AI 時代のプライバシー保護

― 個人情報保護法がリスクベースに変わる機会を捉えて ―

コンサルティング事業本部　パートナー　小林　慎太郎

1　はじめに

個人情報保護法は、施行後３年ごとの見直しが法律で定められており、法改正の作業が鋭意進められている最中にある（2026 年２月執筆時点）。課徴金や団体訴訟制度の創設という規制強化の検討が先行したものの、途中で大きく方針転換し、データ利活用を推進するための規制緩和を前面に打ち出して、企業がリスクに応じて自主的に対処する、いわゆるリスクベースの制度へと変えていく方針が示された。目玉は、本人同意なく個人情報を取り扱うことのできる制度の創設で、AI 開発の促進はその筆頭だ。

本稿では、個人情報保護委員会が公表した「制度改正方針」[※1] をもとに、法改正の全体概要を紹介しつつ、本人同意なく個人情報を取り扱うことのできる制度を中心に、主要な改正内容について解説する。また課徴金をはじめとする法執行が強化される意義を説きつつ、企業経営者が、なぜ個人情報にまつわるデータガバナンスに取り組むことが急務なのかについて明らかにする。なお今後の情勢によって「制度改正方針」が見直される可能性はあり、本稿は現時点の参考情報として参照されたい。

2　利活用を前面に打ち出した異例の改正テーマ構成

「制度改正方針」では「第１適正なデータ利活用の推進 」「第２リスクに適切に対応した規律」「第３不適正利用等防止」「第４規律遵守の実効性確保のための規律」の四つに分類して 12 の具体的なテーマを示した。個人情報保護法は、文字通り、個人情報を保護するための法律であるが、データ利活用の促進を前面に打ち出した異例ともいえる構成となっている（図表 1）。

「制度改正方針」では、本人の同意なく個人情報を取り扱うことのできる場合について「1）第三者提供及び公開されている要配慮個人情報の取得について、統計情報等の作成」および「2）目的外利用、要配慮個人情報取得及び第三者提供に関する規制」を示し、さらに 2）の内訳として三つの類型を示した。

このうち、1）の対象については、統計作成等と整理できる「AI 開発等」を含むとされている。もともと統計作成には、断りなく個人情報を用いることが認められているのだが、目的外利用を抑止するための「法定の規律」の下で、AI 開発における個人情報の利用にもこの解釈を広げようということだ。実際に、AI のアルゴリズムには、統計と同様に、個人との関係性が取り除かれている場合も少なくない。

特に注目されるのは、自社に閉じた利用に限らず、第三者に個人情報を提供して統計作成・AI 開発に用いるケースだ。この場合、法定の規律に従えば、本人同意が不要になる。個人情報の第三者提供に関する同意取得の義務は重く、これまで個人情報の流通を妨げてきた要因だったのだが、それが統計作成・AI 開発においては軽減されるのである。

※１　個人情報保護委員会「個人情報保護法 いわゆる３年ごと見直しの制度改正方針」2026 年１月９日

図表 1　制度改正方針で示された個人情報保護法の改正テーマ

分類	テーマ	規制緩和	規制強化
第1 適正なデータ利活用の推進	1）第三者提供及び公開されている要配慮個人情報の取得について、統計情報等の作成	○	
	2）目的外利用、要配慮個人情報取得及び第三者提供に関する規制： a. 本人の意思に反しない場合 b. 生命等の保護・公衆衛生向上等の場合 c. 病院等による学術研究目的の場合	○	
第2 リスクに適切に対応した規律	3）子供の個人情報の保護		○
	4）身体的特徴に係るデータ（顔特徴データ等）		○
	5）委託先事業者の義務		○
	6）漏えい等発生時の本人通知等の緩和	○	○
第3 不適正利用等防止	7）特定の個人へ働きかけ可能な個人関連情報		○
	8）オプトアウト届出事業者		○
第4 規律遵守の実効性確保のための規律	9）勧告・命令等の強化		○
	10）違反行為中止のための措置等の要請可能化		○
	11）個人情報DB等の不正提供等の罰則強化等		○
	12）課徴金制度の創設		○

