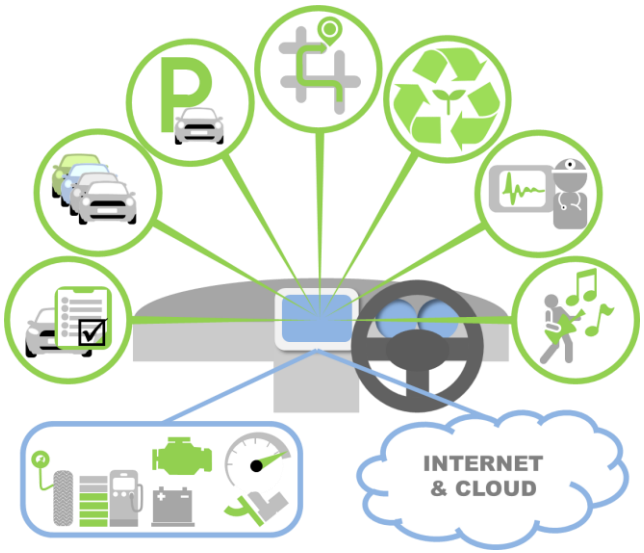
資 料 5

コネクテッドカーにおけるプライバシー保護について



- コネクテッドカーについて
- コネクテッドカー機能やアプリケーションの全体像
- コネクテッドカーで取り扱われるデータ例
- プライバシー保護対策の基本的方向
- 国際標準勧告等によるプライバシー保護機能
- コネクテッドカーにおける課題
- KDDI総研の取り組みの紹介

KDDI総研
主席研究員　平林 立彦

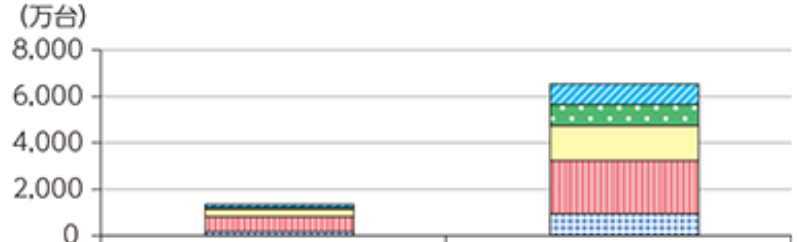
コネクテッドカーについて

コネクテッドカー

コネクテッドカーとは、ICT端末としての機能を有する自動車のことであり、車両の状態や周囲の道路状況などの様々なデータをセンサーにより取得し、ネットワークを介して集積・分析することで、新たな価値を生み出すことが期待されている。

市場規模

富士経済によると、2014年のコネクテッドカーの世界市場は、1,300万台以上となり、スマートフォンを含むモバイル端末連携型のコネクテッドカーを中心に今後、更に拡大すると予想されている。2025年は新車のコネクテッドカーと既存車のコネクテッド化を合わせて、2013年比6倍弱の6,500万台を超えると予測されている。



	2014年（見込）	2025年（予測）
合計	1,350	6,547
その他	131	886
中国	78	925
欧州	324	1,498
北米	650	2,284
日本	167	954

【出典】平成27年版情報通信白書

コネクテッドカー機能やアプリケーションの全体像

高度運転支援(ADAS)※1
・車車間衝突防止
・隊列走行支援
・緊急ブレーキ
・車間／車線維持支援
・渋滞走行支援
・狭路通過支援
・駐車支援
・歩車間事故防止

		次世代プローブデータ※2	車両診断・車両位置
		運転歴対応型保険	盗難・当逃げ等警報
		緊急通報(e-Callなど)	運転コーチング
道路環境・路面監視	車両監視・診断※1	充電制御	注文・支払
交通標識・信号監視	運転者視線監視	道路交通情報	カーシェア予約
運転者への注意・警報	運転者健康監視	高機能ナビゲーション	ドア施錠・開錠
AIコンシェルジェ	AR/死角低減	LBS (イベント案内等)	ナビ・エアコン設定
EV 車向けサウンド	イルミネーション	インターネットラジオ	SNS・メッセージ対応

