位置情報管理システムにおける信頼性による通信型の切り替え方式の提案

森 勇海† 白石 陽†† 高橋 修††

位置情報を利用したサービスが増加する傾向にあり，それらの位置情報サービスは個別に位置情報を管理している．これらの位置情報を共有することで位置情報サービスと位置情報サービス利用者の双方で有益となる．しかし，情報共有を行う上で位置情報サービス利用者の位置プライバシーの保護が問題となる．そこで，位置情報サービス利用者のプライバシー保護とサービスを行う時間を現状と変わらなくするために 2 つの通信型を利用した位置情報管理システムを提案した．この 2 つの通信型を選択する際に位置情報サービスの信頼度により利用する方式を提案する．位置情報サービスの信頼度は位置情報管理システムと位置情報サービス利用者が判断し，それぞれが判断した信頼度を証拠理論を利用して信頼度の集約を行う．

Choice Principle of Communication types by Trust for Location Management System

YUUMI MORI† YOH SHIRAISHI††
OSAMU TAKAHASHI††

Location based services tend to increase, and those location based services manage the location information individually. It becomes useful in a location information service and the both sides of the location based service user by sharing these location information. However, protection of the location privacy of the location based service user becomes the problem when share location information. Therefore We suggest the location information management system that used two communication types. We do not change with the present conditions, and to do privacy protection of the location information service user and time giving a service. We suggest a method to choose by the reliability of the location information service when we choose these two communication types. Location information management system and a location based service user judge the reliability of the location based service and we use an evidence theory with the reliability that each judged and gather the reliability.

†公立はこだて未来大学大学院
Graduate School of Future University Hakodate
††公立はこだて未来大学
Future University Hakodate

1. はじめに

GPS 機能付き携帯電話や RFID タグなどの技術発展により位置情報の取得が容易になっている．それに伴い位置情報を利用したサービス（LBS : Location Based Service）が増加する傾向にある．現在運用されている LBS は個別に位置情報を管理しており，それらの位置情報を共有することにより LBS と LBS 利用者（位置情報提供者）にとって様々な利点がある．図 1 に具体例を示す．

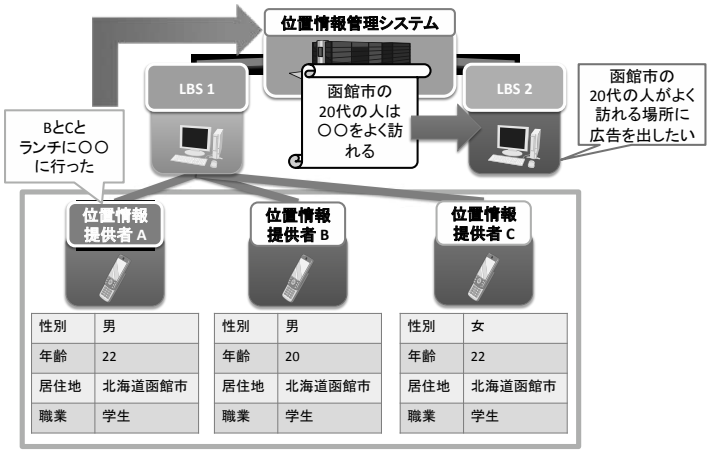

図 1 位置情報の有効活用例

図 1 では，ある地域の 20 代がよく訪れる場所に対して広告を送信したいと考える LBS とその地域の 20 代がよく訪れる場所の情報を持っている SNS 型の LBS が存在したとき，それぞれの情報を共有することができれば広告効果が向上する．そこで現状よりも位置情報をさらに有効活用するために情報共有が必要になる．しかし，情報共有を行うことで LBS による位置情報の不正利用の問題や位置情報提供者のプライバシー保護が問題となる．そこで本稿では位置情報提供者の位置情報と付属する個人情報の管理を行う位置情報管理システムに着目する．位置情報管理システムに関する既存研究[1,2,3]は存在するが，複数 LBS の位置情報を管理する目的でない，もしくは位置情報提供者のプライバシー保護が十分でないといった問題がある．そこで，著者らは位置情報提供者の制御ポリシを利用した位置情報・個人情報の管理・公開制御を行う位置情報管理システムを提案した[4]．提案システムでは位置情報提供者のプライバシー保護と応答時間（LBS が位置情報提供者から情報の要求を受けてからサービスを提供するまでにかかる時間）を現状の LBS と同程度にする必要がある．そのために直

接通信型，経由通信型という 2 つの通信型を導入する．直接通信型は位置情報提供者のプライバシー保護を可能とする．経由通信型は直接通信型に比べて応答時間を短縮する通信型である．この 2 つの通信型の利点と欠点を以下の表 1 にまとめた．

表 1 通信型の比較

	利点	欠点
直接通信型	位置情報提供者のプライバシー保護	応答時間の増大
経由通信型	応答時間の短縮	位置情報提供者のプライバシー侵害の可能性

一般に位置情報提供者は応答時間が速くプライバシー保護の可能な通信型を利用してもらいたいと考えるがそれらを同時に行うことはできない．なぜなら，LBS が位置情報提供者の情報を不正利用することが考えられるためである．そこで，LBS が情報の不正利用しない度合を LBS の信頼度として定義し, LBS が 2 つの通信型のどちらを利用するかを決定するために信頼度を利用する方式を提案する．

