# プライバシー強化技術（PETs）と個人情報保護法

～データ連携の制度的課題～

一般財団法人日本情報経済社会推進協会　電子情報利活用研究部
次長　　松下　尚史

## 1. はじめに

姉妹稿「パーソナルデータはなぜ「集めるほど価値が増す」のか」[1]で示したように、デジタル経済において、パーソナルデータは単体では価値が低く、複数事業者間での集合・連携によってはじめて競争力のある価値が生まれる。しかし連携を実現するためには、技術と制度の両面が揃う必要がある。

技術面では、生データを相手方に開示することなく複数事業者のデータを「計算上連携させる」手法――PETs（Privacy Enhancing Technologies：プライバシー強化技術）――がすでに存在する。秘密計算・差分プライバシー・連合学習などがその代表例であり、理論上は競合他社ともデータを連携させながら自社の情報を守ることを可能とする。

では、制度面の現状はどこまで整っており、何が次の課題として残っているのか。本稿はその問いに答えることを目的とする。なお本稿を、パーソナルデータの経済的特性を整理した姉妹稿「パーソナルデータの価値とは何か～経済学から見た性質・測定・分配～」[2]、および集合によって価値が生まれるメカニズムを論じた姉妹稿「パーソナルデータはなぜ「集めるほど価値が増す」のか」と合わせてお読みいただくと、より体系的な理解が得られる。

## 2. PETsとは何か――技術の概要と実務上の意義・留意点

### 2-1. 三つの主要技術

PETsとは、データを開示することなくその活用を可能にするための技術的手法の総称であり、個人情報保護にとどまらず、企業秘密・研究データなど開示に制約のある情報全般に適用される。自社の顧客データや営業情報を相手方に渡すことなく、互いのデータを秘匿したまま分析結果だけを共有できる技術群であり、生データの開示を伴わずに複数事業者間の連携を成立させる点に本質的な特徴がある。代表的なものとして以下の三類型がある。

第一は秘密計算である。複数の参加者がそれぞれのデータの中身を互いに開示することなく共同で計算を行い、計算結果のみを得る技術である。各参加者は他者のデータの内容を知ることができない。

[1] 「パーソナルデータはなぜ「集めるほど価値が増す」のか」

[2] 「パーソナルデータの価値とは何か～経済学から見た性質・測定・分配～」

第二は差分プライバシーである。データに統計的なノイズを付加することで、個人を特定できないようにしつつ、集団的な傾向を分析可能にする技術である。データを公開・共有する際のリスクを数理的に制御できる点が特徴である。

第三は連合学習である。生データを集約せず、各参加者の端末やサーバーでモデルを個別に訓練したうえで、学習パラメータ（モデルの重み）のみを共有する機械学習の手法である。データそのものを持ち寄ることなく、連携の恩恵を受けることができる。

## 2-2. 実務上の意義と留意点

データ連携プラットフォームに特有の課題として指摘される「ニワトリと卵問題（参加者が少ないから価値が低く、価値が低いから参加者が増えないという悪循環）」と、「競合他社とのデータ共有への心理的・法的障壁」という二つの構造的課題に対して、PETsは技術的な回答を提供しうる。生データの開示なしに連携が可能になれば、参加に伴うリスクが大きく低下することで、連携基盤への参入障壁が下がる。データビジネスにおけるPETsの意義は、単なる情報セキュリティ上の技術にとどまらず、複数事業者間のデータ連携を経済的に成立させるための基盤技術として理解すべきである。

ただし、PETsは万能の解決策ではない点も認識しておく必要がある。差分プライバシーでは保護水準を高めるほど分析精度が低下し、秘密計算では通常の計算と比べて処理時間が大幅に長くなるため、リアルタイム性が求められる用途への適用が難しいなど、いずれの手法もプライバシー保護とデータ活用の間のトレードオフを完全に解消するものではない。また、連合学習においても学習パラメータを通じた間接的な情報漏えいリスクが技術的に指摘されており、実務適用には用途・規模・精度要件に応じた適切な技術選択と専門的な実装能力が求められる。

# 3. 現行制度の到達点と残された課題

## 3-1. リスクベースドアプローチ——日本法における定着状況

リスクベースドアプローチとは、規制の内容を一律に定めるのではなく、リスクの発生確率と影響度に応じて求められる対応の水準を柔軟に設定するという考え方である。この発想は、日本の法体系においてすでに複数の分野で定着している。

