平成２９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
研究代表者名（所属部局・職・氏名）　情報学専攻　准教授　高田哲司

２．研究組織(今年度関わった全ての構成員を記してください。)

＜学内構成員＞

電気通信大学　大学院情報理工学研究科　情報学専攻　教授 太田和夫
電気通信大学　大学院情報理工学研究科　情報学専攻　教授 田中健次
電気通信大学　大学院情報理工学研究科　情報学専攻　教授 崎山一男
電気通信大学　大学院情報理工学研究科　情報学専攻　准教授 大座畠智
電気通信大学　大学院情報理工学研究科　情報学専攻　准教授 岩本貢
電気通信大学　大学院情報理工学研究科　情報学専攻　准教授 岩崎敦
電気通信大学　大学院情報理工学研究科　情報学専攻　准教授 高田哲司
電気通信大学　大学院情報理工学研究科　情報学専攻　特別研究員 渡邉洋平

＜学外構成員＞

東京工業大学　大学院情報理工学院　情報工学系　教授 小池英樹

３．平成２９年度の研究の特筆すべき成果
（研究の主な成果、得られた成果の国内外における位置づけとインパクトなどの点から記述すること）

（１）本ステーションのメンバーである太田教授が，電子情報通信学会のフェロー称号を授与されました．詳細は，以下の Web ページに記載されています
- http://www.ieice.org/jpn/fellow/ichiran29.html

（２）著名 International Journal に論文が掲載されました
情報通信理論分野で最もレベルの高い論文誌である，IEEE Trans. Information Theory に，本ステーションのメンバである岩本准教授，太田教授が執筆した論文「Security Formalizations and Their Relationships for Encryption and Key Agreement in Information-Theoretic Cryptography」(横浜国立大学，四方順司教授との共著)が掲載されました．本論文では，秘密鍵暗号と鍵共有を対象として，情報理論的安全性概念の相互関係を明らかにしました．情報理論的暗号と計算量的暗号の関係も明らかにしており，当該分野における基礎的かつ重要な成果と考えます．
- https://ieeexplore.ieee.org/document/8017625/

（3）主だった研究成果について

「スマートコントラクトを用いた安全で高速なトランザクション確定方式」（大座畠准教授）

分散アプリケーションプラットフォームである Ethereum では、ブロックチェーンにコントラクトと呼ばれるスクリプト群を格納し、自動的に実行することができるスマートコントラクトという仕組みを提供することで、今まで集中管理が必要だったサービスを分散的にすることができるということで注目を集めている。また、スマートコントラクトでは、スクリプトの実行結果もブロックチェーンに格納することができるため、仮想通貨の取引履歴のみならず、様々なものを記録することができる。しかし、Ethereum で、実際の物が介在する取引をする場合、記録されたものが実際に送られ、正しく受け取ることができているのかを確認することができない。そこで、本研究では、実際の物をやりとりする場合、供給側が「提供量」を、需要側は「受け取った量」をブロックチェーンに書き込み、取引に不整合がないかを確認する方式を提案し、実装評価を行った。

「心理的効果の応用によるセキュリティ警告効果の改善の試み」（高田准教授）

セキュリティ警告の効果を阻害する原因の 1 つに馴化がある.この阻害要因を抑制する取り組みが 研究されているが，警告への注目を回復させるにとどまり，その後の対応行動までは考慮されていない．そこで本研究では，セキュリティ警告に「かわいさ」に基づく視聴覚効果を付与することで，馴化の抑制 と安全行動への誘導を試みた.被験者実験の結果，提案する刺激方法に基づく警告は既存警告と比較して 統計的に有意な改善をもたらし，馴化を抑制する効果を発揮しうる可能性が示された.この結果をふまえ， セキュリティ警告における馴化抑制と安全行動への誘導の 2 点について，今後の展望と残されている課題 について議論し，学会にて発表を行った．その結果，ユニークな視点による研究として「CSS2017 コンセプト論文賞」を受賞した.

