個人情報保護を巡る動向

（第 14 回 FMMC 研究会　2022 年 5 月 26 日実施）

個人情報保護委員会事務局次長　　三原　祥二

個人情報保護委員会や個人情報保護法の基本部分に触れながら、個人情報保護委員会で検討を行ってきた令和２年（2020 年）改正、制度を所管する総務省及び個人情報保護委員会の全面的な協力を得つつ、内閣官房情報通信技術（IT）総合戦略室が中心となり検討を行ってきた令和３年（2021 年）改正を中心に、個人情報保護法を概説します。また、国際的なデータ流通が盛んになる中で、個人情報保護あるいはプライバシーの観点から、個人情報保護委員会がどのような取組みを行っているのかについて報告させていただきます。

個人情報保護委員会と個人情報保護法

個人情報保護委員会は、個人情報保護法に基づき設置された合議制の独立機関であり、その使命は、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ため、個人情報（特定個人情報を含む。）の適正な取扱いの確保を図ることです。形態としては、公正取引委員会と同様３条委員会であり、独立性・政治的中立性が制度上担保されています。

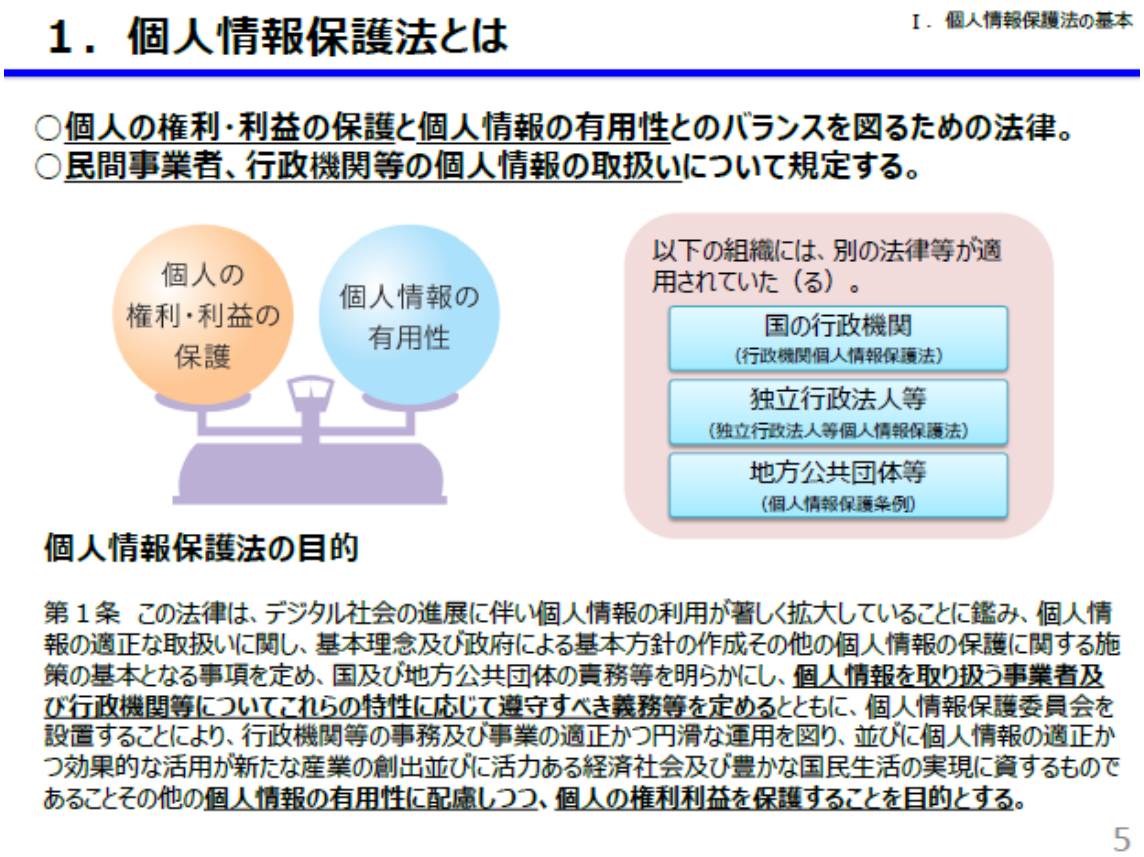
沿革としては、平成 26 年（2014 年）に、特定個人情報保護委員会が設立され、マイナンバーの取扱いを監視・監督する組織として始まっています。個人情報保護法の平成 27 年（2015 年）改正により、平成 28 年（2016 年）１月１日に特定個人情報保護委員会を改組する形で、個人情報保護委員会が設置され、現在は、マイナンバー法関連だけでなく個人情報保護法関連も監視・監督しています。

また、平成 27 年改正の前は、個人情報保護法においては、それぞれの監督については各省の大臣が行う、主務大臣制という仕組みでした。平成 27 年改正法により個人情報保護委員会が設置され、民間部門の監督権限等が主務大臣から個人情報保護委員会に一元化されました。そして、令和３年改正法の施行後は、官民の法制が個人情報保護法に一元化され、かつ監視・監督権限も個人情報保護委員会に一元化され、個人情報保護委員会が全ての分野において監視・監督を行う体制が確立しました。

個人情報保護法は、自治体が先行して個人情報保護条例を各地で成立させた後、平成 15 年（2003 年）に成立しました。その後、何度か大きな節目の改正があり、その主なものは平成 27 年改正、令和２年改正、令和３年改正の３つです。

