象範囲を以下に示す。

ドキュメント名	対象範囲
自動運転バス運行業務定義書素案	自動運転バスの運行業務（運行フロー、ユースケース、役割分担）の定義
データ連携による先読み情報を活用した遠隔支援システム データ要件定義素案	遠隔支援に必要なデータ項目および要件（精度・鮮度・整合性等）の定義
データ連携による先読み情報を活用した遠隔支援システム システムアーキテクチャ設計素案(本ドキュメント)	データ要件を満たすためのシステム構成、データ流通、インターフェース設計
「先読み情報を活用した自動運転バス運行業務」実装ガイドライン策定に向けた検討概要書	先読み情報を活用した遠隔支援の運用方法を整理した全体像を理解するためのサマリー

1.6 参考資料

- データ連携による先読み情報を活用した遠隔支援システム_データ要件定義素案
- デジタルアーキテクチャ・デザインセンター(2025年5月9日).「実証実験用車両情報連携システム仕様書（仮仕様）」
- デジタルアーキテクチャ・デザインセンター.
environmental-information-integration-system.GitHub, 2025
- ITS情報通信システム推進会議.「一般道向け安全運転支援・自動運転システム実験用通信メッセージガイドライン ITS FORUM RC-019 1.0版」

2. システム全体像

本章では、データ連携基盤から取得される先読み情報を活用する際における遠隔支援システムの位置づけおよび全体構造について述べる。

全体のシステムアーキテクチャ構成は、1.3節の図1に示す通り、データ流通システムを介して、環境情報連携システム(路側情報)・車両情報連携システム(車両プローブ情報)と連携しながら、遠隔監視・支援を実現する「データ連携による先読み情報を活用した遠隔支援システム」の運用基盤である。

2.1 システムの役割と目的

データ連携による先読み情報を活用した遠隔支援の役割は、単なる遠隔監視に留まらず、定義したデータ要件、標準化したインターフェースに基づいた情報を遠隔監視コンソール上に統合して遠隔監視者に提供することにより、運行継続性と安全性を両立する遠隔支援を実現することにある。データ連携による先読み情報を活用した遠隔支援の役割は、単なる遠隔監視に留まらず、定義したデータ要件および標準化したインターフェースに基づく情報を遠隔監視コンソール上に統合して遠隔監視者に提供することで、運行継続性の向上を実現することにある。なお、安全性の確保に関する基本方針については、2.1.1項に示す。

具体的には、以下の機能を実現する。

(1) 遠隔監視機能

遠隔監視センターにおいて、以下の情報をリアルタイムに把握する。

- 車両状態（位置、速度、システム状態等）
- 運行状況（ダイヤ、遅延状況等）
- 周辺環境情報（交通状況、路側センサ情報等）

これにより、複数車両の同時監視（1対N運用）を可能とする。

(2) 先読み型遠隔支援機能

データ連携基盤を通じて取得した情報を活用し、車両単独では対応困難な状況に対して、運行継続を支援する。

- 路駐車両、混雑、交差点状況等の事前把握
- 将来リスクの予測に基づく判断支援
- 遠隔監視者による助言生成・提示

これにより、MRM（Minimal Risk Maneuver）の発動回避およびサービス可用性の向上を図る。

（3）データ統合・可視化機能

異種システムから取得されるデータを統合し、遠隔支援の助言提供に適した形で提供する。

- ・ 時刻同期・データ整合性の確保
- ・ 空間情報の統合（地図・車両・路側）
- ・ HMI（ヒューマンマシンインターフェース）上での一元可視化

また、遠隔監視者数Mと自動運転車両台数Nの関係については、1:NまたはM:Nのように複数車両を同時に監視する運用を前提とし、各車両の状態、リスクレベル、対応要否等を識別可能とするために、

- ・ 車両状態に関する異常種別
- ・ 対応要否を示す状態フラグ（例：要対応／監視継続 等）
- ・ 緊急度・優先度を示す属性情報

といった識別用データを設計し、自動運転車両の車両状態データに統合して遠隔監視側に提供する。これにより、遠隔監視者が複数車両の中から優先対応対象を判断可能な情報構造を提供する。

なお、これらの属性情報の具体的な算出ロジックや判定基準、およびそれらをどのように表示、操作に反映するかといったUI/UX設計については、各事業者の自動運転車両の判断ロジックおよび運用方針に依存するため競争領域とし、本書では詳細のフォーマットを定義しない。本機能は、データ要件定義で整理された精度・鮮度・整合性要件を満たすとともに、遠隔支援における状況認識および優先度判断を支える中核機能である。

（4）運用継続性の確保

通信断や一部システム障害が発生した場合でも、運行への影響を最小化する構成とする。

- ・ データ欠損時のフォールバック
- ・ 段階的機能縮退
- ・ 冗長構成の考慮

2.1.1 安全設計の基本方針

本システムは、自動運転車両が自律的に安全状態を維持できることを前提とし、先読み型遠隔支援機能は安全性および運行可用性を向上させるための「補助的機能」と位置づける。

また、障害発生後の対処（フェイルセーフ）に加え、障害の発生確率低減および影響最小化を図る予防的安全設計の観点を取り入れ、システム全体の安全性を確保する。

■ 予防的安全設計

障害発生後の対処に依存せず、障害の発生確率低減および影響最小化を両立する構成とする。具体的には以下の観点で設計を行う。

- 通信経路の冗長化および異常検知（ヘルスチェック、タイムアウト管理等）
- 安全関連通信と非安全通信の論理的分離および優先制御
- 重要処理における状態整合性の確保（遠隔支援リクエストの有効期限管理、再送制御等）
- 異常時の影響範囲を局所化するためのコンポーネント分離設計

■ フェイルセーフ設計（障害発生時の対応）

- MRM（最小リスク動作）との関係: 通信遮断やシステム障害により遠隔支援が利用不能となった場合でも、車両側の安全対策（MRM）によって最小リスク状態へ移行できることを運用前提とする。
- 意思決定の所在: 遠隔支援による助言は車両の意思決定を補完するものであり、車両側の安全判断を代替するものではない。これにより、誤助言や通信遅延が発生した場合でも、車両自体の安全性は損なわれない設計とする。
- フォールトトレランス: 先読み型遠隔支援機能が安全上の単一障害点とならないよう、車両側の安全機能、先読み型遠隔支援機能、データ連携基盤の役割を分離し、独立性を確保する。

2.1.2 遠隔支援が利用不能になった場合の扱い（縮退・責任境界）

先読み型遠隔支援機能は補助的機能であるため、通信断・遅延・認証失効・システム障害等により利用不能となった場合でも、直ちに安全上の危険状態を生じさせないことを前提とする。

利用不能時には、以下の挙動を基本とする。

- 車両側は自律判断を継続し、必要に応じてMRMへ移行可能であること
- 遠隔支援システムは通信状態・支援可否状態を明示的に管理し、遠隔監視者へ通知すること
- 利用不能状態が継続する場合は、運用手順に基づき待機・運行中断等の判断を可能とすること
- 通信復旧後は、状態同期および整合性確認を行った上で支援を再開すること

