背景知識の違いによる匿名加工データの攻撃者モデルの分類と評価

伊藤 聡志[1]　菊池 浩明[1]　中川裕志[2]

概要：データを匿名加工する際，そのデータを悪用しようとする攻撃者を想定する必要がある．攻撃者は背景知識を用いて匿名加工データから個人を再識別しようとするが，どんな背景知識を持つ攻撃者の危険度が高いのかは不明であった．本稿では背景知識の違いによって攻撃者モデルを１０タイプに分け，仮名化のみをした購買データ Online Retail Data Set を用いてそれらの危険度を識別確率の期待値によって評価する．

キーワード：匿名加工，再識別，攻撃者，購買データ

Evaluation of some Attacker models with distinct Background Knowledge of De-identified Dataset

Satoshi Ito[1]　Hiroaki Kikuchi[1]　Hiroshi Nakagawa[2]

Abstract: Before de-identifying datasets, we should suppose attackers who try to use the datasets for wrong purpose. The risk of attackers re-identify individuals from de-identified dataset depends on what background knowledges they have. However, it is not known what kind of background knowledge raises risk of re-identified most. In this paper, we model attackers with representative 10 types with distinct background knowledges. We evaluate risk of these attackers for Online Retail Data Set by mean of probability of record to be identified.

Keywords: De-identification, Re-identification, Attacker, Transaction Data

1. はじめに

企業や組織は収集した顧客データやトランザクションデータを利活用する際，そのデータのリスク評価と匿名加工を行う必要がある．匿名加工は顧客データのような個人情報データから個人が特定されないように，データを加工することであるが，そのためにはデータを悪用しようとする攻撃者を想定する必要がある．例えば，購買データを想定した匿名加工に [1][2] がある．攻撃者は背景知識を用いて匿名加工データから個人を再識別しようとするが，どんな背景知識を持つ攻撃者の危険度が高いのかは不明であった．

既存の攻撃者モデルとして，Domingo Ferrer らによって提案されている最大知識攻撃者モデル（maximum-knowledge attacker）[3] がある．最大知識攻撃者モデルでは元データと匿名加工されたデータの全体を背景知識として持つ攻撃者を想定しているが，これは現実的ではなく，新たな攻撃者モデルを考える必要がある．しかし，攻撃者モデルは対象のデータや仮定によって大きく異なり，想定するのは非常に困難である．

そこで本研究の目的を，背景知識の違いによる攻撃者の危険度の調査とする．UCI Machine Learning Repository から公開されている購買データ Online Retail Data Set の 400 人分に対し，背景知識の異なる代表的な 10 タイプの攻撃者を想定し，それらの危険度を個人識別確率によって評

[1] 明治大学
Meiji University, Nakano, Tokyo, 4-21-1
[2] 東京大学
Tokyo University, Bunkyo, Tokyo, 7-3-1

表 1　購買履歴データ T の概要

属性	内容
顧客 ID	購買をした顧客の ID（5 桁数値）
伝票 ID	購買伝票の ID（6 桁数値）
購買日	購買した年月日（yyyy/mm/dd）
購買時	購買した時分（hh:mm）
購買商品	購買した商品の ID（数値，文字）
単価	購買した商品の単価 ($)
個数	商品を購買した個数

価する．この研究によって，どういった背景知識を持つ攻撃者が危険であるかが判明し，攻撃者の危険度の評価に役立つ．本研究の新規性は，理論値によるリスクモデルの設計と，実データを用いたリスク評価である．本研究の主要な貢献は，ある属性の背景知識を持つ攻撃者による平均識別率は，ある仮定の下で，その属性の持つユニークな値の数と履歴のレコード数のみによって決定することを証明したことである．この仮定の妥当性については，実験的に検証する．

本稿では，2 章で Online Retail Data Set の説明と分析を行い，3 章で 10 タイプの攻撃者の説明をし，4 章で攻撃者の危険度を分析する．

2. Online Retail Data Set

UCI Machine Learning Repository[4] から公開されている Online Retail Data Set は．英国の 1 年間の購買履歴のデータである．このデータは匿名加工・再識別コンテスト PWSCUP[2] で用いられており，その際にコンテスト用に加工されている．本研究では PWSCUP2016 で用いられた，400 人分の購買履歴データ T を用いる．表 1 に T の概要を示す．また，表 2 に T の例を示し，表 3 に T の統計量を示す．

