第3章 安心・安全なICT活用環境の実現と研究開発戦略

第1章及び第2章で分析したように、ICTは成長のエンジンとして機能し、我が国を取り巻く様々な社会的課題の解決に資するツールである。他方、ICTを有効に活用し、そのポテンシャルを引き出すためには、利用者が安心してICTを活用できる環境の整備は不可欠である。

また、ICTの持つポテンシャルを最大限に発揮するとの意味では、あらゆる産業に密接に関連するICT分野において、イノベーションを創出することが、我が国全体の成長につなげていく観点からも重要であり、イノベーション創出のための研究開発戦略は重要である。

本章では、今後、ビッグデータの活用を進めていく上で重要であるパーソナルデータの利用・流通の在り方や利用者が安心してICTを活用するための情報セキュリティに関する動きを紹介するとともに、ICTによるイノベーション創出のための研究開発戦略の検討状況について説明する。

第1節 ビッグデータ活用とパーソナルデータ

ICTの普及により、ライフログ[*1]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。

また、ICTの普及は、クラウドサービスなど国境を越えた情報の流通を極めて容易としており、国際的な調和の取れた、自由な情報の流通とプライバシー保護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。

本節では、海外でのパーソナルデータの活用に関する先進事例を紹介した後、現在、急速に普及するスマートフォンにおける利用者情報の収集に関する議論や、海外におけるパーソナルデータの取扱いに関する議論を紹介する。その後、各国政府や国際機関におけるパーソナルデータ保護に係る制度・政策の動きについて、米国及びEUを中心に紹介する。

続いて、我が国を含む6か国の利用者に対して行った、パーソナルデータの取扱いに係る利用者意識に関するアンケートの結果を紹介した後、我が国におけるパーソナルデータに係るルール作りに向けた総務省の取組について紹介する。

＊1　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。
＊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).

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

(1) 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（図表3-1-1-1）。

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、あるいは匿名化技術*4を適切な形で利用したりする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。

図表3-1-1-1　国内外におけるパーソナルデータ利活用の事例

分野	企業・団体	代表例
情報通信業	AT&T	・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
	Ericsson	・携帯電話回線のトラフィック状況に応じて動的な割引率を設定
	TomTom	・プローブ情報と携帯電話のGPS情報を統合解析して精度の高い交通情報をリアルタイム生成し、ナビゲーションに活用
金融業・保険業	Visa	・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
	Progressive	・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 ・事故リスクを元に、加入者個々人の運転状況に合わせた割引率を設定
	Cardlytics	・銀行と小売業者を仲介し、銀行の取引データに基づいてターゲティングした対象者にクーポンを配布
行政分野、公益事業	埼玉県	・自動車メーカー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
	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すプロジェクト
	ENEL	・2,500万台以上のスマートメータを設置、電力供給を自動マネジメント
その他	Shopperception	・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、顧客の行動を分析 ・販売時点のデータに加え、POB（Point of Buying）データを取得
	Walmart	・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
	TESCO	・顧客の購買履歴などの情報を収集・分析し、顧客にカスタマイズした商品案内やクーポンを提供

（出典）パーソナルデータの利用・流通に関する研究会資料より作成

(2) 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

ア　我が国の制度とこれまでの取組

(ア) 個人情報保護法の制定以前からのもの

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*5。また、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る*6。

公的部門のうち、地方公共団体では独自に個人情報保護条例を早くから制定しており*7、1980年（昭和55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）」*8が採択された後は、同勧告を参考に条例が制定されてきた*9。また、国の行政機関については、1988年（昭和63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」（昭和63年法律第95号）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。

(イ) 個人情報保護法の制定後のもの

A　個人情報保護法の制定

2003年（平成15年）5月に「個人情報の保護に関する法律」（平成15年法律第57号、以下「個人情報保護法」という。）が制定され、2005年（平成17年）4月に全面施行された。同時に「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、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

＊4　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。
＊5　「宴のあと」事件（東京地裁昭和39年9月28日判決）参照。
＊6　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）参照。
＊7　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。
＊8　OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980).
＊9　2013年1月現在では、すべ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。

関する法律を全面的に改正）や「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）も制定・施行された。また、2004年（平成16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。

B　総務省の取組

a　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」（平成16年総務省告示第695号）を改正し、さらに、2009年[*10]、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」（平成16年総務省告示第696号）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」（平成20年総務省告示第153号）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」（平成20年総務省告示第154号）を2008年に策定した。

b　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、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」を公表した。

C　消費者庁・消費者委員会の取組

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、関係行政機関からの報告を取りまとめ、その概要を公表及び消費者委員会への報告を行っており、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き、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、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、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。

D　その他の省庁の取組

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Ba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」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[*11]。

E　社会保障・税番号制度

社会保障・税番号制度（以下「番号制度」という。）は、複数の機関に存在する個人の情報を同一人の情報であるということの確認を行うための基盤であり、社会保障・税制度の効率性・透明性を高め、公平・公正な社会を実現するための社会基盤となるものである。平成25年通常国会において成立した「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」により、平成28年以降、個人番号の利用が開始されることとなった。

＊10　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。
＊11　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」。

イ　諸外国等の制度とこれまでの取組

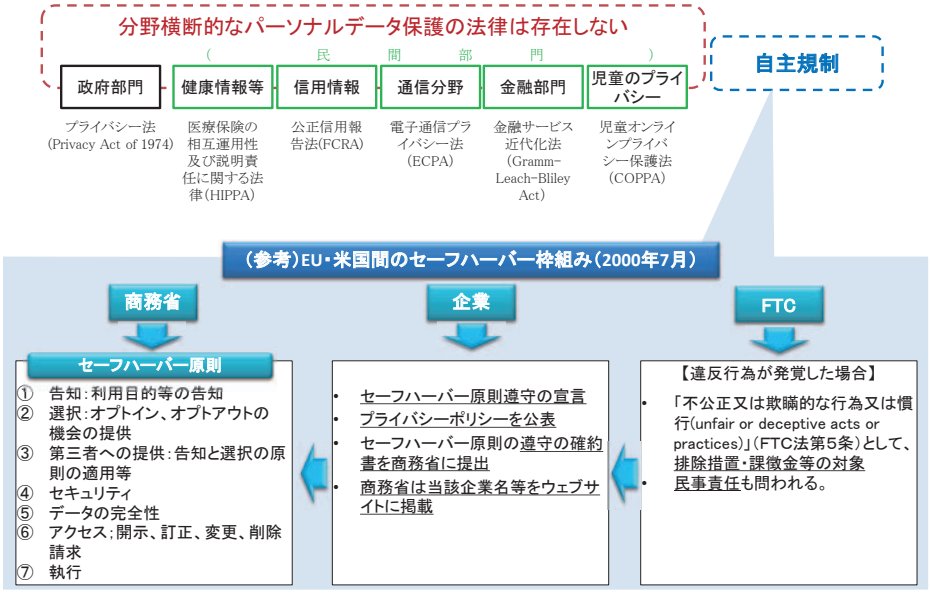
(ア) 米国

A　パーソナルデータ保護に関する制度

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（図表3-1-1-2）。

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連邦取引委員会（FTC）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Bのような政策提言を活発に行うとともに、後記（エ）のような国際的な場でも活発な活動を行っている。

図表3-1-1-2　米国のパーソナルデータ保護に関する制度

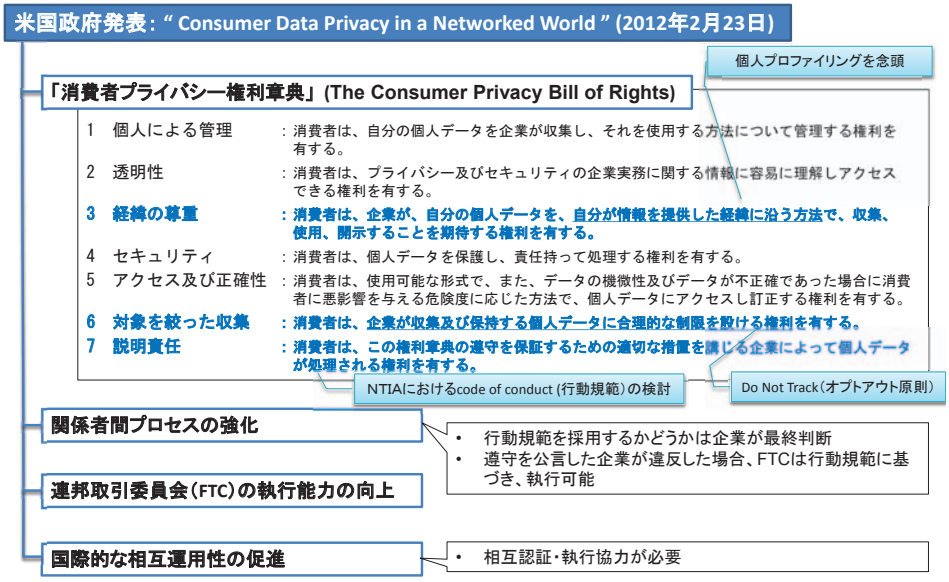


（出典）総務省「パーソナルデータの利用・流通に関する研究会報告書」

B　消費者プライバシー権利章典等の動向

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（Consumer Data Privacy in a Networked World: A Framework For Protecting Privacy and Promoting Innovation in the Global Digital Economy）」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（図表3-1-1-3）。