セキュリティ＆プライバシー管理機能

※1 ADASや車両診断はConnected Carアプリケーションに含まれないが、これらによる警報は含まれる場合がある。
※2 車両及び車両内への持ち込みセンサーなどにより観測された様々なデータが含まれる。（スライド４参照）

コネクテッドカーで取り扱われるデータ例

ISO22837及びW3C Vehicle Data仕様案*等をベースに整理

【凡例】＊http://www.w3.org/2014/automotive/data_spec.html
アンダーライン：ISO22837と重複規定項目　　赤字：プライバシーや企業機密に抵触する可能性の高いもの
[…]内の項目は、W3C等で検討中の項目或いは今後の検討対象

- **時刻情報（タイムスタンプ）**
  - 事象の発生時刻(yy/mm/dd/ hh:mm:ss)
- **位置・方向情報**
  - 緯度・経度・高度・向き（リンク／コード属性情報、距離標位置含む）
  - 車線内位置、車両内位置（Zone）
- **車両属性情報**
  - 車両分類、車両識別番号・鍵ID、ブランド・車種・年式
  - 駆動源、燃料種別、ミッション、[最小旋回半径]
  - 車長、車幅、車高、車重、ドア数、車輪サイズ
  - [車重、軸重]等
- **車両走行状態**
  - エンジン始動・停止（イグニッションキーの位置）車速、加速度(V/H)、トルク、エンジン回転数、Pブレーキ
  - 車輪スピード、ハンドル回転角、ヨーレート
  - アクセル／ブレーキのペダル位置 、スロットル位置、ギヤ オドメータ／トリップメータ、燃料残量、燃費、各ボタン
  - 走行モード、クルーズ・コントロール（速度含む）
  - 前照灯／ハザード／駐車灯及び室内点灯、ウインカー
- **安全運転情報**
  - ABS、シートベルト、エアバッグ、ESC/TCS、接近警報
  - ドア／窓の開閉、チャイルドロック状態、乗車状態
- **気象条件情報**
  - 車内外温度・湿度・気圧、降雨、
  - ワイパー・デフロスター状態
  - エアコン状態（冷暖房、設定温度、ファン強弱／向き）
  - [太陽高度、日陰・日向、降雪、霧]
- **運転環境情報**
  - [道路線形、サグ、路面、信号機、遮断機、道路標識]
  - [障害物、歩行者数・状態※]
  - ※　クラウドにて画像情報を収集し歩行者特徴量を抽出・提供
- **車両メインテナンス情報**
  - [事故・故障履歴] 、異常警報
  - エンジン稼働時間、走行距離／時間
  - エンジン／ミッションオイル、冷却水温、クラッチの滑り
  - タイヤ空気圧、バッテリー状態、ウオッシャ液少量
- **車両パーソナル化情報**
  - 単位系/言語、室内表示照度／レイアウト／色彩
  - [ナビ情報（出発地、目的地、経由地、経路）]
  - [運転行動・操作履歴]
  - 最高速度、ミラー類調整角、シート／ハンドル位置、チャイム
  - サンルーフ／コンバーティブル開閉、走行効果音
- **データ管理情報**
  - 利用可能なデータ項目（個人向け、OEM向け）
  - [データ保存期限、精度]
- **サービス・アプリ管理情報**
  - [デバイス／OS・アプリ認証]
  - [サービスID]
  - [アクセス／利用／購買履歴]
- **運転者・同乗者情報（取得・保存可能な場合）**
  - 運転者・同乗者ID
  - [生体情報（血圧、脈拍、既往症、認知的負荷、眠気、疲労）]

課題：　多くのアプリケーションが時刻・位置情報が重要であり、それらが匿名加工されてしまうと、情報の利用価値が著しく損なわれる場合が多く、一方、時刻・位置情報をキーに異なるデータベースの連結が容易

プライバシー保護対策の基本的方向

- **個人情報保護法等、各国の法制度遵守**
  - EU：General Data Protection Regulation案含む
- **プライバシー・バイ・デザイン(PbD)基本7原則の準拠**
  - Proactive/Preventative-予防的
  - By Default-初期設定化
  - Embedded-組込み
  - Positive-Sum-メリットの組合せ
  - Visibility/Transparency-可視化／透明性
  - Lifecycle Protection-ライフサイクル保護
  - Respect for users-利用者尊重

