

「パーソナルデータの利用・流通に関する研究会」論点整理（案）

I 検討の背景

ICT（情報通信技術）の普及により、ライフログなど多種多様な個人に関する情報を含む大量の情報（いわゆるビッグデータ）がネットワークを通じ流通する社会を迎えている。これにより、新事業の創出、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る一方、個人に関する大量の情報が集積・利用されることによるプライバシー等の面における不安も生じている。

また、ICTの普及は、クラウドサービスなど国境を越えた情報の流通を極めて容易としており、国際的な調和の取れた、自由な情報の流通とプライバシー保護等の双方を確保する必要性が高まっている。こうした中、海外においてもEUのデータ保護規則案の提案¹、米国の消費者プライバシー権利章典の公表²など活発な議論が行われている。

本研究会では、これらを踏まえ、プライバシー保護等に配慮したパーソナルデータ（個人に関する情報）のネットワーク上での利用・流通の促進に向けた方策について検討するものである。

我が国のパーソナルデータの保護に関する法律としては、個人情報保護法³、行政機関個人情報保護法⁴、独立行政法人等個人情報保護法⁵があげられる。また、パーソナルデータの利活用については、統計法⁶、電気通信事業法⁷による通信の秘密の保護、知的財産権の保護、情報公開法⁸による不開示情報の保護なども関連する。

そのうち我が国の個人情報保護の基本法である個人情報保護法は、「個人情報」⁹を同法による保護の対象としている。しかしながら、「個人情報」の「特定の個

¹ European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (2012)*

² White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (2012)*

³ 個人の情報の保護に関する法律（平成15年法律第57号）

⁴ 行政機関の保有する個人情報の保護に関する法律（平成15年法律第58号）

⁵ 独立行政法人等の保有する個人情報の保護に関する法律（平成15年法律第59号）

⁶ 統計法（平成19年法律第53号）

⁷ 電気通信事業法（昭和59年法律第86号）

⁸ 行政機関の保有する情報の公開に関する法律（平成11年法律第42号）

⁹ 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。）

（個人情報保護法第2条第1項）

人を識別することができる」(個人識別性)の要件については、具体的な情報(例えば、端末ID、IPアドレス等)について個人識別性の要件を満たすか否か、あるいは個人識別性がない情報であっても保護対象とすべきものがあるのではないかなど様々な議論が行われている。

そのため、本研究会においては、個人識別性を有する「個人情報」に限定することなく、広く「個人に関する情報」を「パーソナルデータ」と定義して、検討の対象とすることとし、その中で「保護されるパーソナルデータ」の範囲について検討するものである(後記Ⅲ2参照)。

Ⅱ パーソナルデータの利用・流通の促進のための方策

1 パーソナルデータ利活用の可能性

パーソナルデータの利活用については、世界経済フォーラムが、2011年1月に公表した報告「パーソナルデータ：新たな資産カテゴリーの出現」¹⁰において、パーソナルデータは、インターネットにおける新しい石油であり、デジタル世界における新しい通貨であるとし、2020年のデジタルデータの量は2009年の44倍になるであろうと予測している。

また、マッキンゼー社は、2011年5月に公表した報告「ビッグデータ：イノベーション、競争及び生産性の次のフロンティア」¹¹において、ビッグデータにより分野横断的に著しい財産的な価値の創出がなされるとし、その具体例として、医療、公共部門運営、位置情報、小売り、製造をあげている。

さらに、情報通信審議会は、2012年7月の答申「知識情報社会の実現に向けた情報通信政策の在り方 ～Active Japan^{ICT}戦略～」¹²において、2020年に多種多量のデータをリアルタイムに収集・伝送・解析等に利活用して我が国の社会的課題の解決につなげるとともに、数十兆円のデータ利活用市場が創出される環境を構築することを目指すとしている。

加えて、2011年3月11日の東日本大震災発生時の人の動き等を携帯電話やカーナビゲーションの位置情報を利用して、解析し、今後の防災に役立つ試みも報道されている¹³。

このように、パーソナルデータについては、国内外の様々な分野で急速に実際の利活用が進展してきており、今後も技術の進展等とともに、新しい利便性の高いサービスが誕生する可能性が極めて高いと考えられる（参考資料1参照）。

こうしたパーソナルデータの利活用については、適切に情報を開示したり、本人から適切な形で同意を得たり、あるいは本論点整理で示したように匿名化技術を適切な形で利用したりする（後記Ⅲ6参照）といった適正な方法によっていけば、プライバシー侵害等の問題を生じない形で扱うことが可能となるものである。

