

技術検討ワーキンググループ報告書

～「(仮称)準個人情報」及び「(仮称)個人特定性低減データ」
に関する技術的観点からの考察について～

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

平成26年5月

【報告書の概要】

「パーソナルデータに関する検討会」では、平成 25 年 12 月に取りまとめた「パーソナルデータの利活用に関する制度見直し方針」に基づき、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等を行うべく、各論点について詳細な議論を行っているところである。こうした中、提案された「(仮称) 準個人情報」の新たな定義等について、また「(仮称) 個人特定性低減データ」の定義等について、同検討会から技術検討ワーキンググループに対して技術的な観点から検討する旨の依頼を受けたものであり、本報告書は、その検討結果を取りまとめたものである。

1. 検討に当たっての前提条件

技術検討ワーキンググループでは、以下の前提条件を整理し、課題を検討している。

- 「(仮称) 準個人情報」については、特定の個人が識別されて生じる権利利益の侵害を事前に防止する観点から検討。
- 「(仮称) 個人特定性低減データ」については、当該データ単独での個人特定性の低減についてのみを対象とし、また、提供先事業者（受領者）における当該データと照合可能な個人データ等の有無については予見できないことから、提供の際に適正に加工されたものであるものに関しては、何らかの権利利益の侵害が生じた場合には受領者側の責任であるものとして検討。

2. 「(仮称) 準個人情報」の定義等について

○特定の個人が識別されていない情報であっても、特定の個人が識別されるおそれのある情報を「(仮称) 準個人情報」とすることは妥当。その際、特定の個人が識別されるおそれは、多くの場合、当該個人に関する多量又は多様な情報が収集されることによって生じることから、そのような情報収集するものとして識別子を対象とすべき。また、様々な識別子がある中でも、特にその性質・特性から多量又は多様な情報を収集することとなる可能性が高いものに限定することとし、次の指標をもとに特に特定の個人を識別する蓋然性の高い識別子を選定。

- ・ 本人又は本人の所有物と密接性があるもの
- ・ 一意性/単射性があるもの
- ・ 共用性があるもの
- ・ 変更可能性/不変性/利用停止可能性については容易に変更できないもの

○事務局案にある「③移動履歴、購買履歴等の特徴的な行動の履歴」について、現時点では、位置情報、購買履歴、Web 閲覧履歴を一律に「(仮称) 準個人情報」に該当すると判断することは困難。

3. 「(仮称) 個人特定性低減データ」の定義等について

○「(仮称) 個人特定性低減データ」への加工については、最低限の加工方法であっても、データの種類に応じて加工方法等が多様であるから一律の基準を示すことは困難。

○これに合わせて、事務局案の定義を見直し、個人情報又は「(仮称)準個人情報」から特定の個人を識別する蓋然性の低いものに加工を施して、特定の個人を識別することが困難になるようにしたものである旨の定義に変更することを提案。

【目次】

1	検討の背景.....	1
1.1	「パーソナルデータに関する検討会」からの依頼事項.....	1
1.2	検討に当たっての前提条件.....	3
1.2.1	これまでのWGにおける検討との関係.....	3
1.2.2	「(仮称)準個人情報」及び「(仮称)個人特定性低減データ」に起因する権利利益侵害の場合分けについて.....	4
1.2.3	「(仮称)個人特定性低減データ」に関する権利利益侵害発生時の責任について.....	5
2	「『個人情報』等保護されるパーソナルデータの範囲」について.....	6
2.1	「個人情報」と「(仮称)準個人情報」との関係.....	6
2.2	「(仮称)準個人情報」の定義等について.....	7
2.2.1	「(仮称)準個人情報」に該当するものを選定する指標についての検討.....	7
2.2.2	事務局から提案された「(仮称)準個人情報」の定義についての検討.....	9
2.2.3	Web閲覧履歴(Cookie等を含む)に関する検討.....	12
2.2.4	「(仮称)準個人情報」の定義について.....	15
2.2.5	「(仮称)準個人情報」に含まれる具体的な項目について.....	16
3	「(仮称)個人特定性低減データ」について.....	20
3.1	「(仮称)個人特定性低減データ」の定義及び加工方法について.....	20
3.1.1	事務局案についての検討.....	20
3.1.2	「(仮称)個人特定性低減データ」の定義の修正提案.....	24
3.2	「(仮称)個人特定性低減データ」に加工し第三者提供する事業者における取扱いについて.....	25
3.3	「(仮称)個人特定性低減データ」を受領する事業者における取扱いについて.....	26
3.4	「(仮称)個人特定性低減データ」に関する第三者機関への情報の提出と第三者機関による公表について.....	27

1 検討の背景

「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。)」の下に設置されている「パーソナルデータに関する検討会(以下「親会」という。)」では、平成 25 年 12 月に「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。)」を取りまとめた。

この見直し方針に沿って、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 年の通常国会への法案提出を目指すべく、平成 26 年 3 月から親会を再開し、見直し方針に掲げられている各論点について詳細な議論を行っているところである。

この議論の過程である、第 7 回親会(平成 26 年 4 月 16 日開催)において、事務局より、『個人情報等保護されるパーソナルデータの範囲について』として「(仮称)準個人情報」の新たな定義等について、「(仮称)個人特定性低減データ」の定義等について、それぞれ提案がなされた。

これを踏まえ、親会の下に設置されている「技術検討ワーキンググループ(以下「WG」という。)」に対して、「(仮称)準個人情報」及び「(仮称)個人特定性低減データ」について、技術的な観点から検討することを依頼されたものである。

1.1 「パーソナルデータに関する検討会」からの依頼事項

親会から依頼された検討事項は、以下のとおりである。

技術検討WGへの検討依頼事項

5 月下旬に開催予定の「パーソナルデータに関する検討会」を目途に、以下の事項について、技術検討WGで技術的な観点から検討いただき、その結果をご報告いただきたい。

1. 「個人情報」等保護されるパーソナルデータの範囲
 - ・「個人情報」とは異なる定義とする「(仮称)準個人情報」に含む又は、含まない項目等について
2. 「(仮称)個人特定性低減データ」について
 - ・「個人情報」や「(仮称)準個人情報」から「(仮称)個人特定性低減データ」へ加工するにあたっての最低条件

以上

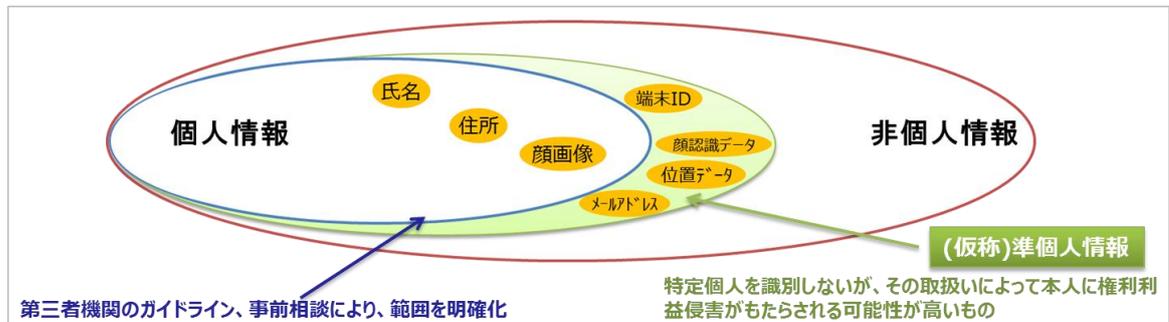
(第 7 回パーソナルデータに関する検討会 【資料 1-3】より)

まず、「(仮称)準個人情報」については、「(仮称)準個人情報」の定義の考え方の整理も含まれており、それを踏まえた上で、具体的にどのような項目が該当するのかが等について検討した。

次に、「(仮称)個人特定性低減データ」については、どのような状態が「(仮称)個人特定性低減データ」であるのかについての定義の考え方、「個人情報」や「(仮称)準個人情報」から加工する場合の最低限かつ具体的な加工方法の整理、「(仮称)個人特定性低減データ」に加工する事業者が「第三者機関」(設置について別途検討中)に提出する事項等についても、併せて検討した。

なお、事務局から提案された「『個人情報』等保護されるパーソナルデータの範囲」についての考え方の概要は、以下のとおりである。

- 現行の個人情報保護法（以下「現行法」という。）の定義をもとに各事業者が情報の取扱いを行っていることに配慮し、「個人情報」の定義を維持する。
- 「個人情報」への該当性の判断については、ガイドライン等による明確化、事前相談の迅速な対応を図る。
- 「個人情報」への該当性の判断主体は一義的には情報を取り扱う事業者であること、また、第三者提供時の容易照合性については提供元を基準に判断すること、をそれぞれ明確化する。
- その上で、個人情報に該当するかどうかの判断が困難ないわゆる「グレーゾーン」を解消すべく、現行法では「個人情報」に該当しないものであっても、特定の個人を識別する蓋然性が高いものを「(仮称)準個人情報」として保護される対象として追加する。



（第7回パーソナルデータに関する検討会 【資料 1-1】 より）

また、同様に事務局から提案された「(仮称)個人特定性低減データ」についての考え方の概要は、以下のとおりである。

- いわゆるビッグデータの活用が、付加価値の創造、イノベーションの促進等我が国の経済成長の一翼を担うものであることに鑑み、特に有用とされるパーソナルデータの利用・流通を図る。
- 現行法においては、個人情報を第三者提供する際には本人の同意が求められるところ、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データを本人の同意なく第三者に提供できる新たな類型として整理する。
- 加工したデータを取り扱う者（提供者及び受領者）が負うべき義務等につき所要の措置を講じる。具体的には、以下のとおり。
 - ✓提供者は、「個人データ」、「(仮称)準個人データ」等から「(仮称)個人特定性低減データ」に加工し、当該データを第三者提供しようとする場合には、第三者機関に対して、加工方法等に関する情報を提出する。なお、「(仮称)準個人データ」を第三者提供しようとする場合には、「(仮称)個人特定性低減データ」に加工しなければならないこととする。
 - ✓受領者は、受領した「(仮称)個人特定性低減データ」について、特定の個人

