事後評価報告書

１．研究課題名：「次世代情報セキュリティシステムの設計と解析」

２．研究代表者名：
２－１．日本側研究代表者：東京大学　今井　浩　教授

２－２．米国側研究代表者：　ラトガース大学　Mario Szededy　教授

総合評価：　秀

３．研究交流実施内容及び成果：
新世代の量子情報セキュリティシステムの設計と量子計算による現代暗号セキュリティの解析に関する研究であり、次世代情報セキュリティシステム、次世代情報セキュリティシステム（特に量子計算による解析）および情報セキュリティ基礎理論（特に計算量理論研究）に関する研究の推進を目的としている。

①　日本側の成果
②　相手国側の成果
計算量理論に基づくセキュリティ解析の技術を有する米国 Rutgers 大学・Rochester 大学と日本側メンバーが従来個別に研究交流してきた実績を発展させて交流しており、いずれのテーマに関しても、日本側研究代表者と米国側研究代表者とが協力して成果が得られていることから、日本側、米国側の成果について切り分けが困難であるため、両者の成果としてまとめる。
(1)次世代情報セキュリティシステムの研究
米国側より、量子通信量計算での種々のアイデア提供を受けて、日本側メンバーで量子通信と量子計算を融合したモデルに関する研究を進め、量子ネットワーク符号化という通信ネットワークで計算を用いて容量を増大させるとともに、同方式による新たな量子セキュリティプロトコルの設計を行った。これらの成果は、ICALP (International Colloquium on Automata, Languages and Programming)や STACS (International Symposium on Theoretical Aspects of Computer Science)において複数の論文で発表されている。
(2)次世代情報セキュリティシステムの解析
量子計算による攻撃に対して次世代情報セキュリティシステムがもつべき耐性を定性的にも定量的にも明らかにすることを可能とする解析方法についての研究であり、代数構造を有する問題に対して群同型判定という新たな枠組みでの量子計算の優越性を示した。
(3)情報セキュリティ基礎理論の研究
情報セキュリティの安全性に対して、理論に基づいた保証を行うため、計算理論および情報

理論における基礎理論が必要となる。このため、本研究においては，現代計算量理論の最先端である確率的検査可能証明に関する研究で Gödel 賞を 2 度受賞している米国側の研究代表者の理論を発展させ、ASIACRYPT (Annual International Conference on the Theory and Application of Cryptology & Information Security), ISAAC (International Symposium on Algorithms and Computation)などの国際会議で成果を発表している。

４．事後評価結果

４－１　総合評価

量子計算、量子通信、それを用いた安全性の基礎理論の構築において、インパクトの大きな成果を上げている。波及効果の大きい基礎理論が得られていることから、今後の持続的な発展が期待できる。

また、若手研究者の国際研究交流という観点を大きな目的の一つとして捉えており、実際に研究リーダだけでなく、多数の若手研究者を海外へ派遣していることは評価に値する。原著論文の数の点からは、その成果も大変大きなものが得られている。ただし、若手研究者の派遣はどちらかというと国際会議での研究発表が中心になっているように見受けられるが、本研究交流が次世代を担う若手研究者を国際交流・共同研究にいざなう機動力となることを期待する。

４－２．研究交流の有効性

日本側、相手側の主要メンバーの研究交流は研究期間中に密に行われており、また、日本側のグローバル 30 に対する支援、また ACM-SIAM SODA (Symposium on Discrete Algorithms) の 2012 年開催地として京都が決定されるなど今後の連携が継続できる基盤もできており、「当該事業を端緒とした相手国との研究交流の増加／持続的な発展の可能性」は十分であると判断できる。

日本側と相手側の共同研究者との交流は、相互に訪問する形で計 20 回行われており、日本側からの講師、助教クラスの若手研究者の多数の派遣に関しては、今後の国際研究交流拡大のきっかけとなることが期待でき、「相手国との研究交流につながる人材の育成」の目的も達成されている。また、セミナーは 7 回、ワークショップは 3 回、日本で開催されている。

４－３．当初目標の達成度評価

計画通りに進め、十分な成果をあげている。4 件の受賞も実績としてあげられており、全体として技術の進展、論文成果は十分であると判断できる。但し、日本側と米国側との共著論文については、両者のアクティビティを考慮するとさらに見込まれたと考えられ、今後のさらなる成果を期待したい。