別紙２

「パーソナルデータの利用・流通に関する研究会」論点整理

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、スマートフォン、タブレット端末などいわゆるスマートデバイスの普及が、我が国においても急速に進展している。スマートデバイスの特徴は、ネットワークに接続した状態で携帯され、いつでもどこでも多種多様なサービスを享受することができることにある。スマートデバイスにおいては、利用履歴、位置情報等様々な情報の蓄積・発信が可能となっており、利便性の高いサービスを安心安全に利用できるようにするため、これらの情報の適正な利活用が確保されることの重要性が増している[1]。

さらに、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[2]、米国の消費者プライバシー権利章典の公表[3]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[4]、行政機関個人情報保護法[5]、独立行政法人等個人情報保護法[6]があげられる。また、

---

1 例えば、スマートフォンにおける利用者情報の取扱いについては、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　－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－」（平成２４年８月）参照

2 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)*

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

4 個人の情報の保護に関する法律（平成１５年法律第５７号）

5 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）

6 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）

パーソナルデータの利活用については、統計法[7]、電気通信事業法[8]による通信の秘密の保護、知的財産権の保護、情報公開法[9]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」[10]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、クッキー等）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）。

7 統計法（平成１９年法律第５３号）
8 電気通信事業法（昭和５９年法律第８６号）
9 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）
10 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）

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」[11]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」[12]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～」[13]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、今後の防災に役立てる試みも報道されている[14]。

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れば、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。

---

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

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

13 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）

14 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[15]。

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[16]。

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。

そのうち、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、取扱い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

---

15 例えば、スマートフォンの利用者情報の問題に関しては、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－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－」（平成２４年８月）１４頁参照

16 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。

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正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、その適正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正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こと

・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こと

・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切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、藤原靜雄・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や、スマートフォン等の識別情報（端末ＩＤ等）などは、一義的にはＰＣやスマートフォンといった特定の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、プライバシー

[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

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。この観点から、ＩＰアドレス、クッキー等についても、保護されるパーソナルデータの範囲に含まれるべきかどうかについて検討していくべきではないか。

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[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[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。

また、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Ⅲ６参照）。

---

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、保護される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、個人の特定を不可能とし、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正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正な取扱いを検討することとすべきではないか（具体的な適正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。なお、この類型に含まれるパーソナルデータについては、プライバシー性の程度に相違があり、これに応じた適正な取扱いが求められると考えられるのではないか。

〇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]

[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

・電話帳情報
・ＧＰＳなどの位置情報
・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

〇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こと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

➢ 上記で例示していない例えば金融・財産情報等についても、どの類型に含まれるとすべきかについて、検討していくべきではないか。

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、主としてパーソナルデータの利活用が行われる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

プライバシー　イニシアティブ　－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－」（平成２４年８月）６１頁参照

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]。

➢ 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正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Ⅲ３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[28]。

➢ 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）

---

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。

28 個人情報保護法においても、「取得の状況からみて利用目的が明らかな場合」は、利用目的の通知・公表義務の適用除外にあたるとされている（第 18 条第４項第４号）。

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、原則として、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。

➢　なお、上記は原則的な取扱いと考えられるが、災害時や防災目的の場合などについて、例外として本人の同意を要しない場合についても、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、当該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いない場合に、オプトアウト[29]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。この場合、同意の撤回の効果についても明らかにしていくべきではないか。

➢　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[30]。

➢　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」[31]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。

---

29 事後的に取扱いの停止を求めること

30 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　－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－」（平成２４年８月））

31 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　－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－」（平成２４年８月）６４頁参照

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Ⅲ２参照）。

➢　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ＦＴＣ（連邦取引委員会）における考え方[32]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

[32] ＦＴＣ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)）

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[33]。

➢ 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の遵守確保の在り方

（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。

[33] 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。

（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。

➢　様々な場において、パーソナルデータの利活用のルールの普及啓発及び予見可能性の向上のため、具体的事例の検討を深めるとともに、検討結果について適切に公開し、事例の蓄積・共有を図ることが有用ではないか。

➢　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。

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）

➢　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、我が国のパーソナルデータの保護についての取組を紹介するとともに、国際的なルールメーキングの議論に積極的に貢献していくべきではないか。

➢　パーソナルデータの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、他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適正な利用・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、技術革新の中で、パーソナルデータの利活用のルールの明確化が迅速に行われ、ルール適用の予見性・透明性が確保される仕組みが必要。

■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、ＯＴＴ[34]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

[34] 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。

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、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[35]。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ともに、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[36]。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

35 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。

36 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

な制度整備について検討を行っていくべきはないか。

「パーソナルデータの利用・流通に関する研究会」

論点整理

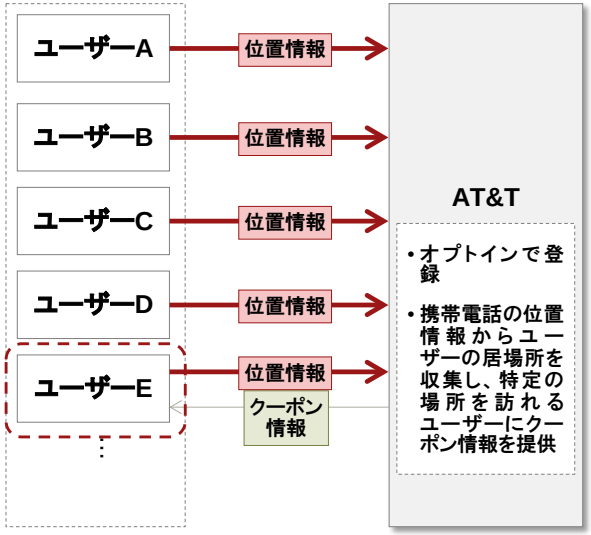
参考資料集

パーソナルデータの利活用の事例①（情報通信業）

参考資料１－１

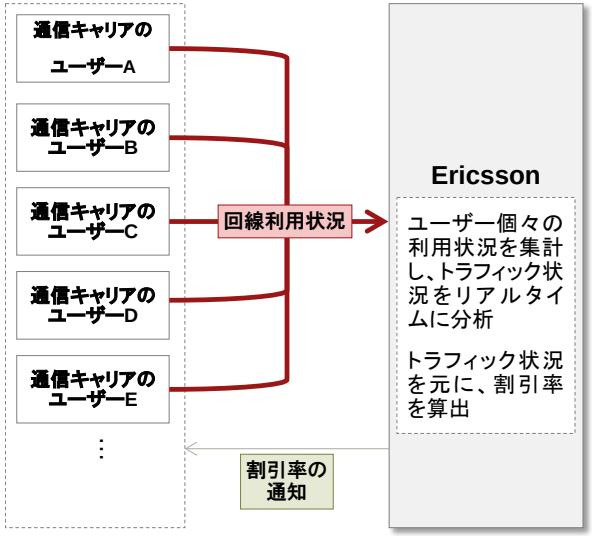
AT&T Shop Alerts

- AT&Tが、Placecastの位置情報プラットフォームを活用し、同社の顧客に対してクーポンを配信
- 飲食店やイベント開催場所など、一定区域内に入ったユーザーに対し、適切なクーポンや割引情報を配信
- 携帯電話のGPS機能を活用することで、ユーザーに対して適切なタイミングで割引情報を提供することができ、広告効果を高めることが可能に



