動的なサービス連携におけるプライバシ保護を考慮したエージェントプラットフォームの構成

An Agent Platform for Dynamic Service Interactions Considering Privacy Protection

上岡英史 Eiji KAMIOKA　山田茂樹 Shigeki YAMADA　田中聡 Satoshi TANAKA

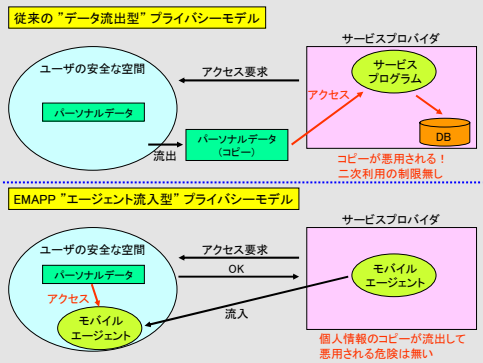
何がわかる？

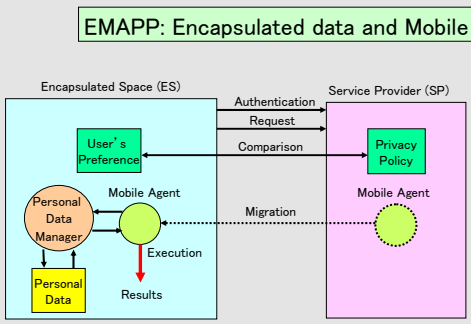
ユビキタスコンピューティング環境においては，ユーザの状況に適応したサービスを提供するため，パーソナルデータの利用が求められる．しかし，パーソナルデータはいったんユーザ領域から外に出ると，ユーザ自身はその所在を制御できなくなり，悪意のあるサービスサービスプロバイダによるパーソナルデータの二次利用によってユーザの不利益を生じる事態に発展しかねない．このような問題を避けるためには，パーソナルデータをユーザの制御範囲から外へ持ち出すことなく，サービスを利用できる環境を構築する必要がある．

どんな研究？

ユーザがパーソナルデータをサービスプロバイダ側に提供してサービスを受けるのではなく，サービスプロバイダがアプリケーションプログラムをモバイルエージェントとしてユーザ側に転送し，ユーザがパーソナルデータを管理・制御できる領域でサービスを実行することにより，パーソナルデータが漏洩することなくサービスを受けることができるエージェントプラットフォームを研究する．

基本アーキテクチャ

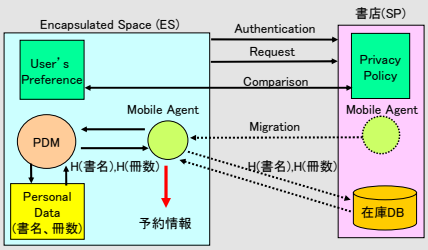




(a) Encapsulated Space (ES)
ユーザに管理された閉じられた空間で，モバイルエージェントはこの領域内でのみパーソナルデータを参照できる
(b) Personal Data Manager (PDM)
パーソナルデータを管理し，モバイルエージェントのインタラクションを制御する
(c) User Preference
パーソナルデータへのアクセスポリシを格納する

研究状況

本の予約サービス



ハッシュ化データを用いたサービス提供方法

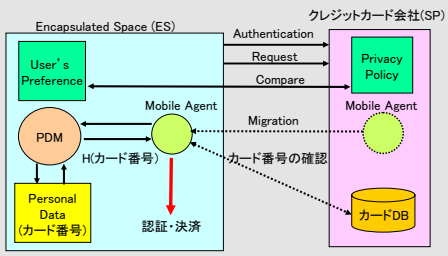
本の予約サービスの場合，モバイルエージェントで全ての本在庫データをESへ運び込むことは事実上不可能である．

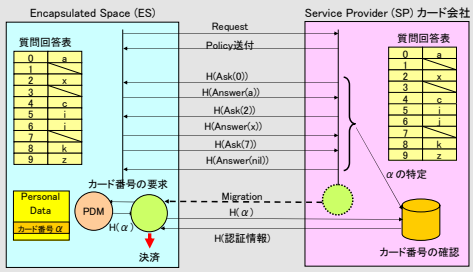
【対策】ハッシュ化データ（本の名前，冊数）値を用いて在庫検索が可能なデータベースを製作する．
【効果】ハッシュ化されたパーソナルデータが外部に持ち出されても，パーソナルデータが二次利用されることはない．

今後の検討課題

(1) ハッシュ化データのみでトランザクションを処理するサービスの具体的実現方法
(2) パーソナルデータの流出度の評価方法確立
(3) 従来型モデルとの定量的比較（処理オーバーヘッド，性能）

DB認証型サービス

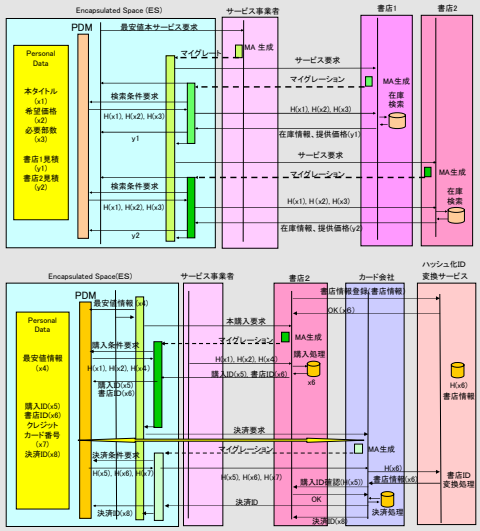




Question/Answer形式インタラクションの導入

クレジットカード決済サービスのように，サービスプロバイダのデータベース自体をモバイルエージェントでESへ運び込むことは事実上不可能である．また，クレジットカード決済サービスは，カード番号なしにはサービスできない．
【対策】
ユーザとサービスプロバイダ間でパーソナルデータ以外のデータを元にquestion/answer形式のインタラクションを行い，パーソナルデータを推定した上で，決済サービスプログラムをモバイルエージェントで運び込み，ハッシュ化されたパーソナルデータを送信して認証／決済を行う．

サービス連携シナリオ（本の最安購入サービス）～見積からカード決済まで～



ハッシュ化データ逆変換サービスの導入

ハッシュ化データ自身を用いてデータベースを構築する方法は，ひとつのサービスプロバイダ単体でのサービスであれば比較的容易であるが，いくつかのサービスプロバイダが連携するようなサービスの場合は，ハッシュ化データを逆変換してパーソナルデータを再生する必要があり，そのためには信頼された第三者機関のハッシュ化データ逆変換サービスが必要である．

NII 連絡先：上岡英史（Eiji KAMIOKA）／ 国立情報学研究所 アーキテクチャ科学研究系 助手
TEL：03-4212-2581　FAX：03-3556-1916　Email：kamioka@nii.ac.jp