移動エージェントとサンドボックスによる安全なサービス個人化手法

久保田 恭守[1,a)]　北形 元[1,2,b)]　高橋 秀幸[1,2,c)]　笹井 一人[1,2,d)]　木下 哲男[1,2,e)]

概要：本稿では，安全なパーソナルデータの活用技術として，サンドボックス型のエージェント動作環境を用いた，移動エージェントによるサービスの個人化手法について提案する．パーソナルデータは，サービスのパーソナライズ等への活用が期待されているが，一方でプライバシーの問題があり，パーソナルデータによる個人の特定や，個人情報の流出，不正な二次利用といったリスクが存在する．そこで，利用者が安全にパーソナルデータを活用するために，安全性の高いパーソナルデータの活用方法が求められている．そこで本稿では，個人の管理下にあるサーバ上にサンドボックス型のエージェント動作環境を設置し，その内部にサービス事業者が用意した移動エージェントを移動させることで，サンドボックス動作環境内で局所的にパーソナルデータを参照し，サービスの個人化を行う仕組みを提案する．本稿ではプロトタイプシステムを用いた実験を行い，その有効性を示す．

1. はじめに

ICT サービスの発展に伴い，利用者が容易にパーソナルデータと呼ばれる情報を生成できるようになった．パーソナルデータは，パーソナライズドサービスやデータ解析の分野での利活用が期待されている [1]．とりわけパーソナライズドサービスでは，情報の多様化や，情報量の増大化などから，利用者が手作業で目当ての情報を見つけ出す負担が増加している．そこで，利用者のパーソナルデータを活用し，サービスを個人化することで，膨大な情報の中から利用者に適切な情報を抽出し，個人の趣味嗜好に合わせた商品の推薦や，個人のコンテキストに合わせた情報の提供を行うことができると考えられる．一方で，パーソナルデータを利活用する上で発生する重要な問題の一つに，プライバシーの問題がある．パーソナルデータには，購入履歴や Web の閲覧履歴など，それだけでは個人の特定につながりにくい情報から，氏名や住所といったそれだけで個人の特定に繋がるような，プライバシー性の高い情報まで含まれている．そのため，サービス事業者に提供した情報から個人が特定される可能性がある．加えて，悪意のあるサービス事業者や攻撃者によって，個人情報の流出や，パーソナルデータの不正な二次利用が引き起こされるリスクが存在する．こうした利用者のプライバシーに対する脅威から，利用者によるパーソナルデータの利活用が阻害されてしまい，パーソナライズにより得られる質の高いサービスや，情報を得ることが困難となる．利用者による，積極的なパーソナルデータの利活用を実現するためには，利用者のプライバシーに配慮した，安全なパーソナルデータの活用技術が必要となる．そこで本稿では，利用者の管理下にあるサーバ上にサンドボックス型のエージェント動作環境を設置し，移動エージェントによる安全なサービスの個人化手法を提案する．本稿ではプロトタイプシステムを用いた実験を行い，本手法の有効性を示す．

[1] 東北大学大学院 情報科学研究科
Graduate School of Information Sciences, Tohoku University
[2] 東北大学 電気通信研究所
Research Institute of Electrical Communications, Tohoku University
[a)] kubota@k.riec.tohoku.ac.jp
[b)] minatsu@riec.tohoku.ac.jp
[c)] hideyuki@riec.tohoku.ac.jp
[d)] kazuto@riec.tohoku.ac.jp
[e)] kino@riec.tohoku.ac.jp

2. 関連研究

2.1 パーソナルデータの管理モデル

従来のパーソナルデータの管理モデルとして，Customer Relationship Management(CRM) と呼ばれるモデルが一般的に用いられている．CRM の代表的なシステムとして，ポイントカードシステムなどが挙げられる．CRM では，サービス事業者によって利用者のパーソナルデータが管理されるため，利用者はサービス事業者が管理している自身のパーソナルデータに直接アクセスし，データを操作することができないという問題がある．また，利用者のパーソナルデータは各サービス事業者によって個別に管理されて

