大阪大学 社会技術共創研究センター
Research Center on Ethical, Legal and Social Issues

ELSI NOTE No.39

2024 年 4 月 1 日

パーソナルデータ利活用のためのリスクマネジメント（1）

プライバシー影響評価（PIA）の制度化

Authors

岸本 充生　大阪大学 社会技術共創研究センター センター長（2024年4月現在）
データビリティフロンティア機構　教授

大阪大学

Osaka University
Research Center on
Ethical, Legal and
Social Issues

目次

はじめに

パーソナルデータの利活用やパーソナルデータを用いて開発された AI の実装には様々なリスクを伴う。これらは次々と新しいものが出てくる以上、安全か危険かという二分法、あるいは、適法か違法かという二分法では扱うことが困難である。また、個人情報保護法においても、「違法」だけでなく「不当」という表現が用いられている（第 19 条など）ように、適法と違法の間のグレーな利用について何らかの判断が必要になってきている。すなわち「リスク」概念が必要不可欠になってきている。情報技術のリスクマネジメント手法としては、いくつかの国や地域ではすでにプライバシー影響評価（PIA）として制度化されており、主に公的機関によるプロジェクトを対象として活用されている。EU で 2018 年から施行されている一般データ保護規則（GDPR）では、高いリスクを発生させる個人データの処理について、「データ保護影響評価（DPIA）」が義務付けられたが、対象は公的機関だけでなく民間部門にも広げられた。日本国内でも、2021 年 6 月に開催された第 177 回個人情報保護委員会において、個人情報保護委員会は、民間組織向けに PIA の取り組みを促進することを表明している[1]。

公的機関による個人データの利活用を対象に PIA の制度化が始まった諸外国に対して、日本では民間や学術レベルでの取り組みが先行しつつある[2]。PIA のやり方は対象に応じて多様でありうるので必ずしも標準化・共通化する必要はないものの、先行する取り組みを知っておくことは国内における今後の実践に役に立つだろう。

本稿では国内における今後の PIA の実践・普及のために、すでに PIA が制度化されている諸外国の PIA の手法を簡単にまとめたものである。PIA へのアプローチとしては、チェックリスト型とリスクアセスメント型、両者のミックス型などが見られる。第 1 節では米国、第 2 節では英国、第 3 節ではオーストラリア、第 4 節ではカナダ、第 5 節ではニュージーランド、第 6 節では EU の動向をまとめた。第 7 節では国際標準化機関（ISO）による規格を紹介した。

---

[1] 第 177 回 個人情報保護委員会 配布資料　資料２　PIA の取組の促進について　https://www.ppc.go.jp/aboutus/minutes/2021/210630/

[2] 日本でも主に公的機関向けに、個人番号（マイナンバー）をその内容に含む個人情報ファイルを取り扱う事務のみを対象として「特定個人情報保護評価」と呼ばれる事前評価が実施されており、これらは「PIA」を呼ばれることがある。
https://www.ppc.go.jp/mynumber/pia2(kaisogo)

1. 米国の動向

●2002 年に成立した「電子政府法（“E-Government Act of 2002”）」[3]の第 208 条「プライバシー規定（Privacy Provisions）」において、省庁が「市民中心の電子政府」を実践するために、PIA の実施が義務付けられた。PIA の目的は、システムの所有者および開発者が、システムのライフサイクル全体を通じてプライバシー保護を組み込んでいることを証明すること、とされている。

●省庁は、(i) 個人識別可能な形で情報を収集、保持、または普及する情報技術を開発または調達する場合、あるいは、(ii) (I)情報技術を使用して収集、保持、または普及されるもので、かつ (II) 特定の個人と物理的またはオンラインで接触することを許可する個人識別可能な形の情報を含む（連邦政府の職員以外の 10 人以上の人に同一の質問が投げかけられるか、同一の報告義務が課される場合）ような情報の新たな収集を開始する場合に、その前に PIA を実施しなければならないとされた。PIA は最高情報責任者（CIO）または同等の職員によってレビューされ、実行可能な場合は/範囲でウェブサイトや官報などで公開されるべきとした。

●電子政府法は、大統領府の行政管理予算庁（OMB）長官に対して、PIA の内容を明記した指針を作成することを指示した。それを受けて、2003 年 4 月に、OMB 長官から各連邦機関の長宛ての覚書（M-03-22）として「2002 年電子政府法のプライバシー規定を実施するための OMB ガイダンス」が公布された[4]。添付資料 A「電子政府法第 208 条実施ガイダンス」の第 II 部 PIA では、定義や対象、内容などが記述されている。

●PIA の定義は「情報がどのように取り扱われているかについての分析であり、(i) その取り扱いがプライバシーに関して適用される法律上、規制上、政策上の要件に適合していることを確認し、(ii) 電子情報システムにおいて識別可能な形で情報を収集、保持、配布することのリスクと影響を判断し、(iii) 潜在的なプライバシーリスクを軽減するために、情報の取り扱いに関する保護および代替プロセスを検討、評価するもの」とした。

●PIA の詳細さの程度は「収集される情報の性質、IT システムの規模および複雑性に見合ったものでなければならない」として比例性の原則が強調され、また PIA は開発の早い段階で実施されるべきであるとしている。また情報のライフサイクル、すなわち収集、使用、保持、処理、開示、

[3] E-Government Act of 2002. https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf

[4] M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002. https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2003/m03_22.pdf

破棄を考慮し、各段階における情報の取り扱いが個人のプライバシーにどのような影響を与えるかを評価する必要があり、様々な専門家による協力が必要であるとしている。

●PIA の内容として以下の事項を分析・記述しなければならないとされた。

- どのような情報が収集されるのか（例えば、性質や情報源）
- 情報を収集する理由（適格性を判断するためなど）
- 情報の使用目的（例：既存のデータを検証するため）
- 情報を共有する相手（例：特定のプログラム目的のための他機関）
- 個人が情報提供を拒否する（情報提供が任意である場合）ために、あるいは情報の（必須の、または許可された利用以外の）利用に同意するためにどんな機会を持っているか、および、個人が同意を与える方法
- 情報がどのように保護されるか（例えば、運用面での対策、および、技術的な対策）
- プライバシー法に基づき、記録システムが作成されるかどうか

●PIA についての最低限の要件を定めた法律と OMB ガイダンスを受けて、連邦省庁はそれぞれ独自のガイドラインを作成している。以下では代表的な例として国土安全保障省（Department of Homeland Security: DHS）を取り上げる。2002 年に成立した「国土安全保障法（Homeland Security Act of 2002）」[5]の第 222 条「プライバシー・オフィサー」において、DHS 長官は新たに任命するプライバシー・オフィサーが責任を持つ 5 項目のうちの 4 番目として、「収集される個人情報のタイプや影響を受ける人数などを含む、個人情報のプライバシーに関する同省の規則案のプライバシー影響評価を実施すること。」が挙げられた。また、2 番目には「プライバシー法の記録システムに含まれる個人情報が、1974 年プライバシー法に規定された「公正情報取り扱い（fair information practices）」を完全に遵守した形で取り扱われることを保証すること。」とされた[6]。