図表3-1-1-3　米国消費者プライバシー権利章典

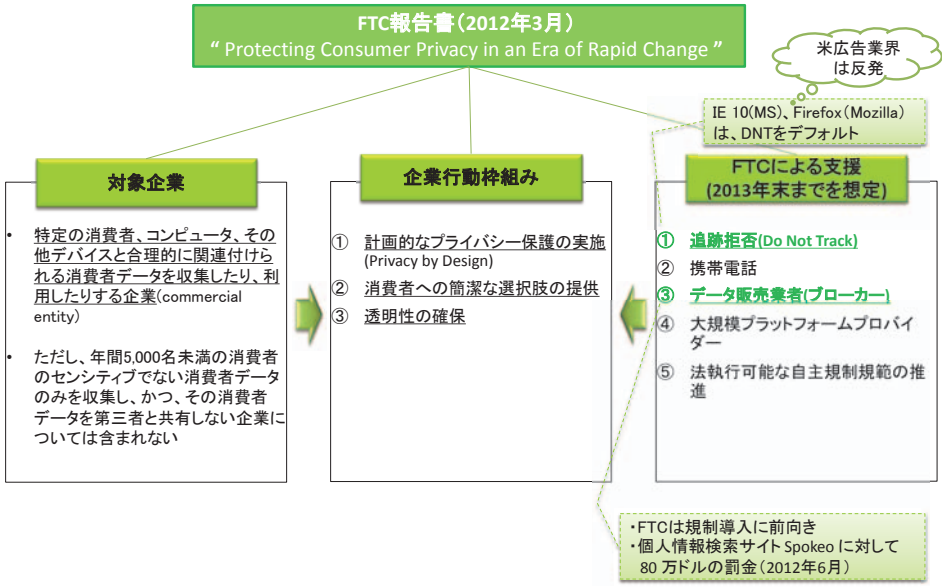


（出典）総務省「パーソナルデータの利用・流通に関する研究会報告書」

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」*12を発表した（図表3-1-1-4）。

図表3-1-1-4　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」



（出典）総務省「パーソナルデータの利用・流通に関する研究会報告書」

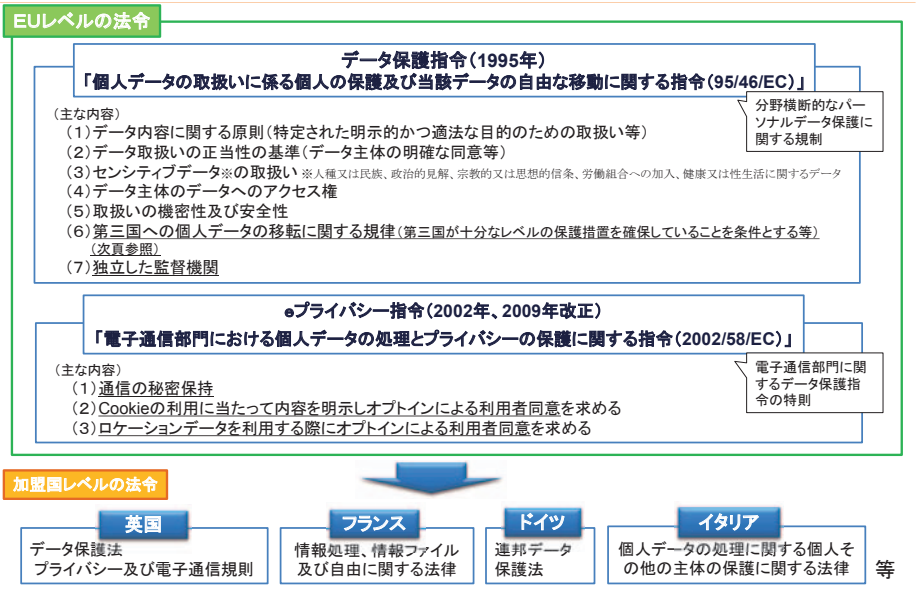
（イ）EU

A　データ保護指令

欧州では、1995年、分野横断的な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」*13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（図表3-1-1-5）。

同指令第28条は、各加盟国にパーソナル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 Protection Authority（DPA）と呼ばれることも多い。）が、各国内でパーソナルデータ保護の監督や後記（エ）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等が構成する機関（第29条作業部会（Article 29Working 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。

図表3-1-1-5　EUのパーソナルデータ保護に関する制度（現行制度）

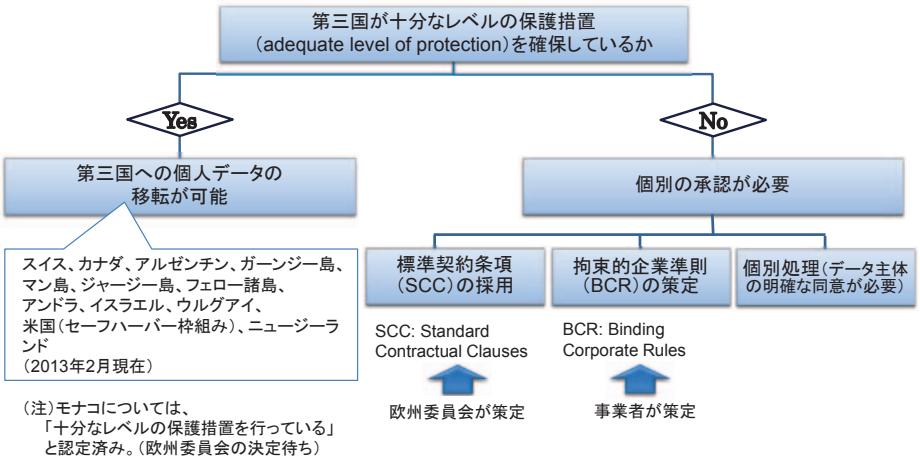


（出典）総務省「パーソナルデータの利用・流通に関する研究会報告書」

*12 Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change (2012).
*13 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.

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（図表3-1-1-6）、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」を挙げている*14*15。

図表3-1-1-6　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



（出典）総務省「パーソナルデータの利用・流通に関する研究会報告書」

B　eプライバシー指令

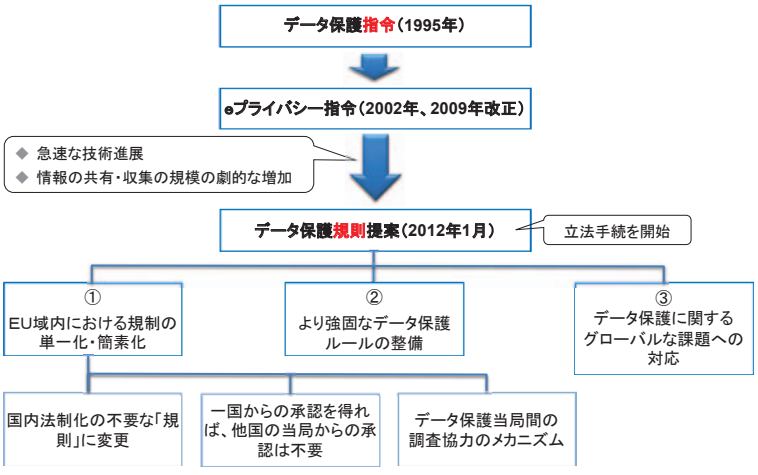
上記Aの分野横断的なデータ保護指令に加え、電子通信部門におけるパーソナルデータ保護に関する特則を規定するものとして、2002年に「電子通信部門における個人データの処理とプライバシーの保護に関する2002年7月12日の欧州議会及び理事会の2002／58／EC指令」*16が採択され、加盟国は当該指令を遵守するために必要な国内法の整備を義務づけられた*17（図表3-1-1-5）。

C　データ保護規則提案

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」*18を欧州議会及び理事会に提案・公表した。

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（図表3-1-1-7）。

図表3-1-1-7　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



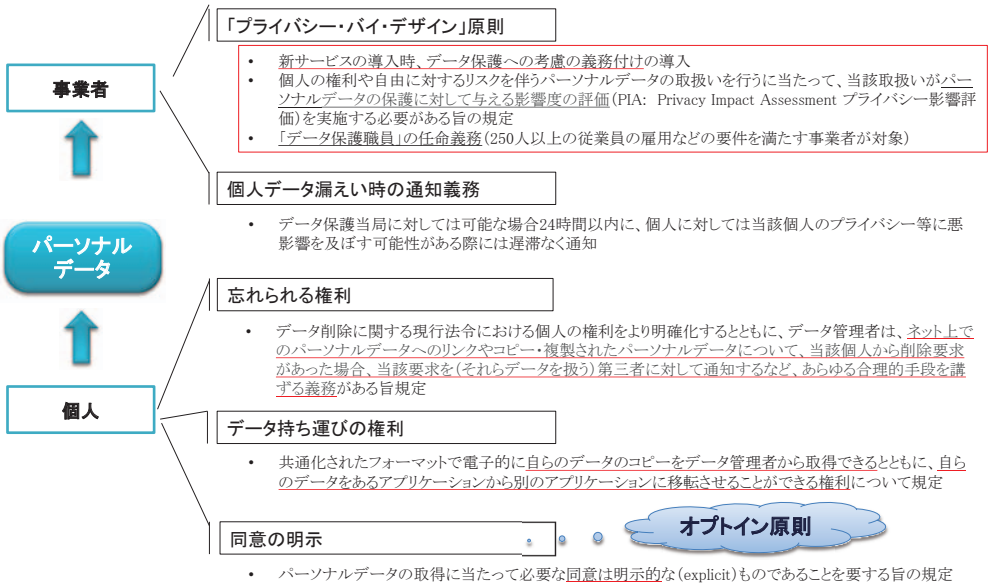
（出典）総務省「パーソナルデータの利用・流通に関する研究会報告書」

*14 Working Party on the Protection of individuals with regard to the Processing of Personal Data, Working Document : Transfers o1 personal data to third countries : Applying Article 25 and 26 of the EU Data Protection Directive (24 July 1998).
*15 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。
*16 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).
*17 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。
*18 前掲脚注2

データ保護規則提案の内容は、今後欧州議会及び理事会との議論の過程で大幅に修正される可能性はあるものの、同提案に盛り込まれている主な事項として、個人には、現行のEU指令に規定されているデータ削除に関する個人の権利をより明確化した「忘れられる権利」や、利用者がサービスを他のサービスに切り替える際など、管理者に妨害されることなく自分のデータを取得し、他のサービスに移転できる「データ持ち運びの権利」の保障、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であることを要する、いわゆるオプトイン原則を適用することとする「同意の明示」等がある。

また、サービス提供事業者に対しては、プライバシー・バイ・デザインの原則を適用し、新サービスの導入時におけるデータ保護への考慮の義務づけの導入やプライバシー影響評価の実施、データ保護職員の任命義務が盛り込まれているほか、パーソナルデータ漏えい時の通知義務も規定されている（図表3-1-1-8）。

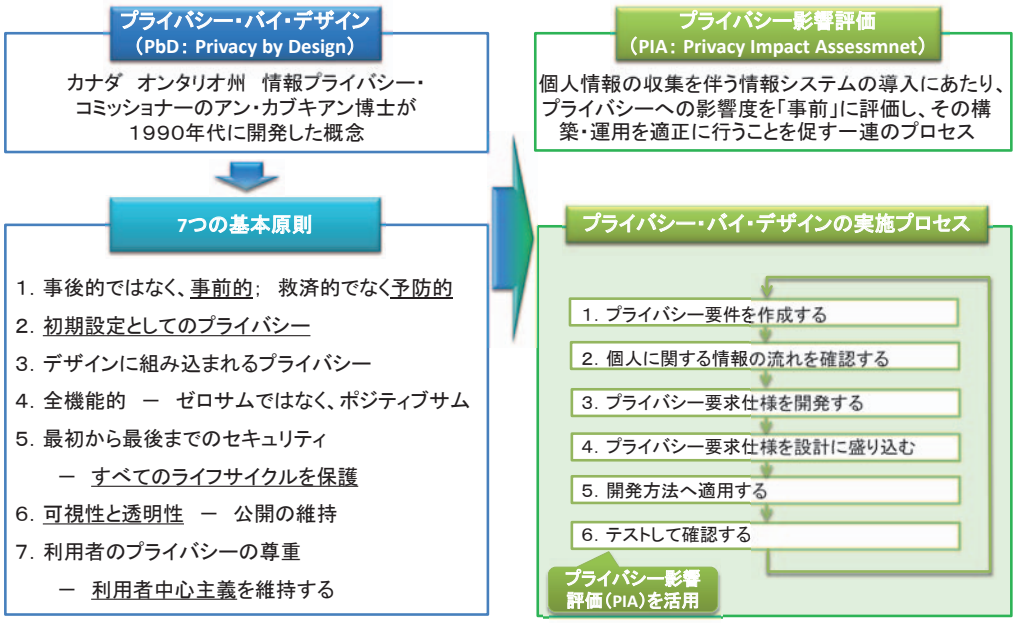
図表3-1-1-8　EUのパーソナルデータ保護に関する制度（データ保護規則提案）②



