情報処理学会論文誌 Vol.60 No.9 1509–1517 (Sep. 2019)

仮名の再同定率に基づく仮名更新頻度の定量的評価

福嶋 雄也[1,a)] 北島 祥伍[1] 満保 雅浩[2]

受付日 2018年12月10日, 採録日 2019年6月11日

概要：近年，パーソナルデータの収集・活用に際し，データ所有者のプライバシを保護しようという動きが強まってきている．このような状況下で，データの匿名加工を行う技術や匿名性を評価する技術の重要性が高まってきているが，これらの研究はいまだ十分とはいいがたい．本論文では，特にWebサイトへのアクセス履歴データを対象とし，時分割による多重仮名化を行った際の仮名更新頻度の安全性について定量的に評価する手法を提案し，実データを用いて検証を行った．

キーワード：プライバシ保護，仮名化，安全性評価，Webアクセス履歴

A Quantitative Evaluation Method of Pseudonym Update by Using Re-identification Rate

Kazuya Fukushima[1,a)] Shogo Kitajima[1] Masahiro Mambo[2]

Received: December 10, 2018, Accepted: June 11, 2019

Abstract: Recently, the importance of privacy preservation to personal data is pointed out, in terms of data collection and/or utilization. Anonymisaiton techninques or anonymity evaluation techniques will increase its importance under such circumstance, but the research of these area is still not enough. In this paper, we especially foucsing on anonymity evaluation method of pseudonymisation, one of the anonymisation techniques. We present a quantitative evaluation method of safeness of pseudonym update on web-browsing history, and apply it to collected data.

Keywords: privacy preservation, pseudonymisation, safety evaluation, web-browsing history

1. はじめに

近年，情報通信技術の発達にあわせ，Google や Amazon 等の大手 IT 企業を中心として多くのパーソナルデータをユーザから収集しビジネスへと活用しているが，その反面，パーソナルデータの収集・活用に際してデータ所有者のプライバシを保護しようという動きが強くなってきている．2018 年には，EU で General Data Protection Regulation（GDPR）が施行され，所有者が EU 内にいるようなデータの処理と移転に大きな規制がかけられた．

このような状況下で，データの匿名化を行う技術の重要性がますます増大している．匿名化技術を活用しパーソナルデータの適切な利活用を行うためには，データの匿名性を定量的に評価する指標を導入することが重要だが，一方でこの指標に関する研究はいまだ十分とはいいにくい．

本論文では，特に Web アクセス履歴データを対象とし，多重仮名化において仮名が安全である期間を定量的に評価する指標を提案し，加えて実際に収集した Web アクセス履歴データに対して提案手法を適用し評価を行う [11]．

2. 背景

2.1 関連研究

匿名性の評価指標として代表的なものに k-anonymity [1] と Differential Privacy [3] があり，加えてこれらの拡張や関連性に関しても多くの研究がある [5], [6]．

[1] 金沢大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Kanazawa University, Kanazawa, Ishikawa 920–1192, Japan
[2] 金沢大学理工研究域
Institute of Science and Engineering, Kanazawa University, Kanazawa, Ishikawa 920–1192, Japan
[a)] k-fukushima@stu.kanazawa-u.ac.jp

文献 [2] では，攻撃者がオリジナルデータの一部を保有する場合に，仮名化データからどの程度オリジナルデータのユーザを特定できるかという点について考察を行っている．

また文献 [4] では，ユーザの位置情報データが高い頻度で収集されるような位置情報ベースサービスにおいて，仮名の交換を行うことで安全性の向上を図る手法を提案している．

2.2 仮名化と仮名の更新

データセット上のあるユーザの識別子を，容易に復元することができない別の文字列に置き換える手法を仮名化といい，置換した文字列を仮名という．また，特に 1 つの識別子に対して複数の仮名が存在するような仮名化を多重仮名化と呼ぶ．2018 年に施行された EU 一般データ保護規則（GDPR）第 4 条 5 号において，仮名化は以下のように定義されている．

> *(5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;*

また文献 [7] において，仮名化は，ユーザの再識別リスクを考慮し以下の性質を満たすべきだとされている．

不可逆性

仮 ID から，仮名化前の識別子が特定されないようにする必要がある．具体的には，ハッシュ化や UUID（Universally Unique Identifier）を用いる手法等が考えられる．

不連続性

履歴データや継続的にデータが提供される場合，同一の識別子に対して割り振られる仮 ID はある一定の期間で更新する必要がある．

非同一性

異なるデータ間において，同一の識別子に対して同一の仮 ID が割り振られないようにする必要がある．

本論文ではこのうち不連続性に着目する．また非同一性に関しては，本論文では単一のデータセットのみを対象として議論するため，これ以降では考慮しない．文献 [7] でも示されているとおり，履歴データにおいて長期間同一の仮名を使用し続けることで，ユーザの再識別リスクが高まる可能性が指摘されている．仮名の更新頻度の違いは，**表 1** に示すような特徴をデータにもたらすとされる [12]．

一方，我々が知る限り仮名の有効期間を定量的に評価し設定する手法は存在せず，根拠なく不適切な有効期間が設定される場合もありうることから，定量的な安全性評価手法の確立が重要である．

表 1 仮名更新頻度の違いによるデータの特徴
Table 1 Data property depends on difference of update frequency.

