# 第 XXIII 部

# インターネットにおける地理位置情報の管理手法

# 第 23 部
# インターネットにおける地理位置情報の管理手法

## 第 1 章　GLI WG 活動報告

GLI WG は、インターネットにおける地理位置情報の管理手法や、応用、課題についての議論や検討を行うことを目的として、2004 年度 5 月に設立された WG である。本章では、本 WG の概要と 2004 年度の活動報告の概要について述べる。

### 1.1 WG 設立の背景と目的

近年、携帯電話や無線 LAN などの普及によりさまざまな移動体がインターネットに接続できるモバイル・コンピューティングの環境が構築されつつある。また、GPS や RFID、無線 LAN、携帯電話の無線基地局などを用いた移動体の位置測位基盤技術の普及も進んでいる。

インターネットは、有線ネットワークを想定して設計された通信技術であるため、今日のように移動体端末が接続される環境において注目される移動体の位置に関する概念や技術がない。たとえば、携帯電話や自動車といった移動端末がネットワークに接続される環境において任意のエリア内に存在する携帯電話や自動車への緊急メッセージ配信や、周辺情報配信などを実現するには、移動体の IP アドレスと位置情報の対応付け技術が必要となる。

これまで WIDE Project では、インターネットにおける移動体の地理位置情報の管理手法が検討され、GLI システムの構築がインターネット自動車 WG 内で行われてきた。GLI システムは、地理位置情報管理機構に必要とされる移動体のプライバシの保護を実現し、また従来の位置情報管理機構では実現されなかった、管理移動体数や管理領域面積に対する規模性を実現している。

本 WG は、GLI システムの普及を目標として GLI システムの定常運用を行い、定常運用を通して GLI システムの改良、実証実験、普及に向けた活動を行う。

### 1.2 GLI システムについて

#### 1.2.1 概要

GLI（Geographical Location Information）システムは、インターネットにおいて移動体の地理位置情報を管理する機構である。移動体とはインターネットに接続されて地理的な空間を移動する物理的対象を想定しているが、固定された物理的対象も速度がゼロの移動体として同様に取り扱うことを想定する。地理位置情報としては緯度・経度・高度を使用する。移動体はその識別子と対応付けてサーバに登録し、ま

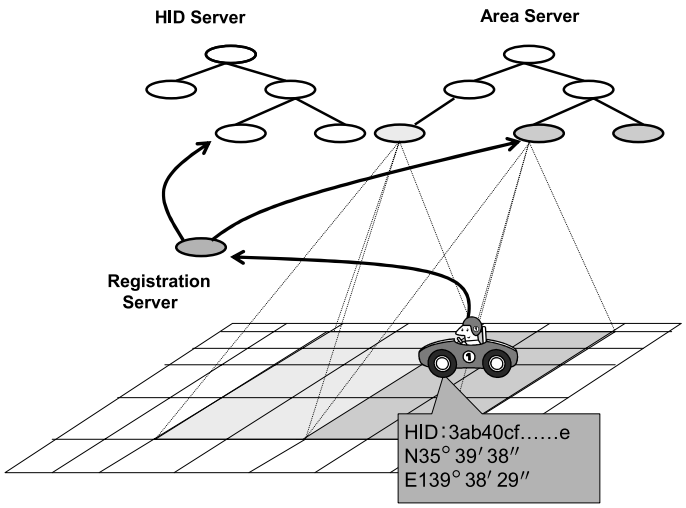


**図 1.1.**　GLI システム概要

た検索クライアントは、識別子と地理位置情報の双方を鍵とした検索を行うことができる。前者を正引き検索といい、後者を逆引き検索という。本システムの概要を図 1.1 に示す。本システムは、登録サーバ（registration server）、HID サーバ（HID server）、エリアサーバ（area server）という 3 種のサーバから構成される。移動体はあらかじめ定められた登録サーバに認証されてから自らの識別子（HID）と地理位置情報を送信する。登録サーバは、移動体から受信した情報を HID サーバ、エリアサーバに転送する。検索は検索クライアントから行い、正引き検索の場合は HID サーバに検索要求を問い合わせ、逆引き検索の場合はエリアサーバに問い合わせる。

#### 1.2.2 サーバの分散管理構造

GLI システムでは、広域に遍在する多数の移動体の地理位置情報を管理するために、管理移動体数と、管理領域に対してシステム全体での可能な処理量を増加させる。サーバを検索機能ごとの 2 つの分散管理形態に分け、またそれぞれのサーバは規模に応じて柔軟に増設して対応できる階層化された分散管理構造を持つ。多数の移動体、多数の検索クライアントによるトラフィックの集中を回避することができる。

#### 1.2.3 セキュリティ・プライバシ保護

GLI システムは、移動体の識別子として信頼関係にある利用者だけが理解できる HID（Hashed ID）を導入し、識別子の面からのプライバシ保護を実現している。したがって移動体の利用者は安心して情報を登録することができる。移動体は、移動体と信頼関係にある利用者（検索クライアント）とだけ HID を生成するための情報を共有し、HID と地理位置情報を登録サーバ経由で登録する。利用者は、正引き検索において移動体の HID を生成して検索の鍵として使用する。また、逆引き検索の場合は検索によって得られた HID を利用者で生成可能な HID と比較することで、信頼関係にある移動体かどうかを確かめることができる。移動体が登録する情報の正確性・信頼性は登録サーバと移動体の間で IPsec を利用した通信を行うことで、通信路の暗号化と通信相手の認証を行うことで確保している。

### 1.3 活動報告概要

#### 1.3.1 広域分散運用実験

GLI システムは大量の移動体の位置情報管理を目的としたシステムであり、大規模管理に対応するためには HID サーバおよびエリアサーバの分散化が必要となる。そこで、複数の拠点にエリアサーバを分散配置し、より実際の運用形態に近い形でシステムの運用を行う広域分散運用実験を実施する。広域分散運用実験で構築した環境は GLI システムの改良および GLI システムを利用したアプリケーションの研究開発に利用する。詳細は、第 2 章で述べる。

#### 1.3.2 Web ベースの GLI アプリケーションに関する検討

GLI システムはインターネット上で位置情報を管理するシステムである。GLI システムを利用するユーザは位置情報の検索を行うためにクライアントソフトウェアを必要とする。しかし、現在の GLI システムの実装は特定のオペレーティングシステムのみ対応しており、検索を行うユーザは GLI システムを利用するために専用のクライアントを動作させる必要がある。そこで、Web を利用した検索サービスを実現する。詳細は、第 3 章で述べる。

#### 1.3.3 GLI のプライバシ保護に関する検討

GLI システムの利便性を向上させる研究としては、地理位置情報公開に関する柔軟なプライバシ保護手法を実現する手法の検討がある。すでに述べたように現状の GLI システムでは移動体の識別子として HID を導入して、第三者からの特定および追跡を防止するという点でのプライバシ保護を行っているが、地理位置情報についてはオープンである。しかし、地理位置情報自体も単独、または時刻と結びついた連続データとなることで、個人を特定する可能性は増加すると考えられる。また精度が高ければ地上の地物の位置をより詳細に特定可能となる。したがって、地理位置情報についてもプライバシを保護してより安全に移動体の位置を登録してもらう必要がある。登録され検索によって得られる地理位置情報の公開する粒度や精度を利用形態による要求に応じて制御することによって、第三者から位置の特定を防ぐことができる。ただし、公開される地理位置情報の粒度が粗すぎる場合は利用可能性が低下するとい

**表 1.1.** 位置情報管理における利用形態別の開示状態・特定可能性

| | 識別子 | | | 地理位置情報 | 検索 | |
|---|---|---|---|---|---|---|
| | 開示状態 | 信頼関係者 | 第三者 | 開示状態 | 正 | 逆 |
| ①パブリック | 公開 | 特定可能 | 特定可能 | 公開 | ○ | ○ |
| ②プライベート | 公開 | 特定可能 | 特定可能 | 特定できないレベルで公開 | ○ | △ |
| | 暗号化して公開 | 特定可能 | 特定不可能 | 公開 | △ | ○ |
| ③ビジネス | 暗号化して公開 | 特定可能 | 特定不可能 | 特定できないレベルで公開 | △ | ○ |
| | 非公開 | | | 非公開 | 内部 | 内部 |

う問題もあるので、プライバシ保護と利用可能性の両面から粒度の限界を設定する必要がある。

この地理位置情報に関するプライバシ保護の導入にあたっては、GLI システムがサポートする 2 つのタイプの検索方法の双方に導入可能であることを目標とする。

次に、利用形態による移動体情報の開示状態について述べる。利用形態としては以下のように、公共的利用・プライベート利用・ビジネス利用があり、それぞれに情報公開の形態が異なる。

- 公共的利用（バスや電車など）: 識別子・地理位置情報ともに公開
- プライベート利用：信頼関係のある利用者間でのみ移動体の特定を許可、第三者からの特定を防止
- ビジネス利用（タクシー車両管理など）: 第三者から特定されない識別子・真の地理位置が特定されにくくなるように変換し、関係者以外には非公開

また、これらの利用形態での GLI システムでの検索可能性について検討したものを表 1.1 に示す。

①のパブリックの状態は、GLI システムにおいて識別子に FQDN を使用し、地理位置情報をオープンにしての利用である。②のプライベートには 2 通り存在し、識別子と地理位置情報のそれぞれいずれかが公開、または暗号化による開示を行っているものである。下段のものは、識別子に HID を導入した現状の GLI システムを意味している。上段は地理位置情報のみを暗号化するが公開レベルを設定して一部を暗号化するものである。③はビジネスでの利用を想定するが、GLI システムのような汎用システムを使用する場合と専用システムを使用するかの区別となる。ビジネス利用では、たとえばタクシーの運行管理などは非公開とし社内だけで利用できればいいが、上段のように汎用システムの場合は、識別子での第三者による特定を防止し、地理位置情報に関しても同様の防止を行うこととなる。この③のビジネスの利用の要求に GLI システムで対応するために、地理位置情報の粒度を考慮し、信頼関係者間でしか真の地理位置情報を公開しないが、第三者にも特定できないレベルでの地理位置情報を提供することが必要となる。本年度は、「柔軟なプライバシ保護を考慮した分散型位置情報システムの提案」として検討した。詳細は、第 4 章で述べる。

### 1.3.4 GLI の実運用性向上に関する検討

多数の移動体が頻繁に登録し、また多数の検索クライアントが頻繁に検索するような状況において、システムをこれらの処理に対応し安定して継続動作させるためには、これまでの検討により実現されたサーバの階層分散管理構造だけでは十分に規模性があるとはいえない部分がある。またサーバの追加や廃止または故障時の動的対応の堅牢性や耐故障性といった部分を実現する機構を検討し、実運用性を向上する必要がある。この課題については、実運用を想定した大規模位置情報管理機構の構築として、第 5 章で詳述する。

### 1.3.5 IETF での活動

GLI システムの普及を目指した活動の 1 つとして、IETF での提案活動を行った。IETF での提案活動では、GLI システムのアーキテクチャや仕様に関する Internet Draft の提出を行い、第 59 回会議と第 60 回会議の geopriv-wg において GLI システムとそのプライバシ保護のしくみについての説明を行った。geopriv-wg での検討の枠組みの中に GLI シ

ステムを入れるために、RFC3693 geopriv Requirements に記述される Location server においてのプライバシ保護実現に関して規模性問題を提起した。また using protocol の一例としての GLI システムを informational RFC として発行すべく提案したが実現しなかった。

### 1.4 今後の課題

今後の課題としては以下のようなものがある。

- GLI システムの改良と評価

  広域分散運用実験を継続して行いながら、システムの安定化に向けた改良を行い、仕様・プログラムソースの公開に向けた準備を行う。また、システムの評価をインターネット ITS アプリケーション開発環境である HAKONIWA を使用して行う。

- Web を利用した登録・検索

  GLI システムを利用可能な環境を広げるため、Web ベースでの登録や検索を可能とする環境が必要である。今年度は検索に関しての検討と開発を行ったが、携帯電話を使用した場合の登録や検索などのこれまでとは異なる環境においてもプライバシ保護を考慮した GLI システムを利用できるようにする。

- アプリケーション開発環境の検討

  GLI システムの普及に向けて、アプリケーションを開発できる環境を構築する。具体的には、基本的な検索機能が利用でき、またいくつかのアプリケーションのタイプに特化した API の検討を行い、C、Java、Perl、PHP などで利用可能なライブラリの提供を行う。