本設計により、遠隔支援は安全機能の前提条件とならず、運行の品質向上を担う拡張補助的機能として位置付けられる。

2.1.3 相互運用性と拡張性

本事業における遠隔支援システム検討では、先読み情報を活用して自動運転車両のスタックや運行停止を未然に回避し、遠隔監視者による助言を「事後対応」から「予防的支援」へと高度化することを狙いとしている。この実現には、特定車両や単一事業者に閉じた情報取得方式ではなく、異なる事業者・車両・サービス間で共通に利用可能な形で先読み情報を取得・連携できる仕組みが不可欠である。そのため、本事業ではデータ連携基盤を介し、V2N（Vehicle to Network）による先読み情報等を取得する構成を設計前提とした。これにより、異なる事業者間における相互運用性を確保するとともに、API（Application Programming Interface）公開およびデータ連携基盤の共用を前提としたコネクタ仕様にに基づき、インターフェース設計を行うことが可能となる。結果として、共通的な実運用への柔軟な適用を実現する。

2.2 関係構成要素

本節では、1.3節で示した対象範囲に含まれる構成要素について、図1に示す構成に基づき、各システムの役割・相互関係の観点から整理する。

2.2.1 自動運転車両

車両内部で取得された車両状態情報および各種走行データを生成する主体である。また、走行状況に応じて遠隔支援の必要性を判定し、遠隔支援リクエストを生成・送信する。本システムは、これらの情報を受信し、遠隔監視および遠隔支援判断に活用する。

2.2.2 データ連携基盤

データ連携基盤は、複数の外部情報源から取得されるデータを統合・標準化し、遠隔監視コンソールへ提供する役割を担う。提供元と利用側を疎結合とすることで、複数事業者・複数システム間での相互運用性を確保する。

本基盤は、以下の情報連携システムと接続される。

(1) 車両情報連携システム

複数車両から収集された車両プローブ情報を統合し、道路状況に関する情報（障害物、渋滞、路面状態等）を生成・提供する。

本システムは、これらの情報を先読み情報として遠隔支援判断に活用する。

(2) 環境情報連携システム

信号機や路側センサ等から取得される交通環境情報を提供する。

提供される情報には、信号状態、路側物標情報、デバイス状態（死活）等が含まれる。

本システムは、これらの情報を車載センサでは取得困難な情報の補完として活用する。

2.2.3 遠隔監視コンソール（遠隔監視センター）

遠隔監視コンソールは、遠隔監視者が車両状態および外部環境情報を統合的に把握し、遠隔支援判断を行うための操作・表示基盤である。

本コンソールは、以下のサブシステムから構成される。

(1) 自動運転車両管理システム

ダイヤ情報、配車情報、便ID／トリップID等の運行管理情報を管理し、複数車両の運行状況を統合的に可視化する。これにより、個別車両の状態を運行全体の文脈の中で把握することを可能とする。

(2) 遠隔支援システム

車両状態データと先読み情報等の情報を統合表示し、遠隔監視者による状況判断および助言提供等を支援する。また、遠隔支援結果を車両へ送信する機能を有する。

(3) 映像・音声システム

車両から送信される映像および音声をリアルタイムに表示し、遠隔監視に必要な視覚・聴覚情報を提供する。本機能は、遠隔監視型レベル4における監視要件への対応として位置付けられる。

2.3 想定利用シナリオ

本システムは、以下の利用を想定する。

- 複数車両の同時監視（1対N運用）
- 車両状態や安全イベントの確認
- 異常発生時の状況把握および助言
- データ連携基盤を介した事業者間データ連携の活用

複数拠点での運用を前提とし、段階的な拡張を想定する。

2.4 システム境界

本システムの責任範囲は、遠隔支援に必要な監視・支援機能および関連するデータ連携機能とする。

以下の項目については、各システム・各事業者に依存する要素であり、本検討における共通設計の対象外(競争領域)として位置付ける。なお、協調領域および競争領域の具体的な整理については、第3章にて詳細に記述する。

- 自動運転車両内部に閉じた判断・制御ロジック
 - ✓ 各業者のADSの設計思想、およびアルゴリズムに依存する。
- 車両固有のセンサ構成および車載実装
 - ✓ 車両ハードウェアおよび構成の差異に依存する
- 各事業者固有の運行ノウハウに基づく最適化処理

- ✓ 運行効率やサービス品質に関わる差別化要素であり、競争領域として各事業者に委ねる

2.5 システム要件とアーキテクチャ設計への反映方針

データ要件定義素案および日立地区でのユースケース検討を踏まえ、遠隔支援システムに求められる主要なシステム要件を以下の通り整理する。

システム要件	要件の背景	アーキテクチャへの反映
先読み情報の活用	路上駐車、工事、渋滞等を事前に把握し、停止回避・運行継続を支援するため	車両情報連携システム・環境情報連携システムからの情報をデータ流通システム経由で遠隔監視コンソールへ連携
遠隔支援リクエストへの確実な応答	車両からの支援要求に対し、対象車両・対象イベントを誤らず応答するため	車両ID、遠隔支援リクエストID、応答結果、応答時刻を最小限の標準IFとして整理
1:N/M:N運用への対応	複数車両を横断的に監視し、優先対応対象を判断するため	異常種別、対応要否フラグ、緊急度／優先度属性を車両状態データに含める
相互運用性の確保	複数事業者・複数ベンダー間で接続可能とするため	データ形式、イベント定義、基本操作フローを協調領域として整理
安全性・運用継続性の確保	通信断・遅延・障害時にも安全側に移行し、影響を局所化するため	フェイルセーフ、予防的安全設計、通信分離、冗長化を設計方針に反映
リアルタイム性とセキュリティの両立	遠隔支援判断に必要な低遅延性を維持しつつ、セキュリティを確保するため	通信種別ごとの分離、認証・暗号化、QoS・優先制御を採用

これらの要件を満たすため、3章以降において、システム構成、協調領域／競争領域、通信方式、セキュリティ、非機能要件の観点からアーキテクチャ設計を行う。

3. システムアーキテクチャ

本章では、遠隔支援システム全体の構成および各構成要素の役割を整理し、全国規模での展開を見据えた標準アーキテクチャの考え方を示す。本アーキテクチャは、既存システムと

の接続や段階的な導入を前提としつつ、相互運用性、拡張性、運用継続性を重視して設計する。

3.1 構成方針

遠隔支援システムの構成にあたっては、以下の方針を基本とする。

3.1.1 疎結合構成の原則

各構成要素は明確な責務を持ち、相互依存を最小化する。特定要素の変更や障害が他構成要素へ波及しない構成とし、段階的な機能追加や改善を可能とする。

図2に示す通り、自動運転車両、遠隔監視コンソール、データ連携基盤は、それぞれ独立した構成要素として配置し、データインターフェースを介して連携する構成とする。これにより、映像・音声系、遠隔支援系、運行管理系、外部情報連携系を個別に追加・変更できる構成とする。

