RFID プライバシー保護を実現する可変秘匿 ID 方式

木下真吾，星野文学，小室智之，藤村明子，大久保美也子

NTT 情報流通プラットフォーム研究所

あらまし　将来，到来するであろうユビキタス社会において，RFID タグはあらゆるアイテムに装着され，さまざまな応用サービスへと発展していく基盤技術として期待されている．一方では，RFID の優れた追跡能力が悪用された場合の消費者プライバシー侵害が問題視されはじめている．本論文では，漠然とした不安がもたれている RFID のプライバシー問題を整理するとともに，その普及条件として最も重要となる低コスト化を考慮した解決方式を提案する．また，将来の標準技術として最も注目されている MIT Auto-ID システムへの適用方式もあわせて紹介する．

Nonidentifiable Anonymous-ID Scheme for RFID Privacy Protection

Shingo Kinoshita, Fumitaka Hoshino, Tomoyuki Komuko, Akiko Fujimura and Miyako Ohkubo

NTT Information Sharing Platform Laboratories

Abstract　RFID is expected as one of the most important infrastructure technology for ubiquitous society, because the RFID tags will be affixed to almost all items and used for various useful ubiquitous services in the future. On the one hand, such a wide deployment of RFID may expose new privacy threats of citizens by abuse of powerful tracking capability of the RFID. We try to make RFID privacy issues clear and propose a low-cost protection method to resolve the privacy issues in this paper. The cost is the most important factor for global diffusion of the RFID. Moreover, this paper shows how to apply our method to the Auto-ID system , which is supposed as the standard of next generation RFID system.

I.　はじめに

近年，無線通信を利用した自動認識技術 RFID(Radio Frequency Identification)が，さまざまな用途に利用されはじめている．例えば，交通系の改札，入館チェック，生産工程，在庫管理，商品の入出荷検品などの効率化手段として利用されている．

RFID タグとは，IC チップとアンテナを内蔵した媒体である．タグは，読取装置と無線通信を行うことにより IC チップ内の情報を非接触で通知することができる．さらに，搭載できる情報量が大きい，複数のタグを一括で読取れる，偽造や複製が困難，読取り速度が高速といったバーコードにはない優れた特徴がある．

一方，現状では RFID タグのコストは数百円程度と高価であるため，比較的高価な商品や，再利用を前提とした IC カードや物流用パレット，ケースなどに適用されることが多い．

こうした状況を反映して，非常に低コストな RFID タグへの期待が高まってきている．数円程度まで低コスト化することにより，生産段階において，あらゆるアイテムへのタグの装着が容易となり，その結果，生産・流通・店舗・消費者・廃棄・再利用といったライフサイクル全体を通した有効利用が可能となるためである．

RFID タグのコストは，2004 年に 5 円程度，さらに 2008 年には 1 円程度まで下がるとの予測がある[1]．また，2003 年現在，大手日用雑貨メーカが既に 5 億個のタグを購入したと報じられているが[2]，その後，装着されるタグの総数は，2004 年には 10 億個，2008 年には 200 億個，2009 年には 500 億個，さらにその後は急速に拡大し 2021 年には 8 兆個にも及ぶと予測されている[1]．

このように，ありとあらゆるアイテムにタグが装着されるようになると，その適用領域は生産・流通の効率化といった領域だけにとどまらず，消費者の手に渡った後のさまざまな応用サービスに発展する可能性が高い．冷蔵庫と連携した食品管理，レシピ推薦，自動注文，賞味期限表示や，薬品への装着による誤服用防止のように既に想定されている応用サービス以外にも，さまざまな可能性を秘めている．こうした意味において，RFID タグは，ユビキタス社会における基盤技術としての期待も大きい．

あらゆるアイテムへのタグの装着に対する期待感が高まる一方，RFID による新たなセキュリティ脅威への警戒感も高まってきている．中でも消費者プライバシーの侵害が最も懸念されている[3, 4]．RFID は，無線を利用して自動的にその存在を外部へ通知してしまうという特徴があるため，スパイ映画等に見られる一種の追跡装置として危険視される傾向がある．近年，こうした警戒感が具体的な形で現れはじめている．タグの装着を計画していた大手アパレルメーカに対して批判が集中し，不買運動までつながった件[5]や，大手小売店が計画していた実証実験において，急きょ商品レベルでのタグ装着をとり止めた件などがあげられる．後者の実験中止の理由の一つに，こうしたプライバシー侵害への批判が起きているためではないかとの指摘もある[6]．

本論文では，こうした低コスト RFID のプライバシー問題に対する技術的な解決方法を提案する．2 章において，既存の RFID システムと現在注目が高まっている MIT の Auto-ID システムとを概説し，3 章で RFID プライバシー問題を分析する．そして，検討を行う上でのコストや対象とするタグなどの条件を 4 章で整理し，5 章において，我々の解決方法及び Auto-ID システムへの適用方法を紹介する．最後に，従来技術との比較やコスト，運用性などに関して考察を行う．