©2016 Information Processing Society of Japan

いるため，パーソナルデータの統括的な利用や，サービス間をまたぐような横断的な活用が難しいという問題がある．

そこで，パーソナルデータを柔軟に活用するためのモデルとして，Vender Relationship Management(VRM) というモデルが提案されている [2]．VRM では，利用者自身がパーソナルデータを管理する．VRM の利点として，パーソナルデータが利用者の管理下にあるため，利用者は各サービス事業者に，どのパーソナルデータを提供するかといった選択が行える．また，利用者のパーソナルデータは全て利用者が管理しているため，あるサービスによって生成されたパーソナルデータを，異なるサービスに提供することができ，サービス間をまたいだ，パーソナルデータの横断的な活用が可能になる．例えば，病院で処方された薬の情報を飲食店に提供することで，利用者は処方されている薬と相性の悪いメニューを知ることができる．こうした VRM に基づいたパーソナルデータの管理の仕組みとしては，Personal Data Store(PDS)[3] や，情報銀行 [4] といった研究が行われている．利用者がパーソナルデータを管理することで，パーソナルデータの活用がの幅が広がるだけでなく，サービス事業者に提供するパーソナルデータの意思決定を行うことで，プライバシー性の高い情報を提供してしまうリスクを下げることができる．しかし，一度サービス事業者に提供したパーソナルデータは，利用者の意志で削除することができないため．パーソナルデータの不正な二次利用を防ぐことはできない．

2.2 VRM に基づくパーソナルデータ活用技術

サービスに提供するパーソナルデータによる個人の特定を防ぐための技術として，匿名化技術を用いた手法が提供されている [5][6]．匿名化技術では，サービス事業者に提供するパーソナルデータに匿名化処理を施すことで，パーソナルデータの精度を下げ， 個人の特定を防ぐことができる．しかし，匿名化により，パーソナルデータの精度が下がるため，パーソナルデータの利用価値自体は低下してしまうトレードオフの問題がある．

このようなトレードオフを解消するために，パーソナルデータをサービス事業者に直接提供せずに，利用者の端末上でサービスの個人化を行う手法が提案されている [7]．この手法では，携帯端末にサービスの個人化を行うための機能を組み込むことで，端末内でパーソナルデータを活用することができ，パーソナルデータの流出を防ぐことができる．しかし，サービスの個人化を行う際には，事前に個人化を行うための機能を組み込んでおく必要があるため，新たなサービスを受けようとするたびに，機能をインストールしなければならない．また，携帯端末という計算機資源が限られた端末に個人化を行うための機構を組み込む必要があり，かつパーソナルデータを端末内に蓄積する必要があるため，計算機に対する負荷が大きいという問題もある．

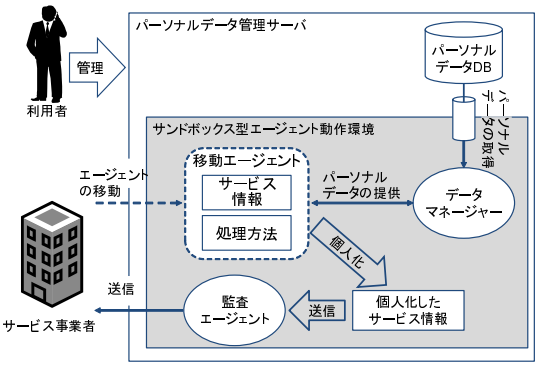


図 1: 移動エージェントによる安全なパーソナルデータ活用手法

サーバに蓄積されたパーソナルデータを安全に活用する技術としては，パーソナルデータの処理を，信頼できる第三者機関に委託する手法が提案されている [8][9]．この手法では，信頼できる第三者機関が利用者とサービス事業者の仲介を行うことで，安全にパーソナルデータを活用することができる．第三者機関は，サービス事業者に対して認証を行い，認証を受けた事業者のみ，第三者を介してパーソナルデータの参照や，個人化の処理を第三者に委託することで，安全なサービスの個人化を行うことができる．この手法の問題として，第三者機関からサービス事業者にパーソナルデータが渡されるため，パーソナルデータの流出など，CRM と同様のリスクがある．