3.1.2 全国展開を前提とした構成

全国展開および複数事業者での利用を前提とし、特定ベンダーや個別実装に依存しない構成とする。地域差や既存インフラ差異を吸収可能な構成とする。図2では、路側情報や車両プローブ情報を、個別システムから直接遠隔監視コンソールへ接続するのではなく、データ連携基盤内のデータ流通システムを介して取得する構成としている。これにより、地域ごとに利用可能な情報源や提供システムが異なる場合でも、遠隔支援側では共通インターフェースを通じて先読み情報を活用できる。結果として、地域・事業者・ベンダーの差異を吸収しつつ、全国展開に適用可能な構成とする。

3.1.3 協調領域と競争領域の分離

デジタル公共財であるデータ連携基盤を活用した遠隔監視・遠隔支援に関わる共通的な仕組みは協調領域として整理し、標準化対象とする。一方、判断ロジックや付加価値サービス等は競争領域とし、各事業者の創意工夫を妨げない構成とする。

各構成要素における具体的な協調領域/競争領域の対象範囲については、3.3節にて詳細に整理する。

3.1.4 安全優先設計

通信障害やデータ遅延等が発生した場合においても、安全に関わる情報が優先的に扱われる設計とする。重要イベントの視認性および到達性を確保することを基本とする。図2では、遠隔監視コンソール側に、遠隔支援システム、自動運転車両運行管理システム、映像・音声システム等を独立した構成要素として配置している。これにより、遠隔支援関連情報、MRM通知、車両状態データ等の安全関連情報を、遠隔監視コンソール上で優先的に把握・処理できる構成としている。

また、映像・音声等の高帯域データと、遠隔支援・運行管理に関わる安全関連情報を論理的に分離して扱うことで、通信量や処理負荷の変動が安全関連情報の伝達に与える影響を抑制する。これにより、通信品質が一時的に低下した場合でも、遠隔支援判断に必要な重要情報の視認性および到達性を確保する。

3.2 アーキテクチャ概要図

本節では、2.5節で整理したシステム要件および設計方針を反映した統合アーキテクチャを示す。遠隔監視センターに配置される遠隔監視コンソールを中核とし、自動運転車両、および車両情報連携システム・環境情報連携システムを統合したデータ連携基盤と相互に接続される構成とする。

遠隔支援における意思決定は、複数のデータを統合的に評価することで行われる。

本検討では、利用されるデータを以下の5種類に分類する。なお、各データの詳細定義はデータ要件定義書にて整理しているため、そちらを参照されたい。

表 1データ分類

データ項目	役割
A. 車両状態データ	車両の現在状態を把握し、遠隔支援の基礎情報として利用
B. 運行管理データ	運行情報を管理し、運行継続可否の判断に利用。
C. 路側情報	遠隔支援に必要な情報(例：路駐車情報)を先読み情報や車両単体で検知不可の死角部分の環境情報として提供し、遠隔支援に利用
D. 車両プローブ情報	
E. 遠隔支援データ	遠隔支援リクエストに応じた助言内容として、遠隔支援に利用

アーキテクチャ概要図(図2)では、各構成要素間の主なデータフロー（アップリンク／ダウンリンク）および役割分担を示し、アーキテクチャ全体の構造を俯瞰的に把握できるように整理する。特に遠隔支援は、遠隔監視により取得される車両状態、映像・音声、運行管理情報等を前提として実施されるため、本図では遠隔監視機能を遠隔支援の基盤機能として位置付け、遠隔支援を成立させるために前提となる遠隔監視機能、自動運転車両、データ流通システム、車両情報連携システム、環境情報連携システムを含めた全体アーキテクチャを示すものである。

データ連携基盤については、車両プローブ情報/路側インフラ情報のいずれを情報源とする場合でも、遠隔支援側で共通的に利用可能なインターフェースを定義する。

これにより、情報源に依存しないデータ連携を実現し、設計・実装の柔軟性および標準化適合性を確保する。

また、遠隔支援の社会実装は段階的に進むことを前提とし、各機能を独立して実装可能な構成とする。

- ・映像・音声等の遠隔監視機能は先行実装・検証が可能
- ・先読み情報はデータ連携基盤を介したAPI連携により提供
- ・情報源に依存しない構成とすることで将来拡張に対応

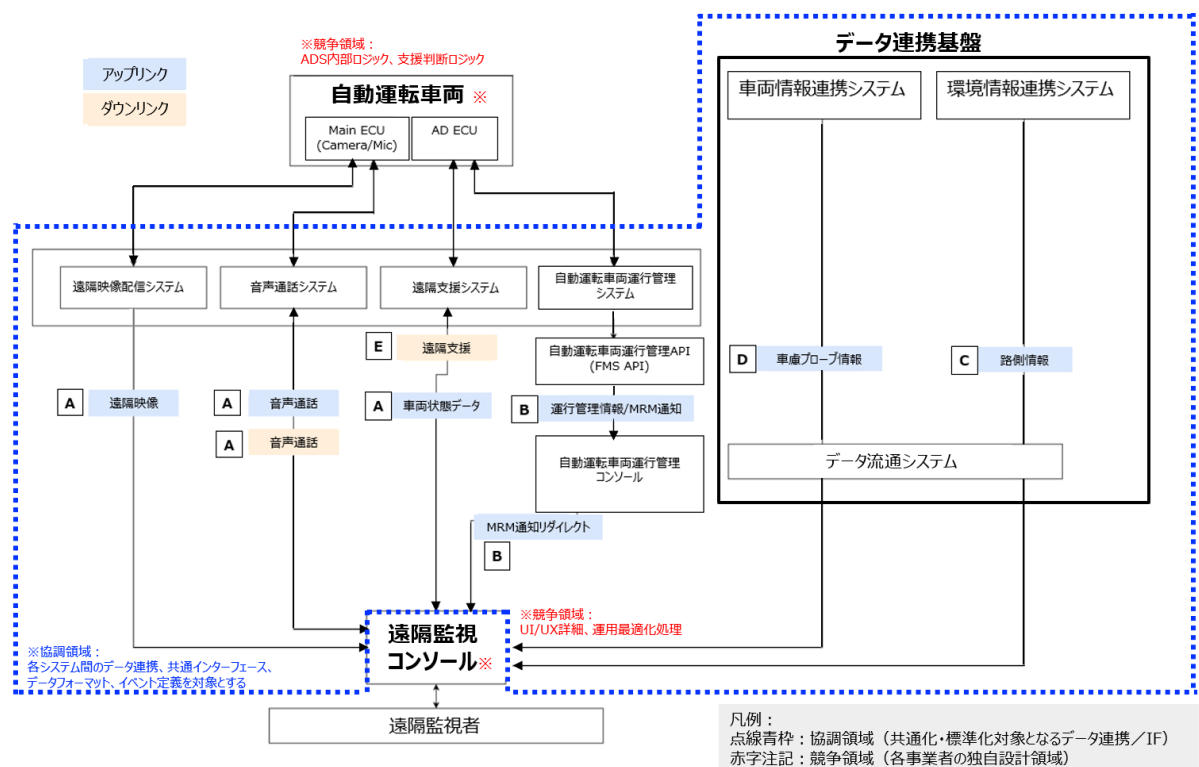


図2: 遠隔監視を含む遠隔支援運行のアーキテクチャ概要図

3.3 機能分担（協調領域/競争領域）

本節では、図2のアーキテクチャ設計概要図に示す構成要素との対応関係を踏まえ、遠隔支援における協調領域/競争領域を整理する。本アーキテクチャでは、複数事業者・複数システム間で相互運用性を確保するために共通化すべきデータ構造、インターフェース、通信・認証方式、イベント定義等を協調領域として位置付ける。一方で、各システム内部の判断ロジック、UI/UXの詳細設計、運用ノウハウ、付加価値サービス等については、各事業者の競争領域として位置付ける。図2では、協調領域と競争領域の関係を色分けして示す。

