

参考資料集

I 個人情報保護法・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抜粋

○ 個人情報の保護に関する法律

(利用目的の特定)

第十五条 個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。

2 個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。

○ 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

(利用目的の特定)

第5条 電気通信事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定するものとする。

2 電気通信事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行わないものとする。

3 前2項の規定により特定する利用目的は、電気通信サービスを提供するため必要な範囲を超えないものとする。

○ 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解説

(1) 本条は、個人情報の適正な取扱いを実現するための前提として、電気通信事業者に対して、その利用目的をできる限り特定させるとともに、その変更も一定の合理的な範囲に留めるものとする。こと、及び、利用目的が電気通信サービスを提供するため必要な範囲を超えないものとするを規定するものである。なお、本条や次条等の個人情報の「利用」とは、第15条の第三者への提供を含む概念である。

(2) 「その利用の目的を…できる限り特定」するとは、個人情報がどのような目的で利用されるかをできるだけ具体的に明確にするという趣旨である。したがって、単に「サービスの提供のため」や「業務の遂行のため」といった抽象的な目的では足りず、例えば、「加入者の本人確認、料金の請求、料金・サービスの変更及びサービスの休廃止の通知のため、加入者の氏名、住所、電話番号を利用します。」のように具体的に特定すべきである。

なお、個人情報に対して、特定の個人を識別できないようにする加工（いわゆる匿名化）を行うことは、個人情報の利用に当たらず、利用目的として特定する必要はない。

○ 個人情報の保護に関する法律

(利用目的による制限)

第十六条 個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。

○ 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

(利用目的による制限)

第6条 電気通信事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱わないものとする。

4 前項の規定にかかわらず、電気通信事業者は、同項各号に掲げる場合であっても、利用者の同意がある場合その他の違法性阻却事由がある場合を除いては、前条の規定により特定された利用目的の達成の範囲を超えて、通信の秘密に係る個人情報を取り扱わないものとする。

○ 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解説

(1) 本条は、電気通信事業者に対して、個人情報の取扱いを利用目的の達成に必要な範囲内に限ることにより、無限定な個人情報の取扱いを排除することを通じて、本人の権利利益侵害を防止しようとするものである。

「個人情報の取扱い」とは、個人情報に関する一切の行為を含む概念であることから、何が「必要な範囲」かについては、様々な側面からこれを判断する必要がある。すなわち、個人情報の取扱いの手段、方法はもちろん、取り扱う個人情報の内容、量等についても、必要な限度を超えないことが必要である。したがって、利用目的に照らして過剰な個人情報の取得も本条によって規制されることになる。例えば、加入者の本人確認のために、加入者の収入や学歴等は必要とはいえず、取得は制限される。

(4) 第4項の規定は、第3項各号の規定の適用がある場合であっても、個人情報が通信の秘密にも該当する場合には、通信当事者の同意なき利用は、違法性阻却事由がある場合を除き許されないことについて念のため確認する趣旨の規定である。

○ 個人情報の保護に関する法律

（取得に際しての利用目的の通知等）

第十八条 個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。

2 個人情報取扱事業者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電子的方式、磁気的方式その他の知覚によっては認識することができない方式で作られる記録を含む。以下この項において同じ。）に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示しなければならない。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。

3 個人情報取扱事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。

4 前三項の規定は、次に掲げる場合については、適用しない。

四 取得の状況からみて利用目的が明らかであると認められる場合

○ 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

（取得に際しての利用目的の通知等）

第8条 電気通信事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表するものとする。

2 電気通信事業者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電子的方式、磁気的方式その他の知覚によっては認識することができない方式で作られる記録を含む。以下この項において同じ。）に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示するものとする。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。

3 電気通信事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表するものとする。

4 前三項の規定は、次に掲げる場合については、適用しない。

四 取得の状況からみて利用目的が明らかであると認められる場合

○ 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解説

(1) 本条は、電気通信事業者に対して、利用目的を通知・公表させることにより、本人の不安感を緩和するとともに、本人自らが必要な注意を払うための契機を提供することにより、本人の権利利益侵害を予防しようとするものである。

(2) 「通知」とは、例えば、郵便、電話、電子メール等によって利用目的を知らせることが想定される。「公表」とは、例えば、インターネット上での公表、パンフレットの配布、事業所の窓口等への書面の掲示・備付け等が想定される。

(3) 第2項は、契約や調査等のため、書面やコンピュータを用いて直接本人から個人情報を取得する場合には、個人情報を取得した後に利用目的を通知・公表することで足りることとはせず、原則として取得前に本人に対して利用目的を明示するものとするものとするものである。明示の方法としては、契約締結時に契約内容を説明する書面に利用目的を記載し、それを契約締結前に交付して示すことなどが想定される。

同項ただし書は、人の生命、身体又は財産の保護のために緊急に必要がある場合にまで、あらかじめその利用目的を明示するものとすることは合理性に欠けることから、このような場合には、取得前の明示は免除するものである。なお、このような場合には、第1項の規定に従って、取得後速やかにその利用目的を通知・公表するものとするものとなる。

(4) 第3項は、利用目的を変更した場合にも通知・公表する必要があることを確認的に規定しているものである。なお、この場合の「利用目的の変更」は、第5条第2項に規定する「変更前の利用目的と相当の関連性を有すると合理的に認められる範囲」内で行わなければならないことは当然である。

○ 個人情報の保護に関する法律

（第三者提供の制限）

第二十三条 個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

- 一～四 （略）
- 2 個人情報取扱事業者は、第三者に提供される個人データについて、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。
 - 一 第三者への提供を利用目的とすること。
 - 二 第三者に提供される個人データの項目
 - 三 第三者への提供の手段又は方法
 - 四 本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。
- 3 個人情報取扱事業者は、前項第二号又は第三号に掲げる事項を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。
- 4 次に掲げる場合において、当該個人データの提供を受ける者は、前三項の規定の適用については、第三者に該当しないものとする。
 - 一 個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託する場合
 - 三 個人データを特定の者との間で共同して利用する場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。
- 5 個人情報取扱事業者は、前項第三号に規定する利用する者の利用目的又は個人データの管理について責任を有する者の氏名若しくは名称を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

