移動型エージェントを活用した安全な電子メニュー個人化システム

北形 元[1]　久保田 恭守[2]　高橋 秀幸[1]　笹井 一人[1]　木下 哲男[1]

概要：本稿では，電子メニューを個人化する移動型エージェントを導入し，アレルギー情報や健康状態等の個人情報をサービス提供者，すなわちレストランへ開示せずに電子メニューを個人化する，安全な電子メニュー個人化システムを提案し，その具体的なシステムについて詳述する．具体的には，個人情報をサービス提供者へ開示する代わりに，サービス提供者側が電子メニューの個人化を行うために必要な情報と手続きを移動型エージェントに格納し，この移動エージェントを個人情報を保持する個人情報管理機構に移動させ，個人情報管理機構内で個人情報を参照させる．この際，一旦個人情報管理機構に移動した移動エージェントが外部へ情報を送信したり，外部へ移動することを禁止することで，個人情報を個人情報管理機構の外へ持ち出せないようにする．個人情報を参照して個人化した電子メニューの内容は，個人情報管理機構内の監査機能を通じてのみ，サーバ側へ返信可能とする．このような仕組みにより，個人情報をサービス提供者へ開示せずに，アレルギーを含む料理や個人の嗜好を反映した，電子メニューの個人化を実現する．

1. はじめに

東日本大震災以降は，安否確認や情報配信等，災害時に求められる重要なサービスを被災地にすばやく提供する手段として，ワイヤレスメッシュネットワークの有用性が再評価されてきた [1]．しかしながら，様々な耐災害 ICT 技術と同様に，災害時のためだけにワイヤレスメッシュネットワークを導入することは，コスト面の問題から難しい．そのため，災害時だけでなく平常時にも利活用できるような，地域密着型のアプリケーションの開発が求められる．

一方で，インターネット上で提供されるオンラインショップをはじめとする様々な商用サービスにおいては，利用者の個人情報を活用し，利用者の嗜好を重視して個人毎にカスタマイズを行う個人適応が広く行われている．これらの個人化の仕組みをを地域型のアプリケーションにも活用できれば，地域に住む人々それぞれにあわせたきめの細かいサービスを実現できると期待できる．

我々はこれまで，広域サービスを対象としてサービス個人化アーキテクチャの提案を行ってきた [2], [3]．本アーキテクチャでは，個人情報を所有者の意思でが自由に操作できるよう，自宅やクラウド上に設置したサーバに格納し，サービス毎に予め定めた個人情報提供ポリシーを適用してフィルタリングを行い，必要最小限の個人情報のみをサービス提供者に提示することにより，個人の嗜好や健康状態などにあわせた個人化サービスを提供可能としている．しかしながら，フィルタリングにより必要最小限にしぼられているとはいえ，一旦サービス提供者側に渡った個人情報の二次利用や悪用をシステム的に防ぐことができないという問題があった．

そこで本稿では，移動型エージェントとサンドボックス技術を活用することで，個人情報をサービス提供側に一切渡さずに，安全にサービスの個人化を行う手法について

2. 個人情報管理に関する関連研究

現在提供されている多くの個人化サービスでは，それぞれのサービス提供者が独自に利用者情報を管理しており，それらの利用者情報が相互に運用されことはない．これを，CRM(顧客関係管理 : Customer Relationship Management) と呼ぶ．CRM は，サービス提供者 (Vendor) が消費者 (Consumer) のデータを分析し，関係をコントロールするという考え方に基づいている．一方これに対して，消費者指向の観点から VRM(業者関係管理 : Vendor Relationship Management) と呼ぶ方式が提唱されている．VRM は，消費者に関する様々な情報，すなわち個人情報を消費者自身

[1] 東北大学電気通信研究所
Research Institute of Electrical Communication, Tohoku University
[2] 東北大学大学院情報科学研究科
Graduate School of Information Sciences, Tohoku University

が保持・管理し，消費者側がサービス提供者を選択するという考え方である．VRM は CRM に比べ，複数のサービスに対し横断的に個人情報を活用することができるというメリットがある．VRM を実現するための具体的な方式として，PDS(Personal Data Store / Personal Data Service) の概念が提案されている [4], [5], [6]．PDS は，個人が自身のデータを蓄積・管理し，他者と限定的に共有して活用することを目的とした個人情報管理方式である．

PDS の考え方に基づき個人情報へのアクセスコントロールを実現する具体的なシステムとして，Higgins Project というソフトウェア開発プロジェクトが推進されている [7]．Higgins Project では，複数のサービス提供者が持つ個人情報を一括管理する Personal Data Service のアーキテクチャを提案しており，各サービスに登録された個人情報を部品として取り込み，これを改めて別のサービスやユーザに公開することができる．これらの個人情報の取り込みや公開は，利用者がコントロールすることが可能である．しかしながら，Higgins Project における Personal Data Service のアーキテクチャは，VRM の実現という点では問題無いが，個人情報はサービス提供者に渡されるため，プライバシーに関わる機微な情報を扱う際に注意が必要となる．