3.3.1 協調領域

複数事業者・複数システムで共通化が求められる領域として、以下を対象とする。

- データ流通システムを介したデータ連携方式
- A～Eのデータ分類および基本的なデータ構造
- 遠隔支援リクエストおよび応答結果を連携するための基本インターフェース
- 遠隔支援・監視に関わる基本的なUI構成および操作フロー
- 認証・認可、通信、セキュリティに関する共通基盤
- 安全に関わるイベント／アラートの共通定義（レベル、優先度、通知先）
- 安全関連情報の優先処理方針

図2においては、データ流通システム、各システム間のデータインターフェース、遠隔支援リクエスト／応答結果、および安全関連イベントの連携部分を協調領域として示す。協調領域は、相互運用性および再現性を確保する観点から標準化対象とし、事業者間で共通理解を形成する。

例えば、路上駐車回避のような遠隔支援ユースケースにおいて、車両が生成した回避行動に対して遠隔監視者が助言を行う基本的な操作フローや、遠隔支援リクエストや応答結果のデータ構造（車両ID、遠隔支援リクエストID等）が事業者ごとに異なる場合、異なるシステム間での連携や運用の引き継ぎが困難となる。このような状況では、複数事業者による共同運行やシステム更新時の相互接続において、個別調整が必要となり、導入コストの増大や運用の非効率化を招く。これに対し、データ形式および基本的な操作フローを標準化することで、異なる事業者・システム間でも同一のインターフェースで接続可能となり、システムの相互接続性が確保されるとともに、運用手順の共通化による教育コストの低減や、1対N／M対N運用の拡張性向上が期待される。また、安全に関わるイベント定義や優先度の共通化により、異なるシステム間でも一貫したリスク認識および対応が可能となり、遠隔支援操作

の再現性および信頼性の向上につながる。このように、協調領域の標準化は、単なる技術的統一に留まらず、運用効率の向上にも寄与するものである。

3.3.2 競争領域

図2においては、自動運転車両内部のADS判断ロジック、遠隔支援システム内部の支援判断プロセス、アラート生成・優先度判定ロジック、遠隔監視コンソールの詳細なUI/UX設計、運行管理の最適化処理等を競争領域として示す。競争領域は、協調領域で定義された共通データ構造およびインターフェースを活用しつつ、各事業者の運用方針、サービス設計、技術方式に応じて独自に設計・高度化される領域である。

具体的には、以下を競争領域として位置付ける。

- ・ 運行状況、交通環境、車両状態等のデータを用いた支援判断プロセス
- ・ 異常兆候やリスクを早期に検知するためのアラート生成、優先度判定ロジック
- ・ 遠隔監視者の判断を支援するUI/UXやワークフロー設計
- ・ 1:N/M:N運用を前提とした監視・支援オペレーションやUI/UXの詳細設計
- ・ データの組み合わせや分析に基づく高度化・最適化処理

特に、異常車両の検知結果、リスクレベル、対応要否等の情報をどのように可視化し、遠隔監視者の意思決定を支援するかについては、各事業者の運用方針やサービス設計に強く依存する。そのため、本書ではこれらの具体的な判断ロジック、画面設計、操作手順の詳細については標準化対象外とする。一方で、これらの判断や可視化を可能とするための識別用データ項目、すなわち異常種別、対応要否フラグ、緊急度・優先度等の属性情報については、協調領域において共通的に定義することを前提とする。

すなわち、本アーキテクチャでは、「判断に必要な情報構造は共通化し、具体的な判断ロジックおよびUI設計は各事業者に委ねる」という役割分担とする。

以上を踏まえ、協調領域および競争領域の整理を表2に示す。

表2 協調領域／競争領域の整理

項目	協調領域として共通化する内容	競争領域として各事業者に委ねる内容
データ連携	データ分類、データ形式、IF仕様、データ流通方式	データ分析、予測、付加価値サービス
遠隔支援操作	リクエスト受信、応答結果、ID紐付け等の基本フロー	具体的な画面設計、操作性、ワークフロー詳細
安全関連イベント	異常種別、対応要否、優先度等の基本属性	優先度判定ロジック、アラート生成ロジック
通信・認証	認証方式、通信方式、セキュリティ基本方針	実装方式、運用ポリシー、監視方式
ADS／車両側	遠隔支援リクエスト／応答IF	ADS内部判断、行動案生成、採否判断

3.4 通信アーキテクチャ

遠隔支援システムにおける通信アーキテクチャは、1対N・M対N運用を前提とし、遠隔監視者が必要な情報を適時に把握し、車両側へ助言結果を確実に返送できることを目的として設計する。通信方式の検討にあたっては、扱うデータの用途に応じて、即時性、信頼性、帯域、許容遅延、運用継続性の観点から要求特性を整理し、それぞれに適した通信方針を採用する。特に、日立市モデルで想定する路上駐車回避等の遠隔支援では、車両状態、遠隔支援リクエスト、映像・音声、先読み情報、遠隔支援結果等が異なるタイミング・用途で利用される。そのため、すべての通信を同一方式で扱うのではなく、通信種別ごとに要求性能を整理し、用途に応じて分離・最適化する構成とする。

表3 通信種別ごとの要求性能と通信方針

通信種別	主な対象データ	要求性能・特性	採用方針
運行管理・支援系通信	車両状態、遠隔支援リクエスト、遠隔支	確実性・到達性を重視。 対象車両・対象リクエス	API／メッセージ通信等により、認証・認可、ID管理、再

通信種別	主な対象データ	要求性能・特性	採用方針
	援結果、運行管理情報	トに正しく紐付くことが必要	送制御、有効期限管理を考慮する
リアルタイム配信系通信	映像、音声、イベント通知	低遅延性・継続性を重視。高帯域となるため、他通信への影響を抑制する必要あり	WebRTC等の低遅延配信技術やPub/Sub型通知を想定し、帯域制御・優先度制御を考慮する
データ連携系通信	路側情報、車両プローブ情報、先読み情報	情報源ごとの差異を吸収し、遠隔支援側で共通利用できることが必要	データ流通システムを介したAPI連携を基本とし、共通データ形式・インターフェースで連携する
監査・ログ系通信	操作ログ、支援履歴、システムログ	即時性よりも完全性・追跡性を重視	高頻度通信とは分離し、蓄積・後追い確認可能な形式で管理する

上記の整理に基づき、本アーキテクチャでは、運行管理・支援系通信、リアルタイム配信系通信、データ連携系通信を分離して設計する。これにより、映像等の高帯域通信による負荷が、遠隔支援リクエストや助言結果等の安全関連情報の伝達に影響しない構成とする。

