ローコストRFIDプライバシ保護方法

木下真吾[†] 星野文学[†] 小室智之[†]
藤村明子[†] 大久保美也子[†]

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．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，漠然とした不安が持たれているRFIDのプライバシ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およびそのプロトタイプシステムも紹介する．

Low-cost RFID Privacy Protection Scheme

Shingo Kinoshita,[†] Fumitaka Hoshino,[†] Tomoyuki Komuro,[†]
Akiko Fujimura[†] and Miyako Ohkubo[†]

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 that is supposed as the standard of next generation RFID system, and describe its prototype system.

1. 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．たとえば，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，読み取り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み取れる，偽造や複製が困難，読み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すでに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，消費者の手にわたった後のさまざまな応用サービスに発展する可能

† NTT情報流通プラットフォーム研究所
NTT Information Sharing Platform Laboratories

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なすで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．なかでも消費者プライバシ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，スパイ映画など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やめた件などがあげられる．後者の実験中止理由の 1 つに，こうしたプライバシ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 プライバシ問題と要件を分析する．そして，検討を行ううえ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，我々の解決方法および Auto-ID システムへの適用方法，プロトタイプシステムの実装について紹介する．最後に，従来技術との比較やコストなどに関して考察する．

2. RFID システム

2.1 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（**図 1**），RFID リーダに対して情報を非接触で送出する．

RFID リーダ：タグから情報を読み取り装置であり，データベースに対して，タグ情報の書き込み・読み取りなどのアクセスを行う．

データベース：タグの ID や，読み取り場所，時間，温度などのセンサ情報，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．

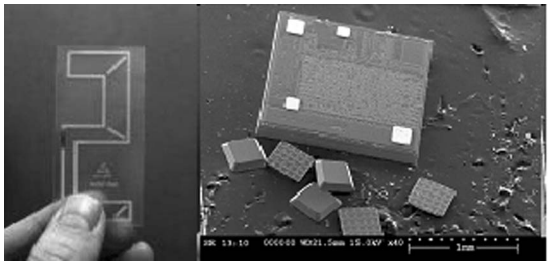

図 1 RFID タグと超小型 IC チップ（写真提供 Alien technology）
Fig. 1 RFID tag and very small IC chip (Photograph by Alien technology).

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）および記憶容量（64 ビット〜数キロバイト），暗号処理プロセッサなどのセキュリティ回路内蔵の有無，利用周波数（13.56 MHz，900 MHz，2.45 GHz）などの組合せによりさまざまな種類が存在する．

現在最も広く利用されている標準 RFID タグの 1 つとして ISO15693/18000-3 がある．このタイプの RFID タグは，Unique ID（UID）と呼ばれるタグを一意に識別するための読み取り専用の ID と，利用者が書き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 8 キロバイト程度もある．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 13.56 MHz 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，2.45 GHz・900 MHz 帯のタグは，数メートルの通信距離をとることも可能である．特に 900 MHz 帯は，10 メートルにも及ぶ通信距離をとることができ，また，数百個にも及ぶ一括読み取り性能を持つなど，タグとして非常に優れた性質を持つ．

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 “データ読み取り要求” 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

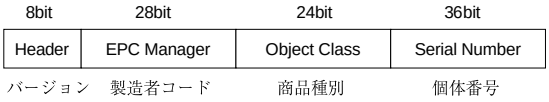

図 2 96 ビット版 EPC
Fig. 2 96 bit EPC.

化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．その代表的な取組みの 1 つに Auto-ID センターによる活動がある．

2.2 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，Electronic Product Code（EPC）[8] と呼ばれる 64 ビットまたは 96 ビットの 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，すべ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の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，商品種別コード，シリアル番号からなる商品属性を表す構造化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 Physical Markup Language（PML），PML サーバのアドレス解決サービス Object Name Service（ONS），読み取り装置の制御や EPC データの転送などを効率的に行うソフトウェア基盤 Savant などの検討も行われている．

Auto-ID システムの構成と情報の流れの例を**図 3** に示す．

Step1：リーダが “ID 取得要求” をブロードキャスト．
Step2：電波到達範囲内にあるタグが “EPC” を返送．
Step3：リーダは，EPC を用いて，ONS サーバへ問合せを行うことにより，EPC を格納すべき PML サーバのアドレスを解決．
Step4：リーダは，EPC および自身の ID，時刻，温度などのセンサ情報を PML サーバへ書き込む．

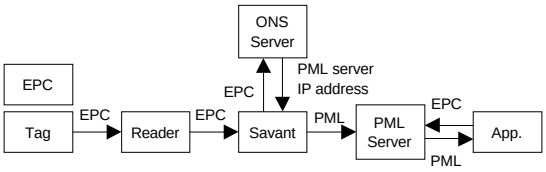

図 3 Auto-ID システム構成例
Fig. 3 Example of Auto-ID system configuration.

3. RFID プライバシ問題

3.1 RFID プライバシ問題とは

前章に述べたように，従来の RFID タグは，リーダに対して ID とユーザデータとを送信する可能性がある．ユーザデータの読み取りには，アクセス制御機能が設けられているものもあるが，ID の読み出しには，そうした制御がなく，リーダさえ持っていればだれ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 の読み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，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などへ活用するために，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み取られてしまう危険性があることなど，プライバシ侵害を危惧する声がある．これに対しては，読み取り・書き込み時のアクセス制御機能や格納データの暗号化などを用いることにより解決できる．さらに，EPC タグなどの次世代の低コストタグには，そもそもこうした情報がなく，すべてデータベース上で管理されるため，上記 ① 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，プライバシ侵害にはつながらないように考えられる．ただし，こうした ID のみであっても，プライバシ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，たとえば，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なく，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，透明なカバンを持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，たとえば，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 と結び付けられた場合，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，RFID がつねに同一のユニークな ID を返答する RFID であれば，EPC に限らず従来の UID においても起こりうる．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できなくなる危険性もある．

