プライバシ保護を考慮した地理位置情報システム

渡辺恭人[†1] 竹内奏吾[†2] 寺岡文男[†2]
植原啓介[†3] 村井純[†4]

プライバシ保護を実現した地理位置情報システム（GLI システム）を提案する．我々が提案している GLI システムは，インターネットに接続している移動体の地理位置情報を地球規模で管理するものである．位置登録者は自分の位置をサーバに登録し，検索者は移動体の識別子を鍵とした位置検索，および地理的領域を鍵とした移動体検索が可能である．GLI システムは地球規模での動作を可能とするため，サーバの階層化による分散管理を導入している．本論文で扱うプライバシ保護とは，第三者による移動体の特定防止，位置特定防止，追跡防止，なりすまし防止およびインターネットにおける盗聴防止，データ改竄防止である．さらにサーバが管理するデータベースの盗難も考慮する．移動体の識別子として HID（hashed ID）を導入することにより，信頼関係のある検索者のみに移動体の特定，位置特定，追跡を可能とし，信頼関係のない検索者には統計情報のみの利用を可能とする．なりすまし防止のため位置登録サーバを導入し，移動体の認証を行う．インターネットにおける盗聴防止および改竄防止には IPsec を利用する．本論文では，プライバシ保護を実現した GLI システムの性能も見積もる．

The Geographical Location Information System with Privacy Protection

Yasuhito Watanabe,[†1] Sohgo Takeuchi,[†2] Fumio Teraoka,[†2]
Keisuke Uehara[†3] and Jun Murai[†4]

We propose the Geographical Location Information (GLI) System with Privacy Proection. The GLI System we propose provides a way to manage geographical location information of mobile entities in the worldwide scale. Mobile entities regiter their location information with servers. Searching clients are able to look up location of mobile entities using specified identifier as a search key and look up identifiers of mobile entities using speified geographical region as a search key. The GLI System has a distributed management method in order to be scaled to the world. In this paper, we introduce HID (Hashed ID) to the GLI System for privacy preservation. The privacy preservation means that a mobile entity must not be identified by unknown persons, the location of a mobile entity must not be realized, and it is impossible to track a mobile entity. We designed the new architecture of GLI System and estimate performance.

1. はじめに

インターネットと携帯端末の急速な普及により，地理的な位置情報を利用して移動するユーザの行動を支援するシステムやアプリケーションサービスが多く開発されている．ユービキタス・コンピューティング[1)]環境では，遍在するコンピュータがユーザの位置を利用してユーザの作業を支援する．たとえば，Active Badge location system[2)]は，個人の身につけた Active Badge によって個人の位置を検出する．Context/Location-Aware Computing[3)]は，このようにして得た位置情報から，属しているホストや人間のグループ，そばにあるアクセス可能な装置などの状況に適応するようなアプリケーションやシステムを提供している．

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では位置情報が大きな役割を果たすにもかかわらず，インターネット上で移動体の位置情報を管理するシステムはなかった．そこで我々は地理位

†1 慶應義塾大学政策・メディア研究科
Graduate School of Media and Governance, Keio University
†2 株式会社ソニーコンピュータサイエンス研究所
Sony Computer Science Laboratories, Inc.
†3 慶應義塾大学 SFC 研究所
SFC Laboratory, Keio University
†4 慶應義塾大学環境情報学部
Faculty of Environmental Information, Keio University

置情報システム（GLI: Geographical Location Information System）を提案した[4),5)]．本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・検索機能の実現している．同時に地球規模で動作するスケーラビリティを実現している．

GLI システムでは，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．

しかし，現在の GLI システムでは，だれでも自由に登録・検索ができるため，以下のようなプライバシに関する問題が発生する．

- 移動体の特定・追跡
- なりすましによる偽の登録
- 登録情報のインターネット上での盗聴・改竄

本論文では，これまでの地理位置情報システムの利点である検索手法を損なうことなく，プライバシ保護を実現した地理位置情報システムを提案する．本論文で目標とするプライバシ保護とは，移動体と信頼関係にある検索者には移動体の識別子や位置情報および付帯情報を公開するが，第三者には個々の移動体の識別を不可能にした統計情報のみを公開することである．その実現のため，HID（Hashed ID）を導入する．これは「移動体の識別子をスクランブルして，アクセスの制御を行う」という提案[6)]に基づいている．同時になりすましや盗聴，改竄も防止する．さらにこのシステムの設計と性能見積りを行う．

便宜上，これまでの GLI システムを旧 GLI システムと呼び，本論文で提案するものを GLI システムと呼ぶ．

2. 地理位置情報システムの概要

図 1 に旧 GLI システムの構成を示す．旧 GLI システムは位置情報および付帯情報を登録する移動体，これらの情報を管理するホームサーバ群とエリアサーバ群，および検索者からなる．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・高度を用いる．付帯情報とは，移動体の移動方向や移動速度などである．