3.4.1 通信設計における基本原則

- ・ 安全関連情報の優先性確保
- ・ 高帯域通信と制御系通信の影響分離
- ・ 障害発生時の影響範囲の限定
- ・ 段階的な拡張が可能な構成

特に、安全関連イベントや遠隔監視に関わる通信については、映像等の高帯域通信の影響を受けないよう論理的に分離を考慮する。また、同期型API通信と非同期型イベント駆動型通信を適切に組み合わせることで、即時性と耐障害性の両立を図る。

3.4.2 通信の基本構成

通信は主に以下の用途に分類され、それぞれの特性に応じた方式を採用する。各通信の対象範囲は図3における該当部分に対応する。

● 運行管理・支援(助言)系通信

(自動運転車両－遠隔監視コンソール間)

運行管理、車両状態取得、遠隔支援操作等に関する通信

- リアルタイム配信系通信（映像、音声、イベント通知等）

(自動運転車両－遠隔監視コンソール間)

映像、音声、イベント通知等のリアルタイム配信に関する通信

- データ連携系通信（車両プローブ情報、路側情報等）

(車両情報連携システム／環境情報連携システム－データ連携基盤－遠隔監視コン

ソール間) 車両プローブ情報、路側情報等の連携に関する通信

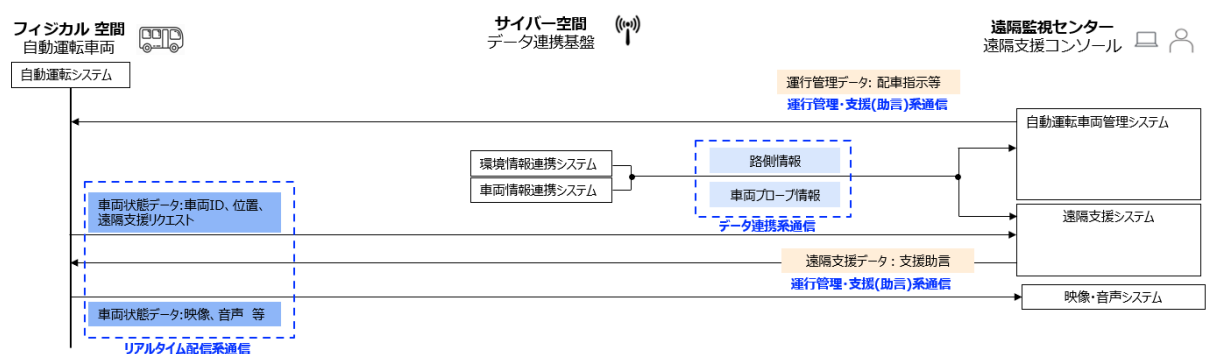


図3: システム通信構成図

3.4.3 運行管理・支援(助言)通信

管理・制御系通信は、遠隔監視センターと各システム間の信頼性を重視し、HTTPSを基本とする。認証・認可と密接に関係する通信であるため、API単位でのアクセス制御を行い、誤操作や権限逸脱が運行へ与える影響を抑制する。

3.4.4 リアルタイム配信系通信

映像・音声・イベント通知等のリアルタイム配信系通信は、低遅延性を考慮した方式を採用する。具体的には、映像・音声配信については WebRTC 等のリアルタイム通信技術、イベント通知については MQTT 等のPub/Sub型メッセージングの活用を想定する。

接続時の認証および購読単位での制御により、必要な情報のみを配信対象とし、不要な負荷や情報過多を防止する。また、通信品質の変動時においても、遠隔支援判断に必要な情報の継続的な取得が可能となるよう、帯域制御や優先度制御を考慮した設計とする。

3.4.5 データ連携系通信

データ連携系通信は、データ連携基盤を介した連携を前提とし、提供元・提供先の識別およびデータ単位での制御を行う。また、提供元ごとの差異を吸収し、共通定義に基づいたデータ形式へ正規化した上で連携を行う。これにより、複数事業者間でのデータ共有や将来的な連携拡張に対応可能な構成とする。

また、共通定義に基づくスキーマ管理およびバージョン管理を行い、後方互換性を考慮した連携を実現する。

3.4.6 運用性および拡張性への配慮

通信アーキテクチャは、運用開始後の拡張や構成変更を前提とし、段階的なスケールアウトや通信方式の追加が可能な構成とする。図2に示す通り、本アーキテクチャでは、運行管理・支援系通信、リアルタイム配信系通信、データ連携系通信を用途ごとに分離し、それぞれ独立した通信経路およびインターフェースとして扱う構成としている。

これにより、例えば新たな路側情報や車両プローブ情報を追加する場合には、データ連携基盤内のデータ流通システム側のインターフェースを拡張することで、遠隔監視コンソール側の基本構成を大きく変更せずに対応可能とする。また、映像・音声等の高帯域通信と、遠隔支援リクエスト・遠隔支援結果等の安全関連通信を論理的に分離することで、通信障害や負荷集中が発生した場合でも、影響範囲を限定し、運行管理や遠隔支援判断への影響を最小化する構成とする。さらに、将来的に監視対象車両数や接続拠点数が増加した場合にも、通信種別ごとに処理能力や接続方式を段階的に拡張できる構成とし、1:N/M:N運用への拡張性を確保する。

3.5 相互運用性の確保

本システムは、複数事業者・複数システムによる利用および将来的な拡張を見据え、相互運用性の確保を重要な設計方針とする。

特定の実装やベンダーに依存せず、異なるシステム間でも円滑に連携可能な構成とすることで、段階的な導入や機能追加を可能とする。

相互運用性は以下の3層で確保する。

1. 技術的相互運用性：標準的な通信プロトコルおよびAPI形式を採用し、特定実装に依存しない接続を可能とする

2. 意味的相互運用性：データ形式、イベント定義、アラートレベルを共通化し、システム間で同一の意味解釈が可能となるよう整理する
3. 運用的相互運用性：通知ルール、責任分界点、障害対応フロー等を整理し、異なる事業者間でも円滑に運用できる前提を整備する

3.5.1 基本方針

相互運用性を確保するため、以下の方針を基本とする。

- システム間連携においては、広く利用されている標準的な通信プロトコルおよびインターフェースを採用する
- データ連携基盤を介した連携を前提とし、提供元・提供先が疎結合となる構成とする
- データ形式やイベントの意味を共通化し、システム間での解釈の差異を最小化する

3.5.2 プロトコルおよびインターフェースの考え方

管理・制御系通信やデータ連携においては、APIベースのインターフェースを基本とし、リアルタイム性が求められる場合にはストリーミング型の通信方式を併用する。これにより、用途に応じた通信方式の選択を可能としつつ、全体として一貫した連携モデルを維持する。インターフェース変更時にはバージョン管理および後方互換性を考慮する。

3.5.3 安全に関わる相互運用性

遠隔支援運行における安全性を担保するため、安全に関わるイベントやアラートについては、レベル、優先度、通知先等の基本的な定義を協調領域として共通化する。これにより、異なるシステムや事業者間であっても、安全に関する情報を同一の意味として扱うことを可能とする。

