参考資料３

諸外国におけるPIA質問票

１　アメリカ

（１）PIAに関する指針

・行政管理予算局（Office of Management and Budget、OMB）によるOMBガイダンス[1]
・国土安全保障省（Department of Homeland Security）によるPIA公式ガイダンス[2]
・国土安全保障省によるPIAテンプレート[3]
・その他の省によるPIAガイダンス・テンプレートも存在する[4]。

（２）行政管理予算局によるOMBガイダンスのうち質問票に相当する事項[5]

①PIAでは以下を分析及び記述しなければならない。
・収集される情報（性質、情報源など）
・収集理由（適格性判断のためなど）
・情報の利用方法（既存データの検証のためなど）
・情報の共有先
・情報提供が任意の場合に、個人が情報を提供するか決定するためにどのような機会があるか
・個人が特定の情報利用に同意を与えるか決定するためにどのような機会があるか（要求される利用又は認証された利用以外で）、また個人がどのように同意を与えられるか
・どのように情報が安全化されるか（運用上及び技術的コントロール）
・プライバシー法552a条に基づいてシステム記録が作成されるか否か

②PIAの結果として、ITシステムや情報収集に関して行政機関がどのような選択を行ったか特定しなければならない。

---

[1] http://www.whitehouse.gov/omb/memoranda_m03-22
[2] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf
[3] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_template.pdf
[4] たとえば内務省→http://www.doi.gov/ocio/privacy/pia.html
[5] OMBガイダンスII C

③PIA の範囲と深度は、収集される情報の性質及びシステムの複雑性に釣り合ったものでなければならない。

・システム開発関連ドキュメント中でプライバシーについて言及しなければならない（必要性の言及、分析機能要件、代替案の分析、フィージビリティー分析、費用対効果分析、初期リスクアセスメントなど）
・システムが個人のプライバシーに与える影響度に言及しなければならない（特に、上記①の各項目に関連する潜在的脅威を特定し評価する）
・概念設計段階で特定されない要素（情報の保管や廃棄など）を検討するため、新たな情報収集を反映するため、又は分析の結果システム若しくは情報収集の設計に際してなされた選択について言及するために、システムをデプロイする前に PIA をアップデートする必要があり得る
・情報ライフサイクル（収集、利用、保管、処理、開示及び破棄）を考え、各段階での情報の取り扱いがどのように個人のプライバシーに影響を与え得るかを評価しなければならない。

④主要なシステムについてはさらに以下の分析を行わなければならない。

・情報収集の結果及び情報フロー
・設計された収集及び取扱い方法の代替案
・各代替案で特定されたリスクを軽減するための適切な措置
・最終設計又はビジネスプロセスの論拠

⑤定型データベースシステム

定型情報や限定的な利用及びアクセスの単純なシステムについては、標準化された PIA アプローチ（チェックリスト又はテンプレート）を用いることができる。

（３）国土安全保障省による PIA テンプレートの概要

- 要約（Abstract）
  - ✧ 事業の名称、事業の簡単な説明、プログラムが作成される理由及び PIA を必要とする理由（事業が個人情報を必要とするため、技術がプライバシーセンシティブであるため、など）を記載する。
- 概説（Overview）
  - ✧ 事業の目的を理解するために必要な背景、プライバシーに影響を与えうる事業を行うことを正当化できる理由を記載する。

記載上の注意

- 事業の目的、部署の名称、法律上の根拠、事業が部署の使命とどのように関係するか
- 事業がどのように個人情報を収集し使用するか（個人情報のライフサイクル（収集から廃棄まで）を詳述する典型的なトランザクションなど）
- プライバシー保護及びリスク軽減のためにプログラムが講じた措置（逐一記述するのではなく全体観を記載する）
- 事業がそれに基づいて運営する契約など
- 外部と共有される所定情報（routine information)、及び外部と情報共有された情報がどのように元々の情報とどのように互換的なのか
- 主要な潜在的プライバシーリスク、プログラムが個人に与える全体的なプライバシーインパクト
- 使用技術、事業のために情報がどう収集されるかについての短い説明

➢ 1.0　権限その他（Authorities and Other Requirements）

✧ 1.1　情報収集を許可し定義する法的権限・契約（Legal authorities and/or agreements）

記載上の注意

- 根拠法や根拠契約をすべて記載する。そしてかかる根拠法や根拠契約が、情報収集及び利用をどのように許可しているかも記載する。

✧ 1.2　SORN（米法特有のプロセス）

✧ 1.3　システムセキュリティプラン（米法特有のプロセス）

✧ 1.4　記録保管期間

記載上の注意

- 事業の必要性に合致する、情報保管に必要な最低限の期間を定めなければならない。
- （米では、NARA(National Archives and Records Administration)による承認という、特有の承認プロセスがあるため、承認を得ているか、得ていない場合は承認を得るためのどの段階にあるかを記載する。）

✧ 1.5　OMB Control number など（米法特有のプロセス）

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

✧ 要求・収集される情報の範囲と収集の理由

✧ 2.1　事業が収集、利用、配布又は保持する情報の特定

記載上の注意

- 情報が収集される個人の分類（category）を特定（Identify）する
- 分類ごとに、事業によって収集され保存される、個人情報を含むすべての情報をリストアップする
- 事業が新しい情報を作成する場合(Score､分析又はReportなど)、それがどのようになされ、その情報の目的が何か
- 事業が他のシステムから情報を受け取る場合、情報が起源したシステムを説明する（どのような情報が返ってきて、どのように利用されるかの説明を含む）

✧ 2.2 事業のために収集される情報及びその情報源・収集方法

記載上の注意

- 2.1で特定された情報を提供する個人を列挙
- 商業データ業者、他省などの、個人以外の情報源から情報を収集する場合、その情報源を記載し、なぜ個人以外の情報源からの情報が要求されるかの理由を記載する
  - 例）RFID、ビデオカメラなど

