資料１

個人情報保護法
いわゆる３年ごと見直しに係る
検討の中間整理
（案）

平成31年４月25日

個人情報保護委員会

目次

【凡例】

平成27年改正法	個人情報の保護に関する法律及び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の一部を改正する法律（平成27年法律第65号）
委員会	個人情報保護委員会
個人情報保護法	個人情報の保護に関する法律（平成15年法律第57号）
ＧＤＰＲ	ＥＵが2016年（平成28年）４月に制定した「一般データ保護規則（General Data Protection Regulation)」。ＥＵ域内の個人データ保護を規定する法として、1995年（平成７年）から適用されている「ＥＵデータ保護指令（Data Protection Directive 95)」に代わり、2018年（平成30年）５月25日に施行。
番号法	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（平成25年法律第27号）
次世代医療基盤法	医療分野の研究開発に資するための匿名加工医療情報に関する法律（平成29年法律第28号）
委員会規則	個人情報の保護に関する法律施行規則（平成28年個人情報保護委員会規則第３号）

第１章　総論

平成27年改正法制定以降の社会・経済情勢の変化を踏まえ、本年１月28日に示した「いわゆる３年ごとの見直しに係る検討の着眼点」に即していわゆる３年ごと見直しを進めてきた。個々の着眼点にはそれぞれに固有の論点はあるものの、全体を俯瞰するならば、おおむね、次のような共通の視点を示すことができる。

第一に、情報を提供する個人の、自らの情報の取扱いに対する関心や、関与への期待が高まっており、個人情報保護法第１条の目的に掲げている「個人の権利利益を保護」するために必要十分な措置を整備することに配意しながら制度を見直すことが必要である。

第二に、平成27年改正法で特に重視された保護と利用のバランスをとることの必要性は、引き続き重要であり、個人情報や個人に関連する情報を巡る技術革新の成果が、経済成長等と個人の権利利益の保護との両面で行き渡るような制度であることが必要である。

第三に、デジタル化された個人情報を用いる多様な利活用が、グローバルに、展開されており、国際的な制度調和や連携に配意しながら制度を見直すことが必要である。

第四に、海外事業者によるサービスの利用や、個人情報を扱うビジネスの国境を越えたサプライチェーンの複雑化などが進み、個人が直面するリスクも変化しており、これに対応し得る制度へと見直すことが必要である。

なお、制度の見直しに当たり、個人情報を巡っては、技術的側面、社会的側面において、急激な変化が進展しており、その傾向が更に強まると見込まれることを踏まえ、制度を見直す上では、可能な限り様々なリスクを考慮の上対応することも重要である。また、新たな産業の創出などを促進する観点からは、事業者自身による自らの事業等の実態に即した個人情報保護のための取組が率先して行われる必要があり、そのような自主的取組が法制度等と相まって、活力ある経済社会及び豊かな国民生活の実現を図っていくことが重要である。

第２章　検討の背景

○　個人情報保護法は、平成15年に制定（平成17年全面施行）されたが、平成27年に改正が行われ、平成29年５月30日に全面施行された。特に、平成27年改正法においては、情報通信技術の進展が著しいこと等から、３年ごとの見直し規定が設けられた。

○　平成27年改正法附則第12条第３項において、政府は、同法の施行後３年ごとに、個人情報の保護に関する国際的動向、情報通信技術の進展、それに伴う個人情報を活用した新たな産業の創出及び発展の状況等を勘案し、平成27年改正法による改正後の個人情報保護法（以下「改正個人情報保護法」という。）の施行の状況について検討を加え、必要があると認めるときは、その結果に基づいて所要の措置を講ずるものとされている。

○　また、同条第２項において、政府は、改正個人情報保護法の施行後３年を目途として、個人情報の保護に関する基本方針の策定及び推進その他の委員会の所掌事務について、これを実効的に行うために必要な人的体制の整備、財源の確保その他の措置の状況を勘案し、その改善について検討を加え、必要があると認めるときは、その結果に基づいて所要の措置を講ずるものとされている。

○　委員会は、平成27年改正法附則第12条の規定を踏まえ、いわゆる３年ごと見直しについて具体的に検討を進めてきた。第83回個人情報保護委員会（平成30年12月17日）において、「個人情報保護委員会の第一期を終えるにあたって」を公表し、前委員長の下で運営されてきた第一期目[1]の終了に際し、これまで５年間の経緯を踏まえ、次期委員会への申し送りとして、現下の状況を基に主な論点を取りまとめた。また、これを踏まえ、第86回個人情報保護委員会（平成31年１月28日）において、「いわゆる３年ごと見直しに係る検討の着眼点」を公表した。

○　委員会では、これらを踏まえ、個人情報保護を巡る国内外の政策、技術、産業等の状況について、消費者からの意見の分析、取りまとめ、経済界からのヒアリングを実施した。本中間整理は、この検討状況について、中間的に整理を行い公表するものである。

○　今回、本整理について、いわゆるパブリックコメントに付し、国民の皆様の御意見を伺い、その御意見等も踏まえつつ、学識経験者を含め各方面の意見を聴きながら検討を進めることとする。

[1] 平成 26 年1月1日の特定個人情報保護委員会の発足から平成 30 年 12 月 31 日まで。

第３章　個別検討事項

個別検討事項では、可能な限り網羅的に検討するとの観点から、「個人情報保護委員会の第一期を終えるにあたって」を踏まえつつ、対象項目を整理し、検討を行ってきた。

第１節　個人情報に関する個人の権利の在り方

１．概況

（１）規定

○　我が国の個人情報保護法では、個人情報、個人データ、保有個人データのそれぞれについて定義が置かれている。それぞれ後者が前者に包含される関係にあり、段階的に規律が上乗せされる構造となっている。個人情報については、取得・利用に関する規律が、個人データについては、それに加えて保管に関する規律及び提供に関する規律が、保有個人データについては、更に加えて開示等の請求に関する規律が課される。

○　国際的には、個人データ関連法制については、多くの国々で、ＯＥＣＤプライバシー・ガイドラインに準拠する形で整備されてきた。我が国の個人情報保護法も、同ガイドラインの８原則と対応しており、国際的にも整合的な制度となっている（表１）。ただ、個人情報保護制度については、それぞれの国・地域によって、文化的・歴史的な背景もあり様々な制度が存在しており、個々の具体的な規定ぶりは異なる部分も存在する。特に、最近は諸外国で新たな立法の動きも存在するところである[2]。

[2] 最近の立法例としては、米国カリフォルニア州消費者プライバシー法、ロシア改正個人データに関するロシア連邦法、中国サイバーセキュリティ法、ベトナムサイバーセキュリティ法、オーストラリアプライバシー改正法、韓国改正個人情報保護法、シンガポール個人情報保護法等がある。

表１　ＯＥＣＤ８原則と個人情報取扱事業者の義務規定の対応（概要）

OECD８原則	個人情報取扱事業者の義務
○ **収集制限の原則** 適法・公正な手段により、かつ情報主体に通知又は同意を得て収集されるべき	○ 偽りその他不正の手段により取得してはならない。（第17条）
○ **データ内容の原則** 利用目的に沿ったもので、かつ、正確、完全、最新であるべき	○ 正確かつ最新の内容に保つよう努めなければならない。（第19条）
○ **目的明確化の原則** 収集目的を明確にし、データ利用は収集目的に合致するべき ○ **利用制限の原則** データ主体の同意がある場合、法律の規定による場合以外は目的以外に利用使用してはならない	○ 利用目的をできる限り特定しなければならない。（第15条） ○ 利用目的の達成に必要な範囲を超えて取り扱ってはならない。（第16条） ○ 本人の同意を得ずに第三者に提供してはならない。（第23条）
○ **安全保護の原則** 合理的安全保護措置により、紛失・破壊・使用・修正・開示等から保護するべき	○ 安全管理のために必要かつ適切な措置を講じなければならない。（第20条） ○ 従業者・委託先に対し必要かつ適切な監督を行わなければならない。（第21条、第22条）
○ **公開の原則** データ収集の実施方針等を公開し、データの存在、利用目的、管理者等を明示するべき ○ **個人参加の原則** 自己に関するデータの所在及び内容を確認させ、又は異義申立を保証するべき	○ 取得したときは利用目的を通知又は公表しなければならない。（第18条） ○ 利用目的等を本人の知り得る状態に置かなければならない。（第27条） ○ 本人の求めに応じて保有個人データを開示しなければならない。（第28条） ○ 本人の求めに応じて訂正等を行わなければならない。（第29条） ○ 本人の求めに応じて利用停止等を行わなければならない。（第30条）
○ **責任の原則** 管理者は諸原則実施の責任を有する	○ 苦情の適切かつ迅速な処理に努めなければならない。（第35条）

○　個人情報保護法における、個人情報の取扱いに係る本人の関与は、制度上の合理性と、適法に事業を営む個人情報取扱事業者の負担等を加味して定められている。例えば、取得時については、要配慮個人情報については同意が必要であること、利用・保管時については、当初の目的の達成に必要な範囲を超えて個人情報を取り扱う際には同意が必要であり、保有個人データの開示請求については、原則として開示しなければならないこと、提供時については、第三者提供に際しては原則として同意が必要であることなどである（表２）。

表２　個人情報保護法における本人の位置付け（概要）

取得時	利用・保管時	提供時
・要配慮個人情報については、本人同意（その他の情報については、取得時に同意不要、第17条） ・通知、公表による利用目的の認知（第18条）	・特定した利用目的の達成に必要な範囲を超えて個人情報を取り扱う場合の本人同意（第16条） ・利用目的の通知の請求（適法に告知していれば事業者は対応不要、手数料可、第27条、第33条） ・保有個人データの開示請求（権利利益を害するおそれがある場合、業務の適正な実施に著しい支障を及ぼす場合、法令違反となる場合は対応不要、手数料可、第28条、第33条） ・事実でない場合の内容の訂正、追加、削除の請求（第29条） ・利用目的や取得に違法性がある場合に限定した利用停止、消去の請求（本人の意向変更に伴う請求は不可、多額の費用を要するなど困難な場合で権利利益保護の代替措置をとる場合、事業者の対応不要、第30条）	・第三者提供に際しての本人同意（委託、事業承継に伴う場合には、本人同意不要、第23条） ・特定の者との共同利用については、利用者の範囲、利用目的等について本人に通知、公表（共同利用固有の本人同意は不要、第23条） ・第三者提供を利用目的とする場合における、第三者提供停止の請求（オプトアウト、第23条） ・外国にある第三者（委託等の場合を含む）に提供する場合の本人同意（指定国・地域への移転の場合、移転先事業者の体制が所定の基準を満たす場合には、同意不要、第24条） ・違法性がある場合に限定した第三者提供停止請求（本人の意向変更に伴う請求は不可、多額の費用を要するなど困難な場合で権利利益保護の代替措置をとる場合、事業者の対応不要、第30条）

（２）個人情報保護法相談ダイヤルに寄せられる意見

○　個人情報に関する個人の権利の在り方を考えるに当たって、当然、個人の意見を丁寧に踏まえることが求められるが、その把握は必ずしも容易ではないと考えられる。このような中、委員会では、個人情報保護法相談ダイヤル（以下「相談ダイヤル」という。）を設置し、日々多くの苦情・相談を受け付けるとともに、委員会が全国各地に出向き意見等を聴取するタウンミーティングを開催している。委員会では、消費者の意見を集約するため、これらの場で寄せられた生の声を活用し分析を行った。

○　相談ダイヤルは、個人情報保護法に関する質問、相談及び苦情の申出についての必要なあっせん等を行うための窓口として委員会に設置されているものである。相談ダイヤルにおいては、法令やガイドラインに基づき説明を行い、苦情が申し立てられた場合には、必要に応じて事業者に確認を行った上で、あっせん、事業者に対する指導・助言等を行い、事案によっては監督部門への通報を行っている。

○　相談ダイヤルに寄せられた相談（平成30年４月１日～同年12月31日）のうち、全体の約８割が質問、約２割が苦情である。相談主体別の受付件数では事業者からの相談が半数以上を占めている一方、事業者からの相談の大半は質問であり、個人からの相談の約４割が苦情であることから、苦情の大半は個人から寄せられるものである。なお、苦情の内容は、第三者提供、利用目的、安全管理措置、開示等（開示、削除・利用停止を含む。）の順に多い（表３）。

表３　個人情報保護法相談ダイヤルの実績値（平成30年４月１日～同年12月31日）

分類	受付件数	相談主体別			問い合わせ内容上位５項目（１質問で複数の項目に該当する場合を含む）				
		事業者	個人	その他（※２）	第三者提供	利用目的	定義	安全管理措置	開示等（※３）
質問	10,294	**6,956**	2,249	1,089	**3,888**	1,898	1,713	1,195	540
苦情（※１）	1,708	14	**1,672**	22	**675**	399	150	290	219
その他	646	114	462	70	25	9	38	7	9
合計	12,648	7,084	4,383	1,181	4,588	2,306	1,901	1,492	768

※１　事業者等における不適正な取扱い等に関する情報提供を含む。

※２　国の行政機関、地方公共団体、弁護士その他からの相談。

※３　削除・利用停止に関する相談を含む。

○　個人から寄せられる相談の主要な相談項目（第三者提供、利用目的、安全管理措置、開示、削除・利用停止）のうち、事業者に対する不満等については、第三者提供及び安全管理措置の割合が、要望等については、第三者提供、開示及び削除・利用停止の割合が比較的高い。事項別の相談の概要は次のとおりである（表４）。

表４　個人からの相談内訳（平成30年４月１日～同年12月31日）

分類		①第三者提供	②利用目的	③安全管理措置	④開示	⑤削除・利用停止
個人からの相談合計(4,383件)のうち、主要な相談の受付件数		1,318	649	544	478	435
個人からの相談合計(4,383件)に対する割合		30%	15%	12%	11%	10%
一般的な質問	実数	363	**441**	168	**235**	**217**
	割合	28%	**68%**	31%	**49%**	**50%**
事業者の個人情報の取扱いに対する不満等	実数	**884**	181	**350**	177	**186**
	割合	**67%**	28%	**64%**	37%	**43%**
要望等	実数	**64**	11	14	**26**	**29**
	割合	**5%**	2%	3%	**5%**	**7%**
その他		7	16	12	40	3

＜第三者提供に関する相談＞

質問の大半は、第三者提供に係る法制度又はオプトアウト制度に関する質問である。また、事業者に対する不満等のうち、個人データの本人同意のない第三者提供に関するものが大半を占めているほか、事業者が家族等への提供に応じないことに関する不満等も寄せられている。要望等としては、名簿の売買禁止を求める意見のほか、名簿を購入した事業者に対して当該名簿の入手先の開示義務付けを求める意見が多く寄せられている。

