Innovative R&D by NTT

優勝チーム解説とChallenge

濱田浩気
NTTセキュアプラットフォーム研究所 /
理化学研究所

概要・目次

- 発表概要
  1. PWS Cup 2017 の「君の名は~ユアネーム~」の手法
  2. 匿名化アルゴリズム公開/非公開による違い

君の名は~ユアネーム~

引用元: PWSCUP 2017 Information
https://pwscup.personal-data.biz/web/pws2017/info.php

- 半角カタカナすみません

概要・目次

- 発表概要
  1. PWS Cup 2017 の「君の名は~ユアネーム~」の手法
     - 岡田 莉奈，正木 彰伍，濱田 浩気
  2. 匿名化アルゴリズム公開/非公開による違い
     - 濱田 浩気，岡田 莉奈，小栗 秀暢，菊池 浩明，中川 裕志，野島 良，波多野 卓磨，正木 彰伍，渡辺 知恵美

- 目次
  - PWS Cup 2017 のルールの振り返り
  - 「君の名は~ユアネーム~」の加工・再識別アルゴリズム
  - 公開/非公開の違い

PWS CUP 2017 のルールの振り返り

コンテストの流れ

1. 各チームはデータを好きなように**加工**
   - **安全**かつ**有用**(元データと近い)となることを目指す

2. 互いのチームの加工データを攻撃(**再識別**)
   - どのレコードが誰なのかを当てる
   - たくさん当てられるほど安全性が低いとみなされる

3. **より安全かつ有用**なデータのチームが**勝者**

データ加工のイメージ

元データ

名前	購入日	単価	商品	数量
顧客1	12/3	1.2	みかん	30
顧客1	12/7	3.8	いちご	7
顧客1	11/7	1.2	みかん	20
顧客1	10/10	4.2	ぶどう	2
顧客2	12/3	1.4	みかん	23
顧客2	9/12	3.9	ぶどう	1
⋮				

加工後のデータ

仮名	購入日	単価	商品	数量
仮1	12/3	1.5	みかん	30
仮1	12/12	3.8	みかん	7
DEL				
仮2	10/10	4.2	ぶどう	4
仮3	12/12	1.4	みかん	23
仮3	9/12	3.9	なし	1
⋮				

名前と仮IDの対応表

	9月	10月	11月	12月	…
顧客1		仮2		仮1	
顧客2	仮3			仮3	
顧客3		仮5		仮5	

勝者の決め方

- 勝者: **総合評価**が**最小**(最良)の加工データ
  - **総合評価** = **有用性評価値** + **安全性評価値**

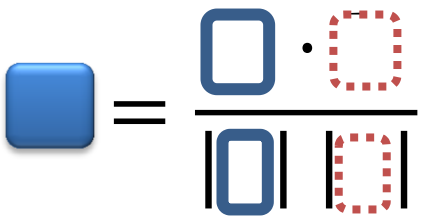
- **有用性評価値** = 6つの指標値の**最大値**(最悪値)
  - E1: item-item 類似度行列 (supplier)の差
  - E2: item-item 類似度行列 (retailer)の差
  - E3: item-item 類似度行列 (top-k)の差
  - E4: 購入日の差
  - E5: 単価の差
  - E6: 削除行割合

- **安全性評価値** = **再識別**された**顧客割合**

有用性指標E1, E2, E3

- 加工前後の[item-item 類似度行列]の平均誤差

	りんご	みかん	ブドウ	なし
りんご	1.0		0.2	0.1
みかん	0.7	1.0	0.4	0.1
ブドウ	0.2	0.4	1.0	0.3
なし	0.1	0.1	0.3	1.0



商品×顧客の数量の集計表

	顧客1	顧客2	顧客3	顧客4	…
りんご	0	3	5	0	…
みかん	1	0	3	0	…
ブドウ	0	0	0	1	…
なし	4	4	1	2	…

- E1,E2,E3は集計対象が少し違うだけ

有用性指標E4, E5, E6

元データ

名前	購入日	単価	商品	数量
顧客1	2/3	1.2	みかん	30
顧客1	2/7	3.8	いちご	7
顧客1	2/7	1.2	みかん	20
顧客1	9/10	4.2	ぶどう	2
顧客2	2/3	1.4	みかん	23
顧客2	9/12	3.9	ぶどう	1
⋮				