II. RFID システム

1) 既存 RFID システム

RFID システムとは，RFID を用いた情報管理ネットワークシステムである．主に，*RFID タグ*，*RFID リーダ*，*データベース*から構成される．

RFID タグ：前述のとおり，超小型の IC チップとアンテナを内蔵した媒体であり，RFID リーダに対して情報を非接触で送出する．

RFID リーダ：タグから情報を読取る装置であり，データベースに対して，タグ情報の書込み・読取り等アクセスを行う．

データベース：タグの ID や，読取り位置・時間，温度等のセンサ情報，商品関連情報など，タグに関連する情報を管理する．このデータベースにより，商品の移動履歴や在庫管理などが可能となる．

RFID タグには，内蔵電池の有無（アクティブタグ／パッシブタグ），キャリータイプ（ID キャリー，データキャリー），メモリタイプ（ROM 型，RAM 型），記憶容量（64bit～数 Kbyte），暗号処理プロセッサ等のセキュリティ回路内蔵の有無，利用周波数（13.56MHz，900MHz，2.45GHz）などの組合せにより様々な種類が存在する．

現在最も広く利用されている標準 RFID タグの一つとして ISO15693／18000-3 がある．このタイプの RFID タグは，UID と呼ばれるタグを一意に識別するための読取り専用の ID と，利用者が書換え可能なユーザ領域とを有する．ユーザ領域の容量は大きいもので 8Kbyte 程度もある．また，ユーザ領域へのアクセス制御機能を有するものもある．利用周波数は 13.56MHz であり，通信距離は，数センチから数十センチ程度である．なお，2.45GHz・900MHz 帯のタグは，数メートルの通信距離を取ることも可能である．特に 900MHz 帯は，10 メートルにもおよぶ通信距離を取ることができ，また，数百個にもおよぶ一括読取り性能をもつなど，タグとして非常に優れた性質をもつ．

RFID タグとリーダとの一般的なプロトコルを示す．
Step1：リーダが“ID 取得要求”をブロードキャスト．
Step2：電波到達範囲内に存在するタグが“ID”を返送（アンチコリジョン機構により，シリアライズされる）．
Step3：リーダから ID を指定してユーザ領域の“データ読取り要求”をブロードキャスト．Step4：指定された ID のタグがユーザ領域の“データ”を返送．

このような現状のタグのコストは，一般的に数百円程度となるため，大規模な普及に対する阻害要因となっている．これを改善するために，タグの低コストによる普及促進をねらったさまざまな取組みが行われている．その代表的なものの一つに Auto-ID センターによる活動がある．

2) Auto-ID システム

Auto-ID センター[7]は，1999 年に設立された MIT に本部を置く次世代バーコードシステムの国際的な研究機関である．あらゆる商品の個体それぞれに RFID タグを装着し，生産者から流通業者，店舗，消費者といったさまざまな利用者がタグを共通利用できるようにすることを目指している．その実現に向けて，Auto-ID センターでは，タグの低コスト化や ID 体系や情報管理方法の標準化などの検討を行っている．

RFID タグの低コスト化に向けて，Auto-ID センターでは，EPC と呼ばれる 64bit または 96bit の ID だけを IC チップに格納し（以降，従来の RFID タグと区別するために EPC タグとする），それ以外の情報は，全てネットワーク側で管理するアーキテクチャを採用している．EPC は，従来の RFID における UID に相当する．しかし，UID がタグ製造メーカによって付与される一意性が保証された任意のコードであったのに対して，EPC は，消費の製造メーカコードと，商品種別コード，シリアル番号とからなる商品属性を表す構造化されたコードとなっている点が異なる（図 2）．

また，さまざまな利用者によってタグを共通利用するために，EPC のコード体系，商品情報（移動履歴など）のデータ記述言語 PML，PML サーバのアドレス解決サービス ONS，読取装置の制御や EPC データの転送などを効率化するソフトウェア基盤 Savant などの検討も行われている．

III. RFID プライバシー問題

前章に述べたように，従来の RFID タグは，リーダに対して ID とユーザデータを送信する可能性がある．ユーザデータの読取りには，アクセス制御機能が設けられているものもあるが，ID の読出しには，そうした制御がなく，リーダさえ持っていれば誰でも自由に読み出せてしまう．また，EPC タグは，リーダに対して EPC を送信する可能性がある．従来の RFID タグ同様に，EPC の読出しにはアクセス制御が設けられていない．また，PML などのデータベースは，通常，流通関連の情報など消費者に直接関係のない情報を管理するために利用されるが，今後，購入・利用履歴などをマーケティング等へ活用するために，消費者に関連する情報が格納されてくる可能性も否定できない．