3.2 プライバシ保護要件

上記の RFID プライバシ問題を解決する最も単純な方法として，EPC タグの Class I チップ[9] でもサポートされている Kill 機能がある．本機能は，たとえば，タグが消費者の手にわた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．もちろん，無効化した場合には，購入以降に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，さまざまな将来の応用サービスの芽を摘むことになる．そのため，本研究では，商品購入後も継続的に RFID の利用ができることを前提条件とする．

RFID タグを生かしたままプライバシ保護を実現するための方法として，大きく以下の 3 つのアプローチが考えられる．

1. ノーマルタグアプローチ：既存の RFID タグを改造することなく，アルミ箔や妨害電波などに外的な手段により電波的な読み取りを防ぐ．後述する Blocker tag 方式などもこの方式に入る．
2. スマートタグアプローチ（アクセス制御）：RFID に読み出し制御機能を持たせ，不正ユーザへの ID 送出自体を防ぐ．
3. スマートタグアプローチ（ID 秘匿化）：RFID から制約なく ID は出力されるが，ID 自体が暗号化などにより秘匿化される．

アプローチ 1 は，商品をアルミ箔付きカバンなどに入れられるか否か，あるいは，妨害電波がすべての所持品の読み取りを防止できているかなど，物理的な制約によって適用範囲が限定的にならざるをえないこと，さらに明示的な対処を忘れると安全性が保てないなどの問題がある．また，アプローチ 2 は，パスワードなどによる保護が一般的となるが，RFID 自体へ搭載するパスワードの更新など管理コストが高いこと，また，パスワードを安全に効率良く管理できたとしても，リーダはタグから ID など識別情報を受信することなくパスワードを送信しないとならないため運用方法が限定されてしまう．たとえば，所有者が持つすべての商品のパスワードを同じにするか，あるいは，商品に仮 ID を印刷しておき，その値をバーコードなどで読み取り，それに応じたパスワードを送信するなどといった手段が必要となる．上記のような問題を考慮し，本研究ではアプローチ 3 に基づき検討を行う．

アプローチ 3 の場合に，ID に求められるセキュリティ要件を以下に示す．

秘匿性：「所持品の漏洩問題」を回避するために，ID に含まれる商品情報が推測されないようにしなければならない．

同定不能性：「ID 追跡問題」を回避するために，タグから送出される秘匿 ID が常に同じであってはならない．さらに，変更された複数の秘匿 ID が同一 ID に基づくものかどうかなど，その関連性が

容易に識別されてはならない．

もちろん，復号の権利を与えられた主体だけは，本来の ID を復号できるようにしなければならない．

4. 検討条件

上記プライバシ保護要件以外の制約・前提条件を以下に整理しておく．

[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 10) 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，0.18 μm ルールの場合，1 mm^2 のチップのコストは\$0.08 程度，1 mm^2 に収まるゲート数は 60 K ゲート程度とされている．この結果，目的のコストを達成するためには，ゲート数を 7.5〜15 K ゲートに抑える必要がある．また，100 ビット程度の ROM のみを搭載した EPC チップが 5〜10 K ゲートとされているため[11]，セキュリティ用におおよそ 2.5〜5 K ゲート程度の追加が可能となる．

[許容転送データサイズ] 13.56 MHz 帯および 900 MHz 帯の転送レートと同時読み取り数は，それぞれ，13.56 MHz：26 Kbps/50 個程度，900 MHz：28 kbps/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 0.5 kbps 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，500 ビット程度が許される．

[メモリのタンパ性] 耐タンパ性メモリは，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．ただし，タグへのデータ書き込みは，物理的な近接や接触，あるいは，リーダからの電波方向調整など盗聴されないよう工夫できる．

[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．

5. 提案方式

5.1 可変秘匿 ID 方式

「所持品の漏洩」と「ID 追跡」といった RFID 特有のプライバシ問題を解決するために必要となる ID に対するセキュリティ要件である「秘匿性」と「同定不能性」とを実現する最も有効な手段として，タグ内での ID 再暗号化処理がある．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，再暗号化された複数の異なる暗号文は，1 つの秘密鍵で復号できる．楕円 ElGamal 暗号などはこうした性質を備える．この再暗号化により，盗聴者が本来の ID 情報，すなわち所持品情報を知ることができなくなる．さらに，その暗号化された ID 値も読み出しごとに異なってくるため，ID 追跡を回避することが可能となる．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，さらに再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．

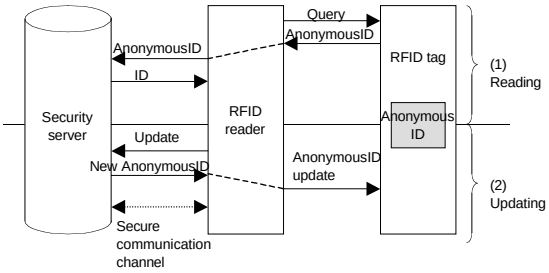

図 4 可変秘匿 ID 方式
Fig. 4 Unidentifiable anonymous ID scheme.