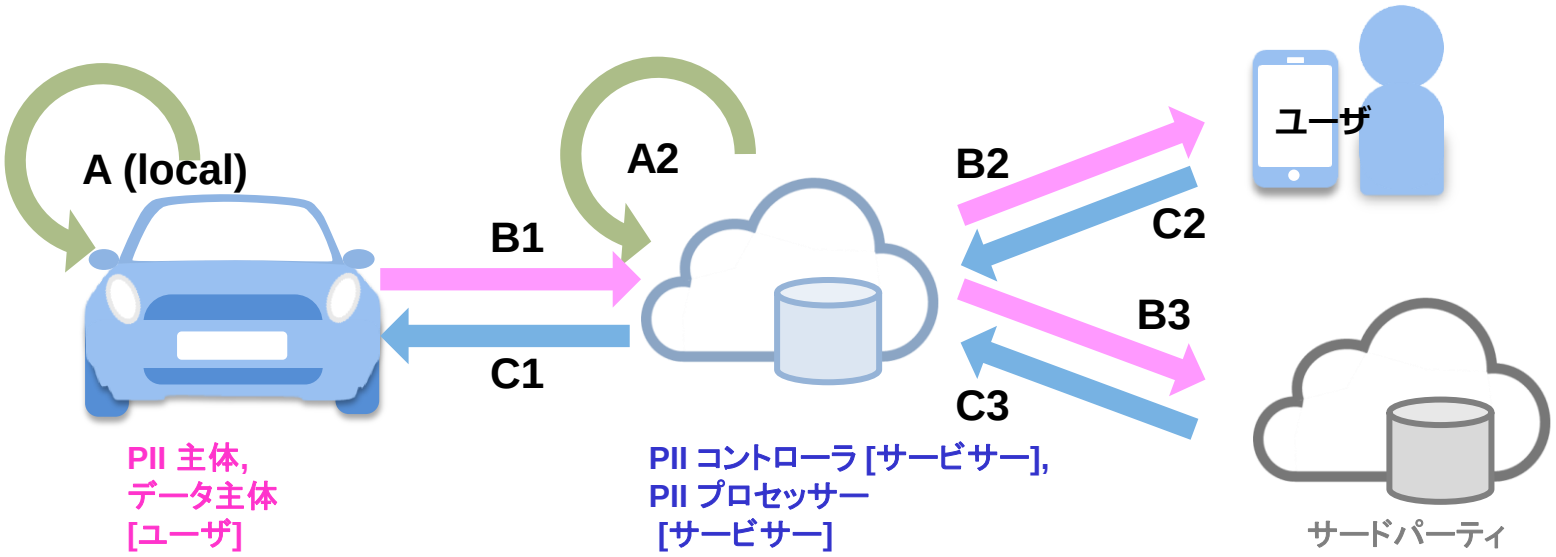
  https://www.privacybydesign.ca/index.php/about-pbd/
- **国際標準勧告等の準拠※**
- **コネクテッドカーの問題への対応**
- **業界・企業の自主規制**
  - ドイツ：Datenschutz im Kraftfahrzeug - Automobilindustrie ist gefordert（第88回ドイツ連邦及び州政府のデータ保護委員会議決議）：自動車におけるプライバシー保護決議（2014年10月8・9日）
  - 米国自動車工業会（AAM）及びグローバル・オートメーカ協会（AGA）：PRIVACY PRINCIPLES FOR VEHICLE TECHNOLOGIES AND SERVICES（2014年11月12日発表）
  - 欧州自動車工業会：ACEA PRINCIPLES OF DATA PROTECTION IN RELATION TO CONNECTED VEHICLES AND SERVICES（9月11日発表）

