子供の個人情報の保護

ICT・コンテンツ産業コンサルティング部　エキスパートコンサルタント　芦田　萌子

1　子供の個人情報の取扱いに関する法改正の動向の整理

個人情報保護委員会は、個人情報保護法のいわゆる「３年ごと見直し」のプロセスにおいて、デジタル社会の進展や国際的な規制動向を踏まえ、子供の個人情報の取扱いに関する規律強化を主要な検討事項として掲げている。

近年、デジタル化の急速な進展により、子供が自らの意思で端末を操作し、インターネットサービスを利用する機会が飛躍的に増大している。これに伴い、子供の個人情報が大量に収集・蓄積され、プロファイリングなどに利用されることで生じる権利利益の侵害リスクが高まっている現状がある。子供は「心身の発達過程にある」ため、その判断能力は未成熟であり、個人情報の不適切な取扱いに伴うリスクや影響を十分に予測・理解することが困難な場合が多い。このような子供という主体の特性に着目し、本人の関与や判断が期待しにくい部分を法的に補完する必要性が高まっている。

現行の個人情報保護法制において、子供の同意能力や保護者（法定代理人）の関与に関する規定は、主にガイドライン※1やQ&A※2における解釈指針に委ねられてきた。しかし、2026年1月に公表された「制度改正方針」※3においては、諸外国の規制動向との整合性や実効的な保護の観点から、従来は解釈指針に委ねられてきた子供の保護に係るルールを、法律上の明文規定へと昇華させる方針が明確に示された。これは、子供のプライバシー保護を事業者の「自主的な配慮」から「法的な義務」へと転換させる重要なパラダイムシフトである。

1）「個人情報保護」と「オンラインセーフティー」の峻別（しゅんべつ）

議論の前提として「個人情報保護」と「オンラインセーフティー」の概念を整理しておく必要がある。本改正が主眼とする「個人情報保護」は、個人情報の保護により、本人の権利利益を保護するものであり、適切な同意取得やデータ処理の適正化を手段とする。一方、「オンラインセーフティー」は、ネット上のいじめ、性的搾取、依存症などの体験・行動リスクから子供を守る概念である。

両者は「子供の保護」という目的で共通するが、アプローチは異なる。本改正は、あくまで情報保護の側面から子供の権利保護を強化するものである。

2）改正により導入される新たな規律

本改正方針において示された、子供の保護に関する主要な論点は以下の3点に集約される。

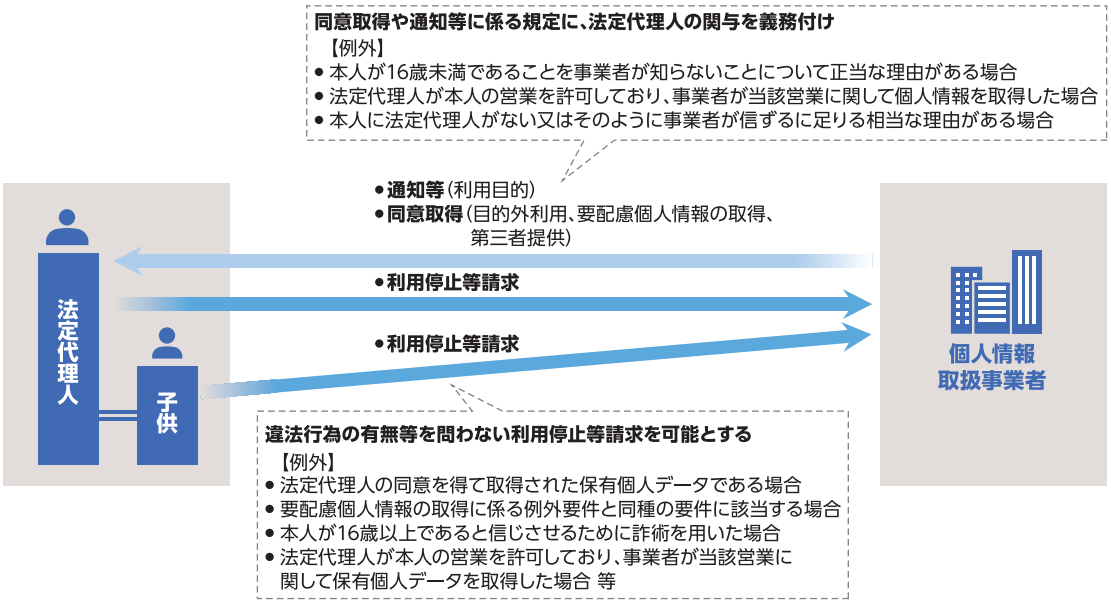
第一に、同意取得などに係る年齢基準の法定化である。これまで解釈上「12歳から15歳まで」と