冒頭触れたとおり、個人情報保護法は、個人の権利利益の保護と個人情報の有用性（利活用）とのバランスを図る法律です（図表１）。ただ、この保護と利活用は、決してトレードオフの関係ではなく、むしろ相互補完関係にある場面も多くあります。例えば、ルールにのっとることによってプライバシーリスクを最小化すること、あるいは個人情報の保護水準を上げることによって、むしろ利活用がしやすくなることも、身近な例として私どもも経験しています。

図表１



個人情報に該当するかの判断にあたっては、特定の個人を識別することができるものかどうかがポイントです。氏名それ自体や顔写真は該当し、例えば企業が保有しているデータの中で氏名などが含まれている場合には、その情報の塊そのものが個人情報として位置づけられます。

個人識別符号は、政令・規則で個別に定められます。DNA、顔、旅券番号、あるいは基礎年金番号などが個人識別符号として定義されています。

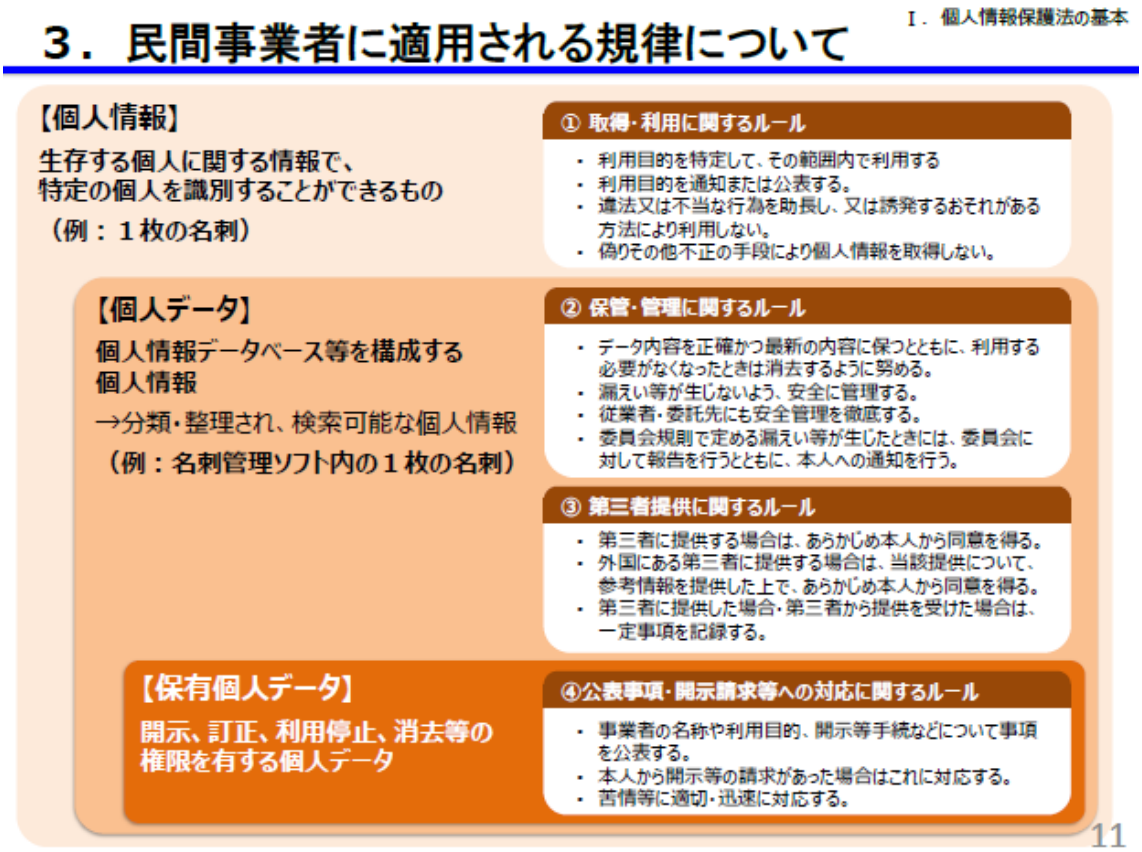
また、要配慮個人情報は、本人の人種、信条、社会的身分、病歴、犯罪の経歴などを基に本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして定められている個人情報です。要配慮個人情報は、取得の場合でも原則として本人の同意が必要になることが注意点となります。

個人情報取扱事業者については、法律上「個人情報データベース等を事業の用に供している者をいう」と定義されます。ここでいう「事業の用に供している」の「事業」とは、一定の目的をもって反復継続して遂行される同種の行為であって、かつ社会通念上事業と認められるものをいい、営利・非営利の別は問わないことがポイントです。個人情報保護法が、事業性を持っている事業者だけではなく、例えばPTAや、学校の名簿を対象とするゆえんといえます。

個人情報保護法における民間事業者に適用される規律

「民間事業者に適用される規律」（図表２）として、個人情報、個人データ、保有個人データ、それぞれの概念ごとに適用範囲は異なりますが、①取得・利用に関するルール、②保管・管理に関するルール、③第三者提供に関するルール、④公表事項等への対応に関するルールがあります。

図表２



「①取得・利用に関するルール」については、個人情報保護法上、原則として、取得の際の本人同意を必要としておらず、利用目的の通知または公表を求めているに留まります。例外として、要配慮個人情報は本人同意をあらかじめ取得することを原則としています。

