モバイルコンピューティングと
ワイヤレス通信 15−19
高度交通システム 3−19
（2000．12．1）

インターネット自動車システムにおける自動車位置情報管理機構

渡辺恭人† 佐藤雅明†
植原啓介†† 村井純†††

インターネット自動車システム[1]では，自動車をインターネット上のノードとして捉え，自動車の情報化を行う．自動車は，位置情報や，センサー情報を始め動的に変化する多数の情報を持っている．自動車の情報化とは，これまで車内において閉じていたこれらの情報を取得してインターネット上に蓄積し，またそれらの情報を処理して，自動車側に有用な情報を提供することである．

本稿では，このような自動車の情報化を行うシステムの一つとして，地理位置情報システム（GLIシステム）を，自動車の位置情報管理機構としてインターネット自動車システムに適用する場合の課題について検討する．また，自動車側から情報を提供するにあたり，プライバシ保護を考慮した地理位置情報システム（GLIsecシステム）の設計・実装とその実験について述べる．本システムをインターネット自動車に適用することにより，自動車からインターネット上への情報提供が安全に行うことが可能となった．

The Location Information Management System in the InternetCAR system

YASUHITO WATANABE,† MASAAKI SATO,† KEISUKE UEHARA†† and JUN MURAI†††

We propose the InternetCAR system. On the system, we treat a car as a node on the Internet, and provide platform to collect and manage each car information.

In this paper, we introduce the Geographical Location Information (GLI) System as a system to manage information of each car. We discuss problems as to such a system should be installed in the InternetCAR system. The design and implementation of GLI system with privacy consideration is also described. We tested our system on the InternetCAR system. Using our system, it is enable to produce information from each car in secure way.

1. はじめに

自動車の急激な普及・増加に伴って，その情報化がさまざまな分野で行われている．例えば，車内では運転を支援するカーナビゲーションシステムにより，現在地周辺の地図を確認でき，目的地までの経路を探索し提供する．道路では，道路交通情報センターなどにより渋滞情報，通過時間情報が，運転者に提供される．また，VICSなどのようにそれらの情報がカーナビゲーション上で確認できる．ただし，カーナビゲーションでは，車内で情報の空間が閉じており，外部から提供される情報サービスにしてもその情報は自動車1台1台から集められたものではない．

インターネット自動車システム[1]では，単に自動車をインターネットに接続するに留まらず，自動車をインターネット上のノードとして捉えた情報化を行う．センサー情報をはじめとする自動車の持つ多様な情報を取得してインターネット上に収集し，その情報を自由に取得して処理し，再び自動車へ提供する．1台の自動車の持つ多様な情報が多数の自動車から集められることによって，社会システムにとって有益な情報と成り得ると考えられる．

本稿では，インターネット自動車システムにおいて，自動車が有するそのような多様な情報のうち，その自動車の位置情報とその管理手法に着目し，地理位置情報システム（GLIシステム）を利用して，自動車の位

† 慶應義塾大学政策・メディア研究科
Graduate School of Media and Governance, Keio University
†† 慶應義塾大学SFC研究所
SFC Laboratory, Keio University
††† 慶應義塾大学環境情報学部
Faculty of Environmental Information, Keio University

置情報を管理する機構として適用する．その適用にあたり，プライバシ保護を考慮した地理位置情報システム（GLIsec システム）を実装し，インターネット自動車の実験環境において，GLIsec システムの実験を行った．

2. インターネット自動車の情報管理

2.1 自動車情報管理の効用

インターネット自動車システム[1]では，単に自動車をインターネットに接続するに留まらず，自動車をインターネット上のノードとして捉えた情報化を行う．センサー情報をはじめとする自動車の持つ多様な情報を取得してインターネット上に収集し，その情報を自由に取得して処理し，再び自動車へ提供する．1台の自動車の持つ多様な情報が多数の自動車から集められることによって，社会システムにとって有益な情報と成り得ると考えられる．

自動車内で取得できる情報は，センサーだけでも300種類を越えると言われるが，位置情報以外では，例えば，ワイパーやライトなどのスイッチ類，シフトのポジション，エンジン回転数，照度，外気温などが挙げられる．このような情報が広域に分散する多数の自動車から集まった場合に，どのようなメリットが得られるかは今後の課題であるが，広域に分散した動的変化情報の分布を観察・監視ができるだけでなく，渋滞などの交通情報や雨量分布などの気象情報，自動車の機能や故障の監視，個人の嗜好といった情報がその位置と結びつけられて様々な効果を持つ情報となる．そのような情報の収集が容易に行えるプラットフォームとなる．