※1　個人情報保護委員会「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）」を指す。「本人の同意」を得ることが求められている場面について、個人情報の取扱いに関して同意したことによって生ずる結果を未成年者が判断できる能力を有していないなどの場合は、親権者や法定代理人などから同意を得る必要があるとされている

※2　個人情報保護委員会「『個人情報の保護に関する法律についてのガイドライン』に関するQ&A」を指す。個別具体的に判断されるべきだが、一般的には、12歳から15歳までの年齢以下の子供の場合には法定代理人などから同意を得る必要があるとされている

※3　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　個人情報保護法の改正方針



出所）個人情報保護委員会「個人情報保護法　いわゆる3年ごと見直しについて」より NRI 作成

幅を持って示されていた同意能力の目安について、欧州「一般データ保護規則（GDPR）」などの国際水準を参照し「16 歳未満」という明確な基準を法律に規定する方針が示された。

第二に、法定代理人の関与の義務化である。16 歳未満の者が本人である場合、事業者が個人情報を取得・利用する際には、原則として法定代理人からの同意取得や、当該法定代理人への通知を行うことが義務付けられる。ただし、実務上の実行可能性を考慮し、事業者が「本人が 16 歳未満であることを知らないこと」について正当な理由がある場合などは例外とする規定も設けられる見込みである。また、手続き的な義務にとどまらず、事業者の責務として、子供の年齢や発達の程度に応じ「本人の最善の利益」を優先して考慮すべき旨の規定が新設される点も特筆すべきである。

第三に、事後的な救済手段の強化として、利用停止等請求権の要件緩和が検討されている。具体的には、過去に法定代理人の同意を得て取得されたデータや、適法に取得されたデータであっても、違法性の有無を問わず、本人の求めに応じて利用停止や消去を請求できる規定の導入が予定されている。

2　諸外国における子供のデータ保護規制との比較

1）GDPR と COPPA における保護理念の相違

日本が法改正にあたり参照している国際的なデータ保護規制には、主に欧州の GDPR と米国の「児童オンラインプライバシー保護法（COPPA）」が存在する。両者は「子供のデータを保護する」という目的においては共通しているものの、その根底にある法的理念やアプローチには明確な差異がある。

GDPR は、子供を独立した「権利の主体」として捉える人権アプローチを基盤としている。GDPR において子供は、自身のデータの取扱いに伴うリスクや結果を十分に認識できない可能性がある「脆弱（ぜいじゃく）な主体」と位置づけられる。したがって、法定代理人（親権者等）の役割は、あくまで判断能力が未成熟な子供を補完し、子供に代わって同意を与える「代理人」としての位置づけとなる。GDPR が透明性を重視し、子供自身に向けた平易な言葉での通知を強く求めるのは、子供の「知る権利」を保障するためである。

