

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

結果概要

2016年5月12日

事務局

1 実施概要

1. 背景・目的等

平成26年に発表された「位置情報プライバシーレポート」では、通信の秘密に該当する位置情報の取扱いについて、「十分な匿名化」の水準や加工の方法・管理運用体制の適切性の評価・検証の在り方を引き続き検討していく必要があり、実証・検証を進めていくべきと示されている。

そこで、本調査研究にて、通信の秘密に該当する位置情報について、その利活用を促進する観点から、契約約款等に基づく事前の包括同意を前提として、第三者提供を視野に、その適切な取扱いに関する課題検討を行った。

2. 実施項目

- ①位置情報の利活用に係るユースケースの設定
- ②ユースケース毎に「十分な匿名化」を行なうための加工の手法の検証
- ③適切な加工の手法・管理運用体制の検証
- ④プライバシー影響評価の評価手順の検討・実施
- ⑤将来の位置情報の収集における利用者の同意取得方法の検討
- ⑥一般的な電気通信の仕組みと位置情報の収集に関する説明方法の検討

3. 協議会の設置

本調査研究の実施にあたり、通信の秘密に該当する位置情報の適切な取扱いについて、実効性があり、プライバシーの適切な保護と社会的な活用の両立に向けた調査研究を行うため、個人情報保護、十分な匿名化加工技術、情報通信関連政策等を専門とする有識者6名を構成員として、協議会を設置した。

(株)NTTドコモ、KDDI(株)、ソフトバンク(株)、エヌ・ティ・ティ・ブロードバンドプラットフォーム(株)、デロイトトーマツ リスクサービス(株)、総務省、個人情報保護委員会、一般社団法人電気通信事業者協会をオブザーバーとし、事務局は(株)シード・プランニングが担当して、事業期間内に5回開催した。

■協議会構成員

| 所属・役職 | 氏名(50音順・敬称略) |
|--------------------------|--------------|
| 筑波大学 大学院システム情報工学研究科 准教授 | 佐久間 淳 |
| 東京大学 空間情報科学研究センター 教授 | 柴崎 亮介 |
| NTTセキュアプラットフォーム研究所 主席研究員 | 高橋 克巳 |
| 東京工科大学 教養学環 准教授 | 村上 康二郎 |
| 東京大学 先端科学技術研究センター 教授 | 森川 博之 |
| 英知法律事務所 弁護士 | 森 亮二(座長) |

2 ユースケースの概要

- 本調査研究では、電気通信事業者の協力のもと、防災、交通、観光など公的分野での利活用ならびに商用分野での利活用が想定されるユースケースを4件設定。その概要は下表のとおり。
- これら4件のユースケースそれぞれに応じて適切と考えられる匿名化の加工を行い、その加工結果より、個人の再特定化・再識別化のリスクが限定されているかについて検証した。

| | 名称 | 概要 | 担当事業者 | 利用する位置情報 |
|---|-------------------------------|--|--------------------------------|----------------------------------|
| ① | 震災等災害時の避難行動分析(防災) | GPS測位した位置情報を用いて平常時の「流動人口」の集計を行い、そこから災害が発生した場合の被害を算出した後、内閣府公表の被害想定との比較を行う。 | NTTドコモ | GPS位置情報 |
| ② | 都市交通整備への活用を想定した空港利用者の動態分析(交通) | 利用者の契約情報及び位置情報を用いて、首都高速中央環状線(大井JCT～初台IC)の開通前後の羽田・成田空港利用者の動態分析を行う。 | KDDI | 携帯電話基地局位置情報 (通信の秘密に該当するものを含む) |
| ③ | スポーツ観戦時におけるユーザの流動性調査(商用) | 九州地区での野球観戦キャンペーンへの応募者から、顧客情報と一定期間における位置情報を取得し、イベント施設周辺エリア及び商業エリア(博多駅等)に滞在した人の①属性、②施設来場頻度・滞在時間、③施設来場前後の立寄り等の分析を行った。 | ソフトバンク | Wi-Fi位置情報 (通信の秘密に該当するものを含む) |
| ④ | 観光客の滞留時間分析、導線分析(観光) | 交通要所及び観光スポットに設置しているWi-Fiエリアを活用して位置情報を取得し、訪日外国人等の各スポットでの接続時間を把握・分析する。 | NTTブロードバンドブラットフォーム (NTT-BP) | Wi-Fi位置情報 |

2.1 ユースケース①(防災)

①震災等災害時の避難行動分析(防災)

| 利用データ | 標本数 | 加工プロセス | 加工分析結果 |
|--|--|---|--|
| <ul style="list-style-type: none"> ■ GPS位置情報 (ユーザID、時刻、経度/緯度) | <ul style="list-style-type: none"> ■ 約23,000名 | <ul style="list-style-type: none"> ■ 直接識別子削除、仮ID化、ハッシュ化、メッシュ化 ■ エリア単位、属性別で集計 ■ 秘匿処理(少人数データの削除) ■ 拡大推計 | <ul style="list-style-type: none"> ■ 今回の実証実験ではどのパターンでも特定の個人が識別されるリスクを確認できなかったが、k=1の場合を加工後のデータとする際には、特定の個人が識別されるリスクが残る可能性も考えられる。 |



加工後のデータイメージ(1)
避難時の行動特性を加味した被害想定算出分布

加工後のデータイメージ(2)
避難時の行動特性を加味した想定死亡者数

| 期間名称 | 平休日 | 時間帯 | メッシュ | 想定死亡者数 |
|------|-----|-----|------------|--------|
| H27夏 | 平日 | 10 | 5035157932 | 4 |
| H27夏 | 平日 | 10 | 5035158434 | 3 |
| H27冬 | 休日 | 10 | 5035158443 | 1 |
| H27冬 | 休日 | 10 | 5035158444 | 7 |
| H27冬 | 休日 | 10 | 5035158624 | 4 |
| H27夏 | 休日 | 10 | 5035158634 | 1 |
| H27夏 | 休日 | 10 | 5035158732 | 3 |

2.2 ユースケース②(交通)

②都市交通整備への活用を想定した空港利用者の動態分析(交通)

| 利用データ | 標本数 | 加工プロセス | 加工分析結果 |
|---|---|---|---|
| <ul style="list-style-type: none"> ■ 契約情報(ユーザID、性別、年齢)、 ■ 基地局位置情報(ユーザID、接続時刻、緯度/経度) | <ul style="list-style-type: none"> ■ 羽田空港利用者:76,919 ■ 成田空港利用者:8,603 | <ul style="list-style-type: none"> ■ 直接識別子削除、仮ID化、ハッシュ化、 ■ メッシュ化、生活圏の排除 ■ 秘匿処理(少人数データの削除)、拡大推計 | <ul style="list-style-type: none"> ■ 位置情報分析により発着地別の流動実態、利用者の実態、特定の地域間を通過する移動量・所要時間を把握できることを確認した。 ■ データは市区町村単位で集約するため、$k \geq 10$の場合、特定の個人を特定するリスクは十分軽減されていると考えられる。 ■ 羽田空港を対象とした、1市区町村あたりの分析対象件数に制限を求めた場合のカバー率は、$k \geq 2$で全件の9割、$k \geq 10$で全件の6割に留まった。k値を上げるにつれて有用性が損なわれることを確認した。 |

加工後のデータイメージ(1)
発地・滞在地(着地)となる市区町村

市区町村⇒成田空港

| Term1 | カウント | 割合 |
|--------|------|-------|
| 千葉県成田市 | 524 | 22.6% |
| 千葉県山武郡 | 64 | 2.7% |
| 千葉県富里市 | 45 | 1.9% |
| Term2 | カウント | 割合 |
| 千葉県成田市 | 524 | 22.0% |
| 千葉県山武郡 | 71 | 3.0% |
| 千葉県富里市 | 50 | 2.1% |

成田空港⇒市区町村

| Term1 | カウント | 割合 |
|--------|------|-------|
| 千葉県成田市 | 295 | 16.3% |
| 千葉県山武郡 | 58 | 3.2% |
| 千葉県富里市 | 49 | 2.7% |
| Term2 | カウント | 割合 |
| 千葉県成田市 | 292 | 14.4% |
| 千葉県富里市 | 57 | 2.8% |
| 千葉県山武郡 | 57 | 2.8% |

加工後のデータイメージ(2)
中央環状線開通前後の移動状況

新宿⇒羽田_平日

| Term1 | 時間帯 | 通過カウント数 | 平均所要時間 |
|-------|-----|---------|--------|
| 開通前 | 8 | 30 | 0:43 |
| 開通前 | 9 | 40 | 0:53 |
| 開通前 | 10 | 45 | 0:56 |
| 開通後 | 8 | 66 | 0:27 |
| 開通後 | 9 | 82 | 0:29 |
| 開通後 | 10 | 77 | 0:41 |

2.3 ユースケース③(商用)

③スポーツ観戦時におけるユーザの流動性調査(商用)

| 利用データ | 標本数 | 加工プロセス | 加工分析結果 |
|---|---|---|--|
| <ul style="list-style-type: none"> ■ Wi-Fi位置情報:切断ログより得られる位置情報(通信の秘密に該当)を取得 ■ 付帯情報:顧客情報より性別・年齢・住所の3項目を利用 | <ul style="list-style-type: none"> ■ 6,608 | <ul style="list-style-type: none"> ■ 直接識別子除外、仮ID付与 ■ 年齢は10歳刻み/緯度・経度を1/8メッシュへ変換、同一のエリアに10分より長く滞在した位置情報データを滞留点として抽出 ■ 集計データ加工:①来場者属性、②来場頻度・入退場時間、③施設来場前後の立寄エリアへ各々集計 ■ 各集計データに対し、k匿名化処理(k=2, 5, 10)を実施 | <ul style="list-style-type: none"> ■ 左記①～③の分析の結果、付帯情報利用により、来場者の基本属性(性別・年代別・都道府県別)分析が可能となりマーケティング利用等に有用であることが確認できた。 ■ 具体的には、位置情報と付帯情報を利用し、来場回数、イベント開催時間と施設への入退場時間・(滞在時間)との比較や、来場前後の周遊(例:対象施設と博多駅等の商業エリア間の往来)を分析することができた。 ■ K=2、5、10のケースにおいて、加工後データから個人を再特定化することは極めて困難もしくは不可能に近く、匿名性は担保される結果となった。 ■ 十分な匿名化による匿名性は検証されたが、k値によっては属性に偏ったデータ削除がなされ有用性が損なわれた。 |

加工後のデータイメージ(1): 入退場時刻

| 年代 | 性別 | エリア名称 | 入場時刻 | 退場時刻 | 件数 |
|----|----|---------|---------|---------|----|
| 30 | 男性 | ヤフオクドーム | 12時～13時 | 16時～17時 | 2件 |
| 50 | 男性 | ヤフオクドーム | 13時～14時 | 17時～18時 | 2件 |

加工後のデータイメージ(2): 来場回数

| 年代 | 性別 | 来場回数 | 件数 |
|----|----|------|----|
| 50 | 男性 | 1回 | 3件 |
| 50 | 男性 | 2回 | 2件 |

加工後のデータイメージ(3): 移動履歴

| 年代 | 性別 | 移動パターン | 件数 |
|----|----|-----------------|----|
| 50 | 男性 | 天神地区 -> ヤフオクドーム | 2件 |
| 50 | 男性 | ヤフオクドーム-> 天神地区 | 2件 |

2.4 ユースケース④(観光)

④観光客の滞留時間分析、導線分析(観光)

| 利用データ | 標本数 | 加エプロセス | 加工分析結果 |
|--|---|---|--|
| <ul style="list-style-type: none"> Wi-Fi位置情報: 基地局ID、時刻、利用言語 | <ul style="list-style-type: none"> 約60,000 | <ul style="list-style-type: none"> 各端末の帰属基地局、利用言語、基地局位置を突合し、利用言語別の滞留時間、動線分布を算出 | <ul style="list-style-type: none"> 滞留時間、動線とも利用言語別に異なる特徴が表れ、外国人別の観光施策へ活用可。 K=5として、4以下のサンプル数データを削除すると、50%以上の統計データが削除される場合がある。 位置粒度を基地局単位でなくスポット単位として場所特定性を低減し、また、時間粒度を1か月として時間特定性も低減することにより、加工後のデータから個人が識別されるリスクは十分軽減されていると考える。 |

