個人情報の保護と流通の両立を目指した個人情報活用システム

西田　玄，林 良一，高倉 健
NTT サイバーソリューション研究所

概要

ネットワーク上で個人情報を扱うＩＴサービスが多数提供されているが，多くのユーザはサービスプロバイダの個人情報の取り扱いに不安を抱いている．そこで筆者らは，ＩＣカードを用いて個人情報をユーザ自身が管理し，安全に利用するための個人情報管理システムを提案してきた．そのプロトタイプを構築し，相手に応じて個人情報の提供範囲を判断する開示制御機能と，個人を特定させずにカスタマイズサービスを受けるための匿名サービス利用機能とを実現したので報告する．また，これらの機能を用いた個人情報管理システムによる仲介機能についてもプロトタイプでのサービス例として紹介する．

Personal Information Practical Use System For Protection And Circulation Of Personal Information

Gen Nishida, Ryoichi Hayashi, Takeshi Takakura
NTT Cyber Solutions Laboratories

Abstract

While there are so many services on the net that ask for personal information of customers, much portion of people still have concerns about the treatment of sensitive information by the service providers. We have proposed a system that enables a user to manage her/his personal information by her/himself. In this paper, we introduce a proto-type implementation of the system that natively supports policy-based access control. With the system's "anonymous credit" function, a user can enjoy customized services without giving any sensitive information to service providers. We also present sample application of infomediary functions built on the system.

1. はじめに

国の行政機関や民間部門において情報化が進むにつれて, 個人情報がデジタル情報として大量に蓄積されつつある. 個人情報を一度サービスプロバイダ（SP）に渡すと，その集積や利用は所有者であるユーザの知らないところで行われていることが多い．そのため，ユーザは自分の個人情報が誤って蓄積されているのではないか，あるいは，正当な権限のない者によって不当に利用・改竄されたりプライバシーを侵害されているのではないか, という不安を抱いている. 現実に個人情報の取り扱いをめぐるトラブルも発生しており, 個人情報の収集や利用についての規制が求められ，また，ユーザが自身の個人情報をコントロールする権利の必要性・正当性も認識されつつある[1]**．昨年ようやく個人情報保護法案が国会に提出されるなど, 今後法整備が進んでいくと考えられるが, 法律による抑止力だけでは上記の問題の完全な解決にはならない．そこで，本研究では，個人情報を所有者であるユーザが管理し, 保護と流通を両立させるシステムを構築することを目標とする．**

個人情報を管理するサービスとして, 代表的なものに Microsoft **社の**.Net My Services[2]**や** Novell **社の** DigitalMe[3]**がある．これらのサービスでは, ユーザが自分の個人情報をネットワーク上のサーバで一元的に管理することで, 電子商取引サイトなどで個人情報を** SP **に容易に提供できるようにする．但し，ユーザは個人情報をサーバに預ける必要があるため, ユーザにとっては自分の知らないところで個人情報のやり取りが行われているという不安が依然として残る．これに対して，個人情報をユーザの** PC **で管理し，ユーザの意志に基づいて他のユーザとネットワークを介してやり取りを行うサービスとして，**OneName[4]**がある．このサービスでは, ユーザは自分の個人情報を自分の** PC **で管理できるので安心感が得られるが，自分の個人情報を自分の** PC **に格納するため，一般ユーザが安全に管理できるかという課題が生じる．**

そこで, 筆者らは個人情報の安全な格納先として IC カードに着目した. IC カードはその耐タンパ性から, セキュリティの高い情報格納デバイスとして注目されている. IC カードに個人情報を格納することで, ユーザは安全に個人情報を管理することが可能となる. また, ユーザは, サービスを利用する時にサービスシステム（SS）に対し, ユーザの意志に基づいて個人情報を提供することができる. しかしこの方法では, SP 側から見ると, ユーザの IC カードがネットワークに接続されていないと IC カード内の個人情報にアクセスできないという問題が生じる. この問題は, 例えば IC カードを携帯電話などと組み合わせることで解決できると考えられるが, 現状の IC カードでの実現は難しい. そこで, ネットワークに接続された個人情報管理サーバを設け, IC カード内の個人情報の複製を蓄積し, アクセス性を保証することとした.

