SBイノベンチャー株式会社
MaskTapチーム/麦わら海賊団

PWSCup2021 Team04の解法

背景

○ 予備戦=>本戦の変更点

- **Index攻撃が禁止**された。
- **情報損失(iloss)制約が強化**された。
- 評価指標に**δ=0.01**が加えられた。

運営の意図を汲み取る

○ 仮説

- **Index攻撃を抑制**
- **Swapping**による匿名化が**難化**
- **メンバーシップ攻撃**(precisionやrecall)の**対策を重視**

匿名化フェーズ

【匿名化方針】

○第一匿名化

1. **ユニークではないレコードを全て抽出**
2. **ユニークなレコードをランダムに抽出**
   (ユニークの定義はuniqrt.pyによる)

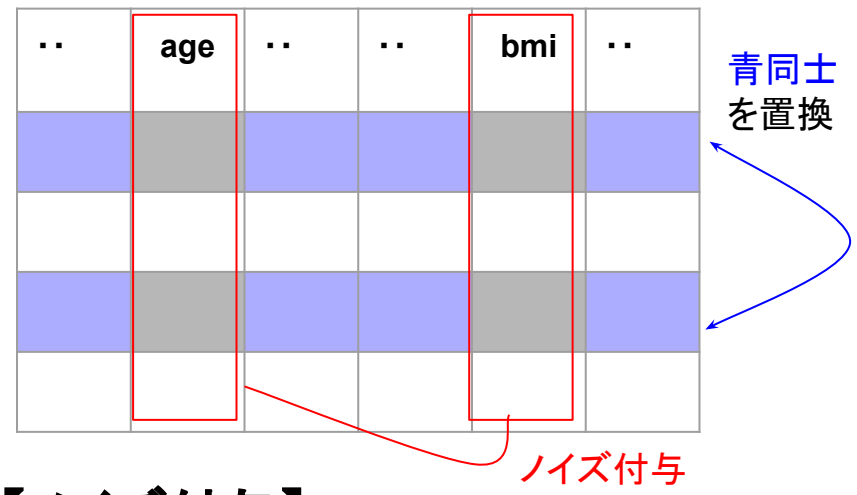
○第二匿名化

3. **ilossに基づいてSwapping**
4. **age, bmi列にノイズ付与**
5. **手動でレコードの値を変更**

(1~2: 第一匿名化, 3~5: 第二匿名化)

【Swapping】

全カラムを置換すると、ノイズ付与の際、**age, bmi列のiloss<=4条件**が難しくなる。
そのため**カテゴリカル列のみを置換**した。
(※ iloss<=4の組み合わせの中に限る。)
(※ 有用性ORを満たすようにseedを変えて何度もtryした。)



【ノイズ付与】

age, bmi列に**ガウスノイズ**(N(0, 4))を付与。
絶対値が4を超える物については**±4でclip**。
ノイズが小さすぎる(絶対値2以下)場合は、**元の値±2の加工**を行った。

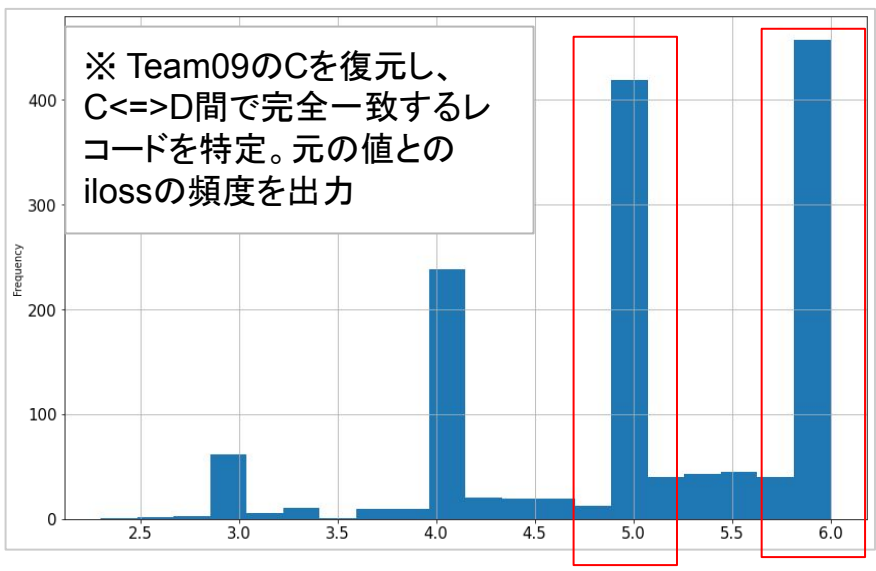
【本戦のBデータ】

mar列の**Separated**という項目が存在しなかった。**属性の組み合わせの総数が5/6倍**になるため、ユニークではないレコード数が多く有利だった可能性がある。

攻撃フェーズ

【予備戦EDA】

DやXが公開されたチームが、どのようにSwappingを行っているかを調査。



本戦では、**iloss=4となるレコード間**で**Swappingされる**可能性が高い

【攻撃方針】

1. **ORPenaltyでメンバーシップ推定**
   (※ 後述。precision, recall対策)
2. **識別はiloss=4の行からランダム**

【ORPenalty】

第二匿名化では有用性ORが大きく変わる変更(eg. White -> Black)が起こりにくい。
Bで値を変更した際のOR変化量に基づき、Penalty行列を作成。

gen	Female	Male
Male	0.51852	0.00000
Female	0.00000	0.51852

race	Black	White	Mexican	Other	Hispanic
White	0.580632	0.000000	0.476799	0.462602	0.269029
Black	0.000000	0.580632	0.065759	0.140057	0.245440
Mexican	0.065759	0.476799	0.000000	0.085918	0.109671
Other	0.140057	0.462602	0.085918	0.000000	0.234719
Hispanic	0.245440	0.269029	0.109671	0.234719	0.000000

Ct<=>D間で**ORPenaltyが大きい行**を**-1**に。

【識別】

Ctのメンバーと推定された各行に対し、**iloss=4に該当する**D内のレコードを抽出。
その中から**randomに3件**選び、回答とした。