情報セキュリティの分野では、NISCの「政府機関等のサイバーセキュリティ対策のための統一基準」が、特定の技術手段を一律に義務付けるのではなく、リスクアセスメントに基づいて対策の要否と水準を決定する構造を採っている。

化学物質管理の分野では、労働安全衛生法に基づく化学物質リスクアセスメントが2016年に義務化され、2023年の改正でさらに強化された。これはALARP（As Low As Reasonably Practicable：合理的に実践可能な限りリスクを低減する）の考え方に近く、「ゼロリスク」ではなく「合理的に低減された残余リスク」を許容する制度設計である。

金融分野では、金融庁の監督指針においても、画一的な技術要件ではなく、リスクに応じた管理水準の設定が求められている。

このように、リスクベースドアプローチは日本の法体系に馴染まない概念ではなく、むしろ複数の重要分野でその有効性が広く認められてきた考え方である。

## 3-2. 個人情報保護委員会によるリスクベースドアプローチの推進

個人情報保護の文脈においても、個人情報保護委員会はリスクベースドアプローチに基づく実務ツールをすでに公式に推奨している。その中心がデータマッピング・ツールキット（2022年10月公表）とPIA（Privacy Impact Assessment：プライバシー影響評価）である。

データマッピングは、元々組織が保有・処理するデータ全般のフローと所在を可視化する汎用的な手法である。個人情報保護委員会は個人情報保護法への対応に適用したツールキットを公表しており、事業者全体としてどのようなデータを取り扱っているのかを把握し、①個人情報保護法を含む当該データに適用される法令の遵守状況の確認、②当該データの取扱状況等に起因するリスクに応じた必要な対応の実施を行うことができるとされている[3]。

とりわけ重要なのは、このツールキットがリスク分析を出発点として設計されているという点である。事業の企画・設計段階でデータマッピング表に記入することで、予定している取り扱いが法令を遵守しているかを事前に検討・是正するとともに、洗い出されたリスクに応じた対応をとることができる[4]。

PIAはさらに明示的にリスクベースドアプローチを体現している。個人情報等の収集を伴う事業の開始や変更の際に、プライバシー等の個人の権利利益の侵害リスクを低減・回避するために、事前に影響を評価するリスク管理手法[5]として位置づけられており、「プライバシー・バイ・デザイン」の考え方を制度的に推進するものである。また、PIAは事業の新規実施時のみならず既存事業の見直しにも有効とされ、対応策実施後の影響度・発生可能性の再評価を含む反復的なリスク管理プロセスとして、組織のリスクマネジメント枠組みに組み込まれることが想定されている。

すなわち、個人情報保護委員会はデータガバナンスにおいてリスクベースドアプローチを積極的に推奨しており、「リスクを可視化し、リスクの大小に応じた対応を取る」という発想はすでに個人情報保護の実務に組み込まれつつある。

## 3-3. 個人情報保護法における残された課題

一方で、PETsという技術的手法の法的位置づけについては、制度的整備が十分でない状況にある。

現行の個人情報保護法ガイドライン（通則編）の解釈においては、暗号化・仮名化等の技術的処理を施しても、特定の個人を識別できる情報である限り個人情報該当性は変わらないとされている[6]。つまり、特定の個人を識別できる状態が残る限り、PETsを適用して生データを開示しない形でデータ連