○ 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

（第三者提供の制限）

第15条 電気通信事業者は、次の各号のいずれかに該当する場合を除くほか、あらかじめ本人の同意を得ないで、個人情報を第三者に提供しないものとする。

- 一～四 （略）
- 2 電気通信事業者は、第三者に提供される個人情報について、本人の求めに応じて当該本人が識別される個人情報の第三者への提供を停止することとしている場合であって、次に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にかかわらず、当該個人情報を第三者に提供することができる。
 - 一 第三者への提供を利用目的とすること。
 - 二 第三者に提供される個人情報の項目
 - 三 第三者への提供の手段又は方法
 - 四 本人の求めに応じて当該本人が識別される個人情報の第三者への提供を停止すること。
- 3 電気通信事業者は、前項第2号又は第3号に掲げる事項を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くものとする。
- 4 次に掲げる場合において、当該個人情報の提供を受ける者は、前3項の規定の適用については、第三者に該当しないものとする。
 - 一 電気通信事業者が利用目的の達成に必要な範囲内において個人情報の取扱いの全部又は一部を委託する場合
 - 三 個人情報を特定の者との間で共同して利用する場合であって、その旨並びに共同して利用される個人情報の項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人情報の管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。
- 5 電気通信事業者は、前項第3号に規定する利用する者の利用目的又は個人情報の管理について責任を有する者の氏名若しくは名称を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くものとする。
- 6 電気通信事業者は、個人情報を第三者に提供するに当たっては、通信の秘密の保護に係る電気通信事業法第4条その他の関連規定を遵守するものとする。

○ 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解説

- (1) 第1項は、個人情報とは、原則として本人の同意なく、第三者に提供できないことを規定したものである。ただし、自己又は他人の権利利益や社会公共の利益のために第三者提供が要請される場合もあるので、そうした場合を第1項各号に例外として定めている。
- (2) 「本人の同意」については、個別の同意がある場合だけでなく、電気通信サービスの提供に関する契約約款において、個人情報の第三者提供に関する規定が定められており、当該契約約款に基づき電気通信サービス提供契約を締結している場合、当該規定が私法上有効であるときも、「本人の同意」がある場合と解される。
- この理は、契約約款が変更される場合も変わりはないので、契約約款の変更により個人情報の第三者提供に関する規定が設けられた場合であっても、当該変更が私法上有効であり変更前に契約締結を行った当事者にも変更後の規定が効力を有すると判断される場合には、「本人の同意」がある場合と解される。
- なお、同意は有効なものでなければならないので、民法（明治29年法律第89号）第90条の公序良俗に反する場合や同法第95条の要素の錯誤がある場合、消費者契約法（平成12年法律第61号）第10条の消費者の利益を一方的に害するものとされる場合など同意が私法上無効とされる場合は、有効な同意があるとは言えないので、同意がある場合とは言えないことは当然である。
- また、無制限に第三者提供を認める規定等契約約款の規定が、利用者の利益を阻害していると認められるときは、電気通信事業法上の業務改善命令の対象となりうる。
- (7) 第2項及び第3項の規定は、個人情報保護法第23条第2項及び第3項と同様の規定であり、いわゆるオプトアウトの仕組みによる第三者提供を認めたものであるが、電気通信事業者が加入者の個人情報を第三者提供する場合は、契約約款により本人の同意を得て行うことが一般的に可能である（上記(2)参照）ので、基本的には本人の同意を得て行うこととすることが望ましいと考えられる。ただし、契約約款により本人の同意を得て行う場合でも、電話帳に掲載する場合など本人の意思をできるだけ尊重すべきものについては、本人の申出により提供を停止するという扱いにすることが望ましい。
- (8) 第4項第1号については、現在、民間企業等においては、顧客情報等大量の個人情報を利用するために必要となる編集・加工等の処理を他の企業に委託することが一般化しつつある。こうした取扱いを第三者提供とした場合、第1項に基づき、処理される個人情報の本人に対し個々に同意を取る必要が生じることとなり、事実上委託行為自体が不可能となるおそれがある。一方、電気通信事業者が個人情報の取扱いを委託した場合には、第12条により、適切な委託先を選定し、委託先に対し必要かつ適切な監督を行う責任が生じ、これらの責任を果たしていない結果、問題が生じた場合には委託元である電気通信事業者も責めを負うこととなる。これらの事情を勘案し、電気通信事業者が利用目的の達成に必要な範囲内で個人情報の取扱いを委託する場合には、電気通信事業者が行う取扱いの一部とみなし、委託先は第三者には該当しないこととしている。なお、一般に個人情報の処理を委託され、その成果物たる処理データを委託元に返すような場合は、そもそも第三者への提供であるとは解されない。
- (10) 第4項第3号及び第5項については、個人情報保護法第23条第4項第3号及び第5項と同様の規定であり、これらの規定を満たす形で特定の者との間で個人情報を共同利用することは本人の同意なく行うことができることを認めたものであるが、電気通信事業者が加入者の個人情報を共同利用する場合は、契約約款により本人の同意を得て行うことが一般的に可能である（(2)参照）ので、基本的には本人の同意を得て行うこととすることが望ましいと考えられる。ただし、契約約款により本人の同意を得て行う場合でも、不払い者等情報の交換の場合のように、本人の権利利益に重大な影響を及ぼす可能性がある情報を交換する場合などには、第4項第3号に掲げられている情報をあらかじめ本人に通知又は本人が容易に知り得る状態に置くなどの措置をとり、本人の権利利益を不当に侵害することのないようにすることが求められる。なお、「本人が容易に知り得る状態に置く」とは、公表が継続的に行われている状態をいい、具体的には、ホームページへの掲載、官報・新聞等への継続的な掲載、事務所の窓口等への書面の掲示・備え付け等の措置をとっていることをいう。
- (11) 第6項の規定は、第1項から第5項までの規定の適用により第三者提供（第4項各号の規定により提供する場合を含む。）が認められる場合であっても、個人情報が通信の秘密にも該当する場合には、通信当事者の同意なき第三者提供（同上）は違法性阻却事由がある場合を除き許されないことについて念のため確認する趣旨の規定である。

○ 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 (位置情報)

第26条 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（移動体端末を所持する者の位置を示す情報であって、発信者情報でないものをいう。以下同じ。）を他人に提供しないものとする。

2 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には、利用者の権利が不当に侵害されることを防止するため必要な措置を講ずるものとする。

○ 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解説

(1) 本条でいう「移動体端末」とは、移動電話端末（端末設備等規則（昭和60年郵政省令第31号）第2条第2項第5号）及び無線呼出端末（同規則第2条第2項第7号）のほか、広く電波等を用いて通信を行うために用いられる端末をいう。また、本条にいう「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をいい、利用明細に記載される着信地域（単位料金区域等）のようなものは含まない。）をいい、端末設備等規則第22条にいう位置情報よりも広い概念である（なお、発信者の位置を示す情報については、前条にその取扱いが規定されているため、位置情報の定義からは除いている。）。電気通信事業者が保有する位置情報は、個々の通話に関係する場合は通信の構成要素であるから電気通信事業法第4条第1項の通信の秘密として保護されると解される。これに対し、通話時以外に移動体端末の所持者がエリアを移動するごとに基地局に送られる位置登録情報は通話を成立させる前提として電気通信事業者に機械的に送られる情報に過ぎないことから、サービス制御局に蓄積されたこれらの情報は通信の秘密ではなく、プライバシーとして保護されるべき事項と考えられる。位置情報を通信の秘密に該当しないと解する場合であっても、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。したがって、外部提供できる場合も通信の秘密の場合に準ずることとした。