3 章で検討する攻撃者は，この履歴データについて，購買日，一日当たりの購買商品の種類数，一日当たりの購買商品の 3 種類の属性とその組み合わせの背景知識によって類型化されている．そこで，T についてのこれらの属性の分布も以下に示し，表 4 にこれらの属性の統計量を示す．

図 1 に T における購買日の出現頻度を示す．横軸の数値は月を示す．購買日の値域は 2010/12/1 から 2011/12/9 までの 373 日間であるが，そのうち購買があるのは 290 日であり，購買が存在しない日もある．

図 2 に T における購買種類数の出現頻度を示す．購買種類数とは 1 日の購買で同時に買われた商品の種類数である．例えば T では，1 種類の購買が最も多く，71 回行われている．T では 114 種類の種類数が生起する．

図 3 に T における購買商品の出現頻度を示す．横軸は頻度の順位を示す．例えば，T で 2781 種類の商品が出現するが，最も多く購買されている商品は 1000 回以上買われている．

表 2　購買履歴データ T の例

顧客 ID	伝票 ID	購買日	購買時	購買商品	単価	個数
12583	536370	2010/12/1	8:45	22728	3.75	24
12583	536370	2010/12/1	8:45	22727	3.75	24
12431	536389	2010/12/1	10:03	22941	8.5	6
12431	536389	2010/12/1	10:03	21622	4.95	8
12431	536389	2010/12/1	10:03	21791	1.25	12
12838	536415	2010/12/1	11:57	22952	0.55	10
12567	537065	2010/12/5	11:57	22837	4.65	8
12567	537065	2010/12/5	11:57	22846	16.95	1
12748	537429	2010/12/6	15:54	84970S	0.85	12
12748	537429	2010/12/6	15:54	22549	1.45	8

表 3　購買履歴データ T,T_2 の統計量

項目	Online Retail T	トイデータ T_2
レコード数 m	38087	10
顧客数 n	400	3
商品数 ω_{goods}	2871	4
購入日 ω_{day}	2010/12/1-2011/12/9	2010/12/1-2010/12/3

表 4　T の 3 種類の属性値の統計量

属性	購買日	購買種類数	購買商品
種類数 ω	290	114	2781
頻度平均値	5.4	13.75	13.7
頻度最大値	21	71	1012
頻度最頻値	5	1	1

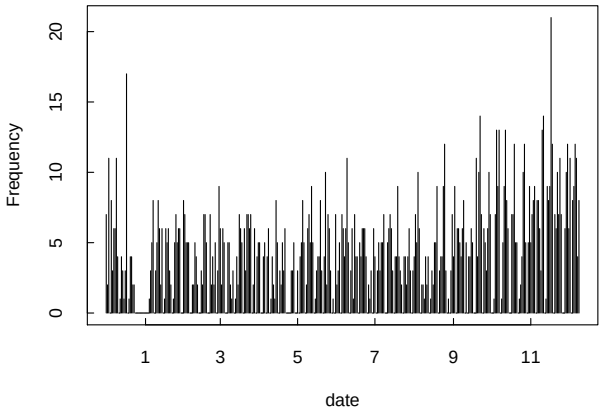

図 1　T における出現頻度の日付分布

3. 背景知識の異なる 10 タイプの攻撃者

購買履歴データ T に対し，背景知識の異なる 10 タイプの攻撃者を想定する．購買履歴データ T を顧客 ID・購買日について，購買商品を整理したデータ $T_{(id,day)}$ を考える．攻撃者は，$T_{(id,day)}$ からある顧客 u についての背景知識を得て，仮名化された T から u を識別しようと試みる場合を想定する．説明のために，表 5 の仮名化された簡易的な購買履歴データ T_2 と，それを変換した表 6 の $T_{2(id,day)}$ を考えよう．

