別紙1

緊急時等における位置情報の取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

～位置情報に関するプライバシーの適切な保護と社会的利活用の両立に向けて～

（案）

平成26年５月

目次

１．位置情報の取扱いに係る検討の背景

(1)　パーソナルデータの利活用への期待と課題

ICT（情報通信技術）の普及・発展に伴い、多種多様な個人に関する情報（パーソナルデータ）を含む大量の情報が、容易に収集・蓄積され、また、これが流通・分析されることで社会に新たな付加価値を生み出す時代を迎えており、これにより、新事業の創出や国民の利便性の向上、より安心・安全な社会の実現などが期待されている。とりわけスマートフォン等の高機能な移動体端末が、国民の新たな生活基盤として、急速に普及しており、利用者の通信履歴や位置情報といった多種多様な利用者情報を取得・蓄積することが可能となってきていることから、電気通信事業者が取り扱うパーソナルデータへの利活用については、とりわけ期待が大きいところである。

その一方で、大量に収集・蓄積されたパーソナルデータが利活用されることによるプライバシー面における不安も生じている。

例えば、平成25年６月には、東日本旅客鉄道株式会社が、ICカード乗車券「Suica」の乗降履歴等の利用データを加工し、これを株式会社日立製作所に提供したことが明らかになったことで、多くの利用者からプライバシー面での批判を受ける事例が発生した。

また、平成25年11月には、株式会社NTTドコモ（以下「NTTドコモ」という。）が提供するサービス「ドコモ地図ナビ」について、従前より、収集したGPS位置情報については、管理・加工について業務委託した上で、統計的に加工したデータを第三者提供していたが、当該サービスの利用規則における位置情報の取扱いに係る記述が利用者にとって分かりづらかったことから、新聞報道等で問題として取り上げられる事例が発生した。

このような問題は、現行の個人情報保護法の下で、パーソナルデータを利活用する際のルールに不明確な部分があったことがその一因となっており、その明確化の必要性が指摘されている（後記(2)総務省パーソナルデータ研究会報告書参照）。これらを受けて、平成25年６月に内閣の高度情報通信ネットワーク社会推進戦略本部（以下「IT総合戦略本部」という。）において決定された「世界最先端IT国家創造宣言」においては、ビッグデータを活用した新産業・新サービスの創出がその柱の１つとして位置づけられるとともに、これを促進する上で、特に利用価値が高いと期待されている「パーソナルデータ」の取扱いについて、その利活用を円滑に進めるため、個人情報及びプライバシーの保護との両立を可能とする事業環境整備が１つの課題とされた。

これを受けて、IT総合戦略本部の下には、「パーソナルデータに関する検討会」（座長：堀部政男　一橋大学名誉教授（当時）（平成26年１月より宇賀克也　東京大学大学院法学政治学研究科教授）（以下「IT本部パーソナルデータ検討会」とい

う。））が設置され、平成25年９月から同年12月にかけて議論がなされた結果、同月には、個人情報及びプライバシーの保護を前提としつつ、パーソナルデータの適切な利活用を進めていくため、個人情報保護法改正に向けた「パーソナルデータの利活用に関する制度見直し方針」（以下「見直し方針」という。）が決定された。見直し方針においては、独立した第三者機関（プライバシー・コミッショナー）の設置や加工により個人が特定される可能性を低減したデータの取扱いについての制度整備等の方向性が示されるとともに、詳細な制度設計を含めた検討を加速させ、その検討結果に応じて、平成26年６月までに、法改正の内容を大綱として取りまとめ、平成27年通常国会への法案提出を目指すこととされた。

(2)　総務省におけるパーソナルデータに係る取組と本検討会の位置づけ

総務省においては、これまでパーソナルデータの取扱いについて、累次の先行的な検討を行ってきたところである。

「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」（座長：堀部政男　一橋大学名誉教授（当時）。以下「諸問題研究会」という。）においては、まず、平成22年５月にとりまとめられた第二次提言において、ライフログ[1]活用サービスについて検討を行っている。この中で、ライフログの活用サービスは、そのサービスの態様によっては、プライバシーを侵害し、かつ、利用者の不安感等を惹起し得ることから、ライフログを取得・保存・利活用する事業者は、利用者に対して一定の配慮をなし、円滑なサービスに資するための対策をとることが望ましいとした上で、ライフログ活用サービスは揺籃期にあることから、自主的なガイドライン等の作成の指針となる「配慮原則[2]」を策定している。

また、諸問題研究会においては、スマートフォンの急速な普及に対応して、平成24年８月に、スマートフォンにおける利用者情報[3]の取扱いについて、「スマートフォ

---

[1] ライフログとは、蓄積された個人の生活の履歴を指し、およそ考え得る蓄積された個人に関する情報の全てが含まれる。具体的なものとしては、ウェブサイトの閲覧履歴、電子商取引サイトにおける購買・決済履歴、携帯端末の GPS により把握された位置情報、携帯端末や自動車に搭載されたセンサー機器により把握された情報、デジタルカメラで撮影された写真、ブログに書き込まれた日記、SNS サイトに書き込まれた交友関係の記録、非接触型 IC を内蔵した乗車券による乗車履歴等から抽出された情報が挙げられている。（第二次提言　Ⅱ２.（1））

[2] 具体的には以下の6つの原則が挙げられた。

① 広報、普及・啓発活動の推進
② 透明性の確保
③ 利用者関与の機会の確保
④ 適正な手段による取得の確保
⑤ 適切な安全管理の確保
⑥ 苦情・質問への対応体制の確保

[3] 利用者の識別に係る情報（氏名、住所等の契約者情報、契約者・端末固有ID等）、第三者の情報（電話帳で管理されるデータ）及び通信サービス上の行動履歴や利用者の状態に関する情報

ン・プライバシー・イニシアティブ」（以下「SPI」という。）をとりまとめている。この中では、個人の人格・思想・信条等にもつながり得るプライバシーに関する情報が、非常に詳細なレベルで大量に保存されており、これらがアプリケーションを通じて自動的に取得され外部に送信され得るという、スマートフォンならではの特性を踏まえ、アプリケーションごとにプライバシーポリシー[4]を策定するとともに、プライバシー性が高いと考えられる情報の取得については、個別の情報の取得について同意取得を求めるという基本的アプローチの下、関係事業者等や業界団体が参照すべき指針として、「スマートフォン利用者情報取扱指針」を提示している。

「パーソナルデータの利用・流通に関する研究会」（座長：堀部政男一橋大学名誉教授（当時）。以下「総務省パーソナルデータ研究会」という。）においては、平成25年６月に、パーソナルデータの適正な利用・流通の促進に向けて、パーソナルデータの利活用のルールを明確化するために、パーソナルデータの利活用の枠組み及びその実現のための方向性を提示した報告書をとりまとめている。この中では、まず、パーソナルデータの利活用の枠組み及びその実現に向けて先行的に実施すべき方向性を提示しており、パーソナルデータの利活用の基本理念及び原則[5]を明確化した上で、具体的なルール（準則）を設定・運用していくこと、保護されるパーソナルデータの範囲については「実質的個人識別性」[6]をメルクマールとして判断する

（通信履歴、アプリケーションの利用履歴、位置情報、写真・動画等）

[4] スマートフォンにおける利用者情報を取得しようとするアプリケーション提供者、情報収集モジュール提供者（これらを提供する広告事業者等を含む。）は、個別のアプリケーションや情報収集モジュール等について、以下の①から⑧までの事項について明示するプライバシーポリシー等をあらかじめ作成し、利用者が容易に参照できる場所に掲示またはハイパーリンクを掲載することとされている。

① 情報を取得するアプリケーション提供者等の氏名又は名称、② 取得される情報の項目、③ 取得方法、④ 利用目的の特定・明示、⑤ 通知・公表又は同意取得の方法、利用者関与の方法、⑥ 外部送信・第三者提供・情報収集モジュールの有無、⑦ 問合せ窓口、⑧ プライバシーポリシーの変更を行う場合の手続

[5] パーソナルデータの利活用の基本理念として、以下の事項を明確にすべきであるとしている。

① 個人情報保護を含むパーソナルデータの保護は、主としてプライバシー保護のために行うものである。

② プライバシーの保護は、絶対的な価値ではなく、表現の自由、営業の自由などの他の価値との関係で相対的に判断されるべきものである。

その上で、基本理念を具体化するものとして、次の7項目をパーソナルデータ利活用の原則として提示している。

① 透明性の確保、② 本人の関与の機会の確保、③ 取得の際の経緯（コンテキスト）の尊重、④ 必要最小限の取得、⑤ 適正な手段による取得、⑥ 適切な安全管理措置、⑦ プライバシー・バイ・デザイン

[6] 「実質的個人識別性」とは、総務省パーソナルデータ研究会報告書において提起された概念であり、プライバシーの保護というパーソナルデータの利活用の基本理念を踏まえて実質的に判断される個人識別性のことをいう。その判断の際には、取得等の際に特定の個人が識別されなかったとしても、他のパーソナルデータとあわせて分析されること等により、特定の個人が識別される可能

こと、その取扱いについては、そのプライバシー性の高低による分類や、取得の際の経緯（コンテキスト）に沿った取扱いか否かの区分に応じて適正に行うべきこと、パーソナルデータの適正な利活用の促進のためには、プライバシーを保護するために利用可能な技術（プライバシー強化技術：Privacy Enhancing Technologies（PETs））を最大限に有効活用することが適切であること等を提言している。また、同枠組の本格的な実施のため、我が国における「プライバシー・コミッショナー制度」について検討を行うことが必要であること、企業等が自主的に宣言したポリシー・ルール等への遵守を確保するための制度を整備すべきこと、その他現行の個人情報保護法の課題について、パーソナルデータの利活用の基本理念であるプライバシーの保護の観点から、必要な制度整備について検討を行うことが必要であるとしている。

本検討会は、これらの先行的な検討も踏まえつつ、電気通信事業者が利用者の移動体端末から取得する位置情報について、その適切な利活用により、防災・減災や街づくり、観光地・商店街の活性化等様々な社会的効果が期待されるとともに、利用者に向けた様々な有用なサービスの展開が期待されるなど、パーソナルデータとしてその利活用が高く期待されていることから、通信の秘密や個人情報、プライバシーを適切に保護しつつ、ビジネス利用も含めたその社会的利活用を促進するため、位置情報の取得、利用及び第三者提供時における適切な取扱いについて所要の整理を行うものである。

なお、本検討会は、IT本部パーソナルデータ検討会での議論も踏まえて検討を行ってきたところであり、その検討結果については、 IT本部パーソナルデータ検討会で継続されている個人情報保護法改正に向けた議論における活用が期待されるものである。

性があることについて、十分に配慮する必要があるとしている。（総務省パーソナルデータ研究会報告書 第3章第1節2.（2））

２．電気通信事業者の位置情報の取扱いに係る現状と課題

(1) 位置情報の種類

電気通信事業者が取り扱う位置情報は、大別して①基地局に係る位置情報、②GPS位置情報、③Wi－Fi位置情報の3つがある。

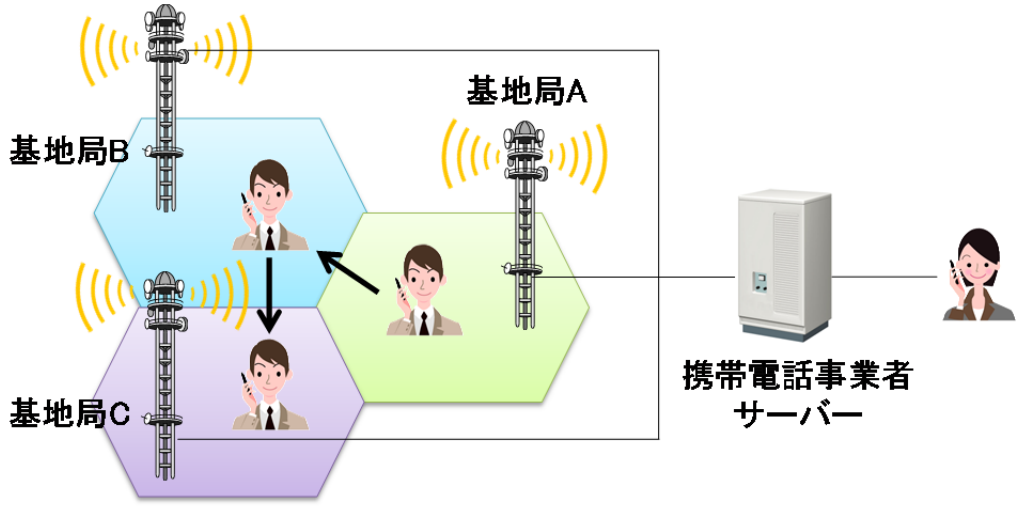
① 基地局に係る位置情報

基地局に係る位置情報は、携帯電話事業者等の電気通信事業者が通話やメール等の通信を成立させる前提として取得している情報のことであり、位置登録情報と個々の通信の際に利用される基地局の位置情報に分けられる。

位置登録情報とは、移動体端末が着信等を行うために、移動体端末がどの基地局のエリア内に所在するかを明らかにするため、移動体端末がエリアを移動するごとに基地局に送られるほか、あるエリア内でも定期的に基地局に送られる情報をいう。具体的には、基地局の識別番号、端末の識別番号、取得日時等によって構成される。実際に通信している際に用いられる情報ではないため、携帯電話事業者等においては個人情報として扱われる。精度は基地局単位であり、概ね数百メートル単位である。

他方、個々の通信の際に利用される基地局情報は、携帯電話事業者等においては通信の秘密として取り扱われ、基地局の識別番号、通信の発信元の識別番号、通信の発信先の識別番号、通信日時等によって構成される。精度は位置登録情報と同じく基地局単位である。

【図表２－１：基地局に係る位置情報】

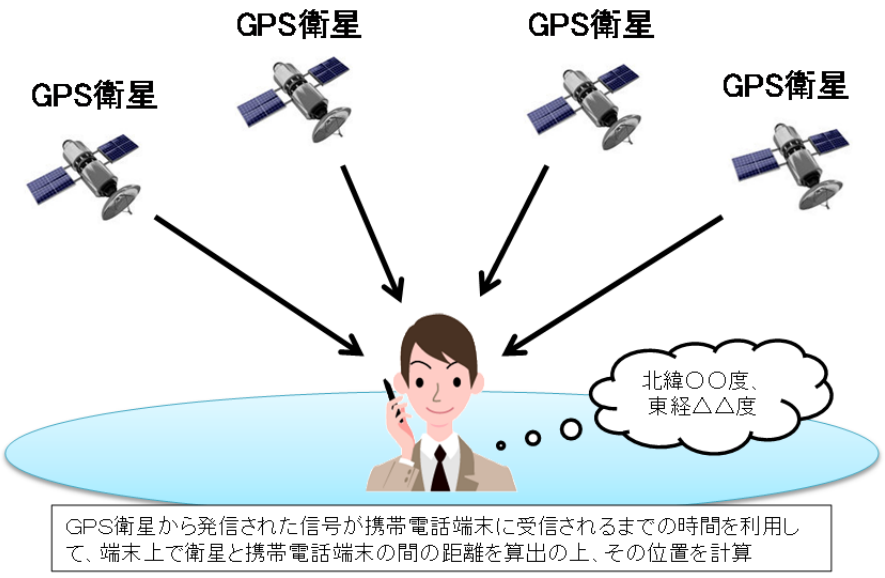


移動体端末が着信等を行うために、移動体端末がどの基地局のエリア内に所在するかを明らかにするため、移動体端末がエリアを移動するごとに情報（基地局の識別番号、端末の識別番号、取得日時等）が基地局に送られる。

② GPS位置情報

GPS位置情報とは、複数のGPS衛星から発信されている電波を携帯電話等の移動体端末が受信して、衛星と移動体端末との距離等から当該移動体端末の詳細な位置を示す位置情報である。緯度経度情報、端末の識別情報、取得日時等で構成される。GPS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上に、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ない。しかし、その精度は緯度経度単位（数メートル～数十メートル単位）であり、基地局に係る位置情報と比べて移動体端末の詳細な位置を示すことが可能である。電気通信事業者においては、GPS位置情報は個人情報として取り扱われることが多いが、より精度の高い位置情報であることから、基地局に係る位置情報と比べ、高いプライバシー性を有するとされている。

【図表2－2：GPS位置情報】



③ Wi－Fi位置情報

Wi－Fi位置情報とは、Wi－Fiのアクセスポイントと移動体端末間の通信を位置情報の測位に応用することによって、利用者によるインターネット接続の前後を問わず取得される位置情報である。例えば、プローブリクエスト（端末が、周囲にある接続可能なアクセスポイントを探すために発信する信号。この信号の中にはMACアドレスが含まれる。）の強度・時間等の情報を用いることで、アクセスポイント[7]のエリア内における端末の相対的位置を推定するものがある。屋内

7 無線端末を相互に接続したり、他のネットワーク（有線LAN等）に接続する無線機器

での測位が難しいGPS位置情報と異なり、屋内外を問わず利用することが可能なWi－Fi位置情報は、精度がアクセスポイント単位（数メートル単位～数十メートル単位）と高いこともあり、大型店舗等で活用される事例が見受けられる。取得される情報としては、アクセスポイントのエリア内の相対的な端末の位置、端末のMACアドレス、取得日時等がある。当該情報が通信の秘密、個人情報あるいはプライバシーのいずれに該当するのか、また当該情報をどのように取り扱うのかについては整理が必要である。

【図表２－３：電気通信事業者が取り扱う位置情報の概要】

	基地局に係る位置情報		GPS位置情報	Wi－Fi位置情報	
	個々の通信の際に利用される基地局の位置情報	位置登録情報		端末利用者とアクセスポイント設置者との間の通信に基づく位置情報	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
概　要		移動体端末が着信等を行うために、移動体端末がどの基地局のエリア内に所在するかを明らかにするため、自動的に取得される位置情報	携帯端末のGPS機能により端末の具体的所在地を示す情報。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。	端末がアクセスポイントと接続し、外部と通信を行う前提として、端末がMACアドレス等をアクセスポイントに送信することにより把握可能な位置情報	端末が特定のアクセスポイントと接続し、外部と通信を行うことにより、把握可能な位置情報
通信の秘密・個人情報への該当性、他の識別情報との結びつき	・電気通信事業者にとって、通信の秘密に該当する。 ・携帯電話事業者の契約者情報と紐づくことから個人情報	・携帯電話事業者の契約者情報と紐づくことから個人情報	・他の個人情報と紐づく場合、個人情報	・他の個人情報と紐づく場合、個人情報 ・MACアドレスと紐づく。	・電気通信事業者にとって、通信の秘密に該当する。 ・他の個人情報と紐づく場合、個人情報 ・MACアドレスと紐づく。
取得の経緯	・通信時に取得される。	・通信の前提として取得される。	・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が、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。
精　度	基地局単位（数百メートル～）		緯度経度情報（数メートル～）	アクセスポイント単位（数メートル～）	
利用者の認識	・通信目的で取得・利用されることについては、予測可能と考えられる。	・携帯電話を使用していなくても、基地局に位置情報を把握されていることについて、利用者の理解が及んでいない可能性がある。	・位置情報を利用することが明らかなサービスを自ら利用する際は、その取得・当該サービスにおける利用について予測可能と考えられる。	・Wi－Fi通信を利用していなくても、アクセスポイントにMACアドレス等が取得されていることについては、利用者の理解が及んでいない。	・通信目的で取得・利用されることについては、予測可能と考えられる。

(2) 日本国内における取扱い

① 法制度等

ア 個人情報の保護に関する法律

個人情報の保護に関する法律（以下「保護法」という。）において、位置情報単独では必ずしも「特定の個人を識別することができる」情報ではないと考えられるが、位置情報が、他の特定の個人を識別できる情報と容易に照合できる場合には、「個人情報」に該当する[8]と考えられる。この場合、個人情報取扱事業者は、情報の取得に際しての利用目的の通知等保護法上の義務の履行が