を識別することを禁止する。併せて、安全管理措置を行わなければならないこととする。

- ✓ 第三者機関は、提供された情報について、営業秘密等の事業者の権利利益を侵害しない範囲で情報を公開することとする。

1.2 検討に当たっての前提条件

1.2.1 これまでのWGにおける検討との関係

WG は、先に取りまとめた「技術検討ワーキンググループ報告書（平成 25年 12月）（以下「前回報告書」という。）」において、技術の進展及び外部情報の増加から、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という観点に立ち、パーソナルデータに関するいわゆる個人識別性を扱うために、「特定」と「識別」の基準を導入した。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。この二つの基準により、パーソナルデータを、識別特定情報（それが誰か一人の情報であることが分かり、さらに、その一人が誰であるかが分かる情報）、識別非特定情報（それが誰か一人の情報であることが分かるが、その一人が誰であるかまでは分からない情報）、非識別非特定情報（それが誰の情報であるかが分からず、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）と分類している。

今回親会から検討を依頼された「（仮称）準個人情報」に関しては、第7回親会【資料 1-2】の3ページにおいて、「特定個人を識別しないが、その取扱いによって本人に権利利益侵害がもたらされる可能性があるもの（技術検討WGにおける「識別非特定情報」に含まれるもの）を新たに類型化し、これを定義することとしてはどうか。」とあるように「（仮称）準個人情報」は上記の識別非特定情報をベースにしたものであり、前回報告書の延長線上の議論である。このため本報告書での「特定」や「識別」などの用語についても前回報告書を継承している。

また、もう一つの検討事項である「（仮称）個人特定性低減データ」についても、前回報告書において提案した本人同意不要な第三者提供向けのデータ類型である「（仮称）法第23条第1項適用除外情報」をベースにしているため、本報告書では、適宜、前回報告書を参照することとする。

ところで、前回報告書では検討課題として「（仮称）法第23条第1項適用除外情報」の範囲は現状では未確定とするしかなかった。これは同範囲が制度的な補完、つまり規律により個人情報及びプライバシーの保護が実現できることが前提になっており、範囲はその規律に依存するためである。その際、「今後の親会における制度的な検討を受けて、再度、「（仮称）法第23条第1項適用除外情報」の範囲や規律に関する技術的な検討が必要となるであろう。」旨を指摘したところである。今回、「（仮称）法第23条第1項適用除外情報」をベースにする「（仮称）個人特定性低減データ」について検討するに当たっても、その範囲が必ずしも明確になっている

とはいえないことから、次の2つの項に示すような前提をおいて、検討したものである。

1.2.2 「(仮称) 準個人情報」及び「(仮称) 個人特定性低減データ」に起因する権利利益侵害の場合分けについて

第7回親会に事務局から提案された「(仮称) 準個人情報」については、「特定個人を識別しないが、その取扱いによって本人に権利利益侵害がもたらされる可能性があるもの」とされているが、ここで本人の権利利益侵害には、次の二つの場合が想定される。

- ①「(仮称) 準個人情報」から何らかの状況で個人が特定されてしまうことで、権利利益侵害が生じる場合
- ②「(仮称) 準個人情報」から個人が特定されないままで、権利利益侵害が生じる場合

これを前回報告書におけるパーソナルデータの3分類（識別特定情報、識別非特定情報、非識別非特定情報）との関係で捉えると、①の場合は識別非特定情報が識別特定情報になり得てしまう状態であり、例えば、「(仮称) 準個人情報」を利用して、個人に関する情報とマッチングした結果、特定の個人が識別されて（個人が誰なのかが分かってしまう状況）、その結果、何らかの個人の権利利益の侵害が生じることである。一方、②の場合は識別非特定情報を通じた侵害、つまり「(仮称) 準個人情報」を利用して、個人に関する情報とマッチングした結果、特定の個人は識別されていないが個人の属性が推定されるなどして、何らかの個人の権利利益の侵害が生じることである。

このように、「(仮称) 準個人情報」及び「(仮称) 個人特定性低減データ」による個人の権利利益の侵害には二つの場合があり、本来はそれぞれの場合に関して検討すべきであるが、WGでは①の場合のみを検討した。これは、「(仮称) 準個人情報」については「個人情報」（識別特定情報）に該当するような特定性が高まり得る識別非特定情報として、また、「(仮称) 個人特定性低減データ」については「個人情報」（識別特定情報）に再特定されにくい程度に特定性が低い識別非特定情報として情報の外形的な特性について検討することとしたものである。

一方、②の場合に関しては、権利利益の侵害に至るかは個々のケースに依存し、ある同じ「(仮称) 準個人情報」又は「(仮称) 個人特定性低減データ」を利用して、個人に関する情報とマッチングしたとしても、個人の権利利益に侵害が生じるケースと生じないケースがあり、さらに、その両ケースの差も明確ではないため、技術的な見地からだけでは検討できないと判断したものである¹。②の場合に関しては、個々のユースケースや制度面を含めて、別途検討すべきである。

¹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の明確化」として「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。」が挙げられている。そこでWGでは「実質的に個人が識別される可能性を有するもの」を検討対象とした。なお「プライバシー保護という基本理念を踏まえて判断」は技術的な見地では検討しきれない。

1.2.3 「(仮称)個人特定性低減データ」に関する権利利益侵害発生時の責任について

「(仮称)個人特定性低減データ」は、WGが前回報告書において「(仮称)法第23条第1項適用除外情報」としていたものであり、特定の個人の識別を不可能にする加工方法等を汎用的に定めることができないものであることを報告した。

本人の同意を得ることなく第三者に提供することとした場合、本人に権利利益侵害がもたらされにくいようにするという安全性の観点からは、特定性をより低減すべきであるが、特定性を低減すると併せて識別性も低減することが考えられる。そのため、特定性を低減していくうちに、仮に識別性がなくなった情報は、非識別非特定情報となり、そもそも保護する必要がなくなる。しかしながら、識別非特定情報としての利活用を考える場合には、特定性を低減させて安全性を確保しつつ、有用性を考慮してある程度の識別性を残すように検討する必要がある。

このようにある程度の識別性を残したままで、特定性を低減した場合には、加工後のデータそのものによる特定の可能性のほかに、他のデータと照合することによる特定の可能性についても考慮する必要がある。

ここでは第三者に提供する場合を想定していることから、照合による特定の可能性については、提供先事業者（受領者）がどのような個人データ等と照合できるかによって変わることとなる。しかし、提供元事業者は、提供先事業者（受領者）がどのような個人データ等と照合できるのかを予見することは、技術的な見地からはできないものである。

このため、「(仮称)個人特定性低減データ」については、次に示す2つの前提の下で、検討した。

前提①

提供元事業者（提供者）による「(仮称)個人特定性低減データ」への加工等については、提供しようとする「(仮称)個人特定性低減データ」単独での特定性の低減についてのみを対象とする。

前提②

提供元事業者（提供者）は、提供先事業者（受領者）における「(仮称)個人特定性低減データ」と照合可能な個人データ等の有無について予見できない。

この前提において、万が一、提供先事業者（受領者）が受領した「(仮称)個人特定性低減データ」を他の情報と照合して、特定の個人を識別した場合には、一義的には提供先事業者（受領者）における特定化禁止に関する違反が問われることとなるものである。

2 「『個人情報』等保護されるパーソナルデータの範囲」について

2.1 「個人情報」と「(仮称)準個人情報」との関係

WGは、検討の結果、多量又は多種の情報が収集されることにより特定の個人が識別されるおそれのある情報を「(仮称)準個人情報」とすることが妥当であると考えた。その理由は、以下のとおりである。

まず、現行法における「個人情報」は、「特定の個人を識別することができるもの」と定義されており、現行法は、この個人情報を基本的な保護対象としている。「個人情報」を保護の客体としている趣旨は、その「名寄せの容易さ」及び「人との結びつきの明確さ」から、取扱いによって本人の権利利益の侵害がもたらされる可能性があるためである。

次に、見直し方針は、制度見直しの方向性について、プライバシーの保護を掲げているところ、個人の特定性がプライバシー侵害の必要条件であるとする複数の裁判例が公表されている²。

このように特定の個人が識別されることによって、個人の権利利益の侵害の危険性が格段に高まるものであることから、現行法では、個人情報を取り扱う事業者の行為を定め、適正に取り扱うことによって、本人の権利利益の侵害を未然に防ぐこととしているものと解することができる。

ところが、情報通信技術が進展した現状では、個人に関する情報の流通量が爆発的に増加するとともに、情報の収集や分析が容易になっており、ある時点において特定の個人が識別されていない情報であっても、他の情報と容易に結びつくことで特定の個人が識別される蓋然性が高まっている（それによって個人の権利利益の侵害が生じ得る）。この点は、前回報告書において、WGが既に指摘したところである。

よって、特定の個人が識別されていない情報であっても、特定の個人が識別されるおそれのある情報を「(仮称)準個人情報」とするという考え方は妥当性があるものと考えられる。

また、特定の個人が識別されるおそれは、多くの場合、当該個人に関する多量又は多様な情報が収集されることによって生じることから、そのような情報収集を行うものを「(仮称)準個人情報」の対象とすべきである。さらに、こうした情報収集を可能とするものとして識別子が相当し得るが、様々な識別子がある中でも、特にその性質・特性から多量又は多様な情報を収集することとなる蓋然性が高いものに限定すべきであると考えられる。換言すれば、「(仮称)準個人情報」となるものの範囲について、識別子となり得るものすべてを対象とするのではなく、相対的に多量又は多様な情報を収集することができないであろう識別子は、対象としないこととすることが適当であると考えられる。

² 裁判例

- ・ 政党機関紙購読アンケート事件（横浜地裁川崎支部判決平成 21 年 1 月 27 日）
- ・ 共同通信社北朝鮮スパイ報道事件（東京地判平成 6 年 4 月 12 日）
- ・ 政党機関紙購読アンケート事件（横浜地裁川崎支部判決平成 21 年 1 月 27 日）
- ・ 長良川リンチ殺人報道事件（最判平成 15 年 3 月 14 日）

