W3C/慶應 Webと車のセミナー

自動車向けWeb技術における今後の課題

AGENDA

- 位置測位情報
- セキュリティ
- プライバシー保護
- 自動車向けWebアプリ管理

2014年12月09日
㈱KDDI総研
取締役・主席研究員
平林 立彦

KDDI Research Institute

■位置測位情報：車の位置情報ユースケース／サービス主体

■ 安全・安心系

- **道路・交通情報※の収集・分析・配信**
  ／道路・交通管理者
- **緊急車両接近情報**
  ／警察、消防
- **事故対応**
  ／警察、消防、保険・ロードサービス会社
- **車両故障救済**
  ／ロードサービス会社・自動車メーカ
- **車両診断・点検・動作モニタリング**
  ／自動車メーカ
- **盗難車両追跡（SVT）**
  ／警察、ロードサービス会社
- **自動パーキング**
  ／自動車メーカ
- **道路環境・詳細地図の更新**
  ／道路・交通管理者、地図会社

※　**道路交通情報**
渋滞情報：渋滞、混雑、順調
交通障害情報：事故、故障車、障害物・路上障害、工事、作業、凍結、規制情報、通行止め・閉鎖、入口閉鎖／制限、大型通行止め、速度規制・徐行、車線規制、チェーン規制、対面通行、片側交互通行
駐車場満空情報

■ 付加価値系

- **ダイナミック経路ナビゲーション**
  ／ナビメーカ、アプリ提供者
- **グループ走行支援（他車位置案内）**
  ／ナビメーカ、アプリ提供者
- **GeoFencing／POIサービス**
  - 域内観光情報配信、広告・クーポン配布等
    ／地域業者・店舗
  - 地域駐車場案内・駐車位置・自車発見支援
    ／駐車場
  - 自動発呼／アプリ提供者
  - 電子番組表変更／AV機器メーカ
  - 域内道路有料化
  - 飛出し多発スポット／道路管理者
  - 暴走車両警報／道路管理者
- **UBI（Usage-Based Insurance）**
  ／保険会社
- **移動・運転の個人記録**
  ／アプリ提供者・ナビメーカ
- **運転スキル評価・コーチング**
  ／自動車メーカ、教習所、アプリ提供者等

いずれも時刻・位置情報が重要であって、それぞれ必要な精度は異なる。
一方、時刻・位置情報をキーに、異なる事業者が容易にデータ連結可能な関係にある。

■位置測位情報：自動車において利用可能な技術

Correction Data over FM radio for D-GPS

Cellular Wi-Fi & BT triangulation

Vehicle Speed

Wi-Fi &BT MAC addresses

Wheel Angle & Rotation

IP address, RFID

On-board Cameras Radar, LIDAR

Electronic Compass

3D Acceleration

V2X (Lane Marker, etc.)

Gyroscope (roll, pitch, yaw)

Conventional Features

Latest Vehicle-specific Features

位置測位情報：現状と課題

- **W3Cの現状**
  - **“Geolocation API Specification”**
    http://www.w3.org/TR/geolocation-API/#coordinates_interface
  - **“Geolocation Working Group Charter”**
    http://www.w3.org/2014/04/geo-charter.html
  - **現行Geolocation API は、センサーなど位置情報源を特定することなく、位置情報を提供**

- **課題**
  - **自ら位置測位をせずとも、位置情報を有する外部デバイスから位置情報を取得するようなユースケースに対応できていないのが実態**
    - 取得のための外部インタフェース標準が未定義
    - 認証プロセス標準が未定義
      - どのデバイスからでも位置情報を配信・提供しても良いのか？
      - どのデバイスでも位置情報を取得しても良いのか？
  - **後述のプライバシー問題への対処**
    - データ連携により、
      「**誰が、どんな時に、どこからどこへ行き、どんな運転をし、どこに立ち寄るか**」など
      本人の知らないところで解明されてしまう危険

■セキュリティ：保護対象と脅威

脅　威

- Unauthorized
  - Access
  - Copy
  - Use
- Disclosure
- DOS Attack
- False Message
- Tamper & Deletion
- Tapping
- Virus

保護対象

- Fundamental Control Function
- Vehicle Info.
- Personal Info.
- Setting Info.
- Application Software
- Contents
- Concentration on Driving
- Privacy

