国民 ID とそれぞれの情報社会
に関する調査研究報告書
（諸外国におけるプライバシー影響評価）

2012 年 3 月

株式会社国際社会経済研究所

目　次

はじめに 3
１．PIA（プライバシー影響評価）の概要 4
　１．１　定義 4
　１．２　日本政府の検討状況 4
　１．３　欧州における状況 19
　１．３．１　EU データ保護指令における PIA 類似の制度：事前評価 19
　１．３．２　EU データ保護指令改定案 20
２．米国の状況 23
　２．１　米国の PIA 制度概要 23
　２．１．１　背景と経緯 23
　２．１．２　DHS のプライバシー遵守プロセス 25
　２．１．３　PIA における各機関の役割分担 27
　２．２　PTA（Privacy Threshold Analysis：プライバシー閾値分析） 27
　２．３　PIA（プライバシー影響評価） 30
　２．４　SORN（個人情報記録システムに関する告知） 36
３．カナダ（連邦）の状況 38
　３．１　カナダ（連邦）の PIA 制度概要 38
　３．２　PIA の実施手順 39
　３．３　コア PIA 42
　３．４　OPC における PIA のレビュー 44
　３．５　複数機関が関与する PIA について 47
４．カナダ（オンタリオ州）の状況 49
　４．１　カナダ（オンタリオ州）の PIA 制度概要 49
　４．２　PIA の構成要素 50
　４．３　PIA の実施手順 53
５．英国の状況 55
　５．１　英国における PIA 導入状況 55
　５．２　ICO（情報コミッショナーオフィス）の概要 56
　５．３　ICO が PIA において果たす役割 57
　５．４　英国における PIA の特徴 57
　５．５　ICO の PIA ハンドブックの概要 58
　５．６　PIA 実施プロジェクトの例 76
　５．７　英国におけるその他の個人情報保護関連の動向 85

６．ドイツの状況 88
６．１　ドイツにおける事前評価 88
６．２　データ保護監察官の概要 89
６．３　eID カードについて 90
７．日本での導入に向けた課題 92

参考文献 97

はじめに

日本政府は「社会保障・税番号制度」の導入にあわせて、番号制度が国民のプライバシーに与える影響を軽減するために、「番号」に関連した情報システムに対する「情報保護評価（＝プライバシー影響評価 Privacy Impact Assessment：PIA）」の実施を謳っている。

プライバシー影響評価（PIA）とは、個人情報を取り扱う情報システムの開発・改修に先立って、プライバシーへの影響を事前に評価し、問題回避のための運用的・技術的な変更を促すための一連のプロセスである。米国、カナダ、オーストラリア、ニュージーランド、英国といった国々では普及が進んでいるが、我が国では未導入の制度であり、制度の詳細については内閣官房主催の情報保護評価サブワーキンググループにおいて 2011 年 8 月から検討が始まったばかりである。

そのため、本事業では欧州・北米等の海外先進国事例の調査を行い、政府・関連省庁に対して情報提供と提言を行うことを目的とする。上期は、欧州（英国、ドイツ）の調査研究を行い、特に、英国では第三者機関によるガイドラインの発行や、行政機関に対する PIA の義務化など近年の動きが活発であるので、重点的に調査を行った。下期は、個人情報保護法制の一環として行政分野において PIA をいち早く導入し、PIA に関して 10 年近い実績と経験のある米国及びカナダの実態調査を実施した。また、2012 年 1 月に公表された EU データ保護指令改定案（EU データ保護規則案）において、新たに官民分野でのセンシティブ情報取扱い等に対する PIA 実施が義務付けられた EU の動向についても文献調査を実施した。

本調査研究が、我が国でのプライバシー影響評価制度の導入に向け、政府における検討の一助となれば幸いである。

１．PIA（プライバシー影響評価）の概要

１．１　定義

PIA は、Privacy Impact Assessment（プライバシー影響評価）の略語である。

「PIA とは何か」ということについては様々な機関等により定義がなされているが、本報告書では瀬戸[1]の定義に従い、「**個人情報の収集を伴う情報システムの導入または改修にあたり、プライバシーへの影響を事前に評価し、問題回避または緩和のための運用的・技術的な変更を促す一連のプロセス**」と規定する。

１．２　日本政府の検討状況

（１）社会保障・税番号大綱

本年 6 月に政府から公表された「社会保障・税番号大綱[2]」（2011 年 6 月 30 日）では、図 1 の通り、「番号」に関連した情報システムに対する「情報保護評価」の実施が謳われている。この情報保護評価が、PIA に該当するものである[3]。

同大綱の「第３　Ⅵ「番号」に係る個人情報の保護及び適切な利用に資する各種措置　12. 情報保護評価の実施」では、情報保護評価の趣旨として、「「番号」に係る個人情報の適正な取扱いを担保するため」、「情報システムの構築又は改修が「番号」に係る個人情報へ及ぼす影響を評価し、その保護のための措置を講じる」と謳われている。

さらに、「行政機関及び関係機関[4]は、「番号」に係る個人情報を取り扱うシステムを開発又は改修する前に、情報保護評価を行政機関又は関係機関内で実施した上で」、「番号制度における個人情報の保護等を目的とする委員会に報告し、その承認を受けるものとする」と規定されている。この「委員会」は、後述の社会保障・税番号制度の法律事項に関する概要（案）では「番号情報保護委員会」と呼ばれているが、諸外国の個人情報保護のための監督機関（いわゆる第三者機関）に相当するものである[5]。同大綱では、情報保護評価の結果は委員会に報告し、承認を受けることとなっているが、後述のように、カナダ、米国、英国、オーストラリア等の諸国では第三者機関が PIA 報告書の承認まで行うケースはない。

また同大綱では、委員会が「行政機関及び関係機関（義務付け対象者）向けガイドライ

---

[1] 瀬戸・伊瀬・六川・新保・村上著『プライバシー影響評価 PIA と個人情報保護』（中央経済社、2010 年）p1。

[2] 政府・与党社会保障改革検討本部「社会保障・税番号大綱」2011 年 6 月 30 日（http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/110630/honbun.pdf）。

[3] なお、「社会保障・税に関わる番号制度についての基本方針」（平成 23 年 1 月 31 日）（http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/110131/honbun.pdf）の時点では、情報保護評価は「プライバシーに対する影響評価」と呼ばれていた。これが、「情報保護評価」と名称変更された理由について、社会保障・税番号制度における個人情報保護対策を検討してきた個人情報保護ワーキンググループでは、口頭で「日本では法令の中でプライバシーについて明文化された規定がないため」との説明がなされている。

[4] 「関係機関」とは、日本年金機構や医療保険者等が該当する。

[5] だたし、諸外国の第三者機関は官民における個人情報保護全般を監督する機関であるのに対し、日本の同委員会は番号制度における個人情報保護のみを監督することとなっている。

ン、並びに地方公共団体及び法令に基づき「番号」を取り扱い得る事業者（非義務付け対象者）向けガイドラインを作成する」ものとされている。委員会は 2013 年前半に設立することが想定されているため、それまでは後述の情報保護評価サブワーキンググループにおいてガイドラインが検討・作成されることとなる。

「社会保障・税番号大綱」（平成 23 年 6 月 30 日）
「第３　Ⅵ 「番号」に係る個人情報の保護及び適切な利用に資する各種措置
12. 情報保護評価の実施
（1）「番号」に係る個人情報の適正な取扱いを担保するため、「番号」に係る個人情報の保護に関する事前評価（以下「情報保護評価」という。）を実施し、情報システムの構築又は改修が「番号」に係る個人情報へ及ぼす影響を評価し、その保護のための措置を講じることとする。
（2）行政機関及び関係機関は、「番号」に係る個人情報を取り扱うシステムを開発又は改修する前に、情報保護評価を行政機関又は関係機関内で実施した上で、その結果をＸＩで後述する内閣総理大臣の下に置く、番号制度における個人情報の保護等を目的とする委員会に報告し、その承認を受けるものとする。
（3）ＸＩの委員会は、行政機関及び関係機関（義務付け対象者）向けガイドライン、並びに地方公共団体及び法令に基づき「番号」を取り扱い得る事業者（非義務付け対象者）向けガイドラインを作成するものとし、情報保護評価の実施についての助言を行うことができることとする。ガイドラインには、情報保護評価を実施しなければならない情報システムについての基準や、情報保護評価の実施方法、実施手順等を記載することとする。
（4）番号制度開始と同時に運用に供される情報連携基盤等のシステムについては、ＸＩの委員会が設立される前に開発が行われることが想定される。そのため、個人情報保護ワーキンググループの下に情報保護評価サブワーキンググループを設置し、情報保護評価サブワーキンググループにてガイドラインを作成し、情報保護評価の実施についての助言等を行うこととする。」

図 1　社会保障・税番号大綱における情報保護評価

（２）情報保護評価サブワーキンググループ

情報保護評価の実施枠組みと情報保護評価ガイドラインの作成を具体的に検討するために、2011 年 8 月、個人情報保護ワーキンググループ[6]の下に情報保護評価サブワーキンググループ[7]（以下「情報保護評価 SWG」という）が設置された。

[6] 社会保障・税に関わる番号制度に関する実務検討会及びＩＴ戦略本部企画委員会の下に設置されたワーキンググループ。
[7] http://www.cas.go.jp/jp/seisaku/jouhouwg/index.html

（３）情報保護評価サブワーキンググループでの検討内容

2011 年 12 月 22 日に公表された「情報保護評価ガイドライン（案）」[8]では、主に以下の内容が提示されている。

○情報保護評価導入の趣旨

番号制度導入により、国家により個人の様々な個人情報が一元管理されるのではないかといった懸念や、「番号」に係る個人情報が不正に追跡・突合されるのではないかといった懸念、財産その他の被害が発生するのではないかといった懸念が生じることが考えられる。そこで、これらの懸念を踏まえ、国民の「番号」に係る個人情報が適切に取り扱われる安心・信頼できる番号制度の構築のために、「番号」に係る個人情報ファイルが取り扱われる前に、個人のプライバシー等に与える影響を予測・評価し、かかる影響を軽減する措置を予め講じるために、情報保護評価を実施する。

○ガイドラインの改定

第三者機関は、個人情報の保護に関する技術の進歩及び国際的動向を踏まえ、少なくとも 3 年ごとに、ガイドライン及び情報保護評価報告書記載事項について再検討を加え、必要があると認めるときはこれを変更する。

○情報保護評価の目的

以下の 3 点を目的とする。

①事後的な対応にとどまらない、積極的な事前対応を行うこと

②情報保有機関が国民のプライバシー等の権利利益保護にどのように取り組んでいるかについて、情報保有機関自身が宣言し、国民の信頼を獲得すること

③第三者機関が確認を行うことで、①②についての厳格な実施を担保すること

○情報保護評価の評価対象

情報保護評価の評価対象は、「個人情報」保護にとどまらない、国民の「プライバシー」保護とする。

情報保有機関は個人情報保護法令を遵守するだけではなく、法的に保護される個人のプライバシーを侵害してはならない義務を負っている。個人情報保護法令はプライバシーを中核とする私人の個人情報を保護するためのものであるが、それによりプライバシーに係る問題のすべてが解決されるわけではないと解される。

そこで情報保護評価では、個人情報保護法令の遵守にとどまらずプライバシー保護についても評価を行うものとする。

---

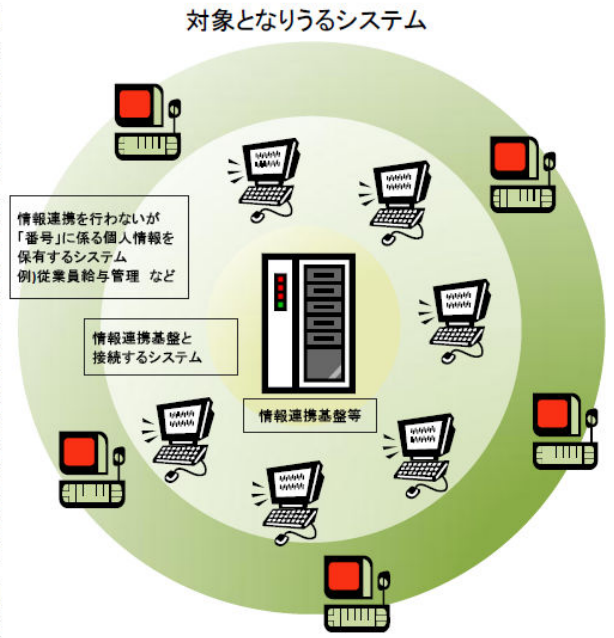
[8] http://www.cas.go.jp/jp/seisaku/jouhouwg/hyoka/dai4/siryou1.pdf

○情報保護評価の義務付け対象者

・行政機関の長[9]
・地方公共団体の長その他の執行機関
・独立行政法人等
・地方独立行政法人
・マイナンバー生成機関
・情報連携基盤を使用する事業者（大綱上の「関係機関」[10]に相当する者）

○対象となりうる機関

1	番号制度情報システム	
	1 運営機関（情報連携基盤・マイポータル）	
	2 「番号」生成機関を担う地方共同法人	
2	社会保障分野	
	1 行政機関（厚生労働省ほか）	
	2 関連独立行政法人	
	3 地方公共団体	約1,800団体
	4 日本年金機構	1団体
	5 国民年金基金連合会	1団体
	6 国民年金基金	約70団体
	7 企業年金連合会	1団体
	8 厚生年金基金	約600団体
	9 企業年金基金（確定給付企業年金 基金型）	約600団体
	10 企業（確定給付企業年金・確定拠出年金）（規約型）	約13,000団体
	11 規約型企業年金信託の受託者たる信託銀行	
	12 石炭鉱業年金基金	1団体
	13 国家公務員共済組合（国家公務員共済組合連合会含む）	約20団体
	14 地方公務員共済組合（地方公務員共済組合連合会・全国市町村職員共済組合連合会含む）	約60団体
	15 日本私立学校振興・共済事業団	1団体
	16 日本鉄道共済組合	1団体
	17 日本たばこ産業共済組合	1団体
	18 NTT厚生年金基金	1団体
	19 農林漁業団体職員共済組合	1団体
	20 全国健康保険協会	1団体
	21 健康保険組合連合会	1団体
	22 健康保険組合	約1,450団体
	23 国民健康保険組合	約170団体
	24 後期高齢者医療広域連合	47団体
	25 社会保険診療報酬支払基金	1団体
	26 国民健康保険団体連合会	47団体
	27 国民健康保険中央会	1団体
	28 保険医療機関	約180,000団体
	29 保険薬局	約50,000団体
	30 介護サービス事業者	約260,000団体
	31 社会福祉協議会	約1,800団体
	32 適用事業所（健康保険・厚生年金保険）	約1,740,000団体
	33 適用事業所（雇用保険）	約2,000,000団体
	34 上記の他、公務員災害補償システムを保有するすべての行政機関・関係機関	
3	税務分野	
	1 国税庁	1団体
	2 地方公共団体	約1,800団体
	3 上記の他、公務員給与システムを保有するすべての行政機関・関係機関	約270団体
	4 源泉徴収義務者・特別徴収義務者（給与所得）	約3,637,000団体
	5 4以外の法定調書提出義務者	



（注1）上記機関は、「番号」に係る個人情報を保有する機関の例として大綱等に記載されているもの。
（注2）上記機関は、情報保護評価の非義務付け対象者（地方公共団体及び民間事業者）を含む。
（注3）地方公共団体については、上記の約1,800の都道府県及び市区町村のほか、厚生福祉に関わる一部事務組合・広域連合（939団体）、職員の退職手当や公務災害に関わる一部事務組合（91団体）、税務徴収に関わる一部事務組合・広域連合（23団体）等が存在する。（「地方公共団体間の事務の共同処理の状況調（平成22年7月1日現在、総務省自治行政局地町村体制整備課）」より、内閣官房社会保障改革担当室が集計したもの）

図 2　情報保護評価の対象となりうる機関及びそのシステム[11]

○情報保護評価の実施対象

「番号」に係る個人情報ファイルを保有しようとする前に、情報保護評価を実施するものとする。具体的には、

9 情報連携基盤も対象となる。なお情報連携基盤は、マイナンバー法案では「情報提供ネットワークシステム」と呼ばれ、総務省の所管となっている。
10 「関係機関」とは、日本年金機構や医療保険者等が該当する。
11 出典：情報保護評価 SWG 資料。

