

個人情報保護法「三年ごとの検討」事項についての意見(2024年版)

慶應義塾大学 総合政策学部 教授 新保 史生

第1 個人情報保護委員会の体制強化

近年、AIをはじめとする新興技術の進展に伴い、個人情報の利用と保護を巡る環境は大きく変化している。この変化に対応し、個人情報保護制度を適切かつ効果的に運用するためには、個人情報保護法委員会（以下、「委員会」という。）の体制強化が不可欠であることから、そのための視点を幾つか提示する。

1 執行体制における課題

個人情報保護法の執行にあたっては、主として以下の三つの側面からの対応が求められる。

- ① 受動的対応：問い合わせや窓口への相談、公益通報等に基づく問題の把握
- ② 第三者通報：当事者以外からの通報による違反行為の発見
- ③ 能動的監視：委員会による自主的な監視活動

これらの対応において、即応性、適切性、網羅性や公平性及び公正性の観点から、さらなる改善が必要である。課徴金制度の導入を検討するにあたってはこれらの観点からの対応が重要であり、より効果的な監視・監督・執行体制の構築が求められる。

2 専門性の強化

上記の監視・監督・執行及びAIをはじめとする新興技術への対応のための一層の専門性の強化が必要である。内部における専門家の育成により、個人情報・プライバシー保護及び情報セキュリティに関する専門知識やAI技術をはじめとする新たな技術に関する専門的知見の確保が求められる。また、当該専門家の育成により、最新の技術開発状況の継続的な把握から新技術がもたらすプライバシーリスクの適切な評価などへの対応も可能になる。

3 外部連携の強化

個人情報保護法の社会的受容性確保のために、ステークホルダーとのコミュニケーション体制の整備が必要である。法改正における議論の過程において、産業界その他のステークホルダーとの間で見解の相違が生じることにより、本来求められている法改正の議論ができない状況に陥ることは結果的に誰の利益にもならない。特に、企業の競争力やイノベーション促進の観点と、個人の権利利益保護のために必要な制度の見直しを実施する際の検討において、適切な連携が図られバランスがとれた議論がなされないと、本来必要な議論の進展を妨げる一因となる。

この点につき、諸外国においては、いわゆる「プライバシー保護団体(Privacy Advocate)」との協力や日頃から議論を行うことで、

三年ごとに見直しのあり方そのものも含めて、法改正における議論の仕方を検討すべきであろう。なお、日本国内にPrivacy Advocateに該当する団体が存在しないことはこれまで指摘されてきたところであり、このような団体の醸成・支援も検討すべきである。

4 法執行の実効性向上

課徴金制度の導入をめぐる検討は、2019年の三年ごとに見直しの際から議論が継続されている検討事項である。この議論は今回の三年ごとに見直しで突如として提起されたもので

はなく、国際的な執行体制の強化の流れに沿った対応としても重要な検討事項でもあることを強調すべきである。

また、2019 年時点では有識者からも反対意見が多かったのは事実であるが、その後の個人情報の違法・不正な利用の状況をはじめ、著しく個人の権利利益を侵害する事例や図利加害目的にあたる事件も発生していること、ならびに、国外では制裁金が課されている事例であって日本国内でも同様の違法な個人情報の取扱いがなされている場合に、日本だけが課徴金の対象にはならない制裁金ヘイブンのような状況が続くことは、日本の個人情報保護法の法執行の実効性の観点からも望ましいとは言えない。