8 保護法第2条第1項「この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。」

求められる。

なお、保有する個人情報を匿名化（個人情報に加工を施すことにより、その情報が誰に関するものであるか分からないよう（特定の個人を識別できないよう）にすることをいうとされている。）する場合や、匿名化された情報を利用する場合に関しては、匿名化が誰に関する情報であるか分からなくするための加工であり、本人の権利利益の保護につながるものであること、また、本人の権利利益を侵害するおそれが小さく、法律上の「個人情報」にも当たらなくなることから、個人情報を匿名化することや匿名化した情報を利用することを利用目的として特定し、本人に通知又は公表することまで求めるものではない[9]と考えられている。

イ　通信の秘密の保護

通信の秘密は、個人の私生活の自由を保護し、個人生活の安寧を保護する（プライバシー保護）とともに、通信が人間の社会生活にとって必要不可欠なコミュニケーションの手段であることから、憲法上の基本的人権の一つとして憲法第21条第２項において保護されている[10]。これを受けて、電気通信事業法において、罰則をもって、「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。」ものとして、通信の秘密を保護する規定が定められており（電気通信事業法第４条第１項、同第179条）、通信の秘密は厳格に保護されている[11]。

「通信の秘密」の範囲には、個別の通信に係る通信内容のほか、個別の通信に係る通信の日時、場所、通信当事者の氏名、住所・居所、電話番号等の当事者の識別符号等これらの事項を知られることによって通信の意味内容を推知されるような事項全てが含まれる[12]。

---

[9] 個人情報保護法に関するよくある疑問と回答（消費者庁個人情報保護推進室：平成 25 年 12 月 20 日更新））

[10] 日本国憲法
第 21 条
2　検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

[11] 電気通信事業法
（秘密の保護）
第4条　電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。
第 179 条　電気通信事業者の取扱中に係る通信（第 164 条第2項に規定する通信を含む。）の秘密を侵した者は、二年以下の懲役又は百万円以下の罰金に処する。
2　電気通信事業に従事する者が前項の行為をしたときは、三年以下の懲役又は二百万円以下の罰金に処する。
3　前二項の未遂罪は、罰する。

[12] 東京地裁平成 14 年4月 30 日判決は、「「通信の秘密」には、通信の内容のほか、通信当事者の住所・氏名・電話番号、発受信場所、通信の日時・時間・回数なども含まれると解する。」と判示して

ウ　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

電気通信事業者における個人情報等の取扱いについては、総務省において、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（以下「個人情報保護ガイドライン」という。）が定められている。個人情報保護ガイドラインは、保護法の規律を踏まえつつ、個人情報だけではなく通信の秘密の観点からも規定していること、保有する個人情報等の数にかかわらず、全ての電気通信事業を行う者が対象であることといった特色がある。個人情報保護ガイドライン第26条では、電気通信事業者が取り扱う位置情報[13]に関して独立した規定を設けており、同条第１項は、電気通信事業者は、利用者の同意がある場合、裁判官の発付した令状に従う場合その他の違法性阻却事由がある場合を除いては位置情報を他人に提供しないものと規定している。なお、本条において、電気通信事業者が保有する位置情報は、個々の通信に関係する場合は、通信の構成要素であることから通信の秘密として保護されると解されるほか、位置登録情報やGPS位置情報のように通信の秘密に該当しないと解する場合であっても、高いプライバシー性を有することから強く保護が図られているものである。

同条第2項では、電気通信事業者が、位置情報を加入者又はその指示する者に通知するサービスを提供し、又は第三者に提供させる場合[14]には、利用者の権利が不当に侵害されないよう必要な措置[15]を講ずるものと規定している。

また、近年、総務省の検討会[16]等において、位置情報の大規模災害時における安否確認への活用等が指摘されているほか、行方不明者や海難による遭難者の捜索に活用できないかとの意見があったことを踏まえ、本検討会において、電気通信事業者は、警察、海上保安庁又は消防その他これに準ずる機関からの要請により救助を要する者の位置情報の取得を求められた場合には、①その者の生命又は身体に対する重大な危険が切迫しており、かつ、②その者を早期に発見するために当該位置情報を取得することが不可欠であると認

いる。

[13] 個人情報保護ガイドライン第 26 条における「位置情報」とは、移動体端末の所持者の所在を表す場所を示す情報（基地局エリア若しくは位置登録エリア程度又はそれらより狭い範囲を示すもの（基地局に係る位置情報やGPS位置情報等））であって、発信者情報でないものをいう。

[14] GPS位置情報等を用いたサービスのうち、他者位置検索型サービスが主として想定されている。

[15] ①利用者の意思に基づいて位置情報の提供を行うこと、②位置情報の提供について利用者の認識・予見可能性を確保すること、③位置情報について適切な取扱いを行うこと、④第三者と連携の上サービスを提供する場合は、提供に関する契約に係る約款等の記載により利用者のプライバシー保護に配慮をすることなどが考えられる。（個人情報保護ガイドライン解説）

[16] 「大規模災害時における通信確保の在り方に関する検討会」最終とりまとめ（総務省、平成 23 年 12 月 28 日公表）等

められる場合に限り、当該位置情報を取得するものとの検討結果をとりまとめ、平成25年９月に個人情報保護ガイドラインの改正が行われたところである（同条第４項）。

エ　スマートフォン・プライバシー・イニシアティブ[17]

スマートフォンに取得・蓄積される利用者情報のうち、位置情報やウェブ閲覧履歴、アプリケーション利用履歴等については、内容・利用目的等によりプライバシー上の懸念があり、相当程度長期間にわたり時系列に蓄積された場合等、態様によって個人が推定可能になる可能性があるとし、アプリケーション提供者は、アプリケーションが提供するサービスへの利用以外の目的で、個人と結びつきうる形でGPSの位置情報などを取得する場合については、原則として個別の情報を取得することについて同意を取得することとされた。

② 国内におけるサービス事例

ア　モバイル空間統計（NTTドコモ）

NTTドコモは、携帯電話ネットワークの仕組みを利用して作成される人口統計情報である「モバイル空間統計」の実用化を平成25年10月から開始した。モバイル空間統計は、基地局に係る位置情報のうち位置登録情報を利用し、基地局エリアごとの携帯電話台数を利用者の属性別（年齢、性別、住所）に集計することによって、人口の地理的分布を推計するものである。

契約者のプライバシーを保護するため、その作成に当たっては、(ｱ)非識別化処理、(ｲ)集計処理、(ｳ)秘匿処理に大別される加工手順を経る。モバイル空間統計を作成・提供する際に遵守すべき基本的事項を定めた「モバイル空間統計ガイドライン」[18]等によれば、以下のように説明されている。

(ｱ) 非識別化処理：運用データ（電気通信サービスを提供する過程で発生するデータの総称であって、位置データおよび属性データを含むものをいう。）から氏名や電話番号、生年月日などの識別情報を取り除く処理であって、識別情報を構成するデータの削除、数値の丸め込み、不可逆符号への変換などを含むものをいう。

(ｲ) 集計処理：非識別化情報（非識別化処理により得られる情報）から統計的な推計を行うことにより、統計的な「集団に関する情報」を導出する処理であって、人数分布の推計、移動人数の推計、性別・年代別などの属性別の人数構成の推計などを含むものをいう。

---

[17] １．(2)を参照

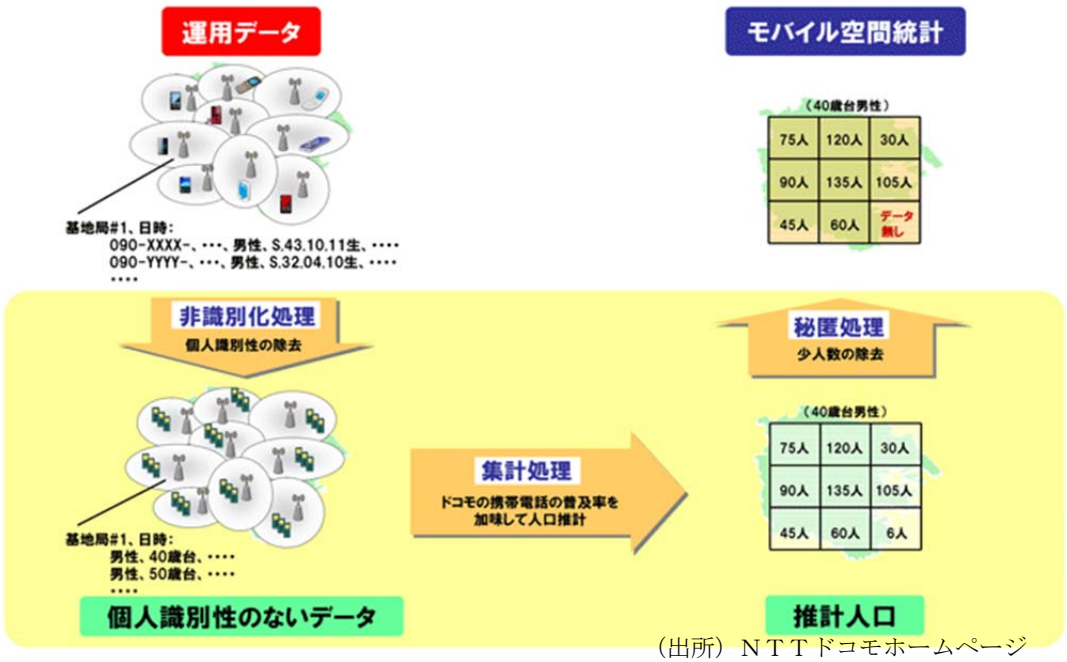
[18] https://www.nttdocomo.co.jp/corporate/disclosure/mobile_spatial_statistics/guideline/index.html

(ウ) 秘匿処理：集計結果に少人数エリアの数値が含まれないようにする処理をいう（統計的に少数であることで個人を推測されやすくなることを防ぐため）。

また、NTTドコモは、上記の「モバイル空間統計ガイドライン」において、モバイル空間統計の作成・提供に関する基本原則のほか、従業員及び業務委託先に対する管理措置や運用データの利用停止手続等について規定している。

「モバイル空間統計」は、公共分野での防災計画やまちづくり、産業分野での商圏調査などさまざまな分野での活用を予定している。

【図表２－４：モバイル空間統計：処理の流れ】



（出所）ＮＴＴドコモホームページ

イ　観光動態調査レポート（KDDI及びコロプラ）

KDDI株式会社（以下「KDDI」という。）と位置情報ゲームのプラットフォームを運営する株式会社コロプラ（以下「コロプラ」という。）は、位置情報により観光客の動きを把握する調査サービスである「観光動態調査レポート」の実証実験を平成25年７月から９月にかけて実施し、同年10月から実用化させている。

本サービスでは、契約者の位置情報（個々の通信の際に利用される基地局情報）の取得が提供の前提となるが、当該位置情報は個々の通信の際に利用される位置情報であり、通信の秘密に該当することから、KDDIは、auスマートフォンユーザーのうちauスマートパス「スタンプカード」の利用者から、当該位置情報を個人が特定できない形式に加工した上で第三者に提供することについての同意の取得を行っている。

KDDIは、誰の情報であるかわからない形式へ加工（非識別化処理）の上、コロプラへ分析を委託する。加工の工程には、(a)生活圏（自宅及び職場等の日常行動範囲）を排除した旅程抽出、(b)位置情報のメッシュ化（500m～数kmメッシュ）（点ではなくエリアで捉えることで個人特定を防止）、(c)個人識別子の秘匿化が含まれる。KDDIから非識別化処理されたデータを取得したコロプラは、授受したデータを統計的に分析し、レポート化し協力自治体へ提供するが、この際、少数サンプルのエリアはデータとして利用しない（集計・秘匿処理）。

本サービスでは、スタンプカードの利用を停止することにより、同意を破棄、レポートへのデータ提供を停止する対応をとっている 。また、本サービス実施に係る「プライバシー保護の仕組み」を自社ホームページ上で公表しており、非識別化処理等について説明を掲載している。

なお、KDDI・コロプラ両社間の契約において、位置情報データの委託業務以外への利用および第三者への開示、ならびに、方法の如何を問わずauスマートフォンユーザーの特定を行わないよう、コロプラには義務付けられている。

観光に特化した本調査を地方自治体等に提供することにより、各自治体の観光における課題発掘や、ターゲットを絞った誘客施策の立案など、地域振興に活用するとしている。

【図表2－5：観光動態調査レポート：処理の流れ】

① 位置情報等利用の同意取得
位置情報データの利用、並びに位置情報データを個人が特定できない形式に加工した上で、第三者に提供することに同意を頂いた au スマートフォンユーザー※の情報を取得します。
※「スタンプカード」 ご利用のお客様
② データの非識別化処理と分析の委託
KDDI は、分析に必要な位置情報データのみを抽出し、誰の情報であるかわからない形式へ加工(非識別化処理)の上、コロプラへ分析・レポート作成を委託します。
③ 集計・秘匿処理後のレポート提供
秘匿処理を加えた上でレポートを完成させ、地方自治体、観光協会等へレポートを提供します。
（出所）KDDI ホームページ

ウ Wi－Fi実証実験システム（G空間EXPOナビ）

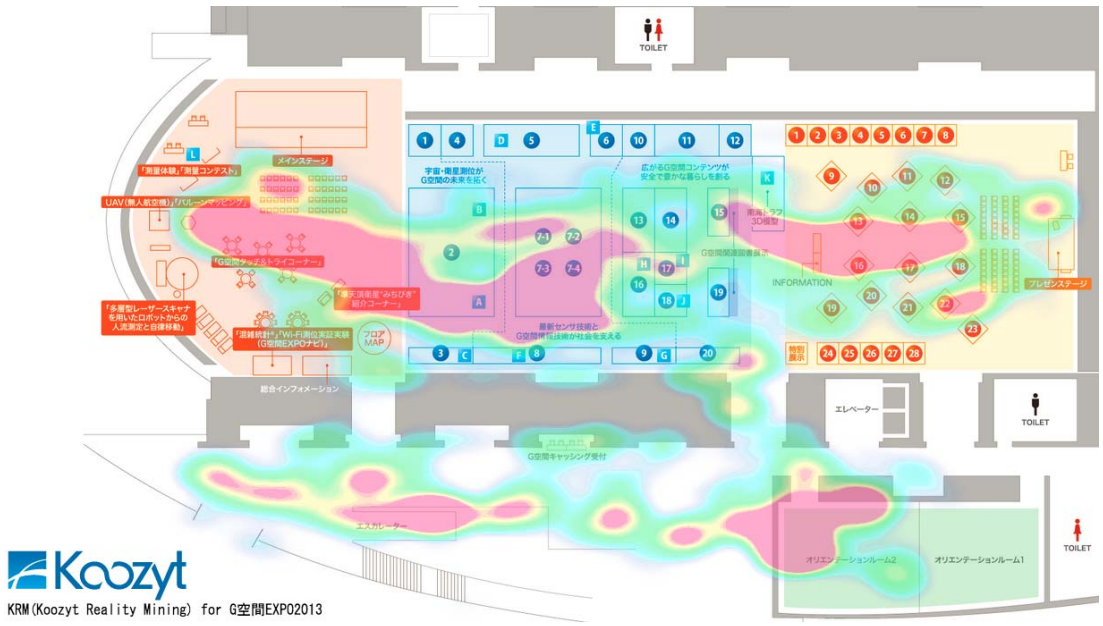
平成25年11月に開催された「G空間EXPO2013[19]」では、Wi－Fi位置情報を

[19] 主催：G空間EXPO2013 運営協議会（構成員：公益社団法人日本測量協会、一般財団法人衛星測位利用推進センター、内閣官房、内閣府宇宙戦略室、国土交通省国土地理院等）

活用したサービスとして「G空間EXPOナビ」が実証実験として行われた。これは、来場者にandroidアプリ「G空間EXPOナビ」をインストールしてもらうことで、Wi-Fi測位により会場内のフロアマップから、現在地を確認できるほか、出展ブースの内容の閲覧や、ステージプログラムの開催時間などを案内するものである。また、当該アプリ利用者の動きをヒートマップで表示することで、館内の混雑状況を可視化するとともに、行動履歴や滞在時間等を集計化することも可能である[20]。

一方で、実証実験では、アプリを利用していない来場者のプローブリクエスト等も取得し、Wi－Fi位置情報を収集してしまう性質上、G空間EXPOナビの利用に関する注意をウェブサイト及びポスターで周知した。具体的には、Wi－Fi位置情報の取得を望まない来場者には会場内で通信機器のWi－Fi機能をオフにするよう周知した上で、サービスにおいて、MACアドレス及び位置情報を収集すること、実際の製品を用いてその動作、分析結果などをリアルタイムに展示会場で確認するために当該情報を取得すること、取得されたデータは個人を特定できない形で保存し分析終了後データは抹消すること、取得した情報は特定の第三者に提供すること等が明示された。

【図表2－6：G空間EXPOヒートマップ】



[20] シスコシステムズ合同会社が会場内のWi－Fi端末の位置情報をクウジット株式会社のサーバーに通知し、同社が端末の位置情報を取得するためのAPI及びヒートマップ構築のためのAPIを提供している。

③ 電気通信事業者協会における検討（電気通信事業者から提示された課題）

携帯電話事業者の保有する運用データ等[21]の利活用については、総務省情報通信審議会において議論が行われ、その重要性が指摘された。その結果、審議会の答申（「知識情報社会の実現に向けた情報通信政策の在り方」（平成24年7月25日答申））により、運用データ等については、個人情報等に配慮しつつ活用するための検討の場の設置や街づくり・防災等への利活用のためのガイドライン策定支援が提言された。

これを受けて、携帯電話事業者が保有する運用データ等の活用の在り方、上記情報を活用するに当たって留意するべき事項等について関係する事業者間で検討し、その結果を取りまとめ、発表することを目的として、平成25年2月、一般社団法人電気通信事業者協会（TCA）を事務局とする「携帯電話事業者の運用データ等の適正な有効利用に関する検討会」（座長：堀部政男　一橋大学名誉教授（当時））が設置された。同年6月まで5回の会合を開催した結果、運用データ等の利活用に当たり、今後の検討課題として以下の課題が挙げられている。

ア CDR[22]の利活用

CDRは、通信の秘密等に配慮して慎重に取り扱うことが必要であるが、諸外国における活用の動向にも配意しつつ、その利活用について、技術進化に伴う通信設備の変化、プライバシー保護技術の進歩等にも配意しつつ的確に対応していくことも重要である。例えば、通信の秘密に属する情報から個々の通信との関連性を除去する行為の可能性、非識別化を行うことの考え方や、サービス内容に応じた利用者の同意の取得方法等について、今後課題を明らかにするとともに検討を深めることも考えられる。

イ Wi-Fi位置情報の利活用

近年、無線LANを位置情報の取得手段として活用することで、GPSでは把握が困難な閉鎖空間内における位置情報として活用する取組等が進められつ

---

[21] TCAの検討会において、運用データとは、電気通信サービスを提供する過程で発生するデータの総称であり、電気通信事業者が電気通信サービスを提供する上で必要となる各種データをいうとされている。具体的には、契約者の属性情報（氏名、年齢、性別、住所等）、位置情報（位置登録情報、Wi－Fi位置情報、GPS位置情報等）、通信履歴（利用者が電気通信を利用した日時、当該通信の相手方その他の利用者の通信に係る情報であって通信内容以外のもの）。なお、GPS位置情報等は、電気通信サービスを提供する過程で通常発生・取得しないデータであるが、利用者の有効な同意を取得する等適切な配慮を行うことにより、運用データ以外の情報を新たに取得して利活用することも可能であるため、同検討会の検討対象となっている。

