2003－OS－93 (7)
2003／5／8

プライバシを考慮したパーソナライゼーションを実現するアプリケーションフレームワーク

田丸 修平[1] 岩谷 晶子[1] 高汐 一紀[1] 徳田 英幸[1 2]
[1] 慶應義塾大学大学院 政策・メディア研究科 [2] 慶應義塾大学 環境情報学部

本論文では，プライバシを考慮した，アプリケーションが個人情報に適応的に動作するためのフレームワークを提案する．ユビキタスコンピューティング環境においては，機器の高性能化，多機能化によって，公共空間におけるアプリケーションの遍在や，携帯端末の高性能化による多様な情報の保持が可能となる．このことは公共空間におけるパーソナライゼーションを可能とする．携帯端末の高性能化によって，携帯端末に保持される情報が現実世界に即した個人情報を扱えるようになるため，プライバシを考慮したフレームワークが必要となる．本稿で提案する個人情報非送信型モデルでは，個人情報の取得と，アプリケーションの動作を決定するコマンドの生成を分離することでプライバシの保護を達成する．本稿で個人情報非送信型モデルを実現する EA-P2 フレームワークの実装を行った．これによって，プライバシの保護と個人情報への適応を両立させたアプリケーションの作成が可能となる．

An Application Framework for Personalized Public Space Considering Privacy

Syuhei Tamaru[1] Akiko Iwaya[1] Kazu Takashio[1] Hideyuki Tokuda[1 2]

[1]Graduate School of Media and Governance, Keio University
[2]Faculty of Environmental Information, Keio University

This paper proposes an software framework which enables application to adapt to user information with the consideration for privacy. In ubiquitous computing environments, sophisticated appliances enable application services to be ubiquitously available in public spaces and the personal devices in this environment holds privacy information. This will make personalization of applications in public spaces possible. With mobile devices's high functionality, information which mobile device retain will be information according to the real world, a framework considering privacy will be needed. We have achieved to preserve privacy in our system by splitting the user information acquisition module and the module which generates commands according to the user information. With this framework, programmers can develop an application striking a balance between preserving user's privacy and adaptation of user's information.

1 はじめに

ユビキタスコンピューティング環境の実現を前提としたアプリケーションが日々研究開発されている．情報機器や多様なセンサの遍在によって，ユーザにとってより快適なアプリケーションの実現が可能となる．アプリケーションがユーザの嗜好に適応するための仕組みとして，ユーザが設定した静的な値に基づいて動作する方法がある．例えば，ユーザインタフェースの設定や，ホットキーの割り当てなどがある．将来的には携帯デバイスの小型化，高性能化によって多様な情報の保持が可能となり，現実世界におけるユーザの**個人情報**をアプリケーションが利用することが可能となる．本稿では，性別や年齢などの不変的な情報から，好み，アプリケーションの設定まで，ユーザの個人情報を広義に用いる．個人情報の導入によって，ユーザの性別や職業に応じてアプリケーションの挙動を変えることが可能となる．つまり，**公共空間におけるアプリケーションのパーソナライゼーション**の実現が可能となる．

本稿では，続く第 2 章で公共空間におけるアプリケーションのパーソナライゼーションについて詳細を述べ，その問題点を指摘する．次に第 3 章でプライバシの保護と個人情報へ

の適応を両立させるための手法として，個人情報非送信型モデルを提案する．第 4 章で設計を行い，第 5 章で個人情報非送信型モデルを実現するためのプロトタイプ実装である EA-P2 フレームワークについて述べる．第 6 章にて定性的及び定量的評価を行い，第 7 章で今後の課題について述べる．

2 公共空間におけるアプリケーションのパーソナライゼーション

本節では，まず本稿の研究対象を明確にするため，公共空間におけるアプリケーションのパーソナライゼーションについて説明し，実現する際の問題点を指摘する．

2.1 個人情報への適応

ユーザは移動先に存在する様々なアプリケーションを利用する．アプリケーションはユーザの携帯端末に保持されている個人情報に適応した動作を行う．これらを実現したものとして，街頭に存在しユーザの障害に応じてインタフェースを切り替えて道案内を行う，障害者のためのナビゲーションシステムであるアクティブポスター [1] や，美術館においてユーザの美術品に対する知識により解説内容を変更する ILEX-0[2]，観光地において旅行者に対して案内を行う PDA 上で動作するブラウザである GUIDE[3] などがある．以上のように，多様なユーザの個人情報に適応した動作を行うことで，ユーザの入力負担の軽減と，公共空間におけるアプリケーションのパーソナライゼーションを実現することができる．これを図 1 に表す．

