東北大学機関リポジトリ
TOUR
Tohoku University Repository

人間性・社会性を考慮した情報サービス構築に関する研究

著者	半井　明大
学位授与機関	Tohoku University
URL	http://hdl.handle.net/10097/53961

平成 23 年度　修士学位論文

人間性・社会性を考慮した情報サービス構築に関する研究

東北大学大学院情報科学研究科 情報基礎科学専攻

博士課程前期 2 年の課程

コミュニケーション論講座 (木下研究室)

B0IM1034　半井 明大

目 次

図 目 次

表 目 次

第1章　序論

本章では，近年の情報サービスの動向と次世代の情報サービスの備えるべき性質について論じ，人間性・社会性を考慮した情報サービス構築に関する問題点を述べる．続いて，本研究の目的と本研究における効果をあげ，最後に本論文の構成について述べる．

1.1　研究の背景

情報サービスが人々の生活に浸透し，人間に歩み寄るところとなってから久しい．事実，近年の情報サービスを広く鑑みると，様々なIT技術の革新に伴い，これまで利用者が情報サービスを利用するために自ら歩み寄り，その存在を意識しながら利用するものであった情報サービスは，情報サービスがより柔軟に利用者に対応し，サービス利用者がその存在を意識しなくとも情報サービスの恩恵を与ることができる情報サービスへとそのあり方を変えてきている．

情報サービスと人間の距離感に関するパラダイムシフトの中で，ユビキタス [1] という考え方が生まれた．ユビキタスという言葉は，情報サービスの人間への歩み寄りをよく表した言葉であり，近年，情報サービスに対する考え方の新機軸として広く注目されている．ユビキタスとは「遍在する計算機資源を意識しなくともいつでもどこでもその恩恵を受ける事ができること」を表し，mobility(移動性)，pervasiveness(遍在性) 等の性質で表現されることが多い．

こうしたユビキタスの考え方に基づき,「いつでも」・「どこでも」その恩恵をサービス利用者が享受できるような情報サービスであるユビキタス情報サービスがユビキタス情報社会を支える重要な要素として注目されてきており，研究・開発が近年，広く行われて

いる．例えば，健康支援システム [2, 3, 4]，ライフログを活用したシステム [5, 6, 7]，ナビゲーションシステム [8, 9, 10] など枚挙にいとまがない．

一方で，人間に寄り添うという意味でサービスのパーソナライゼーションに関する技術の進歩も目を見張る物があると言える．パーソナライゼーションは「その人用にカスタマイズする」という意味であり，既に種々の Web サービス等では，サービス利用者のプリファレンスを収集し，利用者にあったサービスを提供するというものを指す．情報サービスを利用する際に，利用者は時に自ら情報サービスを自ら合った物にするために操作する等，複数の異なるサービスを組み合わせる事でより自らに適した情報サービスの恩恵を得る事ができると考えられる．そこで，情報サービス側でパーソナライゼーションを行い，サービス利用者が意識しなくとも自分のためのサービスが提供される事は非常に重要な事となってくる．パーソナライゼーションに関する研究もまた，数多くの研究がなされており，近年目を見張る物である [11, 12, 13]．更に，パーソナライゼーションを実現した情報サービスも数多く実現され，身近な物となってきている．例えば，Amazon.com[14] における商品推薦システムや，iGoogle[15] におけるウェブページパーソナライゼーションなどが実現された事例として挙げられる．

こうした一連の情報サービスの歩みを受けて，将来のユビキタス情報サービスは，先に述べた移動性や遍在性による「いつでも・どこでも」に加えて,「誰でも・いつものように」利用可能な情報システム，言い換えればサービス利用者の人間性・社会性を考慮した情報サービスの実現が求められることが予想される [16].

本研究においては，人間と情報サービスの間における人間性，並びに社会性を以下のように定義する．

人間性 - ”だれでも”

特別な端末を利用しなくとも自分用にパーソナライズされたサービスが提供できる性質

社会性 - ”いつものように”

使い慣れていないサービスでも柔軟に対応し，各サービスへの個人情報の事前登録

がなくとも慣れ親しんだサービスが提供できる性質

特別な端末を持つ必要性が生まれる事で，サービス利用者は端末を正しく運用しなければならない．しかしながら，その煩雑さによって高度な情報サービスを利用可能な人が限られてしまう可能性がある．従って，先に述べた人間性を保証する事は，その様な制約を取り除き全ての人がその情報サービスの恩恵を与ることを実現する上で重要な性質であると考えられる．

また，サービス利用者に歩み寄る情報サービスを考えるとき，その情報サービスは，例えそれがサービス利用者にとって初めて利用するサービスや不慣れなサービスであったとしても，サービス利用者の状態や生活シーン，状況などを考慮し柔軟にパーソナライズされているべきである．そのためには，サービス利用者の特徴を表す情報を予め各々のサービス提供者に登録しなくとも利活用可能である必要がある．上述の社会性は，複数のサービスの垣根を越えて，サービス間が間接的に連携し，利用者に状態や生活シーン，状況などを考慮した情報サービスの提供を可能にする．

以上述べた人間性・社会性を考慮した情報サービスの構築には，サービス利用者の状況を考慮することが肝要であり，個人情報を利活用し，人間性・社会性を考慮したサービスパーソナライゼーションが必要不可欠となってくる．

尚，本研究において個人情報とは個人情報の保護に関する法律２条１項に定められている「生存する個人に関する情報であって，当該情報に含まれる氏名，生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ，それにより特定の個人を識別することができることとなるものを含む.）」[17] ではなく,「サービス利用者の好みやプリファレンス，健康状態などの個人の特徴を表す情報」を意味するものとする．

1.2　本研究の目的

図 1.1 に人間性・社会性を考慮した情報サービスの例を示す．人間性・社会性を考慮した情報サービスの例としては，薬局における服用中の薬や体調を考慮した医薬品購入補助システム，レストランにおけるアレルギーや体質などの健康情報を利用したメニュー推薦システム，タクシーにおける位置情報や住所情報を利用した行き先指示システム，バス等における体調や年齢などの乗客情報を考慮した公共交通機関システム等が考えられる．

これらの情報サービスは，人間性・社会性を考慮し，誰でも・いつものように情報サービスの恩恵を享受できるようにするために，サービス利用者の個人情報を積極的に利活用し，パーソナライズすることが肝要となってくる．

このような高度なパーソナライゼーションにおいては，サービス利用者が情報サービスを利用するために特別な端末を携行しなければならない制約があった場合，子供や高齢者等の端末を持ち歩き複雑な管理・操作をすることが困難な利用者が情報サービスの恩恵を受けることができないため，情報サービスの人間性が損なわれると考えられる．

また，サービス提供者と個人情報の保有者が一致し，各々のサービス提供者が個人情報を保有している場合，各々のサービス提供者はサービス利用者の個人情報を閉鎖的に管理する．そのため，サービス利用者が同一の利用コンテクストや生活シーンといった利用者の状況を軸に情報サービスをパーソナライズしようとする際に，個人情報を共用する事ができないため，情報サービスの社会性が損なわれると考えられる．

これを受けて本研究では，誰でも・いつもの様に使える，利用者の状況を考慮した情報サービスの実現を目的とする．

そのために，人間性・社会性の両方を考慮した情報サービスパーソナライゼーションが重要となってくる．しかし，従来のサービス提供者とサービス利用者のみからなるパーソナライズモデルにおいては，人間性及び社会性のいずれかを満たす事はできたが，人間性・社会性を両立する事が困難であった．

そこで，本研究ではこの人間性・社会性を両立できないという問題点を解決すべく，開放型の情報サービスパーソナライズ手法を提案する．即ち，サービス利用者が所有する個

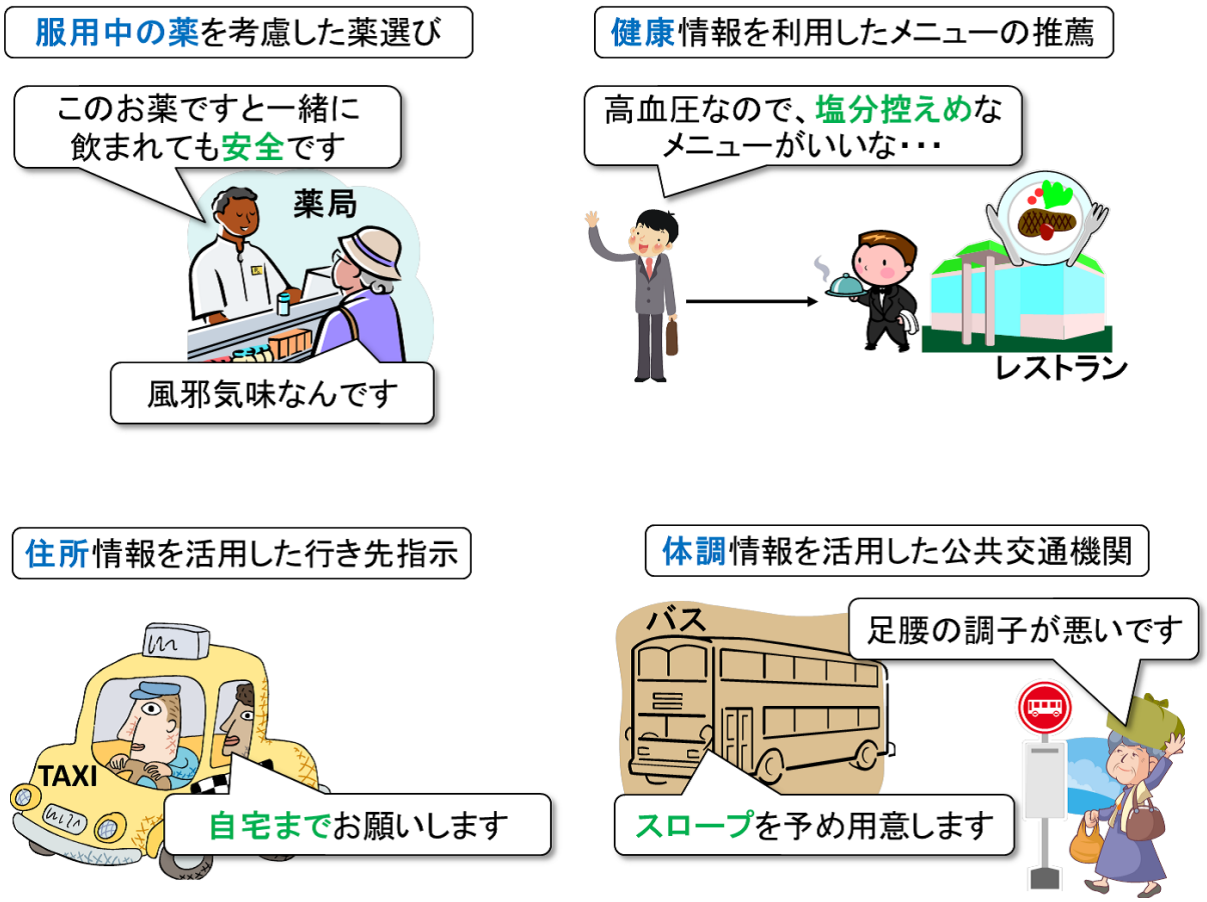


図 1.1: 人間性・社会性を考慮した情報サービスの例

人情報管理機構と開放型の個人情報要求・開示プロトコルを定め，本提案の実現する上で必要な技術要素を与える．また，プロトタイプシステムを用いた情報サービスのカスタマイズに関する実験評価を行い，提案手法の有効性を検証し，本提案によって人間性・社会性を考慮した情報サービスが構築可能である事を示す．

1.3　本研究の効果

本節では，提案手法を用いて人間性・社会性を考慮した情報サービスの構築を実現した際に得られる効果について説明する．既存のパーソナライズ手法による個人情報を用いた情報サービスの構築と提案手法による個人情報を用いた情報サービスの構築の比較の例を図 1.2 に示す．図で取り上げている例は，薬局での医薬品購入補助システムとレストランでのメニュー推薦システムである．

従来のパーソナライズ手法では，サービス利用者は情報サービス毎に利用者に関する情報を予め登録しなければならず，サービス利用者にとって負担となっていた．また，この事前の登録をしないために，個人情報を携帯端末に保持し，それを提示する形も考えられるが，携帯端末に個人情報を保持する事は，携帯端末自体の紛失による個人情報の漏洩，持ち歩く際の運用ポリシーの策定，保有する複数端末間での情報の同期等，端末の運用に関して利用者への負担が増加するため，子供や高齢者等を含む広く様々な人々が利用する情報サービスにおいては問題となってくる．そのため，こうした障害が情報サービスの人間性を著しく阻害していると考えられる．

また，情報サービス側に登録された情報は，各々のサービス提供者が独自の形式やポリシーをもって管理するため，サービス利用者の個人情報をサービス間で共用することは運用上できず，各々の情報サービスの範疇においてのみパーソナライズすることしかできなかった．これは，各々の情報のサービスの枠を越えて，サービスの利用者の状況，コンテクスト，生活シーンといったより柔軟な枠で使い慣れないサービスでもいつものように情報サービスを提供することを困難にしてしまっており，情報サービスの社会性の実現を阻害していると考えられる．

提案手法を用いた場合，サービス利用者は情報サービスで利活用したい個人情報を個人情報管理機構に登録するだけで良く，特別な端末を持ち歩く必要もないため，老若男女誰もが人間性を考慮した情報サービスの恩恵を享受できる．

また，サービス提供者から分離された開放型機構に個人情報を登録してあるため，複数のサービス間で同じ個人情報を共有できる．そのため，サービスの利用履歴や位置情報と

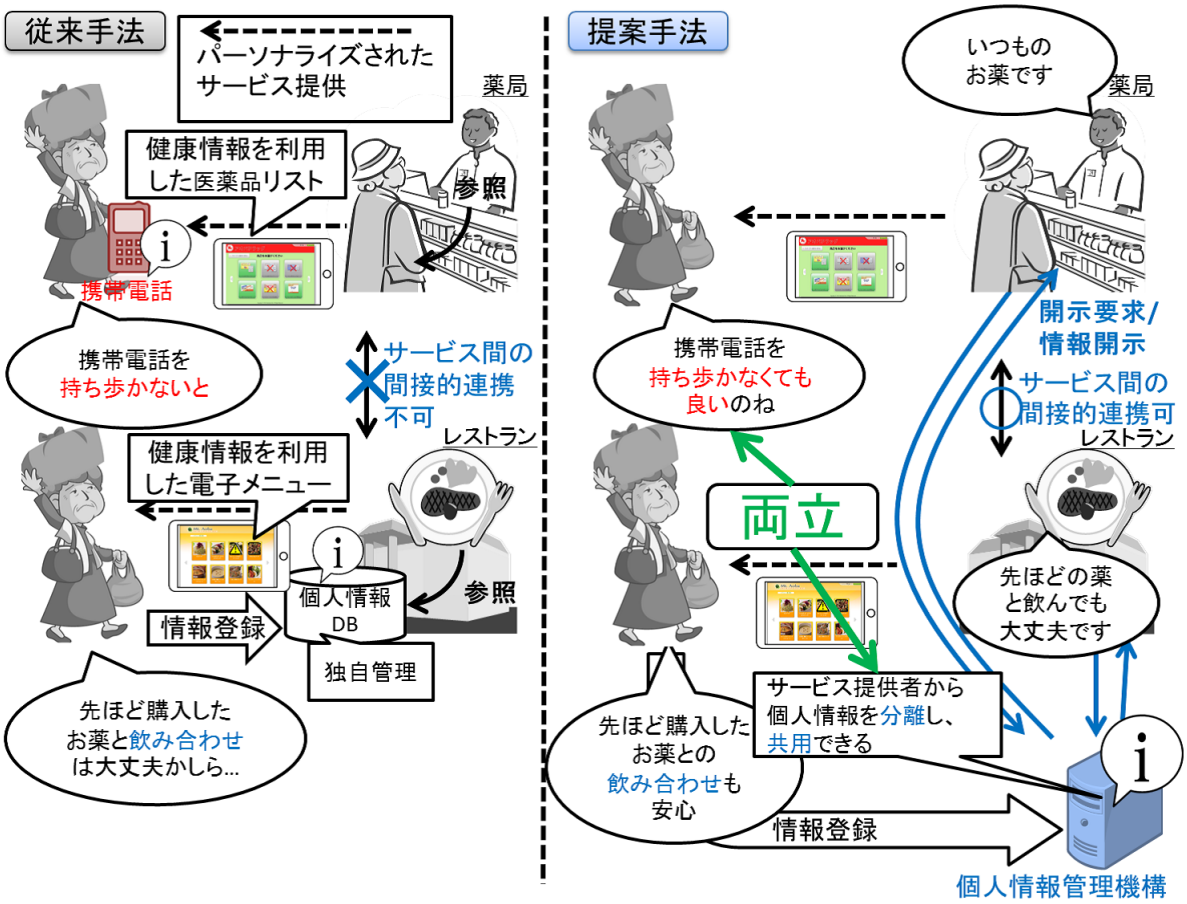


図 1.2: 本研究の効果

いった刻々と変化する動的個人情報を活用する事も容易になるだけでなく，例えば，利用者の食事や医薬品の利用といった「健康」を主軸にしたパーソナライゼーションや，一日の行動等の「コンテクスト」を考慮したパーソナライゼーションといった情報サービスの間接連携よる高度な情報サービスのパーソナライズが実現可能となる．

1.4　本論文の構成

本論文は，以下のような構成となっている．第 2 章において関連研究を紹介し，情報サービスのパーソナライゼーションにおける問題点を述べる．次に，第 3 章において，利用者が所有する個人情報管理機構（U-PIMM）と個人情報を開示・要求と個人情報アクセスの正当性検証を可能にする個人情報開示要求プロトコル（OSPP）からなる開放型の情報サービスパーソナライズ手法を提案する．更に，第 4 章で提案手法のプロトタイプシステムの設計と実装を述べる．その後，第 5 章でデモシステムを用いた情報サービスのパーソナライズに関する実験を通して提案手法の有効性を評価する．最後に，第 6 章でまとめと今後の課題について述べる．

第2章　関連研究と課題

本章ではまず，情報サービスのパーソナライゼーションについて述べ，それらに関する既存研究を紹介する．その後に，情報サービスのパーソナライゼーションについての問題点について述べる．

2.1　情報サービスのパーソナライゼーションと個人情報の利活用モデル

情報サービスのパーソナライゼーションに関する研究は広く行われている．情報サービスのパーソナライズするにあたって，サービス利用者の個人情報は必要不可欠であり，どの様に管理するか，またパーソナライズする際にどの様に利用されるかは情報サービスのパーソナライゼーションにおいて重要な事項となってくる．

次節から，サービス利用者のカスタマイズモデルについて個人情報の管理・利用に着目して論じる．

2.2　関連研究（１）：サービス提供者が個人情報を管理するサービスパーソナライズモデル

始めに，サービス提供者が個人情報を管理するサービスパーソナライズモデルについて，いくつか関連研究を紹介する．

Pharos[18] は，多種多様なコンテンツを含むウェブサイトをパーソナライズする手法である．従来，新しいユーザへのコンテンツレコメンデーションを主体とするパーソナライ