本提案方式では，こうしたコストの問題を解決するために，再暗号化など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 などの再書き換え可能な ROM に再設定させるようにした．以下に，提案方式の ID 復号方法，ID 秘匿化方法，ID 再秘匿化方法，ID 改竄検出方法について説明する．

ID 復号方法

リーダによってタグから読み取られた秘匿 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．また，セキュリティサーバは，ID ごとにアクセス可能なリーダリストを管理する．これにより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 4** の (1) のフェーズ参照）．また，所有者がサーバへのアクセス権を自由に設定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．さらに，タグ付き商品の所有権の移行を反映してリーダリストを更新すれば，以前の所有者（製造会社や店舗など）からであってもアクセスできないようにすることができる．

また，大量の一般商品への RFID 適用を想定し，複

数のセキュリティサーバによる負荷分散と複数の鍵による危険分散とを実現するために，サーバ ID および鍵 ID を秘匿 ID のヘッダ情報として含める ID 体系にした．なお，RFID ごとに異なる鍵を利用した方が，鍵の漏洩による影響の局所化などセキュリティ上は望ましいが，逆に鍵 ID が一意になってしまうためプライバシ侵害につながる可能性がある．一方，鍵を単一にすると，鍵 ID が不要となるためプライバシ保護の観点からは望ましい．しかし，共有する RFID の数に応じて鍵漏洩時の被害も大きくなる．そのため，鍵漏洩の危険性を分散できる程度に，かつ鍵 ID から商品の特定などプライバシ侵害につながらない程度に，鍵を複数の RFID によって共有させる必要がある．詳細な鍵管理方法に関しては，商品種別や流通量・分布など実際の適用環境にも大きく影響されるため，本論文の範囲を超える．

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保護システムが構築できるようになる．

ID 秘匿化方法

本方式の ID 秘匿化方法として，大きく以下の 3 つの方法を用いる．いずれも一般的な暗号技術を利用したものである．

(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，スケーラビリティの低下が問題となる．

(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 のサイズが数キロビット程度必要となり，通常の EPC サイズである 64/96 ビット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持ち，秘匿 ID の大きさを 320 ビット程度に抑えることが可能な楕円曲線暗号を採用した．

ID 再秘匿化方法

ID 秘匿化方法だけでは,「秘匿性」要件を満足できても，秘匿 ID が固定化されてしまうため,「同定不能性」要件を満足できない．そこで，秘匿 ID を再秘匿化させることが必要となる．以下にその手順を示す（図 4 の (2) のフェーズ参照）．いずれも一般的な暗号技術を用いたものである．

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する．

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) ごと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 などの再暗号化の性質を持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，リーダ自体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 へ書き戻す．

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，不正な第三者による長期的な追跡を回避することができる．さらに，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することも可能である．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．

ID 改竄検出方法

本方式では，秘匿 ID を RFID に書き戻す必要があるため，不正リーダによる秘匿 ID の改竄や正規リーダによる誤った書き込みなどを防止する必要がある．

所有者が管理する特定のリーダでのみ再書き込みさせるような利用形態においては，RFID にパスワード

保護による書き込み制御機能に持たせることにより，ある程度安全に運用することが可能となる．また，書き込み時にリーダとの物理的接触を必要とさせることにより，不正リーダによる再書き込みの危険性を軽減させることが可能となる．

本提案方式では，上記のような前提がおけない場合にも適用可能な改竄検出方法を提案する．RFID に読み出し専用型 ROM 領域と，書き換え可能型 ROM 領域の 2 つの領域を持たせる．読み出し専用領域には，サーバ ID および鍵 ID を格納し，書き換え可能領域に秘匿 ID を格納する．すなわち，サーバ ID および鍵 ID が改竄されることはなく，秘匿 ID だけが改竄の対象となる．この結果，仮に秘匿 ID が改竄されたとしても，サーバが復号を行う際，あるいは，正規リーダが再秘匿化する際に，鍵と秘匿 ID との不一致が起こり，復号時の ID 構造確認などによって改竄の有無を検出することが可能となる．もちろん，MAC や署名などを付加することにより，改竄検出の確実性を高めることも可能である．一方，ある RFID の秘匿 ID が，その RFID と同じサーバ ID と鍵 ID とを持った別の RFID に書き込まれた場合，検出できないという問題がある．しかし，商品に関連するサービスなどを利用することによって，改竄の事実をサービスレベルの不一致により検出することができる可能性が高い．また，読み出した ID を再秘匿化せずに書き戻すという攻撃に対しては，自宅玄関の再秘匿化装置など確実に信頼できる装置がある場合には，その時点で再秘匿化されるため安全となる．

5.2 Auto-ID システムへの適用

本提案方式は，RFID 仕様，ID 体系などに依存せず RFID システム一般に対して適用可能な技術である．本節では，提案方式をより具体化するために，将来の RFID 標準システムとして期待されている Auto-ID システムへの適用方法を説明する．

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 5** 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など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，セキュリティサーバを識別するサーバ ID と，秘匿化方法 (a)〜(c) や鍵を識別する鍵 ID（サーバ側で，この 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: 秘匿化方法 (a) のランダム化の場合，36 ビットの任意の秘匿 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 64 ビット〜128 ビット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 など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，160〜320 ビットの暗号化された秘匿 ID を格納する．

現在の Class I EPC タグは，ROM のみを搭載する仕様となっているため，可変秘匿 ID 方式による Serial Number 領域の書き換えはできない．これを実現するためには，書き換え可能型 ROM 領域を搭載するように改良するか，今後，仕様化が予定されている書き換え可能型 ROM 搭載の Class II 以上の EPC タグを利用する必要がある．

処理フロー

Auto-ID システムへの適用構成例を**図 6** に，また，読み取り処理時の情報の流れを以下に示す．

Step 1: 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．

Step 2: リーダは，拡張 EPC をセキュリティサーバに送信する．

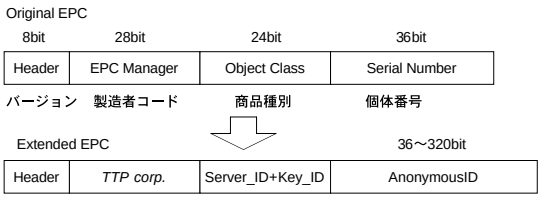

図 5 秘匿 ID 用 EPC
Fig. 5 EPC extension for anonymous-ID.