[22] Call Detail Record. TCAの検討会においては、通信履歴に類似する情報として、米国等を中心に用いられているものとされている。

つある。Wi-Fi位置情報の取扱いは、携帯電話基地局に係る位置登録情報の例などにおいてこれまで整理されてきた考え方が適用されるものも多いと考えられるが、無線LANによる位置情報取得の特性（一般に基地局に係る位置情報より位置精度が高い、端末の識別番号としてMACアドレスを用いている　等）も踏まえ、検討を行うことも考えられる。

ウ　単独では個人識別性を有しない運用データ等の利活用

運用データ等は、それ単独では個人識別性を有しない情報であっても、相当程度長期間にわたり時系列的に蓄積された場合等には、個人が推定可能となる可能性やプライバシー侵害が成立する可能性もある。他方、このようなデータを活用することで、例えば、地点間を移動する人数を把握することが可能になるなど、社会的に有益な利活用の範囲が広がることが想定される。これらに鑑み、それ単独では個人を識別することができない運用データ等について、例えば、当該データへのアクセスを厳格にし、他の情報との照合を禁止した上で保存・蓄積する等の運用管理を行うことで、個人識別性を排除し、上記のような統計的利活用を可能にすることも考えられる。この点について、今後、具体的な事例や他の検討状況も踏まえつつ、対応していくことが求められる。

エ　加工処理段階における運用データ等の第三者提供

今後、運用データ等の利活用を進めるに当たり、提供側と利活用側との間のニーズのマッチングについて仲介者の活用が考えられるが、そのような場合、加工処理段階における運用データ等の仲介者（第三者）への提供についてどのように考えるか、という論点がある。例えば、電気通信事業者から仲介者、研究機関、ベンチャー企業等の第三者に対して運用データ等の加工処理を委託する場合に、適確な管理を求める「一定の条件」を設定する、といったことも考えられるところ。この点について、今後、具体的な事例も踏まえつつ、検討を深めていくことが考えられる。

(3) 諸外国における取扱い

① 法制度等

ア　米国

米国においては、個人情報・プライバシーに関する分野横断的な法律は存在せず、分野毎の個別法と自主規制が基本となっている。電気通信分野においては、通信法（Communications Act）第 222 条で顧客情報のプライバシーを規定しており、電気通信事業者は、電気通信サービス加入者の通信パターン、請求記

録等の消費者固有のネットワーク情報（CPNI[23]）に関して、集計顧客情報（集計データで、個人顧客の身元及び特徴が除去されているもの）については、通信目的外での利用や公開を許容されている。

自主規制としては、携帯電話に代表される移動体通信や無線インターネットなど無線通信に関する国際的な業界団体であるCTIA[24]が、GPS位置情報等を利用した位置情報サービスに関するベスト･プラクティス・ガイドライン[25]を平成 22 年３月に設けている。その二大原則として、位置情報サービス提供者は、位置情報がどのように利用・開示・保護されるかについてユーザーに通知し、その利用・開示について同意を求めることとされている。なお、集計データ及び匿名データはガイドラインの対象外となっている。

加えて、連邦取引委員会（FTC[26]）はモバイル端末上の利用者情報の取扱いについて、スタッフレポートとして「モバイルプライバシーディスクロージャーズ：透明性の確保による信頼の構築」[27]を平成 25 年２月に公表しており、この中では、OS事業者、アプリ開発者双方に対し、位置情報についてはセンシティブ情報として、取得前に消費者に通知し、明白な同意をとることが提言されている。

また、近時Wi－Fi等を利用した位置情報サービスのプライバシーについて議論がなされており、 平成 26 年２月 19 日には、FTCにおいて、モバイル端末の位置情報の活用や消費者プライバシーへの影響等について把握するため、「Spring Privacy Series: Mobile Device Tracking」と題するセミナーが開催された[28]。

米国のシンクタンクであるFPF[29]は、平成 26 年２月、位置分析を行う企業が提供するサービスに対する自主規制の枠組みとして、「移動端末の位置情報分析に関する行動規範」[30]を作成。同行動規範に賛同する位置分析企業とともに、M

---

23 Customer Proprietary Network Information

24 Cellular Telecommunication and Internet Association

25 Best Practices and Guidelines for Location Based Services
http://www.ctia.org/policy-initiatives/voluntary-guidelines/best-practices-and-guidelines-for-location-based-services

26 Federal Trade Commission

27 Mobile Privacy Disclosures: Building Trust Through Transparency: A Federal Trade Commission Staff Report

28 セミナーでは、位置情報サービス提供会社、データ分析会社、市民系団体等によるパネル討議が行われ、消費者の信頼は重要であるが、不特定のデータを追跡することで作成されたヒートマップの作成等、一定の場合には消費者への事前通知が不要な場合も存在する。GPS や Wi-Fi、Bluetooth 等の位置追跡技術により、店舗付近にいる利用者端末へのクーポン配信等が可能になる等の意見の一方で、利用者に気づかれない情報収集の是非、オプトインまたはオプトアウトの選択肢、匿名による情報管理、情報の保存期間といった懸念が存在しており、行動追跡について通知した上で、客がこれを許可するか否か選択できるようにすべき等の意見が出されている。

29 Future of Privacy Forum

30 Mobile Location Analytics Code of Conduct

ACアドレスにより企業に行動を追跡されたくない消費者に一括でオプトアウトさせるウェブサイト（www.smartstoreprivacy.org）を立ち上げている。

行動規範の中では、あるエリアでの位置情報の収集および利用について、エリア内の目立つ場所に掲載し、ウェブサイト上に取得する情報や提供するサービス等について記載した詳細なプライバシーの通知を提供すること（取得される情報が、①個別の端末・利用者に紐付かない、または②直ちに集計され個別の情報が保持されない場合は不要）、消費者の同意がない場合、取得したMACアドレスは即座に非特定化（De-personalized）[31]または非識別化（De-identified）[32]すること、等を求めている。

イ EU

EUにおいては、欧州データ保護指令（Directive 95/46/EC）第 29 条に基づく作業部会（以下「作業部会」という。）が、平成 23 年5月に、スマートフォンやタブレットなどのスマートモバイルデバイス上での位置情報サービスの使用についての意見を公表している[33]。この意見の中では同指令が、基地局に係る位置情報や、GPS位置情報、Wi-Fi 位置情報に対して、適用されることを明確にしている。

なお、同指令前文第 26 条において、データ主体がもはや識別できない(the data subject is no longer identifiable）ようにする方法で匿名化されたデータについては、データ保護の原則は適用すべきでないとされている。

電気通信分野については、電子通信プライバシー指令（2002/58/EC）において、トラフィックデータ[34]について、通信に不必要になった場合に、消去又は利用者を識別できないような状態にしなければならないと規定されており（第6条）、それを超えるマーケティング目的の利用や付加価値サービスの提供については、利用者の同意が必要とされている。位置情報（トラフィックデータを除く。）については、付加価値サービスの提供について利用者の同意を得た場合のほか、当

---

[31] 非特定情報（De-personalized Data）は、①個人への紐付けを不可能とする手段を講じること。（例） MACアドレスのハッシュ化や個人識別情報の削除 ②非特定化された状態での情報の維持を公的に約束すること。 ③提供先がデータを個人識別に利用することを契約上禁止すること。 と定義されている。

[32] 非識別情報（De-identified Data）は、①非識別化を確保する合理的な手段を講じること。（例）集合情報、データへのノイズ付加、統計的サンプリング ②データの再識別化を試みないことを公的に約束すること。③提供先がデータを再識別化することを契約上禁止すること。 と定義されている。

[33] ARTICLE 29 Data Protection Working Party: Opinion 13/2011 on Geolocation services on smart mobile devices

[34] 電子通信ネットワーク上における通信の伝達や、それに係る通信費用の請求書の作成のために処理されるデータを意味する（第2条（b））。

該データが匿名化された場合においても処理が可能とされている。利用者の同意を取得する前には、処理される位置情報の種類、処理の目的及び期間、第三者に提供されるか否かについて通知しなければならない。また、利用者は同意をいつでも取り消すことができることとされている（第9条）。

また、匿名化に関連して、作業部会が、平成 26 年4月、匿名化技術に関する意見を公表している[35]。意見の中では、具体的な匿名化技術についてそれぞれの長所と短所を示した上、個別の事例に応じて匿名化技術の選択や組合せを行う必要があること、仮名化は匿名化の手法ではないこと等について言及している。

【図表2－7：匿名化技術の長所と短所の比較】

	個人特定のリスクは残っているか	他の情報と照合されるリスクは残っているか	属性推定のリスクは残っているか
仮名化（Pseudonymisation）	○	○	○
ノイズ付加（Noise addition）	○	△	△
置き換え（Substitution）	○	○	△
集合化（Aggregation）／k-匿名化（K-anonymity）	×	○	○
l-多様性（L-diversity）	×	○	△
差分プライバシー（Differential privacy）	△	△	△
ハッシュ化（Hashing）／トークン化（Tokenization）	○	○	△

○：リスクあり　×：リスクなし　△：おそらくリスクなし

「Opinion 05/2014 on Anonymisation Techniques」を基に作成

ウ　英国

英国においては、データ保護法（Data Protection Act 1998）の下、識別できる生存する個人に関する位置情報は、「個人データ」に該当すると考えられている。

電気通信分野については、プライバシーと電子通信に関する規制（Privacy and Electronic Communications Regulations 2003）において、位置情報（トラフィックデータを除く。）については、付加価値サービスの提供について利用者の同意を得

[35] ARTICLE 29 Data Protection Working Party: Opinion 05/2014 on Anonymisation Techniques

た場合や、当該データが匿名化された場合に限って処理が可能とされており（第14条(2)）、電子通信プライバシー指令と同旨が定められている。

基地局に係る位置情報、GPS位置情報、Wi－Fi位置情報のいずれも、位置情報として扱われ、個人データに該当しうると考えられている。

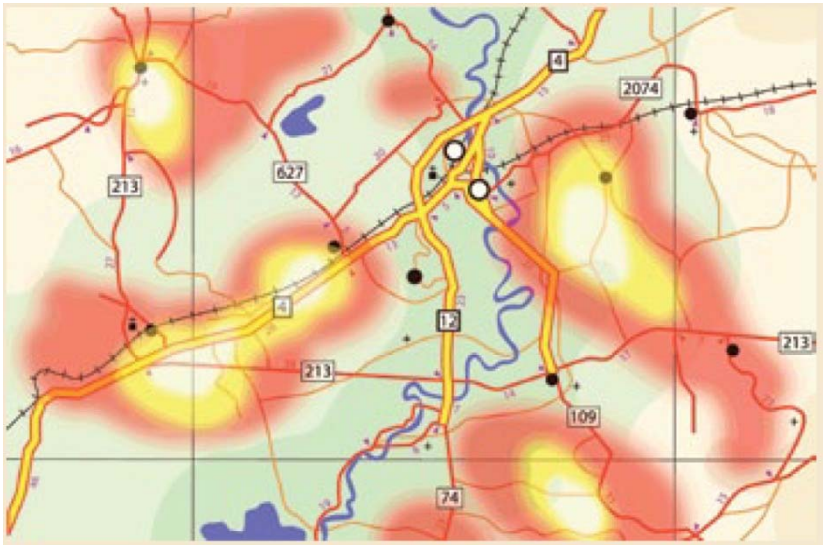
また、英国情報コミッショナー（ICO[36]）は、平成24年11月、ヨーロッパのデータ保護当局として初めて匿名化に関するガイドライン[37]を示している。匿名化は個人のプライバシーを保護するとともに、データ保護法が推進する「プライバシーバイデザイン」の実践例として取り上げられており、その中には「個人データと空間的情報」として、位置情報について言及する章が設けられている。

同ガイドラインでは、データ保護法には、空間的情報（GPSデータ等）の取扱いに関するルールは定められていないが、一部の状況によっては、これらの情報は個人データに相当するとされている。空間的情報のために採用すべき（匿名化の）方法は、保有するデータセットの規模によっても異なるが、一部のケースでは、識別化のリスクを軽減するために、空間的情報を処理して、一定の情報を除去または「曖昧に」する必要があるとされている。 また、空間的情報を公表する際にプライバシーリスクを軽減する原則としては、地図のエリアを拡大して、より多くの土地建物と居住者をカバーすること、公表の頻度または対象期間を縮小して、より多くの出来事を取り上げることによって、最近のケースの特定がより困難になり、その出来事の発生日時等の追加のデータが明らかにならないようにすること、特定の場所または人についての詳細な情報の推測を可能にすることなく、ヒートマップなど概況を示すフォーマットを使用すること、住居レベルに関する空間的情報の公表を避けること等が挙げられている。

[36] Information Commissioner's Office

[37] Anonymisation: managing data protection risk code of practice

【図表２－８：犯罪地図作成のためのヒートマッピング（色分け地図作成）手法】

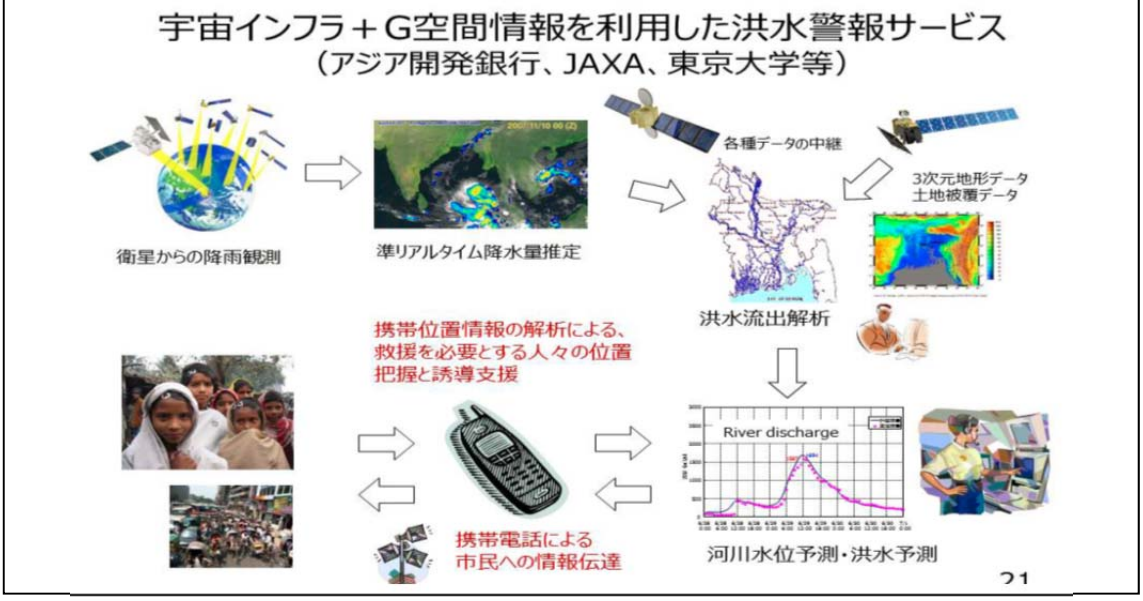


出典：ICO「Anonymisation: managing data protection risk code of practice」

② 公的利用

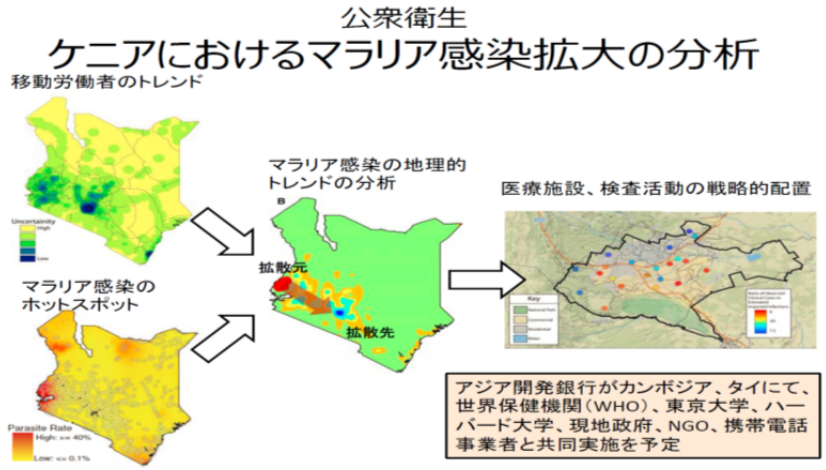
バングラデシュにおいて、アジア開発銀行、JAXA、東京大学等の共同プロジェクトとして、宇宙インフラや G 空間情報を利用した洪水警報サービスが提供されている。これは、衛星からの降雨観測情報等に基づく河川水位予測や洪水予測と、携帯電話の位置情報の解析を組み合わせ、救援を要する人々の位置の把握と誘導支援を行うものである。

【図表２－９：宇宙インフラ＋G空間情報を活用した洪水警報サービス】



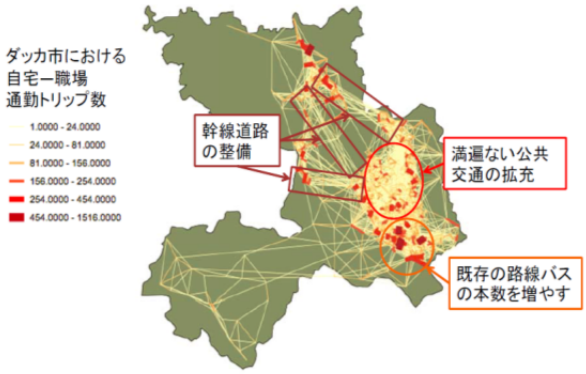
また、公衆衛生対策への活用としては、ハーバード大学等がケニアにおいて、マラリア感染拡大の分析を行った例がある。同様のプロジェクトがカンボジアやタイにおいても、アジア開発銀行により世界保健機関、ハーバード大学、東京大学等と共同で実施が予定されている。

【図表2－10：ケニアにおけるマラリア感染拡大の分析】



バングラデシュの首都ダッカにおいては、携帯電話の位置情報を基にした人の動きの分析を都市交通計画に利用する動きも見られる。

【図表2－11：都市交通計画】



③ ビジネス利用

Verizon Wireless（米国）は、平成 24 年 10 月、企業向けのビジネスインテリジェンスおよびマーケットリサーチのビジネスである「Precision Market Insights」を報道発表した。Precision Market Insights は、携帯電話ネットワークから取得できる利用者の属性別の位置情報とアクセスログの匿名・統計データを活用して、屋外広告、スポーツ競技場、ショッピングモールの顧客特性分析などを、毎週更新されるオンラインポータルで提供する。将来は、モバイル広告にもビジネスを拡大する予定としている。

Telefonica（スペイン）のグローバルビジネス部門であるTelefonica Digitalは、平成24年10月、位置情報を含む自社のビッグデータを活用するサービスである「Smart Steps」を報道発表した。Smart Stepsは、イギリス、ブラジル、ドイツの企業や公共団体に対して、調査地点の訪問者数の計測、比較、影響因子等を分析するサービスである。

【図表2－12：Telefonica- Smart Steps】

Cellint（イスラエル）は、携帯電話ネットワークのプローブデータを利用して、渋滞ポイントや道路の平均移動速度などの道路交通情報をリアルタイムに提供するサービス「Traffic Sense」を平成21年から開始している。イスラエルの他、米国やスウェーデンなどでもサービスを提供している。情報の作成に当たり、プローブデータの他にGPS情報や道路モニター情報を併用している。

