Team 10 宮地研.exe 2021 PWS cup 戦略

MiYaJi Laboratory

匿名化フェーズ

匿名化方法の全体像

削除レコードは入れ替え後のものを参照しなければ有用性を確保できない
→第二匿名化後に第一匿名化を行う

予備選

元データB
↓ データ削除（第一匿名化）
匿名化データD削除行
↓ データ入れ替え（第二匿名化）
入れ替えデータB'

本選

元データB
↓ データ入れ替え（第二匿名化）
入れ替えデータB'
↓ 入れ替え元データの候補が少ないデータの削除（第一匿名化）
匿名化データD削除行

匿名化方針（第二匿名化）

有用性基準ORがかなり厳しい
→有用性を損なわない方法で匿名化する必要

レコードの入れ替えを行うことで匿名化を行う

レコード入れ替えの利点
- 含まれるレコードは変わらないため有用性が損なわれない
- 削除レコードと非削除レコードを入れ替えることで削除行を推測されづらくなる
- レコードが入れ替わることで個人のデータが他のレコードに割り当てられるため個人のレコードがどのレコードか推測されづらくなる

入れ替えの方法
1. 有用性条件ilossが4を超えないレコードを各レコードごとに探索する
2. 入れ替え先の候補が少ないものから行っていき候補がすべて入れ替え済みの場合は入れ替えではなく置き換えを行う

匿名化方針（第一匿名化）

第二匿名化で入れ替え実施

レコード入替に対して有効な攻撃方法

各レコードの入れ替え元の候補（入れ替えても有用性条件ilossが4を超えないレコード）から選択

レコード入替に対して有効な攻撃方法に弱いレコード削除

入れ替え元の候補が少ないレコードは正解率が高い
→入れ替え元の候補が少ないレコードを削除する
- 入れ替え元の候補が25以下のものを削除するのが有用性を満たす中では限界だった

各レコードの入れ替え候補の一覧の一部

0	19	25	31	52	55	75	84	120	144	163	208	233	234	254	256	257	284	322
1	16	75	78	84	129	164	173	213	323	354	362	505	609	647	688	786	799	909
2	27	807	818	852	853	908	974	1018	1061	1134	1186	1259	1316	1345	1376	1534	1604	1748
3	28	33	54	93	111	179	184	186	189	195	251	263	272	299	311	312	346	364
4	16	55	78	92	129	136	158	163	164	190	233	252	257	354	418	464	466	503
5																		
6	56	63	386	493	511	523	560	636	638	690	722	768	795	857	875	961	972	993
7	29	43	49	50	70	112	161	195	241	243	260	268	312	328	351	411	525	532
8	17	102	107	139	196	232	277	304	320	378	443	516	555	557	558	660	712	823
9	34	64	121	220	314	315	367	432	452	522	543	602	622	692	728	762	771	782
10	59	155	162	188	193	279	287	335	347	408	425	529	553	634	668	683	703	836
11	50	67	120	163	164	337	354	357	362	429	447	504	505	536	539	574	588	609
12	25	83	142	144	147	154	183	256	293	294	314	321	322	400	405	419	436	439
13	601	1363	1761	1855	2072	2110	2547	2627	2887	2996	3050	4081						
14	15	22	30	36	199	209	282	306	307	324	368	390	404	409	471	474	497	514

5番のレコードや13番目のレコードが削除対象

攻撃フェーズ

攻撃方針

予備選優秀チームの解析
- Imarkが0→距離による個人推定が困難
- 距離が遠いデータと入れ替え→距離推定を無効化

レコードの入れ替えに対して有効な攻撃を実施

メンバーシップ推定
- 削除レコードと非削除レコードが入れ替えられていた場合メンバシップ推定が非常に難しくなる
→すべてメンバーシップに含まれていると回答すると確実に$recall = 1, prec = 0.5$を取れる
→全てメンバシップに含まれていると回答

個人推定

各レコードの入れ替え元の候補（入れ替えても有用性条件ilossが4を超えないレコード）から回答を選択。

評価値概算

- 特定のレコードの推定が難しい時にメンバーシップに含まれていると回答するべきかの判断指標
- メンバーシップ推定の正答率が0.5、全体でのレコード推定の正答率を0.3とする

表.特定のレコードの正答率と評価値の期待値

正答率	1	0.1	0.01	0.0001
含めた場合	0.16329	0.15865	0.15819	0.15814
含めない場合	0.15810	0.15810	0.15810	0.15810

この結果からメンバシップ推定の正答率が0.5程度の場合
全てメンバーシップに含まれていると回答した方が良いと判断した

攻撃方法（個人推定）

有力な匿名化方法が距離が遠いデータとの入れ替えと推測
→距離が遠いデータと入れ替えに対して強い攻撃を実施

距離が遠いデータと入れ替えへの攻撃方法
→距離が遠いデータを回答とする

個人推定のレコード識別は以下で実施
1. ユークリッド距離が一番遠いデータ
2. 入れ替えた場合にilossが最大となるデータ
3. 入れ替えた可能性があるデータの中からランダム選択

1と2が重複した場合片方をランダム選択に変更する