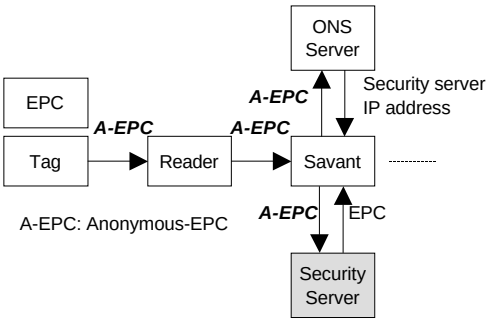

図 6 Auto-ID システムへの適用構成例
Fig. 6 Example of applying to Auto-ID system.

図 7 本への RFID 装着例
Fig. 7 Example of book with a RFID tag.

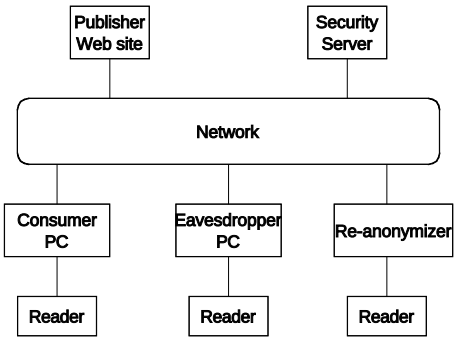

図 8 プロトタイプシステム構成
Fig. 8 Prototype system configuration.

Step 3: 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．
Step 4: 以降は，通常と同様に処理が進められる．

また，通常の処理の透過性を高めるために，セキュリティサーバを PML サーバの代理サーバとして振る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．

5.3 プロトタイプシステム

Auto-ID システムをベースとし，提案方式のプロトタイプシステムを開発した．本システムでは，RFID を装着した書籍を利用している（**図 7**）．また，**図 8** に示すように，書籍購入者の PC，盗聴者の PC，再秘匿化用 PC と，購入者限定サービスを提供する出版社の Web サーバ，秘匿 ID の復号を行うセキュリティサーバがネットワークに接続されている．本システムで利用した RFID およびリーダ装置，ならびに実装した秘匿化方法と利用アルゴリズムなどを**表 1** に示す．

表 1 プロトタイプシステム仕様
Table 1 A specification of the prototype system.

RFID	Philips社 I-CODE SLI
リーダ	FEIG ミッドレンジリーダ
秘匿化方法	ランダム化方法 36ビット乱数
	公開鍵暗号化方法 楕円ElGamal, 鍵長160ビット

図 9 購入者 PC 画面．RFID を用いた購入者限定サービス画面
Fig. 9 Purchaser's PC screen. Purchaser-only service using RFID.

RFID I-CODE SLI は ISO 15693 準拠であり UID が ROM に格納されている．そのため，提案方式で必要となる ID 領域の書き換えが行えない．本プロトタイプでは，書き換え可能型 ROM 領域であるユーザデータ領域を ID 領域と見なして実装した．また，楕円曲線暗号演算法には，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．

次に，本プロトタイプシステムを利用したデモンストレーションシナリオを紹介する．

まず，購入者は自身のリーダに購入した書籍をスキャンさせると，**図 9** に示すような購入者限定サービスサイトにアクセスすることが可能となる．このとき，秘匿 ID がセキュリティサーバによって正規の ID に復号され，購入者 PC がそれを用いて出版社のサイトにアクセスしている．次に，**図 10** は，秘匿化されていない ID を格納した RFID 付き書籍を鞄に入れた購入者が外出し，盗聴者リーダによって不正にスキャンされた場合の様子を示している．それに対し，**図 11** は，提案方式を採用した場合の盗聴者の画面を示している．盗聴者は，ID が暗号化されておりセキュリティサーバに対するアクセス権を持たないため，本来の ID を

図 10 盗聴者 PC 画面 1．所持品盗聴の様子
Fig. 10 Eavesdropper's PC screen 1. Successful eavesdropping on belongings.

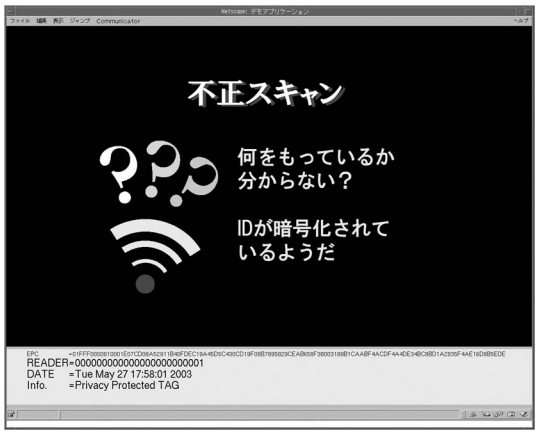

図 11 盗聴者 PC 画面 2．所持品盗聴防止の様子
Fig. 11 Eavesdropper's PC screen 2. Failed eavesdropping on belongings.