①システム用ファイル
②手作業用ファイルのうち一定のもの
を対象とする。

○情報保護評価の実施時期
情報保護評価は、「番号」に係る個人情報ファイルを保有する前に実施しなければならない。具体的には、
①システム用ファイルについてはシステムの要件定義段階までに
②手作業用ファイルについては手作業処理の設計段階までに
情報保護評価を実施しなければならない。

○制度・施策に対する情報保護評価
プライバシー等に与える影響が大きいと考えられる制度・施策については、制度・施策の設計段階でかかる影響の評価・検討が推奨され、情報保有機関の任意の判断で、情報保護評価の枠組みを用いた評価を行えるものとする（図 3 参照）。

図 3　制度・施策に対する情報保護評価[12]

○情報保護評価の実施対象となる変更
情報保護評価は、「番号」に係る個人情報ファイルを新規に保有しようとする場合だけでなく、「番号」に係る個人情報ファイルの取扱いを変更する場合も、その対象とする。

○報告書の単位
システム用ファイルなどにおいては、1 つの「番号」に係る個人情報ファイルに付き 1 つの情報保護評価報告書を作成するよりも、複数の「番号」に係る個人情報ファイルを含む 1

12 出典：情報保護評価 SWG 資料。

つのシステムに付き１つの情報保護評価報告書を作成した方が、「番号」に係る個人情報ファイルの取扱いを分かりやすく明示できる場合も考えられる。

そこで、情報保護評価の対象は「番号」にかかる個人情報ファイルとするが、情報保護評価報告書作成に当たっては、「番号」に係る個人情報ファイルの取扱いのわかりやすさの観点から単位を検討するものとし、１つの報告書において複数の「番号」に係る個人情報ファイルをまとめて記載することも可能とする。

○情報保護評価の実施の仕組み

個人のプライバシー等に対し影響を与える可能性に着目して、以下の三段階にて、実施の仕組みを深めるものとする（図 4 参照）。

①「番号」に係る個人情報ファイルを保有しようとする場合は、しきい値評価を実施する。
②しきい値評価の結果、プライバシー等に対する影響を与える可能性があると認められる場合、重点項目評価を実施する。
③しきい値評価の結果、プライバシー等に対する影響を与える可能性が高いと認められる場合、全項目評価を実施する。

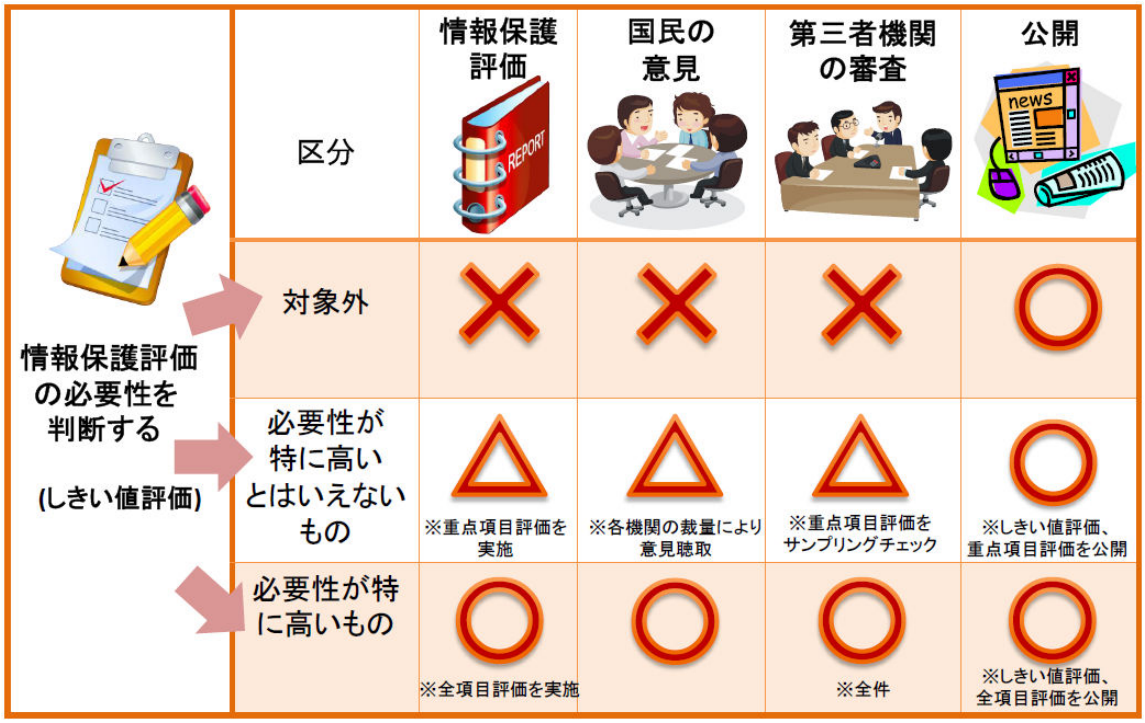


図 4　情報保護評価の実施の仕組み[13]

[13] 出典：情報保護評価 SWG 資料。

○しきい値評価

「番号」に係る個人情報ファイルを保有しようとする場合は、一定の例外[14]を除き、すべてが情報保護評価の対象となる。義務付け対象者は、情報保護評価として、まずしきい値評価を実施し、事実報告書を作成しなければならない。

しきい値評価は、情報保護評価の実施レベルを、「番号」に係る個人情報ファイルの取扱いが有するプライバシー等に与える影響度により振り分けるために行うものである。

情報保有機関は、「情報保護評価（しきい値評価）事実報告書記載事項」に従い、事実報告書を作成し、事実報告書をもとに、当該「番号」に係る個人情報ファイルが、

①しきい値評価のみで足りるものか

②重点項目評価を実施すべきものか

③全項目評価を実施すべきものか

を決定しなければならない（図 5 参照）。

なお、第三者機関は事実報告書について特段承認等を行うものではないが、法運用の統一性・法適合性を確保するための調整を行う観点から、情報保有機関は当該報告書を第三者機関に対し提出しなければならない。

情報保有機関は、事実報告書を第三者機関に対し提出した後、事実報告書を速やかに公表しなければならない。

14 職員の人事、給与、福利厚生に関する事項を記録した「番号」に係る個人情報ファイルや、会計検査院が検査のために保有する「番号」に係る個人情報ファイル。

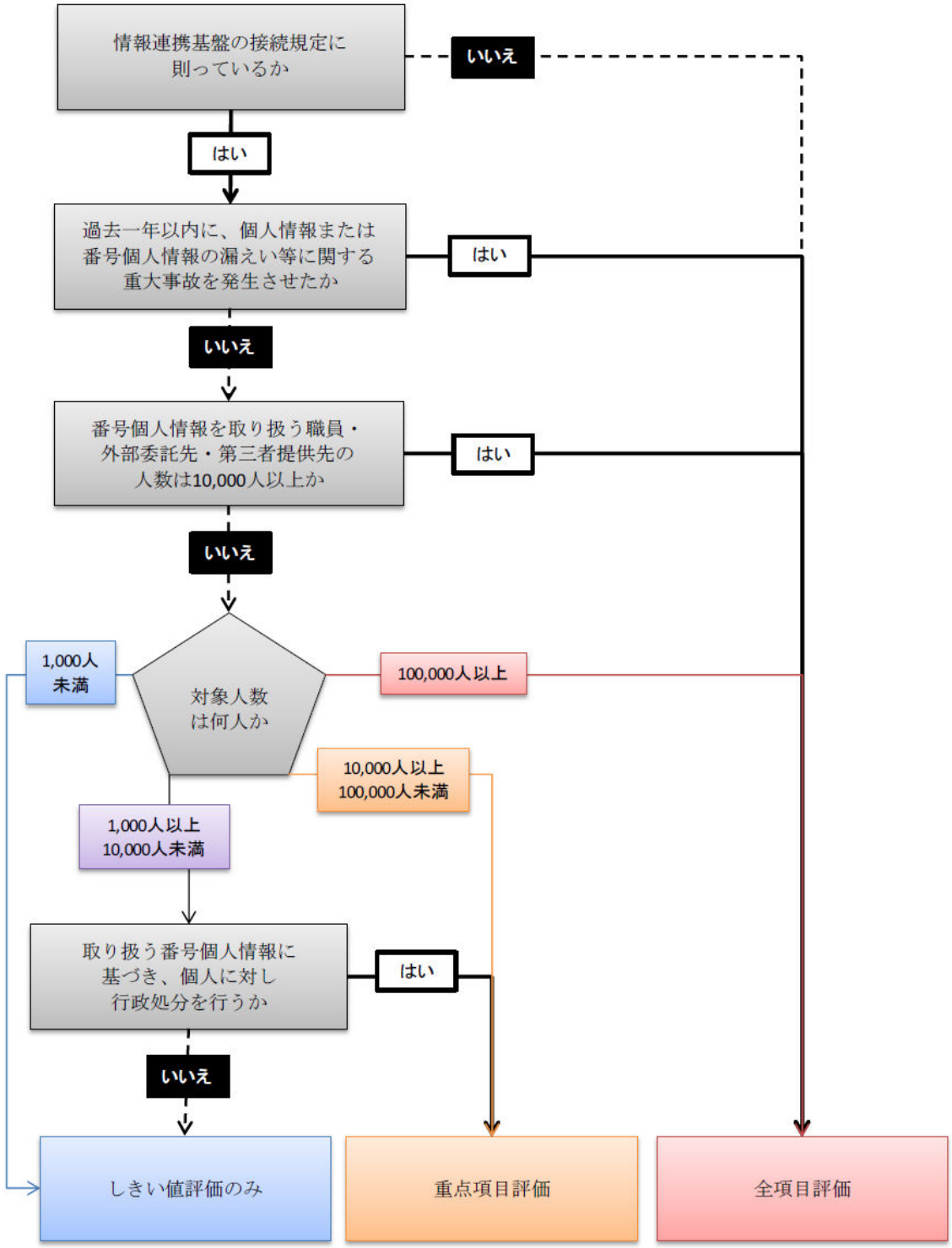


図 5　しきい値評価による振り分けのフロー図[15]

○重点項目評価

重点項目評価は、情報保護評価の必要性が特に高いとまではいえないものについて、全

15 出典：情報保護評価 SWG 資料。

項目評価よりも簡潔に評価を行うものである。

情報保有機関は、事実報告書をもとに、「情報保護評価（しきい値評価）事実報告書記載事項」に示された判断基準に従い、当該「番号」に係る個人情報ファイルが重点項目評価を実施すべきものと認められる場合には、「情報保護評価（重点項目評価）報告書記載事項」に従い重点項目評価を実施し、重点項目評価報告書を作成しなければならない。

情報保有機関の裁量により、重点項目評価報告書について広く国民の意見を求めた上で、それにより得られた意見を元に重点項目評価報告書に必要な見直しを行うプロセスを設けることも可能である。

情報保有機関は重点項目評価報告書を第三者機関に対し提出しなければならない。第三者機関は、重点項目評価報告書のうちいくつかを抽出して点検するものとする。

情報保有機関は、重点項目評価報告書を第三者機関に対し提出した後、当該報告書を速やかに公表しなければならない。

情報保有機関は、重点項目評価を実施することで、「番号」に係る個人情報ファイルの保有が、その事務を遂行する上で必要なのか、「番号」に係る個人情報ファイルを取扱うことでプライバシー等に対しどのような影響を与えるのかを検討することとなり、かかるプロセスを通じて、情報保有機関は、プライバシー等に対する影響を緩和・軽減するためにどうのような措置を講じるのか決定していくこととなる。

○全項目評価

全項目評価は、情報保護評価の必要性が特に高いものについて行う評価であり、詳細かつ慎重な分析・検討が求められる。

情報保有機関は、事実報告書をもとに、「情報保護評価（しきい値評価）事実報告書記載事項」に示された判断基準に従い、当該「番号」に係る個人情報ファイルが全項目評価を実施すべきものと認められる場合には、「情報保護評価（全項目評価）報告書記載事項」に従い全項目評価を実施し、全項目評価報告書を作成しなければならない。

情報保有機関は、全項目評価報告書を作成した後、全項目評価報告書について広く国民の意見を求めなければならず、これにより得られた意見を考慮して全項目評価報告書に必要な見直しを行わなければならない。

情報保有機関は、全項目評価報告書について、第三者機関による審査及び承認を受けなければならない。情報保有機関は、第三者機関の承認を受けた後、速やかに全項目評価報告書を公開しなければならない。

情報保有機関は、全項目評価を実施することで、「番号」に係る個人情報ファイルの保有が、その事務を遂行する上で必要なのか、「番号」に係る個人情報ファイルを取扱うことでプライバシー等に対しどのような影響を与えるのかを検討することとなり、かかるプロセスを通じて、情報保有機関は、プライバシー等に対する影響を緩和・軽減するためにどうのような措置を講じるのか決定していくこととなる。また、よりプライバシー等法的に保

護される権利利益の侵害性の低い方法を採用できないか否かを具体的に検討するため、プライバシー等保護のためのきめ細かい分析・評価を行うことが出来る。

専門性・中立性を有する第三者機関が全件審査することで、情報保有機関以外の第三者の視点から、専門的・中立的・客観的な評価を加えることができ、情報保有機関の行った全項目評価の妥当性を確認することができる。

○事実報告書、重点項目評価報告書及び全項目評価報告書の公表

作成した報告書及びその添付資料は、原則としてすべて公表しなければならない。

ただし、報告書及びその添付資料をすべて公表することで情報セキュリティ上のリスクとなりうる場合や安全保障上のリスクとなりうる場合も考えられ、かかる懸念を有する情報保有機関が第三者機関に対しても不十分な情報しか提供しないことも考えられることから、一定の場合には、第三者機関へは報告書及びその添付資料のすべてを提出した上で、国民に対してはその一部又は全部を要約して公表することができるものとする。

○情報保護評価の全体フロー

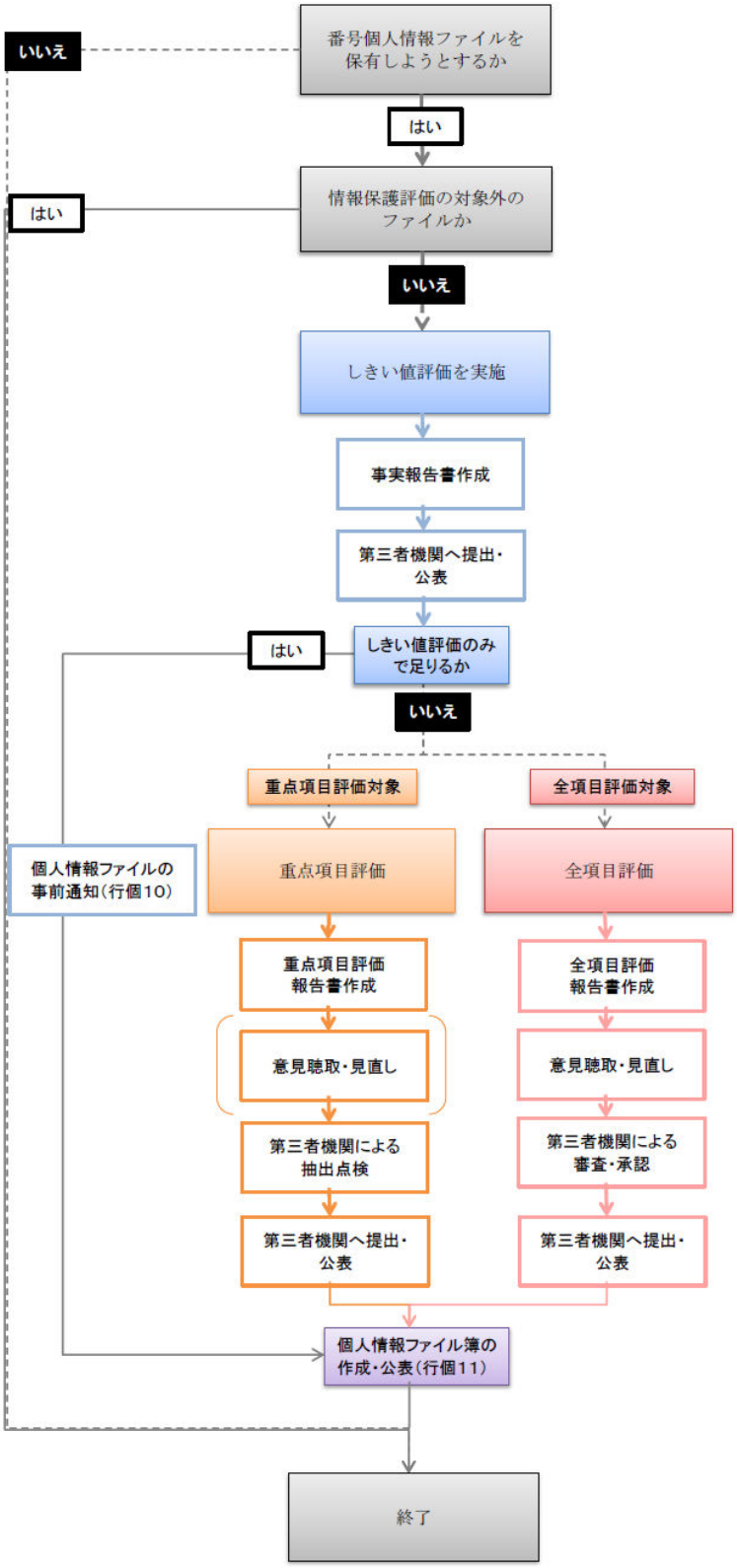


図 6　情報保護評価の全体フロー[16]

