粒度の動的変更による位置匿名性についての考察

中西健一[†] 高汐一紀[††] 徳田英幸[††,†††]

未知のサービスが我々の位置に即したサービスを自律的に提供するユビキタスコンピューティング環境の実現へ向け，近年，多様なロケーションアウェアサービスが実用化，商用化されている．しかし一方で，公開した位置情報を不当に扱わ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いる．本研究では，公開した位置情報を悪用された場合に我々が被る損害を抑えることを目的としており，公開す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する．本フレームワークは，ユーザの望む程度の匿名性を満たすよう，公開する位置情報の粒度を動的に変更する．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．結果，従来は「位置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位置情報を公開する」といった中間解を選択できるようになる．

A Concept of Location Anonymization

Kenichi Nakanishi,[†] Kazunori Takashio[††] and Hideyuki Tokuda[††,†††]

Advances in location-sensing technologies enable ubiquitous applications to provide useful services based on our locations. While we enjoy these services, we are concerned about the violation of our privacy. The concerns are becoming more serious with the shift of service usage to more ubiquitous style where lots of unknown services might perceive our locations to implicitly provide beneficial services. This paper proposes a privacy preservation framework that reduces the damage of privacy-invasion, caused if malicious services try to share our footsteps. The framework discloses our location after location anonymization, the process to roughen the location granularity to keep a certain degree of anonymity. 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.

1. はじめに

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 付き携帯電話の普及は目覚ましく，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すでに実用化，商用化されている[1)]．

これらのサービスを享受する機会の増加にともない，我々の移動履歴が不当に把握されることに対する危機感も増加している．具体的には，複数のサービスに対して異なる移動履歴を公開した後に，それらのサービスによって移動履歴を不当に共有される事態が危惧される．この危機感を払拭しない限り，未知のサービスが自律的に我々の位置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[2),3)] の実現は困難となる．

ロケーションプライバシを保護するべく，すでに様々な手法が提案されてきたが，その多くは，位置情報を公開する前において，サービスのプライバシポリシに基づいて信頼できる（と想定できる）サービスを選別するにとどまっており，位置情報を公開した後における悪事については考慮していない．企業が，自身の公開したプライバシポリシを守らず個人情報を悪用していた事実が多く露呈されている昨今では，プライバシポリシが我々の要求を満たしていようとも我々はそのサービスを完全に信用できない．これらの点から，本

† アクセンチュア株式会社戦略グループ
Strategy & Business Architecture, Accenture Japan Ltd.
†† 慶應義塾大学大学院政策・メディア研究科
Graduate School of Media and Governance, Keio University
††† 慶應義塾大学環境情報学部
Faculty of Environment Information, Keio University

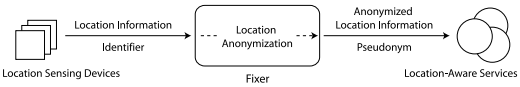

図 1 フレームワークコンセプト
Fig. 1 Concept of the framework.

研究では，ロケーションアウェアサービスを「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，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．

本研究では，公開した位置情報が悪用された場合においても我々が被る損害を抑えることを目的とし，公開す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する．**図 1** にその概要を示す．ユーザの信用対象である *loxy* は，GPS 端末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．結果，従来は「位置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位置情報を公開する」といった中間解を選択できるようになる．

以降，2 章において本研究の目的を明確にし，3 章で位置情報の匿名性を，4 章で本フレームワークの概要を説明する．5 章では一定の仮定に基づき，本フレームワークの **QoS**（*Quality of Service*），**QoP**（*Quality of Privacy*）について議論する．6 章では関連研究を示し，7 章でまとめる．

2. 本研究の目的

本章では，ロケーションプライバシの保護を目的とした既存研究に触れながら，本研究の目的を明確にする．

既存研究の多くは，サービスに公開する位置情報の絶対量を制限する手法を提案している[3)~6)]．ETH チューリッヒの Marc Langheinrich 氏やアリゾナ大学の Ginger Myles 氏は，サービスのプライバシポリシがユーザのプライバシプレファレンスの条件を満たす場合に限り，ユーザの位置情報をサービスに公開する手法を提案している．位置情報の公開条件例としては，時間，場所，コンテクストなどが言及されており，遊園地内においては園内ナビゲーションサービスに，勤務中は会社の勤怠管理サービスに位置情報を公開する，といった利用形態が想定できる．しかし，これらの手法は公開する位置情報を制限する一方，公開した位置情報を悪用される危険性について考慮していない．

