

個人データの匿名化とその限界

Anonymization of Personal Data and Its Limitations

高橋克巳 正木彰伍 濱田浩気

Abstract

パーソナルデータの匿名化の限界と呼ばれる問題について、移動履歴データを題材に解説を行う。パーソナルデータの匿名化の限界とは、データ分析を行うとき、加工されていない個人情報を使った場合得られると期待される成果が、匿名化データを使った場合得られないことがあることを言う。「匿名化」したデータがプライバシー上安全なのか、またそれがどの程度役に立つかの一般的な指標は存在しない。その考えに従って、現在最も注目されているパーソナルデータの代表例である人の移動履歴を対象として匿名化を考えることとする。

キーワード：パーソナルデータ，匿名化，移動履歴，プライバシー保護

1. 匿名化とその限界

パーソナルデータの取扱いに関して匿名化が話題となっている。しかしその一方で匿名化はよく分からないとも言われる。本稿では匿名化について、データを使ったケーススタディを通じて解説する。

匿名化が分かりにくい理由の一つに、匿名化の評価はデータやその利用目的に左右されるという点にある。「匿名化」したデータがプライバシー上安全なのか、またそれがどの程度役に立つかの一般的な指標は存在しない。その考えに従って、本稿は具体的な対象として現在最も注目されているパーソナルデータの代表例である人の移動履歴を対象として匿名化を考えることとする。移動履歴のプライバシーと保護技術については情報処理学会誌⁽¹⁾で解説をした。本稿はその姉妹編となる移動履歴の匿名化のケーススタディである。なお本稿のパーソナルデータのリスクと対策に関する考え方は、IT 戦略本部パーソナルデータ検討会の技術検討 WG で行われた

匿名化の議論^{(2),(3)}に基づく。

匿名化とは一般に個人データを個人データでなくする手続きだと信じられているが、現実的にはなかなか個人と無関係にはならない。むしろ匿名化とは個人に関係するデータの関係性を弱くする加工手続きであると考えるのが適切である。匿名化の限界とは、個人データに対して加工を進めたとき、その加工データが守りたいプライバシーの基準に合致しているのかと、行いたい分析業務の役に立つのかを考える際に起こる。プライバシーが保証できない、若しくはデータが役に立たないときに匿名化の限界である。

2. 匿名化の基本技術

移動履歴の匿名化の基本技術を説明する。移動履歴とは人の移動に応じて蓄積された位置情報の系列であり、位置情報は緯度経度などの場所を示す情報と時刻から成る情報である。位置情報・移動履歴の加工手法（匿名化の技法）には以下のものがある。

- 位置情報のより広いエリア・時間帯への一般化。
- 位置情報の違う位置・時間へのランダムな置換え。
- 移動履歴を構成する位置情報の一部の削除（例、生活圏）。
- 移動履歴の分割（例、10日分の履歴を1日単位

高橋克巳 正員 日本電信電話株式会社 NTT セキュアプラットフォーム研究所
E-mail takahashi.katsumi@lab.ntt.co.jp
正木彰伍 日本電信電話株式会社 NTT セキュアプラットフォーム研究所
E-mail masaki.shogo@lab.ntt.co.jp
濱田浩気 正員 日本電信電話株式会社 NTT セキュアプラットフォーム研究所
E-mail hamada.koki@lab.ntt.co.jp
Katsumi TAKAHASHI, Koki HAMADA, Members, and Shogo MASAKI, Nonmember (NTT Secure Platform Laboratories, NIPPON TELEGRAPH AND TELEPHONE CORPORATION, Musashino-shi, 180-8585 Japan).
電子情報通信学会誌 Vol.98 No.3 pp.193-201 2015年3月
©電子情報通信学会 2015

に分割する)。

- ・ 移動履歴の間引き (例, 1分単位の時間分解能を1時間単位にする)。
- ・ 移動履歴のサンプリング (例, 移動履歴データベースから移動履歴レコードをランダムに抽出し, 母集団との関係を確率的にする)。
- ・ 移動履歴の削除 (例, 移動履歴データベースからリスクのある移動履歴レコードを削除する)。

なお, 上記の位置情報・移動履歴は氏名等の個人が特定できる情報の存在を無視しているが, 一般的には上記の加工を行うならば, 以下の加工をしておくことが前提となる。

- ・ 直接あるいは組合せで個人が特定できる情報の削除, 識別番号化 (例, 氏名)。
- ・ 組合せで個人が特定できる情報の一般化, ランダム化 (例, 年齢)。

3. ケーススタディを行う移動履歴

3.1 データセット

匿名化のケーススタディで利用するデータセットは東京大学空間情報科学研究センター (CSIS) 人の流れプロジェクト⁽⁴⁾の平成10年東京都市圏のデータセットである。このデータは東京都市圏^(注1)のパーソントリップ調査^(注2)データを基に東大CSISが独自処理した「人の流れ」データで, 72.2万人のある平日1日の位置情報が1分間隔で収められている。本スタディでは15分間隔のデータを用いた。

本データから分析用に二つのデータセットを作成した。

- ・ 移動履歴セット A (朝8時台) :

8:00~8:45の間に移動した人の履歴。レコードは人に対応し, 8:00, 8:15, 8:30, 8:45の4ノード(3エッジ)で構成。レコード数269,865。

- ・ 移動履歴セット B (午前中) :

