九州大学学術情報リポジトリ
Kyushu University Institutional Repository

RFIDを用いたデジタルネーミング社会とそのセキュリティ技術

井上, 創造
九州大学 システムLSI 研究センター

安浦, 寛人
九州大学 システムLSI 研究センター

https://hdl.handle.net/2324/6063

出版情報：電子情報通信学会技術研究報告,CAS2003-12,VLD2003-23,DSP2003-43, pp.73-78, 2003-06. 電子情報通信学会CAS研究会,VLD研究会,DSP研究会
バージョン：
権利関係：

[招待論文]RFID を用いたデジタルネーミング社会とそのセキュリティ技術

井上 創造† 安浦 寛人†

†九州大学 システム LSI 研究センター 〒816-8580 春日市春日公園 6-1

E-mail: †{sozo, yasuura}@slrc.kyushu-u.ac.jp

あらまし 本研究では，RFID を用いて現実世界の物品を識別可能にすること，および情報化社会における個人認証の基礎となる個人 ID を実現する基本技術を**「デジタルネーミング」**とよび，社会の基盤として真に社会の役に立つシステムとなるために必要な要素技術を検討する．本稿では，RFID (Radio Frequency Identification) を用いた物品の自動認識技術に焦点を当て，社会基盤システムの観点から検証する．近年，RFID を用いて現実世界の物を自動的に認識するという自動認識技術が脚光をあびている．これは，ユビキタスコンピューティング (Ubiquitous Computing) の根幹をなす基盤として期待されているが，現実を見てみると，現時点での RFID の応用は，特定の組織や場所内でのみ利用されるというクローズなシステムであり，RFID を不特定多数の人間が利用し上記の先進技術の基盤として利用するというオープンなシステムとしてはいまだ普及の機を得ていない．自動認識技術の普及のためには，社会基盤を構成するシステムという視点が重要である．社会基盤システムに必要な要件を議論し，その要件を満たす自動認識技術を確立することが技術やコストの議論とともに必要である．

キーワード RFID，社会基盤システム，デジタルネーミング， 自動認識技術，AUTO-ID

[Invited Paper] Digitally Named World with RFID Tags and Ensuring Security

Sozo INOUE† Hiroto YASUURA†

†System LSI Research Center, Kyushu University 6-1 Kasuga Koen, Kasuga-shi, 816-8580 Japan

E-mail: †{sozo, yasuura }@slrc.kyushu-u.ac.jp

Abstract Our work focuses on the *Digital Naming*, which is the technique for automatically identifying objects in the real world and provides personal IDs for basic scheme for personal authentication in the information society. This paper focuses mainly on the automatic identification of objects using RFIDs (Radio Frequency Identification), and discusses the requirements for becoming social system infrastructure. Automatic identification using RFIDs is gathering attractions as the fundamental technology for realizing ubiquitous computing. However, current applications are mainly in the *closed systems*, which are applied at particular places, or in organizations. For *open systems*, the aspects of social system infrastructure must be well considered, and technology to match the requirements for social system infrastructure must be developed, as well as the efficiency and the costs of the Digital Naming.

Keyword RFID, Social System Infrastructure, Digital Naming, AUTO-ID

1. はじめに

近年，RFID (Radio Frequency Identification) [9] をはじめとするデバイスを用いて現実世界の物を自動的に認識するという自動認識技術が脚光をあびている．これは，どこにでも計算機が存在するような環境を意味するユビキタスコンピューティング (Ubiquitous Computing) [7]や，ロボット技術，現実の世界に仮想の物体を表示する拡張現実感技術 (Augmented Reality) といった先進技術の根幹をなす基盤として，輝かしい未来が約束されているかのように見える．

しかし現実を見てみると,現時点での RFID の応用は，特定の組織や場所内でのみ利用されるというクローズなシステムであり，RFID を不特定多数の人間が利用し上記の先進技術の基盤として利用するというオープンなシス

テムとしてはいまだ普及の機を得ていない．オープンなシステムへの課題としては，RFID タグの低コスト化と規格の標準化が上げられているが，筆者は低コスト化と規格の標準化が達成されれば自動認識技術の普及に十分な条件がそろうとは考えない．

