慶應義塾大学学術情報リポジトリ
Keio Associated Repository of Academic resouces

Title	ユビキタス情報サービス基盤における効率的なプライバシ保護機構とその評価
Sub Title	Efficient location privacy protection in ubiquitous information service infrastructure
Author	高汐, 一紀(Takashio, Kazunori)
Publisher	
Publication year	2012
Jtitle	科学研究費補助金研究成果報告書 (2011.)
JaLC DOI	
Abstract	本研究課題では, 人間を含む移動体プローブが提供する実世界情報に含まれる位置情報にユーザの望む匿名性を付加するサービスフレームワークを提案し, 実環境上に実装, 有効性の評価・ 検証を実証的に行った. 本フレームワークにより, ユーザは自身の望む程度でプライバシを保護できる. 結果, 従来は「個人情報を公開するか否か」の二極でしか選択肢を持たなかったユーザが, 「この程度の匿名性で情報を公開する」といった中間解の選択が可能となった.
Notes	研究種目：基盤研究(C) 研究期間：2009～2011 課題番号：21500080 研究分野：総合領域 科研費の分科・ 細目：情報学・ 計算機システム・ ネットワーク
Genre	Research Paper
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KAKEN_21500080seika

慶應義塾大学学術情報リポジトリ(KOARA)に掲載されているコンテンツの著作権は、それぞれの著作者、学会または出版社/発行者に帰属し、その権利は著作権法によって保護されています。引用にあたっては、著作権法を遵守してご利用ください。

The copyrights of content available on the KeiO Associated Repository of Academic resources (KOARA) belong to the respective authors, academic societies, or publishers/issuers, and these rights are protected by the Japanese Copyright Act. When quoting the content, please follow the Japanese copyright act.

様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年５月３１日現在

機関番号：３２６１２
研究種目：基盤研究（C）
研究期間：2009～2011
課題番号：２１５００８０
研究課題名（和文）ユビキタス情報サービス基盤における効率的なプライバシ保護機構とその評価
研究課題名（英文）Efficient Location Privacy Protection in Ubiquitous Information Service Infrastructure
研究代表者
高汐　一紀（TAKASHIO KAZUNORI）
慶應義塾大学・環境情報学部・准教授
研究者番号：４０２７２７５２

研究成果の概要（和文）：
本研究課題では，人間を含む移動体プローブが提供する実世界情報に含まれる位置情報にユーザの望む匿名性を付加するサービスフレームワークを提案し，実環境上に実装，有効性の評価・検証を実証的に行った．本フレームワークにより，ユーザは自身の望む程度でプライバシを保護できる．結果，従来は「個人情報を公開するか否か」の二極でしか選択肢を持たなかったユーザが，「この程度の匿名性で情報を公開する」といった中間解の選択が可能となった．

研究成果の概要（英文）：
In this project, we proposed a novel privacy preservation framework that reduces the damage of privacy-invasion, caused if malicious services try to share our footsteps. We can set the degree based on our demand: the higher the degree, the harder services misuse our footsteps. Consequently, this framework enables us to utilize ubiquitous location-aware services even though these services might be unknown, untrustworthy, or malicious ones.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,500,000	450,000	1,950,000
2010 年度	1,000,000	300,000	1,300,000
2011 年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,500,000	1,050,000	4,550,000

研究分野：総合領域
科研費の分科・細目：情報学，計算機システム・ネットワーク
キーワード：ユビキタス情報サービス，プライバシ保護，移動体プローブ，ロケーション情報

１．研究開始当初の背景

情報技術の発展にともない，GPS 端末や RF タグなどの位置取得技術が我々の生活に浸透しはじめている．特に GPS 付携帯電話の普及は目覚しく，近隣レストラン検索サービス，外回り勤務者勤怠管理サービスなどの多様なロケーションアウェアサービスが既に実用化，商用化されている．

これらロケーションアウェアサービスを享受する機会の増加にともない，個人情報としての移動履歴が第三者によって不当に把握されることに対する危機感も増加しており，プライバシに対する関心が高まってきた．プローブ情報型のユビキタス情報サービスが浸透するにつれ，その傾向は益々強まるものと予想され，この危機感を払拭しない限り，