加工後のデータイメージ(1): エリア毎の滞留人数(言語別)

| スポット | 時間帯 | 日本語 | 英語 | 仏語 | 韓国語 | タイ語 | 中国語 |
|---------|--------|-------------------|-----------------|----------------|----------------------|----------------------|----------------------|
| 交通拠点 #A | 6-12時 | 33分45秒 (2,215) | 36分34秒 (488) | 33分45秒 (28) | 29分56秒 (13) | <u>44分4秒</u> (5) | 33分22秒 (211) |
| | 12-18時 | 32分57秒 (2,158) | 34分3秒 (350) | 32分37秒 (22) | <u>19分19秒</u> (6) | - | 30分24秒 (138) |
| | 18-24時 | 32分17秒 (1,140) | 31分14秒 (195) | 25分24秒 (23) | <u>46分33秒</u> (2) | <u>36分59秒</u> (7) | <u>25分17秒</u> (6) |
| 観光地 #A | 6-12時 | 27分38秒 (233) | 29分6秒 (91) | 4分53秒 (19) | - | - | 30分8秒 (14) |
| | 12-18時 | 20分59秒 (810) | 23分51秒 (423) | 30分3秒 (44) | <u>7分22秒</u> (1) | <u>50分29秒</u> (2) | 23分20秒 (10) |
| | 18-24時 | 25分1秒 (673) | 25分11秒 (470) | 30分 (61) | - | <u>16分1秒</u> (2) | <u>33分59秒</u> (3) |
| : | : | : | : | : | : | : | : |

加工後のデータイメージ(2):
玄関口から各観光地への移動人数

| 出発地点 | 第一移動先観光地 | | | |
|-------|----------|----|----|-----|
| | #1 | #2 | #3 | ... |
| 玄関口#1 | 32 | 1 | 37 | ... |
| 玄関口#2 | 19 | 0 | 30 | ... |
| 玄関口#3 | 2 | 0 | 4 | ... |

2.5 各ユースケースにおけるリスク評価の概要

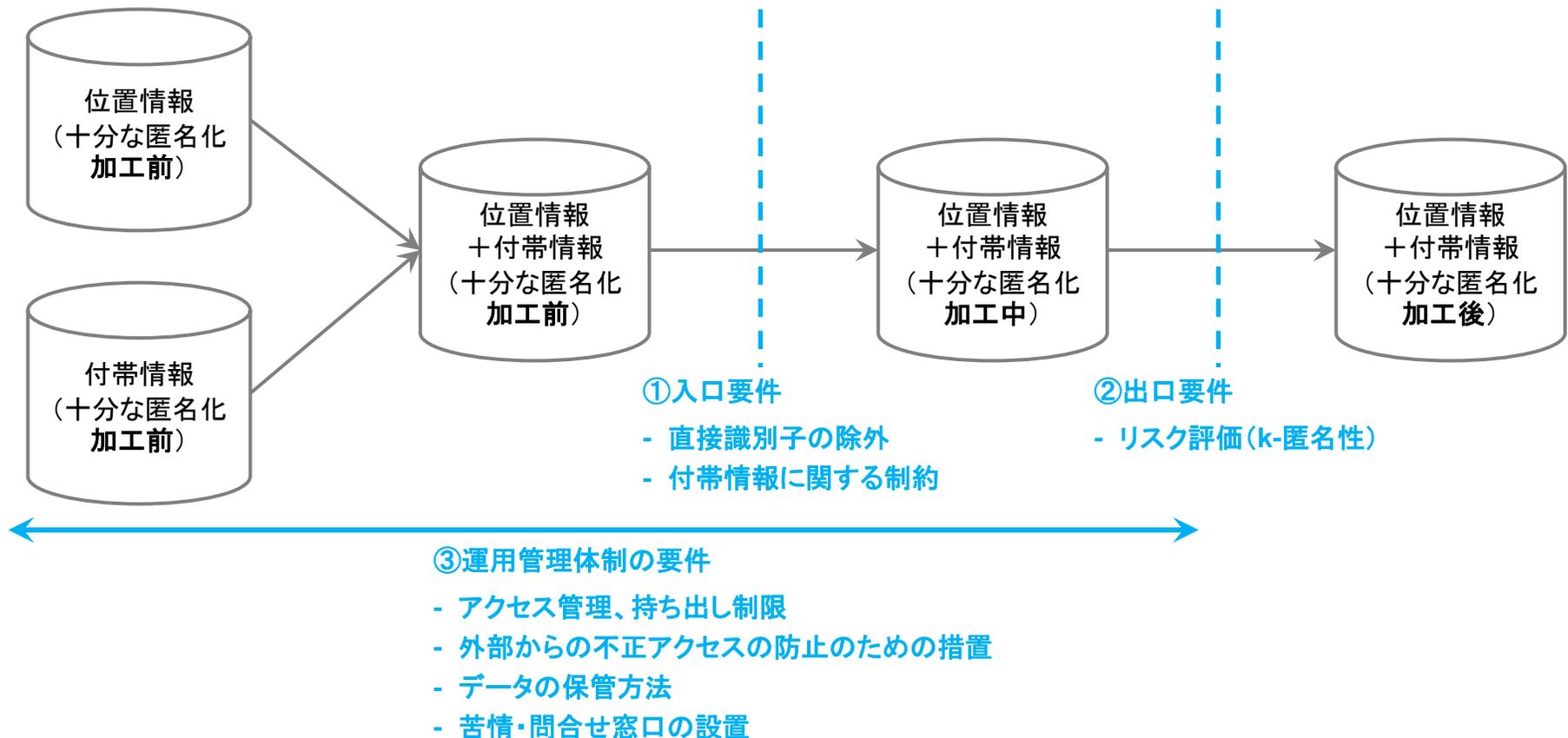
- 各ユースケースについて、(1)適切と考えられる加工方法を検討し、(2)当該方法によるデータ加工を行い、(3)その加工結果において個人の再特定化・再識別化のリスクが限定されているか、評価を行った。
 リスク評価に当たっては、再特定化・再識別化のリスクが(a) 取り扱うデータ及び(b) 取得・加工の内容によって決まるものと仮定し、これらの観点をもとに、8項目の指標を設定。(詳細は参考1-1～1-4を参照)
- 評価の結果、今回の各ユースケースについて、kの値によっては、加工後のデータにおいて特定の個人を識別するリスクが十分に低減されていることを確認した。
- 今後、どのようなケースが「十分な匿名化」に該当するか等、本格運用に向けて更なる検討が望まれる。

| ユースケース | 評価の結果 |
|--------|---|
| ① | <p>■GPS位置情報を250mあるいは500m メッシュで混雑度を集計した結果、被害想定が概ね正しく推定できた。さらには従来の調査で把握が困難だった季節変動や勤務者・観光客の流動も加味した被害想定を算出することができた。</p> <p>■なお、既存の災害シミュレーションでは500m以下のメッシュサイズで算定しており、今回は500mまで広げてもメッシュ内の個体数が1になる場合もあった。より正確な結果が求められる災害救助・防災分野においては課題が残るため引き続き検討が必要である。</p> |
| ② | <p>■仮IDの有効期間を一日に設定、空港エリア等を生活圏(自宅、職場等)とするユーザの除外、空港への発着地データの市区町村単位での集計等により個人特定リスクを低減しつつ、位置情報分析による発着地別の流動実態や属性を紐付けた利用者実態、特定地域間の移動量・所要時間を把握し、公共交通調査としての利活用、対象属性に合せた施策立案の可能性を示した。</p> <p>■なお、k=10の場合、特定個人の識別リスクは十分軽減されながらも、一定程度の有用性が保たれることが確かめられた。</p> |
| ③ | <p>■少数データ排除や仮IDの有効期間設定(分析内容により1日・1か月)、性別年代別の集計等の処理の他、球場周辺エリアと博多駅や天神等の商業エリア等、人通りの多いエリアを対象にメッシュを広く設定した加工処理を行い、個人を再特定するリスクを低減しつつ、来場者の動向(入退場時間、来場頻度、来場前後の2拠点間の周遊)を分析することができた。</p> <p>■なお、k値を大きくした場合はデータ損失が大きくみられ、マーケティング等に用いる有用性が損なわれるという結果も得られた。</p> |
| ④ | <p>■位置情報の分析は、観光の玄関口(駅・空港等)や著名な観光地等のスポット単位。データ分析対象期間は1ヶ月間(標本数:60,000)、観光地別の滞在時間の分析は、午前/午後/夜間の3つの時間帯で分析。観光の玄関口から各観光地への移動人数の分析は、2地点間で分析。</p> <p>■上記の匿名化を行った結果、ある特定の時刻・場所においてWi-Fiを利用した個人を再特定するリスクを低減しつつ、観光の場面において訪日外国人向けの多言語案内等の検討に資する分析を行うことができた。</p> |

3. 適切な加工の手法・管理運用体制の検証

- 各ユースケースの検討に基づき、今後のルールの一般化に向けて、契約約款等に基づく包括同意を前提に、通信の秘密に該当する位置情報の適切な加工の手法・管理運用体制の在り方について検討を実施した。
- 具体的には、データ加工プロセスの各段階に応じて、①加工を始める際の入口要件、②加工を終える際の出口要件、③出口までの管理運用体制の要件の3つの要件を設定し、「十分な匿名化」の要件を整理した。

データの加工プロセスにおける「十分な匿名化」を行うための要件 ①～③



3.1 入口要件、出口要件

①入口要件(加工を行う前の要件)

| | |
|----------|---|
| 直接識別子の除外 | 直接識別子は削除する。なお、仮IDの生成に当たっては、可能な限り短い有効期限を設ける、ハッシュ化等一方向の置き換えを行うといった措置を講じる。 |
| 付帯情報 | 住所(市区町村名まで)、性別、年齢の3つを加えるユースケースを検討した。言語情報の追加については今後の検討課題とする。 |

②出口要件(加工を行った後の要件)

| | |
|-------|--|
| リスク評価 | <ul style="list-style-type: none"> ■ 加工後のデータでは、原則次の条件を満たす(k匿名性): <ul style="list-style-type: none"> (i) 同一時刻のすべての間接識別子において<u>非識別</u>かつ (ii) すべての時間を通じた履歴において<u>非識別</u> ■ 複数のkについて、特定の個人を識別できてしまうリスクを定性的に評価し、評価の結果十分にリスクが低減されるkの値を決める。なお、その際のkの値については、一定程度大きい値から減じていくものとする。 ■ 上記のリスク評価を行う際の指標には、下記を含むものとする(各指標の詳細は次頁を参照)。 <ul style="list-style-type: none"> ①データの項目、②場所の特性、③利用者の特性、④取得期間・時期、⑤位置データの精度、⑥追跡可能な移動履歴の長さ・仮IDの有効期間、⑦データを取得する際の時間間隔、⑧標本数 ■ <u>上記のリスク評価の結果</u>、再特定化・再識別化に関するリスクが十分に低減されていることが判断された場合、k=1が許容される可能性がある。 |
|-------|--|

○今回の実証において、出口要件に係るリスク評価を行った評価指標は以下のとおり。

| (a) 取り扱うデータの内訳に関する指標 | |
|-----------------------------|--|
| ①データの項目 | データに含まれる項目。項目数が多いほどリスクが大きい。 |
| ②場所の特性 | データに紐づく地図上の場所の特徴。機微情報にかかわる場所や詳細な住所等が含まれている場合はリスクが大きい。 |
| ③利用者の特性 | データが対象にしている利用者の特徴。特定の母集団を対象とする場合はリスクが大きい。 |
| (b) 取得・加工の内容に関する指標 | |
| ④取得期間・時期 | データを取得した期間や時期。イベントや事件等が特定される場合リスクが大きい。 |
| ⑤位置データの精度 | データ取得時の位置の精度(携帯電話基地局であれば数十メートル～数百メートル)や加工時のメッシュの間隔等。精度が上がるほどリスクが大きい。 |
| ⑥追跡可能な移動履歴の長さ・仮IDの有効期間 | 特定の利用者を追跡できる地図上の軌跡又は時間的長さ。長いほどリスクが大きい。 |
| ⑦データを取得する際の時間間隔 | データを収集する際の時間的な間隔。間隔が狭いほどリスクが大きい。 |
| ⑧標本数 | 加工の対象となった利用者の数。少ないほどリスクが大きい。 |

3.2 管理運用体制

③管理運用体制の要件(加工途中の要件)

