電気通信事業における
「十分な匿名化」に関するガイドライン

一般社団法人　電気通信事業者協会
一般社団法人　テレコムサービス協会
一般社団法人　日本インターネットプロバイダー協会
一般社団法人　日本ケーブルテレビ連盟

［認定個人情報保護団体］
一般財団法人　日本データ通信協会

平成 29 年 10 月 10 日

目次

はじめに

通信の秘密に該当する位置情報については、総務省の「位置情報プライバシーレポート」（平成 26 年 7 月発表）において、「十分な匿名化」をした上で一定の要件を満たす場合には、契約約款等に基づく事前の包括同意に基づいて利用・第三者提供することができるとされており、これを受けて総務省が平成 27 年度、平成 28 年度に実施した「位置情報に関するプライバシーの適切な保護と社会的活用の両立に向けた調査研究」※1 において、有識者等によって「十分な匿名化」に関するルールに盛り込まれるべき内容がまとめられたところである。

※1 両調査研究では、一般社団法人 電気通信事業者協会に加盟する電気通信事業者がユースケースの設定・実施に関してオブザーバ参加を行った。

平成 29 年 5 月の改正個人情報保護法の全面施行に併せて、一般財団法人 日本データ通信協会が個人情報保護法に基づく認定個人情報保護団体として、以下の電気通信事業関連 4 団体の協力の下で改定した「電気通信事業における個人情報保護指針」において、「通信の秘密に該当する位置情報の匿名化については、電気通信事業法の観点から、本指針とは別に自主的なガイドラインが定められる予定」と記載された。

同協会は、平成 17 年４月以来、総務省の認定を受けた認定個人情報保護団体として、上記４団体を団体構成員とした電気通信個人情報保護推進センターを運営しており、電気通信事業分野における個人情報保護の推進活動を実施してきた経緯があること、上記の両調査研究にオブザーバとして参加しておりこれまでの議論の状況等についても適切に把握していることから、上記個人情報保護指針の記載を受けて、電気通信事業法の通信の秘密の観点から、同協会が事務局を務める形で当該事項に関する５団体による業界の自主的なガイドラインである「『十分な匿名化』に関するガイドライン」（以下、「本ガイドライン」という。）の策定を行った。

電気通信事業関連４団体：一般社団法人 電気通信事業者協会、一般社団法人 テレコムサービス協会、一般社団法人 日本インターネットプロバイダー協会、一般社団法人 日本ケーブルテレビ連盟

本ガイドラインは業界において自主的に作成したものではあるが、本ガイドラインの内容は、上記両調査研究の内容に沿ったものであることから、本ガイドラインに基づいていれば、「通信の秘密」を侵害しない状態でのデータの利活用が可能になると解して差し支えないと考えられる。

ただし、本ガイドラインは電気通信事業法に基づく通信の秘密に関わるものであることから、本ガイドラインの運用等に疑義が生じた場合等においては、電気通信事業法に係る解釈権を有する総務省に確認を行うなどして、通信の秘密を侵害することのないようデータの利活用を行っていく必要がある。

1. 趣旨

本ガイドラインは、電気通信事業法における通信の秘密の保護及びプライバシーの保護の趣旨を踏まえ、電気通信事業者が扱う位置情報を、加工して社会的に活用するための方法に関するルールをとりまとめたものである。

加工方法の要求レベルは、電気通信事業者が扱う位置情報の精度やユースケースによって判断されるべきもので、普遍的な基準を定めることは困難である。このため、本ガイドラインでは、ケースバイケースで「十分な匿名化」の要求レベルについて判断することを前提に、最低限遵守すべき基本ルールを定めるとともに、付属資料として具体的なユースケースとその対応方法等をとりまとめている。

また加工方法の他、消費者の安心・安全に資するよう、安全管理措置、消費者への通知及び消費者の同意・選択、プライバシー影響評価（管理運用体制の適切性の評価･検証）に関して、求められる取組みを定めている。

なお、個人情報に該当する位置情報については、個人情報保護法上の規律も参照する必要がある。

2. 用語の定義

2.1. 十分な匿名化

・ 加工方法の組合せにより、その時点での技術水準では再特定化・再識別化が不可能又は極めて困難といえる程度に加工することをいう。電気通信事業者が扱う位置情報について、通信の秘密及びプライバシーの保護と社会的活用とを両立するため、位置情報と個別の通信とを紐付けることができないように加工する方法として考案された仕組み。レコード単位で見て、位置情報（移動履歴を含む）を含む全てのデータ項目について、同じ値を持つレコードが複数あることを作り出し、通信や個人の識別リスクを十分に低減させることを前提に、制度面、技術面、運用面での対処を規定している。

2.2.位置情報

・ 「電気通信事業分野における個人情報保護に関するガイドライン」第 35 条第 1 項に規定する位置情報をいう。携帯電話の基地局に係る位置情報、GPS による位置情報、Wi-Fi アクセスポイントに係る位置情報等がある。

2.3. 付帯情報

・ 電気通信事業者が扱う位置情報に付帯する情報。電気通信事業者が保有する契約者に係る情報、電気通信サービスを利用する際に本人が登録する情報等がある。本書では、そのうち電気通信事業者が位置情報と結合して利用することができるものを「付帯情報」という。

2.4. 非識別化[1]

・ データの匿名化の程度をあらわす概念の一つ。対象となるデータセットにおいて、レコード単位で見て、全てのデータ項目について、同じ値を持つレコードが複数ある状態にすること。個別の通信や特定の個人を識別されないようにする。非識別化の具体的な手法として、「k-匿名化」がある。

2.5. オプトアウト

・ 本人の明示的な同意を事前に取得せずに、本人の情報を利用し、本人からの求めに応じてその情報の利用を停止する方式。ただし、オプトアウトを採用する場合は、情報の利用目的を事前に通知・公表するとともに、オプトアウトの実質的な機会を確保することが前提となる。

2.6. プライバシー影響評価

・ ある個人情報の取扱いがプライバシーに対して与える影響を、事前に、識別、分析、評価、診断して、対処する一連の活動をいう。

3. 適用範囲

・ 電気通信事業者が扱う位置情報を匿名化して利用する場面。当該位置情報のうち、通信の秘密に該当するものを第一義に想定するが、通信の秘密に該当しないものにおいても、本ルールを適用することは、プライバシー保護の観点からは有効であり、望ましい。

4. 「十分な匿名化」に係る取扱い

4.1. 「十分な匿名化」による加工

4.1.1. 位置情報と付帯情報との結合

・ 「十分な匿名化」には、位置情報と付帯情報とを結合して作成したデータを用いることができる。ただし、結合することのできる付帯情報は、次の条件のいずれかに該当しなければならない。

  ➢ 性別、年齢、市区町村までの住所。

[1] 本ガイドラインの「はじめに」に記述した「位置情報に関するプライバシーの適切な保護と社会的活用の両立に向けた調査研究」の平成 28 年度報告書にある定義を引用しているため、一般に用いるすべての手法を記すものではない。

- 経時的にデータが積み重ねられることのない情報（性別、年齢、市区町村までの住所を除く）で、以下の①ないし③をすべて満たすもの。
  ① 単体では個別の通信や個人を特定することができないものであって、かつ他の情報と照合してもなお、個別の通信や個人を特定する可能性が一般に想定されないもの
  ② 利用者が入力した情報、サービスの提供により電気通信事業者に提供されることが利用者にとって明らかな情報等、電気通信事業者による利用が利用者の想定の範囲内にあるもの
  ③ 「十分な匿名化」をして利用することを公にしているもの
  現時点で考えられる例としては、利用者が入力した趣味嗜好や言語情報（ただし、十分な対象者数が確保できる場合に限る。）がある。

4.1.2. 入口要件

・ 「十分な匿名化」に用いるデータには、「入口要件」として、以下の条件を満たすものに限る。
  - 加工の対象は、位置情報と付帯情報に限る
  - 位置情報と付帯情報とを連結する符号（現に電気通信事業者において扱う情報を相互に連結する符号に限る。）がある場合は当該符号は削除する（当該符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）

4.1.3. 出口要件

・ 「十分な匿名化」により加工した後のデータは、「出口要件」として、次の条件を満たすことで、当該データと個別の通信や特定の個人とを紐付けることができないようにしなければならない。
  - 全てのデータ項目において、適切な非識別性が確保されていること。
  - 次の１）～９）に掲げる評価要素によって、個別の通信や特定の個人が識別されるリスクを評価し、総合的に判断して、同リスクが十分に低減されていること。なお必ずしも１）～９）の全ての評価要素を満たす加工を求めるものではない。

１）付帯情報

・ 付帯情報によっては、個別の通信や特定の個人を識別する可能性が高まることに配慮して選定・加工することが望ましい。
  （対処の例）
  - 加工時に付帯情報として位置情報と結合して用いることが認められる性別であっても、対象とする集団に男女の大きな偏りのあることが想定される場合は、付帯

情報として用いない又は配慮して加工する。

2）場所の特性

・ 対象とする位置情報に、自宅、通勤・通学地が含まれる場合は、配慮して加工することが望ましい。
・ 対象とする位置情報に、要配慮個人情報に関わる場所が含まれている場合は、配慮して加工することが望ましい。

（対処の例）

- 明らかに自宅、通勤・通学先がわかる場合は、これらを除く。
- 特定の疾患を対象とする病院に滞留していることが明らかなレコードを、加工対象から除外する。

3）集団の規模

・ 特定の学校・職場や稀少な趣味嗜好等を持つ集団を対象とした場合、集団の規模によっては、個別の通信や特定の個人を識別する可能性が高まるため、集団の規模に配慮して加工することが望ましい。

（対処の例）

- 特定の趣味嗜好の集団を取り扱う場合、十分な対象者数が得られることを確認する。

4）取得時期の特性

・ 特定のイベントや事件のあった日、時期と一致する可能性がある場合、他の情報を参照することによって、個別の通信や特定の個人を識別する可能性が高まるため、取得時期の特性に配慮して加工することが望ましい。