（出典）総務省「パーソナルデータの利用・流通に関する研究会報告書」

なお、プライバシー・バイ・デザインとは、サービスやアプリなどを開発する際、個人の情報を適切に扱うよう「設計段階で事前に作り込む」という考え方であり、7つの基本原則を定めている（図表3-1-1-9）。実施にあたっては、プライバシーへの影響度を事前に評価し、個人情報の収集を行う情報システムの構築・運用を適正に行うことを促す「プライバシー影響評価」を活用するものである。

図表3-1-1-9　「プライバシー・バイ・デザイン」

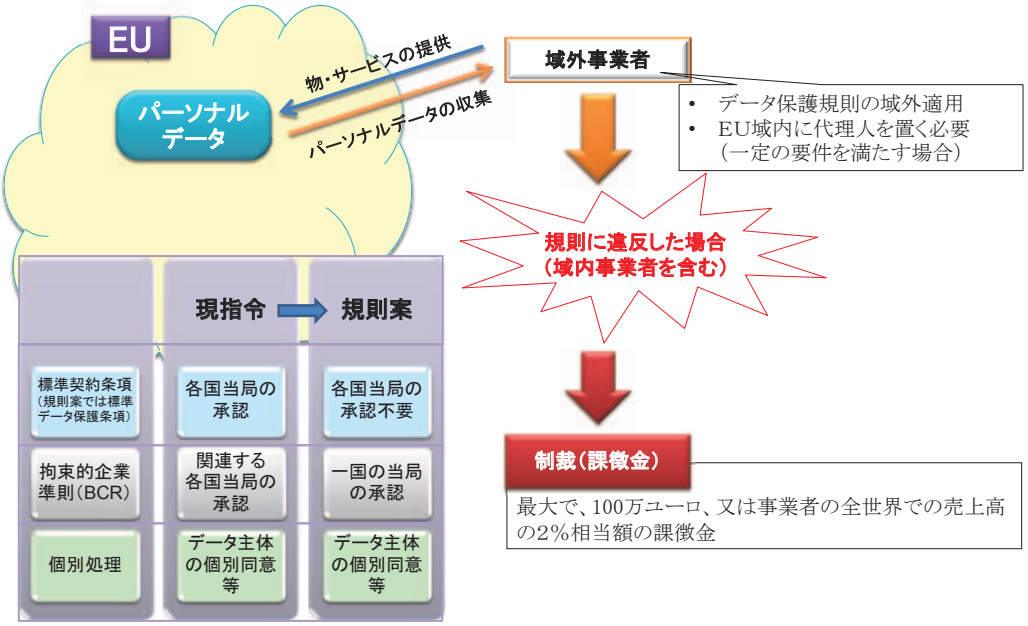


（出典）総務省「パーソナルデータの利用・流通に関する研究会報告書」

さらに、EU域外の事業者がEU域内のパーソナルデータを収集する場合には、データ保護規則の域外適用の対象となるほか、EU域内に代理人を置く必要が生じる場合がある。

そして、規則に違反した事業者は、域内・域外を問わず、最大で100万ユーロ、または事業者の全世界での売上高の2%に相当する課徴金が制裁として課せられるとの規定になっている（図表3-1-1-10）。

図表3-1-1-10　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



（出典）総務省「パーソナルデータの利用・流通に関する研究会報告書」

（ウ）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*19。

（エ）国際機関等

A　OECD

a　OECDプライバシーガイドラインとその改正

1980年、OECDは「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）を策定した*20。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（図表3-1-1-11））などを示したものである。同ガイドラインは、プライバシー保護の主要原則を初めて規定した国際約束であり、各国の個人情報保護法制及び国際的な取組に対し、長年強い影響を及ぼしてきた。

しかしながら、OECDプライバシーガイドラインは、パソコンやインターネットが普及する遥か昔の時代に策定されたものでもあることから、時代にそぐわない規定を修正し所要の規定を追加する必要性が高まってきた。よって、OECDにおいて、30年ぶりに同ガイドラインの改正を行うこととされており、2013年内又は2014年初めに改正案が採択される予定である。

*19　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か国・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か国・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か国・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)）。

*20　前掲脚注8

図表3-1-1-11　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 6.使用後のデータ廃棄 7.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原則の内容がすべて含まれていると述べられている。

（出典）総務省「パーソナルデータの利用・流通に関する研究会報告書」

b　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）[*21]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[*22]。

B　APEC

a　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（図表3-1-1-11）を定める枠組である。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。

b　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、情報の提供、調査等協力を依頼するための枠組である[*23]。2009年11月にAPEC閣僚会議で承認された。

c　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（国・地域）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（まだ、③の手続を済ませたエコノミーはまだない（米国が申請

＊21　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。

＊22　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か国及びEUのデータ保護当局等が参加している（日本は未参加）。

＊23　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か国・地域。

中)。(2013年5月現在))。

C　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、57か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（2012年現在)、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。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。

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*24。

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。
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。

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

APPAは、アジア太平洋地域各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、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。

E　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か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*25。

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）*26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46か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）*27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か国が同追加議定書を締結している。

＊24 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.)。
＊25 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)。
＊26 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data（Convention108).
＊27 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.

F　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に関する国際規格を担当している[*28]。

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。

（3）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

ア　スマートフォンにおける利用者情報の取扱い

パーソナルデータの利活用については、（1）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いる。例えば、この１～２年で急速に普及しているスマートフォンは、常に電源を入れてネットワークに接続した状態で持ち歩くことから、パソコンに比べて利用者との結びつきが強く、利用者の行動履歴や通信履歴等の多数の情報（図表3-1-1-12）を取得することも可能となっている。

図表3-1-1-12　スマートフォンにおける利用者情報の例

区分	情報の種類	含まれる情報
利用者の識別に係る情報	氏名、住所等の契約者情報	氏名、生年月日、住所、年齢、性別、電話番号等の情報や、クレジットカード番号等の個人信用情報等
	ログインに必要な識別情報	各種サービスをネット上で提供するサイトにおいて、利用者を特定するためにログインさせる際に利用される識別情報
	クッキー技術を用いて生成された識別情報	ウェブサイトを訪問時、ウェブブラウザを通じて一時的にパソコンに書込み記載されたデータ等[*29]
	契約者・端末固有ID	OSが生成するID（Android ID）、独自端末識別番号（UDID）、加入者識別ID（IMSI）、端末識別ID（IMEI）、MACアドレス等
第三者の情報	電話帳で管理されるデータ	氏名、電話番号、メールアドレス等
通信サービス上の行動履歴や利用者の状態に関する情報	通信履歴	通話内容・履歴、メール内容・送受信履歴
	ウェブページ上の行動履歴	利用者のウェブページ上における閲覧履歴、購買履歴、入力履歴等の行動履歴
	アプリケーションの利用履歴等	アプリケーションの利用履歴・記録されたデータ等、システムの利用履歴等
	位置情報	GPS機器によって計測される位置情報、基地局に送信される位置登録情報
	写真、動画等	スマートフォン等で撮影された[*30]写真、動画

（出典）総務省「スマートフォンプライバシーイニシアティブ」

スマートフォンにおける利用者情報へのアクセスについては、各OSにより異なる制限が行われている。また、アプリケーション提供サイト運営事業者により、掲載するアプリケーションについて、一定の審査やポリシーが存在している。一方、アプリケーションが利用者情報を収集するためのプログラムインタフェース（API）があらかじめ決まっており、APIを用いた情報収集は比較的容易である。また、収集した情報を含めネットワークに常時接続されるため、クラウドベースの外部サーバと連携したサービスの構築も容易である。

2011年（平成23年）夏頃から、スマートフォンにおける利用者情報の取扱いに関し、議論となった事例（図表3-1-1-13）が多く報道され、我が国においても利用者の関心が高まってきている。

図表3-1-1-13　アプリケーションによる利用者情報の収集に関し、議論となった報道事例

アプリ名	時期	概要
全国共有電話帳	2012年12月	「全国共有電話帳」は、昨年10月、76万人のデータが流出したと騒がれた「全国電話帳」のリメーク版。アプリを導入すると自分のアドレス帳に登録された情報が、登録者全員に共有される。自分自身は公開をOKしたとしても、アドレス帳に入っている知人友人、親兄弟は、まったくの無許可で公開されてしまう。
comm	2012年10月	「当社は、すべてのcomm会員記述情報を無償で複製その他あらゆる方法により利用し、また、第三者に利用させることができるものとします」との利用規約が問題とされた。規約は修正済み。
全国電話帳	2012年9月	アプリ自体は、ハローページとタウンページに掲載された情報を元に作成されているが、インストールした利用者のスマホに登録された電話番号や住所、メールアドレスなどが抜き取られ、利用者間で閲覧できる仕組になっていた。
アップティーピー	2012年4月	ユーザーの端末情報を無断で取得し、これをデータコンサルティングやターゲティング広告に利用した。
ビューン	2012年1月	電子書籍閲覧ソフトが、利用者が読んだ雑誌などの内容やページごとの閲覧時間を無断で記録し送信した。
マガストア	2012年1月	販売した電子書籍の書籍内の閲覧動向を収集した。
金魚すくいゲーム	2011年11月	全地球測位システム（GPS）で測定されたスマホの位置情報を１分間に１回、米国の広告会社に送信。アプリは端末の操作で楽しむ金魚すくいゲームで、ゲームに位置情報は必要ない。
産経新聞iPhone版	2011年11月	2011年11月に公開したアプリの最新版3.0.0に、利用者のページ閲覧履歴を収集し、サーバーに送信する機能が付いていることが明らかになった。
カレログ	2011年9月	恋愛支援アプリと称し、位置情報、バッテリー残量、アプリ一覧、通話記録の外部閲覧が可能であったため問題となった。

（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

＊28 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。

＊29 利用者のパソコン等にデータとして保存された識別符号（クッキー）に結びつけて、ウェブサーバー側等に、利用者に関する情報や最後にウェブサイトを訪れた日時、そのウェブサイトの訪問回数、ウェブサイト内履歴などを記録しておくことができる。

＊30 スマートフォンで撮影された写真の場合、設定により位置情報を含む場合もある。また、解像度の高い画像は、個人識別性を有する可能性があるとの指摘がある。

イ　海外におけるパーソナルデータの取扱い

パーソナルデータの取扱いをめぐり、海外では以下のような議論が生じている（図表3-1-1-14）。

（ア）OSによる位置情報の収集

2011年（平成23年）4月に利用者が位置情報サービスをオフに設定したときもiPhoneの位置情報について収集・記録されていることを研究者等が指摘したことを契機に、米国下院の議員がアップルに対してプライバシーの観点から説明を求める書簡を送付した。

同年5月にアップルのiOS搭載端末やグーグルのAndroid搭載端末において定期的に位置情報を収集・送信していることについて、米国上院司法委員会が公聴会を行い、アップル及びグーグルの代表者等が出席している。

（イ）グーグルによる新プライバシーポリシーの導入

2012年（平成24年）1月にグーグルは、同社全体で60以上あるプライバシーポリシーを同年3月1日より原則1つのプライバシーポリシーに統一すると発表した。これに対して、米国下院議員、米国の36の州・特別区等の司法長官、カナダのプライバシーコミッショナーが書簡を送付し、質問を行うとともに懸念を表明した。同様にEU個人データ保護作業部会議長、フランスの情報処理及び自由に関する国会委員会（CNIL）委員長がEUデータ保護指令へ違反する可能性を指摘し延期を求める書簡を送付した。その後、EU加盟24か国は、同年10月、グーグルに対し、同社が行っている個人情報の収集がプライバシー保護に問題があるとして、連名で改善を要請した。

