

ユビキタスサービスにおける アプリケーション利用環境の移動技術の開発

井谷 茂寛[†] 藤田 卓志[‡]富士通株式会社[†] 株式会社富士通研究所[‡]

1. はじめに

現在、個人がノート PC を持ち歩くモバイルコンピューティングが主流である。しかし今後は、行く先々の環境に用意されたデバイスやサービスを連携して実現される、ユビキタスサービスが主流となると考えている。

筆者らのグループで想定しているユビキタス社会は、多種多様なセンサや RF タグが街中に配置され、全てのデバイスはネットワーク I/F を標準で備え、各物品にも RF タグが添付されている世界である。その社会でのネットワーク利用者の周囲の環境に関する情報を「ネットワークコンテキスト」と定義し、そのネットワークコンテキストに基づいてリソースやサービスを制御するシステムを研究している[1]。

その一環として我々は、「アプリケーションコンテキスト」をコンピュータの利用環境と定義し、ネットワークコンテキストと連携することで、さまざまな環境でアプリケーションコンテキストを利用することを目指している。

本研究の目標は、このアプリケーションコンテキストを、移動中、移動先のさまざまな端末で安全かつ迅速(1 秒以内)に復元し、利用者に対してすぐに利用可能とすることである。

2. 課題とアプローチ

先にあげた目標を実現するためには、「環境の復元速度の高速化」、「アプリケーションコンテキストの管理方法」、「セキュリティ」の 3 つの課題が存在する。以下、個別に説明を行う。

2.1. 環境の復元速度の高速化

端末が利用可能となるまでには、端末の電源を入れてから OS が立ち上がり、ログイン画面が出るまでの「起動時間」と利用者のアプリケーションコンテキストを復元するための「復元時間」がある。「起動時間」については、利用者が専用で使用する端末ならば、常時電源を入れておくことで解決ができる。しかし「復元時間」は、利用者が特定してから復元作業を行うため、リモートデスクトップや VNC などの方法を使わない

限り、ある程度の時間がかかる。リモートデスクトップなどのリモート操作では、レスポンスやサーバ負荷の課題がある。このため、利用者がアプリケーションコンテキストを復元する端末に到着する前に、事前に復元を完了することにより待ち時間をなくすというアプローチをとった。

この前提条件の元、利用者が端末を利用したい時に管理サーバに対して利用要求を行い、管理サーバ側で利用者の位置情報を元に利用者が利用する端末を決定し、利用者を端末へ誘導している間に、アプリケーションコンテキストを復元する方法で実現することとした。

この場合、管理サーバが利用者の位置情報を取得する方法が新たな課題としてあげられる。今回の想定では、街角にさまざまな情報を記した RF タグが設置されており、利用者の携帯端末に搭載された RF タグリーダで RF タグに書かれた情報を取得したり、そのタグ ID を元にネットワークから関連づけられた情報を自動的に取得したりすることが可能である。この情報を利用して利用者の位置の特定を行うこととした。

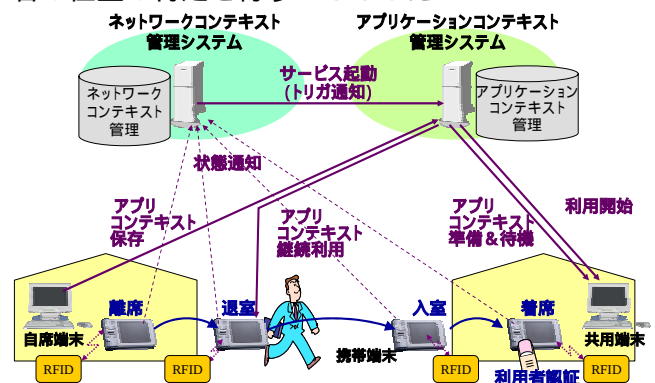


図 1 システム構成図

これを実現するために、図 1 のようなシステム構成とした。利用者は前記の通り、端末を利用したい場合に利用要求をだすこともできるが、会社や学校のように建物に入った時点で、自動的に利用する端末が決定される場合もある。ここではその利用をメインとし、利用者が端末から離れるとき、

