２０２３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　　t
　　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

＜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	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	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	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	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	助教	渡邉 洋平
電気通信大学	産学官連携センター		特任教授	田中健次

＜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

３．２０２３年度の研究の特筆すべき成果

成果１）自動運転シミュレータで生成したデータを用いた連合学習による物体検出

近年の自動運転技術の向上に伴い，自動車が生成するデータ量も急激に増加している．そのため，機械学習を用いてデータを処理することが必要であるが，従来の手法では複数の自動車から生成された生データを中央サーバで集約・管理していたため，ユーザのプライバシを侵害する危険性があった．連合学習ではデータを集約することなく，各車両で生成されたモデルの更新差分を集約することで学習が行われるため，データを他者に送信する必要がない．しかし、連合学習の実用化を考えると，各車両が自車両内で完結して画像データに対する教師あり学習での正解ラベルを作成し，連合学習を行う手法が望まれるが，このような手法は確立されていない．そのため，既存の研究では画像データに対応する既知の正解ラベルが与えられて評価実験が行われ，現実的な利用形態での評価ができない状況となっている．

本研究では自動運転における物体検出において，Multiple Object Tracking を利用することによって各車両がローカルに画像へラベル付けを行い，そのデータをもとに連合学習を行う手法を提案した．さらに複数のカメラ間での物体追跡をLiDARセンサーの情報を用いて実現した。自動運転シミュレータCarlaを用いたデータにより評価実験を行い、有用性を明らかにした。

成果２）

本研究では，制約付きマッチングや警備計画策定といった相異なる利害をもつ主体のインセンティブを調整しながら稀少なリソースを配分する仕組み（メカニズム）を実際のデータから評価・修正する，データ駆動型インセンティブ

工学を構築する．令和 5 年度は以下の 3 つの項目を相互にフィードバックさせながら研究を推進した：項目 1）不確実な環境下における動学ゲームの均衡計算アルゴリズム；項目 2）制約付きマッチングの定量的分析；項目 3）警備計画策定問題の定量的分析．ただし，項目 3 については，当初の想定通りにデータが入手できなかったため、花き市場の定量分析に切り替えた。

関連する研究成果は人工知能と統計のトップ会議である AISTATS2023¥に採択された。今後の国際会議や論文誌への投稿を準備している。

成果３）個人認証の運用方法変更によるパスワード認証の安全性改良

Web サービスへの不正ログインはあとを立たず，その対策が急務となっている．その対策は個人認証であり主流はパスワード認証であったが，安全性への懸念から二段階認証への移行が進められている．しかし現状の二段階認証は誰でも利用可能とはいえず，またすべての Web サービスで提供できる方法ともいいがたい．そこで本論文では，パスワード認証を安全に運用する方法としてログインページを非公開とし，正規ユーザに個別のログインページを割り当てる手法を提案する．この提案によりオンラインによる不正アクセスが困難化できるとともに，フィッシング対策にもなることについて議論を通じて示した．またサービス運用側にとっても利点がある運用方法であることについても述べた．また提案手法の受け入れ可能性について評価実験を行い，二段階認証が使えるユーザであれば本手法も利用できる可能性があることを示した．

４．２０２３年度の研究成果の公表実績

特記なし．
各研究室の Web で情報公開が行われているのであわせて参照されたい

岩本・渡邉研究室：https://iw-lab.jp/
崎山研究室：https://sakiyama-lab.jp/
大坐畠研究室：https://www.net.lab.uec.ac.jp/
高田研究室：http://www.az.inf.uec.ac.jp/

５．外部資金の獲得状況

1. 科研費（基盤研究(A)）日本学術振興会
「スケーラブルな物理セキュリティを可能にする近似計算の設計基盤と理論の構築」
代表者：富山宏之・分担者：崎山一男
直接経費　9,400 千円・間接経費 2,820 千円

2. 科研費（基盤研究(A)）日本学術振興会
「真に高機能暗号の社会展開に資する物理・視覚暗号」
代表者：花岡悟一郎・分担者：岩本貢，渡邉洋平
直接経費　13,200 千円・間接経費 3,960 千円

3. 科研費（基盤研究(A)）日本学術振興会
「情報・計算・暗号の融合によるセキュリティ定量化基盤の構築」
代表者：安永憲司・分担者：岩本貢
直接経費 9,400 千円・間接経費 2,820 千円

4. 科研費（基盤研究（A））日本学術振興会
「データ駆動型インセンティブ工学の構築」
代表者：岩崎敦
直接経費 5,300 千円・間接経費 1,590 千円

5. 科研費（基盤研究(B)）日本学術振興会
「センサーに内在する固有性の拡散と収縮に基づく非暗号学的計測セキュリティ」
代表者：三浦典之・分担者：崎山一男
直接経費　6,300 千円・間接経費 1,890 千円