既存研究の課題として，パーソナルデータを持ち歩かないという性質と，パーソナルデータをサービス事業者に一切渡さないという性質を両立することが難しいという点が挙げられる．

3. 提案

3.1 サンドボックス型エージェント動作環境

本稿では，パーソナルデータを利用者の管理下にあるサーバ上で活用するために，サンドボックス型エージェント動作環境を用いた，移動エージェントによる安全なサービスの個人化手法を提案する．図 1 に提案の概要図を示す．利用者はホームサーバや VPS といった計算機資源上に，パーソナルデータ管理サーバと呼ばれるサーバを設置する．利用者のパーソナルデータはサーバ内に蓄積され，利用者自身で管理することができる．また，パーソナルデータ管理サーバ内にはサンドボックス型のエージェント動作環境が設置してあり，サービスの個人化はこのサンドボックス型エージェント動作環境の内部で行われる．サンドボックス型エージェント動作環境ではサービスの個人化のために 3 つのエージェントが動作を行う．

- **移動エージェント**：
  移動エージェントは，サービス事業者側から移動して

©2016 Information Processing Society of Japan

くるエージェントである．移動エージェントはサンドボックス内でパーソナルデータを参照し，個人化したサービス情報を生成するための処理手続と，個人化を行う対象となるサービス情報を格納して，サンドボックス型エージェント動作環境に移動し，パーソナルデータを参照してサービスの個人化を行う．

- **データマネージャ**：
  データマネージャは，サンドボックス環境内からパーソナルデータ DB にアクセスすることができるエージェントである．データマネージャは，移動エージェントの要求に応じてパーソナルデータ DB にアクセスし，パーソナルデータを取得して移動エージェントに提供する．
- **監査エージェント**：
  監査エージェントは，移動エージェントが生成した個人化したサービスの情報を受け取り，サービス事業者へ送信を行う役割を持つ．監査エージェントが移動エージェントから個人化したサービスの情報を受け取ると，すぐにサービス事業者に送信せず，個人化したサービスの情報の中に利用者のプライバシー情報が含まれていないか監査を行う．監査の結果，個人化したサービス情報が安全であれば，そのまま個人化したサービスの情報をサービス事業者へ送信する．安全でないと判断した場合，個人化したサービスの情報の送信は行わず，代わりに送信できなかった理由をサービス事業者へ送信する．

各々のエージェント同士は，メッセージングによって情報の送信や共有を行うことができる．サンドボックス型エージェント動作環境では，エージェント間の情報の受け渡しは，全てメッセージングによって行われる．

サンドボックス型エージェント動作環境は，動作環境内に存在するエージェントに対して行動の権限を与えることができる．サンドボックス型動作環境による権限の付与は，環境内で生成されたエージェントだけでなく，外部から移動してきたエージェントに対しても，同じように権限の付与が行える．サンドボックス型エージェント動作環境は，利用者が管理しているエージェントに対しては全権限を与え，外部から移動してきたエージェントに対しては，以下の権限を剥奪する．

- 外部への移動
- 外部との通信

サンドボックス型エージェント動作環境による権限の剥奪によって，移動エージェントは参照したパーソナルデータを外部へ送信することや，パーソナルデータを保持したまま別の動作環境へ移動することができなくなる．これによって，移動エージェントはサンドボックス動作環境内でしかパーソナルデータを参照することができず，移動エージェントによるパーソナルデータの流出を防ぐことができる．また，移動エージェントが権限を与えられていない行動をとろうとした場合，サンドボックス型動作環境は，移動エージェントの不正な行動を監査エージェントに報告する．報告を受けた監査エージェントは，サービス事業者に対し，個人化が行えなかった理由を報告する．