一般的に個人情報を取得する場合には、個人情報の利用目的が重要な概念です。まず、個人情報の利用目的をできる限り特定した上で、原則としてあらかじめ公表することが求められます。このように、利用目的について縛りをかけていることが、日本の個人情報保護法の特徴の一つです。さらに、個人情報を取り扱うときには利用目的の範囲内で利用する必要があり、利用目的の範囲を超える場合には、再度本人の同意を取得することになります。また、法令に基づく場合や、人の生命・身体・財産の保護に必要かつ、本人の同意取得が困難な場合など、いくつかの類型については、利用目的による制限の例外として特定され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であっても、本人の同意は不要となります。

「②保管・管理に関するルール」については、個人データを保管・管理するときには、漏えい、滅失又は毀損の防止その他の安全管理措置を講じることが必要です。また、委員会規則で定める漏えい等が生じた場合には、個人情報保護委員会に対して報告を行うとともに、本人への通知を行うことが、令和２年改正で義務化されています。また、データ内容の正確性の確保として、個人データを保有している際に正確かつ最新の内容に保つことと、利用する必要がなくなったときには当該個人データを遅滞なく消去するように努めることが規定されています。

よく話題になる「③第三者提供に関するルール」については、個人データを第三者に提供するときは、原則本人の同意を得る必要があります。ただし、前述の「①取得・利用に関するルール」における利用目的の範囲を変更する場合と同様に、いくつかの類型については、例外として本人の同意を得る必要がないものもあります。また、平成 27 年改正では名簿業者が本人同意を得ずに名簿等を流通させていた実態が議論となりましたが、本人の同意を得る必要がない例外的な規定として、オプトアウト手続き（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場合であって、あらかじめ、次の項目（①個人データを第三者に提供する旨、②提供する個人データの項目、③提供方法、④本人の求めに応じて提供を停止する旨 、⑤本人の求めを受け付ける方法など）について、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）の規定があります。 さらに、委託、事業の承継、共同利用の３つの類型については、同意は必要ありませんが、それぞれ留意点がありますのでご注意ください。

外国にある第三者に個人データを提供する場合には、情報提供のルールが別途あります。通常の第三者提供のルールとは別に、外国にある第三者に提供することについての本人同意を取得することや、外国にある第三者が相当措置を講じるために必要な基準適合体制を整備しているか、例えば契約での確認、あるいは「APEC CBPR (Cross Border Privacy Rules（越境プライバシールール）)」システムなどで担保することが必要になります。加えて、日本が EU 等に対して EU 等の個人情報保護水準が十分な水準であるということを指定していますので、EU 等への提供は国内と同様の扱いになります。なお、逆に EU が日本を認定したものは、GDPR（General Data Protection Regulation（一般データ保護規則））の十分性認定と言われています。

また、事業者が守るべきルールには、本人による関与の観点からのルールもあります。まず、開示請求について、本人から事業者に対して保有個人データの開示を請求された場合には、原則本人に開示するという開示請求権が定められています。

最後に、個人情報保護法には、憲法上の表現の自由をはじめとする各種権利と、個人情報保護とのバランスの結果として、適用除外が設けられています。放送機関や新聞社、通信社その他の報道機関が報道の用に供する目的や、著述を業として行う者が著述の用に供する目的、宗教団体が宗教活動の用に供する目的、政治団体が政治活動の用に供する目的で、個人情報等を取り扱う場合は個人情報保護法の適用除外となります。令和３年改正との関連

で付け加えると、従来は、学術研究の用に供する目的も適用除外の一事由でしたが、令和３年改正で、学術研究については適用除外ではなく原則として通常の規律がかかるとし、その上で、それぞれの規律の中で必要な例外を定めるといった対応をしています。学術研究例外を除いた背景には、前述の EU の GDPR の十分性認定があります。2019 年１月に EU と日本との間で、相互に十分性を認定し、EU から日本を見た場合に、日本の個人情報保護法の規律がかかる部分については、その個人情報保護法の水準が十分であるという認定がなされていますが、個人情報保護法の適用除外については十分性認定の枠外でした。その結果、学術研究では、特にヨーロッパの研究機関などと共同研究を行っている日本の研究者が、国内扱いでのデータの流通ができないというきらいがありました。そこで令和３年改正により、十分性認定の範囲の中に、今後、学術研究も収める狙いも込めて、学術研究はその適用除外が外されたという経緯となります。十分性認定の枠組みの対象範囲の拡大の検討を始めたいと思っております。

個人情報委員会による執行事例

続きまして、近年の個人情報保護委員会の執行事案の例を、紹介します。

１つ目は、就活サイト上で、学生の同意を得ないで、いわゆる内定辞退率を算出するサービスが提供されていたものです。問題点としては、３点挙げられます。まず、Cookie の突合による第三者提供の同意の回避です。Cookie 単体では個人情報に該当しませんが、Cookie が提供された先で、結果的に何らかの情報と結び付いて個人情報になることが明らかであるにもかかわらず、提供する側では特定の個人を識別できないとして提供し、提供先の事業の中で個人情報になっていました。次に、第三者提供の同意を得ずに、内定辞退率を顧客企業へ提供していた問題です。また、プライバシーポリシーで、十分に利用目的が特定されていなかった点、かつ通知、公表がなされていなかった点も問題です。この事案につきましては、個人情報保護委員会として、指導や勧告を行いました。

