PREMIS: Privacy Respected Multi-user Smart-Object Environment
プライバシを考慮した複数ユーザ対応スマートオブジェクト環境

平成 20 年 1 月 30 日

1 背景

2006 年度未踏プロジェクトである “uPackage: a package to realize ubiquitous services with daily objects” において我々は，日用品に小型無線センサノードを取り付け，実世界の状況に応じたサービスを展開するための環境を提案・開発した．利用環境として，Spot & Snap インタラクションを利用した日用品とセンサノードの関連漬け手法である uAssociator や，センサ・ネットワークインフラを管理する uGateway, また，高齢者見守りサービスである uCare や忘れ物検知サービスである uReminder などのサンプルサービスも開発し，当初の目的である利用基盤の整備を達成した．しかしながら，uPackage が提供する基盤システムでは，複数のユーザが同時に利用することが考慮されていないため，プライバシ情報の漏洩やサービス管理の不便さなどの問題が発生すると考えられている．

2 目的

本プロジェクトの目的は，uPackage において考慮されなかった，複数ユーザに対応し，実利用可能なスマートオブジェクト利用環境である，PREMIS システムを構築することである．uPackage システムを複数のユーザが利用する場合，次の 2 点の問題が発生すると考えられる．

- 活動情報漏洩問題
- サービス管理問題

スマートオブジェクトの利用情報は，取り付けられた小型無線センサノードから得られるセンサデータを収集，解析することで容易に知ることが出来る．uPackage システムは，家庭やオフィスなど利用者が限られた場所での利用を想定しているため，ユーザとスマートオブジェクトの利用情報は容易に結びつけられ，プライバシ情報の漏洩につながる．また，複数のユーザが存在するため，スマートオブジェクトとスマートオブジェクトを利用したサービスに対してユーザ情報を付与し，簡便にサービスを操作できなければならない．本プロジェクトでは，uPackage プロジェクトで解決されていないこれら 2 点の問題にを解決し，実運用に耐え得るシステムの構築を目指す．

3 開発の内容

図 2 に PREMIS システムの概要を示す．uPackage システムに加えて，ユーザの活動情報を保護するための機構である PRA システムが uGateway にあたる PREMIS サーバに実装された．また，スマートオブジェクトサービス管理システムが新たに導入された．PRA システムとスマートオブジェクトサービス管理システムについてそれぞれ述べる．

