

1 Wi-Fi位置情報に関する論点

- Wi-Fi位置情報の性質について
 - ・Wi-Fiの仕様として、端末は、アクセスポイント内に入ること、接続の前提としてMACアドレス等をアクセスポイントに送信するが、これにより電気通信事業者（アクセスポイント設置者）が把握可能となる端末の位置情報
 - ・端末が特定のアクセスポイントと接続することにより、電気通信事業者（アクセスポイント設置者）が把握可能な位置情報
- 上記のWi-Fi位置情報と他の位置情報の取扱いの違いについて 等

<主な意見>

【Wi-Fi位置情報の性質】

- Wi-Fiの仕様上、Wi-Fi端末は定期的にプローブ要求というMACアドレスを含んだ信号を発信しており、その信号の強度や到達時間差を複数のアクセスポイントから測位することで、Wi-Fi端末とアクセスポイントの相対的な位置を推定することが可能。
- Wi-Fi端末からアクセスポイントに対して発信されるプローブ要求は、Wi-Fiを利用するために仕様として行われるものであり、停止するためには端末上でWi-Fiの機能をオフにするしかない。
- 個人情報保護法の改正に向けた見直し方針においては、保護されるパーソナルデータの範囲は「実質的に個人が識別される可能性を有するもの」とされ、実質的に個人を一意に識別することに利用されるIDのようなものが入ってくる。MACアドレスもここに入ってくる可能性がある。
- 利用者がアクセスポイントに接続することで、事業者が利用者のいるエリアを把握し、利用者に対してそのエリアに応じた情報を伝えるようなWi-Fiサービスの場合、利用規約等に位置情報を取り扱う旨を記載することで、サービス利用開始時に利用者から同意をとることが可能。

【Wi-Fi位置情報の取扱いについて】

- Wi-Fi位置情報の取扱いについて検討するに当たっては、Wi-Fiサービス提供者が、MACアドレスと他の契約者情報等を紐づけることが可能な状態にあるのかどうかについても考慮に入れるべき。
- MACアドレスはIDとしての識別性が高いため、その取扱いについて検討するに当たっては特別な配慮が必要なのではないか。
- （識別性が高いため）MACアドレスは、収集後すぐに廃棄されるか、もしくは安全に管理される必要がある。オプトインする場合には、ユーザーに対してMACアドレスの性質や事業者内においてどういう情報と突合するのか等について明らかにされる必要があると思うが、これはとても難しい問題。
- MACアドレスは、識別できる情報であって、特定できる情報かどうかはグレーゾーンだと思うが、それを保存すること自体が問題なのか、それとも保存すること自体は問題なくてその後の取り扱いの在り方が問題になるのかという点は整理すべき課題の1つ。
- 通信することを目的としてWi-Fi端末-アクセスポイント間でやりとりされているMACアドレスが、利用者の知らないところで通信以外の目的のために収集・利用されていることには問題があるのではないか。
- 事業者においては、MACアドレスをアノニマイズやハッシュ化して、時間軸でマッチングできないようにするという形での配慮が考えられる。
- オプトアウトの仕組みとして、事業者のウェブページ等において利用者に自分のMACアドレスを入力してもらい、事業者側で当該MACアドレスのデータを消去するという形が考えられる。
- 防犯カメラとのアナロジーで考えると、（MACアドレスを取得していること等について）何らかの形で街頭表示するといったことが必要なのではないか。
- MACアドレスが取得されること自体は仕様だが、その情報をパーソナライズドサービスに使う際の同意の取り方やオプトアウトの仕組みについてはしっかりと考えていくべきではないか。