（対処の例）

- 大規模集客施設において、特定の宗教のイベントが開催されていることが明らかな場合は、当該期間及び当該施設に該当するレコードを、加工対象から除外する。

5）位置の精度

・ 高い精度の位置情報は、個別の通信や特定の個人を識別する可能性が高いため、適切に精度を低減することが望ましい。人口密度の低いエリアを対象とする場合は、特に配慮することが望ましい。

（対処の例）

- 位置精度数メートルの緯度・経度情報を、適切な大きさのメッシュ単位の位置情報に変換する。

６）移動履歴の期間・範囲

・ 移動履歴の期間は長くなったり、特定の時間帯を対象としたりする場合は、次の a)～c)に係るリスクが高くなるため、これらに配慮して加工することが望ましい。

a) パターン性

- 定期的に通っている場所、滞留している場所が分かることにより、自宅、通勤・通学地などが推測されて、個別の通信や特定個人の識別性が高まる。

b) 場所の特性

- 「２）場所の特性」を参照。

c) 識別性

- 履歴の一意性が高まる。その一意性をもって、直ちに個別の通信や特定の個人を識別することができないとしても、一定の配慮をすることが望ましい。

（対処の例）

➢ a)～c)を踏まえ、自宅や通勤・通学地に係るレコードを除外する、移動履歴の期間を短くして提供する、同一の事業者に提供する場合は、履歴の期間が重ならないように提供する等の配慮をする。

７）時間の精度・間隔

・ 時間の精度が高まったり、データを取得する際の時間間隔が短くなったりすると、個別の通信や特定の個人を識別する可能性が高まる。また、詳細な時刻情報は位置情報とセットになることで、異なるデータセット間における共通の識別子として機能し得る。このため、適切に時間の精度を低減したり、間隔を開けたりすることが望ましい。

（対処の例）

➢ 秒単位で取得された時間の精度を、15 分単位にまるめる。

８）対象者数

・ 加工対象とするデータセットに含まれる対象者数が少ないと、個別の通信や特定の個人を識別する可能性が高まることに配慮して加工することが望ましい。なお対象者数の数え方は、付属資料３を踏まえること。

・ 同一の個人が複数台の携帯端末を所持している場合のあることを想定して、携帯端末の台数よりも対象者数が小さくなる可能性のあることに留意することが望ましい。

（対処の例）

➢ データを対象者数でカウントして、適切な規模の対象者数を確保する。

９）データ提供までの期間

・ データを取得してから、「十分な匿名化」により加工した位置情報として提供するまでの期間が短い場合は、他の情報を参照することによって、個別の通信や特定の個人を識別する可能性が高まることに配慮して加工することが望ましい。

（対処の例）

- 位置情報を取得してから「十分な匿名化」により加工した情報として提供するまでの期間を、三ヶ月以上確保する。

4.2. 安全管理措置

4.2.1. 加工方法に関する情報

・ 「十分な匿名化」により加工する際、①元の個人情報、②元の個人情報から削除した個人を特定する記述等および加工方法に関する情報の漏えいを防止するため、次に掲げる措置と同等の安全管理措置を講じなければならない。

- 「電気通信事業における個人情報の保護に関するガイドライン」における「匿名加工情報の作成等（第 28 条 2 項)」に掲げる加工方法に係る安全管理措置に対応する措置。

4.2.2. 「十分な匿名化」による加工途中の位置情報

・ 「十分な匿名化」による加工作業が完了していない位置情報は、通信の秘密を保護するため、次に掲げる措置と同等の安全管理措置を講じなければならない。

- 「電気通信事業における個人情報の保護に関するガイドライン」における「安全管理措置（第 11 条)」、「従業者及び委託先の監督（第 12 条)」、「個人情報保護管理者（第 13 条)」に対応する措置。
- 元の個人情報および元の個人情報から削除した個人を特定する記述等が加工後の情報と照合されることを防止する措置[2]

4.2.3. 「十分な匿名化」がされた位置情報

・ 「十分な匿名化」により加工した位置情報は、個別の通信と紐付けられる可能性が十分に低減されたものであるため、事業者は、通信の秘密保護の観点からは、当該情報に対して特段の安全管理措置を講じなくてよい。

4.3. 通知及び同意・選択

4.3.1. 通知及び同意の取得

[2] 元の個人情報との照合により、十分な匿名化データの安全性が損なわれることがあるので、元の個人情報を第三者提供等する場合は、過去に提供等した十分な匿名化データの安全性が損なわれないように配慮することが望ましい。

・ 通信の秘密を含む位置情報を利用するためには、事前に、その旨を本人に通知し、有効な同意を取得しなければならず、その同意は原則として個別かつ明確な同意でなければない。ただし、「十分な匿名化」により加工した位置情報について、次のすべての条件を満たせば、事前の包括的同意に基づいて活用をすることができる。
  - オプトアウトが適切に提供されている。
  - 加工及び運用管理体制（安全管理措置等）が適切である。
  - プライバシー影響評価（PIA）が適切に運用されている。
・ 事前の包括的同意を取得する場合は、付属資料１を参考に、本人にわかりやすく伝えなければならない。

4.3.2. 苦情・相談窓口

・ 「十分な匿名化」により加工した位置情報の活用をするためには、苦情・相談窓口を設置し、本人からの苦情や相談へ対応しなければならない。

4.4. オプトアウト

・ 事前の包括的同意で「十分な匿名化」により加工した位置情報を活用する場合、本人に、オプトアウトの手段を提供しなければならない。
・ 本人が、ウェブサイト、電話等により容易にオプトアウトすることができるように努めなければならない。

4.5. プライバシー影響評価（PIA）－管理運用体制の適切性の評価・検証－

・ 「十分な匿名化」により加工した位置情報を活用する場合、プライバシー影響評価（PIA）を実施して、通知及び同意・選択の方法、加工方法、安全管理措置の管理運用に係る一連の取組みにおける適切性を評価・検証し、その評価結果を公表する。
・ PIA を実施し、適切な管理運用体制を確保することにより、通信の秘密及びプライバシーの保護を確実にするよう努めなければならない。
・ PIA を実施する際は、付属資料２を参考に、適切な評価項目を設定するとともに適切に評価結果を公表すること。

5. 本ガイドラインの見直し

・ 本ガイドラインは、制度改正や技術の進展を踏まえ、定期的に見直しを行って、所要の措置を講じなければならない。
・ 見直しに当たっては、総務省が実施した調査研究においてユースケースの設定・実施やオブザーバ参加を行った、電気通信事業者協会に加盟する電気通信事業者の知見を踏まえ、電気通信事業関連４団体を始めとした関係者の考えを十分に尊重して検討を行う。

付属資料

・付属１：通知・同意取得に関する文案
  - Web 等での説明事項（案）
  - 包括同意約款（案）
・付属２：プライバシー影響評価（PIA）
  - 評価項目
  - 評価結果の公表方法
・付属３：移動履歴のカウント方法
・付属４：「十分な匿名化」による加工事例
  - 商用の事例
  - 観光の事例
  - 交通の事例

付属1：通知・同意取得に関する文案

Web 等での説明事項（案）

No	項目	モデル案（実際に適用する際には必要に応じてカスタマイズする）
ア	取得者（位置情報の利用事業者）	＊＊＊＊株式会社（以下、当社）
イ	位置情報の種類 ※基地局情報、GPS 位置情報、Wi-Fi 位置情報等	当社は、お客様が利用する端末の位置情報として、基地局位置情報、GPS 位置情報、Wi-Fi 位置情報を取得します。なお、これらには通信の秘密に該当する位置情報が含まれる場合があります。このサイトでは、これらの位置情報のうち、通信の秘密に該当する位置情報を、〇〇約款第〇条に定める匿名化利用（以下、匿名化利用）する場合についてご説明します。 (1)基地局位置情報 お客様の端末が接続した基地局の緯度・経度等の情報およびその時刻 (2)GPS 位置情報 〇〇〇 (3)Wi-Fi 位置情報 〇〇〇
ウ	位置情報の精度、取得頻度、ID 有効期間	当社は、お客様が利用する端末の位置情報を以下のように取得します。 (1)精度　GPS・Wi-Fi 位置情報/数 m～数十 m、基地局位置情報/数百 m (2)取得頻度　通信・通話ごとまたは〇秒ごと (3)ID の有効期間　〇日間以下
エ	加工の手法	当社は、匿名化利用を行う場合、以下の加工手法を組合せて実施することで、お客様から取得した情報（上記位置情報および下記お客様情報）につき、十分な匿名化を行います。 利用する加工手法： (1) 項目削除 加工対象となる個人情報データベース等に含まれる個人情報の項目を削除するもの。例えば、年齢のデータを全ての個人情報から削除すること。 (2)一般化 加工対象となる情報に含まれる記述等について、上位概念若しくは数値に置き換えること。例えば、「年齢 70 歳」を「高齢者」に置き換えること。 (3)丸め（ラウンディング） 加工対象となるデータベースに含まれる数値に対して、四捨五入等して得られた数値に置き換えることとするもの。 《上記(1)～(3)は例示であり、特に各社にて状況に応じ変更する箇所になります。》

