様 式 Ｃ－７－１

平成２１年度科学研究費補助金実績報告書（研究実績報告書）

1. 機 関 番 号 | 1 | 4 | 6 | 0 | 3 |　　2. 研究機関名　奈良先端科学技術大学院大学

3. 研 究 種 目 名　基盤研究（C）　　4. 研究期間　平 成 20 年 度 ～ 平 成 22 年 度

5. 課 題 番 号 | 2 | 0 | 5 | 6 | 0 | 3 | 5 | 6 |

6. 研 究 課 題 名　次世代型グループ情報共有・流通のセキュリティ基盤に関する研究

7. 研 究 代 表 者

研究者番号	研究代表者名	所属部局名	職名
70263431	ﾌﾘｶﾞﾅ　カジ，ユウイチ 楫　勇一	情報科学研究科	准教授

8. 研究分担者（所属研究機関名については、研究代表者の所属研究機関と異なる場合のみ記入すること。）

研究者番号	研究分担者名	所属研究機関名・部局名	職名
	ﾌﾘｶﾞﾅ		
	ﾌﾘｶﾞﾅ		
	ﾌﾘｶﾞﾅ		
	ﾌﾘｶﾞﾅ		
	ﾌﾘｶﾞﾅ		

9. 研究実績の概要

下欄には、当該年度に実施した研究の成果について、その具体的内容、意義、重要性等を、交付申請書に記載した「研究の目的」、「研究実施計画」に照らし、600 字～800 字で、できるだけ分かりやすく記述すること。また、国立情報学研究所でﾃﾞｰﾀﾍﾞｰｽ化するため、図、ｸﾞﾗﾌ等は記載しないこと。

本研究課題では，大規模グループ鍵の更新手法に関する研究，自律分散グループ鍵に関する研究の二つの具体的課題を設定し，研究活動を行っている．

大規模グループ鍵に関する平成21年度の研究では，センサネットワークに代表されるような，計算資源のきわめて乏しい端末を想定したグループ鍵管理手法について検討を行った．グループ鍵管理において必要となる複雑な要件を満足するためには，公開鍵暗号に代表される数論的な手法を利用することが効果的であるが，それら方式では，数百～数千ビット規模の数値演算が必要となるため，計算資源，とくにバッテリ容量に制限のある端末での利用は好ましくない．平成21年度の研究では，センサネットワーク特有の通信形態に特化することにより，単純なハッシュ関数と秘密情報の組み合わせにより，安全で柔軟な鍵管理が可能となる方式を開発した．

自律分散グループ鍵に関する研究では，近年の各種サービスにて頻繁にみられる形態を念頭に置き，ロールベースアクセス制御方式の拡張法について検討を行った．アクセス制御そのものは，暗号鍵の管理と直接の関連はないが，グループ鍵を利用することにより，柔軟で安全性の高いアクセス権管理を実現することができる．とくに，階層型ＩＤベース型暗号によりある種のグループ鍵を実現し，その鍵を用いてユーザ・ロール関係の定義関係を表現することにより，ドメイン間でのロール流用や，ロールの移譲といった仕組みを安全かつ柔軟に実現することが可能となる．平成21年度の研究では，このアプローチの詳細化を行い，他のドメイン横断型情報交換の仕組みとの関係を整理した．

10. キーワード

(1) 情報セキュリティ　(2) 暗号鍵　(3) グループ通信
(4) LKH 法　(5) マルチキャスト通信　(6) 放送暗号
(7)　(8)

（裏面に続く）

11.研究発表（平成２１年度の研究成果）

〔**雑誌論文**〕　計（0）件　　うち査読付論文　計（0）件

著　者　名	論　　文　　標　　題			
雑　　誌　　名	査読の有無	巻	発 行 年	最初と最後の頁

著　者　名	論　　文　　標　　題			
雑　　誌　　名	査読の有無	巻	発 行 年	最初と最後の頁

著　者　名	論　　文　　標　　題			
雑　　誌　　名	査読の有無	巻	発 行 年	最初と最後の頁

〔**学会発表**〕計（5）件　　うち招待講演　計（0）件

発　表　者　名	発　　表　　標　　題	
Y. Kaji	On the Number of Minimum Weight Codewords of SFA-LDPC Codes	
学　会　等　名	発表年月日	発　表　場　所
2009 International Symposium on Information Theory	2009.6.29	Seoul, Korea

発　表　者　名	発　　表　　標　　題	
Y. Kaji	On the Error Performance and Parameter Choices of the Array-Type LDPC Codes	
学　会　等　名	発表年月日	発　表　場　所
Tenth International Symposium on Communication Theory and Applications	2009.7.16	Ambleside, UK

発　表　者　名	発　　表　　標　　題	
Y. Kaji	On the Code Rate and Code Performance of SFA-LDPC Codes	
学　会　等　名	発表年月日	発　表　場　所
電子情報通信学会情報理論研究会	2009.9.30	東京都千代田区

発　表　者　名	発　　表　　標　　題	
杉山，楫	SFA-LDPC符号の低重み符号語の個数について	
学　会　等　名	発表年月日	発　表　場　所
第32回情報理論とその応用シンポジウム	2009.12.2	山口県山口市

発　表　者　名	発　　表　　標　　題	
福永，楫	チャレンジレスポンス相互認証における鍵の運用管理について	
学　会　等　名	発表年月日	発　表　場　所
2010年　暗号と情報セキュリティシンポジウム	2010.1.19	香川県高松市

〔図　書〕　計（　０　）件

著　者　名	出　版　社		
書　　名		発 行 年	総ページ数

12. 研究成果による産業財産権の出願・取得状況

〔出　願〕　　計（　０　）件

産業財産権の名称	発明者	権利者	産業財産権の種類、番号	出願年月日	国内・外国の別
（出願準備中）					

〔取　得〕　　計（　０　）件

産業財産権の名称	発明者	権利者	産業財産権の種類、番号	取得年月日	国内・外国の別

13. 備考

※　研究者又は所属研究機関が作成した研究内容又は研究成果に関するｗｅｂページがある場合は、ＵＲＬを記載すること。
