実運用を想定した大規模位置情報管理機構の構築

慶応義塾大学大学院
寺岡研究室 修士 2 年
栗栖 俊治*

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他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様々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、交通情報等を移動体へ提供するサービス等が上げられる．

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．

2 大規模位置情報管理機構

本章では，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．

*chris@tera.ics.keio.ac.jp

2.1 位置情報管理機構の定義と要求事項

2.1.1 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のメッセージ配信。

2.1.2 位置情報管理機構への要求事項

本節では，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 [5] 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 TaskForce)[1] の geoprivWG(Geographic Location/Privacy)[2] 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 [4] 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、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。この機能は、位置情報を測位する技術にも依存するが、位置情報管理機構としては、位置情報管理機構の管理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

2.1.1 節であげられた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、より実用的な仕組みとなり、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。

2.2 大規模位置情報管理機構

2.2.1 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様々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様々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。

2.2.2 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、2.1.2 節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。

2.2.3 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、2.1.2 節と 2.2.2 節で定義され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，登録頻度は膨大なものとなる。例えば，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．

2.1.2 節より，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．

2.3 既存の位置情報管理機構

2.3.1 Architecture of a Large-scale Location Service

Architecture of a Large-scale Location Service[3] 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，領域による検索の二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しする物体ならば，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．

2.3.2 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て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．

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．

3　先行研究:GLI システム

本章では、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 [13],[12] について述べ、2.2.2 節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。

3.1　GLI システムの概要

以下に，2.1.2 節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)[6] 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を行う管理対象の認証を行う登録サーバと呼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 サーバと呼ばれるサーバ群と AREA サーバと呼ばれるサーバ群の 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，AREA 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 [9] 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 1 にまとめる．

表 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

3.2 実運用化にむけた GLI システムの問題点

3.2.1 冗長性の欠如

2.2.3 節で，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が述べられている．3.1 節より，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．

3.2.2 HID サーバ/AREA サーバにおける故障の考察

GLI システムでは，図 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の HID サーバや AREA 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 AREA 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

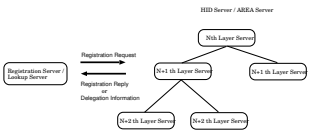

図 1: GLI システムにおける登録・検索時の動作概要

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他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・AREA 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．

4 設計

4.1 サーバの故障を検知する機能

図 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・AREA 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 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 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 2-1) に関しては、動作監視返信待ち状態と認識する (図 2-3)。

4. 登録サーバ・検索サーバにおいても、HID サーバ・AREA サーバの動作監視を行う (図 2-4)。登録要求や検索要求に ACK を返さない HID サーバと AREA サーバを発見すると、その HID サーバや AREA 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 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 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の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後も故障した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。

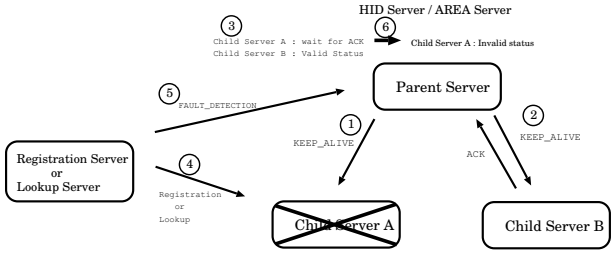

図 2: GLI システムにおける登録・検索時の動作概要

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 実装

FreeBSD 4.10 Release 上で，C 言語により実装を行った．GLI システムは文献 [10] に基づいて実装し、AREA 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() 等を実装した．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．

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．

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 3 に示す結果が得られた．

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 システムにおける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おこなう．さらに，得られた性能評価から，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さい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，AREA サーバの台数，さらに，その時の登

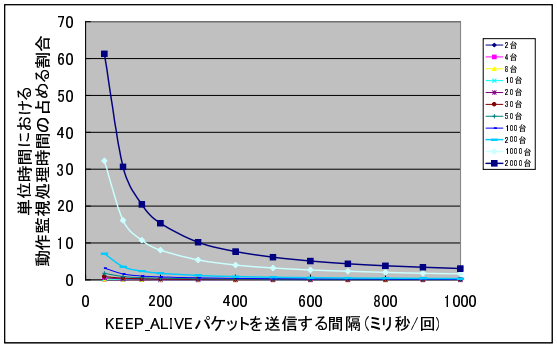

図 3: 単位時間における動作監視処理時間が占める割合

録処理時間，検索処理時間をさす．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 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 に示す測定値を得ている．

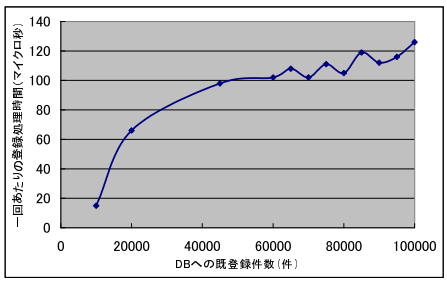

図 4: HID サーバ・登録サーバのデータベースの登録処理時間

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，6.2 節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．

参考文献

[1] http://www.ietf.org.

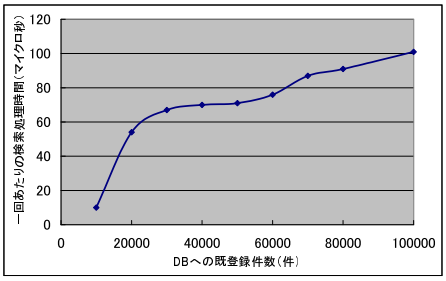

図 5: HID サーバにおける検索処理時間

[2] http://www.ietf.org/html.charters/geopriv-charter.html.

[3] Leonhardi Alexander and Rothermel Kurt. Architecture of a large-scale location service. *Proceedings of the 22nd Internal Conference on Distributed Computing*, 2002.

[4] J.Cuellar, J.Morris, D.Mulligan, J.Peterson, and J.Polk. Geopriv requirements. *RFC3693*, February 2004.

[5] Eija Kaasinen. User needs for location-aware mobile services. *Personal and Ubiquitous Computing*, Vol. 7, No. 1, May 2003.

[6] S. Kent and R.Atkinson. Security architecture for the internet protocol. *RFC2401*, November 1998.

[7] H Krawczyk, M Bellare, and R.Canetti. Hmac:keyed-hashing for message authentication. *RFC2104*, February 1997.

[8] P.Cheng and R.Glen. Test cases for hmac-md5 and hmac-sha-1. *RFC2202*, September 1997.

[9] 栗栖俊治. インターネットを利用した移動体の位置情報管理機構の構築, February 2003.

[10] 栗栖俊治. Gli システム仕様書, June 2003.

[11] 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.

[12] 渡辺恭人, 竹内奏吾, 栗栖俊治, 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の実装と評価. 電子情報通信学会論文誌, No. 8, pp. 1434–1444, August 2003.

[13] 渡辺恭人, 竹内奏吾, 寺岡文男, 植原啓介, 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. 情報処理学会論文誌, Vol. 42, No. 2, pp. 234–242, February 2001.