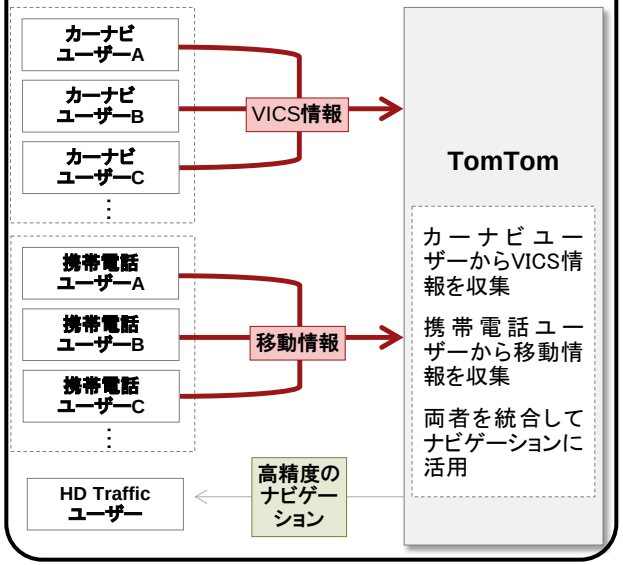
Ericsson DDS (Dynamic Discount Service)

- Ericssonが南アフリカの通信キャリアMTNグループと開発したリアルタイム割引サービスを提供
- 全ユーザーの回線利用状況を集計し、基地局毎のトラフィック状態をリアルタイムに分析
- エリア・時間帯別に、トラフィックに余裕のある場合には高い（最大80%）割引率を動的に設定
- 発展途上国の貧弱な回線であっても、大規模な設備投資を行うことなくトラフィックを最適化可能に



TomTom HD Traffic

- TomTomのカーナビは通信機能を備えており、FM放送を利用して端末の情報を収集（VICSに相当）
- 一方で最大1670万台の携帯電話の基地局情報／GPSデータを匿名化して収集し、利用者の移動速度・進行方向を判別
- 両データを統合することでリアルタイムに精度の高いナビゲーションを提供
- 通常よりも目的地までの時間を平均で15%削減



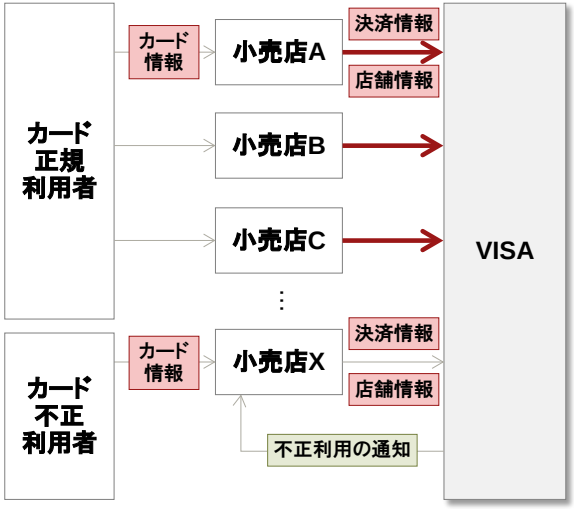
出典：本研究会第2回会合吉川構成員資料、（株）日立コンサルティング作成資料

パーソナルデータ利活用の事例②（金融業・保険業）

参考資料１－２

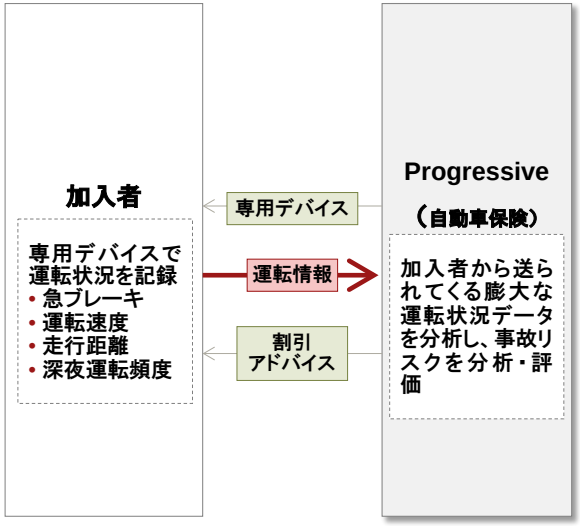
Visa Advanced Authorization

- 各店舗から送られてくる決済情報を、リアルタイムで照合・分析
- 「短時間に大きく離れた店舗で決済が発生したケース」など、不正利用の可能性が高い取引を監視し、取引が発生したその場で店舗に対して通知を実施
- カードの不正利用をリアルタイムに発見し、不正利用を早期に発見、対応することが可能になり、店舗、正規利用者の双方に対し、より高いセキュリティを提供することが可能に



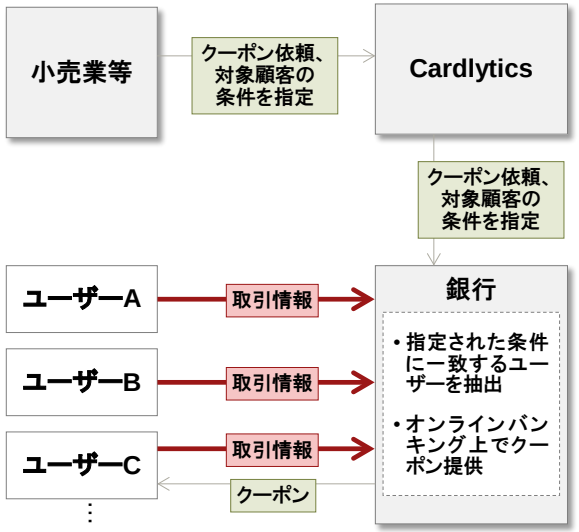
Progressive Snapshot

- 加入者に専用のデバイス（一種のドライブレコーダー）を配布し、詳細な運転状況を記録
- 加入者の事故リスクを分析・評価、個々人の運転状況に合わせた割引率を算定
- インターネットを通して、運転状況のフィードバックや安全運転のアドバイスを実施
- 蓄積された詳細な行動データを解析することで、リスクを適正に判断可能に



Cardlytics

- クーポンを配布したい小売業者等が、Cardlyticsにクーポンの配布条件を依頼
- Cardlyticsは、銀行に対して該当する顧客の抽出を依頼
- 銀行は取引データを分析して該当顧客を抽出し、対象顧客にインターネットバンキング上でクーポンを提供
- 対象顧客抽出やクーポン配布は銀行で行われ、Cardlytics等に個人情報は流出しない