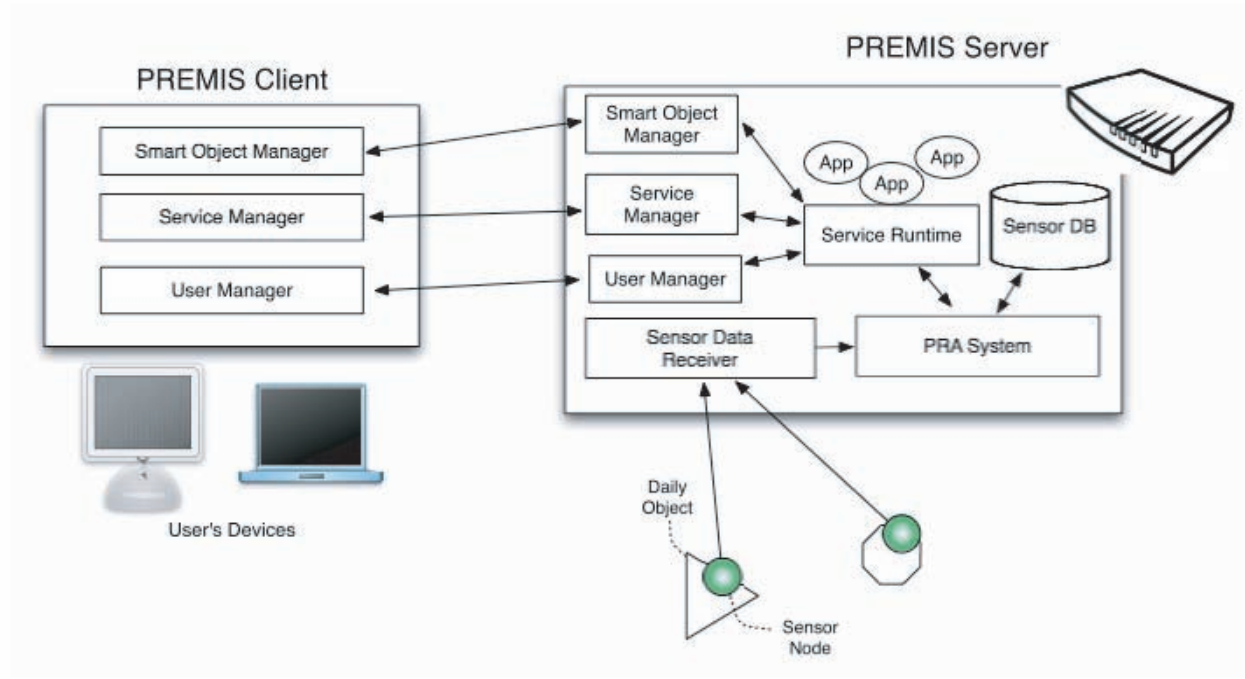

図 1: **Overall System Architecture of PREMIS**

3.1 PRA システム

PRA システムは，スマートオブジェクトから得られるセンサデータに含まれる活動情報を保護する機能を提供する．

スマートオブジェクト環境において発生し得るプライバシ漏洩とは，スマートオブジェクトから得られる活動情報と，その活動を行なっているユーザが簡単に特定できてしまうことから発生する問題である．例えば，Alice と Bob がスケジュールを共有していたとする．その場合，Bob はスマートオブジェクト環境にいなくても，Alice の詳細な活動状況をスケジュール情報とセンサデータを照らし合わせ，解析することで簡単に得ることが出来る．

この問題を解決するために PRA システムでは，センサデータに対する**所有権**と**アクセスコントロール**を規定する．所有権はスマートオブジェクトを利用したユーザに対して与えられる．スマートオブジェクトの利用の検知は，ユーザがスマートオブジェクト環境内に存在していることで判別する．言い替えると，ユーザがスマートオブジェクト環境内に存在している場合，その環境内に存在するスマートオブジェクトから得られるセンサデータの所有権は，そのユーザに対して与えられると言うことである．複数のユーザがいる場合は，センサデータは複数のユーザによって所有されることになる．ユーザが環境内にいるかどうかの判別は，ユーザが持つ RU バッチによって行なう．センサデータに対するアクセスコントロールは，センサデータの公開粒度を変更することで実現する．例えば，0 〜 255 までの値で表現されるセンサデータがある時，公開粒度を落すとは，0 〜 10 という値にセンサデータを変換することを意味する．このアクセスコントロールは，スマートオブジェクト環境外にいるユーザに対して適用される．つまり，Alice と Bob の例では Bob がセンサデータを閲覧しようとする際に適用される．アクセスコントロールの粒度と適用対象は，XML によるポリシ記述言語によって表現され，PRA システムに適用される．

図 2 に PRA システムのアーキテクチャを示す．PRA システムは，図 **??** 中の “PRA system” 部に実装されている機能である．

PRA システムをスマートオブジェクトサービス環境に適用することで，ユーザは実空間を共有していないユーザに対して活動情報の公開粒度をコントロールできるようになる．つまり，センサデータに対するアクセスコントロールが可能となり，プライバシ保護につながると考えられる．

