利用者が主導となりプライバシ情報の開示制御が行える プライバシ情報セキュア流通基盤の実現

宮川　伸也†　西村　祥治†　森　拓也†　佐治　信之†
NEC サービスプラットフォーム研究所†

1. はじめに

近年，携帯端末や IC カード等からプライバシ情報を収集しやすくなったため，それらを活用したサービスを実現しやすくなった．例えば，携帯端末で測位される GPS 情報から目的地までの経路を検索するような位置情報を活用したサービスが増えつつある．利用者から提供される情報のプライバシ性が高いほど，個人により適したサービスを提供できる傾向にある．また，複合的なサービスの場合，複数のサブサービス間で情報が流通される場合がある．一方，プライバシ情報を提供する際，情報漏えいや不正利用によって不利益を被るかも知れないという不安が，利用者には常にある．これを解決するために，プライバシ情報セキュア流通基盤(Privacy Information Secure eXchange，以降では PISX と記す）を開発した．PISX により，サービス開発者はプライバシ情報を保護するサービスを実装でき，利用者はプライバシ情報の流通を制御することができる．本稿では，特に，利用者観点から導入した PISX の機能について述べる．PISX を利用したサービス開発については，文献[1]を参照されたい．

2. プライバシ情報セキュア流通の実現方針

プライバシ情報を広範囲に提供することに対する利用者の抵抗感を軽減するため，次の方針に基づいて PISX を実現する．

- 情報を利用者が信頼できる相手に，許可した範囲だけ開示する
- 情報の所有権は利用者にあり，常に利用者が情報を制御する

利用者は次のような操作を行えるようにする．

(a) サービスには秘匿された情報を提供し，利用者はその開示範囲を設定できるようにする．サービスの信頼度が変わったときに，直ちに開示範囲を変えられるようにする．
(b) 利用者に対して，どのサービスにどのようなプライバシ情報を開示したのかを確認できるようにする．
(c) プライバシ情報をトレースし，利用者の要求に応じて，いつでもそれ以上の流通を中止できるようにする．

サービス開発者は，悪意を持ってプライバシ情報を流出させる意図は無いことを前提とする．

3. アーキテクチャと実現機能

上記(a)～(c)を実現するため，図 1のようなアーキテクチャを設計した．

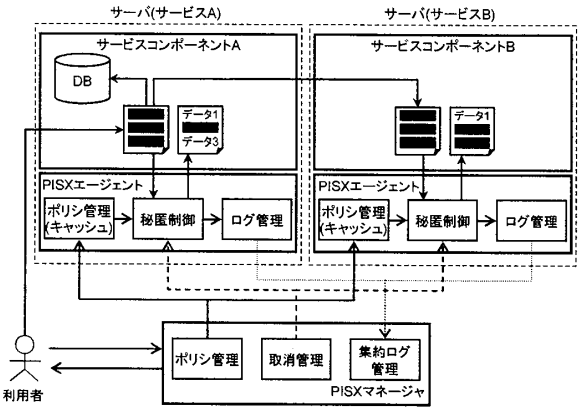


図 1 PISX アーキテクチャ

マネージャは，利用者のインタフェースであり，また，全てのエージェントを統合的に管理する．エージェントは，サービスを実装したサービスコンポーネント毎に配置される．サービスコンポーネントは，利用者から受け取ったプライバシ情報を活用してサービスを提供する．秘匿されたプライバシ情報（図 1の黒四角）を受け取り，エージェントの秘匿制御を使って情報を開示する．データベースへの保存や，他のサービスコンポーネントへの送信には，秘匿された情報を用いる．

3.1. 開示ポリシ設定・変更機能

どのような種類のプライバシ情報を誰に開示するかを利用者が設定できる開示ポリシを導入した．マネージャのポリシ管理は，開示ポリシを管理し，各エージェントのポリシ管理（キャッシュ）にコピーを配付する．変更が要求された場合，直ちにその内容を各エージェントに反映することで，常に利用者の意図を反映した開示・秘匿が行われるようにした．

Privacy Information Secure eXchange – A Platform Allows Users to Control Their Own Privacy Information,
†Shinya Miyakawa, Shoji Nishimura, Takuya Mori and Nobuyuki Saji (Service Platforms Research Laboratories, NEC Corporation)

3.2. プライバシ情報の確認機能

エージェントのログ管理は，情報が開示されたとき，いつ，誰に，どのような情報が開示されたのかをログとして記録する．ログは定期的にマネージャの集約ログ管理に集約され，利用者は参照・確認できる．