加工後のデータ

仮名	購入日	単価	商品	数量
仮1	2/3	1.5	みかん	30
仮1	2/12	3.8	みかん	7
DEL				
仮2	9/10	4.2	ぶどう	4
仮3	2/12	1.4	みかん	23
仮3	9/12	3.9	なし	1
⋮				

- E4: 加工前後の日付の差/31 の平均値
- E5: 加工前後の単価比(小さい方/大きい方)の平均値
- E6: 削除された行の割合

安全性指標

- 再識別された「人」の割合
- ポイント: **全部の月**を当てて初めて**再識別**成功

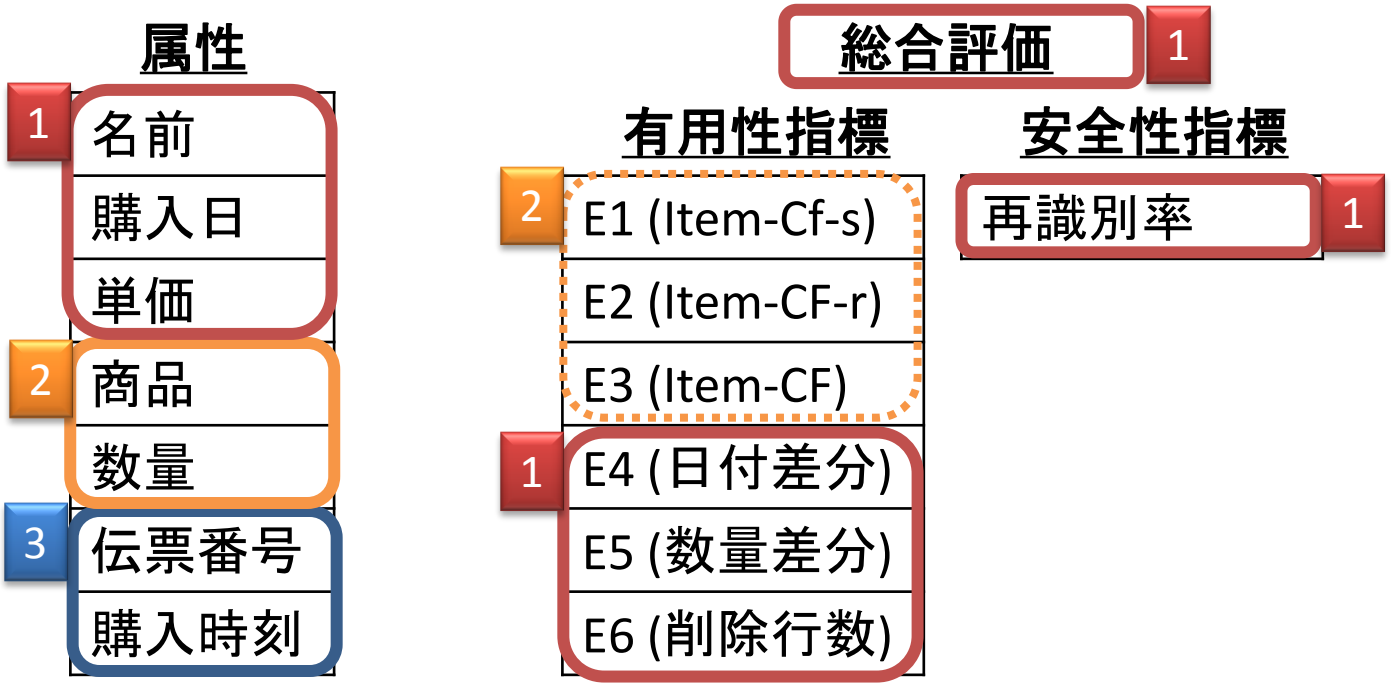
名前と仮IDの対応表

	9月	10月	11月	12月	…
顧客1		仮2		仮1	
顧客2	仮3			仮3	
顧客3		仮5		仮5	

「君の名は~ユアネーム~」の加工手法

加工アルゴリズムの流れ

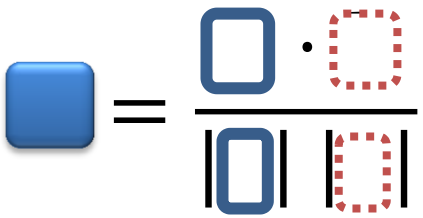
1. 名前，購入日，単価の加工
2. 商品，数量の加工
3. 伝票番号，購入時刻の加工



