

第 XVI 部

自動車を含むインターネット 環境の構築

第16部 自動車を含むインターネット環境の構築

第1章 はじめに

1.1 iCAR WG 2010年度の活動

インターネット自動車WG（以下iCAR WG）では、これまでに移動体通信技術の開発とその実験環境の構築（以下iCAR テストベッド）、他団体と共同による実社会での実証実験への参加活動、および研究成果の標準化活動を行ってきた。2010年度も引き続き、移動体通信技術の可用性の検証およびフィールド実験環境の整備に関する議論を行うため、WIDE研究会や合宿でのBoFを利用した議論に加え、月に1度ポリコムを用いた定例ミーティングを開催し、継続的に研究活動を行っている。2010年度は特に、(1) 700 MHz 帯近距離移動体通信を用いたセンタレスプローブ情報システムの開発・実証プロジェクトや、(2) プローブ情報システムの匿名性・セキュリティ評価基準に関する調査研究および標準化活動のような、ITS と通信に関わる新しい社会基盤の構築・検証・整理などが活動的であった。

1.2 本報告書の構成

2010年度iCAR WGで議論してきた移動体通信技術やセンサネットワークに関する研究開発、センタレスプローブ情報システムの実証実験、プローブ情報システムの安全性やサービスアーキテクチャの体系化に関する議論等、主な活動は以下の通りである。

- 700 MHz 帯近距離移動体通信を用いたセンタレスプローブ情報システムの開発・実証プロジェクト
- プローブ情報システムの匿名性・セキュリティ評価基準等に関する標準化活動
- ISO や IRTF での関連技術の国際標準化に関わる活動

ここでは、報告書の構成として本章に続く章を概説し、各章でその詳細を述べる。

まず、第2章では、700 MHz 帯近距離移動体通信

を用いたセンタレスプローブ情報システムの開発・実証プロジェクトに関する主な活動を概説する。報告書執筆段階ではまだ実証実験の最中であるため評価や結果を述べることはできないが、プロジェクトの目的、開発技術とその検証項目、実証実験概要、標準化に向けた活動などを報告する。

第3章では、プローブ情報システムの匿名性・セキュリティ評価基準等に関する標準化活動を報告する。プローブ情報システムにおける個人情報保護検討の一環として、プローブ情報システム構築の際にプライバシー・セキュリティを議論する上での必要事項の明確化、要件整理などを運用管理面での対応も視野に入れて整理し、国際標準化提案要素としてまとめている。この活動概要について報告する。

第4章では、2009年度の報告書執筆以降に策定・提案した技術標準関連文書を列挙し、概説する。該当する技術標準関連文書は以下の通りである。

- ISO 24100:2010
“Intelligent transport systems — Basic principles for personal data protection in probe vehicle information services”
 - draft-uehara-dtnrg-decentralized-probe-transport-00.txt
“The Transport Protocol for Decentralized Probe Applications for Vehicles”
 - draft-uehara-dtnrg-decentralized-probe-message-00.txt
“The Message Format for Decentralized Probe Applications for Vehicles”
- 続く第5章で、2010年度の活動をまとめる。

第2章 センタレスプローブ情報システムの開発

2.1 背景

これまで、インターネット自動車WGでは、プローブ情報システムに関する研究を推進してきた。既に商用化されているプローブ情報システムでは、車両

から取得したセンシングデータを、携帯電話等を使ってプローブ情報センタに収集し、統計処理等を施してプローブ情報を生成している。今後、プローブ情報システムの普及が進むと、処理すべきデータ容量や通信量が増加し、センターシステムの負荷が増大することが予想される。

そこで、インターネット自動車 WG では、車車間通信を利用したセンタレスプローブ情報システムに関する研究を進めている。センタレスプローブ情報システムは、周囲の車両とセンシングデータの交換を繰り返すことにより、周辺地域のセンシングデータを収集し、車両内で統計処理等の処理を行い、プローブ情報を生成するシステムである。

2.2 センタレスプローブ情報システムの概要

センタレスプローブ情報システムでは、図 2.1 に示すように、各車両がセンシングしたデータを、車車間通信（すれ違い通信）を使って周囲の車両と共有する。メッセージの送信はブロードキャストによって行う。周囲の車両から同種の情報がある程度の数収集できたら、車両において統計処理などの処理を施し、交通情報などのプローブ情報を生成する。生成された情報もセンサデータと同様に車車間通信によって周囲の車両に伝達され、それぞれの車両においてカーナビなどで活用される。

