様式Ｃ-19

科学研究費補助金研究成果報告書

平成２１年５月３１日現在

研究種目：基盤研究（C）
研究期間：2006～2008
課題番号：１８５００９１
研究課題名（和文）　ユビキタス情報空間におけるロケーションプライバシ保護機構とその評価

研究課題名（英文）　Location Privacy Protection in Ubiquitous Information Spaces

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：
本研究課題では，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，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した．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」といった中間解の選択が可能となった．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００６年度	1,500,000	0	1,500,000
２００７年度	1,000,000	300,000	1,300,000
２００８年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,500,000	600,000	4,100,000

研究分野：総合領域
科研費の分科・細目：情報学，メディア情報学・データベース
キーワード：モバイルシステム，ユビキタスコンピューティング

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．

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，我々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いる．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る．

２．研究の目的

本研究の目的は，従来，その利便性のみが議論されてきた公共空間におけるロケーションアウェアサービスを対象に，現在位置や移動履歴を望まない第三者から隠蔽する権利，すなわち，ロケーションプライバシの問題を取り上げ，その保護機構および位置匿名化アルゴリズムを示すとともに，実システム上での評価実験を通して，様々な条件下での，基本性能（運用性），安全性，ユーザビリティ，の各指標を示し，提案アルゴリズムの有効性を実証的に検証することにある．本研究では，既存の位置取得技術を，そのセンシング手法から，(L-I) ポジショニング法，(L-II) トラッキング法，の二種類に分類，さらに，ロケーションアウェアサービスを，その対象となるエリアおよびユーザの違いから，（S-I）トラッキングサービス，(S-II) モニタリングサービス，(S-III) リスニングサービス，の三種類に分類する．まず，簡略化した問題として，「ユーザあるいはエリアを特定可能なロケーションアウェアサービス」を想定し，徐々に問題を「ユーザ，エリアともに特定困難なサービス」に一般化，アルゴリズムの提案と実装，評価を通して，ロケーションプライバシ保護アーキテクチャの詳細を議論する．

３．研究の方法

平成 18 年度

研究計画初年度の平成 18 年度は，簡略化した問題として，「ユーザあるいはエリアを特定可能なロケーションアウェアサービス」を想定し，申請者らが提案しているロケーションプライバシ保護アーキテクチャ location proxy（以下，LOXY）の再検討および拡張を行った．これにより，「匿名性の指標 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，公開位置情報の匿名性を指定できるようになった．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，サービスによる位置情報の悪用を防げるようになる．本フレームワークは，ロケーションアウェアサービスを，その対象となるユーザおよびエリアの違いから，トラッキング，モニタリング，リスニングサービスに分類し，サービスタイプごとに適したプライバシプレファレンスの設定手法を提供している．本成果の意義は，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ある．

平成 19 年度

研究計画 2 年目となる平成 19 年度は，前年度での問題を一般化し，「ユーザ，エリアともに特定困難なサービス」を対象とした場合の位置匿名化問題を扱った．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．

併せて，対象エリアを屋内から屋外へ拡張し，新たに屋外実験プラットフォームを構築，一般化された位置匿名化アルゴリズムを実験プラットフォーム上に実装，評価した．屋外では，屋内環境と異なり，GPS 等によるポジショニング法による位置取得が中心となる．現実に，GPS 付き携帯電話が位置情報を継続的に通知し続ける形態のサービスが出現し始めており，今後，一般化していくものと予想される．LOXY アーキテクチャを実験プラットフォーム上に実装し，GPS によるポジショニングの下，適当な条件の下で動作させ，データを収集，理論的な予測値との比較と併せて，実装されたアルゴリズムの詳細な性能を，基本性能（運用性），安全性，ユーザビリティの軸で評価した．