2.2 システム構築の必要条件

多数のインターネット自動車から情報を収集し，インターネット上から自由に検索して取得するシステムの構築を検討する．このシステムは，大きく分けて，位置を登録する自動車（移動体）とその情報を蓄積して管理するデータベース（サーバ），蓄積された情報を検索するユーザ（検索者）の3者で構成される．このようなシステムを構築する場合，以下のような管理上の条件が必要となる．

大規模性

情報を提供，登録する移動体となる自動車と検索者の数は多数にのぼる．これら多数の登録による情報の蓄積，検索を処理できる必要がある．一つのサーバにおける処理能力を高めることも重要であるが，処理能力の限界を正確に見積もり必要に応じて負荷を分散する構造を持つべきである．

リアルタイム性

多数の移動体が常に移動している．移動体による情報登録，検索者による情報検索ともに情報のリアルタイム性を考慮して，処理を可能な限り高速に行う必要がある．特に検索に関しては，検索条件をシンプルにし，かつ検索結果の数量も絞れるようにすべきである．

プライバシ保護

自動車とともに移動する人間，それが特定ができることと，それがどこにいるかという位置情報は，プライバシに関する情報である．自動車の位置などの情報を提供しても自分が誰かが明らかになるようでは，個人からの情報提供は行われない．情報の提供のメリット以上に，情報の提供しやすさを促進するためには，プライバシの保護が不可欠である．自分が見知らぬ第三者によって特定されること以外のプライバシの保護としては，追跡の防止も重要である．

これらの必要条件を考慮して，我々が提案している地理位置情報システム（GLI システム）のインターネット自動車システムへの適用を検討する．

3. 地理位置情報システムの概要

地理的位置情報システム（GLI: Geographical Location Information System）[2][3]では，現実世界を移動する移動体を対象とし，その識別子と位置情報の登録・検索機能の実現を目指している．移動体は，その位置情報，付帯する状態や属性に関する情報を持つ．本システムにより，計算機やユーザの位置・状態をインターネットを通じて認識することができる．移動体はサーバに位置や状態の情報を登録し，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，移動体を検索することができる．また，インターネットに接続された移動体がその地理的位置に基づいて，近接のサービス・資源を検索するといった移動体通信環境の支援や，地理的に分散した多数の移動体が持つ情報の分布をリアルタイムに観測することができる．また，文献[3]ではサーバの階層化による分散管理を実現しており，地球規模での分散管理が可能となっている．

移動体の識別子としてはFQDN（Fully Qualified Domain Name）☆を用いる．地理位置情報としては緯度・経度・高度で表される1点を考える．付帯情報とは，移動体の移動方向や移動速度などである．GLI システムのサーバ（GLI サーバ）は，移動体が登録した地理位置情報や付帯情報を管理する．またGLI サー

☆ ドットで区切られたホスト名．例えば，mobile.sfc.wide.ad.jp

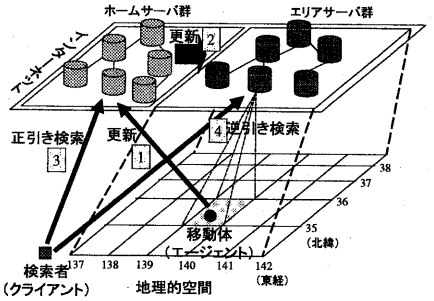

図1 GLIシステムの構成
Fig. 1 Architecture of the GLI System

バは2種類の検索機能を提供する．1つは移動体の識別子を鍵とし，その移動体の位置情報および付帯情報を返すものである（正引き検索）．もう1つは地理的な領域を指定し，その領域に存在する移動体の識別子，位置情報および付帯情報の集合を返すものである（逆引き検索）．

図1にGLIシステムの構成と動作例を示す．GLIサーバは，正引き機能を提供するホームサーバ群と，逆引き機能を提供するエリアサーバ群からなる．それぞれのサーバ群は階層構造をとっており，分散管理によって大規模性を実現している．分散管理の詳細については文献[3]を参照されたい．