✧ 2.3 商業情報源又は公開データを使用しているか？その場合､その理由及びその方法を記載する

記載上の注意

- 例）Lexis Nexisのような商業情報源、又は裁判所の記録のような公開データ
- 例）個人に関する情報の第一次情報源として商業データを使用します。代替案としては、商業データを、個人に関する情報や個人により既に提供された情報を検証するために使用することを検討しています。

✧ 2.4 データの正確性の確保

記載上の注意

- 事業がどのように情報の正確性をチェックしているか
- 正確性チェックのために使用されるプロセスを記述する。商業データ業者が関わっている場合、契約で要求される正確性のレベルを記述する。正確性をチェックしない場合、理由を説明する。
- データの正確性と完全性を向上させるための技術的手段、政策（Policy）又は手続きを記述する
- 例）本事業は、個人に関する決定を下すために情報を利用する前に、個人により提供される情報を、他の情報源による情報（貴組

織内又は外）と照合してチェックすることができます。

- ✧ 2.5 PIA：情報の特徴に関連して

  記載上の注意

  - 収集されるデータの要素に鑑み特定されるプライバシーリスクを記述した上で、各リスクをどのように緩和・軽減するか記述する。
  - その際、FIPPs（Fair Information Practice Principles、FTC の原則）を考慮して答えること
    - 特定目的の原則（Principles of Purpose Specification）
    - 最小化の原則（Principle of Minimization）
    - 個人参加の原則（Principle of Individual Participation）
    - データクオリティ及び完全性の原則（Principle of Data Quality and Integrity）

- 3.0 情報の利用（Uses of the Information）
  - ✧ 3.1 情報利用の方法及び情報を利用する理由

    記載上の注意

    - 収集又は保持される情報の利用を列挙。社会保障番号 SSN が収集される場合、SSN が必要な理由及び使用方法を記述する。
    - 例）本事業は、氏名、生年月日及びパスポート情報を必要とします。その理由は、かかる情報が、テロリストスクリーニングデータベースにとって最適であるからです。
  - ✧ 3.2 データベースにおいて、予測パターンや異常検知のために検索処理、分析処理などを行うか？行う場合、どのようにその結果を使用するか？

    記載上の注意

    - 検索処理、分析処理などの処理結果を、個人の既存記録に付加するのか？ 新しい記録が作成されるのか？ 新しいデータにより個人に対するなんらかの措置がとられるのか？ 新しいデータは、個人についてなんらかの決定を行う公務員からアクセス可能か？その場合、どのような状況下で、そして誰によってその情報が利用されるのか？
    - ※3.1 の後に、どのようにその情報が使用されるかを説明する部分
  - ✧ 3.3 省内での情報共有の状況

    記載上の注意

    - どのチームやどの職位を有する職員が情報共有するか列挙
  - ✧ 3.4 情報利用に関連した PIA

    記載上の注意

- 情報が上記利用に従って扱われることを担保する方法を記述
- 例）ユーザトレーニング、システム処置（アクセス拒絶など）
- FIPPs のうちの透明性の原則や、利用制限の原則などに即した検討も記述する

➢ 4.0　通知（Notice）

✧ 4.1　情報収集前に個人に対しどのように通知がなされるか。通知がなされない場合はその理由

記載上の注意

- この通知にはプライバシーポリシーや PIA、SORN も含む
- かかる通知が十分な理由も記述する

✧ 4.2　個人が利用同意や情報提供拒否、オプトアウトをする機会があるか

記載上の注意

- 個人が情報提供を拒絶できる場合、情報提供の結果は通知に含まれているか
- 個人は特定の利用に対する同意ができるか、それとも包括利用に対する同意となるのか。特定利用に対する同意ができる場合、個人はどのように個々の利用に対して同意するのか。
- 特定利用に対する同意権や情報提供拒絶権の行使方法について通知に含めているのであれば、そのやり方を記載。それができない場合は（If this is not an option）なぜできないか記載する。（いくつかの例では、情報提供の拒絶は、単純に個人が本事業に参加しない選択をした場合を意味する。）

✧ 4.3　通知に関する PIA

記載上の注意

- 事業の目的や上記利用に対応した通知がどのように提供されるのか。最初の情報収集に対する通知が、情報の上記利用とどのように整合するのか。不十分な通知や拒絶・同意機会に関連したリスクをどのように軽減しているのか。
- FIPPs の観点から
  - 透明性の原則：個人に対して十分な通知がなされているか
  - 利用制限の原則:通知に記載された目的のためだけに情報が利用されているか。それを担保するためにどのような手続きがなされているか。
  - 個人参加の原則:アクセスや訂正に関する通知を提供したか？セキュリティ、保管、廃棄に関する情報やコントロールに関す

る通知などはあるか？

- 5.0　データ保管（Data Retention by the project）
  - ✧ 情報を保管する期間
  - ✧ 5.1　情報が保管される期間及びその理由

    記載上の注意
    - 事業が保管する情報の種類を特定する。収集したすべての情報が保管されるのか、特定のものについてのみ保管されるのか
    - 例）本事業は個人識別の検証のために最初に個人情報を大量に収集するが、検証処理が終了次第、検証処理結果（(例）承認済、承認されず）という新しい情報を保持し、その他の情報をすべて削除する。
    - 収集目的と保管期間の結びつきを説明する。事業のために最短期間、最少の情報が保持されるべき。
    - 例）本事業は詐欺が訴追されうる期間、情報を保管し、その後削除する。
    - 一定期間はアクティブステータスで情報を保管し、その後アーカイブするといった場合は、アーカイブ記録についても保管期間を記載する。いつから期間が開始するか記載する。
  - ✧ 5.2　保管に関するPIA