４．平成２９年度の研究成果の公表実績
（主催した研究会・シンポジウム、研究成果の発信状況等）

特になし

５．外部資金の獲得状況
（種別・種目・相手機関（企業）・研究題目・代表者名・直接経費額・間接経費額）

(1) 科研費（基盤研究（Ａ））「レーザーフォールト攻撃による情報漏洩を防ぐ耐タンパー技術の総合的研究」研究代表者：崎山一男　直接経費 ：7,100 千円、間接経費 ：2,130 千円
(2) 科研費（基盤研究(B)）「推測秘匿性に基づく情報理論的暗号理論の新展開」研究代表者：岩本貢，分担者：渡邉洋平 直接経費 ： 3,800 千円、間接経費 ： 1,140 千円

(3) 科研費（基盤研究(A)）「リスクモードとオンラインモニタリング技術高度化に着目した未然防止体系の新展開」研究代表者:鈴木和幸, 分担者 田中健次 直接経費分担額:300千円

(4) 科研費（基盤研究(B)）「ゲーム理論的資源配分メカニズムの定量的評価基盤の構築」研究代表者：岩崎敦 直接経費：4,700千円

(5) 科研費（基盤研究(B)）「情報理論的暗号理論における統一的パラダイムの構築とその応用」, 研究代表者:四方順司(横浜国立大学), 分担者:岩本貢, 直接経費: 1,400千円, 間接経費:420千円.

(6) 科研費（若手(B)）「鍵漏洩に耐性のあるID ベース暗号の高安全かつ高効率な実現」研究代表者:渡邉洋平, 直接経費 ： 900千円、間接経費 ： 270千円

(7) 特別研究員奨励費 「秘匿情報に対して動的アクセス制御とデータ解析を両立する暗号理論の確立」特別研究員：渡邉洋平, 直接経費 ： 800千円、間接経費 ： 240千円

(8) 国際共同研究加速基金（国際共同研究強化）研究題目「不完全情報下における動学ゲームの計量経済学的推定技術の設計・評価」, 研究代表者：岩崎敦, 直接経費：10,800千円.

(9) 寄付金 公益財団法人 大川情報通信基金 2017年度研究助成 研究題目「ブロックチェーンにおける安全で高速なトランザクション確定方式」 研究代表者 大坐畠智 直接経費 100万円

６．今後の研究発展
（外部への発信、外部資金獲得計画を含む）

継続して外部研究予算の獲得を目指す

７．発表論文等（各項目ごとに記載してください。）
「雑誌論文」：著者名・論文標題・雑誌名・査読の有無・巻・発行年(西暦)及びページ

M. Iwamoto, K. Ohta, and J. Shikata, “Security Formalizations and Their Relationships for Encryption and Key Agreement in Information-Theoretic Cryptography,” IEEE Trans. Information Theory, 査読あり, vol. 64, issue 1, pp. 654–685, 2018

R. Yashiro, T. Sugawara, M. Iwamoto, and K. Sakiyama, “Q-class Authentication System for Double Arbiter PUF,” IEICE Trans. on Fundamentals, 査読あり, vol.E101–A, no.1, pp. 129–137, Jan., 2018.

Y. Watanabe and J. Shikata, “Timed-Release Computational Secret Sharing and Threshold Encryption,” Designs, Codes and Cryptography, 査読あり, vol.3(1), pp.17–54, Springer, 2018.

Ryoji Kurata, Naoto Hamada, Atsushi Iwasaki, Makoto Yokoo: Controlled School Choice with Soft Bounds and Overlapping Types. J. Artif. Intell. 査読あり, Res. 58: 153-184 (2017)

Risa Yashiro, Takeshi Sugawara, Mitsugu Iwamoto, and Kazuo Sakiyama, “Q-class Authentication System for Double Arbiter PUF,” IEICE Trans. Fundam. Electron. Commun. Comput. Sci., 査読あり, Vol.E101-A, No.1, pp.129-137, (Jan., 2018).

荻野貴大、高田哲司:″悪性コンテンツの隠蔽方法に着目したマルウェア感染への誘導用 Web ページ検知システムの提案″, 情報処理学会論文誌, 査読あり, Vol.58, No.12, pp.1833−1842, 情報処理学会, 2017.