6. 科研費（基盤研究(B)）日本学術振興会
「十分統計量に基づくシミュレーションベース安全性の深化」
代表者：岩本貢・分担者：渡邉洋平
直接経費 3,300 千円・間接経費 990 千円

7. 科研費（基盤研究(B)）日本学術振興会
「公開鍵暗号の識別不可能性に対する総合的評価技術の開発」
代表者：四方順司・ 分担者：岩本貢
直接経費 3,400 千円・間接経費 1,020 千円

8. 科研費（基盤研究(B)）日本学術振興会
「広範な検索機能と高い効率性を両立する秘匿検索技術の実現」
代表者：渡邉洋平
直接経費 1,900 千円・間接経費 570 千円

9. 科研費（基盤研究(C)）日本学術振興会
「教ではなく育で人の安全行動を促進する方法の提案」
代表者：田中健次
直接経費 1,100 千円・間接経費 330 千円

10. 科研費（挑戦的研究（開拓））日本技術振興会
「セキュリティ解析の新理論～情報量不等式から計算量不等式へ～」
代表者：渡辺峻
直接経費 6,300 千円・間接経費 1,890 千円

11. 科研費（挑戦的研究（萌芽））日本学術振興会
「不完全情報下での逐次的意思決定：機械学習と情報理論からの探索」
代表者：岩崎敦
直接経費 2,300 千円・間接経費 690 千円

６．今後の研究発展

メンバー間および外部研究者との研究協力をさぐりつつ，外部資金の獲得を目指す

７．発表論文等

「雑誌論文」：

Haruka Hirata, Daiki Miyahara, Victor Arribas, Yang Li, Noriyuki Miura, Svetla Nikova, and Kazuo Sakiyama, “All You Need Is Fault: Zero-Value Attacks on AES and a New λ-Detection M&M,” Vol.2024, No.1, pp.133–156, 2023. https://doi.org/10.46586/tches.v2024.i1.133-156

Saya Inagaki, Mingyu Yang, Yang Li, Kazuo Sakiyama, and Yuko Hara-Azumi, “Power Side-channel Attack Resistant Circuit Designs of ARX Ciphers Using High-level Synthesis,” ACM Trans. Embed. Comput. Syst., Vol.22, Issue 5, No.85, pp.1-17, (Sept., 2023). https://doi.org/10.1145/3609507

Mitsugu IWAMOTO, “Information-Theoretic Perspectives for Simulation-Based Security in Multi-Party Computation,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E107.A, Issue 3, pp.360-372, (Mar. 2024). https://doi.org/10.1587/transfun.2023TAI0001

Kyosuke YAMASHITA, Keisuke HARA, Yohei WATANABE, Naoto YANAI, Junji SHIKATA, “Designated Verifier Signature with Claimability”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E107A, Issue 3, pp.203-217, (Mar. 2024). https://doi.org/10.1587/transfun.2023CIP0016

K. Minematsu, J. Shikata, Y. Watanabe and N. Yanai, "Anonymous Broadcast Authentication With One-to-Many Transmission to Control IoT Devices," IEEE Access, vol. 11, pp. 62955-62969, (June, 2023). https://doi.org/10.1109/ACCESS.2023.3288337

Kobayashi, H., Watanabe, Y., Minematsu, K. et al. “Tight lower bounds and optimal constructions of anonymous broadcast encryption and authentication,” Des. Codes Cryptogr. Vol.91, 2523–2562 (2023). https://doi.org/10.1007/s10623-023-01211-x

Kenshi Abe, Kaito Ariu, Mitsuki Sakamoto, Kentaro Toyoshima, Atsushi Iwasaki, “Last-Iterate Convergence with Full- and Noisy-Information Feedback in Two-Player Zero-Sum Games,” Proc. of the 26th Int’l Conf. on Artificial Intelligence and Statistics (AISTATS 2023), 7999-8028, (2023).

嶋野 裕一郎, 宮原 大輝, 崎山 一男, “スマートフォンを利用したサイドチャネル情報の取得に関する基礎研究,” 電気学会論文誌Ｃ（電子・情報・システム部門誌）, 143 巻, 12 号, pp. 1180-1186 (Dec., 2023). https://doi.org/10.1541/ieejeiss.143.1180

「学会発表」：

Momoka Kasuya, Nobuyoshi Morita, Hiroki Yamazaki, and Kazuo Sakiyama, “Automated Extraction for Vulnerability Management on PSIRT: A Case Study of Automotive Industry,” In Proc. International Symposium on Computing and Networking, CANDAR Workshops (CANDARW’23), IEEE, pp.232–238 (Nov., 2023). https://doi.ieeecomputersociety.org/10.1109/CANDARW60564.2023.00046

Maki Tsukahara, Haruka Hirata, Mingyu Yang, Daiki Miyahara, Yang Li, Yuko Hara-Azumi, and Kazuo Sakiyama, “On the Practical Dependency of Fresh Randomness in AES S-box with Second-Order TI,” In Proc. International Symposium on Computing and Networking, CANDAR Workshops (CANDARW’23), IEEE, pp.286–291 (Nov., 2023).
https://doi.org/10.1109/CANDARW60564.2023.00054

Yuki Matsukawa, Daiki Miyahara, Takeshi Sugawara, Kazuo Sakiyama andYang Li, “Exploring Leakage Characteristics and Attacks through Profiles ofScreaming Channels,” The 7th International Conference on Mobile Internet Security (MobiSec 2023), (Dec., 2023).