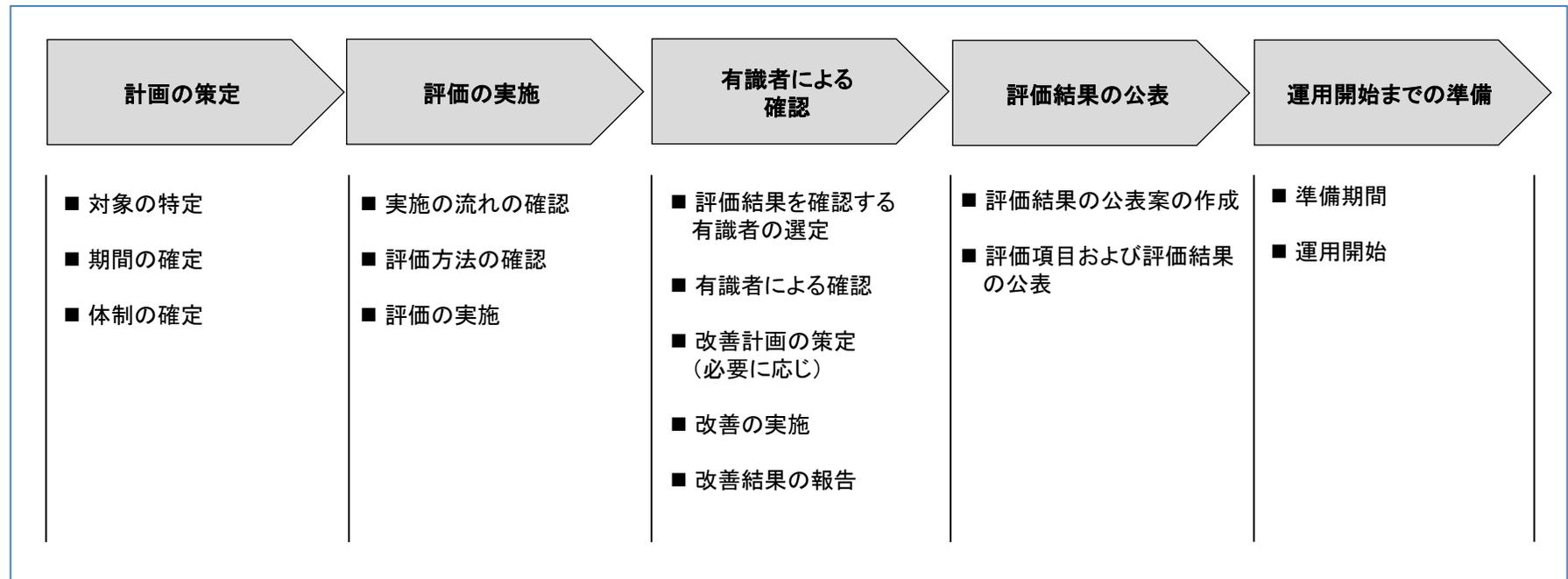
包括同意により通信の秘密に該当する位置情報の利活用を行う際に、電気通信事業者が整備すべき管理運用体制の要件を整理した。これらの要件に基づきPIA評価を行うことで、適切な管理運用体制を担保することを想定。

| 分類 | 小分類 | 実施目的 | 実施内容の例 |
|---------------------|---------|--|---|
| アクセス管理 | ID管理 | 加工に関与する者を特定すること | <ul style="list-style-type: none"> 一意のIDを割り当てる 一定期間未使用のIDを失効させる 等 |
| | 認証管理 | 特定された者だけが作業できるようにすること | <ul style="list-style-type: none"> パスワードの強度確保 等 |
| | アクセス権管理 | 業務上必要な範囲の作業しかできないようにすること | <ul style="list-style-type: none"> アクセス権を職務遂行に必要な最小限に制限する 等 |
| | ログ管理 | 作業内容を追跡できるようにすること | <ul style="list-style-type: none"> 加工前及び加工中データへの全てのアクセスの記録 等 |
| 持ち出し制限 | — | 加工前及び加工中におけるデータの持ち出し(漏洩や不正利用等)を防止すること | <ul style="list-style-type: none"> 加工前及び加工中のデータを取り扱うシステム環境からの外部アクセスの禁止 等 |
| 外部からの不正アクセス防止のための措置 | — | 加工を行う環境の外からの、データの破壊・改ざん・漏洩等を防止すること | <ul style="list-style-type: none"> 加工を行うシステム環境を他のシステム環境と物理的又は論理的に分離する 等 |
| データの保管方法 | — | 加工前及び加工中のデータについて、権限が付与された者にアクセスを限定し、容易に個人を再識別できないように保存すること | <ul style="list-style-type: none"> 加工前及び加工中のデータが格納されているDBやファイルを保存時に暗号化する 等 |
| 苦情・問合せ窓口の設置 | — | 加工に関する苦情や問合せに適切に対応すること | <ul style="list-style-type: none"> オプトアウトに対応する体制・手順・システム等の整備 等 |

4. プライバシー影響評価(PIA)の評価手順の検討・実施

- 位置情報の取扱い過程で、加工の手法・管理運用体制が適切であるか評価を行うため、PIAの評価項目、評価手順を策定。
- PIAでは、位置情報に関するリスク対策をライフサイクルを通じて評価。評価項目は、以下のとおり。
 - (1) 全般的事項、(2) データの取得(抽出)、(3) データの匿名化のための加工、(4) データの保管、(5) データの提供、(6) データの消去
- 各ユースケースに関して、策定した評価項目や手順を適用し、PIA評価を試行的に実施。
- 今後の本格運用に向け、有識者によるPIA結果の確認手順やPIA結果の公表案を検討した(参考2参照)。

PIAの進め方



5. 将来の位置情報の収集における利用者の同意取得方法等

① 包括同意約款(案)の作成

- 通信の秘密に該当する位置情報を包括同意の上で利活用するにあたっては、プライバシー上のリスクについて利用者の理解と信頼を得られるよう、利用者への周知・啓発を行っていくことが重要。
- このため、「位置情報プライバシーレポート」において利用者に対して説明・表示すべきとされた事項と、本調査研究に参加する各電気通信事業者の約款を照らし合わせ、包括同意約款の記載内容(記載事項およびその詳細さ)を整理・検討し、「包括同意約款(案)」を取りまとめた。

包括同意約款モデル(案)

※実際に運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。)を、電気通信役務の提供を目的に取得・利用するほか、お客様に関する契約者情報(市区町村名までの住所情報※¹、年齢、性別に限り※²)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。

【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、かつ利用者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に関する契約者情報、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、契約者情報、その他端末識別符号の当社における匿名化利用(加工後の情報の第三者提供を含みます。)について、別途定める方法により停止を申出することができます。

【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。

※1: 対象範囲については、今後、利用するユースケースに応じて各社で検討することとする。

※2: 利用言語情報は今後の継続検討課題。

②Web等での説明事項(案)の作成

- 「位置情報プライバシーレポート」において、「位置情報のプライバシー性の高さを踏まえれば、電気通信事業者は、利用者から同意を取得する前に、位置情報を取得されることに伴うプライバシー上のリスクについて利用者が理解できるように分かりやすく、かつ利用者が容易に参照できる場所に説明・表示を行うべきである」とされたことを踏まえ、「Web等での説明事項(案)」を取りまとめた。(参考3を参照)
- Webサイトの掲載においては、利用者が確認しやすい場所に掲載することも重要。

③業界としての位置情報取扱いポリシー(案)の作成

- 通信の秘密に該当する位置情報の取扱いについて、今後様々な利活用形態が出てくると想定される中、業界として適切に情報を利活用していく方向性を打ち出していくことが望ましいと考え、業界共通となりうるような汎用的な「位置情報取扱いポリシー」案として、「電気通信事業者の保有する位置情報等の運用データの取扱いについて(案)」を取りまとめた。(参考4を参照)
- 本内容については、業界共通のポリシーとして(一社)電気通信事業者協会のホームページ等で公開されることが望ましいと考えられる。

④一般的な電気通信の仕組みと位置情報の収集に関する説明(案)の作成

- 携帯電話基地局やGPS、Wi-Fi等、位置情報に関する一般的な仕組みについて、広く利用者側の理解が得られるよう、各仕組みの内容や特性を周知・説明する方法を検討し、そのための文面案等を作成した(詳細は、次頁及び参考5を参照)。
- 作成にあたって留意した点は以下のとおり。
 - 仕組みの説明では、図などを取り入れるなどして技術的な内容をなるべく平易に紹介することを念頭に置く。
 - それぞれの仕組みにおいて、どのような特性があるのか、どのような点で通信の秘密が関係するのかを説明する。
 - 位置情報が収集される際には、利用者に対して通常どのような通知があるのか、また収集されることを断る場合にはどのような方法があるのかについて紹介する。

一般的な電気通信の仕組みと位置情報の収集に関する説明(案)(抜粋)

電気通信事業者が取り扱う位置情報に関する一般的な仕組み

(1) 位置情報の概要 1/2

電気通信事業者が取り扱う位置情報とは

電気通信事業者は通信を成立させるために必要な通信端末の位置を把握しており、そうした通信端末の現在地を特定する情報を位置情報といいます。

最近では、アプリケーションを通じて近隣の天気予報や交通情報、店舗情報を取得したり、子供の居場所を確認したりする際にも位置情報が利用されます。

位置情報には以下の3種類があります。そして、取得される位置情報の精度は数メートル～数百メートル単位であり、その精度は位置情報の種類によって異なります。



※1 アクセスポイントのエリア内における通信端末の相対的位置を推定するものです。

※2 都市部では基地局間の距離が近いいため、位置情報の精度が数十メートルの場合もあります。

3 電気通信事業者が取り扱う位置情報に関する一般的な仕組み

6 利用者の受容性調査 実施概要

1. 背景・目的

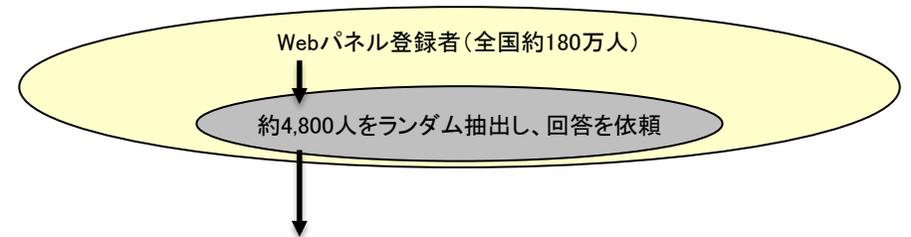
- 電気通信事業者が取得可能な移動体端末の位置情報について、一般の利用者を対象に、包括同意による社会的活用について説明した上で、①各ユースケースの匿名化加工方法に対する受容性、②包括同意による第三者提供・社会的活用に対する受容性、③匿名化の加工方法に対する受容性、④情報管理・運用体制とPIA評価に対する受容性を調査し、不安を感じる層に対して丁寧に説明すべき内容を明らかにするための受容性調査を実施。

2. 実施概要

- Webアンケート調査および対面デプスインタビュー（2016年1～2月に実施）

3. 調査対象

- Webアンケート：約180万人のWebパネル登録者より、全国18～69歳の生活者500人を抽出。回答者は携帯電話、スマートフォン、タブレット端末のいずれかの利用を条件とした。
- 対面デプスインタビュー：Webアンケート回答者より、首都圏居住者12人をリクルート、個別にインタビューを実施。



Webアンケートは下記割付にて500件を回収

| | 男性 | 女性 | 合計 |
|--------|------|------|------|
| 18～29歳 | 50人 | 50人 | 100人 |
| 30～39歳 | 50人 | 50人 | 100人 |
| 40～49歳 | 50人 | 50人 | 100人 |
| 50～59歳 | 50人 | 50人 | 100人 |
| 60～69歳 | 50人 | 50人 | 100人 |
| 合計 | 250人 | 250人 | 500人 |

Webアンケート回答者より、首都圏居住者12人をリクルートし、下記割付でデプスインタビューを実施

| 会場調査 | 男性 | 女性 | 合計 |
|--------|----|----|-----|
| 18～29歳 | 2人 | 2人 | 4人 |
| 30～49歳 | 2人 | 2人 | 4人 |
| 50～69歳 | 2人 | 2人 | 4人 |
| 合計 | 6人 | 6人 | 12人 |

4. 調査項目

- (1)基本属性と利用端末、(2)位置情報の認知度・設定状況・提供に対する意識、(3)各ユースケースにおける位置情報の匿名化加工方法などに対する受容性、(4)個別のユースケースによらない汎用的な匿名化加工方法に対する受容性、(5)位置情報の管理・運用体制と、PIA評価の仕組みに対する受容性、(6)包括同意による位置情報活用の説明方法に対する受容性、(7)包括同意による位置情報の社会的活用に対する受容性