セキュリティ：自動車固有の課題

- Multi-Stakeholders in a Car
  - OEM, Tier1
  - Engineers/Technicians of Dealer, Maintenance Factory, Gas station
    # Manufacturers/Engineers want easy access to vehicles for testing, debugging, data-tuning and upgrading of software
  - Drivers, Passengers
    # In the case of rental car and car sharing, many people, and unspecified people access IVI system.
- Keeping Safe Driving even if any security incidents may arise
  - Fail-Safe Design including Anti-Driver's Distraction
  - Fallback and Rescue Strategies
- Maintenance Scheme
  - Periodical Inspection
  - Difficulties in Frequent Reliable Update and Upgrade
- Web Application Certification
  - Interoperability with in-vehicle system, and between IVI and Smartphone (OS, CPU, memory, display resolution, etc.)
  - Conflict with other applications
  - Assessment of Drivers Distraction Level

■プライバシー：車両・運転データの種別

赤字：プライバシー保護対象となる可能性の高い項目
分類はW3C Vehicle Data Interface 案のほか、ISO22837やC-ITS(Cooperative-Intelligent Transport Systems)の規格化資料等を参照、なお、アンダーライン：ISO22837でのデータ項目

- **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
- **車両属性情報**
  - 車両分類、**車両識別番号・鍵ID、**車種・年式
  - 駆動源、燃料種別、最小旋回半径、最高速度
  - 車長、車幅、車高、車重、軸重等
- **車両走行状態**
  - エンジン始動・停止、車速、加速度、回転数
  - 車輪スピード、ハンドル回転角、ヨーレート
  - アクセル／ブレーキペダル位置、ギヤ位置
  - オドメータ／トリップメータ、燃料残量、燃費
  - ドライブモード、クルーズ・コントロール
  - 前照灯、ハザード灯、ウインカー、ドア／窓
- **安全運転情報**
  - ABS、シートベルト、エアバッグ、TCS、接近警報
- **気象条件情報**
  - 温度・湿度・気圧、降雨、降雪、霧、ワイパー
- **車両メインテナンス情報**
  - **事故・故障履歴**、異常警報、日常点検、車両診断
  - エンジンオイル、タイヤ空気圧、バッテリー状態
- **車両パーソナル化情報**
  - 言語・単位系、室内表示照度／レイアウト／色彩
  - **ナビ情報（目的地、経由地、経路）、運転履歴**
  - ミラー類調整角、シート／ハンドル位置
  - サンルーフ／コンバーティブル開閉、走行効果音
- **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、太陽高度、日陰・日向
- **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**
  - **利用／アクセス履歴**
- **運転者・同乗者情報**
  - **個人認証、健康情報（血圧、脈拍、既往症）、同乗者数**
  - **認知的負荷、眠気、疲労**
  - **行動履歴、購買記録**

【参考1】ドイツ「自動車におけるプライバシー保護決議」

- **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
    （2014年10月8日、9日ハンブルグにて）
  - 詳細は、
    https://www.datenschutz-bayern.de/dsbk-ent/DSK_88-Kfz.html

【前文】（抜粋）

自動車の利用者が監視からの脅威にさらされることなく、自動車利用の自由を確保するため、自動車製造メーカ、配給者、小売店、工場並びに自動車に関連する通信やテレサービス提供者は、その義務の一部として、自動車の利用者による自己決定の裁量を保証しなければならない。

以下の事項を含む。

- プライバシーバイデザインのデータ保護原則を実現し、カスタマイズ化される新モデルや新車両においてデフォルトでプライバシー保護を実現すること
- 車両関連のデータは、最小の範囲で収集され、もはや必要と無くなった場合には、直ちに削除されること
- 契約又は明確な同意のもと、当該データは処理されること
- 車両の運転者、所有者及び利用者に対しては、十分な透明性が保証されること
  車両のどのようなデータが記録され、処理され、どんな目的で誰にどのインタフェースでデータが受持されるのか、運転者等に分かり易く説明する必要があり、変更についても、余裕をもって通知すること
- メーカや他のサービス提供者に対するデータ伝送は、コントロール可能であり、場合によっては阻止も可能となるよう、プライバシーフレンドリーなシステム設定や削除等の選択自由権が与えられること
- 適切な技術や組織対策を通じて、データセキュリティ及びデータの完全性が確保されること

