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

2007－MBL－40 (25)
2007－UBI－13 (25)
2007／2／23

個人の特定と測位情報を制御可能な相互認証型タグシステム

森川 知憲
立命館大学理工学部
Inchoh@ubi.cs.ritsumei.ac.jp

西尾 信彦
立命館大学情報理工学部
nishio@cs.ritsumei.ac.jp

概要

近年，RFID 技術の発展に伴い RFID を用いたサービスが増加してきた．しかし，現在使われている RFID では第三者に簡単にデータを読み取られてしまう危険や，利用者のプライバシーに配慮されていない．本稿では RFID の持つ問題点を解決し，RFID を用いて個人のコンテキストに応じたサービスの提供を安全に行えるタグシステム提案をする．提案するタグシステムは，画像処理と RFID 技術を組み合わせて，利用者の位置情報や個人情報，プレゼンスなどのプライバシー情報が利用者によって制御できる相互認証型タグシステムである．

キーワード： RFID, 画像認識, 個人認証, 位置測定

Mutual Authentication type Tag System that Protects Personal Private Information

Tomonori Morikawa Nobuhiko Nishio
Department of Computer Science, Ritsumeikan University

ABSTRACT

Recently, the number of services with RFID has increased as RFID technologies have been developed. However, those services have been risked on the great danger such as easy theft of user data. Moreover, they have exhibitted a lack of concern for user's privacy. In this paper, we solve these problems and propose the Tag System, which has the capability of safely providing services such as personal context. The Tag System is a mutual recognition type system in which user can control their own private information such as their location, condition and so on by with combining image processing and RFID technologies.

Keyword: RFID Technology, Vision Recognition Processing, Personal Authentication, Location System

1 はじめに

近年，RFID 技術の発展に伴い RFID を利用したサービスが増加してきた．しかし，現在サービスに利用されているパッシブ型 RFID やアクティブ型 RFID は第三者にデータを読み取られる危険がある．また，RFID のデータを読み取っているリーダが信用のできるリーダであることを確かめなければならない．本研究室では RFID 技術を用いてプレゼンス情報を利用する実証実験を行った．1 つは学童を見守るシステムで，RFID のリーダが学童の持つ RFID を検知するとカメラで登下校を撮影して学童の登下校を見守るシス

テムである．このシステムではRFIDを持つ学童がカメラで撮影されたことがわかるが，カメラの画像内に複数の学童が写っている場合に，該当する学童がどこに写っているのかわからない結果となった．画像内での人物特定ができるようにカメラ認識と利用者の特徴情報を用いてシステムが判断できるようにならなければならない．そして，もう1つはカラータグを持った利用者に対して，カメラで利用者のカラータグを認識し利用者の近くに情報を配信するシステムである．このシステムでは，利用者の近くに情報提供が行えているが，その利用者に合わせた情報の配信ができていない．利用者の嗜好に合った情報を配信するためにも，個人を特定し利用者の嗜好情報を反映した情報の提供ができるシステムでありたい．しかし，システム側がカメラを用いて個人を特定ができると公共空間ではプライバシー侵害の恐れがあるため，利用者の意思によってプライバシー情報の制御が行えるシステムでなければならない．本稿ではユーザとシステムの相互認証型のセキュア通信が行え，画像処理とRFIDを組み合わせた位置情報の取得できるタグシステムを提案する．また，本タグシステムでは利用者の意思でプライバシー情報が制御できる設計である．

本稿の構成は全7章で構成され，2章では本研究室が行った実証実験に関する概要と評価，課題をまとめる．3章ではセキュア通信が可能なRFIDの研究と位置情報を取得できるタグを紹介する．4章ではシステムの概要を述べ，5章では，プロトタイプ実装について述べる．6章ではプロトタイプ実装に関する評価を述べ，7章でまとめる．

2 本研究の背景

本章ではタグを用いた実証実験に関する評価，課題をまとめる．

・学童見守り

街中の自動販売機をRFIDリーダと監視カメラを取り付けてネットワークにつなぎ，RFIDをつけた小学生の登下校見守りのためのトレースシステム[1]を構築し，実証評価した．小学生にはUHF帯のパッシブ型タグと426MHz帯のアクティブ型タグをハイブリッドに着用してもらい，アクティブ型タグにより自販機の側にいるというプレゼンスを把握し，パッシブ型タグにより正面の通過のタイミングを検知した．しかし公共空間における監視カメラの設置にはプライバシー侵害の恐れを常に伴なうため，監視カメラでは撮影すべき小学生のパッシブ型タグが認識されたときのみ撮影した．図1は撮影された画像である．図より明かであるように，複数の人物が撮影されるとカメラはどの人物がタグづけされた小学生かを認識できていない．