---

[5] Homeland Security Act of 2002. https://www.dhs.gov/homeland-security-act-2002

[6] 「公正情報取り扱い原則（FIPPs）」自体は Privacy Act of 1974 に明記されたものでなく、1973 年に US Department of Health, Education, and Welfare（HEW）からの諮問委員会が HEW に提案した勧告（"Code of Fair Information Practices" 5 原則）をもとに、Privacy Act of 1974 によって設置された Privacy Protection Study Commission が 1977 年に公表した報告書（第 13 章）https://www.ojp.gov/pdffiles1/Digitization/49602NCJRS.pdf　において 3 点追加され、8 原則（公開、個人のアクセス、個人の参加、収集制限、利用制限、公開制限、情報管理、アカウンタビリティ）に整理されたものである。その後、米国内だけでなく、欧州諸国や OECD

●DHS のプライバシー遵守プロセスは、①プライバシー閾値分析（PTA）、②プライバシー影響評価（PIA）、③記録システム通知（SORN）、④定期的なレビューという 4 つの重要な部分からなる継続的なサイクルとされている[7]。①は PIA が必要か否かを判断するためのものである。

●2004 年にプライバシー室（Privacy Office）は「PIA を簡単に（Privacy Impact Assessments Made Simple）」を公表、続いて 2006 年には「PIA 指針（Privacy Impact Assessment Guidance）2006」を作成し、2007 年にはこれを改訂し「PIA 指針 2007」とした。その後、2010 年に「PIA 指針 2010」に更新された[8]。「PIA 指針 2010」に示された PIA の内容は、「要約」と「概観」に続いて、下記の内容、そして最後に「承認とサイン」とされた[9]。

Section 1.0 権限とその他の要件（Authorities and Other Requirements）

Section 2.0 情報の特徴（Characterization of the information）

Section 3.0 情報の利用（Uses of the Information）

Section 4.0 通知（Notice）

Section 5.0 プロジェクトによるデータの保持（Data Retention by the project）

Section 6.0 情報の共有（Information Sharing）

Section 7.0 救済（Redress）

Section 8.0 監査とアカウンタビリティ（Auditing and Accountability）

●2008 年 12 月末には覚書「PIA に関する DHS ポリシー（DHS Policy Regarding Privacy Impact Assessments）」[10]が公布され、PIA を実施する理由として、1）情報が与えられたうえでの意思決定、2）ライフサイクルでの管理、3）透明性、4）アカウンタビリティ、が挙げられた。また、

において同様の原則が議論された。有名な OECD の「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」は 1980 年に採択された。https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188　FIPPs への言及はないものの、類似した 8 項目の基本原則が定められた（収集制限、データ品質、目的特定、利用制限、セキュリティ保護、公開、個人参加、アカウンタビリティ）。

[7] U.S. Department of Homeland Security, Privacy Compliance Process https://www.dhs.gov/compliance

[8] U.S. Department of Homeland Security, Privacy Impact Assessment Guidance https://www.dhs.gov/publication/privacy-impact-assessment-guidance

[9] PIA のテンプレートも用意された。http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_template.pdf

[10] U.S. Department of Homeland Security, DHS Policy Regarding Privacy Impact Assessment https://www.dhs.gov/publication/privacy-policy-guidance-memorandum

PIA は対象別に 7 つのカテゴリーに分けられた。すなわち、標準的な情報技術、ルールメイキング、人材（DHS の被雇用者や契約労働者）、国家安全保障システム、プログラム、プライバシー的に機微な技術、パイロットテスト、である。

●2008 年 12 月末に同じく公布された覚書「公正情報取り扱い原則（FIPPs）：DHS におけるプライバシーポリシーの枠組み」は、「公正情報取り扱い原則（FIPPs）を、DHS におけるプライバシーポリシーとその実施のための基本原則としての記念するもの」とされ、プライバシー室は国土安全保障法 222 条(2)に基づき、PIA の実施などにおいても FIPPs を使用することが明記された[11]。DHS の FIPPs は以下の 8 項目からなる。DHS の PIA は、これら 8 項目についてそれぞれ、プライバシーリスクとそれらの軽減策を記載する体裁がとられている。

- 透明性 ：DHS は、個人識別可能な情報（PII）の収集、使用、配布、保持に関して透明性を確保し、本人に通知する必要がある。
- 個人の参加: DHS は、PII の使用過程に本人を関与させ、実施可能な限り、PII の収集、使用、普及、および保持について本人の同意を求めるべきである。また、DHS は、DHS による PII の使用に関して、適切なアクセス、訂正、および救済を行うための仕組みを提供すべきである。
- 目的の特定: DHS は、PII の収集を許可する権限を具体的に明示し、PII の使用目的（複数でも可）を具体的に明示する必要がある。
- データの最小化: DHS は、特定された目的を達成するために直接関連し必要な PII のみを収集し、特定された目的を達成するために必要な期間だけ PII を保持すべきである。
- 利用の制限: DHS は、通知において特定された目的のみに PII を使用すべきである。 PII を省外で共有する場合は、PII が収集された目的に適合した目的であるべきである。
- データの質および完全性：DHS は、実行可能な範囲において、PII が正確で、関連して、時宜を得て、完全であることを確保すべきである。
- セキュリティ：DHS は、損失、不正なアクセス/使用、破壊、改ざん、意図しない/不適切な開示などのリスクに対して、適切なセキュリティ保護措置により PII（あらゆるメディア

[11] The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf

において）を保護しなければならない。

- アカウンタビリティと監査：DHS は、これらの原則および適用されるすべてのプライバシー保護要件に準拠していることを示すために、これらの原則を遵守し、PII を使用するすべての職員および請負業者に研修を行い、PII の実際の使用を監査することで、アカウンタブルになるべきである。

●2024 年 1 月 30 日、行政管理予算局（OMB）は、バイデン大統領が 2023 年 10 月末に公布した大統領令 14110「AI の安全でセキュアで信頼に値する開発と利用」に従って、生成 AI を含む AI の急速な発展に対しても PIA をうまく活用するため、既存の PIA ガイダンスをどのように更新する必要があるかについての意見募集を開始した[12]。具体的には、プライバシーリスクに対処し、それらを軽減するための PIA の役割、透明性を促進するための PIA の役割、そして、AI を含む、技術とデータの能力の増進に伴うプライバシーリスクに関する質問項目が列挙された。

