2007－UBI－16 (9)
2007／11／29

プライバシ制御タグ向けサービスプラットフォームの構築

仁野 央孝† 西尾 信彦††

† 立命館大学大学院理工学研究科
〒525-8577 滋賀県草津市野路東 1-1-1
†† 立命館大学情報理工学部
〒525-8577 滋賀県草津市野路東 1-1-1
E-mail: †nino@ubi.cs.ritsumei.ac.jp, ††nishio@cs.ritsumei.ac.jp

あらまし 情報推薦などの個人に特化したサービスを受けるためにはプライバシ情報をサービスに開示しなければならない. 多くのプライバシ情報をサービスに開示することでより個人に特化したサービスを享受することが可能だと考えられるが, 一方では情報漏洩などによりプライバシが侵害される恐れがあるため, プライバシ情報は各々が制御することが望ましい. 本稿ではサービスに開示するプライバシ情報を段階的に制御できる"プライバシ制御タグ"を扱うプラットフォームと, プライバシ制御状態の管理手法を提案する.

Service Platform for Privacy Controllable Tag

Hirotaka NINO† and Nobuhiko NISHIO††

† Graduate School of Science and Engineering, Ritsumeikan University
1-1-1 Nojihigashi, Kusatsu, Shiga, 525-8577 Japan
†† College of Information Science and Engineering, Ritsumeikan University
1-1-1 Nojihigashi, Kusatsu, Shiga, 525-8577 Japan
E-mail: †nino@ubi.cs.ritsumei.ac.jp, ††nishio@cs.ritsumei.ac.jp

Abstract It is nesseary to disclose personal information to enjoy services such as recommendation service. The more personal information we disclose, the more quality of personalization services may improve. However, it increase privacy concerns such as information leak. Personal information should be controlled by on one's own. In this paper, we propose Platform which treats "Privacy Controllable Tag" that controls the level of privacy control, and a mechanism managing privacy control.

1. はじめに

近年,RFID 技術を用いて測位や認証を行う研究が数多く行われている. RFID 技術は IC タグとそれを読み取るリーダ/ライタから構成されており,IC タグが ID を送り返す「パッシブ型」と,IC タグ側から電波で ID を発信し続ける「アクティブ型」に分類される.

パッシブ型はリーダ/ライタから発信される電波を電力に変えて動作するため, 電池を搭載する必要がない. また,IC タグに様々な情報を記憶するとが可能なため, 電子マネーや物品管理, 在庫管理などに応用されている. パッシブ型は電池を搭載する必要がないという利点と引き換えに通信範囲は数センチから 1,2 メートル以内と限定される. ユーザは明示的に通信をおこなわなければならないが, 逆にそれを利用し, ユーザが通信を行ったことをトリガーとして近隣の店舗を推薦するサービスなども提供されている [1], [2].

アクティブ型は IC タグが電池を内蔵しており, 常に ID を発信し続けている. 通信範囲は利用する場の障害物や電波状況にもよるが基本的に 360 度,7m～数 10m の範囲に電波を発信しており, リーダ/ライタがその範囲内

にあればIDを読み取ることができる. この通信範囲を活かし, ユーザにタグを持たせ自動的に入退室管理を行ったり, 子供にタグを持たせ, 居場所を通知する防犯などに応用されている. 「パッシブ型」では明示的に通信を行うことを利用しユーザの正確な測位が可能であるが, 通信範囲が限定される.「アクティブ型」では明示的に通信を行う必要がなく通信はパッシブ型と比べて広範囲だが, それゆえにユーザの正確な測位は行うことができず, ユーザがその周辺に存在しているということしか知ることができない.