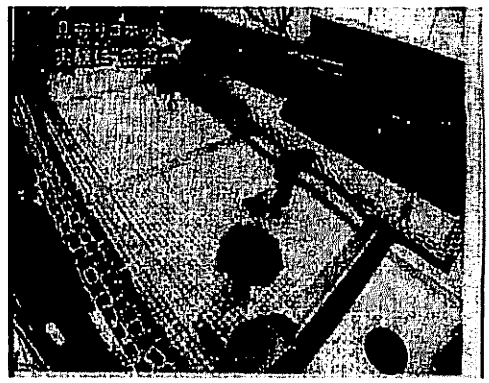

図1 学童見守り

パッシブ型タグはアクティブ型タグに比べ測位範囲が狭いため分解能が高いように思われるが，図1の状況からわかるように人物特定までは至らない．画像内での人物特定ができるようにするためカメラ認識と利用者の特徴情報を用いてシステムが判断できるようにならなければならない．また，カメラでの人物特定ができるよになるとプライバシーに配慮することも課題となる．プレゼンス情報などのプライバシーを利用者が制御できるタグが必要である．

・Wonder Wall

研究室と企業との共同研究で行われている街中広告配信のシステム[2]がある．本システムはプロジェクターを用いて壁に大画面を作り街中を歩く人の移動に合わせてコンテンツを追尾させて，情報を配信するシステムである．図2は実証実験の様子である．このシステムでは利用者が持っているカラータグを認識して，利用者の移動に合わせてコンテンツを変化させて追尾させる仕様になっている．三条あかり景色[3]という京都の古い建物をスクリーンとして作成したコンテンツを映し出すイベントに合わせて，このシステムの実証実験を行った．この実験では利用者の位置情報を取得して利用者の位置に合わせた情報提供が可能となった．しかし，街中情報配信システムをより便利に使用するためにも個人を認証し，個人の嗜好にあった情報を提供することが必要不可欠となる．

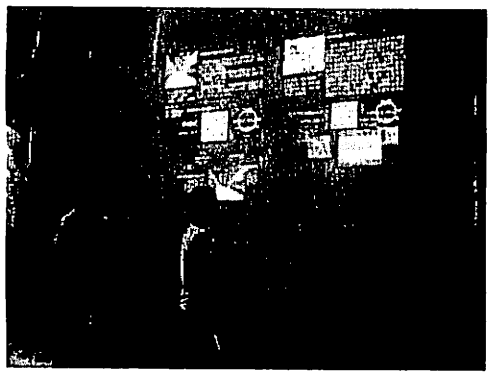

図 2　街中情報配信システム

・問題意識

学童見守りでは複数の人数がカメラに写っていると学童の正確な位置情報がわからなければ特定できない問題点があった．また，Wonder Wall では利用者の位置情報の取得はできているが，個人の特定を行っていないため，利用者の嗜好に合わせた情報配信が出来ていない．個人認証と利用者の位置情報を扱うタグシステムがあれば，利用者により快適なサービス提供が可能になる．しかし，サービス提供側が利用者のプレゼンス情報や嗜好情報を入手しサービスを提供するのは，プライバシー情報管理の観点からは利用者は望ましくない点である．そこで，本研究では個人の特定と位置情報が利用者の意思によって制御できるタグシステムを設計し，プロトタイプ実装をする．

3　関連研究

本章では既存研究を述べる．

3.1　セキュア RFID システムの開発

セキュア RFID システムの開発 [4] では双方向通信のできるアクティブ型 RFID を用いたセキュア RFID システムである．この研究では，利用者がアクティブ型 RFID を持っている場合に，第三者がアクティブ型 RFID のリーダを持っていれば，利用者の存在を容易に知られてしまう問題点を解決した研究である．サービスを提供する側からのリクエストによって初めて利用者のアクティブ型 RFID は電波を出す設計であり，不要に電波を出すことなく第三者にデータを読み取られる危険もない．また，この設計では従来のアクティブ型 RFID と同じバッテリー寿命を達成しており，省電力化が計られている．通信経路データも時刻を混ぜて暗号化することにより，通信経路に流れるデータを毎回違うデータで送るように設計されており，よりセキュアな通信を可能としている．