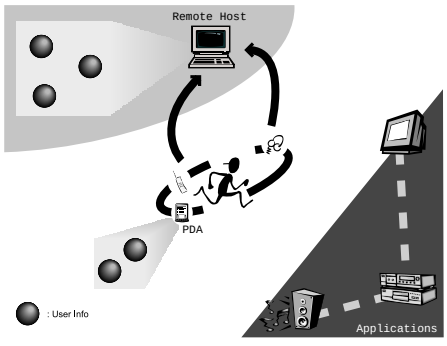

図 1: 公共空間におけるアプリケーションのパーソナライゼーション

2.2 個人情報を用いるアプリケーションの形態

個人情報とアプリケーションは，それぞれが一対になっており，個人情報が保持されている携帯端末は，１つ以上のアプリケーションのための個人情報を保持していることを想定する．例としてデパートがユーザのより好む商品を勧めるアプリケーションを挙げると，個人情報はデパート毎に存在し，個人情報はアプリケーション単位で，各々が異なる携帯端末に保持されている可能性が有る，ということである．この例に沿った個人情報とアプリケーションの関係を図 2 に表す．矢印が，個人情報とアプリケーションがそれぞれ対応していることを示している．

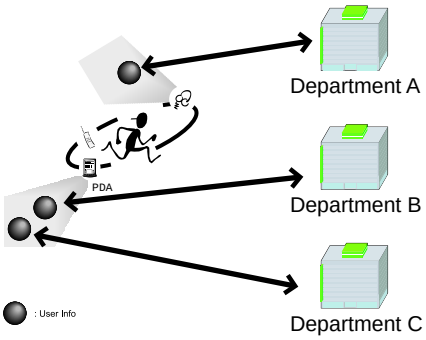

図 2: 個人情報とアプリケーションの形態

2.3 プライバシ

上記の通り個人情報の導入によって，より利便性の高いアプリケーションを実現できる一方で，プライバシの問題が発生する．本稿で述べるプライバシの問題とは，**ユーザの知られたくない個人情報が意図しない他者に知られてしまうこと**である．例えば，ユーザの住所や電話番号などが，意図しない第 3 者に知られてしまうことである．公共空間におけるアプリケーションでは問題がより深刻になる．

公共空間におけるアプリケーションの中には悪意のあるものが存在する可能性がある．つまり，ユーザが意図しない第 3 者に，取得した個人情報を公開したり，ユーザが意図しない個人情報まで取得してしまうアプリケーションの存在である．公共空間においてはこれらのアプリケーションが遍在する．そこで，**ア**

プリケーションを信用しない，という前提で対処する必要がある．

また，高機能化，多機能化した携帯端末を悪意のある第 3 者が手にすることによって，個人情報が保持されている携帯端末とアプリケーションとの通信を傍受される危険性がより高くなる．通常，通信傍受への対応には暗号化を用いるが，前項の悪意のあるアプリケーションに対する有用性がない．

2.4 現行のプライバシ保護手法

現在広く普及しているプライバシ保護手法は**通信相手，または第 3 者に対する依存性**がある．

P3P

W3C[4] が提供する P3P[5] は Web サイト閲覧において，ユーザから取得した個人情報の利用方法及び利用範囲をユーザに開示するためのフレームワークである．ユーザへの開示が個人情報を取得した以後に行われる場合が多い．また，ユーザが長い文章を読む必要がある．さらに，P3P は Web サイトによる個人情報の利用方法及び利用範囲の保障はできない．

プロクシサーバ

Anonymizer[6] などのプロクシサーバは，ユーザがプロクシサーバを経由して Web 閲覧を行うことで，ユーザが使用しているホストの IP アドレスやポート番号などを Web サイトに対して隠蔽する．これによって，プライバシの保護を達成することができるが，プロクシサーバの信頼性という問題がある．

暗号化

SSL[7] などの暗号化は第 3 者への対応策として有効である一方で，通信相手を信用する，という前堤で成り立っている．前節で述べたように悪意のあるアプリケーションの遍在する環境においては有用性がないため，暗号化に変わる手法を用いる必要がある．