一方で, 我々はプライバシに関わる情報 (以下, プライバシ情報) を用いた様々な都市サービスを利用している. 我々が日常的に利用している都市サービスは, 登録の必要はなくその場だけでサービスを提供する揮発的サービスと, 登録されたユーザを対象とし, 永続的にサービスを提供する永続的サービスが両極に位置している. 揮発的サービスは高機能センシング技術を活用し, ユーザのコンテキストを取得してその場だけのサービスを提供する. プライバシ情報を利用せず, 準備もいらないが, 取得できるコンテキストに限界があり, ユーザに特化した有益な情報を与えるのは難しい. 永続的サービスは, 登録されたユーザを対象としているため, ユーザの過去の行動履歴やサービスの利用履歴を利用できる. ユーザが登録した情報や履歴を用いることでユーザに特化した有益なサービスを提供できる. しかしその一方でユーザがサービスに対して開示しなければならないプライバシ情報が多く, 特に行動履歴などは悪用された場合に自らの行動が容易に追跡される可能性もあるため, リスクが高いといえる. このような状況下ではユーザは盲目的に自身の情報をサービスに開示することには抵抗があると考えられる. サービスに開示するプライバシ情報はユーザのその場の状況をユーザ自身が判断し, ユーザによって制御されることが望ましい.

現在多くのサービスがRFIDタグを利用し, 様々なサービスを提供されているが, 既存のRFIDタグではユーザ側から自らのプライバシに関わる情報を制御することはできない. 我々は, ユーザ自らが自身のプライバシ情報をどの程度まで開示するか制御することが可能なタグを"プライバシ制御タグ"と呼んでいる. プライバシ制御タグはユーザの意思によって, サービスへのユーザ自身のプライバシ情報の開示を制御し, 段階的に提供することができる. この機能を利用することにより, ユーザは一度に多くのプライバシ情報を与えなければならない永続的サービスや, 自分に特化した情報を与えることが難しい揮発的サービスに偏ることなく, 自分の意思でサービスのレベルを調整することが可能となる. しかし, プライバシ制御タグを扱うプラットフォームは開発されておらず, プライバシ制御タグの存在だけではサービスを開発することは難しい. 自身のプライバシ情報を制御することでサービスのレベルの調整を行えることは良いが, サービスのレベルは開発されるサービス毎に異なるものである. サービスのレベルはいくつ存在するのか, どの程度までプライバシ情報が開示されるとレベルが変化するのか, サービス開発者はこれらを考慮しながらサービス毎にプライバシ制御情報の管理を行っていかなければならない. また, サービス側がプライバシ制御情報の管理を行うと, ユーザ側でのプライバシ制御が意味を失ってしまう可能性がある. これらの問題を解決するため, プライバシ制御タグを扱うサービスの開発支援を行い, ユーザとサービスの間でプライバシ制御を管理するプラットフォームが必要であると考えられる.

そこで本稿ではプライバシ制御タグを扱うサービスに対してのプラットフォームの構築について述べる. 以下, 2章ではまずプライバシ制御タグについての説明を行う. 3章ではプラットフォームの設計とプライバシ制御状態の管理手法について延べ, 4章ではプラットフォームとサービスのプロトタイプ実装について述べる. 5章で関連研究について述べ, 6章でまとめと今後の課題について述べる.

2. プライバシ制御タグ

この章ではプライバシ制御タグの定義及び機能について述べる.

2.1 プライバシ制御タグの定義

プライバシ制御タグは, アクティブ型程度の通信範囲で通信が可能であり, ユーザによるプライバシ制御が可能なタグである. ユーザはプライバシ制御タグを利用することで自分に関する情報をサービスにどの程度まで開示するか段階的にコントロールすることができる.

2.2 プライバシ制御タグの機能

2.2.1 個人の認証

プライバシ制御タグは, アクティブ型程度の通信範囲での双方向通信が可能なICタグである. よって常に自身のIDを発信し続けることによって, リーダ/ライタでIDを読み取ることができる. タグのIDを読み取ることで識別を行えば, システム側にユーザ情報を管理する機構を設けることでユーザの認証が可能になると考えられる.