(2) 位置情報サービスを自ら提供し、又は第三者と提携の上提供するに当たっては、その社会的有用性と通信の秘密又はプライバシー保護とのバランスを考慮して、電気通信事業者は、利用者（ここでは当該移動体端末の所持者を指す。）の権利が不当に侵害されないよう必要な措置を講じなければならないものとした。「必要な措置」の具体的内容としては、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第三者と提携の上サービスを提供する場合は、提携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。

①の利用者の意思に基づく位置情報の提供に関し、利用者からの同意取得は、個々の位置情報の提供ごとのほか、サービス提供開始時などに事前に行うことも可能である。もっとも、同意取得は移動体端末の操作や書面による確認などの方法により明確に行うべきであるほか、全くの包括的な内容の同意を得ることは適当でなく、位置情報を提供する者の範囲を特定しておくなどすることが望ましい。また、事前の同意は原則として撤回できなければならない。

②の利用者の認識・予見可能性の確保については、画面表示や移動体端末の鳴動等の方法により、位置情報が提供されることを認識できることを可能とすることなどが考えられる。また、合理的な期間、利用者が履歴を確認できるようにすることや、利用者が誤って位置情報を送出することを防止するため、提供されるサービスや移動体端末の機能等について、十分な周知・注意喚起を行うことが望ましい。

③の位置情報の取扱いについては、権限を有しない者が移動体端末の位置情報のモニターができないよう、暗証番号の設定、アクセス端末の限定等の措置が考えられるほか、他の電気通信事業者等が位置情報サービスを提供する場合等において、自社の管理する基地局情報が他者に不当に利用されることのないよう、基地局情報の管理について規程を設けるなどが考えられる。また、GPSによる位置情報など、電気通信サービスの提供に必要な位置情報は、原則として利用者の意思に基づかずに取得してはならない。

④の第三者と提携の上でのサービス提供については、提携に関する契約に係る約款等において、第三者において上記のようなプライバシー保護措置が確保されることを担保することや、利用者のプライバシーが不当に侵害されていると判断される場合には、位置情報の提供を停止できるようにしておくことなどが考えられる。

II 電気通信事業者の取組事例

「モバイル空間統計」とは

- ・電気通信サービスを提供する過程で発生する運用データを、社会の情報基盤の構築・整備を目的として統計化した特定の個人を識別できない情報をいう。
- ・モバイル空間統計により、地域毎の人口の分布(人口分布)や、性別・年齢層別・居住エリア別の人口の構成(人口構成)などを推定することが可能。
- ・モバイル空間統計は、集団の人数のみをあらわす人口統計情報であるため、モバイル空間統計から個人を特定することはできないとされている。

「モバイル空間統計」の作成プロセス

①電気通信サービスを提供する過程で発生する基地局のエリア毎に所在する携帯電話番号及び契約者の属性情報を収集(運用データ)



②非識別化処理: 運用データ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。



③集計処理: 非識別化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。



④秘匿処理: 少人数エリアの数値を除去(統計的に少数であることで個人を推測されやすくなる場合があるため)

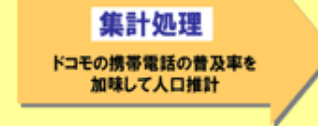
モバイル空間統計



モバイル空間統計

(40歳台男性)

75人	120人	30人
90人	135人	105人
45人	60人	データ無し



秘匿処理 少人数の除去

(40歳台男性)

75人	120人	30人
90人	135人	105人
45人	60人	6人

推計人口

「モバイル空間統計」の特性

対象エリア

全国市区町村役場を100%カバー ※ドコモのサービスエリアに依存

エリアの粒度

500mメッシュ(都市部)～数kmメッシュ(郊外) ※ドコモ基地局の設置間隔に依存

時間帯の頻度

1時間毎で継続的 ※ドコモ基地局がエリア内の携帯電話を把握する頻度に依存

対象年齢層

15歳～79歳 ※十分なサンプル数が確保できる年齢層が対象

「モバイル空間統計」の取組

- ◆有識者研究会(※)を開催し、モバイル空間統計の社会・産業の発展に寄与する利活用のあり方についての検討を実施。
(※)モバイル社会研究所「モバイル空間統計による社会・産業の発展に関する研究会」(座長:堀部政男・一橋大学名誉教授)
- ◆平成22年11月以降、自治体等による各種実証実験を実施。実証事件の結果、モバイル空間統計により、人口分布や人口構成の把握が容易になり、自治体の振興計画や防災計画等の作成・立案に活用できることを確認(⇒平成25年10月実用化)
- ◆モバイル空間統計に関する情報を、報道発表、公式ホームページ、および請求書同封冊子を通じて提供し、モバイル空間統計の概要、有用性、安全性を周知
- ◆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」を作成し、公式ホームページにて公開
- ◆携帯電話契約者の希望により運用データを「モバイル空間統計」から除外する「利用停止手続」を行うことを可能としている。

1. 本ガイドラインの目的

本ガイドラインは、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ることを目的とします。

2. 用語の定義の目的

本ガイドラインの用語の意味は、次のとおりとします。

モバイル空間統計

電気通信サービスを提供する過程で発生する運用データを、社会の情報基盤の構築・整備を目的として統計化した特定の個人を識別できない情報をいいます。公共分野、学術研究分野、産業分野などを提供先として想定し、運用データの一部である位置データおよび属性データに、非識別化処理、集計処理、秘匿処理を行うことにより作成します。

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います。

位置データ

運用データの一部であり、携帯電話などの位置を示すデータであって、データが生じた時刻など、付随する情報を含むものをいいます。

属性データ

運用データの一部であり、電気通信サービスの契約などに際し、契約者から提供されるデータをいいます。

非識別化処理

運用データ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います。

非識別化情報

非識別化処理により得られる情報をいいます。

集計処理

非識別化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います。

集計結果

集計処理により得られる情報をいいます。

秘匿処理

集計結果に小人数エリアの数値が含まれないようにする処理をいいます。

3. モバイル空間統計の作成・提供に関する基本原則

(1) モバイル空間統計は、第4項ないし第7項に定める作成手順に従い、電気通信サービス利用者個人が特定されない統計的な情報として作成します。

(2) モバイル空間統計は、第8項に定める提供方針に従い提供します。

4. モバイル空間統計の作成手順

- (1) モバイル空間統計は、運用データに非識別化処理、集計処理、秘匿処理を行うことにより作成します。
- (2) モバイル空間統計として提供されるデータは、上記3段階の処理すべてが行われたものとします。
- (3) モバイル空間統計を作成するに当たり、上記3段階の処理は、自動的に行われるものとし、そのシステムは関連する社内規程に従って管理します。