3 アプローチ

本節では，前節で述べた公共空間における個人情報を利用したアプリケーションを実現するための，プライバシを考慮したアプリケーションフレームワークについて概要を述べる．まず，対象アプリケーションの基本動作について考察し，個人情報非送信型モデルを提案する．次にその特徴について述べ，最後に実現するための機能要件を挙げる．

3.1 概要

本節では，対象アプリケーションの動作を考察し，個人情報非送信型モデルを提案する．

個人情報送信型モデル

本稿の対象アプリケーションである公共空間における個人情報に適応的なアプリケーションの基本動作について述べる．従来のモデルを，個人情報送信型モデルと呼び，アプリケーションは図 3 のように動作することを想定する．

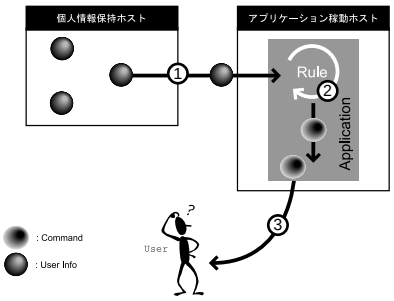

図 3: 個人情報送信型モデル

1. ユーザの個人情報を取得
2. 個人情報とアプリケーションルールに基づいて制御コマンドを生成
3. 制御コマンドに基づいた動作

アプリケーションルールとは，個人情報を基に，１つの解を生み出す式，あるいは式の集合である．本フレームワークでは，個人情報の取得と，制御コマンドの生成を分離して捉える．

個人情報非送信型モデル

本稿では公共空間におけるパーソナライゼーションを実現するための手法として，個人情報非送信型モデルを提案する．基本動作を図 4 に示す．

1. ユーザの携帯端末にアプリケーションルールをダウンロード
2. 個人情報とアプリケーションルールに基づいて制御コマンドを生成
3. 制御コマンドの送信
4. 制御コマンドに基づいた動作

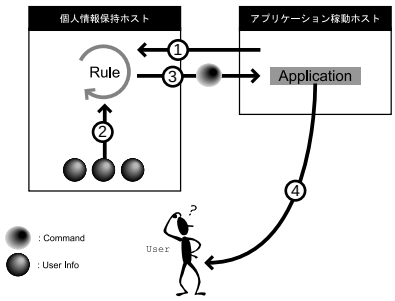

図 4: 個人情報非送信型モデル

3.2 特徴

本項では，個人情報非送信型モデルの特徴を述べる（図 5）.

3.2.1 悪意のあるアプリケーションに対する機密性

本稿で提案する個人情報非送信型モデルでは，個人情報ではなく，制御コマンドをアプリケーションに送信するため，悪意のあるアプリケーションに対して有効である.

3.2.2 悪意のある第 3 者に対する機密性

公共空間において個人情報に適応的なアプリケーションを利用する際，通信を傍受される危険性がある．個人情報非送信型モデルでは個人情報自体が通信されることはないため，個人情報を保護できる.

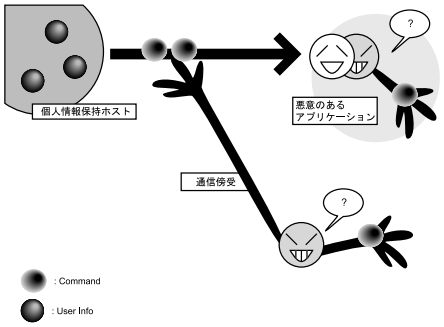

図 5: 特徴

3.3 機能要件

本項では，本稿で提案する個人情報非送信型モデルを実現するアプリケーションフレームワークに要求される機能要件について述べる.

個人情報の機密性

前節で述べたように，本稿では悪意のあるアプリケーションの遍在を前提とするため，アプリケーションへの個人情報の漏洩を防ぐ必要がある.

柔軟な個人情報の記述方式

本研究が提案するフレームワークは様々な個人情報に適応的なアプリケーションを前提とするため，個人情報の記述が柔軟に行われる必要がある.

利便性

ユーザの再入力や回答の負担を軽減する，という個人情報に適応的なアプリケーションの本来の目的を損なわないため，ユーザの負担を増加させずに上記の要件を達成する必要がある.

4 設計

本節では，本稿で提案した個人情報非送信型モデルを実現するためのアプリケーションフレームワークの設計について述べる.

4.1 全体構成

本フレームワークの全体構成を図 6 に示す．個人情報保持ホストはユーザの持つ携帯端末であり，アプリケーション稼動ホストはユーザの移動先の公共空間に存在する.