※ 国際標準勧告等

- ISO/IEC 29100:2011 プライバシーフレームワーク http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123
- THE OECD PRIVACY FRAMEWORK http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm
- CONSUMER DATA PRIVACY IN A NETWORKED WORLD https://www.whitehouse.gov/sites/default/files/privacy-final.pdf
- FTC REPORT: Protecting Consumer Privacy in an Era of Rapid Change https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf
- FTC Staff Report: internet of things Privacy & Security in a Connected World https://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf
- APEC PRIVACY FRAMEWORK http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx2015

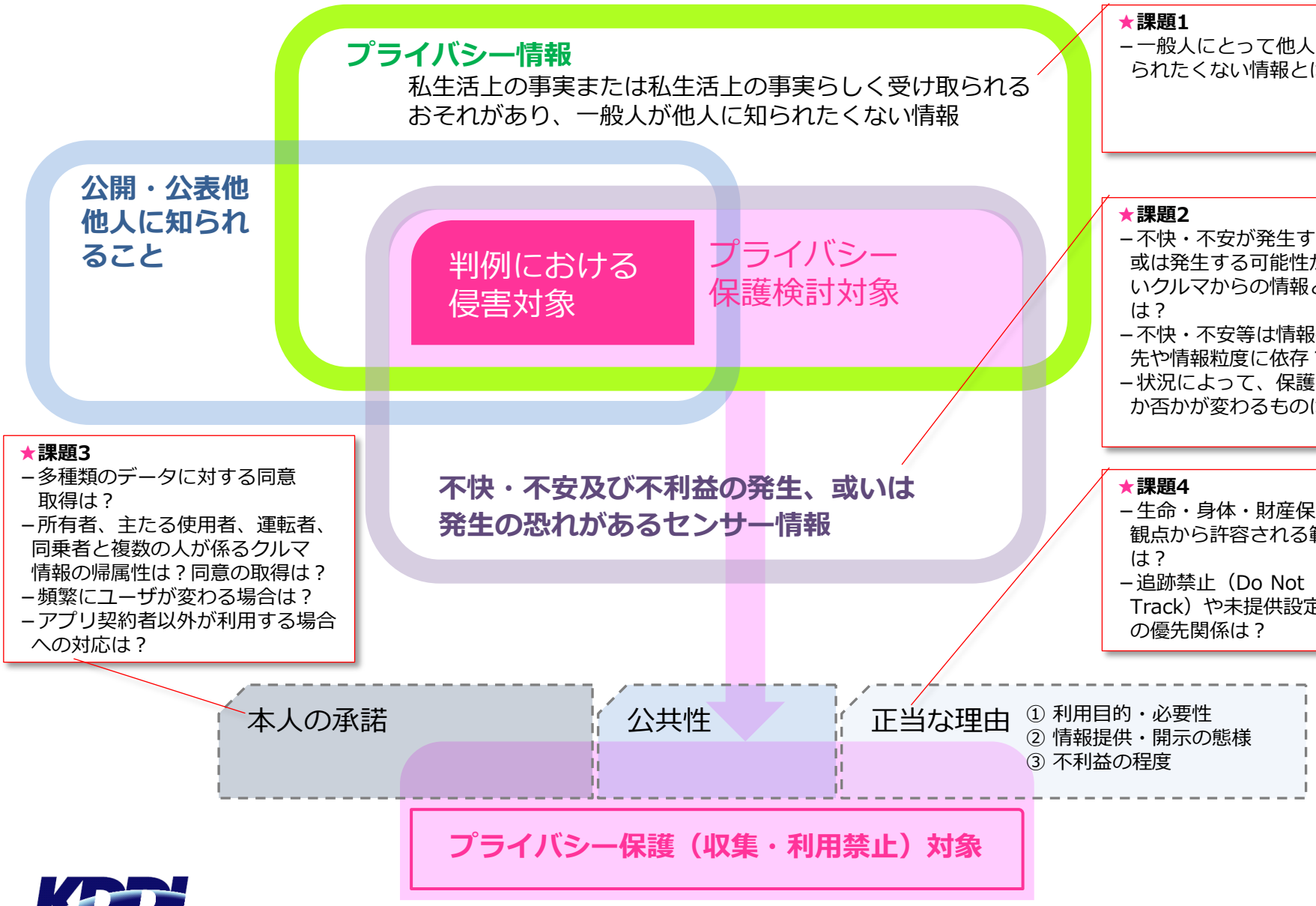
国際標準勧告等によるプライバシー保護機能

- 利用者の選択権設定と同意取得
  - 選択不要データ
