欧米主要国におけるプライバシー強化技術（PETs）の利用に関する法制度に関する調査

2023年3月31日

渥美坂井法律事務所・外国法共同事業

目次

第1　本調査について

1　調査事項

令和 4 年 10 月「欧米主要国におけるプライバシー強化技術（PETs）の利用に関する法制度に関する調査調達仕様書」記載のとおり。

2　調査体制

次の各弁護士・外国弁護士により調査を実施した。

【渥美坂井法律事務所・外国法共同事業　所属】

- 落合孝文（シニアパートナー弁護士）※主担当者
- 藤原理（パートナー弁護士）※副担当者
- 松下外（パートナー弁護士）※副担当者
- 三澤充（パートナー弁護士）
- 湊健太郎（パートナー弁護士）
- 新舎千恵（パートナー弁護士）
- 三浦康晴（オブ・カウンセル弁護士）
- 宮西啓介（アソシエイト弁護士）
- 表大祐（アソシエイト弁護士）
- 藤川由美子（アソシエイト弁護士）
- 星野真太郎（アソシエイト弁護士）
- 森茜（アソシエイト弁護士）
- ニコラス・J・カッソン（アソシエイト）
  ※イングランド及びウェールズ事務弁護士（日本における外国法事務弁護士登録はない。）
- キーラン・ローズ（アソシエイト）
  ※アイルランド共和国弁護士（日本における外国法事務弁護士登録はない。）

【Atsumi & Sakai New York LLP　所属】

- 勝見将也（アソシエイト）
  ※米国イリノイ州弁護士（日本における外国法事務弁護士登録はない。）

また、一般財団法人日本情報経済社会推進協会（JIPDEC）に対して、調査業務の一部を再委託し、下記の者より調査協力を得た。

- 松下尚史（グループリーダー）
- 水島九十九（主席研究員）

3　ヒアリング先個人情報保護機関

本調査の過程において、次の調査対象国・地域のデータ保護機関等に対して、質問票を送付の上で、書面又はインタビュー等による回答を得た。

EU	欧州データ保護監督機関（European Data Protection Supervisor: EDPS）
英国	英国情報コミッショナーオフィス（Information Comissioner’s Office: ICO）
米国	連邦取引委員会（Federal Trade Comission：FTC）
カナダ	カナダプライバシーコミッショナーオフィス（Offuce of the Privacy Commisioner Canada: OPC）

第2　EU

1　プライバシー強化技術（PETs）の名称・技術の概要

（1）調査対象国において、個人データを保護したままで分析等を行うプライバシー強化技術として注目あるいは実用化されている名称と技術の概要。

(1) PETs の定義

ア　関連法令の定め

2016 年 4 月に制定され、2018 年 5 月に施行された「一般データ保護規則（General Data Protection Regulation）」（以下「**GDPR**」という。）は PETs の定義規定を設けていない。また、2022 年 5 月に欧州委員会により採択され、2023 年 9 月から施行される予定となっているデータガバナンス法[1]も、PETs の定義規定を設けていない。

イ　ENISA による定義

(ｱ) 2015 年 ENISA 報告書

欧州連合サイバーセキュリティ機関（The European Union Agency for Cybersecurity）（以下「**ENISA**」という。）が、2015 年 1 月 12 日に公表した報告書「デザインによるプライバシーとデータ保護 - ポリシーからエンジニアリングまで（Privacy and Data Protection by Design － from policy to engineering）」（以下「**2015 年 ENISA 報告書**」という。）[2]は、PETs を次のとおり定義している。欧州データ保護監督機関（European Data Protection Supervisor）（以下「**EDPS**」という。）も、自らのウェブサイト上の用語集[3]にこの定義を掲載している。

情報システムの機能を損なうことなく、個人データを削除又は削減し、あるいは個人データの不必要又は望ましくない処理を防止することによって、プライバシーを保護する情報通信技術（ICT）対策の一貫したシステム

[1] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L152, 2022.6.3, p.1. http://data.europa.eu/eli/reg/2022/868/oj

[2] ENISA, *Privacy and Data Protection by Design – from policy to engineering* (Jan, 2015), https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design 18 頁

[3] EDPS, Glossary, https://edps.europa.eu/data-protection/data-protection/glossary/p_en

この定義は、ENISA が 2022 年 1 月 27 日に公表したレポート「データ保護エンジニアリング（Data Protection Engineering）」（以下「**2022 年 ENISA 報告書**」という。）[4]でも用いられている。

(イ) 2016 年 ENISA 報告書

ENISA は、2016 年 3 月 31 日に「PETs の導入と進化に向けた準備分析（Readiness analysis for the adoption and evolution of PETs）」（以下「**2016 年 ENISA 報告書**」という。）[5]を公表し、その中で、PETs は次の技術を包含するとしている。

> ソフトウェアとハードウェアのソリューション、すなわち特定のプライバシー又はデータ保護機能を達成するため、あるいは個人又は複数の自然人で構成されるグループのプライバシーリスクから保護するための技術的プロセス、方法、知識を包含するシステムを含む、プライバシー又はデータ保護機能をサポートする、あらゆる種類の技術

当該定義は、データ回避とデータ最小化に焦点を当てていない点において、2015 年 ENISA 報告書の定義と比較して広く、広範な技術を含む[6]。2016 年 ENISA 報告書では次の技術が PETs の一例として取り上げられている。

- データシステムの機能を失うことなく、個人データを排除又は削減し、あるいは個人データの不必要かつ/又は望ましくない処理を防止することによってプライバシーを保護する ICT 対策の一貫したシステム[7,8]
- 一般に、個人のプライバシーを保護するのに役立つ幅広い技術を指し、匿名性を提供するツールから、個人情報を開示するかどうか、いつ、どのような状況下で開示するかをユーザーが選択できるようにするものまで、PETs の使用は、

---

[4] ENISA, *Data Protection Engineering* (Jan, 2022), https://www.enisa.europa.eu/publications/data-protection-engineering 9 頁

[5] ENISA, *Readiness analysis for the adoption and evolution of PETs* (Mar, 2016), https://www.enisa.europa.eu/publications/pets 9 頁

[6] 2016 年 ENISA 報告書は、Claudia Díaz, Omer Tene, and Seda F. Gürses. Hero or Villain: The Data Controller in Privacy Law and Technologies. Ohio State Law Journal, 74(6):923–964, 2013.や Zbigniew Kwecka, William Buchanan, Burkhard Schafer, and Judith Rauhofer. “I am Spartacus” - Privacy Enhanc-ing Technologies, Collaborative Obfuscation and Privacy as a Public Good. Artificial Intelligence and Law, 22(2):113–139, 2014.を紹介した上で、広範な定義を採用する旨述べている。

[7] John J. Borking and Charles D. Raab. Laws, *PETs and other Technologies for Privacy Protection. Journal of Information*, Law & Technology (JILT), 1(1), 2001. https://www.researchgate.net/publication/220667925_Laws_PETs_and_Other_Technologies_for_Privacy_Protection

[8] 2016 年 ENISA 報告書は、この定義はデータ回避とデータ最小化に焦点を当てたものであるとしているが、他方で、Borking et al, 前掲注 7 の文献の著者らは他のプライバシー支援技術の存在も認めているともしている。

ユーザーがプライバシー保護について十分な情報を得た上で選択できるようにするもの[9]

- 個人データの収集・使用を最小限に抑え、データ保護規則の遵守を促進するような方法で、情報通信システム及びサービスを設計するのに役立つもの[10]

そのため、EUでは、PETsは広範な技術を含むものとして理解が進む可能性もある[11]。

(2) PETsの種類

ア PETsの分類

(ア) 2022年ENISA報告書

2022年ENISA報告書では、スペインの個人情報保護機関であるAgencia Española de Protección de Datos (AEPD)が作成した「Privacy by Designへのガイド（A Guide to Privacy by Design）」（以下「**2019年AEPDガイド**」という。）[12]上の記載に言及する形で、PETsの分類が技術的特性、追及する目的等に応じ複数あることを指摘した上で、処理されるデータに関する技術的な特性から、次のような整理を提案している。

真実性の確保（Truth-preserving）	プライバシーエンジニアリングの目的は、データの正確さを保ちつつ、その識別力を低下させることである。この目標は、例えば、データの粒度を小さくすることで達成できる（例：生年月日から年齢まで）。このようにすれば、問題とされる目的のために「最小限」でデータの正確性を保つことができる。また、暗号化は真理を守る技術であると見なすことができる。なぜなら、逆方向の暗号化を行うことで、元のデータが完全に復元され、その過程で不確実性が生じることがないからである。
明瞭性の確保（Intelligibility-preserving）	データは、真のデータ主体の属性を開示することなく、データ管理者にとって「意味を持つ」フォーマットで保持される。例えば、入院日付にオフセットを導入することで、日/月/年のフ

[9] Organisation for Economic Co-operation and Development (OECD). *Inventory of Privacy-Enhancing Technologies (PETs)*. Report DSTI/ICCP/REG(2001)1/FINAL, working party on information security and privacy. Technical report, 2002., https://web.archive.org/web/20221219084154/https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?doclanguage=en&cote=dsti/iccp/reg%282001%291/final 4頁

[10] European Commission. *Privacy Enhancing Technologies (PETs) – the existing legal framework. MEMO/07/159*, May 2007. , https://ec.europa.eu/commission/presscorner/detail/en/MEMO_07_159

[11] 第3・1・(1)・イで後述するとおり、英国でも2016年ENISA報告書の定義が有益なものとして取り上げられており、英国では、今後もPETsについて、より広範な定義が採用される可能性がある。

[12] AEPD, *A Guide to Privacy by Design* (Oct, 2019), https://www.aepd.es/es/documento/guia-privacidad-desde-diseno_en.pdf 26頁

	ォーマットは維持しつつも、識別された患者の真のデータとのリンクを断つことできる。また、ノイズの投入は、データの見た目を変えないため、真のデータの機密性を保護することができる明瞭性確保の技術である。
演算可能技術（Operatable Technology）	数学的及び論理的な操作（例えば、合計や比較）が、その適用結果に対して実行可能であること。演算可能であることは必ずしも明瞭性を伴わない。暗号化領域で正しく実行できる演算を用いて（非明瞭な）結果が直接演算可能な暗号化技術の種類が存在するからである。

(ｲ) 2019 年 AEPD ガイド

2019 年 AEPD ガイドでは、達成されるべき目的に応じる分類として、以下の整理が掲載されている[13]。

分類	下位分類	概要
プライバシー保護	擬似匿名化ツール	個人情報を求めない取引を可能にする
	匿名化製品・サービス	データ主体の識別を要求せずサービスへのアクセスを提供する
	暗号化ツール	第三者による文書や取引の閲覧を防ぐ
	フィルタ及びブロッカー	不要なメールやウェブコンテンツの回避
	アンチトラッカー	ユーザーのデジタルフットプリントの削除
プライバシーマネジメント	情報ツール	プライバシーポリシーの作成と検証
	管理ツール	ユーザーID 及び許可の管理

イ　PETs として取り上げられる主な技術

前述の他、具体的にいかなる技術が PETs に該当するかを統一的に論じた文献等は見当たらないものの、次の各文書に示すようにその外延が断片的に示されている。

[13] 元々の出典は、META Group, *Privacy Enhancing Technologies – META Group Report v 1.1* (Mar, 2005), https://danskprivacynet.files.wordpress.com/2008/07/rapportvedrprivacyenhancingtechlologies.pdf である。

なお、EDPS へのインタビューによれば、AI や機械学習における連合学習（federated learning）が、将来の実装に向けて検討され始めているとのことである。

(ア) 2007 年 EC メモ

欧州委員会が、2007 年に公表した文書「PETs – 既存の法的枠組み（Privacy Enhancing Technologies (PETs) – the existing legal framework. MEMO/07/159）」（以下「**2007 年 EC メモ**」という。）[14]では、以下が PETs の例として紹介されている。

一定期間経過後の自動的な匿名化（Automatic anonymisation after a certain lapse of time）	処理されたデータは、データ対象者を識別できる形で、データが当初収集された目的のために不必要な期間、保存されるべきでないという原則を支援するもの。
暗号化ツール（Encryption tools）	情報がインターネット上で送信される際にハッキングされることを防止し、違法な処理から個人データを保護するために適切な措置を講じるというデータ管理者の義務を支援するもの。
クッキーカッター（Cookie-cutters）	ユーザーの PC に設けられ、ユーザーが気づかないうちに特定の命令を実行させるクッキーをブロックすることで、データは公正かつ合法的に処理されなければならず、データ主体が処理について知らされていなければならないという原則の遵守を強化するもの。
プライバシー・プリファレンスのためのプラットフォーム（The Platform for Privacy Preferences (P3P)）	インターネットユーザーが、自身で公開を許可する情報を選択できるようウェブサイトのプライバシーポリシーを分析することができ、情報提供を受けてデータ主体がデータ処理に対して同意したことを保証するのに役立つもの。

(イ) 2014 年 29 条作業部会匿名化意見書

[14] EC, 前掲注 10

29 条作業部会が 2014 年に公表した匿名化技術に関する意見書（Opinion 05/2014 on Anonymisation Techniques）（以下「**2014 年 29 条作業部会匿名化意見書**」という。）[15] は、匿名化技術として、①ランダム化（Randomization）と②一般化（Generalization）の 2 つを挙げている。これらの中には、例えば、差分プライバシー等、一般的に、PETs として取り上げられることがあるものも含まれている。

①ランダム化（Randomization）とは、個人とデータの間の関係性を取り除き、データが十分に不確実になれば特定の個人を識別できなくするものであり、属性にノイズを追加したり、順列を変えたりすることでデータ主体との関係性を作為的に減らすこと等が想定される。その例として挙げられるのは、次の技術である。

ノイズ付加（noise addition）	データセット内の属性を、全体の分布を維持したまま精度が低くなるように修正する技術。当該属性が重大なリスクを及ぼす可能性がある場合に特に有用である。
置換（permutation）	データセット内のある属性値をシャッフルし、一部の属性値を異なるデータ対象者に人工的にリンクさせる技術。データセット内の各属性の正確な分布を保持することが重要な場合に有用である。
差分プライバシー（differential privacy）	データセットから匿名化ビューを生成するときに使用される。匿名化ビューには、事後的に意図的に追加されたランダムなノイズが含まれる、特定の第三者に対するクエリ（一般に、データベース管理システムに対する処理要求をいう。）のサブセットを通じて生成される。差分プライバシーにより、管理者はどの程度のノイズをどのような形で追加する必要があるのかが分かる。

②一般化（Generalization）とは、規模や順序を修正して、データ主体の属性を一般化又は希薄化させる手法が想定される。その例として挙げられるのは、次の技術である。

集積と K-匿名化（aggregation and k-anonymity）	データ対象者を少なくとも K 名の他の個人とグループ化することで、識別されるのを防ぐ技術。例えば、場所の粒度を都市

[15] Article 29 Working Party, *Opinion 05/2014 on Anonymisation Techniques. WP 216, 10*, (Apr, 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf 11 頁。なお、2014 年 29 条作業部会匿名化意見書は GDPR 制定以前のものであるが、2020 年公表の GDPR 第 25 条に基づくデザインによるデータ保護の原則、及びデフォルトによるデータ保護の原則に関するガイドライン（後掲注 41）でも参照されている。また、後掲注 41 によれば、2014 年 29 条作業部会匿名化意見書は、EDPB 内で改訂中であるとされている。

	から国に下げることで、より多くのデータ対象者が含まれるようにする。
L-多様性（L-diversity）/ T-近似性（T-closeness）	L-多様性は K-匿名化を拡張したもので、各同値クラスにおいて全ての属性が少なくとも L 個の異なる値を持つようにすることで、決定論的推論攻撃がもはや不可能であることを保証する技術。 T-近似性は L-多様性の改良版であり、データセット中の属性の初期分布に近い等価クラスを作成することを目的としている。

(ｳ) 2019 年 SODA レポート、2021 年 EDPB 勧告、2021 年 ENISA 報告書

次の各レポートでは、秘密計算（Secure Multi-Party Computation）が言及されている。秘密計算が PETs に該当するか否かについて、各レポートでは明言されていないものの、秘密計算の使用事例とともに、匿名化を含むデータ保護の方法が紹介されている。以下の内容のとおり、データ保護機能をサポートする技術として、前述第 2・1・(1)・イ・(ｱ)の PETs の定義に該当するものと思われる。

- European Union's Horizon 2020 が出資するプロジェクトの一環である SODA が、2019 年 12 月 30 日に公表したレポート「D3.5 使用事例特有の法的側面（D3.5 Use-case specific legal aspects）」[16]（以下「**2019 年 SODA レポート**」という。）
- EDPB が 2021 年 7 月 18 日に公表した勧告「個人データの保護に関する EU の水準への準拠を確保するために転送ツールを補完する措置に関する勧告 01/2020 号（Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data）」[17]（以下「**2021 年 EDPB 勧告**」という。）
- ENISA が 2021 年 1 月 28 日に公表したレポート「データ仮名化：高度な技術と使用事例（Data Pseudonymisation: Advanced Techniques and Use Cases）」[18]（以下「**2021 年 ENISA 報告書**」という。）

秘密計算	複数の参加者が相互に有用な結果を計算する暗号技術。

[16] SODA, *D3.5 Use-case specific legal aspects,* (Dec, 2019) https://soda-project.eu/wp-content/uploads/2019/12/SODA-D3.5-Use-case-specific-legal-aspects.pdf
[17] EDPB, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data,* (June, 2021) https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en
[18] ENISA, *Data Pseudonymisation: Advanced Techniques and Use Cases,* (Jan, 2021), https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases

（Secure Multiparty Computation）	各参加者は秘密情報を入力するが、自分の入力に対する結果のみしか知ることができず、参加者が入力した情報全てにはアクセスすることができない[19]。

（ｴ） 2022 年 ENISA 報告書

2022 年 ENISA 報告書[20]では、匿名化及び仮名化技術として、k-匿名性と差分プライバシーが説明されている。加えて、データマスキング及びプライバシー保護演算との関係で、次の各技術が PETs である旨の記述がある。

準同型暗号（Homomorphic encryption(HE)）	暗号化されたデータを復号化することなく、暗号化されたデータのまま計算を実行することができる技術をいう。HE には、部分的準同型暗号（PHE）と完全準同型暗号（FHE）の 2 種類がある。部分的準同型暗号は、暗号文に対して単一の演算（例えば、加算か乗算のどちらか）しか実行できないのに対し、完全準同型暗号は、多重演算（現在は加算と乗算の両方）に対応しており、暗号化されたデータに対してより多くの計算を実行することができる。
秘密計算（Secure Multiparty Computation）	複数の当事者間で計算を分散し、個々の当事者が他の当事者のデータを見ることができないようにして、当事者間の相互信頼の問題を解決しようとするもの。
信頼できる実行環境（Trusted Execution Environment (TEE)）	デバイスのメインプロセッサー上で動作する耐タンパ性（tamper-resistant。機器やシステムにおいて、その内部の機密情報データや動作等を、外部から解析や改変されることを防ぐ能力）のある処理環境をいう。TEE では、データの処理は分離された領域内で行われる。
秘匿情報検索（Private information retrieval (PIR)）	データ管理者にどの要素が照会されたかを明かすことなく、データベース内の項目を復元することを可能にする暗号技術をいう。データ管理者がどの項目がアクセスされたかを知る

[19] SODA, 前掲注 16・48 頁

[20] ENISA, 前掲注 4・14-18 頁。なお、ENISA は、2022 年 3 月 24 日に「仮名化技術の展開（Deploying Pseudonymisation Techniques）」（https://www.enisa.europa.eu/publications/deploying-pseudonymisation-technique）と題する報告書を公開しており、その 9 頁では、①カウンタ（Counter）、②乱数（Random number）、③ハッシュ関数（Hash function）、④ハッシュベースのメッセージ認証コード (Hash-based message authentication code: HMAC）、⑤暗号化（Encryption）等の仮名化技術が紹介されている。

	のを防ぐことで、どの項目が顧客の関心事であるかを特定できないようにすることができる。
合成データ（Synthetic data）	実際のデータに似ているが、元のデータを参照することができないデータをいう。また、ある集団のパラメータをよりよく推定するために、複数のデータソースを組み合わせること（異なるデータセット間の一種のクロスエンリッチメント）を指すこともある。合成データは、実データとは異なり、生成と処理の際にデータ主体の個人領域を侵さないため、個人の機密性を尊重することができる。他方で、合成データは、その使用によってより正確で偏りのない数値が得られるかどうか、試行錯誤する必要性が懸念される。

（3）PETs 利用のインセンティブ

ENISA のウェブサイトによれば、PETs は、データ最小限化の原則、匿名化、仮名化を中心とするプライバシー原則に従って技術を形成することを目的としていることが示唆されている[21]。データ最小限化の原則とは、その個人データが取り扱われる目的との関係において、十分であり、関連性があり、かつ、必要のあるものに限定されなければならないというものである（GDPR 第 5 条第 1 項第 c 号）。

PETs を利用することの利点、すなわち、インセンティブとして以下の点が挙げられる。

- PETs の利用より、データ保護規則の違反や個人の権利侵害が禁止された行為であり制裁対象であることが明確になるだけでなく、データ保護規則の違反や個人の権利侵害といった行為が技術的に難しくなる[22]。
- PETs の使用は、個人データの収集・使用を最小限に抑え、データ保護規則の遵守を促進する方法で、情報通信システム及びサービスを設計するのに役立つ。PETs を使用することにより、特定のデータ保護規則への違反がより困難となり、又はその発見を助けることになるはずである[23]。
- 必ずしも PETs に限られないものの、匿名化処理のインセンティブとして、「ヘルスケアの観点でビッグデータを活用することは非常に有益であるが、健康関連データは、最も機密性が高く個人的なデータであるため、その機密性を保持

[21] ENISA, *Privacy enhancing technologies*, http://web.archive.org/web/20220902092957/https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies

[22] EC, 前掲注 10

[23] EDPS, 前掲注 3

し、安全な処理を確立することが最も重要である。このため、健康データの匿名化処理には高いインセンティブがある。」と指摘されている[24]。

- EDPS へのインタビューによれば、個人データの効果的な暗号化は、違法なアクセスや改変に対する強力な回避手段となり（ただし、GDPR における管理者及び処理者の義務を軽減するものではないとのこと）、かつ、適切に文書化することで、監督当局に対するコンプライアンスの証明に貢献することができるとのことである。

（4）PETs 利用の障壁

ENISA は、PETs の利用の障壁として、①成熟度及び②インセンティブそれぞれの欠如を強調している[25]。

ア　成熟度の欠如

ENISA は、2016 年 ENISA 報告書[26]において、データ処理者にとって、PETs がいつシステムに実装できるほど成熟するかを判断することは困難であり、また、政治家、監督当局、資金提供機関、標準化団体等の重要な利害関係者にとっても、現在、業務に影響を及ぼすであろう PETs の成熟度を把握していないとしている。また、十分に成熟した PETs が認識されれば、法律、標準化、又は監督当局からその使用が推奨されうること、あまり成熟していないものの有望な PETs が認識されれば、これに対する研究開発投資が進みうることが示唆されている。

なお、ENISA が、2019 年に公表した報告書「ENISA の PETs 成熟度評価リポジトリ（ENISA's PETs Maturity Assessment Repository）」（以下「**2019 年 ENISA レポジトリ**」という。）[27]によれば、ENISA は 2016 年に PETs 成熟度評価オンラインレポジトリというウェブアプリケーションプロトタイプの開発を開始している[28]。2019 年 ENISA レポジトリでは、(a)「技術準備度」（technology readiness）と(b)「プライバシー強化品質」（privacy enhancement quality）の 2 つの尺度から算出される結果を「PET 成熟度」とするものとされ、その評価は、2019 年 ENISA レポジトリの専門家委員会のメンバーとして活動する専門家から選定されることが想定されている。

---

[24] SODA, 前掲注 16・62 頁

[25] ENISA, 前掲注 5・11 頁

[26] ENISA, 前掲注 5・7 頁

[27] ENISA, *ENISA's PETs Maturity Assessment Repository,* (Jun, 2019), https://www.enisa.europa.eu/publications/enisa2019s-pets-maturity-assessment-repository 10-13 頁

[28] ただし、現在当該プロトタイプ（http://pets.enisa.europa.eu）にアクセスすることができず、開発状況は不明である。

より具体的には、(a)技術準備度に関しては、以下の準備レベルが設定されている。

アイデア（Idea）	最も低い技術準備度であり、技術報告書に記載された等、非公式な形でアイデアとして提案されたにとどまる段階。
研究（Research）	当該 PETs が厳密な科学的研究の対象となっており、少なくとも 1 つ、できればそれ以上の学術論文が発表され、その詳細や正しさとセキュリティ、プライバシー特性が論じられている段階。
概念実証（Proof-of-concept）	当該 PETs は実装され、特定の特性についてテストの実施が可能（すなわち、実行コードが利用可能）であるが、実際のユーザーが関与する応用は存在せず、実装機能も完全でない段階。
パイロット（Pilot）	当該 PETs は、実際のユーザー（専門家や学生に限定されている場合がある）が参加する、少なくとも小規模な試験的適用で実際に使用され、又は、使用されようとしている段階。
製品（Product）	最も高い準備度であり、当該 PETs は 1 つ以上の一般に入手可能な製品に組み込まれ、相当数のユーザーが実際に使用され、又は、使用されようとしている段階。
陳腐化（Outdated）	当該 PETs の必要性が薄れた、保守が終了した技術に依存している、代替となる PETs が存在するといった理由で、もう使用されなくなった段階。

他方、(b)プライバシー強化品質に関しては、次の 9 つの品質特性が定義されており、それぞれについて、5 段階のスコア（非常に悪い（very poor）、悪い（poor）、満足（satisfactory）、良い（good）、非常に良い（very good））が振られ、これらを総合したプライバシー強化品質として、同じく 5 段階のスコアによる評価がされる。

- 保護（protection）
- 信頼前提（trust assumptions）
- 副作用（side effects）
- 信頼性（reliability）
- 操作性（operability）
- 性能効率（performance efficiency）
- 保守性（maintainability）
- 移転性（transferability）
- 範囲（scope）

イ　インセンティブの欠如

ENISA は、2016 年 ENISA 報告書において、どの程度のスピードで PETs が進化するかは、その技術の複雑さにもよるものの、それ以上に、技術の進化を実現するためのインセンティブに依存するとしており、開発のためのインセンティブが欠如していることが、PETs 利用の障壁であることを示唆している。

2　データ保護法との関係、データ保護法上の論点

（2）上記において、個人情報、プライバシー保護に関する法律（以下「個人情報保護法等」という。）の観点から論点となっている点（過去論点となった点、事業者による改正要望、政府による改正予定の点も含む。）。

(1) EU におけるデータ保護法の概要

EU におけるデータ保護法としては、2016 年 4 月に制定され、2018 年 5 月に施行された GDPR が存在し、また、2022 年 5 月に採択され、2023 年 9 月から施行されるデータガバナンス法も該当しうる。

ア　GDPR

GDPR は、十分性認定等 EU データ保護指令の内容を引き継ぎつつ更に個人データの厳格な保護を図るものであり、EU 域内におけるデータ保護ルールを一元化して、EU 域内各国における規制の単一化・簡素化を図る一方、より強固な個人データ保護ルールの整備、データ保護に関するグローバルな課題への対応を図っている。

イ　データガバナンス法

データガバナンス法は、個人や産業が生み出す膨大なデータを技術革新や経済成長につなげるために、データの取扱いの安全性を確保する等、データ共有への信頼性を高めながら、EU 域内で官民を超えたデータ共有の促進を目指している。

(2) PETs と EU データ保護法との関係

ア　GDPR

GDPR は、データ保護の原則として、①適法性、公正性及び透明性の原則、②目的の限定の原則、③データ最小化の原則、④正確性の原則、⑤保管の限定の原則、⑥完全性（integrity）及び機密性の原則（安全性の原則）、⑦アカウンタビリティの原則の 7 つの原則を規定しており（GDPR 第 5 条第 1 項）、これらの原則が個人データの処理の方

法の中心に置かれるべきものとされている。PETs は、これらのデータ保護の原則を効果的に実施し、データ処理において必要なセーフガードを組み込むことに資する。

GDPR 上の PETs に関連しうる主な規定は以下のとおりである。

匿名化 **（前文第 26 項）**	「匿名の情報、すなわち特定の若しくは特定可能な自然人に関連しない情報、又はデータ主体が特定されない若しくは特定される可能性のない方法で匿名化された個人データ」には、GDPR は適用されない。
仮名化 **（第 4 条第 5 号）**	「仮名化」とは、追加の情報を用いなければ、個人データを特定のデータ主体に連結することができないような方法による個人データの処理をいう。仮名化がされた個人データは、GDPR 上の個人データに該当し、GDPR の適用を依然として受ける。
「デザインによるデータ保護」及び「デフォルトによるデータ保護」 **（第 25 条）**	データ管理者は、初期設定によりそれぞれの取扱目的に必要な個人データのみを取り扱うための適切な技術的及び組織的措置を講じる義務を負う。
取扱いの安全性 **（第 32 条）**	データ管理者及びデータ処理者は、リスクに適切に対応する一定のレベルの安全性を確保するために、適切な技術上及び組織上の措置をしかるべく実装することとされており、かかる措置の具体例として、「個人データの仮名化又は暗号化」が挙げられている（第 32 条第 1 項(a)）。
データ保護影響評価 **（第 35 条）**	取扱いの性質、範囲、過程及び目的を考慮に入れた上で、特に新たな技術を用いるような種類の取扱いが、自然人の権利及び自由に対する高いリスクを発生させるおそれがある場合、管理者は、その取扱いの開始前に、予定している取扱業務の個人データの保護に対する影響についての評価を行わなければならない。
越境移転 **（第 44 条）**	GDPR 上、個人データを EEA 域外に移転することは原則として禁止されている（第 44 条）が、欧州委員会が、十分なデータ保護の水準を確保しているとの認定（十分性認定）を行った国、地域又は国際機関へのデータ移転の場合（第 45 条第 1 項）や、標準契約条項（SCC）に基づく契約を締結している場合（第 46 条）には、個人データの越境移転が可能となる。