【参考2】米国「車両技術・サービスのプライバシー原則」

PRIVACY PRINCIPLES FOR VEHICLE TECHNOLOGIES AND SERVICES

- **米国自動車工業会（AAM）とグローバル・オートメーカ協会（AGA）の以下の参加会員において、合意した自動車におけるプライバシー保護原則（11月12日発表）**
  - CHRYSLER GROUP、FORD MOTOR、GM
  - BMW北米、MERCEDES-BENZ米国、米国PORSCHE、米国VOLKSWAGEN GROUP、VOLVO CAR GROUP
  - MAZDA北米、MITSUBISHI MOTORS北米.米国TOYOTA MOTOR SALES
- **詳しくは、**
  - http://www.globalautomakers.org/sites/default/files/document/attachments/Automotive%20Privacy%20Principles%2012Nov2014.pdf

【前文】（抜粋）

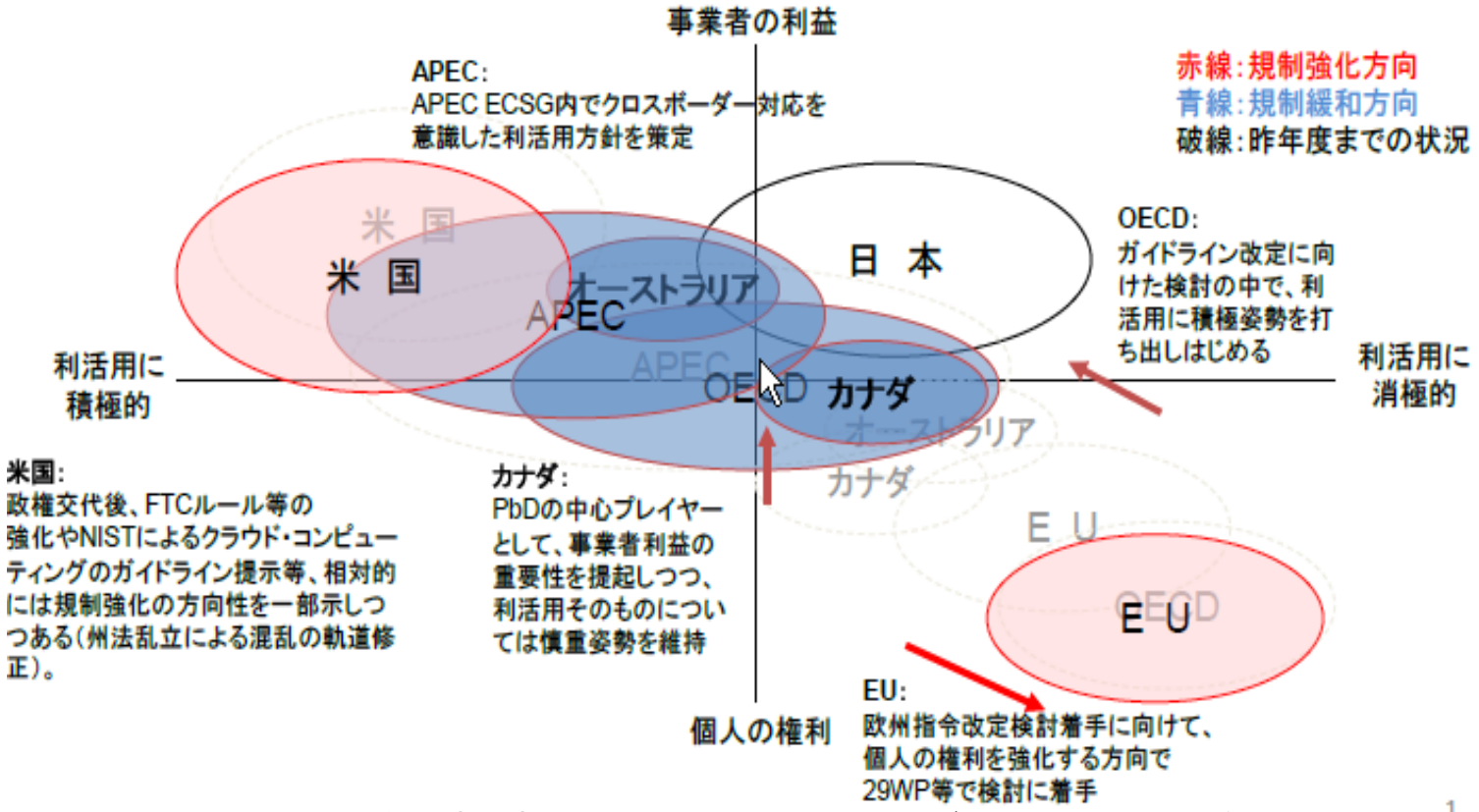
- **本原則は、米国内において、私的利用を目的に、個人に販売又はリースされる車及び軽トラックにおいて入手可能な、車両技術及びサービスに関連する「保護情報」の収集、利用及び共用に適用**
- **本原則は、適用法及び規則に従い、それらを補完するもの**
- **本原則で扱われていないプライバシー対策を採用することは可能**

