平成１８年度研究ステーション研究成果報告書

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　情報システム学研究科 小池 英樹

２．平成１８年度の研究の特筆すべき成果

・次世代暗号研究において新聞雑誌等に数多く取り上げられた.
1. 2007年2月20日：フジサンケイビジネスアイ（第一面）「メルアド」知られない　匿名通信手法、電通大が開発
2. 2007年3月6日：フジサンケイビジネスアイ（第九面）電通大　認証処理時間１０分の１「使い捨てＩＤ」システムコスト低減
3. 2007年4月19日：読売新聞（第二面）メールのパスワード暗号破った -APOP規格解読方法発見-
4. 2007年5月22日発行：雑誌「日経NETWORK6月号」p.63 APOPのぜい弱性

・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１８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）

・　2007 年 2 月 27 日、ＩＳシンポジウム第 11 回信頼性 とシステム安全学を開催した。シンポジウムでは、データベースの信頼性から安全監視、使用性や心理的負荷まで広い観点から、安全、セキュリティ関係の研究発表があり、学内外から参加した研究者による討議が繰り広げられた。

・下記ホームページを通じて，世間の最新のセキュリティ情報を集めこれらをコンパクトにまとめた形式で社会への発信を毎日行っている．アクセスログによると日々，多数のアクセスが全国から行われている.
(http://www.csrs.is.uec.ac.jp:8080/~zetaka/Public/Sec/News/index.html)

４．外部資金の獲得状況

科学研究費補助金
・基盤研究(C)：最小ベクトル問題と格子アルゴリズムの公開鍵暗号への応用に関する研究（代表：太田和夫）130万

・若手研究(B)：双線形写像を用いた暗号プロトコルの提案（代表：國廣昇）120万
・特定領域研究(2)：量子論理回路の最適化に関する研究（代表：西野哲朗）研究分担者として参加
・基盤研究(B)：マルチユーザ情報理論と暗号理論のネットワーク符号化への展開（代表：小林 欣吾）研究分担者として参加

その他：
・電気通信普及財団：研究助成（太田和夫宛）110万円
・国際コミュニケーション基金　研究助成（國廣昇宛） 80万（平成17年度と合わせて）

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

N. Kunihiro W. Abe and K. Ohta, "Maurer-Yacobi ID based Key Distribution Revisited," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E89-A, No.5, pp. 1421-1424(2006)

S. Mukosaka, H. Koike, “Integrated Visualization System for Monitoring Security in Large-Scale Local Area Network”, Proc. on Asia-Pacific Symposium on Visualization, 2007.

他多数.