イ　データガバナンス法

データガバナンス法では、EU 加盟国は、公的機関が、匿名化、差分プライバシー、一般化、抑制、ランダム化、合成データ又は同様の方法の使用、及びよりプライバシーに優しいデータ処理に貢献できるその他の最先端のプライバシー保護方法等、個人データを含むデータベースの分析を可能にする技術を最適に利用できるように支援を提供し、可能な限り多くのデータを共有できるようにしなければならない（前文第 7 項）とされている。

(3) PETs に関わる EU データ保護法上の論点

以下、第 2・2・(2)・アで前述した GDPR 上の枠組みとの関係から、PETs に関する EU データ保護法上の論点のうち、主要と思われるものを紹介する。ただし、EDPS へのインタビューによれば、GDPR における法的義務を軽減、又は、最小化する技術的要件は存在せず、GDPR 第 25 条等、いくつかの条項への遵守を示すことに寄与するにとどまるものと思われる。

ア　匿名化

(ア) 匿名化の意味内容

「匿名化」は「匿名の情報、すなわち識別された若しくは識別可能な自然人に関連しない情報、又はデータ主体が特定されない若しくは識別される可能性のない方法で匿名化された個人データ」（GDPR 前文第 26 項）を実現するものである[29]。GDPR 前文第 26 項は、個人の識別可能性の判断基準に関し、「ある自然人が識別可能であるかどうかを判断するためには、選別のような、自然人を直接又は間接に識別するために管理者又はそれ以外の者によって用いられる合理的な可能性のある全ての手段を考慮に入れなければならない。自然人を識別するために手段が用いられる合理的な可能性があるか否

[29] GDPR の前身であるデータ保護指令の適用期間における議論ではあるが、データ保護監督機関及びおよび法律文献において、個人データの理解につき、識別可能性の絶対的概念と相対的概念という 2 つの立場から議論がなされた。

絶対的概念は、データ管理者又はその他の第三者がその情報を特定の個人を関連付けることができる場合、その情報を個人データとみなす、理論的な識別可能性があれば、データ保護指令の法的効果を惹起させるとする。

これに対し、相対的概念は、データ管理者が個人を識別する現実的な可能性を考慮するものである。個々の具体的なケースでデータ管理者が実際に適用しうる手段のみを考慮に入れることとしており、データ管理者が手段、機会、知識を有するか否かを判断する上で関連する要素を考慮しなければならず、単に仮想的な事象は考慮の対象外としている。第三者の認識と手段及び状況に依存する状況をどの程度まで識別に考慮するかは、GDPR の下で依然議論がなされている。

かを確認するためには、取扱いの時点において利用可能な技術及び技術の発展を考慮に入れた上で、識別のために要する費用及び時間量のような、全ての客観的な要素を考慮に入れなければならない」としている。

また、個人の識別可能性に対し、欧州司法裁判所（ECJ）は一定の判断を示している[30]。この事件は、ドイツ連邦裁判所（BGH）が、動的 IP アドレスを個人データと見なすことができるかどうかという論点の解釈についてガイダンスを求める予備判決手続の要請として、欧州司法裁判所（ECJ）に付託されたものである。欧州司法裁判所（ECJ）は個人の識別可能性を判断する際には、①データ管理者のみならず、むしろデータ管理者又はその他の者によって（not only by the data controller, rather by the data controller or by any other person）、②合理的に使用される可能性のある全ての手段を考慮しなければならない（all the means reasonably likely to be used shall be taken into account）との枠組みによって判断することを判示した。この判示は、2014 年 29 条作業部会匿名化意見書が示した、「管理者又はその他の者によって合理的に使用される可能性が高い手段」という識別の可能性の基準と一致するものとされている[31]。これを裏返せば、「管理者又はその他の者によって合理的に使用される可能性が高い手段」によっても個人が識別することができない場合に初めて、匿名化が実現されたといえる。

前述のとおり、差分プライバシー等の一部の匿名化技術は、PETs として整理されることがあるため、一般論としては、PETs を利用することにより、個人データの匿名化（GDPR 前文第 26 項）を図れる可能性がある。もっとも、スペインデータ保護機関（AEPD）と EDPS が、2021 年 4 月 27 日に共同で公表したペーパー「匿名化に関する 10 の誤解（10 MISUNDERSTANDINGS RELATED TO ANONYMISATION）」（以下「**2021 年 AEPD ペーパー**」という。）[32]では、全ての PETs が匿名化を達成するとは限らないとされている。

具体的な PETs と匿名化の関係に関する各種文献における説明は以下述べるとおりである。

（イ） 暗号化ツール

例えば、第 2・1・(2)・イ・(ア)で述べたとおり、暗号化ツールは PETs として評価されることもあるが、2021 年 AEPD ペーパーでは、鍵暗号方式における暗号化では、個人

---

[30] ECJ decision of 19/10/2016 – C-582/14, Patrick Breyer v Bundesrepublik Deutschland, ECLI:EU:C:2016:779https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0582

[31] 以上につき、SODA レポート（前掲注 16）

[32] AEPD-EDPS, *Joint paper on 10 misunderstandings related to anonymization,* (Apr, 2021), https://edps.europa.eu/data-protection/our-work/publications/papers/aepd-edps-joint-paper-10-misunderstandings-related_en 3 頁

データの仮名化が実現できる可能性があるにとどまり匿名化は実現できないということが示唆されている。

さらに、EDPS へのインタビューによれば、秘密計算方式における暗号化であっても、共有された秘密の断片が存在する以上、個人データの仮名化を実現する可能性があるにとどまり、匿名化は実現できないとのことである。

(ｳ) 差分プライバシー

2014 年 29 条作業部会匿名化意見書では、匿名化が認められるための基準として、①個人の抽出（Singling out）ができないこと、②同一人物の記録との照合（Likability）ができないこと、③特定の個人に関する情報であるとの推定（Inference）ができないことの 3 つを挙げている。その上で、前述の意見書で取り上げられた各技術を評価しているが、例えば、差分プライバシーは匿名化を実現しない可能性があるものとして整理されている。

匿名化技術	①抽出（Singling out）のリスク	②照合（Likability）のリスク	③推定（Inference）のリスク
順列化 permutation	○	○	○
ノイズ付加 noise addition	○	おそらく×	おそらく×
置換 Substitution	○	○	おそらく×
集積と k-匿名化 Aggregation or K-anonymity	×	○	○
l-多様性 L-diversity	×	○	おそらく×
差分プライバシー Differential privacy	おそらく×	おそらく×	おそらく×
ハッシュ化 Hashing/Tokenization	○	○	おそらく×

なお、2014 年 29 条作業部会匿名化意見書は、匿名化技術の使用を検討する場合、管理者において以下のリスクを考慮しなければならないとしている。

- 仮名化されたデータを匿名化されたデータと同等とみなしてしまうこと
- 適切に匿名化されたデータは、個人から何らかの保護措置を奪うと考えること
- 特にプロファイリングの場合、特定の状況下で、適切に匿名化されたデータが個人に与える影響を考慮しないこと

(エ) 秘密計算

第 2・1・(2)・イ・(ウ)で前述した、いくつかの文献では、秘密計算と匿名化の関係についても言及されており、秘密計算は、個人データを仮名化して GDPR 上のデータ保護義務を果たすのに資する可能性があるのみならず、匿名化要件を満たす可能性もあるとされている。

- 2019 年 SODA レポートは、秘密計算は、データ主体を合理的に特定できない方法で匿名化データを作成することで、計算による匿名化の要件を満たす可能性があると指摘している。
- 2021 年 EDPB 勧告は、データ輸出者が、異なる管轄区域にある 2 つ以上の独立した処理者に、個人データを共同処理することを希望する場合、データ輸出者において、秘密計算によりデータの内容が開示されないように処理することで、データの越境移転ができる可能性があることを示唆している。
- 2021 年 ENISA 報告書は、秘密計算が仮名化に有用な手段であることや、それぞれ広告主と商人によって保持された広告を見た人と取引を完了した人のリストを比較しコンバージョン率を測定する方法による、広告の目的にも応用できる可能性を示唆している。

(オ) 合成データ

2022 年 ENISA 報告書では、合成データが匿名化手段として用いられうることを前提にしている記述がいくつかみられる。

まず、同報告書では、表形式でないデータや連続したデータの場合、匿名化はそれほど容易ではなく、また、単純でもないとした上で、例えば、移動データの場合、軌道上の 3 つか 4 つの時空間座標を知るだけで、数百万人の人口から高い確率で個人を再識別するのに十分であるとの問題を指摘し、その合成データ（実際の軌跡の統計的特徴から人工的に生成した軌跡）を公開することが考えられるとしている。また、別の箇所では、匿名化の一態様として用いられる合成データは、延長されかつ潜在的に制限のない保持期間による利益を得る可能性があると説明されている。

イ　デザインによるデータ保護/デフォルトによるデータ保護

2020 年に EDPB が採択した「第 25 条に関するガイドライン―デザイン及びデフォルトによるデータ保護（Guidelines 4/2019 on Article 25 Data Protection by Design and by Default）」（以下「**2020 年 EDPB 第 25 条ガイドライン**」という。）[33]によれば、最先端の成熟度に達した PETs は、リスクベースのアプローチにおいて適切であれば、「デザインによるデータ保護」の原則及び「デフォルトによるデータ保護」の要件に従った措置として採用することができるとされている。もっとも、PETs は、それ自体で第 25 条の義務を必ずしもカバーするものではなく、データ管理者は、その措置がデータ保護の原則及びデータ主体の権利を実施する上で適切かつ効果的であるかどうかを評価しなければならないとされている。

2022 年 ENISA 報告書でも、研究者や技術者の間では、「デザインによるデータ保護」はしばしば特定のプライバシー拡張技術（PETs）の使用と同一視されることを指摘する一方、「デザインによるデータ保護」は、特定の技術の実装に還元されるものでもないことが注意喚起されている。同報告書では、「デザインによるデータ保護」が、実際には、様々な技術的・組織的要素を含むプロセスであり、PETs も含めた技術的・組織的手段を適切かつタイムリーに展開することで、プライバシーとデータ保護の原則を実現するものであることが説明されている。

ウ　取扱いの安全性

GDPR 第 32 条（取扱いの安全性）は最新技術（state of the art）について言及しており、最新技術を考慮した上で適切な技術上及び組織上の措置をしかるべく実装することを管理者及び処理者に義務付けている。最新技術を採用するという要求は条件付きのものであり、「実装費用、取扱いの性質、範囲、過程及び目的並びに自然人の権利及び自由に対する様々な蓋然性と深刻度のリスク」とバランスを取る必要があるとされているが、データ管理者とデータ処理者は、その手段に応じて、どの最新技術を検討すべきかを決定しなければならない。

もっとも、そのような判断は、①何が最新であるかの定義が不明であること、②この問題に関する十分なガイダンスや判例法がないこと、③GDPR は適用が始まったばかりであり、事例が不足していること等のいくつかの要因により、難しい作業であり、更に、最先端の技術であることを確認するための行政機関がないため、裁判所による個別判断とならざるを得ず、そのため、官民の関係者による継続的な研究の対象であるとされている [34]。

---

[33] EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default,* (Oct, 2020), https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf 30 頁

[34] ENISA, 前掲注 27・8 頁

エ　データ保護影響評価（DPIA）

2022 年 ENISA 報告書において、データ保護影響評価（以下、本章において「**DPIA**」という。）は GDPR の下で導入された要請の一つであり、「デザインによるデータ保護／デフォルトによるデータ保護」アプローチの一部と認識することもできると説明されている。もっとも、同時に、同報告書は、GDPR 第 35 条第 7 項（d）「保護措置、セキュリティ対策及びメカニズムを含む、リスクに対処するために想定される措置 …」（the measures envisaged to address the risks, including safeguards, security measures and mechanisms…）に言及することに触れて、DPIA が、従来の技術的及び組織的措置の確保を超えて、必要な保護レベルを確保するための技術につき、より詳細な分析、選択、運用を求めるものである旨を述べている。

前述の DPIA に関する 2022 年 ENISA 報告書の説明は、PETs の利用について直接触れたものでない。もっとも、同報告書の別の箇所では、PETs を利用したデータ処理の運用に際しては、処理毎に全体的な分析を行う必要があり、その際には、DPIA と同様に処理の性質、範囲、文脈、目的等の側面も含まれるべきであることを強調している。そのため、ENISA は、PETs の利用に関して、少なくとも、DPIA 類似のリスク評価を実施することを求めているものと解される。

この点、GDPR 施行前のものであるが、ENISA は、2016 年にオンライン及び携帯プライバシーツールについて、PETs の成熟度の分析の方法論を含む評価と査定に関するフレームワークを提唱している[35]。2022 年 ENISA 報告書では明言されていないものの、PETs の利用に関する文脈で言及されていることに照らせば、PETs 利用の際のリスク分析に当該方法論及びフレームワークが参考になることを示唆するものとは思われる。参考のため、当該方法論及びフレームワークにおける評価項目を紹介する。

一般的な項目	
項目	**概要**
成熟度と安定性	セキュリティとプライバシーに関する既存及び/又は新規の課題にツールが対応する方法、ユーザーグループのセキュリティとプライバシーのニーズに対応するためにツールが発展する方法か否か。
プライバシーポリシーの実施	PETs 開発者/プロバイダが個人データ処理方針のきちんと定義し、関連管理の使用によるこの方針を実施しているか否か。

[35] ENISA, *PETs controls matrix,* (Dec, 2016), https://www.enisa.europa.eu/publications/pets-controls-matrix 14 頁。なお、使用中のデータの暗号化処理ではなく、データの通信（転送中と静止中）に焦点が当てられている。

ユーザビリティ	ユーザーがツールを使用して、有効性、効率性及び満足感をもってプライバシー保護機能を実現できる程度。

※ あらゆる種類のツールに適用可能で PETs の一般的特性を評価することを目的とする項目

個別的な項目		
分類	**項目**	**概要**
セキュリティ保護されたメッセージツール	エンド・ツー・エンドの暗号化	メッセージを読むことができるのは、通信している人だけという通信方式か否か。
	クライアント・サーバーの暗号化	クライアントとサーバーの間に確立された通信路を暗号化しているか否か。
	保存データの安全性	保存データ（ローカル及びリモート）の安全性の程度。
	認証	通信相手の身元確認、通信データの真正性の確認の有無。
	匿名通信	第三者が当該通信の通信相手を特定できるか否か。
VPN	個人情報保護	ユーザーの実際の IP アドレスやその他の識別子を第三者から秘匿しているか否か。
	VPN 暗号化	ユーザーと VPN 事業者の間の通信経路を保護しているか否か。
	悪影響	VPN を利用することによる、ユーザーのオンライン体験に悪影響の有無。
匿名化ネットワーク	匿名性保護	ネットワーク内や第三者から、ユーザーを特定できるか否か。
	暗号化	エンド・ツー・エンド、又はネットワークの特定の部分における通信の安全性を確保しているか否か。
	悪影響	ツールによるユーザーのオンライン体験への悪影響の有無。

トラッキング防止ツール	ブロック機能	さまざまな種類のオンライントラッカーをブロックする機能の有無。
	データ収集	ユーザーのブロック/ブラウジングの習慣に関するデータを収集の有無。
	悪影響	ツールによるユーザーのオンライン体験への悪影響の有無。

※ 明確なカテゴリー/タイプに分類される PETs の特徴を評価し、その技術的特徴及びプライバシー保護機能を詳細に調べるための項目

オ 越境移転

越境移転（GDPR 第 44 条）との関係においては、2021 年にシュレムス II 判決[36]を受けて改正された標準契約条項（Standard Contractual Clauses (SCC)）[37]は、「データ輸入者及び個人データを移転中のデータ輸出者は、偶発的又は違法な破壊、紛失、改ざん、不正な開示又はアクセス（以下「個人データ侵害」という。）につながるセキュリティ違反に対する保護を含む、個人データのセキュリティを確保するための適切な技術的及び組織的措置を実施するものとする」（同第 8.5 項第 a 号）ものとしており、PETs 採用の有無や採用する PETs の種類が問題になる可能性があると考えられる。

また、EDPB 勧告は、PETs 自体には言及していないものの、個人データを越境移転させる場合に、データ輸出者及び輸入者は技術的措置を含む補完的措置の実施を検討するべきとしている。有効な技術的措置のシナリオをいくつか説明しており、例えば、秘密計算の実装により、識別可能なデータが開示されることを設計上防ぐことができるとしている。そのため、秘密計算の実装により、適法に個人データを越境移転させることができる可能性がある。

3 各種ガイドライン

（3）プライバシー強化技術についてデータ保護機関等の公的機関が公表するガイドライン等（個人情報保護法等と当該技術の関係についてのガイドライン等）の名称と主な論点。

[36] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd & Maximillian Schrems, ECLI:EU:C:2020:559 (Jul. 2020), https://curia.europa.eu/juris/document/document.jsf;jsessionid=BD731F5130B963C7072D2F6851E77B5E?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=11046615

[37] European Comission, *Standard contractual clauses for international transfers* https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en

(1) EDPB 等によるもの

ア　2007 年 EC メモ

第 2・1・(1)・イ・(ｲ)において、PETs の一例として記載したとおり、2007 年 EC メモは、PETs は、個人データの収集・使用を最小限に抑え、データ保護規則の遵守を促進するような方法で、情報通信システム及びサービスを設計するのに役立つものとしている。また、第 2・1・(2)・イ・(ｱ)で前述のとおり、PETs の具体例として、一定期間経過後の自動的な匿名化（Automatic anonymisation after a certain lapse of time）、暗号化ツール（Encryption tools）、クッキーカッター（Cookie-cutters）、プライバシー・プリファレンスのためのプラットフォーム（The Platform for Privacy Preferences (P3P)）を紹介している。

イ　2014 年 29 条作業部会匿名化意見書

第 2・1・(2)・イ・(ｲ)で前述のとおり、2014 年 29 条作業部会匿名化意見書は、匿名化技術として、ランダム化（randomization）及び一般化（generalization）の 2 つに整理している。ランダム化の例としては、ノイズ付加（noise addition）、置換（permutation）、差分プライバシー（differential privacy）を、一般化の例としては集積と k-匿名化(aggregation and k-anonymity)と L-多様性（L-diversity）/T-近似性（T-closeness）を挙げている。

ウ　2019 年 SODA レポート

第 2・1・(2)・イ・(ｳ)で前述のとおり、秘密計算（Secure Multi-Party Computation）に言及し、データ主体を合理的に特定できない方法で匿名化データを作成することで、計算による匿名化の要件を満たす可能性があると指摘している。

エ　2020 年 EDPB 第 25 条ガイドライン

2020 年 EDPB 第 25 条ガイドラインは、「デザインによるデータ保護／デフォルトによるデータ保護」に関するガイドラインであり、管理者及び処理者が、考慮すべきデザインの要素とデフォルトの要素を更に詳しく説明している。また、第 2・2・(3)・イで前述のとおり、PETs にも言及しており、PETs に最先端の成熟度に達した PETs は、リスクベースのアプローチにおいて適切であれば、「デザインによるデータ保護」の原則及び「デフォルトによるデータ保護」の要件に従った措置として採用することができるとしている。

オ　2021 年 EDPB 勧告

2021 年 EDPB 勧告は、個人データの越境移転の際に、データ輸出者が第三国を評価し、必要で適切な補足措置を見極めるという複雑な作業を支援するために、EDPB で採択されたものである。また、第 2・1・(2)・イ・(ウ)で前述のとおり、データ輸出者が、異なる管轄区域にある 2 つ以上の独立した処理者に、個人データを共同処理することを希望する場合、データ輸出者において、秘密計算によりデータの内容が開示されないように処理することで、データの越境移転ができる可能性があることを示唆している。

(2) ENISA によるもの

ア 2015 年 ENISA 報告書

2015 年 ENISA 報告書は、様々な成熟度の技術構成要素の一覧を提供することにより、法的枠組みと利用可能な技術的実装手段との間のギャップを埋めることに貢献することを目指すものである。また、第 2・1・(1)・イ・(ア)で前述のとおり、PETs の定義も示しており、情報システムの機能を損なうことなく、個人データを削除又は削減し、あるいは個人データの不必要又は望ましくない処理を防止することによって、プライバシーを保護する情報通信技術（ICT）対策の一貫したシステムとしている。

イ 2016 年 ENISA 報告書

2016 年 ENISA 報告書は、異なる PETs を、その成熟度、すなわち技術の準備状況や提供されるプライバシー概念に関する品質に関して比較できるようにするための方法論を開発することを目的とし、評価尺度の根拠となる専門家の意見と測定可能な指標を収集するための方法論を概説している。また、第 2・1・(1)・イ・(イ)で前述のとおり、PETs は、ソフトウェアとハードウェアのソリューション、すなわち特定のプライバシー又はデータ保護機能を達成するため、あるいは個人又は複数の自然人で構成されるグループのプライバシーリスクから保護するための技術的プロセス、方法、知識を包含するシステムを含む、プライバシー又はデータ保護機能をサポートする、あらゆる種類の技術を包含するとしている。

ウ 2019 年 ENISA レポジトリ

第 2・1・(4)・アで前述のとおり、ENISA は 2019 年 ENISA レポジトリ[38]を公表している。その中で、プライバシーを向上させる様々な方法、ツール、技術に関する知識は明らかに入手可能であるにもかかわらず、最も適切なものを選択することは困難であるとし、プライバシー強化技術（Privacy Enhancing Technologies: PETs）の知識の標準化と

[38] ENISA, 前掲注 27

一元化のため、ENISA は 2016 年に PETs 成熟度評価オンラインレポジトリというウェブアプリケーションプロトタイプの開発プロジェクトを開始したとしている。

PETs 成熟度評価オンラインレポジトリでは、(a)「技術準備度」（technology readiness）と(b)「プライバシー強化品質」（privacy enhancement quality）の 2 つの尺度から算出される結果を「PETs 成熟度」とするものとされ、その評価は、2019 年 ENISA レポジトリの専門家委員会のメンバーとして活動する専門家から選定されることが想定されている。

コミュニケーション戦略、技術的な実装、全体的なアプローチ等、いくつかの理由から、PETs 成熟度評価オンラインレポジトリの更新頻度が低いことにも言及しつつ、当該プロジェクト期間中に得られたフィードバックとして以下を紹介している。

- ネットワーク効果の原則を考慮すると、この PETs 成熟度評価オンラインレポジトリの利用者が増加するためには長期間を要する。そのため、当該プロジェクトとは異なる枠組み（例えば、その分野の特定の専門家の直接関与を得る等）を使って、コミュニティの形成を進めるべきである。
- ユーザーからは、PETs 成熟度評価オンラインレポジトリのブランディングを明確にすることで、ソフト面の信頼要素が向上するというフィードバックが得られた。また、このフィードバックは、PETs 成熟度評価オンラインレポジトリの所有者となる事業者を明確にするか、PETs 成熟度評価オンラインレポジトリを ENISA のコーポレートアイデンティティに統合するべきであることを示している。
- ユーザーからは、デザインやその他の技術的側面もプラットフォームの普及に影響を与えた可能性があるというフィードバックが得られた。このフィードバックは、技術的な実装と保守に更に力を入れるべきであることを示している。

エ　2021 年 ENISA 報告書

第 2・1・(2)・イ・(ウ)で前述のとおり、2021 年 ENISA 報告書は、匿名化及び仮名化技術として、k-匿名化と差分プライバシーを説明されてしている。これらの技術のいくつかを使用した医療分野の事例において、仮名化の可能性や、データ管理モデルの適用可能性を検討している。また、万能な仮名化技術は存在せず、最良の選択をするためには、直面した事例に対する詳細な分析が必要であるとしており、そのために、データの仮名化を行う前に、全体像を批判的に検討することが不可欠であるとしている。

オ　2022 年 ENISA 報告書

2022 年 ENISA 報告書は、データの共有、処理、保存のための新しい技術の出現により、管理と透明性の欠如、データの再利用可能性、データの再識別、プロファイリング、自動化された意思決定等、新しい脅威と課題がもたらされたとしている。そして、データ保護の技術的側面をデザイン及びデフォルトで実践する実務家や組織を支援することを目的として、データ保護エンジニアリングを幅広く検討している。そして、そのために、第 2・1・(2)・イ・(ｴ)で前述したような既存のセキュリティ技術と技法を紹介している。

また、第 2・5 で後述するように、報告書内で検討された分析結果に基づき規制当局や学界に対して提言を行っている。

(3) AEPD によるもの

ア　2019 年 AEPD ガイド

第 2・1・(2)・ア・(ｲ)で前述のとおり、2019 年 AEPD ガイドは、PETs の分類を整理しており、①プライバシー保護として、擬似匿名化ツール、匿名化製品・サービス、暗号化ツール、フィルタ及びブロッカー、アンチトラッカーを、②プライバシーマネジメントとして、情報ツール、管理ツールを分類している。

イ　2021 年 AEPD ペーパー

2021 年 AEPD ペーパーは、匿名化データは、医学、人口統計学、マーケティング、経済、統計学、その他多くの分野の研究の文脈で重要な役割を果たし、関心を高めているとしつつも、同時に関連する誤解も広まっているとしている。そして、第 2・2・(3)・ア・(ｱ)で前述したような、匿名化に関する誤解を 10 件紹介することとで、匿名化についての理解を深め、技術に関する主張をそのまま受け入れるのではなく、確認するよう動機付けている。

4　その他の法令の規定

（4）その他、プライバシー強化技術が普及していく上で、論点となりうる法令の規定（個人情報、プライバシー、データ保護を目的とする規定、データの越境移転を伴う場合の規定）の概要。

欧州委員会は、2023 年 1 月に、欧州における人口及び住居に関する統計規則（Regulation of the European Parliament and of the Council on European statistics on population

and housing）を改正する提案（以下「**欧州人口住居統計規則案**」という。）を提出している[39]。

欧州人口住居統計規則案は、EU の個人データ保護法に完全に沿ったデータ共有を実施するために PETs の採用を明示的に支持するとともに、データ共有を可能にする法的基盤を強化し、革新的なソリューションの開発を奨励するものである。また、機密データ（confidential data[40]）又は個人データのデータ共有が許容され、かつ、任意に実施するために備えることが望ましい条件のひとつとして、第 2・2・(1)・アで述べた GDPR における 7 つのデータ保護の原則（特に、②目的限定の原則、③データ最小化の原則、⑤保管の限定の原則、⑥完全性（integrity）及び機密性の原則（安全性の原則）が挙げられている）を実現するために特別に設計された PETs に基づくことを挙げている（第 13 条第 3 項(b)）。

また、OECD が、2023 年 3 月 8 日に公表した報告書「PETs の動向-現在の規制と政策アプローチ-」（Emerging privacy-enhancing technologies - Current regulatory and policy approaches-）[41]によれば、第 3・1・(2)等において後述するゼロ知識証明（ZKP）が、欧州連合が提案する、域内市場における電子取引の電子識別と信用サービスに関する規則(eIDAS 規則)[42]の一部として計画している、将来の欧州デジタル ID ウォレットを支える重要な技術の 1 つとして認識されていることが示唆されている。

5　その他（政策、世論の動向等、関連事項で有用と考えられる事項）

EDPB 勧告[43]に関して実施されたパブリックコンサルテーションに対するコメント[44]において、秘密計算（Secure Multi-Party Computation）を使用することで、個人データは

---

[39] Proposal for a Regulation of the European Parliament and of the Council on European statistics on population and housing, amending Regulation (EC) No 862/2007 and repealing Regulations (EC) No 763/2008 and (EU) No 1260/2013, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023PC0031

[40] 機密データ（confidential data）とは、直接的又は間接的に統計単位を識別することができ、それによって個人情報が開示されるデータをいうとされている。Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities, https://eur-lex.europa.eu/eli/reg/2009/223/oj の第 3 条第 7 号参照。

[41] OECD, *Emerging privacy-enhancing technologies Current regulatory and policy approaches*, (Mar, 2023), https://www.oecd-ilibrary.org/science-and-technology/emerging-privacy-enhancing-technologies_bf121be4-en;jsessionid=_mg5ApqVrcP0zmEP7MbQxNlWo0CfxsRvTb90IbrW.ip-10-240-5-62, 17 頁

[42] Proposal for a Regulation of The European Parliament and of The Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2021%3A281%3AFIN

[43] EDPB, 前掲注 17

[44] Inpher, Inc., *Public Consultation, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Comments of Inpher, Inc.,*

ランダムな補助番号に変換され、各計算フェーズ後に削除されるため、傍受や再識別が事実上不可能となり安全にデータを移転させることができること、データの最小化、厳格な目的制限が実現されるため GDPR 第 25 条に基づくデザインによるデータ保護の基準を具現化することができることを強調するものがある。