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

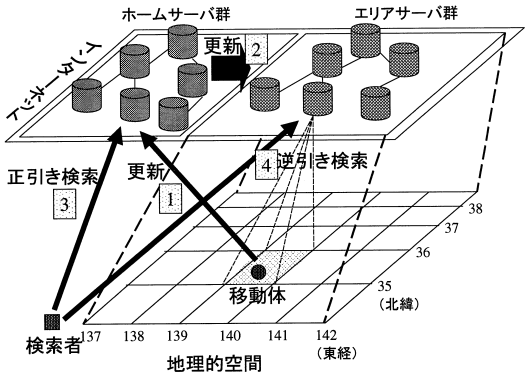

図 1 旧 GLI システムの構成
Fig. 1 Architecture of the old GLI System.

旧 GLI システムは 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検索するものである（正引き検索）．もう 1 つは地理的な領域を鍵とし，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検索するものである（逆引き検索）．図 1 に示すように旧 GLI システムでは，ホームサーバ群は正引き検索を担当し，エリアサーバ群は逆引き検索を担当する．それぞれのサーバ群は階層構造をとっており，分散処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 5) を参照されたい．

図 1 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，たとえば，北緯 35〜36 度，東経 139〜140 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．

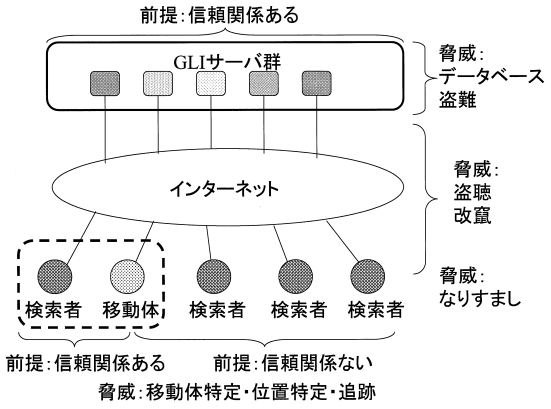

図 2 GLI システムにおける環境と脅威
Fig. 2 Environment and threats in the current GLI System.

3. プライバシ保護の目標

図 2 に GLI システムがおかれる環境とその脅威を示す．GLI サーバ群と移動体および検索者はインターネットを介して通信する．GLI システムでのプライバシ保護を考えるうえで，GLI サーバ群は不正を行わないという前提条件を置く．また，移動体にとって，信頼関係にある検索者と信頼関係のない検索者（第三者）という区別があるものとする．このような前提条件のもと，GLI システムが目標とするプライバシ保護の目標を以下に述べる．

3.1 移動体の特定・追跡の可否

旧 GLI システムにおいては，だれでも自由に登録・検索を行うことができる．したがって，ある移動体の識別子を鍵とする正引き検索によってその位置情報および付帯情報を取得できる．また，ある領域を鍵とする逆引き検索によって得られた結果から，その領域に存在する移動体の特定・追跡が可能である．移動体のプライバシを保護するためには，信頼関係の有無によるアクセスの制御が必要である．正引き検索では，信頼関係にある検索者だけがある移動体を特定し，その識別子を鍵とした検索を行えるようにする．信頼関係のない検索者は移動体の正引き検索を行えないようにする．逆引き検索では，鍵として指定した領域に存在する移動体と信頼関係にある検索者は，検索結果からその移動体の識別子と位置情報および付帯情報を得られるようにする．その移動体と信頼関係にない検索者は移動体を特定できず，位置情報・付帯情報といった統計情報のみを得られるようにする．また信頼関係にない検索者によって追跡が行えないようにする．

3.2 通信データの盗聴・改竄防止

移動体はネットワークを介して GLI サーバに自らの位置情報を登録する．ネットワークを介した通信を行うことで，通信データを盗聴されたり改竄されたりする可能性がある．やりとりされるパケットには移動体の送信元のアドレスが含まれるため，データ部分に含まれる登録情報との対応関係が明らかになる．データ部分を暗号化するなどの方法により，盗聴されても移動体と位置情報との対応関係を明らかにさせないこと，また，通信データが改竄された場合は GLI サーバがその事実を検出できるようにすることを目標とする．

3.3 なりすまし防止

悪意のある移動体が別の移動体になりすまして GLI サーバに偽の位置情報および付帯情報を登録することも考えられる．GLI システムでは GLI サーバが位置情報を登録する移動体を認証し，正しい情報のみを扱うようにする．