知ることができない．さらに，**図 12**，**図 13** は，再秘匿化用 PC によって，関連性のない ID に次々と変更され，追跡ができなくなっている様子を示している．

6. 考　　察

6.1 従来研究との比較

6.1.1 従来研究紹介

Hash Lock 方式[10)]

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．ただし，$metaID$ 自体が固定化されているため，追跡問題が発生しうる．それを回避するため $metaID$ の更新が必要となる．また，ハッシュ回路以外に，$metaID$ 用に書き換え可能型 ROM も必要となる．

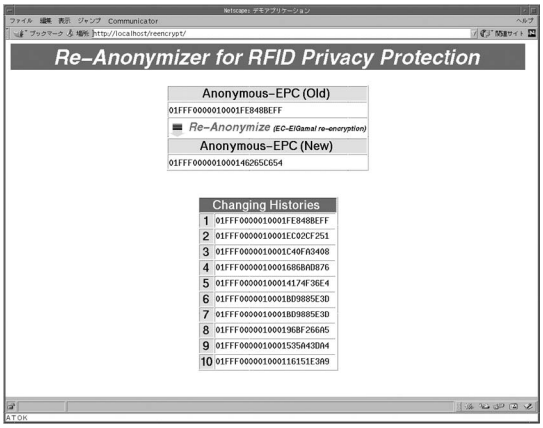

図 12 再秘匿化 PC 画面 1．再秘匿化（ランダム化）を用いた ID 変更の様子
Fig. 12 Re-anonymizer PC screen 1. ID Re-anonymizing using randomizing.

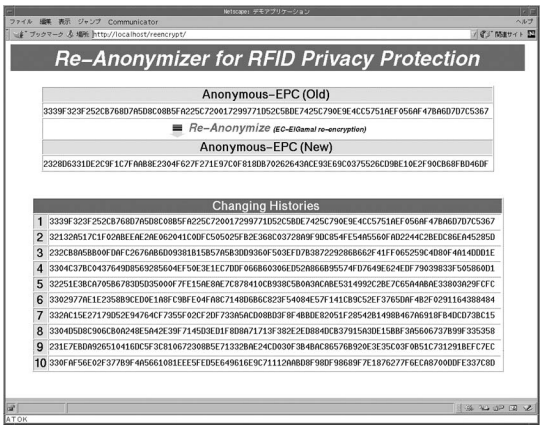

図 13 再秘匿化 PC 画面 2．再秘匿化（公開鍵再暗号化）を用いた ID 変更の様子
Fig. 13 Re-anonymizing PC screen 2. ID Re-anonymizing using re-encryption.

Randomized Hash Lock 方式[10)]

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，自身が管理するすべての 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．

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いる．ただし，我々の提案方式のように暗号文と公開鍵だけを用いて異なる暗号文を生成する再暗号化処理ではなく，紙幣に印刷された平文の ID と乱数とを用いて繰り返し暗号化する方法を採用している．また，ID 更新時の改竄を防止するために，紙幣に印刷されたパスワードを使って書き込みの制御および暗号データの検証を行っている．

Extended Hash-chain 方式[15)]

我々が提案するもう 1 つの方式であり，タグ内に性質の異なる 2 種類のハッシュ回路 H，G を搭載する．タグは要求ごとに $nonceID = G(Key_{\mathrm{i}})$ を生成しリーダに応答し，次回の送信時に備え $Key_{\mathrm{i+1}} = H(Key_{\mathrm{i}})$ 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 $Key_{\mathrm{n}}(\mathrm{n} < \mathrm{i}+1)$ などを管理しており，管理しているすべての ID の Key に対して，タグと同様の計算を繰り返し，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（Extended Hash-chain 方式の Key に相当）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．

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，低コストに実現することが可能となる．ただし，一度の ID 読み出しに，4 回のタグ–リーダ間通信が必要となる．

Blocker Tag [17)]

一種の読み取り妨害機能を搭載したタグ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 を読み取れないようにする．900 MHz 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．RFID をいっさい改造することなく，Blocker Tag を携帯するだけで，所持している RFID タグの読み取りを防止させることができるという優れた特徴がある．しかし，国際標準となっている HF 帯 RFID には効果がないこと，さらに，HF 帯用 Blocker Tag が開発されても，その通信距離がせいぜい 1 m 程度であるため，1 つの Blocker Tag でカバーできる範囲が限定されてしまうなどの問題がある．さらに，周波数帯に関係なく，所持している全 RFID の読み取り防止を行えているかどうか確実に保証できなこと，さらに，他人の所有するする Blocker tag も含め，さまざまな場所に Blocker tag が遍在するようになった場合，妨害しているタグを特定できずに，本来の読み取りさえもできなくなってしまう可能性がある．

6.1.2 比較評価

提案方式と既存方式との比較結果を**表 2** に示す．なお，Blocker tag は，他方式と比べてアプローチが大きく異なり，さらに確実性や実効性などについて不明な点が多いことから今回は比較対象からはずしている．比較基準として，安全性，RFID タグコスト，復号性能（復号スケーラビリティ），運用負担をあげている．安全性に関しては，プライバシ保護レベルを反映する ID の同定不能性とフォワードセキュア性を比較している．秘匿性に関しては，すべての方式で満足されているため，本比較から外している．ここで，同定不能性とは，複数の ID を観測し，それらが 1 つの RFID から出力されたものであるか，別の RFID から出力されたものであるか識別できない性質を意味する．また，フォワードセキュア性とは，RFID タグ内の秘密情報が漏洩した場合でも，過去に収集された ID 情報からプライバシ侵害につながるような情報が得られない性質を意味している．これ以外にも ID の改竄など他の安全性項目もあるが，本比較では，プライバシ保護にのみ関連する項目を比較している．次に RFID タグコストに関しては，IC チップのゲート増加量をもって比較評価することが望ましいが，ASIC の種類，選択するハッシュ関数や乱数生成回路などによって，そのサイズが異なることから，必要となる主な追加回路をあげるにとどめた．ここで紹介している方式の書き換え可能型 ROM サイズはたかだか 500 ビット程度であるため，一般的には，書き換え可能型 ROM はハッシュ演算回路や乱数生成回路に比べて非常に小さいゲートサイズで実装できる．

本表に示すとおり，提案方式および External Re-encryption 方式は，書き換え可能型 ROM のみを搭載すればよく，ハッシュ演算回路や乱数生成回路を必要としないため，他方式に比べコスト面で非常に有効な方式である．なお，XOR based OTP 方式も同様に外部の計算機によって秘匿 ID を更新するタイプで

表 2 RFID プライバシ保護方式比較
Table 2 A comparison of RFID privacy protection methods.

