別紙２

パーソナルデータの利用・流通に関する研究会
報告書 （案）

～パーソナルデータの適正な利用・流通の促進に向けた方策～

平成２５年５月

目次

本報告書の要旨 １
第１章　検討の背景 ５
第２章　パーソナルデータの利用・流通による可能性とその課題 ７
　第１節　パーソナルデータの利用・流通の現状と可能性 ７
　第２節　パーソナルデータの利用・流通に関する制度とこれまでの取組 ８
　　１．我が国の制度とこれまでの取組 ８
　　２．諸外国等の制度とこれまでの取組 １１
　第３節　パーソナルデータの利用・流通の促進に向けた課題 １８
第３章　パーソナルデータの利用・流通の促進に向けた方策 ２１
　第１節　パーソナルデータの利活用の枠組みとその実現に向けて先行的に実施すべき方向性. ２１
　　１．パーソナルデータの利活用の枠組みの体系 ２１
　　２．保護されるパーソナルデータの範囲 ２３
　　３．パーソナルデータの利活用のルールの内容の在り方 ２６
　　４．パーソナルデータの利活用のルール策定の在り方 ３０
　　５．パーソナルデータの利活用のルールの遵守確保の在り方 ３１
　　６．パーソナルデータの保護のための関連技術の活用 ３２
　　７．国際的なパーソナルデータの利用・流通の確保 ３４
　第２節　パーソナルデータの利活用の枠組みの本格的な実施のための方向性 . . . ３５
　　１．基本的な考え方 ３５
　　２．具体的な方向性 ３５
パーソナルデータの利活用の枠組みの実施のためのアクションプラン ３９
用語解説 ４１
参考資料集 ４７

本報告書の要旨

本報告書は、パーソナルデータ（個人に関する情報）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現のための方向性を提示するものである。同枠組みの本格的な実施のためには、国際的な調和や永続性・安定性の確保といった観点からも、我が国におけるプライバシー・コミッショナー制度（パーソナルデータの保護のための独立した第三者機関）について政府全体として速やかに検討を進めていくことが必要である。また、本報告書では、同枠組みをできるだけ早期に実現するため、制度整備を前提とせずに先行的に実施することが求められる取組についても提示する。

１．パーソナルデータの利用・流通による可能性とその課題

パーソナルデータの利活用については、多くの可能性が期待されている一方、プライバシーの保護等の観点から様々な課題が指摘されている。

パーソナルデータの利活用に関する課題の多くは、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。

２．パーソナルデータの適正な利用・流通の促進に向けた方策

（１）パーソナルデータの利活用の枠組みとその実現に向けて先行的に実施すべき方向性

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、以下のようなパーソナルデータの利活用の枠組み及びその実現に向けて先行的に実施すべき方向性を提示する。

ア　パーソナルデータの利活用の枠組みの体系

（ア）パーソナルデータの利活用の基本理念及び原則の明確化と具体的なルールの設定・運用

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

の基本理念及び原則を明確化し、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る。

（イ）パーソナルデータの利活用の基本理念及び原則

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ある。

①個人情報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。

その上で、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ものとして、次の７項目をパーソナルデータ利活用の原則として提示する。

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

イ　保護されるパーソナルデータの範囲

保護されるパーソナルデータの範囲については、「実質的個人識別性」（プライバシーの保護というパーソナルデータの利活用の基本理念を踏まえて実質的に判断される個人識別性）をメルクマールとして判断する。

ウ　パーソナルデータの利活用のルールの内容の在り方

パーソナルデータの取扱いについては、パーソナルデータのプライバシー性の高低による分類や、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沿わない取扱いである場合の区分に応じて、適正に行うべきである。

一方、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、オプトアウトの意思表示をすることを含む。）ができることとすべきである。

また、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。

エ　パーソナルデータの利活用のルール策定の在り方

パーソナルデータの利活用のルール策定に当たっては、「マルチステークホルダープロセス」（国、企業、消費者、有識者等多種多様な関係者が参画するオープンなプロセス）を、取り扱うパーソナルデータの性質や市場構造等の分野ごとの特性を踏まえ、積極的に活用することとすべきである。

オ　パーソナルデータの利活用のルールの遵守確保の在り方

パーソナルデータ利活用のルールが遵守される仕組みとして、まず、企業が自主的に定めたプライバシーポリシーやマルチステークホルダープロセスを活用して策定されたルールなどパーソナルデータの利活用に関するルールの遵守を契約約款に規定することが考えられる。

また、パーソナルデータの利活用のルールの遵守確保についても、マルチステークホルダープロセスを活用し、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。

カ　パーソナルデータの保護のための関連技術の活用

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 Technologies（PETs））を最大限に有効活用することが適切である。

キ　国際的なパーソナルデータの適正な利用・流通の確保

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、国際会議等の場において、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ある。

また、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。

・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。

（２）パーソナルデータの利活用の枠組みの本格的な実施のための方向性

パーソナルデータの適正な利用・流通の促進に向けて、以下のようなパーソナルデータの利活用の枠組みの本格的な実施のための方向性を提示する。

ア　プライバシー・コミッショナー制度

パーソナルデータの適正な利活用の促進のための体制の整備及び国際的な調和の取れた制度の構築の必要性を踏まえれば、パーソナルデータの利活用に関わる様々な問題について、専門的な知見を有する人材が、パーソナルデータの利活用の基本理念及び原則を実質的に判断して、分野横断的に迅速かつ適切に処理していくことを可能とし、かつ、諸外国の制度とも整合のとれた制度とするため、我が国の実情や法制度を踏まえた、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ことが必要である。

イ　マルチステークホルダープロセス等の実効性確保のための取組

また、企業等が自主的に宣言したポリシー・ルール等への遵守を確保するための制度を整備すべきである。

さらに、マルチステークホルダー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を、上記アのプライバシー・コミッショナー制度と整合する形で整備していくことについて、検討を行うことが必要である。

ウ　その他の制度の整備

その他、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・独立行政法人等・各地方公共団体で規律が異なること、プライバシー保護を実質的に確保するための認証制度の在り方など様々な課題が指摘されている。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、上記ア・イとあわせて、必要な制度整備について検討を行うことが必要である。

第１章　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、位置情報等の様々な情報の蓄積・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を行った。

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、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

---

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　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」（2012 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）。

7 統計法（平成１９年法律第５３号）。

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）が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を行ったものである（第３章第１節２．参照）[11]。

---

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）。

11 なお、本報告書中で諸外国等の制度に関し、「個人データ」の用語を用いている場合があるが、これは原文で“personal data”とされているもので、上記の「パーソナルデータ」の定義と異なる意味で使用されている場合である（なお、諸外国等の用語については参考資料１３参照）。

第２章　パーソナルデータの利用・流通による可能性とその課題

第１節 パーソナルデータの利用・流通の現状と可能性

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」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[12]、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[13]。

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」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[14]。

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～」[15]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々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[16]。

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、今後も技術の発達等とともに、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、本人に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、あるいは本報告書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（第３章第１節５．参照）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。

---

[12] “Personal data is the new oil of the Internet and the new currency of the digital world.”（World Economic Forum, *Personal Data: The Emergence of a New Asset Class* (2011), p.5）

[13] ibid, p.7.

[14] McKinsey & Company, *Big Data: The Next Frontier for Innovation, Competition, and Productivity* (2011) , p.8.

[15] 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～」（２０１２年７月２５日）。

[16] 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）。

第２節　パーソナルデータの利用・流通に関する制度とこれまでの取組

１．我が国の制度とこれまでの取組

（１）個人情報保護法の制定以前からのもの

ア　プライバシーに関する判例

プライバシーについて一般的に規定した法律は存在しないが、判例法理上、プライバシーは法的に保護されるべき人格的利益として承認されてきた。

プライバシー侵害の問題を扱った初期のリーディング・ケースは、「宴のあと」事件（東京地裁昭和３９年９月２８日判決）[17]である。同判決は、プライバシー権を「私生活をみだりに公開されないという法的保障ないし権利」と定義づけ、侵害が認められるための要件を「公開された内容が（イ）私生活上の事実または私生活上の事実らしく受け取られるおそれのあることがらであること，（ロ）一般人の感受性を基準にして当該私人の立場に立った場合公開を欲しないであろうと認められることがらであること，換言すれば一般人の感覚を基準として公開されることによって心理的な負担，不安を覚えるであろうと認められることがらであること，（ハ）一般の人々に未だ知られていないことがらであることを必要とし，このような公開によって当該私人が実際に不快，不安の念を覚えたことを必要とする」としている。

最近ではプライバシー保護の対象となる情報は拡大傾向にあり、例えば、早稲田大学江沢民講演会名簿提出事件（最高裁平成１５年９月１２日第二小法廷判決）[18]では、「学籍番号，氏名，住所及び電話番号は，・・・個人識別等を行うための単純な情報であって，その限りにおいては，秘匿されるべき必要性が必ずしも高いものではない。また，本件講演会に参加を申し込んだ学生であることも同断である。」とした上で、「しかし，このような個人情報についても，本人が，自己が欲しない他者にはみだりにこれを開示されたくないと考えることは自然なことであり，そのことへの期待は保護されるべきものであるから，本件個人情報は，上告人らのプライバシーに係る情報として法的保護の対象となるというべきである。」としている。

イ　地方公共団体の取組

---

17 下民集 15 巻 9 号 2317 頁。
18 民集 57 巻 8 号 973 頁。

個人情報保護に関しては、地方公共団体が独自に個人情報保護条例を早くから制定しており[19]、１９８０年に「プライバシー保護と個人データの国際流通についてのガイドラインに関するＯＥＣＤ理事会勧告（ＯＥＣＤプライバシーガイドライン）」[20]が採択された後は、同ガイドラインを参考に条例が制定されてきた[21]。

ウ　国の取組

公的部門のうち国の行政機関については、１９８８年に「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」[22]が制定された。民間部門については、１９８７年に旧大蔵省所管の財団法人金融情報システムセンター（当時）、１９８９年に旧通商産業省、１９９１年に旧郵政省が、それぞれ所管の事業分野等について、個人情報保護に関するガイドラインを策定した。

（２）個人情報保護法の制定後のもの（参考資料２参照）

ア　個人情報保護法の制定

２００３年５月に個人情報保護法が制定され、２００５年４月に全面施行された。同時に行政機関個人情報保護法（行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律を全面的に改正）や独立行政法人等個人情報保護法も制定・施行された。また、２００４年４月に個人情報保護法に基づき「個人情報の保護に関する基本方針」が閣議決定された。

個人情報保護法においては、その監督・執行について専門的な独立した第三者機関のようなものを設置することとはされず、各事業等を所管する大臣が主務大臣として監督・執行を行うという主務大臣制がとられている。

イ　各行政機関の取組

（ア）総務省

---

19 日本においては、1970 年代半ばから地方公共団体で個人的秘密等を保護する条例が制定されるようになった。

20 OECD, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*(1980).

21 なお、2013 年１月現在では、全ての普通地方公共団体（1719 団体）で個人情報保護条例が制定されている。

22 昭和 63 年法律第 95 号。

① 個人情報保護ガイドラインの策定・改正

２００５年の個人情報保護法の全面施行等を受け、１９９１年に策定された「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」を改正し、さらに、２００９年[23]、２０１０年、２０１１年にも改正した。

また、「放送受信者等の個人情報の保護に関する指針」を２００４年に策定、２００９年に改正し、「郵便事業分野における個人情報保護に関するガイドライン」を２００８年に策定、２０１２年に改正し、「信書便事業分野における個人情報保護に関するガイドライン」を２００８年に策定した。

② 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

２００９年４月に「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」を開催し、２０１０年５月にライフログ活用サービスの発展を妨げずに利用者の不安感等を緩和する方策について「配慮原則」の提示等を行う「第二次提言」を公表し（参考資料３参照）、２０１２年８月にスマートフォンの利用者情報の取扱いに関する包括的な対策について「スマートフォン利用者情報指針」の提示等を行う「スマートフォン プライバシー イニシアティブ」（参考資料４参照）を公表した。

（イ）消費者庁・消費者委員会（２００９年９月発足）

消費者庁では、「個人情報の保護に関する基本方針」に基づき、法制度の周知徹底等を図るとともに、個人情報保護法の施行状況について消費者委員会に報告を行っており、同委員会は、そのフォローアップ等を行っている。また、消費者庁は同基本方針に基づく大規模な個人情報の漏えい等個別の事案が発生した際の対応事例の蓄積・整理・情報提供等や、個人情報保護法の施行状況の消費者委員会への報告と公表、個人情報の保護に関する国際的な取組への対応、各省庁及び地方公共団体の苦情相談機関等の窓口等に関する情報の収集・整理・提供、その他個人情報の保護に関する情報収集・調査研究の推進等について、各省庁の協力を得て取りまとめ等を行っている。

（ウ）その他の省庁の取組

[23] 2008 年 7 月 25 日個人情報保護関係省庁連絡会議申合せ「個人情報保護に関するガイドラインの共通化について」を踏まえて改正された。

個人情報保護法が全面施行された２００５年度には、２１分野３３ガイドラインが策定されている（前記（ア）①の総務省のものを含む。）。２００８年の「個人情報保護に関するガイドラインの共通化について」[24]の申合せにより、ガイドラインの名称の共通化等の形式的な整理等がなされた。それ以降も新たなガイドラインの策定・改正が行われており、２０１２年３月３１日現在、２７分野４０ガイドラインが策定されている[25]。

ウ　番号法案（参考資料５参照）

政府は、「社会保障・税番号大綱」[26]に基づき、２０１２年２月に「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」（旧番号法案）を閣議決定し、第１８０回通常国会に提出したが、同国会では継続審議となり、同年１０月召集の臨時国会で衆議院解散に伴い、廃案となった。なお、旧番号法案では、内閣府設置法第４９条（国家行政組織法第３条に相当する規定）の規定に基づく、公正取引委員会等と同様のいわゆる三条委員会（独立行政委員会）として、番号制度における個人情報の保護を所掌とする「個人番号情報保護委員会」を設置することとされていた。

その後、２０１３年３月に同名の「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」（新番号法案）が閣議決定され、第１８３回通常国会に提出された（参考資料５参照）。新番号法案では「個人番号情報保護委員会」の名称を「特定個人情報保護委員会」に改めるとともに、同委員会の権限として特定個人情報（個人番号をその内容に含む個人情報）と共に管理されている特定個人情報以外の個人情報の取扱いに関する指導・助言を加える（同法案第５０条後段）等の修正が行われた。また、新番号法案で追加された同法案附則第６条第２項では、法施行（公布後３年以内）後１年を目途として特定個人情報保護委員会の権限に特定個人情報以外の個人情報の取扱いに関する監視又は監督を追加することについて検討を加えること等を定めている[27]。