3.4 データベース盗難への対処

GLI システムのサーバ群は，それぞれ移動体の情報を登録するデータベースを持つ．そのうち 1 つのデータベースが盗難されても，移動体の特定ができないように工夫する．

4. 解 決 手 法

本章では，前章で掲げたプライバシ保護を実現するための手法について述べる．

4.1 Hashed ID の導入

3.1 節における移動体の特定・追跡の可否を実現するために，本論文では移動体と信頼関係にある検索者間でのみ理解できる情報（以下，符丁と呼ぶ）を移動体の識別子として用いる方式を提案する．移動体は符丁と位置情報・付帯情報を GLI サーバに登録する．正引き検索では，信頼関係にある検索者だけが符丁を鍵として GLI サーバに検索要求を行うことができる．本論文では移動体と移動体と信頼関係にある検索者で秘密鍵を共有し，移動体の真の識別子を鍵付きハッシュ関数に作用させることによって，符丁を生成する方法を提案する．以降符丁を HID（Hashed ID）と呼ぶ．

逆引き検索では，領域を鍵として GLI サーバに検索要求を行い，検索結果としてその領域に存在する移動体の集合が得られる．移動体の集合における検索者と信頼関係にある移動体の特定は，GLI サーバ側で行う方法と検索者側で行う方法がある．前者の方法では GLI サーバが検索者から HID の集合を受け取り検索の結果得られる移動体の HID と比較する．そして GLI サーバが検索結果を返す際，HID が一致したエ

ントリについては HID をつけた位置情報・付帯情報を返し，そうでないものは，位置情報・付帯情報のみを返す．後者の方法では GLI サーバは HID をつけた位置情報・付帯情報を返し，検索者が HID を比較する．前者の方法では信頼関係にない検索者に移動体の HID が公開されない利点があるが，比較する HID の数の増加が GLI サーバの負荷を増加させる欠点を持つ．GLI システムは大規模環境で動作することを目標としているため，サーバのスケーラビリティを重視し，本論文では後者の方法を採用する．

逆引き検索では，HID が第三者である検索者に伝わるため，第三者である検索者は HID を監視し続けることにより，HID から移動体を特定することはできないが，追跡することはできてしまう．追跡を防止するには HID を頻繁に変更する必要がある．HID を変更するごとに移動体と信頼関係にある検索者間で通信を行うとコストが大きくなってしまう．そこで本論文では移動体と信頼関係にある検索者間で時刻同期を前提とし，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する．この結果，真の識別子を ID とすると HID は次の式で表される．

$$\mathrm{HID} = hash(\mathrm{ID} \oplus key(t)) \quad (1)$$

$hash()$ はハッシュ関数を表し，$key(t)$ は時刻の関数，t は時刻を表す．$\oplus$ は結合を意味する．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，これを検索の鍵として使用する．

移動体の識別子として HID を導入することにより，旧 GLI システムにおいて正引き検索の役割を持っていた階層的ホームサーバの代わりに，HID を鍵とした正引き検索を行う階層的 HID サーバを導入する．旧 GLI システムにおいてはホームサーバは FQDN によって階層化を行っていたが，HID の分散管理は HID の値によるサーバの階層化によって行う．また，エリアサーバは，登録される移動体の情報のうち識別子が HID となる（図 4 参照）．

4.2 IPsec の利用

インターネット上での通信における盗聴・改竄防止は，IP Security（IPsec）[10]を利用することで実現できる．IPsec は AH（Authentication Header）[12]と ESP（Encapsulating Security Payload）[11]の 2 つの機能からなる．AH はパケットにハッシュ署名を使用することによって，パケットの改竄防止と送信者認証を実現する．ESP は，暗号を使用して改竄防止と発信者認証と機密性を確保する．GLI システムでは移動体を特定する情報がやりとりされる場合は，ESP を利用して改竄防止と発信者認証と機密性を実現する．それ以外の情報の場合は，AH を利用して改竄防止と発信者認証を実現する．

表 1 各サーバで管理される情報
Table 1 information managed on each server.

