

RFIDにおけるプライバシーを守るためのID管理方法について

井上 創造[†] 安浦 寛人[†]

本論文では、RFIDを用いて物品を識別する「デジタルネーミング」技術におけるプライバシーの問題を指摘し、RFIDタグに暗号回路を必要としない安価な解決方法を提案する。プライバシーは主に、物品と個人が不用意に関連付けられることにより発生する。本論文ではこの問題について、物品のIDを物理的に複数のRFIDタグに分散し、その値を個人が与えるという方法でプライバシーの漏洩を防ぐ。この方法は、RFIDタグを安価に抑えることができる点、利用者がRFIDの利用を望まないかぎりは追加的な費用は発生せずにプライバシーを保護できる点、プライバシーが物理的に視覚化された形態で表現されるため理解しやすい点、プライバシーの初期のIDを復元する方法を残すために物品のライフサイクル管理にも使用できる点で有用である。

Novel ID Management for Protecting Privacy against RFIDs

SOZO INOUE[†] and HIROTO YASUURA[†]

In this paper, we propose an approach to protect privacy in the "Digitally Named World", which is the environment in which radio frequency ID's (RFIDs) are attached to any objects in the world, and any objects in the real world can be found by the readers of the RFIDs and the networked database system. The approach is to assign partial ID sequence to a object, and the rest is given by user-assignable RFID tags. This approach attempts to give users the controllability of the uniqueness of IDs from local to global, thereby enabling IDs private or public ones in the required stage of the object's life cycle.

1. はじめに

近年の計算機システムや情報システムの小型化は、特定の建築物の中の特定の場所に固定されていた計算機資源が人間が生活する環境へ浸透し始めているといえる。このような社会で、社会的な規律や慣習とどのように融和していくかを議論することは、「計算機上で実現される仮想の世界」ではなく、「計算機がいたるところに浸透した現実の世界」を設計するという意味で非常に重要である。情報技術が浸透した現在、金融や医療の分野における情報技術の問題がそのまま現実の社会の事件や問題に直結することが少なくない。つまり「いつでもどこでも何でもできる」という考えだけで情報技術が進歩するのは危険であり、「その状況で何をすべきなのか、何をしてはいけないのか」という考え方への転換が必要である。

本研究では、RFIDが浸透した社会でのプライバシーの問題を考える。RFIDタグとは、無線通信を用いて

物品の識別をするためのIDであり、通常は電源部を持たず、外部から無線で電力が供給される³⁾。RFIDタグを用いて現実の物品を識別可能にすることを「デジタルネーミング」と呼ぶ。RFIDは物品の自動認識の手段として期待されているため⁴⁾、デジタルネーミングの社会との融合を考えることは重要である。

本論文では、デジタルネーミングにおけるプライバシーについて、その問題を指摘し、RFIDタグに暗号回路を必要としない安価な解決方法を提案する。プライバシーは主に、物品と個人が不用意に関連付けられることにより発生する。本論文ではこの問題について、物品のIDを物理的に複数のRFIDタグに分散し、その値を個人が与えるという方法でプライバシーの漏洩を防ぐ。この方法は、RFIDタグを安価に抑えることができる点、利用者がRFIDの利用を望まないかぎりは追加的な費用は発生せずにプライバシーを保護できる点、プライバシーが物理的に視覚化された形態で表現されるため理解しやすい点、プライバシーの初期のIDを復元する方法を残すために物品のライフサイクル管理にも使用できる点で有用である。

以下では、2節で、デジタルネーミング技術と、そこでのプライバシーの問題を述べる。3で関連研究を述

[†] システム LSI 研究センター・大学院システム情報科学研究院情報工学部門 春日市春日公園 6-1
System LSI Research Center, Kyushu University,
{soso/yasuura}@ic.cccu.kyushu-u.ac.jp