センタレスプローブ情報システムは、大きくプラットフォーム部とアプリケーション部から構成される。図 2.2 にセンタレスプローブ情報システムの車載システム構成を示す。センタレスプローブアプリケーションと書かれている部分がアプリケーション部で、それ以外の部分がプラットフォーム部である。アプリケーションとしては、交通情報や降雨情報、安全走行情報などたくさんのアプリケーションが同時に動作することが可能である。アプリケーションによ

間通信（すれ違い通信）を使って周囲の車両と共有する。メッセージの送信はブロードキャストによって行う。周囲の車両から同種の情報がある程度の数収集できたら、車両において統計処理などの処理を施し、交通情報などのプローブ情報を生成する。生成された情報もセンサデータと同様に車車間通信によって周囲の車両に伝達され、それぞれの車両においてカーナビなどで活用される。

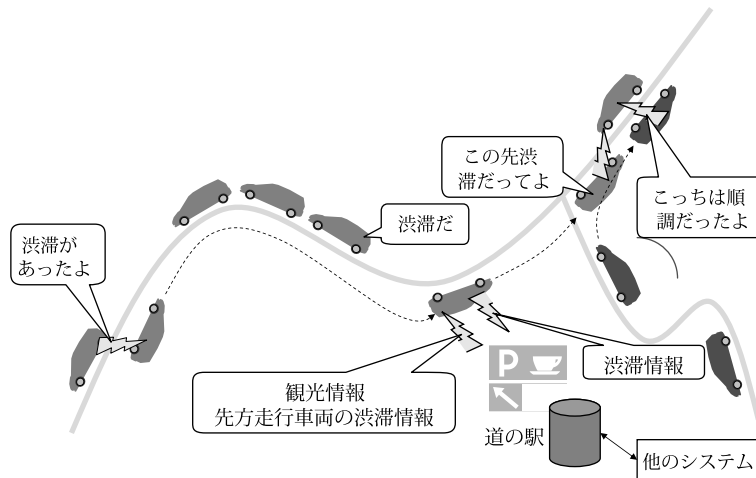


図 2.1. センタレスプローブ情報システムの概念

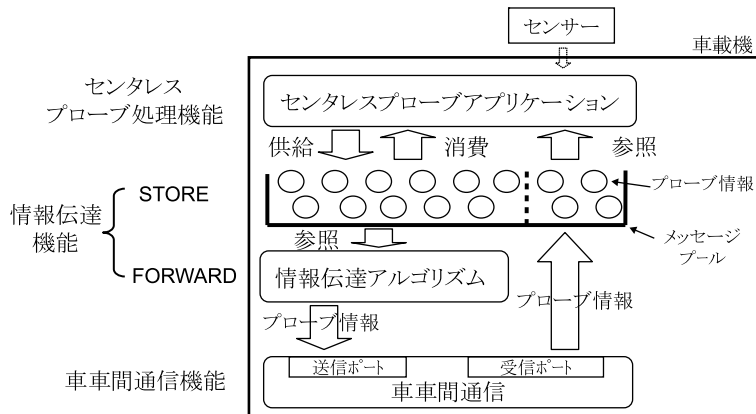


図 2.2. センタレスプローブ情報システムの車載システム構成

てセンサから収集されたデータは、一旦自車両のメッセージプールに格納される。その後、情報伝達アルゴリズムによって選択されたメッセージが、車車間通信機能をつかって車外にブロードキャストされる。ブロードキャストメッセージを受け取った車両は、受信したメッセージをメッセージプールに格納する。アプリケーションは、自車両でセンシングしたデータと他車両から受信したデータの双方を使って、より確度の高い情報を生成し、もう一度メッセージプールに格納する。

このシステムでは、どのような戦略で周囲の車両に情報を伝達するかが重要となる。各車両が持つメッセージプールには多くのセンサデータと生成された情報が入っている。ここでいう戦略とは、メッセージプールに格納されているメッセージから、どのメッセージを選択してブロードキャストするのかを決定するためのアルゴリズムである。筆者らの研究によると、このアルゴリズムを工夫する事により、メッセージプールに格納されているメッセージからランダムに送信メッセージを選択するのに比べて、交通情報を生成するまでにかかる時間を大幅に削減する事が可能になる。