2. 英国の動向

●情報コミッショナー局（ICO）が委託した調査報告書[13]に基づき、2007 年 12 月に ICO が「PIA ハンドブック（PIA Handbook）」を公表した。英国は欧州地域で初めて PIA の指針を制定した国となった。2008 年 6 月に内閣府から発表された報告書「政府におけるデータ取扱い手続き」は、中央政府部門における PIA の使用を義務付け、PIA を政府の情報技術プロジェクトの審査に組み込むことを求めた[14]。ハンドブックは 2009 年 6 月に Version 2.0 として改訂された[15]。

●2010 年 1 月、内閣府は報告書「政府における情報を保護する」を発表し、「データ取扱い審査（Data Handling Review：DHR）」によって、政府機関が大量の個人データを処理する新しいプロジェクトやプログラムについて PIA を実施することを求めた[16]。PIA は初期段階で検討され、

[12] U.S. Management and Budget Office, Request for Information: Privacy Impact Assessments: A Notice by the Management and Budget Office on 01/30/2024 https://www.federalregister.gov/documents/2024/01/30/2024-01756/request-for-information-privacy-impact-assessments

[13] C. Bennett. R. Bayley. A. Charlesworth. R. Clarke. “Privacy Impact Assessments: International study of their application and effects.” https://www.rogerclarke.com/DV/ICO_2007_Study.pdf

[14] U.K. Cabinet Office, Data Handling Procedures in Government: Final Report. June 2008. https://www.gov.uk/government/publications/data-handling-procedures-in-government

[15] U.K. ICO. Privacy Impact Assessment Handbook Version 2.0. https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2013/09/PIAhandbookV2.pdf

[16] U.K. Cabinet Office, Protecting Information in Government. January 2010. https://data.parliament.uk/DepositedPapers/Files/DEP2010-0098/DEP2010-0098.pdf

あらゆる悪影響を軽減または完全に回避できるようにするものとされた。

●2014 年には情報コミッショナー局（ICO）によって「PIA を実施する：行動規範（Conducting privacy impact assessments: code of practice）」に更新された[17]。PIA は「組織がプロジェクトのプライバシーリスクを特定し、低減するのに役立つプロセス」と定義された。この時点では PIA の実施はデータ保護法の法的要件ではなかった。PIA は、1）PIA の必要性を確認、2）情報フローの記述、3）プライバシー関連リスクの特定、4）プライバシーへのソリューションの特定と評価、5）PIA の結果の署名と記録、6）PIA の結果のプロジェクト計画への統合、という 6 つのステップにまとめられた。

●EU 一般データ保護規則(GDPR)の成立と英国内でのデータ保護法（Data Protection Act）施行に伴い、2018 年、名称を EU に合わせて PIA から「データ保護影響評価（DPIA）」とし、個人データの処理が「高いリスクをもたらす可能性が高い」に当たる場合に実施が求められることになった。具体的には以下のようなケースが挙げられた[18]。これらは第 6 節の EU と同様である。

- 重大な影響を及ぼす体系的かつ広範なプロファイリングを使用する場合
- 特別カテゴリーまたは犯罪データを大規模に処理する場合
- 誰でもアクセスが可能な場所を組織的に大規模に監視する場合

●英国 ICO は独自に DPIA のサンプルテンプレートを用意しており、以下の 7 つのステップが示されている。Step 5 では特定されたリスクごとに、害の起きる可能性と害の重大さを 3 段階ずつで評価したうえでリスクの大きさを低・中・高に分類する。Step 6 では主に、中・高に分類されたリスクについて、削減または削除するためのオプションを特定し、対策後の残余リスクを低・中・高で評価し、それらが承認されるか否かを記す。

Step 1: DPIA が必要かどうか判断する（閾値分析）

Step 2: 処理を記述する（データの流れ・性質・文脈・目的を説明）

Step 3: コンサルテーションのやり方を考える（関連するステークホルダーを探索）

---

[17] U.K. ICO, Conducting privacy impact assessments code of practice. Version 1.0, 2014. https://www.pdpjournals.com/docs/88317.pdf

[18] When do we need a DPIA? https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-impact-assessments/

Step 4: 必要性と比例性を評価する

Step 5: リスクを特定し、評価する（害の起きる可能性と害の重大さ）（図１）

Step 6: リスクを軽減する手段を特定する

Step 7: 署名して正式に承認し、成果を記録する

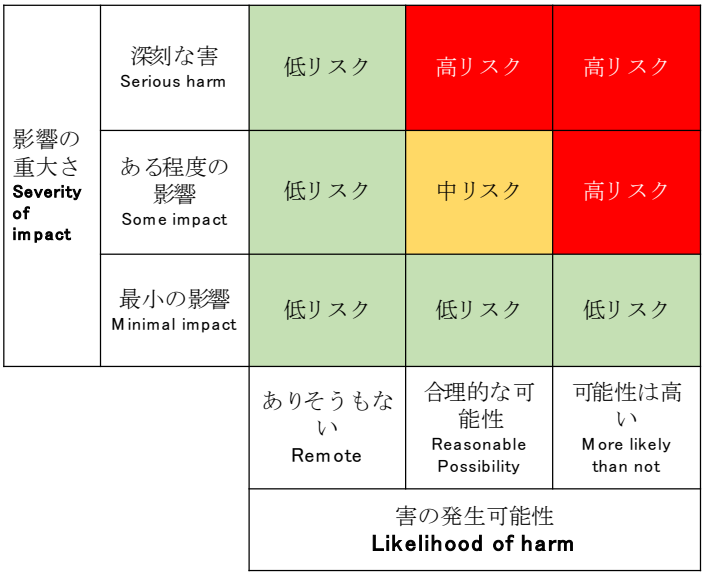

図１　ICO による DPIA のためのリスクマトリクス

●Brexit 移行期間が終了した 2020 年 12 月 31 日以降も英国版 GDPR が施行されたままであり、DPIA の実施は引き続き求められている。ただし脱 GDPR の方向性が示されており、新たに採択される予定の英国独自のデータ保護法では DPIA とは異なる手法が提案される可能性が高い。

3. オーストラリアの動向

●1988 年に制定されたプライバシー法（Privacy Act）に基づき、2001 年に全国プライバシー原則（National Privacy Principles）と 情報プライバシー原則（Information Privacy Principles）が制定された。プライバシー法の 2012 年改訂を受けて、2014 年 3 月に 13 項目からなるオーストラリア・プライバシー原則（Australian Privacy Principles：APPs）が制定された。プライバシー法は、オーストラリア政府機関、年間売上高が 300 万ドル以上の民間組織などを対象として

いる。APPs のためのガイドラインが公表されている[19]。

●プライバシー法の Sec. 33D において、オーストラリア情報コミッショナー局（OAIC）コミッショナーは連邦省庁に対して、(a) 省庁が、個人についての情報の取り扱いを含む活動または機能に従事することを提案する場合、かつ、(b)コミッショナーが、その活動又は機能が個人のプライバシーに重大な影響を及ぼす可能性があると見なす場合に、PIA を行うように指示できるとされた。また、PIA は、(a) その活動または機能が個人のプライバシーに及ぼすかもしれない影響を特定する、及び、(b) その影響を管理、最小化又は排除するための推奨事項を定めるための書面であるとされた。

