セキュアRFIDシステムの開発

塩津真一[†] 山田勇[†] 稲野聡[†]
板崎輝[†] 武仲正彦[†]

近年，様々な用途でRFIDタグの利活用が検討されている．電池搭載型のアクティブRFIDタグを人につけ，人の位置検出に用いるケースも登場してきている．通常，アクティブRFIDタグはIDを一定間隔で広範囲に常時送信する．そのため，第三者が離れた場所から電波を容易に傍受し，タグを持つ利用者の存在を容易に知ることができるというセキュリティ上の問題がある．我々は，このようなセキュリティ上の問題を解決する新しいRFIDタグシステムを考案し，試作検証したので報告する．

Development of Secure RFID System

Shinichi Shiotsu,[†] Isamu Yamada,[†] Satoshi Inano,[†]
Akira Itasaki[†] and Masahiko Takenaka[†]

Recently, Radio Frequency Identification (RFID) tags are examined for various usages. Active type of tags which incorporates a battery is being applied to a person to detect the person's position. Usually, the active tag always widely transmits ID at constant intervals. Therefore, there is a security issue that the radio signal is easily observed from a place away by an uncertain party. The party can easily perceive the existence of the user who has the tag. We report here that we designed a new active RFID tag system that solves such a security issue.

1. はじめに

RFIDタグは，大別すると，リーダ装置からのエネルギーを活用し応答するパッシブ方式と，電池を搭載し電波を自ら発するアクティブ方式の2つの方式がある．それぞれの特徴を**表1**に示す．

前者は低コストで物品へ貼り付けを狙ったものである．レジ効率化，配送センタのピッキング作業，在庫管理，流通・トレーサビリティなどへの応用が期待されている．後者は，電池を搭載することで通信距離を長くできる．しかし，コストが高いため，適用範囲は限定される．パッシブ型，アクティブ型RFIDともに，それぞれの特徴を活かして，様々な用途に応用されつつある[1)]．

アクティブRFIDタグに関しては，通信距離が比較的長いという特徴を活かし，最近，利用者に付け，利用者の位置を知ることで，様々なサービスを提供しようとする試みがなされている．たとえば，「児童の登下校安全対策システム」[2)]，「愛・地球博における展示会向け総合情報支援システム」[3)]，「RFID（無線ICタグ）を活用した，常時，パソコン利用者の認証を行うクライアントセキュリティシステム」[4)]などである．タグ信号を検出するリーダ装置に，タグを持った利用者が近づくと，タグから発せられるIDをリーダ装置が検知し，利用者が意識しなくても適切なサービスが提供される．

しかしながら，こうした試みに対して，セキュリティ上の問題が指摘されている[5),6)]．セキュリティが改善されたアクティブRFIDタグも報告されているが[7)]，問題の本質を解決するには至っていない．我々は，セキュリティ上の問題を解決する新しいRFIDタグシステムを考案，試作検証したので報告する．

以下，2章では従来型アクティブRFIDタグの課題について述べ，3章ではその課題を解決するために考案したシステム方式について述べる．4章では考案した方式を検証するための試作システム，5章では，その検証結果について述べ，最後に6章でまとめを述べる．

† 株式会社富士通研究所
FUJITSU LABORATORIES LTD.

表 1 タグ分類
Table 1 Comparison of tags.

項目	パッシブ RFID タグ	従来型 アクティブ RFID タグ	新提案 セキュア RFID タグ
通信距離	～70cm @13.56MHz ～ 7m@UHF	約 10m	約 10m
バッテリ寿命	半永久 バッテリ不要	約 1 年 (仕様依存)	約 1 年 (仕様依存)
セキュリティ	弱い	無し，弱い	強い
コスト (予想)	数十円	約 1000 円	約 1500 円
アプリケーション	物流・流通	人 セキュリティ弱い ためエリア限定	人 全エリア