筆者らが提案したシステム[5]では, 個人情報管理サーバに, ユーザの定める条件に基づいて SP への個人情報の提供を制御する機能を設ける. そして, ユーザは個人情報をサーバに蓄積する際に, 個人情報を提供する条件を定めておく. これにより SS は, 個人情報管理サーバにアクセスすることで, ユーザの IC カードがネットワークに接続されていない状態でもユーザが許可した範囲で個人情報を取得することが可能となる. 本稿では, 構築した個人情報管理システムのプロトタイプと実装した機能について述べる.

以下, 2 章で, 提案する個人情報管理システムについて説明し機能要件をまとめ, 3 章では, プロトタイプを構築する上で検討した課題について述べる. 4 章では, 構築したプロトタイプをサービス例に沿って説明する. 5 章では, まとめと今後の展望について述べる.

2. 個人情報管理システム

2.1. システムの概要

図 1 にシステムの概要を示す. ユーザは, IC カードに個人情報を格納して管理する. サービス利用時には, サービスを受けるのに必要な個人情報のみを SS に提供し, SS から受け取ったサービス利用履歴を IC カードに蓄積する. そして, IC カードに蓄積されたサービス利用履歴などの個人情報を流通やバックアップの目的で個人情報管理サーバに送信する. 一方, SS が個人情報管理サーバに対して個人情報の要求を行うと, 個人情報管理サーバはユーザの定めた利用条件に基づき要求元に個人情報を提供するかどうか判断し, 提供が許可される場合のみ SS に個人情報が返却される.

提案システムを利用することで, ユーザは, 流通させたい情報やサービス利用に必要な情報を個人情報管理サーバに置いてユーザの意志に基づいて流通させ, プライバシー情報などの保護したい個人情報は IC カード内で安全に管理できる.

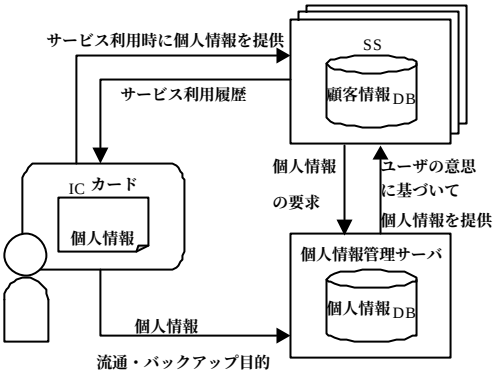

図 1. システムの概要

ここで, システムで取り扱う個人情報を整理しておく. 個人情報として, 本人を特定する氏名や住所などの情報はもちろんのこと, サービスの利用履歴やスケジュール情報やメールなど, あらゆる情報を想定しており, 最終的には個人に関する全ての情報を統一的なスキーマで取り扱うことが目標である. しかし, 利用サービスごとに SS が必要とする個人情報は異なるし, また, ユーザが提供する個人情報もサービスごとに異なるプロファイル情報を用いることもある. このように, 個人情報を統一的に扱えるスキーマの作成は困難であるため, 本システムでは, 将来の統一スキーマを目標としつつ, その第一段階として, 個人情報を以下の 5 つに分類して扱うこととした.

公的個人情報
IC カード発行時に設定する, 本人を特定するための情報. 行政によって定められる情報であり, ユーザは自由に書き換えられない.

一般個人情報
趣味・嗜好・ニックネームなど, 個人を特徴づける情報で, ユーザが自由に設定できる.

サービス固有情報
利用サービスごとに SS が設定する情報であり,

SSが管理する顧客IDやポイントやお買い得情報などが該当し，各 SS が更新権を持つ.