こうした状況において，プライバシー脅威につながる可能性のある情報を以下に整理する．

① データベース上の情報
② タグのユーザデータ領域情報
③ タグの ID 情報

①に関しては，RFID システムに限らず，さまざまな運用管理・技術上の問題が指摘されているが，技術的には，データベースのアクセス制御およびインターネットセキュリティ技術といった既存技術により解決可能である．また，法的には，個人情報保護法によって保護される可能性もある．

②に関しては，ユーザデータに商品情報や移動履歴情報などが格納される可能性があること，さらに，その情報が任意に読取られてしまう危険性があることなど，プライバシー侵害を危惧する声がある．これに対して，読取り・書き込み時のアクセス制御機能を用いることにより解決することができる．さらに，EPC タグなどの次世代の低コストタグには，こうした情報もデータベース上で管理され，上記に示す方法により解決される．

③に関しては，UID や EPC が単なる ID であり，それにひも付けされた消費者の情報がデータベース上で安全に管理されていれば，一見，プライバシー侵害にはつながらないように考えられている．ただし，こうした ID のみであっても，プライバシー問題を引き起こす危険性が残されている．ID に関係するプライバシー問題は大きく以下の 2 つに分類できる．

③-1 所持品の漏洩
③-2 ID 追跡による行動追跡・本人特定

③-1 は，例えば，カバンに入れている物や身につけている物などの情報を，所持者に気づかれること無く，他人に読み取られてしまう危険性があることを示している．極端に表現すれば，透明な洋服を着て，透明なカバンをもっているようなものである．EPC のように，そのコードにメー

カや製品種別などの情報が，含まれている場合には，非常に容易に，所持品の情報を覗き見ることが可能となる．所持品の種類や所有者の意識にも依存するが，所持品の財産的価値を示す紙幣や高額商品，病状などを映す薬，身体的特徴などを表す下着や衣類，趣向や思想などを映し出す書籍など，さまざまな知られたくない情報があると予想される．

③-2 は，例えば，商品を購入する際に，クレジットカードなど個人を特定する情報を提示し，それが商品の ID と結びつけられた場合，その商品の移動追跡により，所持者の移動追跡もできてしまう危険性や，あるいは所持品の ID から本人が特定されてしまう危険性を示している．特に，衣類や靴，時計，カバンなど身につける機会が多い商品ほど長期的な追跡に利用される危険性がある．極端に表現すれば，スパイ映画に登場する追跡装置を知らない間に付けられるようなものである．この問題は，EPC に限らず，RFID が常に同一のユニークな ID を返答する従来の UID においても同様の危険性が起こりえる．さらに，一度，ある所持品の ID と個人を特定する情報とがひも付けられた場合，連鎖的にほかの所持品の ID と名寄せされ，個人追跡を防ぐことが出来なくなる危険性もある．

こうした脅威は，リーダが街のあらゆるところに設置されるような遠い将来の出来事として想定されることが多い．しかし，以下に示すような比較的実現性の高いリーダの利用シーンも想定される．

Scene 1: 街角にリーダが設置され，通行人の所持品をスキャンし，マーケティングや勧誘に利用される．

Scene 2：多くの店舗の万引き防止ゲートが RFID リーダに置き換わり，来店客の所持品がスキャンされる．

Scene 3: 店舗の棚に RFID リーダが設置され，棚に陳列されている商品だけでなく，来店略の所持品もスキャンされる．

Scene 4: 要注意人物の足取りを追跡するために，飛行場のセキュリティゲートが RFID リーダ対応になり，持ち物もスキャンされる．

Scene 5：電車の改札，ビル入館ゲートなどにリーダが設置され，持ち物もスキャンされる．

さらに，上記シーンにおいて，個人を特定される可能性もある．店舗では，購入時にメンバーズカードやクレジットカードを利用するかもしれない．また，航空券や定期などからも個人が特定されてしまう．

上記シーンが，万引き防止やマーケティング，セキュリティ目的などで利用され，消費者や一般市民への利益・安全につなげることを目的として，安全に運用されれば問題ないかもしれない．しかし，追跡の対象がいつの間にか拡大する"ミッション・クリープ"の問題や，誤運用や悪用される危険性もある．

IV. 検討条件

1) Kill 機能

現状の EPC タグの Class I チップ[8]において，唯一サポートされているプライバシー保護機能は，Kill 機能のみである．本機能は，例えば商品購入時に，タグが消費者の手に渡った後二度と機能しないように無効化するためのものである．

この無効化は，消費者にとって，安全性を直感的に理解しやすいものであり，受け入れやすいと考えられる．ただし，無効化を行う手間や，無効化が確実に行われたか否かを確認することが難しいなど，運用上の問題も多い．さらに，無効化した場合には，購入以降に将来想定される購入者サービス，再販売などの二次業者による利用（在庫管理，マーケティング分析など），リサイクル利用など，さまざまな将来期待されている応用サービスの芽を摘むことになる．