¹⁰ World Economic Forum, *Personal Data: The Emergence of a New Asset Class* (2011)

¹¹ McKinsey & Company, *Big Data: The Next Frontier for Innovation, Competition, and Productivity* (2011)

¹² 情報通信審議会「知識情報社会の実現に向けた情報通信政策の在り方 ～Active Japan^{ICT}戦略～」(平成24年7月25日)

¹³ NHK「NHKスペシャル ”いのちの記録”を未来へ～震災ビッグデータ～」(2013年3月3日放送)

2 パーソナルデータの利活用のルールの明確化の必要性

現状では一方で、パーソナルデータの利活用について、プライバシーの保護等の観点からの様々な課題が指摘されており、国内外で数々の問題事例についての報道等がなされている¹⁴。

しかしながら、日本の個人情報保護法を含むプライバシー保護・個人情報保護のルールは、パーソナルデータの利活用を禁止することを目的とするものではなく、パーソナルデータを適正に利活用するため、プライバシー保護等とパーソナルデータの利活用の調和を図ることを目的とするものである¹⁵。

問題は、パーソナルデータの利活用のルールが明確でないため、企業にとっては、どのような利活用であれば適正といえるかを判断することが困難であること、消費者にとっては、自己のパーソナルデータが適正に取り扱われ、プライバシー等が適切に保護されているかが不明確になっており、懸念が生じていることにある。

3 パーソナルデータの利用・流通の促進に向けた方向性の提示

本論点整理では、上記を踏まえ、パーソナルデータの利用・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、後記Ⅲにおいて、パーソナルデータの利活用の枠組み及びその実施のための短期的な方向性を提示するとともに、後記Ⅳにおいて、同枠組みの実施のために必要となる中期的な方向性を提示している。

パーソナルデータの利活用が、プライバシー等の観点から問題となり得るのは、特定の個人と結びつきが強い場合である。したがって、例えば、ビッグデータの利活用において、いわゆるM2M情報¹⁶については、プライバシー等の観点から問題になることは少ないものと考えられる。

パーソナルデータの利活用のうち、ルールの適用関係が必ずしも明確でなく、取扱上その判断に困難な問題が生じる可能性が大きいのは、パーソナルデータ

¹⁴ 例えば、スマートフォンの利用者問題に関しては、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「スマートフォン プライバシー イニシアティブ ー利用者情報の適正な取扱いとリテラシー向上による新時代イノベーションー」（平成24年8月）14頁参照

¹⁵ 個人情報保護法第1条は「個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする」とされている。

¹⁶ Machine to Machine 情報：機械同士が人間を介在せずにやり取りする情報。

なお、いわゆるM2M情報であっても、家庭内に設置される機械や個人が身につける機械の情報など個人に関する情報を含む場合があり、プライバシー等の観点から問題が生じる場合があることに留意することが必要である。

の利用・流通の過程において、個人識別性などの特定の個人との結びつきの強弱を容易に判断することが困難な場合である。

特に、パーソナルデータが、二次利用、三次利用されるような場合においては、当初は特定の個人との結びつきが弱かったとしても、多くの情報が集積され、分析されることにより、個人識別性が生じるなど特定の個人との結びつきが強まる可能性があり、判断が困難な問題が生じる。このような場合には、二次利用者、三次利用者等が、単独でパーソナルデータの本人の同意を取得すること等は困難であり、パーソナルデータの利活用の仕組み全体で適切な取扱いを確保する必要がある。本論点整理では、そのようなパーソナルデータの利活用における特定の個人との結びつきの強弱の判断が困難な場合についても、その適切な取扱いが明確となるような枠組みを提示するよう試みるとともに、そのような枠組みが機能するための中期的な方向性についても提示している。

今後本研究会においては、本論点整理に対しパブリックコメント手続を通じて提出される意見も踏まえ引き続き検討を行い、報告書の取りまとめを行う予定である。なお、報告書の取りまとめの際には、改めて報告書案を公表し、パブリックコメント手続に付する予定である。

Ⅲ パーソナルデータの利活用の枠組み

ここでは、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、パーソナルデータの利活用の枠組み及びその実施のための短期的な方向性を提示している。

1 基本的な枠組み

(基本的考え方)