No	項目	モデル案（実際に適用する際には必要に応じてカスタマイズする）
オ	利用目的	当社は、匿名化利用において、位置情報を以下の目的で利用します。 (1)お客さまに有益と認める情報についての、当社による表示・配信 (2)当社による〇〇サービスに関するマーケティング調査および分析 (3)当社〇〇サービスの品質向上や、新商品・新サービスの企画・開発・提供 (4)当社〇〇サービスについての当社によるご利用状況分析 (5)官公庁、公共団体、一般企業等への人口動態分析、マーケティング分析等の各種分析結果の提供 《上記(1)～(5)は例示であり、特に各社にて状況に応じ変更する箇所になります。》
カ	第三者提供の有無及びその提供先	当社は、上記の利用目的で、個人を容易に特定できないよう十分に匿名化した位置情報等を、反社会的勢力でない第三者に提供することがあります。また、そのような提供先に対し、特定の個人を識別する目的で他の情報と照合しないことを契約上義務付けます。さらに、提供先が別の会社等に提供を行う場合は、それ以降の提供先にも同様の義務を課すことを求めます。
キ	保存期間	加工対象情報（加工前・加工中の位置情報）は、正当業務行為の範囲を超える〇ヶ月のみ保存することとします。十分な匿名化後の情報については、特に保存期間の制限を設けません。
ク	位置情報に紐付けて利用される情報	当社は、匿名化利用において、上記の利用目的を達成するために、以下のお客様情報を位置情報へ紐付けて利用します。 (1)住所（市区町村名までの住所情報とします。） (2)年齢 (3)性別 《上記(1)～(3)は例示であり、特に各社にて状況に応じ変更する箇所になります。》
ケ	本人関与の仕組み	お客様から、位置情報の匿名化利用を停止するようお申し出があった場合、そのお申し出以降、そのお客様の位置情報の匿名化利用を停止いたします（「十分な匿名化」により加工をした場合、加工後の情報は除きます）。 位置情報の匿名化利用停止のご連絡先は以下となります。 (1)Web ページから http://www.***.com/*****/**** (2)電話から ・＊＊携帯電話から: 局番なし ＊＊＊（無料） ・一般電話から: ****-**-****（無料） ・受付時間: 9:00～20:00（土・日・祝日も受付）
コ	情報管理体制	通信の秘密に該当する位置情報を匿名化利用する場合、位置情報の匿名化の加工途中の情報ならびに元の個人情報から削除した情報および加工方法に関する情報についての管理運用体制を適正に構築し運用します。また、加工方法および管理運用体制について評価を行い、その結果を別途公表します。

包括同意約款（案）

モデル案（実際に適用する際には必要に応じてカスタマイズする）

【利用する情報】
当社は、通信の秘密に該当する位置情報（通信の場所、日時、端末識別符号に限ります。）を、電気通信役務の提供を目的に取得・利用するほか、お客様情報（市区町村名までの住所情報、年齢、性別に限ります）とともに、次の利用目的のために、十分な匿名化を行ったうえで利用します。（以下、匿名化利用）
匿名化利用の内容は、以下のとおりです。なお、詳細については、「Web 等での説明事項案」をご参照ください。
《上記お客様情報（市区町村名までの住所情報、年齢、性別）は例示であり、特に各社にて状況に応じ変更する箇所になります。》

【匿名化手法】
個人の再特定化・再識別化が極めて困難といえる程度に加工します。
具体的な匿名化手法は「Web 等での説明事項案」に記載します。

【利用目的】
（1）当社サービスの表示・配信
（2）当社による〇〇サービスに関するマーケティング調査および分析
（3）当社〇〇サービスの品質向上や、新商品・新サービスの企画・開発・提供
（4）当社〇〇サービスについての当社によるご利用状況分析
（5）官公庁、公共団体、一般企業等への人口動態分析、マーケティング分析等の各種分析結果の提供
《上記(1)～(5)は例示であり、特に各社にて状況に応じ変更する箇所になります。別途「プライバシーポリシー」等で記載されたものを参照することも可としますが、その場合、「プライバシーポリシー」において、本包括同意約款に基づいて通信の秘密に該当する位置情報を利用する場合の利用目的の項目が存在し、かつお客様に分かりやすい場所に明記されている必要があります。》

【第三者提供】
上記位置情報およびお客様情報、端末識別符号は、特定の個人を容易に識別できないよう十分な匿名化を行ったうえで、上記利用目的の範囲内で官公庁、公共団体、一般企業等の第三者に提供することがあります。

【情報の利用・第三者提供の停止】
お客様は、当社が取得した位置情報、お客様情報、その他端末識別符号の当社における匿名化利用（「十分な匿名化」により加工した場合、加工後の情報は除きます。）について、以下の URL から停止を申出ることができます。 https://...

【個人情報保護方針】
当社の個人情報保護方針は、別途当社の「プライバシーポリシー」に記載いたします。

【約款の変更】
利用目的の変更や取得するデータ項目の変更に伴い、本約款を変更する場合があります。

付属2：プライバシー影響評価（PIA）

1．評価項目

(1) 全般的事項

(ア) 位置情報や付帯情報（以下、「位置情報等」）の取扱いに関して、責任者や担当者が明確になっていること。また、情報漏えい等、インシデント発生時の報告体制が決められていること。

(イ) 位置情報等を対象に含めたプライバシーポリシーを策定していること。

(ウ) 個人情報保護(安全管理措置を含む)に関する規程、マニュアルが作られており、位置情報等が保護の対象になっていること。

(エ) 上記規程、マニュアルの内容が関係者に周知されていること。上記規程、マニュアルの内容が適時見直されていること。

(オ) 位置情報等を格納する場所が特定されていること。

(カ) 位置情報等へのアクセス権限は、必要な要員にのみ付与されること。原則として 1人1IDとし、共用IDは禁止する。また、不正利用を防止するため、以下のように認証管理を強化すること。また、アクセスが不要になった場合は速やかに削除されること(論理的アクセス/物理的アクセス)。

① パスワードの強度

＊一定以上の文字数

＊英数記号混合

② 以前に使用したパスワードは使用禁止

③ パスワードは一定期間毎に変更

(キ) 位置情報等へのアクセスについて、以下の記録要件を遵守すること。

① アクセスした者、正確な日時、接続元コンピュータ名、成功・失敗を示す情報等を記録すること

② 上記の記録へのアクセス・初期化・停止(一時停止含む)を記録すること

③ 上記の記録は不正アクセスから保護すること

(ク) 位置情報等の取扱いが適切に行なわれているかについて適時状況が確認されていること(監査、自己チェック等)。

(2) データの取得

(ア) 位置情報等の取得に先立って、利用者から同意を得ていること。その際、取得するデータの項目や利用目的等、利用者が同意する内容が明確になっていること。

(イ) 利用者が同意した日時を記録し、いつでも提示できるようにすること。

(ウ) 不必要な情報を取得しないこと。

(エ) 利用等停止の申し入れ等、利用者関与の機会が確保されていること。

（オ）利用目的の変更を行う場合は、変更前の利用目的と関連性を有すると合理的に認められる範囲を超えて行ってはならない。

（カ）合併や営業譲渡等により事業の承継があった場合、承継前の利用目的の達成に必要な範囲を超えて承継前に取得した位置情報等を取扱わないこと。

（キ）取得の際に利用者に対して、位置情報等の取扱いについて分かりやすく説明･表示を行っていること。

① 説明･表示の方法

1. 位置情報取得時における同意取得の場面での説明･表示を行うこと

② 説明事項

1. 取得者（位置情報の利用者）
2. 位置情報の種類（基地局情報、GPS 位置情報、Wi-Fi 位置情報等）
3. 精度、取得頻度、追跡期間
4. 加工方法
5. 利用目的
6. 第三者提供の有無その他第三者提供に関する事項
7. 保存期間
8. 付帯情報の種類（位置情報に紐付けて利用される他の利用者情報）
9. 利用者関与の仕組み
10. 情報管理体制　等

(3) 加工前および加工中のデータ等の保管

（ア）加工前・加工中のデータ、加工の際に元の位置情報等から削除した情報および加工の方法に関する情報等（以下、「加工前データ等」）は、所定の場所で安全に管理されること。

（イ）加工前データ等について、機密性を高める以下のような施策を講じること。

【機密性を高める施策】

① アクセスに対するモニタリング

② 保管時の暗号化

③ 秘密分散　等

（ウ） システムの設置場所等、加工前データ等の保管場所において、媒体や機器の持ち込み・持ち出し制限が行なわれていること。

（エ） システムの設置場所等、加工前データ等の保管場所において、カメラ等の監視装置が設置されていること。また一定期間その監視記録が参照できるようになっていること。

（オ） 利用目的に応じた保管期間を定めること。

（カ） 保管期間経過後または利用目的達成後でも加工前データ等を保管する場合は、相

応の理由を定めること。

（キ） 安全管理に関する教育を従業者に対して実施すること。

（ク） 外部からの不正アクセスを防止するための措置(ファイアウォールの設置等)を講ずること。

（ケ） 加工前データ等を扱う端末等と媒体や機器との接続を制限すること。

（コ） 加工前データ等については、加工後のデータと照合することで特定の個人を再特定しないことを担保するような管理策・方法が講じられていること。

（サ） その他加工前データ等の保管において想定されるリスクに対し、必要な対策を講じておくこと。

(4) 十分な匿名化加工

（ア） 加工作業を担当する要員が、業務外で位置情報等を使用、複製等することに対し予防措置を設けること。

（イ） 加工について作業記録を残すこと、また、加工を行うプログラムの作成・実行・変更・削除の記録を残すこと。作業記録を適時に参照し、意図しない加工が行なわれていないか確認すること。作業記録には、アクセスした者、正確な日時、接続元コンピュータ名等を記録すること。作業記録は不正アクセスから保護すること。

（ウ） 加工方法は、所定のものを用いること。

（エ） 加工作業を担当する要員を限定すること（(1)全般的事項(カ)を参照）。

（オ） 付帯情報は、次の条件のいずれかに該当すること。

① 性別、年齢、市区町村までの住所。

② ①以外の情報で、以下の(i)ないし(iii)を満たすもの。

(i)経時的にデータが積み重ねられることのない情報で、単体では個人を特定することができないものであって、他の情報と照合してもなお、個人を特定する可能性が一般に想定されないものであること、(ii) 利用者が入力した情報、サービスの提供により電気通信事業者に提供されることが利用者にとって明らかな情報等、電気通信事業者による利用が利用者の想定の範囲内にあるものであること、(iii)「十分な匿名化」をして利用することを公にしているものであること。

（カ） 加工を行うことのできるデータは、位置情報と付帯情報に限定され、「入口要件」として、さらに位置情報と付帯情報とを連結する符号（現に電気通信事業者において扱う情報を相互に連結する符号に限る。）を削除すること。

