平成１９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１９年度の研究の特筆すべき成果

・新聞等報道
- 読売新聞朝刊　2007年4月19日（木）二面　メールのパスワード暗号破った

・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１９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）

・2008年２月２８日，ISシンポジウム第１２回「信頼性とシステム安全学」を開催した．(1)危機管理とヒューマンエラー，(2)トラブル未然防止，(3)運転支援技術，(4)意思とリスクコミュニケーション，の４部門において１１件の講演があり，学内外から81名の参加者があった．

４．外部資金の獲得状況

科学研究費補助金：
・基盤研究(C)：暗号プリミティブの安全性検証の自動化への展開（太田和夫） 130万円
・基盤研究(C)：トラブルの未然防止への情報獲得とその共有・活用に関する研究（鈴木和幸）　380万円
・基盤研究(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（田中健次）156万円

その他：
・東芝　　証明可能安全性を備えた暗号方式と証明自動化手法の開発（太田和夫） 99万円
・インフォクラフト 暗号分野に関する基礎研究 （太田和夫）　　42万円
・KDDI　　計算量的安全性を有する暗号プロトコルに関する研究（太田和夫）　200万円
・サイバー創研 MD5の安全性の限界に関する調査・研究（太田和夫）　　121万円
・NTT　　ハッシュ関数を用いたプロトコルの安全性評価（太田和夫）　　97.5万円
・東京電力株式会社　ヒューマンエラー事象分析に関する調査共同研究（鈴木和幸）2565.2万円

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

・Takashi Nishide and Kazuo Ohta, “Multiparty Computation for Interval, Equality, and Comparison without Bit-Decomposition Protocol,” in Proc. of PKC2007, LNCS4450, pp. 343-360, 2007.

・Lei Wang and Kazuo Ohta and Noboru Kunihiro, " New Key Recovery Attack on HMAC/NMAC-MD4 and NMAC-MD5," To appear in Eurocrypt2008.

・ Itoh, M., Sakami, D., Tanaka, K.："Risk Compensation due to Human Adaptation to Automation for System Safety", Tran. of the Society of Instrument and Control Engineers（計測自動制御学会論文集）, Vol.43, No.10, pp.926-934 (2007.10).

・ 坂東幸一，田中健次，川島 浩：「通信ネットワーク事故に関する新聞報道の分析 と評価」, 日本信頼性学会誌「信頼性」, Vol.29, No.7, pp.487-501 (2007.11)

・ 陸 偉，稲葉 緑，田中健次：「アリ型センサシステムによる局部集中監視の制御 に関する研究」, 計測自動制御学会システムインテグレーション部門講演会, pp.112(概要集）, CD-ROM (2007.12)

・渡邊 昌幸、安村 通晃、小池 英樹，ボットネットの特性解明に向けてのIDSルール作成とその検討，情報処理学会コンピュータセキュリティシンポジウム，2007.

・金子 博一、小池 英樹，GoogleMapsとGeoIPを用いた分散Honeypotのログ解析と視覚化，情報処理学会コンピュータセキュリティシンポジウム，2007.

他多数