

M-018

ICカードを用いたモバイル情報サービスシステムの提案

Study of Mobile Information Service System using Smart Card

三科 雄介†
Yusuke Mishina

佐藤 暁子†
Akiko Sato

本林 正裕† 及川 正規†
Masahiro Motobayashi Masanori Oikawa

1. はじめに

時間と空間の制約を越え、必要なサービスを楽しむことができるユビキタス情報社会の到来は間近にある。インフラ面では、携帯電話とICカードが近年目覚ましい発達を遂げ普及しつつある。サービス面では、利用者の置かれた環境や状況に応じて最適な情報を提供する、状況適応型サービスに向けた活動が盛んになりつつある^[1]。

本稿では、ユビキタス情報社会に向けたモバイル情報サービスシステムを提案する。まずインフラとサービスを概観し、ICカード内蔵型携帯電話の有望性を示す。次にシステム要件を分析し、携帯電話と情報キオスクの連携を特徴とするシステムアーキテクチャを提案する。さらに技術課題としてポリシー制御機能とプライバシー保護機能について検討する。最後にまとめと今後の課題を示す。

2. モバイル情報サービスシステム

2.1. システムインフラ

ユビキタス情報社会を支えるシステムインフラは、大きく2つに分けられる。

(1) 基幹インフラ

ネットワーク、サーバ、ストレージ等のバックボーン機器である。ユビキタス情報処理への対応には、高速化、大容量化、相互接続性、QOS制御等の拡張が必要となる。

(2) ユビキタス情報端末

近年、携帯電話やPDA等の携帯情報機器は爆発的に普及した。中でも携帯電話は、加入者飽和への対応策として、インターネット接続やアプリケーション実行等の機能拡張が2.5世代で実施された。この結果、需要が牽引されてユビキタス情報端末としての地位を確立した。

他方で、IT社会でのセキュリティ担保手段として、ICカードが急速に普及しつつある。そしてこれら2つのユビキタス情報社会のキープデバイスは、融合化し発達する方向にある。第3世代携帯電話はUIM (User Identity Module)を内蔵し、セキュリティを要する決済処理を可能とした。

以上を纏めると、第3世代携帯電話は、利用者に最も身近で信頼できるユビキタス情報端末として期待される。

2.2. サービスコンセプト

ユビキタス情報サービスに関しては、様々な検討がなされている。その本質の一つに「コンテキストウェアネス」が挙げられる^[2]。コンテキストウェアネスとは、人や事物の状況に応じて最適なサービスを提供する枠組みであり、その実現には、以下のステップが必要となる。

(1) 人や事物に付随して、コンテキスト情報を発信するユビキタス情報端末やセンサ端末

- (2) 上記端末とサーバを接続するユビキタスネットワーク
- (3) 上記コンテキスト情報を受信して利用するサービスロジックと、そのサービスロジックを実行するサーバ

上記前節で述べた第3世代携帯電話は、利用者の属性情報を安全に保持できるため、コンテキストウェアな情報端末として期待される。

3. システムアーキテクチャの提案

本章では、モバイル情報サービスとして、図1に示すタウン情報サービスを具体的な検討対象に選択し、より詳細に検討する。

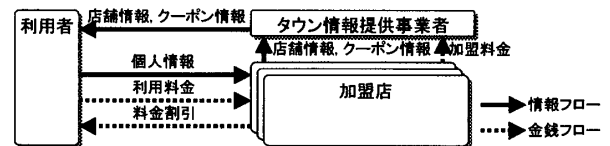


図1. タウン情報サービスの参加者モデル

まず、システム構築の要件と、対応方針を示す。

[要件1] 利用者と加盟店の双方に関してコンテキストウェアネスを有すること

この要件へ対応すべく、利用者と加盟店に関する属性と業務制約条件(ポリシー)を管理し、実行する機能を設けた。

[要件2] モバイル環境の利用者に高い利便性を与えること

[要件3] タウンという実世界環境を活かしたマーケティングを可能とすること

これら3つの要件へ対応すべく、利用者メディアとして携帯電話を、タウン情報提供事業者メディアとして情報キオスクを採用した。

システムの利用イメージを図2に従い説明する。

- ① 利用者は、携帯電話を用いて情報キオスクに接続する。
- ② 携帯電話に内蔵されたICカードチップには、利用者の属性(年齢や嗜好などの個人情報)が格納されている。利用者が許可した個人情報は、情報キオスクに送付される。
- ③ 利用者は、情報キオスクに店舗検索条件(店舗のジャンルや場所、価格など)を入力する。
- ④ 情報キオスクはサーバに接続し、上記②③で得た個人情報と検索条件に合致する店舗情報を検索し表示する。
- ⑤ 利用者は、表示された店舗情報から、必要な店舗情報とクーポン情報を、携帯電話にダウンロードする。
- ⑥ 利用者は、情報キオスクを離れて加盟店へ移動する。
- ⑦ 利用者は、加盟店で購買しクーポンを使用する。利用者が許可した個人情報が、加盟店に送付される。
- ⑧ 加盟店は、回収した個人情報に基づき顧客関係管理(CRM: Customer Relationship Management)を実施する。

