

第12部

自動車を含むインターネット環境の 構築

第1章 序章

自動車を取り巻くシステムは高度に情報化されつつある。現在、世界各国で高度道路交通システム (Intelligent Transport Systems: ITS) が実現されつつあり、交通の管理をより高度なものにしようとしている。

自動車の情報化には大きく2つの意義があると考えられる。1つはITSの様に道路交通システムを高度化させるものであり、もう1つは情報社会システムの中に自動車を存在させるものである。前者は、安全、環境等の広い分野を視野に入れて道路交通システムを円滑に運用することを目標とする。後者は、情報化社会システムの中での自動車の担う役割を検討し、システムとして実現することを目標とする。本プロジェクトでは、常にこの2つの視点に立ちながら、自動車の情報化を目指す。

インターネットカーワーキンググループでは、現在、自動車をインターネットに接続し、情報が流通出来る機構を構築することを目標として活動をしている。インターネットは広く普及した自由にデジタル情報を交換できる情報基盤である。ここに自動車を接続することにより、自動車の情報を一般の情報システムで利用したり、一般に流通している情報を自動車内で利用することが可能となる。また、家電などの情報化が盛んな機器と連係したシステムを構築することも可能となる。自動車は人間の行動を良く反映しており、広く分散して存在している。このため、自動車をセンサーとして捉えることにより、インターネット世界の五感とすることもできる。逆に自動車側から見た場合、閉鎖された空間に情報の流通経路を採り入れることにより、人間にとってより快適な空間とすることが可能である。

自動車をインターネットに接続する為には幾つかの課題がある。本プロジェクトではこれらの課題を以下の6つの研究領域に分けて研究活動を行ってきた。

- ハードウェア
- 基盤ソフトウェア
- 通信システム
- GNSS 支援システム

- 地理的位置情報システム

- アプリケーション

ハードウェアの分野では昨年度までの研究成果を受け、新たな実験環境を構築すべく、専用のハードウェアを作成した。基盤ソフトウェアの分野では、実験に適したOSとしてBSDを選択し、専用のハードウェア上への環境構築を行なった。通信システムの分野では、複数の通信デバイスを利用する際の問題点を洗い出し、実際のシステムを構築し、その可用性を検討した。GNSSの分野では、インターネットを介してGNSS補正情報を配送する仕組みを設計・実装し、標準化への足掛かりを作った。地理的位置情報の分野では、情報の提供や規模性を考慮に入れたサーバを構築し、実験を行なうとともに、プライバシーの保護に関する研究を進めた。アプリケーションの分野では、地理的位置情報を用いた情報検索サービスの構築及びインターネット自動車に備わる機能を利用した地図作成アプリケーション等の実現可能性を示した。

本報告書では、これらの中からSFC Open Research Forum'99における実験報告、GNSS補正情報システム、通信アーキテクチャ、地理的位置情報システムとそのプライバシー保護機構についてを報告する。なお、詳細な報告については「インターネット自動車プロジェクト1999年度研究報告書」参照していただきたい。

第2章 SFC Open Research Forum '99 報告

インターネット自動車コンソーシアムでは、1999年11月19日から20日にかけて行なわれたSFC Open Research Forum (ORF) において、インターネット自動車システムのデモンストレーションをおこなった。本章では、ここで行なったデモンストレーションについて説明する。

2.1 目的

インターネット自動車コンソーシアムでは、1999年度半ばまでに様々な開発をしてきた。1998年度のデモンストレーションからの進捗で特に大きな技術

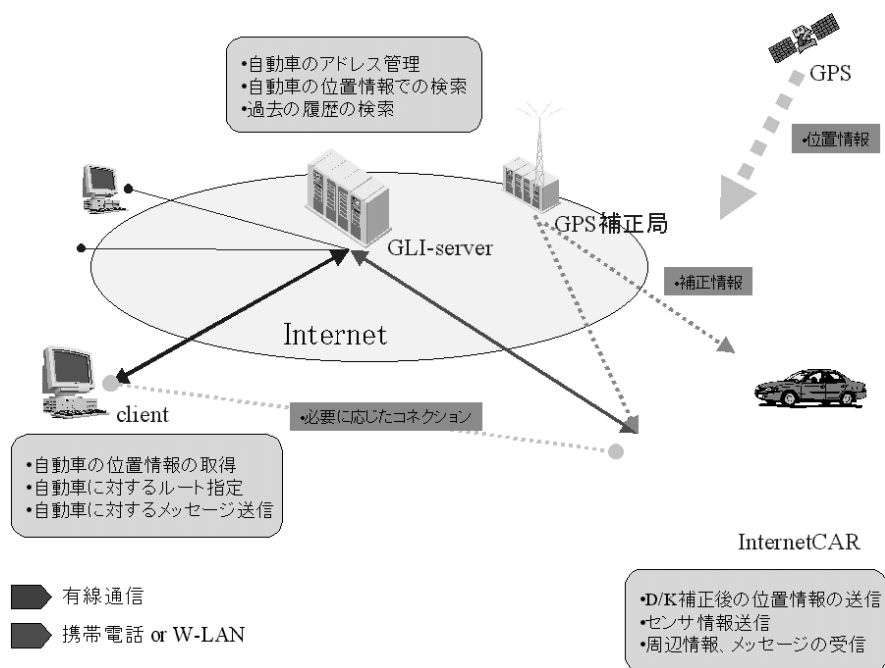


図 2.1 全体構成

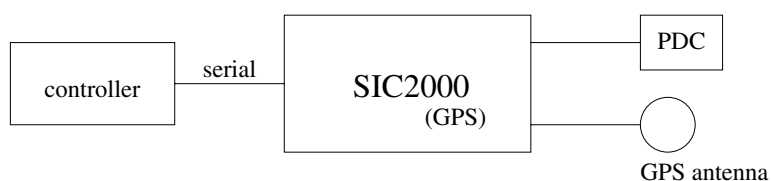


図 2.2 車載機の構成 (普通構成)

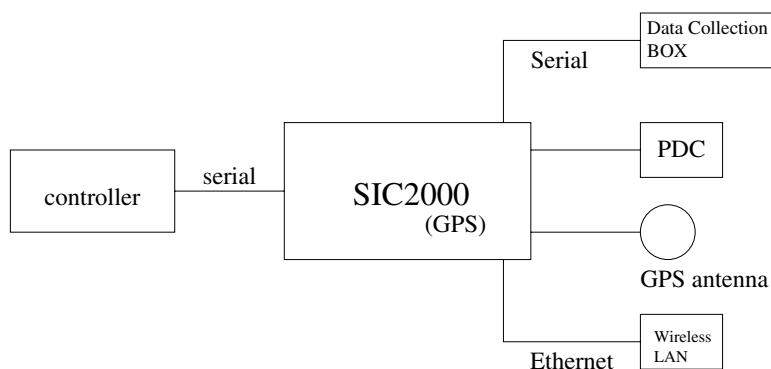


図 2.3 車載機の構成 (高機能型)

開発は、以下の様なものであった。

- 車載専用ハードウェア SIC2000 の開発
- SIC2000 上へのソフトウェアの移植
- 新たなデータベース構造をもつ GLI Server の

開発

- 新たな方式による通信メディア切替え技術の開発
- 安定した GNSS 補正情報配信機構の開発

今回の ORF においては、上記の技術を一つの環境に統合し、デモンストレーションを行なうことを目標とした。

デモンストレーションを行なうことにより、下記の 2 つの目的を達成することができる。

- コンソーシアムにおける技術開発状況を多くの人々に知らしめる。
- これまで開発して来た技術が 1 つの統合環境として動作することを証明する。

2.2 デモンストレーション概要

今年度の ORF におけるデモンストレーションは前節で述べた目標を実現する為、以下のような方針とした。

- 車載機は SIC2000 に統合し、車載アプリケーションは SIC2000 上で動作させる。
- 自動車の位置を含む情報は、新たな GLI サーバ上に登録し、検索ソフトウェアを使った複数の検索方法をデモンストレーションする。
- 通信インフラストラクチャは最低 2 種用意し、通信が連続的に切替えられる様子をデモンストレーションする。
- GNSS ソフトウェアは新たなものを利用し、安定運用を目指す。

上記の方針を受けて、デモンストレーション環境を図 2.1 の様に設計した。この環境では、自動車を 3 台用意し、キャンパス内およびキャンパスの近郊を走行する。キャンパス内の一部には無線 LAN 環境を用意し、無線 LAN のサービスエリア下では自動車は無線 LAN によりインターネットへ接続される。車載機は最低でも GPS からの情報取得を行ない、携帯電話もしくは無線 LAN を介して取得した情報をキャンパス内に設置された GLI サーバへ登録する。一方、デモンストレーション会場では GLI クライアントを用意し、現在の各自動車の位置の表示、条件にあった検索などを行なう。更に、自動車の位置を正確に知る為に、ディファレンシャル GPS の補正情報をインターネットを介して自動車に送る。

2.3 システム構成

本節では、ORF のデモンストレーションにおける各部の詳細構成について述べる。

2.3.1 車載機

今回のデモンストレーションで使用した車載機の構成を図 2.2 に示す。計算機としては SIC2000 を利用し、GPS を内蔵している。電源は自動車毎に異なるが、シガーライタープラグやバッテリーなどから供給した。通信機器としては PCMCIA の携帯モデムカードを介して携帯電話 (PDC) を利用している。

また、更に無線 LAN とデータ収集 BOX を搭載した高機能型も 1 台用意した。高機能型の構成を図 2.3 に示す。

車載機のソフトウェアは、オペレーティングシステムとしては NetBSD を採用している。また、Mobile-IP および MIBSocket の機能を付加してある。アプリケーションソフトウェアとしては、ijj-ppp、ネットワークインターフェイス切り替え用アプリケーション、Mobile-IP のユーザ空間デモン、D/K-GNSS 補正情報配信ソフトウェア、GLI エージェントおよびコントローラ表示用アプリケーションが搭載されている。またリモートメンテナンスの為に、幾つかのユーザコマンドと共に telnetd も用意されている。

SIC2000 はアクセサリスイッチ (ACC) によって電源オンとなり起動する。カーネルが起動した後、GPS の初期化やネットワークの初期化などが行なわれ、GLI エージェント等が起動される。電源オフは、SIC2000 ではソフトウェア的にオフにすることも可能であるが、今回はハードウェアタイマによって電源を落すこととした。起動にはおよそ 20 秒程度の時間がかかる。GPS での位置取得が可能になるまでの時間は状況によって大きく変化するが、10 秒程度から 3 分程度の時間が必要となる。また、ijj-ppp によってネットワークが利用可能になるまでは 30 秒程度必要である。

デモンストレーション時の SIC2000 の写真を図 2.4 に示す。

2.3.2 通信部

通信部は以下の 2 つの要件を満たす必要がある。これらの要件は基本的に、インターネットにおける移動体通信に関する要件である。



図 2.4 デモで使した SIC2000

- インターネット側からの発呼
- 通信デバイス切り替え後の通信継続性

今回のデモンストレーションでは、上記の要件を同時に満たすことの可能な Mobile-IP をシステムに導入した。Mobile-IP はホームエージェントと呼ばれるホストを本来移動ホストが存在すべきネットワークに用意し、移動ホストへのパケットをホームエージェントが移動ホストに転送することによってホストの移動透過性を提供している。移動ホストは移動する度に一時アドレスもしくは自分の面倒を見てくれる移動先のネットワーク上のホストを取得し、ホームエージェントに登録する。ホームエージェントはこの情報を利用して移動ホストのパケットを中継する。

デモンストレーションでの通信デバイスとしては、無線 LAN と携帯電話を利用した。無線 LAN は基地局 2 機を構内に、内周道路の半分がサービスエリアとなるように設置した。基地局は研究室のネットワークにブリッジ接続されている。また、携帯電話では PPP を使い、大学のダイヤルアップポートへ接続した。全体のネットワーク構成を図 2.5 に示す。図において上半分が無線 LAN のサービスエリア、下半分がサービスエリア外で携帯電話を利用する部分である。インターネット上には移動ホスト (ここで

は自動車内の SIC2000) のホームエージェントが用意されており、現在の移動ホストの一時アドレスを管理している。

携帯電話自体は NTT DoCoMo の DoPa (PDC-P) 用のものを用いたが、接続プロバイダが通過プロトコルの制限をしており、Mobile-IP が利用不能になるため、今回は PDC での利用とし、大学内のダイヤルアップポートへの接続とした。このため、ijp-ppp によってネットワークが利用可能になるまでは SIC2000 が起動しはじめてから 1 分程度の時間が必要である。また、このようにして接続された PPP によるリンクは、電波状態などの原因により切断されるまでは、能動的に切断することなく、常時接続の状態となる。無線 LAN に切り替わった後も無線 LAN から携帯電話への切り替えを高速化するために、接続を維持する。また、外的要因によって切断された場合も、自動的に速やかに再接続を試みる。

無線 LAN には BreezeCOM のアクセスポイントと移動局を利用した。これは、10BaseT 経由で接続するタイプのもので、特殊なデバイスドライバ等を必要としない。また、SNMP を使用することにより、機器の様々な状態 (電波強度、接続中のアクセスポイントの ID など) を取得することが可能である。ネットワークインタフェース切り替えでは、この情報を利用した。無線 LAN 装置から電波強度などの