対して米国の COPPA は、親が子供のオンライン情報をコントロールする権限を与えるという、パターナリスティックなアプローチを採っている。

COPPA の主眼は、親の知らないところで子供から情報が収集されることを防ぐ点にあり「親が子供の権利を管理・制限する」という側面が強い。

日本の制度改正の方針は、親権者等の同意取得を義務付けるという形式面においては COPPA の手法に近い。しかし、事業者の責務として「子供の最善の利益」を考慮すべき旨を規定する点や、年齢に応じた自律を尊重する姿勢においては、GDPR や国連の「児童の権利に関する条約※4」の理念との親和性が高いといえる。

2） 規制の適用対象（スコープ）

各国の規制がどの範囲の「子供」および「事業者」を対象としているかを整理する。米国 COPPA は、適用対象を①子供向けのウェブサイト・サービス、または②一般向けであるが子供から個人情報を収集しているという「実際の認識（Actual Knowledge）」がある事業者に限定している。つまり、一般向けサービスであれば、子供が利用していると「知らなかった」場合は、原則として免責される構造にある。一方、英国の「Children’s Code（年齢適正デザインコード）」や GDPR の運用においては、より広範なアプローチが採られている。これらにおいては「子供向け」に特化したサービスだけでなく「子供がアクセスする可能性が高い」サービスも規制の対象となる。

日本の改正方針における例外規定（本人が 16 歳未満であることを事業者が知らないことについて正当な理由がある場合）が、米国の「実際の認識」基準に近いのか、あるいは欧州のような「客観的なアクセス可能性」を問うものになるのかどうかは、今後注視すべきポイントである。

また、保護の対象となる年齢（法定代理人等からの同意取得が必要となる年齢）の閾（いき）値は、国によって異なる。GDPR 第 8 条は、デジタル上の同意年齢を原則「16 歳未満」と設定しているが、加盟国法により「13 歳未満」にまで引き下げることが認められている。米国 COPPA は連邦法として「13 歳未満」を対象としている。

日本の改正案における「16 歳未満」という設定は、米国の連邦基準（13 歳）や韓国（14 歳）よりも広く、GDPR の原則基準と同等の高い保護水準を採用するものと評価できる。

3） 同意取得・年齢確認の実務的要件

法規制の実効性を左右する「同意の取得方法」と「年齢確認」についても、各国の要求水準には濃淡がある。

米国 COPPA は「検証可能な親の同意」を厳格に要求しており、連邦取引委員会（FTC）は、クレジットカード課金、身分証の提示、フリーダイヤルへの通話、ナレッジベース認証（親しか知り得ない質問への回答）など、具体的な確認手法を例示している。対して GDPR および英国は「利用可能な技術を考慮した合理的努力」を求めている。これは一律の厳格な確認を求めるものではなく、サービスのリスクレベルに応じたリスクベースを志向するものである。例えば、データ収集のリスクが低い場合は年齢の自己申告でも許容され得るが、高リスクなプロファイリングを行う場合は、公的身分証などによる厳格な年齢確認や AI を用いた年齢推定が求められる傾向にある。

日本の改正案においては、本人が 16 歳未満であることを事業者が知らないことについて「正当な理由」がある場合の例外規定が盛り込まれる見通しである。この「正当な理由」が認められるための確認措置として、GDPR のようなリスクに応じた柔軟な手法が許容されるのか、あるいはより厳格な確認が求められるのかについては、現時点では定まっておらず、今後注視する必要がある。

※4　18 歳未満を「児童」と定義し、国際人権規約において定められている権利を児童について敷衍（ふえん）し、児童の権利の尊重および確保の観点から必要となる詳細かつ具体的な事項を規定したもの

3　事業者が取り組むべき事項

法改正により、子供の個人情報保護に関するルールが法律上の義務として強化される方向にある中で、事業者は自社のデータガバナンス体制を再点検し、新たな規律への適用に向けた検討を進めていく必要があるだろう。本章では、実務対応の中核になると考えられる「適用対象の特定」「年齢確認の実装」「同意取得プロセスの設計」の 3 点について、先行する事業者の事例も交えながら、今後検討すべき事項を論じる。

