

平成 21 年 5 月 28 日現在

研究種目：若手研究（A）

研究期間：2006-2008

課題番号：18680009

研究課題名（和文） 信頼性を実現する RFID 情報システムの研究

研究課題名（英文） Research of RFID Information Systems with Reliability

研究代表者 井上 創造（INOUE SOZO）  
九州大学・附属図書館研究開発室・准教授  
研究者番号：90346825

## 研究成果の概要：

本研究では、(1)現実の応用に即した RFID の信頼性に対する要求の洗い出しとモデル化により、リンク不能性という概念を特に定式化した。また(2)システム全体で最適となるような高信頼識別技術の構築においてリンク不能性の概念と現実世界の状況を包括した信頼性モデルを築いた。さらに(3)RFID の真正性を保証するためにセキュアで高速な RFID 識別手法や権限管理システムを提案し、(4)図書館、イベント支援、救急、医療分野において実際に実証実験を行って有効性を評価した。

## 交付額

(金額単位：円)

	直接経費	間接経費	合計
2006 年度	5,500,000	1,650,000	7,150,000
2007 年度	7,900,000	2,370,000	10,270,000
2008 年度	6,100,000	1,830,000	7,930,000
年度			
年度			
総計	19,500,000	5,850,000	25,350,000

## 研究分野：情報学

科研費の分科・細目：計算機システム・ネットワーク（安全性・信頼性）

キーワード：RFID, スマートセンサ情報システム, 高信頼性ネットワーク, セキュアネットワーク

## 1. 研究開始当初の背景

RFID(Radio Frequency Identification)を用いた情報システム(RFID情報システム)は、無線通信で現実世界の物や人の識別をする技術であり、情報技術の限界を打ち破

る技術として注目される。RFID情報システムは、以下の用途を持つ。

- (1) 物品や人の自動識別を行い、現実世界の状況を効率的に把握する。
- (2) RFIDタグ(無線識別可能なICチップ)や、RFIDタグが組み込まれた物品の真正性

を保証する。

(1)においては識別の失敗が伴う。従来のエラー回復技術は長時間の通信の品質を重視するが、RFIDでは短時間の識別に特有の**高信頼識別技術**が求められる。(2)の目的を真に満たすためには、RFIDタグが**社会的に信頼された方法で発行され、その真正性を利用者が信頼できる仕組みが必要**だが、現状ではLSIの製造者は限られていることに立脚しているのみである。このようにRFIDは、その**信頼性**についての検討が不足している。

## 2. 研究の目的

本研究では、RFID情報システムの信頼性を実現するために、以下の研究を行う。

- (1) 現実の応用に即した、**RFIDの信頼性に対する要求の洗い出しとモデル化**：紙幣が印刷技術や厳正な発行管理により多様な精度とコストの信頼性を確保しているように、RFIDの信頼性においても多様性が求められるため、この要求を明確化しシステムが扱えるようなモデル化を行う。
- (2) **システム全体で最適となるような高信頼識別技術の構築**：(1)のモデルを用いて、システムが現実世界の知識をコンパクトに記述し、それを利用して識別の信頼性を高める技術を構築する。たとえば、コンテナ内の物品数を記述することで、識別に失敗した場合に検知できるし、商品陳列棚からレジを通る物品のフローを記述することで、レジでの一括清算にもれた商品を検知できる。
- (3) **RFIDの真正性を保証するためのシステム全体の枠組みの設計**：(1)の要求に則し、精度とコストに関して多様性を持つ真正性の保証方法を開発し、系統的な利用法を設計する。

## 3. 研究の方法

- (1) 現実の応用に即した、**RFIDの信頼性に対する要求の洗い出しとモデル化**：初年度は、RFIDの製造者の視点と利用者の視点の両面から広い視野で調査を進める。RFIDの製造者の視点では、システムLSI設計・製造事業者ヒアリングする。さらに、高いレベルの真正性保証の一例として、**紙幣や証券の製造**に詳しい事業者や機関から、信頼のおける発行管理方法について調査をする。利用者の視点では、これまでに何度か