図ではmobile.sfc.wide.ad.jpという識別子を持つ移動体が北緯35度18分18秒，東経139度30分40秒に存在している．移動体は識別子から決定されるホームサーバに識別子，地理位置情報および付帯情報を登録する（図1-（1））．登録を受けたホームサーバは，移動体の地理位置情報から決定されるエリアサーバに，移動体の識別子，地理位置情報および付帯情報を登録する（図1-（2））．

正引き検索を行う検索者は，移動体の識別子から決定されるホームサーバにmobile.sfc.wide.ad.jpという識別子を鍵として検索要求を送信する（図1-（3））．検索要求を受信したホームサーバは，検索結果として北緯35度18分18秒，東経139度30分40秒という地理位置情報および付帯情報を返す．

逆引き検索を行う場合は，例えば，北緯35度～36度，東経139度～140度という領域を鍵とし，この領域から決定されるエリアサーバに検索要求を送信する（図1-（4））．検索要求を受信したエリアサーバは，mobile.sfc.wide.ad.jpという識別子，北緯35度18分18秒，東経139度30分40秒という地理位置情報および付帯情報を返す．指定された領域に他の移動体も登録されている場合は，その情報も返す．

4. プライバシ保護を考慮した地理位置情報システムの概要

4.1 自動車情報化におけるGLIシステムの課題

前節で述べたGLIシステムにより，現実世界を移動する多数の移動体を地球規模で分散管理することができ大規模性を実現した．登録され検索される移動体の情報は，FQDN形式のホスト名と位置情報であるが，いずれも公開情報として扱っている．つまりインターネット上の誰でも，登録されたあらゆる自動車を特定し追跡できる．自動車の情報化として本システムによる管理を行う場合，バスやタクシーといった公共の交通機関に所属する自動車は自らの情報を周知させることができるという理由で，登録する可能性は高いと考えられる．しかし，現実に道路を走行する自動車の多くは私個人の所有で私個人の意志で私個人の用事・目的で移動している．そのような私個人が，1台1台の自動車の情報を広域に偏在する多数の自動車で集められた情報が社会的に有益な情報に成り得ると理解していても，インターネット上に「自分が今どこにいるか」というプライバシに関係する情報を提供することによる危険性が情報の登録を後込みさせる可能性は高い．また，信頼している人間同士でだけお互いの位置を共有したいという要求もある．

したがって，自動車の識別子とその位置情報を管理するGLIシステムを自動車情報の管理機構として導入する場合，プライバシ保護の考慮が重要である．本節では我々が提案しているプライバシ保護を考慮した地理位置情報システム（GLIsecシステム）[4]について述べ，自動車の情報化において本システムが有効かどうかを検討する．特に個々の自動車の情報が収集される際に，プライバシ情報のみを隠蔽し，それ以外の情報は公開情報とすることで，自動車の情報化の利点を損なわない点に注目する．

4.2 プライバシ保護の定義と目標

GLIシステムにおけるプライバシの保護とは，移動体が登録した情報を第三者から隠蔽することを意味する．単に識別子を隠蔽しただけでは，どの検索者も移動体を特定できなくなる．地理的位置情報システムの検索の一つである地理的位置に基づいた検索は，地理的位置情報が隠蔽されている場合は行えなくなるため，識別子のみを隠蔽することが求められる．識別子を隠蔽する場合には，不特定多数の第三者からは隠蔽し，信頼する特定少数に対しては隠蔽しないといったアクセスの制御が必要となる．これらは，既存の地理位置

情報システムの利点である集まった分布情報に対する検索機能を損なうことなく，可能となる．このような検索は，地理的に分散した多数の移動体が持つさまざまな情報の観測であり，例えば，雨量，気温といった状態情報の観測が考えられる．

GLI システムにおけるプライバシ保護は，第三者からの移動体特定を防ぐだけでなく，追跡を防ぐ．また，地理位置情報システムのおかれる環境と脅威として，なりすましによる偽情報の登録，ネットワーク上での盗聴・改竄，データベース盗難を防ぐことを目的とする．