	高頻度	低頻度
利点	仮名どうしの対応関係の推測は困難	各ユーザの特性に着目した解析が可能
欠点	ユーザの短期間の動向しか把握できない	仮名どうしの対応関係を推測されうる

3. 仮名更新頻度の定量的評価

本節では，事前に仮名の更新頻度を設定し多重仮名化を行うような場合において，ある更新頻度を設定することでどの程度仮名の再同定リスクが存在するかを定量的に評価する手法を説明する．

3.1 準備

3.1.1 データ構造

本論文で用いるデータセット D は，**表 2** に例示する形式のアクセス履歴データである．

データセット D の構造は次のように定義される：

$$D = \{(u, access, date)\} \in User \times Access \times Date$$

ここで $User$，$Access$，$Date$ はそれぞれユーザ ID，アクセスしたサイトの URL，アクセス日時の集合を表す．また，D 上のあるユーザ $u \in User$ がアクセスしたサイトの URL の集合を $Access_u$ で表す．

3.1.2 記法および用語の定義

識別子（Identifier）とは，個人を直接識別することのできる属性を指し，一般に氏名やあるサービスにおけるユーザ ID 等が該当する．本論文において識別子は u である．

本論文では，仮名化の起点として定めた時間から，一定の有効期間を迎えるごとにすべてのユーザの仮名を更新する手法を用いて多重仮名化を実現する．データセット D について，多重化仮名化の起点を s，仮名の有効期間を t とし，$i \in \mathbb{Z}_{\geq 0}$ に対して時間帯 B_i を次のように定義する：

$$B_i = \{date \in Date \mid s + it \leq date < s + (i+1)t\}$$

ここで定義した時間帯 B_i は，同一のユーザに対して同一の仮名が割り当てられる時間幅を表しており，この i を時間帯表示と呼ぶことにする．このとき，仮名化を次のように定義する．

定義 1（仮名化）
有効期間を t とするとき，仮名化関数

$$\mathrm{Pse}_t : User \times Date \to P$$

表 2 アクセス履歴のサンプル
Table 2 Sample of web-access history.

User	Access	Date
Alice	www.google.co.jp	08/21 23:52:39
Bob	www.kanazawa-u.ac.jp	08/21 23:54:11
Alice	www.google.co.jp/maps	08/21 23:55:40
Carol	twitter.com/PWScup_Admin	08/21 23:58:21
Bob	acanthus.cis.kanazawa-u.ac.jp	08/21 23:59:02
Alice	mail.google.com/mail	08/22 00:00:36
Carol	twitter.com/ipsjcom	08/22 00:01:10
Carol	www.facebook.com	08/22 00:03:56

を用いて，ある日時 $date$ におけるユーザ u の仮名を $\mathrm{Pse}_t(u, date)$ と表す．ここで，P は仮名の全体集合．

ここで，仮名化関数 Pse_t は以下に示す 3 つの性質を満たすものとする．

(1) 正当性
D 上に存在するすべての $(u, date) \in User \times Date$ に対して必ず一意に対応する仮名 p が存在する．すなわち

$$\forall (u,date) \in User \times Date, \exists! p \ s.t. \ \mathrm{Pse}_t(u,date) = p$$

(2) 単射性（ユーザ，時間帯対仮名）
異なるユーザ，異なる時間帯には必ず異なる仮名が割り当てられる．すなわち

$$\forall u,u' \in User, \forall i,j \in \mathbb{Z}_{\geq 0}; \mathrm{Pse}_t(u,B_i) = \mathrm{Pse}_t(u',B_j) \Leftrightarrow u = u' \wedge i = j$$

(3) 不可逆性
仮名 $\mathrm{Pse}_t(u, date)$ からユーザ u の復元が困難．

このうち，(2) 単射性は，2.2 節における不連続性を保障している．また，D において $u \in User$ を仮名 $\mathrm{Pse}_t(u, date)$ に置き換えて得られる

$$D_t^{\mathrm{P}} = \{(\mathrm{Pse}_t(u, date), access, date)\}$$

を D の仮名化データセットと呼ぶ．

さらに，逆仮名化を次のように定義する．

定義 2（逆仮名化）
$\forall p \in P, \exists (u, date) \in User \times Date \ s.t. \ \mathrm{Pse}_t(u, date) = p$ であるとき，

$$\mathrm{DPse}_t : P \to User, \mathrm{Pse}_t(u, date) \mapsto u$$

を逆仮名化関数という．

ユーザ u に対応する仮名の集合を P_u と表す．

本論文において仮名の再同定とは，ある仮名 $p \in P$ に対し，p が対応するユーザ $\mathrm{DPse}_t(p)$ の仮名集合 $P_{\mathrm{DPse}_t(p)}$ に属する他の仮名 $(P_{\mathrm{DPse}_t(p)} \setminus \{p\})$ を推測することを意味する．

このような仮名間の関係を推測されると多重仮名化の意味をなさないため，再同定を行う攻撃者を想定した際に，攻撃者がどの程度再同定に成功するかという割合いを求めることは重要である．

Algorithm 1 仮名に対する再同定攻撃
INPUT: $D_t^{\mathrm{P}}, p \in P, |P_{\mathrm{DPse}_t(p)}|$
OUTPUT: 仮名候補集合 C_p
Step 1.
$\forall q \in P, q \neq p$ に対し，$Access_p, Access_q$ 間のアクセス履歴の類似度 $\mathrm{Sim}(p, q)$ を求める．
ここで $0 \leq \mathrm{Sim}(p, q) \leq 1$ であり，$\mathrm{Sim}(p, p) = 1$.
Step 2.
$C_p = \emptyset$ に対し
以下を $|P_{\mathrm{DPse}_t(p)}| - 1$ 回繰り返す．

$$C_p \leftarrow \underset{q \in P \setminus (\{p\} \cup C_p)}{\arg\max} \ \mathrm{Sim}(p, q)$$