筆者は，自動認識技術の普及のためには，社会基盤を構成するシステムという視点が重要であると確信する．つい最近，アパレル業の Benetton が RFID タグを商品に埋め込もうとして消費者団体の反対を受け，とりやめたことがニュースとなった[14][15][16]が，これは自動認識技術の普及が，技術あるいはコストの議論だけでは語れないことを如実にあらわしているといえる．現代は IT 技術が社会に直接影響を与える時代であり，自動認識技術に関しても行き当たりばったりの施策では普及は難しいばかりか社会にとって危険でさえある．社会基盤システムに必要な要件を議論し，その要件を満たす自動認識技術を確立することが技術やコストの議論とともに必要である．

われわれは，RFID を用いて現実世界の物品を識別可能にすること，および情報化社会における個人認証の基礎となる個人 ID[6]を実現する基本技術を**「デジタルネーミング」**とよび，社会の基盤として真に社会の役に立つシステムとなるために必要な要素技術を検討している．本稿では，RFID を用いた物品の自動認識技術に焦点を当て，社会基盤システムの観点から検証する．

2. 社会基盤システムの要件

社会基盤システムに求められる要件として，以下の点を挙げる．

● 個人の権利と社会の秩序：社会基盤システムは，社会の秩序を乱さないものであると同時に，個人の権利を守るものである必要がある．

● 単純で理解しやすい原理：利用者の責任を明確にするという観点から，システムの基本的な原理は単純で理解しやすいものでなければならない．基本的な原理を利用者から分かりにくくするようなブラックボックス化は，危険性と責任を利用者が自然に把握することを困難にしてしまい，システムの提供者が危険性に対して全ての責任を負う必要が生じてしまう．

● 信頼性と安定性：人命や個人の財産，プライバシに直結するような社会基盤システムは，数億人希望の利用者に対し，幅広い利用形態を想定した信頼性の保証が必要である．

● 柔軟性と拡張可能性：急速，急激に発展するであろう今後の技術進歩に対して柔軟に対応できるような設計が必要である．技術進歩に対しても，社会基盤システムの基本構造は変えずにすむような基本設計が必要である．

● 危機対応能力：災害や，悪意のある者の故意の攻撃に対して安全で，かつ障害からの迅速な復旧が可能である必要がある．特に，攻撃時や災害時の被害の波及，および復旧にかかる費用を最小限に抑えることが可能なシステムが求められる．

● 経済性：システムの運用が経済的に成り立たなければならない．得られる利潤に対して，ハードウェア，ソフトウェアの構築費用，運用や保守の費用を考慮する必要があるが，現在の携帯電話社会や今後のユビキタスコンピューティング環境では利用されるデバイスの数が非常に多い事を考えると，全体としての消費エネルギーの問題も重要である．

デジタルネーミングを社会基盤システムと考えた時，これらの要件を満たすようなシステムの設計が重要である．

3. デジタルネーミング：実物と情報の融合

デジタルネーミングの本質は，情報と，現実にある物を融合的に管理することにある．

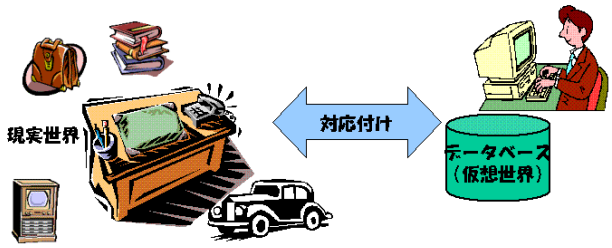

図 1 デジタルネーミング

デジタルネーミングは，図 1のように，物品の情報が記憶された小型IC である**RFIDタグ**と，その読み取り／書き込み装置である**リーダ**で構成される[9]．デジタルネーミングは，RFIDタグに格納されている情報を，リーダからの電磁誘導によって非接触で読み取り／書き込みすることを想定する．RFIDタグは通常，リーダからの電磁誘導により供給される電力を用いて，電源なしで動作する．リーダはRFIDタグに電力を供給し，RFIDタグに格納されている情報との通信を行う．

RFIDタグとリーダの基本的な構成を図 2に示す．RFIDタグは，無線通信を行うRF 回路，計算を行う論理回路，読み出し専用メモリ(ROM)あるいは書き込み可能メモリ(RAM)，およびアンテナから構成される．リーダはRF 回路および制御装置から構成される．RF 回路は送信機と受信機からなる．

