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．設置期間

２０１６年０４月０１日　～　２０２１年０３月３１日

３．研究組織(設置期間中かかわった、全ての構成員を記載してください。)

※所属機関・部局・職は現在のもの、もしくは離脱時のものを記して下さい。

＜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
（～2020 年 3 月 31 日）

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　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　大坐畠　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　岩崎 敦

電気通信大学　大学院情報理工学研究科　情報学専攻　助教　渡邉 洋平
（2016 年 4 月 1 日～2018 年 3 月 31 日，2020 年 4 月～）

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

＜学外構成員＞

東京工業大学　情報理工学院　情報工学系　教授　小池 英樹

４．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、今後の展望などの点から記述すること）

成果１）著名会議・論文誌での研究成果発表について

＊ 暗号理論に関するトップ国内会議である TCC (Theory of Cryptography Conference)に論文が採択された(太田教授，岩本准教授)．修士１年生が筆頭著者であることも特筆に値する．また本研究は，国内会議，研究会での受賞が2件，国際会議での best poster award が1件という成果となった．

＊ 崎山教授による研究で，レーザーフォールト攻撃に対して安全な暗号ハードウェアをセンサとの協調設計により実現し，個体素子のトップジャーナル IEEE Journal of Solid-State Circuits に論文が採択された

- https://ieeexplore.ieee.org/abstract/document/8474958

＊ 崎山教授の指導学生が「レーザー光を使った音情報の漏えいに対する安全性評価」の研究を電子情報通信学会ソサイエティ大会で講演し，学術奨励賞を受賞した

- https://www.uec.ac.jp/news/prize/2020/20200325_2475.html

＊ 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」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言える．

- https://ieeexplore.ieee.org/document/8017625/

成果２）

推測秘匿性と呼ばれる情報理論的な安全性概念は，平均推測秘匿性，最適推測秘匿性に大別される．岩本らは，暗号化がラテン方陣に従う場合に，最適推測秘匿性を満たす方式は完全秘匿（と平均推測秘匿性）を満たすことを示した．しかし，最適秘匿性を満たすが，完全秘匿性も平均秘匿性も満たさない情報理論的暗号方式が存在するかについては未解決であった．この問題を秘密分散法においてこのような非自明な最適推測安全性を満たす方式が構成できることを示した．推測秘匿性に関する理論研究としては重要な知見であると考えている．

成果３）

近年普及が進むクラウド環境において，ゲノム情報のような 100 年以上の長期的な安全性を必要とする情報をどう扱うべきか？という問題は重要な問題である．その問題に現代暗号理論の立場から取り組み，クラウドでの利用を想定した動的アクセス制御機能を有する放送型暗号を提案した．提案方式は情報理論的に安全であり，従って柔軟なアクセス制御機能を持ちつつも長期的な安全性を保証可能である．

成果４）

Tor ネットワークにおける通信品質改善と匿名性分析に関する研究：

通信の秘匿を提供するため P2P ネットワークを用いて匿名性を提供する Tor (The Onion Router) が普及している。しかし、Tor ネットワークでは、Onion Routing と通信経路を混ぜ合わせるため、通信のスループットが出ない問題がある。本研究では、通信経路を分散させることにより、輻輳を回

避する方式を提案し、Tor ネットワークエミュレータで評価をすることでその有効性を明らかにした。さらに Tor ネットワークの匿名性に対する攻撃手法を明らかにし、その分析を行った.

成果５）

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:

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.その結果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を示した．本研究は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.

５．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）

構成員の研究成果は国内外の学術会議で発表されている．詳細については「発表論文」を参照頂きたい．ここではそれ以外の公表実績について述べる.

ワークショップ開催：システム安全学ワークショップ
日付：２０１７年０３月０１日
場所： 電気通信大学　西１０号館２階大会議室
内容： ８件の発表とプロジェクト報告，２件の招待講演

研究会主催開催：Workshop on Cryptography Using Physical Tools,
日時：２０１９年１２月１９日
場所：電気通信大学 東３号館 306 室
世話人：岩本准教授，渡邉助教

６．外部資金の獲得状況

（代表的な資金獲得１０件以内）

1. 科研費（基盤研究(Ｓ)）日本学術振興会
「暗号技術による IoT エコシステムのレジリエンス向上」
代表者：崎山一男，分担者：太田和夫，岩本貢，渡邉洋平　直接経費 149500 千円・間接経費 44850 千円