方式	機関	安全性		RFIDﾀｸﾞ ｺｽﾄ (*2)	復号性能 ｽｹｰﾗﾋﾞﾘﾃｨ (*3)	運用負担
		同定不能性	ﾌｫﾜｰﾄﾞｾｷｭｱ性(*1)			
提案方式 可変秘匿ID方式	NTT	△ ID更新頻度少	○	RAM	ﾃｰﾌﾞﾙ検索 or 共通鍵復号 or 楕円復号	× 定期更新必要
Hash Lock	MIT	△ ID更新頻度少	○	RAM + HASH	ﾃｰﾌﾞﾙ検索 +HASH	×
Randomized Hash Lock	MIT	○ 毎回更新	×	HASH + 乱数生成 (*4)	HASH x M (*6)	○
External Re-encryption	RSA	△ ID更新頻度少	○	RAM	楕円復号	×
Extended Hash-chain	NTT	○	○	RAM + HASH x 2 (*5)	HASH x NM (*7)	○
XOR based OTP	RSA	△ ID更新頻度少	○	RAM	ﾃｰﾌﾞﾙ検索 +4通信 (*8)	×

メリット | デメリット

(*1) RFID内の秘密情報がタンパされた場合でも，過去に収集されたID情報からプライバシ侵害につながる ような情報が得られない性質
(*2) 厳密なゲート換算が難しいため，必要な回路種類によって比較した
ここに書かれている方式の書換可能型ROM（本表ではRAMと記述）は高々500bit程度であるため，
一般的に RAM << HASH, 乱数生成回路の関係が成立する
(*3) 復号時間そのもののではなく，管理ID数と読取り回数に対する復号処理時間のスケーラビリティを評価
(*4) 乱数生成回路としてHASH演算回路を流用することも可能．その場合はHASH回路のみが必要
(*5) 2つのHASH演算回路を共有させることが可能．その場合はHASH回路1つのみで十分
(*6) Mは，サーバが管理しているIDの総数
(*7) Nは，RFIDのリードカウント値（これまでに読取られた累積数
(*8) タグ-サーバ間で4回通信を行う必要があり，セッション状態管理などタイマのないタグには実効上困難

表 3 提案方式と External Re-encryption 方式との比較
Table 3 Proposed method vs. External Re-encryption.

方式	機関	復号依頼主体	復号主体	復号権限管理	復号鍵	復号鍵所有者	ID改竄防止策
提案方式 可変秘匿ID方式	NTT	消費者 （複数人）	ｾｷｭﾘﾃｨ ｻｰﾊﾞ (TTP)	ｾｷｭﾘﾃｨｻｰﾊﾞに 認可リーダ登録	複数種類有 商品で共有	消費者ではない ｾｷｭﾘﾃｨｻｰﾊﾞ (TTP)	鍵ID領域をROM化 により改竄検出
External Re-encryption	RSA	捜査当局 （単一）	未検討	未検討	単一	捜査当局	紙幣に印刷したﾊﾟｽﾜｰﾄﾞを書込み制御に利用 暗号追試による検査

あり，書き換え可能型 ROM のみを搭載する低コスト方式である．本方式では，タグ–サーバ間でデータのやりとりが 2 往復必要であり，他方式の 4 倍の通信回数となる．この通信回数の多さは通信時間の増加につながることはもちろんだが，タグ側にセッションの状態を保存させておく必要があり，電力やタイマなどを持たないタグの場合異常系への対処が困難になる可能性があるなど実用性の問題も大きい．

一方，提案方式と External Re-encryption 方式は，Randomize Hash Lock 方式や Extended Hash-chain 方式に比べて，ID の更新頻度が低くなってしまうため同定不能性が劣る．また，更新を行うための運用負担も高いという問題点がある．このように提案方式および External Re-encryption 方式は，RFID タグに対するコスト制約が非常に強く，毎回 ID を変更する必要がないような安全性要件の場合には有効である．ただし，ID 更新を行うための機器などが社会インフラとして充実することも必要となる．

次に，提案方式と External Re-encryption 方式との比較を行う．両方式は，外部計算機において ID を更新し RFID に再格納するという点において同様である．ただし，紙幣と一般商品といった適用対象の違いから，秘匿 ID の復号方法や改竄防止方法，鍵管理方法などが異なる．これらの違いを**表 3** に整理する．

まず，我々の提案方式では，一般の商品への RFID 適用モデルを想定し，その場合に必要となる復号アーキテクチャも含めて提案している．具体的には，ネットワーク上に秘匿 ID の復号を行う第三者信頼機関としてのセキュリティサーバを配置し，セキュリティサーバに対するクライアントのアクセス制御を秘匿 ID の復号可否制御に利用している．一方，External Re-encryption 方式では，紙幣への RFID 適用モデルを想定しており，その場合には，復号依頼主体も復号主体も，捜査当局に限定されるため，復号モデルを単純化できる．なお，文献 14) には，復号アーキテクチャの詳細は示されていない．

さらに，提案方式では，大量の一般商品に対して，不特定多数の一般消費者が復号を依頼するようなモデルを想定している．この場合，商品すべてを単一の復号鍵に対応させることは，安全上好ましくなく，また運用上も困難となる．そのため，提案方法では，複数の鍵を商品間で共有できるようにしている．一方，External Re-encryption 方式では単一の鍵が利用されている．また，鍵漏洩の危険性を低減させるために，閾値付き秘密分散方法を利用している．こうした単一鍵による管理は，捜査当局だけが閉じた世界で利用する場合には問題が少ないが，上記のように不特定多数によって利用する場合にはその適用が難しい．

