第 XVII 部

自動車を含むインターネット環境の構築

第 17 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 ワーキンググループ 2007 年度の活動

インターネット自動車ワーキンググループ（以下 iCAR ワーキンググループ）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）、財団法人日本自動車研究所や InternetITS 協議会などの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。

本ワーキンググループでは前年度に引き続き、2007 年度も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と、ITS 分野における情報流通および通信基盤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ミーティングを定期的に開催し、継続的に議論および研究活動を行った。

1.2 本報告書の構成

本年度 iCAR ワーキンググループ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としては、センタレスプローブにおける情報伝達アルゴリズムの検討と評価、プローブ情報システムの安全性や個人情報保護と脅威分析、およびプローブ情報システムにおける個人情報取り扱いに関する ISO ガイドラインの策定に関する議論が挙げられる。本章に続く各章として、以下の活動内容と成果を述べる。

2. 情報伝達アルゴリズムとその評価結果
3. プローブ情報システムに存在する個人情報についての脅威分析に関する研究

ここでは、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、センタレスプローブにおける情報伝達アルゴリズムとその評価結果について述べる。近年、プローブ情報システムが注目を浴び、実用化が進みつつある。ここでは、高額な通信費やセンタシステムの負荷が問題となっていることに着目し、2006 年度から車載計算機と車車間通信のみを利用したプローブ情報システムである「センタレスプローブ」（以下、「CLP」）の研究開発を進めている。本年度は、CLP の鍵となる技術の 1 つである情報伝達アルゴリズムを検討し、評価した。

CLP では、車両センサから取得した情報を近隣の車両と交換し、情報を共有する。その情報に統計処理を施すことにより、確度の高い情報を生成する。例えば道路状況であれば、車速を他の車両と共有し、道路と進行方向ごとに統計処理を施すことによって、平均速度を得ることができる。CLP は大きく、交通情報生成配信やヒヤリハット情報生成配信などのアプリケーションそのものである CLP 情報処理部と、アプリケーションが生成する情報を車両間で共有するための情報伝達部から構成され、メッセージプールによって連結される。CLP 情報処理部では、車両センサから取得した情報をメッセージプールに入れたり、メッセージプールに溜まった情報に統計処理を施し、メッセージプールに戻す処理を行う。一方、情報伝達部は、メッセージプールに蓄えられたメッセージのうちどれを優先的に送信するかを決定し、メッセージの送信を行う。また、受信したメッセージは重複検査をした後、重複していないものはメッセージプールに格納する。

この研究成果は、財団法人日本自動車研究所発行の「自動車研究」第 29 巻第 10 号（2007 年 10 月）で発表されている。

第 3 章では、プローブ情報システムに存在する個人情報についての脅威分析に関する研究を詳述する。自動車は、走行状態や周囲の状況を把握する “動くセンサの集合体” としての側面を持つ。プローブ情報システムは、こうした自動車の特性を活かし、自動車の保持するセンサ情報をインターネットなどの情報通信基盤を用いて収集し、統計的な処理などを施すことで交通情報や気象情報、安全運転支援情報などの価値ある情報（プローブ情報）を生成し、生成したプローブ情報を情報通信基盤を活用して利用者に提供するシステムである。

プローブ情報システムは日本を始め欧米でも積極的に研究開発がなされ、一部には実用化されているものもある。一方、プローブ情報システムは渋滞の解消や公共交通機関の利便性向上などの社会的利益に資するシステムであるが、自動車が情報通信基盤を用いて車両の位置や状態に関する通信を行うため、適切なシステム構築・運用がなされない場合には、個人情報の漏洩に繋がる可能性がある。

具体的には、現在 ISO/TC204/WG16 で検討されている車両データには個人を示唆する情報は含まれておらず、匿名での動作が前提となっているが、システムの認証や通信時には何らかの識別子が用いられる可能性が高く、また車両データは必ず位置と時間を含む形で送信されるため、こういった識別子に関して、個人情報となりうる場合には適切な処置を講ずる必要がある。

ここでは、個人情報の取り扱いには国内外で高い関心が集まっていることも鑑み、従来のプローブ情報システムの実運用上の問題点の抽出と脅威分析を行い、これらの脅威についての保護手法を検討した。また、こうした研究成果の一部は国際的なルールとして国際標準化提案を行っており、その活動についても記述する。

この研究成果は、財団法人日本自動車研究所発行の「自動車研究」第 29 巻第 4 号（2007 年 4 月）で発表されている。

第 2 章　センタレスプローブにおける情報伝達アルゴリズムとその評価結果

2.1 はじめに

近年、プローブ情報システムが注目を浴び、実用化が進みつつある。しかし、高い通信費やセンタシステムの負荷が問題となっている。そこで、我々のグループでは 2006 年度から車載計算機と車車間通信のみを利用したプローブ情報システムである「センターレスプローブ」（CLP）の研究を進めている [195]。

CLP では、車両センサから取得した情報を近隣の車両と交換し、情報を共有する。その情報に統計処理を施すことにより、確度の高い情報を生成する。例えば道路状況であれば、車速を他の車両と共有し、道路と進行方向ごとに統計処理を施すことによって、平均速度を得ることができる。

