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

高倉 健，西田 玄，林 良一，櫻井 紀彦
NTTサイバーソリューション研究所
takakura@isl.ntt.co.jp, {nishida, ryo, sakurai}@dq.isl.ntt.co.jp

概要

ICカードサービス提供者が各々で管理している個人情報を、所有者であるユーザ自身が管理するために、個人情報を安全に格納し、利用条件に合致した範囲で流通させる機能を有する個人情報管理システムについて検討した。本システムでは、ICカードに個人情報管理アプリケーションを搭載し、サービス毎に設定している利用条件に基づいて個人情報の開示レベルを判断するという利用制御機能を実現する。またシステムには、複数ユーザの個人情報を管理する個人情報管理サーバを設けており、サーバに格納されている個人情報を各個人が定めた利用条件の範囲内で処理し、ユーザの匿名性を保証しつつサービス提供者に開示する機能を実現する。

Personal Information Management System for IC-card Services

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

Abstract

Most IC-card service systems want personal information(PI) to permit PI-management. Users are worried about privacy and so want some buffer between themselves and the service systems. This paper proposes a system that releases the service systems from having to perform their own PI-management, which means that they do not have to keep PI. The user accesses a service system and is given a service-system-generated-ID. The user then registers the ID with a central independent PI server and indicates what type of PI is available by the PI server. The PI server performs PI-management securely and makes the results available to the service systems as permitted by the user.

1. はじめに

近年、ITサービスにおいて、個人情報を用いたマーケティングが盛んになり、ユーザとサービス提供者(SP)の情報媒介手段としてICカードを用いたシステムが数多く構築されてきている。従来からSPは、会員証やポイントカードを用いて顧客の個人情報を管理し、顧客の囲い込みや動向分析に活用してきた。更に最近は、顧客情報管理の高度化や顧客情報の保護機能が求められるようになり、プライバシーに関わる情報を扱うサービスや、公共サービスに関わる分野では、ICカードの耐タンパー性が特に注目されている。

このようなICカードシステムが多数存在してくると、所持カード枚数が増すという単純な問題や、個人情報が電子化されることによる、ユーザが意図しない情報の流通、あるいは個人情報漏洩の危険が高まるという問題が生じる。ここ数年のICカードの動向[1-3]を見ると、ICチップの性能向上から高機能化と大容量化が進み、1枚のICカードで複数のサービスに対応できる多目的ICカードが登場し、前者の問題は多少なりとも解決されそうである。後者の問題については、SPはユーザの信頼を得るために個人情報利用ポリシーを提示する、あるいは第三者に保証してもらう等の対処が採られている。また社会制度的にも、個人情報保護の法制化が進みつつある。しかし結局のところ、顧客情報(これは個人情報の一部である)をSPが管理している以上、ユーザ自らが制

御することは不可能である。

そこで、個人情報をユーザ自身が管理し、サービスを利用する際にＳＰが要求する個人情報を、ユーザが制御可能な形で提供する方法を考えた。個人情報を不正な利用から保護する技術としては、映像や音楽などのデジタルコンテンツに用いられているカプセル化の技術[4-6]や、個人情報に利用制約を付して公開するという開示制御技術 [7-9]が提案されている。筆者らは、ICカードを用いたサービスシステムに適用するため開示制御技術に着目し、個人情報を安全に格納し、利用条件に合致した範囲で個人情報を流通させる機能を有する個人情報管理システムについて検討した。本稿ではICカードサービスにおける個人情報管理のあり方について考察を行い、試作中のシステムで実現する機能を紹介する。

2 ICカードサービスと個人情報管理

本章では、ICカードサービスシステムで取り扱われる個人情報の内容と利用方法、および、ICカードサービスシステムにおける個人情報管理の現状と、個人情報管理方法についての検討を行い、個人情報管理システムの目標を示す。

