

## PWS Cup 2024 にトヨタ自動車、KDDI 総合研究所、ARISE analytics の三社合同チームで参加、ベストアタック賞を受賞

|                      |                             |
|----------------------|-----------------------------|
| トヨタ自動車株式会社           | 椎名峻平、篠田謙司、中谷翔、吉田琢也          |
| 株式会社 KDDI 総合研究所      | 奥井宣広                        |
| 株式会社 ARISE analytics | 福嶋昌太郎、日比宏明、飯澤優太郎、秋元裕介、湯野川八雲 |

PWS Cup はコンピュータセキュリティシンポジウム(CSS)のプライバシーワークショップ(PWS)のイベントとして毎年開催される、個人データの安全な利活用に向けた匿名化技術を匿名化と攻撃の対戦形式で競うコンテストです。トヨタ自動車株式会社、株式会社 KDDI 総合研究所、株式会社 ARISE analytics は、PWS Cup 2024 に三社合同チームで参加し、10 回目の開催において過去最多タイとなる 21 チームが参加する中、攻撃力が最も高かったチームに送られるベストアタック賞を受賞しました。

### 背景

PWS Cup<sup>[1]</sup>はコンピュータセキュリティシンポジウム(CSS)<sup>[2]</sup>のプライバシーワークショップ(PWS)<sup>[3]</sup>のイベントとして毎年開催される、個人データの安全な利活用に向けた匿名化技術を競うコンテストです。開催は今年で 10 回目を数え、2023 年からは国際版の iPWS Cup も開催されています。コンテストの目標は、有用性が高く、安全性も高いすなわち攻撃が難しい匿名化データの作成であり、各チームが匿名化したデータに対して他のチームが攻撃を行うという対戦形式で行われます。今年はデータ利活用の観点も加わり、匿名化、攻撃、データサイエンスの技術力が競われました。

今回開催された PWS Cup 2024 のテーマは映画レビューであり、単純な匿名化ではプライバシーを保てない恐れがあるという Netflix の事例に基づいた現実に即したテーマ設定となっています。コンテストには海外からの参加を含む過去最多タイとなる 21 チームが参戦し、7/26(金)から 10/16(水)にかけて、予備戦の匿名化フェーズと攻撃フェーズ、本戦の匿名化フェーズと攻撃フェーズが順に行われ、10/24(木)に CSS2024 の PWS セッションの中でプレゼンとポスター発表、結果発表と表彰式が行われました。

トヨタ自動車株式会社、株式会社 KDDI 総合研究所、株式会社 ARISE analytics は、モビリティサービスのデータ分析における個人情報・プライバシー保護の取り組みの一つとして、技術力向上やコミュニティ貢献を目的に、三社合同チームを構成してチーム 20 “KAT-TUNE” として PWS Cup 2024 に参加しました。チーム名には KDDI Research, ARISE analytics, Toyota Motor の頭文字を入れ、TUNE に三社の調和の意味を込めています。

## 発表概要

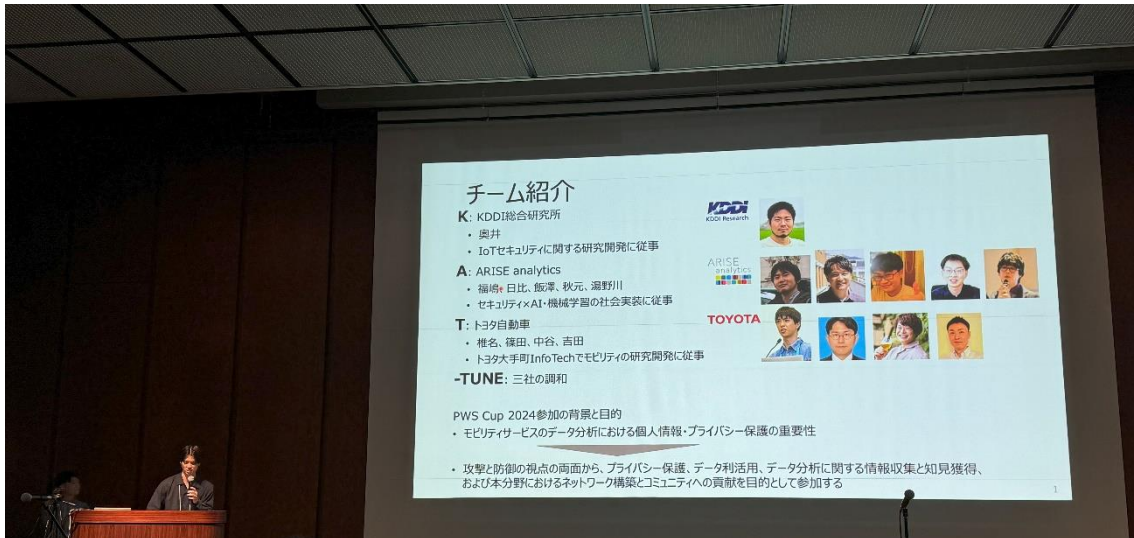
10/24(木)に CSS2024 の PWS セッションの中で行ったプレゼンとポスター発表では、匿名化手法、攻撃手法、データサイエンスについて説明しました。