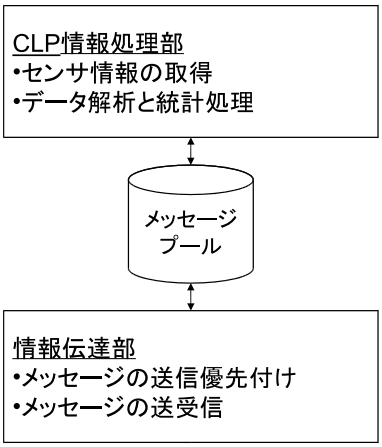

図 2.1.　CLP の構成

CLP は大きく「CLP 情報処理部」「情報伝達部」の二つから構成され、メッセージプールによって連結される（図 2.1）。

交通情報生成配信やヒヤリハット情報生成配信などのアプリケーションそのものである CLP 情報処理部では、車両センサから取得した情報をメッセージプールに入れたり、メッセージプールにたまった情報に統計処理を施し、メッセージプールに戻す処理を行う。一方、アプリケーションが生成する情報を車両間で共有するための情報伝達部は、メッセージプールに蓄えられたメッセージのうち、どれを優先的に送信するかを決定し、メッセージの送信を行う。また、受信したメッセージは重複検査され、重複していないものはメッセージプールに格納される。

2.2 情報伝達部の概要

情報伝達部は大きく、「情報伝達アルゴリズム」と「送受信処理」に分けることができる。本節では情報伝達部の全体概要と送受信処理について述べる。情報伝達アルゴリズムについては、次節で詳しく説明する。

2.2.1 情報伝達部に求められる要件

情報伝達部は、車両間で情報を交換する戦略が実装される部分である。戦略とはすなわち、メッセージプールに蓄えられた情報のうち、どの情報を優先的に周囲の車両に配信するかを決定することである。

交通情報生成配信などの CLP アプリケーションには、確度の高い情報を生成する情報生成フェーズと生成された情報を他の車両に伝達するための情報

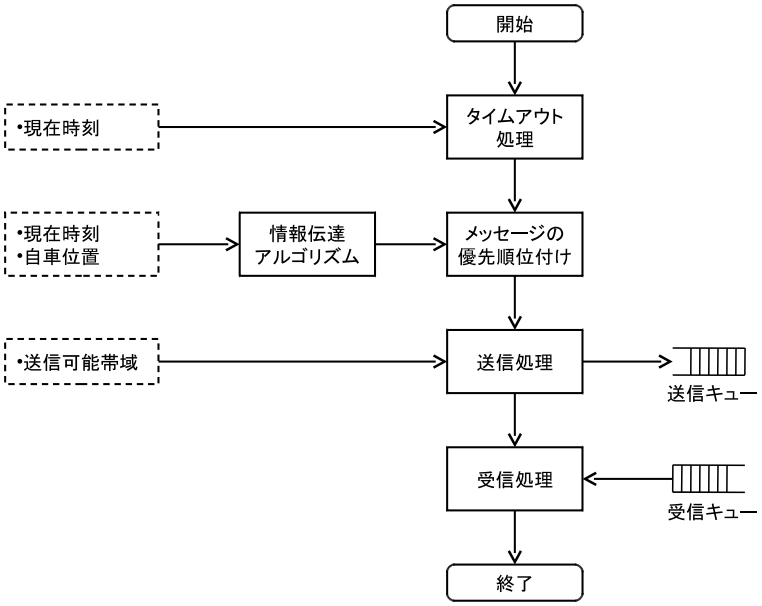

図 2.2. CLP 情報伝達部の構成

配信フェーズが存在する。情報生成フェーズにおいては、統計処理などを行うために必要なデータ数をいかに早く収集できるかが重要となる。一方、情報配信フェーズにおいては、生成された情報をいかに早く遠くまで伝達できるかが重要となる。

2.2.2 情報伝達部の動作概要

図 2.2 に情報伝達部の動作概要を示す。情報伝達部は定期的に図に示した処理を行う。はじめに、メッセージプールをスキャンし、タイムアウトしている情報を削除する。その後、メッセージプールに残っている情報のうち、どれを優先的に送るべきかを情報伝達アルゴリズムに基づいて決定する。優先順位付けされたメッセージは、優先順位の高い方から順に送信可能帯域の制限まで送信キューにコピーされる。送信キューに入れられたメッセージは送信モジュールによって車外にブロードキャストされ、他の自動車の受信キューに格納される。その後、受信処理として受信モジュールによって受信キューに格納された情報のうち、メッセージプールに存在しないものはメッセージプールに格納される。

2.2.3 送受信処理における輻輳制御

CLP における送受信処理では、輻輳制御が重要となる。全ての車両が通信可能帯域いっぱいに情報を送信するような状況では、送信メッセージの衝突が起こり、結果としてどの車両もメッセージを受信できない状況が起こり得る。そこで、周囲の車両の台数やメッセージ送信量に応じて、送信するメッセージ量を制御する機構が必要となる。