---

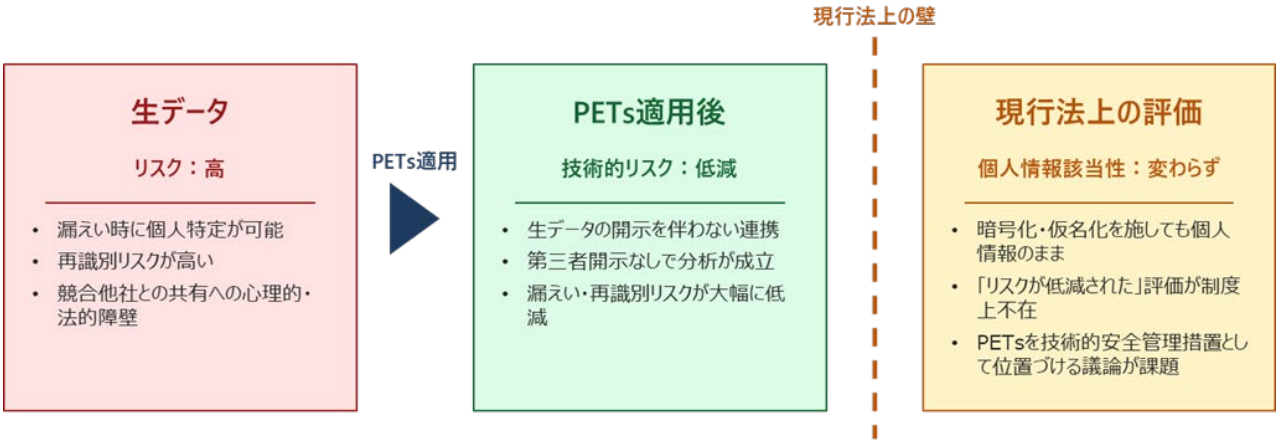
[3] 個人情報保護委員会「データマッピング・ツールキット（個人情報保護法関係）」（2022年10月13日公表）。他、別紙資料を含め、データガバナンス（民間の自主的取組）ページ内に掲載。

[4] 個人情報保護委員会「データマッピング・ツールキット（個人情報保護法関係）」pp.6-7（2022年10月）。

[5] 個人情報保護委員会「PIAの取組の促進について――PIAの意義と実施手順に沿った留意点」（2021年6月30日公表）。データガバナンス（民間の自主的取組）ページ内に掲載。
同文書はPIAを「事業の新規実施時のみならず、既存事業の見直しにも有効」（p.3）と位置づけ、対応策実施後のリスクマップの再評価・修正を含む反復的プロセスとして示している（p.17、図表10）。また、PIAの基となるJIS X 9251:2021は、PIAを「組織のより広範なリスクマネジメントの枠組みに組み込まれたもの」と定義している（同文書p.3 脚注2参照）。

[6] 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）」（令和6年4月最終改正）。同ガイドラインは、暗号化・仮名化等の技術的処理後も、特定の個人を識別できる状態にある情報については個人情報保護法上の個人情報に該当すると解釈している。秘密計算等のPETsについては、同ガイドラインに個別の言及はなく、技術的保護措置としての法的位置づけは現時点で明示されていない。

携を行った場合であっても、個人情報としての取り扱いが求められ、「技術的保護措置の適用によってリスクが低減された」という評価が制度上明確に位置づけられていない。




*技術的リスク低減と法的評価のギャップ —— PETsを「技術的安全管理措置」として位置づけることが論点*

**図表 1　PETs適用による技術的リスク低減と現行法上の評価のギャップ**

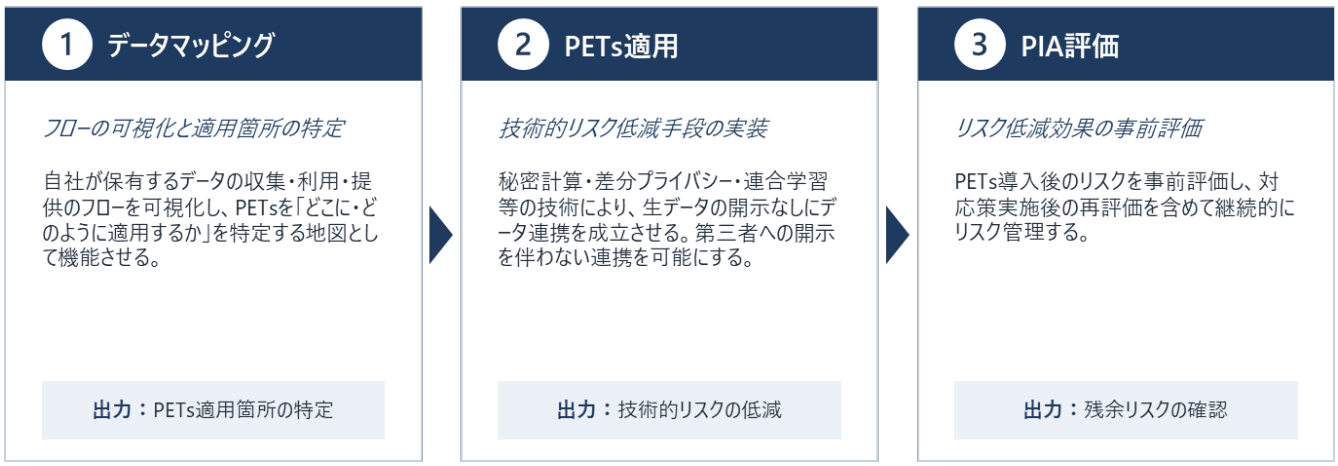
この点は、データマッピング・PIAとPETsの接合という観点から整理するとより明確になる。