また、我が国も個人情報保護法上の法令遵守及び利用者に対するわかりやすい説明等の対応をすることが重要である旨を文書で通知を行い注意喚起したほか、韓国が個人情報保護規定遵守の観点から勧告を行い、消費者による訴訟も提起されるなど、世界的に様々な動きが見られた。

図表3-1-1-14　パーソナルデータの取扱いをめぐって議論となった主な事例

	北　米	欧　州
2010年	12月： ウォールストリートジャーナルが、独自調査により、スマートフォンのアプリケーションによる利用者情報の取扱いについて、問題点を指摘する記事を掲載。	
2011年	4月： Pandora（インターネットラジオ視聴アプリ）が複数の広告会社へユーザー情報を送信していたことについて、米国連邦検事局が召喚状を発していたことが証券取引委員会に提出され書類により明らかになった。	
	5月： iOS及びAndroid OSによる位置情報取得が問題となり米国上院司法委員会の公聴会へアップル社、グーグル社の代表者が出席（端末の位置情報の取得方法及び履歴の保存方法等）。	
	12月： 「Carrier IQ」というネットワーク診断用ソフトウェアが一部のiPhone及びAndroid端末において端末内の利用者情報を取得し、Carrier IQ社への送信が疑われた問題。 連邦取引委員会（FTC）や連邦通信委員会（FCC）がCarrier IQ社に聞き取り調査。 アップル、AT&T、スプリント・ネクステル、T-Mobile、HTC、サムスンが採用を認める。	**ドイツ** Carrier IQについてバイエルン州のデータ保護規制当局がアップル等に対し、情報提供を求める。
	12月： モバイルマーケティングアソシエーション（MMA）は、アプリケーション開発者が消費者にプライバシーポリシーを分かりやすく伝えられるように配慮し「モバイル・アプリケーション・プライバシーポリシー」を発表。	
2012年	1月： グーグルの新プライバシーポリシーについて、8人の米国下院議員がグーグル社CEOのラリー・ペイジ氏宛てに書簡を送付し、質問を行うとともに懸念を表明。	**EU** 「個人データ保護規則」案を公表。
	1月： 携帯通信事業者の業界団体 GSMA(GSM Association）は、携帯端末向けのプライバシー原則（Mobile Privacy Principles)を発表し個人情報にアクセスし収集するアプリケーションやサービスを利用する消費者のプライバシーが尊重される必要があるとした。また、携帯端末向けアプリケーション開発におけるプライバシーデザインのガイドライン（Privacy Design Guidelines for Mobile Application Development）について発表した。	
	2月： ・iPhone用のSNSアプリ「Path」が電話帳情報等を利用者の同意を得ないままPathサーバーに送信していたとされる問題。アップル社は米国下院議員からの書簡を受け、ユーザー承認の必要性について見直しを検討。 ・グーグルの新プライバシーポリシーについて、米国の36の州・特別区等の司法長官がグーグル社CEOのラリー・ペイジ氏宛てに書簡を送付し、懸念を表明。 ・グーグルの新プライバシーポリシーについて、カナダのプライバシーコミッショナーが米グーグル社に書簡を送付し、質問を行うとともに懸念を表明。 ・米カリフォルニア州司法長官が、モバイルデバイス市場の大手6社（アップル、グーグル、アマゾン、マイクロソフト等）がプラットフォームを通じて提供するすべてのアプリについてプライバシーポリシーを明示的に提示すること等をこれらの企業と合意したことを発表。 ・FTCスタッフレポート「子供のためのモバイルアプリ」:アンドロイドOS及びiOSのアプリ各100ずつ（合計200）の調査結果として、「プライバシーに係る情報公開水準は不十分である」旨を発表。 ・ホワイトハウス「プライバシー権利章典」を発表（7箇条：①個人のコントロール、②透明性、③経緯の尊重、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）。	**EU** グーグルの新プライバシーポリシーについて、個人データ保護作業部会議長が、ラリー・ペイジ氏宛てに発効延期を求める書簡を送付。 **フランス**（CNIL） グーグルの新プライバシーポリシーについて、CNIL委員長がラリー・ペイジ氏宛てにEUデータ保護指令へ違反する可能性を指摘し、再度延期を求める書簡を送付。 **英国** ケンブリッジ大学コンピュータ研究所等によるAndroid向けアプリケーションの利用者情報の収集状況を分析。
	3月： ・グーグルの新プライバシーポリシーが1日付で発効。 ・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保護」:FTCがトラッキング拒否の簡易化等今後取り組む「5つの主要なエリア」を公表。	**フランス**（CNIL） がグーグルの新プライバシーポリシーについて、ラリー・ペイジ氏宛てに質問を送付。これに対し、グーグルは4月20日付で全質問に対し回答。
	・商業活動上のプライバシー及び個人情報の保護に関し、EU・米国が共同声明を発表。プライバシー保護に係る双方の取組を尊重すること、プライバシー侵害に関する共同監視、セーフハーバー協定の有効性等について確認されている。	
	5月： ・オンライン、モバイルメディアにおける広告及びプライバシー開示に関するワークショップ:FTCは、オンラインやモバイル環境における広告やプライバシー開示に関するベストプラクティスの考察など新たなガイダンスの必要性を考えることを目的として、官民の関係者を集めた会合を5月30日に開催。	

（出典）総務省「スマートフォンプライバシーイニシアティブ」

（ウ）その他の事例

2010年（平成22年）2月にグーグルのメールサービス「Gmail」の機能として組み込まれたソーシャルサービス「Google Buzz」において、利用者の事前の同意を取得することなく、Gmailで収集した情報をGoogle Buzzにおいて利用したことが議論の対象となった（その後、翌年11月に同サービスはGoogle＋に統合された。）。

また、2009年（平成21年）12月、フェイスブックは利用者が非公開に設定していた可能性のある「Friends List」などの情報を、利用者の事前同意を取得することなく、すべての利用者から閲覧可能とした。同社はこのほかにも、外部のアプリケーションソフト提供者が必要以上の個人データにアクセスできる状態にするなどしていた。

米国連邦取引委員会（FTC）は、これらのサービスが利用者に損害を及ぼす「不公正または欺瞞的行為」に該当すると判断し、両社に対して今後20年間にわたって総合的なプライバシー保護プログラムを実施し、第三者による隔年の監査等を義務づけるなどの是正措置を講じた。

ウ　我が国におけるパーソナルデータの利活用をめぐる課題

以上で述べたように、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[*31]。

各国で議論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。

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、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全体で適正な取扱いを確保する必要が生じているといえよう。

＊31 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。

2　パーソナルデータの取扱いに関する利用者意識の国際比較

総務省では、パーソナルデータの取扱いに係る利用者の意識について、各国で違いがあるか実態を把握するため、日本・米国・英国・フランス・韓国及びシンガポールの利用者を対象としたアンケート調査*32*33を実施したところ、その結果を以下に紹介する。

（1）パーソナルデータの取扱いに係る認識

保護されるべき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では「特定の個人を識別することができるもの」と定義しているところであるが、その中には氏名のように通常公にされている情報から、人に知られたくない情報まで、プライバシー性には違いがあるものと考えられる。

本アンケートでは、保護されるパーソナルデータについて利用者の意識を尋ね、その結果に関し、①一般パーソナルデータ（プライバシー性が高くないパーソナルデータ）、②慎重な取扱いが求められるパーソナルデータ（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）の3つに区分し*34、それぞれのデータの取扱いに係る利用者意識の比較を行った。

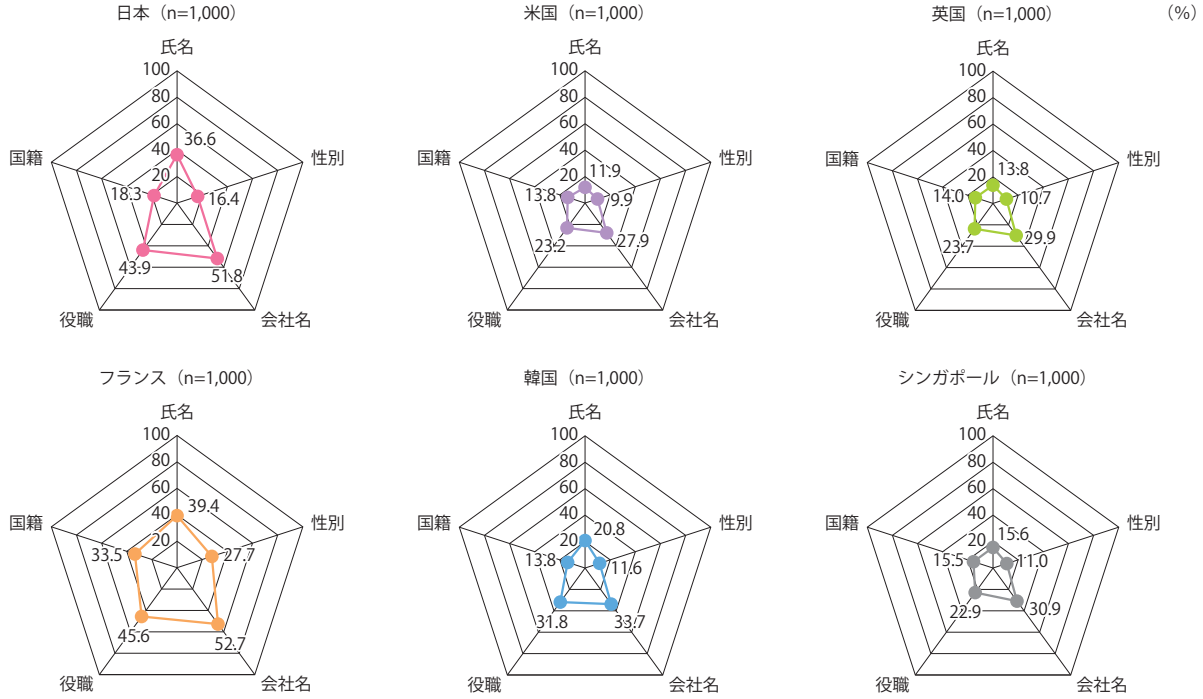
ア　一般パーソナルデータ

一般パーソナルデータとなる可能性があるものとして、ここでは、氏名、性別、会社名、役職及び国籍の5項目について、「当該情報をどんな場合でも提供・公開したくない」と回答した利用者がどの程度存在するか、図表3-1-2-1としてまとめた。

これらの情報は、全般的に「どんな場合でも提供・公開したくない」と回答した割合は低く出ているが、フランスは他国と比較した場合、「どんな場合でも提供・公開したくない」との回答が高く出る結果となっている。

特徴的な点は、レーダーチャートの形状が各国とも類似している点である。米国や英国では「提供・公開したくない」との回答がいずれのデータでも低く出ているのに対し、日本やフランスではいずれのデータでも高く出る結果となっている。つまり、特定のデータについて、ある国では極端に高いまたは低いという結果にはなっていない。

