科学研究費助成事業（基盤研究（Ｓ））事後評価

課題番号	18H05289	研究期間	平成３０(2018)年度 ～令和４(2022)年度
研究課題名	暗号技術による IoT エコシステムのレジリエンス向上	研究代表者 （所属・職） （令和５年３月現在）	崎山　一男 （電気通信大学・大学院情報理工学研究科・教授）

【令和５(2023)年度　事後評価結果】

評価		評価基準
○	A＋	期待以上の成果があった
	A	期待どおりの成果があった
	A－	一部十分ではなかったが、概ね期待どおりの成果があった
	B	十分ではなかったが一応の成果があった
	C	期待された成果が上がらなかった

（研究の概要）

IoT エコシステムのレジリエンスは IoT 社会における重要なトピックであることから、本研究では、漏洩耐性をもつ暗号システムや漏洩検知技術を主要な研究対象としている。主に IoT のデバイスのレベルでの特に暗号鍵を中心に情報漏洩を防ぎ、システムの安全性を高めることを目的としており、その社会的重要性は高い。本研究が対象とする IoT システムは計算資源が限られた小型コンピュータから成るものの、機器の数が非常に多く、日常生活のモニターなどに使われるため、ひとたび脆弱性が見つかり攻撃に利用されると、その社会的な被害は甚大になりがちである。

（意見等）

当初計画していた研究項目は概ね全て達成しているほか、当初の計画に入っていなかった物理攻撃対策を評価するための AES 暗号化デバイスも国際共同研究により追加で開発しており、期待以上の成果が上がったと評価できる。また、研究計画で挙げられていた研究項目のうち、漏洩耐性のための理論研究は特に優れた成果を生み、国際的にも高く評価された。そのほか、本研究が生み出した暗号化デバイスにおける情報漏洩の機構を評価するための実験用ハードウェア、情報漏洩検知のためのセンサも国際的に高く評価されている。