Yuuki Nakahama, Satoshi Ohzahata, Ryo Yamamoto,
“Auto Annotation using Object Tracking with Multiple in-vehicle Cameras for Federated Learning”, Proc. of International Conference on Artificial Intelligence in Information and Communication (ICAIIC), 6 pages, (2024).

Amada, T., Iwamoto, M., Watanabe, Y., “Efficient Result-Hiding Searchable Encryption with Forward and Backward Privacy,” Information Security and Cryptology (ICISC 2023), (March 2024). https://doi.org/10.1007/978-981-97-1238-0_10

Ono, T., Shinagawa, K., Nakai, T., Watanabe, Y., Iwamoto, “Single-Shuffle Card-Based Protocols with Six Cards per Gate,” Information Security and Cryptology – ICISC 2023. (March 2024), https://doi.org/10.1007/978-981-97-1238-0_9

Uchizono, S., Nakai, T., Watanabe, Y., Iwamoto, M., “Constant-Deposit Multiparty Lotteries on Bitcoin for Arbitrary Number of Players and Winners,” Information Security and Cryptology – ICISC 2023. (March 2024). https://doi.org/10.1007/978-981-97-1238-0_8

Sugimoto, K., Nakai, T., Watanabe, Y., Iwamoto, M., “The Two Sheriffs Problem: Cryptographic Formalization and Generalization,” Combinatorial Optimization and Applications. (COCOA 2023), (Dec. 2024), . https://doi.org/10.1007/978-3-031-49611-0_37

T. Nishiuchi, S. Fujita, Y. Watanabe, M. Iwamoto and K. Sawada, "Packet Analysis and Information Theory on Attack Detection for Modbus TCP," IECON 2023- 49th Annual Conference of the IEEE Industrial Electronics Society, pp. 1-6, (Oct. 2023).
https://doi.org/10.1109/IECON51785.2023.10312507

Watanabe, Y., Yanai, N., Shikata, J., “IoT-REX: A Secure Remote-Control System for IoT Devices from Centralized Multi-designated Verifier Signatures,” Information Security Practice and Experience. ISPEC 2023. (Nov. 2023). https://doi.org/10.1007/978-981-99-7032-2_7

渡邉祐貴, 高田哲司, ”Web ブラウザにおけるフィッシングページ検出の実現可能性調査”, コンピュータセキュリティシンポジウム(CSS’23), 8 pages, (Oct. 2023).

根本啓佑, 高田哲司, ”ログインページの運用方法変更によるパスワード認証の安全性改良法”, 第 16 回インターネットと運用技術シンポジウム（IOTS2023）, (Dec. 2023).

中濱雄喜, 大坐畠智, 山本嶺, ”Federated Learning のための複数車載カメラによる物体追跡を用いたラベル付け”, 信学技報, vol. 123, no. 219, IN2023-33, pp. 5-10, (Oct. 2023).

田中健次, 坂東幸一, ”想定外事象を想定した未然防止のための信頼性・安全性の方法論の提案”, 日本品質管理学会 第 131 回研究発表会、(May. 2023).

「招待講演発表」：

特になし

「図書」：

特になし

「受賞」：

「辻井重男セキュリティ論文賞」
K. Asano, K. Emura, A. Takayasu, Y. Watanabe, “A Generic Construction of CCA-secure Attribute-based Encryption with Equality Test”, 2023 年 7 月, https://www.uec.ac.jp/news/prize/2023/20231002_5673.html

「KISTI Best Paper Award」
Y. Watanabe, T. Tomita, J. Shikata, “Lattice-based Multi-Entity Identification Protocols”, 2023 年 12 月, https://www.uec.ac.jp/news/prize/2023/20231225_5894.html

「企業冠賞 シー・オー・コンウ”賞」
根本啓祐, 高田哲司, ”ログインページの運用方法変更によるパスワード認証の安全性改良法”, 2023 年 12 月.

「SCIS 論文賞」

浅野 京一，渡邉 洋平，“CCA 安全な鍵更新可能公開鍵暗号の安全性解析と効率的な一般的構成法”，2024 年 1 月，
https://www.uec.ac.jp/news/prize/2024/20240315_6090.html

「特許出願」：

特になし

「その他」：

特になし

以上.