前述のとおり，本稿において位置情報の悪用とは複数のサービスによる位置情報の共有を指す．ドレスデン工科大学の Andress Pfizmann 氏らは，複数サービスによる特定ユーザの個人情報の共有を防ぐために，サービスごとに異なる仮識別子を適用する手法を提案している[7)]．しかし，異なる識別子が同一ユーザの識別子であると判別される可能性がある．これを識別子の関連付けと定義する．サービス S が取得した識別子 x の位置情報の集合を $S(x)$ と表現する．サービス S_1，S_2 は，$S_1(a) \cap S_2(b)$ を発見できれば識別子 a，b を関連付けて $S_1(a) \cup S_2(b)$ を共有できる．本稿では，$S_1(a) \cap S_2(b)$ に該当する情報として，$L_{linkable}$ をあげる．

$L_{linkable}$ は，同一ユーザによる，同一時刻において同一位置を示す位置情報である．識別子 x の位置情報を $location(x)$ と表現すると，S_1 が $location(k) = L_a$ を，S_2 が $location(m) = L_a$ を連続した時間に取得し，そのタイミングに L_a に入ったユーザは 1 人だと判別できた場合，$L_a = L_{linkable}$ となり，k と m を関連付けられてしまう．この危険性は L_a に存在するユーザ数が少ないほど高くなる[8)]．

本研究の目的は，サービスによる $L_{linkable}$ の発見を各々のユーザが望む程度で防止することである．したがって，本研究における議論の対象は，公開された位置情報からユーザの移動履歴が正確に分かるか否かではなく，複数のサービスによって不当に移動履歴を共有されるか否かとなる．

3. 位置情報の匿名性

本章では，位置情報の匿名性について述べた後，匿名性の設定軸である *locset* について説明し，位置情報の匿名化について述べる．

3.1 位置情報の匿名性

匿名性を理論的かつ定量的に解釈した業績は，匿名通信機構を構築し，アノミティセットの概念を提案した David Chaum 氏の研究に端を発する[9)]．同氏の発表論文に基づき，匿名性についての関連用語を一般化，形式化した 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” と再定義しており，匿名性はアノニミティセットに比例すると明言している[7]．この概念の適用により，本稿では，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．

3.2 locset

本フレームワークは，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 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．

ユーザは各々のサービスに対して異なる信用度をいだくため，公開する位置情報の匿名性もサービスごとに変更できることが望ましい．しかし一方で，利用するすべてのサービスに対して各々の値を設定する手法はユーザにかかる負担が大きく，また，未知のサービスの利用が困難となる．本フレームワークでは，ユーザは locset をサービスタイプ，または特定のサービスに対して設定できる．サービスタイプに対する設定により，未知のサービスを即興的に利用できるようになり，特定サービスに対する設定により，信用度の高いサービスに対しては匿名性の低い位置情報を公開できるようになる．

3.3 位置情報の匿名化

位置情報を匿名化する際，loxy はすべての位置情報を階層化した状態で扱う．階層化の手法は 4.2 節で後述する．匿名化の概要を記した Java コードを**図 2** に示す．条件「該当位置のアノニミティセット ≧ locset」を確認し（3 行目），条件が満たされない場合には階層を 1 つあげる（4 行目）．条件を満たすまで確認処理を再帰的に行う（7 行目），条件を満たした時点の粒度で位置情報が公開される（6 行目）．locset=1 の場合は条件が必ず真となるので，GPS 端末から受信した位置情報がそのまま公開される．

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 $L_{linkable}$ を発見し，識別子を関連付けられる．これを防ぐため，loxy 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．

```
01 Area anonymize(Area area, int locset){
02    do{
03       if( area.anonymitySet() < locset )
04          area = area.getParent();
05       else
06          return area;
07    }while( area.hasParent() );
08    return null;
09 }
```

図 2 位置情報の匿名化
Fig. 2 Location anonymization.

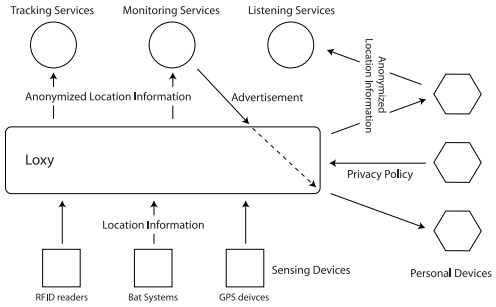

図 3 フレームワーク
Fig. 3 Framework.