4.3 解決手法

HID（Hashed ID）の導入

移動体と検索者間における信頼関係の有無によって，特定できるかどうかを制御するには，移動体と信頼関係にある検索者だけが理解できる秘密の識別子を移動体と共有し，この秘密の識別子を GLI サーバに登録すればよい．また，移動体と検索者が通信することなく，頻繁に変化する秘密の識別子を共有する方法として，両者の時刻同期を前提として，鍵付きハッシュ関数の鍵として時刻情報を使用する方法を提案している．ハッシュの結果得られる値を HID（Hashed Identifier）とし，これを秘密の識別子として利用する．時刻情報としては，基準時刻（ts）と HID 変更の間隔（ttl）を導入する．

もともとの識別子を ID とすると HID は次のような式で表される．

$HID = hash(ID \oplus (ts + ttl * n))$ （nは0以上の整数）

n の値は現在時刻から計算でき，$ts + ttl * n <$ 現在時刻 $< ts + ttl * (n+1)$ のような関係となる．この式から求められる HID の値は時刻によって変化する．移動体は，信頼関係にある検索者と HID 生成に必要な情報 ID, ts, ttl を安全な通信路を使用して事前に共有しているものとする．最初の登録（$T = ts$）時に，移動体は $HID0 = hash(ID + ts)$ と位置情報等をサーバに送信する．$ts + ttl <= T < ts + 2 * ttl$ では，$HID1 = hash(ID + ts + ttl)$ となる．このように，HID は時間とともに変化する．ある移動体と信頼関係にある検索者は，その移動体と時刻が同期しているので，同時刻に同じ HID を生成することができ，検索の鍵として使用する．

HID を用いた登録と検索

HID を導入した GLI システムにおける登録・検索に関して述べる．登録者となる移動体 A と，A と信頼関係にある検索者 B．この 2 者では，HID 生成に必要な情報を共有する．A と信頼関係にない検索者 C は，A の HID 生成に必要な情報は持たないとする．まず A は識別子 ID_a からハッシュ関数を利用して A の HID として，HIDa を得る．A は HIDa と A の位置情報を GLI サーバに送信する．サーバには HIDa と位置情報が登録される．次に検索者 B は，A の位置情報を知りたいので，A の識別子 ID_a からハッシュ関数により HIDa を生成し，GLI サーバに対して，HIDa を検索の鍵として検索要求を行う．サーバは登録されている HID から HIDa にマッチするものを検索し，その位置情報を検索者 B に送信する．検索者 C は A の HID として HIDa を生成できないため，検索要求することができない．

逆引き検索はある位置領域を指定し，その領域に属する移動体を検索する．登場する移動体と検索者は正引き検索と同様である．GLI サーバにはすでに A の HID と位置情報が登録されているとする．A と信頼関係にある検索者 B がある位置領域を指定してその領域に属する移動体を検索要求する．サーバでは該当する移動体の HID とその位置情報をリストとして B に送信する．B では，検索結果の HID を B で計算できる HID と比較し，HIDa を発見し，A がその領域に属していたことがわかる．C は同様の検索を行い，結果として同じリストを受信する．しかし，C は HIDa を計算できないので，受信した HID に対応する移動体の特定はできないが，公開情報である位置情報，その領域に属する移動体の数などの統計情報を得ることができる．

HID 生成のハッシュ関数

HID の生成には，鍵付きハッシュ関数（HMAC: Keyed Hashing for Message Authentication）[6] を使用する．また HMAC と組み合わせて使用するハッシュ関数としては，処理速度やセキュリティの強度から SHA-1（Secure Hash Algorithm）[5] が適当である．したがって，HID の生成には，HMAC-SHA1[6] を使用する．

登録サーバの導入による移動体認証

移動体を認証し，移動体の情報は登録せずにデータベースを持つ HID サーバに転送を行う登録サーバを導入する．データベースを持つ HID サーバは登録 HID によって固定されないため，認証が困難になる．登録サーバを導入することにより，移動体は常に同じ登録サーバと認証し，なりすましによる偽の登録を防止する．また，登録サーバにより移動体と移動体の情報を登録する HID サーバとの関連を無くすことができる．