- パーソナルデータを含むビッグデータの利活用の促進は、これからの新事業創出のための1つの重要な要素。他方、個人の安心・安全の確保のためには、パーソナルデータの適切な保護が必須であり、その双方が調和のとれた関係を目指すことが重要。
- ビッグデータの利活用を円滑に進めるためには、パーソナルデータが適切に取り扱われていることについて、信頼性が確保され、強化されることが必要不可欠。
- 事業創出の観点からパーソナルデータを積極的に利活用できるようにするとともに、個人の安心・安全を確保するためには、パーソナルデータの利活用のルールが明確となるメカニズムの構築が必要。
- パーソナルデータの保護については、個人情報保護法上の個人情報保護（以下単に「個人情報保護」という。）とプライバシー保護との関係を整理した上で、分かりやすく、一般的な国民の感覚に適合した枠組みとする必要。
- また、EU、米国などにおける様々な議論の現状を踏まえ、国際的な調和に配慮する必要。他方、プライバシーについての考え方は、各国・各地域における文化や歴史に深く根ざしたものであることにも留意が必要。

(主な論点)

- パーソナルデータの利活用の枠組みについては、パーソナルデータの利活用の原則を明確化し、その上で、具体的なルール（準則）を設定・運用していくこととすべきではないか。
- まず、パーソナルデータの保護の目的を明らかにするという観点から、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はないか。
 - 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¹⁷。

- ✓ なお、上記①において、「主として」としたのは、個人情報保護法の目的が「個人の権利利益を保護すること」（同法第1条）とされていることを踏まえたものである¹⁸。また、ここでいうプライバシーとは、基本的に個人の自己情報コントロールの側面を念頭に置いたものである¹⁹。
- 次に、上記のパーソナルデータの利活用の基本理念を具体化するパーソナルデータ利活用フレームワークとして、以下のような項目を掲げてはどうか。また、それ以外に含めるべき項目はないか（参考資料2参照）。
 - ・ **透明性の確保**
パーソナルデータの利用に関し、本人が必要な情報に容易にアクセスする機会を提供すること
 - ・ **本人の関与の機会の確保**
パーソナルデータの本人が、パーソナルデータをどのように利用されるかについて関与する機会を確保すること
 - ・ **取得の際の経緯（コンテキスト）の尊重**
パーソナルデータの利用は、本人がパーソナルデータを提供した際のコンテキストに沿って、本人の期待と合致する形態で行うこと
 - ・ **必要最小限の取得**
パーソナルデータの取得は、パーソナルデータの利用目的の実現のため必要最小限のものとする
 - ・ **適正な手段による取得**
パーソナルデータの取得は、適正な手段によるものとする
 - ・ **適切な安全管理措置**
パーソナルデータは、パーソナルデータの性質に沿って適正な安全管理措置をとること

¹⁷ EU 欧州委員会においても、データ保護規則提案の中で「個人データ保護の権利は絶対的な権利ではなく、社会におけるその機能との関連で考慮されるべきものである」（“[T]he right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society”）としている。

(European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)* (2012))

¹⁸ なお、『『個人の権利利益』とは、個人情報の取扱いの態様いかんによって侵害されるおそれのある『個人の人格的、財産的な権利利益』（大綱）全般であり、**プライバシーはその主要なものであるが、それに限られない。**」（園部逸夫編、藤原静雄・個人情報保護法制研究会著『個人情報保護法の解説〈改訂版〉』（平成17年））と考えられているが、具体的にプライバシー以外にどのような権利利益が含まれるかについては必ずしも明らかでない。

¹⁹ 平成24年4月に内閣官房が個人情報保護ワーキンググループ・情報保護評価サブワーキンググループでの検討を踏まえ公表した「行政手続における特定の個人を識別するための番号の利用等に関する法律案」に基づく「特定情報保護評価指針素案（中間整理）」では、番号制度導入の目的の一つとして「国民の権利を守り、国民が自己に関する情報をコントロールできる社会の実現」をあげている。

・プライバシー・バイ・デザイン

パーソナルデータを利用する者は、商品開発時などそのビジネスサイクルの全般にわたって、プライバシーの保護をデザインとしてあらかじめ組み込んでおくこと

2 保護されるパーソナルデータの範囲

(基本的考え方)

- 現行の「個人情報」の範囲や、諸外国や国際機関等で保護の対象とされているパーソナルデータの範囲等を踏まえて、保護されるパーソナルデータの範囲を画定。
- 個人情報保護法が個人識別性を「個人情報」の要件としている（前記 I 参照）ことは、諸外国や国際機関等で保護の対象としているパーソナルデータの範囲と概ね同様（参考資料 3 参照）。
- ただし、米国の消費者プライバシー権利章典などでは、保護の対象を、特定個人に「連結可能（linkable）」な情報とし、スマートフォンや家庭のコンピュータの識別子など特定のコンピュータその他のデバイスに連結するデータも含むとしていることにも留意が必要（同上）。
- なお、パーソナルデータが、個人識別性等の要件を満たさず、ここでいう「保護されるパーソナルデータ」に該当しない場合であっても、他の法令により保護されている場合²⁰があることに留意が必要。

