

先進モビリティサービスのための情報通信プラットフォームに関する コンソーシアム成果報告会

実証実験環境（柏の葉・高蔵寺・けいはんな）

名古屋大学大学院情報学研究科

助教

山田峻也

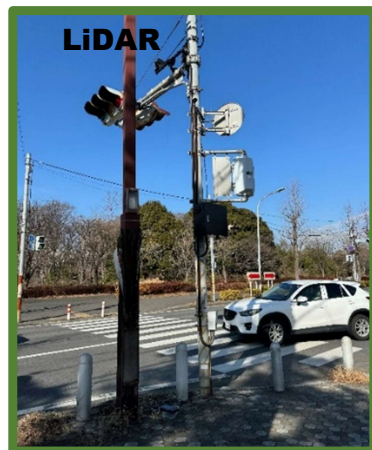
実証実験環境について

- 自動運転車のセンサーの死角が発生しやすく，協調型路側機の情報が必要となるユースケースでの自動運転車の安全・円滑走行支援の検証を実施
- 想定したユースケース
 - 交差点での右左折，駐車場での駐車
- 実証実験を実施した地域
 - 柏の葉，高蔵寺，けいはんな

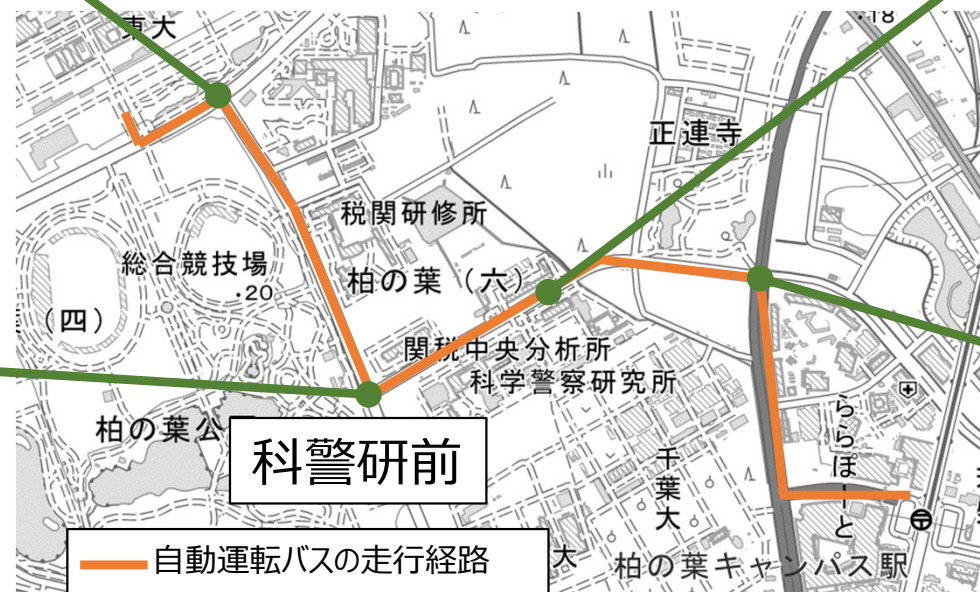


柏の葉：協調型路側機の概要と実証内容

- 柏の葉キャンパス駅から東大柏キャンパスまでの走行経路に協調型路側機を設置
- 協調型路側機の支援による自動運転バスのレベル4 走行の実現可能性を検証
- まずは協調型路側機だけで十分な安全性を確保できるように設置を進めており、コストと性能のトレードオフのバランスを見極めながら最適化を図る予定



自動運転バス



高蔵寺：協調型路側機の概要と実証内容

- ・ 愛知県春日井市高蔵寺ニュータウン内に協調型路側機を設置
- ・ 住宅密集地で自動走行するL2自動運転カートにおいて，協調型路側機を活用し，人の介入が必要な箇所を自動化できるかを検証中
- ・ 公共施設駐車場において，自動バレーパーキングの実現に向けた検証を実施



自動運転カート

公共施設駐車場
(グループふじとう)

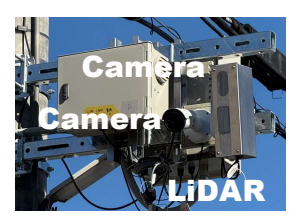


石尾台小学校
北西交差点

スクランブル式の信号交差点

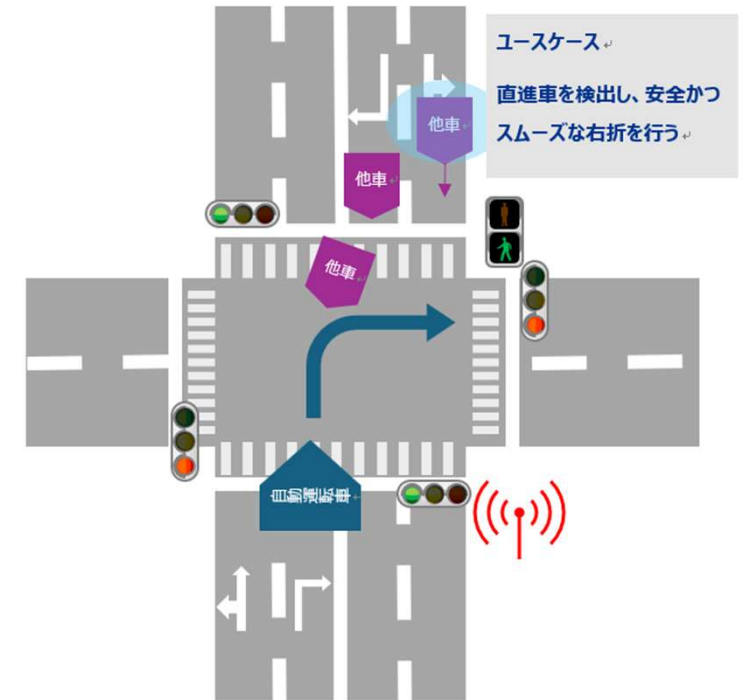


無信号交差点



けいはんな：協調型路側機の概要と実証内容

- けいはんなオープンイノベーションセンター前の交差点に協調型路側機を設置
- 自動運転カートが右折する際に死角となる直進対向車を検出することで、安全かつ円滑な右折が実現可能かを検証した
- コンソーシアム参加企業である富士ソフトが担当し、コンソーシアムの成果物が活用された



自動運転カート

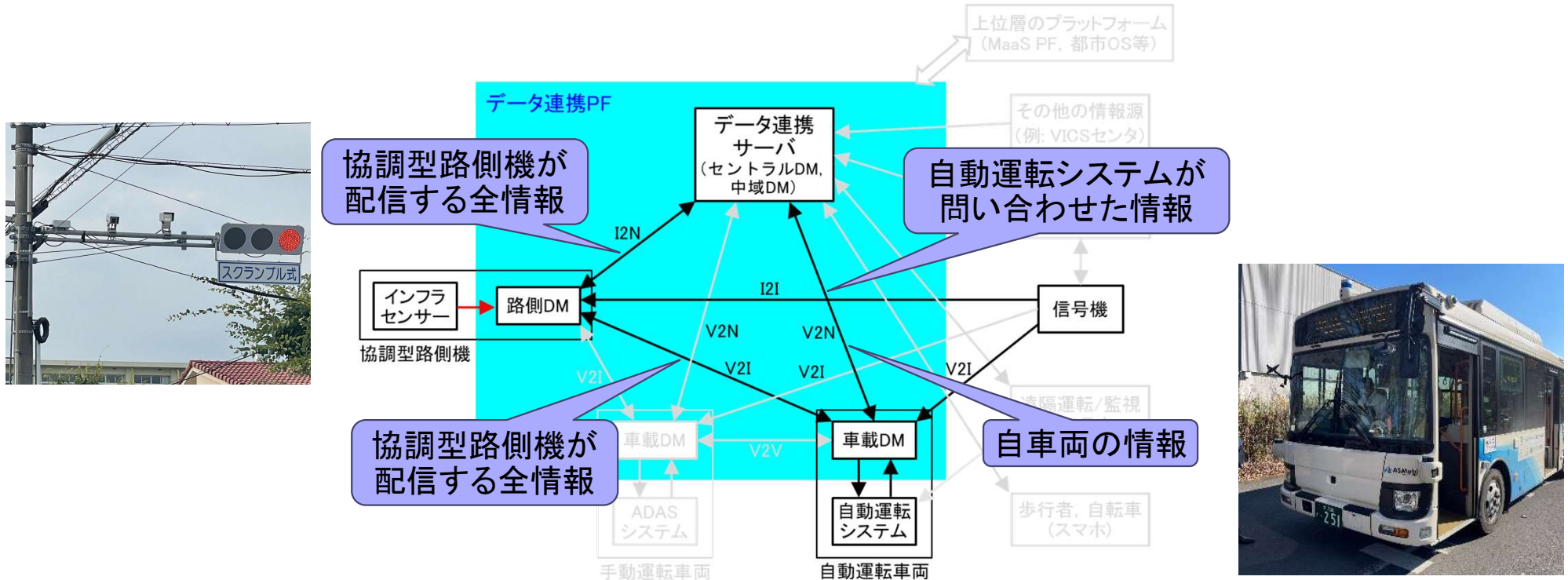
京都スマートシティ推進協議会レポート、「複数モビリティの協調運行に関する実証を実施」より



Google street viewより

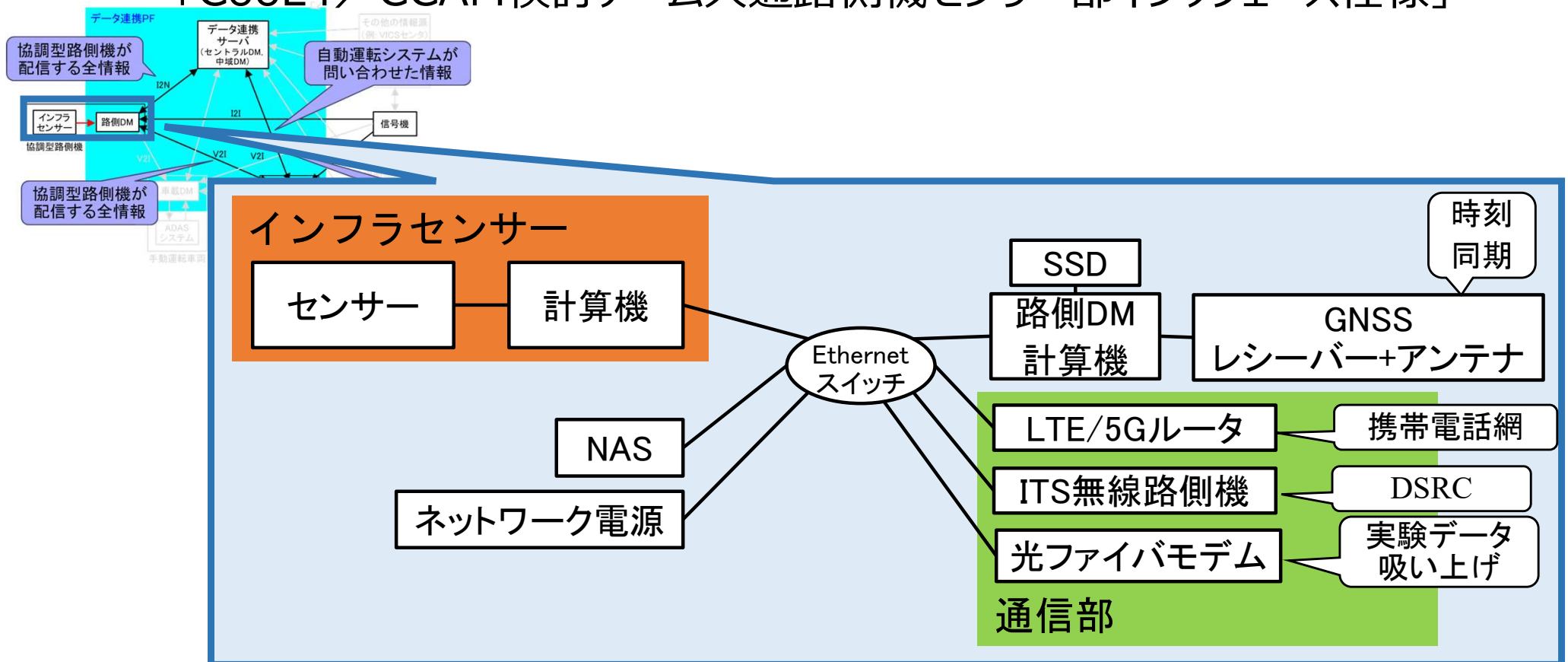
実証実験でのシステム構成

- データ連携サーバー：
 - 協調型路側機や自動運転車が配信する情報を統合的に管理
- 自動運転車：
 - DSRCを使ったブロードキャスト通信：
 - 協調型路側機が配信する全情報を直接取得
 - 携帯電話網：
 - データ連携サーバーから必要な情報を取得，自車両の情報を出力



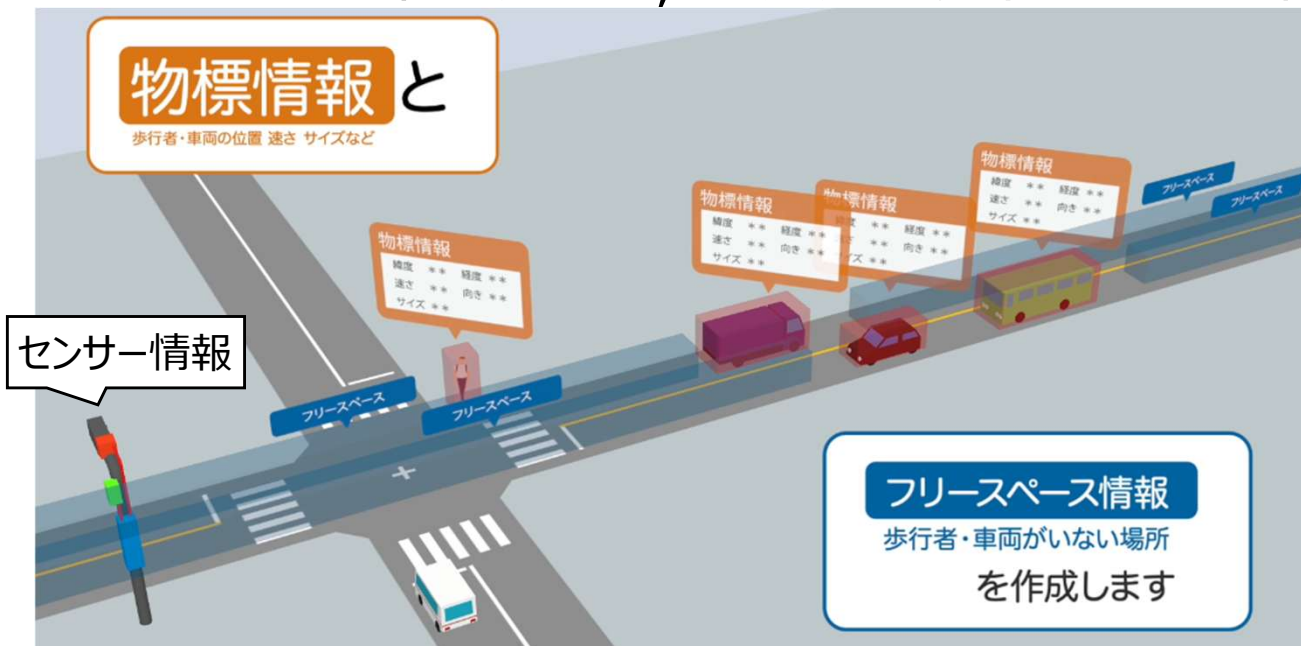
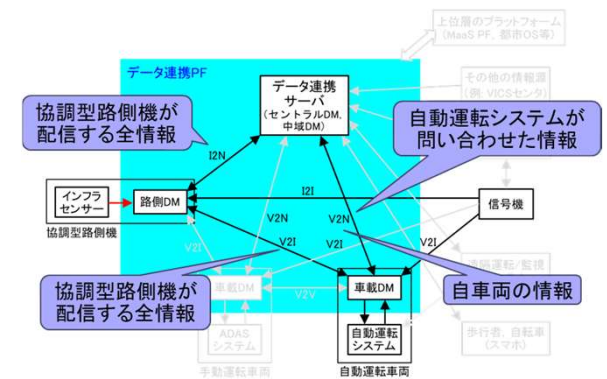
協調型路側機のシステム構成

- 通信部には，3つの通信機器を搭載
- インフラセンサーには複数のセンサーメーカーの製品を使用 ←6社の導入実績あり
- インフラセンサーから路側DMに送信される情報には，ITS Japan CCAM検討チームと共同で策定したフォーマットを使用
 - 「CooL4／CCAM検討チーム共通路側機センサー部インタフェース仕様」



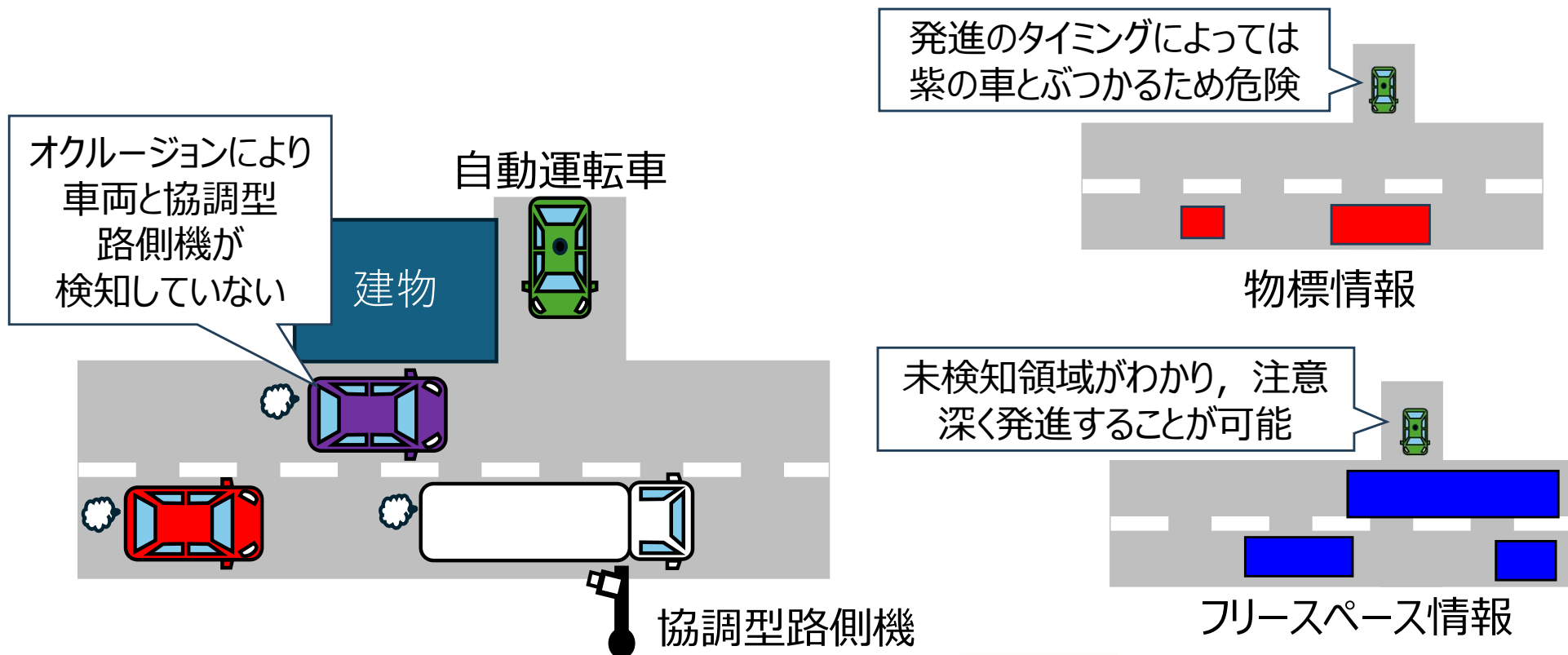
協調型路側機が配信する情報

- センサ情報・物標情報・フリースペース情報・信号情報
 - センサー情報：
 - 設置位置，検知範囲，稼働状態など
 - 物標情報：
 - 物標の種別・位置・サイズ・速度・精度など
 - フリースペース情報：
 - 物標が存在しない領域
 - 信号情報：
 - 現在の灯色と，次の灯色変化の予定時間



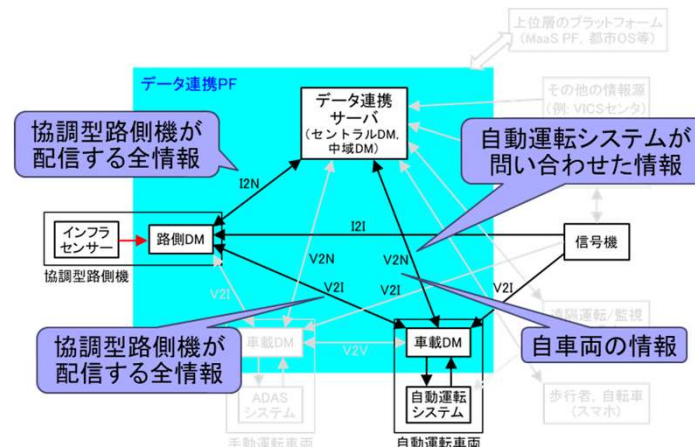
フリースペース情報について

- 多くの実証実験では、物標情報の共有のみにとどまる例が多い
 - オクルージョン領域にある車両情報は、取得・共有されない可能性があり、これは安全上のリスクとなる
- 自動運転車は、安全に進行可能なフリースペースの情報をもとに走行
 - 路側インフラ側でフリースペース情報そのものを共有するほうが直接的であり、衝突回避や経路計画の精度を高め、安全性を向上させる可能性がある