なお、特定の個人を識別することによって、個人の権利利益の侵害の危険性が格段に高まるものであることは上述のとおりであるが、特定の個人が識別されなければ権利利益の侵害が生じないわけではない。我が国の法制度は、特定の個人が識別されなくても権利利益の侵害が生じ得ることを正面から認めている。例えば、「行政機関の保有する情報の公開に関する法律」第5条第1号は、「特定の個人を識別することはできないが、公にすることにより、なお個人の権利利益を害するおそれがあるもの」を不開示情報（開示請求の対象とならない情報）としている。どのようなものがこれに当たるかについては、個人の人格に密接に関わる情報である等の説明がなされている³。

このように特定の個人を識別することなく権利利益の侵害が生じるおそれのあるものについては、その存在は明らかであり、また、識別子を利用した多量又は多様な情報の収集が、この種の権利利益の侵害につながる可能性があることも十分に予想し得るところである。しかしながら、結局のところ、どのような情報が「個人の人格に密接に関わる」か等は、WGの専門的知見の及ぶところではないため、この問題については、親会における検討に委ねることとする。

さらに、一事業者内に「個人情報」と「(仮称)準個人情報」が混在して存在する場合において、それらが一体となって特定の個人に結び付いて利用・管理されているものに関しては、全体として「個人情報」としての取扱いが求められるものである。特に、複数の項目によって特定の個人が識別されている場合において、当該項目に「(仮称)準個人情報」に含まれる多量又は多様な情報を収集することとなる蓋然性が高い識別子に該当する項目がある場合には、個人情報としての取扱いを要するものである。同様に、通常は「(仮称)準個人情報」に含まれる多量又は多様な情報を収集することとなる蓋然性が高い識別子と考えられる項目であっても、ある特異な状況においては、その項目だけで個人情報となり得る場合があるものと考えられる（例えば、氏名、会社名等が明示されているメールアドレス）。

なお、本検討は、「(仮称)準個人情報」となる範囲の明確化をしたものであり、法の条文において個人情報の定義に内包させるべきか否かを検討したものではない。

2.2 「(仮称)準個人情報」の定義等について

2.2.1 「(仮称)準個人情報」に該当するものを選定する指標についての検討

2.1において述べたとおり、WGは、様々な識別子がある中でも、特にその性質・特性から多量又は多様な情報を収集し、特定の個人が識別されることとなる蓋然性が高いものに限って対象とすべきであると考えた。そこで、いかなる識別子が「特にその性質・特性から多量又は多様な情報を収集し、特定の個人が識別されることとなる蓋然性が高い」かの判断要素・指標を明らかにする必要がある。この点について検討した結果は、以下のとおりである。

(ア) 本人に付与されるものか、所有物に付与されるものか。

本人に付与されたものは、本人の所有物に付与されたものと比較して、本人との直

³ 宇賀克也（東京大学教授）／著「新・情報公開法の逐条解説（第6版）」（有斐閣）71頁

接的な関係があることから、特定の個人を識別する蓋然性は高いといえる。

また、本人に直接に付与されたものではないが、例えば、携帯電話等は、常に所有者が持ち歩いており、他人が使用するケースも極めて稀であると考えられ、こうした携帯電話等のモバイル通信機器に付与された番号等については、本人との密接性から、特定の個人を識別する蓋然性は、他の機器等と比較して高くなり得る。

(イ)一意性（重複性）

他と重複することがないように、一つの対象に一つの識別子が付与されている場合には、対象が異なっても同一の識別子が存在する可能性がある場合と比較して、特定の個人を識別する蓋然性が高いといえる。

(ウ)単射性

個人の集合から識別子への写像において、ある値域に属する元がいずれもその定義域のただ一つの元の像として表されるものであり、一対一の写像の関係にあるものは、一対多、あるいは多対一の関係にあるものと比較して、特定の個人を識別する蓋然性が高いといえる。（上記（イ）「一意性」（重複性）と一体的に検討。）

(エ)共用性

本人や所有物等に付与された番号や記号である識別子について、当該識別子を発行・管理する事業者に限らず発行された識別子を取得しようとした複数の事業者が独立に取得できる場合（識別子を発行・管理した事業者に依ることなく直接取得できる場合を含む。）には、発行・管理する事業者のみで利用する場合と比較して、同一の識別子を広く複数の事業者で保有する（共用する）可能性が高まることから、多くの情報を収集しやすくなり、特定の個人を識別する蓋然性が高いといえる。

また、複数の事業者に限らず、一事業者であっても様々な業種にわたって広くサービスを提供している場合には、単一のサービスを提供している一事業者よりも情報が集積し、個人が特定される蓋然性は高くなるといえることから、このように複数のサービスで利用されている場合も当該指標に合致するものとして考えることとする。

(オ)変更可能性

本人の意思により、付与された番号等が変更可能であるものと、変更できないものとは、個人の特定性に差が生じる。

また、本人の意思により変更可能であるものであっても、容易には変更できない場合には、容易に変更できる場合と比較して、個人の特定性に差が生じることがあり、特定の個人を識別する蓋然性が高くなり得る。

(カ)不変性

本人の意思に依らず、時間や状態によって動的に変化するものは、外的要因によって変化しない静的なものと比較して、特定の個人を識別する蓋然性が低くなることが多い。なお、本指標は、主として身体的特徴に関するものであると考えられ、静的で不変性があるものは変更が困難なものとして、上記「(オ) 変更可能性」に含めて検討することが可能であると考えられる。

(キ)利用停止可能性

一旦識別子が付与されたものについて、本人の意思等の何らかの事情により、当該識別子に関する利用を停止できる機能がない場合には、機能がある場合と比較して、特定の個人を識別する蓋然性は高くなるといえる。具体例としては、適正なオプトアウトの機能が設けられている場合には、本人の意思により容易に識別子と紐づく情報を切り離すことができる。なお、本指標についても、上記「(オ) 変更可能性」に含めて検討することが可能であると考えられる。

(ク) 継続性（利用期間）

継続して同じ番号等を使用する場合には、短期間で削除・変更される場合と比較して、特定の個人を識別する蓋然性が高くなるといえる。

もともと、継続性がある情報が必ずしも特定の個人を識別するとは限らず、一時的にしか用いられないものであっても特定の個人を識別する蓋然性の高いものはあるなど、結局他の性質によって特定性が判断されることとなるため、継続性そのものを何らかの指標とすることは困難であると考えられる。

(ケ) 利用範囲/データの規模

一般的に、利用範囲が広範になると、多くの情報の集積が進むと考えられる一方、利用範囲を限定しデータを絞ることによって、特定の個人を識別する蓋然性が高くなる場合も考えられる。したがって、利用範囲/データの規模を指標とすることについては、その特性から困難であると考えられる。

その他、(コ) 悉皆性、(サ) 外観識別性、(シ) 外部情報入手可能性、(ス) 本人到達可能性等の項目も考えられるが、特に特定の個人を識別する蓋然性を高くするような性質や特性を有しているものではないと捉え、具体的な指標としていない。以上を踏まえ、指標となり得る(ア) から(ケ) の9項目について検討した結果、(ク) 継続性(利用期間) 及び(ケ) 利用範囲/データの規模については、指標として機能することが明確ではないことから、除外する。また、(イ) 一意性(重複性) と(ウ) 単射性については一体的に検討することが妥当であり、(オ) 変更可能性、(カ) 不変性、(キ) 利用停止可能性については、ほぼ同一の視点で検討できるものであり、これらを一つの指標として検討しても差し支えないものと考えられる。よって、指標については、(ア) については本人又は本人の所有物と密接性があるもの、(イ) 一意性/単射性があるもの、(エ) 共用性があるもの、(オ) 変更可能性/不変性/利用停止可能性については容易に変更できないもの(静的であるもの)として、これらのすべての指標に該当する場合は、多量又は多様な情報を収集し、特に特定の個人を識別する蓋然性が高い識別子とすることが適当であると考えられる。

2.2.2 事務局から提案された「(仮称) 準個人情報」の定義についての検討

事務局から提案された「(仮称) 準個人情報」の定義は、以下のとおりである。

【事務局案】

個人情報に該当するものを除き、 <u>生存する個人に関する情報であって、次に例示するもの及びこれに類するものを含む情報</u>

- ① パスポート番号、免許証番号、IP アドレス、携帯端末 ID 等の個人または個人の情報通信端末（携帯電話端末、PC 端末等）等に付番され、継続して共用されるもの
- ② 顔認識データ、遺伝子情報、声紋並びに指紋等、個人の生体的・身体的特性に関する情報で、普遍性を有するもの
- ③ 移動履歴、購買履歴等の特徴的な行動の履歴

事務局案として提示された具体的な分類である①から③のうち、①については、正に他と区別するために識別子として付与されている性質のものであり、②については、身体的特徴等から他人とは異なる一意性を導くことができるものである。これらについては、多量又は多様な情報を収集する識別子として機能するものであることが認められる。他方で、③については、①又は②とは異なる分類となることから、「③移動履歴、購買履歴等の特徴的な行動の履歴」について、どのような状態であることが多量又は多様な情報を収集する識別子相当としての機能を有する場合であるかを検討する必要がある。

なお、ここでいう「移動履歴、購買履歴等の特徴的な行動の履歴」は、①に示すような他の識別子を伴っていない場合を前提としており、移動履歴又は購買履歴そのものが、特徴的であることから識別子として機能する場合があることを指摘しているものである。

(ア) 移動履歴と購買履歴の特性

移動履歴と購買履歴は人の行動履歴であり、他人の行動との相違については、通常、その情報が蓄積されればされるほど、特定の個人が識別される可能性は高くなる。また、他人とは違う特異な日時に、又は特異な行動（乗降客数の少ない駅での乗降、一点ものの買い物等）をすることで、他人と区別される可能性が高いといえ、個人を識別できる情報であるということは可能である。ただし、いったい何が特徴的な行動履歴で何がそうでないかを一律の基準に基づいて判断することは困難である。