ユーザは locset をサービスタイプや特定サービスごとに変更できるため，同一ユーザの移動イベントであっても複数のサービスに対して異なる粒度で公開されることが推測され，サービスが位置情報を悪用するのはさらに困難になる．

4. フレームワーク概要

本章では，本フレームワークの概要として，位置取得技術，位置情報形式，位置匿名化処理，サービスタイプについて述べる☆．本フレームワークの概要を**図 3** に示す．

4.1 位置取得技術

本稿では，ユーザが GPS 端末を携帯しており，GPS 端末がユーザの位置情報を継続的に loxy へ通知する環境を想定している．現実に，この形式で位置情報を取得するサービスが出現し始めており，携帯端末が継続的に位置情報を発信し続ける形式は今後一般化していくと予想される．

loxy は継続的にユーザの位置情報を受信するが，そのたびにサービスに対して移動イベントを発行するとは限らない．ユーザの位置情報は，サービスタイプ，または特定のサービスに対して設定されたユーザのプ

☆ 位置取得技術，位置情報形式とも，本稿における議論に必要な部分のみに言及する[10]．

```
 1 <?xml version="1.0" encoding="UTF-8" ?>
 2 <request type="location_info">
 3    <location type="absolute">
 4       <device id="gps42b6da18c93e5f7" />
 5       <datum>wgs84</datum>
 6       <unit>dms</unit>
 7       <lat>35,20,12.24</lat>
 8       <lon>138,59,49.59</lon>
 9       <note><alt>30</alt></note>
10    </location>
11 </request>
```

図 4 絶対座標系位置情報
Fig. 4 Absolute location model.

ライバシプレファレンスに従って公開される．

4.2 位置情報形式

GPS 端末は，絶対座標系の形式で位置情報を loxy へ通知する．絶対座標系は，デバイス識別子と緯度経度が記述された位置情報であり，GPS 端末や Galileo 端末からの受信を想定して定義されている．**図 4** に示されるように，位置情報には，デバイス識別子（4 行目），測位系（5 行目），座標系（6 行目），緯度経度（7，8 行目），備考（9 行目）が含まれる．座標系は度分秒表記（DMS）と度分表記（DM.M），10 進表記（D.D）のいずれかで表記される．

位置情報を匿名化するためには位置情報を階層化する必要がある．loxy 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 $(1/100\text{ 秒})^2 = 7.8 \times 10^{-2}\,\mathrm{m}^2 \fallingdotseq (28\,\mathrm{cm})^2$，最も粗い粒度の位置情報は $(1\text{ 分})^2 = 2.8\,\mathrm{km}^2$ となる☆．最小粒度 $(28\,\mathrm{cm})^2$ 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 $\geqq 2$ 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 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 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 $\geqq$ 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，**図 5** に示すように，緯度，経度とも最小値の組合せ $(a|b)$ を始点（7〜10 行目），緯度，経度とも最大値の組合せ $(c|d)$ を終点（11〜14 行目）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．

```
 1 <?xml version="1.0" encoding="UTF-8" ?>
 2 <event>
 3    <pseudonym>levowelvnm</pseudonym>
 4    <location type="gps">
 5       <datum>wgs84</datum>
 6       <unit>dms</unit>
 7       <origin>
 8          <lat>35,20,10.24</lat>
 9          <lon>138,59,48.64</lon>
10       </origin>
11       <terminal>
12          <lat>35,20,12.79</lat>
13          <lon>138,59,51.19</lon>
14       </terminal>
15       <note><alt>30</alt></note>
16    </location>
17 </event>
```

図 5 公開位置情報
Fig. 5 Disclosed location information.

表 1 サービス分類
Table 1 Service types.

	Tracking	Monitoring	Listening
対象ユーザ	特定	—	—
対象エリア	—	特定	—

4.3 ロケーションアウェアサービス

本フレームワークでは，**表 1** に示されるように，ロケーションアウェアサービスを対象エリア，対象ユーザの違いからトラッキングサービス，モニタリングサービス，リスニングサービスに分類している．それぞれの特徴を**表 2** に示す．

