

外部センサーを用いた行動履歴の個人蓄積システム

井上 知洋 中村 隆幸 中村 元紀 †

我々は、様々な場所に配置された各種センサーから得られる情報を利用して、個人の日常に関わる様々な履歴情報を記録し蓄積するシステム GreenTown を提案する。このシステムは、ユーザの位置推定などを行うユーザ識別部が監視カメラなどの各種外部センサーを制御して特定のユーザに関わる履歴情報を切り出した上で、履歴情報をそのユーザ個人が管理するストレージ領域に蓄積していく事の特徴とする。本稿では、既存のシステムが履歴情報の蓄積とユーザのプライバシー保護を両立する事が困難である事を示した上で GreenTown の構成を示し、ユーザのプライバシーを確保しつつ、履歴情報をユーザのストレージに一元的に蓄積していく手法を説明する。

A Personal Storage System for Daily Activity Recording Using External Sensors

Tomohiro INOUE Takayuki NAKAMURA Motonori NAKAMURA †

We propose a personal storage system “GreenTown” that records and stores everyday activities obtained from external sensors set in various public/semi-public places. This system consists of the user identification unit, the control unit of external sensors such as surveillance cameras, and the ubiquitous storage. With GreenTown system, user’s daily records are collected from external sensors and stored in the storage space that the user have own administration right of. In this paper, we explain the challenge of protecting users’ privacy, and show the architecture of GreenTown system that overcomes it.

1 はじめに

いわゆるユビキタス社会においては、様々なソースから得られる情報を蓄積して、将来のサービスに活用することが重要な意味を持つ。現在でも、電子メールをはじめとした容量の比較的小さな情報を長期間にわたって保存し活用することは一般的に行われている。最近では音声や映像といった、より大容量のデータを蓄積し活用する取り組みも、現実的な研究プロジェクトとして始まっている。例えば、MyLifeBits [1] では個人が一生のうちに体験する出来事についての様々な情報を PC のハードディスクに蓄積することを念頭に置いて、蓄積された情報を様々な場面で活用する方法について研究している。

個人の一生の情報を蓄積するためにどれくらいの記憶容量とコストが必要か、例えば 200 kbps の動画データの場合で考える。現在のハードディスクの容量単価 (100 円/GB) を考えると、一年分の動画データを保存するために必要なコストは、現時点において 80,000 円程度である。ハードディスクの容量単価は 2 年で半分になるという経験則を適用すると、総額 30 万円以下程度のコストで 50 年以上の長さの映像データを蓄積することが可能である。

このように記憶容量の面では、人が一生のうちに体験する出来事を記録し、将来のために蓄積しておく事は、既に十分現実的になってきている。

我々はこのような膨大な容量のストレージに、個人の日常の行動履歴を記録し、蓄積していくための枠組みについて研究を行っている。

以下、2 節において行動履歴を蓄積する際のアプローチや課題について説明し、3 節で我々の提案する行動履歴の個人蓄積システムの構成を示す。4 節では提案システムのもたらす効果を示し、関連研究との関係を 5 節で説明する。

2 個人行動履歴の蓄積

2.1 履歴情報の取得元センサーデバイス

ユーザの行動履歴を記録するためには、ユーザの行動に関わる情報 (以下、履歴情報と記す) を、様々な情報源を用いてできるだけ多く取得する事が望ましい。このとき、ユーザの行動をセンシングするデバイスは、ユーザ本人が所有するデバイスと、そうでないデバイスに分けて考える事ができる。

2.1.1 個人所有デバイス

前者は、デバイスの所有権およびセンシング対象がユーザ個人に強く結びついているデバイスである。ユーザが家の中などにおいて占有的に使用する PC や、ユーザが持ち運ぶデジタルカメラなどのポータブルデバイスなどが例として挙げられる。これらのデバイスが取得する情報は、基本的にデバイスを所有するユーザに関わる情報である。また、これらのデバイスは所有するユーザの管理権限下にある。このため、ユーザはこれらのデバイスからいつでも自身の行動履歴に関わる情報を引き出してくることができる。