2.1 個人情報

ICカードサービスシステムにおいてＳＰが取り扱うユーザに関する情報は、ユーザを特徴付ける情報（住所、氏名、趣味、嗜好、など）と、当該ＳＰにおけるユーザの顧客情報（顧客ID、利用日、購買品目、取引金額、ポイントカード得点、など）とに分けられる。前者はユーザのプライバシー情報であり、サービス利用にあたりユーザがＳＰに提供する必要がある。後者はＳＰが独自に収集する情報である。

コンテンツ流通の動向が記された文献[10]では、情報をPrivacy, Knowledge, Privilege の3つに区分して考えている。プライバシー情報はユーザが保護したい情報であるが、プライバシー情報の一部と顧客情報を組み合わせると、SPにとって価値のあるマーケティング情報となり、ノウハウ情報(Knowledge)、あるいは所有権を主張すべき情報(Privilege)と位置付けることができる。これは流通させたい情報である。このように、ICカードサービスシステムで個人情報を扱う際には、保護と流通の両立を図らなければならない。

顧客情報の中にはサービス利用時の履歴情報が含まれているが、履歴情報はSP側だけでなくユーザ側でも収集できる。そこで本稿では、ユーザが管理する個人情報としてプライバシー情報と履歴情報を取り上げる。プライバシー情報を保護しつつ、プライバシー情報と履歴情報とで構成されるマーケティング情報を流通させるシステムを目標に、検討を進める。

2.2 個人情報管理方法

従来のICカードサービスシステム（SS）では、図1に示すように、各ＳＳにユーザが個人情報を提供しており、ユーザＡの個人情報インスタンスがＳＳ毎に管理されていた。ICカードは、各サービスがユーザを識別するための情報と、各SSに提供した個人情報の蓄積媒体としての役割を果たしている。このため、ＳＳ毎に別々のICカードが用意され、ユーザは複数のカードを持ち歩く必要があった。また、カード枚数が多くなるだけでなく、個人情報の一元管理ができないという問題があった。すなわち、各ＳＳで個人情報が管理されているため、個人情報に変更（例えば転居による住所変更）が生じたときに、全てのＳＳに対して変更処理を行う必要が生じていた。これは、個人情報はユーザ自身の情報であるにも関わらず、本人が情報内容を制御できないという根本的な問題に関わるものである。

近年、処理性能と記憶容量が向上した多目的ICカードが登場し、図２に示すように、1枚のICカードで複数のサービスに対応できる仕組みが実現できるようになった。ICカードプラットフォームとして、サービスシステム開発およびサービス提供のための共通基盤に関する研究[3]も行われている。しかし、個人情報はやはりSP毎に管理されており、先述の問題は解決していない。

そこで、図３に示すように個人情報のインスタンスをICカードに持ち、ＳＳ毎に提供する仕組みを検討した。ICカードの個人情報インスタンスをユーザ自身が更新できるようにすることで、個人

情報のユーザ自身による一元管理が可能になる。これは電子名刺、あるいは個人情報管理代行アプリケーションに相当し、ICカードではないが、実際のインターネットサービスにも類似サービスが登場[12-15]し、シングルサインイン機能などの各種機能を提供している。

図3のシステムをSP側から評価すると、SSが個人情報を管理しなくなり、また、ICカードの個人情報インスタンスにSS側からアクセスすることもできないので、SPにとってみれば、ユーザに働きかける手段がない、あるいは顧客動向が把握できない等、サービス遂行に差し障りが生じる。個人情報の複製をサービスシステムで管理する方法も考えられるが、ユーザの中には、SPに提供した個人情報の漏洩、あるいは個人情報の意図しない使われ方を懸念する意見があり、望ましい解決方法にはならない。

そこで、SSで複製を持つことなくSSから個人情報インスタンスへのアクセスを実現するために、図3において、ICカードそのものをアクセス可能にする方法を検討した。ICカードそのものにアクセスするには、ICカードを更に高機能化して表示機能や通信機能を付加する必要がある。ICチップ搭載の携帯電話も開発されており、筆者らは、近い将来にICカードが(ICカードの形を取るかどうか分からないが)携帯電話や携帯端末の一部として利用されると予想している。しかし、ICカードの高機能化は現時点での実現は難しい。