この点も含め、諸外国のデータ保護機関（DPA）との比較において、①執行権限の強化、②国際協力体制の整備、③越境データ移転への対応能力の向上が必要である。

委員会の体制強化と法執行の実効性向上は、デジタル社会から AI 時代へと変革期における個人の権利利益の保護と適正な個人情報の利活用の両立のために不可欠である。

第2 個人情報保護法のいわゆる3年ごと見直しの検討の充実に向けた視点（案）

「現行制度の基本的前提に係る再検討にあたっての視点の例」への意見

（意見がある部分のみ掲載）

- | |
|--|
| <p>1 個人情報取扱事業者による個人データの利用の適正性を本人の関与により規律しようとする仕組みの実効性</p> <p>① 個人情報取扱事業者が自ら利用目的を特定し、その範囲内で個人データを利用することを義務付け、通知・公表によりそれを本人が認識し、必要な関与・監視を行うとともに、本人との関わりの中で、事業者のデータの取扱い態様が必要に応じ是正され改善されるという、当事者間での自律的なガバナンスを重視する現行制度の考え方は、引き続き妥当か。利用目的の公表を通じた社会におけるモニタリングを通じて規律されることについてどう考えるべきか。</p> <p>② 法が期待する本人による関与・監視を行う前提として、利用目的や事業者におけるデータ処理の態様などについて認識・理解できることが必要であるが、デジタル化の進展や AI 等の新たな技術の急激な社会実装を背景に、本人が十分に理解できるような利用目的の特定、データ処理に関する説明の在り方について、どう考えるか（本人の合理的な関与を妨げ得るダークパターンをめぐる論点を含む。）。</p> |
|--|

【2019 年版 新保意見書の以下の部分を再掲】

1－2 個人情報保護委員会の権限の拡充

- ・ 法執行、制裁措置の実効性向上
- ・ 個人情報保護方針の法定（現状は、法第7条第1項の規定に基づく「個人情報の保護に関する基本方針」において、事業者が行う措置の対外的明確化として、「事業者が個人情報保護を推進する上での考え方や方針（いわゆる、プライバシーポリシー、プライバシーステートメント等）を策定・公表すること」が示されているのみ。）

個人情報取扱事業者による個人データの利用の適正性を公にする方法として、個人情報保護方針やプライバシーポリシー等の掲載が行われている。しかし、それらの公表はあくまで「自主的」な取り組みであって、個人情報取扱事業者の義務としての公表ではない。

「個人情報の保護に関する基本方針」第7条第1項において、「6 個人情報取扱事業者等が講ずべき個人情報の保護のための措置に関する基本的な事項」について「個人情報

取扱事業者等が取り扱う個人情報等に関する事項」として、「個人情報取扱事業者等は、法の規定に従うほか、上記２（２）①の民間部門ガイドライン及び認定個人情報保護団体の個人情報保護指針等に則し、例えば、プライバシーを含む個人の権利利益を一層保護する観点から、個人情報保護を推進する上での考え方や方針（いわゆる、プライバシーポリシー、プライバシーステートメント等）を対外的に明確化するなど、個人情報の保護及び適正かつ効果的な活用について自主的に取り組むことが期待されているところであり」との定めによる自主的な取り組みにとどまっている。

よって以下の二点についての検討が求められる。

① 個人情報取扱事業者の義務としての個人情報保護方針の公表

② 法定公表事項の明確化と整理

①の趣旨は上記の通りであり、②の趣旨は、現状では法定公表事項を個人情報取扱事業者が個人情報保護方針として自主的に公表する際に、個人情報保護法の条文において「公表」と記載されている条文を一つずつ確認し、それらをまとめて個人情報保護方針等に記載している。そのため、「利用目的の公表を通じた社会におけるモニタリングを通じて規律されることについて」十分にその目的を達成できていないだけでなく、本来公表が義務づけられている事項が公表されていないなど、モニタリングの対象となる法定公表事項の公表そのものが適正に行われていない側面がある。

さらに、個人情報保護方針等に記載されている事項と実際の個人情報の取扱いが異なる場合であっても法令違反とはならないため、いわゆる「コピペ個人情報保護方針」が無数に公表されており、事業者の個人情報の取扱いの実態を反映していないものも多い。

本意見の趣旨は、プライバシーポリシー等における表示事項と異なる個人情報の取り扱いが行われている場合には、「不公正又は欺瞞的取引」に該当するものとして法執行を行う対象としている米国の連邦取引委員会法第５条が定める手続同様の法執行を念頭に置いたものであるため、個人情報保護委員会の権限の強化とともに考えるべき論点である。