† 日本電信電話 (株) NTT 未来ねっと研究所,
NTT Network Innovation Laboratories, NTT Corporation

一方、このような個人所有デバイスのみによって個人の行動履歴を蓄積する事には限界もある。まず、家の中などに据え置かれたデバイスでは、ユーザが特定の場所にいる間の履歴情報しか得る事ができない。一方で、ユーザが持ち歩けるセンサーの数には限界があるため、ポータブルデバイスから多様な種類の情報を得る事は期待できない。また、一般にポータブルデバイスの電源寿命はユーザの日常活動を一日分記録できるほど長くない。このため、個人所有のデバイスのみによって個人の日常の履歴情報を記録する事は、現実的な限界がある。

このような限界を克服し、ユーザになるべく負担をかけない形で多くの履歴情報を蓄積するためには、個人所有ではないデバイスを用いる方法を用意する必要がある。

2.1.2 非個人所有デバイス（外部センサー）

将来のユビキタス社会においては、ユーザのコンテキストに適応した様々なサービスが提供されると期待されている。そのためサービス事業者やそれと提携した建物管理者は、コンテキスト推定のために、ユーザの状態を看視するためのセンサーを様々な場所に配置するようになると予想される。

つまり将来の社会では、ユーザ自身がセンサーデバイスを持ち歩かなくとも、ユーザに関わる情報が様々な場所に埋め込まれた、非個人所有の環境センサーによって取得されている可能性が高い。これらのデバイス（以下、外部センサーと記す）を履歴情報の取得元として利用できれば、個人所有デバイスを用いた場合の限界を克服して、多くの情報を蓄積し、利用する事が可能となる。

しかしこれらの外部センサーは、ユーザ個人ではなく第三者によって設置されたセンサーデバイスであり、ユーザ自身はセンサーに関するアクセス権を持たない。例えば、街角に設置された監視カメラはその場所に滞在したユーザの映像を撮影し記録しているが、撮影対象となったユーザは自分が撮影された情報を参照する事は通常できない。そのため、このようなセンサーを用いて個人の履歴情報を蓄積するためには、外部センサーによって記録された様々な情報をユーザ自身が参照できるようにするための、総合的な履歴情報蓄積プラットフォームが必要となる。

2.2 既存システムの問題点

外部センサーを用いた履歴情報の蓄積プラットフォームの不完全な例として、図 1 に示すような、様々な場所に設置された外部センサーがそれぞれのレポジトリに取得した情報を蓄積しているシステムについて考える。特定の場所に滞在するユーザの履歴情報を、独自設置のセンサーによって記録する事業者が複数並列して存在する図 1 のよう

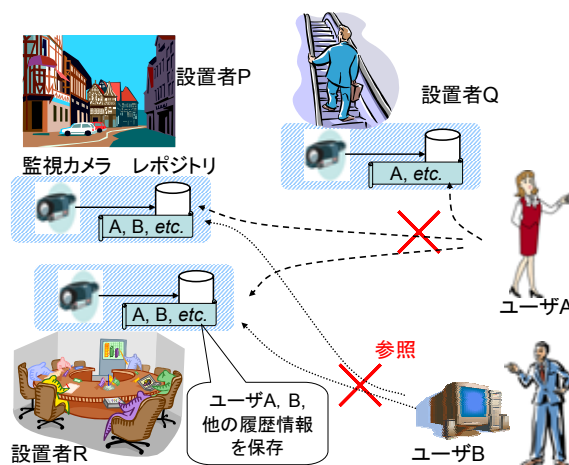


図 1 リトルブラザー型システム

な履歴情報蓄積システムを、本稿ではリトルブラザー[2]型システムと便宜的に呼ぶ*。

街角に設置される監視カメラの数が近年増加していることからわかるように、リトルブラザー型システムは徐々に一般化しつつあるが[3]、このシステム上でユーザが自由に個人の情報履歴を利用するためには、以下のような課題があると考えられる。

2.2.1 プライバシー保護との両立が困難

リトルブラザー型システムでは、それぞれのセンサー設置者のレポジトリに、センサーで記録した全ての情報が記録される。この状態において、センサーによって記録された履歴情報をユーザが参照することを考える。