4.3.1 トラッキングサービス

トラッキングサービスは特定ユーザの移動を一定期間追跡する．例として，外回りに出ている部下の移動を把握する勤怠管理サービスや，行動履歴からユーザの嗜好を推測し，ユーザの好みそうなスポットを推薦するナビゲーションサービスなどがあげられる．

loxy は，ユーザが許可する期間に限り，移動イベントをトラッキングサービスに通知する．移動イベントにはサービスごとに異なる仮識別子が付加される．ユーザは，サービスに同一人物としてトラッキングされたい任意の期間，同一の仮識別子を適用できる．同一の仮識別子を長期間適用するほど位置情報を悪用される危険性は高まるので，必要がなければ仮識別子は

☆ 東京都付近において，1 分あたり，緯度約 31 m，経度約 25 m.
☆☆ 100 倍された秒の最大値は 5,999 であり，これを 2 進数で表現するには 13 桁必要である．
☆☆☆ 13 桁の 2 進数は 8,912 個の数を表現できるため，最大値が 60 を超える可能性がある．その場合は最大値を 59.99 とする．

表 2 サービス特性
Table 2 Service characteristics.

Service Type	Tracking	Monitoring	Listening
利用形態	プッシュ型	プッシュ型	プル型
位置取得元	loxy	loxy	ユーザ端末
プレファレンス	各サービス	サービスタイプ	—

```
 1 <?xml version="1.0" encoding="UTF-8" ?>
 2 <policy>
 3    <services type="tracking">
 4       <service address="tracker.zii.jp" port="2403">
 5          <locset>5</locset>
 6          <period type="time">
 7             <day>weekday</day>
 8             <start>13:00</start>
 9             <finish>17:00</finish>
10          </period>
11          <expiration>2005-03-31</expiration>
12       </service>
13       <service address="ls.keio.ac.jp" port="2403">
14          <locset>10</locset>
15          <period type="ondemand" />
16          <expiration>2004-10-12</expiration>
17       </service>
18    </services>
19    <services type="monitoring">
20       <locset>10</locset>
21       <period>10</period>
22       <advertisement>ken@realken.com</advertisement>
23       <service address="monitor.zii.jp" port="2403">
24          <pseudonym type="perdurable" />
25          <locset>1</locset>
26          <period />
27          <advertisement>ken@socueus.com</advertisement>
28          <expiration>2004-10-12</expiration>
29       </service>
30    </services>
31 </policy>
```

図 6 プライバシプレファレンス
Fig. 6 Privacy preference.

頻繁に変更することが望ましい．

ユーザは，利用したい各々のトラッキングサービスに対してプライバシプレファレンスを記述する（**図 6**，3〜18 行目）．loxy は，GPS 端末から位置情報を受信すると，該当ユーザのプレファレンスから，その時点がトラッキング許可期間に該当するサービスエントリを確認する．エントリが存在する場合，該当エントリに記述された locset に基づいて位置情報を匿名化する．その結果が前回の匿名化の結果と異なる場合，該当サービスに適用している仮識別子を添えて，エントリに記述されたアドレスへ移動イベントを通知する．

4.3.2 モニタリングサービス

モニタリングサービスは，特定エリア内における任意ユーザの移動を把握する．例として，スーパで買物中のユーザにまだ回ってないコーナにおける特売情報を通知するサービスや，テレビを視聴中のユーザが移動すると移動先のディスプレイに映像出力を切り替えるサービスなどがあげられる．サービスからメッセージを受信する場合には，ユーザは携帯電話や PDA などの端末を携帯している必要がある．

モニタリングサービスは，基本的にユーザが対象エリアに入るたびに異なるユーザとして認識し，対象エリア内のみにおいてユーザを識別，追跡する．したがって loxy は，ユーザがサービスの対象エリアに入るたびに新たな仮識別子を生成し，ユーザが該当エリアを出るまでの間，その仮識別子を適用する．サービスは，ユーザの仮識別子を用い，loxy を解してユーザ端末へメッセージを配信できる．

ユーザは，サービスタイプに対してプレファレンスを設定する（図 6，19〜22 行目）．必要であれば，特定のサービスに対して固有の値を設定できる（23〜30 行目）．全モニタリングサービスを把握している loxy は，GPS 端末から位置情報を受信すると，該当位置を対象エリアとしたサービスの有無を確認する．サービスが存在する場合，該当ユーザのプレファレンスから，そのサービスに対するエントリがあるか確認する．エントリがある場合は該当エントリを，ない場合にはサービスタイプに対するエントリを適用する．その時点がエントリ内のトラッキング許可期間に該当する場合，該当エントリに記述された locset に基づいて位置情報を匿名化する．その結果が前回の匿名化の結果と異なる場合，該当サービスに適用している仮識別子を添えて（初回の場合は新たに生成）移動イベントを発行する．