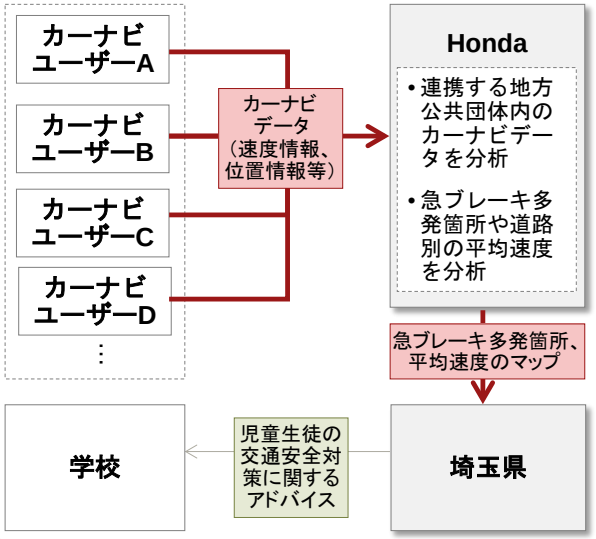
出典：本研究会第2回会合吉川構成員資料、（株）日立コンサルティング作成資料

パーソナルデータ活用の事例③（行政分野、公益事業）

参考資料１－３

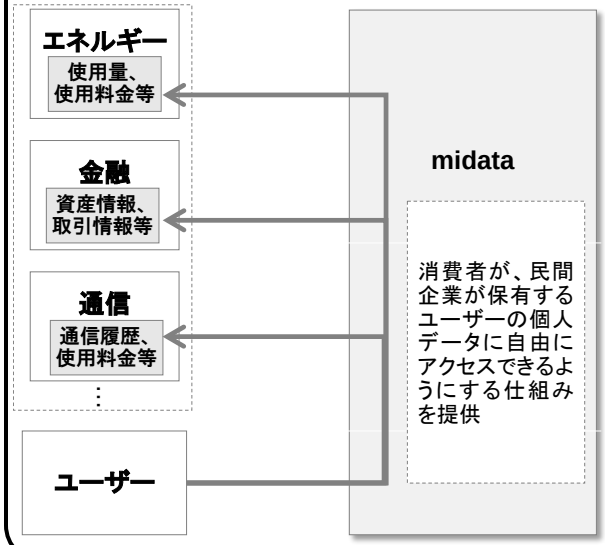
埼玉県 カーナビデータ活用

- 埼玉県では、Hondaと連携してカーナビデータの分析結果を道路行政に活用
- 車の位置情報や速度情報から急ブレーキの多発箇所を分析・抽出し、区画線の設置や街路樹の伐採によって事故件数が減少
- また、児童生徒等の交通安全対策のため、登下校時の急ブレーキ多発箇所や通学路における車の平均走行速度を分析、登下校時の人員配置や注意喚起に活用



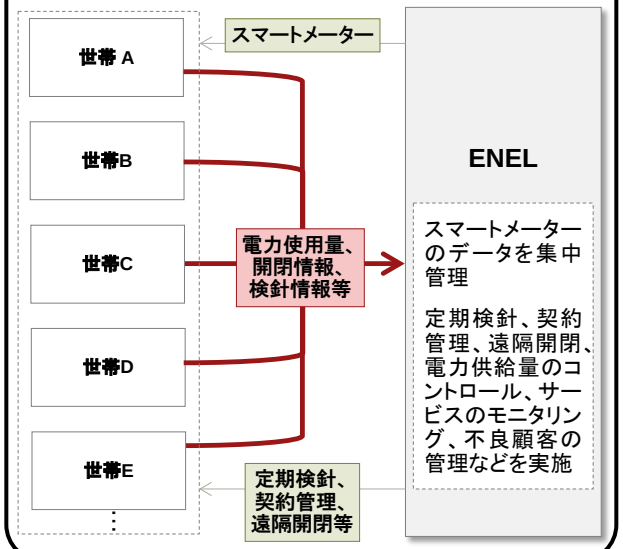
midata

- 消費者が民間企業の持つ自分の個人データに自由にアクセスできるようにすることを目指し,英政府主導で2011年に開始されたプロジェクト
- midataにはエネルギー、金融、通信などの業界から20を超える企業がパートナーとして個人データを提供
- 民間保有の個人データ活用を狙ったMidataHackathonなども開催された



ENEL Smart Meter

- ENELはイタリアの電力会社であり、スマートメーターの大規模設置を実施、顧客3300万戸のほとんどに導入を完了
- スマートメーターのデータは、PLC（電力線通信）およびGSM（携帯通信）を経由して集中管理
- 定期検針（15分間隔）、契約管理、遠隔開閉、電力供給量のコントロール、サービスのモニタリング、不良顧客の管理などを遠隔で実施可能



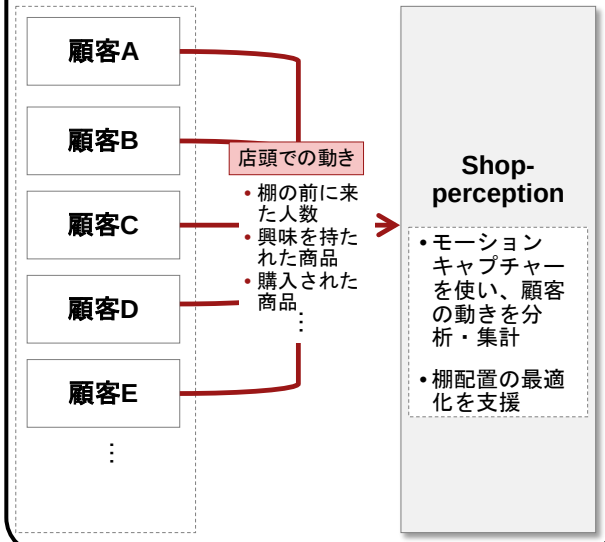
出典：本研究会第5回会合奥屋構成員資料、（株）日立コンサルティング作成資料

パーソナルデータ利活用の事例④（小売業）

参考資料１－４

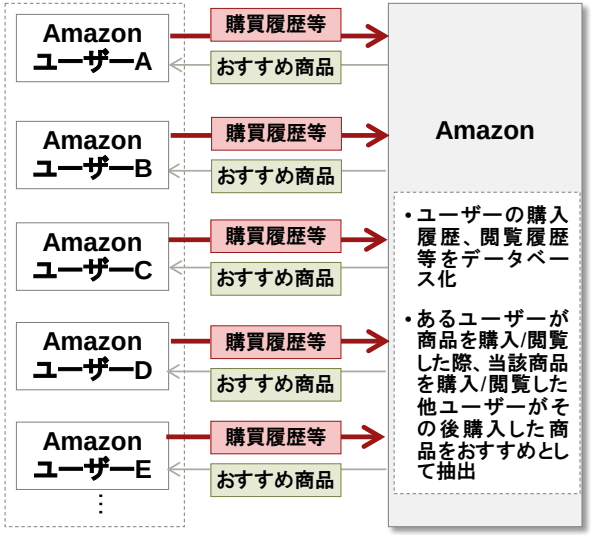
Shopperception

- 小売店の陳列棚に設置されたKinectモーションキャプチャーシステムにより、手に取られた商品や顧客の動線等を機械的に分析・記録することが可能
- 販売時点（Point of Sales）のデータに加え、POB（Point of Buying）データを取得
- 「興味は持たれたが購買に至らなかった商品」と「全く興味が持たれなかった商品」の区別が可能になり、販売促進費の投資を最適化



