基般

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―

高橋 克巳　NTT セキュアプラットフォーム研究所

個人の移動履歴の保護とは

移動履歴の取り扱いが議論を呼んでいる．人の移動が分かれば，商店は無駄なく仕入れができ，自治体は効率よく道路を整備できるだろう．一方，移動履歴をみだりに流通させると，誰かがどこに行ったかが他人に分かってしまい，その結果不都合が起きてくる可能性がある．

パーソナルデータの保護に関して聞かれる質問の代表に「これは個人情報に該当しますか？　該当するならどういう匿名化をすればいいですか？」という 2 点セットがある．しかし移動履歴活用の現状はそれほど単純ではない．

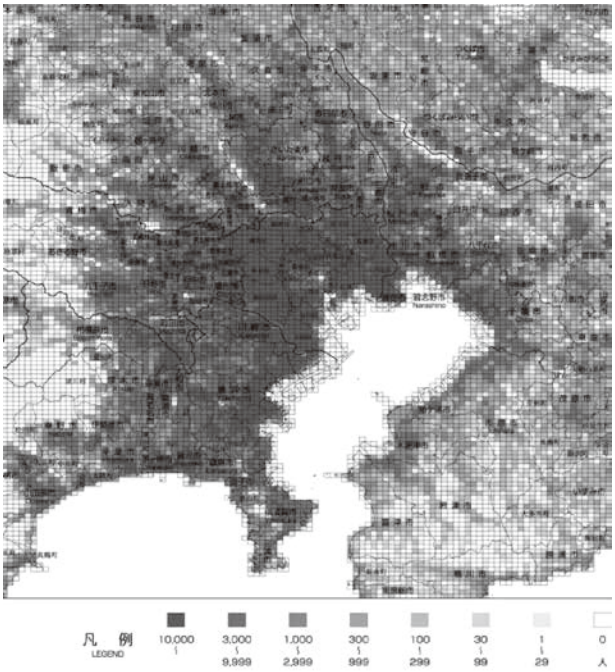
移動履歴の保護を考える上で，その履歴が個人情報に該当するのかしないのかは最初に考慮すべきポイントである．法律上の個人情報に該当するのであれば，その取扱いには法律上の制約が存在し，それに基づいた保護が必要である．しかし移動履歴が個人情報なのかそうでないのかの判断は悩ましい．たとえば「A さんが B 地点から C 地点に移動した」という履歴は個人情報であるし，「30 万人が昨日東京から大阪に移動した」は個人情報ではないだろう．では個人の氏名と結びつきのない「ある人の昨日 1 日分の 1 時間間隔の GPS 位置情報」や「ある人の 1 週間分の乗降駅名」はどうだろうか？　こういった問題に答えるのは簡単ではない．一方，利用しようと考えていた移動履歴が個人情報でないと判断できたとしても，さらに何らかの保護策をしないといけないのではないだろうか？などと悩む声も聞く．移動履歴を利用する事業者にとって，個人情報かどうかの判断は難しく，判断できたとしてもすっきりとしない，それが現状である．

本稿では思い切って，移動履歴の保護をそれが個人情報に該当するか否かの 2 元論で考えるのをやめることにしてみよう．本稿の移動履歴の保護に対する立場は〈個人情報を匿名化する〉のではなく，その代わりに〈個人情報をデータ分析に支障が出ない限り個人が分からないように加工して，残るプライバシーリスクを明らかにする〉ことである．すなわち，活用する際にプライバシー上のリスクを判断し，それを減じるためにどんな措置を講じたか，その結果どんなリスクが残ったかを明らかにする規律を持つことである．その規律の中身は一律に決まるものではなく，移動履歴の性質に応じて決まるものだ．この具体例の検討は，現在各所で行われているが十分ではない．こういったプラクティスを少しでも数多く，具体的に積み上げていくことが我々情報処理技術者の役割である．本稿の目的は，移動履歴のプラクティスを集積するために，移動履歴のプライバシーリスクとそのリスクを軽減する手法の類型化について考えることである．

位置情報と移動履歴

■ 位置情報と移動履歴の性質

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る．動物や機械の移動履歴もあるかもしれないが本稿では対象としない．位置情報は緯度