5. 非識別化処理

- (1) 非識別化処理では、氏名や電話番号、生年月日などの識別情報を取り除くとともに、集計処理用の不可逆符号を付与します。
- (2) 上記集計処理用の不可逆符号の生成に当たっては、不可逆符号からの識別情報の復元を防止するため、安全な一方向性関数を用います。
- (3) 上記一方向性関数としては、例えば、国内外の評価プロジェクトや評価機関により推奨されているハッシュ関数に基づく、鍵付ハッシュ関数を用います。
- (4) 鍵付ハッシュ関数に係る鍵は、内部での鍵管理者を別にするなど、厳格な運用管理体制を敷きます。

6. 集計処理

- (1) 集計処理では、非識別化情報を集計することにより、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の統計的な推計を行います。
- (2) 集計処理により得られる集計結果は、第5項における集計処理用の不可逆符号を含まないものとします。

7. 秘匿処理

- (1) 秘匿処理では、集計結果から小人数エリアを取り除く処理を行います。
- (2) 秘匿処理は、公的統計での採用事例や国内外の技術開発動向を参考に、集計結果の有用性および個人特定防止の観点から適切な手法を用いて実施します。

8. モバイル空間統計の提供

- (1) モバイル空間統計の提供に当たり、提供時の契約条件において公序良俗に反する利用を禁止するとともに、利用目的を定めるものとします。
- (2) 提供先によるモバイル空間統計の公開や再提供については、提供時の契約条件により定めるものとします。

9. 従業員および業務委託先に対する管理措置

- (1) モバイル空間統計の作成および提供に係る組織の情報管理責任者（以下、管理責任者という。）は、モバイル空間統計を取扱う社員等に対し、本ガイドラインに基づく安全管理が図られるよう、必要かつ適切な監督を行います。
- (2) モバイル空間統計の作成および提供に係る業務を業務委託する場合、管理責任者は、当該モバイル空間統計の安全な管理が図られるよう、当該委託先に対して必要かつ適切な監督を行います。

10. 運用データ利用停止手続

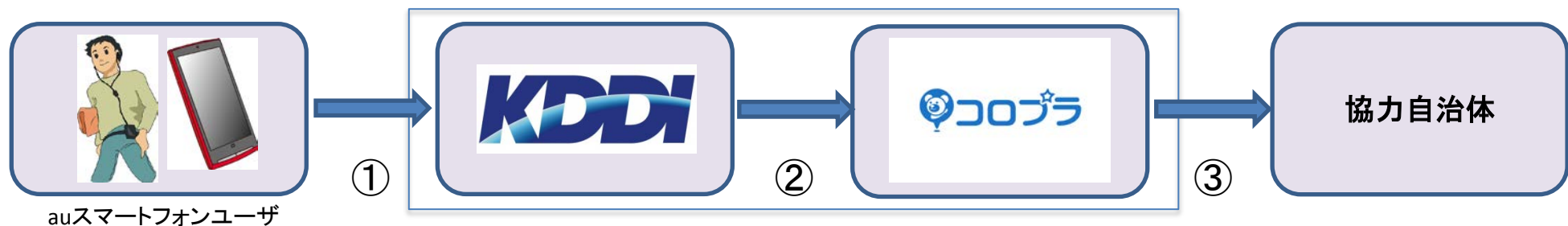
- (1) お客様から、モバイル空間統計への運用データの利用を停止するようお申し出があった場合、当該お客様について、運用データの利用を停止します。
- (2) 運用データの利用を停止したお客様から利用再開の許可を得た場合、許可時点以降に生成された当該お客様に関する運用データをモバイル空間統計の作成に利用できるものとします。

観光動態調査レポートの概要

- ◆位置情報ビッグデータ(*1)を用いて観光客の動きを統計的に把握することができる調査・分析レポート(平成25年10月開始)
- ◆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ことを狙いとしている。

(*1) auスマートフォンユーザのうちスタンプカードサービスを利用するユーザーより、KDDIが同意の上取得した上で、誰の情報であるかわからない形式に加工した、位置情報データおよび性別・年齢層の属性情報

位置情報ビッグデータの提供フロー



①位置情報データの利用及び、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したauスマートフォンユーザの情報を取得。(次頁イメージ)

②KDDIは、誰の情報であるかわからない形式へ加工(非識別化处理)の上、コロプラへ分析を委託。
具体的には、(a)生活圏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)、(c)個人識別子の秘匿化を行っている。
なお、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、コロプラに義務付け。

③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。この際、少人数の秘匿処理(少数サンプルのエリアはデータとして利用しない)をしている。

観光動態調査レポートの取組

- ◆平成25年7月18日～同年9月30日にかけて三重県伊勢市、埼玉県及び徳島県を対象地域とした実証実験を実施。
- ◆実証実験において一定の成果が得られたことから、同年10月29日より、地方自治体や観光協会などを対象として、観光動態調査レポートの提供を開始。併せて、東日本大震災によって被災した岩手県・宮城県・福島県に対しては、レポートを無償提供。
- ◆実証実験開始時、サービス提供開始時の2度に渡り、プレスリリースを実施し、利用目的や提供フローを公表。
- ◆Webサイトに、「プライバシー保護の仕組み」として、非識別化及び秘匿処理を公表。
- ◆スタンプを貯めるとauポイントに交換でき、そのポイントで様々な商品と交換可能。単にお客様からデータ取得するのではなく、メリットのある仕組みを用意。
- ◆スタンプカードの利用を停止することにより、同意を破棄し、本レポートへのデータ提供を停止する対応を取ることでオプトアウトの機会を提供。

auスマートパス
「スタンプカード」利用上のご注意事項

-途中省略-
スタンプカードのご利用にあたっては、以下の事項をご了解下さい。

1. 取得する情報
(1) Web利用履歴 (IS-NET等接続先)
-途中省略-
(2) 位置情報 (通信・通話をした場所)
ご利用のau端末から行った通信・通話の場所 (緯度・経度など) を取得します。
2. 利用目的
(1) 当社がお客様に有益と認める情報表示・配信
(2) サービス品質向上・新サービス開発
(3) 各種サービスのご利用状況分析
なお、個人を特定できない形式に加工した上で、コンテンツプロバイダー等の第三者に情報を提供する場合があります。
3. 取得契機
通信の終了時点で情報を生成・取得致します。
4. 提供の終了
-途中省略-
☒ 規約に同意して登録する

▲同意取得画面イメージ

auスマートパス

スタンプカード

メンテナンスのお知らせ

アンケート
ポイント＆ラッキー
クーポン
おかいもの
おでかけ
Fashion WALL
Fitness
アプリでスタンプ

♥スタンプカードとは？
スタンプカードとは、各サービスを利用することで、スタンプを貯めることができるサービスです。
当月貯めたスタンプは翌月auポイントに交換が可能です。