データマッピングの本質は「自社が保有するデータの取扱フローを可視化する」ことである。フローが可視化されれば、「どこでどのようにデータが動いているか」が特定できる。PETsとの接合点はここにある。可視化された各フローに対して「ここにPETsを適用すれば、第三者へのデータ開示なしに連携が成立する」という技術的判断が下せるからである。すなわちデータマッピングは、PETsを「どこに・どのように適用するか」を特定するための地図として機能しうる。

その先にPIAが接続する。PETsの適用箇所がデータマッピングによって特定されれば、次のステップは「PETsを導入した場合にリスクがどの程度低減されるか」の事前評価であり、これはまさにPIAの目的と一致する。

整理すると、データマッピングが「フローの可視化と適用箇所の特定」、PETsが「技術的リスク低減手段の適用」、PIAが「その効果の事前評価」という三段階の連鎖として位置づけられる。

*データ把握 → 技術的リスク低減 → 影響評価という三段階を連動させることで、リスクベースドアプローチが実務として機能する*




**図表 2　データマッピング・PETs・PIAの三段階の連鎖**

前節で確認したとおり、個人情報保護委員会はデータマッピング・PIAを通じてリスクに応じた対応を推奨している。しかし、そのリスク評価の枠組みの中で、PETsの導入がリスク低減としてどう評価されるかについては、明示的なガイダンスはいまだ示されていない。この点は引き続き整備が求められる課題である。もっとも、個人情報保護委員会は2024年6月の中間整理においてPETsの位置づけを「引き続き検討する」論点として明示しており[7]、2025年3月公表の「制度的課題に対する考え方」ではPETsの活用が提供元の義務軽減につながりうる考え方も示されるなど、制度的整備に向けた議論はすでに始まっており、方向性は徐々に開かれつつある。

## 4. 欧米との比較——制度設計の参照点として

日本の今後の制度整備を検討するにあたり、欧米における制度設計の動向は有益な参照点となる。

EU（GDPR）においては、仮名化・匿名化・PETsの適用が、データ保護バイデザイン（Article 25）および安全管理措置（Article 32）の履行手段として明示的に位置づけられており、リスクの大小に応じた措置の選択においてPETsが有効な手段として制度上組み込まれている。技術的保護措置の適用がリスク評価に反映される設計となっており、事業者がPETsを活用するインセンティブが制度上担保されている[8]。

英国（ICO）は2023年にPETsに関するガイダンスを公表し、差分プライバシー・連合学習・秘密計算それぞれについて、個人情報保護の観点からの評価と実務上の活用指針を具体的に示している。事業者の実務判断に直結する形でPETsが制度的に位置づけられている点が特徴である[9]。

米国（NIST）においては、プライバシーフレームワーク（NIST Privacy Framework）においてPETsが技術的リスク低減手段として組み込まれており、連邦政府のデータ活用戦略においてもその位置づけが強化されつつある[10]。

---

[7] 個人情報保護委員会「個人情報保護法 いわゆる3年ごと見直しに係る検討の中間整理」（令和6年6月27日公表）第4章「その他」。PETs（プライバシー強化技術）の位置づけの整理は「ステークホルダーの意見やパブリック・コメント等の結果を踏まえ、引き続き検討する」と明記されている。同委員会は2025年3月5日に「個人情報保護法の制度的課題に対する考え方」を公表し、PETsを活用した場合の提供元の義務・負担軽減の可能性についても言及している。
なお、2026年4月7日には「個人情報の保護に関する法律等の一部を改正する法律案」が閣議決定されたが、同改正案はPETsを技術的安全管理措置として位置づけるものではない。ただし、改正案は統計作成等を目的とした第三者提供に係る本人同意を不要とする特例（第30条の2）を新設しており、複数事業者間のデータ連携を促進する制度整備の方向性自体は本稿の議論と整合的である。なおこれは同意取得負担の軽減によるアプローチであり、PETsをリスク低減手段として直接評価する仕組みではない。

