平成２４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　情報メディアシステム学専攻　教授 小池英樹

２．平成２４年度の研究の特筆すべき成果

・ 認証ICチップの安全性を実証した.
・ Social Network Service上での安全性を高めるシステムを開発した.
・ 似顔絵認証や同時押し認証など，新しい認証方式を提案した.
・ 金融システム事故を例に，新聞報道のあり方を分析した.
・ 匿名通信Torネットワークにおける中継ノード選択方式を提案した.
・ 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.
・ 政府関連の会議に委員として参加し，我が国のセキュリティ対策への貢献を行った．具体的には以下のとおり.
  ・ 経済産業省「コンピュータセキュリティ早期警戒態勢整備委員会」
  ・ 経済産業省「新世代情報セキュリティ対策委員会」

３．平成２４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１７回「信頼性とシステム安全学シンポジウム」，平成２５年２月２８日，参加者数６６名
・ 日経産業新聞（1 月 16 日、6 面）「情通機構など　物理的特性使い　IC チップ暗号化」
・ 化学工業日報（1月16日、8面）「M2M用暗号・認証ICチップの安全性実証　NICTなど 実装コストも削減」

４．外部資金の獲得状況
・ 科研（Ｂ）[代表]180＋54万円「グレイゾーンでの判断能力を目指したリスクマネジメント論の体系化」

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）
・ 各種暗号方式の安全性評価を行う.
・ ソーシャルメディアセキュリティの研究を進める.
・ 標的型攻撃のような、人為的なミスを検知するための方式の開発を始める.
・ 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.

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
・ International Workshop on Security (IWSEC)にてBest Paper Award受賞.

（受賞論文）Yu Sasaki, Lei Wang, Yasuhiro Takasaki, Kazuo Sakiyama, and Kazuo Ohta, “Boomerang Distinguishers for Full HAS-160 Compression Function” International Workshop on Security (IWSEC).

- Shugo Mikami, Hirotaka Yoshida, Dai Watanabe, Kazuo Sakiyama, “Correlation Power Analysis and Countermeasure on the Stream Cipher Enocoro-128v2,” IEICE Trans. Fundam. Electron. Commun. Comput. Sci.,Vol.96-A, No.3, pp.697-704, (Mar., 2013).
- Yang Li, Kazuo Ohta, and Kazuo Sakiyama, “A New Type of Fault-Based Attack: Fault Behavior Analysis,” IEICE Trans. Fundam. Electron. Commun. Comput. Sci., Vol.A96-A, No.1, pp.177-184, (Jan., 2013).
- Midori Hirose, Akira Utsumi, Hiroshi Yoshiura: A Private Information Detector for Controlling Circulation of Private Information through Social Networks, 2nd International Workshop on Resilience and IT-Risk in Social Infrastructures (RISI 2012),Prague, Czech, Aug. 2012.
- Tomotaka Okuno, Hiroshi Yoshiura: Identifying Anonymous Posts of Job Seekers, 21st USENIX Security Symposium (USENIX Security '12), Bellevue, US, Aug. 2012, poster session.
- Yutaka Nishiwaki, Hiroshi Yoshiura: Virtualizing Secret-Shared Database System, 21st USENIX Security Symposium (USENIX Security '12), Bellevue, US, Aug. 2012, poster session.
- Naoto Kiribuchi, Ryo Kato, Takashi Nishide, Tsukasa Endo, Hiroshi Yoshiura: Batch Logical Protocols for Efficient Multi-party Computation, IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E95-A, No.10, pp.1718-1728,Oct. 2012.
- Naoto Kiribuchi, Ryo Kato, Takashi Nishide, Tsukasa Endo, Hiroshi Yoshiura: Reducing Communication Complexity of Random Number Bitwise-Sharing for Efficient Multi-party Computation, Journal of Information Processing, Vol.20, No.4, pp.861-870, Aug. 2012.
- 益尾文里、高田哲司: "似顔絵認証: 情報認知の個人差を用いた記憶照合型個人認証への推測攻撃に対する安全性向上策の提案", コンピュータセキュリティシンポジウム2012 (CSS 2012), 情報処理学会コンピュータセキュリティ研究会, in CD-ROM, Nov. 2012
- 国分佑樹、高田哲司:"同時押し認証: 暗証番号認証の改善を目指した一つの試み", マルチメディア, 分散、協調とモバイルシンポジウム (DICOMO 2012), 情報処理学会, pp.197-204, July 2012
- Timothy Girry Kale・Satoshi Ohzahata・Toshihiko Kato, A Performance Enhancement Method of Tor Circuit by Employing Flags Selection on Cooperative Relays, 信学技報, vol. 112, no. 307, IN2012-118, pp. 45-50, 2012.
- 坂東幸一, 田中健次：「新聞報道は事故をどう報じているか−金融情報システム事故を例にとって」日本信頼性学会誌, Vol.34, No.6, pp.416-423, 2012.