4.3.3 リスニングサービス

リスニングサービスはユーザ端末から位置情報を受信し，該当位置に適した情報を返答する．ユーザはサービスを利用するために携帯電話や PDA などを用いる必要がある．例として，近隣にあるレストランを検索するサービス，最寄駅の時刻表を表示するサービスなどがあげられる．これらは，位置取得機能付き携帯電話の浸透により我々にとって馴染み深いサービスである．

リスニングサービスは基本的にユーザを識別せず，リクエストを受信するたびに異なるユーザからの要求として認識する．よって，位置情報に仮識別子などは付加されない．サービスがユーザを認識，認証する必要がある場合は，ユーザ端末とサーバ間で認証処理を行えばよく，本フレームワークでその方法を規定する

必要はない．

プライバシプレファレンスにリスニングサービス用のエントリは存在しない．loxy は，ユーザ端末から locset を受信し，その値に基づいて匿名化した位置情報を返信する．ユーザ端末は受信した位置情報をサービスへ公開する．

5. 考　　察

本章では，携帯電話端末数，GPS 付き携帯電話端末数に基づき，位置情報の匿名化によって公開される位置情報の粒度を推測し，本フレームワークの **QoS**，**QoP** について考察する．

5.1 シミュレーション

関東地域において，携帯電話，GPS 付き携帯電話の普及率は一律であるとの仮定に基づき，人口密度 d_{pop}[people/km^2] のエリア r_n[km^2] における携帯電話端末数 $as_{all}[subjects]$，GPS 付き携帯電話端末数 $as_{pgs}[subjects]$ を以下の式から求める☆．GPS 付き携帯電話端末数は急速に増加しており，as_{gps} は as_{all} に近づきつつある．

$$as_{all} = d_{pop} \times 0.76 \times r_n \quad [subjects]$$

$$as_{gps} = d_{pop} \times 0.06 \times r_n \quad [subjects]$$

絶対座標系位置情報における第 n 階層の粒度 r_n は $7.8 \times 4^{n-1} \times 10^{-8}$ [km^2] $(0 < n < 14)$ となる☆☆．

これらの式に，東京都渋谷区，神奈川県藤沢市，関東全域における d_{pop} 12,500，5,500，1,500 [people/km^2] を適用して，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 7** に示す．実線は as_{all} を，点線は as_{gps} を示しており，第 7，8，9 階層の粒度はそれぞれ $(18\,\mathrm{m})^2$，$(36\,\mathrm{m})^2$，$(71\,\mathrm{m})^2$ である．また，対象物が 2 次元空間上に均等に分散しているとの仮定に基づき，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 8** 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．以降，図 7，8 に基づき本フレームワークの QoS について考察する．

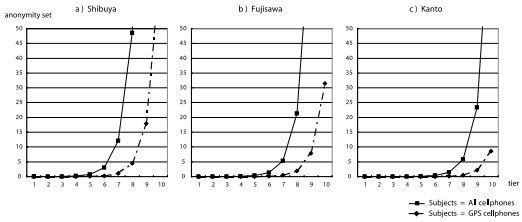

図 7 階層，エリア別アノニミティセット
Fig. 7 Simulated anonymity sets.

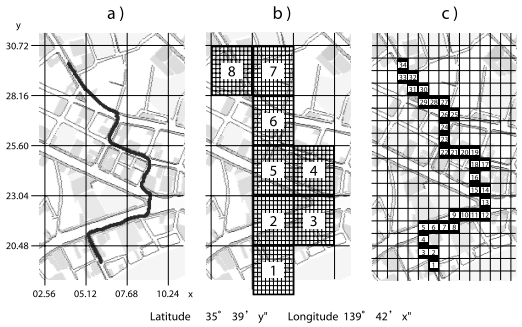

図 8 公開位置情報（ユーザ分布が均一の場合）
Fig. 8 Disclosed location information - i.