＜利用目的に関する相談＞

質問の大半は、利用目的に係る法制度に関する質問である。また、事業者に対する不満等のうち、個人情報の目的外利用に関するものが大半を占めているほか、利用目的の通知又は公表に関する不満等も寄せられている。要望等としては、事業者が個人情報を取得又は利用する際に本人の関与を求める意見等が寄せられている。

＜安全管理措置に関する相談＞

質問の大半は、安全管理措置に係る法制度に関する質問である。また、事業者に対する不満等のうち、個人情報の漏えいに関するものが半数程度、その他個人情報の杜撰な取扱いに対する不満等も寄せられている。要望等とし

ては、漏えい報告等の義務化を求める意見や漏えい等を起こした事業者に対する罰則の強化を求める意見等が寄せられている。

＜開示に関する相談＞

開示に係る手続全般に関する質問、又は事業者の保有している相談者自身に関する個人データを知る方法を問う質問が大半を占めており、相談者は、事業者が相談者自身に関してどのような情報を保有しているのか把握したいという意向を持っていることが窺える。また、事業者に対する不満等のうち、開示されなかったことに関する不満等が最も多く寄せられている。このほか、開示手続の遅延等の事業者の対応に関する不満、一部不開示とされたことや開示された文書等の内容が請求者の認識と異なっていたことなどの開示請求の結果に関する不満、開示手続において事業者から提出を求められた書類の種類等や手数料の金額が妥当でないなどの開示手続に関する不満等もあった。要望等としては、開示請求者の利害に関わる場合、当該請求者が開示に係る個人情報の「本人」でなくても開示されるようにするべきといった開示請求権者の範囲の拡大を求める意見等が寄せられている。

＜削除・利用停止に関する相談＞

質問の大半は、削除・利用停止に係る手続全般に関する質問である。事業者に対する不満等のうち、事業者が削除・利用停止に応じないことに関する不満等が最も多く寄せられている。このほか、削除・利用停止手続の遅延等の事業者の対応に関する不満、削除・利用停止手続において事業者から提出を求められた書類の種類や内容等が必要な範囲を超えているなどの削除・利用停止手続に関する不満等もあった。要望等としては、削除・利用停止の義務化を求める意見や、削除・利用停止手続に伴い事業者が取得する個人情報の範囲等について規制を求める意見等が寄せられている。

（３）苦情あっせんの実施

○　委員会は、個人情報保護法第61条第２号に規定する苦情の申出についての必要なあっせん及びその処理を行う事業者への協力に関する事務を行うための窓口として、あっせん窓口を設置・運用している。

○　平成30年度においては、16件のあっせんを実施し、このうち、12件の事案が解決に至っている。具体的には、委員会から事業者に苦情内容を伝達した結果、事業者の対応により、相談者から納得を得られたケース、事業者の説明を委員会が分かりやすく説明することで相談者から納得を得られたケース等が挙げられる。なお、あっせんを実施した16件のうち、個人情報保護法第23条（第三者提供の制限）に関する事案が９件と、約６割を占めている。

（４）タウンミーティングでの意見

○　委員会では、日常的に個人情報に接する消費者や自治会・企業関係者等の方々に、個人情報の保護やその取扱いに関して感じている悩み・疑問点等について意見交換していただき、個人情報保護に関する制度や運用等について理解を深めていただくとともに、制度に対する御意見をいただくため、平成30年度においては、全国７か所でタウンミーティングを開催している。

○　平成30年度に開催したタウンミーティングでの意見の全体的な傾向は次のとおりであった。

・消費者や消費者団体の関係者からは、名簿の取扱いを含め、個人情報に係る消費者自身の自覚の重要性や、地域での情報共有に係る課題、日常生活におけるスマートフォンやインターネットに関する個人情報の取扱いに係る不安感や、子供の頃から個人情報に関する教育啓発の重要性を指摘する意見があった。

・消費生活相談の関係者からは、名簿や架空請求に関する相談が多くあること、消費者が事業者のサービスを利用する際には利用規約を十分に確認することが重要であることや事業者との間で削除・第三者提供に係るトラブルの相談についての意見があった。

・自治会の関係者からは、災害時の要支援者の対応に係る課題についての意見や自治会内での日常業務や行政との連携などに関する意見があった。

・企業関係者からは、サイバー攻撃を含む安全管理措置の重要性を指摘する意見や、消費者との関係で事業者が直面する課題に関する意見、法解釈に係る意見等があった。

○　これら意見のうち、「３年ごと見直し」に関連した意見を見ると、

・最も多かったのは、いわゆる名簿等販売事業者（以下「名簿屋」という。）への対策に関する意見であった。例えば、「古い名簿が出回っているのではないか」「高校の名簿が流出しているのか子供に結婚の勧誘がくるようになった」などである。

・「ＳＮＳにおけるリスクの顕在化」に関連しては、近年のネット社会の普及において「消費者自身の自覚が重要」という意見や、「ＳＮＳを利用する若者の被害が増えており、小中学生の頃から個人情報に関する教育啓発が必要ではないか」などといった意見があった。

・データ活用の多様化と個人の権利に関連して、インターネットサービスなどを利用する時に、「自分の個人情報がどのように使用されるのか」という心配の声や、事業者のサービスを利用する際に、「利用規約に予め同意のチェックマークが付いており、必要のないサービスまで受けてしまった」

等、事業者側の説明責任についての意見があった。

・「訂正、利用停止、削除等」に関連して、消費生活相談の関係者からは「事業者からの勧誘をやめてほしい」、「自分の個人情報を削除してほしい」という相談が多く寄せられているとの意見があった。こうした利用停止・削除請求について、「事業者の判断に委ねられており、話がこじれることもある」という意見があった。

・このほか「海外事業者のサービスを利用しているが、ウェブ上のやりとりなど、様々な個人情報が取得されていると思うが、適切に管理されているのか疑問を感じている。」という意見もあった。

２．開示請求に関する状況

（１）開示請求を巡る実態

○　開示請求については、平成27年改正法により、本人による開示の請求が、裁判所に訴えを提起することができる請求権であることが明確化された。

○　しかし、相談ダイヤルへの相談の状況等を見ると、一部事業者の対応について消費者からの不満が見られる状況にあり、また、開示請求に応じなくてもよい場合を法定する例外規定の拡大解釈とも受けとれる不適切な対応事例が見られた。こうした実態を踏まえ、委員会では、開示請求権に係る法の考え方を明確化するため、「個人情報の保護に関する法律についてのガイドライン（通則編）」について、昨年12月25日改正を行った。また、この改正内容を踏まえ、Ｑ＆Ａの関係部分も改正を行った。

○　具体的には、開示請求の例外として認められる個人情報保護法第28条第２項第２号の「個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合」について、個人情報取扱事業者の業務の実施に関し、単なる支障ではなく、より重い支障を及ぼすおそれが存在するような例外的な場合に限定され、単に開示すべき保有個人データの量が多いという理由のみでは、一般には、これに該当しないことを明確化した。また、併せて、個人情報保護法第32条第２項の「個人情報取扱事業者は、本人に対し、開示等の請求等に関し、その対象となる保有個人データを特定するに足りる事項の提示を求めることができる」との規定は、本人に対し、開示を請求する保有個人データの範囲を一部に限定する義務を課すものではなく、また、個人情報取扱事業者に対し、本人が開示を請求する範囲を限定させる権利を認めるものでもないことを明確化したところである。

（２）開示請求を巡る国際比較

○　開示請求については、今回調査した多くの国々[3]において法律上の規定が整備されている。これらの国々の制度は類似点も多い規定となっているが、開示の形式等について差異も見られる。

○　ＥＵのＧＤＰＲ、我が国の個人情報保護法ともに、事業者は、本人の求めに応じて、保有する個人データを提供する義務が課せられている。一方、我が国が原則書面の交付で取り扱うのに対し、ＧＤＰＲにおいては、特定の条件を満たす場合には、本人が他の用途で利用しやすい電子的形式で、本人又は本人が望む他の事業者に、個人情報を提供する義務が課されており「データポータビリティの権利」と称されている（ＧＤＰＲ第20条）。なお、本人が望む他の事業者に直接個人情報を提供させることができるのは、技術的に実行可能な場合に限定されている。

３．利用停止等に関する状況

（１）利用停止等を巡る状況

○　個人情報保護法上、利用停止等（利用の停止又は消去）についての個人の権利行使には一定の制約が課されている。例えば、利用停止等に応じる義務を課されているのは、個人情報を目的外利用したときや、不正の手段により取得した場合に限られている。このほか、第三者提供の停止の請求に応じる義務があるのも、法の規定に違反して第三者提供されている場合に限られている。

○　なお、日本において比較的多くの事業者が活用している民間の取組であるプライバシーマーク[4]において審査基準の根拠とされている「ＪＩＳ Ｑ １５００１個人情報保護マネジメントシステム－要求事項」においては、本人の保有個人データの利用停止、消去又は第三者提供の停止の請求を受けた場合は、原則として応じる義務があることとされており、自主的に個人情報保護法の水準を超えた対応が行われている。

（２）利用停止等を巡る国際比較

○　今回調査を行った、ＥＵ、中国等ともに、我が国の個人情報保護法に定める利用停止等に相当する内容については、法令上の規定が整備されていた。

---

[3] 米国カリフォルニア州法、EU、中国の状況について第 95 回委員会（平成 31 年3月 20 日）資料（個人情報保護を巡る国内外の動向）を参照。

[4] プライバシーマーク制度は、日本工業規格「JIS Q 15001 個人情報保護マネジメントシステム－要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を評価して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認めるもの（現在の一般財団法人日本情報経済社会推進協会（JIPDEC）が本制度を創設して平成 10 年 4 月 1 日より運用を開始）

各国の制度の内容には類似点も多いが、訂正等の請求に事業者が応じるべき場合や軽減措置の内容等については、差異が見られる。

○　特に、ＥＵのＧＤＰＲについては、旧来の「ＥＵデータ保護指令」(Data Protection Directive 95) の下では規定のなかった、消去権、プロファイリングに係る規定が新たに設けられており、概要は次のとおりである。

・消去権については、本人は、一定の場合に、事業者に対して、当該本人に関する個人データを不当に遅滞なく消去させる権利が認められている。もっとも、表現の自由及び情報伝達の自由の権利の行使に取扱いが必要な場合等、適用の例外も規定されている[5]。

・また、プロファイリングについては、大きく分けて、異議を申し立てる権利（ＧＤＰＲ第21条）と、自動的な意思決定に服さない権利（ＧＤＰＲ第22条）が規定されている。

・異議を申し立てる権利は、「公共の利益又は公的権限の行使のために行われる業務の遂行」又は「正当な利益の追求」を法的根拠とする、プロファイリングそのものを含む個人データの取扱いに対して、異議を申し立てる権利（ＧＤＰＲ第21条第１項）であり、この権利を行使された事業者は、本人の利益を超越する、個人データの取扱いに係る正当化根拠等を示せない限り、プロファイリングそのものを含む個人データの取扱いを止めなければならないとされている。なお、「正当な利益の追求」によらず、「本人同意」を法的根拠としたとしても、同意を撤回されれば削除権の対象となる（ＧＤＰＲ第17条第１項(b)）。なお、ダイレクトマーケティングを目的とする個人データの取扱いに関しては、事業者の事情（取扱いに係る正当な根拠の有無）にかかわらず、この権利の行使の対象となる（ＧＤＰＲ第21条第２項）。

・また、自動的な意思決定に服さない権利（ＧＤＰＲ第22条）については、

---

[5]【事業者が消去の義務を負う場合の例】
- 個人データの収集や取扱いの目的に関して、当該個人データが必要なくなった場合
- 本人が個人データの取扱いについての同意を撤回し、かつ、当該取扱いに関して他の法的根拠がない場合
- 本人が、第 21 条第1項に基づいて個人データの取扱いに対して異議を申し立て、かつ、取扱いに関して優先する他の法的根拠がない場合、又は、ダイレクトマーケティングを目的とした取扱いに対して異議を申し立てる場合
- 個人データが不法に取り扱われた場合
- 個人データが EU 法又は EU 加盟国の国内法の義務の遵守のために消去されなければならない場合

【適用されない場合の例】
- 表現の自由及び情報の自由の権利の行使に取扱いが必要な場合
- 事業者が従う EU 法又は EU 加盟国の国内法の義務の遵守のために取扱いが必要な場合、又は公共の利益等のために取扱いが必要な場合
- 公共の利益の目的、科学的若しくは歴史的研究目的又は統計目的の達成のために取扱いが必要な場合

プロファイリングを含むもっぱら（solely）自動的な個人データの取扱いに基づく意思決定に服さない権利とされ、プロファイリングそのものではなく、意思決定に服さない権利が規定されている。なお、本人との契約の締結又は履行に必要な場合等は対象外であり、また、人が介在すればこの権利の対象とはならないとされている。

４．オプトアウト規定と名簿屋対策の状況

（１）オプトアウト規定を巡る状況

○　オプトアウト規定とは、第三者に提供される個人データについて、本人の求めに応じて提供を停止することとしている場合であって、あらかじめ、個人データの第三者への提供を利用目的とすること、提供される個人データの項目、第三者への提供の方法、求めに応じて提供を停止すること及び本人の求めを受け付ける方法を本人に通知し、又は本人が容易に知り得る状態に置いた上で、本人の同意を得ることなく第三者に提供することを認める規定であり、個人情報保護法上、第三者提供の際に求めている本人同意の原則の例外である（個人情報保護法第20条）。

○　改正個人情報保護法では、平成26年に発生した民間企業における大規模漏えい事案が契機となって、名簿屋対策を目的とし、オプトアウト規定を利用する事業者の委員会への届出義務及び委員会による公表の規定が導入された。同時に導入された個人情報保護法第25条（第三者提供に係る記録の作成等）及び第26条（第三者提供を受ける際の確認等）の規定と相まって、違法な名簿屋による個人データの不正な流通を抑止しようとするものである。

○　改正個人情報保護法でオプトアウトを行う事業者による委員会への届出状況について、平成30年度末時点での届出書公表済件数は186件となっている。

（２）名簿屋に関する実態調査（平成29年度）

○　委員会は、平成29年度、個人情報の第三者提供事業等の実態調査を実施したところ、概要は以下のとおりである。

○　名簿屋としては、設立後20年以上の事業者が多く、従業員は２～20名程度、年間売上高は数百万円～１億円程度、数千万件～１億件の個人データを基に顧客ニーズに応じたリストを提供していた。また、主な取得元は、過去の住民基本台帳、同業者、同窓会名簿、主な提供先は、呉服店、自動車教習所、学習塾、不動産、金融業等であり、同業者間取引が行われているほか、名簿屋と購入者の仲介を行う「ブローカー」が存在していた。なお、業界団体と

