

PWS Cup 2024 Team20: KAT-TUNE

奥井
株式会社 KDDI総合研究所

K

福嶋、日比、飯澤、秋元、湯野川
株式会社 ARISE analytics

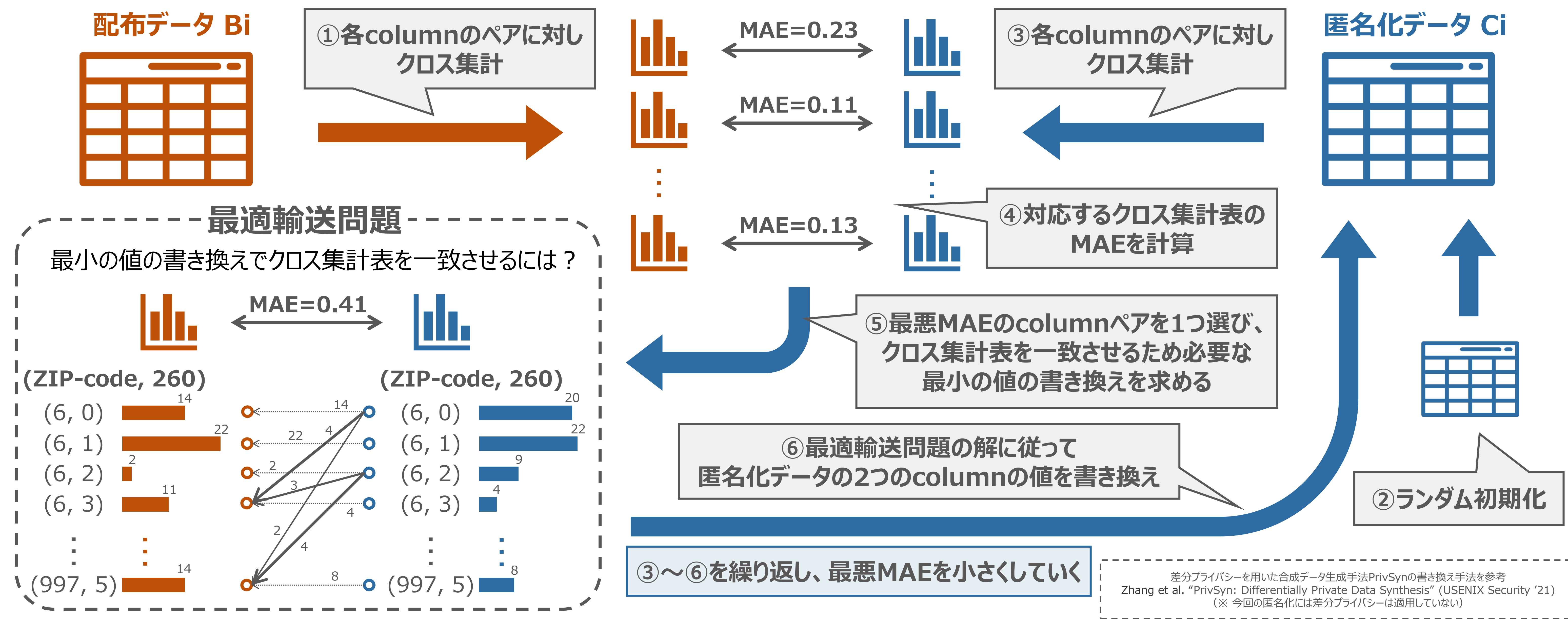
A

椎名、篠田、中谷、吉田
トヨタ自動車 株式会社

T

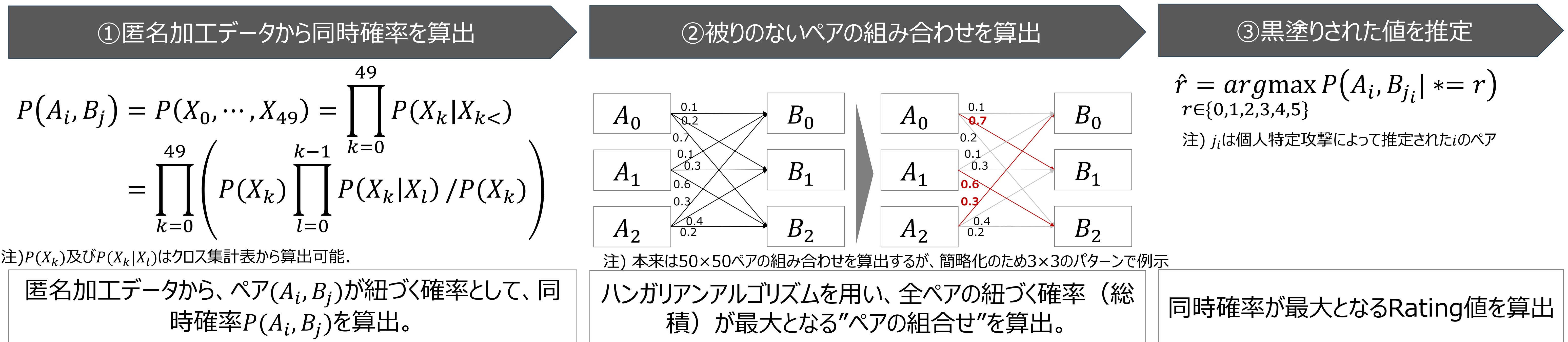
三社の調和
-TUNE

匿名化手法：最適輸送を用いた合成データ生成



攻撃手法：ハンガリアンアルゴリズムを用いた全体最適攻撃

	個人特定攻撃	DB再構築攻撃
攻撃フェーズの目標	Ratingsデータの各レコード(以下 B_j)に紐づく基本属性データのレコード(以下 A_i)を推定すること。	Ratingsデータで黒塗りされた元データの値を推定すること。
仮説	B_j のペアとなる A_i を被りなく紐づける組み合わせの中では、正しいペアの組合せを選んだ際に、全ペアの紐づく確率は最大化されるのではないか？	正しいペアが選択できているのであれば、黒塗り部分に正しいRatingの値を代入した際に、そのペアの紐づく確率は最大化されるのではないか？



データサイエンス：推薦システム開発におけるKAT-TUNE匿名化手法の有用性評価

問い：匿名化データは推薦システム開発に有用なのか？ → 手法：匿名化後でも特徴量間の相互作用効果が残っているかを評価することで検証

2次相互作用の影響度合いの評価手法