④ 問題事例

位置情報を活用したサービスが増える一方で、プライバシーとの関係からその活用が問題視される事例も見られる。

米国では、平成23年11月、ショッピングモールで行われた顧客の追跡実験が、上院議員の申入れによって中止となった。この実験に技術提供を行った企業は、実験で使用されたのは、携帯電話が基地局との通信に使うTMSI（Temporary Mobile Subscriber Identifier）というIDで、このIDは携帯電話端末が基地局のエリアから出れば自動的に変更される永続性のないIDであること、IDは暗号化、匿名化されて使用されること、Bluetoothやwi－Fiにおいても同種の情報（ID）を端末に付与し、事業者に受信させており、既に利用されている技術であること等を主張したが、デジタル社会における市民の自由の保護を標榜する非営利団体であるEFF[38]からは、他の手段で特定の時間に店舗に誰がいたかの情報が入手できれば、その顧客が店舗で何を購入したかを特定できるとの意見が出されている。

[38] Electronic Frontier Foundation

また、英国においては、平成 25 年８月、ロンドン市街で行われた広告表示パネル付のゴミ箱「bin」の実験が、自治体によるICOへの告発で中止となった。「bin」には、Wi－Fi機能がONになっている通行人の端末からMACアドレスを取得し、ターゲティング広告を表示する機能があった。

(4)　本検討会における論点

以上の背景・現状を踏まえ、本検討会においては、次のとおり論点を整理し、検討を行った。

論点１　位置情報の取扱いの在り方について

電気通信事業者が取り扱う位置情報については、これまでもそのプライバシー性の高さから、他の個人情報と比べて高い保護が求められてきたところであり、これを踏まえつつ、適切にプライバシー等を保護するとともにその利活用を促進するため、利用者からの同意取得や利用者に対する説明・表示の在り方について、検討を行った。

論点２　位置情報の加工（いわゆる匿名化）について

これまで特定の個人が識別できないように加工（いわゆる匿名化）した個人情報は、もはや個人情報に当たらず、利用者の同意なく利用・第三者提供が可能であるとされてきたが、どの水準まで加工すればよいかといった点については明確でなかった。また、個人情報を匿名化した上で利活用していても、利用者にとってその取扱いが不透明であることが、利用者に不安を与える事案も発生している。

このため、電気通信事業者が取り扱う位置情報について、匿名化した上で利活用するために、加工に当たってはどのような方法が考えられるか。また、その加工の程度に応じてどのような取扱いが考えられるか。匿名化した上で位置情報を利活用する場合であっても適切な取扱いとして何が考えられるかについて、検討を行った。

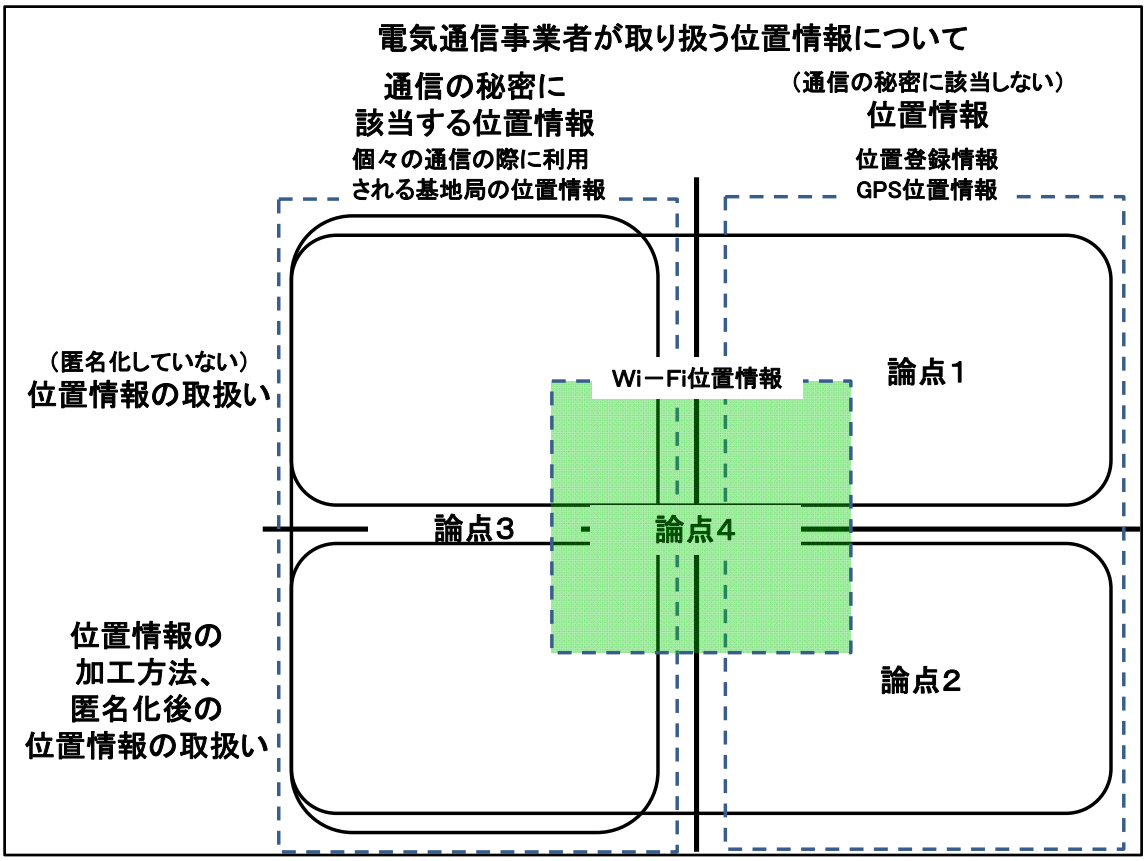
論点３　通信の秘密に該当する位置情報について

通信の秘密に該当する位置情報については、基本的に利用者の有効な同意がない限り、これを利用することは通信の秘密の侵害に当たる。しかし、通信の秘密に該当する位置情報についても、これをビッグデータとして利活用していくことへの期待が高まっているところである。このため、通信の秘密に該当する位置情報について、加工した上で利用・第三者提供することが、電気通信事業法上の通信の秘密の侵害に該当し得るかどうか。また、該当し得るとして、この場合の有効な同意の取得の在り方について、検討を行った。

論点４　Wi－Fi位置情報について

Wi－Fi位置情報については、当該情報が通信の秘密、個人情報に該当するのか、あるいはプライバシーの観点から保護すべきものであるのか、また当該情報をどのように取り扱うのかについて、整理が必要である。他方で、近年、Wi－Fi等の無線LANを位置情報の取得手段として活用することで、GPSでは把握が困難な閉鎖空間内における位置情報を取得・活用する取組等が進められつつある。このため、利活用が期待されているWi-Fi位置情報について、基地局に係る位置情報やGPS位置情報についてこれまで整理してきた考え方を踏まえつつ、その性質と取扱いについて、検討を行った。

【図表２－13：各論点の関係について】



３．位置情報の取扱いの在り方について[39]

(1)　位置情報のプライバシー性

電気通信事業者が取り扱う位置情報については、これまで保護法における取扱いよりも高いレベルの保護が求められてきた。具体的には、個人情報保護ガイドライン第26条においては、電気通信事業者が取り扱う位置情報について、利用者の同意又は違法性阻却事由がない限り第三者提供ができない旨等が規定されている。これは、基地局に係る位置情報については、個々の通信に関係する場合は、通信の構成要素であるから通信の秘密として保護されること、位置登録情報については、「ある人がどこに所在するかということはプライバシーの中でも特に保護の必要性が高い上に、通信とも密接に関係する事項であるから、通信の秘密に準じて強く保護することが適当」であること、また、GPS位置情報については、「基地局に係る位置情報と比べ、より詳細に所在地を示す位置情報であるところ、その場所に所在することそれ自体によって、個人の趣味嗜好、さらには思想信条まで容易に推測できる場合がある。また、一定期間追跡すれば、個人の行動状況まで詳細に把握することも可能となる」ことから、「基地局に係る位置情報と比べ、高いプライバシー性を有する」こと[40]による。

位置情報について、他の個人情報やプライバシーと比べて高いレベルの保護を求めているのは、他の先行的検討でも同様である。

SPIにおいては、位置情報といった利用者の行動履歴や状態に関する情報について、内容・利用目的等によりプライバシー上の懸念があり、相当程度長期間にわたり時系列に蓄積された場合等、態様によって個人が推定可能になる可能性があるとし、アプリケーション提供者は、アプリケーションが提供するサービスへの利用以外の目的で、個人と結びつきうる形でGPSの位置情報などを取得する場合については、原則として個別の情報を取得することについて同意を取得することとされた[41]。

総務省パーソナルデータ研究会報告書においては、継続的に収集される位置情報等について、仮に氏名等の他の実質的個人識別性の要件を満たす情報と連結しない形で取得・利用される場合であったとしても、特定の個人を識別することができるようになる蓋然性が高く、プライバシーの保護という基本理念を踏まえて判断すると、実質的個人識別性の要件を満たし、保護されるパーソナルデータの

---

[39] 3. 及び4. で整理する位置情報の取扱いは、一般的な位置情報に関するものであり、通信の秘密に該当する位置情報については、これらに加え、通信の秘密に保護の規律に従った対応が求められることとなることに留意する必要がある。なお、後記5. では、通信の秘密に該当する位置情報の取扱いのうち、特に加工（いわゆる匿名化）した上で利用・第三者提供することと通信の秘密との関係について検討を行っている。

[40] 個人情報保護ガイドライン解説　第 26 条第4項の解説参照

[41] SPI　第4章1、第5章1各論①(2)

範囲に含まれるとした上で、スマートフォンやタブレット端末など移動体端末に蓄積されるGPSなどの位置情報といったパーソナルデータについては、慎重な取扱いが求められるパーソナルデータとして分類している[42]。

このように位置情報は、ある人がいつどこに所在するかを示す情報であることから高いプライバシー性を有し、精度が詳細であるほど、また、一定期間連続するほど、そのプライバシー性が高まるという特徴を有している。

(2) 位置情報の取得等に関する同意取得等

① 個別かつ明確な同意の原則

このように、位置情報はその高いプライバシー性から、これまでの整理においても、他の個人情報やプライバシーより高い保護を求められてきており、これを踏まえた取扱いが必要である。

まず、電気通信事業者は、原則として、その提供するサービスごとに、位置情報の取得・利用・第三者提供について、利用者から同意を取得することが適当であると考えられる。

利用者の同意があったと言えるためには、利用者が位置情報の取扱いについて同意しているということを最低限理解できる状況であることが必要である。他方で、契約約款等は、利用者側に交渉の余地がなく、読まれない可能性がある点で、同意取得としての実質が弱いと考えられ、単に契約約款等に記述をしたとしても、利用者が位置情報の取扱いについて合理的に予測できない状況では、同意が有効と評価できない場合がある[43]。

位置情報の高いプライバシー性も踏まえれば、電気通信事業者においては、位置情報の取得・利用・第三者提供について個別かつ明確に[44]利用者の同意を得ることが必要である。

同意の取得は、当該サービスにおいて、位置情報を最初に取得する前に行うべきである。また、取得した位置情報について、その取扱いを変更する場合など、当初同意を得た範囲外で利用、第三者提供する場合には、改めて、その利用、

---

42 総務省パーソナルデータ研究会報告書 第3章第1節2.(2)、同節3.(2)

43 法務省法制審議会民法(債権関係)部会において進められている民法(債権法)改正の議論の中では、約款規制が検討されている。検討中の約款規制の1つとして、「不意打ち条項」に関するルールがある。これによれば、「約款に含まれている契約条項であって，他の契約条項の内容，約款使用者の説明，相手方の知識及び経験その他の当該契約に関する一切の事情に照らし，相手方が約款に含まれていることを合理的に予測することができないもの」は、契約内容にならないこととなる。(民法(債権関係)の改正に関する要綱案の取りまとめに向けた検討(11)参照)

44 「個別かつ明確な同意」とは、位置情報の取扱いについての同意であることを本人が認識した上で画面上でのクリックなどにより行う「個別」の同意であり、かつ、画面上でのクリックや文書による同意など外部的に同意の事実が「明確」な同意を意味している。必ずしも位置情報の取得の「都度」同意を取得することまでを求めるものではない。

第三者提供の前に同意取得することが必要である[45]。

② 例外としての包括的な同意

①のとおり、位置情報の高いプライバシー性も踏まえれば、原則として、位置情報の取扱いについては個別かつ明確に同意を取得することが必要であると考えられるが、例外として、利用者が、そのコンテキストから位置情報を取得・利用されることが予測できる場合には、契約約款等で記述することで包括的に同意を取得することも許容されうると考えられる[46]。これは、例えば位置情報を利用することが明らかなサービス（地図ナビゲーションサービス等）について、そのサービスに必要な範囲内で取得・利用するような場合である。

ただし、コンテキストから予測できる取得・利用の範囲は、限定的に捉えるべきであり、例えば、地図ナビゲーションサービスであれば、取得した位置情報を地図上に位置を表示する機能以外で利用することは、コンテキストの範囲外というべきである。

また、包括的な同意が許容されうる場合であっても、個別かつ明確な同意を取得することは望ましい取組みである。

③ 通信を成立させるために必要不可欠な位置情報の取得・利用

通信を成立させるために必要不可欠な位置情報を取得し、通信のために利用することは、利用者の同意を取得しなくても許容されると考えられる[47]。

(3) 利用者に対する説明・表示

① 利用者に対し説明・表示すべき事項

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。具体的な説明事項としては、以下の項目が挙げられる[48]。

---

[45] 現行保護法上も、当初の利用目的を超えて情報を利用する場合は、改めて本人の同意が必要である（保護法第16条第1項）。なお、保護法上、第三者提供のために、利用者の同意を得ることが原則となっているが（保護法第23条第1項）、位置情報については、情報の取得時の同意取得を原則としており、情報取得時に、第三者提供も含めた同意を取得することが通常と考えられる。

[46] ただし、通信の秘密に該当する位置情報については、通信の秘密の保護の規律に従った対応が求められる。

[47] このような取扱いは、位置情報の高いプライバシー性を踏まえ、正当業務行為あるいはそれと同等に評価できることから許容されるものである 。また、このような取扱いは、明らかにプライバシー上のリスクが低いと考えられ、このような観点からも許容されるものと考えられる。

[48] なお、経済産業省においても、パーソナルデータを利活用したビジネスを行う上で、特に、パー

ア　取得者（位置情報の利用者）
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）
ウ　精度、取得頻度、追跡期間
エ　利用目的
オ　第三者提供の有無及びその提供先
カ　保存期間
キ　位置情報に紐付けて利用される他の利用者情報
ク　利用者関与の仕組み　　等

② 記載時の注意事項

ア　精度、取得頻度、追跡期間

位置情報は、その精度や、継続して取得され軌跡として把握されるか否かによってプライバシー性の高低が異なってくる。詳細な位置情報を取得する場合や一定期間継続して取得することで軌跡として把握する場合には、その精度や取得頻度、追跡期間といった位置情報のプライバシー性を高める要素について説明を行うことが望ましい。

イ　利用目的

位置情報の利用目的については、できる限り具体的に記載されていることが望ましい。とりわけ、利用者が容易に予測できないような位置情報の利用目的については、丁寧に説明することが必要である。

ウ 第三者提供の有無及びその提供先

位置情報を第三者に提供する場合、その提供先についてはできる限り具体的に記載されていることが望ましい。

ソナルデータを取得する際に取り組むべき、消費者への情報提供・説明のあり方を示す「評価基準」を取りまとめている。（平成26年3月26日付報道発表）

この中では、パーソナルデータを利活用して提供されるサービスについて、事業者がパーソナルデータを取得し利用する際に行う消費者に対する情報提供や説明の内容として、以下の7項目が必要かつ重要な記載事項として挙げられている。

1.提供するサービスの概要
2.取得するパーソナルデータと取得の方法
3.パーソナルデータの利用目的
4.パーソナルデータやパーソナルデータを加工したデータの第三者への者提供の有無及び提供先
5.消費者によるパーソナルデータの提供の停止・訂正の可否及びその方法
6.問合せ先
7.保存期間、廃棄

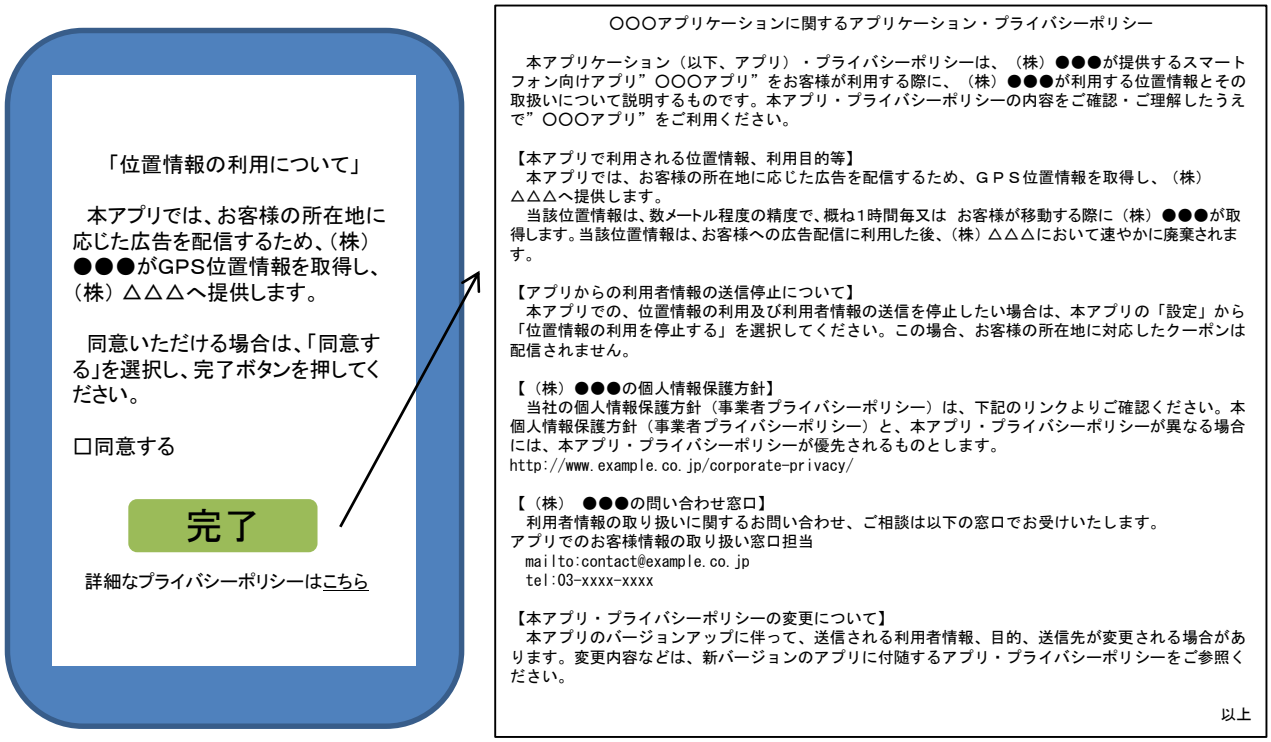
エ　保存期間

位置情報の保存期間は、利用目的に対して必要な範囲内で定めることが必要である。また、位置情報を加工（いわゆる匿名化）して利用するために、他の利用目的のために定めた保存期間を超えて加工前・加工途中の情報を保存する場合には、その期間を保存期間として定めることが必要である（4.（4）②（イ）で後述）。

③　概要版による説明・表示

利用者が内容を理解した上で同意をするためには、説明・表示が簡明であることが求められる。位置情報の種類、利用目的、第三者提供の有無といった特に重要な点について、概要として説明・表示し、詳細については別途誘導して説明する等の対応が推奨される。