しては、「特定非営利法人日本個人データ保護協会」が存在していた。

○　また、名簿屋における業務状況としては、適正な取得を前提とすれば、住民基本台帳の閲覧禁止（平成18年）以降、新規の個人情報の入手は（公開情報を除き）困難となっており、当該台帳情報の利用価値がなくなれば、多くの名簿販売事業の継続が難しくなる傾向にある。また、個人情報保護法改正の影響及び同法の履行状況については、実態調査等により、３分の２程度の事業者においてはおおむね適切な取扱いがなされていることを確認した。一方、個人からの問合せへの対応においては、入手経路を回答しない事業者が存在した。

（３）名簿屋に関する実態確認（平成30年度）

○　名簿屋を含むオプトアウト手続の届出事業者158件のうち、平成29年度に30件、平成30年度に37件の名簿屋に対し、実態確認を行った。また、未届けの疑いがあると判明した事業者３件も実態確認を行った。

○　確認対象先に対し、事業内容や個人情報の取扱状況、取得及び提供時に係る確認・記録義務の履行状況を確認するため、書面により調査票を送付するとともに、当該調査票の回答内容を確認するため、臨場等によるヒアリングを実施した（表５）。

表５　名簿屋に対する実態確認の結果（平成30年度）[6]

実施区分	調査結果	件数
未届けの疑いがある事業者	新たに届出書を提出	3件
届出事業者	確認・記録義務等の履行に問題がないと考えられる先	23件
	確認・記録義務等の履行に問題がある先	14件
	（内　取得時の確認・記録が不十分な先）	*（10件）*
	（内　提供時の記録が不十分な先）	*（3件）*
	（内　その他）	*（3件）*
30年度の実態確認の中で把握した未届けの疑いがある事業者	新たに届出書を提出	7件
	現在、調査確認中	39件

○　未届事業者に対しては、新たに届出書を提出するように、また確認・記録義務の履行に問題がある先に対しては、適正に履行する体制を整備するよう、必要に応じて、指導・助言を行った。

[6]　第 101 回個人情報保護委員会（平成 31 年4月 12 日）における　資料1－1「個人情報保護を巡る国内外の動向（オプトアウト規定（名簿屋対策）の現状・苦情あっせんの取組）」から引用。

○　今回の調査の結果、届出事業者が第三者提供をやめた場合、届出の取下げに関する規定がないことや、オプトアウト届出に係る変更の届出は、取り扱う個人データの内容や提供方法を変更した場合は必要だが、住所や屋号が変わった場合の変更届出規定がないなどの課題も確認された。

○　未届けの疑いがある事業者の存在について、引き続き調査を行い、届出を指導するとともに、届出事業者について、確認・記録義務の履行等の業務実態について、引き続きモニタリングしている。

５．検討の方向性

（１）全体

○　個人及びデータを活用する事業者の双方にとって、本テーマは影響が大きく、今後、影響や実効性、実態を踏まえ、慎重かつ丁寧な検討が求められる。特に、相談ダイヤルに寄せられた意見やヒアリングの結果をみると、消費者側と事業者側で意見の分かれる点も多く、多面的な検討が求められる。

○　我が国の個人情報保護法はＯＥＣＤ８原則に対応しており、個人データに関する個人の権利に対応する規定においても国際的に調和のとれたものになっている。しかし、この本人の関与に関する部分は、相談ダイヤルに寄せられる事業者の取扱いに対する不満等の中でも、制度に関連しての意見が多い部分であり、重点的に検討を行う必要があると考えられる。

（２）個人情報保護法相談ダイヤルの充実

○　相談ダイヤルは、平成27年改正法で個人情報保護法に基づく監督権限が委員会に一元化されたことを受けて設けられた。

○　委員会では、相談ダイヤルを、消費者・事業者との接点として重視してきた。相談等が寄せられた事案については、消費者等が可能な限り納得感を得られるよう、丁寧な対応に努めており、今後ともこの取組を着実に進めることは重要である。また、相談ダイヤルに寄せられた情報を契機として、個人情報の取扱いに関し指導を行った事例もあり、監督業務における情報収集の契機としても重要である。さらに、寄せられた内容について、相談内容の秘匿性を守りつつ、貴重な意見として集約していくことも重要である。

○　また、苦情あっせんについては、委員会が苦情あっせんを実施したことにより、消費者等と事業者の間では解決できなかった事案が解決に至っており、一定の成果を上げていると考えられる。

○　今後、相談ダイヤルについては、ＡＩを使ったチャットボットを導入する[7]など、更なるサービスの充実に向け取り組む必要がある。

（３）開示請求

○　開示請求については、平成27年改正法により請求権であることが明確化されたが（個人情報保護法第28条）、相談ダイヤルには事業者に対する不満が多く寄せられており、また、これまで委員会が行った団体へのヒアリングでも、開示請求への対応について消極的意見があった。加えて、相談ダイヤルに寄せられる情報を見ても、必ずしも制度が正しく理解され、又は運用されていないと思われるケースも散見された。

○　個人情報の本人に対する開示は、利用目的等の通知、公表等の仕組みと相まって、個人情報の取扱いの透明性を高めるものである。加えて、開示の請求は、訂正、利用停止等の請求の前提となる手続でもあり、これらは一体となって個人情報に対する適切な本人からの関与の仕組みを構成する。その意味でも、開示の仕組みは、個人情報の適正な取扱いに関するルールの中でも重要な仕組みの一つである。

○　このような法の趣旨を踏まえ、今後、開示請求については、法の趣旨を踏まえ、引き続き企業が適切に対応を行っているか、その対応状況を注視する必要があるとともに、委員会として、企業に対して制度の周知に努める必要がある。

○　一方、開示の提供形式について、個人情報の保護に関する法律施行令（平成15年政令第507号）第９条で「書面の交付による方法」を原則としつつ、「開示の請求を行った者が同意した方法があるときは、当該方法」とされている。しかし、情報通信技術の活用による行政手続等に係る関係者の利便性の向上並びに行政運営の簡素化及び効率化を図るための行政手続等における情報通信の技術の利用に関する法律等の一部を改正する法律案（いわゆる「デジタル手続法案」）において、民間手続における情報通信技術の活用の促進等が謳われる中、個人情報保護法における開示の際の電磁的形式による提供の明確化についても、今後、利用者の利便性も考慮しつつ、検討していく必要がある。

○　なお、いわゆるデータポータビリティに関連しては、既に民間における自

[7] Web上において、24 時間無人で質問対応を行うことが可能になるよう、相談者の質問の意図を認識して回答を表示させるものの導入を検討している。

主的取組として、情報銀行の取組も行われている（本章第３節２（４）において後述）が、個人情報保護法に沿った形でこのような取組が自主的に行われることは歓迎すべきものである。一方、データポータビリティの法的な義務化については、そもそも個人の権利利益の保護といった個人情報保護の観点以外に、産業政策や競争政策といった幅広い観点が存在する。ＥＵではＧＤＰＲで新たに導入されたところだが、ある管理者から別の管理者へ直接個人データを移行させる規定については、技術的に実行可能な場合に限定されている。我が国では、その必要性等について、消費者ニーズや事業者のメリット・実務負担等を含め、議論が現在様々な場で行われている段階であることから、このような議論の推移を見守る必要がある。

（４）利用停止等

○　利用停止等に関しては、相談ダイヤルに寄せられる意見や、タウンミーティングにおける議論でも、消費者からは、自分の個人情報を事業者が削除・利用停止しないことへの強い不満が見られる。一方、プライバシーマークの審査基準の根拠である「ＪＩＳ　Ｑ　１５００１個人情報保護マネジメントシステム－要求事項」のように、事業者の中には顧客の利用停止等の要求に対応する例も存在することも踏まえ、利用停止等に関して、個人の権利の範囲を広げる方法について検討する必要がある。

○　平成27年改正法により、個人情報取扱事業者は、利用する必要がなくなった個人データを遅滞なく消去する努力義務が追加された（個人情報保護法第19条）。このような法令上の要請に応えてデータの最小化を行う事業者も多いと考えられるが、必ずしもそのような対応を行っていない事業者も存在することが想定される。今後、企業の実務上の問題を整理する必要がある。

○　また、消去については、例えば、事業者が本人からの請求に基づき個人情報を（本人の請求に基づき消去した事実を含め）完全に消去してしまうと、当該事業者は、過去に消去請求をした者であるという事実を含め、当該本人に関する情報を一切保有しないことになるが、その後、再び当該本人の個人情報を取得した場合に当該個人情報を利用することの可否等の消費者の利便や実務上の論点もある。

○　加えて、事業者によっては、安全管理上の理由等から、個人情報データベース等を部門ごとに別々に管理している場合もあり、このような場合に全部門の個人データを容易に名寄せし、利用停止等ができるような体制になっているかという論点もある。

○　利用停止等については、消費者側からの根強い要望に対して、個人の権利を保護していく観点からどのようにすれば一定の対応が可能か、企業側の実態も踏まえつつ、具体的に検討していく必要がある。

（５）オプトアウト規定と名簿屋対策

○　いわゆるオプトアウト規定については、平成27年改正法で委員会への届出義務が創設された。制度としては一定程度有効に機能しているものと評価される。

○　名簿屋対策については、古くから問題とされていた中、従来、名簿屋対策に責任を持つ主務官庁が必ずしも明確でなかったところ、平成27年改正法により、届出義務が課されるオプトアウト規定が導入されるとともに、委員会が一元的に対応することが可能となった。こうした中、前述のとおり、相談ダイヤルやタウンミーティングの中で対策の徹底を求める意見が多いことから、実態をよく把握しつつ、執行面も踏まえて検討する必要がある。

○　特に、今回の調査で、確認・記録義務の履行が不十分な事業者や未だ届出のない可能性がある事業者が存在することが分かった。また、本人がオプトアウトの要否を判断する手がかりとなる、オプトアウト手続に関する委員会への届出の内容と実際の業況が異なる業者が存在することも判明している。

○　このような実態を踏まえ、まずは、今回、指導等を行った事業者の業務実態や未届事業者の把握を継続的に行うなど、現行制度の執行による名簿屋対策の徹底を進め、個人情報保護法に適合しない形で名簿等が取り扱われている場合には必要な措置をとる必要がある。

○　他方、現行制度に関する課題としては、情報入手先の開示の必要性やオプトアウトの届出内容に事業者の事業実態が的確に反映されるような仕組みの工夫の必要性などが挙げられ、上記執行の徹底を通じた現行制度の下での対策の効果も踏まえつつ、更に幅広く検討を進める必要がある。

第２節　漏えい報告の在り方

１．我が国における現状

（１）規定

○　個人情報取扱事業者は、漏えい等事案が発覚した場合は、その事実関係及び再発防止策等について、委員会等に対し、速やかに報告するよう努めることとされている。これは、個人情報保護法第20条に規定する個人データの安全管理措置義務の一環として、「個人データの漏えい等の事案が発生した場合等の対応について」（平成29年個人情報保護委員会告示第１号）に基づくものである。

（２）対象

○　現在の告示では、対象事案について、以下の①から③までのいずれかに該当する事案（以下「漏えい等事案」という。）を対象としている。

①　個人情報取扱事業者が保有する個人データの漏えい、滅失又は毀損
②　個人情報取扱事業者が保有する加工方法等情報の漏えい
③　上記①又は②のおそれ

○　また、漏えい等事案が発覚した場合に講ずべき措置として、以下が規定されている。

①　事業者内部における報告及び被害の拡大防止
②　事実関係の調査及び原因の究明
③　影響範囲の特定
④　再発防止策の検討及び実施
⑤　影響を受ける可能性のある本人への連絡等
⑥　事実関係及び再発防止策等の公表

○　なお、①実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合、又は、②ＦＡＸ若しくはメールの誤送信又は荷物の誤配等のうち軽微なものの場合、のいずれかに該当する場合は、報告を要しないこととしている。

（３）漏えい報告に係る執行の状況

○　委員会が受領した漏えい報告の件数は、平成29年度は3,338件、平成30年度上半期は2,191件となっている。漏えい報告の中には、委員会に直接提出されるもの、個人情報保護法第44条に基づき権限を委任している大臣を経由するもの、同法第47条に規定する認定個人情報保護団体を経由して報告されるものが存在する。漏えい人数が５万人以上の事案の件数を見ると、平成29年度は13件、平成30年度上半期は14件となっている。

○　漏えい事案の発生原因は、平成29年度、平成30年度上半期を通じて、書類及び電子メールの誤送付、書類及び電子媒体の紛失が約８割を占めている。このうち、大規模漏えい事案の発生原因については、インターネットを経由した不正アクセスが約７割となっている。また、１件当たりの漏えい人数は100人以下のものが８割以上となっている。

○　委員会が積極的に働きかけた事例としては、漏えい等事案の報道発表を端緒として事業者に連絡を行った結果、漏えい報告が提出された事案、ソーシャルモニタリング（委員会が不適切事案を早期に把握するために、ソーシャルメディア等における情報をモニタリングする手法）を端緒として事業者に連絡を行った結果、漏えい報告が提出された事案などがある。

○　なお、事業者からの個人データの漏えい等事案の状況[8]を見ると、以下のとおりである。
・漏えい等した人数については、500人以下の事例が93.6%と大半を占めている。
・漏えい等した情報の種類については、顧客情報が92.9%と大半を占めている。
・漏えい等した情報の形態については、紙媒体のみが60.1%、次いで電子媒体のみのものが37.6%となっている。
・漏えい等元・漏えい等した者については、事業者の従業者の不注意によるものが52.9%、委託先の従業者の不注意によるものが34.0%となっている。
・漏えい等した後の改善措置状況については、従業者による安全管理措置として講じられているのは、人的措置が71.5%、次いで組織的措置が34.4%になっている。事業者による本人への対応としては、本人への謝罪・連絡が91.9%となっている。

○　委員会としては必要に応じて、再発防止策の実施や個人情報の適切な取扱いを行うように個人情報保護法第41条に基づく指導・助言を行うほか、立入検査等を実施するケースもある。

○　また、外国にある個人情報取扱事業者のうち、日本にいる者に対して物品やサービスの提供を行い、これに関連して本人から個人情報を取得した者が、外国においてその個人情報を取り扱う場合は、個人情報保護法第75条に基づき、同法第20条（安全管理措置）の規定も適用される。このような外国にある個人情報取扱事業者が日本の利用者の個人データを含む漏えい等事案を

[8] 平成29年度年次報告(期間:平成29年5月30日～平成30年3月31日)

発生させた場合には、日本にある個人情報取扱事業者と同様に、漏えい報告の対象となる。

○　外国事業者の事例への対応としては、

・国外に所在する外国事業者の漏えい等により、当該事業者のサービスを利用していた国内事業者の顧客の個人データが漏えいした事案について、当該外国の事業者に対し国内事業者のリストの提出を求め、国内事業者に漏えい等報告の提出を促した事案（本章第５節１(2)及び第６節１(3)において再掲）