ズでは，レコメンデーションするための利用者のデータが出揃わず初期段階で適切なレコメンデーションができないというコールドスタート問題を抱えていたが，Pharos では Social Network Service から類似する利用者を捜し，そこから共通するプリファレンスを抽出することで，よりスムーズなレコメンデーションを可能にする手法である．

ペルソナカード [19] は，サービスを利用する際に一サービス利用者をペルソナという「個人の社会的な顔」をベースにサービス固有 ID と公開ペルソナ ID という双方の識別子を用いる事で認証を行い，ペルソナ単位で個人情報の交換が可能になるため，よりきめ細やかなパーソナライゼーションを安全に行う事が可能である．

Ubiquitous Personal Study[20] は，個人情報のハブとなる機構であり，分散したユーザのプリファレンスを集めて統合することができる．開示に関する制御は特になく，事実上サービス提供者側で自由に収集したプリファレンスを管理する形になる．

Feature Modeling と persona を活用した電子サービスのパーソナライズ手法 [21] はサービス利用者から収集したペルソナをユーザプロファイルとして，ユーザのニーズを検出しながらサービス利用者に提示されるユーザインターフェース等をパーソナライズする手法である．

サービス提供者が個人情報を管理するサービスパーソナライズモデルは，図 2.1 に示すように，サービス提供者がサービス利用者の個人情報を閉鎖的に管理し，サービス利用者は，個々の情報サービスの範疇でパーソナライズされたサービスを受ける形となる．

このモデルの利点は，個人情報を持ち歩かなくともパーソナライズされた情報サービスを利用できる点である．これは，特別な端末を持ち歩かなくとも，誰もが情報サービスを受けられるということになる．一方，このモデルの欠点は，情報サービスのパーソナライズを受けるためには，サービス利用者の個人情報を事前に登録しておかなければならないと言う点である．また，登録されたサービス利用者の個人情報は，各々のサービス提供者が閉鎖的に管理するため異なるサービス間で共用する事はできず，異なるサービス間での間接的な連携が困難であるという点も欠点として考えられる．

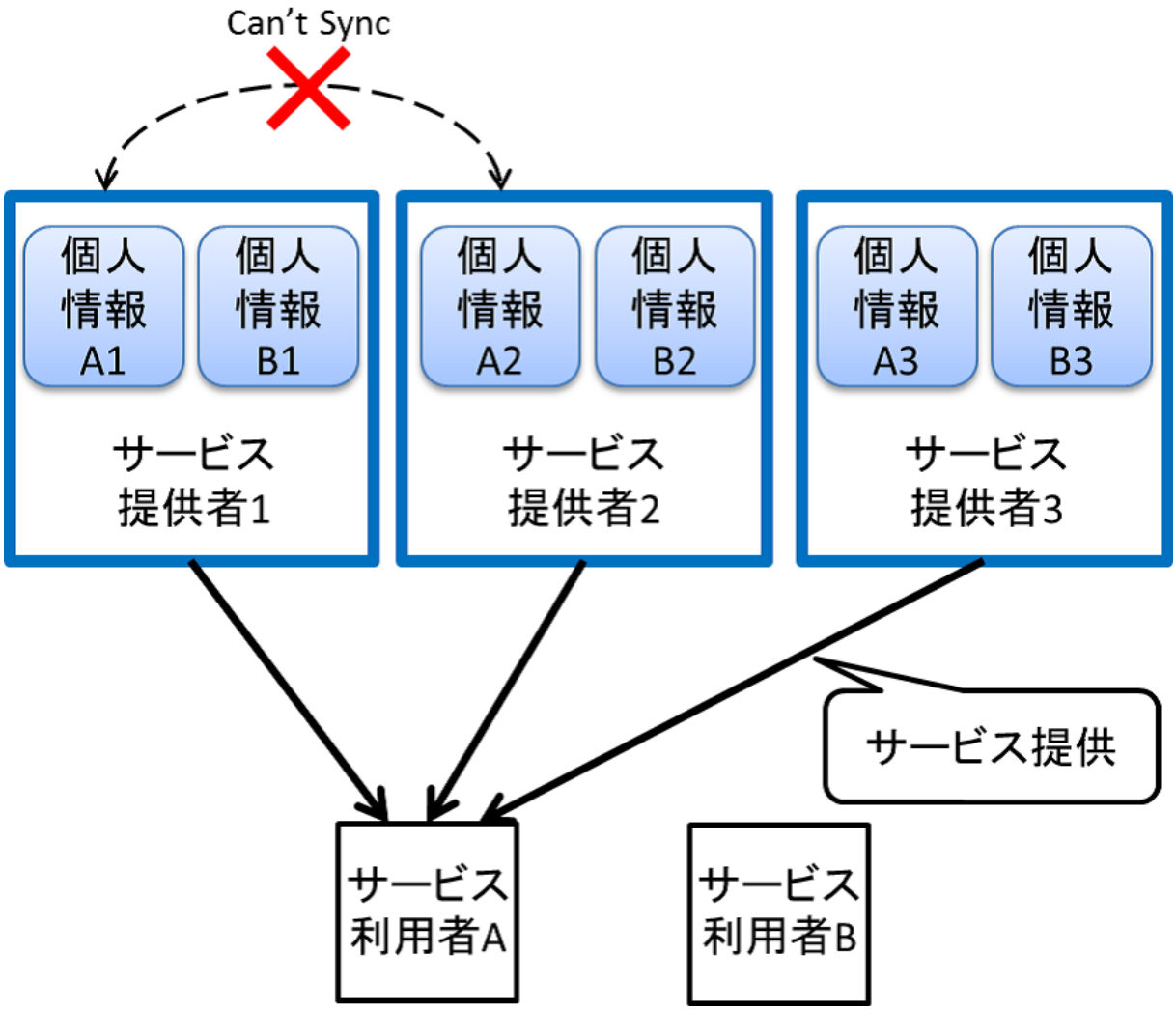


図 2.1: 関連研究（1）：サービス提供者が個人情報を管理するサービスパーソナライズモデル

2.3 関連研究（２）：サービス利用者が個人情報を保持するサービスパーソナライズモデル

次に，サービス利用者が個人情報を保持するサービスパーソナライズモデルについて，いくつか関連研究を紹介する．

PRIME[22] は研究機関主導の次世代個人情報交換システムである．PRIME プロジェクトでは，個人情報をサービス利用者が安心して利用できるようにするためにサービス利用者の個人情報開示ポリシーとサービス提供者の個人情報利用ポリシーを定義し，個人情報交換時にそれらのネゴシエーションを行う．PRIME では，サービス提供者とユーザクライアントである端末双方に PRIME middleware を導入することで高度な個人情報交換のネゴシエーションを可能にし，サービス提供者が取得した個人情報にラベルを付けて管理することで，ネゴシエーションによって決められた利用ポリシーに従った運用が強制できる．

personal home server[23] は，家庭のホームネットワークにおいて居住者のプリファレンスに従った電気機器の利用を可能にするパーソナライズ手法である．personal home server はサービス利用者が個人的に所有する携帯端末や腕時計，ジャケットなどに実装される．そのため，いつでもどこでも持ち歩く事ができ，そこに格納されているプリファレンスを用いて家庭の電気機器を発見し，自分用の設定を施すことが可能になる．

モバイル端末を用いた広告パーソナライズ手法 [24] は，コンテンツパーソナライゼーションの手法の一つである．サービス提供者はサービス利用者側にある個人情報を獲得し，人工知能モジュールが推論する事でターゲットのサービス利用者に提示されるアドバタイズメントをパーソナライズできる手法である．

Mobile Information Service Broker[25] は，移動情報サービスのパーソナライズの際のアイデンティティ管理のフレームワークであり，パーソナライズの際のプリファレンスの扱いについてポリシーコントロールを行い，プリファレンスのプライバシーを保護しつつ，個人情報を活用できる手法である．

サービス利用者が個人情報を保持するサービスパーソナライズモデルは，図 2.2 に示すように，サービス利用者が自身の個人情報を携帯端末等に保持し，持ち歩くモデルであ

る．そして，サービス利用時には，サービス提供者に個人情報を提示し，サービス提供者は提示された個人情報を用いて情報サービスをパーソナライズする．

このモデルの利点は，利用者の個人情報が利用者側の携帯端末にあるので，異なるサービス間で個人情報を共用でき，サービス間での間接的連携が可能である点である．一方，このモデルの欠点は，端末携帯時の情報流出防止や複数端末間の情報同期の確保などをはじめとする一連の携帯端末に関する運用の煩雑さが生じるためサービス利用者への負担が増加すると考えらえる点である．

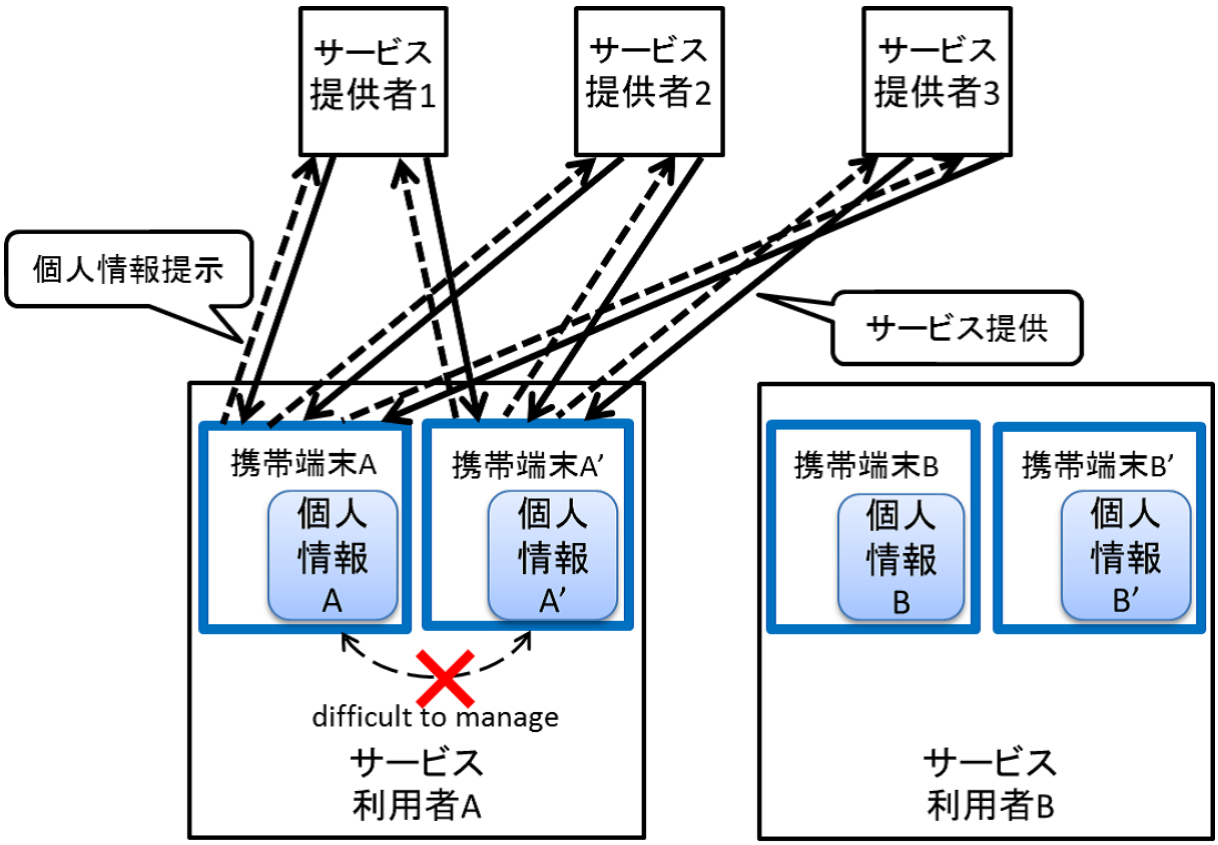


図 2.2: 関連研究（２）：サービス利用者が個人情報を保持するサービスパーソナライズモデル

2.4　関連研究が抱える問題点

本節では 2.2 節，2.3 節で紹介した関連研究についてそれぞれの特徴を改めてまとめながらその抱える問題点を説明する．

関連研究（１）の問題点（図 2.3(a)）

1. 情報サービスの提供者と個人情報の分離ができない
2. 事前にサービス利用者の個人情報を登録がないと情報サービスをパーソナライズすることできない
3. 異なる情報サービス間で利用者の個人情報が共用できず，サービス間の間接的連携が困難である

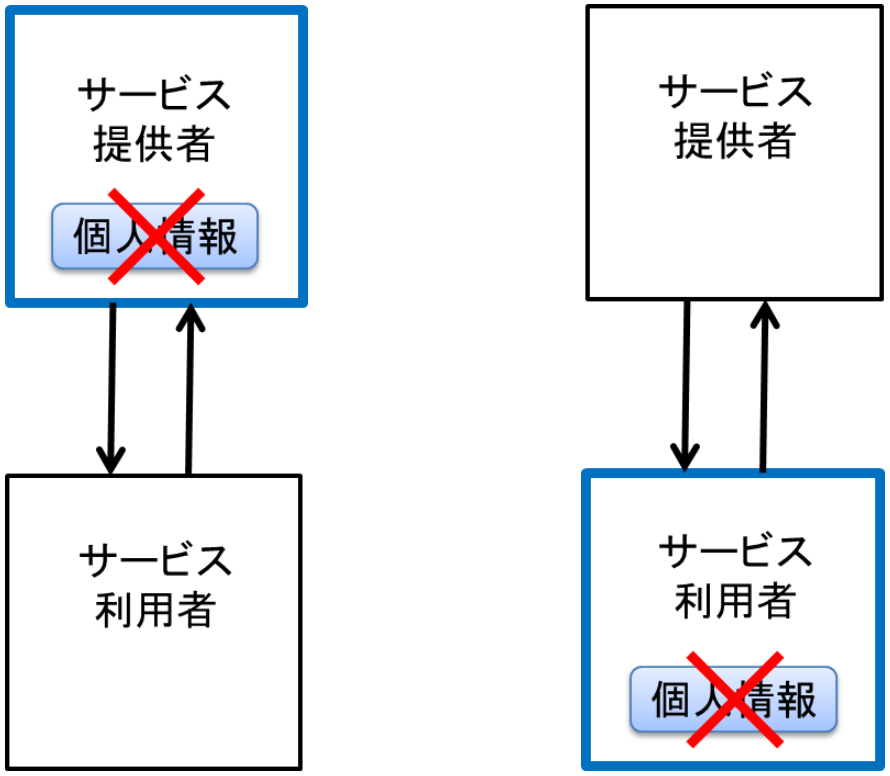
関連研究（２）の問題点（図 2.3(b)）

1. 携帯端末を使って，個人情報を携行しなければならない
2. 端末携帯時の情報流出防止や複数端末間の情報同期の確保等，運用・携行の煩雑さによる利用者の負担が増加してしまう

関連研究（１）については，特に特別な端末がなくとも情報サービスをパーソナライズできるため，情報サービスの人間性が確保できているものの，利用者の個人情報が各サービスで閉鎖的に管理されるため，情報サービスの社会性が実現できない．

また，関連研究（２）については，個人情報をサービスサイドから分離しているため，個人情報を柔軟に共用できるようになり，情報サービスの社会性が確保されていると言える．しかし，携帯端末を持ち歩かなければならないため，携帯端末からの物理的な情報漏洩の防止や，複数端末間の同期等の運用に関する手間が山積し，利用者の負担になる煩雑さである．故に，全てのサービス利用者が利用できるとは言い難く，情報サービスの人間性を損ねていると考えられる．

以上から，人間性・社会性の両方を確保するためには，現在のサービスパーソナライズモデルにおいては，両者が互いにトレードオフの関係になっており，実現できないと言える．そこで，このトレードオフを解消し，人間性・社会性を考慮した情報サービスの構築を実現するための技術が必要であると言える．



(a) 関連研究（１）の問題点　　(b) 関連研究（２）の問題点

図 2.3: 関連研究の問題点

第3章　提案：開放型の情報サービスパーソナライズ手法

本章では，本研究における目的を達成するため，2 章で提起した関連研究の問題点を解決するための「開放型の情報サービスパーソナライズ手法」について述べる．

3.1　提案手法の概要

3.1.1　提案手法の概要と解決する技術課題

人間性・社会性を考慮した情報サービスの構築のためには，人間性・社会性を共に満たす情報サービスのパーソナライズが必要である．

そこで本研究では，開放型の情報サービスパーソナライズ手法を提案する．提案の概要は図 3.1 に示すとおりである．本提案手法は，サービス提供者・サービス利用者と物理的に独立させ，どのサービスからでもネットワーク的にアクセス可能な場所にサービス利用者の個人情報を置くことで，関連研究の問題点を解決する．

この手法を実現するために解決すべき技術課題を以下に示す．

1. 開放性（どのサービスからでもアクセス可能である性質）をもつ個人情報管理機構（本研究）
2. 個人情報を共用するための個人情報要求開示プロトコル（本研究）
3. 個人情報を最低限必要なだけ開示する制御機構
4. 通信内容を第三者から傍受されないセキュアな通信路

上述の 4 つの技術課題について，我々の研究グループでは，技術課題 3[26]，技術課題 4[27, 28] の課題についてそれぞれ研究し，課題の解決を行ってきた．そこで本研究では，未解決である研究課題１，研究課題２についてそれぞれ具体的に提案し，技術的課題の解決を目指す.