  - 事前同意が必要となるデータ
- 利用者のデータ・アクセス権／参加権
  - 閲覧
  - 追跡禁止
  - 修正・消去
  - 忘れられる権利
- データの使用目的の明確化
- データ収集・保管の制限・最小化
- 利用制限
- データ品質・精度
- データ・セキュリティ
- 二次利用の許可と管理
- プライバシー管理の透明性



PII: Personally Identifiable Information

コネクテッドカーにおける課題



課題１　他人に知られたくない情報とは？

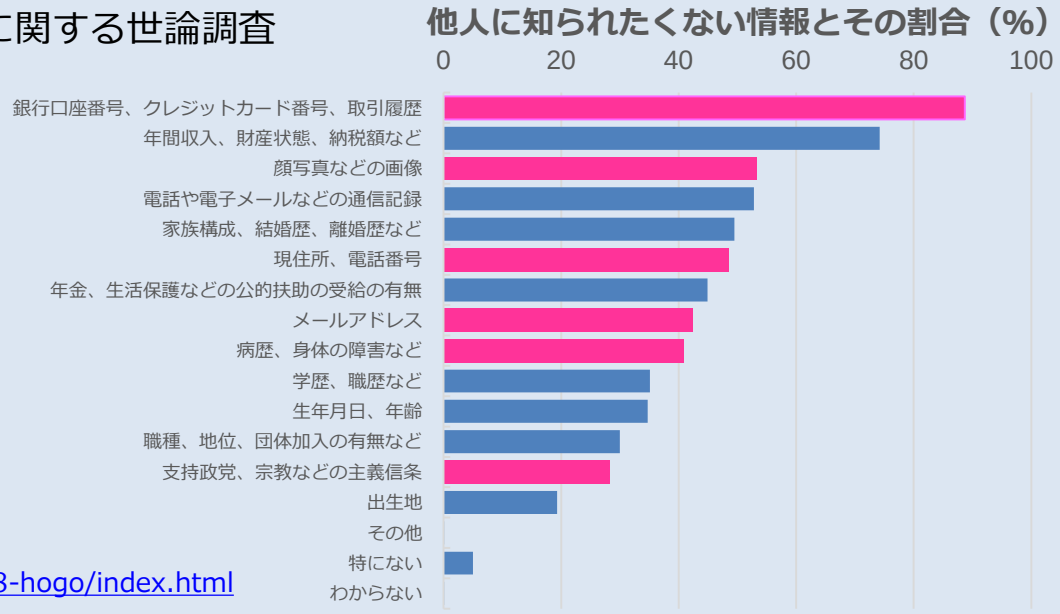
■ 機微情報

- **JIS Q15001: 2006**
  - 思想，信条及び宗教に関する事項
  - 人種，民族，門地，本籍地，■身体・精神障害，犯罪歴，その他社会的差別の原因となる事項
  - 勤労者の団結権，団体交渉及びその他団体行動の行為に関する事項
  - 集団示威行為への参加，請願権の行使，及びその他の政治的権利の行使に関する事項
  - 保健医療及び性生活
- **OECD**
  - 社会的差別を受けうる情報

■ その他、他人に知られたくない情報

- **経済的・身体的被害を受けうる情報**
  - ■ 銀行口座番号、クレジットカード番号
  - ■ 個人信用情報
  - ■ サービス利用者ID・パスワード
  - ■ 指紋、身体的特徴 （個人識別性の高い特徴）
  - ■ 日常の生活習慣・行動（違反）・住所
- **情報開示の受容性に個人差がある情報**
  （不安・不利益の程度に個人差あり）
  - 電話番号・メールアドレス・ハンドルネーム
  - 趣味・嗜好、性格
  - 交友関係、学歴・結婚歴