実証実験環境のまとめ

- 柏の葉，高蔵寺，けいはんなの3つの地域で，協調型路側機を活用した自動運転車の安全・円滑走行支援の検証を実施
- インフラセンサーから路側DMに送信する情報(→)
 - ITS Japan CCAM検討チームと共同で策定した共通フォーマットを使用
 - RoAD to the L4およびITS JapanのWEBサイトにて公開
 - Cool4/CCAM検討チーム共通路側機センサー部インタフェース仕様
 - https://www.road-to-the-l4.go.jp/activity/theme04/pdf/Cool4_SensorInterfaceSpecification_ver110.pdf
- 路側DMから配信される情報 (→)
 - センサ情報・物標情報・ freespace情報・信号情報
 - API仕様はRoAD to the L4のWEBサイトにて公開
 - Cool4 データ連携PF API仕様
 - https://www.road-to-the-l4.go.jp/activity/theme04/pdf/Cool4_DataIntegrationPF_API_Specification_v090.pdf



先進モビリティサービスのための情報通信プラットフォームに関する コンソーシアム成果報告会

フュージョン

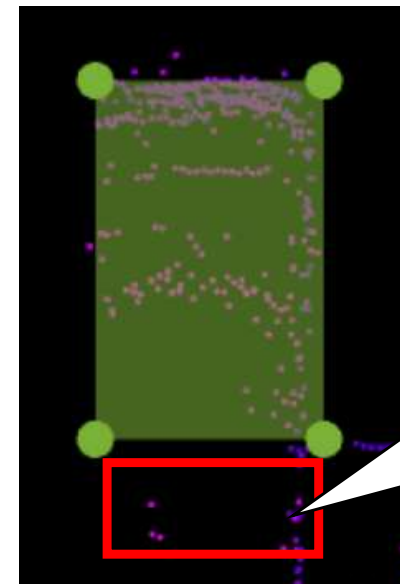
名古屋大学 未来社会創造機構
研究員
川田 福和

単体の路側機による物標認識を運用する際の懸念

- 画角によっては物標の全体を観測することができないことがある
- この状態で推定した物標の外接矩形は，物標全体を観測した場合と比較して小さくなり，その物標位置もずれる
- この情報を頼りに自動走行を行うと衝突事故につながるおそれがある



車両全体を観測している場合

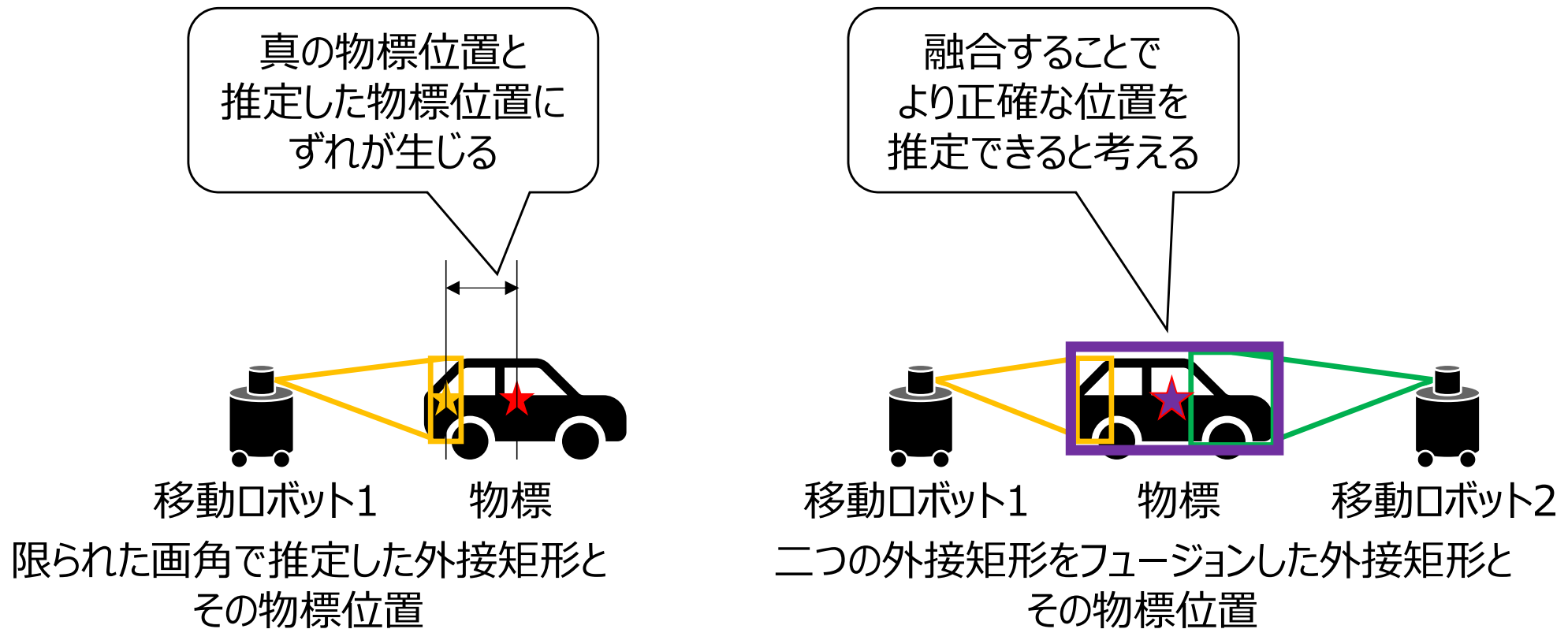


車両後方の
情報が欠けて
いる

車両の一部を観測している場合

複数の視点から得られた物標情報を融合する案

- ロボット分野では、複数の視点から検知した物標情報をフュージョンしその物標位置を推定する方法*が提案されている
- この考え方を路側機（Road Side Unit: RSU）に導入する活動をしている
 - 正確な測位により安全な自動走行を支えるため



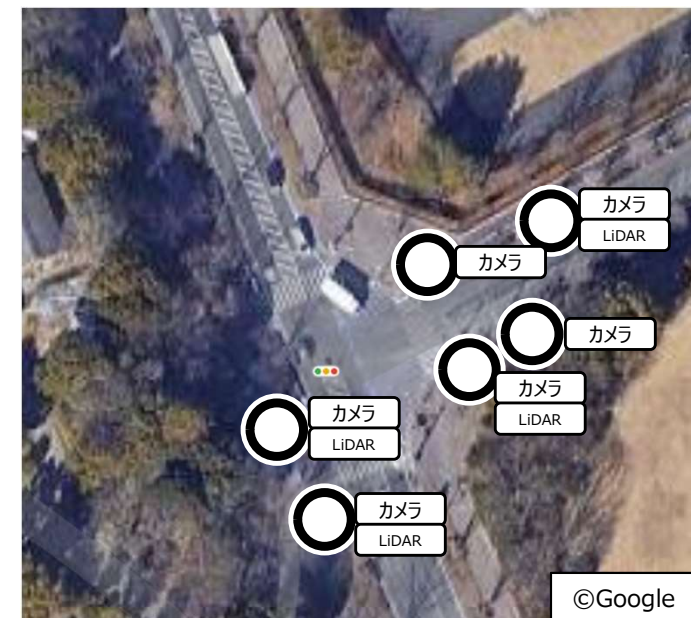
*泉, 橋本, 田村, 高橋 : 複数台の移動ロボットによるレーザ距離計測に基づく移動物体大きさ・姿勢推定法;
日本機械学会論文集, Vol. 81, No. 827, pp.14-00388-14-00388 (2015)

複数の路側機で観測できる環境で検証

- 愛知県春日井市石尾台小学校北西交差点
 - 2台の路側機
 - 走行車両の自己位置と観測領域の比較実験を実施(2023年, 2024年)
- 東京大学柏の葉キャンパス周辺の丁字路
 - 6台の路側機
 - 歩行者の参照位置と観測位置の比較評価を実施 (2025年)



愛知県春日井市
石尾台小学校北西交差点



柏の葉キャンパス周辺
丁字路

2023年から現在までのフュージョンに関する取り組み

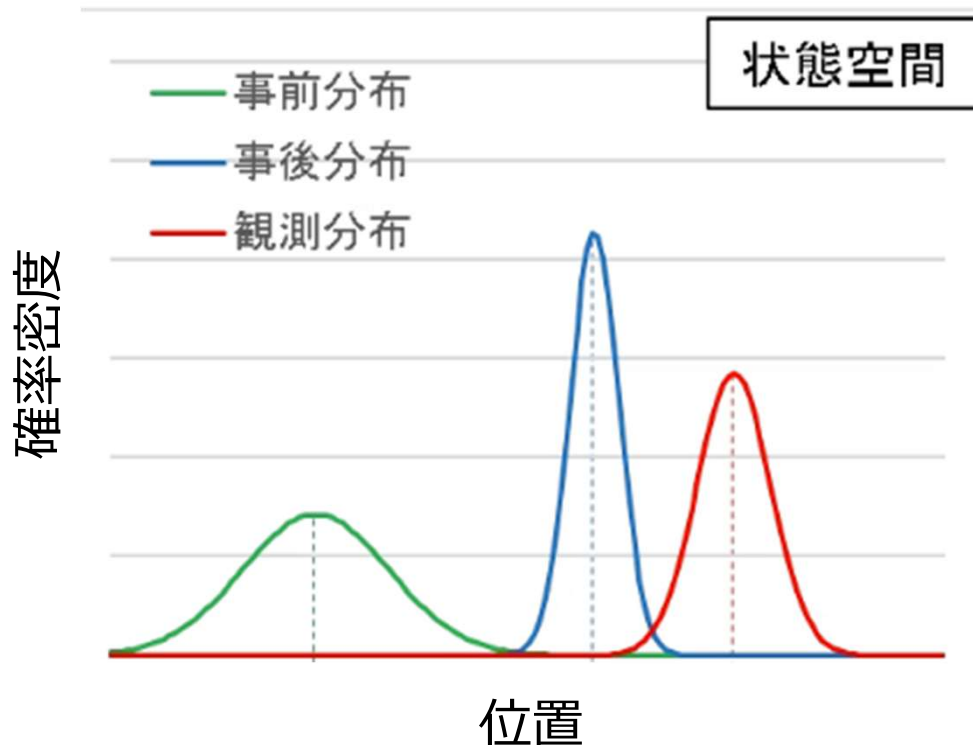
- 等速直線運動で線形な動作をサポートするフュージョン機能から始めた
- その後、速度が変化したり非線形（旋回など）な動作をする対象をサポート
- 現在はこれまで仮で設定していた誤差の事前知識をデータから学習して用いる取り組みをしている

これまでのフュージョンに関する取り組み

年度	対応動作モデル	カルマンフィルタ	誤差の事前知識
2023年度	等速直線運動	線形	仮の値
2024年度	停止・一定速度・直進加速	線形・非線形	仮の値
2025年度	継続	継続	データから学習した値

融合に用いる基本的なアルゴリズム：線形カルマンフィルタ

- 正規分布仮定の事前データ(事前分布)と観測結果(観測分布)からより精度が良いと思われる事後のデータ(事後分布)を得る手法
 - 精度高い：誤差の平均や分散が小さいこと
- 古くはミサイル兵器，最近はロボットや自動運転車両の位置の推定などに用いられてきた



事後分布

$$= \text{事前分布} + K (\text{観測分布} - H \text{事前分布})$$

K: カルマンゲイン

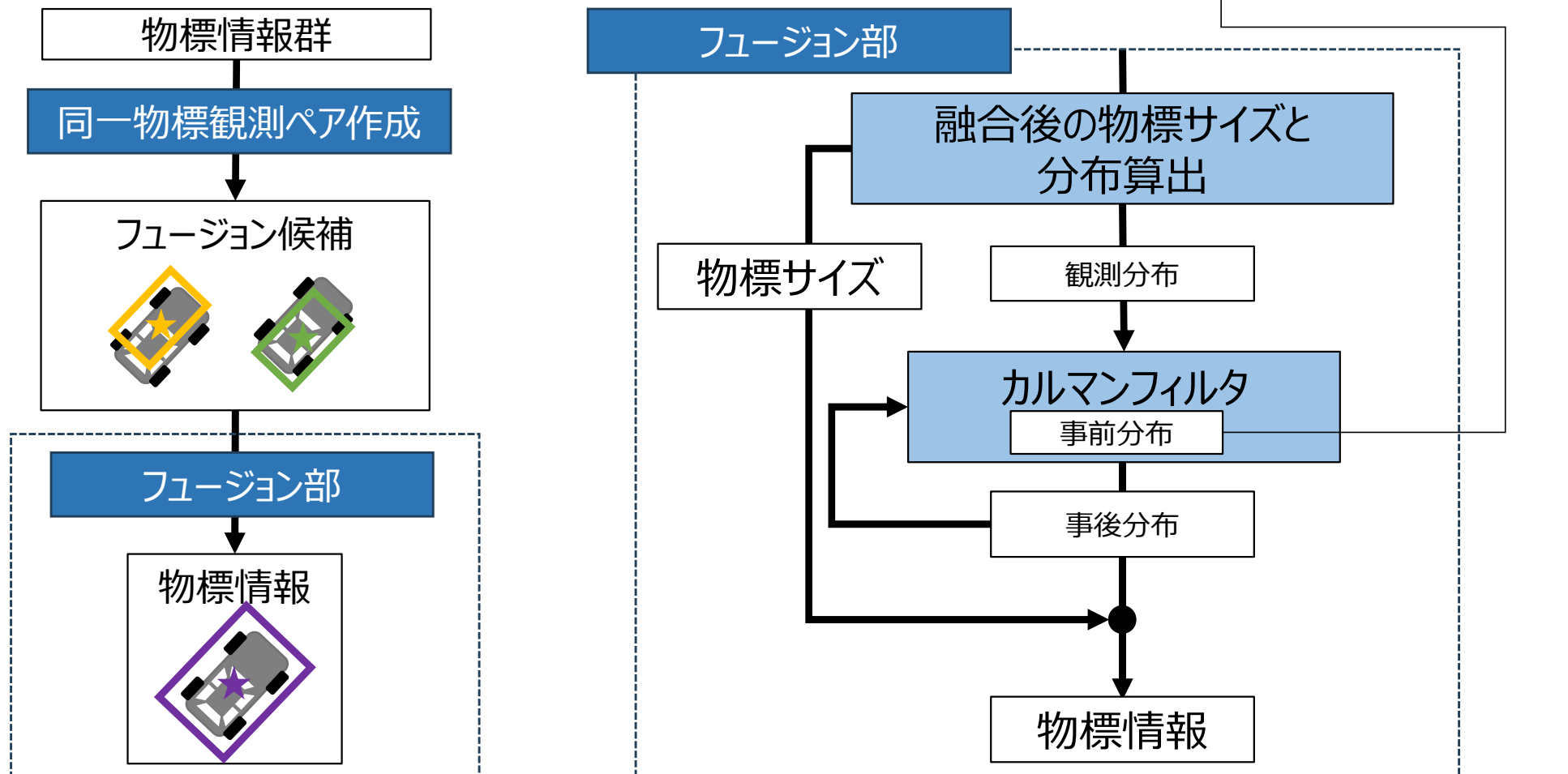
誤差が最小になるような値 = 分散が最小になる値

H: 観測行列 (事前分布から観測結果を抽出)

<https://qiita.com/MoriKen/items/0c80ef75749977767b43>

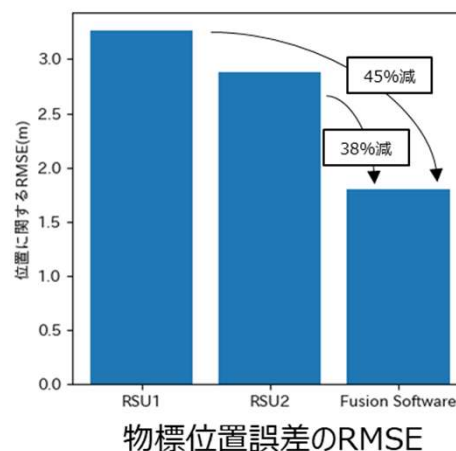
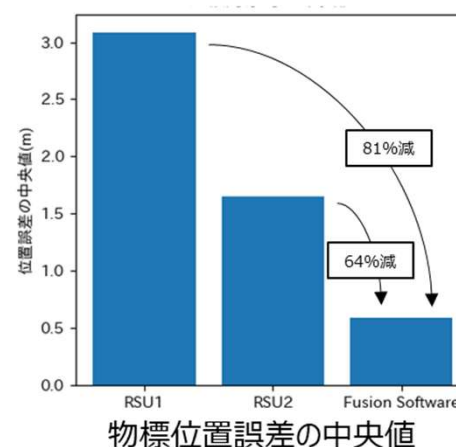
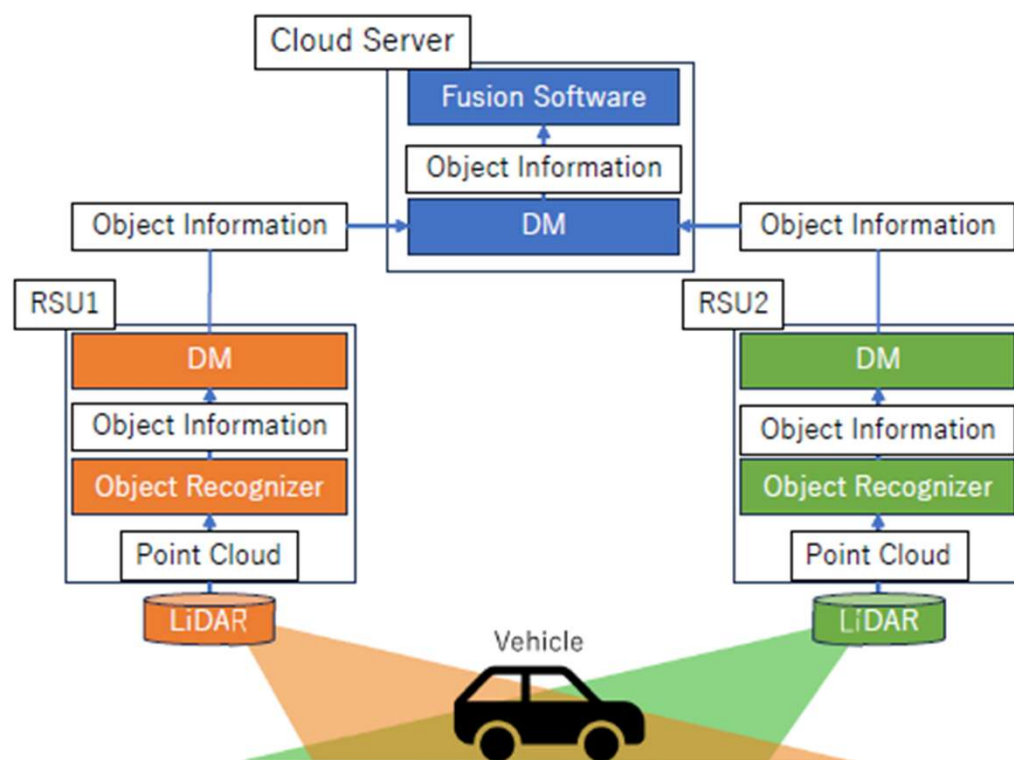
本研究におけるカルマンフィルタの使用方法

- 二つのセンサから得られた物標情報をフュージョン部に入力
- カルマンフィルタに通して分布の登録・更新
- サイズを付与して物標情報とする



2023年度：等速直線運動・線形モデルのフュージョンシステムの構築

- 二台のRSUが認識した車両の情報をクラウドに配備したソフトで融合
- 誤差の中央値を抑える効果があることを確認
 - 処理前
 - 数メートルの誤差
 - 処理後
 - 0.5m程度