２．諸外国等の制度とこれまでの取組

（１）米国

---

24 前掲脚注 23 参照。
25 消費者庁「平成 23 年度　個人情報の保護に関する法律施行状況の概要」。
26 2011 年６月 30 日 政府・与党社会保障改革検討本部決定。
27 新番号法案は一部修正（上記の事項に修正はない。）の上、2013 年５月９日に衆議院で可決された。

ア　パーソナルデータ保護に関する制度（参考資料６参照）

米国ではパーソナルデータの保護に関し、分野横断的な法律は存在せず、分野ごとの個別法と自主規制を基本とするものとなっている。

米国のパーソナルデータの保護については、独立行政委員会であるＦＴＣ（Federal Trade Commission:連邦取引委員会）が大きな役割を果たしており、自主規制の遵守についての監督、排除措置、課徴金の附課等の執行措置等を行う他、下記イのような政策提言を活発に行うとともに、後記（４）のような国際的な場でも活発な活動を行っている（参考資料１６及び１７も参照）。

イ　消費者プライバシー権利章典等最近の動向

２０１２年２月、ホワイトハウスにより政策大綱「ネットワーク化された世界における消費者データプライバシー」が発表された。同政策大綱では「消費者プライバシー権利章典」が提示された（参考資料７参照）。

また、同政策大綱の発表後、ＦＴＣは、２０１２年３月、消費者データを収集し利用する企業の行動枠組みについてまとめた報告書である「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」[28]を発表した（参考資料８参照）。

（２）ＥＵ（参考資料９参照）

ア　現行制度

（ア）データ保護指令

欧州では、１９９５年、分野横断的にパーソナルデータ保護に関し、「個人データの取扱いに係る個人の保護及び当該データの自由な移動に関する１９９５年１０月２４日の欧州議会及び理事会の９５／４６／ＥＣ指令」[29]が採択され、加盟国は当該指令を遵守するために必要な国内法の整備を義務づけられた。

同指令第２８条は、各加盟国にデータ保護のための独立した監督機関の設置を義務づけている。これに基づき各国で設置されたデータ保護機関（Data

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

[29] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Protection Authority（ＤＰＡ）[30]）が、各国内でパーソナルデータ保護の監督や後記（４）のような国際的な場で活動を行うとともに、同指令第２９条に基づき全加盟国の監督機関が構成する機関（第２９条作業部会（Article29Working Party）と呼ばれる。）が政策提言等の積極的な活動を行っている。

また、同指令第２５条は、ＥＵ域内から第三国への個人データの移転は、原則として第三国が十分なレベルの保護措置を確保していることを条件としているが（参考資料９－２参照）、上記の第２９条作業部会は、その「十分なレベルの保護措置」の要素の１つとして、「独立した機関の形態をなす外部監督の制度」をあげている[31, 32]。

（イ） ｅプライバシー指令

上記（ア）の分野横断的なデータ保護指令に加え、電子通信部門におけるパーソナルデータ保護に関する特則を規定するものとして、２００２年に「電子通信部門における個人データの処理とプライバシーの保護に関する２００２年７月１２日の欧州議会及び理事会の２００２／５８／ＥＣ指令」[33]が採択され、加盟国は当該指令を遵守するために必要な国内法の整備を義務づけられた[34]。

イ　データ保護規則提案（参考資料１０参照）

２０１２年１月、欧州委員会は「データ保護指令」を抜本的に改正する「個人データの取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の規則（一般的データ保護規則）の提案」[35]を欧州議会及び欧州理事会に提案・公表した。

---

30 英国・情報コミッショナー、フランス・情報処理及び自由に関する国家委員会、ドイツ・連邦データ保護・情報自由監察官など（参考資料 16 参照）。

31 Working Party on the Protection of individuals with regard to the Processing of Personal Data, *Working Document：Transfers of personal data to third countries：Applying Article 25 and 26 of the EU Data Protection Directive*（24 July 1998）.

32 消費者庁「個人情報保護制度における国際的水準に関する検討委員会報告書」（2012 年３月）７頁～９頁参照。

33 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

34 なお、本指令は、2009 年に一部改正され、Cookie の利用に当たって内容を明示しオプトインによる利用者同意を求めること等が規定された。

35 前掲脚注２。

同規則提案においても、各加盟国に独立した監督機関の設置を義務づけていることやＥＵ域内から第三国への個人データの移転は原則として第三国が十分なレベルの保護措置を確保していることを条件としていることは、現行のデータ保護指令と同様である。なお、同規則提案においては、「十分なレベルの保護措置」の要素の１つとして、独立した監督機関の存在及びそれが効果的に機能していることが明記されている（同規則提案第４条第２項（ｂ））。

（３）その他の地域

パーソナルデータの保護については、欧米諸国等の先進国で先行的に制度が整備されてきたが、他の地域においても徐々に整備が進められ、現在では大半の国でパーソナルデータ保護に関する法律が制定されるに至っており、そのうち多くの国でパーソナルデータの保護のための独立した第三者機関が設置されている[36]。

（４）国際機関等

ア　ＯＥＣＤ（Organisation for Economic Co-operation and Development：経済協力開発機構）

（ア）ＯＥＣＤプライバシーガイドラインとその改正

１９８０年、ＯＥＣＤ理事会はＯＥＣＤ加盟国に対し「プライバシー保護と個人データの国際流通についてのガイドライン」（ＯＥＣＤプライバシーガイドライン）について、勧告を行った[37]。同ガイドラインは、プライバシー保護・個人の自由と個人データの自由な流通の実現の双方のバランスを図り、個人データの取扱いに関する原則（ＯＥＣＤ８原則（参考資料１２参照））などを示したものである。

なお、同ガイドラインについては、現在、改正作業が進められている。

---

[36] オーストラリア・ニューサウスウェールズ大学のグレアム・グリーンリーフ教授によれば、2012年1月現在で94カ国・地域で、パーソナルデータの保護に関する法律が制定されており、そのうちヨーロッパ以外で同教授が調査した33カ国・地域のうち、カナダ、ニュージーランド、オーストラリア、韓国、香港、マレーシア等の25カ国・地域でパーソナルデータの保護のための独立した第三者機関が設置されている（Graham Greenleaf ,*Japan's data privacy laws compared with laws in other Asian countries, and globally*(2012)）。

[37] 前掲脚注20。

（イ）ＧＰＥＮ（Global Privacy Enforcement Network：グローバルなプライバシーの執行に係るネットワーク）

プライバシー保護法の執行に係る越境協力に関するＯＥＣＤ勧告（２００７年６月１２日採択）[38]を受け、プライバシー保護法の越境執行の協力を支援・促進するため、世界のプライバシー保護の執行機関が連携することを目的に、２００８年より執行問題や傾向、経験を議論する定期的な会合等を開催している[39]。

イ　ＡＰＥＣ（Asia Pacific Economic Cooperation：アジア太平洋経済協力）

（ア）ＡＰＥＣプライバシーフレームワーク

ＡＰＥＣプライバシーフレームワークは、ＡＰＥＣにおけるパーソナルデータの保護の原則（参考資料１２参照）を定める枠組みである。２００４年にＡＰＥＣ貿易・投資委員会（Committee on Trade and Investment（ＣＴＩ））傘下の電子商取引運営グループ（Electronic Commerce Steering Group（ＥＣＳＧ））がとりまとめ、同年１１月にＡＰＥＣ閣僚会議で承認された。

（イ）ＣＰＥＡ（Cross Border Privacy Enforcement Arrangement：越境プライバシー執行協力）

ＣＰＥＡは、パーソナルデータが国境を越えて委託、移転、共有等されているときに、国境を越えた先での漏えい等があった場合、移転元エコノミー（国・地域）における執行機関が、自エコノミーにおけるパーソナルデータ保護法令の執行のために、移転先エコノミーにおける執行機関に対し、情報

---

[38] OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy(2007). 同勧告の主な内容は、①他国の執行機関と協力できるようにするため、プライバシー保護法を執行するための国内の枠組みを改善すること②国境を越えたプライバシー保護法の執行協力を容易にするために有効な国際的な仕組みを開発すること③通知、苦情付託、調査支援及び情報共有を通して行うことを含む相互支援を提供すること④プライバシー保護法の執行協力の促進を目的とした議論及び活動に、関連する利害関係者を参加させることとされている。※プライバシー保護法とは、国内法又は規則のことであって、その執行が、個人データを保護する効果を持ち、OECD プライバシーガイドラインに準拠したもの。

[39] オーストラリア、カナダ、中国、フランス、ドイツ、イスラエル、イタリア、韓国、メキシコ、オランダ、ニュージーランド、スペイン、英国、米国等 24 ヶ国及び EU のデータ保護当局等が参加している（日本は未参加）。

の提供、調査等協力を依頼するための枠組みである[40]。２００９年１１月にＡＰＥＣ閣僚会議で承認された。

（ウ）ＣＢＰＲ制度（Cross-Border Privacy Rules System：越境プライバシールール制度）

ＣＢＰＲ制度は、ＡＰＥＣプライバシーフレームワークへの適合性を国際的に認証する制度である。２０１１年１１月にＡＰＥＣ閣僚会議で承認された。

ＣＢＰＲ制度に参加するためには、①ＣＰＥＡに参加する、②エコノミーとしてＣＢＰＲ制度へ参加する、③エコノミーが認証機関を登録するとの３つの手続を踏む必要がある。ＣＰＥＡの参加エコノミーのうち、米国及びメキシコが②の手続を済ませている（③の手続を済ませたエコノミーはまだない（米国が申請中）。（２０１３年５月現在））

ウ　データ保護プライバシー・コミッショナー国際会議（International Conference of Data Protection and Privacy Commissioners）

データ保護プライバシー・コミッショナー国際会議は、１９７９年から毎年開催されている会合で、アルゼンチン、オーストラリア、カナダ、フランス、ドイツ、ギリシャ、アイスランド、イスラエル、イタリア、メキシコ、モロッコ、オランダ、ニュージーランド、ノルウェー、ペルー、韓国、英国、ウルグアイ、米国等５７ヶ国のパーソナルデータの保護機関がメンバーとして参加している（２０１２年現在）。日本からはメンバーとして正式な参加が認められている機関はなく、消費者庁にオブザーバー資格が認められているのみである。

同会議では、各国のパーソナルデータの保護機関により、パーソナルデータに関する様々な課題についての議論等が行われている。

なお、同会議の参加資格は以下を満たすパーソナルデータの保護機関とされている[41]。

① 法的文書に基づき設置された公的な機関であること。

② パーソナルデータ又はプライバシー保護に関する法律の実施の監督を行うものであること。

---

40 現在の参加国はオーストラリア、カナダ、香港、日本、韓国、メキシコ、ニュージーランド、米国の８カ国・地域。

41 同会議の参加資格を認証するための手続及び基準は、2001 年のフランスでの会合で初めて文書として定められ、何度か改正された後、2010 年のイスラエルでの会合で現在の形に改正されている（データ保護プライバシー・コミッショナー会議・理事会規則：Executive Committee：Rules and Procedures.）。

③　運用する法律がデータ保護又はプライバシーに関する中心的な国際的な文書と整合的であること。
④　その機能を実行するため適切な範囲の法的な権限を有していること。
⑤　適切な自律性と独立性を有していること。

エ　ＡＰＰＡ（Asia Pacific Privacy Authorities：アジア太平洋プライバシー機関）

ＡＰＰＡは、アジア太平洋地域のパーソナルデータの保護機関がメンバーとして参加し、パーソナルデータに関する様々な課題についての議論等を行っている組織であり、１９９２年の発足以降、年２回のフォーラムを開催している。
２０１２年現在、オーストラリア、カナダ、香港、マカオ、ニュージーランド、韓国、米国のパーソナルデータの保護機関がメンバーとして参加している（日本からは消費者庁がオブザーバーとして参加）。
なお、ＡＰＰＡの参加資格は以下のいずれかを満たすパーソナルデータの保護機関とされている。
①　データ保護プライバシー・コミッショナー国際会議のメンバーであること。
②　ＡＰＥＣ・ＣＰＥＡに参加していること。
③　ＯＥＣＤ・ＧＰＥＮに参加していること。

オ　欧州評議会（Council of Europe（ＣｏＥ））

欧州評議会はＥＵ全加盟国、旧ユーゴスラビア諸国、ロシア、ウクライナ、トルコ等の４７ヶ国が加盟する国際機関である。なお、日本は欧州評議会のオブザーバー国となっている[42]。
欧州評議会の閣僚委員会は１９８０年に「個人データの自動処理に係る個人の保護に関する条約（条約第１０８号）」（欧州評議会条約第１０８号）[43]を採択した。同条約は、ＯＥＣＤプライバシーガイドラインとほぼ同様なデータ保護の基本的原則を示したものである。同条約は欧州評議会非加盟国であっても

[42] オブザーバー国は原則閣僚委員会以外の会合、専門家委員会に参加することが可能であり、投票権はないが発言権を有している。また、欧州評議会からの招待があれば、部分協定や拡大協定会合等への参加が可能である。2013 年４月現在、オブザーバー国は日本、米国、カナダ、メキシコ及びバチカンの全５か国である（外務省 HP「欧州評議会（Council of Europe）の概要」（http://www.mofa.go.jp/mofaj/area/ce/gaiyo.html）より）。
[43] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention108).

参加が可能であり（同条約第２３条）、２０１３年５月現在で欧州評議会非加盟国のウルグアイを含む４５カ国が同条約を締結している。

さらに、２００１年に「個人データの自動処理に係る個人の保護に関する条約への監督機関及び越境データ流通についての追加議定書」（欧州評議会条約第１０８号追加議定書）[44]が採択された。同追加議定書は３か条からなるもので、独立した監督機関の設置、締約国以外の国への個人データの移転の制限等について定めている。欧州評議会条約第１０８号を締結した国は、欧州評議会非加盟国であっても同追加議定書に参加が可能であり（同追加議定書第３条）、２０１３年５月現在で欧州評議会非加盟国のウルグアイを含む３４カ国が同追加議定書を締結している。

カ　ＩＳＯ（International Organization for Standardization：国際標準化機構）、ＩＥＣ（International Electrotechnical Commission：国際電気標準会議）

ＩＳＯは、電気及び電子技術分野を除く全産業分野に関する国際規格の作成を行う国際標準化機関であり、ＩＥＣは、電気及び電子技術分野の国際規格の作成を行う国際標準化機関である。ＩＳＯとＩＥＣの合同の専門委員会であるＪＴＣ１の傘下のＳＣ２７／ＷＧ５が、アイデンティティ管理及びプライバシー技術を担当している[45]。

２０１１年に、プライバシーに関する共通的な用語の特定、PII（personally identifiable information：個人識別可能情報）の処理に関する関係者及びその役割の定義等を示すISO/IEC 29100:2011 Privacy framework が規格化された。

第３節　パーソナルデータの適正な利用・流通の促進に向けた課題

パーソナルデータの利活用については、第１節で記載したとおり、多くの可能性が期待されている一方、プライバシーの保護等の観点からの様々な課題も指摘されており、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[46]。

---

44 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows.