3.1 節で T における背景知識の説明をし，3.2 節で各攻撃者の説明を T_2 と $T_{2(id,day)}$ を用いて行う．

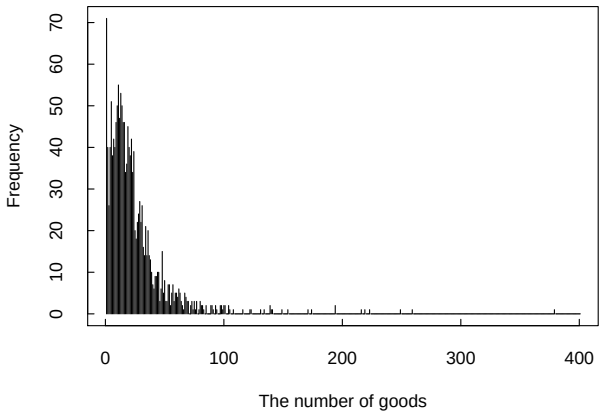

図 2 T における一日当たりの購買商品種類数の頻度分布

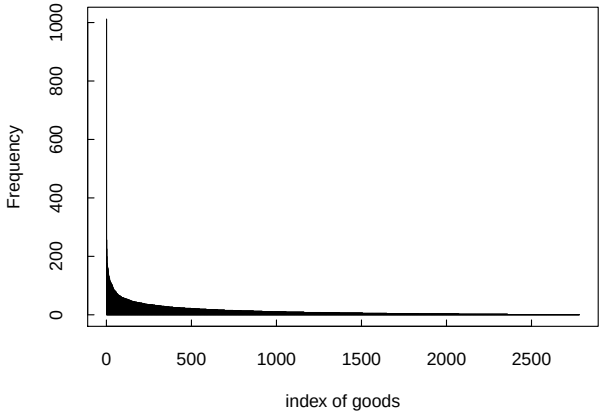

図 3 T における購買商品の頻度分布

表 5 小規模購買履歴データ T_2

仮名	伝票 ID	購買日	購買時	購買商品	単価	個数
1	100	2010/12/1	8:45	パン	1.45	2
1	100	2010/12/1	8:45	本	3.75	1
1	200	2010/12/1	20:10	お茶	0.85	2
2	300	2010/12/1	10:03	パン	1.45	3
1	400	2010/12/2	15:07	お茶	0.85	3
3	500	2010/12/2	11:57	パン	1.45	4
3	500	2010/12/2	11:57	ジュース	1.25	4
3	600	2010/12/3	15:54	本	3.75	1
3	600	2010/12/3	15:54	お茶	0.85	10
3	600	2010/12/3	15:54	ジュース	1.45	10

表 6 T_2 の仮名と購買日についての購買商品の表 $T_{2(id,day)}$

仮名 \ 購買日	2010/12/1	2010/12/2	2010/12/3
1	パン，本，お茶	お茶	
2	パン		
3		パン，ジュース	本、お茶，ジュース

3.1 T における背景知識

攻撃者が得る可能性のある T についての背景知識について考える．T の 7 属性は，大きく「誰が買ったか（顧客 ID，伝票 ID）」，「いつ買ったか（購買日，購買時）」，「何を買ったか（購買商品，単価，個数）」の 3 種類の情報に分類することができる．しかし 3 つのうち，攻撃者が「誰が買ったか」の情報を背景知識として得ることは考えにくいため，背景知識として得る可能性のあるのは「いつ買ったか」，「何を買ったか」についての情報であると考えられる．本研究では，これら 2 グループそれぞれの代表的な「購買日」，「購買商品」の 2 属性に加え，顧客が 1 日の購買で商品を「何種類買ったか」という情報に注目し，これらを攻撃者が得る背景知識として想定している．

「いつ買ったか」は知っている・知らないの 2 通り，「何種類買ったか」は知っている・知らないの 2 通り，「何を買ったか」は知らない・1 商品知っている・全商品知っているの 3 通りであるため，これらを組み合わせると 12 通りの攻撃者ができる．しかし，「何種類買ったか」を知らないのに「何を買ったか」を全て知っているのは矛盾するため，それらを除いて攻撃者のタイプは表 7 の 10 タイプになる．

表 7 10 タイプの攻撃者

攻撃者	いつ	何種類	何を
0	×	×	×
1	×	×	1 商品
2	×	○	×
3	×	○	1 商品
4	×	○	全て
5	○	×	×
6	○	×	1 商品
7	○	○	×
8	○	○	1 商品
9	○	○	全て

3.2 10 タイプの攻撃者

3.2.1 攻撃者 0（無知識）

攻撃者 0 は背景知識を一切持っていない攻撃者である．T_2 の顧客数を $n = 3$ とすると，攻撃者 0 は n 人の顧客からランダムに u を識別するため，u を識別できる確率は，$\frac{1}{n} = \frac{1}{3}$ である．

3.2.2 攻撃者 1（1 商品）

攻撃者 1 は，u が購買した商品を 1 種類だけ知る攻撃者である．例えば攻撃者 1 が「u はお茶を買った」という背景知識を持っている場合，T_2 でお茶を購買している顧客は仮名 1,3 の 2 人だけなので，このどちらかが u である．この場合，攻撃者 1 が背景知識から u を識別できる確率は $\frac{1}{2}$ である．