出典）総務省統計局 平成 22 年国勢調査に関する地域メッシュ統計関東大都市圏 人口総数 より引用

図 -1　人の位置の偏り

経度などの場所を示す情報と時刻からなるとする．

人の位置情報は空間的に偏りがあり，かつ一意性がある．**図 -1** は東京の人口を 1 キロメートルメッシュ単位で図示したものである．これは深夜のある時刻の東京近郊の住民の位置情報とみることもできる．人の位置情報は居住や勤労を含めて地理的制約を受けるので一様にもランダムにも分布しない偏りのある情報である．偏りがあることで，人が多数いる地域が現れる．さらに人の移動は地理的制約を受け，無作為に次の地点を選べないため〈自分を隠す〉同じ移動履歴を持つ人々を見いだすことの期待が持てる．しかし，人の位置に偏りがあるとしても，位置（空間と時間）の分解能を上げれば〈まったく同じ場所・時間〉に同じ人がいることはなくどの位置情報も同じものが 2 つと存在しない一意な情報になる．移動履歴は位置情報の系列である．一意性のある位置情報を系列化すると一意性のある移動履歴となる．位置の分解能を下げて位置情報の一意性をなくすことは可能だが，必ずしもその移動履歴の一意性がなくなるとは限らず，系列数を増やすことで一意になる．移動履歴の偏りの性質は保護に役立つが，一方一意性が保護を困難にする．

■ 移動履歴の保護

移動履歴の保護をするためには，プライバシーリスクを明らかにすることと書いた．プライバシーリスクの代表的なものは，活用するデータから個人が特定されることである．個人の特定により，移動履歴に含まれていた秘密情報，たとえば内緒の寄り道先が，誰かに知られるといった不利益が想定される．一般に移動履歴単体で個人が特定されることはないが，移動履歴は多くの場合一意性のある情報であり，一意性のある情報は他の情報と組み合わせることによりその履歴が誰のものか分かる，すなわち個人特定に至る可能性がある．ほかにもいくつかの留意すべきリスクがあるが詳しくは後述する．

移動履歴の保護は，単なる技術的措置ではなく，技術と運用ポリシーのセットで考えることが妥当である．移動履歴を誰かに提供する場合，何らかの情報が提供先に知られる．その何らかの情報が，不幸にもある個人の特定に至る調査のパズルの最後の 1 ピースになることが絶対にないとは言えない．プライバシーリスクが否定できないとき，とるべき態度はどのようなものか．リスクをなくすために，たとえば位置の分解能を 50 キロメートル四方まで粗く加工するような〈匿名化〉を行うことも考えられるが，そのようなデータは有用なのだろうか．おそらく多くの移動履歴データ分析において〈役に立つデータはプライバシーリスクを持つ〉という考えが当てはまるだろう．したがって，技術がそのリスクをできるだけ小さくし，残ったリスクが悪用に用いられることを運用ポリシーで禁じるということが現実的ではなかろうか．

以上から技術の役割は，移動履歴の活用業務が行える範囲内で，プライバシーリスクができるだけ低くなるよう，履歴データを加工することである．そのためには移動履歴の活用業務の類型化が必要である．

■移動履歴の活用

移動履歴を使って何をするのか？　一般に，データ分析の目的が不明であれば，〈とりあえずできるだけ高い精度の位置を，できるだけ長い系列で使いたい〉ということになるかもしれないが，プライバシーリスクを低くするためには適切な情報量を持つ移動履歴を使うべきである．ここでは移動履歴活用業務を類型化する目的で，移動履歴の情報量のパラメータを考察する．パラメータは情報量が多い順に記述しており，下位にいくほどプライバシーのリスクが小さくなる．移動履歴の活用を考えるときは，どのような情報があればよいのかを考え，下記のパラメータを参考にして必要以上に詳細な移動履歴を使わないことがプライバシーリスクを減じることにつながる．なお，下記のパラメータの選定，および各パラメータを組み合わせたときのリスクの定量化には未知の部分が多く，数理的な解析が必要である．