履歴情報

サービスを利用した時の利用履歴で，各 SS が追記権を，ユーザが削除権を持つ.

利用条件情報

システムに格納された個人情報を流通させる際に課すべき利用条件を記した情報であり, ユーザが設定する.

2.2. 機能要件

従来の SS を利用する場合，ユーザは様々な個人情報を提供する必要がある. ユーザが顧客登録を行う時には, ユーザの本人性を確認するために免許証や氏名などが要求される．また，ユーザが購入した商品を配達するための住所や, ダイレクトメールを送信するための電子メールアドレスを要求されることもある. さらに，SP はユーザから取得した個人情報を独自に管理しているため, ユーザが個人情報を更新したくても全ての SP の個人情報を更新するのは困難であり，また，SP がユーザの意図に反して個人情報を利用することもある. このような現状に対するユーザの要求をまとめてみた.

- 提供する個人情報は最低限におさえたい
- 提供した個人情報を自分の知らないところで勝手に利用されたくない
- SP への個人情報の提供はユーザ自身の意志で行いたい.
- 自分の個人情報を利用する場合は, その対価を受け取りたい

一方で，SP としては，これまで通りユーザの個人情報を収集したいと考えているため，SP の要求として,

- より多くの個人情報を収集して利用したい
- 信頼できる個人情報が欲しい
- 公正に個人情報を利用していることを証明したい

が考えられる．これらを踏まえ，提案システムに要求される機能を以下にまとめてみた.

① SP がユーザの許可なしに個人情報を勝手に利用できない仕組み（開示制御機能）
② SP に個人を特定させずにユーザがサービスを受けられる仕組み（匿名サービス利用機能）
③ SP とユーザ間の処理を管理サーバが仲介することで個人情報の利用を公正に行い，必要に応じてユーザに利益の一部を還元する仕組み（サービス仲介機能）

それぞれの機能について次章で検討する.

3. 検討事項

3.1. 開示制御機能

個人情報をネットワーク上で安心して取り扱うためには, ユーザの意志に反した個人情報の流通を防止する仕組みが求められる. つまり, 提供先の SP やその利用目的に応じ，どのレベルの個人情報を提供するかを判断する機能が必要である. この機能を開示制御機能と呼んでいる.

開示制御機能を実現する仕組み[6-8]を図 2 に示す．ここで, コンテンツ提供者はユーザであり, コンテンツは個人情報に該当する. ユーザは自分のコンテンツ(個人情報)にコンテンツを提供する際の条件（コンテンツポリシー）を付けてサーバに格納する．SP（利用者）は利用要求条件（利用者ポリシー）を提示してサーバの個人情報にアクセスする．サーバでは，コンテンツポリシーと利用者ポリシーの折衝が行われ, 個人情報各要素の開示／非開示の判断が行われ，SP は開示された部分の個人情報と利用許諾情報を受け取る．現在は，利用者の本人認証や属性認証も条件として記述でき, この結果に基づき情報提供の範囲を定める制御が実現されている.

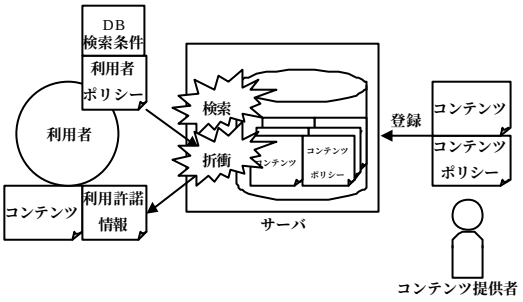

図 2. 開示制御の仕組み

提案システムでは，ユーザから SS への個人情報の提供には，ユーザが IC カードを用いて SS を利用する時と，SS が個人情報管理サーバの個人情報にアクセスする時の 2 つのケースが存在する．そこで，IC カード及び個人情報管理サーバに開示制御機能を実装し，SS からの個人情報の要求に対してユーザが設定する条件に基づいて開示制御を行う必要がある. プロトタイプでは開示制御機能の簡易版として, 個人情報の各カラムの開示／非開示を SS ごとに定めた利用条件情報を用いて判断する制御を実装することとした.