2) 制約・前提条件

[利用 RFID タグ]ID のみ搭載する低コスト RFID タグを対象とする．

[コスト]文献[9]によると$0.05 タグを実現させる場合，IC にかけられるコストは$0.01～$0.02 となる．また，0.18μm ルールの場合，1㎜^{2} のチップのコストは$0.08 程度，1㎜^{2} に収まるゲート数は 60Kgates 程度とされている．この結果，目的のコストを達成するためには，ゲート数を 7.5K～15Kgates に抑える必要がある．また，100bit 程度の ROM のみを搭載した EPC チップが 5K～10Kgates とされているため[10]，セキュリティ用におおよそ 2.5～5Kgates 程度の追加が許される．

[許容転送データサイズ]13.56MHz 帯および 900MHz 帯の転送レートと同時読み取り数は，それぞれ，13.56MHz: 26Kbps/50 個程度，900MHz: 128kbps/200 個程度であるため，タグ 1 個あたりの転送レートは，およそ 0.5kbps 程度となる．すなわち，1 秒間に 1 回の読み取りにおいて送出可能な最大データサイズは 500bit 程度が許される．

[メモリのタンパー性]耐タンパー性メモリは，高コストとなるため，RFID タグのメモリに対して耐タンパー性の仮定はおかない．すなわちメモリ上のデータは，物理的なアタックなどにより，漏洩する可能性がある．

[タグ-リーダ間通信]タグ-リーダ間の無線通信は盗聴の危険性がある．

[タグ書込み制御]タグへのデータ書き込みは，物理的に近接させり接触させたり，あるいはリーダからの電波方向を調整するなど盗聴されないよう工夫できる．あるいはパスワード等によるメモリ書き込み時のアクセス制御機能を利用できる．

[ネットワーク・データベース]リーダ-データベース間には安全な通信路が提供されている．データベース上のデータは，アクセス制御機能により安全に管理される．

V. 提案方式：秘匿 ID

1) 所持品漏洩問題対策

本節では，ROM のみを搭載する RFID に適用可能なプライバシー保護の一方式を紹介する．この制約のもとでは，上記に示したプライバシー問題のうち，③-1 の「所持品の漏洩」のみを防ぐことが可能となる．

秘匿 ID 基本方式

本方式は，RFID にアクセス制御用の特別な回路を用いることなく，秘匿化（暗号化など）した ID を RFID に格納することによって，不正者による所持品の漏洩を防ぐ方法である．秘匿 ID は，信頼できるセキュリティサーバによって正規の ID に代理復号される．復号時に必要な情報であるサーバ ID 及び鍵 ID は，秘匿 ID のヘッダ情報として含めておく．なお，鍵 ID は，タグ毎に一意なものではなく，相当数のタグによって共有させる．また，サーバにアクセス許可されたリーダのみが代理復号結果を得られるようになっている(図 1 の(1)参照)．

リーダからサーバへのアクセス時に認証や暗号通信を利用することにより，アクセス権を持たないリーダからの ID 不正読取を防ぐことができる．所有者がサーバへのアクセス権を自由に管理できるようにすれば，所有者のリーダだけでなく，他の信頼できるリーダに対しても，アクセス権を与えることができるようになる．このように，RFID 自身には秘匿化した ID のみを搭載し，リーダやサーバのセキュリティ管理に既存のインターネットセキュリティ技術を活用することにより，低コストなプライバシー保護システムが構築できるようになる．

また，ID の秘匿化方法として，我々は，大きく以下の 3 つの方法を検討している．

(a) ランダム化：任意の数字を秘匿 ID として格納し，サーバ側で秘匿 ID と正規 ID との対応関係を管理する方法である．この方法は秘匿 ID の大きさを任意に設定できるという利点がある．一方，サーバ側でテーブル検索処理が必要となるためスケーラビリティ低下が問題となる．

(b) 共通鍵暗号化：正規の ID を共通鍵暗号で暗号化したものを RFID に格納し，サーバ側において，代理復号する方法である．この方法は，公開鍵暗号化方法に比べて，秘匿 ID サイズが小さく，高速に復号でき，ランダム化方法に比べてスケーラビリティが高いという利点がある．一方，ランダム化方法に比べて一般的に大きな秘匿 ID サイズが必要となる．また，公開鍵暗号化方法に比べて，鍵管理のコストを低減するために，サーバ側が一括して ID の暗号化処理を行う必要があるといった運用面での負担も大きい．

(c) 公開鍵暗号化：正規の ID を公開鍵暗号で暗号化したものを RFID に格納し，サーバ側において，代理復号する方法である．この方法は，生産者などが公開鍵を用いて自由に ID を暗号化できるため，運用面での負担が小さいという利点がある．RSA などの暗号を利用した場合，秘匿 ID のサイズが数 Kbit 程度が必要となり，通常の EPC サイズである 64／96bit に比べて非常に大きくなるため，我々は同程度のセキュリティ強度をもち，秘匿 ID の大きさを 320bit 程度に抑えることが可能な楕円曲線暗号を採用した．