（キ） 加工をした後のデータは、「出口要件」として、次の条件を満たすこと。

① 全てのデータ項目において、適切なk－匿名性が確保されていること。

② 次の１）～９）に掲げる評価要素によって、特定の個人が識別されるリスクを定性的に評価し、同リスクが十分に低減されていること。

１）付帯情報

2）場所の特性
3）母集団の特性
4）取得時期の特性
5）位置の精度
6）移動履歴の期間・範囲
7）時間の精度・間隔
8）対象者数
9）データ提供までの期間

（ク）その他データの加工において想定されるリスクに対し、必要な対策を講じておくこと。

(5) 加工後のデータの提供その他の利用

（ア） 加工後のデータの利用は、位置情報等の取得時に同意を取った利用目的に限定して行われること。

（イ） 第三者(委託・再委託も含む)への提供は、位置情報等の取得時に同意を取っている場合に限り行われること

（ウ） 第三者(委託・再委託も含む)への提供にあたって手続きが定められており、決められた目的以外での提供ができないルールになっていること。

（エ） 第三者(委託・再委託も含む)への提供の記録が残されること(日付、目的、責任者名)。

（オ） 提供される加工後のデータの項目や提供方法が、提供に先立って公表されていること(委託・再委託の場合必須ではない)。

（カ） 加工後のデータを第三者(委託・再委託も含む)に提供する場合、利用者から要求があった場合、または利用者のプライバシーが不当に侵害されていると判断される場合は、加工後のデータの提供を停止できるようにしておくこと。

（キ） 加工後のデータを第三者(委託・再委託も含む)に提供する場合、本人を識別するために、加工後のデータを他の情報と照合してはならず、加工前データ等を取得しないことを、契約書等で提供先に義務づけること。

（ク） その他加工後のデータの提供その他の利用において想定されるリスクに対し、必要な対策を講じておくこと。

(6) データの消去

（ア） 加工前および加工中のそれぞれのデータについて、不必要なものは消去すること。加工前データ等も速やかに消去すること。

（イ） 利用目的を終了した加工後のデータを速やかに消去すること。

（ウ） データ消去の際には、ダミーデータを上書きする等、容易にデータの復元ができな

いようにすること。

（エ） サーバやストレージ、外部記憶媒体等を廃棄する際には、データが復元できないように、消磁等の論理的対応か物理的な破壊を行うこと。

（オ） その他データの消去において想定されるリスクに対し、必要な対策を講じておくこと。

2. 評価結果の公表方法

電気通信事業者のホームページ等で、有識者の確認結果を踏まえた PIA 評価結果を公表する。

【推奨版】

評価項目ごとに、評価結果を公表する。PIA を初めて実施する事業者は、利用者への情報提供において透明性を高めるため、上記案を推奨する。

図表 PIA 結果（公表版）①推奨版

PIA　結果（公表版）

項番	リスク対策	関連する基準等	評価結果
1. 全般的事項			
1.1	位置情報や付帯情報の取扱い・・。	電気通信事業における・・・	YYYY　年 MM　月までに、位置情報の取り扱いの見直しサイクルを社内規程等に明記する予定です。 上記以外について、特段齟齬は見られませんでした。
∫	∫	∫	
1.9	位置情報や付帯情報の取り扱いが適切に・・・	電気通信事業における・・・	
2.　データの取得（抽出）			
2.1	データの取得（抽出）に先立って・・		左記リスク対策について、資料閲覧とヒアリングを行った範囲では、特段齟齬は見られませんでした。
∫			
2.11	十分な匿名化を施した場合でも・・		
3.　データの匿名化加工			
6. データの消去			

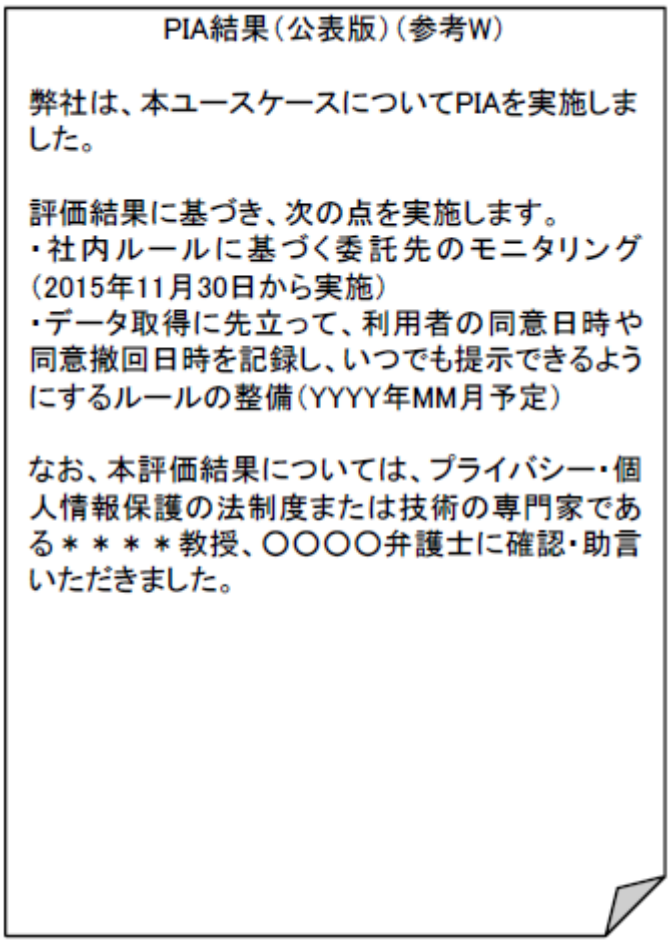
PIA　結果（公表版）

項番	リスク対策	関連する基準等	評価結果
1. 全般的事項			
1.1	位置情報や付帯情報の取扱い・・。	電気通信事業における・・・	YYYY　年 MM　月までに、位置情報の取り扱いの見直しサイクルを社内規程等に明記する予定です。 上記以外について、特段齟齬は見られませんでした。
∫	∫	∫	
1.9	位置情報や付帯情報の取り扱いが適切に・・・	電気通信事業における・・・	
2.　データの取得（抽出）			
2.1	データの取得（抽出）に先立って・・		左記リスク対策について、資料閲覧とヒアリングを行った範囲では、特段齟齬は見られませんでした。
∫			
2.11	十分な匿名化を施した場合でも・・		
3.　データの匿名化加工			
6. データの消去			

【簡略版】

PIA 評価項目・評価観点と齟齬が少ない等、プライバシーへの影響が特に小さいと評価される場合は、簡略な方法で公開することも考えられる。

図表 PIA 結果（公表版）②簡略版



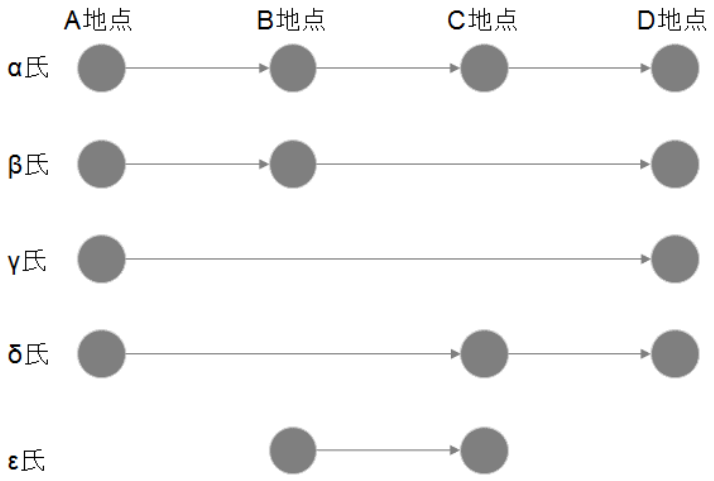
付属3：移動履歴のカウント方法

ある人物の位置情報を複数つなげると、その人の移動履歴が構成される。このとき、移動履歴の数え方を明確にしておかなければ、分析結果を利用する側にとって混乱が生じたり、個別の通信や特定個人の識別リスクが高まったりするおそれがある。このため、ここでは、移動履歴のカウント方法とその適用上の留意事項について整理する。

■移動履歴のカウント方法

移動履歴のカウント方法は、「図1　移動履歴のカウントに係るサンプルモデル」を用いて、「ホップ」と「トリップ」という用語を定義して説明する。本モデルにおいて、●を通過地点（あるいは滞留地点）、時間軸を左から右に経過するものとし、同一時間軸上の地点は時刻が同一もしくは同一とみなすものとする。

図 1　移動履歴のカウントに係るサンプルモデル



ホップ

移動履歴の最小単位。2 地点間の移動を1ホップ、3 地点間の移動を 2 ホップと数える。1 地点に滞留しているだけの場合は 0 ホップとなる。

図 1 のモデルで考えると、α氏は、A 地点から D 地点までの移動にあたって、A→B、B→C、C→D の 3 ホップをしていると数える。一方、β氏は、A 地点から D 地点まで移動にあたって、A→B、B→D の 2 ホップをしていると数える。

トリップ

移動履歴のカウント単位。連続する複数のホップをつなげた”一連のホップ”を分析対象とする場合は、これを1トリップとしてカウントする。1 ホップのみであっても、これを移動履歴とし

て分析対象とする場合は、1トリップとしてカウントする。

図 1 のモデルで考えると、α氏において A→B、B→C、C→D の一連のホップを分析対象とする場合は、A→B→C→D という一つのトリップとしてカウントする。このとき、図 1 では、A→B→C→D のトリップに該当するのは、α氏のみである。

また α氏において、A→B、B→C、C→D のホップそれぞれを分析対象とする場合は、各ホップを独立のトリップとしてカウントする。このとき、図 1 では、A→B のトリップに該当するのは α氏と β氏の 2 名、B→C のトリップに該当するのは α氏と ε氏の 2 名、C→D のトリップに該当するのは α氏と δ氏の 2 名となる。