3.2.3 攻撃者 2（何種類）

攻撃者 2 は，u が 1 日に何種類の商品を購買したかを知る攻撃者である．例えば攻撃者 2 が「u はある日，3 種類の商品を購買した」という背景知識を持っている場合，T_2 で 1 日に 3 種類の商品を購買しているのは仮名 1,3 の 2 人だけなので，このどちらかが u である．この場合，攻撃者 2 が背景知識から u を識別できる確率は $\frac{1}{2}$ である．

3.2.4 攻撃者 3（何種類，1 商品）

攻撃者 3 は，u のある 1 日の購買商品種類数と，購買し

た商品を 1 種類だけ知る攻撃者である．例えば攻撃者 3 が「u はある日，3 種類の商品を購買し，その内 1 種類はお茶である」という背景知識を持っている場合，T_2 でこれに当てはまるのは仮名 1,3 の 2 人だけなので，このどちらかが u である．この場合，攻撃者 3 が背景知識から u を識別できる確率は $\frac{1}{2}$ である．

3.2.5 攻撃者 4（何種類，全商品）

攻撃者 4 は，u のある 1 日の購買商品種類数と，その日購買した商品を全て知る攻撃者である．例えば攻撃者 4 が「u はある日，3 種類の商品を購買し，その内容はパン，お茶，本である」という背景知識を持っている場合，T_2 でこれに当てはまるのは仮名 1 だけなので，仮名 1 が u である．この場合，攻撃者 4 が背景知識から u を識別できる確率は 1 である．

3.2.6 攻撃者 5（いつ）

攻撃者 5 は，u がいつ購買したかを 1 日分だけ知る攻撃者である．例えば攻撃者 5 が「u は 2010/12/1 に購買をした」という背景知識を持っている場合，T_2 で 2010/12/1 に購買をしているのは仮名 1,2 の 2 人だけなので，このどちらかが u である．この場合，攻撃者 5 が背景知識から u を識別できる確率は $\frac{1}{2}$ である．

3.2.7 攻撃者 6（いつ，1 商品）

攻撃者 6 は，u がいつ購買したかを 1 日分と，その日購買した商品の 1 つを知る攻撃者である．例えば攻撃者 6 が「u は 2010/12/1 に本を買った」という背景知識を持っている場合，T_2 でこれに当てはまるのは仮名 1 だけなので，これが u である．この場合，攻撃者 6 が背景知識から u を識別できる確率は 1 である．

3.2.8 攻撃者 7（いつ，何種類）

攻撃者 7 は，u がいつ購買したかを 1 日分と，その日に購買した種類数を知る攻撃者である．例えば攻撃者 7 が「u は 2010/12/1 に 1 種類の商品を買った」という背景知識を持っている場合，T_2 でこれに当てはまるのは仮名 2 だけなので，仮名 2 が u である．この場合，攻撃者 7 が背景知識から u を識別できる確率は 1 である．

3.2.9 攻撃者 8（いつ，何種類，1 商品）

攻撃者 8 は，u がいつ購買したかを 1 日分と，その日に購買した種類数と，購買した商品を 1 種類だけ知る攻撃者である．例えば攻撃者 8 が「u は 2010/12/1 に 3 種類の商品を買い，そのうち 1 種類はパンである」という背景知識を持っている場合，T_2 でこれに当てはまるのは仮名 1 だけなので，仮名 1 が u である．この場合，攻撃者 8 が背景知識から u を識別できる確率は 1 である．

3.2.10 攻撃者 9（いつ，何種類，全商品）

攻撃者 9 は，u がいつ購買したかを 1 日分と，その日に購買した種類数と，購買した商品を全て知る攻撃者である．例えば攻撃者 9 が「u は 2010/12/1 に 3 種類の商品を買い，その内容はパン，本，お茶である」という背景知識を持っている場合，T_2 でこれに当てはまるのは仮名 1 だけなので，仮名 1 が u である．この場合，攻撃者 9 が背景知識から u を識別できる確率は 1 である．

4. 攻撃者の危険度の評価

4.1 平均識別確率

本研究では攻撃者の危険度として，背景知識 X を持つ攻撃者により，履歴 T から任意の顧客 u が識別される確率の期待値を用い，これを平均識別確率と呼ぶ．またその際，攻撃者が各背景知識を得る確率はその知識の T_2 における頻度に比例すると仮定する．

