九州大学大学院
システム情報科学紀要
第7巻 第2号 平成14年9月

Research Reports on Information Science and
Electrical Engineering of Kyushu University
Vol.7, No.2, September 2002

RFIDタグを用いた安全で効率の良いデジタルネーミング社会について

井上 創造* ・ 安浦 寛人*

Toward the Digitally Named World with Security and Convenience Using RFID Tags

Sozo INOUE and Hiroto YASUURA

(Received June 20, 2002)

Abstract: Recent years' advances in information technology and system LSI technology are spreading computing resources into ubiquitous places in the real world. In such an environment, 'What we should not do' is important as well as 'What we can do', since the problem in the computer science directly results in the problem in the real world. In this paper, we discuss the possibility and challenges in the 'Digitally Named World', which is the environment in which 'radio frequency ID's (RFIDs) are attached to any goods in the world, and any objects in the real world can be found by the readers of the RFIDs and the networked database system. Especially, we address the problem of security, privacy, total power consumption, and lifecycle management of the objects, and we propose the method for managing privacy about the relationship between objects and individuals.

Keywords: RFID, Digitally named world, Networked database system, Ubiquitous computing, Privacy management, Computer security

1. はじめに

近年，情報技術およびシステムLSI技術が急速に進歩したことにより，計算機資源を従来では考えられなかったようなさまざまな場所で利用できるようになってきている．高度な動画像処理やプログラム実行が可能な携帯電話は一つの例である．

このように，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することが，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」という考え方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タグを用いて，効率的かつ安全な社会を実現することを目指す．**RFIDタグ**とは，無線通信を用いて物品の識別をするためのIC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．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．

本論文では，RFIDタグにより物品が計算機により識別可能になったデジタルネーミング社会について，その可能性と問題点を示す．デジタルネーミング社会は，セキュリティやエネルギー問題，環境問題とあわせて考慮する必要がある．特に，物品と個人が不用意に関連付けられることによる個人情報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，個人が物品に識別子を与えるという方法で，個人情報を保護する方法を提案する．この方法は，常に物品の唯一の識別子は保存されているため，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．

以下では，2.節でRFIDタグの基本的な構造と応用を述べ，3.節で，デジタルネーミング社会の可能性と課題を議論する．4.節で，個人情報を秘匿したままデジタルネーミング社会を実現する方法を提案する．5.節で結論を述べる．

2. RFID タグ

RFIDタグとは，無線通信を用いて物品の識別をするためのICである．本節では，デジタルネーミングを実現するRFIDタグおよびその背景となる基礎的な技術を述べる．

平成14年6月20日受付
* 情報工学部門

2.1 RFID タグの構造

RFIDタグの基本的な構造を**Fig. 1**に示す．通常は電源部を持たず，外部から無線で電力およびクロックが供給される．RFIDタグは外部から電力を受け取り，内部で計算を行なった後，無線で結果を出力する．電力の供給と通信を行なう外部の機器を，**リーダ**と呼ぶ．RFIDタグの内部には，無線通信を行なうRF (Radio Frequency) 回路や計算を行なうロジック回路のほか，読み込み専用メモリ(ROM)あるいは書き込み可能メモリ(RAM)を持つことができる．

メモリの記憶容量は，64キロバイトの製品が出現している．また形状は，小型で種々の形状をしたものが存在し，カード，キーホルダ，シールといった形のものがある．アンテナ部を除いた部分が1mm角以下のものも発表されている[6]．

リーダとRFID間の通信に要する時間は0.5秒程度で，通信距離は最大で5メートル程度が可能である．

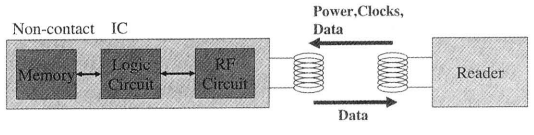

Fig.1　An RFID tag

2.2 RFID タグの応用

RFIDタグの応用は，主にメモリに物品の識別子，つまりその物品に与えられる唯一の値を記憶させ，大量にある物品を効率よく管理するために用いられる．

食料品や服飾の小売店では，商品にRFIDタグをつけることによって販売管理システムと連携し，小売のコストダウンを図っている．また，物品の製造や物流の工程では，各部品や製品にRFIDタグをつけることによって生産，物流システムと連携し，効率化が実現できる．このような応用では，RFIDタグが非接触型の通信を行なうことができることが利点として活用されている．たとえば小売店では，レジで従業員が商品を手にとってバーコードリーダにかざすという手間が必要ない．また，生産，物流システムでは，同じラインを流れる多品種の製品群を確実に管理することができる．