商品，数量の加工(1/2)

item-item 類似度行列

	りんご	みかん	ブドウ
りんご	1.0	■	0.2
みかん	0.7	1.0	0.4
ブドウ	0.2	0.4	1.0



商品×顧客の数量の集計表

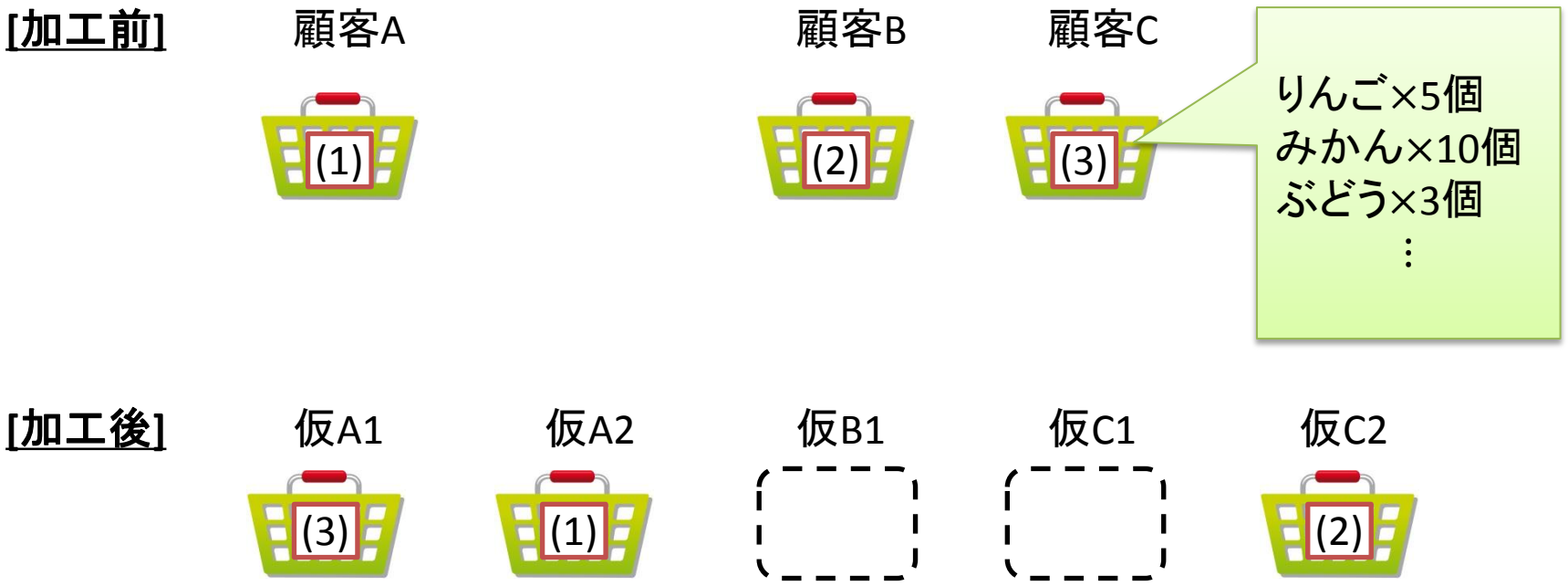
	顧客1	顧客2	顧客3	顧客4	…
りんご	0	3	5	0	…
みかん	1	0	3	0	…
ブドウ	0	0	0	1	…

観察:  を入れ替えても類似度行列は不変

➔  を入れ替えても E1, E2, E3 は不変

商品，数量の加工(2/2)