【図表3－1：スマートフォンアプリケーションにおける概要版・詳細版のイメージ】



④　委託の取扱い

電気通信事業者が位置情報を取り扱う場合においては、位置情報の管理や加工といった情報の取扱いについて委託を行う場合がある。現行保護法上、個

人情報の取扱いの委託は第三者提供に当たらず[49]、したがって、同意取得も不要であることから、必ずしも位置情報を取り扱う電気通信事業者がその取扱いを委託している旨は必ずしも公表されていない。しかし、電気通信事業者が取得した位置情報について管理や加工の委託を行い、それが明らかにされていない結果、自身の位置情報に意図しない電気通信事業者が関わっていることに利用者が不安を覚えるケースも生じている。一部の電気通信事業者においては、利用者への透明性の確保の観点から、位置情報の取扱いについて、その委託関係を当該サービスのウェブページ等で明示しているケース[50]がある。情報の取扱いの委託は、その責任は委託元にあり、委託先の情報管理体制について委託元の監督が及んでいることが前提であることから、改めて利用者の同意を取得することは必要ないと考えられるが、位置情報の取扱いに係る委託関係について、利用者に対し分かりやすく説明・表示することは推奨すべき取組みであると考えられる[51]。

(4) 利用者関与の仕組み

位置情報は、ある人がいつどこに所在するかという情報であり、一度同意をした後でも、位置情報が取得等されることについて、事後的な同意内容の変更（設定変更）[52]を望む場合が容易に想定される。位置情報のプライバシー性の高さも踏まえれば、電気通信事業者は、位置情報の取扱いについて、利用者が事後的に同意内容を変更できる（設定変更できる）機能が設けられることを原則とすべきである[53]。

なお、携帯電話の位置登録情報やWi－Fiのプローブリクエスト等の情報については、それぞれのシステムに基づく仕様として、通信の前提として自動的に取得されるものであり、およそその取得自体を拒否する場合には、端末側での機能のオフによって対応するものであると考えられるが、電気通信事業者が、当該情報を

---

[49] 保護法第23条第4項第1号。保護法において「委託」とは、委任契約、請負契約といった契約の形態・種類を問わず、個人情報取扱事業者が他の者に個人データの取扱いの全部又は一部を行うよう依頼する契約の一切を含む。具体的には、個人情報取扱事業者が外部の情報処理会社等に対して個人データの入力、編集、出力等の処理を行うことを依頼すること等が想定されている。

[50] 例えば、KDDIが提供するスマートフォン向けアプリ「auナビウォーク」では、同アプリで取得するGPS位置情報等について、業務委託先である株式会社ナビタイムジャパンの管理するサーバへ送信される場合がある旨、アプリ利用規約内において説明されている。

[51] なお、通信の秘密に該当する位置情報については、通信の秘密の保護の規律に従った対応が求められることに留意する必要がある。

[52] 本報告書において「事後的な同意内容の変更」とは、位置情報の取得・利用・第三者提供について同意した後、事後的にその同意の効果を将来に向かって消滅させることをいう。

[53] なお、事後的に同意内容を変更する（設定変更する）機能があることが、利用者に容易に認識され、また、利用者がその機能を利用することが容易に可能であることは、利用者が同意を継続的に与えていると評価できる場合もあると考えられる。

取得後、通信目的外で利用することについては、同意取得とその同意内容の変更（設定変更）の機能が必要である。

(5) 公的分野での利活用

災害救助や防災分野といった公的分野において、電気通信事業者が取り扱う位置情報の利活用への期待が高まっている。

本検討会における緊急時の取扱いの整理では、本人の同意なくGPS位置情報等を取得し、第三者提供できるのは、人命救助という緊急避難の場面において、一定の条件を満たした上、第三者提供先が救助機関に限定した場合とされた[54]。このことからすれば、公的分野での利活用ということを以て、本人の同意なく位置情報を利用・第三者提供することは困難であると考えられる。

しかしながら、公共性の高い分野での利活用であれば、利用者に裨益するものでもあり、利用者の同意も得やすいと考えられる。また、一定の公的目的の下、一定の公的主体に限定しての利用・第三者提供であれば、利用者へのプライバシー上のリスクを低減させることも可能であると考えられ、さらに、このような利活用の場面において、一定程度の匿名化を行う場合には、プライバシー上のリスクを更に低減することも可能である。

このため、位置情報の公的分野での利活用においては、利用目的・主体・取扱い方法（保存期間、加工の方法、管理運用体制等）に応じたプライバシー上のリスクや利用者の受容度[55]等を勘案して、その取扱いの在り方が検討されうる[56]。

利用目的、主体、取扱い方法に応じたプライバシー上のリスクや利用者の受容度等とこれに応じた取扱いの在り方については、実証を行っていくことが必要であ

---

54 人命救助等におけるGPS位置情報の取扱いに関するとりまとめ　第4参照

55 位置情報の利活用に対する利用者の受容度を調査したものとして、総務省情報通信政策研究所が平成 26 年5月に公表した「位置情報の利用に対する意識調査」が参考となる。（参考資料1参照）

この中で、位置情報の利用について目的別に「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」に分けて最も近い考えを問うたところ、「災害（緊急）」「防災・防犯」については、「許容できる／条件付きで許容できる」を合わせて、それぞれ 95.4%、93.8%といった高い許容度が示された一方で、「観光促進のための統計」については同 73.2%、「広告マーケティングやサービス向上」については同 55.3%と、許容度に違いが見られた。

また、目的別にどのような主体にまで位置情報を提供することができるか問うたところ、「災害（緊急）」「防災・防犯」では、「国（防災）」が、それぞれ 87.0%、85.1%が許容するという高い許容度が示された。次いで「国（警察）」「地方公共団体」が6割超と続いている。

56 公的主体が収集した位置情報のプライバシーに係る裁判事例として、Nシステム事件が挙げられる。この中では、違法性の判断基準として、① 取得、保有、利用される情報が個人の思想、信条、品行等に関わるかなどの情報の性質、② 情報を取得、保有、利用する目的が正当なものであるか、③ 情報の取得、保有、利用の方法が正当なものであるか、④ 情報管理の厳格さなどを総合して判断すべきとされている。（東京地裁平成 13 年 2 月 6 日判決、東京地裁平成 19 年 12 月 26 日判決）

る。公的目的に限っても、大規模災害時の救助・捜索といった人の生命・身体に関わる極めて公共性の高いものから観光振興のように関連する企業等の事業活動に帰着するものまで広範であり、また、公的主体についても、国や地方公共団体から非営利団体まで幅広く存在している。まずは、利用者からの理解が得られやすい災害救助・防災分野といった公共性の高い分野における、国、地方公共団体といった公的主体への第三者提供について、実証を進めていくべきであると考えられる[57]。

[57] 総務省においては、G空間×ICTプロジェクトを推進しており、プロジェクトの1つである「G空間プラットフォームの構築」の中で、電気通信事業者が保有する位置情報等の運用データについて、プライバシー等に配慮しつつ、災害時の個人の避難誘導や迅速な安否確認等を実現するための環境を整備するための実証を平成 26 年度以降行っていく予定。（参考資料2参照）

４．位置情報の加工（いわゆる匿名化）について[58]

(1) 位置情報の加工方法

位置情報を利活用するに当たっての、個人が特定される主なリスクとそれに対応する加工方法として、以下のものが挙げられる。

位置情報を取り扱うに際しての個人が特定されるリスクの例

- 位置情報に伴う氏名や属性情報等の記述から個人が特定[59]されてしまう。
- 詳細な位置情報と時間から個人が特定されてしまう。
- 位置情報と他のデータが、位置情報を用いてマッチングされ、その結果個人が特定されてしまう。
- 特徴的な位置情報の履歴から生活圏や行動パターンがわかり、個人が特定されてしまう。

対策となる加工方法の例

- 直接あるいは組み合わせで個人が特定できる情報の削除、仮名化
- 組み合わせで個人が特定できる情報の一般化、ランダム化
- 位置情報（時間）のより広いエリア（時間帯）への一般化、違う位置（時間）へのランダムな置き換え（図表４－１、４－２）
- 生活圏情報や行動パターンの削除、一般化、置き換え（図表４－３）
- 仮名の短い時間での更新、長い履歴の削除、分割や間引き（図表４－４）
- 位置情報の取得間隔の適切な設定（極端に短い間隔にしない）
- 上記の手法を用い位置情報と属性情報を適切に加工し、全ての属性に対して、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。（図表４－５）

---

[58] 脚注 37 参照

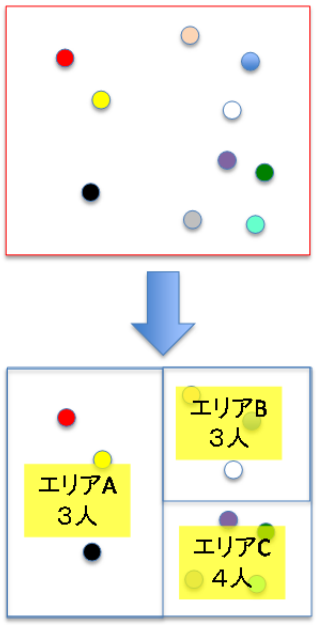
[59] 以下、「特定」及び「識別」の用語を用いる際には、IT本部パーソナルデータ検討会で整理された定義による。（参考資料3参照）

【図表４－１：位置情報の一般化の例】

（10名のある時刻における位置情報を扱うケース）

位置
位置1
位置2
位置3
位置4
位置5
位置6
位置7
位置8
位置9
位置10

位置
エリアA
エリアA
エリアA
エリアB
エリアB
エリアB
エリアC
エリアC
エリアC
エリアC



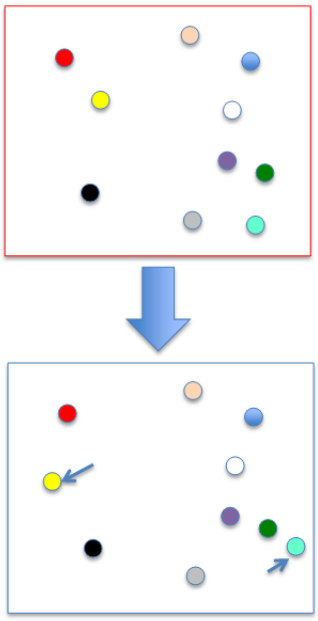
※位置を適切なサイズのエリアに拡大させて、エリアごとに十分な人数を確保する。

【図表４－２：位置情報のランダム化の例】

（10名のある時刻における位置情報を扱うケース）

位置
位置1
位置2
位置3
位置4
位置5
位置6
位置7
位置8
位置9
位置10

位置
位置1
位置2’
位置3
位置4
位置5
位置6
位置7
位置8
位置9
位置10’



※いくつかの位置の場所をランダム化（不規則にずらす、置き換える）することにより知られたくない位置が確定的にもれることを防ぐ。

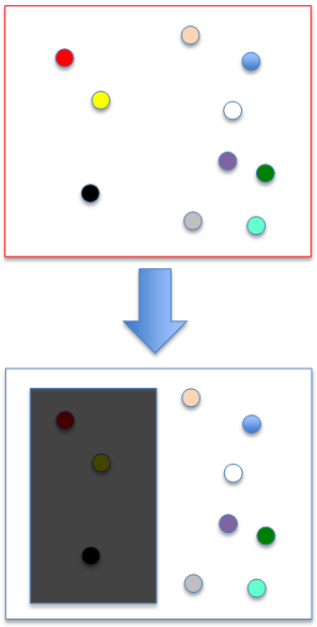
【図表４－３：生活圏情報等の削除の例】

（10名のある時刻における位置情報を扱うケース）

位置
位置1
位置2
位置3
位置4
位置5
位置6
位置7
位置8
位置9
位置10

位置
位置1
位置2
位置3
位置4
位置5
位置6
位置7
位置8
位置9
位置10

（注．黒塗りは削除を示す）

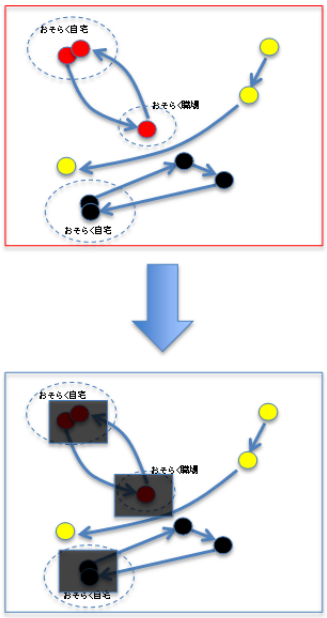


※　自宅の位置情報を削除。
必要に応じて職場や病院などの
位置情報を削除（分析目的による）

（3名の移動履歴を扱うケース）

ID	時刻	位置
ID01	08:00	位置1
ID01	09:00	位置2
ID01	20:00	位置1
ID02	08:00	位置3
ID02	10:00	位置4
ID02	15:00	位置5
ID02	21:00	位置3
ID03	08:00	位置6
ID03	09:00	位置7
ID03	20:00	位置8

ID	時刻	位置
ID01	08:00	位置1
ID01	09:00	位置2
ID01	20:00	位置1
ID02	08:00	位置3
ID02	10:00	位置4
ID02	15:00	位置5
ID02	21:00	位置3
ID03	08:00	位置6
ID03	09:00	位置7
ID03	20:00	位置8



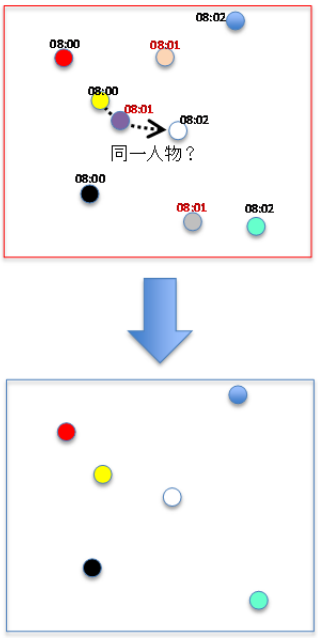
※　ID01の自宅と職場、ID02の
自宅を削除。

【図表４－４：更新間隔の間引きの例】

（複数名の時刻をまたぐ位置情報を扱うケース）

時刻	位置
08:00	位置1
08:00	位置2
08:00	位置3
08:01	位置4
08:01	位置5
08:01	位置6
08:02	位置7
08:02	位置8
08:02	位置9

時刻	位置
08:00	位置1
08:00	位置2
08:00	位置3
08:01	位置4
08:01	位置5
08:01	位置6
08:02	位置7
08:02	位置8
08:02	位置9



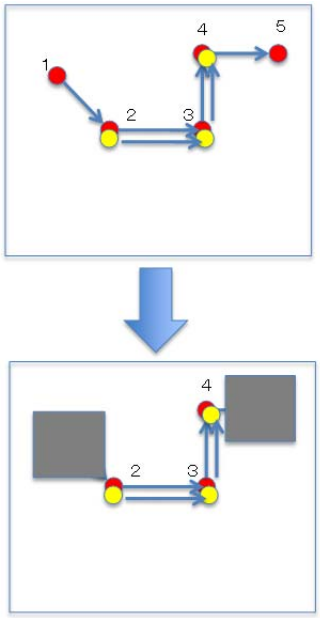
※　時間的に近接した位置情報を間引いて、移動の軌跡の推定を防止する。

【図表４－５：位置情報の複数化の例】

（複数名の移動履歴を扱うケース）

ID	時刻	位置
ID01	08:00	位置1
ID01	09:00	位置2
ID02	09:00	位置2
ID01	10:00	位置3
ID02	10:00	位置3
ID01	11:00	位置4
ID02	11:00	位置4
ID01	12:00	位置5

ID	時刻	位置
ID01	08:00	位置1
ID01	09:00	位置2
ID02	09:00	位置2
ID01	10:00	位置3
ID02	10:00	位置3
ID01	11:00	位置4
ID02	11:00	位置4
ID01	12:00	位置5

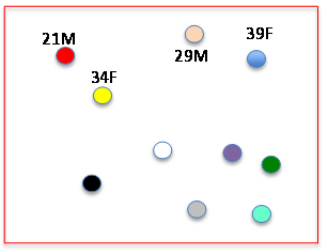


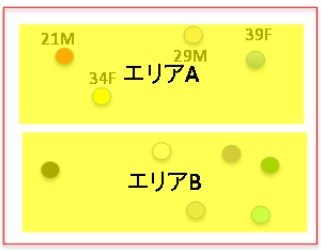
※　同じ行動の人がいる軌跡を使う。
《同時間・同位置》の人は現実には存在しないため、位置のまとめ・時間のまとめ、および系列長の制限を行う。
同じ行動の人が多数いるほど個人識別が起こりにくい。

（10名のある時刻における位置情報と属性情報（年齢・性別）を扱うケース）

年齢	性別	時刻	位置
21	男	08:00	位置1
34	女	08:00	位置2
29	男	08:00	位置3
39	女	08:00	位置4
57	男	08:00	位置5
49	女	08:00	位置6
55	男	08:00	位置7
.....	.....	.....	.....

年齢	性別	時刻	位置
20代	男	08:00	エリアA
20代	男	08:00	エリアA
30代	女	08:00	エリアA
30代	女	08:00	エリアA
50代	男	08:00	エリアB
50代	男	08:00	エリアB
40代	女	08:00	エリアB
.....	.....	.....	.....