べ、4節で、個人情報秘匿したままデジタルネーミングを実現する方法を提案する。5節で結論を述べる。

2. デジタルネーミングとプライバシー

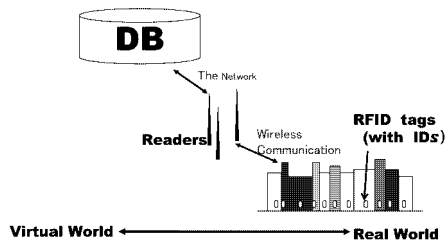


図 1 想定するデジタルネーミングシステム

デジタルネーミングのために、図 1 に簡単に示すようなシステムを想定する。想定するシステムでは、物品につけられた RFID タグは、ネットワークに接続されたリーダと交信する。利用者は、RFID タグにかかれた識別子を用いてネットワーク上のデータベースを検索することにより、物品についての種々の情報を得ることができる。このような、RFID タグには識別子、つまり ID のみが与えられ、リーダがネットワークに接続されたシステムは、AUTO-ID センター¹⁸⁾ やユビキタス ID センター¹⁹⁾ でも構想されており、今後普及することが予想される。

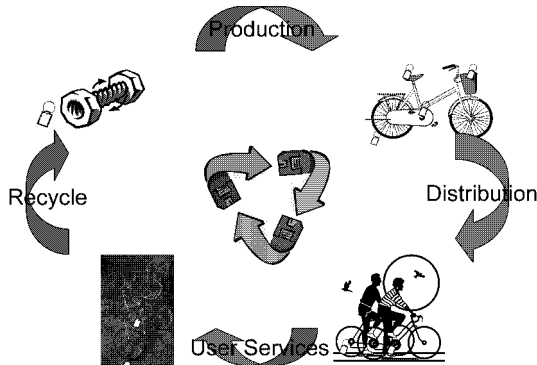


図 2 物品のライフサイクル

デジタルネーミングにおける重要な特徴は、図 2 に示すように、物品の製造、供給、消費、リサイクルといった、ひとつの物品に対して所有者が遷移しながら物品の管理が行われる点である。つまり、物品の製造時に、物質や、その抽出の方法、解体の方法といった、リサイクルや資源の再利用に必要な情報を埋め込むことによって、効率的なリサイクルを行なうことができる。バーコードをはじめとする現在のタグの方式は、

記録できる情報量が少ない、汚れると使えない、タグとリーダが接触しないと情報を伝えることができない、といった制限から、リサイクルにいたるまで管理が可能なシステムは実現できていない。

また、このように RFID タグを物品のライフサイクルのなかで一貫して使用することは、RFID タグのコストを実質的に削減することを可能にする。つまり、RFID タグのコストを複数の所有者が分担することができるため、所有者一人当たりの RFID タグのコストは抑えることができる。

2.1 ID そのもののプライバシー

デジタルネーミングにおいては、物品やリーダが、公共の空間など、複数の人間が共有する空間におかれることも考えられる。RFID は受動的な無線通信を行なうが、無線通信では、通信が第三者により容易に盗聴されるし第三者が介入し信号を発生することができる。このことが、RFID から発信される ID そのものが、システム運用者にとってプライバシー、つまり個人情報を漏洩する問題につながる可能性がある。以下ではこの問題を詳しく述べる。

ID そのものが契機となって個人情報を漏洩する場合は以下の 3 つに分けられる。

- A. 物品の ID とその所有者が、ネットワーク上のデータベースにおいて不用意に関連付けられてしまう場合。
- B. 物品の ID と所有者が、現実世界における観察を通じて関連付けられてしまう場合。
- C. 物品の ID と所有者が、過去の認識の履歴をもとに関連付けられてしまう場合。

A については、たとえば消費者が物品を購入する際に、販売店のデータベースにおいて消費者と物品が関連付けられてしまうと、リーダがいたるところに配置された世界では、その後の物品の動きが追跡されてしまう。これはひいては、消費者が常に持参する物品の場合、消費者の行動が販売店に追跡されてしまうことにつながってしまう。その消費者本人にとっては、所有する物品を管理できることは利点となるが、本人の望まない相手にまで物品を追跡されるのはプライバシーの観点から問題がある。