ポイント＆ラッキー
スピードくじに当たればスタンプGET！

アンケート
アンケートに答えたらスタンプGET！
(内容に応じてスタンプ数は変動します)

[スタンプカードをやめる](#)

ページTOPへ

スタンプカード

©KDDI

▲利用停止フロー

auスマートパス

スタンプカード

利用停止

スタンプカードの利用を停止すると、以下のサービス提供がご利用できなくなります。

1. アンケートコーナーの利用ができません
2. スタンプカードが利用できません

【ご注意！】
auポイント交換前のスタンプは、全て削除されます。

また、以下のお客様情報の利用を停止致します。

1. Web利用履歴 (IS-NET等接続先)
2. 位置情報 (通信・通話をした場所)

ページTOPへ

スタンプカード

©KDDI

auスマートパス

スタンプカード

利用停止完了

スタンプカードの利用を停止いたしました

ページTOPへ

スタンプカード

©KDDI

Ⅲ 海外における位置情報の取扱い

- ✓ 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条において顧客情報のプライバシーを規定。電気通信事業者は、顧客に関する専属的な網情報(CPNI)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、携帯電話業界団体CTIA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・ガイドラインを2010年3月に採択している。その二大原則は以下の通りであり、**位置情報サービス提供者は、ユーザーに通告し、同意を求めること**とされている。
 - ・ ユーザーに位置情報がどう利用されるか、開示されるか、保護されるかについて、通知し、ユーザーが位置情報を利用する決断を下す際の情報を提供することで、位置情報に関するコントロールを与える。
 - ・ ユーザーに位置情報の利用、開示について同意を求め、いつでも同意を撤回する権利を与える。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。
- ✓ FTC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」を2013年2月に公表しており、**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等を使っ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、本年2月19日には、FTCにおいて「Spring Privacy Series: Mobile Device Tracking」と題するセミナーを開催。(詳細次頁)。

✓ FTCセミナーにおける議論

FTCは、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、セミナーを開催し、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を実施。参加者の主なコメントは以下のとおり。

- ・消費者の行動分析を通じて、会計時の待ち時間減少や商品選別・商品棚配置の最適化等消費者の利便性を高めることが可能となる。
- ・消費者の信頼は重要であるが、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。(例: 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)
- ・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一方、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。
- ・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。

✓ フューチャー・オブ・プライバシー・フォーラム(FPF)の取組

米国のシンクタンクであるFPFは、位置分析を行う企業が提供するサービスに対する強制力を持った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」を作成。同行動規範に賛同する位置分析企業とともに、MAC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。

- ・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または非識別化すること。

- 《非特定情報の定義》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。
- 《非識別情報の定義》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。

- ・モバイル端末の位置情報の分析についてオプトアウトの機会を提供すること。(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)
- ・個別の端末情報は保存期間を定めて保持すること。

位置情報を活用したサービスイメージの一例

レジ

サービス提供場所

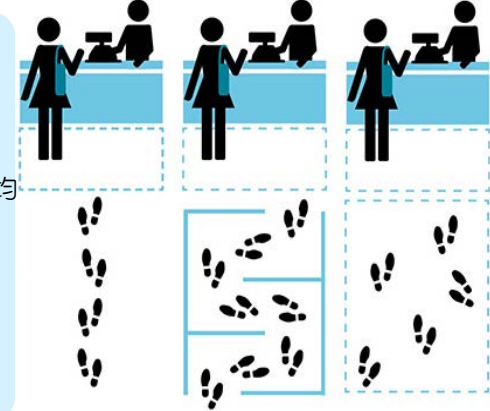
-サービス提供時間の平均

行列

-長さ

-待ち時間

-並ぶのを断念する割合



上記の項目を分析し、会計時の待ち時間減少につなげる

欧州レベル

- ✓ EUの第29条作業部会は、2011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。この意見の中では**欧州データ保護指令(Directive 95/46/EC)**が、**携帯電話の三角測量や、Wi-FiアクセスポイントとGPSを利用するなどによって生成された位置情報に対して、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)**ような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**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)。

英国内

- ✓ 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。**
- ✓ 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、電子通信プライバシー指令と同旨が定められている。
- ✓ なお、英国においては、GPS情報、携帯電話端末が取得した基地局情報、携帯電話端末が取得したWi-Fi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。
- ✓ 英国情報コミッショナーは、**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を示している。**(詳細次頁)

匿名化に対する本ガイドラインの基本的な認識及び目的

- ✓ 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。
- ✓ 個人データの効果的な匿名化は可能であり、望ましく、社会が個人のプライバシーを保護しながら豊富なデータ源を入手できるように手助けとなることを提示。

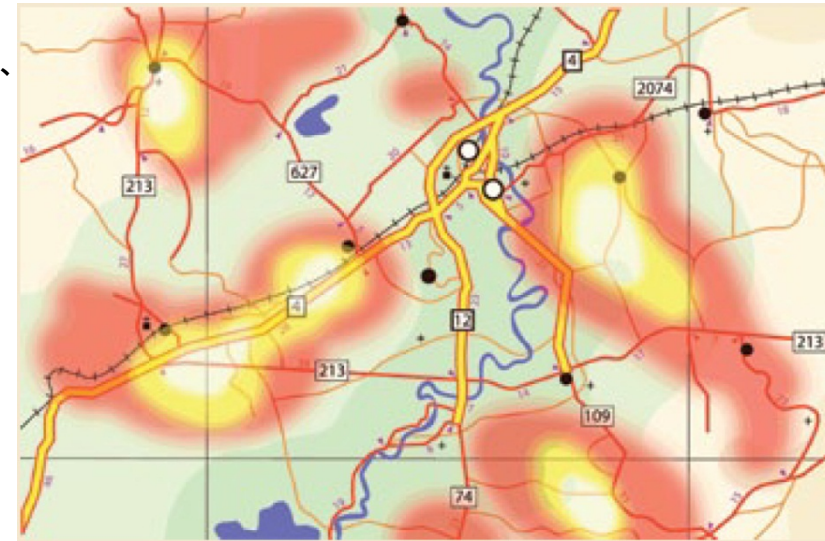
再識別化のリスクについて

- ✓ データ連結を通じた再識別化のリスクは基本的に予知できない(何のデータが将来公開されるか等を評価することは不可能)。
- ✓ 再識別化の結果が、個人が損害、苦悩、経済的損失を被った状態にさらされるため重大となりうるケースでは、組織は以下を行うべき。
 - ・データの開示について、データ主体(本人)に生じ得る結果を説明し、同意を求める。
 - ・より厳密な形態のリスク分析及び匿名化を採用する。