■移動履歴をカウントする際の留意事項

次の１～3に留意して、移動履歴をカウントすることが有効である。

1. 対象とするトリップの分け方を明確にする。

移動履歴として、どのホップまたは一連のホップをトリップの対象とするのかを特定する。なお、同一データセットに異なるトリップの分け方を適用して異なる匿名化データを作成することには注意が必要である。たとえば、同一のデータセットから作成した 2 種類の匿名化データにおいて、一方の匿名化データで A→B→C が 5 件、もう一方の匿名化データで B→C→D が 6 件あった場合、A→B→C→D と移動した履歴が 1 件であることがわかってしまう場合があるからである。

2. データセットにおいて、同時に、ホップが重なり合う異なるトリップを集計しない。

図 1 のモデルで考えると、A→B→C→D のトリップを集計する場合は、同時に、B→C の集計を行ってはならない。同一人物の移動を 2 重にカウントすることになるからである。

3. リピータ（同一人物の同一トリップ）へ配慮する。

同一人物が同一のトリップを繰り返す場合がある。通勤、通学、通院のような日常的な移動に加え、観光やレジャーなどの不定期の移動も、同一人物による同一トリップに該当する可能性がある。

リピータのトリップを分析対象とする場合は、個人単位でトリップを集約するなどの配慮が必要である。

一方、観光地への入込客を延べ人数で集計したい場合は、個人単位で集約して集計することはしないが、個人の識別性への配慮は必要である。たとえば、対象とするトリップが 100 件あったとしても、すべて同一人物によるものである場合は、識別リスクが高まるため、個人単位で集計して非識別性を評価する必要がある。

付属4:「十分な匿名化」による加工事例

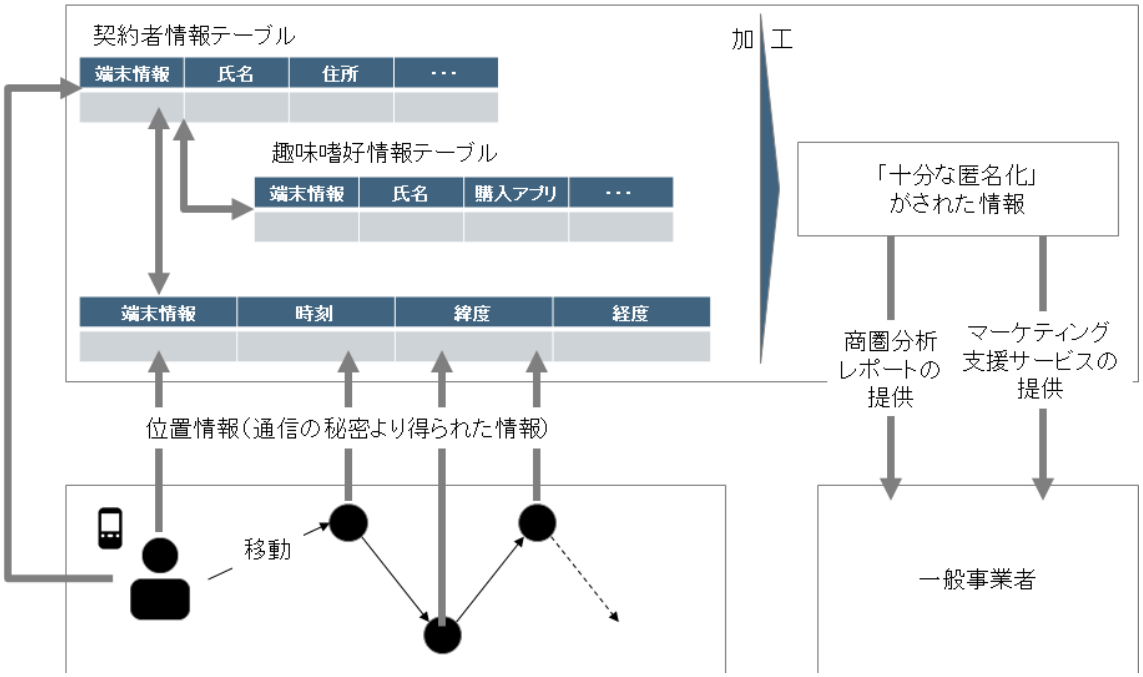
1. 商用の事例 [3]

1)ユースケース

本ユースケースは、電気通信事業者が保有する通信の秘密に該当する位置情報や契約者情報等を、「十分な匿名化」の枠組みを活用して、一般事業者等へ提供するものである。

電気通信事業者においては、店舗の商圏の分析 [4]や、マーケティング支援サービス等の販売促進活動に活用することが想定される。

図表 1-1 電気通信事業者が保有する位置情報を利用するユースケースのイメージ



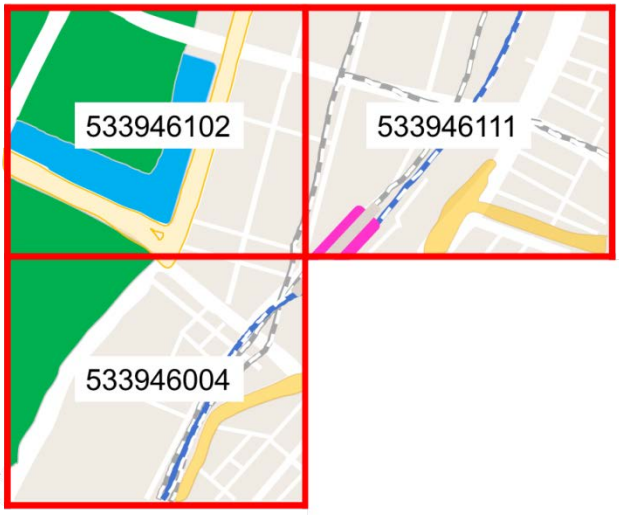
本ユースケースで取扱う位置情報は、都心で不特定多数の人が来訪する一般的なオフィス・商業エリアを対象とし、スマートフォン等の携帯端末の基地局との通信で得られる位置情報を、秘匿加工の前処理段階で、1/2 メッシュコード(500m 四方のメッシュコード)に変換して用いる。

---

[3] 本事例の作成に用いたデータはすべて、加工方法の検討用に作成したダミーデータを用いている。

[4] 例えば、新店舗の立地条件を考える際に、ターゲットとしたい顧客層の移動状況を分析することが考えられる。

図表 1-2 対象エリアにおけるメッシュのイメージ（数値はメッシュコードを表す）



付帯情報については、端末契約時の契約者情報、及び電気通信事業者が提供するアプリ購入時に、契約者から同意を得て取得する趣味嗜好情報から構成される。

全てのテーブルは、端末識別符号によって紐付けが可能である。

図表 1-3 位置情報に関するデータのレイアウトイメージ

契約者情報

端末識別符号	氏名	性別	生年月日	住所
008542314-5	田中　一郎	男	1972 年 4 月 4 日	東京都千代田区丸の内 6-5-3
088539881-2	佐藤　幸子	女	1993 年 12 月 9 日	東京都西東京市保谷町 2-8-18
063381312-1	鈴木　博	男	1938 年 8 月 23 日	神奈川県横浜市旭区二俣川 236

趣味嗜好情報

端末識別符号	趣味嗜好
008542314-5	オペラ観劇
028809315-1	野球観戦
088539881-2	マジックショー

位置情報

端末識別符号	日時	メッシュコード
008542314-5	20161128132415	533946004
008542314-5	20161128150212	553946004
028809315-1	20161130020249	533946111

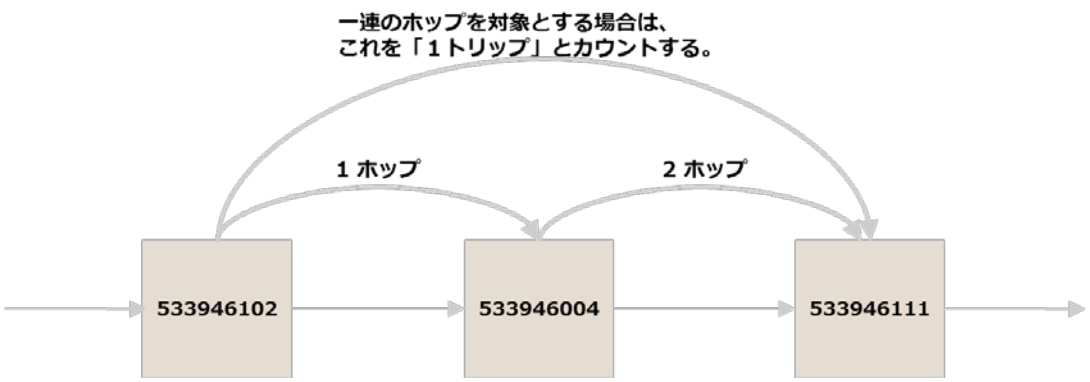
＜移動履歴のカウント方法＞

本ユースケースでは、利用者の移動履歴から予め定義した滞留点を抽出し、二つの滞留点間の移動を 1 ホップ、三つの滞留点間の移動を 2 ホップとする。一つの滞留点のみの位置情報の場合は、0ホップとする。同一メッシュで 15 分以上連続した位置情報がある場合は、利用者が、同メッシュ内のエリアに滞留しているものとみなし、当該メッシュを滞留点とする。

連続する複数のホップをつなげた”一連のホップ”を分析対象とする場合は、これを1つの移動履歴（トリップ）としてカウントする。なお 2 重カウントを避けるため、トリップを構成するホップを、同時には移動履歴の単位としてカウントしない。

また、個人単位でトリップを集約して、リピータの移動も把握できるようにする。

図表 1-4 移動履歴のカウント方法



2）考慮すべき事項とリスクに対応した具体的な加工方法の検討

＜位置情報と付帯情報との結合＞

付帯情報の条件を踏まえ、契約者情報、趣味嗜好情報を次の通りに加工した上で、端末識別符号をキーにて、位置情報と結合する。

- 氏名は、削除する。
- 性別は、加工せず、そのまま用いる。
- 生年月日は、20 歳未満、20 代、30 代、40 代、50 代、60 代、70 歳以上の7つの年代に置き換える。（丸め）
- 趣味嗜好は、一般的なカテゴリとする。マイナーなカテゴリは、他のカテゴリと統合して、一般化する。