6.1 利用者の受容性調査 調査結果

1. 個別同意と包括同意による受容性の違い

- Webアンケートでは、回答者500人に対し、移動体端末の位置情報の取得・活用について、「個別同意」と「包括同意」を説明した上で、それぞれの受容性を質問した。「個別同意」よりも「包括同意」の方が若干、受容性が低い結果となったが、**全体的な傾向は類似しており、差は比較的小さい。**

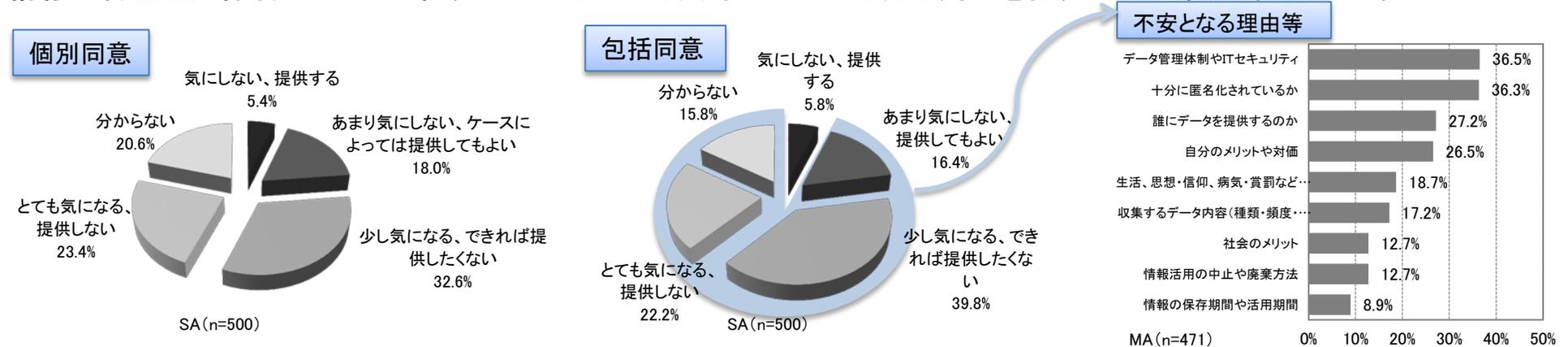
2. 受容性を高めるために必要と考えられる方策

- Webアンケートにおいて、包括同意について「気にしない、提供する」以外を選択した回答者(n=471)に対して、不安となる理由等を質問した。その結果、**包括同意において不安となる理由等は「データ管理体制やITセキュリティ」(36.5%)、「十分に匿名化されているか」(36.3%)が上位となった。**
- また、Webアンケートの回答者から抽出した12人に対し、携帯ショップの店頭をイメージした「包括同意」の実演デモを行い、それについてデプスインタビューを実施。その結果、**①包括同意による位置情報の利用・提供がどのような枠組の下で行われるか※1、②匿名加工の方法、③情報の管理運用体制とPIAの内容、④説明・周知項目を説明すると、包括同意に対する受容性が肯定的な方向に変化することが観察された※2。**

※1 十分な匿名化を行った上で利用・提供するものであり、契約書面やホームページなどで、利用・提供する情報の内容・範囲、匿名化の方法、利用目的、第三者提供の有無、利用・提供を中止する方法を明記・周知するものであること。

※2 12人中7人が肯定的な方向に変化。当初、「とても気になる、提供しない」、「少し気になる、できれば提供したくない」と回答した者については、全員が肯定的な方向に変化。

- このことから、**包括同意による受容性を高めるためには、包括同意により位置情報の利用・提供を行う旨や、匿名加工の方法、情報の管理運用体制やPIAの内容、オプトアウトの方法等について十分な周知を行うことが必要と考えられる。**



調査概要

調査目的

電気通信事業者が取得可能な位置情報について、位置情報を提供し、多様な目的に利用される事に対する携帯利用者の意識に関して調査を行う。

調査対象 / 調査手法

1 調査対象

- 18以上69歳までの男女
- 各年代300人(10代のみ100人) 計1,600サンプル
- 携帯電話保有者を対象

| | 男性 | 女性 | 合計 |
|--------|-----|-----|-------|
| 18-19歳 | 50 | 50 | 100 |
| 20-29歳 | 150 | 150 | 300 |
| 30-39歳 | 150 | 150 | 300 |
| 40-49歳 | 150 | 150 | 300 |
| 50-59歳 | 150 | 150 | 300 |
| 60-69歳 | 150 | 150 | 300 |
| 合計 | 800 | 800 | 1,600 |

2 調査手法

- 調査会社(株式会社クロスマーケティング)のパネルに対するウェブアンケート
- 調査の企画・分析に当たっては東京大学情報学環 橋元 良明教授、東京大学大学院学際情報学府博士課程(橋元研究室在籍) 河井 大介氏にご協力頂いた。

調査期間

□2014年3月21日(金)~2014年3月23日(日)

9 位置情報の利用に対する許容度(全体)

Q あなたの位置情報を次のような目的に利用することについて、あなたの考えに最も近いのはどれですか。

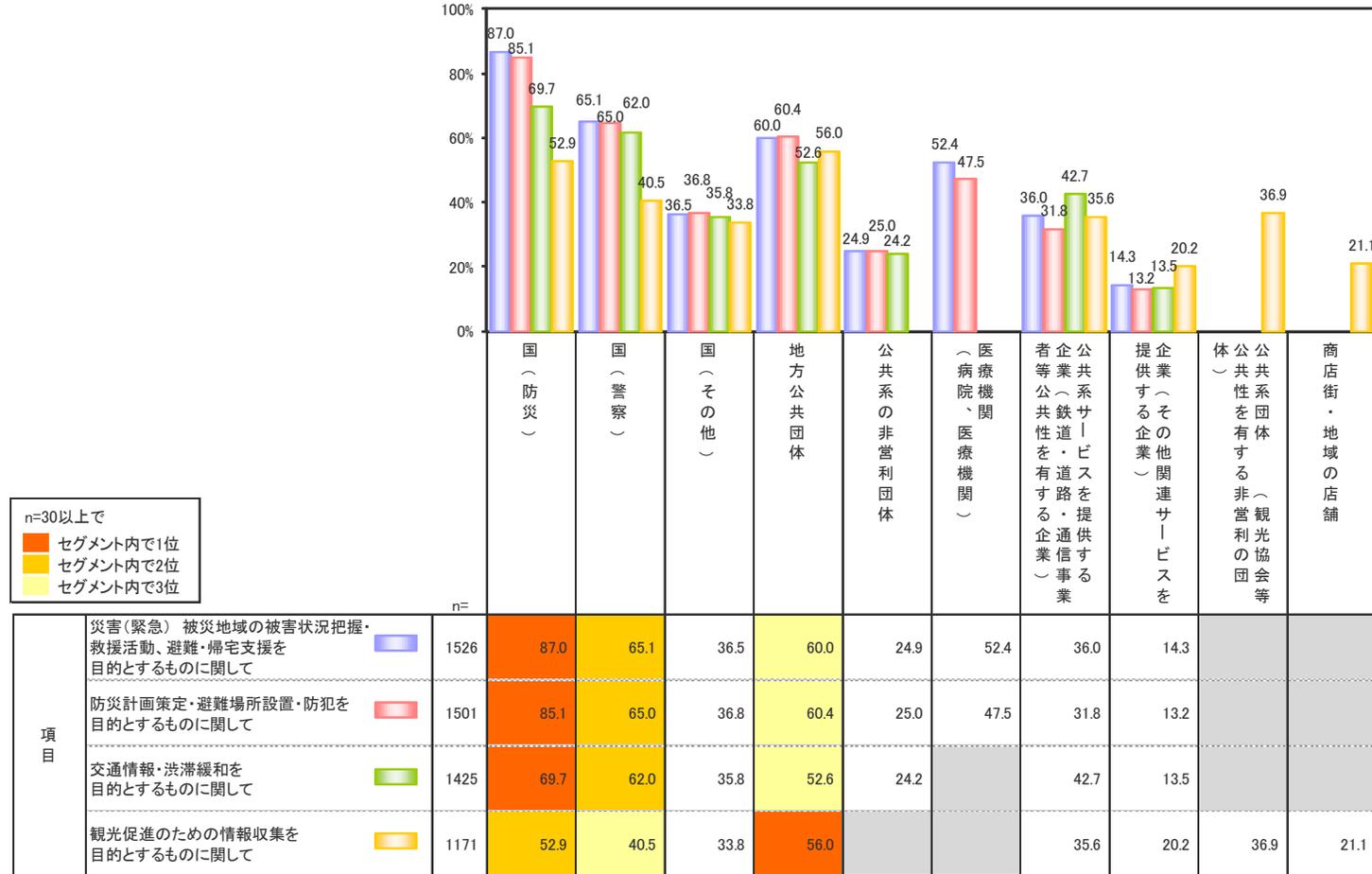
| 項目 | n | 許容できる・計 (%) | | | 許容できる・計 |
|---------------------------------|------|-------------|------------|---------------|---------|
| | | 許容できる | 条件付きで許容できる | どんな場合でも許容できない | |
| 災害(緊急) 被災地域の被害状況把握・救援活動、避難・帰宅支援 | 1600 | 67.3 | 28.1 | 4.6 | 95.4 |
| 防災計画策定・避難場所設置・防犯 | 1600 | 58.3 | 35.5 | 6.2 | 93.8 |
| 交通情報・渋滞緩和 | 1600 | 45.0 | 44.1 | 10.9 | 89.1 |
| 観光促進のための統計 | 1600 | 20.3 | 52.9 | 26.8 | 73.2 |
| 企業による地図ナビゲーションサービス(無料) | 1600 | 24.1 | 51.4 | 24.5 | 75.5 |
| 企業による最寄りの店舗情報・クーポン配信(無料) | 1600 | 20.5 | 50.5 | 29.0 | 71.0 |
| ソーシャルメディアの利用 | 1600 | 11.0 | 43.2 | 45.8 | 54.2 |
| 広告・マーケティングやサービス向上 | 1600 | 9.1 | 46.1 | 44.8 | 55.3 |

※n=30未満は参考値のため灰色。

- 位置情報の利用に対する目的別の許容度は、「災害(緊急)」「防災・防犯」については「許容できる」がそれぞれ67.3%、58.3%。さらに「条件付きで許容できる」を合わせると、それぞれ95.4%、93.8%と特に高い。次いで交通情報・渋滞緩和(89.1%)となっているが、公共性が高く、自分の安全に関わるものほど許容度が高い傾向。
- 企業が利用する場合であっても、「地図ナビゲーションサービス」「最寄りの店舗情報・クーポン配信」といった自分にメリットがあるサービスを楽しむためであれば、それぞれ75.5%、71.0%と比較的、許容度が高い。ただし、「条件付きで許容」の割合が5割超と高くなる。

10 位置情報の提供を許容できる主体(公共目的のみ・全体)

Q 下記の目的について位置情報をどのような主体にまで提供することが許容できますか。



- 「災害(緊急)」「防災・防犯」では、「国(防災)」が特に高く、それぞれ87.0%、85.1%が許容すると回答。次いで、「国(警察)」「地方公共団体」が6割超で続く。
- 「交通情報・渋滞緩和」でも「国(防災)」がトップであるが、69.7%と下がり、2番目の「国(警察)」と差が縮まる。
- 「観光促進」では、国を許容する割合が減り、「地方公共団体」が56.0%で一番に。
- 「医療機関」は5割前後、「公共系サービスを提供する企業」については3~4割の人が許容できると回答。