【移動履歴のパラメータ】

A. 移動履歴の長さ
- 長い履歴が必要か（多数の位置の系列）
- 2 点間の履歴でよいか（起点・終点の 2 地点）
- 地点別でよいか（1 地点）

B. 位置情報（場所）の分解能
- 数センチメートル単位（手を伸ばした棚）
- 数十センチメートル単位（店内の個所が分かる）
- 数メートル単位（立ち寄った店舗が分かる）
- 数百メートル単位（商店街・大規模施設）
- 町・駅圏・観光施設圏
- 市区町村
- 地域

C. 位置情報（時間）の分解能
- 秒単位
- 5 分単位
- 1 時間単位
- 日単位

D. 位置情報（場所）の網羅性
- 場所を限定しない
- 場所を限定（特定地立ち寄り履歴のみ）

E. 位置情報（時間）の網羅性
- 時間を限定しない
- 時間を限定（ある日時の移動履歴のみ）

個人情報保護に関する基礎知識

個人情報保護の法律に関する基礎知識について簡単に触れる．

個人情報の保護に関する法律（平成十五年五月三十日法律第五十七号）[1] において，個人情報は「特定の個人を識別できるもの」と定義されている．個人情報を取り扱う事業者においては，利用目的の特定，適正な取得，第三者提供の制限などが義務として定められており，目的をはっきりさせず，勝手に集めてはならず，勝手に他人に渡してはならない．ただし適用除外もあり「大学その他の学術研究を目的とする機関若しくは団体又はそれらに属する者　学術研究の用に供する目的」の場合は義務が適用されないと明記されている．

現在この保護法は改正に向けた議論が行われている．内閣に設置された IT 総合戦略本部で開かれたパーソナルデータに関する検討会がその場で，その検討は 2013 年 9 月から行われ，2014 年 6 月に「パーソナルデータの利活用に関する制度改正大綱」としてまとめられた．

改正の趣旨はビッグデータ時代になり，移動履歴に代表される個人情報であるのかないのか分かりにくいパーソナルデータの活用を円滑に行うことにある．活用は同意をとって行うならば基本的に問題がないが，本人の同意なしの利活用（第三者提供を含む）を行う方法が議論された．それに関する問題点が同検討会に設置された技術検討ワーキンググループで議論されている．

技術 WG が議論したのは，主に以下の 2 点である．

(1) 匿名化の限界

(2) 識別情報のプライバシーリスク

前者の匿名化に関しては「いかなる個人情報に対しても適用できる汎用的な匿名化は存在しない」と

結論づけ，ケースバイケースの対応が必要だとされた[2]．この議論の中で用いられた用語が「特定」と「識別」である．匿名情報というあいまいな概念が退けられ，その代わりに，「識別非特定情報」（それが誰か1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，さらに，それが誰か一人の情報であることが分からない）という概念が導入された．個人情報から氏名，住所，年齢，性別を取り除くだけの非特定化処理は容易であるがプライバシーリスクが残る可能性が高い．一方，非識別のレベルまで加工することはデータに応じた丁寧な対応が必要で，しかも非識別のレベルまで加工したデータは，データマイニング対象として果たして意味があるのだろうかということが問題となったのである．そこで，もし（非特定）識別情報のレベルのデータを活用したいのであれば，なんらかの運用上の制約を伴わせることが妥当であるとされた．すなわち識別情報に対して個人特定を行わないことを宣言し，それに反した場合に法的なペナルティを受けることがその例である．

後者の識別情報のプライバシーリスクに関しては，「準個人情報」という用語を用いてリスクのある情報が提案された[3]．（非特定）識別情報は文字通り誰の情報であるかは分からないが，個人が特定されるおそれのある情報数十をピックアップして詳細な分析が行われた．その結果，個人に対して大量または多量の情報が収集され得る「識別子」相当の情報が準個人情報であると報告がされている．準個人情報の基準としては，「本人または本人の所有物と密接性」があり，「一意」で「共用性」があり，「変更できない」ものとされた．具体的には，運転免許証番号や端末のMACアドレスなどのID的なもの，および指紋，DNA，顔認識データなどの生体情報的なものが指摘された．この中で移動履歴に関しても慎重な検討が行われ「移動履歴はその情報が蓄積されればされるほど，個人が特定される可能性が高くなる．また，他人と違う特異な日時に，または特異な行動をすることで他人と区別される可能性が高いといえる．ただし何が特徴的な行動履歴であるのかを一律の基準に基づいて判断することは困難である」と，準個人情報とはされなかったが特性が指摘されている．