3.2 評価手法の概要

本提案手法は，3.1.1 項において定義した構造の Web アクセス履歴データを保有するデータ加工者が，多重仮名化を行うにあたり適切な更新頻度を定めようとする状況を想定している．加工者は，事前に定めた仮名有効期間 t でデータセット D を多重仮名化し，D_t^{P} を生成する．次に，Algorithm 1 に示す再同定攻撃を行う攻撃者モデルを想定し，その攻撃者が実際に再同定攻撃を行った際に，どの程度再同定に成功するかを表す平均再同定率（Average Re-identification Rate，ARR_t）を求め，それを更新頻度 t における安全性評価値とする．以下，多重仮名化データの生成，想定する攻撃者モデルおよび平均再同定率の定義を示す．

3.2.1 多重仮名化データの生成

事前に設定した更新頻度 t ごとに，D 上のすべてのユーザの仮名を更新する．たとえば 1 週間分のアクセス履歴データに対して更新頻度を 24 時間と設定した場合，1 人のユーザに対して最大 7 個の仮名が存在することになる．ある時間帯にアクセスが存在しない場合は当然仮名は割り振られないため，ユーザに対応する仮名数は必ずしも最大値（上記の例の場合 7）になるとは限らない．

3.2.2 仮名に対する再同定攻撃

Algorithm 1 に示す再同定攻撃を行う攻撃者モデルを想定する．攻撃者の背景知識は仮定 1 に示すとおりとする．

仮定 1（攻撃者の事前知識）
- 更新頻度 t における仮名化データセット：D_t^{P}
- ある仮名 $p \in P$ と同一のユーザに割り当てられている仮名数：$|P_{\mathrm{DPse}_t(p)}|$

ここで，攻撃者は仮名 p が割り当てられているユーザ $(\mathrm{DPse}_t(p))$ を知ることはできず，当該ユーザに割り当てられている仮名数（$|P_{\mathrm{DPse}_t(p)}|$）のみを知ることができる．3.1.2 項でも示したように，安全な多重仮名化を実現する

ためには，再同定攻撃に対する耐性がどの程度あるかを示すことは重要である．本論文で定義する再同定率（定義 3）を求めるためには仮名ごとの割当て仮名数を知る必要があり，攻撃者を含めてリスクを評価するためのモデルを定義するうえで，攻撃者がこのような割り当て仮名数を知っている状況を想定している．

匿名化・再識別技術を競う PWS Cup 2016 [9] および PWS Cup 2018 [10] をはじめ，匿名化技術に関する研究やコンテスト等では攻撃者モデルとして加工前のオリジナルデータと加工データすべてを保有する最大知識攻撃者モデル [8] が採用される例が多い．

一方，本論文における攻撃者モデルでは，攻撃者の知識を仮定 1 に限定し，そのデータからアクセス履歴の類似度をもとに仮名のグルーピングを行う攻撃者を想定する．想定する攻撃者は，Algorithm 1 に示す再同定攻撃を行う．

Algorithm 1 で示した再同定攻撃手法は，アクセス履歴にはユーザごとに固有の傾向があるという仮定に基づいている．そこから，ある 2 つの仮名間でアクセス履歴の類似性が高い場合には，その 2 つの仮名は同一ユーザの仮名であると見なして，攻撃者は再同定を行う．ここで再同定とは，ある仮名と同一ユーザに対応する他の仮名の推測を行うことを表す．

3.2.3 安全性評価

定義 3（再同定率）

更新頻度を t とし，攻撃者が Algorithm 1 に従って再同定攻撃を行ったとする．ある仮名 $p \in P$ に対する再同定率を

$$\frac{|C_p \cap (P_{\mathrm{DPse}_t(p)} \setminus \{p\})|}{|P_{\mathrm{DPse}_t(p)} \setminus \{p\}|}$$

と定める．

本論文において再同定率とは，ある仮名 p に対して攻撃者が再同定攻撃の結果選択した候補 C_p のうち，実際に正しく p と同一ユーザの仮名である割合を表す．

次に，定義 2 に従って更新頻度 t における平均再同定率 ARR_t を次のように定める：

$$ARR_t = \frac{1}{|P|} \sum_{p \in P} \frac{|C_p \cap (P_{\mathrm{DPse}_t(p)} \setminus \{p\})|}{|P_{\mathrm{DPse}_t(p)} \setminus \{p\}|}$$

ARR_t の値は，攻撃者の再同定攻撃が平均してどの程度正しく仮名を当てられているかを示しており，値が 0 に近いほど今回想定している再同定攻撃への耐性があることを示す．

3.3 ARR_t の意味合いと妥当性

ARR_t の値を用いることで，ある更新頻度 t においてどの程度仮名の再同定リスクが存在するかを評価することができ，具体的なリスクの大小に基づいた更新頻度の設定が可能になる．本論文においては，ある仮名の更新頻度に対して単一の値を用いて評価を行うことを目的とし，全仮名に対する再同定率の平均値を評価に用いているが，この値はあくまでデータにおける大局的な傾向を示しているにすぎない．データの匿名化に用いられる技術のうち，仮名化あるいは多重仮名化は，それ単体で十分な匿名性を確保できる手法ではなく，実用上は他の匿名化技術と組み合わせて用いられる．そのため，本提案手法では仮名更新頻度の安全性についてデータ全体の傾向について評価を行い，その後各仮名の再同定率に基づいて，仮名ごとに個別の加工を行うというような運用が考えられる．

4. 実データによる評価

本章では，提案手法を実際に収集した Web アクセス履歴データに適用して評価を行う．

4.1 評価に使用するデータについて

評価には，NICT 委託研究『Web 媒介型攻撃対策技術の実用化に向けた研究開発』の一環として収集された Web アクセス履歴データを使用する．当該データは，不正 Web サイトへのアクセスを検知するセキュリティソフトの利用者から収集した，表 2 で示したサンプルと同様の構造を持つデータであり，各レコードは (ユーザ ID, アクセスしたサイトの URL, アクセス日時) で構成される．なお，本データは情報処理学会倫理綱領に基づく形で提供されたものである．

