「マルチメディア，分散，協調とモバイル
(DICOMO2013)シンポジウム」 平成25年7月

情報銀行システムにおける 個人情報蓄積機構の機能設計と実装

秋山 寛子[†1] 山内 正人[†1] 柴崎 亮介[†2,†3] 砂原 秀樹[†1]

概要：社会に散在する個人情報を統合し新たな価値を生成することを目的とし，個人情報の名寄せを個人が自ら実現し，管理する「安心感」の仕組み，それを社会的に透明な方法で集約して価値を生み出す仕組みとして，”情報銀行”プロジェクトを行っている．この社会的システムの実現に向けて，技術的側面や，監査の仕組みや経営・運用などを含めた組織デザインを行い，社会に受容されるための検討を行っている．本研究では，個人情報の提供者が安心して情報を提供できる仕組みを，技術的な面から設計した．まず，情報提供者の個人情報を，プライバシーを守りつつ匿名化された情報として社会へ活用できるよう，秘匿にする情報と公開する情報とに分離するアクセス制御の仕組みを設計した．次に，情報の開示先や使用用途を情報提供者本人が制御できる仕組みを設計した．それぞれの基本的な設計およびプロトタイプを実装し，今後の課題について検討した．

Design and Implementation of Personal Activity Information Storing Feature in Information Bank System

Hiroko Akiyama[†1] Masato Yamanouchi[†1] Ryosuke Shibasaki[†2,†3] Hideki Sunahara[†1]

1. はじめに

”情報銀行”とは，個人情報の高次利用を目的とし，”個人口座”と呼ばれるデータベースに個人情報を蓄積し，匿名性を保ったまま任意の種別の情報を抽出し，情報を統計や産業へ利用するサービス事業者へと提供する仕組みである [1].

社会生活の中で個人活動や行動履歴における情報はデジタル化され，収集されている [2]．スマートフォンをはじめとした個人情報端末の普及は，より多様かつ詳細な情報を収集することを可能としている．これらの情報を基としたサービスは，個人の趣味趣向や，地域性，時節を考慮した物となる為，より有用なサービスを提供できる可能性を持っている．個人向けのサービスとしては，健康サービスや，安否確認，広告やマーケティングなどが考えられる．また，社会貢献のサービスとしては，災害対応やリアルタイム統計，それらを利用した政策の企画・実施支援などが行える．さらには，学術的に，個人行動のモデル化，予測などに活用することができる．

しかし，現状では，これらの個人情報を有効に利活用できていない [3]．まず，多くの活動情報は個人，企業，政府など，ばらばらな場所や組織が保有しているため，断片的な状態となっている．断片的となっている情報をつなぎ合わせて価値のある「総合情報」をつくる仕組みができれば，デバイスのセンシングやデータマイニング等の技術の進歩を社会にいかすことができ，社会にも個人にも有益な様々な情報を生成することが可能となる．そこで，個人情報の名寄せを個人が自ら実現し，管理する「安心感」の仕組み，それを社会的に透明な方法で集約して価値を生み出す仕組みである”情報銀行”システムを提案する．

本論文では，2 章にて情報銀行システムの概要，3 章にて情報提供者に情報を提供してもらえる仕組みについての考察，4 章にて情報提供者のプライバシーを守るためのア

†1 現在，慶應義塾大学大学院メディアデザイン研究科
Presently with KMD, Yokohama, Kanagawa 223–0061, Japan
†2 現在，東京大学空間情報科学研究センター
Presently with CSIS, Meguro, Tokyo 153–8505, Japan
†3 現在，東京大学生産技術研究所
Presently with IIS, Meguro, Tokyo 153–8505, Japan

クセス制御方式の提案，５章にてプロトタイプ作成，６章にて今後の課題について述べる．

2. 情報銀行システムの概要

”情報銀行”システムには，「情報提供者」，「情報利用者」，「情報銀行」という３つの主体者が存在する [4]．情報提供者とは，個人活動履歴を情報銀行へ蓄積する存在である．情報利用者とは，個人情報を活用して，様々なサービスや研究，統計等へ役立てる存在を表す．情報銀行は，情報提供者の情報を受信・蓄積し，プライバシーに配慮し保管し，情報利用者からのリクエストに対し該当するデータを返答する機関である．システムの概略を図１に示す．