1）適用対象となる製品・サービスの特定（棚卸しとリスク評価）

まず、どの製品・サービスが規制の適用対象となるかについては、現時点では「子供向け」の定義や「混合オーディエンス（一般向けだが子供も利用するサービス）」の扱いなど、具体的な基準が確定していない。

しかし、その上で、仮に規律上で対象範囲が包括的に示された場合や、グレーゾーンが残る場合であっても、事業者として説明責任を果たせるよう、以下の 2 段階のプロセスで検討を進めていく必要があると考えられる。

（1）自社サービスの棚卸し

最初に行うべきは、自社が提供しているすべての製品・サービスにおいて、どのようなユーザー層から、どのようなデータを収集しているかという実態の正確な把握（棚卸し）であろう。例えば、部門ごとに分散していたサービス台帳を統合し「生年月日情報の取得有無」などの項目を追加して、網羅的に整理することが考えられる。

（2）リスク評価の実施

棚卸しで抽出されたサービスについて、それが規制対象になり得るかどうか、また子供の権利利益にどのような影響を与え得るかという「リスク評価」を行うことが重要になると考えられる。具体的には、コンテンツの性質や実際の利用者層などの要素を総合的に考慮し、自社サービスが意図せず子供を引き付けていないかどうか、あるいは実態として子供が利用している状況にないかどうかを評価していくことになるだろう。

改正案では「本人が 16 歳未満であることを事業者が知らないことについて正当な理由がある場合」の例外規定が設けられる見通しである。もし自社サービスを「対象外」と判断する場合であっても、漫然と判断するのではなく、上記のような客観的なリスク評価を行った上で「子供向けではないと判断した根拠」を文書化しておくことが、将来的な「正当な理由」の主張において重要になってくると考えられる。

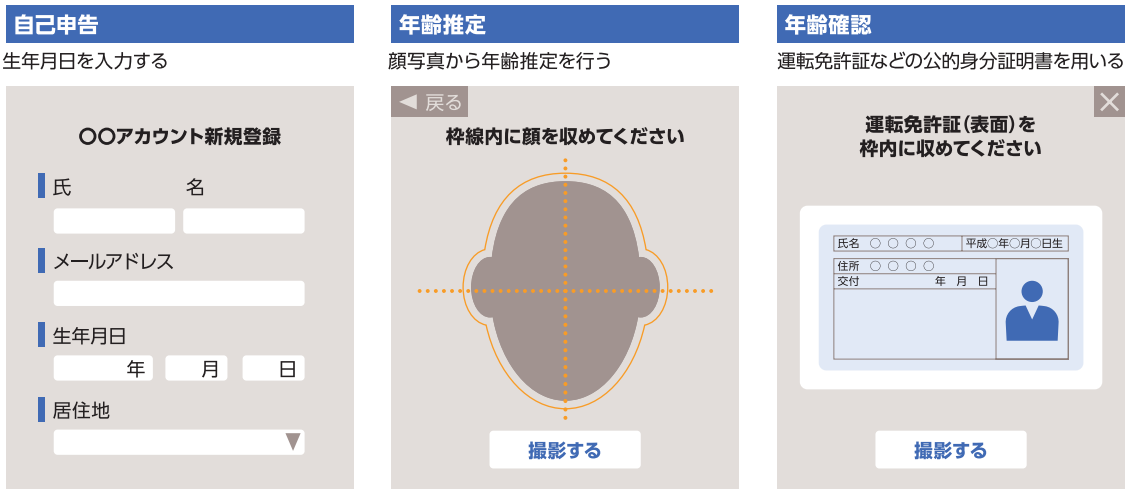
2）年齢適合性の確認の技術的実装

規制対象となる場合、ユーザーが「16 歳未満か否か」を判別する仕組みの導入検討が必要となる。しかし、あらゆるサービスに対して一律に厳格な本人確認を求めることは、ユーザビリティーを著しく低下させるだけでなく、本来不要な身分証データなどを収集することでの安全管理措置の観点からの負担増や、身分証を持たない子供をサービスから排除してしまう懸念もある。したがって、サービスが子供に与えうるリスクの高低を見極め、そのリスクに見合った確からしさを持つ手法を選択するというアプローチが求められることになるだろう。