注）前年度まで改正テーマに含まれていた「漏えい等報告の合理化」「団体による差止請求制度・被害回復制度」は継続検討課題とされた
出所）個人情報保護委員会「個人情報保護法 いわゆる3年ごと見直しの制度改正方針」（2026 年 1 月 9 日）をもとに NRI 作成

また、同意取得義務のある要配慮個人情報の取得に際しても、法定の規律に従って統計作成・AI 開発に用いるのであれば、本人同意が不要とされる点も注目される。要配慮個人情報とは病歴や健康診断の結果などを指す。これまでウェブサイトをクローリング（自動プログラムによる情報収集）する場合、意図せず要配慮個人情報を取得してしまい、同意取得義務に違反するおそれがあったが、統計作成・AI 開発において解消されることにつながる。

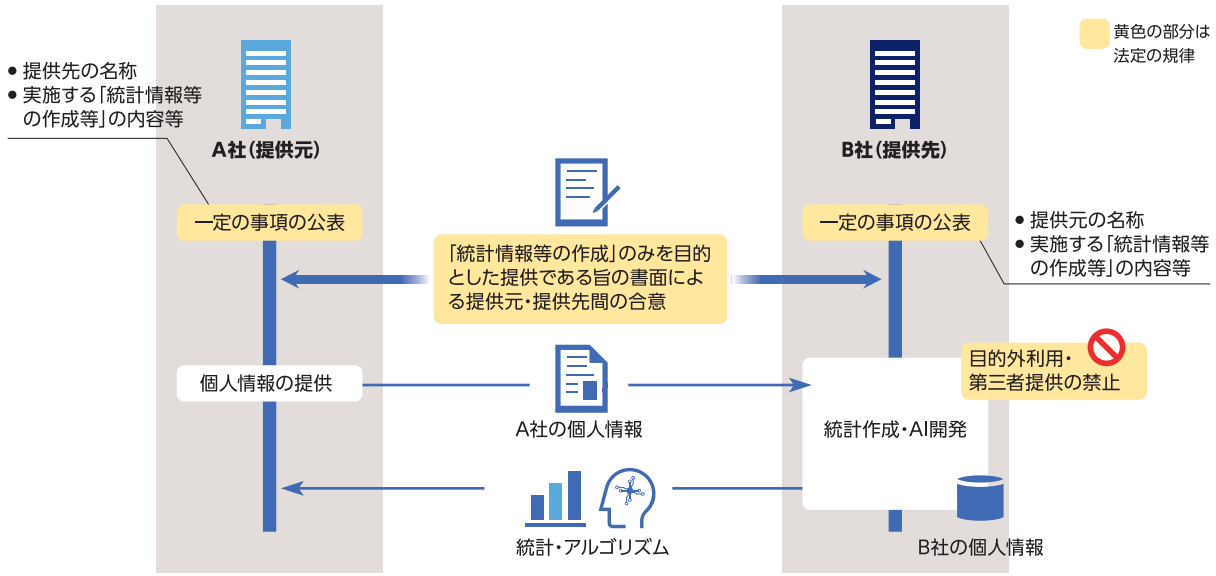
また「2)-a. 本人の意思に反しない場合」もビジネスへのメリットが大きい。オンラインショッピングやホテルの予約サイトなどでは、サービス提供者へ個人情報の第三者提供が生じるため、サイトの運営者は本人から同意を取得しなければならない。「制度改正方針」では、こうしたサービス利用に伴って生じる第三者提供について、取得の状況からみて本人の意思に反しない取扱いであるとして、本人の同意を不要とすることが示された。

3　統計作成・AI 開発のための条件は厳しくない

本人同意を免除する条件となる法定の規律とは、どのような内容であろうか。統計作成・AI 開発を理由にして、広く個人情報の利用を認めてしまうと、不適切な利用や第三者提供義務違反を誘発することになりかねない。一方、規律が複雑で対応の難しいものであると、匿名加工情報がそうであったように、事業者から敬遠されて、制度の普及が停滞しかねない。このため、制度改正方針で示された規律は、透明性と目的外利用の制限にフォーカスした原則的な内容となっているようだ。