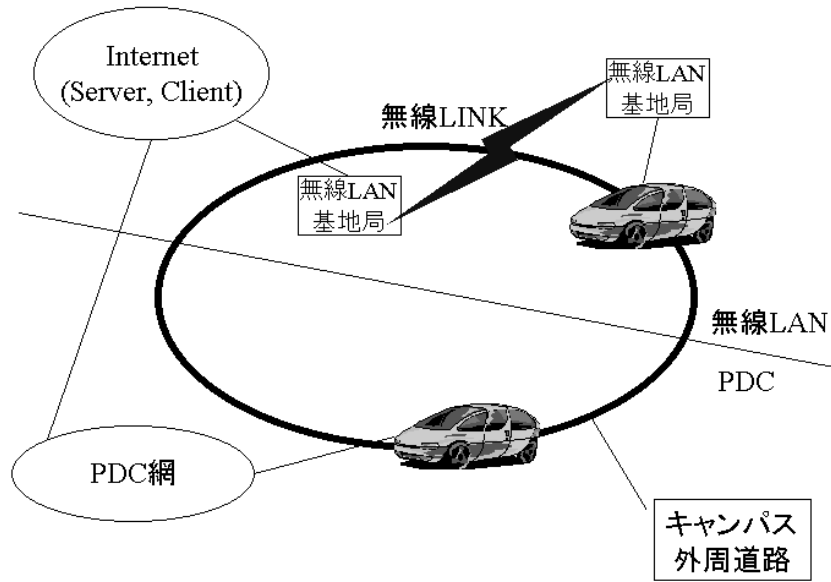


図 2.5 ネットワーク構成

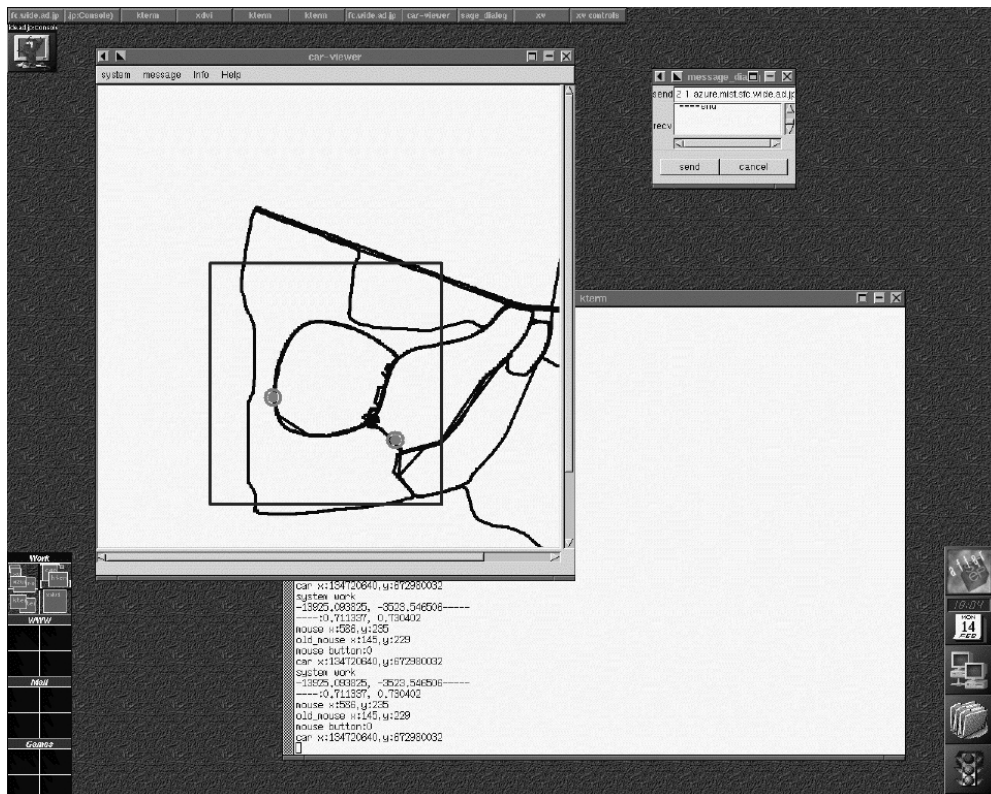


図 2.6 デモンストレーション用アプリケーションのスクリーンダンプ

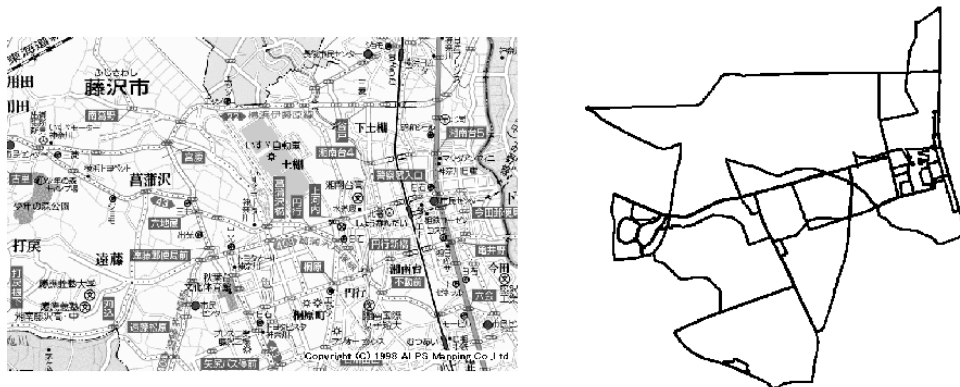


図 2.7 GLI を利用した地図の作成

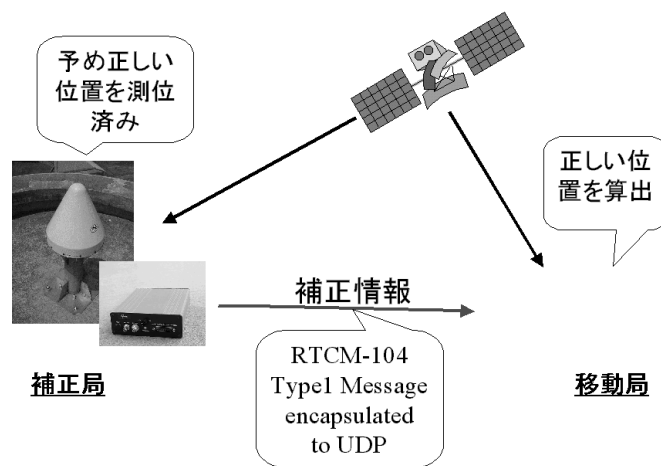


図 2.8 GNSS 差動補正の仕組み

情報を得る為には SNMP を用いるが、このためには SIC2000 と無線 LAN 機器の間で IP 的に通信を行なう必要がある。今回の実験では車載の無線 LAN 機器と SIC2000 の間にプライベートネットワークアドレスを設定し、SNMP を利用できる環境を構築した。

無線 LAN によるネットワーク接続では、DHCP を用いてアドレスの自動取得機能を導入した。自動車が無線 LAN のサービスエリアに入ると、SNMP で取得できる電波強度によりこれを検知し、DHCP クライアントを起動してアドレスを取得する。取得が終了すると、Mobile-IP のアップデートメッセージをホームエージェントに送り、また、経路が無線 LAN を利用するように変更され、ネットワークインタフェース切り替えが行なわれる。

2.3.3 GLI 部とアプリケーション

GLI システムは、地理的位置情報をインターネット上で扱う為の仕組みである。インターネット上のエンティティの地理的位置を管理し、他の計算機がその情報を利用することを可能にしている。

今回のデモンストレーションでは、新たな GLI システムを導入した。新たなシステムでは自動車 (移動ホストの ID) を鍵とした検索の他に、位置および時間を鍵とした検索を可能としている。具体的には、ある範囲を指定した自動車の検索、ある位置から最も近くに存在する自動車の検索等が可能となっている。

今回のデモンストレーションでは、1 台の GLI サーバを用いて自動車の位置を管理した。自動車上の GLI エージェントは、1 秒毎に ID と共に現在の位置を緯度・経度・高度の形式で GLI サーバへ通知する。GLI サーバではこの情報より、個々の検索ア

ルゴリズム毎のデータベースを構築し、クライアントへのサービスに備える。

このような GLI 部を利用して、自動車の走っている様子を表示する為のアプリケーションを作成し、デモンストレーション会場で運用した。このアプリケーションでは GLI サーバの機能を利用して、自動車の現在位置等を表示することが可能である。さらに、直接自動車と通信を行なうことにより、リアルタイムで自動車が走行している様子をモニタリングする機能も備えている。アプリケーションのスクリーンダンプを図 2.6 に示す。

また、予備実験として、インターネット自動車システムを用いて地図を作成する実験を行なった。実際に自動車が走行した走行履歴をプロットすることにより、道路地図を作成する実験である。実際に作成した地図を図 2.7 に示す。作成された地図の精度は実用に十分であり、ベクトル化などを行なうことにより、実際の地図の補強材料として利用可能であることがわかった。

2.3.4 GNSS 部

Global Navigation Satellite System (GNSS) とは、GPS 等の衛星を使った位置測量システムの総称である。近年の情報サービスでは位置情報が大きな意味を持つようになり、GNSS のような位置測量システムが多く利用されるようになった。また、単独測位の GNSS システムでは数十メートルの精度での測位が限界である為、差動型、干渉型などの補正を組み込んだ測位手法が利用されるようになっている。今回のデモンストレーションでは、差動型補正を導入した GPS を利用することとした。システムでは干渉型を利用することも可能であるが、通信速度が不十分と判断して差動型とした。PDC を利用した場合の通信速度は 9600 bps である。これは、干渉型を利用するぎりぎりの速度であり、他の通信と通信路を共有することが難しい。

利用した GNSS 補正情報配信プロトコルは UDP を利用し、RTCM-104 のメッセージを基準局から移動局まで直接配送するものである。RTCM-104 の 1 メッセージを UDP の 1 データグラムにカプセル化し、配送する。基準局側にはサーバを設置し、移動局側のクライアントからの補正情報要求メッセージにより、補正情報の配信を始める。要求メッセージは定期的に送られ、要求が続いている間は補正情

報が配送される。今回のデモンストレーションでは差動型補正の GPS による位置取得を行なったため、移動局に配送した RTCM-104 メッセージは Type 1 のみである。補正の概要を図 2.8 に示す。

2.4 まとめ

今回のデモンストレーションでは、開発した技術を統合し、如何に表現するかを目標とした。今回運用したものを以下にまとめる。

- NetBSD on SIC2000
- SIC2000 コントローラによる表示機能
- Mobile-IP
- MIBSocket (カーネルからのネットワーク状態の取得)
- ネットワークインタフェーススイッチ
- 位置情報データベースと車載機からの登録
- 自動車との直接通信による位置表示
- GLI を介した検索 (自動車指定、最近検索、エリア検索)
- インターネットによる D-GPS 補正

今回のデモンストレーションでは、個々の技術は順調に動作した。しかし、これらを組み合わせる場合に幾つかの問題が発生した。問題は特に、ネットワーク周りで多く見られた。以下に、問題と今回の解決策をまとめる。

OS のバッファのワード境界問題

NetBSD on SIC2000 上でネットワークソフトウェアを利用するにあたり、PPP および SNMP ソフトウェアでワード境界問題が発生した。カーネルから得たバッファ(mbuf)がワード境界に揃っていない為、long 等のデータ型をそのまま扱えない問題である。本来は、カーネルから渡されるバッファをワード境界に揃えるようにカーネル側を改良するべきであるが、今回は、アプリケーションソフトウェア側でバッファをコピーし、ワード境界を揃えることで対応した。

論理ネットワークの扱い

今回は Ethernet を経由して接続するタイプの無線 LAN 機器を利用した。その為、無線 LAN の状態を知る為に SNMP を利用する必要がある。この為無線部は、外部との通信に利用する為のグローバルアドレスネットワークと、無線 LAN 機器と通信する為のローカルアドレスネットワークの 2 つの論理ネットワークが存在する必要があった。つまり、SIC2000 の Ethernet インターフェイスには 2 つのアドレスを設定する必要が生じた。ここで、Mobile-IP が自分のアドレスを登録する際に、場合によってはローカルアドレスを登録してしまうという問題が生じる。今回は、ローカルアドレスを無視するコードを Mobile-IP ソフトウェアに導入することにより、この問題に対処した。

会場におけるデモンストレーションとしては、今回はアプリケーションを見てもらうことが主となり、導入された新しい技術を十分に見せることができなかった。今後、デモンストレーションを行なう場合は、複雑な技術をわかりやすく見せる為の工夫が必要である。

第 3 章 インターネットを用いた補正情報配信システムの設計と実装

本章では、今回設計および実装を行った GNSS 補正情報配信機構についてのべる。

3.1 本研究の背景

GPS (Global Positioning System) に代表される人工衛星を利用した測位システム (以下 GNSS: Global Navigation Satellite System) は高精度な位置情報を地球上のあらゆる場所で提供することを可能にするシステムである。

GNSS では高精度に軌道情報を把握した最低 4 つの人工衛星からの電波を受信することにより、地球上での位置を決定するシステムである。

GPS は米軍が管理する GNSS システムであり現在、現在も運用が続けられている。このうち一部が民生利用に開放されており、誰もが自由に利用することが出来る。2000 年現在、米国の GPS 以外にも

ロシアの GLONASS が部分運用中であり、EU の GALILEO が計画中であり、2008 年の稼働を目指している。

GNSS はカーナビゲーションや船舶、航空機の航法システムをはじめ、測量や地球物理の研究まで広く利用されているが、我々がもっとも日常的に接するシステムとしてはカーナビゲーションがあげられる。

電子化された地図と位置情報およびそれに付随する情報を組み合わせて利用するカーナビゲーションは現在もっとも一般に普及している GNSS を用いたシステムである。しかしながら、GNSS を用いた単独測位は誤差が大きく、GNSS のうちもっとも一般的に利用されている米国の GPS の民生利用では約 100m 程度の誤差が生じる。