事実: 顧客ごとのバスケットを顧客間で入れ替えても類似度行列(E1, E2, E3)不変

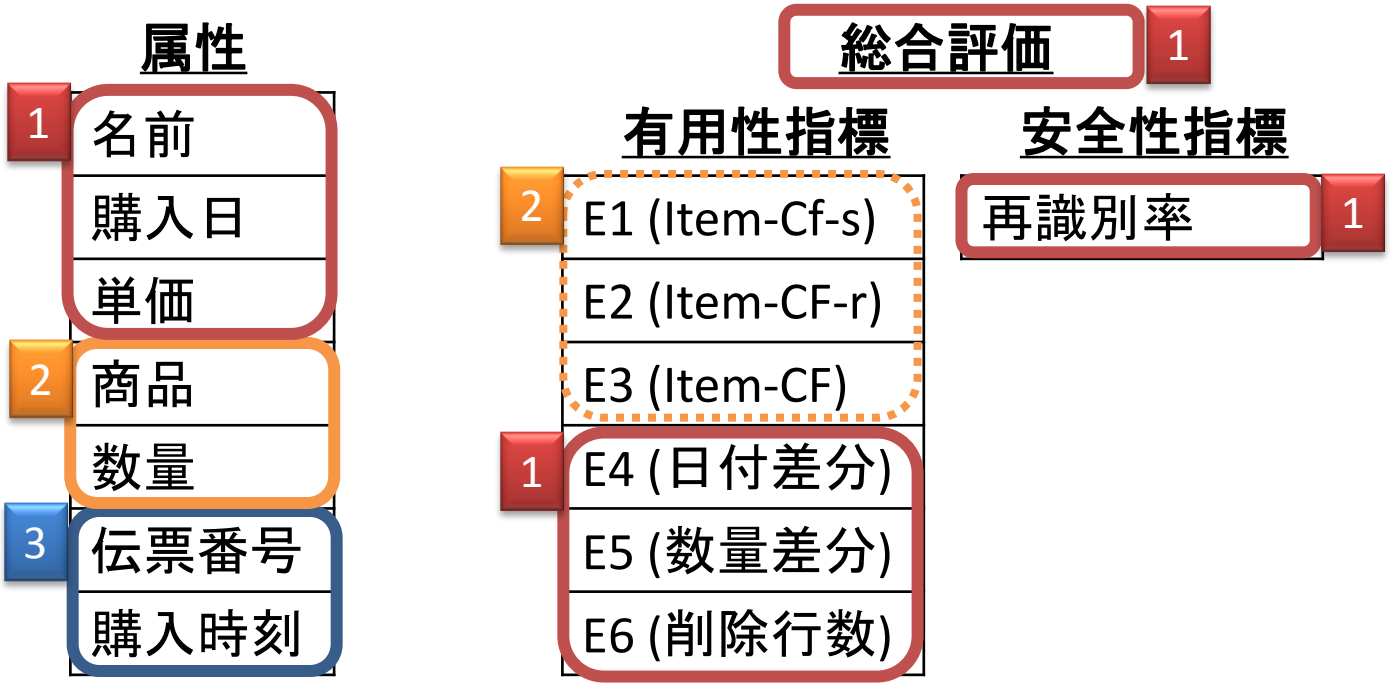


➔ 各バスケットを加工後の仮顧客に再割り当て

＝ E1,E2,E3 が 0 のまま商品，数量をスワップ

加工アルゴリズムの流れ

1. 名前，購入日，単価の加工
2. 商品，数量の加工
3. 伝票番号，購入時刻の加工



名前，購入日，単価の加工(1/3)

事実: **全ての月**を当てると**再識別**成功

➔ 1ヶ月でも当てられなければよい

➔ 顧客ごとに**一部の月だけ**を保護

名前と仮IDの対応表

	11月	12月	1月	2月	…
顧客1	仮1	仮2	仮2	仮3	
顧客2				仮4	
顧客3	仮5	仮6		仮7	
顧客4			仮8		
顧客5	仮9	仮10		仮10	
顧客6				仮11	
⋮					

名前，購入日，単価の加工(2/3)

元トランザクションの集計表

	11月	12月	1月	2月	…
顧客1	33回	95回	83回	3回	
顧客2				2回	
顧客3	35回	57回		35回	
顧客4			2回		
顧客5	40回	68回		10回	
顧客6				12回	
⋮					

名前	…	購入日	単価
顧客1	…	2/1	5.2
顧客1	…	2/10	3.8
顧客1	…	2/13	6.4
顧客2	…	2/10	2.5
顧客2	…	2/17	3.7

名前	…	購入日	単価
DEL	…		
仮1-2	…	2/10	3.2
仮1-2	…	2/13	5.0
仮2-2	…	2/10	3.2
仮2-2	…	2/13	5.0

1. 保護対象 選定
2. グループ 化
3. グループ 内で (行数，購入日，単価) 統一

安全性の評価値の見積もり

安全性の評価値 = (再識別された人の数)