交通機関においては，非接触型のICカードによる電子支払いシステムが実用化されている．改札機にリーダが設置され，利用者は接触型の改札機に比べてすばやく改札を通り過ぎることができる．また，カードの中のRFIDタグにはIDが記録され，金額の情報はリーダに接続された中央のデータベースに記憶されているため，定期券の場合はICカードが紛失しても身分証明により再発行することが可能である[5]．また，紙幣や，コンサートやイベントにおけるチケットにもRFIDタグが埋め込まれ，偽造防止を狙う試みが行なわれている[6]．非接触型のタグは，接触による消耗がないため，10年ほど耐用できることが利点である．

自動車の鍵にRFIDタグを埋め込むことによって，自動車の盗難防止に大きな効果が上がっている．自動車のエンジンは，鍵のシリンダ部が，鍵と，RFIDタグの識別子を確認しないと発動しない．

食品業界では，食品の安全を保障するため，家畜の個体識別を行なう試みがなされている．家畜に，カプセル型，注射型，首輪型といったRFIDタグをつけることによって，同種の家畜の個体ごとに栄養管理を行なうことができる．

また，図書館などで大量にある蔵書を，RFIDタグによって管理し，容易に検索できるようなシステムも実用化されている．蔵書にRFIDタグを付加し，本棚にリーダを付加することにより実現している．従来の文献検索システムとは異なり，検索対象の蔵書の位置まで検索できることが利点である．仮に利用者が所定の位置に蔵書を置かなかったとしても検索できる．

このように，RFIDタグを応用したシステムでは，非接触型の通信を利用して，現実の世界の多様な形状，または一見では区別できないような物品に対する識別を，長期間にわたって提供することにより，効率的なサービスや，盗難防止，偽造防止といった安全性を実現している．

2.3 他の識別システムとの比較

RFIDタグによるシステムは，他の識別システムと比較しても優れる点が多い．他の主な識別システムとの比較を**Fig. 2**および**Fig. 3**に示す．この情報は文献2)を参考にした．

図において，音声認識やバイオメトリクスは，識別の対象が人間であるという前提があるため，デジタルネーミングのための技術には適さない．

	バーコード	OCR	画像認識	音声認識	バイオ（指紋）	接触型カード	RFIDタグ
識別対象	物品	文字	人、物品	人	人	カード	物品
リーダの価格	安い	安い	高い	高い	高い	安い	普通
人による識別	制限あり	可能	可能	可能	困難	不可能	不可能
不正な複製、変更	可能	可能	可能	可能（録音テープを使う）	不可能	不可能	不可能
読み書き速度	4s以下	4s以下	5s以上	5s以上	5〜10s以上	4s以下	0.5s
最大通信距離	0〜50cm	0〜1cm	直線で見える距離	0〜50cm	方式による	直接接触	0〜5m（日本の現状では2m）
一括読み取り	難しい	難しい	視界に入れば可能	難しい	難しい	難しい	容易

Fig.2　Readers in several identification systems

図から，RFIDタグが優れる点として，不正な複製や改

	バーコード	OCR	画像認識	音声認識	バイオメトリクス	接触型カード	RFIDタグ
データ容量(バイト)	1〜100	1〜100				16k-64k	16k-64k
個体の価格	非常に安い(0〜数円)	安い				普通〜高い	高い(100円〜2万円)
汚れや泥れによる破損	あり	あり				あり	なし
向きや位置の制限	低い	低い				あり	なし
劣化の影響	あり	あり				あり(接触部分)	影響なし

Fig.3 Identification targets in several identification systems

造ができない，読み書き速度が速い，一括読み取りが容易である，データの書き込みが可能である，記憶容量が大きい，タグの破損や劣化の影響がないという点が上げられる．

また，システムの運用によって利点にも欠点にもなりうる点として，タグに書かれた情報を人が識別が不可能である点，通信距離が長い点，タグの向きや位置の制限がない点が上げられる．タグの情報を人間が読めない点は，鉄道の乗車券の残額を見たいような場合には不便であるが，クレジットカードのように個人情報が書き込まれている場合には利点となりうる．通信距離とタグの向きや位置については，タグの位置を特定したい場合や，改札機のように近くに居ることによって人間の意思表示を把握する場合には，通信距離や向きに制限があるほうがシステムとしての利点となる．