例として，攻撃者 5 が $T_{2(id,day)}$ から得られる背景知識とその生起確率を表 8 に示す．$T_{2(id,day)}$ の場合，攻撃者 5 が得る可能性のある背景知識は「2010/12/1 に買い物をした」，「2010/12/2 に買い物をした」，「2010/12/3 に買い物をした」の 3 種類だが，それぞれの確率は異なり，頻繁に起きていることについての背景知識は得やすい．また，表 8 に各背景知識に当てはまる人数と u が識別される確率を示す．例えば，攻撃者 5 が「u は 2010/12/3 に買い物をした」という背景知識を得た場合，2010/12/3 に買い物をしているのは仮名 3 だけなので，u を識別できる確率は 1 となる．各背景知識の生起確率と識別確率，識別確率の期待値を表 8 に示す．この場合，攻撃者 5 は「u は 2010/12/3 に買い物をした」という背景知識を 0.3 の確率で得て，その背景知識によって u が識別される確率は 1 であるため，この背景知識によって u を識別される確率は $0.3 * 1 = 0.3$ となる．また，全ての履歴についての背景知識の識別確率の期待値を T_2 に対する攻撃者 5 の危険度とする．この場合，攻撃者 5 の危険度は 0.65 であり，これはこの攻撃者が u についての背景知識を得たとき，平均 65% の確率で u を識別できることを意味する．

また，T_2 に対する攻撃者 3 について考える．攻撃者 3 が $T_{2(id,day)}$ から得られる背景知識を表 9 に示す．例えば，「3 種類，本」の購買は 2 回生起しており，その生起確率は $\frac{2}{10} = 0.2$ である．また，「3 種類，本」に当てはまる顧客の人数は 2 人であり，識別確率は 0.5 である．そして，T_2 の場合，攻撃者 3 の危険度は 0.8 である．この場合は履歴に記録される回数=当てはまる人数となっているが，そうでない場合もあることに注意せよ．例えば仮名 1 が 3 日間毎日本のみを買っていた場合，「1 種類，本」の出現回数は 3 回になるが，当てはまる人数は 1 人である．

4.2 平均識別確率の理論値

定義 4.1 背景知識 X の要素 x について，履歴 T で x を満たすレコード（行）の集合を R_x．x を満たす顧客の集合を U_x とする．

例 4.1 T_2 の場合，$X = \{2010/12/1, 2010/12/2, 2010/12/3\}$ について，x = 2010/12/1 のとき，$R_x = \{1, 2, 3, 4\}$，

$U_x = \{1, 2\}$ である．

仮定 4.1 $|R_x| = |U_x|$ である．

例 4.2 T_2 の場合，X=「いつ買ったか」であるとき，仮定 4.1 が成立するのは 0 回，成立しないのは 3 回である．

「いつ買ったか」,「何種類買ったか」,「何を買ったか」のうち，1 種類のみの背景知識 X を持つ攻撃者の平均識別確率は次の定理で与えられる．

定理 4.1 仮定 4.1 のもと，購買履歴データ T について，単一の背景知識 X を持つ攻撃者の平均識別確率 $Pr(\text{identify}|X)$ は，

$$Pr(\text{identify}|X) = \frac{\omega_X}{m}$$

である．

(Proof) x を X の要素とし，T で x が生起しているレコードの集合を R_x，T で x に当てはまる仮名の集合を U_x，$\omega_X = |X|$ としたとき，攻撃者の平均識別確率は

$$Pr(\text{identify}|X) = \sum_{x \in X} \frac{|R_x|}{m} \frac{1}{|U_x|}$$

である．このとき，$|U_x| = |R_x|$ と仮定すると，

$$Pr(\text{identify}|X)' = \sum_{x \in X} \frac{1}{m} = \frac{\omega_X}{m}$$

となり，定理 4.1 が成り立つ． (Q.E.D)

例 4.3 T_2 を用いて定理 4.1 の説明を行う．X =「いつ買ったか」とする．例えば x =「2010/12/1 に買った」とすると，$R_x = \{1, 2, 3, 4\}$,$U_x = \{1, 2\}$ である．また，$m = 10$, $\omega_X = 3$ であるため，x を背景知識として持つ攻撃者の平均識別確率は $\frac{1}{|U_x|} = \frac{1}{2}$ であり，その生起確率は $\frac{|R_x|}{m} = \frac{4}{10}$ である．よって，「いつ買ったか」を背景知識として持つ攻撃者の平均識別確率は

$$Pr(\text{identify}|X) = \sum_{x \in X} \frac{|R_x|}{m} \frac{1}{|U_x|} = \frac{4 + 3 + 6}{20} = 0.65$$