2. 科研費（基盤研究（Ａ））日本学術振興会
「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」
代表者：崎山一男　直接経費 30100 千円・間接経費 9030 千円
3. 科研費（基盤研究(Ａ)）日本学術振興会
「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」代表者：鈴木和幸 分担者：田中健次 直接経費 30200 千円・間接経費 9060 千円
4. 科研費（基盤研究(Ｂ)）日本学術振興会
「想定外事象を想定した従来手法とノンテクスキルとの融合型高信頼性・安全性方法論」
代表者：田中健次 直接経費 7600 千円・間接経費 2280 千円
5. 科研費（基盤研究(Ｂ)）日本学術振興会
「推測秘匿性に基づく情報理論的暗号理論の新展開」
代表者：岩本貢 分担者：渡邉洋平　直接経費 14100 千円・間接経費 4230 千円
6. 科研費（基盤研究（B））日本学術振興会
「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」
代表者：岩崎敦　直接経費 13300 千円・間接経費 3990 千円
7. 国際共同研究加速基金（国際共同研究強化）日本学術振興会
「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」
代表者：岩崎敦，直接経費 10,800 千円・間接経費 3240 千円
8. 公益財団法人 大川情報通信基金 2017 年度研究助成
「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」
代表者：大坐畠智　直接経費 100 万円
9. 共同研究 三菱電機（株）
「秘匿検索暗号の理論研究」
代表者：太田和夫，直接経費 455 千円・間接経費 45 千円
10. 共同研究　トヨタ IT 開発センター
「V2X システムにおける過信に配慮した情報提示方法の検討・評価」
代表者：田中健次，直接経費 1,324 千円・間接経費 132 千円

７．発表論文等（各項目とも、代表的な５件以内）
「雑誌論文」：
Ryoji Kurata, Naoto Hamada, Atsushi Iwasaki and Makoto Yokoo,
"Controlled School Choice with Soft Bounds and Overlapping Types",
Journal of Artificial Intelligence Research, 査読有, Vol.58, (2017), pp.153-184.
https://doi.org/10.1613/jair.5297

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, 査読有, Vol.64, Issue 1, (2018), pp.654—685.
https://doi.org/10.1109/TIT.2017.2744650

Yuichi Komano, Kazuo Ohta, Kazuo Sakiyama, Mitsugu Iwamoto, and Ingrid Verbauwhede,
“Single-Round Pattern Matching Key Generation Using Physically Unclonable Function,”
Security and Communication Networks, 査読有, Vol. 2019, Article ID 1719585, (2019), 13 pages.
https://doi.org/10.1155/2019/1719585

Kohei Matsuda, Tatsuya Fujii, Natsu Shoji, Takeshi Sugawara, Kazuo Sakiyama, Yu-ichi Hayashi, Makoto Nagata, and Noriyuki Miura,
“A 286 F2/Cell Distributed Bulk-Current Sensor and Secure Flush Code Eraser against Laser Fault Injection Attack on Cryptographic Processor,”
IEEE Journal of Solid-State Circuits, 査読有, Vol.53, No.11, (2018). pp. 3174-3182.
https://doi.org/10.1109/JSSC.2018.2869142

平野伸将, 榎本 恵, 関根道昭, 田中健次, “高齢運転者における複数同時危険事象の認識に視覚的な注意喚起が与える影響”, ヒューマンインタフェース学会論文誌, 査読有, Vol.21, No.1, (2019). pp.111-120.
https://doi.org/10.11184/his.21.1_111

「学会発表」：
Timothy Girry Kale, Satoshi Ohzahata, Celimuge Wu, Toshihiko Kato,
“Improving the Tor Traffic Distribution with Circuit Switching Method”,
IEEE 17th Int’l Conference of High Performance Switching and Routing (HPSR),
2016 年 6 月, Yokohama, Japan.
https://doi.org/10.1109/HPSR.2016.7525647

Bando, K., Matsuno, Y., Ishigaki, Y., Tanaka, K.
"A Prototype Implementation of a Failure Database for Information Sharing with the General Public — A Case Study on Radiation Risk Information after Fukushima Nuclear Disaster,”

The 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2016 年 6 月, Toulouse, France.