3.2　赤外線を用いた屋内位置取得

赤外線を用いた屋内位置測位システム [5] では，システムの要求に対して赤外線 LED を光らせて，画像処理により光を特定し利用者の位置を取得するというものである．このシステムでは WirelessLAN を用いて個人端末へ命令を送り，その命令に対して利用者の赤外線 LED が光る仕様となっている．赤外線透過のフィルムを使うことにより，可視光線をカットして赤外線 LED の光だけが位置測位システムに見える状態となる．

4　システムの構成と設計

本章では満たすべきシステム要件とシステムの構成，システムフロー，システム設計を述べる．

4.1　システム要件

本稿で提案するタグシステムの満たすべき要件は下記の通りである．

・双方向認証

従来通りに利用者側を認証してシステムがサービスを開始することに付け加え，認証を行うサーバ側が信用できる認証サーバであるかを特定することも必要となる．

・経路内での暗号化

第三者に送受信しているデータがわからないように，経路内を流れる情報は暗号化が必要である．

・位置情報の取得

利用者の位置情報を特定するために，画像処理を用いて認証システムが利用者の判断ができるように，決められたパターンで点滅するように命令をだす必要がある．また画像認識から利用者を見失っても，再度，利用者の位置情報取得できる必要がある．

・点滅パターン決定アルゴリズム

点滅パターンを第三者が容易に推定出来ないように，毎回点滅パターンを変える必要がある．

・プライバシーコントロール

利用者が快適にサービスを受けるためにもプライバシー制御を行い，利用者の要求に合わせたサービス提供を行う必要がある．

・Vision におけるプリアンブル

画像認識を行う場合に，利用者の端末がサーバによって決められたパターンに点滅を始めていいか判断を行うのに必要となる．また複数人が同時に点滅開始のプリアンブルを送信することにも対応が必要である．

4.2 システム構成

システム構成に関する各機構が行っている処理を述べる．図 3 はシステム構成図である．RF 通信経路では共通鍵方式の暗号化が行われている．

・個人端末

個人端末ではアクティブ型 RFID を用いて同調機構と通信を行っている．また，個人端末は自分の位置を知らせるために発光できる．利用者は個人端末でプライバシーレベルの設定ができる．

・画像認識機構

画像認識を用いた利用者の追跡及び Vision 信号を受信する．

また，画像認識機構ではカメラに利用者が写っている場合は追跡を行っており，位置情報を同調機構に送信している．

・画像認識と個人端末との同調機構

画像認識で認識した利用者を個人端末からの情報と関連付けて，利用者の位置情報の取得と個人認証を行う．

・サービス提供機構

画像認識と個人端末との同調機構より得られた個人の位置情報を基にサービスを提供する．

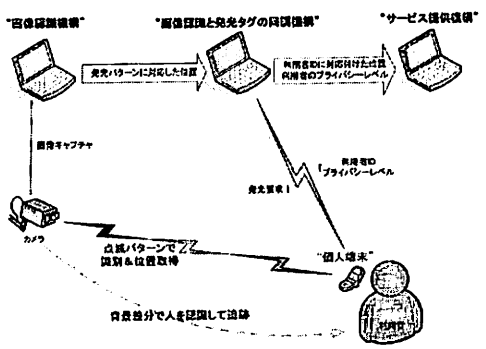

図 3 システム構成図

4.3 システムフロー

図 4 はシステムフローを表している．図中の数字は各機構での処理を表していて，内容は各機構で述べる．

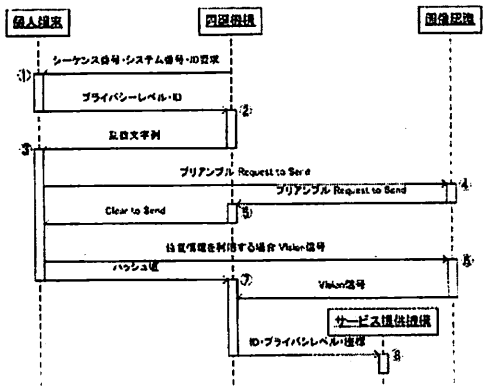

図 4 システムフロー

始めに同調機構から個人端末にシーケンス番号・システム番号・ID 要求を送信する．

1 では，同調機構より受信したシーケンス番号が適正であるか判断する．不適切な場合は個人端末が応答することなく終了する．システム番号がサービスごとに割り振られており，各サービスに対応したプライバシーレベルを参照する．参照したプライバシーレベルがサービスを受ける設定であれば，プライバシーレベルと ID を認証サーバへ送信する．