(イ) 移動履歴

複数の位置情報の履歴の集合である移動履歴は、正確な時刻と組み合わせることによって、また、当該情報の取得の頻度が高ければ高いほど、個人の生活圏や行動パターンが分かり、特定の個人の識別につながる可能性が高くなるものである。また、継続的な履歴の取得は、繰り返される行動パターンが分かり、それによっても特定の個人の識別につながる可能性が高くなる。

移動履歴が購買履歴と異なる点としては、複数の事業者が同時にかつ独立して同じ情報を取得できることが挙げられる。例えば、携帯電話にインストールされている複数のアプリケーションから同時にかつ独立して時刻と GPS 情報を取得することが可能であり、これが情報を集積する識別子として機能する可能性がある。また、GPS 情報等の極めて精度の高い位置情報に関しては、2 地点間以上の位置情報である移動履歴とする必要もなく、時刻との組合せによって、特定の個人を識別する可能性が高い情報となり得る。（例えば、深夜 2 時の正確な緯度経度の情報は、自宅である可能性が高いと考えられる。また、同じ時間帯での同種の情報の取得が数回

繰り返され、同じ位置情報が得られるのであれば、その緯度経度がほぼ自宅であると推定されるであろう。)

こうしたことから、移動履歴については、2 地点以上の位置情報の行動履歴に限らず、正確な（一地点の）位置情報と時刻の組合せによって、特定の個人を識別する識別子として機能するものと考えられる。

しかしながら、移動履歴については、その情報量、取得期間・取得頻度、位置情報や時刻の精度等の個別の条件によって、特定の個人を識別する場合もあれば、他人と何ら区別なく特定の個人を識別できない場合があり、どのような状態であれば識別子として機能する特徴的な状態であるかを一律に定めることは困難である。

その上で、時刻を伴う位置情報、移動履歴を何らかの基準で特徴の有るものと無いものに分類することなく総体として捉えた場合、2.2.1 で示した指標（(ア)については本人又は本人の所有物と密接性があるもの、(イ)一意性/単射性があるもの、(エ)共用性があるもの、(オ)変更可能性/不変性/利用停止可能性については容易に変更できないもの（静的であるもの）をすべて満たすか否か、について検討した結果、特に、「(オ)変更可能性/不変性/利用停止可能性については容易に変更できないもの（静的であるもの）」という指標への該当性について、一律な判断が困難であるという結論に達した。例えば、スマートフォン上のアプリケーションを考えた場合、GPS 位置情報の取得については、端末上で位置情報を取得しない設定にしたり、位置情報を取得するサービスを利用しないようにしたりなど、本人の意思で容易に利用停止できるという考え方もある一方、取得された位置情報の利用を停止するということについては、サービス提供者が本人からの申出により利用停止する機能を提供していない限り利用停止することはできず、利用停止は容易ではない、とする考え方もある。

以上を踏まえ、現時点では、移動履歴を「(仮称)準個人情報」の範囲には含めず、実態を踏まえたより詳細な検討を加えることが必要であるものと考えられる。

(ウ) 購買履歴

購買履歴は、顧客単位に購入品名や数量、購入日時、購入店名などを記録した情報である。購買履歴に氏名や会員番号等の特定の個人を識別し得る属性情報が含まれていなくても、継続的な履歴の取得により、繰り返される行動パターン等が分かり、その結果として特定の個人の識別につながる可能性がある。したがって、長期間にわたり、継続的に取得された購買履歴については慎重な取扱いが必要である。また、履歴の取得期間が短くても、特徴的な購入がある場合は、特定の個人の識別につながり得ることに留意すべきである。例えば、一点ものの購入、購入の数量、時刻、場所等が特異な場合には、他の情報と照合することで、特定の個人の識別につながる可能性がある。

その他、購買履歴が個人の権利利益に影響するという点では、購入品の種目にも留意すべきである。医薬品等については個人の病歴を含む可能性があること、書籍等については思想信条を含む可能性があることは否定できない。一方で、一般の食品や日用品に関しては、その購入品名や数量、場所、時間等に特徴がなければ、直ちに特定の個人の識別につながる可能性は低いといえる。

以上のように、長期の継続的な履歴取得、特徴的な購入がある場合、購入品に関する一意な番号（個体識別可能な番号）を含む場合、購入者が公開される場合などにおける購買履歴は、特定の個人を識別し得る情報となり、その場合には特定の個人の識別性のおそれの高いものとして扱うべきだが、一方で、特定の個人の識別性に実質的に影響のない購買履歴も多い。このため、仮に購買履歴を「(仮称)準個人情報」として扱うにしても、すべての購買履歴を「(仮称)準個人情報」とすべきではなく、上記の特定の個人の識別につながり得るような購買履歴に限定されるべきであるが、どのような状態であれば識別子として機能する特徴的な購買履歴となるかを一律に定めることは困難である⁴。

また、2.2.1 に示した指標への妥当性については、(ア) と (オ) の要件を満足する。さて食料品や日用品などは販売数が多く、ある商品の購入者は一人に限定されず、多数の購入者がいると考えられ、その商品の購入と個人が一对一に対応付けられるとはいいいにくい。また、購買履歴は広く販売されている商品でも、購入品の組合せに特徴がある場合があるが、一般に取得期間が短い履歴であれば、特定の個人と対応づけられる可能性は低くなる。以上より、購買履歴には(イ) 一意性/単射性があるとは必ずしもいえない。よって、現時点では、購買履歴を「(仮称)準個人情報」の範囲には含めず、実態を踏まえたより詳細な検討を加えることが必要であるものと考えられる。

なお、購入履歴に、購入品の個体識別ができる番号（シリアル番号など）や、RFID タグを貼付するなどして商品毎に付番した一意な番号（個体識別可能な番号）などが含まれる場合は、購入商品には(イ) 一意性/単射性があることになり、それを含む購買履歴は「(仮称)準個人情報」として保護されるべきである。このほか、一般の購買履歴には、購入店名など多様な情報が付随するが、購入店名は位置情報となり、位置情報に関わる取り扱いをすべきである。また、購買履歴に付随する情報によっては特定の個人の識別につながる可能性があることもあり、注意して取り扱う必要がある。

2.2.3 Web 閲覧履歴（Cookie 等を含む）に関する検討

「(仮称)準個人情報」に含まれる項目を整理するに当たり、親会においても Cookie の取扱いについて指摘があったところであり、Cookie に限らず Web 閲覧履歴を取得するための技術的な仕組みとそれによって取得される Web 閲覧履歴の取扱いについて検討した。

(ア) Web 閲覧における識別子の現状

Web 閲覧履歴は、直ちに特定の個人を識別するとは限らなくても、個人の関心事、趣味嗜好を反映するとともに、事業者においてはビジネス上の関心などが表れるために、その取扱いに留意すべきである。 Web 閲覧履歴を調べる方法として広く利用

⁴ 基準は明らかではないが、食料品や日用品など、販売数が多く、さらにその購入者が多いような商品に関しては、ほぼ特定の個人を識別する可能性はないと見てよいと考えられる。なお、該当する商品に医薬品や書籍などを含めるかは慎重な議論が必要である。

されているのが、Cookie（参照：IETF RFC 2965, HTTP State Management Mechanism, published in 2000, available at: <http://www.ietf.org/rfc/rfc2965.txt>）である。Cookie は、事業者が提供する Web サービスへのアクセスにおいて、ある個人が同じ Web サーバに複数回にわたって接続したとき、前回の設定（ログイン状態や入力など）を保持できる一方、サーバはその情報をもとにしてユーザのアクセス履歴の収集を容易にする。また、Cookie は大きく分けて、ファーストパーティ Cookie とサードパーティ Cookie がある。ファーストパーティ Cookie は現在表示中のドメイン又はサブドメイン内のサーバによって発行された Cookie であり、アクセス履歴として、利用者の現在表示中のドメイン又はサブドメインへのアクセス時間や頻度等を調べるなど、そのドメイン又はサブドメインに関するアクセス履歴を収集することができるが、利用者が同じサーバ又は同じドメイン内のサーバに再びアクセスしたとき、再ログインを不要とすることや、前回のアクセスの際の入力情報などを保持するなど、利用者にとって利便性もある。

一方、サードパーティ Cookie は、Web ブラウザに表示されている現在表示中のドメイン及びサブドメインにはない他のドメインに属するサーバによって発行された Cookie であり、Web ページに不可視な情報として埋め込まれることが多く、一般に利用者はサードパーティ Cookie の存在に気づくことは難しい。サードパーティ Cookie は、ファーストパーティ Cookie と同様に、Web 閲覧履歴を収集するものであるが、ドメインが異なる多数の Web ページにサードパーティ Cookie が埋め込まれていると、利用者が当該 Web を閲覧した時、サードパーティ Cookie の発行者は利用者を識別し、さらにその利用者による複数のドメインにおける過去の閲覧履歴と情報をマッチングすることができる。つまり、サードパーティ Cookie を通じて、ドメインをまたがった Web 閲覧履歴を調べることが可能となる。その結果として、サードパーティ Cookie の発行者は、ファーストパーティ Cookie と比較して広く利用者の関心事や趣味嗜好を分析することが可能となり、その情報をもとにして広告を選別的に Web ブラウザ上で表示することができる。なお、サードパーティ Cookie に関しては、広告が利用者に応じて選択・表示されるという利便性はあるが、利用者にとって積極的な利便性があるとは言い難いと考えられる。

この他、Cookie Sync と呼ばれる技術で、ある事業者が他事業者の Cookie（正しくは Cookie を通じて各 Web ブラウザに付番された識別子）を共用する手法も広く利用されており、Cookie による Web 閲覧履歴の収集範囲は広がっている状況である。