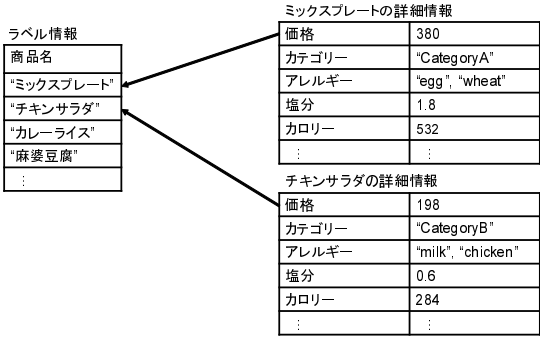


図 2: レストランを例にしたサービス情報の構造

また，移動エージェントによって生成された個人化したサービス情報は，監査エージェントによって安全性の確認を行うため，個人化したサービス情報内にプライバシー情報を紛れ込ませたとしても情報の流出を防ぐことができる．

3.2 移動エージェントによるサービスの個人化

移動エージェントは，サービスの個人化を行うために，サービスの情報と処理手続を格納して移動を行う．移動エージェントが格納するサービス情報は，利用者に個人化したサービスとして提供する前の，加工されていない状態の情報がリスト形式で記述されている．図 2 にレストランを例にしたサービス情報のデータ構造を示す．リスト内の各要素は，大きく分けでラベル情報と詳細情報にわけられる．ラベル情報は商品名のような実際に利用者に提示するための情報や，商品 ID などの識別子が記述されている．詳細情報には，パーソナルデータを利用してサービスを個人化するために必要な情報が記述されている．処理手続は，エージェントが実行できる処理のかたまりで構成されており，サービス情報とパーソナルデータが入力として与えられると，個人化されたサービス情報が生成される．処理手続は移動エージェントによって実行される．

次に，移動エージェントによるサービスの個人化の手順を示す．図 3 は，移動エージェントとデータマネージャ間のメッセージングによるデータの受け渡しの例である．利用者は，サービス事業者に対して個人化サービスの要求を行う．このとき，要求を行うために提示する情報は，移動先のサンドボックス型エージェント動作環境のアドレスを知らせるだけで良いので，サービスの要求を行うために，プライバシー性の高い情報を提示する必要はない．サービス事業者は，利用者から個人化サービスの要求を受けると，サービスの情報と，処理手続を格納した移動エージェント

©2016 Information Processing Society of Japan

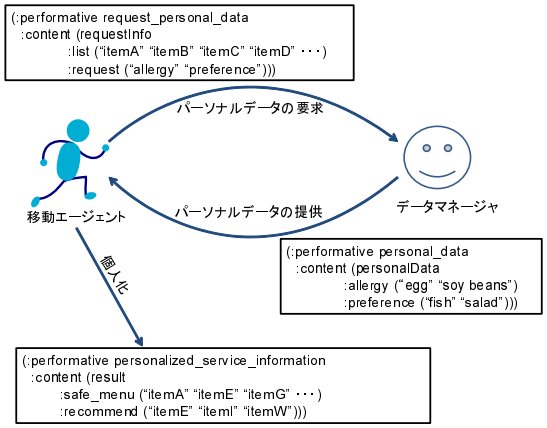


図 3: 移動エージェントとデータマネージャ間の情報の受け渡しの例

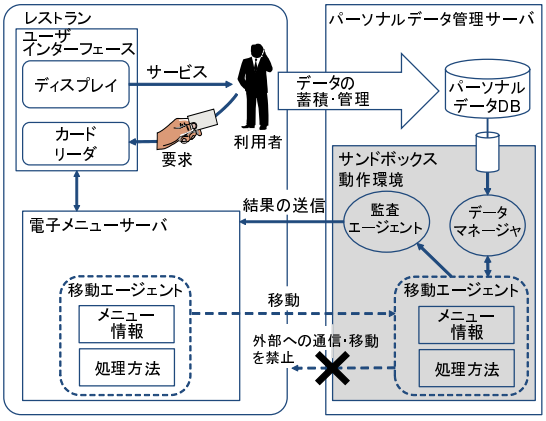


図 4: レストランを例にしたプロトタイプシステム

を，サンドボックス型の動作環境へ移動させる．サービスから移動してきた移動エージェントは，データマネージャに対してサービス情報のラベル情報のリストと，参照したいパーソナルデータを送信する．データマネージャが受け取ったサービス情報は，監査の際に利用するため，一度監査エージェントに送信する．その後，データマネージャは移動エージェントの要求に合ったパーソナルデータを DB から取得して移動エージェントに提供する．移動エージェントはパーソナルデータを受け取ると，処理手続に従ってサービス情報の個人化を行う．個人化では，サービス情報のリストから必要な要素だけを抽出し，ソートなどの処理が行われる．