2. 従来型アクティブ RFID タグの課題

本章では従来型アクティブ RFID タグの課題について述べる．通常のアクティブ RFID タグは，ID をつねに広範囲に常時送信している．これは,「私はここにいますよ」という電波を発信していることと等価である．そのためタグをつけた利用者が公共の場を移動する場合，安価なリーダ装置により，離れた場所から容易に傍受・追跡される恐れがある．たとえ ID を暗号化していたとしても電波を発すること自体が脅威となる．また傍受した信号をリプレイすることにより，他人になりすまして進入するという危険もある（**図 1** 参照）．

このようなセキュリティ上の問題を解決しない限り，アクティブ RFID タグを広く普及させることはできない（特に人が所持する用途で），と筆者は考える．よって，従来型のアクティブ RFID タグの適用先は，たとえばオフィスなどの安全な場所に限定されるべきである．

パッシブ RFID タグでも同様の課題がある．パッシブ RFID タグは，基本的にリーダ装置からの問合せに対してのみ応答する．したがって，リーダ装置が設置されてないところでタグ自身から不要な電波を発することはない．しかし，リーダ装置からの問合せに対しては，基本的に応答してしまうため，やはり，離れた場所から ID を読み取られるという危険が潜む．13.56 MHz 帯のタグであれば，大型のアンテナを使っても通信距離はせいぜい 70 cm 程度であるため，その危険性は低い．ところが，今後，普及が期待されている UHF 帯のタグでは 3～7 m 程度の通信距離が確保できるといわれており，通信距離が長いほど，運用における利便性は向上するが，離れた場所から ID が読み取られるという危険性が増す．

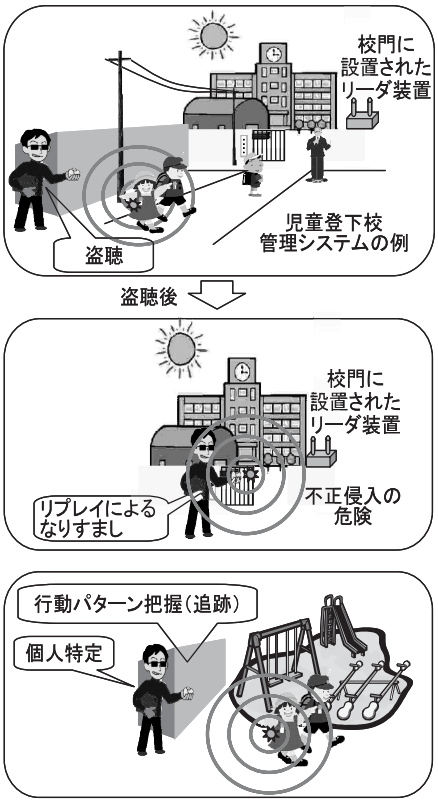


図 1 従来型アクティブ RFID の課題
Fig. 1 The issues on the security for conventional active tag.

以上より，どのような環境においても安心して所持することが可能な，これら課題を解決する方式の提案が求められている．

3. システム方式

本章では 2 章に記載したアクティブ RFID タグの課題を整理し，セキュリティ要件を明らかにしたうえ，要件を満たす方式を提案する．

3.1 脅　　威

従来のアクティブ RFID タグでの主な脅威は下記のとおりである．

(1)　アクティブ RFID タグから常時発信される電波が安価なリーダ装置で捕捉され追跡される危険

第三者が，利用者に気づかれることなく，離れた場所からその存在を知ることができる．ID までは理解できなくてもタグの所持を検知される．アクティブ RFID タグが十分に普及していない状況下においては，電波を発していること自体が脅威となる．

(2)　ID が盗聴される

捕捉した電波から ID が盗聴されることで，個人が

特定されてしまう（ID まで理解）.

(3) 再送攻撃によるなりすまし

アクティブ RFID タグから発せられる電波を捕捉し（あるいは，偽造タグにより），リーダ装置付近で再送すると，利用者になりすますことができる.

3.2 セキュリティ要件

前記の脅威に対するセキュリティ要件は以下のとおりである.