9:00~12:00の間に移動した人の履歴。9:00, 10:00, 11:00, 12:00の4ノード(3ホップ)で構成。レコード数214,374。

3.2 単独の位置情報の概観

移動履歴全体を理解するために, 朝8時の単独の位置

(注1) 対象エリアは以下国土交通省サイトを参照。http://www.mlit.go.jp/crd/tosiko/pt/city/tokyo/04.html

(注2) 各都市圏の交通計画協議会が行う人の移動に関する調査票による調査。

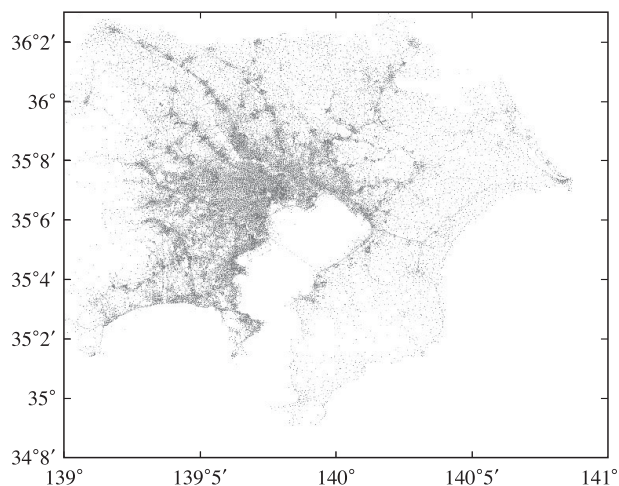


図1 8時の位置情報

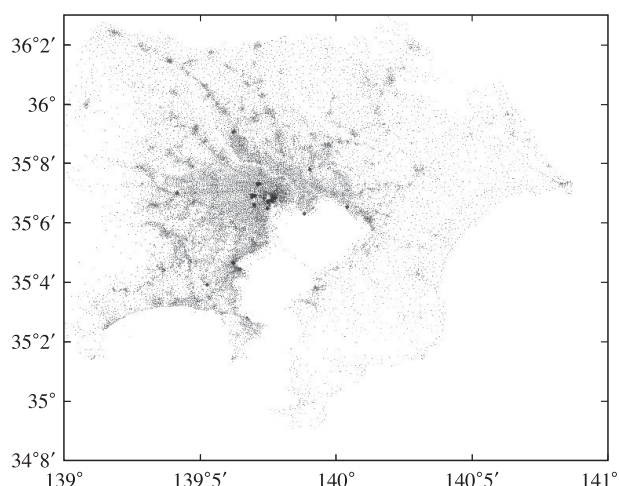


図2 12時の位置情報

表1 単独の位置情報の概観 (値は全て10万人当りに換算)

	セット A /8時	セット B /12時
誰かがいる位置の数	52,000	18,000
一人の人しかいない位置の数 ($k=1$)	45,000	10,000
人口が集中している位置の数 (0.1%超)	0	12

情報と, 12時の位置情報を図1, 2に示す。色の濃い部分は人数が多い。どちらもおおむね似た図になるが, 8時は多くの人が位置的に単独に存在していて ($k=1$, 同じ条件を満たすレコードの数を慣習に基づいて $\langle k \rangle$ で表すことにする。), 12時は8時と比べて, 人が都心部に集中している傾向がある。表1に, 8時, 12時の単独の位置情報の概観を記す。

3.3 移動経路の概観

続いて, 移動経路全体を理解するために, 移動履歴

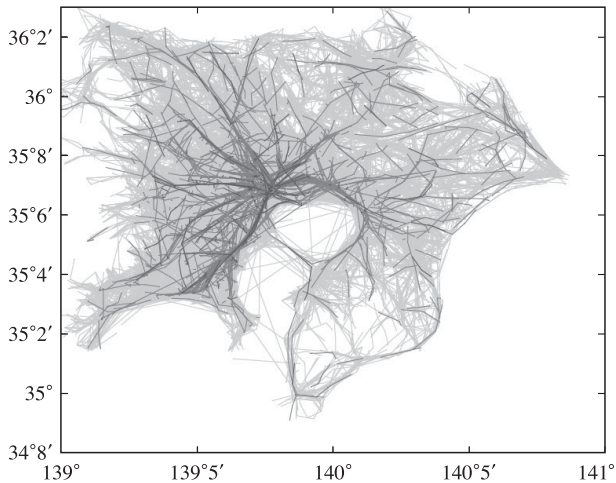


図3 長距離移動の例(セット A(8 時台)で 10 km を超えるもの)

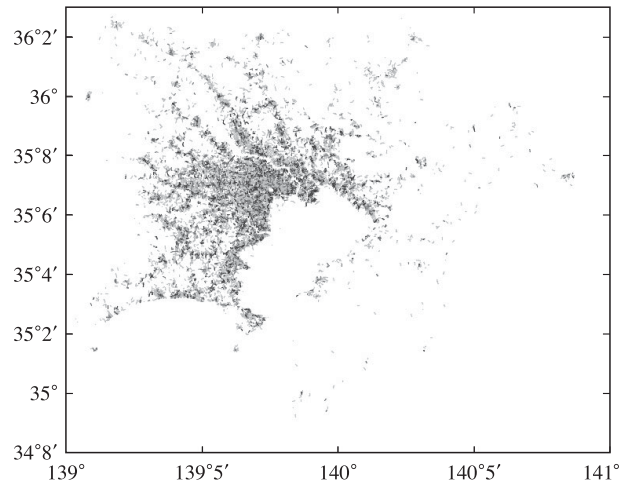


図6 短距離移動の例(セット B(午前中)で 1 km に満たないもの)