    記載上の注意
    - データ保管期間に関するリスクとその対応策
    - 保管期間が長いほど、情報のセキュア化とその正確性、完全性を保証する必要が大きくなる。
    - システムの目的やミッションに沿った期間としなければならない。
    - FIPPsの観点から
      - 最小化の原則（Principle of Minimization）：目的にとって必要な情報のみ保管しているか
      - データクオリティ及び完全性の原則（Principle of Data Quality and Integrity）：関連性のなくなった個人情報及び不要となった個人情報を消去するためのポリシーや手続きが、PIA上で記載されているか
- 6.0　情報共有（Information Sharing）
  - ✧ 外部の機関（他の連邦政府機関、地方政府機関、民間事業者）との情報共有
  - ✧ 6.1　通常のオペレーションとしてDHS（国土安全保障省）の外部と情報共有がされるか？その場合組織を特定し、情報がどのようにアクセ

スされ利用されるのかを記載する。

記載上の注意

- 個別の名称を挙げるよりもどのような種類の組織と共有するのかを記載する

✧ 6.2　外部共有（6.1）が SORN（1.2）とどのように整合するか（米法特有のプロセス）

✧ 6.3　再配布の制限

記載上の注意

- DHS（国土安全保障省）と情報を共有した外部機関が、さらに他の組織とかかる情報を共有することに課されうる制限を記述する

✧ 6.4　外部への開示記録をどのように保持するか

記載上の注意

- Privacy Act subsection c により、法の適用除外になる場合でも、DHS（国土安全保障省）は誰に対してどの記録を開示したかについての報告を保管しなければならない。事業がかかる記録を保持している場合、どの情報が保管されるか列挙する。記録を保持しない場合、その理由を記載する。

✧ 6.5　情報共有に関する PIA

記載上の注意

- 外部との情報共有に関連するプライバシーリスクを記載。かかるリスクがどのように緩和されたのか。
- アクセス制限が実装されているか、外部との適切な共有を担保するために監査ログが定期的にチェックされているか。たとえば MOU(Memorandum Of Understanding)、契約などが外部機関や外国政府との間で締結されているか
- 外部との情報共有が、事業の目的や当初の収集の利用とどのように整合しているか

➢ 7.0　救済（Redress）

✧ 個人が救済を求める手続き。記録へのアクセス、正確性確保、苦情申立ても含む。

✧ 7.1　個人が自身の情報にアクセスできるための手続き

記載上の注意

- 情報公開法（FOIA）や Privacy Act の実務を含める
- 利用者用の苦情窓口（Customer Satisfaction unit）があれば、連絡先情報とともにそれも記述

✧ 7.2　個人が情報を訂正するための手続き

- ✧ 7.3　訂正手続きを個人にどのように通知するか
- ✧ 7.4　救済に関するPIA

記載上の注意

- 事業がPrivacy Act及びFOIA法下でアクセス及び訂正に関し提供している救済について記載する
- FIPPsの観点から
  - 個人参加の原則（Principle of Individual Participation）：自分に関する記録を事業が保持しているか否かについて、個人が知ることができるか
  - 個人参加の原則（Principle of Individual Participation）：アクセスや訂正が拒否された場合、その理由や不服申立てについて個人に通知されるか
  - 個人参加の原則（Principle of Individual Participation）：自分に関する情報が、自分の知らない間に目的外利用されることを、個人が防止するためのメカニズムがあるか

- ➢ 8.0　監査及び責任（Auditing and Accountability）
  - ✧ 8.1　PIAに記載されたプラクティス通りに情報が利用されることを、事業はどのように確保するか

記載上の注意

- 監査手段のほか、情報共有プロトコル、特別なアクセス制限、その他の手当てなどの技術的、政策的予防措置を記載
- 各々のユーザがアクセスできる記録を、監査手段において特定できるのか。アクセス制限（あるユーザは読み取りのみ可能であるが、その他のユーザは改変可など）があればそれについて記載する
- 自己監査か、第三者監査か、Office of Inspector General かGovernment Accountability Office(GAO)が監査するか説明する
- 情報の不正利用を検知する自動ツールの有無（例：特定の記録にアクセスがなされた際、記録が適正に利用されたか確認するため、監督者へ通知がなされた上で監督者がチェックする）

- ✧ 8.2　プライバシートレーニング

記載上の注意

- 適切な取り扱いのための研修
- ユーザトレーニングが完了したことを確保するための手当て

- ✧ 8.3　どのユーザが情報にアクセスできるか決定する手続き及び方法

記載上の注意

- 電子媒体及び紙媒体双方の情報にアクセスする個人に関する手続き及び認証
- 情報にアクセスする外部者を特定し、どのような役割の下かかる外部者がアクセスを行うのか特定する。
- リモートアクセスが許可されている場合、又は外部記憶やデバイスがシステムと接続している（Interact）場合は、通信（Transmission）及びデータストレージをセキュア化するための措置を記述する（例：暗号化、二要素認証（two-factor authentication））

✧ 8.4　事業が、情報共有契約、覚書、情報の新しい利用、システムへの新しいアクセスをどのようにレビューし承認するのか

記載上の注意

- 例:すべての覚書は、プログラムマネージャー、Component Privacy Officer、カウンセルによってレビューされ、その後 DHS に公式レビューのために送付されます

➢ 署名（Approval Signature）

２　オーストラリア

（１）PIA に関する指針

・プライバシーコミッショナーオフィスによる PIA ガイド[6]

（２）プライバシーコミッショナーオフィスによる PIA ガイドのうち質問票に相当する事項

PIA ガイドは PIA について特定の形式を要求するものではなく、プロジェクト及び収集される情報の性質に応じた柔軟な対応を行うべきとされている。

一般的に PIA プロセスの主要フェーズは以下の 5 つ[7]。

①プロジェクト説明
②情報の流れのマッピング及びプライバシーフレームワーク
③プライバシーに対する影響の分析
④プライバシーマネジメント
⑤推奨事項

①プロジェクト説明[8]