3.2. 匿名サービス利用機能

個人情報の中にはプライバシーに関わる情報も含まれることがあるので，SP への個人情報の提供が必要なサービスではユーザの心理的抵抗が大きい．そこで，筆者らはユーザが SP に個人を特定させずにサービスを利用できるようにする機能が必要であると考えた. この機能を匿名サービス利用機能と呼んでいる.

ユーザがサービスの利用登録を匿名で行う場合，SS はユーザの個人情報を取得せずに顧客 ID を発行してユーザに提供することになるが，この方法ではユーザが顧客 ID を容易に改竄できてしまう．そこで，ユーザの鍵ペアと顧客 ID を関連付けして SS が署名することで，この問題を防ぐこととした. サービス利用登録の流れについて図 3 に示す. ユーザの所有する IC カードから SS に公開鍵を提供し，SS は顧客 ID を発行して, 受け取った公開鍵と共に SS の秘密鍵で署名してサービス利用証明書を作成し，IC カードに書き込む.

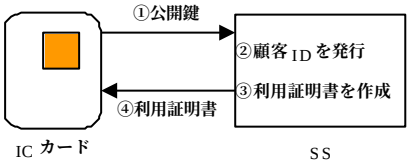

図 3. サービス利用登録の流れ

ユーザがサービスを利用する時は，SS は IC カードからサービス利用証明書を受け取り, 利用証明書からユーザの公開鍵を取得してチャレンジ＆レスポンスによる IC カードの認証を行う．ユーザは利用証明書以外の個人情報を SS に提供する必要がないので，SP に個人を特定させずにサービスの利用が可能となる.

ところが通常, ユーザは 1 つの公開鍵をシステム共通で用いるため，SS どうしがその公開鍵をキーに個人情報を名寄せできてしまうという問題がある. 図 4 を用いて具体的に説明すると，サービス A に提供した氏名情報とサービス B に提供した生年月日情報が公開鍵をキーに結び付けられてしまう．そこで，筆者らは公開鍵による名寄せを防止するために，SS ごとに異なる公開鍵を使用する方法を提案していた[5]．ユーザの IC カードから SS に提供される公開鍵を SS ごとに異なるものにすることで，SS どうしがその公開鍵をキーにユーザの個人情報を名寄せすることを防ぐことが可能となる.

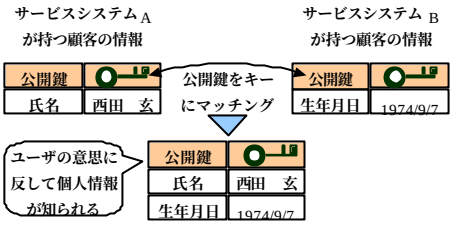

図 4. 公開鍵による名寄せ

現状の IC カードでは, SS ごとに鍵ペアを IC カード内部で生成すると時間がかかるため, プロトタイプでは予め鍵ペアを複数個作成して IC カードに格納しておき，その中から選択して使用する方法で実装している.

本システムでは, 個人情報管理サーバは信頼されることを前提としているが, システムのセキュリティを更に高めるため, 個人情報を暗号化して個人情報管理サーバに格納したり, 個人情報を細分化することで管理者にデータベース内の個人情報を参照させない仕組み[9]が提案されている. このようなサーバの信頼性を保証する方式については今後検討を進めたい.

3.3. サービス仲介機能

本システムにおいて, 個人情報管理サーバは, ユーザと SP の間に立って個人情報のやりとりを仲介する機能を提供している. これを個人情報管理サーバのサービス仲介機能と呼ぶ. 個人情報管理サーバで実現する開示制御機能は, ユーザの個人情報の SP への提供を代行する機能であり，また，匿名サービス利用機能は，SP の要求するユーザの身元保証を個人情報管理サーバに委託処理してもらう機能である.