サーバ	情報の種類
登録	移動体の IP アドレス・HID サーバの IP アドレスおよび tag・エリアサーバの IP アドレスおよび tag
HID	HID・位置情報・付帯情報
エリア	HID・位置情報・付帯情報

なお，IPsec を利用するためにはノード間において秘密鍵の共有などを事前に行う必要がある．このような関係を Security Association（SA）という．GLI システムにおいてはサーバ間にはあらかじめ SA を確立しておくものとする．

4.3 登録サーバの導入

移動体が登録を行う際にはなりすまし防止のため GLI サーバはその移動体を認証する必要がある．前述のように IPsec はノード認証の機能を持つので，GLI システムは IPsec を用いて移動体の認証を実現する．しかし，移動体と HID サーバ群の関係や，移動体とエリアサーバ群との関係は，移動体の HID と位置情報によって固定されず刻々と変化するので，移動体が登録を行うたびに HID サーバおよびエリアサーバと SA を確立しなければならない可能性があり，オーバヘッドとなる．そのため，登録サーバ群を導入し，登録サーバが移動体を認証するようにする．移動体を 1 つの登録サーバに関連づけることにより，移動体と登録サーバ間にあらかじめ固定的な SA を確立することが可能となる．

4.4 データベースの分割

本論文で提案する GLI システムは，HID サーバ群・エリアサーバ群・登録サーバ群の 3 つのサーバと移動体により構成される．各サーバで管理される情報を**表 1** に示す．詳細は 5.3 節で述べる．

このように，データベースを分割することにより，各サーバに特定情報は存在しない．したがって，各サーバのうちどれか 1 つが盗難にあった場合に，盗まれた登録情報から移動体を特定することは不可能であり，実用上問題は少ない．

5. GLI システムの設計

本章では，前章で述べた解決手法を導入した GLI システムの設計について述べる．

5.1 HID の生成

4.1 節で示した HID 生成式 (1) における鍵 $key(t)$

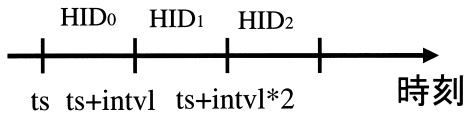

図 3 HID 生成の時間変化
Fig. 3 Process for generating Hashed Identifier.

は時刻情報とともに変化する．登録と検索において同一の HID を移動体と信頼関係にある検索者間で共有するため，$key(t)$ をある時間間隔で変化させるようにする．本論文では $key(t)$ を以下のように定義する．

$$key(t) = ts + intvl * n \quad (2)$$

ts は基準時刻，$intvl$ は HID 変更の時間間隔，n は 0 以上の整数である．ここで $ts + intvl * n \leq t < ts + intvl * (n + 1)$ とする．真の識別子を ID とすると HID は次の式で表される．

$$\mathrm{HID} = hash(\mathrm{ID} \oplus (ts + intvl * n)) \quad (3)$$

n の値は現在時刻から計算でき，$ts + intvl * n <$ 現在時刻 $< ts + intvl * (n + 1)$ のような関係となる．この式から求められる HID の値が時刻によって変化する過程を**図 3** に示す．時刻 ts 時に，移動体は $\mathrm{HID}_0 = hash(\mathrm{ID} \oplus ts)$ と位置情報などをサーバに送信する．$ts + intvl \leq$ 時刻 $< ts + 2 * intvl$ では，$\mathrm{HID}_1 = hash(\mathrm{ID} + ts + intvl)$ となる．

しかし，ID と ts および $intvl$ が何らかの理由によって第三者に洩れた場合，第三者は時間とともに変化する HID の生成が可能となってしまう．したがってさらに $intvl$ より大きい一定間隔（INTVL）で信頼関係にある移動体と検索者間で ID と ts および $intvl$ を交換し鍵を変更することにより，より安全性が保たれる．

5.2 HID 生成のハッシュ関数

HID の生成に用いる一方向性ハッシュ関数としては，鍵付きハッシュ関数（HMAC: Keyed Hashing for Message Authentication Code）[8]が適当である．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）[7]が適当である．SHA-1 は異なる入力値から同一の出力値を生成する可能性がほとんどなく，出力値に偏りもないハッシュ関数で，MD4 や MD5 に比べて一意性の点で優れている．したがって，HID の生成には，HMAC-SHA1 [8),9)]を使用する．

HMAC-SHA1 は，入力値として任意の文字列と 160 bit の鍵により，160 bit の値を出力する．本論文では，入力値に ID，鍵には ts（32 bit）と $intvl$（32 bit）に加えて，予測不可能な値として残りの 96 bit は乱数を使用する．ID は真の識別子であり，形式が自由な任意の文字列とする．

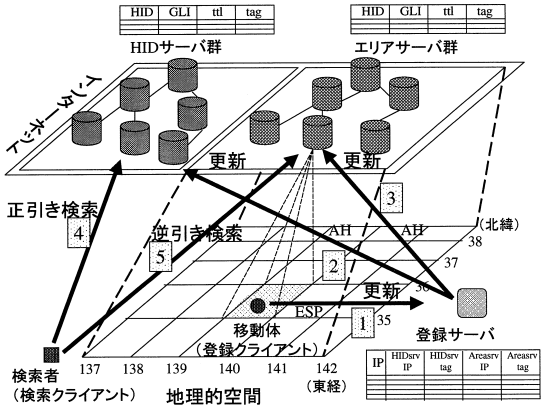

図 4 プライバシ保護を考慮した GLI システム構成
Fig. 4 Basic architecture of the GLI System with privacy protection.