＜入口要件＞

端末識別符号が、位置情報と付帯情報とを連結する符号に該当する。位置情報と付帯情報とを結合した後、これを削除する、又はハッシュ化等により一方向に仮 ID 化をする。

＜出口要件＞

全てのデータ項目において適切な非識別性を確保し、あわせて、9つの評価要素によって、個別の通信や特定の個人が識別されるリスクを評価する。

本ユースケースにおける1）～9）の評価指標に基づいた処理方法および、1）～9）を踏まえた総合評価に基づく処理方法を示す。

1）付帯情報

- 付帯情報によっては、個別の通信や特定の個人を識別する可能性が高まることに配慮して選定・加工することが望ましい。
- 本ユースケースでは、配慮すべき対象として、趣味嗜好情報が該当する。例えば、この情報に「マジックショー」のような出現頻度の低いカテゴリがある場合、それらは「観劇」のカテゴリに統合して、一般化する。

2）場所の特性

- 対象とする位置情報に、自宅、通勤・通学地が含まれる場合は、配慮して加工することが望ましい。また、対象とする位置情報に、要配慮個人情報に関わる場所が含まれている場合は、配慮して加工することが望ましい。
- 本ユースケースでは、位置情報の精度を 500 メートル四方のメッシュに変換していることから、自宅、通勤・通学先が特定される可能性は低いが、万全を期す場合、契約者情報を用いて、対象とするエリアに自宅のある個人のレコードを削除する。要配慮個人情報に関わる場所については、都心で不特定多数の人が来訪する一般的なオフィス・商業エリアであることから、特に配慮はしない。

3）集団の規模

- 特定の学校・職場や稀少な趣味嗜好等を持つ集団を対象とした場合、集団の規模によっては、個別の通信や特定の個人を識別する可能性が高まるため、集団の規模に配慮して加工することが望ましい。
- 本ユースケースでは、個別の通信や特定の個人を識別する可能性のある集団を対象としていないため、特に配慮しない。

4）取得時期の特性

- 特定のイベントや事件のあった日、時期と一致する可能性がある場合、他の情報を参照することによって、個別の通信や特定の個人を識別する可能性が高まるため、取得時期の特性に配慮して加工することが望ましい。

- 本ユースケースでは、対象エリアにて、配慮が必要な特定のイベントや事件等が期間内になかったなかったとみなし、特に配慮しない。

5）位置の精度

- 高い精度の位置情報は、個別の通信や特定の個人を識別する可能性が高いため、適切に精度を低減することが望ましい。人口密度の低いエリアを対象とする場合は、特に配慮することが望ましい。
- 本ユースケースでは、位置情報を 500m 四方のメッシュとしていること、都心で不特定多数の人が来訪する一般的なオフィス・商業エリアであることから、特に配慮はしない。

6）移動履歴の期間・範囲

- 移動履歴の期間は長くなったり、特定の時間帯を対象としたりする場合は、次の a)～c)に係るリスクが高くなるため、これらに配慮して加工することが望ましい。
  - a) パターン性
    - 定期的に通っている場所、滞留している場所が分かることにより、自宅、通勤・通学地などが推測されて、個別の通信や特定個人の識別性が高まる。
  - b) 場所の特性
    - 「2）場所の特性」を参照。
  - c) 識別性
    - 履歴の一意性が高まる。その一意性をもって、直ちに個別の通信や特定の個人を識別することができないとしても、一定の配慮をすることが望ましい。
- 本ユースケースでは、位置情報を 500m 四方のメッシュとしていること、都心で不特定多数の人が来訪する一般的なオフィス・商業エリアであることから、更なる加工はしない。ただし期間を長くすることで、差異の大きな個人が識別される場合は、トップコーディングを行う。また同一の事業者に提供する場合は、履歴の期間が重ならないように提供する等の配慮をし、各期間の履歴が結びつかないようにする。

7）時間の精度・間隔

- 時間の精度が高まったり、データを取得する際の時間間隔が短くなったり、個別の通信や特定の個人を識別する可能性が高まる。また、詳細な時刻情報は位置情報とセットになることで、異なるデータセット間における共通の識別子として機能し得る。このため、適切に時間の精度を低減したり、間隔を開けたりすることが望ましい。
- 本ユースケースでは、秒単位で取得された時間の精度を、15 分単位に丸める。

8）対象者数

- 加工対象とするデータセットに含まれる対象者数が少ないと、個別の通信や特定の個人

を識別する可能性が高まることに配慮して加工することが望ましい。また、同一の個人が複数台の携帯端末を所持している場合のあることを想定して、携帯端末の台数よりも対象者数が小さくなる可能性のあることに留意することが望ましい。

- 本ユースケースでは、対象者数でカウントして、一定規模の対象者数が確保されることを確認する。

9）データ提供までの期間

- データを取得してから、「十分な匿名化」により加工した情報として提供するまでの期間が短い場合は、他の情報を参照することによって、個別の通信や特定の個人を識別する可能性が高まることに配慮して加工することが望ましい。
- 本ユースケースでは、位置情報を 500m 四方のメッシュとしていること、都心で不特定多数の人が来訪する一般的なオフィス・商業エリアであることから、特に配慮はしない。

＜加工後のデータのイメージ＞

上記の考え方に基づいて加工されたデータは、図表 1-5 のようになる。

図表 1-5 商用のユースケースにおける加工後のデータのイメージ

時期	年代	性別	住所	趣味嗜好	移動履歴	人数
2016 年 10 月 12 日 13 時～15 時	40 代	女性	埼玉県 さいたま市	観劇	5339460004 → 553946004	15 人
	60 代	女性	東京都 練馬区	観劇	5339460004 → 553946004	35 人
	50 代	男性	群馬県	スポーツ観戦	5339460004 → 553946004	13 人
	60 代	男性	東京都 練馬区	観劇	5339460004 → 533946111	8 人
	40 代	女性	千葉県 千葉市	観劇	5339460004	75 人
…	…	…	…	…	…	…

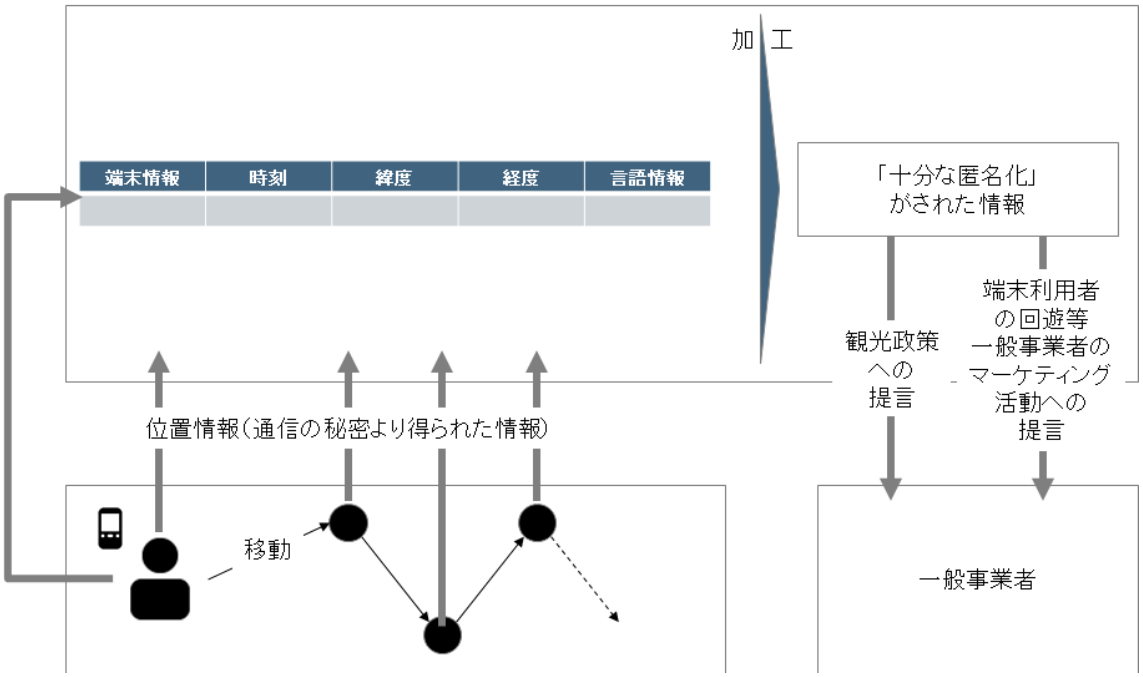
2. 観光の事例 [5]

1）ユースケース

本ユースケースは、通信事業者が保有する通信の秘密に該当する Wi-Fi 位置情報（端末利用者がアクセスポイントから外部と通信を行うことで把握される位置情報）やその他の情報を、「十分な匿名化」の枠組みを活用して、一般事業者等へ提供するものである。

電気通信事業者においては、利用者（海外からの観光客等も含む）の動態や利用ルート等の把握をし、それを観光政策や立地戦略に資するサービス [6]として、第三者に提供することが想定される。

図表 2-1 通信事業者が保有する位置情報を利用するユースケースのイメージ



本ユースケースで取扱う位置情報は、外国人観光客がよく訪れる観光地を対象とし、スマートフォン等の携帯端末による、鉄道の駅や文化施設、観光スポット等に設置されたアクセスポイントとの通信で得られるものを対象とする。複数のアクセスポイントが一つの駅や施設等に設置されている場合は、秘匿加工の前処理段階で、駅や施設等の単位に集約する処理を行う。