また、センタレスプローブ情報システムは、センタ型のプローブ情報システムと排他的な関係にある訳ではない。センタレス型で交換した情報を、広域通信網を備えた車両がまとめてセンタに送る仕組みや、交通情報などの生成された情報のみをセンタに送る仕組みなど、幾つかのセンタレス型-センタ型連携の仕組みを取り入れる事が可能である。また、道路の周囲にある自動販売機や信号機等にセンタレスプローブ情報システムの車載器と同様のものを設置して、システムの動作安定度の向上を図る事も考えられる。このような、センタレスプローブ情報とセンタ型システムの連携やセンタレスプローブ情報システムの機能強化を図るための仕組みについては、

未だ研究段階であり、今後の研究成果が待たれる分野である。

2.3 700 MHz 帯無線通信を使ったセンタレスプローブ情報システムの開発

インターネット自動車 WG でこれまで開発してきたセンタレスプローブ情報システムは通信メディアとして 2.4 GHz 帯の無線 LAN を使用してきた。しかし、2.4 GHz 帯の無線 LAN では、見通しで 100 m 程度の通信範囲しか確保することが出来ず、普及率が低い段階では十分なセンシングデータが集まらないことが問題となった。そこで、2010 年度は、700 MHz 帯無線通信装置を使ったセンタレス型プローブ情報通信システムの開発を行う。

700 MHz 帯は、テレビのデジタル化の後、再編される予定の無線帯域で、ITS への割当も検討されている。ここでは、この無線通信システムを利用することとした。また、同時にこれまでの研究成果を公開すべく、下記の点について標準化案を作成する。

1. 700 MHz 帯を利用する近距離移動体通信方式として検討されている ITS 情報通信システム推進会議の暫定仕様である RC-006 では、5.8 GHz DSRC における ASL のような IP 通信を実現するための LLC SAP は規定されていない。そこで本事業では、700 MHz 帯を利用する近距離移動体通信で IP 通信を実現するための LLC SAP の技術規格を策定する。策定した技術規格は、ITS 情報通信システム推進会議規格部会の運転支援通信システム実用化専門委員会実証実験検討タスクグループにて議論し、標準化を目指す。
2. センタレスプローブ情報システムにおけるプラットフォーム部分のアーキテクチャの技術規格を策定する。情報を周辺の車両に伝えるための戦略（位置情報に基づく情報伝達等）を含めた情報流布シナリオを幾つか策定し、情報伝達アルゴリズム

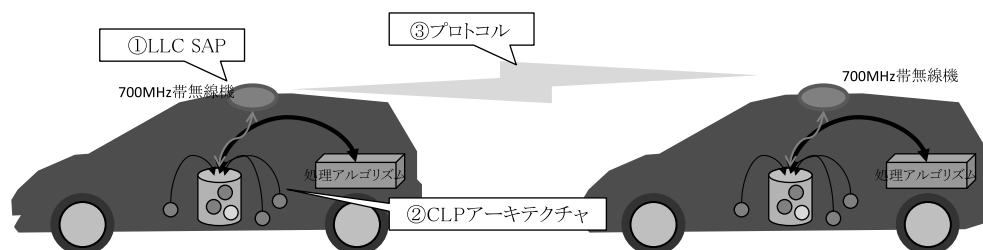


図 2.3. センタレスプローブ情報システムにおける標準案作成ポイント

ム等のアーキテクチャを策定する。策定した技術規格については、ISO/TC204/WG16において紹介し、標準化への方策を探る。慶應とJARIのメンバーのうち3名は既にISO/TC204/WG16のExpert登録をしており、日頃からISOの活動に参加しているため、スムーズな技術紹介が可能と考える。

3. IPアプリケーションプロトコルとしては、CLPプラットフォームの通信部が必要となるアプリケーションプロトコルの技術規格を策定する。具体的には、車両が取得したデータを送信する際のパケットフォーマットや送信手順について規格化する。IPアプリケーションプロトコルについては、慶應義塾大学の知見を活かし、Internet-DraftとしてInternet Engineering Task Force (IETF) に提案し、国際標準化の方策を探る。