また、新しいタイプの Cookie 相当の技術や手法が次々と生まれており、その一例を挙げると、Supercookie や Flash cookie などがあり、HTML5 の Web Storage でも Cookie 相当の情報を保持できる可能性がある。さらに従来の Cookie などを Web ページに置くことなく、Web ブラウザの種類やバージョン、インストール済みのプラグインの種類、OS、IP アドレスなどの情報から高精度で、接続された Web ブラウザを識別する技術（いわゆるフィンガープリント技術であり、代表的なものとして、ADTruth がある。）が登場しており、その情報をもとに、利用されている Web ブラウザを識別する情報を収集したり、Web ブラウザの識別子も

発行されたりといったことが行われている。

このように、Web ブラウザの閲覧履歴は、主に広告目的とはいえ、ドメインをまたいで広範囲に収集・利用されており、それを実現する技術は日進月歩に進化している状況にあるといえる。

(イ) Web 閲覧履歴情報の取扱い

Cookie を含む Web 閲覧に関する識別子などは、それ自体は特定の個人を識別するものではないが、Web アクセスに関する端末やブラウザに一意に割り当てられる、識別情報といえる。上記のように Web 閲覧履歴は、多くの Web サイトにまたがって多様な個人の関心事、趣味嗜好を収集することが可能である。このため、Cookie など Web ブラウザにおける識別子を利用することで、特定の個人を識別する可能性が生じ得るため、特定性をもつ情報として扱うべきものといえる。しかしその一方で、広く利用されている多くの Web ブラウザには Cookie を制限する機能があり利用者の意思で一定程度の制限が可能であるほか、利用者の利便性につながるものであることを踏まえ、すべての Cookie を含む Web に関わる端末やブラウザを識別する情報を制限すべきではないと考えられる。また、当該分野は技術の移り変わりが早いことから、技術そのものではなく、個人又は個人が利用する Web ブラウザを識別する情報が共有される範囲によって、取扱いを定めることが適当である。例えば、①単一の特定の事業者だけで保有される場合、②複数の特定の事業者で共用される場合、③不特定多数の事業者で保有される場合に分類することなどが考えられる。具体的には、①の場合に関しては、利用者が現在表示中のドメイン名から Cookie の発行／利用者である事業者が特定できることに加え、利用者の利便性にもつながるものであることから、情報の取得時における同意は不要とするとも考えられる。②と③の場合に関しては、Cookie やそれに関連する情報の発行主体（利用者）である事業者が明記されるとともに、収集される Web アクセス履歴の利用目的や提供先の明記、同意取得、オプトアウトなどを行うことが考えられる。

2.2.1 で示した指標（(ア) 本人又は本人の所有物と密接性があるもの、(イ) 一意性/単射性があるもの、(エ) 共用性があるもの、(オ) 変更可能性/不変性/利用停止可能性については容易に変更できないもの（静的であるもの））への該当性については、まず、Cookie は（ア）と（イ）を満たしている。他の Web に関わる端末やブラウザを識別する情報については、一対一に識別子を割り当てられているとは限らないが、その割り当ては高精度であることから、（ア）と（イ）を満足するといえる。（エ）については、ファーストパーティ Cookie などは一般的には共用性があるとはいえないが、上記のとおり多様な手法や技術があり、その中には共用性が認められるものもある。（オ）については、例えばブラウザの設定によって Cookie を受け入れないようにすることが可能である一方で、すべてのブラウザについてそのような設定が可能なのではなく、さらに Cookie の種類によってはそのような設定ができない場合もある。このように Cookie を含む Web に関わる端末やブラウザを識別する情報に関しては、その取り扱いが多様であるために、（オ）についても一律に該当するか否かを判断できるものではない。

以上を総合的に判断した結果、Cookie を含む Web に関わる端末やブラウザを識

別する情報は（ア）と（イ）については要件を満たすが、（エ）についてはその情報の共用範囲によるために、一律に判断できない。また、（オ）についても一律に判断できないが、その情報取得の目的や範囲が何らかの方法で利用者がわかり、さらに利用者が識別子としての番号そのものをリセット又は取得・利用停止を選択できる機能（例えば、オプトアウト）を有している場合は、（オ）を満足しないといえる。ただし、利用者における当該機能の実行可能性をより詳細に分析を加えながら、個別に精査・判断するべきといえる。このためWGでは、技術的な見地から Cookie を含む Web に関わる端末やブラウザを識別する情報の取扱いを検討したが、「（仮称）準個人情報」とすべきか否かに関する一律な基準を設けることはできない。その取扱いは個別ケースに依存して、技術的な見地だけで判断できることではなく、Cookie を含む Web に関わる端末やブラウザを識別する情報を「（仮称）準個人情報」を、制度的な側面と合わせ、引き続き検討が必要すべきと考えられる。

さらに、Web 観覧履歴が、利用者が過去に見た Web 観覧先を表す情報（例えば観覧した URL など）の集まりであったとき、その観覧先を示す情報に「個人情報」に相当する情報が含まれれば、それぞれは「個人情報」として扱うべきであり、「個人情報」が含まれず、「（仮称）準個人情報」に相当する情報に相当する情報が含まれれば、「（仮称）準個人情報」として扱うべきである。なお、個人に依拠して動的に生成される Web ページに関しては、その Web ページを指し示す情報の中に、その個人を識別する識別子等が含まれ、2.2.1 の要件（イ）と（エ）を満たす場合、「（仮称）準個人情報」となりえることがあり、慎重な取り扱いが必要である。なお、Web 観覧履歴に含まれる観覧先を表す情報が指し示した Web ページの内容による特定の個人の識別の可能性は否定できないが、技術だけで判断できないことから、WG としては扱わないこととした。

2.2.4 「（仮称）準個人情報」の定義について

以上の検討を踏まえ、事務局が先に提示した「（仮称）準個人情報」の定義を、以下に示す事項を含む趣旨となるように変更することを提案する。

- ・ 個人情報ではないこと
- ・ 生存する個人に関する情報に含まれる識別子又は識別子に相当するものであって、①一意性/単射性を有するもの、②共用性を有するもの、③変更又利用停止が容易ではないもの、または不変性を有するものであること
- ・ 上記の条件をすべて満たす識別子又は識別子に相当するものであって、密接性を有するものとして、以下のいずれかに該当するものであること
 - ア) 個人又は個人が使用する通信端末機器等に関するもの
 - イ) 個人の身体的特性に関するもの
 - ウ) 上記の 2 項目のほか、特定の個人の識別につながる多量又は多様な情報の収集を可能にするもの
- ・ ア) については、付番された本来の用途まで制約しようとする趣旨ではないことを明確化すること

(例えば、IP アドレスや MAC アドレスを例にとって考えてみた場合、IP アドレスは、IP ネットワーク上に接続された機器を識別するために指定する番号であり (MAC アドレスは、データリンク層の物理アドレス)、いわばインターネットなどの IP ネットワークにおける個々の機器等の住所に相当する。IP ネットワークにおいて IP アドレスの交換は通信を成立される上での前提条件であり、これを「(仮称) 準個人情報」として定義することにより、付番された本来の用途まで制約をしようとする趣旨ではないことを明確化しておくものである。)

- ・ア) からウ) に含まれる具体的な項目については、技術の進展等の急速な時代の変化への対応が必要であることから、政令等で追加、変更、削除ができるようにすること、また、第三者機関が適切かつ迅速な判断を可能とする仕組みとすること
- ・上記の要件を満たす識別子又は識別子に相当するものに付随する個人に関する情報も「(仮称) 準個人情報」に含むものとする

ただし、ウ) のカテゴリーについては、上記のとおり、明確に当該分類に該当するといえる項目として判断できたものはないが、その一方で、識別子として機能するほか、多量又は多様な情報収集の結果として、特定の個人を識別することなく「個人の人格に密接に関わる」情報となる可能性を有するものであり、特定性のない情報でありながら個人の権利利益を侵害する可能性があるものとして、親会における検討が期待されるものである (2.1 参照)。

2.2.5 「(仮称) 準個人情報」に含まれる具体的な項目について

2.2.1 から 2.2.4 に基づき、「(仮称) 準個人情報」に含まれる具体的な項目について検討した結果を示す。

まずは、下記のとおり、個人情報の取扱いと関係すると考えられる現存する識別子又は識別子としての性質を持つと考えられるものを挙げ、それらを各指標に沿って分類した。その上で、すべての指標に合致した識別子等が、特に特定の個人を識別する蓋然性が高いものとして、「(仮称) 準個人情報」に該当することとしたものである。なお、本検討においては、考えられる識別子等を網羅的に挙げて検討したのではなく例示を挙げて検討したものである。また今後の技術進展等によっても状況は変化するものと考えられることから、常に最新の状況に見合った見直しを行っていくことが必要である。

個人情報の取扱いと関係すると考えられる現存する識別子又は識別子としての性質を持つと考えられるもの

個人又は個人が使用する通信端末機器等に関するもの	運転免許証番号、パスポート (旅券) 番号、健康保険証の記号・番号 (健康保険被保険者証記号番号等)、雇用保険被保険者番号、金融機関の口座に関する番号、クレジットカード番号、メールアドレス、ユーザ
--------------------------	--

	ID・パスワード(複数事業者、又は一事業者内の複数サービスで共用)、ユーザID・パスワード(一事業者内)、ナンバープレート(自動車登録番号標等)番号、固定電話番号、携帯電話番号、Webフィンガープリント ⁵ 、情報通信端末シリアルナンバー(携帯電話端末シリアルナンバー等)、MACアドレス、情報通信端末ID、ICカードの固有ID、ソフトウェアシリアル番号 ⁶ 、不動産番号、IPアドレス(V6)
個人の身体的特性に関するもの	声紋、指紋、静脈パターン、虹彩、DNA、顔認識データ、掌形、生体認証で使用されるデータ ⁷ 、歩行パターン、筆跡、性別、肌の色、人種、家族構成、血液型、髪の色、血圧、脈拍、身長、体重
上記のほか、特定の個人の識別につながる多量又は多様な情報の収集を可能にするもの	