45 JTC（Joint Technical Committee）１は、ISO と IEC 合同の専門委員会の１つで、IT 分野の標準化をするために 1987 年に ISO と IEC の合同で設立された。JTC1 の傘下には 18 の分科会（SC：Subcommittee）等があり、そのうち SC27 は IT セキュリティ技術を担当している。SC27 には５つの WG（Working Group）があり、そのうち WG５がアイデンティティ管理とプライバシー技術を担当している。

46 例えば、スマートフォンの利用者情報の問題に関しては、前掲脚注１の資料の１４頁参

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[47]。

パーソナルデータの利活用に関する課題の多くは、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。

パーソナルデータの利活用において、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。

そして、パーソナルデータの利活用のうち、プライバシー等に係る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ることから、パーソナルデータの利活用に係る仕組み全体で適正な取扱いを確保する必要がある。

また、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・独立行政法人等・各地方公共団体で規律が異なること、プライバシー保護を実質的に確保するための認証制度の在り方など様々な課題が指摘されている[48]。

本報告書は、上記を踏まえ、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、次章において、

照。

47 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。

48 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～」（２０１１年７月）参照。

パーソナルデータの利活用の枠組み及びその実現のための方向性を提示するものである。同枠組みの本格的な実施のためには、国際的な調和や永続性・安定性の確保といった観点からも、我が国におけるプライバシー・コミッショナー制度（パーソナルデータ保護のための独立した第三者機関）について政府全体として速やかに検討を進めていくことが必要である。また、本報告書では、同枠組みをできるだけ早期に実現するため、同章第１節においては、制度整備を前提とせずに先行的に実施することが求められる取組についても提示する。

第３章　パーソナルデータの適正な利用・流通の促進に向けた方策

第１節　パーソナルデータの利活用の枠組みとその実現に向けて先行的に実施すべき方向性

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現に向けて先行的に実施すべき方向性を提示することとする。

１．パーソナルデータの利活用の枠組みの体系

（１）基本的な考え方

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重要な要素の一つである。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である。

また、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となる。

こうしたことから、新事業創出において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である。

その際、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がある。

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もある。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である。

（２）具体的な方向性

ア　パーソナルデータの利活用の基本理念及び原則の明確化と具体的なルールの設定・運用

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基本理念及び原則を明確化し、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ある。

イ　パーソナルデータの利活用の基本理念及び原則

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ある。

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[49]。

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[50]。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[51]。

その上で、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ものとして、本報告書では、次の７項目をパーソナルデータ利活用の原則として提示する（参考資料１２参照）。

・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経緯（コン

---

[49] 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（前掲脚注２。）。

[50] 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≫』（2005 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。

[51] 2011 年６月に公表された「社会保障・税番号大綱」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。

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。

・プライバシー・バイ・デザイン[52]

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。

ウ　パーソナルデータの利活用の具体的なルールの設定・運用

パーソナルデータの利活用の具体的なルールは、上記イで述べたパーソナルデータの利活用の基本理念及び原則を踏まえこれらを実質的に確保するという観点で策定されるべきものであり、その内容及び策定の在り方については、後記３．及び４．で述べることとする。

また、パーソナルデータの利活用の具体的なルールの運用・解釈についても、パーソナルデータの利活用の基本理念及び原則を指針としてこれを実質的に確保するという観点で行われるべきである。

２．保護されるパーソナルデータの範囲

（１）基本的な考え方

パーソナルデータの利活用の枠組みにおいて、保護されるパーソナルデータの範囲については、プライバシーの保護というパーソナルデータの利活用の基本理念を踏まえて考えるべきである。

その際、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する必要がある。

なお、パーソナルデータが、ここでいう「保護されるパーソナルデータ」に

---

[52] 参考資料１１参照

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[53]があることに留意が必要である。

（２）具体的な方向性

一般的に、パーソナルデータの利活用に関し、プライバシーが問題になるのは、当該パーソナルデータと特定の個人の結びつきが強い場合である。そして、パーソナルデータと特定の個人の結びつきが強い場合とは、当該パーソナルデータについて当該特定個人を識別する蓋然性がある場合と考えられる。

また、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（第１章参照）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である（諸外国や国際機関等では、「識別された又は識別可能な個人（identified or identifiable individual）に関する情報」と定義している例が多い。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。）（参考資料１３参照）。

したがって、保護されるパーソナルデータの範囲については、現行の個人情報保護法と同様に、個人識別性を有するものとすることが、基本的には妥当であると考えられる。

しかしながら、具体的に個人識別性の該当性について判断し、保護されるパーソナルデータの範囲を画定するに当たっては、プライバシーの保護というパーソナルデータの利活用の基本理念を踏まえて実質的に判断することが必要であると考えられる。ここで、プライバシーの保護というパーソナルデータの利活用の基本理念を踏まえて実質的に判断される個人識別性を、概念上明確にするため、「実質的個人識別性」と呼ぶこととする[54]。

実質的個人識別性について判断する際には、取得等の際に特定の個人が識別

---

53 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。

54 なお、個人情報保護法の「個人情報」の要件である個人識別性も「特定の個人を識別することが『できる』」として蓋然性・可能性を要件として規定されており（諸外国等のidentifi[able]、link[able]なども同様。）、その該当性判断に当たっては法の趣旨に従って判断することが必要となるため、同様の実質的な判断を行うことは文言上は排除されてないと考えられる。しかしながら、現行の個人情報保護法の「個人情報」の範囲と本報告書の「保護されるパーソナルデータ」の範囲の関係及び両者に相違がある場合の適切な取扱いの在り方等については、これまでの解釈・運用（各省庁の個人情報保護ガイドライン等）との関係の整理等も踏まえ、引き続き検討していくことが必要であると考えられる。

されなかったとしても、他のパーソナルデータとあわせて分析されること等により、特定の個人が識別される可能性があることについて、十分に配慮する必要がある。

他方、実質的個人識別性を有する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[55]。

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装置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、プライバシーの保護という基本理念を踏まえて判断すると、実質的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の範囲に含まれると考えられる。

なお、ＩＰアドレス、クッキーについては、必ずしも全ての場合に継続的に特定の装置を識別するものではないことから、全ての場合において保護されるパーソナルデータの範囲に含まれるものではなく、一般的には、他の保護されるパーソナルデータと連結する形で取得・利用される場合に、実質的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の範囲に含まれると整理されるべきものと考えられる。しかしながら、ＥＵのｅプライバシー指令が、全てのクッキーをその規律の対象としていることなども踏まえ、更に検討していく必要があると考えられる。

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、仮に氏名等の他の実質的個人識別性の要件を満たす情報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[56]、特定の個人を識別することができるようになる蓋然性が高く、プライバシーの保護という基本理念を踏まえて判断すると、実質的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の範囲に含まれると考えられる。

他方、例えば、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、実質的個人識別性はないといえることから、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[57,58]。なお、どのような状態になれば、再識

---

55 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。

56 なお、他の実質的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、それにより実質的個人識別性の要件を満たすこととなるため、保護されるパーソナルデータに当たることとなる。

57 同上。

別化を不可能又は十分に困難にしたものであるといえるかについては、その考え方を整理し、提示していく必要がある。

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、後記６．（２）のとおり、適切なセーフガードを設定すれば、実質的個人識別性はないといえるため、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できると考えられる[59]（後記５．参照）。

３．パーソナルデータの利活用のルールの内容の在り方

（１）基本的な考え方

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、そのプライバシー性の高低に応じて適正に取り扱うことが必要である。

また、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、適切な在り方を考えるべきである。

さらに、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である。

（２）具体的な方向性

ア　パーソナルデータのプライバシー性の高低による分類

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て適正に取り扱うべきである。

---

[58] 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。

[59] 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、実質的個人識別性の要件を満たすことになるから、保護されるパーソナルデータとなると考えられる。

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）
②慎重な取扱いが求められるパーソナルデータ
（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いもの。
一般パーソナルデータ又はセンシティブデータ以外の保護されるパーソナルデータ）
③センシティブデータ
（保護されるパーソナルデータのうちプライバシー性が極めて高いもの）

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。
・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。なお、慎重な取り扱いが求められるパーソナルデータについては、情報により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（後記イ参照）。
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[60]
・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１４参照）、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。
・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

[60] 前掲脚注１の資料の６１頁参照。

・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

また、金融・財産情報については、ＥＵ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ではセンシティブデータとされていないものの、他人に知られたくないという意味でプライバシー性が相当程度高い情報であるといえることから、我が国の実情に照らしてセンシティブデータに含まれるとすることについて、更に検討していくべきと考えられる。

イ　パーソナルデータの取扱いの在り方

パーソナルデータの取扱いについては、アで述べたパーソナルデータのプライバシー性の高低による分類や、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沿わない取扱いである場合の区分に応じて、適正に行うべきである。

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と考えられる[61]。

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と考えられる。

なお、ここで、「個別的」な同意とは、画面上でのクリックなど特定のパーソナルデータについての特定の取扱いについての同意であることを本人が認識した上で行うことを前提とした同意を意味し、「包括的」な同意（契約約款による同意など本人が特定のパーソナルデータについての特定の取扱いについて認識することは必ずしも前提としていない同意）の反対概念と整理している。また、「明示的」な同意とは、画面上でのクリックや文書による同意など外部的に同意の事実が明確である同意を意味し、状況により同意の意思が推測される場合の「黙示」の同意の反対概念として整理している。

また、慎重な取扱いが求められるパーソナルデータの取扱いの在り方については、以下のように整理できるのではないかと考えられるが、その具体的な在り方（どのような情報がプライバシー性が比較的低く、どのような情報がプライバシー性が比較的高いと考えるべきか等）については、具体的な利活用状況に即して今後更に検討していく必要があると考えられる。

---

61 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）。

	取得の際の経緯（コンテキスト）に沿う取扱いをする場合	取得の際の経緯（コンテキスト）に沿わない取扱いをする場合
慎重な取扱いが求められるパーソナルデータ	【プライバシー性が比較的低いもの】 明示的かつ包括的な同意	明示的かつ個別的な同意
	【プライバシー性が比較的高いもの】 明示的かつ個別的な同意	

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、今後その具体的な在り方について検討していく必要がある[62]。

一方、パーソナルデータの本人は、原則として[63]、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[64]の意思表示をすることを含む。）ができることとすべきである。

なお、この場合の同意の撤回の効果については、それ以後のパーソナルデータの取扱いの停止を求めるものであって、それ以前のパーソナルデータの取扱いを違法・不当なものとするものではないと考えることが適当である。

また、パーソナルデータを利用する者には、パーソナルデータ利活用の原則として提示した項目である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。

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、

---

62 個人情報保護法第 16 条第 3 項及び第 23 条第 1 項は、以下の場合を、利用目的による制限及び第三者提供の制限の適用除外として規定している。
①法令に基づく場合
②人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
③公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
④国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

63 例外としては、契約により同意の撤回が制限される場合などが考えられる。

64 事後的に取扱いの停止を求めること。

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[65]。

その際、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。この点については、総務省「スマートフォン プライバシー イニシアティブ」[66]などで、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、「スマートフォン プライバシー イニシアティブ」についてはこれを踏まえた業界団体によるガイドラインが策定される等の取組も既に行われているところ（参考資料１５参照）、適切な表示の在り方等について、実証実験等を通じ、更に検討を進めていくべきである。

４．パーソナルデータの利活用のルール策定の在り方

（１）基本的な考え方

パーソナルデータの利活用のルール策定に当たっては、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等を考慮し、「マルチステークホルダープロセス」（国、企業、消費者、有識者等多種多様な関係者が参画するオープンなプロセス）を、取り扱うパーソナルデータの性質や市場構造等の分野ごとの特性を踏まえ、積極的に活用することとすべきである。

（２）具体的な方向性

マルチステークホルダープロセスを活用する際には、情報通信、医療・介護など分野ごとの特性を踏まえ、ルール策定の対象・範囲を適切に設定することが必要である[67]。

その際、マルチステークホルダープロセスにおける国の役割は、参加者による適切かつ円滑な合意形成を促す観点から、マルチステークホルダープロセス

---

65 前掲脚注１の資料。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。

66 前掲脚注１の資料の６４頁参照。

67 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。

の場の提供、ルール策定の対象・範囲の設定、パーソナルデータの利活用の原則から求められるルールの内容の提示、議論の方向性及び結論がパーソナルデータの利活用の基本理念及び原則に沿ったものであることの検証などとすることが適切である。

また、マルチステークホルダープロセスに参加する企業等においては、同プロセスを活用して策定されたルールを遵守することで、プライバシーの保護に配慮し、適正にパーソナルデータを利活用していることが明確となり、同企業等に対する国民・消費者の信頼醸成につながることが期待される。このため、同プロセスを活用し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・消費者に周知する等の活動を推進していくことが必要である。

なお、マルチステークホルダープロセスが円滑に進むよう、今後発展が期待されるセクターを選定し、実証実験等を通じた、具体的なケーススタディを推進していくことが必要である。

５．パーソナルデータの利活用のルールの遵守確保の在り方

（１）基本的な考え方

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である。

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である。

（２）具体的な方向性

パーソナルデータの利活用のルールが遵守される仕組みとして、まず、企業が自主的に定めたプライバシーポリシーや、前記４．のマルチステークホルダープロセスを活用して策定されたルールなどパーソナルデータの利活用に関するルールの遵守を契約約款に規定することが考えられる。

また、パーソナルデータの利活用のルールの遵守確保についても、マルチステークホルダープロセスを活用し、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。

さらに、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あると考えられる。

なお、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行っていくべきである。

６．パーソナルデータの保護のための関連技術の活用

（１）基本的な考え方

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 Technologies（PETs））を最大限に有効活用することが適切である。

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である。

（２）具体的な方向性

暗号化技術については、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ある。

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いないことが確実である場合には、漏えいしたデータを他の分散データと組み合わせ復号した場合に保護されるパーソナルデータとなるものが含まれているとしても、当該漏えいしたデータのみでは有意な情報がないことから、実質的影響はないものとして捉えることが可能である[68]。

匿名化技術については、前記２.（２）のとおり、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、実質的個人識別性はないといえることから、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。なお、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と考えられる（前記２.