1 Wi-Fi位置情報に関する論点

<主な意見(前頁の続き)>

【他の位置情報との取扱いの違いについて】

- 今後の技術進展によりどのような位置情報として出てきても、対応が可能となるような議論が必要。その点で、2点目の他の位置情報の取扱いとの違いについては重要。

【利用者に対する周知啓発について】

- 利用者は、(通信さえしていなければ)Wi-Fiの電波を切ったつもりで、実際には電波が出ていることを理解していない人も多い。事業者側と利用者側で意識のギャップが大きいと思う。関係者が協力して利用者への説明や対応を行い、ギャップを埋めていくことが必要ではないか。

【MACアドレスの取扱い及び特徴について】

- (位置情報の問題とは別に)MACアドレスの取得・保存の問題を考えるべきではないか。
- 「MACアドレスの取得は、Wi-Fiの仕様である」とするのはミスリーディングではないか(通常のWi-Fi通信の利用の仕方と、一定の期間の保存を伴う利用の仕方は区別されるべき。通常のWi-Fi通信に伴って生じる親機による一時的な取得は、保存を伴わないので、トラッキング、名寄せ、漏えい等の問題は生じない。)
- MACアドレスは、端末を変更しない限り、不変であるとの特徴を有するため、①長期間のトラッキングや名寄せの可能性、②(cookieとは異なり)事業者を横断する情報統合の可能性があるのでないか。

2 位置情報の取扱いに関する論点

- 位置情報の取扱い（利用者に対する説明・表示、同意取得、第三者提供等）の在り方について
 - ・利用者に対する説明・表示の在り方
 - －説明すべき項目（取得する位置情報の種類／精度／利用目的／第三者提供先／取得頻度／保存期間 等）
 - －説明の表示方法
 - ・位置情報の取得及び第三者提供に関する同意取得の在り方（包括的又は明示的な同意、同意取得時期・表示方法 等）
 - ・位置情報の取得及び利用の中止等利用者関与の在り方
 - ・位置情報の性質を決める要素（通信の秘密に含まれるか否か／精度／継続的な取得・利用等）に応じて取扱いに差異を設けるべきか。
 - ・位置情報を取り扱う主体や利用目的に応じて考慮すべき事項 等

<主な意見>

【利用者に対する説明・表示】

- 医療におけるインフォームドコンセントの場面や、金融取引で金融商品を販売する場面では、同意の前の説明が問題になる。特に金融取引の場面では、契約を締結することに対する意思は認められるが、事業者側の説明が足りないということで、義務違反があるという責任の問われ方をする。個別に同意取得するときでも、位置情報取得に伴うリスクや負担を理解できる程度の説明はしておくことが望ましい。
- 位置情報として、何を取得して利用するのか、位置だけではなく機器番号情報(MACアドレス)を取得すること、必要以上の情報を取得しないことなどを透明化して利用者にわかるようにすべき
- 位置情報を取得する場合に保存期間を明示することは重要。利用者に説明された目的で通常考えられる保存期間とはかけ離れて無期限に保管し、全く異なる目的で使用することは正当ではない。
- 同意なく利用できる情報もあるかもしれないが、一方で、どうして同意なく利用できるのかということについて最低限の説明をする必要があるのではないか。

【同意取得】

- スマートフォンプライバシーイニシアティブにおいては、GPS等の位置情報について、アプリケーションで利用することが明らかでない場合について、取得の際に同意をとることが原則とされている。これは、特にスマートフォンデバイスのように持ち歩く、自分の体に近いものについて、同意がとれるときには取得の同意をとるべきという趣旨と解され、1つの考え方の出発点になる。
- 位置情報を取り扱うに当たっての有効な同意があったと言うためには、自分が位置情報を取得されることに同意しているとの認識があった上で同意ボタンを押すというのが基本的な原則ではないか。
- 約款を使った契約は、同意取得としての実質は弱いという議論が一般的にされている。約款に書かれた文言が合意内容になるのは、この契約を結べば自分には当然にこういう義務や負担が発生するのではないかと、ある程度予測ができれば、読んでいない約款であっても、当事者が義務や負担を負うという考え方。そうすると、このサービスを利用すると、自分は当然に位置情報を取得されると予測がつくサービスの利用規約に同意をした場合には、位置情報取得の同意があるといえるかもしれない。
- 民法上、事前の同意が全く認められないところで、オプトアウトの仕組みを作っても、同意があったとは評価できない。
- 位置情報取得の同意というのは、いつでも撤回可能とされているようなものであり、個別同意を継続的に与えていると評価できる状況を作り出す必要があるのではないか。