(1) タグから自発的に電波を発信せず，リーダライタからの問合せに対してのみ応答する

捕捉を避けるために，正当なリーダライタから問合せがあったとき以外は電波を発しない.

(2) 送受信データは毎回ランダムになるよう暗号化

秘匿性を向上させるため単純な暗号化ではなく送受信データが毎回ランダムになるよう暗号化.

(3) ある一定時間経過したリーダライタからの信号には応答しない

再送攻撃によるなりすましに対応するため一定時間以上経過したリーダライタからの信号には反応しない.

3.3 リーダライタ–タグ間の相互認証方式

前記のセキュリティ要件 (1) を実現するためにリーダライタ–タグ間では毎回相互認証を行う．リーダライタからの 1 回の問合せに対して 1 回の判定で認証が完了することを基本とし，タグ側で認証されなかった場合にはいっさい電波を発しない方式とした．また，回路規模や処理時間増加による消費電力の増大を抑えるため，暗号化方式は，共通鍵暗号化方式（DES）を採用した．類似の方式として，タグ側の負担を比較的軽くすることが可能なハッシュ関数を用いた Randomized Hash 方式[9]，Extended Hash-chain 方式[10] なども提案されている．これらはいずれもタグからの返信後，リーダライタ（またはサーバ）側で認証されるものであり，タグ内で認証されない限り電波を発しないという本セキュリティ要件を満たせないため本システムでは採用していない.

また，要件 (2) を実現するために，ワンタイム情報を含めて暗号化することで送受信データを毎回ランダム化する．また，ワンタイム情報には，リーダライタ/タグそれぞれに搭載されている時計（時刻情報）を利用した．これは要件 (3) を実現するためでもある．受信データに含まれる時刻と，自身で所持している時刻の比較を行い，その差が許容値を超えればなりすましと判定している．ワンタイム情報として時刻情報を利用すること自体は他のシステム[11] でも利用されている.

図 2 にリーダライタ–タグ間の認証処理のフローを示す．リーダライタ，タグは，それぞれ暗号化のための鍵（Key），SysID（システム固有の ID で，サービスごとに規定される）を所持する．タグ側には，自分自身の ID（TagID）を所持する．これらは秘密に保護されなければならない．またリーダライタ/タグには時計が内蔵されており，それぞれの時刻（Time）は同期している必要がある.

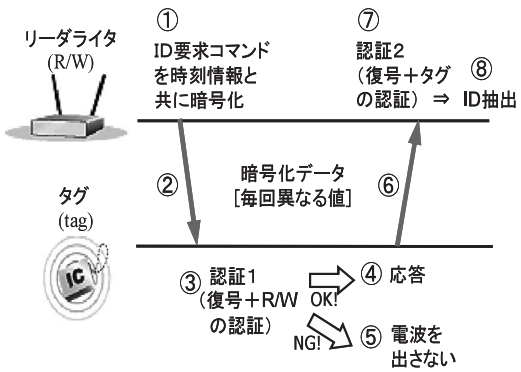


図 2 リーダライタ–タグ間の認証処理フロー
Fig. 2 The flow of the attestation process between reader/writer and tag.

以下，図 2 のフローを解説する.

① リーダライタは ID 要求コマンドを，時刻データ（Time），SysID データとともに，共通鍵（Key）を用いて暗号化して送信する.

② リーダライタから送信される空中信号は，時刻データ（Time）を入れて暗号化しているため，毎回異なる信号となり，秘匿性が向上する.

③ タグ側では認証処理が実行される．具体的には復号処理後，復元した SysID がタグで所持している SysID データと一致し，かつ，復元した時刻データ（Time）とタグで所持している時刻データ（Time）とのずれが許容値以下の場合，リーダライタが認証されたと判断する.

④ 認証されたと判断された場合，タグは，TagID を時刻データ（Time）とともに，暗号化し応答する.

⑤ 認証されない場合，タグは処理を終了し，アクションを起こさない（電波を出さない）.

⑥ タグからの応答は，時刻データ（Time）を入れて暗号化しているため，毎回異なる信号となり秘匿性が向上する.