このような，プライバシーに関わる個人情報の安全な利活用を目的としたアプリケーションよりのシステムとして，サンドボックス型のプラットフォームが提案されている [8]．このプラットフォームでは，個人情報の「収集」「集計」「画面生成」処理を分離し，「画面生成」処理を利用者端末上のサンドボックス内で実行することにより，利用者端末に保持されている個人情報を活用しながら，個人化したサービスを提供することが可能である．しかしながら，本プラットフォームの仕組み上，利用者が個人情報を保持した端末を携帯する必要があり，画面表示も携帯した端末内でしか行えないという制約がある．

3. 先行研究：開放型情報パーソナライズ手法

我々の先行研究として，利用者が外出した先々で個人化されたサービスを受けるためのアーキテクチャとして，Socio-familiar Personalized Service （以降，S-P サービスと略記）を提案してきた [2], [3]．S-P サービスの具体例としては，下記のようなサービスが想定されている．

- 利用者がレストランにおいて料理を注文する際に，利用者のアレルギーや高血圧など，公開するのが躊躇されるような，しかしながらメニューの選択に不可欠な個人情報が，レストランに設置された情報端末からメニューシステムに伝達され，利用客の健康状態に応じたメニューを提示する．
- 同様に，タクシーに乗って「自宅まで」と伝えるだけで，自宅の住所がタクシーのナビに自動的に伝達され，細かい経路を説明せずとも自宅に帰宅できる．

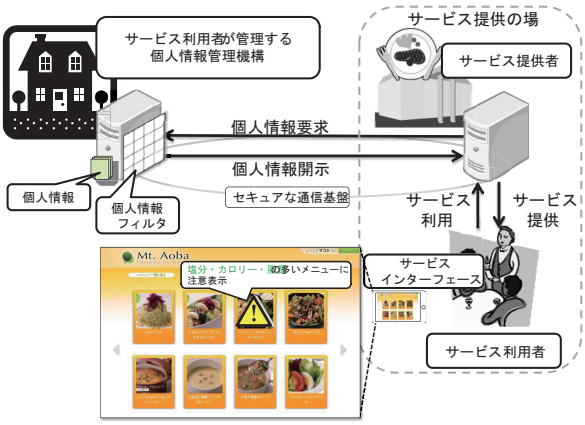

図 1 S-P サービスの概念に基づく開放型の情報パーソナライズ手法の概要

- 同様に，薬局で薬を購入する際に，既に服用している他の薬と併飲しても問題が無い安全な薬だけを選んでくれる．

図 1 に，S-P サービスの概念に基づく具体的な個人化サービスの仕組みとして，開放型の情報パーソナライズ手法の概要を示す．この手法では，利用者がレストランや薬局等のサービス提供の場でサービスを受ける際に，サービス提供者が利用者の個人情報管理機構へ個人情報の開示を要求し，サービスの業種に応じた必要最小限の個人情報のみがフィルタリングされ，サービス提供者に提供される．これにより，利用者は基盤個人情報を携帯せずとも，個人化されたサービスを享受することが可能となる．この特徴は，前述したサンドボックス型のプラットフォーム [8] が持つ，個人情報を携帯しなくてはならないという制約を解消するものである．しかしながら，必要最小限ではあるが，個人情報の一部がサービス提供者側に伝達されてしまうため，サービス提供者側による個人情報の漏えいや不正利用をシステム的に防ぐことはできないという問題がある．

4. 移動型エージェントによる安全な電子メニュー個人化システム

前述したサンドボックス型のプラットフォームと開放型の情報パーソナライズ手法両者の問題を解決するためには，次の (1)(2) の 2 つの条件，すなわち (1) 個人情報を個人が携帯する端末やデバイスに保持せず，かつ (2) 個人情報をサービス提供者側に渡さずにサービスを個人化するという条件を同時に満足する必要がある．そこで本稿では，レストランの電子メニューを対象に，移動型エージェントを活用した安全なサービス個人化システムを提案する．

図 2 に，移動型エージェントを活用した安全な電子メニュー個人化システムの概要概要を示す．本システムは，サービス提供者側が電子メニューの個人化を行うために必要な情報と手続きを移動型エージェントに格納し，この移