2. 要求条件

提案する位置情報管理システムでは複数の LBS が管理していた位置情報を管理できるように対応し，位置情報提供者のプライバシーを保護できるものでなければならない．高橋ら[5]が挙げた位置情報を取り扱う上でのプライバシー保護要件を参考に本稿で必要となるプライバシー保護要件を定める．以下に示す位置情報の不正利用問題を防ぐことを本稿でのプライバシー保護要件とする．

(1) 個人の位置情報を集約した位置情報管理システムから情報が公開あるいは漏洩されてしまう場合
(2) 特定の人にしか使用許可していない位置情報が，無意識または故意に，使用許可した人以外に漏れてしまう場合
(3) 不特定多数（個人を特定しない）の位置情報に個人特定情報が付加されて公開されてしまう場合
(4) 悪意のある第三者が，位置情報を取得し，公開する場合

(1)の問題は，システム自体のセキュリティに関わる問題なので本研究では対象外とする．また，(2)，(4)の問題は位置情報提供者の場合と LBS の場合がある．本研究では LBS の場合を対象とする．

本研究では悪意のある行動をする LBS を MLBS(Malicious Location Based Service)とする．MLBS は次に該当するものと定義する．

- 利己的な行動
  - 位置情報の取得のみを繰り返す.
- 位置情報の不正利用

位置情報の不正利用問題に対処するとともに，現状の LBS と同じ応答時間（LBS が利用者から情報の要求を受けてからサービスを提供するまでにかかる時間）でサービスを提供することも必要である．

3. 関連研究

3.1 位置情報管理システム

位置情報管理システムの関連研究として，GLI システム[1]，ULP[2]や，Yahoo の FireEagle[3]がある．

3.1.1 GLI(Geographical Location Information)システム

渡辺ら[1]が提案・実装した GLI システムは物理的空間を移動する移動体の地理的位置情報をインターネット上で管理するシステムである．GLI システムは位置情報を登録する登録サーバとエリアサーバ（位置情報を緯度経度の度・分・秒による階層構造によって階層化した複数のサーバ群）によって位置情報を管理する．また，位置情報をパブリック（第三者への情報提供を容認）とプライベート（許可したもの以外への情報提供を拒否）の識別子をつけて管理することで，位置情報提供者のプライバシーを保護している．加えて，HID(Hashed ID)と呼ばれる擬似 ID を利用したアクセス制御機構により，盗聴・改竄・なりすましなどのセキュリティの脅威に対応している．

3.1.2 ULP(Universal Location Platform):汎用的位置情報基盤

原ら[2]が提案・実装した ULP はインターネット上で汎用的に位置情報を取り扱う機構である. ULP は位置情報取得･管理機能を持つ LMS(Location Management System), 空間参照変換機能を持つ LTS(Location Transform System), これらの機能を利用した位置情報提供機能を持つ LIS(Location Information System)から構成され，それぞれの機能ごとに分散化することで規模拡張性（スケーラビリティ）を確保している．多様な位置情報測位デバイスに対応し，さらに空間参照系変換機能により指定した位置の表現形式で対応することかできる．また，位置情報の公開，解像度変更の条件を規定したプライバシールールを用いることで位置情報提供者のプライバシーを保護している．さらに, CA(Certificate Authority)によって配布される証明書を利用して認証を行うことでなりすましを防止している．

3.1.3 Fire Eagle

Fire Eagle[3]は Yahoo が運営しているサービスプラットフォームで，位置情報登録 API と検索 API を提供している．位置情報提供者が登録した位置情報に関しては許可した LBS もしくは LBS 利用者にのみ公開される．位置情報が公開される際に精度の変更を行うことかできる．

3.1.4 関連研究の比較検討

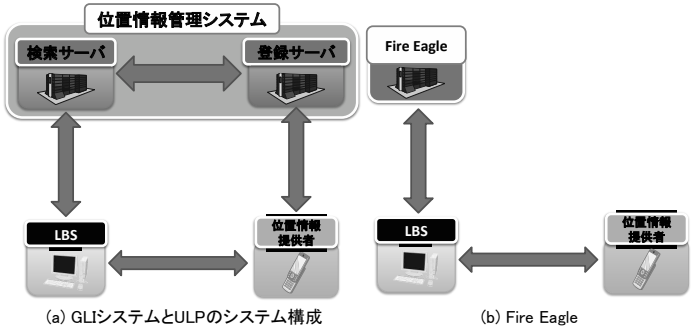

図 2 関連研究のシステム構成

図 2(a)に示すように GLI システムと ULP は位置情報の登録時, 利用者が直接システムに登録を行い，位置情報の検索時は LBS が検索する．つまり，これらのシステムでは位置情報を管理するシステム（登録サーバなど）を介してサービスを行うため，現状の LBS よりも位置情報提供者への応答時間が増加すると予想される. それに対して FireEagle は位置情報提供者の位置情報の登録が LBS を介して行われるので現状と変わらない応答時間でサービスを行える．しかし， LBS を介すことで MLBS による位置情報の不正利用が考えられる．このように提案方式の要求条件を満たす位置情報管理システムは存在しない．以上の比較検討結果を表 2 に示す.