デジタル化の進展や AI 等の新たな技術の急激な社会実装に伴い、不知・不識のうちに取得し利用される個人情報の種類や量が増えていることから、法定公表事項として明示、通知又は公表すべき事項を整理し、事業者と本人双方にとって AI 時代における個人情報保護の取扱状況を個人情報保護方針等を通じて認識しやすい環境を整える必要がある。

なお、利用目的について個人情報の取扱いの実状に即していない場合や抽象的・形式的に公表している場合に、どこまで実際の利用目的と整合性があるのか確認することが困難な側面もあるため、表示義務違反に対する法執行については慎重な検討を要する。

④ 事業者が利用目的を特定した後、急速に進展する技術を新たに利用しようとした際に、「関連性を有する合理的に認められた範囲」における利用目的の変更として許容される範囲の精査が必要か。

利用目的の変更として許容される範囲については、これまでも以下のような観点からの問題がある。

① 利用目的への記載忘れに対応するための利用目的変更

② 関連性を有する合理的に認められた範囲として許容される利用目的の変更の範囲

③ 新たな技術の登場に伴う利用目的の変更

①利用目的への記載忘れに対応するための利用目的変更については、個人情報保護法が

制定された当初、「電話、ファックス、郵便において連絡します」と定めていた利用目的に、「電子メール」が記載されていないことが利用目的の特定違反に当たるかという議論がなされていた。いわゆる過剰反応の一つとして現在はそのような追記が利用目的違反にあたるとの議論は不要であろう。

②関連性を有する合理的に認められた範囲として許容される利用目的の変更の範囲については、過去の経済産業分野の個人情報保護ガイドラインにおいては、「3.2.2 利用目的の変更」として許容される事例として、「例えば、蕎麦店が出前の注文を受ける際に、年越し蕎麦の注文を受けることは、当初の利用目的である『出前の注文の受付』に関連性を有する合理的に認められる範囲と考えられます。」と記述されていた。

また、2015 年の法改正の際の国会審議における答弁では、「電力会社が、顧客に省エネを促す目的で、家庭内の機器ごとの電気使用状況を収集して、その使用量等を分析して顧客に提示をしていた場合、あるいは、同じ情報を用いて家電制御技術の研究開発とか、その顧客の安否確認のサービスを行うということができるようというふうなことが考えられる」との回答がなされていた。

いずれの例も、合理的に認められた範囲として許容される利用目的の変更の範囲としては説明が解りづらかったが、そもそも利用目的の変更として本人同意を得ずに変更が可能な範囲について、合理的な説明が必要ではないか。

なお、当該手続については利用目的変更をオプトアウトで認めるという案も過去の法改正においては議論がなされたが、今後もその議論はすべきではない。

また、合理性の判断が難しいがゆえに、明確な基準を示すことが逆に利用目的の抽象化につながるおそれがある点にも留意が必要である。

③新たな技術の登場に伴い追記された技術や手段等については、①の利用目的に記載していなかった事項を新たに追記することとも関係する。新たな技術が開発されるに伴い、例えば、監視カメラや各種センサーを設置し個人情報を取得するための利用目的を公表していた場合に、新たにロボットを介した個人情報の取得についてロボットが明記されていないことをもって利用目的違反とするかについては、当該ロボットによる個人情報の取扱いに応じて適宜判断されるべきものである。

新たな技術の出現に伴って、その技術を全て網羅的に示すことが利用目的の特定義務の趣旨ではなく、その情報がどのような目的で利用されるのかが利用目的の特定における本来の趣旨である。ゆえに、新たな技術の出現によって、利用目的の本質そのものが異なる場合には、合理的に認められた範囲の精査ではなく、目的外利用としての本人同意の対象とすべきである。

⑤ 個人データの利用目的や利用態様などからその取扱いの正当性を裏付ける基準を導入する等の実体的ルールを設けることにより、本人の関与による規律に依存せず、事業者自身による判断と事後の結果責任（本人の事後救済措置の強化等）により、適正な取扱いを担保するアプローチについて、どのように考えるか。