そこで、個人情報インスタンスをアクセス可能な場所に置く方法を考えた。本稿では、個人情報管理サーバを設置して、ICカードの個人情報インスタンスの複製を蓄積管理する仕組みを提案する。図4.の構成をとることにより、SSは個人情報管理サーバにアクセスすることで従来のサービスレベルを遂行できる。同時に、個人情報管理サーバには、個人情報の漏洩や、ユーザが意図しない個人情報の利用を防止するために、個人情報に利用条件を付してSPに提供する開示制御機能を設ける。SSが個人情報インスタンスにアクセスする仕組みは、ICカードと個人情報管理サーバの二系統があるため、開示制御機能をICカードAP、および、個人情報管理サーバAPとして構築する。

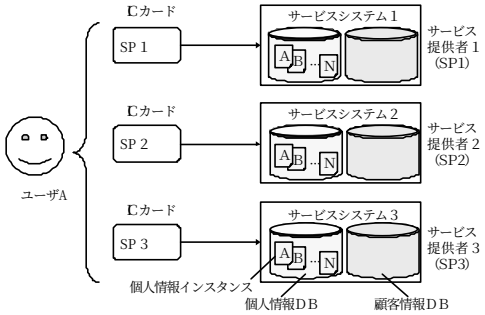


図1. 従来のICカードサービスシステム

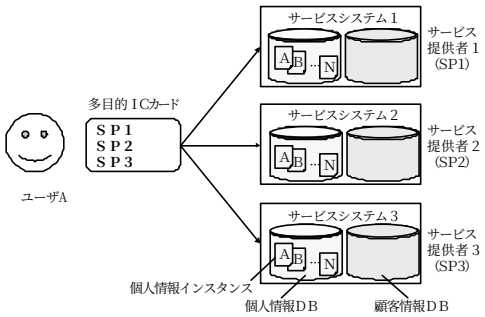


図2. 多目的ICカードを用いた場合

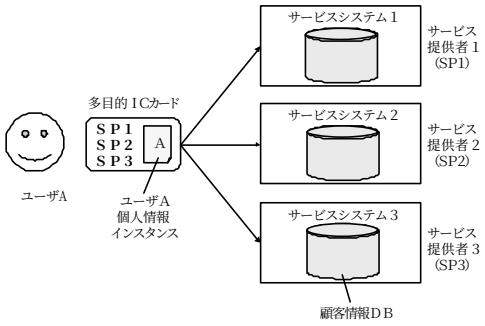


図3. ICカードに個人情報インスタンスを格納

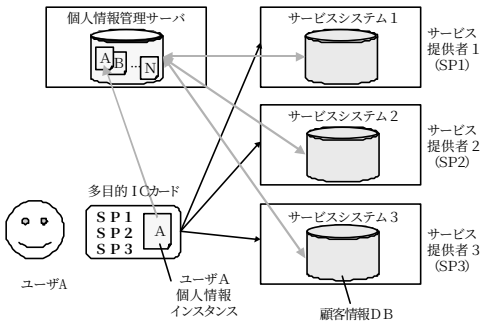


図4. 個人情報管理サーバに個人情報インスタンスを格納

3. 個人情報管理システム

3. 1. システム概要

個人情報管理システムは、図5. に示すように、主としてICカード(カード)、サービスシステム(SS)、個人情報管理サーバ(サーバ)の3つの要素から構成される。個人情報管理システムで実現すべき機能には、

- ICカードに蓄積された個人情報インスタンスを、SP毎に開示制御する機能
- 個人情報管理サーバの個人情報DBへの処理要求を、利用条件に基づき実行する機能
- SPを利用するユーザの匿名認証機能

がある。これらを実現するための、各構成要素の機能について説明する。

ICカード

カードには、各種サービスAPの他に、個人情報管理AP(管理AP)を搭載しておく。管理APは、個人情報インスタンスを蓄積し、サービスAPに応じ開示制御した個人情報をSSに提供する。サービス利用時には履歴情報を収集し、個人情報インスタンスに追加する。また、個人情報インスタンスのユーザが定めた情報と、該情報の利用条件情報をサーバに送信する。