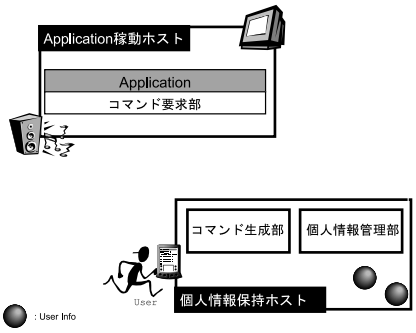

図 6: 全体構成図

ユーザは個人情報保持ホストとして携帯端末を保持し，移動先の公共空間に存在するアプリケーションを利用する．コマンド要求部はアプリケーション稼動ホスト上で動作し，コマンド生成部，個人情報管理部は個人情報保持ホスト上で動作する.

コマンド要求部

アプリケーションルールを送信し，個人情報保持ホストに制御コマンドを要求する．

個人情報管理部

アプリケーションルールに必要な個人情報を取得し，コマンド生成部に提供する．

コマンド生成部

アプリケーションルールと個人情報を基に，制御コマンドを生成する．

4.2 基本動作

基本動作を図 7 に示す．

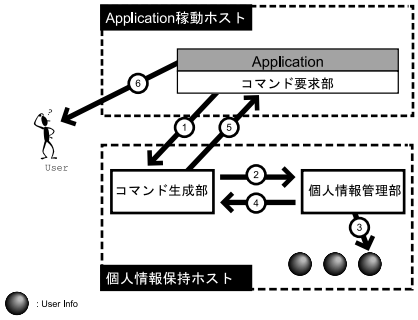

図 7: 基本動作

1. コマンド要求部がアプリケーションルールを送信する
2. アプリケーションルールに従って，個人情報管理部に個人情報を要求する
3. 個人情報管理部が必要な個人情報を取得する
4. 個人情報をコマンド生成部に返す
5. 制御コマンドを生成，アプリケーションに制御コマンドを返す
6. 制御コマンドに基づいた動作

4.3 個人情報のテンプレート

自由なアプリケーション作成のためには，アプリケーション作成者が個人情報を自由に定義できる必要がある．そのために本フレームワークではテンプレートを提供する．テンプレートには情報の種別を表す要素名を自由に定義できること，様々な値を記述できることが必要である．

4.4 アプリケーションルール

アプリケーションルールは個人情報同様に，アプリケーション作成者による記述の余地を残す必要がある．そこで個人情報と同様にテンプレートを提供する．テンプレートには以下の要素が必要となる．

- 必要な個人情報の種類
- コマンド生成のための式
- 生成されるコマンドの型

4.5 コマンド要求部

コマンド要求部は，アプリケーション稼動ホストに存在し API の役割を果たす．アプリケーションはコマンド要求部を経由し，アプリケーションルールを送信する．また，コマンド要求部によってアプリケーションは個人情報保持ホストから制御コマンドを取得する．

4.6 コマンド生成部

コマンド生成部は，アプリケーションルールを取得する．次に，アプリケーションルールが必要とする個人情報管理部に個人情報を要求し，個人情報管理部から返された値とアプリケーションルールに基づいたコマンド生成を行う．

4.7 個人情報管理部

個人情報管理部は，個人情報の種類を識別し，アプリケーションルールが必要とする値をコマンド生成部に返す．

5 実装

本節ではプロトタイプ実装である EA-P2（Enhancing Privacy and Adapting User Information for Personalized Public Space）フレームワークについて述べる．

5.1 実装環境

実装は WindowsXP 上で Java 言語を用いて行った．JDK のバージョンは 1.3.1 を使用した．個人情報の記述には XML[12] を使用し，XML パーサには Sun Microsystems の JAXP（JavaAPI for XML Processing） ReferenceImplementation を用いた．

5.2 個人情報

データ記述の柔軟性の観点から，個人情報の記述形式は XML を用いた．XML の DTD を図 8 に示す．

```
<?xml version="1.0" encoding="Shift_JIS"?>
<!ELEMENT userinfo (data+)*>

<!ELEMENT data EMPTY>
<!ATTLIST data name CDATA #REQUIRED>
<!ATTLIST data value CDATA #REQUIRED>
```

図 8: 個人情報の DTD

アプリケーション作成者は必要な個人情報を要素 data に記述する．各要素は属性 name によって識別され，その値を属性 value によって表す．個人情報は個人情報管理部によって管理される．

