（様式４－１）

二国間交流事業 共同研究報告書

平成　23 年　10 月　31 日

独立行政法人日本学術振興会理事長　殿

共同研究代表者所属・部局　九州工業大学大学院工学研究院

職・氏 名（ふりがな）　准教授・井上創造（いのうえそうぞう）

1. 事　業　名　相手国（　中国　）との共同研究　　振興会対応機関（　NSFC　）

2. 研 究 課 題 名　現実世界の制約を利用した RFID の安全性とプライバシ保護技術の研究

3. 全 採 用 期 間

平成 21 年 4 月 1 日 ～ 平成 23 年 9 月 30 日 （ 2 年 6 ヶ月）

4. 経 費 総 額

(1) 本事業により執行した研究経費総額　4,021 千　円

初年度経費 1,410 千　円、　２年度経費 1,220 千円、　３年度経費 1,391 千円

(2) 本事業経費以外の国内における研究経費総額　1,000 千　円

5. 研究組織

(1) 日本側参加者（代表者は除く）

氏名（ふりがな）	所属・職名	研究協力テーマ
櫻井 幸一	九州大学・教授	セキュリティ理論
稲永 俊介	九州大学・特任准教授	セキュリティ理論
野原康伸	九州大学・学術研究員	セキュリティプロトコル
服部祐一	九州工業大学・大学院博士前期課程	実験システム開発
寺浦信之	九州大学・大学院博士後期課程	セキュリティプロトコル
馬建華	法政大学・教授	プロトコル設計
中村優斗	九州工業大学・大学院博士前期課程	応用システム設計
照本旭生	九州工業大学・大学院博士前期課程	実験実施
李林	九州工業大学・大学院博士前期課程	応用システム開発
中村 徹	九州大学・大学院博士後期課程	セキュリティプロトコル
蘇 春華	九州大学・大学院博士後期課程	セキュリティ検証
Uddin Mohammad Mesbah	九州大学・助教	プロトコル設計
竹森正起	九州工業大学・支援研究員	実験システム開発

(2) 相手国側研究代表者

所属・職名・氏名

北京大学・教授・Chen Zhong

(3) 相手国参加者（代表者は除く）

氏名	所属・職名（国名）	研究協力テーマ
Huiping Sun	Pekin University, Assistant Professor（中国）	物理制約を考慮したプロトコル
Shengyuan Wang	Pekin University, Associate Professor（中国）	セキュリティプロトコルの高度化
Zhi Guan	Pekin University, Assistant Professor（中国）	セキュリティプロトコルの実装
Wei Xin	Pekin University, Ph. D Candidate（中国）	セキュリティプロトコルの改良と実装
Shengyuan Wang	Pekin University, Associate Professor(中国)	セキュリティ理論
Yongming Jin	Pekin University, Ph. D Candidate（中国）	実験と評価

6．研究実績概要（全期間を通じた研究の目的・研究計画の実施状況・成果等の概要を簡潔に記載してください。）

本研究では，セキュリティとプライバシを満たす RFID の識別プロトコルを開発し，それを理論的かつ実際的に検証することを目的とした．その際に，RFID タグのコストやリーダ（読み取り機）側での処理時間も考慮し，実用に値する RFID システムへの道を開く．この目的が達成されれば,これまでと異なるオープンな形での RFID システムの普及が可能となり,それを前提としたユビキタスコンピューティングの新たな研究フィールドが生まれることが期待できる．

初年度は，双方の持つ技術的な蓄積とシステムを公開しあうために，双方での研究会と見学会を開催し知識を共有した．

まず 7 月に相手国研究者が日本を訪問し，日本側がこれまでに行ってきた RFID のセキュリティとプライバシに関する研究成果の説明を行い，相手国の研究グループに理論的背景を含めて理解を深めてもらった．また見学として，

・ 九州大学が持つ RFID 図書館,
・ RFID に対応した 60 万冊規模の自動書庫,
・ われわれのグループが開発にかかわった非接触型 IC カードによる学生・職員証システム

を見学してもらい，相手国側研究グループに実システムの実感を得てもらった．

また 8 月に，日本側研究者が中国を訪問し，相手国側がこれまでに行ってきた情報セキュリティ分野における研究成果の説明をしてもらい，日本側との背景知識のすり合わせを行った．相手国側におけるソフトウェア開発体制や開発環境を見学し，具体的な実証システム開発のイメージを得た．また，1 月に，日本側研究代表者が再度相手国を訪問し，新しいプロトコルのアイデアを議論した。この議論は引き続き，2 月に相手国研究者が日本を訪れた際に議論を深めた．

2 年度目は，7 月に北京大学においてワークショップ(The 1st China-Japan Workshop on RFID Application and Security) を開催し，本研究参加者の中では日本側からは井上・櫻井・稲永が，中国側からは Zhong Chen, Huiping Sun, Zhi Guan が研究の最新状況を報告し，有益な議論を行った。

この中で、理論検証グループは，最新の理論研究のサーベイや，プライバシを保護するための理論的枠組みについて発表を行った。また実証実験グループにおいては，RFID の追跡可能性についてのモデル化および，RFID 書架の信頼性向上について発表した。これらの成果は国際会議論文や論文誌へとつながっている．さらに，このワークショップに参加した Jinhua Ma 氏および寺浦氏とも積極的に議論し，次年度本研究に参加してもらうこととなった。

最終年度においては,これまでの研究成果を発表しあって更なる研究の発展を試みた．まず 7 月に北京大学から 3 名が日本を訪問し，第 2 回ワークショップ(The 2nd Japan-China Workshop on RFID Application and Security)を行い，成功を収めた．また 8 月には日本側研究者が中国を訪問し，今後も引き続き協力体制を継続することに合意した．さらには 9 月に日本側研究者が中国を再度訪問し，研究成果発表および今後の研究体制や研究テーマ申請に関する調整を行った．

これらの成果は，2011 年 4 月に中国無錫で行われた RFIDsec 2011 Asia において，井上が Keynote Speaker としての招待講演につながった

研究期間中において行った主な活動は上記の通りだが，この他に研究代表者や分担者が何度も北京大学を訪問した．また遠隔会議システムを用いた会議も適宜実施した．またワークショップにおいても日本自動認識協会，日本ユニシス, NTT, 中国電子標準化協会，Jiangu Joyque 社にも参加してもらい産学交流も行った．