➔ 個別に再識別成功確率を見積もって総和

	11月	12月	1月	2月
顧客1	33回	95回	83回	3回
顧客2				2回
顧客3	35回	57回		35回
顧客4			2回	
顧客5	40回	68回		10回

$$(\text{顧客1の再識別成功確率}) = \frac{1}{3} \times \frac{1}{2} = \frac{1}{6}$$

$$\text{評価値の期待値} = \frac{1}{6} + \frac{1}{2} + \frac{1}{3} + 1 + \frac{1}{3} = \frac{7}{3} = 2.33$$

名前，購入日，単価の加工(3/3)

	11月	12月	1月	2月
顧客1	33回	95回	83回	3回
顧客2				2回
顧客3	35回	57回		35回
顧客4			2回	
顧客5	40回	68回		10回

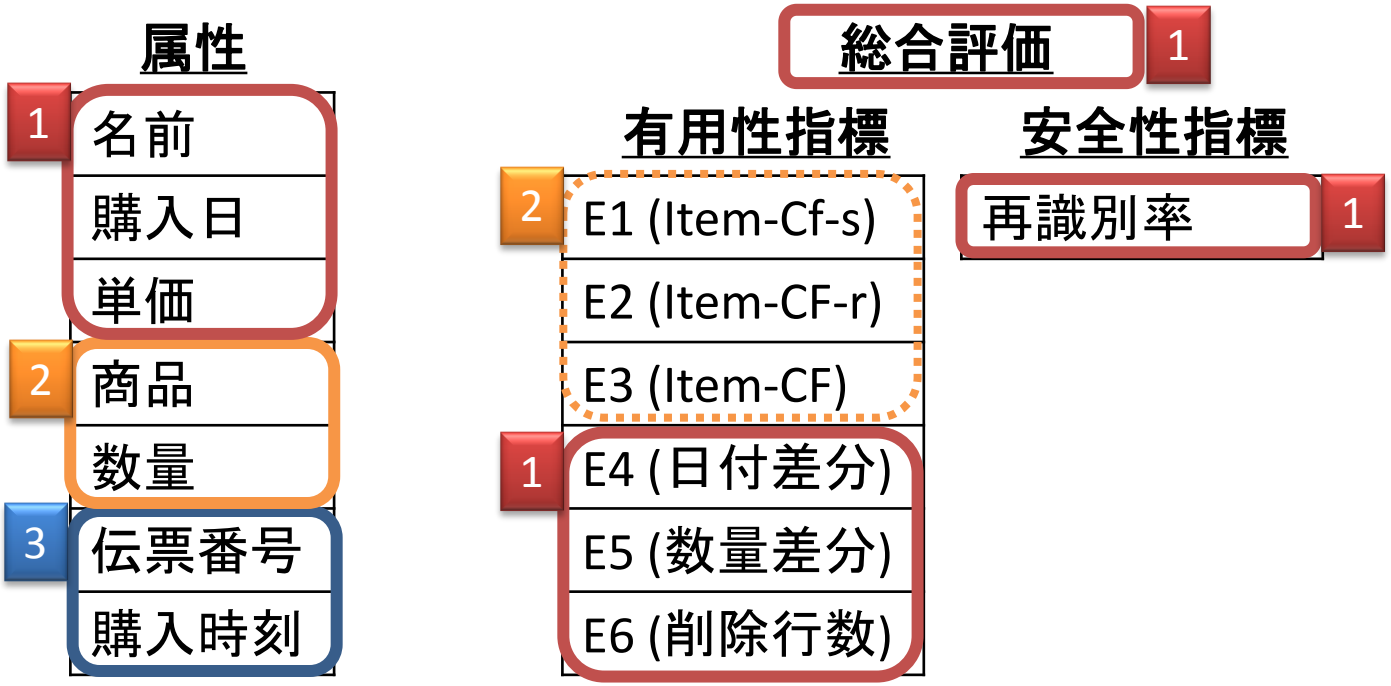
- 保護対象とグループ分けが決まると・・・
  - 有用性指標 E4, E5, E6 が計算できる
  - 安全性評価値の期待値が計算できる

➔ 総合評価の期待値が計算できる

➔ 総合評価が小さくなるグループ分けを探索

加工アルゴリズムの流れ

1. 名前，購入日，単価の加工
2. 商品，数量の加工
3. 伝票番号，購入時刻の加工



「君の名は~ユアネーム~」の再識別手法

再識別a: おひとり様狙い

12365,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL
12373,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL
12378,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL
12384,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL
12393,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL
12412,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL
12455,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL
12483,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL
12513,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL
12566,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL
12579,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL,DEL