しかし、周囲に何台の車両が存在するかを計測することは難しい。そこで、メッセージの受信量に応じて送信するメッセージ量を制御する方式を取り入れた。実際には式 (1) によって、送信帯域を制御することとした。

$$B = \frac{B_{max} - B_{recv}}{2} \tag{1}$$

ここで、B_{max} は通信デバイスの利用可能帯域を、B_{recv} は前回の CLP 伝達部処理における受信帯域を、B は送信可能帯域を示す。つまり、全帯域から受信した帯域を引き、さらにその半分を送信に利用できる帯域としている。これによって、輻輳を抑制することができる。

2.3 情報伝達アルゴリズム

情報伝達アルゴリズムは、情報をどのように伝達させたいかによってさまざまな方式が考えられる。本研究では、比較対象としてメッセージプールの情報をランダムに送信する「ランダム配信アルゴリズム」、情報生成フェーズにおいて利用される「収束アルゴリズム」、情報配信フェーズにおいて利用される「拡散アルゴリズム」の 3 つのアルゴリズムを実装した。

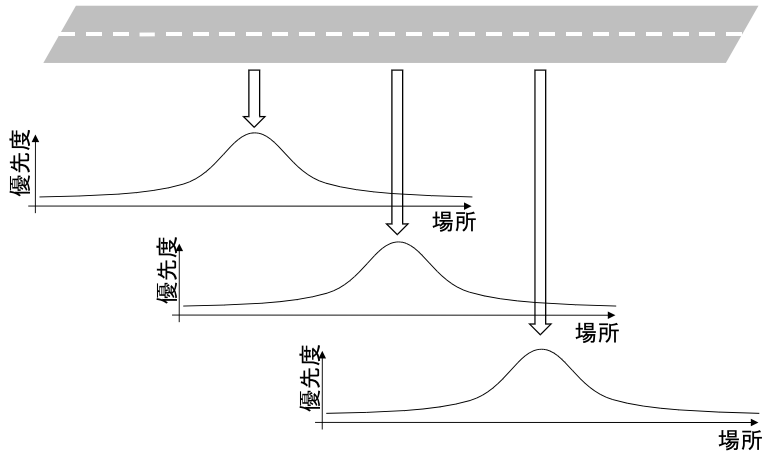

図 2.3.　収束アルゴリズムの概念図

2.3.1 ランダム配信アルゴリズム

本来、情報伝達アルゴリズムでは時刻や車両の位置などのパラメータによってメッセージプール内の情報に優先順位を付け、優先順位の高いものから送信する。一方、ランダム配信アルゴリズムではパラメータを用いず、全てのメッセージが同じ確率で送信される。本研究では、本アルゴリズムを他のアルゴリズムの性能を測るための比較対象として用いる。

2.3.2 収束アルゴリズム

情報生成フェーズにおいては、いかに短時間に統計処理のための同種の情報を収集できるかが重要になる。今回の研究では、CLP アプリケーションとして旅行速度情報を対象とした。この場合同種の情報とは、同じ道路の同じ方向に走行する車両の情報となる。

同じ道路の同じ方向に走行する車両の情報を効率よく収集するため、位置と時刻に基づく情報配信アルゴリズムを実装することとした。具体的には図 2.3 に示すように、ある場所の情報については、その場所の周辺で情報が頻繁に配信されるようにすることで、情報が生成された場所の近くで素早く統計処理可能な数の情報を収集できるようにした。

今回の実験においては、式 (2) のような重みづけを行った。ここで p は重みを、l は情報が生成された位置から現在位置までの距離を、l_0 は情報配信範囲を、Δt は前回同じ情報が配信されてからの経過時間を、T_k は同じ情報を頻繁に送信することを抑制するための定数を示す。ただし、この式が適用されるのは $l < l_0$ の場合においてのみで、それ以外の場合は、$p = 0$ となる。

$$p = 1 - \frac{l}{l_0} \cdot \frac{\Delta t}{t_k} \tag{2}$$

2.3.3 拡散アルゴリズム

情報配信フェーズにおいては、いかに短時間に情報を必要としている車両に対して、情報を配信できるかが重要となる。旅行速度情報では、その場所に向かっている車両に対して情報を配信することとなる。

今回の研究ではカーナビゲーションシステムなどを前提としていないため、車両が走行する経路は未知である。そこで、必ずしも正しい方向とは限らないが、生成された情報の走行方向と逆の方向に情報を配信することとした（図 2.4）。

配信アルゴリズムとしては、本来、決められた配信方向に限り情報が配信されるべきであるが、忠実にその動作を実装した場合、情報生成箇所の後方に車両が存在しないとそこで配信が止まってしまう。そこで、今回は情報生成箇所の周辺では円形に情報を配信し、それ以外の場所では後方のみに情報が配信されるようにした。

今回の研究においては、配信方向においては式 (3)