2.2.2 プライバシ制御

プライバシ制御タグの最大の特徴としてユーザが自身の情報をどの段階までサービスに開示するかコントロールが可能であることが挙げられる. 近年では大衆向けではなく, 個人に合わせた情報を提供するサービスが増えている. しかし, これらのサービスはユーザのプライバシ情報をサービスに開示しなければならない. ユーザにとって自身に関する詳細な情報 (年齢や趣味, 嗜好) はサービ

ス提供側に与えれば与えるほどリスクが増すと考えられるので可能な限り開示したくはない．さらに近年では街中に多くの公共端末が用意されており，このような第三者が数多く存在する環境ではなおさら抵抗があると考えられる．しかし，情報を全く開示しなければ自分に特化したサービスを享受することはできない．サービスに開示するプライバシ情報はユーザのその場の状況をユーザが判断し，ユーザによってコントロールされることが望ましい．プライバシ制御タグにはユーザの意思をサービスに伝える機能があり，この機能を利用することでユーザはそれらの情報をどの程度まで開示するか決定することができる．

2.3 想定されるサービス

1章で述べたように，我々が日常的に利用している都市サービスは，登録されたユーザを対象とし，永続的にサービスを提供する永続的サービスと，登録の必要はなくその場だけでサービスを提供する揮発的サービスが両極に位置していると考えられる．永続的サービスのように，ユーザが提供するプライバシ情報は多ければ多いほどサービスはユーザに適した情報を与えることができる．しかしその反面，過去の利用履歴や行動履歴などがサービスに開示され，ユーザが抱えるリスクは高まるといえる．揮発的サービスのようにユーザはサービスに登録する必要がなく，その場だけで完結するようなサービスでは，ユーザのプライバシ情報をほとんど利用しないため，ユーザに適した情報を与えることは難しくなる．

プライバシ制御タグの特徴は，このような両極に位置しているサービスの間に段階を設け，ユーザの意思によってプライバシ情報を開示する程度を調整できることにある．プライバシ制御タグを利用したサービスとは，このようにユーザの意思によって揮発的なサービスから永続的なサービスに段階的に近づいていくサービスであると考えられる．

例えば街中で飲食店の推薦を段階的に行うシステムが考えられる．ユーザが何も情報を開示しない場合では，自分に特化した情報を得ることはできない．しかしユーザが，自分の位置 → 自分の嗜好 → 財布の中の金額 → 昨日何を食べたかという情報を段階的に開示していくことで，サービスはユーザのプライバシ制御状態に応じてユーザに適している可能性の高い店舗を推薦することが可能になる．

3. プラットフォームの設計

本章ではプラットフォームの設計について述べる．

3.1 プラットフォームの概要

本稿でのプラットフォームとはプライバシ制御タグを利用したサービスの開発を支援するサービスプラットフォームである．図1にプラットフォームの全体図を示し，それぞれの役割について詳しく述べる．

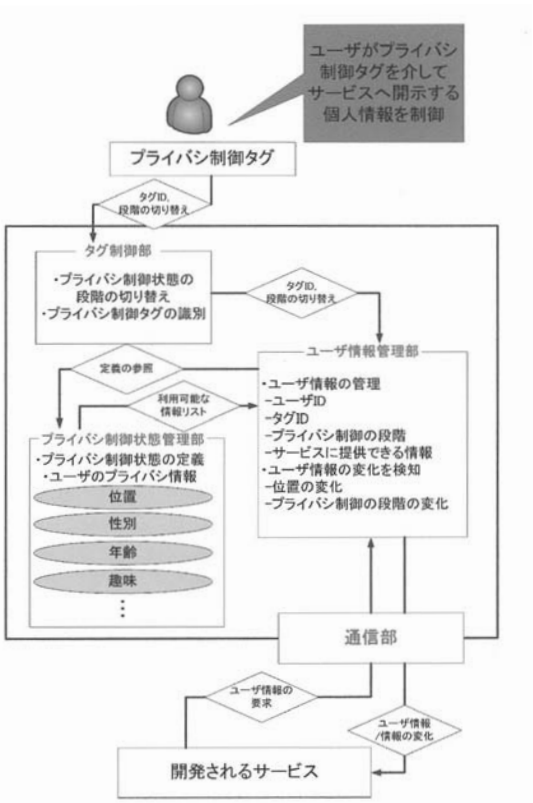

図1 プラットフォームの設計

- タグ制御部

プライバシ制御タグではユーザ側が自身の情報の開示の程度を決定できる．タグ制御部ではユーザからプライバシ制御状態の切り替えの意思を受け取る．サービスの段階によってどの程度まで情報を開示するかはサービスによって定義されるものだが，段階の切り分けはユーザが行うため，ユーザから切り替えのサインが発せられる．また，タグ制御部ではプライバシ制御タグから取得可能な情報を受け取る．例えば位置や個人認証によって得た情報などである．これらの情報をユーザ情報管理部へと引き渡す．