本論文においては，上記のデータより 2016/12/10 から 12/16 までの一週間分を抽出し，そのうち特にアクセスの傾向が顕著に表れると考えられる，7 日間すべてにおいてアクセスが確認された 103 人のユーザのアクセス履歴に限定して評価を行う．このデータに関する統計量を**表 3** に示す．

4.2 シミュレーション手法

本論文では，仮名の更新頻度として 24，12，8，6，4，3，2，1 時間の 8 通りを設定し，それぞれに対して提案手法を適用する．また，アクセス履歴として URL 全体を対象とする場合とドメインのみを抽出した場合それぞれについて評価を行う．

Algorithm 1 における類似度の評価指標としては Jaccard 係数を用いる．すなわち，異なる 2 つの仮名 p，q に対して

$$\mathrm{Sim}(p, q) = \frac{|Access(p) \cap Access(q)|}{|Access(p) \cup Access(q)|}$$

と定める．

4.3 評価結果と考察

4.3.1 アクセス履歴の類似性について

本提案手法は，アクセス履歴にはユーザごとに固有の傾向があるという仮定に基づいているが，まずこの点について評価を行う．**表 4** は，アクセス履歴としてドメインを

表 3 評価に使用するデータの統計量
Table 3 Data statistics.

評価に使用するデータのレコード数	673,335
1 人のユーザが 1 日にアクセスするユニークドメイン数の平均	63.56

表 4 Jaccard 係数の平均値（ドメイン）
Table 4 Average of Jaccard index (domain).

更新頻度（時間）	全通りの組合せ	同一ユーザどうしの組合せ
24	0.1252	0.3528
12	0.1220	0.3216
8	0.1181	0.3041
6	0.1139	0.2927
4	0.1114	0.2890
3	0.1067	0.2782
2	0.1032	0.2735
1	0.0923	0.2662

対象とした場合に，Algorithm 1 の Step 1 において導出した，各更新頻度における仮名間の Jaccard 係数の平均値を示したものであり，ここで「全通りの組合せ」とは相異な 2 つの仮名の組全通りの Jaccard 係数の平均値であり，「同一ユーザ同士の組合せ」とは同一ユーザに対応する仮名の組全通りの Jaccard 係数の平均値を表す．また**図 1**，**図 2** はそれぞれ更新頻度 24 時間および 1 時間の際の「全通りの組合せ」の Jaccard 係数の度数分布を示しており，グラフ上の点は各度数中の「同一ユーザ同士の組合せ」の割合を表している．

8 通りの更新頻度いずれに対しても，同一ユーザ同士の組合せにおける平均値は，全通りの組合せにおける平均値のおよそ 3 倍となっており，ユーザごとに特定の Web サイトを閲覧する/しないという傾向が存在することが分かる．

また図 1 から分かるように，更新頻度を 24 時間と設定した場合において Jaccard 係数が 0.5 以上となる組合せはその大部分が同一ユーザ同士の組合せだが，他方更新頻度を 1 時間とした場合にはその傾向は薄れている．すなわち，仮名の更新頻度が高い場合，いい換えるとユーザの短期間の動向のみに着目した場合では，ユーザごとの固有の傾向は表れにくくなっている．

次に，フルパスの URL を対象とした場合に同様の解析を行った結果を**表 5**，**図 3**，**図 4** に示す．フルパス URL を対象とした場合においても，ドメインを対象とした場合と同様の結果が得られているが，URL が完全に一致する件数は少なく，全体的に Jaccard 係数の値は低くなっている．

これらの結果から，本シミュレーションで用いた Web アクセス履歴においては，ユーザごとに特定のサイトへアクセスする/しないといった固有の傾向が存在し，このような特性に基づいた評価手法は有効であると考える．

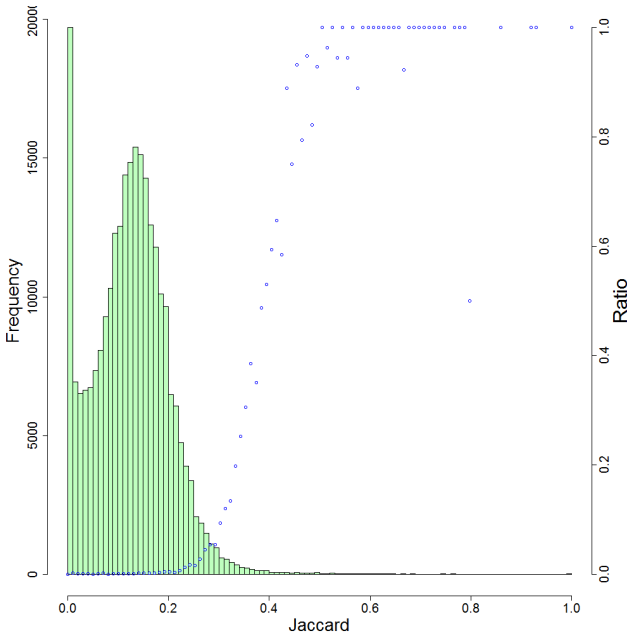


図 1 Jaccard 係数の度数分布（ドメイン，更新頻度 24 時間）
Fig. 1 Frequency distribution of Jaccard index (domain, update frequency 24 hour).