5.3 構　　成

本提案システムの構成を**図 4** に示す．本システムは，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，GPS などの位置取得装置から位置情報を取得し，その時刻における HID を生成する．HID と位置情報・付帯情報および有効期限 ttl をあらかじめ関連づけられた登録サーバへと送信する（図 4 (1)）．

登録サーバは，登録を受け付ける登録クライアントを認証し，あらかじめ関連づけられた登録クライアント以外からの登録は受け付けない．登録クライアントから登録サーバへの通信は移動体を特定する情報を含むため，ESP を使用し盗聴・改竄を防止する．同時に，登録サーバは ESP によって登録クライアントを認証する．登録サーバは，受け付けた位置情報および付帯情報を蓄積せず，HID の値によって決定される HID サーバ，および位置情報の値に従って決定されるエリアサーバに，HID，位置情報・付帯情報，有効期限を送信する（図 4 (2)，(3)）．HID サーバおよびエリアサーバは登録されたエントリをそれぞれのデータベース内で一意に示す情報である tag を登録サーバに返す．登録サーバと HID サーバおよびエリアサーバの通信は，移動体を特定する情報を含まないので，AH を使用して改竄のみを防止する．

各サーバで管理される情報を表 1 に示す．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 の値によって決定される HID サーバの IP アドレス，位置情報の値によって決定される

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，位置情報・付帯情報，有効期限を受信して蓄積する．また，HID サーバは，検索クライアントから HID を鍵とした移動体の検索である正引き検索を受け持つ（図 4 (4)）．エリアサーバは，そのエリアサーバが管理している位置領域に存在する移動体の HID，位置情報・付帯情報，有効期限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である逆引き検索を受け持つ（図 4 (5)）．

5.4 登録・更新

登録クライアントが行う登録と更新における通信と各サーバの動作の手順を述べる．登録クライアントが行う更新の通信と各サーバの動作の手順について，HID サーバは HS-old と HS-new，エリアサーバは AS-old と AS-new が存在するものとする．

登録クライアントは HID，位置情報・付帯情報，有効期限を登録サーバに送信する際に認証される（**図 5** (1)）．登録サーバは，データベースを見て，登録クライアントのエントリがあれば，そのエントリが示す HID サーバ（HS-old）およびエリアサーバ（AS-old）へエントリを削除要求を送信する（図 5 (2)，(3)）．その後，登録サーバは受信した HID より HID サーバ（HS-new）を決定し，位置情報によりエリアサーバ（AS-new）を決定し，HID，位置情報・付帯情報，有効期限の登録要求をそれぞれに送信する．HID サーバおよびエリアサーバはデータベースに受信した情報を登録し，登録したエントリを示す tag を登録サーバへ送信する．登録サーバは HID サーバ，エリアサーバから tag を受信し，データベース中の登録クライアントのエントリを更新する（図 5 (4)，(5)）．削除と登録処理において，両者が同一のサーバに対して行われる場合は，1 回の送信で行う．登録サーバは登録完了を登録クライアントに通知する（図 5 (6)）．

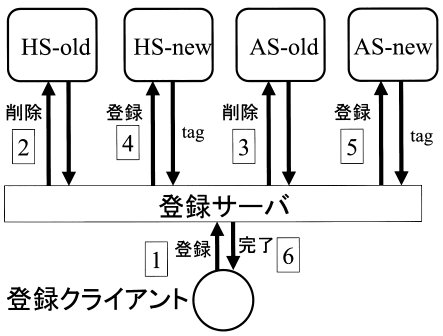

図 5 登録・更新
Fig. 5 Update process.

5.5 正引き検索

正引き検索は，検索したい移動体と信頼関係にあり HID 生成に必要な情報を共有している特定可能検索クライアントのみが行える．正引き検索は次のような手順で行われる．検索クライアントは登録クライアントのその時点での HID を生成する．検索クライアントは HID により HID サーバを決定し，検索要求する．HID サーバは受信した HID に対応するエントリを検索し，HID と位置情報・付帯情報を返信する（図 4 (4)）．

5.6 逆引き検索

検索クライアントは検索したい位置領域からエリアサーバを決定し，領域情報を送信し検索要求を行う．エリアサーバは受信した領域に対応するエントリを検索し，HID と位置情報・付帯情報のリストを返信する（図 4 (5)）．