- ユーザ情報管理部

プライバシ制御タグによって変化するユーザの状態を管理する．ユーザ情報管理部はタグ制御部からプライバシ制御タグから発せられる情報を受け取る．例えば，ユーザの位置やプライバシ制御状態はユーザの移動や意思によって刻々と変化するものであり，ユーザ情報管理部は各ユーザの状態をプライバシ制御状態に応じて管理を行う．ユーザの状態に変化があれば，それらの情報を通信部へと渡し，サービスへ通知する．

- プライバシ制御状態管理部

プライバシ制御状態の定義は実装されるサービスによって異なることが予想される. プライバシ制御状態管理部ではそれらサービスによって異なるプライバシ制御状態の管理を行う. 例えば, サービス A では位置情報を開示するのが第一段階としても, サービス B では位置情報と個人の認証までが第一段階と定義するかもしれない. これらサービスのプライバシ制御状態管理手法については後述する.

- 通信部

サービスとプラットフォーム間の通信を行う. 主にサービスからの要求を受け取り, ユーザ情報管理部からの返答をサービスに返す. また, プラットフォーム側で発生するイベント (ユーザの位置の変化, プライバシ制御レベルの変化) をサービスに通知する. サービス側での実装の言語を限定させないため, 通信部は言語非依存で実装される必要がある.

3.2 プライバシ制御状態管理手法

3.2.1 プライバシ制御状態の定義

プライバシ制御状態の定義は実装されるサービスによって異なると考えられる. よってサービスによってプライバシ制御状態の定義が行われなければならない. プライバシ制御の定義は段階数の定義と情報開示の定義に大別される. 図 2 にサービスによる定義の例を示し, それぞれの定義について述べる.

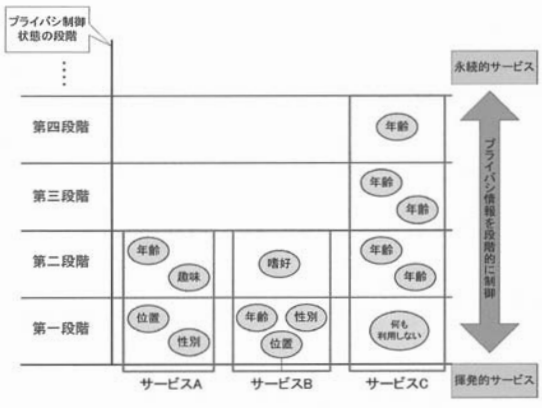

図 2 サービスによるプライバシ制御状態の定義例

- 段階数の定義

プライバシ制御タグを利用することで, ユーザはサービスに対して段階的に自身のプライバシ情報を開示していくことが可能になるが, プライバシ制御状態の段階はいくつ用意するかは実装される各サービスによって異なるものである. サービスによってはプライバシ制御状態の段階として五段階必要かもしれないし, 二段階で十分かもしれない. プラットフォーム側でこの段階数を定義してしまうと, 実装されるサービスの自由度を下げてしまい, 開発の妨げになる可能性があるので望ましくない. よってプライバシ制御状態の段階数はサービスによって定義される. 例えば, 図 2 のサービス A,B は段階を二段階に定義し, サービス C は四段階に定義している. プライバシ制御状態の段階は低ければ低いほど揮発的サービスに近く, 段階を上げるに連れて永続的サービスに近づいていく.