表 2 既存研究の比較検討結果

	GLI システム	ULP	FireEagle
許可しない LBS への情報漏洩可能性	なし	なし	あり
MLBS による情報取得の可能性	なし	なし	あり
応答時間	増大	増大	現状と変わらない

3.2 信頼度の関連研究

信頼の度合を測る関連研究は Marianne ら[6]や Jøsang ら[7]が調査している. Marianne ら[6]はアドホックネットワーク上で利己的なノードや悪意のあるノードを判別する手法について述べている．Jøsang ら[7]は，Google の page rank や amazon などで利用されている評判や信頼度を利用したシステムの比較検討を行っている．これらの論文から信頼度評価手法を表 3 のように分類できる.

表 3 信頼度評価手法

手法		方法
プロファイル[8]		通信相手の提示しているプロファイル情報により信頼性を評価
推薦情報[9]		通信相手が他のユーザにより良い通信が行えるという推薦情報を利用
評判	単純平均[10]	良い評価と悪い評価の平均値により信頼性を評価
	確率モデル[11]	ベイズモデルの応用により信頼性を評価
	信頼の輪[12]	信頼できるユーザの連鎖を利用
	フローモデル[13]	過去の履歴によるローカルな信頼度をシステム中の評判の構造を利用し, 各ユーザのローカルな信頼度を基にした固有値計算を行うグローバルな信頼度計算手法

プロファイル方式は自分で作成するプロファイルを利用するので MLBS が存在したときに，その MLBS は自分を良い LBS と相手を誤認させることが可能なので使用できない．評判方式は想定する環境が P2P 環境などの中央管理者が存在しないものである場合に有効である. 提案方式では中央管理者が存在するため評判方式を利用しない．しかし，提案方式では位置情報提供者からの信頼度を収集し統合することが必要となる. そこで, 評判方式の信頼の輪を利用した方式で信頼度を集約する際に証拠理論[14]を利用した方式[15]がある．証拠理論は信頼などの不確実な情報を解釈することができる．従って，信頼度を計算したい LBS の推薦情報（信頼度）を設定し，証拠理論を利用して集約し，LBS の信頼度により通信型の選択を行う方式を提案する.

4. 位置情報管理システム

提案する位置情報管理システムは位置情報提供者の制御ポリシ（システム内で情報を利用する際の方針を規定したもの）を利用して位置情報・個人情報の管理・公開制御を行う．

4.1 システム構成

提案システムの構成を図 3(a)に示す．提案システムは位置情報提供者，LBS，ポリシサーバ(PS : Policy Server)， 位置情報管理サーバからなる．位置情報提供者は位置情報をシステムに提供する（LBS 利用者である場合もある）．PS は位置情報提供者の制御ポリシの登録・参照・変更とサービスへの制御ポリシに基づいた位置情報の提示を行う．位置情報管理サーバは位置情報提供者から登録された位置情報を制御ポリシに基づき管理する．また，提案システムの利用イメージを図 3(b)に示す．複数の LBS と位置情報提供者が存在し，位置情報提供者により登録された情報を制御ポリシに基づき加工を行うことで他の LBS（最終的には他の位置情報提供者）に対して利用可能にする機能を提供している．

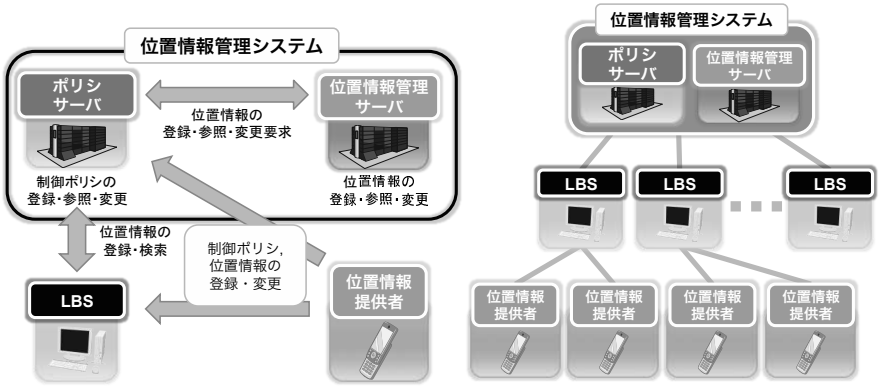

図 3 提案システムの基本構成と利用イメージ

4.2 管理情報

提案システムが管理する情報は位置情報，制御ポリシ，個人情報の 3 つとする．

(1) 位置情報

経度，緯度，高度，建物名や部屋名，測定時刻である．建物名や部屋名は位置情報提供者が任意に入力する．

(2) 制御ポリシ

制御ポリシの項目は公開時間，公開エリア，公開個人情報，位置情報保持時間，加工公開である．PS が制御ポリシの設定を行う．位置情報提供者がある LBS を利用し始める前に LBS から位置情報提供者に制御ポリシの設定をするように促すようにする．このときに LBS の契約約款とともに提案システムの個人情報利用の約款も提示するようにすることで位置情報提供者へプライバシーポリシの承諾を得る．