・外国事業者の漏えいであって、当該事業者の協力が得られなかった事案について、海外の個人情報保護当局との執行協力として、委員会の対応状況の情報提供、漏えい等事案の発生原因や再発防止策の情報の共有を行った事案

・国外に所在する事業者がソーシャルプラグインを設置している他のウェブサイトを閲覧した場合、ボタンを押さなくてもユーザーＩＤやアクセス履歴等の情報が当該事業者に送信されてしまうことや、取得した個人情報の一部が第三者に不正に提供されたケースがあったことから、①ユーザーへの分かりやすい説明や本人からの同意の取得の徹底、②同社がプラットフォーマーとしての責任を認識し、プラットフォーム上のアプリケーションの活動状況の監視を徹底すること等を指導した事案

等がある。

２．諸外国の現状

○　漏えい報告については、多くの国々で法令上義務化されている。漏えい報告の相手方は、原則として、本人と監督機関の双方となっている。また、漏えい報告の期限として、いずれの国でも速やかな対応を要求しているが、特に、ＥＵのＧＤＰＲは、具体的な時間制限として個人データ侵害を認識した時から72時間以内の当局に対する通知を要求している。

○　また、漏えい報告に係る軽減措置について、日本では高度な暗号化が施されている場合等、実質的に個人データが漏えいしていないと判断される場合に軽減措置が講じられているが、多くの国々[9]で、暗号化がされている場合や個人の権利・自由にリスクを発生させるおそれがない事案等について報告不要とされている。

○　このように、諸外国では大きな方向性では類似点も見られるものの、対象

[9] 米国（カリフォルニア州法、ニューヨーク州法）、EU、中国の状況について第 86 回委員会（平成 31 年1月 28 日）資料（個人情報保護を巡る国内外の動向）を参照。

とする事案、期限、軽減措置等の詳細については、相違点も見られるところである。

○　なお、国際的には、データ保護プライバシー・コミッショナー国際会議（以下「ＩＣＤＰＰＣ」という。）やＯＥＣＤ（欧州経済協力機構（Organisation for Economic Co-operation and Development））といった多国間での枠組みでも、各国の漏えい報告の状況を当局間で情報を共有し、効果的な執行活動に活かしていくという議論が行われている。

３．検討の方向性

（１）基本的考え方

○　漏えい報告は、委員会が漏えい事案を把握し、個人の権利利益の保護を図るためのいわば起点と考えられる。個々の事業者を適切に監督するというだけでなく、当局が、事業者が参考にすべき情報を積極的に事業者に対して発信したり、助言したりすることによって、事業者の適切な対応につなげていくという意義も大きい。漏えい報告の在り方を検討する上では、このような多面的意義を踏まえて議論を行う必要がある。

○　委員会における執行の現状からみても、漏えい報告を端緒として、当委員会による行政指導につながった事例も存在するなど、委員会の事業者監督において、効果的な手段となっている。

○　諸外国においては、多くの国で漏えい報告が義務とされている。一方、我が国では、法的な義務ではないにもかかわらず、漏えい報告について、多くの企業で適切に対応されており、これは、我が国事業者の個人情報保護に対する意識の高さとも考えられる。

○　一方、漏えい報告は法令上の義務ではないため、積極的に対応しない事業者も一部に存在している。仮に、事業者側が公表等しない場合、委員会が事案を把握できない可能性があり、適切な対応が行われない懸念がある。

○　また、事業者側から見ても、漏えい報告について、一定の軽減措置を設けることを前提に、法令上明確に位置付けた方が、企業側が報告の要否に係る判断に迷わないとも考えられる。

○　加えて、国際的な議論の潮流の観点からしても、ＩＣＤＰＰＣやＯＥＣＤといった多国間での枠組みで、各国の漏えい報告の状況を当局間で情報共有するという方向で議論がなされている状況を考慮する必要がある。

○　したがって、国内における法執行の安定性や、国際的な議論の潮流等を勘案すると、漏えい報告について、法令上明記し、一定の場合について義務付けをすることも検討する必要がある。

（２）勘案すべき事項

○　漏えい報告について、諸外国の立法例をみても、法令上義務としているものの、対象とする事案、期限、軽減措置、本人への通知等において、多様な状況にある。これら諸外国の立法例も参考としつつも、我が国ではどうあるべきか、影響や実効性等も加味しながら、今後具体的に検討していく必要がある。

○　仮に、漏えい報告を義務化する場合、軽微な事案についても全て報告を求めると、報告対象となる事業者の負担のみならず、報告を受領する執行機関としても制度の趣旨目的に比しコストが過剰となる可能性がある。

○　漏えいの件数、重大性、原因、漏えいした情報の内容等を考慮し、報告義務を課すことも考えられる。例えば、漏えいデータの件数（例：数件程度から数百万件）や情報の内容（例：公知情報、非公知情報、要配慮個人情報等）によって、本人や社会への影響は大きく異なると考えられる。しかしながら、数件程度の漏えいであったとしても、漏えいした情報の内容によっては、本人への影響が大きい場合もあり得る。報告義務を課す場合、中小規模事業者の負担も考慮しつつ、これら要素を加味した検討が必要である。

○　また、本人への通知等の在り方についても検討が必要である。本人への通知は、個人の権利利益の保護の観点からも重要と考えられるか、執行機関への報告と同様な形で連絡を求めるのか、一定の要件を設けるのか、検討が必要である。さらに、本人への通知等の具体的な方法・手段について検討する必要がある。

○　加えて、漏えい報告については、速やかに報告を求めるのが原則であることは言うまでもないが、法令で明示的な期限を設けるべきかについても、現状における報告実態を踏まえつつ、検討する必要がある。

○　なお、現在、漏えい報告の報告先については、一定の場合、委員会以外に、個人情報保護法第44条に基づき権限を委任している大臣及び認定個人情報保護団体に対して提出することを認めている。当該方式は現在有効に機能していると考えられることから、今後の検討においても、この方法を活かしていくことが考えられる。

第３節　個人情報保護のための事業者における自主的な取組を促す仕組みの在り方

１．認定個人情報保護団体制度

○　認定個人情報保護団体は、業界・事業分野等で事業者による個人情報の保護の推進を図るために、自主的な取組を行うことを目的として、委員会の認定を受けた法人（法人でない団体で代表者又は管理人の定めのあるものを含む。）である。個人情報保護法第47条第１項各号で規定される業務（対象事業者の個人情報等の取扱いに関する苦情の処理など）を行うほか、業界の特性に応じた自主的なルールである「個人情報保護指針」を作成し、その個人情報保護指針に基づいて対象事業者を指導していくことが求められている。

○　現在、43団体が認定されており、自主的なルールである個人情報保護指針は全ての団体において作成されており、一部の団体においては匿名加工情報などに関し、特徴あるルールを定めている。

○　委員会が平成29年度に実施した「個人情報の保護に関する事業者の取組実態調査（アンケート）」の結果[10]によれば、認定個人情報保護団体への加入状況は事業者規模による差が大きく、中小規模事業者で加入していると回答した事業者の割合は6.3%にとどまっている。また、認定団体が存在しない業種（製造業、その他サービス業）では比較的加入率が低い結果となっている。また、認定団体に期待する役割としては、「指針の策定による業界内のルール作り」、「指針の策定や研修の実施などを通じた情報提供」の割合が大きい。

○　認定団体における個人情報保護指針の「上乗せ規定」の状況としては、個人データの取扱いに関する責任者の設置義務などの規定を盛り込んでいる例も存在する。

２．事業者の自主的取組の状況

（１）総論

○　プライバシーマークやＡＰＥＣのＣＢＰＲの認証等を取得することにより、その審査基準である「ＪＩＳ　Ｑ　１５００１　個人情報保護マネジメントシステム－要求事項」等に準拠した体制を整備し、個人情報保護の取組を進めている事業者が存在する。

○　個人情報保護に関連する国際標準として、プライバシーフレームワークに

[10] 第 88 回個人情報保護委員会（平成 31 年2月８日）における資料1「個人情報保護を巡る国内外の動向（事業者における取組を促す仕組みの在り方関係）」から引用。データは「個人情報の保護に関する事業者の取組実態調査（平成 29 年度）報告書」（平成 30 年3月）の国内事業者向けアンケート結果によるもの。

関するＩＳＯ/ＩＥＣ ２９１００や情報セキュリティマネジメントシステム（ＩＳＭＳ）に関するＩＳＯ/ＩＥＣ ２７００１等があり、これらの認証を取得する事業者も存在する。

○　データ管理体制の整備及び向上の観点から、ＪＩＳ Ｑ １５００１では個人情報保護管理者等の責任及び権限について規定している。海外では、ＯＥＣＤガイドラインやＥＵのＧＤＰＲにおいてデータ保護管理者についての規定が存在する。

○　そのほか、事業者における自主的取組を推奨する仕組みとして、「情報信託機能の認定に係る指針」や「行動ターゲティング広告ガイドライン」（本節２（４）において後述）等が存在する。このように、認定個人情報保護団体ではないが、業界・業務の特性に応じ、個人情報に関連した自主的ルールを策定し、運用している例が存在している。

○　プライバシー影響評価（Privacy Impact Assessment：ＰＩＡ）の考え方を取り入れた仕組みとしては、番号法における特定個人情報保護評価や生産性向上特別措置法（平成30年法律第25号）における「革新的データ産業活用計画」（革新的な技術又は手法を用いたデータの収集、活用、これらを通じた企業間連携等により生産性を向上させる計画。以下同じ。）の協議が存在する。

（２）認証等の仕組みの事例

○　ＡＰＥＣのＣＢＰＲ（Cross Border Privacy Rules）システム

ＡＰＥＣ参加国・地域において、事業者のＡＰＥＣプライバシーフレームワーク[11]への適合性を認証する仕組みである。

事業者の個人情報保護の水準を国際的に判断するために有効な仕組みであり、我が国においては、ＣＢＰＲシステムの認証を行う団体として一般財団法人日本情報経済社会推進協会（以下「ＪＩＰＤＥＣ」という。）が認定されており、平成30年度末時点での我が国のＣＢＰＲ認証事業者数は３社である。

○　プライバシーマーク制度

平成10年４月１日より、ＪＩＰＤＥＣが運営する自主的な取組である。日本工業規格「ＪＩＳ Ｑ １５００１ 個人情報保護マネジメトシンステムー要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を評

[11] APEC プライバシーフレームワークは、OECD プライバシー・ガイドラインをモデルに、APEC 地域の電子商取引の促進を目的として 2004 年に採択された。

価して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認めている（平成30年度末時点での付与事業者数は16,210社）。

プライバシーマークの取得事業者は、全体の86.2%が中小規模事業者であり、特に、製造業・その他や卸売業において中小規模事業者の割合が高い。また、ＩＳＭＳの認証事業者は、従業員数が100人以下の割合は５割弱となっている。

○　ＥＵのＧＤＰＲにおける認証（Certification）制度

加盟国等は、管理者及び処理者による取扱業務が本規則を遵守することを証明する目的のために、データ保護認証方法、データ保護シール及びデータ保護マークを設けることを奨励しなければならないとされている。なお、この仕組みについては、現在、施行のための準備が行われている段階であり、今後の動向に注視していく必要がある。

（３）データ管理の責任体制に関する規定の例

○　ＥＵのＧＤＰＲにおけるデータ保護オフィサー（Data Protection Officer：ＤＰＯ）

ＧＤＰＲにおいては、「定期的かつ体系的な大規模監視を必要とする場合」、「大規模のセンシティブデータを処理する場合」には、「組織内部においてＧＤＰＲの遵守を監視するデータ保護責任者を選任する」とされている。

○　ＯＥＣＤプライバシー・ガイドライン

プライバシーマネジメントプログラムの構築や、個人データに影響を及ぼす重大なセキュリティ侵害があった場合等の関係者への通知について責任を有する者として、データ管理者（※）が位置付けられている。

※　国内法によって個人データの内容及び利用に関して決定権限を有する者を意味し、当該管理者又はその代理人が、当該データを収集、保有、処理若しくは提供するか否かは問わない。

○　ＪＩＳ Ｑ １５００１：２０１７における個人情報保護管理者及び個人情報保護監査責任者

トップマネジメント（経営層）が、個人情報保護管理者及び個人情報保護監査責任者を定め、それぞれ、以下に示すような責任及び権限を割り当てることが規定されている。

①個人情報保護管理者

個人情報保護マネジメントシステムの見直し及び改善の基礎として、トップマネジメントに個人情報保護マネジメントシステムの運用状況を報

告する。

②個人情報保護監査責任者

監査を指揮し、監査報告書を作成し、トップマネジメントに報告する。監査員の選定及び監査の実施を担い、監査の客観性及び公平性を確保する。

○　個人情報保護法（ガイドライン）

個人情報取扱事業者は、取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のため、必要かつ適切な措置を講じること、従業者及び委託先の適切な監督を行うことが求められている。そのためには、組織の在り方は様々であるとしても、何らかの形で担当者が定められることが適切と考えられる。

（４）事業者における自主的取組を促す仕組みの例

○　個人情報保護法（認定個人情報保護団体の個人情報保護指針）

個人情報保護指針とは、認定個人情報保護団体が、対象事業者の個人情報等の適正な取扱いの確保を目的として、個人情報に係る利用目的の特定、安全管理のための措置、開示等の請求等に応じる手続その他の事項又は匿名加工情報に係る作成の方法、その情報の安全管理のための措置等に関して、業界の特性等に応じた具体的な履行方法を定める自主的なルールである。

認定個人情報保護団体は、個人情報保護指針を作成するよう努めることとされており、認定個人情報保護団体は、個人情報保護指針の作成に当たっては、消費者の意見を代表する者その他の関係者の意見を聴きながら指針を作成するよう努め、作成後は、個人情報保護委員会に当該指針を届け出る必要がある。

○　情報信託機能の認定に係る指針ver1.0（総務省・経済産業省）

総務省及び経済産業省では、平成29年11月より、「情報信託機能の認定スキームの在り方に関する検討会」を開催し、本検討会において、いわゆる「情報銀行」に求められる情報信託機能[12]に関し、民間団体等による任意の認定制度の在り方について、平成30年６月「情報信託機能の認定に係る指針ver1.0」[13]を公表した。

この指針においては、情報セキュリティ等の基本原則として「国際標準・

[12] いわゆる「情報信託機能」は、情報銀行に関する各省庁の検討会で使用されている用語であって、個人情報の本人の指示又はあらかじめ指定した条件に基づき、個人情報等の第三者提供の可否を判断し、本人又はデータ保有者に代わって提供する機能を指すとされる。

[13] 「情報信託機能の認定に係る指針 ver1.0」は、一定の要件を満たした者を社会的に認知するため、民間の団体等による任意の認定の仕組みとして、総務省・経済産業省により策定された（平成 30 年 6 月 26 日公表）。同指針は、①認定基準、②モデル約款の記載事項、③認定スキームから構成され、認定を行う団体は、本指針に基づき、認定制度を構築・運用する。

