M-135

ユビキタスサービス基盤 (4)
～ユビキタス情報管理基盤～

A Ubiquitous Service Platform (4)
- A Ubiquitous Resource Management Platform -

谷 幹也† 山口 智治† 田口 大悟† 仁野 裕一† 高橋 三恵† 野田 潤† 柏谷 篤† 山田 敬嗣†

Mikiya TANI Tomoharu YAMAGUCHI Daigo TAGUCHI Yuichi NINO Mie TAKAHASHI Jun NODA Atsushi KASHITANI Keiji YAMADA

1. はじめに

ネットワークで接続された多様な情報機器によって，生活に密着した情報サービスが提供されるユビキタス環境が社会に浸透しつつある．我々は，このユビキタス環境において，人に優しく安全で便利なサービスを容易に実現できるユビキタスサービス基盤[1]の構築を目指している．

近年モバイル機器は，アドレス帳・メール履歴・クーポン券など様々な情報を扱えるようになり，サービスや個人に関する情報を保持できるようになっている．これによりモバイル機器内の情報（携帯情報）をユビキタス機器（POSやKIOSK端末等）と連携して活用することで，より簡単便利なサービスの享受が可能になってきている．例えば，携帯電話で保持している住所や氏名の情報を配送サービスの宛先として直接使用するなど，サービスの質や効率を向上することができる．このような使われ方が増加する中で，個人情報の盗用・流出等のプライバシー侵害の危険，情報のコピー・改ざん等による偽情報の危険などに対する不安も高まってきている．アンケート調査[2]においてもＥＣ参入への最大不安要因として，自己データの漏洩が 70%を超え，携帯電話による決済の問題点としては，①支払いトラブル 51%②個人情報の漏洩 49%③紛失の影響 47%という結果が出ている．本報告では，モバイル機器に保持した情報を保護しながら活用することで，より簡単・便利で安全なユビキタスサービスを提供できる基盤としてユビキタス情報管理基盤を提案する．

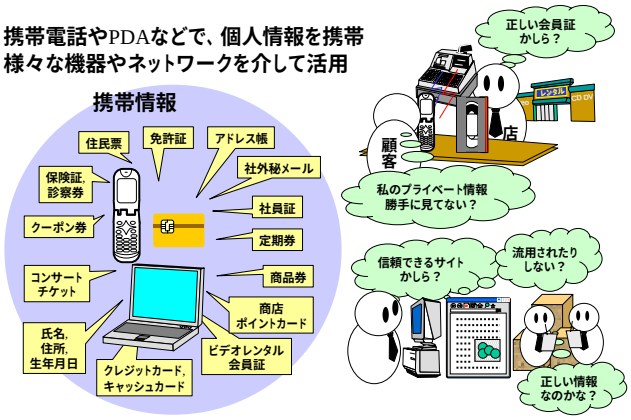

図 1 ユビキタス情報管理の対象

† NEC インターネットシステム研究所，Internet Systems Research Laboratories， NEC Corporation

2. ユビキタス情報管理基盤

2.1. 仮定する環境

ユビキタス環境下では，常時携帯性を持つモバイル機器(特に, 携帯電話)は個人認証デバイスとして利用することも多くなる．特に，コミュニケーションが主であったモバイル機器の役割が，個人が保持する様々な情報を蓄積保持し，これを活用してサービスを受ける個人用情報リポジトリへと変化していくことで，より一層強力な認証デバイスとして機能する．本報告では，モバイル機器が個人情報を格納するリポジトリとなり，モバイル機器とユビキタス機器が連携してサービスを受けられる環境を仮定する．このように格納された個人情報（＝携帯情報）は，利用時点での情報特性によって，図２の６つに分類することができる．

図 2 携帯情報の種類

一般的に個人情報とされるユーザ側作成情報の他に，サービス提供者側作成した情報として，他者への複製によって情報提供者側にリスクを生じさせる電子チケットなどの有価情報，著作権保護を行なう必要のあるコンテンツ情報がある．ユーザ側にリスクを生じさせるものとして，医療カルテなどのサービス履歴情報と電子証明書がある．それぞれの特性に応じて適切な管理を行なう必要がある．

2.2. 解決する課題

これら携帯情報が常時携帯されている端末に保持され，その重要度が上がるにつれ，次の二つの問題が生じる．まず，常時携帯性のゆえに増加する端末の破壊・故障・盗難による情報喪失問題がある．また，後者に起因する問題として，重要な情報が漏れたり，悪用されたりする漏洩問題がある．この二つの問題を解決するためには，携帯情報を安全に分散保持し(携帯情報管理), サービス提供のために授

受する情報を最小限にし(機器間認証・交渉), 他機器に提供後の情報もアクセス制御(保護流通)をする必要がある.

2.3. 解決手法

ユビキタス情報管理基盤は，次に述べる三つの必須構成要素とそれらを束ねる報流通モデルから成る(図３).

1) 携帯情報管理：端末の破壊や故障からの携帯情報保護を実現．様々な種類の情報に対する分散管理・同期機構.

2) 機器間認証・交渉：アドホックに機器を認証し流通可能性を確認できる認証機構と，サービス提供のために必要最小限の情報授受を実現する交渉機構.

3) 情報保護流通：著作権管理と同様の権利管理機構を個人情報に適用することで，携帯情報の目的外利用防止及び提供した個人情報の流通を追跡・管理する機構.