我々が試作したプロトタイプ[11]では，ランダム化方法と公開鍵暗号化方法とを実装している．公開鍵暗号アルゴリズムとして楕円 ElGamal を，また楕円曲線暗号演算法として，NTT で開発した OEF 高速化技術[12]を採用することにより，サーバ側の復号処理の高速化を図っている．

2) ID 追跡問題対策

上記の秘匿 ID 方式は，③-1 の所持品漏洩問題に対する解決策として有効ではあるが，③-2 の ID 追跡問題の解決手段にはならない．それは ID が暗号化されていても常に同じ値となってしまい追跡に利用できるためである．

この問題を解決する最も有効な手段として，タグ内での再暗号化処理があげられる．ここで述べる再暗号処理とは，確率暗号の性質を利用し，暗号文と公開鍵だけを用いて，異なる暗号文を生成する処理を意味する．確率暗号とは，同じ平文を暗号化するたびに異なる暗号文を得ることができる暗号を意味する．また，再暗号化された異なる複数の暗号文は，一つの秘密鍵で復号できる．先に述べた楕円 ElGamal 暗号はこうした性質を備える．この再暗号化により，毎回異なる秘匿 ID がタグから応答されるようになるため，ID 追跡を回避することが可能となる．また，サーバ側の復号処理は，先に述べた秘匿 ID のときと同様に行え，負荷が増えることもない．

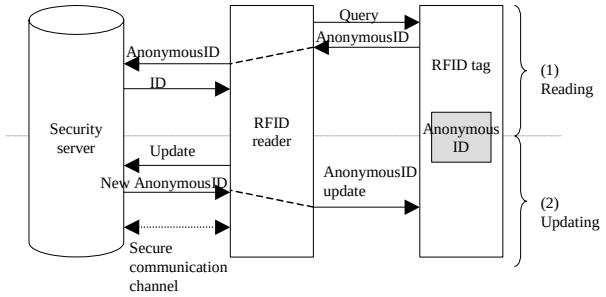

図1 可変秘匿ID方式

ただし，タグ内でこうした処理を行うためには，タグ内に秘匿 ID と公開鍵とを格納し，さらに暗号回路を実装する必要があるため，その実現はコスト的に困難となる．

可変秘匿 ID 方式

上記の理由から，再暗号化の処理をタグ内では行わず，実装コストの低い外部コンピュータや IC カードなどによって行い，更新された秘匿 ID を EEPROM などの再書込み可能な ROM に再設定させるようにした．

具体的なプロトコルを以下に示す（図 1 の(2)参照）．

Step 1: リーダが秘匿 ID の更新依頼を前述のセキュリティサーバへ送信．サーバは，既存のインターネットセキュリティ技術を用いてリーダを認証．

Step 2: サーバは，秘匿 ID に含まれる鍵 ID を取得し，新しい秘匿 ID を作成し返送する．

前述の秘匿化方法(a)～(c)の生成方法は以下のとおり．

(a)ランダム化：サーバにおいて，ほかと衝突しない新たな秘匿 ID を任意に生成し，それらの対応関係を更新する．

(b)共通鍵暗号化：サーバにおいて，正規 ID と結合させるためのパディングデータとして乱数を新たに生成し，結合データを再度暗号化する．

(c)公開鍵暗号化：楕円 ElGamal 等の再暗号化の性質をもった暗号アルゴリズムを利用して，新たな秘匿 ID を生成する．公開鍵により再暗号化が可能となるため，サーバだけでなくリーダ自身が暗号処理を行うことも可能．

Step 3: リーダが受信した秘匿 ID を RFID へ書き込む．

可変秘匿 ID 方式の拡張

さらに，暗号化する鍵の変更（鍵 ID 変更）や，さらにセキュリティサーバの更新（サーバ ID 更新＋鍵 ID 更新）も安全性の面で有効である．サーバの変更により，履歴情報が一つのサーバに過度に集中することによる危険を分散させることが可能となる．

また，タグあるいはリーダに複数の秘匿 ID をまとめて取得・格納しておき，順次利用するという方式に拡張できる．秘匿 ID を実際に更新しなくても，異なる ID が送出されるため，頻繁に更新が行えないような環境においては有効である．このように，タグの外部リソースを利用して定期的に秘匿 ID を更新することにより，長期的な追跡を回避することができる．