2 では，乱数文字列を生成し個人端末へ送信する．個人端末より受信した ID よりパスワードを呼び出して，乱数文字列と合わせてハッシュ化を行う．個人端末より受信したプライバシーレベルが位置情報を使う設定ならば，ハッシュ値を用いて Vision 信号の点滅パターンを決定する．

3 では，同調機構より受信した乱数文字列を用いて ID と共にハッシュ化を行う．プライバシーレベルで位置情報を使うように設定されているならば，ハッシュ値を用いて Vision 信号の点滅パターンを決定する．また，画像処理機構に Vision 信号を送信するならば，通信を開始するというプリアンブルを画像認識機構に送信する．同調機構からプリアンブルの応答があれば，ハッシュ値を同調機構へ送信し，Vision 信号は画像認識機構に送信する．プリアンブルの応答がない場合は一定時間待ち，再度プリアンブルを送信する．

4 では，個人端末より受信したプリアンブルを同調機構に送信する．

5 では，画像認識機構よりプリアンブルを受信すると，同調機構が個人端末からの Vision 信号を受信できる場合，個人端末に Clear to Send を送信した．

6 では，個人端末より受信した Vision 信号を同調機

構に送信する．

7では，個人端末から受信したハッシュ値が正しいデータであるか判定して個人認証を行う．個人認証ができたならば，サービス提供機構にプライバシーレベルを送信する．また，プライバシーレベルが位置情報を使う設定になっているならば，画像認識機構より受信したVision信号をハッシュ値と合わせて個人認証を行う．その後，プライバシーレベルと利用者の位置情報をサービス提供機構に送信する．

8では，同調機構より受信したIDとプライバシーレベルを基に提供するサービス内容を生成する．また，受信した座標より利用者へのサービス提供位置を決める．

利用者が位置情報を使う場合に画像内から利用者を見失えば，2の処理より再度利用者の位置情報の取得を行う．

4.4 システム設計

システム要件を基にシステム設計を述べる．

・双方向認証

双方向認証では3章で述べたセキュアRFIDシステムの開発と同じ仕様で設計を行う．また，双方向認証でのRF経路の暗号化についても同じ仕様である．

・経路内での暗号化

双方向認証が成立した後で行われている処理では乱数文字列やパスワードと乱数文字列のハッシュ値がRF経路でやりとりされるため毎回異なる暗号文が流れる．

・位置情報の取得

位置情報の取得では認証サーバがカメラの画像内にいる利用者の位置を特定する．画像内で利用者を特定するためには点滅パターンを決定しておく必要がある．

・点滅パターン決定アルゴリズム

点滅パターンを決定するためにハッシュ値を用いて決定する．ハッシュ値を使用することで，毎回異なった点滅パターンを生成することが可能である．またRF経路を流れるハッシュ値を点滅パターンに振り分けることにより，RF経路の暗号強度も向上出来ると考えられる．ハッシュ値は１６進数の４０桁で構成され，ハッシュ値の上位２桁を用いて，上位２桁を加算し，上位４桁，下位５桁を除く３１桁から点滅パターンを決めるハッシュ値を１桁抜き出す．抜き出されたハッシュ値を１６進数から２進数に直し，0なら消灯，1なら点灯と4 bitの点滅パターンを作成する．図5は点滅パターンを決定するためのアルゴリズムを分かり易く図示したものである．

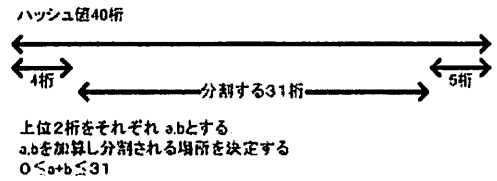

図5 点滅パターン決定アルゴリズム

・プライバシーコントロール

利用者に合ったサービス提供が選択できる必要があるため，プライバシーの制御が必要不可欠である．利用者はサービスに合ったプライバシーレベルを設定しておき，サービスの利用環境に入るとシステムがプライバシーレベルに応じたサービスを開始するものである．プライバシーレベルの設定は，位置情報を使う・個人認証をするを組み合わせた4パターンと，サービスを受けないを足した5段階で設定する．