各センサー設置者のレポジトリには複数のユーザの履歴情報が混在したまま蓄積されており、そこに蓄積された情報がどのユーザに関わる情報かといったユーザ識別は行われていない。このときあるユーザが、蓄積された全ての履歴情報の中から、自分が記録された部分の情報を切り出して参照する事は一般に困難である。これには二つの理由がある。

一つは、蓄積された情報の中から特定の個人が記録された部分のみを切り出す事が技術的に困難なことである。長時間の音声や動画データの中から、特定の個人が記録されている部分を切り出す事は、画像認識の技術の進歩などによって可能になってきているが、そのためには顔画像などの個人識別のための特徴情報をユーザの数だけあらかじめ保持しておかなければならない。これは、街角に設置された監視カメラなどのセンサーにとって現実的ではない。

二つめに、仮にユーザ識別による個人履歴情報の切り出しが技術的に可能であったとしても、ブ

* 政府などの一つの大きな権力が個人を監視することをビッグブラザーと呼ぶのに対する連想的呼称

プライバシー保護の観点からユーザの識別そのものが許されない可能性が高い、という理由がある。

街角監視カメラなどの公共的なセンサーの運用にあたっては、撮影された個人の同定は事件などが発生した場合以外には行わない、という事が暗黙の前提となっている。すなわちこれらのセンサーは、撮影対象に対する匿名性確保を前提として運用が許可されていると言える。この匿名性確保の前提のため、センサーはたとえ技術的に可能であったとしても記録されたデータに対して個人識別をするような解析は行えず、結果として特定の個人が記録された履歴情報を切り出すことは不可能となる。

以上のような理由により、リトルブラザー型システムにおいては、ユーザに対して個人の履歴情報を開示する事が困難だという問題が存在する。これを克服し、各ユーザのプライバシーを保護しながら、それぞれの履歴情報を各ユーザに参照可能とすることが課題となる。

2.2.2 データ可用性の低下

仮に上記の問題が解決して、センサーによって記録された個人の履歴情報をユーザが参照することが可能になったとしても、このデータが各センサー設置者のレポジトリにのみ存在している状況では、履歴情報の可用性（データ利用可能性）が低いという問題が存在する。

まず2.1.1節で説明したような個人所有のセンサーデバイスを用いて個人の履歴情報を記録する場合について考える。例えば、家庭内のセンサーデバイスから履歴情報を取得する際は、その蓄積先はホームサーバなどの家庭内の端末になる事が妥当であろう。ポータブルセンサーデバイスを用いた場合には、一緒に携帯しているストレージデバイスに蓄積することができる。このとき、個人の履歴情報は個人所有の単一あるいはごく少数のレポジトリに一括して蓄積されるため、ユーザはいつでもレポジトリから自分の過去の履歴情報にアクセスして利用することができる。

一方で、非個人所有のセンサーデバイスを利用する場合、リトルブラザー型システムでは、自分の過去の履歴情報を参照したいと思ったときにその情報が蓄積されているセンサー設置者の運用するレポジトリにアクセスすることになる。このとき、そのレポジトリはセンサー設置者の独自のポリシーによって運用されているため、ユーザがアクセスした時にたまたまメンテナンス中で参照ができないかもしれない。あるいは、設置者がセンサーを撤去したことに伴って、レポジトリそのものが破棄されてしまっていて、以後永久に参照が不可能になっているかもしれない。

このようにリトルブラザー型システムでは、自分の過去の履歴情報に恒久的にアクセスするにあ

たって十分なデータ可用性を保証することができないという問題が存在する。

2.2.3 履歴情報の有効活用が困難

さらに、各個人の履歴情報がセンサー設置者のレポジトリにのみ存在している状況では、データの一元管理ができないため履歴情報利用の利便性が低いという問題も存在する。

ユーザは自分の過去の情報をアクセスするために、過去に滞在した様々な場所のレポジトリにアクセスして、その都度情報を取得しなければならない。これは、過去の行動の中から重要な出来事を検索したり、意味のある傾向を抽出するなどといったデータマイニング的な履歴情報の利用モデルにおいて、著しいパフォーマンスの低下を招き、結果として履歴情報を有効に活用することが困難となる。