IPsec の利用による盗聴・改竄の防止

移動体が登録サーバに HID と位置情報を送信する

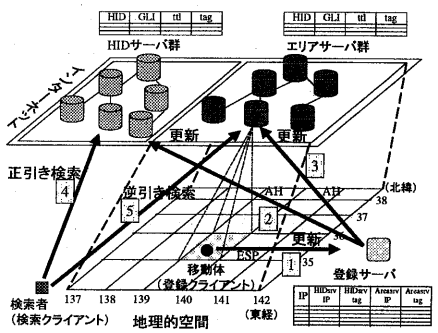

図2 GLIsecシステム構成

Fig. 2 Basic architecture of the GLI System with privacy consideration

場合，その間での通信が盗聴された場合，送信元である移動体のアドレスとHIDが対応付けられる．サーバ間の通信でやりとりされるのはHIDと位置情報とttlだけであり，これらの情報から移動体は特定されないため盗聴されてもよいが，改竄を防ぐ必要がある．このような場合，IPsec[7]の機能を利用することで解決できる．移動体を認証し登録サーバとの通信の機密性，完全性を確保するためにESPを使用する．サーバ間では，AHを利用して改竄を防止する．

4.4 設　　計

前章までに述べた解決手法から，**図2**のようなGLIsecシステム構成を導入する．

本システム上で管理する情報を挙げる．GLI（Geographical Location Information）は移動体の地理位置情報であり，緯度，経度，高度によって指定される1地点を示す．GLIは公開情報として扱う．ID（identifier）は移動体の識別子であり，FQDNやIPアドレスなど，形式は任意である．HID（hashed identifier）は，IDをもとにハッシュ関数（HMAC-SHA1）によって生成される数値で160bitの長さを持つ．移動体はこれをGLIとともにサーバに送信し登録する．検索者は信頼関係にある移動体のHIDを生成でき，正引き検索に使用する．

本提案システムは，登録サーバ群，HIDサーバ群，エリアサーバ群という3種のサーバ群と登録クライアント，検索クライアントという2種のクライアントから構成される．

登録クライアントは，移動体で動作するプログラムで，GPSなどの位置取得装置からGLIを取得し，識別子と鍵からHIDを生成する．GLIとHIDと有効期限であるttlを特定の登録サーバへと送信する（図2-(1)）．

登録サーバは，登録クライアントからのGLI登録を受け付けるプログラムである．登録サーバは，GLI登録を受け付ける登録クライアントを認証し，特定の登録クライアント以外からの登録は受け付けない．登録サーバは，受け付けた位置情報登録を蓄積せず，HIDの値，GLIの値に従って特定されるHIDサーバ，エリアサーバに対して，HID，GLI，ttlを送信する（図2-(2)(3)）．

登録サーバは，登録クライアントから登録を受け付ける際にそのIPアドレス，HIDの値によって特定されるHIDサーバのIPアドレス，GLIの値によって特定されるエリアサーバのIPアドレスを保持する．また，HIDサーバ，エリアサーバへの登録時に返されるデータベースエントリのtagも保持する．

HIDサーバは，登録サーバからHID，GLI，ttlを受信して蓄積する．また，検索クライアントからのHIDを鍵とした移動体の検索，正引き検索を受け持つ．既存のGLIシステムにおけるホームサーバのデータベース部の役割を持ち，正引き検索を受け持つサーバである．HIDサーバは，HIDの値によって登録するHIDサーバが決定され，移動体にとってHIDサーバは固定されない．HIDサーバのはHIDによる階層化により分散管理する．

エリアサーバは，サーバは特定の位置領域に存在する移動体のHID，GLI，ttlを登録サーバから受信して蓄積する．また，検索クライアントからの位置領域を鍵とした移動体の検索，逆引き検索を受け持つ．エリアサーバ群は受け持つ領域に従って木構造をなし，その管理構造は緯度・経度によって分割されたメッシュによって構成される木構造を利用した分散管理を行う[3]．

検索クライアントは，正引き・逆引きの検索要求をサーバに対して行いその結果を受信するプログラムである（図2-(4)(5)）．ある信頼関係にある移動体とHIDを生成するための情報を共有している検索者と，そうでない検索者が存在する．前者は移動体をHIDにより特定できるため特定可能検索クライアントとし，そうでない検索者，つまりある移動体のHIDを生成するための情報を持たない検索者が使用する検索クライアントを特定不能クライアントとする．