16 出典：情報保護評価 SWG 資料。

○個人情報ファイル保有時点における情報保護評価報告書の確認

情報保護評価は、「番号」に係る個人情報の取扱いが、プライバシー等に対し特段の影響を及ぼさないことを保証するためのものであるが、情報保護評価報告書に記載された措置が実際に講じられない場合は、そのようなことが保証されないこととなる。

また情報保護評価は、情報保有機関が国民のプライバシー等の保護にどのように取り組んでいるかについて宣言し、国民の信頼を獲得することを目的としているが、情報保護評価報告書に記載された措置が実際に講じられない場合は、情報保護評価の宣言が偽りのものとなってしまう。

そのため、情報保有機関は、「番号」に係る個人情報ファイルを保有する時点において、当該「番号」に係る個人情報ファイルの取扱いが情報保護評価報告書の記載通りであることを自ら確認しなければならない。

情報保護評価報告書の完成後に、システムの仕様変更等が行われ、情報保護評価報告書の記載事項と実態が異なった場合なども、情報保有機関はすみやかに情報保護評価報告書の記載事項を修正しなければならない。

仮に、情報保護評価報告書に事実と反する記載が認められる場合は、第三者機関の助言・勧告等を受けることとなる。

○情報保護評価の未完了に対する措置

情報保護評価を実施していない「番号」に係る個人情報ファイルについて、情報連携を行わせると、不適正な取扱いがなされていたり、又は個人のプライバシー等に影響を与えうる「番号」に係る個人情報ファイルがネットワークを通じてやりとりされることとなり、適正な取扱いがなされている他の「番号」に係る個人情報ファイル、他の情報提供者又は情報照会者のシステムや情報連携基盤に対し、悪影響を及ぼすおそれがある。

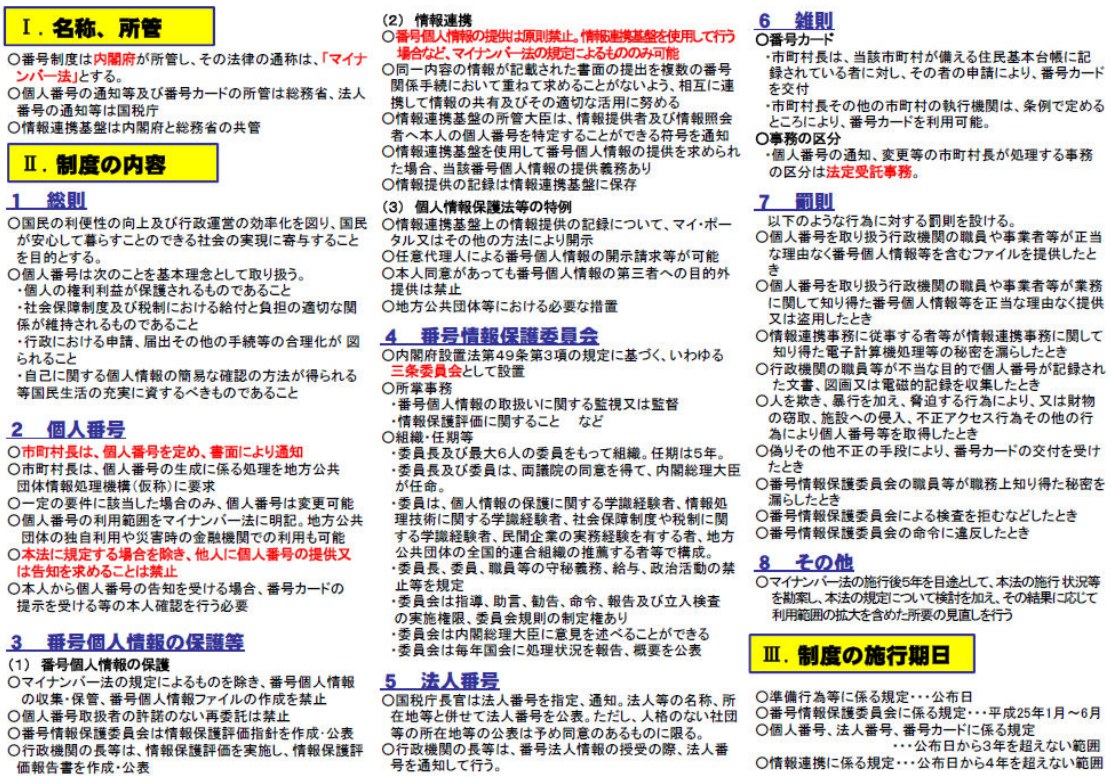
そこで、情報保護評価を実施しなければならないにもかかわらず情報保護評価を完了していないものについて、情報連携を行うことを禁止することとする。また、情報連携を行わない機関については、第三者機関の助言・勧告権限等に基づき、是正を促すものとする。

○情報保護評価報告書の虚偽記載等に対する措置

情報保護評価報告書の記載事項について、情報保有機関が意図的に虚偽記載をしたり、結果的に実態との乖離が生じていたときは、第三者機関の助言・勧告・立入検査権限等に基づき、是正を促すものとする。

（４）社会保障･税番号制度の法律事項に関する概要（案）

社会保障・税に関わる番号制度に関する実務検討会は、2011 年 12 月 16 日に「社会保障・税番号制度の法律事項に関する概要（案）」[17]を公表した。同概要（案）の「Ⅱ．制度の概要　３．番号個人情報の保護等」では、「番号情報保護委員会は、情報保護評価のための情報保護評価指針を作成し、公表する。」「番号情報保護委員会は、技術進歩や国際動向を踏まえ、少なくとも３年ごとに指針を再検討し、必要が認められれば変更する。」「行政機関の長、地方公共団体の長等は、番号個人情報ファイルの取扱いが個人の権利利益に及ぼす影響を評価するために情報保護評価を実施し、情報保護評価報告書を作成した上で公表する」、また、「４．番号情報保護委員会」では、その所掌事務として「番号個人情報の取扱いに関する監視又は監督に関すること」「情報保護評価に関すること」「番号個人情報の保護についての広報及び啓発に関すること」「その他法律により番号情報保護委員会に属せられた事務」が挙げられている。これらは、社会保障・税番号大綱で示された方針を踏襲するものである。



Ⅰ．名称、所管

○番号制度は内閣府が所管し、その法律の通称は、「マイナンバー法」とする。
○個人番号の通知等及び番号カードの所管は総務省、法人番号の通知等は国税庁
○情報連携基盤は内閣府と総務省の共管

Ⅱ．制度の内容

1　総則

○国民の利便性の向上及び行政運営の効率化を図り、国民が安心して暮らすことのできる社会の実現に寄与することを目的とする。
○個人番号は次のことを基本理念として取り扱う。
・個人の権利利益が保護されるものであること
・社会保障制度及び税制における給付と負担の適切な関係が維持されるものであること
・行政における申請、届出その他の手続等の合理化が 図られること
・自己に関する個人情報の簡易な確認の方法が得られる等国民生活の充実に資するべきものであること

2　個人番号

○市町村長は、個人番号を定め、書面により通知
○市町村長は、個人番号の生成に係る処理を地方公共団体情報処理機構（仮称）に要求
○一定の要件に該当した場合のみ、個人番号は変更可能
○個人番号の利用範囲をマイナンバー法に明記。地方公共団体の独自利用や災害時の金融機関での利用も可能
○本法に規定する場合を除き、他人に個人番号の提供又は告知を求めることは禁止
○本人から個人番号の告知を受ける場合、番号カードの提示を受ける等の本人確認を行う必要

3　番号個人情報の保護等

(1) 番号個人情報の保護
○マイナンバー法の規定によるものを除き、番号個人情報の収集・保管、番号個人情報ファイルの作成を禁止
○個人番号取扱者の許諾のない再委託は禁止
○番号情報保護委員会は情報保護評価指針を作成･公表
○行政機関の長等は、情報保護評価を実施し、情報保護評価報告書を作成･公表

(2) 情報連携
○番号個人情報の提供は原則禁止。情報連携基盤を使用して行う場合など、マイナンバー法の規定によるもののみ可能
○同一内容の情報が記載された書面の提出を複数の番号関係手続において重ねて求めることがないよう、相互に連携して情報の共有及びその適切な活用に努める
○情報連携基盤の所管大臣は、情報提供者及び情報照会者へ本人の個人番号を特定することができる符号を通知
○情報連携基盤を使用して番号個人情報の提供を求められた場合、当該番号個人情報の提供義務あり
○情報提供の記録は情報連携基盤に保存

(3) 個人情報保護法等の特例
○情報連携基盤上の情報提供の記録について、マイ･ポータル又はその他の方法により開示
○任意代理人による番号個人情報の開示請求等が可能
○本人同意があっても番号個人情報の第三者への目的外提供は禁止
○地方公共団体等における必要な措置

4　番号情報保護委員会

○内閣府設置法第49条第3項の規定に基づく、いわゆる三条委員会として設置
○所掌事務
・番号個人情報の取扱いに関する監視又は監督
・情報保護評価に関すること　など
○組織･任期等
・委員長及び最大6人の委員をもって組織。任期は5年。
・委員長及び委員は、両議院の同意を得て、内閣総理大臣が任命。
・委員は、個人情報の保護に関する学識経験者、情報処理技術に関する学識経験者、社会保障制度や税制に関する学識経験者、民間企業の実務経験を有する者、地方公共団体の全国的連合組織の推薦する者等で構成。
・委員長、委員、職員等の守秘義務、給与、政治活動の禁止等を規定
・委員会は指導、助言、勧告、命令、報告及び立入検査の実施権限、委員会規則の制定権あり
・委員会は内閣総理大臣に意見を述べることができる
・委員会は毎年国会に処理状況を報告、概要を公表

5　法人番号

○国税庁長官は法人番号を指定、通知。法人等の名称、所在地等と併せて法人番号を公表。ただし、人格のない社団等の所在地等の公表は予め同意のあるものに限る。
○行政機関の長等は、番号法人情報の授受の際、法人番号を通知して行う。

6　雑則

○番号カード
・市町村長は、当該市町村が備える住民基本台帳に記録されている者に対し、その者の申請により、番号カードを交付
・市町村長その他の市町村の執行機関は、条例で定めるところにより、番号カードを利用可能。
○事務の区分
・個人番号の通知、変更等の市町村長が処理する事務の区分は法定受託事務。

7　罰則

以下のような行為に対する罰則を設ける。
○個人番号を取り扱う行政機関の職員や事業者等が正当な理由なく番号個人情報等を含むファイルを提供したとき
○個人番号を取り扱う行政機関の職員や事業者等が業務に関して知り得た番号個人情報等を正当な理由なく提供又は盗用したとき
○情報連携事務に従事する者等が情報連携事務に関して知り得た電子計算機処理等の秘密を漏らしたとき
○行政機関の職員等が不当な目的で個人番号が記録された文書、図画又は電磁的記録を収集したとき
○人を欺き、暴行を加え、脅迫する行為により、又は財物の窃取、施設への侵入、不正アクセス行為その他の行為により個人番号等を取得したとき
○偽りその他不正の手段により、番号カードの交付を受けたとき
○番号情報保護委員会の職員等が職務上知り得た秘密を漏らしたとき
○番号情報保護委員会による検査を拒むなどしたとき
○番号情報保護委員会の命令に違反したとき

8　その他

○マイナンバー法の施行後5年を目途として、本法の施行状況等を勘案し、本法の規定について検討を加え、その結果に応じて利用範囲の拡大を含めた所要の見直しを行う

Ⅲ．制度の施行期日

○準備行為等に係る規定･･･公布日
○番号情報保護委員会に係る規定･･･平成25年1月～6月
○個人番号、法人番号、番号カードに係る規定
･･･公布日から3年を超えない範囲
○情報連携に係る規定･･･公布日から4年を超えない範囲

図 7　社会保障・税番号制度の法律事項に関する概要（案）の要点[18]

---

17 http://www.cas.go.jp/jp/seisaku/bangoseido/dai14/siryou2.pdf
18 出典：社会保障・税に関わる番号制度に関する実務検討会資料

（５）行政手続における特定の個人を識別するための番号の利用等に関する法律案（マイナンバー法案）

内閣官房社会保障改革担当室が作成した「行政手続における特定の個人を識別するための番号の利用等に関する法律案」[19]（以下、「マイナンバー法案」という）及び関係法律の整備法案は、2012 年 2 月 15 日に閣議決定され、同日、国会に提出された。

マイナンバー法案では、情報保護評価について第 14 条及び第 15 条で規定されている。なお、用語上、情報保護評価は「特定個人情報保護評価」という表現に改められている[20]。

第 14 条では、個人番号情報保護委員会が特定個人情報保護評価に関する指針を作成し、公表すること、また 3 年ごとに指針について再検討することが規定されている。

第 15 条では、第 1 項において、行政機関の長等[21]は「特定個人情報ファイル[22]」を保有しようとするとき、又は特定個人情報ファイルに重要な変更を加えようとするときは、事前に、個人番号情報保護委員会規則に定める事項を評価した結果を記載した評価書を公示し、広く国民の意見を求めなければならないと規定されている。また、同条第 2 項において、行政機関の長等は、国民からの意見を十分に考慮した上で評価書に必要な見直しを行った後に、個人番号情報保護委員会の承認を受けなければならないと規定されている。さらに、同条第 4 項において、行政機関の長等は、評価書について委員会の承認を受けたときは、速やかに当該評価書を公表しなければならないと規定されている。

マイナンバー法案のこれらの規定は、社会保障・税番号大綱で示された方針を踏襲するものである。

---

19 http://www.cas.go.jp/jp/houan/120214number/houan_riyu.pdf

20 「社会保障･税番号制度の法律事項に関する概要（案）」で第三者機関は「番号情報保護委員会」という名称で呼ばれていたが、これもマイナンバー法では「個人番号情報保護委員会」という表現に改められた。

21 行政機関の長、地方公共団体の機関、独立行政法人等、地方独立行政法人及び地方公共団体情報システム機構、並びに情報提供ネットワークシステム（社会保障・税番号大綱では情報連携基盤と呼ばれていたシステム）を利用する情報照会者及び情報提供者を指す。