サービスシステム

SSには、SSが提供するサービスAPと、サーバを利用するためのAPIを搭載しておく。サービスAPはユーザの要求に応じサービスを提供する。その際にカードとSSの間でチャレンジ&レスポンスを用いた顧客認証を匿名で行う。また、サーバに対しAPIを用いて個人情報DBの利用要求を送信する。

個人情報管理サーバ

サーバには、個人情報管理サーバAP(管理サーバAP)と、サーバの個人情報DBに対するリクエストを処理するためのAPIを搭載しておく。管理サーバ AP は、ユーザが送信した個人情報と利用条件情報の蓄積管理サービスをユーザに提供する。また、個人情報DB処理リクエストを、サーバがSSから API を介して受信すると、各個人情報を開示制御情報に基づく利用範囲内で処理し、SSに結果を返送する。特にSSが、個人情報DBをSSの顧客DBと連携させて得られた処理結果に基づくアクションを各ユーザにとる場合、管理サーバ AP はSSとユーザの仲介を行う。またサーバは、ユーザやSSに対しチャレンジ&レスポンスを用いた相互認証を行う。

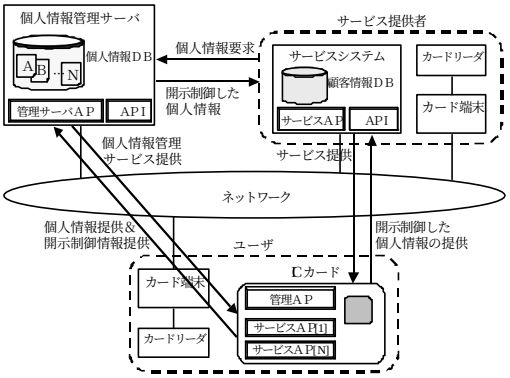


図5. 個人情報管理システム概要図

3. 2 開示制御機能

本稿で提案しているシステムは現在試作中だが、これに先立ち、ICカードの管理APで簡単な開示制御機能を実現しているので、その画面を図6に示し説明する。

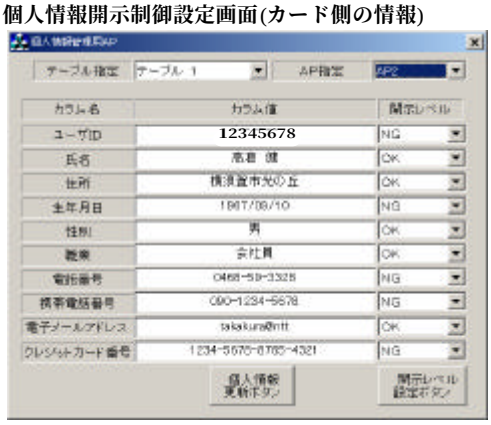
図6上図は、ICカードを挿入したカード端末上で参照されるICカードの個人情報および開示制御情報の設定画面である。カードに蓄積する個人情報としてカラムに記された値を設定し、開示制御対象とするAPへの各カラムの開示レベルを、OK/NGの二値で制御している。

該当するSSでカードから個人情報を入手しようとした場合、図6下図の個人情報開示結果が、サービス提供者のカード端末上に表示される。開示制御の結果、非開示のカラムは(比較しやすいように)空白カラムとして表れる。

本試作システムにおいて、カード側の開示制御機能は、同様の管理APで実現する。一方、サーバ側の開示制御機能は、カードの開示制御に加え、利用条件を判断した処理が求められる。サーバは、個人情報を各ユーザに代わって提供しており、いわば情報流通仲介サービスを提供している。つまり、サーバ側に求められる機能は、情報仲介機能[11]に求められる機能を含む幅広いものである。当面試作システムでは、開示制御

情報として設定可能な利用条件のみを対象とした処理を実現することとする。

個人情報開示制御設定画面(カード側の情報)