プロジェクトの「大きい絵」が必要であり、以下を含むものとする。

・全体的な目的
・全体的な目的が組織の目的とどのように合致するか
・プロジェクトの範囲
（取り扱われる個人情報の品質、機微性、プロジェクトの重要性、プロジェクトの規模・複雑性、組織をまたがるプロジェクトか否か、プロジェクトが持つ国民への影響）
・既存プログラムや他のプロジェクトとの関連性
・主要なプライバシー要素
（例：収集される情報の範囲・種類、セキュリティ対応、データ品質の確保、情報の使用・開示方法、外部委託の有無、技術・法令の新規性、個人情報の新たな収集を伴うか、個人情報の新

6 http://www.privacy.gov.au/materials/types/download/9509/6590
7 PIA ガイド xii
8 PIA ガイド Module B – Nature of the Project も参照

たな取扱い方法を伴うか）

・新規プロジェクトか既存プロジェクトの変更か

既存プロジェクトの変更で、かつ範囲が比較的限定されている場合（例：小規模な調整にとどまり、セキュリティ措置が正しく講じられた上で収集がなされ、限定された量の、機微情報以外の個人情報の利用がなされる場合）、小規模 PIA のみが必要となる場合が多い。

②情報の流れのマッピング及びプライバシーフレームワーク

・取り扱われる個人情報は何か
・どのように個人情報が収集・使用されるか
・内部フロー
・開示
・セキュリティ措置
・データ品質措置
・情報の流れに適用されるプライバシー、守秘その他関連法令
・情報の流れに適用される組織内、業界内等ルール
・現在の個人情報環境とプロジェクトがそれにどのような影響を与えるか
・個人が情報にアクセス・訂正請求する方法
・認証管理システム

＜参考→PIA ガイド　Module C : Mapping Information Flows＞

１　収集

※不必要又は関連性のない個人情報を収集していないか、侵害的な収集を行っていないか

・組織の機能又は活動に収集がどのように関係するか
・収集を正当化する公衆の便益は何か
・プロジェクトにとってなぜ個人情報が必要なのか（特定の項目や種類がなぜ必要なのか）
・情報は識別されない形又は匿名にて収集できるか否か
・個人は一部又はすべての個人情報を提供しないことを選択できるか否か
・どのように情報が収集されるのか
・一定の個人に対して不合理に侵害的な方法となりうるか

１．１　収集の範囲

※不必要又は関連性のない個人情報を含む大量収集を行っていないか

・収集される個人情報（例：名前、住所、職業、識別番号）
・収集元
　（例：個人から直接、他の個人から、他の組織から、公開情報から）
・なぜ各情報が収集されるのか
・情報に対価が支払われるか、有価値物と交換されるか否か
・個人情報収集時に、個人の状況はどのように考慮されるか
　（例：文化的多様性、聴覚障害、英語以外の言語）
　（例：経済的、政治的、宗教信念的、健康、性的、生体、ジェネリック情報など収集の機微性や各収集の目的を特定）
・情報収集の法的権限又は法的要求
・検討されたものの採用されなかった代替収集案
　（例：非識別データの使用）
・個人の同意を取得する場合は、概要を記載する
　（例：収集の一部又は全部について同意しないと、個人が利用できない特定のサービスや便益があるか）

１．２　通知

※収集の事実やその目的に個人が気づいていないことはないか。個人に対し驚きのないように透明な方法で個人情報を常に取り扱うこと。

収集に関して個人に与えられる情報、及びかかる情報がどのように提供されるかを特定し説明すること。説明には以下を含むこと。

(a)目的・権限
・なぜ個人情報が収集されるのか
・収集は法によって認められているのか又は法によって要請されているのか。該当する場合は何法か
(b)使用・開示

・収集の目的と整合する使用・開示
・開示先（・再開示先）
・収集目的以外の目的に用いられることが想定される使用又は開示
(c)選択
・個人情報の取扱方法について個人が選択できる場合、個人はそれをどのように知るか。貴組織は個人に通知したか

１．３収集方法

※内密に行われる収集は一般的にきわめてプライバシー侵害的であり、規定された状況下以外で行われてはならない

以下を特定し説明すること。
・個人情報はどの程度の頻度で収集されるか
（1 度のみか、継続的にか）
・写真、指紋、虹彩、薬物テスト、ジェネリック情報の収集など、潜在的に機微性又は侵害性を有する収集方法
・内密に行われる収集方法（例：監視、Web サイトクッキー）、なぜそれが必要で適切といえるのか
・技術はプライバシー保護型か侵害型か、そしてなぜそのような技術を用いているのか

２　使用

※驚きのないように！個人情報は個人が予測できる方法で使用すること
・一般に「使用」とは、個人情報に対して、情報が収集された組織によって何が起こるかを意味する。

２．１　使用

以下を特定し説明すること。
・個人情報のすべての使用（予測されうるが一般的でないものも含む）
・上記使用がどのように収集目的に関連しているか
・情報収集後になされた使用目的の変更
・派生目的のための使用を防止するための措置

２．２　派生目的

※計画にない派生目的のために個人情報を使用しないこと

派生目的に情報が使用されうる場合は、以下を特定し説明すること

・派生目的に同意が要求されるか
・収集目的に直接関連した使用であるか
・派生目的使用を拒絶しても、当該個人はプロジェクトに参加し続けることができるのか
・派生目的使用を拒絶した個人についてはどうなるのか
・新しい、計画にない目的で個人情報を取り扱うことになった場合、個人は決定にどのように関わるのか

２．３　データ連携・マッチング

※不必要又は計画にないデータ連携を行わないこと

異なる目的のために収集された個人情報を統合することはプライバシーリスクをもたらす（たとえば、以前は利用できなかった個人情報や、目的に照らして不必要な個人情報を明らかにしてしまう）。