5.2 QoS: Quality of Service

4.2 節で述べたとおり，サービスは，匿名化された位置情報として，ユーザの存在するグリッドの始点と終点を受信する．サービスは，該当グリッド内においてユーザが存在している点を，始点，もしくは始点と終点の中間（グリッドの中心）などと仮定できるため，匿名化された位置情報のためにサービスが利用できなくなる事態は想定されない．しかし，該当位置の仮定は可能でも断定は不可能であるため，グリッドの粒度によってはサービスの QoS に影響が生じる．

図 7 から，地域によって開きが生じるが，およそ第 7，8，9 階層周辺である程度のアノニミティセットを確保できることが分かる．第 9 階層の粒度 $(71\,\mathrm{m})^2$ は，端から端まで徒歩 1，2 分で移動できる距離であり，図 8–b が示すよう，単一グリッド内に複数の道が存在している可能性が高く，サービスは受信した位置情報からユーザの大まかな移動履歴は把握できるが，ユーザの歩いた道を断定するには至らない．よって，この粒度の位置情報では，近隣のレストランや最寄駅の時刻表を検索するサービスは QoS を損なわずにサービスを展開できるが，歩行者を対象としたナビゲーションサービスや近隣で空車のタクシーを配車するサービスは QoS を損なう可能性がある．一方，第 7 階層の粒度 $(18\,\mathrm{m})^2$ は，端から端まで徒歩 1，20 秒

☆ 2004 年 1 月時点，関東地域において，人口は約 40,280 千人，携帯電話契約数は約 30,580 千台，GPS 付き携帯電話契約数は 2,560 千台である．よって，携帯電話，GPS 付き携帯電話の普及率はそれぞれ 30,580/40,280 = 0.76，2,560/40,280 = 0.06 と算出できる．

☆☆ 4.2 節で述べたとおり，絶対座標系の位置情報は 14 層に階層化され，最下層の粒度は $7.8 \times 10^{-8}\,\mathrm{km}^2$，階層があがると粒度は 4 倍となる．

で移動できる距離であり，図 8–c が示すよう，単一グリッド内に複数の道が存在している可能性は稀であり，サービスは受信した位置情報からユーザの歩いた道筋をかなりの精度で把握できる．よって，この粒度の位置情報では，ナビゲーションサービスやタクシー配車サービスも，QoS を損なわずに正確な道案内や敏速なタクシー配車などのサービスを提供できる．

以上の考察から，公開された位置情報の粒度によってはサービスが十分な QoS を発揮できない事態が想定される．したがって，実用化に向けては，サービスが取得した位置情報よりもさら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．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．例として，locset を 30 に設定したユーザが，渋谷区において第 8 階層の位置情報を公開している場合を想定する．第 7 階層の粒度で位置情報を参照する必要のあるサービスは，その旨を記したプライバシポリシをユーザに提示する．ユーザは「4 人以上 13 人以下が同じエリアに存在する粒度で位置情報を公開する☆」ことを承諾して QoS の高いサービスを享受するか否かを，プライバシポリシに基づき決定できる．

図 7 から，公開される位置情報の粒度は，該当地域の人口密度によって異なることが理解できる．一時的な人口密度の減少によって位置情報の粒度が粗くなるたびにユーザへ細かい粒度の位置情報を公開する許可を申請するのは非現実的なため，上述の拡張機能は，サービスが望むよりも粗い粒度の位置情報を一定回数以上連続して受信した後にのみ実行される．しかし，永続的に人口密度が極端に少ない地域においては，locset を低く設定しない限り，拡張機能が頻繁に実行される可能性がある．本研究では，サービスを信用に足らないエンティティと想定しているため，サービスのプライバシポリシに基づいて情報公開の是非を決定する本拡張機能は，使い始め時における実用的な locset の範囲の学習や，例外的に細かい粒度の位置情報を要求された際など，あくまで補助的利用にとどめておくべきである．したがって，人口密度の低い農村部では位置情報の匿名性を犠牲にする可能性が高く，人口密度の高い都市部であるほど，高い匿名性で粒度の細かい位置情報を公開できるため，本フレームワークの実用性が高いといえる．

☆ 図 7–a から，第 7 階層におけるアノニミティセットは $3 <$ locset < 13

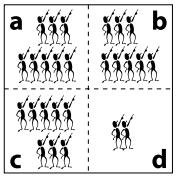

図 9 公開位置情報（ユーザ分布が偏った場合）
Fig. 9 Disclosed location information - ii.