また、ENISA は 2022 年 ENISA 報告書[45]において、以下の提言を行っている。

- 学界は、政策指導や研究資金提供の面での EU の各機関の支援を受けて、データ保護原則の実践を支援できるセキュリティ技術や手法の展開を模索し続けるべきである。
- 規制当局（データ保護当局や EDPB 等）、欧州委員会、及び、EU の関連機関は、前述の技術や手法の利点を普及させ、その適用と展開に関するガイダンスを提供するべきである。
- IPEN（Internet Privacy Engineering Network）[46]のような技術者支援を目的としたイニシアチブは、実務家、研究者、アカデミアによって更に支援されるべきである。
- データ保護当局や EDPB 等の規制当局は、関連する技術や手法の最先端のソリューションに関連して、EU 全域でグッドプラクティスを議論し、促進する必要がある。
- 規制当局及び欧州委員会は、データ保護の適切なエンジニアリングを確保するために、GDPR 第 42 条に基づき、関連する認証制度の設立を促進すべきである。

6　調査対象国・法域における PETs の利用に関する調査結果

本調査の結果明らかとなった対象国・法域における PETs の利用に関する調査結果は次のとおりである。

調査項目	調査結果
個人情報（personal date）を暗号化（秘密分散を含む。以下同じ。）した場合に個人情報以外の情報分類への変更	• 暗号化により、データ主体の識別可能性がなくなった場合には、当該データは匿名化データに変更され、GDPR は適用されない。識別可能性の理解には争いがある（データ管理者における現実的な識別可能性で足りるのか、絶対的な識別可能性まで要求される

（https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/inpher-_edpb_supplementary_measures_comment.pdf 2 頁

[45] ENISA, 前掲注 4

[46] https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en

調査項目	調査結果
の有無	のか）ものの、GDPR においては、取扱いの時点において利用可能な技術及び技術の発展を考慮に入れた上で、識別のために要する費用及び時間量のような、全ての客観的な要素を考慮した、管理者又はそれ以外の者によって用いられる合理的な可能性とされている（GDPR 前文第 26 項）。 • 追加情報により識別できる程度である場合、仮名化データに変更される可能性がある。もっとも、仮名化データの情報分類は個人データのままである。
個人情報を暗号化することにより、軽減される義務・恩恵	• 暗号化により匿名化データに変更された場合、GDPR は適用されない。 • 匿名化データに変更されない場合でも、「デザインによるデータ保護／デフォルトによるデータ保護」の規定（GDPR 第 25 条）、取扱いの安全性の規定（GDPR 第 32 条）上、管理者に要求される適切な技術的措置を講じていると認める、ひとつの要素となる可能性がある。 • 暗号化により、識別可能なデータが開示されることを設計上防ぐことができる場合、適法に個人データを越境移転させることができる可能性がある。 • ただし、EDPS へのインタビューによれば、GDPR はリスクベースのアプローチを採用し、何ら技術的な要件を課しておらず、その結果として GDPR における法的義務を軽減する技術的要件は存在しないとのことである。
個人情報を用いて二者以上が有する個人情報について秘密計算を行うための要件･手続と法律上の規制の有無	処理の性質に応じてデータ管理者又はデータ処理者に要求される要件・手続・規制が適用される。
二者以上がデータを提供してデータ分析事業者が関わる場合のそれぞれの法律上の関係性	同上

調査項目	調査結果
個人情報を匿名化/仮名化することにより、軽減される義務・恩恵	• 個人情報を匿名化した場合、GDPR は適用されず、GDPR 上の義務を負わない。 • 個人情報を仮名化した場合、「デザインによるデータ保護／デフォルトによるデータ保護」の規定（GDPR 第 25 条）、取扱いの安全性の規定（GDPR 第 32 条）上、管理者に要求されている適切な技術的措置を講じていると認める、ひとつの要素となる可能性がある。また、適法に越境移転することができる要件を満たす可能性がある。
義務軽減・恩恵のために、匿名化/仮名化以外の要件（ある場合）。	特に見当たらない。
プライバシー強化技術を用いることによる個人情報保護法等上の法的なメリット（義務の軽減、恩恵等）	「デザインによるデータ保護／デフォルトによるデータ保護」の規定（GDPR 第 25 条）、取扱いの安全性の規定（GDPR 第 32 条）上、管理者に要求されている適切な技術的措置を講じていると認める、ひとつの要素となる可能性がある。また、適法に越境移転することができる要件を満たす可能性がある。

第3　英国

1　プライバシー強化技術（PETs）の名称・技術の概要

（1）調査対象国において、個人データを保護したままで分析等を行うプライバシー強化技術として注目あるいは実用化されている名称と技術の概要。

(1) PETs の定義

ア　関連法令の定め

英国においては PETs の利用に関する特別の法令は存在せず、また、英国の UK GDPR[47] 及び「2018 年データ保護法（Data Protection Act 2018）」（以下「**DPA 2018**」という。）は、PETs の定義規定を設けていない。

イ　ICO による定義

英国のデータ保護機関である英国情報コミッショナーオフィス（Information Commissioner's Office）（以下「**ICO**」という。）も、PETs について、次のとおり、画一的な定義を用いていない。

例えば、ICO のウェブサイトでは、PETs は「個人データの使用を最小限に留めつつ、データの安全性を最大化することによって基本的なデータ保護原則を具体化する技術」と説明されている [48]。

また、ICO が 2022 年 9 月に公表した「匿名化、仮名化及びプライバシー強化技術に関するガイダンス草案（Draft anonymization, pseudonymisation and privacy enhancing technologies guidance」（以下「**2022 年 ICO ガイドライン草案**」という。）の第 5 章「プライバシー強化技術（Privacy-enhancing technologies： PETs」（以下「**2022 年 PETs ガ**

[47] 英国では、2020 年 1 月 31 日に同国が EU を離脱したことに伴い GDPR が国内法となっている。以下「UK GDPR」という。

[48] ICO, *Data protection by design and default*', (last visited Mar 8, 2023), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

イドライン草案」という。）[49] [50]では、ENISA による次の定義が PETs の「有益な定義」として紹介されている[51]。

> ソフトウェアとハードウェアのソリューション、すなわち特定のプライバシー又はデータ保護機能を達成するため、あるいは個人又は複数の自然人で構成されるグループのプライバシーリスクから保護するための技術的プロセス、方法、知識を包含するシステム

ウ　CDEI による定義

科学・イノベーション・テクノロジー省に属する独立した諮問機関である「データ倫理及びイノベーションのためのセンター（The Centre for Data Ethics and Innovation: CDEI)」が 2021 年 7 月に公表した「プライバシー促進技術の導入ガイド」[52]（以下「**2021 年 CDEI 導入ガイド**」という。）では、PETs は、「プライバシー又はセンシティブ情報の機密性を保護するあらゆる技術的方法」と広義に定義されている[53]。この定義による場合には、PETs には、広告ブロックブラウザ拡張から匿名コミュニケーションのための Tor ネットワークまでが広範に含まれることになる。

第 2・1・(1)・イ・(イ)で前述したとおり、ENISA は、2015 年 ENISA 報告書で用いていた PETs の定義を 2016 年 ENISA 報告書で、データ保護原則に言及しない、より広範な定義で置き換えている。そのため、2022 年 ICO ガイドライン草案であえて 2016ENISA 報告書と同様の定義が用いられていることや、CDEI において広義に定義されていることを踏まえると、英国では、EU と同様に PETs は広範な技術を含むものとして理解が進む可能性がある。

(2) PETs の種類

2022 年 PETs ガイドライン草案によれば、主要な PETs として以下のものがある（詳細は別紙を参照）。なお、ICO は、これらは既存の PETs の例を挙げているにとどまり、これらのうちのある特定の PETs を ICO が支持する趣旨ではないとしている。

---

[49] ICO, *Chapter 5: Privacy-enhancing technologies (PPETs) – Draft anonymization, pseudonymisation and privacy enhancing technologies guidance*, (Sep, 2022), https://ico.org.uk/media/about-the-ico/consultations/4021464/chapter-5-anonymisation-pets.pdf

[50] 2022 年 ICO ガイドライン草案は、第 5 章の「PETs に関する ICO ガイドライン草案」（2022 年 PETs ガイドライン草案）の他に、「匿名化の紹介」（第 1 章）、「匿名化を効果的なものとするための方法」（第 2 章）、「仮名化」（第 3 章）及び「アカウンタビリティとガバナンス」（第 4 章）の各章が存在する。第 2 章と第 3 章については後述する。

[51] ICO, 前掲注 48

[52] CDEI, *Privacy Enhancing Technologies Adoption Guide (BETA version)*, (last visited Mar 8, 2023), https://cdeiuk.github.io/pets-adoption-guide/adoption-guide

[53] CDEI, 前掲注 52 の*'Background'* の *What are PETs?*, (last visited Mar 8, 2023), https://cdeiuk.github.io/pets-adoption-guide/what-are-pets

準同型暗号（Homomorphic encryption (HE)）	暗号化されたデータを解読することなく、暗号化されたデータのまま計算を実行することができる技術をいう。HE には、①完全な準同型暗号（FHE）、②相当程度の準同型暗号（SHE）、③部分的な準同型暗号（PHE）の 3 種類がある。HE は、大規模に利用することには不向きである。
秘密計算（Secure multiparty computation (SMPC)）	異なる当事者が、データを他の当事者と共有することなく、組み合わせたデータを共同で処理することのできるプロトコール（コンピュータ間でデータを送るための一連の規則）をいう。秘密を分割して各関係者に分配し、処理の内容やプロトコールの設定によって、全部又は一部の関係者に結果を知らせることができる。
秘匿共通集合演算（Private set intersection (PSI)）	SMPC の一種であり、各当事者が独自のデータセットを持ち、それらのデータセットを公開・共有することなく、二つのデータセットが共通する要素のみを求めることができる計算方法をいう。例えば、クライアントのみが PSI の結果を知っており、サーバーホストは PSI サービスを管理し、クライアントの問い合わせに対応できるようにするクライアント・サーバー型が一般的な手法である。
連合学習（Federated learning (FL)）	複数の異なる当事者がそれぞれのデータを用いて AI に学習させる技術をいう。AI が識別したいくつかのパターンを組み合わせて、単一のより正確なモデルを作成する。その際、学習データを当事者で共有する必要はない。FL には、①集中設計と②分散設計の 2 つのアプローチがある。
信頼できる実行環境（Trusted execution environments (TEE）)	コンピューターデバイスの中央処理装置 (CPU) 内の安全な領域をいう。TEE は、システムの他の部分から分離された方法で、コードの実行とデータへのアクセスを可能にする。
ゼロ知識証明（Zero-knowledge proofs (ZKP)）	証明者が検証者には知られていない秘密を保有している旨を検証者に証明することができるプロトコールをいう。
差分プライバシー（Differential privacy）	ある計算の出力が個人に関する情報をどの程度明らかにするかを測定する方法をいい、「ノイズ」をランダムに注入するものである。ノイズとは、データセット内のデータをランダムに

	変更することで、個人を識別しにくくするものをいう。差分プライバシーには、①集計時にノイズを加える「グローバル差分プライバシー」と、②1 各ユーザーが集計前に個々のレコードにノイズを追加する「ローカル差分プライバシー」の 2 つの種類がある。
合成データ（Synthetic data）	データ合成アルゴリズムによって生成された人工的なデータで、実データのパターンや統計的特性を再現するものをいう。合成データは、大規模なデータセットにアクセスできない環境において、AI モデルを学習させるための有効なツールとなり得る。合成データには、①元データの一部の変数だけを合成した「部分合成データ」と、②全ての変数を合成した「完全合成データ」の 2 種類がある。

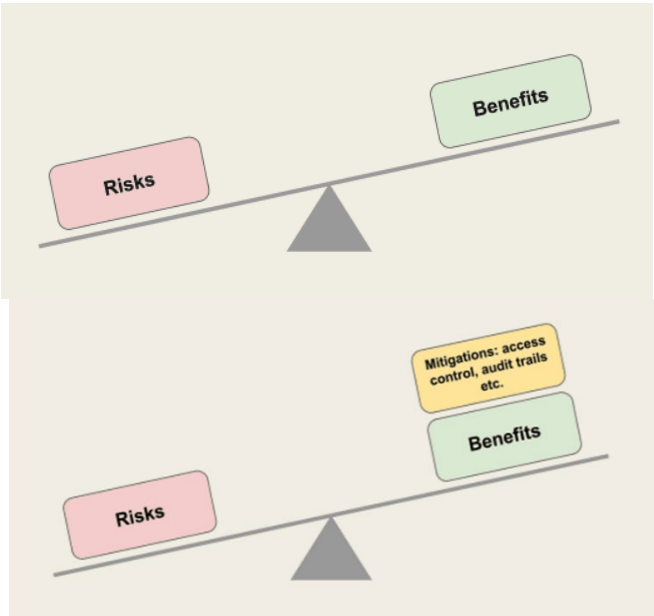
2022 年 PETs ガイドライン草案は、前述の PETs を機能の観点から次のとおり整理している。

機能	説明	PETs の例
処理を行っているデータに関係する個人の識別可能性を低減するもの	元の個人データに含まれる個人とデータとの間の関連性を切断ないし弱化させることを目的とする。これにより、データ最小化の原則の達成に資する。ただし、取扱いの種類によっては、個人の識別性が低減されたデータでは十分な有用性がなく、取扱いの目的に対して不適合となる場合が生じ得る。	• 差分プライバシー • 合成データ
データの隠蔽及び遮蔽に焦点を当てるもの	個人の識別可能性を低減する PETs とは異なり、データの有用性や正確性に影響を与えることなく、個人のプライバシーを保護することを目的とするものである。これにより、データの安全性の原則の達成に資する。	• 準同型暗号 • ゼロ知識証明
個人データへのアクセスを分割又はコントロールするもの	データの有用性及び正確性に影響を与えることなく、共有される個人データの量を最小化し、完全性と機密性を確保することを目的とするものである。個人データの取	• 信頼できる実行環境 • 秘密計算

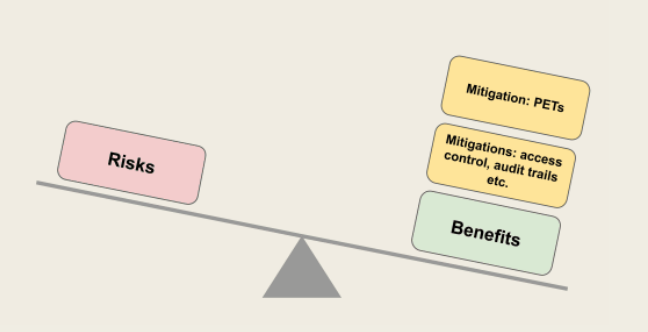
	扱い、管理、保管のためのシステムやデータ・アーキテクチャを用いる。これにより、データ処理の性質に応じて、データ最小化の原則とデータの安全性の原則の双方を達成することに資する。	• 秘匿共通集合演算 • 連合学習

(3) PETs 利用のインセンティブ

事業者は、個人の基本的権利であるプライバシーを保護する義務を負っているため、事業者が個人データを取り扱うおうとする際には、法的な懸念、倫理的な懸念、レピュテーションにおける懸念を考慮しなければならない。とりわけ、大規模な個人データを取り扱う場合や AI を用いた処理を行う場合には高度のリスクを伴う。そのために事業者がリスク回避的になって、社会にとって有益な方法でデータを利用することが阻害されている場合があり得る。この点で、事業者は、PETs を利用することにより、このようなリスクを管理し、低減させることができる。すなわち、PETs は、事業者にとってイノベーションを可能にするもの（enabler for innovation）として、価値あるデータ・シェアリングやデータの取り扱いにとって新たな機会を拓くものとなる[54]。



[54] もっとも、PETs は全ての状況において有益であるわけではない。例えば、PETs を利用することによって違法又は反倫理的な個人データの取り扱いが正当となるわけではない。



（2021 年 CDEI 導入ガイドより）

この点に関して、従来より、プライバシーを保護する形でのデータ利用は、匿名化（anonymisation）の方法によるものがよく知られている。匿名化によって、データセットの中から個人を特定可能な情報が除去され、データ主体は合理的な方法によっては再び特定されることはないから、UK GDPR は匿名化された個人データには適用されない。従って、匿名化されたデータはプライバシーリスクを生じさせないが、その一方でデータ利用の有用性は減少させられざるを得ない。他方、匿名化していないデータを利用すれば、データ利用の有用性は高くなるものの、プライバシーリスクが生じる。このように匿名化においてはプライバシーリスクとデータ利用の有用性が相反する関係にあるところ、PETs を利用すれば、プライバシーリスクを減少させつつ、データ利用の有用性を高めることができる。

法的な観点から言えば、PETs は、技術面において、データ保護に関する原則の遵守（data protection compliance）を実施する手段として位置付けられる。2022 年 PETs ガイドライン草案においても、PETs は「デザインによるデータ保護」と密接に関連するものと整理されており、PETs 利用の利点として、次の 2 点が挙げられている。なお、PETs の実際の有用性は、取扱い対象となるデータのセンシティビティの程度による。

- PETs の利用により、データ管理者が個人データを他者に共有することなく、あるいはデータ処理者が個人データに直接アクセスすることなく（すなわち、これらによって個人に対するリスクを低減しつつ）、個人データのさらなる分析を行うことが可能となる。このようにして個人データを共有し、相互にリンクさせ、又は分析を行うことで、データ保護の原則を遵守しながら、個人データから貴重な洞察を獲得することが期待できる。
- PETs を使用すれば、データセットの中にある個人データのプライバシーを侵害することなく、データセットから洞察を得ることができる。適切な PETs を利用すれば、通常であればセンシティブ情報であるために共有することが許されないデータセットにアクセスすることが可能となる。

（4）PETs 利用の障壁

2022 年 PETs ガイドライン草案では、PETs は、個人に対する侵害のリスクを低減することに役立つものの、データ保護原則の要件を全て満たすための「万能薬」とみなされるべきではないことが強調されている。すなわち、PETs を利用する場合であっても、データ処理は、適法、公正かつ透明でなければならない。そのため、PETs の利用を検討するに先立ち、意思決定プロセスの影響、データ処理の目的の特定（正当な処理目的の特定）、及び正確性とアカウンタビリティの両要件をどのように遵守できるかを評価することが必要である。

PETs の利用にあたっては、とりわけ以下の各点に留意する必要があるとされている。

成熟度の欠如	PETs の中には、拡張性、標準の利用可能性、攻撃に対する堅牢性の点で十分に成熟しているとは言えないものが存在する。従って、これらの点について十分に成熟した PETs を利用すべきである。PETs の成熟性を評価するにあたって考慮すべき要素については後述する。
専門知識の欠如	PETs を設定し、適切に使用するためには、高度な専門知識を必要とする場合がある。専門知識が不十分な場合、PETs の実装に誤りが生じたり、プライバシー保護とデータ利用の実用性の適切なバランスを実現できないおそれがある。従って、必要な専門知識を欠いている場合には、適切なレベルのサポートを提供する製品又はサービスの利用を検討する必要がある。
実装における過誤	PETs を実装することが理論上可能であるとしても、それが実際にそのとおりに適用されるか否かは別問題である。理論とおりに実装がなされなかった結果、個人の権利や自由に対するリスクが生じることが起こり得る。従って、攻撃や脆弱性は定期的に監視されなければならない。 また、適切な組織的措置が欠如している場合には、PETs の本来の効果を低下させ、あるいは完全に損なわせるおそれがある。従って、信頼できるデータ処理を実現するためには、契約上の管理等の法的義務を明確にし、監視及び監査プロセスを含む組織的管理を講じた上で、サイバー攻撃やデータ管理の

	脆弱性の有無を定期的に監視し、適切な措置を講じることができる態勢を整備しておくことが必要となる。

前述のうち、PETs の成熟性の判断基準に関して、2022 年 PETs ガイドラインは次のとおり説明している。

すなわち、前述したとおり、PETs にも様々な種類があり、その成熟度も多様である。PETs を利用する場合には、成熟した PETs を利用すべきである。PETs の成熟度を決定する方法もいくつか存在するが、一般的なアプローチは「技術成熟度（Technology Readiness Levels）」である。これは、観念上のものから市場化がなされているものまで、成熟度に応じて PETs を異なるカテゴリーに分類するものである。

PETs の適切性を評価するその他のアプローチとして、①PETs が提供する保護、②利用される脅威モデルにとっての個人データ漏洩のリスク、③拡張可能性（scalability）及び複雑性の問題に、より焦点を当てて成熟性を判断するものもある。

理論上のものにとどまった未成熟な PETs を実装することは困難である。従って、（PETs の標準化は未だ初期段階にあるものの）標準（standards）が存在する場合には、データ保護措置の設計と実装において当該標準を考慮に入れるべきである。例えば、標準 [55]を参照することにより、以下の点について更なる詳細や指針を得ることができる。

- 特定の攻撃とそれに対する軽減のための方法
- 特定の脅威モデルに必要な技術的及び組織的措置（例えば、契約上の管理及びアクセスコントロール等のセキュリティ対策）
- セキュリティ特性を確実に保持するために必要な技術的及び組織的措置（暗号鍵の管理、セキュリティパラメータ等）

ここでいう「標準」は、抽象的な基準が存在するわけではなく、その PETs が、どの産業セクターにおいて、どのように用いられるかによって変わるものである。データ処理のサイクルの全ての段階において必要な保護がなされるよう、複数の技術を組み合わせることが必要となる場合もあり得る。

2　データ保護法との関係、データ保護法上の論点

[55] 2022 年 PETs ガイドライン草案の 36 頁以下では、PETs の業界標準の利用可能性に関する参照表が掲載されている。同表では、PETs の使用例ごとに、①標準が利用可能性であるか（利用可能である場合は、その標準の内容）、②知られている制約（弱点）が示されている。

（2）上記において、個人情報、プライバシー保護に関する法律（以下「個人情報保護法等」という。）の観点から論点となっている点（過去論点となった点、事業者による改正要望、政府による改正予定の点も含む。）。

（1）英国データ保護法の概要

英国では、2020 年 1 月 31 日に EU を離脱したことに伴い、同年 12 月 31 日時点で適用されていた GDPR を含む EU 法は国内法となっている（UK GDPR）。UK GDPR は、英国における個人データの処理に関して、重要な原則及び権利・義務を定めている。

また、DPA 2018 は、UK GDPR を補完し調整する形で英国のデータ保護制度の枠組みを定めた一般法であり、UK GDPR が適用されない法執行又は諜報目的に関する国内実施法部分を含むものとなっている[56]（以下、UK GDPR と DPA 2018 とを併せて「**英国データ保護法**」という。）。

（2）PETs と英国データ保護法との関係[57]

英国データ保護法は、英国におけるデータ保護の原則として、①適法性、公正性及び透明性の原則、②目的の限定の原則、③データ最小化の原則、④正確性の原則、⑤保管の限定の原則、⑥完全性（integrity）及び機密性の原則（安全性の原則）、⑦アカウンタビリティの原則の 7 つの原則を規定しており（UK GDPR 第 5 条第 1 項）、これらの原則が個人データの処理の方法の中心に置かれるべきものとされている。PETs は、これらのデータ保護の原則を効果的に実施し、データ処理において必要なセーフガードを組み込むことに資する。英国データ保護法上の PETs に関連しうる主な規定は以下のとおりである。

匿名化 **（前文第 26 項）**	匿名化情報とは、「匿名の情報、すなわち特定の若しくは特定可能な自然人に関連しない情報、又はデータ主体が特定されない若しくは特定される可能性のない方法で匿名化された個人データ」をいう。匿名化情報は個人データではないため、これを取り扱う場合でも UK GDPR は適用されない。

[56] DPA 2018 は、1998 年データ保護法を更新するもので、2018 年に発効した。英国の EU 離脱を受けて 2021 年 1 月 1 日に改正がなされた。

[57] PETs と最も関係性を有するのは英国データ保護法であるが、この他にも、ICO が所管する環境情報規則（Environmental Information Regulations)、情報自由法（Freedom of Information Act)、電子識別・認証及び信頼サービス規則（Electronic identification and trust services)、及びプライバシー及び電子通信に関する規則（Privacy and Electronic Communications Regulations)など、PETs と一定の関連性を有する法令が存在する。

仮名化 **（第 4 条第 5 号）**	「仮名化」とは、個人の特定につながる追加情報とは別途保管され、かつ技術的及び組織的措置によって、追加情報なしでは個人を特定できないような方法で個人データを処理することをいう。匿名化とは異なり、追加情報と組み合わせることで自然人の特定が可能になることから、仮名化された情報は、「個人データ」に該当し、UK GDPR の規制が適用される。仮名化によって、データ主体の特定が困難になるため、データ主体のリスクは緩和される。
適切な技術的・組織的な対策を実施する処理者を利用する義務（第 28 条）	管理者が個人データの処理に際して処理者を利用する場合、管理者は、当該処理が UK GDPR に定める義務に適合するような態様で適切な技術的・組織的な対策を実施することについて十分な保証を提供する処理者のみを利用することができる（第 28 条第 1 項）
「デザインによるデータ保護」及び「デフォルトによるデータ保護」 **（第 25 条）**	管理者は、UK GDPR の要件に適合するものとし、かつ、データ主体の権利を保護するため、処理の方法を決定する時点及び処理それ自体の時点の両時点において、データの最小化のようなデータ保護の基本原則を効果的な態様で実装し、その処理の中に必要な保護措置を統合するためにデザインされた、仮名化のような、適切な技術的措置及び組織的措置を実装しなければならない。また、管理者は、その処理の個々の特定の目的にために必要な個人データのみが処理されることを、デフォルトで確保するための適切な技術的措置及び組織的措置を実装しなければならない。
取扱いの安全性 **（第 32 条）**	管理者及び処理者は、「適切な技術的及び組織的措置」によって個人データを安全に処理することが必要であり（セキュリティの原則）、このためには、リスク分析、組織的ポリシー物理的・技術的対策等を検討する必要がある。どのような対策を講じるかを決定する際には、最新の技術や導入コストを考慮することができるが、それらは管理者の状況と処理が引き起こすリスクの両方に適したものである必要がある。適切な場合には、仮名化や暗号化等の手段の使用を検討する必要がある。
データ保護影響評価 **（第 35 条）**	「データ保護影響評価（Data Protection Impact Assessment: DPIA）」とは、データ処理の前に実施される個人データ保護に関する影響評価を意味し、処理が個人の権利及び自由に対

	して高度のリスクをもたらす可能性がある場合に、管理者が実施することが義務付けられている。リスクのレベルを評価するには、個人への影響の可能性と入内性の両方を考慮する必要がある。
越境移転（第 44 条）	UK GDPR 上、英国国外の国や国際組織への個人データの移転を原則として禁止されている（第 44 条）が、英国政府が、独自の権限により、十分なデータ保護の水準を確保しているとの認定（十分性認定）を行った国、地域又は国際機関へのデータ移転の場合（第 45 条第 1 項）や、標準データ保護条項（Standard Data Protection Clauses: SDPC）に基づく移転の場合（第 46 条第 2 項(c)）、拘束的企業準則（Binding Corporate Rules: BCR）による移転の場合（第 46 条第 2 項(b)、第 47 条）、データ主体による同意による移転の場合（第 49 条第 1 項(a)）等には、個人データの越境移転が例外的に許容される。

(3) PETs に関わる英国データ保護法上の論点

ア　匿名化

PETs と類似する概念として「匿名化技術（anonymisation techniques）」がある。匿名化された個人データには UK GDPR は適用されない。全ての PETs が効果的な匿名化をもたらすわけではなく、また、PETs を利用することなく匿名化を達成することもできる（匿名化技術の全てが PETs に該当するわけではない。）。そのため、2022 年 PETs ガイドライン草案においては、PETs と匿名化技術は相互に関連しているものの（例えば、差分プライバシーを設定することによって、特定の個人に関する情報を明らかにすることを回避することができる。）、異なる概念であるとされている。

なお、匿名化（anonymisation）に類似するものとして暗号化（encryption）がある。暗号化の場合には、復号鍵を保有していればデータセットを復号することによって個人を再特定することが可能であることから、この点において匿名化とは異なる。前述のとおり匿名化された個人情報には UK GDPR は適用されないのに対して、暗号化された個人データは依然として個人データであることから、UK GDPR が適用される [58]。

イ　デザインによるデータ保護/デフォルトによるデータ保護

[58] ICO, *What is encryption?*, (last visited Mar 8, 2023), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/what-is-encryption/

UK GDPR 第 25 条は、「デザインによるデータ保護」及び「デフォルトによるデータ保護」を規定している。同条によると、データ管理者は、UK GDPR の要件を充足し、かつ、データ主体の権利を保護するために、データ処理の方法を決定する時点及びその方法に基づいてデータ処理を実施する時点の両時点において、データ保護の基本原則を効果的な方法で実行し、その処理の中に必要な保護措置を統合するようデザインされた、適切な技術的措置及び組織的措置を実装しなければならない（UK GDPR 第 25 条第 1 項）。また、データ管理者は、個々の処理の特定の目的のために必要な個人データのみが処理されることを、デフォルトで確保するための適切な技術的措置及び組織的措置を実装しなければならない（UK GDFPR 第 25 条第 2 項）。

PETs を利用することにより、以下の各事項が可能となることを通じて、「デザインによるデータ保護」及び「デフォルトによるデータ保護」のアプローチを実行することができるとされている[59]。