位置情報提供者は制御ポリシを LBS ごとに設定することが可能．制御ポリシの設定をしていない LBS からの情報要求があった場合には加工公開を利用する．

1) 公開時間
位置情報提供者が LBS に一週間のうち何曜日，一日のうち何時から何時までは公開するかを設定する．
2) 公開エリア
a 指定した範囲（都道府県エリア，市区町村エリア）にいる場合は公開するかを設定する．
b 指定した都道府県，市区町村にいる場合は詳細に公開するかを設定する．
3) 公開個人情報
LBS に対して公開する個人情報を設定する．
4) 加工公開
公開許可していない LBS から位置情報の要求があった時や公開時間，公開エリア以外の位置情報を要求された時に，情報を加工して公開するかどうかを設定する．
5) 位置情報保持時間
登録された位置情報をいつまでシステム内に保持しておくかを設定する

(3) 個人情報

位置情報提供者の年齢や性別などの個人情報である．位置情報提供者が登録する個人情報の項目は LBS が定義し，提案システムが登録・管理を行う．

この他に LBS が使用するサービス情報がある．サービス情報は LBS がサービスを行うにあたり必要とする情報である．例えば，案内サービスであれば目的地情報，娯楽サービスである Twitter の場合は 140 文字のコメントなどである．

4.3 処理手順

提案システムの処理手順を図 4 に示す．処理手順はユーザ登録フェーズと LBS 利用フェーズの 3 つに分かれている．ユーザ登録フェーズは LBS を利用するために位置情報提供者が LBS へのユーザ登録を行う手順である．LBS 利用フェーズは実際に LBS を利用しサービスを行う手順である．位置情報検索フェーズは制御ポリシに基づき位

置情報の公開の決定や加工処理を行う手順である．位置情報検索フェーズは制御ポリシに基づき位置情報の公開の決定や加工処理を行う手順である．

1．ユーザ登録フェーズ
　位置情報提供者が利用したい LBS へユーザ登録を行う．次にその LBS が要求する個人情報を登録する．提案システムが位置情報提供者の個人情報を管理する．そして，PS が位置情報提供者の位置情報や個人情報を管理するルールを規定した制御ポリシの登録を行う．
2．LBS 利用フェーズ
　LBS が位置情報提供者の位置情報の登録やサービスを行うにあたり必要になる位置情報の検索を行う．
3．位置情報検索フェーズ
　検索パラメータと制御ポリシのマッチングを行う．制御ポリシとのマッチングで，位置情報を公開の可否，もしくは位置情報または個人情報を加工して公開するかが決定される．

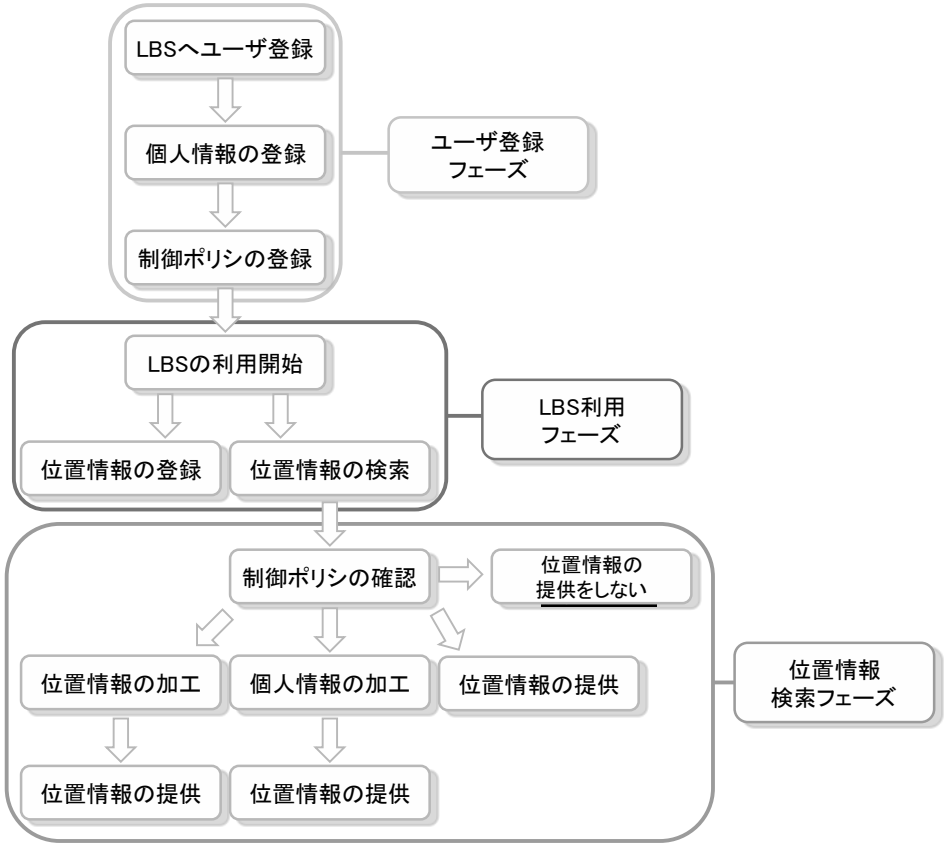

図 4 提案システムの処理手順

4.4 情報の通信型
　提案システムでは 2 つの通信型を用いて情報の通信を行う．位置情報提供者の情報を LBS 経由で通信する「経由通信型」と，位置情報提供者の情報をシステムに直接通信する「直接通信型」である．図 5 にその手順を示す．