個人情報開示結果（SS 側の情報）

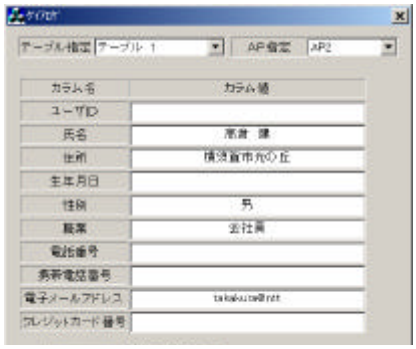


図６．個人情報開示制御の実現例

３．３ 個人情報ＤＢ連携機能

次にサーバの個人情報ＤＢとSSの顧客情報ＤＢの連携機能について説明する。

従来SS内で管理していた個人情報を外部のサーバに蓄積するシステムアーキテクチャの変更は、個人情報を含めて顧客情報管理を行っていたＳＰにとって問題である。SPたちに本システム構成を受け入れてもらうためには、サーバに正確で鮮度の良い情報を蓄積すること、そしてＳＳから容易にアクセスできることが求められる。

ユーザに、正確で鮮度の良い情報をサーバに提供してもらうには、サーバの信頼性が重要である。試作システムでは、先に述べた開示制御機能に加え、各システム構成要素間で公開鍵暗号方式によるチャレンジ＆レスポンスを用いた相互認証を行う。

一方、サーバへのアクセスを容易にするには、個人情報ＤＢをＳＳの顧客情報ＤＢと連携させるための仕掛けが必要になる。両者のＤＢを関連付ける方法はいくつか有るが、本システムでは、ＳＰのID(SSID)とSPが個人に払い出した顧客 IDのセットを用いている。

SSID と顧客 IDによるＤＢマッチングをより安全に実現するために、カードとSSの間では、ユーザが匿名のままでもＳＳに信頼してもらえるよう、公開鍵暗号方式の鍵ペアをSS毎に使い分けている。複数のＳＳに共通の公開鍵を利用すると、公開鍵を主キーとして相関をとることで複数ＳＳにまたがった個人情報が結び付けられ、利用者像が割り出される危険がある。公開鍵のSS毎の使い分けは、これを防ぐための措置である。

３．４ 個人情報管理システムの処理の流れ

ここで、個人情報管理システム全体としての処理の流れを図7にまとめておく。

ユーザ（カード）およびＳＳには、固有 IDとしてユーザ ID(UID)とSSID が各々割り当てられる。個人情報管理システムを利用するユーザはサーバに個人情報を登録しておく。これは、サーバの個人情報ＤＢにインスタンスとして蓄積される。

ユーザが新しいサービスを利用するには、最初にＳＳに利用申請を行う。ユーザは公開鍵暗号方式で用いる鍵ペアをＳＳ用に生成し、公開鍵($PK_{U1,S2}$)をＳＳに送付する。SSはユーザに顧客 ID(図の例では S2ID)を発行し、S2ID と公開鍵($PK_{U1,S2}$)にＳＳの秘密鍵(SK_{S2})を用いて証明証を生成する。SSはユーザに、利用許可情報として、証明証とＳＳの公開鍵(PK_{S2})とSSID を送付する。ユーザは送付された情報から顧客 ID等を抽出し、利用サービスとして SSID とS2ID のセットをサーバに登録する。

ユーザがサービスを利用するには、SSによる顧客認証が必要である。特にユーザのプライバシー情報の流通機会を抑えるため、試作システムでは匿名認証を行う。ユーザがSSから受け取っていた証明証をＳＳに送付すると、ＳＳは証明証を解析し、SSへのアクセスが利用申請済のユーザの顧客 IDであることを確認する。またＳＳは、アクセスしてきたユーザが信頼できる顧客であるかどうか、必要に応じてサーバにサービス登録状

況を確認しても良い。

サービス履歴はＳＳとユーザの双方において蓄積可能である。ユーザが収集した履歴情報は、ユーザの意思に基づき、サーバの個人情報ＤＢに追記される。またＳＳでは、利用履歴を顧客ＤＢで管理する。