22 情報保護評価ガイドライン案にいう「「番号」に係る個人情報ファイル」に該当する。

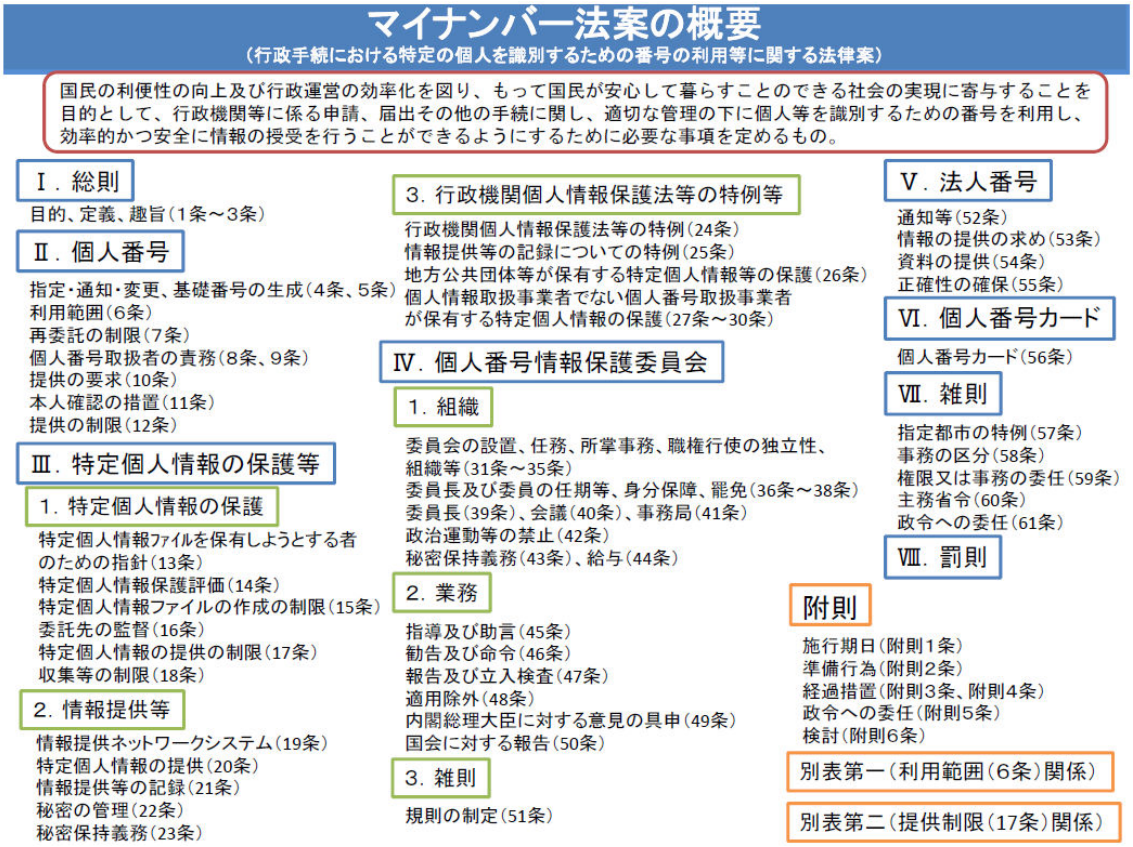


図 8　マイナンバー法案の概要[23]

[23] 出典：内閣官房資料

１．３　欧州における状況

１．３．１　EU データ保護指令における PIA 類似の制度：事前評価

1995 年に採択された「EU データ保護指令」（正式名称は、「個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する 1995 年 10 月 24 日の欧州議会及び理事会の 95／46／EC 指令」）は、EU 加盟国及び EEA（欧州経済領域）加盟国合計 30 ヶ国に対して同指令に基づく国内法規を要求するものであり、また、EU 域外の国に対してもデータ移転に当たって「十分なレベル」の個人データ保護を要請するものであるため、個人情報保護の分野では極めて影響力の強いフレームワークである。我が国の個人情報保護法及びプライバシーマーク制度も、EU データ保護指令の影響を受けて制定されている。

この EU データ保護指令第 20 条において、「Prior checking」（事前評価）が規定されている。この事前評価の制度は、PIA そのものではないが類似した制度である。

EU 指令[24]上の条項であるので、EU 加盟国（及び EEA 加盟国）[25]は自国の国内法に反映させる必要があるが、国内法への反映状況等は国により様々である。EU 加盟国及び EEA 加盟国合計 30 カ国中、少なくとも 16 カ国で条文化されている[26]。

- オーストリア（個人データ保護法第 18 条）
- フランス（情報処理・データと自由に関する法律第 25 条）
- ドイツ（データ保護法第 4d 条）（後述）　など

EU データ保護指令第 20 条の条文訳（弊社訳）は図 9 の通りである。

---

[24] EU の規制については、規則、指令、決定、勧告、見解の 5 種類がある。左ほど強制力が強い。指令（Directive）は、含まれている目的が国内法に置き換えられたときにのみ各国に効力を持つ。また、国内法への置き換えに際し、加盟国にはある一定の裁量権が与えられている。また指令は、定められた期間内に国内法に置き換えられなければならないということも決められている。（「EU（欧州連合）の主な法体系について」『制電 Vol.32―6 October 2006』http://www.neca.or.jp/control/green/PDF/kank0610.pdf を参考にした。）

[25] 2011 年 9 月現在、EU 加盟国はベルギー、ドイツ、フランス、イタリア、ルクセンブルク、オランダ、デンマーク、英国、アイルランド、ギリシャ、スペイン、ポルトガル、オーストリア、フィンランド、スウェーデン、キプロス、チェコ、エストニア、ハンガリー、ラトビア、リトアニア、マルタ、ポーランド、スロバキア、スロベニア、ブルガリア、ルーマニアの計 27 カ国。また 2011 年 5 月現在、EU 加盟国以外の EEA 加盟国はアイスランド、リヒテンシュタイン、ノルウェーの 3 カ国。これらの合計 30 カ国が EU 指令の対象となる。

[26] Loughborough University, 'APPENDIX H: Broad Jurisdictional Report for the European Union', "Privacy Impact Assessments: International Study of their Application and Effects",（2007 年 10 月）（http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/lbrouni_piastudy_apph_eur_2910071.pdf）。

EU データ保護指令第 20 条　事前評価（Prior checking）

1. EU 加盟各国は、データ主体の権利や自由に対して明示的なリスクを提示するおそれのあるデータ処理を特定し、これらのデータ処理がその開始に先立って吟味されるように評価を行うものとする。

2. このような事前評価は、データ管理者からの通知の受領の後に監督機関によって、もしくはデータ保護職員によって実施されるものとする。データ保護職員は、疑義が有る場合には監督機関に相談しなければならない。

3.（略）

図 9　EU データ保護指令第 20 条 事前評価

１．３．２　EU データ保護指令改定案

（１）改定の背景

上記の EU データ保護指令については、今般 2 年以上の検討及びコンサルテーション期間を経て改正され、新たに EU データ保護規則（Regulation）（「個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の規則」）として採択される見込みである。

従来の EU データ保護指令は、それを元に各加盟国が国内法を整備する仕組みであったが、「規則（Regulation）」は直接、EU 各加盟国の官民部門に適用される。今まで各国の国内法が微妙に異なり、多国籍企業が各国のデータ保護法を遵守しなければいけなかったが、新規則によって EU 域内では一本化されることとなる。

今回の改正は、従来の指令の採択から 15 年以上が経ち、インターネットを初めとする急速な技術的進歩やグローバル化の進展によって発生してきた新たな課題に対処するためのものである。具体的には、クラウドコンピューティング（EU 域外へのアウトソーシング）やソーシャルネットワーキングサービスにおけるデータ保護のあり方、多国籍企業のビジネスに過度な負担をかけるような非効率・非整合的な規制の改善等が課題となっていた。

欧州委員会では、従来の指令について 2009 年 5 月から見直しを始め、2 回のパブリックコンサルテーションの実施（2009 年 7 月～12 月、2010 年 11 月～2011 年 1 月）、また改正による影響評価（impact assessment）の実施も経て、2012 年 1 月 25 日に改正案が公表された。欧州委員会は今後、欧州議会及び欧州連合理事会と緊密に協力し、2012 年内の合意を目指している。採択から 2 年後に発効の見込みである。

（２）EU データ保護指令改定案における「データ保護影響評価」

EU データ保護指令改定案（EU データ保護規則案）では、管理者（個人情報を取扱う公共機関や事業者等）の義務がいくつか追加されているが、そのうちの 1 つとして、データ保護影響評価の実施義務が追加された。

すなわち、改定案の「第 33 条　データ保護影響評価」において、プライバシーリスクが高い個人データ処理（人事評価情報、信用情報、位置情報、医療健康情報、遺伝子情報、生体情報、監視カメラ情報等を取扱う場合）について、データ保護影響評価（プライバシー影響評価に該当）の実施義務が規定されている。

EU データ保護規則案　第 33 条　データ保護影響評価

1.予定されている処理活動がその性質、範囲又は目的に基づきデータ主体の権利と自由に明示的なリスクを提示する場合には、管理者又は管理者を代理する処理者は、当該処理活動が個人データ保護に与える影響について評価を実施するものとする。

2.とりわけ以下の処理活動は、本条第 1 項で規定したような明示的リスクを提示する。

(a)自動処理に基づき、かつ当該個人に関する法的影響を生じさせる措置を引き起こす若しくは当該個人に重大な影響を与えるような、自然人に関する個人的側面の体系的かつ広範な評価、又は、とりわけ自然人の経済状況、位置、健康、個人的嗜好、信頼性若しくは行動を分析若しくは予測するための処理活動。

(b)性生活、健康、人種、及び民族的起源に関する情報、又はヘルスケアの提供、疫学研究、若しくは精神疾患若しくは伝染病に関する調査のための処理活動であって、当該データが大きな規模で特定の個人に対する措置又は決定を行うために処理される場合。

(c)公共のアクセス可能なエリアのモニタリング、とりわけ、光学電子機器を利用している場合（ビデオ・サーベイランス）。

(d)子ども、遺伝子データ、又は生体データに関する大規模なファイリングシステムにおける個人データ。又は、

(e)第 34 条(2)(b)に従い監督機関のコンサルテーションが必要とされる、その他の処理活動。

3.影響評価は、データ主体及びその他の関係する者の権利と正当な利益を考慮に入れながら、少なくとも、予定されている処理活動の全般的記述、データ主体の権利と自由へのリスクの評価、リスクに対処するために予定されている対策、安全管理措置（safeguards, security measures）、個人データ保護を保証するためのメカニズム、本規則への遵守を証明するためのメカニズムを含むものとする。

4.管理者は、商業的若しくは公共的利益の保護、又は当該処理活動のセキュリティに影響を与えることなく、意図された処理に関して、データ主体や代表者の見解を求めるものとする。

5.管理者が公的機関又は公的団体であって、かつ当該処理が処理活動に係るルールと手続きを規定した第 6 条(1)(c)に従った法的義務及び EU の法令で規定された法的義務に起因するものである場合、加盟国が当該処理活動に先立つ影響評価の実施を必要とみなさない限り、第 1 項から第 4 項は適用されないものとする。

6.欧州委員会は、本条第 1 項と第 2 項で規定された明示的なリスクを提示すると考えられる

処理活動に関して、より詳細な基準と条件を規定するために、また第 3 項で規定された影響評価に関して、スケーラビリティ（拡張性）、検証及び監査可能性の条件を含め、より詳細な要件を規定するために、第 86 条に則り委任された法令を採択する権限を与えられるものとする。そのことによって、欧州委員会は中小企業のための特別措置を考慮するものとする。

7.欧州委員会は、第 3 項で規定された影響評価を実施し、検証し、監査するための基準と手続を規定することができる。これらの実施法令は、第 87 条(2)で規定された審査手続に則り採択されるものとする。

２．米国の状況

２．１　米国の PIA 制度概要

２．１．１　背景と経緯

（１）米国における PIA 導入の背景と経緯

米国における PIA の根拠法令としては、「2002 年電子政府法」[27]の第 208 条 b 項において連邦行政機関に対する PIA の実施義務を規定している。

電子政府法第 208 条（プライバシー規定）は、「1974 年プライバシー法」[28]（連邦行政機関を対象）の古い規定だけでは情報時代における技術進歩に対応できないため、プライバシー法を補完するために策定されたものである。第 208 条では、連邦行政機関における PIA の実施義務及びウェブサイト上でのプライバシーポリシーの告知義務が規定されている。

第 208 条の規定に則り、2003 年 9 月に OMB（行政管理予算局）が PIA に関する内容を含むガイダンス 「OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002（OMB ガイダンス）」[29]を発行している。

電子政府法第 208 条プライバシー規定[30]

(a) 目的

この条は、市民中心の電子政府を推進する行政機関が、個人情報のプライバシー保護を十分に確保することを目的とする。

(b) プライバシー影響評価

(1) 行政機関の責務

A 一般規定

行政機関は、次のことを行うに先立ち、B で定める措置を講じなければならない。

（ｉ）識別可能な形態で情報を収集し、維持し、又は配信するために情報技術を開発し、又は調達すること。

（ⅱ）次の情報収集に新規に着手すること。

（Ⅰ）情報技術を使用して収集、維持、又は配信を行うもの

（Ⅱ）連邦政府の行政機関、外郭機関（instrumentality）又は職員に該当しない、10 人若しくはそれ以上の者に同一の質問を行ない、又は同一の報告要件を課した場合において、物理的に、又はオンラインで特定の個人との連絡を可能とす

---

27 http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

28 合衆国法典第 5 編第 552a 条に該当する。
http://www.law.cornell.edu/uscode/usc_sec_05_00000552---a000-.html

29 http://www.whitehouse.gov/omb/memoranda_m03-22/

30 電子政府法第 208 条の日本語訳については、平野美惠子訳「2002 年電子政府法（公法律第 107－347 号）」（平野美惠子「米国の電子政府法」『外国の立法 217』（2003 年 8 月））（http://www.ndl.go.jp/jp/data/publication/legis/217/21701.pdf）、p31～32 より引用した。

る識別可能な形態の情報が含まれるもの

B 行政機関の活動

各行政機関は、A に基づき要求される範囲で次のことを行わなければならない。

(ⅰ) プライバシー影響評価の実施

(ⅱ) 行政機関の長が決定したときは、最高情報責任者又は同等の上級職員によるプライバシー影響評価の再審査の確保

(ⅲ)(ⅱ)に基づく再審査の終了後、実行可能な場合は、当該機関のウェブサイト上への掲載、連邦官報に掲載又はその他の方法によりプライバシー影響評価を公表すること。

C 機密扱いの情報

セキュリティ上の理由から、又は評価のなかに機密情報、機密扱いの情報若しくは個人情報が含まれているときは、それを保護するために、B□ⅲについては、これを修正し、又は実施しないことができる。

D 長官に対する写しの提供

行政機関は、資金の拠出を要求した各システムに関するプライバシー影響評価の写しを長官に提供しなければならない。

(2) プライバシー影響評価の内容

A 一般規定

長官は、プライバシー影響評価に必要な内容を明記したガイダンスを行政機関に発表しなければならない。

B ガイダンス

(ⅰ) ガイダンスは、プライバシー影響評価の対象となる情報システムの規模、当該システム内に識別可能な形態で存在する情報のセンシティビティ及びその情報を不正に開示したことから生じる被害のリスクに見合うものでなければならない。

(ⅱ) ガイダンスは、プライバシー影響評価が次のことに取り組むことを要求しなければならない。

(Ⅰ) どのような情報を収集するのか。

(Ⅱ) 何故その情報を収集するのか。

(Ⅲ) 行政機関による情報の使用目的

(Ⅳ) 情報共有を行う相手

(Ⅴ) 収集の対象となる情報及び情報共有の方法に関し、本人の同意を得るためにどのような告知又は機会が用意されているか。

(Ⅵ) 情報の安全性はどのように保たれるか。

(Ⅶ) 記録システムは合衆国法典第５編第 552a 条(一般に「プライバシー法」として引用される。)に基づき開発されているか。

(3) 長官の責任

A 長官は、諸機関のためにプライバシー影響評価の実施に関する政策及び指針を策定しなければならない。

B 長官は、連邦政府全体のプライバシー影響評価の実施の進捗を監視しなければならない。

C 長官が適当と判断したときは、識別可能な形態の情報が存在する既存の情報システム又は継続中の情報の収集に関しても、長官は、諸機関にプライバシー影響評価の実施を要請しなければならない。

(c) 行政機関のウェブサイト上のプライバシー保護　（略）

(d) 定義　（略）

（２）国土安全保障省における経緯

国土安全保障省（Department of Homeland Security: DHS）については、「2002 年国土安全保障省設立法」[31]第 222 条（プライバシーオフィサー）において、長官が任命した CPO（チーフプライバシーオフィサー）が PIA の実施に責任を負うことを規定している。同法に基づき、DHS のプライバシーオフィスが設立された[32]。

DHS プライバシーオフィスは、2004 年、2006 年、2007 年に PIA に関するガイダンスを発行している。2008 年 12 月には、DHS のチーフ・プライバシー・オフィサー（CPO）が「プライバシーポリシーガイダンス覚書」[33]を発行した。同覚書では、どのような場合に PIA が必要か等を規定している。

2010 年 6 月には、DHS プライバシーオフィスが PIA ガイダンスの更新版「Privacy Impact Assessment: The Privacy Office Official Guidance」[34]を発行している。

２．１．２　DHS のプライバシー遵守プロセス

DHS においては、新たなプログラム・システムを導入するときや、既存のプログラム・システムに重要な変更がなされるときには、一定の「プライバシー遵守プロセス」を実施することによって、それらが法令を順守していること及びプライバシーへの適正な配慮がなされていることをチェックすることとなっている。この「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）