個人データと空間的情報

- ✓ 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。
- ✓ 空間的情報が合法的な目的のために公表されている場合、個人のプライバシーの保護とのバランスをとることができる最大限の詳細度を達成することを目指すべきであり、プライバシー影響評価(PIA)は当該目標の達成のために実践すべき。
- ✓ 空間的情報のために採用すべき(匿名化)方法は、保有するデータセットの規模によっても異なる。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。
- ✓ 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以下が挙げられている。
 - ・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。
 - ・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。
 - ・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。
 - ・住居レベルに関する空間的情報の公表を避ける(当該情報の公表には個人データの処理を伴うことがあるため)。

犯罪地図作製のためのヒートマッピング (色分け地図作成)手法



匿名データの開示形態について

- ✓ 匿名データの利用者が直面する問題は、一方では、彼らは自身の使用目的のために豊富で十分に利用できるデータを欲しているが、もう一方では、再識別化が発生しないことを望んでいる。
- ✓ 匿名データを広く社会全体に公表することとアクセス制限を区別することが重要(集計的かつ連結不可能なデータは公表しやすい一方、アクセス制限を用いると、データの更なる開示または使用に対する制限がなく、かつ、安全性が維持される。)

Ⅳ パーソナルデータに関する検討会
パーソナルデータの利活用に関する制度見直し方針
技術検討ワーキンググループ報告書（抜粋）

I パーソナルデータの利活用に関する制度見直しの背景及び趣旨

我が国の個人情報保護制度については、これまで国民生活審議会や消費者委員会個人情報保護専門調査会等において様々な課題が指摘され、議論されてきたところであるが、具体的な解決に至っていないものもある。これまで行ってきた検討で蓄積された知見を活かし、時代の変化に合った制度の見直し、改善が求められている。

今年で個人情報保護法の制定から10年を迎えたが、情報通信技術の進展は、多種多様かつ膨大なデータ、いわゆるビッグデータを収集・分析することを可能とし、これにより新事業・サービスの創出や我が国を取り巻く諸課題の解決に大きく貢献する等、我が国発のイノベーション創出に寄与するものと期待されている。特に利用価値が高いとされているパーソナルデータについては、個人情報保護法制定当時には想定されていなかった利活用が行われるようになってきており、個人情報及びプライバシーに関する社会的な状況は大きく変化している。その中で、個人情報及びプライバシーという概念が広く認識され、消費者のプライバシー意識が高まってきている一方で、事業者が個人情報保護法上の義務を遵守していたとしても、プライバシーに係る社会的な批判を受けるケースも見受けられるところである。また、パーソナルデータの利活用ルールの曖昧さから、事業者がその利活用に躊躇するケースも多いとの意見もある。

さらに、企業活動がグローバル化する中、情報通信技術の普及により、クラウドサービス等国境を越えた情報の流通が極めて容易になってきている。国内に世界中のデータが集積し得る事業環境の整備を進めるためにも、海外における情報の利用・流通とプライバシー保護の双方を確保するための取組に配慮し、制度の国際的な調和を図る必要がある（EU:「データ保護規則」提案、米国:「消費者プライバシー権利章典」公表、OECD:「OECDプライバシーガイドライン」改正等）。

このような状況の変化を踏まえ、平成25年6月に決定された「世界最先端IT国家創造宣言」において、IT・データの利活用は、グローバルな競争を勝ち抜く鍵であり、その戦略的な利活用により、新たな付加価値を創造するサービスや革新的な新産業・サービスの創出と全産業の成長を促進する社会を実現するものとされていることから、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利活用により民間の力を最大限引き出し、新ビジネスや新サービスの創出、既存産業の活性化を促進するとともに公益利用にも資する環境を整備する。さらに、事業者の負担に配慮しつつ、国際的に見て遜色のないパーソナルデータの利活用ルールの明確化と制度の見直しを早急に進めることが必要である。

II パーソナルデータの利活用に関する制度見直しの方向性

このような背景・趣旨を踏まえ、個人情報及びプライバシーを保護しつつ、パーソナルデータの利活用を躊躇する要因となっているルールの曖昧さの解消等を目指して行うべき制度見直しに関する主な方向性については、次の通り考えるものとする。

1. ビッグデータ時代におけるパーソナルデータ利活用に向けた見直し

・個人情報及びプライバシーの保護に配慮したパーソナルデータの利用・流通を促進するため、個人データを加工して個人が特定される可能性を低減した個人データに関し、個人情報及びプライバシーの保護への影響並びに本人同意原則に留意しつつ、第三者提供における本人の同意を要しない類型、当該類型に属するデータを取り扱う事業者（提供者及び受領者）が負うべき義務等について、所用の法的措置を講ずる。

・共同利用やオプトアウト等第三者提供の例外措置の要件の明確化、利用目的拡大に当たって事業者が取るべき手続きの整備、わかりやすいプライバシーポリシーの明示等パーソナルデータの取扱いの透明化等を検討する。

2. プライバシー保護に対する個人の期待に応える見直し

・適切なプライバシー保護を実現するため、保護すべきパーソナルデータの範囲、個人情報の開示及び訂正（追加又は削除を含む。）等における本人関与の在り方、取り扱う個人情報の規模が小さい事業者の取扱い、プライバシー影響評価の導入、データ取得時等における手続きの標準化等について検討する。

・専門的知見の集中化、機動的な法執行の確保、及び諸外国の制度との整合を取りつつパーソナルデータの保護と利活用の促進を図るため、独立した執行機関（第三者機関）を設置する。第三者機関に行政処分等の権限を付与するとともに、プライバシーに配慮したデータ利活用の促進を図る観点から、罰則の在り方、法解釈・運用の事前相談の在り方等を検討する。

さらに、これらの対応と併せて、個人情報及びプライバシーの保護を有効に機能させるため、事業者が自主的に行っているパーソナルデータの保護の取組を評価し、十分な規律に服することが担保される、マルチステークホルダープロセス※の考え方を活かした民間主導の枠組みの構築を検討することにより、パーソナルデータ利活用のルールが遵守される仕組みを整備する。

※マルチステークホルダープロセス: 国、事業者、消費者、有識者等の関係者が参画するオープンなプロセスでルール策定等を行う方法のこと。

3. グローバル化に対応する見直し

・プライバシーに配慮したパーソナルデータの利活用は、グローバルに対処すべき課題であり、我が国の事業者がグローバルに適切なパーソナルデータの共有、移転等を行えるようにするため、諸外国の制度や国際社会の現状を踏まえた国際的に調和の取れた制度を検討するとともに、他国へのデータ移転の際の確実な保護対策等について検討する。

・国境を越えた情報流通の実態を踏まえた海外事業者に対する国内法の適用等について検討する。

III パーソナルデータの利活用に関する制度見直し事項

1. 第三者機関（プライバシー・コミッショナー）の体制整備

パーソナルデータの保護と利活用をバランスよく推進する観点から、独立した第三者機関による、分野横断的な統一見解の提示、事前相談、苦情処理、立入検査、行政処分の実施等の対応を迅速かつ適切にできる体制を整備する。