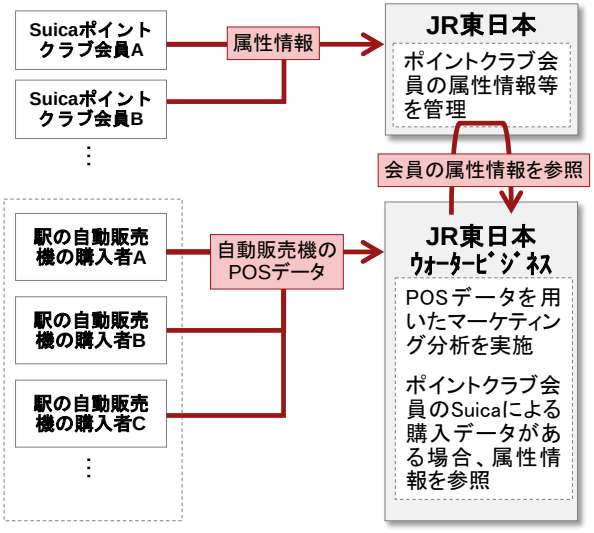
Amazon おすすめ商品

- Amazon おすすめ商品は、利用者が好みそうな商品をオンラインストア上に表示する仕組み
- 利用者の購入履歴、商品の閲覧履歴等のデータを基に、協調フィルタリング等の技術を用いて自動的に作成、表示される
- 利用者が購入履歴や閲覧履歴等はWeb上で参照でき、商品ごとにおすすめ商品の表示に利用するかどうかを指定することも可能



JR東日本ウォータービジネス

- JR東日本ウォータービジネスは駅の自動販売機を管轄する会社であり、自動販売機のPOSデータを保有
- Suicaポイントクラブ会員のSuicaで購入されたPOSデータについて、購入者の属性情報を参照し（ただし、事前同意がある人のみ）、マーケティング情報としての質を向上
- 取扱商品の選定や商品開発に活用し、購買ニーズの喚起や売上の向上に寄与



出典：本研究会第2回会合吉川構成員資料、（株）日立コンサルティング作成資料

参考資料２

パーソナルデータの保護の原則の比較

OECD プライバシーガイドライン（1980）	欧州評議会第108号条約（1981）及び同追加議定書（2001）	EU データ保護指令（1995）	EU データ保護規則案（2012）	APEC プライバシーフレームワーク（2004）	ISO/IEC 29100:2011 Privacy framework	米国消費者プライバシー権利章典（2012）	（参考）スマートフォンプライバシーイニシアティブ（2012）
プライバシーと個人の自由を保護し、かつプライバシーと情報の自由な流通という基本的ではあるが競合する価値を調和させること	個人の権利と基本的な自由、特に個人データの自動処理に関するプライバシーの権利の尊重の保証（データ保護）	自然人の基本的な権利及び自由、特にそのプライバシーの権利の保護	自然人の基本的権利と自由、特にその個人データの保護の権利の保護	パーソナルインフォメーションに対するプライバシーの保護と情報の自由な流通	このプライバシーの枠組みは、組織がPII(Personally Identifiable Information)に関連するプライバシー保護要件を定義することを助けることを意図する	個人の権利と個人データに関する企業のとるべき義務を定める	関係事業者等は、利用者がスマートフォンやそれを通じて提供される利便性の高いサービスを安全・安心に利用できる環境を整備するために、個人情報やプライバシーを保護しつつスマートフォンにおける利用者情報を取り扱う
1. 収集制限の原則 2. データ内容の原則 3. 目的明確化の原則 4. 利用制限の原則 5. 安全保護の原則 6. 公開の原則 7. 個人参加の原則 8. 責任の原則	1. 独立した監督機関 2. 司法による救済 3. データ越境制限 4. 最小データ取得原則 5. 公正で合法的な手続き 7. 使用後のデータ廃棄 8. センシティブデータの保護 （※）	1. 独立した監督機関 2. 司法による救済 3. データ越境制限 4. 最小データ取得原則 5. 公正で合法的な手続き 6. 監督機関への報告 7. 使用後のデータ廃棄 8. センシティブデータの保護 9. 意思決定の自動化の制限 10. ダイレクトマーケティング利用におけるオプトアウト （※）	1. 独立した監督機関 2. 司法による救済 3. データ越境制限 4. 最小データ取得原則 5. 公正で合法的な手続き 6. 監督機関への報告 7. 使用後のデータ廃棄 8. センシティブデータの保護 9. 意思決定の自動化の制限 10. ダイレクトマーケティング利用におけるオプトアウト （※）	1. 被害防止の原則 2. 通知の原則 3. 収集制限の原則 4. 個人情報使用の原則 5. 選択の原則 6. 個人情報完全性の原則 7. セキュリティ保護の原則 8. アクセスと訂正の原則 9. 説明責任の原則	1. 同意と選択 2. 目的の正当性と明確性 3. 収集の制限 4. データ最小化 5. 利用、保管、公開の制限 6. 精度と品質 7. 公開性、透明性と通知 8. 個人参加とアクセス 9. 説明責任 10. 情報セキュリティ 11. プライバシー・コンプライアンス	1. 個人のコントロール 2. 透明性 3. 経緯（コンテキスト）の尊重 4. 安全性 5. アクセスと正確性 6. 対象を絞った収集 7. 説明責任	1. 透明性の確保 2. 利用者関与の機会の確保 3. 適正な手段による取得の確保 4. 適切な安全管理の確保 5. 苦情・相談への対応体制の確保 6. プライバシー・バイ・デザイン

※欧州評議会第108号条約及び同追加議定書、EUデータ保護指令、EUデータ保護規則案についてはGraham Greenleaf教授（ニューサウスウェールズ大学法学部）の公開資料（The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?, Research Paper Series No 2012/12）による。なお、これらにはOECDプライバシーガイドラインの8原則の内容が全て含まれていると述べられている。