3.3 監査エージェントによる安全性の検証

個人化したサービス情報は，サービス事業者に送信するため監査エージェントに渡される．監査エージェントは事前に受け取った加工前のサービス情報と，個人化されたサービス情報の比較を行い，個人化したサービス情報にプライバシー情報が含まれていないか確認する．このとき，個人化されたサービス情報の要素数が元のサービス情報よりも多い場合や，元のサービス情報に含まれていない情報が含まれている場合などには，パーソナルデータが含まれている可能性があるとして，パーソナルデータの送信は行わず，サービス事業者に個人化が行えなかった理由を報告する．

個人化したサービスの情報が監査を受けてサービス事業者へ送信されると，サービス事業者は個人化したサービスの情報を用いて利用者に個人化サービスを提供する．

4. 設計と実装

4.1 プロトタイプシステムの構成

本手法の有効性を確認するために，レストランの電子メニューサービスを例として，プロトタイプシステムの設計と実装を行った．エージェントは，エージェント開発・実行環境である IDEA[10] を用いて実装を行った．図 4 にプロトタイプシステムの概要図を示す．プロトタイプシステムは，利用者のパーソナルデータ管理サーバ，レストランに設置されたユーザインターフェース，および電子メニューサーバで構成されている．ユーザインターフェースは，利用者が電子メニューサーバに対してサービスの要求を行う他に，実際に個人化された電子メニューを確認することができる．電子メニューサーバは，利用者からサービスの要求を受けると個人化を行うための移動エージェントを生成する．生成された移動エージェントは，サービス情報としてレストランのメニュー情報と，メニュー情報を個人化するための処理手続を格納して利用者のパーソナルデータ管理サーバに移動し，3 章で説明した個人化の流れに従ってサービスの個人化を行う．

4.2 利用シナリオ

利用シナリオとして，利用者のアレルギー情報を活用した場合と，利用者の好みの情報を利用した場合を考える．

アレルギー情報を活用する場合，利用者は事前に医師からアレルギーに関する診断を受けており，診断結果に基づいたアレルギー情報がパーソナルデータ DB に保管されている．これまでは，利用者がレストランでメニューを注文するには，自身で各メニューごとにアレルギー情報を確認し，利用者の持つアレルギーが含まれているか確認する必要があった．そこで，レストランの事業者は新たに電子メニューの個人化サービスを導入し，利用者のアレルギーが含まれているメニューに対して警告を表示するサービスの提供を行っている．レストランに訪れた利用者は，どのメニューが安全に食べることができるのか知りたいので，個人化サービスを受けるために，自身のパーソナルデータ管理サーバのアドレスが記録されている IC カードを，カードリーダにかざす．カードリーダは IC カードから利用者の

©2016 Information Processing Society of Japan

図 5: アレルギー情報を用いた個人化結果

サーバのアドレスを取得し，個人化を行うための移動エージェントを生成する．移動エージェントはラベル情報としてメニュー名が，詳細情報としてアレルギー情報が記述されたメニュー情報と，メニュー情報のリストからからアレルギー情報が含まれていないメニューのみを抽出するための処理手続を持って，利用者のパーソナルデータ管理サーバへ移動する．移動エージェントはデータマネージャからアレルギー情報を受け取り，メニュー情報の詳細情報として記述されているアレルギー情報と合わせて，個人化したメニュー情報を生成する．監査エージェントは個人化したメニュー情報を確認し，生のパーソナルデータが含まれていないことを確認した後に，個人化したメニュー情報を電子メニューサーバへと送信する．図 5 に実際にサービスの個人化を行った結果を示す．個人化によって，アレルギーの含まれているメニューに対して，警告のマークが表示されていることが確認できる．