5.3 アプリケーションルール

本フレームワークではアプリケーションルールのテンプレートとしてインタフェースを提供する．このインタフェースを実装することで，アプリケーションルールを作成できる．evaluate メソッドの引数によって必要な個人情報の XML ファイルを指定する．図 9 にインタフェースを示す．

```
interface EAP2ApplicationInterface{
  public char evaluate(String file);
}
```

図 9: アプリケーションルール

5.4 コマンド要求部

コマンド要求部のアプリケーションルール移送の動作を図 10 に示す．アプリケーション作成者が実装した ApplicationRuleImpl オブジェクトを個人情報保持ホストに移送する．

```
ObjectOutputStream os
 = new ObjectOutputStream
            (s.getOutputStream());
os.writeObject(new ApplicationRuleImpl());
```

図 10: アプリケーションルールの移送

アプリケーションからの呼び出し例を図 11 に示す．getCommand メソッドによって，コマンド要求を行う．返り値は制御コマンドになり，制御コマンドを基にアプリケーションは個人情報に基づいた挙動を行う．

アプリケーションの記述は 1 行であり，アプリケーション作成者が本フレームワークを容易に利用することを可能とした．

```
char command ;
UserInfoRequest ur
   = new UserInfoRequest(hostAddr,port);
command = ur.getCommand();
```

図 11: アプリケーションによるコマンド要求部の呼び出し例

5.5 コマンド生成部

アプリケーションルールの取得を図 12 に示す．取得したアプリケーションルールの evaluate メソッドを用いて，コマンドを生成する．これによって，アプリケーションルールの自由な作成を実現する．

```
ObjectInputStream ois
 = new ObjectInputStream
              (s.getInputStream());
ApplicationRule appRule
 = (ApplicationRule)ois.readObject();

command = appRule.evaluate();
```

図 12: アプリケーションルールの取得

5.6 個人情報管理部

個人情報が記載された XML ファイルから要素を取りだす．前章で設計した通り，携帯端末上での動作を前提としているため，API には比較的高速処理が可能な SAX（Simple API for XML）を用いた．図 13 に個人情報解析の動作を示す．

5.7 応用例

本フレームワークを利用した応用例として，公共空間における電子広告版（PPM : Personalized Public Message-Board）を実装した．PPM の実装には，慶應義塾大学徳田研究室と内田洋行 [8] が共同開発した，Smart

```
public void startElement
    (String URL,String localName,
     String qName,Attributes attrs){
 if(qName.equals("data")){
   for(int i=0;i<attrs.getLength();i++){
     data[i] = attrs.getValue(i);
   }
 …
```

図 13: XML の解析

```
<?xml version="1.0" encoding="Shift_JIS"?>
<!DOCTYPE userinfo SYSTEM "EAP2.dtd">
<userinfo>
  <data name="age" value="23"/>
  <data name="sex" value="lady"/>
  <data name="nation" value="japan"/>
  <data name="job" value="student"/>
</userinfo>
```

図 14: 個人情報の記述例

Furniture[9] を用いた．PPM はユーザの年齢や性別に基づいて広告内容を変更する．PPM のデモンストレーションを慶應大学湘南藤沢キャンパスで行われた Open Research Forum2002[10] において行った．

6 評価

本節では EA-P2 のプロトタイプの評価を定量的評価と定性的評価に分けて行う．

6.1 定量的評価

本節では，5 章で述べた EA-P2 フレームワークのプロトタイプ実装の定量的評価を行う．定量的評価は個人情報保持ホストの処理時間を測定した．測定の目的は今後の改良の参考とすることである．測定環境を以下に示す．

測定環境

マシンの仕様を表 1 に示す．

表 1: 測定環境

CPU	PentiumIV 2.0GHz
主記憶	1.00GB
OS	Windows XP 5.10.26

測定方法

測定した内容は以下の通りである．
A．個人情報の解析にかかる時間
B．個人情報の取得から制御コマンド生成までの時間
全て 100 回実行した．また，測定に用いた個人情報を図 14 に示す．

測定結果

全体の処理は平均 330msec，A は平均 290msec，B は平均 40msec であった．個人情報の解析に全体の約 8 割を所要しているため，今後は解析にかかる処理の短縮が必要である．