個人情報の取扱いにおいて、「公益性」や「正当性」についてこれまで議論の経緯が存在しないことと、GDPR（一般データ保護規則）が定める「正当な利益（Legitimate Interests）」に基づく個人データの処理を念頭に置いた議論は、日本の個人情報保護法と EU の制度の根本的な相違を認識していないため注意が必要である。GDPR が定める手続は

正当な利益に該当する場合に義務を解除することが本旨ではなく、データ主体の同意等を前提としつつデータ管理者の正当な利益とデータ主体の利益を比較衡量した上で、合理的に想定できる範囲内で必要最小限の個人データを必要な目的で利用するための手続である。

⑥ 高度なデータ分析を通じ、本人の権利利益に影響を与える活動が多様化・拡大する中で、プロファイリングなどデータ処理結果を使用して本人に働きかける事業活動であって、本人の権利利益に相当な影響を与え得るものについて、類型的な利用目的規制や本人の関与の強化を通じて、本人の権利利益の保護の実効性を高めることが必要か。

プロファイリングはこれまで幾度となく議論されてきた課題であり、山本龍彦教授の見書等に基づいて法改正の議論を具体化すべきである。

AI 特有のリスクへの対応としても、① AI による自動的な意思決定や個人情報の自動処理に伴い個人の権利利益に重大な影響を及ぼす場合、②個人データ処理の委託先やデータ処理事業者が使用するアルゴリズムの透明性確保措置とも関連した検討が必要である。

ただし、AI によるデータ処理においては透明性の確保が困難な場合が多く、説明可能な AI の実装に必要な事項についての検討が必要である。

⑦ 本人による関与・監視により事業者におけるデータの取扱いが改善されるためには、当該事業者が自律的に取扱いの適正化を図ろうとする意思があることが前提として必須であるが、もとより、改善の意思はなく、本人の権利利益に十分な配慮のない事業者については、本人の関与による規律には期待できず、異なる措置により、不適正な取扱いを抑止・停止することが必要か。

本人関与への対応ができていない場合として、個人情報保護法について十分な認識がないがゆえに、ある意味で本人関与対応リテラシーが十分ではないことに起因する問題と、法令違反行為を隠蔽するために意図的に開示等の請求に応じない場合では事情が異なる。

後者の事業者側による違法行為の発覚をおそれるがゆえの対応拒否については、個人情報保護委員会による執行体制強化により、①相談窓口等への相談に基づく対応、②当該事業者内部や第三者からの通報、③委員会によるモニタリング結果による対応、によって不適正・違法な本人関与によって個人の権利利益が侵害されている問題への対処が求められる。

3 個人データの第三者提供を原則として禁止する仕組みの妥当性

個人情報取扱事業者を本人の関与・監視することを通じた利用の適正性担保の仕組みを前提とすることから、本人の関与が著しく困難になる第三者提供を原則として禁止している。一方、その提供先における利用目的が特定の個人への影響を伴わない一般的・汎用的な分析に限定されるなど本人の関与を通じた規律によらない規律を導入することに合理性がある場合や、本人にとって、提供時の認識に照らし、当該第三者に対する提供を当然のものと思うなど躊躇するとは想定されない場合、さらには、利用目的の継承などを通じ、当該第三者への提供後も、提供前と同等に本人の権利利益の保護が図られる状態が保証される場合など、第三者提供を禁止する必要のない類型はあるか。

個人情報保護法が定める個人データの第三者提供の制限は、オプトアウトをはじめとして適用除外が明記されており第三者提供の原則禁止を回避できる手続きが定められている。

る。本人がデータ提供に伴う影響を合理的に予見可能であり、特段の不利益や懸念を感じない場合、本人の同意が不要な適用除外の追加を検討してもよいのではないか。

個人データの第三者提供を原則禁止とし本人同意要件を課している一方で、例えば学校行事において旅行代理店に企画を依頼する場合、学生・生徒の個人データの提供については本人同意が必要であるが、本人にとってはそのような場合に個人データが提供されることは当然想定されることである。第三者提供の同意要件以外にも、例えば、SNS 等においては本人が自らの要配慮個人情報も含めて公開しているにもかかわらず、当該情報を取得する場合には本人同意が必要である点も同様の問題である。