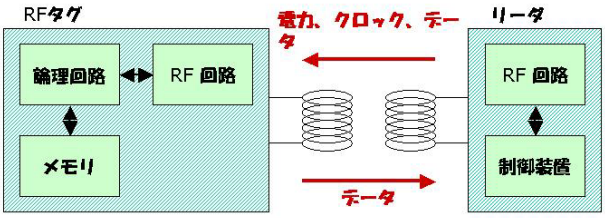

図 2 RFID タグとリーダの基本構成

3.1. デジタルネーミングの応用

RFIDを用いたシステムは，主にRFIDタグのメモリに識別子，つまりその物品を識別するため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ている．

航空会社では，航空手荷物にRFIDタグを取り付けることによって管理システムと連携し，手荷物管理の効率化を図っている．また，手荷物の仕分けのコスト削減，手荷物の紛失防止やセキュリティの向上が効果として挙げられる．現在，航空手荷物にはバーコードのタグが取り付けられ,手荷物の管理や自動仕分けに利用されている．しかし，バーコードの認識率は世界的には70 %程度といわれて，結果として手荷物の誤った仕分けや紛失が発生する．その理由として，タグの大きさや形状が異なる，タグの取り付け位置が一定ではない，タグが折れたり汚れたりすると認識することができないといった点が挙げられる．一方，RFIDタグを取り付けることで，無線通信で情報を読み取ることが可能になり，手荷物の誤った仕分けや紛失を防ぐことが可能になる．実際に，成田空港などでRFIDを用いた航空手荷物管理システムの実証実験が行われ，認識率は99 %以上と報告されている[12]．また，手荷物をチェックインした日時や場所，手荷物の重量をRFIDタグに書き込むことで，手荷物の中身やそのものをどこかで盗まれてないかどうかを確認することができ，セキュリティを向上させることも可能となる．

流通の分野では，商品にRFIDタグを取り付けることによって生産，物流，在庫，販売管理システムと連携し，流通の効率化を図っている．物品の生産，物流，在庫の工程では，RFIDタグが取り付けられた複数の部品や製品を，梱包した状態でリーダのゲートを通過させ，内容物の情報や在庫の情報を同時に認識させる.これによって，同じラインを流れる多品種の物品を一括管理することが可能になる．販売時には，RFIDタグが取り付けられた複数の商品をかごやカートに乗せたまま，リーダのゲートを通過させ，商品の情報を同時に認識させることで，多くの商品の精算を一括で行うことができる[13]．例えば，レジで従業員が商品をひとつひとつ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くなる．

このように，デジタルネーミングでは，無線通信を利用して，現実の世界の多様な形状，また一見では区別できないような物品に対する識別を提供することにより，効率的なサービスや，盗難防止のようなセキュリティを実現することができる．

3.2. 情報と物の融合

デジタルネーミングでは，これまでの情報技術と異なり，現実の実物の性質を考慮する必要がある． 表 1 に，実物と情報の基本的な性質の比較を示す．

表 1 実物と情報の一般的な性質

	実物	情報
物理法則に	従う	従わない
複製	困難	データの複製が可能
重さや形	有り	無し
位置	有り	無し
経年変化（鮮度や耐久性）	有り	無し
移動	時間がかかる	かからない（通信）
加工	労力がかかる	瞬時
観察	容易	表示デバイスが必要
所有権の概念	有	無

まず，実物は情報と異なり，物理法則に従う存在である．具体的には以下のような性質が伴う．

- 重さや形を持つ．
- 存在する位置が決められる．
- 鮮度や耐久性といった，時間とともにいやおうなしに変化する性質も持つ．
- 加工や移動には，現実世界における常識的な時間や労力を要する

一方，情報は，物理法則に従わず，重さや形，位置の概念は持たない．したがって加工や移動は一瞬で可能であり，この性質なしには現在の通信やネットワークは成り立たない．

次に，物体は情報と異なり，複製が容易ではない．情報技術は，キャッシュにあげられるように，データの複製が容易であることを利用してきた．逆に物体は，複製が困難であることを利用されることがある．たとえば，身分証明書や貨幣は，複製あるいは偽造が困難であるという前提の上に成り立っている．

次に，実物は通常，観察が容易であるのに対し，情報を観察するためには表示用のデバイスが必要である．こ

の性質と，情報が物理法則に従わないという上記の性質は，情報システムの利用者に対して，常識的な感覚を欠落させ，システムに対する自然な理解を妨げる原因となる．

また，実物には通常，所有権が存在することが多い．さらに，所有権は生産者から流通業者，小売業者，消費者のように委譲されていくものである．情報に所有権が生じるのは，デジタルコンテンツなど，現時点では一部である．所有権の概念は，実物と所有者の関係が定義されるという意味でプライバシの問題と関わりを持つ．この問題については4.1節で扱う．