上記の項目を各指標に沿って、分類した結果は、以下のとおりである。

(ア) 本人又は本人の所有物との密接性

本人又は本人の所有物と密接性があるもの	運転免許証番号、パスポート(旅券)番号、健康保険証の記号・番号(健康保険被保険者証記号番号等)、雇用保険被保険者番号、外国人の在留に関する番号(在留カード番号、特別永住者証明書番号、外国人登録証明書番号)、金融機関の口座に関する番号、クレジットカード番号、メールアドレス、ユーザID・パスワード(複数事業者、又は一事業者内の複数サービスで共用)、ユーザID・パスワード(一事業者内)、ナンバープレート(自動車登録番号標等)番号、固定電話番号、携帯電話番号、Webフィンガープリント、情報通信端末シリアルナンバー(携帯電話端末シリアルナンバー等)、MACアドレス、情報通信端末ID、ICカードの固有ID、ソフトウェアシリアル番号、不動産番号、IPアドレス(V6) 声紋、指紋、静脈パターン、虹彩、DNA、顔認識デー
---------------------	---

⁵ Cookie を含む Web に関わる端末やアプリケーションソフトウェア (Web ブラウザを含む) を識別する情報

⁶ 個人や端末を識別することができるものに限る。

⁷ センシングした生データだけではなく、生体認証方式固有の方法で数値化したデータも含む。また、顔画像認識データも含む。

	タ、掌形、生体認証で使用されるデータ、歩行パターン、筆跡、性別、肌の色、人種、家族構成、血液型、髪の色、血圧、脈拍、身長、体重
上記以外のもの	

(イ) 一意性/単射性

一意性/単射性があるもの	運転免許証番号、パスポート（旅券）番号、健康保険証の記号・番号（健康保険被保険者証記号番号等）、雇用保険被保険者番号、金融機関の口座に関する番号、クレジットカード番号、メールアドレス、ユーザID・パスワード（複数事業者、又は一事業者内の複数サービスで共用）、ユーザID・パスワード（一事業者内）、ナンバープレート（自動車登録番号標等）番号、固定電話番号、携帯電話番号、Webフィンガープリント、情報通信端末シリアルナンバー（携帯電話シリアルナンバー等）、MACアドレス、情報通信端末ID、ICカードの固有ID、ソフトウェアシリアル番号、不動産番号、IPアドレス(V6)、声紋、指紋、静脈パターン、虹彩、DNA、顔認識データ、掌形、生体認証で使用されるデータ、歩行パターン、筆跡
上記以外のもの	性別、肌の色、人種、家族構成、血液型、髪の色、血圧、脈拍、身長、体重

(エ) 共用性

共用可能性があるもの	運転免許証番号、パスポート（旅券）番号、健康保険証の記号・番号（健康保険被保険者証記号番号等）、雇用保険被保険者番号、外国人の在留に関する番号（在留カード番号、特別永住者証明書番号、外国人登録証明書番号）、金融機関の口座に関する番号、クレジットカード番号、メールアドレス、ユーザID・パスワード（複数事業者、又は一事業者内の複数サービスで共用）、ナンバープレート（自動車登録番号標等）番号、固定電話番号、携帯電話番号、Webフィンガープリント、情報通信端末シリアルナンバー（携帯電話端末シリアルナンバー等）、MACアドレス、情報通信端末ID、ICカードの固有ID、ソフトウェアシリアル番号、不動産番号、IPアドレス(V6)、声紋、指紋、静脈パターン、虹彩、DNA、顔認識データ、掌形、生体認証で使用されるデータ、歩行パターン、筆跡、性別、肌の色、人種、
------------	--

	家族構成、血液型、髪の色、血圧、脈拍、身長、体重
上記以外のもの	ユーザ ID・パスワード(一事業者内)

(オ) 変更可能性/不変性/利用停止可能性 (静的であるもの)

変更、利用停止等が容易にできないもの(静的であるもの)	運転免許証番号、パスポート(旅券)番号、健康保険証の記号・番号(健康保険被保険者証記号番号等)、雇用保険被保険者番号、外国人の在留に関する番号(在留カード番号、特別永住者証明書番号、外国人登録証明書番号)、金融機関の口座に関する番号、クレジットカード番号、メールアドレス、ナンバープレート(自動車登録番号標等)番号、固定電話番号、携帯電話番号、情報通信端末シリアルナンバー(携帯電話端末シリアルナンバー等)、MAC アドレス、情報通信端末 ID、IC カードの固有 ID、ソフトウェアシリアル番号、不動産番号、IP アドレス(V6)、声紋、指紋、静脈パターン、虹彩、DNA、顔認識データ、掌形、生体認証で 사용되는データ、歩行パターン、筆跡、性別、肌の色、人種、家族構成、血液型、髪の色、
上記以外のもの	ユーザ ID・パスワード(複数事業者、又は一事業者内の複数サービスで共用)、ユーザ ID・パスワード(一事業者内)、Web フィンガープリント、血圧、脈拍、身長、体重

以上の結果を踏まえ、すべての指標に合致し、「(仮称)準個人情報」の定義に該当する具体的な項目(例)は、以下のとおりである。

「(仮称)準個人情報」の定義に該当する具体的な項目(例)

個人又は個人が使用する通信端末機器等に関するもの	運転免許証番号、パスポート(旅券)番号、健康保険証の記号・番号(健康保険被保険者証記号番号等)、雇用保険被保険者番号、外国人の在留に関する番号(在留カード番号、特別永住者証明書番号、外国人登録証明書番号)、金融機関の口座に関する番号、クレジットカード番号、メールアドレス、ナンバープレート(自動車登録番号標等)番号、固定電話番号、携帯電話番号、情報通信端末シリアルナンバー(携帯電話端末シリアルナンバー等)、MAC アドレス、情報通信端末 ID、IC カードの固有 ID、ソフトウェアシリアル番号、不動産番号、IP アドレス(V6)
個人の身体的特性に関する	声紋、指紋、静脈パターン、虹彩、DNA、顔認識デー

るもの	タ、掌形、生体認証で使用されるデータ、歩行パターン、筆跡
上記のほか、特定の個人の識別につながる多量又は多様な情報の収集を可能にするもの	

- * WG において、移動履歴、購買履歴、Web 閲覧履歴については、様々な情報を収集する識別子としての機能を有し、特定の個人を識別し得る場合があるものであるといえるが、どのような場合がこうした「(仮称) 準個人情報」に該当するものとなるか、その要件を一律に規定することは困難であるもの、と判断している。
- * 今後の技術進展等によっても「(仮称) 準個人情報」に該当する項目は変化するものと考えられることから、常に最新の状況に見合った見直しを行っていくことが必要である。
- * 上記の試行的な整理において、「(仮称) 準個人情報」に例示されていない項目であっても、それらを複数組み合わせることによって、又は適用範囲を限定することによっても、特定の個人を識別する蓋然性が高い「(仮称) 準個人情報」相当の識別子として機能する場合が容易に考えられる。このような情報の組み合わせに基づく特定の個人の識別が発生しないことを技術的に保証するためには、データを過度に抽象化する必要があるが、そのような措置はデータの利活用における本来の重要な利便性を大きく損ないかねないことでもある。また、こうした可能性は、「(仮称) 個人特定性低減データ」であっても同様である。ついては、受領者側において、特定の個人を識別することを目的とした個人データの収集がなされないようにすることが極めて重要である。

3 「(仮称) 個人特定性低減データ」について

3.1 「(仮称) 個人特定性低減データ」の定義及び加工方法について

3.1.1 事務局案についての検討

事務局から提案された「(仮称) 個人特定性低減データ」の定義は、以下のとおりである。

【事務局案】

「(仮称) 個人特定性低減データ」とは、次に掲げるものをいう。

- ① 個人データについて、当該データに含まれる氏名、生年月日その他の記述等により特定の個人が識別できるものを削除する等政令で定める方法による加工を施し、個人が特定される可能性を低減したもの
- ② 「(仮称) 準個人データ」について、当該データに含まれる法〇条〇項各号に掲げるもの^注を削除する等政令で定める方法による加工を施したもの（注：「(仮称) 準個人デー

タ」の定義規定)

- ③ ①又は②について、他の情報を加える等加工を施したもの
(「(仮称) 準個人情報」、「個人情報」となったものを除く。)

(第7回パーソナルデータに関する検討会 【資料1-2】より)

なお、この「(仮称) 個人特定性低減データ」の利用・流通については、

- ・ 個人情報を第三者へ提供する際の本人の同意に代えて、個人データを加工して特定の個人が識別される可能性を低減したデータ(「(仮称) 個人特定性低減データ」)を本人の同意なく第三者へ提供できる新たな類型として整理する。
- ・ 加工したデータを取り扱う者(提供者及び受領者)が負うべき義務等につき所要の措置を講じる。
- ・ 第三者機関(設置について別途検討中)においては、営業秘密等の事業者の権利利益を侵害しない範囲で情報を公開する。

という枠組みとすることで、個人情報及びプライバシーの保護に配慮することを提案しているものである。この枠組みは本人同意による第三者提供の代わりに、同意不要な第三者提供を実現する枠組みであり、第三者提供の基本は同意取得であるべきである。したがって、本枠組みは同意により取得されたデータの第三者提供を縛るものではない。

ここで、WGのミッションは、「(仮称) 個人特定性低減データ」の定義と、「個人データ」又は「(仮称) 準個人データ」から「(仮称) 個人特定性低減データ」に加工する際の最低限の加工方法について検討することであるが、まずは、前報告書において示したとおり、データの加工において、データの利活用における有用性と当該データ内の個人の特定性や識別性を低減させることはトレードオフの関係にあり、また、データの種類や量が多種多様であることから、データの加工方法は利活用の実態に即して個別に判断されるべきものであることを指摘しておきたい。