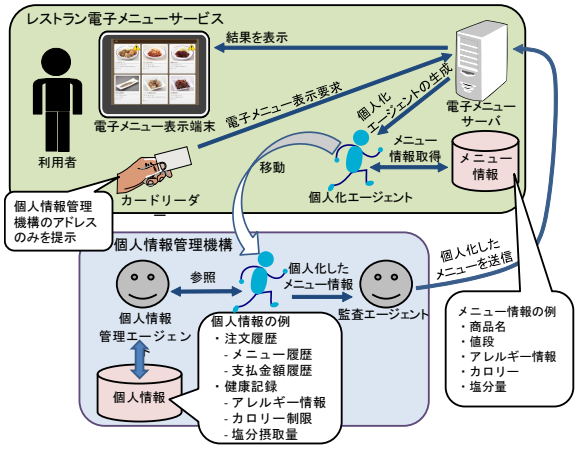

図 2 移動型エージェントを活用した安全な電子メニュー個人化システムの概要

動エージェントを個人情報を保持する個人情報管理機構に移動させ，個人情報管理機構内で個人情報を参照させる．この際，一旦個人情報管理機構に移動した移動エージェントが外部へ情報を送信したり，外部へ移動することを禁止することで，個人情報を個人情報管理機構の外へ持ち出せないようにする．個人情報を参照して個人化した電子メニューの内容は，個人情報管理機構内の監査機能を通じてのみ，サーバ側へ返信可能とする．このような仕組みにより，個人情報をサービス提供者へ開示せずに，アレルギーを含む料理や個人の嗜好を反映した，電子メニューの個人化を実現する．本システムの詳細な動作を下記に示す．

(1) 利用者がレストランに設置された電子メニュー表示端末にアクセスする．この際利用者は，IC カード等により，個人情報管理機構のアドレスを電子メニューシステムに与える．

(2) 利用者の個人情報管理機構のアドレスを取得した電子メニューサーバは，レストランのメニューを個人化するためのメニューデータと手続きを保持した移動型エージェント（以降，個人化エージェントと表記）を生成し，個人情報管理機構に移動させる．

(3) 個人情報管理機構に移動した個人化エージェントは，個人情報が格納されたデータベース (DB) にアクセスし，サービス提供に必要なデータのカスタマイズを実行する．この際，個人情報管理機構により個人化エージェントによる外部との通信，および外部への移動を禁止し，サンドボックス化することで，個人情報が外部に送信されることを防ぐ．

(4) 個人化エージェントがカスタマイズしたメニューデータを，監査エージェント経由で間接的に電子メニューサーバへ返送する．この際，監査エージェントにより，返信されるデータに不正に個人情報が含まれていないかをチェックする．

(5) カスタマイズされたメニューデータを受け取った電子メニューサーバは，電子メニュー表示端末にメニューを表示する．

5. プロトタイプシステムの設計と実装

5.1 マルチエージェントによる設計と実装

前述の電子メニュー個人化システムの有効性を検証するため，プロトタイプシステムの設計と実装を行った．以下に，各エージェントの役割と動作を示す．

MenuManager レストラン内のメニュー情報を保持し，下記の MobileAgent の生成，および利用者へ電子メニューを提示する．

MobileAgent MenuManager からレストランのメニュー情報とそれを個人化するための手続を持ち，電子メニューサーバから個人情報管理機構側へ移動する．移動後に個人情報を参照し，アレルギー情報を元にメニューデータを個人化する．

RFIDAgent 利用者の RFID を読み取り，個人情報管理機構のアドレスを Menu Manager に通知する．

DatabaseManager 個人情報が格納されたデータベース（DB）を管理し，MobileAgent からのアクセス要求に従い個人情報を開示する．

Audit MobileAgent がサービス提供側へ返信するデータを監査し，MenuManager へ返信する．

プロトタイプシステムの実装においては，エージェント環境として，Java で実装されている IDEA v1.3.1(DASH v1.9.7h1)[9] をベースに，独自にエージェントワークプレイスのサンドボックス化のための機能を追加した．具体的には，Java の PermissionCollection クラスを使用し，外部から移動してきたエージェントのスレッドに対して，通信やローカルリソースへのアクセスを禁止する仕組みを追加した．

図 3 に，プロトタイプシステムの全体図を示す．図の左側がレストランに設置される電子メニュー表示端末であり，右奥が個人情報管理機構である．図 3 に，電子メニュー表示端末を示す．

5.2 動作実験

図 5 に，プロトタイプシステムを用いた動作実験の画面を示す．図の上段は個人化する前のメニューであり，左下が小麦アレルギーを持つ利用者が使用した際の結果，右下が同様に鶏アレルギーを持つ利用者が利用した際の結果である．図から分かる通り，個人化により利用者の持つアレルギーに該当する料理に注意マークが付与され，誤ってアレルゲンを含むメニューを選ぶリスクが軽減されることが確認できた．