調査してきた、図書館や廃棄物運搬、大規模消防活動の専門家に具体例を絞りヒアリングする。

- (2) **システム全体で最適となるような高信頼識別技術の構築**：これ研究でこの方法の有効性の初歩的な確認はできている。この方法の有効性を現実的に確認するため、**現実の状況の記述をより詳細化し、RFID情報システムの高信頼化**をできる方法を構築する。この方式設計には、RFIDタグにはハッシュ関数と同程度の計算機能を想定し、提案方式は、誤り訂正理論を応用した評価を行う。さらに計算機シミュレーションと実環境での実験による評価を行う。
- (3) **RFIDの真正性を保証するためのシステム全体の枠組みの設計**：**RFIDタグの製造・発行時から回収・廃棄にいたるライフサイクルにわたって真正性を保証する枠組み**を、1のヒアリング結果を元に設計し、2の成果と合わせてRFIDが貨幣のように社会基盤として通用するための仕組みを構築する。これには暗号を用いた認証プロトコルと否認防止プロトコルをRFIDタグ単体およびシステム全体で用いるが、**種々の精度とコストを持つ真正性の保証方法を多様に持つRFID情報システムの基盤が必要**となると考えられる。そのため、その系統的な利用法を設計しソフトウェアとして提供することを予定する。
- (4) **システムの実設計と実証実験による有効性の評価**：1～3で構築した信頼性保証技術を実際の場で検証し、本研究で得られた成果の有効性と実用性を評価する。具体的な実験対象としては、大学の備品の管理や、証明書発行、廃棄物運搬管理といったものを計画する。これらの実験が成功すれば、**九州大学の新キャンパスでの大規模な実験へと発展**

させることも検討する。

#### 4. 研究成果

得られた研究成果を、行った研究の方法にあわせて述べる。

##### (1) 現実の応用に即した RFIDの信頼性に対する要求の洗い出しとモデル化

紙幣が印刷技術や厳正な発行管理により多様な精度とコストの信頼性を確保しているように、RFIDの信頼性においても多様性が求められるため、この要求を明確化しシステムが扱えるようなモデル化を行った。特に個人情報保護における重要な視点であるリンク不能性について定式化し、以下の(2)との関連を調べた。文献[4][12]ではRFIDの一つである非接触ICカードを包括的な情報システムとしてとらえ、その課題を挙げた。文献[7][20][32]ではRFIDなどで実現される自動認識におけるプライバシーと個人情報保護について技術的な観点からまとめた。文献[19][33]では図書館におけるRFIDの事例を全国的に調査し、信頼性に関する問題を洗い出した。

さらに、センサーデバイスのようなアクティブなRFIDを含めたシステムの通信プロトコルを設計し、それらを、RFIDリーダを組み込んだ書架[10]や、医療応用のためのシステムに適用[13]し、その履歴を元に安全性や信頼性を解析した。

また、RFIDと電子ペーパーと親和性が高いことを洗い出し、それによる応用と求められる信頼性を文献[3]にまとめた。

##### (2) システム全体で最適となるような高信頼識別技術の構築

現実の状況の記述を詳細化し、RFID情報システムの高信頼性をできる方法を構築した。この方式設計には、RFIDタグにはハッシュ関数と同程度の計算機能を想定し、提案方式は、誤り訂正理論を応用した評価を行った。評価は、計算機シミュレーションおよび理論値による評価を行い、この2つを整合した評価をおこなった。

文献[23]では、RFIDリーダの配置およびその間の経路を無向グラフで表現し、それにより現実の状況を記述した。これを用いてRFIDの読み取りミスを検出する手法を提案し実験により評価した。さらに[26]では、これらをマルコフモデルでモデル化し、グラフの形状と信頼性およびリンク不能性がどう変化するかをシミュレーションにより明らかにした。

一方、文献[16][29]ではさらに、ブルームフィルタという検索のためのフィルタを

用いてセキュアなRFID識別を高速に行う方法を提案し、シミュレーションおよび理論的な評価を行った。

##### (3) RFIDの真正性を保証するためのシステム全体の枠組みの設計

RFIDタグの製造・発行時から回収・廃棄にいたるライフサイクルにわたって、安全性と信頼性を守ったまま識別を行う仕組みを考案した。その際にサーバ側の識別の手間が問題になるため、これを高速化する手法を提案した。文献[6]では、k段ID照合という木構造のID構造を提案し、これにより識別時間を $O(N)$ から $O(\log N)$ ( $N$ はRFIDタグの数)に押さえた。この論文はIPSJ Digital Courier船井若手奨励賞を受賞した。