---

31 http://www.dhs.gov/xabout/laws/law_regulation_rule_0011.shtm

32 連邦の各省にプライバシーオフィスに相当する部局が存在し、各省における PIA 等のプライバシー保護活動を監督しているが、DHS は入出国管理や移民管理を始めとして、米国市民の個人データを取扱うプログラムやシステムが多いため、本報告書では DHS における PIA について主に記載する。

33 http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-02.pdf

34 http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf

③個人情報記録システムに関する告知（SORN）

④プライバシー法ステートメント

から成る。

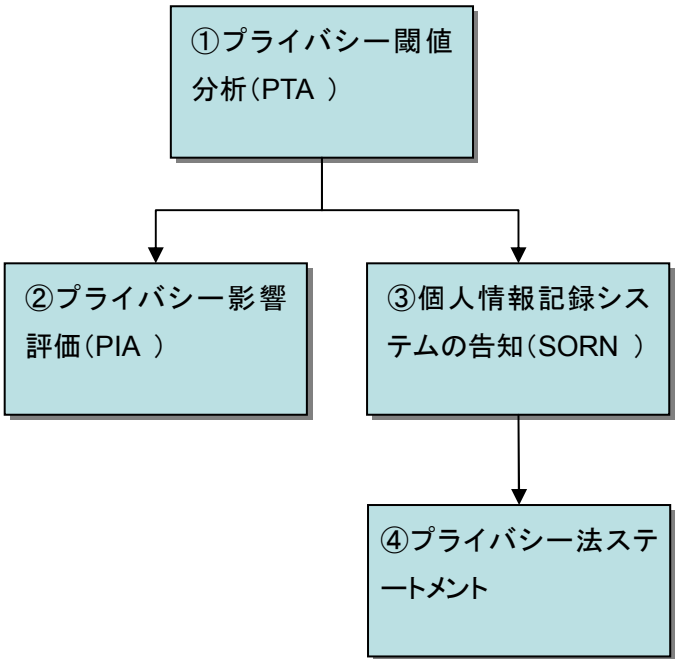


図 10　米国 DHS のプライバシー遵守プロセス

詳細は 2.2 節以下に記載するが、以下では各プロセスの概要を述べる。

①プライバシー閾値分析（PTA）

新たなプログラムやシステム等がプライバシーへの影響を有するかを判断し、さらなる PIA や SORN が必要かを決定するためのツールである。PTA は、当該プログラムやシステムに何の変更もない場合でも、3 年ごとにレビューが必要である。

②プライバシー影響評価（PIA）

事前にプログラムやシステムのプライバシーリスクを特定し、軽減するための意思決定ツールである。

PIA によって、どんな個人識別情報（PII）をどのような目的で収集し、どのように利用するか等について、一般市民に理解してもらう。また、FIPP s（公正な情報取扱い 8 原則）に則りプライバシーへの影響を評価し、それらの影響を軽減する。

③個人情報記録システムに関する告知（SORN）

連邦行政機関が保有する個人情報記録システムにおける個人情報取扱いについて、公開

する制度である。1974 年プライバシー法の e 項（４）号[35]で規定されている。

SORN は、日本の行政機関個人情報保護法における「個人情報ファイル簿」に相当する。

④プライバシー法ステートメント

個人から個人情報を収集する際に、申請書などに記載しておく個人情報取扱い方針のことである。1974 年プライバシー法の e 項（３）号[36]で規定

２．１．３　PIA における各機関の役割分担

DHS における PIA 実施に関係する範囲であるが、PIA における各機関・部局の役割分担は、以下の通りである。

○OMB（Office of Management and Budget：行政管理予算局）

・連邦行政機関における PIA 実施の監督を行う。
・連邦行政機関向けの PIA ガイダンスの作成・発行を行う。
・各機関が予算要求に関連して提出した PIA 報告書のチェックを行う。

○DHS プライバシーオフィス

・DHS 省内で実施した PIA のレビュー、助言を行う。
・CPO（チーフプライバシーオフィサー）が上記 PIA の承認を行う。
・PIA に限らない一般的な任務として、以下を行う。
　・DHS におけるプライバシー遵守の監督及び支援
　・DHS でのプライバシー・イシューに関して、DHS 長官や議会に報告

○DHS の各部門（税関・国境警備局、連邦緊急事態管理庁、移民・関税執行局等）

・新たなプログラムやシステム等に対して PIA を実施する。
・各部門（component）ごとにプライバシーオフィサーが存在。

２．２　PTA（Privacy Threshold Analysis：プライバシー閾値分析）

○概要

PTA は、新たなプログラムやシステム等がプライバシーへの影響を有するかを判断し、さらなる PIA や SORN が必要かを決定するためのツールである。DHS の「プライバシーポリシーガイダンス覚書」[37]で規定されている。

なお、PTA は DHS 独自の制度である。

---

35 合衆国法典第 5 編第 552a 条 e 項（４）号に該当する。
36 合衆国法典第 5 編第 552a 条 e 項（３）号に該当する。
37 http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-02.pdf

○PTA の実施目的

事前にプライバシーへの影響の有無を確認し、プライバシー遵守のための計画を立てること、及び DHS プライバシーオフィスの決定を記録することが、PTA の実施目的である。

○PTA の実施対象

PTA は、以下のプログラムやシステムに対して実施する。

- 新たなプログラム[38]、システム、技術、規則制定（rule-making）
- 既存のプロジェクト[39]に以下のような変更が加わるとき
  - ・新たな個人識別情報（PII：personally identifiable information）を収集するとき
  - ・PII を異なる目的で利用するとき
  - ・PII を削減するとき

なお、PTA については、プログラムやシステムに何らの変更が加わらない場合でも、3 年ごとにレビューと再認定が必要である。

○PTA の実施件数

DHS では、年間に 600～700 件程度の PTA を実施している。

○PTA の実施手順

当該プログラムやシステム等のプログラムマネジャーやシステムオーナー（以下、総称してプログラムマネジャーと言う）が、当該部門のプライバシーオフィサーと協力して PTA を作成し、DHS プライバシーオフィスに提出する。

DHS プライバシーオフィスで PTA をレビューし、さらなる PIA や SORN が必要か否かを決定する。

38 「プログラム」は、日本でいう「制度」に近い。
39 「プロジェクト」は、プログラム、システム、技術、規則制定の総称である。

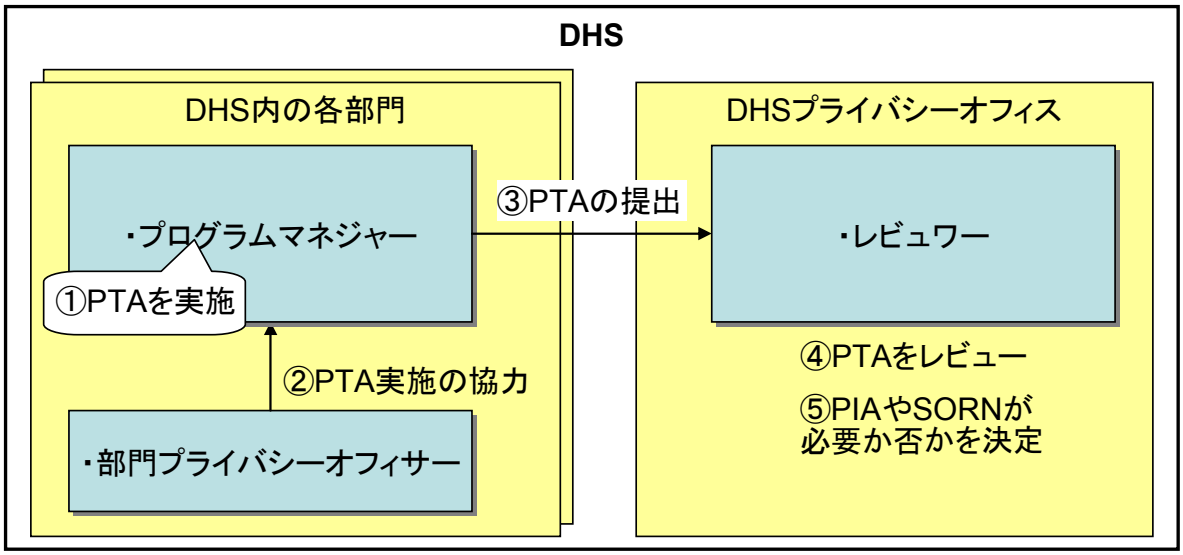


図 11　米国 DHS における PTA の実施手順

○PTA の結果、PIA が必要とされないケース

PTA を実施した結果、PIA が必要とされないと判断されるのは、以下のケースである。

・PTA において PII（個人識別情報）が特定されなかった場合

・2002 年（電子政府法制定）以降に何の変更もない既存システムの場合

・DHS 職員の情報のみを取扱うシステムの場合

○PTA の記載内容（DHS プライバシーオフィス作成の「PTA テンプレート」[40]より）

- プロジェクトの概要（プログラムマネジャーが作成）
- 詳細質問（プログラムマネジャーが作成）
  1．プロジェクトとその目的の記述
  2．プロジェクトのステータス（新規／既存）
  3．取扱われる個人情報の情報主体（職員／委託先職員／一般市民）
  4．社会保障番号（SSN）の利用・収集とその理由
  5．取扱われる個人情報の種類（氏名、住所、メルアド等）
  6．プロジェクトが技術／システムの場合、それがインフラのみに関わるものであるか（通信ログでどんなデータを記録しているか）
  7．システムは個人識別情報を DHS の他のシステムと授受等しているか
  8．FISMA 追跡システム内に、認証と認定（C&A：FISMA で規定された 1 プロセス）の記録があるか。
- プライバシー閾値レビュー（DHS プライバシーオフィスのレビュワーが作成）

[40] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pta_template.pdf

- 「プライバシーセンシティブなシステムではない（PII を含まない）」
- 「プライバシーセンシティブなシステムである」
  - システムのカテゴリー
    - 「IT システム／国土安全保障システム／レガシーシステム／人事システム／規則／その他」
  - 決定内容
    - 「PTA で十分／検討中／PIA は不要／PIA が必要／SORN は不要／SORN が必要」

２．３　PIA（プライバシー影響評価）

（１）概要

PIA は、事前に新たなプログラムやシステム等のプライバシーリスクを特定し、軽減するための意思決定ツールである。上述のように、2002 年電子政府法の第 208 条で連邦行政機関は PIA を実施することが義務付けられている。

連邦行政機関は PIA を実施することにより、FIPPs（公正な情報取扱い 8 原則）に則ってプライバシーへの影響を評価し、それらの影響を軽減する。また、PIA 報告書を公表することで、どのような個人識別情報（PII）をどのような目的で収集し、どのように利用するか等について、一般市民に理解してもらう。

（２）PIA の基盤としての FIPPs

FIPPs（Fair Information Protection Principles：公正な情報取扱い諸原則）とは、1974 年プライバシー法を貫く 8 原則であり、以下の 8 つから成る[41]。

1974 年プライバシー法における FIPPs

①公開の原則（Openness Principle）
②個人アクセスの原則（Individual Access Principle）
③個人参加の原則（Individual Participation Principle）
④収集制限の原則（Collection Limitation Principle）
⑤利用制限の原則（Use Limitation Principle）
⑥開示制限の原則（Disclosure Limitation Principle）
⑦情報管理の原則（Information Management Principle）
⑧説明責任の原則（Accountability Principle）

このプライバシー法における FIPPs をベースに、DHS プライバシーオフィスは DHS 用

[41] http://epic.org/privacy/ppsc1977report/c13.htm

に FIPPs を再定義しており[42]、それは以下のものである。

DHS における FIPPs
①透明性（Transparency）
②個人参加（Individual Participation）
③目的明確化（Purpose Specification）
④データ最小化（Data Minimization）
⑤利用制限（Use Limitation）
⑥データ正確性と完全性（Data Quality and Integrity）
⑦セキュリティ（Security）
⑧説明責任と監査（Accountability and Auditing）

DHS プライバシーオフィスでは、DHS 各部門に対して、この FIPPs に則り PIA を実施するように指導しており、プライバシーオフィスが各部門から提出を受けた PIA 報告書をレビューする際にも、この FIPPs に基づいてレビューを行っている。

（３）PIA の実施目的

DHS の PIA ガイダンス[43]によれば、PIA を実施する目的は、プログラムマネジャーがシステムやプログラムの開発ライフサイクル全体を通じてプライバシー保護を意識的に組み込んでいることを一般市民や議会に対して保証することであり、また、開発の開始時点からプライバシー保護がシステムに組み込まれていることを保証することで、事後にコストをかけたり、当該プロジェクトの実現が危うくなることを防ぐことである。

（４）PIA の実施対象

PIA の実施対象は、前節で挙げた PTA の対象となるプログラムやシステムのうち、PTA によって PIA が必要と判断されたものであるが、DHS の「プライバシーポリシーガイダンス覚書」[44]では、別の切り口から、以下のような整理がなされている。

- PII を取扱かったり収集したりする新たなプログラムやシステムを開発や調達するとき
- PII に影響を与える予算を OMB に提出するとき
- PII に影響を与えるパイロット実験を行うとき
- PII に影響を与えるプログラムやシステム改修をするとき

---

42 http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf
43 http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf
44 http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-02.pdf

・ PII の収集・利用・維持を伴うような新たな規則制定（rule-making）や改定を行うとき

（５）PIA の実施件数

DHS では、年間に 100 件程度の PIA を実施している。

（６）PIA の実施期間

通常は PTA 開始から PIA 承認まで 3～6 ヶ月である。

ただし規則制定に対する PIA は 1 年以上かかる。規則制定プロセスに付随して PIA を実施するためである（後述）。

（７）PIA の実施手順

PTA において PIA が必要だと判断された場合、当該プログラムやシステム等のプログラムマネジャーと当該部門の CIO が、当該部門のプライバシーオフィサーやカウンセルと協力して PIA を実施、ドラフトを作成し、DHS プライバシーオフィスに提出する。その際、PIA ガイダンスと PIA テンプレート[45]を使用する。

DHS プライバシーオフィスで PIA ドラフトをレビューし、何回も部門とやり取りし、最終的に DHS の CPO が承認する。

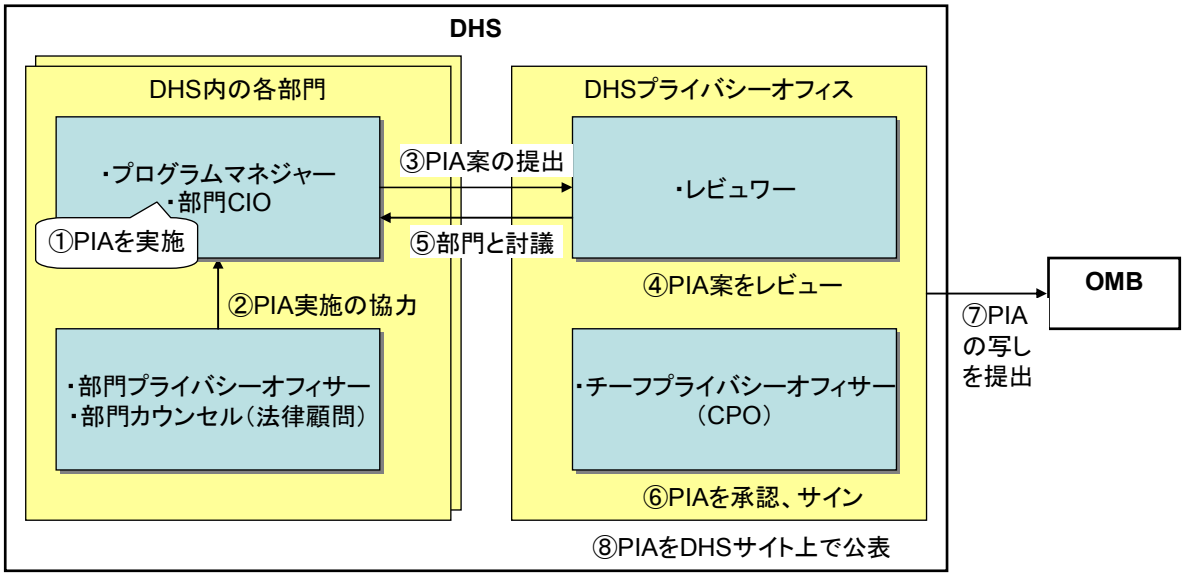


図 12　米国 DHS における PIA の実施手順

（８）PIA の提出と公表

予算要求がなされたシステムについては、 DHS の CPO による承認後、OMB に PIA 報

[45] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_template.pdf

告書の写しを提出する。

OMB が提出された PIA について不十分であると懸念する場合は、懸念に対処するために行政機関と協働し、PIA が適切なものとなるように調整を行う。これまで、OMB が DHS 提出の PIA について不承認としたことはない。