移動履歴の持つプライバシー上のリスク

本章では位置情報のプライバシーリスクの類型化を試みる．リスクは移動履歴を受け取った側（受領者）が移動履歴から何が分かるかにかかわる問題で，個人の特定に関するものと，それ以外のものに大別される．個人特定の基本的なものは我が国を含む各国の個人情報保護法の定義によるものであるが，他は法制度になっておらず，技術的観点から指摘するものである．ここに列挙したリスクには大きさに差があり，かつ網羅性もあるとはいえない．したがって，これらリスクをしらみつぶしに対応していくというのではなく，リスクの自発的な調査と，必要性を判断した上での対応が求められる．

■移動履歴の仮定

本稿で扱う移動履歴の定義を，以下の項目からなると仮定する．

識別番号＋位置情報の系列（緯度・経度・時間）＋秘密情報

氏名等の個人が特定できる情報は取り除かれているとし，個人を参照するために割り振られた識別番号で管理されるとする．同番号は個人に対して任意に与えられるものとし，運用に応じて個人を1年間管理するものもあれば，1時間のみ管理するものもあるとする．位置情報の系列は，左記運用の単位に応じた同一の識別番号の位置情報が複数まとめられているものとする．秘密情報はたとえばその人の購入物品などが考えられるが，位置情報の中の秘密にしておきたい場所であってもよい．秘密情報は移動履歴の構成上本質的ではないが，秘密情報がないと保護を考える必要がないため便宜的に入れている．なお問題の単純化のため，秘密情報に氏名，住所，年齢や性別等の個人特定につながる属性はないものと

する．

■個人特定 1（特徴的な場所による他の情報との照合）

移動履歴に含まれる位置に特徴的な場所と解釈できるものが含まれる場合，特徴的な場所を使って他の情報と照合することにより個人特定がされる．たとえば，移動履歴から自宅住所が分かれば，その住所を使って名簿等と照合し，個人の特定ができる．特徴的な場所の例としては，自宅住所や個人事務所所在地などがある．

■個人特定 2（パターン性のある移動履歴同士のマッチング）

パターン性を持った移動履歴があり，そのパターンが他でも既知である（他の手段でも収集されている）場合，両者をマッチングすることができればより情報量の多いデータが作り出され，その結果個人特定に至る．たとえば，移動履歴にユニークな通勤経路が含まれている場合で，他のサービスで通勤経路と氏名を同時に把握したデータがある場合，前者は後者とのマッチングで個人特定が起こる．移動履歴が複数のサービスで利用されることが当たり前になってくると，このリスクへの備えの必要性が現実的になる．

■個人特定 3（受領者の知識に依存した特定）

移動履歴の中に受領者が知り得た情報がある場合，個人特定がされる．たとえば，受領者がある人が何時何分にどこにいたか目撃していた場合，ある人が自分が何日何時にどこにいたかを SNS で公開していた場合などがこれにあたる．このリスクは移動履歴ならば必ず起こることではなく，受領者がたまたま知り得たとしても，その情報を使った個人特定をしなければ済むことである．ただし，SNS 情報を大量に継続的に収集し続けると，このリスクが容易に実現される可能性がある．

■個人到達（待ち伏せ）

パターン性を持った移動履歴がある場合，その履歴に従えば，（誰かは分からないが）その人に意図的に出会う（待ち伏せする）ことができる．移動履歴に特徴的なリスクである．秘密情報に〈金持ち〉のような属性がある移動履歴は公開しないに越したことはないだろう．