## 第 2 章　GLI システムの広域分散運用実験について

GLI WG では、位置情報管理機構である GLI システムの実運用を見据え、広域分散運用実験を開始した。本章では現在、定常運用をしている GLI システムの広域分散運用実験について述べる。

### 2.1 広域分散運用実験とは

GLI システムは多数の移動体の位置情報管理を目的としたシステムであり、大規模管理に対応するためには HID サーバおよびエリアサーバの分散化が必要となる。そこで、複数の拠点にエリアサーバを分散配置し、より実際の運用形態に近い形でシステムの運用を行う広域分散運用実験を実施する。広域分散運用実験で構築した環境は GLI システムの改良および GLI システムを利用したアプリケーションの研究開発に利用する。

### 2.2 目的

#### GLI システムの動作検証

GLI システムの実装および基本的な動作確認はすでに完了している。しかし、より実運用に近い環境で GLI システムの動作確認を行い不具合を解消することにより、システムをさらに安定化させる必要がある。また、マニュアルの整備など実運用時に必要となる事項の把握を行い、ノウハウの蓄積を図る。

#### システムの定性的・定量的評価

エリアサーバは地理的領域を管理領域とするため、サーバの分散化は各地域の移動体の数などを考慮する必要があるが、エリアサーバの分散形態に関する検証は未実施である。そこで本実験環境を利用して評価を行い、GLI システムのサーバ群の効率的なトポロジや必要な分散数といった実運用に必要となるパラメータおよびサービスクオリティの導出を行う。また、システムの問題点を把握し、今後の研究開発課題とする。

#### テストベッドの構築

GLI システムを利用したアプリケーションの開発や GLI システムの検証に利用可能な環境として定常運用環境を整備し、研究開発の効率化を図る。

### 2.3 実験環境

GLI システムの分散運用体制として、慶應義塾大学湘南藤沢キャンパス（慶應 SFC）、慶應義塾大学矢上キャンパス（慶應矢上）、電気通信大学（UEC）、奈良先端科学技術大学院大学（NAIST）の 4 拠点でエリアサーバの管理を行う体制を整備した。また、HID サーバは慶應 SFC において一元管理体制とし、登録サーバ、正引き検索サーバ、逆引き検索サーバは各拠点に配置した。

**表 2.1.** 各エリアサーバの管理領域

| レベル | 管理拠点 | 管理地域 | 緯度・経度 |
|---|---|---|---|
| root | 慶應 SFC | 下記以外の全領域 | — |
| 度 | NAIST | 西日本 | (北緯 20 度、東経 120 度)〜<br>(北緯 50 度、東経 137 度) |
| 度 | 慶應矢上 | 東日本 | (北緯 20 度、東経 137 度)〜<br>(北緯 50 度、東経 150 度) |
| 分 | UEC | 東京都調布市周辺 | (北緯 35 度 35 分、東経 139 度 20 分)〜<br>(北緯 35 度 60 分、東経 139 度 39 分) |
| 分 | 慶應矢上 | 東京都千代田区周辺 | (北緯 35 度 35 分、東経 139 度 39 分)〜<br>(北緯 35 度 60 分、東経 139 度 60 分) |
| 分 | 慶應 SFC | 神奈川県藤沢市周辺 | (北緯 35 度 0 分、東経 139 度 20 分)〜<br>(北緯 35 度 35 分、東経 139 度 35 分) |
| 分 | 慶應矢上 | 神奈川県横浜市周辺 | (北緯 35 度 0 分、東経 139 度 35 分)〜<br>(北緯 35 度 35 分、東経 139 度 60 分) |

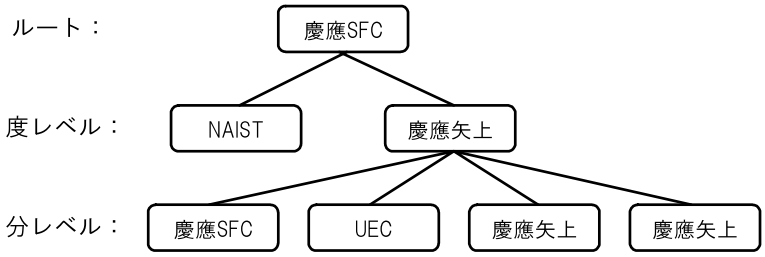


**図 2.1.** エリアサーバの分散形態

### 2.3.1 エリアサーバの分散化

GLI システムにおいてエリアサーバの分散化は地理的領域に基づいて行う。つまり、緯度・経度を基に各サーバの管理領域が決定する。具体的には緯度・経度の単位である度・分・秒の値を利用して 3 階層の分散化が可能である。

本実験では、ルートサーバを慶應 SFC に設置し、度レベルを管理するサーバを NAIST と慶應矢上の 2 拠点に、関東地域を分レベルで管理するサーバを慶應 SFC、慶應矢上、UEC の 3 拠点に 4 台設置した。各サーバの管理領域は、GLI システムの登録クライアントを搭載した車両の走行区域を基にし、車両が各サーバの管理領域を効率的に移動するよう考慮して決定した。エリアサーバの分散形態を図 2.1 に、各エリアサーバの管理領域を表 2.1 に示す。また、各サーバの管理領域を地図上にまとめたものを図 2.2 に示す。

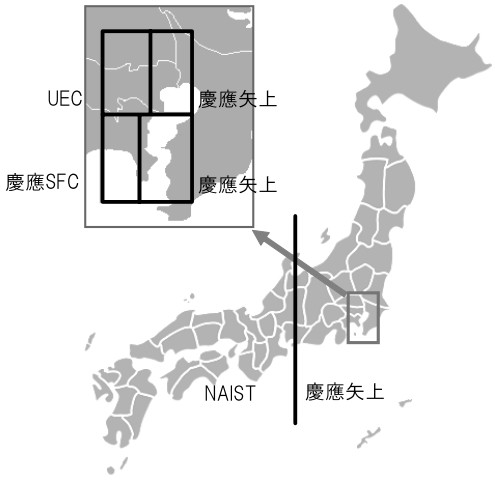


**図 2.2.** 広域分散運用実験の環境

### 2.3.2 位置情報の登録

広域分散運用実験では実データによる位置情報の登録も実施する。インターネット自動車 WG との連携により、インターネット自動車 WG が保有する実験車両に GLI システムの登録クライアントを搭載

し、GLI システムへの位置登録を行っている。また、インターネット ITS 協議会の協力により横浜市営バスに GLI システムの登録クライアントを搭載し、常時 GLI システムへ位置情報が登録される環境を実現している。

### 2.4 結果

GLI システムの動作を検証し、分散運用時および連続稼働時に発生する数個の不具合を修正した。また、システムの起動や設定を容易に行えるようマニュアルを整備した。その後 2004 年 9 月から現在まで継続的に GLI システムを運用している。インターネット自動車 WG が保有する実験車両による GLI システムの登録サーバへの位置情報登録要求の様子を図 2.3 に、実験車両の検索結果を図 2.4 に示す。

### 2.5 今後の課題

本年度 GLI WG では本章で述べた広域分散運用実験の環境を利用して、GLI システムの動作検証およびソースコードの修正、Web を利用したアプリケーションの研究開発などを実施した。今後も本実験環境を維持し、次に挙げる本年度実施できなかった事項および本実験で明らかになった課題についての検討を進める。

**定量的評価**　インターネット自動車 WG が開発した HAKONIWA を利用した実験を行い、GLI シス

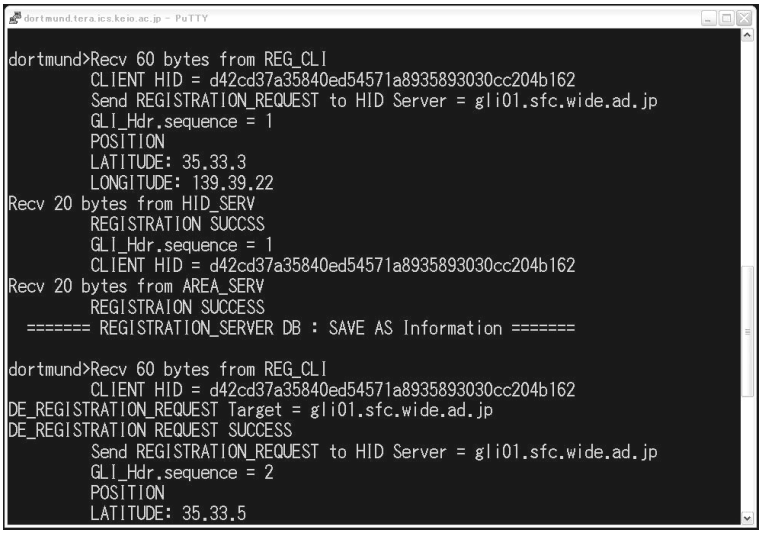


**図 2.3.**　位置情報登録要求の例

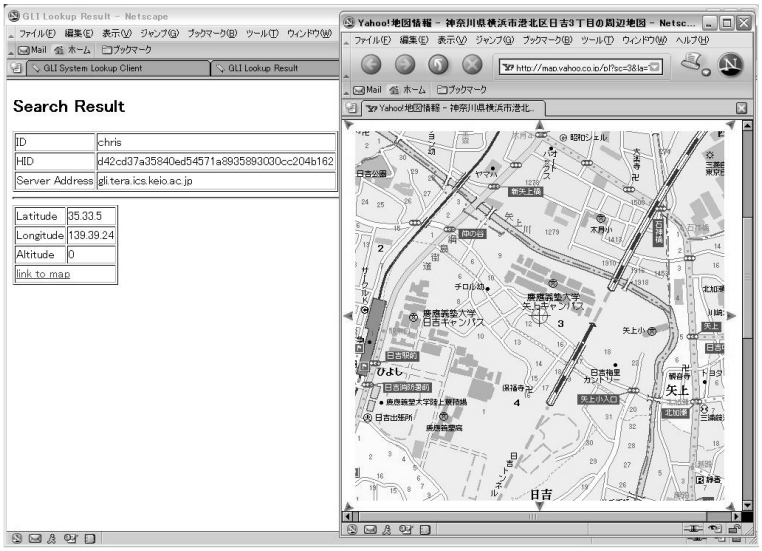


**図 2.4.**　正引き検索結果の例

テムサーバ群の分散数やトポロジといったパラメータの導出を行う。

**GLI システムサーバ群の管理の自動化** エリアサーバおよび HID サーバの管理領域の変更を動的に行う機能の検討を行う。

**ソースコードおよび仕様書の公開** 本実験により安定化したソースコードおよび仕様書を公開する。

## 第 3 章 GLI システムにおける Web を利用したアプリケーション開発

GLI WG では GLI システムの普及に向けた活動の一環として、GLI システムを利用したアプリケーションの開発を行っている。本章では Web を利用したアプリケーションとして、GLI システム Web クライアントおよびバス運行状況検索システムについて述べる。

### 3.1 GLI システム Web クライアント

#### 3.1.1 背景と目的

GLI システムはインターネット上で位置情報を管理するシステムである。GLI システムを利用するユーザは位置情報の検索を行うためにクライアントソフトウェアを必要とする。しかし、現在の GLI システムの実装は FreeBSD のみ対応しており、検索を行うユーザは GLI システムを利用するために FreeBSD 上でクライアントを動作させる必要がある。そのためユーザは特定のオペレーティングシステムによる環境を用意する必要があり、GLI システムの普及が困難、という問題がある。そこで、Web を利用した検索サービスを実現する。Web を用いる利点を以下に挙げる。

- Web によるサービスが普及している。
- ユーザは Web ブラウザさえ用意すればよく、ユーザの OS に依存しない。

Web を利用することにより、ユーザに対して手軽に GLI システムを利用できる環境を提供し、GLI システムの普及を目指す。

#### 3.1.2 Web クライアント概要

本項ではプロトタイプとして開発した Web クライアントの概要について述べる。

GLI システムは正引き検索と逆引き検索の 2 種類の検索をサポートする。正引き検索とは移動体の識別子を検索の鍵として、位置情報を取得する検索である。一方、逆引き検索とは地理位置の領域を検索の鍵として、領域の中に存在する移動体の識別子の集合を取得する検索である。Web クライアントは Web を利用して正引き検索および逆引き検索を実現する。図 3.1 に Web クライアントの構成を示す。なお図 3.1 の HID 変換鍵情報とは、移動体の真の識別子から GLI システムが使用する疑似的な識別子（HID）へ変換するために用いる鍵情報である。詳細は 3.1.4 項にて述べる。