２つ目は、破産者情報掲載サイトへの対応です。破産情報は、破産手続開始決定の公告として官報に掲載され、それ自体は公知の情報です。しかし、破産者の公告された個人情報を、データベース化して地図にプロットすることや、住所氏名を並べて公開することは、第三者提供の同意を得ておらず、公知情報であったとしても、自身の運用するウェブサイトに掲載することは違法といえます。このサイト事業者の連絡先などは当初不明でしたが、公示送達も使いながら、勧告や命令を行い、結果的にサイトは閉鎖されました。この問題は再発もあり得ますし、個人情報保護委員会に対していまだに類似の相談があるという状況です。そのため、今後とも必要な監督を行って参ります。

３つ目は、SNS のアプリを運営している会社に対する指導です。海外の委託先に対して、安全管理措置を十分に施していたか、あるいはその委託先の監督を適切に行っていたかということ、さらにはどのような情報が海外に送信されているのかを含めて、利用者への適切な説明がなされていたかが、問題になりました。法令違反は認められませんでしたが、安全

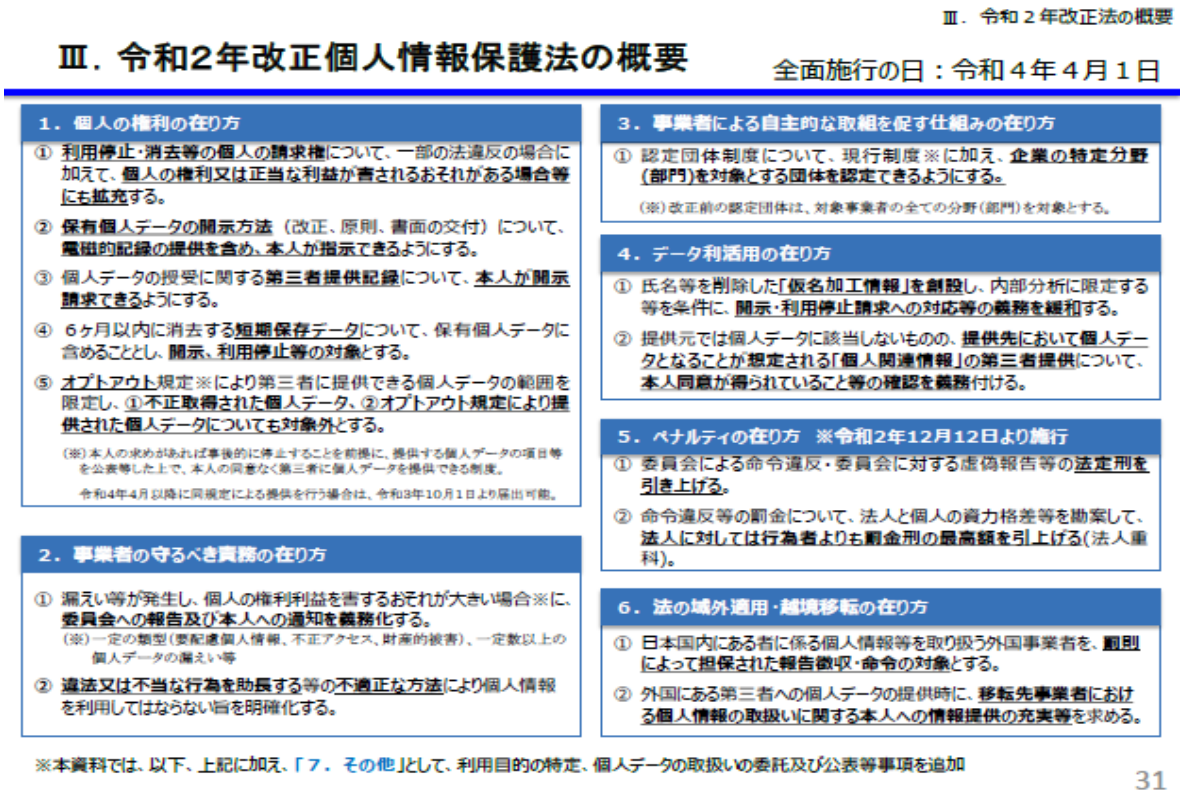
管理措置等に不十分な点があったため、指導を行った事案です。

令和２年改正と令和３年改正の概要

個人情報保護委員会では、令和２年改正の検討直前に５つの視点を設定しました。個人の権利に対して国民がより高い意識を持つようになっていた背景や、AI 等を含む革新的な技術が普及してきたこと、国境を越えるデータ流通に対し新たなリスクが出てきていたこと、AI・ビッグデータへの対応といった視点を基に、法改正の検討を行いました。

令和２年改正は、図表３にあるように、①個人の権利の在り方（利用停止・消去等の個人の請求要件の緩和等）、②事業者の守るべき責務の在り方（漏えい等の報告等の義務化、不適切な利用の禁止）、③事業者による自主的な取組を促す仕組みの在り方、④データ利活用の在り方（仮名加工情報の創設、提供先における個人データとなることが想定される情報の第三者提供の制限）、⑤ペナルティの在り方（法定刑の引き上げ等）、⑥法の域外適用・越境移転の在り方（法の域外適用の範囲の拡大、越境移転データ移転時の本人への情報提供の充実等の義務付け）が大きなテーマでした。

図表３



まず、「個人の権利の在り方」について、利用停止、消去等の個人の請求権を拡充しました。令和２年改正前は利用停止、あるいは消去等を個人として請求できる場合が限られており、一部の法違反の場合だけでした。令和２年改正では、改正前の場合に加え、利用する必要がなくなった場合、重大な漏えい等が発生した場合、本人の権利又は正当な利益が害され