検索クライアントは，信頼関係にある移動体群の HID を生成し，検索結果の HID と比較することで信頼関係にある移動体を特定できる．生成した HID と一致する移動体が存在しない場合は，位置と個数など統計情報のみ取得できる．

6. 考　　察

6.1 時刻同期の妥当性

時刻同期の手法としては，ネットワーク経由で時刻同期を行う NTP [13]がある．NTP を使用してインターネット上で時刻を伝送する場合の誤差は 20 ミリ秒程度であり，ネットワークの混雑により増加する可能性はあるが，現状の時刻同期手法としては最も有用である．式 (3) における intvl の値は 1 分から 5 分程度の時間を想定しており，NTP の誤差と比較して大きい値である．したがって誤差によって HID を同期できない可能性は低い．

6.2 移動体の追跡

登録クライアントが長い期間同じ位置に停止していると，時間の経過とともに位置は変化しないが HID は変化する．このような場合，HID が変化しても変化の前後に注目していればどの登録クライアントがどの HID なのかを区別することはできる．また類似した状況として，あるエリアサーバが管理する位置領域に 1 つの登録クライアントだけが存在する場合，移動していてもその登録クライアントの HID を区別できる．HID を正引き検索することによって追跡が可能になってしまう．どちらの場合も HID の有効期限内でのみ可能である．

6.3 HIDの衝突

HIDはHMAC-SHA1という鍵付きハッシュ関数を利用して生成する．HMAC-SHA1による出力値の衝突可能性は，使用されるハッシュ関数SHA-1の衝突可能性に依存する．文献7)によると，SHA1は異なる入力値に対して同一のハッシュ値を返す可能性は実用上問題ないほど低い．登録しようとしているHIDがすでに使用されている場合はエラーとして登録クライアントに通知し，識別子や鍵を変更して再度登録を試みる．

6.4 パケット盗聴

登録サーバの近傍において登録クライアントから登録サーバへの通信と，登録サーバからHIDサーバおよびエリアサーバへの通信が同時に盗聴された場合を考える．登録クライアントから登録サーバへの通信はESPにより暗号化されるが登録クライアントのIPアドレスは明らかになる．登録サーバからHIDサーバおよびエリアサーバへの通信はAHを使用するため，パケットの内容（HID，位置情報・付帯情報，有効期限）は明らかになる．したがって，登録クライアントのIPアドレスとHIDは対応づけられる可能性がある．実際は登録サーバの近傍において，このような盗聴は困難であると思われるので，実用上問題は少ない．

6.5 未対応事項および対象外事項

3章で述べたような前提が破られる場合の攻撃について述べる．たとえば，本システムが攻撃されて特権ユーザ権限まで盗まれてしまった場合に関しては対象外である．

データベースの盗難に関しては，登録サーバを含む2つのデータベースが盗まれた場合はその対応づけから移動体を特定することはできるが，これに関しては未対応である．ある登録クライアントと信頼関係にある検索クライアントが登録クライアントになりすまして偽のHIDを登録することは可能である．これに関しても未対応である．

第三者がある移動体のHID変更の前後に注目し，近傍に存在する他の移動体が少数である場合，移動体を特定することはできないが，HIDの変化を追跡できる可能性はある．これに関しても対象外である．

7. 性能評価

旧GLIシステムにプライバシ保護の機能を導入することにより増加すると思われるオーバヘッドを測定し，実装後の性能を見積もる．オーバヘッドは，登録クライアントにおけるHID生成，登録クライアントと登録サーバ間でのESPによる認証・暗号化・復号化の処理，および登録サーバとHIDサーバ間，登録サーバとエリアサーバ間のAHによる改竄チェック処理がある．ここでは，この3つについて実装後に増加するオーバヘッドとして見積もる．測定は，文献5)と条件をほぼ同じとするため，Intel社製MMX Pentium（233 Mhz）CPU搭載のIBM PC互換機を使用して行った．

7.1 HID生成

HMAC-SHA1という鍵付きハッシュ関数は，Open SSLパッケージに含まれるライブラリ関数を利用した．サンプルプログラムを作成しその関数の前後において計測を行った．HMAC-SHA1の入力値としては，鍵は20 byteのランダムな文字列，IDもランダムな文字列とした．以上の入力値からIDの長さを16 byte，64 byte，128 byte，256 byte，512 byte，1024 byteと変化させ，それぞれ100000回繰り返して測定した．その平均値を，**表2**に示す．単位はマイクロ秒である．

7.2 ESPの処理

実験では，実際の登録情報サイズと同じ 48 byte（HID20 byte，位置情報24 byte，ttl 4 byte）のデータを持つUDPのパケットをESPを使用して50回送受信した．暗号化・復号化のための鍵は両者であらかじめ交換してあるものとする．それぞれの処理時間の平均値を，**表3**に示す．単位はマイクロ秒である．

7.3 AHの処理

AHはパケット全体に対してハッシュ署名を作成する．ハッシュ署名にはHID作成と同様にHMAC-SHA1を使用するため，処理時間の測定は表2の結果と同一になる．

7.4 登録・検索の性能見積り

旧GLIシステムにおけるホームサーバへの位置登

表2 HID生成に要する時間（マイクロ秒）
Table 2 time for generating HID.

