平成１７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 教授 小池 英樹

２．平成１７年度の研究の特筆すべき成果

・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として参加した．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，我が国からは本グループだけである．

・研究ステーションが協力し,大学院情報システム学研究科講義「情報セキュリティ」の授業を行った。これは、電気通信大学の教官と企業の研究者,技術者とが協力して、大学院学生を対象に、最新の研究トピックを教授するものである。科目等履修生約６０名の受講者があり、情報セキュリティのさまざまな側面についての実状が理解できたと好評であった。

・理系１００分野の大学学科・専攻ランキング「学問前線２００６」（河合塾編著）において，情報セキュリティ分野の研究者ランキングにおいて，国際的に活躍する研究者として選ばれた１３名に，本ステーションのメンバー４名（太田和夫教授，小池英樹教授，國廣昇助教授，吉浦裕教授）が選ばれた．ちなみに残りの 9 名の所属内訳は東京大（３名），横浜国立大（２名），九州大（１名），奈良先端大（１名），東京電機大（１名），静岡大（１名）であり，本学が最も多かった．

３．平成１７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）

・　2006 年 2 月 28 日、電気通信大学ＩＳシンポジウム第 10 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）

・ 特定領域研究：量子アルゴリズムに対する公開鍵及び秘密鍵暗号の安全性評価（代表者：太田）
・ 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する研究（代表者：太田）
・ 基盤研究(C)：（鈴木）
・ 基盤研究(C)：情報受信側の自主判断を促進する災害情報と判断評価のサポート機構（田中）
・ 特別研究員奨励費：（鈴木）

（研究助成）

・ NTT データ共同研究「安心と安全」（吉浦）
・ 国際コミュニケーション基金「安全な量子プロトコルの構築法に関する研究」（國廣）
・ 本田技研（鈴木）
・ NTT 環境エネルギー研究所「災害初動期から復興期にかけての防災情報共有に関する研究」（田中）
・ 船井電機「ホームネットワークセキュリティ」（小池）

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）

・ 量子暗号における公開鍵及び秘密鍵暗号の安全性評価を行う.
・ 電子透かしとその安全性に関する研究を進める.
・ 信頼性とシステム安全学の見地から人および社会とセキュリティに関する研究を進める.
・ The Japanese Honeynet Project の活動の一環として不正侵入検知および「おとりシステム」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続ける.

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

・Y. Komano, K. Ohta, A. Shimbo and S. Kawamura, "Toward the Fair Anonymous Signatures: Deniable Ring Signature," CT-RSA2006, pp. 174-191, 2006.
・Y. Komano, K. Ohta, A. Shimbo and S. Kawamura, "On the Security of Probabilistic Multisignature Schemes and their Optimality," MyCrypt2005, pp.132-150, 2005.
・H. Yoshiura, I. Echizen, "Maintaining Picture Quality and Improving Robustness of Color Watermarking by Using Human Vision Models", IEICE Trans. Information and Systems, Vol.E89-D, No.1, P.256-270
・ Yasuhiro Takahashi and Noboru Kunihiro : A quantum circuit for Shor's factoring algorithm using 2n+2 qubits, Quantum Information and Computation, Vol.6 No.2, pp.184-192, 2006.

・ Yasuhiro Takahashi and Noboru Kunihiro : A LINEAR-SIZE QUANTUM CIRCUIT FOR ADDITION WITH NO ANCILLARY QUBITS, Quantum Information and Computation, Vol.5 No.6, pp.440-448, 2005.

・ H.Koike, K.Ohno: Visualizing Cyber Attacks using IP Proc. Of Workshop on Visualization for Computer Security (VizSEC2005), IEEE Visualization 2005, IEEE/CS, 2005.

（招待講演）

・米山一樹, 國廣　昇, 太田和夫, 非線形ランプ型秘密分散法,電子情報通信学会2006年総合大会,

・國廣昇, 内藤祐介, 佐々木悠,ハッシュ関数に対する攻撃の最新動向,茨城大工学部, 2006年2月8日

・Suzuki, K. and Karim, M. R.(2005):Reliability Lifetimes Analysis Based on Warranty Data, The 2005 International Applied Reliability Symposium, Singapore. (Invited Talk)

・Suzuki, K. and Jin, L.(2005):Optimal Decision for Preventive Maintenance Using Multiple Reliability Information, Fourth International Symposium on Business and Industry Statistical, Palm Cove, Australia.
(Invited Talk)

・田中健次：「人間に依存する冗長化の落とし穴-効果的な冗長化は如何に実現で きるか-」, IEEE Reliability Society Tokyo Chapter 講演会 (2005.10).

・田中健次：「『危険を回避する仕組み』から『安全を創り出す人間』へ」品質月間特別講演会, 松江 (2005.11).