(主な論点)

- 保護されるパーソナルデータの範囲について、現行の個人情報保護法が個人識別性を有するものとしていることは、基本的には妥当であると考えられるのではないか。
- ただし、保護されるパーソナルデータの範囲を画定するにあたっては、プライバシーの保護という基本理念を踏まえて実質的に判断する必要があるのではないか。その際には、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併せて分析されることにより、特定の個人が識別される可能性があるということについて、十分に配慮する必要があるのではないか。
- 具体的には、個人の PC の IP アドレスや、個人のスマートフォンの識別番号などは、一義的には PC やスマートフォンといった特定の機械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

²⁰ 通信の秘密（電気通信事業法第 4 条第 1 項）に当たる場合、知的財産権として保護される場合、情報公開法上の不開示情報に当たる場合（同法第 5 条第 1 号柱書本文後段参照）等

シー保護の観点から、保護されるパーソナルデータの範囲に含まれると考えるべきではないか。

また、継続的に収集される購買・貸出履歴、視聴履歴、位置情報等については、仮にそれ自体が氏名等の個人識別性の要件を満たす情報（上記の特定の機械を識別する情報のうち、実質的に特定の個人と継続的に結びついているものを含む。）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²¹、特定の個人を識別することができるようになる可能性が高く、プライバシーの保護の観点から、保護されるパーソナルデータの範囲に含まれると考えるべきではないか。

➤ 上記のような特定の個人との結び付きが強いパーソナルデータ以外のパーソナルデータは、保護されるパーソナルデータには当たらず、パーソナルデータの利活用の枠組みの観点からは制約を受けずに、自由に利活用することができると考えられるのではないかと²²。

➤ 一般に公開されている国の統計情報など再識別化を不可能又は十分に困難にしたといえるものについては、保護されるパーソナルデータには当たらず、自由に利活用することとして差し支えないと考えられるのではないかと^{23, 24}。ただし、どのような状態になれば、再識別化を不可能又は十分に困難にしたといえるかについて、その考え方を示していく必要があるのではないかと。

また、他の情報との連結等により再識別化の可能性のある匿名化されたパーソナルデータについても、後述の通り、適切なセーフガードを設定することにより、保護されるパーソナルデータに当たらないとして、利活用を行うことが可能と整理すべきではないか²⁵（後記Ⅲ 6 参照）。

²¹ それ自体が個人識別性の要件を満たす情報と連結する形で取得・利用する場合には、個人識別性の要件を満たし、保護すべきパーソナルデータに当たると考えられる。

²² ただし、当該情報が通信の秘密（電気通信事業法第4条第1項参照）に当たる場合など他の法令が適用される場合には、それらの法令に適合することが求められる。

²³ 同上

²⁴ NTTドコモが設立したモバイル社会研究所が開催した「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」は、2010年6月に公表した「社会・産業の発展に寄与する『モバイル空間統計』利活用のあり方に関する報告書」において、「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って、個人の特性を不可能とし、特定個人の行動履歴を把握することは一切できないようにすることにより、モバイル空間統計の作成・提供・活用がプライバシー保護や個人情報保護の観点から問題となることは通常ないと考えられる。」としている。

²⁵ なお、匿名化されたパーソナルデータが再識別化された場合は、個人識別性の要件を満たすことから、保護されるパーソナルデータとなると考えられる。

3 パーソナルデータの性質に応じた取扱い

(基本的考え方)

- 保護されるパーソナルデータの中には、氏名などの通常公にされている情報から、健康に関する情報など人に知られたくない情報まで様々な性質のものがある。このため、保護されるパーソナルデータを一律に取り扱うのではなく、その性質に応じて適切に取り扱うことが必要。
- とりわけ、機微なパーソナルデータ（センシティブデータ）については、特に慎重な取扱いをすることが必要。

(主な論点)