■属性推定と濡れ衣

個人の特定が起こらなくても，プライバシーの問題が起こることがある．それが属性推定と濡れ衣という現象である．

同一の位置情報の系列 L1 を持つ移動履歴が複数あり，そのすべてが同じ秘密情報 S1 を持つとき，その移動履歴データベースに含まれる個人は，位置情報の系列 L1 を持つならば，属性 S1 を持つことが推定されてしまう．また，同様に同一の位置情報の系列 L1 を持つ移動履歴が複数あり，そのどれかが秘密情報 S1 を持つとき，位置情報の系列 L1 を持つならば，属性 S1 を持っているかもしれないことを疑われる可能性がある．これらはたとえば（移動ではないが）A 地域に居住していれば B という病気に感染しているという推定，あるいはまれな B という病気が A 地域で発生したので A 地域に居住していれば B という病気に感染しているかもしれないという濡れ衣，などが典型例となる．

移動履歴の持つリスクの軽減方法

■移動履歴・位置情報加工の基本技法

移動履歴や位置情報を加工する基本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き換え
- 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，本稿での移動履歴の仮定では氏名等の個人が特定できる情報は取り除かれていることとしたが，一般的には上記の加工を行うならば，以下の加工が前提となる．
- 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）

■移動履歴の持つプライバシー上のリスクを軽減する加工方法

前説で述べた加工方法を組み合わせて，移動履歴のプライバシーリスクを下げてみることを考察する．

図-2，**図-3** はそれぞれ位置情報の一般化，ランダムな置き換えの概念を示したものである．一般化はエリア単位で扱うことでエリアあたりに複数の人がいる状況を作り出し個人識別性を下げる．たとえば位置をメッシュで管理し，そのメッシュの面積を大きくする．ランダム化は位置を実際とは異なる位置に確率的に移動させることで，その位置が実際の位置なのか，人工的な位置なのか分からない状況を作り，個人識別性を下げる．たとえば位置の値にノイズを乗せたり，他の人の位置と置き換える．どちらのデータも元の位置とは異なるデータになる場合があるが，統計的に扱う場合そのデメリットを補う方法がある（前者は代表値として扱う，後者は補正して使う，等）．

図-4 は一般化による移動履歴のプライバシー保護の例である．削除を組み合わせて使っている．2つの移動履歴の近接する位置情報同士を，位置を一般化することにより同一視することで，単独の場所をなくす．最終地点は地理的に異なるため，一般化でまとめることができず，削除をしている．この一般化は k=2 の k- 匿名化[4]（同じ属性を持つレコードが少なくとも k 個存在することを保証する加工方法）相当であり，同じエリアにいる人数（k の値）が大きければ大きいほどプライバシーリスクは小さくなる．一般化として扱うエリアを広くするほどリスクは下がるが，エリアの決定は簡単ではない．位置情報には偏りがあるため，一様な一般化を行うと，位置情報が粗な地域では必要な非識別性が得られない場合がある．また，包含される位置情報数に応じてエリアを決めると，行政界や街としてのまとまりとは無縁で分析に扱いにくいエリアが形成されてしまう可能性もある．非識別度（k の値の大きさ），一般化の分解能（の小ささ），一般化されたエリアの使いやすさ，削除される位置情報の少なさ，等の最適化が課題である．なお，いわゆるヒートマップ（人の平面分布の多寡を色で表現したもの）も位置