- 目的のために必要なデータのみを処理することを確保することによって、データ最小化の原則を遵守すること
- 適切なレベルの安全性を提供すること
- 堅牢な匿名化又は仮名化ソリューションを実装すること（もっとも、全ての PETs が効果的な匿名化をもたらすわけではないし、また、PETs を用いることなく匿名化を達成することは可能である。）
- 個人データへのアクセスを許可されていない者が個人データを認識できないようにすることによって、個人データ侵害から生じるリスクを最小限にすること

ウ　取扱いの安全性

処理する個人データを保護するために実装する安全措置（技術的及び組織的措置）は、その処理によってもたらされるリスクに対して「適切な」レベルを有するものでなければならない（完全性及び機密性の原則、セキュリティの原則。UK GDPR 第 5 条第 1 項(f)）。何が「適切な」安全措置であるかは、それぞれの置かれている状況、処理の内容、もたらされるリスクの内容によって変わり得るため、その判断にあたっては、情報セキュリティリスクを評価した上で物理的・技術的対策を講じる必要がある。また、どのような措置を動じるかについて決定する際には、最新の技術や導入コストを考慮することも可能であるが、それらは管理者の状況と処理が引き起こすリスクの双方に適合したものである必要がある。この点で、ICO は、国家サイバーセキュリティセンター（National

[59] UK GDPR, Article 25 and Recital 78 (data protection by design and by default) and Articles 5(1)(f), 32 and Recital 83 (security)

Cyber Security Centre: NCSC）と協力して、管理者に適した対策を評価する際に使用できるアプローチを開発している。このアプローチは、①セキュリティリスクの管理、②サイバー攻撃からの個人データの保護、③セキュリティ事象の検知、④影響の最小化という 4 つの目的に基づくものとなっている [60]。

PETs を利用することによって、個人データの処理にあたって「適切な技術的及び組織的措置」を講じなければならないという原則（完全性及び機密性の原則）を遵守することに資する。

もっとも、2021 年 CDEI 導入ガイドでは、PETs は、それ単独で用いられるというよりは、適切なアクセスコントロールや監査証跡（オーディットトレイル）、情報ガバナンスの取り決めを含んだ、より広範なプライバシーデザインの一部として適用されるべきであることが指摘されている [61]。従って、「適切な技術的及び組織的措置」を講じるにあたっても、PETs の利用のみで足りるものではなく、他の対策を併せて講じることが求められるものと考えられる。

エ　越境移転

UK GDPR においては、個人データを英国及び英国による十分性認定（adequacy decision。UK GDPR 第 45 条）を受けている国以外の第三国に移転することは原則として禁止されている（UK GDPR 第 44 条）が、「適切な保護措置（appropriate safeguards）」（UK GDPR 第 46 条第 1 項）が提供されている場合には例外的に個人データを第三国に移転することが認められる。

この「適切な保護措置」のひとつとして、UK GDPR では「標準データ保護条項（standard data protection clause: SDPC）」が挙げられている（UK GDPR 第 46 条第 2 項(c)）。ICO は、2021 年 8 月、SDPC に該当するものとして、「国際データ移転契約書（International Data Transfer Agreement: IDTA）」[62]のドラフトを公表し、併せて、移転リスク評価（Transfer Risk Assessment: TRA）に関するガイダンス [63]のドラフトを公表した。これらの契約書及びガイダンスはシュルムス II 判決に対応するものであって、パブリックコンサルテーションを経た後に英国議会に提出され、2022 年 3 月 21 日に発効した。これにより、

---

[60] ICO, *Security outcomes*, (last visited Mar 8, 2023), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/security-outcomes/

[61] CDEI, 前掲注 52 の'*Background*'の *Opportunities*, (last visited Mar 8, 2023), https://cdeiuk.github.io/pets-adoption-guide/opportunities

[62] ICO, *International Data Transfer Agreement*, (Mar 21, 2022), https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf。なお、IDTA の逐条ガイダンスが作成されることになっているが、未公表である。

[63] ICO, *Transfer risk assessments*, (last visited Mar 8, 2023), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/transfer-risk-assessments/

英国においてはIDTAを移転ツールとして用いることにより、第三国への個人データの越境移転を行うことが可能となっている[64]。

IDTAでは、第1部（Part1）「表」において、当事者の情報（表1）や個人データの移転目的等の移転に関する詳細（表2）、移転される個人データの詳細（表3）を記載する欄に加えて、表4として「安全要件」の表題の下、組織的安全措置や技術的安全最小要件を記入する欄が設けられている。また、第2部（Part2）では、「追加的保護条項」の表題の下、追加的な技術的安全保護措置や追加的な組織的保護措置等を記入する欄が設けられている。

データ輸出者及びデータ輸入者は、IDTAの締結にあたってこれらの各欄に適切な事項を記載した上で、安全要件と追加的保護条項を含めたIDTA全体を遵守するものとされている（IDTA第8.1.1条）。安全要件と追加的保護条項は、個人データ侵害の発生リスク及び個人データ侵害がデータ主体へもたらす影響に対して適切なレベルのものでなければならない（IDTA第8.1.2条、第8.5条）。各当事者は、定期的に安全要件と追加的保護条項を含めたIDTA全体が「適切な保護措置」を提供するものになっているかどうかを見直すことが義務付けられている（IDTA第9.1.1条）。

この安全要件や追加的保護条項として記載する技術的安全措置や組織的安全措置の具体的内容として、PETs 採用の有無や採用する PETs の種類が問題になる可能性があると考えられる。

オ　データ保護影響評価（DPIA）

PETsの利用とDPIAとの関係について、2022年PETsガイドライン草案では①PETsの利用を検討すべき場合を決定する局面と②実際にPETsを利用するか否かを決定する局面の2つの局面において、DPIAを実施することで決定のための指針を得ることができるとしている。

(ｱ) PETsの利用を検討すべき場合を決定するという局面

データを取り扱う場合に、PETs（又はPETsの組み合わせ）を利用することが適切であるかどうかは状況次第である。例えば、プロジェクトの設計段階では、PETs の導入を検討すべきである。また、個人データを大規模に取得・分析する場合（例えば、AIアプリケーション、モノのインターネット、クラウドコンピューティングサービス等）は、特に PETs を利用することが適しているものと考えられることから、PETs の利用が積極的に利用されるべきである。これらの検討において、DPIAを行うことによって検討の指針を得ることができる。

---

[64] 当事者間においてIDTAが法的拘束力のある契約として締結された場合に、第三国への個人データの越境移転を可能とする「適切な保護措置」が提供されたものと見なされることになる（IDTA・頭書）。

(ｲ) PETs を利用するか否かを決定すべき局面

PETs を利用することが目的の達成にとって適切であるか否かを決定する際にも、DPIA が有用な指針を提供する。具体的には、以下の点が考慮されることとなる。

予定しているデータ処理の性質、範囲、文脈及び目的	「性質」とは、その個人データでもって行おうとしている事柄であり、「範囲」とは、データ処理が及ぶ範囲のことである。また、「文脈」とは、より広範な見地（データ処理の期待や効果に影響を及ぼしうる内部的及び外部的な要因を含む。）を意味する。「目的」とは、その個人データの処理を行おうとしている理由のことである。ICO が公表している DPIA に関するガイダンス[65]では、DPIA を実施するかの判断におけるデータ処理の「性質」「範囲」「文脈」及び「目的」のそれぞれについて、更に詳細な説明がなされている[66]。
予定しているデータ処理が個人の権利・自由にもたらすリスク	データ処理を行うことによって、データ主体の権利・自由に対していかなるリスクがどの程度もたらされ得るかを検討すべきである。
最先端の PETs と PETs を導入するためのコスト	PETs がデータ処理の目的に照らして十分に成熟したものであるかを理解するためには、PETs の最先端のものを検討すべきであるが、必ずしも最新の技術を実装しなければならないというわけではない。どの PETs を実装するかの検討においては、導入コストもひとつの要因となり得る。

3　各種ガイドライン

（3）プライバシー強化技術についてデータ保護機関等の公的機関が公表するガイドライン等（個人情報保護法等と当該技術の関係についてのガイドライン等）の名称と主な論点。

(1) ICO のガイドライン

[65] ICO, *Date Protection Impact Assessments (DPIAs)*, (last visited Mar 8, 2023), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

[66] ICO, *How do we do a DPIA?*, (last visited Mar 8, 2023), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how5

ア　2022 年 PETs ガイドライン草案

前述のとおり、ICO は、2022 年 9 月、2022 年 PETs ガイドライン草案[67]を公表[68]した[69]。このガイドライン草案は、ステークホルダーから意見を聴取するためのものとして作成されたものであり、現在、同年 12 月末日までを期限に行われたパブリックコンサルテーションの結果を踏まえて、内容の改訂が行われている。2023 年 5 月又は 6 月頃を目途に、改訂内容を含めて、「プライバシー強化技術に関するガイダンス」という一つの最終文書として公表がなされ、最終的なパブリックコンサルテーションに付された後、年内に最終的なガイドラインが公表される見込みとなっている。

2022 年 PETs ガイドライン草案は、PETs がもたらす便益や、現在利用可能な様々な種類の PETs を説明するとともに、PETs がデータ処理機関によるデータ保護法の遵守にいかに役立つかを説明する内容となっている。この PETs に関する ICO ガイダンス草案は、後述する仮名化と匿名化に関するガイダンス草案の一部をなすものである。

2022 年 PETs ガイドライン草案のポイントは、次のとおりである。

- PETs は、データ処理における「デザインによるデータ保護」及び「デフォルトによるデータ保護」アプローチを実証することに資する。
- PETs は、目的のために必要なデータのみを処理し、データ処理に関する適切なレベルのセキュリティを提供することにより、データ最小化の原則の遵守に資する。
- PETs を利用することによって、個人のデータを確実に保護しつつ、他の方法では共有できないようなセンシティブなデータセットにアクセスすることが可能となる。
- PETs は、データ保護原則を全て満たす「万能薬」とみなすべきではない。PETs を利用する場合であっても、データ処理は、法令に基づき公正かつ透明なものでなければならない。
- 個別事案に応じて DPIA 等の適切な評価を行い、PETs が目的に適合しているか否かを判断する必要がある。DPIA とは、あるプロジェクトにおける個人デー

---

[67] ICO, 前掲注 49

[68] ICO 公式ウェブサイト (last visited Mar 8, 2023), https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-publishes-guidance-on-privacy-enhancing-technologies/,

[69] この ICO ガイドライン草案は、後述する仮名化についてのガイドライン草案などとともに、「匿名化、仮名化及びプライバシー強化技術に関するガイダンス草案」という一つの文書の中の一つの章（第 5 章）を構成するものと位置付けられている。

タに関するリスクを特定し最小化することをサポートするためのプロセスである[70]。

ICOは、2022年PETsガイドライン草案を起点としてPETs利用の増進を目指しており、そのために標準化、認証、障壁の低減といった方法を検討中である。また、2022年PETsガイドライン草案に加えて、「AIと金融犯罪」や「AIとヘルスケア」といった特定の状況に焦点を絞ったガイドラインを新たに作成することも計画中であり、また、公的機関によるガバナンスの分野におけるPETsの利用に関するガイドラインの策定も検討中であるが、未だ初期的な検討段階に留まっているとのことである[71]。

イ　その他のICOのガイドライン草案

ICOは、2022年PETsガイドライン草案に先立ち、2022年ICOガイドライン草案の第2章として「匿名化を効果的なものとするための方法に関するガイドライン草案」（以下「**2022年匿名化ガイドライン草案**」という。）を、第3章として「仮名化に関するガイドライン草案」（以下「**2022年仮名化ガイドライン草案**」という。）をそれぞれ作成・公表していた。2022年PETsガイドライン草案において言及されている「個人識別性」や「仮名化」の概念、内容及び基準は、これらのガイドライン草案に記載されているところに依拠することとされている。

なお、2022年匿名化ガイドライン草案及び2022年仮名化ガイドライン草案についても、2022年PETsガイドライン草案と同時に2022年12月末日を期限としてパブリックコメント手続に付されていた。その結果を踏まえて、ICOは、現在、(1)匿名化及び仮名化に関するガイダンス、(2) PETsに関するガイダンスという2つの成果文書を作成中である。(1) 匿名化及び仮名化に関するガイダンスは、①匿名化の紹介、②個人識別性、③仮名化、④アカウンタビリティとガバナンスの各章[72]を含んだ一つの最終文書として作成される予定である。(2) PETsに関するガイダンスは、従前の2022年PETsガイドライン草案（2022年ICOガイドライン草案の第5章）を改訂したものを独立した一つの

---

[70] ICO, *Data protection impact assessments*, (last visited Mar 8, 2023), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/にて、DPIAのプロセス及び結果を記録する方法に関するテンプレートの一例（サンプル）を公表している：
https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fico.org.uk%2Fmedia%2Ffor-organisations%2Fdocuments%2F2553993%2Fdpia-template.docx&wdOrigin=BROWSELINK。
また、同ウェブサイトではDPIAに関するチェックリストが公表されている。

[71] 2023年3月17日に実施したICOのインタビューによる。

[72] これに加えて、「仮名化とリサーチ」についての新たな章を追加した上で、様々な技術がデータ保護法を遵守したデータ・シェアリングの促進に如何に利用され得るかを示すケース・スタディも含むものとすることが計画されているとのことである。

文書とする形で作成される予定となっている。これらの 2 つの最終文書は、2023 年春の終わり頃までに公表され、最終的なパブリックコメント手続に付される見込みとされている。

現在、公表されている匿名化及び仮名化に関する各ガイドライン草案の概要は、以下のとおりである。

(ｱ) 2022 年匿名化ガイドライン草案

ICO は、2021 年 10 月、「匿名化を効果的なものとするための方法に関する 2022 年 ICO ガイドライン草案」[73]を公表した。2022 年匿名化ガイドライン草案のポイントは、以下のとおりである。

- 識別可能性とは、個人の氏名に限らず、特定の個人を他の者と区別することができる他の情報に関するものをいう。
- 個人を特定できるかどうかを評価するにあたっては、「合理的に使用される可能性の高い手段」を考慮する必要がある。具体的には、識別に必要なコストや時間、利用可能な技術、時間の経過に伴う技術の発展状況等の客観的な要因に基づいて行う必要がある。一方で、仮説的、理論的な識別可能性を考慮する必要はなく、状況に照らして識別が合理的にできるか否かにより判断する。また、情報そのものだけでなく、データの公開の種類（一般公開か、特定の集団に対する公開か）や、相手の手元にある情報の状態等、当該情報が処理される環境についても考慮する必要がある。
- 匿名の情報を一般公開することを検討する場合には、特定の集団や個々の組織に対して公開する場合よりも、効果的な匿名化を実現するために、より強固な技術を導入することを検討すべきである。
- 自らが行っているリスク評価と意思決定プロセスについて適切な間隔で見直しを行うべきである。

(ｲ) 2022 年仮名化ガイドライン草案

ICO は、2022 年 2 月、「仮名化に関する 2022 年 ICO ガイドライン草案」[74]を公表した。2022 年仮名化ガイドライン草案のポイントは、以下のとおりである。

---

[73] ICO, *Chapter 2: How do we ensure anonymisation is effective? - Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance*, (Oct 2021), https://ico.org.uk/media/about-the-ico/documents/4018606/chapter-2-anonymisation-draft.pdf

[74] ICO, *Chapter 3: pseudonymisation - Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance*, (Feb 2022), https://ico.org.uk/media/about-the-ico/consultations/4019579/chapter-3-anonymisation-guidance.pdf

- 仮名化とは、個人を特定する情報を置換、削除又は変換し、その情報を分離する技術をいう。匿名化されたデータであっても、依然として個人データであり、データ保護法が適用される。
- 仮名化は、①データ処理がもたらす個人情報の漏洩リスクを軽減し、②「デザインによるデータ保護」を実施することができ、③適切な安全性を確保するとともに、④データを有効活用すること（アーカイブ化、科学・歴史研究、統計目的その他の目的での活用や一般的な分析等）ができる。
- 仮名化と匿名化を混同しないように留意する必要がある。仮名化は、個人情報の漏洩リスクを低減し、安全性を向上させるための方法にすぎず、データ保護法が適用されない程度に個人データを変換するものではない。
- 仮名化を効果的に実施するためには、①目標を明確にし、②リスクを詳細に分析し、③最も適切な仮名化措置を講じ、④成果を文書化することが必要である。

（2）CDEI の 2021 年 CDEI 導入ガイド

CDEI は、2021 年 7 月に 2021 年 CDEI 導入ガイドを公表した。このガイドは、予定している又は現に行っているプロジェクトにとって PETs がいかに有用であり得るかを事業者が検討することのサポートを目的としている。

2021 年 CDEI 導入ガイドでは、事業者が自らのプロジェクトにとっていずれの PETs が有用であり得るかについて検討するためのフローチャートが掲げられている。このフローチャートはインターアクティブなものとなっており、表示される質問に回答していくことで、最終的に、有用と考えられる PETs の説明が表示される仕組みとなっている。また、PETs について伝統的な PETs と新興の PETs に分類した上で主な PETs について説明がなされている。更に、現実に PETs が使用されている事例[75]を集めた「使用事例のレポジトリ」[76]が挙げられており、実例に即して、PETs がどのように便益をもたらすかの情報が記載されている。

2021 年 CDEI 導入ガイドのポイントは以下のとおりである。

- 事業者は、リスク回避的に行動し、法的義務の遵守及びレピュテーションリスクを管理するために、社会にとって有用となる方法によってデータが使用されることを回避しがちである。PETs はこれらのリスクを減少させ、データを用いたイノベーションの機会を拓くものとなる。

---

[75] 例えば、Apple や Facebook、Microsoft、AUSTRAC、Enveil などによる使用事例が掲載されている。

[76] CDEI, 前掲注 52 の*'Adopting PETs'の Repository of Use Cases*, (last visited Mar 8, 2023), https://cdeiuk.github.io/pets-adoption-guide/repository

- PETs も万能ではなく、技術的専門性の欠如、使用コスト、誤った使用がなされるリスク等といった限界が存在する。
- PETs を伝統的な PETs と新興の PETs に分類した上で、PETs の種類・内容とその使用について具体例が挙げられている。

4　その他の法令の規定

（4）その他、プライバシー強化技術が普及していく上で、論点となりうる法令の規定（個人情報、プライバシー、データ保護を目的とする規定、データの越境移転を伴う場合の規定）の概要。

本調査の範囲では、調査日現在、該当するものは見当たらなかった。

5　その他（政策、世論の動向等、関連事項で有用と考えられる事項）

（1）EU 離脱後の英国の国家データ戦略における PETs の位置付け

現在、英国においては、EU 離脱後の英国における新しいデータ保護制度の策定が進められている。英国政府は、2020 年 9 月、政策ペーパー「国家データ戦略（National Data Strategy）」[77]を公表した[78]。国家データ戦略においては、データ利用に対する公衆の信頼を確保しつつ、データの価値を解放してデータ利用がもたらす便益を駆動力として英国の社会と経済を発展させるという方向性が謳われている。

この国家データ戦略の重要な一部を構成するものとして、2022 年 7 月、「データ保護・デジタル情報法案（Data Protection and Digital Information Bill）」（以下「**DPDI**」という。）[79][80]が英国下院に上程された。DPDI は、既存の英国データ保護法（UK GDPR 及び DPA 2018）の修正を提案するものとなっており、データ主体の権利を十分に確保して EU GDPR における十分性認定の地位を維持しつつも、データ利用の拡大による英国の社会・経済のポジティブな変容をもたらすことを目的としている。DPDI の多く規定は UK GDPR を基にした内容であるが、UK GDPR の規定に対して重要な変更が加えら

---

77 Government of United Kingdom, *Policy paper – National Data Strategy*, (updated December 9, 2020), https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy

78 同年 12 月に改訂がなされている。

79 *Data Protection and Digital Information Bill*, (last visited March 8, 2023), https://publications.parliament.uk/pa/bills/cbill/58-03/0143/220143.pdf

80 もっとも、2022 年 9 月の首相交代に伴って、英国下院議会での審議が停止されたまま（現状は第 1 読会が終了した状態）、現在に至っている。

れているものも見られ、EU 離脱後の英国におけるデータ保護制度の改革（EU GDPR からの離脱）の重要な一歩と位置付けられている。

このように、DPDI は、EU GDPR とは異なり、データ主体のデータ保護の要請とデータ利用の要請とのバランスを、データ利用により比重を置いた形で図ろうとするものであるが、これを可能にするための手段の一つとして PETs が重要な役割を果たすとの指摘がなされている [81]。

（2）PETs の研究開発に関する政策イニシアティブ

英国において、PETs の研究開発に関する様々な政策イニシアティブが進行中である。

ア　ICO による政策イニシアティブ

ICO は 2019 年 7 月より規制サンドボックスの運用を開始した。そこでは、公益性が認められるセクターにおいて革新的かつ安全な方法で個人データを用いた製品やサービスを創出する組織・団体が対象となっている [82]。Datasphere Initiative が公表した報告書「データのためのサンドボックス」（Sandboxes for data: creating spaces for agile solutions across borders）[83]では、国境を超えた規制サンドボックスによって達成されることが期待されるイノベーションの分野のひとつとして、PETs が取り上げられている [84]。

また、ICO は、2022 年 2 月、ビジネス・エネルギー・産業戦略省が資金提供を行っているプロジェクト「公益のための PETs」（PETs for Public Good）の一環として、学術機関、リサーチ機関及びデータ保護の専門家とともにヘルスケア分野の機関との一連のワークショップを開催した。このワークショップでは、PETs がヘルス分野において安全で、適法で、かつ経済的に価値のあるデータ・シェアリングをいかに促進するか、またヘルスケア機関がそれらの技術を利用することを促進するためには何が必要かについて議論がなされた。ICO は、2022 年 PETs ガイドライン草案の改訂においてワークショップの成果を反映するとともに、ヘルスケア分野を超えた様々な産業分野において安全かつ適法なデータ・シェアリングを可能にするソリューションを構築することを目指している [85]。

---

[81] CPO Magazine のウェブサイト, (last visited Mar 8, 2023), https://www.cpomagazine.com/data-protection/privacy-enhancing-technology-can-solve-the-uks-data-reform-bill-protection-concerns/

[82] ICO, *Regulatory sandbox*, (last visited Mar 23, 2023), https://ico.org.uk/for-organisations/regulatory-sandbox/

[83] Datasphere Initiative, *Sandboxes for data: creating spaces for agile solutions across borders*, (May 2022), https://www.thedatasphere.org/wp-content/uploads/2022/05/Sandboxes-for-data-2022-Datasphere-Initiative.pdf.

[84] Datashpere Initiative, *Sandboxed for data*, 前掲注 83・29 頁

[85] ICO, *ICO consults health organisations to shape thinking on privacy-enhancing technologies*, (Feb 2022), https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/02/ico-consults-health-organisations-to-shape-thinking-on-privacy-enhancing-technologies/

更に、ICO が 2022 年 12 月に公表した報告書「Tech Horizons Report」[86]では、新しい技術が英国におけるデータ保護枠組とどのように関係するかについての検討がなされている。とりわけ、IoT（Internet of Things）に関しては、多数の装置が使用されて相互に接続されることによって、過剰な情報が収集されるおそれがあるとの認識の下、データ処理の目的の達成に必要な最小限の情報を決定することの重要性が増している旨の指摘がなされている。この点において、スマートスピーカーやスマートホームハブといった装置には、個人情報が伝達される前に一定の PETs が適用されるように仕組まれたものが増加しているとされている。それと同時に、全ての PETs が IoT 設定の全種類にとって有用であるわけではないとの指摘もなされている[87]。

イ　合成データの利用を通じた大規模データの利用可能性の拡大

国家統計局（Office for National Statistics）が統計目的で取得している大量のデータを政府機関、民間企業及び学術機関等が利用することができるようにするために、国家統計局のデータ・サイエンス・キャンパスは、2019 年 1 月、実際の生データを置き換える形で合成データを創出するパイロット事業の結果を公表した[88]。現在は、差分プライバシーのようなプライバシー促進技術を用いた方法に焦点を当てながら、データセットへのアクセスを可能にする合成データの適用についての研究が実施されている。

また、公共政策の効果検証において個人データの利用へのニーズが高まっている。ある公共政策が人々の生活に与える実際の影響を測定するためには大量のデータが必要であるが、他方でそのような個人データの利用にはプライバシー侵害への懸念が不可避的に生じる。そこで、国立科学技術芸術国家基金（Nesta）の完全子会社である社会目的会社である行動インサイトチーム（Behavioural Insights Team：BIT）は、ロー・ファイな合成データの潜在的な利用可能性を提唱し[89]、ロー・ファイな合成データを創出するためのユーザーガイド「Python notebook」[90]を作成し、公表している。また、BIT は国家統計局とともに、上記のアプローチを国家統計局による Secure Research Service（認証された調査者に対して、公益のための調査事業目的に限り、未公表のデータへのアクセスを

---

[86] ICO, *Tech Horizons Report*, (Dec 2022), https://ico.org.uk/media/about-the-ico/documents/4023338/ico-future-tech-report-20221214.pdf

[87] ICO, *Tech Horizons Report*, 前掲注 86・33 頁

[88] Office for National Statistics, *ONS methodology working paper series number 16 - Synthetic data*, (Jan, 2019), https://www.ons.gov.uk/methodology/methodologicalpublications/generalmethodology/onsworkingpaperseries/onsmethodologyworkingpaperseriesnumber16syntheticdatapilot

[89] Behavioural Insights Team, *Accelerating public policy research with synthetic data*, (Dec 2021), https://www.adruk.org/fileadmin/uploads/adruk/Documents/Accelerating_public_policy_research_with_synthetic_data_December_2021.pdf Behavioural Insights Team, *Blog: Accelerating public policy research with easier & safer synthetic data* (Mar 2022), https://www.bi.team/blogs/accelerating-public-policy-research-with-easier-safer-synthetic-data/

[90] Behavioural Insights Team, *Python notebook: Create a Low-Fidelity Synthetic Data Set*, (last visited March 23, 2023) https://colab.research.google.com/drive/1xax64hSDf15WE8v49vpqaRUKDvjppXMQ

認めるサービス）[91]及び同サービスを他の政府機関にも拡張するイニシアティブである Integrated Data Service[92]と統合する方法について検討中である [93]。

ウ　米英政府間の PETs 成熟促進に関するチャレンジ公募（Innovation Prize Challenge）

第 4・5・(1)で後述のとおり。

（3）英国王立協会の報告書

英国における最古かつ最も権威があるとされる学術団体である王立協会（Royal Society）は、2019 年に報告書「実務におけるプライバシーの保護：データ分析のためのプライバシー強化技術の現在の利用、発展及び限界（Protecting privacy in practice: the current use, development and limits pf Privacy Enhancing Technologies for data analysis）」（以下「**2019 年英国王立協会報告書**」という。）[94]を公表した。この 2019 年英国王立協会報告書では、PETs の概要を提示した後、「センシティブデータの保護及び個人の利益の保護」と「データ分析による便益」との間のバランスをとろうとする中で PETs が一定のリスクを軽減する潜在性を有していること、従って、PETs は、受容不可能なリスクを生み出すことなくデータセットを利用できる新しい機会を創出し、データ・エコノミーを創り変える大きな潜在力をもたらしうることが指摘されていた。また、PETs の導入を促進するために、まずは政府が PETs の利用によってデータ分析の新しい機会が創出されることを自らの経験でもって示し、これを共有すべきこと（政府が PETs の導入のための重要なインフルエンサーとなるべきこと）が勧告されていた。

その後、王立協会は、2019 年英国王立協会報告書を踏まえて、2023 年 1 月、新たな報告書「プライバシーからパートナーシップへ：データ・ガバナンスと共同分析におけるプライバシー強化技術の役割（From privacy to partnership: the role of Privacy Enhancing Technologies in data governance and collaborative analysis）」（以下「**2023 年英国王立協会報告書**」という。）[95]を公表した。この報告書では、責任あるデータ利用において PETs がいかにして重要な役割を果たしうるかを検討するものとなっている [96]。また、それに

---

[91] Office for National Statistics, *Secure Research Service*, (last visited March 22, 2023), https://www.ons.gov.uk/aboutus/whatwedo/statistics/requestingstatistics/secureresearchservice

[92] Office for National Statistics, *Integrated Data Service*, (last visited March 22, 2023), https://integrateddataservice.gov.uk/

[93] Bahavioural Insights Team, Blog, 前掲注 89

[94] The Royal Society, *Protecting privacy in practice*, (Mar 2019), https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/Protecting-privacy-in-practice.pdf?la=en-GB&hash=48A28CDF4FB012663652BE671CFFED08

[95] The Royal Society, *From privacy to partnership*, (Jan 2023), https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/From-Privacy-to-Partnership.pdf

[96] The Royal Society, *From privacy to partnership*, 前掲注 95・21 頁以下

引き続いて、①PETs の市場の構築、②PETs の標準、評価及び保証、③PETs の使用事例について説明と検討が加えられている。

①（PETs の市場の構築）では、PETs の導入を妨げている要因として、(a)PETs とそれがもたらす便益についての一般的な認知が欠如していること、(b)データ保護義務と PETs の関係についての理解が欠如していること、(c)PETs の発展に必要となる暗号化の理解が学問上のものに留まっており、市場を動かしているプレイヤーの認識との間に大きな齟齬があること等が指摘されている[97]。