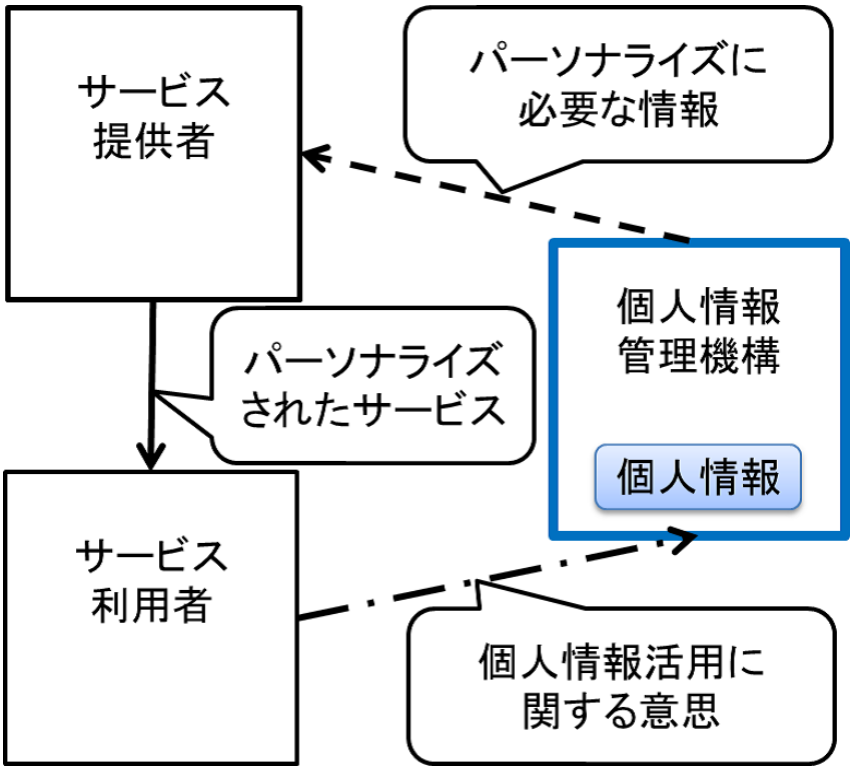


図 3.1: 提案：開放型の情報サービスパーソナライズ手法

3.1.2 提案手法の構成

開放型の情報サービスパーソナライズ手法の構成を図 3.2 に示す．開放型の情報サービスパーソナライズは，以下の二つから構成されている．

1. サービス利用者が所有する個人情報管理機構 U-PIMM(User-owned Personal Information Management Mechanism)

2. 個人情報要求開示プロトコル OSPP(Open Service Personalization Protocol)

サービス利用者は，自身が所有する個人情報管理機構 U-PIMM に個人情報を登録し，個人情報開示ポリシーを設定する事で，個人情報の活用に関する意思を反映させる．そして，個人情報要求開示プロトコル OSPP によって，個人情報の要求・開示や個人情報アクセスの正当性検査を行う．

次節より，提案手法の構成要素であるサービス利用者が所有する個人情報管理機構 U-PIMM と個人情報要求開示プロトコル OSPP についてその詳細を述べていく．

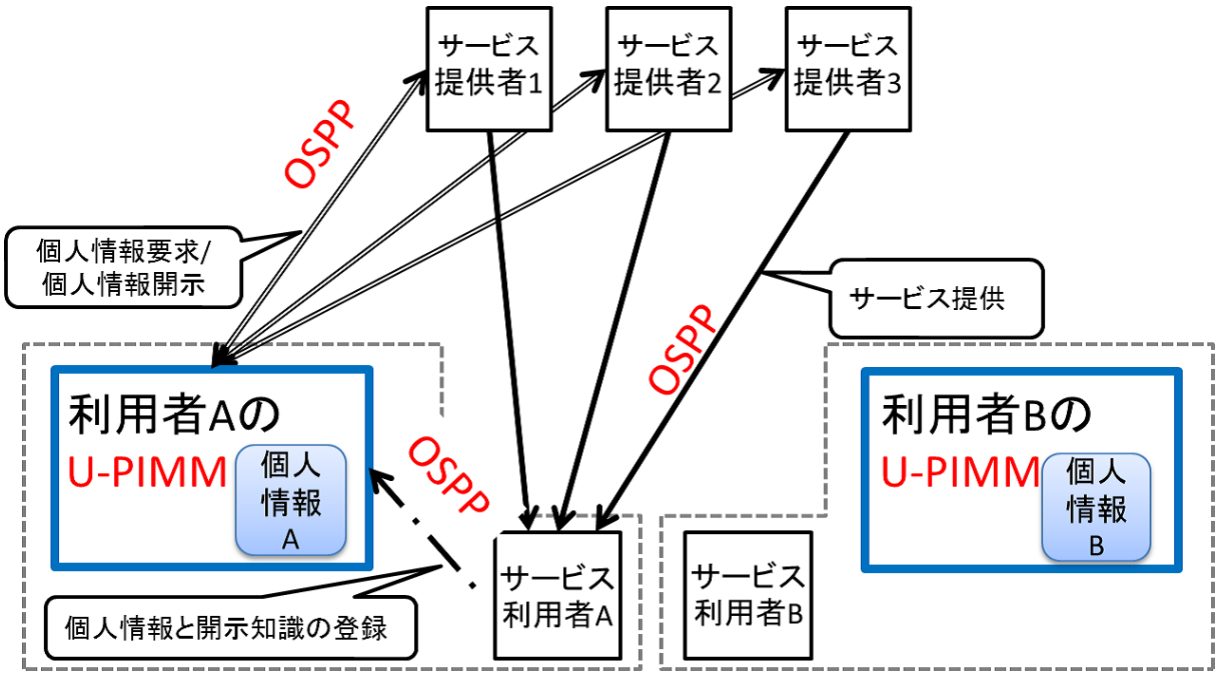


図 3.2: 開放型の情報サービスパードナライズ手法の構成

3.2　サービス利用者が所有する個人情報管理機構: U-PIMM

サービス利用者が所有する個人情報管理機構 U-PIMM(User-owned Personal Information Management Mechanism) について説明する．U-PIMM の概要を図 3.3 に示す.

U-PIMM は，サービス提供者・サービス利用者両者から独立した場所にある個人情報管理機構である．本機構は，様々なサービス提供者からの個人情報のアクセスを可能とし，個人情報の活用に関して開放性の確保を実現している．これによりサービス利用者の事前登録の煩雑さを解消し，複数サービス間での個人情報の共有を通してサービス間の間接的連携，それによる高度なパーソナライズを可能にする.

U-PIMM の構成要素を以下に述べる.

個人情報

本機構の所有者であるサービス利用者の個人情報．利用者が予め利用したい個人情報を登録する．個人情報は大きく分けて以下の二つがある.

(1) 静的個人情報 中期的，長期的に変更されない静的な利用者に関する情報

(2) 動的個人情報 短期間で動的に変化・更新される利用者に関する情報

上述の 2 種類の個人情報について，サービス提供者から扱う.

個人情報開示知識

本機構に登録されている個人情報の開示に関するポリシーの知識記述．各々のポリシーは，そのポリシーで扱う個人情報の種類を定め，サービスのタイプと個人情報を使う目的の 2 点について，扱う個人情報を開示するか否かを定義する.

個人情報フィルタ

サービス提供者からの個人情報要求と個人情報開示知識を照合し，開示する個人情報をフィルタリングする機構.

個人情報アクセス検証機構

サービス提供者から個人情報要求があった際に，個人情報アクセス確認用トークン

を発行する．サービス利用後にサービス提供者から発行されるサービスレシートを用いて，アクセスの正当性を検証する．

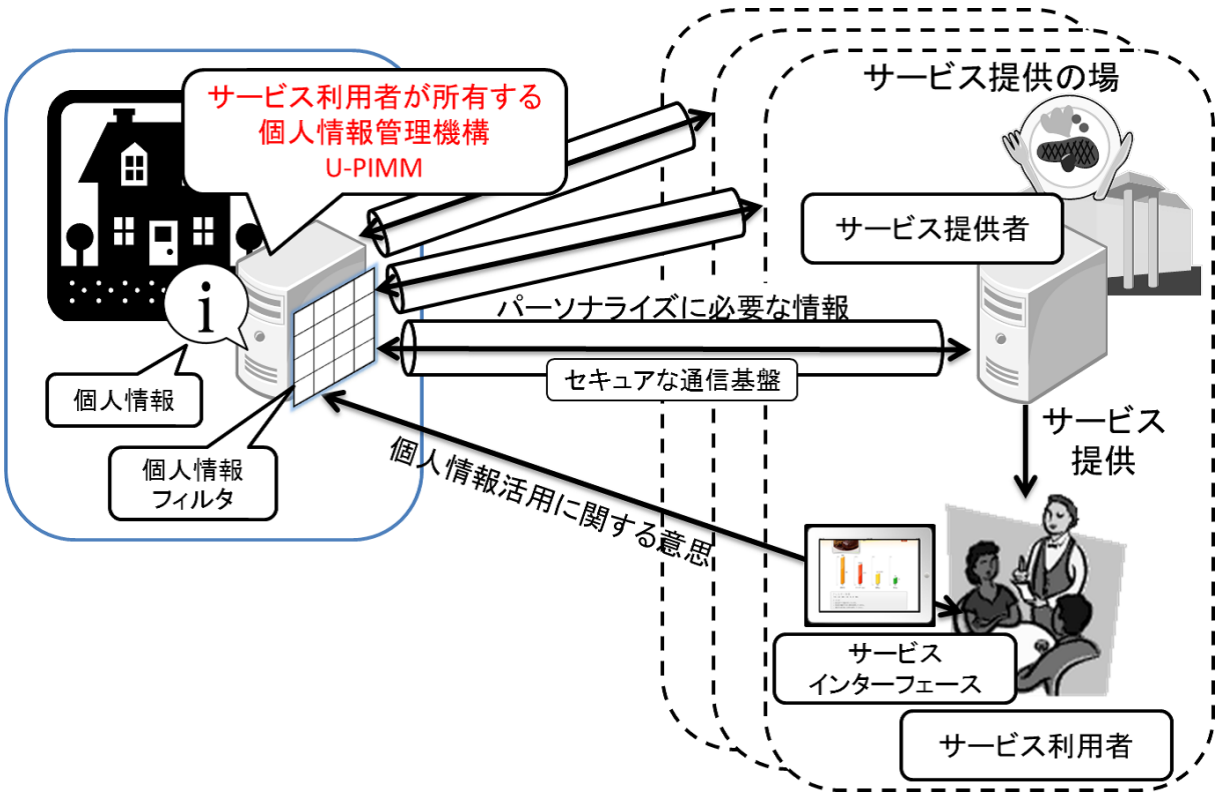


図 3.3: User-owned Personal Information Management Mechanism(U-PIMM) の概要

3.3　個人情報要求開示プロトコル: OSPP

個人情報要求開示プロトコル OSPP(Open Service Personalization Protocol) について述べる.

本プロトコルは，前節の利用者が所有する個人情報管理機構 U-PIMM を導入したサービスパーソナライズモデルにおいて，個人情報の要求開示，またそれを通した異なるサービス間の個人情報の共有を実現する.

提案プロトコルの概要を図 3.4 に示す.

また，提案プロトコルの概要を以下のように示す.

①サービス要求

サービス利用者は，サービス利用者識別子（ユーザ ID）をパスワードと共に提示し，サービスにログインする.

②個人情報要求

サービス提供者は，ユーザ ID を元にサービス利用者の U-PIMM を検索する．その後に，サービス提供者と U-PIMM 間で公開鍵の交換を行い，セキュアな通信路を確保した上で，情報サービスのパーソナライズに必要な個人情報を要求する.

③開示個人情報フィルタリング

サービス提供者から個人情報の要求を受けた U-PIMM は，個人情報開示知識と個人情報要求を比較し，開示する個人情報を決定する.

④個人情報利用確認文字列生成

U-PIMM は個人情報の利用に関する事後確認のためにランダム文字列を生成する.

⑤個人情報アクセスログの作成

U-PIMM は個人情報アクセスに関するログを生成する．ログには以下の項目を記述する.

- アクセス日時

- アクセスしてきたサービス名
- アクセスしてきたサービスの IP アドレス
- 返答内容

⑥個人情報開示

フィルタリングされた開示して良い最低限の個人情報を開示する．また，生成したランダム文字列も開示する情報に添付する．

⑦サービス構築

U-PIMM より開示された個人情報を用いて，サービス利用者にパーソナライズされた情報サービスを構築する．尚，何も開示されない場合は，通常時のパーソナライズされていない情報サービスを生成することとする．

⑧サービス提供

サービスインターフェースを介して，情報サービスをサービス利用者に提供する．

⑨サービス利用レシートの発行

U-PIMM からサービス利用者の個人情報の開示を受けた際に，一緒に受け取ったランダム文字列を用いてレシートを発行する．発行手順を以下に示す．

1. サービス提供者が提供したサービス内容等，いわゆるサービス内容の記述を生成する（ノーマルレシート部）．
2. サービス名，U-PIMM からの開示メッセージと U-PIMM から添付されたランダム文字列の組みをサービス提供サーバの秘密鍵を用いて暗号化する（個人情報アクセス確認コード）．
3. ノーマルレシートと個人情報アクセス確認コードを合わせて，レシートとしサービス利用者に渡す．

⑩サービス利用ログのフィードバック

サービス提供者はサービス利用者の U-PIMM にサービス利用ログをフィードバック

する．U-PIMM 側では動的個人情報として，この利用ログを保存し異なるサービスにおけるパーソナライズにおいても利用可能にする．

⑪個人情報アクセスの正当性検証

サービス利用後に，サービス利用者は自らの U-PIMM とレシートを用いて，サービスを提供するコンテクストにおいてのみ個人情報にアクセスしたことを検証する．

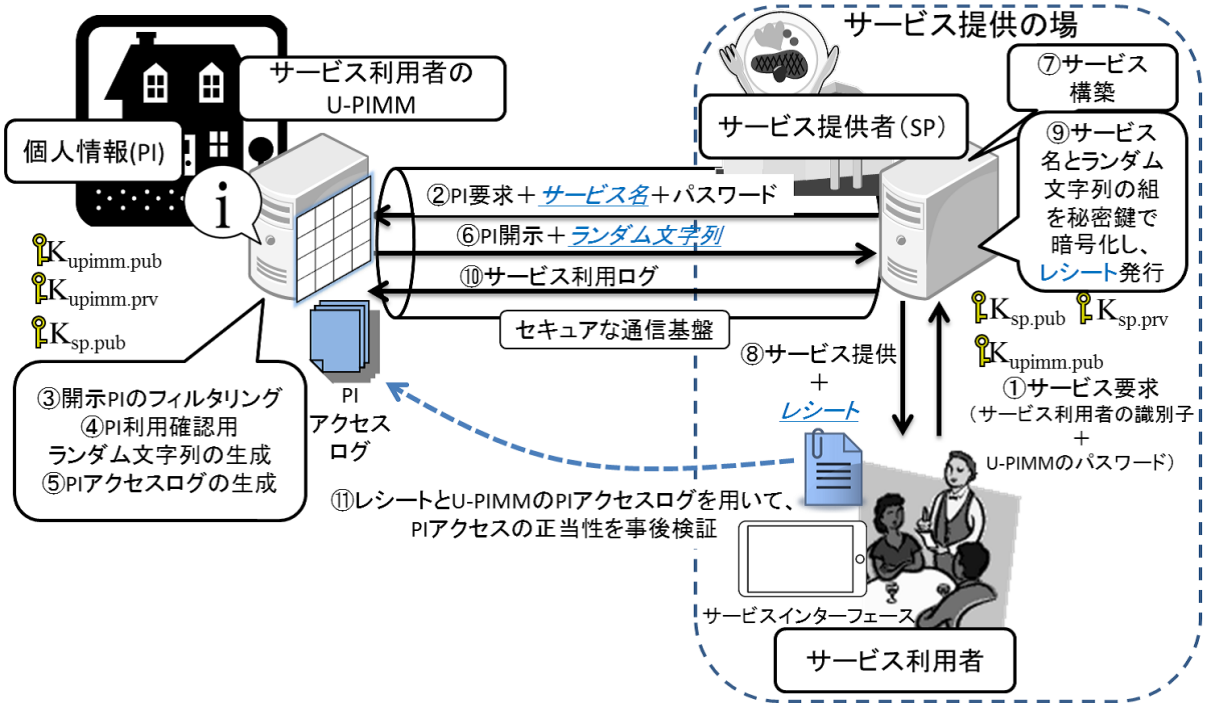


図 3.4: Open Service Personalization Protocol(OSPP) の概要

表 3.1: 変数定義

変数	定義
USER	サービス利用者実体
U-PIMM	サービス利用者の U-PIMM 実体
SERVICE	サービス提供サーバ実体
USER.ID	サービス利用者の識別子
SERVICE.ID	サービス提供者の識別子
SERVICE.public_key	サービス提供サーバの公開鍵
SERVICE.private_key	サービス提供サーバの秘密鍵
U-PIMM.public_key	U-PIMM の公開鍵

次に，詳細な OSPP におけるメッセージングについて述べていく．まず，変数定義を表 3.1 に示す．また，図 3.5 に提案プロトコルの流れを示す.

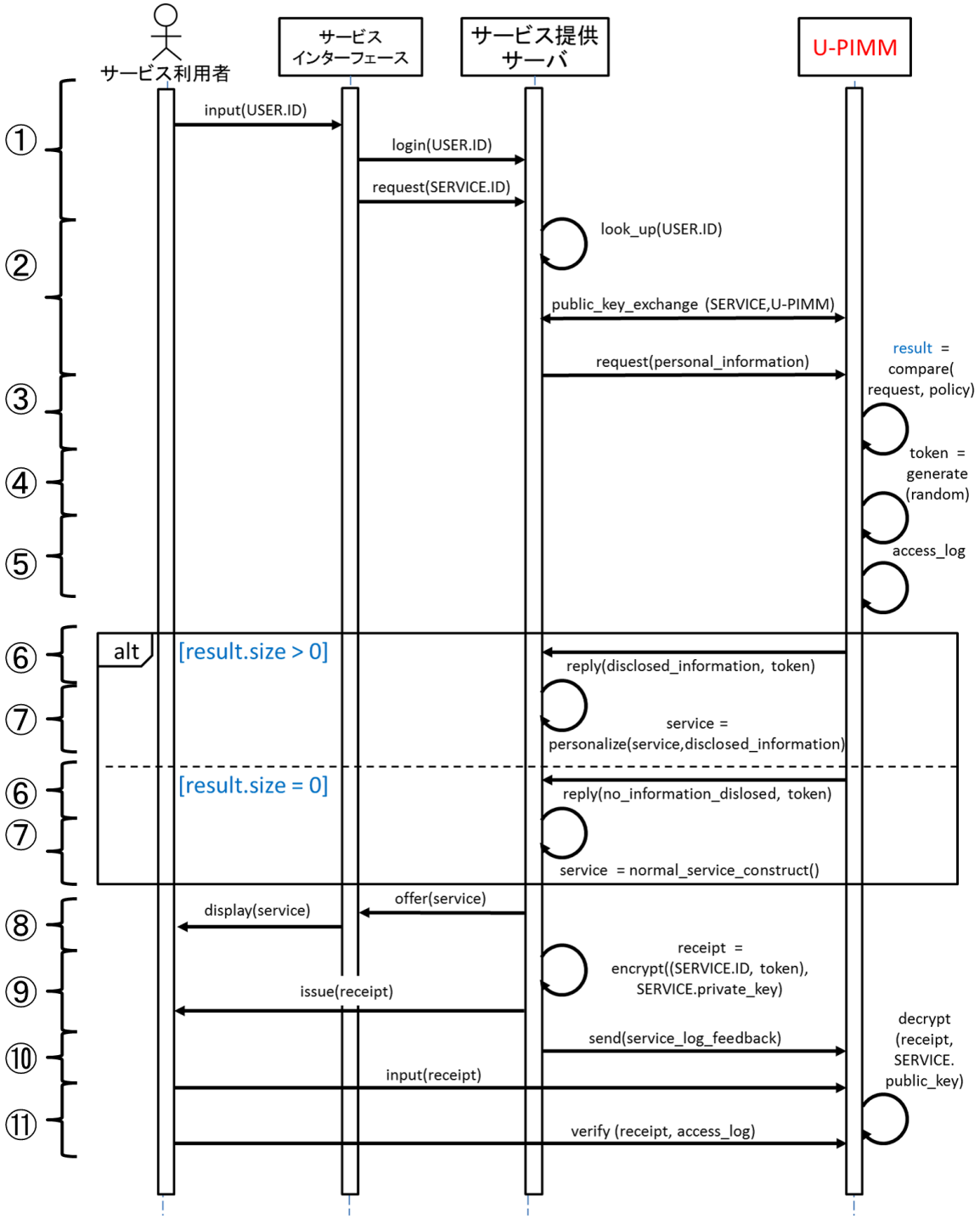


図 3.5: 提案プロトコルの流れ図

メッセージや処理の詳細を以下に述べる．尚，サービス利用者（User: U），サービスインターフェース（Service Interface: SIF），サービス提供サーバ（Service Provider Server: SPS），U-PIMM（U-PIMM）をそれぞれ略記号として用いる．