3 GreenTown

2.2節で説明したような、従来のリトルブラザー型システムの抱える課題を解決する新しい履歴情報蓄積システムとして、我々は外部センサーを用いた行動履歴の個人蓄積システム（GreenTown）を提案している[4]。

GreenTown は、様々な場所に設置された公共的な外部センサーを用いて、ユーザの身のまわりで起きた出来事（履歴情報）を、ユーザ個人が管理するストレージ領域に蓄積していくことを特徴とするシステムである。なかでも GreenTown は、街角に設置された監視カメラなどによって取得される映像情報を蓄積する事を主な目的としている。

3.1 アーキテクチャの概要

図2に GreenTown の構成を示す。GreenTown は主に、個人の位置を取得するユーザ識別部と、音声や映像を主とした個人履歴情報を取得するセンサー部、履歴情報を格納するストレージ部によって構成される。以下に、これらの三つの機能部の動作の概略を示す。

3.1.1 ユーザ識別部

ユーザ識別部は、ユーザの位置を測定する位置センサー(1)と、位置センサーの出力を元にユーザの論理位置を決定する位置特定部(2)、センサー部にデータの蓄積指示を行う蓄積指示部(3)によって構成される。

位置センサー(1)として例えば無線タグなどのデバイスを用い、ユーザの存在に関する情報を取得する。位置特定部(2)はセンサーから位置への推論規則を保持し、得られた情報からユーザの論理位置を特定する。論理位置とは、建物や部屋等の論理的なトポロジと、その場所で利用可能な A/V センサーの配置とを勘案して任意に定めた座標系である。

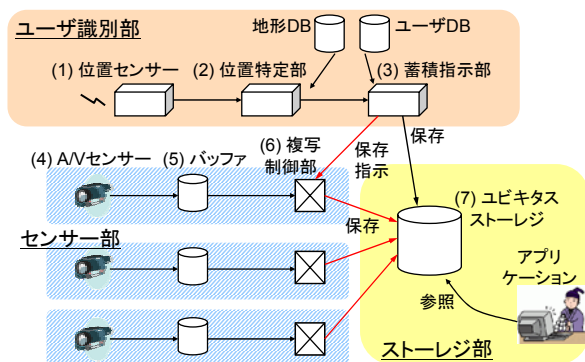


図 2 GreenTown の構成

蓄積指示部(3)は地形DBを用いて論理位置に存在するA/Vセンサー(4)を探索し、蓄積対象の情報源を特定する。そして、ユーザがその場所に滞在した期間についての時刻情報を複写制御部(6)に送信し、滞在期間中のセンサーデータを保存するように指示する。

ユーザの位置情報は、後で情報を取り出す際のインデックスとしても利用するので、ユビキタスストレージ(7)に蓄積する。

蓄積指示部(3)がアクセスするユーザDBには、ユーザ毎に各情報の蓄積先となるストレージのデータIDと、そのアクセス鍵が保管されている。また例えば位置センサーに無線タグを用いた場合、ユーザと無線タグIDの対応関係も併せて保管される。

ユーザ識別部の運用モデル

GreenTownでは、GreenTown専用位置センサー(1)を設置するのではなく、他のサービスと共用して使われる位置情報インフラストラクチャを利用することを想定している。ユーザ識別部全体としての機能も、携帯電話会社が提供する位置情報サービスと同様に、ユーザの自発的な契約の元で提供されることを意図している。

3.1.2 センサー部

センサー部は、監視カメラを想定するA/Vセンサー(4)と、取得したセンサーデータの一時的格納先であるバッファ(5)、そして複写制御部(6)によって構成され、セットとして各センサー設置者によって運用される。

複写制御部(6)は蓄積指示部(3)からの蓄積指示を受けると、指定された滞在期間中のセンサーデータをバッファ(5)から読み出し、ユビキタスストレージ(7)上のストレージ領域に保存する。このとき、センサーデータはセンサーの記録対象であるユーザ個人の管理するストレージ領域に保存される。

センサーを接続するネットワークが、無線接続などで一時的に切断されることもあり得る。その場合、蓄積指示部(3)から複写制御部(6)への指示が遅れて到着し、また複写制御部(6)からストレ