[8] Regulation (EU) 2016/679（GDPR）, OJ L 119, 4 May 2016. Article 25（データ保護バイデザイン・バイデフォルト）は仮名化等の技術的措置を義務履行の手段として明示的に位置づけており、Article 32（安全管理措置）はリスクに応じた技術的・組織的措置の実施を求めている。PETsの適用はこれら両条のリスクベースドな履行において有効な手段として制度上組み込まれている。

[9] Information Commissioner's Office（ICO）, "Privacy-enhancing technologies (PETs)"（2023年6月19日公表）。差分プライバシー・連合学習・秘密計算等8種類のPETsについて、データ保護法上の評価と実務上の活用指針を示している。DPO向けのパートIと技術者向けのパートIIから構成される。

[10] National Institute of Standards and Technology（NIST）, "Privacy Framework Version 1.0"（2020年1月公表）。プライバシーリスクの特定・管理・対応のための自発的な枠組みであり、PETsを技術的リスク低減手段として組み込んで

これらに共通するのは、「PETsをリスクベースドアプローチの枠組みの中に明示的に位置づける」という方向性である。この方向性は、個人情報保護委員会がデータマッピング・PIAにおいてすでに採用している考え方と整合的であり、日本における次のステップを考えるうえで参考になる。

## 5. 議論すべき論点の整理

本稿の考察を踏まえ、今後の議論において論点となりうる事項を整理する。

第一に、データマッピング・PIAの枠組みとPETsの接合である。データの性質・目的に応じたPETsの選択基準と、データライフサイクルのどの段階でPETsを適用すべきかが既存の枠組みの中で明確になれば、PETsは特別な技術的取り組みではなく、通常のデータガバナンスの一部として位置づけられる。そのためには、第3章で整理したとおり、データマッピング・PETsの適用・PIAという三段階の連鎖を明示的なガイダンスとして示すことが、事業者の実務判断を大きく助けると考えられる。

第二に、PETsを「技術的安全管理措置」として位置づける可能性である。個人情報保護法第23条は『必要かつ適切な安全管理措置』を求めており、個人情報保護委員会のガイドライン（通則編）はその具体的な内容を『事業の規模及び性質、個人データの取扱状況等に起因するリスクに応じて』決定するものとしている。この安全管理措置は、会社法上の善管注意義務の観点からも経営者が履行責任を負う事項であり、データ管理上のリスクへの対応は経営判断として重くのしかかる。このリスクベースドアプローチはPETsの活用と整合的であるが、現行ガイドラインにはPETsを技術的安全管理措置の一形態として明示的に位置づける記述が存在しない。PETsの導入がリスク低減として法的に評価されることが明確になれば、事業者は法的不確実性を抱えることなくPETsを活用できるようになるとともに、経営者にとっての善管注意義務・安全管理措置上の負担軽減にも直結する。

第三に、制度的不確実性が競争条件に与える影響の問題である。PETsの法的位置づけが未整備のまま推移する場合、欧米においてPETsを活用した大規模データ連携が制度的に許容される環境が整う一方で、日本企業は同等の取り組みに対して高い法的不確実性を抱え続けることになる。この状況が長期化すれば、データビジネスにおける競争条件に構造的な差異が生じるリスクがある。これは個別企業の問題にとどまらず、日本のデータ経済全体の発展に関わる論点として、官民双方で共有されるべき問題意識である。技術的な手段はすでに存在する。制度的な位置づけの整備が、その活用を可能にする条件となる。技術と制度が揃ったとき、データ連携の可能性は初めて現実のものになる。



いる。なお、NISTは2023年12月に差分プライバシーの評価ガイドライン草案（SP 800-226）を公表し、パブリック・コメントを経て2025年3月に最終版“Guidelines for Evaluating Differential Privacy Guarantees”として正式公表した。AIへの適用を含むPETsの制度的位置づけの強化を示すものである。

**JIPDEC　電子情報利活用研究部　　次長　　松下　尚史**

青山学院大学法学部卒業後、不動産業界を経て、2018年より現職。経済産業省、内閣府、個人情報保護委員会の受託事業に従事するほか、G空間関係のウェビナーなどにもパネリストとして登壇。その他、アーバンデータチャレンジ実行委員。

実施業務：

・自治体DXや自治体のオープンデータ利活用の推進
・プライバシー保護・個人情報保護に関する調査
・ID管理に関する海外動向調査
・準天頂衛星システムの普及啓発活動　など