[68] 電気通信事業における個人情報保護に関するガイドライン第 22 条第１項第２項及びその解説参照。

参照）。

一方、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における考え方[69]等を踏まえ、次のような条件をすべて満たす場合は、実質的個人識別性はないといえるため、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できると考えられる。

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ある。

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の担保措置についても検討する必要があると考えられる[70]。

なお、暗号化技術、匿名化技術については、より高度化・実用化に向けた研究開発を支援するととともに、情報漏えいや再識別化等によるプライバシーインパクトを考慮し、実態上問題が生じないと考えられる状態についての共通的な理解の醸成、鍵管理や再識別化の防止措置を含む運用に関するガイドラインや事例集の作成等を推進すべきである[71]。

---

69 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（前掲脚注 28 の 22 頁参照）。

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（前掲脚注 28 の 22 頁脚注 113。）。

70 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。

71 EU のデータ保護指令の前文（26）及びデータ保護規則提案の前文（23）は、「データ保護の原則は、データ主体がもはや識別可能でないような方法で匿名化されたデータには適用するべきでない」としている。

また、英国の情報コミッショナー事務局（Information Commissioner's Office（ICO））は 2012 年 11 月に個人データを適切に匿名化するための考え方やケースを示すガイドライン（Anonymisation: managing data protection risk code of practice）を公表している。さらに、オーストラリア情報コミッショナー事務局（Office of the Australian Information

その他の関連技術として、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ある。

また、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に向けた取組の推進を働きかけていくべきである。

７．国際的なパーソナルデータの適正な利用・流通の確保

（１）基本的な考え方

国際的なパーソナルデータの適正な利用・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である。

なお、本節で示す先行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、次節で述べる本格的な対応が不可欠であると考えられる。

（２）具体的な方向性

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、国際会議等の場において、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ある。

また、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。

- 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。

Commissioner）は 2013 年４月に非識別化に関する諮問文書案（De-identification of data and information consultation draft April 2013）を公表している。

第２節　パーソナルデータの利活用の枠組みの本格的な実施のための方向性

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、前節で提示したパーソナルデータの利活用の枠組みの本格的な実施のための方向性を提示することとする。

１．基本的な考え方

前節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制度的な取組が必要不可欠である。

これらの制度的な取組が必要なものについては、政府全体として速やかに検討を進めていくことが必要である。

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、世界最高水準のＩＣＴ社会の実現、我が国の経済成長にも寄与することとなると考えられる。

２．具体的な方向性

（１）プライバシー・コミッショナー制度

ア　パーソナルデータの適正な利活用の促進のための体制の整備

パーソナルデータの適正な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、絶え間ない技術革新の中で、パーソナルデータの利活用の基本理念及び原則を実質的に確保する観点から、パーソナルデータの利活用のルールの明確化が適切かつ迅速に行われ、ルール適用の予見性・透明性が確保される仕組みが必要である。

また、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、さらに、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、事前の相談や事後の紛争解決などに当たり、迅速かつ柔軟な判断が求められる。

こうした機能を適切に果たしていくためには、パーソナルデータの利活用に関わる様々な問題について、専門的な知見を有する人材を集め、パーソナルデータの利活用の基本理念及び原則を実質的に判断して、分野横断的に迅速かつ

適切に処理していく体制の整備が必要不可欠である。

イ　国際的な調和の取れた制度の構築

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であり、特に、クラウドサービス、検索サービス、ＯＴＴ[72]サービスなど、国境を越えて提供されるサービス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である。

国際的に見ると、パーソナルデータの保護については、国によりその根拠法令や機関の構成・性質等に違いはあるものの、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、欧米諸国等の先進国をはじめとして多数である。米国においては、独立行政委員会であるＦＴＣが、主としてパーソナルデータの保護の監督を行っている。また、ＥＵ諸国においては、ＥＵのデータ保護指令及び各国の国内法に基づき各国が設置するデータ保護のための独立した監督機関であるデータ保護機関（ＤＰＡ）が、パーソナルデータの保護の監督を行っている。さらに、その他の地域においても、多くの国でパーソナルデータの保護のための独立した第三者機関が設置されている（第２章第２節２.、参考資料１６参照）。

そして、このような各国における体制を背景として、パーソナルデータの利活用については、国際的に、各国のプライバシー・コミッショナーが政策について意見を表明し、調整を行う体制が形成されている[73]。

また、パーソナルデータの国際的な流通については、ＥＵがＥＵ域内から第三国への個人データの移転は原則として第三国が十分なレベルの保護措置を提供していることを条件としているが（第２章第２節２.（２）ア（ア）参照）、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（参考資料９－２参照。ＥＵ・米国間のセーフハーバー枠組みについては、参考資料６参照）、ＥＵ・日本の間では、ＥＵは日本

[72] Over The Top の略。OTT サービス：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。

[73] 例えば、2011 年 11 月に開催されたデータ保護プライバシー・コミッショナー会議（第２章第３節２.（４）ウ参照）においては、大規模な自然災害が発生した場合のパーソナルデータの取扱いの在り方について「データ保護と大規模な自然災害に関する決議」が採択された。なお、同決議においては、2004 年のインド洋津波などがその背景として言及されているが、我が国の機関は同会議に正式参加していないこともあり、2011 年 3 月 11 日に発生した東日本大震災については言及されていない。

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[74]、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となっている。

我が国における制度整備に当たっては、こうした諸外国の制度や国際社会での現状を踏まえて、パーソナルデータの利活用について国際的な場で我が国の政策について意見を表明し調整を行うことができる機関を整備することが必要不可欠である。

ウ　我が国におけるプライバシー・コミッショナー制度

上記ア・イのパーソナルデータの適正な利活用の促進のための体制の整備及び国際的な調和の取れた制度の構築の必要性を踏まえれば、パーソナルデータの利活用に関わる様々な問題について、専門的な知見を有する人材を集め、パーソナルデータの利活用の基本理念及び原則を実質的に判断して、分野横断的に迅速かつ適切に処理していくことを可能とし、かつ、諸外国の制度とも整合のとれた制度とするため、我が国の実情や法制度を踏まえた[75]、我が国におけるプライバシー・コミッショナー制度（パーソナルデータの保護のための独立した第三者機関）について検討を行うことが必要である。

（２）マルチステークホルダープロセス等の実効性確保のための取組

企業が自主的に定めたプライバシーポリシーや前節４．のマルチステークホルダープロセスを活用して策定されたルールなどについては、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[76]。よって、諸外国の制度にならって（参考資料１７参照）、企業等が自主的に宣言したポリシー・ルール等への遵守を確保するための制度を整備すべきである。

加えて、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同プロセスを活用して策定されたルールなどが適用される一方、同プロセスに参加しない企業についてはルールが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、同プロセスに参加しルールを遵守する企業にインセンティブを与え

---

74 EU の日本のパーソナルデータの保護に関する評価については、前掲脚注 32 の 14 頁、70～74 頁参照。

75 なお、我が国において職権行使の独立性が認められている機関としては、公正取引委員会や番号法案で設置されることとされている「特定個人情報保護委員会」（第２章第２節第１．（４））などの独立行政委員会などがあげられる。

76 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得る。

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基本理念及び原則の遵守を確保するための仕組みを、上記（１）のプライバシー・コミッショナー制度とも整合する形で整備していくことについて、検討を行うことが必要である。

（３）その他の制度の整備

その他、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・独立行政法人等・各地方公共団体で規律が異なること、プライバシー保護を実質的に確保するための認証制度の在り方など様々な課題が指摘されている[77]。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、上記（１）・（２）とあわせて、必要な制度整備を行うことについて検討すべきである。

[77] 前掲脚注 48 参照。

パーソナルデータ利活用の枠組みの実施のためのアクションプラン

平成２５年内に以下の取組を推進するための総合的な基本方針を策定するとともに、特に先行的に実施すべき事項については、速やかに着手し、平成２５年度内に具体化を図る。なお、本アクションプランについては、ＰＤＣＡを実施するとともに、社会経済環境の変化を踏まえた適時適切な見直しを行うこととする。

１．先行的に実施すべき事項

（１）マルチステークホルダープロセスによるルール策定等

ア　マルチステークホルダープロセスにおけるパーソナルデータの利活用のルール策定やルール遵守を円滑に進めるため、必要な事項や論点等の洗い出し、検討

イ　今後発展が期待されるセクターを選定し、マルチステークホルダープロセスの実施、実証実験等を通じた具体的なケーススタディの開始

（２）パーソナルデータの保護のための関連技術の活用

ア　再識別化を不可能又は十分に困難にしたといえる状態についての考え方の整理

イ　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、本人の同意を得なくても利活用を行うことが可能となるための措置について、透明性確保の措置及び遵守の担保措置についての検討

ウ　暗号化技術について、実態上問題が生じないと考えられる状態についての共通的な理解の醸成、鍵管理を含む運用に関するガイドラインや事例集の作成等を推進

エ　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

オ　ＤＮＴに対応した機能の実装に向けた取組の推進の働きかけ

（３）パーソナルデータ利活用のルールの遵守の確保

ア　プライバシーポリシーやマルチステークホルダープロセスを活用して策定されたルールなどパーソナルデータの利活用に関するルールの遵守を契約約款に規定することにより担保することについて、上記（１）イで選定されたセクターを中心に実施を促進

イ　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、消費者と事業者の紛争解決を行うための、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の設置準備

２. 本格的な実施のための検討事項

パーソナルデータの適正な利用・流通の促進に向けて、以下の事項について、政府全体として速やかに検討を進めていくための体制作りの促進

- 我が国におけるプライバシー・コミッショナー制度
- 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
- マルチステークホルダー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
- その他現行の個人情報保護法について指摘されている課題の解決に必要な制度整備

用語解説

ＡＰＥＣ	Asia Pacific Economic Cooperation（アジア太平洋経済協力）の略。アジア太平洋地域の 21 の国と地域が参加する経済協力の枠組みであり、貿易・投資の自由化、ビジネスの円滑化、人間の安全保障、経済・技術協力等の活動を行っている。 【第２章第２節２．（４）イ、エ、参考資料１３】
ＡＰＰＡ	Asia Pacific Privacy Authorities（アジア太平洋プライバシー機関）の略。アジア太平洋地域のパーソナルデータの保護機関がメンバーとして参加し、パーソナルデータに関する様々な課題についての議論等を行っている。 【第２章第２節２．（４）エ】
ＤＮＴ	Do Not Track の略。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のこと。 【第３章第１節６．（２）、参考資料８】
ＤＰＡ	Data Protection Authority（データ保護機関）の略。ＥＵ諸国において、データ保護指令及び各国の国内法に基づき各国が設置するデータ保護のための独立した監督機関（英国・情報コミッショナー、フランス・情報処理及び自由に関する国家委員会、ドイツ・連邦データ保護・情報自由監察官など）。 【第２章第２節２．ア（ア）、第３章第２節２．（１）イ、参考資料１６】
ｅプライバシー指令	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)（電子通信部門における個人データの処理とプライバシーの保護に関する２００２年７月１２日の欧州議会及び理事会の２００２／５８／ＥＣ指令）。分野横断的なデータ保護指令に加え、電子通信部門におけるパーソナルデータ保護に関する特則を規定する。 【第２章第２節２．（２）ア（イ）、第３章第１節２．（２）、参考資料９、１０】
ＦＴＣ	Federal Trade Commission（連邦取引委員会）の略。消費者保護等を目的とし、連邦取引委員会法（Federal Trade Commission Act）等の執行を行う米国の政府機関。パーソナルデータの保護、スパムメール対策等をも所掌する。

	【第２章第２節２.（１）イ、第３章第１節６.（２)、第３章第２節２.（１）イ、参考資料６、８】
ＧＰＳ	Global Positioning System（全地球測位システム。）の略。人工衛星を利用して、利用者の地球上における現在位置を正確に把握するシステム。 【第３章第１節３.（２）ア】
ＩＤ連携	identity federation.複数のサービスの間で、主にある主体を識別するために、当該主体に関する（認証結果を含む。）属性の集合（identity）を交換・管理する取り決め。一度の認証で複数のウェブサイトにログインできるシングルサインオン（ＳＳＯ）などの活用例がある。 【第３章第１節６.（２)】
ＩＰアドレス	インターネットやイントラネットなどのＩＰ（Internet Protocol）ネットワークに接続されたコンピュータや通信機器１台１台に割り振られた識別番号。データ通信における送信元の識別等に使われる。 【第１章、第３章第１節２.（２)】
ＩＳＯ／ＩＥＣ	ＩＳＯ（International Organization for Standardization：国際標準化機構）は、電気及び電子技術分野を除く全産業分野に関する国際規格の作成を行う国際機関であり、ＩＥＣ（International Electrotechnical Commission：国際電気標準会議）は電気及び電子技術分野の国際規格の作成を行う国際機関である。ＩＳＯ／ＩＥＣには合同のＪＴＣ（Joint Technical Committee：合同専門委員会）があり、ＩＴ分野の標準化を担当するＪＴＣ１の傘下のＳＣ２７／ＷＧ５（(Subcommittee：分科会、Working Group：作業部会の略。)）が、アイデンティティ管理とプライバシー技術を担当している。 【第２章第２節２.（４）カ】
ISO/IEC 29100:2011 Privacy framework	２０１１年に規格化された、プライバシーに関する共通的な用語の特定、PII（personally identifiable information：個人識別可能情報）の処理に関する関係者及びその役割の定義等を示すＩＳＯ／ＩＥＣの国際規格 【第２章第２節２.（４）カ、参考資料１２、１３、１４－１】
ＯＥＣＤ	Organisation for Economic Co-operation and Development（経済協力開発機構）の略。経済・社会分野において多岐にわたる活動（分野横断的な活動を含む。）を行っている先進34カ国からなる国際機関であり、事務局はパリにある。 【第２章第２節１.（１）イ、２.（４）ア、オ、参考資料１２、１３】
ＯＥＣＤプライバシーガイドラ	Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data（プ