●「プライバシー（オーストラリア政府機関-ガバナンス）APP コード 2017」[20]は、プライバシー法[21]のもとで、OAIC により 2017 年 10 月に制定され、2018 年 7 月に施行された。対象は連邦省庁である。APP コードの第三部が PIA に関する部分であり、12 が PIA の実施、13 が PIA の公表、14 が共同 PIA、15 が PIA の登録となっている。

●PIA は「高いプライバシーリスクを伴うすべてのプロジェクト」に対して実施しなければならないとされた。具体的には、「プロジェクトが、個人のプライバシーに重大な影響を与える可能性が高い新規の個人情報の取り扱い、または個人情報の取り扱い方法の変更を伴うと省庁が合理的に判断した場合」とされた。また、「重要なことは、すべての PIA が長く、複雑である必要はないということである。むしろ、PIA で取られるアプローチは、リスクのレベルに比例しているべきである。PIA は、プロジェクトの規模、複雑さ、リスクレベルに応じて適応可能な柔軟で拡張性のあるツールであることが意図されている。」[22]と注記さている。

●「プライバシー影響評価の実施に関するガイド（PIA ガイド）」は OAIC によって、2006 年に公表され、2010 年に改訂されたのち、現行のものは 2021 年に公表された[23]。そこでは PIA を実施するための 10 段階プロセスが提案された（下記）。PIA は第一義的にはプロジェクトが

---

[19] Office of the Australian Information Commissioner, Australian Privacy Principles guidelines. https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines

[20] Office of the Australian Information Commissioner, Privacy (Australian Government Agencies – Governance) APP Code 2017 https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/australian-government-agencies-privacy-code

[21] Sec. 26G において APP コードの策定が指示された。APP コードの内容は Sec. 26C に規定されている。APP コードは APPs を適用あるいは遵守するための方法が記述されたものである。

[22] Office of the Australian Information Commissioner, When do agencies need to conduct a privacy impact assessment? https://www.oaic.gov.au/privacy/guidance-and-advice/when-do-agencies-need-to-conduct-a-privacy-impact-assessment

[23] Office of the Australian Information Commissioner, Guide to undertaking privacy impact assessments. https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments

プライバシーに関する法律に違反するリスクを評価し、そのリスクを軽減するための管理策を特定するものであるが、PIA は単なるコンプライアンスチェックを大きく超えるものであるとされた。つまり「プライバシーの観点からプロジェクトの「全容を語る」ものであり、コンプライアンスを超えて、プロジェクトで計画されている個人情報の利用が地域社会に受け入れられるかどうかなど、より広いプライバシーへの影響とリスクも考慮しなければならない。」とされた。PIA を実施するタイミングは、プロジェクトの設計に影響を与えることを可能とするためにプロジェクトの十分早い段階である必要がある。

●PIA を実施するための 10 段階プロセス

1. 閾値評価（Threshold Assessment）：PIA の実施が必要かどうかを判断するため。
2. PIA の計画：範囲、実施主体、コンサルテーション等
3. プロジェクトの（簡潔な）説明
4. ステークホルダーの特定と協議
5. 情報フローの把握：本人確認が必要であるかどうか、どのような/どのように個人情報が収集されるか、利用と開示、情報の品質を確保するためのプロセス、実施されている（または実施される予定の）安全対策、個人が自分の個人情報にアクセスし、修正することができる能力
6. プライバシー影響分析およびコンプライアンスチェック：プロジェクトが 13 の各 APP を遵守しているかどうかを検討：

    APP1　個人情報のオープンで透明性のある管理、　APP2　匿名性と仮名性

    APP3　募集された個人情報の収集、　APP4　未承諾の個人情報への対応

    APP5　個人情報収集の通知、　APP6　個人情報の使用または開示

    APP7　ダイレクトマーケティング、　APP8　個人情報の国境を越えた開示

    APP 9　政府関連識別子の採用、使用、開示、　APP10　個人情報の質

    APP11　個人情報のセキュリティ、　APP12　個人情報へのアクセス

    APP13　個人情報への訂正

7. プライバシー管理 - リスクへの対応

8. 提言

9. 報告：提案された PIA 報告書のフォーマットは次のとおりである。

エグゼクティブサマリー、PIA 方法論、プロジェクトの説明、分析、結論、附録

10. 対応とレビュー：勧告への対応、独立したレビュー／監査

●OAIC は、PIA レポートの公開を強く推奨しているが、全文を公開することが困難な場合があることも認識しており、そういう場合は、要約版あるいは編集版の公開を推奨している。また、PIA は報告書の作成で終わるのではなく、継続的なプロセスであることも強調されている。

●本 NOTE では割愛したが、オーストラリアでは州レベルでの PIA の取り組みも盛んである。

4. カナダの動向

●カナダ政府は 2002 年 5 月 2 日に「プライバシー影響評価ポリシー（Privacy Impact Assessment Policy）」を施行した[24]。PIA は、プログラムやサービスの設計または再設計の全体を通してプライバシーが考慮されていることを確認するための枠組みとされた。本ポリシーには、PIA 実施を支援するための「プライバシー影響評価ガイドライン：プライバシーリスクを管理するための枠組み（Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks）」が付いている[25]。ガイドラインには、プロジェクト開始（予備的 PIA を含む）、データ分析、プライバシー分析、PIA 報告書という 4 段階の PIA プロセスが示されている。ガイドラインの附録 A には PIA の目次が提示されている。6 のサマリー表ではリスクの大きさは低・中・高の 3 段階で表記されることになっている。

1．エグゼクティブサマリー

2．はじめに　2.1 報告書の目的　2.2 PIA の範囲　2.3 参考資料　2.4 参加者　2.5 法規制と政策　2.6 本報告書で使用する略語

3．プロジェクト提案書

[24] 現在は効力はないが、ここにアーカイブされている。https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=12450
[25] 現在は効力はないが、ここにアーカイブされている。https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=12451

4．データフロー分析　4.1 業務フロー図と説明　4.2 データフロー表

5．プライバシー分析

6．プライバシーリスク管理計画　6.1 プライバシーリスクの軽減　6.2 サマリー表

7．コミュニケーション戦略

財務委員会（Treasury Board）からプロジェクトの予備的承認（Preliminary Project Approval）を得ようとする連邦政府機関は、PIA の結果を提出書類の本文またはプロジェクト概要に記載しなければならない。実効的承認（Effective Project Approval）を得ようとする機関は、PIA に従ってプライバシーリスクを回避または軽減するために取られた、または取られる予定の措置を要約した状況報告書を、提出書類の本文またはプロジェクト概要に記載しなければならない。