このように，デジタルネーミングにおいては情報の基本的な性質に現実の物の性質が基本的なレベルで伴ってくるという点で，今後の情報技術に大きな変革を起こす可能性がある．

上記の性質から，デジタルネーミングにおいては，RFIDの，情報と物の両方の性質が与える影響を考慮したシステムの設計が必要である．

さらに，現実の物を直接扱うようなシステムにおいては，現実に直接影響を与えるために，慎重にシステムの設計および導入を行う必要がある．以下では，社会基盤システムとしての要件を達成するための技術をこれらの性質をふまえて論じる．

4. デジタルネーミングを実現する要素技術と課題

本節では，デジタルネーミングにおいて，2節で述べた社会基盤としての要件を満たすための課題と要素技術を述べる．

4.1. プライバシ

プライバシの問題に対しては，個人を特定できないという匿名性や，個人を特定できなくてもその行動（あるいはセッション）を把握できてしまうというリンク可能性といった分類がなされている[1][2]．

デジタルネーミングにおいては，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，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．

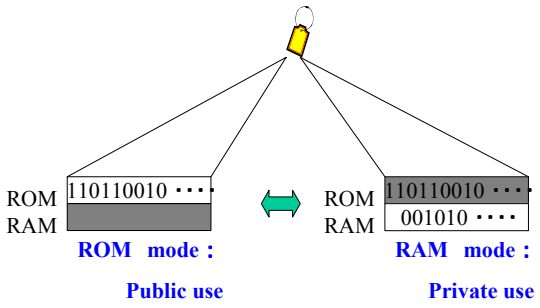

図 3. 本人にのみ理解できる ID の付与

筆者らは，3について，「RFID タグとやりとりされる情報から，物品を所有する個人を特定できない」ことを目標とするプライバシ保護技術を提案している[5][4]．RFID に対して唯一で永久的な ID(Public ID)ではなく，所有者が自分で決めた ID(Private ID)を必要に応じて変更しながら付与する方法である（図 3. 本人にのみ理解できる ID の付与）．所有者以外にはこの ID を読めるが，その ID が何を意味しているかわからない(匿名性)．ちょうど，入学試験での合格発表の現場で，居合わせた人は同じ情報を見ているのに，合格したかどうかは番号との対応を知る本人のみであることと同じ原理である．また，所有者が定期的に安全な場所Private IDを書き換えることでリンク可能性を防ぐことができ，物のライフサイクルの過程で所有者が変遷することにも対応できる．MIT の AUTO-ID センターは，ハッシュ関数と擬似乱数生成器を RFID に組み込むことで,匿名性の確保とトレーサビリティの回避を実現するほうを提案している[3]．この方法は，ID が毎回の更新で自動的に変わり，筆者らの提案のように安全な場所で書き換える必要がない点が優れているが,ハッシュ関数と擬似乱数生成器を RFID に付加する必要があり，数千～数万ゲートの回路の増大が必要となってしまう．筆者らが提案する方法は，所有者を認証するための機構と，Public ID と Private ID を記憶するメモリが必要であるが，ハッシュ関数と擬似乱数生成期を用いるより小さな回路規模で実現することが可能であると考えられる．

4.2. 理解しやすい仕組み

電子投票や電子決済といった，現実の重要な取引が電子化されることは，効率がよくなる一方，情報の，観察が容易でないという性質によって，わかりにくいものとなる恐れがある．特に無線通信においては物理的な接触がなくても通信が可能であるため，知らず知らずのうちに信用できないデバイスと通信を行ってしまう可能性がある．また，情報は高速に処理されるため，処理の間に人間の思考が介入する余地がなく危険である．

例として，IC カードは近年，身分証明や電子マネー，住民基本台帳カードといったようにマルチアプリケーシ

ョン化が進んでいるが，これは例えば財布の中身をひとつのカードに集約する役割を果たしていると言うことができる．しかし，通常の財布では支払いの際に財布を店員に預けて支払うことはないはずであり，マルチアプリケーションのカードで電子マネー機能を用いて支払うときに，住民基本台帳番号も見せなければならないことがあれば利用者にとってはプライバシが不安である．IC カード内部では，アプリケーション間でデータの孤立性を保つよう設計されているかもしれないが，実物として見えない仕組みであるため利用者にとっては理解しにくいものであり，これまで実物に帰着させていたものを情報のみの世界に閉じ込めてしまうことの弊害といえる．