その際、実効的な執行かつ効率的な運用が確保されるよう、社会保障・税番号制度における「特定個人情報保護委員会」の機能・権限の拡張や現行の主務大臣制の機能を踏まえ、既存の組織、権限等との関係を整理する。

2. 個人データを加工して個人が特定される可能性を低減した個人データの個人情報及びプライバシー保護への影響に留意した取扱い

個人情報及びプライバシーの保護に配慮したパーソナルデータの利用・流通を促進するため、個人データを加工して個人が特定される可能性を低減した個人データに関し、個人情報及びプライバシーの保護への影響並びに本人同意原則に留意しつつ、第三者提供における本人の同意を要しない類型、当該類型に属するデータを取り扱う事業者（提供者及び受領者）が負うべき義務等について、所要の法的措置を講ずる。

3. 国際的な調和を図るために必要な事項

＜諸外国の制度との調和＞

諸外国の制度や国際社会の現状を踏まえ、国際的なルール作りに積極的に参加しつつ国際的に調和の取れた制度を構築し、日本企業が円滑かつグローバルに事業が展開できる環境を整備するとともに、海外事業者に対する国内法の適用や第三者機関による国際的な執行協力等の実現について検討する。

＜他国への越境移転の制限＞

グローバルな情報の利用・流通を阻害しないことと、プライバシー保護とのバランスを考慮し、パーソナルデータの保護水準が十分でない他国への情報移転を制限することについて検討する。

＜開示、削除等の在り方＞

本人の自身の情報への適正かつ適時の関与の機会を確保することが、本人の不安感を払しょくするとともに、事業の透明性を確保することにもつながることから、取得した個人情報の本人による開示、訂正（追加又は削除を含む。）、利用停止（消去又は提供の停止を含む。）等の請求を確実に履行できる手段について検討する。

＜パーソナルデータ利活用のルール遵守の仕組みの構築＞

第三者機関への行政処分等の権限の付与・一元化について検討するとともに、プライバシーに配慮したデータ利活用の促進を図る観点から、罰則の在り方等を検討し、パーソナルデータ利活用のルールを遵守する仕組みを整備する。

＜取り扱う個人情報の規模が小さい事業者の取扱い＞

本人のプライバシーへの影響については、取り扱うデータの量ではなくデータの質によるものであることから、現行制度で適用除外となっている取り扱う個人情報の規模が小さい事業者の要件とされる個人情報データベースを構成する個人情報の数が5,000 件以下とする要件の見直しを検討する。その際、取り扱う個人情報の規模が小さい事業者の負担軽減についても併せて検討する。

＜行政機関、独立行政法人等及び地方公共団体が保有する個人情報の取扱い＞

行政機関、独立行政法人等及び地方公共団体における個人情報の定義や取扱いがそれぞれ異なっていることを踏まえ、それらの機関が保有する個人情報について、新たに設置する第三者機関の機能・権限等に関する国際的な整合性、我が国の個人情報保護法制の趣旨等にも配慮しながら、必要な分野について優先順位を付けつつその対応の方向性について検討する。

4. プライバシー保護等に配慮した情報の利用・流通のために実現すべき事項

＜パーソナルデータの保護の目的の明確化＞

パーソナルデータの保護は、その利活用の公益性という観点も考慮しつつ、プライバシーの保護と同時に利活用を促進するために行うものであるという基本理念を明確にすることを検討する。

＜保護されるパーソナルデータの範囲の明確化＞

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し、プライバシー保護という基本理念を踏まえて判断するものとする。

また、プライバシー性が極めて高い「センシティブデータ」については、新たな類型を設け、その特性に応じた取扱いを行うこととする。

なお、高度に専門的な知見が必要とされる分野（センシティブデータが多く含まれると考えられる情報種別を含む。）におけるパーソナルデータの取扱いについては、関係機関が専門的知見をもって対応すること等について検討する。

＜プライバシーに配慮したパーソナルデータの適正利用・流通のための手続き等の在り方＞

透明性の確保を原則として、利用目的の拡大に当たって事業者が取るべき手続きや第三者提供における本人同意原則の例外規定（オプトアウト、共同利用等）の在り方について検討するとともに、パーソナルデータ取得時等におけるルールの充実（同意取得手続きの標準化等）について検討する。

また、個人情報取扱事業者における個人情報の適正な取扱いを確保するため、個人情報の漏えい、その他のプライバシー侵害につながるような事態発生の危険性、影響に関する評価（プライバシー影響評価）の実施、公表等については、事業者の過度な負担とならないように配慮しつつ、評価事項・基準、評価対象、実施方法、評価方法等の具体化を「特定個人情報保護委員会」が行う特定個人情報保護評価の仕組みを参考に検討する。

Ⅳ 今後の進め方

本方針に基づき、詳細な制度設計を含めた検討を加速させる。検討結果に応じて、平成26年（2014年）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（2015年）通常国会への法案提出を目指すこととする。

技術検討ワーキンググループ報告の要約(Executive Summary)

1. はじめに

技術検討ワーキンググループ(以下「本WG」という。)は、パーソナルデータに関する検討会(以下「親会」という。)の下に「匿名化されたパーソナルデータの扱い」について検討するために設置された。

□親会からの依頼事項

合理的な水準まで匿名化されたパーソナルデータは、第三者提供における本人同意原則の例外として、通常の個人情報とは異なる取扱いができるのではないか、との問題提起により、(1) 個人情報保護法(以下「現行法」という。)において導入可能な「再識別不可能データ」化(提供事業者において容易照合性のない技術的匿名化)措置の内容、及び(2) 新たな立法措置を前提とした「合理的な技術的匿名化措置」の内容の検討を、米国FTCが公表したFTCスタッフレポート「急速な変化の時代における消費者プライバシーの保護」匿名化に関する三要件(いわゆる「FTC3要件」)他を念頭において行った。

□本WGでの検討に当たっての前提となる考え方

現行法における「個人情報」等の用語の定義は、技術的観点からは明確であるとは言えないことから、本WGでは個人情報に関して下記のような整理をした上で検討した。
(1) 現行法の「容易照合性」については、①現行法の解釈が明確ではないこと及び②現行法制定時よりも、技術の進展によりプライバシー侵害をもたらす可能性のある他の情報との照合可能性が高まっていることから、現行法の「容易照合性」の要件とは独立に検討を行った。
(2) 個人情報に関するいわゆる個人識別性については、「特定」と「識別」に分けて議論した。ここで「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。一方、「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」(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。
また、上記の「特定」及び「識別」の定義を踏まえ、個人情報を加工することにより作成される情報を下記の3つのカテゴリーに分けて議論した。

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(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)