●2010 年 4 月に「プライバシー影響評価に関する指令（Directive on Privacy Impact Assessment）」が施行され、これが先の「プライバシー影響評価ポリシー」に取って代わった[26]。2024 年現在もこれが効力を持っている。省庁の適切な上級職員又は幹部は、PIA を完了させるために以下のプロセスを遵守する責任を負うとされた。

A）PIA の開始、B）複数の機関が関与している場合、C）PIA（コア PIA 要素）の完了、D）PIA の内部承認、E)通知および登録、F）コア PIA の公開報告、G）PIA の共有。

附録 B によれば、個人情報に関わるプログラムや活動に対して財務委員会（Treasury Board）の承認を得ようとする政府機関は、以下の責任を負う。

- プロジェクト計画の可能な限り早い段階で PIA を開始するためにあらゆる合理的な努力をすること。
- 提出書類の本文において、PIA が完了したかどうかを明らかにし、イニシアチブの緊急性または優先性のために PIA が完了しなかった場合は、PIA の完了のためのスケジュールを明らかにすること。
- 財務委員会にプロジェクトの承認を求める際、プライバシー問題やリスクに対処するために取られた、または取られる予定の対策をプロジェクト概要に明記すること。

[26] Government of Canada, Directive on Privacy Impact Assessment. 2010. https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=18308

- 新規または大幅に変更されたプログラムまたは活動で、実施前または財務委員会事務局（TBS）が定めた期間内・条件下で TBS の承認を受けたものについては、PIA を完了させること。

附録 C にはコア PIA に必要な内容が提示されている。第 II 部「リスク領域の特定と分類」では、政府機関全体で一貫したリスク分類と測定を行うために、下記のような標準化されたリスク領域と、それぞれに共通のリスクスケール（最低の 1 から最高の 3 あるいは 4 まで）が提示されている。レベル 3 または 4 と認定されたリスク領域の数が多ければ対処する必要があるとされる。

a. プログラムまたは活動のタイプ

b. 含まれる個人情報のタイプや文脈

c. プログラムまたは活動のパートナーと民間部門の参加

d. プログラムまたは活動の期間

e. プログラムが影響を及ぼす対象の人数

f. 技術とプライバシー（※ここだけ Yes/No 回答）

g. 個人情報の移転の程度

●プライバシーコミッショナー事務局（OPC）も PIA のガイドを公表している[27]。OPC は連邦政府機関が実施する PIA を支援している。また、図 2 のような、PIA を実施する必要があるか否かを判断するためのフローチャートを提供している。

[27] Office of the Privacy Commissioner of Canada, Expectations: OPC's Guide to the Privacy Impact Assessment Process. Revised March 2020. https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/

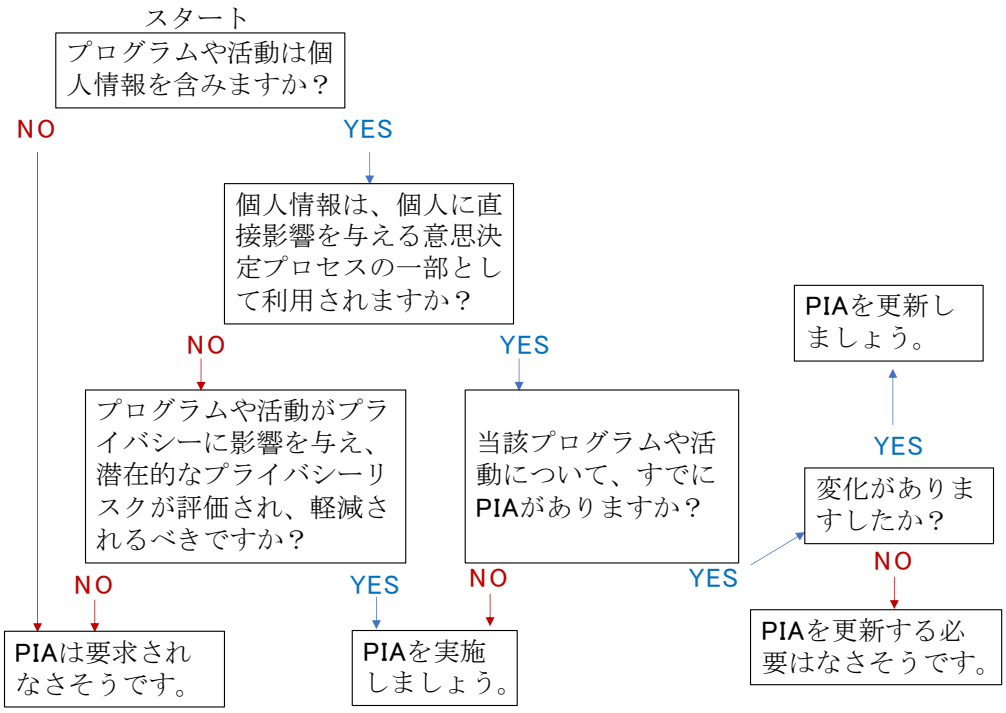

図２　PIA を実施する必要があるか否かの判断フローチャート（PIA ガイドの Figure 1）

また 9 段階の PIA プロセスも提示されており、１．PIA の必要性を確認、２．計画する、３．相談する（OPC を含む）、４．必要性と比例性を評価する、５．固有のリスクを特定し評価する、６．軽減する対策を作る、７．承認を得る、８．TBS と OPC に報告する、９，継続的に監視する、となっている。

●本 NOTE では割愛したが、カナダでも州レベルでの PIA の取り組みも盛んである。

5. ニュージーランドの動向

●1993 年のプライバシー法（Privacy Act 1993）では PIA への具体的な言及はなかったが、Part 2 「情報プライバシー原則（Information privacy principles：IPP）」で提示された情報の収集から破棄までのライフサイクルにおける個人情報の管理方法について定めた 12 のプライバシー原則を実践するために、PIA の実践が要請されるようになった。2002 年にはプライバシーコミッショナー事務局（Office of the Privacy Commissioner：OPC)から「PIA ハンドブック」が公表

された[28]。2020 年のプライバシー法（Privacy Act 2020）は、1993 年のプライバシー法（Privacy Act 1993）に代わり、2020 年 12 月 1 日に施行された。2020 年のプライバシー法では情報プライバシー原則（IPP）の項目数が 12 から 13 に増えた[29]。

●プライバシーコミッショナー事務局（OPC）は、PIA を行うかどうかの判断を容易にするための 2 つの部分からなる指針（2015 年作成のツールキット）を公表した[30]。「ブリーフ・プライバシー分析（Brief Privacy Analysis）」のテンプレートが用意されており、チェックリストに Yes/No で回答し、1 つでも Yes があると初期リスクアセスメントとしてそれぞれを低・中・高の 3 段階で評価し、中・高とされた項目にはリスク低減策を記述する欄が設けられている。最終的に完全な PIA が必要かどうかについて判断される。第 2 部には PIA のテンプレートが用意されており、13 の原則ごとに遵守状況をチェックすることでリスクを抽出する仕組みになっていた。2024 年 2 月にはツールキットがさらに更新された[31]。PIA の基本的なステップは以下の 6 段階からなる。