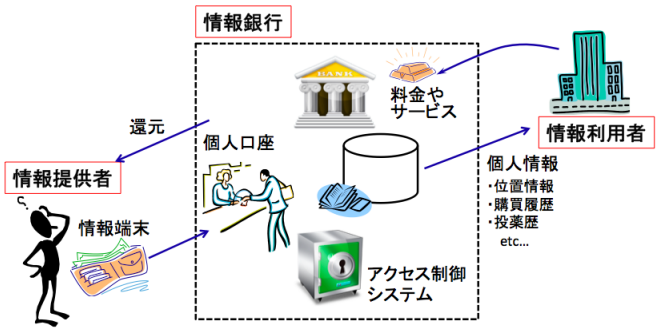

図 1 情報銀行の概要

情報提供者は，まず，情報銀行内に個人口座を開設する．スマートフォン等の情報端末から個人活動データを生成や取得し，個人口座へと送信する．個人活動情報は，情報端末内のセンサ等を利用してセンシングしたり，web サービスを利用したりして生成され，個人口座内に蓄積される．

情報銀行は，情報提供者から送信された個人情報を収集し，プライバシーやセキュリティに配慮して保管する．ここで，個人口座内の全てのデータへのアクセス権を所有する存在は，その口座を開設した情報提供者のみであり，データの開示先，使用用途については，個人口座の持ち主が自ら制御や監視を行うことが可能とするという仕組みを導入する．これにより，個人情報の所有者本人が自らの情報を集約・統合することができ，かつ，その保管状況の制御・管理を行えるようにすることで，個人情報の不信感や不安を軽減することが期待できる．

情報利用者は，情報銀行から蓄積された個人情報を受け取り，新たな情報やサービスを生成し，その情報提供者に対して，生成された価値を還元する．

3. 個人の活動情報の収集と管理

情報銀行システムに蓄積された様々な種類の個人情報を必要に応じて抽出し活用することで，新しい価値をもつ情報を生み出すことができる．より質が高く新しい価値を持つ情報を生み出すには，多くの情報を集める必要がある．本章では，個人情報を提供してもらうために必要な要件について考察し，その技術的な実現方法について考える．

3.1 情報提供に対するモチベーションの向上

情報提供者に，積極的に自身の情報を提供してもらうためには，情報銀行としてどのようなアプローチをとる必要があるかについて考察する．

情報提供者のモチベーション向上のためには，情報提供者への利益の確保が効果的である．情報利用者は，このシステムを利用することで，求める情報を柔軟に取得することが可能となるため，大きな利益を得ることができる．そこで，情報利用者は，情報使用料として情報銀行へ料金を支払う．あるいは，情報を活用し生成されたサービスを，情報提供者へ対して還元する．情報提供者は，サービスや料金を受け取り利益を得るようにする．もしくは，使用用途に合意した上で，寄付という形も選択できるようにする．

また，情報提供者の，個人情報を提供することへの不安や不信感を取り除くことが必要である．そのためには，まず，情報提供者のプライバシーを守るための確かなセキュリティを確立することは必須である．セキュリティ対策として，個人情報をやり取りするための通信技術，必要に応じた暗号技術，不正なアクセスなどから守るためのストレージシステムの設計等，複数の技術を総合的に組み合わせた設計を行う．また，情報銀行全体の運用として，監査機関の導入や本人確認の認証に用いるための法的整備なども含めた組織設計も必要である．次に，情報提供者の情報銀行の使用感を良くすることも必要である．全体の運用に関することや，導入しているセキュリティについてなど，情報提供者に対して，積極的に使ってもらうための組織デザインについての，効果的な説明がなされることで，自分の情報がどう扱われるかについての把握が可能となるため，不安の軽減となることが期待できる．また，把握だけでなく，自分自身で，自分の情報の開示について制御できる仕組みを導入すれば，不安感や不信感をさらに払拭できることが期待できる．