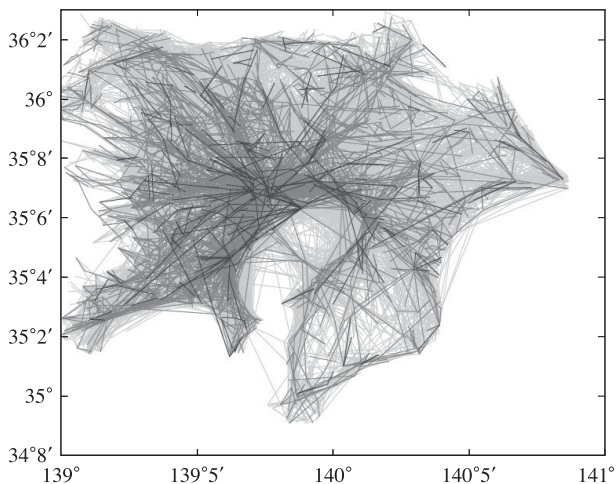


図4 長距離移動の例(セット B(午前中)で 10 km を超えるもの)

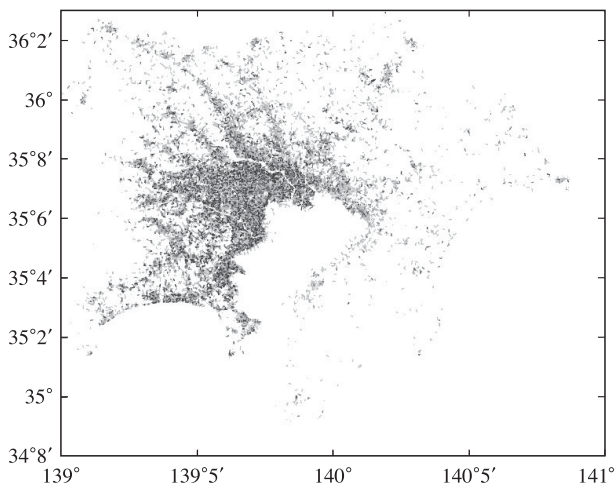


図5 短距離移動の例(セット A(8 時台)で 1 km に満たないもの)

表2 移動履歴の概観 (値は全て 10 万人当りに換算)

	セット A	セット B
長距離履歴のレコード数 (10 km 超)	27,000	28,300
長距離履歴のユニーク経路数 (10 km 超)	26,800	27,300
一人の人しかいない長距離履歴の数 ($k=1$)	26,500	26,400
短距離履歴のレコード数 (1 km 未満)	21,100	14,700
短距離履歴のユニーク経路数	17,900	13,300
一人の人しかいない短距離履歴の数 ($k=1$)	15,500	12,100

A と移動履歴 B を図 3~6 に図示する。全ての移動履歴を表示することは困難なので、長い距離を移動した履歴と短距離のものに分けて表示を行った。色の濃い部分は人数が多い。

移動履歴は一般に一意性が高くなる (ばらばらになる)。長距離履歴はセット A (朝 8 時台) では、一部の特徴的な履歴を除くとほとんどがばらばらになり、セット B (午前中) の方が複数の人に共通する特徴的な履歴を見いだせる。一方、短距離履歴はセット A の方がより特徴を見いだせる傾向がある。表 2 に記した移動履歴 A, B の概観からも、セット A の方が、 $k=1$ のレコード数の割合が低いことが分かる。

4. 匿名化の考え方

4.1 識別性

本稿では、匿名化を「移動履歴と移動をした個人との関係を弱くすること」と捉えて解説を行う。そのために理解しておく必要がある概念に「識別性」がある。識別性がある状態とは、そのデータが誰か一人の情報であることである。以下に識別性に関するものを含む「パーソナルデータ検討会」のレポートから引用する。

- ・ 識別特定情報：
それが特定の誰か一人の情報であることが分かる。
- ・ 識別非特定情報：
それが誰か一人の情報であることが分かるが、その一人が誰であるかまでは分からない。
- ・ 非識別非特定情報：
それが誰の情報であるかが分からず、更に、それが誰か一人の情報であることが分からない。

識別性のあるデータは、誰か一人のデータなので、①他の情報と照合することにより機械的に個人が特定されるリスクがあり、更にその履歴にパターン性がある場合は、②パターン性のある履歴同士のマッチングにより、より情報量の多いデータが作り出されるリスクがある。更に位置情報は誰かが見ている場合もあり、またそれを詳細にブログ等を書いたりすると③固有な知識に基づく個人特定のリスクも考慮する必要がある⁽¹⁾。

移動履歴の識別性を低くすることにより、個人との関係を極めて弱い状態に持っていくことができる。

4.2 移動履歴の匿名化

移動履歴は、以下のような「位置情報の時系列」の集まりと考えることとする。

$$\{(x_1, y_1, t_1), (x_2, y_2, t_2), \dots, (x_n, y_n, t_n)\}$$

ただし x_a, y_a は時刻 t_a におけるある人の地理的な位置。

移動履歴には「氏名」といった個人が直接特定できるデータや「年齢」「性別」といった様々な属性データが伴われているケースもあるだろう。本稿では直接特定できるデータは適切に削除されているものとする^(注3)。また、それ以外のデータは単純化のため議論に含めない^(注4)。

移動履歴の匿名化とは移動履歴の x, y, t を加工して、個人との関係を弱くすること、すなわち個人の特定性や識別性を減じることである。ただし、本稿の匿名化に対する立場は、いたずらに高い非識別の度合いを追求することではない。パーソナルデータを利用する際には業務に必要なデータの種類とレベルを把握した上で、できるだけプライバシーのリスクを減じるためのデータへの加工を行い、その上で残るリスクを明らかにしてデータ分析を行うことが重要である。その際に一つの指標となるのが、データの識別性がどの程度減じられているかという点である。