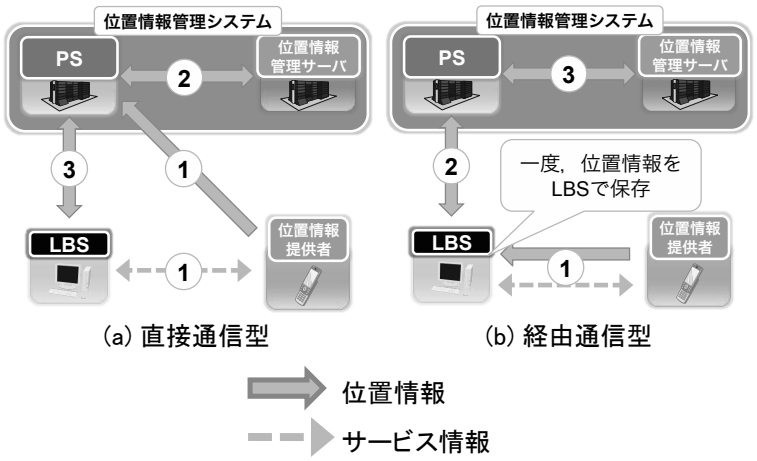

図 5 提案システムの通信型

各通信型の動作順序を示す．各番号は図中の番号と対応する．

a) 直接通信型
(1) 位置情報提供者は LBS からサービスを受けるために位置情報をシステムに送信し，サービス情報を LBS に送る．
(2) 位置情報を受信した PS は位置情報管理サーバに位置情報を送信する．
(3) LBS は位置情報提供者の要求に応じて必要な位置情報を PS に問い合せる．PS は要求された位置情報を位置情報管理サーバから取得する．このとき，PS では位置情報提供者の制御ポリシに応じて公開の可否を決定，もしくは位置情報の加工，個人情報の加工を行い公開するか決定し，結果を LBS に送信する．
b) 経由通信型
(1) 位置情報提供者は LBS からサービスを受けるために位置情報とサービス情報を LBS に送信する. LBS は受信した情報をもとに位置情報提供者にサービスを行う．
(2) LBS は受信した情報を一定時間ごと，もしくは位置情報提供者へのサービスが終わった段階で保存してある位置情報をシステムに送信する．
(3) 位置情報を受信した PS は位置情報管理サーバに位置情報を送信する．

4.5 信頼度による通信型の選択方式

表 1 でも示したように，2 つの通信型にはそれぞれ利点と欠点があり，どの LBS にどの通信型を割り当てるかということが問題になる．LBS は位置情報提供者に対して少ない応答時間でサービスを提供したいという要求があり，位置情報提供者は少ない応答時間とプライバシー保護を両立させてほしいという要求がある．LBS と位置情報提供者の双方の要求を満たすために経由通信型で通信が行える環境が適切である．しかし，経由通信型では MLBS による情報の不正利用問題があるため安易に使用することはできない．そこで LBS の信頼度を設定し，信頼できる LBS を利用する場合には経由通信型，信頼できない LBS を利用する場合には直接通信型を用いる．この信頼度による通信型の選択方式について説明する．

4.5.1 信頼度設定手順

LBS の信頼度を設定するために，以下の手順で LBS をサービス種別ごとに分類する．分類することで後述する信頼度の集約作業を分散することが可能となる．
(1) PS が LBS をサービス種別ごとに分類する．分類したものを Set として定義する．
(2) 分類された集合の代表（SH : Set Head）を選出
　　PS がシステム信頼度をもとに選出する．
(3) SH は集合内の LBS 信頼度を管理し，定期的に PS に報告する

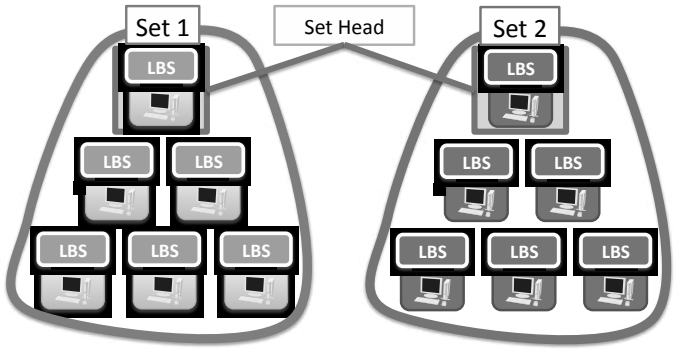

図 6 SH の選出

LBS が提案システムを利用し始めたときから，その LBS は位置情報提供者と PS，他の LBS から信頼度を判断される．個々に判断された信頼度は SH と PS で集約される．このときに証拠理論[7]を利用した情報集約を行う．こうして設定された信頼度により通信型の選択を行う．また，信頼度の低い LBS に対して情報公開の制限を設ける．

4.5.2 信頼の定義

武田[16]によれば，信頼という場合，ある情報を信頼するという場合もあるが，むしろある人を信頼するというほうが一般的である．つまり，信頼の度合とはある人

が別の人をどれだけ信頼するかの度合である．このとき信頼の基本的機能とはリスク環境の中で自己の不利益を最小にすることである．そのために相手の信頼を推量する必要がある．信頼を推量する際に必要となるのは，信頼を推量したい相手の態度や自分とその相手の関係の経験である．そこで，利用する情報は信頼を推量したい相手の行動から得られる行動情報とそれ以外の外部から得られる外部情報である．この情報は行動情報に重みをおいて利用される．そこで，提案方式で利用する信頼度にも外部情報と行動情報を含むようにする．