7. 総括 -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-

| 検証実施項目 | 検証できたこと | 今後の課題 |
|--|---|--|
| ユースケースの設定と「十分な匿名化」を行なうための加工の手法の検証 | <p>各ユースケースに応じて適切と考えられる加工方法を検討し、その方法によってデータの加工を行い、その加工の結果、個人の再特定化・再識別化のリスクが限定されているかについて検証した。今回の防災、交通、商用、観光の4件のユースケースにおいては、kの値を一定程度大きくした際に、再特定化・再識別化のリスクが十分軽減されたことが確認できた。</p> | <ul style="list-style-type: none"> ・今回の各ユースケースは、「十分な匿名化」の取組み事例として取扱うが、今後の本格運用時において、各ユースケースに類似するケースの準用基準や一般化に関して継続検討 |
| 適切な加工の手法・管理・運用体制の検証 | <p>各ユースケースの検討に基づき、今後のルール的一般化に向けて、契約約款等に基づく包括同意を前提に、通信の秘密に該当する位置情報の適切な加工の手法・管理運用体制の在り方について検討を実施。 (入口要件、出口要件、運用管理要件の整理)</p> | <ul style="list-style-type: none"> ・付帯情報に「言語情報」を含めることの可否 ・本格運用に向けたリスク評価指標に関する考え方 ・本格運用時における出口までの管理運用の要件 ・防災等を利用目的とする場合におけるK=1許容の可否 |
| プライバシー影響評価(PIA)の評価手順の検討・実施 | <p>位置情報の取扱い過程で、加工の手法・管理運用体制が適切であることの評価を行なうため、プライバシー影響評価の評価項目、評価手順を検討し策定。それらをもとに各ユースケースに関し評価を実施し、その結果を取りまとめた。</p> | <ul style="list-style-type: none"> ・本格運用時におけるPIA評価手続の具体化 |
| 将来の位置情報の収集における利用者の同意取得方法の検討 | <p>位置情報の収集を行なう際に利用者から同意を得る方法に関し、個別のケースによらない汎用的な方法(契約約款等の基づく事前の包括同意)や、利用者によるその周知・説明を行なうための方法を検討し、周知・説明のための文面案等を作成。</p> | <ul style="list-style-type: none"> ・整理した「包括同意約款(案)」、「Web等での説明事項(案)」、「電気通信事業者の保有する位置情報等の運用データの取扱いについて(案)」を掲載するまでの手順の具現化 |
| 一般的な電気通信の仕組みと位置情報の収集に関する説明方法の検討 | <p>携帯電話基地局やGPS、Wi-Fi等、位置情報に関する一般的な仕組みについて、広く利用者側の理解が得られるよう、各仕組みの内容や特性を周知・説明する方法を検討し、そのための文面案を作成。</p> | <ul style="list-style-type: none"> ・整理した「説明文面案」の運用と周知・説明する方法の具現化 |
| 利用者の受容性調査の実施 | <p>「包括同意」による位置情報の取得・活用についての受容性が、①包括同意による位置情報の利用・提供がどのような枠組の下で行われるか、②匿名加工の方法、③情報の管理運用体制とPIAの内容、④説明・周知項目を説明することで、受容性が高まることを確認。</p> | <ul style="list-style-type: none"> ・本格運用時に向け、通信の秘密に該当する位置情報を取扱う電気通信事業者における利用者への周知と説明の具現化準備 |

参考資料

参考1-1 リスク評価(NTTドコモ)

参考1-2 リスク評価(KDDI)

参考1-3 リスク評価(ソフトバンク)

参考1-4 リスク評価(エヌ・ティ・ティ・ブロードバンドプラットフォーム)

参考2 PIA評価結果の公表

参考3 Web等での説明事項(案)

参考4 電気通信事業者の保有する位置情報等の運用データの取扱いについて(案)

参考5 一般的な電気通信の仕組みと位置情報の収集に関する説明(案)

参考1-1 匿名化加工に関するリスク評価(NTTドコモ)

| | リスク評価指標 | リスク観点からの指標の特徴 <プライバシーリスクから見た属性 の特徴> | リスクの軽減・回避手段等 | | リスク評価指標 | リスク観点からの指標の特徴 <プライバシーリスクから見た属性 の特徴> | リスクの軽減・回避手段等 | | |
|---|--|--|---|---|---|---|---|--|---------------------------|
| 1 | データの項目 ⇒項目が多い ほどリスクが 大きい ⇒属性毎にリ スク面での特 徴を有する為、 特徴に即した リスク軽減加 工が必要 | ① GPS側位した位置情報 (緯度・経度) データの精度を粗くすること により、利用者が所在する 場所による本人特定リスク が軽減。 | 緯度・経度を250メートルメッシュへ加工 し、データの精度を粗くすることで、本人 特定リスクを軽減させた。 分析パターン②では、H22国勢調査にお いて500mメッシュ人口が900人に満た ないメッシュでは500mメッシュで集計、その 他のメッシュでは250mメッシュで集計 | 4 | 取得期間・時 期 ⇒イベントや事 件等が特定され る場合リスクは 大きい | イベントや事件があった日、 期間と一致する場合、本人 特定リスクが増加。 | 下記の期間中にデータ取得を行った が、イベントや事件が起きた箇所 ではなく、和歌山県沿岸部を対象と しているため、本人特定リスクは低い。 ◆平成27年1月1日～平成27年1月 31日:冬季 ◆平成27年8月1日～平成27年8月 31日:夏季 | | |
| | | ② 日時 データの精度を粗くすること により、利用者が所在する 時間による本人特定リスク が軽減。 | 日付データを「H27年夏」「H27年冬」の期 間名称へ、秒単位の時刻データを1時間 単位へ加工し、データの精度を粗くする ことで、本人特定リスクを軽減させた。 | | | | | ※1.データの項目①②にて 既述 | ※1.データの項目①②にて既述 |
| | | ③ ユーザID 直接識別子として、本人を 特定し得る情報であるため、 間接識別子へ変更が必要。 | ユーザIDを仮IDへ置き換え、加工途中の 集計処理の段階で仮IDを除去することで、 不可逆な措置を施し、本人特定リスクが 軽減させた。 | | | | | 追跡可能な移 動履歴の長 さ・仮IDの有 効期間 ⇒履歴が多い ほど、有効期間 が長いほどリス クが大きい | 追跡期間が短いほど、本人 特定リスクが軽減。 |
| 2 | 場所の特性 ⇒機微情報に かかわる場所 や住所等が 含まれている場合 リスクは大きい | 機微情報にかかわる場所 や住所等が含まれている場 合、本人特定リスクが増加。 | 履歴情報を属性判定(自宅、勤務、流動) に利用しエリア単位、属性別で集計を行 い、分析パターン②では、さらに居住者 の少ないエリアの自宅情報(自宅者)を 除去することで、本人特定リスクを軽減さ せた。 | 7 | データを取得 する際の時間 間隔 ⇒間隔が狭い ほどリスクが大 きい | データを取得する間隔が長 いほど、本人特定リスクが軽 減。 | データの取得頻度は最短5分単位であ るが、加工の中で、非特定化処理として 時刻を1時間単位に変換することで、本 人特定リスクを軽減させた。 | | |
| 3 | 利用者の特性 ⇒特定の母集 団を扱う場合リ スクは大きい | 特定の職業や同じ趣味・嗜 好等を持つ母集団を対象と した場合、母集団の数及び 母集団に所属する人数に よっては、対象の限定がし やすくなるため、本人特定リ スクが増加。 | 本ユースケースは、NTTドコモが提供す る「ドコモ地図ナビ」サービスのオート GPS機能の利用者から利用許諾を得た 上で送信される位置情報を対象として いるため、本人特定リスクは低い。 | 8 | 標本数⇒少な いほどリスクが 大きい | 全体標本数(得られたデータ 全体のレコード数)が多いほ ど、本人特定リスクが軽減。 | 約23,000名のデータを取得することで、 本人特定リスクを軽減させた。 | | |

参考1-2匿名化加工に関するリスク評価(KDDI)

| リスク評価指標 | リスク観点からの指標の特徴 <プライバシーリスクから見た属性 の特徴> | リスクの軽減・回避手段等 | リスク評価指標 | リスク観点からの指標の特徴 <プライバシーリスクから見た属性 の特徴> | リスクの軽減・回避手段等 |
|--|---|---|---------|--|--|
| データの項目 ⇒項目が多い ほどリスクが大 きい ⇒属性毎にリ スク面での特 徴を有する為、 特徴に即した リスク軽減加 工が必要 | ①位置（緯度・経度）の特徴 分解能（データの精度）により、 位置の特定の可能なレベル が異なる。（例、数センチ／数 十センチ／数メートル／数十 メートル／数百メートル／市 区町村／地域）数メートルの 場合、立ち寄った店舗等が判 明可能。 精度を粗くすることにより、リ スクを軽減可能。 | 「空港利用者の発地/滞在地（着地）/属性 分析」については、加工後データを市区町 村単位で集計することにより、位置を特定 されるリスクを軽減した | 1 | ③識別符号 識別符号は、「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」ものであり、個人 を特定しうる「識別子」相当の 情報であると考えられている ため、識別子に準じた取扱い が必要。 | 識別符号は使用せず、仮のIDへ置き換 えた。 元の識別符号と仮IDとの照合情報は破 棄し、不可逆な措置を施すことによりリス クを軽減させた。 |
| | ②時刻（時間）の特徴 秒単位から分・時・日のレベ ルがある。 精度を粗くすることによりリス クを軽減可能。 （例、1分単位→1時間単 位） | ・分析にあたり、秒単位のデータを15分刻 みに加工し、分解能を粗くした。した。 ・分析対象地メッシュに60分以上滞留した ユーザを分析対象とした。 ・（交通実態の分析では）羽田空港～新宿 間3時間以内に通過した移動を分析対象 とした。 上記3点の加工によりリスクを軽減させた。 「同一メッシュに60分以上滞留したユー ザ」については、より限定されたユーザを 対象としているが、上記No.1のメッシュの 状況を踏まえるとそれ自体では特定の ユーザを識別できるとは想定しづらい。ま た同様に「羽田空港～新宿間を3時間以 内に通過した移動を対象についても、同 区間の交通量を勘案するとそれ自体では 特定のユーザを識別できるとは想定しづ らい。 | | ④性別 通常は、男女いずれかの属 性値をとる。 | 性別は、特段の加工は施していない。 （男女いずれかの属性値を採用） |
| | | | | ⑤年齢 実年齢をそのまま用いた場 合、他の情報（受領者が独自 に入手した名簿情報）との照 合により、個人特定のリス クがある。 一般化（5歳、10歳等階級化） することにより、リスクを軽減 できる。 階級化した場合においても特 徴的な年齢（例100歳代）が 含まれる場合、他の情報と照 合する事により個人特定の 可能性は否定できない為、削 除すべきと考える。 | 分析にあたり、年齢を5歳刻みに一般化 し、更に、加工後データは、10歳刻みに 階級化の上、20歳未満と60歳以上は 各々集約することでリスクを軽減させた。 |

参考1-2匿名化加工に関するリスク評価(KDDI)

| リスク評価指標 | リスク観点からの指標の特徴 ＜プライバシーリスクから見た属性の特徴＞ | リスクの軽減・回避手段等 |
|--|---|---|
| 2 場所の特性 ⇒機微情報にかかわる場所や住所等が含まれている場合リスクは大きい | ⑥場所の特性 機微情報にかかわる場所や住所等が含まれている場合リスクは大きい | 羽田/成田空港を含め近隣の地域は、それ自体特段配慮を要する場所とは言えず、機微情報に該当しないと考える。 |
| 3 利用者の特性 ⇒特定の母集団を扱う場合リスクは大きい | ⑦利用者の特性 特定の職業や同じ趣味・嗜好等を持つ母集団を対象とした場合、母集団そのものの数によっては、対象の限定がしやすくなる為、リスクは大きくなる。 | 対象ユーザは、個別に同意を得たユーザ（全国に分布） 全国にランダムに分布したユーザを対象としており、特定のユーザ層やユーザの集合を類推できるとは言えず、特定のユーザを識別できるとは想定しづらい。 |
| 4 取得期間・時期 ⇒イベントや事件等が特定される場合リスクは大きい | ⑧取得期間・時期 特定のイベントや事件のあった日、期間と一致する可能性がある場合、他の情報（受領者が独自に入手した情報）との照合により、個人特定のリスクがある。 | Term1：2015年2月7日～2015年3月6日（中央環状線 開通前一ヶ月） Term2：2015年3月7日～2015年4月6日（中央環状線 開通後一ヶ月） 上記2ヶ月間、羽田空港/成田空港を含め近隣の地域で特定のイベントや事件等を類推できるとは言えず、特定のユーザを識別できるとは想定しづらい。 |
| 5 位置データの精度 ⇒精度が上がるほどリスクは大きい | ※位置（緯度・経度）については1.①で既述 | 「空港利用者の属性分析」では、係数による拡大推計の加工を実施することによりリスクを軽減させた。 |

| リスク評価指標 | リスク観点からの指標の特徴 ＜プライバシーリスクから見た属性の特徴＞ | リスクの軽減・回避手段等 |
|---|---|--|
| 6 追跡可能な移動履歴の長さ・仮IDの有効期間 ⇒履歴が多いほど、有効期間が長いほどリスクは大きい | ※ 仮IDの有効期間については、1.③で既述 ⑨移動履歴 ・トレースする時間が長ければ長い程、起点から終点の履歴が長い程、又ホップ数が多ければ多い程リスクが高い ・特徴的な場所の推定 移動履歴に含まれる位置に個人を特定する為の鍵となる特徴的な場所と解釈可能な場所が含まれる場合（例、自宅住所）、特徴的な場所を使って他の情報（受領者が独自に入手した情報）と照合することにより個人特定がなされる（例、移動履歴から自宅住所→名簿と照合） ・パターン性のある移動履歴 パターン性のある移動履歴があり、既知である（他手段でも収集されている）場合、両者を照合することで、個人特定のリスクがある。（例、移動履歴にユニークな通勤経路を含む場合、他のサービス等で通勤経路と氏名を把握したデータがある場合、個人特定がなされる） 移動履歴の中に、 受領者が知り得た情報 がある場合、個人特定のリスクがある。（例、目撃者（日付、時間、場所）又はSNS等での公開情報） | 仮ID有効期間は、1日（日毎に異なるようハッシュ化）に限定することによりリスクを軽減させた。 2ホップ利用：空港利用者の発地/滞在/属性分析 4ホップ利用：交通実態の分析（特定地点間の移動量/移動所要時間） ホップ数は、上記数値に留めることによりリスクを軽減した。 上記仮IDとホップ数の有効期間では、同一ユーザを追跡する範囲が限定されており、特定のユーザを識別できるとは想定しづらい。 分析対象地は、指定期間に羽田/成田空港周辺を通過したユーザであり、利用者の自宅や勤務先等と紐づける情報を含まない。また、分析対象地を生活圏（自宅・職場）と推定されるユーザは除外した。 |