ジへの書き込みが遅延される。この場合でも、バッファ(5)に該当期間中のセンサーデータが残っていれば、前述の動作で同様に対応できる。

センサー部の運用モデル

GreenTownでは蓄積する情報として、商店街や通路などに設置された監視カメラによる映像を主なターゲットとしている。このとき、センサー部は自治体的組織や建物管理者などによって運用されるが、撮影される人々からの明示的な承認を得ていない上でセンサーが設置されている事も想定される。

また、ユーザは日常生活において訪れる様々な場所に設置された監視カメラの全てについて、撮影された映像の機密性が守られるという想定はユーザにとって現実的でない。このように、センサー部はユーザから必ずしも信頼されていない状況において運用されていると言える。

3.1.3 ストレージ部

ストレージ部は、センサー部によって収集されたユーザの履歴情報の最終的な蓄積先であり、ユーザ毎に論理的に切り離されたストレージ領域を持つ。この領域に、A/Vセンサー(4)から得た情報がそのまま蓄積される。また、ユーザの位置情報履歴も同時に蓄積される。

GreenTownでは主に監視カメラなどから得られる比較的大容量の映像データを扱うため、ストレージ部はネットワークの状況に依らず大容量データを扱える機能が必要である。そのためユビキタスストレージ(7)は下記の要求条件を満たすものがよい。(a) ネットワーク全体で柔軟に複製を作成・移動でき、それらが単一の空間として扱えること(分散透過)。(b) ネットワーク断でも情報の保存・参照ができること(切断時操作)。(c) 複数の情報ストリームをひとまとまりとして複製管理できること(グループ化)。これらを満たすシステムの例としてCAOSS[5]があり、現在のGreenTownはこれをユビキタスストレージとして利用する。

CAOSSは図3に示されるようなP2P的なアーキテクチャを持つ分散型ストレージシステムであり、一意なデータIDで識別されるデータの集合について、ネットワーク上で自由にデータの複製を作ったり移動させたりすることを可能としている。

さらにGreenTownでは、蓄積された履歴情報をアプリケーションが利用する際の利便性の提供のため、取り出し制御部(8)を設ける。取り出し制御部は、時系列に沿って履歴情報へアクセスする機能をアプリケーション(9)に提供する。さらに、重複する情報の削除や古い情報の再圧縮、インデックスづけなど情報の整理を行う。情報の整理を取り出し時まで遅延することで、様々な環境に設置されるセンサー部が情報を蓄積する際の手順を簡素化できる。

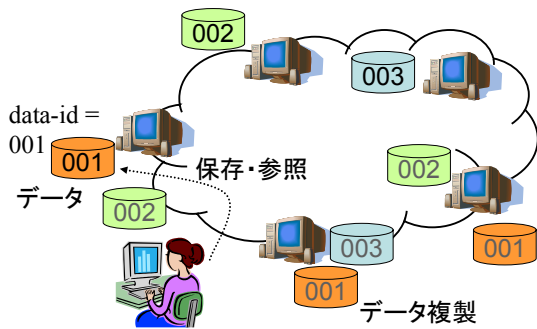


図3 ユビキタスストレージ (CAOSS)

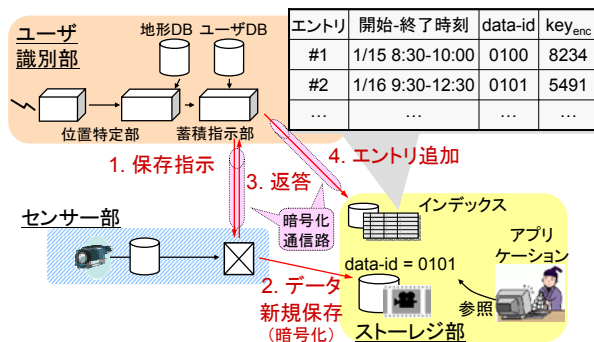
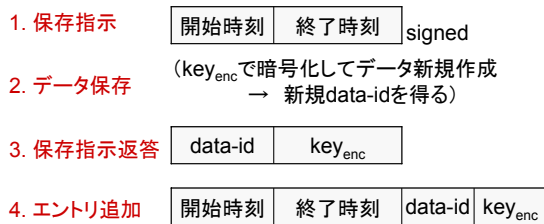