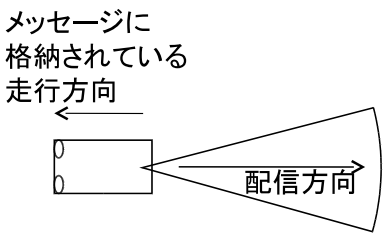

図 2.4.　拡散アルゴリズムにおける配信方向

のような重みづけを行った。ここで、l_1 は情報配信範囲を示し、l_0 より十分に長い距離を取ることとした。また、配信方向以外では収束アルゴリズムと同様の重みづけを行った。

$$p = 1 - \frac{l}{l_1} \cdot \frac{\Delta t}{t_k} \tag{3}$$

2.4 情報伝達アルゴリズムの評価

今回の研究において開発した情報配信アルゴリズムを、シミュレーションを用いて評価した。本節では、シミュレーション概要とシミュレーション結果について述べる。

2.4.1 シミュレーションの概要

今回の研究において開発した情報配信アルゴリズムを評価するためにシミュレータを開発した。開発したシミュレータは、交通流シミュレータと通信シミュレータを組み合わせたものである。

本シミュレータを用いて、東京西部地区のシミュレーションを行った。シミュレーション規模は東西約 10 km × 南北約 20 km で、幅 5.5 m 以上の道路をすべて含んでいる。また、朝 6 時から朝 9 時までの 3 時間のシミュレーションを行った。この間、延べ 27 万台の車両が生成されている。さらに、CLP 車両の混入率は 5%とした。

2.4.2 収束アルゴリズムの評価

前項で述べたシミュレーションによって、収束アルゴリズムの評価を行った。評価は、同じ時点の車速情報が 3 つ以上集まった場合に旅行速度情報が生成されるアプリケーションを利用し、旅行速度情報が生成されるまでにかかった時間を比較することによって行った。

シミュレーション結果を図 2.5 および図 2.6 に示す。それぞれ、調布駅周辺及び東八道路周辺における旅行速度情報生成にかかった時間の頻度分布である。

調布駅周辺の場合を見てみると、ほとんどの旅行速度情報が 3 分以内に生成されているのに対して、ランダム配信の場合は 12 分かかっているものもあることがわかる。東八道路の場合にも同様の傾向が見て取れる。これは、ランダム配信アルゴリズムの場合はばらばらの場所で情報が配信されるため、同一地点に関する情報を収集しにくいためと考えられる。

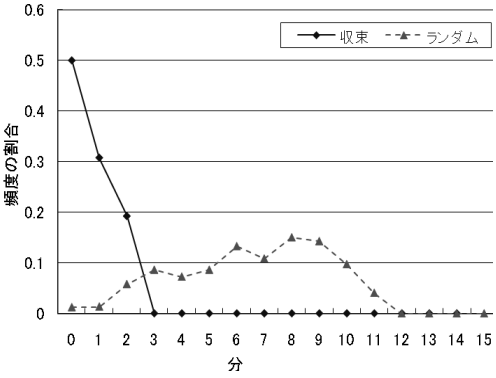

図 2.5. 渋滞情報生成時間（調布駅周辺）

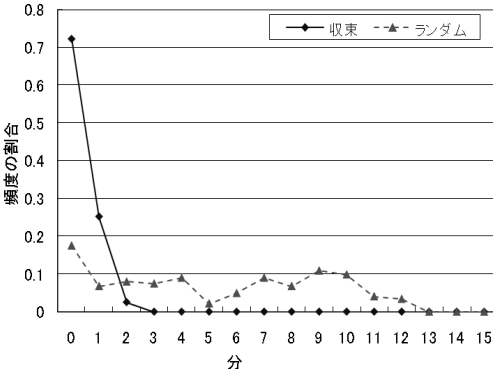

図 2.6. 渋滞情報生成時間（東八道路周辺）

2.4.3 拡散アルゴリズムの評価

収束アルゴリズム同様に、拡散アルゴリズムの評価もシミュレーションを用いて行った。評価は、配信方向に対してどの程度早く情報を配信できるかを計測することにより行った。しかし、今回のアルゴリズムにおいては拡散アルゴリズムと収束アルゴリズムにおいて有意な差は見られなかった。

原因としてはシミュレーションパラメータの設定が不適切だったことが考えられる。今回のシミュレーションではプローブ車両の混入率を 5%としたため、期待値としては 20 台に 1 台がプローブ車両となる。一般的な車両の長さは約 5 m、渋滞時の車間を 2 m とすると、渋滞時に 20 台の自動車が並ぶと 140 m となり、今回想定した通信メディアの通信範囲ぎりぎりとなる。このため、車速以上に情報を伝達するのが難しくなる。

今後、混入比率を高めたり、より適切な無線デバイスを想定することによって、よりよい結果が得られると考えられる。

2.5 まとめ

本章では、CLP のための情報伝達アルゴリズム及びその評価について述べた。CLP では、アプリケーションが利用するための多様な情報配信アルゴリズムが必要となる。今回は収束アルゴリズムと拡散アルゴリズムの開発を行った。また、シミュレーションを用いてこれらのアルゴリズムを評価し、特に収束アルゴリズムが情報を収集する上で有効に機能することを確認した。

