事後評価報告書
（日本–台湾研究交流「セキュアでディペンダブルな IoT ポータブル デバイスのための研究」）

１．　研究課題名：

「IoT デバイスのための新しい軽量暗号システムに関する研究と台湾の eHealth 環境への応用」

２．研究代表者名：

日本側：　大阪大学 大学院工学研究科 教授　宮地 充子

相手側：　長庚大学 資訊管理学系 教授 許 建隆

３．総合評価：　A

４．事後評価結果

（１）研究成果の評価について

本研究交流は、計算能力やバッテリ等のリソースが限られる IoT デバイスにおいても実行可能な軽量暗号技術を開発し実装・検証することにより、安全で安心な IoT システムの確立に資することを目指すものであり、当初の計画で提案された日本側が開発する公開鍵暗号、共通鍵暗号、ホワイトボックス暗号に関する基礎的な研究成果が 10 件の国際共著論文によって発表され、さらに国際共著を含む総原著論文、査読付き国際会議論文数は 67 件、関連の招待講演は 6 件となり十分な成果が認められる。

双方の連携によって軽量な共通鍵暗号を実装、医療環境向けの IoT 機器の安全認証システムを提案し、そのプロトタイプを実証した点は評価できる。軽量共通鍵暗号及び認証方式については、実機上での実装評価を実施し、実際の計算量、消費電力量を明確にした。また、軽量公開鍵暗号についても、C 言語で実装し最小のメモリ量で最速の処理が実現できることを実証した。これにより eHealth のアプリケーション実装が十分可能であることを明確にしたことは評価できる。

（２）交流成果の評価について

人材育成の観点では、日本側研究拠点に台湾出身の教員が複数含まれていることも功を奏し、台湾側の学生受け入れ、日本の学生の台湾への派遣、共同ワークショップ開催など特に若手研究者の人材育成、研究交流が進んだ点は評価できる。

協働関係の観点では、定期的な遠隔会議を開催し、研究連携を推進した実績は評価できる。さらに台湾での国際会議 NSS2016 の開催、２度の共同ワークショップ、7 回のセミナー及び研究ミーティングを実施した。国際会議及びワークショップについては内容が web で公開されており、日本－台湾の共同研究の成果を広く PR した点は評価できる。

（３）その他

なし

以上