（1）自己申告（Self-declaration）

生年月日や年齢の数値をユーザー自身に入力させる方法は、導入コストが低く、ユーザー体験への阻害要因も少ない。一方で、容易に年齢を偽れる（虚偽申告）というデメリットがある。そのため、子供の権利利益に対するリスクが比較的低いサービスや、まずは簡易なスクリーニングを行う初期段階の手法として検討されるべきものと考えられる。例え

図表 2　年齢適合性の確認アプローチ例



出所）NRI 作成

ば、あるゲーム会社では、アカウント登録時に生年月日を入力させる「自己申告」を基本としつつ、デフォルト値を設定しないなど、年齢入力画面をニュートラルなデザインにすることで、安易な年齢詐称を誘発しない工夫が行われている。

(2) 年齢推定（Age Estimation）

AI 技術などを用いて年齢層を推測する方法である。顔画像解析などが代表的であり、身分証を持たない子供の年齢を推定できる利点がある。一方で、顔画像という機微なデータの取得に対するプライバシー懸念や、AI の判定精度やバイアスに関する課題がある。自己申告では不十分だが、身分証提出までは求めにくい中程度以上のリスクがあるサービスにおいて、プライバシー保護措置を講じた上での導入が検討されるだろう。例えば、あるエンターテインメント事業者では、サードパーティー製の年齢推定技術を導入し、スマートフォンのカメラで撮影した顔画像から年齢を推定する仕組みを取り入れている。この際、プライバシー保護の観点から、撮影した画像データは年齢推定後即座に破棄し、サーバーに保存しない仕様とすることで、過度なデータ取得リスクを低減している。

(3) 年齢確認（Age Verification）

公的な身分証明書（運転免許証、パスポート、マイナンバーカードなど）や携帯キャリアの契約情報に基づいて年齢を確定する方法である。確実性は最も高いが、ユーザーの心理的抵抗感が強く離脱を招きやすい点や、事業者が高度な個人情報を保有・管理するリスクが生じるというデメリットがある。したがって、子供に対するリスクが極めて高いサービスや機能に限定して適用するのが現実的な判断となるだろう。

3) 親権者等からの同意取得プロセスの設計

16 歳未満のユーザーについては、法定代理人の同意取得が義務付けられる方向であるが、その確認手法については、取り扱うデータの性質や利用目的のリスク度合いに応じたリスクベースアプローチの検討が必要になると考えられる。

(1) リスクに応じた同意確認強度の使い分け

すべてのサービスにおいて、クレジットカード情報や公的身分証を用いた厳格な本人確認を求めることは、ユーザーへの過度な負担となるだけでなく、不要な個人情報を収集することにもなりかねない。そのため、リスクに応じた確認強度の使い分けが議

論の俎上（そじょう）に載るだろう。

① 高リスクなサービスの場合

位置情報の追跡、プロファイリング広告、第三者提供など、子供の権利利益に対するリスクが高い場合には、なりすましを排除できる比較的高度な確認が求められると考えられる。この場合、「ファミリーアカウント」などの親の身元が認証された基盤を活用することは選択肢のひとつとなるだろう。その他には、クレジットカードによる少額決済や、本人確認書類の確認など、コストと手間をかけてでも確実性を担保する手法の導入が考えられる。

② 低〜中リスクなサービスの場合

一方で、リスクが相対的に低いサービスにおいては、より簡易な手法も許容される可能性がある。例えば、子供に入力させた親のメールアドレス宛に同意確認メールを送り、そのリンクをクリックさせる「メール・プラス」の手法や、SMS 認証などが考えられる。これらは厳密な意味での本人確認（親であることの証明）としては弱いが、サービスのリスクとの均衡において「合理的な努力」として認められる余地があると判断される可能性はある。

