

事後評価報告書（日本－インド研究交流）

1. 研究課題名：「数理科学的手法による暗号アルゴリズム解析とネットワークセキュリティ強化評価」

2. 研究代表者名：

2－1. 日本側研究代表者：

九州大学 大学院システム情報科学研究所 情報工学部門 教授 櫻井 幸一

2－2. インド側研究代表者：

インド統計学研究所 応用統計学ユニット 教授 Bimal Roy

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

日本とインドの双方の研究能力と研究実績を生かした国際的な共同研究である。計画書の段階から具体的かつ詳細な課題と目標および担当研究者を検討して、計画書にそった実施が行われ、期待以上の成果がでている。K2 暗号評価、非可換暗号提案、鍵配送最適化、ボット対策等、多くの研究課題を掲げていたが、それぞれ目標を達成している。理論をベースにしながらも、KDDI 研究員を招聘したり、特許を申請したりするなど、実用化を目指しており、評価できる。K2 暗号は以前からの成果であるが、本プロジェクトでインド研究者を交えて評価検討を行って国際標準化できたことは大きな成果である。

（2）交流成果の評価について

シンポジウム、ワークショップ、セミナーを 10 回以上開催しており、大変活発に交流が行われた。また、プロジェクト以外の研究員も適宜加えて交流を進めた。インド側複数メンバーが本研究成果も一部含めて学位取得に至っており、人材育成に貢献があったとみられる。他の関連研究課題とワークショップを共同開催して連携を深め、関連知識の獲得を目指しているのは評価できる。

（3）その他（研究体制、成果の発表、成果の展開等）

多くの研究発表がなされ、今後につながる活動を行っており、また、国際規格化にも成功して普及につながったことは評価できる。