4. セキュリティ

本章では、遠隔支援のシステムアーキテクチャ全体に共通するセキュリティ設計の基本的な考え方を整理する。自動運転車両、データ連携基盤、遠隔支援システム等の複数の構成要素がネットワークを介して接続される分散システムであり、特に遠隔支援においては通信機能の活用が前提となることから、不正アクセス、なりすまし、通信内容の漏洩・改ざん、サービス停止等のリスクに対する包括的な対策が不可欠である。

4.1 セキュリティ基本方針

自動車分野におけるサイバーセキュリティの国際標準であるISO/SAE 21434を参照し、車両および関連システムを含むサイバーセキュリティ確保の考え方に準拠することを前提とする。さらに、UNECE WP.29 (UN-R155) に基づくサイバーセキュリティ管理 (CSMS) の考え方、および国土交通省「自動運転車の安全技術ガイドライン」や「RoAD to the L4プロジェクト」報告書に示される要件を踏まえ、開発・運用を通じた継続的なセキュリティ確保を行う。

具体的には、情報セキュリティの3要素および運用管理に基づき、以下の通り取り組む。

(1) 機密性 (Confidentiality)

- 通信およびデータの機密性を保護し、情報の漏洩や不正利用を防止する。
- 通信経路の暗号化：映像、音声、車両状態データ等の盗聴を防止するためのエンドツーエンドの暗号化。
- 認証・認可基盤の構築：強固な認証機構により、正当な権限を持つ利用者およびシステムのみアクセスを限定。
- 境界防御の徹底：車外ネットワークから車内制御系 (CAN等) ネットワークへの不正侵入を遮断するネットワーク分離構成の採用

(2) 完全性 (Integrity)

データおよび支援情報の改ざんを防止し、システムの真正性を担保する。

- 改ざん検知機能の実装：メッセージ認証コード (MAC) やデジタル署名による、データ送信時の整合性確認。
- 相互認証の実施：システム間通信において、接続先が正当な機器であることを確認する相互認証プロトコルの採用。
- 異常検知時の安全制御：不正操作やデータの不整合を検知した際、直ちに警告を発し、車両を安全状態に移行させる制御。

(3) 可用性 (Availability)

- 遠隔支援・自動運転の継続性を維持し、障害時でも安全を担保する。
- 冗長化設計：単一障害点（SPOF）を排除したシステム構成およびフェイルオーバー機能の確保。
- MRM：通信遮断やシステム異常時に、車両を安全に停止・維持させるセーフモード設計。
- QoS（通信品質）制御：帯域制限や高負荷時においても、安全維持に必要な最小限の通信・機能を優先的に確保。

また、本システムは遠隔支援において一部のデータにリアルタイム性が要求されることを踏まえ、情報セキュリティの確保に加え、セキュリティ対策がシステムの性能・遅延・運用性に与える影響を考慮した設計を行う。具体的には、通信遅延や処理負荷が遠隔支援判断に影響を与えないよう、以下の方針に基づき設計する。

・データの重要度および用途に応じてセキュリティ適用レベルを分離する（例：制御系・イベント通知は高信頼・低遅延を優先し、ログ・分析系は高強度を優先）

・リアルタイム性が求められるデータについては、認証・暗号処理の方式や頻度を最適化し、遅延を抑制する

・映像・ログ等の高帯域データについては、制御系通信と論理的に分離し、セキュリティ処理による負荷影響を局所化する

これらを踏まえ、セキュリティ強度と処理性能・運用負荷とのトレードオフを考慮したリスクベースの設計とする。上記のセキュリティ基本方針は、アーキテクチャ設計において、認証・認可、通信保護、通信分離、権限管理、監査ログの各要素として反映する。具体的な反映箇所を表2に示す。

表4 セキュリティ基本方針とアーキテクチャ設計への反映箇所

観点	セキュリティ方針	アーキテクチャ設計への反映
認証・認可	正当な利用者・システムのみアクセス可能とする	遠隔監視コンソール、データ流通システム、外部情報連携システム間のAPI接続に対し

観点	セキュリティ方針	アーキテクチャ設計への反映
		て、OIDC／OAuth 2.0 による認証・認可を適用
通信保護	通信経路上の盗聴・改ざんを防止する	車両－遠隔監視コンソール間、データ流通システム－遠隔監視コンソール間の通信に暗号化および相互認証を適用
権限分離	利用者・システムの役割に応じて操作範囲を制御する	遠隔監視者、管理者、監査者等の役割に応じて、車両情報の参照範囲や支援操作権限を分離
通信分離	高帯域通信と安全関連通信の相互影響を抑制する	映像・音声等のリアルタイム配信系通信と、遠隔支援リクエスト・応答結果等の支援系通信を論理的に分離
可用性	通信障害・高負荷時にも重要情報を優先する	MRM通知、遠隔支援リクエスト、車両状態データ等の安全関連情報を優先的に処理・表示する構成
監査性	障害・不正発生時に追跡可能とする	遠隔支援操作、認証履歴、APIアクセス、支援結果等を監査ログとして記録

4.2 認証・認可

4.2.1 利用者認証（SSO）

遠隔監視センターのコンソール（遠隔監視コンソール等）に対する利用者認証は、OIDC（OpenID Connect）によるSSOを前提とする。利用者は外部IdPで認証され、コンソールは認証結果として発行されるIDトークン／アクセストークンを用いてバックエンドAPIへアクセスする。

APIアクセスは OAuth 2.0 Bearer Token を基本とする。これは、Web/API間の認証・認可におけるデファクトスタンダードであり、既存のクラウド基盤やセキュリティ機構（Id

P、API Gateway等）との親和性が高く、相互運用性および実装容易性を確保できるためである。認証はAuthorization: Bearer <access_token> により実施する。アクセストークンの有効期間は短期間(例：1時間程度)とし、期限切れ時はリフレッシュトークンまたは再認証により継続性を確保する。必要に応じてMFA等の認証ポリシーはIdP側で統制する。

4.2.2 システム認証

各システム間通信およびデータ連携においては、接続主体（サービス／デバイス）を識別するための機械認証を実施する。

サービス間通信はOAuth 2.0（Client Credentials）によるトークン認証を基本とし、各サービスは発行されたアクセストークンを用いてAPIアクセスを行う。

4.2.3 認可

認可はRBAC（役割ベースアクセス制御）を基本とし、利用者の役割（例：遠隔監視者／管理者／監査者）および運用スコープ（例：事業者、拠点、車両単位）に基づき実施する。これにより、参照可能な車両情報や実行可能な操作（監視、支援、管理設定等）を明確に分離し、権限逸脱を防止する。

リアルタイム通信（WebSocket等）を利用する場合は、接続時の認証に加え、接続後の購読範囲（車両ID、データ種別）を権限に基づいて制御し、許可された範囲のみデータ配信および操作を可能とする。

4.3 通信の保護

本システムでは、通信内容の機密性および完全性を確保するため、通信の用途や特性に応じた保護方式を採用する。特に、遠隔支援運行に関わる通信は用途ごとに要求特性（低遅延性、信頼性、帯域特性等）が異なるため、画一的な方式ではなく、通信種別に応じた保護を行う。