となる．また，$|U_x| = |R_x|$ と仮定すると，

$$Pr(\text{identify}|X)' = \sum_{x \in X} \frac{1}{m} = \frac{\omega_X}{m} = 0.3$$

となる．

定理 4.2 仮定 4.1 のもと，購買履歴データ T について，背景知識 X と独立な Y を同時に持つ攻撃者の平均識別確率 $Pr(\text{identify}|X, Y)$ は，

$$Pr(\text{identify}|X, Y) = \frac{\omega_X \omega_Y}{m}$$

である．

(Proof) x を X の要素とし，y を Y の要素とする．T で x が生起しているレコードの集合を R_x，T で x に当てはまる仮名の集合を U_x としたとき，背景知識 X, Y が同時に発生する確率は独立性を仮定すると，$Pr(X, Y) = Pr(X)Pr(Y) = \frac{|R_X|}{m} \frac{|R_Y|}{m}$ である．また，仮定 4.1 をおくと，その背景知識に当てはまる人数は $m \frac{|R_X|}{m} \frac{|R_Y|}{m}$ であるため，リスクは $\frac{1}{m \frac{|R_X|}{m} \frac{|R_Y|}{m}}$ となる．よって，X, Y を同時に持つ攻撃者の平均識別確率は

$$\begin{aligned} Pr(\text{identify}|X, Y) &= \sum_{x \in X} \sum_{y \in Y} \frac{\frac{|R_X|}{m} \frac{|R_Y|}{m}}{m \frac{|R_X|}{m} \frac{|R_Y|}{m}} \\ &= \sum_{x \in X} \sum_{y \in Y} \frac{1}{m} \\ &= \frac{\omega_X \omega_Y}{m} \end{aligned}$$

となり，定理 4.2 が成り立つ． (Q.E.D)

例 4.4 T_2 を用いて定理 4.2 の説明を行う．X =「いつ買ったか」とし，Y =「何種類買ったか」とする．例えば x =「2010/12/1 に買った」，y =「1 種類買った」とすると，$R_x = \{1, 2, 3, 4\}$，$U_x = \{1, 2\}$，$R_y = \{1, 2\}$，$U_x = \{4, 5\}$ である．また，$m = 10$，$\omega_X = 3$，$\omega_Y = 3$ であるため，x と y を背景知識として持つ攻撃者の識別確率は仮定 4.1 をおき，独立性を仮定すると $\frac{1}{m \frac{|R_x|}{m} \frac{|R_y|}{m}} = \frac{10}{8}$ であり，その生起確率は $\frac{|R_x|}{m} \frac{|R_y|}{m} = \frac{8}{100}$ である．よって，「いつ買ったか」と「何種類買ったか」を背景知識として持つ攻撃者の平均識別確率は $Pr(\text{identify}|X, Y)' = \frac{\omega_X \omega_Y}{m} = 0.9$ となる．

定理 4.3 仮定 4.1 のもと，購買履歴データ T について，独立に発生する複数の背景知識 $X_1, X_2, \cdots, X_k$ を持つ攻撃者の平均識別確率 $Pr(\text{identify}|X_1, X_2, \cdots, X_k)$ は，

$$Pr(\text{identify}|X_1, X_2, \cdots .X_k) = \frac{\omega_{X_1} \omega_{X_2} \cdots \omega_{X_k}}{m}$$

である．（証明略）

4.3 Online Retail についての攻撃者の危険度の実測値

表 10 に購買履歴データ T に対する各攻撃者の危険度を示す．実測値は 4.1 節の例と同様の手順で実際に求めた攻撃者の危険度（平均識別確率）であり，理論値は 4.2 節の定理を用いて求めた値である．T の場合，表 4 より $\omega_{day} = 290$，$\omega_{num} = 114$，$\omega_{goods} = 2781$ である．

攻撃者 1,2,5 は順に「何種類買ったか」,「何を買ったか（1 商品）」,「いつ買ったか」を背景知識として知る攻撃者だが，その中では攻撃者 5 の危険度が最も高く，0.1851 であった．また，攻撃者の危険度は複数の種類の背景知識を持つことで大きく上昇した．

4.4 考察

4.4.1 実測値と理論値について

表 11 に平均識別確率の実測値と理論値に基づく攻撃者のランクを示す．どちらの場合も最も危険度が低いのは攻撃者 0（何も知らない）であるが，最も危険度が高い攻撃者は異なり，理論値の場合は攻撃者 8（いつ，何種類，商品 1 品を知っている），実測値の場合は攻撃者 9（いつ，何