以上示したように、本システムでは街というリアルな場所に情報キオスクを設置することで、容器要件3の街の状

† (株)日立製作所 中央研究所, Hitachi, Ltd., Central Research Laboratory

況に応じたマーケティングを可能としている。リアルマーケティングの一例として店舗と情報キオスクの距離に応じてクーポンの割引率を変更するなどが考えられる。



図2. タウン情報サービスの利用イメージ

4. 技術課題と対応

4. 1. ポリシ制御機能

タウン情報サービスで、利用者の属性に応じて店舗情報を提示するには、ポリシ制御機能が必要となる。

本稿では「ポリシ」を、情報サービスの運用に際してシステムが満たすべき制約条件と定義する。具体的には、制約条件はエンティティの属性をパラメタとする条件式で示される。例えば、「利用者(エンティティ)の年齢(属性)が20歳以上ならば、ワインのクーポンを提示する」は、タウン情報サービスでのポリシの一例である。

報告者らは、ICカード運用管理システムを対象としたGlobalPlatform(GP)のProfiles Specification^[3]をベースに、モバイル情報サービスに好適なポリシ制御方式を検討した。その結果 GP仕様には以下の問題点があることが判明した。

[問題1] セキュリティの問題

GP仕様では、ポリシをエンティティの属性群の一つとして定義する。このため制約条件の充足判定者に、判定には不要な属性を含む全ての属性が提示されてしまう。そして、制約条件の充足判定に不要なデータ転送が生じるため、データ転送効率が低下する問題がある。

[問題2] 制約条件の表現能力の問題

GP仕様では、ポリシを構成する制約条件を下記の様なXMLデータとして表現する。

```
<ConflictRule Source="CardProfile.ProfileVersion"
  Target="ApplicationProfile.ProfileVersion" Rule="="=>
```

GP仕様には、下記の制約が存在する。

- ①二項関係 Rule が、数値比較演算子に限定される
- ②比較対象値の型が、暗黙で数値型に限定される
- ③複数の ConflictRule の関係が、AND 並列に限定される

上記問題を解決する新たなポリシ制御仕様を検討した。

[対策1] ポリシは属性値とは独立して管理する

上記問題1は、ポリシを属性群の一つとして規定する点に起因する。そこで、ポリシを属性群から独立させた。さらにポリシの充足制約処理を2フェーズに分けた。まずポリシを収集して充足判定に必要な属性を決定し、その後に必要な属性のみを収集して充足判定する仕様とした。

[対策2] ポリシの制約条件の記述文法を拡張する

上記問題2は、記述文法の単純性に起因するため、下記に示す拡張を実施し上記①~③に対応した。

```
<Statement>
<Or> <Statement cond="c1" /> <Statement cond="c2" /> </Or>
</Statement>
```

```
<Cond-Group>
<Cond Name="c1" Ref="#CardProfile.OSPlatform" Rule="EQUAL">
<Value Type="String">JAVA</Value>
</Cond>
<Cond Name="c2" Ref="#CardProfile.OSVersion" Rule="LESS">
<Value Type="Decimal">2.1</Value>
</Cond>
</Cond-Group>
```

4. 2. プライバシ保護機能

本システムは、第3世代携帯電話内のICカードに格納した利用者の個人情報を用いて、コンテキストウェアなタウン情報サービスを実現する。ICカードを選択した理由は、ICカードの耐タンパ性により個人情報を保護するためである。しかしポリシ制御の制約条件の充足判定(以下、マッチング処理と呼ぶ)時に、ICカードから個人情報を読み出した時点で、ICカードによる情報保護の保障は失われる。

上記課題を解決するプライバシー保護方式を説明する。提案方式の基本コンセプトは下記の2点である。

- (1) マッチング処理は情報キオスクで実施する
プライバシーを最優先すれば、ICカードでマッチング処理を実施すべきである。しかし、ICカードチップの情報処理能力の面で非現実的なため、上記選択とした。
- (2) 情報キオスク内に、耐タンパ性を持つHSM(Hardware Security Module)を導入する。

ICカードとHSM間でセキュアチャネルを確立して利用者の個人情報を転送し、情報処理能力の高いHSM上でマッチング処理を代行実施する。マッチング処理終了後、転送された個人情報は破棄する。本方式により、マッチング処理の効率性は保ちつつ、情報キオスクより上流のサーバ側への個人情報流出を阻止することが可能となる。

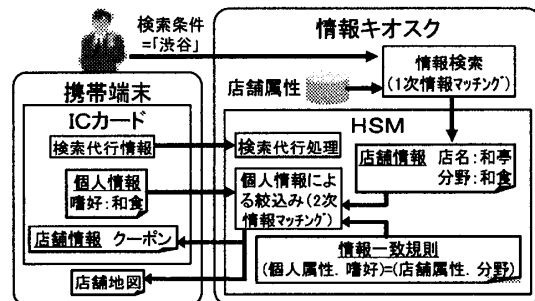


図3. 個人情報を保護する情報マッチング方式

5. おわりに

第3世代携帯電話内のICカードに格納した個人情報を用いてコンテキストウェアネスを実現する、モバイル情報サービスを提案した。現在試作システム第1版を開発終了し、その有効性を検証中である。今後の課題として、より高度な属性情報の流通制御方式の検討が挙げられる。

参考文献

- [1] "Goopas", <http://www/goopas.jp/noflash/top.html>, 小田急電鉄(株).
- [2] 中島 久雄: "ユビキタスネットワーク時代のマーケティング戦略", 知的資産創造, (株)野村総合研究所, 2002/1.
- [3] GlobalPlatform: "GlobalPlatform Systems Profiles Specification", Version 1.1.0, September 2003.