(注3) 氏名等の直接個人特定ができるデータを削除したとしても、削除した後のデータが元のデータ等の氏名を含むデータと容易に照合できる場合は個人情報とみなされる。

(注4) 他の属性は位置情報と同様に加工することで、個人の非識別を達成できることは言うまでもない。

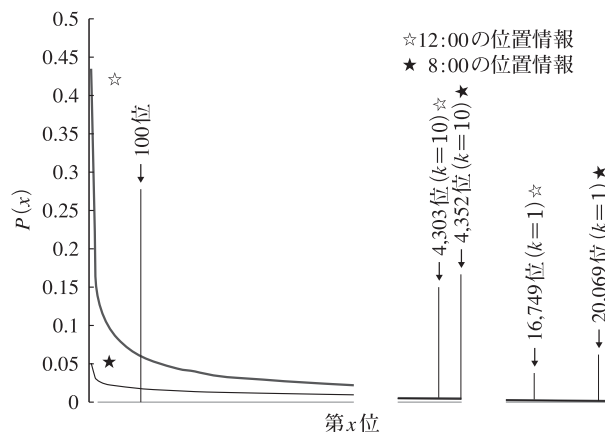


図7 位置の出現順位と出現頻度

4.3 集合匿名化

パーソナルデータを一意に識別できないようにする代表的な手法が集合匿名化である。「 k -匿名化」とはその代表で、保護対象とした属性に対して同じ属性を持つレコードが少なくとも k 個存在するようにデータを加工する。集合匿名化においてはあるレコードが特定の誰かのものであると判断しようにも、その対象をその集合の中から絞り込むことができない。 k -匿名化されているデータにおいては、それが k という値でパラメータ化される。

図7に8時と12時の単独の位置情報の出現頻度を示す。グラフの横軸は出現順位で、縦軸は出現頻度である。例えば、12時の頻度1位の場所は新宿駅東口で、2位は横浜駅西口である。このグラフはいわゆるロングテールと呼ばれ、オンラインショップの商品の売れ行きなどで起きている。これらの位置情報を k -匿名化する場合は、まず保護の基準値を決め、「2-匿名」を確保する場合は $k=1$ となる点（12時の場合は16,749位）を探し、その右側の位置に対して何らかの保護を行う。移動経路の場合は、このようなロングテールの状態で分布する位置の中から移動先の位置を選んで行動するため、基本的に図7のロングテールよりも更に「長い尻尾」、すなわち保護対象が増える⁽⁵⁾。

5. 移動履歴の匿名化のケーススタディ

5.1 匿名化のための一般化メッシュトリー

ここから移動履歴の匿名化のケーススタディ実演に入る。本スタディは東京大学空間情報科学研究センターの人の流れデータ⁽⁴⁾を用いた研究⁽⁶⁾に基づく。ここでは集合匿名化の方法として、一般化と削除による方法を採用する。一般化とは値を丸めたり、上位の概念に変換することで、孤立していたデータを集合化する方法である。一方、一部の外れ値を持つレコードを除くと元々集合化

されているようなデータに対しては、その外れ値を削除することも有効である。一般化と削除を併用することも可能である。

位置情報の一般化は、より広いエリアへ変更することによってできる。今回は地理的領域（メッシュ）を階層化したトリーを作成し、一般化はトリーの末端から上位階層に上ることにより行う。実験のために2種類のメッシュトリーを作成した。一つは単純メッシュトリーでもう一つは人口メッシュトリーである。両メッシュの例を図8、9に示す。

単純メッシュトリーは各階層で各メッシュの面積が等しくなるようにした。全体領域からトップダウンに、面積を半分にするように縦または横方向の領域分割を行っている。一方人口メッシュトリーは各階層で各メッシュに存在する人口が同じになるようにした。同じくトップダウンに人口が半分になるように縦または横方向の領域分割を行っている。なお人口メッシュトリーは7:45の時点の単独位置情報に基づいて作成した。両トリーは次

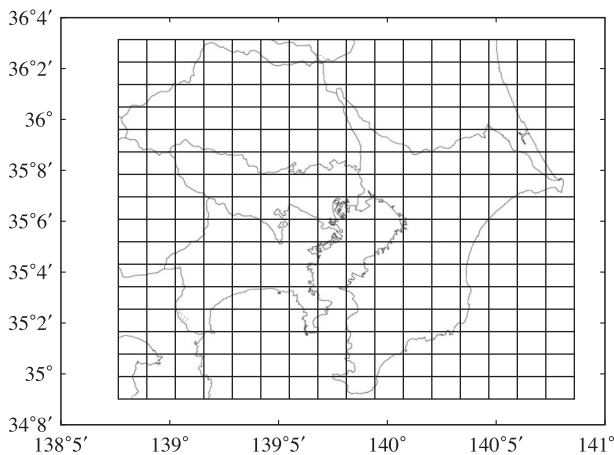


図8 単純メッシュの例（メッシュ数128）

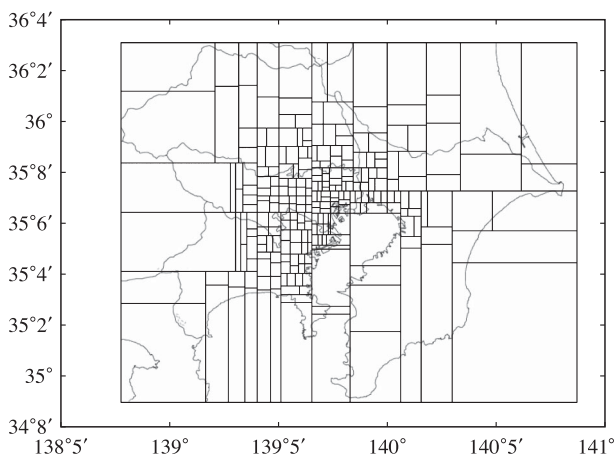


図9 人口メッシュの例（メッシュ数256）

のような性質を持つ。

・ 単純メッシュ：

トリーの階層が深く、トリーの同じ階層での集合匿名化の度合いにはばらつきがある。このため一定の匿名化レベルを得るためには人口が粗な地域に引きずられて階層を高くする極端な一般化が起こることがある。