我々にとって未知のサービスが自律的に我々の個人情報に即したサービスを提供するユビキタスコンピューティング環境の実現は困難となる．したがって，プライバシを保護しつつも，有用なサービスを効率的に享受できる環境を実現するサービスフレームワークや社会基盤の確立が急務であった．

２．研究の目的

本研究課題が想定するユビキタス情報サービスインフラでは，環境固定のセンサネットワークインフラだけでなく，無線携帯端末を身に着けた人間をも，細粒度の移動体プローブ（ヒューマンプローブ）とみなし，携帯端末が備える各種センサにより取得される実世界情報をそのロケーション情報とともにリアルタイムに収集，加工し，実世界人群行動予測や実空間雰囲気モニタリング等の高次実世界コンテクストの抽出に適用する．プローブとなるユーザはこれらの情報を提供することへの対価として，ロケーションアウェアサービスに代表される様々なユビキタス情報サービスを享受することができる．しかし，プローブ情報には，ユーザのロケーションを始め，様々な個人情報が含まれており，その収集にあたっては，プライバシ保護の仕組みを慎重に検討する必要がある．

本研究の目的は,サービスに公開した個人情報が悪用された場合にユーザが被る被害を抑えることにある．位置匿名化によってロケーションプライバシを保護するサービスフレームワークならびにその実現機構を提案，その性質を定性的に議論するだけでなく，研究代表者らが並行して開発中のユビキタス情報空間アクセスオープンプラットフォーム上での実装を通して有効性の評価・検証を実証的に行う．これらの議論を踏まえ，順次，匿名化の対象を個人情報全般に拡張し，生きた公共空間上でのプライバシ保護機構に必要な要件とその効果を明らかにする．

３．研究の方法

研究計画初年度となる平成 21 年度は,(a) 問題の分析と評価指標の検討，(b) 小規模実験プラットフォームの構築，(c) 評価用実世界情報プローブサービスの実装と位置匿名化アルゴリズムの検討を並行して実施した．具体的には，先行関連研究の分析と問題点の洗い出しを進めるとともに，評価指標としての QoS (Quality of Service) および QoP (Quality of Privacy) の視点から，個人情報匿名化に関する議論の形式化を行った．また，公共空間を想定した屋内に小規模な実験プラットフォームを構築し，位置匿名化アルゴリズムの評価に用いる位置抽象化支援ミドルウェアを設計，実装，その基本性能を評価した．これにより，ロケーションプライバシを保護するためのインフラシステム側の条件，位置抽象化支援ミドルウェアが備えるべき要件を詳細化することができた．さらに，単純化した問題として「ユーザあるいはエリアを特定可能なサービス」を想定し，その具体例として，実世界人群行動予測，実空間雰囲気モニタリングを実装，位置匿名化アルゴリズムの基礎的評価を行った．

研究計画 2 年目となる平成 22 年度は，問題を一般化するとともに，対象エリアを屋外公共空間へ拡張した．具体的には，対象となるユーザ集合，エリア集合ともに特定が困難となるリスニングサービスをも支援対象として含むよう，位置匿名化アルゴリズムの一般化を進めるとともに，実装に向けた詳細化の見直しを行い，アルゴリズムの定性的な検討を行った．また，本研究課題で設定した目標の達成を検証するための統合評価環境として，屋内，屋外両プラットフォームならびに各種テストベッドで統一的に利用可能なベンチマークフレームワークを設計，実装した．さらに，次年度に向けた準備として，実験プラットフォームをキャンパス規模に拡大，同実験プラットフォーム上に上記ベンチマークフレームワークを構築し，より複雑な条件下での実証実験に向けた機能検証を実施した．

研究計画最終年度となる平成 23 年度は，前年度までの議論を踏まえ，提案手法の精緻化ならびに評価を行った．具体的には，位置匿名化アルゴリズムの一般化をさらに進めるとともに，アルゴリズムの定性的な評価を行った．また，屋内，屋外両プラットフォームならびに各種テストベッドで利用するベンチマークフレームワークの充実化を図るとともに，より複雑な条件下での実証実験を通して，他手法との性能面での比較評価を行い，提案アーキテクチャの有用性を実証的に検証した．