好みの情報を活用する場合，パーソナルデータとしてサーバ内に蓄積された他の飲食店での注文履歴から，利用者の好みの情報を抽出することができる．レストランでは，利用者の好みの情報を用いて，利用者が好みそうなメニューを推薦するサービスを提供しており，利用者がレストランでカードリーダに IC カードをかざすと，移動エージェントがメニュー情報と，利用者の好み情報からおすすめのメニューのみを抽出する処理手続を格納して，利用者のサンドボックス型動作環境へ移動する．移動したエージェントはデータマネージャから利用者の好みの情報を受け取り，メニュー情報の詳細情報に含まれる各メニューのジャンルを用いて，メニューのリストから該当するメニューを抽出する．また，利用者は過去にも同じレストラ

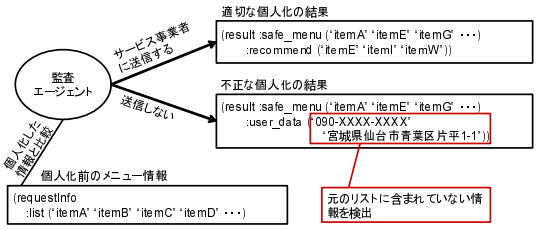


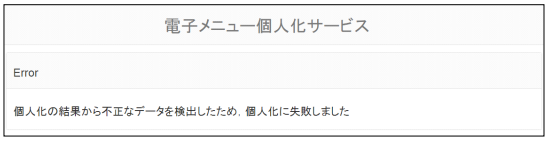
図 6: 監査エージェントによる安全性の検証

ンに訪れたことがあるため，その際の注文履歴の情報をデータマネージャから受け取ると，抽出したメニューから利用者が今まで注文した経験のないメニューを優先的に表示するように，リストの順番のソートを行う．こうして生成された個人化したメニュー情報は監査エージェントに送信さる．監査エージェントは，個人化したメニュー情報が安全だと判断し，レストランの電子メニューサーバに送信する．結果として，は利用者におすすめのメニューとして個人化したメニュー情報を提示することができる．

4.3 サンドボックス型動作環境の安全性

サンドボックス型エージェント動作環境の安全性を示すために，悪意のあるサービスが不正にパーソナルデータを取得しようとした場合の例を示す．パーソナルデータを取得する方法として，データマネージャから取得したパーソナルデータを所持したまま，移動エージェントが外部へ移動する場合と，移動エージェントが外部にパーソナルデータを送信する場合，個人化したメニュー情報にパーソナルデータを混入させた場合を考える．初めに，移動エージェントがパーソナルデータを受け取りそのまま外部へ移動する場合，移動エージェントはサンドボックス型動作環境から，外部へ移動する権限を与えられていないため，エージェントの移動はサンドボックス動作環境によって防がれる．サンドボックス型動作環境は，監査エージェントに対して不正な移動を阻止したことを報告し，監査エージェントはサービスの個人化が失敗したことをサービス事業者に

(a) 不正な移動による個人化の失敗



(b) 監査による個人化の失敗

図 7: サービスの個人化に失敗した際のメニュー画面

©2016 Information Processing Society of Japan

報告する．移動エージェントによる外部への通信も，移動の際と同様に，サンドボックス型動作環境によって通信が阻止され，監査エージェントがサービス事業者へ結果を報告する．

図 6 に，移動エージェントが個人化したメニュー情報の中にパーソナルデータを埋め込む場合の例を示す．移動エージェントは，アレルギー情報だけでなく，利用者の電話番号と住所の情報をデータマネージャに要求したとする．移動エージェントは，データマネージャから受け取った住所情報を，メニュー情報の中に追加し，住所情報が入ったメニュー情報を，監査エージェントに送信する．監査エージェントは，事前に受け取っていた個人化を行う前のメニュー情報のラベル部の情報を所持しているため，元の情報と個人化した情報を比較を行う，適切に個人化が行われていれば，個人化したメニュー情報は，元のメニュー情報でのみ構成されているが，個人情報が埋め込まれると，元のメニュー情報に無い情報が追加される．監査エージェントが監査を行った結果，元のリストに含まれていない情報が個人化したリストの中にあることを検出した．その結果，監査エージェントは個人化した情報の中にプライバシー情報が含まれている可能性があると判断し，サービス事業者には個人化した結果を送信せずに，個人化が行えなかった理由をサービス事業者へ送信する．図 7 に個人化に失敗した際の例を示す．サービスの個人化は行われず，代わりに画面上部に個人化が失敗した理由が表示されていることが確認できる．したがって，個人の管理下にあるサーバ上で，不正なパーソナルデータの流出を防ぎながら，移動エージェントによる安全なサービスの個人化が行えることを確認できた．