具体例として、他社に自社が保有する個人情報を提供する場合でみてみよう（図表 2）。A 社の保有する顧客の個人情報を B 社に提供し、B 社は受け取った A 社の個人情報と自社（B 社）で保有する個人情報を突き合わせて分析し、A 社の顧客の属性分布などの統計を作成して提供することを想定する。このとき、次の三つの規律への対応が求められるとされている。いずれも特別な知識や技能がなくとも、対応可能なものと考えられる。

図表 2　他社に自社が保有する個人情報を提供して統計作成・AI 開発する場合



出所）個人情報保護委員会事務局「個人情報保護法のいわゆる 3 年ごと見直しについて」（2026 年 1 月）をもとに NRI 作成

- ▼ AB 両社は、それぞれ提供元・提供先の名称、実施する統計作成等の内容等の一定の事項を公表する
- ▼ AB 両社で、統計作成等のみを目的とした提供である旨を記した書面による合意をする（契約書を取り交わす）
- ▼ B 社には、受け取った個人情報の目的外利用および第三者提供の禁止義務が生じる

このケースは、A 社の個人情報を、B 社が保有する AI アルゴリズムに学習させて、A 社の顧客用にチューニングして AI アルゴリズムを提供する場合にも適用できる。またデータクリーンルームをはじめ、複数の企業が保有する個人情報を共有・分析する場合など、さまざまな応用が考えられる。

傘下に複数事業を抱えている企業の場合など、本人同意なく統計作成や AI 開発を行えるようになり、商品開発やマーケティングへの活用が期待される。

4　役割増すデータガバナンス

「制度改正方針」で示された限りでは、法定の規律は、透明性と目的外利用の制限にかかわる原則的なものにとどまっており、一見すると対応のハードルは高くないように思える。ポリシーや規程などの文書を整えれば、すぐにでも保有する個人情報を使って AI 開発ができそうだ。しかしいくら社内規程で、個人情報の目的外利用や第三者提供を禁止していても、それをきちんと管理・運用することのできる体制、すなわちデータガバナンスが伴わなければ、違反行為を抑止することはできない。

前述のケースを例に考えてみよう。B 社は、A 社から提供された個人情報を、他の情報と明確に区別して取り扱うことのできる安全管理措置を組織的かつ技術的に講じておかなければならない。これを怠ってしまうと、意図せずにデータを目的外で利用してしまうリスクがある。また、契約で規定された統計作成・AI 開発を果たしたら、速やかに A 社から提供された個人情報を消去し、目的外利用や漏えいなどのリスクを取り除くことも欠かせない。

データを提供する側の A 社においてもデータガバナンスは必須となる。データ提供にあたって、B 社

のデータ管理体制をきちんと評価した上で、契約を締結する必要がある。さらには個人情報をそのまま渡すのではなく、目的達成に照らして過剰となる情報は削除したり仮名化したりして、データの最小化を図ることが望ましい。

またプライバシー強化技術（PETs：Privacy Enhancing Technologies）を活用して、リスクを低減することも有効であろう。とりわけ、データを暗号化したまま複数社のデータを個人ごとに突合して処理することのできる「秘密計算」や、分散環境で複数の参加者でモデルを共有しながら学習を行う「連合学習」といったPETsは「制度改正方針」で示されたケースとの親和性は高く、活用が期待される。

保有する個人情報を有効活用するために、データ活用基盤を導入する企業は増大しており、取得の経緯の異なるデータが、同じサーバーに格納されることは珍しくない。もちろんアクセス制御などによって分別管理されているのだが、担当者が異動したり、時間が経過したりすると、どうしても事故は起こりやすくなる。データ活用と保護を両立するためには、データガバナンスを確立することが不可欠である。

5　抑止力としての課徴金　－アメとムチでデータガバナンスを推進

データガバナンスの重要性を説いたが、多くの企業にとっては直接収益をもたらすものではなく、法定でもない限り、投資が後回しになりがちだ。このとき、並行して創設が進められている課徴金が大きな意味を持ってくる。