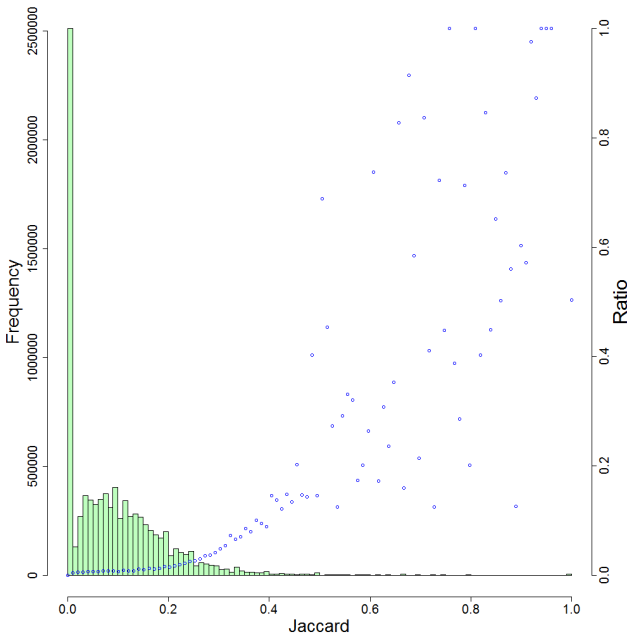


図 2 Jaccard 係数の度数分布（ドメイン，更新頻度 1 時間）
Fig. 2 Frequency distribution of Jaccard index (domain, update frequency 1 hour).

4.3.2 平均再同定率の評価

次に，提案手法に基づいて各更新頻度に対する平均再同定率 ARR_t を導出した結果を**表 6** に示す．

フルパス，ドメインいずれを対象とした場合でも，仮名の更新頻度をより高く設定することで平均再同定率の値は低下しており，その意味で安全性は向上しているといえる．

次に，ドメインを対象とした場合に，更新頻度を 24 時間および 1 時間に設定した際の各仮名に対する再同定率の

表 5 Jaccard 係数の平均値（フルパス）
Table 5 Average of Jaccard index (full path).

更新頻度（時間）	全通りの組合せ	同一ユーザ同士の組合せ
24	0.00581	0.0422
12	0.00641	0.0411
8	0.00646	0.0408
6	0.00634	0.0405
4	0.00646	0.0414
3	0.00642	0.0409
2	0.00634	0.0403
1	0.00610	0.0419

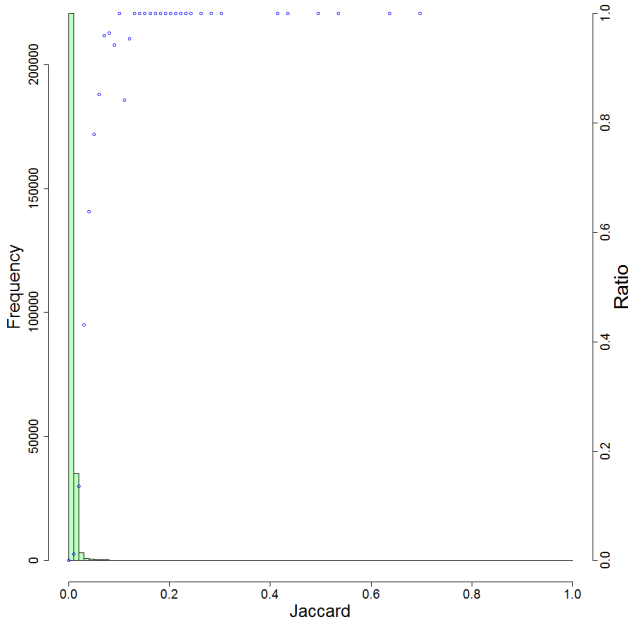


図 3 Jaccard 係数の度数分布（フルパス，更新頻度 24 時間）
Fig. 3 Frequency distribution of Jaccard index (full path, update frequency 24 hour).

度数分布をそれぞれ**図 5**，**図 6** に示す．

更新頻度 24 時間の場合においては，再同定率が 1 となる仮名が全 720 個中 178 個存在し，全体のおよそ 25%の仮名について同一ユーザに対応する他の仮名がすべて再同定される結果となった．また，更新頻度が 1 時間の場合では平均再同定率は 0.2688 であり，ある仮名に対して平均して 27%程度しか，対応する他の仮名を再同定されないことが分かる．

またフルパス URL を対象とした場合でもほぼ同様の結果が得られたが，どの更新頻度に対してもドメインを対象とした場合より平均再同定率の値は大きくなった．これらをまとめた結果を**図 7** に示す．

これらの評価結果から，今回シミュレーションに用いたデータにおいて，提案手法は有効であると考える．

4.4 更新頻度の定め方について

本論文では，プライバシリスクの定量化の一環として平

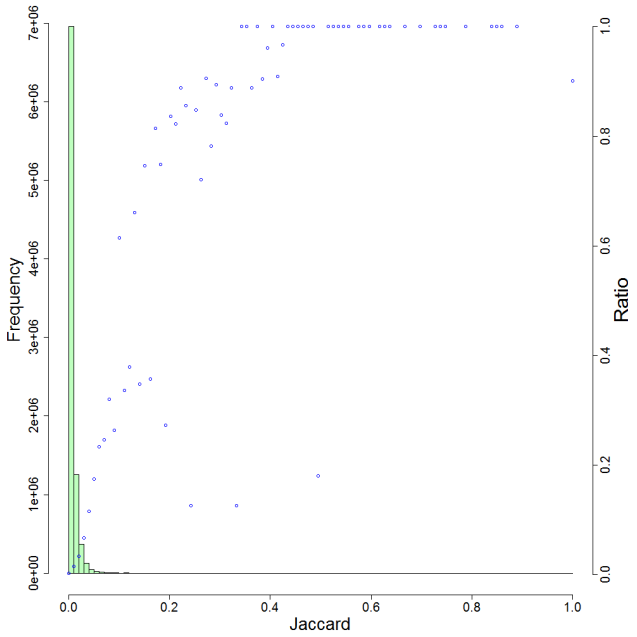


図 4 Jaccard 係数の度数分布（フルパス，更新頻度 1 時間）
Fig. 4 Frequency distribution of Jaccard index (full path, update frequency 1 hour).