図 3.1 の左図は従来の GLI システムの構成である。

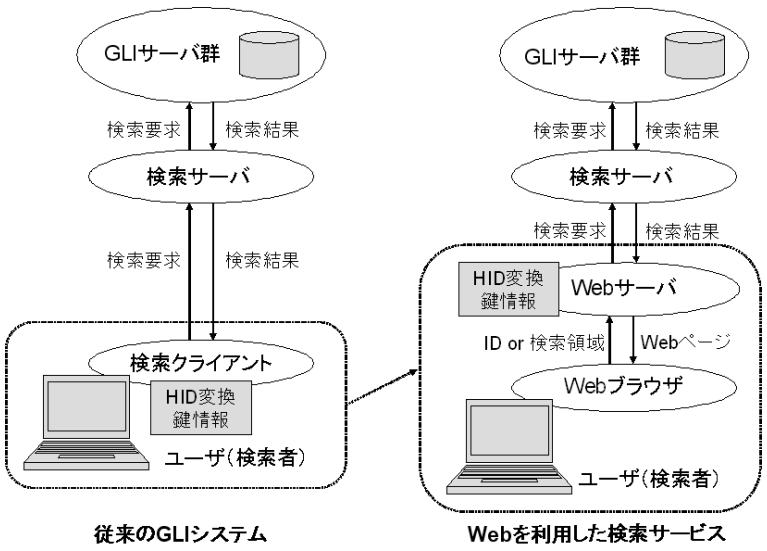


**図 3.1.** Web クライアント構成

検索者であるユーザはノート PC などの検索端末上で検索クライアントを実行し、検索要求を行う必要がある。

一方、図 3.1 の右図は開発した Web クライアントの構成である。ユーザは検索端末から Web ブラウザで Web サーバにアクセスし、CGI によって検索対象（ID または検索領域）を Web サーバに送信する。Web サーバは検索端末から受信した検索の鍵を元に検索要求パケットを生成し、検索要求を行う。Web サーバは検索応答パケットから検索結果の Web ページを生成し、Web ブラウザへの出力とする。HID 変換情報は Web サーバにて保持する。

実装は GLI システム検索クライアントをベースとし、Web サーバ上で GLI システムへの検索を実行する CGI を C 言語にて開発した。また、付加機能として逆引き検索結果を地図上にプロットする CGI を PHP にて開発した。

### 3.1.3 Web クライアント動作例

検索クライアントの動作例として、逆引き検索の検索結果を図 3.2 に示す。検索結果の上部が検索要求の内容（検索領域、検索サーバのアドレス）、下部が検索によって得られた移動体の位置情報である。

### 3.1.4 現状と今後の課題

開発した Web クライアントはプロトタイプであり、セキュリティやプライバシについて以下の問題点がある。

#### Web サーバ・Web ブラウザ間のセキュリティ

GLI システムでは IPsec を用いることで通信路上でのデータの盗聴・改竄を防止する。Web クライアントでの検索（図 3.1 右）は、従来の GLI システム（図 3.1 左）に比べて Web サーバを導入することにより、Web サーバ・Web ブラウザ間の通信路が新たに生まれる。しかし、ブラウザのみを使用するユーザが IPsec を用いることは困難であり、Web サーバ・Web ブラウザ間の通信路上にて悪意のある者による検索データの盗聴・改竄などが行われる可能性がある。そこで Web サーバ・Web ブラウザ間の通信に SSL を利用し、データの盗聴・改竄などを防止する。

#### HID 変換の鍵情報（hid.conf）の取り扱い

GLI システムでは、クライアントにて移動体の真の識別子（FQDN など）にハッシュ関数をかけることで疑似的な識別子（HID）を生成し、HID を移動体の識別子として扱う。そして、この HID 変換の鍵情報（hid.conf）を信頼者間で共有することにより

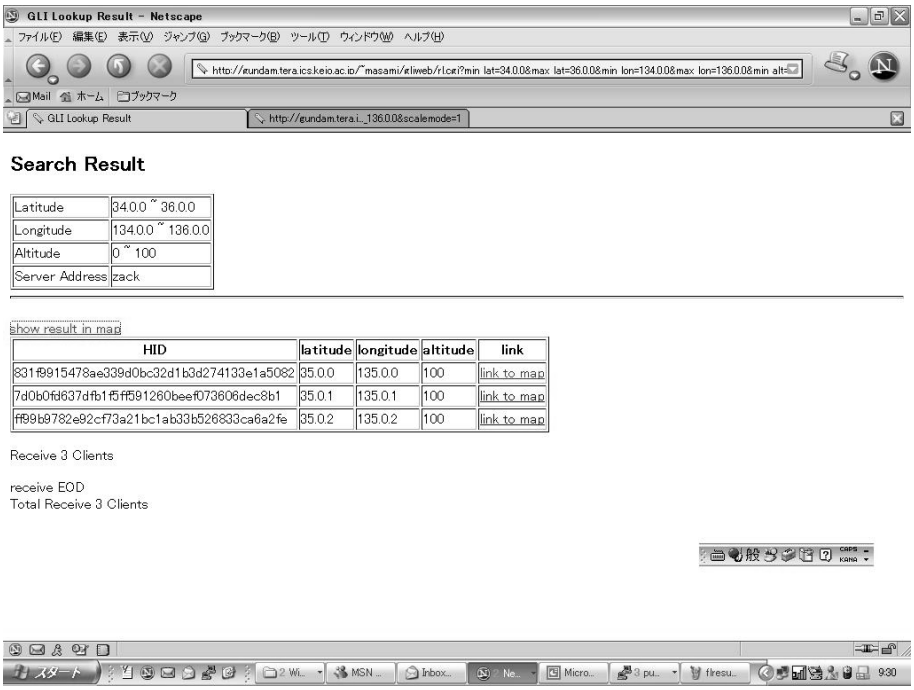


**図 3.2.**　逆引き検索の検索結果

プライバシ保護を実現する。GLI システムは鍵情報の漏洩を防ぐためにクライアントにてローカルに鍵情報を保持するセキュリティモデルである。しかし、開発したプロトタイプでは Web サーバ上に鍵情報を保持する実装としたため、GLI システムのセキュリティモデルに適合しない。そこで現在、鍵情報の扱いについて検討を行っている。以下に現在の GLI システムのセキュリティモデルに適合するモデルを 2 例、適合しないモデルを 2 例示す。

**GLI システムのセキュリティモデルに適合するモデル（図 3.3）**

- Web サーバが検索要求を行うモデル（手法 1、図 3.3 左）
  鍵情報はローカルに保持する。JAVA applet などを利用して Web ブラウザにて HID 変換処理を行い、Web サーバに対して検索対象となる HID や検索領域を送信する。Web サーバは受信した検索対象を元に GLI システムに対して検索要求を行う。
- Web ブラウザが検索要求を行うモデル（手法 2、図 3.3 右）
  鍵情報はローカルに保持する。Web サーバから HID 変換処理を行う JAVA applet などをダウンロードし、Web ブラウザにて HID 変換処理を行う。Web ブラウザが GLI システムに対して直接検索要求を行う。

**GLI システムのセキュリティモデルに適合しないモデル（図 3.4）**

- 鍵情報を毎回送信するモデル（手法 3、図 3.4 左）
  検索時に Web ブラウザは検索対象となる ID や検索領域とともに鍵情報を Web サーバへ送信する。Web サーバにて受信した鍵情報を元に HID 変換処理を行い、GLI システムに対して検索要求を行う。
- 鍵情報をあらかじめ Web サーバに保持するモデル（手法 4、図 3.4 右）
  今回開発したプロトタイプとほぼ同様のモデルである。ユーザは検索を行う前にあらかじめ Web サーバに鍵情報を登録する。Web ブラウザは検索時に検索対象となる ID や検索領域を Web サーバに送信する。Web サーバは受信した検索対象を元に HID 変換を行い、GLI システムに対して検索要求を行う。

以上の 4 例について以下の観点から比較した。表 3.1 に示す。

- GLI システムのセキュリティモデルに適合する。
- JAVA を必要とするなどのユーザ端末に対する負荷が小さい。
- 地図データなどのインターネット上のさまざまな情報を利用した位置情報の加工が容易である。
- SSL を用いることによるユーザ（検索者）の認証が可能である。

表 3.1 より、手法 1 および手法 2 は従来のセキュリティに適合するが、ユーザ端末への負担が大きく、

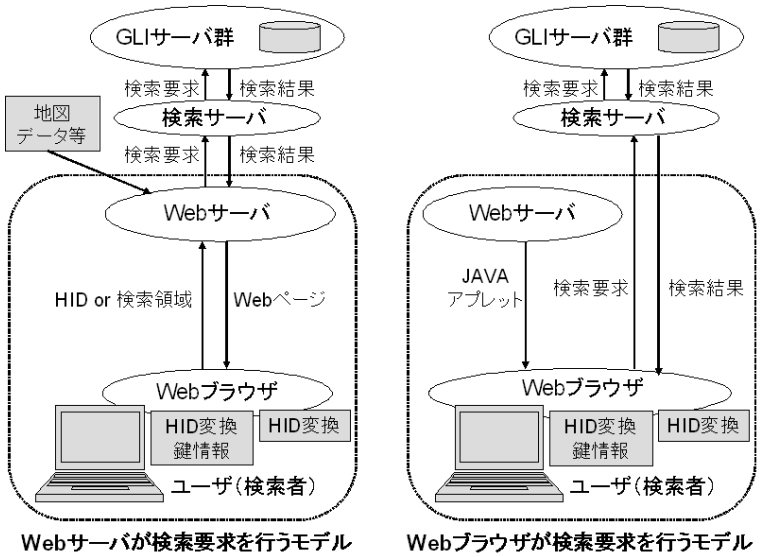


**図 3.3.** GLI システムのセキュリティモデルに適合するモデル

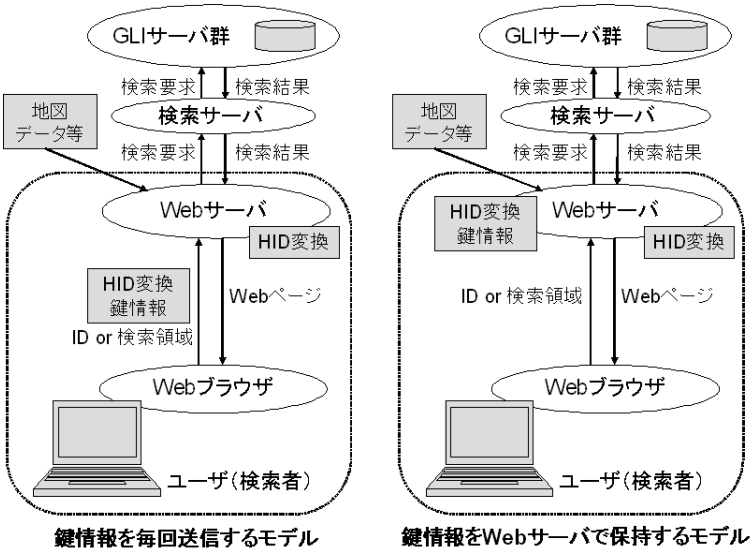


**図 3.4.**　GLI システムのセキュリティモデルに適合しないモデル

**表 3.1.**　モデルの比較

| 比較項目 | 手法 1 | 手法 2 | 手法 3 | 手法 4 |
|---|---|---|---|---|
| GLI システムのセキュリティモデルに適合 | ○ | ○ | × | × |
| ユーザ端末に対する負担が小さい | × | × | ○ | ○ |
| 位置情報の加工が容易 | △ | × | ○ | ○ |
| SSL によるユーザの認証が可能 | ○ | × | ○ | ○ |

位置情報の加工が困難であるという短所がある。一方、手法 3 および手法 4 は従来のセキュリティモデルに適合しないが、ユーザ端末への負担が小さく、位置情報の加工が容易であるという長所がある。したがって手法 3 および手法 4 により得られる長所を生かすため、従来の GLI システムのセキュリティモデルとは異なる Web クライアント独自のセキュリティモデルの考案が必要であると考えられる。

## 3.2 バス運行状況検索システム

2004 年 10 月、名古屋にて ITS 世界会議が開催された。GLI WG では GLI システムの普及活動としてバス運行状況検索システムを開発し、テクニカルツアーにてデモンストレーションを行った。