参考1-2匿名化加工に関するリスク評価(KDDI)

| | リスク評価指標 | リスク観点からの指標の特徴 <プライバシーリスクから見た属性 の特徴> | リスクの軽減・回避手段等 |
|---|---|--|---|
| 7 | データを取 得する際の 時間間隔 ⇒間隔が狭 いほどリスク が大きい | ※時刻(時間)については1. ③で既述 | ※時刻(時間)については1.③で既述 |
| 8 | 標本数 ⇒少ないほ どリスクが大 きい | <p>⑩全体標本数(得られた データ全体のレコード数)</p> <p>標本数が多ければ多い程、 多くの人数から個人を特定 する確率が低くなる為、標本 数は多い程リスクは低い。</p> <p>⑪サンプル数(「全体標本 数」から、加工等を行い実際 に分析に使用したレコード 数)</p> <p>サンプル数が多ければ多い 程、多くの人数から個人を特 定する確率が低くなる為、サ ンプル数は多い程リスクは 低い。</p> | <p>全体標本数</p> <ul style="list-style-type: none"> ・羽田空港利用者: 91,836件 ・成田空港利用者: 11,720件 <p>サンプル数</p> <ul style="list-style-type: none"> ・羽田空港利用者: 76,919件 ・成田空港利用者: 8,603件 <p>各空港利用者数はさらに十分に多いと想 定されるため、特定の個人を識別できると は想定しづらい。</p> |

参考1-3匿名化加工に関するリスク評価(ソフトバンク)

| リスク評価指標 | リスク観点からの指標の特徴 ＜プライバシーリスクから見た属性 の特徴＞ | リスクの軽減・回避手段等 |
|--|--|--|
| データの項目 ⇒項目が多いほどリスク が大きい ⇒属性毎に リスク面で の特徴を有 する為、特 徴に即した リスク軽減 加工が必要 | ①位置(緯度・経度)の特徴 分解能(データの精度)により、位置の特定の可能なレベルが異なる。(例、数センチ／数十センチ／数メートル／数十メートル／数百メートル／市区町村／地域)数メートルの場合、立ち寄った店舗等が判明可能。 精度を粗くすることにより、リスクを軽減可能。 | ＜リスクを軽減する加工＞ 緯度・経度を125mメッシュへ加工し、分解能を粗くした。 更に分析対象エリアを広く捉えることにより、位置を特定されるリスクを軽減した。 (例 天神地区においては、125mメッシュ24個の集合) |
| | ②時刻(時間)の特徴 秒単位から分・時・日のレベルがある。 精度を粗くすることによりリスクを軽減可能。(例、1分単位→1時間単位) | ＜リスクを軽減する加工＞ 緯度・経度を125mメッシュへ変換後、同一のメッシュに連続して10分以上滞在した位置情報のみに絞り込み、滞留点として抽出。(中間処理) さらに、連続して20分以上滞在した情報のみを対象として抽出した。 |
| | ③識別符号 識別符号は、「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」ものであり、個人を特定しうる「識別子」相当の情報であると考えられているため、識別子に準じた取扱いが必要。 | ＜リスクを軽減する加工＞ 識別符号は使用せず、仮のIDへ置き換えた。 元の識別符号と仮IDとの照合情報は破棄し、不可逆な措置を施すことによりリスクを低減させた。 ＜分析に利用した仮IDの有効期間＞ ①入退場・来場回数分析:約一ヶ月 ②移動行動:1日 さらに、仮IDの有効期間を限定することによりリスクを軽減させた。 |

| リスク評価指標 | リスク観点からの指標の特徴 ＜プライバシーリスクから見た属性 の特徴＞ | リスクの軽減・回避手段等 |
|---------|--|--|
| 1 | ④住所 利用する住所の範囲によりリスクは異なる。 より広いレベルで範囲を限定する程、リスクは低くなる。(例、都道府県レベル) 住所全項目(都道府県市区町村丁目番地号建物名部屋番号)を使用した場合、例えば単身世帯では一意性が有り、他の情報(受領者が独自に入手した名簿情報)との照合により、個人特定のリスクがある。 また、市区町村レベルの住所情報においても、特徴的な住所(例、過疎地)の場合、サンプル数によっては市区町村レベルでもリスクがある為、特徴的な住所(過疎地等の少数データ)は除外すべきと考える。 | ＜リスクを軽減する加工＞ 住所情報の取得は、市区町村レベルの住所コードを取得し、分析の為に用いたレベルは、来場者の都道府県別集計でのみ利用。 住所は都道府県レベルの広域でのみ利用することでリスクを軽減させた。 都道府県情報のみでは一意性が無く、リスクは低い。 |
| | ⑤性別 通常は、男女いずれかの属性値をとる。 | ＜リスクを軽減する加工＞ 性別に関しては特段の加工は施していない |

参考1-3匿名化加工に関するリスク評価(ソフトバンク)

| リスク評価指標 | リスク観点からの指標の特徴 ＜プライバシーリスクから見た属性の特徴＞ | リスクの軽減・回避手段等 |
|---------|--|---|
| 1 | <p>⑥年齢</p> <p>実年齢をそのまま用いた場合、他の情報(受領者が独自に入手した名簿情報)との照合により、個人特定のリスクがある。</p> <p>一般化(5歳、10歳等階級化)することにより、リスクを軽減できる。</p> <p>階級化した場合においても特徴的な年齢(例100歳代)が含まれる場合、他の情報と照合する事により個人特定の可能性は否定できない為、削除すべきと考える。</p> | <p>＜リスクを軽減する加工＞</p> <p>年齢は、10歳刻みに階級化することでリスクを軽減させた。</p> <p>特徴的な年代はサンプルに含まれていなかった。</p> |
| 2 | <p>場所の特性 ⇒機微情報にかかわる場所や住所等が含まれている場合リスクは大きい</p> <p>⑦場所の特性</p> <p>機微情報にかかわる場所や住所等が含まれている場合リスクは大きい</p> | <p>球場施設及び4つの対象エリアは一般的な商業エリアであり、機微情報に該当しないと考える。</p> |
| 3 | <p>利用者の特性 ⇒特定の母集団を扱う場合リスクは大きい</p> <p>⑧利用者の特性</p> <p>特定の職業や同じ趣味・嗜好等を持つ母集団を対象とした場合、母集団そのものの数によっては、対象の限定がしやすくなる為、リスクは大きくなる。</p> | <p>本ユースケースにおいては、野球に興味がある可能性は高いと想定されるが、一般的かつ十分に多くの人がもつ趣味嗜好と考えられる為、リスクは低いと考えられる。</p> |

| リスク評価指標 | リスク観点からの指標の特徴 ＜プライバシーリスクから見た属性の特徴＞ | リスクの軽減・回避手段等 |
|---------|--|--|
| 4 | <p>取得期間・時期 ⇒イベントや事件等が特定される場合リスクは大きい</p> <p>⑨取得期間・時期</p> <p>特定のイベントや事件のあった日、期間と一致する可能性がある場合、他の情報(受領者が独自に入手した情報)との照合により、個人特定のリスクがある。</p> | <p>2015年8月の約1か月間(7/27～8/31)のうち、試合開催日が対象</p> |
| 5 | <p>位置データの精度 ⇒精度が上がるほどリスクが大きい</p> <p>※位置(緯度・経度)については1.①で既述</p> | <p>ランダム化は実施しない</p> <p>数値の置き換えも実施していない</p> <p>人口比率等の係数での加工等も実施していない</p> |

参考1-3匿名化加工に関するリスク評価(ソフトバンク)

| リスク評価指標 | リスク観点からの指標の特徴 ＜プライバシーリスクから見た属性の特徴＞ | リスクの軽減・回避手段等 | リスク評価指標 | リスク観点からの指標の特徴 ＜プライバシーリスクから見た属性の特徴＞ | リスクの軽減・回避手段等 |
|---|--|--|------------------------------------|---|--|
| 6 追跡可能な移動履歴の長さ・仮IDの有効期間⇒履歴が多いほど、有効期間が長いほどリスクが大きい | <p>※仮IDの有効期間については、1.③で既述</p> <p>⑩移動履歴</p> <ul style="list-style-type: none"> ・トレースする時間が長ければ長い程、起点から終点の履歴が長い程、又ホップ数が多ければ多い程リスクが高い ・特徴的な場所の推定 <p>移動履歴に含まれる位置に個人を特定する為の鍵となる特徴的な場所と解釈可能な場所が含まれる場合(例、自宅住所)、特徴的な場所を使って他の情報(受領者が独自に入手した情報)と照合することにより個人特定がなされる(例、移動履歴から自宅住所→名簿と照合)</p> <ul style="list-style-type: none"> ・パターン性のある移動履歴 <p>パターン性のある移動履歴があり、既知である(他手段でも収集されている)場合、両者を照合することで、個人特定のリスクがある。</p> <p>(例、移動履歴にユニークな通勤経路を含む場合、他のサービス等で通勤経路と氏名を把握したデータがある場合、個人特定がなされる)</p> <p>移動履歴の中に、受領者が知り得た情報がある場合、個人特定のリスクがある。</p> <p>(例、目撃者(日付、時間、場所)又はSNS等での公開情報)</p> | <p>＜リスクを軽減する加工＞</p> <p>試合開催日の1日に限定し、1時間刻みで集計。ホップ数を2(起点→終点の2地点間の移動)に留めることでリスクを低減した。</p> <p>分析対象としたエリアは、ヤフオクドーム周辺、博多駅、天神地区、中洲地区、キャナルシティ周辺の広い商業エリアであり、利用者の自宅や勤務先等と紐づける情報を含まない。</p> <p>ヤフオクドームと各商業エリアの2地点間の移動は、パターン性を有するが、多くの一般の利用者移動するルートであると考えられる為、この2地点の移動パターンから個人を特定するリスクは考えられない。</p> <p>さらに、ヤフオクドームと各商業エリアは、一般の利用者が多数往來するエリアである為、個人を特定するリスクは低いと考える。</p> | 7 データを取得する際の時間間隔⇒間隔が狭いほどリスクが大きい | <p>※時刻(時間)については1.③で既述</p> | <p>＜リスクを軽減する加工＞</p> <ul style="list-style-type: none"> ・時刻は20分以上滞留した人を対象。 <p>入退場分析および移動パターン分析は試合開催日を対象に1時間刻みで集計。来場頻度は、1か月間を対象に日数を集計(※項番1と重複するので、整理が必要)</p> |
| | <ul style="list-style-type: none"> ・パターン性のある移動履歴 <p>パターン性のある移動履歴があり、既知である(他手段でも収集されている)場合、両者を照合することで、個人特定のリスクがある。</p> <p>(例、移動履歴にユニークな通勤経路を含む場合、他のサービス等で通勤経路と氏名を把握したデータがある場合、個人特定がなされる)</p> <p>移動履歴の中に、受領者が知り得た情報がある場合、個人特定のリスクがある。</p> <p>(例、目撃者(日付、時間、場所)又はSNS等での公開情報)</p> | <p>さらに、ヤフオクドームと各商業エリアは、一般の利用者が多数往來するエリアである為、個人を特定するリスクは低いと考える。</p> | | <p>⑪全体標本数(得られたデータ全体のレコード数)</p> <p>標本数が多ければ多い程、多くの人数から個人を特定する確率が低くなる為、標本数は多い程リスクは低い。</p> <p>⑫サンプル数(「全体標本数」から、加工等を行い実際に分析に使用したレコード数)</p> <p>サンプル数が多ければ多い程、多くの人数から個人を特定する確率が低くなる為、サンプル数は多い程リスクは低い。</p> | <p>全体標本数</p> <ul style="list-style-type: none"> ・収集した利用者は九州地域に居住する8,314名 <p>サンプル数</p> <ul style="list-style-type: none"> ・有効な位置情報を取得できた利用者は、6,608名 <p>ヤフオクドームにおける観客動員数は、3.5万人以上存在する為、ドーム周辺エリアの来場者はさらに多いと想定される。</p> <p>また、分析対象となる各商業エリア(博多駅、天神地区、中洲地区、キャナルシティ周辺は、更に多数の来場者が存在する。</p> |
| 8 標本数⇒少ないほどリスクが大きい | | | | | |