- 情報開示の定義

プライバシ制御タグで制御できるユーザのプライバシ情報には, ユーザの現在いる場所やより正確な位置, 年齢や性別, 趣味, 嗜好など様々な情報が考えられる. これらの情報をどの程度まで開示することを第一段階, 第二段階とするのかは開発されるサービスによって異なり, サービスによって定義されるべきものである. 仮にこの情報開示の定義をプラットフォーム側で行ってしまうと, サービス側が必要な情報を取得できない可能性や, 取得する必要のない情報までも提供してしまう可能性がある. 情報開示の程度はサービスによって動的に定義される必要がある. 例えば, 図 2 のサービス A はユーザの位置, 性別までが第一段階と定義しているが, サービス B ではさらに年齢まで加えた状態を第一段階としている. また, サービス C では何も情報を利用しないことを第一段階としている. このように情報開示の程度はサービスによって定義される.

3.2.2 プライバシ制御状態の定義の開示

プライバシ制御状態をユーザが制御することで自身のプライバシ情報の開示をコントロールしているつもりでも, サービスがプラットフォームから自由にユーザの情報を引き出すことが可能であると, プラットフォームは意味を失ってしまう. つまり, ユーザ側からは制御されているように見えるが, 実際はサービスがユーザの情報を全て手にしており, ユーザの切り替えに合わせて情報を提供しているという事態が考えられる. 例えば, サービスはプライバシ制御段階の第一段階として, ユーザのプライバシ情報全てを取得できるように定義されれば, ユーザの把握できないところでプライバシ情報がすでにサービスに渡ってしまう可能性がある. このような事態を避けるため, プラットフォームは, ユーザに対してサービスが定義したプライバシ制御状態の定義を開示する. ユーザが開示されている定義を見ることで, どの段階にどのプライバシ情報が割り当てられているか理解し, 自身で情報の開示の制御を行うことができる. こうすることでユーザが意図しない間にサービスにプライバシ情報が提供されるという事態を避けることができる.

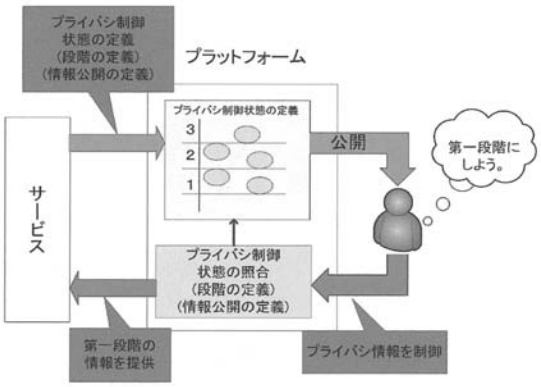

図 3　プライバシ制御状態の定義の公開

4.　プロトタイプ実装

本章では実装したプラットフォームのプロトタイプ及びサービスについて述べる.

プライバシ制御タグはユーザによってプライバシ制御状態の切り替えを行う機能を有しているため, タグ側からシステムに対して送信する機能を持っていなければならない. また, プライバシ制御に段階を持たせるため, 個人認証や測位が行えるものが望まれる. そこで, プライバシ制御タグには我々が開発した RFID 技術と画像認識技術を組み合わせた PRECOG-Tag [3] を用いて, 実装を行った. 以下,PRECOG-Tag, プラットフォーム, サービスの実装についての説明を行う.

4.1　PRECOG-Tag

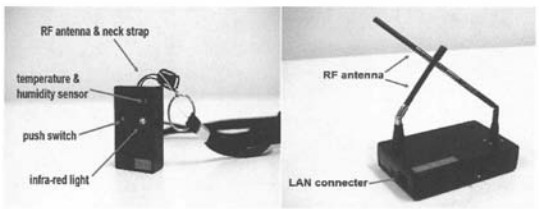

図 4　PRECOG-Tag とリーダ/ライタ

4.1.1　個人の認証

PRECOG-Tag は RFID 技術と画像認識技術を組み合わせ, 正確な測位を可能にしたアクティブ型の IC タグである. よって常に自身の ID を発信し続けている. 個人の認証にはこのアクティブ型 RFID の機能を用いる. アクティブ型の RFID は数 10m まで通信が可能なため, その通信範囲にリーダ/ライタがあれば ID を読み取ることができる. タグの ID を読み取ることで識別を行えば, システム側にユーザ情報を管理する機構を設けることでユーザの認証が可能になる.