4.5 実　　装

前節の設計に基づいて行ったGLIsecシステムの実装について述べる．GLIsecシステムの実装は，既存のGLIシステムへの拡張として行う．既存のGLIシステムでは，移動体の識別子をFQDNとしてGLIを登録し，識別子も公開情報として扱う．これにHIDとGLIを登録・検索するGLIsecシステムをその拡張と

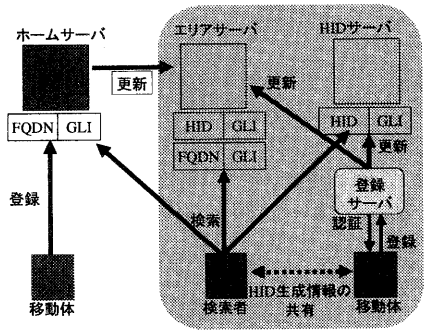

図3　実装のシステム構成
Fig. 3　Architecture of the GLI and GLIsec System implementation

して実装することにより，移動体の識別子を FQDN と HID の両方を使用して登録・検索を行えるという，GLI システムと GLIsec システムが一つのシステムとして動作する．

両システムはエリアサーバを共用するため，エリアサーバに HID と FQDN の両方を処理できるように，既存のエリアサーバを拡張して HID の登録を行うようにした．

図3 に実装したシステム構成を示す．

識別子を公開情報として扱う場合，移動体は自分を管理するホームサーバに FQDN と GLI を登録する．ホームサーバは登録された GLI から該当するエリアサーバに対して，FQDN と GLI を送信して登録する．GLIsec を使用する移動体は，HID を生成し，自分を管理する登録サーバから認証され，HID と GLI を登録サーバに送信する．登録サーバは HID の値から該当する HID サーバに HID と GLI を転送して登録する．また，登録サーバは GLI から該当するエリアサーバに対して，HID と GLI を送信して登録する．エリアサーバには，HID と GLI と，FQDN と GLI という 2 種類のデータが登録される．検索者は FQDN を指定した正引き検索を行う場合は検索したい移動体が管理されるホームサーバに FQDN を鍵として検索要求を行う．ある移動体と信頼関係にある検索者は HID 生成情報から HID を生成し，HID の値から HID サーバを決定し，HID を鍵として検索要求を行う．ある地理的範囲を指定しての逆引き検索を行う場合は，その範囲に該当するエリアサーバを指定して検索要求する．

HID 生成情報の記述

信頼関係にある移動体と検索者が共有する HID 生成情報は，あらかじめ共有されるが，本実装では `hid.conf` というファイルを持つことにより，共有する．このファイルはオフラインかまたは安全な通信路にて交換するものとする．`hid.conf` の形式を，図4 に示す．

```
#ID          ts          ttl   r1    r2    r3
riho-m@sfc   969189102   600   123   456   789
icar1@sfc    969168349   300   345   678   321
```

図4　`hid.conf` ファイルの形式
Fig. 4　format of `hid.conf` file

実装環境

実装は FreeBSD4.1 で行ったが，FreeBSD3.X や NetBSD1.4，NetBSD1.5 などでも動作を確認している．プログラミング言語は，C および C++を使用し，gcc および `g++ version 2.95` でコンパイルされている．HID 生成には HMAC-SHA1 という鍵付きハッシュ関数を使用するが，`openssl-0.9.5a` パッケージに含まれるライブラリ関数を使用した．

5. 実験環境

前節で実装したシステムをインターネット自動車に導入して実験を行った．ここでは実験環境の概要について述べる．

5.1 車載ハードウェア

車載ハードウェアには，SIC2000 というインターネット自動車用に設計されたハードウェアを使用した．RS232C インタフェース 4 口，PC Card のインタフェースを 4 スロット持つ．ハードディスクはなくフラッシュメモリを持つなど，自動車での使用を考慮した仕様となっている．このハードウェアのオペレーティングシステムとして NetBSD をポーティング [8] し，インターネット自動車用の各アプリケーションを実行する．

5.2 ネットワーク環境

実験ネットワーク環境を**図5** に示す．網掛けの部分は無線 LAN が利用可能な部分，それ以外では携帯電話での通信を行う．インターネット自動車は周回道路（SFC メビウスリング）を走行し，自動的に利用可能な通信インタフェース切替えを行いながら通信を継続する．