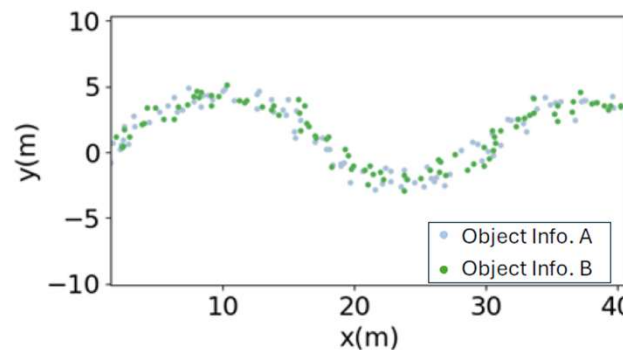


2024年度：3種の運動モデル・非線形動作対応

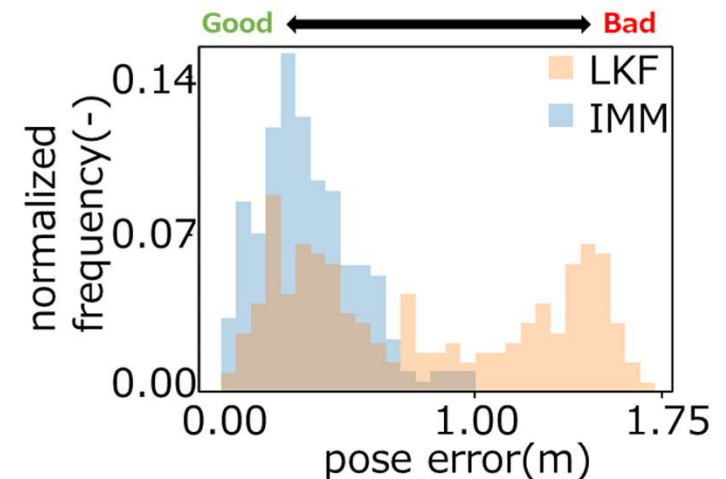
- Intracting Multimodel法（IMM法）を導入
 - 複数の運動モデルに基づく推定値を重みづけして融合する手法
 - 車両が行うと思われる動作の内, 下記モデルを使用した
 - 一時停止, 加減速, 等速直進
 - 拡張カルマンフィルタによる非線形動作の線形近似も実施
- 旋回を含むテストにおいて昨年度以上の位置精度が得られた
 - 従来：1m超
 - 今回：0.5m

$$f^1 \begin{pmatrix} x_t \\ y_t \end{pmatrix} = \begin{pmatrix} x_{t-\tau} + \Delta \hat{x} \tau \\ y_{t-\tau} + \Delta \hat{y} \tau \end{pmatrix}$$
$$f^2 \begin{pmatrix} x_t \\ y_t \\ \theta_t \\ v_t \\ \dot{\theta}_t \end{pmatrix} = \begin{pmatrix} x_{t-\tau} + \left(v_{t-\tau} \tau + \frac{1}{2} \Delta \dot{v}_{t-\tau} \tau^2 \right) \cos \theta_{t-\tau} \\ y_{t-\tau} + \left(v_{t-\tau} \tau + \frac{1}{2} \Delta \dot{v}_{t-\tau} \tau^2 \right) \sin \theta_{t-\tau} \\ \theta_{t-\tau} + \dot{\theta}_{t-\tau} \tau + \frac{1}{2} \Delta \ddot{\theta}_{t-\tau} \tau^2 \\ v_{t-\tau} + \Delta \dot{v}_{t-\tau} \tau \\ \dot{\theta}_{t-\tau} + \Delta \ddot{\theta}_{t-\tau} \tau \end{pmatrix}$$
$$f^3 \begin{pmatrix} x_t \\ y_t \\ \theta_t \\ v_t \\ \dot{v}_t \end{pmatrix} = \begin{pmatrix} x_{t-\tau} + \left(v_{t-\tau} \tau + \frac{1}{2} \Delta \dot{v}_{t-\tau} \tau^2 + \frac{1}{6} \Delta \ddot{v}_{t-\tau} \tau^3 \right) \cos \theta_{t-\tau} \\ y_{t-\tau} + \left(v_{t-\tau} \tau + \frac{1}{2} \Delta \dot{v}_{t-\tau} \tau^2 + \frac{1}{6} \Delta \ddot{v}_{t-\tau} \tau^3 \right) \sin \theta_{t-\tau} \\ \theta_{t-\tau} + \dot{\theta}_{t-\tau} \tau + \frac{1}{2} \Delta \ddot{\theta}_{t-\tau} \tau^2 \\ v_{t-\tau} + \dot{v}_{t-\tau} \tau + \frac{1}{2} \Delta \ddot{v}_{t-\tau} \tau^2 \\ \dot{v}_{t-\tau} + \Delta \ddot{v}_{t-\tau} \tau \end{pmatrix}$$

運動モデル



旋回を含むテストデータ

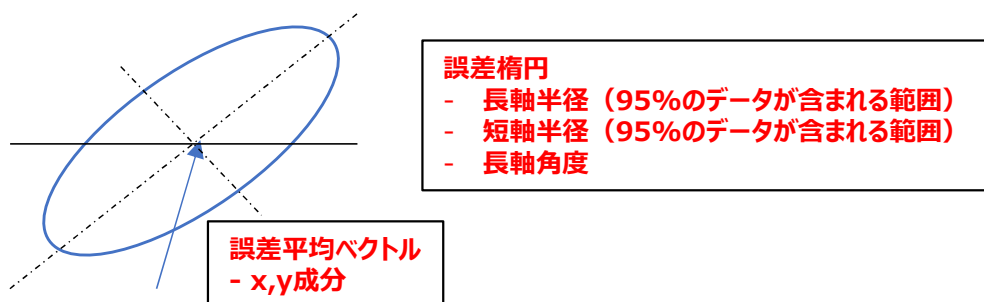


位置誤差分布

その他詳細はの情報交換会にてポスター展示します

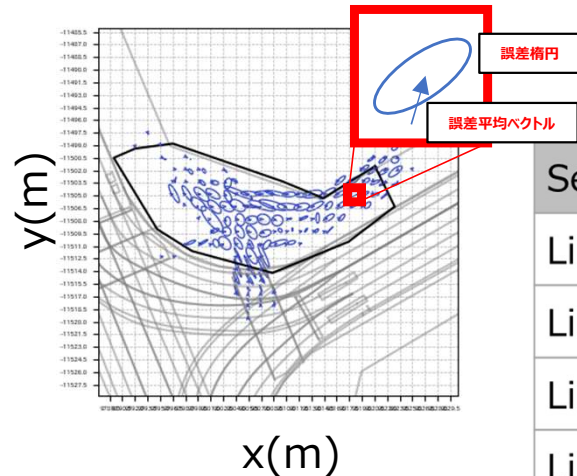
2025年度：実環境データから誤差モデルを構築（1/2）

- これまでの手法の共通の課題
 - **系統誤差を考慮していないこと**
 - カルマンフィルタで扱う誤差分布の平均は0であるとしている
 - 実際はセンサの取り付け角のずれなどで一定方向のずれがある
 - **誤差を表現する楕円パラメータが仮のパラメータのままであること**
- 対応
 - 観測位置に応じた誤差パラメータを持つモデルを実環境から構築して物標情報を補正する
 - 誤差パラメータ（二次元正規分布）
 - 平均ベクトル
 - » これでデータを補正することで差し引くことで系統誤差を除去
 - 誤差楕円パラメータ
 - » 実際のデータから得られたパラメータをデータに付与



2025年度：実環境データから誤差モデルを構築（2/2）

- 観測物標の姿勢(θ), 位置(x, y)を入力すると対応する正規分布パラメータが得られるモデルデータを, 実環境データから学習
- 最終的に誤差中央値を0.4m強まで抑えた



地図上に表示した正規分布マップ

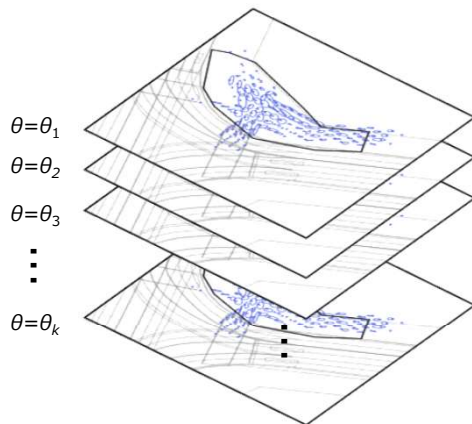
観測物標の位置誤差統計量

Sensor	Med(m)	IQR(m)
LiDAR 1	0.560	0.362
LiDAR 2	0.568	0.324
LiDAR 3	0.511	0.381
LiDAR 4	0.548	0.338

正規分布マップによる平行移動後の位置誤差統計量

Sensor	Med(m)	IQR(m)
LiDAR 1	0.435	0.445
LiDAR 2	0.436	0.435
LiDAR 3	0.461	0.392
LiDAR 4	0.453	0.408

Med: 中央値 IQR: 四分位範囲



位置誤差統計量

	Med(m)	IQR(m)
生データを用いたフュージョン	0.46266	0.35647
正規分布マップを用いたデータをフュージョン	0.41297	0.35789

Med: 中央値 IQR: 四分位範囲

姿勢毎の正規分布マップ (k: 姿勢のグループ数)

成果・課題

- 成果
 - 加減速や旋回など実環境で行われるような動作を行う対象の位置をより正しく推定できるようになっている
 - 複数台の路側機を組み合わせることで、位置精度は中央値で0.4m強
 - そのような精度が求められるODDに 대응することができる
 - 公道の実データから誤差を学習することでフュージョンに有効な効果を与えることができた
- 課題
 - 実データの誤差モデル検討と評価を通じて、ばらつきに関しては十分にモデル化できていない可能性がある
 - 理論的には、カルマンフィルタを通せばばらつきは小さくなるはずであるため
 - 処理遅延への対策
 - 位置精度向上分が交差点通過への程度貢献するかを確認

本研究を通して

- 実環境のデータを参照値付きで取得できることは非常にありがたい
 - Cool4の別チームより参照値付のデータを提供いただいた
 - 現場の課題を把握し、それに対して対処ができる
 - それを以って評価したアルゴリズムは自信をもって学外に報告できる
 - 個別にデータが必要な場合は：
 - 自己位置を算出できる車両が名大にはある
 - 得られたデータは外注でアノテーション可能
- 企画から評価・発表まですべてを自身で行う経験ができた
 - 企画：研究テーマの提案，運営委員会を経て決定
 - 実現・評価：定期的な報告と議論により方向性の確認
 - 発表：対外的なフィードバックを得て研究に反映



学会で発表している様子(2023) 学会で発表している様子(2024)

以上

先進モビリティサービスのための情報通信プラットフォームに関する コンソーシアム成果報告会

セキュアな情報通信網とプライバシー保護

名古屋大学
研究員
竹内僚祐

アジェンダ

- 研究背景
 - DMでのセキュリティ、プライバシー対策機能 全体図
- セキュアな情報通信網
 - ユニキャスト通信
 - ブロードキャスト通信
- プライバシー保護
 - 車両のプライバシー保護
- 今後の課題
- 全体まとめ

研究背景

研究背景 セキュリティとプライバシーのリスクと対策

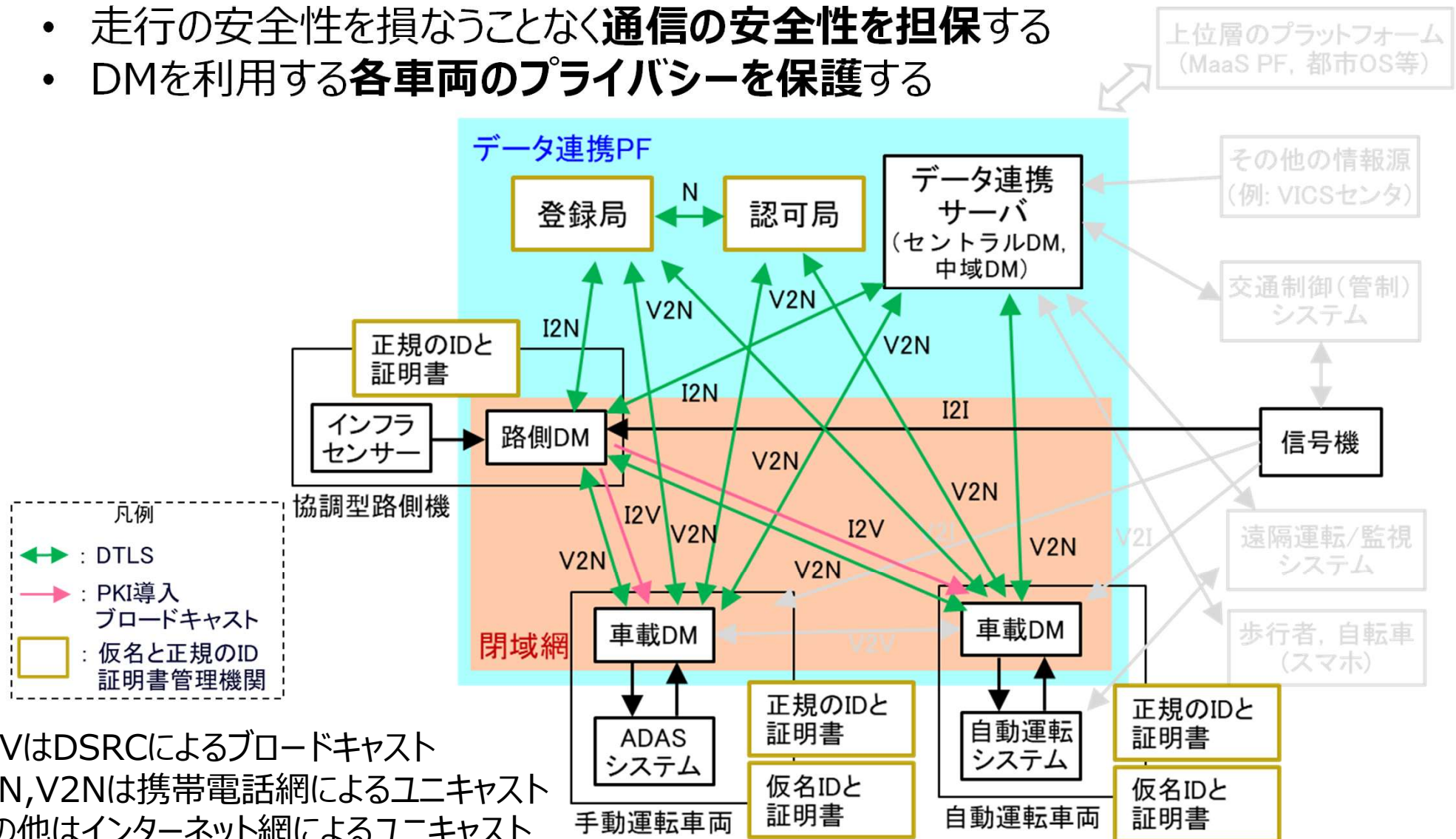
- 一般的なWebサービスでのリスク
 - 情報窃取、改ざん、不正アクセス、なりすましなどのセキュリティリスク
 - 個人情報の漏洩、意図しない利用などのプライバシーリスク
- リスク対策
 - 暗号通信プロトコルの利用 (例. SSL/TLS)
 - 不正アクセス予防 (例. 多要素認証, クローズドネットワーク)
 - 情報の機密性消失加工 (例. 漏洩に備えた情報の匿名化)
- **V2X環境においても同様にリスクは存在するため対策が必要である。**
- 欧州のETSI(European Telecommunications Standards Institute)や北米のSAE(Society of Automotive Engineers)といった標準化機構ではセキュリティリスクやプライバシーリスクに備えた仕様を作成している。
 - 例1)ETSI TS 102 941
 - 「高度道路交通システム (ITS) セキュリティ 信頼性とプライバシー管理」
 - 例2)SAE J2945/1
 - 「V2V安全通信のための車載システム要件」

研究背景 ダイナミックマップへの対策導入

- ダイナミックマップ(DM)には**携帯電話網を利用したユニキャスト**と、**DSRCを利用したブロードキャスト**の通信経路が備わっている。
 - 標準仕様に沿って、各通信経路に対してのセキュリティリスク対策およびプライバシーリスク対策を取り入れる必要がある。
 - ただ、実際にDMの構成に既存仕様を取り込むには、以下課題があった。
 - 運用や詳細が未定義となっている部分がある
 - DMの3層構造への適応
- **DMで運用可能な構成を検討し、リスク対策を担当する新規機能を取り入れた。**

DMのセキュリティ機能導入後 全体構成図

- DMでのセキュリティ機能取り込み目的
 - 走行の安全性を損なうことなく**通信の安全性を担保**する
 - DMを利用する**各車両のプライバシーを保護**する

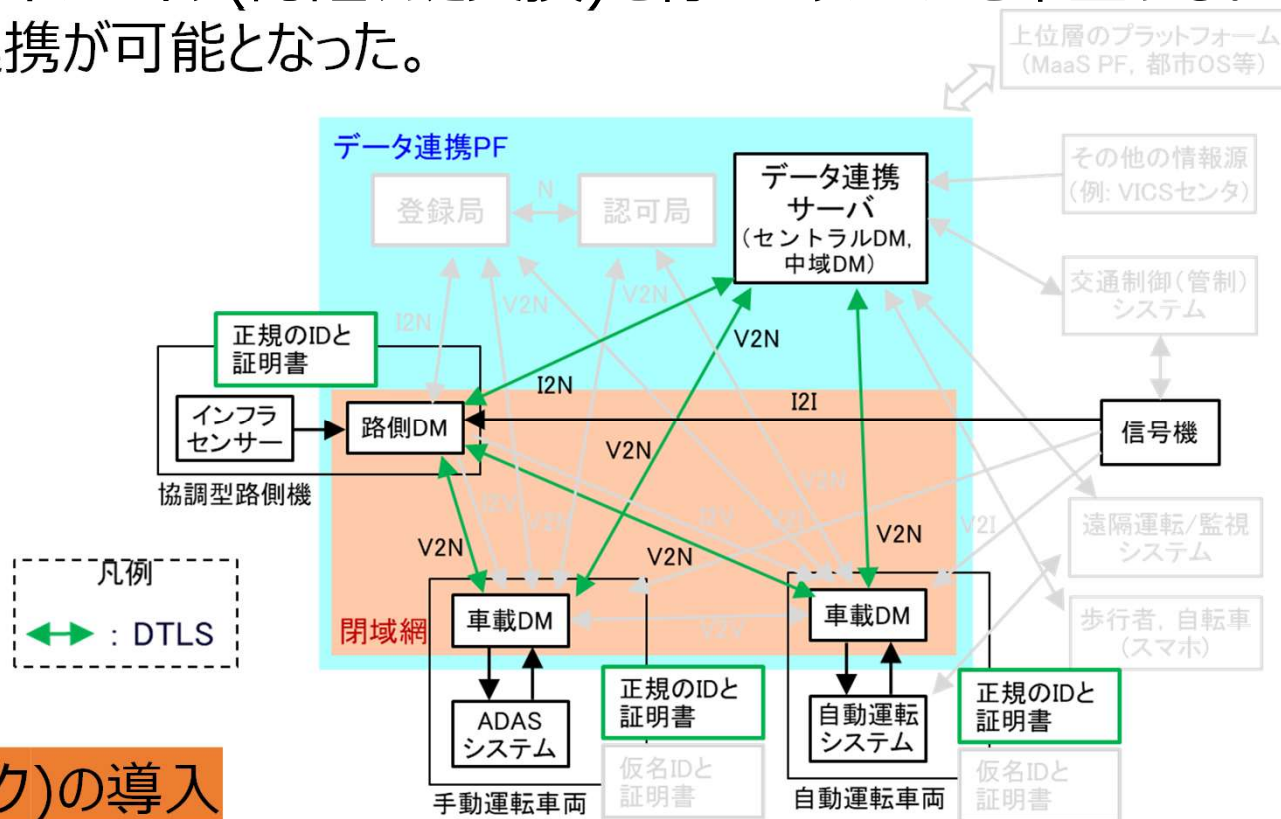


セキュアな情報通信網

ユニキャスト通信へのセキュリティ取り組み

- DTLS(Datagram Transport Layer Security)プロトコルの導入

TLSをベースにUDP通信でも機密性、完全性、認証を確保するプロトコル。
セキュリティ確保のため、ハンドシェイク(認証、鍵交換)を行いセッションを確立する。
→ 暗号通信による情報連携が可能となった。

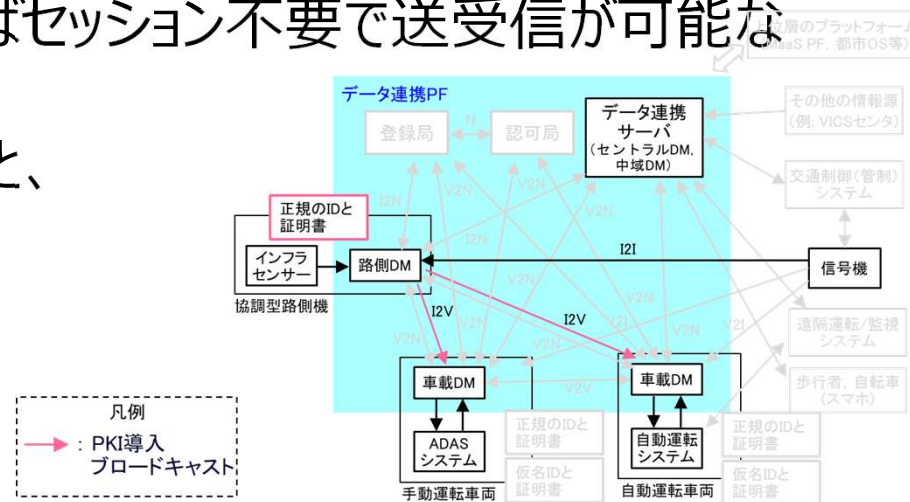


- 閉域網(クローズドネットワーク)の導入

閉域網を利用することで、不正な第三者からのアクセスを遮断する。
→ 閉域網導入までに一定数検出されていた、路側機へのブルートフォース攻撃が検出されなくなった。

ブロードキャスト通信へのセキュリティ取り組み

- ブロードキャスト通信でのPKI導入 ※PKI:Public Key Infrastructure 公開鍵基盤
現在利用しているDSRCは、機材さえあればセッション不要で送受信が可能なブロードキャスト通信である。
セキュリティ対策を導入せずに送信を続けると、
 - 不正なメッセージの傍受、解析
 - 不正な送信元からのメッセージ送信といったことが考えられる。