②（PETs の標準、評価及び保証）では、現時点で PETs に特化した標準はほとんど存在しないものの、隣接領域（例えばサイバーセキュリティや AI）における標準を参照しうること、そして、将来において PETs に特化した標準が構築されれば、そのような標準がユーザーの信頼を促進する保証の基礎となり得ることが指摘されている[98]。

③（PETs の使用事例）では、公益のための PETs の使用事例の欠如が PETs の利用の妨げになっているとの認識の下、(a)ヘルス研究や診断のための生体データの利用、(b)IoT におけるプライバシーの強化、(c)集合知（collective intelligence）、犯罪検知及びデジタルガバナンスにおける投票等の場面において PETs がもたらしうる潜在的な便益が示されている。これらの使用事例を通して、PETs は、（データ保護の問題に対する「万能薬」ではないものの）責任あるデータ・ガバナンス・システムを構築するための「新しい積み木（building block）」となり得るとされている[99]。

以上を受けて、2023 年英国王立協会報告書は、国家機関や超国家機関が優先事項として PETs のプロトコールや標準を策定すべきこと、英国政府はデータガバナンスにおける PETs の責任ある利用を促進するために「国家 PETs 戦略」を構築すべきこと[100]等の勧告を行っている。

6　調査対象国・法域における PETs の利用に関する調査結果

本調査の結果明らかとなった対象国・法域における PETs の利用に関する調査結果は次のとおりである。

調査項目	調査結果
個人情報（personal date）を暗号化（秘密	• UK GDPR は匿名化された個人データには適用されない。匿名化をするためには、個人データから重要な要素

[97] The Royal Society, *From privacy to partnership*, 前掲注 95・35 頁以下

[98] The Royal Society, *From privacy to partnership*, 前掲注 95・42 頁以下

[99] The Royal Society, *From privacy to partnership*, 前掲注 95・56 頁以下

[100] 「国家 PETs 戦略」は、「国家データ戦略」や「国家 AI 戦略」（Government of United Kingdom, *National AI Strategy*, (Sep 22, 2021), https://www.gov.uk/government/publications/national-ai-strategy）を補完するものとなるとされている。

分散を含む。以下同じ。）した場合に個人情報以外の情報分類への変更の有無	を除去して、個人が特定できないようにしなければならない。 • 暗号化を行ったものの、再び個人を識別することができるのであれば、そのデータは完全に匿名化されているとは言えず、単に仮名化されているにとどまる。従って、そのようなデータは依然として個人データである。
個人情報を暗号化することにより、軽減される義務・恩恵	• 暗号化により匿名化データに変更された場合、UK GDPR は適用されない。 • 匿名化データに変更されない場合でも、「デザインによるデータ保護／デフォルトによるデータ保護」の規定（UK GDPR 第 25 条）、取扱いの安全性の規定（UK GDPR 第 32 条）上、管理者に要求される適切な技術的措置を講じていると認める、ひとつの要素となる可能性がある。 • 暗号化により、識別可能なデータが開示されることを設計上防ぐことができる場合、適法に個人データを越境移転させることができる可能性がある。
個人情報を用いて二者以上が有する個人情報について秘密計算を行うための要件・手続と法律上の規制の有無	処理の性質に応じてデータ管理者又はデータ処理者に要求される要件・手続・規制[101]が適用される。
二者以上がデータを提供してデータ分析事業者が関わる場合のそれぞれの法律上の関係性	同上
個人情報を匿名化/仮名化することにより、軽減される義務・恩恵	UK GDPR は匿名化された個人データには適用されない。それゆえ、匿名化はリスクを限定する方法となり得、またデータ主体にとって便益となるものである。
義務軽減・恩恵のた	特に見当たらない。

[101] ICO, *Controllers and Processors*, (last visited on Mar 8, 2023), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/を参照。

めに、匿名化/仮名化以外の要件（ある場合）。	
プライバシー強化技術を用いることによる個人情報保護法等上の法的なメリット（義務の軽減、恩恵等）	「デザインによるデータ保護／デフォルトによるデータ保護」の規定（UK GDPR 第 25 条）、取扱いの安全性の規定（UK GDPR 第 32 条）上、管理者に要求されている適切な技術的措置を講じていると認める、ひとつの要素となる可能性がある。また、適法に越境移転することができる要件を満たす可能性がある。

第4　米国

1　プライバシー強化技術（PETs）の名称・技術の概要

（1）調査対象国において、個人データを保護したままで分析等を行うプライバシー強化技術として注目あるいは実用化されている名称と技術の概要。

（1）PETs の定義

ア　関連法令の定め

現在、米国で施行されているデータ保護に関する法律においては、PETs について明確な定義が置かれているものは見つかっていない。なお、PETs とは、複数の異なる技術及び技法を含む概念であると考えられている[102]。

イ　ホワイトハウスによる定義

ホワイトハウス（科学技術政策局; Office of Science and Technology Policy）は、2022 月 6 月 9 日付の PETs 発展に関する情報依頼書（Request for Information on Advancing Privacy-Enhancing Technologies）[103]において、PETs を以下のように定義している。

プライバシーを保護するデータ共有及び分析技術。データの分離性及び機密性を維持しながら、参加者間でのデータ共有及び分析を可能にする一連の技術及びアプローチを指す。

また、2022 年 6 月 20 日付の Advancing a Vision for Privacy-Enhancing Technologies と題したレポート[104]内では、PETs を以下のように定義している。

研究者や医師等が、機密性の高いデータそのものにアクセスする事無く、当該データから知見を得ることを可能にするテクノロジー

ウ　サンフランシスコ連邦準備銀行による定義

サンフランシスコ連邦準備銀行（Federal Reserve Bank of San Francisco）は、2021 年 6 月 1 日に、PETs のカテゴリー、使用事例及び留意事項等についてまとめた、Privacy

---

[102] Federal Reserve Bank of San Francisco, *Privacy Enhancing Technologies: Categories, Use Cases, and Considerations* (Jun, 2021), https://www.frbsf.org/economic-research/wp-content/uploads/sites/4/Privacy-Enhancing-Technologies-Categories-Use-Cases-and-Considerations.pdf 3 頁

[103] The White House- Office of Science and Technology Policy (OSTP), *Request for Information on Advancing Privacy-Enhancing Technologies* (Jun, 2022), https://www.govinfo.gov/content/pkg/FR-2022-06-09/pdf/2022-12432.pdf

[104] The White House, Advancing a Vision for Privacy-Enhancing Technologies (Jun, 2022), https://www.whitehouse.gov/ostp/news-updates/2022/06/28/advancing-a-vision-for-privacy-enhancing-technologies/

Enhancing Technologies と題する Fintech Edge Special レポート（以下「**FRSBS レポート**」という。）において、PETs を以下のように定義している。

> 処理作業において、個人に対するプライバシー及びセキュリティのリスクを最小限に抑えつつ、データから価値を引き出す事を可能とするシステム、過程及び手法の総称 [105]

（2）PETs の種類

FRSBS レポートによれば、次の各技術が PETs として挙げられている。

ア　非識別化（de-identification）

個人を識別するデータそのものを書き換える手法であり、特定の個人を識別する必要が無い場合（統計をとり人種や年齢層の全体的な傾向を把握したい場合等）に使用されることがある。具体的な方法は以下のとおりである。

匿名化（anonymization）	個人を識別する情報を除外する手法。「匿名化（anonymization）」の技術は、「非識別化（de-identification）」のテクノロジーの一環として位置づけられている [106]。 なお、一般的な匿名化の方法としては、 ● マスキング（masking; データセット内の値（value）を隠したり変更したりすることで、データ自体へのアクセスは可能にしつつも、元の値の解析を不可能にする方法） ● 一般化（generalization; 複数の異なる値を 1 つの範囲にまとめる等により、その内容をより大局的に表示し、データ個々の特性を確認しにくくする方法） ● 置換（perturbation; 数値にノイズを加える等によりデータ要素をランダム化することで、分析の精度に影響を与えることなく曖昧さを加える方法） ● スワッピング（swapping; データセット内のデータを再配置し、属性値（attribute values）が元のデータと一致しなくする方法） 等が挙げられる 。[107]また、後述の仮名化（pseudonymization; データセットに含まれる直接的な識別子を仮名又は人工の識別子に置き換えてマスキングする方法）及び合成データ

[105] Federal Reserve Bank of San Francisco, 前掲注 102・3 頁

[106] Federal Reserve Bank of San Francisco, 前掲注 102・6-7 頁

[107] Immuta Inc., What Are the Top Data Anonymization Techniques? (May, 2022), https://www.immuta.com/blog/data-anonymization-techniques/

	（synthetic data; 実際の機密データを反映しつつも本物とは異なる、アルゴリズム等で機械的に生成されたデータ）を匿名化の方法として含める見方もある。なお、連邦取引委員会（Federal Trade Comission）（以下「**FTC**」という。）へのインタビューによれば、本報告書作成時において、匿名化の包括的な定義を設けている法令等があるとは認識していないとのことである。
差分プライバシー（differential privacy）	無作為に抽出されたノイズと呼ばれるデータを追加する手法であり、データセットの組み合わせによる再識別が困難であることが利点の一つである。ノイズが加わってもデータを集約して正確に分析することが可能である。例えば、米国国政調査局 (U.S. Census Bureau)によって使用されている [108]。
合成データ（synthetic data）	オリジナルのデータを基に代用となる新しいデータを創り上げる手法。例えば、英国金融行動監視機構 (Financial Conduct Authority)が開催した Tech Sprints というイベントにおいて、参加企業に対し商品開発のために使用可能な合成データが提供された [109]。
仮名化（pseudonymization）	非センシティブな互換識別子と置き換える手法。ペイメントカード業界セキュリティ標準評議会 (Payment Card Industry Security Standards Council)によってトークン化 (torkenization; センシティブなデータをトークンに置き換える仮名化の一種)がカードのデータ保護の方法として認められている [110]。

イ　暗号化（encryption）

データを一時的に閲覧・使用不可にしたり、許可の無いアクセスを防いだりすることで保護する手法として最も代表的なものであり、元の平文 (plaintext)を暗号文(ciphertext)に変換するが、暗号解読 (decryption)を行えば平文に戻すことが可能となる手法をいう。なお、FTC へのインタビューによれば、暗号化を行うことによって米国デー

[108] Federal Reserve Bank of San Francisco, 前掲注 102・10 頁

[109] Federal Reserve Bank of San Francisco, 前掲注 102・11 頁

[110] Federal Reserve Bank of San Francisco, 前掲注 102・8 頁

タ保護法における分類が変わる（例えば、異なるカテゴリーに分類される等）訳ではないとのことである[111]。暗号化の主な手段は、具体的には以下のとおりである[112]。

対照的暗号法（symmetric cryptography）	暗号化のうち、暗号化及び暗号解読に同じ鍵を使用するものいう。
非対照的暗号法（asymmetric cryptography）	暗号化のうち、暗号化及び暗号解読に異なる鍵を使用するものをいう。日常的に目にする、メールやウェブサイトへのログインや、ビットコインの受け渡し等は、この非対照的暗号法の一例といえる。
準同型暗号（homomorphic encryption）	従来の暗号化では静止中や移動中のデータが保護されていたが、準同型暗号法では、それに加え使用中のデータも保護することができる。例えば、データ漏洩時に該当するパスワードが流出したかの監視等に使用される（当該分析の最中でもパスワード自体は引き続き保護される。）。

① その他の PETs

複数当事者計算法（multi-party computation）	データ分析において対象となるデータを複数のシェアに分け、各シェアは別々の当事者によって分析される。これにより、仮にあるシェアの分析においてデータへの不正アクセス等が認められた場合においても、その他のシェアに危険が及ぶ事態を避けることができる。スタンフォード大学によって独自に開発されたデータ収集システム「PRIO」(対象者のプライバシーに関するデータをシステム側が学ぶこと無く統計データを収集することを可能にする技術)もこの一例に当たると思われる[113]。

[111] FTC の立場からは、暗号化がされているかどうかにかかわらず、個人データ保護に際し「詐欺的（deceptive）」又は「不公平（unfair）」な行為が確認できるかという点が対応に関して重要な基準であるとのことである。かかる基準からすると、データの暗号化が消費者への被害リスクを軽減するという面では有効となり得るものの、暗号化自体が必須の要件ということではなく、FTC による判断はあくまで上記の基準をもとに、消費者への利益と被害のバランスを考慮して行われるとのことである。当該判断は包括的なものであり、暗号化は一つの考慮要素であるものの、十分条件ではなく、暗号化がされているからといって FTC の観点からして適切なデータ保護がされているとはいえないとされる。また、当該基準の判断を行う場合には、「合理的な保護（reasonable security）」措置が講じられていることが重要であり、例えば、現代のテクノロジー環境にそぐわない、古い暗号化の方法が使用されている場合、合理的な保護措置が講じられていないとみなされる可能性があるとのことである。

[112] Federal Reserve Bank of San Francisco, 前掲注 102・12-14 頁

[113] Federal Reserve Bank of San Francisco, 前掲注 102・15-16 頁

データ分散（data dispersion）	対象データをランダムに分け、各部分を別々のロケーションに保管する。例えば、社会保障番号の 9 桁をランダムに分割して別々の場所に保管することで、オリジナルのデータを解読されることを防ぐことができる[114]。
マネージメント・インターフェース（management interface）	組織内のデータセットと従業員の間に入り、アクセス権の管理等を行う[115]。
デジタル・アイデンティティ（digital identity）の証明	米国における車両管理局（Department of Motor Vehicles）により発行される証書が、当事者の運転能力だけでなく、その他幅広い身元確認の目的においても使用されている[116]。
ゼロ知識証明（zero-knowledge proofs）	特定の情報が真実であることを証明するために、それを証明するデータそのものを開示することなく、暗号アルゴリズムを用いて、その真偽を検証することができる技術を指す[117]。
連合学習（federated learning）	機械学習を行うにあたり、（各機関から）関連データを一つの機械学習モデルに送るのではなく、当該関連データを持つ各機関に機械学習モデルを送り、各機関で学習を行った後にその結果のみを集積することによって、関連データそのものを開示することなく分散的な機械学習を行う方法を指す。例えば、健康情報に関する機械学習を行う際に、各病院にて機械学習モデルを使用し、その結果のみを集めることで、当該病院で保持されている患者の機密情報等を病院外に出すことなく、機械学習を完了する事ができる[118]。

（3）PETs 利用のインセンティブ

ア　PETs の目的

FRSBS レポートでは、PETs の目的として、以下の 3 点が挙げられている。

[114] Federal Reserve Bank of San Francisco, 前掲注 102・16-17 頁

[115] Federal Reserve Bank of San Francisco, 前掲注 102・17-18 頁

[116] Federal Reserve Bank of San Francisco, 前掲注 102・19 頁

[117] BBVA, Zero Knowledge Proof: how to maintain privacy in a data-based world, https://www.bbva.com/en/zero-knowledge-proof-how-to-maintain-privacy-in-a-data-based-world/

[118] TNO, Federated learning: get to know privacy-preserving data analysis, https://www.tno.nl/en/technology-science/technologies/federated-learning/

- データの分析等において、特定の個人を識別する必要が無い場合に、個人を識別するデータそのものを書き換えることにより個人の識別可能性を低減すること
- 対象となるデータを一時的に閲覧・使用不可にしたり、許可の無いアクセスを防いだりすることでプライバシーを保護すること
- 前述のデータの書き換えや保護とは異なる新たな手法（複数当事者計算法(Multi-Party Computation)、データ分散 (data dispersion)等）で、データ処理・管理・保管におけるプライバシーの向上をはかること

イ　PETs 利用の利点

FRSBS レポートでは、PETs を利用することによって、以下のような利点があると考えられている。

- データに紐づけされている個人に対するプライバシー及びセキュリティ上のリスクを最小限に抑えつつ、当該データから価値を引き出す事ができる。
- 特に金融や医療等の、機密データの収集が大規模に行われる業界では、データを保護しつつ、本人確認や研究等の目的で活用することが可能となる。
- プライバシー及びセキュリティ上のリスクを抑える事で、収集を含めたデータの利用を促し、その結果として新しい商品、サービス及びテクノロジー等の開発に繋がる[119]可能性も指摘されている。

ただし、米国の個人情報保護法制上、特定の種類の PETs を利用した場合に利点が生じるような制度は見当たらない。

もっとも、HIPAA の下での非識別化（de-identification）の基準（Standard）に沿って非識別化がなされたデータは、HIPAA 及び CCPA の適用を免れることができるため、このような非識別化（de-identification）の基準を満たすことができる PETs を導入すれば、法的観点からも利点が生じるといえる。また、再識別（re-identification）を困難とすることができる差分プライバシー（differential privacy）等の PETs を選択すれば、一旦非識別化されたデータが再識別されるリスクが低下し、再識別による CCPA[120]や HIPAA 上の規制 [121]を回避することが可能になるという法的観点からの利点も生じるものと考えられる。加えて、FTC へのインタビューによれば、州法によってはデータ漏洩の際に当該データが暗号化（又は仮名化若しくは匿名化）されていた場合、通知を必要としないものもあるとのことであり、法規制による義務をあらかじめ軽減しうるということも利点の一つと考えられる。

（4）PETs 利用の障壁

[119] Federal Reserve Bank of San Francisco, 前掲注 102・3-4 頁
[120] Cal. Civ Code §1798.148.
[121] 45 C.F.R 164.502(d)(2)(i)-(ii).

PETs の利用に関しては、とりわけ以下の各点に留意する必要があるとされている。

PETs 使用者側の運用能力	テクノロジーの導入には使用者側のノウハウが求められるものの、PETs はその多くが現時点で広く浸透していないことから、適切に運用するための能力が使用者側に備わっていないケースも想定される [122]。この場合、十分なノウハウを持つ事業者に運用を委託することも考えられるが、そうすると第三者がデータ等を扱うことによるリスクが別途生じることとなる。また、例えば、前述の同型暗号化等のテクノロジーは、その運用に多大なコンピューティング能力を使用するため、使用者に対するコストもその分上がることとなる [123]。
各 PETs 技術の発展段階	前述のとおり、PETs は比較的新しい概念であり、またその種類も広義にわたることから、まだ開発の初段階である技術も存在する。各 PETs 技術によって発展の段階が異なることから、使用者にとっては、どの PET を導入するべきか、また、運用にあたりどのようなリソースが必要か判断することが難しいのが現状である [124]。
既存のデータ権利との関係	データ主体が自身の個人データの取得や削除を求めることができる既存のデータ主体の権利等を行使するにあたり、PETs との関係が問題となることも考えられる。例えば、個人データの削除に応じる際には、当該個人と削除するデータの紐づけが必要となるが、前述の非識別化の過程で個人を識別する要素が完全に削除されている場合はどう対応すべきか、という問題が生じる。また、いったん非識別化されたデータを再度、非識別化することが法的に禁じられている場合は、データ主体の権利への対応が更に難しくなると思われる [125]。ただし、カリフォルニア消費者プライバシー法 (California Consumer Privacy Act of 2018) では、データの再非識別化 (re-identification)を、医療関連の行為や非識別化のテストや分析等 [126]の一定の目的のために許可している [127]。

[122] Federal Reserve Bank of San Francisco, 前掲注 102・5 頁

[123] Federal Reserve Bank of San Francisco, 前掲注 102・5 頁

[124] Federal Reserve Bank of San Francisco, 前掲注 102・5 頁

[125] Federal Reserve Bank of San Francisco, 前掲注 102・5 頁

[126] Cal. Civ Code §1798.148, 前掲注 120

[127] Federal Reserve Bank of San Francisco, 前掲注 102・5-6 頁

犯罪捜査過程との関係	また、末端間の暗号化 (end-to-end encryption)では、データの送受信者のみが当該データを閲覧することができ、電話会社等の中間業者はその内容を確認することができない仕様となっているものの、こういった PETs 技術が犯罪捜査の観点からは好ましくないと主張する声もあり、PETs の利便性と犯罪捜査におけるニーズのバランスのとり方も課題の一つと考えられる [128]。
PETs 導入に関するインセンティブの低さ	PETs の導入には、使用者側にとって多かれ少なかれコストが発生することとなる。同時に、PETs 技術によっては、ある程度浸透し一定の使用者数に達するまでその効果を発揮することが難しいものもあると考えられ、各々の使用者が率先して自主的に導入に踏み切る土壌が現時点で整っていない可能性も指摘される [129]。
技術が複雑であり専門的なスキルが必要	PETs には様々な技術やシステムがあるため、PETs を導入する事業者は、十分な専門知識を有していなければ、これらのツールを導入するにあたってどのようなリソースが必要か理解することも困難であると考えられる [130]。
その他の課題	更なる研究開発の必要性と一般化が可能なソリューションの欠如を現段階の PETs における課題として挙げている [131]。

2　データ保護法との関係、データ保護法上の論点

（2）前述において、個人情報、プライバシー保護に関する法律（以下「個人情報保護法等」という。）の観点から論点となっている点（過去論点となった点、事業者による改正要望、政府による改正予定の点も含む。）。

(1) 米国データ保護法の概要

ア　現行法

(ｱ) 連邦法

[128] Federal Reserve Bank of San Francisco, 前掲注 102・6 頁

[129] Federal Reserve Bank of San Francisco, 前掲注 102・6 頁

[130] Federal Reserve Bank of San Francisco, *Privacy Enhancing Technologies: What Are They and Why Do They Matter? (Jun, 2021),* https://www.frbsf.org/our-district/about/sf-fed-blog/privacy-enhancing-technologies-data-use-protection/

[131] OECD, 前掲注 41・35 頁。

個人情報の保護に関する法律によって、個人情報の取扱いを包括的に規定している日本と異なり、連邦法のレベルでは、金融（グラム・リーチ・ブライリー法: Gramm-Leach-Bliley Act）、医療（医療保険の相互運用性及び責任に関する法律: Health Insurance Portability and Accountability Act of 1996）、児童保護（児童オンラインプライバシー保護法: Children's Online Privacy Protection Act of 1998）等の各分野において、データ保護に関する法令が別々に存在している[132]。連邦法レベルでは、本報告書作成時現在、後述のデジタル・プライバシー・テクノロジー促進法(Promoting Digital Privacy Technologies Act)の法案が国会に提出され、下院で可決されている。なお、FTC へのインタビューによれば、現行の米国法において、個人データの域外移転に関する規制は無いとのことである[133]。また、少なくとも連邦法の観点からは、GDPR 等の「管理者（controller）」や「処理者（processor）」といった当事者関係の枠組みに適用される規制は確認されていない[134]。

① グラム・リーチ・ブライリー法（Gramm-Leach-Bliley Act: GLBA）

「グラム・リーチ・ブライリー法（Gramm-Leach-Bliley Act）」（以下「**GLBA**」という。）の対象となる各金融機関は、「顧客のプライバシーを尊重し、当該顧客の非公開個人情報のセキュリティ及び機密性を保護する」義務を負う[135]。また、各金融機関は、自身のプライバシーポリシー及びプライバシーに関する取組み等について、消費者に書面で説明を行うことが求められている[136]。加えて、金融機関は消費者の非公開個人情報を第三者と共有する前に、消費者にその旨を事前に通知し、第三者との情報共有を拒否する機会を与えなければならない[137]。

② 医療保険の相互運用性及び責任に関する法律（Health Insurance Portability and Accountability Act of 1996: HIPPA）

「医療保険の相互運用性及び責任に関する法律（Health Insurance Portability and Accountability Act of 1996）（以下「**HIPAA**」という。）の下では、原則として、医療機関等の対象者（covered entity）若しくはビジネスアソーシエートが、保護対象保健情報（protected health information: PHI）を患者の同意無しに第三者に開示することを禁止

---

[132] Wirecutter, Inc., *The State of Consumer Data Privacy Laws in the US (And Why It Matters)* (Sep, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

[133] ただし、データ処理者のモニタリングや、プライバシーポリシー内の消費者に対する誓約の遵守は、域外転移を含むいかなる場合においても必要とされる。

[134] 例えば、FTC の立場からは、特定の行為が「詐欺的（deceptive）」又は「不公平（unfair）」であるかが判断基準であり、管理者及び処理者の区別は特に考慮されていないとのことである。

[135] 15 U.S.C. §6801(a).

[136] 15 U.S.C. §6803(a).

[137] 15 U.S.C. §6802. ただし、FTC へのインタビューによれば、個人情報を第三者に提供しない場合においても、GLBA 下において、企業は自身が保持する個人情報を把握し、モニタリングするよう求められるとのことである。

している[138]。PHI とは、電子的又はその他の媒体で保管・送信される個人の特定が可能な情報（individually identifiable information）を指すが[139]、非識別化（de-identification）がされている情報については、前述の PHI の「個人の特定が可能な情報」の定義から除外されるものと明示されている[140]。

また、米国保険福祉省（United States Department of Health and Human Services）は、HIPAA プライバシールール[141]における非識別化の方法に関するガイダンス[142]を公開しており、HIPAA プライバシールール上の非識別化の 2 種類の方法について、よくある質問に回答する形で説明を行っている。

まず、第一の非識別化の方法として、HIPAA プライバシールール§164.514(b)(1)記載の「専門家による判断（Expert Determination）」が存在し、この方法には（1）情報が個人を特定できないようにするための、一般的に認められた統計的及び科学的な原理と方法に関する適切な知識及び経験を有する者が、(i) 上記の原理と方法を適用した上で、個人情報の予期される受信者が当該情報の対象個人を特定するために同情報を（単体又はその他合理的に入手可能な情報と合わせて）利用するリスクが非常に小さいと判断し、（ii）この判断を正当化する分析方法及びその結果を文書化する必要がある。この方法に関し、本ガイダンスでは、「専門家」[143]の定義や、専門家にとって受け入れ可能なリスクのレベル、専門家の判断の有効期間等について説明している。

次に、第二の非識別化の方法としては HIPAA プライバシールール§164.514(b)(2)記載の「セーフ・ハーバー（Safe Harbor）」方式であり、これにはまず（2）（i）個人又はその親族、雇用者、世帯員の氏名、（州より小さいレベルの地区表記、電話番号、車両情報、社会保障番号、IP アドレス、生体情報等の 18 種類の情報を削除した上で、(ii) 対象事業者側で、当該情報が（単体又はその他の情報と合わせて）対象者の識別に使用され得ることを実際に知っていないことが求められる。この方法に関し、本ガイダンスでは、「実際に知っている（actual knowledge）」[144]ことの意味や、ZIP コードが非識別

---

[138] 45 CFR §164.502(a) , 前掲注 121

[139] 45 CFR §160.103.

[140] 45 CFR §164.514.

[141] Office for Civil Rights Headquarters, U.S. Department of Health & Human Services, *The HIPAA Privacy Rule* (Mar, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

[142] Office for Civil Rights Headquarters, U.S. Department of Health & Human Services, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* (Oct, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#rationale

[143] 本ガイダンスによると、「専門家」に該当するために特定の学位や証書は必要とされず、実務・学術的な経験や、その他の訓練課程等が考慮され、統計学、数学、その他科学的な分野の専門家が想定されているとのことである。

[144] 本ガイダンスによると、「実際に知っている」とは、削除後に残った情報が（単体又はその他の情報と合わせて）対象者を識別されるために使用され得るという、明確かつ直接的な知識を対象事業体側が有することを指すとし、（削除がなされた後でも）残存する情報が独特な役職や公になっている臨床的な出来事に関するものである等の理由により、対象事業体側で当該情報によって個人識別が可能であると考えられる場合を例に挙げている。

化された情報に含まれ得るか、（内科医の名前等の）全ての個人の氏名を削除する必要があるか等といった点について説明している。

(ｲ) 州法

連邦法と並行し、各州においてもデータ保護に関する法律が制定されており、州法レベルでも分野別の規定がなされている[145]。

① カリフォルニア州消費者プライバシー法（California Consumer Privacy Act: CCPA）

カリフォルニア州では、分野別ではなくて、より包括的にデータ保護を規定する「カリフォルニア州消費者プライバシー法（California Consumer Privacy Act）」（以下「**CCPA**」という。）を 2018 年 6 月 28 日に制定した[146]。同法が適用される事業者等は、カリフォルニア州の消費者に関する個人情報を保護するために、合理的な実施方法や手続（reasonable security procedures and practices）を実施しなければならない[147]。また、同消費者によって、自身のどのような個人情報が収集されたのか知る権利[148]や、個人情報の販売を拒否（オプトアウト）する権利[149]、又は個人情報の削除を求める権利[150]の行使がなされる場合、事業者にはその都度対応が求められ、前述の個人情報保護及び消費者の権利行使への対応にあたり、PETs の活用が重要視される[151]。ただし、CCPA において、PETs そのものに言及する記載は見当たらない。なお、カリフォルニア州では CCPA 制定後の 2020 年 11 月 3 日付で、「カリフォルニア州プライバシー権利法（California Privacy Rights Act）」（以下「**CPRA**」という。）[152]が住民投票により可決され、CCPA を更に強化する内容となっているが、CPRA においても PETs 自体についての規制は設けられていない。

なお、CCPA の下での「個人情報」の定義は、「特定の消費者又は家庭を特定し、関連付け、説明し、合理的に関連付けることができ、又は直接的若しくは間接的に関連付けることができる情報」[153]とされているが、HIPAA に関連する非識別化の要件[154]に沿って非識別化がされている患者情報から派生した情報については、同定義の対象外としている[155]。

---

145 Husch Blackwell, *2023 State Privacy Law Tracker* (Feb, 2023), https://www.huschblackwell.com/2023-state-privacy-law-tracker

146 Cal. Civ. Code § 1798.100

147 Cal. Civ. Code § 1798.100(e)，前掲注 146

148 Cal. Civ. Code § 1798.110

149 Cal. Civ. Code § 1798.120

150 Cal. Civ. Code § 1798.105

151 iapp, *With proposed privacy tech law comes validation of an industry* (Feb, 2021), https://iapp.org/news/a/with-proposed-privacy-tech-law-comes-validation-of-an-industry/

152 California Legislative Information, *AB-1490 California Privacy Rights Act of 2020: California Protection Agency* (May, 2021), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB1490.