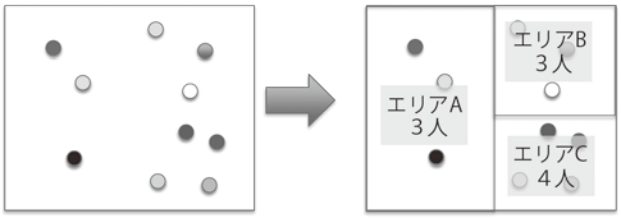


図-2　位置情報の一般化

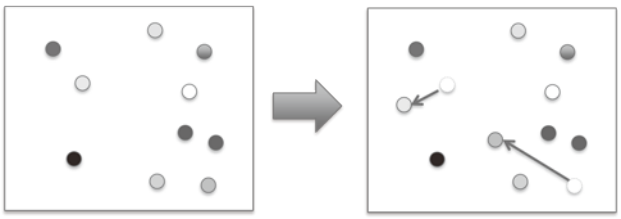


図-3　位置情報のランダム化

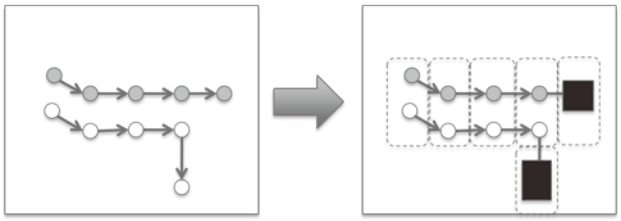


図-4　移動履歴の一般化

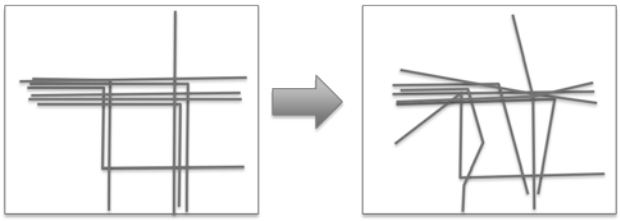


図 -5　移動履歴のランダム化

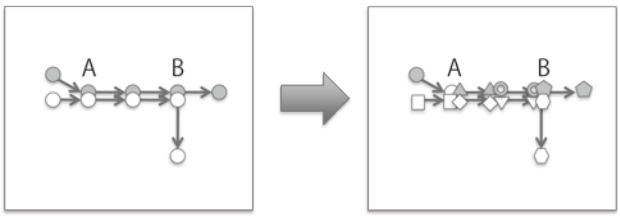


図 -6　移動履歴の分割と交差

情報を一般化したデータの表現の一形態である．

図 -5 はランダム化（もしくは Obfuscation）による移動履歴のプライバシー保護の例である．図 -3 で説明した考えで識別性を下げる．この方法では基本的には位置情報の分解能は変わらず，上位エリアという概念は発生しない．ただし，確率的に測定値と異なる位置情報が存在する．ランダム化の度合いと非識別度の関係（ランダム化の安全性評価は直感的に分かりにくいが，k- 匿名性との論理的整合性があると考えられている），ランダム化の度合いとデータ有用性の関係，データの補正方法（再構築などと呼ばれる），等が課題である．

図 -6 は分割と交差による移動履歴のプライバシー保護[5]の例である．図では各ノードが単位時間毎の位置情報を示しているが，移動履歴を単位時間の長さで始点終点の形式に分割し，かつ分割履歴間の関係を断ち切る（異なる識別番号を振る）．図では交差点 A と交差点 B で 2 つの移動履歴が交差しているが，履歴を分割することで，北西から A に入ってきた履歴が B で東に抜けるのか南に右折するのかは分からない．このような仮定をおいたとき移動履歴は確率過程として表現され，プライバシーの安全性はある人がどのノードに移動していくかの不確かさ（エントロピーの和）として評価される．各分割履歴を時間的に前後と独立事象として扱うと，たとえば元々のオリジナルの履歴の始点と終点に相関がある場合（北から来た人は南に抜ける）の評価ができないなど，長い履歴のプライバシーと偏りの評価のトレードオフが課題である．

移動履歴の保護と活用の制度化の現状

移動履歴の保護の制度化の状況として注目すべきものは，前述の個人情報保護法改正に向けた「パーソナルデータ検討会」が 2014 年 6 月までに行った報告群である．前述の通り，安易な匿名化に頼る状況に警鐘を鳴らす内容となっており，プライバシーリスクのある識別情報の活用は運用上の制約を伴わせることを基本としている．最終的にまとめられた「大綱」においても〈匿名化〉の文字はなく〈加工〉という表現がとられていることが象徴的である．報告書[2]では乗車履歴の識別性分析が報告されており，乗車履歴は多くの場合識別情報となり，識別を防ぐためには数多くのレコードを削除する必要があることが述べられている．また報告書[3]では移動履歴の継続・広域的な収集のリスクについて分析がなされ，準個人情報としての保護の必要性の認定こそ慎重に避けられたが，配慮が必要であることが報告された．