・Visionにおけるプリアンブル

画像処理を用いて，画像内での信号をやりとりを行う場合に，認証サーバ側がデータを受ける状態であるか判定するために必要である．個人端末から認証サーバへの受信要求を点滅信号として流し，認証サーバがそれに応答すると，個人端末からの点滅信号が送られる．

5 プロトタイプ実装

本章では本システムの現在の実装に関して述べる．

5.1 動作環境

プロトタイプの動作環境としてはThinkPad X60s [6]を用いて認証サーバを構築している．認証サーバはJavaで記述しており，画像認識もこのPCで動作している．画像認識を行うカメラとして，Logicoolの Webカメラ QcamFusion [8]を用いている．個人端末としてはDoCoMoのSH902i [7]を使用している．本携帯電話に搭載されているピクチャーライトをiAppliから使用して，認証サーバへの点滅信号を送信している．

5.2 現在の実装状況

現在の認証サーバと個人端末の通信は，RF通信の代わりとしてインターネット上にある認証サーバと携帯電話網を介して通信をする実装を行っている．認

証サーバから乱数文字列を送信して，個人端末がIDと乱数文字列を混ぜたハッシュ化を行い，さらにハッシュ値を基に点滅パターンを決定する．認証サーバはハッシュ値と点滅パターンを個人端末から受信し，認証サーバと個人端末からのデータが一致すれば，個人認証する実装である．点滅によって送られるパターンは4bit，１６通りである．点滅パターンを挟むように点灯を1bitづつ付加しているため，点滅で送る信号は全部で6bitとなる．

6 評価

本章では，5章で述べたプロトタイプ実装の評価を述べる．

6.1 評価

プロトタイプ実装に関する評価を述べる．

・認証速度・認証率

現在の実装環境での安定的に認証を行える速度を計測した．本実装ではJavaで記述された画像認識を用いているため，使用しているWebカメラのキャプチャー速度の限界までは達していない．現在の環境下で安定的に認証を行える速度としては，点滅信号を150msで切り替えるのが画像認識の限界である．

・認証時間

認証時間に関しては個人端末が認証サーバにVision信号を渡し，認証するまでの時間を計測した．それまでの個人端末と認証サーバ間のやりとりでは現在HTTP通信で行っているため，処理時間と考えないものとする．個人端末からのVision信号は6 bit送られ，150msごとに信号が切り替わるため，約1秒の認証時間を要している．

7 まとめ

本稿では個人の特定と位置情報が利用者の意思によって制御できるタグシステムを設計・実装・評価を述べた．本タグシステムでは利用者の位置情報取得と利用者の個人認証をカメラを用いて行い，利用者の意思に応じたサービス提供が可能なタグシステムを引き続き実装する．

参考文献

[1] 地域防犯のための ICT 活用, http://www.pref.osaka.jp/gyokaku/ITreport17/

[2] Nobuhiko Nishio, Koji Shuto, Kiyoto Tani, Takamichi Ishihara, Tomonori Morikawa, Wonder Wall:Realization of Interactive Wall in the Movie Minority Report, Demos of UBICOMP'06(Sep.2006)

[3] 三条あかり界色, http://www.dokyoto.jp/machi/akari/index.htm

[4] 塩津 真一, 山田 勇, 稲野 聡, 板崎 輝, 武仲 正彦, " セキュア RFID システムの開発" , 情報処理学会 マルチメディア，分散，協調とモバイル (DICOMO2006) シンポジウム論文集, pp.353-356, (2006)

[5] Muneyuki Sakata, Hiroshi Sasaki, Masataka Imura, Yoshihiro Yasumuro,Yoshitsugu Manabe, Kunihiro Chihara, Active IR-tag User Location Systemfor MR Collaborative Environment, 3rd CREST/ISWC Workshop onAdvanced Computing and Communicating Techniques for Wearable InformationPlaying, pp.90-93, Oct. 2004, Arlington, VA, USA

[6] 日本IBM, http://www.ibm.com/jp/

[7] NTT DoCoMo, http://www.nttdocomo.co.jp/

[8] Logicool, http://www.logicool.co.jp/