3) Auto-ID システムへの適用

EPC

提案方式を EPC へ適用する場合のデータ構成例(拡張 EPC)を図 2 に示す．

EPC Manager: 本来，製造メーカコードを示す領域にはセキュリティサーバを運用する会社等のコードを格納する．

Object Class: 本来，商品種別コードを示すこの領域には(a)～(c)の秘匿化方法の種別を示すサービス ID と(b)(c)で

利用する鍵 ID（サーバ側で鍵 ID と利用アルゴリズムや鍵情報との対応が管理されている）とを格納する．

Serial Number: (a)のランダム化の場合，36bit の任意の秘匿 ID を格納する．(b)の共通鍵暗号化の場合，暗号種別や鍵長に応じて 64bit～128bit の暗号化された秘匿 ID を格納する．ここにあげた秘匿 ID 長は、AES，Camellia 等のブロック暗号を想定したものであるが，同じ鍵長でよりブロック長の小さい暗号を用いれば同等の安全性を持つ短い秘匿 ID を実現でき，また そのようなブロック暗号は一般的に構成可能である[20][21]．(c)の公開鍵暗号化の場合，暗号種別に応じて，160bit～320bit の暗号化された秘匿 ID を格納する．

処理フロー

Auto-ID システム適用時の情報の流れを以下に示す．Step1:リーダは，拡張 EPC の EPC Manager あるいは Object Class も含めて，ONS サーバへ問合せを行うことにより，代理復号を実行するセキュリティサーバのアドレスを解決する．Step2:リーダは，拡張 EPC をセキュリティサーバに送信する．Step3: セキュリティサーバは，リーダの認証が成功したのち復号し，その結果をリーダに返送する．Step4: 以降は，通常と同様に処理が進められる．

また，通常の処理と透過的にするために，セキュリティサーバを PML サーバの代理サーバとして振舞わせることも可能である．リーダは秘匿 ID と通常の EPC を区別することなく，ONS によって解決されたサーバへ送信する．セキュリティサーバは，復号した EPC から真の PML サーバのアドレスを解決し，リーダに代わり PML サーバへアクセスするという形態である．

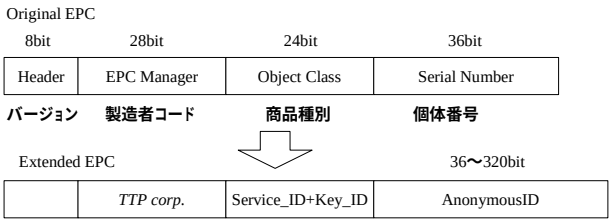

図2 秘匿ID用EPC

4) その他のセキュリティ脅威への対策

プライバシー保護機能だけでなく，ID の複製やなりすましを検出するために，MAC／電子署名付き ID も同時に検討した．電子署名アルゴリズムとして NTT で開発した楕円公開鍵暗号ベースの ECAO[13]を採用している．ECAO は EPC データを署名データに内包できるメッセージリカバリタイプの署名アルゴリズムであるため，EPC に署名データを付加する必要があるアタッチタイプと比べて必要メモリサイズを 80bit 程度削減することが可能となる．検証速度は遅いが，より署名データ(160bit)の短い Boneh らによる Short signature[19]の利用も有効である．

VI. 考察

1) 従来研究との比較

Hash Lock **方式**[9]

Hash Lock 方式は，タグ内にハッシュ回路のみを搭載した低コストな ID 読み取りアクセス制御方法である．タグは，リーダ側で管理する鍵 *key* のハッシュ値(*metaID*=*hash*(*key*))を保存しており，リーダからの ID 取得要求に対して，*metaID* を返送する．リーダは，*metaID* に対応する *key* をタグに送信し，タグが *key* のハッシュ値と *metaID* とを比較することによって，リーダを認証する．正しく認証された場合に，タグは ID を返送する．

本方式では，*metaID* 自体が固定化されているため，追跡問題が発生しうる．そのため *MetaID* の更新が必要となる．また，ハッシュ回路以外に，*metaID* 用に書換可能 ROM も必要となる．

本方式に比べて，我々の提案方式はハッシュ回路を必要としない分，低コストで実現できる．

Randomized Hash Lock **方式**[9]

Hash Lock 方式を拡張した方式であり，タグ内にハッシュ回路と乱数生成回路とを搭載した ID 可変方法である．タグは，生成した乱数 R と ID との結合ハッシュ値($hash(ID||R)$)を計算し，乱数 R と合わせてリーダに送信する．リーダは，自身が管理する全ての ID と受信した R とから，同様のハッシュ計算を行い比較し，一致する ID を見つけ出す．

我々の方式に比べて，タグ内で毎回 ID を変更できるため，安全性は高い．しかし，リーダが管理する全ての ID に対してハッシュ計算を行う必要があるため，スケーラビリティに課題が残る．また，ハッシュ回路と乱数生成回路を必要とするためコスト的な問題も検討が必要となる．

External Re-encryption **方式**[14]