6.2 定性的評価

本節では，は第 3 章であげた機能要件に基づいて，EA-P2 の定性的評価を行う．

個人情報の機密性

個人情報はコマンドに変換されることによって，第 3 者からの個人情報の保護は達成される．一方で，アプリケーションルールに基づいた制御コマンドの逆算によって，個人情報の特定が可能なため，悪意のあるアプリケーションに対する保護としては不充分である．実用化のために，アプリケーションルールの記述方式を改良する必要がある．

柔軟な個人情報の記述方式

アプリケーション作成者は，DTD に従う限り，自由に個人情報の項目を設定することができる．例えば，レンタルビデオ店で本フレームワークを用いて，ユーザの好む俳優の映画を紹介するアプリケーションを作成する場合，ある店では “好きな俳優” という要素を持ち，別の店では，“好きな男優”，“好きな女優” と分けることも可能であり，アプリケーションによって柔軟に対応することができる．

利便性

本フレームワークによってユーザの入力回答が増加することはないため，個人情報に適応したアプリケーションの本来の目的である利便性を損なっていない．よって，利便性は達成されたといえる．

7 結論と今後の課題

本稿では公共空間におけるアプリケーションのパーソナライゼーションを紹介し，実現

の際に問題となるプライバシの保護を行うための個人情報非送信型モデルを提案した．これを実現するための EA-P2 フレームワークの実装，評価を行った．本フレームワークを用いることで，ユーザは個人情報を保護しながら，個人情報に適応的なアプリケーションを利用することができる．一方で，アプリケーション作成者は，本フレームワークを用いることで，公共空間における個人情報に適応的なアプリケーション作成を容易に行うことができる．

本フレームワークの実用化に向けて，今後以下に述べる課題を解決する必要がある．

ユーザによる判断基準の導入

現在の実装では，アプリケーション作成者の自由度は達成されたが，個人情報の機密性が十分に達成されていない．そこでユーザによるアプリケーションルールへ提供する個人情報のカスタマイズを可能にする必要がある．

個人情報の処理

現在の個人情報の解析方式では，住所などの階層構造を持つ個人情報を扱うことができない．そこで個人情報の記述方式，解析方式を改良する必要がある．また，個人情報の追加，削除などの情報を編集する機能を提供する．

位置情報のプライバシ

本稿での対象アプリケーションが利用できる情報として，位置情報は重要である．今後は位置情報も考慮にいれた公共空間におけるアプリケーションのパーソナライゼーションについて考察する．また，その際に Mist[11] などで議論されている位置情報のプライバシ保護についても取り組む．

参考文献

[1] 本田良司，鈴木和弘，鳥原信一，久世和資：“アドホック・ネットワークとアクティブ電子広告版”，情報処理学会 コンピュータシステム・シンポジウム NO.13,pp.47-52, 東京（2000）
http://www.torihara.com/wit/ap/

[2] A.Knott and C.Mellish and J.Oberlander and M.O’Donnell, “Sources of Flexibility in Dynamic Hypertext Generation”, In Proceedings of the 8th International Workshop on Natural Language Generation, Herstmonceux Castle, UK, june 1996.

[3] Davies,N.,K.Mitchell,K.Cheverst,and G.S.Blair,“Developing a Context Sensitive Tourist Guide”, Technical Report Computing Department,Lancaster University.March 1998.

[4] World Wide Web Consortium
http://www.w3.org/

[5] Platform for Privacy Preferences Project, http://www.w3.org/P3P/

[6] Anonymiser
http://www.anonymizer.com/

[7] OpenSSL,http://www.openssl.org/

[8] 株式会社 内田洋行
http://www.uchida.co.jp/

[9] 青木崇行, 村瀬 正名, 松宮 健太, 中澤 仁, 西尾 信彦, 高汐一紀, 徳田 英幸：“Smart Furniture: Improvising Ubiquitous Hot-spot Environment”，情報処理学会情報家電コンピューティング研究グループ第 4 回研究会 Vol.4 November. 2002.

[10] SFC Open Research Forum 2002
http://www.kri.sfc.keio.ac.jp/ORF/2002/

[11] Jalal Al-Muhtadi, Roy Campbell, Apu Kapadia, M.Dennis
Mickunas, Seung Yi, “Routing Through the Mist: Privacy Preserving Communication in Ubiquitous Computing Environments”, http://citeseer.nj.nec.com/506969.html.

[12] W3C. Extensible Markup Language (XML) 1.0. http://www.w3.org/TR/REC-xml.