デジタルネーミングにおいても，実物が観察しやすいという特徴を生かした，理解しやすい運用の枠組みを構築することが課題である．

文献[11]では，指輪の形をした認証用デバイスをかざして認証をするといった，実物に即した認証の方法を提案しており、今後の情報技術と利用者とのインタフェースの新しい方向性がうかがえる。

4.3. 信頼性

社会基盤システムとしてのひとつの重要な点は，システムの信頼性である．

RFIDは無線通信に基づくため，電波の干渉によってリーダがRFID の認識に失敗したり，利用者がRFID を故意に認識させないというように，通信の品質や認識の信頼性を保つことが難しいことが多々ある[8]．このことは，デジタルネーミング自体のシステムの信頼性に直結するため，重要な課題である．

このような問題に対して，単純にリーダにおける認識の確実性を上げることを考えるのではなく，リーダの性能は変わらなくてもシステム全体で何らかの工夫をすることで，システムの信頼性を向上させるという考え方が必要である．筆者らは，デジタルネーミングにおける信頼性の問題について，複数のリーダが計算機ネットワークにつながっていることを利用して，システム全体でRFID の認識の信頼性を向上させる方法を提案している[10]．

提案手法では，以下の基本概念によって動作する．

１．リーダをノードとし，それらの間の通過可能な経路を枝とする有向グラフを，**経路ルール**としてサーバに登録しておく（図 4）．

２．複数のRFID が同時に行動することがわかっている場合には，サーバは認識された複数のRFID をまとめて**グループ**として登録する．

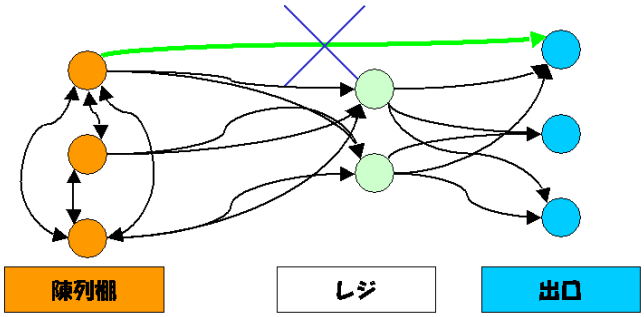

図 4 経路ルールの有効グラフ

この仕組みにより，いくつかのRFIDタグが認識に失敗した際にも，経路ルールとグループの情報を元に失敗の検出が可能となる．この方法は完全に失敗を検出できる方法ではないが，このようにRFIDとリーダ単体での信頼性ではなく，システム全体としての信頼性を考えるアプローチは新しいものであり，今後このようなシステマティックな手法がさらに開発されることが望まれる．

4.4. 拡張可能性

デジタルネーミングでは，無数の IC カードや RFID を社会に普及させることを想定するが，社会基盤システムとしての柔軟性と拡張可能性の観点から重要なことは，いったん普及した IC カードや RFID を回収するのは高いコストがかかるということである．

サーバ側は数が少なく，管理者の手元で交換できるため，交換のコストが低いが，RFID は短期間に交換することは難しい．

技術革新に対して柔軟に対応できるためには，どのように供給／回収するか，あるいは供給した後にどのように機能変更するかという，RFID のライフサイクルをシステムの設計の際に考慮することが重要であると考える．

関連する例として，クレジットカードは通常有効期限が来たら再発行されるのに対し，銀行のキャッシュカードは有効期限がないため，いつまでも更新されずに使われるカードが残る．クレジットカードのように一定期間で更新されるような仕組みを用いるのが１つの方法である．しかし RFID のように大量の物に用いる場合は，大量の RFID タグを交換するコストと,物のライフサイクルを考慮しなければならず，今後検討すべき課題である．

4.5. 危機管理

コストに対する要求が厳しい RFID においては，すべての攻撃に対する防御を高いレベルで実現することは難しいことが考えられる．したがって，2節で述べたように，攻撃を受けたときに被害を最小限に抑え，迅速に