※　例えば、位置のまとめをしながら全ての属性も加工して、複数人いる状況を作る。IDあり、時点が複数のケースでも拡張可能。

電気通信事業者においては、上記を参照し、位置情報を利活用するに当たっての個人を特定されるリスクを把握した上で、対応した加工を適切に行うことが重要である。

上記のとおり、位置情報の加工の方法は様々であるが、その加工の程度によって、以下の(2)又は(3)の2つの段階に分けられると考えられる。

(2)　「十分な匿名化」

(1)で挙げた加工方法等の組み合わせにより、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言える程度に加工（以下このように加工することを「十分な匿名化」という。）された位置情報については、個人を特定されるリスクが大きく低減されており、利用者の同意なく利用・第三者提供することが可能であると考えられる[60]。

「十分な匿名化」に当たっては、例えば「全ての属性に対して、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、具体的にどの程度の「複数」であればよいか等、「十分な匿名化」の水準は、あらかじめ一律に示すことは困難とされており、データセットの性質やその利活用の態様に応じて異なってくる。電気通信事業者においては、適切にプライバシー上のリスクを把握した上で、可能な限り十分に加工を行うことが必要と考えられる。また、共通の性質を有するデータセットについて、同様の利活用を行う事業者間においては、「十分な匿名化」の共

[60] なお、通信の秘密に該当する位置情報については、後記5. 参照。

通的な基準について検討を進めていくことが必要であり、実証も行いつつ、基準の整備等を行っていくことが適当であると考えられる。

(3) （仮称）個人特定性低減データ

IT本部パーソナルデータ検討会での議論を踏まえれば、「十分な匿名化」と言える程度までには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については、「（仮称）個人特定性低減データ」（以下「低減データ」という。）として取り扱われることが想定される。

低減データは、提供者及び受領者が個人の再特定を行わないことを法的規律で制限することを前提として、一定程度の加工を施すことにより、利用者の同意なく利用又は特定の受領者への第三者提供を認める制度として検討されている。

その加工の程度について考えてみた場合、データの利活用における有用性と個人の特定性・識別性の低減させることはトレードオフの関係にあり、可能な限り加工を行うことが望ましいものの、その利用目的等に応じ、ケースバイケースで判断されるものと考えられる。

他方で、低減データと言えるための最低限の加工を施すことは必要であると考えられるが、そのメルクマールとしては、少なくとも当該データから「直接」個人が特定されることはないよう適切な加工がなされていることが必要であり、その上で、電気通信事業者においては、「利用目的に対して必要最小限の情報」になるよう加工を行うことが必要であると考えられる。

電気通信事業者が取り扱う位置情報について検討した場合、

- 直接個人が特定できる情報（氏名や顕著な特徴）の削除、仮名化 【データから「直接」個人が特定されないための必須の加工】
- 同時に提供する他の属性情報等は必要最小限とし、可能な限り一般化、ランダム化を行う。
- 位置情報や時間の精度は必要最小限とし、より広いエリアへの一般化、違う位置へのランダム化を行う。
- 生活圏情報や行動パターンは、可能な限り、これを削除、一般化、置き換えを行う。
- 仮名は可能な限り短い時間で更新し、位置の履歴は可能な限り短くする（削除、分割、間引き）。
- 位置情報の取得頻度は必要最小限（極力間隔を空ける）とする。

等の加工を、電気通信事業者において適切に選択して行うことが想定される。

低減データとして求められる加工の程度は、その制度的枠組にも依存する。現在、その制度設計については、IT本部パーソナルデータ検討会での議論が継続しているところである。電気通信事業者が取り扱う位置情報の低減データの取扱い

は、IT本部パーソナルデータ検討会での検討結果と位置情報の高いプライバシー性を踏まえ、検討していく必要がある[61]。

(4) 匿名化した場合における適切な取扱い

① 利用者に対する説明・表示

位置情報が「十分な匿名化」がなされ、あるいは低減データとして取り扱われるとしても、再特定化・再識別化といったプライバシー上のリスクはゼロではない。また、位置情報が利用されていること自体への不安感をとりのぞくためには、プライバシーが侵害されるおそれが低いということ自体が利用者に対し分かりやすく説明されることが望ましい。このため、電気通信事業者においては、「十分な匿名化」を施した場合、あるいは低減データとして取り扱う場合であっても、利用者に対して、その位置情報の取扱いについて分かりやすく説明・表示を行うべきである。

ア 説明・表示の方法

説明・表示を行う方法としては、位置情報取得時等における同意取得の場面での説明・表示に加えて行うほか、当該サービスのウェブページや利用者に配布される広報冊子等によって、広く利用者に周知を行うことが想定される。

イ 説明事項

具体的な説明事項としては、位置情報取得時等における同意取得の場面での説明・表示事項に準じ、以下のような事項が挙げられる。

(ア) 取得者(位置情報の利用者)
(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)
(ウ) 精度、取得頻度、追跡期間
(エ) 加工の手法
(オ) 利用目的
(カ) 第三者提供の有無その他第三者提供に関する事項
(キ) 保存期間
(ク) 位置情報に紐付けて利用される他の利用者情報
(ケ) 利用者関与の仕組み 等

なお、第三者提供に関する事項とは、位置情報取得時等における同意取得の場面での説明・表示事項のように、具体的な第三者提供先を記述することも

[61] 本検討会では、位置情報を念頭に低減データの加工に係る試行的な検討を行ったものである。低減データは、個人情報保護法の改正によって創設が予定されている制度であり、現行法において、このようなデータが利用者の同意なく利用・第三者提供できるわけではない。

想定されるが、利用者への透明性確保の観点から、可能な範囲で、第三者提供先の属性や、再特定・再識別を禁止する旨の契約条件等について記載することを求めるものである。

② 加工前・加工途中の位置情報の保存について[62]

ア 加工前・加工途中の情報の取扱い

加工前・加工途中の情報を保有している場合、加工後の情報の再特定・再識別の可能性や、加工前・加工途中の情報を保有していることによる漏洩等のリスクが生じる。この点、加工前・加工途中の情報を保有していることが直ちに再特定・再識別等の問題に繋がるわけではないが、電気通信事業者においては、加工前・加工途中の情報を保有していることへのプライバシー上のリスクを認識し、加工前・加工途中の情報については破棄するか、あるいは適切な管理体制・方法の下、加工後の情報と別に保存すること[63]等が必要である。適切な管理体制・方法とは、当該情報が漏洩等しないよう適切に保管するという意味での管理体制・方法（保護法で言うところの安全管理措置）に加えて、取り扱う体制を明確に分離した上で保存する等、加工後の情報と照合することで識別特定情報としないことを担保するような管理体制・方法である。

イ 保存期間

個人情報を加工して利用するために、加工前・加工途中の情報を他の利用目的に必要な期間（通信目的や加工前の情報を取得した際の本来の利用目的に必要な期間）を超えて保存しているとの指摘がなされている。この点、加工して利用する目的で、加工前・加工途中の位置情報を他の利用目的に必要な期間を超えて保存する場合には、電気通信事業者は、位置情報取得時の同意取得の際[64]の説明・表示において、加工して利用する目的での保存期間を利用

---

62 なお、通信の秘密に該当する位置情報については、後記5．(2)参照。

63 参考として、IT本部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及びFTCレポートにおける以下の記述を参照。
・「「（仮称）法第 23 条第 1 項適用除外情報」の取扱条件の検討において、提供者（現行法の個人情報取扱事業者）が、「（仮称）法第 23 条第1項適用除外情報」を作成した後に、元の個人情報を破棄せずに継続保有している場合があり、そこでは両情報を容易に照合できる場合とそうでない場合が存在するが、容易に照合できる場合においては、容易照合性に関する例外規定の設定やこの場合の特別な運用・管理に関する規定の整備等について検討が必要である。」（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 3．(4)エ.(ア)）
・「事業者が、識別可能なデータとこのように非識別化されたデータの双方を保持・使用する場合は、これらのデータは別々に貯蔵すべきである。」（FTCレポート「急速な変化の時代における消費者プライバシーの保護」注釈113訳）

64 3．(4)（イ）において、例外的に利用者の同意を取得せずに位置情報を取得・利用できる場合として「通信を成立させるために必要不可欠な位置情報の取得・利用」に限定しているところ、これ

者に対して示すべき[65]である。この際、加工後の情報を利用するために、必要最小限度の期間となっていることが必要である。

③ 利用者関与の仕組み

位置情報が「十分な匿名化」がなされ、あるいは低減データとして取り扱われ、電気通信事業者が利用者の同意なく利用・第三者提供ができたとしても、位置情報の取扱いに係るオプトアウト機能（利用者からの申出に基づき、申出以降その利用者のデータを匿名化した上での利活用を行わないこと）を設けることは望ましいと考えられる[66]。

特に、利用者がそのサービスから容易に退出できない場合、利用者が位置情報を匿名化した上で利活用されたくないとしても、当該サービスを利用せざるを得なくなる。位置情報を匿名化した上で利活用されることが、利用者にとって当該通信サービスを利用するための条件とならないようにすることが必要である[67]。

また、オプトアウトを認めることで、統計上の有意性を失ってしまう等により、その利用目的が果たせない場合があるといった意見もあるが、公的分野での利活用においては、その利用目的等に応じたオプトアウトの在り方について、実証を進めるとともに、必要に応じて、ガイドライン等に定めることも適当であると考えられる。

(5) 現行のサービス事例

現在、電気通信事業者が、利用者から取得した位置情報について匿名化した上で、これを非個人情報として利用者の同意なく第三者提供しているサービスの1つとして、NTTドコモによる「モバイル空間統計」が挙げられる。

を超えて位置情報を保存する場合、利用者からは同意を取得することが必要となる。

65 個人情報保護ガイドライン上、そもそも個人情報は、「原則として利用目的に必要な範囲内で保存期間を定めるものとし、当該保存期間経過後又は当該利用目的を達成した後は、当該個人情報を遅滞なく消去するもの」とされており（第10条第1項）、定めた保存期間を超えて個人情報は保存することはできない。このため、個人情報を匿名化した上で利用することは、個人情報の「利用」には当たらないと解されているものの、匿名化して利用するために加工前・加工途中の情報を、匿名化して利用する目的での保存期間を示すことなく、元の保存期間を超えて保存することはできない。

66 例えば、位置情報等を匿名化して利活用することが、サービス提供の前提となっているアプリケーションサービス等も想定され、このような場合であって、利用者が容易に当該サービスから退出することができる場合には、その旨を利用者関与の方法として説明・表示をしておくことで、オプトアウト機能を設けないことも許容されるものと考えられる。

67 例えば、MNOが提供する携帯電話サービスは、利用者が容易に退出することは難しいと考えられ、位置登録情報を匿名化した上で利活用することは、そのサービス提供の条件とすべきではない。

モバイル空間統計においては、利用者の携帯電話の位置登録情報その他の運用データについて、非識別化処理、集計処理、秘匿処理といった匿名化処理を行い、集団の人数を表す統計情報に加工している（2⑵②アを参照）。利用者に対する説明・表示については、加工方法等について説明したガイドライン等がNTTドコモWebページにおいて公開されているほか、利用者に対して送付される請求書同封冊子等でもその説明がなされている。

位置情報の保存については、加工前の位置登録情報について、その取得後、機械的にモバイル空間統計に加工された後は、速やかに破棄されているとのことである。

また、利用者関与の仕組みとして、オプトアウト機能が提供されており、利用者は、NTTドコモへの電話での問い合わせにより、自身の位置登録情報についてモバイル空間統計へ利用されることを停止することが可能となっている。

以上を踏まえれば、モバイル空間統計は、電気通信事業者が取得した位置情報について、「十分な匿名化」と適切な取扱いに配意した先行的な取組事例と言え、こうした取組事例及びその現状と課題なども参考に、本検討会の報告を踏まえた取組が深められることが期待される。

５．通信の秘密に該当する位置情報の取扱いについて

(1)　通信の秘密に該当する位置情報

前記2．（2）①イのとおり、通信の秘密は厳格に保護されており、通信の秘密に該当する情報については、利用者の有効な同意がない限り、これを利用することは通信の秘密の侵害[68]に当たると解されている。前記3．及び4．の検討は、一般的な位置情報に関するものであるが、位置情報が通信の秘密に該当する場合には、これらに加え、通信の秘密の保護の規律に従った対応が求められることとなる。

一方、前述のとおり、通信の秘密に該当する位置情報についても、これをビッグデータとして適切に利活用していくことへの期待が高まっている。

そこで、通信の秘密に該当する位置情報について、加工（いわゆる匿名化）した上で利用・第三者提供することと通信の秘密との関係について以下のとおり検討を行った。

(2)　通信の秘密に該当する位置情報の加工（いわゆる匿名化）

①　検討の前提

ア　通信の秘密の侵害

通信の秘密に該当する位置情報について、加工した上で利用・第三者提供することは、通信の秘密の利用に当たるため、利用者の有効な同意がない限り、通信の秘密の侵害に該当し得ると考えられる[69]。

イ　有効な同意の取得の在り方

通信の秘密についての同意は、契約約款等に基づく事前の包括同意のみでは、一般的に有効な同意と解されておらず、個別の同意でなくてはならないと解されている。

しかしながら、ビッグデータ時代において、位置情報の適正な利活用により、

---

[68] 通信の秘密を侵害する行為は、知得（積極的に通信の秘密を知ろうとする意思のもとで知得しようとする行為）、窃用（発信者又は受信者の意思に反して利用すること）、漏えい（他人が知り得る状態に置くこと）の3類型に大別されている。なお、ここにいう、知得や窃用には、機械的・自動的に特定の条件に合致する通信を検知し、当該通信を通信当事者の意思に反して利用する場合のように機械的・自動的に処理される仕組みであっても該当し得る。

[69] (参考)
いかなる個人情報に対しても、識別非特定情報や非識別非特定情報となるように加工できる汎用的な方法は存在しないこと、もっとも、個人情報の種類・特性や利用の目的等に応じて技術・対象を適切に選ぶことにより、識別非特定情報や非識別非特定情報に加工することは不可能ではないものの、一旦識別非特定情報や非識別非特定情報に加工できたとしても、他の情報との突き合わせ等により、再び識別特定情報となる可能性がある（IT本部パーソナルデータ検討会技術検討ワーキンググループ報告書より）。

国民生活の向上や社会経済活動の促進等様々な社会的効果が期待されている中で、利用者の利益に配慮して、位置情報の適正かつ円滑な利活用を促進する必要性も高い。

そこで、位置情報の適正かつ円滑な利活用を促進する観点から、通信の場所、日時及び利用者・端末識別符号（利用者又は端末を識別する符号であって、利用者又は端末の属性を識別できるものを除く。以下同じ。）について、「十分な匿名化」[70]をした上で利用・第三者提供する場合に関しては、個別の同意がある場合のほか、契約約款等に基づく事前の包括同意であっても、一定の条件の下においては、有効な同意ということはできないか検討を行う。

② 検討

ア 契約約款等に基づく事前の包括同意

契約約款等に基づく事前の包括同意のみでは、一般的に有効な同意と解されていない。その理由としては、次の2つの理由が挙げられる[71]。

ⅰ 契約約款は当事者の同意が推定可能な事項を定める性質であり、通信の秘密の利益を放棄させる内容はその性質になじまないこと

ⅱ 事前の包括同意は将来の事実に対する予測に基づくため対象・範囲が不明確となること[72]

(ア) 理由ⅰとの関係

これを通信の秘密に係る位置情報の匿名化について考えてみると、対象となる情報の範囲は、通信内容以外の通信の構成要素のうち、通信の場所、日時及び利用者・端末識別符号に限定され、かつ、上記の情報を「十分な匿名化」をして利用・第三者提供をする場合、個人の特定・識別は不可能又は極めて困難であるから、個別の通信の存在・内容が推知される可能性は極めて少ない。したがって、この場合、加工の手法・管理運用体制が適切であれば、利用者に不利益が生じる可能性は極めて少ないため、通常の利用者が許諾することが想定しうるといえ、契約約款の性質になじまないとまではいえない。

なお、加工の手法・管理運用体制（「十分な匿名化」の過程で作成される情報の管理体制を含む。）の適切性については、適切に評価・検証が行われることが求められると考えられる。

---

[70] 4.(2)参照

[71] 第二次提言Ⅰ2.(2)③ウ(脚注7)より

[72] 同意の対象・範囲が不明確となることにより、利用者に不測の不利益が生じることに問題意識がある。

（イ） 理由 ii との関係

契約約款等による包括同意であっても、利用者が、一旦契約約款等に同意した後も、随時、同意内容を変更できる（設定変更できる）契約内容であって、当該契約約款等の内容（事後的に利用者が同意内容を変更できる（設定変更できる）こと並びに「十分な匿名化」後の情報の利用目的及び第三者提供に関する事項を含む。）並びに加工の手法・管理運用体制及びその適切性の評価・検証結果について、利用者に対する相応の周知が図られている場合には、契約約款等による包括同意当時において予測し得なかった事情が将来生じた場合についても、随時、利用者が同意内容を変更することができることから、将来、利用者が不測の不利益を被る危険を回避できる。

イ 「十分な匿名化」をする加工途中の非特定化情報の保存

なお、電気通信事業者が、通信の場所、日時及び利用者・端末識別符号（以下、イにおいて、これらの情報を併せて「元情報」という。）について、「十分な匿名化」をする加工途中の情報を保存することが考えられる。

この点、元情報は電気通信事業の業務の遂行上必要な範囲で設定された保存期間で保存されているものであり[73]、包括同意の下で「十分な匿名化」をした情報を利用・第三者提供する場合に、元情報を非特定化した情報（以下、単に

---

[73] 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
（通信履歴）
第 23 条 電気通信事業者は、通信履歴（利用者が電気通信を利用した日時、当該通信の相手方その他）の利用者の通信に係る情報であって通信内容以外のものをいう。以下同じ。）については、課金、料金請求、苦情対応、不正利用の防止その他の業務の遂行上必要な場合に限り、記録することができる。
2 （略）
（解説）
（1）通信履歴は、通信の構成要素であり、電気通信事業法第4条第1項の通信の秘密として保護される。したがって、これを記録することも通信の秘密の侵害に該当し得るが、課金、料金請求、苦情対応、自己の管理するシステムの安全性の確保その他の業務の遂行上必要な場合には正当業務行為として少なくとも違法性が阻却されると考えられる。
（2）～（4）（略）
（5） いったん記録した通信履歴は、第10条の規定に従い、記録目的に必要な範囲で保存期間を設定することを原則とし、保存期間が経過したときは速やかに通信履歴を消去（個人情報の本人が識別できなくすることを含む。）する必要がある。この保存期間については、提供するサービスの種類、課金方法等により各電気通信事業者ごとに、また通信履歴の種類ごとに異なり得るが、その趣旨を没却しないように限定的に設定すべきであると考えられる。また、保存期間を設定していない場合には、記録目的を達成後、速やかに消去する必要がある。ただし、法令の規定による場合その他特別の理由がある場合には例外的に保存し続けることができると考えられる。自己又は第三者の権利を保護するため緊急行為として保存する必要がある場合は、その他特別な理由がある場合として保存が許されると考えられる。

「非特定化情報」という。）を、元情報の保存期間内で保存することは、利用者に不利益を生じさせるものではなく許されると考えられる。ただし、前記ア（ア）のとおり、その管理体制が適切であり、それについて適切に評価・検証が行われている必要がある。

一方、非特定化情報について、安全性を高める措置[74]を施すことなどにより特定の利用者を識別することが極めて困難になるような状態にした場合で、元情報の保存期間を超え、「十分な匿名化」をして利用・第三者提供をするために必要な最小限度の一定期間保存することについては、具体的な保存期間、安全性を高める措置の在り方等も含め、さらに検討していくことが必要であると考えられる。

ウ　結論

以上のことからすれば、通信の秘密に該当する位置情報である通信の場所、日時及び利用者・端末識別符号（利用者又は端末を識別する符号であって、利用者又は端末の属性を識別できるものを除く。）について、「十分な匿名化[75]」をした上で利用・第三者提供することについては、

（ア） 対象となる情報の範囲が、通信内容以外の通信の構成要素のうち、通信の場所、日時及び利用者・端末識別符号に限定されること

（イ） 加工の手法・管理運用体制（「十分な匿名化」の過程で作成される情報の管理体制を含む。）が適切であること及びそれについて適切に評価・検証が行われていること

（ウ） 利用者が、いったん契約約款等に同意した後も、随時、同意内容を変更できる（設定変更できる）契約内容であって、同意内容の変更の有無にかかわらず、その他の提供条件が同一であること

（エ） 契約約款等の内容（事後的に利用者が同意内容を変更できる（設定変更できる）こと並びに「十分な匿名化」後の情報の利用目的及び第三者提供に関する事項を含む。）並びに加工の手法・管理運用体制及びその適切性についての評価・検証結果について、利用者に対する相応の周知[76]が図られていること

のすべての要件を満たしている場合であれば、契約約款等に基づく事前の包括同意であっても、有効な同意ということができると考えられる。なお、「十分な匿名化」をする加工途中の非特定化情報についての考え方は前記イのとおりであ

[74] 例えば、識別符号をハッシュ化すること等が考えられる。

[75] 4．(2)参照。

[76] 当該契約約款の内容等について、ウェブサイトへの掲載や料金明細通知書へのパンフレットの同封等の方法を始め利用者に分かりやすい方法により、周知を図ることが推奨される。

る。また、契約約款は、少なくとも後記③イの事項を分かりやすく規定することが求められる。

また、後述のとおり、「十分な匿名化」の水準及び加工の手法・管理運用体制の適切性の評価・検証方法については、引き続き検討していくことが必要であり、実証・検証を進めていくことが適切であると考えられる。

なお、通信の秘密に該当する位置情報(「十分な匿名化」の過程で作成される情報を含む。)について、「十分な匿名化」をした上で利用・第三者提供すること以外のために利用することは、同意の範囲を超えることとなるため、通信の秘密の窃用となり、通信の秘密を侵害することとなる。

③ 通信の秘密に該当する位置情報の利活用の在り方

ア 契約約款に記載すべき事項

前述のとおり、通信の秘密に該当する位置情報である通信の場所・日時及び利用者・端末識別符号について、「十分な匿名化」をした上で利用・第三者提供することについては、契約約款等に基づく事前の包括同意であっても、有効な同意ということができると考えられるが、その場合、契約約款においては、少なくとも以下のような内容を分かりやすく規定すべきと考えられる。