また、RFIDを用いた認証において、その認証権限を譲渡することにより運用の柔軟性と安定性を高めるモデルを発表し、携帯電話上のFelicaチップに実装した[21]。

##### (4) システムの実設計と実証実験による有効性の評価

上記で構築した信頼性向上技術を現実的な場で検証するため、イベント支援や図書館、ユビキタス医療といった実際の現場で成果を応用し、提案手法を評価した。

文献[8][9]では、国際会議の場でRFID情報システムを提供し、参加者同士のネームタグにつけたRFIDタグを用いてお互いの学会におけるネットワークを可視化した。これにより学会における交流が活性化することが分かったが、一方でプライバシーに関する問題も顕在化され、(1)のモデルがデモンストレーションできた。

文献[5][22][24][25][31]では、大規模な救急活動において負傷者を分別するトリアージにおけるRFIDの活用を試みた。この中でRFIDタグの中に情報を書き込み、それが紛失せず、複製の中で最新の状態になるようなプロトコルを提案し、100人規模の負傷者を想定してRFIDタグをトリアージタグに用いることで情報の収集時間と搬送時間がどちらも約半分になることを検証できた。

図書館の分野では、電子化が進んだ図書館においてRFIDの安全性と、利用者の認証や認可といった柔軟な権限管理をWeb2.0の枠組みの上で実現するために、SNS(Social Networking Service)を基盤とした権限管理の枠組みを提案し、実装した[1][11][27][30]。また、RFIDにおいて用いられる安全性の高い高速識別技術を、図書館の種々のシステム間の連結において用い、その効果を定量的・定性的に評価できた[17][18]。この中でRFIDタグを添付した書籍を効率よく識別する実験のために、

RFID書架を導入しそれをWebと連携するシステムにおいて信頼性向上技術を適用した[27].

ユビキタス予防医療の分野では、アクティブRFIDやセンサを用いた利用者からのデータの秘匿性について、トラフィック解析の技術による脆弱性の可能性を、国際的な共同研究により指摘した[2].

また、医療応用のためのシステムにおいて大規模な実証実験を行い、生活習慣病予防医療のような応用において必要となる要求を洗い出した[13].

さらに、これらのRFID情報システムが社会に与える影響について、情報システム構築の観点ばかりではなく、経済的視点や医療の視点といった社会応用的な視点から考察を加え、真に世の中の役に立つシステムについての知見を得、論文にまとめることができた[14].

本研究成果の一部は、九州大学で平成21年度から九州大学全学に採用されたICカードにも採用されている。

#### 5. 主な発表論文等

(研究代表者、研究分担者及び連携研究者には下線)

[雑誌論文](計 12件)

#### 査読あり

- [1] Masanori Nakakuni, Eisuke Ito, Yoshiaki Kasahara, Sozo Inoue, Hiroshi Dozono, "Construction and Use Examples of Private Electronic Notary Service in Educational Institutions," WSEAS Transaction on Advances in Engineering Education, Issue 1, Vol.5, ISSN: 1790-1979, pp.676-686, Nov., 2008.
- [2] Benessa Defend, Mastrooreh Salajegheh, Kevin Fu, and Sozo Inoue "Protecting Global Medical Telemetry Infrastructure," I3P White Paper, [http://www.thei3p.org/repository/whitepaper-protecting\\_global\\_medical.pdf](http://www.thei3p.org/repository/whitepaper-protecting_global_medical.pdf) 15 pages, Jan. 2008.
- [3] 服部励治, 井上 創造 "電子ペーパーが創

るユビキタス社会 電子ペーパークライアントを目指して," *情報処理学会誌*, vol. 28, No. 8, pp. 873-883, Aug. 2007.