以下を特定し記載すること。

・（貴組織又は他の組織が）異なるデータベースに保有された情報と個人情報をデータマッチングするか、連携するか又は相互参照する意図や潜在性
・データマッチング、連携又は相互参照がどのように行われうるか
・個人に対し影響を与える決定で、データマッチング、連携又は相互参照をもとにして行われるもの
・情報の不適切なアクセス、使用及び開示を制限するための措置
・監査その他の監督のための仕組み
・データ連携の正確性を確保し、個人が不正確なデータマッチングにより悪影響を受けないための保護措置
　（例：個人はデータ連携について知らされているか）

３　開示

※驚きのないように、個人に開示について知らせること
※予期しない開示はプライバシーに関する苦情につながりうる

以下を特定し記載すること。
・誰に対し、どのように、なぜ個人情報が開示されるのか
・貴組織によって保有されているのと同様に、開示される情報がどのようにプライバシーリスクから保護されるのか。
（例：プライバシー法又は類似のプライバシー法令の対象となる）
・情報は公開されるか又は登録され開示されるか
・個人は開示について知らされているか。その際個人がとりうる選択肢は何か（公開する、差し止めるなど）
・開示は法によって認められているか要請されているか。関連条項を特定する。

４　開示及び訂正
※不正確な情報は誰にとっても問題を引き起こしうる

・自己の個人情報に個人がどのようにアクセスできるか（費用も記載する）
・自己の個人情報を個人がどのように訂正できるか

５　セキュリティ
※内部者・外部者による不正なアクセス及び使用を防ぐこと
IT、通信及び物理的セキュリティ対策を評価すること
（例：ノート PC、暗号化、敷地及びシステムへのアクセス（物理的及びオンライン上））

以下を記載すること。
・個人情報を喪失、不正アクセス、不正利用、不正改変、不正開示その他の不正から保護するためのセキュリティ対策
・敷地間でどのようにデータが移動するか
・個人情報が人によって管理される場合どのように保護されるのか
・アクセス可能な者はだれか
・アクセスを認証する者はだれか
・不正利用又は不適切なアクセスを防止し検知するシステム

・セキュリティ違反があった場合にとられる措置（例：個人への通知）

５．１　保管及び破棄

※不必要に個人情報を保管しないこと

以下を特定し記載すること。

・個人情報が識別できないようにされる時期又は廃棄される時期

・上記がどのように安全になされるのか

・情報保管ポリシー、廃棄スケジュールが実施されているか

・上記ポリシーおよび記録廃棄に関する関連法令への遵守がどのように評価されるか

６　データ品質

※品質の低いデータに基づいて決定を行わないこと

以下を特定し記載すること。

・個人情報が不正確又は最新でないことで個人にどのようなことが起こるか

（情報を用いてなされる決定の種類、不正確な情報のリスク、情報の最新性をどのように保持するかも記載すること）

・関連性があり、最新かつ完全な情報のみが使用又は開示されることを担保するプロセス

・個人情報を以前に提供された者に対し、どのように情報の更新を行うか

７　本人確認

※必要ない限り、本人確認を行わないこと

以下を特定し記載すること。

・匿名情報又は識別されない情報を用いてプロジェクトを進行できる範囲

・本人確認が必要か否か。必要とされる確信の程度

・どのように本人確認がなされるか

・個人に対し発行される新しい識別番号が必要か。その目的、当該番号が他の目的や他の組織によって採用されうるか、それを防ぐ

ための措置
・当該識別番号やその他の識別番号についての予想される使用及び開示
・個人の適格性など、その他確認が必要な情報

③プライバシーに対する影響の分析

・影響が不可避か
・プライバシーに対する影響はプロジェクトの目標に影響をどのように与えるか
・特定の情報にアクセスする個人の選択についてプロジェクトがどのように影響を与えるか
・情報が収集される内容・文脈

＜参考→PIA ガイド　Module D：Privacy Impact Analysis＞

プライバシーに対する影響の分析は、以下を調査する。

・情報の流れが、個人情報が取り扱われる方法についての個人の選択にどのように影響を与えるか
・個人の生活に対する侵襲性の程度
・プライバシー法への遵守
・プロジェクトが社会の期待とどのように適合しているか

主要な質問

・プライバシー関連法令（Module E,F を参照）や、個人情報に適用されるその他特定の法令上の義務を、プロジェクトが遵守しているか
・個人が情報のコントロールを断念せざるをえなくなるか。その場合はその程度
・個人が貴組織と関わる方法をプロジェクトが変更するか
（例：より頻繁に本人確認が実施される、異なる状況で確認される、費用、本人確認書類を有さない個人又は団体に対する影響）
・プロジェクトにおいて個人情報が取り扱われる方法について、個人にとって重大な決定（サービスや便益に関する決定など）を行うか。かかる決定について適切に知らせるような正確な関連情報を提供しているか。
・苦情対応の仕組みがあるか
・プライバシーに対する違反をどのように取り扱うか

・問題が生じた際の監査・監督のための仕組み（緊急手続きを含む）があるか
・機能の逸脱がありうるか
（例:プロジェクトのために収集した個人情報を他の目的に使用することに利益があるか？将来的にかかる事態が起こりうるか？）
・認証されていないユーザにとって価値のある情報か
（例:他者が金銭を支払う情報か。他者がアクセスしようと相当の努力を行う情報か。）
・（物理的又は財産的）侵害や（公然又は秘密裏の）監視を完全に正当化することができるか。またそれらは効果に釣り合ったものか。プロジェクトの目的達成のための唯一の方法か。侵害性がもっとも少ない方法で行われるか。法令又は司法当局に服するものか。どのような監査・監督措置がとられるか。
・プロジェクトは、公衆がプライバシーに対して有する価値とどのように整合しているか
（例:新しい個人識別の方法をとるか、重大なデータベースを作成するか、ジェネリック又は生体情報を使用するか）
・プライバシーが、費用対効果や投資価値の分析の要因として考慮されているか