2. 現行法における技術的課題の検討

□匿名化に関わる技術と限界

いわゆる匿名化と考えられていたもの(本WGでは識別特定情報(個人情報)を識別非特定情報または非識別非特定情報への加工すること)の技法は多種多様である。例えば、個人を特定し得る情報の削除(属性削除)、氏名等のユニークな番号への変換(仮名化)、住所などを広いエリアに置き換える(あいまい化)、希少な情報の削除等があり、通常は、それらを組み合わせる用いる。ただし、一般的には、個人情報を匿名化することにより情報の利活用における有用性は低下することになる。
さらには、一般的にインターネット等に公開されている外部情報との突き合わせによって識別非特定情報から個人を特定できることや、非識別非特定情報からは当初想定できなかった特定の個人の情報が抽出される可能性が排除できない。すなわち、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。従って、検討事項(1)に対しては、第三者提供を念頭に一定の匿名化措置(個人情報のある定められた手順で加工)を行っても、必ず識別性または特定性を無くせるわけではなく、またそうした匿名化の措置に対して一般的な水準を作ることもできない。

□ケースバイケースの対応が必要

汎用的な匿名化方法は存在しないものの、ケースバイケース、つまり個人情報の種類・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。乗降履歴情報の例では、仮名化によりその情報単体における個人の特定を無くせたとしても、外部情報との突き合わせにより特定の個人が分かる可能性は必ずしもゼロとはいえない。ある経路の利用者が一人であればその時点で識別される状態となり、それを避けるためには多くの希少な経路の情報を捨てることが求められる。また、どの経路を捨てるかは各経路の日々の乗車数に依存し、経路を捨てることで情報の有用性が下がる可能性もあるため、ケースバイケースの対応が必要である。

□外部情報との突き合わせ技術

一方で、外部情報との突き合わせの可能性は広がっている。インターネットの発展により外部情報は増えると共に、情報を突き合わせるための技術が進展している。例えば、顔認識技術を利用することにより、二つの情報に含まれた異なる写真でも同一人物の写真であればその同定は容易になっており、突き合わせることが可能な範囲は拡大していることに留意すべきである。

3. 新たな法的措置を前提とした技術的課題への対応

非特定化、非識別化または非識別非特定化の措置を行った個人情報、元の個人情報と比較して特定化または識別化の困難性は高まっている。こうした情報については、制度的な制約により安全性を確保されるのであれば、例外的に流通を容易にすることが認められる可能性があり、それを想定した技術的な検討を行った。

上述のように匿名化を行っても、個人の特定が不可能になるとは限らないことを勘案し、個人情報の第三者提供に関する同意原則の例外規定と位置づけられる新たなカテゴリーとして「(仮称)法第23条第1項適用除外情報」の導入を検討した。具体的には個人情報の第三者提供において、提供者・受領者(第三者)による特定化・識別化が禁止されることを前提に、ある範囲で個人の特定性・識別性を低減している個人情報を第三者に提供することを可能とする方法である。

・「(仮称)法第23条第1項適用除外情報」の提供者及び受領者に課せられる制約

提供者が個人情報を第三者(受領者)に提供する場合、受領者において特定化、識別化または識別特定化を禁止するにしても、個人の特定性または識別性が低下した情報(「(仮称)法第23条第1項適用除外情報」)に加工すべきである。また、受領者は個人情報の特定化、識別化または識別特定化を行なわないことが求められる。さらに、突き合わせられる外部情報が予測できないことから、「(仮称)法第23条第1項適用除外情報」の不特定多数への公表は禁止されるべきである。

・「(仮称)法第23条第1項適用除外情報」の規律に関する予備的議論

「(仮称)法第23条第1項適用除外情報」に関わる特定化、識別化または識別特定化を制限する規律に関しては親会での議論が必要であるが、本WGではFTC3要件を念頭に予備的な議論を行った。

1. 提供者は「(仮称)法第23条第1項適用除外情報」となるための措置を施すこと。
2. 提供者は「(仮称)法第23条第1項適用除外情報」の特定化、識別化または識別特定化をしないことを約束・公表等すること。
3. 提供者と受領者(第三者)との間の契約において、受領者が「(仮称)法第23条第1項適用除外情報」の特定化、識別化、または識別特定化することを禁止すること。(または、受領者(第三者)が「(仮称)法第23条第1項適用除外情報」を特定化、識別化または識別特定化しないで取扱うものであることを条件とすることを制度化。)

ただし、我が国においては、2. については、このような約束を守らせる法的手段がないため新たな立法措置が必要である。また、3. については、契約による禁止の履行を提供者が求めることが期待できるのか疑問が残る。代替的措置として、契約上の義務ではなく法制度上の義務とすることについても検討が必要である。さらに、「(仮称)法第23条第1項適用除外情報」の定義については、新たな法的措置が定まっていない現時点で明確に規定することは困難である。

なお、受領者が、受領した「(仮称)法第23条第1項適用除外情報」またはそれを元に作成した情報を別の第三者に提供する場合、提供先である別の第三者にも「(仮称)法第23条第1項適用除外情報」に関わる同様の規律が及ぶべきである。

4. 今後の検討課題について

本節では、親会にて方針を決定した後に議論すべきと考える事項や、当該WGでは時間的制約から議論しきれない事項等の今後の検討課題を、以下のとおり整理している。今後の本分野に関する詳細かつ具体的な検討の際の一助として頂きたい。

○新たな類型としての「(仮称)法第23条第1項適用除外情報」について

- ・制度的枠組みにより提供者及び受領者が個人情報及びプライバシーの保護を実現することが前提であるが、現時点では、制度的枠組みが不明確。
- ・更なる制度的枠組みを踏まえ、類型の範囲やそのための技術的要件等についての具体的な議論が可能と思料。

○立法措置を前提とした「合理的な技術的匿名化措置」について

- ・親会の依頼をもとに、いわゆる「FTC3要件」を念頭にした検討の詳細化。
- ・仮に「FTC3要件」類似の制度を採用する場合には、提供者の約束や受領者の契約上の義務が実効的に実施される担保的な措置等の技術的な検討が必要。

○ユースケースなどを想定した詳細検討

- ・取り扱う個人情報に含まれる属性情報の種類や利用の目的等を個別に判断することで、個別の事情に見合った合理的な匿名化の措置を行うことは不可能ではないが、詳細は議論できなかった。これは第三者提供される情報の種類や利用の目的等を明確ではなかったためである。今後、これらの情報が明確になった後に詳細な議論が必要であろう。

V その他

ライフログ活用サービスに係る 「配慮原則」

(諸問題研究会第二次提言)

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

スマートフォン利用者情報の 取扱いに係る「基本原則」

(スマートフォン プライバシー イニシアティブ)

- 透明性の確保
- 利用者関与の機会の確保
- 適正な手段による取得の確保
- 適切な安全管理の確保
- 苦情・相談への対応体制の確保
- プライバシー・バイ・デザイン

パーソナルデータ利活用の原則

(パーソナルデータ研究会報告書)

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