そこで、衛星測位での精度を高める研究、サービスが多く存在する。このうち、差動方式と呼ばれるものがある。差動測位は 2 地点で同時に測位し、その際の共通の誤差要因について取り除こうと言うものである。ここで、2 地点の一方を基準局 (BS: Base Station)、もう一方を移動局 (RS: Rover Station) とする。基準局ではあらかじめ高精度で緯度経度高度の位置情報が分かっている。

この方式はその情報を利用して測位衛星と地上の間の大気の影響などの共通の誤差要因を取り除き移動局での測位の精度の向上を図るものである。本論文ではこの測位精度の向上を補正と呼ぶ。こういった方式を取るものにディファレンシャル (differential) 方式やキネマティック (kinematic) 方式がある。

Differential 方式を用いた DGPS はあらかじめ位置を測定した基準局上でリアルタイムに誤差を算出し、算出された誤差を移動体側の GPS 受信機で利用することにより精度を向上させる方式であり、その誤差を 1m 程度に減少させることが出来る。

さらに精度の高い位置情報を得ることの出来る Real-Time Kinematic GPS は衛星から送信される搬送波の位相を利用することにより、精度を向上させる方法である。RTK-GPS を用いることにより実時間計測において数 cm 程度の精度と測量並の精度で位置情報を得ることが出来る。しかしながら、RTK-GPS を行うためには DGPS に比べ補正情報の量が増大し、また許容遅延時間が小さくなる。

これらの実時間な高精度測位を行う場合には、何らかの手段で補正のための情報を基準局から移動局に送信する必要がある。本研究では、この実時間で

の高精度な測位を目標としている。

3.2 本研究の目的

一般に、D/RTK-GNSS を用いた測位には GNSS 受信機と補正情報を送受信するための機器、測位した情報を得るための計算機が必要である。従来、D/RTK-GNSS の補正情報は FM ラジオの副搬送波、MCA 無線、中波ビーコンを用いて配送されている。しかしながらこれらの方式には導入時のサービス提供者側の負担が大きい、専用の受信機が必要になるなどの数々の問題点があった。そこで、本研究では補正情報配送の通信路としてインターネットを用い、それらの問題点を解消する。

本研究では、主に以下のことを行う。

- 補正情報をインターネットを用いて配送する機構の設計、実装を行う。
- 補正情報をインターネットで配送する際のプロトコルの仕様を設計する。

本研究では、主に移動計算機の利用者が高精度の D/RTK-GNSS を利用する際、補正情報を容易に利用できる環境を提供する。

具体的には、基準局からインターネット上のユーザへ補正情報を配送する機構および、配送プロトコルについて設計、実装を行った。

従来補正情報の多くは RTCM SC-104 形式 [102] である。この形式は狭帯域かつ信頼性の低い通信路を想定したものであり、インターネット上を RTCM SC-104 形式を用いて補正情報を配送するのは効率が悪い。そこでインターネットを用いて補正情報を配送するのに適したプロトコルを設計する必要がある。

また、インターネット上ではサービスエリアを限定する必要はない。よって、移動局で使用するのに最も適した補正情報が配送されることが望まれる。そのためには補正情報について抽象化を行い要求に基づく配送が行われる必要がある。

3.3 インターネットを用いる配送機構の提案

本節では、インターネットを用いる補正情報配送機構のモデルを提示する。

3.3.1 本機構の目的

D-RTK/GNSS を用いて精度の高い測位を行う場合、移動局として以下の要件を満たすことが重要である。本研究で開発する機構の目的はこれらの要件を満たすシステムを構築し、その性能を明らかにすることである。

- 必要な補正情報の選択
移動局が必要とする補正情報はその位置や測位方法によって、それぞれ異なっている。本機構ではそれぞれの移動局に対して適切な情報が提供される必要がある。さらに移動局で、測位に使用される補正情報のフォーマットが一致しなければならない。GNSS 受信機への入力は一般的には RTCM SC104 形式が利用されることが多いが、これは補正情報の配送機構内部において別のフォーマットを取ることを許さないものではなく、よりインターネットに適した形式を利用することが望ましい。
- 地理的な近さ
移動局と基準局は地理的に近い方が良い。これは測位に利用する衛星の位置関係および衛星と受信局との間の大気や電離層の影響など様々な要因に大きな差がない方が良好な測位を行えるからである。
- 衛星の一致
移動局、基準局それぞれから観測される測位衛星がディファレンシャル測位では 4 個以上、リアルタイムキネマティック測位では 8 個以上同一のものが観測されなければいけない。
- 遅延の少さ
リアルタイム測位の場合には、移動局と基準局の通信の遅延は少なければ少ないほど精度のよい測位が行える。
- 通信帯域の確保
移動局と基準局との間で十分な通信帯域が確保されなければならない。

既存の補正情報配送機構ではこれらの要件が導入時に決定してしまうことであり、導入後の変更は容易ではない。このような要件は通信媒体として何を利用するかで決定されることが多く、システムは通信媒体を含めて決定されているからである。インター

ネットを用いることにより、規定される通信手段を物理的な通信媒体から仮想的なインターネット接続へと変えることが出来る。そのため、今後の技術の進歩やコストの低下、また測位を行う場所などに合わせて自由に通信媒体を選択することが可能になる。

このようにシステムが既存のシステムとの互換性を保ちつつ発展性を持つ点も我々の提案するシステムの優位な点であると考えられる。

3.3.2 補正情報配送モデルの提示

本機構で用いるモデルを補正情報配送モデルとし、以下に述べる要素から構成されるものとする。補正情報を生成する基準局、それを利用する移動局、さらにそれらの配送を行う配送局より構成される。モデルを図 3.1 に示す。これは既存の補正情報配送機構の問題点を考慮した結果である。

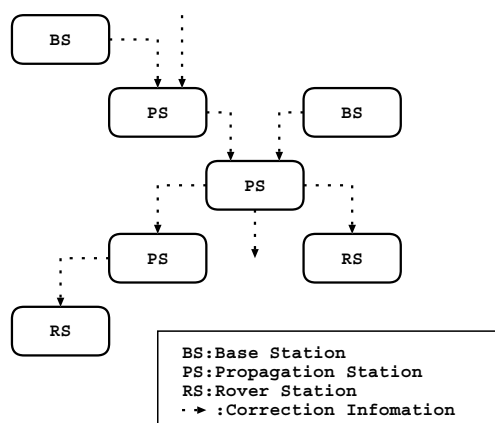


図 3.1 System Tree

- 補正情報の表現

補正情報を表現する。これによってどのような補正情報を取得するかを表現して要求を与える。

- 規模性を考慮する

一極集中せず分散して補正情報を提供できるようにする。

- サービス透過性

どの基準局にこういった補正情報が存在するのかを考慮することなく要求を行うことができるようにする。

上記を考慮することで図 3.1 のような階層化が可

能で補正情報を投下適に扱うことができるモデルを提案する。

各局の機能を以下のように定義する。さらに、補正情報の送信側を上流 (局)、受信側を下流 (局) とする。

- 基準局 (BS: Base Station)

補正情報を生成し、下流局へ送信する。下流局は、移動局、配送局、またはマルチキャストグループの場合が有り得る。図 3.2 を参照。

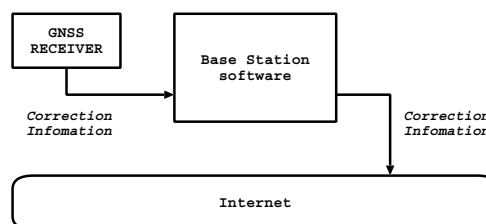


図 3.2 Base Station

- 移動局 (RS: Rover Station)

補正情報を受信し、利用する。必要な基準局の補正情報を上流局に要求する。図 3.3 を参照。

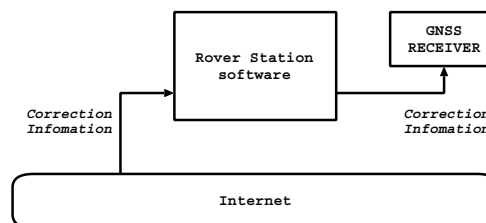


図 3.3 Rover Station

- 配送局 (PS: Propagation Station)

上流局からの補正情報を下流局に転送する。また、下流局の要求に応じて、どの基準局からの情報を配信するか取捨選択する。図 3.4 を参照。

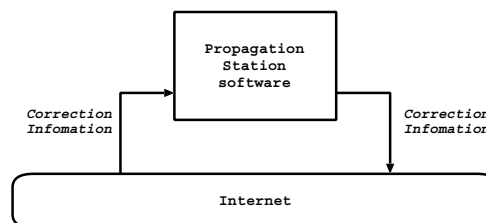


図 3.4 Propagation Station

また、これらのうち最低限、基準局と移動局が 1 つずつあれば本モデルは構成できるとする。また、基準局と移動局の間には幾つの配送局が存在しても良い。

本プロジェクトではこのモデルに従いプロトコルやそれぞれの局で利用するソフトウェアの設計と実装を行った。

3.3.3 本機構の概要

本機構は、D/RTK-GNSS の補正情報の配送機能を提供する。補正情報の配送を下流局の要求に基づいて行う配送局という概念を導入する。配送局の導入によって帯域の節約や補正の精度の向上などの効果が期待される。

本機構は補正情報配送モデルより構成される。基準局、移動局は以下から構成される。

- GNSS 用アンテナ

- GNSS レシーバ

- 計算機

以下のものを備えたものである必要がある。

- 補正情報配送プログラム
- ネットワークインタフェース
- GNSS 受信機インタフェース

基準局、移動局のアンテナを図 3.5、図 3.6 に示す。

配送局は計算機のみから構成される。

補正情報を配送する際に様々な要素が考えられる。どのような補正情報をいつどのような送信間隔で送信するのかを表現する必要がある。本機構で抽象化するものを以下に挙げ、説明する。

- 基準局の緯度経度

基準局の緯度経度をあらわす。緯度は dd.ddddd...、経度は ddd.ddddd... である。(それぞれ double であらわされるため、15 桁まで)

- 基準局の識別子

基準局を識別する必要がある、基準局 ID(BSID) として第 3.3.3 節で後述する。

- RTCM SC-104 にあるメッセージタイプ 1-63 のうち複数のものである。

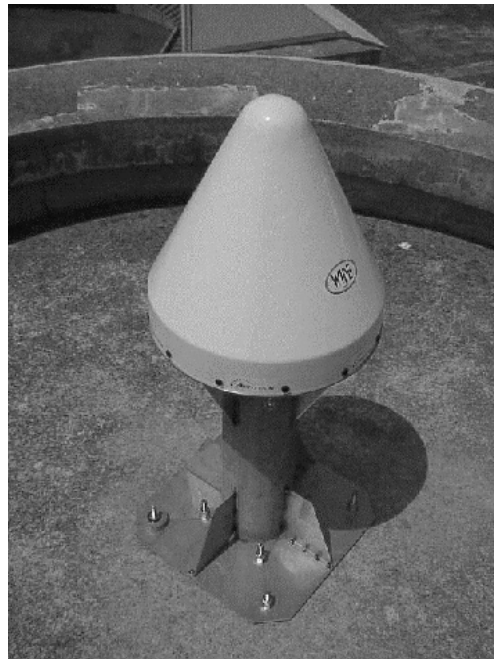


図 3.5 Base Station's Antenna



図 3.6 Rover Station's Antenna

- 補正情報の送信間隔

上流局から下流局への補正情報の送信間隔をあらわす。基準局で補正情報を生成する間隔が最大値であり、単位は秒である。

本機構では、基準局の ID が一意に定義されている必要がある。しかし、RTCM SC-104 の規格では基準局 ID(RID: Reference Station ID) が 12bit し定義できない。これは 4096 局の区別しかできずインターネットのような大規模システムでは不十分である。そこで本機構では以下のように基準局 ID を定義し、将来的な基準局の増加にも対応できるようにした。

まず始めに全体の基準局 ID を 44bit 長とし、インターネット基準局 ID (I-BSID: Internet Base Station ID) とする。インターネット基準局 ID の前半 32bit 部分をエリア ID とし、後半 12bit 部分をローカル ID とする。図 3.7 を参照。

ここで、32bit 長のエリア ID は後述する方法で基準局の緯度経度から一意に定まる。また、12bit 長のローカル ID はそのエリア内で一意であれば良い。その定義の仕方は次に述べる。

BSID on the Internet

$$\text{Area BSID} + \text{local BSID} = \text{I-BSID}$$

図 3.7 Internet BSID

図 3.8 のように地球上を緯度経度に応じて分割し、それをエリアと呼ぶ。緯度経度をそれぞれに 16bit ずつで分割する。エリア ID はそれにつけられる ID である。

始点 (0,0) は北緯 90 度、西経 180 度とする。東経の正方向に向かって x 軸、南緯の正方向に向かって y 軸を設定する。したがって、北緯 $long$ 度、東経 lat では次の式ようになる。ただし、南緯、西経はそれぞれ北緯、東経の負の値を取るとする。

$$(x, y) = \left(\left\lfloor \frac{(90 - long) \times 65534}{180} \right\rfloor, \left\lfloor \frac{(lat + 180) \times 65534}{360} \right\rfloor \right) \quad (3.1)$$

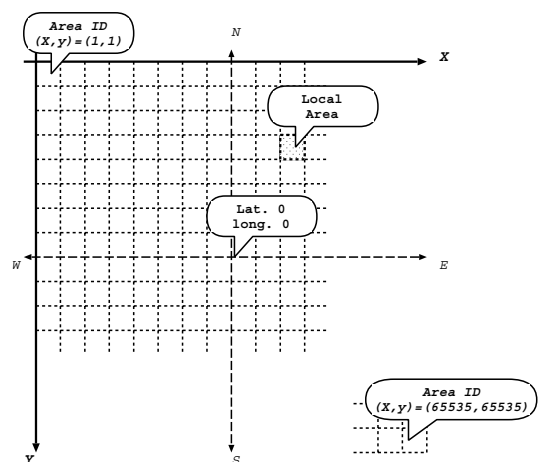


図 3.8 Area ID

ローカル ID は同一なエリア内でエリア内で一意である。本機構はローカル ID の割り振りの方法について議論しない。ただし、ローカル ID を前述の RTCM SC-104 に定める RID にそのまま使用する事は可能である。図 3.9 のようにエリアの外で同じ