4.1.2　測　　位

a)　アクティブ型 RFID による測位

PRECOG-Tag はアクティブ型の IC タグであるため, 自身の ID を常に発信している. 通信可能な範囲にリーダ/ライタがあれば ID を読み取ることができる. この機能を利用することで, リーダ/ライタが ID を読み取ることができればその周囲数 10m の範囲にユーザが存在すると判断することができる.

b)　赤外線認識による測位

PRECOG-Tag はアクティブ型の RFID タグであることに加えて画像認識技術を利用した赤外線認識による測位を行うことができる.PRECOG-Tag は赤外線 LED が備え付けられている. この赤外線 LED はリーダ/ライタから命令を行うことで発行を促すことが可能であり, 赤外線の発光をカメラなどの映像機器で認識することで, 数 cm〜数 10cm 単位の測位を行うことができる.

4.1.3　プライバシ制御

PRECOG-Tag の前面にはボタンが設けられており, ボタンを押すことでユーザの意思を伝えることができる. このボタンと赤外線 LED の発光を利用し, このタグでは情報開示の段階として現在四段階に切り替え可能である. 図 5 にそれぞれの状態とその遷移方法を示し, それぞれの状態について詳しく述べる.

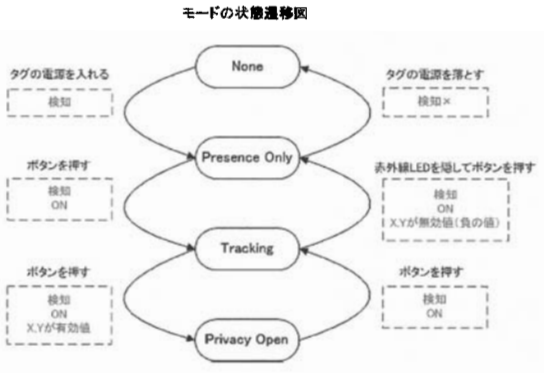

図 5　プライバシ制御レベルの状態遷移

- None

ユーザはサービスに対して何も情報を提供しない. ユーザはタグの電源を off にした状態であり, タグからは電波は発信されていない. よってユーザがリーダ/ライタと通信可能な位置にいたとしてもサービス側にユーザの存在は認識されない.

- Presence Only

ユーザはサービスに対して自身の存在だけを伝える. ユーザはタグの電源を on にした状態であり, この時点でタグから電波の発信が始まる. よってユーザがリーダ/ライタと通信可能な範囲に入ると, リーダ/ライタがタグ

の ID を検知し, ユーザの存在を確認する. この段階ではサービスはユーザがリーダ/ライタの通信範囲内にいるという存在だけはわかるが, 通信範囲内のどこにいるのか詳しい位置は分からない. タグの電源を off にすることで Presence Only → None へと切り替わる.

- Tracking

ユーザはサービスに対して自身の存在に加え, さらに正確な位置を開示する.Presence Only の状態でボタンを押すと, ユーザの状態は Tracking へと切り替わる. ユーザが Tracking に切り替えるとリーダ/ライタを介してタグに取り付けられている赤外線 LED に対して発光命令が送信され, 赤外線 LED の発光, 点滅が始まる. この赤外線をカメラで認識することによりユーザがリーダ/ライタの通信範囲内のどこにいるか, という詳しい位置を知ることができる. また, 赤外線 LED は点滅し続けるように命令が行われるため, サービスはユーザが移動してもリアルタイムにユーザの詳しい位置を知ることができる.Presence Only の状態に切り替える場合は手などでタグに取り付けられている赤外線 LED を隠し, カメラから認識できない状態にしたうえでボタンを押す. タグの電源を off にすれば None の状態まで戻る.

- Privacy Open

ユーザはサービスに対してさらに自身の個人情報の利用を許可する. ユーザが Tracking の状態でボタンを押すと, ユーザの状態は Privacy Open へと切り替わる. サービスはユーザの個人情報を利用したサービスを提供することができる. 個人情報の利用を禁止し,Tracking の状態へと切り替えたい場合は Privacy Open の状態でボタンを押す. タグの電源を off にすれば None の状態まで戻る.