2.2. アプリケーションコンテキストの管理方法

利用者のアプリケーションコンテキストを端末間で移動可能とするために、更に以下の 3 つの課題について検討する必要がある。

1. 利用者が普段利用するアプリケーションから、アプリケーションコンテキストをとりだしたり、設定したりする仕組みの確立
2. 各アプリケーション固有の情報を共通化するためのメタデータフォーマットの確立
3. 保存、復元時の矛盾解消の仕組みの確立
 - 1 については汎用的、共通な枠組みを作成する。
 - 2 のデータ保持方法については、各アプリケーションが保持するデータを調査し、抽象化を行う。具体的には、拡張子を用いたデータとプログラムの関連づけを参考にして、抽象化フォーマットを作成する予定である。
 - 3 については、端末上で復元したいアプリケーションがなかった場合や、設定すべき設定値が設定できないアプリケーションの対応方法などを別途矛盾処理としてルール化し、図 2 のように対応処理を記述する。

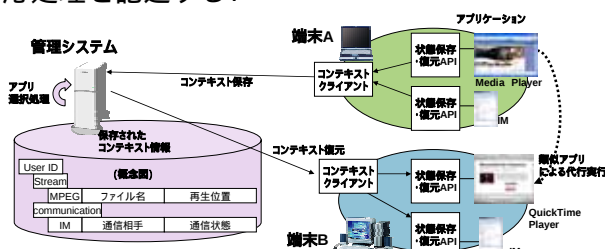


图 2 矛盾处理对处例

2.3. セキュリティ

システムで使用する通信には、接続先認証と通信路の暗号化を行い、各通信の盗聴やなりすましによるデータ改竄などの不正行為を防ぐ。また、環境を復元中の端末を正当な利用者以外に使用されないように、復元開始時に端末にスクリーンロックをかけることとした。また利用者が端末に到着した時に、携帯端末上の指紋センサ[2]を使用して本人確認を行い、管理サーバから復元端末に対してロック解除の通知を行うようにした。

3. 試作システム

図 1 のシステムの試作を行った。試作システムでは、保存・復元を行うアプリケーションとして Web ブラウザ (Internet Explorer) にしぼり、アプリケーションコンテキストとして、「表示 URL」、「画面サイズ」、「画面位置」とした。

利用した携帯端末は、富士通研究所で試作したポケットサイズの情報端末".u Pocket"[3]で、手のひらサイズの大きさに SVG の液晶, マルチ RF タグリーダ, 無線 LAN, Sweep 型指紋認証装置を備えている。管理サーバ, 自宅端末, 共用端末には PC を使用し, 管理サーバの OS は, RedHat Linux9 で、保存・復元用端末には Windows XP を用いた。

利用者の位置情報取得には、この“u Pocket”で自宅端末と共用端末にそれぞれ関連づけられた RF タグを読み取ることで行う。図 1のように部屋の入室時に RF タグを読み取り、利用者が共用端末に到着するまでにアプリケーションコンテキストを復元することができた。

現在、利用者の退室時に自動的にアプリケーションコンテキストを保存して端末を終了する処理が未実装であるが、コントローラとなる携帯端末から各端末をリモートで保存し、その後終了したり、復元操作が可能であり、利用者が部屋から出たり、端末から離席したりしたイベントに対して、このリモート保存処理やリモート復元処理を実行する部分を作り込めば、図 1 の構成を実現した試作システムとなる。

4. まとめ

今回の試作により、利用者が端末の前に来た時点ですぐに以前の作業状態から作業を開始でき、利用者がログイン、ログアウトなど煩雑な処理を意識せず、Web ブラウジングに専念できる環境が構築できた。今後は、更にシームレス化を実現し、実証実験を行う予定である。

謝辭

本研究は、平成 16 年度 総務省委託研究(ユビキタスネットワーク制御・管理技術の研究開発)により実現したものである。関係各位に深く感謝致します。

参考文献

- [1] 高瀬,五十嵐,武吉,掛水:”状況依存型サービス起動及びリソース検索方式”,電子情報通信学会,ネットワークシステム研究会,NS2003-243
- [2] 森,佐々木,新崎:バイオメトリクス認証技術,雑誌 FUJITSU 2003-7月号,Vol54,No.4,P.272.
- [3]<http://pr.fujitsu.com/jp/news/2003/10/31-1.html>