5.3 デモアプリケーション

GTK+を使用して X-Window 上のデモアプリケーション（`car-viewer`）を実装した．デモアプリケーションは，地図を表示し，GLI および GLIsec システムに実装されている検索を実行した結果発見されたインターネット自動車を地図上に表示する検索クライアントである．地図データは，慶應義塾大学湘南藤沢キャ

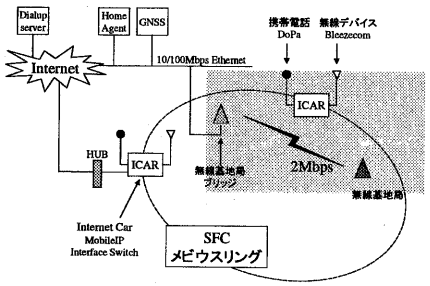

図5　実験ネットワーク環境
Fig. 5　network environment for the experiment

ンパス周辺～小田急線湘南台駅周辺をインターネット自動車で自走した座標データから作成した．

car-viewer で検索を行う場合，まず検索の種類を正引き，逆引きから選択する．正引きの場合，識別子を入力するが，入力された識別子が自分が持っている hid.conf に記述される ID であれば HID を生成し検索の鍵として使用する．そうでなければ，FQDN 形式のホスト名として検索の鍵に使用する．検索の鍵が HID なら HID サーバへ，FQDN ならホームサーバへ送信される．

逆引きの場合は，マウス等のポインティングデバイスにより 2 点を指定する．指定された 2 点によって得られる矩形を対象とした検索を行う．検索の結果，HID および FQDN と GLI が得られ，地図上に表示される．FQDN はそのまま表示される．HID の場合は，hid.conf から生成できる HID と比較し，一致したものは信頼関係にある移動体としてその id を表示する．一致しなかったものは信頼関係にないものとし，HID を表示する．

5.4 実験結果

実験では，FQDN を識別子として登録するインターネット上の移動ホスト（2 台）と，HID を識別子として登録するインターネット自動車（2 台）を使用して行った（**表 1**）．検索クライアントは 3 台で，1 台は HID による正引き検索，残り 2 台は逆引き検索を行うが，HID を登録するインターネット自動車との信頼関係の有無がある（**表 2**）．

以上のような構成で，登録クライアントにより登録された情報が検索クライアントによって取得できること，検索結果が信頼関係の有無によって識別子の表示が制御されていることを確認し，GLI システムと GLIsec システムの統合，プライバシ保護が機能していることを確認する．

表1　登録クライアントの種類
Table 1　list of registering clients for the experiment

番号	識別子	
1	FQDN	tera.csl.sony.co.jp
2	FQDN	sohgo.csl.sony.co.jp
3	HID	jun@wide
4	HID	riho-m@sfc

表2　検索クライアントの種類
Table 2　list of registering clients for the experiment

番号	信頼関係	
1（正）	有	jun@wide
2（逆）	有	jun@wide, riho-m@sfc
3（逆）	無	

5.5 HID 指定による正引き

検索クライアント 1 により登録クライアント 3 を HID を指定して正引き検索を行う．検索クライアント 1 は登録クライアント 3 と信頼関係にあるので，同じ HID を生成できる．car-viewer による検索結果を**図 6** に示す．

図6　HID 指定による正引き検索結果
Fig. 6　result of searching reliable entity by specifying HID

登録クライアント 3 と時刻を同期し，HID 生成情報を共有していなければ，同じ時間に同じ HID を生成できない．従って，本検索では，正しく検索が行われている．

5.6 逆引き検索

次に，登録クライアント 3 および 4 と信頼関係にある検索クライアント 2 と，信頼関係のない検索クライアント 3 で，同じような範囲指定による逆引き検索を行う．car-viewer による検索結果を図 7，図 8 に示す．

登録クライアント 3 および 4 と信頼関係にある検索クライアント 2 において逆引き検索を行うと，検索結果に HID を識別子としたものがあった場合には，hid.conf から生成できる HID を検索結果の HID を比較する．一致すれば信頼関係にあるものとして，ID を表示する．この場合，一致しているので ID が表示され，移動体を特定できている．