3.3. プライバシ情報の取消機能

利用者は，すでに提供したプライバシ情報を確認し，思ったよりもプライバシ性が高い等の理由により，プライバシ情報の流通を中止することができる．マネージャの取消管理は，秘匿時の対象情報の除去，秘匿済み対象情報の非開示を，各エージェントの秘匿制御に伝達する．

すでに開示したサービスに対して開示しなかったことにすることはできないが，新たに情報を開示しようとするサービスに対して効果がある．

4. モデルサービスへの適用

携帯端末で測位される GPS 情報を用いて，「近く」や「よく行く場所」のグルメ情報をお薦めするモデルサービス[2]に PISX を適用した．システムは，行動情報預かりコンポーネントと推薦コンポーネントから構成され，GPS 情報を行動情報預かりコンポーネントに保存し，GPS 情報を変換して得られるエリア情報を推薦コンポーネントに流通する．各コンポーネントには，PISX エージェントが備えられている．

GPS 情報とエリア情報には，表 1のようにプライバシレベルを付与した．自宅や勤務地について，住所を特定できる情報をレベル高，最寄りの駅やバス停を推測できる情報をレベル中，首都圏では駅が複数含まれる程度の情報をレベル低と定義した．

表 1 情報のプライバシレベル

データ種別	内容	レベル
GPS 情報	緯度・経度	高
1/4 地域メッシュ	250m 四方エリア	高
基準地域メッシュ	1km 四方エリア	中
2 倍地域メッシュ	2km 四方エリア	低

開示ポリシは，利用者にわかりやすいように 3 種類に限定し，プライバシレベル毎に推薦コンポーネントに開示可能か否かを設定できるようにした（表 2 の○と×で表記）．

表 2 ポリシ開示度による開示制御

レベル / 開示ポリシ	高	中	低
標準提供モード	○	○	○
一部提供モード	×	○	○
最小提供モード	×	×	○

提供する情報のプライバシ性が高いほど，個人の行動傾向に合う推薦が行われる．

5. 利用者によるプライバシ情報の制御

モデルサービスでは，開示ポリシの設定・変更，プライバシ情報の確認・提供取消が図 2 と図 3 のように行われる．

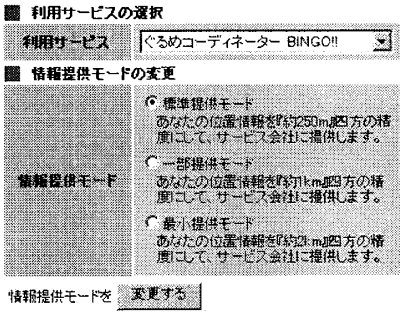
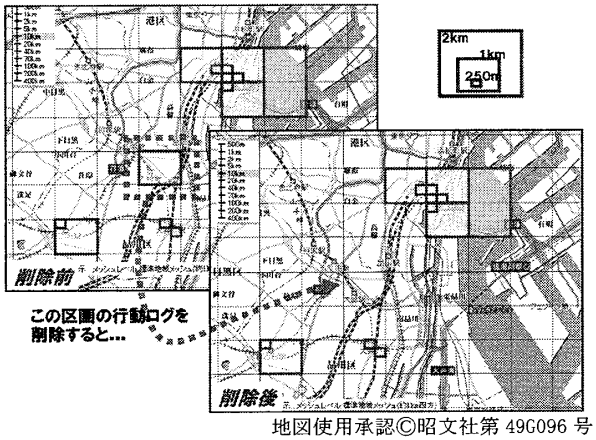


図 2 開示ポリシ設定画面



地図使用承認©昭文社第 49G096 号

図 3 プライバシ情報の確認と削除

6. おわりに

プライバシ情報を活用するサービスにおいて，利用者が安心して情報提供を行えるように，開示範囲の設定・変更，プライバシ情報の確認・提供取消が行える PISX を設計した．

PISX をモデルサービス上に実装し，利用者からプライバシ情報を制御できることを説明した．

PISX 導入によるプライバシ情報の流通効果については，今後，さらなる評価が必要である．

なお，本研究は，経済産業省「情報大航海プロジェクト」のモデルサービスとして，株式会社 NTT ドコモを中心とした「マイ・ライフ・アシストサービス」実証実験の一環として実施した．

参考文献

[1] 西村祥治 他，"プライバシ情報セキュア流通基盤におけるプライバシ情報開示制御の実現"，
第 71 回情報処理学会全国大会，5E-3(発表予定)
[2] 菅野亨太 他，"利用者状況に適した方式を推薦するマルチモード推薦システム の実現"，
第 71 回情報処理学会全国大会，2C-3(発表予定)