B は、物品の置かれた現実世界の情報を通して個人が特定されてしまう問題である。たとえば、物品が住居の中におかれている場合、その物品の所有者はその住居の住人にある程度特定されてしまう。別の例として、個人が非接触型の乗車券を識別する鉄道の改札口を通ったときにその個人が携帯する物品の情報を読み取った場合、その物品がその個人の所有物であること

を推測できてしまう。これは、本人を氏名などで特定はできないとしても、「目の前にいる人物」という特定の仕方ができるという例である。

AとBの混合した場合もありうる。たとえば、目の前にいる人が持っている物品のIDを読み、そのIDから標準化されたEPCコード¹⁶⁾やISO-15903¹⁷⁾のような標準化された値をよみ、その値を元にコードが意味する商品の種類を読み取る場合である。標準化されたコードは標準化されたデータベースにアクセスするという意味でAに属する。またこの例では、物品を唯一に識別しなくても、物品の種類を特定するだけで問題になりうることに注意が必要である。

Cは、物品とそのIDの関連が漏洩しなくても、同じIDを何度も漏洩することが問題になることを意味している。たとえば、スーパーマーケットのポイントカードのIDを用いてPOSシステムを検索することにより、特定の顧客に対してどのような購入履歴をもつかを知ることができる。同様に、固定したIDを持つ物品を持って列車で移動すれば、その乗客の行動は追跡できる。Cのみがプライバシーの問題になるかどうかは社会的な議論が必要だが、列車の例とBと組み合わせれば、目の前にいる人の行動履歴がわかるというように、AやBと組み合わせることにより、Cによるプライバシーの問題は大きくなることは確かである。

さらに、文献¹⁸⁾では、特に位置情報という現実世界の情報に対して、IDの値がわからなくても発生するプライバシーを指摘している。たとえば、ある部屋からRFIDをもつ物品が1つだけ出て別の部屋に入った場合は、そのIDがわからなくても物品の履歴をとることができる。このことは、位置情報と組み合わせれば、プライバシーの問題は拡大する可能性がある事を示している。

2.2 低コストRFIDタグの限界

デジタルネーミングにおいてプライバシーを保護するためには、利用者がリーダを通してRFIDタグと交信する際に、リーダを扱うための認証をすることにより達成できるように思える。しかし、以下のような場合が考えられるため、これは十分でない。

- リーダを扱うための認証を通った利用者は、そのリーダの通信圏内にあるすべてのRFIDタグと交信することができる。そのため、その利用者にアクセスが許されていない物品でも、そのリーダの圏内にあれば識別が可能になってしまう。
- 悪意を持った人間が、自分で認証を必要としないリーダを作った場合、リーダの通信圏内にある物品を識別することが可能になってしまう。

- RFIDタグとリーダ間の通信を暗号化することは現時点の低コストRFIDタグでは難しいため、RFIDタグとリーダ間の通信は簡単に傍受される。RFIDタグとリーダの間で物品の識別子を流すと、悪意を持った人間がこの通信を傍受した場合、その物品の識別子を知ることが可能になってしまう。

つまり、RFIDタグが通信する相手を信用されたリーダのみに限定することは不可能であり、なおかつ通信内容を傍受されないようにすることも不可能である。デジタルネーミングにおいてはRFIDタグは大量に必要なため、RFIDタグにかけられるコストは非常に低いため、この問題は重要である。

3. 関連研究

Weisらは、ハッシュ関数と擬似乱数生成器をRFIDタグに実装することにより、プライバシーを保護する方法を提案している⁹⁾。この方式は、RFIDタグが毎回自動的に異なる値をIDとして返答するもので、IDを安全な場所と方法で更新する必要がないという点が優れている。しかし、この方式はハッシュ関数と擬似乱数生成器という、数万ゲートを必要とする回路をRFIDに組み込む必要があり、一般的な暗号方式ほどではないとしてもRFIDタグのコストが増大してしまう。デジタルネーミングにおいては、どんなに安いRFIDタグであってもプライバシーを保護することは重要である。