5.3 QoP: Quality of Privacy

前節では，対象ユーザが 2 次元空間上において均等に拡散している想定に基づき公開位置情報を算出したが，実際には場所，時間によってユーザの分布具合は異なる（それらを平均すると前節の結果に近づく）．以降，ユーザの分布が異なる場合の単純な例を示し，サービスが $L_{linkable}$ を発見できる可能性について検証する．

$L_{linkable}$ を発見するためには，該当位置のアノニミティセットを取得するか，同一エリアに 2 人以上が存在できない粒度の位置情報を取得する必要がある．本フレームワークにおいて前者は不可能である．したがって，後者の可能性を検証するために，取得した位置情報よりも細かい粒度でユーザの位置を推測できる可能性について考察する．

単純な例として，**図 9** に示すような，4 グリッドのうち 1 つのみアノニミティセットが極端に少ない場合を想定する．グリッド a，b，c におけるアノニミティセットを n，グリッド d におけるアノニミティセットを $m(m << n)$ とし，すべてのユーザが $m <$ locset $\leqq n$ に設定していた場合，a，b，c に存在するユーザは最小グリッドの粒度で位置情報を公開し，グリッド d に存在するユーザのみが 1 階層上の粒度で位置情報を公開する．サービスが，各ユーザの設定した locset，もしくは各グリッドのアノニミティセットを取得できれば「実線グリッドの粒度で位置情報を公開したユーザはグリッド d に存在する」事実を導けるが，本フレームワークにおいてはどちらの値も参照不可能である．よって，サービスが取得した位置情報以上の粒度で該当ユーザの位置を推測するのは困難である．

以上の考察から，$L_{linkable}$ を発見できる確立は単純に「1 / 同一位置に存在しているユーザ数」に近似した値となり，locset に反比例して低くなる．

6. 関 連 研 究

本章では，ロケーションプライバシの保護を目的と

した関連研究として，pawS，Geopriv，Mix Zone について述べる．

6.1 pawS

本フレームワークと同様，未知のサービスも即興的に利用できる要件を考慮した関連研究として，ETH チューリッヒの Marc Langheinrich 氏が提案した pawS があげられる[3]．pawS では，サービスが公表している *Privacy Policy* がユーザの設定した *Privacy Preference* の条件を満たす場合，サービスに位置情報を公開する．

pawS では，位置情報の参照目的や管理方法などに基づき，位置情報を公開するサービスを選択できる一方，一度公開した位置情報を悪用される危険性については対応しておらず，法による規制の必要性を説いている．また，pawS では，特定のエリアにおいて任意のユーザを対象にしたサービスに主眼を置いているため，モニタリングサービスとリスニングサービスに対応しているが，特定のユーザを追跡し続けるトラッキングサービスには対応していない．

6.2 Geopriv

本フレームワークと同様，位置情報の粒度を変更する要件を考慮した関連研究として，IETF の Geopriv ワーキンググループがあげられる[6]．Geopriv では，ユーザが各サービスに対して設定した *Privacy Rule* に基づき位置情報を公開する．

Geopriv は，Privacy Rule 設定軸の例として公開位置情報の精度・粒度をあげているが，ユーザが具体的にどのように公開する粒度を設定し，どのように粒度が変更され，どのような形式で公開されるのか明記されていない．また，ユーザは利用するすべてのサービスに対して Privacy Rule を設定する必要があるため，未知のサービスを即興的に利用できない．

6.3 Mix Zone

本フレームワークと同様，識別子の関連付けを防止する要件を考慮した関連研究として，ケンブリッジ大学の Alastair Beresford 氏，Frank Stajano 氏の研究があげられる[11]．両氏は，識別子の関連付けを防ぐため，あるグループのメンバ全員がどのサービスにも位置情報を公開していないエリアを *Mix Zone* と定義して，Mix Zone 内でサービスに公開する識別子を変更する手法を提案している．両氏は，Mix Zone により識別子の変更時における匿名性を満たすことを目的としている一方，本研究では粒度の動的変更により単一位置情報自身の匿名性を満たすことを目的としている．

同手法では，ユーザがいずれかのグループに所属する点，グループのメンバ全員が位置情報を公開しない Mix Zone が存在する点から，特定コミュニティにおけるサービスに適しているが，不特定多数のユーザを対象にする公共空間においては，メンバのグルーピング方法や，Mix Zone の存在などが実現性に欠ける．また，ユーザは利用するすべてのサービスを事前に登録する必要があるため，未知のサービスを即興的に利用できない．

7. ま と め

本稿では，サービスに公開した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た．本フレームワークにおいて，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指定できる．locset の値が大きいほど，公開する位置情報の匿名性は高くなり，複数のサービスによる不当な移動履歴の共有は困難になる．locset の設定を含むプライバシプレファレンスは，対象ユーザ，対象エリアの差異に基づき分類されたトラッキング，モニタリング，リスニングサービスの各サービスタイプごとに，それぞれ適切な手法で設定される．

