5ZE-2

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

森 勇海† 白石 陽† 高橋 修†

公立はこだて未来大学 システム情報科学部†

1. はじめに

近年，携帯端末や RFID などのセンサ・タグ情報などにより位置情報の取得が容易になってきている．それにより，位置情報を利用したサービス（以下，LBS）が増加する傾向にあり，位置プライバシーの保護と情報共有が問題となっている．位置プライバシーの保護とは第三者によってある人の現在，もしくは過去にいた位置を知られることを防ぐことである．情報共有の問題は，図 1(a)に示すように現状ではそれぞれの LBS が独自に位置情報を管理しているため，利用者はそれぞれの LBS に位置情報を提供しなければならない．さらに LBS 間で安全に位置情報を共有する方法が少ない．そこで，図 1(b)に示すように LBS が個別に管理していた位置情報の共有を可能にし，さらに位置プライバシー保護を考慮した位置情報の管理を行う位置情報管理システムの提案を行う．

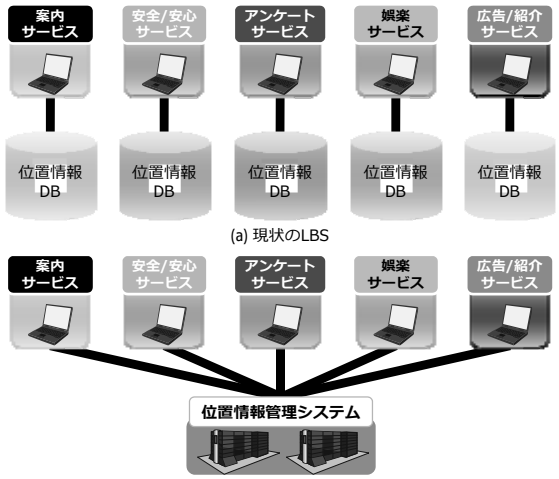

図 1 LBS の現状と提案システム利用イメージ

2. 関連研究

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．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は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管理するシステムを介してサービスを行うため，現状の LBS よりも利用者への応答時間（LBS が利用者から情報の要求を受けてから提供するまでにかかる時間）が増加すると予想される．それに対して FireEagle は利用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 を介すことで悪意のある LBS による位置情報の悪用が考えられる．

本稿では，利用者のプライバシー保護のため，に利用者の情報を LBS へ公開する範囲を制御する制御ポリシを利用する．利用者の制御ポリシの設定項目を増やすことでより安全なプライバシー保護を提供するとともに，位置情報の共有を可能にする．

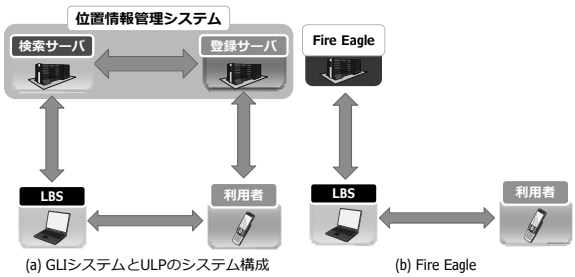

図 2 関連研究のシステム構成

3. 提案システム

提案システムは位置情報の管理機能と検索機能を持つ．本稿では提案システムの構成と管理機能の概要について述べる．プライバシー保護要件を満たした上で位置情報の共有を行うシステムを提案する．

3.1 プライバシー保護要件と対策

高橋ら[4]が挙げた位置情報利用時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以下に示す．

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）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

以上の要件はシステム管理者の問題であり，提

A location information management system with privacy protection for location information sharing between location-based services

Yuumi Mori†, Yoh Shiraishi†, Osamu Takahashi†

†School of System Information Science, Future University Hakodate

案システムでは要件を満たすために制御ポリシによる情報の管理・公開の設定を行う．

3.2 システム構成

提案システムの構成を図 3 に示す．提案システムは位置情報提供者，LBS，ポリシサーバ，位置情報管理サーバからなる．位置情報提供者は自分の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）．ポリシサーバは位置情報提供者の制御ポリシの登録・参照・変更とサービスに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を管理する．