【個別原則】（抜粋）

- **透明性**
- **選択性**
  - 保護対象
    - マーケティングの基礎として地理位置情報、生体情報又は運転者行動情報を利用する場合
    - 系列外のサードパーティの目的のために、地理位置情報、生体情報又は運転者行動情報を共用する場合
  - 保護対象外
    - 参加会員、所有者、登録利用者、運転者、歩行者又はその他（救急サービス提供者との情報共有を含む）の安全、財産又は権利を保護するため合理的な必要がある場合
    - 安全、運用、コンプライアンス又は保証の目的 **!?**
    - 内部的な研究又は製品開発の目的の場合
    - 会社の合併、取得又は参加会員の事業を含む売却を進めるために合理的に必要な場合
    - 合法な政府の要求、規制上の要件、法秩序上で合理的に必要な場合、（急迫した状況、又は、適用可能な法的権限が無い限り、令状又は裁判所の命令が必要）
    - 盗難されたと合理的に認定される車両の位置又は発見の支援を行う場合
- **コンテキストへの配慮**
  - 様々なコンテキストがあるが、どのように保護情報が利用及び共用されるかについて明確で、意味ある通知を行う場合に限り認められるものとする。
- **データの最小化・非特定化・保持**
- **データ・セキュリティ**
- **データ保全性**
- **説明責任**

■プライバシー：日本は何処を目指していくのか？

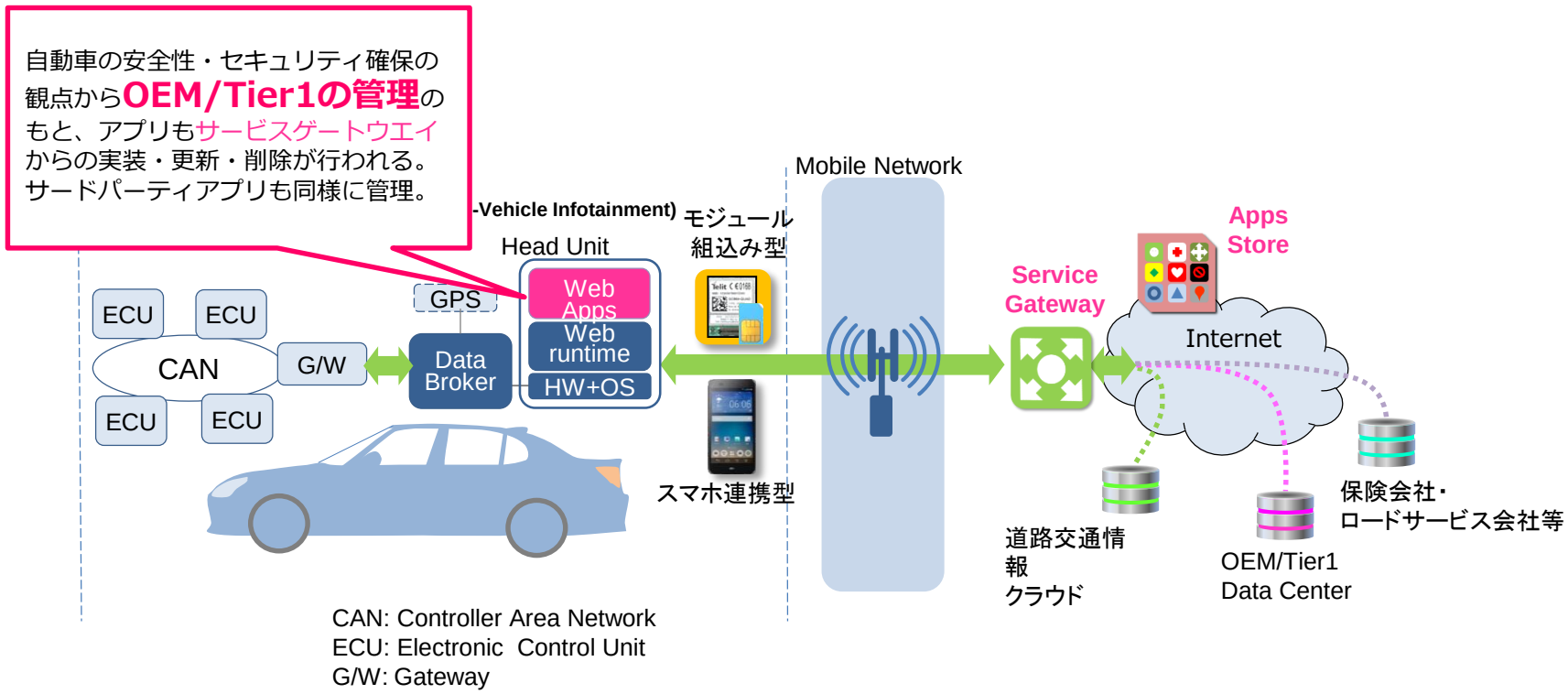
- **13年12月の「パーソナルデータ制度見直し検討会」報告書の方向性は欧州型に近い**
  - EU新規則案が通った場合には更に日本は不利な状況に追い込まれることを検討会の主要メンバーは危惧。
- **実業界の懸念**
  - 「ビッグデータはまだまだいろいろ試している段階。基本的に自由なデータの利用を認め、問題のある点について個別に対応していく、アメリカの方式を目指すべき」（ヤフー別所氏2014年1月21日記者説明会）