大久保らも、ハッシュ関数を2つRFIDタグに実装することにより、Weisらと同様のプライバシー保護を行う方法を提案している^{11),12),14)}。この方法は、RFIDタグに元のIDを継続的に格納せずにIDを変更していくために、Weisらの手法に比べて、RFIDタグそのものへの物理的な攻撃に強いと言える。

Juelsらは、ある範囲のIDの値をランダムに応答するような、ブロッカータグというRFIDタグの使用を提案している¹⁰⁾。ブロッカータグを物品のRFIDタグと同時に使用している間は、物品のRFIDタグのIDを読み取ることができないため、利用者が希望する間に選択的にIDをリーダから隠すことが可能となる。この方法は物品のRFIDタグには追加的なコストは必要がない点で利点があるが、Tree-WalkingプロトコルというUHF帯で用いられる限定的な認識プロトコルにのみ有効である点、ブロッカータグの通信圏を物品のRFIDタグと比較して十分広くしなければならぬ点、利用者がブロッカータグに追加的なコストを払わないとプライバシーが守られない点に問題がある。筆者らは、書換え可能なメモリをRFIDタグに追加

して ID を手動で書き換え、元の ID を隠す方法を提案している¹¹⁾。この方法は上記の方法と比較して、安全な環境で書き換えが必要になる点が問題であるが、暗号回路を用いる方法に比べ RFID タグのコストを抑えることが可能である。また、筆者らはさらに、RFID タグを物理的に分割することでプライバシーを保護する方法を提案している¹²⁾。次章からはこの方法を発展させた方法を提案する。

RFID のプライバシーについて、法的な側面からの議論も始まっており^{10),13)}、技術的な解決策とともに、社会的に受け入れられるシステムを模索することが必要である。

4. プライバシを守るための ID 管理

本節では、2.1 節で指摘した「RFID タグとやりとりされる情報から、物品に関連する個人を特定できない」ことを実現するための ID 管理方式を提案する。提案する方式は、以下のような基本的な考え方を組み合わせるものである。

- (1) プライバシを守りたい場合には、ID を他の ID と競合がおきるような長さに物理的に分割することにより物品を唯一に識別できないようにする。ただし必要な場合には、何らかの方法で元の ID に戻す方法を用意しておく。
- (2) 物品の所有者が、自分で生成する ID をその RFID タグに与えることにより、他人には物品とその ID の関連が分からないが自分だけにはわかるようにする。

提案する手法は、ID の唯一性を、必要に応じてデジタルネーミングシステム全体から、所有者の範囲まで可変にする方法である。プライバシーの問題は、物品のライフサイクルの中で、常に起きるわけではない。たとえば、物品が消費者の手に渡ったときにはこのような問題が発生するが、図 2 における、製造や物流、リサイクルの段階では必要がなく、むしろ誰にでも物品を識別できたほうが、環境問題への効果や効率の面で利点が多い。提案する手法は、必要に応じてプライバシーの保護を選択することができるものである。

4.1 ID の物理的な分割

提案する手法では、まず物品に対する ID を図 3 に示すように、次の 2 つの領域に分ける。

- **クラス ID:** 物品の ID のうち、データベースのキーとなりえたり、標準化された ID 体系に関連付けることができるフィールド。たとえば、バーコード標準における JAN コード体系が物品の ID に含まれる場合、この部分が該当する。

- **純 ID:** 物品の ID のうち、クラス ID でないフィールド。このフィールドは、製品のシリアル番号のように、クラス ID が同一の物品のなかで識別するために与えられることが多い。