・ 人口メッシュ：

トリーの階層が浅く、トリーの同じ階層での集合匿名化のばらつきは低い。このため極端な一般化は生じにくい、メッシュの面積・形状にばらつきが出る。

図8、9はそれぞれメッシュ数が256個の例である。

例えば、両メッシュトリーを用いて8:00時点での単独位置情報（移動履歴セットA、レコード数は269,865、ユニーク位置種数140,408）に対する $k=2$ の集合匿名化を行ってみる。メッシュ数256（ $=2^8$ 、およそ10km四方相当）レベルでは、人口メッシュでは全ての位置情報が256通りに理論値に近い等分の人口で一般化され2-匿名が達成される。一方、単純メッシュでは172通りに一般化され、うち「一人しかいない危険な」メッシュ（ $k=1$ メッシュ）が2個現れるので、このメッシュのデータを削除すれば集合匿名化が達成される。

メッシュ数32,000（ $\approx 2^{15}$ 、およそ1km四方相当）レベルでは、人口メッシュでは27,380通りに、単純メッシュでは10,704通りに一般化される。 $k=1$ メッシュは単純メッシュで2割弱、人口メッシュでは1割弱現れ、2-匿名を達成するためにはこれらのメッシュを削除することになる。 $k=1$ メッシュはデータセットの位置情報のマイクロな偏り（例えば、同じ位置情報が多数いる）ことによる一般化トリーの飽和によって生じる。

5.2 移動履歴の匿名化実験1

それでは、移動履歴の匿名化実験を行う。目的は移動履歴に対して、集合匿名化を行うとき、どのようなパラメータで、どのような匿名化が達成できるかを体験するためである。概要を以下に示す。

匿名化を行う際のパラメータ

- ・ 集合匿名化の安全性指標（ $k=2, 5, 10$ ）
- ・ 移動履歴の長さ（ホップ数=1, 2, 3）
- ・ 時間帯（朝8時台/9時~12時（午前中））

匿名化手法

- ・ 一般化トリーによる位置情報（緯度経度）の一般化

匿名化の結果の評価指標

- ・ 集合匿名化達成率（一般化の結果、 k 値の条件を満たすレコードの割合）

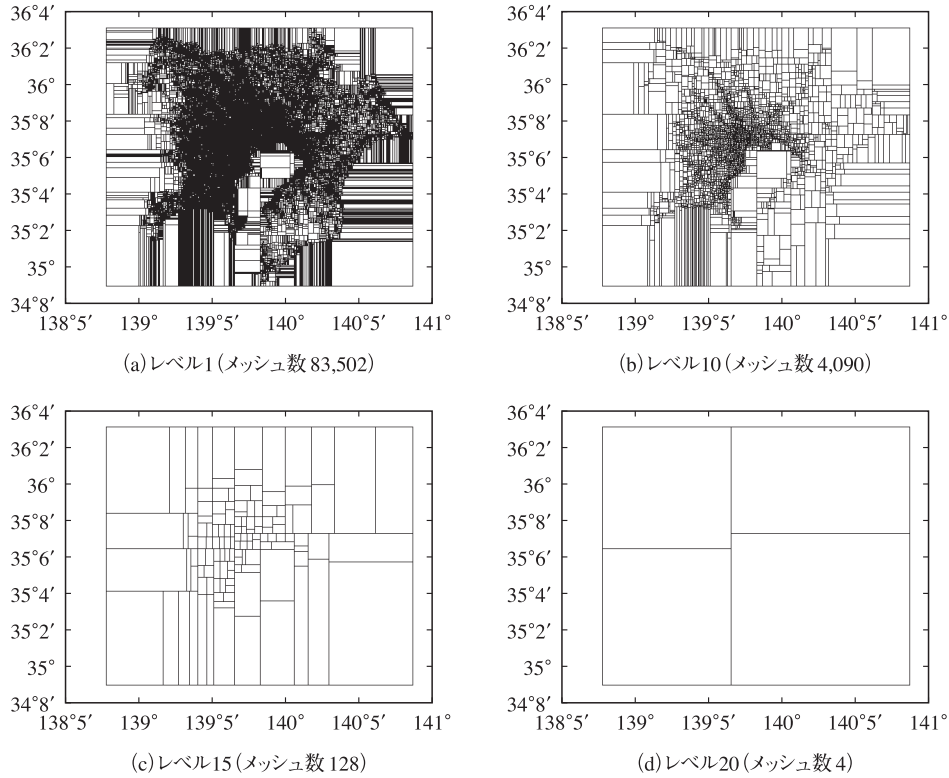


図10 人口メッシュトリーの例 東京都市圏を83,000個から1個のメッシュへと22レベルに階層的に分割した。

データセット

- ・ 移動履歴セット A (朝8時台) : 27万レコード
 - ・ 移動履歴セット B (午前中) : 21万レコード
- 一般化トリー (レベル)
- ・ 人口メッシュトリーの1~22階層 (図10)