イン	ライバシー保護と個人データの国際流通についてのガイドライン)。プライバシー保護･個人の自由と個人データの自由な流通の実現の双方のバランスを図り、個人データの取扱いに関する原則（ＯＥＣＤ８原則）などを示すガイドライン。１９８０年にＯＥＣＤ理事会がＯＥＣＤ加盟国に対し同ガイドラインについて勧告を行った。 【第２章第２節１.（１）イ、（４）ア、オ、参考資料１２】
暗号化技術	ある情報について、決まった手続に従って情報を変換することにより、第三者に盗み見られて内容を知られたり､改ざんされたりしないようにする技術のこと。 【第３章第１節６.（２)】
ウェブブラウザ	ウェブサイトを閲覧するためのアプリケーションソフト。 【第３章第１節６.（２)】
欧州評議会	Council of Europe.人権、民主主義、法の支配の分野で国際社会の基準策定を主導する汎欧州の国際機関。伝統的に活動してきた人権、民主主義、法の支配等の分野のほか、最近では薬物乱用、サイバー犯罪、人身取引、テロ、偽造医薬品対策、女性に対する暴力などの問題についても対応している。ＥＵ全加盟国、旧ユーゴスラビア諸国、ロシア、ウクライナ、トルコを含む４７ヶ国が加盟している。 【第２章第２節２.（４）オ、参考資料１２、１３、１４－１】
欧州評議会条約第１０８号	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data（個人データの自動処理に係る個人の保護に関する条約（条約第１０８号)）。１９８０年に採択された欧州評議会の条約。ＯＥＣＤガイドラインとほぼ同様なデータ保護の基本的原則を示すものである。２０１３年２月時点では、欧州評議会非加盟国のウルグアイを含む４５ヶ国が同条約を締結している。 【第２章第２節２.（４）オ、参考資料１２、１３】
欧州評議会条約第１０８号追加議定書	Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows（個人データの自動処理に係る個人の保護に関する条約への監督機関及び越境データ流通についての追加議定書)。２００１年に採択された、欧州評議会条約第１０８号の追加議定書。3か条からなるもので、独立した監督機関の設置､締約国以外の国への個人データの移転の制限等についても定めている。 【第２章第２節２.（４）オ、参考資料１２、１３、１４－１】
クッキー	ウェブサイトの提供者が、ウェブブラウザを通じて訪問者の PC 等に一時的にデータを書き込んで保存させる仕組みで､利用者に関する情報や

	最後にサイトを訪れた日時、そのサイトの訪問回数などを記録しておくことができることから、認証など利用者の識別に使われる。 【第１章、第３章第１節２．（２）、参考資料１－４】
クラウドサービス	クラウドコンピューティングサービス（Cloud Computing Service）の略。データサービスやインターネット技術等が、ネットワーク上にあるサーバー群（クラウド：雲）にあり、ユーザーは今までのように自分のコンピュータでデータを加工・保存することなく、「どこからでも、必要な時に、必要な機能だけ」利用することができる新しいコンピュータ・ネットワークの利用形態。 【第１章、第３章第１節２．（１）イ】
契約者・端末固有ＩＤ	契約者自身や契約者が所持する端末（スマートフォンや携帯電話等）を識別する番号の総称。 【第３章第１節３．（２）】
個人情報	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）。 【第１章、第２章第２節１．（１）ア　等】
個人情報保護法	個人の情報の保護に関する法律（平成１５年法律第５７号）。 【第１章　等】
実質的個人識別性	プライバシーの保護というパーソナルデータの利活用の基本理念を踏まえて実質的に判断される個人識別性（本報告書での定義）。 【第３章第１節２．（２）、６．（２）】
消費者プライバシー権利章典	２０１２年２月、米国ホワイトハウスにより政策大綱「ネットワーク化された世界における消費者データプライバシー（Consumer Data Privacy in a Networked World ）」が発表され、同政策大綱で「消費者プライバシー権利章典（The Consumer Privacy Bill of Rights）」が提示された。 【第１章、第２章第２節２．（１）イ、第３章第１節２．（２）、参考資料７、１２、１３】
情報理論的安全性	情報理論（通信における情報伝達の数学的理論）に基づいて暗号解読の可能性に着目した暗号の安全性に関する概念。この安全性を満たす暗号では、攻撃側がどれほどの計算能力を有していようとも、公開情報を見たときに暗号文を復号するための鍵となる情報を推測できない。 ⇔　計算量的安全性 【第３章第１節６．（２）】
スマートフォン	従来の携帯電話端末の有する通信機能等に加え、高度な情報処理機能が備わった携帯電話端末。様々なアプリケーションをインストールするこ

	とで、多様な目的のために活用することができる。 【第１章、第２章第２節１.（２）(ア)、第３章第１節２.（２）、３（２）ア、イ】
タブレット端末	触れて操作が行える液晶画面（タッチパネル）を搭載した端末。通信機能に加え、高度な情報処理機能が備わっており、様々なアプリケーションをインストールすることで、多様な目的のために活用することができる。 【第１章、第３章第１節３.（２）ア】
端末ＩＤ	端末（スマートフォンや携帯電話等）等を識別する番号の総称。 【第１章、第３章第１節２.（２)】
データ保護プライバシー・コミッショナー国際会議	International Conference of Data Protection and Privacy Commissioners.１９７９年から毎年開催されている会合で、アルゼンチン、オーストラリア、カナダ、フランス、ドイツ、ギリシャ、アイスランド、イスラエル、イタリア、メキシコ、モロッコ、オランダ、ニュージーランド、ノルウェー、ペルー、韓国、英国、ウルグアイ、米国等５７ヶ国のパーソナルデータの保護機関がメンバーとして参加している（２０１２年現在)。日本からは正式な参加が認められている機関はなく、消費者庁にオブザーバー資格が認められているのみである。各国のパーソナルデータの保護機関により、パーソナルデータに関する様々な課題についての議論等が行われている。 【第２章第２節２.（４）ウ、エ】
データ保護規則提案	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)（個人データの取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の規則（一般的データ保護規則）の提案)。 【第２章第２節２.（２）イ、第３章第１節６.（２)、参考資料１２、１３、１４－１、１７】
データ保護指令	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data(個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する１９９５年１０月２４日の欧州議会及び理事会の９５／４６／ＥＣ指令)。 【第２章第２節２.（２）ア（ア）(イ)、イ、第３章第２節２.（１）イ、参考資料９－１、９－２、１０－１、１２、１３、１４－１、１７】

匿名化技術	特定の個人を識別できないように、又は、特定の個人を識別できる可能性を小さくするため、情報を加工する技術。 【第２章第１節、第３章第１節６．（２）】
トラストフレームワーク	一定のポリシーに準拠していることについて認定・監査を行うことにより、プライバシー・セキュリティに関する信頼性を担保し、ＩＤ連携や自由なデータ移転を促進・協力しようという、ＩＤ発行・認証者やサービス提供者によって作られた枠組みのこと。 【第３章第１節６．（２）】
パーソナルデータ	個人に関する情報（本報告書での定義）。 【第１章　等】
秘密分散技術	秘密を守りたいデータ（元データ）を複数のデータ（分散データ）に分けて守る暗号化技術。複数の分散データに分けられた元データは決められた数の分散データを集めないと、復号されない。 【第３章第１節６．（２）】
プライバシー強化技術	Privacy Enhancing Technologies（PETs）．プライバシーを保護するために利用可能な技術のこと。匿名化技術や暗号化技術等がある。 【第３章第１節６．（１）】
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。 【第３章第１節１．（２）イ、参考資料４，１０－２、１１、１２】
プライバシーポリシー	パーソナルデータを利用する者が明らかにする、パーソナルデータの取扱いに関する方針。 【第３章第１節３．（２）イ、５．（２）、第２節１．、２．（２）】
保護されるパーソナルデータ	パーソナルデータのうち、本報告書が提示するパーソナルデータの利活用の枠組みにおいて保護の対象とするパーソナルデータ（本報告書での定義）。 【第１章、第３章第１節２．等】
ライフログ	蓄積された個人の生活の履歴をいい、購買・貸出履歴、視聴履歴、位置情報等々が含まれる。 【第２章第２節１．（２）イ（ア）】
連結可能匿名化	必要な場合に特定の個人を識別できるように、その人と新たに付された符号又は番号の対応表を残す方法による匿名化のこと。 ⇔　連結不可能匿名化 【第３章第１節６．（２）】

参考資料集　目次

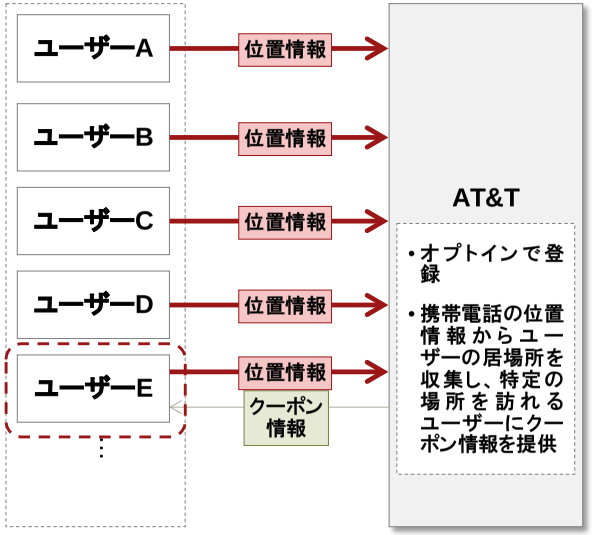
参考資料１　パーソナルデータの利活用の事例・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・４８
参考資料２　我が国の個人情報保護法の体系・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・５２
参考資料３　「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会」第二次提言（2010 年 5 月）　・・・５３
参考資料４　スマートフォン プライバシー イニシアティブ（2012 年８月）（利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会）・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・５４
参考資料５　「行政手続における特定の個人を識別するための番号の利用等に関する法律案」（番号法案）（2013 年 3 月に提出されたもの）の概要・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・５５
参考資料６　米国（連邦政府）のパーソナルデータ保護に関する制度・・・・・・・・・・・・・・・・・・・５６
参考資料７　米国消費者プライバシー権利章典・・・・・・・・・・・・・・・・・・・・・・・・・・・・・５７
参考資料８　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」　・・・・・・・・・５８
参考資料９　EU のパーソナルデータ保護に関する制度（現行制度）・・・・・・・・・・・・・・・・・・・５９
参考資料１０　EU のパーソナルデータ保護に関する制度（データ保護規則提案）・・・・・・・・・・・・・６１
参考資料１１　プライバシー・バイ・デザイン・・・・・・・・・・・・・・・・・・・・・・・・・・・・・６４
参考資料１２　パーソナルデータの保護の原則の比較・・・・・・・・・・・・・・・・・・・・・・・・・・６５
参考資料１３　保護対象となるパーソナルデータの範囲の比較・・・・・・・・・・・・・・・・・・・・・６６
参考資料１４　センシティブデータの範囲の比較・・・・・・・・・・・・・・・・・・・・・・・・・・・６７
参考資料１５　簡潔な表示に関する検討・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・６９
参考資料１６　各国のパーソナルデータ保護の監督機関の比較・・・・・・・・・・・・・・・・・・・・７１
参考資料１７　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・・・・・・・・・・・・・・・７２

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

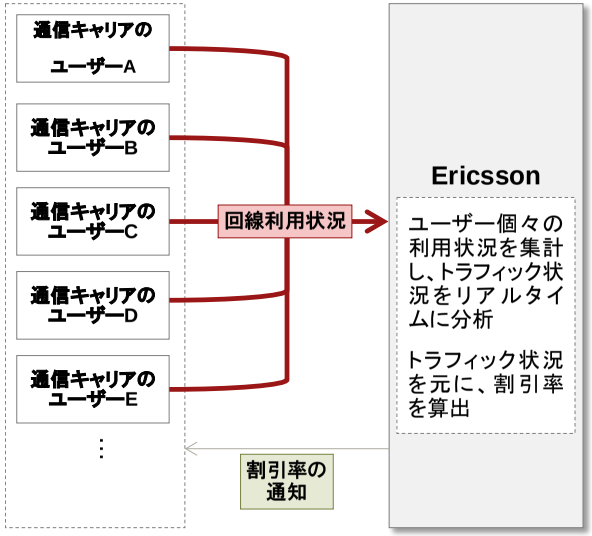
AT&T Shop Alerts（米国）

- 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
- ※AT&Tのプライバシーポリシーに、取得する情報の種類、利用目的、第三者提供や情報収集時の同意取得、オプトアウトに関する記載がある



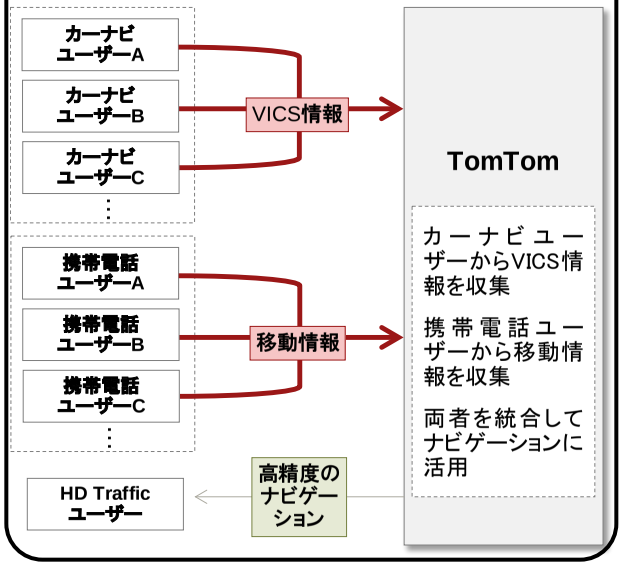
Ericsson DDS（南アフリカ）

- 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（DDS : Dynamic Discount Service)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
- ※MTNのプライバシーポリシーに、取得する情報の種類、利用目的、情報収集時の同意、情報収集時の同意に基づく第三者提供に関する記載がある



TomTom HD Traffic（オランダ）

- 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
- ※TomTomのプライバシーポリシーにユーザライセンス取得時の同意取得、取得する情報の種類、利用目的に関する記載がある



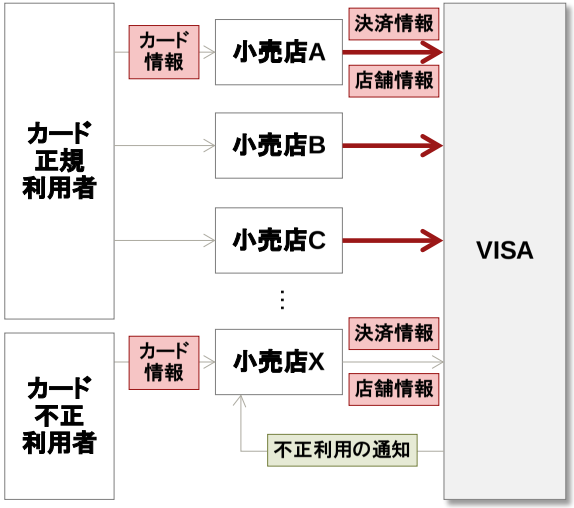
出典：本研究会第4回会合吉川構成員資料、（株）日立コンサルティング作成資料より作成