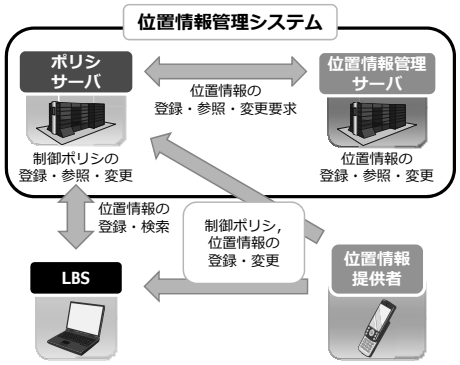

図 3 提案システムの基本構成

3.3 情報の通信

提案システムでは 3.1 の要件を満たし，さらに現状の LBS とほとんど変わらない応答時間を実現するために図 4 に示すような 2 つの通信型で情報の通信を行う．

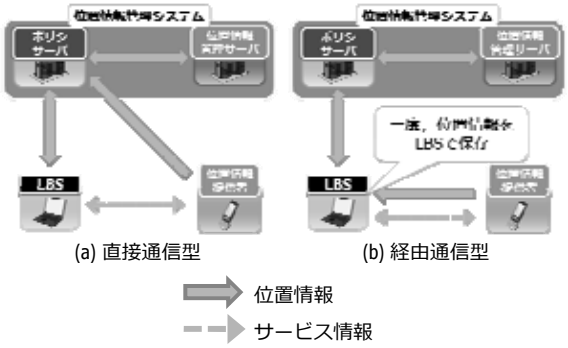

図 4 提案システムの情報の流れ

3.3.1 情報の扱い

図 4(a)に示すような直接通信型の方式では位置情報提供者はサービスを受けるために LBS が利用する情報（サービス情報）を LBS に送り位置情報はシステムに登録し，LBS から情報要求があったときに開示される．経由通信型の方式では位置情報は一度 LBS で利用し，その後システムに位置情報を登録する．

3.3.2 通信型の比較

直接通信型は LBS を介して位置情報の通信を行わないので情報を知られる危険性が低い．悪意のある LBS による情報取得や位置情報提供者の許可しない LBS への情報漏洩の危険が少ない．しかし，位置情報提供者への応答時間が現状よりも増加してしまう．経由通信型ではそれらの危険性が高くなるが，現状の LBS と変わらない応答時間で動作する．

通常は直接通信型の方式で情報は制御されるが緊急通報などの安心・安全サービスや信頼度の高い LBS については経由通信型で行われる．

3.4 制御ポリシ

制御ポリシの項目を表 1 に示す．制御ポリシは LBS ごとに設定することが可能である．

表 1 制御ポリシ

制御ポリシ	内容
公開時間	指定時間内のみ情報公開
公開エリア	指定エリア内のみ情報公開
公開個人情報	指定個人情報の情報公開
位置情報保持時間	位置情報をシステム内に保持する時間

4. 考察

関連研究との比較検討結果を表 2 に示す．このように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．

表 2 関連研究との比較

	GLI システム	ULP	Fire Eagle	提案システム
許可しない LBS への情報漏洩	○	○	×	○
悪意のある LBS による情報取得	○	○	×	○
LBS 間の情報共有	○	○	○	○
応答時間	×	×	○	△

5. おわりに

本稿では位置情報提供者のプライバシー保護を考慮したサービス間の情報共有を行うための位置情報管理システムを提案した．位置情報提供者に対して安全な情報利用のための情報管理手法に着目した．さらに，制御ポリシの利用で位置情報提供者のプライバシー保護を考慮しながら情報共有が可能となる．

今後，提案方式の暗号化による情報の安全な通信についての検討やさらに効率的な利用を促進する制御ポリシの提案を行う．また，提案システムの実装を行い性能検証する必要がある．

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, 2003.8
[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, 2006.12
[3]. Yahoo!，“fire eagle”, http://fireeagle.yahoo.net/ (200912/18)
[4]. 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, 2007.7