国内規格の考え方も参考に、情報セキュリティ及びプライバシー保護対策を徹底すること(例：ＪＩＳ　Ｑ　１５００１　個人情報保護マネジメントシステム（要求事項)、ＩＳＯ/ＩＥＣ　２９１００（ＪＩＳ　Ｘ　９２５０）プライバシーフレームワーク)」が記載されている。

○　行動ターゲティング広告ガイドライン（一般社団法人日本インタラクティブ広告協会（ＪＩＡＡ))

インターネットユーザー（利用者）のウェブサイト上での行動履歴情報を収集し、そのデータを利用して広告を表示する行動ターゲティング広告に関して、会員社が遵守すべき基本的事項を定めたガイドラインである。

○　他の分野における認証や民間資格の例

他の分野において、事業者における望ましい取組として、認証マークを活用している事例も見られる。例えば、次世代育成支援対策推進法（平成15年法律第120号）に基づく「くるみん認定」(厚生労働省)、いわゆる女性活躍推進法に基づく「えるぼし認定」（厚生労働省）や、「健康経営優良法人制度」（日本健康会議)、「攻めのＩＴ経営銘柄」(経済産業省・東京証券取引所）など、様々な形で認証マークを活用して推奨している。

また、個人情報保護に関連する民間の資格制度として一般財団法人全日本情報学習振興協会が実施する「個人情報保護士」などがある。

（５）プライバシー影響評価制度（ＰＩＡ）の考えを取り入れた制度

自ら情報漏えい等のリスクを評価し、その対策を講じる趣旨を踏まえた制度として、以下のようなものがある。

○　特定個人情報保護評価

特定個人情報保護評価は、番号法に基づき、事前に特定個人情報の取扱いに関するリスクを分析し、その対策を講じることを対外的に明らかにすることにより、個人のプライバシー等の権利利益の侵害の未然防止、国民・住民の信頼の確保を目的とするものである。国の行政機関や地方公共団体等がマイナンバーを保有する前に自ら情報漏えい等のリスクを評価し、その対策について書面に記載して公表する制度であり、委員会のウェブサイトで公表している。

※　評価項目：Ⅰ 基本情報、Ⅱ 特定個人情報ファイルの概要、Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策、Ⅳ その他のリスク対策、Ⅴ 開示請求、問合せ、Ⅵ 評価実施手続について記載している。

※　2,852の評価実施機関が32,341の事務について特定個人情報保護評価書を公表している。（平成31年１月末時点）

○　生産性向上特別措置法における革新的データ産業活用計画の協議

「革新的データ産業活用計画」は、生産性向上特別措置法に基づき、一定のサイバーセキュリティ対策が講じられたデータ連携・利活用に必要となるシステムや、センサー・ロボット等の導入などにより短期間で生産性の向上を図ることを目的とするものであり、主務大臣が認定を行い、減税措置等を講ずるものである。

主務大臣による革新的データ産業活用計画の認定に際し、取り扱われるデータに個人情報が含まれる場合であって、特に必要があるものとして政令で定める場合に、主務大臣から委員会への協議が同法に定められている。

革新的データ産業活用計画の認定申請書においては、個人情報の取扱いに関する記載事項を以下のとおり定め、事業者は、個人情報保護法を遵守するために、リスク分析及びリスクを軽減するための措置を講じることについて記載することとなっている。

①　革新的データ産業活用において用いられる個人データの種類
②　計画の主たる目的として活用する個人データの内容及びその取扱いの方法
③　個人情報保護法及び関連法令等の遵守並びにそれを担保する方法

３．検討の方向性

（１）認定個人情報保護団体制度の充実

○　認定個人情報保護団体制度は、平成27年改正法において、マルチステークホルダーの意見を聴いた上での個人情報保護指針策定の努力義務や、対象事業者に対し、個人情報保護指針を遵守させるための措置が努力義務から義務へ変更されるなど、役割の強化がなされた。

○　認定個人情報保護団体制度は、民間事業者による自発的取組を促すことで個人情報の保護のレベルを高めることを狙った我が国独自の制度であったが、事業者の自発的な取組を法規制の重要な要素として位置付ける仕組みとして、ＥＵのＧＤＰＲにおいても認証制度が導入されるなど、国際的にも注目される仕組みである。

○　認定個人情報保護団体のうち、一部の団体では、積極的に対象事業者を指導・支援したり、個人情報保護指針で独自ルールを定めたりするなどの取組が行われている。しかし、一部の団体においては、対象事業者のない団体等、必ずしも積極的でない団体も存在している。

○　また、認定個人情報保護団体制度については、加入状況の観点から課題も存在する。例えば、

・個人情報保護法が平成27年改正法以前は、各主務大臣制であった影響もあり、構成団体の多くが業界単位となっていること

・インターネット関連サービス業等、業態が多様化しているものについては、必ずしも「業界団体」に加入していない事業者も多く、加入率が低い傾向にあること

などが挙げられる。

○　今後、認定個人情報保護団体制度の重要性に鑑み、その期待される役割が十分に発揮されるよう、以下の（２）に掲げる事項と併せ、認定個人情報保護団体の活動を活性化させる観点と、認定団体の対象事業者となることのメリットを高める観点との両面から、制度の在り方や、委員会による支援の在り方について検討を深めていく必要がある。

○　委員会による支援としては、現在、認定個人情報保護連絡会を定期的に開催し活動に有用な情報の提供や、団体相互の情報共有等の促進を図っている。また、平成30年度は、対象事業者となるメリットを提供する趣旨で、新たな取組として、対象事業者向け実務研修会を全国５か所で開催している。さらに、認定個人情報保護団体シンポジウムを開催し、認定個人情報保護団体制度や、個別の団体の活動の状況、対象事業者となることの意義等について、周知、広報に努めている。

○　一方、制度の在り方については、認定個人情報保護団体制度が、現状、企業単位での加入が前提となっている点が、活動の幅を制約しているとの見方がある。大企業等、幅広い事業分野を有する企業については、企業側から見た場合、企業全体の業務に対応した認定個人情報保護団体を見つけることが難しい場合が想定される。また、逆に認定個人情報保護団体側から見ると、当該団体の特性に適さない部門も含め、対象事業者となる企業全体に関する業務に対応せざるを得ない可能性がある。実際、委員会が行った経済関係団体へのヒアリングにおいても、この点を指摘する意見もあった。このような状況を踏まえ、認定個人情報保護団体制度の長所も活かしつつ、例えば、特定の分野に特化し、指針等ルール単位や分野単位で認定等を行う新たな仕組みを設けることが考えられる。

（２）民間の自主的取組の推進

○　個人情報保護法は、認定個人情報保護団体制度を含め、民間事業者の自主

的な対応を尊重する制度設計が行われてきており、民間の自主的取組が促進されるような仕組みは、法の趣旨からも望ましいものと考えられる。

○　特に、インターネットなど、新たな利用分野では個人情報保護に関する問題が発生しやすいが、このような分野ではビジネスモデルの変革や技術革新等も著しいことから、法の規定を補完する形で、民間主導で自主ルールが策定、運用されることは望ましく、これらの取組が促進される仕組みを検討する必要がある。

○　個人データの取扱いに関する責任者の設置、ＰＩＡの取組、企業の自主的な取組を推奨する仕組みなどについて、他の政策分野で例のある手法も参考としつつ、検討を深めていくことが考えられる。

○　特に、ＰＩＡについては、評価書の作成に係る事業者の負担を考慮に入れつつ、特に、大量の個人データを扱う事業者にとっては、このプロセスを通じた事前評価を行うことで、個人データの管理や従業員への教育効果等も含め、事業者自身にとって、効率的かつ効果的に必要十分な取組を進めるための有用な手段であることを踏まえ検討する必要がある。

第４節　データ利活用に関する施策の在り方

１．匿名加工情報制度

（１）制度の概要

○　匿名加工情報制度は、個人情報よりも緩やかな規律の下、事業者間のデータ取引やデータ連携を含むパーソナルデータの利活用を促進することを目的に、平成27年改正法により新たに導入された制度である。

（２）活用の状況

○　匿名加工情報の作成・提供に係る公表状況を調査したところ、平成30年度末時点で約380社の事業者が公表しており、様々な業種において匿名加工情報の活用が進展しつつある。特に、調剤薬局や健保組合など、ヘルスケア分野において、匿名加工情報の活用が進んでいる。

○　委員会では、パーソナルデータを含むビッグデータの適正な利活用環境の整備に向けて、匿名加工情報について、認定個人情報保護団体等が自主ルールを策定する際の、また事業者において同制度を利用する際の参考とするため、「匿名加工情報　パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて」と題する事務局レポートを作成し、平成29年２月27日に公表した。加えて、事例集の公表[14]を行い、小売、調剤薬局、健保組合の事例等、具体的な事例について情報発信を行っているところである。

○　委員会が事業者に対して実施したアンケート調査によれば、匿名加工情報の利活用に係るメリットとしては、個人情報漏えいリスクの低減、第三者提供や目的外利用について本人同意が不要など手続の負担軽減、本人同意が不要なため大量のデータを利活用できる、との回答が多くなっている。一方、課題としては、匿名加工情報についてよく知らないとの回答が一番多く、次いで、利用方法が分からない、自社データへのニーズがあるのか分からない、分析するための人材がいない、レピュテーションリスク等が心配、の順となっている。

○　なお、認定団体における取組状況としては、43団体中21団体が、個人情報保護指針において、匿名加工情報に関する規定を盛り込んでいる。

（３）ＥＵのＧＤＰＲにおける匿名化及び仮名化との比較

○　我が国の匿名加工情報については、「特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人

[14] 個人情報保護委員会事務局「匿名加工情報・個人情報の適正な利活用の在り方に関する動向調査（事例集）」（平成 30 年 3 月）

情報を復元することができないようにしたもの」（個人情報保護法第２条第９項）と定義されており、作成・提供に関する義務や再識別の禁止が規定されている。

○　一方、ＧＤＰＲでは、匿名化（Anonymisation）については、前文に関連した記載はあるものの、定義は条文自体には規定されていない。運用上の規律としては、元の個人データを本人が特定されないように加工するとともに、加工手法等に関する情報を削除することが匿名化の条件とされている。

○　また、ＧＤＰＲの仮名化（Pseudonymisation）については、「追加的な情報が分離して保管されており、かつ、その個人データが識別された自然人又は識別可能な自然人に属することを示さないことを確保するための技術上及び組織上の措置の下にあることを条件として、その追加的な情報の利用なしには、その個人データが特定のデータ主体に属することを示すことができないようにする態様で行われる個人データの取扱いを意味する。」（第４条(5)）とされている。運用上の規律としては、第25条のデータ保護バイデザインや第32条の取扱いの安全性において、適切な技術的及び組織的な措置の例として挙げられている。また、個人データよりも負荷の軽い規律となっており、第11条(2)には、データ主体が、自己の権利の行使の目的のために、自身の識別ができるようにする付加的な情報を提供する場合を除き、第15条から第20条までの規定（※）は適用されないとされている。

※　第15条（データ主体によるアクセスの権利）、第16条（訂正の権利）、第17条（消去の権利（「忘れられる権利」））、第18条（取扱いの制限の権利）、第19条（個人データの訂正若しくは消去又は取扱いの制限に関する通知義務）、第20条（データポータビリティの権利）

２．その他データ利活用に関する施策の現状

（１）次世代医療基盤法

○　次世代医療基盤法は、医療分野の研究開発に資するための匿名加工医療情報に関し、匿名加工医療情報作成事業を行う者の認定、医療情報等及び匿名加工医療情報の取扱いに関する規制等について定めることにより、健康・医療に関する先端的研究開発及び新産業創出を促進し、もって健康長寿社会の形成に資するため、平成30年５月に施行されたものである。具体的には、高い情報セキュリティを確保し、十分な匿名加工技術を有するなどの一定の基準を満たし、医療情報の管理や利活用のための匿名加工を適正かつ確実に行うことができる者（以下「認定事業者」という。）を認定する仕組みを設けるものであり、医療機関等は、あらかじめ本人に通知し、本人が提供を拒否しない場合、認定事業者に対して医療情報を提供できることとしている。この

認定事業者の認定を主務大臣（内閣総理大臣、文部科学大臣、厚生労働大臣及び経済産業大臣）が行うに当たっては、委員会への協議が義務付けられている。

（２）生産性向上特別措置法（革新的データ産業活用計画の認定制度）

○　革新的データ産業活用計画を認定し、一定のサイバーセキュリティ対策が講じられたデータ連携・利活用に必要となるシステムや、センサー・ロボット等の導入などにより短期間で生産性の向上を図ることができるようＩｏＴ設備投資への減税措置や金融上の支援を講じるもので、計画の認定に際し、取り扱われるデータに個人情報が含まれる場合であって、特に必要なものとして政令で定める場合には、委員会への協議が法定されている。

３．パーソナルデータの利活用に関する民間事業者等による取組

情報銀行やデータ取引市場などの取組が進展するほか、ＡＩ・ＩｏＴ技術の進展に伴い、コネクテッドカーやＡＩスピーカーのほか、ＡＩスコアリングやターゲティング広告などの取組も進展している。特にコネクテッドカーやＡＩに関しては、ＩＣＤＰＰＣでも議論がなされている。

（１）情報銀行

○　情報銀行は、個人とのデータ活用に関する契約等に基づき、ＰＤＳ（Personal Data Store）等のシステムを活用して個人のデータを管理するとともに、個人の指示又は予め指定した条件に基づき個人に代わり妥当性を判断の上、データを第三者（他の事業者）に提供する事業である。

○　総務省及び経済産業省は、平成29年11月より、「情報信託機能の認定スキームの在り方に関する検討会」を開催し、本検討会において、いわゆる「情報銀行」に求められる情報信託機能に関し、民間団体等による任意の認定制度の在り方について、平成30年６月「情報信託機能の認定に係る指針ver1.0」を公表したところである。

○　民間団体による自主的取組として、「情報銀行」事業を審査・認定する「情報銀行認定」事業が開始されている。

（２）データ取引市場

○　データ保有者と当該データの活用を希望する者を仲介し、売買等による取引を可能とする仕組み（市場）である。

○　平成29年11月にデータ流通ビジネスに積極的に取り組む企業数十社によ

り「データ流通推進協議会」が設立され、民間主導でのデータ流通事業者認定制度構築を視野に入れた検討が開始された。

○　同協議会では、データ提供者・利用者の双方が安心してデータ流通に参加する上での基盤となるデータ流通事業者が満たすことが望ましい事項や、具体的な認定制度運用の在り方を検討するため、「運用基準検討委員会」、「技術基準検討委員会」、「利活用促進委員会」及び「認定・監査委員会」の４つの委員会が設けられ、産業界・政府・学識経験者等を交えての議論が進められている。