平成 20 年度

本研究計画の最終年度となる平成 20 年度は，位置匿名化アルゴリズムおよびロケーションプライバシ保護アーキテクチャの完成度を高めるとともに，より広範囲，より複雑な条件下での実証実験を行った．具体的には，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．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効性を実証的に検証した．本研究で検討した方式を統合的に評価，検証することで，GPS 等によるポジショニング法主体の屋外型位置取得インフラストラクチャと，RF-ID 等によるトラッキング法主体の屋内型位置取得インフラストラクチャの両者を，シームレスに支援可能なロケーションプライバシ保護環境を構築し，実用的な技術水準に到達することが可能となる目処が立った．

４．研究成果

本項では，本研究課題の主たる成果であるロケーションプライバシ保護アーキテクチ

ャについて述べる．

(1)概要

本研究課題では，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．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．

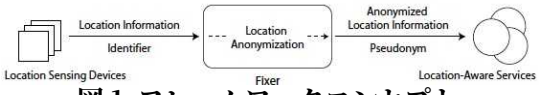

図 1 フレームワークコンセプト

(2)位置情報の匿名性

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．この概念の適用により，本研究課題では，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．

我々の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 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．

位置情報を匿名化する際，LOXY は全ての位置情報を階層化した状態で扱う．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．