4.2 プラットフォームのプロトタイプ実装

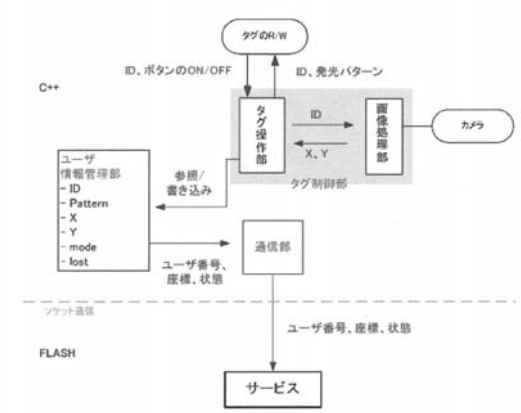

図 6 プラットフォームの実装

プラットフォームは C++を用いて実装した. また, プライバシ制御タグを利用するサービスを Flash を用いて実装した.

- タグ制御部

タグ制御部の実装は PRECOG-Tag の機能上, タグ操作部と画像処理部に分けて行った. タグ操作部では PRECOG-Tag から発信される ID, プライバシ制御状態の切り替えを受信する. また PRECOG-Tag の赤外線 LED へ発光命令を行う. 画像処理部は PRECOG-Tag の赤外線光を認識し, ユーザの正確な位置を取得する.

- ユーザ情報管理部

タグ制御部からタグ ID, タグの位置, プライバシ制御レベルの情報を受け取り, 各ユーザごとに管理する. また, ユーザの位置やプライバシ制御レベルはユーザの行動によって変化するので, それらの変化をイベントとして捉え, サービスにイベント情報を引き渡す.

- 通信部

ユーザ情報管理部から受け取った情報をサービスへと送信する. 通信部では受け取った情報を XML 形式に変換し, ソケット通信を用いてサービスに情報を送信する.

4.3 サービス概要

タグから情報を取得し, サービスへと提供するプラットフォームのプロトタイプとユーザが開示する情報の程度によって与える情報が変化するサービスを実装した. 図 7 にサービスの全体図を示す.

図 7 のようにタグを利用するユーザとプロジェクタの間に透明なスクリーンを配置する. このサービスではユーザがサービスへ与える情報によってスクリーンに表示される情報に変化をもたらすことができる. ユーザが自身の情報の開示を段階的にコントロールすることで様々な変化をスクリーン越しに確認することができる.

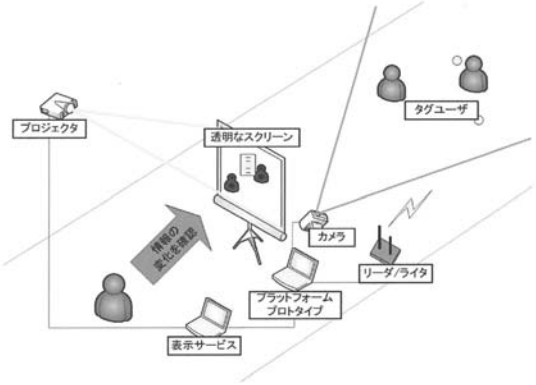

図 7 サービス全体図

a) サービスシナリオ

ユーザは PRECOG-Tag を首から下げ, リーダ/ライタの通信可能範囲に移動する. ユーザが PRECOG-Tag の

ボタンを押すとプライバシ制御状態が None から Presence に遷移し, スクリーンにはユーザの存在を示すアイコンが表示される. ユーザがもう一度ボタンを押すとプライバシ制御状態は Presence から Tracking に遷移し, ユーザの正確な位置がサービスに伝えられ, スクリーンにはユーザを囲む枠が表示される (図 8 左側のユーザ). この状態でユーザが移動を行うと, ユーザを囲む枠はユーザの移動に合わせてユーザを追跡する. ユーザがさらにスイッチを押すとプライバシ制御状態は Tracking から Privacy Open に遷移し, サービスはユーザの個人情報の公開が許可され, スクリーンにはユーザの名前や画像といった情報が表示される (図 8 右側のユーザ).