第3章 プローブ情報システムの匿名性・セキュリティ評価基準等に関する標準化

3.1 研究開発の概要

現在、各国で開発・展開が行われているプローブ情報システムには、共通のフレームワークは存在していない。本WGでは、2002年からプローブ情報システムで取り扱う個人情報に関する検討を開始し、その成果を「プローブ情報システムにおける個人情報の基本原則」として取りまとめて国際標準化機構(ISO)において国際標準化を実施したが、情報提供者が安心して情報を提供できる基盤を構築するために必要な具体的なプライバシー・セキュリティ対策に係る基本的な考え方や適切な処置については未整備であった。

そこで、本WGでは2007年から「プローブ情報システムにおける個人情報保護の基本原則」を基礎とし、プローブ情報システムを実用化するために必要なプローブ情報システムのアーキテクチャ(周辺環境)の研究開発及び国際標準化活動を実施した。具体的には、プローブ情報システムの現状と動向、およびプローブ情報システムにおいて必要な個人情報保護を見定めつつ、プローブ情報システム構築の際にプライバシー・セキュリティを担保するために必要な事項を明確にした。また、プローブ情報について、

プライバシーを保護した上でセキュアに取り扱うための要件を整理し、評価基準として取り纏めるべき要素を抽出すると共に、その実現のための手法を明確化した。この際、技術的機能だけでなく、運用管理面での対応も視野に入れた整理を行い、併せて国際標準化提案要素として整理した。

3.2 目標とする国際標準の内容

先行して標準化活動が行われた「プローブ情報システムにおける個人情報保護の基本原則(ISO 24100:2010)を基礎とし、セキュリティやプライバシーを考慮したプローブ情報システムのアーキテクチャの研究開発、および国際標準化活動を実施した。ISO 24100では、個人情報保護の観点からのプローブ情報システムの構築に際する基本原則を定めているが、実構築にあたっては、この基本原則に則ったシステムの構築に関するより具体的な技術的リファレンスが必要となる。

そこで、本活動ではISO 24100では未整備であった、情報提供者が安心して情報を提供できる基盤を構築するために必要な具体的なプライバシー・セキュリティ対策に係る基本的な考え方や適切な処置についての検討、および標準化をスコープとした。

3.3 実施内容

1. プローブ情報システムのプライバシー・セキュリティ評価基準の検討
2009年度までの検討を基に、匿名認証方式やセキュアな通信路に関する検討結果を踏まえたプライバシー・セキュリティ評価基準に関する国際標準提案のための検討をおこなった。また、プローブ情報システムの評価基準として必要な要素の調査、および原案のとりまとめを実施した。
2. 匿名認証方式を用いたセキュアなプローブ情報システムの検討
2009年度までの開発を基に、処理速度や規模性を考慮した匿名認証方式を活用したプローブ車両の認証システムの実証実験をおこない、評価基準の原案の根拠とした。
3. プローブ情報システムにおけるセキュアな通信路の為のインターフェイスの検討
2009年度までの開発を基に、処理速度や規模性を考慮した通信路のためのインターフェイスの実証実験をおこない、評価基準の原案の根拠とした。

4. 国際標準化活動

国際標準案の概要、および作業範囲については、2009年8月に開催されたISO/TC204/WG16北九州国際会議にて紹介した後に、参加する国際専門家と議論を行い、IS化を目指して議論を進めていくことで合意した。しかし、前述の国際会議が日本での開催であったため、欧州からの参加国が無かったことを受け、スコープの明確化と標準案の具体化を先行して進めると共に、次回のドイツ会議（2009年12月）にてあらためて紹介と議論を行って参加国を募った後に作業開始とするスケジュール案が妥当とされ、PWI提案は次回プレナリにて行うこととなった。その後、ドイツ会議では、日本からのスコープ案に、日本、米国、ハンガリー、ドイツ、オーストラリアが賛成し、PWI提案の条件が整った。その結果を受け、2010年4月のニューオリンズ総会にてPWI提案がPWI 16461“Criteria for Privacy and Integrity protection in Probe Vehicle Information Systems”として承認され、日本側がドラフト執筆をリードする形で議論が進んでいる。

