平成２５年度研究開発成果概要書

課題名　　：軽量暗号プロトコルの省リソースデバイスに対する実装効率向上に関する研究
採択番号　：１６２
個別課題名：
副題　　：プライバシ保護とセキュリティレベル切替えが可能なセキュアＲＦＩＤタグの実現

（１）研究開発の目的

「プライバシ保護とセキュリティレベルの切替え機構を実装した 1 チップパッシブ RFID タグ」の実装技術のフィージビリティを確認する。

（２）研究開発期間

平成 24 年度から平成 26 年度（3 年間）

（３）委託先

株式会社　サイバー創研＜幹事会社＞、国立大学法人　電気通信大学、株式会社　日立製作所

（４）研究開発予算（契約額）

総額　185 百万円（平成 25 年度　61 百万円）

※百万円未満切り上げ

（５）研究開発課題と担当

課題 1：アプリケーションを考慮した普及促進に資する技術の研究開発

1. アプリケーションに応じたセキュリティレベルの制御技術（㈱サイバー創研）
2. セキュリティレベルに応じた軽量暗号プロトコルへの普及促進に資する機能の搭載技術　（学校法人電気通信大学）

課題 2：１チップ実装技術の研究開発

1. 軽量暗号プロトコルの実装技術（学校法人　電気通信大学）
2. 暗号化方式の選定と実装技術（㈱　日立製作所）

（６）これまで得られた研究開発成果

		（累計）件	（当該年度）件
特許出願	国内出願	4	2
	外国出願	0	0
外部発表	研究論文	0	0
	その他研究発表	13	7
	プレスリリース	0	0
	展示会	0	0
	標準化提案	0	0

国内特許出願累計件数に関する補足説明

H24 年度は、電通大　１件、サイバー創研　１件で合計２件

H25 年度は、電通大　１件、サイバー創研　１件で合計２件

電通大の H24 年度の出願１件は公知技術であることが判明したため，H25 年度に取り下げた

（７）具体的な成果実施内容と成果

課題 1) アプリケーションを考慮した普及促進に資する技術の研究開発

課題 1)-(1)）アプリケーションに応じたセキュリティレベルの制御技術（㈱サイバー創研）

タグのプライバシ保護レベルの安全な切替えを実現するために、タグとサーバ間のメッセージシーケンスを策定した。また、プライバシ保護レベル切替え中の電力不足発生に対応するためにタグが保持すべき情報と情報の切替条件を抽出した。さらに、タグディジタル部の消費電力と負荷の違いが電力供給部に与える影響をシミュレーションで検証した。

課題 1)-(2)セキュリティレベルに応じた軽量暗号プロトコルへの普及促進に資する機能の搭載技術（国立大学法人電気通信大学）

1 回目の RFID タグを作製し、機能検証を行った。具体的には、試作チップのメモリの物理マッピングの策定を行い、RTL シミュレーションで機能検証を完了した。ディジタル部とアナログ部を含めたレイアウトの基本設計・詳細設計を完了し、１回目の試作チップを外注により作製した、アンテナと接続し、機能検証とフィージビリティ検証を行った。

課題 2) １チップ実装技術の研究開発

課題 2)-(1)）軽量暗号プロトコルの実装技術（学校法人　電気通信大学）

軽量暗号プロトコルのハードウェア実装による機能検証を行った。具体的には、昨年度策定した軽量暗号プロトコルの各種パラメータにもとづきハードウェアに実装した。そして、FPGA を用いてディジタル部全体のハードウェア実装による基礎実験と機能検証を行った。

課題 2)-(2)）暗号化方式の選定と実装技術（㈱　日立製作所）

暗号コアの選定では、静的電力とピーク電力の評価を行った。平成 24 年度実施の性能評価結果と電力評価結果にもとづき、暗号コアとしてハッシュ関数 SPONGENT-160 を選択した。1 回目チップ試作用の暗号コアを開発し、仕様書をまとめた。暗号コアの軽量実装技術では、消費電力と処理速度のトレードオフ関係を明らかにした。