パーソナルデータの利活用の事例②（金融業・保険業）

参考資料１－２

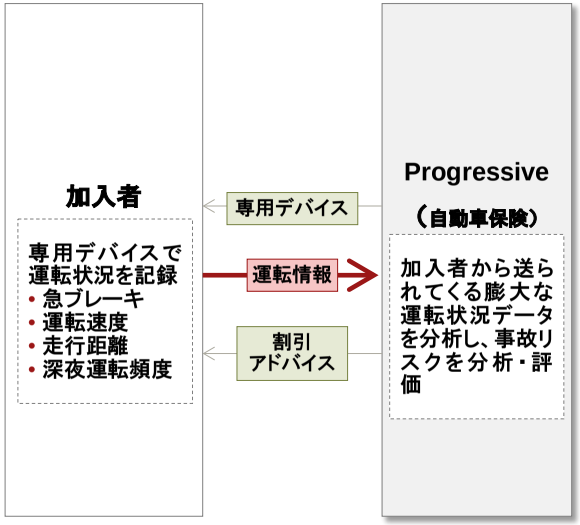
Visa Advanced Authorization（北米）

- 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
- ※同サービスに関するプライバシーポリシーは公開されていないが、各店舗での決済情報をVISAが分析し、不正利用と思われる場合に店舗に通知するため、決済情報を第三者提供することはない



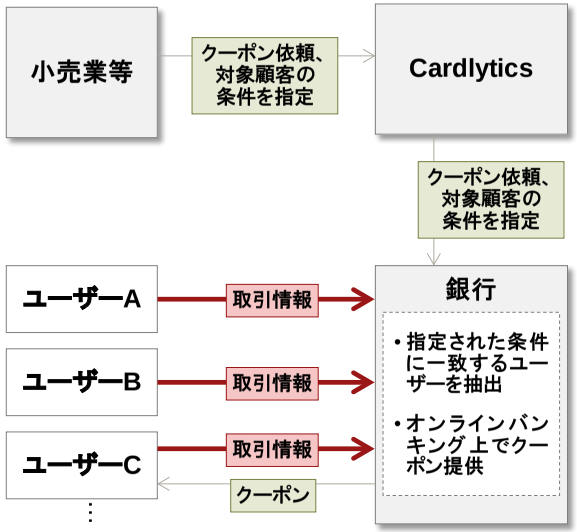
Progressive Snapshot（米国）

- 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
- ※Snapshotサービスの利用規約に、取得する情報の種類とサービス利用時の同意取得、Progressiveのプライバシーポリシーに、取得する情報の種類、利用目的に関する記載がある



Cardlytics（米国）

- 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等に第三者提供することはない



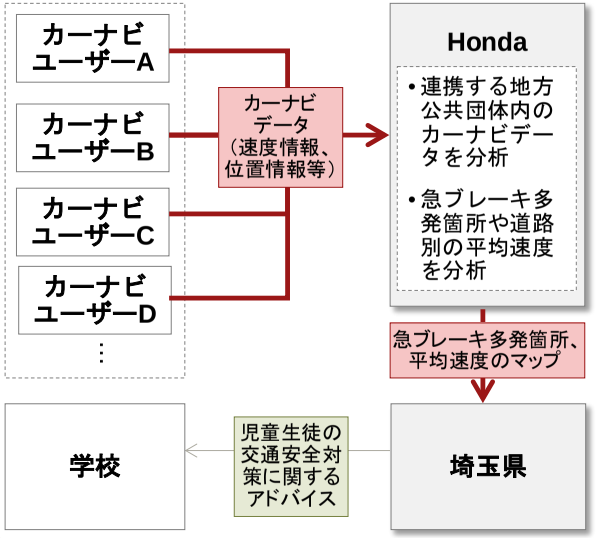
出典：本研究会第4回会合吉川構成員資料、（株）日立コンサルティング作成資料より作成

パーソナルデータの利活用の事例③（行政分野、公益事業）

参考資料１－３

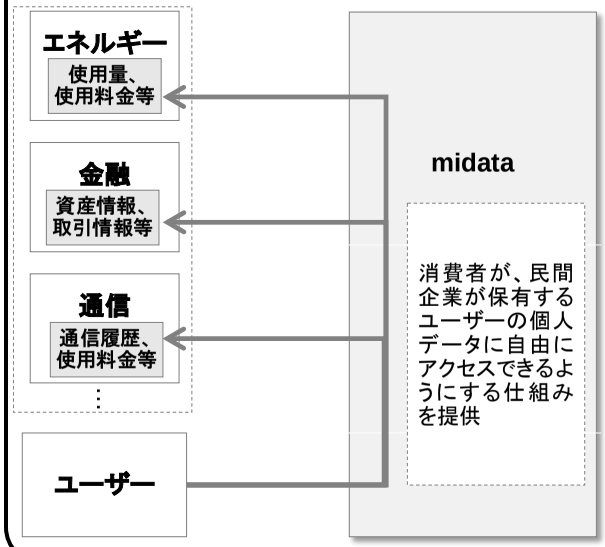
埼玉県 ｶｰﾅﾋﾞﾃﾞｰﾀ活用（日本）

- 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
- ※同サービスの利用規約に、取得する情報の種類、利用目的、情報収集時・第三者提供の際の同意取得に関する記載がある



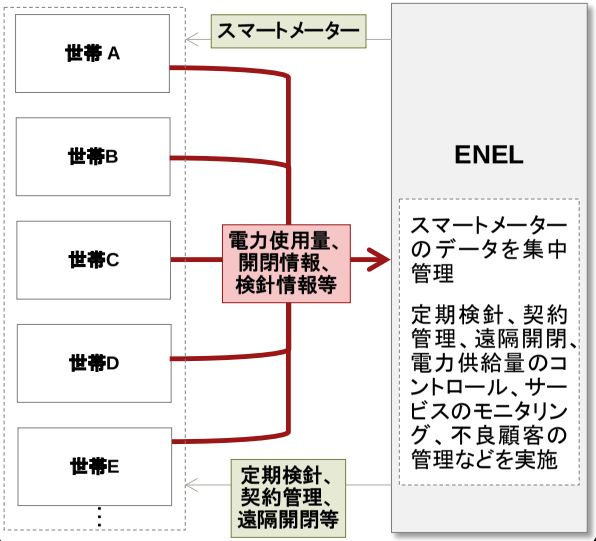
midata（英国）

- 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（イタリア）

- 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
- ※パーソナルデータの取扱いは契約時の説明書に記載されているためその内容を確認できないが、世帯からのデータの管理や定期検診等のサービスはENELが行うものであり、データを第三者提供することはない



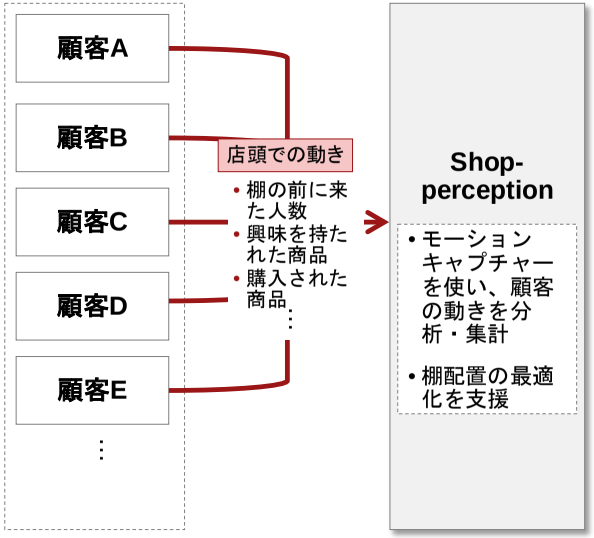
出典：本研究会第5回会合奥屋構成員資料、（株）日立コンサルティング作成資料より作成

パーソナルデータの利活用の事例④（小売業）

参考資料１－４

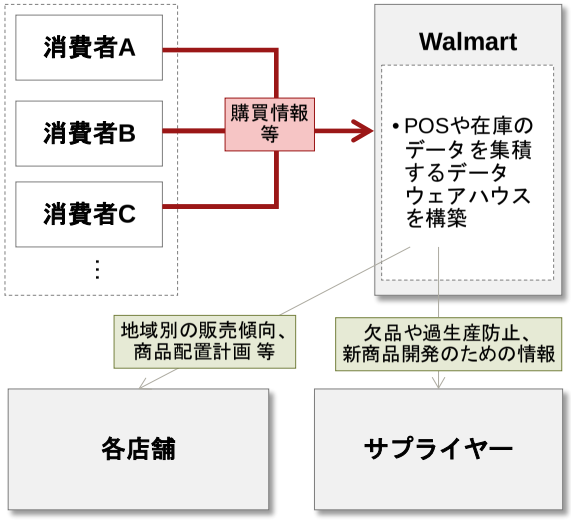
Shopperception（米国）

- 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
- 販売時点のPOS（Point of Sales）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
- ※Shopperceptionのサービスを導入する小売店がパーソナルデータについて適正な取扱いをすれば問題は生じない



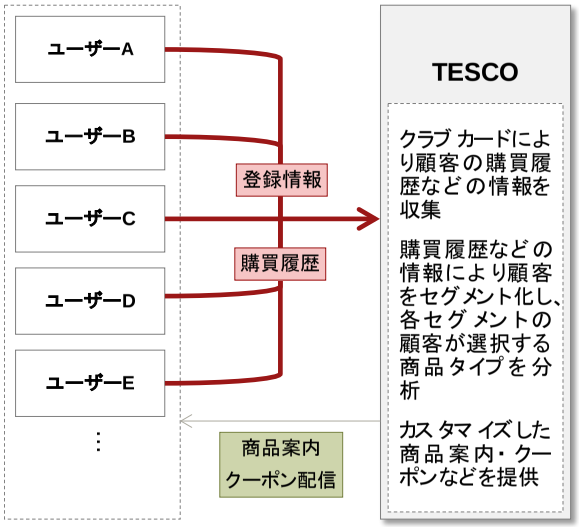
Walmart Data-warehouse（米国）

- Walmartでは、POSや在庫のデータを集積するデータウェアハウスを構築
- POSデータ分析から、同時購入されやすい商品を同じ売り場に配置するなどのクロスマーチャンダイジングを展開
- また、データはサプライヤーとも共有され、店舗とサプライヤーが協力して欠品や過生産の防止、新商品開発等に活用
- ※プライバシーポリシーにて、消費者の購入情報を収集している旨や、データをマーケティング等に活用する旨、サプライヤーと共有する旨について述べている



TESCO Club-card（英国）

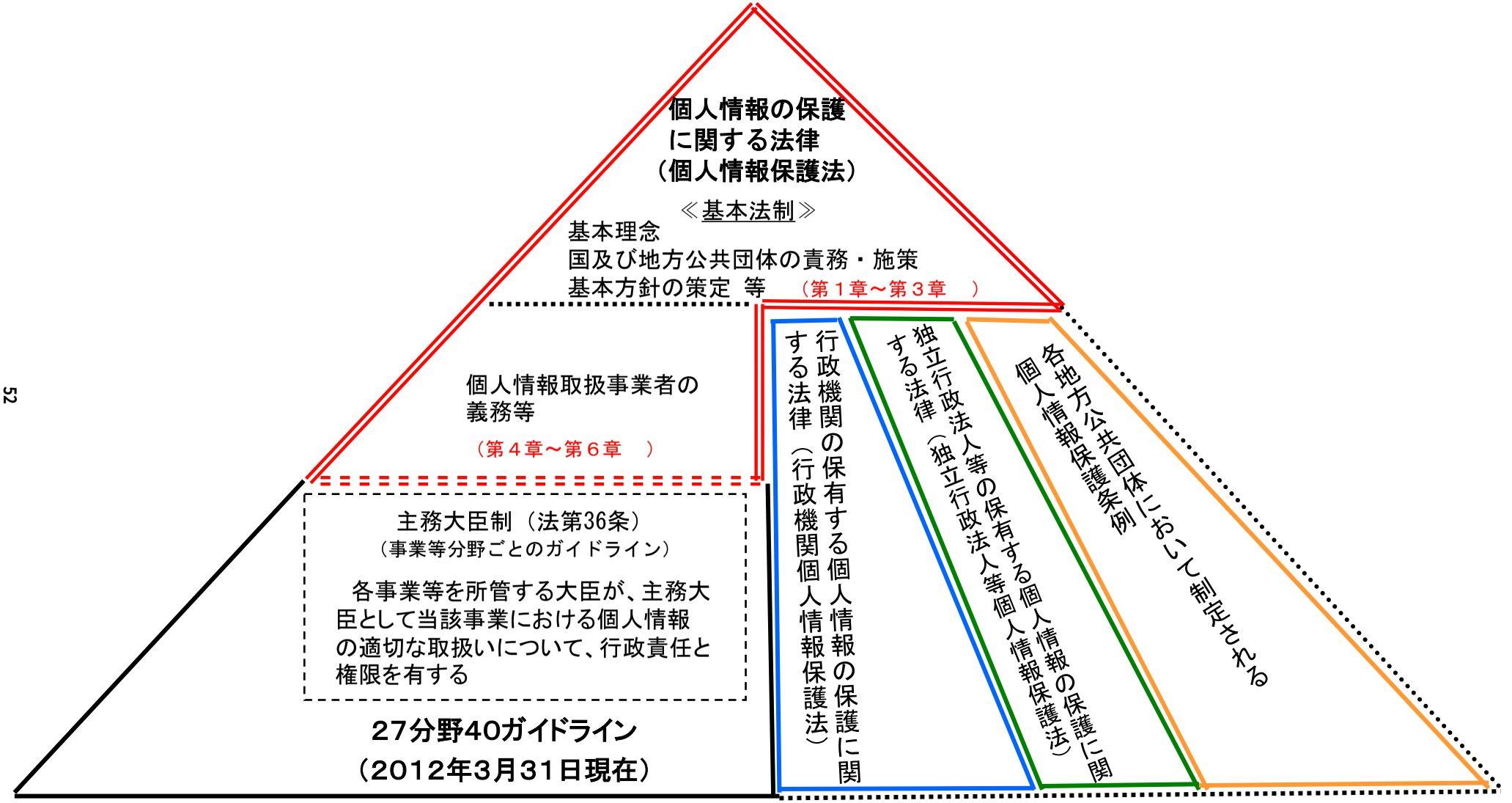
- TESCOでは、ポイントプログラムであるクラブカードにより顧客の購買履歴などの情報を収集
- 購買履歴などの情報を用いて顧客を類型化し、各類型の顧客が選択する商品タイプを分析
- 顧客に対し、カスタマイズした商品案内やクーポンなどを提供
- ※クラブカードのプライバシー・クッキーポリシーには、取得する情報の種類、利用目的、Webサイトを通じたサービスを受ける場合にはそれらの情報の取得に同意する旨が記載されている