### 3.2.1 デモンストレーション概要

デモンストレーションの概要を以下に示す。

**期間**　2004 年 10 月 19 日、21 日

**会場**　インターネット ITS 協議会　名古屋事務所

**内容**　“横浜市営バス運行状況検索システム”

GLI WG ではインターネット ITS 協議会の協力により、横浜市営バスに GLI システムの登録クライアントを搭載し、バスの位置情報を管理する実験を行っている。この実験を利用し、横浜市営バスの運行状況をリアルタイムに表示する。また、バスの持つセンサ情報やカメラなどのデータを付帯情報として表示する。

### 3.2.2 システム概要

図 3.5 にシステム構成を示す。登録クライアントを搭載したバスは位置情報を GLI サーバに、センサ情報を Vehicle-Info サーバに登録する。デモンストレーションでは横浜市営バスでの実験が中断していたため、疑似的な登録クライアントを開発し、バスからの登録については過去の情報を利用して仮想的に実現した。サービスを利用するユーザは Web ブラウザを利用して Web サーバにアクセスする。Web サーバは GLI サーバおよび Vehicle-Info サーバに検索を行い、検索結果や地図情報などを利用して Web ページを生成し、Web ブラウザへ出力する。

実装は、Web ブラウザによる検索については 3.1.2 項で述べた Web クライアントのプロトタイプ実装を

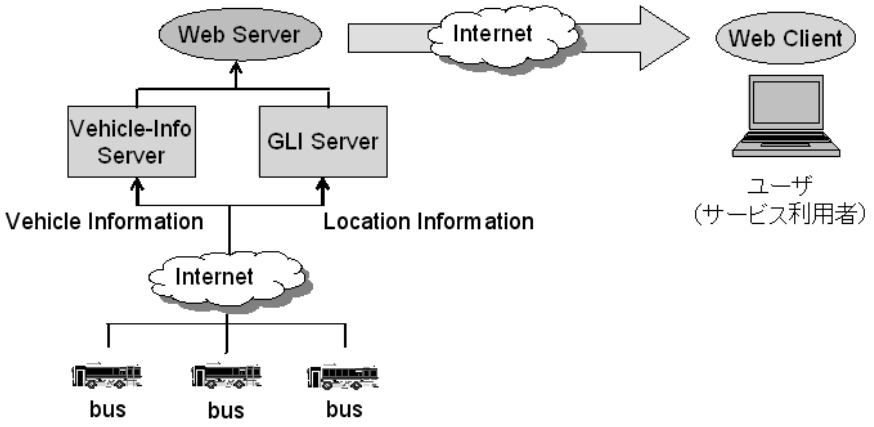


**図 3.5.** システム構成

ベースとして開発した。また、疑似登録クライアントについてはGLIシステム登録クライアントをベースに開発した。

### 3.2.3 システム動作例

システムの動作例を図3.6に示す。地図にGLIシステムの逆引き検索結果として現在走行しているバスがアイコンとして表示され、右側のフレームにて走行しているバスの位置情報とセンサ情報（速度センサ、ウィンカー）、前方のカメラ画像が表示される。

## 3.3 おわりに

本章ではWebを利用したアプリケーションとして、GLIシステムWebクライアント、バス運行状況検索システムについて説明した。今後も引き続きアプリケーションの開発を行い、GLIシステムの普及を進めると同時に、応用例としての位置情報サービスについて研究を進める予定である。


**図 3.6.** バス運行状況検索システム動作例

## 第 4 章　柔軟なプライバシ保護を考慮した分散型位置情報システムの提案

### 概要

本章では、柔軟なプライバシ保護を実現した地理位置情報システム（GLIPSE システム）を提案する。GLIPSE システムは、インターネットに接続している移動体（以下、Agent と呼ぶ）の地理位置情報（緯度・経度・高度）を管理する。従来の位置情報システムと異なり本システムでは、Agent が設定するプライバシポリシのもとで公開する位置情報を制御できる。これは、アクセス制御表とルールを管理するサーバを導入することにより行う。公開する位置情報を制御することにより、第三者による Agent 特定、位置情報特定、および Agent 追跡を防止する。また、IPsec の ESP と AH を利用することにより、インターネットにおける盗聴防止、データ改竄防止、なりすまし防止も実現している。暗号や電子署名処理にかかる時間を測定し、本システムの性能を見積もる。

### 4.1 はじめに

近年、インターネットと携帯端末の急速な普及により、移動するユーザの地理的な位置情報を利用するアプリケーションが多く開発されている。単純なアプリケーションとしては、NTT ドコモが 2000 年 1 月より提供している「どこ Navi」サービスがある。さらに、地理的位置情報を利用するアプリケーションが様々な場面で利用されることが期待されている [336]。しかしながら、地理的位置情報を管理することで享受できるメリットの一方でプライバシ侵害などの新たな問題が予想される。

たとえば、情報がサービス提供者以外に利用されてしまう、匿名で提供した位置情報が個人と対応づけられてしまうなどの問題が生じる。このような問題を防ぐために IETF geopriv WG では、位置情報システムにおけるプライバシ保護を考慮するための要求仕様が議論され、[48] で公開している。だが、現状ではこれを実装したシステムはない。

[369] でプライバシ保護を考慮した地理位置情報システム（GLI: Geographical Location Information）が提案された。このシステム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および付帯情報の登録・検索機能を実現している。GLI システムでは、時とともに変化する匿名の識別子で登録することにより移動体の特定・追跡を防止している。また、この識別子は移動体と信頼関係にある者は移動体と対応づけることができ、信頼関係のない者には統計情報しか公開しないことでプライバシを保護している。

しかし、実際にプライバシを保護するためには位置情報を公開するか・しないかだけではなく、公開する情報を含めて、よりきめ細かく制御する必要がある。たとえばユーザはある時間帯のみ、あるエリア内でのみ、または目的に応じて位置情報を公開するか・しないかを決めたい。このようにさまざまな条件に応じて公開する位置情報を調整することが求められている。

この概念を考慮した例としては、[340] が知られている。しかし、位置情報システムの応用範囲を広げる、位置からその場にいる移動体を検索する機能がなく、サーバの分散化も考慮されていない。そこで、GLI システムの高度な検索機能を損なうことなく、[48] で議論されているプライバシ保護の肝心となる要求を適用した新たな位置情報システム GLIPSE（Geographical Location Information with Privacy and Security Enhancement）を提案する。

### 4.2 セキュリティ上の脅威とプライバシ保護の目標

GLIPSE システムは、大きく分けて、位置情報を登録するエンティティ（以下、Agent と呼ぶ）、情報を管理するサーバ群（以下、Servers と呼ぶ）と、位置情報を検索しそれを利用するエンティティ（以下、Client と呼ぶ）からなる。各エンティティはインターネットを介して通信を行う。プライバシ保護をするためには、各エンティティが管理するデータおよびそれぞれの通信に対する脅威からデータを守らなければならない。[52] では、IETF WG で議論された位置情報システムにおける脅威分析が公開されている。

ここでは、Servers を基本的に信用しないという前提の上で GLIPSE システムのセキュリティ上における脅威を抽出し、プライバシ保護の目標を定める。

#### 4.2.1 プライバシ侵害

GLI システムでは信頼関係の有無でしか情報を制御できない。Agent と、信頼関係を結んでいる Client

すべてとの間で同じ秘密を共有しているため、一度許可したClientのアクセスを再度禁止することが難しい。したがって、Agentが許可した目的外で利用されることを防ぎにくくなり、Agentのプライバシが侵害される危険性がある。また、あるエリア内に登録するAgentが少ない場合においては、時とともに変化する匿名の識別子を利用しても、Agentを特定される可能性があり、プライバシ侵害につながる。したがって、信頼関係があるかどうかでのみ制御するのではなく、さまざまな条件に応じて精度を含めて位置情報を制御できるシステムを設計する。

#### 4.2.2 通信路での盗聴、改竄

インターネットを介して通信を行うことにより、通信データが盗聴されたり、改竄される可能性がある。通信中のデータには送信元のIPアドレスが含まれるため、そのデータを特定のAgentと対応付けられる可能性がある。また、過去に盗聴したデータを利用して、位置情報とすり替える再生攻撃も考えられる。したがって、データが盗聴されても盗聴者に解釈できず、データが改竄されたり古いデータを再送信された場合でも、各エンティティがそれを検出できるようにする。

#### 4.2.3 なりすましの脅威

悪意を持つ要素がAgentになりすまして偽の位置情報を登録し、Serversになりすまして Agentが登録するデータを奪ったり、またあるClientになりすまして Agentがその Clientに許した位置情報を得てしまうなどの危険性がある。したがって、なりすまし防止ができる、各エンティティが互いに認証し合えるメカニズムを扱えるようにする。

#### 4.2.4 データベースの盗難・書換

位置情報を管理するServersはそれぞれAgentとその位置情報を対応づけられるデータベースを持っているので、Serversのデータベースが盗難されたら、Agentを特定される可能性がある。したがって、データベースが盗難された場合においても、許されたエンティティ以外には解読できないようにする、またはAgentにとって最低限の被害しか及ばないようにシステムを設計する。

### 4.3 プライバシ保護のための機構

本節では、GLIPSEシステムにおけるプライバシ保護のための機構について述べる。

#### 4.3.1 アクセス制御表とRule Serverの利用

ユーザのプライバシポリシはアクセス制御表（Access Control List、ACL）に記述される。ACLでは、何種類の精度の位置情報を用意するか、どのClientに対してどの情報を渡すかなどがリストされる。本章ではACLについて、異なる精度の情報を$n$個生成する方法と、その選択ポリシをリストすることのみで、詳細は定めない。

Clientは位置情報を取得するためにACLを管理する要素から毎回許可を取得しなければならないため、Agent自身がACLを管理するのは現実的ではない。したがって、サーバ群の中にACLを管理するためのRule Serverを導入する。Clientにどの情報を渡すかを決めるためにはRule Serverに問い合わせる形にする。このようにすることによって情報取得権を持つClientのみが、Agentに許された情報を取得できることになり、4.2.1項の脅威に対処できる。

#### 4.3.2 情報の暗号化と認証機能—IPsecの利用

通信路での機密性を高めるために、IP Security（IPsec）のESP（Encapsulating Security Payload）[163]を使用する。ESPで各エンティティでの送信時に位置情報と送信するそのほかの情報を暗号化し、データの完全性や発信者認証も行う。これは、4.2.2項の盗聴対策に効果があり、過去のデータによる再生攻撃にも有効である。また、ESPの発信者認証機能により4.2.3項の悪意要素によるなりすまし防止もできる。改竄防止と発信者認証機能のみが必要な通信の場合は、IPsecのAH（Authentication Header）[162]を利用する。

IPsecを使用するためにはエンティティ間において秘密鍵の共有などのSecurity Association（SA）が必要になる。SA確立時にはIKE（Internet Key Exchange）[120]を用いる。

GLIPSE中にはPKI[335]を構築し、IKEで利用する各要素の公開鍵や電子署名の正当性をGLIPSEのCAが保証できるようにする。

#### 4.3.3 Servers で管理するデータの分割

データベース盗難の対策として、各サーバで管理するデータを分割する。特に、位置情報とその所有者情報を対応付けられないようにこれらを別のサーバで管理する。両方の情報が別々に管理できない場合、1 つの情報所有者に対して 1 台のサーバが管理するようにする。これにより、そのサーバが乗っ取られた場合でも、1 人の所有者の情報のみ漏洩することになり、4.2.4 項を満たすことができる。

### 4.4 提案システムの設計

#### 4.4.1 構成

GLIPSE システムは位置情報を登録する Agent(A)、ACL を管理する Rule Server（RS)、位置情報を管理する Data Server（DS)、各地理位置情報に対応した Agent の情報を管理する Area Server（AS）と位置情報を検索する Client（C）から構成される。分散管理については [352] と同様の手法を用いる。