るおそれがある場合には、利用停止、消去等の請求ができるようになりました。

また、保有個人データの開示方法は、従来、書面の交付による方法が原則となっていましたが、電磁的記録の提供を含め本人が指示できるように改正されました。

加えて、個人データの授受に関する第三者提供記録について、本人が開示請求できるようにする改正が行われました。改正前においてもトレーサビリティを確保するために、個人データを第三者提供する際には、その記録の作成と保存義務が義務付けられていましたが、当該記録が開示請求の対象かどうかについての明確な規定がなかったため、本人が開示請求できるようにしました。

さらに、デジタル化が進んだため、6か月以内に消去するデータであったとしても、保有個人データの一環として、開示、利用停止等の対象化しました。

そして、名簿を売買する事業者等がオプトアウト規定に基づいて提供したもの個人データを入手した場合、それを再びオプトアウト規定に基づいて提供することを禁止しました。

次に、「事業者の守るべき責務の在り方」について、漏えい等報告及び本人通知の義務化は、事業者に対して非常に大きな影響があったものと認識しております。改正前は、漏えい等が発生した場合、個人情報保護委員会へは任意報告であり、努力義務でしたが、今回の改正で義務化しました。その報告等の対象は、要配慮個人情報の漏えい等、財産的被害のおそれがある漏えい等、不正の目的によるおそれがある漏えい等、あるいは典型的な不正アクセスの場合には、件数が1件であっても、個人情報保護委員会への報告等の対象となります。また、1,000件を超える漏えい等については、上記の事例に当てはまらなくても報告や本人通知が義務化されました。

また、従来から、法律上、個人情報を適正に取得すべきという適正な取得という条項がありましたが、この適正取得に加え、取得後の利用についても適正に利用する必要があるとして、不適正な方法による利用の禁止を明確化しました。この点、事前のパブリックコメントや、コンサルテーションの中で、不適正な利用の範囲が広くなると事業活動を阻害してしまうという懸念をお寄せいただき、現状は、不適正な利用の典型的なケースとして、法令違反の行為や公序良俗に反している等社会通念上適正と認められない行為等、相当程度悪質なケースを想定しています。

「法の域外適用・越境移転の在り方」について、越境移転に関する情報提供に関しても改正を行いました。改正前は、外国にある第三者に個人データを提供できる場合は、本人同意を得るか、基準適合体制を整備した事業者であるか、あるいはEU、英国のように個人情報保護法の水準が同等であると認めた国や地域であるか、という3つの要件のいずれかを満たす必要がありました。今回の改正では個人データを外国に移転する場合には、さらに本人に対する情報提供を求めます。前述のとおり、個人データを外国に移転する際には、元々本人からの同意取得が原則必要ですが、さらに、同意取得時に本人に対して、移転先の所属国の名称や当該外国における個人情報の保護に関する制度などを予め情報提供することが必要となりました。この点、当該規定は、原則として事業者自身が外国制度等を調査すること

を想定しているものの、産業界からいただいた、事業者の過度な負担にならないように、事業者が参考にできる情報として、個人情報保護委員会において外国における個人情報の取扱いに関する法制度の概要を取りまとめて公表すべきとの意見も踏まえ、外国における個人情報の保護に関する制度について一定の情報を取りまとめて公表しました。これらも活用しながら、本人への情報提供の充実に努めていただきたいと思っております。

また、域外適用の強化については、改正前は指導・勧告までは海外の事業者に行うことができましたが、改正前の権限に加え、罰則に担保された報告徴収・命令を行うことができるようになりました。

「データの利活用の在り方」について、仮名加工情報の創設を行いました。従来から、匿名加工情報という制度はありましたが、使用状況が限定されていました。仮名加工情報という概念を新しく設け、仮名加工情報として加工をすれば内部分析に限定する等の条件はあるものの、利用目的の変更が本人の同意を得ることなく可能になる、漏えい等報告も除外になるなど、いくつかの義務を緩和しました。

また、執行事案の１つとして紹介しましたが、Cookie など、それ自体は個人情報に該当しないものの、提供先において個人データとなることが想定されているような情報の第三者提供につきましては、個人データと同様に本人同意を得ることが原則として必要になるよう制度改正を行いました。上記情報は、個人関連情報という新しい概念として設けられております。

「ペナルティの在り方」について、GDPR では、金額で言うと、場合によっては数十億円、あるいは全世界売り上げの４パーセント等、数百億円単位の課徴金を課される可能性がありました。そのため、日本国内での対応が議論となりましたが、課徴金については、産業界から反対の意見があり、またそもそも課徴金が不当利得を基準として算定している等、わが国の法体系の中での法制的な課題もありましたので、今後の検討としました。結果、通常の罰則ということで罰金刑含め、若干法定刑の引き上げを図りました。ここで注目するべき点として、法人重科として、１億円以下の罰金が新設されています。

以上が令和２年改正の法律上の改正事項のポイントです。ここからは、法律より下位で手当している箇所を、３点紹介します。

まず、「利用目的の特定の明確化」です。前述のとおり、個人情報保護法上、利用目的をできる限り特定することが大原則ですが、その一環として、いわゆるプロファイリングにも関連して、利用目的を特定する際に、本人が予測できる程度に利用目的を特定しておくことが必要であるということを、Q&A において明確化しました。次に、「公表事項の充実」です。元々事業者の名称、利用目的、開示請求等の手続き等は公表等する必要がありましたが、これらに加え、安全管理措置のために講じた措置も公表事項として追加することで、本人の関与のために事業者の透明性を高めていくことを図っております。最後は、「個人データ取扱いの委託」です。委託の解釈について、明確化を図りました。個人データの取扱いの委託において、委託先において、委託元から提供された個人データを、いわゆる「混ぜるな危険」