図表3-1-2-1　どのような場合でも提供・公開したくないデータ（一般パーソナルデータ）



（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

＊32　日本、米国、英国、フランス、韓国及びシンガポールの20歳以上の男女各1,000名（合計6,000名）を対象にウェブアンケートを実施。ネットアンケート調査会社が保有するモニターから、世代、男女比が均等になるよう抽出・割付を行った。
具体的には「インターネット接続・利用状況」、「パーソナルデータの範囲・利用・取扱いに係る意識」、「情報セキュリティに係る認識・意識・対策状況」などを主な調査項目として設計した。調査の概要は付注11参照。

＊33　アンケート調査の実施及び分析にあたっては、慶應義塾大学総合政策学部　新保史生教授及び筑波大学図書館情報メディア系　石井夏生利准教授の協力を得た。

＊34　データの区分に際しては、「パーソナルデータの利用・流通に関する研究会」における区分を参考にした。

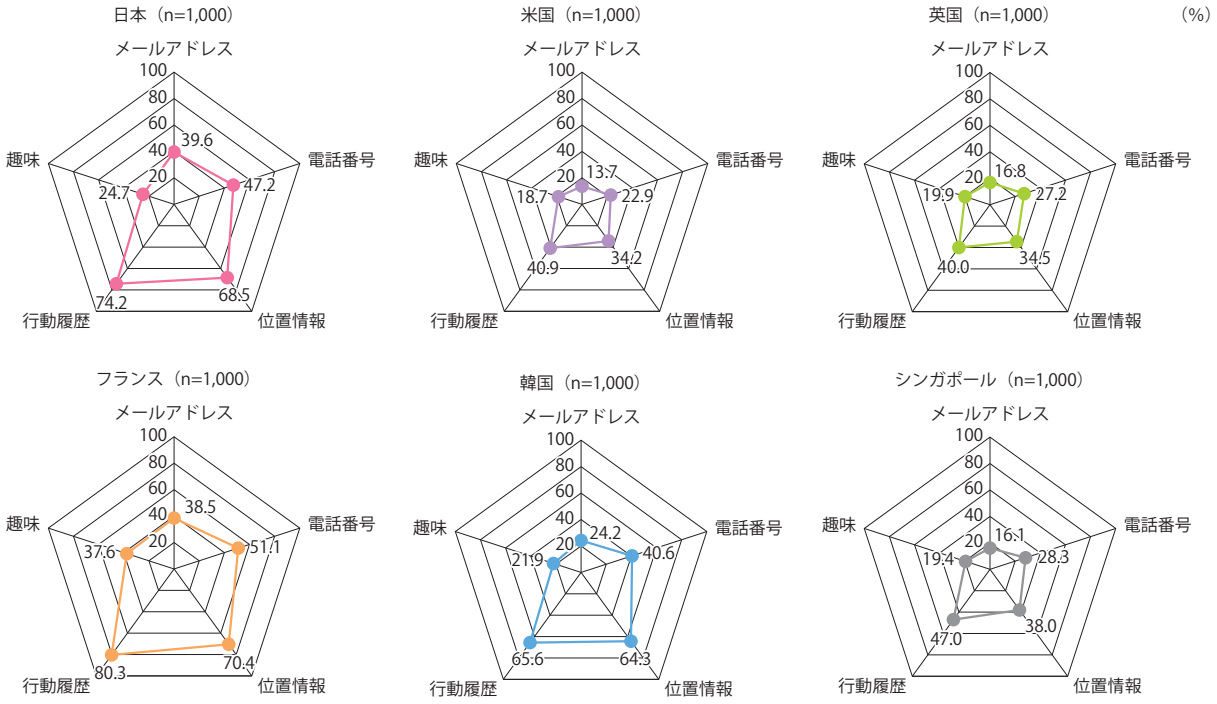
イ　慎重な取扱いが求められるパーソナルデータ

続いて、慎重な取扱いが求められるパーソナルデータとなる可能性があるものとして、ここではメールアドレス、電話番号、位置情報、行動履歴及び趣味の５項目について、「当該情報をどんな場合でも提供・公開したくない」と回答した利用者がどの程度存在するかについて比較を行った（図表3-1-2-2）。

いずれの国でもメールアドレスや趣味については、「どんな場合でも提供・公開したくない」との回答は比較的低く出ているのに対し、位置情報、行動履歴については、比較的高く出る結果となった。

国別で比較した場合、日本、フランス及び韓国では、「どんな場合でも提供・公開したくない」との回答が他の３か国より高く出る結果となっている。また、レーダーチャートの形状が各国とも類似している点についても、一般パーソナルデータの結果と同様である。

図表3-1-2-2　どのような場合でも提供・公開したくないデータ（慎重な取扱いが求められるデータ）



（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

ウ　センシティブデータ

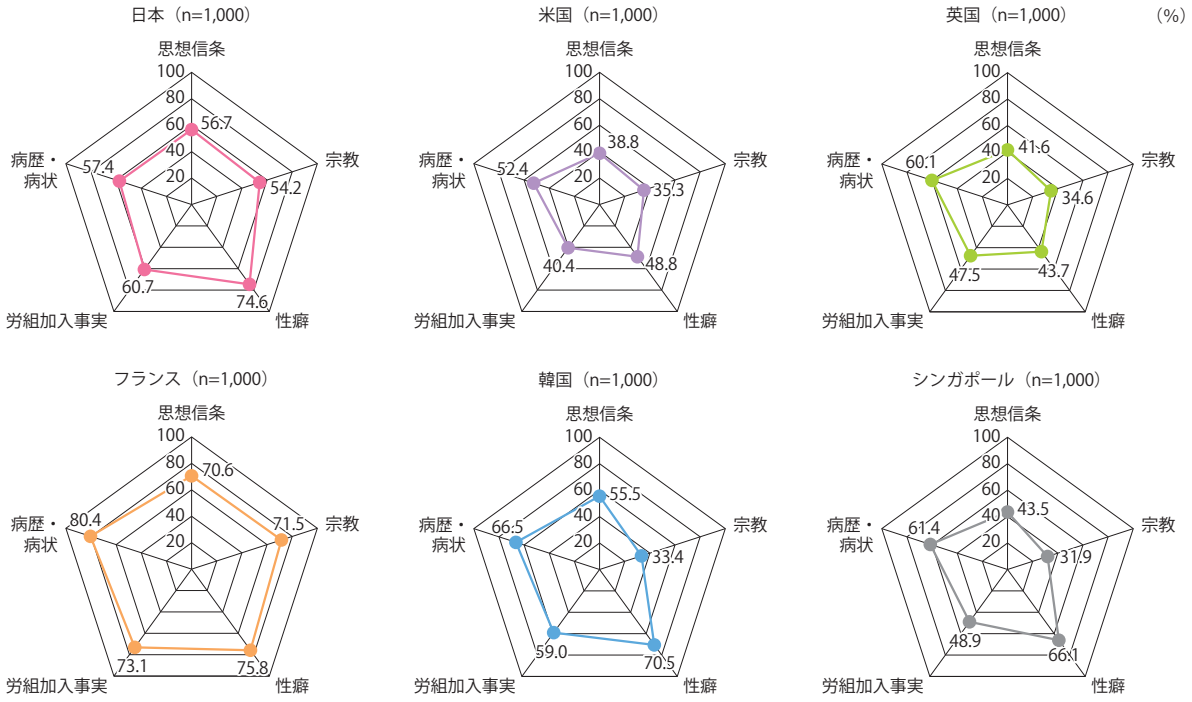
さらに、センシティブデータと考えられるものとして、ここでは思想信条、宗教、性癖、労組加入事実及び病歴・病状の５項目について、「当該情報をどんな場合でも提供・公開したくない」と回答した利用者がどの程度存在するかについて比較を行った（図表3-1-2-3）。

センシティブデータは他のデータに比べて、どの国でも「どんな場合でも提供・公開したくない」と回答した割合は高めに出ている。また、米国や英国ではいずれの項目も比較的低く出ているのに対し、フランスではいずれの項目も比較的高く出る傾向は、一般パーソナル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の場合と同様である。

５項目の中で比較すると、米国、英国及びフランスでは病歴・病状を「どんな場合でも提供・公開したくない」と回答した割合が他の項目と比べて高いのに対し、日本、韓国及びシンガポールでは性癖が最も高い結果となった。

なお、レーダーチャートの形状がいずれの国も近似している点は、一般パーソナル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の場合と同様である。

図表3-1-2-3　どのような場合でも提供・公開したくないデータ（センシティブデータ）



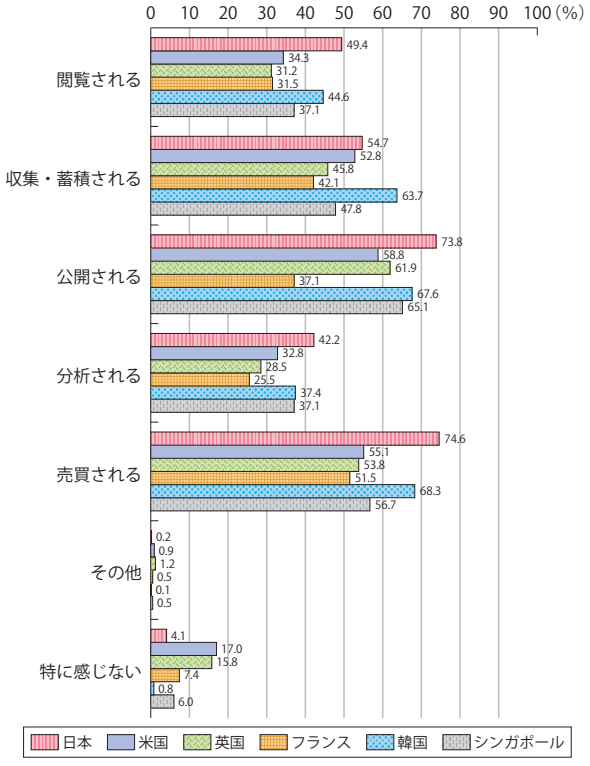
（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

（2）サービス提供事業者の利用方法に対する利用者の意識

サービス提供事業者からサービス利用者に対し、サービス向上等を理由にパーソナルデータの利用を求められた場合、どのような利用方法に対して抵抗感を感じるかについて、6か国で比較を行った。

その結果、日本では、閲覧、収集・蓄積、公開、分析、売買等、いずれの利用方法においても、他の国と比較すると「抵抗を感じる」という回答の割合が高い。特に欧米と比較すると、様々な行為に対して抵抗を感じるという結果となっている（図表3-1-2-4）。