⑦ タグからの信号を受信したリーダライタは，正当なタグからの応答かを判断するために認証処理を行う．具体的には，復号処理後，復元した時刻データ（Time）と，リーダライタで所持

している時刻データ（Time）とのずれが許容値以下の場合，TagID が正当なタグからの応答と判断する．

⑧ 抽出された TagID がシステムの中で利用される．

3.4 安 全 性

(1) 耐タンパ性について

本試作システムではタグの低コスト，低消費電力の観点から，最も単純な共通鍵暗号化方式（DES）を使用したが，共通鍵の場合，1 つのタグから鍵が流出すれば，全システムに影響が及ぶ．そのためタグには耐タンパ性が要求される．また，システムによって鍵を使い分ける等の工夫が必要である．

(2) 再送攻撃によるなりすまし対策について

再送攻撃によるなりすましを検出する方法としては，前述のとおり，リーダライタ/タグそれぞれの時刻差を利用している．前提条件としてリーダライタ/タグそれぞれの時刻同期が必要であるが，実際には完全に同期させるのは難しく誤差が生じるため許容値に幅を持たせる必要がある．しかし幅を持たせるということは，逆に再送攻撃の機会を与え，安全性を低める結果となる．時刻の誤差を小さくする方法としては，時計の精度を上げる必要があるが，それは高性能な水晶部品が必要となりコストアップにつながる．そのほか，リーダライタ–タグ間で一定時間ごとに時刻合わせをする方法もあるが，用途によっては必ずしも頻繁にアクセスする機会があるわけではなく，その場合，やはり大きな誤差が生じる．よって，許容値設定については実際にシステムに要求されるセキュリティ強度，コストなどに応じて最適値を選択すべきである．

4. 試作システム

前章で解説した方式を実装するリーダライタ，タグを試作した．セキュリティ要件を満たすこと以外に，試作タグが実用的な電池寿命（ボタン電池で電池寿命約 1 年）を実現できることにも重点を置いた．

まず，システムにおける秘密情報の管理であるが，リーダライタ側においては，秘密情報（鍵 [Key]，時刻 [Time]，SysID，TagID）は，より安全なサーバにおいて管理され，情報はリーダライタ制御端末をスルーして，タグと直接やりとりする構成とした．

タグ側においては，耐タンパ性を高めるため，秘密情報（鍵 [Key]，時刻 [Time]，SysID，TagID）は，タグ内の RAM 領域に格納され，電池が外された場合には秘密情報がクリアされる構成とした．

また，再送攻撃によるなりすまし判断のための許容値は 60 秒に設定した．今回の試作システムでは，リーダライタ/タグそれぞれに所持している時計の精度を決定する水晶部品には，コストを優先し汎用的な部品を使用した．そのため月あたりの誤差が約 ±15 秒生じる．たとえば，リーダライタ側がプラス側に最大，タグ側がマイナス側に最大ずれた場合，リーダライタ–タグ間で月あたり最大約 30 秒の誤差が生じる．たとえば，2 章の図 1 に示した児童登下校管理システムでの利用を想定した場合，夏休み期間中を考慮したとしても 2 カ月に 1 回は，リーダライタ–タグ間でアクセスが期待でき，同期をとることが可能である．そのため許容値は 約 30 秒 × 2 カ月 = 60 秒 に設定している．

