社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2006－MBL－36（56）
2006－UBI－10（56）
2006／2／17

セキュアタグを用いた アプリケーション環境の保存・移動技術の開発

板崎 輝† 塩津 真一† 稲野 聡† 井谷 茂寛† 山田 勇†

†富士通株式会社 〒674-8555 神奈川県川崎市中原区上小田中 4-1-1

E-mail: †{akira.itasaki, sshiotsu, inano, s.idani, yamada.isamu}@jp.fujitsu.com

あらまし PC などのコンピューティング環境を持ち歩く現在のような使い方だけではなく,行く先々のコンピュータ上に各自の環境を移動させ,利用するシーンが今後広まっていくと筆者らは考えている.このような利用シーンにおいては,位置情報を基に各自の利用環境を行く先々のコンピュータ上で安全かつ迅速に復元する機能が必要となる. これを実現するためには位置検出技術が必要となり,筆者らが開発したセミパッシブ型セキュアタグシステムを適用することにした.これは通常の RFID タグに比べ,必要な時以外は電波を発しないセキュリティやプライバシーに配慮したタグシステムである.本論文では,我々の目指すサービスの実現例と,それを実現するために使用したセキュアなタグシステムを中心に報告する.

キーワード RFID，アクティブタグ，RFID システム，セキュリティ，位置管理

The Development of the Save and Movement of Applications Environment with Secure RFID tag System

Akira Itasaki† Shinichi Shiotsu† Satoshi Inano† Idani Shigehiro† and Isamu Yamada†

†FUJITSU company limited 4-1-1 Kodanaka, Nakahara-ku, Kawasaki city Kanagawa, 674-8555 Japan

E-mail: †{akira.itasaki, sshiotsu, inano, s.idani, yamada.isamu}@jp.fujitsu.com

Abstract: We are carrying about mobile PC now. It will be expected that each one's PC environment is moved to the PC placed at destination without mobile PC. In such a use scene, we will need the functions that restore user's PC environment safely and promptly on various PCs. To achieve such functions, we started this research.

Because the system required the positional detection technology, we decided to apply the secure semi-passive RFID system that authors had developed to it. This tag system doesn't emit electric waves to keep security and privacy compared with usual RFID tag system. In this thesis, it reports the example of achieving the service at which we aim and the RFID system that uses it to achieve it.

Keyword RFID, Active tag, RFID System, Security, Location management

1. はじめに

個人のコンピューティング環境として,現在は個人がデスクトップPCやモバイルPC等のコンピュータを所有し,その場所で,あるいは持ち運んで使用するという使い方が主流である.しかし今後は,これらの使い方に加えて,行く先々にあるコンピュータやネットワーク等の環境を利用して個人のコンピューティング環境を実現し,場所によらず継続してアプリケーションやサービスの利用を可能としたユビキタスサービスが実現され普及すると考えている.この実現には,起動中のアプリケーションの種類,ファイルの状態など”アプリケーションコンテキスト”と呼ぶ個人のコンピューティング環境の状態を迅速に保持し,移動,復元させる必要がある.

そこで我々は,ネットワークで結ばれた様々な環境下でアプリケーションコンテキストを自動保存し,移動先で迅速に復元するための技術開発を行った.開発における課題として, 利用者が待つことなく端末を利用するための「環境の復元速度の高速化」,利用者の状態や移動などに伴って,情報をシステム全体で安全に扱う「セキュリティ」,利用者の移動を検知し環境の復元速度を高速化するため

の「RFID タグによる位置検出」が挙げられる.

このうち,「環境の復元速度の高速化」については次章で,「セキュリティ」については 3 章でそれぞれ述べる.4 章では,この技術を実現するにあたって必要な位置検出手段に利用した,セミパッシブ型タグシステムについて述べる.これは我々のグループが開発した RFID タグシステムであり,セキュリティを確保した上で,従来のアクティブ RFID タグと同程度の通信距離等の性能を持つ. 5 章ではこの技術を元にアプリケーションコンテキストを自動的に保存・移動するシステムの試作について述べ, 6 章で本論文をまとめる.

2. 環境の復元速度の高速化

端末が利用可能となるまでにかかる時間には,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,ログインから利用者のアプリケーションコンテキストを復元するまでの「復元時間」がある.「起動時間」については常時電源を入れておく等の手段で解決できる. 一方「復元時間」は,利用者が利用端末を特定してから復元作業を行うため,利用者が端末に到着してから復元作業を開始した場合,利用者がその間,端末の前で待つことになる.この問題を解決するため,利用者が端末に到着する前にそれを検知し,アプリケーションコンテキストの復元作業を開始しておくことにより,待ち時間を短縮するというアプローチをとった.