課徴金は、上限のある罰金とは異なり、違反行為を通じて得た利得の納付を違反者に命じることができ、それによって違反行為を抑止する効果がある。事前規制では日進月歩で進展するデジタル技術に対応できないため、欧米をはじめとする諸外国では、事後的に巨額の制裁金を科すことのできる制度の導入が進んでいる。

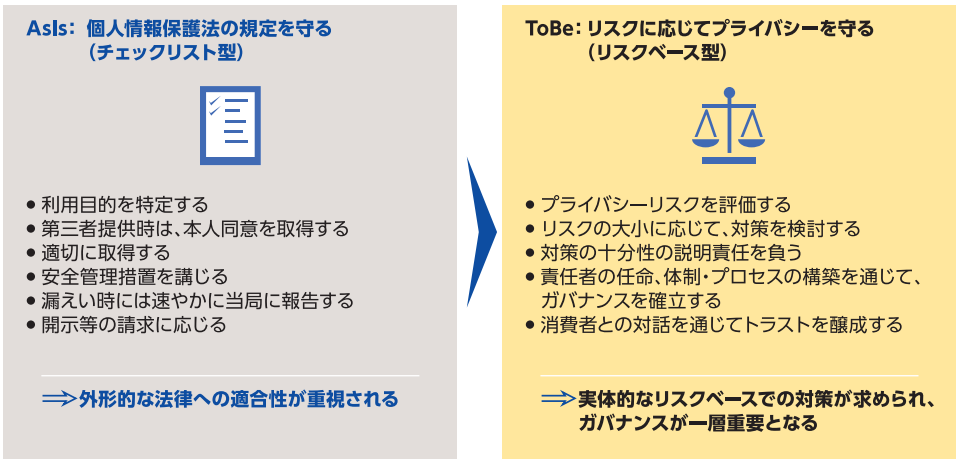
「制度改正方針」で示された課徴金の制度では、個人情報の不適正利用や不正取得、そして「1）第三者提供及び公開されている要配慮個人情報の取得について、統計情報等の作成」で生じる違反への適用が予定されている。適切にデータガバナンスに取り組んでいない事業者には、大きな制裁を機動的に科すことのできるよう、課徴金が抑止力として準備されているのである。

一方、行政府が課徴金納付を命じるかどうかの判断にあたっては、主観的要素（必要な対策を講じていたかどうか）が考慮されることとされている。すなわち適切にデータガバナンスに取り組んでいた場合には、課徴金が減額されるのである。これは、事業者がデータガバナンスに取り組むインセンティブとなりうる。課徴金制度は、データ活用に取り組む事業者を萎縮させるものとして導入に反対する向きもあるが、一方で事業者のデータガバナンスへの取り組みを促す仕組みも有しており、まさに行政府にとって、アメとムチの両面を備えた事業者を御すためのツールであることがわかる。

個人情報保護法はこれまで多くの事業者にとって、「利用目的を特定する」「第三者提供時は本人同意を取得する」といった個別の規定への適合性を確認するいわば「チェックリスト型」の法律で、外形的な法律への適合性が重視されてきた。それが本改正によって、規制緩和を通じて一定の裁量を事業者に与えつつ、課徴金などによって機動的に制裁を科すことのできる「リスクベース型」へと変貌しようとしている。事業者には「プライバシーリスクを評価する」「リスクの大小に応じて対策を検討する」といった実体的なリスクベースでの対策が求められ、データガバナンスが一層重要となる（図表3）。

個人情報保護法の次期改正によって、AI開発をはじめ、リスクに応じて柔軟にデータ活用を検討できるようになり、投資対効果の判断を、守りから攻めへと変えていくことができる。また、提携先や委託

図表３　チェックリスト型からリスクベース型へと制度が変わろうとしている



出所）NRI 作成

先の評価は、リスク対応への取り組みが重要な判断基準となっていくことが予想され、データガバナンスの成熟度が、競争優位の源泉となり得る。

　すなわち、次期改正の法益を享受するためには、事業者は自らデータガバナンスを確立しなければならないのである。

（監修：前原　孝章）

筆者

小林　慎太郎（こばやし　しんたろう）
株式会社 野村総合研究所
コンサルティング事業本部　パートナー
専門は、ICT 公共政策