第 3 章　プローブ情報システムに存在する個人情報についての脅威分析に関する研究

3.1 はじめに

現在、自動車を取り巻く環境は大きく変化している。自動車は単体でさまざまな情報を持ち、これらの情報を活用することで安全かつ快適な走行を実現している。個々の自動車が持つ情報を利用する総合的な情報交通システムは、さまざまな道路交通問題の根本的な解決手段として注目されている。その実現形態として、道路交通に関する総合的な情報通信システムである高度道路交通システム（Intelligent Transport Systems: ITS）の構築が世界規模で盛んに行われている。自動車の情報化は社会全体の利益に繋がり、その必要性は高い。同時に、自動車と情報通信産業などに関連する分野で、大規模な新規市場の形成や情報通信社会を支える一つの基盤としての役割も期待されている。プローブ情報システム [172] は、自動車の保持するセンサ情報をインターネットなどの汎用的な情報通信基盤を用いて収集し、統計的な処理などを施すことで交通情報や気象情報、安全運転支援情報などの価値ある情報（プローブ情報）を生成し、生成したプローブ情報を情報通信基盤を活用して利用者に提供するシステムである。システム構築にあたっては専用基盤を必要としないため、既存の ITS に比べてより広範囲な情報の収集・提供が可能である。プローブ情報システムは日本だけでなく欧米でも積極的に研究開発がなされ、Floating Car Data（FCD）[43] など一部実用化がなされている事例もある。

プローブ情報システムは汎用的な情報通信基盤を用い、個々の車両の存在位置や時刻と共に自動車の情報を収集するため、情報提供者の活動履歴や個人情報の漏洩を保護するためには、適切なシステム構築と運用が不可欠である。

そこで本研究では、プローブ情報システムにおける個人情報に関する脅威について分析し、これらの脅威についての保護手法（プロテクションメソッド）を述べる。具体的には、まず一般的なプローブ情報システムの汎用的なモデル（リファレンスアーキテクチャ）を構築し、このモデルに基づいた脅威分析を行う。次に、この脅威分析の結果に基づき、プロテクションメソッドに関する提案を行う。この提案の一部は、国際的なルールとして国際標準化提案を行っている最中である。最後に、現在の国際標準化に関する動向を述べる。

3.2 プローブ情報システムの概要

既存の ITS では、自動車は交通流としてみなされ、その情報は専用基盤を用いて収集される。前述のように自動車はさまざまなセンサを持っているが、これらセンサの情報は活用されていない。プローブ情報システムでは、自動車の持つ情報を情報通信基盤によって収集し、直接活用するシステムである。プローブ情報システムは、世界各国で研究開発がなされており、本研究では、ISO/TC204/WG16/SWG16.3 にて検討され、国際標準化の対象となっているプローブ情報システム（ISO CD22837）[25] を前提とする。プローブ情報システムの概要を図 3.1 に示し、用語を以下に定義する。

自動車センサ

自動車に搭載され、車両や周囲の状況、ドライバの挙動などを検知することができる機器。温度センサや速度計、ワイパや前照灯のほか、ブレーキ（ABS）挙動センサやステアリングセンサなども含まれる。

プローブデータ

プローブ情報システムが活用しやすいように、自動車センサの情報をルールに基づき正規化した情報の総称。プローブデータには、後述のプローブデータエレメントとプローブメッセージからなる。

プローブデータエレメント

プローブメッセージを構成する、自動車に設置された個々のセンサの持つデータを正規化した情報。

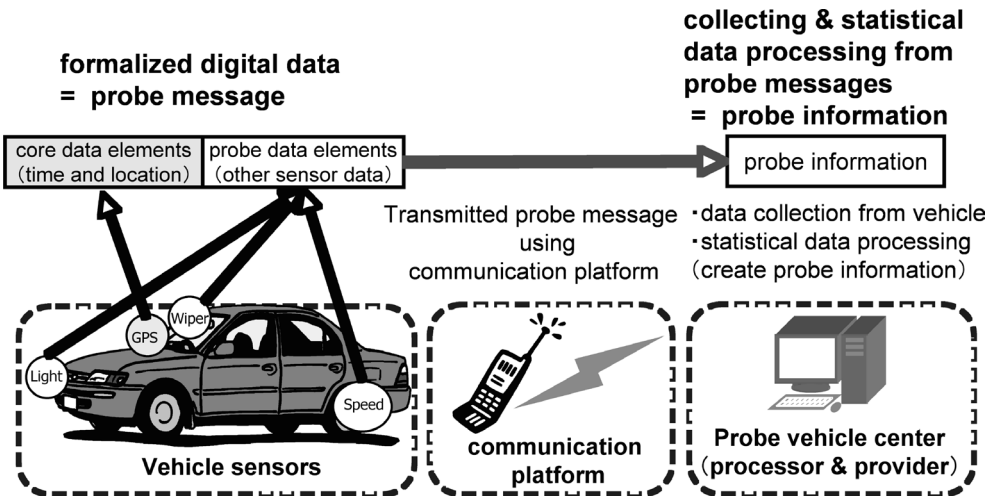

図 3.1.　プローブ情報システムの概要

コアデータエレメント

全てのプローブデータに存在するデータエレメント。プローブデータが構築された時刻を示す情報と位置を示す情報。

プローブメッセージ

送信するために成型された 1 つ以上のプローブデータエレメントとコアデータエレメントからなる情報群。

プローブ情報

センタ側設備などで統計処理などを施されて生成された提供情報。他のシステムからの情報を活用して処理をされることもある。

ISO/TC204/WG16/SWG16.3 が定義するプローブ情報システムにおいては、プローブデータは「個人情報を含まない」と定義されている。これは、プローブ情報システムは多数の自動車や他のシステムから情報を収集し、統計的な処理などを行って交通情報などのプローブ情報を生成することを前提としているため、個々の自動車を識別する必要が無いからである（ISO の場では、個々の自動車の識別を必要とするようなプローブ情報システムは、「プローブ情報システム機能を有するテレマティクスシステム」として区別して定義されている）。