153 Cal. Civ Code§1798.140(v)(1).

154 45 C.F.R.§164.514.，前掲注 140

155 Cal. Civ Code§1798.146(a)(4)(A).

② コロラド州プライバシー法（Colorado Privacy Act: CPA）

コロラド州では、2021 年 7 月 7 日付で「コロラド州プライバシー法（Colorado Privacy Act）」（以下「**CPA**」という。）[156]が可決されており、2023 年 7 月 1 日に施行される予定となっている。同州政府の機関や、HIPAA に関連する一定のデータや文書、GLBA の対象となる金融機関やデータ等は、CPA の対象外とされる [157]。CPA の下での「個人データ」の定義は「識別された個人又は識別可能な個人に紐付けされた、若しくは合理的に紐付け可能な情報」とされ、非識別化がされたデータ（de-identified data）や一般に公開されているデータはこれに含まれない [158]。

③ バージニア州消費者データ保護法（Virginia Consumer Data Protection Act: VCDPA）

バージニア州では 2021 年 3 月 2 日に「バージニア州消費者データ保護法（Virginia Consumer Data Protection Act）」（以下「**VCDPA**」という。）VCDPA[159]が可決されており、2023 年 1 月 1 日に施行されている。同州政府の機関や、非営利団体、HIPAA に従って制定された連邦行政命令集特定条項の対象団体、GLBA の対象となる金融機関やデータ等は、VCDPA の対象外とされる [160]。VCDPA の下での「個人データ」の定義は「識別された個人又は識別可能な個人に紐付けされた、若しくは合理的に紐付け可能な情報」とされ、非識別化がされたデータや一般に公開されているデータは、これに含まれない [161]。

④ ユタ州消費者プライバシー法（Utah Consumer Privacy Act: UCPA）

ユタ州では 2022 年 3 月 24 日に「ユタ州消費者プライバシー法（Utah Consumer Privacy Act）」（以下「**UCPA**」という。）[162]が可決されており、2023 年 12 月 31 日に施行される予定となっている。同州政府の機関や、非営利団体、HIPAA で保護される健康情報、GLBA の対象となる金融機関やデータ等は、UCPA の対象外とされる [163]。UCPA の下での「個人データ」の定義は「識別された個人又は識別可能な個人に紐付けされた、若しくは合理的に紐付け可能な情報」とされ、非識別化がされたデータ、集約されたデータ、及び一般に公開されているデータは、これに含まれない [164]。

⑤ コネチカット州データプライバシー法（An Act Concerning Personal Data Privacy and Online Monitoring: CTDPA）

156 C.R.S. 6-1-1301.
157 C.R.S. 6-1-1304(2).
158 C.R.S. 6-1-1303(17).
159 Va. Code Ann. Title 59.1, Ch. 53.
160 Va. Code Ann. §59.1-576B.
161 Va. Code Ann. §59.1-575.
162 Utah Code Ann. Title 13, Ch. 61.
163 Utah Code Ann. §13-61-102(2).
164 Utah Code Ann. §13-61-101(24).

コネチカット州では 2022 年 5 月 10 日に「コネチカット州データプライバシー法（An Act Concerning Personal Data Privacy and Online Monitoring）」（以下「**CTDPA**」という。）が可決されており、2023 年 7 月 1 日に施行される予定となっている [165]。同州政府の機関や、非営利団体、GLBA の対象となる金融機関やデータ、HIPAA で保護される健康情報等は、CTDPA の対象外とされる [166]。CTDPA の下での「個人データ」の定義は「識別された個人又は識別可能な個人に紐付けされた、若しくは合理的に紐付け可能な情報」とされ、非識別化がされたデータ及び一般に公開されているデータは、これに含まれない [167]。

イ　改正法案

(ｱ) 連邦法

① デジタル・プライバシー・テクノロジー促進法（Promoting Digital Privacy Technologies Act）の法案

現時点では法案であるものの、2021 年 2 月 4 日に、米国議会上院（S. 224）[168]及び下院（H.R. 847）[169]それぞれで、「デジタル・プライバシー・テクノロジー促進法（Promoting Digital Privacy Technologies Act）」の法案が提出された。同法案は下院で 2022 年 5 月 12 日に可決されているものの、上院においては未可決のまま次期国会に入ったため、再度下院での可決が必要となっている。

同法案では、「米国国立科学財団（National Science Foundation）（以下「**NSF**」という。）に、能力に応じた適切な選考過程を通じ PETs の研究プログラムを支援する事を求め [170]、また、情報技術研究開発（Networking and Information Technology Research and Development; NITRD）、NSF、FTC 等の政府機関の間で PET の開発・展開・採用を早めるため相互協力するよう義務付けている。また、同法案では NSF や FTC 等の特定の機関に対し、PETs 研究や政策助言等に関する報告を行うよう規定している [171]。

また、同法案は PETs について、「データ若しくはデータセットに含まれる個人情報のプライバシー及び機密性を強化するためのソフトウェアソリューション、技術的プロセス又はその他の技術的手段」と定義している [172]。FTC へのインタビューによれば、本報告書作成時において、同法案以外に PETs の包括的な定義を設けているものを認識していないとのことである。

---

165 Public Act No. 22-15.
166 Public Act No. 22-15 §3(a)(b).
167 Public Act No. 22-15 §1(18).
168 CONGRESS.GOV, S. 224 – Promoting Digital Privacy Technologies Act (Feb, 2022), https://www.congress.gov/bill/117th-congress/senate-bill/224
169 CONGRESS.GOV, H.R. 847– Promoting Digital Privacy Technologies Act (Feb, 2022), https://www.congress.gov/bill/117th-congress/house-bill/847
170 Promoting Digital Privacy Technologies Act, S. 224/H.R. 847, 117th Cong. §3 (2022). https://www.congress.gov/bill/117th-congress/house-bill/847
171 Promoting Digital Privacy Technologies Act, 前掲注 170, §5,§6.
172 Promoting Digital Privacy Technologies Act, 前掲注 170, §2.

② 米国データプライバシー保護法（American Data Privacy and Protection Act: ADPPA）法案

現時点では法案であるものの、2022 年 6 月 21 日に、米国議会下院（H.R. 8152）[173]で、米国データプライバシー保護法（American Data Privacy and Protection Act）（以下「**ADPPA**」という。）が提出された。

同法案の対象となる事業体の範囲は広く、(a)対象となるデータを収集、処理若しくは移転する事業体若しくは個人であり、米国連邦取引委員会法の適用を受ける者、米国通信法第 2 編の適用を受ける電気通信事業者、及び自身若しくはその構成員の利益を目的とした事業を行うために設立されたわけではない組織、又は(b)他対象事業体との間に支配・被支配・共同支配の関係にある若しくは他対象事業体と同じブランドを共有する者が含まれている[174]。

また、同法案の対象となるデータは、(a)個人を識別し、若しくは個人と関連付けられ、又は個人に合理的に関連付けられる可能性のある情報、あるいは(b)1 人以上の個人を識別し、若しくは当該個人と関連付けられ、又は当該個人と合理的に関連付けられる可能性のある端末を指し、それから派生するデータ及び特有の識別子も含まれる可能性がある[175]。ただし、非識別化がされたデータや公開されている情報等は、対象データには含まれないと明記もされている[176]。

同法案は、(a)対象事業体の消費者に対する忠実義務（Duty of Loyalty）[177]、(b)消費者のデータに関する権利（Consumer Data Rights）[178]、(c)企業の説明責任（Corporate Accountability）[179]、及び(d)執行、適用性及び雑則（Enforcement, Applicability, and Miscellaneous）[180]の 4 編から構成され、消費者にプライバシー関連の権利を与えるとともに、対象事業体に対する関連当局（FTC）の監督メカニズムを設定している。

(ｲ) 州法

前述の州の他にも、いくつかの州[181]では本報告書作成時点において、各州議会にデータ保護・プライバシー関連の法案が提出されている。この中で、いわゆる「PETs」若しくは「privacy enhancing technologies」を明示的及び包括的に規制している法案は確認

[173] American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022). https://www.congress.gov/117/bills/hr8152/BILLS-117hr8152rh.pdf

[174] American Data Privacy and Protection Act, 前掲注 173, §2(9).

[175] American Data Privacy and Protection Act, 前掲注 173, §2(8)(A).

[176] American Data Privacy and Protection Act, 前掲注 173, §2(8)(B).

[177] American Data Privacy and Protection Act, 前掲注 173, Title I.

[178] American Data Privacy and Protection Act, 前掲注 173, Title II.

[179] American Data Privacy and Protection Act, 前掲注 173, Title III.

[180] American Data Privacy and Protection Act, 前掲注 173, Title IV.

[181] 本報告書作成時においては、以下の州が挙げられる：ニューヨーク州、テキサス州、イリノイ州、ワシントン州、オレゴン州、オクラホマ州、ミネソタ州、アイオワ州、インディアナ州、ケンタッキー州、テネシー州、ニュージャージー州、ニューハンプシャー州、バーモント州、マサチューセッツ州、ロードアイランド州、及びハワイ州。

されていないものの、テキサス州[182]やアイオワ州[183]の様に、個人データの定義から非識別化（de-identified）されたデータが除外されると明記する法案も存在する。また、ロードアイランド州[184]で提出された法案では暗号化（encrypted）されたデータ、並びにケンタッキー州[185]の法案では（非識別化に加え）仮名化（pseudonymous）されたデータがそれぞれ個人データの対象外と明記されている。

（2）PETs と米国データ保護法との関係

現時点において PETs そのものに言及して規制する米国データ保護法は見当たらず、PETs 及びその使用は規制されていないものと考えられる。また、PETs に関する一貫した定義も現段階では明記されていないと考えられる。一方で、前述のデジタル・プライバシー・テクノロジー促進法案のように、PETs の定義を明確化する動きもあるものの、例えば、同法案の場合は PETs 研究を促進するための政府機関間の取り組みについて規定しており、PETs の販売や使用そのものを規制するものではない。

（3）PETs に関わる米国データ保護法上の論点

ア　匿名化/仮名化/暗号化

ICO が 2022 年 9 月に ICO ガイドライン草案を提出したように PETs と匿名化技術を異なる概念としている国もある中、米国における位置づけとしては、匿名化、仮名化及び暗号化は、PETs の一種としてみなされているように見受けられる。例えば、前述のとおり、FRSBS レポート内では、匿名化、仮名化及び暗号化を、それぞれ異なる PETs の種類として扱っている[186]。加えて、同じく前述の法案では、PETs の定義を極めて広義に設定しており[187]、また、NSF の支援を受け得る PETs の研究対象として匿名化及び仮名化を明示している[188]。

イ　デザインによるデータ保護/デフォルトによるデータ保護

GDPR 及び UK GDPR 等で規定される「デザインによるデータ保護」及び「デフォルトによるデータ保護」の概念は、これまで米国法において明確な定義や区別がされていなかったものの、前述の概念を盛り込む新しい州法として、「カリフォルニア州年齢適正デザインコード法（California Age-Appropriate Design Code Act）」（以下「**CAADCA**」という。）[189]が 2022 年 9 月 15 日に州知事により署名され、2024 年 7 月 1 日に施行が予定されている。

---

182 H.B. 1844.
183 S.S.B. 1071.
184 H.5354185 S.B. 15.
185 S.B. 15.
186 Federal Reserve Bank of San Francisco, 前掲注 102・4 頁
187 Promoting Digital Privacy Technologies Act, 前掲注 170.
188 Promoting Digital Privacy Technologies Act, 前掲注 170 §3(1) (2022).
189 Cal Civ Code § 1798.99.28-40.

CAADCA では、18 歳以下の児童がアクセスする可能性のあるオンライン上のサービス、製品、又は機能を提供する事業体（business）（「事業体」の定義は CCPA と同様とされる[190]。）に、当該サービス、製品、又は機能のデザインが、児童に対し（実際若しくは潜在的に）有害な影響を与えるものでないか等を確認する DPIA を行う等の義務を設けている[191]。また、当該サービス、製品、又は機能によって児童に対し与えられるプライバシー設定のデフォルトを高いプライバシーレベルとすること[192]や、原則として児童のプロファイリングをデフォルトでしないこと[193]、及び児童の位置情報をデフォルトで収集、販売、共有しないこと[194]も義務付けられている。CAADCA における「デフォルト」は「オンラインサービス、製品、又は機能に対して事業体が採用する事前選択されたオプション」[195]と定義されている。ターゲット広告目的でのデータ処理や個人データの販売、その他消費者に危害が及ぶリスクを高める処理活動について DPIA を行うよう求め、コロラド州[196]の CPA においても消費者に危害が及ぶリスクを高める処理活動について DPIA を行うよう規定している。

ウ　その他

その他、PETs の成熟性や安全性に関する具体的な基準について調査したものの、この点を特に明示する公開文献は不見当であった。また仮に PETs を利用する場合、個人情報法制上、利点が生じる PETs の種類についても調査を行ったが、米国の個人情報保護法制上、特定の種類の PETs を利用した場合に利点が生じるような制度は見当たらない。

もっとも、HIPAA の下での非識別化（de-identification）の基準（Standard）に沿って非識別化がなされたデータは、HIPAA 及び CCPA の適用を免れることができるため、このような非識別化（de-identification）の基準を満たすことができる PETs を導入することによって、法的観点からの利点が生じるといえる。また、再識別（re-identification）を困難とすることができる差分プライバシー（differential privacy）等の PETs を選択すれば、一旦非識別化されたデータが再識別されるリスクが低下し、再識別による CCPA[197]や HIPAA 上の規制[198]を回避することが可能になる利点も生じるものと考えられる。加えて、前述のとおり、州法によっては暗号化（又は仮名化若しくは匿名化）されたデータであれば、データ漏洩時の通知義務を免除するものも存在するとのことである。

---

190 Cal Civ Code § 1798.99.30(a).
191 Cal Civ Code § 1798.99.31(a)(1)(B).
192 Cal Civ Code § 1798.99.31(a)(6) , 前掲注 191
193 Cal Civ Code § 1798.99.31(b)(2) , 前掲注 191
194 Cal Civ Code § 1798.99.31(b)(5) , 前掲注 191
195 Cal Civ Code § 1798.99.30(b)(3), 前掲注 190
196 C.R.S. 6-1-1309(1).
197 Cal. Civ Code §1798.148, 前掲注 120
198 45 C.F.R 164.502(d)(2)(i)-(ii).

3　各種ガイドライン

（3）プライバシー強化技術についてデータ保護機関等の公的機関が公表するガイドライン等（個人情報保護法等と当該技術の関係についてのガイドライン等）の名称と主な論点。

前述のとおり、サンフランシスコ連邦準備銀行は、FRSBS レポートを発行[199]している。本 FRSBS レポートは、政策決定者やビジネスリーダーによるデータセキュリティとプライバシー保護の分野における監督と意思決定を補足するため、PETs のカテゴリー分けや事例解説、及び現存する課題や留意事項の紹介を通じ、PETs の包括的な概要を説明する報告書と位置付けられている[200]。また、HIPAA プライバシールールにおける非識別化のガイダンスについては、前述第 4・2・(1)・ア・(ｱ)・②記載のとおりである。

4　その他の法令の規定

（4）その他、プライバシー強化技術が普及していく上で、論点となりうる法令の規定（個人情報、プライバシー、データ保護を目的とする規定、データの越境移転を伴う場合の規定）の概要。

前述第 4・2・(1)・イ記載の改正法案のとおりである。

5　その他（政策、世論の動向等、関連事項で有用と考えられる事項）

(1) 米英政府間の PETs 成熟促進に関するチャレンジ公募（Innovation Prize Challenge）

---

[199] Federal Reserve Bank of San Francisco, 前掲注 102

[200] Federal Reserve Bank of San Francisco, 前掲注 102・2 頁。また、米国国勢調査局（United States Census Bureau）による差分プライバシー関連の情報（https://www.census.gov/programs-surveys/decennial-census/decade/2020/planning-management/process/disclosure-avoidance/differential-privacy.html）（選挙区改正において使用される国税調査局の情報から、個人情報を除外するために差分プライバシーを起用した試みを、差分プライバシーの概要等と合わせて説明している）や、米国標準技術局（National Institute of Standards and Technology）によるプライバシー強化暗号技術（Privacy-Enhancing Cryptography）に関する情報（https://csrc.nist.gov/Projects/cryptographic-standards-and-guidelines）（ブロック暗号法（block cipher techniques）やスキップジャック・アルゴリズム（Skipjack algorithm）等のいわゆるプライバシー強化暗号技術について、該当する連邦情報処理基準書（Federal Information Processing Standards; FIPS）や特別出版物（Special Publication; SP）の情報を交え説明している）等も、広義にはプライバシー技術に関するリソースと考えられる。

2021 年 12 月の民主主義サミット（Summit for Democracy）において、PETs 成長促進に関する米英政府間の協力関係が発表された[201]。当該チャレンジ公募企画は、2022 年 7 月に正式に開始され、学会・工業会・その他幅広い一般階層から集まった両国のイノベーターからプライバシーに配慮した金融犯罪防止への対処等の PETs ソリューションを募集し、優秀なアイデアには賞金が割り当てられることとなっている[202]。本チャレンジでは、第 1 トラック（金融犯罪の検出能力改善）及び第 2 トラック（パンデミックにおける感染リスクの予想）の 2 つのトラックのいずれか又は両方を選択し、それぞれに対応できる PET ソリューション（連合学習）の開発が求められる[203]。両方のトラックに対応する単一のソリューションの開発には、ボーナスポイントが与えられるとのことである[204]。また、チャレンジは、「概念論文（Concept Paper）」「ソリューション試作（Solution Development）」「レッド・チーミング（Red Teaming）」の 3 フェーズから構成され[205]、このうち、フェーズ 1 の概念論文では、既に優秀者が発表されている[206]。フェーズ 1 の優秀者は、2023 年 1 月 24 日までに、それぞれ提案したソリューションのプロトタイプを試作することとなっている（フェーズ 2）[207]。レッド・チーミング（フェーズ 3）では、フェーズ 2 で試作されたプロトタイプに対し参加者（フェーズ 1 を通過しなかった者も含む。）が 2023 年 2 月 13 日から 28 日にかけて攻撃を仕掛け、その準備期間が現在、フェーズ 2 と並行して進んでいる。本チャレンジのソリューションは、2023 年上半期の第 2 回民主主義サミットにおいて、バイデン大統領によって発表される予定である[208]。

（2）PETs に関するパブリックコメントの募集

米国科学技術政策局（Office of Science of Technology Policy: 以下「**OSTP**」という。）は、情報技術研究開発内の委員会や米国人工知能構想局（National Artificial Intelligence Initiative Office）等を代表し、2022 年 6 月 9 日から同年 7 月 8 日にかけて、PETs の導入及び発展に関する米国の国策について、学会・民間セクター・市民社会等からパブリックコメントを募集した。

当該パブリックコメント募集では、以下の 10 のトピックについて回答を募っている。

① PETs 推進に関する具体的な研究の機会

② PETs の具体的な技術的側面及び制限

---

201 The White House, *US and UK to Partner on Prize Challenges to Advance Privacy-Enhancing Technologies* (Dec, 2021), https://www.whitehouse.gov/ostp/news-updates/2021/12/08/us-and-uk-to-partner-on-a-prize-challenges-to-advance-privacy-enhancing-technologies/

202 Privacy-Enhancing Technologies PRIZE CHALLENGES, U.K.-U.S. prize challenges Accelerating the adoption and development of privacy-enhancing technologies (PETs), https://petsprizechallenges.com/

203 OECD, 前掲注 41・37 頁。

204 PET PRIZE CHALLENGES, 前掲注 202

205 PET PRIZE CHALLENGES, 前掲注 202

206 DRIVEN DATA LABS, MEET THE WINNERS OF THE U.S> PETS PRIZE CHALLENGE: PHASE 1 (Nov, 2022), https://drivendata.co/blog/federated-learning-pets-prize-winners-phase1

207 DRIVEN DATA LABS, U.S. PETs Prize Challenge: Phase 3 (Red Teams), https://www.drivendata.org/competitions/139/nist-federated-learning-3-red-teams/

208 DRIVEN DATA LABS, 前掲注 207

③ PETs 導入により特に恩恵を受けると思われるセクター・アプリケーション・分析方法
④ PETs 促進のために使用・改正・導入が可能な規制等
⑤ PETs 促進のために使用・改正・導入が可能な法令等
⑥ 前述の他に PETs 促進のために使用・改正・導入が可能なメカニズム
⑦ PETs 導入に際するリスク
⑧ PETs 導入に有益な既存のベストプラクティス
⑨ 前述の他に PETs 導入に対する課題、
⑩ その他 PETs 導入に関連する情報[209]、である。

その結果、各界の 70 を超える回答者からコメントがあり[210]、当該コメントは NITRD の公式ホームページ上で公開されている。回答者の業界カテゴリーとしては民間企業（Accenture, Amazon Web Services, Deloitte Consulting, IBM Research, Intel Corporation, Google, Mastercard, Meta, Mozilla, NTT Research, Visa Inc）、教育機関（Carnegie Mellon University, Georgetown Massive Data Institute, University of Southern California Information Sciences Institute）及び個人が主となっている。

具体的な PETs 技術としては、全体的に、差分プライバシー（differential privacy）、連合学習（federated learning）、合成データ（synthetic data）、並びに準同型暗号（homomorphic encryption）に関する言及が回答の中では多く見受けられる。回答者の声については、業界や業種によって様々であり必ずしも一貫性があるとは言えないものの、例えば、PETs 導入には依然として高いコストが求められることから適切なインセンティブが必要であるというコメント[211]や、コンプライアンス基準（「匿名化」等の定義）を明確化しつつも、当該基準を遵守するための技術的アプローチについては柔軟性を保つべきという声が挙げられている要である[212]。また、非識別化（de-identification）されたデータはデータ保護法の適用範囲外にする等[213]、一定の PETs を施したデータを法の規制対象に含めない方が好ましいというコメントも見られるとのことである[214]。

---

[209] Office of Science and Technology Policy, *Request for Information on Advancing Privacy-Enhancing Technologies* (Jun, 2022), https://www.nitrd.gov/request-for-information-on-advancing-privacy-enhancing-technologies/

[210] ただし、回答者によっては前述の内いくつかのトピックに回答を限定した者も多く、また回答のフォーマットもそれぞれ異なっている。

[211] Meta, *Request for Information (EFI) on Advancing Privacy Enhancing Technologies* (Jul, 2022), https://www.nitrd.gov/rfi/2022/87-fr-35250/Meta-PET-RFI-Response-2022.pdf 6 頁; Carnegie Mellon University, *Request for Information (EFI) on Advancing Privacy Enhancing Technologies* (Jun. 2022), https://www.nitrd.gov/rfi/2022/87-fr-35250/Carnegie-Mellon-University-PET-RFI-Response-2022.pdf 10 頁

[212] Visa Inc, *Request for Information (EFI) on Advancing Privacy Enhancing Technologies* (Jul, 2022), https://www.nitrd.gov/rfi/2022/87-fr-35250/Visa-PET-RFI-Response-2022.pdf 2 頁

[213] Amazon Web Services (AWS), *Request for Information (EFI) on Advancing Privacy Enhancing Technologies* (Jul, 2022), https://www.nitrd.gov/rfi/2022/87-fr-35250/Amazon-Web-Services-PET-RFI-Response-2022.pdf 4 頁; Google, *Request for Information (EFI) on Advancing Privacy Enhancing Technologies* (Jul. 2022), https://www.nitrd.gov/rfi/2022/87-fr-35250/Google-PET-RFI-Response-2022.pdf 7 頁

[214] Mastercard, *Request for Information (EFI) on Advancing Privacy Enhancing Technologies* (8 Jul. 2022), https://www.nitrd.gov/rfi/2022/87-fr-35250/Mastercard-PET-RFI-Response-2022.pdf 3 頁

（3）匿名化等に関する連邦取引委員会（FTC）の動向

2022 年 7 月 11 日、FTC 副所長代理を務めるクリスティン・コーエン氏は、収集した個人データの匿名化を謳う企業等に対し、当該データが実際に匿名化されていない場合には、連邦取引委員会法（FTC Act）に違反する「詐欺的な取引行為（deceptive trade practice）」[215]として厳しく追及する旨表明した[216]。FTC は、主に自身が出す命令等を通じて、テクノロジー発展の促進に貢献している。当該発言は、2022 年 6 月に、人工的な妊娠中絶の権利を認めた 1973 年の「ロー対ウェイド判決」を米国最高裁が覆したことで、州検察側が中絶希望者を起訴するために個人に関するデータをテック企業等から取得する等といった、プライバシーに関する懸念が生じたことに起因すると思われる。コーエン氏は、企業が匿名化を謳うデータの多く（特に位置情報）が実際は再識別可能であり、収集されたデータの匿名性について誤った主張をしている企業に対して FTC が厳しい姿勢で臨むと述べている[217]。

また、FTC によるプライバシー事案の制裁件数も安定的に推移しており、企業が FTC により処罰を受けたプライバシー及びセキュリティ関連の事例として、2021 年に 7 件、2022 年は 7 件、2023 年にも既に 1 件の案件を公表している。一例は以下のとおりである。

- FTC は、カリフォルニアを拠点とするオンライン広告プラットフォームである OpenX Technologies, Inc.が、2021 年 12 月に 13 歳以下の児童に関する個人データを保護者の同意無く収集したとして申立てし、2 百万米ドルの示談命令を下した[218]。
- 2022 年 4 月、FTC は、Kurbo, Inc.及びその子会社である WW International, Inc.（旧社名：Weight Watchers）を、13 歳以下の児童の個人データの不正取得やセンシティブな個人データの無期限の保持等に関して申し立てし、示談命令を下した[219]。
- 2022 年 5 月、FTC は Twitter, Inc.が 2014 年～2019 年にかけて、2 要素認証等の「セキュリティ目的で」収集したユーザー情報（電話番号及びメールアドレス）

---

[215] FTC へのインタビューによれば、当局による取り締まりの基準は、特定の行為がいかに「詐欺的（deceptive）」もしくは「不公平（unfair）」であるかであり、管理者や処理者といったカテゴリーを考慮して判断するものではないとのことである。例えば、PETs の間違った使用はデータ漏洩等に類似する危害をもたらす場合があり、その際当該行為が「不公平」と見なされる可能性がある。また、PET 使用について誤解を招く発言等があった場合、当該行為が「詐欺的」と見なされることもあり得るとのことである。

[216] JD Supra, LLC, *Anonymization v. De-Identification, Post-Dobbs; Rumblings from the FTC* (Jul, 2022), https://www.jdsupra.com/legalnews/anonymization-v-de-identification-post-6960540/

[217] PCMag, *FTC to Crack Down on Sites That Claim Your Data Is 'Anonymized' When It's Not* (Jul, 2022), https://www.pcmag.com/news/ftc-to-crack-down-on-sites-that-claim-your-data-is-anonymized-when-its

[218] Federal Trade Commission, *Advertising Platform OpenX Will Pay $2 Million for Collecting Personal Information from Children in Violation of Children's Privacy Law* (Dec, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/12/advertising-platform-openx-will-pay-2-million-collecting-personal-information-children-violation

[219] Federal Trade Commission, *FTC Takes Action Against Company Formerly Known as Weight Watchers for Illegally Collecting Kids' Sensitive Health Data* (Mar, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-company-formerly-known-weight-watchers-illegally-collecting-kids-sensitive

が、ターゲット広告等のセキュリティ以外の目的に使用されていたとして、当該行為が詐欺的であるとし、当該ユーザー情報の収集を必要としない認証方法を設けるよう求めた[220]。

- 2022 年 6 月、FTC は、CafePress に対し、社会保障番号を含む消費者のセンシティブな個人データの保護措置に不備があり、また大規模なデータ漏洩を隠蔽しようと試みたことを理由に、500,000 米ドルの罰金や改善措置を求める示談命令を下した[221]。
- 2022 年 8 月、FTC は Kochava Inc.に対し、医療機関や宗教施設等、センシティブな場所への出入りを把握できる位置情報を、億を超える台数の携帯機器から取得し販売したとして、訴訟を起こした[222]。

なお、データ保護関連の取り締まりにおいて、FTC による判断基準は、特定の行為が「詐欺的（deceptive）」又は「不公平（unfair）」であるかであり、PETs の使用は必ずしも必要とされない。開発環境や業界基準、時代に沿った「合理的な保護（reasonable security）」が求められ、包括的に柔軟性をもって判断される。「詐欺的」とは、合理的な消費者を欺く、重要な行為又は不作為を指し、例えば、企業が消費者に対し、個人データと暗号化や匿名化を謳ったものの、当該データの非暗号化や非匿名化が可能であった場合、この発言が(意図的でなかったとしても)詐欺的と見なされる可能性がある[223]。対して、「不公平」とは、消費者によって合理的に回避することができず、また対消費者あるいは競合上の利益によって相殺されない、実質的な損害を消費者に与える、又はその可能性を含む行為又は不作為を指す。