実験結果を図11, 12に示す。図11は集合匿名化の安全性指標を $k=5$ に固定してメッシュの階層を変化させた場合、集合匿名化がどの程度達成できるかを見たものである。(a)が8時台、(b)が午前中のデータに対するものである。左のグラフにおいて、長さが1ホップの履歴では、何もしなくても $k=5$ を満たすレコードが2割弱存在する(元データの解像度にも依存するので一般的な事実かどうかは注意が必要)が、長さが3ホップの履歴では一般化を行わないと $k=5$ を満たさない。すなわちこの条件下でデータを「安全に活用」するためには、元データの粒度を保ちたいのであれば1ホップの履歴で8割以上を削除する必要がある、さもなくば一般化を行って、粒度の丸まりを受け入れるしかない。

図12は集合匿名化の安全性指標を $k=2, 5, 10$ と変化させたとき、集合匿名化がどの程度達成できるかを見たものである。データセット A と B に対して、長さが1ホップのものと3ホップのものを対比させている。移動履歴が短い方が長い方よりも、また顕著ではないが8

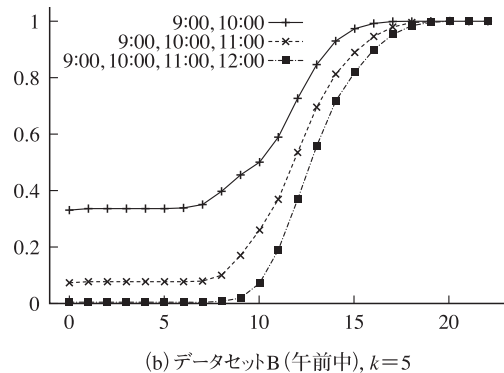
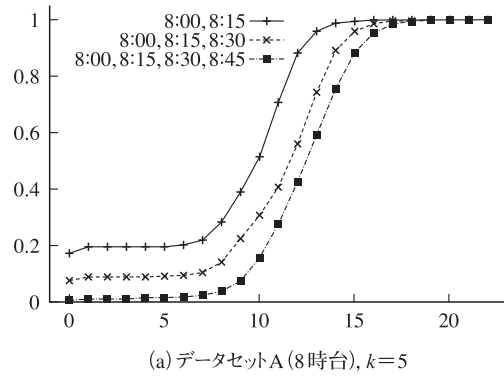


図11 移動履歴の匿名化、安全性指標を固定(横軸は匿名化のレベル、縦軸は集合匿名化達成率)

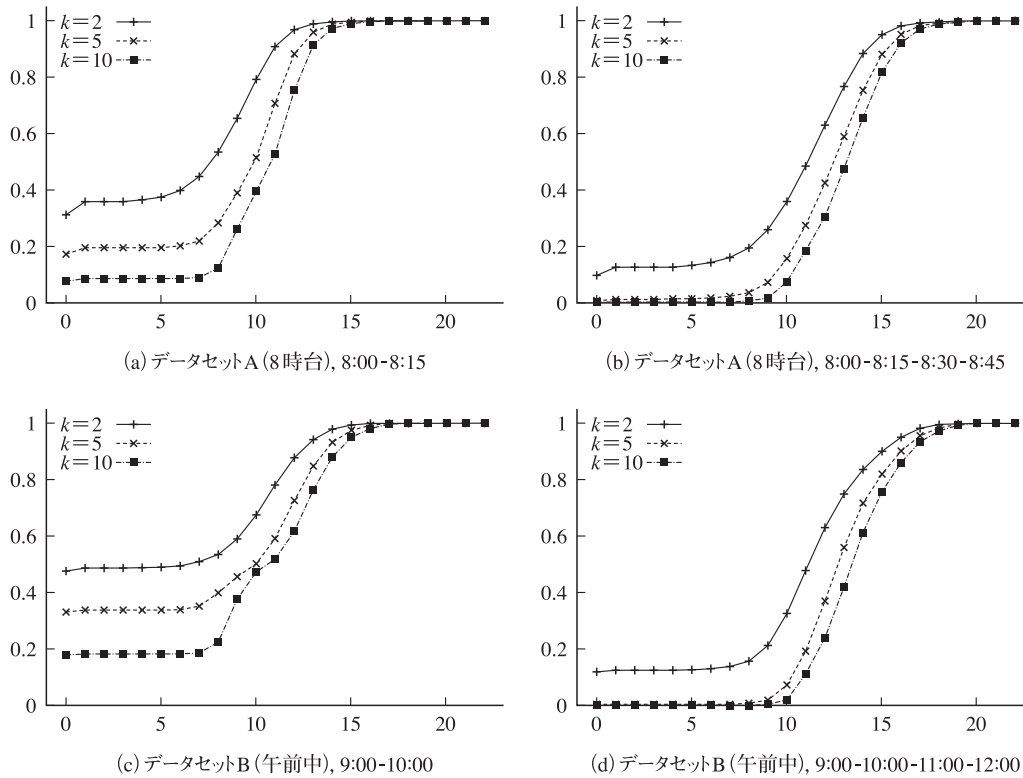


図 12 移動履歴の匿名化, 安全性指標を変化 (横軸は匿名化のレベル, 縦軸は集合匿名化達成率)

時台 (45 分間) の方が午前中 (3 時間) よりも, 集合匿名化が達成しやすい, すなわち「同じような行動を取っている人」が多い。以上から, このデータセットにおいては, 集合匿名化の考えにおいて安全と主張できるデータを作るためには, 以下の選択肢がある。このように何かを犠牲にしなくては匿名化データは得られない。

- 元データの位置の粒度を保ちたいのであれば, データの大半を削除する (多くの人が移動する経路のみ使う)。
- 元データを一般化して, 一定数のデータも併せて削除する (例, 図 11 (a) の場合, 一般化レベル 12 の数 km 四方相当の一般化を受け入れ, 10~60% 程度のデータを削除する)。