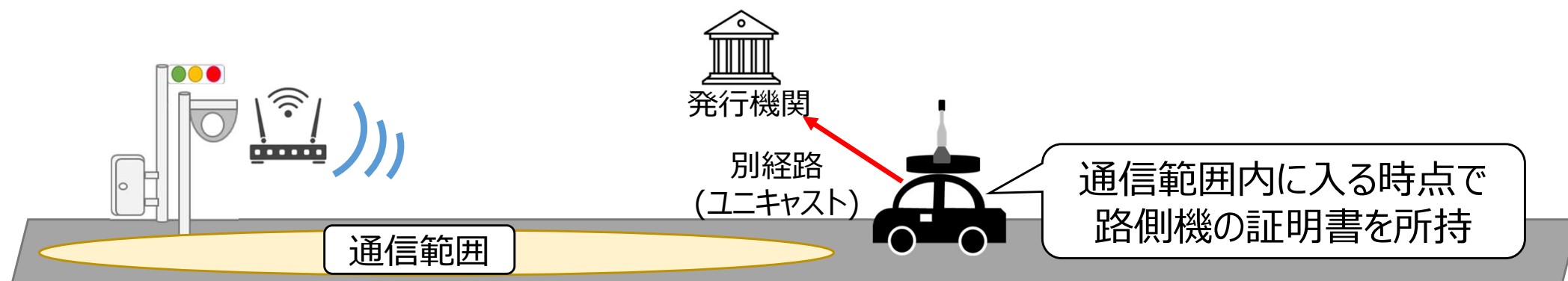


→ ブロードキャスト通信でも認証と暗号通信を行うためPKIを導入した。



ブロードキャスト通信へのPKI導入 課題

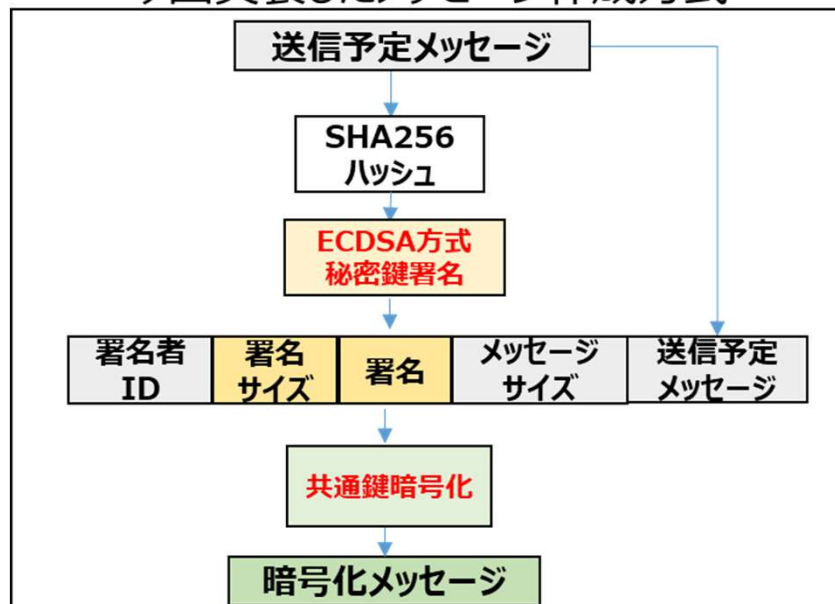
- DMのブロードキャスト通信へPKIを導入する課題は以下2点。
 - 通信範囲に制限があり、車両が移動して通信範囲を出入りする。**
通信可能範囲に入った車両はすぐにメッセージを受信したいが、証明書を持っていないければ公開鍵が入手できず、署名検証が行えない。
 - ハンドシェイクによる証明書交換が行えない。**
常に証明書をメッセージに付与し続けるのはメッセージサイズを圧迫し非効率的。
車両製造時点で全路側機の証明書を持たせることは、容量や管理・更新の面から望ましくない。
- 車両がブロードキャスト通信範囲に侵入する前に、路側機の証明書を発行した機関から**別経路(ユニキャスト通信)**で路側機証明書を手入手する手法を導入した。



ブロードキャスト通信へのPKI導入 新規実装詳細

- PKI導入時のブロードキャスト通信用メッセージ構造
 - ETSIの仕様書内では、ブロードキャスト通信メッセージに署名と暗号化を施す際、署名作成後、暗号化の加工順としている。
- ETSIの加工順を採用したメッセージ作成方式をDMに実装した。
 - 署名は、送信予定メッセージのheaderも含めた内容を基に作成する。
 - 共通鍵で暗号化、復号を実施する。

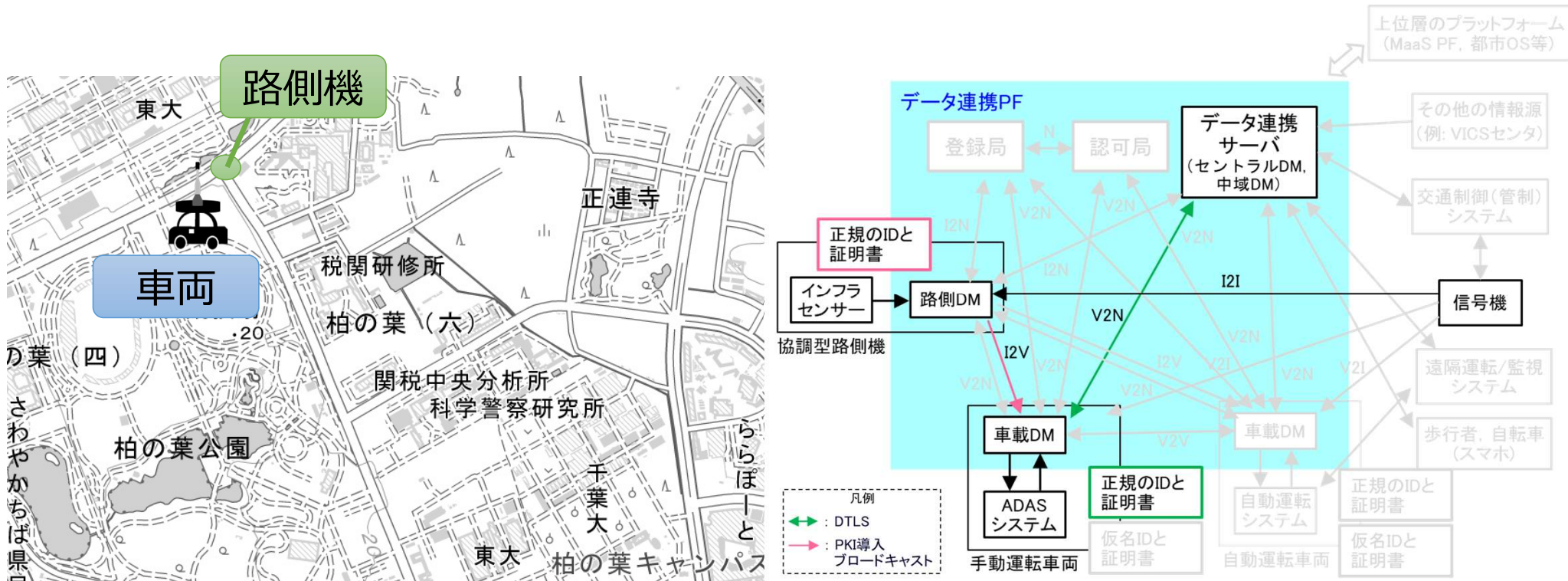
今回実装したメッセージ作成方式



実装内容の柏の葉公道環境実験

- 実験目的
 1. 実際の環境で動作確認、処理遅延を計測する。
 2. 送り主の身元検証機能の効果を確認する。
→署名検証に失敗するケースを作成。メッセージが廃棄されることを確認する。
- 実験方法

1台の路側機と1台の車両間で実験を行った。
路側機証明書はクラウド上のデータ連携サーバに設置し、取得することとした。



柏の葉公道環境での実験 実験結果 1

- 実際の環境で動作確認、処理遅延を計測する。
 - 署名が検証されたメッセージは正しく受信できることが確認できた。

路側DM 送信プロセス

車載DM 受信プロセス

車載DM 情報表示アプリ

ファイル(F) 編集(E) 設定(S) コントロール(C) ウィンドウ(W) ヘルプ(H)	ファイル(F) 編集(E) 設定(S) コントロール(C) ウィンドウ(W) ヘルプ(H)	ファイル(F) 編集(E) 設定(S) コントロール(C) ウィンドウ(W) ヘルプ(H)
<pre> dm2.conf]INTERFACE_NAME_2: eth0 dm2.conf]UDP_PORT_NUMBER_2: 50047 dm2.conf]SEND_LIST_2: ./its_send_list.csv dm2.conf]SOCKET_TYPE_2: 0 dm2.conf]CS_PACKET_SIZE_2: 9500 *** .././../conf/./send_list_v4.csv START *** 1901000101, 35.78,139.81 *** .././../conf/./send_list_v4.csv END *** Signing completed. ===== Signing completed. ===== Signing completed. ===== Signing completed. ===== Signing completed. ===== Signing completed. ===== Signing completed. ===== Signing completed. ===== </pre>	<pre> 2025-02-12 05:35:04,920 LINE:63 INFO ProcSender - start [GetIPifaddr] 指定されたインターフェース名のIPアドレスを抽出します。 2025-02-12 05:35:04,920 LINE:256 INFO ProcSender - sid_sq_id_received_time_m p削除処理実行 [GetIPifaddr] 候補: 127.0.0.1 [GetIPifaddr] 抽出成功: 127.0.0.1 2025-02-12 05:35:04,921 LINE:145 INFO NwReceiver - lo sockfd_common = 4 2025-02-12 05:35:04,984 LINE:204 INFO NwReceiver - lo sockfd_commonで受信 ev ret[0].data.fd == 4 recvfrom:480 1901000145.key 371 374 256 Verify Success 2025-02-12 05:35:04,985 LINE:227 INFO NwReceiver - 480 2025-02-12 05:35:04,985 LINE:288 INFO NwReceiver - lo Recvfrom Success! 2025-02-12 05:35:04,985 LINE:292 INFO NwReceiver - lo src_station_id:19010001 45, dst_station_id:90000000, src_station_type:0, dst_station_type:0, transmiss ion_flag:0, duplication_check_id:1739338504915186532, lane_id:0, retry_level:0 , retry_data_id:0, retry_lifetime:0, msg_type:2, cs_message_detail:0, fd_name: 2025-02-12 05:35:04,986 LINE:303 INFO NwReceiver - lid=0,8504986751386 2025-02-12 05:35:04,987 LINE:90 INFO ProcSender - src_station_id:1901000145, dst_station_id:90000000, src_station_type:0, dst_station_type:0, transmission flag:0, duplication_check_id:1739338504915186532, lane_id:0, retry_level:0, re try_data_id:0, retry_lifetime:0, msg_type:2, cs_message_detail:0, fd_name:2025 -02-12 05:35:05,184 LINE:204 INFO NwReceiver - lo sockfd_commonで受信 ev_ret[0].data.fd == 4 </pre>	<pre> 9223430521424454221,666423309888,0,2,100,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,100,4326,35900 0,8000001,0,-132768,-132768,-132768,15,17,101,0,0,10001,0,-132768,-132768,-132768,15 0,16383,13496,32767,-1000,1001,11363,7200,50,65535,50,65535,170,65535,0,7,91,91,0 5,15,255,0,0,0,0,36001,[8781] </pre>

- PKIの導入前後を比較し、路側機からメッセージが送信され、車両が受信し情報がDBへ登録されるまでの処理遅延結果が右表。
 - PKI導入により遅延は増加したが、平均遅延目標は300msのため許容内であると判断した。
(目標値はETSIの要求目標から設定)

処理遅延	全体平均
導入前	199.1ms
導入後	223.1ms

柏の葉公道環境での実験 実験結果 2

- 送り主の身元検証機能の効果確認
 - 署名作成に使う秘密鍵を変えたケースと、署名を付与しないケースを実施

路側DM
送信プロセス

車載DM
受信プロセス

車載DM
情報表示アプリ

使用された秘密
鍵が違うケース

署名が付与され
ていないケース

```
cool14@ubuntu: /dm2/cs/bin$ ./dm2cs_send
[INFO] DM2_CONF_DIR_PATH = ../../conf/
[dm2.conf] MY_STATION_ID: 1901000145
[dm2.conf] SEND_NETWORK_NUM: 2
[dm2.conf] INTERFACE_NAME_1: eth0
[dm2.conf] UDP_PORT_NUMBER_1: 55555
[dm2.conf] SEND_LIST_1: ./send_list_v4.csv
[dm2.conf] SOCKET_TYPE_1: 2
[dm2.conf] CS_PACKET_SIZE_1: 1442
[dm2.conf] INTERFACE_NAME_2: eth0
[dm2.conf] UDP_PORT_NUMBER_2: 50047
[dm2.conf] SEND_LIST_2: ./its_send_list.csv
[dm2.conf] SOCKET_TYPE_2: 0
[dm2.conf] CS_PACKET_SIZE_2: 9500
*** ../../conf/./send_list_v4.csv START ***
901000101, 35, 78, 139, 81
*** ../../conf/./send_list_v4.csv END ***
Signing completed.
=====
Signing completed.
=====

dm2@ubuntu: /dm2/cs/bin$ ./dm2cs_recv
[INFO] DM2_CONF_DIR_PATH = ../../conf/
[dm2.conf] MY_STATION_ID: 226
[dm2.conf] RECEIVE_NETWORK_NUM: 1
[dm2.conf] INTERFACE_NAME_1: lo
[dm2.conf] INTERFACE_IP_VER_1: 4
[dm2.conf] UDP_PORT_NUMBER_1: 50047
[dm2.conf] SOCKET_TYPE_1: 0
[dm2.conf] CS_PACKET_SIZE_1: 9500
2025-02-12 05:52:28,886 LINE:104 INFO NwRcv_main - ProcReceiver, NwSender生成

cool14@ubuntu: /dm2/cs/bin$ ./dm2cs_send
[INFO] DM2_CONF_DIR_PATH = ../../conf/
[dm2.conf] MY_STATION_ID: 1901000145
[dm2.conf] SEND_NETWORK_NUM: 2
[dm2.conf] INTERFACE_NAME_1: eth0
[dm2.conf] UDP_PORT_NUMBER_1: 55555
[dm2.conf] SEND_LIST_1: ./send_list_v4.csv
[dm2.conf] SOCKET_TYPE_1: 2
[dm2.conf] CS_PACKET_SIZE_1: 1442
[dm2.conf] INTERFACE_NAME_2: eth0
[dm2.conf] UDP_PORT_NUMBER_2: 50047
[dm2.conf] SEND_LIST_2: ./its_send_list.csv
[dm2.conf] SOCKET_TYPE_2: 0
[dm2.conf] CS_PACKET_SIZE_2: 9500
*** ../../conf/./send_list_v4.csv START ***
901000101, 35, 78, 139, 81
*** ../../conf/./send_list_v4.csv END ***
not signing.
=====
not signing.
=====

2025-02-12 05:48:37,198 LINE:39 INFO ProcSender - start
2025-02-12 05:48:37,198 LINE:111 INFO NwReceiver - lo receiver start
2025-02-12 05:48:37,199 LINE:48 INFO ProcSender - exit
[GetIPifaddrs] 指定されたインターフェース名 lo の IP アドレスを抽出します。
2025-02-12 05:48:37,199 LINE:63 INFO ProcSender - start
2025-02-12 05:48:37,199 LINE:256 INFO ProcSender - sid_sq_id_received_time_ms
削除処理実行
[GetIPifaddrs] 候補: 127.0.0.1
[GetIPifaddrs] 抽出成功: 127.0.0.1
2025-02-12 05:48:37,199 LINE:145 INFO NwReceiver - lo sockfd_common = 7
2025-02-12 05:48:37,284 LINE:204 INFO NwReceiver - lo sockfd_common で受信 ev
ret[0].data.fd == 7
recvfrom:418
1901000145.key
0
374
sign not granted
2025-02-12 05:48:37,285 LINE:227 INFO NwReceiver - -1
2025-02-12 05:48:37,285 LINE:230 INFO NwReceiver - lo Recvfrom fail
2025-02-12 05:48:37,384 LINE:204 INFO NwReceiver - lo sockfd_common で受信 ev
ret[0].data.fd == 7
recvfrom:418
1901000145.key
0
374
sign not granted
2025-02-12 05:48:37,385 LINE:227 INFO NwReceiver - -1
2025-02-12 05:48:37,385 LINE:230 INFO NwReceiver - lo Recvfrom fail
```

→ 車載DM受信プロセスでメッセージが遮断されたことを確認した。

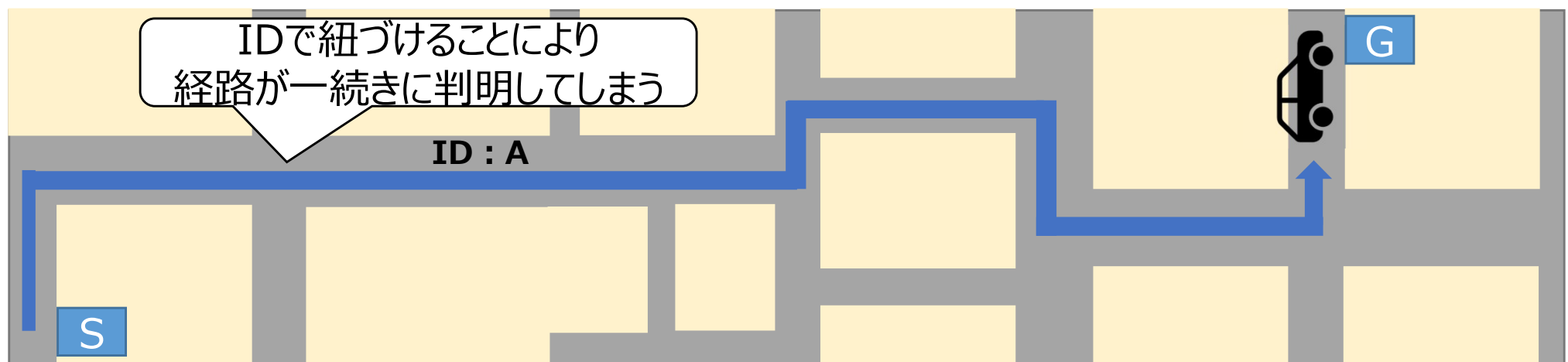
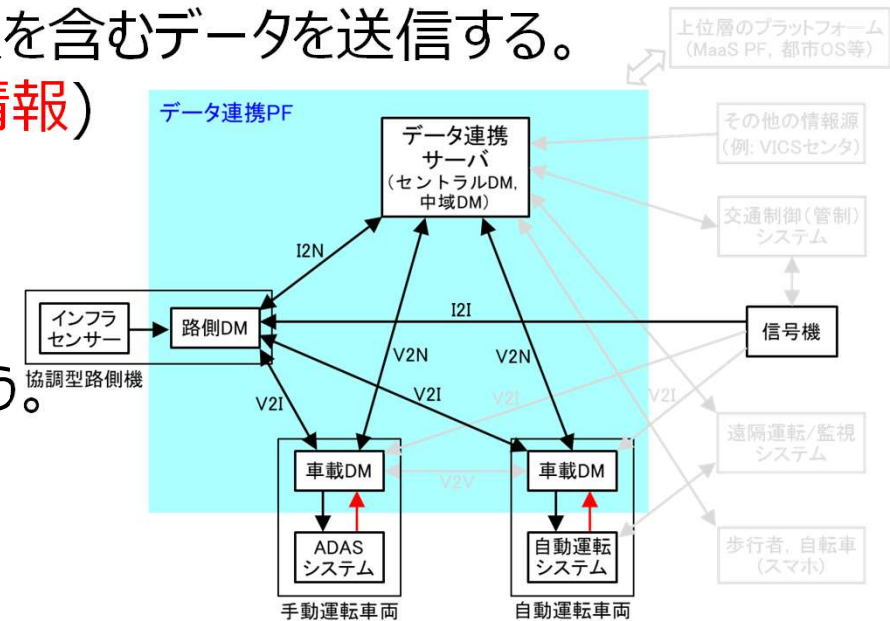
セキュアな情報通信網 まとめ

- DMにはユニキャスト、ブロードキャストと2つの通信経路が存在する。
- 両経路でETSIの仕様に沿い、セキュアな情報連携を行うための取り組みを行った。
 - ユニキャスト通信では、なりすましや盗聴のリスクに対し、暗号通信である**DTLSを導入**することで対応した。
また、不正アクセスのリスクに対して、**閉域網を導入**することで対応した。
- ブロードキャスト通信では、不正な受信送信による情報窃取、なりすましのリスクに対し**PKIを導入**することで対応した。
 - 移動する車両とブロードキャストの通信範囲という制限に対し、サーバーとなる路側機の証明書を、車両が事前にユニキャスト通信で受け取る手法で解決した。
- 実験による検証結果
 - 署名が不正なメッセージに対して受信時点で遮断する効果を確認した。
 - PKI導入後の増加した処理遅延は許容範囲内であった。

プライバシー保護

V2Xにおけるプライバシー保護の必要性

- 長距離の走行位置トラッキングによるプライバシーの侵害
 - 車両は走行中、自身のID及び位置情報を含むデータを送信する。
(各運転システムから送られる**自己物標情報**)
- 攻撃者が自己物標情報のログを得た際、実際に車両を追跡せずとも、走行経路を長距離で把握することが可能となってしまう。
- このような車両のプライバシーリスクに対し各標準化機構の仕様では、IDや証明書の定期的変更を定義している。