また、それは、文字通りに完全に匿名化されたデータに加工することを求めているものではない「(仮称) 個人特定性低減データ」であっても同様である。「個人データ」又は「(仮称) 準個人データ」から「(仮称) 個人特定性低減データ」に加工する際の最低限の加工方法とは、端的には「(仮称) 準個人データ」の状態ではないデータとすることが想定されているものと捉えることができるが、上記の「(仮称) 準個人情報」における検討で示したとおり、「(仮称) 準個人情報」に該当する項目も多種多様であり、通常一つのデータ内には「(仮称) 準個人情報」のア)からウ)に該当する識別子が1項目のみではなく複数併存しているほか、それに紐づく属性情報の質も量も多岐にわたっているものと考えられ、これを一様に「(仮称) 個人特定性低減データ」に加工する方法として整理することは困難である。

なお、参考までに、「個人データ」又は「(仮称) 準個人データ」から「(仮称) 個人特定性低減データ」への加工において、想定される特定の個人が識別されるリスク(以下「個人特定リスク」という。)とその個人特定リスクを回避するための加工

方法について検討した結果を示す。

「(仮称) 個人特定性低減データ」には、次のような個人特定リスクが存在すると考えられる。

個人特定リスク1：「(仮称) 個人特定性低減データ」から直接特定の個人が識別される。

これは、元々の「(仮称)個人特定性低減データ」自体が保有するリスク

個人特定リスク2：「(仮称) 個人特定性低減データ」と他のデータが、(共通サービスのユーザ ID などの識別子を用いて) 機械的に個人の識別子若しくは識別子相当のものによる複数の情報のマッチングがなされ、その結果特定の個人が識別される。

これは、元々の「(仮称)個人特定性低減データ」自体が保有するリスク

個人特定リスク3：「(仮称) 個人特定性低減データ」から提供先事業者(受領者)の知識に依存して個別的に特定の個人が識別される(購買履歴から偶然 SNS などですそれに合致する購買行動を発見し、そこから特定の個人を識別)

これは、元々の「(仮称)個人特定性低減データ」自体が保有するリスクではなく、1.2.3 に示す提供先事業者(受領者)において「(仮称) 個人特定性低減データ」と照合可能な個人データ等の有無について予見できないことから生じるリスク

上記の個人特定リスクに対応して当該リスクを回避するための加工方法を考察する。

個人特定リスク1 を低減する方法：

「個人データ」から「(仮称) 個人特定性低減データ」に加工する場合、特定の個人を直接識別する属性を予め定め(例 氏名、生年月日、住所、所属団体)、それらすべてを削除若しくは加工(例 住所は都道府県に丸める等の固定的な加工)を行う。

※ この方法を用いると、(例えば、氏名等による)個人特定性を一定程度低減することができるが、逆に予め定められた属性以外を用いた特定の個人が識別される可能性を排除できないことに留意する必要がある。本方法を採用する場合には、「(仮称) 個人特定性低減データ」が《どの属性により直接個人特定性を低減するのか》を予め共通に定めておく、あるいは第三者提供を行う事業者が明らかにしておく必要があると考えられる。

※ 上記のほか、予め定めた属性から個人特定性を低減する方法は削除や固定的な加工によらず、前回報告書に記載した様々な加工技術を組み合わせた方法でも可能であると考えられる。

個人特定リスク2を低減する方法：

「個人データ」又は「(仮称)準個人データ」から「(仮称)個人特定性低減データ」に加工する場合、識別子又は識別子に相当するものが、異なる事業者間で識別子若しくは識別子相当のものによる複数の情報のマッチングを可能とする性質を持たないように加工する。すなわち、識別子を削除又は仮名化して本人との関係性を低減する。なお履歴データに関しては移動履歴として後述する。

※ 密接性は、仮名化を行うことで低減できると考えられるが、一意性/単射性は保持されたままとなる。一意性/単射性に対応する場合には、下記の「個人特定リスク3を低減する方法」が有用である。

※ 共用性は、仮名化を行うことで低減できると考えられるが、仮名の利用期間の長さや提供先の数の多さによって個人特定リスクがどのように変化するかは未知の部分もあり、継続した分析とそれに対応する規律の検討が必要である。

※ 変更可能性/不変性/利用停止可能性はデータの取得時に定まる性質であり、(仮称)個人特定性低減データ」にも継承される。

個人特定リスク3を低減する方法：

「個人データ」又は「(仮称)準個人データ」から「(仮称)個人特定性低減データ」に加工する場合、特徴的な値を持つ属性、複数属性の特徴ある組合せの削除や加工する方法、あるいはすべての属性の組合せに対して元の「個人データ」との1対1の結びつきを持たせないように加工する方法(例 k-匿名化や適切な一部抽出(サンプリング)等)が有用である。

※ 本加工を技術的に達成することは難易度が高い。

なお、移動履歴については、その特性に応じた加工が求められる。

個人特定リスク1を低減する方法(移動履歴の場合)：

特定の個人を直接識別する属性を予め定め(例 氏名、生年月日、住所、所属団体)、それらすべてを削除若しくは加工(例 住所は都道府県に丸める等の固定的な加工)を行う。ただし位置と時間の組合せから住所や所属団体の推定が可能な場合、当該位置情報を削除若しくは加工を行う。

個人特定リスク2を低減する方法(移動履歴の場合)：

「個人データ」又は「(仮称)準個人データ」から「(仮称)個人特定性低減データ」に加工する場合、識別子又は識別子に相当するものが、異なる事業者間で識別子若しくは識別子相当のものによる複数の情報のマッチングを可能とする性質を持たないように加工する。

- ・ 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
- ・ 仮名の短い時間での更新、長い履歴の削除、分割や時間間隔の間引き
- ・ 上記の手法を用いて位置情報を適切に加工し、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

※ 本加工の結果は識別子若しくは識別子相当のものによる複数の情報のマッチングの不可能さを保証するものではない。

個人特定リスク3を低減する方法（移動履歴の場合）：

「個人データ」又は「(仮称) 準個人データ」から「(仮称) 個人特定性低減データ」に加工する場合、特徴的な値を持つ属性、複数属性の特徴ある組合せの削除や加工する方法、あるいはすべての属性の組合せに対して元の「個人データ」との1対1の結びつきを持たせないように加工する方法（例 k-匿名化や適切な一部抽出（サンプリング）等）が有用である。

- ・ 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
 - ・ 仮名の短い時間での更新、長い履歴の削除、分割や時間間隔の間引き
 - ・ 上記の手法を用いて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
- ※ 本加工を技術的に達成することは難易度が高い。

上記全般に対する考え方：

個人特定リスク1と個人特定リスク2への対応の措置は必須である。これらは、「(仮称) 個人特定性低減データ」に内在するリスクだからである。その一方で、個人特定リスク3については、専ら提供先事業者（受領者）の行為によって生じるリスクであり、提供先事業者（受領者）による特定の禁止を規定することによりカバーできると考えることもできる。また、識別子の扱いであるが、継続性を小さくする（同一の識別子（仮名化されている場合はその仮名を含む。）を長期間使わない）、悉皆性を低くする（一部抽出（サンプリング）する）、到達可能性を排除する（メールアドレス等の削除）などの加工を行うことが望ましい（特に規模の大きなデータにおいては、一部抽出は有効な方法だと考えられる）。

上記の検討も参考に、個別のユースケースを想定して、具体的な加工方法を検討することは可能であると考えられることから、今後より詳細な検討が行われることを期待したい。

3.1.2 「(仮称) 個人特定性低減データ」の定義の修正提案

上記のとおり、「(仮称) 個人特定性低減データ」については、すべてのデータに対して有効となるような具体的な加工方法を提示することは困難であることから、「個人情報」、「(仮称) 準個人情報」の定義において、特定の個人を識別すること、あるいはその特定の個人を識別する蓋然性が高いこととしていることを踏まえると、「(仮称) 個人特定性低減データ」をその性質や特性で規定とした場合、特定の個人を識別させる蓋然性の低いものになるよう加工を施して特定の個人を識別する

ことが困難になるようにしたものとする考えられる。

以上の検討を踏まえ、事務局が先に示した「(仮称) 個人特定性低減データ」の定義を、以下に示す事項を含む趣旨となるように変更することを提案する。

- ・「個人データ」から「(仮称) 個人特定性低減データ」にする場合には、特定の個人を識別させる情報に加工を施して、特定の個人を識別することができないようにしたもの
(ただし、上記の加工により、「個人データ」が「(仮称) 準個人データ」となる場合には、更に下記の加工を行う必要がある。)
- ・「(仮称) 準個人データ」から「(仮称) 個人特定性低減データ」にする場合には、当該データに含まれる識別子(又は識別子に相当する機能を有するもの*)に加工を施して特定の対象を識別することができないようにしたもの
*) 2.2.4 で示した「(仮称) 準個人情報」の定義の変更案において、ウ)に該当するものを含むとする場合に該当するものであって、識別子ではないが履歴情報等が識別子に相当する機能を有するものを考慮する必要がある。
- ・上記の2項目のほか、「(仮称) 個人特定性低減データ」に加工等を行った場合で、引き続き「(仮称) 個人特定性低減データ」であるもの(加工等により、「個人データ」又は「(仮称) 準個人情報」となったものは除く。)

なお、「(仮称) 個人特定性低減データ」という名称については、受領者側において特定の個人を識別することを禁止するものであることを明確にする意味で、「(仮称) 特定禁止データ」と改称すべきであるとの意見もあった。

ところで、「(仮称) 準個人情報」と「(仮称) 個人特定性低減データ」を比較すると、以下ようになる。両者はともに特定の個人を識別することのない情報であるが、「(仮称) 準個人情報」に含まれる個人を一人ひとり区別する情報(例えば識別子)は、外部のデータと突き合わせることにより、その情報から特定の個人を識別できることがある。例えば、外部のデータとして、個人の氏名等とメールアドレスが組となるデータがある場合、「(仮称) 準個人情報」にメールアドレスが含まれると、これが突き合わされて特定の個人の識別に至る。一方、「(仮称) 個人特定性低減データ」においては、個人を一人ひとり区別する情報は加工されているため(例えば仮名化により生成された識別子)、その加工を行った提供者だけが知り得る情報を利用しないと、特定の個人の識別は困難となる。