図表3-1-2-4　サービス提供事業者によるパーソナルデータの利用方法のうち、抵抗感を感じる方法



いずれの国も n=1,000

（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

（3）パーソナルデータの取扱いに関する許容範囲

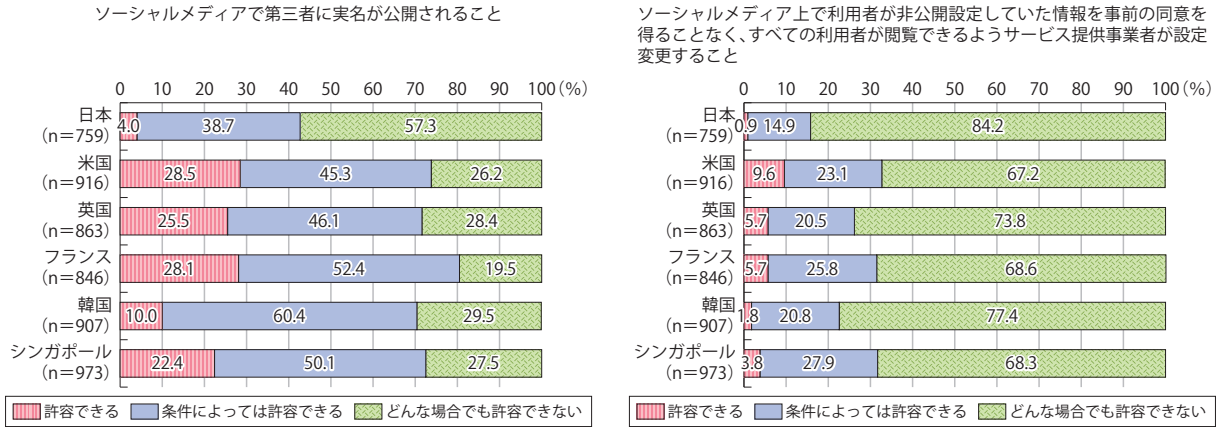
ソーシャルメディアや電子商取引、ビッグデータ等の利用場面におけるパーソナルデータの取扱いについて、6か国の利用者に対し、許容できるか否かについて尋ねた。

ア　ソーシャルメディア利用の際のパーソナルデータの取扱いに関する意識

「ソーシャルメディアで第三者に実名が公開されること」については、日本が他の5か国より抜きんでて「どんな場合でも許容できない」との回答が高い結果となった。

「ソーシャルメディア上で利用者が非公開設定していた情報を事前の同意を得ることなく、サービス提供事業者がすべての利用者が閲覧可能なように設定変更すること」については、いずれの国でも「どんな場合でも許容できない」との回答が高い結果となった（図表3-1-2-5）。

図表3-1-2-5　パーソナルデータの取扱いに関する許容範囲（ソーシャルメディア利用時）



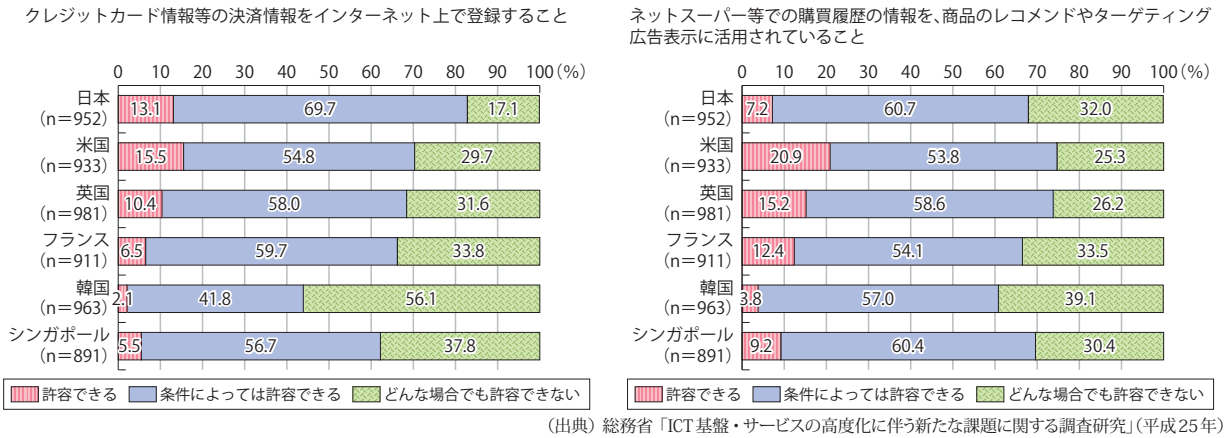
（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

イ　インターネットショッピングを利用する際に登録したパーソナルデータの取扱いに関する意識

「クレジットカードの決済情報をインターネット上で登録すること」については、韓国では56.1％が「どんな場合でも許容できない」と答えたのに対し、日本では17.1％にとどまっている。

また、購買履歴を商品のレコメンドやターゲティング広告表示に活用することについては、いずれの国も3割前後が「どんな場合でも許容できない」との回答であった（図表3-1-2-6）。

図表3-1-2-6　パーソナルデータの取扱いに関する許容範囲（インターネットショッピング利用時）



（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

ウ　ビッグデータ関連サービスへの意識

続いて、ビッグデータ関連サービスに対する利用者の意識を尋ねた（図表3-1-2-7）。

まず、異なるサービスで登録されたパーソナルデータが関連づけられることについては、どの国も4割前後の利用者が、また、会員登録サービスにパーソナルデータを登録した場合、別のサービス提供事業者が当該データを利用することについては、5割前後の利用者が「どんな場合でも許容できない」としている。いずれもフランスでは「許容できない」の割合が、他の国より高く出ている。

「取得した位置情報をもとに近隣のお勧め情報がスマートフォン等の携帯端末に通知されること」は、アジア圏では「許容できる」、「条件によっては許容できる」といった回答が半数を占める結果となった。

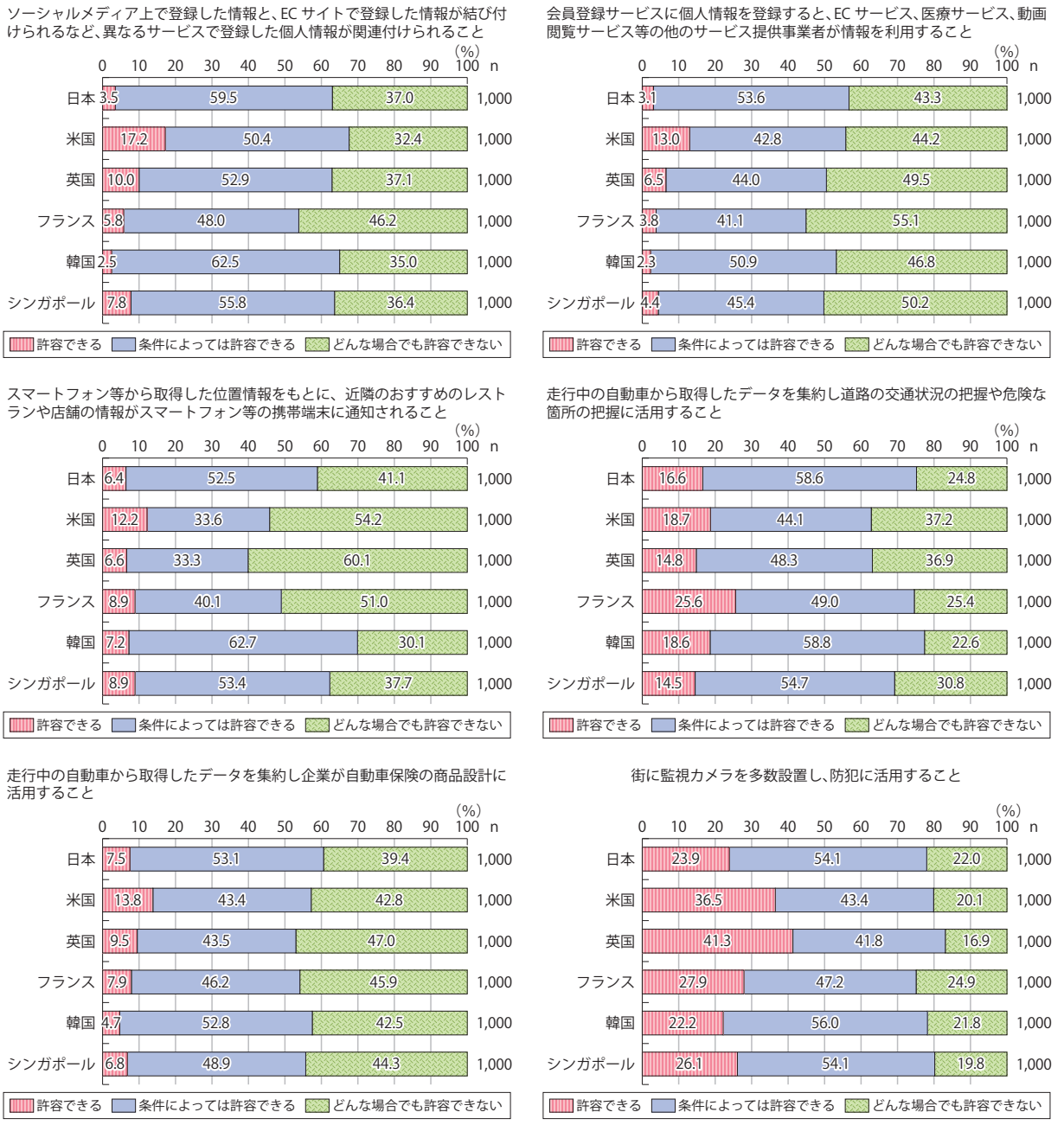
「走行中の自動車から取得したデータを集約し交通状況の把握や危険な箇所の把握に活用すること」については、いずれの国も６割以上が「許容できる」、「条件によっては許容できる」と回答したが、「走行中の自動車から取得したデータを集約し企業が自動車保険の設計に活用すること」については、それをやや下回る結果となっている。

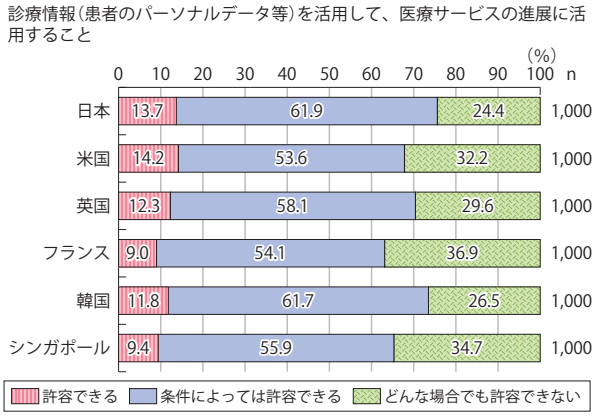
「街に監視カメラを多数設置し、防犯に活用すること」については、いずれの国も８割前後が「許容できる」「条件によっては許容できる」と回答している。

「診療情報（パーソナルデータ）を医療サービスの進展に活用すること」については、いずれの国も６割以上が「許容できる」、「条件によっては許容できる」と回答している。

このように具体的な利用イメージがあり、かつ、特に安心・安全の観点から利用者にとってメリットがあると思われる利用方法については、利用者の抵抗感は小さいという結果になった。

図表3-1-2-7　パーソナルデータの取扱いに関する許容範囲（ビッグデータ関連サービス）





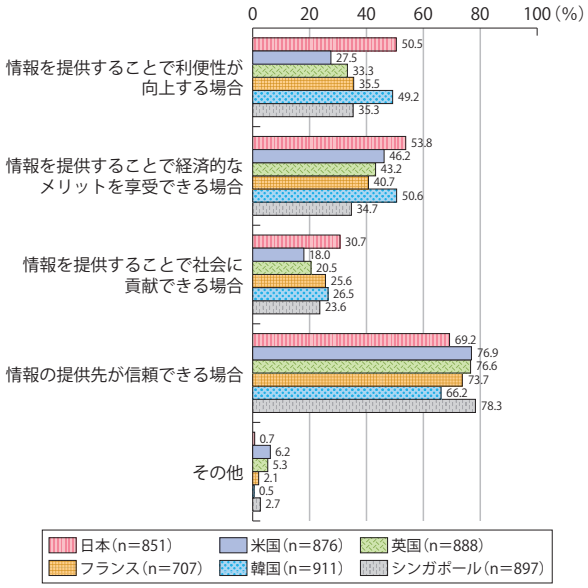
（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