出典：本研究会第４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より作成

我が国の個人情報保護法の体系

参考資料２



○配慮原則

◆対象情報

配慮原則の対象となる情報は、特定の端末、機器及びブラウザ等を識別することができるものとする。対象情報は、個人情報保護法上の個人情報であるか否かを問わない。

◆対象事業者

対象となる事業者は、対象情報を事業（ただし、対象情報を蓄積せずに行う事業は除く。）の用に供している者とする。

◆配慮原則

①広報、普及、啓発活動の推進

対象事業者その他の関係者は、利用者のリテラシーの向上や不安感や不快感の払拭に資するべく、対象情報を活用したサービスの仕組みや、本配慮原則に基づく取組について、広報その他の啓発活動に努めるものとする。

②透明性の確保

対象事業者その他の関係者は、対象情報の取得・保存・利活用及び利用者関与の手段の詳細について、利用者に通知し、又は容易に知り得る状態に置く（以下「通知等」という。）よう努めるものとする。通知等に当たっては、利用者が容易に認識かつ理解できるものとするよう努めるものとする。

③利用者関与の機会の確保

対象事業者は、その事業の特性に応じ、対象情報の取得停止や利用停止等の利用者関与の手段を提供するよう努めるものとする。

④適切な手段による取得の確保

対象事業者は、対象情報を適正な手段により取得するよう努めるものとする。

⑤適切な安全管理の確保

対象事業者は、その取り扱う対象情報の漏えい、滅失又はき損の防止その他の対象情報の安全管理のために必要かつ適切な措置を講じるよう努めるものとする。

⑥苦情・質問への対応体制の確保

対象事業者は、対象情報の取扱いに関する苦情・質問への適切かつ迅速な対応に努めるものとする。

スマートフォン プライバシー イニシアティブ（2012年8月）

（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）

参考資料４

スマートフォンの利用者情報の取扱いに関する包括的な対策を提案。アプリケーション提供者や情報収集モジュール提供者等を中心に、アプリケーション提供サイト運営事業者・OS提供事業者、移動体通信事業者等のスマートフォンの関係事業者に広く適用可能な**「スマートフォン利用者情報取扱指針」**等を示す（以下は同指針の概要）。

【総論】　**１　基本原則**

２　適用対象

３　用語の定義

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

【各論】

１　利用者情報取得者における取組（アプリ提供者、情報収集モジュール提供者、広告配信事業者）

（1）プライバシー・ポリシーの作成

☞ 以下の項目を記載したプライバシーポリシーを、アプリケーションや情報収集モジュールごとに分かりやすく作成する（簡略版も作成する。）。

（記載項目）

① 情報を取得するアプリ提供者等の氏名又は名称
② 取得される情報の項目
③ 取得方法
④ 利用目的の特定・明示
⑤ 通知・公表又は同意取得の方法、利用者関与の方法*1,2
⑥ 外部送信・第三者提供・情報収集モジュールの有無
⑦ 問合せ窓口
⑧ プライバシーポリシーの変更を行う場合の手続

*1　同意取得：　一部のプライバシー性の高い情報については、原則同意を取得する（電話帳、位置情報、通信履歴等）。
*2　利用者関与：利用者がアプリによる利用者情報の利用や取得の中止を希望する場合に、その方法を記載する。

（2）適切な安全管理措置

・ 利用者情報の漏洩、滅失、毀損の危険回避の措置を講ずる。

（3）情報収集モジュール提供者に関する特記事項

・ アプリケーション提供者へ①取得する情報の項目、②利用目的、③第三者提供の有無等について通知する。

２　その他の関係事業者における取組

（1）移動体通信事業者・端末提供事業者：　アプリ提供者の適切な取扱い支援・啓発活動、連絡通報窓口の整備等を行う。
（2）アプリ提供サイト運営事業者、OS提供事業者：　同上、OSによる利用許諾がある場合に分かりやすい説明を行う。
（3）その他関係しうる事業者：　アプリケーション紹介サイトは有益な情報源となり得る。

「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」（番号法案）（2013年３月に提出されたもの）の概要

参考資料5

基本理念（第3条）

○　個人番号及び法人番号の利用に関する施策の推進は、個人情報の保護に十分に配慮しつつ、社会保障、税、災害対策に関する利用の促進を図るとともに、他の行政分野及び行政分野以外の国民の利便性の向上に資する分野における利用の可能性を考慮して行う。

個人番号（第7条～第16条）

○　市町村長は、法定受託事務として、住民票コードを変換して得られる個人番号を指定し、通知カードにより本人に通知。盗用、漏洩等の被害を受けた場合等に限り変更可。中長期在留者、特別永住者等の外国人住民も対象。
○　個人番号の利用範囲を法律に規定。①国･地方の機関での社会保障分野、国税･地方税の賦課徴収及び災害対策等に係る事務での利用、②当該事務に係る申請･届出等を行う者（代理人･受託者を含む。）が事務処理上必要な範囲での利用、③災害時の金融機関での利用に限定。
○　番号法に規定する場合を除き、他人に個人番号の提供を求めることは禁止。本人から個人番号の提供を受ける場合、個人番号カードの提示を受ける等の本人確認を行う必要。

個人番号カード（第17条･第18条）

○　市町村長は、顔写真付きの個人番号カードを交付。
○　政令で定める者が安全基準に従って、ＩＣチップの空き領域を本人確認のために利用。（民間事業者については、当分の間、政令で定めないものとする。）

個人情報保護（第19条～第57条等）

○　番号法の規定によるものを除き、特定個人情報（個人番号をその内容に含む個人情報）の収集･保管、特定個人情報ファイルの作成を禁止。
○　特定個人情報の提供は原則禁止。ただし、行政機関等は情報提供ネットワークシステムでの提供など番号法に規定するものに限り可能。
○　民間事業者は情報提供ネットワークシステムを使用できない。
○　情報提供ネットワークシステムでの情報提供を行う際の連携キーとして個人番号を用いないなど、個人情報の一元管理ができない仕組みを構築。
○　国民が自宅のパソコンから情報提供等の記録を確認できる仕組み（マイ･ポータル）の提供、特定個人情報保護評価の実施、特定個人情報保護委員会の設置、罰則の強化など、十分な個人情報保護策を講じる。

法人番号（第58条～第61条）

○　国税庁長官は、法人等に法人番号を通知。法人番号は原則公表。民間での自由な利用も可。

検討等（附則第6条）

○　法施行（公布後３年以内）後３年を目途として、個人番号の利用範囲の拡大について検討を加え、必要と認めるときは、国民の理解を得つつ、所要の修正を講ずる。
○　法施行後１年を目途として、特定個人情報保護委員会の権限に特定個人情報以外の個人情報の取扱いに関する監視・監督を追加すること等について検討を加え、その結果に基づいて所要の措置を講ずる。

米国（連邦政府）のパーソナルデータ保護に関する制度

参考資料６

分野横断的なパーソナルデータ保護の法律は存在しない

（民間部門）

政府部門	健康情報等	信用情報	通信分野	金融部門	児童のプライバシー
プライバシー法（Privacy Act of 1974）	医療保険の相互運用性及び説明責任に関する法律（HIPPA）	公正信用報告法(FCRA)	電子通信プライバシー法（ECPA）	金融サービス近代化法（Gramm-Leach-Bliley Act）	児童オンラインプライバシー保護法（COPPA）

自主規制

（参考）EU・米国間のセーフハーバー枠組み（2000年7月）

商務省

セーフハーバー原則

① 告知：利用目的等の告知
② 選択：オプトイン、オプトアウトの機会の提供
③ 第三者への提供：告知と選択の原則の適用等
④ セキュリティ
⑤ データの完全性
⑥ アクセス；開示、訂正、変更、削除請求
⑦ 執行

企業

- セーフハーバー原則遵守の宣言
- プライバシーポリシーを公表
- セーフハーバー原則の遵守の確約書を商務省に提出
- 商務省は当該企業名等をウェブサイトに掲載

FTC

【違反行為が発覚した場合】

- 「不公正又は欺瞞的な行為又は慣行(unfair or deceptive acts or practices)」（FTC法第５条）として、排除措置・課徴金等の対象
- 民事責任も問われる。

米国消費者プライバシー権利章典

参考資料７

米国政府発表：“ Consumer Data Privacy in a Networked World ” (2012年2月23日)

「消費者プライバシー権利章典」(The Consumer Privacy Bill of Rights)

1	個人による管理	：消費者は、自分の個人データを企業が収集し、それを使用する方法について管理する権利を有する。
2	透明性	：消費者は、プライバシー及びセキュリティの企業実務に関する情報に容易に理解しアクセスできる権利を有する。
3	**経緯の尊重**	**：消費者は、企業が、自分の個人データを、自分が情報を提供した経緯に沿う方法で、収集、使用、開示することを期待する権利を有する。**
4	セキュリティ	：消費者は、個人データを保護し、責任持って処理する権利を有する。
5	アクセス及び正確性	：消費者は、使用可能な形式で、また、データの機微性及びデータが不正確であった場合に消費者に悪影響を与える危険度に応じた方法で、個人データにアクセスし訂正する権利を有する。
6	**対象を絞った収集**	**：消費者は、企業が収集及び保持する個人データに合理的な制限を設ける権利を有する。**
7	**説明責任**	**：消費者は、この権利章典の遵守を保証するための適切な措置を講じる企業によって個人データが処理される権利を有する。**

個人プロファイリングを念頭

NTIAにおけるcode of conduct (行動規範）の検討

Do Not Track（オプトアウト原則）

関係者間プロセスの強化

- 行動規範を採用するかどうかは企業が最終判断
- 遵守を公言した企業が違反した場合、FTCは行動規範に基づき、執行可能

連邦取引委員会（FTC）の執行能力の向上

国際的な相互運用性の促進

- 相互認証・執行協力が必要

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」

参考資料８

FTC報告書（2012年3月）
“ Protecting Consumer Privacy in an Era of Rapid Change ”

米広告業界は反発

IE 10(MS)、FF（Mozilla）は、DNTをデフォルト

対象企業

- 特定の消費者、コンピュータ、その他デバイスと合理的に関連付けられる消費者データを収集したり、利用したりする企業(commercial entity)
- ただし、年間5,000名未満の消費者のセンシティブでない消費者データのみを収集し、かつ、その消費者データを第三者と共有しない企業については含まれない

企業行動枠組み

① 計画的なプライバシー保護の実施 (Privacy by Design)
② 消費者への簡潔な選択肢の提供
③ 透明性の確保

FTCによる支援 (2013年末までを想定)

① 追跡拒否(Do Not Track)
② 携帯電話
③ データ販売業者(ブローカー)
④ 大規模プラットフォームプロバイダー
⑤ 法執行可能な自主規制規範の推進

・FTCは規制導入に前向き
・個人情報検索サイトSpokeo に対して80 万ドルの罰金（2012年6月）

EUのパーソナルデータ保護に関する制度（現行制度）①

参考資料９－１

データ保護指令（1995年）
「個人データ処理及びデータの自由な移動に関する個人の保護に関する指令（95/46/EC）」

分野横断的なパーソナルデータ保護に関する規制

（主な内容）
（1）データ内容に関する原則（特定された明示的かつ適法な目的のための取扱い等）
（2）データ取扱いの正当性の基準（データ主体の明確な同意等）
（3）センシティブデータ※の取扱い ※人種又は民族、政治的見解、宗教的又は思想的信条、労働組合への加入、健康又は性生活に関するデータ
（4）データ主体のデータへのアクセス権
（5）取扱いの機密性及び安全性
（6）第三国への個人データの移転に関する規律（第三国が十分なレベルの保護措置を確保していることを条件とする等）
（次頁参照）
（7）独立した監督機関

eプライバシー指令（2002年、2009年改正）
「電子通信部門における個人情報の処理とプライバシーの保護に関する指令（2002/58/EC）」

電子通信部門に関するデータ保護指令の特則

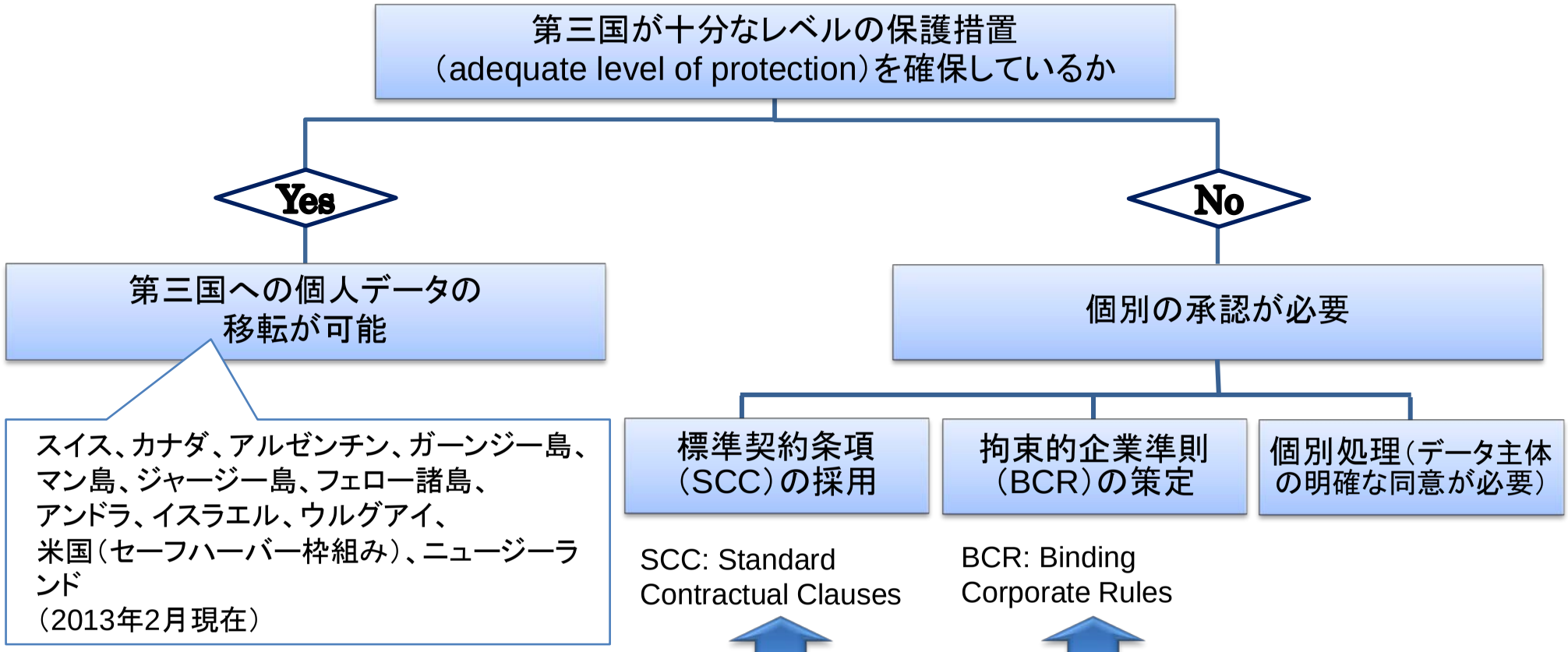
（主な内容）
（1）通信の秘密保持
（2）Cookieの利用に当たって内容を明示しオプトインによる利用者同意を求める
（3）ロケーションデータを利用する際にオプトインによる利用者同意を求める