復旧するという視点が重要になってくる．問題となるひとつの例をあげると,プライバシに関する話題であるが，指紋認証や網膜認証によるバイオメトリクス認証は，利用者に対するバイオメトリクス情報を変更することができないため，一旦利用者とバイオメトリクス情報の関連が公になってしまえば，その利用者は一生涯公になったバイオメトリクス情報から逃れることができない．RFID においては,書き込み可能メモリに ID を保持することにより ID の書き換えが可能であるため,この問題に対照することが可能である．社会基盤システムにとっては，このように迅速に攻撃に対応できる仕組みが必要である．これは ID と利用者の関連が漏洩するという問題に対する例であるが，その他にも種々の攻撃や危機に対する検討が今後必要である．

4.6. 経済性

システムが経済的に成り立たなければならないことは，システムにかかわる事業者それぞれが経済的に利益を得る必要があるのは当然であるが，ここでは，社会全体としての経済性を考える上で重要となる，システム全体としてのエネルギー消費を問題にする．RFID のリーダの消費電力を約 0.3W と見積もり,物品に添付された RFID を読み取るために一人あたり 1 個のリーダを使い続けるとすると仮定すると，60 億人が 1 日で消費するエネルギーは，約 430 万 kWh であり，これは一日 100 万 kWh の発電量を持つ原子力発電所 4 基分に相当することになる．今後ユビキタスコンピューティングを実現するにあたり，このような社会全体としての経済性の議論も重要となる．

5. おわりに

本稿では，RFID を用いて現実世界の物品を識別可能にするための社会基盤システム「**デジタルネーミング**」について，真に社会の役に立つシステムとなるために必要な要素技術を検討した．

九州大学では，平成１７年秋から，福岡市西部の新しいキャンパスに統合移転する計画が進められている．この新しいキャンパスを舞台に，デジタルネーミングの応用実験を計画中である．たとえば，引越しにかかわる備品の自動管理といった応用例が考えられる．

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費（課題番号14GS0218）によるものである．議論いただいた研究室諸氏に感謝する．

参考文献

[1] D. Chaum, “Untraceable electronic mail, return address, and digital pseudonyms”, *Communications for the ACM*, 1981.

[2] S. Seys, et al., “Anonymity and Privacy in Electronic Services Deliverable 2 - Requirement study of different applications”, *APES Documents,* https://www.cosic.esat.kuleuven.ac.be/apes/

[3] 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*, 2002.

[4] 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.

[5] 井上創造，安浦寛人，“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”，*九州大学大学院システム情報科学紀要,* Vol.7, No.2, pp. 131-137, 2002 年 9 月.

[6] 浜崎 陽一郎 and 安浦 寛人, ``PID を用いた安全な社会システムの構想", *九州大学大学院システム情報科学紀要*, Vol.7, No.2, pp.139-148, Sep. 2002.

[7] M. Weiser, “Some computer science issues in ubiquitous computing”, *Communications of the ACM*, Vol.36, No.7, pp. 74-85, Jul. 1993.

[8] H. Vogt, “Efficient Object Identification with Passive RFID Tags”, *Proceedings of International Conference on Pervasive Computing*, Aug. 2002.

[9] Finkenzeller K., “RFID ハンドブック　非接触型 IC カードの原理と応用”, *日刊工業新聞社*, 2001 年2月.

[10] 萩原 大輔，井上 創造，and 安浦 寛人，``RFID を用いたディジタルネーミング社会における信頼性の向上''，***第 14 回データ工学ワークショップ (DEWS2003)***, 2003 年 3 月.

[11] L. Bussard, Y. Roudier, “Embedding Distance-Bounding Protocols within Intuitive Interactions”, *1st Int'l Conf. Security in Pervasive Computing (SPC2003),* Germany, Mar. 2003.

[12] 国土交通省，“「RFID 技術応用による航空手荷物管理システムに関する調査研究報告書」について”, http://www.narita-airport.or.jp/naa/airport/greenport/, 2001_11_12/06_news.pdf, 2002年4月.

[13] 石川俊治，“IC タグ(RFID)とAuto-ID Center 活動”, *第3回21 世紀のマイクロエレクトロニクスセミナー「ユビキタスネットワーク社会実現のためのキー・テクノロジー」*,2002 年11 月.

[14] http://discover.npr.org/features/feature.jhtml?wfId=1236873

[15] http://www.nocards.org/AutoID/overview.shtml

[16] http://www.epic.org/