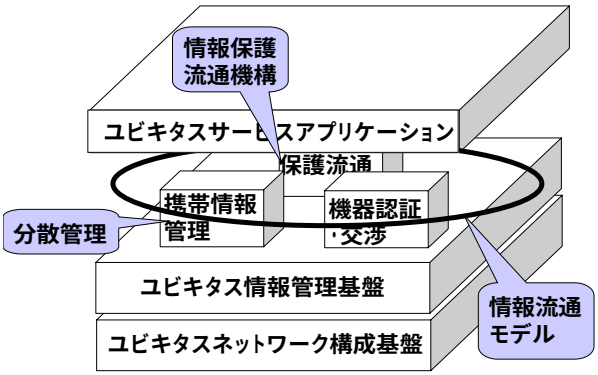

図 3　ユビキタス情報管理基盤の構成

3. ユビキタス情報管理基盤の構成要素

3.1. 携帯情報管理

端末の破壊／故障／盗難などによる携帯機器に格納される情報の喪失を防止するためには，ホーム PC，ネットワークストレージなどに分散格納し，バックアップ／リストアを行なえば良いように思える．しかし，図 2 にあるような様々な種類の情報を保持している場合，これでは十分ではなく, 情報の特性に合わせた柔軟な分散管理が必要になる．例えば，電子チケット，ポイントなどの有価情報では，バックアップ後の利用量を適切に反映しない限り不正利用につながる．このため，本基盤は，冗長性を持たせた分散格納，冗長情報への排他的アクセス制御，情報特性と機器特性とに応じた分散管理方式[4]を持ちこれを実現する.

3.2. 機器間認証・交渉

必要な情報を簡単に受け渡しすることで，ユビキタスサービスをより簡単・効率的に利用できることが，携帯端末に情報を保持する一つの強い要因である．しかし，プライバシー保護の観点では，サービスを受けるために提供する情報はできるだけ少ないことが望ましい．同様に，一度他機器に提供した情報に関しても他へ転送される際，各機器と情報自体が相互に認証し，最低限の情報交換を目指して逐次交渉を行ないながら流通することで，より安全な情報の授受管理を行なう事が出来る．ユビキタス情報管理基盤は，携帯端末とサービス提供機器との間でのスケーラブルな交渉手段を持つと共に，情報授受後も独自の情報流通モデル[3]を利用することによって，情報授受を最小化しながら効果的なサービスを受けることが可能である.

3.3. 保護流通

モバイル機器から情報を提供する際，情報を適切な機器にのみ公開するアクセス制御と，既に受け渡してしまった情報に関しても，目的外利用・不要な再転送を防止すると共に，流通した情報の追跡・管理を行なえる機構を持つことで，ユーザの不安を減少させ，ユビキタスサービス活性化につなげることができる．本基盤は，前者を実現する手段として，機器に含まれるプロファイル情報を利用した容易なグループ形成とグループ内秘匿通信を行える情報保護流通機構[5]を持ち，後者の実現には，流通する情報を自律オブジェクトとして扱かう独自の情報流通モデル[3]を持つ.

4. 関連研究

プライバシー保護に関しては既に標準化が進み P3P[6]や LibertyAlliance[7]の研究があるが，前者ではユーザ端末とサーバとの間での交渉方式が対象で，一度流通した後での情報漏えい防止はスコープに入っていない．後者では，ウェブサービス間での統一的な認証とプライバシー保護についての議論がなされているが，プロトコルとインタフェースが対象で，実現方式は論じていない．情報漏えい防止という観点でも，ルールベースフィルタリングなど，情報授受段階でのアクセス制御に関する研究は TIHI[8]等多数あるが，本基盤では，提供後の情報へのアクセス制御についても対象とすることでより安心できるサービス提供が可能となる.

5. おわりに

本報告では，モバイル機器に格納した情報を安全に利用するための基盤として，携帯情報管理，機器間認証・交渉，保護流通の三つの構成要素からなるユビキタス情報管理基盤を提案した．本基盤は，ユビキタスサービス実現のために我々が構築しているユビキタスサービス基盤のサブ基盤である．現在，それぞれの構成要素に関して，分散管理，保護流通モデル，保護流通機構を中心とした研究を進めている．今後，これらの開発を進めると同時に，ユビキタスネットワークサービス上で重要となるコンテキスト流通に関するアクセス制御についても着手し，システム全体の本格的実装，評価を行っていく予定である.

参考文献

[1] 柏谷他,ユビキタスサービス基盤(1)～ユビキタスネットワーク構成基盤，FIT2003.

[2] 総務省，情報通信分野の安全性と将来技術に関する調査，2002 年 2 月 Web 調査

[3] 田口他.ユビキタスサービス基盤(5)～情報流通モデル～,FIT2003

[4] 田口他.ユビキタスサービス基盤(6)～ユビキタス情報の分散管理～,FIT2003

[5] 野田他，ビキタスサービス基盤(7)～ユビキタス・オフィス・サービス～,FIT2003

[6] P3P，http://www.w3.org/P3P/(03/07/10)

[7] LiberyAlliance, http://www.projectliberty.org/ (03/07/10)

[8] Wiederhold, Gio: "Future of Security and Privacy in Medical Information"; in Renata Bushko (ed): *Future of Health Technology*, Studies in Technology and Informatics, vol.80, IOS Press, Amsterdam, 2002, pages 213-229.