参考資料３

保護対象となるパーソナルデータの範囲の比較

OECD ガイドライン（1980）	「個人データ」とは、識別された又は識別されうる個人（データ主体）に関する全ての情報を意味する。 "personal data" means any information relating to an identified or identifiable individual (data subject);
欧州評議会第 108 号条約（1981）及び同追加議定書（2001）	「個人データ」とは、識別された又は識別可能な個人（「データ対象者」）に関連する全ての情報を意味する。 "personal data" means any information relating to an identified or identifiable individual ("data subject");
EU データ保護指令（1995）	「個人データ」とは、識別された、又は識別可能な自然人「データ主体」に関連する全ての情報を意味する。識別可能な人とは、直接的又は間接的に、特に識別番号又は一つ若しくはそれ以上の身体的、生理的、精神的、経済的、文化的又は社会的な識別性に関連する固有の要素によって、識別されうる人である。 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;
EU データ保護規則案（2012）	「個人データ」とは、あるデータ主体に関する全ての情報である。「データ主体」とは、識別された自然人、又は管理者若しくはそれ以外の自然人若しくは法人によって合理的な範囲で使用される手段をもって直接的又は間接的に識別された自然人である。特に、識別番号、位置データ、オンライン識別子又は当該者の身体的、生理的、遺伝的、精神的、経済的、文化的又は社会的な識別性に関連する一つ若しくはそれ以上の固有の要素によって識別されうる自然人のことである。 'personal data' means any information relating to a data subject; 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;
APEC プライバシーフレームワーク（2004）	「個人インフォメーション」とは、識別された又は識別可能な個人に関する全ての情報を意味する。（中略）単独ではそうした基準に満たない情報であっても、他の情報と併用すれば個人を特定できる場合はそれを個人情報とみなす。 Personal information means any information about an identified or identifiable individual. （中略）It also includes information that would not meet this criteria alone, but when put together with other information would identify an individual.
ISO/IEC29100:2011 Privacy framework	[個人識別可能情報(PII)](a)その性質が関連する PII の本人を識別するために利用可能な、又は(b)直接的又は間接的に PII principal に連結可能な全ての情報 [personally identifiable information PII] any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal [PII の本人]個人識別可能情報(PII)に関連する自然人 [PII principal] natural person to whom the personally identifiable information (PII) relates
米国プライバシー権利章典（2012）	消費者プライバシー権利章典は、個人データの商業利用に適用される。この用語（個人データ）は、特定の個人に連結可能な全てのデータをいい、集約されたデータを含む。個人データは、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みうる。例えば、利用記録を作成するために使われるスマートフォンや家庭のコンピュータの識別子は個人データである。 The Consumer Privacy Bill of Rights applies to commercial uses of personal data. This term refers to any data, including aggregations of data, which is linkable to a specific individual. Personal data may include data that is linked to a specific computer or other device. For example, an identifier on a smartphone or family computer that is used to build a usage profile is personal data.
(参考)個人情報の保護に関する法律(2003)	「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。

参考資料４－１

センシティブデータの範囲の比較（諸外国、国際機関等）

欧州評議会第 108 号条約（1981）及び同追加議定書（2001）	民族の起源、政治的見解、宗教その他の思想を明らかにする個人データ及び健康又は性生活に関する個人データ は国内法が適用されて適切な保護がなされることなしに自動的に処理されるべきではない。犯罪処罰に関連する個人データ も同様である。 Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.
EU データ保護指令（1995）	加盟国は、人種又は民族の起源、政治的見解、宗教的又は哲学的な思想、労働組合の加盟状況を明らかにする個人データ 及び 健康又は性生活に関するデータ の処理を禁止する。 Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.
EU データ保護規則案（2012）	人種及び民族の起源、政治的見解、宗教や思想、労働組合の加盟状況を明らかにする個人データ の処理及び 遺伝データ又は健康若しくは性生活、犯罪処罰若しくは関連する保護措置に関するデータ の処理を禁止する。 The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited.
ISO/IEC29100:2011 Privacy framework	例えば、PII の本人の人種、民族の起源、宗教若しくは哲学的信条、政治的見解、労働組合の加盟状況、性生活若しくは傾向及び身体的又は精神的健康に関する情報 を含む。他の法域では、センシティブな PII は 個人情報の盗難を容易に知る情報 又は 重要な財政的損害を自然人にもたらすこととなる情報（例えば、クレジットカード番号、銀行口座情報、パスポート番号、社会保障番号、免許証番号その他の政府発行 ID）及び PII の本人のリアルタイムの位置情報を決定するのに利用することができる情報 を含みうる。 Examples include information revealing race, ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, sexual lifestyle or orientation, and the physical or mental health of the PII principal. In other jurisdictions, sensitive PII might include information that could facilitate identity theft or otherwise result in significant financial harm to the natural person (e.g., credit card numbers, bank account information, or government-issued identifiers such as passport numbers, social security numbers or drivers' license numbers), and information that could be used to determine the PII principal's real time location.
米国 FTC 報告書「急速に変化する時代における消費者プライバシーの保護」（2012）	委員会は、以下で議論するように、子供（注：13 歳未満）、金融及び健康に関する情報、社会保障番号並びに一定の位置情報 は、少なくともセンシティブデータであると定義する。 The Commission defines as sensitive, at a minimum, data about children, financial and health information, Social Security numbers, and certain geolocation data, as discussed below.

参考資料４－２

センシティブデータの範囲の比較（個人情報保護法に基づく各省庁のガイドライン）

金融分野における個人情報保護に関するガイドライン （金融庁）	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 （総務省）	債権管理回収業分野における個人情報保護に関するガイドライン （法務省）	医療情報システムの安全管理に関するガイドライン （厚生労働省）	職業紹介事業者、労働者の募集を行う者、募集受託者、労働者供給事業者等が均等待遇、労働条件等の明示、求職者等の個人情報の取扱い、職業紹介事業者の責務、募集内容の的確な表示等に関して適切に対処するための指針 （厚生労働省）	派遣元事業主が講ずべき措置に関する指針 （厚生労働省）	福祉関係事業者における個人情報の適正な取扱いのためのガイドライン （厚生労働省）
第６条 機微（センシティブ）情報について １ 金融分野における個人情報取扱事業者は、政治的見解、信教（宗教、思想及び信条をいう。）、労働組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活、並びに犯罪歴に関する情報（以下「機微（センシティブ）情報」という。）については、次に掲げる場合を除くほか、取得、利用又は第三者提供を行わないこととする。 ①～⑧（略）	（取得の制限） 第４条 （略） ２ 電気通信事業者は、次の各号に掲げる個人情報を取得しないものとする。ただし、自己又は第三者の権利を保護するために必要な場合その他社会的に相当と認められる場合はこの限りでない。 一 思想、信条及び宗教に関する事項 二 人種、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	第５ 機微（センシティブ）情報について １ 債権回収会社は，政治的見解，信教（宗教，思想及び信条をいう。），労働組合への加盟，人種及び民族，門地及び本籍地，保健医療及び性生活，並びに犯罪歴に関する情報（以下「機微（センシティブ）情報」という。）については，次に掲げる場合を除き，取得，利用又は第三者提供を行わないこととする。 (1)～(7) （略）	4.3 例示による責任分界点の考え方の整理 （略） ただし、受託する事業者は保存した情報の漏えい防止、改ざん防止等の対策を講じることは当然であるが、感染症情報や遺伝子情報等機微な情報の取り扱い方法や保存期間等を双方協議し明記しておく必要がある。	１ 個人情報の収集、保管及び使用 (1) 職業紹介事業者等は、その業務の目的の範囲内で求職者等の個人情報（略）を収集することとし、次に掲げる個人情報を収集してはならないこと。（略） イ 人種、民族、社会的身分、門地、本籍、出生地その他社会的差別の原因となるおそれのある事項 ロ 思想及び信条 ハ 労働組合への加入状況	10 個人情報の保護 (1) 個人情報の収集、保管及び使用 イ 派遣元事業主は、（略）、次に掲げる個人情報を収集してはならないこと。（略） (ｲ) 人種、民族、社会的身分、門地、本籍、出生地その他社会的差別の原因となるおそれのある事項 (ﾛ) 思想及び信条 (ﾊ) 労働組合への加入状況	２．本指針の基本的考え方 （略） 社会福祉事業を実施する事業者は、多数の利用者やその家族について、他人が容易には知り得ないような個人情報を詳細に知り得る立場にあり、社会福祉分野は個人情報の適正な取扱いが強く求められる分野であると考えられる。 例えば、①保護施設における被保護者の生活記録や困窮に至った事情、②身体障害者更生援護施設や知的障害者援護施設における利用者の障害の種類及び程度、③保育所における両親の就業状況、④児童養護施設における児童の生育歴や家庭環境、⑤婦人保護施設における入所者の家族の状況、⑥社会福祉協議会における世帯更生資金の借受人の経済状況、など は特に適正な取扱いが強く求められる情報であると考えられる。

雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての留意事項について （厚生労働省）	農林水産分野における個人情報保護に関するガイドライン （農林水産省）	経済産業分野のうち信用分野における個人情報保護ガイドライン （経済産業省）	経済産業分野のうち個人遺伝情報を用いた事業分野における個人情報保護ガイドライン （経済産業省）	個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン （経済産業省）	船員派遣元事業主が講ずべき措置に関する指針 （国土交通省）	無料船員職業紹介事業者、船員の募集を行う者及び無料船員労務供給事業者が均等待遇、労働条件等の明示、求職者等の個人情報の取扱い、募集内容の的確な表示に関して適切に対処するための指針 （国土交通省）
４ その他事業者が雇用管理に関する個人情報の適切な取扱いを確保するための措置を行うに当たって配慮すべき事項 (4) ＨＩＶ感染症やＢ型肝炎等の職場において感染したり、蔓延したりする可能性が低い感染症に関する情報や、色覚検査等の遺伝情報については、職業上の特別な必要性がある場合を除き、事業者は、労働者等から取得すべきでない。	２ 取得の制限 農林水産関係事業者は、その事業の遂行に必要な場合に限り、個人情報を取得するものとする。また、思想、信条、宗教その他社会的差別原因となり得る個人情報の取得又は保有に当たっては、その適正な取扱いの確保に特段の配慮を加えるよう努めるものとする。	（１－２）機微（センシティブ）情報 与信事業者等は、機微（センシティブ）情報（政治的見解、信教（宗教、思想及び信条をいう。）、労働組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活、並びに犯罪歴に関する情報）については、取得、利用又は第三者提供を行わないこととする。	（１－２）機微（センシティブ）情報 個人遺伝情報取扱事業者は、事業に用いる個人遺伝情報を除き、政治的見解、信教（宗教、思想及び信条をいう。）、労働組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活、並びに犯罪歴に関する情報等については、法令等に基づく場合を除き、取得又は利用を行わないこととする。	(オ)主務大臣等への報告 ａ．個人情報取扱事業者が認定個人情報保護団体の対象事業者の場合 （略）ただし、以下の場合は、経済産業大臣（主務大臣）に、逐次速やかに報告を行うことが望ましい。 ・ 機微にわたる個人データ（(a)思想、信条又は宗教に関する事項、(b)人種、民族、門地、本籍地（所在都道府県に関する情報のみの場合を除く。）、身体・精神障害、犯罪歴その他社会的差別の原因となる事項、(c)勤労者の団結権、団体交渉その他団体行動の行為に関する事項、(d)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事項、(e)保健医療又は性生活に関する事項等）を漏えいした場合	(一) 個人情報の収集、保管及び使用 イ 船員派遣元事業主は、（略）、次に掲げる個人情報を収集してはならないこと。（略） (ｲ) 人種、民族、社会的身分、門地、本籍、出生地その他社会的差別の原因となるおそれのある事項 (ﾛ) 思想及び信条 (ﾊ) 労働組合への加入状況	一 個人情報の収集、保管及び使用 （一） 無料船員職業紹介事業者等は、（略）、次に掲げる個人情報を収集してはならないこと。（略） イ 人種、民族、社会的身分、門地、本籍、出生地その他社会的差別の原因となるおそれのある事項 ロ 思想及び信条 ハ 労働組合への加入状況