3.4 関連する発表成果物等

- 佐藤雅明, 繁富利恵, 上田憲道, 党聡維, 植原啓介, 砂原秀樹, 村井純, “プローブ情報システムのためのプライバシーを考慮した匿名認証方式の提案と評価”, 情報処理学会論文誌, Vol.50, No.1, January 2009
- Michiko Izumi, Masaaki Sato, Hideki Sunahara, “Requirements for protection methods of personal information in vehicle probing system”, Proc. of The 2007 International Symposium on Applications and the Internet (SAINT2007), January 2007
- Masaaki Sato, Michiko Izumi, Hideki Sunahara, Keisuke Uehara, Jun Murai, “Threat analysis and protection methods of personal information in vehicle probing system”, Proc. of The Third International Conference on Wireless and Mobile Communications (ICWMC), March 2007
- Rie Shigetomi, Masaaki Sato, Keisuke Uehara, Akira Otsuka, Hideki Sunahara, Hideki Imai,

“An Efficient Scheme to Protect Privacy in Probe Vehicle Information System”, ITS Telecommunications, 2008. ITST 2008. 8th International Conference, pp. 84–88, October 2008

- 佐藤雅明, “プローブ情報システムの個人情報についての脅威分析に関する研究”, 自動車研究, 第29巻第4号, pp. 159–164, April 2007
- 佐藤雅明, 繁富利恵, 上田憲道, 党聡維, 和泉順子, 植原啓介, 砂原秀樹, 村井純, “プライバシーを考慮した匿名認証方式によるプローブ情報システムの構築”, 情報処理学会 ITS 研究会研究報告, 2009-ITS-37, June 2009
- 和泉順子, 佐藤雅明, 砂原秀樹, “プローブ情報システムへの匿名性評価手法導入のための一考察”, 情報処理学会電子化知的財産・社会基盤 (EIP) 研究報告, Vol.2009-EIP-45, No.2, September 2009

第4章 策定・提案した関連技術標準文書の概要

4.1 ISO 24100:2010 “Intelligent transport systems — Basic principles for personal data protection in probe vehicle information services”

プローブ情報システムにおける個人情報保護に関する基本原則をまとめた技術標準文書であり、経済産業省基準認証研究事業「プローブ情報システムにおける個人情報保護」の研究成果の一つである。2002年より継続的に議論してきた、プローブ情報システムが内包する個人情報・プライバシーに対する脅威分析やセキュリティ要求事項の検討、基本ルールのガイドライン等を議論し、整理・策定した技術標準である。個人情報の保護に関しては各国法制に違いがあり、国際標準として作成するスコープの合意が最大の課題であったため、国際標準化機構 (ISO) 内の ITS を担当する技術委員会である TC204 の中の WG16 にて検討を行った。プローブ情報システムの特定とアプリケーションでの個人情報および識別子、リファレンスとなるアーキテクチャに関する議論を重ね、2010年4月に国際標準として公開された。

開発した技術の実社会への反映を考慮し、社会全体の利益に資するような研究開発を目指していきたい。

4.2 draft-uehara-dtnrg-decenterlized-probe-message.txt “The Message Format for Decentralized Probe Applications for Vehicles”

センタレスプローブ情報システム (CLP, decentralized probe system) の車車間通信で用いるアプリケーションメッセージフォーマットを規定する文書である。この文書は、2010年11月に北京で開催された IETF/IRTF に合わせて Internet-Draft として投稿された。今後は IRTF DTN WG において議論を継続する予定である。

(wide-paper-icar-dtnrg-decentralized-probe-message-00.txt 参照)。

4.3 draft-uehara-dtnrg-decenterlized-probe-transport.txt “The Transport Protocol for Decentralized Probe Applications for Vehicles”

センタレスプローブ情報システム (CLP, decentralized probe system) で用いる車車間通信におけるトランスポートプロトコルを規定する文書である。実際の車車間通信環境は車両の移動に伴い動的に変化するため、限られた帯域下における送受信の挙動や送信側のエラーコレクションによるメッセージ到達率向上などを検討している。この文書は、2010年11月に北京で開催された IETF/IRTF に合わせて Internet-Draft として投稿された。今後は IRTF DTN WG において議論を継続する予定である。

(wide-paper-icar-dtnrg-decentralized-probe-transport-00.txt 参照)。

第5章 まとめ

2010年度の iCAR WG の研究活動は、インターネット移動体通信技術の研究開発だけでなく、700MHz帯を利用したセンタレスプローブ情報システムの研究開発と実証実験、センサデータ (プローブデータ) の安全な流通やサービスアーキテクチャに関しても活発に議論し、より実社会のニーズを反映した分野へと広がりを見せた。今後も本WGでは