しかし、プローブ情報システム内においては、プローブデータに含まれない部分で個人情報が取り扱われる可能性がある。情報通信基盤を用いて情報を収集する際の通信 ID や、システムが車載機器を認証するために持ちうる個々の ID は個人情報である場合がある。また、コアデータエレメントは自動車の「存在位置」と「時刻」から構成されている。何らかの方法で自動車が特定される場合は、プローブデータは個人の活動に繋がる可能性がある。特に、連続したプローブデータは個人の活動履歴（移動軌跡）となり、私有地や特定の場所と結びついた情報になった場合には個人のプライバシに関する重大な問題となりうる。

プローブ情報システムを構築し普及させていくには、情報提供者の個人情報に関する不安を取り除くため、適切なシステム構築と運用を行う必要がある。

3.3 プローブ情報システムに存在する個人情報

プローブデータに直接的に個人を識別することができる情報が含まれていなくても、OECD のプライバシ・ガイドラインで言及されるように、間接的に個人が識別できる場合には個人情報として取り扱う必要がある。

本研究では、プローブ情報システムに存在する個人情報は、「プローブ情報システムが、自動車から情報通信基盤を介してプローブデータを収集する際に、直接的あるいは間接的に個人を識別することができる情報」と定義する。これは、容易に参照可能なデータベースによって個人を識別できる情報を含む。

参照可能なデータベースについては、表 3.1 のように 2 種類に分類できる。本研究では、プローブ情報システム自体が所有するデータベースに加え、外部の主

表 3.1.　個人情報を参照できるデータベース

	内部データベース	外部データベース
定義	プローブ情報システム自身が所有するデータベース	プローブ情報システム以外の主体である公共企業体あるいは民間企業が管理運営しているデータベース
例	• 加入者登録情報 • 個人とそれらのパスワードのデータベース	• 個々の住宅が身元確認可能な地図 • アドレス帳 • イエローページ • Domain name server[1] のゾーンデータベース

1 インターネット上の IP アドレスおよびドメインネーム（FQDN）に関するデータベース

体が所有するデータベースでも、容易に参照可能で間接的に個人を特定することが可能であれば、プローブ情報システムの個人情報として取り扱うこととした。

プローブ情報システムにおいて用いられる認証は、情報送信者のなりすましやサービス不能攻撃といった脅威に対応するため、情報送信者が主張する自己同一性が正当であることを確証する機能であり、認証情報には情報送信者を特定する何らかの情報が含まれる。そのため、プローブ情報システムが認証を行う場合、認証情報が個人を直接特定できる場合は個人情報となる。一方で、認証情報が特定の意味を持たない記号や数字などの文字列（パラメータ）の場合は、認証情報だけでは個人を直接特定することはできないため、認証情報が個人情報となりうる状態とは以下の様に整理される。

- 認証情報が個人を直接特定できるとき
- 認証情報だけでは個人を直接特定できないが、認証情報と特定の個人を対比できるデータベース（このようなデータベースを「認証情報データベース」と呼ぶ）が存在し、それを参照することができるとき

同様に、暗号化を行う場合、個人を特定して暗号化を行う方式と個人を特定しないで暗号化を行う方式がある。個人を特定して暗号化を行う場合、プローブデータ収集主体が送られてきたプローブメッセージを復号化するとき使用する暗号化情報は、個人情報となりうる。一方、一般的に暗号化情報は特定の意味を持たない記号や数字などの文字列（パラメータ）であり、暗号化情報だけで個人を直接特定することはできない。従って、暗号化情報が個人情報となりうる状態とは以下の様に整理される。

- 個人を特定して暗号化を行う場合であって、暗号化情報が個人を直接特定できるとき
- 個人を特定して暗号化を行う場合であって、暗号化情報だけでは個人を直接特定できないが、暗号化情報と特定の個人を対比できるデータベース（このようなデータベースを「暗号化情報データベース」と呼ぶ）が存在し、それを参照することができるとき

3.4 リファレンスアーキテクチャ

3.3 節に基づき、プローブ情報システムに存在する個人情報について検討するため、ISO CD22837 を拡張する形でリファレンスアーキテクチャを定義する。ISO CD22837 のリファレンスアーキテクチャは、プローブデータの定義を行うことが目的であり、アプリケーションが取り扱うデータについての定義を行っている。本研究では、プローブ情報システムの情報提供者と収集者で交換されるプローブデータ以外の情報も含んで個人情報を検討するため、通信関連する概念についての拡張を行った。本研究で定義するリファレンスアーキテクチャを図 3.2 に示し、追加した機能の定義を以下に述べる。

