# 平成２１年度研究ステーション研究成果報告書

※学科・専攻を超えた、或いは研究室の枠を超えた複数のメンバーによる組織的な研究活動について記載してください

１．研究ステーション名　情報セキュリティ研究ステーション
代表者名　情報メディアシステム学専攻　小池英樹

２．平成２１年度の研究の特筆すべき成果

次世代暗号理論についての研究を行った．多くの外部資金を獲得するとともに，せの成果の一部は電子情報通信学会において基礎境界ソサイエティ論文賞を受賞した．

科研費研究のテーマである「安全社会の獲得を目指した事故情報活用システムの機 構」構築を目指して、ユーザ・産業界・行政の三位一体による、トラブル情報活用の仕組みに取り組んだ。危険情報の受入れに対する心理的 影響、過信に関する実験や新聞情報の信頼性調査研究などにも取り組み、さまざまな 角度からトラブル情報の有効的活用を検討した。

不正侵入者の行動を分析するためのおとりシステム「ハニーポット」の国際アライアンス The Honeynet Project(http://www.honeynet.org)に The Japanese Honeynet Project として参加し，不正アクセス手法に関する情報交換を行っている．本アライアンスには米国，英国，フランス，ドイツ，ポルトガル，スペイン，ノルウェー，イタリア，パキスタン，ブラジル，ギリシア，フィリピン，中国，ニュージーランドなどが参加しており，本グループは日本の代表としての役割をになっている．

３．平成２１年度の研究成果の公表実績（主催した研究会、研究成果の発信状況等）

第１４回「信頼性とシステム安全学シンポジウム」，平成２２年２月２６日
参加者数７５名，発表件数１２件

４．外部資金の獲得状況

・科学研究費（基盤C）　暗号プリミティブの安全性検証の自動化への展開
　直接経費額　1,300,000円　　間接経費額　390,000円　　合計　1,690,000円

・受託研究　日本電信電話（株）
物理・論理・方式の各レイヤにおける暗号の安全性証明自動化手法に関する研究
直接経費額　　2,307,000円　間接経費額　693,000円　合計　3,000,000円

・共同研究　（株）東芝

実装攻撃に安全な暗号方式と安全性証明自動化手法の開発
直接経費額　　650,000円　間接経費額　65,000円　合計　715,000円

・共同研究　（株）キャンパスクリエイト
暗号プロトコル安全性評価の研究
直接経費額　　2,400,000円　間接経費額　240,000円　合計　2,640,000円

・共同研究　三菱電機（株）
検索可能暗号の研究開発
直接経費額　　1,818,182 円　間接経費額　181,818 円　合計　2,000,000 円

科研費基盤（C）「安全社会の獲得を目指した事故情報活用システムの機構」　(19510142)
平成21年度　143万円（直接110万円、間接33万円）
平成 19-21 年度　３年間合計額 455 万円（直接 350 万円、間接 105 万円）

５．今後の研究発展（外部への発信、外部資金獲得計画を含む）

・次世代暗号に関する研究を継続する
・The Japanese Honeynet Projectとしての活動を続け，国際的なセキュリティへの貢献を続ける.
・社会学的見地から信頼性と安全性に関する研究を進める.
・ホームページによるセキュリティ情報の発信を続け，国内のセキュリティへの貢献をする.

６．代表的なピアレビュー論文発表、学会プレナリ、招待講演発表、特許出願、受賞等

Yu Sasaki, Lei Wang, Kazuo Ohta and Noboru Kunihiro, "Extended Password Recovery Attacks against APOP, SIP, and Digest Authenticaiton," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E92-A, No. 1, pp. 96-104, 2009.
(基礎境界ソサイエティ論文賞)

(1) 坂東幸一，田中健次：「新聞報道による情報システム事故の信頼性・安全性の分 析」日本信頼性学会誌「信頼性」，Vol.31, No.6, pp.412-419 (2009)

(2) 稲葉 緑，田中健次：「高齢者に適した見落とし防止警報に関する実験的検討」，ヒューマンインタフェース学会論文誌，Vol.11, No.4, pp359-367 (2009)

(3) Inaba, M., Tanaka, K. :"Difference in effective feedback to improve risk understanding in driving between ages", Society for Judgment of Decision Making 30th Annual Conference, 5 (2009)

清野 祥之(電気通信大学　大学院情報システム学研究科), 小池 英樹, “マルウェア解析のための通信視覚化”情報処理学会コンピュータセキュリティシンポジウム, 2009.

窪田 幸, 小池 英樹, 安村 通晃, “パケットキャプチャによる画像の収集と表示手法の研究”, 情報処理学会コンピュータセキュリティシンポジウム, 2009.