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更に困難になる．

```
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

(3)匿名化処理

GPS 位置情報（度分秒表記（DMS））を例に，LOXY における位置情報匿名化処理の詳細を述べる．

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 x 10^{-2} m^2 $(28cm)^2$，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 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[1]．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 ≧ 1ocset」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)評価

GPS 機能付携帯電話端末を例に，提案フレームワークの QoS，QoP を評価する．

特定地域において，携帯電話，GPS 付携帯電話の普及率は一律であるとの仮定に基づき，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．実線は全携帯端末数，点線は GPS 機能付携帯端末数を示しており，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．

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 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．

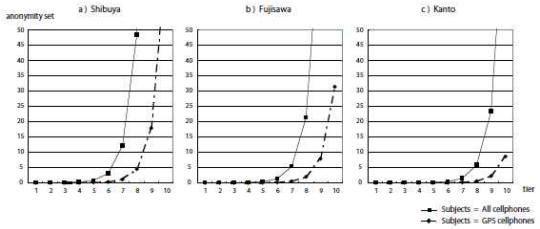

図 3 階層・エリア別アノニミティ

[1] 100 倍された秒の最大値は 5999 であり，これを 2 進数で表現するには 13 桁必要である．

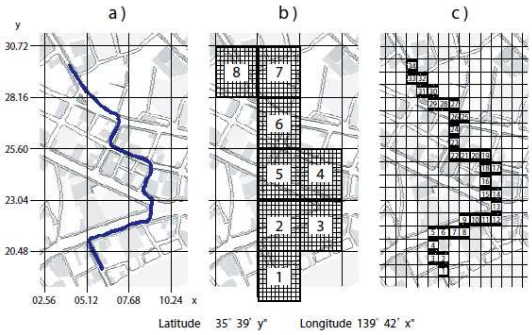

図 4 公開位置情報

① QoS: Quality of Service

前述の通り，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 3 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解る．第 9 階層の粒度(71 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 4 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(18m)^{2}は，端から端まで徒歩 1，20 秒で移動できる距離であり，図 4 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．提案フレームワークでは，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．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3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明らかである．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留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．

②QoP: Quality of Privacy

ユーザの分布が異なる場合の単純な例を示し，サービスによる識別子の関連付けの可能性について検証する．

サービスが識別子を関連付けするためには，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．提案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，本研究課題では，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議論した．

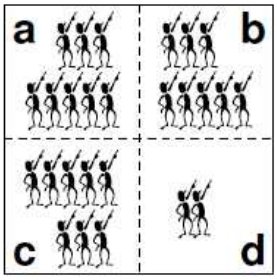

図5 ユーザ分布の偏り

単純な例として，図5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 ($m \ll n$)とし，全てのユーザが$m <$ 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一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．結果，関連付けが可能となる確率は単純に「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．

(5)まとめ

本研究課題では，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，その有用性を評価した．提案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．この値が大きいほど，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．

QoSとQoPに関する議論では，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充分なサービスを提供できることを確認できた．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，サービスによる関連付けをユーザの望む程度で防げることが解った．

本研究課題の成果は，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．

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　6 件）

1. 岩井将行・高汐一紀・他，“CroSSML －ネットワークロボット間の通信プロトコルの提案－”，電子情報通信学会誌，91（5），pp.366-373，2008.（査読有り）
2. 戸辺義人・高汐一紀・他，“アーバンセンシング基盤に向けて”，人工知能学会誌，23（4），pp.474-479，2008.（査読有り）
3. 山本秀典・高汐一紀・他，“環境適応サービスを狙いとしたミドルウェア相互接続の一方式”，電気学会論文誌（電子・情報・システム），128-C(8)，pp.1327-1332，2008.（査読有り）
4. 米澤拓郎・高汐一紀・他，“Spot & Snap: DIY Smart Object Service を実現するセンサノードと日用品の関連付けインタラクション”，情報処理学会論文誌，48（3），pp.1381-1392，2007.（査読有り）
5. 神武直彦・高汐一紀・他，“ユビキタス環境構築のためのブロック型情報機器連携技法”，情報処理学会論文誌，48（3），pp.1405-1416，2007.（査読有り）
6. Naohiko Kohtake，Kazunori Takashio，et.al.，“Self-Organizable Panel for Assembling DIY Ubiquitous Computing”，Springer-Verlag Personal and Ubiquitous Computing Journal，ONLINE FIRST，2006.（査読有り）

〔学会発表〕（計　9 件）

1. Kei Suzuki，Kazunori Takashio，et al.，“Toward Real-Time Extraction of Pedestrian Contexts with Stereo Camera”，5th International Conference on Networked Sensing Systems (INSS 2008)，pp.115-118，June 17-19，2008，Kanazawa，Japan.（査読有り）
2. 橋爪克弥・高汐一紀・他，“exPhoto: 周辺環境とユーザの心理状態を記録・再現するデジタルフォトメディアの構築”，人工知能学会 全国大会，2008 年 6 月 11-13 日，旭川．
3. 鈴木慧・高汐一紀・他，“Toward Real-Time Extraction of Pedestrian Contexts with Stereo Camera”，情報処理学会 第 18 回ユビキタスコンピューティングシステム研究会，2008 年 5 月 15・16 日，小樽．
4. Takuro Yonezawa，Kazunori Takashio，et al.，“uPackage: A Package to Enable Do-It-Yourself Style Ubiquitous Services with Daily Objects”，IPSJ 4th International Symposium on Ubiquitous Computing Systems，November 25-28，2007，Akihabara，Japan.（査読有り）
5. Takuro Yonezawa，Kazunori Takashio，et al.，“Towards A Better Understanding of Association between Sensor Nodes and Daily Objects”，1st International Workshop on Design and Integration Principles for Smart Objects，September 16-19，2007，Innsbruck，Austria.（査読有り）
6. Akinori Komaki，Kazunori Takashio，et al.，“ClickCatalog: Retracing Precious Memory using Paper-based Media Controller”，IEEE International Conference on Machine Learning and Cybernetics，August 19-22，2007，Hong Kong，China.（査読有り）
7. Ryo Osawa，Kazunori Takashio，et al.，“Smart Furoshiki: A Context Sensible Cloth for Supporting Human Life”，12th International Conference on Human-Computer Interaction，July 22-27，2007，Beijing，China.（査読有り）
8. 米澤拓郎・高汐一紀・他，“日常物とセンサノードの関連付け手法の提案”，情報処理学会 第 13 回ユビキタスコンピューティングシステム研究会，2007（14），pp.179-186，2007 年 2 月 22 日，秋葉原．
9. Ryo Osawa，Kazunori Takashio，et.al.“OreDesk: A Tool for Retrieving Data History Based on User Operations”，8th IEEE International Symposium on Multimedia，pp.762-765，December 11-13，2006，San Diego CA，USA.（査読有り）

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