- 保護されるパーソナルデータは、そのプライバシー性の高低により、次の3類型に分類し、それぞれの類型に応じた適切な取扱いを検討することとすべきではないか（具体的な適切な取扱いの在り方については、後記Ⅲ5参照）。
 - ①一般パーソナルデータ
（保護されるパーソナルデータのうちプライバシー性が高くないもの。センシティブデータ及び慎重な取扱いが求められるパーソナルデータ以外の保護されるパーソナルデータ）
 - ②慎重な取扱いが求められるパーソナルデータ
（センシティブデータ以外のプライバシー性が高いパーソナルデータ）
 - ③センシティブデータ
（プライバシー性が極めて高いパーソナルデータ）
- 一般パーソナルデータの範囲については、例えば、以下のようなものが含まれると考えられるのではないか。
 - ・氏名など本人を識別する目的などで一般に公にされている情報
 - ・本人の明確な意図で一般に公開された情報
 - ・名刺に記載されている情報など企業取引に関連して提供される情報（ビジネス関連情報）
- 慎重な取扱いが求められるパーソナルデータの範囲については、例えば、以下のようなものが含まれると考えられるのではないか。
 - 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以下のようなパーソナルデータ²⁶
 - ・電話帳情報
 - ・GPSなどの位置情報

²⁶ 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「スマートフォンプライバシーイニシアティブー利用者情報の適正な取扱いとリテラシー向上による新時代イノベーションー」（平成24年8月）61頁参照

- ・通信内容・履歴、メール内容・送受信履歴等の通信履歴
- ・アプリケーションの利用履歴、写真・動画
- ・契約者・端末固有ID

○継続的に収集される購買・貸出履歴、視聴履歴、位置情報等

➤ センシティブデータの範囲については、諸外国における定義や、現在の各省庁の個人情報保護法に基づくガイドライン等も踏まえて（参考資料4参照）、我が国の実情に適合したものとする必要があるが、例えば、以下のようなものとするのが考えられるのではないか。

- ・思想、信条及び宗教に関する情報
- ・人種、民族、門地、身体・精神障害、犯罪歴、病歴その他の社会的差別の原因となるおそれのある事項に関する情報
- ・勤労者の団結権、団体交渉その他団体行動に関する情報
- ・集団示威行為への参加、請願権の行使その他の政治的権利の行使に関する情報
- ・健康又は性生活に関する情報

4 パーソナルデータの利活用のルール策定の在り方

(基本的考え方)

■ パーソナルデータの利活用のルール策定に際しては、ICT分野が急速な技術革新が継続的に進展している分野であり、関係者の意見を的確かつ迅速に反映する必要性が高いことなどを考慮し、「マルチステークホルダープロセス」を最大限活用することが適当。

(主な論点)

- ルール策定に際しては、原則として国、企業、消費者、有識者等によって形成された合意をルールとする「マルチステークホルダープロセス」（多種多様な関係者が参画するオープンな検討を通じたルール策定のプロセス）によることを基本とすべきではないか。
- ルール策定における国の役割は、マルチステークホルダープロセスの場の提供、及び、議論の方向性がパーソナルデータの利活用の原則に沿ったものであることの検証を基本とすべきではないか。
- 情報通信、医療・介護など分野毎の固有の事情に対応したルール策定のため、個別分野における専門的知見も含んだ議論ができるよう、マルチステークホルダープロセス毎に適切に議論の範囲を設定することが必要ではないか²⁷。

²⁷ 米国 NTIA（国家電気通信情報庁）では、2012年7月から、モバイルアプリに関するプ

- マルチステークホルダープロセスによるルール策定が円滑に進むよう、今後発展が期待されるセクターを選定し、実証実験等を通じ、具体的なケーススタディを推進していくことが必要ではないか。
- マルチステークホルダープロセスに参加するインセンティブを与えるため、同プロセスによって策定されたルールの普及啓発とともに、同ルールを遵守している企業を国民・消費者に周知するなどの活動を推進していくことが必要ではないか。

5 パーソナルデータの利活用のルールの在り方

(基本的考え方)

- パーソナルデータの利活用のルールの内容については、諸外国や国際機関等での議論等を踏まえ、国際的に調和のとれたものとすることが必要。
- 保護されるパーソナルデータの中には、氏名などの通常公にされている情報から、健康に関する情報など人に知られたくない情報まで様々な性質のものがある。保護されるパーソナルデータを一律に取り扱うのではなく、その性質に応じて適切に取り扱うことが必要（再掲）。

(主な論点)