簡潔な表示に関する検討①

総務省の「スマートフォン プライバシー イニシアティブ」を踏まえた取組

■MCF（モバイル・コンテンツ・フォーラム）による「スマートフォンのアプリケーション・プライバシーポリシーに関するガイドライン」の策定・公表

＜ガイドラインの構成＞

第1部：充足すべき必要要件

第2部：実装にあたっての推奨要件

第3部：実装にあたってのモデル案

「アプリケーション・プライバシーポリシー」のモデル案と作成ガイドを提示。**詳細な本編**だけでなく**概要**の作成方法についても提示。

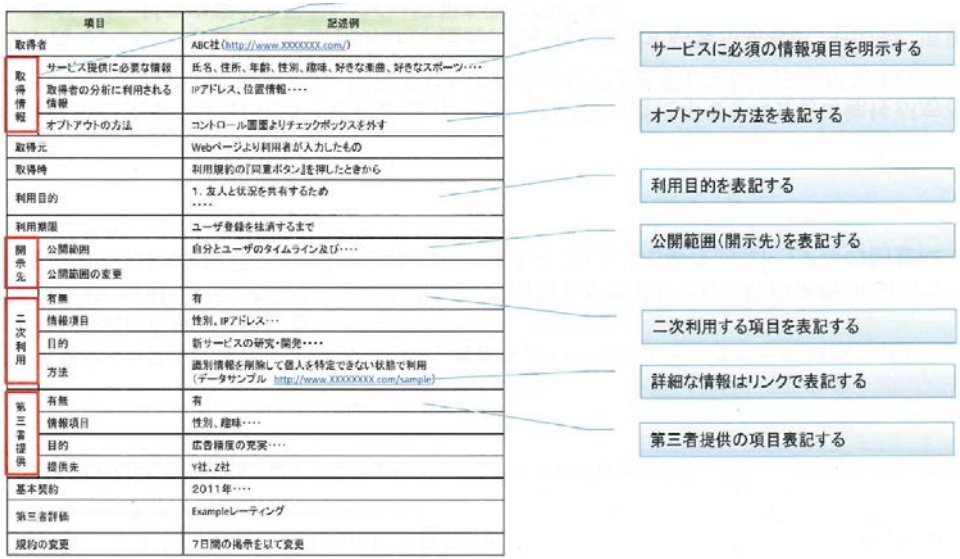
アプリケーション・プライバシーポリシーのモデル案

第１条（定義）
第２－１条（取得される情報の項目、利用目的、取得方法）
第２－２条（お客様ご自身によりご登録いただく情報）
第３条（同意）
第４－１条（外部送信）
第４－２条（第三者提供）※第三者提供がある場合
第５条（利用者関与の方法）
第６条（サービスの終了と情報の取扱い）
第７条（個人情報保護方針（プライバシーポリシー）等へのリンク）
第８条（情報の開示、提供）
第９条（取得された情報の公開、共有）
第10条（問い合わせ窓口）
第１１条（変更）

（参考）アプリケーション・プライバシーポリシー概要版

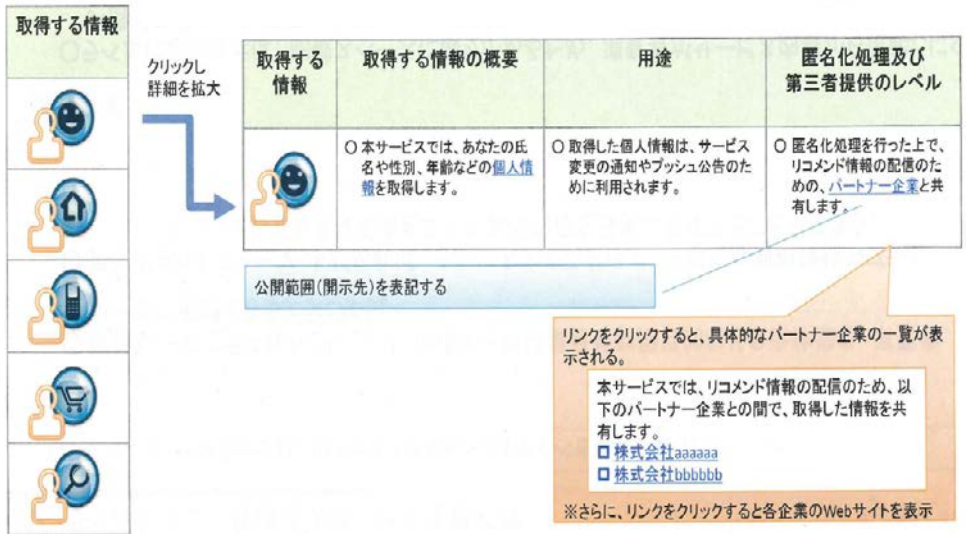
経済産業省パーソナルデータ WG における取組

■ラベル表示による一覧表示のイメージの提示



項目		記述例
取得者		ABC社（http://www.XXXXXXX.com/）
取得情報	サービス提供に必要な情報	氏名、住所、年齢、性別、趣味、好きな楽曲、好きなスポーツ……
	取得者の分析に利用される情報	IPアドレス、位置情報……
	オプトアウトの方法	コントロール画面よりチェックボックスを外す
取得元		Webページより利用者が入力したもの
取得時		利用規約の『同意ボタン』を押したときから
利用目的		1. 友人と状況を共有するため ……
利用期限		ユーザ登録を抹消するまで
開示先	公開範囲	自分とユーザのタイムライン及び……
	公開範囲の変更	
二次利用	有無	有
	情報項目	性別、IPアドレス……
	目的	新サービスの研究・開発……
	方法	識別情報を削除して個人を特定できない状態で利用 （データサンプル http://www.XXXXXXXX.com/sample）
第三者提供	有無	有
	情報項目	性別、趣味……
	目的	広告精度の充実……
	提供先	Y社、Z社
基本契約		2011年……
第三者評価		Exampleレーティング
規約の変更		7日間の掲示を以て変更

■アイコンによる表示のイメージの提示



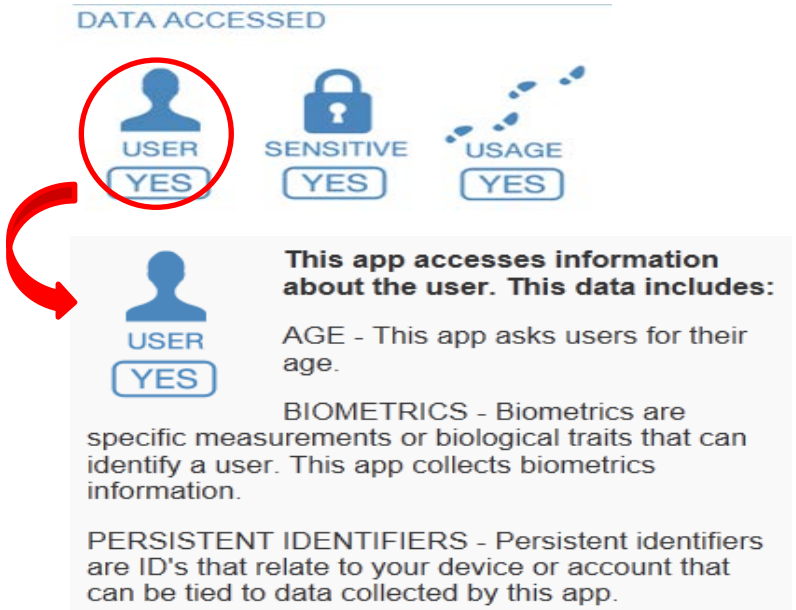
出典：経済産業省パーソナルデータ WG 資料

簡潔な表示に関する検討②

NTIA のマルチステークホルダー会合における検討

■ADA（アプリ開発者協会）他による利用者許諾の簡略な告知画面案

■ACT（競争的テクノロジー協会）による Privacy dashboard 案



カンターラ・イニシアティブにおける検討

■情報標準共有ラベル

情報取得者は、以下の目的のためにあなたの情報を取得しようとしています。

取得者	Facebook（http://www.facebook.com/）
取得情報	ステータス更新 [実際に見てみる]
取得元	このWebページからのステータス更新
取得時	「投稿」ボタンを押した時
利用目的	1. 友人と状況を共有するため。 2. あなた向けにカスタマイズされた広告を表示するため。
利用期限	元データおよび共有がすべて削除されるまで
開示先	自分と友達のタイムライン及び、Facebook の OpenGraph API を利用する、read_stream の許可をうけたアプリケーション。
追加条件	
基本契約	2011年4月26日付 https://www.facebook.com/legal/terms
第三者評価点	Exampleレーティング社 4.3/5 (2011/11/4)
規約の変更	一部例外を除き、７日間の掲示をもって変更