(1) input(USER.ID) (U→SIF)

サービス利用者 USER の識別子 USER.ID を入力する．

(2) login(USER.ID) (SIF→SPS)

USER.ID を送り，ログインする（任意でパスワードを用いる）．

(3) request(SERVICE.ID) (SPS→U-PIMM)

サービス提供サーバ SERVICE へサービスリクエストを送る．

(4) look_up(USER.ID) (SPS)

USER の U-PIMM の IP アドレスを任意の方法で検索する．

(5) public_key_exchange(SERVICE, U-PIMM) (SPS⇌U-PIMM)

サービス提供サーバ SERVICE と U-PIMM で任意の方法で公開鍵を交換する．

(6) request(personal_information) (SPS→U-PIMM)

U-PIMM にサービスに必要な個人情報を要求する．

(7) result = compare(request, policy) (U-PIMM)

個人情報要求メッセージ request と個人情報開示知識 policy を比較し，開示する知識を決定する．結果は result に格納する．

(8) token = generate(random) (U-PIMM)

個人情報利用確認文字列 token をランダムに生成する．

(9) access_log (U-PIMM)

アクセスログを生成する．

(10) ALTERNATIVE: check $result.size$

result の大きさ，即ち開示する個人情報があるか否かを判定する．

(10-A) $result.size > 0$ **: More than 1 element of personal information is disclosed.**

1. reply(disclosed_information, token) (U-PIMM→SPS)
   開示する個人情報 disclosed_information と個人情報利用確認文字列 token を返答する．
2. service = personalize(service, disclosed_information) (SPS)
   開示された個人情報 disclosed_information を用いてサービスをパーソナライズする．パーソナライズされたサービス内容を service に格納する．

(10-B) $result.size = 0$ **: No personal information is disclosed.**

1. reply(no_information_disclosed, token) (U-PIMM→SPS)
   個人情報は開示されない．個人情報利用確認文字列 token のみを返答する．
2. service = normal_service_construct() (SPS)
   平常時のサービス内容を構築する．サービス内容を service に格納する．

(11) offer(service) (SPS→SIF)

サービス内容 service をサービスインターフェス SIF に返す．

(12) display(service) (SIF→U)

サービス内容をサービス利用者 U に提示する．

(13) receipt = encrypt((SERVICE.ID, token), SERVICE.private_key) (SPS)

SERVICE.ID と token をサービス提供サーバの秘密鍵 SERVICE.private_key で暗号化し，レシート receipt を生成する．

(14) issue(receipt) (SPS→U)

レシート receipt をサービス利用者 U に発行する．

(15) send(service_log_feedback) (SPS→U-PIMM)

サービスの利用ログ service_log_feedback を U-PIMM にフィードバックする.

(16) input(receipt) (U→U-PIMM)

レシート receipt を U-PIMM に入力する.

(17) decrypt(receipt, SERVICE. public_key) (U-PIMM)

レシート receipt をサービス提供サーバ SERVICE の公開鍵 SERVICE. public_key で復号する.

(18) verify (receipt, access_log) (U→U-PIMM)

レシート receipt とアクセスログ access_log を比較し個人情報のアクセスを検証する.

個人情報のアクセスの正当性検証アルゴリズム

個人情報のアクセスの正当性検証アルゴリズムは図 3.6 に示す通りである．検証アルゴリズムは以下のような手順を踏む.

入力: R（レシート），AL（アクセスログ）

出力: UA（不正アクセスのリスト）

1. UA に AL を代入する.
2. R の復号を試行する.
   2.1. 復号が成功した場合は，このまま処理を続行する.
   2.2. 復号が失敗した場合は，サービス提供者が不正なレシートを渡した事が判明する．処理は終了する.
3. インデックス変数 i を 1 に初期化する.
4. （※）ある R のアクセス検証コード v_i について，AL のログの中に一致するログ l が存在するか調べる
   4.1. l が存在する場合は，UA から l を取り除く.
   4.2. l が存在しない場合は，UA に v_i を加える.
5. i に i+1 を代入する.
6. i>n の真偽をチェックする
   6.1. 真なら UA を出力して終了.
   6.2. 偽なら※に戻る.

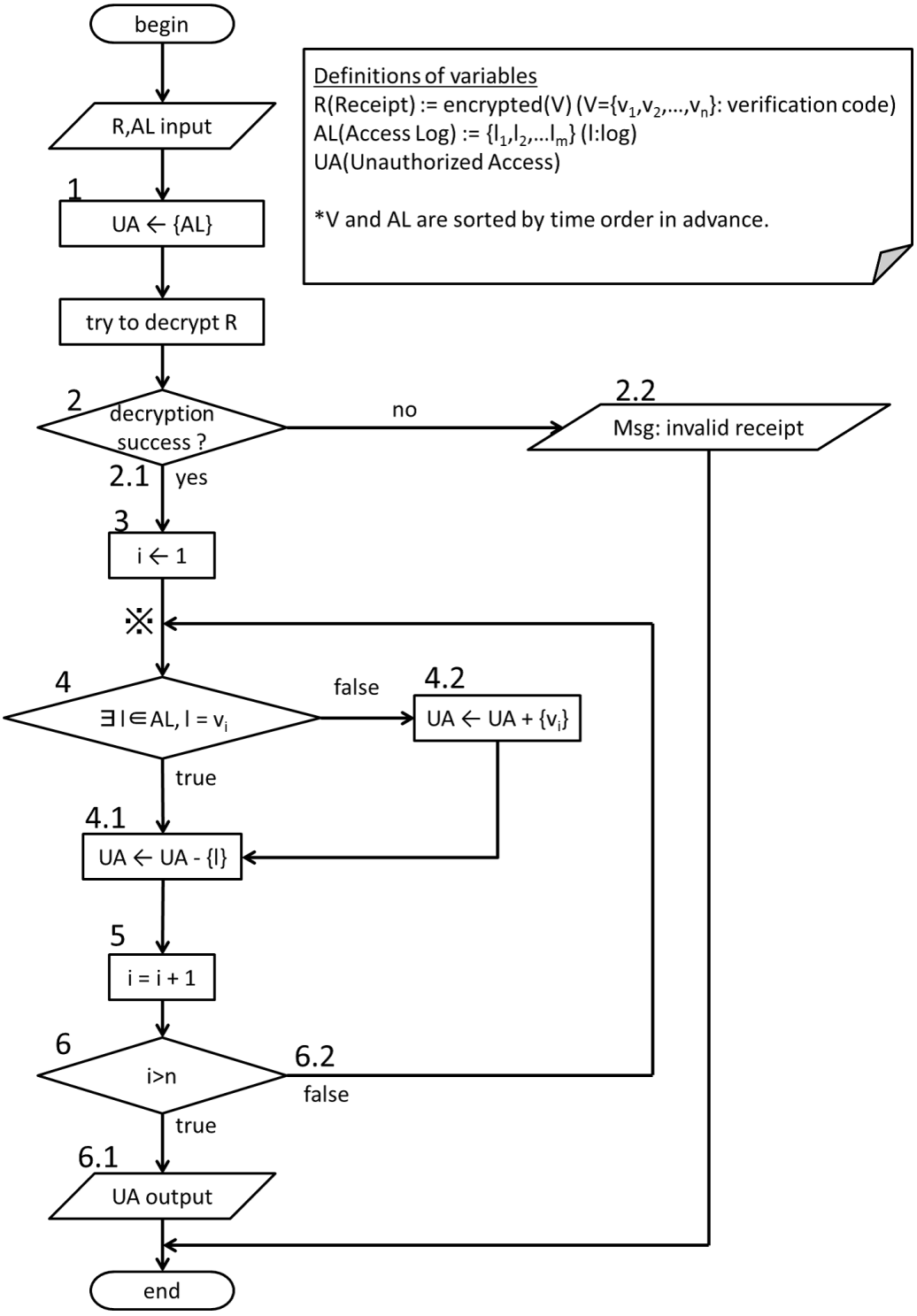


図 3.6: 個人情報のアクセスの正当性検証アルゴリズム

3.4　本提案の適用範囲

本節では，本提案の適応範囲について述べる．人間性・社会性を考慮し，情報サービスを構築するために，本手法では個人情報を利活用し，情報サービスのパーソナライズを行う．その際に，個人情報の適切な取り扱いという観点からサービス利用者とサービス提供者の間で何らかの信頼の根拠が必要となる．

本提案の適応範囲としては,「サービス利用者がサービス提供者と face-to-face の状態で利用する情報サービス」であるとする．これは，サービス利用者が情報サービスを利用しているというコンテクストにおいてのみサービス提供者が U-PIMM の個人情報を参照している事を OSPP によって検証できるためである．

この検証できるという事実は，サービス利用者にとって利用したサービスが正当に自分自身の個人情報を参照されたことを確認できるという安心感を与える事ができる．即ち，サービス提供者がサービス利用者の個人情報を不正利用することに対する抑止力にもなると言える．

第4章　プロトタイプシステムの設計と実装

本章では，提案手法に基づいた情報サービスのプロトタイプシステムについて，その設計と実装を述べる．

4.1　プロトタイプシステムの設計と実装

本節では，提案手法の構成要素やそれを用いたサービスのプロトタイプについて，それぞれの詳細設計を述べる．

4.1.1　U-PIMM

サービス利用者が所有する個人情報管理機構 U-PIMM の設計について述べる．図 4.1 に U-PIMM の設計概要を示す．U-PIMM サーバは，サービス利用者，または一世帯につき一つのホームサーバを想定し，常時，ネットワークを通じてアクセス可能な端末とする．また，サービス利用者一人につき，その個人情報の管理を担当する U-PIMM サーバは必ず一台とし，重複は許さないものとする．U-PIMM は起動時に担当するサービス利用者と自身の紐付けを行う．具体的には，サービス提供者・利用者が共にアクセス可能な分散ハッシュテーブル [29, 30] を用い，以下の key,value を put する．

$$(key, value) = (\text{ユーザ } ID, U-PIMM \text{ の } IP \text{ アドレス})$$

U-PIMM は，以下の構成要素からなる．

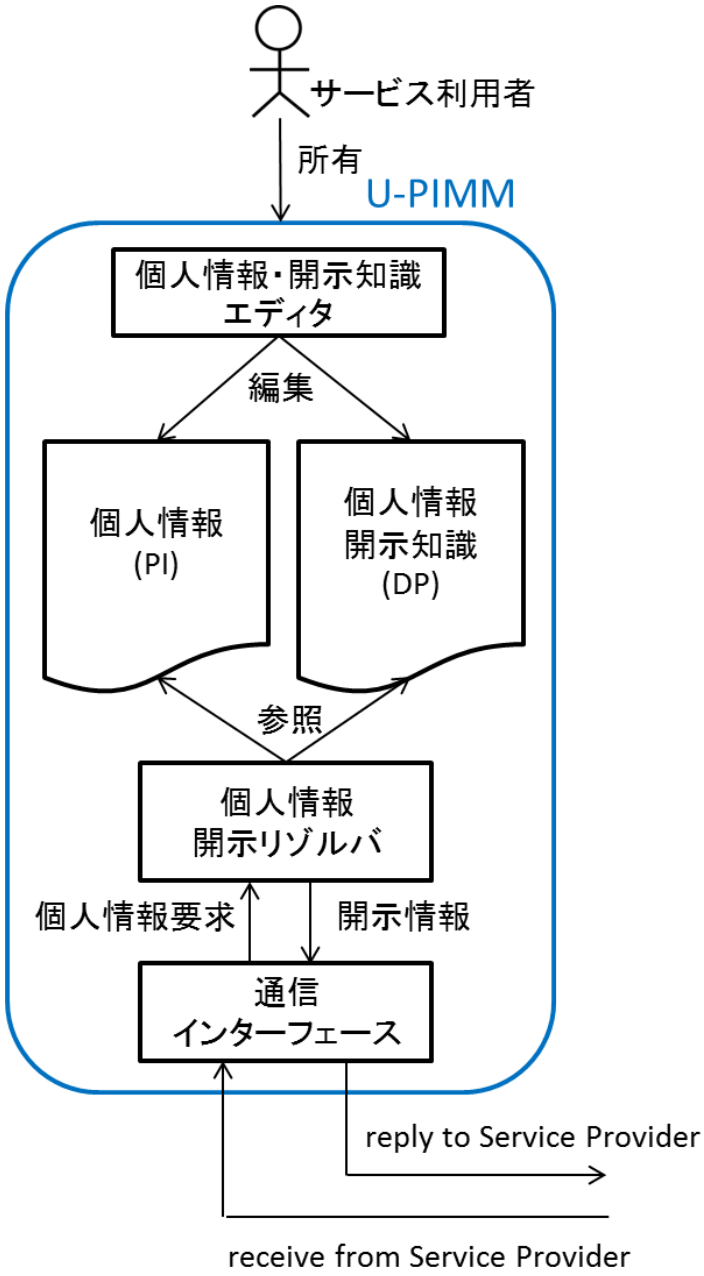


図 4.1: U-PIMM の設計概要

個人情報・開示知識エディタ

個人情報・開示知識エディタは，サービス利用者が個人情報とその開示知識を編集するためのエディタである．プロトタイプシステムにおいては Web ベースのインターフェースを備えており，これを通してサービス利用者は利活用する個人情報や開示知識の操作を行う．個人情報・開示知識エディタのインターフェースを図 4.2 から図 4.6 に示す．エディタは以下の項目のタブからなる．

1. 一般タブ
2. アレルギータブ
3. 健康タブ
4. ポリシータブ
5. 履歴タブ

一般，アレルギー，健康に関する個人情報の編集とポリシー設定による開示知識の編集，サービス利用ログの管理がそれぞれのタブ上でできるようになっている．以下に，個々のタブについて詳細を述べる．

図 4.2: 個人情報・開示知識エディタ:一般

一般タブで扱う個人情報は，本名，ニックネーム，年齢，宗教である．各項目について適応するポリシーを選択可能である．

図 4.3: 個人情報・開示知識エディタ:アレルギー

アレルギータブでは，利用者がアレルギーを持つ食品を設定することが可能である．取り扱う品目は消費者庁がアレルギー表示の義務づけ・推奨を行っている以下の 25 品目である [31].

アレルギー品目

（表示義務づけ）

えび，かに，小麦，そば，卵，乳，落花生

（表示推奨）

あわび，いか，いくら，オレンジ，キウイフルーツ，牛肉，くるみ，さけ，さば，大豆，鶏肉，バナナ，豚肉，まつたけ，もも，やまいも，りんご，ゼラチン

図 4.4: 個人情報・開示知識エディタ:健康

健康タブでは，食品摂取の際のエネルギー (kcal)，塩分 (g)，脂質 (g) の 3 項目について目標摂取栄養素を設定できる．また，オプションとして性別，年齢，身長，運動強度，高血圧の有無から算出することも可能である．また，食事に関する予算設定もこのタブで行える．

図 4.5: 個人情報・開示知識エディタ:ポリシー

ポリシータブでは，個人情報の開示に関するポリシーを設定できる．ポリシーは，サービスタイプ・利用目的によってポリシーを作成でき，これらのポリシーを各々の個人情報に対して適用する．

図 4.6: 個人情報・開示知識エディタ:履歴

履歴タブでは，サービス利用者が摂取した食べ物，服用した薬，サービス利用履歴といった情報を管理できる．各履歴は日にち毎のタブでも管理されており，時系列毎にアクセス可能である．

利用者の個人情報，個人情報開示知識，個人情報開示リゾルバ

利用者の個人情報，個人情報開示知識，個人情報開示リゾルバからなる個人情報フィルタリング機能に関わる部分は，Osawa らの手法 [26] に基づき設計を行った．

利用者の個人情報

利用者の個人情報は静的個人情報・動的個人情報の 2 種類を扱う．それぞれ具体的に以下の個人情報について今回の実装では扱った．

1. 静的個人情報：氏名，ニックネーム，年齢，宗教，アレルギー，目標摂取栄養素（エネルギー，塩分，脂質）
2. 動的個人情報：サービス利用履歴，食事の履歴，薬品の服用履歴

個人情報開示知識

利用者の個人情報開示に関するポリシーを記述したもの．サービスと目的について，どの個人情報を開示するか定義する．個人情報の各項目は，この開示知識を適用する形でその開示制御を行う．

表現形式

個人情報，及びその開示知識は AllegroGraph[32] という RDF データベースを用いて実装した．個人情報・開示知識の記述例を図 4.7 に示す．RDF はリソースの関係を主語 (Subject), 述語 (Predicate)，目的語 (Object) の 3 つの要素で表現する [33]．これはトリプルというデータモデルであり，個人情報，開示知識それぞれにおいては，次のようなトリプルで定義する．

個人情報

< subject, predicate, object > = < サービス利用者, 述語, 対象 >

開示知識

< subject, predicate, object > = < ポリシー名, サービスタイプ, サービスインスタンス >

< subject, predicate, object > = < ポリシー名, ポリシー適用, 適用する個人情報の項目 >

図 4.7: 個人情報・開示知識記述例

個人情報開示リゾルバ

サービス提供者からの個人情報開示要求と個人情報開示知識を照合し，開示する情報を決める．開示する情報は Prolog を用いて導出する．導出関数は以下に示す通りである．

開示情報導出関数

```
(<– (disclose ?user ?type ?purpose ?object)
   (q- ?user !p:has_policy ?policy)
   (q- ?policy !p:disclose_type ?type)
   (q- ?type !rdfs:subClassOf !p:service_type)
   (q- ?policy !p:disclose_purpose ?purpose)
   (q- ?purpose !rdfs:subClassOf !p:PIusage_purpose)
   (q- ?policy !p:apply_policy ?object))
```

今回のプロトタイプシステムにおいて，個人情報開示リゾルバが扱うルールの数，またファクトの数，即ち RDF データベースにストアされているトリプルの数をそれぞれ表 4.1 に示す.