- パーソナルデータの取扱いについては、取得の際の経緯（コンテキスト）に沿った取扱いである場合と、それ以外の取得の際の経緯（コンテキスト）に沿わない取扱いの場合に分けて、適切な在り方を検討していくべきではないか。
- また、パーソナルデータの取扱いについては、前記Ⅲ 3のパーソナルデータのプライバシー性の高低により分類した類型に応じて、適切な在り方を検討していくべきではないか。
- 例えば、一般パーソナルデータについて、取得の際の経緯（コンテキスト）に沿った取扱いをする場合は、一般的には、明示的な同意を求める必要はないのではないか。
- 一方、取得の際の経緯（コンテキスト）に沿わない取扱いやセンシティブデータの取扱いについては、明示的かつ個別的な同意を求めることが必要となるのではないか。また、この場合の適切な「明示的」あるいは「個別的」な同意の在り方についても検討していくべきではないか。
- パーソナルデータの本人は、原則として、パーソナルデータの取扱いについて同意した場合であっても当該同意を撤回すること（明示的な同意をして

プライバシー保護に関するルール策定のため、マルチステークホルダープロセスを実施している。

いない場合に、オプトアウト²⁸の意思表示をすることを含む。) ができることとすべきではないか。

- パーソナルデータを利用する者には、透明性の確保の観点から、どのようなパーソナルデータをどのように利用しているか等について適切な形で開示することが求められるのではないか。
- 具体的には、パーソナルデータを利用する者の氏名・名称、利用するパーソナルデータの項目、取得方法、利用目的、本人関与の方法、第三者提供の有無、問い合わせ窓口及びこれらを変更する場合の手続について、プライバシーポリシー等の形で、本人が容易にアクセスできるような形で開示することが求められるのではないか²⁹。
- また、本人に分かりやすく情報を伝えるため、ラベルやアイコン等による簡潔な表示を行うことも求められるのではないか。この点については、「スマートフォン プライバシー イニシアティブ」³⁰など、内外で消費者に分かりやすく情報を伝えるため、簡潔な表示を行うことの重要性が指摘されており(参考資料5参照)、適切な表示の在り方等について、実証実験等を通じ、さらに検討を進めていくべきではないか。

6 パーソナルデータの保護のための関連技術の有用性

(基本的考え方)

- パーソナルデータの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 Technology: PET)を最大限に有効活用することが適切。
- 他方、プライバシーを保護するために利用可能な技術に関しては、当該技術を適用することで、パーソナルデータの利活用に関するルールの遵守がどのように確保されることになるのかについて、具体的かつ分かりやすく説明していくことが必要。

(主な論点)

- 平文で保存されているデータと暗号化して保存されているデータとの間

²⁸ 事後的に取扱いの停止を求めること

²⁹ スマートフォン上のアプリケーション提供者等による利用者情報の取扱いについては、透明性確保の観点から、「スマートフォン利用者情報取扱指針」が示されている。

(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「スマートフォンプライバシー イニシアティブー利用者情報の適正な取扱いとリテラシー向上による新時代イノベーションー」(平成24年8月))

³⁰ 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「スマートフォンプライバシー イニシアティブー利用者情報の適正な取扱いとリテラシー向上による新時代イノベーションー」(平成24年8月) 64頁参照

での情報漏えいした場合等に生じるプライバシーインパクトの違いを考慮して、それぞれ違った取扱いにするよう分野横断的に整理すべきではないか。

特に、情報理論的安全性を有する秘密分散技術を適用しているデータについて、復号するために必要となる数の分散データが漏えいしておらず、かつ適切な運用管理が行われている場合には、漏えいしたデータに保護されるパーソナルデータが含まれているとしても、保護されるパーソナルデータの漏えいに当たらないと整理できるのではないか。

- 前述のように、一般に公開されている国の統計情報など再識別化を不可能又は十分に困難にしたといえるものについては、保護されるパーソナルデータには当たらず、自由に利活用することができるとして差し支えないと考えられるのではないか。ただし、どのような状態となれば、再識別化を不可能又は十分に困難にしたといえるかについて、その考え方を示していく必要があるのではないか（前記Ⅲ 2 参照）。
- 他の情報との連結等により再識別化の可能性がある匿名化されたパーソナルデータについては、米国 F T C（連邦取引委員会）における考え方³¹等を踏まえ、次のような条件をすべて満たす場合は、保護されるパーソナルデータには当たらないとして、本人の同意を得なくても、利活用を行うことが可能と整理すべきではないか。

①適切な匿名化措置を施していること

②匿名化したデータを再識別化しないことを約束・公表すること

③匿名化したデータを第三者に提供する場合は、提供先が再識別化をすることを契約で禁止すること

この際、匿名化により非識別化されたデータと元の識別可能なデータ（連結可能匿名化における対応表を含む。）の双方を保持・使用する場合は、これらのデータは別々に保管することとすべきではないか。