＜参考→PIA ガイド Module E:Compliance Checklist for Agencies＞
行政機関向けコンプライアンスチェックリスト（未翻訳）
＜参考→PIA ガイド Module F : Compliance Checklist for Organizations＞
民間・NPO 向けコンプライアンスチェックリスト（未翻訳）

④プライバシーマネジメント
プライバシー保護とプロジェクトの目標双方が達成可能であること（プロジェクトの目標を譲歩することを必ずしも意味しない）。

＜参考→PIA ガイド Module G : Privacy Management＞
PIA で特定されたプライバシーに対する悪影響に対し、以下の対策を行うことができる。
・利益との均衡
プロジェクトの目的、組織の利益と影響を受ける個人の利益の

間に適切な均衡がなければならない

・最小限の原則

・均整

便益とプライバシーの間は釣合いがとれていなくてはならない。便益は実現されるか。

・透明性及び説明責任

プライバシー対策は、適切な通知及びプライバシーポリシーによって個人に対し常に透明でなければならない。組織は、個人情報をどのように管理するか、苦情処理、監査、監視方法を含めて説明しなければならない。

・柔軟性

プロジェクトによって影響を受ける個人の多様性を考慮しなければならない。

（例：特定の個人にとって、他者とは異なり機微性が高くなる情報がある。）

・成果物

プライバシー保護は、法令その他の拘束力のある義務及び新しい技術に組み込まれなければならない。

・プライバシー保護技術（PET）

・実装後のレビュー

⑤推奨事項

プロジェクトの将来的事項について推奨事項を記載すること。

PIA 報告書では不可避の影響又はリスクを特定し、それらを許容可能なレベルまで軽減するか又は除去する方法を推奨しなければならない。それら推奨事項の例としては以下。

・プロジェクトの目標、影響を受ける個人の利益と組織の利益との間により適切なバランスを保つような推奨事項

・さらなる対話の必要性

・プライバシーに対する影響が重大すぎてプロジェクトが進行できないか否かに係る推奨事項

３　イギリス

（１）PIA に関する指針

・　ICO による PIA ハンドブック[9]

（２）ICO による PIA ハンドブックで報告書に記載すべきとされている事項

・プロジェクトの説明
・プロジェクトから生じるプライバシーに関する問題の分析
・プライバシー侵害性を正当化する事由
・検討された代替案と決定の論拠
・採用されたプライバシー設計
・スキームやアプリケーションに対する国民の受容性に対する分析
（・利害関係者との意見交換の要約）
（・組織・個人の連絡先）
（・プロジェクト背景、PIA 計画書など）
（・関連法令・ガイドラインの参照）

※なお、スクリーニング質問で顕在化した、プライバシーに関する問題の分析を記載することも望ましい。スクリーニング質問については、参考資料８「諸外国における PIA 要否等判断基準」７ページ以下ご参照。

[9] http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

４　カナダ

（１）PIA に関する指針

- カナダ財務委員会（Treasury Board of Canada Secretariat）による PIA 指令[10]
- カナダ財務委員会による PIA ガイド：プライバシーリスク管理のためのフレームワーク[11]

（２）カナダ財務委員会（Treasury Board of Canada Secretariat）による PIA 指令のうちの質問票に相当する事項

以下は、PIA に含めるべき内容の最低限のものである。

＜セクションⅠ―概要及び PIA の開始＞

a. 政府機関。複数機関による PIA の場合は、主政府機関。
The government institution or, in the case of a multi-institutional PIA, the lead government institution.

b. 政府機関の長、又はプライバシー法 10 条（個人情報バンク）に対応する代表者。複数機関による PIA の場合は、関係する各政府機関の長もしくは代表者。
The head of the government institution or delegate for section 10 of the Privacy Act or, in the case of a multi-institutional PIA, the head or delegate of each government institution involved in the program or activity.

c. 新しく導入するか又は大幅な変更を行うプログラム又は政府活動に対する責任官
The appropriate senior official or executive for the new or substantially modified program or activity.

d. 政府機関のプログラム又は政府活動の名称及び説明。複数機関による PIA の場合は、主政府機関のプログラム又は政府活動の名称及び説明。

---

10 http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308&section=text
11 http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld01-eng.asp

Name and description of the program or activity of the government institution or, in the case of a multi-institutional PIA, of the lead government institution.

e. プログラム又は政府活動の法的権限。複数機関による PIA の場合は、関係する各政府機関の法的権限。
Legal authority for the program or activity or, in the case of a multi-institutional PIA, the legal authority for each government institution involved in the program or activity.

f. プログラム又は政府活動が、新たな個人情報バンクに関連しているものか、既存の個人情報バンクを大幅に変更するものかの特定。既存の個人情報バンクについては、タイトル、登録番号及びバンク番号によって識別されることとする。
Identification of whether the proposal is related to a new PIB or will substantially modify an existing PIB. Existing PIBs are to be identified by their title, registration number and bank number.

g. プロジェクト若しくは政府活動又は変更の概要。
Short description of the project, initiative or change.

h. 複数機関による PIA の場合、主政府機関は、そのプログラム又は政府活動を支持する、PIA の完成及び承認に対する手順を記載する。最低限、関係する各政府機関を識別し、別の手順により決定されない限り、プログラム又は政府活動に関する各政府機関の役割を適切に記載するものとする。
In the case of a multi-institutional PIA, the lead government institution will describe the approach for the completion and approval of the PIA in support of the program or activity. At a minimum, a multi-institutional PIA will identify the government institutions involved and ensure that the role of each institution with respect to the program or activity is adequately documented, unless otherwise determined by the approach.