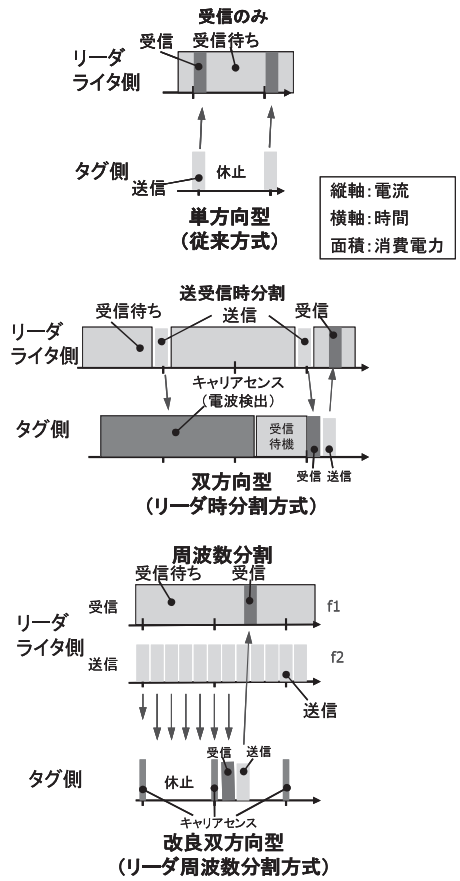


図 3 リーダライタ–タグ通信タイミング図
Fig. 3 Timing diagram of reader/writer and tag.

次に，タグの実用的な電池寿命を達成するための構成について述べる．**図 3** に単方向型（従来方式），双方向型（リーダ時分割方式），改良双方向型（リーダ周波数分割方式）それぞれにおけるリーダライタ–タグ間のデータのやりとりを示す．従来型アクティブ RFID タグ（単方向型）は，タグ側は ID 送信動作だけであるため受信回路が不要であった．また ID 送信に関しても送信，休止を繰り返す間欠動作とすることで省電

表 2 共通仕様
Table 2 Common specification.

項目	内容
タグ数	最大 $2^{\wedge 128}$ 個
通信距離	約 10m
周波数	315MHz 帯
送信電力	500uV/m@3m (微弱無線規格準拠)
通信方式	FSK 方式
通信レート	38.4kbps
セキュリティ方式	共通鍵暗号化方式(DES) による暗号通信

表 3 リーダライタ仕様
Table 3 Reader/writer specification.

項目		内容
ホスト I/F	据置型	USB, LAN, WLAN
	USB ドングル型	USB
電源	据置型	USB バスパワー又は, DC5V AC アダプタ
	USB ドングル型	USB バスパワー
外形寸法	据置型	100mm x 80mm x 25mm (アンテナ含まず)
	USB ドングル型	77mm x 25mm x 8mm

表 4 タグ仕様
Table 4 Tag specification.

項目	内容
電源	リチウムボタン電池 (DC3V)
サイズ	34mm x 34mm x 5mm (電池除く)

力化が図れた．しかし今回提案した相互認証方式を実現しようとした場合，タグ側での受信動作が新たに必要となる（双方向型）．単純に双方向通信にした場合，リーダライタ側は，送信，受信の時分割動作となり，送信の密度が低くなる．この密度の低いリーダライタからの送信信号をとらえるにはタグ側で長時間キャリアセンスの必要があり，タグ側の消費電力が増大し，実用的な電池寿命を達成できないという問題があった．

これらに対し改良双方向型では，リーダライタの送受信周波数を分けることで（周波数分割方式），リーダライタの送信密度を上げることが可能となり，タグ側ではキャリアセンス時間を大幅に削減し，低消費電力化が可能となる．

ここで注意しなければならないのがキャリアセンス間隔である．省電力化のためにはキャリアセンス間隔を広げたほうが有利であるが，必要以上に広げすぎると，たとえば人の動線管理に使用するような用途の場合に問題が生じる．移動速度によってはタグが休止期間中にリーダライタが設置された特定のエリアを通り抜けてしまい正確な動線管理が行えないからである．アプリケーションによっても異なるが，一般的にキャリアセンス間隔は 1 秒程度の間隔で設計されることが多い．今回の試作システムは 1 秒で試作した．

通信方式は 315 MHz 帯の微弱無線方式とした．これは免許が不要で，比較的低コストで実現できるためである．そのため通信距離は約 10 m となっている．無線方式については，実際には，使用するアプリケーションに応じて，たとえばさらに通信距離を要求されるような用途では長距離通信可能な無線方式を選択すべきである．

また暗号化処理については本試作では比較的負荷の軽い共通鍵暗号化方式（DES）を用いているため，リーダライタ/タグそれぞれに搭載のコントローラ（マイコン）によってソフトウェア処理で実現している．