- [4] 井上 創造、安浦寛人, "非接触ICカード技術の概観と展望," *情報処理学会誌*, Vol.48, No.6, pp.551-555, Jun. 2007.
- [5] 園田 章人, 井上 創造、岡 賢一郎, 藤崎 伸一郎, "RFIDを利用した救急トリアージシステムの実証実験," *情報処理学会論文誌*, Vol. 48, No. 2, pp.802-810, Feb. 2007..
- [6] Yasunobu Nohara, Toru Nakamura, Kensuke Baba, Sozo Inoue and Hiroto Yasuura, "Unlinkable Identification for Large-scale RFID Systems," *IPSJ Journal*, Vol. 47, No. 8, pp. 2362-2370, Aug. 2006.
- [7] 井上 創造、野原 康伸, and 安浦 寛人, "自動認識におけるプライバシーと個人情報保護技術", *電子情報通信学会誌*, Vol.89, No.5, pp.390-394, 2006.
- [8] Shin'ichi Konomi, Sozo Inoue、Takashi Kobayashi, Masashi Tsuchida, Masaru Kitsuregawa, "Supporting Colocated Interactions at an Academic Conference Using RFID and Social Network Displays," *IEE Pervasive Computing*, 5 (3), pp.48-56. IEEE Computer Society, Los Alamitos, Jul. 2006.
- [9] 井上 創造、木實 新一, 小林 隆志, 土田 正士, 喜連川 優, "RFIDを用いた学会参加者ネットワーク表示システムとその利用," *日本データベース学会 Letters*, Vol.5, No.1, pp.81-84, Jun. 2006.
- U  
査読無し
- [10] 井上創造, 小山健一郎, "種々の画面サイズに対応した仮想書架Webインタフェース", 九州大学附属図書館研究開発室年報2007/2008, pp.8-11, Oct. 2008.
- [11] 井上 創造、堀 優子, "SNSにおける新し

い信頼モデルと図書館における応用,”  
九州大学附属図書館研究開発室年報, pp.  
22-29, Oct. 2007.

- [12] 井上 創造, 安浦 寛人, “非接触ICカードの原理と体系化,” 九州大学附属図書館研究開発室年報, pp. 20-25, Oct. 2007.

[学会発表](計 18 件)

#### 査読あり

- [13] 井上創造, 中島直樹, “センサネットワークを用いた生活習慣病予防医療”第2回デジタルメディスン・イニシアチブ講演会抄録集, IEEE EMBS West Japan, pp.7, Oct.,2008.
- [14] Osamu Sudoh, Sozo Inoue and Naoki Nakashima, “eService Innovation and Sensor Based Healthcare,” *Proc. IFIP International Federation for Information Processing*, Vol. 286/2008, pp.1-14, Springer Boston, Aug. 2008.
- [15] Daisuke Ikeda and Sozo Inoue, “A Sustainable Model based on the Social Network Service to Support the Research Cycle,” *Proc. of The 3<sup>rd</sup> International Conference on Open Repositories*, <http://pubs.or08.ecs.soton.ac.uk/17/>, 4 pages, Apr. 2008.
- [16] Yasunobu Nohara, Sozo Inoue, Hiroto Yasuura, “A Secure High-Speed Identification Scheme for RFID Using Bloom Filters,” *Proc. of 3rd International Conference on Availability, Reliability and Security*, pp.717-722, Mar. 2008.
- [17] Sozo Inoue, Daisuke Ikeda, “A New, Sustainable Model for the Institutional Repository: A CSI Project ”integration and Presentation of Diverse Information Resources”, *DRF Int’l Conf. 2008*, pp.58. Jan. 2008.

- [18] Sozo Inoue, Yuko Hori, Daisuke Ikeda, “Trustworthy SNS for Institutional Repositories,” *DRF Int’l Conf. 2008*, (Poster), Jan. 2008.
- [19] Sozo Inoue, Daisuke Miyaoka, Daisuke Ikeda, Toshiro Minami, Kiyotaka Fujisaki, “RFID Application for Library”, *Proc. Int’l Workshop on Real Field Identification*, pp.w4-31--38, Nov. 2007.
- [20] Yasunobu Nohara, Sozo Inoue, Hiroto Yasuura, “Toward Efficient Identification for Privacy-preserving Hash-based RFID Schemes,” *Proc. Int’l Workshop on Real Field Identification*, pp.w4-46--51, Nov. 2007.
- [21] 山崎 知美, 井上 創造, 中村 徹, 野原 康伸, 安浦 寛人, “権利管理システムへの権利貸与機能の適用について,” *マルチメディア, 分散, 協調とモバイル (DICOMO2007) シンポジウム*, pp.251-257, Jul. 2007.
- [22] 園田 章人, 井上 創造, “救急活動における個人情報の効率よい利用について”, *電子情報通信学会 第18回データ工学ワークショップ論文集 (CDROM)*, 6 pages, Mar. 2007.
- [23] Yasunobu Nohara, Sozo Inoue, Hiroto Yasuura, “Unlinkability and Real World Constraints in RFID Systems,” *Proc. Pervasive RFID/NFC Technology and Applications Workshop* pp.371-376, Mar., 2007.
- [24] Sozo Inoue, Akihiko Sonoda, Kenichiro Oka, and Shinichiro Fujisaki, “Triage with RFID Tags,” *Proc. 1st International Conference on Pervasive Computing Technologies for Healthcare 2006*, (CD-ROM, 7 pages), 2006.
- [25] Sozo Inoue, Akihiko Sonoda, Kenichiro Oka, and Shinichiro Fujisaki, “Emergenc

