平成２３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２３年度の研究の特筆すべき成果

・ 本研究では、日本で多くのユーザを獲得しているWinnyを対象とし、ファイル流通制御を実現する方式を開発した.
・ 安定・高速なノードを優先して選び、かつ、ネットワーク的な地理的を考慮することにより、スループットの改善をする方式を提案した.
・ 人間の作業や人間エラーを防ぐための安全対策に潜む落とし穴を明らかにし、それを防ぐためのトータルセキュリティ（セーフティ）のあり方、マネジメントについて研究した。特に、人間エラーが発生しやすいグレイゾーンを考慮した、安全保証と危険回避の使い分けに関する研究では、シンポジウムでの発表に対して、第41回信頼性・保全性シンポジウム特別賞の受賞が決まっている.
・ インターネットコンテンツからの個人情報の漏洩検知と防止技術，データベース保護技術，Webサイト成り済まし検知技術について研究を行った.
・ 利便性と安全性のより良いバランスを目指した個人認証技術について研究を行った.
・ 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.
・ 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」
  ・ 経済産業省「ボット対策委員会」

３．平成２３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１６回「信頼性とシステム安全学シンポジウム」，平成２４年２月２８日
参加者数８１名，発表件数１１件

４．外部資金の獲得状況
・ 科研費(基盤C)「プライバシー保護のための個人情報の検知および照合技術の研究」
・ 奨学寄付：柏森財団 「情報の活用と保護を両立する秘匿計算技術の研究 」
・ 科研費(基盤B):「グレイゾーンでの判断能力向上を目指したリスクマネジメ ント論の体系化」
・ 科研費(基盤A)：「次世代品質・信頼性情報システムの研究と開発」

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）

- データベースセキュリティと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.
- 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.

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

- 平成22年度情報処理学会論文賞（平成23年6月受賞）
- 平成22年度日本・セキュリティマネジメント学会論文賞（平成23年6月受賞）
- 第41回信頼性・保全性シンポジウム特別賞受賞

- T. Yamada, I. Echizen, H. Yoshiura: PC-based Real-time Video Watermark Embedding System Independent of Platform for Parallel Computing, LNCS Trans. on Data Hiding and Multimedia Security, LNCS 7110, pp.15-33. Nov. 2011.
- 加藤慧，小宮山功一朗，瀬古敏智，一瀬友祐，河野耕平，中山心太，吉浦裕：コンテンツベースフィッシング検知手法大規模実例評価と改良，日本セキュリティマネジメント学会誌，Vol.25, No.2, pp.42-56, 2011年9月.
- N. Kiribuchi, T. Nishide, T. Endo, H. Yoshiura: Accelerating Multiparty Computation by Efficient Random Number Bitwise-Sharing Protocols, Proc. of the 12th Intl. Workshop on Information Security Applications (WISA2011), LNCS 7115, pp.187-020, 2011.
- N. Kiribuchi, R. Kato, T. Nishide, H. Yoshiura: Batching Multiple Protocols to Improve Efficiency of Multi-party Computation, Proc. of the 7th Intl. Conf. on Information Security and Cryptology (Inscrypt'2011), 2011.
- 中澤　大暁，吉田 雅裕，大坐畠 智，中尾 彰宏，川島 幸之助，Winnyネットワークにおける検索クエリの遮断によるファイル流通制御方式,電子情報通信学会　和文論文誌Ｂ，Vol. 95-B, No. 5, pp. 636-648, 2012. （ネットワークシステム研究会推薦論文）
- T. Kale, S. Ohzahata, T. Kato, Improving Tor Circuit Performance with Guard Relay Nodes,IEICE 総合大会，BS-3-14, 2012.
- 稲葉緑，田中健次: 「水害時の避難へのモチベーションに影響を及ぼす情報提 示内容についての実験的検討」，日本災害情報学会誌 災害情報，No.10, 127-136 (2011.4)
- 田中健次:「安全保証と危険回避の使い分けに関する一考察　–使用説明書と警 告表示のあり方–」第41回信頼性・保全性シンポジウム発表報文集，JUSE，pp.373-378 (2011.7)　（第41回信頼性・保全性シンポジウム特別賞受賞）
- 稲葉 緑，田中健次，宇佐美 稔，戸塚康男：「医療現場での作業中断によるヒ ューマンエラーの分類と要因」医療の質・安全学会誌，Vol.6, No.3, pp.313-331 (2011.9).
- Bando,K., Tanaka K. :″ Trend Analysis of Accidents and Dependability Improvement in Financial Information Systems,″ 17th IEEE Pacific Rim International Symposium on Dependable Computing, California, pp.234-243 (2011.12).