- 通信の場所、日時及び利用者・端末識別符号について、「十分な匿名化」をして利用すること
  （例） 通信の場所、日時及び利用者・端末識別符号について、個人を特定・識別できない形式に加工した上で利用する
- 「十分な匿名化」後の情報の利用目的
  （例） 新サービス開発に利用するため
- 第三者提供する場合には第三者提供に関する事項
  （例） 当社が別に周知するコンテンツプロバイダーに情報を第三者提供する。
- 事後的に利用者が同意内容を変更できる(設定変更できる)こと
  （例） 上記の利用・第三者提供は、利用者が設定変更を申し出た場合、中止できる

イ 今後実証・検証を行うべき事項

前述のとおり、前記②ウの要件を満たせば、通信の秘密に該当する位置情報である通信の場所、日時及び利用者・端末識別符号について、「十分な匿名化」をした上で利用・第三者提供することが許容されると考えられるところ、検討の前提である「十分な匿名化」の水準[77]については、総務省及び関係事業者に

[77] 前記4. ⑵のとおり、データセットの性質やその利活用の態様に応じて異なってくる。

おいて[78]引き続き検討をしていくことが必要である。その際には、一般的・抽象的基準を設定するだけではなく、具体的にどのような場合であれば、そのような基準に合致しているといえるかについて実証し、明らかにしていくことが適切であると考えられる。

また、前記②ウ(イ)の要件である加工の手法・管理運用体制(「十分な匿名化」の過程で作成される情報の管理体制を含む。)の適切な評価・検証の在り方について、総務省及び関係事業者において引き続き検討していく必要があると考えられる。具体的には、プライバシー影響評価(PIA:Privacy Impact Assessment)を実施することや、その評価基準(「十分な匿名化」の水準に合致していることの基準を含む。)、評価方法、第三者による検証、評価・検証結果の公表・報告・意見募集、PDCAサイクルによる見直し等について検討する必要があると考えられる。同様に、総務省及び関係事業者において、具体的な加工の手法・管理運用体制の在り方について、安全性を確保するための技術(暗号化、秘密分散技術等)等も含め、実証・検証も進めていくべきと考えられる[79]。

[78] 具体的には、総務省及び関係事業者において、法律や匿名化技術の専門家等の有識者を含めた検討の場を設け、その中で実証・検証を行っていくことなどが想定される。

[79] 脚注 75 と同じ。

６．Ｗｉ－Ｆｉ位置情報について

(1) Ｗｉ－Ｆｉ位置情報の性質

アクセスポイント設置者たる電気通信事業者が取得できるWi－Fi位置情報は、大別して、①インターネット接続のための準備段階として行われる端末利用者とアクセスポイント設置者との間の通信に基づく位置情報と、②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に分けることができる。（図表6参照）

前者の端末利用者とアクセスポイント設置者との間の通信に基づく位置情報について考えるに、

- 位置情報の基となるプローブリクエスト及び接続要求（Wi－Fi端末がアクセスポイントに接続するために送信する信号、以下「プローブリクエスト等」という。）の情報は、Wi－Fiという通信システムの仕様上、通信を成立させる前提としてアクセスポイント設置者に取得されていると考えられる。
- プローブリクエスト等の情報に含まれるMACアドレスは、端末やアクセスポイント等のネットワーク機器に原則として一意に割り当てられ、利用者側では変更困難なものである。MACアドレスは、単体では個人識別性を有しないが、総務省パーソナルデータ研究会報告書においては、「個人のPCやスマートフォン等の識別情報（端末ID等）などは、一義的にはPCやスマートフォンといった特定の装置を識別するものであるが、実質的に特定の個人と継続的に結びついており、プライバシーの保護という基本理念を踏まえて判断すると、実質的個人識別性の要件を満た」すものとされ[80]、SPIにおいては、MACアドレス等の契約者・端末固有IDについて、単体では個人識別性を有しないが、同一IDに紐付けて行動履歴や位置情報を集積する場合、プライバシー上の懸念があるとされ、「個人情報に準じた形で取り扱うことが適切」とされた[81]。また、見直し方針においても、「保護されるパーソナルデータの範囲については、実質的に個人が識別される可能性を有するもの」とするとされている[82]ことから、プローブリクエスト等の情報に含まれる端末のMACアドレスは、実質的な個人識別性を有するものとして、今後個人情報保護法上保護される情報として取り扱われる可能性がある。
- 単独又は複数のアクセスポイントによって把握される位置情報は、数メートル単位で位置の把握が可能と精度が高く、MACアドレスその他の特定の識別子と紐づいて継続的に取得された場合、端末利用者の移動の軌跡も把握可能であることから、他の位置情報と同様に高いプライバシー性を有しており、当該

80 総務省パーソナルデータ研究会報告書 第3章第1節2.(2)
81 SPI 第5章1各論①(2)
82 見直し方針 4. 中＜保護されるパーソナルデータの範囲の明確化＞参照

位置情報自体が実質的な個人識別性を有する場合もあると考えられる。

以上のとおり、MACアドレスと紐付いて取得されること、及び位置情報としてのプライバシー性の高さを踏まえると、当該Wi－Fi位置情報については、基本的に基地局に係る位置情報やGPS位置情報など他の位置情報と同様の取扱いをすることが適当である。[83]

また、後者の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は、個々の通信と関係するものであり、通信の秘密に該当する位置情報として取り扱うことが適当である。

【図表６：Ｗｉ－Ｆｉ位置情報の基となる通信について】

(2) Ｗｉ－Ｆｉ位置情報の取扱い

① 端末利用者とアクセスポイント設置者との間の通信に基づく位置情報

本とりまとめでの整理を踏まえ、以下のように取り扱うことが適当である。

ア 通信目的で取得・利用する場合

プローブリクエスト等の情報が、Wi－Fiの仕様上通信の前提として取得され、通信目的の範囲内で利用された後、速やかに破棄される場合は、電気通信事業者は、利用者の同意を取得しなくても許容されるものと考えられる。ただし、

---

[83] Wi－Fi位置情報については、

・ Wi－Fiアクセスポイントの範囲内でなければ位置情報は把握できない。小規模な事業者であって、他の事業者とも情報を共有していなければ、把握できる利用者の位置情報の範囲は限定的である。

・ 必ずしも他の利用者情報を取得しなくてもWi－Fiサービスを提供することが可能であり、Wi－Fiサービス事業者において、Wi－Fi位置情報と紐づく利用者情報を有していない場合がある。

といった点について、留意が必要との意見もあったが、本文の通り、MACアドレスとの結びつきと位置情報としてのプライバシー性の高さを踏まえれば、(2)の取扱いが必要となるものである。

Wi－Fiの仕様上、機械的にMACアドレスが取得されること等Wi－Fiの仕組みについては、利用者の十分な理解が進んでいないことから、今後利用者への周知啓発に努めていくことが必要である。

イ　通信以外の目的で利用・第三者提供する場合

プローブリクエスト等の情報を基にしたWi－Fi位置情報が、通信目的以外の利用目的で利用・第三者提供されることについて、Wi－Fi端末利用者が予測しているものとは考えられず、電気通信事業者は、原則としてWi－Fi端末利用者の個別かつ明確な同意を取得すべきであり、また、事後的に同意内容を変更できる（設定変更できる）機能を設けることが必要である。

ウ　「十分な匿名化」・低減データ化された場合

当該Wi－Fi位置情報が、「十分な匿名化」がなされた場合、あるいは低減データとして取り扱われる場合、電気通信事業者は、利用者の同意なく利用・第三者提供することが可能と考えられる。しかし、利用者の現状の認識を考えると、当該Wi－Fi位置情報が利活用されていることに関しては十分な方法で説明・表示を行うことが必要である。例えば、Wi－Fiのアクセスポイントの設置場所は、基本的には施設内や限定された空間（商店街やショッピングセンター等）であることが想定されるため、当該施設等において看板・ポスター等を掲示し、Wi－Fi位置情報の利活用等についてWi－Fi端末利用者に対し周知することが考えられる。

また、Wi－Fi位置情報を匿名化して利活用する場合、位置情報の取扱いに係るオプトアウトの機能を設けることが望ましいと考えられる[84]。特に、Wi－Fi位置情報が、利用者の意思と関係なく、端末がアクセスポイントのエリア内にあることで取得されてしまうプローブリクエスト等を基にしていることを踏まえる必要がある[85]。

---

[84] 例えば、電気通信事業者が、利用者から取得した位置情報を匿名化して利活用することを条件に、無料でWi－Fi通信サービスを提供している等、位置情報を匿名化して利活用することがサービス提供の前提となっている場合であって、利用者が容易に当該サービスから退出することができる場合には、その旨を利用者関与の方法として説明・表示をしておくことで、オプトアウト機能を設けないことも許容されるものと考えられる。

[85] Wi－Fiのアクセスポイントは、端末の利用者がそのアクセスポイントを利用する意思がなくても、その通信の仕組み上、端末のプローブリクエスト等を収集してしまう。これを考慮すると、当該アクセスポイントのエリアに入らない事が容易でない空間（例えば当該アクセスポイントのエリアに公衆の施設が含まれる場合）等で、オプトアウトの機能を設けず、その結果、位置情報を匿名化した上で利活用されることが、当該エリアでWi－Fi通信を利用（端末上Wi－Fi機能をオンにすることも含む。）する条件になってしまうことは適当ではないと考えられる。

② 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

個別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、通信の秘密に該当するものであり、基本的に個々の通信の際に利用される基地局の位置情報と同様、５．の整理に沿った取扱いとなる。

③ 関係者との連携

Wi－Fi位置情報の利活用においては、電気通信事業者のみならず、エリアオーナー等他の事業者等も関係者として想定される。Wi－Fi位置情報の利活用を進めていくにあたっては、電気通信事業者と関係者らが連携して、本検討会の整理を踏まえた適切な利活用を推進していことが望ましい[86]。

[86] 例えば、アクセスポイント設置場所付近での看板・ポスター等での周知に当たっては、エリアオーナーとの協力が必要であろう。また、電気通信事業者とそれ以外の事業者複数が連携して提供するようなサービスでは、連携する事業者においても、本検討会の整理を踏まえた適切な同意取得や説明・表示を行う必要がある。

７．今後の取組み

(1)　本検討会の整理を踏まえた位置情報の取扱い

本検討会の位置情報の取扱いに係る整理を踏まえ、まずは、電気通信事業者において、個別かつ明確な同意の取得や利用者に対する分かりやすい説明・表示等に取り組み、適切に位置情報の利活用を行っていくことが望ましいと考えられる。

公的分野での利活用や匿名化した位置情報の利活用についても、事業者において適切にプライバシー上のリスクを把握し、可能な範囲でその取組を進めていくことが望ましい。さらに、下記の実証を進め、その成果を共有することで、その利活用を推進していくことが必要である。

現状、電気通信事業者が取り扱う個人情報及び通信の秘密については、個人情報保護ガイドライン及びその解説の形でとりまとめられているが、下記の実証や今後見込まれている保護法の改正の状況を踏まえ、位置情報の取扱いを個人情報保護ガイドライン及び解説に反映させることが適当である。

なお、本検討会における整理は、電気通信事業者を対象としたものであるが、移動体端末から取得される利用者の位置情報については、その高いプライバシー性から強く保護が求められるものであり、電気通信事業者以外の事業者においても、本検討会における整理を踏まえた取扱いが行われることが期待される。

(2)　公的分野での利活用の実証

位置情報の公的分野での利活用においては、利用目的・主体・取扱い方法（保存期間、加工の方法、管理運用体制等）に応じたプライバシー上のリスクや利用者の受容度　等を勘案して、その取扱いの在り方が検討されうる　。

利用目的、主体、取扱い方法に応じたプライバシー上のリスクや利用者の受容度等とこれに応じた取扱いの在り方については、実証を行っていくことが必要である。公的目的に限っても、大規模災害時の救助・捜索といった人の生命・身体に関わる極めて公共性の高いものから観光振興のように関連する企業等の事業活動に帰着するものまで広範であり、また、公的主体についても、国や地方公共団体から非営利団体まで幅広く存在している。まずは、利用者からの理解が得られやすい災害救助・防災分野といった公共性の高い分野における、国、地方公共団体といった公的主体への第三者提供について、実証を進めていくべきであると考えられる

(3)　加工した位置情報の適切な利活用

「十分な匿名化」の水準については、共通の性質を有するデータセットについて、同様の利活用を行う事業者間で、その共通的な基準について検討を進めていくことが必要であると考えられる。とりわけ通信の秘密に該当する位置情報については、総務省及び関係事業者において引き続き検討をしていくことが必要である。また、その際

には、一般的・抽象的基準を設定するだけではなく、具体的にどのような場合であれば、そのような基準に合致しているといえるかについて実証し、明らかにしていくことが必要である。

通信の秘密に該当する位置情報については、加工の方法・管理運用体制（「十分な匿名化」をする過程で作成される情報の管理体制を含む。）の適切性について、適切に評価・検証が行われることが求められると考えられ、その在り方について、総務省及び関係事業者において引き続き検討していく必要があると考えられる。具体的には、プライバシー影響評価（PIA）を実施することや、その評価基準（「十分な匿名化」の水準に合致していることの基準を含む）、評価方法、第三者による検証、評価・検証結果の公表・報告・意見募集、PDCAサイクルによる見直し等について検討する必要があると考えられる。

また、総務省及び関係事業者において、具体的な加工の方法・管理運用体制の在り方について、安全性を確保するための技術（暗号化、秘密分散技術等）等も含め、実証・検証も進めていくべきと考えられる。

(4)　利用者への周知啓発

電気通信事業者が位置情報の利活用を進めていくに当たっては、利用者の理解と信頼関係の下、これを行っていくことが重要である。位置情報を取り扱う電気通信事業者においては、本検討会で整理された位置情報の取扱いを基に、利用者に対し適切に説明・表示を行うことが必要である。また、本検討会においては、Wi－Fiの仕組みが利用者において理解されておらず、そのような中でWi－Fi位置情報が利活用されることについての懸念も示された。事業者、政府、消費者団体等が協力し、利用者に対して、このような電気通信の仕組みも含めて、位置情報の利活用とその成果について広く周知を行い、利用者の理解を醸成していくことが重要である。

位置情報の利用に対する意識調査（総務省情報通信政策研究所） 抜粋

参考資料1

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

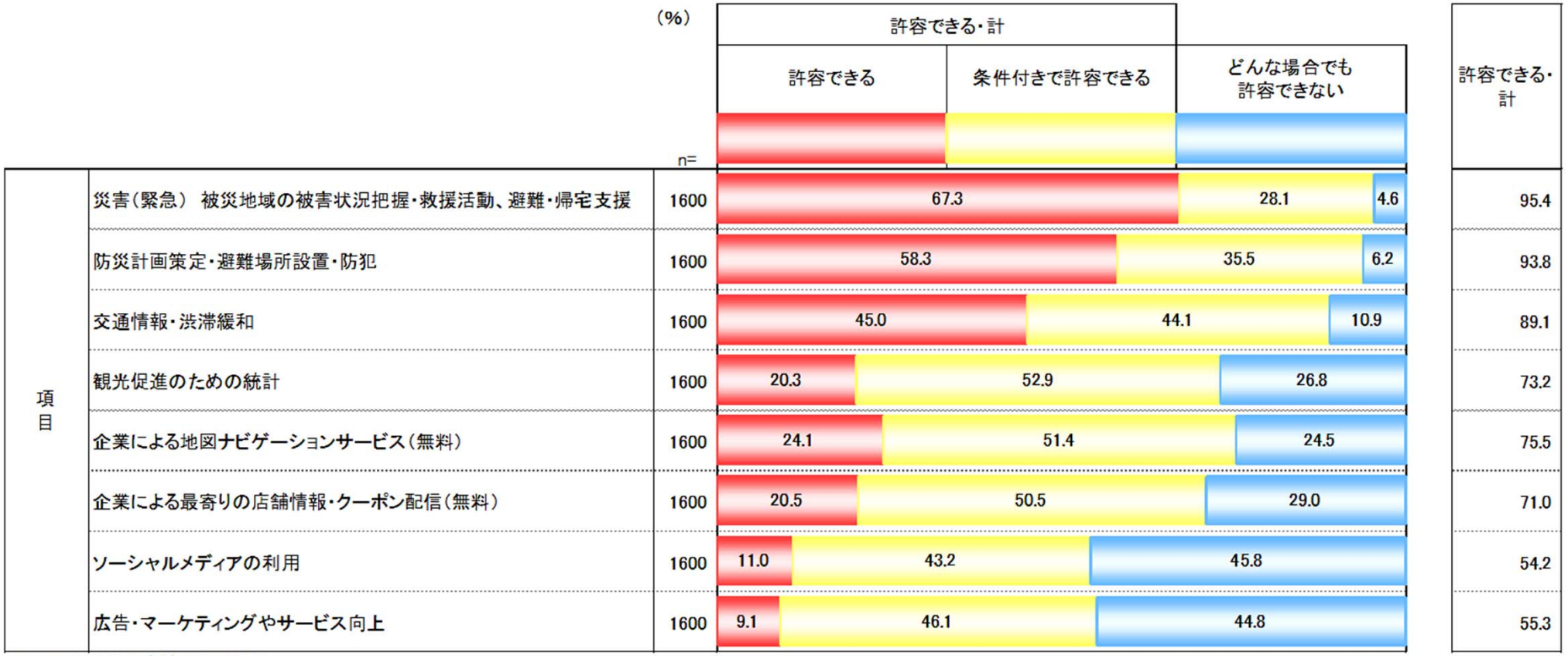
- 調査会社（株式会社クロスマーケティング）のパネルに対するウェブアンケート
- 調査の企画・分析に当たっては東京大学情報学環 橋元 良明教授、東京大学大学院学際情報学府博士課程（橋元研究室在籍） 河井 大介氏にご協力頂いた。

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。



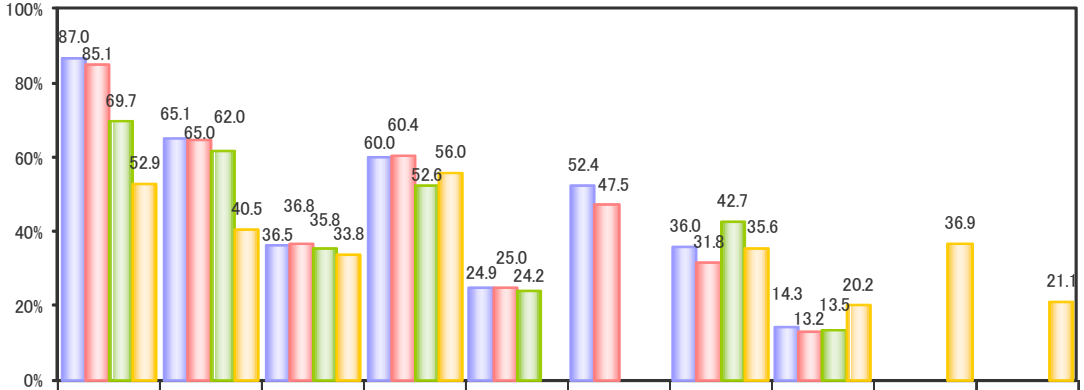
項目		n=	許容できる	条件付きで許容できる	どんな場合でも許容できない	許容できる・計
	災害（緊急） 被災地域の被害状況把握・救援活動、避難・帰宅支援	1600	67.3	28.1	4.6	95.4
	防災計画策定・避難場所設置・防犯	1600	58.3	35.5	6.2	93.8
	交通情報・渋滞緩和	1600	45.0	44.1	10.9	89.1
	観光促進のための統計	1600	20.3	52.9	26.8	73.2
	企業による地図ナビゲーションサービス（無料）	1600	24.1	51.4	24.5	75.5
	企業による最寄りの店舗情報・クーポン配信（無料）	1600	20.5	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、「地図ナビゲージョンサービス」「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享受するためであれば、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。



n=30以上で
- セグメント内で1位
- セグメント内で2位
- セグメント内で3位

項目		n=	国（防災）	国（警察）	国（その他）	地方公共団体	公共系の非営利団体	医療機関（病院、医療機関）	公共系サービスを提供する企業（鉄道・道路・通信事業者等公共性を有する企業）	企業（その他関連サービスを提供する企業）	公共系団体（観光協会等公共性を有する非営利の団体）	商店街・地域の店舗
	災害（緊急） 被災地域の被害状況把握・救援活動、避難・帰宅支援を目的とするものに関して	1526	87.0	65.1	36.5	60.0	24.9	52.4	36.0	14.3		
	防災計画策定・避難場所設置・防犯を目的とするものに関して	1501	85.1	65.0	36.8	60.4	25.0	47.5	31.8	13.2		
	交通情報・渋滞緩和を目的とするものに関して	1425	69.7	62.0	35.8	52.6	24.2		42.7	13.5		
	観光促進のための情報収集を目的とするものに関して	1171	52.9	40.5	33.8	56.0			35.6	20.2	36.9	21.1