車両プライバシー保護の取り組み 各標準化機構の仕様調査

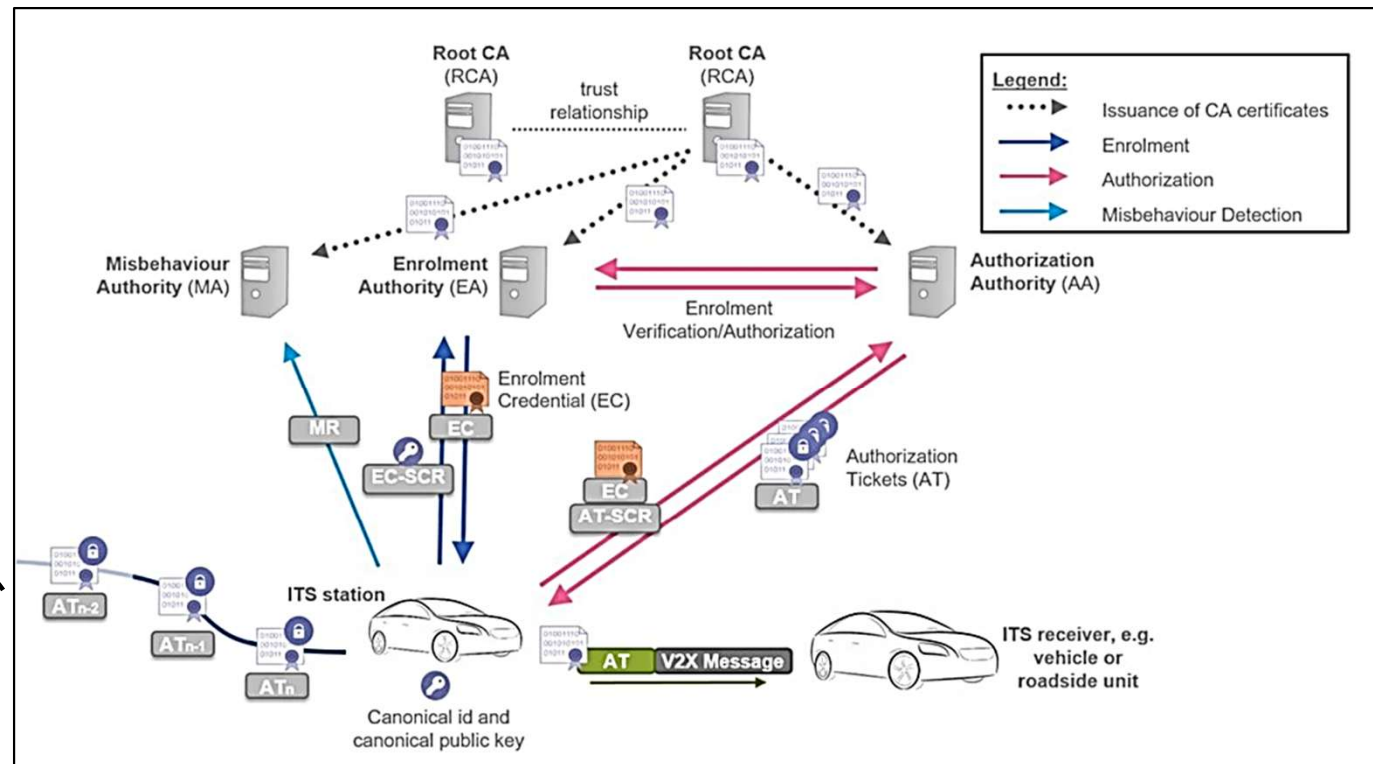
- 仮名ID
 - **欧州 ETSIの仕様定義**
ETSI TS 102 941
Intelligent Transport Systems (ITS) Security; Trust and Privacy Management;
 - 仮名と追跡不可を担保することで、メッセージ送信者のプライバシーを保護。
 - 一時的なID(仮名ID)を使用し、正規のIDを送信しない。
 - PKI機関の義務と役割を、正規のIDを検証する登録機関と、仮名IDの管理を担当する認可機関に分離する。
 - **北米 SAE**でもSAE J2945/1にて同様のIDと証明書の短期切り替えが定義されている。
 - 仮名IDを使用した自己物標情報を送信することで、1つのIDからは走行経路を部分的にしか把握されない効果がある。



→特にETSIの仮名IDによる仮名性確保とPKI機関の役割分離の仕組みを導入した。

参考) ETSIのPKIアーキテクチャ

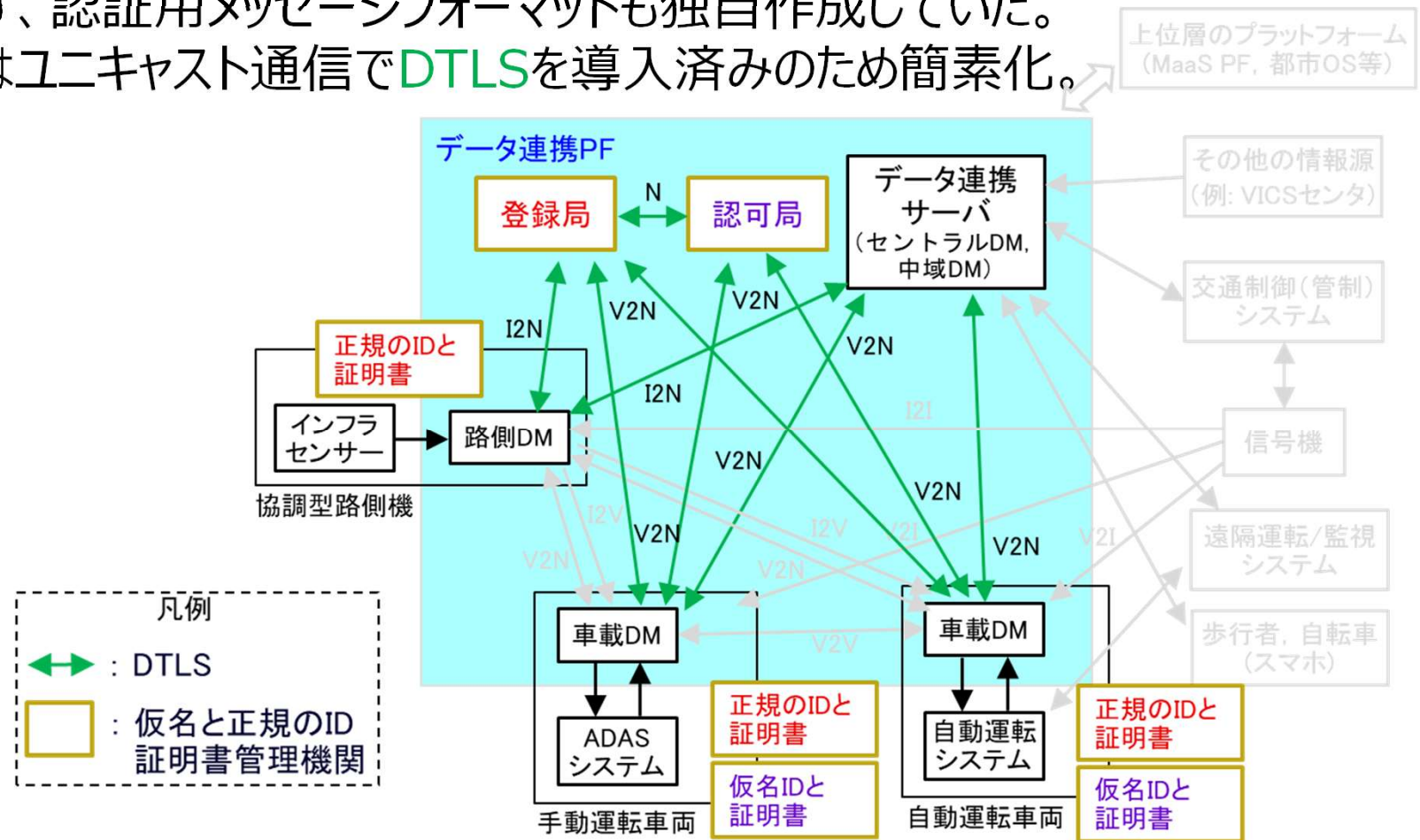
- 管理機関と証明書の説明
 - EA** : Enrollment Authority (正規のID検証を行う登録機関)
 - AA** : Authorization Authority (仮名ID管理を行う認可機関)
 - MA** : Misbehavior Authority (不正行為検出管理機関)
 - EC** : Enrollment Certificate (正規のID証明書)
 - AT** : Authorization Tickets or Pseudonym Certificate (V2V/V2I通信用仮名ID証明書)
- 仮名IDは一時的な使い捨てIDではあるが、システムで認められているIDであることを担保するため、証明書を発行する。
- 正規のIDと仮名IDが車両外で紐づかないよう、各ID管理機関を分離している。
 - EAは正規のIDを管理
 - AAは仮名IDを管理



ETSI TS 102 940 V2.1.1 (2021-07)
Intelligent Transport Systems (ITS); Security; ITS communications
security architecture and security management

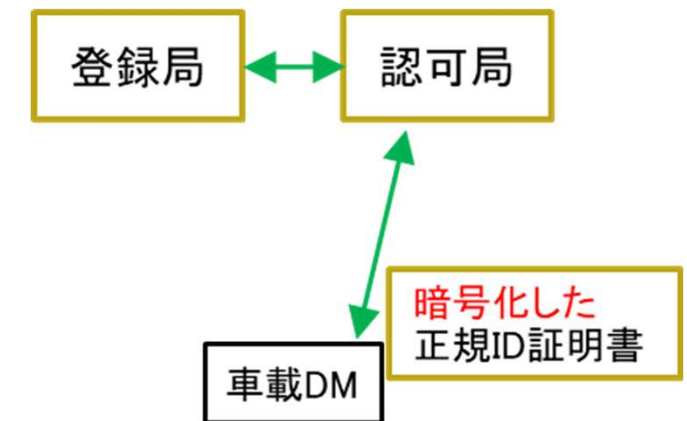
DMへのプライバシー保護機能導入

- 仮名機能導入後の構成
 - 登録局および認可局を別サーバとしてクラウドで運用した。
 - 登録局が正規のIDを管理し、認可局が仮名IDを管理することは仕様通り。
 - ETSI仕様では特定通信形式に依存しない形態のため、一般の暗号層(TLS)を利用せず、認証用メッセージフォーマットも独自作成していた。
 - DMはユニキャスト通信でDTLSを導入済みのため簡素化。



DMのプライバシー保護機能運用

- DMでの仮名運用方法
 - 車両による仮名要求時、暗号化した正規IDの証明書を添付し、認可局が登録局へ検証を依頼する。
 - 正規のIDで認証を行うとともに、正規のIDと仮名IDが車両以外の地点に平文で揃うことを回避した。



- ETSIの仕様では路側機のプライバシーやIDについて未定義であった。
 - 路側機はIDを変更せず正規IDとして登録局で管理することとした。ブロードキャストのPKIにおける事前取得先も登録局となった。
- ETSIでは、仮名証明書を期限内で能動的に失効する手法を定義していない。
 - 登録局、認可局にてDBで証明書情報を管理することとした。またOCSP(Online Certificate Status Protocol)を参考とした、適宜失効問い合わせと応答の仕組みを作成した。

仮名の導入後データ連携実験

- 実験目的
 - 仮名IDを使った自己物標情報の送信と性能の測定
 - 実験時の走行経路
 - 科警研交差点通過：1台の路側機を通過し仮名切り替え
 - 東大前～柏の葉キャンパス駅前区間：4台の路側機を通過し仮名切り替え
- ※ 路側機付き交差点の侵入と退出時に自動で仮名IDを切り替える。



仮名の導入後データ連携実験 実施

- 科警研交差点通過の実施結果 ID変更有

車外映像



車内映像



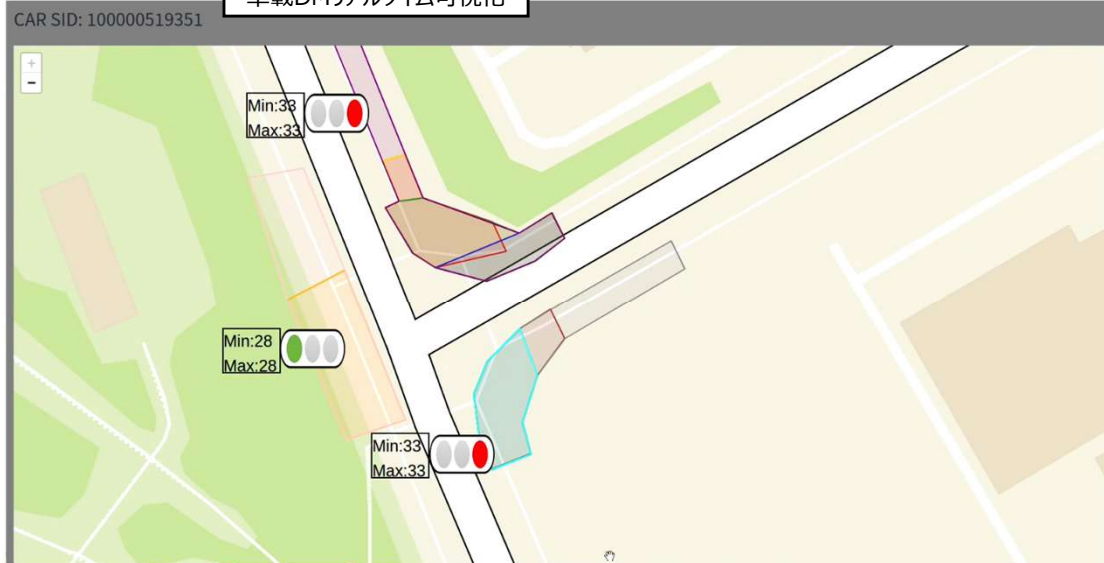
replay map

データ連携サーバの物標情報ログ再生



★ 仮名変更想定ポイント

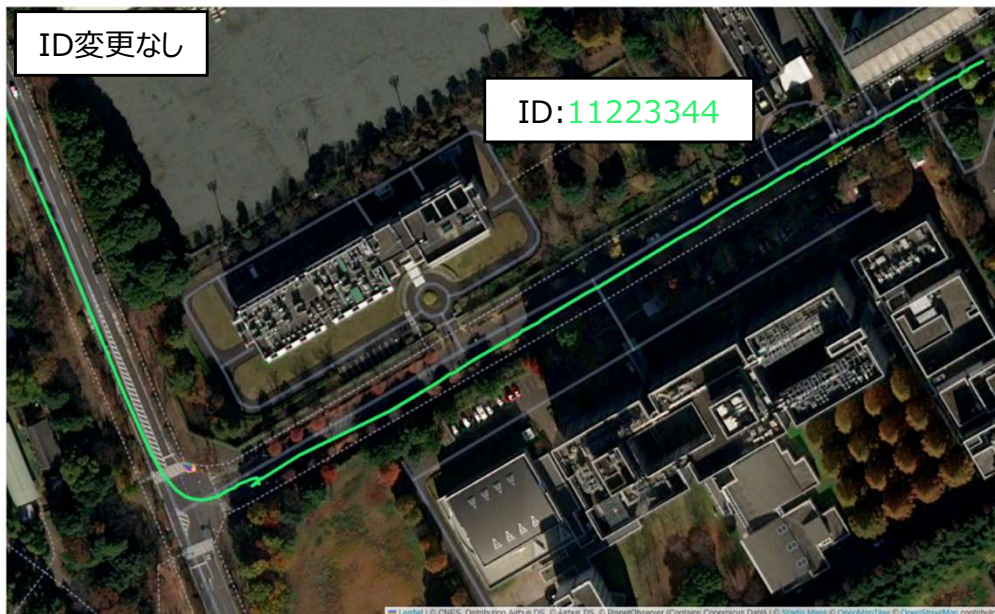
車載DMリアルタイム可視化



仮名の導入後データ連携実験 自己物標情報ログ軌跡全表示

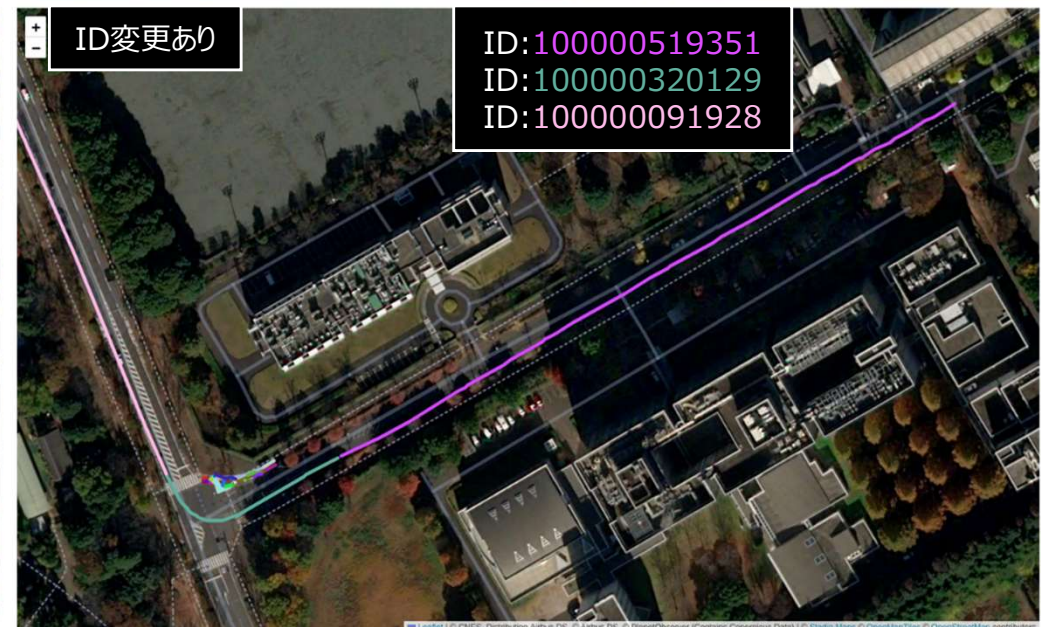
- 科警研交差点通過結果 ID変更ありなし比較

replay map



1つのIDから走行ルートを最初から最後まで
トラッキングできてしまう

replay map



例として、ID:100000091928の経路のみをトラッキングしても
交差点を曲がってきたか、直進してきたか判別できない

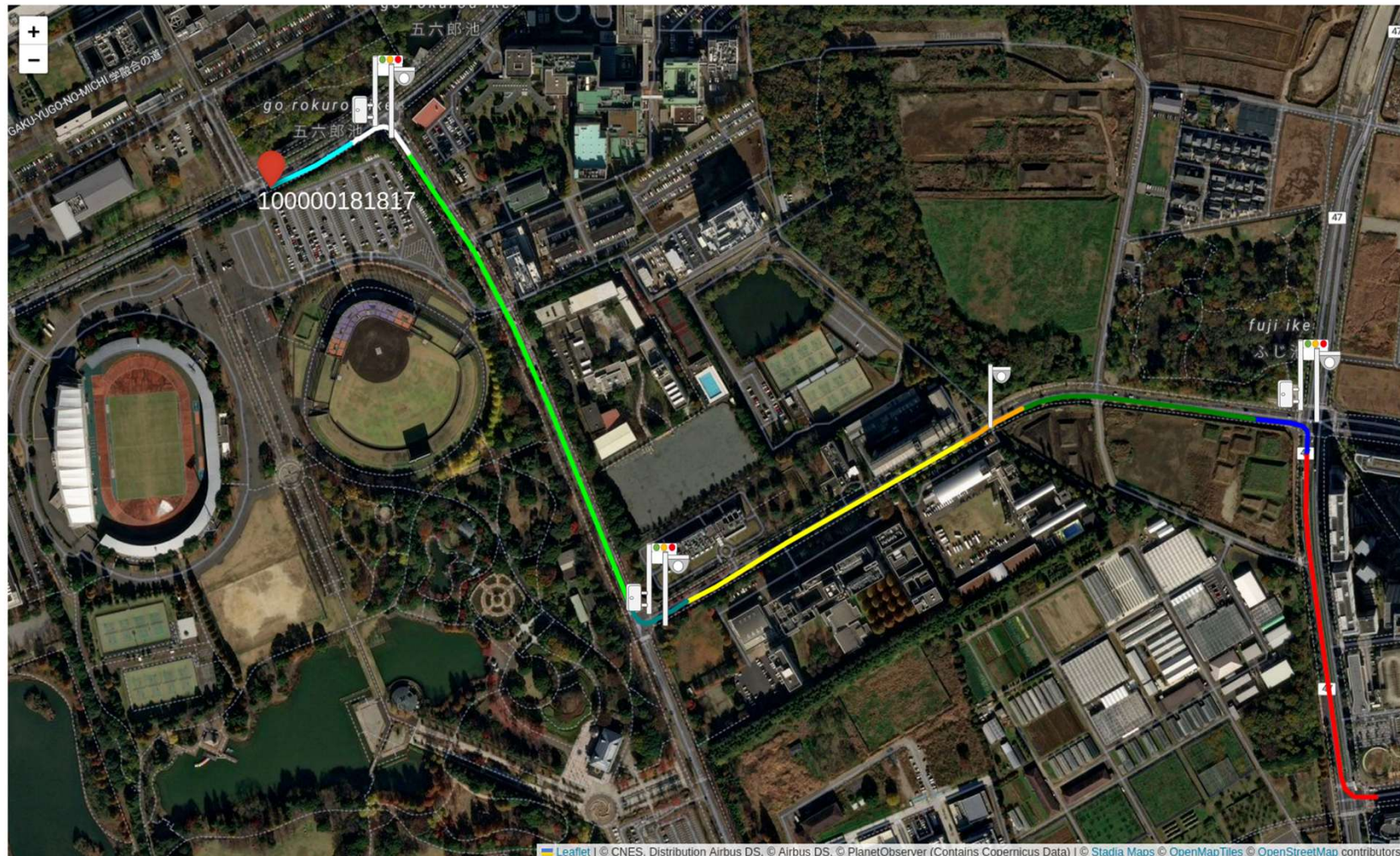
→ DMでの仮名IDを付与した自己物標情報の連携と、
IDを用いた経路追跡が細かく途切れることを確認できた。