3.2 情報提供者による情報開示管理

情報提供者の不安感を除く方法として，情報提供者が自ら，自身の情報の開示に関する制御を行える仕組みについて考える．

3.2.1 情報提供者と情報銀行

情報提供者は，複数の種別の個人情報を蓄積する．例えば，位置情報や購買履歴，運動履歴など，さまざまな種類が考えられる．その情報のうち，開示してサービスを受けたいと感じるものと，開示したくないものとがあると考えられる．また，それは，情報の種別だけに依らず，開示先である情報利用者によっても開示に対する心境が異なると考

えられる．それは，情報利用者の社会的な認知や個人的な感覚によって，信頼度が異なるからであり，また，情報利用者によって，情報の使用目的が異なるからでもある．情報利用者は，個人向けサービスを生成する会社であったり，社会的な利益を産出するための統計分析機関であったり，大学などの研究機関であったりするため，その使用目的は様々である．そこで，情報利用者は，個人情報の使用用途を明示するべきであり，情報提供者はその使用用途を参照し，個人情報を開示するか選択できることがのぞましい．

以上より，自身の個人情報のうち，開示を許可する情報利用者，また，その使用用途について選択できる仕組みが必要であると考える．

3.2.2 情報利用者と情報銀行

個人口座に蓄積される個人情報は，正しく「情報提供者本人のもの」でなければならない。個人口座内の情報の全てを参照し，入出力ができるのは本人だけとする．そこで、個人口座へのアクセスには本人であることを確認する認証技術が必要となり，その認証に使用される情報は，他に知られてはならない秘匿な情報である．

一方で，個人口座が完全に秘匿状態であると，情報利用者がリクエストする情報に対する返答ができない．そこで，匿名性を保ったまま個人情報を抽出するために，情報利用者が検索に用いることのできる，公開用の個人情報が必要である．

以上より，情報提供者に関する情報は，秘密用と公開用との２つのテーブルを作成する．そして，この二つのテーブルを関連づけることで，個人口座と情報提供者とを１対１で関連づけることができ，かつ，匿名性を保ったまま情報利用者からの検索を行うことが可能となる．

4. 情報提供者による情報の蓄積と開示の制御方法

本章では，前章で述べた情報提供者が情報の開示制御を自ら行える方法についての詳細を述べる．

4.1 情報提供者に関する情報の管理方法

個人口座には，情報を蓄積する情報提供者と，情報を求める情報利用者とがアクセスする．そこで，それぞれのアクセスの管理方法について設計する．

まず，情報提供者のアクセスについて考える．個人の活動情報は，情報銀行の外部より情報端末を用いて生成され，ネットワークを経由して蓄積される．その際，情報銀行の自分の口座へアクセスできるのは本人だけでなければならない．そこで，個人口座へのアクセスには名前とパスワードを使用するなどの本人を認証するシステムにする．アクセス時に使用する名前とパスワードは，データの盗み見や改ざん等のトラブルを引き起こす可能性があるため，他に最も知られてはならない情報である．したがって，認証や個人を特定できるような情報を格納するための秘匿にすべき情報の集団が存在するといえる．そこで，このような個人を特定することが可能となる情報だけを集めたテーブルを作成し，情報提供者と個人口座とを結びつける情報とする．

次に，情報利用者からのアクセスについて考える．情報利用者は，「横浜市在住の 20 代女性の 2013 年 4 月の位置情報」などのように，情報の活用用途に対応する情報提供者の情報を求める．したがって，個人を表す情報を用いて，情報提供者を検索できる仕組みが必要である．ただし，その際には，個人を特定することなく匿名の状態で情報を抽出する必要がある．そこで，情報提供者の検索に使うことのできる公開用のテーブルを作成する．

以上より，情報提供者に関する情報については，知られてはいけない（または知られたくない）秘密の情報と，検索に使える公開の情報との二つに分離して管理するべきである．ここで，秘密用のテーブルからは公開用のテーブルにバインドしてあり，情報提供者は公開用のテーブルの内容を管理できるようにする．そして，この二つのテーブルを関連づけることで，個人口座と情報提供者とを１対１で関連づけることができ，かつ，匿名性を保ったまま情報利用者からの検索を行うことが可能となる．逆に，公開用のテーブルからは，秘密用のテーブルは見えないような仕組みにする．このような仕組みをもつ２つのテーブルを作成することで，本人を認証・特定できると同時に，匿名性を保ったまま検索をすることが可能となる（図 2）．