種類，商品全てを知っている）となった．しかし，攻撃者 8 の背景知識量は明らかに攻撃者 9 より少なく，危険度も攻撃者 9 の方が高くなるのが自然である．

また，表 10 より，平均識別確率の実測値と理論値は誤差が非常に大きく，理論値の値が 1 を超えてしまうものもある．その理由は，「算出方法が異なること」と「不自然な仮定をおいていること」だと考えられる．

攻撃者と理論値の実測値と理論値の算出方法は異なり，例えば実測値では背景知識 x の生起確率 p_x を

$$p_x = \frac{x \text{ の生起する回数}}{\text{背景知識の生起回数の合計}}$$

としているが，理論値では p_x を

$$p_x = \frac{T \text{ の } x \text{ についてのレコード数}}{T \text{ のレコード総数}} = \frac{|R_x|}{m}$$

としている．

また，理論値では 2 つの大きな仮定を置いている．「背景知識の生起する回数と当てはまる人数が等しいこと（$|U_x| = |R_x|$）」と「独立性（$Pr(X,Y) = Pr(X)Pr(Y)$）」である．図 4，5，6 に，それぞれ「いつ買ったか」，「何種類買ったか」，「何を買ったか」についての，生起頻度と当てはまる人数の散布図を示す．相関係数は順に 1.0，0.985，0.924 であり，いずれも強い相関がある．このことから，背景知識の生起する回数と当てはまる人数が等しい仮定 4.1 は成立していると考えられる．

しかし，独立性の仮定には大きな問題がある．独立性を仮定すると，背景知識「x かつ y」の生起確率は $p_x p_y$ となり，これは 0 にならない．しかし実際のデータでは背景知識 $x \in X$ と $y \in Y$ の組み合わせの中には生起しないものも非常に多い．例えば T の購買日と購買種類数に注目した $T_{(day,num)}$ を考えると，$\omega_{day} = 290$，$\omega_{num} = 114$ より，$\omega_{day}\omega_{num} = 33060$ となるが，このうち背景知識として生起するのは 1473 種類のみ（0.46%）であった．このことより，独立性の仮定は不自然であると考えられる．

4.4.2 攻撃者の背景知識について

本研究では，ある顧客の 3 種類の属性についての情報の 1 日分を背景知識として持つ弱い攻撃者を想定している．しかし現実の場合は，攻撃者は複数日・複数人分の情報を背景知識として持つことが想定できる．

また，攻撃者が「何を買ったか」についての情報を「知らない」，「1 商品知っている」，「全て知っている」の 3 つの場合に分類しているが，「k 商品知っている」時のリスクは想定できていない．

5. おわりに

Online Retail Data Set の 400 人分の購買履歴データ T に対し，背景知識の異なる 10 タイプの攻撃者を想定し，それらの危険度（平均識別確率）の実測値を求め，実際に各攻撃者の T に対する危険度を調査した．その結果，「いつ買ったか」，「何種類買ったか」，「何を買ったか（1 商品）」という情報のうち，「いつ買ったか」という背景知識を持つ攻撃者の危険度が高いことが判明した．また，複数の種類の背景知識を持つことで攻撃者の危険度は大きく上がることが判明した．

また，攻撃者の危険度の理論値を，「背景知識の生起する回数と当てはまる人数が等しいこと」と「独立性」を仮定して求めた．しかし，独立性の仮定は不自然であり，理論

表 8 T_2 に対する攻撃者 5 の危険度

背景知識	回数	生起確率	人数	識別確率	リスク
2010/12/1	2	0.4	2	0.5	0.2
2010/12/2	2	0.3	2	0.5	0.15
2010/12/3	1	0.3	1	1	0.3
合計	5	1			0.65

表 9 T_2 に対する攻撃者 3 の背景知識

背景知識	頻度	生起確率	人数	識別確率	リスク
1 種，パン	1	0.1	1	1	0.1
1 種，お茶	1	0.1	1	1	0.1
2 種，パン	1	0.1	1	1	0.1
2 種，ジュース	1	0.1	1	1	0.1
3 種，パン	1	0.1	1	1	0.1
3 種，本	2	0.2	2	0.5	0.1
3 種，お茶	2	0.2	2	0.5	0.1
3 種，ジュース	1	0.1	1	1	0.1
合計	10	1			0.8