本システムの説明をする準備として、以下のものを定義する。

- $E_A(M)$
  メッセージ $M$ を鍵 $A$ で暗号化したもの（暗号文)。
- $S_A(M)$
  メッセージ $M$ に $A$ の署名を付加したもの。
- $Cert_A$
  $A$ の証明書。
- $L$
  Agent が登録する位置情報。本システムで扱う位置情報は、現実世界で移動するエンティティの地理的な位置情報 [緯度、経度、高度] である。$L$ は ACL で指定した異なる精度 $n$ 種類で登録できる。
- $ID$
  Agent の元々の識別子。インターネット上の IP アドレス、FQDN やユーザ名、現実世界での名前などにあたる。
- $pseudoID$
  ID をスクランブルした、時とともに変化する識別子。第三者による Agent の $ID$ との対応付けは困難である。この識別子は Area Server 内での Agent の匿名性を保っている [336]。
- $ttd$
  位置情報の有効期限。ある程度位置情報が更新されないとき、各サーバのデータベースから Agent の情報を削除するまでの時間である。
- $i$
  位置情報の精度を表す番号。
- 正引き検索
  ID を鍵として Agent の位置情報を検索する機能。たとえば、ある Agent の ID を指定して検索すると、許可された精度の位置情報が得られる。
- 逆引き検索
  地理的な位置情報を鍵として、その領域に存在する Agent を検索する機能。たとえば、検索する範囲を 2 点の位置情報で指定して（北緯 50 度〜51 度、東経 100 度〜101 度）検索すると、その範囲内にいる Agent 群と、その位置情報のリストが得られる。

#### 4.4.2 動作

本項では、登録処理、正引き処理と逆引き処理のそれぞれについて、通信手順を説明する。

**登録処理**

登録処理の手順を図 4.1 に示す。さらに詳しい手順を図 4.2 に示す。

Agent は位置情報 $L$ と $ID$、オプションとして $ACL$ と $ttd$ を Rule Server に ESP で登録要求を送る。

Rule Server は ACL に基づいて位置情報 $L$ を $n$ 通り計算し、各 $L$ に対する鍵 $K_i$ を生成する。データセット $[ID, i, E_{K_i}(L_i), ttd)]$（$ttd$ はオプション）のリストを ESP で Data Server に登録要求として送る。このようにして、1 つの Agent に対してさまざまな精度の位置情報を Data Server に登録する。

同様に、Rule Server はデータセット $[pseudoID, i, L_i, ttd]$（$ttd$ はオプション）のリストを Area Server に登録要求として ESP で送る。このようにして、1 つの $pseudoID$ に対し、さまざまな位置情報を登録することが可能である。

**正引き処理**

正引き検索処理の手順を図 4.3 に示す。さらに詳しい手順を図 4.4 に示す。

Client は検索したい $ID$ を Rule Server に検索要求として ESP で送る。

Rule Server は ACL に基づいて Client に許された位置情報の精度 $i$ を決定し、その精度 $i$ に対する

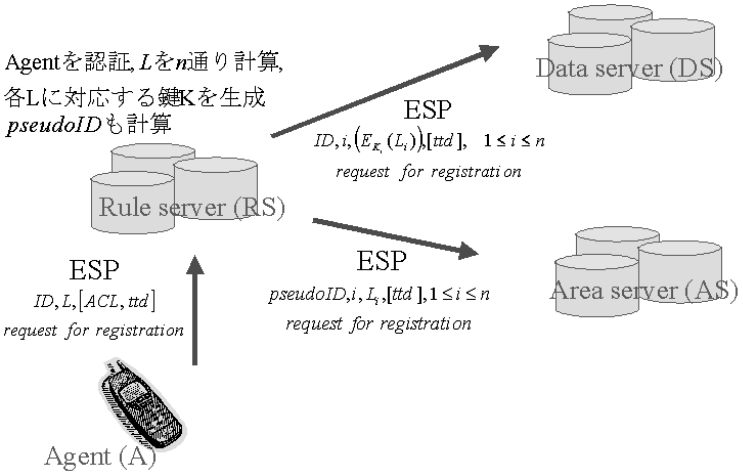


**図 4.1.** 登録手順

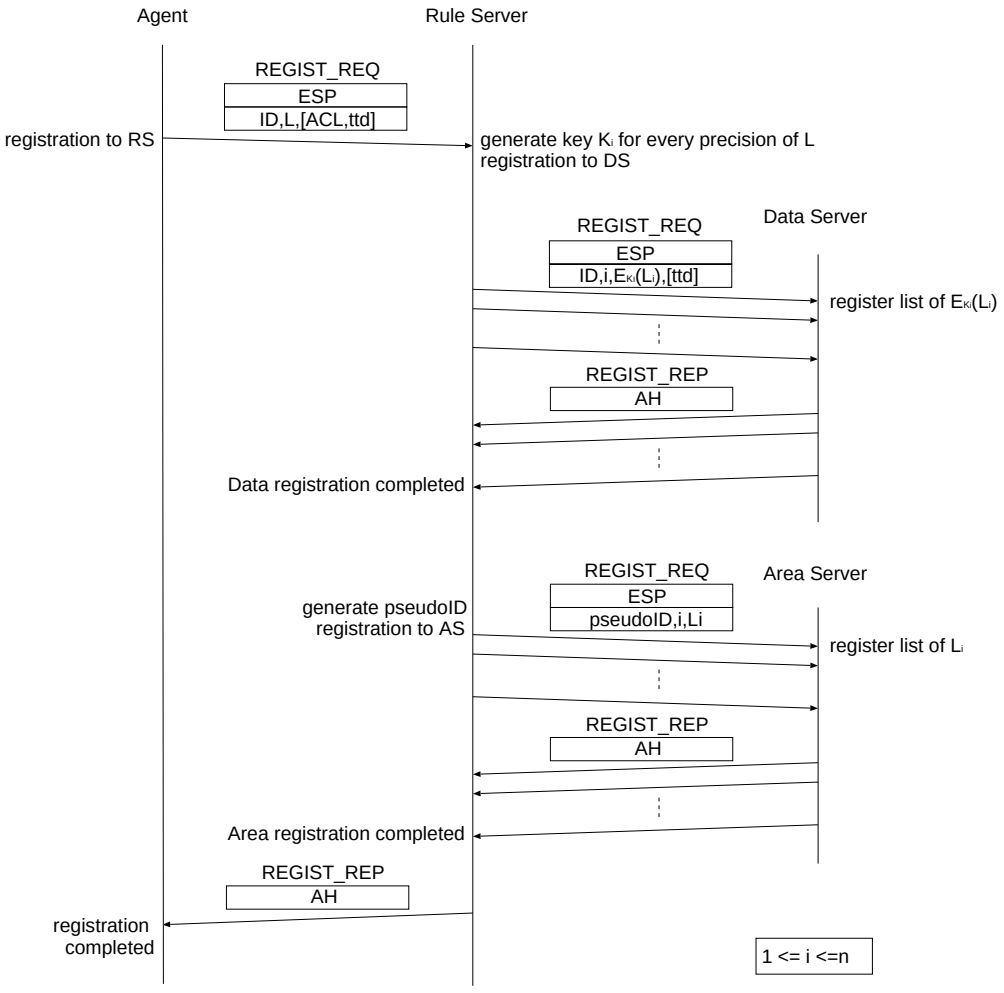


**図 4.2.** 登録処理（詳細）

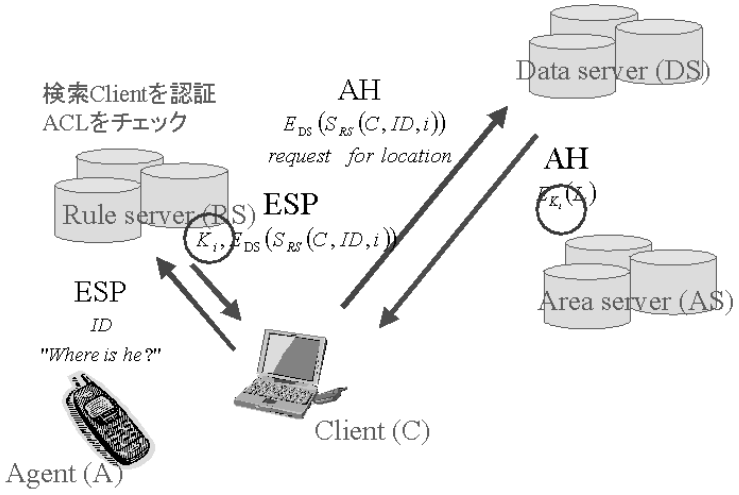


**図 4.3.**　正引き検索処理

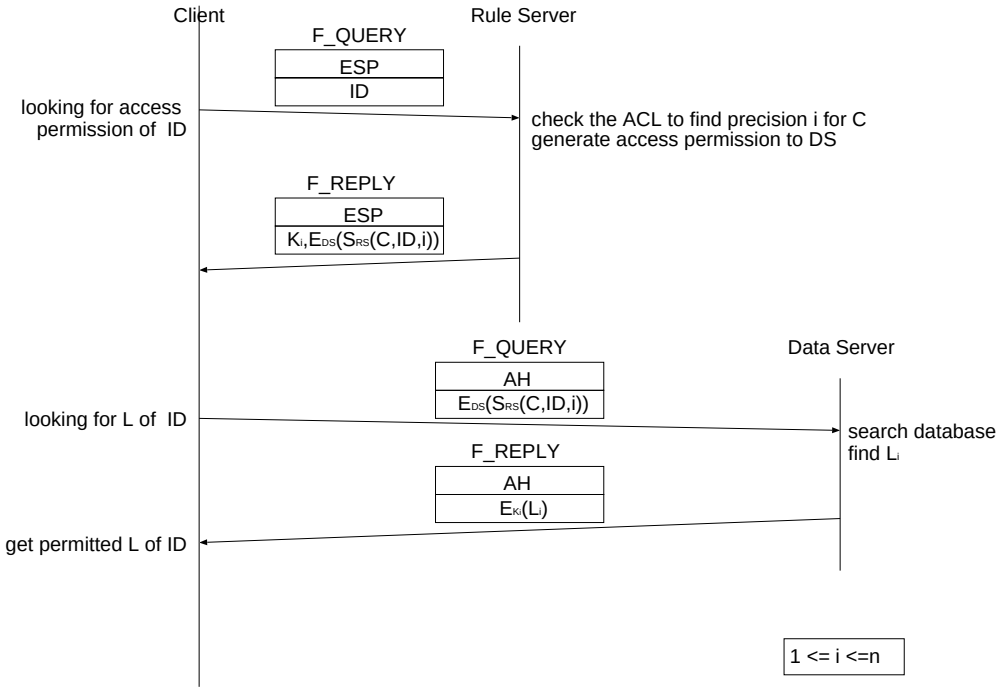


**図 4.4.**　正引き検索の手順（詳細）

鍵 $K_i$ とアクセス許可を Data Server の公開鍵で暗号化し、データセット $[K_i, E_{DS}(S_{RS}(C, ID, i))]$ を ESP で Client に送り返す。

Client はそのアクセス許可を Data Server に送る。Data Server は鍵 $K_i$ で暗号化されたままの情報を AH で Client に送り返す。

Client は Data Server から受信した鍵 $K_i$ で復号化し、Agent の位置情報を取得する。

**逆引き検索**

逆引き検索処理の手順を図 4.5 に示す。図 4.6 にその詳細を示す。

Client は検索したい範囲指定し、Area Server に AH で検索要求を送る。

Area Server は要求された範囲に $m$ エントリを発見すると、各エントリに対してどの位置情報を返せばいいのかを Rule Server に問い合わせる。Rule Server は ACL を確認し、各エントリに対して Agent が許可した位置情報の番号 $i$ を Area Server に返す。

