事後評価報告書（日本－インド研究交流）

１．研究課題名：「RFID とセンサネットワーク向け暗号基礎技術とそれを用いた構成要素の設計および安全性評価」

２．研究代表者名：

２－１．日本側研究代表者：

産業技術総合研究所　セキュアシステム研究部門　研究グループ長　渡辺　創

２－２．インド側研究代表者：

インド工科大学ルールキー校　数学科　准教授　Sugata Gangopadhyay

３．総合評価：（　Ｂ　）

４．事後評価結果

（1）研究成果の評価について

ストリーム暗号の安全性評価に関して、インド側の解析技術と日本側の暗号設計技術を融合して k-normality という新たな安全性指標を提示することができ、複数のストリーム暗号の安全性が低いことを示した点が評価できる。従来方式との比較があるともっとよかったであろう。

提案書には 5 つの目標が掲げられているが、最終報告書ではそれらの提案目標に関する成果の記述がないものがある。目標に対して示されている成果は、かなり限定されたものである印象を受ける。

（2）交流成果の評価について

共同研究を通じて k-normality が提案できており、交流の成果があがったといえる。また、多くのワークショップを開催して交流を推進し、多くの成果発表を行っている点も評価できる。ただ、発表論文の著者が、日本側は招聘研究員が主体となっており、本研究に加わった共同研究者との連名の論文がやや少ない。今後、日イ共同研究体制をさらに強化し、研究はもとより人材育成などの視点からも具体的な交流を深められることを期待する。

（3）その他（研究体制、成果の発表、成果の展開等）

提案書では日本側は 4 名で実施するとあったが、最終的に 15 名に増えている。ここまで増やすのには必要性があったと思われるが、その理由が明確に書かれていない点が残念である。