英国	フランス	ドイツ	イタリア
データ保護法	情報処理、情報ファイル及び自由に関する法律	連邦データ保護法	個人データの処理に関する個人その他の主体の保護に関する法律

等

EUにおけるパーソナルデータ保護に関する制度（現行制度）②
－データ保護指令における第三者への個人データ移転の仕組み－

参考資料９－２



（注）モナコについては、
「十分なレベルの保護措置を行っている」
と認定済み。（欧州委員会の決定待ち）

EUのパーソナルデータ保護に関する制度（データ保護規則提案）①

参考資料１０－１

データ保護指令（1995年）

eプライバシー指令（2002年、2009年改正）

- 急速な技術進展
- 情報の共有・収集の規模の劇的な増加

データ保護規則提案（2012年1月）

立法手続を開始

① EU域内における規制の単一化・簡素化
- 国内法制化の不要な「規則」に変更
- 一国からの承認を得れば、他国の当局からの承認は不要
- データ保護当局間の調査協力のメカニズム

② より強固なデータ保護ルールの整備

③ データ保護に関するグローバルな課題への対応

EUのパーソナルデータ保護に関する制度（データ保護規則提案）②
― より強固なパーソナルデータ保護ルール ―

参考資料１０－２

事業者

「プライバシー・バイ・デザイン」原則（参考資料１１参照）

- 新サービスの導入時、データ保護への考慮の義務付けの導入
- 個人の権利や自由に対するリスクを伴うパーソナルデータの取扱いを行うに当たって、当該取扱いがパーソナルデータの保護に対して与える影響度の評価（PIA: Privacy Impact Assessment プライシー影響評価）を実施する必要がある旨の規定
- 「データ保護職員」の任命義務（250人以上の従業員の雇用などの要件を満たす事業者が対象）

個人データ漏えい時の通知義務

- データ保護当局に対しては可能な場合24時間以内に、個人に対しては当該個人のプライバシー等に悪影響を及ぼす可能性がある際には遅滞なく通知

パーソナルデータ

個人

忘れられる権利

- データ削除に関する現行法令における個人の権利をより明確化するとともに、データ管理者は、ネット上でのパーソナルデータへのリンクやコピー・複製されたパーソナルデータについて、当該個人から削除要求があった場合、当該要求を（それらデータを扱う）第三者に対して通知するなど、あらゆる合理的手段を講ずる義務がある旨規定

データ持ち運びの権利

- 共通化されたフォーマットで電子的に自らのデータのコピーをデータ管理者から取得できるとともに、自らのデータをあるアプリケーションから別のアプリケーションに移転させることができる権利について規定

同意の明示

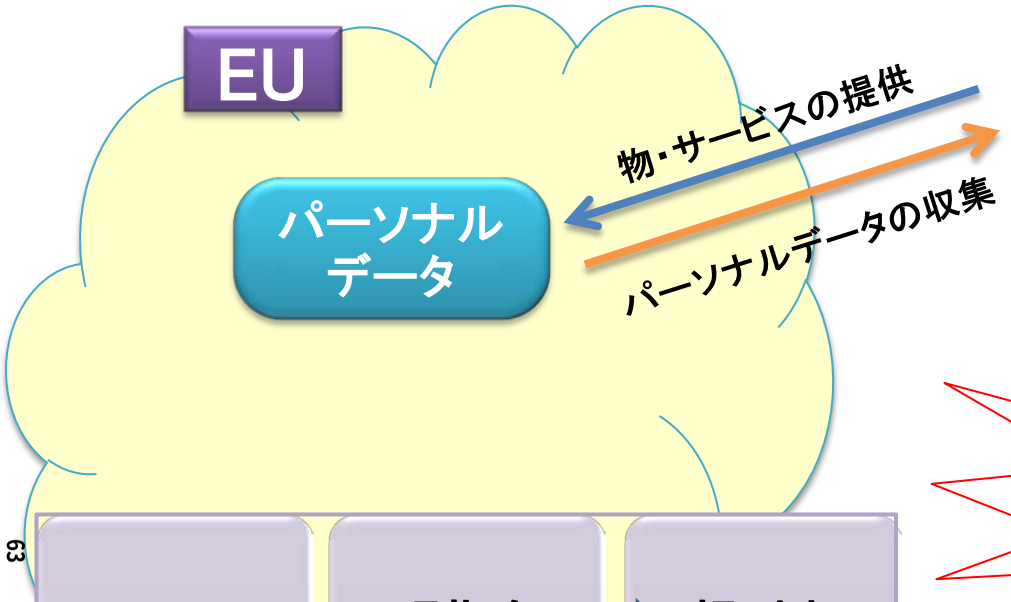
オプトイン原則

- パーソナルデータの取得に当たって必要な同意は明示的な（explicit）ものであることを要する旨の規定

EUにおけるパーソナルデータ保護に関する制度（データ保護規則提案）③

参考資料１０－３

－ グローバルな課題への対応 －



域外事業者

- データ保護規則の域外適用
- EU域内に代理人を置く必要（一定の要件を満たす場合）

規則に違反した場合（域内事業者を含む）

制裁（課徴金）

最大で、100万ユーロ、又は事業者の全世界での売上高の2%相当額の課徴金

	現指令	規則案
標準契約条項（SCC）	各国当局の承認	承認不要
拘束的企業準則（BCR）	関連する各国当局の承認	一国の当局の承認
個別処理	データ主体の個別同意等	データ主体の個別同意等

「プライバシー・バイ・デザイン」

参考資料１１

プライバシー・バイ・デザイン（PbD：Privacy by Design）

カナダ　オンタリオ州　情報プライバシー・コミッショナーのアン・カブキアン博士が１９９０年代に開発した概念

7つの基本原則

1. 事後的ではなく、事前的；　救済的でなく予防的
2. 初期設定としてのプライバシー
3. デザインに組み込まれるプライバシー
4. 全機能的　－　ゼロサムではなく、ポジティブサム
5. 最初から最後までのセキュリティ
   －　すべてのライフサイクルを保護
6. 可視性と透明性　－　公開の維持
7. 利用者のプライバシーの尊重
   －　利用者中心主義を維持する

プライバシー影響評価（PIA：Privacy Impact Assecemnet）

個人情報の収集を伴う情報システムの導入にあたり、プライバシーへの影響度を「事前」に評価し、その構築・運用を適正に行うことを促す一連のプロセス

プライバシー・バイ・デザインの実施プロセス

1. プライバシー要件を作成する
2. 個人に関する情報の流れを確認する
3. プライバシー要求仕様を開発する
4. プライバシー要求仕様を設計に盛り込む
5. 開発方法へ適用する
6. テストして確認する

プライバシー影響評価（PIA）を活用

参考資料１２

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）	欧州評議会条約第 108 号(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

※欧州評議会条約第 108 号及び同追加議定書、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（オーストラリア・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、同資料では、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１３

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可能な個人（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);
欧州評議会条約第 108 号（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（「データ主体」）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、識別可能な人である。 '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を意味する。「データ主体」とは、管理者その他の自然人又は法人によって合理的な範囲で使用される手段、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、文化的若しく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り、直接的又は間接的に識別された自然人を意味する。 '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ものを含む。 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)その情報に関する 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１４－１

センシティブデータの範囲の比較①（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１４－２

センシティブデータの範囲の比較②（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」（２０１２年８月７日）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。

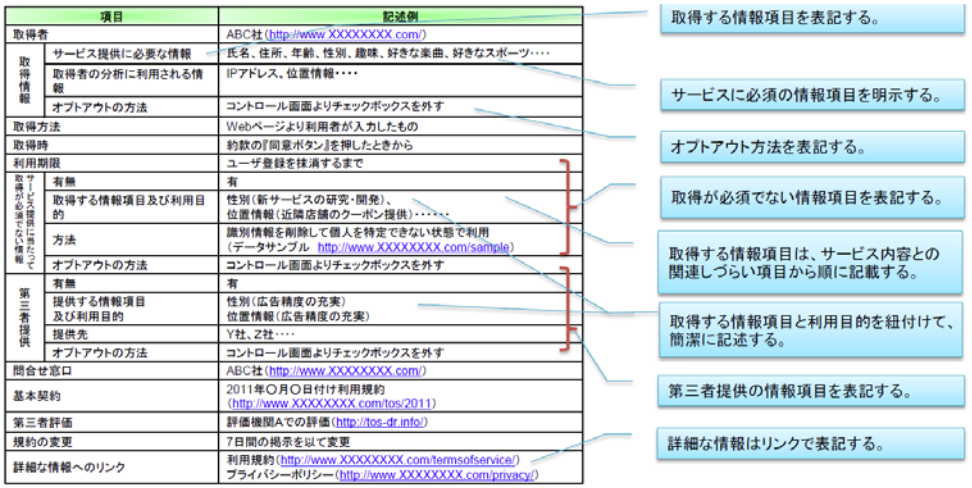
アプリケーション・プライバシーポリシーのモデル案

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）

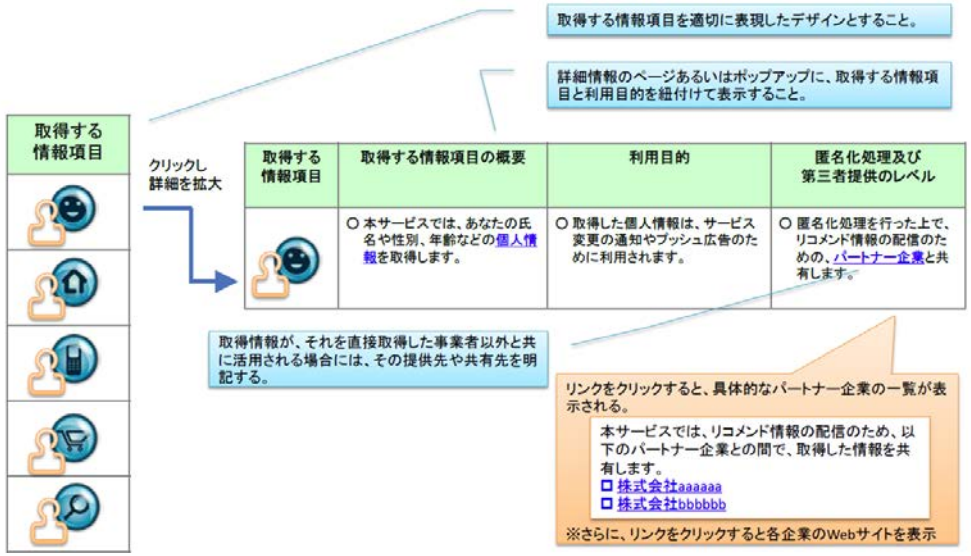
（参考）アプリケーション・プライバシーポリシー概要版

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



■アイコンによる表示のイメージの提示

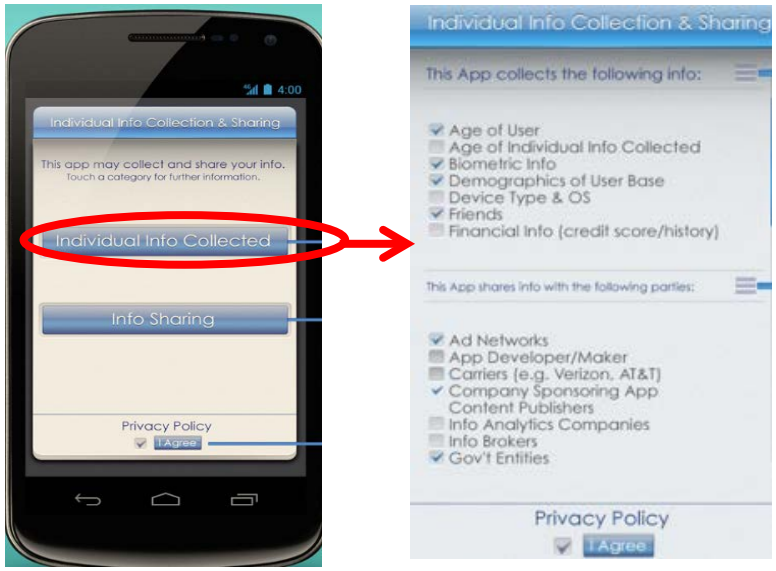


出典：経済産業省 IT 融合フォーラムパーソナルデータ ワーキンググループ報告書
「パーソナルデータ利活用の基盤となる消費者と事業者の信頼関係の構築に向けて」
（２０１３年５月１０日）

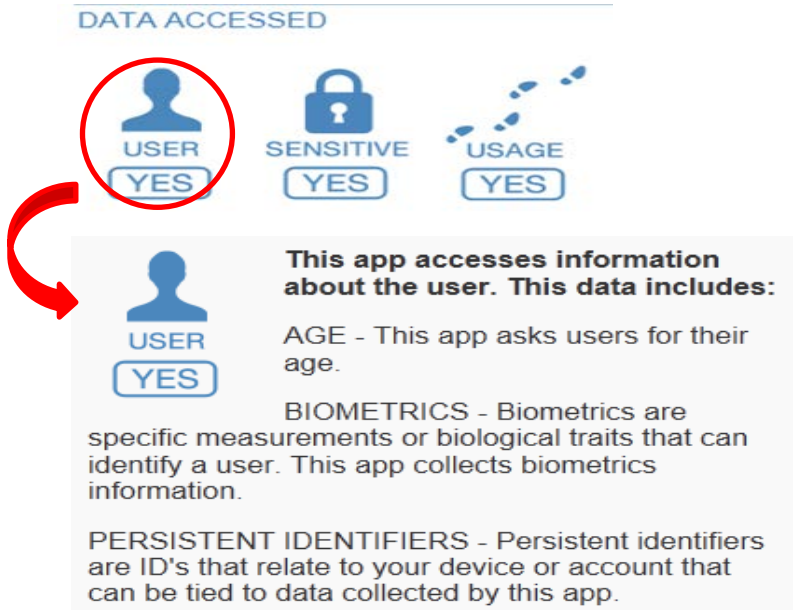
簡潔な表示に関する検討②

米国 NTIA（国家電気通信情報庁）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１６

各国の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 （Information Commissioner）	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 (Privacy Commissioner of Canada)	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))	※各州の法律 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） （オンタリオ州の場合）	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 (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（Australian Information Commissioner） プライバシーコミッショナー（Privacy Commissioner） （前者が後者の上位にあたる。）	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）	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(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１７

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	—