この場合、これらの措置が採られていることについての透明性確保の措置や上記の約束や契約が遵守されることについての担保措置についても検討する必要があるのではないか³²。

³¹ F T C は、事業者が、①データが合理的に非識別化（de-identify）するための措置をとる、②そのデータを再識別化（re-identify）しないことを公に約束する、③そのデータの移転を受ける者が再識別化することを契約で禁止するとの要件を満たせば、当該データは特定の顧客、コンピュータその他のデバイスに、合理的に連結可能な（reasonably linkable）データには当たらないとしている。

なお、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としている。

（Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (2012)）

³² なお、匿名化されたパーソナルデータが再識別化された場合は、個人識別性の要件を満たすことから、保護されるパーソナルデータとなる。また、上記①～③の措置がとられた

- 暗号化技術、匿名化技術については、より高度化に向けた研究開発を支援するとともに、実態上問題が生じないと考えられる復号や再識別化が困難な状態（レベル）についての一般的な理解（共通認識）の醸成、技術的・運用的ガイドラインの作成等を推進すべきではないか。
- プライバシーの保護とパーソナルデータの利活用を両立できるトラストフレームワークの構築に向け、国際的な協調も視野にプライバシー保護に配慮したID連携の実証、標準化、普及啓発等を推進していくべきではないか。
- 多くのウェブブラウザにおいて実装が進むDNT（Do Not Track：利用者が自身のウェブの閲覧行動を追跡（トラッキング）されることを望まない場合に、トラッキングの拒否をウェブサービス提供者等に伝えるウェブブラウザの機能）について、ウェブブラウザの利用者に対しDNTについての周知啓発を行うとともに、広く各業界団体等を通じて、ウェブサービス提供者等にDNTに対応した機能の実装を働きかけていくべきではないか。

7 パーソナルデータ利活用のルール遵守確保の在り方

（基本的考え方）

- 個人の安心・安全を確保するためには、パーソナルデータの利活用のルールが適切に遵守される仕組みの構築が前提条件として必要。
- 上記の仕組みの構築に際しては、ルールの実効性や迅速な対応が可能となるメカニズムであることが必要。

（主な論点）

- 企業が自主的に定めたプライバシーポリシーの遵守を契約約款に規定することで、その遵守を担保することが考えられるのではないか。
- 同様に、前記Ⅲ4のマルチステークホルダープロセスにおいて策定されたルールの遵守を担保する手段として、プライバシーポリシーにマルチステークホルダープロセスにおいて策定されたルールの遵守を規定し、同プライバシーポリシーの遵守を契約約款に規定することが考えられるのではないか。
- パーソナルデータに関し専門的な知見を有する有識者などからなる機関を設置し、パーソナルデータの利活用のルールに関する判断の提示や、消費者と企業間の紛争解決を行うことが考えられるのではないか。
- 現行の個人情報保護法の下では、各省庁は、パーソナルデータの利活用の原則に基づき、政府内で適切に連携を図り、同法に基づく権限の行使等をしていくべきではないか。

にもかかわらず、再識別化がなされた場合は、上記の約束や契約違反の責任が問われることにもなる。

8 国際的なパーソナルデータの利用・流通の確保

(基本的考え方)

- 国際的なパーソナルデータの利用・流通が確保されるためには、国際的に調和のとれたパーソナルデータの保護が行われ、個人の安心・安全が確保されることが必要。
- 短期的な取組においても、これらの視点は重要であるが、国際的なルールとの調和を図るためには、後記IVで述べる中期的な対応が不可欠。

(主な論点)

- 我が国において国際的に調和のとれたパーソナルデータの利活用の枠組みを実現し、国際的なパーソナルデータの自由な流通の確保の実現に向けて、OECD、APEC等の場において、国際的なルールメイキングの議論に積極的に貢献していくべきではないか。
- 国際的な調和のとれた保護を実現するため、以下の事項について、その実効性等について検討していく必要があるのではないか。
 - ・ 国際的なパーソナルデータ保護の執行協力
 - ・ 我が国のパーソナルデータ保護のルールの国際的な適用の可能性
 - ・ パーソナルデータの保護が十分になされていない国等へ我が国からパーソナルデータを移転する場合に、十分なセーフガードを求めること
- 我が国におけるパーソナルデータの利活用のルールを守ることにより、国際的にプライバシー等の保護の水準が十分であると認められ、海外から我が国国内への情報流通についても円滑に行われる環境が確保されるために、どのような取組が必要か。