また、CPO により承認された PIA 報告書は DHS のサイトで公表する（連邦官報にも概要部分は公表される）。なお、安全上の理由、又は機密情報・センシティブ情報・プライベート情報を保護する理由から、一部を公表しなくてもよい。

（９）規則制定時のプロセス

DHS における PIA の実施対象は大きくは情報システムに関連するもの（プログラム、システム、技術）と、行政機関による規則制定（rule-making）とに分かれる。後者は国土安全保障省設立法第 222 条で付加されたもので、電子政府法第 208 条の規定にはない。

規則制定（rule-making）の例としては、例えば、ある化学施設を守るために、テロリストウォッチリストを用いて全ての従業員をスクリーニング検査するという法律が議会を通り、具体的な規則を制定する権限が DHS に付与されるケースがあった。この場合、規則制定が従業員のプライバシーに影響を与える可能性があるため、併せて PIA を実施することが必要である。

このようなケースにおける規則制定のプロセスは、以下の通りである。

① DHS の関係部門が上記の法律を施行するための規則案を連邦官報（Federal Register）に掲載する（Notice of proposed rulemaking）。

② DHS プライバシーオフィスがこの時点での PIA を公表する。
（規則案のプライバシーへの影響がどのようなものがあり、どのようにリスクを軽減したかを示す。）

③ 規則案に対するパブリックコメントが来る。

④ 修正した規則案を連邦官報に掲載する。これは、全てのコメント（プライバシー関連含む）に対応したもの。

⑤ 新たな PIA を実施し、リスクと軽減策を再評価し、それらを反映した最終的な規則を制定する。

⑥ 同規則に関する SORN を公表する。

（10）PIA 報告書

PIA 報告書は、以下の内容に関して文書化したものである。

- DHS がなぜ当該プログラムを立ち上げるのか。
- どんな PII が、誰から、何の目的で収集されるのか。
- その PII は誰と、何の目的でシェアされるのか。
- 個人にどんな通知（notice）が提供されるのか。

・ どうやって個人は自分の情報にアクセスできるのか。
・ どんな安全措置が取られているのか。
・ 技術が個人のプライバシーにどんな影響を与えるのか。
・ どんなプライバシーリスクが特定され、どんな軽減策が取られたのか。

DHS の PIA ガイダンス及び PIA テンプレートでは、PIA 報告書の構成として、以下のものを規定している。

○プログラムの概要
・ プライバシーへの影響が分かるようなコンテキストを記載する。
・ 個人情報を取扱う典型的なトランザクションを記載する。

○セクション１：法的権限とその他の要件
・ 当該プログラムやシステムが準拠する法律や規則を洗い出し、それらによって個人情報の収集や利用が許可されていることを説明する。
・ その他、データ保持期間が法律を遵守しているか等の確認を行う。

○セクション２：情報の特徴
・ 情報を収集される個人の分類と、収集・保持する情報の特定を行う。当該プログラムやシステムで収集する情報を減らせば、プライバシーの問題も少なくなる。とりわけ、SSN は ID 窃盗等で悪用される恐れがあるため、非常にセンシティブな情報である。
・ 情報の収集源の特定を行う。本人、第三者（商業ソース／公開情報）など。
・ 情報の正確性のチェック方法を記述する。
・ プライバシー影響分析として、ある種類の情報を収集する場合、どのようなプライバシーリスクがあり、どのようにリスクを軽減すべきかについて検討する。その際、FIPPs の目的明確化の原則、データ最小化の原則、個人参加の原則、データ正確性と完全性の原則を考慮する。

○セクション３：情報の利用
・ どのように情報を利用するか、利用目的は何かを記載する。
・ 情報がシェアされる省内の他部門を特定する。
・ プライバシー影響分析として、情報を目的内で適切に利用するための対策について記述する。その際、透明性の原則、利用制限の原則を考慮する。

○セクション４：通知
・ 収集に先立ち、どのように個人が通知を受けているかを記述する。
・ 個人に同意したり、拒否したり、オプトアウトする機会が与えられているかを記述する。
・ プライバシー影響分析として、通知がプロジェクト目的に合致したものであるかを

検討する。その際、透明性の原則、利用制限の原則、個人参加の原則を考慮する。

○セクション５：プロジェクトによるデータ保持

- 情報をどのくらいの期間、何の目的で保持するかを説明する。
- プライバシー影響分析として、情報を一定期間保持し続けることのリスクと、その軽減策について議論する。その際、データ最小化の原則、データ正確性と完全性の原則を考慮する。

○セクション６：情報のシェアリング

- 情報を提供する外部の機関について特定する。
- 再提供の制限について記述する。
- どのように提供の記録をとるかを記述する。
- プライバシー影響分析として、外部の機関と情報をシェアするリスクと、その軽減策について議論する。

○セクション７：訂正（救済）

- 個人が自分の情報へアクセスするための手続きについて記述する。
- 誤った情報を個人が訂正するための手続きについて記述する。
- 個人がこれらの訂正手続きをどのように認識できるかについて記述する。
- プライバシー影響分析として、プライバシー法で規定された以上の訂正手続きを提供できないか議論する。その際、個人参加の原則を考慮する。

○セクション８：監査と説明責任

- 実際の情報取扱いがPIAで謳われた内容と合致していることをどのように保証するかを記述する。
- 当該プロジェクトに携わる職員にどのようなプライバシートレーニングを提供するかを記述する。
- 職員が情報へのアクセスを得るための手続きについて記述する。

（11）DHS プライバシーオフィスにおける PIA レビューの方法

上記の PIA 報告書のセクションごとに、FIPPs の各原則に合致しているかという観点から、システマティックに評価する。

プログラムやシステムを具体的にイメージして、情報収集等が適切か等について、当該部門も交えながら、非常に長く議論する。

例えば、上記のセクション 2 については、収集する情報がなぜ必要か、何のベネフィットがあるのか、収集する情報を減らしても目的を実現できるのではないかといった観点からレビューする。

レビューの際には、プライバシーとは何かといった、そもそも論には立ち返らない。

２．４　SORN（個人情報記録システムに関する告知）

○概要

SORN（System of Records Notices：個人情報記録システムに関する告知）とは、連邦行政機関が保有する個人情報記録システムにおける個人情報取扱いについて公開する制度である。1974 年プライバシー法（合衆国法典第 5 編 552a 条）が準拠法令である。具体的には、552a 条の e 項（４）号で規定されている。

日本の行政機関個人情報保護法の「個人情報ファイル簿」に相当する。

SORN は連邦官報（Federal Register）で公表される。一般市民は、SORN で公表されて初めて、自分の情報に対するアクション（開示請求等）を取ることが可能になる。

○System of Records（個人情報記録システム）

「ある行政機関のコントロール下にある一連の記録であって、そこから個人の名前、又は識別番号、シンボル若しくは個人に割り当てられたその他の識別項目によって情報が検索されるもの」（合衆国法典第 5 編 552a 条 a 項（５）号）と定義されている。

○SORN での通知事項

SORN での通知事項は、DHS の SORN ガイダンス[46]によれば、以下の事項である。

- 収集目的
- 対象となる個人、記録される情報
- 情報のシェアリング
- 保持期間
- 自己情報の開示・訂正手続き　等

○SORN の実施手順

PTA で SORN が必要と判断された場合、当該部門はガイダンスとテンプレートを用いて SORN ドラフトを作成し、部門のプライバシーオフィサーとカウンセルに提出し、その後 DHS プライバシーオフィスに提出する。

DHS の CPO の承認を受けた後、SORN はコメントのために OMB と議会に提出され、それから連邦官報に 30 日間掲載される。この 30 日間の掲載が終わる前に当該システムやプログラムの運用を開始してはならない。

○プライバシー法の適用除外

プライバシー法において、CIA や刑法の法執行機関・部門（警察を含む）は、SORN 等の義務の適用から除外されることとなっている。

この適用除外事項には、個人への通知（SORN）のほか、開示・訂正請求への対応や、記

[46] http://www.dhs.gov/xlibrary/assets/privacy/privacy_guidance_sorn.pdf

録情報を目的達成に必要なものに限定すること等がある。

３．カナダ（連邦）の状況

３．１　カナダ（連邦）の PIA 制度概要

（１）背景と経緯

○ PIA 導入の背景と経緯

1990 年代後半、「プライバシー法」[47]（及び、民間分野の個人情報保護に関する法律）を効果的かつ体系的に遵守するための 1 つのツールとして、PIA が検討された。

2002 年のカナダ財務委員会事務局（TBS）の「Privacy Impact Assessment Policy」（PIA ポリシー）[48]において、連邦政府機関に PIA 実施が義務化された。また、TBS は PIA ポリシーの付属書類として、「PIA Guidelines: A Framework to Manage Privacy Risks」（PIA ガイドライン）を発行した。

2010 年には TBS が「Directive on Privacy Impact Assessment」（PIA 指令）[49]を策定し、同年 4 月から施行された。PIA ポリシーは PIA 指令によって失効した。PIA ポリシーは政府機関の負担が大きかった（コストや時間がかかる、外部コンサルタントの使用等）ため、効率化を図るために新たに PIA 指令を策定した。

2011 年 3 月には、カナダ連邦プライバシーコミッショナー事務局（OPC）が「Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada」（OPC ガイド）[50]を発行した。これは、PIA 指令の下で政府機関が OPC に提出する PIA の品質を向上させるためのものである。OPC ガイドでは、政府機関が「公正な情報取扱い 10 原則」（後述）に沿って PIA を実施することを推奨している。

2012 年 2 月現在、PIA 指令に対応した TBS のガイドラインは未策定である。

○PIA の目的

OPC へのインタビューによると、PIA の目的は 2 つあり、1 つは政府機関が自ら法令順守を確認するとともに、想定されるプライバシーリスクを軽減すること、もう 1 つは一般市民に対して政府機関のプログラムがプライバシーを守っていることを示すことである。

（２）連邦・州コミッショナーの所轄範囲

○連邦プライバシーコミッショナー事務局（OPC）の所轄範囲

「プライバシー法」と、「個人情報保護及び電子文書法」（PIPEDA）[51]の運用を監督する。

---

47 連邦政府機関に適用される。1982 年に制定された。
http://laws-lois.justice.gc.ca/eng/acts/P-21/index.html
48 http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450
49 http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=18308
50 http://www.priv.gc.ca/information/pub/gd_exp_201103_e.cfm
51 連邦・州の民間分野に適用される。2000 年に制定された。また、1991 年の銀行法など、

すなわち、連邦政府機関と、連邦・州の民間企業等における個人情報保護を監督している。

○州プライバシーコミッショナー事務局の所轄範囲

州のプライバシー法（州政府機関に適用）の運用を監督する。

民間分野についても、州が PIPEDA と実質的に同様な立法を行った場合には、州内の当該分野については PIPEDA の適用から除外され、州法が適用される（PIPEDA 第 26 条第 2 項）。

例えばオンタリオ州は「Personal Health Information Protection Act, 2004」を制定しているため、医療分野については民間機関にも同法が適用され、州情報プライバシーコミッショナー事務局の監督を受けることとなっている。

（３）連邦における各機関の役割分担

○TBS（Treasury Board of Canada Secretariat：カナダ財務委員会事務局）

連邦政府内でプライバシー関連法令の運用に責任を持つ機関である。指令やポリシーの策定も行い、PIA ポリシー（2002 年）や PIA 指令（2010 年）を策定している。

連邦政府機関から PIA（後述のコア PIA のみ）の提出を受けるが、コア PIA に対するコメントや承認は行っていない。

○OPC（Office of the Privacy Commissioner of Canada：連邦プライバシーコミッショナー事務局）

議会に対して責任を負うオンブズマンである。ポリシーや指令の策定において、TBS に協力している。

連邦政府機関から PIA の提出を受け、レビューする権限を持つ。連邦政府機関に PIA に関する助言や勧告を行っている。ただし、PIA の承認は行わない。

○連邦政府機関

プログラムやアクティビティに対して PIA を実施する。また、コア PIA を自らのサイト上で部分的に公表する。

３．２　PIA の実施手順

PIA の実施手順は、以下の通りである。

①対象となるプログラムやアクティビティのプログラムマネジャーが、PIA 指令の付属文書 C に沿って、コア PIA（後述）を実施する。

②プログラムマネジャーは、コア PIA に基づき、自機関のプライバシー部門と相談して、

民間の個別分野を規制する連邦法も別途、存在する。

追加的な PIA（フル PIA）が必要かを決定する[52]。

③当該政府機関内で定めた承認プロセスにしたがって、コア PIA の内部承認を行う。

④プログラムマネジャーは、コア PIA を個人情報バンク（PIB）（後述）と一緒に、TBS に提出する[53]。

⑤TBS は、PIB を登録・変更するために、コア PIA の義務的要件が満たされていること（必要な項目が含まれているかどうか）のみを確認（confirm）する。

- TBS は政府機関に対して、コメントや助言は与えない。
- コア PIA に必要項目が含まれない場合には、制度上は、当該プロジェクトの予算承認をしないことも可能である。
- 追加的文書（フル PIA）の提出は受けていない。

⑥TBS は、PIB のレビューを行い、承認し、登録する。

- PIB のレビューと承認については、委任も可能である。

⑦プログラムマネジャーは、コア PIA を OPC に提出する。

⑧OPC は、コア PIA をレビューする。

- レビューの間、政府機関に電話やメールで相談・質問をしたり、会合を開いたり、追加的な文書を求める場合がある。

⑨OPC は、政府機関に助言、コメントを含む勧告状を送付する。

- OPC は、追加的な分析（フル PIA）を要求することも可能である。
- OPC が PIA を受け取ってから勧告状を送付するまで、通常は 3 ヶ月程度かかる。

⑩プログラムマネジャーは、勧告に対する対応策及び実施スケジュールについて回答する。

- OPC の勧告状には強制力がないので、政府機関は必ずしも従わなくてもよい。
- ただし従わなかった場合には、OPC が年次報告書にその旨を掲載する。また、OPC がハイリスクなプログラムとみなして監査を行う場合もある。

⑪プログラムマネジャーは、コア PIA を部分的に公表する。

- コア PIA の「セクション１：概要」と「セクション２：リスク領域の特定とカテゴリー化」の(a)～(h)を公表する。
- 公表に当たっては、セキュリティ要件や、その他の機密性、法的要件を尊重する。

---

[52] コア PIA の結果に基づきフル PIA 実施の必要性を判断するための客観的なスクリーニング基準はない。（どのカテゴリーのリスクが何レベルであれば実施する等の基準）

[53] PIA ポリシー下では、TBS は PIA の提出を受けなかった。PIA 指令において初めて、TBS は PIA（コア PIA のみ）の提出を受けるようになった。