ID を使うことはあり得る。

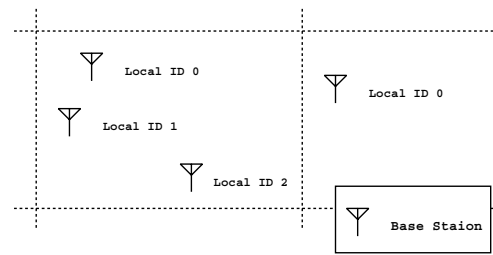


図 3.9 Local ID

3.4 本年度の進捗および今後の課題、予定

本年度は、提案したモデルに基づき Scrache と呼ぶ実装を行ない実験・評価を行なった。実験に用いた GNSS 基準局は、慶応大学湘南藤沢キャンパスおよび奈良先端科学技術大学院大学、WNOC-TOKYO の 3 箇所の作業がほぼ完了している。また、残りの地点に関しては現在作業中である。

開発中のソフトウェアおよび実験局を利用した実験を行い、まとまった成果を挙げることが出来たと考えている。この成果をまとめ ION-GPS99 (ナッシュビル:アメリカ) および GNSS'99 (ジェノバ:イタリア) の 2 つの GNSS に関する国際会議において Internet を用いた補正情報の配信サービスに関して成果の発表を行うことが出来た。このうち ION-GPS99 ではセッションごとの論文賞を受けることが出来、インターネットを利用した高精度な GNSS に対する関心の高さを伺い知ることが出来た。

今後の予定としては、さらに研究をすすめ、インターネットならではの広域性と高帯域性を利用した広域環境での補強システムに準ずるシステムの構築や、インターネットを利用する上で起こりうる問題点となる遅延のジッタに関する問題や、サーバ選択に関する問題などを解決するためにさらに研究をすすめて行く予定である。

第4章 通信アーキテクチャ

4.1 目的

インターネット自動車では GNSS の補正情報や地理的位置情報等、リアルタイム性が重要となる通信を、常時ネットワークに接続しながら行う必要がある。また将来理想となるインターネット自動車通信システムにおいては、これらの補正情報や位置情報に加えて、音声や動画等のストリームデータの配信もリアルタイムで行えることが望まれる。またこれに加えて、隣接した車同士での車車間通信を実現することにより、運転者同士の直接的な情報交換や、インターネット自動車による Ad-Hoc Network[103][104]の構築も可能となる。

しかし現在のインターネットは、固定された計算機環境を前提としているため、インターネット自動車のように移動しながら常時通信を行う場合には、様々な問題が生じる。インターネット自動車は基本的に、運用中は常時ネットワークに接続し、インターネット上の他の計算機と通信し続ける必要がある。しかし携帯電話や PHS 等といった既存の広域無線網では課金等の問題がある為、これを常時使用することは好ましくない。また現在普及しつつある無線 LAN は高帯域で安定した通信デバイスであるが、その利用範囲は非常に狭いものとなっている。このため現在のインターネット自動車通信システムでは、これらの通信デバイスを状況に応じて使い分けることが必要となる。しかしこのような利用方法は、インターネット上での接続位置の移動を引き起こしてしまう為、後述するような数多くの問題が生じてしまう。

これらを踏まえた上で、今年度はインターネット自動車に必要な通信システムを構築する際に必須となる、以下の基盤技術に関する問題を解決する。

- 常時接続
- 移動透過性 (連続移動透過性 / 発呼可能性)

インターネットへの常時接続は、現在でも携帯電話や PHS 等の広域無線網を利用すれば可能である。しかしこれらは、利用に際して高額な課金が生じる

こと、また狭帯域・高遅延といった不安定な通信デバイスである、などの問題がある。現在では無線 LAN のように高帯域・低遅延な通信デバイスも登場している。しかしこれらは狭域通信網であり、ごく狭い範囲のみで利用可能である。したがってインターネット自動車の通信システムは、これら複数の通信デバイスを状況に応じて使い分けながら、インターネットへの常時接続をおこなうことが必要となる。

移動透過性の問題はさらに、連続移動透過性と発呼可能性の2つに分けることができる。連続移動透過性は、計算機の移動により引き起こされる IP アドレスの変化を、その計算機上で動作しているアプリケーションから隠蔽することである。連続移動透過性が保証されないと、計算機上のアプリケーションは移動のたびに通信を切断し、新たにコネクションを張り直さなければならない。発呼可能性とは、インターネット上の他の通信相手が、インターネット自動車に対してそのネットワーク上の位置に関わらず、常に発呼できることである。インターネットでは、計算機の識別子として IP アドレスを用いている。インターネット自動車の IP アドレスはネットワーク上を移動することによって変化するが、これにより通信相手はインターネット自動車に対す識別子としての IP アドレスを一意に指定することができなくなる。インターネット自動車が移動しながら安定した通信を行うためには、このような移動透過性も充分保証しなければならない。

4.2 アプローチ

本章では、前述した目的実現のためのアプローチについて述べる。

4.2.1 常時接続に対するアプローチ

常時接続のアプローチとしては、広域サービスである携帯電話や PHS 等の単一通信デバイスのみを用いた接続方式と、複数の通信デバイスを使い分ける接続方式が挙げられる。しかし、携帯電話は高遅延で低帯域な通信デバイスである。インターネット自動車では、GNSS のアプリケーションやストリーム配信などを考慮すると、できるだけ高帯域で低遅延な通信デバイスを利用しなくてはならない。現在では、無線 LAN などの高帯域で低遅延な通信デバイスが登場してきている。それぞれの通信デバイスは、

遅延、帯域や利用範囲等に特徴がある。例えば、携帯電話では高遅延、低帯域、広域であり、無線 LAN では低遅延、高帯域、狭域である。現在、1つのデバイスで低遅延で高速、広域でしかも複数のホストを支援する事は不可能であるため、これらを組み合わせて利用することが必要である。そこで、デバイスの特性によりこれらを切替える Vertical handoff[105]を行うことで、常時接続を実現すると共に通信効率を高める。Vertical Handoff とは、計算機が持つ複数の通信デバイスを、計算機上で動作しているネットワークアプリケーションに対して透過的な形で切替えることである。

また将来的には、インターネット自動車で利用可能な通信デバイスが、新たに開発されることも考えられる。これらも考慮して、インターネット自動車では、複数通信デバイスの動的な切替えによる、インターネットへの常時接続を実現する。当初から複数の通信デバイスを利用することを考慮することにより、新たな通信デバイスの導入も比較的容易に行うことが可能である。

一方、通信デバイスを複数用いる事により考えられる問題点としては、通信デバイスを切替えた時に、継続中の通信が切断されてしまうことが考えられる。これは通信デバイスを切替えた時点で IP アドレスが変化してしまうためである。しかしこの問題は、次に述べる移動透過性の実現によって解決可能である。

4.2.2 移動透過性に対するアプローチ

移動透過性を保証することで、移動することによって生じるネットワーク接続の切断および再接続、あるいは Vertical Handoff による通信デバイスの切替え時に起きる IP アドレスの変化等を隠蔽することが可能である。インターネット自動車システムでは、移動計算機における移動透過性技術である Mobile-IP[106]を用いる。Mobile-IP を用いることにより、連続移動透過性と発呼可能性を同時に実現することが可能となる。Mobile-IP の詳細については 4.3.2 で述べる。

4.3 システム概要

本章では、インターネット自動車の通信システムで利用する、デバイス及び技術についての解説を行う。その後、想定されるインターネット自動車の

システム環境について述べる。

4.3.1 利用可能な通信デバイス

移動計算機環境において利用可能なデバイスは、現状ではかなり限定されている。インターネット自動車では、以下の2つの通信デバイスを採用した。

- 無線 LAN BreezeCom

無線 LAN のデバイスとして、BreezeCom のアクセスポイント及び移動局を利用した。本デバイスの特徴としては、2Mbps の通信速度、10BaseT 経由での接続によりデバイスドライバの開発が不要であること、またアクセスポイント同士は無線ブリッジを介して接続が可能であるため、広範囲な無線エリアを容易に構築できること、等が挙げられる。また SNMP[107]を利用することで、デバイス内の情報データベース (MIB[108]) にアクセスし、情報を取得することが可能である。

- 携帯電話 NTT Docomo DoPa

携帯電話は、NTT DoCoMo の DoPa (PDC-P) を用いた。本デバイスの主な特徴は、通信速度が 9600bps であること、また利用に際して課金が生じること、などが挙げられる。本実験では、接続プロバイダが通過プロトコルの制限をしており、Mobile-IP が利用不能になるため、PDC で利用した。インターネットへの接続先としては、大学内のダイヤルアップポートを選択した。

4.3.2 利用する技術

本節では、インターネット自動車の通信システムとして必要とされる技術についての説明を行う。

- Interface Switch (IFswitch)

IFswitch は、複数の通信デバイスを、移動計算機環境の変化に応じて動的に切替える技術である。移動計算機環境の変化としては、例えば通信デバイスのリンク状態や、インターネットへの接続性などが挙げられる。このような環境変化は、後述する MIBsocket を用いて取得する。また、携帯電話等の課金されるデバイスを考慮し、通信デバイスの利用優先度などのポリシーを定義することもできる。IFswitch

を用いることで、複数の通信デバイスを切替える Vertical handoff が実現できる。

- Mobile-IP

Mobile-IP は、移動ホスト MN(Mobile Node)の移動先を、MN の拠点となるネットワーク(ホームネットワーク)上のホスト HA(Home Agent)が管理することにより、位置透過性を実現する技術である。MN は通信を行う際は常に、送信元 IP アドレスとしてホームアドレス(Home Address)を用いる。ホームアドレスは、移動計算機である MN をインターネット上で一意に識別するための IP アドレスであり、MN がホームネットワーク上に接続している際の IP アドレスと同一である。

MN の通信相手 CN(Correspondent Node)は、常に MN のホームアドレスに対して通信を行う。HA は MN の移動先を把握し、MN がホームネットワークにいない時には、ホームアドレスを指定した MN 宛てのパケットを MN の移動先へ転送する。MN は移動後、移動先で取得した IP アドレスである CoA(Care of Address)を HA に対して登録(Registration Request / Reply)する。これにより HA は、MN 宛てのパケットを受け取った際、このパケットに送信元アドレスが HA、宛先アドレスが CoA となる IP ヘッダを新たに付加し(カプセル化)、CoA に転送することができる。

- MIBsocket

MIBsocket は、ネットワークエンティティの動的な状態変化に対応する、ネットワークエンティティの管理機構である。ネットワークエンティティの状態を、メッセージの交換を用いて取得あるいは設定することができる。また、移動などに伴うネットワークエンティティの状態変化を、ユーザ空間に対して通知することができる。MIBsocket が扱う全てのネットワークエンティティは、MIB のデータ構造に準拠している。

- Dynamic Host Configuration Protocol (DHCP) [109]

DHCP は、ネットワークに関する自動設定を行うための技術である。クライアントである

計算機が、接続したネットワーク上で動作している DHCP サーバに対して要求を行うことで、IP アドレスや経路情報、DNS サーバなどに関する情報を取得、設定することができる。

- Point-to-Point Protocol (PPP) [110]

PPP を用いることにより、モデムを介してインターネットへの接続が可能になる。PPP は、シリアルリンク上で IP データグラムをカプセル化、データリンク接続を確立するためリンク制御(LCP)や IP アドレス割り当てなどのネットワーク制御(NCP)を行う。

- Simple Network Management Protocol (SNMP)

SNMP は、TCP[111]/IP プロトコル群を用いて動作するネットワーク機器を管理するために開発・標準化された、ネットワーク管理プロトコルである。SNMP は、ネットワーク管理ステーション(NMS)と管理対象ノード(MN)で構成される。ネットワーク管理ステーションは、ネットワークを制御・監視する計算機であり、SNMP を用いて管理対象ノードとの通信を行う。管理対象ノードは、ネットワーク管理ステーションからの要求を受けとり、これを実行する計算機あるいはデバイスを指す。2つの計算機間では MIB (Management Information Base) と呼ばれる同一データベース構造を用いる。ネットワーク管理ステーションは、管理対象ノードが持つ変数を取得したり設定する事ができる。また管理対象ノードは、システム内で起きた状態変化をネットワーク管理ステーションに通知するための機構であるトラップを持つ。

4.3.3 想定されるネットワーク環境

図 4.1 は、本インターネット自動車で想定しているネットワーク環境である。

インターネット自動車上では、Mobile-IP や IF-switch を行う各種ソフトウェアが動作している。インターネット自動車は、携帯電話や無線デバイス等複数の通信デバイスを用いて、インターネットに接続する。接続時に IP アドレスを取得するための方法