4.5.3 提案方式で利用する信頼度

提案方式で利用する信頼度は位置情報提供者がLBSに対して設定する提供者信頼度，LBS同士で設定するLBS信頼度，PSがLBSに対して設定するシステム信頼度がある．それぞれの信頼度は信頼度を判断する対象本体から得られる情報（行動情報）とそれ以外の外部から得られる情報（外部情報）から構成される．以下にそれぞれの信頼度について説明する．

(1) 提供者信頼度

以下の値が0〜1になるように設定する．提供者信頼度は外部情報がサービス満足度で行動情報が位置情報送信頻度と制御ポリシの評価と設定する．

- サービス満足度
  - LBSからサービスを受けた位置情報提供者がどれだけLBSに満足しているかの度合
- 位置情報送信頻度
  - 位置情報提供者がLBSを利用した際に位置情報を送信した頻度
- 制御ポリシの評価
  - 位置情報提供者がLBSに対して設定した制御ポリシを評価した値

提供者信頼度の設定方法は以下の手順で行う．

1. 位置情報提供者はLBS利用開始前にサービス満足度の開始値を設定
2. 位置情報提供者はLBS利用後，サービス満足度の終了値を設定
3. サービス満足度をPSに送信
4. PSはサービス満足度，サービス利用時に位置情報を送信した回数，制御ポリシの評価から提供者信頼度を設定

(2) LBS信頼度

以下の値が0〜1になるように設定する．LBS信頼度は外部情報が提供者信頼度と位置情報提供者数で行動情報が監視結果と設定する．

- 提供者信頼度
- 位置情報提供者数
  - LBSに登録している位置情報提供者の数から設定する値
- 監視結果
  - 監視方法は以下に示す図7(a)のように行う．まず，SHがLBSに監視する対象のLBSを指定する．監視する内容は位置情報の登録数と情報の要求回数である．監視対象のLBSはそれらの情報を監視しているLBSとSHに送信する．SHは監視情報を定期的にPSに送信し不正がないか確認を行う．不正があった場合はシステムからの除外や取得できる情報に制限をかける．また，図7(b)のように監視を行うべきLBSが監視をしなかった場合，監視をしなかったLBSのLBS信頼度を最低にするようにする．

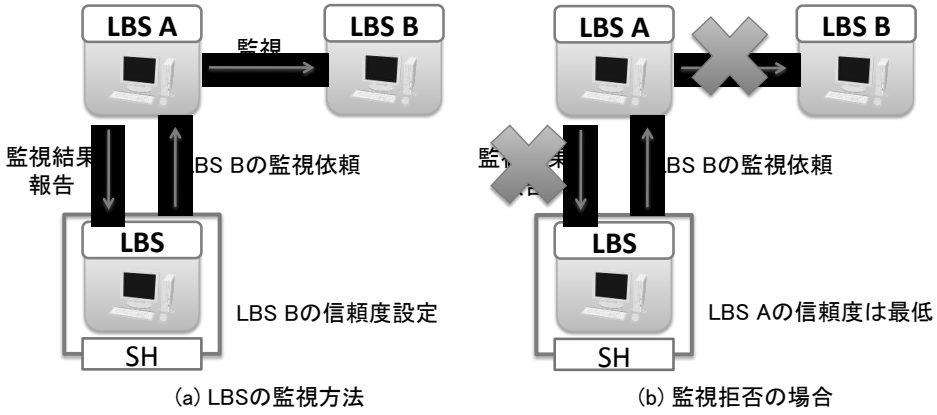

図7 LBSの監視方法

(3) システム信頼度

以下の値が0〜1になるように設定する．システム信頼度は外部情報がLBS信頼度で行動情報が位置情報登録頻度と情報取得頻度と設定する．

- LBS信頼度
- 位置情報登録頻度
  - LBSが一定時間内に位置情報を登録した頻度
- 情報取得頻度
  - LBSが一定時間内に位置情報を要求した頻度

4.5.4 信頼度集約方法

証拠理論を利用した信頼度の集約を行う．証拠理論は不確実な情報の解釈と意思決定を行えるため利用した．LBSの信頼性は不確実なものなので利用可能である．

• 証拠理論[14]

ある有限個の命題の集合 X（$X=\{x_1,\ldots,x_n\}$．$x_1,\ldots,x_n$ は互いに排他的で 1 つの命題を除き全てが偽）を識別集合という．このような識別集合が存在したとき，証拠理論を用いることが可能となる．証拠理論には信念割当関数を定義し情報統合を行うという 2 つのステップが存在する．信念割当関数とは識別集合の命題の真偽に関する信念を表すものである．信念割当関数を $m(2^X \rightarrow [0,1])$としたとき，信念割当関数は次の公理を満たすようにする．

[信念割当関数の公理]

(i) $m(A) \geq 0, A \in 2^X$

(ii) $m(\phi) = 0$

(iii) $\sum_{A \in 2^X} m(A) = 1$

情報統合とは複数の信念割当関数を結合することである．情報統合は[ステップ 1]命題の論理積とその評価（予備割当関数の構成）と[ステップ 2]予備割当関数から信念割当関数への変換という 2 つのステップからなる．

[ステップ 1]