【参考】内閣府個人情報保護に関する世論調査



＜凡例＞
■　：車両内外で今後直接取得可能、或は可能となりうる情報

http://survey.gov-online.go.jp/h18/h18-hogo/index.html

課題2　クルマからの情報の不安等に対する検討

- **不快・不安・不利益が発生する、或は発生しうる情報**
  - **課題１での機微情報及びその他、他人に知られたくない情報**
  - **上記情報が推定可能となる情報**
  - **ただし、これらは下記条件で異なる**
    - 個人
    - 情報提供先
    - 対象情報とその粒度
    - 情報の発生状況

- **情報の組合せによりセンシティブ性が高まる例**
  - 交通違反
    - 車速、位置情報
    - シートベルト
    - パーキング・ブレーキ
    - 乗車人数
  - 自宅・行先
  - 走行ルート

  など

- **不快・不安等を軽減する措置**
  - 情報提供先に応じた対象情報の選択及び粒度変更
  - 情報の一般化・匿名化

課題3　同意取得に対する検討

- **多数のデータ種別に対する合理的かつ効率的な同意取得と個人設定の自由度は？**
  - **自動車のセンシングデータに対する全面利用許諾／収集拒絶**
  - **カテゴリー別設定**

    【一例】
    - 運転の安全性に係るデータ
      - エアバッグ、ABS、故障診断、
      - ドア・窓開閉
    - 自動車のステータス情報
      - イグニッション、バッテリー、燃料、シート位置、ハンドル／ミラー設定位置
    - 運転記録
      - 時刻・位置情報、目的地、ルート
      - アクセル、ブレーキ、ハンドル、速度、燃費等
    - 運転環境
      - 気象、気温、湿度、CO2、道路線形
      - 他の車両や歩行者の動き等
    - 一般的な個人情報
      - 携帯電話番号、メールアドレス
      - 加入サービスID/ PW、注文・支払
      - 音楽等の趣味嗜好
  - **全項目の個別設定**

- **所有者、主たる使用者、運転者、同乗者と複数の人が係るクルマ情報の帰属性と同意の取得は？**
  - **運転者・同乗者識別性に依存**
    - マルチユーザで個人識別が可能であれば、個別に同意が必要（同乗者を含む）
    - 同乗者の同意なしでも、運転者の同意があれば、乗車人数の情報利用に問題はないか？
  - **データの帰属性=同意主体**
    - IDによる整理（デバイスID、免許証、指紋など）
    - 生体情報（顔写真、指紋、虹彩、声紋）
    - 推定情報（運転癖、シート／ハンドル位置、音楽）
  - **カーシェアなどで頻繁にユーザが変わる場合も基本は、上記のとおり対応**
  - **乗車時ごとの設定・抹消の簡便化は必須**
  - **アプリ契約者以外が利用する場合への対応は？**

    将来的にはＩＤによる個別管理
    - 従量制課金サービス
    - レコメンデーション／カスタマイゼーションに影響（誤差）が生じる

- **将来的な同意取得方法の方向性に対する国際的コンセンサスが重要**

課題4　同意原則の例外に対する検討

■ 同意原則の例外事由

- **法令による場合**
- **緊急避難**
- **生命・身体・財産保護**

【想定される事例】

- 運転者、同乗者、歩行者等の生命を守る、或いは負傷等から救済するため、合理的に必要となる場合
- 盗難されたと合理的に認定される車両の位置特定又は発見支援を行うため、必要となる場合
- 凶悪犯罪捜査（誘拐、テロ、殺人等）に、車両の位置特定又は発見支援を行うため、法的権限内において合理的に必要となる場合
- 天変地異等の発災時（橋梁倒壊、トンネル崩落、落盤等）における被災車両・被災者の特定又は発見支援を行うため、法的権限内において合理的に必要となる場合

■ プライバシーポリシー

- **同意の例外事由についてはプライバシーポリシーに規定**
- **Do Not Trackと例外事由との優先性を明記**
- **例外ルールを適用可能とするアプリやデータ送付先の分別が必要**