- Probe payload generation
  プローブデータや認証情報など、アプリケーション層での処理に関わるデータ群の生成を行う。プローブデータ発信者の認証やデータの正当性確認はここで行われる。
- Probe package sending
  “Probe payload generation” によって構築されたデータ群に対し、通信に必要な情報である probe header を付加してプローブデータ発信者から送信される情報パケットを作成し、プローブ収集主体に通信基盤を介して発信する。通信基盤とプローブデータ発信者の間で行われる処理はここで行われる。

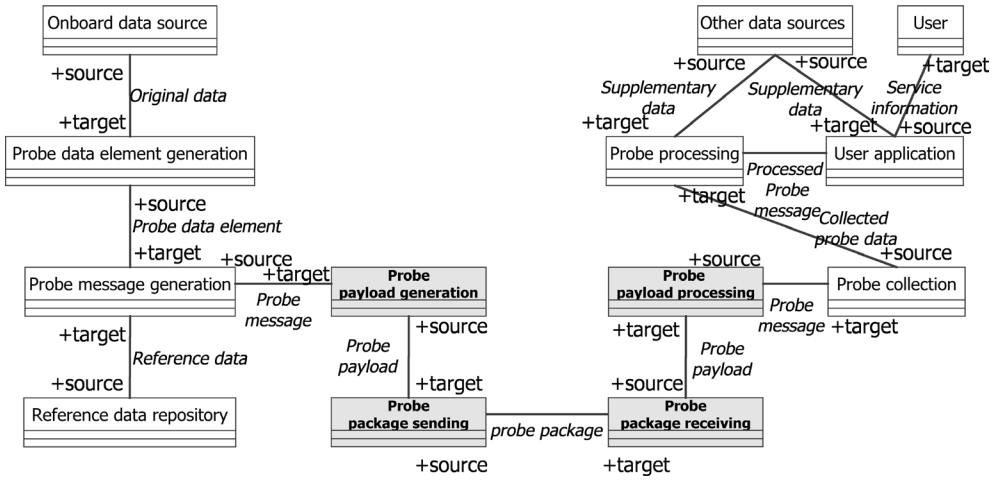

図 3.2. リファレンスアーキテクチャ

- Probe package receiving
  “Probe package sending” が発信した情報パケットを受信し、通信に必要な情報である probe header を取り除いてデータを取り出し、“probe payload processing” に送る。
- Probe payload processing
  “Probe package receiving” から受信したデータ群に対し、内部に含まれている情報に応じてプローブデータ発信者の認証やデータ正当性の検証を行った上でプローブデータを取り出す。

3.5 脅威分析

3.4 節にて定義したリファレンスアーキテクチャに基づき、プローブ情報システムに存在する個人情報についての脅威分析を行った。脅威事例については、1) プローブ情報システム特有の個人情報にかかる脅威と 2) プローブ情報システムによらない情報通信システム全般に生じる脅威の 2 種類に整理可能であり、プローブ情報システムにおいて特に求められるのは前者の脅威である。

1. プローブ情報システム特有の個人情報にかかる脅威
   a) 通信 ID の目的外利用
   通信 ID が個人情報である場合において、収集主体が本来通信にのみ利用するべき情報（通信 ID）とプローブメッセージを結合して目的外利用を行うことで、プローブ情報提供者の権利・利益を脅かしたりする行為
   b) 認証情報の目的外利用
   個人を特定することができる認証を行っている場合において、収集主体が本来認証にのみ利用するべき情報（認証情報）とプローブメッセージを結合して目的外利用を行うことで、プローブ情報提供者の権利・利益を脅かしたりする行為
   c) 暗号化情報の目的外利用
   個人を特定することが可能な暗号化によって通信路の安全を確保している場合において、収集主体が本来通信路の暗号化にのみ利用するべき情報（暗号化情報）とプローブメッセージを結合して目的外利用を行うことで、プローブ情報提供者の権利・利益を脅かしたりする行為
   d) システムの運用上知りうる情報の目的外利用
   車載機の配布・販売や、情報収集に関する取り決めにおいて知り得た個人情報を有する場合において、収集主体が知り得た情報とプローブメッセージを結合して目的外利用を行うことで、プローブ情報提供者の権利・利益を脅かしたりする行為
   e) 個人が推測可能なプローブメッセージの利用
   主体そのものがもつ DB、もしくは収集主体以外の、公的機関や企業などの DB と発信位置などを照合することで個人を推測することが可能な場合において、収集主体が該当するプローブメッセージを利用して、プローブ情報提供者の権利・利益を脅かしたりする行為
   f) 通信 ID の不正取得
   収集主体が密かに個人が特定できる通信 ID を収集することにより、プローブ情報発信者の