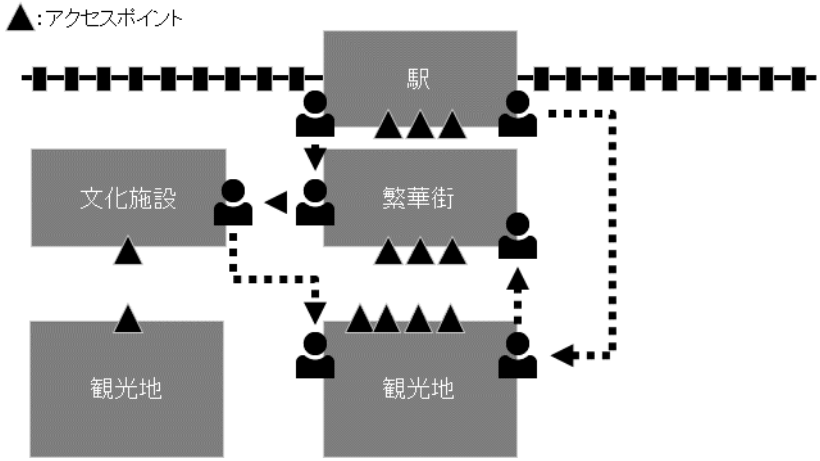
---

[5] 本事例の作成に用いたデータはすべて、加工方法の検討用に作成したダミーデータを用いている。

[6] 例えば、観光客が回遊するルートとそうではないルートの可視化、特定の利用者が主回遊するルートの可視化を通して、観光政策の検討や観光客取り込みに向けたマーケティング戦略の検討に資する提言をサービスとして実施することが考えられる。

付帯情報については、アクセスポイント利用時に選択する言語情報、アクセスポイントの具体的な地名・位置を紐付ける情報から構成される。テーブルは、MAC アドレスおよびアクセスポイントによって紐付けが可能である。

図表 2-2　観光地におけるユーザーの移動イメージ



図表 2-3 位置情報に関するデータのレイアウトイメージ

利用者情報

MAC アドレス	言語
19-88-76-55-18-99	英語
26-99-88-25-55-66	中国語（簡体字）
18-66-70-09-81-33	日本語

※言語情報は、利用者がアクセスポイント接続時に選んだ言語情報を使用することを想定

位置情報

MAC アドレス	取得時刻	アクセスポイント番号
19-88-76-55-18-99	20170223145731	XXX-XXXX-XX1
19-88-76-55-18-99	20170223192651	XXX-XXXX-XX5
26-99-88-25-55-66	20170228124539	XXX-XXXX-YZ3

アクセスポイント位置情報変換テーブル

アクセスポイント番号	地点名
XXX-XXXX-XX1	東京都　東京駅
XXX-XXXX-XX5	東京都　東京駅
XXX-XXXX-YZ3	東京都　東京駅丸の内ビル

※アクセスポイントは、特定の施設等に立地されることが多いため、位置情報もそれに紐付けて整理する
※アクセスポイントは、1 つの施設に複数存在することが多いが、本ユースケースでは、それらは 1 つの施設に紐付けて整理する

＜移動履歴のカウント方法＞

本ユースケースでは、利用者の移動履歴を、連続する複数のホップをつなげた一連のホップとしてカウントする。2 重カウントを避けるため、トリップを構成するホップを、同時には移動履歴の単位としてカウントしない。

観光地への入り込み客数を延べ人数で把握するため、個人単位で集約して集計することはしない。ただし、個人の識別性への配慮のため、加工時に非識別性の評価は行う。

2）考慮すべき事項とリスクに対応した具体的な加工方法の検討

＜位置情報と付帯情報との結合＞

付帯情報の条件を踏まえ、利用者情報を次の通りに加工した上で、端末識別符号をキーにして、位置情報と結合する。

- 言語情報は、一般的なカテゴリとする。マイナーなカテゴリは、他のカテゴリと統合して、一般化する。

＜入口要件＞

MAC アドレスが、位置情報と付帯情報とを連結する符号に該当する。位置情報と付帯情報とを結合した後、これを削除する、又はハッシュ化等により一方向に仮 ID 化をする。

＜出口要件＞

全てのデータ項目において適切な非識別性を確保し、あわせて、9つの評価要素によって、個別の通信や特定の個人が識別されるリスクを評価する。

本ユースケースにおける1）～9）の評価指標に基づいた処理および、1）～9）を踏まえた総合評価に基づく処理を示す。

1）付帯情報

- 付帯情報によっては、個別の通信や特定の個人を識別する可能性が高まることに配慮して選定・加工することが望ましい。
- 本ユースケースでは、配慮すべき対象として、言語情報が該当する。相対的に少ないと

想定される言語情報については、「その他の言語」のカテゴリに統合して、一般化する。なお本ユースケースでは、このような出現頻度の低い言語は想定しておらず、よって、特段処理は実施しない。

2）場所の特性

- 対象とする位置情報に、自宅、通勤・通学地が含まれる場合は、配慮して加工することが望ましい。また、対象とする位置情報に、要配慮個人情報に関わる場所が含まれている場合は、配慮して加工することが望ましい。
- 本ユースケースでは、場所を地名に置き換える処理をして取り扱っていることから、本項目に係るさらなる処理は実施しない。

3）集団の規模

- 特定の学校・職場や稀少な趣味嗜好等を持つ集団を対象とした場合、集団の規模によっては、個別の通信や特定の個人を識別する可能性が高まるため、集団の規模に配慮して加工することが望ましい。
- 本ユースケースでは、個別の通信や特定の個人を識別する可能性のある集団を対象としていないため、特に配慮しない。

4）取得時期の特性

- 特定のイベントや事件のあった日、時期と一致する可能性がある場合、他の情報を参照することによって、個別の通信や特定の個人を識別する可能性が高まるため、取得時期の特性に配慮して加工することが望ましい。
- 本ユースケースでは、対象エリアにて、配慮が必要な特定のイベントや事件等が期間内になかったとみなし、特に配慮しない。

5）位置の精度

- 高い精度の位置情報は、個別の通信や特定の個人を識別する可能性が高いため、適切に精度を低減することが望ましい。人口密度の低いエリアを対象とする場合は、特に配慮することが望ましい。
- 本ユースケースでは、アクセスポイントを地名に置き換えること、外国人観光客がよく訪れる観光地を対象としていることから、特に配慮はしない。

6）移動履歴の期間・範囲

- 移動履歴の期間は長くなったり、特定の時間帯を対象としたりする場合は、次の a)～c)に係るリスクが高くなるため、これらに配慮して加工することが望ましい。

  a)　パターン性

- 定期的に通っている場所、滞留している場所が分かることにより、自宅、通勤・通学地などが推測されて、個別の通信や特定個人の識別性が高まる。

b） 場所の特性

- 「2）場所の特性」を参照。

c） 識別性

- 履歴の一意性が高まる。その一意性をもって、直ちに個別の通信や特定の個人を識別することができないとしても、一定の配慮をすることが望ましい。

- 本ユースケースでは、アクセスポイントを地名に置き換えること、外国人観光客がよく訪れる観光地を対象としていることから、更なる加工はしない。ただし、期間を長くすることで、差異の大きな個人が識別される場合は、トップコーディングを行う。また同一の事業者に提供する場合は、履歴の期間が重ならないように提供する等の配慮をし、各期間の履歴が結びつかないようにする。

7）時間の精度・間隔

- 時間の精度が高まったり、データを取得する際の時間間隔が短くなったりすると、個別の通信や特定の個人を識別する可能性が高まる。また、詳細な時刻情報は位置情報とセットになることで、異なるデータセット間における共通の識別子として機能し得る。このため、適切に時間の精度を低減したり、間隔を開けたりすることが望ましい。
- 本ユースケースでは、一定期間内における利用者による地点間の移動を把握することを目的とするため、時間の精度・間隔に係るデータ項目は、加工後のデータセットには含まれない。このため、特に配慮はしない。

8）対象者数

- 加工対象とするデータセットに含まれる対象者数が少ないと、個別の通信や特定の個人を識別する可能性が高まることに配慮して加工することが望ましい。また、同一の個人が複数台の携帯端末を所持している場合のあることを想定して、携帯端末の台数よりも対象者数が小さくなる可能性のあることに留意することが望ましい。
- 本ユースケースでは、対象者数でカウントして、一定規模の対象者数が確保されることを確認する。

9）データ提供までの期間

- データを取得してから、「十分な匿名化」により加工した情報として提供するまでの期間が短い場合は、他の情報を参照することによって、個別の通信や特定の個人を識別する可能性が高まることに配慮して加工することが望ましい。
- 本ユースケースでは、アクセスポイントを地名に置き換えること、外国人観光客がよく訪れる観光地を対象としていること、時間の精度・間隔は集計の過程で削除していることか

ら、特に配慮はしない。

＜加工後のデータのイメージ＞

上記の考え方に基づいて加工されたデータは、図表 2-4 のようになる。

図表 2-4 観光のユースケースにおける加工後のデータのイメージ

時期	言語	移動履歴	人数
2016 年 10 月	英語	東京駅→新宿駅→横浜駅→箱根駅	35 人
	英語	有楽町駅→皇居→歌舞伎座→有楽町駅	13 人
	英語	東京駅→浅草駅→雷門→両国国技館→東京駅	10 人
	中国語	東京駅→銀座→舞浜駅→ディズニーランド→・・・	120 人
・・・	・・・	・・・	・・・