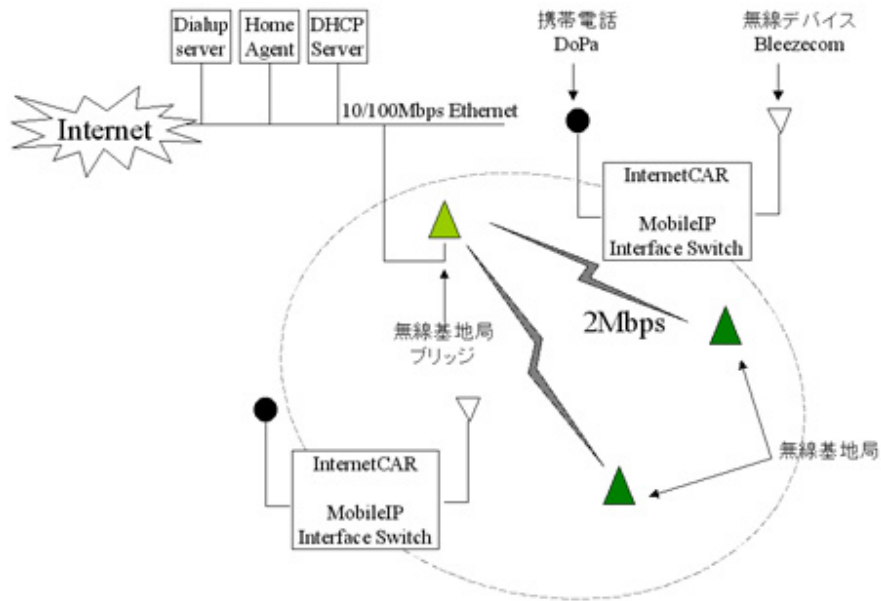


図 4.1 ネットワーク構成図

として、PPP と DHCP を用いる。PPP や DHCP のサーバはインターネット上に設置されている。また、Mobile-IP の HomeAgent も同様に、インターネット上に設置されている。インターネット自動車は、通信環境に応じて通信デバイス（通信網）を切替えて通信する。無線エリアは、BreezeCOM の基地局および無線ブリッジを用いて構築する。

4.4 システムの設計

本章では、前章で紹介した通信デバイスや技術を統合した、インターネット自動車通信システムの設計を述べる。インターネット自動車の通信では、前述した様々な技術が連係して動作することが必要である。しかし、現在の移動計算機環境に関するシステムおよびソフトウェアは、それぞれで単独で開発されているため、実際にこれらを統合することは難しい。

インターネットへの常時接続を保証するためには、通信デバイスを動的に切替える IFswitch デモンや、IP アドレスを取得するための DHCP や PPP、そして通信デバイスのリンクの状態を取得する SNMP や MIBsocket を統合して動作させなくてはならない。例えば通信デバイスを動的に切替える場合には、

IFswitch デモンは切替えのトリガーとして、リンクの状態や IP アドレスの取得情報を利用するからである。そこで、SNMP や PPP、DHCP により得られた情報を IFswitch デモンに通知する仕組みが必要である。これらを解決する方法としては、スクリプトを用いてバッチ処理的に解決する方法と、各ソフトウェアを統合する新たなシステムを導入する方法がある。本インターネット自動車では、図 4.2 で示したように、各ソフトウェアの統合機構として MIBsocket を利用する。

MIBsocket の役割は、各ソフトウェアが取得した情報を MIBsocket を介して、待機しているソフトウェアに通知するものである。例えば、PPP や DHCP が IP アドレスを取得すると、この情報は MIBsocket を介して IFswitch に通知される。また、SNMP で取得したリンクの状態や、MIBsocket から直接取得できるリンクの状態も同様に、MIBsocket を介して IFswitch に通知される。

MIBsocket を用いる事により、ソフトウェア同士で取得した情報を共有したり、他のソフトウェアの状態に応じた動作を行うことが可能となる。一方、MIBsocket に対応していない他のソフトウェアの起動や操作に関しては、スクリプトによるバッチ処理を用いている。

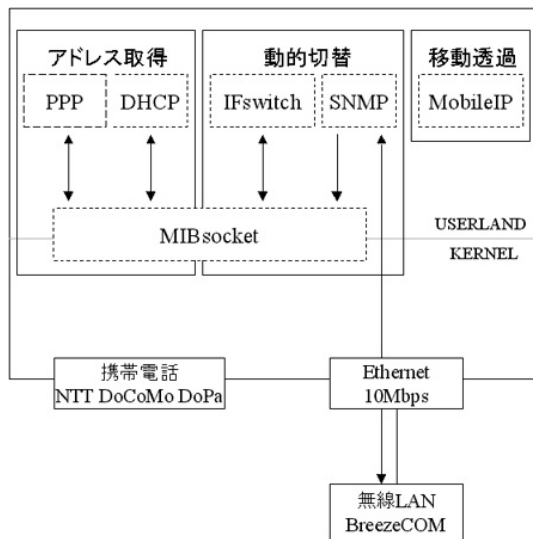


図 4.2 技術統合

また IFswitch は、移動透過性を保証する機構である Mobile-IP と連動しなくてはならない。IFswitch が通信デバイスを切替えた場合、Mobile-IP は HA に対して、切り替わったデバイスに対応する新たな CoA を登録しなくてはならないからである。IFswitch は経路表を書き換えることにより通信デバイスを切替えるが、この時点で Routing ソケットにアドレス変更を通知するメッセージが送信される。Mobile-IP は Routing ソケットを開いて待機しているため、IFswitch が通信デバイスを切替えた時点で、新たな CoA を HA に登録することが可能である。

4.5 システムの実装

本システムの実装は、インターネット自動車用に新たに開発された車載計算機である SIC2000 ハードウェアに対応した OS(NetBSD[112]) 上で行った。実装作業をソフトウェア毎に、表 4.1 にまとめた。

4.5.1 他 OS からのソフトウェア移植

SIC2000 の OS である NetBSD に、他の OS 環境で既に開発されていた各ソフトウェアの移植作業を行った。移植を行ったソフトウェアは以下の通りである。

- Mobile-IP
Mobile-IP は、東芝で開発された実装を用いた。対応プラットフォームは、BSD/OS と

FreeBSD である。本 Mobile-IP の特徴は、主要機能のほとんどがユーザ空間で実装されていることである。主な移植作業は、NetBSD カーネル内における Mobile-IP 用仮想デバイス等の移植、およびユーザ空間での Mobile-IP ソフトウェアの構築である。

- MIBsocket
MIBsocket は、raw socket として FreeBSD 上で実装されている。移植作業としては、カーネルの再構築と MIBsocket 用のライブラリの構築が挙げられる。
- IFswitch
IFswitch に関しては、MIBsocket と同様、FreeBSD で実装されたものを移植して用いた。
- PPP
NetBSD では、カーネル内部に PPP 機能が実装されている。しかし、インターネット自動車では PPP のみで通信するのではなく、複数の通信デバイスを切替える必要がある。ユーザ空間で実現されている IJ-PPP を用いた。
- DHCP
NetBSD の配布パッケージには、Internet Software Consortium (ISC) が開発した DHCP の実装が含まれている。しかし WIDE 版 DHCP に MIBsocket 対応機能を追加したものが既に存在していたため、今回はこれを NetBSD に移植して用いた。

4.5.2 各ソフトウェアの MIBsocket 対応

- IFswitch
IFswitch は FreeBSD におけるオリジナル実装で既に、MIBsocket から情報を取得し、動的に通信デバイスを切替えるように設計されている。
- PPP
NetBSD ではカーネル内での PPP が実装されている。しかし今回では、MIBsocket への対応や IFswitch との協調動作等を考慮し、ユーザ空間で実現されている IJ-PPP に MIBsocket 機能の追加を行ったものを使用した。

表 4.1 実装作業

ソフトウェア	他 OS からの移植 (対応 OS)	MIBsocket への対応
Mobile-IP	○ (BSD/OS, FreeBSD)	×
MIBsocket	○ (FreeBSD)	-
IFswitch	○ (FreeBSD)	○
PPP	○ (FreeBSD)	○
DHCP	○ (FreeBSD, BSD/OS, NEWS, Solaris)	○
SNMP	×	○

● DHCP

MIBsocket 対応機能を追加した DHCP クライアントは、前節で述べた通り WIDE 版の DHCP で対応した実装が既に存在していたため、これを用いる。

4.5.3 インターネット自動車内部構造

図 4.3 がインターネット自動車システムの通信部分の内部構造である。

物理層 (Physical Layer) として、携帯電話と無線 LAN を使用した。今回用いた無線 LAN (Breeze-Com) は 10BaseT イーサネット経由の接続であるため、独自のデバイスドライバは必要ない。もちろん本通信システムでは、新たな通信デバイスが登場した場合でも、デバイスドライバさえあれば適宜追加して利用することが可能である。

カーネル層 (kernel layer) における新たな機能は、主に Mobile-IP に関する処理と MIBsocket に関する処理の 2 つに分けることができる。

まず、Mobile-IP に関する処理について述べる。物理層から カーネル層に上がってきた全てのパケットは、IP 層に渡される。Mobile-IP のパケットは IPinIP の形式でカプセル化されているパケットであるため、raw IP として処理され ユーザ空間 (Userland) にいる Mobiled に渡される。Mobiled は、このパケットのカプセル化を解除した後で、仮想デバイスである tunnel デバイスを使ってもう一度 IP 層に戻す。これにより、全てのアプリケーションは Mobile-IP 独自の処理を意識する必要なく、通常の通信と同様の処理でパケット受信が行える。また、送信するパケットは全て、送信元 IP アドレスがホームアドレスに置き換えている。この際の ARP の処理などには、Mobile-IP 独自の改良が加えられ

ている。

次に MIBsocket の処理について述べる。MIBsocket では、メッセージパッシング機構を Raw ソケットを用いて実現している。また、MIBsocket が管理するカーネル内の MIB 情報は、カーネル内で保持している構造体とのマッピングを用いて管理されている。ネットワークエンティティの状態変化は、表 4.2 で示した方法により検知する。

ユーザ空間では DHCP や PPP が動作し、IP アドレスの取得や開放を行う。DHCP や PPP は MIBsocket に対応しているため、IP アドレスの取得や開放のメッセージを MIBsocket に書き込むことで、MIBsocket を開いて待機している他のアプリケーションに通知することができる。また、信頼性を確保するため MIBsocket には許可という機能があり、全てのアプリケーションは許可を取得しない限り MIBsocket を介してメッセージを送信することはできない。

SNMP は、10BaseT イーサネットの先にある無線デバイスと通信して、MIB 情報を取得しなければならない。この時、イーサネットの先の無線デバイスにも IP アドレスを割り当てる必要がある。イーサネット側には DHCP で取得したグローバル IP アドレスが付けられるため、無線デバイスに対してもグローバル IP アドレスを割り振る必要がある。しかし、リンクの状態を得るためだけに IP アドレスを消費するのは無駄である。この問題の解決方法として、イーサネット側にプライベート IP アドレスをエイリアスとして設定し、無線デバイス側にも同様にプライベートな IP アドレスを設定することにした。この方法によってさらに、DHCP でアドレスを取得できていない状況においても、SNMP を用いて無線デバイスの MIB 情報にアクセスすることも可能となった。

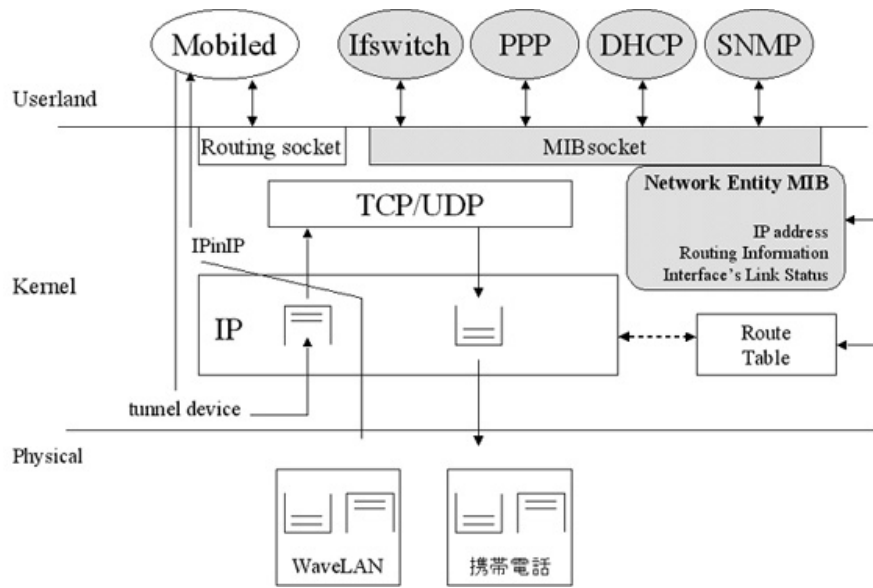


図 4.3 内部構造

表 4.2 ネットワークエンティティの状態変化の検知

トラップ	トラップの対象	検知方法
リンク	リンクの状態	通信デバイスのデバイスドライバ
IP アドレス	IP アドレスの設定や削除	Routing ソケット (rt_newaddrmsg())
経路	経路の追加や削除	Routing ソケット (route_output())

IFswitch、PPP、DHCP、SNMP のアプリケーションは、それぞれが取得した IP アドレスやリンクの状態等の情報を、MIBsocket を介して共有することができる。IFswitch は、アドレス取得機構である PPP や DHCP からのメッセージと、SNMP やカーネル内部から送信されるリンクの状態を、MIBsocket から取得し保持する。これらの情報に加え、通信デバイスの優先順位ポリシーなどの設定も利用して、通信デバイスを動的に切替えている。今回のインターネット自動車通信システムでは、無線のリンク状態として SNMP により取得できる無線のシグナル強度を用いた。

また IFswitch では、切替える時のオーバーヘッドを減らすため、携帯電話は常時接続している。通信デバイスを切替えるたびに新たに PPP や DHCP を実行し、IP アドレスを取得する場合には、デバイス切替え時に数秒程度の通信切断状態が生じてしまうからである。今回の場合では、携帯電話はパケット単位で課金されているため、このような方式をとっても特に問題はない。しかし、無線 LAN はその利