ＳＳがサーバの個人情報を参照するには、サーバに SSID とS2ID のセットで個人情報照会要求を送信する。サーバはこのセットをキーとしてユーザを特定する。サーバは、該当ユーザの個人情報に対し、要求元 SSに対し定めた利用条件に基づいて、開示しても良い情報をＳＳに提供する。ＳＳでは、受け取った個人情報を、ＳＳが所有する顧客情報とＤＢ連携して、当該ユーザに関するより詳細な情報を構築することができる。

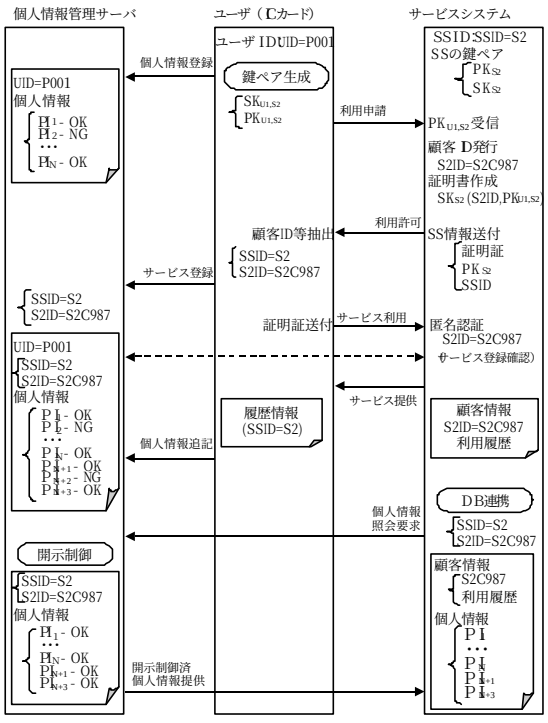


図 7. 個人情報管理システムの処理の流れ

4. まとめ

現在の ICカードサービスには、個人情報の所有者であるユーザが自身の個人情報を管理できないという問題がある。そこで、ユーザ自身が個人情報を管理可能にし、個人情報の保護と流通を両立する仕組みを検討した。その実現方法として、筆者らは個人情報管理サーバを用いてサービス提供者から個人情報にアクセスでき、また、ユーザの意思に基づき個人情報を開示制御するシステムを提案し、現在試作中である。

本システムの目的として、個人情報の漏洩や、ユーザが意図しない個人情報の利用の防止を挙げた。しかし、個人情報管理サーバの開示制御の結果としてサービス提供者に渡された情報については、漏洩や流通を防ぐことができない。今後は、個人情報の開示制御後の利用を制御するために、カプセル化技術の導入についても検討していきたい。

参考文献

[1] ICカード総覧 2000, シーメディア (1999).

[2] eコマースシステム技術体系, フジ・テクノシステム (2001).

[3] 山本修一郎 他:ネットワーク指向ICカードプラットフォーム,NTTR&D, Vol.49, N0.12, pp.759-776(2000).

[4] 谷口展郎 他: Javaを用いた動画配信用著作権保護カプセル,情処研報 DPS-98-6. pp.31-36 (2000).

[5] 阿部剛仁 他:Java を用いた動画配信カプセルの実装, 情処 DPS ワークショップ (2000).

[6] 西岡秀一 他:コンテンツ流通情報管理機構の実現, 情処研報 DPS-102-14 (2001).

[7] 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 DPS100-4, pp.19-24(2000).

[8] 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).

[9] 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).

[10] 櫻井紀彦 :カプセル化コンテンツの動向と展望, 情処研報 EIP-12-1, pp.1-6(2001).

[11] 前川徹 :インフォメディアリ(情報仲介業), 情報処理 vol.41 No.10, pp.1150-1151(2000).

[12] Passport, http://www.passport.com/

[13] Persona, http://www.persona.com/

[14] digitalme, http://www.digitalme.com/

[15] Lumeria, http://www.lumeria.com/, http://www.superprofile.com/