また、FTC による制定が予定されている「商業監視及びデータセキュリティに関する貿易規制規則（Trade Regulation Rule on Comemrcial Surveillance and Data Security）」については、パブリックコメントの募集期間が一度、2022 年 11 月 21 日まで延長されており[224]、1 万を超えるコメントが寄せられたものの、今後 FTC により採決を行い草案の作成をした後に再度コメントを募ることとなり、当該スケジュールに関する期日等は定められていないとのことである。

（4）その他米国における PETs 関連の研究開発の現状について

---

[220] Federal Trade Commission, *On FTC's Twitter Case: Enhancing Security Without Compromising Privacy* (May, 2022), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2022/05/ftcs-twitter-case-enhancing-security-without-compromising-privacy

[221] Federal Trade Commission, *FTC Finalizes Action Against CafePress for Covering Up Data Breach, Lax Security* (Jun, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-finalizes-action-against-cafepress-covering-data-breach-lax-security-0

[222] Federal Trade Commission, *FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations* (Aug, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other

[223] すなわち、データの非識別化について企業が主張する場合、処理者等による再識別化は不可能であり、また、企業側が自身のデータ保護措置が高水準に保たれていることを確認していなければならない。

[224] Federal Trade Commission, *Trade Regulation Rule on Commercial Surveillance and Data Security* (Oct, 2022), https://www.federalregister.gov/documents/2022/10/20/2022-22813/trade-regulation-rule-on-commercial-surveillance-and-data-security

米国では現在、PETs に関する研究開発は、全米科学財団（National Science Foundation）、米国標準技術局（National Institute for Standards and Technology）、米国国立衛生研究所（National Institutes of Health）、米国エネルギー省（U.S. Department of Energy）、米国退役軍人省（U.S. Department of Veterans Affairs）、疾病予防管理センター（Centers for Disease Control and Prevention）、国防高等研究計画局（Defense Advanced Research Projects Agency）等の、米国政府内で研究資金を受託している機関で行われている。このような外部研究は、PETs の商業的なソリューションの開発のためではなく、主に学術及び非営利活動の分野で行われている[225]。

6　調査対象国・法域における PETs の利用に関する調査結果

本調査の結果明らかとなった対象国・法域における PETs の利用に関する調査結果は次のとおりである。

調査項目	調査結果
個人情報（personal data）を暗号化（秘密分散を含む。以下同じ。）した場合に個人情報以外の情報分類への変更の有無	現行法では、特に見当たらない。
個人情報を暗号化することにより、軽減される義務・恩恵	現行法では、特に見当たらない。
個人情報を用いて二者以上が有する個人情報について秘密計算を行うための要件・手続と法律上の規制の有無	現行法では、特に見当たらない。
二者以上がデータを提供してデータ分析事業者が関わる場合のそれぞれの法律上の関係性	現行法では、特に見当たらない。
個人情報を匿名化/仮名化することにより、軽減される義	HIPAA の下での基準に沿って個人データの非識別化が行われた場合、当該データは HIPAA 及び CCPA の適用を逃れることができる。

[225] OECD, 前掲注 41・34 頁。

務・恩恵	
義務軽減・恩恵のために、匿名化/仮名化以外の要件（ある場合）。	現行法では、特に見当たらない。
プライバシー強化技術を用いることによる個人情報保護法等上の法的なメリット（義務の軽減、恩恵等）	再識別を困難とする PETs（例：差分プライバシー）を使用することで、一旦非識別化されたデータが再識別されるリスクを軽減し、再識別による CCPA や HIPAA 上の規制を回避することが可能となる。

第5　カナダ

1　プライバシー強化技術（PETs）の名称・技術の概要

（1）調査対象国において、個人データを保護したままで分析等を行うプライバシー強化技術として注目あるいは実用化されている名称と技術の概要。

（1）PETs の定義

ア　関連法令の定め

連邦法として、民間部門を規律する「個人情報保護及び電子文書法」（Personal Information Protection and Electronic Documents Act。以下「**PIPEDA**」という。）においては PETs の定義規定を設けていない。

カナダの個人情報保護に関する監督機関であり法執行を行う「カナダプライバシーコミッショナーオフィス」（Office of the Privacy Commissioner of Canada）（以下「**OPC**」という。）へのインタビューによれば、その理由は、PETs は、カナダにおいて新しい研究分野であり、その定義、基準、恩恵及びリスクに関するパブリック・コンサルテーションについての共通認識を未だ得られていないから、とのことである。

イ　Office of the Privacy Commissioner of Canada によるまとめ

OPC が作成したレポート[226] [227]（以下まとめて「**OPC レポート**」という。）によると、PETs について一般的に使われる定義は存在しないものの、共通する特徴は、以下であるとまとめられている[228]。

- プライバシーの原則及び法律に違反するリスクを軽減又は排除する
- 個人についてデータの保有量を最小限に抑える
- 個人が自身に関する情報を管理する権限を常に有する

（2）PETs の種類

OPC レポートにおいては、(3)ア（PETs 利用の目的）において説明する PETs の目的を達成するため、以下の複数の PETs の機能又は能力が組み合わせて使用されることが想定されるとされている。

インフォームドコンセント	個人が何について同意しているのか明確に理解することを要求すること

[226] OPC, *Privacy Enhancing Technologies – A Review of Tools and Techniques* (November 2017) https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/
[227] OPC, *Privacy Tech-Know blog: Privacy Enhancing Technologies for Businesses* (April 12, 2021) https://priv.gc.ca/en/blog/20210412/
[228] OPC, 前掲注 226 内の脚注 6

（Informed consent）[229]	
データ最小化（Data Minimization）	サービスやアプリケーションにおいて厳密に必要最小限の情報のみを処理することを要求すること
データ追跡（Data Tracking）	個人が個人情報を管理するために、提供した情報に関して、いつ・誰に・どのような状況であったかを記録・保存・参照する方法のこと
匿名化（Anonymity）	ユーザーが希望する匿名性の程度を選択できるようにすること 当該技術を用いることにより、ユーザーは、自身が希望する匿名性の程度を選択できるようにすることができる（たとえば、仮名、アノニマイザー、又は匿名データの資格情報を使用）。
コントロール（Control）	個人が第三者に開示する情報の種類や量を制限できるようにすること
契約条件の交渉（Negotiation of terms and conditions）	個人が契約条件を個別の契約として交渉できること
技術的な施行（Technical enforcement）	個人が契約条件を交渉できる場合、利用規約によりオンラインサービスプロバイダーと商人との間の技術的な構築を強制すること
適用のリモート監査（Remote audit of enforcement）	オンラインサービスプロバイダーや加盟店が提供する利用規約の施行をリモートで監査する機能を個人に提供すること
法的権利の使用（The use of legal rights）	データ保護法・プライバシー法が規定する、組織が保有する個人情報にアクセスする権利、情報の正確性と完全性に関して異議を述べる権利、修正する権利等の権利行使に関して、権利行使のプロセスを自動化すること
合成データ（Synthetic date[230]）	実際のデータと同じ統計的特性を保持することを目的としてアルゴリズムによって偽のデータを作成すること 識別可能なデータのように見えるという特徴がある。 以下のとおり賛否両論や留意すべき点がある高度な非識別化技術である。 ＜肯定的な意見＞

[229] OPC,前掲注 226

[230] OPC, *Privacy Tech-Know blog: When what is old is new again – The reality of synthetic data* (October 12,2022), https://www.priv.gc.ca/en/blog/20221012/

	・再識別を狙うための従来型の攻撃からの保護が可能 ・高次元のデータセットの統計的特性を捉えることが可能 ・非識別化プロセスをより高度に自動化することが可能 ＜否定的な意見＞ ・ソースデータの記録が合成データ内に残存する場合、依然として再識別が可能 ・一般的には属性の漏洩を防ぐことが出来ない ＜留意すべき点＞ ・人工知能及び機械学習システムにおけるバイアスを再現する可能性がある。 ・合成データと他の非識別化技術を組み合わせることで、プライバシーと実用性の間で同じか同程度のトレードオフが発生する。

また、OPC は、具体的に以下の 4 種の PETs に言及している。連合学習や差分プラバシーについては、理論的な開発が進んでいるものの、その複雑性から企業における実際の導入はほとんどない。今後 10 年間の導入事例が注目されるべきであるとされている[231]。

連合学習（Federated Learning）	データそのものを共有することなくデータを分析し、そのデータに基づいて意思決定又は予測を行うための方法をいう。 企業が複数のデバイスやデータソースにまたがってプライバシーを保護したデータ分析を行うことに寄与する。
差分プライバシー（Differential Privacy）	データ連携や再構成攻撃の可能性を大幅に低減するために使用できる多くのツールの 1 つ。 暗号分野で生まれた概念であり、組織が保有する数学的に定義された量のノイズ（偽のデータ）を加えることで、元のデータに誰の何についてのデータが含まれていたか知ることを非常に困難にし、プライバシーを保護する方法をいう。
準同型暗号（Homomorphic Encryption）[232]	データを暗号化したままデータ処理ができる暗号化方式をいう。

[231] OPC, 前掲注 227

[232] Statistics Canada,Privacy Preserving Technologies Part Two: Introduction to Homomorphic Encryption(March 3,2022), https://www.statcan.gc.ca/en/data-science/network/homomorphic-encryption

秘密計算技術（Secure Multiparty Computation）[233]	データを暗号化したまま計算できる技術をいう。

OPC へのインタビューによれば、カナダで最も頻繁に使用されている PETs は匿名化であり、このうち最も使用されていると考えられているのは「k-匿名性」（匿名化されたデータがもつ特性の 1 つ）とのことであるが、最近より使われてきている匿名化技術は「合成データ」とのことである。また、カナダでの PETs の議論の状況については、実際に利用されている技術という訳ではないものの、中央銀行のデジタル通貨との関連において準同型暗号やゼロ知識証明についての議論が頻繁になされ、学術的な場において差分プライバシーや連合学習について時折議論されるとのことである。

なお、OPC は、2004 年に(i)プライバシーに関する独立した非営利の研究を支援する、(ii)プライバシー政策の開発を促進する、(iii)カナダにおける個人データの保護を促進する目的でプログラムを創設した。OPC は、このプログラムにおいて、過去に特に PETs に関連する提案を募集し、財政的貢献をしたことがある[234]。

(3) PETs 利用のインセンティブ

ア PETs 利用の目的

OPC レポートによると、PETs が利用される主要な目的は、リスクへの対処と個人のプライバシー保護である[235]。

すなわち、PETs は、個人を特定する情報の開示、データトラフィックと個人を特定する情報のリンク、データコンテンツ転送に関連した位置情報の開示、ユーザープロファイルの開示その他の情報開示自体に関する潜在的又は現実的なリスクに対処することを目的とするものである。

また、個人が、サービスプロバイダーにどのような情報を共有するか、いかなる状況で当該情報を共有するか、第三者がその情報をどのような目的で使用するかを決定できるようにすることで、個人のプライバシーを保護することも目的としている。これらの目的を達成するため、複数の PETs が組み合わせて使用されることが想定される。

イ PETs 利用の利点

---

[233] OPC, *Communiqué: Promoting Data Free Flow with Trust and knowledge sharing about the prospects for International Data Spaces* (September 8, 2022), https://www.priv.gc.ca/en/opc-news/speeches/2022/communique-g7-220908/、上記に PETs の技術の 1 つとして記載されている。

[234] OECD, 前掲注 41

[235] OPC, 前掲注 226

OPC レポートにおいて、PETs を利用する利点として挙げられているのは以下である[236]。

- PETs のうち連合学習は、個人のプライバシーを保護しつつ、企業が複数のデバイスやデータソースにおけるデータ分析を行うのに役立つ。
- PETs のうち差分プライバシーは、データ連携・データ再構築への攻撃の可能性（the likelihood of data linkage and reconstruction attacks）を大幅に減少させるために使用できるツールの 1 つとして考えられている。

また、法的な観点から言えば、「消費者プライバシー保護法（Consumer Privacy Protection Act）」以下「**カナダ CPPA**」という。）の改正法案においては、匿名化された情報は、カナダ CPPA の規制の対象外となる[237]。また、個人情報が一旦、匿名化処理されると、第三者提供が自由となると考えられる等の点で、利用のインセンティブがあると言える。なお、他方、非識別化された情報は、依然としてカナダ CPPA の規制の対象となる[238]が、研究開発目的や社会的に有用な目的等、一定の場合に非識別化された情報に関連する個人の認識又は同意なしに特定の使用・開示が許される[239]。また、カナダ CPPA 上の第三者提供に関する一定の規定は非識別化された情報については適用されない[240]。

（4）PETs 利用の障壁[241]

前述(2)のとおり、PETs には様々な種類があるが、現在のところ、研究の場面から市場や人々の生活において浸透したものがほとんどない理由としては、以下の点が指摘されている。

インセンティブの欠如	現在の経済環境や規制環境による限り、例えば、PETs 利用に関する同意に関連する技術を浸透させるインセンティブがほとんどない。このため、技術の更なる開発だけでは大きな変化につながる可能性は低い。オンラインでは、ターゲット広告のための個人情報の収集と処理に収益源を置いているが、個人情報処理に関する許可は黙示の同意に依存している。ユーザーが行動を起こしやすくする同意技術、特に、オプトアウトに

[236] OPC, 前掲注 227

[237] Parliament of Canada, BILL C-27 (first reading, June 16, 2022) PART 1 Consumer Privacy Protection Act 第 6 条第 5 項 https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading

[238] Parliament of Canada, 前掲注 237, BILL C-27 PART 1 Consumer Privacy Protection Act 第 2 条第 3 項

[239] Parliament of Canada, 前掲注 237, BILL C-27 PART 1 Consumer Privacy Protection Act 第 2 条第 3 項、第 21 条、第 22 条 1 項、第 39 条第 1 項

[240] 第 Parliament of Canada, 前掲注 237, BILL C-27 PART 1 Consumer Privacy Protection Act 第 2 条 3 項、第 56 条第 2 項（c）、第 71 条第 3 項

[241] OPC, 前掲注 226

	ついては、収益源を減らす可能性があることから PETs 利用を促進するインセンティブがない。
技術の複雑性	PETs は平均的な消費者には複雑過ぎ、操作には専門的な知識やスキルが必要になる。
需要の欠如	利用可能なツールに関する知識の欠如に一部起因している可能性があるが、プライバシー保護に対する消費者の需要が少ないという点も挙げられる。
政府の意向	政府が、イノベーションを阻害することをおそれ、プライバシー保護に関する規制を望まない点も、PETs 利用の障壁になっている可能性がある。
技術に対する信頼性	PETs のうちの多くは、試作段階や限られた試験での使用段階にあり、実際の使用や使用に伴う個人情報処理への影響を測定した経験が少ない。そのため、潜在的なユーザーは、PETs 技術を信頼しない可能性がある。
ネットワーク効果を享受しにくい点	一部の PETs 技術は利用される機会や場面が限定的なこともあり、いわゆる「ネットワーク効果」(より多くの人々がそれを使用するにつれて、商品やサービスの価値が高まる現象)を享受しにくいと考えられている点が PETs 促進の障壁になりうる。

2　データ保護法との関係、データ保護法上の論点

（2）上記において、個人情報、プライバシー保護に関する法律（以下「個人情報保護法等」という。）の観点から論点となっている点（過去論点となった点、事業者による改正要望、政府による改正予定の点も含む。）。

(1) データ保護法の概要 [242]

ア　現行法

カナダには、連邦法として、①公的部門を規律する「プライバシー法」(Privacy Act)、②PIPEDA が存在する。プライバシー法は、政府機関による個人情報の収集、利用及び開示に適用される [243]。PIPEDA は、商業活動における全ての個人情報の収集、利用及び開示について規制する。また、PIPEDA は、実質的にこれに類似する独自の法令を有していない全ての州の個人情報に適用される（現在、ケベック州、ブリティッシュコロン

[242] OPC, *Summary of privacy laws in Canada*（January 2018）https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

[243] プライバシー法第 2 条 https://laws-lois.justice.gc.ca/eng/acts/P-21/page-1.html#h-397177

ビア州及びアルバータ州に関しては、実質的にこれに類似する法令が存在する。）。なお、PIPEDA では、個人情報とは特定可能な個人に関する情報を意味する[244]。

イ　改正法案の概要[245][246]

(ｱ) 改正法案名

連邦政府は、PIPEDA を廃止し、以下の法律を制定することにより、プライバシー法を包括的に改正することを計画している（以下「**法案 C-27**」という。法案 C-27 は、2022 年 6 月に議会に上程されている。以下、後述の各法律を包括的に「**データ保護関連新法**」という。）[247]。

- カナダ CPPA
- 「個人情報・データ保護裁判所法（Personal Information and Data Protection Tribunal Act）」（以下「**PIDPTA**」という。）
- 「人工知能及びデータ法（Artificial Intelligence and Data Act）」（以下「**AIDA**」という。）
- カナダ CPPA、PIDPTA 及び AIDA の策定を含んだ「デジタル憲章実施法（Digital Charter Implementation Act）」（以下「**DCIA**」という。）

(ｲ) 改正法案の具体的内容

DCIA の第 1 部にはカナダ CPPA が規定されている。カナダ CPPA は、個人情報保護法及び電子文書法の一部を廃止し、カナダにおける商業活動のための個人情報の収集、使用、及び開示を規制する新しい法制度に置き換えるものである。これにより、カナダ CPPA は、既存の規制を維持しつつも、近代化あるいは拡張し、個人情報保護のために民間組織に新しい規制を課すものとなる。また、カナダ CPPA は、民間組織がこれらの規制を遵守するよう監督するという、OPC が担っている役割を強化するものになると考えられる。また、カナダ CPPA の下では、データを管理する組織は、物理的、組織的及び技術的なセキュリティにより個人情報を保護しなければならず、その保護の程度は情報の機密性に比例したものであることを要する。この点は、個人方法保護法及び電子文書法で定められていた要件が引き継がれている。加えて、カナダ CPPA の規制を遵守

---

[244] PIPEDA 第 2 条（1）　https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/page-1.html#h-416888

[245] The Government of Canada, *Bill C-27: An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts* (November 4, 2022) https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c27_1.html

[246] The Government of Canada, *New laws to strengthen Canadians' privacy protection and trust in the digital economy* (June 16, 2022), https://www.canada.ca/en/innovation-science-economic-development/news/2022/06/new-laws-to-strengthen-canadians-privacy-protection-and-trust-in-the-digital-economy.html

[247] なお、紙の記録に代わる電子的な代替手段に関する個人情報保護及び電子文書法の規定は「電子文書法（The Electronic Documents Act）」という新しい名称の下で維持される。

するための指針となるものが AIDA であり、この取り組みを支援するために AI・データ室の設置が予定されている[248]。

次に DCIA の第 2 部には PIDPTA が規定されている。これは、OPC が下した発行された命令に対する不服申立てを審理するための新しい行政裁判所を創設し、カナダ CPPA の下で創設された新しい行政罰の制度を適用する根拠となるものである。

更に、DCIA の第 3 部には AIDA が規定されている。これは、人工知能システムを用いた国家間及び州間の貿易及び商業を規制するための新しい措置を定めるものである。AIDA では、人工知能システムの設計、開発及び使用に関する共通の要件を確立することが予定されている。また、個人やその利益に重大な損害を与える可能性のあるデータや人工知能システムに関する特定の行為を禁止する規定も設けられている。

OPC へのインタビューによれば、本改正によりプライバシー保護の枠組みを近代化する目的としては、デジタル経済において個人のプライバシーが適切に保護されることを保証し、組織が情報にアクセスして責任を伴ったイノベーションを実現することを保証することにある。新しい要件により、情報の収集や使用において、より明確かつ透明性のある情報を提供する必要があるため、個人情報の取得がより困難になることも想定される。他方、組織が個人の同意なしに個人情報を扱う柔軟性を持つことも想定される。また、情報の悪用を阻止するために必要な監視を行うため、組織がデータの取扱方法についてより説明責任を果たし、時には OPC による命令や行政処罰に従うことも求められる。

なお、OPC へのインタビューによれば、法案 C-27 の目的の一つに、カナダが、EU の GDPR ルールの下において、引き続き妥当な立場を維持することがある。

(2) PETs と改正法案との関係

以下で述べるとおり、前述のデータ保護関連新法においては PETs に関連する規定が存在している。具体的には、カナダ CPPA に、匿名化（anonymization）と非識別化（de-identification）に関する規定が存在している。

OPC へのインタビューによれば、匿名化された情報は個人情報とは見なされないため、カナダ CPPA の保護対象とならない。他方、非識別化された情報は依然として個人情報として定義されるため一定の場合の除きカナダ CPPA の対象となる。このため、匿名化された情報と非識別化された情報の違いを法的に明確に定義することで、データを取り扱う事業者に対し適切な匿名化の取組みを促進し、また、匿名化のための標準又はベストプラクティスとなるべき技術の開発を促すことを目的としているとのことである。

また、カナダ CPPA においては、非識別化された情報は引き続きカナダ CPPA の対象となるため、データを取り扱う事業者にとって情報を非識別化するインセンティブがないようにも思えるが、非識別化された情報の使用又は開示に関する同意の要件や、非識

[248] OECD, 前掲注 41

別化情報に関する義務について例外を設けることで（6 において後述）、非識別化の取組や技術の開発に対するインセンティブはなおも存在するとのことである。

加えて、時間をかけて標準やベストプラクティスを開発することを可能にする意図で、匿名化や非識別化に関し特定の技術の使用には触れないかたちでの既定文言としており、かつ、現時点で特定のベストプラクティスとして想定されている技術がある訳ではないとのことである。カナダ CPPA 上に具体的な技術を念頭に置いた基準を設けてしまうと、時間の経過に伴う技術の発展に対応しない規定となってしまうからである。

次に、AIDA には、AI システムで使用するために匿名化されたデータを処理する者に対する規制が存在している。

なお、PETs との直接の関係については要検討であるが、法案 C-27 の第 55 条では個人情報の消去について規定されている[249]。同条では、組織は、組織の管理下にある個人情報の処分について個人から書面による要請を受けた場合、組織は、本人が、情報の収集、使用、又は開示に対する同意を全部又は一部撤回した場合に、実行可能な限り速やかにその情報を処分しなければならない、と定められている。

(3) PETs に関わるデータ保護法上の論点

ア　非識別化・匿名化・仮名化の区別[250][251][252]

(ｱ) 現行法

現行法上は、PIPEDA に匿名化の規定があるが、「de-identify」、「anonymize」及び「pseudonymize」を区別しておらず、匿名化された個人情報を同じように扱っている点が問題となっていた。

(ｲ) 改正法案

改正法案においては、以下のとおり、現行法の内容を改めようとする対応がなされているが、それでもなお、以下の論点が残されている。

---

[249] Parliament of Canada, 前掲注 237, BILL C-27

[250] FASKEN, *Under Bill C-27: Implications for Data Analytics(November 24,2022)*, https://www.fasken.com/en/knowledge/2022/11/24-anonymization-and-de-identification-under-bill-c-27#:~:text=The%20federal%20government%E2%80%99s%20proposed%20Consumer%20Privacy%20Protection%20Act,organizations%20create%20and%20use%20%E2%80%9Cbig%20data%E2%80%9D%20in%20Canada..

[251] Barry B.Sookman, *CPPA: problems and criticisms – anonymization and pseudonymization of personal information* (December 6,2022),https://www.mccarthy.ca/en/insights/blogs/techlex/cppa-problems-and-criticisms-anonymization-and-pseudonymization-personal-information

[252] Barry B.Sookman, *CPPA: identifying the inscrutable meaning and policy behind the de-identifying provisions* (December 7,2022),https://www.barrysookman.com/2020/12/07/cppa-identifying-the-inscrutable-meaning-and-policy-behind-the-de-identifying-provisions/

- カナダ CPPA では、匿名化（anonymization）[253]と非識別化（de-identification）[254]を明確に区別している。具体的には、匿名化が有効になされた場合、匿名化された情報はカナダ CPPA の範囲から除外されるものとする一方で、非識別化された情報は依然としてカナダ CPPA の対象となるとされているため、非識別化された情報の使用と開示は特定の場合を除き規制される(6 において後述。また、再識別行為に厳しい制限をかけている。）。しかし、前述例外要件を含めた不明確又は過度に厳格な匿名化・非識別化基準は、匿名化又は非識別化された情報の作成と使用を希望する組織にとっては基準が不明確であり、有用と考えられる情報の利用によってもたらされる組織の利益を阻害することになると考えられる [255]。これらの問題点を背景に、情報使用による利益と個人のプライバシー保護のバランスを探る観点から、カナダ CPPA に基づく匿名化基準と非識別化基準が 1 つの論点として議論されている。

  この論点について、OPC へのインタビューによれば、定義規定が不明確であるのは情報を匿名化するための最良の手段に関するベストプラクティスが発展することを可能にすることを意図しているものの、一方で再識別のリスクをゼロにすることは不可能にしており、法案審議中にも多くの関係者が匿名化の意味を解釈する際の合理的基準の必要性を指摘していたとのことである。

  また、OPC へのインタビューによれば、OPC は今後、業界の専門家と協力して匿名化と非識別化のための適切な技術に関するガイドラインを策定する可能性があるとのことであるが、仮に OPC が前述ガイドラインを策定しない場合であっても、OPC は利害関係者に対し、同人らが作成した業界規範を承認する機会を設ける予定であるとのことである。
- また、GDPR では匿名化・仮名化された一部の情報は規制されないにもかかわらずカナダ CPPA では規制される点からも議論されている（なお、GDPR が規定する仮名化（pseudonymization）は、一般にカナダ CPPA の非識別化（de-identification）と同義と考えられる。）。

---

[253] Sookman, 前掲注 251。匿名化とは、一般に受け入れられているベストプラクティスに従って、個人情報を不可逆的かつ永続的に変更し、直接的又は間接的に、いかなる手段によっても、情報から個人を特定できないようにすることをいう。

[254] Sookman, 前掲注 251。非識別化とは、個人を識別できる危険性は残るものの、個人情報を直接識別できないように修正することをいう。

[255] Dentons Data, *Best practices in data management – What organizations should know about de-identifying information in Canada* (May 31, 2022) https://www.dentonsdata.com/best-practices-in-data-management-what-organizations-should-know-about-de-identifying-information-in-canada ある組織が個人情報を匿名化するためにデータ変換を行った場合、当該組織は変換された当該データを匿名化された情報であってカナダ CPPA の対象ではないと見なす一方、規制当局は変換されたデータを非識別化された情報と見なす場合があり得る。この場合、当該情報は非識別化された情報に過ぎないためカナダ CPPA の対象となり、その結果、当該組織は想定に反しこのデータに関する法定要件を遵守する義務を負うことになってしまう点が指摘されている。

イ　匿名化に関する定義の統一性

各州法において、匿名化に関する規定が存在するが、連邦及び州毎にその定義が異なっており、統一的でないことが問題となっている。

この点に関連して、OPC へのインタビューによれば、既存の枠組みでは、カナダ CPPA は、各州のプライバシー保護法を実質的に類似したものとして指定し、州内の活動についてはそれが連邦法に優先することを認めており、また、指定されるための基準を定めた規則を発行する権限を各州に与える。この枠組みは、可能な限り各州のプライバシー保護法がカナダ CPPA に調和する内容を奨励するように設計される予定とのことである。

ウ　同意とプライバシー

OPC は、2016 年 5 月、「同意とプライバシー」と題する討議文書を公表した[256]。概要は、PIPEDA の要は同意であるという認識に基づき、スマートフォン、クラウド・コンピューティング等の技術や、個人情報への無制限アクセス及び自動処理等の企業実務の変化を踏まえ、同意モデルの改善又は代替策を提案し、また、主たる論点の概要を述べる、といったものであった。そのうち、同意モデルの代替策として匿名化が列挙されている。

エ　プライバシー影響評価（PIA）とは

データ保護影響評価（Data Protection Impact Assessment）（以下「**PIA**」という。）は、個人情報の利用が個人情報の保護（Data Protection）あるいはプライバシー（Privacy）に与える影響の程度を評価するものである。カナダでの取組状況[257][258][259]としては、カナダ財務委員会事務局（Treasury Board Secretariat）（以下「**TBS**」という。）が 2002 年に策定したプライバシー影響評価ポリシー（Privacy Impact Assessment Policy）により、行政機関にプライバシー影響評価（Privacy Impact Assessment）の実施が義務付けられた。なお、TBS は、2010 年に PIA 指令（Directive on Privacy Impact Assessment）を策定し、PIA に伴う政府の過度な負担を省き、効率化に努めている。更に、TBS は、2020 年に「サービスとデジタルに関する方針（Policy on Service and Digital）」を発表しプライバシー保護の必要性を概説した。この方針では、副大臣は「部門の情報やデータを管理するあらゆる計画や戦略の中でもプライバシーが扱かわれることを確実にする」責任を負うものとされている。これは PETs に明確に言及していないが、新技術の採用計画（PET

[256] OPC, *Consent and privacy* (May 2016), https://www.priv.gc.ca/media/1806/consent_201605_e.pdf
[257] The Government of Canada, *Privacy Impact Assessment Policy* (May 2, 2002), https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=12450
[258] The Government of Canada, *Directive on Privacy Impact Assessment* (April 1, 2010), https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=18308
[259] OPC, *Expectations: OPC's Guide to the Privacy Impact Assessment Process* (March 2020),https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003

