

## サンドボックス環境を用いた移動型エージェントによる 安全なサービス個人化手法

久保田 恭守<sup>†</sup> 北形 元<sup>‡</sup> 高橋 秀幸<sup>‡</sup> 笹井 一人<sup>‡</sup> 木下 哲男<sup>‡</sup>  
 東北大学 情報科学研究科<sup>†</sup> 東北大学 電気通信研究所<sup>‡</sup>

### 1 はじめに

ICT サービスの普及に伴い、サービスを個人化する技術が活用されている。利用者は個人情報をサービス提供者に提示して個人化したサービスを得られるが、提示した個人情報が不正に二次利用される危険から、利用者は安心してサービス提供者に個人情報を提示できない。そこで本稿では、個人情報をサービス提供者に渡さずにサービスの個人化を行うため、サンドボックス型エージェント動作環境を導入した、移動型エージェントによる安全なサービス個人化手法を提案し、プロトタイプシステムの設計と実装を行う。

### 2 関連研究

現在、利用者の個人情報はサービス提供者が管理し、利用者に個人化サービスを提供する機会が多い。しかし、一般にサービス提供者が管理する個人情報は、利用者が直接変更や取消などの操作ができないという問題がある。そこで、個人情報を利用者が管理しサービス提供者に提示することで、安全なサービスを実現するための研究が行われている。Sharifi らは、利用者が直接制御可能な個人情報を、匿名化によって保護しているが、匿名化により個人情報の利用価値は低下してしまう [1]。Jong らは、利用者の携帯端末に蓄積した個人情報を利用し、個人情報を端末外に出さずにサービスの推薦を行う手法を提案している [2]。しかし、携帯端末の紛失時に個人情報が漏洩してしまう可能性がある。

### 3 移動エージェントによるサービス個人化手法の提案

#### 3.1 移動エージェントによるサービス個人化

本稿では、外部への通信を制限したエージェント動作環境に個人情報を保持し、その中にサービスを個人化するエージェントを移動させ、個人情報を局所的に参照さ

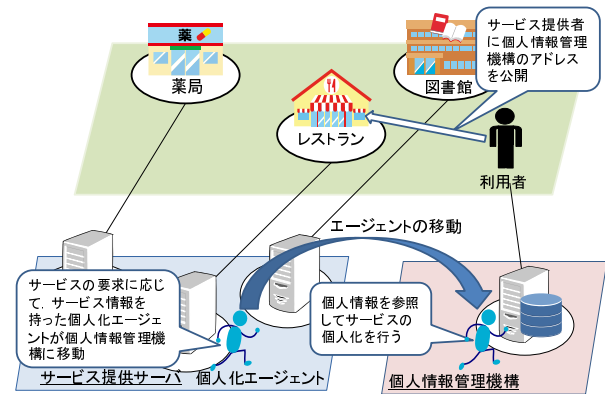


図1 移動エージェントによるサービス個人化手法の概要

せることで、安全にサービスを個人化する手法を提案する。図1に提案手法の概要を示す。ネットワーク上には個人情報管理機構とサービス提供サーバを設置する。個人情報管理機構は利用者自身が管理し、第三者による個人情報の操作はできない。個人情報管理機構に蓄積されている個人情報は、内部でのみ参照できる。利用者は、サービス提供者に個人情報管理機構のアドレスのみを提示し、サービス提供者は個人情報管理機構にサービスの情報を持った個人化エージェントを移動させる。移動した個人化エージェントは個人情報を参照してサービスの情報を個人化しサービス提供者に返信する。これにより、利用者の個人情報をサービス提供者に提示せずにサービスを個人化できる。

#### 3.2 サンドボックス型エージェント動作環境

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を参照しているため、不正に移動や通信することで利用者の個人情報が漏洩する危険がある。そこで、サンドボックス型のエージェント動作環境を導入し、個人化エージェントの移動や通信による個人情報の漏洩を防ぐ。図2にサンドボックス型エージェント動作環境の概要を示す。サンドボックス型エージェント動作環境には、利用者の個人情報を提示する個人情報管理エージェントと、個人化したサービス情報を監査する監査機能を設置する。サービス提供サーバから移動してきた個人化エージェントは、利用者に提示するサービス情報と、サービス情報を個人化する手続きを所持しており、個人情報管理エージェントを通して利用者の個人情報の参照を行い、手続きに従ってサービス情報を個人化する。個

Secure Service Personalization Method using Mobile Agent with Sandbok Place.

<sup>†</sup> Yasumori Kubota. Graduate School of Information Sciences Tohoku University.

<sup>‡</sup> Gen Kitagata, Hideyuki Takahashi, Kazuto Sasai, Tetsuo Kinoshita. Research Institute of Electrical Communication Tohoku University.