IV パーソナルデータの利活用の促進に向けた中期的な課題への対応

ここでは、パーソナルデータの利用・流通の促進に向けて、前記Ⅲで提示したパーソナルデータの利活用の枠組みの実施のために必要となる中期的な方向性を提示している。

(基本的考え方)

- パーソナルデータの利活用の促進のためには、自己のパーソナルデータが適切に保護されているという国民の信頼を確保・強化するとともに、企業が安心してパーソナルデータの利活用ができるよう、パーソナルデータの利活用のルールの明確化が行われることが確保されることが必要。
- 国境を越えて情報が流通する環境の下、自由な情報の流通とパーソナルデータ保護の双方を確保する国際的に調和の取れた制度の構築が必要。特に、クラウドサービス、検索サービス、OTT³³など情報の利用・流通に関連するサービスにおいて、国境を越えるものが主要なものとなっている現状を踏まえれば、国際的に調和の取れた制度の整備は不可避。
- パーソナルデータの国際的な流通について、EU・米の間では、セーフハーバー枠組みにおいて、自由な流通が行われるスキームが成立している一方、EU・日本の間では、EUは日本がパーソナルデータの十分な保護を行っているとは認定しておらず、各企業に個別の対応が求められるなど、日本は著しく不利な立場に立たされており、このような状態の速やかな解消が必要。
- 国際的に見ると、EUを中心としてパーソナルデータの保護については、独立した第三者機関であるプライバシーコミッショナーが設置され、分野横断的なパーソナルデータの取扱いに関する運用が行われている国が多い。また、米国においても、主として独立行政委員会であるFTCが、パーソナルデータの保護の監督をしているところであり、こうした諸外国の制度も踏まえた検討が必要（参考資料6参照）。
- 前記Ⅲで提示したパーソナルデータの利活用の枠組みの実施については、プライバシーポリシーの明確化やその遵守の確保など事業者の自主的な取組や現行制度の運用改善等により、短期的に解決が可能と考えられるものもあるが、その永続性・安定性の確保のためには、個人情報保護法の在り方の見直しなど中期的な取組が必要不可欠。これらの中期的な取組が必要なものについては、上記視点を踏まえ、政府全体として速やかに検討を進

³³ Over The Top の略。動画データや音声データなどのコンテンツを通信事業者のサービスによらずに提供するサービス。

めていくことが必要。

(主な論点)

- パーソナルデータの保護は、分野横断的に統一的な見解を求められることが多く、また、主としてパーソナルデータの利活用が行われるICT分野は技術革新が激しく、迅速かつ柔軟な判断が求められることを踏まえれば、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べきではないか。
検討に際しては、パーソナルデータの利活用のルールの明確化が行われ、自己のパーソナルデータが適切に保護されているという国民の信頼が確保・強化されるとともに、企業が安心してパーソナルデータの利活用が可能となる環境を実現する視点が重要ではないか。
- また、諸外国との協調によって、パーソナルデータの国際的な円滑な流通を確保していくことが重要ではないか。これにより、企業の国際展開や国境を越えたビッグデータの活用などが容易になり、我が国の経済成長にも寄与するのではないか。
- 前記Ⅲ 4 のマルチステークホルダープロセスにおいて策定されたルール、企業が自主的に定めたプライバシーポリシーのいずれについても、企業が自主的に契約としての効力を持たせることに合意しない限り、一般的には法的な拘束力はないのが現状である³⁴。諸外国の制度にならって（参考資料7参照）、企業等が自主的に宣言したルール・ポリシー等への遵守を確保するための制度を整備すべきではないか。
- また、マルチステークホルダープロセスに参加する企業については厳格なルールが適用される一方、同プロセスに参加しない企業については何のルールも適用されないといった不公平な状況の発生を防止するため、同プロセスに参加する企業にインセンティブを与えると同時に、同プロセスに参加しない企業についてもパーソナルデータの利活用の原則の遵守を確保するための仕組みについても検討していくことが必要ではないか。
- 現行の個人情報保護法については、小規模事業者の扱い、共同利用の在り方、民間事業者・行政機関・独立行政法人・各地方公共団体で規律が異なることなど様々な課題が指摘されている³⁵。これらの課題についても、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っていくべきはないか。

³⁴ これらのルール等への違反が、個別分野において各種業法などで業務改善命令等の執行の対象となることはありうる。

³⁵ 消費者委員会個人情報保護専門調査会「個人情報保護専門調査会報告書～個人情報保護法及びその運用に関する主な検討課題～」(平成23年7月)参照