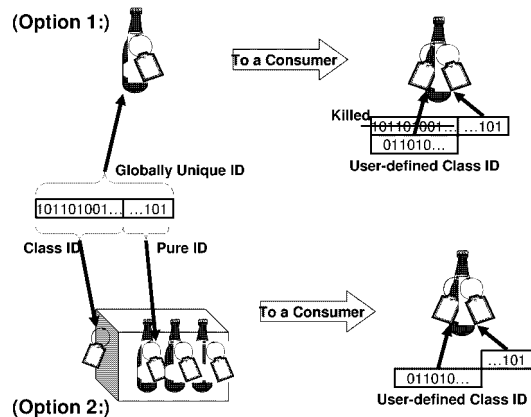


図 3 ID の物理的な分割

純 ID だけでは、他の物品の純 ID と重複する可能性があるため、たとえば別の会社の製品の同じシリアル番号といったように、物品を唯一に識別できないことに注意する。さらに、物品の所有者（例：小売業者）は商品を次の所有者（例：消費者）に渡す時点で、クラス ID を無効にする。この方法としては、初めからクラス ID を物品の RFID に持たせない方法と、消費者に渡す時点でクラス ID のみを無効化（Kill¹⁴⁾、文献¹⁵⁾）する方法が考えられる。前者の場合は、箱や、防犯用タグといった消費者に渡す前に外されるものにクラス ID を入れておくことが考えられる。

次の所有者（例：消費者）は、RFID を利用する必要がなければ何もする必要はないが、RFID を利用したければ、自分用のいくつかのクラス ID（ユーザクラス ID）を持つ RFID タグを用意しておく。このタグをシール状などにしておいて物品に添付することで、自分のクラス ID と純 ID の結合値が自分用の物品 ID となる。

ユーザクラス ID の生成の仕方を以下に示す。物品 i のユーザクラス ID u_i は、所有者が秘密にもつ値 k_i と、物品の純 ID p_i を、一方方向関数で変換したものである。以下では前者の例を用いて説明する。この場合、ハッシュ関数 H を用いて、 $u_i = H(k_i \| p_i)$ と定義できる。ただし、 k_i, p_i および H は、以下の条件を満たす必要がある。

- (1) $u_i \| p_i$ が他の物品と十分な数だけ重複する。つ

まり、ある物品 o_i について、 $u_{o_i}|p_{o_i} = u_{o_j}|p_{o_j}$ となる。このことは、 u_{o_i} と p_{o_i} がそれぞれ他の物品と重複する可能性があることを意味する。

(2) $u_{o_i}|p_{o_i}$ が他の物品と重複しない。つまり、どの物品 o_j についても、 $u_{o_i}|p_{o_i} \neq u_{o_j}|p_{o_j}$ となる。

(3) $u_{o_i}|p_{o_i}$ が同じ所有者の他の物品と重複しない。つまり、所有者 U のどの物品 $o_{U,i}$ についても、 $u_{o_i}|p_{o_i} \neq u_{o_{U,i}}|p_{o_{U,i}}$ となる。

(2) を多数の利用者で実現するためには工夫がいるが、たとえば利用者の ID と乱数を結合し十分長いビット列を出力するハッシュ関数で変換することで実現できる。

4.2 ユーザクラス ID 付与時の ID の認識

所有者が RFID を利用する必要がなければ、物品には p_{o_i} のみが ID として残ることになるが、このときには (1) の条件より p_{o_i} が他の物品と多数重複するため、物品の認識には利用できない。

以下では、単一のリーダが、物品 o に対して、ユーザクラス ID u_{o_i} および純 ID p_{o_i} を認識した場合の物品 ID の識別方法を示す。所有者は、自分が管理する u と純 ID p のリストから、 $u_{o_i} = H(u|p)$ を満たすような o を検索することで物品が o であることを識別できる。他の物品と誤識別する恐れについては、(3) の条件から所有者の物品について $u|p$ が重複するような u は存在しないため、所有者にとって $u|p$ に対して u は一意に決定し、かつ (2) の条件から物品が異なれば $u|p$ が異なるため、誤識別はおきない。

リーダの圏内に複数の物品がある場合には、複数ある u および p をすぐに関連付けることができないが、圏内の物品のすべての u と p の組について上記の検索をすることで識別が可能である。

