平成20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20年度の研究の特筆すべき成果

・新聞報道
　日本看護協会の事故事例分析検討委員会に依頼された．アラーム情報事故解析を，大学院前期課程学生と共に進めた．その途中結果が，読売新聞の第一面(2009.3.19)で取り上げられた．

・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20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２7日，ISシンポジウム第１３回「信頼性とシステム安全学」を開催した．（発表件数１２件，参加者７０名）

４．外部資金の獲得状況

太田：
・科学研究補助金　基盤C　19500009　直接経費1,100,000円　間接経費330,000円
・産学連携研究経費　（株）東芝　直接経費900,000円　間接経費90,000円
・　〃　日本電信電話（株）　直接経費750,000円　間接経費225,000円
・　〃　三菱電機（株）　直接経費909,091円　間接経費90,909円
・　〃　（株）インフォクラフト　直接経費900,000円　間接経費160,000円
・奨学寄付金　（株）日立製作所システム開発研究所　寄付申請額600,000円　共通経費60,000円

田中：
・科学研究費補助金　基盤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」，156万円（直接120万円，間接36万円）

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

学術論文

Takashi Nishide, Kazuki Yoneyama, Kazuo Ohta, "Attribute-Based Encryption with Partially Hidden Ciphertext Policies" IEICE Trans. on Fundamentals, vol.E92.A, No.1, pp.22-32, Jan. 2009.

Bagus Santoso and Kazuo Ohta, "A New 'On the Fly' Identification Scheme: A Trade-off of Asymptoticity between ZK and Correctness," IEICE Transactions on Fundamentals of Electronics, Communications and
Computer Sciences, Vol. E92-A, No.1, pp.122-136, 2009.

Yu Sasaki, Lei Wang, Kazuo Ohta and Noboru Kunihiro, "Extended Password Recovery Attacks against APOP, SIP, and Digest Authenticaiton," IEICE Transactions on Fundamentals of Electronics, Communications
and Computer Sciences, Vol.E92-A, No. 1, pp. 96-104, 2009.

Lei Wang, Kazuo Ohta and Noboru Kunihiro, "Near-Collision Attacks on MD4: Applied to MD4-Based Protocols," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences,
Vol.E92-A, No.1, pp. 76-86, 2009.

Masami Izumi, Kazuo Sakiyama, Kazuo Ohta, "A New Approach for Implementing the MPL Method toward Higher SPA Resistance," in Proc. of The Forth International Conference on Availability, Reliability and
Security (AReS 2009), IEEE Computer Society, pp.181-186, March, 2009.

Kazuki Yoneyama, Satoshi Miyagawa, Kazuo Ohta, "Leaky Random Oracle", International Conference on Provable Security (ProvSec2008), LNCS5324, pp.226-240, 2008.

Yu Sasaki, Lei Wang, Kazuo Ohta, and Noboru Kunihiro, "Security of MD5 Challenge and Response: Extension of APOP Password Recovery Attack", CT-RSA2008, LNCS vol. 4964, pp. 1-18, 2008.

Kouichi Itoh, Noboru Kunihiro, and Kaoru Kurosawa, "Small Secret Key Attack on a variant of RSA (due to Takagi)," in Proc. of CT-RSA2008 LNCS4964, pp. 387-406, 2008.
Lei Wang, Kazuo Ohta, and Noboru Kunihiro, "New Key Recovery Attack on HMAC/NMAC-MD4 and NMAC-MD5," Eurocrypt2008, LNCS vol. 4965, pp. 27-253, 2008

坂東幸一，田中健次：「金融情報システム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.31, No.1, pp.77-91 (2009.1)

Bando, K., Tanaka, K.："Analysis on Trend of Accidents in Financial Information Sysmtes Reported by Newspapers from the Viewpoint of Dependability", Proc of the 7th Asian Test

Symposium，pp.440-450 (2008.11).

田中健次，伊藤 誠：「信頼性・安全性確保のためのユーザと企業の情報共有と活用」，日本品質管理学会誌「品質」，Vol.38, No.4, pp.41-47 (2008.12)

人間によるHoneypot の攻撃元ログ調査を支援するUser Interface の提案, マルウェア対策研究人材育成ワークショップ 2008(MWS2008)，２００８．

今澤貴夫，小池英樹，高田哲司，GPSデータを用いた位置認証システムとその停留点算出方式，情報処理学会コンピュータセキュリティシンポジウム(CSS2008) , 2008.

招待講演

太田和夫，川合豊，"暗号系の安全性証明不可能性の統一的アプローチを目指して--設計ゴール，攻撃シナリオ，数論仮定のトレードオフ--, " 第3回公開鍵暗号の安全な構成とその応用ワークショップ. [東京にて2009年3月23
日]

田中健次，「いかに防ぐか！ヒューマンエラーとコミュニケーションエラー」，徳島看護協会研修会招待講演(2008.9).

田中健次，「ヒューマン・エラーとコミュニケーション・エラー如何に防ぐか」，武蔵野赤十字病院講演会 (2008.11).

書籍

Michael Sipser （著），太田和夫，田中圭介 （監訳）．阿部正幸，植田広樹，藤岡淳，渡辺治（訳）．計算理論の基礎（原著第2版）
１オートマトンと言語．共立出版，2008/05.

Michael Sipser （著）．太田和夫，田中圭介 （監訳）．阿部正幸，植田広樹，藤岡淳，渡辺治（訳）．計算理論の基礎（原著第2版）
２計算可能性の理論．共立出版，2008/05.

Michael Sipser （著）．太田和夫，田中圭介 （監訳）．阿部正幸，植田広樹，藤岡淳，渡辺治（訳）．計算理論の基礎（原著第2版）
３複雑さの理論．共立出版，2008/05.

受賞

太田和夫，IPA賞（情報セキュリティ部門）http://www.ipa.go.jp/about/press/20080516.html

特許

H20年度
【整理番号】08-028JP00
【出願番号】特願2008-289266
【出願日】2008/11/11
【発明の名称】本人確認システム
【発明者】Bagus Santoso(院生(D4)), 〓山一男准教授, 太田和夫教授

【整理番号】08-046JP00
【出願番号】特願2009-008609
【出願日】2009/01/19
【発明の名称】データ格納システム及び情報送信装置及びサーバ装置
【発明者】伊藤　隆(三菱電機), 北原恵介(院生(M2)), 坂井祐介(学生(4)), 太田和夫教授

以上.