４．研究成果

(1) 実験プラットフォーム

報告者らのグループはこれまでにも,慶應義塾大学湘南藤沢キャンパス（SFC）内に，Smart Space Laboratory，Smart Living Room，Smart Corridor を構築，運用している実績があるが，本研究課題に関連して，新たに屋外実証実験用プラットフォームを整備した．

今,日本では街路灯光源の LED 化が急速に進んでいる．報告者らは，LED 化されることにより生じた灯具内のスペースを有効活用し，屋外にヒューマンプローブ／移動体プローブインフラを実現するための様々な通信機器を設置した．電力の恒久的な供給能力と，持って生まれた高精度な位置情報という街路灯の特徴を生かし，新しい形での実世界情報取得インフラを実現した（図 1)．

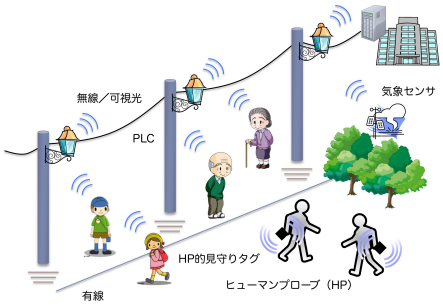

図 1 街路灯ベース実世界情報取得インフラ

(2) サービスフレームワーク

本研究課題では，ヒューマンプローブが発信する実世界情報のうち，特にプローブの位置情報に着目し，ユビキタス情報サービスを「ユーザから取得した位置情報を悪用する可能性のあるエンティティ」と想定し，特に，位置情報の悪用を「サービスが他のサービスと共謀してユーザの位置情報を共有すること」と定義する．また，位置情報のアノニミティセットを該当位置に存在するユーザ数とし，“単一位置情報の匿名性は該当位置に存在するユーザ数に比例する”と定義する[1]．

本研究課題が提案するサービスフレームワーク LOXY II の概要を図 2 に示す．ユーザの信用対象である匿名化エンジン Fixer は，GPS 端末や RF-ID，無線インフラ等の位置取得機構からユーザの位置情報を受け取り，位置情報の匿名化を行った後，サービスに対して移動イベントを発行する．匿名化とは，ユーザの望む匿名性を満たすよう位置情報の粒度を変更する処理を指し，移動イベントとは，匿名化された位置情報とユーザの仮識別子が含まれた情報を指す．設定された匿名性が高いほど，サービスによる位置情報の悪用は困難となるため，ユーザは自身の望む程度でプライバシを保護できる．

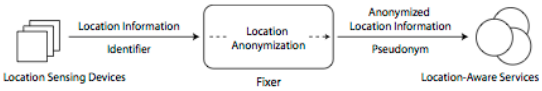

図 2 フレームワークコンセプト

(3) 位置情報の匿名化処理

本フレームワークでは，公開位置情報の匿名性を設定する変数として locset を導入する．ユーザは「locset 人以上が同じ位置に存在する粒度」で位置情報を公開するように設定する．各ユーザの locset と位置情報を把握している LOXY II は，条件「該当位置のアノニミティセット ≧ locset」を満たすよう位置情報を匿名化し，その結果をサービスに公開する．locset の値が大きいほど，位置情報の匿名性は高くなり，サービスによる位置情報の悪用は困難になる．

位置情報を匿名化しても，サービスが任意のエリアのアノニミティセットを把握できてしまうと，識別子を関連付けられる可能性が高くなる．異なるサービスが，あるエリアにおいてアノニミティセットが 1 増加したことを把握すると同時に，異なる識別子の付加された移動イベントを受信した場合，サービスは容易に識別子を関連付けられる．これを防ぐため，LOXY II は任意のエリアのアノニミティセットをサービスから隠蔽する．

GPS 位置情報（度分秒表記（DMS））を例に，LOXY II における位置情報匿名化処理の詳細を述べる．LOXY II は，受信した緯度経度を 1/100 秒まで記述した DMS 形式に変換し，秒の部分を階層化の対象とする．したがって，最も細かい粒度の位置情報は$(1/100\text{秒})^2$=7.8 x 10^{-2} m^2 ≒ $(28\text{cm})^2$，最も粗い粒度の位置情報は$(1\text{分})^2$ = 2.8 km^2となる．最小粒度$(28\text{cm})^2$の同一グリッドには同時に 2 人以上存在できないため，locset ≧ 2 の場合，匿名化の結果は必ずこの粒度よりも粗くなる．Locset = 1 の場合，受信した位置情報をそのまま公開する．