本方式は，ユーロ紙幣への RFID 装着を想定したプライバシー保護方式であり，タグ内に格納している暗号化された ID がレジなどで更新される．暗号化には，公開鍵暗号の再暗号化を利用しており，また，バーコード等の併用による安全な ID 書き換えなども具体的に検討されている．

基本的な方式は，我々の方式のうち，リーダ側で行う公開鍵暗号化を用いた秘匿 ID 可変方式と同様である．我々の方式は，さらにランダム化や共通鍵暗号などにも対応しており，コスト等の要求条件により柔軟に対応できる．また，再暗号化(再秘匿化)処理をリーダだけでなく，セキュリティサーバでも実行でき，さらに，鍵やサーバ自体の変更できるなど，拡張性と安全性に優れている．

Extended Hash-chain **方式**[15]

我々が提案するもう一つの方式であり，タグ内に性質の異なる二種類のハッシュ回路 H, G を搭載する．タグは要求毎に $nonceID=G(Key_i)$ を生成しリーダに応答し，次回の送信時に備え $Key_{i+1}=H(Key_i)$ により鍵を更新する．次に，リーダは，*nonceID* をセキュリティサーバに送信し正規の ID を取得する．セキュリティサーバは，ID と Key_n (n<i+1)などを管理しており，管理している全ての ID の *Key* に対して，タグと同様の計算を繰返し，取得した *nonceID* と一致する ID を検索する．

Key が漏洩した場合でも，それ以前に収集された複数の *nonceID* が同一の ID に対応するものか否か判定することが困難であるといったフォワードセキュアな性質がある．一方 Randomized Hash Lock 方式では，(R, $hash(ID||R)$)が収集対象となるため ID が漏洩した場合には過去に収集されたものが容易に解読されてしまう危険性がある．

また，ハッシュ回路のみ利用するため，非常に低コストで実現できる可能性がある．二種類のハッシュ回路の共有化を検討することにより，さらなる低コスト化も可能である．

ただし，Randomized Hash Lock 方式以上に，サーバ側の負荷が高く，スケーラビリティに課題があり，現在，サーバ分散，高速検索などの方法を検討している．

XOR based One-time Pad 方式[16]

本方式では，リーダとタグとが複数のランダムな鍵列を共有しておき，それらを相互に交換することにより，相互を認証する．認証が正しく行われた場合，タグは ID をリーダに送信する．また，鍵列の更新には XOR 関数のみを利用するため低コストである．

ただし，一度の ID 読出しに，4 回のタグ-リーダ間通信が発生することや，更新された鍵列が盗聴などにより推測されやすいなどの問題が残る．

Blocker Tag [17]

一種の読み取り妨害機能を搭載したタグ・機器を身につけておくことにより，一緒に所持している他のタグから ID を読取れないようにする．900MHz 帯で利用されているアンチコリジョンアルゴリズムの仕組みを逆手にとった妨害方法である．我々の方式とは異なるアプローチである．

2) コスト等の制約条件

IV章の制約条件について，以下に考察を行う．

[コスト] 制約条件としてセキュリティ拡張用に 2.5K～5Kgates 程度の追加を条件とした．本提案方式では，追加回路として秘匿化方式(a),(b),(c)それぞれ，36bit，128bit，320bit 程度の書き換え可能な ROM を必要とする．

EEPROM のメモリセル面積が，数μm^2 程度であり，前述した"0.18μm ルールの場合の収容ゲート数 60Kgates/mm^2"という前提を用いれば，320bit のメモリ用に，多くとも数百ゲート程度必要になると試算できるため条件を満たしている．ただし，書き込み制御などの周辺回路も考慮する必要がある．

[許容転送データサイズ]最も転送サイズの大きくなる(c)の場合でも 400bit 程度であり，制約条件である最大 500bit を満足している．

[メモリのタンパー性]タグ上には，秘匿 ID のみが格納されているため，漏洩したとしても問題がない．

[タグ-リーダ間通信]秘匿 ID のみが流れているため，漏洩したとしても問題がない．

3) 運用性

本方式の場合，プライバシ保護の強度は，秘匿 ID の更新頻度に大きく依存する．そのため確実に短周期に更新が行われ，しかもその作業負担がまったく生じない運用方法が必要となる．例えば，導入コスト等を無視すれば，家の玄関に更新装置を設置し出入りするだけで所持品の ID が自動更新される仕組みなどが可能かもしれない．

4) 社会制度面からの対策

RFID タグがあらゆるアイテムに装着される将来の社会では，誤った利用や過度の不安，そして感情的な拒絶など人々の混乱を招く可能性がある．今回紹介した技術的な方策だけではなく，利用方法に関する正しい情報開示，啓蒙活動，企業側の運用ポリシ／規制，あるいは法的保護手段を早い時期から検討しておく必要がある．

RFID タグを導入するにあたって守るべき消費者の権利が Garfinkel によって整理されている[18]．こうした権利をさらに具体化し，社会制度及び技術面での対応策を検討していく必要がある．

