平成２６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の研究開発
採択番号　：１６２
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＜代表研究者＞、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　183 百万円（平成 26 年度　57 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（株式会社サイバー創研）
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（株式会社日立製作所）

（6）これまで得られた研究開発成果

		（累計）件	（本年度）件
特許出願	国内出願	7	5
	外国出願	1	1
外部発表	研究論文	0	0
	その他研究発表	23	10
	プレスリリース	1	1
	展示会	0	0
	標準化提案	0	0

【プレスリリースに関する補足説明】

平成 26 年度に発表したニュースリリースは電気通信大学及び日立製作所でそれぞれ個別にリリースした（件数としては 1 件とカウント）、関連して新聞報道：4 件、電子ニュース：多数を確認している（但し、報道のカウントとしては、0 件）

（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)

利用シーンを想定したシミュレーション検証と課題 1)-(2)で作製された試作チップによる実機検証を実施し、それぞれの検証で得られる結果を合わせて、RFID タグチップのフィジビリティ検証を行った。

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）

H25 年度に試作した１回目の試作チップのフィジビリティ検証の結果に基づき、H26 年度に試作するチップ（２回目）の基本仕様の策定を行った。1 回目に試作したセキュア RFID タグを追加で購入し、測定結果の確度を高めた。また、アナログ部とデジタル部の回路パラメータを調整し、チップの低消費電力化を図るとともに、通信距離とのトレードオフを明らかにした。さらに、2 回目に試作するチップをアンテナ基板と接続し、タグとしての性能評価を行った。

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）

H25 年度に試作したチップの実証実験結果に基づき、２回目に試作するチップに搭載する軽量暗号プロトコルの基本仕様を策定し、RTL シミュレーションと FPGA を用いた機能検証を行った。さらに、軽量暗号プロトコルの軽量実装技術を確立するために、試作したチップを用いて、軽量暗号プロトコルの機能を実証実験で検証し、軽量暗号プロトコルの軽量実装技術のフィジビリティ検証を行った。

課題 2)-(2) 暗号化方式の選定と実装技術（㈱　日立製作所）

2 回目チップ試作用の暗号コアの選定では、暗号モジュールの消費電力、回路面積と処理時間の評価を実施した。上記ハードウェア実装性能の評価結果に基づき、暗号コアとしてハッシュ関数 SPONGENT とハッシュ関数 Keccak を選出した。暗号コアの軽量実装技術では、2 回目チップ試作用の暗号コアのハードウェア基本仕様をまとめ、暗号コアの開発を行った。また、暗号コア実装性能のトレードオフ評価を行った。