4.3.1 管理・制御系通信（API／状態通知）

運行管理、車両状態取得、助言指示等の管理・制御系通信は、HTTPSを基本とし、TLS（TLS1.2以上）による暗号化を行う。

これらの通信は、認証・認可と密接に関係するため、OAuth 2.0 Bearer Token による認証とRBACに基づく認可を組み合わせる実施する。

通信の信頼性および可用性を確保するため、再送制御やタイムアウト、リトライ方針を適切に設計し、障害時の影響範囲を限定する。

4.3.2 リアルタイム配信系通信（映像・音声・イベント）

遠隔映像、音声通話、アラート通知等のリアルタイム配信系通信は、TLS上でのWebSocket（wss）等を用いて実現する。接続時にトークンによる認証を行い、接続後は購読単位（車両ID、データ種別）で配信範囲を制御する。低遅延性が求められる通信については、通信経路やプロトコルの選択により、制御系通信と論理的に分離し、相互の影響を抑制する。

4.3.3 データ連携系通信（プローブ情報・路側情報）

車両プローブ情報や路側デバイスからの交通環境情報など、データ連携系通信は、TLSにより暗号化された通信経路を基本とする。データ連携基盤を介した連携においては、提供元・提供先を識別可能な認証方式を用い、許可された範囲のみデータを受け渡す。データ量が大きい場合や遅延許容度が高い場合は、管理・制御系通信と分離したチャンネルを用い、帯域制御や負荷分散を行う。

4.3.4 通信分離および障害影響の限定

上記の通信については、用途や特性に応じて論理的な分離を考慮し、特定の通信における障害や負荷が他の通信へ過度に影響を与えない構成とする。

特に、映像・音声等の高帯域通信については、運行管理や制御系通信の安定性を損なわないよう、通信方式や制御方法の選定により影響の抑制を図る。これにより、遠隔支援運行全体としての安定性確保を目指す。

4.4 監査ログ

運用時の追跡可能性を担保するため、監査ログを取得・管理する。

監査ログには、利用者の操作履歴、認証・認可の結果、主要なシステムイベント等を記録し、障害時の原因分析、不正アクセスの検知、事後検証を可能とする。複数システムを横断した調査が必要となるため、相関ID等によりログを関連付け可能な形で保持する。

5. 非機能要件

本章では、全国規模での遠隔支援運行を安定的に実現するために必要となる非機能要件について整理する。

本システムは、複数車両・複数拠点での同時運用や1対N運用を前提とするため、機能要件に加えて、可用性、性能、拡張性、運用性を考慮した設計とする。

5.1 可用性・冗長化

遠隔支援運行においては、システム障害が運行全体へ影響を及ぼす可能性があるため、可用性を重要な非機能要件と位置付ける。

特に、遠隔監視センター側のシステムやデータ連携基盤など、複数車両に影響を与える構成要素については、単一障害点とならない構成を考慮する。

現実的な運用や既存システム構成を踏まえ、完全な冗長化を前提とするのではなく、障害発生時の影響範囲を限定し、運行継続や迅速な復旧が可能な構成を考慮する。本要件は、3章で示した疎結合構成、通信種別ごとの分離、および2.1.1項で示した安全設計方針に基づき、障害発生時の影響範囲を局所化することで実現する。さらに、遠隔支援は車両側の自律判断を補完する機能であるため、利用不能時には車両側が必要に応じてMRM等の安全側挙動へ移行できることを前提とする。これにより、遠隔支援システム自体が安全上の単一障害点とならない構成とする。

5.2 性能要件

遠隔支援システムにおいては、遠隔監視者が適切な状況認識および助言を行うために必要な応答性および情報提供の即時性を性能要件として重視する。

特に、車両位置・状態や映像ストリーム等の動的データについては、単なる通信遅延時間だけでなく、遠隔支援における判断成立性との関係で評価する必要がある。

本設計における遅延要件は、既存の遠隔監視実証および国際標準を踏まえて整理する。成田空港における遠隔監視実証³⁾では、映像伝送のエンドツーエンド遅延は400 ms以内とされており、遠隔監視が成立する映像伝送性能の参考値が示されている。一方、本事業では遠隔監視に加えて遠隔支援（助言）を対象とするため、映像の遅延だけでなく、車両位置・状態情報の遅延によって生じる空間的な位置ずれを考慮する必要がある。

このため、ISO 7856:2025における遅延に起因する距離誤差（Serr / DEDTL）の考え方を参考とし、DEDTL 3 m以下（通常条件）を満たすことを条件として、遅延時間および更新

周期を設定する⁴⁾。本事業では、一般道を走行する自動運転バス（最高時速40 km程度）を想定するため、単純な映像遅延時間ではなく、車速に応じた遅延起因の距離誤差を評価指標として用いる。これにより、車速条件が異なる場合でも、遠隔監視者が参照する車両位置・状態情報と実際の車両状態との空間的なずれを一定範囲内に抑えることを設計上の目安とする。

一方、路側物標情報⁵⁾や車両プローブ情報⁶⁾等の準動的データについては、外部システムにおける更新周期が情報種別ごとに異なる。これらは各システムの用途に応じて設計されるものであり、必ずしも遠隔支援に必要な更新周期と一致するものではない。そのため、本設計では、外部システムの仕様をそのまま適用するのではなく、遠隔支援における利用目的および時間変化の特性に応じて、以下のように扱う。

- ・ 遠隔支援判断に直接用いるデータ

車両位置・状態、遠隔支援リクエスト、重要イベント通知等については、遠隔監視者の状況把握および助言判断に直接影響するため、即時性および到達性を重視する。

- ・ 状況認識を補完するデータ

路側物標情報、車両プローブ情報等については、車両単体では把握しにくい死角情報や先読み情報として活用するため、一定時間内に情報が有効であること、ならびに他データとの時間的整合性を重視する。

- ・ 運行判断を支援する参照系データ

運行管理情報、気象、規制情報等については、即時性よりも正確性、一貫性、更新時点の明確性を重視する。

これにより、すべてのデータに一律の更新周期を設定するのではなく、遠隔支援判断への影響度、データの時間変化特性、通信負荷を踏まえて、データ種別ごとに適切な鮮度・遅延要件を設定する方針とする。

上記の観点を踏まえて、主な動的データに対する性能目安については、参照資料「データ連携による先読み情報を活用した遠隔支援システム データ要件定義素案：5.2 データ種別ごとの更新周期・遅延目安」に基づき、仮値として整理する。現時点の実証条件および適用対象を踏まえ、自動運転バスレベルの運行（一般道・最高時速40 km）を前提とした目安として整理する。また、本数値は先読み型遠隔支援機能の成立を前提とした上位要件として定

義するものであり、各システム間における個別の更新周期や処理遅延の内訳については、本章の検討対象外とする。なお、これらの数値は今後の実証結果や運用条件に応じて見直すことを前提とする。