$\{m_1(F):F \in 2^X\}$，$\{m_2(F):F \in 2^X\}$の 2 つの信念割当関数があった時，次の予備割当関数 $q(A)$に当てはめる．

$$q(A) = \sum_{F,G:F \cap G \neq \phi} m_1(F) m_2(G)$$

[ステップ 2]

予備割当関数から信念割当関数へ次の Dempster の規則を用いて変換する．

$$m(A) = \frac{q(A)}{1 - q(\phi)}, A \neq \phi$$

信頼度集約を行うために次の前提を設定する．

[前提]　信念割当関数を次のように定義する．

• $m(\{T\})$：LBS が信頼できるとする確率
• $m(\{\neg T\})$：LBS が信頼できないとする確率
• $m(\{T, \neg T\})$：LBS が信頼できるかどうか不明とする確率

信頼度集約手順は次のように行う．

1.　それぞれの信頼度の項目 α_i（提供者信頼度であればサービス満足度，位置情報送信頻度，制御ポリシの評価）を証拠理論適用のため「Good」「Normal」「Bad」の三段階に分類する．
   • 「Good」を G とする．$(0.66 \leqq \alpha_i \leqq 1.0)$
   • 「Normal」を N とする．　$(0.31 \leqq \alpha_i \leqq 0.65)$
   • 「Bad」を B とする．　$(0.0 \leqq \alpha_i \leqq 0.3)$
2.　それぞれの 3 つの評価に応じて信念割当関数を計算する．

まず，得られた 3 つの G/N/B の組み合わせに応じて信頼度の「Trustworthy」「Trustworthy or Not」「Not Trustworthy」の評価を決める．その際に行動情報に重み付けるようにする．

提供者信頼度とシステム信頼度は以下の条件により決定する

• 「Trustworthy」評価
   − 行動情報が G もしくは N で外部情報が G もしくは N．ただし行動情報が 2 つ G であった場合のみ外部情報は B でも可．
• 「Trustworthy or Not」評価
   − 行動情報が G もしくは N（G が 2 つの場合は除く）で外部情報が B ではない（ただし行動情報に 1 つでも G が含まれていた場合は B でも可）．
• 「Not Trustworthy」評価
   − 行動情報に 1 つ以上の B が存在する場合

LBS 信頼度は以下の条件により決定する．

• 「Trustworthy」評価
   − 行動情報が G で外部情報が G もしくは N．ただし外部情報が 2 つ N であった場合は含まれない．
• 「Trustworthy or Not」評価
   − 行動情報が N で外部情報の B が 2 つ以上ではない（ただし行動情報に G 外部情報が G と B となっている場合も可）．
• 「Not Trustworthy」評価
   − 行動情報に 1 つ以上の B が存在する場合

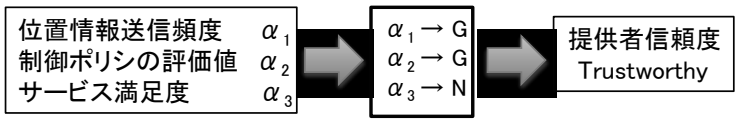

図 8 提供者信頼度の評価決定例

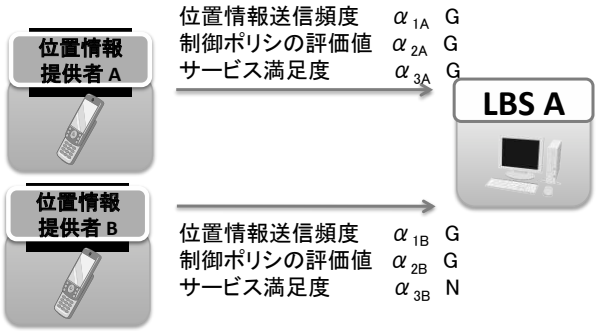

図 9 提供者信頼度の信念割当関数導出例

信頼度の各項目から評価を決定した後，以下の手順で $m(\{T\})$ / $m(\{\neg T\})$ / $m(\{T,\neg T\})$を求める．

- 「Trustworthy」評価の時
  図 9 の例に基づいて説明する．まず G 評価の合計（GS とする）が
  $\alpha_{1A} + \alpha_{1B} + \alpha_{2A} + \alpha_{2B}$ = GS のように求める．同様に N 評価の合計（NS とする）が
  α_{3B} = NS となる．
  そして，次のような比と条件 $m(\{T\}) + m(\{T,\neg T\}) = 1$ から
  GS : NS = $m(\{T\})$: $m(\{T,\neg T\})$
  $m(\{T\})$と $m(\{T,\neg T\})$を求める．
- 「Trustworthy or Not」評価の時
  「Trustworthy or Not」評価の時に求めるのは $m(\{T,\neg T\})$のみである．これは証拠理論の条件から $m(\{T,\neg T\}) = 1$ と定まる．
- 「Not Trustworthy」評価の時
  「Trustworthy」評価の時と計算式としては変わらないが求めるものは $m(\{\neg T\})$と $m(\{T,\neg T\})$になる．条件は $m(\{\neg T\}) + m(\{T,\neg T\}) = 1$．求める比は「Not Trustworthy」の値の合計を BS とすると，
  BS : NS ＝ $m(\{\neg T\})$: $m(\{T,\neg T\})$
  となる．