第三者が物品を識別しようとしても、所有者の秘密値 u_{o_i} を知らないために識別ができない。このことを以下に検証する。第三者が知りうるのは、ユーザクラス ID u_{o_i} および純 ID p_{o_i} のみである。これだけの情報では、(1) の条件から、他に重複する u_{o_i} 、 p_{o_i} 、あるいは $u_{o_i}|p_{o_i}$ が存在するため、第三者にとって物品の識別ができない。

4.3 議 論

本節で提案した方法により、2.1 節 A、B で示した、「物品の ID と、その物品を使う個人がネットワーク上にあるデータベースまたは現実世界における観察において不用意に関連付けられてしまう」問題は防ぐことができる。たとえば、販売店のデータベースにおいて消費者と物品が関連付けられても、その後消費者がクラス ID をユーザクラス ID に置き換えることによって、販売店は物品の ID のすべてを知ることができな

くなくなってしまう。また、2.2 節で示したうちの 1 つの方法で RFID タグの情報がリーダに読まれても、その情報がどの物品と関連するのかを理解できるのは、ユーザクラス ID を付加した本人だけである。

逆に、ユーザクラス ID を付加した本人にとっては、ユーザクラス ID を付加する際に、物品のもともとのクラス ID と、ユーザクラス ID と純 ID を知ることができるため、物品に関するネットワーク上のデータベースと、現実世界における物品の検索を両方利用することが可能である。

さらに、提案する方法は、RFID にたよらない方法でもとの ID を復元する方法を提供することができる。たとえば、製品が回収された場合、メーカーは製品の外見からクラス ID を特定し、純 ID と組み合わせることで元の ID を得ることができる。ただし現場にない製品の場合は外見からクラス ID を特定できないので、純 ID だけでは元の ID を知ることはできない。つまり現場で物品を扱うという限定された場合にのみ元の ID を復元できる。

また提案する方法は、所有者が希望するときのみコストをかけた RFID の利用を可能にし、希望しない場合は利用者はコストをかけずにプライバシーを守秘することができる。さらに、利用者は、物理的にタグを分割するという方法により、プライバシーの保護に対して理解しやすい可視化の手段を得ることができる。暗号化を用いたほかの手法では、利用者にプライバシーが保護されていることの明示的な説明手段が必要となることが考えられる。

以上のことから、「本人以外には、RFID タグとやりとりされる情報から、物品を特定できない」ことが実現できるが、「RFID タグとやりとりされる情報から、物品に関連する個人を特定できない」と結論づけるには早計である。2.1 節 C でも示した、「所有者の行動が物品の認識履歴から特定されてしまう」問題を検討する必要がある。つまり、物品と ID (つまりクラス ID と純 ID の結合) を関連付けなくとも、ID の認識の履歴をみることにより、一旦 ID と所有者が関連付けられるとそのプライバシーの漏洩が拡大する問題である。たとえば、駅の改札口において、個人とともに移動する物品の ID を読めば、その ID の認識履歴を元にその個人の過去、あるいは未来の行動が追跡できてしまう。この問題を解決するためには、ユーザクラス ID を、文献^{[9],[14]}のような手法を用いて定期的に書き換えることが有効な手段の一つであるが、RFID タグに追加回路が必要になることと、認識時にリーダ側で検索処理に時間がかかることが問題になる可能性があ

る。本手法では、ユーザクラス ID がそのままでは多数重複しているため、この問題を回避できる可能性があるが、地理や物品の移動をモデル化しての詳細な検証が今後必要である。

また、プライバシーではなくセキュリティの問題として、第三者が物品の ID を成りすまさせることが考えられる。RFID タグに書かれた情報が成りすまされた場合には、監視を続けるリーダが、成りすましが発生したことを物品の所有者に通知できるようにすることにより、この問題を解決することができるが、この手法は、リーダが RFID を常には監視できないような環境や読み取り精度が低いリーダでは有効ではないため、更なる検討が必要である。