- 目論見: 消された「おひとり様」を確実に当てる！
- 結果: あまり当たらず

再識別b: 貪欲法

- 月を多くまたぐ仮名から貪欲的に顧客推定
  - 最も近い(行数，日，単価)の顧客と推定

加工データの集計表

	11月	12月	1月	2月
仮名1	2回	3回		
仮名2				5回
仮名3	10回		15回	7回
仮名4		6回		

元データの集計表

	11月	12月	1月	2月
顧客1	仮3	8回	仮3	仮3
顧客2				18回
顧客3	仮1	仮1		

- 結果:
  - いくつか相性のいいチームがあった(半数程度正解)
  - しかし上位のチームには歯が立たず

アルゴリズム公開/非公開

背景: アルゴリズムの公開･非公開

匿名化界隈では･･･

アルゴリズムを隠せば
より安全じゃない？

公開するべき！

– どちらの意見もそれなりに存在

暗号業界では･･･

公開して当然！

アルゴリズムが知られても
安全でなきゃダメ！

– DESをはじめ多くの現代暗号はアルゴリズム公開

目的・手段

目的:

匿名化アルゴリズムの公開と非公開で
安全性がどれくらい違うかを調べる

でもどうやって？

➔「君の名は~ユアネーム~」の加工アルゴリズムを
PWS Cup 担当委員が再識別

再識別アルゴリズム概要

入力: 元データ，匿名化データ，各評価値，
コンテストルール，[匿名化アルゴリズム]
出力: 名前と仮名の対応付け

再識別アルゴリズム一覧

手法名	匿名化手法	検討期間	試行回数	再識別数(平均値)	再識別数(最大値)	試行回数	再識別数(最大値)
PWS Cup	**見ない**	≤1時間	30	-	19	3	19
						3	19
						2	15
						8	12
						6	10
						4	8
						3	5
						1	3
(見積もり)	**見る**	-	-	**40**	-		

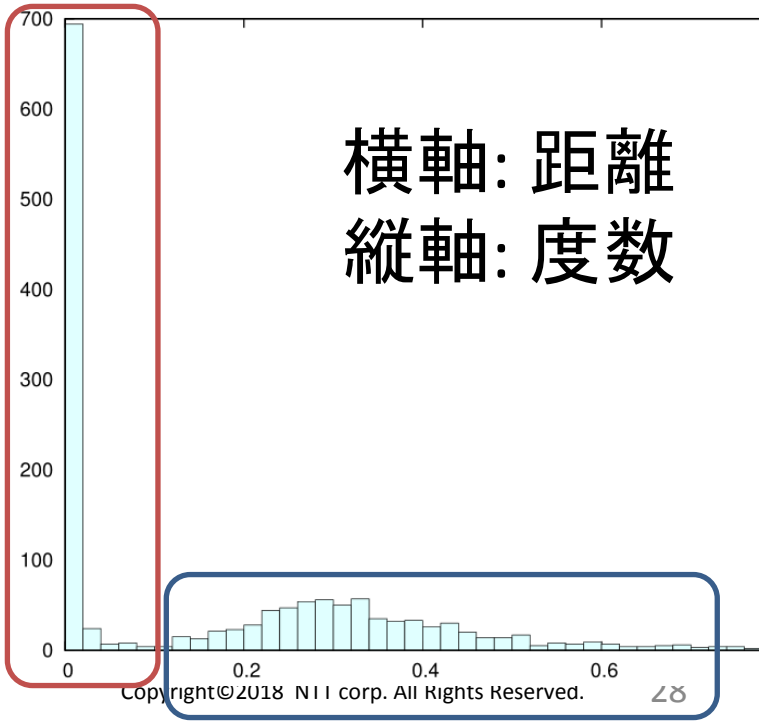
再識別3(加工アルゴリズムを見ない)