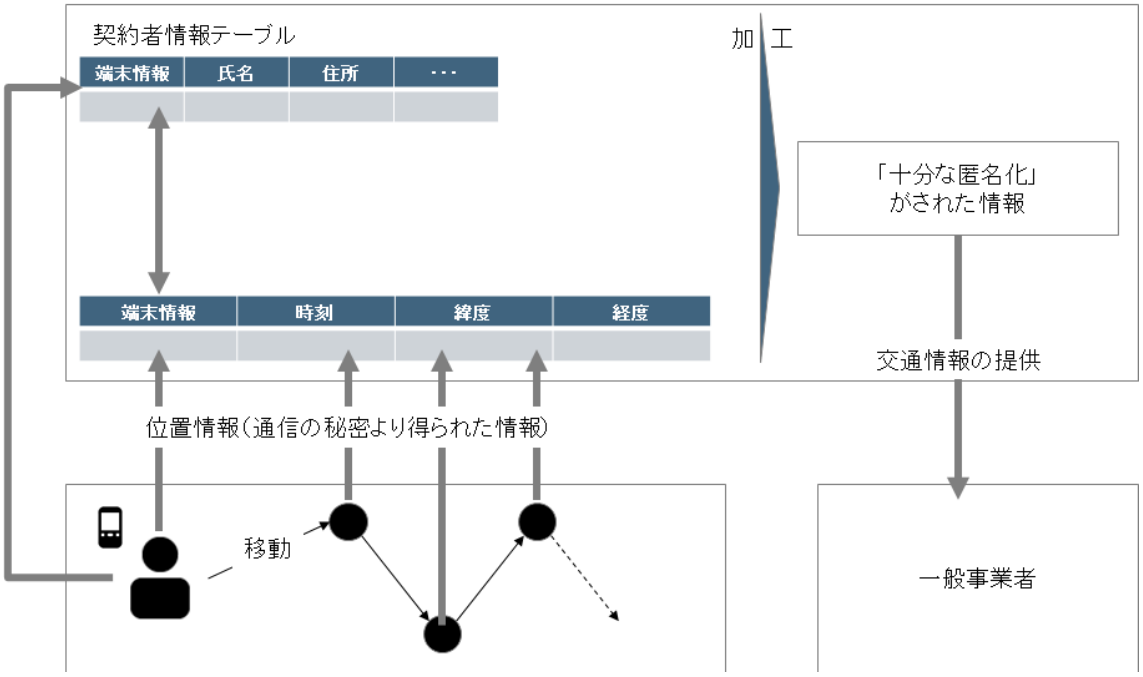
3. 交通の事例 [7]

1）ユースケース

本ユースケースは、電気通信事業者が保有する通信の秘密に関する位置情報（個々の通信の際に把握される基地局の位置情報）や契約者情報等を、「十分な匿名化」の枠組みを活用して、一般事業者へ提供するものである。

電気通信事業者においては、交通渋滞情報の提供や、路線の交通量の逼迫情報を分析したりするサービスに活用することが想定される。

図表 3-1 電気通信事業者が保有する位置情報を利用するユースケースのイメージ



本ユースケースは、出発地点または到着地点を羽田空港あるいは成田空港に設定して、両空港間の移動動態に係る分析データの提供を対象とする。

スマートフォン等携帯端末の基地局との通信で得られる位置情報と、端末契約時の契約者情報から構成される、図表 3-2 のようなデータ構造を前提として検討する。全てのテーブルは、端末識別符号によって紐付けが可能である。

[7] 本事例は、平成 27 年度に実施した調査研究におけるユースケースを参考に作成している。

図表 3-2 位置情報に関するデータのレイアウトイメージ

契約者情報

端末識別符号	氏名	性別	生年月日	住所
008542314-5	田中　一郎	男	1972 年 4 月 4 日	東京都千代田区丸の内 6-5-3
088539881-2	佐藤　幸子	女	1993 年 12 月 9 日	東京都西東京市保谷町 2-8-18
063381312-1	鈴木　博	男	1938 年 8 月 23 日	神奈川県横浜市旭区二俣川 236

位置情報

端末識別符号	時刻	緯度	経度
008542314-5	20161128132415	35.658593	139.745441
008542314-5	20161128150212	35.658593	139.745992
028809315-1	20161130020249	38.688721	140.663542

※時刻は年月日時刻（秒単位）まで収集可能と想定

＜移動履歴のカウント方法＞

本ユースケースでは、利用者の移動履歴を、出発駅、経由地、到着地の3地点間のホップとトリップでカウントする。

交通量を把握するため、個人単位で集約して集計することはしない。ただし、個人の識別性への配慮のため、加工時に非識別性の評価は行う。

2）考慮すべき事項とリスクに対応した具体的な加工方法の検討

＜位置情報と付帯情報との結合＞

付帯情報の条件を踏まえ、契約者情報、趣味嗜好情報を次の通りに加工した上で、端末識別符号をキーにして、位置情報と結合する。

氏名は、削除する。

- 性別は、加工せず、そのまま用いる。
- 生年月日は、20 歳未満、20 代、30 代、40 代、50 代、60 代、70 歳以上の7つの年代に置き換える。（丸め）
- 住所は県と市区町村のレベルまでに限定

＜入口要件＞

端末識別符号が、位置情報と付帯情報とを連結する符号に該当する。位置情報と付帯情報とを結合した後、これを削除する、又はハッシュ化等により一方向に仮 ID 化をする。

＜出口要件＞

全てのデータ項目において適切な非識別性を確保し、あわせて、9つの評価要素によって、個別の通信や特定の個人が識別されるリスクを評価する。

本ユースケースにおける1）～9）の評価指標に基づいた処理方法および、1）～9）を踏まえた総合評価に基づく処理方法を示す。

1）付帯情報

- 付帯情報によっては、個別の通信や個人を特定する可能性が高まることに配慮して選定・加工することが望ましい。
- 本ユースケースでは、特にこれに該当する情報は見受けられないため、本項目に係る処理は実施しない。

2）場所の特性

- 対象とする位置情報に、自宅、通勤・通学地が含まれる場合は、配慮して加工することが望ましい。また、対象とする位置情報に、要配慮個人情報に関わる場所が含まれている場合は、配慮して加工することが望ましい。
- 本ユースケースでは、契約者情報を用いて、対象とするエリアに自宅のある個人のレコードを削除する。要配慮個人情報に関わる場所については、空港、駅および高速道路のジャンクションといった公共性の高い場所を対象としていることから、特に配慮しない。

3）集団の規模

- 特定の学校・職場や稀少な趣味嗜好等を持つ集団を対象とした場合、集団の規模によっては、個別の通信や特定の個人を識別する可能性が高まるため、集団の規模に配慮して加工することが望ましい。
- 本ユースケースでは、個別の通信や特定の個人を識別する可能性のある集団を対象としていないため、特に配慮しない。

4）取得時期の特性

- 特定のイベントや事件のあった日、時期と一致する可能性がある場合、他の情報を参照することによって、個別の通信や特定の個人を識別する可能性が高まるため、取得時期の特性に配慮して加工することが望ましい。
- 本ユースケースでは、対象エリアにて、配慮が必要な特定のイベントや事件等が期間内になかったとみなし、特に配慮しない。

5）位置の精度

- 高い精度の位置情報は、個別の通信や特定の個人を識別する可能性が高いため、適切に精度を低減することが望ましい。人口密度の低いエリアを対象とする場合は、特に配慮することが望ましい。
- 本ユースケースでは、緯度・経度情報を、空港、駅および高速道路のジャンクション等の単位に変換する。

6）移動履歴の期間・範囲

- 移動履歴の期間は長くなったり、特定の時間帯を対象としたりする場合は、次の a)～c)に係るリスクが高くなるため、これらに配慮して加工することが望ましい。
  - a） パターン性
  - ➢ 定期的に通っている場所、滞留している場所が分かることにより、自宅、通勤・通学地などが推測されて、個別の通信や特定個人の識別性が高まる。
  - b） 場所の特性
  - ➢ 「2）場所の特性」を参照。
  - c） 識別性
  - ➢ 履歴の一意性が高まる。その一意性をもって、直ちに個別の通信や特定の個人を識別することができないとしても、一定の配慮をすることが望ましい。
- a)～c)を踏まえ、本ユースケースでは、

  ・自宅や通勤・通学等の生活圏に係るレコードを除外する。

  ・仮 ID の振り方を 1 日単位で変えることで、識別性を低減する。

  する。

  といった処理をする。また同一の事業者に提供する場合は、履歴の期間が重ならないように提供する等の配慮をし、各期間の履歴が結びつかないようにする。

7）時間の精度・間隔

- 時間の精度が高まったり、データを取得する際の時間間隔が短くなったりすると、個別の通信や特定の個人を識別する可能性が高まる。また、詳細な時刻情報は位置情報とセットになることで、異なるデータセット間における共通の識別子として機能し得る。このため、適切に時間の精度を低減したり、間隔を開けたりすることが望ましい。
- 本ユースケースでは、一定期間内における利用者による地点間の移動を把握することを目的とするため、時間の精度・間隔に係るデータ項目は、加工後のデータセットには含まれない。このため、特に配慮はしない。

8）対象者数

- 加工対象とするデータセットに含まれる対象者数が少ないと、個別の通信や特定の個人

を識別する可能性が高まることに配慮して加工することが望ましい。また、同一の個人が複数台の携帯端末を所持している場合のあることを想定して、携帯端末の台数よりも対象者数が小さくなる可能性のあることに留意することが望ましい。

- 本ユースケースでは、本ユースケースでは、対象者数でカウントして、一定規模の対象者数が確保されることを確認する。

9）データ提供までの期間

- データを取得してから、「十分な匿名化」により加工した情報として提供するまでの期間が短い場合は、他の情報を参照することによって、個別の通信や特定の個人を識別する可能性が高まることに配慮して加工することが望ましい。
- 本ユースケースでは、場所が、空港、駅および高速道路のジャンクションといった公共性の高い場所を対象としていること、時間の精度・間隔は集計の過程で削除していることから、特に配慮はしない。

＜加工後のデータのイメージ＞

上記の考え方に基づいて加工されたデータは、図表 3-4 のようになる。

図表 3-4　交通のユースケースにおける加工後のデータのイメージ

時期	年代	性別	出発駅	到着地	経由地	人数
2016 年 10 月平日	40 代	女性	新宿駅	羽田空港	浜松町駅	50 人
	60 代	女性	新宿駅	羽田空港	大井 JCT	75 人
	40 代	男性	浜松町駅	羽田空港	－	25 人
	60 代	男性	高田馬場駅	成田空港	大井 JCT	8 人
2016 年 10 月 休日祝日	40 代	女性	新宿駅	羽田空港	大井 JCT	100 人
	40 代	女性	池袋駅	羽田空港	浜松町駅	100 人
	20 代	女性	新宿駅	成田空港	大井 JCT	40 人
	50 代	男性	浜松町駅	羽田空港	－	14 人
…	…	…	…	…	…	…