「学会発表」：発表者（代表）名・発表標題・学会等名・発表年月日・発表場所

T. Nakai, S. Shirouchi, M. Iwamoto and K. Ohta, “Four cards are enough for card-based three-input voting protocol utilizing private permutations,” ICITS2017 (conference track), LNCS 10681, pp.153–165, Springer, Nov.-Dec., 2017. Hong Kong.

Y. Watanabe, “Broadcast Encryption with Guessing Secrecy,” In: ICITS 2017 (conference track), LNCS 10681, pp.39–57, Springer, Nov.-Dec., 2017. Hong Kong

A. Takayasu and Y. Watanabe, “Lattice-based Revocable Identity-based Encryption with Bounded Decryption Key Exposure Resistance,” In: ACISP 2017, Part I, LNCS 10342, pp.184–204, Springer, July, 2017. Auckland, New Zealand.

Kohei Matsuda, Tatsuya Fujii, Natsu Shoji, Takeshi Sugawara, Kazuo Sakiyama, Yu-ichi Hayashi, Makoto Nagata, and Noriyuki Miura, “A 286F^2/Cell Distributed Bulk-Current Sensor and Secure Flush Code Eraser Against Laser Fault Injection Attack,” Dig. Tech. Papers, 2018 IEEE Intl. Solid-State Circuits Conference (ISSCC’18), IEEE, #21.5, pp.352-354, (Feb. 2018), San Francisco, USA

Takeshi Sugawara, Natsu Shoji, Kazuo Sakiyama, Kohei Matsuda, Noriyuki Miura, and Makoto Nagata, “Exploiting Bitflip Detector for Non-Invasive Probing and its Application to Ineffective Fault Analysis,” In Proc. Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC’17), IEEE, pp.49-56, (Sep., 2017), Taipei, Taiwan.

Natsu Shoji, Ryuga Matsumura, Takeshi Sugawara, and Kazuo Sakiyama, “An Evaluation of Ineffective Fault Analysis on AES using Single-Bit Bit-Set/Reset Faults,” Poster Session,

IWSEC2017 (Aug., 2017), Hiroshima, Japan.

Ishigaki Y., Matsuno Y., Tanaka K. : "Agile way of Risk Awareness by Smartphone-connected Environmental Sensors," 14th Inter. Conference on Information Systems for Crisis Response and Management (ISCRAM) (May, 2017). Albi, Occitanie Pyrénées-Méditerranée, France.

Matsuno Y, Ishigaki Y, Tanaka K.,: "Models of Consensus Building among Citizens and Professionals in SNS," 14th Inter. Conference on Information Systems for Crisis Response and Management (ISCRAM) (May, 2017). Albi, Occitanie Pyrénées-Méditerranée, France.

Ishigaki Y., Tanaka K. Pradana A. H., Matsumoto Y., Maruo Y. : "Citizen Sensing for Environmental Risk Communication- Action Research on PM2.5 Air Quality Monitoring in East Asia - " The 2nd International Conference on Cyber-Technologies and Cyber-Systems (CYBER 2017).November, 2017. Barcelona, Spain.

Fuuki Shigenaka, Tadashi Sekiguchi, Atsushi Iwasaki, Makoto Yokoo: Achieving Sustainable Cooperation in Generalized Prisoner's Dilemma with Observation Errors. AAAI 2017: 677-683, Feb., 2017. San Francisco, USA.

Yasushi Kawase, Atsushi Iwasaki: Near-Feasible Stable Matchings with Budget Constraints. IJCAI 2017: 242-248, Aug. 2017. Melbourne, Australia.

Tetsuji Takada: " Authentication Shutter: Alternative Countermeasure against Password Reuse Attack by Availability Control ", 12th Int'l Workshop on Frontiers in Availability, Reliability and Security (FARES 2017) in conjunction with ARES 2017, Aug. 2017, Reggio di Calabria, Italy,

Ryo Minakawa, Tetsuji Takada: "Exploring Alternative Security Warning Dialog for Attracting User Attention: Evaluation of "Kawaii" effect and its Additional Stimulus Combination",Emerging Research Projects and Show Cases (SHOW 2017), in conjunction with iiWAS 2017, Dec. 2017. Salzburg, Austria.