観察: ほぼ**無加工**と**全然違う**値が混在

方針: 匿名化データを2種に分けて処理

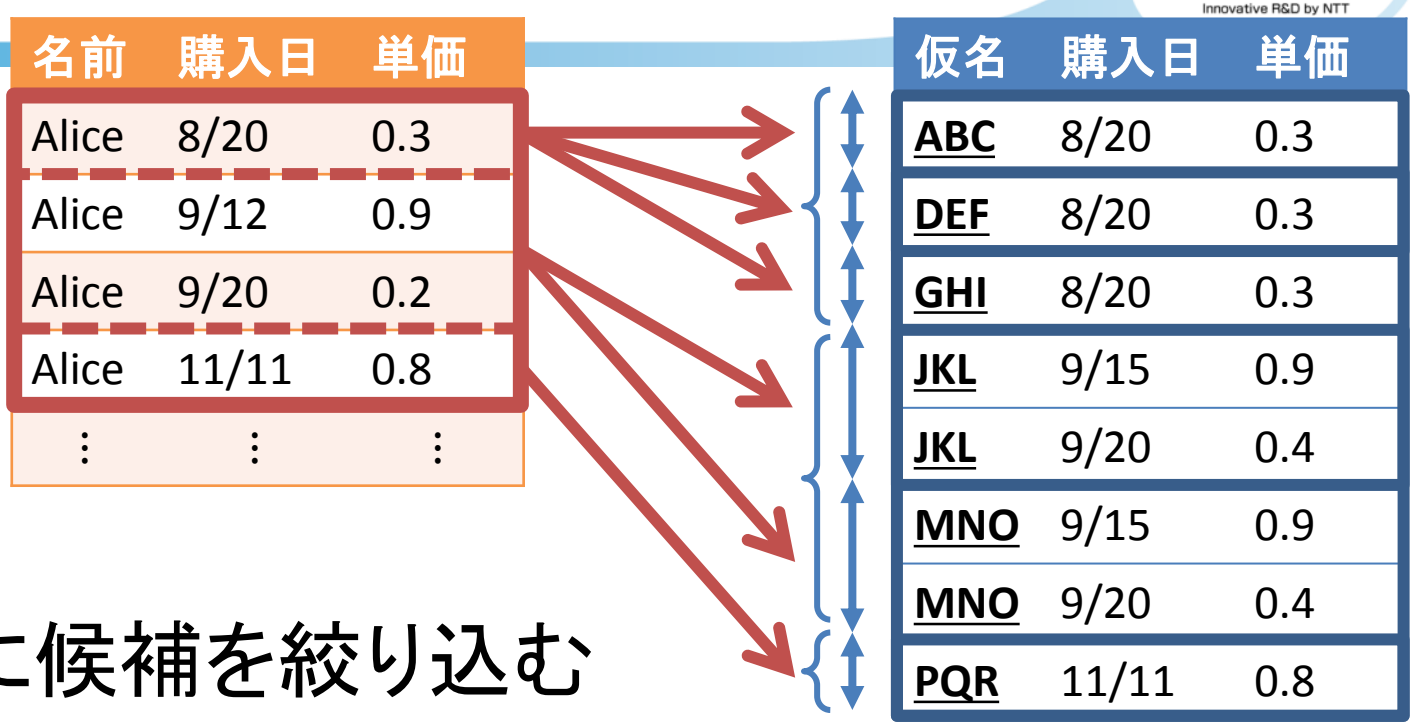
- **加工少な目**な仮名→近い名前を推測
- **加工多め**の仮名→ ランダムな名前を推測

- 匿名化データの分類:
  (仮名,月)ごとに
  最も近い(名前,月)との距離



横軸: 距離
縦軸: 度数

再識別5(加工アルゴリズムを見た)



1. 月ごとに候補を絞り込む
   - 匿名化アルゴリズムの特徴を利用
     - 1ヶ月単位で分割
     - レコード数はあまり減らない
2. 候補内からランダムに選択