仮名の導入後データ連携実験 複数の交差点通過時のログ軌跡

- 東大前～柏の葉キャンパス駅前区間走行結果 ID変更走行の全体結果
 - 4つの路側機付き交差点通過時IDを変更し、計9個の仮名使用を確認できた。

replay map

Deploy



仮名の導入後データ連携実験 PKI受信全体の処理遅延

- PKI導入ブロードキャスト受信を行うための時間測定まとめ
 - 現在想定するブロードキャスト受信までの手順、
[仮名取得→仮名切り替え→路側機証明書取得→PKIブロードキャスト受信]
1件目のメッセージを受信するまでの**合計処理遅延**を算出した。
 - <車両と認可局、登録局間のDTLSコネクションがすでに確立されている場合>
 $237\text{ms} + 5\text{ms} + 85\text{ms} + 208\text{ms}(\times) = 535\text{ms}$
 - <車両と認可局、登録局間のDTLSコネクションが確立されていない場合>
 $1,604\text{ms} + 5\text{ms} + 709\text{ms} + 208\text{ms}(\times) = 2,526\text{ms}$
- ※ 実験時、路側DMが信号機情報を得てから、車載DMが情報をDBに登録するまでの処理遅延平均
- コネクションを確立していない状態では合計処理遅延が長い。
また今後通信台数(車両)が増えることで、仮名取得や路側機証明書取得の所要時間は増加する可能性がある。

本課題は、車載DMが携帯電話網を活用し、路側機付き交差点接近前段階で、各種証明書のやり取りを実施するなど、運用面で対応することを考えている。

プライバシー保護 まとめ

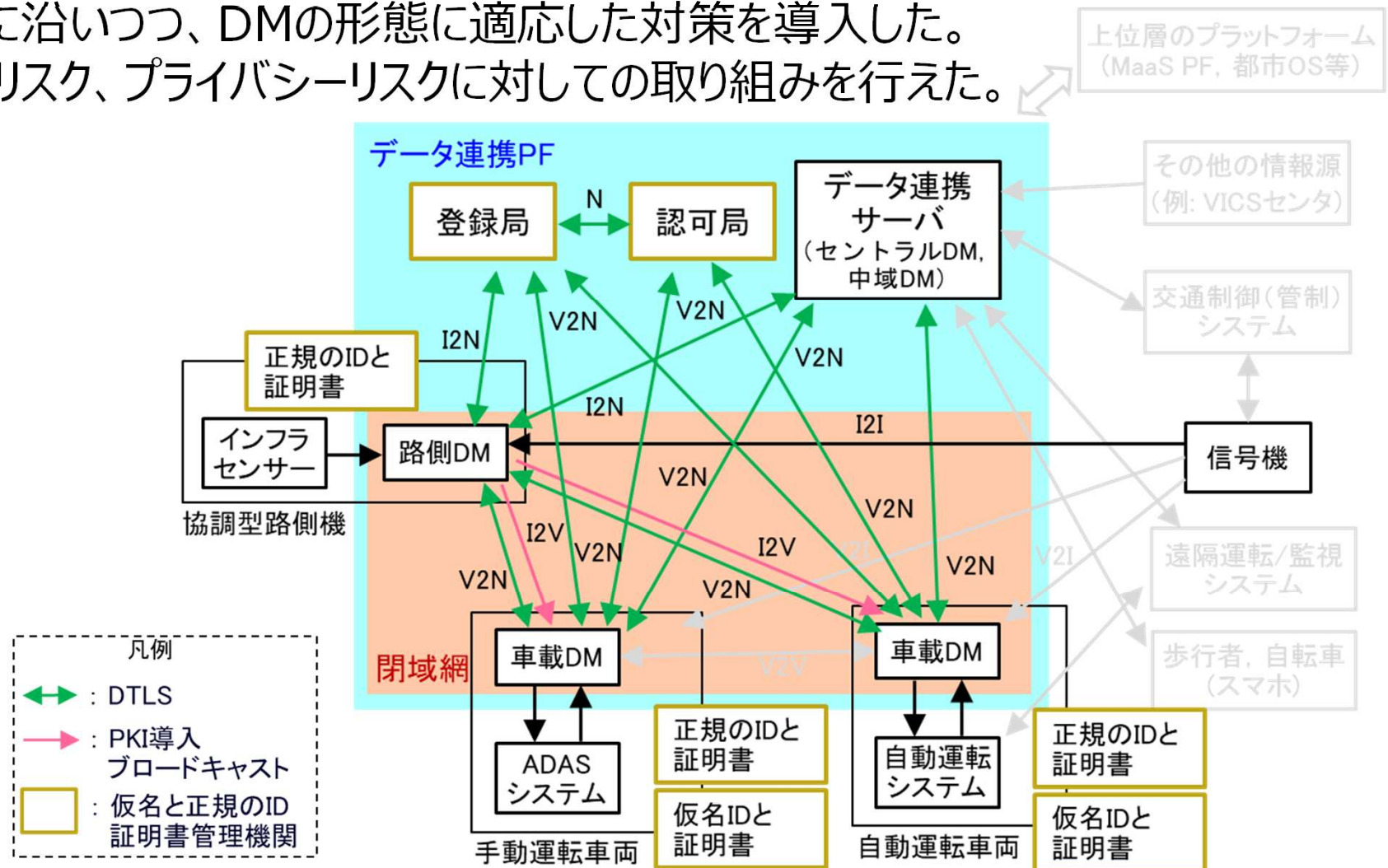
- DMを利用する車両は自身のIDと位置情報を自己物標情報として送信する。
- ログを用いた経路追跡から、車両所有者のプライバシーを保護する取り組みを行った。
 - ETSIの仕様を参考に仮名の概念を導入し、正規のIDとは異なる、使い捨ての**仮名IDを追加**した。また**認可局と登録局の各ID管理機関**を設置した。
 - ETSIの仕様で詳細な定義がされていなかった路側機のプライバシー扱いについて、運用方法を検討し導入した。
 - 他ETSI内では未定義だった運用面についても同様に検討と導入を行った。
- 実験による検証結果
 - DMが自身のIDを適宜変更しながら走行できること、自己物標情報を仮名IDに変更することで、ログによるトラッキングが途切れることを確認した。
 - 仮名を運用するための処理遅延について各機関と車両がコネクションを確立しているかどうかで、遅延に大きな影響が出ることが分かった。
本課題は、運用面で解決が可能と考えている。

今後の課題

- セキュアな情報通信網
 - 安全性評価
 - 安全性の評価指標を標準規格等を利用して評価する
 - 閉域網内部での異常通信検出
 - 不正な行動及び通信を行う機器が出現した場合の判別方法を検討する
- プライバシー保護
 - 多数の車両が存在する場合の性能測定
 - シミュレーションの利用により、大量の車両が仮名および証明書を扱う環境を作成し検証する
 - 仮名変更および、証明書事前連携基準の戦略
 - 仮名変更や、証明書取得の詳細な運用方法を検討する
(例. 周囲に他車両がない場合に仮名を変更しても効果が見込めない)
 - テストケースの策定
 - ETSIが実施するプラグテストを参考に、テストケースを検討する

全体まとめ

- V2X環境においても一般的なWebサービス同様のリスクが存在し対策が必要である。
- ETSIやSAEといった標準化機構では各リスクに備えた仕様を作成している。
- 標準仕様に沿いつつ、DMの形態に適応した対策を導入した。
セキュリティリスク、プライバシーリスクに対する取り組みを行えた。



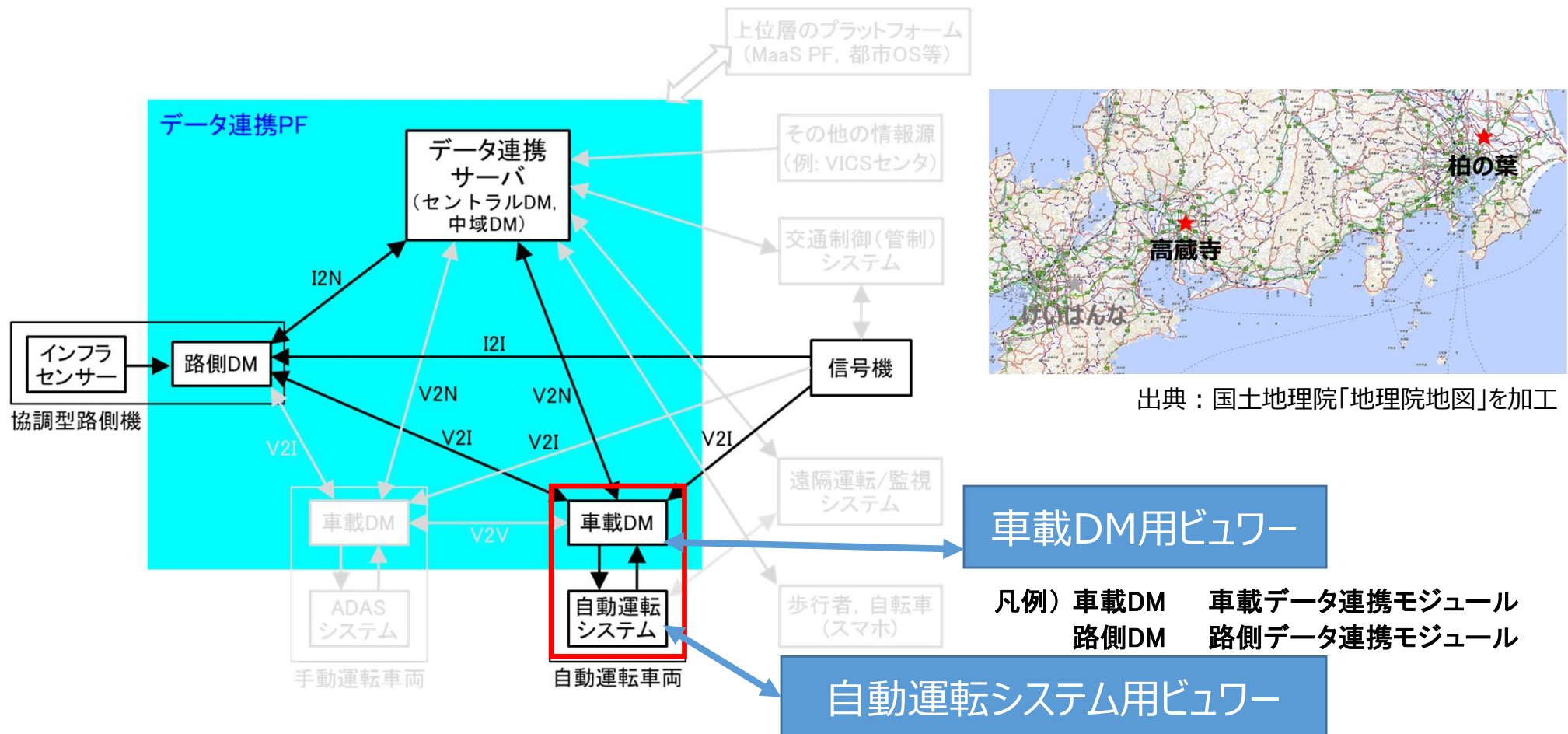
先進モビリティサービスのための情報通信プラットフォームに関する コンソーシアム成果報告会

レベル4自動運転バスの交差点通過支援

名古屋大学
研究員
草山真一

この資料の位置づけ

- **CooL4で取り組んでいるユースケースと自動運転車両内（自動運転システムと車載DM）の仕組み**を紹介する資料
- 自動運転システム、車載DMそれぞれと繋がっているビューワーの映像を使用
- 実証実験の様子は、主に柏の葉について紹介する。一部、高蔵寺も紹介する。



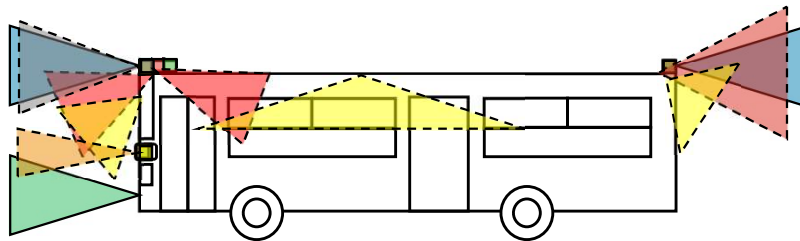
アウトライン

- Cool4 レベル4自動運転バス
 - バス内概要
 - 車載DMの構成図および車内配置図
 - 走行ルートと協調型路側機の位置
 - 車載DMに届けられる通信路の特徴
 - 車載DM内のソフトウェアの仕組み
 - 走行中の車内ディスプレイ表示
 - 車載DM用ビュー
- 自動運転車両の交差点通過支援
 - 信号灯色の変化を先読みした交差点通過判断
 - 物標情報を活用した交差点通過判断
- まとめ

Cool4 レベル4自動運転バス - 概要

【自動運転システム】

- 単独で、車両・歩行者等の物標や信号機の灯色を検知し、認識する能力を有する。



【凡例】	
	中距離 LiDAR × 4
	高解像度 LiDAR × 1
	遠距離&信号認識用カメラ × 1
	中距離用カメラ × 5
	近辺用カメラ × 4
	ステレオカメラ × 1



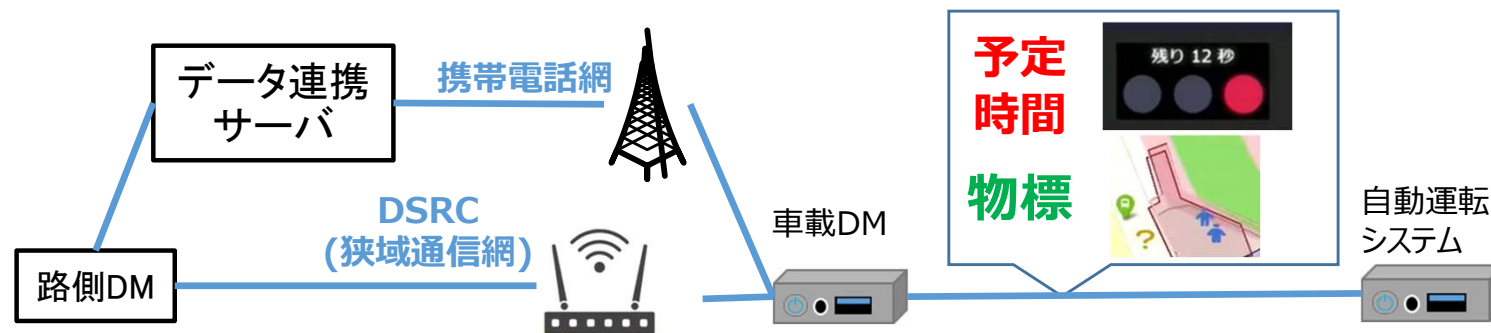
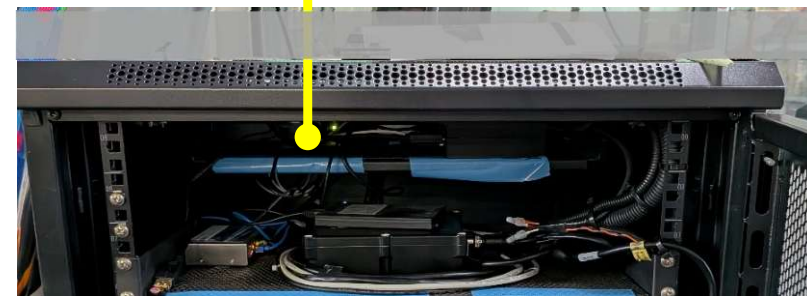
先進モビリティ株式会社より提供

【車載DM】

- 2種類の通信経路を使って、協調型路側機が検知した情報を自動運転システムへ連携
- 自動運転バスが交差点を円滑に通過するために
信号の灯色が変化する予定時間や
車載センサーから死角となる物標等を連携

車載DM

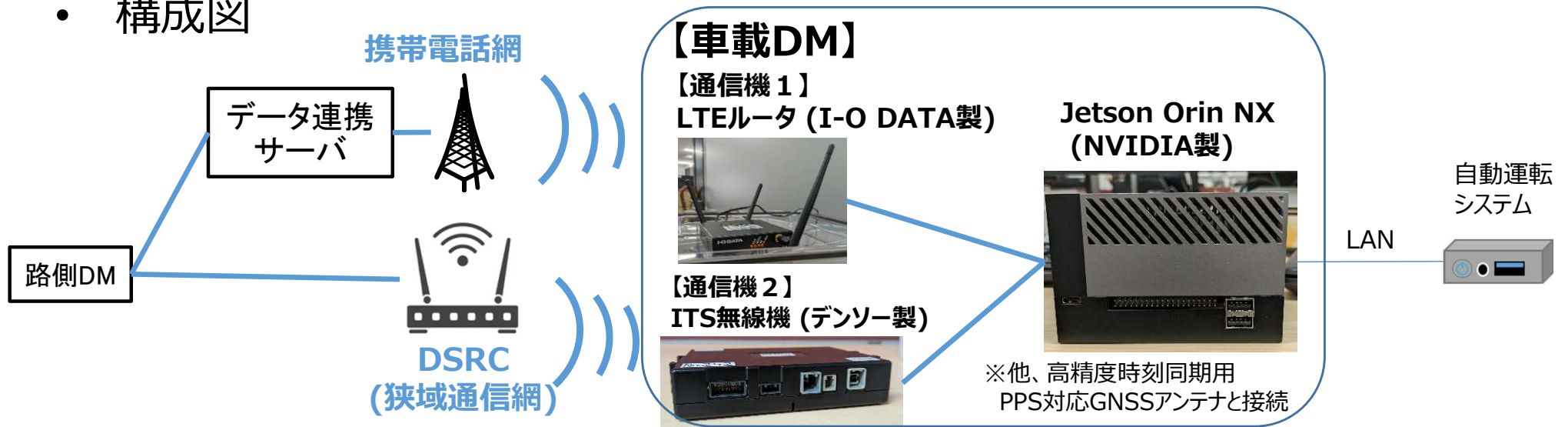
(車内のBOXを開けた様子)