IDの長さ（byte）	平均（マイクロ秒）
16	30.053
64	33.483
128	36.953
256	44.363
512	58.441
1024	87.421

表3 ESPにおける暗号化および復号化の処理時間（マイクロ秒）
Table 3 time for encrypting and decrypting of ESP in the IPsec.

処理	平均
暗号化	1471.9
復号化	1461.2

表 4 登録完了時間の見積り（マイクロ秒）
Table 4 estimation of time for registering data to servers.

処理区間	処理内容	時間
登録クライアント・登録サーバ	登録	540.5
登録クライアント・登録サーバ	HID+暗号化 +復号化	2963.2
登録サーバ・HID サーバ	登録	540.5
登録サーバ・HID サーバ	AH 処理*2	73.9
登録サーバ・エリアサーバ	登録	361.0
登録サーバ・エリアサーバ	AH 処理*2	73.9
合計		4553.0

表 5 検索時間の見積り（マイクロ秒）
Table 5 estimation of time for registering data to servers.

検索種類	処理内容	時間
正引き	旧 GLI 正引き検索	392.1
	HID 生成	30.1
	計	422.2
逆引き	旧 GLI 逆引き検索	333.3
	本提案方式追加	0
	計	333.3

録の性能は，1850 リクエスト/秒であるので 1 リクエストあたり 540.5 マイクロ秒要する．エリアサーバへの位置登録の性能は，2770 リクエスト/秒であるので，1 リクエストあたり 361 マイクロ秒要する．旧 GLI システムにおける処理時間をもとに GLI システムの登録処理時間を見積もる．AH には HMAC-SHA1 を使用し，処理時間はパケットのデータ部が 108 byte（IP: 20 byte，AH: 32 byte，UDP: 8 byte，HID・位置情報・付帯情報・有効期限：48 byte）であるため，表 2 から近似値として 128 byte の値を使用する．HID 生成には ID の長さ 16 byte のものを使用する．登録に関する各処理区間における追加処理内容から処理時間を見積もり，**表 4** に示す．

同様に検索に関しても見積りを行う．旧 GLI システムにおける検索の性能は，正引き検索が 2550 リクエスト/秒，逆引き検索が 3000 リクエスト/秒である．それぞれの 1 リクエストあたりの処理時間は，392.1 マイクロ秒，333.3 マイクロ秒となる．本論文の提案方式では正引き検索には，HID を生成する時間が追加されるが，逆引きに追加される処理はない．見積もった処理時間を**表 5** に示す．

8. 結　　論

本論文では，移動体のプライバシ保護機能を付加した GLI システムを提案した．本提案方式では，移動体の識別子と位置情報・付帯情報のうち，識別子をハッシュ関数に入力させることで得られた値を HID（Hashed ID）として利用する．これにより移動体の信頼関係にない検索者からの特定を防止した．また，ハッシュ関数の入力値として時間変化する鍵を信頼関係のある検索者と共有することにより，信頼関係のある検索者には特定を許し，時間とともに変化するため追跡の可能性を減少させることができた．また，データベースを分割することにより盗難による移動体の特定を防止した．また，付加される機能の性能評価を行い，増加するオーバヘッドの見積りを行った．

今後はこの設計を基にした実装を行い，実験運用を行う．さらに，グループでの HID 生成情報共有，鍵の変更と配送などに関する検討を行う予定である．

謝辞 本研究の契機となるアイデアを提供していただいた奈良先端科学技術大学院大学助教授の砂原秀樹博士，および和泉順子氏に感謝いたします．また，本研究において貴重なご助言・ご協力をいただいた WIDE プロジェクト，rover ワーキンググループ，慶應義塾大学環境情報学部徳田・村井・楠本・中村研究室，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いたします．

