様 式 Ｃ－７－１

平成２２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	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

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．平成21年度までは，二つの課題について，やや独立した形で研究を進めてきたが，最終年度にあたる平成22年度の研究では両課題を融合し，自律分散的な大規模グループにおける鍵管理についての検討を行った．

現実世界における組織や団体においては，一貫したポリシーの下で管理される権利や権限と，現場裁量等により柔軟に設定できる権利・権限等が混在している．従来のアクセス制御関連の研究では，前者の仕組みを実現するための研究に多くの努力が費やされてきたが，現実世界の柔軟性をコンピュータシステム・ネットワークにおいて実現するためには，後者の柔軟な仕組みを安全に実現することも必要となる．本研究では，この問題に対処するため，階層型ロールベースアクセス制御方式を利用した権限管理の仕組みを提案した．単純にグループ鍵を認証目的に利用する場合と比べ，ユーザの持つ権限や属性に対応した認証等の実現が可能となっている．また，権限の委任や他者の推薦，信用の裏書等といった個人間の信頼関係を表現することも可能となっており，自律的に変化する信頼関係に対して柔軟に追従できる仕組みの実現に成功した．提案手法では，権限情報と鍵情報の一部とが統合されていることもあり，比較的シンプルな「アカウント」－「パスワード」関係の拡張として，本提案手法を実現することもできる．提案手法の有用性や効率についても評価するため，コンピュータソフトウェアとして提案手法を実装し，検証実験等も行った．

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２２年度の研究成果）

〔**雑誌論文**〕　計（　1　）件　　うち査読付論文　計（　1　）件

著　者　名	論　　文　　標　　題			
野田潤，楫勇一，中尾敏康	複数の大規模グループに同時参加するセンサノード向けグループ鍵管理方式			
雑　　誌　　名	査読の有無	巻	発 行 年	最初と最後の頁
情報処理学会論文誌	有	52	2011	1160-1172

〔**学会発表**〕計（　5　）件　　うち招待講演　計（　1　）件

発　表　者　名	発　　表　　標　　題		
Kai Zhou, Yuichi Kaji	A Mutual Authentication Using Visual Secret Sharing---an easy way to protect novice users from phishing fraud		
学　会　等　名		発表年月日	発　表　場　所
Workshop on Error-Correcting Codes and Cryptography (招待講演)		2010年4月23日	中国・揚州市

発　表　者　名	発　　表　　標　　題		
Ryo Yoshinaka, Yuichi Kaji, Hiroyuki Seki	Chomsky-Schutzenberger-Type Characterization of Multiple Context-Free Languages		
学　会　等　名		発表年月日	発　表　場　所
4th International Conference on Language and Automata Theory and Applications		2010年5月27日	ドイツ・トリア

発　表　者　名	発　　表　　標　　題		
Kai Zhou, Yuichi Kaji	Anti-Phishing Mutual Authentication Using the Visual Secret Sharing Scheme		
学　会　等　名		発表年月日	発　表　場　所
2010 International Symposium on Information Theory and Its Applications,		2010年10月19日	台湾・台中市

発　表　者　名	発　　表　　標　　題		
Yuki Tomotani, Yuichi Kaji, Hiroyuki Seki	Secure User-Role Assignment in Cross-Organizational Role-Based Access Control		
学　会　等　名		発表年月日	発　表　場　所
電子情報通信学会技術研究報告		2010年12月14日	群馬県・渋川市

発　表　者　名	発　　表　　標　　題		
友谷有希，楫勇一，関浩之	クロスドメインロールベースアクセス制御におけるユーザ・ロール関係記述方式		
学　会　等　名		発表年月日	発　表　場　所
2011年　暗号と情報セキュリティシンポジウム		2011年1月26日	福岡県・北九州市

〔**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（　1　）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
鍵管理装置、サービス提供装置、アクセス管理システム、アクセス管理方法、制御プログラム、およびコンピュータ読み取り可能な記録媒体	楫勇一 関浩之	奈良先端大	特許出願 2010-149517	2010年 6月30日	国内

〔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。