○　平成30年９月には、データ提供者とデータ利用者の仲介と決済を提供するデータ取引市場運営事業者認定基準「データ取引市場運営事業者認定制度_D2.0」が策定・公開されている。

（３）ＡＩ・ＩｏＴの利活用の状況

○　昨今、世界中の様々なものがインターネットにつながるＩｏＴ時代が到来し、世界のＩｏＴデバイス数の推移などを見てもＩｏＴデバイスの伸長が見込まれている。また、ＡＩの発達を受けて、様々なサービスの展開が進んでおり、例えば、ＡＩのパーソナルアシスタント機能を活用したＡＩスピーカーについては、大手ＩＣＴ事業者が音声対話型サービスを市場に投入しており、音声情報の活用が進んでいる。また、ＡＩスコアリングについては、Ｊスコアや芝麻信用など、顧客の信用力をスコア化するサービス提供が進展している。

○　こういったＡＩ・ＩｏＴの活用の進展により、多様な分野で新たなサービス等の進展が期待される一方、ビジネス生態系の変化とともに、新たなルールの必要性について指摘する意見もある。

○　我が国においては、政府全体のＡＩに関する検討が進んでいる。例えば、内閣府が事務局を務める「人間中心のＡＩ社会原則会議」は、７つの原則[15]からなる「人間中心のＡＩ社会原則」を取りまとめ、国内外から広く意見を募った上で、本年３月29日に本原則を策定した。この原則の中では、プライバシー確保の原則において、パーソナルデータが本人の望まない形で流通したり、利用されたりすることによって、個人が不利益を受けることのないよう、パーソナルデータを扱わなければならない旨記載されている。

15　AI 社会原則は、「AI-Ready な社会」において、国や自治体をはじめとする我が国社会全体、さらには多国間の枠組みで実現されるべき社会的枠組みに関する原則であるとして、「人間中心の原則」「教育・リテラシーの原則」「プライバシー確保の原則」「セキュリティ確保の原則」「公正競争確保の原則」「公平性、説明責任及び透明性の原則」「イノベーションの原則」が挙げられている。

○　また、第40回ＩＣＤＰＰＣでも、「ＡＩにおける倫理及びデータ保護についての宣言」において、「強力なデータ保護及びプライバシー保護措置は、データ処理過程における個人の信頼の構築に資し、データ共有を推進することによりイノベーションを促進するとされているとともに、ＡＩシステムの開発・使用等においては、人間の尊厳等と同様に、個人データの保護及びプライバシーの権利が尊重されなければならず、個人がＡＩシステムの管理及び理解を維持できる解決策が提供されなければならない」としており、ＡＩの開発における人権保護のための本質的価値として、６つの指導原則[16]を支持している。また、ＩＣＤＰＰＣでは、同宣言に沿った指針を定めるため、ＡＩワーキンググループが創設され、委員会もメンバーとして参加している。

４．ターゲティング広告

（１）概要

○　インターネット広告ビジネスでは、インターネットユーザーの個人関連情報[17]（登録情報、行動履歴情報、デバイス情報などで個人情報及び個人情報以外のユーザーに関する情報が含まれる。）を取得し、利活用している。このように、利用者の様々な情報を活用した広告の配信等が行われ、これは一般にターゲティング広告などと呼ばれている。ターゲティング広告は、企業にとって有用であると同時に、利用者にとっても興味関心のある広告に接する機会が増えるという利点がある。ターゲティング広告の配信までの流れとしては、サイト訪問時に、クッキーや広告ＩＤ等と結び付いた利用者のサイト訪問履歴等が取得され、広告配信に利用されるというものがある。

---

[16] ICDPPC は、AI の開発における人権保護のための本質的価値として、次の指導原則を支持する。
1. AI 及び機械学習の技術は、基本的人権を尊重し、公正の原則に従ってデザイン、開発及び使用されるべき。
2. AI システムは、説明責任と同様に、その潜在的な影響及び結果に対する継続的な注意及び警戒が確保されるべき。
3. AI システムの透明性及び明瞭性は、効果的な執行の観点から、改善されるべき。
4.「エシックス・バイ・デザイン」の全体アプローチの一部として、AI システムは、プライバシー・バイ・デフォルト及びプライバシー・バイ・デザインの原則の適用により、責任をもってデザインされ開発されるべき。
5. すべての個人の権限強化が推進され、広範な参画の機会の創設と同様に、個人の権利行使が促進されるべき。
6. AI におけるデータの使用の結果もたらされるであろう違法なバイアス又は差別は軽減及び緩和されるべき。
※ICDPPC では、同宣言に沿った指針を定めるため、AI ワーキンググループが創設され（個人情報保護委員会もメンバーとして参加）、2019 年 10 月予定の第 41 回 ICDPPC に向けて、より具体的な指針を策定予定。（平成 31 年3月4日第 91 回委員会資料から）

[17] 第 98 回個人情報保護委員会（平成 31 年3月 29 日）における一般社団法人日本インタラクティブ広告協会（JIAA）説明資料から引用。JIAA のプライバシーガイドラインにおいて「個人情報およびインフォマティブデータのうち統計情報等を除いた部分を総称していう。」と定義。なお、インフォマティブデータは、「個人を特定することができないものの、プライバシー上の懸念が生じうる情報、ならびにこれらの情報が統計化された情報であって、特定の個人と結びつきえない形で使用されるもの」とされている。

○　ターゲティング広告の実態は多様であるが、代表的には、以下のようなものがある。[18]

・属性ターゲティング広告

　ユーザーが自ら登録を行った年齢、性別、居住地等の属性情報を利用して広告を配信

　例）サイトに年齢と性別を登録したユーザーをその年代・性別に分類（35歳・男性と登録→30代男性のユーザー）

・行動ターゲティング広告

　ユーザーの閲覧履歴や購買履歴等の行動履歴情報から、興味関心や消費行動を類推して広告を配信

　例）サイトを訪問したユーザーをそのサイトカテゴリーに関連した商品を購入しそうなユーザー群に分類（海外旅行に関するコンテンツを閲覧→旅行に興味がありそうなユーザー）

・リターゲティング広告

　ユーザーが訪れた広告主サイトでの行動履歴情報を基に、その広告主サイトへの再訪を促す広告を配信

・コンテンツターゲティング広告

　ユーザーの情報を利用せず、ユーザーが閲覧しているサイトのコンテンツに合った広告を配信

○　ターゲティング広告では、ＰＣやスマートフォン等のブラウザごとのクッキー上に発行されるＩＤに紐付いて蓄積される情報（サイト閲覧履歴等）や、スマートフォン等のＯＳが発行する広告識別子に紐付いて蓄積される情報が使われることが多いとされる。これら端末識別子は、一般には、それ単体では個人識別性を有しないため、個人情報保護法上の個人情報とは解されない。ただし、このような端末識別子であっても、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場合は、個人情報となる。

（２）消費者のプライバシーに関する懸念

○　利用者に関する情報を活用したターゲティング広告は、前述のとおり、企業にとって有用であると同時に、利用者にとっても興味関心のある広告に接する機会が増えるという利点がある。

○　しかし、ターゲティング広告を巡っては、以前から、消費者からプライバ

[18] 第98回個人情報保護委員会（平成31年3月29日）における一般社団法人日本インタラクティブ広告協会（JIAA）説明資料から引用。

シーに対する懸念等が指摘されてきており、例えば、知らないうちにデータが収集されること、個人の詳細なプロファイルが集積されることによるリスク、センシティブ情報が悪用されるおそれ[19]などである。

○　特に、最近は、スマートフォンの普及等により、ウェブ上の検索履歴や閲覧履歴のみならず、位置情報を含めた広い意味での行動履歴が利用され得る状況にある。このような幅広い情報を膨大に収集し、解析、利用することについて、プライバシー上懸念があるとの意見もある。

（３）自主ルールによる規律

○　日本インタラクティブ広告協会（ＪＩＡＡ）では、ユーザーがプライバシーに関する懸念や広告に対する不信感を抱くことのないよう、事業者はユーザーに対して、どの事業者が取得したどのような情報が広告に利用されているのか、ユーザーが容易に知ることができ、十分な情報を基にデータの取得又は利用の可否を選択できる簡便な仕組みを提供する必要があると考え方の下、インターネット広告ビジネスのために取得される個人関連情報の取扱いに関して、「プライバシーポリシーガイドライン」及び「行動ターゲティング広告ガイドライン」を策定、技術の進展やビジネスの実態の変化に応じて、継続的かつ機動的に見直しを行うなどの取組を推進している。

○　「プライバシーポリシーガイドライン」においては、クッキー等の識別子情報や位置情報、閲覧履歴、購買履歴といったログ情報等の個人に関する情報で、個人を特定することができないもののプライバシー上の懸念が生じ得る情報を「インフォマティブデータ」としている。個人情報保護法における「個人情報」と「インフォマティブデータ」から「統計情報」を除いたものを「個人関連情報」として、取扱基準を定めている。

○　また、「行動ターゲティング広告ガイドライン」においては、行動履歴情報を利用した行動ターゲティング広告でのユーザーへの「透明性の確保」（データの取扱いについての分かりやすい説明）と「関与（オプトアウト）の機会の確保」（データの取得又は利用の可否を容易に選択できる手段の提供）の徹底を原則としている。広告配信経路が複雑化し、事業者が複数のサービスを組み合わせ提供している現状に合わせ、事業領域を「媒体運営者」、「情報取得者」、「配信事業者」に区分して定義を明確にし、その事業領域ごとに遵守事項を規定している。

---

[19] 米国連邦取引委員会（FTC）行動ターゲティング広告に関するタウンミーティングでの問題提起（2007年）（第98回個人情報保護委員会（平成31年3月29日）における一般社団法人日本インタラクティブ広告協会（JIAA）説明資料から引用）

５．検討の方向性

（１）匿名加工情報制度

○　匿名加工情報については、既に一定程度の活用が進みつつあるところであるが、企業アンケート結果にあった、利用方法が分からない、自社データへのニーズがあるのか分からない、分析するための人材がいない、レピュテーションリスク等といった意見は、いずれも、具体的な匿名加工情報の利活用モデルについて、必ずしも企業が把握できていないことも大きな背景の一つと考えられ、委員会として、引き続き、具体的な利活用モデルやベストプラクティス等を発信していくことが重要である。

（２）「仮名化」の検討

○　ＥＵにおいては、個人情報としての取扱いを前提としつつ、若干緩やかな取扱いを認める「仮名化」が規定され、国際的にもその活用が進みつつある。

○　我が国においても、「仮名化」のような個人情報と匿名加工情報の中間的規律の必要性については、従前から経済界からの要望もあるところであるが、具体的なニーズの有無、開示請求や利用停止等本人関与の在り方を含めた規律の在り方等について、ＥＵの規律のレベルの実態、国際的な動向も踏まえ、具体的に検討していく必要がある。

（３）技術の進展に伴うデータ利活用への対応

○　技術の進展に伴い、データを活用した新たなサービスが次々と生まれてきているところである。これはイノベーションが促進されている証であるが、その中における個人情報の取扱いについては、実態を踏まえて対応していくことが重要である。

○　このような取扱いについては、個人情報保護法に直接関係する論点もあれば、同法とは直接は関係しない論点もあり、その実態に応じて論点も多様であることが想定される。委員会としては、まずは法令の規定に即し対応を行っていくこととなるが、その際、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という同法の趣旨を踏まえ、検討することが重要である。

○　例えば、産業界からは、ガイドライン等での法の解釈の明確化を求める意見もあるが、一方で、技術の進展が早い中、法解釈を固定化することで、イノベーションを阻害するおそれがあるのでないかという声もある。ガイドライン等については、この両面を踏まえつつ、委員会として、産業界からの意見を含め、広く継続的に意見を聴いていく必要がある。

○　また、委員会としては、企業や行政機関における検討に対しても、できるだけオープンな形で対応していくことが重要と考えられる。特に、企業が個人情報について、利活用を含め、より相談しやすい環境を求める意見は多く聴かれるところであり、具体的にどのような体制が考えられるか検討する必要がある。

（４）データ利活用に関する国際的な取組の必要性

○　国際的なデータ利活用を促進する上でも、個人データの保護が適切になされていることが重要である。今年はＡＰＰＡやＧ２０サイドイベントが予定されているところであるが、引き続き、個人データの保護と利活用について、国際的な議論をリードしていくことが重要である。

○　特に、ＡＩと個人データ保護・プライバシーとの関係については、データ保護プライバシー・コミッショナー国際会議でも議論が始まっている。ＡＩについては、我が国でも関係省庁での議論が進められているところであり、国際協調の観点等からも、ＡＩとデータ保護との議論について、国内の議論の状況を踏まえた上で、積極的に貢献していくことが重要である。

（５）ターゲティング広告を巡る対応の在り方

○　ターゲティング広告については、現在広くインターネット広告で活用されている手法の代表例と言えるが、実態は非常に複雑かつ多様である。

○　提供元では必ずしも個人情報でない場合であっても、提供先で照合可能な情報が保有され、個人情報になる可能性や、多様な機器・サービスから詳細な情報が集積的に統合され、特定の個人を識別でき個人情報と同値になる可能性等も考えられる。

○　ターゲティング広告のベースとなるウェブ技術は進化が著しく、本来、イノベーションを阻害することを避ける観点からも、まずは、自主ルール等による適切な運用が重要である。自主ルール等については、強制力や自主ルール等に参加していない者の存在など、一定の限界があるのも事実であるが、今後、可能な限り民間の自主性を活かしつつ、認定個人情報保護団体制度等を活用するなど自主ルールを執行可能な形としていくことを含め検討する必要がある。

○　クッキー等について、例えば、一定の要件に該当するものについて個人情報保護法上の個人識別符号とするなど、その位置付けを明確化することも考

えられるが、クッキー等自体は、「識別子」としてセッション管理[20]を含め広範に用いられる技術であり、利用特性も多様であることから、現行法の規定に加えて、クッキー等をあえて個別に規律する必要性含め、慎重に検討する必要がある。

○　一方、クッキー等であっても、会員情報等と紐付けられ特定の個人を識別できるような場合は、個人情報保護法上の個人情報として取り扱われる必要がある。しかし、事業者の中には理解不足と思われる事例も散見されるため、今後、委員会としても、実態を注視しつつ、適切に執行を行っていく必要がある。

[20] ユーザーがログインしてから、ログアウトするまで、ログイン情報を保持したままページを移動できるよう、複数の Web ページからなる一連のやりとりを管理する仕組み