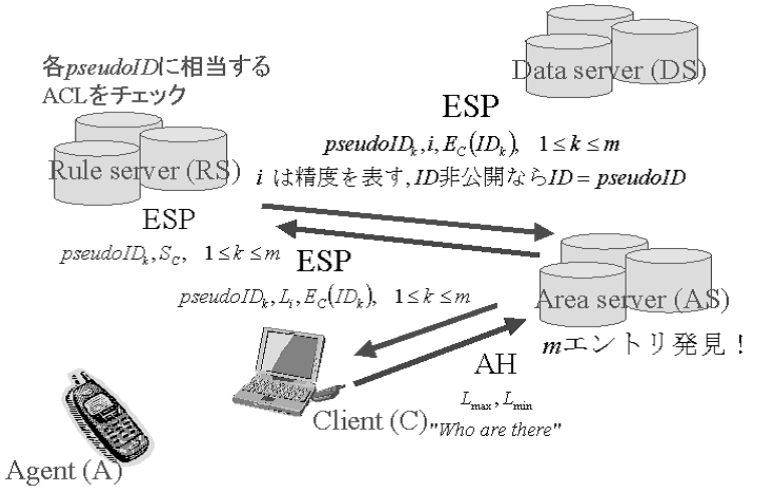


**図 4.5.** 逆引き検索の手順

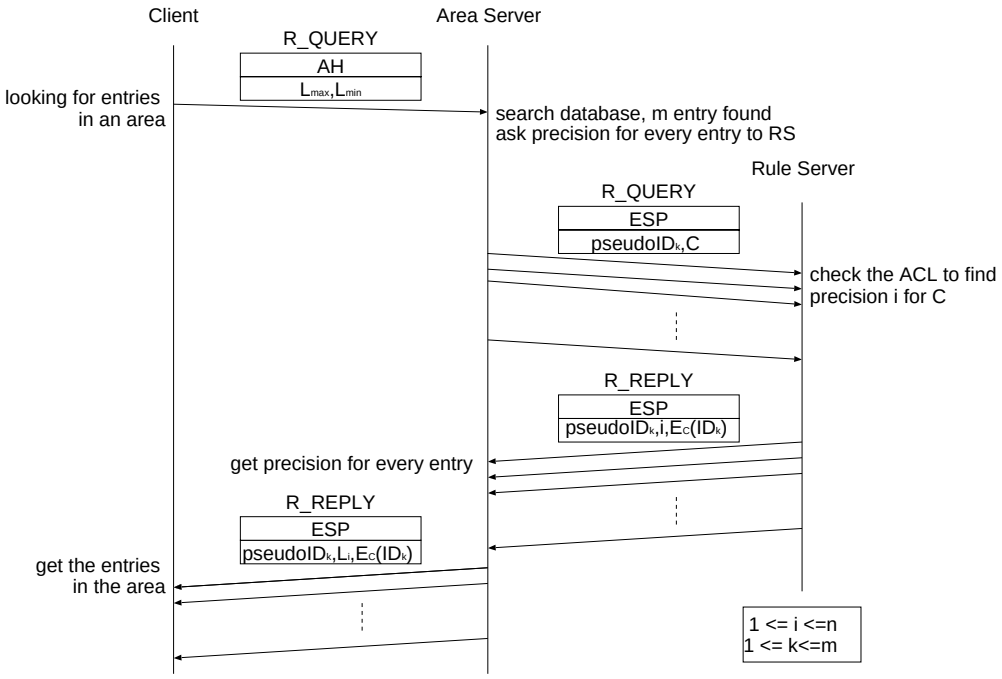


**図 4.6.** 逆引き検索処理（詳細）

その Client に対して Agent の *ID* を明らかにしてもよい場合には、その *ID* を Client の公開鍵で暗号化して同時に返す。そうでなければ、*pseudoID* を渡す。このようにして、Agent が許可した情報しか Client に渡さないことになる。

## 4.5 評価および考察

本システムにおいては、暗号処理の部分に大きな負荷がかかると予想される。本実装に向けて、準備実験として本システムで利用する各種暗号の処理時間を測定し、システム全体の性能の見積もりを行った。また、電子署名の生成と認証の処理時間も測定した。

全ての実験は AiCrypto ライブラリ関数 [4] を使用して行った。測定は、Intel 社製 Pentium 4（2.40 GHz）CPU を用いた FreeBSD4.9-RELEASE 上で行った。

### 4.5.1 暗号の処理

まず、公開鍵暗号による暗号化と復号化の処理時間を測定した。測定に用いた関数は AiCrypto ライブ

**表 4.1.** RSA における暗号化および復号化の処理時間

| 処理 | 平均処理時間 |
|---|---|
| 暗号化 | 1.2 msec |
| 復号化 | 46.9 msec |

**表 4.2.** 3DES CBC モードにおける暗号化および復号化の処理時間

| 処理 | 平均処理時間 |
|---|---|
| 暗号化 | 1.5 msec |
| 復号化 | 1.4 msec |

ラリの RSAprv_doCrypt() と RSApub_doCrypt() という関数である。使用した鍵の長さはそれぞれ、modulus INTEGER $n$ 1024 bit、publicExponent INTEGER $e$ 17 bit と privateExponent INTEGER $d$ 1024 bit である。ランダムな 128 byte の入力値で暗号化と復号化を 10000 回処理し、測定した。結果を表 4.1 に示す。

同様に、共有鍵暗号による暗号化と復号化の処理時間を測定した。使用した関数は DES3_cbc_encrypt() と DES3_cbc_decrypt() である。192 bit の鍵長に、実装で使用するデータペイロードに十分な大きさとして、4096 byte の入力値を 10000 回処理し、測定した。結果を表 4.2 に示す。

#### 4.5.2 電子署名の処理

認証に使用する電子署名の生成および検証するための処理時間を測定した。利用した関数は電子署名生成の場合は、OK_do_signature()、その署名の検証の場合は、OK_do_digest() と OK_do_verify() である。128 byte の平文に 128 byte の秘密鍵、SHA1withRSAEncryption アルゴリズムで 10000 回処理し、測定した。結果を表 4.3 に示す。

**表 4.3.** SHA1 および RSA 暗号化による電子署名の処理時間

| 処理 | 平均処理時間 |
|---|---|
| 署名の生成 | 47.4 msec |
| 署名の検証 | 1.3 msec |

#### 4.5.3 登録、検索の性能見積り

IKE、ESP、AH、暗号や電子署名の処理回数を数え上げ、4.5.1 項と 4.5.2 項の測定結果を代入し、登録や各検索全体の処理時間とその性能の見積もりを 1 回目と 2 回目以上の処理に分け、表 4.4 にまとめた。なお、$n$ は公開する位置情報の精度の数、$m$ は検索で発見したエントリ数である。

**表 4.4.** 処理時間と性能の見積もり

| 処理 | | 登録 ($n = 2$) | 正引き検索 | 逆引き検索 ($m = 20$) |
|---|---|---|---|---|
| 処理時間 (msec) | 1 回目 | $148.8 + 3n$ $= \mathbf{154.8}$ | **247.1** | $148.7 + 5.6m$ $= \mathbf{260.7}$ |
| | 2 回目以上 | $1.4 + 3n$ $= \mathbf{7.4}$ | **99.7** | $5.6m$ $= \mathbf{112}$ |
| 性能 (req/sec) | 1 回目 | **6** | **4** | **4** |
| | 2 回目以上 | **135** | **10** | **9** |

#### 4.5.4 従来の位置情報システムとの比較

本項で、プライバシの保護について従来の GLI システムと比較する。

GLI システムでは Agent がある位置に長時間停止していると、匿名の *ID* が変化しても、その匿名の *ID* がどの Agent の *ID* であるかが対応づけられてしまう。また、GLI システムでは、匿名の ID の有効期間内には Agent の追跡ができてしまう。なぜなら、正引き検索で利用する検索鍵は逆引き検索で取得できるためである。しかし、GLIPSE システムでは、アクセスを Client ごとに制限することとそれぞれの検索に異なる *ID* を用いることにより、両方の問題を回避できる。

GLI システムでは、Agent と信頼関係にある Client は匿名の *ID* を生成し、偽の位置情報を登録可能である。それに比べ、本システムは電子署名により各エンティティの認証を行っているため、権限のあるエンティティ以外は偽の登録ができない。したがって、プライバシ保護の面においては、GLIPSE システムがより優れているといえる。

#### 4.5.5 サーバの盗難・書換

GLIPSE システムで各サーバが管理する情報を表 4.5 にまとめた。Rule Server は最も信頼されるサーバで、Agent とその Agent の位置情報の対応を含めてすべて管理している。本システムにおいては、1 つの Rule Server は 1 台の Agent を管理するとする。したがって、Rule Server が乗っ取られた場合、1 台の Agent の情報しか影響されないで済む。1 つの Rule Server で複数の Agent を管理することも可

**表 4.5.** 各サーバで管理する情報

| サーバ | 管理する情報 |
|---|---|
| RS | A、DS、AS の IP アドレス、$ACL$、$ID$、$pseudoID$、鍵 $K_i$、$L$ |
| DS | RS の IP アドレス、$ID$、$E_{K_i}(L_i)$ |
| AS | RS の IP アドレス、$pseudoID$、$L_i$ |

能だが、サーバ運用コストとプライバシ保護の機能はトレードオフの関係にある。

Data Server は Agent の $ID$ 情報を持つが、管理する位置情報は暗号化されたものしか持たない、また Area Server は位置情報を持つが、本当の $ID$ は持たない。このため、一度に両方のサーバが乗っ取られても、Agent を特定・追跡されない。

### 4.6 おわりに

本章では、さまざまな条件に応じて位置情報の公開精度を制御できる GLIPSE システムの枠組みを提案した。本システムでは、Rule Server に登録する Agent ごとの ACL（アクセス制御表）を持たせることにより柔軟なプライバシ保護を実現した。また、IPsec の ESP を利用することで各通信路での機密性を高め、データが盗聴されても Agent の特定、追跡を防止できた。IPsec の AH を利用することで各要素の成りすましも防止した。最後には、現状の位置情報システム [369] に付加された機能の性能評価を行い、増加するオーバーヘッドの見積もりを行った。

本システムの問題点は、暗号にかかる処理時間である。したがって、より性能の良いシステムを設計するためには暗号処理を軽減するための工夫が必要である。今後はそれについて改良と実装を行い、システム全体の性能を評価する。また、Rule Server が管理する情報の機密性を高める仕組みも検討する。さらに、このシステムを効果的に利用できるアプリケーションを検討する。

## 第 5 章　実運用を想定した大規模位置情報管理機構の構築

### 5.1 背景

近年、ワイヤレスネットワークの多様化、普及が進み、ユーザは携帯電話、PDA といった携帯型小型計算機を使用して、いつ、どこにいてもネットワークに接続できるモバイル・コンピューティングの環境が整備されている。また、GPS などの位置情報取得インフラの整備が進み、カーナビゲーションなどのようにユーザは気軽に現在位置情報を取得し、利用することが可能となっている。上記のように、いつ、どこにいてもネットワークに接続することが可能、かつ現在位置の取得が可能な環境においては、移動体は自身の位置情報をほかの移動体へ通知したり、自身が位置する地点の周辺情報を取得することが可能となる。

現在、移動体の位置情報通知や移動体へ配信する周辺情報に関する関心が高まりさまざまな研究がなされている。具体的には位置情報交換サービスや、移動体が位置する地点の周辺の店舗、天候、交通情報などを移動体へ提供するサービスなどが挙げられる。

このように移動体の位置情報を利用して提供されるサービスを位置情報サービスという。

### 5.2 大規模位置情報管理機構

本節では、位置情報サービスにおける位置情報管理機構の役割を定義し、位置情報管理機構への要求事項を決定する。次に、大規模位置情報管理機構の定義を行い、位置情報管理機構との相違について述べ、大規模位置情報管理機構への要求事項を定義する。そして、既存の大規模位置情報管理機構について大規模位置情報管理機構への要求事項に照らして考察する。

#### 5.2.1 位置情報管理機構の定義と要求事項

**定義**

位置情報サービスには、移動体が自身の位置情報を取得・利用して、周辺の情報を取得するものと、自分以外の他者の位置情報を取得して利用するものに分類される。位置情報サービスで必要とされるのが、移動体の位置情報を管理する機能である。位置情報の管理とは、位置情報を登録し、検索できることである。位置情報を管理することで、以下のようなことが可能となる。

**物体の位置情報の探索**

指定した物体の位置情報を取得する。

**位置情報に基づく物体の探索**

指定した位置情報（地点・範囲）に存在する物体を探索する。

**位置情報に基づくサービスおよび資源探索**

指定した位置情報（地点・範囲）に存在するサービスまたは資源を探索する。

**位置情報に基づく通信**

指定した位置情報（地点・範囲）に存在する物体からの情報収集や物体へメッセージを配信する。

**位置情報管理機構への要求事項**

ここでは、位置情報管理機構への要求事項を導出する。位置情報管理機構は位置情報サービスをサポートする機構であるため、位置情報管理機構は、位置情報サービスへの要求事項をもとに導出される。文献 [155] では位置情報サービスに対するユーザのニーズを調査し、ユーザは位置情報サービスに対する関心・興味はあるが、自身の位置情報が、自分が意図しない第三者に取得されることを恐れること、ユーザはいつ・どこにいても位置情報サービスが利用できることを望むという調査結果を導出している。以上より、以下の要求事項が導出される。