（4）サービス提供事業者にパーソナルデータを提供する条件

パーソナルデータをサービス提供事業者に提供する条件を尋ねたところ、全体的な傾向としては「情報の提供先が信頼できる場合」であれば提供しても良いという回答がどの国においても多い結果になった（図表3-1-2-8）。

国ごとに比較すると、日本では、「情報を提供することで経済的なメリットを享受できる場合」と「情報を提供することで利便性が向上する場合」が回答の５割を超えて高い特徴が見られる。なお、この傾向は韓国も類似している。

図表3-1-2-8　パーソナルデータをサービス提供事業者に提供する条件

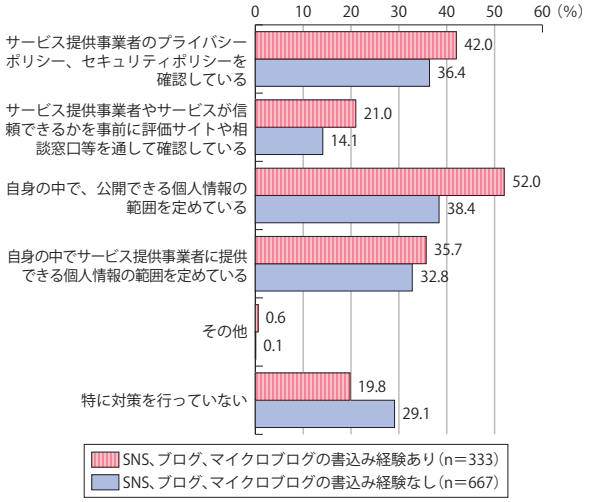


（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

（5）パーソナルデータ保護のための対策の実施状況（日本のみ）

パーソナルデータの保護のために日常から対策を講じているか否かについて、我が国の利用者に限って、SNS、ブログ及びマイクロブログへの書き込み経験の有無により、どの程度差が生じるか分析を行った。その結果、これらへの書き込み経験を有する利用者は経験を有しない利用者に比べ、いずれの対策についても、「講じている」と回答した割合が高く出る結果となった（図表3-1-2-9）。

図表3-1-2-9　パーソナルデータ保護のために日常から講じている対策



（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

（6）スマートフォンにおける利用者情報収集に関する意識

スマートフォンにおける利用者情報の収集が議論になっていることは先に述べたが、そのような利用者情報の取扱いに関する利用者の意識について尋ねた（図表3-1-2-10）。

利用承諾を求める画面の認知度は、韓国が78.2%、日本は69.7%と高かったのに対し、フランスは54.3%とやや低い結果が出た。

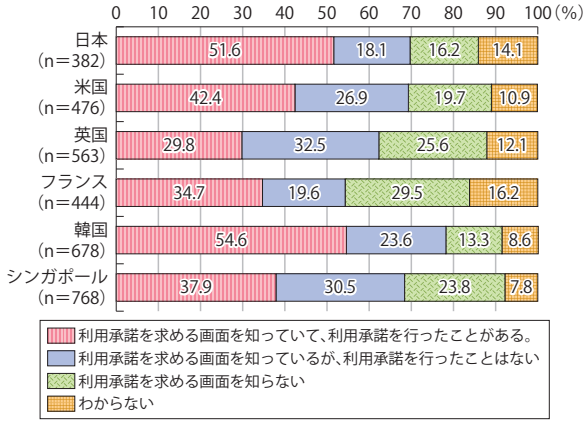
スマートフォンに保存されている利用者情報がサービス提供事業者からアクセスされることについては、3割以上が「どんな場合でも許容できない」と回答している。特にフランスでは52.7%がそのように回答している。

スマートフォンを利用するようになって、利用者情報への意識に変化があったかを聞いたところ、韓国やシンガポールでは「取扱いに敏感になった」、「登録を控えるようになった」との回答の合計が6割を超える結果となった。日本を含め他の国でも5割を超えている。

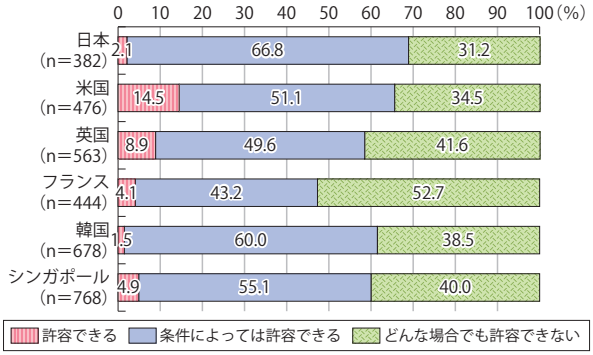
スマートフォンのアプリ利用時にサービス提供事業者がポリシー変更を行うことについては、日本を含む5か国では「利用者の同意を得た上で変更するならば問題ない」との回答が最も多かったが、米国は「サービス提供事業者が変更点を明確にすれば問題ない」との回答が最も多い結果となった。

図表3-1-2-10　スマートフォンにおける利用者情報の取扱いに関する意識

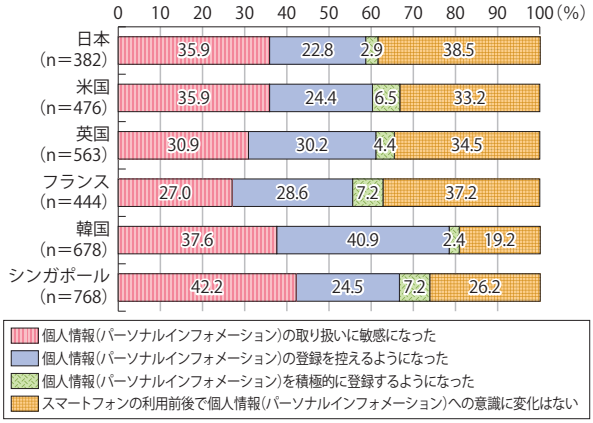
「収集する利用者情報に関する利用許諾」を求める画面が提示されることを知っているか。この画面を読んで、アプリケーションを使う前に承諾・同意を行ったことはあるか。



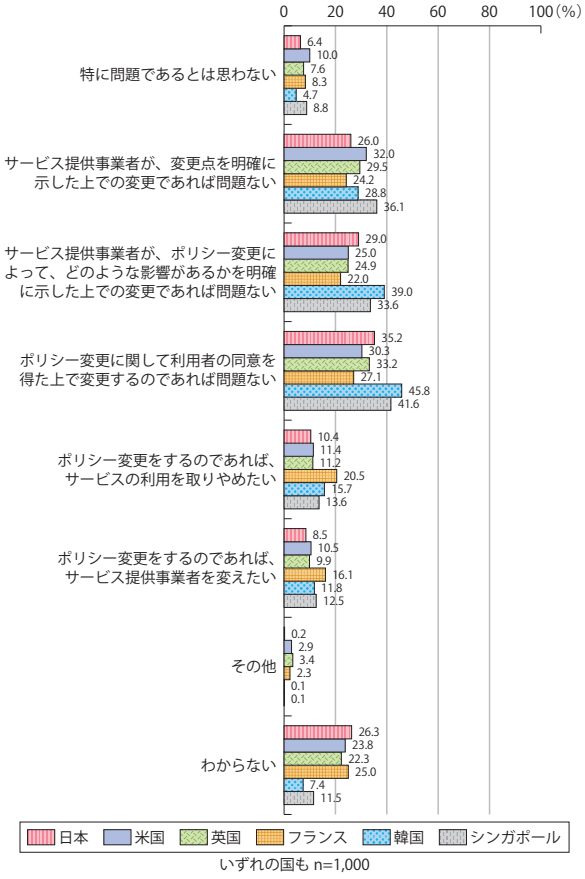
スマートフォンに保存されている個人情報（パーソナルインフォメーション）が、サービス提供事業者にアクセスされている可能性があることについてプライバシーの観点からどのように感じるか。