表 6 提案手法の評価結果
Table 6 Result of proposed method evaluation.

更新頻度（時間）	平均再同定率（ドメイン）	平均再同定率（フルパス）
24	0.6309	0.7063
12	0.4817	0.5544
8	0.4294	0.4971
6	0.3896	0.4608
4	0.3630	0.4230
3	0.3341	0.3889
2	0.3083	0.3585
1	0.2688	0.2950

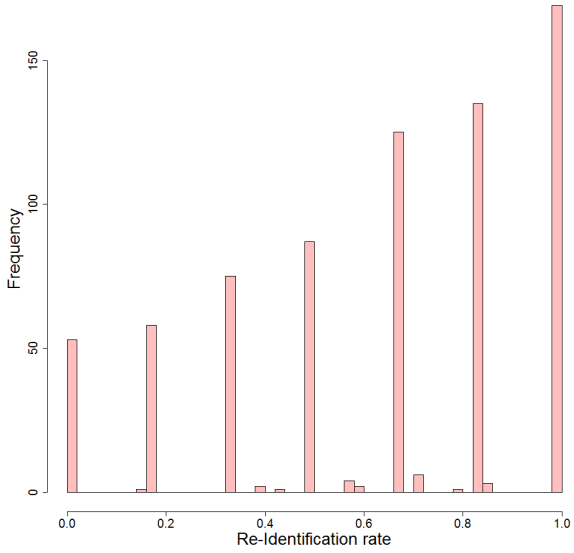


図 5 再同定率の度数分布（ドメイン，更新頻度 24 時間）
Fig. 5 Frequency distribution of ARR (domain, update frequency 24 hour).

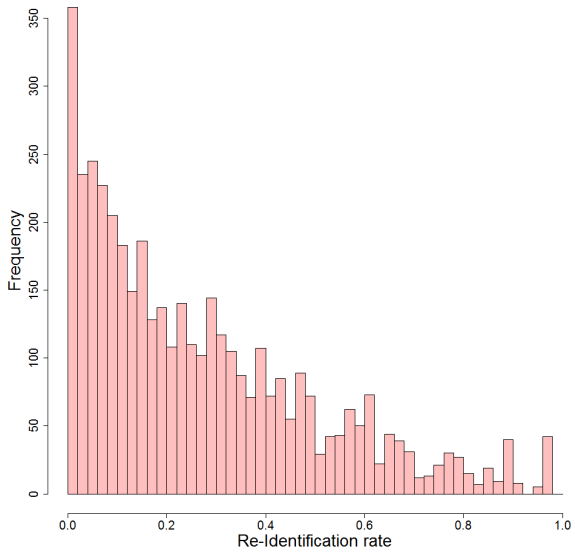


図 6 再同定率の度数分布（ドメイン，更新頻度 1 時間）
Fig. 6 Frequency distribution of ARR (domain, update frequency 1 hour).

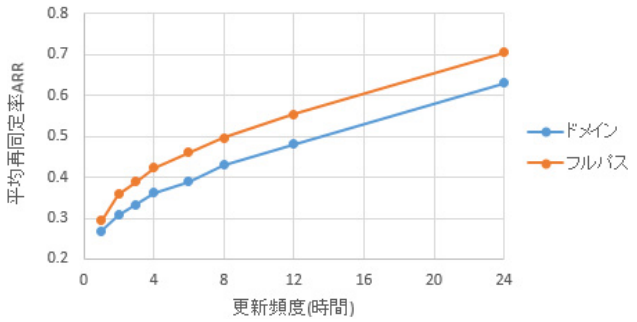


図 7 平均再同定率の変化
Fig. 7 Changes of ARR.

均再同定率という値を定義した．この平均再同定率の値が具体的にどうなると良いかという点については，一般には法制度やガイドライン等を参考に，ユースケースごとに個別で評価されるべきである．本節では，更新頻度の求め方の一例として，データの有用性を評価する指標を新たに導入して考察を行う．

12/10〜12/16 の 1 週間の間に，4.1 節で示した 103 人から収集したデータにおけるユニークなドメイン数は 6,865 であり，この値を本節における有用性評価の基準とする．簡単のため 12/10 の一日分のデータに注目し，更新頻度 $t = 24, 12, 8, 6, 4, 3, 2, 1$ 時間の 8 通りそれぞれについて，12/10 のデータを 12/10 00:00:00 を基準に t ごとに分割する．ある更新頻度 t において，分割したそれぞれのデータにおけるユニークなドメイン数を求め，さらに分割したデータすべてについてその平均値を求める．この値を，1 週間分のユニードメイン数である 6,865 で除した値を更新頻度 t における有用性評価値とする．

例として更新頻度を $t = 8$ 時間とした場合，12/10 の一日分のデータを 00:00〜07:59，08:00〜15:59，16:00〜23:59 の 3 つに分割し，それぞれについてユニークなドメイン数を求める．この 3 つのデータにおけるそれぞれのユニークドメイン数の平均値を 6,865 で除した値が $t = 8$ 時間とした場合の有用性評価値となる．この有用性評価値の意味合いとしては，仮名ごとの最長の履歴の長さが t 時間である場合に，当該データにおいて元データ（本論文においては 1 週間）に対してどの程度の割合のドメインを再現できているかを表している．

表 7 有用性評価値
Table 7 Utility evaluation.