**プライバシの保護**

位置情報を公開する相手は、その位置情報の持ち主の許可する相手に限定される必要がある。このような位置情報公開に関するプライバシ保護について、インターネットに関する技術の国際標準化組織である IETF（The Internet Engineering Task Force）[132] の geopriv WG（Geographic Location/Privacy）[104] では、位置情報を扱う上での保護すべきプライバシの要求事項 [48] を規定している。geopriv WG のまとめた要求事項においても、位置情報の公開は位置情報の持ち主、または、位置情報の持ち主と関係のあるものによって、制御される必要があるとされている。したがって、位置情報管理機構は位置情報の公開を、位置情報の持ち主によって制御できる機能が必要である。

**管理領域に対する規模性**

移動体は、あらゆる場所へと移動する。したがって位置情報管理機構は、位置情報の管理対象が、どこにいても、その位置情報を管理できる必要がある。位置情報管理機構は、管理する領域が特定の個所に限定されるのではなく、あらゆる場所を管理領域とすることが可能な管理領域に対する規模性を実現する必要がある。

**位置情報の信頼性**

位置情報管理機構の提供する検索機能により取得された位置情報は、その位置情報の持ち主以外のものの位置情報であってはならない。したがって、位置情報管理機構は、位置情報管理対象の位置情報の信頼性を実現する必要がある。

**位置情報の安全性なやりとり**

位置情報管理機構に登録された位置情報は、位置情報を登録した者によってのみ更新・削除されるべきであり、位置情報を登録したもの以外の者による位置情報の改竄は防止しなければならない。また、位置情報の登録時や検索時の位置情報をやりとりする際に、登録者や検索者以外の第三者による情報の盗聴も防止しなければならない。したがって、上記のような位置情報の改竄・盗聴といった位置情報の安全なやりとりにおける障害は防止される必要がある。

**安定した継続運用**

位置情報管理機構は、常時登録・検索ができる必要性がある。

**検索機能**

位置情報管理機構により実現されるサービスは、物体の識別子による検索と、位置情報による検索の 2 つの検索に集約される。したがって、位置情報管理機構は移動体の指定した検索と、領域を鍵とした検索の 2 つの検索機能が必要である。

以上の要求事項を満たすことで、より実用的なしくみとなり、位置情報サービスをサポートする位置情報管理機構が確立される。

### 5.2.2 大規模位置情報管理機構

**大規模位置情報管理機構の定義**

大規模位置情報管理機構とは、位置情報を管理する対象を特定せずにさまざまな種類の物体の位置情報を管理することで、特定のサービスに特化せずにさまざまなサービスをサポートできることを実現する位置情報管理機構である。

**大規模位置情報管理機構への要求事項**

通常の特定の物体のみの位置情報管理や、特定のサービスのみをサポートする位置情報管理機構とは異なり、膨大な数の物体の位置情報を管理することが可能である。たとえば、自動車は日本全国で約 7000 万台、携帯電話は日本全国で約 8000 万台存在してい

る。このような膨大な数の物体の位置情報を管理するには、5.2.1 項で述べた通常の位置情報管理機構への要求事項に加え、管理移動体数に対する規模性を実現する必要がある。

**大規模位置情報管理機構の運用**

大規模位置情報管理機構の運用時には、これまでに定義した要求事項を満たして運用されなければならない。大規模位置情報管理機構では、管理する移動体数が膨大なため、機構への登録要求数や、登録頻度も膨大なものとなる。たとえば、約 6000 万台といった膨大な数の位置情報の登録処理や検索処理を、物理的に 1 台のデータストレージマシンで担当するには、非常に高性能なマシンスペックが必要である。さらにトラフィックの集中が発生するため、このトラフィックを処理できる広帯域なネットワークも不可欠である。現状では、上記のような単独のマシンで大規模位置情報管理機構のすべての処理を行うための高性能マシンや、広帯域ネットワークを用意するには莫大なコストが必要となる。そのため、実際に大規模位置情報管理機構を運用するには複数のデータストレージマシンで、処理を分担する手法がより実用的な手法である。

上記のような複数のマシンによる分散管理を $N$ 台のマシンで行う際、そのマシンの 1 台あたりの MTBF（Mean Time Between Fairures）を $M$ とすると、システム全体における MTBF の平均は $M/N$ となり、利用するマシンの台数が増えるほどシステム全体の MTBF は短くなる。

5.2.1 項より、位置情報管理機構には安定した継続運用が求められている。したがって、複数のマシンによる分散管理形態にて成り立つ大規模位置情報管理機構では、自身を構成するマシンの故障時にも位置情報管理機能を提供できるという堅牢性が必要である。

### 5.2.3 既存の位置情報管理機構

**Architecture of a Large-scale Location Service**

Architecture of a Large-scale Location Service[6] では、大規模位置情報管理機構の構築を目指して、インターネット上に複数のデータストレージマシンを木構造の階層型に分散配置する分散管理形態を導入したシステムを提案している。このシステムを位置情報管理機構への要求事項に照らして考察する。まず、検索機能として、識別子による検索と、領域による検索の 2 つの機能をサポートしている。また、緯度経度を位置識別子として扱うことにより地球上に存在する物体ならば、その物体の位置情報を管理することができるという管理領域に対する規模性を備えている。以上の 2 点に関しては、位置情報管理機構への要求事項を満たしているといえる。しかし、位置情報の正確性・信頼性に関する考慮が欠如しており、位置情報の持ち主以外の者によるなりすましの防止ができない。また、位置情報の安全なやりとりに関する考慮も欠如しており、インターネット上で位置情報のやりとりを行う上で脅威となるデータの盗聴・改竄を防止できない。管理移動体数に対する規模性に関しては、分散管理形態を導入することにより実現している。しかし、分散管理形態をとる大規模位置情報管理機構において重要となるシステムの堅牢性に関しては、言及されていない。

**携帯電話を利用した位置情報管理サービス**

携帯電話を利用した位置情報管理サービスとして、NTT ドコモの DLP（Docomo Location Platform）や、KDDI の GPS MAP が挙げられる。これらは、携帯電話を管理対象とした位置情報管理機構であり、大規模位置情報管理機構にはあたらない。これらのサービスは相手を指定した検索、領域による検索をサポートし、さらにキャリア内にとどまるサービスであるためプライバシの保護、位置情報の正確性・信頼性、安全な位置情報のやりとりが実現されている。

### 5.2.4 現状のまとめ

膨大な数の移動体の位置情報の管理を目的としない位置情報管理機構に関しては位置情報管理機構への要求事項を満たすものも存在している。しかし、膨大な数の移動体の位置情報の管理を目的とする大規模位置情報管理機構に関しては、位置情報管理機構としての要求事項を満たしつつ、大規模位置情報管理機構特有の要求事項である管理移動体数に対する規模性や堅牢性を実現できている位置情報管理機構は存在しない。

## 5.3 先行研究：GLI システム

本節では、インターネットによる位置情報管理機構

である GLI（Geographical Location Information）システム [369, 370] について述べ、5.2.2 項で示された位置情報管理機構への要求事項に照らして GLI システムを考察する。さらに、大規模位置情報管理機構としての妥当性について検討し、実運用を可能とする大規模位置情報管理機構を実現する上での問題点を明らかにする。

### 5.3.1 GLI システムの概要

以下に、5.2.1 項で示した大規模位置情報管理機構への要求事項を基づき、GLI システムの設計を考察する。

#### 検索機能

GLI システムでは、識別子を鍵とした検索と領域を鍵とした検索をサポートする。識別子を鍵とした検索では検索者は位置情報を取得したい相手の識別子を鍵として GLI システムに検索できる。GLI システムでは、識別子を鍵とした検索を正引き検索と呼ぶ。検索者は任意の領域を鍵として、その領域内に存在する管理対象の識別子と位置情報のリストを取得できる。GLI システムでは、領域を鍵とした検索を逆引き検索と呼ぶ。

#### プライバシ保護

GLI システムでは、プライバシ保護を実現するために、管理する移動体の識別子に Hashed ID（HID）と呼ばれる識別子を採用している。HID は、鍵付ハッシュ関数に移動体の真の識別子と秘密鍵を作用させて生成される。HID を利用することにより移動体は、信頼関係のある検索者とのみ秘密鍵を共有し、信頼関係のない第三者による位置情報の検索を防ぐことが可能となる。

#### 管理領域に対する規模性

GLI システムでは位置情報の識別子に緯度・経度を採用しており、地球上に存在する移動体を管理することが可能であり、管理領域に対する規模性を実現している。

#### 位置情報の安全なやりとり

GLI システムは、インターネットを利用した位置情報管理機構であるため、ネットワークを介して位置情報の送受信がおこわなわれる。したがって、データの盗聴の危険性があるが、GLI システムでは IP Security（IPsec）[164] を利用してデータの盗聴を防止している。

#### 信頼性

GLI システムは、なりすましの防止と、データの改竄を防止することで信頼性を実現している。GLI システムは、IPsec の認証機能を利用して位置情報の登録と管理対象の認証を行う登録サーバとよばれるサーバが存在する。登録サーバと位置情報の登録者の間には、Security Authentication（SA）をあらかじめ確立しておくことで、なりすましの防止を行う。また、GLI システムにおけるサーバ間の通信には、IPsec の暗号化機能を利用してデータの改竄を防止している。

#### 管理移動体数に対する規模性

GLI システムでは、インターネット上にデータストレージマシンを木構造の階層状に配置する分散管理形態を導入することで、管理移動体数に対する規模性を実現している。GLI システムでは、検索機能ごとに HID サーバとよばれるサーバ群とエリアサーバとよばれるサーバ群の 2 種類の分散サーバ群を設置している。これらのサーバ群は、HID サーバで最大 $\sum_{n=1}^{40} 16^{n-1}$ 台、エリアサーバで最大 $180 \times 360 + 180 \times 360 \times 60 \times 60 + 180 \times 360 \times 60 \times 60 \times 60 \times 60$ 台での分散管理を可能としている。この分散手法については文献 [352] で詳細が述べられている。

以上で挙げられた大規模位置情報管理機構への要求事項に関する GLI システムの考察を以下の表 5.1 にまとめる。

**表 5.1.**　大規模位置情報管理機構への要求事項と GLI システムの現状

| 要求事項 | GLI システム |
|---|---|
| 検索機能 | 識別子検索と領域検索をサポート |
| プライバシ保護 | HID による匿名化により実現 |
| 管理領域に対する規模性 | 全地球規模での管理 |
| 信頼性・安全な通信 | IPsec による盗聴・改竄防止 |
| 管理移動体数に対する規模性 | 位置情報の分散管理により実現 |

#### 5.3.2 実運用化にむけた GLI システムの問題点

**冗長性の欠如**

5.2.2 項で、分散管理形態による大規模位置情報管理機構は、実運用化においてシステムの堅牢性を実現する必要があることを述べている。5.3.1 項より、GLI システムは膨大な数のサーバから構成されることが可能であるが、このときの GLI システムの MTBF は非常に短いものとなりうる。GLI システムでは、GLI システムを構成するマシンの故障を想定していない。すなわち、GLI システムは、実運用を可能とするシステムの冗長性が実現されていない。

#### 5.3.3 HID サーバ/エリアサーバにおける故障の考察

GLI システムでは、図 5.1 に示すように登録要求や検索要求を受け付けた登録サーバや検索サーバが、木構造の階層型分散形態をとる HID サーバやエリアサーバの Root サーバから順次、委任情報を取得して、最終的に該当する HID サーバやエリアサーバへ位置情報を登録したり、検索結果を取得したりする。この時、木構造における Root サーバや、中間層のサーバが故障すると、故障したサーバへの登録・検索ができなくなるだけでなく、故障したサーバより下位層への委任情報を取得できなくなり、故障したサーバ以外でも複数のサーバへの登録・検索が不能となる。したがって、一部のサーバの故障により、GLI システムの一部〜全体への登録・検索が不能となる可能性がある。

GLI システムに、サーバ故障を対処する堅牢性を実現するには、以下の機能を実現する必要がある。

**サーバの故障を検知する機能**

常に、各サーバの動作状況を監視し、故障を検知したときには、登録・検索不能状態から復帰するために故障したサーバの情報をほかのサーバに通知する必要がある。

**故障したサーバの処理を代替する機能**

各 HID サーバ・エリアサーバでは、登録・検索処理と、下位層への委任情報の提供処理を行っている。サーバの故障を検知する機能より通知されたサーバの担当していた登録・検索処理と、下位層への委任情報を提供する処理を代替する機能を実現しなければならない。