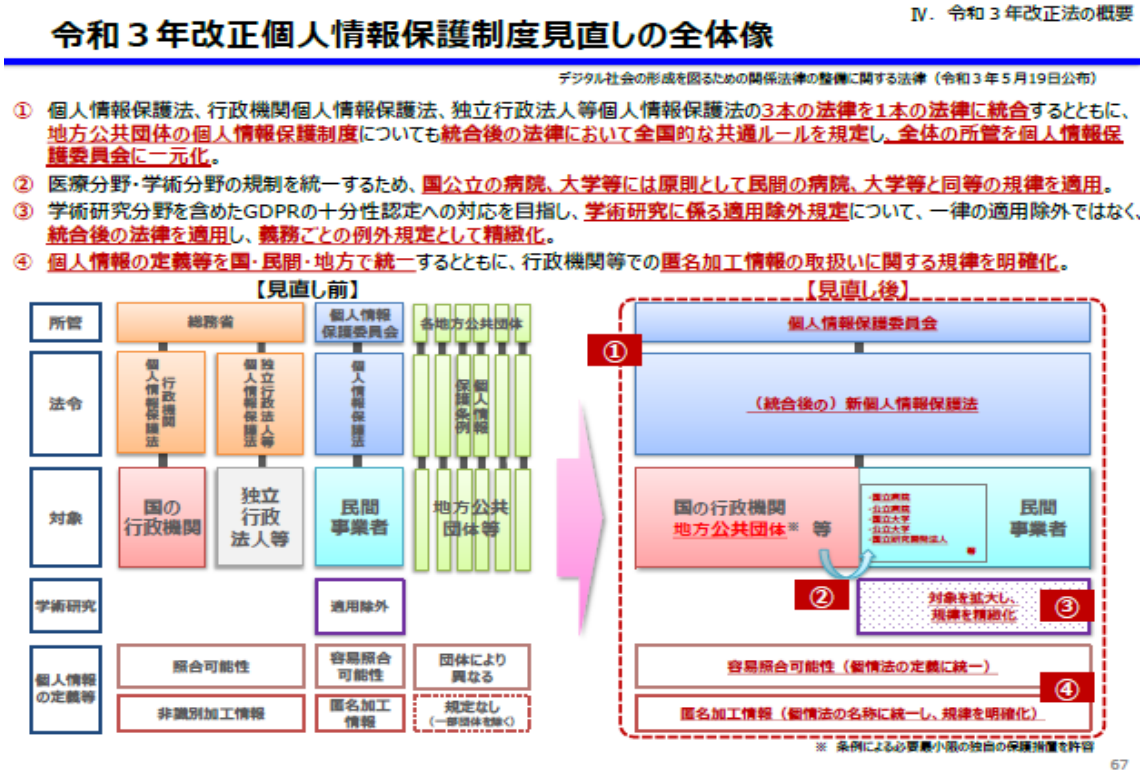
ということで、他の個人データ又は個人関連情報と突合することはできないという解釈を明確化しました。

続きまして、令和３年改正の概要について、簡潔に申し上げたいと思います。

改正法の目的は、特に国と地方で個人情報保護のルールの統一、一本化することによって、データ流通も図っていくことにあります。改正法の全体像を示した図表４の左側で示したように、従来は、民間部門に対して個人情報保護法の規律がかかり、その部分にのみ個人情報保護委員会が監督をしており、一方で国の行政機関や独立行政法人に対しては、行政機関個人情報保護法や独立行政法人個人情報保護法という規律がかかり、総務省の行政管理局が所管しておりました。また、自治体については、2,000 弱ある自治体が、それぞれ個人情報保護条例を制定して、その運用を図っており、ばらばらだったことが一つの課題でした。これらに対して見直しを行い、法改正後は個人情報保護法の中に従来の法令等を一本化、共通化、統合することと合わせて、その監視・監督体制についても、個人情報保護委員会に一元化しました。

令和４年４月に国の行政機関、独立行政法人等につきましては、この令和３年改正が施行されております。他方で、自治体については、条例の改廃もあり、令和５年４月に全面施行というスケジュールとなります。