鈴木慎之介, 渡邉洋平, 岩本貢, 太田和夫, “ロバスト秘密分散法 CFOR 方式における精密な安全性解析,” 暗号と情報セキュリティシンポジウム 2018 (SCIS 2018), 2A3-3, Jan., 2018. 新潟県

駒野雄一, 岩本貢, 太田和夫, 崎山一男, “PUF 応用に向けた新たな物理仮定と端末認証方式への応用,” 暗号と情報セキュリティシンポジウム 2018(SCIS2018), 2D1-1, Jan., 2018. 新潟県

渡邉洋平, “SXDH 仮定に基づく短いパラメータ長を達成する放送型暗号,” 暗号と情報セキュリ

ティシンポジウム 2018 (SCIS 2018), 3A3-3, Jan., 2018. 新潟県

黒木慶久, 古賀優太, 渡邉洋平, 岩本貢, 太田和夫, “3 枚のカードで実現可能な 3 入力多数決プロトコル,” 暗号と情報セキュリティシンポジウム 2018 (SCIS 2018), 3B1-4, Jan., 2018. 新潟県

古賀優太, 鈴木慎之介, 渡邉洋平, 岩本貢, 太田和夫, “カードを用いた複数人でのマッチングプロトコル,” 暗号と情報セキュリティシンポジウム 2018 (SCIS 2018), 3B1-5, Jan., 2018. 新潟県

早坂健一郎, 川合豊, 小関義博, 平野貴人, 岩本貢, 太田和夫, “マルチユーザで利用可能な共通鍵型秘匿検索に向けて,” 暗号と情報セキュリティシンポジウム 2018(SCIS2018), 3C2-1, Jan., 2018. 新潟県

野島拓也, 渡邉洋平, 岩本貢, 太田和夫, “ダミーエントリの作成方法に着目した共通鍵検索可能暗号 CGKO 方式の改良,” 暗号と情報セキュリティシンポジウム 2018 (SCIS 2018), 3C2-2, Jan., 2018. 新潟県

松崎なつめ, 穴田啓晃, 金岡晃, 渡邉洋平, “鍵更新機能付き検索可能暗号の一般的構成,” 暗号と情報セキュリティシンポジウム 2018 (SCIS 2018), 4A2-6, Jan., 2018. 新潟県

松原祐衣子, 宮元冬景, 菅原健, 崎山一男, “C66x DSP におけるペアリングの高速実装,” 2018 年暗号と情報セキュリティシンポジウム (SCIS2018), 2D4-4, 5 pages, (Jan., 2018), 新潟県

松村竜我, 菅原健, 崎山一男, “光に重畳したサイドチャネル情報に関する基礎的な解析,” 2018 年暗号と情報セキュリティシンポジウム (SCIS2018), 3D2-3, 6 pages, (Jan., 2018), 新潟県

辰巳恵里奈, 菅原健, 崎山一男, “デバイスドライバを用いた Row Hammer のテストツール,” 2018 年暗号と情報セキュリティシンポジウム (SCIS2018), 3D3-2, 5 pages, (Jan., 2018), 新潟県

菅原健, 崎山一男, 梨本翔永, 鈴木大輔, 永塚智之, “パブリッククラウド上の FPGA における悪性ハードウェア,” 2018 年暗号と情報セキュリティシンポジウム (SCIS2018), 3D3-4, 8 pages, (Jan., 2018), 新潟県

菅原健, 庄司奈津, 崎山一男, 松田航平, 三浦典之, 永田真, “フォルト検出センサを悪用した非侵襲プロービング攻撃,” 2018 年暗号と情報セキュリティシンポジウム (SCIS2018), 3D3-6, 3 pages, (Jan., 2018), 新潟県