権利利益を脅かしたりする行為

g) 認証情報/暗号化情報の不正取得

収集主体が密かに個人が特定できる認証/暗号化情報を収集することにより、プローブ情報発信者の権利利益を脅かしたりする行為

2. プローブ情報システムによらない情報通信システム全般に生じる脅威

これに該当する脅威は、一般的な情報通信システムにも共通する脅威であるため、詳細は省略するが、以下のような脅威が考えられる。

- 車載システム・センタシステムへの攻撃
- 通信路における盗聴・改竄、なりすまし
- 車群による意図的な欺瞞情報の送信
- 故障機器が引き起こす偽情報によるシステム障害

3.6 脅威分析に基づく個人情報保護手法

3.5 節に挙げた脅威分析に基づき、プローブ情報システムを構築する際の対処方針としては、技術的な対応と運用的な対応の二つが考えられる。プローブ情報システムにおける個人情報保護は、これらのどちらか一方によって実現することは不可能であり、適切な手法で構築されたシステムの上で、適切な運用を行うことで初めて実現される。以下に二つの手法に関する考察を述べる。

技術的な対応

プローブ情報システムは、その用途や目的、規模に応じてさまざまな構築方法が考えられ、用いられる技術も、構造によって異なってくる。しかし、基本的には以下の 2 つは最低限満たされる必要がある。

1. 安全な通信路の利用
2. 匿名化処理技術

前者はプローブ情報システムに限らず、情報通信システム一般に当てはまる要素だが、情報提供者が移動する自動車であるプローブ情報システムでは、通信状態が動的に変更していくため、現在どのような通信路・通信基盤を用いているかを確認することはとても重要である。

後者は、プローブ情報システムが取り扱うプローブデータと、通信や認証時に用いられる個人情報を切り離して管理する技術である。プローブ情報システムにおいて個人情報と他の情報を適切に切断し、匿名化して取り扱うことが可能であれば、プローブ情報の活用において個人情報漏洩の危険性は限りなく低くなる。

一方、完全な匿名性が実現された場合には、悪意のある第 3 者からの故意による攻撃に対してシステムを防御することが難しくなり、システムの運用に深刻な影響を与える。そのため、特別な権限を持つ管理者（escrow agent）のみは、必要に応じて匿名化情報から個を特定できる機能を備えるなどの技術が必要になる。

運用的な対応

プローブ情報システムにおいて個人情報を保護するためには、適切に構築されたシステムの上で、プローブデータとその付帯情報を適切に取り扱う必要がある。こうした取り扱いに関するルールを定めそれに基づき運用することは、システムの社会的受容性を高めると共に、普及展開を可能にする。また、こうした運用ルールは利用者をはじめとして広く社会に公開されるべきであり、情報開示などの要求に迅速に対応できるようなインターフェイスを用意することも重要である。

3.7 運用ルールの標準化活動

3.6 節で述べた脅威分析に基づく個人情報保護手法、特に運用的な対応については、その必要性を啓蒙すると共に、個人情報を適切に保護するためのプローブ情報システムの運用に関して統一した基準を策定する必要がある。本研究では、前述までの検討結果をもとに、ISO/TC204/WG16 の中でプローブ情報システムにおける個人情報保護 [13] についての議論を行い、国際的な基本原則に関する標準化を行っている。

3.8 おわりに

プローブ情報システムは渋滞の解消や公共交通機関の利便性向上などの社会的利益に資するシステムである一方、自動車が情報通信基盤を用いて車両の位置や状態に関する通信を行うため、適切なシステム構築・運用がなされない場合には、個人情報の漏洩に繋がる可能性がある。

本研究では、プローブ情報システムにおける個人情報に関する脅威について分析し、これらの脅威についての保護手法（プロテクションメソッド）を述べた。また、こうした研究成果の一部は国際的なルー

ルとして国際標準化提案を行っており、その活動状況についても報告を行った。今後は、こうした研究成果をもとに、各国の状況を鑑みつつ、グローバルな統一ルールを策定するため、諸国のさらなる理解と協力を取り付ける活動を進めると共に、ルールに基づく個人情報保護を実現する具体的なシステムの構築、特に規模性を踏まえたシステムの開発が求められる。

なお、本研究は、経済産業省の委託を受け、慶應義塾大学 SFC 研究所が行った委託事業の結果を取りまとめたものである。本研究の実施にあたり多大な支援を頂いた経済産業省自動車課、および産業技術環境局産業基盤標準化推進室の皆様、および、ISO/TC204/WG16（特に SWG16.3 プライバシグループ）のメンバに謝意を表します。

第 4 章　まとめ

本年度の iCAR ワーキンググループの研究活動は、インターネット移動体通信技術の研究開発だけでなく、センサデータ（プローブデータ）の情報伝達アルゴリズムや安全な流通に関わる技術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。

また、2007 年度は、MIP6 および NEMO の機能などの移動体通信技術、特に MR の機能に関して、Nautilus6 ワーキンググループと議論を重ねてきた。この議論と両ワーキンググループにおいて蓄積した技術および情報を 2008 年度の活動につなげていく予定である。センサネットワークの構成やデータ形式、データ交換などに関しては Live E! プロジェクトと適宜連携・意見交換を行っており、今後も協調しつつ議論を継続していく。

今後も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。