一方，RFIDタグが劣る点として，リーダやタグの価格が比較的高い点があげられる．この問題は技術の進展に伴い解決へと向かう見込みがある．

3. 来たるべきデジタルネーミング社会

携帯電話やモバイルPC，PDA(Personal Digital Assistance)の普及により，無線通信を用いた電子機器の識別はすでに可能となりつつある．デジタルネーミングとは，電子機器に限らずあらゆる物品を電子的に識別可能とすることであるが，無線通信が可能な電子機器により，すでにデジタルネーミングが部分的に社会に浸透し始めているといえる．

本節では，デジタルネーミングを実現する基礎的な技術を紹介し，デジタルネーミングが社会に浸透した際に起こりうる問題点を明らかにする．

3.1 無線通信技術

無線LANやBluetoothにより，無線通信によりデータ通信を行なう方法が普及しはじめている．無線通信は，機器が自由に移動できるという特徴を持つが，次のような欠点を持つ．

1. 電波が届く範囲の機器で通信路を共有する必要がある．
2. 無線通信は，情報が空間を伝わるため，第3者による盗聴が比較的容易である．

1に関しては，空間を共有する機器の間では，通信路の数が基本的に1つしかないということである．そのため，周波数分割方式などの，通信の多重化が行なわれる．

また，2に関しては，データの秘匿性を保つための種々の技術が開発されてきた．たとえばBluetoothでは，データの暗号化や認証，周波数ホッピングといった方式が採用されている．

しかし，RFIDタグにおいては，タグにおける処理能力の制約から，Bluetooth で用いられるような高度なセキュリティ技術をそのまま用いることができないことが問題となる．

3.2 セキュリティ

デジタルネーミング社会においては，物品がRFIDにより受動的な無線通信を行なうことを想定するが，無線通信では，前節で述べたように通信が第3者により容易に盗聴される．つまり，物品との通信は第3者に盗聴されたとしても安全なシステムを構築しなければならない．ここで言うシステムの安全性とは，次の要素である．

1. 悪意を持った人間による攻撃に見舞われても，システムが安定して運用できること．
2. 悪意を持った人間に成りすまされ，RFIDタグやリーダに記された情報の改ざんをされないようなシステムであること．
3. 個人情報が不用意に他人に漏れないようなシステムであること．

1については，悪意を持った人間が，RFIDタグやリーダに記された情報を知っているか否かによって攻撃の方法が異なると考えられる．たとえば前者の場合，タグとの通信を盗聴して得た個人情報を用いてシステムの情報を改ざんするといったことが考えられ，2と関連する問題となる．また，後者の場合，無差別に大量の通信を行なうことによりシステムの機能を停止させることなどが考えられるが，これは通信を第3者に盗聴されることとは直接的には関係ないので，ここでの議論からは除外する．

2については，現在のRFIDタグの能力では暗号通信は望めないため，悪意を持った人間がRFIDタグやリーダのいずれか一方に成りすまして他方へ不正な情報を送ることは容易である．これを防ぐ方法としては，RFIDタグやリーダに重要な情報を送る場合には接触型の通信に限定し暗号化する方法や，重要な情報については通信距離を安全と認められる距離に限定する方法が考えられる．しかしこれらは，システムの利便性を損なったり，システムの運用形態に依存する方法なので，さらに良い手法が望まれる．

3については，個人情報が直接RFIDタグに記述される場合と，RFIDタグに記された物品の識別子から個人が特定される場合に分かれる．前者については，たとえばクレジットカード番号がRFIDタグに記述されることだが，RFIDタグの通信は盗聴が容易であるという性質から，このように個人情報をRFIDタグに記述することは望ましくない．後者については，a. 物品の識別子と，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において不用意に関連付けられてしまうこと，またはb. 物品の位置情報から個人が特定されてしまうことにより，物品を追跡することにより個人の行動が追跡されてしまう問題が起こりうる．b.については4.節で議論する．