この場合,利用者が使用する端末を管理サーバが先に決定する必要が生じる.今回は,利用者がセミパッシブ型セキュアタグ（以下タグ）を所持し,それを読み取るリーダライタを各端末および移動先の部屋の入り口に配置することによって実現した（図 2-1 参照）.ここで, 管理サーバは,利用者のアプリケーションコンテキストと位置情報の管理,利用者が移動先で使用する端末を決定するための機能を有する.タグについては 4 章で詳しく説明する.

以下, 復元速度高速化の具体的なしくみについて述べる.利用者が移動元の情報端末から離れたとき,端末はスクリーンロック後,管理サーバに通知し,管理サーバは

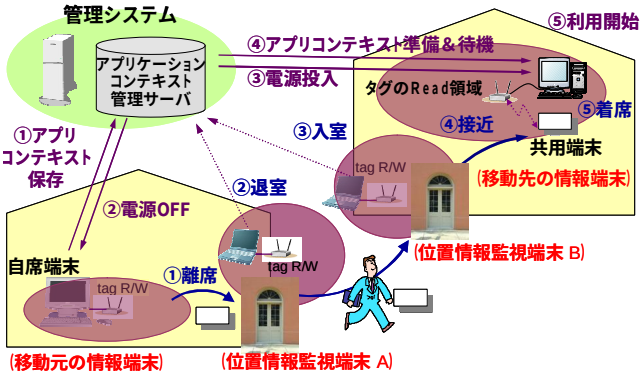

図 2-1 システム構成図

アプリケーションコンテキストを保存する.退室したとき,位置情報監視端末からサーバへとその情報が通知され,サーバは一定時間経過した後,利用者が再入室しなければログアウトし,端末の電源を落とす.入室の場合も同様に位置情報監視端末からサーバへと通知され,サーバは入室した利用者に対応する端末の電源を入れる.さらに, その端末上にアプリケーションコンテキストを復元する.尚, 利用者は,端末を利用したい場合に別の端末から利用要求を出すこともできる.通常は,移動先の建物（部屋）に入った時点で管理サーバによって自動的に利用する端末が決定される.

これらにより利用者は使用中の端末から席を立ち,移動先の端末に着席後,即座に以前の環境から作業を進めることが可能となる.

3. セキュリティ

リーダライタ,端末,サーバ間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,環境を復元する端末を正当な利用者以外に使用されないように,環境の復元開始から利用開始まで端末にスクリーンロックをかけることとした.今回試作したシステムでは,利用者が端末に到着した時に FeliCa カード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えるようにした.タグのセキュリティについては次章の認証方式の項で説明する.

4. RFID タグによる位置検出

2 章「環境の復元速度の高速化」で述べたように,その実現には特定な利用者の入退出や端末に着席していることを安全に適切な距離範囲で位置検知する必要がある.今回のシステムでは位置検知に我々が開発した方式のセミパッシブ型セキュアタグを用いた.

4.1. RFID タグの比較

タグの分類を表 4-1 に示す.位置検知に使用する RFID の選択にあたっては,セキュリティ上利用者の位置を第三者に検知されないこと,部屋に存在していることを検知可能な通信距離があることが求められる.

まず,パッシブタグとアクティブタグを比べた場合,アクティブタグは電池を搭載することで非搭載のパッシブタグに比べ通信可能距離が長くなるが,一定時間ごとに常時電波を送信するため,容易に傍受,追跡される恐れがあり,セキュリティ的に問題がある.

UHF 帯のパッシブタグの場合は,リーダライタからの問い合わせに対してのみ応答するため不要な電波の送信は無い.しかし ID を含む通信信号が暗号化されていないため,偽造リーダライタからの問い合わせにも応答する恐れや,傍受によって ID と個人とが関連付けられてしまう恐れがある.一般的にパッシブタグはコスト優先のため,セキュリティ対策を施してないのが実情である.

項目	パッシブタグ (UHF)	アクティブタグ	セミパッシブタグ (提案方式)
通信距離	～4m	＞10m	～10m
セキュリティ強度	○	× (常時送波)	◎
コスト	◎	△	△
適用先	物流 流通	人 (場所限定)	人 (制約無し)
拡張性	×	○ (センサ付加)	◎ (センサ付加、ネットワーク化)

表 4-1　各種 RF タグの比較

今回,我々が開発し本システムに使用したセキュア・セミパッシブ方式の RFID システム（以下,提案方式）は,従来のアクティブタグの通信距離を維持しつつ,セキュリティ強度を UHF 帯のパッシブタグ以上に強化したことを特徴としている.また従来のアクティブタグが送信専用であるのに対し,提案方式は受信機能も搭載しているため,ネットワーク化への対応等の拡張性にも優れている.