匿名化では最適輸送を用いて合成データを生成する手法を考案しました。有用性指標は満点 100 のうち 95 まで上げることができたものの、有用性を上げると攻撃しやすくなるというトレードオフを考慮してコンテストでは 72 に抑えたデータを利用しています。

攻撃では統計量を用いた確率ベースの最適マッチングというアプローチを取りました。最適化にはハンガリアンアルゴリズムを利用しています。結果としてこの攻撃は大きな効果を上げましたが、統計量の値しか用いない手法でありながら効果的であったという事実は、統計量であっても大量に公開されると個人が特定されるリスクが高いことを示唆しています。

データサイエンスでは提案した匿名化手法は推薦アルゴリズムに有用かという観点で Factorization Machines を用いた評価を行いました。結果、有用性指標によっては推薦システム開発で間違った示唆を与える可能性があり、匿名化手法を改善する余地があることが分かりました。

より詳しい内容は PWS Cup 2024 のサイトで公開されているポスター<sup>[4]</sup>をご参照ください。



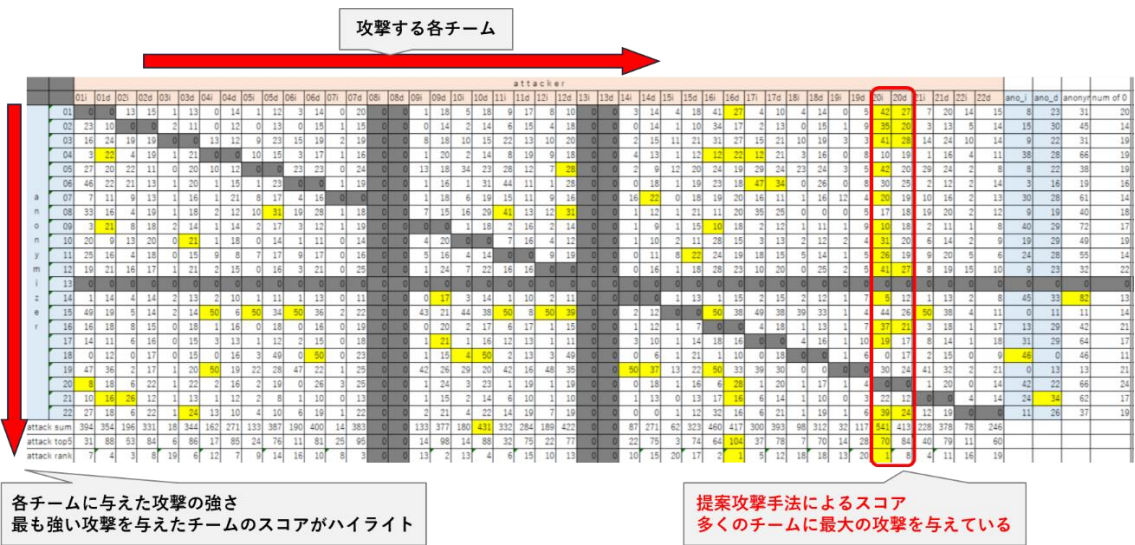
プレゼンするトヨタ自動車 椎名と ARISE analytics 日比



ポスター発表で説明する ARISE analytics 日比、トヨタ自動車 篠田、椎名（左から）

結果

コンテストの開始当初こそ出遅れて予備戦匿名化部門 16 位と振るわなかったものの、予備戦攻撃部門は 2 位、本戦匿名化部門は 2 位、本戦攻撃フェーズは 2 位と挽回し、総合 7 位と健闘しました。また、攻撃部門では、最高の攻撃力を持つチームに送られるベストアタック賞を受賞しました。なお、競技説明や結果を含む PWS Cup 2024 発表会資料<sup>[5]</sup>やチーム KAT-TUNE のポスター<sup>[4]</sup>等は PWS Cup 2024<sup>[1]</sup>のページで公開されています。



本戦におけるチーム毎の攻撃力評価(PWS Cup 2024 発表会資料<sup>[5]</sup>より抜粋して加筆)



表彰式での ARISE analytics 日比、群馬大学 千田准教授、トヨタ自動車 椎名 (左から)

## 参考 URL

- [1] PWS Cup 2024  
<<https://www.iwsec.org/pws/2024/cup24.html>>
- [2] コンピュータセキュリティシンポジウム 2024  
<<https://www.iwsec.org/css/2024/index.html>>
- [3] プライバシーワークショップ(PWS)  
<<https://www.iwsec.org/pws/index.html>>
- [4] チーム 20 KAT-TUNE ポスター  
<[https://www.iwsec.org/pws/2024/Images/pwscup2024\\_poster\\_team20.pdf](https://www.iwsec.org/pws/2024/Images/pwscup2024_poster_team20.pdf)>
- [5] PWS Cup 2024 発表会資料  
<[https://www.iwsec.org/pws/2024/Images/20241024\\_PWSCUP2024.pdf](https://www.iwsec.org/pws/2024/Images/20241024_PWSCUP2024.pdf)>