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

井上 知洋†　　中村 隆幸†　　中村 元紀†
† 日本電信電話（株） NTT 未来ねっと研究所

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，個人レベルにおいて一般的に行われている．最近では，ウェアラブルカメラなどを用いてより大容量の情報を蓄積し活用する取り組みも始まっている．

我々は，社会の様々な場所に設置された公共的なセンサーを用いて，個人の日常の行動履歴を記録し蓄積するシステム（GreenTown: 以下 GT と記す）を提案している[1]．GT のように個人所有でないセンサーを用いて個人情報を記録するシステムでは，記録対象となる個人のプライバシーを保護する枠組みが必要となる．本稿では GT が抱えるプライバシー上の課題について概要を述べる．その中でも，記録対象となるユーザの匿名性を確保したまま，公共的なセンサーからユーザに関わる情報を取得し，蓄積する方式について提案する．

2 個人履歴のユビキタス蓄積システム

ユビキタス社会においては，ユーザやその周囲の様子を把握するためのセンサーが様々な場所に設置されることが予想されている．我々はこのように配置された多数のセンサーを使って，ユーザの身の回りに起きた出来事を主に映像と音声で蓄積することを目的とした，個人履歴のユビキタス蓄積システム (GT) を提案している[1].

図 1 に GT の構成を示す．GT は主に，個人の位置を取得するユーザ識別部と，声や映像の情報を取得するセンサー部，個人履歴情報を格納するストーレ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．

ユーザ識別部

ユーザ識別部は，ユーザの位置を把握する位置特定部(2)と，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．まず，位置特定部が何らかの手段でユーザの位置情報を取得する．その後，地形データベースを参照してユーザの現在位置に存在する A/V センサー(4) を特定する．蓄積指示部は該当 A/V センサーを管理するセンサー部に対して，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．

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) によって構成される．複写制御部は蓄積指示部から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から読み出し，ユビキタスストーレジ(7) 上のストーレジ領域に保存する．このとき，センサーデータは撮影対象である個人の管理するストーレジ領域に保存される．

ストーレジ部

ストーレジ部は，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ーレジ領域を持つ．

GT 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，ストーレ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ような分散型のストーレジシステムで構成される必要がある．GT では，この条件を満たすユビキタスストーレジ(7) として，P2P 型のオンラインストーレジシステム[2] を利用している．

3 プライバシー保護

監視カメラなどを用いた従来の情報蓄積システムでは，撮影された情報はカメラの設置・運営者が保管しており，その情報に運営者以外がアクセスすることはできない．このためユーザは撮影された自分の映像を参照し利用する事ができない．また，ユーザから必ずしも信用されない第三者によって個人の履歴情報が管理されることは，プライバシー情報の流出という不安をもたらす．

GT は，様々な運営者が設置したセンサーによって取得されるユーザの履歴情報を，ユーザ個人が管理するストーレジ領域に蓄積することを特徴とする[1]．これにより，従来複数のセンサーが各々個別に保存していた断片的履歴情報を，個人個人が一括して扱う事が可能となり，情報利用の利便性が向上する．同時に，履歴情報の管理権限がユーザ個人に帰属するためプライバシー上の問題が低減される．

一方，ユーザが GT を用いて日常活動を記録する際には様々な主体によって運営されているセンサーを利用する必要があるが，これらのセンサーが悪意をもって運用されている場合は，依然としてユーザのプライバシーが侵害される可能性がある．

以降の節では，GT が想定する各機能部の信頼モデルを明らかにした上で，センサー部（監視カメラ）によるプライバシー侵害の可能性とその対応方法ついて説明する．

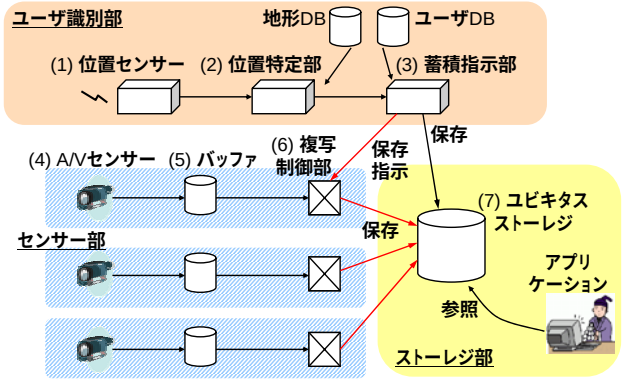


図 1 個人履歴ユビキタス蓄積システムの概要

A Secure Storage Scheme for the Ubiquitous Logging System of Personal Data
Tomohiro Inoue, Takayuki Nakamura, Motonori Nakamura
† NTT Network Innovation Laboratories, NTT Corporation