3.3　エネルギー問題と環境負荷

情報技術が社会に広範囲に普及した今，情報技術も他の分野にもれず，地球エネルギー問題や環境問題と切り離すことができなくなってきている．

デジタルネーミング社会では，個々の物品が計算および無線通信を行なう．したがって，全世界において消費される電力およびエネルギーは膨大なものになる．システムの構築においては無駄なエネルギー消費を減らすことが重要である．この問題は，1人の人間が日常使用する物品は大量にあることを考えると，全世界の人間がデジタルネーミングに身を置くことになるときに深刻になることが予想される．特に，RFIDタグによるシステムでは，無線通信により，電力，クロック，データをRFIDタグに供給する事と，無線通信は拡散による損失が大きいことから，損失の少ない無線伝送方式や，無駄な情報の通信を省くことが，システム全体の，ひいては全世界の消費エネルギーを削減することに寄与すると考えられる．

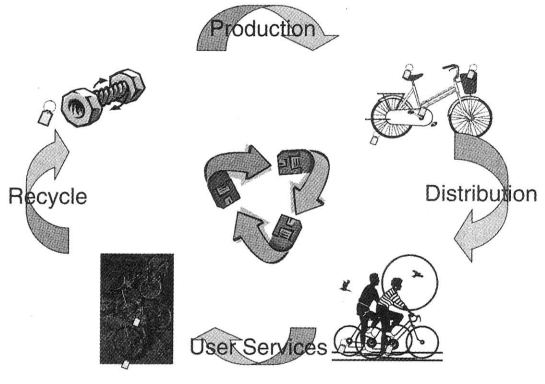

Fig.4　The lifecycle of an object

デジタルネーミング社会の実現によって，システム全体の消費エネルギーという問題が重要な課題となる一方，**Fig. 4**に示すように，物品の製造，供給，消費，リサイクルといった，理想的な循環型の社会が実現できる可能性がある．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，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，そのようなリサイクルに必要な情報はタグには記述されない．

また，現在の資源リサイクルは，物品をスクラップして，薬品を使うなどの手の込んだ方法で資源を抽出するといった，物品の材料そのものから得られる直接的な情報を扱う方法であり，タグに記述された情報を，いわばメタデータとして用いる方法に比べてコストがかかる．このような，タグを長期間利用して循環型の社会を実現することにより，地球環境へ負担をかけない人間社会を実現することができる．タグやサービスにかかるコストは，タグを共用することで削減できることが考えられる．

3.4　デジタルネーミング社会における課題

デジタルネーミング社会により，利用者に便利な社会が期待できる反面，本節で述べたように，新たな問題が生じる．まず，無線通信を基本とすることにより，セキュリティに対する対策がこれまで以上に重要となる．悪意を持った人間による攻撃や成りすましに対して，安全なシステムが望まれる．特に，物品の識別子から，個人の情報が間接的に第3者に漏れてしまうことがあると問題となる．また，無線通信は損失する消費エネルギーが大きい方法なので，効率の良い通信方法が重要となる．しかし，デジタルネーミング社会の実現により，物品をそのライフサイクルを通して管理することが可能になるため，無線通信によるエネルギー消費と，資源のリサイクルによる環境への負荷の軽減の効果を大域的に計算したときに，環境への負荷が軽減できるような社会を目指すべきである．

4.　デジタルネーミング社会における個人情報の保護

3.2節でも触れたように，安全なデジタルネーミング社会を実現するためには，1. 悪意を持った人間による攻撃に見舞われても，システムが安定して運用できること，2. 悪意を持った人間により，RFIDタグやリーダに記された情報の成りすましや改ざんをされないようなシステムであること，3. 個人情報が不用意に他人に漏れないようなシステムであること，が必要である．本節では，この中でも特に3について，たとえRFIDタグの情報が盗聴されたとしても個人情報が他人に漏れないようなシステムの枠組みを提案する．

このような個人情報の安全性を守るために，「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」ことを目標とする．これを実現するためには次の2点を防ぐことが必要である．

1. 物品の識別子と，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において不用意に関連付けられてしまうこと
2. 物品の位置情報から個人が特定されてしまうこと

1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．

2は，物品の置かれた位置に関する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．そのような静的な位置情報ではなくとも，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．この例のように位置情報から物品と個人の関連が分かってしまうと，1の問題につながる．

この節では，このような問題を解決するためのシステムの枠組みを示す．提案する枠組みは，物品に関連する個人が，その個人が生成する識別子をその物品に与えることにより，他人には物品とその識別子の関連が分からないようにする方法である．