参考1-4匿名化加工に関するリスク評価(エヌ・ティ・ティ・ブロードバンドプラットフォーム)

| | リスク評価指標 | リスク観点からの指標の特徴 <プライバシーリスクから見た属性 の特徴> | リスクの軽減・回避手段等 | | リスク評価指標 | リスク観点からの指標の特徴 <プライバシーリスクから見た属性 の特徴> | リスクの軽減・回避手段等 | | | | |
|---|--|--|--|---|-------------------------------|---|---------------------------------|---|--|--|--|
| 1 | データの項目 ⇒項目が多いほどリスクが大きい ⇒属性毎にリスク面での特徴を有する為、特徴に即したリスク軽減加工が必要 | ①位置の特徴 分解能(データの精度)により、位置の特定の可能なレベルが異なる。(例、数センチ/数十センチ/数メートル/数十メートル/市区町村/地域)数メートルの場合、立ち寄った店舗等が判明可能。 精度を粗くすることにより、リスクを軽減可能。 | ・端末が接続したWi-FiのAP位置を用いており、位置精度は交通要素、観光地などのスポット単位。 ・各スポットの占有面積分だけ位置の不確定性があり、位置特定されるリスクは軽減されていると考える。 | 3 | 利用者の特性 ⇒特定の母集団を扱う場合リスクは大きい | ⑤利用者の特性 特定の職業や同じ趣味・嗜好等を持つ母集団を対象とした場合、母集団そのものの数によっては、対象の限定がしやすくなる為、リスクは大きくなる。 | Wi-Fiの利用者であり、特定の母集団に限るといった事情はない | | | | |
| | | ②時刻(時間)の特徴 秒単位から分・時・日のレベルがある。 精度を粗くすることによりリスクを軽減可能。(例、1分単位→1時間単位) 端末のWi-Fi APへの接続時間 | <リスクを軽減する加工> ・端末がWi-Fi APへ接続した時間を用いる。 ・今回の分析では、「午前」、「午後」、「夜間」の3時間帯に分類して加工。各時間帯とも1か月間のサンプル数をカウント。 ・時間粒度を1か月と長くとることにより、動線分析などからの個人特定リスクを軽減している。 | | | ⑥取得期間・時期 特定のイベントや事件のあった日、期間と一致する可能性がある場合、他の情報(受領者が独自に入手した情報)との照合により、個人特定のリスクがある。 | | 1ヶ月間取得しているため、一般的には特定のイベントや事件等を特定するのは困難と考える。 | | | |
| | | ③利用言語の特徴 端末が利用する言語情報 位置情報(位置、時刻)以外の付帯情報に該当する。 | <リスクを軽減する加工> ・分類は6言語のみ。都道府県別、市町村別など分類数がより多い住所情報と比べると個人特定のリスクは低いと考える。 ・Wi-Fiスポットの位置であり、著名な観光施設等を想定したダミーデータを用いている。 | | | 5 | | | 位置データの精度 ⇒精度が上がるとリスクが大きい | 1.①で既述 | 1.①で既述 |
| | | ④場所の特性 機微情報にかかわる場所や住所等が含まれている場合リスクは大きい | <リスクを軽減する加工> ・想定する著名な観光施設は、公開されている公共場所であり、機微情報に関わる場所は含まれていない。 | | | 6 | | | 追跡可能な移動履歴の長さ・仮IDの有効期間 ⇒履歴が多いほど、有効期間が長いほどリスクが大きい | ⑦移動履歴 ・トレースする時間が長ければ長い程、起点から終点の履歴が長い程、又ホップ数が多い程リスクが高い ⑧仮IDの有効期間 ・今回はダミーデータを利用 | <リスクを軽減する加工> ・ホップ数を2(玄関口→次の観光地の2地点間の移動)に留めることでリスクを低減した。 ・速度情報は用いていない |

参考1-4匿名化加工に関するリスク評価(エヌ・ティ・ティ・ブロードバンドプラットフォーム)

| | リスク評価指標 | リスク観点からの指標の特徴 <プライバシーリスクから見た属性 の特徴> | リスクの軽減・回避手段等 |
|---|---|--|---|
| 7 | データを取得する際の時間 間隔 ⇒間隔が狭いほど リスクが大きい | ※時刻(時間)については1. ②、3で既述 | ※時刻(時間)については1.②、3で既述 |
| 8 | 標本数 ⇒少ないほどリ スクが大きい | ⑨全体標本数(得られたデー タ全体のレコード数) 標本数が多いほど多い程、 多くの人数から個人を特定 する確率が低くなる為、標本 数は多い程リスクは低い。 ⑩サンプル数(「全体標本 数」から、加工等を行い実際 に分析に使用したレコード 数) サンプル数が多いほど多い 程、多くの人数から個人を特 定する確率が低くなる為、サ ンプル数は多い程リスクは低 い。 | ・サンプル数については -1日あたり1,500～2,000端末 -1か月取得でサンプル数6万件 であり、個人特定のリスクは低いと考 える。 ・Wi-Fi APを通じて取得できる端末数 (サンプル数)は、 -Wi-Fi機能を装備するスマートフォン、 タブレットを所持するユーザ かつ、 -各スポットでWi-Fiを使用したユーザ に限られるため、各スポットの実際の訪 問数(標本数)と比較してごく一部と考え られ、この観点からも個人特定のリスク は低いと考えられる。 |

参考2 PIA評価結果の公表

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。

| 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)(参考W)

弊社は、本ユースケースについてPIAを実施しました。

評価結果に基づき、次の点を実施します。
 ・社内ルールに基づく委託先のモニタリング(2015年11月30日から実施)
 ・データ取得に先立って、利用者の同意日時や同意撤回日時を記録し、いつでも提示できるようにするルールの整備(YYYY年MM月予定)

なお、本評価結果については、プライバシー・個人情報保護の法制度または技術の専門家である***教授、〇〇〇〇弁護士に確認・助言いただきました。

【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。

【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小さいと評価される場合は、例外的に簡略な方法で公開することも考えられる。

参考3 Web等での説明事項(案)

| No | 項目 ※位置情報プライバシー ポートP29 | モデル案(実際に適用する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 | <p>当社は、契約者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。</p> <p>(1)基地局位置情報 契約者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</p> <p>(2)GPS位置情報 〇〇〇</p> <p>(3)Wi-Fi位置情報 〇〇〇</p> |
| ウ | 位置情報の精度、取得頻度、ID有効期間 | <p>当社は、契約者が利用する端末の位置情報を以下のように取得します。</p> <p>(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</p> |
| エ | 加工の手法 | <p>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、契約者から取得した情報(上記位置情報および下記契約者情報)につき、十分な匿名化を行います。</p> <p>利用する加工手法:</p> <p>(1)削除・仮名化 データの属性・項目を削除、またはそれらを異なる符号や番号へ置換します。 例: 氏名を削除します。電話番号を異なる番号に置き換えます。 生活圏情報(自宅、職場等)を削除します。</p> <p>(2)一般化 データの属性・項目を要約します(一定の範囲にある複数のレコード同士でまとめます)。 例: 地図上いくつかのエリアを設け、そのエリアに含まれているレコードは同じ位置属性を持つとします。</p> <p>(3)ランダム化 位置情報を不規則にずらす、または置き換えます。 例: 位置情報(緯度・経度)にランダムな値を加えます。</p> <p>《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。》</p> |

| | | |
|---|-----------------------|---|
| オ | 利用目的 | <p>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。</p> <p>(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</p> <p>《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。》</p> |
| カ | 第三者提供の有無及びその提供先 | <p>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、個人を再特定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。</p> |
| キ | 保存期間 | <p>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。</p> |
| ク | 位置情報に紐付けて利用される他の利用者情報 | <p>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、以下の契約者情報を位置情報へ紐付けて利用します。</p> <p>(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</p> <p>《契約者情報は、住所、年齢および性別に限られます。》</p> |
| ケ | 利用者関与の仕組み | <p>契約者から、位置情報の匿名化利用(加工後の情報の第三者提供を含みます)を停止しようお申し出があった場合、そのお申し出以降、その契約者の位置情報の匿名化利用を停止いたします。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。</p> <p>(1)Webページから http://www.***.com/****/****</p> <p>(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)</p> |
| コ | 情報管理体制 | <p>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および匿名化した情報についての管理運用体制を適正に運用します。また、加工の手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。</p> |

参考4 電気通信事業者の保有する位置情報等の運用データの取扱いについて(案)

電気通信事業者の保有する位置情報等の運用データの取扱いについて(案)

ICT(情報通信技術)の普及・発展に伴い、電気通信事業者が電気通信サービスを提供する過程で取得する位置情報等の情報(以下「運用データ」)を適切に取扱うことを前提として、いわゆる「ビッグデータ」として、様々な付加価値を生み出す時代を迎えており、これら情報の利活用を通じた安心安全な社会の実現や新事業の創出、国民の利便性の向上に、大きな期待が寄せられているところです。

当協会においては、会員である携帯電話事業者等、関係事業者が利用者のプライバシーを適切に保護しつつこれらの情報を利用することが可能となるよう、これら情報の取扱いに係る基本的な考え方を取りまとめ、ここに示すことと致しました。当協会及び関係事業者各社(以下「事業者」)は、各種法令に加えてこの考え方を順守し、利用者に引き続き安心して電気通信サービスをご利用頂けるよう取り組んでまいります。

1. 利用目的等の公表

事業者は、運用データを利用するときは、その利用目的を定めて公表するものとします。

ただし、公表した利用目的の範囲内で第三者(委託先を除きます)に提供することなく利用する場合、個別に利用者の同意を取得して利用する場合および利用について違法性阻却事由がある場合(以下、併せて「サービス利用」といいます)を除きます。なお、通信の秘密に該当する運用データを包括的同意に基づいて利用するときは、利用する情報の項目を公表するものとします。

2. 十分な匿名化加工

通信の秘密に該当する運用データを包括的な同意に基づいて利用する場合には、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言える状態に匿名化する加工を施します。ただし、サービス利用の場合を除きます。

3. 運用データの第三者提供

事業者は、運用データをサービス利用する場合を除き、第三者(委託先を含みます)に提供するときは、その第三者に対してあらかじめ定めた目的を逸脱する利用を禁止するとともに、①十分な匿名化加工がなされた通信の秘密に係る運用データを包括的な同意に基づいて提供する場合には、その第三者による再特定化および再識別化を禁止することとし、②その他の匿名化された運用データの提供の場合は、その第三者による再特定化を禁止することとします。

4. 利用者関与の仕組み(オプトアウトの提供)

事業者は、運用データをサービス利用する場合を除き、利用・第三者提供(委託先に対する提供を除きます)を停止するよう利用者から申出があった場合には、その申出以降の当該利用者の運用データの利用・第三者提供を停止します。

5. 運用データの管理運用体制の整備及び定期的評価

事業者は、運用データの管理運用体制を適切に整備するとともに、通信の秘密に係る運用データをサービス利用以外に用いるときは、管理運用体制の適切性について定期的に評価を行い、その結果を公表するものとします。

6. 法令等の遵守

事業者は、運用データを利用する場合には、関連法令等を遵守しつつ適切に対処します。

以上

【関連情報】

- ・電気通信事業における個人情報保護に関するガイドライン
http://www.soumu.go.jp/main_content/000365000.pdf
- ・位置情報プライバシーレポート
http://www.soumu.go.jp/main_content/000293966.pdf

【関係事業者一覧】

参考5 一般的な電気通信の仕組みと位置情報の収集に関する説明(案)