y Healthcare Support: RFID Based Massive Injured People Management,” *Proc. Pervasive Healthcare Workshop in Ubicomp 2006 (UbiHealth)*, (Web publication), 9 pages, 2006.

- [26] Sozo Inoue, Daisuke Hagiwara, Hiroto Yasuura, “Systematic Error Detection for RFID Reliability,” *Proc. Int’l Conf. Availability, Reliability and Security (ARES)*, pp.280-286, Apr. 2006.

#### 査読無し

- [27] 井上 創造, 小山 健一郎, “種々の画面サイズに対応した仮想書架Webインタフェース”, 九州大学附属図書館研究開発室年報2007/2008, pp.8-11, Oct. 2008.
- [28] 案浦 スミタカ, 荒木 寛幸, 井上 創造, 池田 大輔, “SNSを用いた研究支援と認証認可付き検索システム,” *デジタル図書館 Vol. 34*, pp. 21--32, Mar., 2008.
- [29] 野原 康伸, 井上 創造, 安浦 寛人, “ブルームフィルタを用いた高速RFID識別方式”, *コンピュータセキュリティシンポジウム2007(CSS2007) 予稿集*, Vol.2007, No.10, pp.301-306, Oct. 2007.
- [30] 井上 創造, 堀 優子, 池田 大輔, “SNS (Social Networking Service) における信頼と図書館における応用,” *第33回デジタル図書館ワークショップ*, pp.31-42, Nov. 2007.

〔図書〕(計3件)

- [31] Sozo Inoue, Akihito Sonoda, Hiroto Yasuura, “Triage with RFID tags for Massive Incidents,” *RFID Handbook: Application, Technology, Security and Privacy*, Syed Ahson and Mohammad Ilyas (Ed.), CRC

Press, pp.329-349, 2007.

- [32] Yasunobu Nohara, Kensuke Baba, Sozo Inoue, Hiroto Yasuura, “Privacy and Personal Information Protection in RFID Systems,” *RFID Handbook: Application, Technology, Security and Privacy*, Syed Ahson and Mohammad Ilyas (Ed.), CRC Press, pp. 485-497, 2007.
- [33] 井上 創造, 宮岡大輔, 池田大輔, 南俊朗, 藤崎清孝, “図書館へのRFID導入事例,” *RFID技術ガイドブック*, pp.89-92, (株)電子ジャーナル, 2007.

〔産業財産権〕  
出願状況(計 0 件)

取得状況(計 0 件)

〔その他〕

- [34] 井上 創造, 案浦スミタカ, “図書館におけるSNSの連携と応用,” *大学の図書館*, No. 405, 第26巻8号, pp.130-137, Aug., 2007.
- [35] 井上 創造, 増永良文, “災害救助を迅速化するRFIDトリアーシステム,” *月刊DBマガジン*, pp.122-123, 翔泳社, Sep. 2007.
- [36] 井上 創造, “ICタグを利用したトリアーシステム(第1回),” *日経RFIDテクノロジー*, pp.22-27, Jun. 2006.
- [37] 井上 創造, “ICタグを利用したトリアーシステム(最終回),” *日経RFIDテクノロジー*, pp.21-23, Jul. 2006.

#### 6. 研究組織

(1) 研究代表者

井上 創造 (INOUE SOZO)

九州大学・附属図書館研究開発室・准教授  
研究者番号: 90346825

(2) 研究分担者

(3) 連携研究者

野原 康伸 (NOHARA YASUNOBU)

九州大学・大学院システム情報科学研究所・  
学術研究員