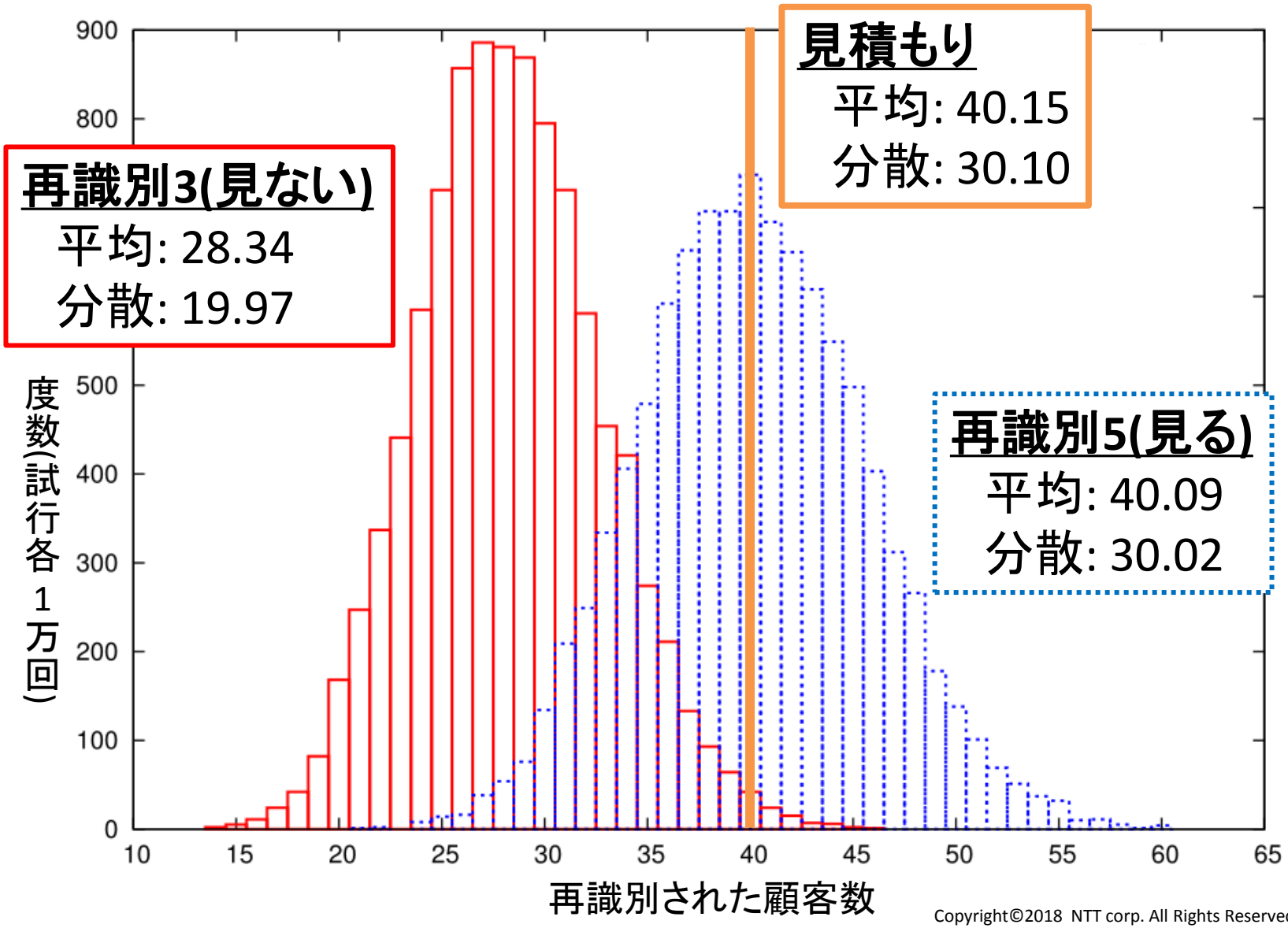
➔ (1.が正しければ)見積もりくらい再識別できる

結果(1/2): 各手法の再識別率

手法名	匿名化手法	検討期間	試行回数	再識別数(平均値)	再識別数(最大値)
PWS Cup	**見ない**	≤1時間	30	-	19
再識別2	**見ない**	≥ 10日	1	25	25
再識別3	**見ない**	≥ 10日	10000	**29**	46
再識別4-1	**見る**	-	10	28	34
再識別4-2	**見る**	-	10	29	37
再識別4-3	**見る**	-	10	28	32
再識別4-4	**見る**	-	10	29	43
再識別4-5	**見る**	-	10	29	35
再識別5	**見る**	-	10000	**40**	60
(見積もり)	**見る**	-	-	**40**	-

試行回数	再識別数(最大値)
3	19
3	19
2	15
8	12
6	10
4	8
3	5
1	3

結果(2/2): 見ない，見る，見積もりの比較



まとめ

- 「君の名は~ユアネーム~」の加工・再識別
- 加工アルゴリズムを知っていたら？の検証

- 委員のみなさま，参加者のみなさま，
  ありがとうございました.