サービス仲介機能を用いると，例えば，SP が全ユーザの個人情報を統計処理したい場合に, 全ユーザに個人情報の提供を求める代わりに個人情報管理サーバに統計処理を依頼すれば, サーバが所有する個人情報に対し統計処理が実行され，SP は処理結果を得ることができる．また，SP が，ある条件に合致するユーザに情報提供したい場合に, 個人情報管理サーバに情報提供処理を依頼することで，SP にユーザの個人情報を公開しなくても, 該当ユーザへの情報提供が可能になる.

このように, 個人情報管理サーバのサービス仲介機能により，ユーザは SP への個人情報の提供を必要最小限に抑え，システムとして，開示制御機能と匿名サービス利用機能と合わせ，個人情報の保護と流通の両立をサポートすることができる.

4. プロトタイプシステム

前章で述べた検討結果を踏まえ，個人情報の保護と流通を可能とする個人情報管理システムのプロトタイプを構築した．また，サービス仲介機能の例として，統計情報提供機能とダイレクトメール（DM）発送代行機能を実装した．

図 5 にプロトタイプのシステム構成を示す．SS 端末は，ユーザが IC カードの ID／パスワードを入力したり SS から受け取る利用履歴情報を確認したりするための端末であり，ユーザにとって信頼できる端末でなければならないため，SS とは別に設けている．各構成要素間の通信では相互にチャレンジ＆レスポンスによる認証を行うことで不正なアクセスや成りすましを防いでいる．プロトタイプシステムでは，認証局が登録局を兼ねている．

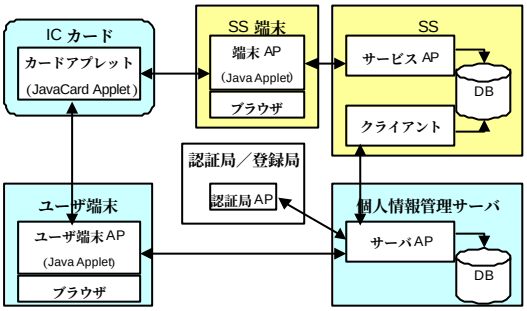

図 5. プロトタイプのシステム構成

プロトタイプシステムの動作について，SS としてコンビニエンスストアを例に，実際の画面を使用して説明する．

(1)事前処理

まず，IC カードの発行について説明する．ユーザは運転免許証などを登録局に提示してユーザ登録を依頼する．登録局は個人情報管理サーバにユーザ登録を依頼し，個人情報管理サーバはユーザ ID を払い出して登録局に送信する．登録局は，受け取ったユーザ ID に基づいてユーザの鍵ペアと証明書を作成し，公的個人情報と合わせて IC カードへの書き込みを行う．

ユーザは発行してもらった IC カードをユーザ端末に接続し，IC カード内に自分の一般個人情報として氏名（ニックネーム）・連絡先住所・電話番号などを登録しておく．

次に，SS の利用手続きについて説明する．ユーザは利用したいサービスの利用登録を SS に要求し，SS は顧客 ID を発行してサービス利用証明書を作成し，ユーザの IC カードに書き込んでおく．

(2)サービスの利用

ユーザは IC カードを利用してコンビニエンスストアで買い物をする．すると，ユーザの購入品情報が SS から利用履歴情報として SS 端末に送信され，画面上に表示される（図 6）．ユーザは表示された利用履歴情報の確認を行い，IC カードを挿入し履歴情報として書き込む．これにより，ユーザは簡単に履歴情報を収集することが可能となる．

図 6. SS 端末での利用履歴情報の表示

(3)個人情報の管理

ユーザは自宅のユーザ端末に IC カードを挿入し，IC カードに蓄積された履歴情報などの個人情報の閲覧／変更を行う．このとき，個人情報の一部を，流通やバックアップの目的で個人情報管理サーバに送信することができる．このとき，送信する個人情報に関する利用条件も同時に個人情報管理サーバに送信する．さらに，IC カードのメモリ容量に応じて，不要な個人情報を IC カードから削除することができる．