主な動的データに対する性能目安

- 車両位置・状態データ(動的データ)
更新周期：100～200 msを基本目安
許容条件：ISO 7856のSerr/DEDTLの考え方にに基づき、遅延に起因する距離誤差（Serr）3m以下を満たすこと
用途：路上駐車回避、停車判断、再発進判断等
- 映像ストリーム(動的データ)
更新頻度：15 fps以上を基本
高精度な状況確認が必要な場合：30 fpsを推奨
イベント発生時の更新：0.1秒以内
用途：現場状況の視覚確認、周辺車両・障害物・信号状況の把握
- 路側物標情報 / 信号機状態/車両プローブデータ(準動的データ)
更新周期：0.5～1秒程度
用途：障害物有無判定、交差点進入可否判断

車両管理情報や気象・規制情報等の準静的データについては、即時性よりも信頼性・一貫性を重視する設計とする。また、高帯域データ（映像・音声・ログ）の通信・処理については、用途や優先度に応じて管理・制御系や安全関連情報の処理と論理的に分離し、通信量や処理負荷の変動があっても、遠隔支援運行の中核となる判断機能の性能を安定して維持できる構成とする。³⁾⁴⁾⁵⁾⁶⁾

なお、人の判断スピードとデータの変化特性を踏まえると、0.5秒より細かい更新は効果が限定的であるため、本検討ではこの値を更新周期設計の下限の目安としている⁷⁾。

3) 空港における遠隔監視型自動運転に向けた通信冗長化設計による映像監視技術の実現

4) ISO 7856:2025 Clause 9~10

5) ITS FORUM RC-019 1.0版

6) 実証実験用 車両情報連携システム 要求仕様書(仮仕様)

7) 人の判断スピードとデータの変化特性を踏まえると、0.5秒より細かい更新は効果が限定的であるため、この値を下限としています。

5.3 スケーラビリティ

本システムは、車両台数や運行エリアの増加、ならびに1対N・M対N運用の拡大を前提とし、運用単位の増加に対して段階的に対応可能な構成とする。アーキテクチャ上は、図2に示す通り、自動運転車両、データ連携基盤、遠隔監視コンソールを独立した構成要素として分離し、車両単位・運行単位・データ種別単位で処理および通信を管理できる構成とする。特定の車両や拠点が追加された場合でも、車両ID、便ID、遠隔支援リクエストID等により対象を識別し、影響範囲を限定して処理できる構成とする。また、路側情報や車両プローブ情報等の外部情報は、データ流通システムを介して遠隔監視コンソールへ提供することで、地域や情報源の追加に対しても、遠隔支援側の基本構成を大きく変更せずに対応可能とする。

遠隔監視コンソール側では、複数車両の状態、異常種別、対応要否、緊急度／優先度等を集約し、遠隔監視者が優先対応対象を判断できる情報構造を提供する。これにより、車両台数や運行エリアの拡大に対して、システム全体を一括で変更するのではなく、構成要素ごとに段階的に拡張可能なアーキテクチャとする。

5.4 運用・保守

本システムは、複数事業者・複数システムによる継続的な運用を前提とし、運用・保守においても疎結合な構成を基本とする。各構成要素は可能な限り独立して運用・保守が行えるよう設計し、特定のシステム変更や障害対応が他のシステムや運行全体へ過度に影響を与えないことを重視する。システムの状態把握および障害対応を円滑に行うため、各システムは監視、ログ、アラートを通じて自身の状態を把握可能とし、必要に応じて関係者間で情報共有が行える構成とする。特に、高頻度・大容量のログ（映像・音声、デバッグログ等）の収集経路と、システム障害やセキュリティに関わるクリティカルなアラート通知経路とは論理的に分離し、アラートの確実な配信とリアルタイム性を担保する。

また、構成変更や機能追加、保守作業については、運行への影響を最小限に抑えるため、段階的な適用や切り戻しが可能な運用を考慮する。これにより、個別システムの更新や運用改善を柔軟に行いながら、遠隔支援運行全体としての安定運用を維持する。

6. 将来拡張および展開方針

6.1 1対N運用への対応

将来的な複数車両同時監視を前提とし、遠隔監視者1名が複数車両を効率的に監視・支援可能な構成への高度化を図る。そのため、各車両の状態、異常種別、対応要否、優先度等を識別可能とするデータ構造を前提とし、遠隔監視者が優先対応対象を判断可能な情報基盤を整備する。

本事業検討では、遠隔支援動作に有効なデータ構成およびインターフェースを整理するとともに、それらの情報を活用した1対N遠隔監視・遠隔支援に関わる基本的なUI構成および操作フローについて、コンセプトレベルで整理した。

これらについては、相互運用性および運用の再現性を確保する観点から、以下の基本構造を共通化対象とする。

- ・ 複数車両の状態を一覧で把握する俯瞰表示（車両一覧・マップ等）
- ・ 特定車両の詳細情報を確認する個別表示（車両状態、周辺環境、先読み情報等）
- ・ 車両またはシステムからの遠隔支援リクエストの通知および提示
- ・ 遠隔監視者による支援判断（承認／却下等）を行う基本操作フロー

これらは、遠隔支援動作シーケンス（状態把握 → リクエスト → 判断 → 対応）に対応する基本的な構成要素として位置付ける。

なお、具体的な画面レイアウト、情報配置、操作方法等の詳細については、各事業者の運用方針およびサービス設計に依存するため、競争領域とする。

具体的には、以下の観点で段階的な改善を行う。

- 安全関連イベントの優先度制御および表示集約
- 車両単位ではなく運行単位での状況把握
- 異常兆候の早期検知および通知方式の改善
 - 個別通知に加え、複数車両に対する共通通知・一斉通知の仕組みの整備
 - 複数車両への一斉指示・制御を可能とする運用機能の検討
 - 運行状況に応じた担当者の動的切替および負荷分散の仕組みの導入
- 遠隔監視者の負荷を考慮したUI/UXの最適化

これにより、車両台数の増加に伴う業務負荷の過度な増大を抑制するとともに、個別対応中心の運用から、複数車両を横断した効率的な運用への拡張を可能とする。

6.2 通信・セキュリティの高度化

運用実績およびリスク評価を踏まえ、通信方式、認証・認可、ログ管理等を含むセキュリティ全体の見直しを段階的に実施する。これにより、運用拡大および脅威環境の変化に対して継続的に適応可能な構成とする

特に以下を見直し対象とする。

- 通信経路の冗長化および品質制御の高度化
- トークン管理方式の強化および有効期限管理の最適化
- アクセス制御粒度の細分化
- 監査ログの統合管理および分析機能の強化

6.3 標準化と競争領域の整理

先読み型遠隔支援機能を利用するバス運行事業者および、本アーキテクチャに基づく各システムを保有・提供する関係事業者は、標準化されたインターフェースおよびデータフォーマットを前提とし、標準化・規格化動向を踏まえながら、協調領域と競争領域の整理を関係主体間で継続的に見直すものとする。

協調領域については、相互運用性を確保するため、データ形式、イベント定義、基本的なUI構成等の共通化を進める。

一方、競争領域については、各事業者が独自に高度化可能な判断ロジック、UI/UX、運用ノウハウを確保し、差別化を可能とする。これにより、標準化と競争優位性の両立を図る。本整理は、将来的な全国展開を見据え、継続的に見直しを行う。