4.2. セミパッシブ型タグ (提案方式)

提案方式のタグは，電波の傍受,追跡を防ぐため,パッシブタグと同様にリーダタイタからの問い合わせに対してのみ応答する方式とした．さらに,問い合わせに対し応答すべきリーダライタを特定し、偽造リーダライタへの応答を防ぐため,リーダライタとタグ間で相互認証を行う方式とした.図 4-1 にリーダライタ-タグ間の認証処理フローを示す.

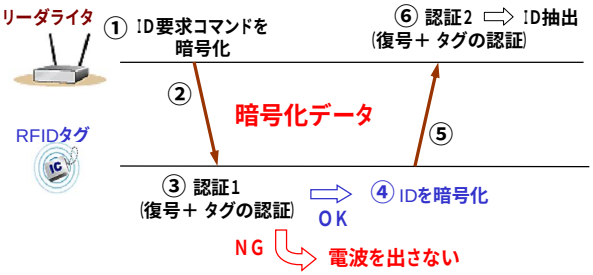

図 4-1 リーダライタ,タグ間の認証処理フロー

リーダライタとタグは,それぞれ暗号化のための鍵を所持する.さらにタグ側には,自分自身の ID を所持する.これらは秘密に保護されねばならない.

通信フローとしては,①リーダライタは ID 要求コマンドを暗号化し,②タグへ送信する.③リーダライタからの信号を受信したタグは認証処理を行い,認証に失敗した場合は,不当なリーダライタからの問い合わせと判断し,タグはアクションを起こさない（電波を送信しない）.認証に成功した場合はコマンドを実行する.例えば ID 要求コマンドの場合は,タグ ID を返信する.その場合も,④タグは ID を暗号化した上で⑤リーダライタへ送信する.⑥タグからの信号を受信したリーダライタは認証処理を行った後,認証に成功すれば正当なタグからの応答と判断し,ID を抽出し,処理を完了する.

これらにより正当なリーダライタからの問

い合わせのみにタグが応答するセキュアなシステムを実現している.

5. 試作システム

提案方式の RFID タグによる位置検出を含めたアプリケーション保存・移動システムの試作を行った.そのシステム構成を図 2-1 に示す.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), 文書作成ソフト（Microsoft Word）, 表計算ソフト（Microsoft Excel）を選択した.アプリケーションコンテキストとしては,「表示 URL」（IE）,「作成したファイル」（Word, Excel）,「画面サイズ」,「画面位置」とした.

管理サーバ,自宅端末,共用端末,位置情報監視端末には PC を使用し,管理サーバの OS には RedHat Linux 9 を,自宅,共用,位置情報監視端末には Windows XP を用いた.位置検出には前述の提案方式の RFID タグを使用した.

利用者の位置情報取得は,RFID タグをリーダで読み取ることで行う.図 2-1 に示すように,①端末から一定距離以上離れた際には端末のロック,アプリケーションコンテキストの保存を自動的に行う.②退室後,一定時間経過後には端末の電源を落とす.③入室時には RFID タグを読み取り,利用者が共用端末に到着するまでに電源投入し,④アプリケーションコンテキストを復元する.⑤その結果,利用者は着席と同時に作業を継続できる.

以上の動作を位置情報監視用端末での検知・通知や,管理サーバでのデータデースの情報による復元端末の特定とコンテキストの復元作業の開始を連携して行うようにし,その動作を確認した.また,アプリケーションコンテキストを復元した段階ではスクリーンロックをかけ, FeliCa カードを用いてログイン認証を行うという動作も確認した.これによって,利用者は起動時間待ちやパスワード入力に煩わされることなく作業を継続できる.

6. まとめと今後の展開

今回,アプリケーション環境の保存・移動の実現について検討し,試作システムを構築した.そして試作システムにより,利用者が端末の前に着席した時点ですぐにWebブラウジングや文書作成,表計算など,移動前の作業を継続して行えることを検証した.

今後は,今回提案したタグ機能と FeliCa 機能を携帯電話などの携帯端末に付加することで,様々な場所での位置検知と連動させ,利用者が移動中にも携帯端末を用いてアプリケーション環境を安全に継続して使用できるシステムを構築していく予定である.

謝辞

本研究は,平成 17 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.

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] 井谷,藤田:”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”第 67 回情報処理学会全国大会

[4] 山田:” Secure Active RFID Tag System” Ubicomp2005 Workshop