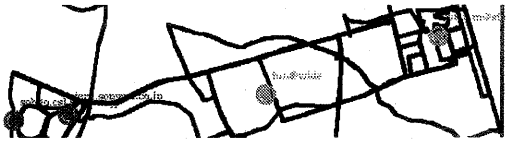

図7　逆引き検索結果（1）
Fig. 7　result of rectangle search （1）

登録クライアント3および4と信頼関係にない検索クライアント3において逆引き検索を行うと，検索クライアント2と同様に，検索結果にHIDを識別子としたものがあった場合には，　hid.conf から生成できるHIDを検索結果のHIDを比較する．一致すれば信頼関係にあるものとして，IDを表示する．この場合，一致していないのでHIDが表示され，特定することはできない．

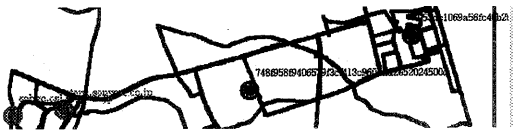

図8　逆引き検索結果（2）
Fig. 8　result of rectangle search （2）

逆引き検索結果（1）と逆引き検索結果（2）では同様に，FQDNを識別子とする2つの登録クライアントが表示されている．GLIシステムとGLIsecシステムのどちらから登録された登録クライアントも，検索クライアントによって検索できている．したがって，両システムの機能が同一システムで動作している．

6. まとめと今後の課題

本稿では，自動車の情報化にあたってのインターネット自動車でのアプローチ，つまり自動車をインターネット上の1ノードと捉え，自動車が持つ様々な情報を取得してインターネット上に収集して提供することの必要性を議論した．また，自動車の持つ情報と位置との関連から，その管理手法の一つとして，地理位置情報システムを取り上げ，必要条件を検討した．あらゆる自動車からの情報提供を実現するための必要条件の一つであるプライバシ保護を考慮した地理位置情報システム（GLIsecシステム）を提案し，既存のGLIシステムの拡張として実装した．このGLIsecシステムをインターネット自動車の位置管理機構として導入し，実験環境を利用してその動作実験を行い，動作を確認した．

今後は，自動車が持つ他種類の情報を位置情報と関連づけてどのように蓄積および管理するかを検討し，インターネット自動車の情報管理機構として検討していまた，多数の自動車からの登録・検索を想定した耐久試験および性能評価を行い，より実用的なシステムの実現と運用を目指す．GLIsecシステムとしての課題は，HID生成情報の共有手法，グループを対象としたプライバシ保護，HIDサーバの分散管理などの課題に取り組むとともに，交通流や雨量・温度分布に関するアプリケーションの開発も行う．

謝辞

本研究において貴重な御助言を頂いたWIDEプロジェクト，roverワーキンググループ，インターネット自動車プロジェクト，慶應義塾大学環境情報学部村井研究室，政策・メディア研究科モービル広域ネットワークプロジェクトの皆様に感謝致します．

参考文献

1) Keisuke Uehara, Yasuhito Watanabe, Hideki Sunahara, Osamu Nakamura, Jun Murai : InternetCAR - Internet Connected Automobiles, Proc. of INET'98. Internet Society, 1998.
2) Yasuhito Watanabe, Atsushi Shionozaki, Fumio Teraoka, Jun Murai, "The design and implementation of the geographical location information system.", Proc. of INET'96. Internet Society, June 1996.
3) 竹内 奏吾, 中村 嘉志, 多田 好克: インターネットにおける地理位置情報管理システムの設計と実装, 情報処理学会 マルチメディア，分散，協調とモーバイル（DICOMO'99）シンポジウム論文集, pp. 405-410, June, 1999
4) 渡辺 恭人, 竹内 奏吾, 寺岡 文男, 村井 純: プライバシ保護を考慮した地理位置情報システム, 情報処理学会 コンピュータセキュリティ研究会,（2000-CSEC-11-4）, pp. 19-24, Sep. 2000
5) National Institute of Standards and Technology （NIST）, FIPS PUB 180-1: Secure Hash Standard, April 1995.
6) Krawczyk, H., Bellare, M. and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.
7) Kent, S., and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998
8) 杉本信太, 植原啓介, 三屋光史朗, 村井純, "車載コンピュータへのBSDの応用", 日本ソフトウェア科学会, 第3回プログラミングおよび応用のシステムに関するワークショップ（SPA2000）, March, 2000