- 4 個人データの取扱い態様の多様化の下における、データの適正な取扱いに係る義務を負うべき者の在り方
- ① データ処理技術の進展により、クラウド技術を利用した高度なデータ処理サービスや AI の実用化などにより、本人から個人データを取得し本人に対し取扱いの責任を負う立場の個人情報取扱事業者が、その個人データに係るデータベースの構築やその処理のプロセスについて、実質的には第三者に依存するケースが拡大。
 - ② 現在は、本人に対し責任を負う個人情報取扱事業者が、従業員や委託先の監督を通じて、安全確保等の義務を果たすこととなっているが、データ処理の担い手や、安全管理等の措置を講ずる権能の帰属実態を踏まえこの規律の整理は妥当か。

個人情報保護法第 25 条は、個人情報取扱事業者が個人データの取扱いの全部又は一部を委託する場合の委託先の監督義務を定めている。一方、同法第 66 条は、行政機関等については保有個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報の安全管理のために必要かつ適切な措置を講じることが定めているにとどまり、委託先の監督義務は定められていない。

令和三年改正個人情報保護法により官民一元化が図られているため、行政機関等と個人情報取扱事業者では異なる義務となっている点についての見直しが必要である。

その上で、データ処理技術の進展により、クラウド技術を利用した高度なデータ処理サービスや AI の実用化などに伴う委託先の監督責任のあり方や安全管理等の措置を講ずる権能の帰属実態を踏まえた規律の整理を検討することが考えられる。

日本の個人情報保護法は、EU の GDPR（一般データ保護規則）とは異なり、管理者（Controller）と処理者（Processor）で義務を分けていないため、クラウドサービス提供者や AI ベンダーなど、実質的にデータ処理を行う第三者（処理者）に対する直接的な規律が EU の GDPR とは異なるのは当然のことである。

第 105 回 個人情報保護委員会(令和元年 5 月 17 日(金))に提出した意見書を再掲

個人情報保護法附則第12条に基づく「三年ごとの検討」事項についての意見

慶應義塾大学 総合政策学部 教授 新保 史生

【総論的事項】

1 個人情報保護制度のあり方

- ・ 官民双方におけるシームレスな個人情報の適正な取扱いと保護
- ・ 不公正・不公平感がない個人情報保護法執行
- ・ 個人の権利利益保護意識の高まりに対応する柔軟かつ的確な見直し
- ・ 日常的なデータの越境流通を前提とした国際的な個人情報保護への取り組みの促進

2 法改正の見直しのあり方

- ・ 施行後三年後ではなく「三年ごとの検討」としての見直しのあり方
- ・ A I の普及を前提とした個人情報の取扱環境の変化を見据えた制度変革

【各論的事項】

1 個人情報保護委員会の権限及び所掌事務について

1-1 個人情報保護委員会の執行権限の範囲を民間部門及び公的部門の双方とすること

- ・ O E C D プライバシーガイドラインその他の国際的な個人情報保護制度一般において、第三者機関の執行権限は官民双方を対象としている
- ・ 民間部門との不均衡が生じないように公平な執行体制を整備することが必要
- ・ 個人情報保護委員会は、番号法に基づく特定個人情報の取扱いに係る事務を掌るため、その執行権限は、行政機関、独立行政法人等、地方公共団体、地方独立行政法人及び個人情報取扱事業者その他の事業者を既に対象としている
- ・ 官民データ活用推進のため、匿名加工情報・非識別加工情報をはじめとする定義の統一化等も必要