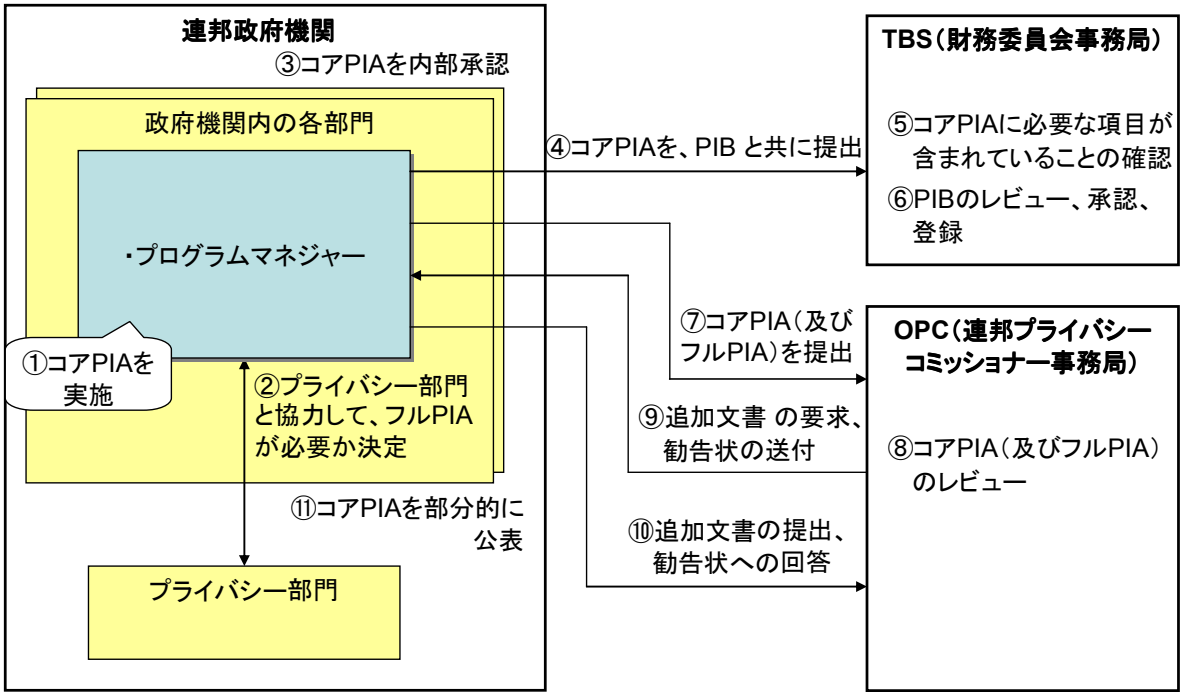


図 13　カナダ連邦政府機関における PIA の実施手順

○パブリックコンサルテーションについて

PIA ポリシーでは PIA 実施プロセスにパブリックコンサルテーションが含まれていたが、PIA 指令では効率性重視のために省かれ、市民との関係については PIA を部分的に公表するのみとなった。

○OPC が PIA の承認を行わない理由

その理由は明確ではないが、インタビューでは以下の趣旨の説明有り。

「OPC は政府機関等に対する市民からの苦情を受け付け、当該政府機関を調査し、勧告を行う権限がある。そのため、政府機関の公表した PIA に対して市民から苦情が来た場合、OPC が承認したものだと対処することが難しくなるため。」

○PIB（Personal Information Bank：個人情報バンク）

プライバシー法で、「政府機関のコントロール下にある個人情報のセットであって、個人の名前、又は識別番号、シンボル若しくはその他の個人に割り当てられた識別項目によって組織化された、又は検索が意図されたもの」と定義されている。

米国の System of records や、日本の個人情報ファイルに相当する。

プライバシー法の下では、政府機関の長は自機関の PIB を特定し、公的に報告する義務がある。また、カナダ財務委員会の長は、PIB をレビューし、承認し、登録する義務がある。

３．３　コア PIA

○コア PIA の概要

2010 年の PIA 指令において規定された制度であり、PIA ポリシー時代の「Preliminary PIA」に相当する。コア PIA において、さらなる PIA（フル PIA）が必要か否かを判断する。

○コア PIA の実施対象

新たなプログラムやアクティビティ[54]、又は重要な変更のあるプログラムやアクティビティが、コア PIA の実施対象である。

より正確には、プログラムやアクティビティが以下のような条件下にある場合、コア PIA を実施する（PIA 指令より）。

① 個人に直接に影響を与えるような意思決定プロセスにおいて、個人情報が利用されている、又は利用が意図されている場合
② 行政目的で個人情報が利用される、又は利用が意図されているような既存のプログラムやアクティビティに重要な変更がなされる場合
③ プログラムやアクティビティを政府の他のレベルや民間部門に外注又は移転し、それがプログラムやアクティビティへの重大な変更につながる場合
④ 通常は１つのプログラムに対して１つの PIA を実施するが、プログラム内の個別のアクティビティに対しても PIA が必要になる場合

○コア PIA 開始のタイミング

プログラムやアクティビティを開始する前。特に、調達時（上記③）には、入札を行う前に実施する。

ただし、多くの政府機関がこれらの開始後にコア PIA を実施している実態があるとのことである。

○コア PIA の記載内容

コア PIA の記載内容は、PIA 指令の付属文書 C で、以下のように規定されている。

・ セクション１：概要と PIA 開始

54 「プログラム」とは、各政府機関が義務として実行するものであり、日本で言う「制度」に近い。ex.学生ローン・プログラム、雇用保険プログラム等。他方、「アクティビティ」は、プログラムの実行をサポートするためにプログラム内で実施する個別の活動である。ex.学生に関する統計調査、退職者に関する統計調査等。

- セクション２：リスク領域の特定とカテゴリー化
  (a)プログラム又はアクティビティの種類（リスクレベル 1～4）
  (b)含まれる個人情報の種類とコンテキスト（リスクレベル 1～4）
  (c)プログラム又はアクティビティのパートナー、民間部門の参画（リスクレベル 1～4）
  (d)プログラムやアクティビティの期間（リスクレベル 1～3）
  (e)プログラムの規模（リスクレベル 1～4）
  (f)技術とプライバシー
  (g)個人情報の移動（リスクレベル 1～4）
  (h)プライバシー違反の際に個人や職員に影響を与える潜在的なリスク
  (i)プライバシー違反の際に機関に影響を与える潜在的なリスク
- セクション３：プログラムやアクティビティにおける個人情報要素の分析
  a.収集される個人情報の要素の特定（名前、住所等）
  b.収集される個人情報の各要素に関連したサブ要素の特定（姓、ミドルネーム、名、番地、市町村、都道府県、郵便番号等）
  c.個人情報の記録方法の特定（紙、電子、録音、画像記録、生体サンプル等）
- セクション４：プログラムやアクティビティにおける個人情報の流れ
  a.個人情報の収集源や、個人情報の作成方法の特定
  b.個人情報の利用及び提供範囲（内部及び外部）の特定
  c.個人情報が送信される場所及び保存される場所の特定
  d.個人情報にアクセスできるエリア、グループ及び個人の特定
- セクション５：プライバシー遵守分析
  a.少なくとも以下の領域をカバーし、遵守のための具体的措置を特定する
    ・収集の権限
    ・直接収集、通知、同意
    ・保持
    ・正確性
    ・利用
    ・提供
    ・運用面、物理面、技術面の安全管理措置
    ・技術とプライバシーに関するイシュー
- セクション６：分析とレコメンデーションの概要
  a.リスクの特定とカテゴリー化から導かれた結論又はレコメンデーションの記載
- セクション７：添付文書のリスト
- セクション８：公式な承認

○PIA の実施体制

OPC の意見では、コア PIA に限らず、PIA の実施体制は理想的には以下のメンバーから成るものである。

- プログラムマネジャー　１人
- 当該政府機関のプライバシー部門の担当者　１人
- IT 関係の担当者　１人
- その他、法律専門家、コミュニケーション専門家

○PIA の実施期間

プログラムに応じて、通常は 3 ヶ月～1 年間程度かかる。

ただし、OPC によれば、1 年間もかかるのは当該機関の組織に何らかの問題がある場合とのことである。

○政府機関が PIA を実施する上での課題（OPC へのインタビューより）

OPC へのインタビューによれば、政府機関が PIA を実施する上での課題は以下のものが挙げられる。

- 担当者へのプライバシー教育、意識向上
- アセスメントを適切に行えないケース
  - 各機関の中での適任者がアセスメントに関わらない場合など
- 実施のタイミングが早すぎるケース
- PIA でリスクが特定されたが、リスク軽減について機関内での協力が得られないケース
  - リスク軽減にはコストやヒューマンリソースが必要になるため
  - 特に、パワーリレーションに阻まれる場合。機関内で下位層の人が分析しても、上位層の人が許可しない場合、リスクを特定してもリスク軽減策が実行されない

３．４　OPC における PIA のレビュー

○OPC における PIA のレビュー方法

OPC が PIA 報告書を政府機関から受け取ったら、リスクの大きさに応じて優先順位を決める。OPC は、受領した全ての PIA を詳細にレビューしているわけではなく、最も重大なリスクがあると思われるイニシアティブにレビューのためのリソースを集中させている。

優先順位付けに当たっては、以下の要素に基づき、優先順位が「高い」「中程度」「低い」を決定する。

「国家安全保障」

「本人確認・本人認証」
「遺伝子情報」
「情報技術」
「公共/メディアの関心の高さ」
「議会の関心の高さ」
「影響を受ける対象者数」
「センシティブ性（医療情報、人種情報等)」
「類似の PIA/イシュー」

2010 年度に OPC が受領した PIA は 52 件、レビューした PIA は 87 件（うちリスク高としてレビューしたものは 19 件)。2009 年度は受領 PIA が 102 件、レビューPIA が 33 件であった。2010 年度は前年度の PIA のレビュー残しがあったので、受領 PIA よりもレビューPIA の数が大きくなっている。

OPC のレビュー担当のオフィサーを割り当てる。何らかの専門的な知識が必要な場合は、専門家を呼ぶ場合もある。ex. パブリックセーフティの専門家、IT の専門家等。

OPC では、下記のようなレビュー用テンプレートを使ってレビューを行っている。

○OPC における PIA レビュー用テンプレート

- Oakes Test（必要性と釣り合いに関する Four-Part Test）: いわゆる「比例原則」[55]に対応するもの
  - 当該手段はニーズ（目的）に対して明確に必要なものであるか
  - 当該手段はニーズに対して効果的なものであるか
  - プライバシーへの影響はニーズと釣り合ったものであるか
  - 同じ目的を達成するのに、よりプライバシーへの影響の少ない他の手段はないか
- プロジェクトの概要
- PIA に関するチェックリスト
  - Preliminary PIA であるか？
  - PIA は内部で実施されたものか？
  - Threat and Risk Assessment も併せて実施されているか？
  - 十分なエグゼクティブサマリーがあるか？
  - プロジェクトの記述は完全なものか？
  - プロジェクトの根拠又はニーズは明確なものか？
  - どんな個人情報の要素が含まれているか？

[55] 達成されるべき目的とそのために取られる手段としての権利・利益の制約との間に均衡を要求する原則。

- 取扱われる情報は十分に記述されているか？
- 情報はセンシティブなものであるか？
- プロジェクトには具体的な法的権限付けがあるか？
- 業務プロセスのダイアグラムは十分なものか？何が不明確か？
- どんなプライバシー・イシュー／影響／リスクが特定されているか？
- 全てのプライバシーリスクが特定されているか？
- 全てのリスクは管理可能なものか？
- リスクの軽減策は適切なものか？
- 資金を拠出する政府機関はきちんと対応しているか？

・ 業務プロセス、データ要素、データの流れ
・ プロジェクトが現在どのフェーズにあるか
・ プライバシーリスク、軽減策、コメント、勧告
  - カナダ規格協会の策定した「公正な情報取扱い 10 原則」[56]に沿ってプライバシーリスクを評価する。
    - ✧ 説明責任（Accountability）
    - ✧ 目的明確化（Identifying Purposes）
    - ✧ 同意（Consent）
    - ✧ 収集の制限（Limiting Collection）
    - ✧ 利用・提供・保持の制限（Limiting Use, Disclose, and Retention）
    - ✧ 正確性（Accuracy）
    - ✧ 安全管理措置（Safeguards）
    - ✧ 公開性（Openness）
    - ✧ 個人のアクセス（Individual Access）
    - ✧ 苦情対応（Challenging Compliance）
・ 全般的な評価、その他の特筆すべき事項、勧告の概要
  - 提出された PIA でカバーされていないプライバシーリスクや、想定される大きな社会的懸念について言及する。

○OPC ガイドにおける PIA 報告書のフォーマット

OPC ガイドでは、PIA 報告書のフォーマットとして、以下が指定されている。

・ 適切なレベルの権限者が署名をしたカバーレター
・ プロジェクトの詳細概要（目的、根拠、顧客、アプローチ、プログラム、パートナーを含む）
・ 関係者のリスト、関係者の役割と責任

[56] http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code

- 取扱われる個人情報の種類、データフローの記述
- プロジェクトに関係する法律やポリシーのリスト（個人情報収集の法的権限を示すため）
- プロジェクトに関係するプライバシーリスクを特定するプライバシー分析（少なくとも、公正な情報取扱い 10 原則について対処するべき）
- PIA で特定されたプライバシーリスクに対処するために導入される軽減策について述べた詳細なリスク軽減計画
- プライバシーを重視したコミュニケーション戦略の概要（必要な場合）
- プライバシー違反へのインシデント対応、開示・訂正請求への対応、苦情対応に関する内部手続きの詳細

○OPC ガイドにおける PIA 報告書の添付書類

OPC ガイドでは、PIA 報告書と一緒に OPC に提出すべき添付書類として、以下のものが指定されている。

- プロジェクト固有のプライバシーポリシーと手続き
- Threat and Risk Assessment で特定されたプライバシーリスクの概要、それらのリスクへの対応策に関する説明
- 情報シェアリングに関する権利と責任を規定した法律文書や合意、覚書のコピー
- データマッチングに関する評価
- 情報シェアリングに関する第三者との契約のコピー
- 個人情報収集時に使用される申請書のコピー（プライバシーステートメントを含む）
- 個人情報管理のための教育資料のコピー
- PIB に関する記述
- 政府機関サイトに掲載した PIA 概要のコピー

３．５　複数機関が関与する PIA について

（１）連邦プライバシーコミッショナー事務局（OPC）の見解

OPC は、ある新たなイニシアティブが複数の政府機関を跨るものである場合、複数の機関で 1 つの PIA を実施することを奨励している。これを「アンブレラ PIA」と呼んでいる。

OPC がアンブレラ PIA を推奨する理由は、OPC ガイド（2.4 節）に記載されている[57]。

---

[57] 「水平的なイニシアティブが増えていること、また連邦政府が顧客中心サービスを強調していることによって、OPC では複数機関を跨る PIA や、複数の管轄地域に跨る PIA の数が増加している。各々の PIA にとって、1 つの省や局がプライバシーに関する強力な政策的リーダーシップを果たすことが重要である。このことは、OPC との整合的なコミュニケーションを保証し、全ての参加機関の間でのプライバシーリスクの効果的な特定を保証することの一助となる。このことはまた、関連するプログラムやイニシアティブを跨った

要点は以下の 3 つである。

- イニシアティブに参画する全ての機関においてプライバシーリスクを効果的に特定できるようにするため。
- プライバシーリスク軽減策を参画機関を跨って実施できるようにするため。
- 参画機関に期待されるプライバシープラクティスをガイダンスとして提供するため。

必要に応じて、アンブレラ PIA の下で、各機関が個別の PIA を行うことも可能である。

なお、TBS 策定の PIA 指令でも、1 つの機関がリーダーになり、他の機関を取りまとめて PIA を実施することが謳われている。

（2）オンタリオ州情報プライバシーコミッショナー事務局（IPC）の見解

州の各政府機関が 1 つのイニシアティブとしてシステムを導入するような場合、2 つの種類の PIA が存在する。1 つは当該イニシアティブに対する包括的 PIA であり、もう 1 つは個別の政府機関で実施する PIA である。

州の各政府機関が 1 つのイニシアティブとしてシステムを導入する場合とは、例えば、州政府機関で ID マネジメントシステムを導入するような場合である。この場合、イニシアティブに対して包括的な PIA を実施するが、既存のシステムに与える影響が各政府機関で異なると考えられる場合には、個別の PIA も実施する。

また、各政府機関が異なる目的で当該システムを導入するような場合は、個別の PIA が必要である。例えば、1 つのカードを各機関が異なる目的で利用するような場合である。

ID 連携システムにおける複数機関 PIA に関しては、IPC は「The New Federated Privacy Impact Assessment」（2009 年 1 月）という提言書を公表している。

（3）ロビン・ベイリー氏（Linden Consulting 代表）[58]の見解

複数機関を跨ったイニシアティブについては、各機関の代表者からなる代表委員会が Big PIA を実施し、その結果を各機関に遵守させるべきである。

代表委員会は、同じ種類の機関からの代表者は 1 人にする等、なるべくメンバーを少なくするべきである。その後、各機関で必要に応じて、個別の PIA を実施するようにする。

プライバシーリスク軽減戦略の実施を保証することの一助となる。この意図は、情報の共有へのニーズを正当化したりするためのビジネスケース（投資対効果検討書）を統合したり、政府の省庁を跨った情報の共有をカナダ国民に知らせるための共通のコミュニケーション戦略を立てたり、当該イニシアティブに参画する全ての省や局のためのガイダンスとして期待されるプライバシープラクティスの堅固な基盤を提供するような、包括的な PIA を実施することである。」

58　カナダで著名なプライバシーコンサルタントであり、ブリティッシュ・コロンビア州のプライバシーコミッショナーからの委託を受けて、各国（NZ、米国、オーストラリア等）における PIA 調査も実施している。