このような手順で求められた $m(\{T\})$，$m(\{\neg T\})$，$m(\{T,\neg T\})$を証拠理論による情報集約の手順で集約し各信頼度とする．提供者信頼度，システム信頼度は PS が集約・計算を行い，LBS 信頼度に関しては SH が集約・計算を行う．システム信頼度により通信型の選択を行う．

5. 考察

提案システムの評価を表 4 に示す．提案システムでは位置情報提供者の情報漏洩や悪意のある LBS からの情報取得を防ぎながら現状の LBS とほとんど変わらない応答時間を実現できる．また，先行研究での情報共有は情報が一つにまとめられているだけでそれぞれの LBS で相互に情報を利用することはできない．しかし，提案システムでは加工公開を用いることで各 LBS の情報を相互に利用できる．さらに，LBS の信頼度により安全な通信型を利用することで位置情報提供者のプライバシー保護が可能となる．

表 4 提案システムの評価

		GLI システム	ULP	FireEagle	提案システム
プライバシー保護要件	(1)	○	○	○	対象外
	(2)	○	○	×	○
	(3)	○	○	×	○
	(4)	○	○	×	○
LBS 間での情報の相互利用		不可能	不可能	不可能	可能
応答時間		増大	増大	現状と変わらない	現状と変わらないか増大

○：防止可能　×：防止不可能

6. おわりに

本稿では位置情報管理システム上で LBS の信頼度により 2 つの通信型を選択する方式を提案した．LBS の信頼度を定義し，位置情報提供者とポリシサーバから設定できるようにした．また，LBS 同士での監視を取り入れることにより，LBS に責任をもたせることができた．複数の位置情報提供者からの信頼度や LBS 信頼度を証拠理論により集約することで，不確実な信頼度の解釈が行える．

今後，信頼度を三段階に分類する際の値の設定やシステム信頼度による通信型の選択を行う際の閾値を求める必要がある．シミュレーションによりそれらの最適値を求める．LBS で利用される位置情報の通信量を調査し，位置情報送信頻度や位置情報登録頻度，情報取得頻度の設定値を決める必要がある．また，LBS の監視方法や内容も検討の余地がある．

参考文献

[1] 渡辺恭人, 竹内奏吾, 栗栖俊治, 寺岡文男, 村井純: “プライバシー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, Vol.J86-B, No.8, pp.1434-1444, 2003

[2] 原史明, 沼田雅美, 植原啓介, 砂原秀樹, 寺岡文男: “Universal Location Platform:汎用的位置情報基盤の設計と実装”, 情報処理学会論文誌, Vol.47, No.12, pp.3112-3123, 2006

[3] Yahoo!, “fire eagle,” http://fireeagle.yahoo.net/ (2009 12/18)

[4] 森勇海, 白石陽, 高橋修: “サービス間の位置情報共有のためのプライバシー保護を考慮した位置情報管理システムの提案”, 情報処理学会全国大会, pp.673-674, 2010

[5] 高橋幸雄, 辻井重男: “位置認証と情報セキュリティに関する考察”, 情報処理学会研究報告, 2007-CSEC-38, (1), pp.1-6, 2007

[6] Marianne A. Azer, Sherif M. El-Kassas, Abdel Wahab F. Hassan, Magdy S. El-Soudani, “A Survey on Trust and Reputation Schemes in Ad Hoc Networks,” IEEE The Third International Conference on Availability, Reliability and Security, pp.881-886, 2008

[7] Jøsang, A., Ismail, R., Boyd, C, “A Survey of Trust and Reputation Systems for Online Service Provision,” Decision Support Systems Vol.43(2), pp.618-644, 2007

[8] Stakhanova, N., Basu, S., Wong, J., and Stakhanov, O., “Trust Framework for P2P Networks using Peer-Profile based Anomaly Technique,” Proceedings of the 2nd International Workshop on Security in Distributed Computing Systems, pp.203-209, 2005

[9] Chopra, K. and Wallace, W., “Trust in Electronic Environments,” Proceedings of 36th Annual Hawaii International Conference on System Sciences, pp.331-340, 2003

[10] Sergey, B., and Lawrence, P., “The Anatomy of a Large-Scale Hypertextual Web Search Engine,” Proceedings of the 7th International Conference on World Wide Web, 1998

[11] Withby, A., Josang, A., and Indulska, J., “Filtering Out Unfair Ratings in Bayesian reputation Systems,” Proceedings of the 3rd International Joint Conference on Autonomous Agents and Multi Agent Systems, 2004

[12] Guha, R., Kumar, R., Raghavan, P., and Tomkins, A., “Propagation of Trust and Distrust,” Proceedings of the 13th International Conference on World Wide Web, pp.401-412, 2004

[13] Kamvar, S., Scholosser, M., and Garcia-Molina, H., “The EigenTrust Algorithm for Reputation Management in P2P Networks,” Proceedings of the 12th International Conference on World Wide Web, PP.640-651, 2003

[14] Shafer, G., “A Mathematical Theory of Evidence,” Princeton University Press, 1976

[15] Yu, B. and Singh, M.P., “Distributed Reputation Management for Electronic Commerce,” Computational Intelligence, Vol.18,No.4(2002), pp.535-549, 2002

[16] 武田英明,『コンピュータソフトウェア』, Vol.22, No.4, pp.19-25, 2005