表 4.1: ルールの数とファクトの数

項目	数
ルールの数（個）	5
ファクトの数 （個）	785

通信インターフェース

サービス提供サーバとの通信を行うインターフェースである．Java 言語を用いて実装した．SSL ソケットによってサービス提供サーバからのコネクションを待ち受け，マルチスレッドで各メッセージに対する処理を行う．

U-PIMM に対するログインに関しては，パスワード認証を用いている．パスワードについては，アルファベット大文字小文字と数字の混合したものとする．桁数については，1024 桁とした．

4.1.2 OSPP

OSPP に関しては，XML によるメッセージ記述をしている．XML メッセージのスキーマ（DTD）を付録 A に示す.

ログインについては

通信路については，分散型の公開鍵交換手法である HDAM[27, 28] を用いて，公開鍵の交換を行うことで， 暗号化通信を実現している．HDAM は，既に公開鍵を交換済みな信頼できるホストのみを辿り，公開鍵を交換する．以上により，第三者による通信の傍受を防止する.

また，OSPP 中のレシートについて，図 4.8 にその一例を示す．点線上部は通常のレシート同様にサービスの内容が記述されており，点線下部の「Personal Information Utilization Log.」からは，個人情報の利用に関するログを記述している．各項目の内容について以下に示す.

SERVICE NAME

サービス利用者の U-PIMM アクセス時に用いたサービス名

U-PIMM_ACCESS_TIME

U-PIMM にアクセスした時刻を表すタイムスタンプ

ISSUED RANDOM TOKEN

U-PIMM から発行された 10 桁のランダム文字列

VERIFICATION CODE

サービス名とランダム文字列を RSA 暗号化した 256 桁の検証コード

REPLIED_XML

U-PIMM からサービス提供者に開示された XML メッセージ

********** Aoba Drug **********
[SHOPPING LIST]
Cold Medicine A ￥924

Thank you for using our service. Have a nice day!

Personal Information Utilization Log.
[SERVICE NAME] Aoba Drug

[U-PIMM_ACCESS_TIME] 20111229194522620

[ISSUED RANDOM TOKEN] 4MYkU7SVXj

[VERIFICATION CODE]
6f4118b2aacb94336e5b82baff817385fc4f9a72
3d71ba60e1d054207ff96b39757f5b8a1ac1ec24
f3b1792f750d2c97c2fc49ecb133602e5c4e6d01
e290a84ffe284a2383d38c30bf860e6baa4ce8b9
718ede8fccfaef1a06f8fb3d7786fbfdb60de451
6a5b4a9ff64dfb0eb9b00a98393254b209147425
2f0e575fac8e2192

[REPLIED_XML]
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pi_request SYSTEM "pi_reply.dtd" >
<pi_reply>
<pi_owner>
<dai_id>user1</dai_id>
</pi_owner>
<requestor>
<dai_id>drug_store_aoba</dai_id>
</requestor>
<service_type type="pharmacy"/>
<usage_purpose purpose="recommend"/>
<pi_update_timestamp>20111215140756</pi_update_timestamp>
<pi>
<any_data type="age">40</any_data>
<any_data type="pseudonym">マコト</any_data>
</pi>
</pi_reply>

図 4.8: レシートの例

4.1.3　サービス事例

提案手法を適応したサービス事例として，以下の 2 つのサービスをプロトタイプとして設計・実装した．

1. 薬局サービス

2. レストランサービス

それぞれの事例について詳細を以下に述べていく．

1. 薬局サービス

薬局における医薬品購入補助システムを実装した．そのインターフェースを図 4.9 に示す．医薬品を購入する際に，既往歴や飲み合わせ，体質，疾患の内容等を考慮した適切なものを選択する事は時に煩雑である．そのため，サービス利用者それぞれにあったパーソナライズが施された医薬品購入補助システムの需要は高い．しかしながら，自分にあった医薬品を選ぶために公にセンシティブである自らの健康に関する情報を店先で提示することに抵抗を覚えるサービス利用者も多いと考えられる．本システムでは，提案手法を導入する事で，自らに関する個人情報について店先で口に出さずともパーソナライズされた医薬品のリストが提示される．

提示される医薬品リストは，図 4.9(a) に示されるような各々の医薬品について，購入についてアドバイスが必要な物にアドバイスをつけた一覧を提供する．また，各医薬品の写真をタッチすると，図 4.9(b) に示されるような各医薬品についての詳細な記述を表示する．この詳細表示には，飲み合わせ，年齢制限，その他注意事項も記述されており，サービス利用者が医薬品を購入する際のガイドラインとなる．

(a) アドバイス付き医薬品購入リスト

(b) 医薬品の詳細表示

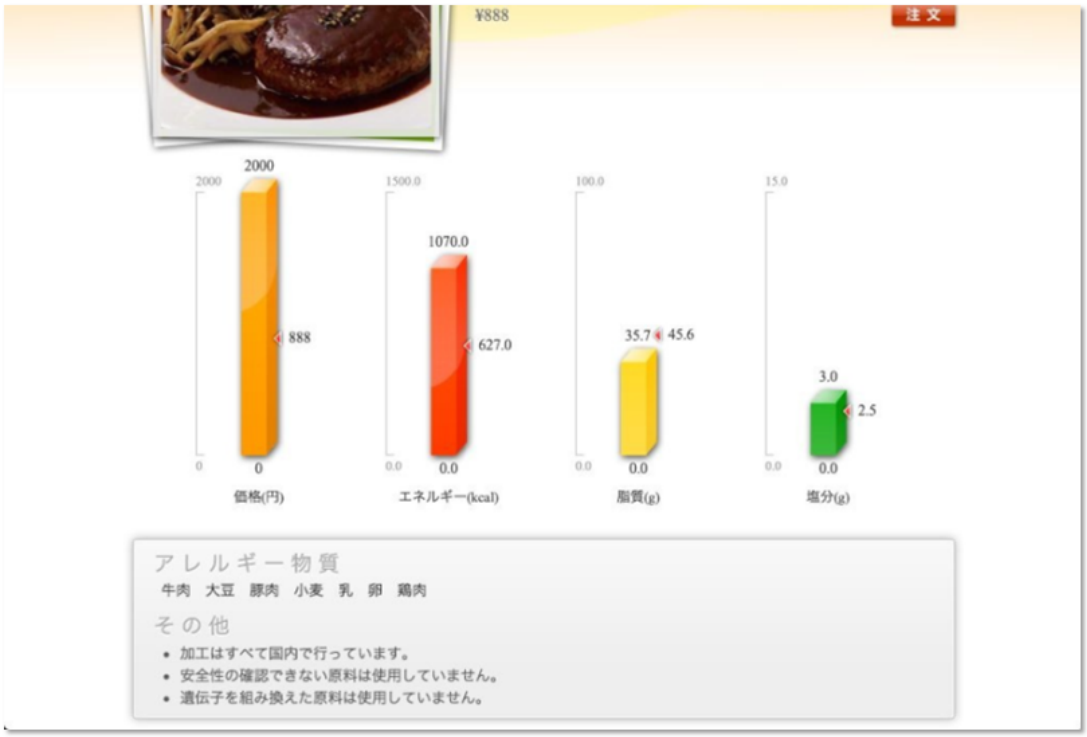
図 4.9: 薬局内での医薬品購入システムのサービスインターフェース

2. レストランサービス

レストランにおけるメニュー推薦システムを実装した．そのインターフェースを図 4.10 に示す．レストラン等で食事をする際に，気をつける事は多岐にわたっている．自分のアレルギーや疾患に合わせた食べ物を注意して注文する，宗教上食べる事ができない物を避けて注文する等の他に，また，自分で意識しなくとも，自らが服用している医薬品との相性を考慮した食事をしたい等の要求も高い．こうした要求を考慮し，メニュー表を提示するためにメニュー表を予めパーソナライズし，サービス利用者にとって注文しやすいメニュー表を提示する事が有効である．しかしながら，こうしたメニュー表の提示のために，レストランのテーブルなどでセンシティブな情報を含む個人情報を口頭で伝えることを良しとしない利用者も多いと考えられる．本システムでは，提案手法を導入する事で，自らに関する個人情報について店先で口に出さずともパーソナライズされたメニュー表が提示される．

提示される電子メニュー表は，図 4.10(a) に示されるような各々のメニューについて，注意事項や推薦事項がある物にアドバイスをつけた一覧を提供する．また，各メニューの写真をタッチすると，図 4.10(b) に示されるような各メニューについての詳細な記述を表示する．この詳細表示には，栄養素に関する記述や金額，含まれるアレルギー食品のリスト，その他注意事項も記述されており，サービス利用者がメニューを注文する際の手助けになる．

(a) アドバイス付きメニュー表



(b) メニューの詳細表示

図 4.10: レストラン内でのメニュー推薦システムのサービスインターフェース

4.2　プロトタイプシステムの構成

図 4.11 に本プロトタイプシステムの構成を示す．プロトタイプシステムは，U-PIMM サーバ，レストランサーバ，薬局サーバの 3 つのホストで構成されており，マシン構成は以下のようになっている．

U-PIMM サーバ

CPU: Intel Core i5 2.67GHz

RAM: 4GB

OS: Windows 7

Software: Allegro Prolog, Allegro Graph(RDF Database)

レストランサーバ

CPU: Intel Core2Duo 2.53GHz

RAM: 4GB

OS: Windows 7

Software: Tomcat 5, JRE 6, MySQL 5

薬局サーバ

CPU: Intel Core i5 2.67GHz

RAM: 4GB

OS: Windows 7

Software: Tomcat 5, JRE 6, MySQL 5

また，サービスの端末が利用する無線 LAN のアクセスポイントが用意されており，これらのホストと無線 LAN のアクセスポイントは同じネットワークにあるものとする．

2 つのサービスサーバには，利用者がサービス利用時にカードログインするための RFID カードリーダ [34] が取り付けられており，サービス利用者はカードリーダにカードをかざす事でログインをする．

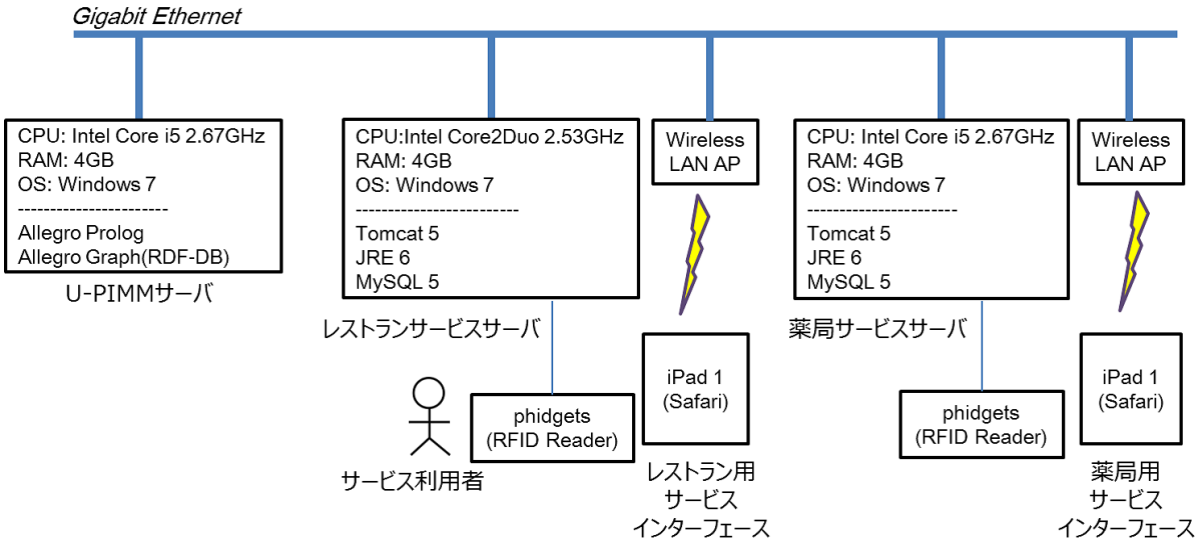


図 4.11: プロトタイプシステムの構成

第5章　実験と評価

本章では，プロトタイプシステムを用いた実験を行い，提案手法の有効性を評価する．まず，プロトタイプシステムを用いて行った実験について，シナリオ等を整理する．次に，各々のシナリオについて提案手法が評価項目を満たしているか確認し，最後に，これらの結果から考察を行う．

5.1　実験概要

本節では，提案手法の有効性を示すための実験について，その概要を述べる．

5.1.1　実験目的

本実験の目的は人間性・社会性を考慮した情報サービスの構築ができるかを確認することである．具体的には，本提案のプロトタイプシステムを用いて，人間性・社会性を考慮して情報サービスを構築できるか検証する．

5.1.2　各実験の内容

先述の目的のために，以下の 2 つの実験を行った．その内容とそれぞれのシナリオについて，以下に示す．

実験１

特別な端末を携行しなくともパーソナライズされたサービスを利用できる事を示す

シナリオ (a)：レストランサービス

サービス内容: メニュー推薦

サラリーマンの男性（40 歳）とその息子（7 歳）がレストランで食事をとる（以下，それぞれ「お父さん」,「男の子」と呼ぶ）．お父さんは，主治医から高血圧のため塩分や脂質の多い料理の摂取を制限されている．また男の子は，卵アレルギーを持っており．レストランのメニュー推薦システムにより，電子メニュー表から推薦されたメニューを注文する．

シナリオ (b)：薬局サービス

サービス内容: 医薬品購入補助

幼稚園児の女の子（4 歳）が薬局に行って，風邪薬を買う．薬局で販売されている風邪薬には服用に関して年齢制限があるものがある．そこで，女の子の医薬品を購入する際に医薬品購入補助システムを用いてどの薬を買うべきかのアドバイスをもらう．

実験２

U-PIMM を介した異なるサービス間の間接的連携ができることを示す．

シナリオ：二つのサービスにおいて個人情報を共用する事例

仕事帰りの女性（35 歳）が薬局にいった後にレストランを利用する．女性は最近風邪気味なので，まず薬局で風邪薬を購入する．薬局で購入した薬は，アルコールとの飲み合わせが悪いため，以降の食事に気をつけなければならない．風邪薬を購入後に，レストランに行って食事をとる．この際，レストランのテーブルにあるタッチパネル式の電子メニュー表からメニューを注文する．

5.1.3 評価項目

評価項目は以下の 3 つとし，第 2 章で述べた関連研究との定性評価を行う．

複数サービスでの個人情報の共用

異なるサービス間においてサービス利用者の個人情報を共用する事ができるか

サービス提供者への個人情報事前登録の有無

サービス利用者が情報サービスのパーソナライズを受ける際に，個人情報を事前に登録しておく必要があるか

サービスを利用する上で携行する必要があるもの

パーソナライズされた情報サービスを利用する際に，携行しなければならないならない物

5.2　実験１

5.2.1　実験目的

特別な端末を携行しなくともパーソナライズされたサービスを利用できる事を示す.

5.2.2　実験条件

実験１の実験条件をそれぞれ以下に示す.

実験１（a）

- お父さんと男の子がレストランで食事をとる.
- お父さんは，主治医から高血圧のため塩分や脂質の多い料理の摂取を制限されている.
- 男の子は，卵アレルギーを持っている.

実験１（b）

- 女の子（4 歳）が薬局に行って，風邪薬を買う.
- 風邪薬には年齢制限がかかっているものがある.

5.2.3　実験手順

実験１の実験手順をそれぞれ以下に示す.

実験１（a）

1. 特別な端末を使わず，カードのみを所持し，レストランサービスのカードリーダにカードを通す.
2. レストランサービスの電子メニュー表から推薦されたメニューを選択する.

3. 利用者の特徴を考慮しパーソナライズされたメニューが表示されることを確認する.

実験１（b）

1. 特別な端末を使わず，カードのみを所持し，薬局サービスのカードリーダにカードを通す.
2. 薬局の電子薬品リストから推薦された医薬品を選択する.
3. 利用者の特徴を考慮しパーソナライズされた医薬品リストが表示されることを確認する.

5.2.4　実験結果

始めに，実験１ (a) のレストランサービスの実験結果について述べる．サラリーマン男性のお父さんがレストランサービスを利用した際の結果を図 5.1 に示す.

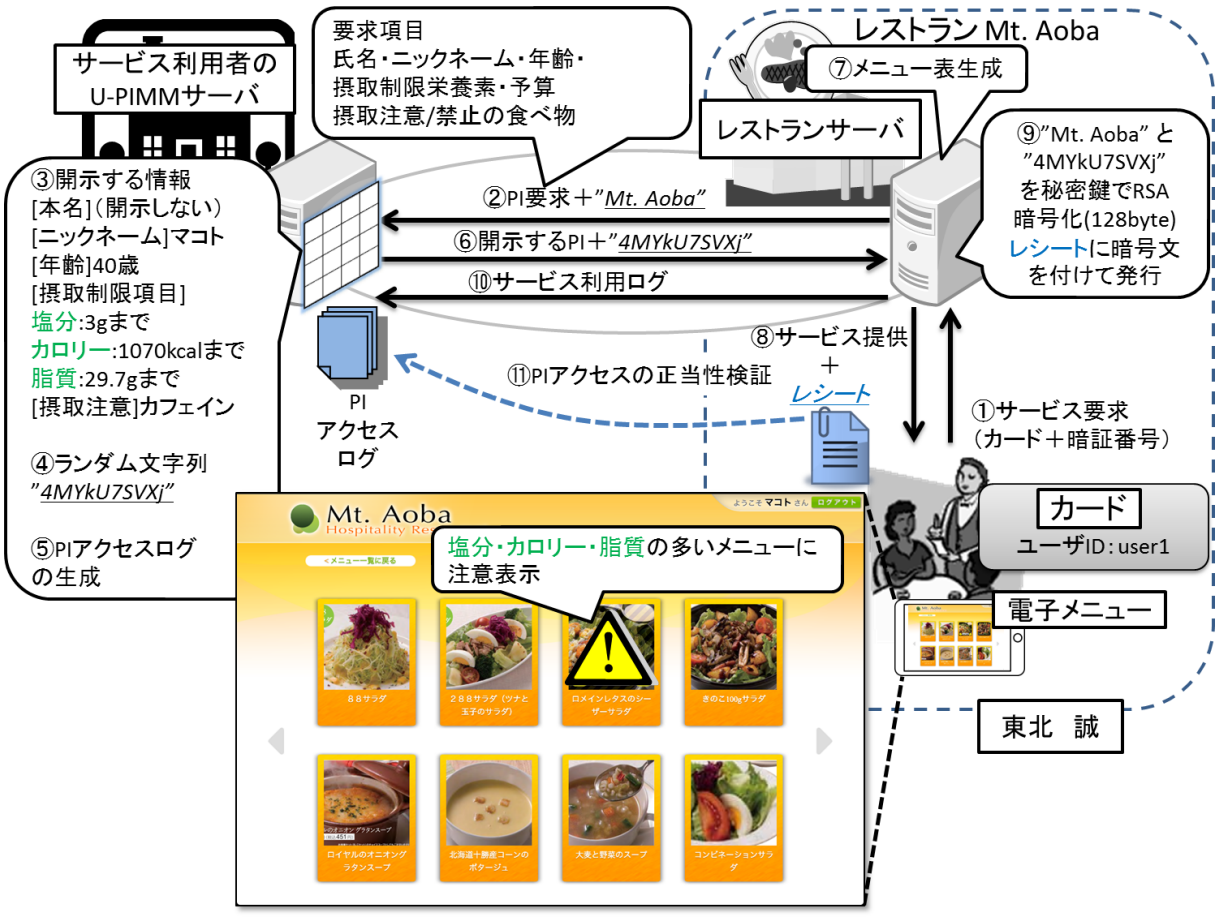


図 5.1: 実験１（a）：お父さんの場合の動作結果

```
<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE pi_request SYSTEM "pi_request.dtd" >
  <pi_request>
  <requestee>
    <dai_id>user1</dai_id>
  </requestee>
  <requestor>
    <name>Mt. Aoba</name>
    <dai_id>Mt_Aoba_dai_id</dai_id>
  </requestor>
  <service_term>
    <dai_id>family restaurant st</dai_id>
  </service_term>
  <pi_usage_policy>
    <service_type type="restaurant"/>
    <usage_purpose purpose="recommend"/>
  </pi_usage_policy>
  <requested_pi>
    <pi_type type="real_name">
    <pi_type type="pseudonym"/>
    <pi_type type="age"/>
    <pi_type type="limited_nutrition"/>
    <pi_type type="budget"/>
    <pi_type type="taboo_to_take"/>
    <pi_type type="caution_to_take"/>
  </requested_pi>
</pi_request>
```

図 5.2: 実験１（a)：個人情報要求メッセージ（お父さんの場合）

まず始めに，お父さんがレストランでカードをかざすと，カードに格納されたユーザ ID（user1）がレストランサーバに渡された．その後，レストランサーバは，user1 の U-PIMM サーバを検索し，U-PIMM サーバに対して，図 5.2 の様な XML メッセージを送り，個人情報を要求した．この時，要求した個人情報を以下に示す.