Shoei Nashimoto, Daisuke Suzuki, Takeshi Sugawara, Kazuo Sakiyama,
”Sensor CON-Fusion: Defeating Kalman Filter in Signal Injection Attack,”
Asia Conference on Computer and Communications Security (AsiaCCS),
2018 年 5 月, Incheon, Korea.
https://doi.org/10.1145/3196494.3196506

Yoshiki Abe, Mitsugu Iwamoto, Kazuo Ohta,
“Efficient Private PEZ Protocols for Symmetric Functions,”
Theory of Cryptography Conference (TCC),
2019 年 12 月, Nuremberg, Germany.
https://link.springer.com/chapter/10.1007/978-3-030-36030-6_15

A.Iwasaki, T.Sekiguchi, S.Yamamoto, and M.Yokoo,
"Repeated Multimarket Contact with Private Monitoring: A Belief-Free Approach,"
The 34th AAAI Conference on Artificial Intelligence (AAAI),
2020 年 2 月, New York, USA.
https://www.aaai.org/Papers/AAAI/2020GB/AAAI-IwasakiA.8710.pdf

「招待講演発表」：
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, September, 2017. 山口県

岩本貢, “秘密計算の安全性～プライバシーを保ちつつどこまで計算できるか”, 第 8 回バイオメトリクスと認識・認証シンポジウム(SBRA), 発表年月日：2018 年 11 月 20 日, 場所：KDDI 飯田橋駅前ビル

Kazuo Sakiyama, “Keynote: Towards Resilient IoT System – How to Evaluate Information Leakage,” The First International Workshop on Hardware Oriented Cybersecurity (HwSec2018), (Dec., 19, 2018), Vietnam..

Kazuo Ohta, “Strong Forward Privacy for Dynamic Searchable Encryption,” Seminar at Google – Searchable Encryption Talk, New York, NY, USA, Jul. 25th, 2019.

Kazuo Ohta, “Card-based Majority Voting Protocols with Three Inputs Using Three Cards,” the International Secure Multi-party Computation Forum, Zhejiang, China, Jun. 1st, 2019.

「図書」：

著者名：小林欣吾，佐藤創(監訳)

出版社名：共立出版

署名：「数学ゲーム必勝法」

発行年：２０１６

原著：Elwyn R. Berlekamp, John H. Conway, Richard K. Guy, “Winning Ways for Your Mathematical Plays,” A K Peters/CRC Press, 2001.

（第 1 巻 第 5 章の翻訳を岩本貢准教授が担当）.

「受賞」：

「第１４回ディペンダルブルシステムワークショップ 最優秀論文発表賞」

授与団体：日本ソフトウェア科学会ディペンダブルシステム研究会

受賞者：坂東幸一、松野 裕（日本大学）、石垣 陽、田中健次

受賞標題：「市民等と障害情報を共有する障害データベースの構築の試み」

受賞年月日： ２０１６年１２月

https://sites.google.com/site/jssstdsw/dsw2016

「SCIS 論文賞」

授与団体：2017 年暗号と情報セキュリティシンポジウム（SCIS2017）

受賞者：粕谷桃伽，町田卓謙，崎山一男

受賞標題：XOR モデルを用いたサイドチャネル認証

受賞年月日：２０１７年１月

https://www.ieice.org/~isec/award-SCIS.html

「CSS2017 コンセプト論文賞」

授与団体：コンピュータセキュリティシンポジウム（CSS 2017）

受賞者：皆川諒，高田哲司

受賞標題：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

受賞年月日：２０１７年１０月

http://www.iwsec.org/css/2017/award.htm

「Best Poster Award」
授与団体：The 13th International Workshop on Security (IWSEC 2018)
受賞者：Erina Tatsumi, Kazuo Sakiyama and Takeshi Sugawara (The University of Electro-Communications),
受賞標題：A Case Study of Row Hammer under Different Refresh Rates
受賞年月日：２０１８年９月
http://www.ipsj.or.jp/award/iwsec-award3.html

「Best Poster Award」
授与団体：The 14th International Workshop on Security (IWSEC 2019)
受賞者：Yoshiki Abe, Mitsugu Iwamoto, Kazuo Ohta (The University of Electro-Communications)
受賞標題：How to improve the private PEZ protocol for general functions
受賞年月日：２０１９年８月
https://www.iwsec.org/2019/posters.html

「特許出願」：

"動的検索可能暗号処理システム及び動的検索可能暗号処理方法,"
渡邉洋平, 岩本貢, 太田和夫, 特願 2019-3908, (出願年月日：平成 31 年 1 月 11 日), 国内

「その他」：ホームページ等

「暗号王になる」子供の科学, pp. 11-21, 誠文堂新光社 (太田和夫教授の取材協力), 2016 年 11 月号.

渡邉洋平, "国際会議参加報告: 4th Heidelberg Laureate Forum," Fundamentals Review, Vol. 10, No. 3, pp.220-221, 電子情報通信学会, 2017. Available at https://www.jstage.jst.go.jp/article/essfr/10/3/10_220/_pdf

以上.