(4)個人情報の利用

個人情報管理サーバには複数のユーザの個人情報が集積することになる．SS が利用したい個人情報を要求すると，個人情報管理サーバはユーザが設定した利用条件に基づいて要求された個人情報を提供してよいかどうか判断し，提供してよい個人情報だけを SS に提供する．

図 7 の例では，SS は，趣味がテニスのユーザの生年月日・性別・趣味・履歴情報を取得している．このとき，個人情報提供の対価を SP から徴収してユーザに還元するようなサービスも考えられる．

図 7. マーケティング情報の取得

(5)DM 発送代行サービス

個人情報管理サーバのサービス仲介機能を利用して, エスクローや決済代行など様々なサービスが考えられる. その中で典型的なサービスとして，プロトタイプでは DM 発送代行サービスを実装した（図 8）.

SS は，DM を発送したいユーザの条件を指定し, DM の発送を個人情報管理サーバに依頼する．個人情報管理サーバは，SS が指定した条件に合うユーザを検索し, さらに検索されたユーザに DM を発送してよいかどうかを判断し，発送を許可しているユーザに DM を発送する．図の例では，SS は，趣味がテニスのユーザに対して，テニスラケットの特売情報を DM 発送しているが，ユーザの住所や氏名を知ることはできない.

図 8. DM 発送代行サービス

一般に, プライバシーを保護したいというユーザの要求と, パーソナライゼーションサービスを提供するためにユーザの個人情報を収集したいという SP の要求を同時に満たすことは難しい．しかし，本稿で提案した匿名サービス利用機能を用いることで, ユーザの匿名性を維持しつつパーソナライゼーションサービスの提供を可能としている.

5. まとめ

本稿では, ユーザが自分の個人情報を自分で管理するためのシステムとして, 個人情報の保護と流通を両立する個人情報管理システムを提案し, 構築したプロトタイプシステムについて報告した.

提案システムでは, ユーザが設定した利用条件に基づいて個人情報の開示制御を行うことによりユーザの意志に基づいた個人情報の保護と流通を実現し，また，個人情報管理サーバの与信を受けることで, ユーザが匿名でサービスを利用できる仕組みを実現した．さらに，個人情報管理サーバのサービス仲介機能を利用して，統計情報提供機能や DM 発送代行機能を実現し，ユーザが SP に提供する個人情報を必要最小限に押えつつ様々なサービスを享受できる例を示した.

今後は, ユーザ端末にも個人情報管理サーバ相当の機能を持たせて，SS に対してユーザが直接個人情報を提供する機能についても検討を進めたい．さらに将来的には IC カードを携帯電話などと組み合わせることで, 個人情報管理におけるユーザのコントロール性を拡張したいと考えている.

参考文献

[1] 堀部政男: プライバシーと高度情報化社会，岩波新書（2000）.

[2] .NetMyServices, http://www.microsoft.com/myservices/

[3] DigitalMe, http://www.digitalme.com/

[4] OneName, http://www. onename.com/

[5] 高倉健　他: IC カードサービスのための個人情報管理システムの検討，情処研報 DPS-104-5，pp.25-30（2001）.

[6] 山本太郎　他: 医療情報システムにおける情報開示制御方式, 情処研報 DPS-100-4, pp.19-24（2000）.

[7] 寺西裕一　他: 利用規約に基づくマルチメディアコンテンツ流通システムの設計, 情処研報 DPS-99-94，pp.31-36（1999）.

[8] 寺西裕一　他: マルチメディアコンテンツ流通における利用制約機構, マルチメディア・分散・協調とモーバイルシンポジウム論文集，pp.213-218（1999）.

[9] 保倉保 他: 「電子割符」のデジタル社会への応用, 情処研報 EIP-8, pp.19-25（2000）.