を含む可能性がある）を含め、カナダ政府が実施するあらゆる計画や取り組みに適用されるという意味で PETs に関わる話である。[260]。

また、OPC も、効率的な PIA の運用のため、政府が参照すべき PIA のガイドを策定している。これによれば、政府は次の公正な情報取り扱い 10 原則に沿った PIA の実施が推奨されているが、PETs についての言及は特に見当たらなかった。

① 責任の原則（Accountability）
② 目的明確化の原則（Identifying Purpose）
③ 告知・同意の原則（Consent）
④ 収集制限の原則（Limiting Collection）
⑤ 利用・開示・保持制限の原則（Limiting Use, Disclosure, and Retention）
⑥ 正確性の原則（Accuracy）
⑦ 安全保護措置の原則（Safeguards）
⑧ 公開の原則（Openness）
⑨ 個人参加の原則（Individual Access）
⑩ コンプライアンス挑戦の原則（Challenging Compliance）

オ　その他

PETs の成熟性や安全性に関する具体的な基準について調査したものの、この点を特に明示する公開文献は不見当であった。また、仮に PETs を利用する場合、個人情報法制上、利点が生じる PETs の種類についても調査したものの、この点を特に明示する公開文献は不見当であった。

3　各種ガイドライン

（3）プライバシー強化技術についてデータ保護機関等の公的機関が公表するガイドライン等（個人情報保護法等と当該技術の関係についてのガイドライン等）の名称と主な論点。

データ保護機関等の公的機関が公表するプライバシー強化技術についてのガイドライン等に関する情報は以下のとおりである。

(1) オンタリオ州

オンタリオ州は、2016 年 6 月、「構造化データにおける非識別化ガイドライン（De-identification Guidelines for Structured Data）」を公表した [261]。

(2) ブリティッシュコロンビア州

[260] OECD, 前掲注 41
[261] Information and Privacy Commissoner of Ontario, *De-identification Guidelines for Structured Data* (June 2016), https://www.ipc.on.ca/wp-content/uploads/2016/08/Deidentification-Guidelines-for-Structured-Data.pdf

ブリティッシュコロンビア州は、2021 年 10 月、部分的に「非識別化・匿名化された記録の開示に関するガイダンス（De-Identification Guidance）」を公表した。同ガイダンスには、個人情報開示のプロセスに関する記載がある [262]。概略すると次の①から③のとおりである。

① 「情報の自由及びプライバシーの保護に関する法律」（The Freedom of Information and Protection of Privacy Act）」の第 3 部又は他の法律によって開示が許可されているかを検討する。
② 開示が許可されている場合、非識別化・匿名化の内容が適切かどうか、例えば非識別化が開示に関連するリスクを適切に低減しているか検討する。
③ 部分的に非識別化・匿名化された情報を開示するビジネス上の必要性又は根拠を検討する。

（3）有意な同意取得のためのガイドライン

OPC は、2021 年 8 月、「有意な同意取得のためのガイドライン（Guidelines for obtaining meaningful consent）」を改定した [263]。これは、組織が個人情報を収集、使用及び開示に当たり同意を取得すべき場合に、以下の基本原則に従うことを規定している。

① 同意を得るに際し、収集される個人情報、個人情報の共有先、個人情報の収集・使用・開示の目的、リスク等の重要な要素を強調すること
② 個人情報の詳細の程度と取得のタイミングを制御できるようにすること
③ 個人に「はい」「いいえ」の明確な選択肢が提供されること
④ 様々なコミュニケーションツールを用いて個人情報の取扱いについて説明すること
⑤ 同意のプロセスにはユーザーの視点を考慮すること
⑥ 同意を継続的なプロセスとし、フォローアップ等の措置をとること
⑦ 説明責任を果たすこと

4　その他の法令の規定

（4）その他、プライバシー強化技術が普及していく上で、論点となりうる法令の規定（個人情報、プライバシー、データ保護を目的とする規定、データの越境移転を伴う場合の規定）の概要。

[262] Gorvernment of BRITISH COLUMBIA, *De-Identification Guidance* (October 2021), https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-privacy/privacy-impact-assessments/sharing-personal-information/de-identification_guidance.pdf
[263] OPC, *Guidelines for obtaining meaningful consent* (May 2018),https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/

その他法令に関する論点としては以下の 2 点が挙げられる。

(1) AIDA 法案における人工知能に関する点[264]

法案 C-27 中の AIDA 案は、AI 規制の法的枠組みについての草案であり、欧州委員会の人工知能法の後を追う形で議会に上程されたものである[265]。

AI システムで使用するために匿名化されたデータを処理する者は、①データを匿名化する方法、②匿名化されたデータの使用又は管理について（今後の規則に従って）対策を講じなければならないものとされている。

(2) 越境移転のガイドラインの点[266][267]

ア　現行法

PIPEDA はデータの越境移転に関して具体的な制約を定めていない。ただし、国際的なデータの移転を含め、第三者としての情報処理業者への個人情報の移転は全て、PIPEDA 上の説明責任原則に従うことになる。そのため、こうしたデータの移転を行う組織は、その保有又は保管する個人情報に関し、処理のために当該情報が第三者に移転された後も引き続き責任を負う。当該組織は、当該処理業者による個人情報保護水準を同程度とするために、契約その他の手段を利用するものとする。PIPEDA を含むカナダの法律によると、データの越境移転について、国の監督機関に届出又はその許可を得る必要はない、とされている。

この点について、OPC へのインタビューによれば、OPC は「国境を越えた個人データ処理に関するガイドライン（Guidelines for processing personal data across borders）」[268]（以下「**越境個人データガイドライン**」という。）を作成しており、これによれば、PIPEDA4.1.3 の「同等レベルの保護（Comparable level of protection）」とは、個人情報を提供された第三者が、当該個人情報が移転されなかった場合に受ける保護と（全面的に同じレベルでなければならないという訳ではなく）一般的に考えて同等のレベルの保護を提供しなければならないことを意味するとのことである。

また、OPC へのインタビューによれば、越境個人データガイドラインは「情報が処理される場所がカナダであろうと外国であろうと関係なく、組織は、情報が第三者の処理者のもとにある間、不正な使用や開示から保護するためにあらゆる合理的な措置を講じなければならない」と規定する。また、「個人情報を第三者に提供する組織は、個人情報が当該第三者によって適切に保護されていることを保証するために、当該第三者が、

---

264 FASKEN, *The Regulation of Artificial Intelligence in Canada and Abroad: Comparing the Proposed AIDA and EU AI Act* (October 18,2022) ,https://www-fasken-com.translate.goog/en/knowledge/2022/10/18-the-regulation-of-artificial-intelligence-in-canada-and-abroad?_x_tr_sl=en&_x_tr_tl=ja&_x_tr_hl=ja&_x_tr_pto=sc

265 Parliament of Canada, 前掲注 237, BILL C-27 PART 3 Artificial Intelligence and Data Act 6 条

266 OPC, *Processing Personal Data Across Borders Guidelines* (1992), https://priv.gc.ca/media/1992/gl_dab_090127_e.pdf

267 OPC, *Guidelines for processing personal data across borders* (January 2009), https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127/

268 https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127/

個人情報を確実に保護できるようスタッフの教育や効果的なセキュリティ対策を含んだポリシーとプロセスを備えるようにしなければならない」、「個人情報を第三者に提供する組織は、第三者の個人情報の取扱状況を監査する権利を有し、正当な理由がある場合にはその権利を行使しなければならない」と規定している。

なお、越境個人データガイドラインには PETs の記載は見当たらない。

イ　改正法案

OPC へのインタビューによれば、カナダ CPPA は、州境を越えた個人情報の転送を意図したものではなく、現行法と同様に、国境を越えた情報の転送は制限されていない。しかし、情報を転送する組織は、カナダ CPPA に従い個人情報の保護を保証する責任を負い続け、組織がプライバシーについての懸念を抱かせるような管轄区域に個人情報を移転する場合、当該組織は移転についての透明性を確保することが求められる。

5　その他（政策、世論の動向等、関連事項で有用と考えられる事項）

PETs に直接･間接に関連すると考えられるその他の点として以下の 3 点が挙げられ、以下説明する。

(1) デザインによるプライバシー保護（Privacy by Design）[269]

デザインによるプライバシー保護とは、システムの企画・設計段階からあらかじめ個人情報及びプライバシーを保護する施策を組み込み、システムのライフサイクル全体を通して一貫したプライバシー保護の取組みを行う考え方をいう。デザインによるプライバシー保護の考え方は国際的な広がりを見せており、プライバシー論議を牽引する役割を果たしている。

デザインによるプライバシー保護は PETs にポジティブ・サム（互いに利益を得る）のアプローチを加えた考え方であり、PIA の元となる概念とされる。

Information and Privacy Commissioner of Ontario の 2013 年のレポート「監視の昔と今（SURVEILLANCE, THEN AND NOW）」の中で紹介されている Toronto Transit Commission Report（TTC レポート）では、PET の一例として、ビデオ監視カメラで撮影された個人の画像を見えなくするために使用できるオブジェクトベースの暗号化というものがあるとのことである。また、同 TTC レポートでは、新しい PETs の研究に常に注意を払い、可能な限りこれらの技術を採用するとの記載がなされているとのことである [270]。

デザインによるプライバシー保護を実行する技術や分野に制限はないが、2012 年に公表された「デザインによるプライバシー保護の運用」（Operationalizing Privacy by Design）101）の中で、9 つの適用分野が紹介されている。具体的には、監視カメラ、バ

---

[269] Information and Privacy Commissoner of Ontario,Privacy by Design The 7 Foundational Principles(January 2011), https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

[270] Information and Privacy Commissioner Ontario, Canada-SURVEILLANCE, THEN AND NOW:Securing Privacy in Public Spaces, pp35-36, (June,2013), https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-surveillance.pdf

イオメトリクス、スマート・メーター及びスマート・グリッド、モバイル機器/通信、近距離無線通信（Near Field Communication）、RFID 及びセンサー技術、IP 位置情報、遠隔医療、ビッグデータ及びデータ分析である。

デザインによるプライバシー保護の考え方それ自体はプライバシー強化技術であると直接的に言える訳ではないものの、PETs の実用化の背景にある考え方であることから本項に記載したものである。また、PETs に関する規定がなくとも、機関は、プライバシー・バイ・デザイン等のプライバシー保護の構築に関連する原則を適用し、ベストプラクティスに基づき、新しいプログラムを実施したり、既存のプログラムを更新したりすることがある。

（2）De-identification（非識別化）の方法 [271]

De-identification（非識別化）の方法としては以下の 5 つが挙げられる。

調査項目	調査結果
再編集（Redaction）	記録から機密データを消去又は抹消すること
サプレッション（Suppression）	少人数のグループやユニークな特徴を持つ個人を特定できないように、配布前にデータ（例えば、表のセルや行、又はレコードのデータ要素）を削除すること
ぼかし（Blurring）	1 つ又は複数のデータ要素を組み合わせることにより、データの精度を下げること。これには以下が含まれる。 • 集計（Aggregation）： 個々の被験者のデータを他の十分な数の被験者と組み合わせて、単一の被験者の属性を偽装すること（例えば、個人の値の代わりにグループの平均値を報告すること）。 • 一般化（Generalization）： ある範囲の値を収集又は報告すること（例：生年月日の代わりに年齢又は年齢範囲を使用）、個々のデータをセットのメンバーとして含めること（例：固有のケースを組み込んだカテゴリーを作成）、正確な金額の代わりに丸められた値を報告すること
マスキング（Masking）	1 つのデータ要素をランダムな値や作り物の値、又はデータセット内の別の値で置き換えること、これは手動又はアルゴリズムを使用して行うことができ、多くの場合、以下のテクニックと関連している。

[271] SAN JOSÉ STATE UNIVERSITY, *Table of De-Identification Techniques*, https://www.sjsu.edu/research/docs/irb-deidentification-techniques-table.pdf

	• 仮名化/コード化（Pseudonymization/Coding） • 実名を偽名に、実値を偽値に置き換えること • 摂動（Perturbation）： 機密情報を、現実的だが真正ではないデータ（合成データ）で置き換えたり、あらかじめ決められたマスキングルールに基づいて元のデータを変更したりすること • スクランブル/暗号化（Scrambling/Encryption）： データをアルゴリズムでスクランブルし、適切な鍵にアクセスできる者のみが暗号化されたデータを見ることができる • ノイズと差分プライバシー（Noise and Differential Privacy）： カテゴリー変数の値をランダムに誤分類することでエラーを発生させる統計的手法
サブサンプリング（Subsampling）	データ全体ではなく、データ全体からランダムに抽出したサブサンプルを公開すること

（3）個人健康情報を非識別化する際の考慮要素[272]

オンタリオ州の医療プライバシー法である「Personal Health Information and Protection Act」（以下「**PHIPA**」という。）は、「個人健康情報」（Personal Health Information）の収集、使用及び開示について規定している。

オンタリオ州の情報・プライバシーコミッショナー（IPC）は、非識別化情報が PHIPA の適用外であると述べている。これは、非識別化情報に法的なプライバシー保護を要求することにより、非識別化のインセンティブの低下や、不必要な負担を発生させる可能性があるためである。

その一方、IPC は、個人情報を非識別化するプロセスは、PHIPA における情報の「使用」と見なされると明言している。これは、個人健康情報は高度な機密性を有するため、個人健康情報を取り扱う医療クリニック群（カストディアン）に対し、個人医療情報の収集、利用、開示に責任を持たせるという観点に基づくものである。

（4）連邦裁判所の判決

カナダ連邦裁判所は、2023 年 1 月 25 日、カナダの情報公開制度の下で、個人に関する情報をどの程度まで匿名化して公開することができるかについての判決を下した。同

[272] DENTONS, *Considerations for de-identifying personal health information: Guidance from Ontario's Information and Privacy Commissioner* (June 24,2022) https://www.dentons.com/en/insights/articles/2022/june/23/considerations-for-deidentifying-personal-health-information

裁判所は、プライバシーの権利は、情報へのアクセスよりも「最優先」であると認識されなければならないと判断した。[273]。

6　調査対象国・法域における PETs の利用に関する調査結果

本調査の結果明らかとなった対象国・法域における PETs の利用に関する調査結果は次のとおりである。

調査項目	調査結果
個人情報を匿名化/非識別化することにより、軽減される義務・恩恵	**【現行法】** 匿名化又は非識別化される前の情報とこれらがなされた後の情報を比べると、情報に対する規制の有無や程度に差があることから、以下この点を説明する。 前提として、個人情報の収集・使用・開示の方法については PIPEDA 上、以下を含む様々な規制の対象となる [274]。 • 個人情報収集の目的が収集開始以前の段階で特定 • 法律で別途認められる場合を除き個人情報の収集、利用又は開示には、個人への告知及び当該個人の同意を必要とすること • 個人情報の収集が組織が特定した目的のために必要なものに限定されること。情報が公正かつ適法な手段で収集されること • 収集した情報の利用、保有及び開示がその収集目的に限定されていること • 個人情報がその利用目的に必要とされるだけ、正確、完全及び最新であること • 漏洩等事案発生時の本人及び監督機関等への報告する義務があること **【改正法案】[275]** 一方、データ保護関連新法によると、以下のとおり、個人情報について、匿名化又は非識別化されることにより異なる取扱いがなされることとされる。

[273] Federal Court Decisions, Cain v. Canada(Health)(January 25.2023), https://decisions.fct-cf.gc.ca/fc-cf/decisions/en/item/522872/index.do
[274] The Government of Canada, Justice Laws Website(Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) (SCHEDULE 1(Section 5),(April 13,2000), https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-7.html
[275] FASKEN, 前掲注 250

	• まず、匿名化された情報はカナダ CPPA の規制の対象外となる[276]。 • また、非識別化された情報は依然としてカナダ CPPA の規制の対象となる[277]が、以下の一定の場合、非識別化された情報に関連する個人の認識又は同意なしに特定の使用・開示が許される[278]。 ① 内部研究、分析、開発目的 ② 見込みのある商取引に関連した使用・開示 ③ 社会的に有益な目的（健康に関する目的、公共施設やインフラの提供又は改善、環境保護、その他所定の目的）のために、政府、医療機関、教育機関に開示する場合 • なお、非識別化された情報については、個人情報の場合に課される以下の規制から外れるが、これ以外については個人情報と同様に扱う必要がある[279]。 ① 個人情報がその利用目的に必要とされるだけ、正確、完全及び最新であること ② 本人による個人情報への本人アクセス権、個人情報の修正、廃棄、又は同じデータモビリティフレームワーク内の別の組織への開示を求める個人からの要求に対応すること
義務軽減・恩恵のために、匿名化/非識別化以外の要件（ある場合）。	カナダ CPPA 上、個人情報の取扱いに関し、匿名化又は非識別化することで得られる恩恵は前述のとおりである。この恩恵を受けるための匿名化又は非識別化以外に必要な別途の要件については、本調査報告書作成時点では特段存在しないと考えられるが（ただし、非識別化には後述のとおり条件が存在する。）、匿名化・非識別化のためのデータ処理及び処理済みデータの第三者提供の各場面における論点について、特に個人の同意の要否の点について説明する。 **【匿名化のためのデータ処理に必要な要件・手続】[280]**

[276] Parliament of Canada, 前掲注 237, BILL C-27, PART 1 Consumer Privacy Protection Act 第 6 条第 5 項

[277] Parliament of Canada, 前掲注 237, BILL C-27 PART 1 Consumer Privacy Protection Act 第 2 条第 3 項

[278] Parliament of Canada, 前掲注 237, BILL C-27 PART 1 Consumer Privacy Protection Act 第 2 条 3 項、第 21 条、第 22 条第 1 項、第 39 条第 1 項

[279] Parliament of Canada, 前掲注 237, BILL C-27 PART 1 Consumer Privacy Protection Act 第 2 条第 3 項、第 55 条、第 56 条、第 63 条第 1 項

[280] FASKEN, 前掲注 250

	カナダ CPPA は、組織が個人の認識や同意なしに個人情報を匿名化することを明示的に許可していないが、匿名化は個人情報を廃棄する手段であり、廃棄には同意が必要ないこと等を理由に同意は不要であると解釈される。 **【非識別化のためのデータ処理に必要な要件・手続】**[281] カナダ CPPA 上、個人情報を非識別化する場合、情報を非識別化するために使用される技術的及び管理的措置が、情報を非識別化する目的及び情報の機密性に比例することを条件に、個人の認識又は同意なしに行うことが可能であると考えられる[282]。 なお、カナダ CPPA は、個人情報の再識別に厳しい制限を課している。組織が個人情報を非識別化した後は、以下の目的がある場合を除き、個人情報を個人の識別に使用することはできない[283]。 • 組織が導入したセキュリティ保護措置の有効性のテストを実施するため • カナダ CPPA、連邦法又は州法に基づく要求事項を遵守するため • 非識別化された情報を使用して開発されたモデル、プロセス及びシステムの公正さ及び正確さのテストを実施するため • 非識別化プロセスの有効性のテストを実施するため • カナダ CPPA 第 116 条に基づき委員が許可した目的又は状況のため
匿名化処理済みデータの第三者提供に必要な要件・手続	カナダ CPPA 上、いったん匿名化処理されると、第三者提供に必要な要件・手続はないと考えられる。
非識別化処理済みデータの第三者提供に必要な要件・手続	カナダ CPPA 上の、第三者提供に関する以下の規定は非識別化された情報にも適用される[284]。 • 「個人の同意は、組織が個人の同意を求める時点又はそれ以前に、組織が個人に対し個人情報を開示する可

[281] FASKEN, 前掲注 250

[282] Parliament of Canada, 前掲注 237, BILL C-27 PART 1 Consumer Privacy Protection Act 第 20 条、第 74 条

[283] Parliament of Canada, 前掲注 237, BILL C-27 PART 1 Consumer Privacy Protection Act 第 75 条

[284] Parliament of Canada,前掲注 237, BILL C-27 PART 1 Consumer Privacy Protection Act 第 2 条第 3 項、第 15 条第 3 項（e）、第 63 条第 2 項

	能性のある第三者の名前又は第三者の種類を個人に提供した場合にのみ有効である。」 • 「組織が情報を開示した場合、本人の同意なく開示した場合を含め、開示先の第三者又は第三者の名称を本人に提供しなければならない。」 他方、カナダ CPPA 上の第三者提供に関する以下の規定は非識別化された情報については適用されない[285]。 • 「個人情報が正確、完全かつ最新でなければならない範囲を決定する際、組織は、情報が第三者に開示されるかどうか等の個人の利益を考慮しなければならない。」 • 「組織は、情報の修正について本人との間で合意が得られない場合、その旨を記録し、適切な場合には、情報にアクセスできる第三者にその旨を通知しなければならない。」

[285] Parliament of Canada,前掲注 237, BILL C-27 PART 1 Consumer Privacy Protection Act 第 2 条第 3 項、第 56 条第 2 項（c）、第 71 条第 3 項

技術名	概要	利点	注意事項
準同型暗号（Homomorphic encryption (HE)）	暗号化されたデータを解読することなく、暗号化されたデータのまま計算を実行することができる技術をいう。HE には、①完全な準同型暗号（FHE）、②相当程度の準同型暗号（SHE）、③部分的な準同型暗号（PHE）の 3 種類がある。 ①完全な準同型暗号（FHE）は、サポートする演算の種類やその複雑さに制限がないため、あらゆる関数を計算することができ、優れたデータ保護と実用性を提供できる。他方で、演算が複雑になればなるほど、より多くのリソースと時間が必要になる。②相当程度の準同型暗号（SHE）は、暗号化されたデータに対して、より少ない加算と乗算を可能とするが、対応できる関数の種類に制限があるため、対応可能な内容に限界がある。③部分的な準同型暗号（PHE）は、動きが早く、かつデータ保護にも優れているものの、加算と乗算のいずれかしか実行することができず、対応可能な関数の種類に制限があるため、対応できる内容にも限界がある。	HE は、個人情報を暗号化された状態で保管するため、データの安全性と機密性を確保し、データ漏洩のリスクを最小限に抑えることができる。また、暗号化されていても、暗号化されていないデータで計算した場合と同じ計算結果を導出することが可能である。	HE を用いる場合には、(a)正しいアルゴリズムを選択し、(b)適切な秘密鍵を選択し、(c)適切なソフトウェアを選択するとともに、(d)秘密鍵の安全性を確保する必要がある。特に HE では、秘密鍵が出力の解読に使用される可能性があるため、適切な技術的・組織的手段を用いて、秘密鍵を安全に管理することが重要となる。また、オリジナルの秘密鍵が流出した場合に備えて、直ちに新しい秘密鍵を生成できるようなプロセスを確立しておくことが必要となる。
秘密計算（Secure multiparty computation (SMPC)）	異なる当事者が、データを他の当事者と共有することなく、組み合わせたデータを共同で処理することのできるプロトコール（コンピュータ間でデータを送るための一連の規則）をいう。秘密を分割して各関係者	誰がデータ入力をしたかが明らかにされず、サイバー攻撃者によるプロトコールの出力が容易でないため、安全性の原則を維持できる。また、SMPC は、他の当事者と共同で処理を行った場合でも、共有データが	計算コストがかかるため、リアルタイムで大規模な処理を行う場合には適さない可能性がある。また、欠損データを代替値で置き換えること、データの重複を排除すること、結合するデータセットの一致が不正確な場合のレコードリンケージ等、

	に分配し、処理の内容やプロトコールの設定によって、全部又は一部の関係者に結果を知らせることができる。	保存されないため、データ漏洩によるリスクを最小限に抑えることができる。	達成すべき未解決の課題が残されている。更に、SMPC を効果的に利用するためには、技術的な専門知識とリソースが必要となる。
秘匿共通集合演算（Private set intersection (PSI)）	SMPC の一種であり、各当事者が独自のデータセットを持ち、それらのデータセットを公開・共有することなく、二つのデータセットが共通する要素のみを求めることができる計算方法をいう。例えば、クライアントのみが PSI の結果を知っており、サーバーホストは PSI サービスを管理し、クライアントの問い合わせに対応できるようにするクライアント・サーバー型が一般的な手法である。	PSI は、両当事者からの識別可能な入力データを組み合わせたデータを単一の当事者が保有することができないため、安全性の原則を維持することが可能である。また、PSI プロトコールは、設定された共有の要件に応じて、匿名の集計統計のみを表示するように設定することもできる。	不適切な共通項や過剰分析による再識別のリスクがある。また、当事者の一方又は双方が、個人に関する情報を明らかにしようとして、架空のデータを使用するおそれがある。
連合学習（Federated learning (FL)）	複数の異なる当事者がそれぞれのデータを用いて AI に学習させる技術をいう。AI が識別したいくつかのパターンを組み合わせて、単一のより正確なモデルを作成する。その際、学習データを当事者で共有する必要はない。 FL には、(a)集中設計と (b)分散設計の 2 つのアプローチがある。(a)集中型 FL では、コーディネーションサーバーがモデルやアルゴリズムを作成し、そのモデルの複製を各分散データソースに送出する。複製されたモデルは、各ローカルデータソースで自己学習し、生成された分析を送り返す。その分析結果は、他のデータソースからの分析結果と合成され、コーディネーションサーバーによって中央のモデルに統合される。	①モデルのトレーニング段階において処理される個人データを最小限にし、②他の PETs と組み合わせることで適切なレベルの安全性を提供し、③データを一箇所に集めることがないため、データ漏洩によるリスクを最小限に抑えることができる。	ローカルの機械学習モデルに個人情報が含まれている可能性がある。また、FL の一部として共有される情報は、モデル更新の逆計算、モデルが識別したパターンの観察やメンバーシップ推論のような他の攻撃によって、機械学習モデルのローカルトレーニングに使用される個人データを間接的に公開する可能性がある。従って、サイバー攻撃者がモデルの経時変化を観察したり、特定のモデルの更新を観察したり、モデルを操作したりすると、リバースエンジニアリングによる個人データの漏洩のリスクが高まる可能性がある。

	このプロセスが繰り返されることで、常にモデルが改良される。他方、(b)分散型 FL では、中央の調整サーバーは関与せず、各エンティティがそれぞれ通信し、グローバルモデルを直接更新することができる。		
信頼できる実行環境（Trusted execution environments (TEE)）	コンピューターデバイスの中央処理装置（CPU）内の安全な領域をいう。TEE は、システムの他の部分から分離された方法で、コードの実行とデータへのアクセスを可能にする。	処理を CPU の特定の部分に限定し、外部からアクセスできないようにすることができるため、データ漏洩から防止し、データの完全性、データの機密性、コードの完全性を保証することができ、セキュリティの原則と「デザインによるデータ保護」の要求の両方を満たすことができる。また、TEE はリスクを軽減するために講じた措置の証拠を提供し、それが適切であったことを証明することができるため、説明責任の原則の遵守できる。更に、TEE は製造及びサプライチェーンの安全性を高めることができる。	一度に処理できるデータが限られているため、利用可能なメモリの不足に起因して大規模な処理ができない可能性が生ずる。また、他の PETs との併用について、未解決の課題が残されている。更に、データを共有する環境でデータを処理する場合には、データ漏えいのリスクが高まる。
ゼロ知識証明（Zero-knowledge proofs (ZKP)）	証明者が検証者には知られていない秘密を保有している旨を検証者に証明することができるプロトコールをいう。例えば、ある証明者は、自分の年齢が何歳であるかを明かすことなく、ZKP を使って自らの年齢が X であると知っていることを検証者に証明できる。検証者は、証明者の応答により、証明者が X を知っているか否かを検証する。	個人データの量を必要な範囲に限定するため、データ最小化の原則に適合している。また、実年齢等の機密データを他者と共有する必要がないため、安全性の原則を充足することができる。	プロトコールの実装が不十分な場合に、コードのバグ、配備時の不備、ZKP プロトコールの実装方法から収集できる余分な情報に対する攻撃等の弱点が発生する可能性がある。
差分プライバシー（Differential privacy）	ある計算の出力が個人に関する情報をどの程度明らかにするかを測定する方法をいい、「ノイズ」をランダムに注入するものである。ノイズとは、データセット内のデータ	いずれのモデルも、適切なレベルのノイズが追加されていれば、他の目的のために匿名化されたデータとして活用することが可能となる。	差分プライバシーを適切に設定しない場合には、サイバー攻撃者が複数のクエリから知識を蓄積して個人を再特定することにより、個人データが漏えいするリスクがある。

	をランダムに変更することで、個人を識別しにくくするものをいう。差分プライバシーには、集計時にノイズを加える「グローバル差分プライバシー」と、各ユーザーが集計前に個々のレコードにノイズを追加する「ローカル差分プライバシー」の 2 つの種類がある。		
合成データ **（Synthetic data）**	データ合成アルゴリズムによって生成された人工的なデータで、実データのパターンや統計的特性を再現するものをいう。合成データは、大規模なデータセットにアクセスできない環境において、AI モデルを学習させるための有効なツールとなり得る。合成データには、元データの一部の変数だけを合成した「部分合成データ」と、全ての変数を合成した「完全合成データ」の 2 種類がある。	データを合成することによって小さなデータセットから大きなデータセットを生成することができるため、データ最小化の原則を遵守することに資する。	合成データが元のデータの正確な代理となるか否かは、手法やモデルの実用性に準拠することとなるところ、合成データが実データを模倣していればいるほど、その有用性は高い一方で、個人情報の漏えいのリスクは大きくなる。また、合成データの生成方法の中には、モデル逆引き攻撃に脆弱なものが存在するため、十分なデータの保護を図る必要がある。