ただし，物品のライフサイクルの中で，このような問題が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，**Fig. 4**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．そこで，提案する枠組みは，必要に応じて個人情報の保護のための運用方法を切り替えることのできるものとする．

4.1 想定するシステム

ここでは，**Fig. 5**のようなデジタルネーミングシステムを想定する．ここで，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．物品やリーダは，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

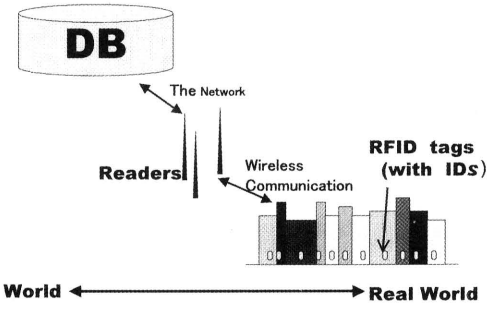

Fig.5　The system architecture

えられる．そのため，利用者がリーダを通してRFIDタグと交信する際には，リーダを扱うための認証をすることが必要であると考えられる．これにより，本節冒頭で目標として掲げた，「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しくみ」を実現することが可能であるように思える．しかし，以下のような場合が考えられるため，これは達成できない．

- 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，リーダを扱うために認証を行なわないようなシステムを作った場合，そのシステムのすべての利用者が，リーダの通信圏内にある物品を識別を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では難しいため，RFIDタグとリーダの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，このようなシステムの構成では，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．

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，ミューチップ[6]などで想定されており，今後普及することが予想される．

4.2 特定の利用者にのみ利用できるような物品の識別

本論文で提案する，特定の利用者にのみ利用できるような物品の識別のための枠組みを以下に示す．その概略を**Fig. 6**に示す．

1. 各RFIDタグは，読み込み専用メモリ (ROM)および，読み書き可能メモリ(RAM)を持つ．
2. ROM上には，物品を識別するための，唯一の識別

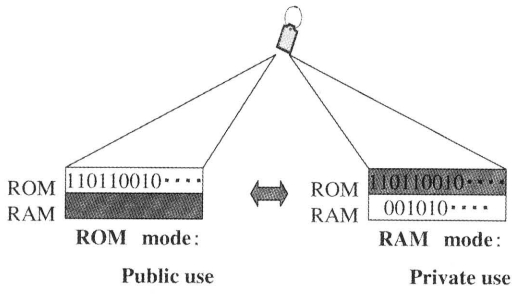

Fig.6　Restriction of identification to limited users

子が出荷時に書き込まれている．

3. ROMとRAMは排他的にしか利用できない．使用するメモリをRAMとROMの間で変更する際には，特定の権限を与えられた利用者が「RAM使用モード」と「ROM 使用モード」の間を切り替えないといけない．

3において，モードの切り替えを特定の権限を与えられた利用者に限定する方法は，モードの切り替えに個人認証を行なう方法や，モードの切り替え時に接触型通信にしか許さない，あるいは数cmの距離の接触型に限定する方法が考えられるが，どの方法がシステム運用において適切かは議論の余地がある．

このような枠組みにより，以下のようなシステムの運用が可能となる．

- ROM使用モードでは，だれでも利用できるような物品の識別が可能である．これは，ROM上には唯一の識別子が出荷時に書き込まれているためである．
- RAM使用モードでは，特定の利用者だけが利用できるような物品の識別が可能である．つまり，RAMには，特定の権限を与えられた利用者が，その利用者しか知らない識別子を書き込むことによって，それ以外の者は，物品の識別子を知ることができても，それがどの物品の識別子なのか対応付けることができないため，結果として物品の識別子を知らないのと同じことになる．この点については4.3節で詳しく述べる．

  また，このモードの時にはROMを読めないため，唯一の識別子を得ることも不可能である．
- 一つのRFIDタグで，だれでも利用できる物品の識別と，特定の利用者が利用できるような物品の識別を必要に応じて使い分けることができる．たとえば，物品の製造，出荷，販売の時にはROM使用モードを用いて物品を一貫して管理し，消費者の手に渡った際に消費者がRAM使用モードに切り替え，消費者による識別子をRAMに書き込む．これにより，以降はこの物品はその消費者にのみ識別が可能となる．さらに，物品が廃棄された際には，自治体がそのRFIDタグをROM使用モードに切り替え，物品の製造時の識別子を得，リサイクルに利用する．このようなことがモードの切り替えにより可能になる．
- この過程で，個別の識別子を書き込む利用者は，識別子を書き込む際に一旦RAMの内容を消すことによりROMが読めるので，ROMにかかれた物品の唯一の識別子の情報を読むこともできる．このため，利用者は物品の唯一の識別子から，ネットワーク上のデータベースを検索して物品に関する種々の情報を得ることができる．