なお, グラフの曲線の傾向であるが, 一般化が機能する区間 (x が 10~15 の間など) においては, 一般化のレベル (X 軸) と達成率 (Y 軸) は比例する (X 軸が階層なので対数的に増える)。また, 一般化レベルが一定の値に達するまで匿名化の達成率 (Y 軸) は変化しないのは, 一般化手法に影響を受けているものと考えられる。このケースでは人口メッシュトリーが低位では飽和しているため低ランクでは変化が起きにくい。

5.3 移動履歴の匿名化実験 2 (分析への適用)

移動履歴の利用目的には, ある地点から別な地点への移動者の属性を理解しマーケティングに用いる, といったものが考えられる。人の流れデータは位置情報以外の属性情報も含むので, ここではそれら属性も用いて簡単なデータマイニングを行ってみよう。

使うデータセットはデータセット A 相当のデータで, 更に属性として年齢 (5 歳刻み), 性別, 移動目的 (通勤/通学) を持つもので, これに対して人口メッシュ (メッシュ数 256 レベル) を用いて安全性指標 $k=5$ の集合匿名化を行った。そこから 1 ホップの移動履歴のうち X 地点にいる人は Y 地点へ移動する特徴があるものを抜き出した結果が図 13, 14 である。(相関ルール分析を行い, 最小サポート値 0.00001 のものを抜き出した。) 図 13 は移動目的が通勤のもので, 都心へ集中するトラヒックが明示されている。図 14 は通学のもので, こちらは通学圏といった近隣のメッシュへの移動が見て取れることが興味深い。

6. 匿名化の限界とその先にあるもの

ここまで, 移動履歴の匿名化のケーススタディを行った。利用した人の流れデータも人の移動履歴の一例にすぎないし, 今回採用した人口メッシュ方式の一般化が最良の方式であると提案するものではないが, 匿名化にま

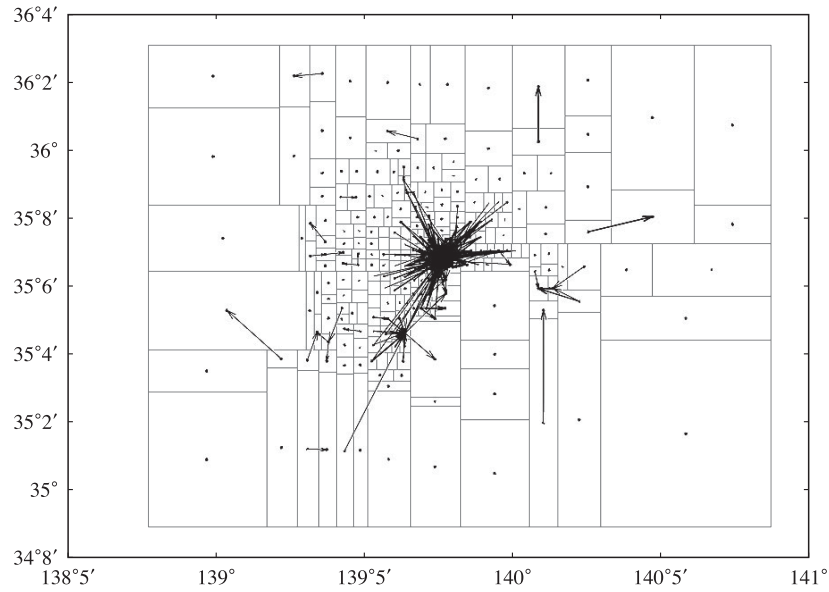


図13 移動履歴の相関ルール（通勤）

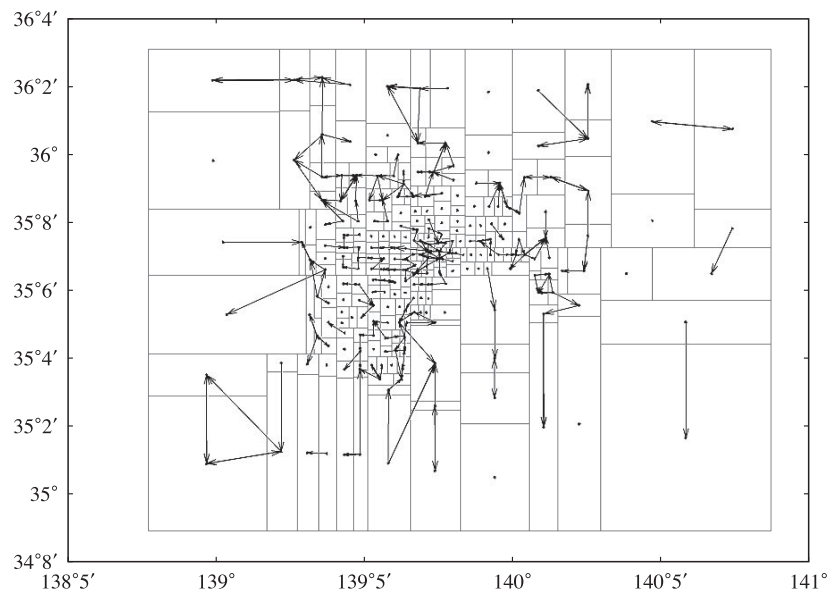


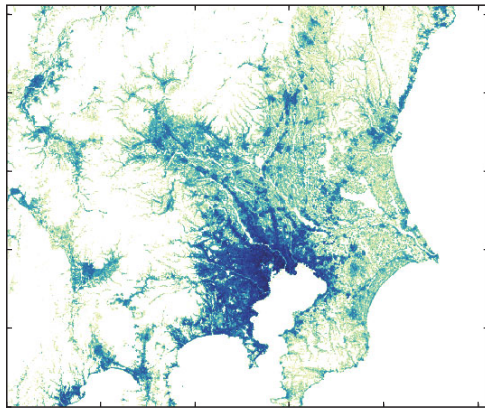
図14 移動履歴の相関ルール（通学）

つわるプロセスの概要と、それがどの程度〈役に立つ〉のかの感触はつかんで頂けたものと思う。集合匿名化を行うと、データを粗くするか、データを削除するかという選択肢を受け入れる必要がある。このような性質に関する具体的な技術情報の共有とそれに基づくベストプラクティスの集積が重要である。