1. 収集（Gather）：PIA を実施するために必要なすべての情報を収集する。
2. チェック（Check）：プライバシー原則に照らして確認する
3. リスク（Risk）：実際のプライバシーリスクとその軽減方法を見出す。
4. 作成（Produce）：PIA を作成する（報告書のテンプレートを使うことを推奨）。
5. 行動を起こす（Take action）：対策が実施される。
6. 審査（Review）：プロジェクトの進展に伴い、必要に応じて PIA を見直し、調整する。

---

[28] New Zealand Privacy Commissioner Office, Privacy Impact Assessment Handbook, 2002. https://privacy.org.nz/publications/guidance-resources/privacy-impact-assessment-handbook/

[29] 情報プライバシー原則（IPP）の表題は次のとおりである。原則 1：個人情報の収集目的、原則 2：個人情報の提供元、原則 3：主体からの情報収集、原則 4：個人情報の収集方法、原則 5：個人情報の保持とセキュリティ、原則 6：個人情報へのアクセス、原則 7：個人情報の訂正、原則 8：利用または開示前に確認する個人情報の正確性等、原則 9：個人情報を必要以上に保管しないこと、原則 10：個人情報の利用制限、原則 11：個人情報の開示制限、原則 12：ニュージーランドの外への個人情報の開示、原則 13：固有の識別子。

[30] New Zealand Privacy Commissioner Office, Privacy Impact Assessment Toolkit, 2015. https://www.privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/Privacy-Impact-Part-1.pdf

[31] New Zealand Privacy Commissioner Office, Privacy Impact Assessment Toolkit, 2024. https://privacy.org.nz/publications/guidance-resources/privacy-impact-assessment-toolkit/

●リスクアセスメントのやり方は「情報プライバシー原則（IPP）」の各項目に当てはめながら複数のリスク項目を抽出し、それぞれにリスク軽減策を提案するものであるが、実際の PIA 報告書では様々な手法がとられている。抽出されたリスク項目ごとに対策前と対策後のリスクレベルをそれぞれ、非常に低い（黄緑）、低い（黄色）、中くらい（オレンジ）、高い（赤）、の 4 段階で評価されることが多い。いくつかの PIA 報告書では、抽出されたリスク項目ごとに、対策前と対策後の発生可能性（likelihood）と影響の大きさ（consequence）を 4 段階ずつ[32]あるいは 5 段階ずつ[33]で見積もって、番号を付けてリスクマップに配置するものである（図３）。全体リスクは 2 つのスコアを掛け合わせて、4 段階（非常に低い、低い、中くらい、高い）で評価される。

	わずかな Minor	まあまあの Moderate	重大な Major	深刻な Severe
ほぼ確か Almost certain				
ありそう Likely				
ありうる Possible				
ありそうにない Unlikely				

	ほとんどない Insignificant	わずかな Minor	まあまあの Moderate	重大な Major	深刻な Severe
確からしい Certain					
ありそう Likely					
ありうる Possible					
ありそうにない Unlikely					
めったにない Rare					

図３　ニュージーランドの PIA で用いられるリスクマップの例

※縦軸は「発生可能性（Likelihood）」、横軸は「影響の大きさ（Consequence）」を示す。

●リスクアセスメントにおける「リスク」の対象は幅広いものになるため、例えば第一次産業省（MPI）は「影響の大きさ（consequence）」と「発生可能性（likelihood）」のそれぞれにリスククライテリアを定めている[34]。また、Health New Zealand では、「影響の大きさ（consequence）」については、リスク分類、つまり「守りたいもの」として、「レピュテーション」「公衆衛生部門への信頼と信用」「戦略的」「運用上」「健康と安全」「財務的（省庁内、省庁外、設備投資）」「法的遵守」「契約履行」「環境」「技術」を挙げ、それぞれ 5 段階で目安を示している。財務影響については具体的な金額の目安が提示されている。

●AI については、ニュージーランド政府は 2020 年、政府機関によるアルゴリズム利用のための

[32] 例えば、第一次産業省（MPI）による、漁船へのオンボードカメラの設置に関する PIA 報告書（2019 年）では 4 段階ずつのリスクマップが使われている。https://www.mpi.govt.nz/dmsdocument/39269-On-board-cameras-project-privacy-impact-assessment-19-December-2019

[33] 例えば、第一次産業省（MPI）による、ボディカメラの導入に関する PIA 報告書（2022 年）では 5 段階ずつのリスク「ヒートマップ」が使われている。https://www.mpi.govt.nz/dmsdocument/50512-Privacy-impact-assessment-PIA-Body-worn-cameras-programme

[34] 先に引用した、漁船へのオンボードカメラの設置に関する PIA 報告書（2019 年）の Appendix F を参照。

指針として「ニュージーランド・アルゴリズム憲章」を発表した[35]。透明性、パートナーシップ、人々、プライバシー・倫理・人権、人による監督についてのコミットメントに同意した省庁はこれに署名をすることになっており、意図しない悪影響が発生する可能性とその相対的な影響度と照らし合わせてスコア化し、総合的なリスクレベルを導き出す「アルゴリズム評価報告書」を作成することになっている。そのためのツールとして「アルゴリズム影響評価（Algorithm Impact Assessment: AIA）」ツールキットが発表された[36]。2023 年 12 月には「アルゴリズム閾値評価」「アルゴリズム影響評価質問紙」「アルゴリズム影響評価報告書テンプレート」「アルゴリズム影響評価ユーザーガイド」が公表された。テンプレートによると、潜在的な害（harm）のアセスメントは PIA と同様、影響の大きさ（Impact）と発生可能性（likelihood）をそれぞれ 5 段階ずつで評価し、総合的なリスクレベルも 5 段階（非常に低い、低い、中くらい、高い、危機的な）に区別された[37]。発生可能性は 12 か月間の発生可能性として「＞80%、60-80%、40-60%、20-40%、＜20%」の 5 段階で分けられた。また、省庁自身にとってのリスクに焦点が当てられていることが特徴である。

6. EU の動向

●EU では 2018 年 5 月に施行された「一般データ保護規則（GDPR）」の第 35 条「データ保護影響評価（DPIA）」の第 1 項に、「処理の性質、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処理が、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、コントローラーは、その処理の開始前に、予定している処理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」と記載された。公的機関だけでなく、民間組織も対象となる。第 3 項には DPIA が求められるケースとして次の 3 つの例が挙げられた。