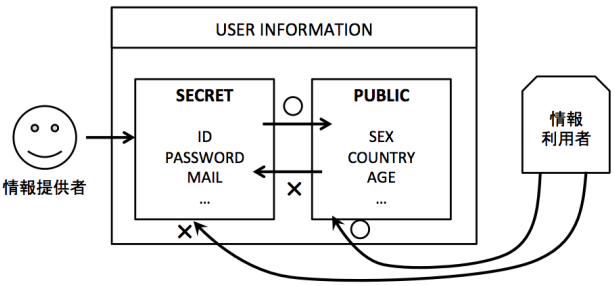

図 2 情報提供者に関する情報のテーブル構成

4.2 情報利用者への情報開示管理方法

情報提供者による，情報の開示の制御は，

- 許可する開示先の選択
- 情報の使用用途の選択

を情報提供者自らが行えるような仕組みを持たせることで実現する（図 3）．

まず，情報の開示を許可する情報利用者の選択方法について考える．情報銀行は，情報利用者と個人情報の使用について，「他への流用は行わない」，「提示した使用目的以外

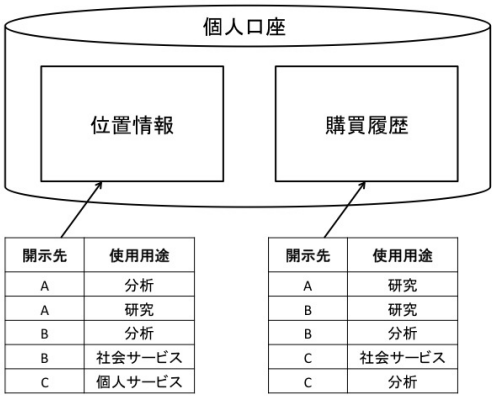

図 3 個人情報の開示制御方法

の用途には利用しない」等といった約束を取り決め，信用できる組織を情報利用者とする．また，情報利用者と情報銀行とは，個人情報を扱うため暗号通信を行うので，鍵の生成や配布などの処理が必要となる．したがって，情報銀行は情報利用者の一覧を保有する．そして，この一覧を情報の開示制御に用いる．

次に，使用用途についても一覧を作成する．使用用途に関しては，情報提供者が任意で項目を作成する方法も考えられるが，用途の意味の重複や曖昧さの回避や，意図しない使用の予防，情報提供者の操作負担の軽減のため，情報利用者との取り決めに対応した，使用用途項目を定義する．そして，決定した使用用途の一覧を作成する．

このようにして作成した，開示先と使用用途の一覧を用いて，個人の開示制御の条件を作成する．情報提供者が，開示を許可する情報利用者を指定し，さらに使用用途の制限を設定する．また，ある使用用途に関しては，いかなる情報利用者に対しても開示を許可する，というような一括管理も行えるようにする．

5. プロトタイプ実装

本章では，前章で提案したような匿名性を保ったまま情報を蓄積・抽出できるプロトタイプシステムについて述べる．プロトタイプは，MySQL を用いて実装した．プロトタイプが行う動作は以下である．

(1) 個人情報の公開用テーブルより，任意の情報提供者を検索
(2) 該当する情報提供者の開示管理テーブルを参照し，任意の開示先及び使用用途に対して開示可能か確認する
(3) 開示可能であれば，求める情報を抽出する

上記の操作を行うため，データベースを一つ作成し，そのデータベース内に以下のテーブルを作成した．

各テーブルに格納されている情報とその役割について述べる．情報提供者に関する情報を格納するテーブルは，user_information_secret と user_information_public

```
+-------------------------+
| Tables_in_test          |
+-------------------------+
| access_control_company  |
| access_control_purpose  |
| company                 |
| purpose                 |
| user_information_public |
| user_information_secret |
+-------------------------+
```