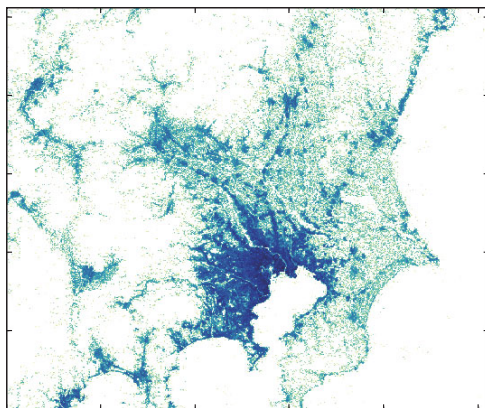
匿名化手法の代表である集合匿名化を中心に議論してきたが、それ以外の方法についても触れる。集合匿名化に代わる方法として、データに「雑音」を乗せて、本当のデータを分からなくするランダム化手法がある。ランダム化で安全性の理論の解析が進んでいるものに、

P_k -匿名化（確率的な匿名性を達成する個票のランダム化）や差分プライバシー（集計データから個人のデータの特性を防ぐ集計データのランダム化）がある。これらはいわば人工的にデータを作成するアプローチであり、実ビジネスでこれらがどのように受け入れられていくかは未知の部分があるが、データを粗くするか、データを削除するかという集合匿名化の煩わしさを避けたいのであれば、ランダム化が極めて有力であると筆者らは考えている。

ここに移動履歴のランダム化の例を示したいところであるが、図15に静的な位置情報の集計データをランダム



(a)オリジナル



(b)差分プライバシーを適用

図 15 位置情報の集計データのランダム化の例 ((a)オリジナル, (b)差分プライバシーを適用)

ム化した最新の研究成果を文献(7)の講演スライドより引用する。データは平成 22 年国勢調査 500 メートル四方の地域メッシュ人口を用い、メッシュ人口の各値を保護するためにランダム化をしている。行った処理は地域メッシュ人口に対してラプラス雑音を付与することを基本としたもので、差分プライバシーと呼ばれる性質(集計値から個の影響を排除する)が達成されている。

移動履歴の匿名化には限界が存在する。匿名化によるデータ活用は、その限界をよく理解した上で行うことが重要である。更なるその限界を超えて、例えばデータの粒度を細かく扱いたいとか、データを削除なく使いたい

あるとかの必要があるならば、そのデータのプライバシーリスクを明らかにした上で、できるだけリスクを小さくした活用が重要である。

文 献

- (1) 高橋克巳, “個人の移動履歴の保護—プライバシーリスクを明らかにした利活用—,” 情報処理, vol. 55, no. 12, pp. 1373-1380, Dec. 2014.
- (2) パーソナルデータに関する検討会, 技術検討ワーキンググループ: 報告書, 2013.
<http://www.kantei.go.jp/jp/singi/it2/pd/dai5/siryou2-1.pdf>
- (3) パーソナルデータに関する検討会, 技術検討ワーキンググループ: 報告書, 2014.
<http://www.kantei.go.jp/jp/singi/it2/pd/dai10/siryou1-2.pdf>
- (4) 東京大学空間情報科学研究センター, 「人の流れプロジェクト」.
<http://pflow.csis.u-tokyo.ac.jp/>
- (5) 菊池浩明, 高橋克巳, “乗降履歴データの安全な匿名化は可能か?,” 第 31 回暗号と情報セキュリティシンポジウム (SCIS2014), 303-4, 2014.
- (6) R.S. Yamaguchi, K. Hirota, K. Hamada, K. Takahashi, K. Matsuzaki, J. Sakuma, and Y. Shirai, “Applicability of existing anonymization methods to large location history data in urban travel,” 2012 IEEE Intl Conf on Systems, Man and Cybernetics, pp. 997-1004, 2012.
- (7) 寺田雅之, 鈴木亮平, 山口高康, 本郷節之, “大規模集計データへの差分プライバシーの適用,” コンピュータ・セキュリティ・シンポジウム 2014, 301-2, 2014.

(平成 26 年 10 月 31 日受付 平成 26 年 11 月 28 日最終受付)



高橋 克巳 (正員)

昭 63 東工大・理・数学卒。平 18 東大大学院情報理工学系研究科博士課程了。昭 63 日本電信電話株式会社 (NTT) 入社。情報検索, データマイニング, 暗号, プライバシー保護の研究に従事。現在, NTT セキュアプラットフォーム研究所主席研究員。博士 (情報理工)。



正木 彰伍

平 20 名大・理・物理卒。平 25 同大学院素粒子宇宙物理学専攻博士課程了。同年日本電信電話株式会社入社。以来, プライバシー保護技術の研究開発に従事。現在, 同社研究員。博士 (理学)。平 23-24 年度日本学術振興会特別研究員。



濱田 浩気 (正員)

平 19 京大・工・情報卒。平 21 同大学院修士課程了。同年日本電信電話株式会社入社。以来, プライバシー保護技術の研究に従事。現在, 同社研究員。平 23 SCIS 論文賞, 平 23 年度情報処理学会論文賞, 平 24・平 26 CSS 論文賞, 平 25 年度山下記念研究賞各受賞。