表 10 T に対する攻撃者 0〜9 の危険度

攻撃者	実測値	理論値
0	0.0025	0.0025
1	0.0965	0.0730
2	0.0807	0.0030
3	0.7974	8.3239
4	0.9788	4.5436
5	0.1851	0.0076
6	0.8945	21.1749
7	0.9400	0.8680
8	0.9750	2413.9433
9	0.9994	1317.6433

表 11 実測値と理論値についての攻撃者の危険度順位

順位	実測値	攻撃者
1	**9**	**8**
2	4	**9**
3	**8**	6
4	7	3
5	6	4
6	3	7
7	5	1
8	1	5
9	2	2
10	0	0

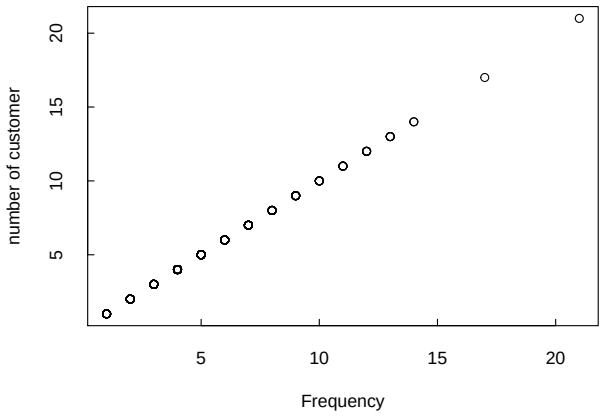

図 4 T における購買日の頻度と人数の散布図

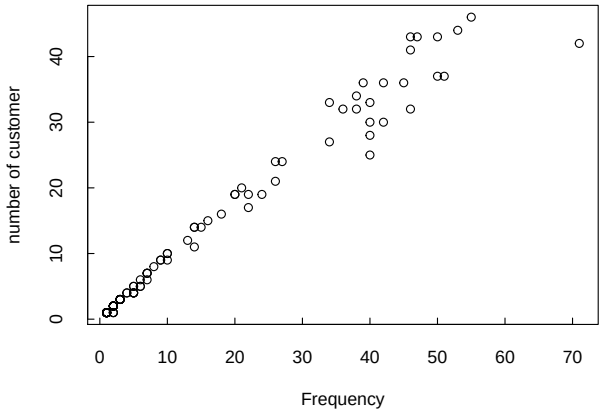

図 5 T における購買種類数の頻度と人数の散布図

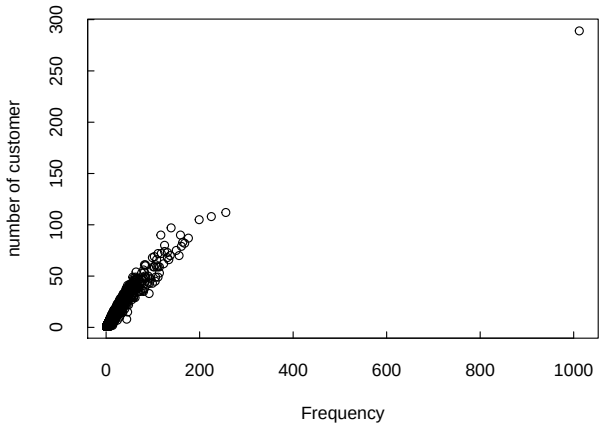

図 6 T における購買商品の頻度と人数の散布図

値の精度は悪くなった．

攻撃者のさらなる一般化や匿名加工を行った場合の攻撃者の危険度の変化，危険度の理論値の精度向上を今後の課題とする．

参考文献

[1] 菊池浩明，山口高康，濱田浩気，山岡裕司，小栗秀暢，佐久間 淳：“匿名加工・再識別コンテスト Ice & Fire の設計”，CSS 2015, pp.363-370, 2015.

[2] 菊池浩明，小栗 秀暢，野島 良，濱田 浩気，村上 隆夫，山岡 裕司, 山口 高康, 渡辺 知恵美：“PWSCUP:履歴データを安全に加工せよ”，CSS2016, pp.271-278, 2016.

[3] Josep Domingo-Ferrer, Sara Ricci and Jordi Soria-Comas, ”Disclosure Risk Assessment via Record Linkage by a Maximum-Knowledge Attacker”, 2015 Thirteenth Annual Conference on Privacy, Security and Trust (PST), *IEEE*, 2015.

[4] UCI Machine Leaning Repository `http://archive.ics.uci.edu/ml/index.php`, referred in 2017.