図4 蓄積手順



これらの通信は盗聴されないよう暗号化
通信路で守られる

図5 メッセージの構成

ストレージ部の運用モデル

将来は、一人で複数の端末を利用するユーザの利便性のために、大規模なオンラインストレージサービスが提供されると考えられる。GreenTownではそのように提供されるストレージ領域に、センサー部から得られた個人の履歴情報を蓄積する。ユーザはISPと契約するようにストレージプロバイダと契約した上でサービスを利用するため、ユーザ識別部と同様にストレージ部もユーザからの信頼の上で運用されていると想定される。

あるいは、ユーザが履歴情報の蓄積先としてホームサーバ等の完全に信頼できる個人所有端末を選択することも考えられる。このときストレージプロバイダは、ホームサーバまで履歴情報を移動させるためのリダイレクト的な役割をはたす。

3.2 実際の蓄積と参照手順

図4にGreenTownにおける履歴情報の蓄積手順の概要を示す。図5は各コンポーネント間で受け渡されるメッセージの構成を表している。

あるユーザAの位置が測定された場合、ユーザ識別部はユーザAが滞在した場所にあるセンサー部に対して、滞在期間内のセンサーデータを蓄積するように指示する(1)。この蓄積指示にはユーザAを識別できるような情報は含まれない。

指示を受けたセンサー部は、該当期間のセンサーデータをバッファから参照し、新しく生成した共通暗号鍵keyで暗号化した後、新規データとしてユビキタスストレージ上に保存する(2)。

このときのデータの識別子(data-id)と暗号鍵を保存指示の返答としてユーザ識別部に通知する(3)。返答を受けたユーザ識別部は、ユーザAの行動履歴一覧が保存されたインデックスをユーザDBを用いて特定し、「滞在期間情報、履歴情報の保存されたデータのdata-id、暗号鍵」からなる新しいエントリを追加する(4)。

ユーザが過去の履歴情報を参照するときは、ユーザDBに登録した自分の履歴情報インデックスから参照したい時刻が含まれる場面(エントリ)を検索し、結果として得られたdata-idから実際の履歴情報データを読み出す。図4では簡便のためインデックスを単一としているが、実際には画像、動画、移動履歴などのセンサー種別に応じた複数のインデックスをもち、ユーザDBで指定されるインデックスをルートとする階層構造を持つ。

4 効果

4.1 プライバシー保護との履歴蓄積の両立

2.2節で述べたように、リトルブラザー型の履歴情報蓄積システムでは、プライバシー上の問題から、外部センサーによって取得される履歴情報をユーザが参照する事は困難であった。

GreenTownでは、位置センサーと外部センサーを連携させることによってユーザの滞在期間を特定し、その部分を該当ユーザの管理するストレージ領域にコピーする。これによって、ユーザは自分の行動が記録されたセンサー情報(履歴情報)を参照することが可能となる。

この際、ユーザから必ずしも信頼されない外部センサーには個人特定につながるような情報は一切渡さず、個人特定が必要となる蓄積動作はユーザから信頼されているユーザ識別部が代行して行っている。このため、外部センサーは保存しようとしているデータがどのような個人の履歴情報なのかについて推測することはできず、外部センサーにとって記録対象の個人は匿名のままである[6]。

このようにGreenTownは、ユーザのプライバシーを守りながら外部センサーから履歴情報を取得し、蓄積していく事が可能である。

4.2 データ可用性と利便性の向上

GreenTown では、各センサーによって取得された履歴情報をユーザが管理するストレージ領域にコピーして蓄積する。データは主にユーザのホームサーバにあたる端末に一括して蓄積されるため、ユーザ主管による履歴情報の一元管理が可能となる。このため、リトルブラザー型システムの課題であった、履歴情報利用の可用性低下と有効性低下の問題が克服される。