LOXY II は，緯度，経度の秒を 2 進数に変換後，その位によって位置情報を階層化する．丸め誤差を防ぐため，秒の値を 100 倍した後に 13 桁の 2 進数に変換する．よって，位置情報は 14 階層に分けられ，1 階層上がるごとに粒度は 4 倍となる．

階層化した後，LOXY II は，条件「緯度経度それぞれの度，分，2 進数変換された秒の上位 n 桁が等しいユーザ数 ≧ locset」を，n = 13 から確認する．条件を満たすまで n をデクリメントして確認作業を続ける．条件を満たした時点で，下位 13 − n 桁を 0 に置換した値を 10 進数に変換して 100 で割った秒を最小値，下位 13 − n 桁を 1 に置換した値を同様に処理した値を最大値とする．LOXY は，緯度，経度とも最小値の組み合わせ(a|b)を始点，緯度，経度とも最大値の組み合わせ(c|d)を終点とした位置情報をサービスに公開する．これは，4 点(a|b)，(a|d)，(c|b)，(c|d)に囲まれたエリアを示す．

(4) 定性的・定量的議論

ヒューマンプローブをはじめ，移動体プローブの実環境でのアクセスツールとなる，GPS 機能付スマートフォンを例に，LOXY II の QoS（Quality of Service）を議論する．

東京都渋谷区，神奈川県藤沢市，関東全域での第 n 階層における各地域の平均アノニミティセットを算出した結果を図 3 に示す．実

[1] Andreas Pfitzmann 氏，Marit Kohntopp 氏は，匿名性を“the state of being not identifiable within a set of subjects”，アノニミティセットを“the set of all possible subjects who might cause an action”と定義しており，匿名性はアノニミティセットに比例するとした．

線は全携帯端末数，点線はGPS機能付スマートフォン数を示しており，第7，8，9階層の粒度はそれぞれ(18 m)^2，(36 m)^2，(71 m)^{2}である．

東京都渋谷区においてサービスが第 9，7 階層の位置情報を取得した例を図 4 に示す．(a)は実際にユーザが歩いた道のり，(b)，(c)は取得した位置情報が第9階層，第7階層の場合である．(b)はユーザの移動履歴を大まかに示す程度である一方，(c)はユーザの歩いた道のりを相当な精度で示している．

直感的にも明らかなように,公開された位置情報の粒度によってはサービスが充分なQoS を発揮できない事態が想定される．したがって，サービスが取得した位置情報よりも更に細かい粒度の位置情報を要する場合，細かい粒度の位置情報が必要な理由などを記したプライバシポリシをユーザに提示し，該当粒度による位置情報の参照を申請する拡張機能を考慮する必要がある.LOXY II では，ユーザは，要求された位置情報の粒度を公開した際のアノニミティセットと，享受できるサービスのQoSを照らし合わせて要求を承諾するか否かを決定できる．

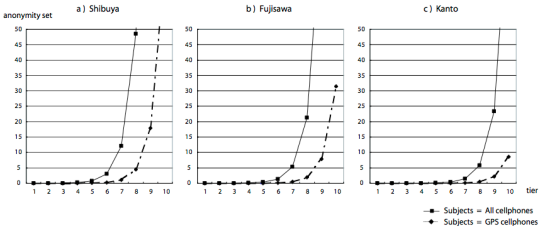

図 3 階層・エリア別アノニミティ

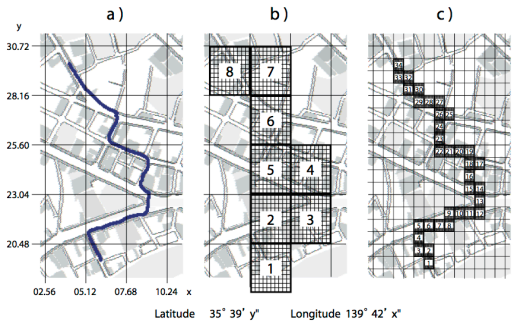

図 4 公開位置情報

(4) まとめ

移動体プローブがサービスに公開した個人情報，特に位置情報が悪用された場合において，ユーザが被るプライバシの侵害を抑えるサービスフレームワークを提案し，各種実験を通して，その有用性を評価した．本研究課題の成果は，従来は「個人情報を公開するか否か」の二極でしか選択肢を持てなかったユーザが，情報の匿名化によって「この程度の匿名性で情報を公開する」といった中間解を選択できるようになる恩恵を，実証的に示した点にその意義がある．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 2 件）