庄司奈津, 菅原健, 岩本貢, 崎山一男, “ブロック暗号へのプロービング攻撃における鍵復元効率の正確な評価モデル,” 2018 年暗号と情報セキュリティシンポジウム (SCIS2018), 3D3-5, 8 pages, (Jan., 2018), 新潟県

梨本翔永, 鈴木大輔, 菅原健, 崎山一男, “センサフュージョンの攻撃耐性に関するセキュリティ評価,” 2018 年暗号と情報セキュリティシンポジウム (SCIS2018), 3D4-1, 8 pages, (Jan., 2018), 新潟県

小堀 輝, 大坐畠 智, 山本 嶺, 加藤聰彦, ”スマートコントラクトを用いた実際のやりとりを相互に確認する方式の検討”, 電子情報通信学会 総合大会, March, 2018, 東京都.

今田 寛, 大坐畠 智, 加藤 聰彦, “プロセス間通信と端末間通信の把握による踏み台追跡”, 情報処理学会、2017-SPT-23, May, 2017, 東京都.

中西建登, 大坐畠 智, 加藤聰彦, “Bitcoin における安全な決済確定高速化手法の検討”, 信学技報, vol. 117, no. 3, NS2017-3, pp. 13-18, April, 2017. 富山県

山岸 伶, 高田 哲司: ″私的な連想情報の再認による個人認証と安全性評価″, コンピュータセキュリティシンポジウム 2017 (CSS 2017), October, 2017, 山形県

皆川 諒, 高田 哲司: ″馴化を抑制しうる新たなセキュリティ警告の探求:かわいいとその付加刺激の効果に関する評価″,コンピュータセキュリティシンポジウム 2017 (CSS 2017), October, 2017, 山形県

服部夢二、 高田哲司: ″ 安全な秘密情報利用の動機付けを目的とした個人認証のゲーム化″, 第 80 回 CSEC 研究発表会, March, 2018, 東京都,

「招待講演発表」 : 発表者(代表)名・発表標題・学会等名・発表年月日・発表場所

M. Iwamoto, “Secret sharing schemes under guessing secrecy,” Cryptographic Technologies for Securing Network Storage and Their Mathematical Modeling, MI Lecture Notes, Kyushu University, June, 2017. 福岡県

岩本貢, “情報理論的安全性 −さまざまな視点から−,” 誤り訂正符号のワークショップ（入門講演）, September, 2017. 山口県

渡邊洋平, ” 情報理論的安全性に基づく放送型暗号 ～古典的結果と最近の進展～” 電子情報通信学会 情報理論研究会, 2017-09-IT, September, 2017. 山口県

「図書」 : 著者名・出版社名・書名・発行年(西暦)及び総ページ数(共著の場合、最初と最後のページを記載)

特になし

「受賞」：授与団体・受賞者(代表者)名・受賞標題・受賞年月日

(1) 授与団体：12th Int'l Workshop on Security (IWSEC 2017)，受賞者：庄司 奈津，受賞標題：「Best Poster Award」，受賞年月日：2018/09/01

(2) 授与団体：2017 年暗号と情報セキュリティシンポジウム（SCIS 2017），受賞者：粕谷桃伽，受賞標題：「SCIS 論文賞」，受賞年月日：2017/01/27

(3) 授与団体：サイバーセキュリティシンポジウム道後 2018，受賞者：庄司奈津、菅原健，岩本貢，崎山一男，受賞標題:「SEC 道後 2018 学生研究賞」，受賞年月日:2018/03/01

(4) 授与団体:コンピュータセキュリティシンポジウム 2017(CSS2017)，受賞者:皆川諒，受賞標題「CSS2017 コンセプト論文賞」，受賞年月日:2017/10/25

(5) 授与団体:コンピュータセキュリティシンポジウム 2017(CSS2017)，受賞者:山岸伶，受賞標題「CSS2017 学生論文賞」，受賞年月日:2017/10/25

「特許出願」：出願した特許の名称・発明者・権利者・種類・番号・出願年月日・国内外別

特になし

「その他」：ホームページ等

特になし