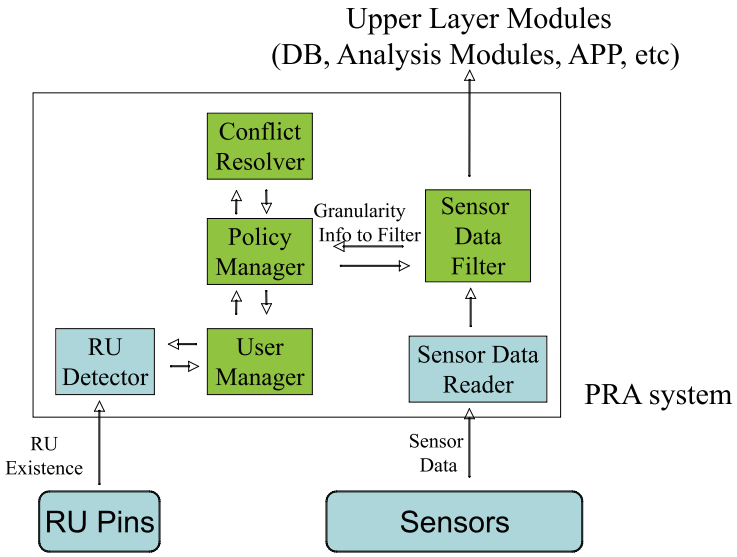

図 2: **PRA システムアーキテクチャ**

3.2 スマートオブジェクトサービス管理システム

スマートオブジェクトサービスを容易に管理し，さらにサービス記述能力を高めるため，サービスマネージメントソフトウェアとサービス記述言語である SOSDL (Smart Object Service Description Language) を設計・開発した．

はじめに、SOSDL について述べる。uPackage プロジェクトでは、ユーザは uServiceMaker を利用することでシンプルなサービスが構築できた。しかしながら、uServiceMaker は単純な if-then ルールしかサポートしていなかったため、より複雑なサービスを構築するためには C や Java などの汎用的プログラミング言語を用いるしかなかった。現状のコンテキストアウェアサービスの実現手法についても、単純な手法（if-then ルール）と複雑な手法（汎用言語によるプログラミングやベイジアンネットワークを利用した学習）の 2 極化が起こっている。SOSDL は，従来の複雑な手法より簡易に利用可能であるが，従来の単純な手法と比べ記述力の高いサービス記述言語とその動作環境の構築を目的とする．SOSDL は XML 形式で記述されており、スマートオブジェクトのイベントの時間的関係性を表現できる。また、スマートオブジェクトとイベントの分離が可能となっており、ユーザの環境に柔軟に対応できる。すなわち、SOSDL はアプリケーションに対し、（１）シンプルさを持ち（２）高い表現能力を有し（３）再利用が可能な環境を提供する。

次に，サービスマネージメントソフトウェアについて述べる．我々は PREMIS サーバ側で動作するソフトウェアと，クライアント側で動作する PREMIS Manager という 2 つのソフトウェアを開発した．サーバソフトウェアは Smart Object Image と SOSDL で記述されたサービスを管理する。また、SOSDL の XML を解釈し，サービスを動作させるランタイムが動作する。センサデータは PRA システムから取得し（すなわちプライバシ保護機能を有す）、もしあるスマートオブジェクトのイベントが発火すると、それに対応するアクションを行う。PREMIS Manager は、PREMIS サーバと通信を行い、ユーザがスマートオブジェクト及びアプリケーションを容易に管理するためのソフトウェアである。uPackage システムでは，サービスを利用するまでに複数のソフトウェアを利用しなければならなかったが，PREMIS Manager を利用することで，ログイン（ユーザ認証）機能、スマートオブジェクト管理機能、サービスマネージャの３つの機能を一度に利用可能であり，タスクの簡易化が可能である．図 3 にスマートオブジェクト管理画面の様子を示す．