1. 伊藤昌毅・高汐一紀・他，“Chameleon：多様な状況下の機器指定を実現する複数インタラクション統合技術”，情報処理学会 論文誌，52 (4)，pp.1571-1585，2011.（査読あり）
2. 青木崇行・高汐一紀・他，“制御ルールを考慮したセンサアクチュエータネットワーク機構の構築”，情報処理学会 論文誌 コンピューティングシステム（ACS)，2 (2)，pp.178-191，2009.（査読あり）

〔学会発表〕（計 11 件）

1. Takuya Takimoto, Kazunori Takashio, et al.,“Lupe: Information Access Method based on Distance between User and Sensor Nodes using AR technology”, ACM 13th International Conference on Ubiquitous Computing (Ubicomp 2011), Demo Paper, September 17-21, 2011, Beijing, China.（査読あり）
2. Tetsuro Horikawa, Kazunori Takashio, et al.,“PACUE: Efficient Heterogeneous Processor Allocations in PCs”, Workshop on UnConventional High Performance Computing 2011 (UCHPC 2011), August 29, 2011, Bordeaux, France.（査読あり）
3. 瀧本拓哉・高汐一紀・他，“Lupe：AR 技術を用いた対象とユーザの距離に基づいた情報取得手法”，情報処理学会 UBI 研究会 第 31 回研究発表会，2011 年 7 月 14 日・15 日，九州大学 西新プラザ.
4. グエンザー・高汐一紀・他，“着座パターンによる人物特定アルゴリズムの提案”，情報処理学会 UBI 研究会 第 31 回研究発表会，2011 年 7 月 14 日・15 日，九州大学 西新プラザ.
5. 西山勇毅・高汐一紀・他，“野球選手の投球動作変化を用いた疲労度取得手法の提案”，情報処理学会 UBI 研究会 第 31 回研究発表会，2011 年 7 月 14 日・15 日，九州大学 西新プラザ.
6. Naoya Namatame, Kazunori Takashio, et al.,“UDS: Uninterruptible Sensor Data Supply for Sustainable Context Aware System”, 7th International Conference on Networked Sensing Systems (INSS 2010), June 15-18, 2010, Kassel, Germany.（査読あり）
7. Naoya Namatame, Kazunori Takashio, et al.,“SensingCloud: Open and Global

Sensor Network using Distributed Aggregation Mechanism”, Pervasive 2010 Workshop: Ubicomp in the Large: Collaborative Sensing and Collective Phenomena, May 17, 2010, Helsinki, Finland. (査読あり)

8. Takuya Takimoto, Kazunori Takashio, et al., “Extate: Visualizing wireless networks by using AR technology”, The 4th International Workshop on Ubiquitous Virtual Reality (IWUVR2010), May 17, 2010, Helsinki, Finland. (査読あり)
9. 青木崇行・高汐一紀・他, “u-Photo Mobile: 携帯電話上の静止画写真を用いたサービス可視化と制御”, 情報処理学会 ユビキタスコンピューティングシステム研究会, 2009 年 7 月 16 日, 京都けいはんな.
10. 山本純平・高汐一紀・他, “MOLMOD: 生体情報を用いた雰囲気を取得する手法の構築”, 情報処理学会 ユビキタスコンピューティングシステム研究会, 2009 年 7 月 16 日, 京都けいはんな.
11. Tomotaka Ito, Kazunori Takashio, et al., “Snappy: A Snap-based Human Interaction for Multiple Device Collaboration”, 7th International Conference on Pervasive Computing (Pervasive 2009), Demo Paper, May 11-14, 2009, Nara, Japan. (査読あり)

６．研究組織

(1)研究代表者

高汐 一紀 (TAKASHIO KAZUNORI)
慶應義塾大学・環境情報学部・准教授
研究者番号：４０２７２７５２

(2)研究分担者

なし

(3)連携研究者

なし