(2) ユーザーインターフェース（UI）／ユーザーエクスペリエンス（UX）と透明性の確保

同意取得の実効性を高めるためには、システム的な認証だけでなく、子供自身が主体的に親へ相談できるような UI ／ UX の工夫も不可欠な要素となると考えられる。登録フローの中で唐突に「親のクレジットカード番号を入力せよ」といった画面が表示されるだけでは、子供が萎縮してサービス利用を諦めるか、あるいは隠れて親のカードを持ち出すといった不適切な行動に出るリスクも否定できない。子供に対して「なぜ親の同意が必要なのか」を平易な言葉で説明し「この画面をおうちの人に見せてね」と促すプロセスを挟むことは、子供が納得して親を巻き込む（相談する）きっかけをつくり、結果として親によって、ふさわしい確認と同意が行われる可能性を高めることにつながるだろう。

例えば、あるゲーム会社では、子供と推定されるユーザーの登録フローにおいて、まず子供向けの平易な言葉で同意の必要性を説明し、その上で親向けの詳しい説明画面を表示する二段構えの構成を採用している。これにより、親子間の対話を促し、実質的な同意取得をサポートしている。

(3) 同意のライフサイクル管理（撤回と更新）

同意取得時だけでなく、取得した同意を事後的にどのように管理するかについても、システム対応を含めた検討が必要になると考えられる。

まず、親権者が後から同意を撤回できる仕組みの整備である。一度同意したとしても、家庭の方針の変化などにより「やはりデータの利用を停止したい」と考えた際に、容易に同意を撤回（オプトアウト）できる手段を提供することは、信頼性確保の観点から重要となるだろう。初回の同意取得時だけでなく、利用目的を変更する際に、親権者から同意の取り直しをすることのできる仕組みや、個人情報保護法では義務として定められてはいないものの、BIOC[※5]の観点から、事後的に同意を撤回する仕組みが必要になると考えられる。

次に、子供の成長に伴う同意主体の切り替えである。サービス利用中に子供が 16 歳に達した場合、データ利用の同意権は親権者から本人へと移行する。そのため、年齢到達のタイミングをシステムで検知し、改めて本人（元子供）に対して自身のデータ利用に関する意思確認（再同意）を求めるプロセスを組み込むことも、長期的なコンプライアンス順守のために検討すべき論点となるだろう。

※5　BIOC (the Best Interests of the Child)：子どもの最善の利益

4　おわりに

個人情報保護法の改正による子供の保護強化は、国際的な潮流に即した不可避な流れであるが、運用にあたっては「保護」と「自律」のバランスが重要となる。子供の個人情報を保護しつつも、過度な制限によって子供のデジタル社会への参加や成長の機会を不必要に阻害してしまわないアプローチが求められるだろう。また、変化の速いデジタル技術に対応するためには、法律で骨格を定めつつ、具体的な確認手法などはガイドラインや自主規制で柔軟に補完する役割分担が不可欠である。事業者には、今回の法改正を単なるコンプライアンスコストと捉えず「子供の最善の利益」を考慮した製品設計（BIOC by Design）を通じてユーザーからの「信頼」を獲得し、競争優位性へと転化させる視座が期待される。規制当局、事業者、社会が対話を重ね、子供の権利保護と健全なデジタル社会の発展を両立させていくことが、今後の最大の課題である。

（監修：小林　慎太郎）

筆者

芦田　萌子（あしだ　もえこ）
株式会社 野村総合研究所
ICT・コンテンツ産業コンサルティング部
エキスパートコンサルタント
専門は、プライバシーガバナンスに関する制度設計、実装支援など
E-mail: m-ashida@nri.co.jp