また，ID を再格納する場合の改竄防止策についても，提案方式では鍵 ID 領域の ROM 化と復号結果の正当性検証により書き換え可能型 ROM 上の秘匿 ID の改竄検出を行う．この方法では，同一の鍵 ID を持つ別の秘匿 ID に変更されてしまう危険性が残ってしまうが，その場合でも ID が再秘匿化でき固定化されることない．さらに，RFID を用いた商品に関連するサービスなどを利用することによって，サービスレベルでの妥当性検証により改竄の事実を検出することができる可能性が高い．一方，External Re-encryption 方式では，紙幣に印刷された ID やパスワードを用いて RFID への書き込み制御を実現している．印刷パスワードによって財布の中にある紙幣の ID を不正に書き換えられることを防げる．さらに，再暗号処理に用いる乱数パラメータも RFID 内に保持しておき，そのパラメータと，印刷された本来の ID と公開鍵とから暗号データを生成し，格納されている秘匿 ID と比較することによって改竄検出を行う．この方法では，ID とパスワードとが印刷表示可能な商品であること，さらに商品 1 つ 1 つを取り出し，バーコードなどにより ID やパスワードを光学的に読み取る必要があるなど，その適用範囲が制限されてしまう．また，パスワード値としては，本来の ID に対するディジタル署名値が利用されているが，この値はリーダから RFID へ保護されず送出されるため盗聴されやすいばかりでなく，この値自身がユニークな値となるため追跡情報として悪用される危険性も残る．

このように，我々の提案方式は，復号アーキテクチャの具体化，より安全でかつ運用性に優れた鍵管理方法の採用，適用性や運用性を妨げない改竄検出方法など，より一般商品への RFID 適用性に優れたものとなっている．

また，External Re-encryption の関連研究として，文献 22) に，公開鍵情報を必要とせず，乱数生成のみで再暗号化を実現する Universal Re-encryption 方法が提案されている．External Re-encryption 方式のように単一の公開鍵を利用すれば，すべての RFID が同一の公開鍵を共有するため，そこからプライバシ侵害につながる危険性が少なくなる．しかし，大量の RFID に対する公開鍵が単一の場合，秘密鍵漏洩時の影響がはかりしれないため，通常は複数の鍵を利用することが多い．鍵の数が RFID の数と同等程度に多い場合には，その鍵情報あるいは鍵の ID 自身が一種の ID 情報となりうるため，それに基づくプライバシ侵害の危険性が残ってしまう．

Universal Re-encryption 方法は，再暗号処理時に公開鍵鍵情報を公開する必要がないため，より高いレベルのプライバシ保護を実現する．しかし，公開鍵情報を秘密にできても，復号時には依然として復号鍵を特定する必要がある．すなわち，結局は RFID から出力される秘匿 ID の中に復号鍵を特定するような鍵 ID を含ませておく必要がある．もちろん，この復号鍵 ID がユニークかつ固定化されないようにしなければならない．なお，この方法では，ベースとなる ElGamal 暗号と同等の安全性を確保するために 2 倍の鍵長およびメッセージ長を必要とするといった効率面でも課題もある．

上記のように，Universal Re-encryption 方法は復号時には ID が必要になってしまうこと，鍵長やメッセージ長が 2 倍必要となること，など総合的に評価すると，鍵を複数用意し，暗号化方法として通常の再暗号化処理を行う我々の提案方法の方がシステムトータ

ルとして優れていると考えられる．

6.2 コストなどの制約条件の評価

4 章に述べた制約条件について，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 2.5 K〜5 K ゲート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，36 ビット，128 ビット，320 ビット程度の書き換え可能型 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 “0.18 μm ルールの収容ゲート数 60 K ゲート/mm^2” という前提を用いれば，320 ビットのメモリ用に，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 400 ビット程度であり，制約条件である最大 500 ビットを満足している．
［メモリのタンパ性］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．

6.3 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は，これまで人々が経験したことのない未知の社会となるため，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．

こうした状況に対しては，技術的な方策だけではなく，技術や危険性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．

これまでにガイドラインとして，Garfinkel による「RFID タグを導入するにあたっての守るべき消費者の権利[18]」や，Auto-ID センターの後継機関である EPCGlobal[23] による「Guidelines on EPC for Consumer Products[24]」，RFID 反対派である CASPIAN[3] による「Position Statement on the Use of RFID on Consumer Products[25]」，また，日本においては経済産業省による「電子タグに関するプライバシ保護ガイドライン[26]」などのいくつか提案されている．

こうしたガイドラインは，事業者，消費者間との合意形成上，非常に有効な手段になると思われる．しかし，実際のガイドライン検討および運用にあたっては，不正行為が行われた場合のセーフガードの役割を担う法律との整合性を，それぞれの国で施行されているプライバシ関連法制の違いを念頭におきながら検討していくことが重要となる．特に，日本では，“個人情報の保護に関する法律（平成十五年法律第五十七号)” いわゆる個人情報保護法との整合性が不可欠になると思われる．現在の個人情報保護法では，RFID のような自動認識技術による個人情報の収集が明示的に規定されおらず，その適合性に関しては議論の余地が残されている．こうした問題を明確化するために，我々は，上記の RFID 利用ガイドラインと，個人情報保護法および日本の既存法律との整合性検証を行っている[27]．今後は，この結果を，日本における安全な RFID 利用，さらには，各国の法律の違いなどを考慮したグローバルなガイドライン策定・運用に役立てる予定である．

7. 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問題の 1 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 1 つの問題である追跡問題を解決する．さらに Auto-ID システムへの適用方法とプロトタイプシステムを紹介した．