4.3 個人情報の自己利用権の強化

4.1 節で述べたように、GreenTown を導入する事によって、ユーザは外部センサーによって取得された個人履歴情報にアクセスできるようになる。例えば、いままで監視カメラによって一方的に撮影されていたユーザも、自分の写っている範囲の情報は自分で利用する事が可能となる。これは、情報の自己利用権（自分に関わる情報は自分で管理できるべき）の強化という GreenTown の副次的な産物である。

このように自己利用権の強化がシステムチックに可能になってくると、監視カメラを設置する側に、記録したデータを設置者だけで利用するのではなくユーザにも還元するべきといった圧力がかかる事が期待できる。この圧力は、無節操な監視カメラの設置を改めさせることにつながる。一方で情報の自己利用権が得られるようになると、監視カメラなどを様々な場所に設置することが許容されやすくなることも考えられる。

GreenTown は、両者のバランスをとった、ユビキタス社会における適正なセンサーの設置・運用のための基盤技術を提供できる。

5 関連研究

Microsoft Research の MyLifeBits [1] では、ユーザの日常活動で接する情報をなるべくデジタル化して個人の PC 上に貯めていくとともに、そのように貯められた多くの情報を使って、ユーザの日常の活動を補助する方法を研究している。MyLifeBits では蓄積する履歴情報として、ユーザが直接扱うことのできる各種書類や写真などのデータを対象としており、研究の主なターゲットは情報を蓄積する際の DB 形式や、役に立つ情報をユーザに提供する際のインタフェース (GUI) である。

GreenTown では、個人の履歴情報の情報源として個人が直接接する範囲の情報だけでなく、環境的に埋め込まれている外部センサーなどを用いてなるべく広い範囲の情報を集める事を目的としている。その際、外部センサーを扱う場合に必須となるプライバシー保護の枠組みを確立している。一方で、蓄積された履歴情報の利用方法について

は、MyLifeBits やデータマイニング技術等、他研究の成果を利用する事を期待している。

MyLifeBits に限らずいわゆるユビキタスサービスの研究では、サービス提供者がセンサーおよびそこから取得される情報に対する管理権を全て持っているという前提に立つ場合が多い。この前提の上では、プライバシー情報の提供とサービスによる利便性享受との間のトレードオフをどう解決するかが課題となる。しかし、事業者が全てのセンサーを設置・管理できるような比較的狭い領域を超えると、複数の事業者が設置した多様なセンサーが取得する情報を、プライバシーを保護しつつどのように連携させるか、という課題が生まれる。GreenTown はこの課題に対し、全ての情報を一度ユーザの手元に集めて、その上で各種情報の連携による新しい利用方法を探る、というアプローチをとる。

6 まとめ

本稿では、身の回りのできごと（履歴情報）を主に映像と音声で蓄積することを目的としたセンサー情報の個人蓄積システム (GreenTown) について、実現に向けた課題を明らかにし、それを解決するシステム構成を提案した。GreenTown は、公共の外部センサーと位置センサーを連携させることによって個人が記録されたセンサー情報の一部を個人の履歴情報として切り出し、ユーザ個人のストレージ領域に自動的に蓄積することができる。現在、提案したシステムのプロトタイプ実装を完了し、動作の評価を進めている。

参考文献

- [1] Gemmell, J., Bell, G., Lueder, R., Drucker, S. and Wong, C., "MyLifeBits: Fulling the Memem Vision", *ACM Multimedia 02*, pp. 235-238 (2002).
- [2] 東浩紀, "情報自由論 (2)", 中央公論 2002 年 8 月号
- [3] 池田信夫, "個人情報ほだれのものか", RIETI 政策シンポジウム, 2002 年 2 月, <http://www.rieti.go.jp/projects/denshi/02.pdf>
- [4] 中村, 井上, 中村, "ユーザ位置に連動した外部センサー情報の個人蓄積システム", FIT2003, M-45
- [5] 井上, 中村, 久保田, "動的なネットワーク環境に適した適応型オンラインストレージシステムの提案", DPS 研究会 2002-DPS-110, 情報処理学会, pp. 55-60 (2002).
- [6] 井上, 中村, 中村, "個人履歴のユビキタス蓄積システムにおける安全な情報蓄積方式", 情処全大 5H-3, 2004 年 3 月