第５節　ペナルティの在り方

１．我が国における現状

（１）制度の概要

○　個人情報保護法における個人情報取扱事業者に対する罰則は、大きく分けて３類型が存在する。

①　個人情報データベース等不正提供罪

業務に関して取り扱った個人情報データベース等を自己若しくは第三者の不正な利益を図る目的で提供し、又は盗用した場合

【１年以下の懲役又は50万円以下の罰金】

②　命令違反

委員会による命令に違反した場合

【６月以下の懲役又は30万円以下の罰金】

③　虚偽の報告・資料提出、立入検査拒否

委員会による報告徴収・資料提出要求・質問・検査を拒否し、又は虚偽を述べた場合や、認定個人情報保護団体が、委員会に対して認定業務に関する報告をせず、又は虚偽の報告をした場合

【30万円以下の罰金】

（２）監督の状況

○　委員会では多様な手法を通じて個人情報の取扱いの実態把握に努めており、漏えい等報告のほか、委員会への情報提供・苦情や報道、ソーシャルモニタリング等を端緒として、漏えい等事案や個人情報等の不適切な取扱いを把握し、必要に応じて、立入検査、報告徴収、指導・助言等を行っている。その対象としては、個人データの漏えい等事案が最も多く、そのほかに個人情報取扱事業者による個人情報の不適切な取得、本人同意を得ていない個人データの第三者提供等の事案がある。

○　個人データの漏えい等事案に係る監督は、被害拡大・二次被害の防止のための対策や適切な再発防止策の策定・履行の状況の確認などであるが、おおむね、委員会による指導等を通じて、事業者による個人情報等の適切な取扱いが確保されていると考えられる。平成27年改正法の施行から平成30年度末時点までにおいて、委員会が勧告及び命令を行った事例、個人情報取扱事業者に対し個人情報保護法に基づく罰則が適用された事例は存在しない。

○　委員会による指導等の代表的なものとして、以下のような事例がある。

＜国内にある事業者の事案＞

・　不正アクセスや職員による不正持出しを発生原因とする漏えい事案について、立入検査等を実施し安全管理措置等の状況を確認するとともに、技術的安全管理措置の改善のほか、組織体制の抜本的な見直しを行うよう指導・助言を行った。

・　不正アクセスを発生原因とする漏えい事案について、再発防止策の実施等に関し、ウェブサイトのプログラム修正を行った場合には、当該ウェブサイトのリリース前にセキュリティチェックを行う必要があることなどについて指導を行った。

・　事業者が個人情報を不適切に取得していた事案について、個人情報保護法に基づく報告を求め、再発防止策の実施を指導するとともに、その実施状況についても報告を求め、改善状況を確認した。

・　その他、本人同意を得ずに従業員等が顧客の個人データをウェブサイトに掲載したとの情報提供について、事業者に対し事実関係を確認の上、個人情報の適正な取扱いに関し、従業員等に周知・徹底するように指導を行った事案や、開示請求を受け付けないとする事業者に、適切に対応するよう指導を行った。

＜国外にある事業者の事案＞

・　国外に所在する事業者の漏えい等により、当該事業者のサービスを利用していた国内事業者の顧客の個人データが漏えいした事案について、当該外国の事業者に対しサービスを利用する国内事業者のリストの提出を求め、国内事業者に漏えい等報告の提出を促した。

・　海外の個人情報保護当局に対し、委員会の対応状況について情報提供を行うとともに漏えい等事案の発生原因や再発防止策について情報の共有を求めるなど、海外の個人情報保護当局との執行協力を行った。

・　国外に所在する事業者がソーシャルプラグインを設置している他のウェブサイトを閲覧した場合、ボタンを押さなくてもユーザーＩＤやアクセス履歴等の情報が当該事業者に送信されてしまうことや、過去に取得した個人情報の一部が第三者に不正に提供されたケースがあったことから、①ユーザーへの分かりやすい説明や本人からの同意の取得の徹底、②同社がプラットフォーマーとしての責任を認識し、プラットフォーム上のアプリケーションの活動状況の監視を徹底すること等を指導した。

２．諸外国の現状

○　米欧など諸外国でも、ペナルティに係る制度は整備されているが、①行政上の手続としての制裁金の有無、②金額の多寡、③域外適用される規定の範

囲に関し差異が見られる。

○　特に、諸外国での最近の立法例として、ＧＤＰＲのように極めて高額な制裁金の事例も見られる。具体的には、ＧＤＰＲでは「効果的であり、比例的であり、かつ、抑止力のあるものであることを確保する」として、ＧＤＰＲ違反に対して、最大2,000万ユーロ以内又は前年度の全世界総売上高の４％のうち高い方を上限とする極めて高額な制裁金が科されうることが規定された。

＜ＧＤＰＲの例＞

・上限金額：　制裁金の上限には２種類あり、事業者の義務違反等に対する制裁金よりも、データ主体の権利、個人データの移転、監督機関の命令への不服従等の違反行為に対する制裁金は２倍重く設定されている。

・位置付け：　制裁金は行政罰の位置付けで、行政上の手続を通じて科される。

・裁量性：　制裁金の上限金額は著しく高額である一方で、軽微な違反行為に対しては、注意処分とすることもできる。制裁金を科すか否か、制裁金の多額については、データ取扱いの性質や故意又は過失等の11の評価要素[21]に基づき判断される。

○　また、ＧＤＰＲでは、ＥＵ域内に所在するデータ主体に対する商品又はサービスの提供やデータ主体のＥＵ域内における行動の監視に関する個人データ処理について、原則として全ての規制が適用されるとされる。

３．我が国の法令に基づき賦課される金銭の性質

○　我が国の法令上の整理では、法令に基づき賦課される金銭の種類には、課徴金、罰金、過料、科料などがある。このため、ペナルティの議論をする際には、金額の大小のみでなく、賦課される金銭の性質に応じた検討が必要と

[21] GDPR第 83 条第2項において、以下の 11 項目が挙げられている。
① 関係する取扱いの性質、範囲及び目的を考慮に入れた上で、違反行為の性質、重大性及び持続期間、並びに、その違反行為によって害を受けたデータ主体の人数及びデータ主体が被った損害の程度、② 違反行為の故意又は過失、③ データ主体が被った損失を軽減するために管理者又は処理者によって講じられた措置、④ 管理者又は処理者によって実装された技術上及び組織上の措置を考慮に入れた上で、管理者又は処理者の責任の程度、⑤ その管理者又は処理者による過去の関連する違反、⑥ 違反を解消するための、及び、違反の潜在的な悪影響を低減させるための、監督機関との協力の程度、⑦ 違反によって影響を受けた個人データの種類、⑧ その違反が監督機関の知るところとなった態様、とりわけ、その管理者又は処理者がその違反を通知したのかどうか、及び、通知した場合、どの範囲で通知したのか、⑨ 関係する管理者又は処理者に対し、同じ事項に関して、第 58 条第 2 項に規定する措置が過去に命じられていた場合、それらの措置の遵守、⑩ 承認された行動規範の遵守、又は、承認された認証方法の遵守、⑪ その違反行為から直接又は間接に得た財産的な利益若しくは回避された損失のような、その案件の事情に適用可能な上記以外の悪化要素又は軽減要素

なる。

○　課徴金には独占禁止法、金融商品取引法等の例があるが、一般に、国がその司法権又は行政権に基づいて国民に賦課し国民から徴収する負担で租税以外のものであり、刑罰ではなく行政上の措置となっている。課徴金の場合、課徴金の納付等に係る手続や、課徴金の計算基準については、法令レベルで詳細に定められている。

○　罰金については、例えば個人情報保護法第83条（個人情報データベース等不正提供罪）等があるが、財産刑（刑罰）の一種であり、罰金の額は、原則として１万円以上とされている（刑法第15条）。

○　科料については、例えば軽犯罪法等の例があるが、財産刑（刑罰）の一種で、科料の額は、原則として1,000円以上、１万円未満（刑法第17条）となっている。

○　過料については、例えば個人情報保護法第88条（認定個人情報保護団体の届出義務違反等）等があるが金銭罰の一種であり、刑罰ではなく、行政罰の一種である行政上の秩序罰として、「過料」が科されるものである。

４．検討の方向性

○　個人情報保護法では、個人情報取扱事業者に課される罰則について最大でも１年以下の懲役又は50万円以下の罰金とされていることから、現行のペナルティの体系では実効性が不十分な事業者を念頭に、ペナルティの強化が必要との議論がある。

○　平成27年改正法の施行後の国際的状況を見ると、ペナルティの強化が大きな潮流となっているのは否定できない。しかし、国際比較の観点では、各国ごとに国全体の法体系やペナルティに対する考え方に違いがあり、我が国の実態、法体系に照らして望ましい在り方を検討していく必要がある。

○　現状においては、不適正な個人情報の取扱いがあった場合、捕捉された案件に関しては、委員会による指導等により違法状態が是正されているのが実態であり、勧告・命令や罰則の適用事例は存在しない。これは、企業にとって、消費者からの信頼を失うことのコストが大きいことなどが背景として考えられる。実際、ヒアリングにおいても、産業界からは、事業者は個人情報保護法を遵守しており、ペナルティの引上げに慎重であるべきとの意見があった。

○　また、課徴金の導入や罰則の引上げなどのペナルティ強化については、個人の権利利益の保護に資するとの見方がある一方で、事業者の過度な萎縮を招き、ひいては創意工夫や技術革新の果実を国民が十分に享受できなくなる可能性があるとの見方もあり、ペナルティの相当性についての比較衡量が必要である。

○　加えて、改正個人情報保護法では、いわゆる5,000件要件が撤廃されたこともあり、事実上全国民がステークホルダーとなる裾野の広い法律となったため、ペナルティも、国内の中小事業者も含めて広範囲に適用対象になり得ることに留意が必要である。その影響の大きさに鑑み、立法事実を精査の上、議論する必要がある。

○　課徴金制度について導入を求める意見もあるが、我が国他法令における立法事例の分析も併せて行う必要がある。また、目的達成のための手段として、罰則の強化や、勧告措置や外国当局との執行協力で担保されている現行の域外適用の仕組みでは果たして不十分なのか、罰則とは別に課徴金を導入する必要があるのかについても、様々な観点から検討する必要がある。

第６節　法の域外適用の在り方及び国際的制度調和への取組と越境移転の在り方

１．我が国における現状

（１）制度の概要

○　社会経済のグローバル化を含むビジネスモデルの多様化に伴い、個人情報が多様な形態により海外で取得・処理されていることを踏まえ、平成27年改正法により、いわゆる域外適用に関する規定が導入された。

○　個人情報保護法第75条では、外国における個人情報の取扱いについて、国内にある者に対する役務等の提供に関連してその者を本人とする個人情報を取得した個人情報取扱事業者を規律対象としており、同法第４章第１節（個人情報取扱事業者の義務）の規定の多くが適用対象となっている。また、委託等の契約等に基づき取得した海外の事業者に対する規律は、本人から直接取得した委託元等の事業者を規律対象とすることで、間接的に規律される形態となっている。なお、委託等に拠らない場合、提供先の事業者には提供元事業者を通じた間接的規律が及ばないが、原則、提供に係る本人の同意が前提となる。

○　加えて、個人情報保護法第78条では、外国執行当局への必要な情報提供に関する規定も整備された。外国の事業者が日本にある者の個人情報を不適切に取り扱った場合に、外国の執行当局が外国の法令に基づく執行をすることができるよう、必要な情報提供を行うことができることとされた。本規定により、相互主義に基づき、我が国も外国執行当局に対し、情報の提供を求めることが可能となった。

○　委員会は、国際的な執行協力の枠組みであるＧＰＥＮ（グローバルプライバシー執行ネットワーク）に正式メンバーとして参加するなど、外国の執行当局との連携を強化してきており、外国執行当局とも連携しつつ、日本にある者に対して、サービス等を提供する外国事業者に対しても、措置をとっている。

○　また、平成27年改正法により個人データの越境移転に関する規制も新たに導入された。個人情報保護法第24条では、個人情報取扱事業者が個人データを外国にある第三者に提供するに当たっては、①当該第三者が、我が国と同等の水準にあると認められる個人情報保護制度を有している国として委員会規則で定める国にある場合、②当該第三者が、個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制として委員会規則で定める基準に適合する体制を整備している場合、③第三者提供の制限の例外（個人情報保護法第23条第１項各号）に該当する場合、のいずれかに

該当する場合を除き、あらかじめ外国にある第三者への個人データの提供を認める旨の本人の同意を得る必要があることとされた。

（２）国際的制度調和への取組

○　我が国は、様々な国際枠組みの多くに関わっている国の一つであるが、一方で、アジア太平洋地域を中心とする日本と関係の深い多くの国々が参加する枠組みと、ＥＵが参加する枠組みとは、重なる部分が少なく、これらの国々を含めた国際的な枠組みを目指していくことが、大きな課題の一つである。

○　委員会では、主要な国・地域との二国間の協力関係を構築するとともに国際機関等を通じた多国間の協力を平行して進めてきた。ＥＵ（英国を含む。）とは個人情報保護法第24条に基づく国の指定とＧＤＰＲに基づく十分性認定を同時に行う、いわゆる相互認証を、米国とはＡＰＥＣのＣＢＰＲを推進している（Ｐ26参照）ほか、平成27年改正法の施行によって正式メンバーとして承認されたデータ保護プライバシー・コミッショナー国際会議等に積極的に参画してきた。

○　特に、個人情報保護法では、平成27年改正法において、域外適用の規定の実効性を担保するために外国執行当局への情報提供の規定が置かれたが、これに関連して、国際的な執行協力の枠組みであるＧＰＥＮに正式メンバーとして参加するなど、外国の執行当局との連携を強化してきている。

（３）域外適用の状況

○　個人情報保護法に基づく域外適用に関する執行状況として、平成29年度は、漏えい報告10件、指導助言４件、平成30年度は、漏えい報告20件、指導助言15件となっている。

○　国外にある者であって漏えい等報告を提出した者の多くは、インターネットを介して日本でサービスを提供している事業者であり、特に観光業関連（航空、ホテル、鉄道等予約）からの報告が全体の約27%（30件中８件）となっている。

○　また、漏えい等報告を提出した者の多くがインターネットを介して事業を行っていることから、不正アクセスによる被害が60%（30件中18件）であり、その他の漏えい等の発生原因としては、メール等の誤送付、紛失等となっている。なお、国内事業者による漏えい等事案における不正アクセスの割合は約14%（平成30年度）となっている状況と比べると、海外事業者の漏えい事案は、不正アクセスによる被害割合が相対的に多くなっている。

○　漏えい等報告を提出した者（計28件）の所在国は、米国が50%超で、このほか、ヨーロッパ地域と、アジア・オセアニア地域の国が約25%程度である。

○　国外にある者への個人情報保護法に基づく指導は、漏えい等事案における被害の拡大防止、影響を受ける可能性のある本人への連絡等、適切かつ迅速な対応を求めるなどの安全管理措置関連のほか、顧客への利用目的の分かりやすい説明の要求等となっている。