5. おわりに

本稿では，パーソナルデータを安全に活用するために，利用者が管理するサンドボックス型エージェント動作環境へ，サービス事業者の移動エージェントを移動させることで，外部にパーソナルデータを持ち出すことを防ぎながら，安全にサービスの個人化を行える手法を提案し，プロトタイプシステムの設計と実装を行い，その有効性を示した．

今後の課題として，移動エージェントに格納するデータサイズと，処理時間の関係を計測する予定である．利用者のサーバ内でサービスの個人化を行う場合，サービスの個人化に要する処理時間は，サービス事業者が所有しているサービス情報のデータサイズや，処理方法の設計に依存するため，データサイズが小さい場合は，処理に要する時間は少なくて済むが，データサイズが大きい場合に，処理時間の増加が懸念される．そこで，利用者の要求に対して即座に個人化したサービスを提供できるよう，様々なデータサイズに対して，どの程度の処理時間が必要になるかといった定量的な評価を行う必要がある．

また，個人化したサービス情報の監査を行う際に，不正検出が困難な例として，ステガノグラフィと呼ばれる手法を用いたデータの隠蔽が挙げられる．ステガノグラフィとは，例として，文章の各行の先頭の文字だけを取り出すと別の文章が現れる，といったもので，目的の個人情報を埋め込むために，サービス情報に工夫を加えることでデータの隠蔽が可能となる．したがって，ステガノグラフィが用いられると，加工前のサービスの情報と，個人化したサービスの情報の比較だけでは，パーソナルデータの埋め込みの検出が困難になると考えられる．そのため，監査を行う際に，個人化したサービス情報の中にプライバシー情報が含まれているか判別しにくい状態であっても，安全性を適切に評価できるよう，監査エージェントの機能について議論を行う必要がある．

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] 高度情報通信ネットワーク社会推進戦略本部：パーソナルデータの利活用に関する制度改正大綱.
[2] Berkman Center for Internet and Society: Project VRM, Harvard University (online), available from ⟨http://projectvrm.org/⟩ (accessed 2016-06-21).
[3] 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. 26, No. 6, pp. 872–878 (2013).
[4] 柴崎亮介：情報銀行コンソーシアム，，入手先 ⟨http://www.information-bank.net/⟩（参照 2016-06-21）.
[5] L. Sharifi and M.H. Beisafar: User-side Personalization Considering Privacy Preserving in Cloud Systems, *2013 27th International Conference on Advanced Information Networking and Applications Workshops*, pp. 797–802.
[6] 浜本一知，田原康之，大須賀昭彦：ユーザ背景情報及びコミュニティ状況を考慮した匿名度制御によるプライバシ保護エージェントの提案，電子通信学会論文誌 D，Vol. 94, No. 11, pp. 1812–1824 (2011).
[7] JongWoo Ha, Jung-Hyun Lee and SangKeun Lee: EPE: An Embedded Personalization Engine for Mobile Users, *IEEE Ingernet Computing*, Vol. 18, No. 1, pp. 30–37 (2013).
[8] 井上智洋，前大道浩之，筒井章博，依田育生，鈴木 誠，森田博之：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，研究報告ユビキタスコンピューティングシステム (UBI)，Vol. 41, No. 51, pp. 1–6 (2014).
[9] Moiso, C. and Minerva, R.: Towards a User-Centric Personal Data Ecosystem The Role of Individuals' Data, *2012 16th International Conference on Intelligence in Next Generation Networks(ICIN)*, pp. 202–209.
[10] 木下哲男：IDEA，，available from ⟨http://www.k.riec.tohoku.ac.jp/idea/⟩ (accessed 2016-06-22).

©2016 Information Processing Society of Japan