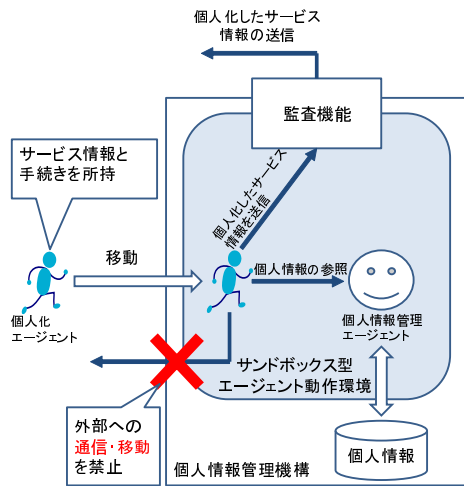


図2 サンドボックス型エージェント動作環境

個人化エージェントは、サンドボックスにより移動や通信が禁止されているため、個人情報管理機構外への個人情報の流出を防ぐことができる。また、監査機能が個人化したサービス情報を監査することで、個人化したサービス情報をサービス提供サーバへ安全に送信できる。

#### 4 設計と実装

レストランの電子メニューサービスを例に、プロトタイプシステムの設計・実装を行った。プロトタイプシステムの概要を図3に示す。プロトタイプシステムは、レストランの電子メニューサービスと、個人情報管理機構で構成されている。利用者は個人情報管理機構のアドレスが記録されたICカードをカードリーダーにかざす。電子メニューサーバは、メニュー情報と手続きを所持した個人化エージェントを、個人情報管理機構へ移動させ、個人情報管理エージェントから個人情報を参照させて、手続きに従ってメニュー情報を個人化する。個人化したメニュー情報は、監査エージェントが監査し電子メニューサーバに送信され、電子メニュー表示端末に結果が表示される。

実装したプロトタイプシステムを利用して、利用者のアレルギー情報を活用した電子メニューの個人化実験を行った。メニュー情報には料理名とアレルギー項目、カロリー、塩分、料金の情報が含まれており、手続きには利用者のアレルギー情報を活用して、アレルギーが含まれないメニューを抽出する処理が記述されている。図4に個人化されたメニューの出力結果を示す。利用者のアレルギー情報が活用され、アレルギーを含んだメニューに警告が表示されていることがわかる。

#### 5 おわりに

本稿では、サンドボックス型エージェント動作環境を導入した、移動エージェントによる安全なサービスの個

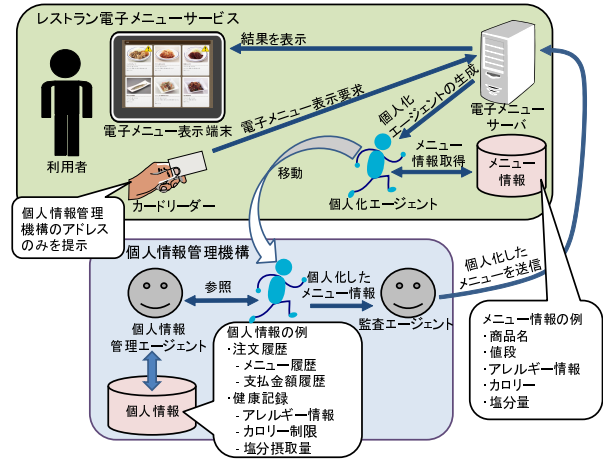


図3 電子メニューサービスを例にしたプロトタイプシステム

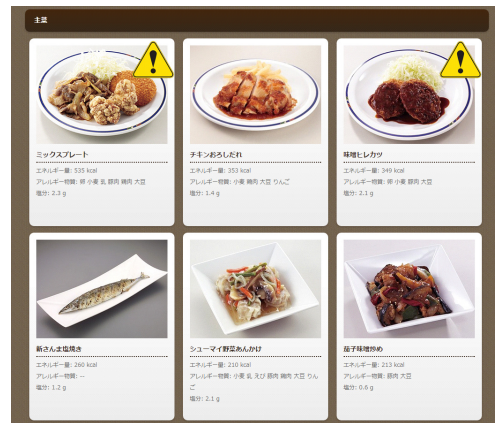


図4 アレルギー情報を用いて個人化したメニュー

人化手法を提案し、プロトタイプシステムの設計と実装を行った。

#### 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] Sharifi, L, Beisafar, M.H. User-side personalization considering privacy preserving in cloud systems. In *Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on*, pp. 797-802. IEEE, 2013.

[2] JongWoo Ha, Jung-Hyun Lee, and Sangkeun Lee. *EPE: An Embedded Personalization Engine for Mobile Users*, Vol. 18. In *Internet Computing*, IEEE, 2013.