VII. おわりに

将来，到来するであろうユビキタス社会において，RFID タグは，ありとあらゆるアイテムに装着され，さまざまな応用サービスへと発展していく基盤技術として期待されている．しかし，一方では，RFID の優れた性質が悪用された場合のプライバシー問題が指摘されはじめている．

本論文では，漠然とした不安として語られている RFID のプライバシー問題を，技術的な側面から整理するとともに，普及条件として最も重要となる低コスト化を考慮した解決方式を提案した．提案方式は，ID の秘匿化によりプライバシー問題の一つである所持品の漏洩問題を解決している．さらに，秘匿 ID を外部のコンピュータ資源を利用して低コストに更新させることにより，もう一つの問題である追跡問題を軽減させることができる．また，提案方式には，コストや運用上の課題が残されていること，さらには，社会制度面からの検討もあわせて行う必要があることを述べた．

今後，こうした課題に対して取組み，安心できるユビキタス社会の実現に向けて研究をすすめていく．

参考文献

[1] J. Dunlap, G. Gilbert, L. Ginsburg, P. Schmidt, J. Smith, “If You Build It, They Will Come: EPC™ Forum Market Sizing Analysis,” White Paper ACN-AUTOID-BC007, MIT Auto-ID Center, Feb. 2002.

[2] RFID Journal, “Gillette to Purchase 500 Million EPC Tags,” http://www.rfidjournal.com, Nov. 2002.

[3] C.A.S.P.I.A.N, http://www.nocards.org.

[4] 高木浩光, “固定 ID は"デジタル化された顔"-プライバシー問題の勘 所,” NIKKEI NET, http://it.nikkei.co.jp, Apr. 2003.

[5] BOYCOTT BENETTON, http://boycottbenetton.org.

[6] CNET, “Wal-Mart cancels 'smart shelf' trial,” http://www.cnet.com, Jul. 2003.

[7] MIT Auto-ID Center, http://www.a utoidcenter.org.

[8] Auto-ID Center, “ 860MHz–960MHz Class I Radio Frequency Identification Tag Radio Frequency& Logical Communication Interface Specification Proposed Recommendation, Version 1.0.0,” Technical Report MIT-AUTOID-TR-007, Nov. 2002.

[9] S. A. Weis, “Security and Privacy in Radio-Frequency Identification Devices,” Masters Thesis. MIT. May, 2003.

[10] S. E. Sarma, S. A. Weis and D. W. Engels, “Radio-Frequency Identification: Security Risks and Challenges,” RSA Laboratories Cryptobytes, vol. 6, no.1, pp.2-9. Spring 2003.

[11] “書籍向け IC タグの試作システム登場，プ ライバシー保護は暗号化で,” NIKKEI IT Pro, http://itpro.nikkeibp.co.jp, Apr. 2003.

[12] T. Kobayashi , H. Morita, K. Kobayashi and F. Hoshino, “Fast Elliptic Curve Algorithm Combining Frobenius Map and Table Reference to Adapt to Higher Characteristic,” EUROCRYPT '99, May 1999 Proceedings, Lecture Notes in Computer Science, vol. 1592, pp. 176-189, 1999.

[13] M. Abe and T. Okamoto, “A Signature Scheme with Message Recovery as Secure as Discrete Logarithm,” ASIACRYPT '99, November 1999 Proceedings, Lecture Notes in Computer Science, vol. 1716, pp. 3 78—389, 1999.

[14] A. Juels and R. Pappu, “Squealing Euros: Privacy Protection in RFID-Enabled Banknotes,” In R. Wright, ed., Financial Cryptography 2003 Springer-Verlag, 2003.

[15] M. Ohkuhbo, K. Suzuki, S. Kinoshita, “Forward-Secure Privacy Protection for Low Cost RFID,” to be apperred in CSS 2003.

[16] A. Juels, “Privacy and Authentication in Low-Cost RFID Tags,” In submission. 2003.

[17] A. Juels, R. Rivest, and M. Szydlo, “The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy,” In submission. 2003.

[18] S. L. Garfinkel, “Adopting Fair Information Practices to Low Cost RFID Systems,” Ubicomp 2002, Sep. 2002.

[19] D. Boneh, H. Shacham, and B. Lynn, “Short signatures from the Weil pairing,” ASIACRYPT '01, pages 514-532, LNCS no. 2139, 2001.

[20] Lars R. Knudsen, “The Security of {Feistel} Ciphers with Six Rounds or Less,” Journal of Cryptology: the journal of the International Association for Cryptologic Research, vol. 15, no. 3, pp. 207-222, 2002.

[21] Ronald L. Rivest, “The RC5 Encryption Algorithm,” Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings, Lecture Notes in Computer Science, vol. 1008, pp. 86-96, 1995.