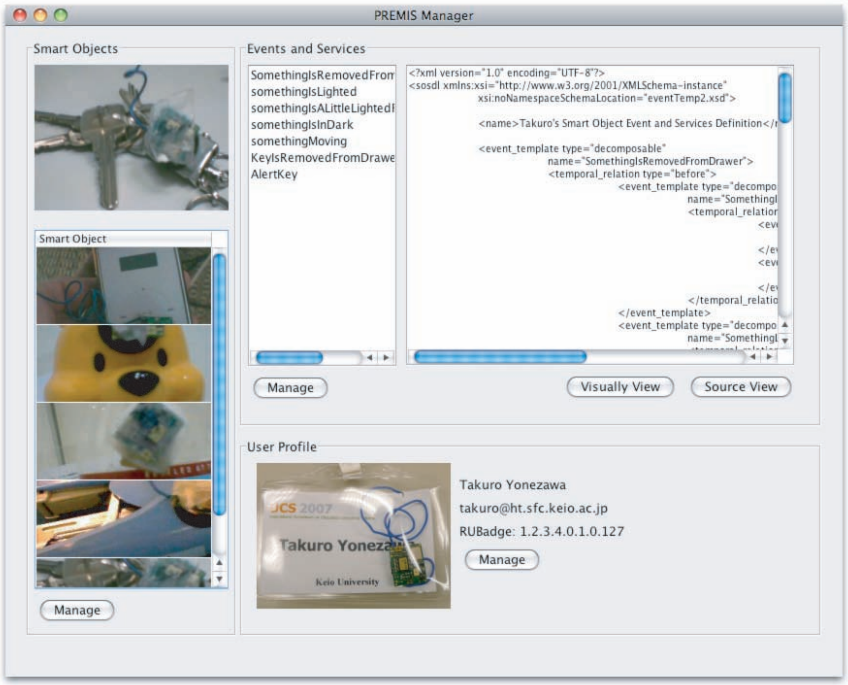

図 3: **Main Window of PREMIS Manager**

4　従来の技術との相違

既存のユビキタス環境におけるプライバシ保護技術は，コンテキスト解析技術を利用し，センサデータに含まれる活動情報を抽出し，その抽出した活動情報に対するアクセスコントロールをユーザに対して提供する仕組みとなっている．しかし，既存の手法では対象となる活動情報のみの保護となり，システムの可用性が低くなる欠点がある．本手法では，さまざまなコンテキスト解析手法やサービスを PRA システムのみで扱えるため，可用性が高いと言える．また，センサデータを保護対象としていることから，上位に位置するサービスやアプリケーションによる情報漏洩の危険性も既存研究と比べると低くなる利点がある．

5　期待される効果

本プロジェクトでは，uPackage プロジェクトにおいて実現されたスマートオブジェクト環境を複数ユーザ対応とするため，ユーザの活動情報を保護するための PRA システムと，サービス管理機能を有する SOSDL システムを追加した．

PRA システムは，スマートオブジェクトサービスのみならず，全てのセンサデータを利用したシステムに対して，ユーザの意図しない活動情報の漏洩を防ぐ効果を提供する．近年，本プロジェクトと同様に物流管理システムの構築や，介護支援システム，ミーティング支援サービスなど，センサデータを活用したサービス展開が試みられているが，ヨーロッパにおける RFID を装着した洋服の不買運動に見られるように，センサを活用したサービスの普及をプライバシ情報の漏洩に対する不安が足止めしている．PRA システムによってプライバシ情報の漏洩を防止できることは，センサデータに対する不安を軽減し，サービスの普及を促進する効果が期待できると考えられる．

6　普及の見通し

本プロジェクトでは，スマートオブジェクトサービスを実運用する際に必須となる，プライバシ保護機能と，スマートオブジェクトサービスの管理機能の開発に注力したが，家庭内での実運用を考える時，PREMIS サーバの小型・省電力化，センサノードのさらなる小型化，ソフトウェアの最適化などを行なう必要がある．ソフトウェアの最適化に関しては，今後我々が行なっていく予定であるが，PREMIS サーバの小型・省電力化とセンサノードの最適化に関しては，ハードウェア開発が必要となるため協賛団体をつのり，共同開発していく必要がある．また，uPackage プロジェクトにおいて述べたパッケージを作成するためにも販売力のある企業との連係が不可欠であると考えられる．

7　開発者名

榊原 寛 (慶應義塾大学政策・メディア研究科 (2008 年 3 月時点))
米澤 拓郎 (慶應義塾大学政策・メディア研究科 (2008 年 3 月時点))