3 位置情報の加工（いわゆる匿名化）に関する論点

- 位置情報を特定の個人が識別できないように加工するにはどのような手法が考えられるか。加工により個人の特定性、識別性が一定程度低減された位置情報について、どのように取り扱うのが望ましいか。
（パーソナルデータに関する検討会技術ワーキンググループ報告書等を踏まえ検討）
 - ・ 位置情報に対する非特定化、非識別化または非識別非特定化措置の検討
 - ・ 既に行われている加工手法に関する評価
 - ・ 低減の程度に応じた取扱い方法に関する検討
 - ・ 第三者提供に際して提供者及び受領者の取扱いにおいて考慮すべき事項
 - ・ 匿名化した場合における適切な取扱いについて 等

<主な意見>

【パーソナルデータに関する検討会技術ワーキンググループでの議論】

- 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においては、本人同意を不要とする2通りの第三者提供が考えられた。1つは、新たな法的措置を前提とした第三者提供。これは、情報を匿名化しても、一般的には個人識別に関するリスクが残ることから、本人の特定性、識別性を困難にした上で、新たな法的措置とセットにすることで、本人同意なしで第三者提供を可能とするモデル。もう1つは、不特定多数への公表を含む第三者提供で、特定や識別のリスクが極めて低い形に加工されたものに限られるべきである。
- 新たな法的措置を前提とした第三者提供について、FTC3要件を念頭に検討されたが、2番目の提供者が識別化しないことを約束・公表するという要件、3番目の契約において提供者、受領者間で識別化等を禁止するという要件について立法措置が必要でないかとされている。
- どこまで匿名化した情報であれば、新たな法的措置を前提とした第三者提供の対象になるという水準についてはこれからの検討となっている。情報の性質によって違いがあることも考えられる。
- 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では、汎用的な匿名化の手法はないということだったが、データベースが決まって、利用方法が決まればやりようはあるという結論だったと思う。本検討会においては、位置情報を含んだデータベースをこう使うのであれば、こういう匿名化ができるということは、時間をかけて検討する意味があるのではないか。

3 位置情報の加工(いわゆる匿名化)に関する論点

<主な意見(前頁の続き)>

【個人の特定性、識別性が一定程度低減された位置情報について】

- 第三者提供で識別をすることはできなくなってしまうと、使う側からすると非常にきつい制約になってしまい、社会に付加的な価値を生み出すことができない。新たな法的措置を前提とした第三者提供の枠組みというのは非常に重要。
- 研究目的等で位置情報を利用する場合、個人を特定する必要性はほとんどない。他方で、識別性を落としてしまうと、データとしては役に立たない場合がある。
- 保護される情報の範囲を明確にして、例えば識別非特定情報についても法の保護の対象とした上で、それは正当な目的があって、その目的との関係でバランスがとれた利用、提供の仕方であれば違法性はないという形で、段階を取り分けて物事を考えたほうが、わかりやすいのではないか。
- 公衆衛生や都市計画等の分野では、(経年変化を見るため)長期間にわたってのデータの取得が必要となるため、利用目的を達しつつ(識別化の)リスクをできるだけ下げるための識別化防止措置を柔軟に作れるようにすることが重要ではないか。
- 個人の特定性、識別性が一定程度低減された位置情報であっても、当該データにより明らかに個人が特定できる情報は削除されるべき。