5. ま と め

本論文では、RFID タグにより物品が計算機により自動的に識別可能となるデジタルネーミング技術について、そのプライバシー問題と解決のための ID 管理方式を提案した。デジタルネーミングでは、物品と個人が不用意に関連付けられることによるプライバシーの問題が新たな問題として発生する。本論文ではこの問題について、ID を物理的に分割し、その一部を所有者が決定した値として与えるという方法で、プライバシーを保護する方法を提案した。この方法は、常に物品の本来の ID を復元できる方法が残されているため、物品のリサイクル時にデジタルネーミングが役立つという点で、物品のライフサイクルの管理が可能であり、環境問題にも貢献できる方法である。

謝 辞

本論文は、平成 14-15 年度科学研究費補助金学術創成研究・課題番号 14CS0218 および、平成 15-16 年度科学研究費補助金若手研究・課題番号 15700100 によるものである。

参 考 文 献

- 1) S. Inoue, S. Konomi, H. Yasuura, "Privacy in the Digitally Named World with RFID Tags", Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing, (2002).
- 2) S. Inoue, H. Yasuura, "RFID Privacy Using User-Controllable Uniqueness", RFID Privacy Workshop, Nov. (2003), <http://rfidprivacy.org/>.
- 3) P. Hewkin, "Smart Tags - The Distributed Memory Revolution". IEEE Review (1989).
- 4) R. Want, K. P. Fishkin, A. Gajjar, B. L. Harrison, "Bridging Physical and Virtual Worlds

- with Electronic Tags". Proc. Int'l Conf. CHI 99 (1999) pp. 370-377.
- 5) M. Weiser, "Some Computer Science Issues in Ubiquitous Computing". Communications of the ACM, 36(7) (1993) pp. 75-84.
- 6) Finkenweller, K., 「RFID Handbook」, Nikken Kogyo Pbl. Japan (2001).
- 7) S. E. Sarma, S. A. Weis, D. W. Engels, "Radio-frequency Identification Systems", CHES'02, LNCS no. 2523, Springer-Verlag, (2002), pp. 454-469.
- 8) S. A. Weis, S. E. Sarma, R. L. Rivest, D. W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", Int'l Conf. Security in Pervasive Computing, (2003).
- 9) A. Juels, R. Rivest, M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", (2003), <http://theory.lcs.mit.edu/~rivest/>.
- 10) S. Garfinkel, "Adopting Fair Information Practices to Low Cost RFID Systems", Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing, (2002).
- 11) 大久保美也子, 鈴木幸太郎, 木下真吾, "Forward-Secure RFID Privacy Protection for Low-cost RFID", Proc. Computer Security Symposium (CSS'03), Oct., (2003).
- 12) 木下真吾, 星野文学, 小室智之, 藤村明子, 大久保美也子, "RFID プライバシー保護を実現する可変秘匿 ID 方式", Proc. Computer Security Symposium (CSS'03), Oct., (2003).
- 13) 藤村明子, 鈴木幸太郎, 木下真吾, 森田光, "法制度から見た RFID プライバシー保護実現手段に関する考察", Proc. Computer Security Symposium (CSS'03), Oct., (2003).
- 14) Miyako Ohkubo, Koutarou Suzuki, Shingo Kinoshita, "Cryptographic Approach to a Privacy Friendly Tag", RFID Privacy Workshop, Nov. (2003), <http://rfidprivacy.org/>.
- 15) D. Chaum, "Untraceable electronic mail, return address, and digital pseudonyms", Communications for the ACM, 1981.
- 16) A. R. Beresford, F. Stajano, "Location Privacy in Pervasive Computing", IEEE Pervasive Computing Magazine, pp.48-57, Jan-Mar. 2003.
- 17) ISO/IEC, SC31, WG2, <http://usnet03.us-council.org/sc31/sc31.wg2.cfm>.
- 18) MIT AUTO-ID Center Homepage, <http://www.autoidcenter.org/>.
- 19) Ubiquitous-ID Center Homepage, <http://uidcenter.org/>.