3.1 信頼モデル

ユーザ識別部

GT では位置識別システムの例として，携帯電話事業者などが提供する位置情報サービスを想定している．一般に携帯電話事業者はユーザの位置情報を基地局単位で把握し記録しているが，これはプライバシーの侵害とは見なされない．これは，個人情報の機密性（位置情報が外部に流出しない事）についてユーザが事業者を信頼しているためである．この信頼は，携帯電話の利用契約を通して成り立っている．

GT のユーザ識別部として位置情報サービスを提供する事業者も，同様の枠組みによってユーザからの信頼を得ていると想定できる．

センサー部

GT 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．これらの監視カメラは自治体的組織や建物管理者などによって設置・運用されているが，一般には撮影される人々からの明示的な設置承認を得ていない場合が多い．

また，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，監視カメラ（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．

ストーレジ部

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ーレジサービスが提供されると考えられる．GT ではそのように提供されるストーレジ領域に，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ーレ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ーレジ部もユーザからの信頼を得ていると想定できる．

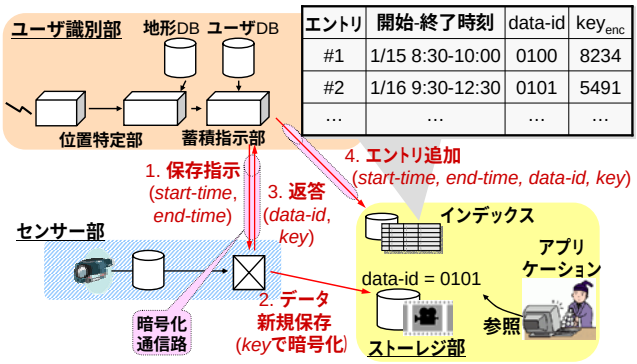
3.2 想定されるプライバシーの侵害

GT では，ユーザ識別部とストーレジ部はユーザから信頼されている一方で，センサー部は信頼されていない．このため，悪意のあるセンサー部（監視カメラ）によってプライバシーが侵害される可能性について考えなければならない．

監視カメラ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．すなわち監視カメラは，撮影対象に対する匿名性確保を前提として設置が許可されていると言える．

2 節で説明したように，監視カメラはユーザ識別部から指示された情報に基づいて，ユーザの滞在期間内のデータを切り出してストーレジに保存する．このとき，ユーザ識別部が監視カメラに対して撮影対象のユーザの個人情報（ユーザ ID など）を渡してしまうと，カメラは切り出されたデータが特定のユーザを撮影した映像であると容易に判定できてしまう．

これはユーザにとっての匿名性の喪失を意味する．もしこの監視カメラが悪意をもって運営されている場合，撮影映像が個人同定された上で第三者に流出する可能性があり，明確なプライバシー侵害が発生する．このため，センサー部に関してはユーザの匿名性を保ったまま履歴情報を蓄積することが GT の課題となる．



エントリ	開始-終了時刻	data-id	key_{enc}
#1	1/15 8:30-10:00	0100	8234
#2	1/16 9:30-12:30	0101	5491
…	…	…	…

図 2 履歴情報の匿名的な蓄積手順

3.3 履歴情報の匿名的な蓄積手順

GT ではユーザの履歴情報を蓄積する際，履歴情報データをコンテンツとインデックス（メタデータ）に分離し，ユーザ識別部がセンサー部に代行してインデックスを更新する事によって，上記の課題を解決する．

図 2 に GT における履歴情報の蓄積手順の概要を示す．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ーレジ上に保存する(2)．このときのデータの識別子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識別子，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，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データ識別子から実際の履歴情報データを読み出す．

3.4 効果

前節の蓄積手順は，必ずしも信頼されないセンサー部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うことを特徴とする．これによって，センサー部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，センサー部にとって記録対象の個人は匿名のままである．

4 おわりに

本稿では個人履歴のユビキタス蓄積システム (GreenTown) におけるプライバシー保護の枠組みと想定する各機能部の信頼モデルについて説明した．また，信頼されないセンサー部によるプライバシー侵害を防止するために，ユーザの匿名性を確保したまま履歴情報を取得し蓄積する方法を提案した．

参考文献

[1] 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

[2] 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ーレジシステムの提案, DPS 研究会 2002-DPS-110, 情報処理学会, pp. 55-60 (2002).