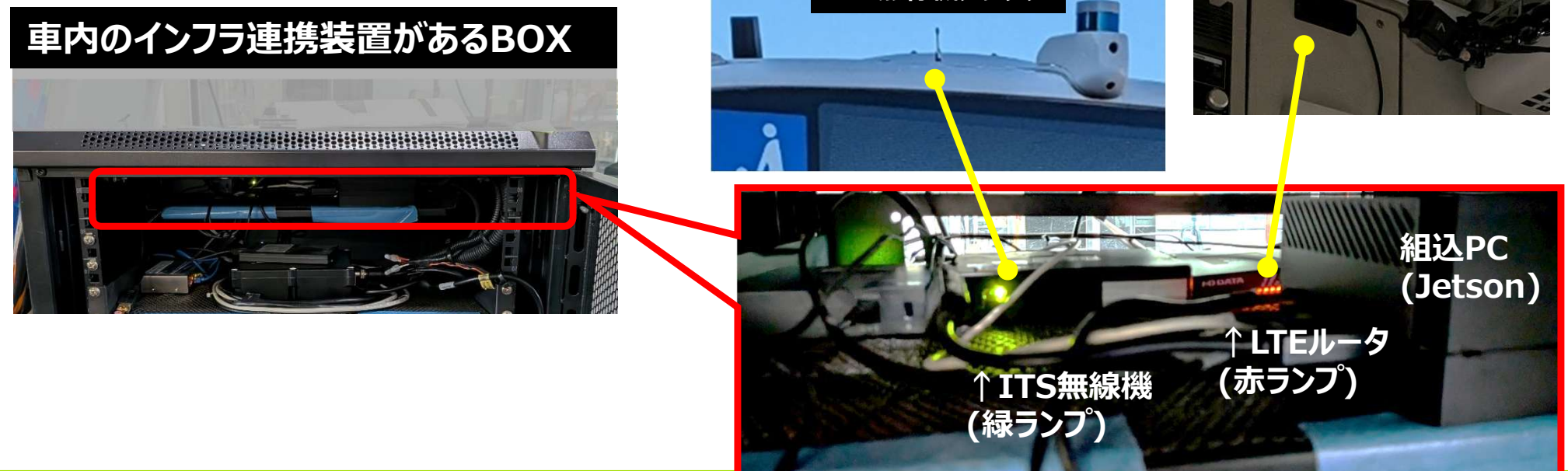
Cool4 レベル4自動運転バス

- 車載DMの構成図および車内配置図

・ 構成図



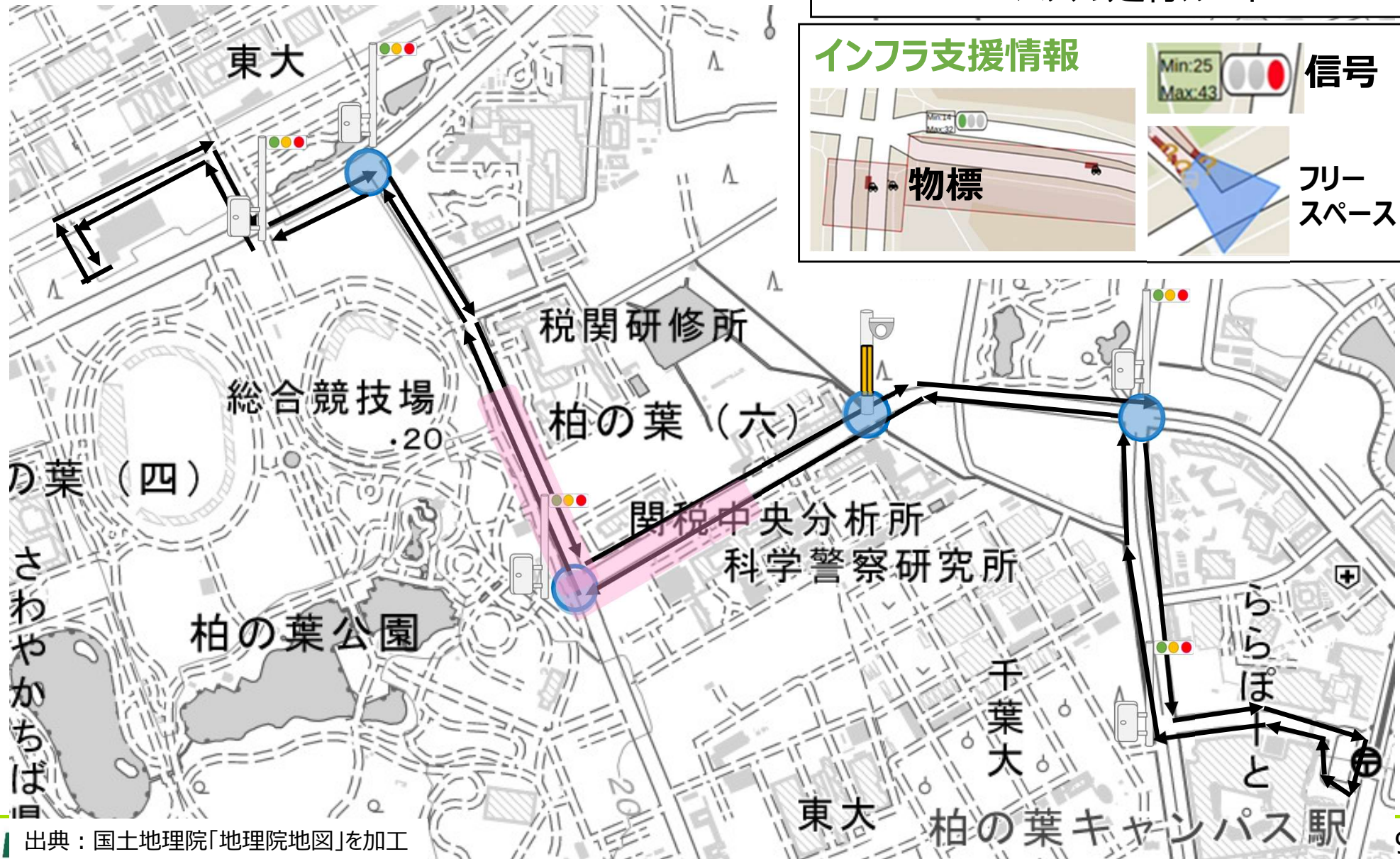
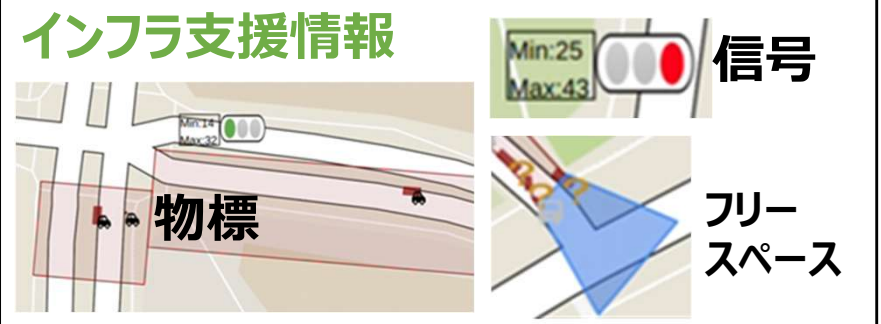
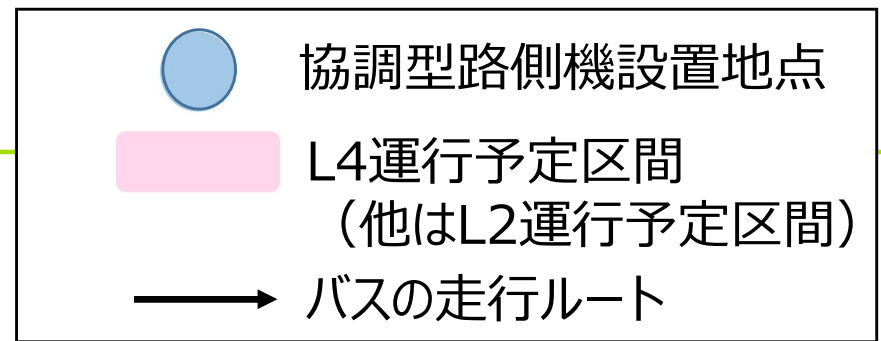
・ 車内配置図



CooL4 レベル4自動運転バス

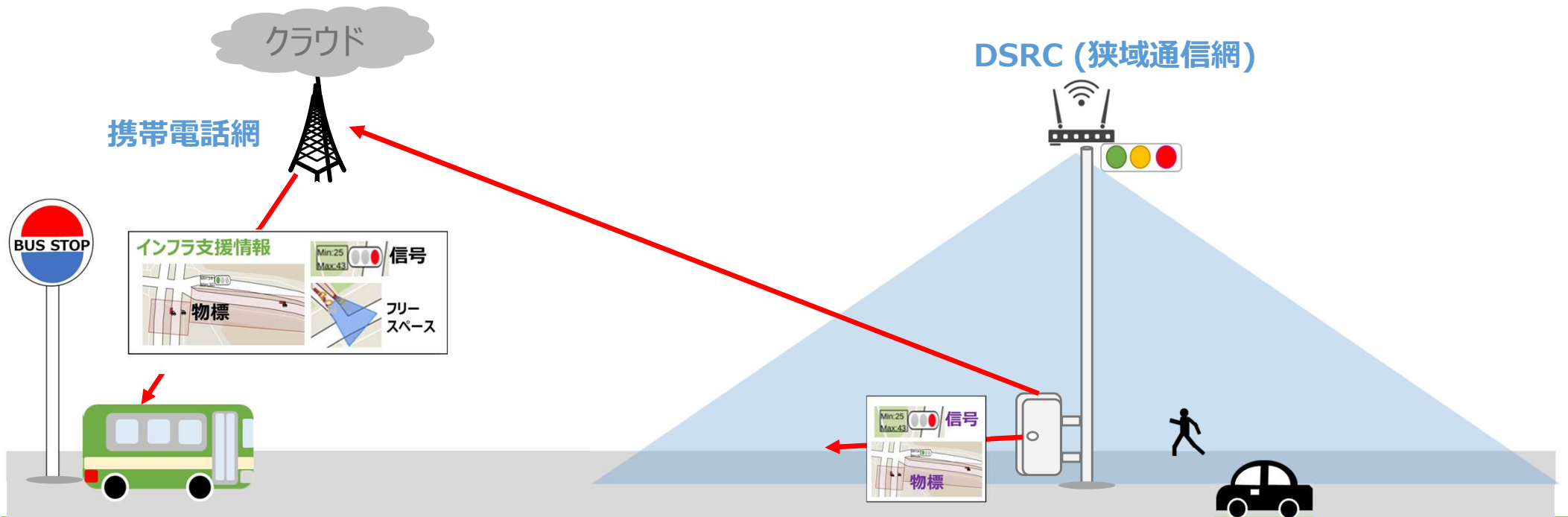
- 走行ルートと協調型路側機的位置

- バス走行中に、**4箇所ある協調型路側機**から**インフラ支援情報**を提供



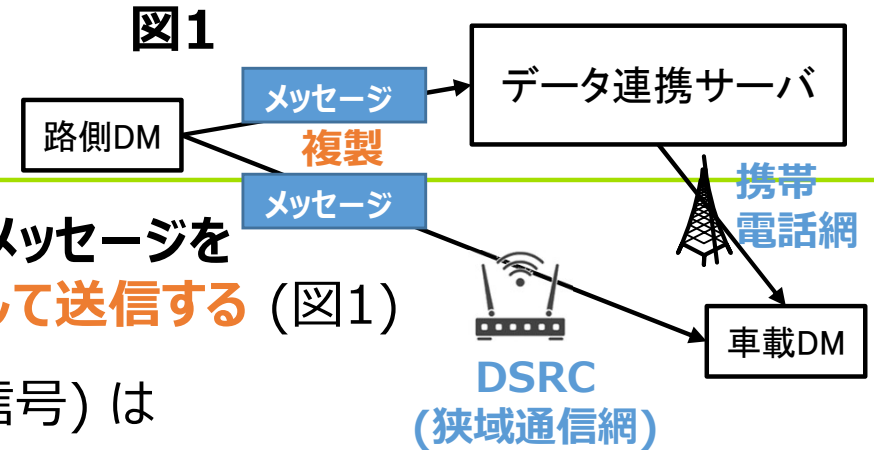
車載DMに届けられる通信路の特徴

- 2つの通信路を使って、車載DMに届けられる
 - 携帯電話網
 - **全てのインフラ支援情報（物標・信号・ freespace）** をクラウド経由で送信
 - メリット：停留所で事前に動作チェックが可能
 - デメリット：遅延のゆらぎは大きい
 - DSRC
 - 電波受信範囲内の**物標・信号情報**を送信。
 - メリット：低遅延
 - デメリット：受信範囲・帯域が狭い



車載DM内のソフトウェアの仕組み

図1



- 路側DMは物標/ freespace/ 信号毎に分けてメッセージを作成し、2つの通信路に送る際、メッセージを複製して送信する（図1）
- DSRCの受信範囲内だと、複製した情報（物標・信号）は車載DMへ二重に届くが、先に届いた方を採用する。
 - 後から届いたデータはヘッダをチェックし重複除去（図3）
- メッセージは、暗号・署名・圧縮処理（図2）がされているため、車載DM内で復号・検証・展開処理（図3）を行い、ストリーム型データベースに格納する。
 - 車載DM用ビューは、このデータベースから情報を取り出して表示
- 自動運転システムへは、UDP形式のデータに変換して送信（図3）
 - 自動運転システム側では制御・認識・ビュー表示に活用。

図2) 電文の中身

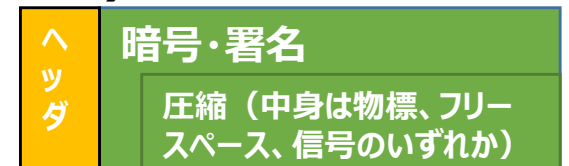
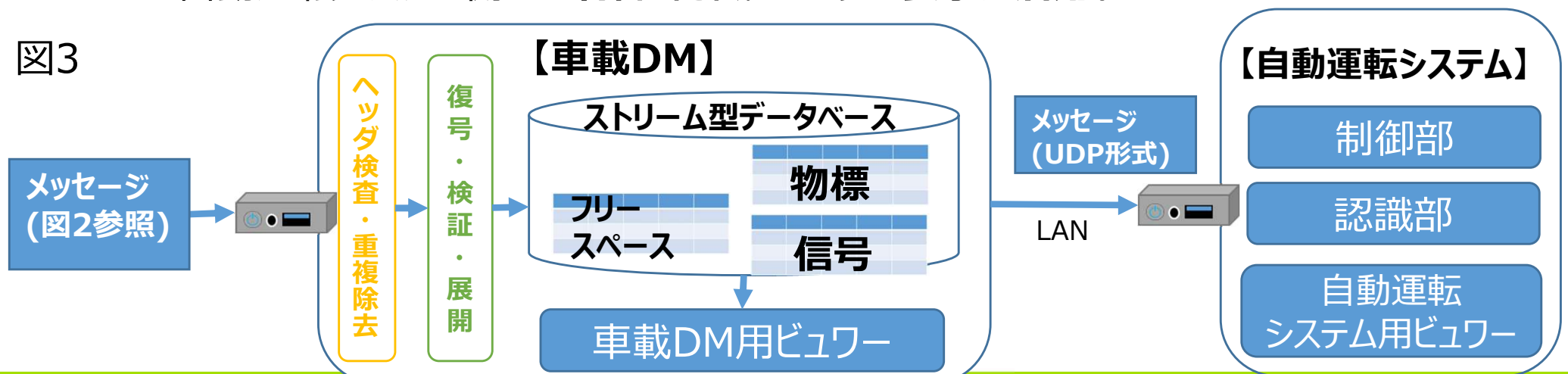


図3



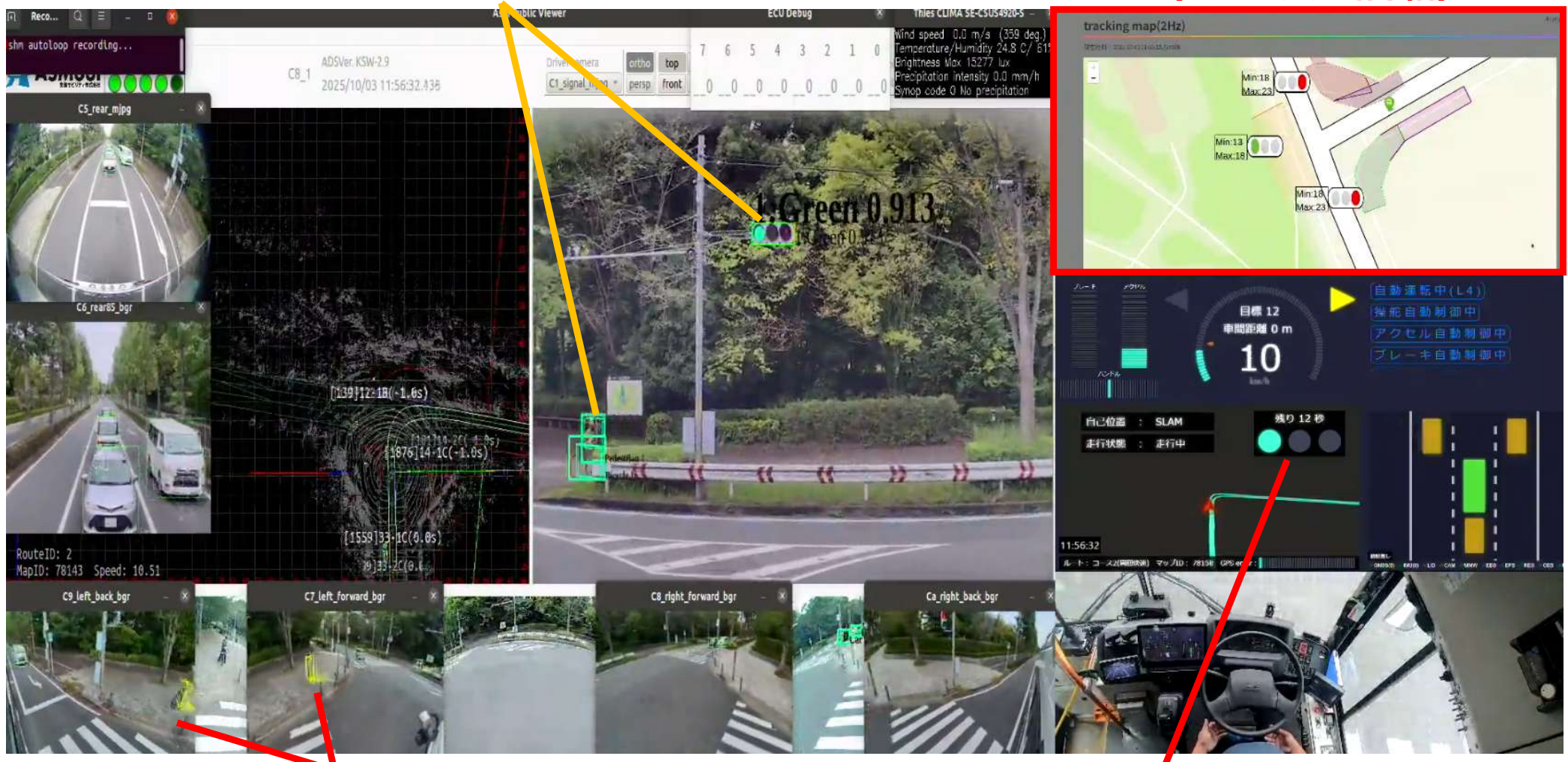
Cool4 レベル4自動運転バス

- 走行中の車内ディスプレイ表示

- ディスプレイにリアルタイムで、複数のビューを使って表示

自動運転システム単独で認識している物標・信号情報

車載DM用ビュー
(次ページにて詳細)



インフラから届けられた物標情報を
自動運転システム用ビューで表示

インフラから届けられた信号情報を
自動運転システム用ビューで表示

車載DM用ビュー - 概要

- 4箇所ある協調型路側機から届くインフラ支援情報を俯瞰視点で描画
 - バスが停留所にいる時
 - 信号情報のみ描画
 - バスが走行している時
 - 次へ向かう交差点のインフラ支援情報全てを描画



アイコンの説明

バスの現在位置



信号の灯色



信号の残秒数
(範囲)

Min: 20
Max: 25

路側機内部のセンサーを使って、認識した物標

車両



車両のサイズ

人



自転車



バイク



電車



不明



センサーの
検知範囲



フリースペース
(物標が存在しない
領域を動的に生成)

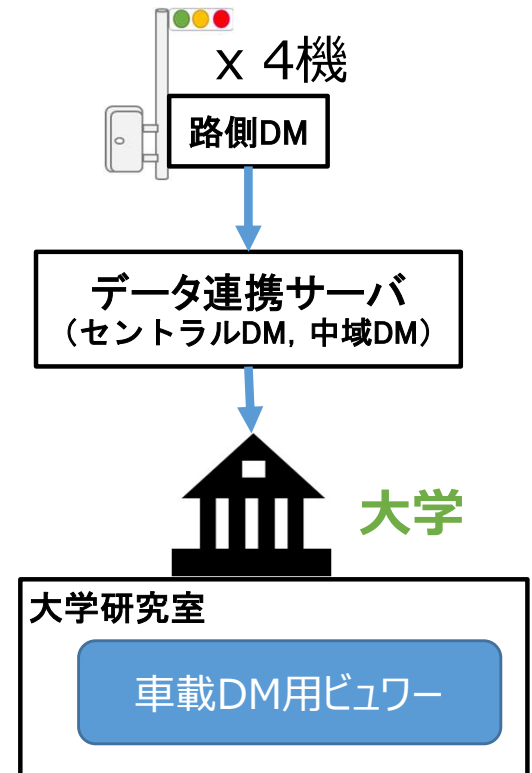


車載DM用ビュー

- 路側機の遠隔監視にも活用

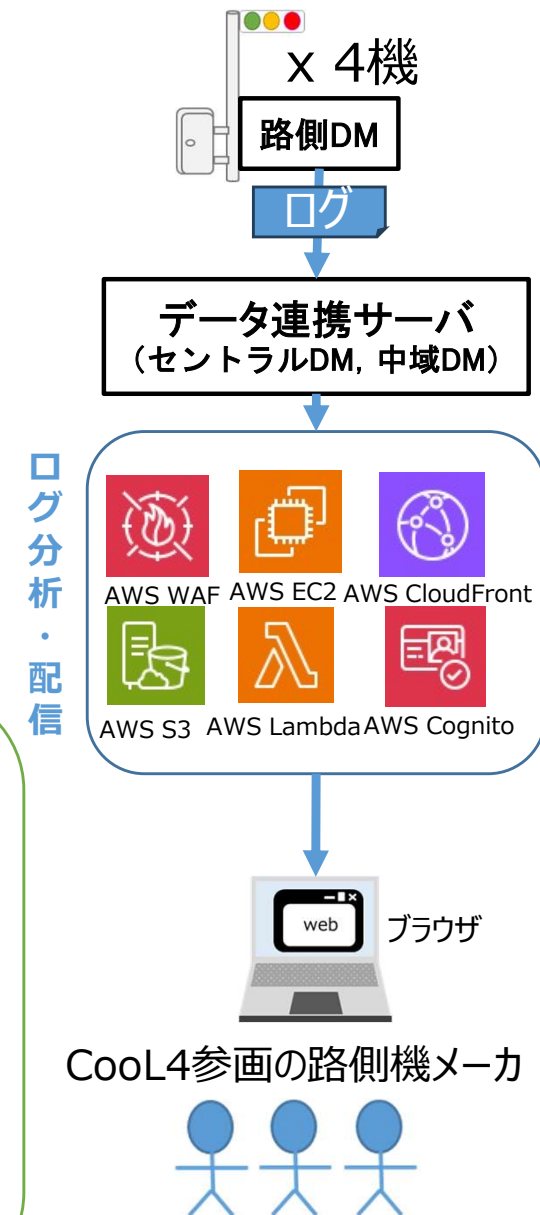
- データ連携サーバを通して、**協調型路側機の4機全ての情報を送信**
 - 走行ルート上の各交差点の状況が、全て捉えられる。

大学研究室の様子



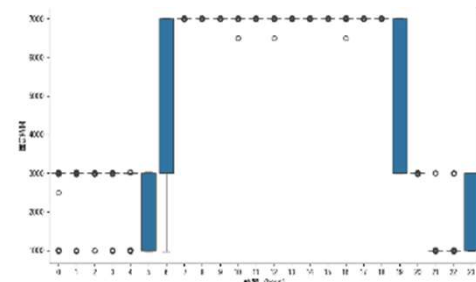
補足) データ連携サーバ内での分析・配信

- 協調型路側機内の**ログをクラウド上で分析し、関係者にのみ配信する仕組み**を構築
 - 利用場面 1 (センサー設置時)
 - 物標の検出数やプロット状況をすぐさま連携
 - センサーの画角調整やパラメータ調整に寄与
 - 利用場面 2 (長期的な分析)
 - 継続的にデイリーで分析結果を配信**
 - 路側機メーカーはブラウザ上で状態をモニタリングしつつ、カイゼン活動続ける事が可能。

