平成２６年度北陸地区国立大学学術研究連携支援報告書

研究グループ名	情報セキュリティ研究会（HISS） （支援期間：平成 25 年度～平成 26 年度）	
大学名	所属	氏名
北陸先端科学技術大学院大学	情報科学研究科	○宮地充子
北陸先端科学技術大学院大学	情報科学研究科	面和成
北陸先端科学技術大学院大学	情報科学研究科	陳嘉耕
福井大学	工学研究科	○廣瀬勝一
※　各大学の研究グループ責任者の氏名には○印。		

その他の機関の構成員	機関名	所属	職名	氏名
	広島市立大学 信州大学	大学院情報科学研究科 情報工学科	准教授 助教	双紙正和 岡崎裕之

成果概要

近年，電子社会の進展およびユビキタス機器の普及に伴い，暗号学は様々な技術分野と融合し，新しいアプリケーションの実現に必要不可欠になってきている．暗号学のパイオニア研究や新しい展開・応用先を発掘するフロンティア研究は，安全・安心な電子社会のさらなる促進に向けて，ますます重要になるといえる．

このような背景のもと，情報セキュリティ研究会（HISS）は以下を目標として，暗号フロンティア研究会を毎年主催している．

1. 第一線の研究者間の人材交流．
2. 異なる組織で行われている最先端の研究の融合．
3. 異なる研究分野の有機的な結合，融合．
4. 第一線の研究者のさらなる研究発展のためのインスピレーションの交換．

具体的には，以下の研究者に招待講演を依頼し，北陸先端科学技術大学院大学において第５回及び第６回研究会を実施した．さらに，講演終了後には，講演者のみで研究に関するフリーディスカッションを実施し，各講演者の研究分野の融合や新しい研究課題の開拓に関して議論した．

[第５回暗号フロンティア研究会]
井上大介（NICT），高木剛（九州大学），花岡悟一郎（産業技術総合研究所），藤澤克樹（中央大学），安田雅哉（富士通研究所），山西 健司（東京大学）
[第６回暗号フロンティア研究会]
石川博（早稲田大学），河原林健一（国立情報学研究所），高木剛（九州大学），高橋克巳（NTT セキュアプラットフォーム研究所），峯松一彦（NEC）

獲得した外部資金

・CREST（H26～H31），ビッグデータ統合利活用促進のためのセキュリティ基盤技術の体系化，宮地充子（代表），375,000 千円．
・基盤研究(C)（H25～H27），証明可能安全性を有する応用指向セキュリティプロトコルの開発，廣瀬勝一（代表），3,800 千円．
・若手研究(B)（H25～H28），準同型認証子による効率の良いデータ認証手法に関する研究，面和成（代表），2,500 千円．
・若手研究(B)（H27～H30），共通鍵暗号の精密解析に関する研究， 陳嘉耕（代表）， 4,630 千円．
・基盤研究(C)（H27～H30），ハッシュ連鎖の柔軟な構成法およびそれを応用した軽量認証法の研究，双紙正和（代表）．