用可能範囲が狭い為、範囲外では IP アドレスを取得できない。そのため無線 LAN 側では、DHCP で動的にアドレスを取得する。

さらに、IFswitch と Mobiled との統合について述べる。Mobiled は今回、MIBsocket には対応していない。Mobiled は、Routing ソケットからのアドレス変更通知を取得し、HA に対して新たな CoA の登録を試みる。IFswitch が IP アドレスや経路表を書き換えて通信デバイスを切替えると、Routing ソケットにはこれらの情報が変更された旨の通知が行われる。このため Mobiled は MIBsocket への対応機能を追加しなくても、IFswitch が通信デバイスを切替えた時点で再登録を行うといった協調的な動作が可能である。

4.6 まとめ

本年度は、インターネット自動車通信システムの基盤技術として、ネットワークへの常時接続性、及び移動透過性に関する実証を行った。この結果、既

存の移動計算機環境に対応する技術を統合することに関する問題や、無線 LAN 等の通信デバイスの動作に対する予測不可能性の問題、等がわかった。

移動計算機環境に対応する技術は既に多くが存在し、利用できる実装も幾つかあるものの、それぞれは全く独自に開発されているため、それらを連動させて単体のシステムとして運用することは容易でない。今回のインターネット自動車通信システムでは、MIBsocket を中心とする情報交換・共有の枠組を導入するとともに、システム起動時に実行される数種類のスクリプトを用意することにより、これらの技術を連動させることを可能とした。また、無線 LAN などの通信デバイスの予測不可能性は、有線と違い電波が周りの環境に非常に左右されやすいのが、その主な原因である。周りの環境とは例えば、大気の状態や建物の位置などであり、これらの条件により無線では干渉やフェージングといった問題が起きる。そのため、実験の度にその結果が異なるなどの問題が生じた。

今後は、理想とされるインターネット自動車通信システムを実現するため、現在のシステムに対して新たな技術を導入する必要がある。現在までのインターネット自動車通信システムは、主にインターネットと車とのネットワーク接続および通信に関する基盤技術を研究対象としている。しかし今後は、インターネット自動車で利用される様々なアプリケーションの特性も考慮した、応用的な通信技術に関しても研究を行う必要がある。例えば、現在行われている GNSS 補正情報や GLI の地理的位置情報に加え、MP3 や動画像等ストリームデータの配信などといった、より帯域を必要とし、かつリアルタイム性が重視される通信も考慮しなくてはならない。このためには具体的には QOS の導入や、複数の通信デバイスを同時利用して通信の負荷分散を行う、などといった対応策が考えられる。

また、今後数多くの車がインターネットに接続するという状況を考慮すると、スケーラビリティ（規模性）の問題や、セキュリティに関する問題等も解決する必要がある。そのための方法としては様々な手法が考えられるが、将来性等を考慮すると、次世代インターネットプロトコルである IPv6 への対応が必須であると考えられる。現在のインターネット自動車システムは、現在広く普及し安定して用いられている IPv4 を元に構築されているが、アドレス

空間の枯渇問題や IPsec 等への対応を行うために、今後 IPv6 への対応も考慮した開発を続けてゆく必要がある。

第 5 章 GLI システムの改良と実証実験

地理的位置情報システムは、インターネット上の識別子と現実世界の地理的位置情報を対応付けることで、現実世界のエンティティの識別子と地理的位置情報が登録される。これを利用して、ユーザは、インターネット上で識別子と位置からエンティティを検索することができる。これまで地理的位置情報システムでは、地理的位置情報と識別子、時刻の情報が登録できていたが、エンティティ固有の様々な情報の登録はできなかった。また、膨大な数のエンティティの情報の登録・検索が行われるが、その検索の種類や、地理的位置をキーにした検索に関してはあまり考慮されていなかった。

本稿では、登録される情報と検索の種類、データ構造について考察し、検索の種類に応じたデータベースを導入することで、システムの改良を行った。また、インターネット自動車を利用して、GLI システムの実証実験を行い、改良された検索を行ういくつかのアプリケーションを動作させることで、用意された検索機能の有効性が確かめられた。また、検索の形式の整理、拡張可能なデータベース構造、アプリケーションに必要な地理的位置情報に関する課題を明らかにした。

5.1 はじめに

インターネットの実用的なアプリケーションの研究に関心が集まりつつある。いくつかのアプリケーションは、モバイル・コンピューティングやユービキタス・コンピューティング [113] といった研究分野で見られる。これらは、現実世界のエンティティとコンピュータ・ネットワーク上のユーザを疑似的に実現、あるいは対応付けることを目指している。そのようなアプリケーションではユーザの位置情報を利用することの重要性が注目されている。

我々が提案している地理的位置情報 (GLI) システム [114] では、現実世界の物理的なエンティティとインターネット上のオブジェクトを、地理的位置情

報と識別子によって対応付けることを目指している。この対応付けにより、計算機やユーザといった現実世界の物理的エンティティをインターネットを通じて認識することができる。エンティティはサーバに位置や状態の情報を送信し、クライアントは、識別子や位置を鍵とした検索要求をサーバに送信することにより、エンティティを検索することができる。

GLIシステムで取扱うエンティティ数は大規模であり、登録されるデータ量は膨大な数となる。エンティティが持つ多様なデータの登録と拡張性、検索の種類や性能に関係するデータベースの構造に関しては、あまり考慮されていなかった。本稿では地理的位置情報システムにおけるデータの種類の登録、アプリケーション側から要求される検索の種類について考察し、GLIシステムの改良を行う。また、同時期に実施された SFC Open Research Forum におけるインターネット自動車の実験環境において、改良した地理的位置情報システムの実証実験を行った。

5.2 GLIシステムの概要

5.2.1 GLIシステム概念

地理的位置情報 (GLI) システムは、現実世界の様々なエンティティの地理的位置とその状態情報を識別子に対応付けて登録管理し、また検索を可能とするシステムである。インターネット自動車では、自動車の持つ位置と多くのセンサーが持つ情報を識別子 (Full Qualified Domain Name: FQDN) とともに登録し、自動車の識別子や、地理的な位置、範囲をキーとした検索が可能となっている。

GLIシステムでは、エンティティ上でエージェントというソフトウェアが動作しており、GPSなどの位置取得デバイスで取得した緯度・経度・高度・速度、および状態情報を識別子とともにサーバに対して送信する。サーバはそれらの情報をデータベースに登録する。クライアントはサーバに対し、エンティティの識別子または位置情報をキーとした検索要求を送信する。サーバでは検索要求により、データベースを検索しクライアントに回答する。また、クライアントは特定のエンティティのエージェントに対して直接情報を問い合わせることもできる。文献 [114] で提案された GLI システムでは、上記のようなエージェント・サーバ・クライアントという構成である。

現在の GLI システムの基本構成を図 5.1 に示す。

サーバの分散管理機能を考慮した文献 [115][116][117] では、サーバを 2 つの機能に分割した。サーバにはエリアサーバとホームサーバの 2 つがある。どのエージェントも特定のホームサーバに所属しており、ホームサーバに位置情報を送信する。エリアサーバは特定の範囲のエンティティの位置情報を管理しており、ホームサーバから該当するエリアサーバに更新情報が送信される。

5.2.2 GLIシステムの問題点

GLIシステムではグローバルな環境でのサーバ分散管理に関していくつかの提案 [114] を行っており、文献 [116][117] でも提案されている。しかし、エリアを小さく分割するサーバ分散管理においては、サーバの数を増加させることにより、1サーバ当たりが管理するエンティティ数は相対的に減少するが、1つのエリアへのエンティティの登録やクライアントからの検索要求が集中する可能性がある。1つのサーバにエンティティの登録とクライアントからの検索要求が集中した場合でも、登録はもとより、検索も高速に行う必要がある。特に、データベースに集まったデータに対して行われる地理的な位置や範囲を用いた検索に関しては、これまであまり考慮されていなかった。そこで、地理的位置情報の登録・検索に適したデータベース形態を検討し、設計・実装を行う。特に、地理的位置をキーとしたさまざまな検索のパターンに関して考察し、それぞれに対してより高速に回答可能なシステムを目標とする。また、登録のパケットフォーマットをより多様なエンティティからのデータに対応できるように改良する。

5.3 GLIシステムの改良

5.3.1 地理的位置情報検索の高速化

GLIシステムでは地理的位置情報のような2次元、3次元のデータと、それに付帯したデータも加えた更に高次元のデータを大規模数蓄積し高速に検索する必要がある。このような高次元点データの取扱いは、画像などのマルチメディアデータに対する内容検索のための手法としての特徴ベクトルを類似検索において多く必要とされ、最近接検索を高速化する手法がいくつか提案されている。その中で SR-tree[118]

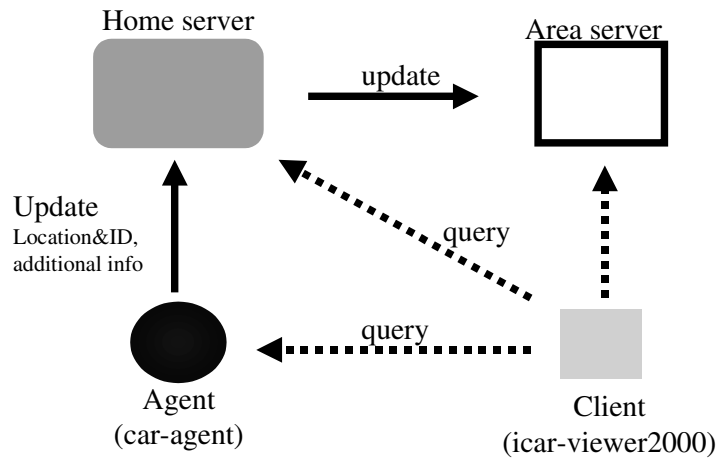


図 5.1 GLI システム基本構成

は、高次元点データに対する最近接検索を高速化するためのインデックス構造である。SR-Tree は R*-Tree や SS-Tree より更に高速であり、特に次元が高くなった場合の性能が高く、レコード数が膨大になっても性能の劣化が少なく、記憶装置との入出力も少ないという特徴がある。地理的位置情報だけでなく高次のデータを扱う可能性も考慮して、SR-Tree を導入する。

5.3.2 検索パターンと蓄積データの種類の

GLI システムには、インターネット上のエンティティから地理的位置情報や付帯する情報をサーバに登録送信する。1 つのエンティティの情報を全て蓄積すると膨大な量になる。基本的には最新の情報だけを蓄積する。しかし、GLI システムへ登録される情報の利用方法を判断するために、履歴に関する情報を求める検索要求を追加し、検索要求の種類に応じて複数の形式で情報を蓄積する。

検索パターンは、登録されるデータのうち、識別子、地理的位置情報、時刻のいずれかをキーとして使用する検索を基本とし、以下のような種類の検索を用意する。

- 識別子からの検索
- 識別子指定と履歴検索

- 最近検索: 1 点の位置をキーに指定
- 範囲検索: 2 点の位置から範囲を指定
- 時間範囲検索: 2 つの時刻を指定

これらの検索パターンとキーに使用されるデータの種類から、データベースの種類は以下のようにする。

- 識別子をキーとする検索のデータベース: GDBM
- 地理的位置情報をキーとする検索のデータベース: SR-Tree
- 時間をキーとする検索のデータベース: SR-Tree
- 識別子を指定した履歴: 追記型バイナリデータファイル

識別子には FQDN ホスト名を使用している。このデータの登録と検索に関しては、汎用的でシンプルな GNU Database Management (GDBM) のデータベースライブラリ (gdbm-1.8.0) を使用した。Sleepy Cat 社の Berkely DB ライブラリも使用可能であるが、今回は使用していない。

SR-Tree は、文献 [118] の作者が提供するライブラリ (HnSRTree-1.3.1) を使用する。

5.3.3 実装

5.2.1 節で述べたように、GLI システムは、基本的には移動ホストから位置情報などのデータを送信するエージェントと、登録するデータを受け付け、問い合わせ要求をするクライアント、それを受け付け検索結果を応答するサーバ、の3者で構成される。

本実装では、サーバの分散管理は考慮しないため、ホームサーバ、エリアサーバを区別しない。それぞれの構成要素について以下のように設計・実装した。

データフォーマット:

本システムで取扱うデータには、大きく位置情報、状態情報に分けられる。位置情報は測地系と緯度・経度・高度・速度で構成される。状態情報は、データ形式は個別に定義する。それぞれ更に細かいデータセットがあり、id と subid で識別する。

- 位置データ (id=0)
 - － 固定 (sub id=0)
 - － 目的地 (sub id=1)
 - － 単独測位 GPS 位置 (sub id=2)
 - － Differential 補正 (sub id=3)
 - － RTK 補正 (sub id=4)

プロトコルおよびパケットフォーマット:

本システムの各要素間で通信されるパケットの基本的な構成を図 5.2 に示す。

エージェントからサーバに送信されるパケットは、ヘッダと位置情報データ、状態情報からなる。ヘッダには、識別子、データの個数、タイムスタンプなどを含む。状態情報の個数はエージェントが動作するエンティティによって異なり可変である。

クライアントからサーバへの検索要求パケットは検索情報を含むヘッダと検索のキーからなる。その応答パケットはヘッダと検索の結果からなる。検索結果は、識別子、位置データ、状態情報で1つの単位とする。個数は可変である。

サーバ:

サーバでは、検索の種類に応じたデータベースを用意する。パケットを待ち、エージェントからであれば全てのデータベースに登録する。クライアント

からであれば検索の種類に該当するデータベースを検索し、応答する (図 5.3)。

エージェント (car-agent):

car-agent は、GPS などの位置取得デバイスから位置情報を取得しその他のデータと合わせてそのエンティティの識別子 (FQDN) を付けて、UDP でサーバへ送信する。送信する主なデータは、識別子 (FQDN)、位置データ (緯度・経度・高度・測地系・速度)、状態情報 (id, subid, データ)、時刻である。