図 3 実装したプロトタイプシステムの全体図

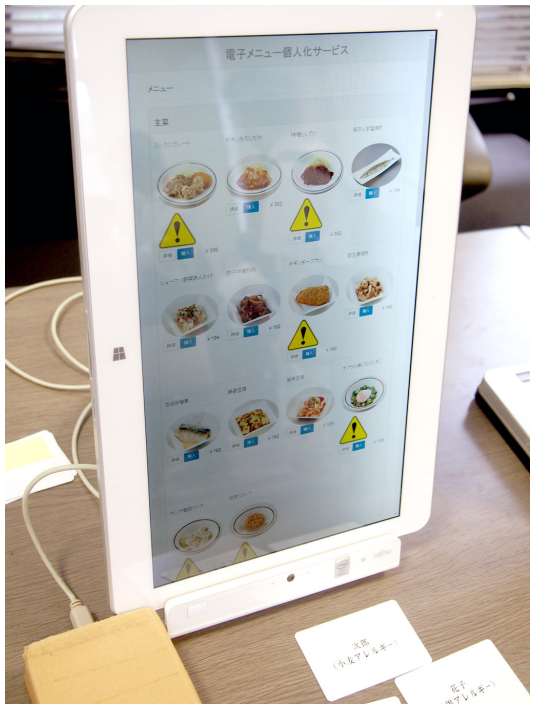

図 4 電子メニュー表示端末

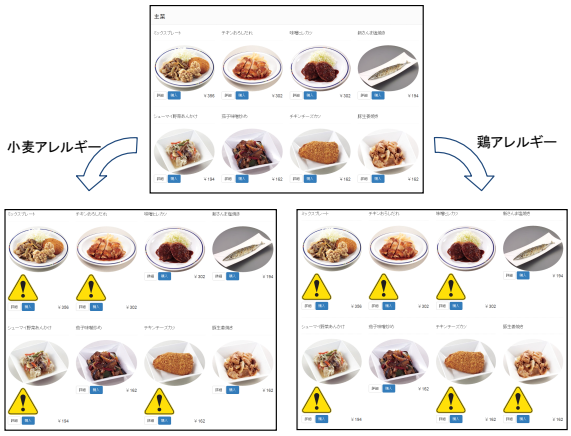

図 5 アレルギー情報を考慮し個人化された電子メニューの出力

6. おわりに

本稿では，電子メニューを個人化する移動型エージェントを活用し，アレルギー情報等の個人情報をサービス提供者，すなわちレストランへ開示せずに電子メニューを個人化する，安全な電子メニュー個人化システムを提案し，その具体的なシステムについて述べた．さらに，実装したプロトタイプシステムを用いた動作実験を通じ，提案システムの有効性を示した．今後は，メッシュ型ワイヤレスネットワークのプラットフォームを用いてより大規模な実験を行い，提案システムの有効性を評価する予定である．

謝辞 本研究成果は，独立行政法人情報通信研究機構（NICT）の委託研究「メッシュ型地域ネットワークのプラットフォーム技術の研究開発」により得られたものである．

参考文献

[1] Inoue, M., Ohnishi, M., Peng, C., Li, R. and Owada, Y.: NerveNet: A Regional Platform Network for Context-Aware Services with Sensors and Actuators, *IEICE TRANSACTIONS on Communications*, Vol. E94-B, No. 3, pp. 618–629 (2011).

[2] 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，電気情報通信学会論文誌 B，Vol. J94-B, No. 4, pp. 492–502 (2011).

[3] 半井明大，大澤由憲， 今村理，武田敦志， 北形元，ChakrabortyDebasish，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，全国大会講演論文集，Vol. 2011, No. 1, pp. 389–391（オンライン），入手先 ⟨http://ci.nii.ac.jp/naid/110008601227/⟩ (2011).

[4] Mitchell, A.: *Right Side Up: Building Brands in the Age of the Organized Consumer*, Harper Collins Business (2001).

[5] 橋田浩一：分散 PDS による個人データの自己管理，人工知能学会誌， Vol. 28, No. 6, pp. 872–878 (2013).

[6] Kirkham, T., sandra winfield, Ravet, S. and Kellomaki, S.: The Personal Data Store Approach to Personal Data Security, *IEEE Security & Privacy*, Vol. 11, No. 5, pp. 12–19 (online), DOI: http://doi.ieeecomputersociety.org/10.1109/MSP.2012.137 (2012).

[7] Eclipse Foundation: Higgins Project (2004).

[8] 知洋井上，浩之前大道，章博筒井，育生依田，誠 鈴木，博之森川：パーソナルデータの安全な利活用のためのサンドボックス型分散プラットフォームの設計，情報処理学会研究報告. UBI, [ユビキタスコンピューティングシステム]， Vol. 2014, No. 51, pp. 1–6（オンライン），入手先 ⟨http://ci.nii.ac.jp/naid/110009676813/⟩ (2014).

[9] Kinoshita lab: IDEA/DASH Tutorial, , available from ⟨http://www.k.riec.tohoku.ac.jp/idea/index.html⟩ (accessed 2016-08-04).