参 考 文 献

1) Weiser, M.: Some Computer Science Problems in Ubiquitous Computing, *Comm. ACM* (July 1993).
2) Want, R., Hopper, A., Falcao, V. and Gibbons, J.: The Active Badge Location System, *ACM Trans. Information Systems*, Vol.10, NO.1, pp.91–102 (Jan. 1992).
3) Schilit, B.N., Adams, N.I. and Want, R.: Context-Aware Computing Applications, *Proc. Workshop on Mobile Computing Systems and Applications*, Santa Cruz, CA, pp.85–90, IEEE Computer Society (Dec. 1994).
4) Watanabe, Y., Shionozaki, A., Teraoka, F. and Murai, J.: The design and implementation of the geographical location information system, *Proc. INET '96*, Internet Society (June 1996).
5) Takeuchi, S., Watanabe, Y. and Teraoka, F.: The GLI System: A Global System Managing Geographical Location Information of Mobile Entities, *Proc. WPMC '00* (Nov. 2000).
6) Izumi, M., Takeuchi, S., Watanabe, Y., Uehara, K., Sunahara, H. and Murai, J.: A Proposal on a Privacy Control Method for Geographical Location Information Systems, *Proc. INET '00*, Internet Society (June 2000).
7) National Institute of Standards and Technology (NIST), FIPS PUB 180-1: Secure Hash Standard (Apr. 1995).

8) Krawczyk, H., Bellare, M. and R. Canetti: HMAC: Keyed-Hashing for Message Authentication, RFC 2104 (Feb. 1997).
9) Cheng, P. and Glenn, R.: Test Cases for HMAC-MD5 and HMAC-SHA-1, RFC 2202 (Sep. 1997).
10) Kent, S. and Atkinson, R.: Security Architecture for the Internet Protocol, RFC 2401 (Nov. 1998).
11) Kent, S. and Atkinson, R.: IP Encapsulating Security Payload, RFC 2406 (Nov. 1998).
12) Kent, S. and Atkinson, R.: IP Authentication Header, RFC 2402 (Nov. 1998).
13) Mills, D.L.: Network Time Protocol, RFC 958 (Sep. 1985).

(平成 12 年 5 月 22 日受付)
(平成 12 年 10 月 6 日採録)

渡辺　恭人（学生会員）

1970 年生．1996 年慶應義塾大学政策・メディア研究科修士課程修了．同大学環境情報研究所訪問所員を経て，同大学政策・メディア研究科後期博士課程在学中．修士（政策・メディア）．現在，コンピュータネットワークトラフィック解析，インターネットにおける地理位置情報に関する研究に従事．ACM 会員．

竹内　奏吾（正会員）

1973 年生．1999 年電気通信大学大学院情報システム学研究科情報システム設計学専攻博士前期課程修了．同年（株）ソニーコンピュータサイエンス研究所入社．インターネット運用管理，モバイルコンピューティングに興味を持つ．

寺岡　文男（正会員）

1959 年生．1984 年慶應義塾大学大学院修士課程修了．同年キヤノン（株）入社．1988 年（株）ソニーコンピュータサイエンス研究所入社．現在，同社シニアリサーチャ．工学博士．1991 年日本ソフトウェア科学会高橋奨励賞受賞．1993 年元岡記念賞受賞．コンピュータネットワーク，オペレーティングシステム，分散システム等の研究に従事．特に移動透過性を提供するプロトコル VIP（Virtual IP）の開発を通して IETF の Mobile IP 分科会の活動に貢献．2000 年より本学会理事．著書に「ワイヤレス LAN アーキテクチャ」（共著，共立出版）．監訳に「詳解 Mobile IP」（共監訳，プレンティスホール出版）．ACM，IEEE，日本ソフトウェア科学会各会員．

植原　啓介（正会員）

1970 年生．1995 年電気通信大学大学院電気通信学研究科情報工学専攻博士前期課程修了．慶應義塾大学環境情報研究所研究員，慶應義塾大学環境情報学部助手，慶應義塾大学大学院政策・メディア研究科後期博士課程を経て，現職，慶應義塾大学環境情報研究所研究員に至る．移動通信プロトコル，移動計算機環境等の研究に従事．修士（工学）．ACM，IEEE 各会員．

村井　　純（正会員）

現職：慶應義塾大学環境情報学部教授．1955 年生．1984 年慶應義塾大学工学部数理工学博士課程修了．1987 年博士号取得．1984 年東京工業大学総合情報処理センター助手，1987 年東京大学大型計算機センター助手．1990 年慶應義塾大学環境情報学部助教授を経て 1997 年より現職．1999 年慶應義塾大学 SFC 研究所所長．1984 年 JUNET を設立．1988 年 WIDE プロジェクトを設立し，今日までその代表として指導にあたる．社団法人日本ネットワークインフォメーションセンター理事長．インターネットソサエティ（ISOC）理事．ICANN 暫定ボード．著書に「インターネット」，「インターネット II」（岩波新書），監訳に「インターネットシステムハンドブック」（インプレス），「IPv6：次世代インターネットプロトコル」（プレンティスホール）等がある．