【加工手法等】

- 生活圏に関する情報は、ニーズがある一方で、個人の特定のおそれがあり、利用に当たってはプライバシーに対する配慮とのバランスが課題。
- 蓄積したデータというのは個人の動線ではなく、集団の動線の分析という形で最終的に加工することが必要だと思うが、データの取得の時間、場所を必要最小限にするであるとか、IDの変換、特に継続的にいつまでの分をとるのかを明示する等、しっかりとルール化していく必要があるだろう。
- どのような特定性、識別性が必要かということは、取り扱う主体や利用する目的との関係で決まってくる。一律に識別性を落とさなければならないということになると、ケースによっては全く意味がない場合がある。
- 事例を通して、あるデータをとるためにはこれぐらいの精度でこれぐらいの期間位置情報を取得することが必要といった類型をスタディできるとよい。

【適切な取扱いについて】

- 匿名化の加工がなされていたとしても、利用者への透明性や本人の関与の確保の観点からは、オプトアウトの手続きが必要ではないか。
- 匿名性を実現すると、複数人が位置的には区別不能になるが、範囲内の他の個人や施設にいると間違えられるケースもあるため、匿名化が引き起こす問題(例:他の施設にいると間違えられるのを避けたいために当該地域にアクセスしなくなると地域分断を引き起こすおそれがある。)についても考慮する必要があるのではないか。

本検討会における論点とこれまでの構成員等のご意見

4 通信の秘密に該当する位置情報に関する論点

- 通信の秘密に該当する位置情報を特定の個人が識別できないように加工することは、電気通信事業法上の通信の秘密の侵害に該当しうるのか。
この場合の、特定の個人が識別できないように加工することについての有効な同意取得の在り方。

<主な意見>

- CDRは、通信の秘密に該当するため個別かつ明確な同意が必要であり、仮にそれを利用した場合には、現状では窃用に当たると理解。仮にこういったものを利用していくときに、一定の条件を付すことによって利用可能と整理することはできないか。
- 個別の同意を事前に取得して位置情報を利用する場合、サンプルの確保が課題となり、ビッグデータとしての利活用を推進することは難しい。特に通信の秘密に含まれる位置情報について、包括同意でも利用が可能になると、活用の幅が広がり、自治体等のニーズに応えられるようになる。

5 その他

<主な意見>

【基本原則】

- これまで整理されてきたパーソナルデータの取扱いに係る基本原則を踏まえつつ、位置情報として必要な部分もあわせて考えていくことが必要。
- 情報取得の段階から最後の利用の段階まで、どれだけ透明性を持たせられるのかというところが、これからの発展につながるのではないか。

【位置情報の性質、主体、目的に応じた取扱い】

- 緊急時の取扱いの検討の視点からは、位置情報の性質、主体、目的によって、その取扱いに当たって必要な条件(方法)が異なってくるのではないか。
- 位置情報のプライバシーに係る裁判事例として、Nシステムの裁判事例では、公道での写真撮影というかなり粗い集め方であっても、裁判所はそのプライバシーの懸念を明らかにしている。裁判所はどのように適法性を判断するかというと、まずは取得される情報の性質がどのようなものかということ、それから、その情報取得、保有、利用する目的がどうか。それから、取得、保有、利用の方法がどうか。これを総合して判断するとしている。
- 現状の個人情報保護法でも第23条第1項第2号において、人の生命、身体又は財産の保護のために必要がある等の場合は第三者提供に伴う本人同意が不要となっており、災害時の取扱いについても法令で措置することが考えられる。

【検討に当たっての視点】

- 各項目を検討する際の視点として、国際的調和の観点も重要。
- プライバシーに関する意識は、国(社会)によって違いがあることも踏まえる必要。

【情報の適切な管理について】

- そもそも自分の位置情報を他人に知られたくない、あるいは気持ち悪いということ自体を解決するのであれば、秘密計算技術といった暗号技術を活用することで、分析者がデータを見ないで統計分析をできる等、高いプライバシー保護が実現できるのではないか。