更新頻度（時間）	有用性評価値
24	0.2820
12	0.1817
8	0.1407
6	0.1170
4	0.0893
3	0.0742
2	0.0566
1	0.0362

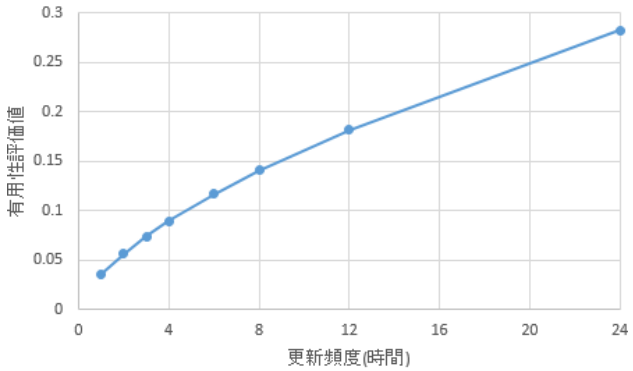


図 8 有用性評価値の変化
Fig. 8 Changes of Utility index.

8 通りの更新頻度に対して上記手法で有用性評価値を求めた結果を**表 7** および**図 8** に示す．

図 7 における平均再同定率の変化と同様に，更新頻度を高く設定するほど有用性の値は低下している．

この有用性の値を用いて更新頻度を定める一例として，たとえばデータ利用者がデータの有用性評価値 0.1 以上を要望している場合，本論文における有用性の定義では更新頻度が 6 時間以上の場合に有用性が 0.1 以上となっているため，その中で最も平均再同定率の値が低い（すなわち再同定リスクが小さい）更新頻度 6 時間を設定することができる．さらに，本論文で定義した平均再同定率の値を用いて，更新頻度 6 時間とした場合における再同定リスクの値を顧客等に定量的に示すことができる．

4.5 課題

本論文における提案手法の課題として，特に以下の 3 点が存在すると考えている．

再同定手法の妥当性

提案手法では，3.2.2 項で示した情報のみを持ちアクセス履歴の類似度に基づいて再同定攻撃を行う攻撃者を想定している．シミュレーションの際には類似度評価の指標として Jaccard 係数を採用しているが，この類似度ではデータの特徴をとらえきれない場合もありうる．今後，重み付き Jaccard 係数等，他の類似度評価手法も参考にしながら，より現実的な攻撃者モデルを検討する．

平均再同定率による評価の妥当性

安全性の評価指標として，各仮名の再同定率の平均値 ARR_t を用いているが，他方 4.3 節で示したように，平均値は 0.63 程度であっても全体のおよそ 25%の仮名で再同定率が 1 となるような例も存在する．平均値を用いた大局的な傾向に加え，再同定率の分布に基づいた評価も可能であり，今後さらに他の評価指標についても検討する．

計算量

本提案手法において，Algorithm 1 の Step 1 および 2 いずれもデータサイズが大きくなると膨大な計算時間が必要となる．そのため，4.1 節で行ったように対象とするユーザを限定して手法を適用するといった運用や，より簡易的な手法による評価が考えられる．

評価に用いるデータについて

本論文では 4.1 節で示したように，7 日間すべてにアクセスのあるユーザのデータに限定して評価を行った．筆者らが行った予備的な実験の結果，この条件を外したデータからランダムに抽出した複数のユーザに対して提案手法を適用しても同様の傾向が得られたため，このような条件の有無によって本提案手法における評価結果に大きな影響はないと判断したが，今後より詳細な検討を行い，どのようなデータについても適用可能であることを示していく．

5. より簡易的な評価手法

本節では，4.4 節で述べた提案手法のうち，特に計算量の改善について検討するため，より簡易的な評価手法の検討および収集データでの評価を行う．4.3.1 項での結果から，Jaccard 係数の大きなペアは同一ユーザに対応する仮名ペアである割合が多く，更新頻度がより低い場合にこの特徴は強く表れている．この特徴を用い，Algorithm 1 の Step 1 終了後，Jaccard 係数の大きい順に一定数の仮名ペアを候補として抽出し，そのうち同一ユーザに対応する仮名ペアである割合いを用いて簡易的に更新頻度の評価を行う．さらに攻撃者の事前知識についても，ユーザごとの仮名数にかわり，以下に示す仮定 2 のように加工前データにおけるユーザ数を知っている状況を考える．

仮定 2（攻撃者の事前知識）

- 更新頻度 t における仮名化データ：D_t^{P}
- 加工前データ D におけるユーザ数：$|User|$

仮定 2 の下で，Algorithm 1 をより簡素化した Algorithm 2 を用いて評価を行う．

Algorithm 2 簡易的な再同定攻撃

INPUT: $D_t^{\mathrm{P}}, |User|$
OUTPUT: 仮名ペア候補集合 C
Step 1.
$\forall p, q \in P, q \neq p$ に対し，$Access_p, Access_q$ 間のアクセス履歴の類似度 $\mathrm{Sim}(p, q)$ を求める．
ここで $0 \leq \mathrm{Sim}(p, q) \leq 1$ であり，$\mathrm{Sim}(p, p) = 1$.
Step 2.
$C = \emptyset$ に対し
以下を ${}_{\lfloor \frac{|P|}{|User|} \rfloor}\mathrm{C}_2 \cdot |User|$ 回繰り返す．

$$C \leftarrow \underset{(p,q) \in P \setminus C}{\arg\max}\ \mathrm{Sim}(p, q)$$

表 8 簡易的な再同定攻撃における評価値
Table 8 Evaluation of a method in Sect. 5.