出典）経済産業省IT融合フォーラム・パーソナルデータWG第1回会合資料より 2012年11月

自動車向けWebアプリ管理

- サービスゲートウエイ
  - セキュリティ、プライバシー保護、安定動作、ドライバーズ・ディストラクション、実行環境の制約等の観点からのアプリ認定、ダウンロード・実装、更新、削除を実施
  - 車種×接続タイプ×動作環境（OS等）×アプリ数
- 当面、OEM管理体制が現実的なWebアプリのエコシステム



今後関連するW3Cグループ

- **Tracking Protection Working Group**
  http://www.w3.org/2011/tracking-protection/
  - DNT:1　Do not track – indicate to web site that you do not want to be tracked

- **Privacy Interest Group**
  https://www.w3.org/Privacy/
  - Discussion, not specs.
  - Anything privacy and web related. Does reviews of specs from WGs for privacy issues.
  - Develop use cases and requirements to suggest new privacy work in WGs.
  - A major concern in W3C about privacy is fingerprinting. Sites can use information about the device and software to identify the device (and person). EFF (Electronic Freedom Foundation) Panopticlick project demonstrated identifying devices out of millions.

- **Web Application Security Working Group**
  http://www.w3.org/2011/webappsec/
  - CORS (Cross Origin Resource Sharing)
  - CSP (Content Security Policy)
  - Subresource Integrity
  - Secure Cross-Domain Framing/Mixed Content
  - Lightweight Isolated / Safe Content, etc.

- **Web Cryptography Working Group**
  http://www.w3.org/2012/webcrypto/
  - JavaScript APIs for crypto, hash
  - Next Steps: Authentication, Hardware Tokens and Beyond Workshop
    - http://www.w3.org/2012/webcrypto/webcrypto-next-workshop/Overview.html
    - 10-11 September 2014, Silicon Valley (Mountain View), California

- **Web Security Interest Group**
  http://www.w3.org/Security/IG/
  - Discussion, not specs.
  - Anything security and web related.
  - Reviews specs from WGs for security issues.
  - Develop use cases and requirements to suggest new security work in WGs.

- **W3C Linking Geospacial Data Workshop (March 5-6 in London)**
  http://www.w3.org/2014/03/lgd/
  http://www.w3.org/2014/03/lgd/report.php
  - Joint WG is expected to be created collaboratively by W3C and OGC (Open Geospacial Consortium)