クライアント:

サーバへの検索要求送信と応答受信のためのインタフェースを提供する。ユーザから入力された問い合わせ要求タイプと検索データをサーバに送信し、応答を受信する。本実装ではサンプルプログラムと基本ライブラリを作成した。これをベースにアプリケーションの設計・実装を行う。

5.3.4 アプリケーションの設計と実装

以上で実装された GLI システムにおいて、クライアントアプリケーションの設計と実装を行う。GLI システムにおけるサンプルアプリケーションは2種類であり、1つはユーザが指定した検索種類とパラメタにより、サーバから検索結果を受け取り、グラフィカルに表示するプログラム、もう1つは、特定のエンティティのエージェントに対して直接問い合わせることにより、リアルタイムに情報を取得し、グラフィカルにプロットするプログラムである。

検索要求型

検索要求型アプリケーションは、以下のような手順で実行される。

1. ユーザが検索の種類を選択する。
2. ユーザが検索の種類に応じて入力インタフェースを表示
3. 検索に必要なパラメタをキーボードまたはマウスを使用して入力
4. 検索要求をパケット化する
5. サーバに送信し、結果の応答を待つ
6. 応答を受信し、あれば画面にプロットして表示



図 5.2 パケットフォーマット概要

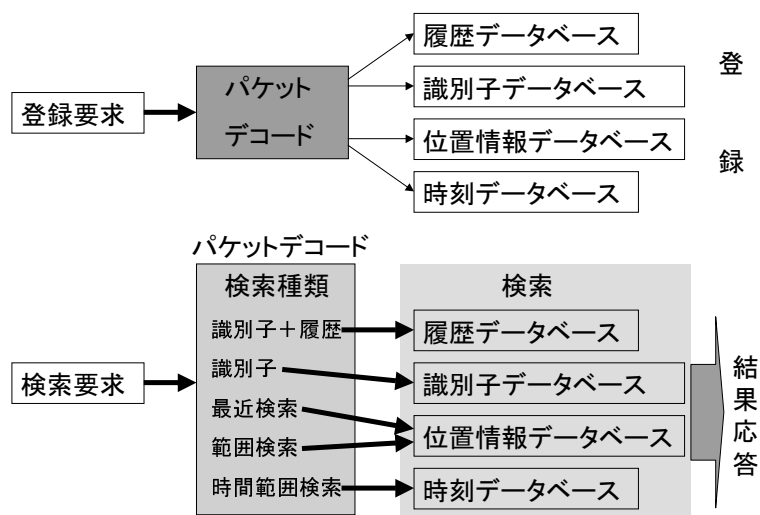


図 5.3 サーバ構造

リアルタイム型アプリケーション

リアルタイム型アプリケーションでは、サーバを経由せず、指定したエンティティで動作するエージェントと直接通信を行う。エージェントは UDP で接続されるとデータを送信し始め、停止の制御パケットを送信すると停止する。このようなアプリケーションでは以下のような手順で実行される。

1. ユーザが検索の種類を選択し、必要なパラメタを入力する
2. 指定したエージェントに送信し、結果の応答を

待つ

3. 応答を受信し、あれば画面にプロットして表示
4. 停止制御パケットを送信して終了

実装

実装は、FreeBSD3.3 上の XFree86(3.3.2) を用い、GUI のツールキットとして GTK+1.2 を使用し、C 言語で行った。

5.4 まとめと今後の課題

本稿では、地理的位置情報システムの問題点として、検索に関して検索パターンの検討とデータベース部分に関して改良を行った、また登録されるエンティティの状態情報の登録に関して柔軟なバケットフォーマットへ改良し、これらの設計実装を行った。また、インターネット自動車によるインターネット移動体通信基盤の実験環境の中で、改良された本システムの実証実験としてシステム、クライアントアプリケーションを動作させ、改良点を確認した。また、インターネットにおける移動体通信の要素技術に関して、実験の概要とその成果について述べ、いくつかのインターネット移動体通信技術を同時に運用する実験が今後の次世代移動体通信環境を構築する上で重要であることを示した。

現在進行中であるインターネット自動車、インターネット移動体通信環境の構築に関する研究、今後、より実用的な段階へ進むためには、基盤となるソフトウェアやアーキテクチャの構築に加えて、既存のアプリケーションを移動体通信環境に適応させるミドルウェア、自動車や移動体を考慮したアプリケーションやシステム、インタフェースなどの課題についても検討する必要があると考えられる。

第6章 地理的位置情報システムにおけるセキュリティ機能

6.1 はじめに

6.1.1 背景

近年、インターネット技術および小型化・軽量化の進んだ携帯端末が一般に普及している。これにより、固定ホストからのインターネットアクセスだけでなく、移動計算機を用いたモバイル・コンピューティングという新しい計算機の利用方法が広まりつつある。このように、移動する計算機やインターネットに接続可能な車などの非計算機の数が増大することによって、その位置が広域に分散し、ネットワーク・トポロジが変化するという状況になっている。しかし、インターネット上に固定または移動するコン

ピュータが遍在している環境においては、利用者と共に計算機も移動するため、現実空間での地理的位置情報をネットワーク上で扱うシステムの需要が高まってきていると言える。

このような要求に対して、携帯電話網の利用やモバイル・コンピューティング環境、無線 LAN 環境、またはナビゲーション・システム等により得られた位置情報は非常に有効である。現在開発が進められている位置情報サービスの中には、携帯電話網など通信基盤を限定して利用するものも存在するが、様々な通信基盤を限定することなく、それらから得た情報を公開できるインターネット上で、位置情報を管理・蓄積することが、適切であると考ええる。

6.1.2 現状とその問題点

元来インターネットは、ネットワーク上にある資源をその現実空間の位置を特に意識することなく利用することができる、という特徴を持っている。そのため、計算機の物理的な位置とネットワーク空間での位置とは関連づけられていない。しかし前述のように、移動計算機の数が増加し、インターネット上に固定または移動計算機が偏在するようになると、計算機の移動に伴うネットワーク空間での位置情報だけでなく、現実空間での地理的位置情報をもインターネット上で取り扱えるアプリケーションの需要が増す。

そこで、ネットワーク上の空間でのエンティティ(車・人・計算機・プロセスなど)の位置と、GPS(Global Positioning System)等で取得した現実空間のエンティティの位置の相互関係の定義を行い、ネットワーク上の空間と現実の空間の対応づけを実現するためのシステムアーキテクチャとして、1996年に GLI(Geographical Location Information)システム [114] が構築された。これによって、現実世界の位置情報を用いてネットワーク上に存在する計算機へのアクセスが可能となり、現在、InternetCARプロジェクトにおいて、車の位置情報を管理するために、この GLI システムを用いている。

しかし、現段階での GLI システムにはセキュリティ機能が未定義である。つまり、全ての利用者の

位置情報を知ることが可能であり、情報を得ることのできる人とそうでない人とを区別する機能は実現されていない。本来、移動計算機の位置情報はプライバシーに深く関わる情報を多く含んでおり、不用意な外部からの遠隔操作によっては、重大な事故が発生することも考えられる。このため、移動計算機の特定と位置情報の公開に伴ったプライバシー保護問題は非常に深刻であると言える。

そこで、本章では移動する計算機の地理的な位置情報とネットワーク空間との対応をプライバシー制御機能を付加して管理する GLI システムを提案する。提案するアーキテクチャモデルでは、GLI の構成要素 (Home Server、Area Server、Agent、Client) にアクセス制御機能または暗号化技術を加えて、公開情報と非公開情報の区別をつける。これによって、GLI による位置情報の不特定多数による無制限な利用を防ぐことが可能であると考えられる。また、GLI 情報を管理するためのネットワーク上の識別子として、従来の GLI システムで用いられていた IP アドレスや FQDN (Fully Qualified Domain Name) に代えて、そのままでは個人を特定できない pseudo ID を導入することを検討する。

6.2 位置情報サービスにおけるプライバシー管理のための必要条件

位置情報サービスは一般に研究開発されつつあるが、どのシステムにも広域分散環境での実用性を考える上では欠点を有している。そこで本節では、広域分散環境と個人情報 (プライバシー) の保護を念頭においた位置情報サービスにおける必要条件を以下のように抽出し、それぞれについて考察する。

● システム管理に用いる識別子に関する考察

- － 他情報による推測の不可能性
- － 識別子の有効期限の必要性
- － 第三者による識別子生成の不可能性

● 個人情報の保護に関する方法

- － データの加工方法
- － 加工のタイミング

● システムの構成要素の動作

- － 識別子とデータとの分割管理
- － 公開情報に対する、クライアントの要求に応じた検索可能性
- － 非公開情報に対する、適切なクライアント以外からの検索不可能性
- － ユーザ識別メカニズム
- － 通信切断時における振舞い

6.2.1 システム管理に用いる識別子

位置情報を現実空間で取得し、個人情報保護しながらインターネット上で公開、管理するためには、現実空間でのエンティティの識別子とは別の識別子も必要となる。この節では、インターネット上におけるシステム上の識別子が持つべき以下の性質について議論する。

他情報による推測の不可能性

システム上の管理識別子が、その生成に必要な情報以外の情報からも生成または推測できる場合、エンティティの成りすましが可能になる。したがって、システム管理に用いる識別子は、他情報からは生成、推測が不可能である必要がある。

識別子の有効期限の必要性

管理上の識別子に有効期限が設定されていない場合、一般には情報のキャッシュなどの工夫によって処理能力は向上する可能性があるが、何度も通信をすることによって、第三者からその識別子を持つエンティティが誰であるか (何であるか) を推測することが可能となる。したがって、位置情報の管理に用いる識別子は、セキュリティの観点から有効期限を設定し、一定期間で (または毎回) 適切に変更されるべきである。

第三者による識別子生成の不可能性

管理に使用する識別子は、エンティティ一意に生成されることが必要とされる。それには、識別子の生成にはその所有者特有の情報 (例えば、暗号やハッシュ

シュに使用される salt など) を加えることが有効であると言える。

6.2.2 個人情報の保護

ここでは、個人情報などの保護すべき情報の完全性や機密性をいかにして保つかということについて議論する。

データの加工方法

地理的位置情報の所有者 (提供者) 情報やその個人データについては、第三者に盗聴・改竄されないことが必要になる。これには、データ自体を加工する方法、つまり暗号技術を用いることが一般に知られている。つまり、個人情報の保護のためには、暗号技術を用いて、情報の完全性と機密性を保つ必要がある。

加工のタイミング

保護すべき情報を暗号化する、または暗号化処理を施されたデータを復号化する等、暗号技術を用いる場合は、その処理のタイミングによってシステムにかかる負荷やシステムを構成する要素の役割、性質等が変わる。つまり、処理負荷や構成要素の性質を考慮に入れ、対象とするシステムに適した処理のタイミングを決定することが重要となる。そこで、本システムに対する情報加工のタイミングを、サーバ上での加工、通信路上での加工、クライアント上での加工、に分類し、各々について以下のように考察した。

サーバ上での加工

位置情報サービスを提供するサーバ上で暗号化 / 復号化処理を行うのは、処理の負荷としては最適であると言える。しかし、サーバ上で情報を加工する場合、サーバを信頼するという前提が必要となり、第三者がサーバに侵入した場合、情報の完全性や機密性は保たれない。また、クライアントからサーバに生の情報を渡す (逆もまた同様) 場合に盗聴・改竄される可能性があることも、無視できない問題である。

通信路上での加工

クライアントからサーバへ、またはサーバからクライアントへ情報を伝達する時に、ネットワーク上に生の情報を流さない配慮として、通信路上、例えば組織毎に内外のネットワーク管理をしている Firewall やルータなどで暗号化 / 復号化する、という方法がある。この方法では、サーバ上で管理、蓄積する情報やクライアントが受けとる情報が、生の情報であるため、サーバやクライアントの負荷は最も軽い。しかし、サーバ上での加工の場合と同じく、サーバを信頼するという前提が必要であり、第三者にサーバを乗っ取られたり、正規のクライアントになりすまされたりした場合、何の保護にもなり得ない。

クライアント上での加工

モバイル・コンピューティング環境では、持ち運ぶクライアントは出来るだけ軽くした方がよい、という Thin Client の提案 [119] がなされている。つまり、移動するクライアント上で処理負荷の高い暗号技術を用いるのはモバイルコンピューティング環境では有益ではないと言える。しかし、クライアント上でデータを加工してサーバに送信することで、侵入者は通信路上やサーバを盗聴しても意味のある情報を得ることは出来ない。また、サーバを信頼するという前提は必要なく、クライアントは自分で情報を加工し、その情報取得可能者を自分で指定することも可能となる。

以上より、サーバを信頼するという条件を必要としないことから、クライアント上での加工が、本システムには最適であると考えられる。そこで、クライアント上 (本システムにおける Agent、Client) で暗号技術を用い、情報の加工や情報取得可能者の指定を処理することにした。

6.2.3 システムの構成要素の動作

前節までで、システムで用いる識別子と、情報の保護に関する考察を行った。ここでは、本システムでその識別子を用いて、どのように情報を蓄積、管理すれば情報が保護されるのか、という点において考察し、システムの構成要素の振舞いについて述べ

る。

識別子とデータとの分割管理

システム管理に用いる識別子と、その識別子に対応するデータは、分割して蓄積、管理されるべきである。つまり、その識別子に対応しているデータがそのまま同じ場所に蓄積されている場合、何らかの方法でその識別子が誰のもか判明した時に、対応するデータまでが知られてしまう。したがって、識別子は検索のキーとして使うだけで、対応するデータは分割して別の場所に格納することが理想である。