○　事例としては、ソーシャルプラグインが設置された一部のウェブサイトでは、閲覧しただけでユーザーがアクセスしているサイト等の情報がソーシャルネットワーキングサービス事業者に送信されることがあることについて、委員会ウェブサイトで注意喚起を行い、当該事業者に対し、個人情報を取得することがあることをより明確にユーザーに周知することなどを指導した事案や、国外に所在する事業者の漏えい等により、当該事業者のサービスを利用していた国内事業者の顧客の個人情報が漏えいした事案について、当該外国の事業者に対し任意の協力として国内事業者のリストの提出を求め、国内事業者に漏えい等報告の提出を促した事案があった（詳細はＰ44参照）。

○　また、海外の個人情報保護当局に対し、委員会の対応状況について情報提供を行うとともに漏えい等事案の発生原因や再発防止策について情報の共有を求めるなど、海外の個人情報保護当局との執行協力を行った事例があった。

（４）データ越境移転の現状

○　データ全般についてみると、情報通信技術の進展に伴い、世界的にデータ流通が急速に伸長している状況にある。特に、ネットワークの状況から見れば、国境を越えたデータ移転が一般化している状況にある。例えば、世界のデータ流通量（ＩＰトラフィック）は、2017年の1,217億ギガバイト（122エクサバイト）から、2021年には278エクサバイト（2017年の2.3倍）まで増加するとの予測が存在している[23]。また、国境を越えて移動するデータの量も増えており、世界の越境データ流通量を測ると、2001年の毎秒1,608ギガビットから2016年にはその165倍の26.5万ギガビットまで増加しているとの試算が存在する。

○　また、我が国を起点とした越境データの状況についてみると、国外ＩＳＰ

[23]　JETRO 地域・分析レポート 「急増する世界の「データ」流通量」
(https://www.jetro.go.jp/biz/areareports/2018/380fd5f0d9c4bb4d.html)

（インターネットサービスプロバイダ）等と交換されるトラヒック（帯域）についてみると、2004年から2016年までの間で、流入・流出ともに数十倍規模で増加している[24]。また、我が国を起点とした越境インターネット帯域幅の相手方となる国、地域のシェアを見ると、国別では米国が約４割で最多、地域別ではアジア地域が約６割で最多となっている[25]。

（５）個人情報の越境移転の現状

○　国際的なデータ移転が活発に行われている一方、委員会による企業を対象とするアンケート調査[26]によれば、個人情報については84%超が「越境移転はしていない」と回答している。また、越境移転をしている中では、海外拠点や関係会社との間で個人情報をやり取りするケースが多くなっている。

○　越境移転する個人情報の内容や相手国については、越境移転する個人情報の内容は、従業員の個人情報が76%超と最大であり、次いで、取引先の個人情報が43%超と大きく、消費者の個人情報は、対内（外国→日本）では19.0%、対外（日本→外国）では12.1%となっている。また、越境移転する相手国は、中国が最大であり、対内では71.5%、対外では67.7%。次いで、米国、ＥＵ等の順となっている。

○　越境移転に関する課題は、対内、対外とも「相手国の制度にあわせた取り扱いを行うのが負担である」との回答が多く、対内では48.0%（対内では最大）、対外では40.4%を占めている。また、対内では「相手国の制度を調べるのが負担である」との回答も41.0%と多くなっている。一方で、「課題はない」と回答した事業者も多く、対内では40.0%、対外では44.4%（対外では最大）を占めている。越境移転に関する課題への対応者としては、「個人情報担当社員」や「法務担当社員」により対応するケースが多くなっている。

２．諸外国の現状

○　域外適用については、今回調査した各国では、中国以外では法律上の規定が整備されているが、日本に比べ、ＥＵ等の方が、適用される対象範囲が広い。なお、域外適用される規定の執行を担保するための規定では、我が国の

---

[24] 平成29年情報通信白書。国外ISP（インターネットサービスプロバイダ）等と交換されるトラヒック（帯域）についてみると、2004年から2016年までの間で、in（国外から国内へ）は約50倍、out（国内から国外へ）は約25倍に増加している。

[25] 『ジェトロ世界貿易投資報告 2018 年版－デジタル化がつなぐ国際経済』オンデマンド版（日本貿易振興機構編）P40（https://www.jetro.go.jp/world/gtir/2018.html）

[26] 第91回個人情報保護委員会（平成31年3月４日）における資料1「個人情報保護を巡る国内外の動向（法の域外適用の在り方及び国際的制度調和への取組と越境移転の在り方関係）」から引用。データは「個人情報の保護に関する事業者の取組実態調査（平成29年度）報告書」（平成30年3月）の国内事業者向けアンケート結果によるもの。

ように執行協力によるものが多いが、ＥＵのＧＤＰＲでは、域外適用の円滑な遂行の観点から、代理人等の設置義務を置いている。

○　越境移転については、今回調査した各国では法律上の規定又は枠組みを整備しているが、規制対象やその手法、担保措置は様々である。

○　また、個人情報が越境移転される中、移転先国における制度の在り方が、個人情報保護を巡る新たな政策課題になってきている。データ保護関連法制については、多くの国々で、ＯＥＣＤプライバシー・ガイドラインに準拠する形で行われてきたが、近年、データ保護関連法制が、途上国を含め世界に広がる中で、一部の国において国家管理的規制が見られるようになっている。データの国内での保存等を義務付けるデータローカライゼーション、民間のデータに対するガバメントアクセス[27]に関する規定がその代表例であり、これらの規制に関しては議論のあるところである。

○　データローカライゼーションについては、①プライバシーの保護、②自国内の産業保護、③安全保障の確保、④法執行／犯罪捜査などを標ぼうして導入される例がある。こうしたデータローカライゼーションは、経済に深刻なマイナスの影響を及ぼすとの試算結果があるが、経済的な側面ばかりではなく、言論の自由や社会的流動性、政治運動や社会運動への市民参加を妨げる可能性も指摘されている。

○　広範なデータローカライゼーション規制の拡大は、国際的な電子商取引を拡大していく上での障壁となり、ひいては技術革新や経済成長を阻害することから、我が国政府としては、環太平洋パートナーシップ協定（ＴＰＰ）の電子商取引章や2016年のＧ７香川・高松情報通信大臣会合での共同宣言など、正当な公共政策上の理由を有さない同種の規制を抑止するための国際協力体制の構築を進めてきている。

３．検討の方向性

（１）基本的方向性

○　我が国は、ＥＵとの相互認証やＡＰＥＣのＣＢＰＲ等の取組を進め、グローバルな連携に努めてきた。今後、国際的なデータ流通がより増大していく中、国際的制度調和がより重要になってくるが、米欧双方の関係機関と良好な関係を築いてきた委員会が個人データの保護と円滑な流通に向けて国際的な議論をリードしていく必要がある。

[27] ガバメントアクセスについて、明確な定義はないが、民間事業者が保有する情報を捜査当局等の行政機関が取得することを指すことが多い。

○　個人情報に係る制度を巡る国際的な議論は、二国間、多国間ともに、ここ数年、活発化している状況にある。平成27年改正法では、個人情報保護法第６条に「国際機関その他の国際的な枠組みへの協力を通じて、各国政府と共同して国際的に整合のとれた個人情報に係る制度を構築するために必要な措置を講ずる」との規定が追加されたが、今後、当該規定の趣旨を踏まえつつ、昨今の国際的な議論の進展を受け、我が国がこうした議論をリードし国際的な制度調和への取組を進めるため、委員会の国際交渉体制の強化にも取り組んでいく必要がある。

（２）域外適用の在り方

○　いわゆる域外適用については、平成27年改正法によって、法の適用関係が明確化された。この結果、外国にある個人情報取扱事業者であっても、国内にある者に対して物品やサービスの提供を行い、当該サービス等の提供に関連し、国内にある者から取得した個人情報を外国において取り扱っている場合には、当該個人情報を我が国の個人情報保護法により保護できるものとなった。

○　ただし、平成27年改正法の立法時においては、日本の行政機関が、外国の事業者に対して、その外国の領土内で報告徴収・立入検査（第40条）や命令（第42条第２項、第３項）を行うことは、外国の主権との関係上困難であると考えられ、外国の事業者に対して、報告徴収・立入検査や命令については規定されなかった。

○　仮に、外国の事業者に本法の義務規定に違反する行為があると認められ、指導・助言又は勧告を行っても改善されない等、より強力な措置をとる必要がある場合には、委員会が、個人情報保護法に相当する外国の法令を執行する外国の当局に対して、その外国の法律に基づく執行の協力を求めて（第78条）、実効性を確保することとされた。

○　しかし、このような状況について、外国事業者とのイコールフッティングの確保の観点から問題であるとの指摘がある。もっとも、外国事業者について、捕捉されている限りでは、現時点で個人情報保護法上、指導・助言又は勧告を行っても改善されない状況というのは発生していない状況にある。

○　いずれにしても、域外適用については、現行法の域外適用の範囲や、執行手法について、各国主権との関係整理の視点も含めて、引き続き検討する必要がある。他の国内法の状況も勘案して検討する必要がある。

○　なお、域外適用との関係で、罰金等が科せられないことを踏まえ、課徴金制度の導入を求める意見や、国内取得個人情報の国内サーバー保存義務付けなどを求める意見等もあるが、ＷＴＯ協定や環太平洋パートナーシップ協定（ＴＰＰ）で示されている、国境を越えるサービスの提供に関する内国民待遇、最恵国待遇等の原則（いわゆる無差別原則）の考え方や、外国事業者に対する法執行の在り方という視点も踏まえて、検討を深める必要がある。

（３）越境移転の在り方

○　海外への業務委託の一般化やビジネスモデルの複雑化が進む中、個人データの越境移転に伴うリスクも変化しつつある。いわゆるデータローカライゼーションやガバメントアクセスに係る海外の立法例はその一例と考えられる。

○　個人情報の越境移転の機会が広がる中で、国や地域における制度の相違は、個人や、データを取り扱う事業者の予見可能性を不安定なものとし、個人の権利利益の保護の観点からの懸念も生じる。外国政府による過度なデータローカライゼーションは、前述のとおり、技術革新や経済成長にマイナスの影響をもたらすのみならず、個人の便益をも阻害し得るところであり、また、過度なガバメントアクセスは、個人の権利利益の保護の観点から看過しがたいリスクをもたらし、個人データのフリーフローを支える信頼を損なわせ得る。

○　このようなリスクをもたらし得る個人データの越境移転について、平成27年改正法で新たに規定された、外国にある第三者への提供の制限との関係で、どうとらえるべきか検討することが考えられる。しかし、グローバルなデータフリーフローは、デジタルエコノミー時代のイノベーションの前提でもあることから、リスクを精査し、事業者等の実態をよく踏まえた上で、どのような措置が考えられるか見極める必要がある。

（４）本人への情報提供の在り方

○　個人情報は、情報を提供する本人が予測可能な範囲で使われる、というのが基本であり、これは、データの複製や移転が非常に容易となったデジタル化社会においても守られるべき概念である。一方、ＳＮＳ、物・サービスのｅコマースが定着し、外国事業者が個人情報を直接取得し多様に利活用する事例が増大する中、個人にとって取扱いが分かりにくくなるリスクが存在する。

○　したがって、このようなリスクについて、個人が予見できるよう、事業者からの本人に対する情報提供の在り方について工夫することも考えられる。

第７節　その他の論点

○　これまでの委員会の審議の過程において、「個人情報保護委員会の第一期を終えるにあたって」等に直接掲げていない事項についても、意見が寄せられた論点が存在する。

○　官民を通じた個人情報の取扱いに関する論点も複数指摘されたところであり、具体的には、行政機関、独立行政法人、地方公共団体、民間事業者等の法律等の統合を求める意見や、委員会が行政機関や地方公共団体における個人情報の取扱いについても所管することを求める意見等があった。この論点に関する政府としての検討に際しては、委員会としても適切に対応していく必要がある。

参考

中間整理をまとめるに当たっては、以下の活動の中で、寄せられた意見も参考とさせていただいた。

１．個人情報保護法相談ダイヤルに寄せられた意見

平成29年５月30日から、委員会事務局内に設置されている窓口（※）において、個人情報の取扱いに関する質問、苦情、あっせんの申出等を受け付けており（１日平均約70件（平成30年度））、その中で寄せられた御意見を分析し参考としている（第93回委員会資料参照）。

※　改正個人情報保護法の全面施行（平成29年５月30日）に合わせ、従来設置していた「個人情報保護法質問ダイヤル」を改組したもの。

２．タウンミーティング

日常的に個人情報に接する消費者や自治会・企業関係者等の方々に、個人情報の保護やその取扱いに関して感じている悩み・疑問点等について意見交換していただき、個人情報保護に関する制度や運用等について理解を深めていただくとともに、制度に対する御意見をいただくため、全国７か所でタウンミーティングを開催した。

場所	開催日	参加者
大分県	平成30年 ６月11日	消費者２名、消費生活相談員１名、自治会１名、企業１名
滋賀県	平成30年 12月18日	消費者団体２名、消費生活相談員１名、自治会１名、企業１名
青森県	平成31年 １月22日	消費者１名、消費生活相談員１名、自治会１名、企業１名
島根県	平成31年 １月30日	ＰＴＡ１名、消費生活相談員１名、自治会１名、企業１名
愛知県	平成31年 ２月５日	消費者２名、消費生活相談員１名、自治会１名、企業１名
高知県	平成31年 ２月12日	消費者２名、自治会２名、企業２名
栃木県	平成31年 ２月22日	消費者１名、消費生活相談員１名、企業１名

３．経済界からのヒアリング

回次	開催日	団体名
第89回	平成31年２月19日	在日米国商工会議所
〃	〃	日本ＩＴ団体連盟
第92回	平成31年３月12日	電子情報技術産業協会
第96回	平成31年３月26日	日本商工会議所
〃	〃	全国商工会連合会
第97回	平成31年３月27日	日本経済団体連合会
第98回	平成31年３月29日	日本インタラクティブ広告協会
第99回	平成31年４月１日	新経済連盟

４．個人情報保護法シンポジウム

平成31年１月25日、法曹・企業活動・消費者相談・サイバーセキュリティ対策など、様々な立場から個人情報保護法に関わる有識者の方々を招き、「個人情報保護法シンポジウム～暮らしの中の個人情報のこれからを考える～」を開催。

本シンポジウムでは、個人情報を巡る最新動向の紹介や個人情報の保護・利活用の今後をテーマとして各分野の有識者によるパネルディスカッションを通じて意見をいただいた。

５．認定個人情報保護団体シンポジウム

平成31年３月６日、「認定個人情報保護団体シンポジウム～認定個人情報保護団体の意義と今後の可能性を考える～」を開催。

二部構成で実施したパネルディスカッションには、計８団体の代表者がパネリストとして参加し、制度に対する要望等を含めて意見をいただいた。（日本ＩＴ団体連盟以外は認定個人情報保護団体）