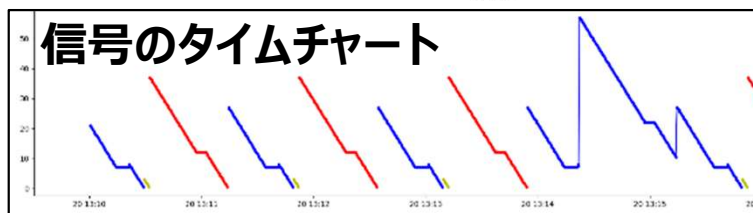


分析結果例

時間毎の傾向



信号のタイムチャート



物標のプロット状況



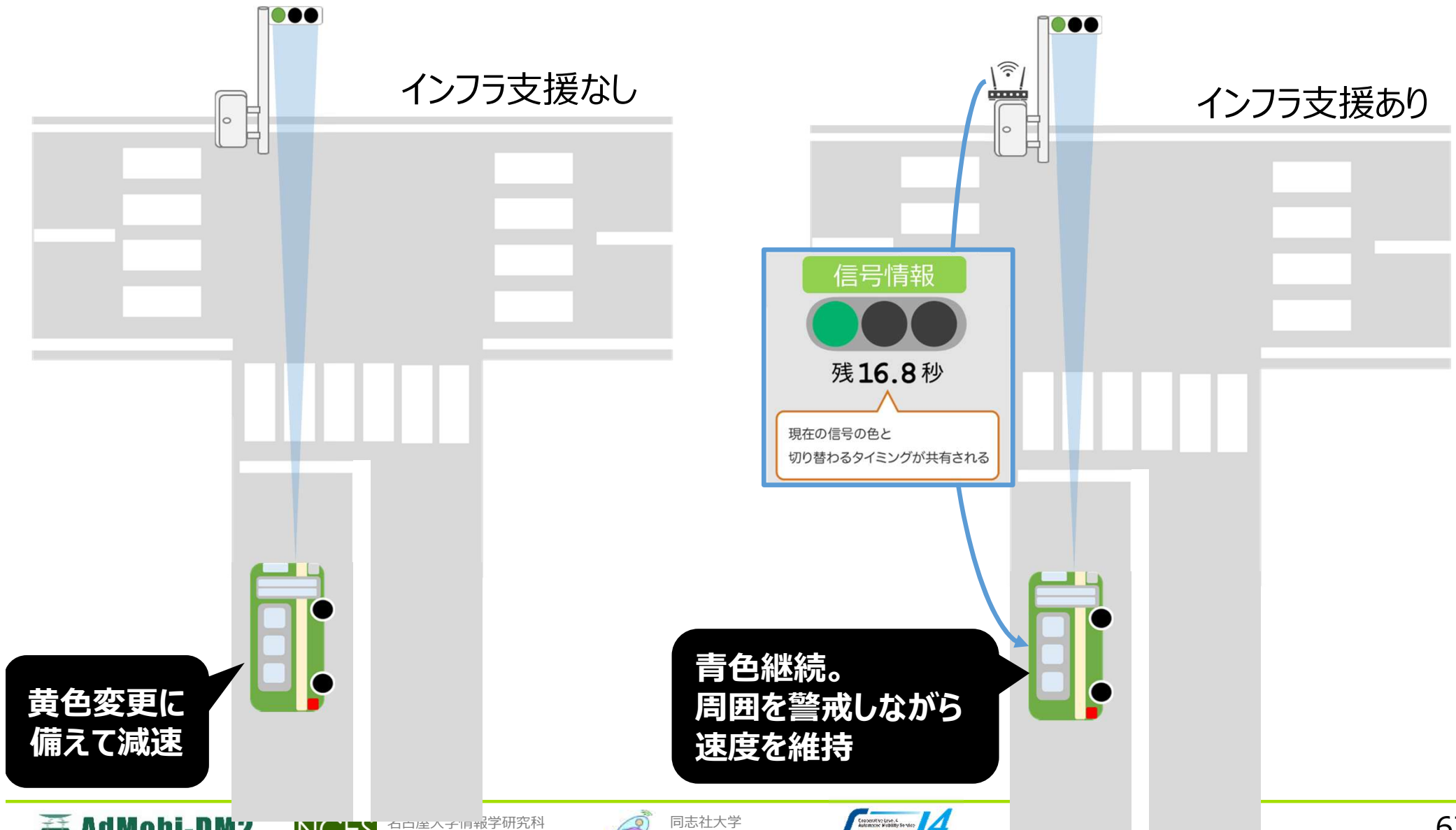
Map Data From OpenStreetMap

-
- 自動運転バスの交差点通過支援
 - 信号灯色の変化を先読みした交差点通過判断
 - 物標情報を活用した交差点通過判断

自動運転バスの交差点通過支援

- ユースケース1「信号灯色の変化を先読みした交差点通過判断」(1)

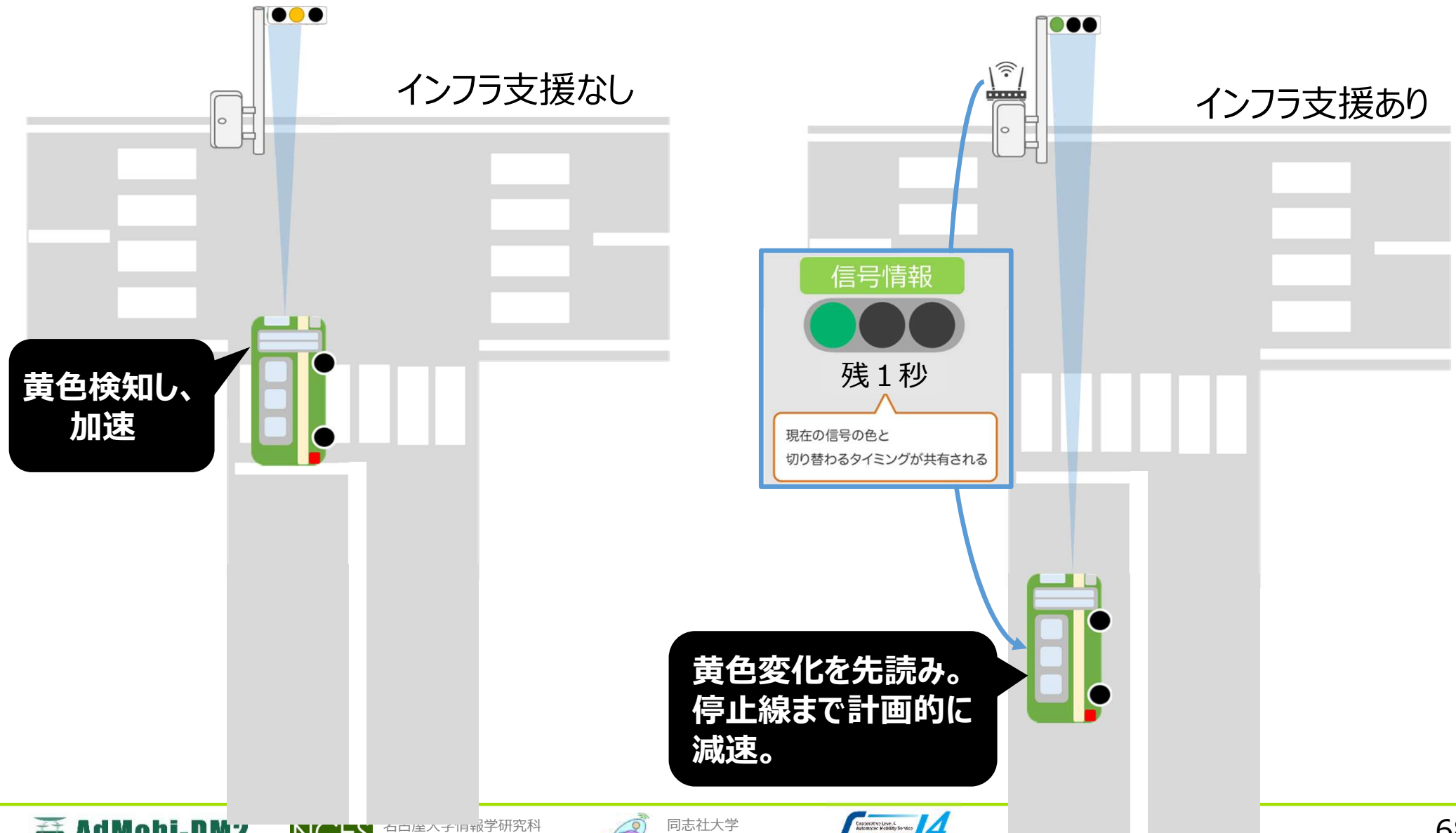
- **信号の灯色が変化する予定時間**をバスに知らせる事で、バス側は、
信号灯色の変化を先読みした交差点通過判断ができる → **円滑性向上**



自動運転バスの交差点通過支援

- ユースケース1「信号灯色の変化を先読みした交差点通過判断」(2)

- 停止線を超える前に、黄色・赤色になる変化を先読みし、停止線まで安全に減速。 → **急加速による車内事故のリスク低減**



自動運転バスの交差点通過支援

- ユースケース1「信号灯色の変化を先読みした交差点通過判断」(3)

- 黄色・赤色になる変化を先読みし、**停止線まで計画的に減速**している様子

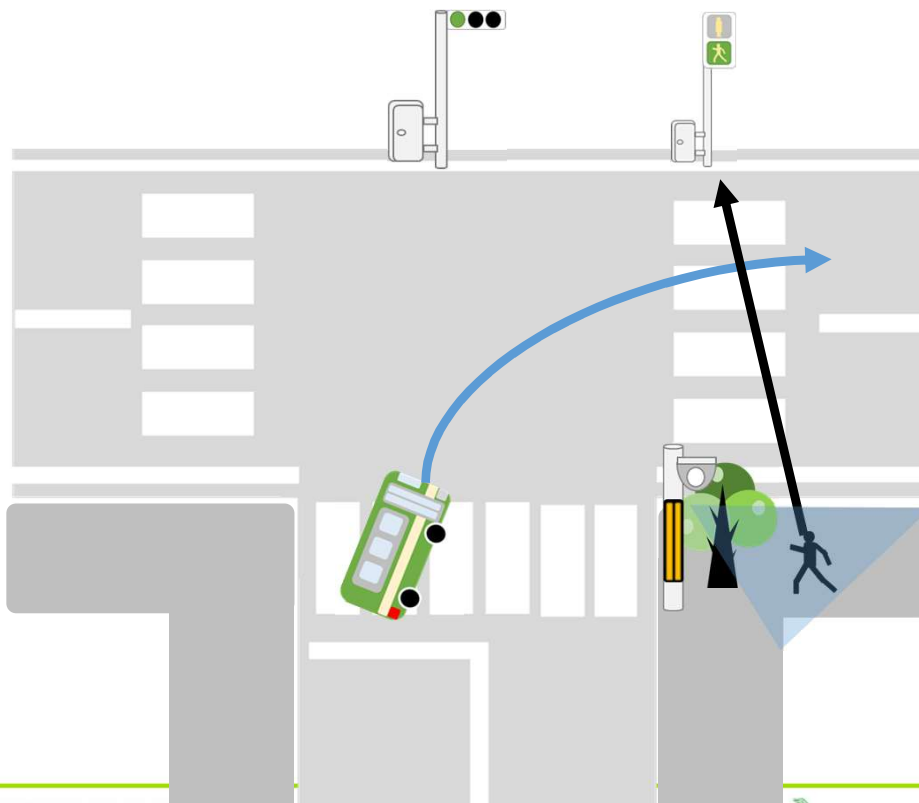


自動運転バスの交差点通過支援

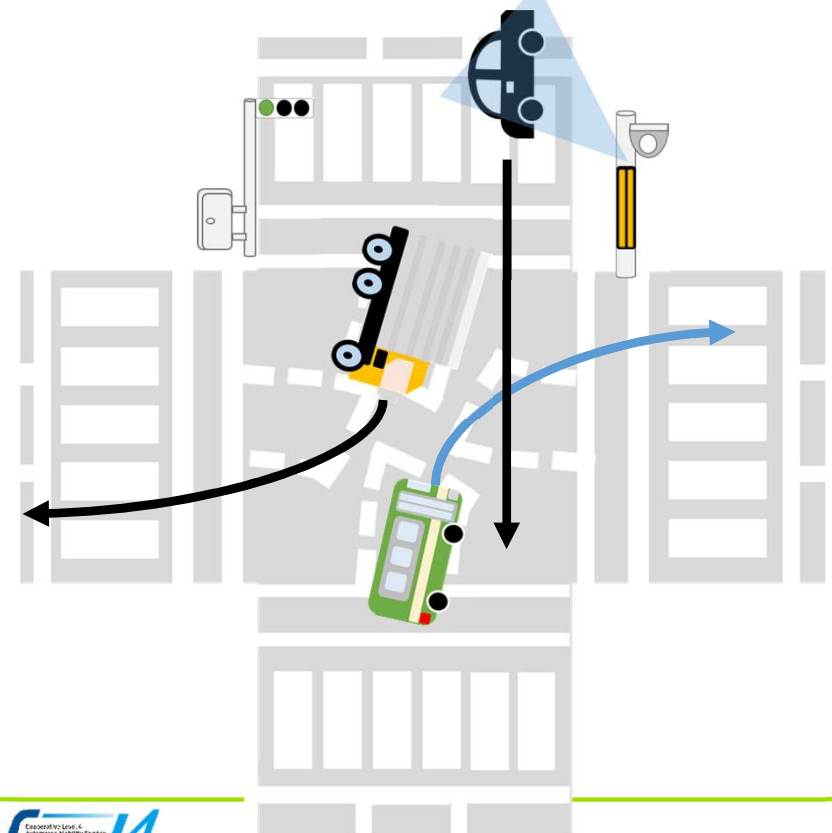
- ユースケース2「物標情報を活用した交差点通過判断」

- **車載センサーから死角となる物標を知らせること**
 - 自律のみの走行課題
 - 死角が解消されるまで低速で徐行する必要がある。
 - インフラ支援の効果
 - **既定範囲内**に物標が存在する場合は、計画的に停止
 - 物標が存在しない場合は、低速徐行せずに発進可能 → **円滑性向上**

i) 既定範囲：交差点右折先の横断歩道

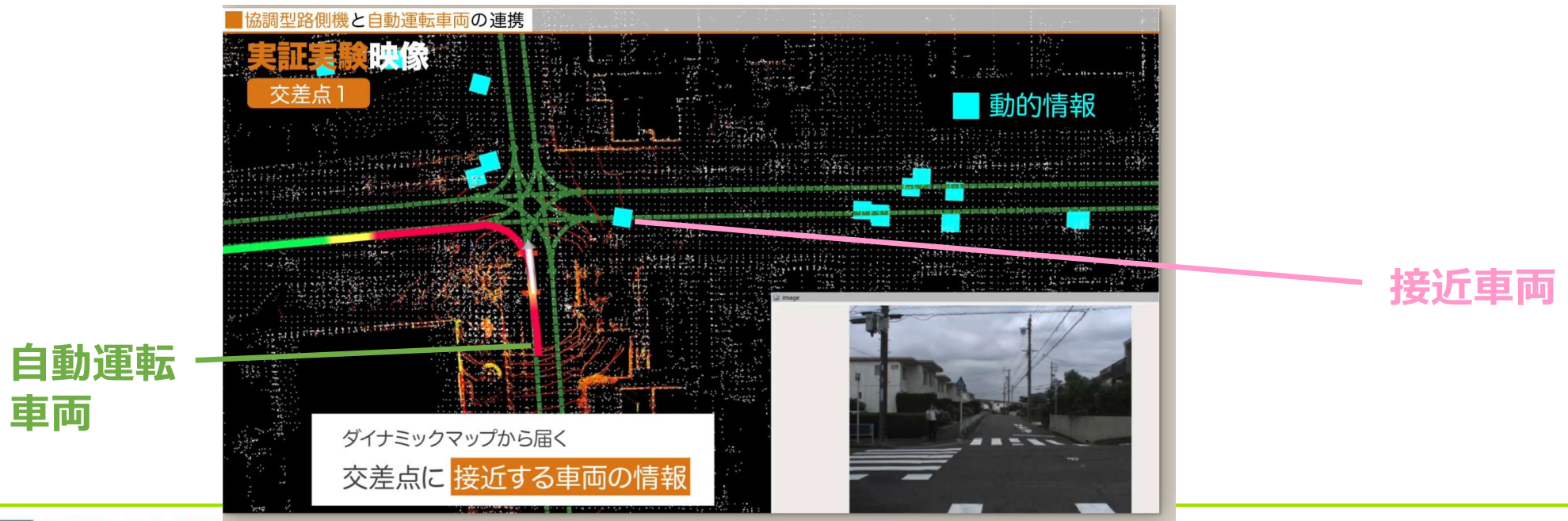


ii) 既定範囲：交差点右折時の対向車線



ユースケース2「物標情報を活用した交差点通過判断」 - 各地域での取り組み状況

- 柏の葉の実験内では、
制御へ反映せず、機能検証を行っている段階
 - 受信ログによる機能検証
 - 自動運転システム内のビューア表示（右図）
 - 仮想空間シミュレーションを用いた活用効果検証
- 高蔵寺では制御に反映した機能検証を実施済
 - 交差点左折時において、DMが**接近車両**の情報を連携し、**自動運転車両**がその情報を制御に活用（下図、次ページに動画）



ユースケース2「物標情報を活用した交差点通過判断」

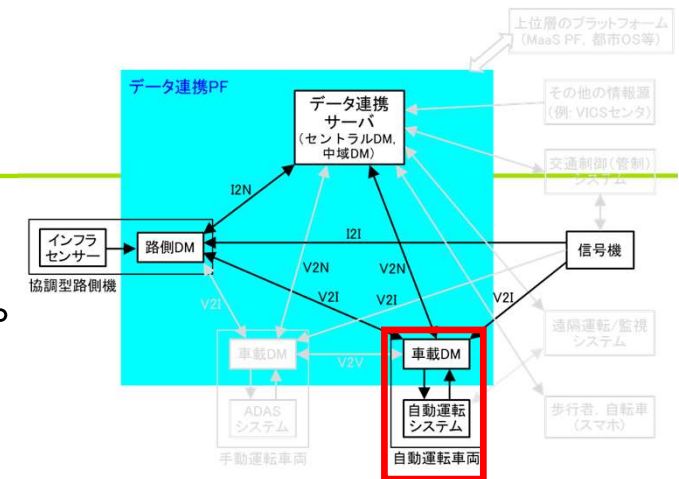
- 高蔵寺での実証実験の様子（動画）

- 交差点左折時において、DMが**接近車両**の情報を連携し、**自動運転車両**がその情報を制御に活用。**接近車両**が通り過ぎるまで**計画的に停止**した後、左折する。



まとめ

- Cool4で取り組んでいるユースケースと自動運転車両内（自動運転システムと車載DM）の仕組みについて紹介した。
- レベル4自動運転車両においても、我々の情報通信プラットフォームを利用することで、協調型路側機のインフラ支援情報が有用である事が確認された。



出典：国土地理院「地理院地図」を加工

物標情報を活用した交差点通過判断



信号灯色の変化を先読みした交差点通過判断



補足) 柏の葉における5G/LTE (携帯電話網) 利用について

- 協調型路側機1機が5G/LTEを利用するにあたって必要になる帯域

コンテンツ	帯域
物標 30件 ※1,2	144 kbps
信号 5件 (灯器IDのリストの数) ※1,2	40 kbps
参考) ストリーミング動画	低品質 (720p,15fps) : 800 kbps 高品質 (4K) : 12 Mbps

- 1ヶ月あたりの通信量
 - 毎日朝～夕方の12時間、配信を続けた場合の通信量。

コンテンツ	通信量 / 月
物標 30件 ※1,2	22 GB
信号 5件 (灯器IDのリストの数) ※1,2	6 GB
両方	28 GB

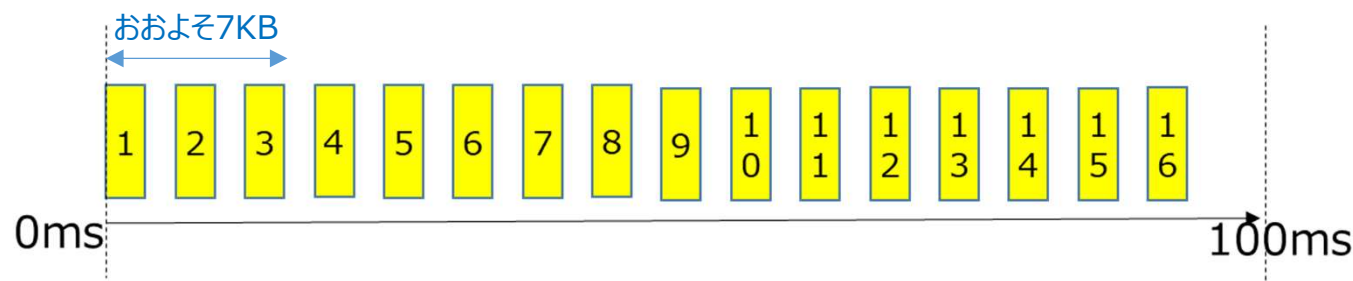
※ 1 : 100ミリ秒間隔で通信した場合の帯域 (圧縮率は変動するため、おおよその値)

※ 2 : 協調型路側機に取り付けるセンサーの数、信号灯器IDのリストの数が多い場合、必要になる帯域・通信量は増加する。

「信号灯器IDのリスト」については、CooL4 データ連携PF API仕様を参照。

補足) 柏の葉におけるDSRC (狭域通信網) 利用について

- ITS無線機の仕様
 - 100ミリ秒を1つの制御単位として、路車間通信で利用できる時間帯をスロット (下記、黄枠) として定義
 - 複数の路側機が同じ周波数帯で電波を発射すると、干渉してしまうため、**1交差点あたり利用できるスロット数は、最大3スロットまで。**
 - 3スロットでおおよそ 7 KB 送信可能



- 仕様に基つき、柏の葉では、1交差点あたり最大3スロットを利用

100ミリ秒あたりに送信する件数と必要になる帯域 (※圧縮率は変動するため、おおよその値)

	30件	70件	120件		5件
物標	1.5 KB	3 KB	6.5 KB	信号	0.5 KB

- 物標数が少ない交差点：信号と物標両方が最大3スロットに収まる。
- 物標数が多い交差点：最大3スロットに収まらなくなる可能性が生じるため、信号 or 物標どちらかを送る。