要求された個人情報

氏名，ニックネーム，年齢，摂取制限栄養素（塩分，カロリー，脂質），予算，摂取注意/禁止の食べ物

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE pi_request SYSTEM "pi_reply.dtd" >
<pi_reply>
  <pi_owner>
    <dai_id>user1</dai_id>
  </pi_owner>
  <requestor>
    <dai_id>Mt_Aoba_dai_id</dai_id>
  </requestor>
  <service_type type="restaurant"/>
  <usage_purpose purpose="recommend"/>
  <pi_update_timestamp>20110906135554</pi_update_timestamp>
  <pi>
    <any_data type=“real_name"></any_data>
    <any_data type="age">40</any_data>
    <any_data type="pseudonym">マコト</any_data>
    <budget price="2000"/>
    <limited_nutrition limit_value="3" type="SALT"/>
    <limited_nutrition limit_value="1070" type="CALORIE"/>
    <limited_nutrition limit_value="29.7" type="FAT"/>
    <caution_to_take substance="CAFFEINE"/>
  </pi>
</pi_reply>
```

図 5.3: 実験１（a)：個人情報開示メッセージ（お父さんの場合）

レストランサーバから個人情報の開示要求を受けた U-PIMM サーバは，サービス利用者が設定した個人情報開示知識を用いて，開示する個人情報を決定した．この時，個人情報開示メッセージを図 5.3 の様に生成した．また，開示された個人情報の内容を表 5.1 に示す.

表 5.1: U-PIMM サーバが開示した情報（お父さん）

開示項目	開示内容
本名	（開示しない）
ニックネーム	マコト
年齢	40
塩分（摂取上限）	3(g) まで
カロリー（摂取上限）	1070(kcal) まで
脂質（摂取上限）	29.7(g)
制限注意食品	カフェイン

その後，個人情報アクセス確認用のランダム文字列として,「4MYkU7SVXj」を生成した．その後に，アクセスログを生成し，個人情報開示メッセージとランダム文字列をレストランサーバに返答した．

U-PIMM サーバからの返答を受け取ったレストランサーバは，まず，開示された個人情報を元に，メニュー表を作成した．その後に，電子メニュー表を通して，それをお父さんに提示した．次に，レストランの名前である「Mt.Aoba」と U-PIMM サーバが発行したランダム文字列を「4MYkU7SVXj」の組みをレストランサーバの秘密鍵を用いて，RSA で暗号化した．その後に，レシートにこの暗号文を付加し，レシートをお父さんに発行した．最後に，レストランサーバはサービスの利用に関するログを U-PIMM サーバにフィードバックした．

電子メニュー表の提示内容

表示された電子メニュー表は，図 5.1 に示されているように，塩分・脂質の多いメニューについて，注意喚起が出た．これは，高血圧であるというお父さんの状況を考慮して，電子メニュー表がパーソナライズされたと言える．

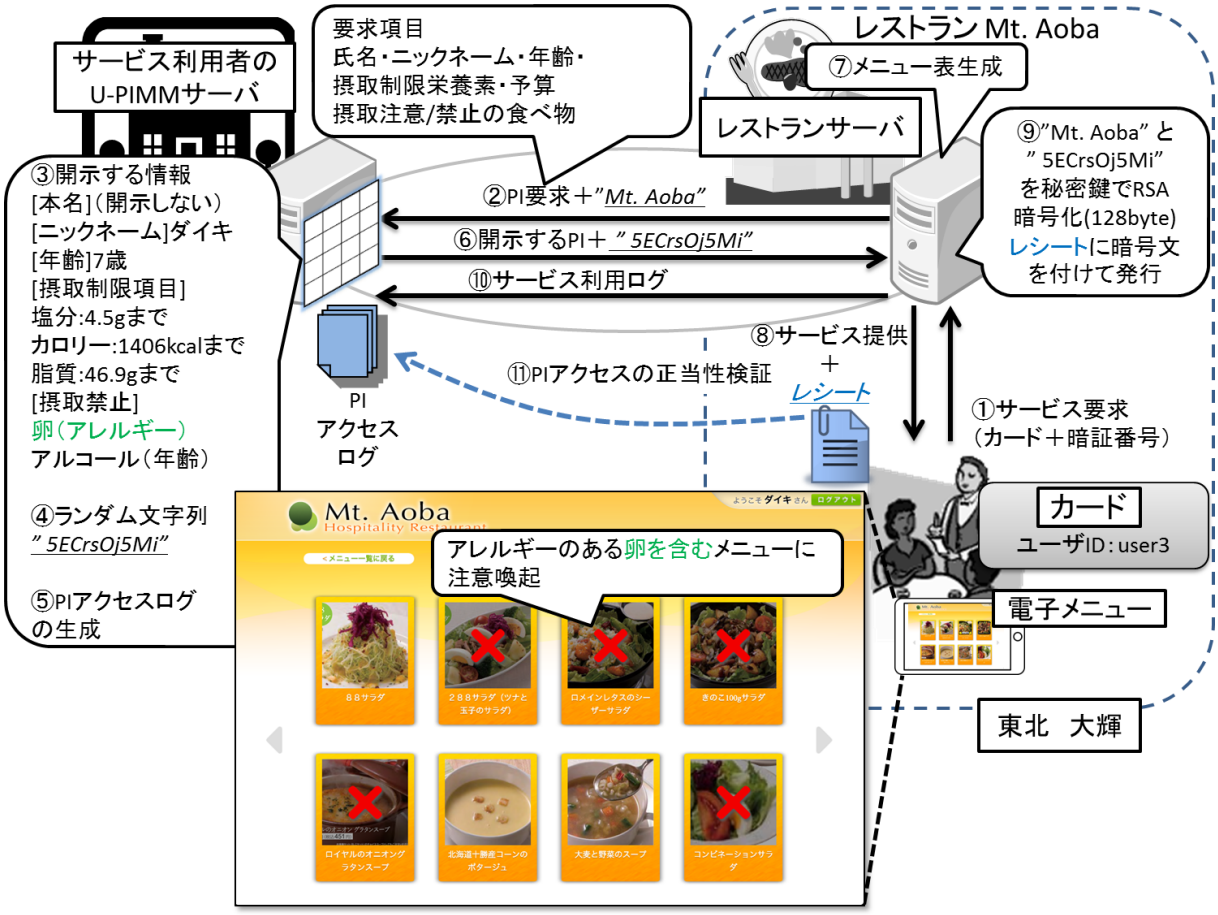


図 5.4: 実験１（a）：男の子の場合

次に，息子である男の子がレストランサービスを利用した場合の結果を図 5.4 に示す．

まず始めに，男の子がレストランでカードをかざすと，カードに格納されたユーザ ID（user3）がレストランサーバに渡された．その後，レストランサーバは，user3 の U-PIMM サーバを検索し，先ほどと同様に U-PIMM サーバに対して，個人情報を要求した．この時，要求した個人情報を以下に示す．

要求された個人情報

氏名，ニックネーム，年齢，摂取制限栄養素（塩分，カロリー，脂質），予算，摂取注意/禁止の食べ物

表 5.2: U-PIMM サーバが開示した情報（男の子）

開示項目	開示内容
本名	（開示しない）
ニックネーム	ダイキ
年齢	7
塩分（摂取上限）	4.5(g) まで
カロリー（摂取上限）	1406(kcal) まで
脂質（摂取上限）	46.9(g)
制限禁止食品	卵（アレルギー），アルコール（年齢）

レストランサーバから個人情報の開示要求を受けた U-PIMM サーバは，サービス利用者が設定した個人情報開示知識を用いて，開示する個人情報を決定した．開示された個人情報の内容を表 5.2 に示す．

その後，個人情報アクセス確認用のランダム文字列として,「5ECrsOj5Mi」を生成した．その後に，アクセスログを生成し，個人情報開示メッセージとランダム文字列をレストランサーバに返答した．U-PIMM サーバからの返答を受け取ったレストランサーバは，まず，開示された個人情報を元に，メニュー表を作成した．その後に，電子メニュー表を通して，それを男の子に提示した．次に，レストランの名前である「Mt.Aoba」と U-PIMM サーバが発行したランダム文字列を「5ECrsOj5Mi」の組みをレストランサーバの秘密鍵を用いて，RSA で暗号化した．その後に，レシートにこの暗号文を付加し，レシートを男の子に発行した．最後に，レストランサーバはサービスの利用に関するログを U-PIMM サーバにフィードバックした．

電子メニュー表の提示内容

表示された電子メニュー表は，図 5.4 に示されているように，材料に卵が含まれているメニューに注意喚起が表示された．これは，卵アレルギーであるという男の子の状況を考慮して，電子メニュー表がパーソナライズされたと言える．

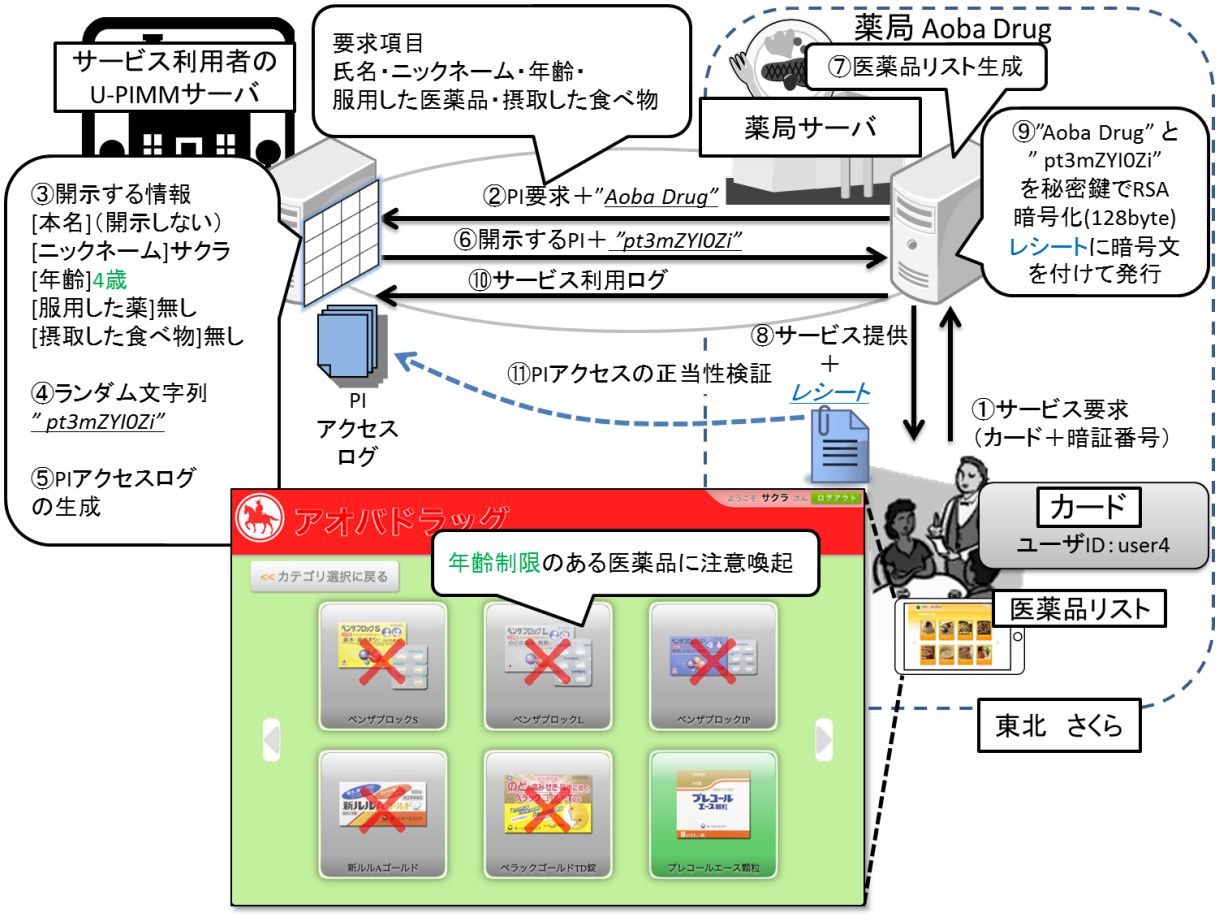


図 5.5: 実験１（b）女の子の場合

最後に，実験１ (b) の薬局における医薬品購入システムの実験結果を図 5.5 に示す.

まず始めに，女の子がレストランでカードをかざすと，カードに格納されたユーザ ID（user4）が薬局サーバに渡された．その後，薬局サーバは，user4 の U-PIMM サーバを検索し，先ほどと同様に U-PIMM サーバに対して，個人情報を要求した．この時，要求した個人情報を以下に示す.

要求された個人情報

氏名，ニックネーム，年齢，服用した医薬品，摂取した食べ物

薬局サーバから個人情報の開示要求を受けた U-PIMM サーバは，サービス利用者が設

表 5.3: U-PIMM サーバが開示した情報（女の子）

開示項目	開示内容
本名	（開示しない）
ニックネーム	サクラ
年齢	4
服用した医薬品	無し
摂取した食べ物	無し

定した個人情報開示知識を用いて，開示する個人情報を決定した．開示された個人情報の内容を表 5.3 に示す．

その後，個人情報アクセス確認用のランダム文字列として,「pt3mZYI0Zi」を生成した．その後に，アクセスログを生成し，個人情報開示メッセージとランダム文字列を薬局サーバに返答した．U-PIMM サーバからの返答を受け取った薬局サーバは，まず，開示された個人情報を元に，医薬品のリストを作成した．その後に，店頭のタッチパネルを通して，それを女の子に提示した．次に，薬局の名前である「Aoba Drug」と U-PIMM サーバが発行したランダム文字列を「pt3mZYI0Zi」の組みを薬局サーバの秘密鍵を用いて，RSA で暗号化した．その後に，レシートにこの暗号文を付加し，レシートを女の子に発行した．最後に，レストランサーバはサービスの利用に関するログを U-PIMM サーバにフィードバックした．

タッチパネルの医薬品リストの提示内容

表示された医薬品リストは，図 5.5 に示されているように，年齢制限によって服用できない物について網がけがされた．これは，女の子の年齢を考慮して，医薬品リストがパーソナライズされたと言える．

5.3 実験２

5.3.1 実験目的

U-PIMM を介した異なるサービス間の間接的連携ができる事を示す

5.3.2 実験条件

実験条件を以下に示す.

- 仕事帰りの女性（35 歳）が薬局にいった後にレストランを利用する.
- 女性は風邪気味である.
- 風邪薬の中には，アルコールとの飲み合わせが悪いものがある.

5.3.3 実験手順

実験手順を以下に示す.

1. 薬局サービスで風邪薬を購入する.
2. レストランサービスでメニューを選択する.
3. 薬局サービスでの購入履歴を反映し，パーソナライズされたメニューが表示されるかを確認する.

5.3.4 実験結果

次に，薬局サービスとレストランサービスの間接的連携に関する実験結果について述べる．まず，女性は薬局で店頭のタッチパネルを操作し，風邪薬を購入した．薬局での風邪薬の購入履歴は個人情報要求開示プロトコル OSPP により U-PIMM サーバにフィード

図 5.6: 実験２：通常時のメニュー表示

バックされ，記録された．その後，レストランを訪れ，店内の電子メニュー表を用いてメニュー推薦システムを利用した．通常時のメニュー表示を図 5.6 に示す．

この時，U-PIMM サーバにある先ほどの薬局での購入履歴が参照され，電子メニュー表のパーソナライズが行われ，図 5.7 の様な表示結果，即ちメニュー表において,「アルコール」を含むメニューに×マークが表示された．これは，薬局とレストランの間で利用履歴が共用されたと言い換える事ができる．

この時，参照された購入履歴の中には，購入した風邪薬に関する情報も含まれていた．先ほど購入した風邪薬は，以下の食べ合わせ・飲み合わせについて注意事項があった．

- 痛み止め
- 酔い止め
- 風邪薬
- アルコール

この中に食べ合わせ・飲み合わせのリストの中にアルコールがあったため，レストランサーバがメニュー表を生成する際に，飲み合わせを考慮し,「アルコール」を含むメニューに注意喚起がなされた．

図 5.7: 実験２：薬局で風邪薬購入後のメニュー表示

5.4　考察

本節では，5.2 節,5.3 節で述べた実験結果を元に考察を述べる．

実験（1）

特別な端末を用いて個人情報を携行しなくとも，ユーザの個人情報を活用し情報サービスのカスタマイズを実現できる事が確認できた．

実験（2）

サービス提供者から個人情報を分離する事で，フィードバックされたサービスの利用ログを異なるサービス間で共用し，異なるサービス間の間接的連携が可能である事が確認できた．

5.5　評価

本節では，5.2 節，5.2 節，5.4 節を元に，評価について述べる．既存研究との比較に基づく定性評価を図 5.8 に示す.

5.5.1　複数サービスでの個人情報の共用

本節では「異なるサービス間においてサービス利用者の個人情報を共用する事ができるか」について述べる.

既存手法（1）において，サービス利用者の個人情報は各々のサービス提供者によって閉鎖的に管理されている．これは，各サービス提供者によってセキュリティポリシーや運用に関するポリシーが異なるだけでなく，競合相手に個人情報を渡すことが運用・経営という観点から事実上不可能である事が理由として挙げられる．従って，複数サービスでの個人情報の共用ということは極めて困難であると言える.

既存手法（2）おいて，サービス利用者の個人情報はサービス利用者の携帯端末に管理されている．これは言い換えれば，どのサービスからでも携帯端末に保持されている同じ個人情報が参照されることになる．従って，複数サービスの個人情報の共用は可能であると言える.

提案手法においては，サービス利用者の個人情報はサービス利用者の U-PIMM に管理されている．そして，サービス提供者は U-PIMM に対して OSPP プロトコルにより，個人情報の要求・開示を行い，サービス利用者の個人情報を利用する事となる．この時，いずれのサービスも利用者の U-PIMM の個人情報を参照している事になる．したがって，複数サービスの個人情報の共用は可能であると言える.

5.5.2　サービス提供者への個人情報事前登録の有無

本節では「サービス利用者が情報サービスのパーソナライズを受ける際に，個人情報を事前に登録しておく必要があるか」について述べる．

既存手法（1）について，サービス提供者がサービス利用者に対してパーソナライズされた情報サービスを提供するためには，必ず個人情報を前もって自分の管理下のデーターベースなどに登録してある状態でないとパーソナライズができない．そのため，サービス利用者は必ず前もって各サービスのサービス提供者に対して個人情報を提供する必要がある．従って，サービス提供者への個人情報事前登録の有無については必要であると言える．

既存手法（2）について，サービス利用者はパーソナライズされた情報サービスを利用する際に，パーソナライズに必要な個人情報を携帯端末から提示する．つまり，携帯端末に情報を予め入れておけば，各々のサービスに対する個人情報の登録は不要であると言える．従って，サービス提供者への個人情報事前登録の有無については不要であると言える．

提案手法について，サービス利用者がパーソナライズされた情報サービスを利用する際には，サービス提供者は U-PIMM に登録された個人情報を利用する．つまり，U-PIMM に個人情報を登録しておけば，各々のサービスに対する個人情報の登録は不要であると言える．従って，サービス提供者への個人情報事前登録の有無については不要であると言える．

5.5.3　サービスを利用する上で携行する必要があるもの

本節では,「パーソナライズされた情報サービスを利用する際に，携行しなければならないならない物」について述べる．

既存手法（1）について，サービス利用者は自身を識別できるものがあれば，パーソナライズされた情報サービスを受ける事ができる．従って，サービスを利用する上で携行する必要があるものは，自らの ID などが記録されたカード程度であると言える．

既存手法（2）について，サービス利用者は自らの個人情報を保持するために，個人情報の入ったスマートフォンや PDA などといった計算能力のある携帯端末を携行する必要が出てくる．従って，サービスを利用する上で携行する必要があるものは，計算能力のある携帯端末が挙げられる．

提案手法について，サービス利用者は自身を識別できる物があればよく，サービス提供者はその情報を用いて U-PIMM にアクセスし，個人情報要求をすることができる．即ち，特に特別な機器・端末等を携行しなくとも良いと言える．従って，サービスを利用する上で携行する必要があるものは，自らの ID などが記録されたカード程度だと言える．

5.5.4　各評価項目の両立について

本節では，各評価項目について各手法が両立可能かについて述べる．

既存手法（1）について，特に特別な端末を携行しなくとも情報サービスをパーソナライズできるため，誰もがパーソナライズされた情報サービスを利用可能だと言える．従って，本研究における人間性を達成している．しかしながら，複数サービス間での個人情報の共有が極めて困難であるため，サービス間での間接的連携はほぼ不可能である．また，必ず前もって個人情報をそれぞれのサービスについて登録する必要性が生じており，本研究における社会性を達成することができないと言える．

一方，既存手法（2）について，携帯端末に個人情報を保持し携行するため，複数サービスでの個人情報の共用が可能となり，複数サービス間で間接的連携が可能であると言えるまた，各々のサービス提供者への個人情報の事前登録が不要である事から，あたかもいつものように情報サービスを利用する事が可能であると言える．従って，本研究における社会性を達成している．しかしながら，個人情報の運用のために必ず計算能力のある携帯端末を持ち歩かなければならず，携行する事により携帯端末の情報漏洩や所有する複数の携帯端末間の同期などに代表される運用の煩雑さが生まれる．また，特別な機器や携帯端末を持つ事自体が全ての人が誰もが利用できることを阻害すると考えられる．従って，本研究における人間性を達成する事ができないと言える．

提案手法においては，特別な端末を携行しなくともパーソナライズされた情報サービスを利用できるため，誰もがカードを持ち歩く程度でパーソナライズされた情報サービスの恩恵を享受できる．また，サービス利用者がパーソナライズされた情報サービスを受ける際に，U-PIMM に管理されている個人情報をサービスが参照するため，初めて利用する情報サービスや馴染みのない情報サービスでも，あたかもいつものようにその情報サービスを利用する事ができるようになる．従って，サービス提供者と個人情報の分離と個人情報の不携行を両立し，本研究における人間性と社会性を両立することを達成していると言える．

	複数サービスでの 個人情報の共用	サービス提供者への個人 情報事前登録の有無	サービスを利用する上で 携行する必要がある物
既存手法（１）： サービス提供者による 個人情報管理	極めて困難	必要	カード
既存手法（２）： 利用者携帯端末を 用いた個人情報管理	可能	不要	計算能力のある 携帯端末
提案手法： 開放型の情報サービス パーソナライズ手法	可能	不要	カード

両立

図 5.8: 既存手法との比較

5.6　本研究の成果

本節では，本章で得た評価結果を基に，本研究の成果についてまとめる．

本研究では，人間性と社会性についてその両方を考慮し，誰でも・いつものように使える利用者の状況を考慮した情報サービスの実現を目指した．

本研究における人間性とは,「特別な端末を利用しなくとも自分用にパーソナライズされたサービスが提供できる性質」であった．この性質によって，老若男女問わずに誰もが自分用にパーソナライズされた情報サービスを利用できるようになる．また，本研究における社会性とは,「使い慣れていないサービスでも柔軟に対応し，各サービスへの個人情報の事前登録がなくとも慣れ親しんだサービスが提供できる性質」であった．

従来の情報サービスパーソナライズ手法は，個人情報の管理領域がサービス提供者・サービス利用者のいずれかになっており，前者が人間性，後者が社会性を満たす情報パーソナライズによって片方の性質のみをもつ情報サービスの構築を構築することができていた．しかしながら，それぞれ片方の性質を満たすために，もう片方の性質を満たす事ができないトレードオフがあったため，人間性と社会性を両立した情報サービスを構築する事はできなかった．

本研究の提案である開放型の情報サービスパーソナライズ手法は，個人情報の管理領域をサービス提供者・サービス利用者ともに物理的に分離した個人情報管理機構とし，そこで管理されている個人情報を利活用するために必要なプロトコルを与える事で，人間性・社会性の両方を満たす情報サービスのパーソナライズが可能となり，これをもって人間性・社会性を考慮した情報サービスが可能になったと言う事ができる．

第6章　結論

6.1　まとめ

本研究の目的は，誰でも・いつもの様に使える，利用者の状況を考慮した情報サービスの実現することである．そのためには，人間性・社会性を考慮した情報サービスを構築する必要があった．そこで本論文では，サービス利用者が所有する個人情報管理機構 U-PIMM(User-owned Personal Information Management Mechanism) と個人情報開示プロトコル OSPP(Open Service Personalization Protocol) からなる開放型の情報サービスパーソナライズ手法を提案した．本手法は，サービス利用者が所有する個人情報管理機構 U-PIMM に利用者の個人情報を登録し，個人情報の要求相手による個人情報の開示制限と個人情報アクセスの正当性検証を可能にする個人情報開示プロトコル OSPP を導入する事で，誰でも・いつもの様に情報サービスのパーソナライズが可能となる．そして実験の結果より，情報サービスにおけるパーソナライズの実現と異なるサービス間の間接的連携が可能であることを示した．この事から，個人情報管理機構 U-PIMM により，個人情報をサービス提供者・利用者と分離する事で，特別な端末を携行しなくともパーソナライズされた情報サービスを利用できるようになったと言える．これにより，誰もが利用可能な心のこもったサービスが実現可能となり，情報サービスの人間性が実現できたと評価できる．また，個人情報要求開示プロトコル OSPP によりサービス提供者への個人情報の事前登録がなくとも，複数サービスでの個人情報の共用が可能になったと言える．これにより，使い慣れないサービスでもあたかもいつものようにサービスが利用できるようになり，情報サービスの社会性が実現できたと評価できる．

よって，提案手法を用いる事で，個人情報のサービス提供者・利用者からの分離と特別

な端末の不携行の両立を実現し，誰でもいつもの様に情報サービスをパーソナライズすることができる．以上により，本論文における提案が人間性・社会性を考慮した情報サービスを構築することを可能にすると結論づける．

6.2　今後の課題

本研究において，サービス利用者のためのパーソナライズに用いられる情報は，サービス利用者自身によって入力された物であった．今後は，サービス利用者自身によって入力された情報だけではなく，サービス利用者以外の主体によって作成された情報も活用できる仕組みが必要であると考えられる．例えば，医療機関で発行される電子カルテやお薬手帳，行政が発行する住民票や高齢者証明などのように，その情報をサービス利用者が誤記してしまったり虚偽の報告をしたりすることで，サービス利用者が損害を受けたり，本来，情報サービスからその恩恵を享受すべき人の権利を損なうような場面が出てくると考える．これは，言い換えれば「情報の作成者が誰なのか」を明らかにする事が必要であると考えられる．

この課題に対する具体案としては，情報作成者が情報に対して電子署名を付加し，署名された情報をサービス利用者の U-PIMM に保存するといった手段が考えられる．これにより，情報の作成者が誰なのかを付加された署名から明らかにする事ができる．即ち，サービス提供者は署名を確認することで，その情報が信頼の置ける人物や団体によって生成された情報である事を検証できるようになるため，信頼性の高い情報を必要とする情報サービスへの本提案の適用が可能になると考えられる．

情報サービスがサービス利用者にとってより便利な物になってゆく今日において，サービス利用者に寄り添うように情報サービスがパーソナライズされることはごく自然な事となってきている．しかしながらその一方で，パーソナライズに用いられるサービス利用者の個人情報の扱いはとても難しくなってきており，サービス利用者の意図に反してサービス提供者が恣意的に運用したり，サービス利用者自身が管理するにせよ，サービス利用のための個人情報の開示や個人情報のアクセスに対する正当性確保等を念頭に置きなが

らの運用は困難を極める．従って，特別な端末や煩雑な運用に縛られない老若男女「誰もが」利用できる情報サービスのパーソナライズが求められている．また，情報サービスがサービス毎に閉鎖的に個々の範疇でのみサービス利用者と対峙するのではなく，例えば，サービス利用者の生活スタイルや利用者の置かれているコンテクスト，行動規範といったより広い意味でサービス利用者の「いつも通り」を考慮したパーソナライズが求められてきている．こうしたパーソナライズはいかにサービスを越えて個人情報を利活用するかが肝要であることは明らかである．

本研究で扱った情報サービスの人間性や社会性というものは，以上述べたこれからの情報サービスがあるべき姿となるための満たすべき性質であり，より真の意味で情報サービスがサービス利用者に歩み寄ることを実現する一助となったと考えられる．そして将来，情報サービスがより高度に発展し便利になっていく中で，情報サービスがサービス利用者と共に歩んで行くための様々な技術が生み出され，より豊かな情報社会になると確信している．

謝辞

本論文は筆者が東北大学大学院情報科学研究科情報基礎科学専攻博士課程前期２年の課程に在籍中の研究成果をまとめたものです.

本論文を終えるにあたり，日頃の研究活動の際に貴重な御指導を賜りました東北大学電気通信研究所教授 木下哲男先生に心から感謝致します.

また，東北大学電気通信研究所教授 外山芳人先生，並びに東北大学電気通信研究所教授 鈴木陽一先生には，本論文をまとめる上で多大な御助言に賜り，また御多忙の中本論文の審査をしていただきました．謹んで感謝致します.

東北大学電気通信研究所准教授 北形元先生には，学部時代より，日々の研究活動や研究室生活など数多くの有益な御指導，御助力，御助言を賜りました．また，本論文をまとめる際にも，常日頃より沢山の示唆に富んだ研究に関するディスカッションをしていただきました．今までご教示いただいた事は，私のこれからの支えとなると確信しています.謹んで深く感謝致します.

東北大学電気通信研究所客員教授・名誉教授 白鳥則郎先生には，この様な興味深く意義ある研究テーマを与えていただき，また研究を進める上で沢山の造詣の深い御指導，御助言に加え，広く，心強い御助力を賜りました．心より深く感謝致します.

東北大学大学院情報科学研究科教授 橋本和夫先生には，日頃行われたディスカッション等を通し，御助言を数多く賜りました．また，本研究を進める上で，様々な示唆に富んだ御指導，御助力を賜りました．そのウィットに富んだご教示はこれからも私の糧となると思います．謹んで深く感謝致します.

東北学院大学教養学部情報科学科准教授 武田敦志先生には，御多忙の中，数多くの貴重な御助言，御助力を賜りました．また，研究活動について，相談に乗っていただき，そ