図 8　サービス実行時の様子

5. 関連研究

RF タグの普及に伴い, 位置情報管理に関するプライバシを考慮し, 慶應義塾大学の岩井氏らはプライバシを考慮する電子タグ位置情報管理機構:Tachyon [4] を提案している. 岩井氏らは,RF タグの特性によりユーザの意図が反映されていなくても位置情報が取得できてしまう可能性を問題として取り上げている. この問題を解決するため, 各ユーザのプライバシポリシを保持している Representation と呼ばれる分散オブジェクトを各リーダに接続している計算機に配置し, それらに交渉を行わせることでユーザの位置情報公開の相手, 範囲, 時間帯を限定した. しかし, この手法ではプライバシポリシをユーザ側が記述する必要があり, ユーザが情報公開の相手, 範囲, 時間帯などを変更したいと考える度にプライバシポリシを記述しなおさなければならない. 本稿で提案した手法ではプライバシ制御状態の定義はサービス側が行うため, ユーザはプライバシ制御状態の段階の切り替えを行うだけでよく, 負担が少ないと考えられる.

また, 大阪大学の宮本氏らは, プライバシとサービス品質のトレードオフを考慮した個人情報制御機構:GrIP [5] の提案している. 宮本氏らは, ユーザにはできる限り個人情報を開示せずに個人化サービスを利用したいという要求があるが, その場合にプライバシ保護とサービス品質のトレードオフが生じると述べている. この問題を解決するため, 特定確率というプライバシを客観的に評価する基準を定義し, ユーザが特定確率を指定することで, 開示する個人情報が制御できると提案されている. 特定確率はユーザ個人が特定されるリスクから計算され,GrIP がプライバシとサービス品質のトレードオフを解決する情報の種類やその粒度の組み合わせを探索し, 個人情報を制御する. しかし, システムが特定確率をもとに自動的に利用可能なサービスを選定するため, ユーザの特定確率の指定によっては求めているサービスを利用できない可能性がある. また, 個人情報を制御しているのは GrIP であり, ユーザは自分のどんな情報がサービスに公開されているのかその場で判断はできない. 本稿で提案した機構では, ユーザがその場で自らの状況を判断し, プライバシ制御状態の切り替えを行うことができる. また, サービスが定義したプライバシ制御状態はユーザに公開されるので, 自分がどんな情報をサービスに公開したかその場で判断することができる.

6. まとめと今後の課題

本稿では, プライバシ制御タグを利用するサービスの開発するためのプラットフォームの構築について述べ, それぞれのサービスによって異なるプライバシ制御状態の管理手法について述べた. また, プロトタイプとして PRECOG-Tag を使用し,PRECOG-Tag を扱うサービスとプラットフォームの実装を行った. しかし, 現段階ではプライバシ制御状態管理手法は実装されておらず, ユーザの情報の開示の程度はサービス側に依存している. 今後はプライバシ制御管理手法の実装を行い, 情報開示の程度をユーザ側に決定させなければならない. また, 現段階では異なるサービスの同時利用は想定していないため, サービスのプロトタイプを複数実装し, 要件に応じてプラットフォームの構築を行う.

文　献

[1] トルカ,NTT DoCoMo, http://www.nttdocomo.co.jp/service/osaifu/

[2] PiTaPa グーパス, PiTaPa グーパス株式会社, http://www.goopas.jp/pg/pc/index.html

[3] Nobuhiko Nishio 'PRECOG-Tag:Privacy-Controllable Personal Identification' :UbiComp Poster Session, 2006,September

[4] 岩井将行, 高橋元, 門田昌哉, 中島達夫, 徳田秀幸:"Tachyon:プライバシを考慮する電子タグ位置情報管理機構", 情報処理学会全国大会論文集,pp.49-53(2004)

[5] 宮本崇弘, 竹内亨, 奥田剛, 春本要, 有吉勇介:"プライバシとサービス品質のトレードオフを考慮した個人情報の提案",DEWS,2005