＜セクションⅡ―リスク分野の特定及び分類＞
リスクスケールは昇順による（レベル１は潜在リスクが最も低いことを表し、

レベル４は潜在リスクが最も高いことを表している)。

まず、それぞれのリスク分野単独で評価するが、次により深い分析が必要かどうかを決定するために個々のリスク分野における結果を集合で評価する。レベル３又はレベル４であれば、そのリスク分野はより包括的な方法でリスク分析を行う必要がある。

a) プログラム又は政府活動の種類 Type of program or activity	リスク スケール
特定の個人についての決定を含まないプログラム又はサービス Program or activity that does NOT involve a decision about an identifiable individual	1
プログラム、政府活動、政府サービスの管理 Administration of program or activity and services	2
コンプライアンス又は規制のための調査や執行 Compliance or regulatory investigations and enforcement	3
犯罪調査や犯罪に対する法の執行又は安全保障 Criminal investigation and enforcement or national security	4

b) 個人情報や文脈の種類 Type of personal information involved and context	リスク スケール
権限あるプログラムによって、個人から直接収集したか、又は開示について個人の同意を得た、文脈上の機微性がない個人情報のみ Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program.	1
収集後に、他の機関が保持する個人情報の使用について	2

同意を得た、文脈上の機微性がない個人情報 Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source.	
社会保険番号、医療や金融などの機微性がある個人情報、又は個人情報の周辺の文脈に機微性がある場合（つまり、未成年、成年被後見人又は代理行為についての個人情報） Social Insurance Number, medical, financial or other sensitive personal information or the context surrounding the personal information is sensitive; personal information of minors or of legally incompetent individuals or involving a representative acting on behalf of the individual.	3
詳細な略歴、疑い、身体情報などの機密性のある個人情報又は個人情報の周辺の文脈に特に機微性がある場合 Sensitive personal information, including detailed profiles, allegations or suspicions and bodily samples, or the context surrounding the personal information is particularly sensitive.	4

c)協力者や民間部門の関与 Program or activity partners and private sector involvement	リスクスケール
一政府機関内で完結する（同一政府機関内のプログラム間のやり取り） Within the institution (among one or more programs within the same institution)	1
他の政府機関が関与する With other government institutions	2
他の機関や連邦・州・地域の連合や地方自治体が関与する With other institutions or a combination of federal,	3

provincial or territorial, and municipal governments	
民間企業や国際組織、海外政府が関与する Private sector organizations, international organizations or foreign governments	4

d) プログラム又は政府活動の期間 Duration of the program or activity	リスク スケール
１回限りのプログラム又は政府活動 One-time program or activity	1
短期間のプログラム又は政府活動 Short-term program or activity	2
長期間のプログラム又は政府活動 Long-term program or activity	3

e) プログラムにより影響を及ぼされる対象 Program population	リスク スケール
内部管理目的のプログラムで個人情報が使用され、特定の従業員に影響を与える The program's use of personal information for internal administrative purposes affects certain employees.	1
内部管理目的のプログラムで個人情報が使用され、すべての従業員に影響を与える The program's use of personal information for internal administrative purposes affects all employees.	2
外部管理目的のプログラムで個人情報が使用され、特定の個人に影響を与える The program's use of personal information for external administrative purposes affects certain individuals.	3
外部管理目的のプログラムで個人情報が使用され、すべ	4

ての個人に影響を与える The program's use of personal information for external administrative purposes affects all individuals.	

f) 技術及びプライバシー Technology and privacy
新しく導入されるか又は大幅に修正されるプログラム又は政府活動は、個人情報の生成、収集又は取扱いに関して当該プログラム又は政府活動を支援するために、新しい電子システムを実装するか、又は新しいアプリケーション若しくはソフトウェアを使用するか。 Does the new or substantially modified program or activity involve implementation of a new electronic system or the use of a new application or software, including collaborative software (or groupware), to support the program or activity in terms of the creation, collection or handling of personal information?
新しく導入されるか又は大幅に修正されるプログラム又は政府活動は、レガシーIT システムへの修正を必要とするか。 Does the new or substantially modified program or activity require any modifications to information technology (IT) legacy systems?
（特定の技術問題とプライバシー） Specific technological issues and privacy 新しく導入されるか又は大幅に修正されたプログラム又は政府活動は、新しい技術を実装するか、又は以下のいずれかの活動を含むか。 ・認証方法の強化 ・監視 ・自動化された個人情報分析、個人情報マッチングなど Does the new or substantially modified program or activity involve implementation of new technologies or one or more of the following activities: ・enhanced identification methods; ・surveillance; or ・automated personal information analysis, personal information matching and knowledge discovery techniques?

上記の質問の回答が「はい」の場合、プライバシーに対する懸念及びリスクが潜在することを示しており、検討（及び、必要があれば軽減策）が必要である。 A **YES** response indicates the potential for privacy concerns and risks, which will require consideration and, if necessary, mitigation.

g) 個人情報の伝達 Personal information transmission	リスク スケール
個人情報は閉じられたシステム内で使用される（すなわち、インターネット、イントラネット、その他のシステムと接続せず、文書の流通もコントロールされている）。 The personal information is used within a closed system (i.e., no connections to the Internet, Intranet or any other system and the circulation of hardcopy documents is controlled).	1
個人情報は、少なくとも一つの他のシステムと接続するシステム内で使用される。 The personal information is used in a system that has connections to at least one other system.	2
個人情報はポータブル装置（たとえば、USB キー、フロッピーディスク、ノートパソコンなど）に移される。 The personal information is transferred to a portable device (i.e., USB key, diskette, laptop computer), transferred to a different medium or is printed.	3
個人情報は無線通信で送信される。 The personal information is transmitted using wireless technologies.	4

h) プライバシー違反の際、個人や従業者に対し影響を与える潜在的リスク
Potential risk that in the event of a privacy breach, there will be an impact on the individual or employee.

i) プライバシー違反の際、組織に対し影響を与える潜在的リスク

Potential risk that in the event of a privacy breach, there will be an impact on the institution.

注：h)やi）の追加ガイダンスとして、政府機関は「プライバシー違反ガイドライン」を参照できる。

Note: For additional guidance on items h) and i), government institutions can refer to the Guidelines for Privacy Breaches.