スマートフォンを利用し始めて、個人情報（パーソナルインフォメーション）の取り扱いに関する意識は変化したか。



スマートフォンのアプリケーションを利用する際に、サービス提供事業者が利用規定を変更するなど、ポリシー変更を行う場合があることについてどのように感じるか。



（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

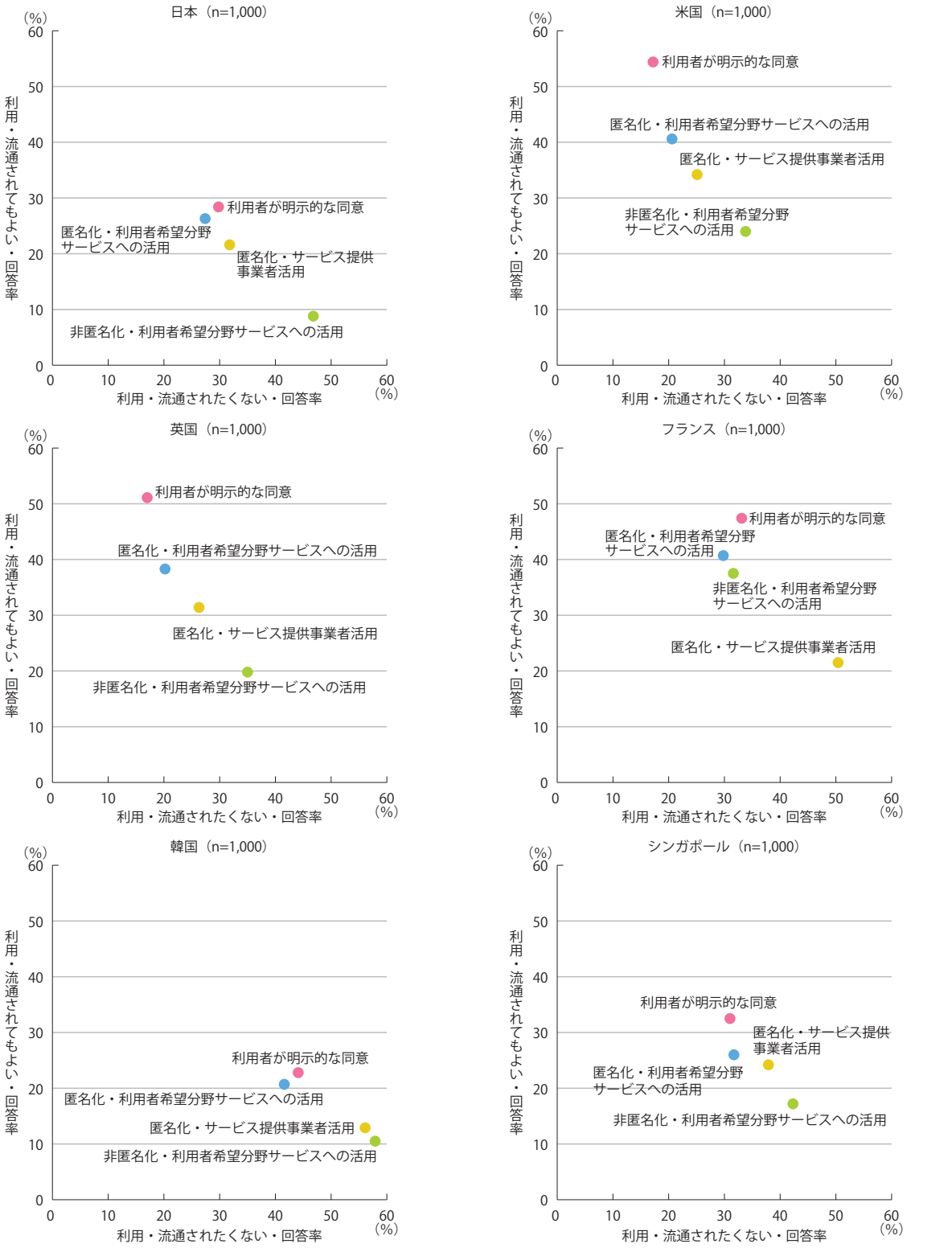
（7）パーソナルデータの利用・流通のための条件

パーソナルデータの利用・流通のための条件について、「利用者が明示的な同意を行った場合」、「サービス提供事業者が匿名化を行った場合」、「サービス提供事業者が匿名化を行った上で、利用者が希望する分野・サービスに限って活用する場合」、「利用者が希望する分野・サービスにおいて、匿名化を行わない場合」の4つの条件について、それぞれの場合において、パーソナルデータの利用・流通を認めるかを各国の利用者に尋ねた。その結果について、「利用・流通されても良い」回答率と「利用・流通されたくない回答率」の関係性を図式化したのが、図表3-1-2-11である。

いずれの国も「利用者が明示的な同意を行った場合」において、「利用・流通されても良い」回答率が最も高くなる結果となった。ただし、欧米では5割前後に達するのに対し、アジアでは3割程度にとどまった。

続いて、フランス以外では、「サービス提供事業者が匿名化を行った上で、利用者が希望する分野・サービスに限って活用する場合」、「サービス提供事業者が匿名化を行った場合」の順に「利用・流通されても良い」回答率が高くなる結果となったのに対し、フランスでは「サービス提供事業者が匿名化を行った場合」より「利用者が希望する分野・サービスにおいて、匿名化を行わない場合」の方が「利用・流通されても良い」回答率が高くなり、匿名化という保護手段よりも利用目的を優先させる傾向にあることがうかがえる。

図表3-1-2-11　パーソナルデータの利用・流通のための条件

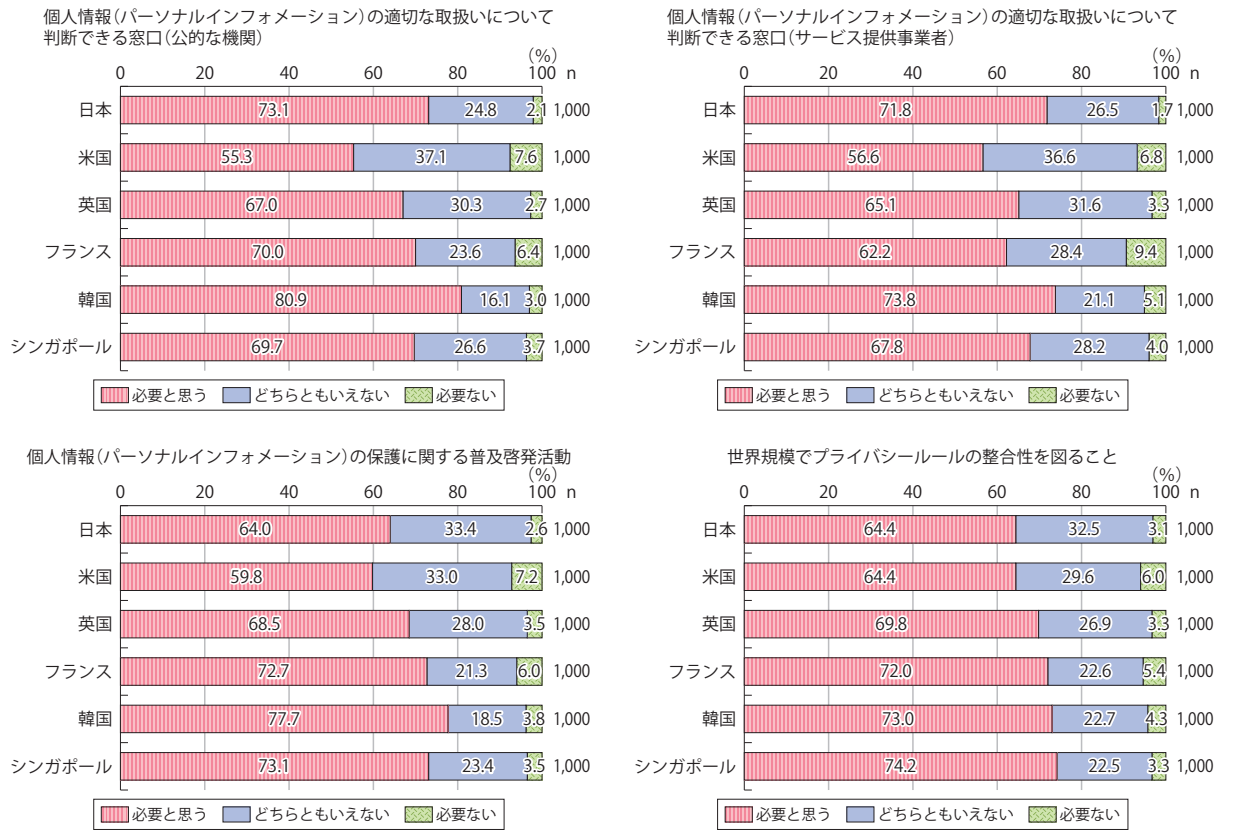


（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

(8) プライバシー保護のために必要と思う政策

プライバシー保護のために必要と思う政策について各国の利用者に尋ねたところ、「公的な機関またはサービス提供事業者における個人情報の適切な取扱いを判断できる窓口の設置」、「個人情報の保護に関する普及啓発活動」、「世界規模でプライバシールールの整合性を図ること」のいずれにおいても、「必要である」との回答が最も高くなった（図表3-1-2-12）。

図表3-1-2-12　プライバシー保護のために必要と思う政策



（出典）総務省「ICT基盤・サービスの高度化に伴う新たな課題に関する調査研究」（平成25年）

以上の結果から、我が国利用者の意識の特徴をまとめると、パーソナルデータについて「どのような場合でも公表したくない」と回答する割合は、米国・英国に比べると高めである。プライバシー侵害の経験を有する回答者は約2割で、パーソナルデータを保護するために日常から対策を実施している割合も低い。また、閲覧、公開、分析、売買等の様々な行為に対して「抵抗を感じる」という回答の割合が高く、どの行為が違反となるかその境界が曖昧な傾向が見られる。

パーソナルデータをサービス提供事業者に提供する条件として、いずれの国でも全体的な傾向としては「情報の提供先が信頼できる場合」であれば提供しても良いとの回答であるが、我が国では、「情報を提供することで経済的なメリットを享受できる場合」と「情報を提供することで利便性が向上する場合」が回答の5割を超えて高い傾向がある。

パーソナルデータを取り扱う事業者が、どのような対応をすればパーソナルデータを登録し、利用・流通されても良いかについて尋ねた設問の結果を見ると、日本においては、明示的な同意や匿名化・暗号化をすれば、2～3割の回答者がパーソナルデータを「利用・流通されても良い」としている。

3　政府の取組

（1）IT総合戦略本部の取組

本年6月にIT総合戦略本部において決定した新しいIT戦略「世界最先端IT国家創造宣言」において、ビッグデータを活用した新産業・新サービスの創出を促進する上で、特に利用価値が高いと期待されている「パーソナルデータ」の取扱いについては、①その利活用を円滑に進めるため、個人情報及びプライバシーの保護との両立を可能とする事業環境整備を進めること、②また、環境整備に当たっては、プライバシーや情報セキュリティ等に関するルールの標準化や国際的な仕組作りを通じた利便性向上及び国境を越えた円滑な情報移転が重要であり、OECD等国際交渉の場を活用し、国際的な連携を推進すること、③既に、スマートフォンの利用者情報の取扱いなど先行的にルール策定が行われた分野については、取組の普及を推進することが盛り込まれている。

また、「世界最先端IT国家創造宣言」では、速やかに、IT総合戦略本部の下に新たな検討組織を設置し、個人情報やプライバシー保護に配慮したパーソナルデータの利活用のルールを明確化した上で、個人情報保護ガイドラインの見直し、同意取得手続きの標準化等の取組を年内できるだけ早期に着手するほか、新たな検討組織が、第三者機関の設置を含む、新たな法的措置も視野に入れた、制度見直し方針（ロードマップを含む）を年内に策定することとされている。

さらに、2014年以降に、制度見直し方針に示されたロードマップに従って、国際的な連携にも配慮しつつ、順次パーソナルデータ利活用環境を整備し、利活用を促進することとされている。

（2）総務省の取組－パーソナルデータの利用・流通に関する研究会の開催－

総務省では2012年（平成24年）11月より「パーソナルデータの利用・流通に関する研究会」を開催した。同研究会の報告書では、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及びその実現のための方向性が以下のとおり提示された。なお、詳細は同研究会報告書[*35]を参照されたい。

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

（ア）パーソナルデータの利活用の枠組の体系

A　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。

B　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

＊35 http://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000071.html

（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*36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。

イ　パーソナルデータの利活用の枠組の本格的な実施のための方向性（図表3-1-3-1）

（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、我が国の実用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。

＊36 オプトアウトの意思表示とは、本人の同意なく第三者に個人情報が提供される場合において、第三者への提供をやめるよう、本人（その個人情報によって識別される特定の個人）が意思表示を行うこと。

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。

図表３-１-３-１　パーソナルデータの利活用の枠組の本格的な実施

・事業者の自主的な取組みや現行制度の運用改善等では、法的拘束力が十分でなく、**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。

・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寄与。

以下の事項について、**政府全体として速やかに検討**を進めていくことが必要

○我が国におけるプライバシー・コミッショナー制度

・パーソナルデータに関し、国民の信頼を確保し、実質的な判断を行う、**専門的な知見を有する人材が、分野横断的に迅速かつ適切に処理していく体制の整備**が不可欠

・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・コミッショナーを設置している国**が、**欧米など先進国を始め国際的には多数**

これを前提に、**各国のプライバシーコミッショナーが意見表明・調整を行う体制が国際的に形成**されている。

・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、ＥＵと我が国の間のパーソナルデータの自由な流通に支障

○マルチステークホルダープロセス等の実効性の確保

・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**整備

・**マルチステークホルダープロセスに参加する企業**への**インセンティブ**

・**マルチステークホルダープロセスに参加しない企業**にも**プライバシー保護を確保**するための仕組み

○現行の個人情報保護法に関する制度整備

・小規模事業者の扱い、共同利用の在り方、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等