1-2 個人情報保護委員会の権限の拡充

- ・ 法執行、制裁措置の実効性向上
- ・ 個人情報保護方針の法定（現状は、法第 7 条第 1 項の規定に基づく「個人情報の保護に関する基本方針」において、事業者が行う措置の対外的明確化として、「事業者が個人情報保護を推進する上での考え方や方針（いわゆる、プライバシーポリシー、プライバシーステートメント等）を策定・公表すること」が示されているのみ。）

1-3 個人情報保護法を根拠とする認証制度の創設

- ・ 個人情報保護委員会に認証部門を設置した公的制度としての運用
- ・ O E C D プライバシーガイドラインが定めるプライバシー・マネジメント・プログラム、教育、評価指標、プライバシー保護技術を向上するための措置への対応
- ・ G D P R に基づくシールプログラム（認証制度）との相互認証
- ・ プライバシー／データ保護影響評価の実施

2 国際的な対応について

2-1 法の域外適用

- ・ 前述の個人情報保護委員会の権限行使の拡充による法執行及び制裁措置の実効性向上を踏まえ、外国事業者による個人情報保護法違反への域外適用の実効性確保

2-2 越境データの保護と利用・国際標準

- ・ 越境データの保護と利用促進のための新たな制度的枠組みの提案と構築
 - ・ A P E CのC P E A（越境執行協力取決め）に該当する「O E C Dプライバシー保護法執行における越境協力に関する理事会勧告」（2007）に加え、A P E CのC B P R（越境プライバシールール）に該当する新たな「O E C Dガイドライン」の提案を行うことにより、越境データ流通の促進と越境執行協力体制・認証システムの構築を目指す
 - ・ 国際的な相互認証制度の構築（自主的な取り組みの国際的な展開：前述の個人情報保護法を根拠とする認証制度を活用）
- ・ IIS Q 15001 の国際展開に向けた方策を検討すること（国際標準としての提案（ISO 化））

3 個人情報取扱事業者の義務の見直し

3-1 個人の権利（請求権）のあり方

- ・ 手続違反による場合に限定しない請求権行使規定の整備
- ・ 開示等の対象となる保有個人データの期間（6ヶ月要件）撤廃
- ・ 個人データ・ポータビリティ確保のための実効ある方策の検討

3-2 漏えい報告の義務化の方向性

- ・ 報告義務対象となる漏えい事象の明確化
- ・ 本人に不利益が及ぶ場合の本人への通知義務の範囲
- ・ 漏えい報告懈怠に対する罰則の適用

令和元年5月に提出した意見についての令和2年及び3年改正による対応状況

1 個人情報保護委員会の権限及び所掌事務について

1-1 個人情報保護委員会の執行権限の範囲を民間部門及び公的部門の双方とすること → 令和3年改正により対応済

1-2 個人情報保護委員会の権限の拡充

→ 引き続き検討が必要な事項

1-3 個人情報保護法を根拠とする認証制度の創設

→ 「GDPRに基づくシールプログラム（認証制度）との相互認証」の実現に向けた取り組みを進めるべき

2 国際的な対応について

2-1 法の域外適用

→ 平成 27 年改正で設けられた域外適用に関する規定は令和 2 年改正でも対応済

2-2 越境データの保護と利用・国際標準

- ・ 越境データ流通の促進と越境執行協力体制・認証システムの構築を目指すべき
- ・ 国際的な相互認証制度の構築
- ・ JIS Q 15001 の国際展開に向けた方策を検討すること（国際標準としての提案（ISO 化））

→ 引き続き検討が必要

3 個人情報取扱事業者の義務の見直し

3-1 個人の権利（請求権）のあり方

- ・ 開示等の対象となる保有個人データの期間（6 ヶ月要件）撤廃
- ・ 手続違反による場合に限定しない請求権行使規定の整備

→ 令和 2 年改正により対応済

3-2 漏えい報告の義務化の方向性

- ・ 報告義務対象となる漏えい事象の明確化
- ・ 本人に不利益が及ぶ場合の本人への通知義務の範囲
- ・ 漏えい報告懈怠に対する罰則の適用

→ 令和 2 年改正により対応済