更新頻度（時間）	評価値（ドメイン）	評価値（フルパス）
24	0.5312	0.5460
12	0.4316	0.4627
8	0.3869	0.4122
6	0.3207	0.3702
4	0.2857	0.3282
3	0.2566	0.3081
2	0.2373	0.2832
1	0.2055	0.2437

ここで，$\frac{|P|}{|User|}$ はあるユーザに対応する仮名数の平均値であり，当該ユーザに関する同一仮名ペアの個数をここでは ${}_{\lfloor \frac{|P|}{|User|} \rfloor}\mathrm{C}_2$ として計算を行う．次に，定義 2 の再同定率に対応する指標として，ここでは以下の評価値を用いる：

$$\frac{|\{(p, q) \in C | \mathrm{DPse}_t(p) = \mathrm{DPse}_t(q)\}|}{|C|}$$

4.2 節と同様の条件で，収集データにおいて上記評価値を求めた結果を**表 8** に示す．

表 6 における手法とは異なる評価尺度を用いた結果ではあるが，いずれの場合でも表 6 における平均再同定率の値にくらべ 76〜90%程度の値になっており，値の増減に関しては表 6 と同様の傾向を示している．また計算量についても，Algorithm 1 においては各仮名ごとに Step 2 の動作を行っていたのに対し，Algorithm 2 では Step 2 は 1 度しか実行されないため，Step 2 に限定した場合の計算量は Algorithm 1 と比べ $1/|P|$ 程度になっている．これらの結果より，3 章での提案手法より再同定の成功率は低下するものの，計算量削減の観点ではこのような簡易的な手法も有効であると考える．今後，より 4 章における成功率に近づけるような手法について更に検討を行っていく．

6. まとめ

本論文では，Web アクセス履歴におけるユーザ固有の特徴に基づいた，時分割による多重仮名化の安全性について

定量的に評価する手法を提案した．同時に実際に収集したデータに対して手法を適用し，アクセス履歴の類似度に基づいて評価を行う提案手法の有効性を示した．

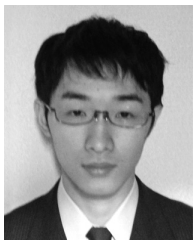
謝辞 本研究成果の一部は，NICT 委託研究『Web 媒介型攻撃対策技術の実用化に向けた研究開発』の一環として得られたものです．

参考文献

[1] Sweeny, L.: k-anonymity: A model for protecting privacy, *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, Vol.10, No.5, pp.555–570 (2002).
[2] 早稲田篤志，野島 良，盛合志帆，菊池浩明：良い仮名化悪い仮名化，2017 年暗号と情報セキュリティシンポジウム（SCIS2017），2D1-6 (2017).
[3] Dwork, C. et al.: Calibrating noise to sensitivity in private data analysis, Theory of Cryptography Conference, Springer Berlin Heidelberg (2006).
[4] Mano, K., Minami, K. and Maruyama, H.: Pseudonym exchange for privacy-preserving publishing of trajectory data set, *2014 IEEE 3rd Global Conference on Consumer Electronics* (*GCCE*), IEEE (2014).
[5] Machanavajjhala, A., Kifer, D., et al.: l-diversity: Privacy beyond k-anonymity, *ACM Trans. Knowledge Discovery from Data* (*TKDD*), Vol.1, No.1, p.3 (2007).
[6] Ikarashi, D. et al.: k-Anonymous microdata release via post randomisation method, *International Workshop on Security*, pp.225–241, Springer International Publishing (2015).
[7] 経済産業省：事業者が匿名加工情報の具体的な作成方法を検討するにあたっての参考資料（「匿名加工情報作成マニュアル」）Ver1.0 (2016)，入手先 ⟨http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/tokumeikakou.pdf⟩（参照 2018-11-13）.
[8] Domingo-Ferrer, J. and Muralidhar, K.: New directions in anonymization: Permutation paradigm, veriability by subjects and intruders, transparency to users, *CoRR*, abs/1501.04186 (2015).
[9] 菊池浩明, 小栗秀暢, 野島 良ほか：PWSCUP：履歴データを安全に匿名加工せよ，コンピュータセキュリティシンポジウム，pp.271–278 (2016).
[10] 濱田浩気，荒井ひろみ，小栗秀暢ほか：PWS Cup 2018：匿名加工再識別コンテストの設計〜履歴データの一般化・再識別〜，コンピュータセキュリティシンポジウム 2018，3D3-5 (2018).
[11] 福嶋雄也，北島祥伍，満保雅浩：Web アクセス履歴における仮 ID の更新頻度に関する考察，コンピュータセキュリティシンポジウム 2017 論文集 (2)，pp.1358–1365 (2017).
[12] 中川裕志：プライバシー保護入門：法制度と数理的基礎，勁草書房 (2016).

福嶋 雄也

2017 年金沢大学理工学域電子情報学類卒業．現在，金沢大学大学院自然科学研究科電子情報科学専攻博士前期課程に所属．プライバシ保護技術にかかわる研究に従事．



北島 祥伍

2017 年金沢大学理工学域電子情報学類卒業．現在，金沢大学大学院自然科学研究科電子情報科学専攻博士前期課程に所属．エッジコンピューティングを用いたセキュアなシステム構築に関する研究に従事．

満保 雅浩 （正会員）

1988 年金沢大学工学部電気・情報工学科卒業．1993 年東京工業大学大学院理工学研究科博士後期課程修了．博士（工学）．同年北陸先端科学技術大学院大学助手．その後，東北大学助教授，筑波大学助教授・准教授を経て 2011 年から金沢大学教授．情報セキュリティの教育・研究に従事．