また，提案方式には，コストやシステム性能，プライバシ保護の強度が更新頻度に大きく依存してしまうことなど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などもあわせて行う必要があることを紹介した．

今後，こうした課題に対して取り組み，RFID を利用した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予定である．

参考文献

1) Dunlap, J., Gilbert, G., Ginsburg, L., Schmidt, P. and Smith, J.: If You Build It, They Will Come: EPC^{TM} 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 (Nov. 2002).

http://www.rfidjournal.com
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”—プライバシ問題の勘所，NIKKEI NET (Apr. 2003). http://it.nikkei.co.jp
5) BOYCOTT BENETTON. http://boycottbenetton.org.
6) CNET, Wal-Mart cancels ‘smart shelf’ trial (July 2003). http://www.cnet.com
7) MIT Auto-ID Center. http://www.a utoidcenter.org
8) Brock, D.L.: The Electronic Product Code (EPC) – A Naming Scheme For Physical Objects, White Paper MIT-AUTOID-WH-002, MIT Auto-ID Center (Jan. 2001).
9) 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).
10) Weis, S.A.: Security and Privacy in Radio-Frequency Identification Devices, Masters Thesis, MIT (May 2003).
11) Sarma, S.E., Weis, S.A. and Engels, D.W.: Radio-Frequency Identification: Security Risks and Challenges, *RSA Laboratories Cryptobytes*, Vol.6, No.1, pp.2–9 (Spring 2003).
12) Kobayashi, T., Morita, H., Kobayashi, K. and Hoshino, F.: Fast Elliptic Curve Algorithm Combining Frobenius Map and Table Reference to Adapt to Higher Characteristic, *Proc. EUROCRYPT ’99*, LNCS 1592, pp.176–189 (1999).
13) Abe, M. and Okamoto, T.: A Signature Scheme with Message Recovery as Secure as Discrete Logarithm, *Proc. ASIACRYPT ’99*, LNCS 1716, pp.378–389 (1999).
14) Juels, A. and Pappu, R.: Squealing Euros: Privacy Protection in RFID-Enabled Banknotes, *Financial Cryptography 2003*, Wright, R. (Ed.), Springer-Verlag (2003).
15) Ookuhbo, M., Suzuki, K. and Kinoshita, S.: Cryptographic Approach to a Privacy Friendly Tag, *RFID Privacy Workshop@MIT* (Nov. 2003). http://www.rfidprivacy.org
16) Juels, A.: Privacy and Authentication in Low-Cost RFID Tags, In submission (2003).
17) Juels, A., Rivest, R. and Szydlo, M.: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, In submission (2003).
18) Garfinkel, S.L.: Adopting Fair Information Practices to Low Cost RFID Systems, *Ubicomp 2002* (Sep. 2002).
19) Boneh, D., Shacham, H. and Lynn, B.: Short signatures from the Weil pairing, ASIACRYPT ’01, LNCS 2139, pp.514–532 (2001).
20) Knudsen, L.R.: 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) Rivest, R.L.: The RC5 Encryption Algorithm, *Proc. Fast Software Encryption: 2nd International Workshop*, Leuven, Belgium, 14–16 December 1994, LNCS 1008, pp.86–96 (1995).
22) Golle, P., Jakobsson, M., Juels, A. and Syverson, P.: Universal re-encryption for mixnets, In submission (2002).
23) EPCGlobal. www.epcglobal.org
24) EPCGlobal, Guidelines on EPC for Consumer Products. http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html
25) CASPIAN, Position Statement on the Use of RFID on Consumer Products (Nov.14 2003).
26) 経済産業省：電子タグに関するプライバシ保護ガイドライン. http://www.meti.go.jp/feedback/data/i40316aj.html
27) 藤村明子，鈴木幸太郎，木下真吾，森田 光：RFID プライバシ保護の実現に関する法制度及び技術的提案，情報ネットワーク法学会第 3 回研究大会予稿集，pp.23–26 (2003).

(平成 15 年 11 月 28 日受付)
(平成 16 年 6 月 8 日採録)

木下 真吾

1991 年大阪大学基礎工学部物性物理学科卒業．同年日本電信電話株式会社に入社．以来，分散システム，インターネットプロトコル，セキュリティの研究開発に従事．現在，情報流通プラットフォーム研究所主任研究員．1998 年 DiCoMo98 ベストプレゼンテーション賞受賞，2003 年 CSS2003 優秀論文賞受賞．電子情報通信学会会員．

星野 文学

1996 年東京大学工学部物理工学科卒業．1998 年同大学院工学系研究科修士課程修了．同年日本電信電話株式会社に入社．

小室 智之

1998 年東京工業大学大学院電気電子工学専攻修了．同年日本電信電話株式会社に入社，情報通信研究所に配属．PKI の分野を中心に研究開発に従事．2004 年 4 月より，東日本電信電話株式会社法人営業本部に勤務．

藤村 明子

1997 年慶應義塾大学法学部法律学科卒業．1999 年同大学院政策・メディア研究科修士課程修了．同年日本電信電話株式会社入社．現在，情報流通プラットフォーム研究所に所属し，法制度と情報セキュリティ技術の相互補完の観点から研究を推進．著書に『サイバーセキュリティの法と政策』（NTT 出版）等．情報ネットワーク法学会，電子情報通信学会各会員

大久保美也子

1995 年信州大学工学部電気電子学科卒業．1997 年同大学院修士課程修了．同年 NTT 入社．2004 年中央大学大学院理工学研究科情報工学博士課程修了（工学博士）．暗号プロトコル等の研究に従事．2000 年 SCIS 論文賞受賞．IACR，電子情報通信学会各会員．