### 5.4 設計

#### 5.4.1 サーバの故障を検知する機能

図 5.2 に故障を検知する機能の動作概要を示す。

1. 階層構造をとる HID サーバ・エリアサーバでは、上位層のサーバが下位層サーバの動作状況を監視する（図 5.2-1、2）。
2. 動作状況の監視には、動作監視パケット（KEEP_ALIVE パケット）を上位層サーバが、下位層サーバに対し送信し、動作監視パケットを受信した下位層サーバは、ACK パケットを返信する（図 5.2-2）。
3. 上位層サーバでは、動作監視パケットに対し返信を返した下位層サーバに関しては正常に動作していると認識する。動作監視パケットに返信を返さない下位層サーバ（図 5.2-1）に関しては、動作監視返信待ち状態と認識する（図 5.2-3）。
4. 登録サーバ・検索サーバにおいても、HID サーバ・エリアサーバの動作監視を行う（図 5.2-4）。登録要求や検索要求に ACK を返さない HID サーバとエリアサーバを発見すると、その HID サー

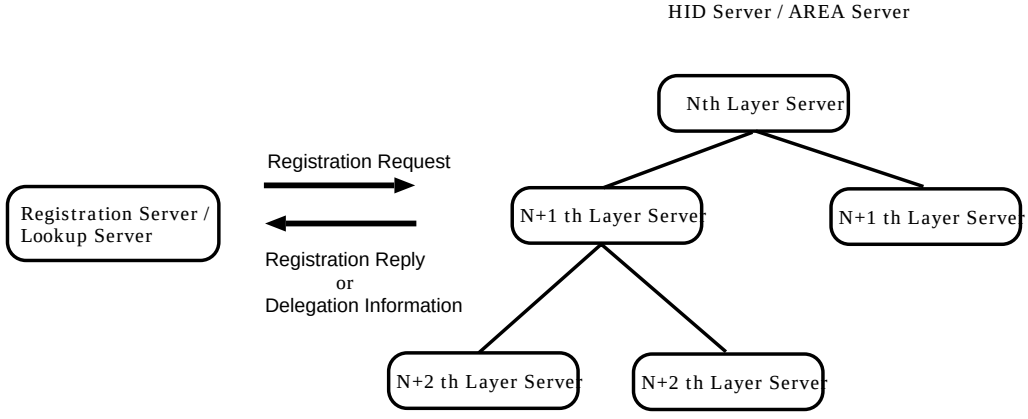


**図 5.1.** GLI システムにおける登録・検索時の動作概要

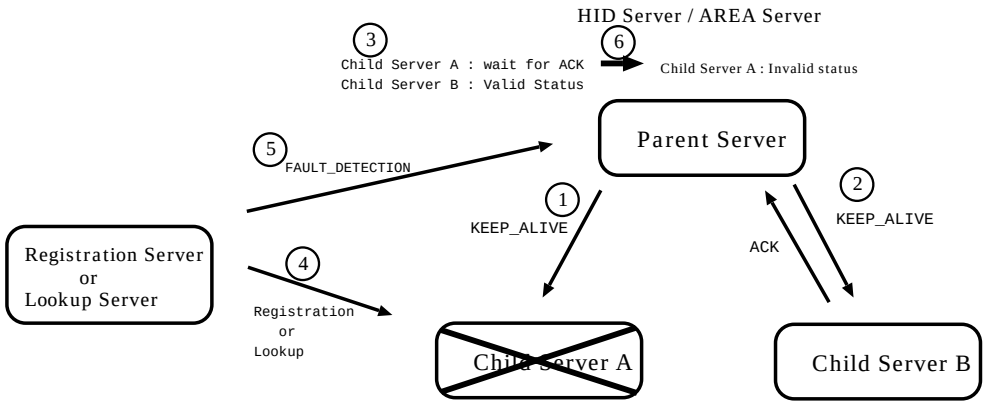


**図 5.2.**　サーバ故障検知機能の動作

バやエリアサーバの上位層のサーバに対し故障検知パケットを送信する（図 5.2-5）。

5. 故障検知を受信した上位層のサーバでは、故障検知をされた下位層のサーバの動作監視状態を確認し、正常に動作しているとされていた場合は下位層のサーバは正常に動作しているとする。故障検知をされた下位層のサーバの動作状況が動作監視返信待ち状態であるときは、下位層のサーバが故障したと断定する（図 5.2-6）。
6. 下位層のサーバが故障したと断定されると、上位層のサーバでは故障した下位層サーバへ譲渡していた管理権限を、故障したサーバの処理を代替する機能をもつエンティティに譲渡する。また、委任権限を譲渡したあとも故障したと断定した下位層のサーバに対して動作監視パケットを送信しつづけ、ACK があった場合、その下位層のサーバが復帰したと断定する。下位層サーバの復帰が断定されると、別サーバに委任していた管理権限を、復帰した下位層サーバへ譲渡する。

#### 5.4.2 故障したサーバの処理を代替する機能

故障したサーバの処理は、故障したサーバと同一階層に所属するサーバが分担する。上位層サーバではあらかじめ下位層の各サーバの故障時の処理を代替するサーバを決定しておく。そして、下位層のサーバの故障を検知すると、あらかじめ決めておいたサーバに対し、管理権限を譲渡する。同一階層に複数のサーバが存在しない場合は、故障時にのみ動作するバックアップ専用サーバを設置する。

### 5.5 実装

FreeBSD4.10-RELEASE 上で、C 言語により実装を行った。GLI システムは文献 [351] に基づいて実装し、エリアサーバ、HID サーバに動作監視処理を行う関数として send_keep_alive() や transact_keep_alive() などを実装した。また、KEEP_ALIVE パケットを送信するプロトコルには通信時のオーバヘッドを減らすために UDP を使用した。

### 5.6 今後の予定

評価では、堅牢性についての評価、および考察を行い、さらに大規模位置情報管理機構としての実運用環境を想定した評価を行う。

#### 5.6.1 冗長性の評価

冗長性の評価においては、サーバ故障発生時から、検索・登録不能となる時間の性能測定を行う。また、動作監視機能を付加したことによるオーバヘッドの測定を行う。オーバヘッドの測定では、監視する下位層サーバ数と KEEP_ALIVE パケットを送信する間隔を変化させて単位時間における動作監視処理時間の割合を導出したところ、図 5.3 に示す結果が得られた。

#### 5.6.2 実運用を想定した評価

**大規模台数の移動体の位置情報を管理する際の動作パラメータの導出**

GLI システムにおいて各エンティティにおける登録・検索処理時間を測定し、登録・検索にかかる処理時間について考察を行う。さらに、得られた性能

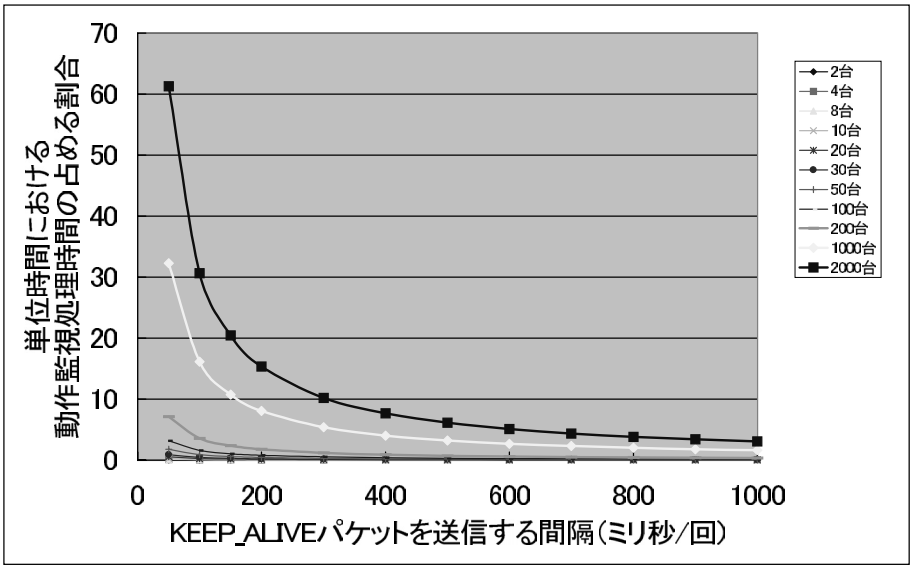


**図 5.3.** 単位時間における動作監視処理時間が占める割合

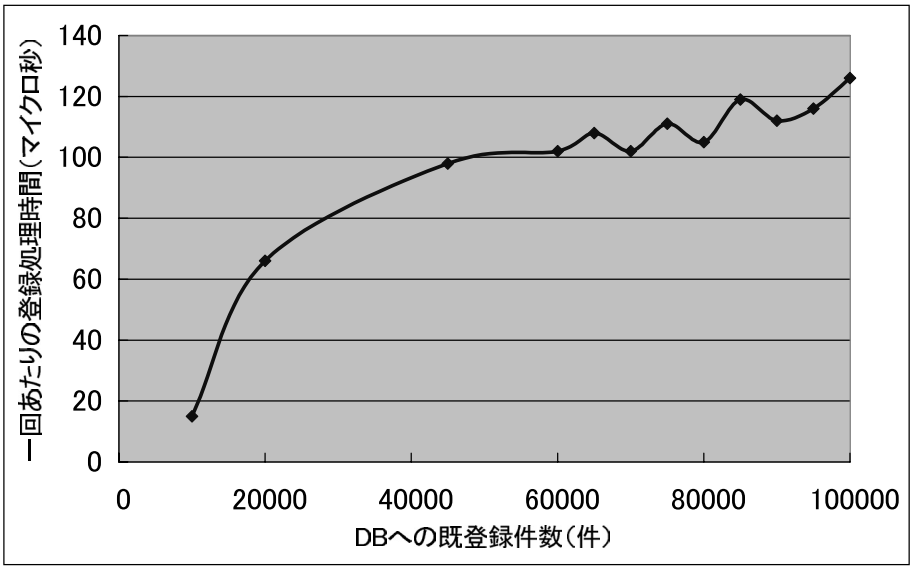


**図 5.4.** HID サーバ・登録サーバのデータベースの登録処理時間

評価から、大規模位置情報管理機構が想定する大規模台数の移動体の位置情報を管理する際のパラメータの導出を行う。パラメータは、登録サーバの台数、HID サーバの台数、エリアサーバの台数、さらに、その時の登録処理時間、検索処理時間を指す。現在、登録サーバと HID サーバにおけるデータベースの登録処理時間として図 5.4 に示す測定値、HID サーバにおける検索処理時間として図 5.5 に示す測定値を得ている。

**実環境における評価**

ITS シミュレータである HAKONIWA を利用して、HAKONIWA の生成した自動車の位置情報を、5.6.2 項で得られたパラメータをもとに分散管理を行い実環境における位置情報管理機構としての有効性を示す。

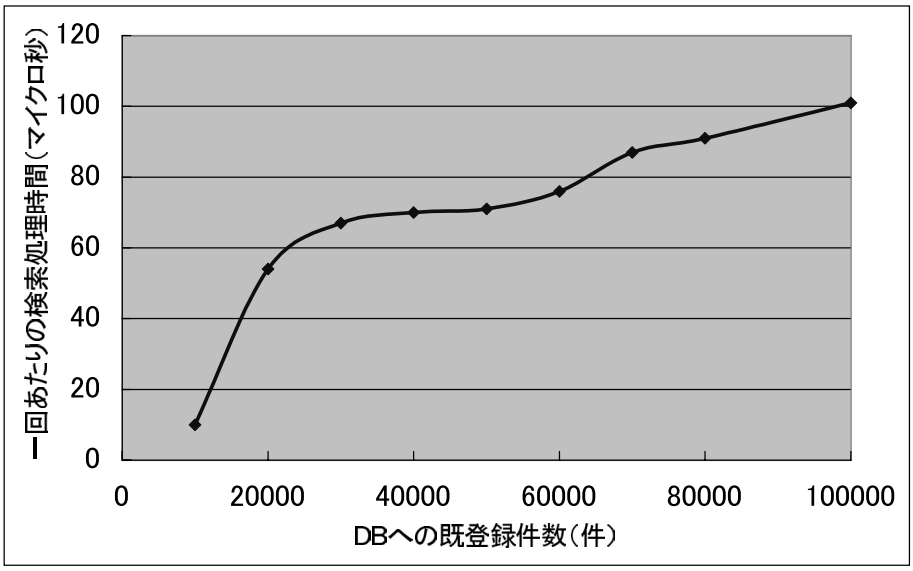


**図 5.5.**　HID サーバにおける検索処理時間