3.2 「(仮称) 個人特定性低減データ」に加工し第三者提供する事業者における取扱いについて

個人情報又は「(仮称) 準個人情報」から「(仮称) 個人特定性低減データ」に加工し第三者提供する際の事業者の対応について、まずは、上記のとおり、データの特性や加工方法には多様性があり、「(仮称) 個人特定性低減データ」とするための最低限の加工方法を定義することはできないことから、特定の個人の識別性を低減させるこ

とと利活用の二ーズとのバランスを考慮し、事業者自らの判断と責任において、適切な加工を施すことが必要である。 ついては、仮に、「(仮称)個人特定性低減データ」の受領者において特定の個人が識別され、何らかの個人の権利利益に侵害が生じた場合、その事案のそもそもの発端として、提供したデータが適正に加工されたものであったか否かが問題にならないとも限らないことから、提供した「(仮称)個人特定性低減データ」への加工の適正性に関して、責任の明確化等の観点などから、何らかの証拠を保存する等の対策を施すことに等について検討することが必要であると考えられる。

また、提供した「(仮称)個人特定性低減データ」への加工の適正性に関しては、「特定の個人を識別できない」状態というものが、どのようなものであるかという解釈の提示や、加工方法等のベストプラクティスの提示、ガイドラインの策定、事前相談の充実等を図り、加工方法等の柔軟性を制約することなく、明確にするよう努めることが必要である。

なお、個人データについては、特定性がある状態のデータのまま、特段の加工を施さなくても、本人の同意を得ることによって第三者提供は可能である。本人との関係、事業者における取扱いと個人特定リスクとの関係性等を慎重に判断した上で、第三者提供するための適切な方法を選択すべきである。同様に、「(仮称)準個人情報」についても、一律に「(仮称)個人特定性低減データ」として第三者提供を可能とするのではなく、本人の同意という手段が取り得るのであれば、これを可能とする規律を設けることについても検討すべきである。

また、加工方法等の情報について第三者機関に提出することとされているが、この点については、3.4において後述する。

3.3 「(仮称)個人特定性低減データ」を受領する事業者における取扱いについて

「(仮称)個人特定性低減データ」の受領者における取扱いとしては、当該データに関する特定の個人を識別することの禁止、及び安全管理措置を採ることが提案されている。

「(仮称)個人特定性低減データ」に関する特定の個人を識別することを禁止する規定に関して、特定の個人を識別することを防ぐ具体的な手法を示すことが有効であると考えられることから、多様なユースケースを想定した検討を行うことにより、具体的な方法等に関するベストプラクティスの提示、ガイドラインの策定等を進めることが重要である。

一方、「(仮称)個人特定性低減データ」に関する安全管理措置の具体的な内容としては、「個人データ」については、漏えい、滅失又はき損の防止の観点からの安全管理が求められるところ、「(仮称)個人特定性低減データ」が完全に匿名化され特定の個人を識別することができないデータではないという特性とその取扱いに注目し、滅失又はき損の防止といった観点での安全管理は除外し、

- ①特定の個人を識別しないための適切な措置を講じなければならない、
- ②(事業者自らにおける、又は委託先からの)情報漏えいが生じないよう、適切な措置を講じなければならない、

という二点での安全管理措置が必要であることを明確化すべきであると考えられる。

また、上記の情報漏えい等に関する安全管理措置の具体例としては、データの利用期限を定め利用終了後は速やかにデータを破棄すること、ネットワークと切り離された環境を構築し、当該環境内でのみデータの分析等を実施すること等が挙げられる。なお、加工の程度（特定個人の識別性の低減化の程度）によって必要な安全管理措置は異なるものであり、利活用に実態に応じた適切な対策を講ずることが必要である。この他、実際に情報漏えいが生じてしまった場合の手続（周知の方法、第三者機関への報告手続等）については、実際に生じるであろう被害の程度に即したものとし、ガイドライン等で明確化することが望まれる。

これに加え、仮に、受領者において、受領した「（仮称）個人特定性低減データ」に、特定の個人を識別するような情報が含まれることを発見した場合には、速やかに利用を中止するほか、本件について提供者及び第三者機関に通報するとともに、提供者は直ちに事態の把握と改善に努めなければならないといった趣旨の対応をすることについて検討すべきであると考えられる。この際、受領者に一定の期間、当該データを保全することが必要となる可能性もある。

3.4 「（仮称）個人特定性低減データ」に関する第三者機関への情報の提出と第三者機関による公表について

「（仮称）個人特定性低減データ」の第三者提供に当たって、第三者機関は提供元事業者（提供者）から加工方法等に関する情報の提出を受け、そのうち営業秘密等事業者の権利利益を害しない範囲で情報を公開するとされている。

第一に、「（仮称）個人特定性低減データ」の第三者提供が、提供先事業者（受領者）の取扱いと相まって、本人の同意なく第三者に提供できる新たな類型として整理されるものであることに鑑み、「（仮称）個人特定性低減データ」の提供先事業者（受領者）が誰であるかを把握しておくことは、当該情報を把握するための方法の如何を問わず、必須であると考えられる。

なお、ある事業者が「（仮称）個人特定性低減データ」（「低減データ A」とする。）を第三者提供する際に、当該低減データ A に、他の事業者から受け取った「（仮称）個人特定性低減データ」（「低減データ B」とする。）の情報が含まれる場合も考えられる。この場合、第三者機関に提出される情報（又は、第三者機関が把握すべき情報）には、低減データ A の提供先事業者（受領者）の情報に加えて、低減データ B の提供元事業者（提供者）に関する情報も含めるべきであると考えられる。これは、複雑なデータの流通が想定される中で、第三者機関が迅速かつ的確に状況を把握できるようにしておくことが、何らかの事態が発生した際の権利利益侵害の最小化につながるものであり、事業者の負担を著しく増加させるものではないことから、有効な手段である。

また、第三者機関において「（仮称）個人特定性低減データ」に係る情報を集約する意味は、仮に「（仮称）個人特定性低減データ」から特定の個人が識別され、それによって何らかの権利侵害が生じてしまった場合、その原因の調査と対策を第三者機関が行うために必要となる情報を予め保持しておくことが重要であると考えられる。

さらに、「(仮称)個人特定性低減データ」を取り扱う事業者がそれぞれ異なった公表方法によって公表事項を公表することに代えて、例えば、第三者機関がホームページ上で一覧性を持って公表する等、何らかの個人の権利利益の侵害は当該個人が気付くことが多いと考えられ、そのために、当該個人が自身に関するデータがどのような事業者で利用・保管されているか、容易に確認できる手段を提供するためであると考えられる。

このうち、何らかの事案が生じた場合の調査等に必要となる最小限の情報を事前に把握しておくことについて、様々なデータの種類や多様な加工方法が想定できる中で、第三者機関の機能・能力がまだ不明確な段階にあることとも相まって、技術的な観点から必須となる項目を整理するに至らなかった。なお、第三者機関が事案の検証を詳細に行うこととした場合、提供者から実際に受領者に対して提供された「(仮称)個人特定性低減データ」そのものがなければ、正確かつ詳細な調査は不可能であるが、極めて膨大なデータ量になると想像される実データを事業者から第三者機関に提供してもらい、かつ、それを保管することは困難であり、また、権利利益の侵害のおそれの程度において行う事業者の対応としては著しくバランスを欠いていると考えられることから、実データの提供を求めることは現実的ではない。

その他、「(仮称)個人特定性低減データ」の加工に関して、事業者から第三者機関に提出する情報の項目として想定されるものとしては、以下のようなものが挙げられる。

- ①提供者事業者（提供者）情報
- ②提供先事業者（受領者）情報
- ③提供期間、頻度
- ④データの種別1（個人データ、準個人データの別、機微情報の有無）
- ⑤データの種別2（購買データ、移動履歴、WEB閲覧履歴等の別）
- ⑥データの規模
- ⑦加工方法の概要（各項目の粒度、低減の程度が判別できる程度のサンプルを含む）

これらの項目については、事業者から提出を求める内容の粒度（詳細さ）や頻度を踏まえ、個人情報やプライバシーの保護と事業者の取扱いのバランスを図り、必要かつ最小限なものとなるよう、検討することが求められる。なお、上記項目に関して、変更が生じた場合は事前又は所定期間内に速やかに第三者機関に変更内容を提出することが求められる。

一方、第三者機関における「(仮称)個人特定性低減データ」に関する公表事項については、「(仮称)個人特定性低減データ」を取り扱っている事業者名は必要であると考えられるが、それ以外の項目の公表の必要性については、技術的な見地ではなく、制度的な観点での判断であると考えられる。

(参考) 技術検討 WG における検討経緯と構成員

1. 検討経緯

◆第5回 (平成26年4月17日 (木))

親会からの依頼事項について

◆第6回 (平成26年5月13日 (火))

親会への報告事項について

※会議資料

<http://www.kantei.go.jp/jp/singi/it2/pd/index.html>

2. 技術検討ワーキンググループ構成員 (敬称略、五十音順)

いとう しんすけ
伊藤 伸介 中央大学 経済学部 准教授

おかむら ひさかず
岡村 久和 日本IBMスマーター・シティー事業・部長

きくち ひろあき
菊池 浩明 明治大学 総合数理学部 教授

さくま じゅん
佐久間 淳 筑波大学 システム情報工学研究科 准教授

◎ さとう いちろう
佐藤 一郎 国立情報学研究所 アーキテクチャ科学研究系 教授

さとう よしひろ
佐藤 慶浩 日本ヒューレットパッカーード 個人情報保護対策室長

たかはし かつみ
高橋 克巳 NTTセキュアプラットフォーム研究所 主席研究員

まつもと やすし
松本 泰 セコム株式会社 I S 研究所 コミュニケーションプラットフォーム
フォームディビジョン マネージャー

○ もり りょうじ
森 亮二 英知法律事務所 弁護士

◎は主査、○は主査代理