※n=30未満は参考値のため灰色。

- 「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。

参考資料2

G空間×ICTプロジェクトと連携した電気通信事業者が取り扱う位置情報の公的分野での利活用に係る実証について

◆　電気通信事業者が保有する位置情報について、プライバシー等に適切に配慮して取り扱いつつ、他のG空間データと組み合わせ、<u>災害時の個人の避難誘導や迅速な安否確認や防災計画策定への活用等を実現</u>するための環境を整備

他のG空間データ

地方公共団体
（大学、研究機関等）

地方公共団体や大学、研究機関等が共同で公益分野での利活用モデル、データの連携モデルの開発、実証を行う。

位置情報を提供

電気通信事業者

避難誘導や
安否確認を実施

位置情報を取得

- 必要な加工の方法
- 保存期間
- 管理運用体制
- 利用者の受容度

⇒　同意の取得方法や利用者関与の方法等を検討

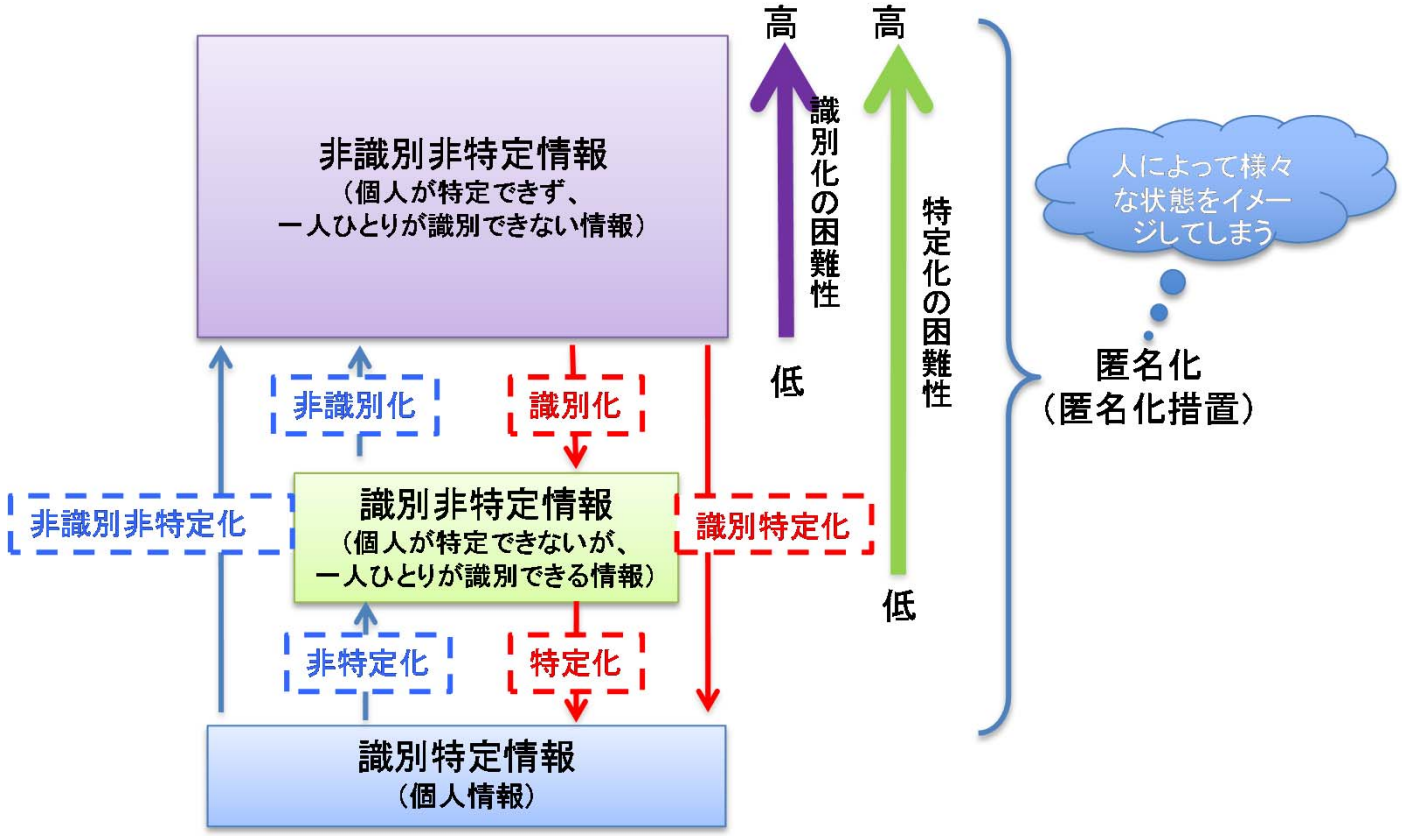
【ロードマップ】

◆　2015年度末までに、プライバシーに配慮して、位置情報等に関する公益的な利活用モデルを構築しつつ、他のG空間データとの連携や取扱いに関するルール（匿名化や透明性の確保に関するルール等）の策定に寄与

◆　2020年までに、利用者がプライバシー等に不安を覚えることがない環境で高度な利活用を実現

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）　参考資料3で示された特定・識別の用語について

○ 「識別」とは、「ある情報が誰か一人の情報であることが分かること」である。つまり、ある情報が誰の情報であるかが分かるかは別にして、ある人の情報と別の人の情報を区別できることである。
○ 「特定」とは、「ある情報が誰の情報であるかが分かること」である。「識別」のうち、特定の誰かの情報であることが分かる場合が、特定といえる。



いわゆる「匿名化」技術により加工・作成される情報のカテゴリー

No	用語	用語の説明
1	識別特定情報	個人が（識別されかつ）特定される状態の情報（すなわち「個人情報」） （それが誰か一人の情報であることがわかり、さらに、その一人が誰であるかがわかる情報）
2	識別非特定情報	一人ひとりは識別されるが、個人が特定されない状態の情報 （それが誰か一人の情報であることがわかるが、その一人が誰であるかまではわからない情報）
3	非識別非特定情報	一人ひとりが識別されない（かつ個人が特定されない）状態の情報 （それが誰の情報であるかがわからず、さらに、それが誰か一人の情報であることが分からない情報）

本検討会における整理の各位置情報への簡易なあてはめ　　別紙1

（1） 基地局に係る位置情報

位置登録情報の取得　※1

① 取得した位置情報を（「十分な匿名化」をせずに）利用・第三者提供　※2

・（当該目的で位置情報を取得する前に）利用者の個別かつ明確な同意が必要。
【報告書3．(2)①】

・利用者が同意内容を変更できる手続を設けること。
【報告書3．(4)】

② 取得した位置情報を「十分な匿名化」をして利用・第三者提供

・ウェブページやアプリのプライバシーポリシー等で「十分な匿名化」をした上で利用することについて分かりやすく説明・表示を行う。
【報告書4．(4)①】

・「十分な匿名化」をした上で利用することについてのオプトアウトの手続を設けることが望ましい。
【報告書4．(4)③】

個々の通信の際に利用される基地局の位置情報の取得（通信の秘密に該当する位置情報）　※1

① 取得した位置情報を（「十分な匿名化」をせずに）利用・第三者提供

・（当該目的で位置情報を取得する前に）利用者の個別かつ明確な同意が必要。
【報告書3．(2)①】

・利用者が同意内容を変更できる手続を設けること
【報告書3．(4)】

② 取得した位置情報を「十分な匿名化」をして利用・第三者提供

・「十分な匿名化」をした上で利活用すること等について同意が必要（契約約款等による包括的な同意も可能）。
【報告書5．(2)②ウ】

・「十分な匿名化」をした上で利活用することについて利用者が同意内容を変更できる手続を設けること。
【報告書5．(2)②ウ】

※1　基地局に係る位置情報については、通信を成立させる前提として携帯電話事業者等の電気通信事業者が取得するものであり、これを通信目的で利用することは、正当業務行為及びこれと同等に評価できることから、通信目的での取得・利用については、利用者から同意を取得する必要はない。【報告書3．(2)②】

※2　「匿名化」には、「十分な匿名化」と「（仮称）個人特定性低減データ」の2つの段階があるが、「（仮称）個人特定性低減データ」は、個人情報保護法の改正によって創設される予定の制度であり、現時点においては、「十分な匿名化」を行うことが必要。次頁以降も同様。【報告書4．(2)(3)】

※3　①かつ②（取得した位置情報を匿名化せずに通信目的外で利用・第三者提供することに加え、これとは別目的で位置情報を匿名化して利用・第三者提供する）の場合には、①と②の取扱いをそれぞれ満たす必要がある。

（2） GPS位置情報

GPS位置情報の
取得・利用・第三者提供

・（位置情報を取得する前に）個別かつ明確な同意が必要。【報告書3．(2)①】

・アプリのプライバシーポリシー等で分かりやすく説明・表示も行う。
【報告書3．(3)①】

・利用者の同意内容の変更の手続を設けること。【報告書3．(4)】

GPS位置情報を利用者が
その提供の際の経緯（コンテキスト）
から予測できる範囲でのみ
取得・利用する場合

・契約約款等による包括的な同意が許容される。【報告書3．(2)②】

・アプリのプライバシーポリシー等で分かりやすく説明・表示も行う。
【報告書3．(3)①】

・利用者の同意内容の変更の手続を設けること。【報告書3．(4)】

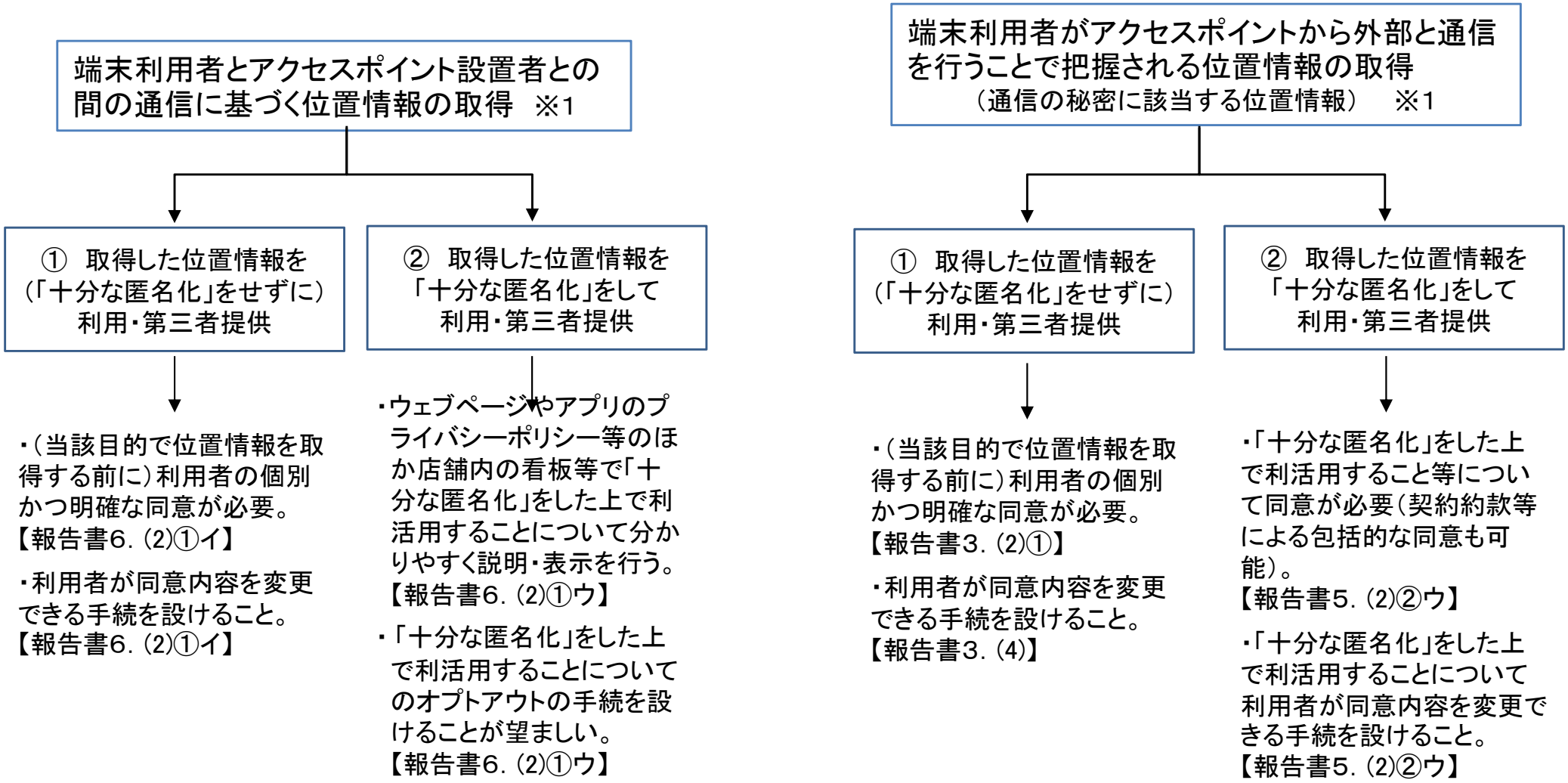
取得した位置情報を
「十分な匿名化」をして
利用・第三者提供する場合

左記の取扱いに加え、

・アプリのプライバシーポリシー等で「十分な匿名化」をした上で利用することも含めて分かりやすく説明・表示を行う。【報告書4．(4)①】

・「十分な匿名化」をした上で利活用することについてのオプトアウトの手続を設けることが望ましい。
【報告書4．(4)③】

（3） Wi－Fi位置情報



※1　Wi－Fi位置情報については、通信を成立させる前提としてアクセスポイント設置者等の電気通信事業者が取得するものであり、これを通信目的で利用することは、正当業務行為及びこれと同等に評価できることから、通信目的での取得・利用については、利用者から同意を取得する必要はない。

※2　①かつ②（取得した位置情報を匿名化せずに通信目的外で利用・第三者提供することに加え、これとは別目的で位置情報を匿名化して利用・第三者提供）の場合には、①と②の取扱いをそれぞれ満たす必要がある。

別紙2

位置情報プライバシーガイド（案）

1．通信サービスにおける位置情報の仕組みについて知りましょう

携帯電話事業者等の電気通信事業者は、通信システムの仕組みを利用して携帯電話やスマートフォンといった通信端末がどこにあるのかを把握することができます。（この通信端末がどこにあるのかという情報をここでは位置情報といいます。）

まずは、電気通信事業者が取り扱う位置情報について、どのようなものがあるのか理解しましょう。

① 基地局に係る位置情報

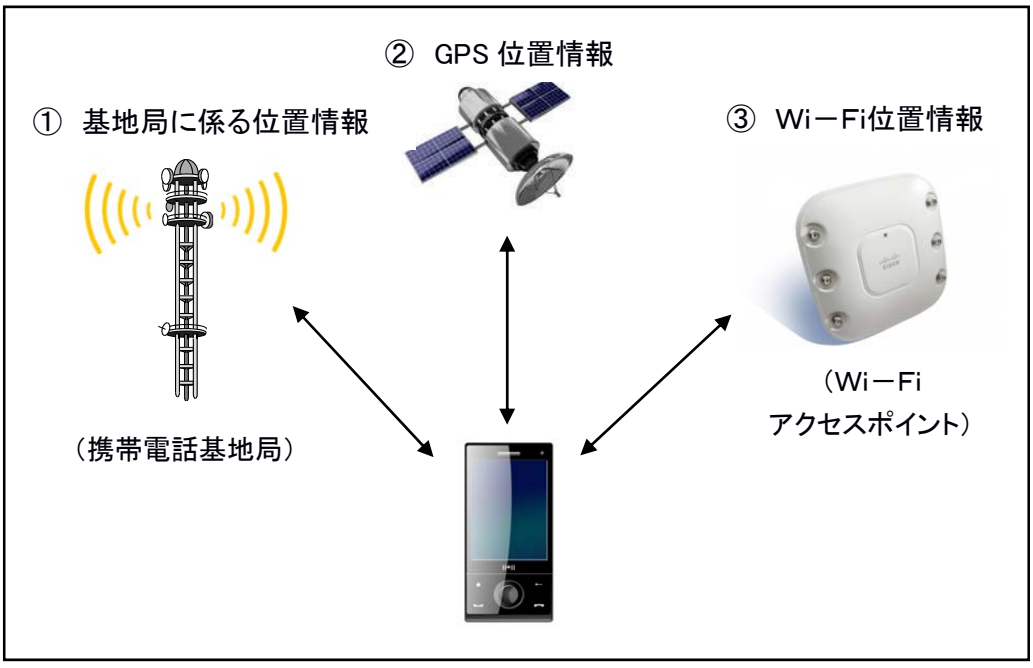
携帯電話事業者等が通話やメール等の通信を成立させる前提として取得している、通信端末がどの基地局のエリア内にいるのかを示す情報です。

② GPS位置情報

複数のGPS衛星から発信されている電波を通信端末が受信して、衛星と端末との距離等から当該端末な詳細な位置を示す情報です。

③ Wi－Fi位置情報

Wi－Fiのアクセスポイントと通信端末間の通信を基に、通信端末がどのアクセスポイントのエリア内にいるのかを示す情報です。



これらの位置情報は、基地局に係る位置情報のように、そもそも通信を成立させるために必要なものや、GPS位置情報のように、利用者が地図ナビゲーションサービスといったサービスを利用する際に必要なものがありますが、電気通信事業者が、これとは別の目的で位置情報を取得・利用・第三者提供する場合もあります。

2. 位置情報の取扱いについて確認しましょう

通信を成立させるための目的以外で、利用者の通信端末の位置情報を取得・利用・第三者提供する場合には、電気通信事業者は、利用者から同意を取得するとともに、その取扱いについて利用者に対し分かりやすく説明・表示することが求められています。

利用者の側でも、通信サービスやアプリケーションの利用の際に、位置情報の取扱いについて同意を求められたときや、位置情報の取扱いについて説明・表示があった場合には、その内容をしっかりと確認することが重要です。

また、Wi－Fi位置情報については、アクセスポイントの設置場所において、位置情報の取扱いについて掲示している場合があります。

【位置情報取得同意画面の例】

電気通信事業者においては、利用者が事後的に位置情報の取得等を停止することができる仕組みを設けている場合があります。位置情報の取扱いについて同意したけれども、後から変更したい場合などには、このような仕組みを利用してください。

また、通信端末から、位置情報の基となる通信機能を使わないよう端末側で設定することもできます。通信端末のGPSやWi－Fiの機能の状況については、通常、通信端末の「設定」のアイコン等から確認することができます。

【Wi－Fi機能の設定画面の例】