公開情報に対する、クライアントの要求に応じた検索可能性

エンティティの持つ位置情報や、エンティティの移動速度と位置、またはワイパーなどのセンサから分かる交通情報や天気情報など、一般に有益である位置情報とその付随情報に関しては、公開されるべきである。したがって、このような公開情報は、いつでも誰にでも取得可能な状態になっていることが望ましい。

非公開情報に対する、適切なクライアント以外からの検索不可能性

位置情報を提供した利用者(本システムでは Agent)の個人情報に関しては、たとえ侵入者にサーバにあるデータベースを盗まれたとしても、解読困難(意味のある情報を得られない)であることが望まれる。つまり、情報の所有者情報は堅牢に保護され、その情報を正しく取得できるのは、その情報所有者が指定したクライアントのみに限定されるべきである。

ユーザ識別メカニズム

一般的な位置情報だけでなく、その情報の所有者の詳細な位置情報や個人情報を要求したクライアントが、本当に情報取得の権利を持つかどうか識別するメカニズムが必要になる。したがって、アクセス制御表(ACL: Access Control List)や認証機能を用いた識別を付加することが望まれる。一般的なネットワークアプリケーションでは、公開鍵暗号系の電

子署名などを用いた認証のメカニズムが普及しつつある [120]。

通信切断時における振舞い

移動している間に Agent が自身の位置情報を取得、登録する場合がある。この時、一時的に通信媒体が変わったり(例えば、有線 LAN から無線 LAN へ、LAN から携帯電話へ、等)通信途中で回線が切断したりする可能性がある。モバイル・コンピューティング環境では、このような突然の通信切断もシステムが関知し、適切な処理を行うことが望まれる。

以上、モバイル・コンピューティング環境を想定した位置情報サービスを行うシステムの理想条件および必要条件を提示した。本研究では、情報の完全性および機密性を保証するために暗号技術を用いることを検討し、その処理はクライアント上で行うことが最適であると考えた。また、システム管理に用いる識別子や、データと識別子の管理方法についても考察し、それらに対する必要条件を検討した。これらを踏まえた上で、セキュリティに関して理論的に堅牢なシステムと実用に耐え得る処理速度や負荷を考慮に入れたアーキテクチャモデルを提案し、プロトタイプとして構築することを目指した。

6.3 提案するシステムのアーキテクチャ

位置情報管理システムのアーキテクチャモデルとして、サーバにおくデータの内、保護が必要なものを抽出し、そのデータ自体をあらかじめ暗号化して管理、蓄積するアーキテクチャモデルを提案する。つまり、通信路上で暗号化するのではなく、あらかじめ暗号化しておくことによって、生のデータの状態を減らし、安全性を増すことを期待している。情報を事前に個々に暗号化することによって、

- クライアント(エージェント)での処理が増えるという欠点があげられるが、
- 通信路上で覗き見されても意味のある情報は得られない
- 適切な鍵を持たない利用者は、意味のある情報を得られない

という利点が存在するため、今回はこのモデルを採用した。

提案するアーキテクチャモデルの着眼点を以下にあげ、詳細を述べる。

- 個人情報の暗号化とアクセス制御機能 (認証機能) の考察
- 情報管理のための識別子の導入

基本的には、地理的な位置 [緯度、経度、高度]、エンティティの速度 [方向、速度]、エンティティの属性情報 [ライトの点灯、外気温等] を公開情報とする。この公開情報は、エンティティの地理的な位置と移動速度により交通情報や駐車場情報が作成可能であったり、外気温やワイパなどのセンサ、ライト等の属性情報から気象情報が作成されたりする。これらはインターネット上で扱う情報として、非常に有益であると言える。

6.3.1 個人情報の暗号化

実際の地理的位置情報は公開可能情報とし、プライバシー保護としてその情報の所有者情報に関して暗号化処理を施す。具体的には、その情報毎にアクセス制御情報を付加することで、情報取得権利を持つ利用者のみがその情報を正しく復号化できることを目指す。暗号化技術を用いることによって個人情報は適切な利用者にのみ取得可能とし、一般に有益な地理的位置情報は公開する、という機能の実現のため、本節では、本システムに用いる場合の既存の暗号技術に関する考察を行う。

公開鍵暗号を用いる方法

個人情報の暗号化は、アクセス許可を与える利用者 (共通のグループのメンバなど) の公開鍵で暗号化し、データをサーバに蓄積する。これにより、それぞれの情報には許可を与える利用者の数だけ暗号データのリストが付けられることになる。実際には情報そのものを公開鍵で暗号化するのではなく、ひとまず別な暗号鍵 (通常は共通鍵暗号系を用いる) で暗号化しておき、それをそれぞれの利用者の公開鍵

で暗号化するなどの工夫が必要になる。この方法では、暗号化と同時にアクセスする Client の認証が可能であり、情報を問い合わせる Client の持つ鍵が1つで済むが、共通鍵暗号に比べて処理時間が大きい。

共通鍵暗号を用いる方法

個人位置情報を共通鍵暗号で暗号化しておくことによって、それぞれは暗号化された状態でサーバに蓄積される。その情報に対してアクセスを許可する利用者にも、暗号化に用いた共通鍵を提供しておく。つまり情報を問い合わせる Client は、アクセス可能な情報の共通鍵の束を保管することになる。ただし、共通鍵暗号系を用いる条件として、鍵と情報そのものが別々に送信されることが必要となる。この方法では、公開鍵暗号に比べて処理速度が速く、鍵の変更も当事者間の鍵を変えることによって可能となる。しかし、情報を問い合わせる Client の管理すべき鍵の数が多くなる。

暗号処理による処理速度低下の問題から、データの暗号化には共通鍵を用いた方法が本システムには適切であると考えられる。したがって、地理的位置情報の暗号化には共通鍵暗号を利用し、図 6.1 のようなアーキテクチャモデルを提案する。

本論文に用いた表記法としては、以下のようなものが挙げられる。

- $E\{M\}$
メッセージ M を暗号化したもの (暗号文)
- ACL
アクセス制御表 (Access Control List)
- グループ
同じ鍵 (暗号化に用いる秘密鍵) を共有しているエンティティの一群
- pseudo ID
本プロトタイプシステムで管理上用いる識別子。これを見ただけではそのエンティティが誰であるか分らない。また、この識別子は AS 内で一意性を保っており、各エンティティの他の情報からは推測不可能である。
- real ID
エンティティの元々の識別子。インターネット

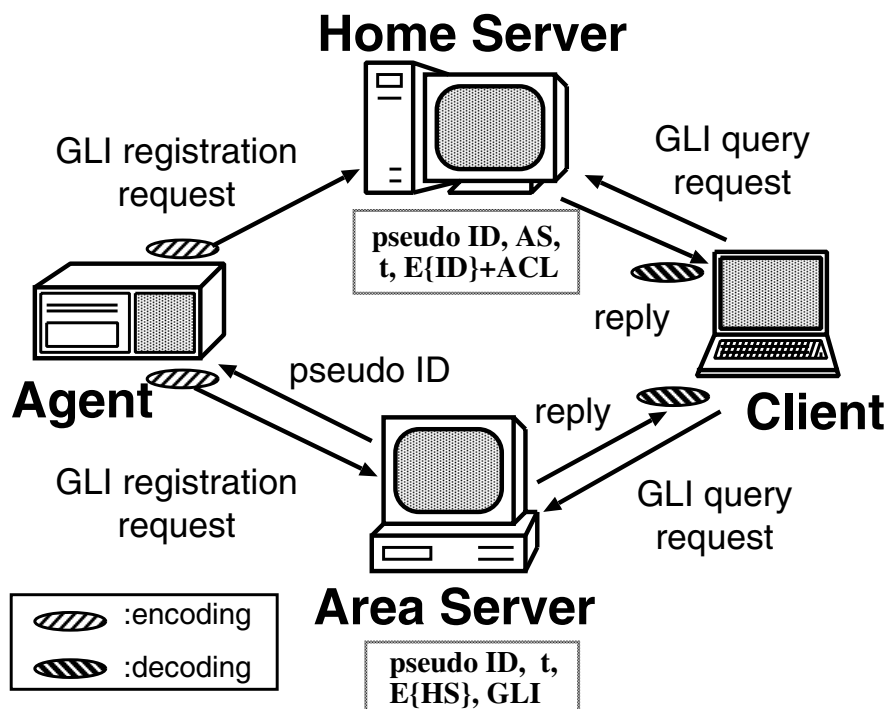


図 6.1 提案するアーキテクチャモデル

上の IP アドレスや FQDN やユーザ名、現実社会での名前などにあたる。

このモデルを用いる際には、アクセスする利用者の認証をどうすべきか、また共通鍵を用いた場合に最初の鍵配送をどのように行うか (鍵配送問題)、を検討する必要がある。

6.3.2 pseudo ID の導入

前節で述べたとおり、本システムの管理上の識別子に関して、セキュリティの観点よりいくつかの必要条件が存在する。本研究ではこれらの必要条件を考慮に入れ、地理的位置情報システムの管理に適切な識別子を導入する。

具体的には、情報管理のための ID と情報自体との直接のつながりをなくし、ID からは情報の所有者を類推できない仮 ID (pseudo ID) の導入が必要となる。このような pseudo ID の生成法として、以下で実用的な暗号学的ハッシュ関数を用いることを検討した。ここで、実用的な暗号学的ハッシュ関数とは、

以下の 2 つに大別される [121]。

- 独自にヒューリスティックな設計をしたもの
- DES などのブロック暗号を連鎖模式的に用いて実現したもの

本研究の pseudo ID の生成には、ヒューリスティックな設計のハッシュ関数を採用した。用いる一方向性ハッシュ関数には、鍵付ハッシュ関数 (HMAC: Keyed-Hashing for Message Authentication [122]) や SHA (Secure Hash Algorithm [123] [124]) が適当であると考え¹。また、各 Area Server 内で一意性を保つことが重要であるため、この pseudo ID の生成には、地理的位置情報を登録する Agent の情報だけでなく、Area Server の情報も加える必要がある。

6.4 まとめ

インターネット技術の周知と携帯端末の普及に伴って、モバイル・コンピューティングという計算機の利

¹ SHA と MD5、DES hashing との処理速度比較については、 $SHA < DES < MD5$ となっている [124]。

用方法が広まりつつある中、無線 LAN 環境、またはナビゲーション・システム等により、位置情報はインターネット上の様々なアプリケーションにとって有意性を増している。そのため、現在までに多くの企業や学術研究期間で位置情報サービスについての研究がなされてきているが、広域分散環境での実用性を備え、個人情報等のプライバシー保護を考慮したものはない。そこで、本研究ではセキュリティ(プライバシー保護)を考慮した地理的位置情報管理システムの提案とプロトタイプ的设计を行った。

システムアーキテクチャモデルの設計にあたり、情報の完全性および機密性に関しては暗号技術を用い、システム管理上では pseudo ID を導入することによって個人情報の無制限な流出を防ぐことを確認した。

6.4.1 今後の課題

前述の問題点を解決し、より堅牢で利用しやすいシステム構築のために以下の問題を検討することで、実用に耐え得るプライバシー保護機能を持った地理的位置情報管理システムを構築することを今後の課題とする。

- 共通鍵暗号のための鍵配送問題
共通鍵暗号のための鍵配送問題に関しては第4章3節で考察した。今後はこの考察を基に、本システムに最適の方法を適用して必要に応じて安全に共通鍵を配送する機能を付加する。
- 通信の秘匿性
登録する情報だけでなくインターネット上での通信自体も、システムの不正利用者に分からないようにする、という性質が、本研究には必要になってくる。これについては、IPsec やトンネリング、NAT (Network Address Translation) などの技術を利用することを検討する。
- Agent のなりすまし
システム管理上の識別子に、さらに工夫をする。
- 暗号化 / 復号化する鍵の選択
複数の group key を保持している場合、どの鍵を用いて暗号化 / 復号化すべきかを、ユー

ザの意志をシステムが感知して自動選択する機能を付加する。

今後は共通鍵暗号を用いることによって発生する鍵配送問題や、分散環境に特化した細かな振舞いについて、プロトタイプシステムの改良を行い、実用に耐え得る位置情報サービスを行うシステムの構築を目指す。また、これはセキュリティを考慮した地理的位置情報管理システムとして WIDE InternetCAR プロジェクトで運用実験をする予定である。

最後に、今回提案したアーキテクチャモデルは、インターネットにおけるプライバシーを考慮した情報流通を目的とするシステムの一例としても意味を持ち、他のネットワークアプリケーションにも応用可能であると考えられる。

第7章 総括

自動車の情報化は、現在、産業や各省庁など多くの方面で進められている。本プロジェクトではこれらの現状を踏まえて、我々なりのインターネット自動車の在り方と新規性を追求していくことが重要な鍵となる。

これまでの数年にわたる研究でインターネット自動車を実現する為の課題が浮き彫りになった。インターネット自動車システムでは社会的問題、技術的問題の双方を考慮する必要がある。社会的問題では ITS 等の既存の道路交通システムとの関係を明確にするとともに、将来の情報社会の中で自動車が果たす役目および果たせる可能性のある事項についてまとめる必要がある。一方、技術的な問題としては多くのセンサ情報を処理する為の仕組みや複数のメディアを使った通信、外部支援環境との協調などを挙げることが出来る。また、双方の接点に存在する問題として、情報を交換する為の抽象化を行ない、それを規格化していくという課題がある。

今後、本コンソーシアムでは更に高度な技術課題を解決する方向で研究を進める。近年ではインターネット技術も広く利用されるようになり、自動車を単にポイント - ポイントでインターネットに接続し、自動車から情報を取り込むような環境は比較的簡単

● 第 12 部 自動車を含むインターネット環境の構築

に構築できるようになった。今後はより高度で広い用途に利用できる情報環境作りが必要になると考えられる。これを受けて、自動車のより進んだ情報化を支援する技術の開発に取り組む予定である。