総務省は 2014 年 5 月に位置情報プライバシーレポート[6]と題する検討会報告書を公表している．このレポートでは「位置情報の加工（いわゆる匿名化）」の検討を主要 4 課題の 1 つとして取り上げ報告を行っている．この報告書の特徴的な点は，加工（匿名化）のターゲットをパブリックデータと制限付き提供データの 2 つに明確に区別して論じている点である．パブリックデータとは提供先も提供先における制約も限定せずに〈公開〉できるデータであり，そのデータをプライバシーリスクなく作成する方法を「十分な匿名化」と呼んでいる．十分な匿名化の例としては「すべての属性に対して，同じ位置情報（移動の軌跡を含む）が複数ある状況を作り出す」としている．ただしどの程度の「複数」であればよいかなどの水準はデータセットの性質やその利活用の態様に応じて異なるとしている．一方，制限

付きデータは「十分な匿名化の程度まで加工されていなくても，個人が特定される可能性を一定程度低減した位置情報」とした上で，個人特定性を低減する方法を細かに列挙している．

移動履歴のすがすがしい活用に向けて

個人の移動履歴の保護と利活用に関して，移動履歴の性質を類型化し，プライバシー上のリスクを考察した上で，リスクを軽減するための移動履歴の加工方法を列挙した．

移動履歴を活用することは，プライバシー上のリスクの残る情報，すなわち識別非特定を活用することになる．これら情報の活用はその情報が個人情報である・ないの２元論に依るのではなく，使う上でのリスクを明らかにした上で，必要最小限の情報だけを使うことでリスクを最小にする規律を提案した．

この考えに基づいて，昨年話題になった鉄道の乗降履歴提供の問題を技術的観点から再考してみよう．提供された履歴データは「識別番号，生年月，性別，乗降駅名，利用日時，鉄道利用額」から構成されていた．このデータのリスクは個人特定１は起きにくく（あえて言えば乗降客数が極端に少ない駅を利用する場合に起き得るか），個人特定２の発生の可能性は未知と評価すべきで，せいぜい受領者の知識に依存した個人特定３が起きる程度ではないかと考えられる．不利益を増大させる秘密情報は履歴に通常行かない〈秘密にしておきたい駅〉が含まれる場合であろう．これらのリスクをどうとらえるかであるが，リスクさらに下げるためには，乗降客数の少ない駅のレコードの削除や，秘密情報に相当し得る情報の削除（たとえば，通常のパターンでは想定できない乗降駅か）などが考えられるだろう．その上で，個人特定３は発生頻度はともかく発生の可能性の否定は困難である（履歴の提供会社は，提供先に個人特定および，個人特定が可能な使い方はさせないとしている）．これを残存リスクとして明らかにしておけば，実際の不利益が見えてくる．残ったリスクが受容できない人にはオプトアウトの手段を提供する．

ここまで述べてきたように，移動履歴をすがすがしく活用するために技術的にできることは，たとえば自宅の判明を防ぐ加工方法や，移動履歴中の秘密情報を見つける方法など，その分かりやすい説明の提供と社会受容の獲得も含めて数多くある．また，リスクのうち実態が未知のものもあり，特にパターン性のある履歴の集積の問題は継続した研究が必要だろう．本稿が移動履歴活用のベストプラクティスの体系化の一助になることを願う．

参考文献

1) 個人情報の保護に関する法律（平成十五年五月三十日法律第五十七号），http://law.e-gov.go.jp/htmldata/H15/H15HO057.html
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) Sweeney, L. : Achieving k-Anonymity Privacy Protection Using Generalization and Suppression. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10(5) : pp.571-588 (2002).
5) Beresford, A. R. and Stajano, F. : Location Privacy in Pervasive Computing, in IEEE Pervasive Computing Magazine, IEEE. pp.46-55 (2003).
6) 総務省 緊急時等における位置情報の取り扱いに関する検討会報告書：位置情報プライバシーレポート，http://www.soumu.go.jp/main_content/000293966.pdf

(2014 年 9 月 9 日受付)

■**高橋 克巳（正会員）** takahashi.katsumi@lab.ntt.co.jp
東京工業大学理学部数学科卒業．東京大学情報理工学系研究科博士課程修了．博士（情報理工学）．NTT 研究所にて情報検索，データマイニング，情報セキュリティ，暗号の研究開発に従事．現在 NTT セキュアプラットフォーム研究所主席研究員．