図表４



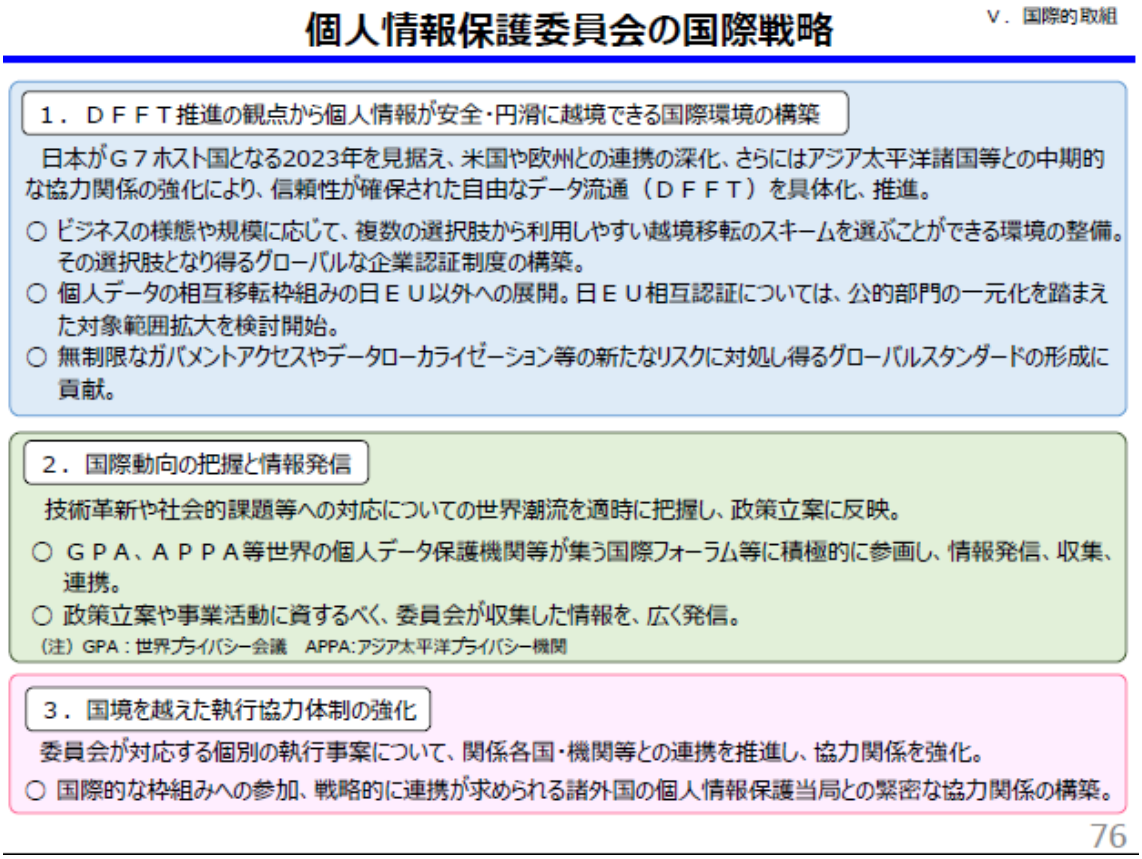
国際データ流通への取組

最後に、個人情報保護委員会が行っている国際的な取組について紹介します。

個人情報保護委員会では、国際戦略を定めています（個人情報保護委員会決定（令和４年３月 30 日））（図表５）。国際戦略には三つの柱があり、１つ目は DFFT（Data Free Flow with Trust（信頼性のある自由なデータ流通））の推進です。２つ目は国際動向の把握と情報発信です。具体的には、GPA（Global Privacy Assembly（世界プライバシー会議））や、APPA（Asia Pacific Privacy Authorities（アジア太平洋プライバシー執行機関））といったプライバシーに関する世界的なデータ保護機関同士の会議での情報の収集と発信の機会を活用しています。

３つ目は、国境を越えた執行協力体制の強化です。例えば、グローバルな企業に関する同一の事案については、日本だけではなく他国のデータ保護機関と連携して執行を行うような場面が想定されることから、協力関係を強化していこうとしています。

図表５



次に外国との個人データの越境移転に関する取組を紹介します。欧州と日本との間では、それぞれ EU からは GDPR に基づく十分性認定、日本からは個人情報保護法に基づく国指定を行っており、EU と日本の間で相互認証の枠組が発効しています。相互認証に係る EU との交渉は厳しい局面もありましたが、2019 年１月に相互認証が発効しました。発行から２年を経過して、現在、EU・日本相互の個人情報保護に係る制度の最新の状況について確

認等を行う相互レビューを実施しています。

また、DFFT 推進の一環として、日本、米国及び EU の３極の協力による信頼性のある国際的な個人データ流通の枠組みも模索しています。既存の枠組みとして、日本と EU との間には、既に相互認証があり、EU と米国の間でも、これまでセーフハーバーやプライバシーシールドといった枠組により、一定程度のデータ流通が行われていたことから、日本は、EU から日本へ移転された個人データを米国にも流通しやすくするような枠組みを提案し、日米欧の３極間での議論を継続しています。

グローバルな企業認証スキームの構築にも取り組んでいます。APEC には CBPR システムという越境移転ルールがありますが、この CBPR システムは、グローバル展開を志向することになっています。2022 年 4 月には、今後、APEC の枠を超えて、例えば、欧州の国や APEC 域外の国も参加できるような仕組みの構築を目指す、グローバル CBPR の設立を共同で宣言しました。前出の EU と日本の間の相互認証が国・地域の単位でなされているのに対し、CBPR システムは企業単位の認証により越境移転を可能にするものです。

加えて、OECD プライバシーガイドラインに関する取組も行っています。OECD プライバシーガイドラインは、1980 年に策定されたもので、世界各国のデータ保護機関がグローバルスタンダードとして参照しています。同ガイドラインには「OECD プライバシー８原則」が規定されており、これらは、今日に至るまで個人情報保護に適用可能な完成度の高い原則となっています。しかし、従来の OECD プライバシーガイドラインでカバーできなかった部分として、近年、特にこの 10 年ほどで顕著になってきた個人情報保護・プライバシーを取り巻く新しいリスク、としてデータローカライゼーションや無制限ガバメントアクセスといったリスクが取り上げられています。