本稿では，携帯電話端末数と GPS 付き携帯電話端末数に基づき，本フレームワークを利用した際の QoS と QoP について議論した．QoS に関しては，正確な位置を要求しないサービスは，匿名化された位置情報を用いて十分なサービスを提供できることが分かった．正確な位置を要求するサービスが匿名化された位置情報を用いて QoS を損なうか否かは，ユーザが存在する地域の人口密度やユーザが設定した locset の値によって異なることも確認できた．QoP に関しては，位置匿名化によって，サービスによる $L_{linkable}$ の発見をユーザの望む程度で防げることが分かった．

本稿は，従来は「位置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，位置匿名化によって「この程度の匿名性で位置情報を公開する」といった中間解を選択できるようになる恩恵を示した点にその意義がある．

参 考 文 献

1) Abowd, G.D., Dey, A.K., Brown, P.J., Davies, N., Smith, M. and Steggles, P.: Towards a Better Understanding of Context and Context-Awareness, *Proc. 1st international symposium on Handheld and Ubiquitous Computing*, pp.304–307, Springer-Verlag (1999).
2) Weiser, M.: The Computer for the 21st Century, *Scientific American*, Vol.265, No.3,

pp.66–75 (1991).
3) Langheinrich, M.: A Privacy Awareness System for Ubiquitous Computing Environments, *Proc. Ubicomp 2002*, Lecture Notes in Computer Science, Vol.2498, pp.237–245, Springer-Verlag (2002).
4) Ginger Myles, A.F. and Davies, N.: Preserving Privacy in Environments with Location-Based Applications, *IEEE Pervasive Computing*, Vol.2, No.1 (2003).
5) Cranor, L., Langheinrich, M., Marchiori, M., Presler-Marshall, M. and Reagle, J.: The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, W3C Recommendation (2002).
6) Cuellar, J. and Morris, D.M.J.: Request for Comments: 3693 Geopriv Requirements. http://www.ietf.org/rfc/rfc3693.txt
7) Pfitzmann, A. and Kohntopp, M.: Anonymity, Unobservability, and Pseudonymity — A Proposal for Terminology, *International Workshop on Design Issues in Anonymity and Unobservability 2000*, Lecture Notes in Computer Science 2009, pp.1–9, Springer-Verlag (2000).
8) Rodden, T., Friday, A., Muller, H. and Dix, A.: A Lightweight Approach to Managing Privacy in Location-Based Services, Technical Report Equator-02-058 (2002).
9) Chaum, D.L.: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability, *J. Cryptology*, Vol.1, No.1 (1988).
10) 中西健一，高汐一紀，中澤　仁，徳田英幸：位置情報の動的変更によるプライバシ保護機構，日本ソフトウェア科学会 SPA2004 (2004).
11) Beresford, A.R. and Stajano, F.: Location Privacy in Pervasive Computing, *IEEE Pervasive Computing*, Vol.2, No.1 (2003).

(平成 17 年 2 月 9 日受付)
(平成 17 年 7 月 4 日採録)

中西　健一

1979 年生まれ．慶應義塾大学環境情報学部在籍中，2000 年 4 月より徳田研究室所属．主な研究テーマはユビキタスコンピューティング環境におけるプライバシ・セキュリティ保護．研究に従事する一方，2002 年 3 月ソフトウェア開発業開業，同年 7 月株式会社ソキュアス技術顧問役拝命．2004 年 9 月慶應義塾大学大学院政策・メディア研究科修士課程修了．現在，アクセンチュア株式会社戦略グループ在籍．

高汐　一紀（正会員）

1967 年生まれ．1995 年慶應義塾大学大学院理工学研究科後期博士課程単位取得退学．電気通信大学電気通信学部情報工学科助手を経て，現在，慶應義塾大学環境情報学部助教授．主に，分散実時間システム，小型デバイス向けモバイルアプリケーション，ユビキタスコンピューティングの研究に従事．日本ソフトウェア科学会，ACM，IEEE 各会員．博士（工学）．

徳田　英幸（正会員）

1952 年生まれ．慶應義塾大学より工学修士．カナダ，ウォータールー大学より Ph.D.（Computer Science）．現在，慶應義塾大学大学院政策・メディア研究科委員長．分散リアルタイムシステム，マルチメディアシステム，通信プロトコル，超並列・超分散システム，ユビキタスシステムなどの研究に従事．IEEE，ACM，日本ソフトウェア科学会各会員．