の度に思慮深く意義ある御指導を賜りました．ご教示を通して，研究の面白さを教えていただいた事は私にとってとても大きな事でした．心より，深く感謝致します．

東北大学サイバーサイエンスセンター教授 菅沼拓夫先生には，折に触れ，広く研究室生活において多大なる御助力いただきました．また大学院セミナー等を通して，平素より数多く示唆に富んだ御指導，御助言を賜りました．賜りましたポイントを押さえたアドバイスは，本論文をまとめる上で大変参考になりました．心より深く感謝致します．

東北大学電気通信研究所助教 高橋秀幸先生には，研究活動は勿論の事，研究室生活に至るまで幅広く日頃から多くの御指導，御助言を賜りました．大学院セミナー等にいただいた細かなアドバイスは，本論文をまとめる上でとても参考になりました．心より深く感謝致します．

東北大学電気通信研究所助教 笹井一人先生には，大学院セミナー等で日頃から多くの御指導，御助言を賜りました．心より深く感謝致します．

東北大学大学院情報科学研究科コミュニケーション論講座の和泉諭先輩には，学部生の頃より，研究活動のみならず，研究室生活全般でお世話になりました．お忙しい中，研究活動をする上で具体的にどう考え行動すべきか等の沢山のノウハウをご教示いただけたことは私のこの研究室生活の宝です．心より感謝いたします．

東北大学大学院情報科学研究科コミュニケーション論講座の伊藤大視先輩には，研究活動において，沢山の御助言と特にプログラミングに関して様々な示唆に富んだアドバイスをいただきました．その論理的かつ的確な研究に対する姿勢は，研究を進める上でとても参考になりました．謹んで感謝致します．

東北大学大学院情報科学研究科コミュニケーション論講座の Khamisi Kalegele 先輩には，研究活動において，様々な御助言を頂いただけでなく，そのインターナショナルな視点からの様々な見識に基づく知見を与えていただきました．心より感謝致します．

東北大学大学院情報科学研究科コミュニケーション論講座の魏文鵬先輩には，研究活動に関してお忙しい最中相談に乗っていただき，沢山の御助言を頂いただけでなく，研究室生活においても様々な御助力を賜りました．謹んで感謝致します．

株式会社電通国際情報サービスの中山誠也先輩には，在学中，私の研究生活を始める

上での様々なスキルや知識を丁寧に御指導して頂いただけでなく，本研究の元となった学士の研究において多大なる御助言・御助力を頂きました．その際に頂いた御指導が無ければ，本研究はまとめられなかったと思います．心より感謝致します．

ヤフー株式会社の今村理先輩には，在学中，本研究を進める上で貴重なご意見を賜り，本研究の詳細について貴重なお時間を頂いて，意義ある議論を重ねる事ができました．また，本研究における提案手法のプロトタイプシステムの設計・実装に関しまして多大なる御助力を賜りました．ここに深く感謝致します．

東北大学大学院情報科学研究科コミュニケーション論講座の同学の皆様には，研究活動や研究室生活において，支え合い，時に励まし合いながら，貴重な示唆，御助言をいただきました．皆様のおかげで研究生活がとても充実した楽しい物となり，私の精神的な支えとなりました．皆様と苦楽を共にし，研究活動や研究室生活をやり通した事はこれからも私の支えとなると思います．ここに深く感謝致します．

東北大学大学院情報科学研究科先端情報共有技術論 (KDDI) 寄附講座の大澤由憲さんには，本研究を進めるにあたり，学部時代より互いに協力し，時に沢山の議論を重ねながら研究を進めました．また，本研究の提案手法のプロトタイプシステムの設計・実装に関しまして多大なる御助力を賜りました．ここに深く感謝致します．

東北大学大学院情報科学研究科コミュニケーション論講座の後輩の皆様には，研究室生活において精神的支えとなっただけでなく，研究活動において，時に機知に富んだ御助言をいただきました．加えて，皆様の研究活動について微力ながらご意見申し上げたことが，自身の研究に対する洞察を深めることに繋がりました．ここに感謝致します．

最後に，研究生活を含め，この仙台の地での生活を内外で支えてくれた多くの友人達，共に生活をしながら日常生活を支え合った弟，そして，経済的にも精神的にも大きな支えとなった両親に対して最大限の感謝の意を表し，本論文を締めくくりたいと思います．

発表論文

国際会議

1. Akihiro Nakarai, Akira Sakatoku, Atsushi Takeda, Gen Kitagata, Debasish Chakraborty, Kazuo Hashimoto and Norio Shiratori, “An Overlay Authentication Network for Active Utilization of Private Information”, 10th Annual International Symposium on Applications and the Internet, pp.185-188, July. 2010

2. Satoru Imamura, Akihiro Nakarai, Yoshinori Osawa, Atsushi Takeda, Gen Kitagata, Norio Shiratori, and Kazuo Hashimoto, “Private information utilization scheme toward ubiquitous society, ”SOIM-GCOE10, Sendai, Japan, October. 2010.

研究会・ワークショップ

1. 半井明大，中山誠也，武田敦志，北形元，橋本和夫，白鳥則郎，“プライバシーを考慮した分散認証法の提案”, 電子情報通信学会 2010 総合大会講演論文集 (通信講演論文集 2), p.S-93, 2010.03

2. 半井明大, 中山誠也, 武田 敦志, 北形元, 橋本和夫, 白鳥則郎, “個人情報の安全な利活用に向けた分散型認証法の提案”, マルチメディア，分散，協調とモバイル (DICOMO2010) シンポジウム, pp.1480-1485, 2010.07

3. 北形元，半井明大，大澤由憲，今村理，武田敦志，橋本和夫, 木下哲男，白鳥則郎, “個人情報の安全な利活用のためのオーバーレイ認証ネットワークの提案”, 平成 22 年度 電気関係学会東北支部連合大会講演論文集, p.101, 2010.08

4. 今村理, 半井明大, 大澤由憲, 武田敦志, 北形元, 白鳥則郎, 橋本和夫, “分散認証基盤を活用したプライベート情報交換アーキテクチャの提案” , 第 9 回情報科学技術フォーラム講演論文集 (FIT2010), 第 4 分冊, pp.259-262, 2010.09

5. 東北大学 大学院情報科学研究科, “個人情報の安全な利活用のための分散型情報交換アーキテクチャ” 第 9 回情報科学技術フォーラム (FIT2010), 2010.09

6. 北形元, 半井明大, 大澤由憲, 今村理, 武田敦志, 橋本和夫, 白鳥則郎, “Socio-familiar Personalized Service の概念に基づくメニュー推薦システム”, 第 18 回マルチメディア通信と分散処理ワークショップ論文集 (DPSWS2010), IPSJ SIG Technical Report pp.2010-2011, 2010.10

7. 北形元, 半井明大, 大澤由憲, 今村理, 武田敦志, 橋本和夫, 白鳥則郎, “Socio-familiar Personalized Service の概念に基づくメニュー推薦システム”, 第 18 回マルチメディア通信と分散処理ワークショップ (DPSWS2010), 2010.10

   (**ベストデモンストレーション賞**)

8. 今村理, 半井明大, 大澤由憲, 武田敦志, 北形　元, 白鳥則郎, 橋本和夫, “ユビキタス環境に適したプライベート情報交換アーキテクチャの提案”, 第 18 回マルチメディア通信と分散処理ワークショップ論文集 (DPSWS2010), pp.75-80 2010.10

9. 半井明大, 大澤由憲, 今村理, 武田敦志, 北形元, Chakraborty Debasish, 橋本和夫, 白鳥則郎, 木下哲男, “パーベイシブ環境におけるサービスの個人化とその応用”, 情報処理学会第 73 回全国大会講演論文集, pp.389-391, 2011.3

10. 大澤由憲, 今村理, 半井明大, 武田敦志, 北形元, 白鳥則郎, 橋本和夫, “個人情報を活用した人にやさしいサービスの実現方法に関する検討”, 情報処理学会第 73 回全国大会講演論文集, pp.549-551, 2011.3

11. 半井明大, 大澤由憲, 武田敦志, 北形　元, 橋本和夫, 白鳥則郎, 木下哲男, “利用者が所有する個人情報を活用したサービス横断的個人化方式の提案” 電子情報通信

学会情報ネットワーク研究会, 信学技報 IN2011-77, pp.49-52, 2011.9

参考文献

[1] Mark Weiser, “The Computer for the Twenty-First Century,” Scientific American, pp. 94-10, September 1991

[2] 和泉諭, 加藤靖, 高橋薫, 菅沼拓夫, 白鳥則郎, “オントロジを利用した健康支援システムの提案とその評価,” 情報処理学会論文誌, Vol.49, No.2, pp.822-837, 2008.

[3] Satoru Izumi, Kazuhiro Yamanaka, Yoshikazu Tokairin, Hideyuki Takahashi, Takuo Suganuma, and Norio Shiratori, “Ubiquitous Supervisory System based on Social Contexts using Ontology,” Mobile Information Systems (MIS), Vol.5, No.2, pp.141-163, 2009.

[4] Dimitrios D. Vergados, “Service personalization for assistive living in a mobile ambient healthcare-networked environment,” Personal Ubiquitous Comput. Vol.14, No.6 , pp.575-590, September 2010.

[5] Myong-Woo Lee, Adil Mehmood Khan, and Tae-Seong Kim, “A single tri-axial accelerometer-based real-time personal life log system capable of human activity recognition and exercise information generation,” Personal Ubiquitous Comput. Vol.15, No.8 , pp.887-898, December 2011.

[6] Masanobu Abe, Yuji Morinishi, Atsuhiko Maeda, Masakatsu Aoki, and Hirohito Inagaki, “A life log collector integrated with a remote-controller for enabling user centric services,” Consumer Electronics, IEEE Transactions on , Vol.55, No.1, pp.295-302, February 2009

[7] Eric Steinhart, “Survival as a Digital Ghost,” Minds and Machines, Vol.7, No.3, pp.261-271, 2007

[8] Derek Reilly, Bonnie Mackay, Carolyn Watters, and Kori Inkpen, “Planners, navigators, and pragmatists: collaborative wayfinding using a single mobile phone,” Personal Ubiquitous Comput. Vol.13, No.4 , pp.321-329, May 2009.

[9] Liliana Ardissono, Tsvi Kuflik and Daniela Petrelli, “Personalization in cultural heritage: the road travelled and the one ahead,” User Modeling and User-Adapted Interaction, Online First, October 2011.

[10] Koji Kamei, Tetsushi Ikeda, Hiroyuki Kidokoro, Masayuki Shiomi, Akira Utsumi, Kazuhiko Shinozawa, Takahiro Miyashita, and Norihiro Hagita, “Effectiveness of Cooperative Customer Navigation from Robots around a Retail Shop,” Privacy, Security, Risk and Trust (PASSAT), 2011 IEEE Third International Conference on and 2011 IEEE Third International Confernece on Social Computing (SocialCom) , vol., no., pp.235-241, 9-11 Oct. 2011

[11] Michael S. Bernstein, Desney Tan, Greg Smith, Mary Czerwinski, and Eric Horvitz, “Personalization via friendsourcing,” ACM Trans. Comput.-Hum. Interact. Vol.17, No.2, Article 6, 28 pages, May 2008.

[12] Jaime Teevan, Susan T. Dumais, and Eric Horvitz, “Potential for personalization,” ACM Trans. Comput.-Hum. Interact. Vol.17, No.1, Article 4, 31 pages, April 2010.

[13] Kevin McNally, Michael P. O ’Mahony, Maurice Coyle, Peter Briggs, and Barry Smyth, “A Case Study of Collaboration and Reputation in Social Web Search,” ACM Trans. Intell. Syst. Technol. Vol.3, No.1, Article 4, 29 pages, October 2011

[14] Amazon, http://www.amazon.com/

[15] iGoogle, http://www.google.com/ig

[16] 橋本和夫, 北形元, 高橋秀幸, 武田敦志, チャクラボルティデバシシュ, 白鳥則郎, “Socio-familiar Personalized Service の提案とその応用-次世代ユビキタスサービスを実現する

ネットワークソフトウェアへ向けて-, ”電子情報通信学会論文誌, Vol.J94-B,No.4,pp.492-502, Apr. 2011.

[17] 個人情報の保護に関する法律（平成十五年五月三十日法律第五十七号）Available: http://law.e-gov.go.jp/cgi-bin/idxsearch.cgi

[18] Shiwan Zhao, Michelle X. Zhou, Xiatioan Zhang, Quan Yuan, Wentao Zheng, and Rongyao Fu, “Who is Doing What and When: Social Map-Based Recommendation for Content-Centric Social Web Sites, ”ACM Trans. Intell. Syst. Technol. Vol.3, No.1, Article 5, Oct. 2011

[19] Aya Okamoto, “A Proposal of Distributed Authentication Platform and Public Identifiers - On Appropriateness of Web Traversal Anonymous Authentication using OpenID -, ” IEICE Technical Report, Vol.SITE2008-53, No.IA2008-76(2009-03), 2008.

[20] Hong Chen and Qun Jin, “Ubiquitous Personal Study: a framework for supporting information access and sharing,” Personal Ubiquitous Comput. Vol.13, No.7, pp.539-548, Oct. 2009

[21] Miriam Gil, Pau Giner and Vicente Pelechano, “Personalization for unobtrusive service interaction,” Personal Ubiquitous Comput. Online First, -, Jun. 2011.

[22] Dieter Sommer, Marco Casassa Mont, and Siani Pearson, “PRIME Architecture V3,” https://www.prime-project.eu/

[23] Tatsuo Nakajima and Ichiro Satoh, “A software infrastructure for supporting spontaneous and personalized interaction in home computing environments,” Personal Ubiquitous Comput. Vol.10, No.6, pp.379-391, Sep. 2006.

[24] S. Uribe, F. Alvarez, J. M. Menendez, and G. Cisneros, “Visual Targeted Advertisement System Based on User Profiling and Content Consumption for Mobile Broadcasting Television, ”Mob. Netw. Appl. Vol.16, No.3, pp.361-374, Jun. 2011.

[25] Jose M. Alamo, Antonio M. Fernandez, Ruben Trapero, Juan C. Yelmo, and Miguel A. Monjas, “A Privacy-Considerate Framework for Identity Management in Mobile Services,” Mob. Netw. Appl. Vol.16, No.4 , pp.446-459, August 2011.

[26] Yoshinori Osawa, Satoru Imamura, Atsushi Takeda, Gen Kitagata, Norio Shiratori and Kazuo Hashimoto, “A Proposal of Privacy Management Architecture,” Proceedings of the 10th IEEE/IPSJ International Symposium on Applications and the Internet, 2010.

[27] Atsushi Takeda, Chakraborty Debasish, Gen Kitagata, Kazuo Hashimoto and Norio Shiratori, “Proposal and Performance Evaluation of Hash-based Authentication for P2P Network,” IPSJ Journal,Vol.50, No.2, pp.737-749, 2009.

[28] Atsushi Takeda, Seiya Nakayama, Gen Kitagata, Debasish Chakraborty, Kazuo Hashimoto, and Norio Shiratori, “Hash-based Distributed Public Key Infrastructure for Ubiquitous Environments ”in Proc. of the 4th International Conference on Complex, Intelligent and Software Intensive Systems (CISIS2010),pp.376-383, Feb. 2010.

[29] Ion Stoica, Robert Morris, David Karger, M. Frans Kaashoek, and Hari Balakrishnan, “Chord : A Scalable Peer-toPeer Lookup Protocol for Internet Applications”, IEEE/ACM Trans. Networking, Vol.11, No.1, pp.17-32, 2003.

[30] Overlay Weaver, Available: http://overlayweaver.sourceforge.net/

[31] 消費者庁　アレルギー物質を含む加工食品の表示ハンドブック, http://www.caa.go.jp/foods/pdf/syokuhin19.pdf

[32] AllegroGraph, http://www.franz.com/agraph/allegrograph/

[33] Resource Description Framework(RDF): Concepts and Abstract Syntax, http://www.w3.org/TR/rdf-concepts/

[34] Phidgets, http://www.phidgets.com/

付 録A　OSPPプロトコルのメッセージスキーマ

以下に，個人情報要求メッセージ，個人情報開示メッセージ，サービス利用ログメッセージの３つのメッセージのスキーマをDTD形式で示す．尚，各DTD中のLIST １，２，３の内容は以下に示すとおりである．

LIST1

BEEF|PORK|CHICKEN|MACKEREL|BREVOORT|PRAWN|
JP_RADISH|ONION|CABBAGE|CARROT|BEANSPROUT|
CHIVEE|TOMATO|PARSLEY|CELERY|GREEN_ONION|
EGGPLANT|SPINACH|SQUASH|CUCUMBER|
CH_MUSHROOM|BAMBOO_SPROUT|LOTUS_ROOT|
BURDOCK|WOOD_EAR|CH_CABBAGE|CORN|
BROWN_SEAWEED|HIJIKI|FUNORI|
TENGUSA|KELP|APPLE|LEMON|POTATO|AROID|SOYBEAN|
KIDNEY_BEAN|TAPIOCA|SWORD_BEAN|DRIED_JP_RADISH|
DRIED_BONITO|MISO|RICE_MISO|TOFU|GELATIN|CHEESE|
FRIED_TOFU|KONJAC|NATTO|STARCH|GARLIC|GINGER|SESAMI|
CHILLI|WASABI|CURRY_POWDER|JP_BASIL_BERRY|
RICE|WHEAT|CRUMB|BUCKWHEAT| MILK|EGG|SAKE_LEES

LIST2

CAFFEINE|SODA|ALCOHOL|SHRIMP|CRAB|WHEAT|
BUCKWHEAT|EGG|MILK|PEANUT|ABALONE|SQUID|
SALMON_CAVIAR|ORANGE|KIWI_FRUIT|BEEF|
WALNUT|SALMON|MACKEREL|SOYBEAN|CHICKEN|
BANANA|PORK|MATSUTAKE|PEACH|YAM|APPLE|GELATIN

LIST3

BUFFERIN_A|NORSHIN_PURE|SARIDON_WI|HEADACHE_POWDER|
EVE_A|NEW_SEDES|NARON_ACE|ANERON_NYSCAP|
SENPA|TRAVELMIN|PANSIRON_TRAVEL|SAVE|SAVE_DRINK|BENZA_BLOCK_S|
BENZA_BLOCK_L|BENZA_BLOCK_IP|NEW_LULU_A_GOLD|
PELACK_GOLD_TD|PRECOL_ACE_POWDER|CAKONAL2|
SS_KAKKONTOH_POWDER_A|KAIGEN|SENPA_DRINK