電気通信事業者が取り扱う位置情報に関する一般的な仕組み

(1) 位置情報の概要 1/2

電気通信事業者が取り扱う位置情報とは

電気通信事業者は通信を成立させるために必要な通信端末の位置を把握しており、そうした通信端末の現在地を特定する情報を位置情報としています。

最近では、アプリケーションを通じて近隣の天気予報や交通情報、店舗情報を取得したり、子供の居場所を確認したりする際にも位置情報が利用されます。

位置情報には以下の3種類があります。そして、取得される位置情報の精度は数メートル～数百メートル単位であり、その精度は位置情報の種類によって異なります。



※1 アクセスポイントのエリア内における通信端末の相対的位置を推定するものです。

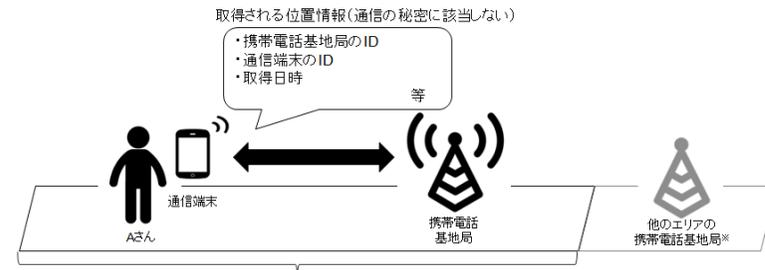
※2 都市部では基地局間の距離が近いため、位置情報の精度が数十メートルの場合もあります。

3 電気通信事業者が取り扱う位置情報に関する一般的な仕組み

電気通信事業者が取り扱う位置情報に関する一般的な仕組み

(2) 基地局に係る位置情報 1/2

通信端末は、いつでも着信を受けられるように使っていない時でも携帯電話基地局とこまめに連絡を取り合っています。複数の携帯電話基地局ごとにエリアをわけて通信端末の位置を管理しています。このような技術を位置登録としています。



通話やメール等を行っていない時でも、いつでも着信を受けられるように、Aさんの通信端末は携帯電話基地局とこまめに連絡を取り合っています。通信端末と携帯電話基地局が連絡を取り合うと、基地局に係る位置情報(携帯電話基地局のID、Aさんの通信端末のID、取得日時等)を電気通信事業者が取得します。位置登録で取得される位置情報は、実際に通信している際に用いられる情報ではないため、「通信の秘密」に該当しません。通話やメールを行う時の通信の仕組みは、次頁でご説明します。

※通信端末は所在するエリアにある携帯電話基地局と連絡を取り合うため、他のエリアの携帯電話基地局とは連絡を取り合っていません。

5 電気通信事業者が取り扱う位置情報に関する一般的な仕組み

電気通信事業者が取り扱う位置情報に関する一般的な仕組み

(1) 位置情報の概要 2/2

電気通信事業者が取得する位置情報は、主に次のように分類され、中には通信の秘密*に該当するものと該当しないものがあります。

電気通信事業者が取得する位置情報

| | 携帯電話基地局 | GPS | Wi-Fi |
|------------|---|---|---|
| 概要 | いつでも着信を受けられるように通信端末が携帯電話基地局と連絡を取り合っているときに取得される基地局に係る位置情報(詳細はP6をご参照ください) | GPS機能およびサービスを利用するときに取得される通信端末の位置情報(詳細はP7をご参照ください) | Wi-Fiを利用する際に通信端末がWi-Fiのアクセスポイントと接続の準備を行っているときに取得される通信端末の位置情報(詳細はP8をご参照ください) |
| 通信の秘密への該当性 | ・通信の秘密に該当しない ・通信の秘密に該当する | ・通信の秘密に該当しない | ・通信の秘密に該当しない ・通信の秘密に該当する |
| 取得の経緯 | ・通信の前提として取得される ・通信時に取得される | ・利用者が当該情報を取得する機能・サービスを利用する際に取得される。また、設定によりバックグラウンドで取得されることもある | ・通信の前提として取得される ・通信時に取得される |

上記の位置情報の分類ごとに、位置情報が取得される仕組みについては次頁以降で詳しくご説明します。

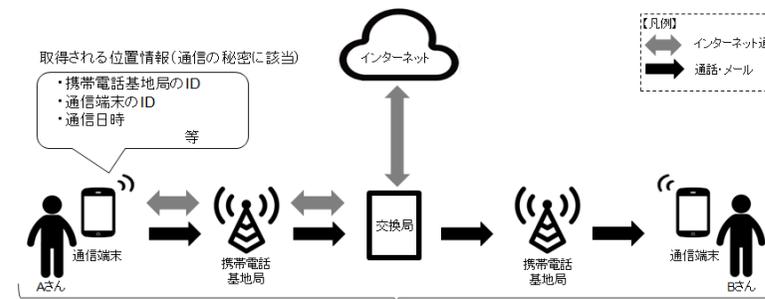
※電話や電子メールといった通信について、勝手に第三者が見たり利用したりしてはいけないとすることを、「通信の秘密の保護」といい、日本国憲法や電気通信事業法等で定められています。

4 電気通信事業者が取り扱う位置情報に関する一般的な仕組み

電気通信事業者が取り扱う位置情報に関する一般的な仕組み

(2) 基地局に係る位置情報 2/2

通信事業者が通話やメール等の通信を提供するために、電気通信事業者は位置情報を取得しています。携帯電話基地局を利用した通話やメールの方法は以下のとおりです。



AさんがBさんに通話やメールを行う際に、基地局に係る位置情報(携帯電話基地局のID、AさんとBさんの通信端末のID、通信日時等)を電気通信事業者が取得します。Aさんがインターネットを利用した時も基地局に係る位置情報が取得されます。通話やメール、インターネット等を行うときに取得される位置情報は「通信の秘密」に該当します。

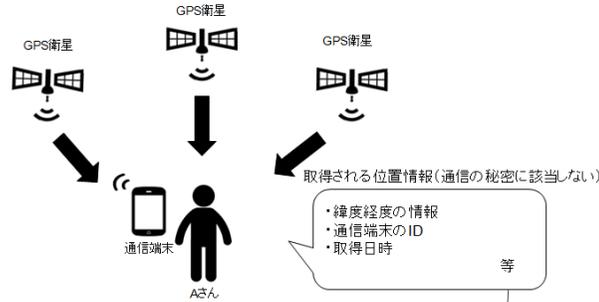
6 電気通信事業者が取り扱う位置情報に関する一般的な仕組み

参考5 一般的な電気通信の仕組みと位置情報の収集に関する説明(案)

電気通信事業者が取り扱う位置情報に関する一般的な仕組み

(3)GPSの位置情報

GPSとは、人工衛星を利用して通信端末の現在位置を割り出すシステムです。GPSの位置情報は、個々の通信を成立させるために必要な情報ではありません。そして、電気通信事業者が通信を成立させる前提として取得するものでもありません。例えば、アプリケーションを通じて子供の居場所確認や、交通情報、店舗情報の取得などに利用されます。



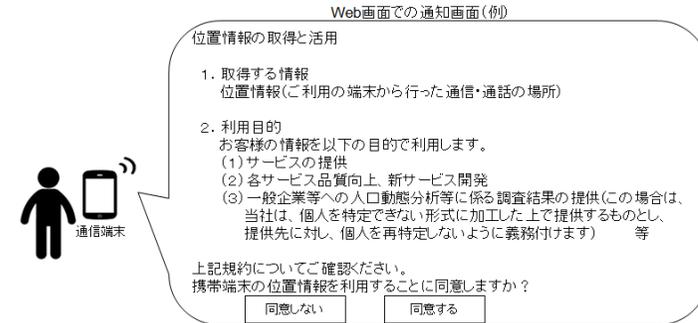
AさんがGPS機能およびサービスを利用する際に通信端末の位置情報(緯度経度情報、Aさんの通信端末のID、取得日時等)が取得されます。この時に取得された位置情報は、個々の通信を成立させるために必要な情報ではないため、「通信の秘密」に該当しません。

7 電気通信事業者が取り扱う位置情報に関する一般的な仕組み

電気通信事業者が取り扱う位置情報に関する一般的な仕組み

(5)位置情報の取得の一般的な通知方法

通信端末の位置情報は、位置情報を利用した機能やサービスごとに設定したり、利用や第三者への提供に同意するかどうか決めることができます。一般的な通知方法としてWeb画面等で取得する情報等を表示し、個別に同意を得ています^{*1}。ただし、通話やメール等の通信を成立させるために必要不可欠な位置情報の取得や、位置情報が取得されることが明らかなサービス(地図ナビゲーション等)での位置情報の取得においては、個別に同意を得ていない場合があります。



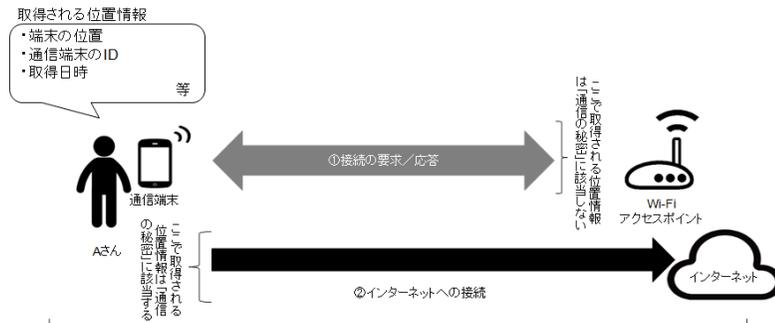
※1 現在、通信の秘密に係る位置情報については、十分な匿名化を前提に、契約約款等で記述することによる包括的な同意で利用できないか検討が進められています。

9 電気通信事業者が取り扱う位置情報に関する一般的な仕組み

電気通信事業者が取り扱う位置情報に関する一般的な仕組み

(4)Wi-Fiの位置情報

Wi-Fiとは、スマートフォンやタブレットなどのネットワーク接続に対応した機器を、無線(ワイヤレス)でネットワークに接続する技術のことです。電気通信事業者は、Wi-Fiの接続を提供するために通信端末の位置情報を取得しています。



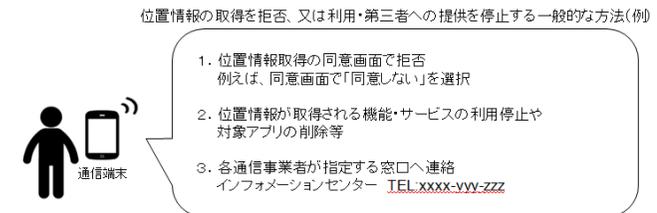
AさんがWi-Fiを利用する際に通信端末の位置情報(端末の位置、Aさんの通信端末のID、取得日時等)が取得されます。インターネットに接続された際に取得される位置情報(図の②)は、個々の通信を行うに際してのアクセスポイントに係る位置情報であることから、「通信の秘密」に該当します。一方で、接続の準備段階として取得される位置情報(図の①)は「通信の秘密」に該当しません。

8 電気通信事業者が取り扱う位置情報に関する一般的な仕組み

電気通信事業者が取り扱う位置情報に関する一般的な仕組み

(6)位置情報の取得拒否の一般的な方法

位置情報を利用する機能やサービスを利用する際に位置情報が取得されることを拒否、又は利用・第三者への提供を停止する仕組みを設けている場合があります。位置情報の取得を拒否、又は利用・第三者への提供を停止する場合の一般的な方法として、位置情報が取得される機能・サービスの利用停止や各通信事業者が指定する窓口へ連絡する方法があります。



10 電気通信事業者が取り扱う位置情報に関する一般的な仕組み

参考5 一般的な電気通信の仕組みと位置情報の収集に関する説明(案)

電気通信事業者が取り扱う位置情報に関する一般的な仕組み

(7) 位置情報の匿名化

昨今、位置情報も含めて個人情報を含むビッグデータの利活用が進んでおり、匿名化した上で観光・防災・街づくりなど生活の様々なシーンへの活用がされ始めています。
電気通信事業者においても、取得した位置情報を以下のように特定の個人を識別できないように匿名化して利用している場合があります。

匿名化のための加工の方法(例)

| | |
|-------|--|
| 仮名化 | 直接あるいは他の情報と組み合わせることで個人を特定できる情報を符号や番号等に置き換えること。 |
| メッシュ化 | 位置情報を点ではなくエリアで捉えることで個人特定を防止すること。 |
| 一般化 | 他の情報と組み合わせることで個人が特定できる情報を要約等すること。例えば、時間情報を時間帯へ要約する等。 |

匿名化のイメージ(例)