4.3 議論

4.2節で提案した方法により，4.節で示した，「物品の識別子と，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RAMを書き換えることによって，販売店は物品の識別子を知ることができなくなってしまう．また，4.1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，RFIDタグのRAMに識別子を書き込んだ本人だけである．

逆に，RFIDタグのRAMに識別子を書き込んだ本人にとっては，識別子を書き込む際に，物品とRAM上の識別子と，ROM上の唯一の識別子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．

また，3.2節の2で示した問題として，「悪意を持った人間による，RFIDタグやリーダに記された情報の成りすましや改ざん」に対しても安全なシステムを実現することが可能である．RFIDタグに書かれた情報が改ざんされた場合には，改ざんされたことが物品に関連する利用者に通知できるようすることにより，この問題を解決することができる．

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．4.節でも示した，「物品の位置情報から個人が特定されてしまう」問題を検討する必要がある．つまり，一旦RAM上の識別子が第3者に知られた状況で，位置情報を介してRAM上の識別子と個人との関連が明らかになってしまうと，以降のその個人の監視が不可能ではなくなるからである．このときの状況としては，次のような場合が考えられる．

1. 個人の住宅にある物品のRAM上の識別子から，RAM上の識別子と個人の関連が分かってしまう．

2. 駅の改札口において，個人とともに移動する物品のRAM上の識別子が分かってしまう．

この問題を解決するためには，RAM上の識別子を定期的に書き換えることが考えられる．

このように利用者が物品の識別子を頻繁に書き換えるような状況では，複数の利用者間での識別子の重複管理が必要になる．単純な解決としては，識別子のうち特定の領域を利用者を特定する部分とし，残りをその利用者が自由に設定する物品の識別子とする方法が考えられるが，この方法だと第3者に物品に関連する利用者を特定することが可能になってしまい，本来の目的である，物品と個人の関連を秘匿することが達成できない．この問題に対しては2つの方針が考えられる．1つは，個人が使える識別子を管理する信用できる組織を設置すること，もう1つは，ある程度識別子が重複しても問題なく利用できるようなシステムを実現することである．後者については，物品が一瞬にして離れた位置に移動することはないという性質を利用することで，識別子が重複する物品を区別することも可能であるので現実的な方法となる可能性がある．

5. ま と め

本論文では，RFIDタグにより物品が計算機により識別可能になったデジタルネーミング社会について，その可能性と問題点を示した．デジタルネーミング社会は，セキュリティやエネルギー問題，環境問題とあわせて考慮する必要がある．特に，物品と個人が不用意に関連付けられることによる個人情報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，個人が物品に識別子を与えるという方法で，個人情報を保護する方法を提案した．この方法は，常に物品の唯一の識別子は保存されているため，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14-18年度科学研究費補助金学術創成研究・課題番号14GS0218によるものである．

本論文は、2001年度に開催された「超セキュリティシステム技術調査研究会」において交わされた議論に多大な示唆を得た。

本研究を行なうにあたり，有用な議論をいただいた、安浦・村上・松永研究室の諸氏、特に当研究室セキュリティグループの、浜崎陽一郎氏、萩原大輔氏，野原康伸氏に感謝します．

参 考 文 献

1) Konomi, S. “QueryLens: Beyond ID-based Information Access”. To appear in: Proc. 4th Int'l Conf.Ubiquitous Computing (Ubicomp2002) (2002).
2) Finkenzeller, K. ,「RFIDハンドブック」, 日刊工業新聞社.
3) MIT AUTO-ID Center Homepage, http://www.autoidcenter.org/.
4) 高橋史忠, 田野倉保雄 「発信源はゴマ粒チップ」, 日経エレクトロニクス, (2002年2月25日号) , pp. 109–147
5) JR東日本, 「Suica」 http://www.jreast.co.jp/suica/index.html.
6) 日立製作所ニュースリリース「世界最小の非接触ICチップ「ミューチップ」を開発」 http://www.hitachi.co.jp/New/cnews/2001/0628b/index.html(2001).