```
<?xml version="1.0" encoding="UTF-8"?>

<!ELEMENT pi_request (requestee, requestor, service_term,
pi_usage_policy, requested_pi)>

<!ELEMENT requestee (dai_id)>

<!ELEMENT requestor (name, dai_id)>
<!ELEMENT service_term (dai_id)>
<!ELEMENT pi_usage_policy (service_type+, usage_purpose+)>
<!ELEMENT requested_pi (pi_type+)>

<!ELEMENT name (#PCDATA)>
<!ELEMENT dai_id (#PCDATA)>
<!ELEMENT service_type EMPTY>
<!ATTLIST service_type type
(restaurant|transporter|health_care|pharmacy) #REQUIRED>
<!ELEMENT usage_purpose EMPTY>
<!ATTLIST usage_purpose purpose
(recommend|transport_things|transport_people) #REQUIRED>
<!ELEMENT pi_type EMPTY>
<!ATTLIST pi_type type
(real_name|pseudonym|religion|age|favorite_food|wanted_nutrition|limited_nutrition|
taken_drug|eaten_food|taboo_to_take|caution_to_take) #REQUIRED>
```

図 A.1: 個人情報要求メッセージの DTD

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Document Root -->
<!ELEMENT pi_reply (pi_owner, requestor, service_type*, usage_purpose*, pi_update_timestamp,
pi)>
<!-- Document Header -->
<!ELEMENT pi_owner (dai_id)>
<!ELEMENT requestor (dai_id)>
<!ELEMENT dai_id (#PCDATA)>
<!ELEMENT pi_update_timestamp (#PCDATA)>
<!-- Service Info & PI Usage Policy -->
<!ELEMENT service_type EMPTY>
<!ATTLIST service_type type (restaurant|transporter|health_care|pharmacy) #REQUIRED>
<!ELEMENT usage_purpose EMPTY>
<!ATTLIST usage_purpose purpose (recommend|transport_things|transport_people) #REQUIRED>
<!-- PI  -->
<!ELEMENT pi (any_data|favorite_food|wanted_nutrition|limited_nutrition|budget|
taboo_to_take|caution_to_take|eaten_food|taken_drug)*>
<!-- String Data -->
<!ELEMENT any_data (#PCDATA)>
<!ATTLIST any_data type (real_name|pseudonym|religion|age) #REQUIRED>
<!-- for Restaurant Service -->
<!ELEMENT favorite_food EMPTY>
<!ATTLIST favorite_food kind (          LIST 1          ) #REQUIRED>
<!ATTLIST favorite_food value CDATA #REQUIRED>
<!ELEMENT wanted_nutrition EMPTY>
<!ATTLIST wanted_nutrition type (CALORIE|RED|YELLOW|GREEN) #REQUIRED>
<!ATTLIST wanted_nutrition min_value CDATA #REQUIRED max_value CDATA #REQUIRED>
<!-- for Family Restaurant Service -->
<!ELEMENT limited_nutrition EMPTY>
<!ATTLIST limited_nutrition type (CALORIE|SALT|FAT) #REQUIRED limit_value CDATA #REQUIRED>
<!ELEMENT taboo_to_take EMPTY>
<!ATTLIST taboo_to_take substance (     LIST 2     ) #REQUIRED>
<!ELEMENT caution_to_take EMPTY>
<!ATTLIST caution_to_take substance (   LIST 2   ) #REQUIRED>
<!ELEMENT budget EMPTY>
<!ATTLIST budget price CDATA #REQUIRED>
<!-- for Pharmacy Service -->
<!ELEMENT taken_drug EMPTY>
<!ATTLIST taken_drug name (          LIST 3          ) #REQUIRED>
<!ELEMENT eaten_food EMPTY>
<!ATTLIST eaten_food substance (       LIST 2       ) #REQUIRED>
```

図 A.2: 個人情報開示メッセージの DTD

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- Document Root -->
<!ELEMENT pi_usage_log (pi_owner, requestor, pi_usage_policy,  log)>

<!-- Document Header -->
<!ELEMENT pi_owner (dai_id)>
<!ELEMENT requestor (dai_id, name)>
<!ELEMENT name (#PCDATA)>
<!ELEMENT dai_id (#PCDATA)>

<!-- Service Info & PI Usage Policy -->
<!ELEMENT pi_usage_policy (service_type+, usage_purpose+)>
<!ELEMENT service_type EMPTY>
<!ATTLIST service_type type (restaurant|transporter|health_care|pharmacy) #REQUIRED>
<!ELEMENT usage_purpose EMPTY>
<!ATTLIST usage_purpose purpose (recommend|transport_things|transport_people) #REQUIRED>
<!-- Log -->
<!ELEMENT log (taken_drug|eaten_food)>

<!-- for Restaurant Service -->
<!ELEMENT eaten_food (dish)*>
<!ELEMENT dish (substance*,description?)>
<!ATTLIST dish name CDATA #REQUIRED>
<!ATTLIST dish price CDATA #REQUIRED>
<!ATTLIST dish calorie CDATA #REQUIRED>
<!ATTLIST dish salt CDATA #REQUIRED>
<!ATTLIST dish fat CDATA #REQUIRED>
<!ELEMENT substance EMPTY>
<!ATTLIST substance name (          LIST 2          ) #REQUIRED>
<!ELEMENT description (#PCDATA)>

<!-- for Pharmacy Service -->
<!ELEMENT taken_drug (drug)*>
<!ELEMENT drug (taboo_with*,caution_with*, description?)>
<!ATTLIST drug unique_name (          LIST 3          ) #REQUIRED>
<!ATTLIST drug display_name CDATA #REQUIRED>
<!ATTLIST drug price CDATA #REQUIRED>
<!ELEMENT taboo_with (food)*>
<!ELEMENT caution_with (food)*>
<!ELEMENT food EMPTY>
<!ATTLIST food substance (          LIST 2          ) #REQUIRED>
```

図 A.3: サービス利用ログメッセージの DTD