以上の構成をまとめ，**表 2** にシステムの共通仕様

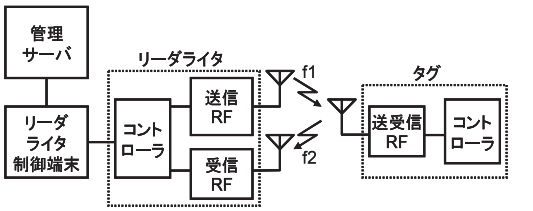


図 4 システム構成図
Fig. 4 System configuration diagram of reader/writer and tag.

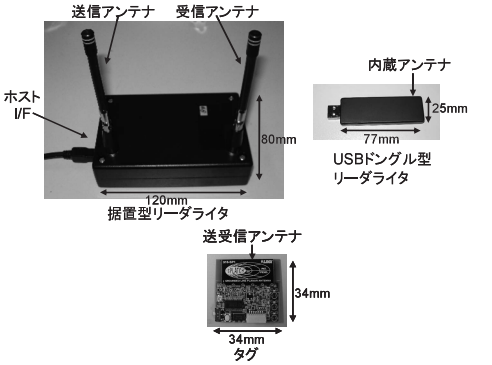


図 5 試作リーダライタ，タグの外観図
Fig. 5 Photograph of reader/writer prototype and active tag prototype.

を，**表 3** にリーダライタ仕様を，**表 4** にタグ仕様を示す．また，**図 4** にシステム構成図を，**図 5** に試作したリーダライタ，タグの外観図を示す．

5. 検　　証

前章記載の試作システムを用いて，提案方式の動作検証を行う．

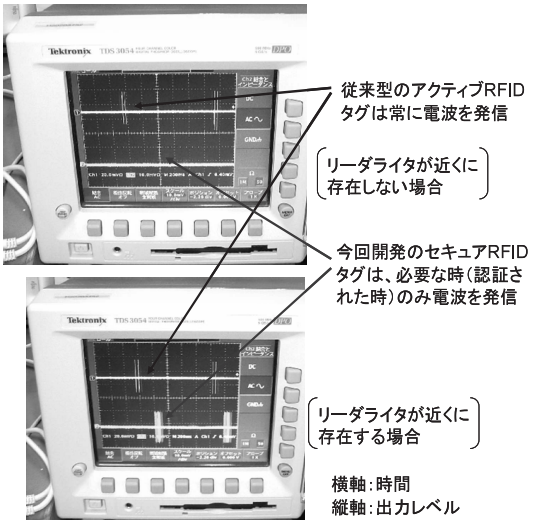


図 6 従来型アクティブタグとの出力信号比較
Fig. 6 Comparison of output signals with conventional active tag and secure/new tag prototype.

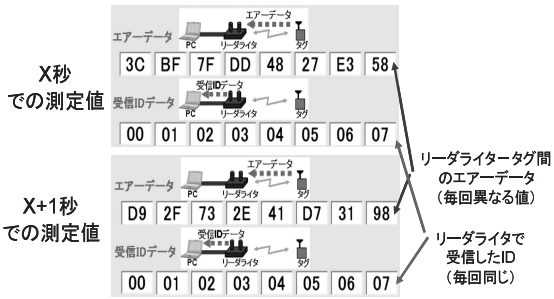


図 7 ランダム暗号化検証
Fig. 7 Random encryption inspection.