複数機関での PIA の場合、各々の政府機関は、最低でも b)、c)、f)、g)、h)、i)に回答しなければならない。一方、主政府機関は、a)、d)、e）に回答しなければならない。

＜セクションⅢ—プログラム又は政府活動での個人情報の構成要素の分析＞

a. 収集する個人情報の各要素の特定（例えば、１）名前、２）住所)。
Identify each element of personal information collected (for example: 1) name, 2) address).

b. 収集する個人情報の各要素の下位要素の特定（例えば、１）名字、名前、２）通り名、番地、都市名、州名、郵便番号)。
Identify sub-elements associated with each element of personal information collected (for example: 1) first name / middle initial / last name, 2) street name / street number / city / province /postal code).

c. 個人情報がどのように記録されるか特定する。書面、電子的、聴覚記録、視覚記録、生体サンプル、その他（具体的に特定する）など。
Identify how the personal information will be recorded: on paper, electronically, audio recordings, visual image recordings, human biological samples or other (specify).

複数機関による PIA の場合、関係する各政府機関は、最低限、収集するか又は開示する個人情報の各要素を特定しなければならない。

＜セクションⅣ—個人情報の流れ＞

a. 個人情報の収集源及び個人情報の生成方法の特定
Identify the source(s) of the personal information collected and /

or how the personal information will be created.

b. 個人情報を使用・開示する、内部及び外部機関の特定。すなわち、個人情報へアクセスするか又は個人情報を取り扱う分野・グループ・個人、及び個人情報が誰に提供・開示されるかの特定。
関連する場合、以下の情報を含めること。
Identify both internal and external sources for the personal information's use and disclosure, that is, identify the areas, groups and individuals who have access to or handle the personal information and to whom it is provided or disclosed. Where relevant, include the following information:

- プログラム又は政府活動に対して責任を有する政府機関（個人情報バンクの表題及び番号も記載する）
Government institution responsible for the program or activity (provide PIB title and number);
- プログラム又は政府活動に対して責任を有する他の政府機関（個人情報バンクの表題及び番号も記載する)、又は
Other government institution responsible for the program or activity (provide PIB title and number); or
- 非連邦政府機関（たとえば、州政府、自治体、先住民政府、外国組織、国際組織など）若しくは民間部門
Non-federal government institution (e.g., provincial or territorial, municipal, or Aboriginal governments or councils, organization of a foreign state, international organization) or private sector.

c. 個人情報はどこを通過し、保存又は保持されるのかの特定
Identify where the personal information will transit and will be stored or retained.

d. どの分野、グループ、個人が個人情報にアクセスできるのかの特定
Identify where areas, groups and individuals can access the personal information.

政府は、個人情報の流れを示すフォーマットを決定することとなっている。

複数機関によるPIAの場合は、関係する各政府機関は、最低限、個人情報の

流れの概略を記載することに責任を有している。主政府機関は、関係する各政府機関間の個人情報の流れの概略を記載することに責任を有している。

＜セクションⅤ―プライバシーコンプライアンス分析＞

a. 最低限、プライバシーコンプライアンス分析は、以下の分野をカバーし、各分野の要求事項を満たす特定のコンプライアンス活動を特定しなければならない。
At a minimum, the privacy compliance analysis must cover the following areas and identify specific compliance actions taken or to be taken to meet with each area's requirements:

- 収集権限（プライバシー法４条）
  Collection authority (section 4 of the Privacy Act)
- 直接収集、通知及び同意（プライバシー法５条）
  Direct collection, notification and consent, as appropriate (section 5 of the Privacy Act)
- 保持（プライバシー法６条）
  Retention (section 6 of the Privacy Act)
- 正確性（プライバシー法６条２項）
  Accuracy (section 6(2) of the Privacy Act)
- 使用（プライバシー法７条）
  Use (section 7 of the Privacy Act)
- 開示（プライバシー法８条）
  Disclosure (section 8 of the Privacy Act)
- 安全管理措置
  Administrative, physical and technical safeguards
- 技術及びプライバシー課題
  Technology and privacy issues
  - ✧ システム、ソフトウェア、プログラムアプリケーションに影響があり、その結果、個人情報の生成、収集、保持、使用、開示及び処分に関連する現行のアクセスコントロールやプライバシー慣行に影響し得る、ビジネス要件に対する変更を示す。
    Indicate any changes to the business requirements that have an impact on the system, software or program application and, consequently, may affect the current access controls and privacy practices related to the creation, collection, retention, use, disclosure and disposition of personal

information.

- ✧ 維持されるか又は大幅に修正される現行の IT レガシーシステムやサービスが、プライバシー要件に遵守しているか決定する。
  Determine whether the current IT legacy systems and services that will be retained or those that will be substantially modified are compliant with privacy requirements.
- ✧ 新しい電子環境におけるプライバシー保護要件に関連する啓発活動を特定する。
  Identify any awareness activities related to protection of privacy requirements in the new electronic environment.

複数機関による PIA の場合は、関係する各政府機関は、最低限、管理下の個人情報に対するプライバシー慣行の概略を記載する責任を有する。

＜セクションⅥ—分析結果の概要及び勧告＞

a. リスク特定及び分類から導き出された結論又は勧告を、認識されたリスクに応じた方法で文書化する。
   Document the conclusion drawn or recommendations resulting from the risk identification and categorization in a manner that is commensurate with the risk identified.

＜セクションⅦ—付録文書リスト＞

a. 使用した文書又は PIA に関連する文書を挙げる。但し、添付不要である。

＜セクションⅧ—正式な承認＞

a. 政府機関の承認プロセスに従って、PIA が正式に承認されたことを示す。
b. 複数機関による PIA の場合は、主政府機関が、PIA が正式に承認された旨決定したことを示す。

上記セクションの完成及び要求された情報の提出をもって、PIA の最低要求事項が満たされる。