図 4 作成したテーブル

の二つを作成した．user_information_secret は秘密にしておきたい情報を格納してあり，情報提供者本人以外のアクセスが不可であるようアクセス制御されている．user_information_public は情報利用者が検索に使用できるように，開示可能な個人情報を格納している．company と purpose テーブルには，開示先である情報利用者一覧，使用用途一覧を入力し，それぞれに番号を付与した．access_control テーブルには，情報提供者の情報開示に関する制御情報を格納しており，開示を許可する情報利用者番号と使用用途一覧とを組み合わせることで表現している．

これらのテーブル同士の関連は図 5 のように表すことができる．

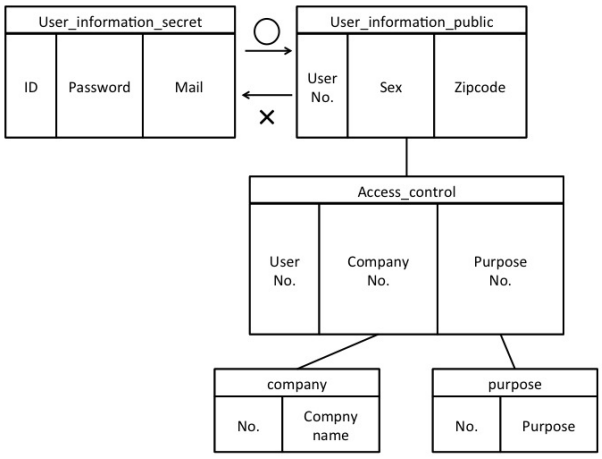

図 5 情報提供者情報のテーブル

これらのテーブルに対して，条件を指定し結合することで，情報利用者からのリクエストに対応する情報を抽出することが可能となる．以下は，クエリ文の一例である．

```
select * from user_information_public
join access_control_company
on user_information_public.sex='F'
and user_information_public.uid=access_control_company.uid
and access_control_company.cid=2
join access_control_purpose
on user_information_public.uid=access_control_purpose.uid
and access_control_purpose.pid=3;
```

これは，

- 対象情報提供者：女性
- 抽出情報：郵便番号
- 情報利用者番号＝2，使用用途番号＝3 には開示を許

可されている

という条件に該当する情報を抽出する命令文である．

6. まとめと今後の課題

本論文では，情報銀行の背景とシステムの概要について述べ，情報提供者が安全に，かつ安心して個人の情報を提供できる仕組みについて考察した．

その技術的実現方法として，個人情報の匿名性を保ちつつ，情報の利用者からは該当情報を検索できるような個人情報の管理方法を考察した．また，情報提供者が個人情報を提供することへの不安や不信感の払拭のために，情報の開示先や使用用途を自ら管理や制御できる仕組みについて設計し，プロトタイプ実装を行った．

しかし，作成したプロトタイプは，これらの要件を満たす最小限の機能を持つだけのものであるため，かなり限定的な動作しか行えなかった．より大きなサイズのデータでの演算や，ネットワークを経由したアクセス方法，情報利用者との運用方法等，実際に社会で運用する場合の状況を想定した実験を今後行う必要がある．また，情報を活用して生成されるデータの質の向上のために，データベースの管理方法について更なる検討が必要である．

謝辞

本研究は JSPS 科研費 24650031 の助成を受けたものである．

参考文献

[1] 東京大学・空間情報科学研究センター, “「情報銀行」: 個人活動情報のエコシステム”, 入手先 ⟨http://shiba.iis.u-tokyo.ac.jp/?page_id=410⟩ (2013.05.14)

[2] 美崎薫（著）:ライフログ入門, 東洋経済新報社 (2010)

[3] 東京大学・空間情報科学研究センター, “情報銀行構想について”, 入手先 ⟨http://i.csis.u-tokyo.ac.jp/event/20101005/index.files/11_06_KokaiDoc.pdf⟩ (2013.05.14)

[4] 東京大学・空間情報科学研究センター, “情報銀行: 個人情報を自ら管理し社会に役立てる仕組みの実現”, 入手先 ⟨http://shiba.iis.u-tokyo.ac.jp/research/contextaware/pdf/infobank.pdf⟩ (2013.05.14)