5.1 セキュリティ要件の検証

(1) タグが自発的に電波を発信せず，リーダライタからの問合せに対してのみ応答しているかを検証する．

図 6 に従来型アクティブ RFID タグとの出力信号比較を示す．従来型は一定間隔ごとにつねに電波を発しているが，今回開発したセキュア RFID タグは，近くにリーダライタが存在しない場合は，電波を発していない．リーダライタが近くに存在する場合，すなわちリーダライタからの問合せがあったときのみ，認証したうえで応答を返すことを確認した．

(2) 送受信データが毎回ランダムになるよう暗号化されているかを検証する．

図 7 に時刻 X でのタグからリーダライタへの送信エアデータをキャプチャした結果と，それを復号した結果，および，時刻 X＋1 秒時のタグからリーダライタへの送信エアデータをキャプチャした結果と，それを復号した結果を示す．キャプチャした送信エアデータは 1 秒ごとにランダムな値に置き換わっていることが確認できた．またリーダライタ装置で復号した ID データは毎回同じ値になることも確認した．

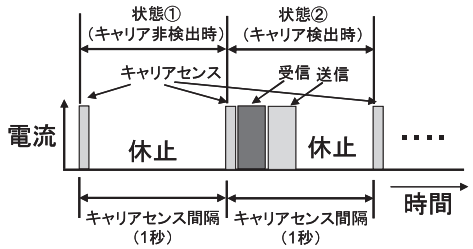


図 8 タグの代表的な動作状態での電流分布
Fig. 8 Electric current distribution in a representative state of a tag.

(3) ある一定時間以上経過したリーダライタからの信号に応答しないかを検証する．

リーダライタの信号をキャプチャ後，再送攻撃を行うことを擬似的に検証するため，タグの時計を意図的に進めて検証した．4 章に記載のとおり，なりすましの判断の際に使用する許容値は，本試作システムでは 60 秒に設定している．検証の結果，タグの時計の進め方を許容値以下にした場合は，リーダライタからの問合せ信号に対してタグが正常に応答することを確認した．また，許容値を超える値に進めた場合，リーダライタから問合せ信号を出しても，タグからは何も応答しないことを確認した．

5.2 電池寿命の検証

試作タグがセキュリティ要件を満たしながら実用的な電池寿命（ボタン電池で電池寿命約 1 年）を実現できるかを検証する．

タグの動作状態は，代表的な 2 つの状態に分類できる．**図 8** にその様子を示す．

1 つはキャリア非検出状態（状態 ①）であり，もう 1 つはキャリア検出状態（状態 ②）である．キャリア非検出状態は，リーダライタが近くに存在しない状態であり，キャリアセンス後，キャリア非検出と判断しすぐに休止状態に入る．一方キャリア検出状態は，リーダライタが近くに存在する状態であり，キャリアセンス後，キャリア検出と判断し受信処理を行い，タグ ID を返信後，休止状態に入る．

各状態での 1 秒あたりの平均消費電流を以下に示す．

キャリア非検出時（状態 1）⇒ 約 25 [uA/sec]

キャリア検出時（状態 2）⇒ 約 290 [uA/sec]

たとえば，2 章の図 1 に示した児童登下校管理システムを想定した場合，正門を通過するのは 1 日に数回程度である．よって正門に設置したリーダライタの信号（キャリア）を検知し，データの送受信を行う回数

も数回程度となる．リーダライタの信号を検知する時間を 1 日あたり 1 分（60 秒）とした場合，平均電流 Iavg. [uA/sec] を計算すると以下のとおりとなる．

1 日のトータル時間 Tmin [分] は，

Tmin [min/day]=24 [hour/day]×60 [min/hour]

Iavg. [uA/sec]={1 [min/day]×290 [uA/sec]
+(Tmin [min/day]−1 [min/day])×25 [uA/sec]}
/Tmin [min/day]=25.2 [uA/sec]

よって，消費電流はキャリア非検出時（状態①）の電流でほぼ決まる．リチウムボタン電池 CR2032（容量 = 220 mAh）の場合，電池寿命は約 1 年となり，ほぼ実用的な電池寿命を達成することが可能となる．

6. ま と め

セキュリティ機能を強化する新しい RFID タグ方式と試作システムを紹介した．本システムは，従来のアクティブ RFID タグで大きな問題となっていたセキュリティ上の問題を解決している．また，実用的なバッテリ寿命も達成し，製品化に向けた大きなハードルを越えている．今後は，実用化に向けたシステム全体の設計と，様々な用途への適用を考えてゆきたい．