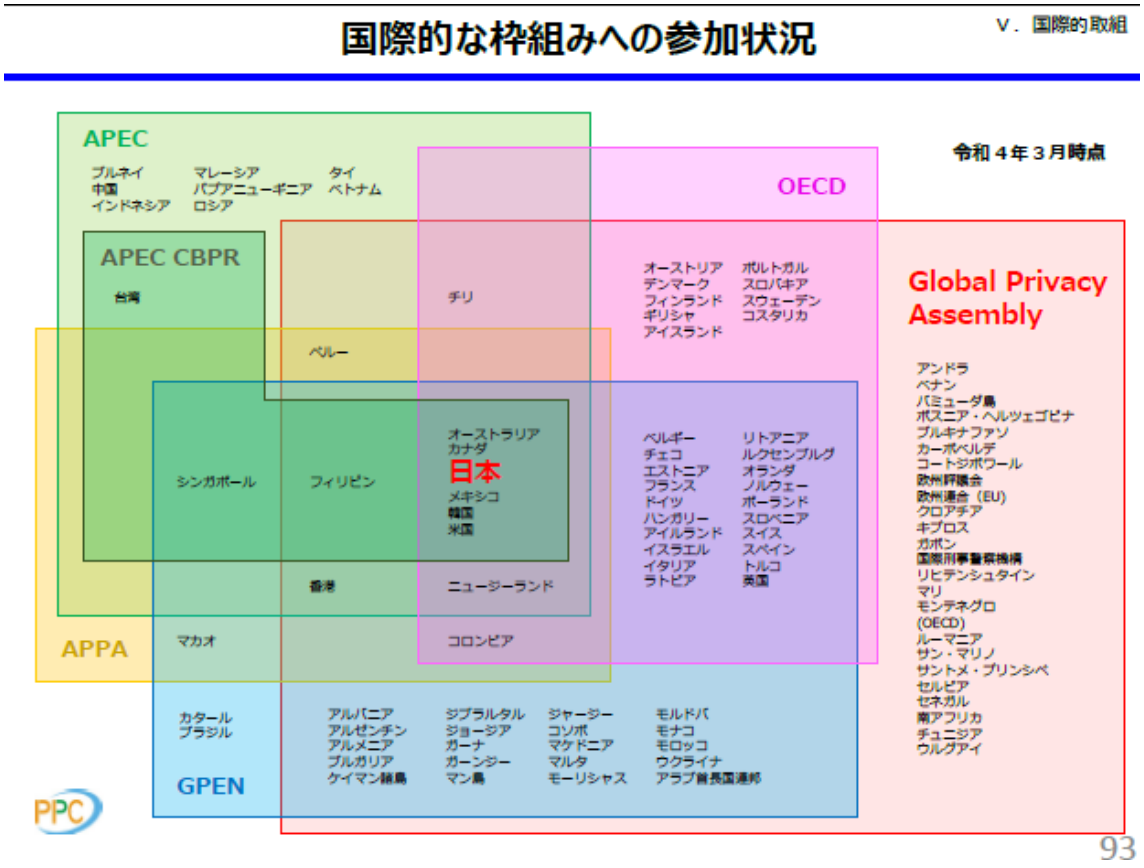
ガバメントアクセスとは、例えば、捜査当局が裁判所の令状を持って民間事業者が保有している個人データにアクセスすることがあります。このほか、日本では行われていませんが、事実上、強制力を伴うような形で、政府が民間事業者が保有する個人データへアクセスするような場合があり得、このような無制限なガバメントアクセスのリスクがあるという認識を OECD 加盟各国で共有してその対応のための議論を進めています。

具体的には、2020 年の 12 月に OECD の CDEP（Committee on Digital Economy Policy（デジタル経済政策委員会））で「民間セクターの保有する個人データへのガバメントアクセス」という宣言文を公表し、これに沿う形で、現在 OECD 加盟各国が参加するドラフティング・グループを形成し、ガバメントアクセスに関する新しい原則策定の作業を行っているところです。

DFFT の推進として、企業認証制度の構築、日米欧や OECD の枠組みでの議論等、様々な活動を行っています。更に、図表６で示すように、OECD をはじめとして、GPA、APEC、APPA や、執行協力の文脈では GPEN（Global Privacy Enforcement Network（グローバルプライバシー執行機関ネットワーク））等の枠国際的な組みにも共通して参加している状況です。

特に、2023 年には日本が G7 議長国となるため、DFFT に関して、G7 のデータ保護機関同士での横の連携を図っています。2021 年 9 月には各国のコミッショナー（日本は個人情報保護委員会の委員長）が参加して、G7 の各国のデータ保護機関との間で初のランドテーブルを開催しており、G7 の場でもデータ保護機関同士の協力を進めて行くことが合意されています。ガバメントアクセスや個人データの越境移転に関する執行協力には、日本としても重点を置いて取り組むため、2023 年に向けて準備を進めています。

図表 6



最後に、ご案内になります。個人情報保護委員会には、国民の皆さまから相談をいただくダイヤルがあり、年間で２万件ほどの相談をいただく中で、直接国民の皆さまからの声を聞いております。ビジネス向けには、２年間ほどの運用ですが、PPC（Personal Information Protection Commission（個人情報保護委員会））ビジネスサポートデスクということで、企業に対して個別に、必要があれば対面で、オンラインでも、個別相談を受け付けています。昨年は 50～-60 件のご相談をいただいており、そういった活動も行っておりますので、ぜひご活用いただければと思っております。