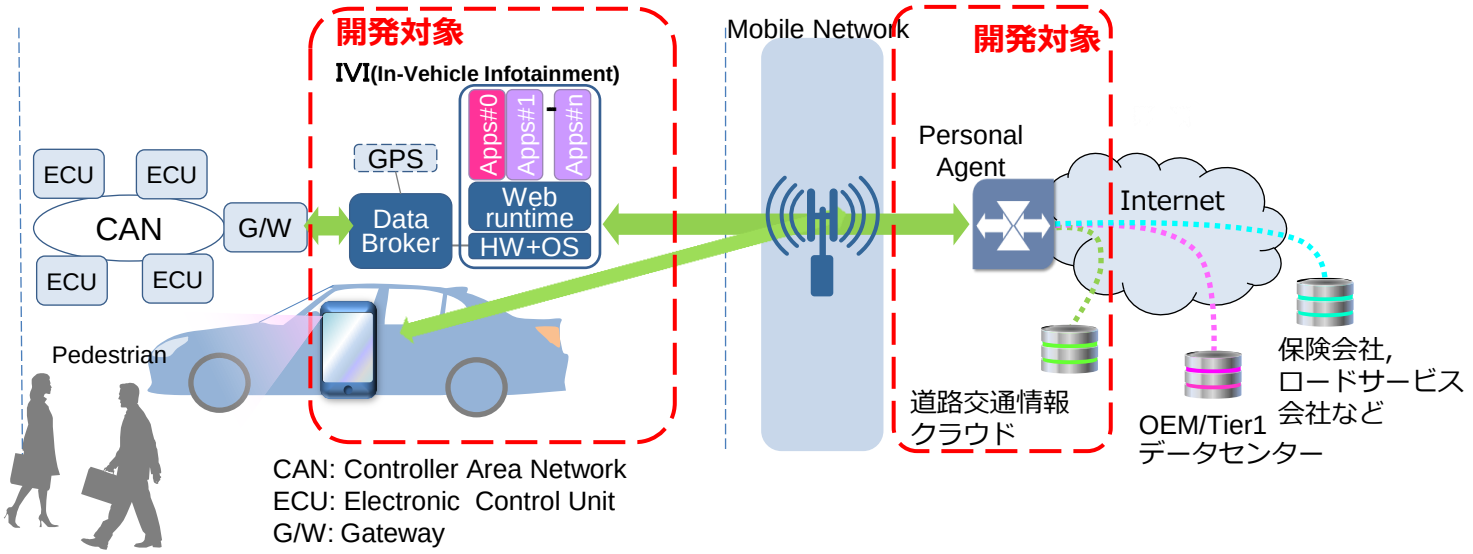
■ その他例外事由として検討すべき事項

- **危険予知・危険回避のための情報提供**
  - 路面状況（凍結、陥没、冠水）の提供
  - 緊急ブレーキ／ＡＢＳ作動個所情報の提供
- **危険走行**
  - 健康状況の急変事態の通報
  - 自動走行車の異常通報（制御不能状態）

KDDI総研の取り組みの紹介

- **総務省次世代ITS委託研究開発※1 Web技術を活用した情報収集・配信技術の開発※2において、PbDに基づく次世代プローブデータ処理技術を開発中**
  - プロトタイプによる社会実装手法の確立
  - 国際標準化テーマの洗い出し・標準化

- **W3C※3 Automotive Business GroupとWorking Groupメンバー**
  - Web API仕様の検討への参加
  - Security & Privacy Task Force モデレータ



※1 SIP（戦略的イノベーション創造プログラム）「自動走行システム」における個別施策の一つとして「ICTを活用した次世代ITSの確立」に関する総務省委託研究開発（H26年度から３か年）

※2 自動走行及び事故低減に有用な危険予知・危険回避を実現するため、次世代プローブデータの収集とこれらに基づく注意喚起情報の配信を、プライバシー保護を含め効率的に行うWeb技術の開発

※3 World Wide Web Consortiumの略。Web相互運用性の確保を目的とした各種技術の標準仕様および指針を策定するコンソーシアム規格の標準化団体。なお、モデレータはKDDIとして活動