参 考 文 献

1) RFID JOURNAL. http://www.rfidjournal.com/
2) 児童一人一人の登下校を確認する安全対策システムを導入．http://pr.fujitsu.com/jp/news/2004/09/27-1.html
3) 産総研,「愛・地球博」に無線 IC タグを活用した情報支援システムを提供．http://techon.nikkeibp.co.jp/article/NEWS/20050131/101257/
4) RFID（無線 IC タグ）を活用して，常時，パソコン利用者の認証を行うクライアントセキュリティシステム［パソロックん］の発売．http://www.cnes.co.jp/business/press/20050127.html
5) PCWEB：情報化社会に忍び寄る危険 — 産総研・高木浩光氏に聞く．http://pcweb.mycom.co.jp/articles/2005/01/01/takagi/003.html
6) EPIC：California School Drops RFID Tracking Program. http://www.epic.org/privacy/rfid/brittan-letter.pdf
7) Kinoshita, S., Ohkubo, M., Hoshino, F., Morohashi, G., Shionoiri, O. and Kanai, A.: Privacy Enhanced Active RFID Tag, *1st International Workshop on exploiting context histories in smart environments*, Germany (May/11/2005).
8) Yamada, I., Shiotsu, S., Itasaki, A., Inano, S., Yasaki, K. and Takenaka, M.: Secure Active RFID Tag System, *Ubicomp2005 Workshop* (2005).
9) Sarma, S.E., Rivest, R.L. and Engels, D.W.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, *Security in Pervasive Computing*, LNCS, Vol.2802, pp.201–212 (2003)
10) Ohkubo, M., Suzuki, K. and Kinoshita, S.: Cryptographic Approach to a Privacy Friendly Tag, *RFID Privacy Workshop, MIT* (2003).
11) RSA セキュリティ RSA SecurID. http://www.rsasecurity.com/japan/products/securid/index.html

(平成 18 年 10 月 31 日受付)
(平成 19 年 4 月 6 日採録)

塩津 真一

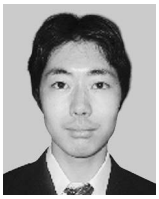
昭和 60 年富士通（株）入社．超高速伝送用 IC，放送用システム LSI 等の半導体設計開発を経た後，モバイル端末に関わる無線技術，RFID システムの研究開発に従事．現在，（株）富士通研究所パーソナルシステム研究センター主任研究員．DICOMO2006 優秀論文賞受賞．

山田 勇（正会員）

昭和 60 年（株）富士通研究所入社．超音波診断装置，医療画像の研究開発を経た後，モバイル端末に関わる無線技術，トラステッド端末技術，省電力技術の研究開発，RFID システムの研究開発に従事．電気学会，IEEE 各会員．現在，（株）富士通研究所パーソナルシステム研究センター主管研究員．

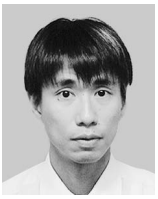
稲野 聡（正会員）

昭和 55 年富士通（株）入社．並列計算機，データマイニング，ストレージシステム，モバイル端末に関わる省電力化技術の研究開発を経た後，RFID システムの研究開発に従事．現在，（株）富士通研究所パーソナルシステム研究センター研究員．電子情報通信学会会員．



板崎　輝

平成 16 年（株）富士通研究所入社．モバイル端末に関わる無線技術，RFID システムの研究開発に従事．現在，（株）富士通研究所パーソナルシステム研究センター研究員．



武仲　正彦

平成 4 年（株）富士通研究所入社．公開鍵・共通鍵暗号の攻撃・実装技術，サイドチャネル攻撃，ネットワークセキュリティの研究開発に従事．現在，（株）富士通研究所 IT コア研究所セキュアコンピューティング研究部主任研究員．平成 14 年コンピュータセキュリティシンポジウム（CSS2002）優秀論文賞受賞，平成 17 年（財）電気科学技術奨励会第 53 回電気科学技術奨励賞受賞．電子情報通信学会会員．