- プロファイリングを含め、自動的な処理に基づくものであり、かつ、それに基づく判断が自然人に関して法的効果を発生させ、又は、自然人に対して同様の重大な影響を及ぼす、自然人に関する人格的側面（personal aspects）の体系的かつ広範囲な評価（evaluation）

[35] Algorithm charter for Aotearoa New Zealand https://www.data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-charter/

[36] Data.govt.nz. Algorithm Impact Assessment toolkit https://www.data.govt.nz/toolkit/data-ethics/government-algorithm-transparency-and-accountability/algorithm-impact-assessment-toolkit/

[37] New Zealand Government, Algorithm impact assessment report, December 2023.の Appendix 2 を参照。

- 第 9 条第 1 項に規定する特別な種類のデータまたは第 10 条に規定する有罪判決及び犯罪行為と関連する個人データの大規模な処理
- 公衆がアクセス可能な場所に対する体系的な監視

●2017 年、GDPR 第 35 条を実践するために、欧州データ保護当局（WP29）は「DPIA と処理が「高リスクになる可能性が高い」かどうかの判断に関するガイドライン」を公表した[38]。そこでは「高リスクになる可能性が高い」かどうかを判断するための 9 つの基準が示された。これらのうち 2 つ（場合によっては 1 つでも）該当する場合には DPIA の実施が必要であるとした。

- プロファイリングを含む評価（evaluation）やスコアリング
- 法的あるいは同様の重大な効果を持つ自動化された意思決定
- 体系的な監視
- 機微なデータあるいは高度に個人的な性質を有するデータ
- 大規模なデータ処理
- データセットの照合や統合
- 脆弱なデータ主体に関するデータ
- 新しい技術あるいは組織的なソリューションの革新的な利用や適用
- 処理そのものが「データ主体の権利の行使やサービスや契約の利用を妨げる」ケース

●DPIA は、データ処理前にデータ保護責任者（DPO）が実施することとされ、一般的な反復プロセスとして、1)予想される処理の記述、2)必要性及び比例性の評価、3)既に織り込み済みの対策、4)権利と自由に対するリスクの評価、5)予期されるリスク対策、6)文書化、7)モニタリングとレビュー、の段階が示されさらに最初に戻るプロセスが示された。リスクアセスメントの方法は具体的には示されていない。また、DPIA の公開自体は GDPR の法的義務ではなく、コントローラーが決定することとされているが、サマリーや結論部分などは公開されることが推奨されて

[38] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01)
https://ec.europa.eu/newsroom/article29/items/611236　個人情報保護委員会による仮訳がある。
https://www.ppc.go.jp/files/pdf/dpia_guideline.pdf

いる。

●2024 年 3 月に欧州議会で採択された AI Act では、高リスク AI システムを使用する前に、当該システムを実装する事業者に、「基本的権利影響評価（fundamental rights impact assessment）」を実施することが義務付けられた[39]。第 29a 条によると、下記の項目からなる評価を実施しなければならない。まだ詳細は分からないが今後ガイドラインなどにより具体的な手順などが示されるものと考えられる。

a）高リスク AI システムがその意図された目的に沿って使用される場合の、実装者のプロセスの説明

b）各高リスク AI システムが使用される予定の期間及び頻度の説明

c）特定の文脈における使用により影響を受ける可能性のある自然人及び集団のカテゴリー

d）(c)に従って特定された人又は集団のカテゴリーに影響を及ぼす可能性のある具体的な危害のリスク

e）使用説明書に従った、人による監督措置の実施に関する記述

f）これらのリスクが顕在化した場合にとるべき措置（内部統制および苦情処理メカニズムに関する取り決めを含む）

●EU 全体のものを紹介したが、フランスなどの加盟国レベルでも PIA や DPIA の取り組みがあるが本稿では割愛した。

7. 国際標準化委員会（ISO）

●国際標準化委員会（ISO）では PIA は、最初は TC68(金融サービスの専門委員会)において 2008 年 4 月に、ISO 22307（金融サービスーPIA）として発行された[40]。内容は金融サービスに特化したものではなく、一般的な PIA プロセスが記述されていた。

●2017 年 6 月に、国際電気標準会議（IEC）と共同で、PIA に関する国際標準規格 ISO/IEC 29134

[39] European Parliament, Artificial Intelligence Act: MEPs adopt landmark law. Press Release. 13 March 2024. https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law

[40] ISO 22307:2008 Financial services - Privacy impact assessment, https://www.iso.org/standard/40897.html

が発行された[41]。最新のものは 2023 年版である[42]。PIA に関するプロセスと PIA 報告書の構成と内容に関するガイドラインを示したもので、あらゆる種類と規模の組織に適用可能なものである。PIA は単なる「ツール」でなく、取り組みのできるだけ早い段階から始め、プライバシーバイデザイン（privacy by design）[43]を確保するための「プロセス」であると冒頭に述べられている。以下に内容を紹介する[44]。

●第 5 章では、PIA を実施することのメリットは何か、アクター（データ提供者、管理主体、規制当局、顧客）ごとの PIA の目的は何か、アカウンタビリティ（PIA を実施し、その結果の質を保証する）の所在、PIA のスコープや規模はその影響の大きさに比例することなどが説明されている。

●第 6 章では実際に PIA を実施するためのプロセスに関するガイダンスとなっている。項目ごとに、目標、インプット、期待されるアウトプット、アクション、実施ガイダンスからなる。6.2 節では、閾値分析（threshold analysis）と呼ばれる、そもそも PIA を実施する必要があるのかどうかを決めるプロセスが解説されている。個人情報を扱う新規の技術やサービスなどを扱う場合、特に配慮を要する個人情報を処理する場合、法規制・データ処理の目的・データフローなどが変更された場合、事業を拡大・買収する場合で、プライバシーへの影響が認識される際に PIA を実施・更新することが求められるとされた。

●6.3 節は準備段階を扱う。

- PIA チームを設置したうえで、リスクアセスメント及びマネジメントの方法や基準を定めること、具体的にはリスクの影響の大きさ（impact）と発生可能性（likelihood）を判定するための基準やスケールを、データ提供者と組織の両方の視点から定める。
- PIA の計画を立て、必要な費用や人的資源を割り当てる。
- 評価対象のスコープを正確に記述する。具体的にはデータの種類やデータフロー、それらの手続き、ステークホルダーの特定などが含まれる。

---

41 ISO/IEC 29134:2017 Information technology - Security techniques -- Guidelines for privacy impact assessment. https://www.iso.org/standard/62289.html

42 ISO/IEC 29134:2023 Information technology - Security techniques -- Guidelines for privacy impact assessment. https://www.iso.org/standard/86012.html