参考資料６

パーソナルデータ保護の監督機関の比較

	監督機関名称	所管法令	管轄	組織形態	任命方法
米国	連邦取引委員会（Federal Trade Commission(FTC)） ※Department of Health and Human Services、Federal Communication Commission なども個別分野を監督	連邦取引委員会法、金融サービス現代化法、公正信用報告法、児童オンラインプライバシー保護法等	民間部門（一部事業を除く）	委員会（5 名）	大統領によって指名、上院で承認、大統領が任命
ＥＵ	欧州データ保護監察官 (European Data Protection Supervisor(EDPS))	Regulation (EC) No 45/2001 of 18 December 2000	EU 機関	独任制	欧州委員会が公募でリストアップした候補から欧州議会と欧州理事会が任命
英国	情報コミッショナー事務局 （Information Commissioner's Office(ICO)）	データ保護法、情報自由法、プライバシー及び電子通信規則、環境情報規則	民間部門・公的機関	独任制	司法省が候補者を選定し、総理大臣へ推薦。政府が指名し、女王により任命
フランス	情報処理及び自由に関する国家委員会 (Commission nationale de l'informatique et des libertés(CNIL))	情報処理、情報ファイル及び自由に関する 1978 年 1 月 6 日の法律第 78-17 号	民間部門・公的機関	委員会（17 名）	裁判官 6 名、国会議員 4 名、経済・社会評議会委員 2 名は各々の機関が選出・任命。 上院・下院議長が IT 専門家を 2 名任命、首相が IT 又は市民的自由の専門家 3 名を任命。 委員長と 2 名の副委員長は委員から選出
ドイツ	連邦データ保護・情報自由監察官	ドイツ連邦データ保護法 （民間部門・公的機関を包括的に規制）	鉄道・郵便・通信部門及び連邦の公的機関	独任制	連邦政府の提案に基づき、ドイツ議会が選定し大統領が任命
	各州の監督機関		鉄道・郵便・通信部門以外の民間部門及び各州の公的機関	州により異なる	州により異なる
カナダ	カナダプライバシーコミッショナー事務局 (Office of the Privacy Commissioner of Canada(OPC))	プライバシー法（連邦の公的機関）、個人情報保護及び電子文書法（連邦及び州の民間部門。４州は州法が適用。医療分野の個別法を持つ州もある）	民間部門・連邦の公的機関	独任制	総督が上院と下院によって選定されたプライバシー･コミッショナーを任命
	各州プライバシーコミッショナー 例：オンタリオ州情報プライバシーコミッショナー (Information and Privacy Commissioner, Ontario Canada(IPC)) ※右の所管法令、任命方法は IPC の場合	※各州が州の公的機関の個人情報保護法を持つ オンタリオ州情報の自由及びプライバシー保護法（州政府、大学等） 自治体の情報の自由及びプライバシー保護法（市、警察、図書館、学校等） 個人の健康情報保護法（医療施設）	各州公的機関（民間部門も対象とする場合あり）	独任制	州副知事により任命 （オンタリオ州の場合）
ニュージーランド	プライバシーコミッショナー事務局 (The Office of the Privacy Commissioner)	プライバシー法	民間部門・公的機関	独任制	主務大臣の推薦に応じ総督が任命
オーストラリア	オーストラリア情報コミッショナー事務局 （Office of the Australian Information Commissioner(OAIC)） Australian Information Commissioner, Privacy Commissioner 及び Freedom of Information Commissioner(FOI)の３人のコミッショナーがおり、そのうち Australian Information Commissioner が他の 2 名の上位にあたる	オーストラリア情報コミッショナー法（Australian Information Commissioner Act） プライバシー法（Privacy Act） FOI 法（Freedom of Information Act）	民間部門・公的機関	独任制	政府からの助言をもとに総督が各コミッショナーを任命
シンガポール	シンガポール個人情報保護委員会(The Personal Data Protection Commission Singapore(PDPC))	個人情報保護法(PDPA)	民間部門	委員会(3~17名)	通信情報大臣が任命
韓国	個人情報保護委員会	個人情報保護法	民間部門・公的機関	委員会（15 名）	委員５名ずつ大統領・国会・大法院長が選出・指名

参考資料７

企業等が自主的に定めるルールについての根拠法令の比較

	米国	EU		英国	オランダ	イタリア	アイルランド
企業等が自主的に定めるルールについての根拠法令	FTC 法（Federal Trade Commission Act） 第 5 条 (a)(1) 不公正又は欺瞞的行為又は慣行は違法である (a)(2) FTC は違反行為に対し差止を行うことができる (b) FTC は違反行為に対し排除命令を行うことができる (m)(1)(A) FTC は違反行為に対し民事制裁金（1 万ドル以下）を請求することができる	データ保護指令（General Data Protection Directive） 第 27 条 1. EU 加盟国及び欧州委員会は、行動規範の策定を推奨しなければならない 2. EU 加盟国は、業界団体等が行動規範について国家機関の意見を聞くために付託できるように定めなければならない	データ保護規則案（General Data Protection Regulation (proposal)） 第 38 条 1. EU 加盟国、監督機関、欧州委員会は行動規範を策定することを奨励しなければならない 2. EU 加盟国において、業界団体等が行動規範について監督機関に意見を求めることができる 3. データ管理者の団体は、行動規範の草稿を欧州委員会に提出することができる 4. 欧州委員会は、提出された行動規範が妥当性を持っているか否かを決するために施行法を採択することができる	不公平な商取引からの消費者保護に関する規則（The Consumer Protection from Unfair Trading Regulations（CPRs）） 第 3 条 (1) 不公平な商業慣行は禁止される (4)(a) 第 5 条の誤解を生む行動は不公平な商業慣行である 第 5 条 (3)(b) 事業者が遵守に同意した行動規範を守らないことは、誤解を生む行動に該当する	個人データ保護法 第 25 条 1. 行動規範を策定する組織は、行動規範が法律を履行していると宣言するよう要求することができる 4. 要求に対する決定は、一般行政法における決定と同等と見なされる	個人データ保護法 第 12 条 1. 監査当局は、事業者による行動規範の策定を支援する 3. 行動規範に含まれる条文の遵守は、公的部門・民間部門を問わず個人データの処理が合法的であるための必要条件である	データ保護法 第 13 条 1. 監査当局は、業界団体による行動規範の策定を支援する (3)(a)(i) 承認された行動規範は、法律としての効力を持つ
備考	企業が自主的に宣言したプライバシーポリシーやその他のプライバシーに関する宣言や約束に違反した場合は、FTC 法第５条が適用される	—	—	OFT（英国公正取引庁）「Online Targeting of Advertising and Prices」 ・ターゲティング広告にはデータ保護法だけでなく CPRs が適用されうる ・消費者が実態を知らずにターゲティング広告を行うことは CPRs に違反する可能性がある	—	報道、歴史学、統計や学術研究、信用情報管理に関する行動規範が策定されている	—