43 後付けでプライバシー対策を実施するのではなく、設計当初からプライバシー配慮が組み込むというコンセプトを表す概念である。

44 第 7 章は PIA 報告書のコンテンツであるため省略した。

- リスクや懸念事項を見出すためにもステークホルダーと意見交換することが推奨される。

●6.4 節は PIA の実施段階についてである。

- データフロー図を完成させる。
- ユースケースにおけるユーザの非意図的なものも含む潜在的な行動を予測する。
- 法的に要求されたり、類似のプロジェクトで実施されたりしているプライバシー保護の要件を特定する。
- 評価対象となるリスクを特定したうえで[45]、リスク分析を実施する。発生可能性（likelihood）と影響の大きさ（impact）のレベルを見積もる[46]。分析は定性的でも、半定量的でも、定量的でも、それらの組み合わせでもよいが、実践的には定性的な分析が用いられることが多い。リスク分析の結果は、対策の優先順位付けに役に立つようにリスクマップに示される[47]。
- リスク項目ごとに最も適切なリスク対策オプションを提示する。対策には、リスク削減、リスク保持、リスク回避、リスク移転という 4 つのオプションがある。
- PIA 報告書を完成させ、サマリーを加え、企業秘密部分を除いて公表するとともに、リスク対策を実施する。事後的にレビューあるいは監査を自らまたは第三者によって実施する。プロセスに大きな変更が加えられた場合は PIA を更新する。

●Annex A には、あくまでも参考上のものとしたうえで、影響のレベル（level of impact）と発生可能性（likelihood）の見積もの目安が例示されている[48]。さらに、4 段階×4 段階のリスクマップが示されている。

---

[45] リスク特定のツールやテクニークを用いると書かれているものの具体的な言及はない。リスク項目の事例は Annex B に列挙されている。

[46] 具体的な方法は、あくまでも参考として、Annex A に記述されている。

[47] Figure D.2 に 4×4 のリスクマップの例が示されている。

[48] ISO/IEC 29134 の Annex A より著者作成

表１　影響のレベルと発生可能性の見積もの目安

	影響の大きさのレベル分け	発生可能性のレベル分け
1 無視できる（negligible）	データ提供者は、影響を受けないか、多少の不便を被るだろうが、それは難なく克服できるだろう（情報の再入力にかかる時間、煩わしさ、苛立ちなど）。	選択されたリスク源にとって、支援資産の特性を悪用した脅威の実行は不可能と思われる（例えば、バッジリーダーとアクセスコードで保護された部屋に保管された紙文書の盗難）。
2 限定的な（limited）	データ提供者は、大きな不便に遭遇する可能性があるが、多少の困難（余分なコスト、ビジネスサービスへのアクセス拒否、恐怖、無理解、ストレス、軽い体調不良など）にもかかわらず乗り越えることができだろう。	選択されたリスク源にとって、支援資産の特性を悪用した脅威の実行は困難と思われる（例：バッジリーダーで保護された部屋に保管された紙文書の盗難）
3 重大な（significant）	データ提供者は、重大な帰結に遭遇する可能性があるが、それは深刻な困難（資金の不正流用、銀行によるブラックリスト入り、財産の損失、雇用の喪失、召喚状、健康状態の悪化など）を伴うものの、克服できるはずである。	選択されたリスク源にとって、支援資産の特性を悪用した脅威の実行は可能であると思われる（例えば、受付で一旦チェックインしなければアクセスできないオフィスに保管された紙文書の盗難など）。
4 最大の（maximum）	データ提供者は、乗り越えられない重大な、あるいは取り返しのつかない帰結に遭遇しうる（返済不能な負債や就労不能などの経済的困窮、長期にわたる精神的・肉体的疾患、死亡など）。	選択されたリスク源にとって、支援資産の特性を悪用した脅威の実行は極めて容易であると思われる（ロビーに保管された紙文書の盗難など）。

出展）ISO/IEC 29134:2023 Annex A

注）本表では”PII principals”（個人を特定できる情報に関係する人）を、欧州 GDPR に合わせて「データ提供者」と訳している。

おわりに

ISO も含めて 7 つの国・地域・機関の PIA の取り組みを概観した。浮かび上がってきた共通するポイントを最後にまとめておきたい。

●PIA は単なるツールではなく、プロセスであることが強調されている。結果だけでなく、プロセスを通して、プロジェクトやシステムの全体像の把握、ステークホルダーの把握や参加、ステークホルダーへの説明と信頼の獲得といったメリットが得られることの重要性が指摘されている。

●工学分野などの従来のリスクアセスメントは、エンドポイント（何を守りたいか）が自明で、客観性・定量性を追求するものであったのに対して、情報技術分野のリスクアセスメントは、リスク項目の洗い出しが重要であり、リスクの見積もりは主観的・定性的にならざるを得ない。その目的も、正確な評価を追求することよりも、自組織内及び社会に対して、当該データ利活用が「安全である」と考えていることを具体的に示すことにある。

●社会（特に個人のプライバシー）への影響の大きなものほど、詳細な PIA を実施すべきとしている。これは比例性（proportionality）の原則と呼ばれることもある。これは常識的な態度であるものの、ガイドなしに自ら判断することは困難であると指摘されることもある。

●リスクの評価方法には、原則と照らし合わすチェックリスト方式（米国やオーストラリア）から影響の大きさと発生可能性の二軸でのリスクマップ（英国、ニュージーランド、ISO/IEC）まで多様であることである。二軸の場合も、３×３の英国と４×４の ISO/IEC、5×5 のニュージーランドがある。

最後に、本 NOTE は「プライバシー」影響評価を扱ったが、AI も含むパーソナルデータ利活用のリスクはプライバシーに限らない。むしろプライバシーに限定することで大事なリスクを見逃してしまうリスクが高くなりかねない。実際、AI の社会実装に伴うリスクは最近”AI Safety”として議論されているが、その場合のリスクは、誤情報・偽情報や著作権の侵害、民主主義への脅威など多様である。枠組みとしては PIA を使いつつ、対象とするリスク、言い換えると「何を守りたいか」を拡大していく必要があるだろう。その場合に PIA という呼称が実態を合わなくなる可能性もある。その際は、別の呼称を与えてもよいだろうし、単に「リスクアセスメント」としてもよいかもしれない。

ELSI NOTE No. 39
令和 6 年 4 月 1 日

パーソナルデータ利活用のためのリスクマネジメント（1）

プライバシー影響評価（PIA）の制度化

岸本 充生　　大阪大学 社会技術共創研究センター　センター長（2024 年 4 月現在）
データビリティフロンティア機構　教授

Risk Management for Personal Data Utilization (1)

Institutionalization of Privacy Impact Assessment (PIA)

Atsuo KISHIMOTO　　Osaka University

大阪大学 社会技術共創研究センター
Research Center on Ethical, Legal and Social Issues

〒565-0871 大阪府吹田市山田丘 2-8
大阪大学吹田キャンパステクノアライアンス C 棟 6 階
TEL 06-6105-6084
https://elsi.osaka-u.ac.jp

大阪大学

Osaka University
Research Center on
Ethical, Legal and
Social Issues