４．カナダ（オンタリオ州）の状況

４．１　カナダ（オンタリオ州）の PIA 制度概要

（１）PIA の根拠規程

カナダのオンタリオ州における PIA の根拠規定には、以下のものがある。

・ オンタリオ州行政サービス省の「Procurement Directive」（調達指令）：
州の政府機関（省）に「個人情報やセンシティブ情報の提供（release）をもたらすような物品やサービスの調達の実施」に先立ち、PIA を行うことを要求している。

・ オンタリオ州行政サービス省の「Corporate Policy on Protection of Personal Information」（個人情報保護に関する共同ポリシー）：
州の政府機関（省）に、「個人情報を含む情報システムやデータベースの作成や重要な変更など、個人情報の収集・利用・提供に重要な変更」がある場合には PIA を実施することを要求している。

・ 他にオンタリオ州内閣経営委員会の「Management and Use of Information & Information Technology Directive」（情報及び情報技術の管理と利用に関する指令）にも規定がある。

（２）各機関の役割分担

○オンタリオ州行政サービス省の情報・プライバシー・アーカイブ部門（Information, Privacy and Archives Division：IPA）

オンタリオ州においては、プライバシーコミッショナー事務局（IPC）よりもむしろ IPA が PIA に関する重要な役割を担っている。

IPA は、州の政府機関から準備分析（Preliminary Analysis）の提出を受け、レビューを実施、助言を提供する。州の政府機関からその他の PIA 文書のレビュー依頼を受けて、レビューすることも可能である。

IPA はオンタリオ州の共通リソースとして、行政サービス省のみならず、州の全ての政府機関にサービスを提供している。

「オンタリオ州公共サービスのための PIA ガイド」を策定している。

○オンタリオ州情報プライバシーコミッショナー事務局（Office of the Information and Privacy Commissioner of Ontario：IPC）

IPC は、ハイリスクと考えられるプロジェクトに対して、PIA のレビューを実施している。また、医療分野における PIA ガイドラインを策定している。

プライバシーコミッショナーの Ann Cavoukian 博士は「Privacy by Design」の提唱者として世界的に有名である。

○州の政府機関

プロジェクトマネジャーが PIA を実施し、プロジェクトスポンサー（意思決定者）が PIA を承認する。

プライバシーに重大な影響のある事柄については、IPA に相談を行っている。

PIA の公開義務は特にない。

４．２　PIA の構成要素

○PIA の実施対象

IPA の PIA ガイド[59]によれば、PIA の実施対象は、「個人情報の収集・利用・提供に重要な変更」がある場合や、「個人情報やセンシティブ情報の提供をもたらすような物品やサービスの調達」を実施する場合である。

該当するプロジェクトの例は、以下の通りである（IPA の PIA ガイドより）。

- 新しいプログラム
- 既存のプログラムへの大きな変更
- 新たな技術、又はプライバシーへの影響が知られている技術の使用
- 技術への大きな変更
- データベースの作成や変更
- 識別・認証スキームの作成や変更

○PIA の構成要素

IPA は、PIA の構成要素として、以下の 3 つを定めている。

①Preliminary Analysis（準備分析）

PIA 実施対象となる全てのプロジェクトに対して実施し、さらなる分析が必要か否かを判断するためのツールである。

②Privacy Risk Analysis（プライバシーリスク分析）

単に FIPPA（オンタリオ州の情報の自由・プライバシー保護法）を遵守することを超えて、プロジェクトが及ぼす広範なプライバシーへの影響について認識するためのツールである。

③Privacy Design Analysis（プライバシーデザイン分析）

プロジェクトが FIPPA の要件を遵守するための方法を詳細に特定するためのツールであ

[59] Information, Privacy and Archives Division, “Privacy Impact Assessment Guide for the Ontario Public Service”, （2011 年 7 月改訂）

る。

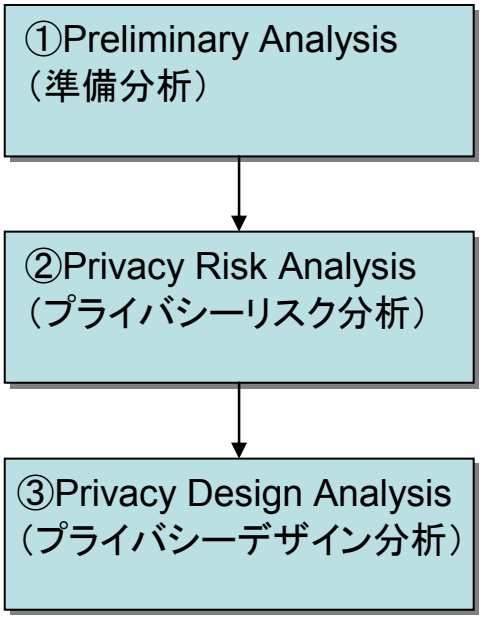


図 14　カナダ・オンタリオ州における PIA の構成要素

（１）Preliminary Analysis（準備分析）

PIA の実施対象となる全てのプロジェクトは、まず Preliminary Analysis を実施する。質問表に回答し、プロジェクトが個人情報を含むものか否か、そして FIPPA（オンタリオ州の情報の自由・プライバシー保護法）[60]に則って保護する必要があるか否かを決定する。プロジェクトの概念フェーズ（後述）で実施する。

州の政府機関は Preliminary Analysis を IPA に提出し、IPA のレビューを受ける。IPA で不十分と判断した場合は、IPC からコメントを貰う。

（２）Privacy Risk Analysis（プライバシーリスク分析）

FIPPA への単なる遵守を超えて、プロジェクトが及ぼす広範なプライバシーへの影響について認識するためのツールである。

Preliminary Analysis の結果、プロジェクトが個人情報を含むものであることが示された場合、かつ広範なプライバシーへの影響を評価する必要がある場合に、Privacy Risk Analysis を実施する。

プロジェクトのプライバシーリスクやその発生可能性、影響度、対処の優先順位、対応策を特定することが目的である。プロジェクトの概念フェーズで、プロジェクトの方向性を決定する前に、いくつかの選択肢を評価する際に実施する。実施に当たっては、IPC のプライバシー・デザイン 8 原則[61]の遵守を確認する。

---

60 オンタリオ州政府機関が対象となる法律。

61 http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=318

プロジェクトスポンサー（プロジェクトの意思決定者）によるレビューと承認が必要である。

（３）Privacy Design Analysis（プライバシーデザイン分析）

プロジェクトが FIPPA の要件を遵守するための方法を詳細に特定するためのツールである。

プロジェクトにおける業務プロセスや役割、責任、システム、アプリケーション、技術等のレビューが含まれる。具体的には、以下を明確化する。

- 関連する業務プロセス
- 役割と責任
- プロジェクトをサポートする技術
- 個人情報のフロー
- プライバシーリスク、発生可能性、影響度、対処の優先順位、対応策
- FIPPA を遵守する方法に関するレコメンデーションとアクションアイテム

特定されたプライバシーリスクを軽減するための行動計画を作成することが目的である。プロジェクトの実施フェーズの前に実施する。

プロジェクトスポンサーによるレビューと承認が必要である。

○オンタリオ州公共サービスのプロジェクトマネジメント・フレームワーク

なお、オンタリオ州公共サービスのプロジェクトマネジメント・フレームワークは、「概念（Concept）」→「定義（Definition）」→「計画（Planning）」→「実施（Implementation）」→「完了（Close-Out）」の 5 つのフェーズから成る。

PIA ガイドでは、Preliminary Analysis と Privacy Risk Analysis はプロジェクトの概念フェーズで、Privacy Design Analysis は実施フェーズの前に実施するものと規定されている。

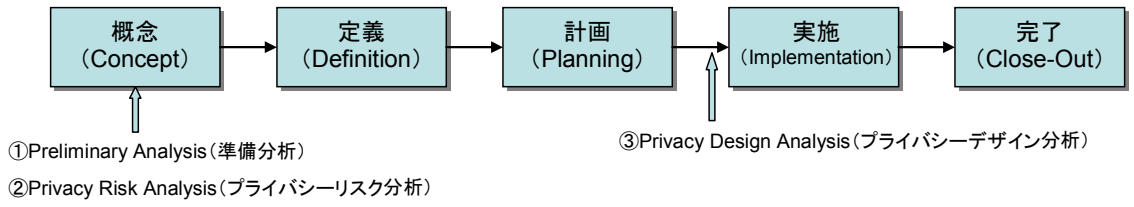


図 15　カナダ・オンタリオ州公共サービスのプロジェクトマネジメント・フレームワーク

４．３　PIA の実施手順

オンタリオ州における PIA（Preliminary Analysis、Privacy Risk Analysis 及び Privacy Design Analysis）の実施手順は、図 16 の通りである。

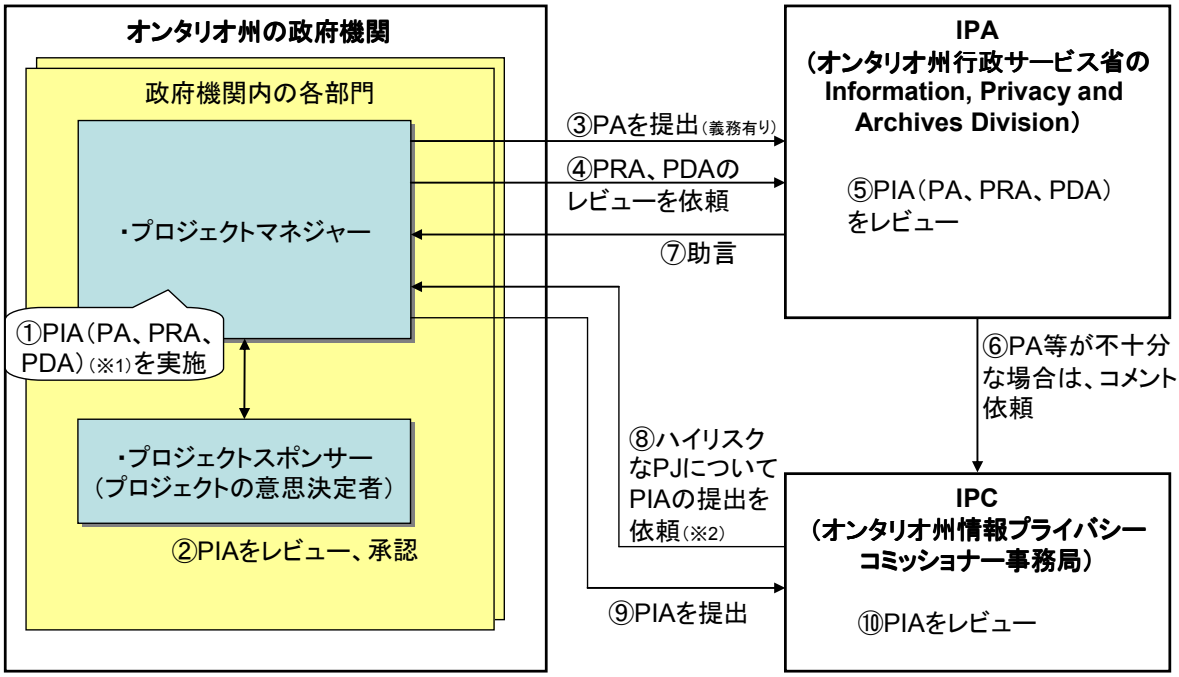


図 16　カナダ・オンタリオ州政府機関における PIA の実施手順

○PIA の承認

あるプロジェクトがファンディングを受けるためには、プロジェクトスポンサー（プロジェクトの意思決定者）に対して PIA を提示し、承認を受けることが必要である。

ゲーティッドファンディング[62]の場合は、ファンディングの各段階ごとに PIA を実施し、そのつど承認を受けることが必要である。

○PIA におけるパブリックコンサルテーション

PIA プロセスの中で必ずパブリックコンサルテーションをしないといけない訳ではないが、特に一般市民への影響が大きいプロジェクトについては実施している。例えば、トロント郊外への監視カメラの設置、オンタリオ州における IC 運転免許証の導入等の場合には、実施したとのことである。

62 ゲーティッドファンディングとは、政府機関の大きなプロジェクトの場合、プロジェクトを段階ごとに管理し、段階ごとにファンディングすることを指す。

○PIA 実施をいかに保証するか

PIA は法令上の義務ではないので、PIA を実施しない州政府機関や、きちんと実施していない州政府機関に対する罰則はない。ただし、PIA を実施しないことでプライバシー違反（privacy breach）が起こった場合、その機関が自らの評判を落とすことになる。IPC としては、Privacy by Design の哲学を広めることで、政府機関に自ら遵守してもらうように働きかけている。

５．英国の状況

５．１　英国における PIA 導入状況

（１）PIA 導入の背景

情報コミッショナーオフィス（Information Commissioner's Office : ICO）の「監視社会に関する報告書[63]」（2006 年）の中で、英国における監視社会（CCTV、ID カード等）の進展に対処するための手段として PIA に言及しており、この報告書が PIA 導入の 1 つの契機となっている。

（２）その後の経緯

2007 年 5 月頃、ICO が PIA 国際調査（カナダ、 オーストラリア、米国等）と、ハンドブック作成を公募し[64]、2007 年 12 月に ICO が PIA ハンドブック"Privacy Impact Assessment Handbook"を発行した。PIA ハンドブックは、2009 年 6 月に第二版[65]が発行されている。

この PIA ハンドブックの中では、PIA の対象となるシステム[66]は、個人データの処理を伴うもの全般（官民を問わない）とされている。

2008 年 6 月には内閣府が報告書"Data Handling Procedures in Government"[67]を発行し、その中で、中央省庁に対して、個人情報を取扱う新しい制度・システムに関して PIA 実施を義務化している[68]。同報告書は、2007 年の歳入関税局での 2500 万人分のデータ入り CD-R 紛失事件を受けたものである。中央省庁に対する PIA 実施の義務付けは、法令化されたものではないが、2010 年 1 月までに中央省庁で 270 件の PIA が実施[69]されている。

さらに 2010 年 8 月には、法務省が省庁向け PIA ガイダンス"Undertaking Privacy Impact

---

63 Information Commissioner's Office, "A Report on the Surveillance Society: For the Information Commissioner by the Surveillance Studies Network",（2006 年 9 月）（http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf）。

64 Information Commissioner's Office, "Privacy Impact Assessments Project - Invitation to bid",（2007 年）（http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/piap_inv_to_tenderfinal.pdf）。

65 Information Commissioner's Office, "Privacy Impact Assessment Handbook Version 2.0",（2009 年 6 月）（http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html）。

66 PIA ハンドブックの中では、PIA を実施する対象を指す用語として "Project" の語が使われているが、本報告書では「システム」と読み替えている。

67 Cabinet Office, "Data Handling Procedures in Government: Final Report",（2008 年 6 月）（http://www.cabinetoffice.gov.uk/sites/default/files/resources/final-report.pdf）。

68 既存のシステムに対しては、監査制度がある。

69 Cabinet Office, "Protecting Information in Government",（2010 年 1 月）（http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/caboffprotectinfo.pdf）。

Assessments”[70]を発行した。この PIA ガイダンスは賛否両論あった ICO ハンドブックを省庁向けに簡易化したものであり、とりわけデータ保護法への遵守に特化した内容となっている。

５．２　ICO（情報コミッショナーオフィス）の概要

ICO は、英国におけるデータ保護（および情報公開）のための第三者機関であり、EU データ保護指令第 28 条で加盟各国に要請された「監督機関」に該当する。官民におけるデータ保護法への遵守を監督することがミッションである。

ICO の活動内容は大きく 3 つある。

①個人や団体から法律違反に関する苦情を受け付け、対応する。

②団体に対して法律に従うためのベストプラクティスや教育を提供する。

③団体・個人に対して執行通知を発行する。

PIA は②の活動の一環である。

ICO の体制

現コミッショナーはグレイアム氏（2009 年 6 月～）で 4 代目である。初代コミッショナーは 1984 年に任命された（当時はデータ保護登録官）。職員数は 327 名（2010 年現在）であり、本部はマンチェスター郊外の Wilmslow にある[71]。

省庁との関係

各政府機関から独立した機関であるが、法務省との結び付きは強い。

情報コミッショナーは法務省が公募し、法務省の国務大臣が選定し、庶民院（衆議院）の委員会が承認し[72]、女王が任命することとなっている。

ICO の権限

英国のデータ保護･プライバシー有識者[73]によると、ICO の政府に対する発言権はそれほど強くないとのことである。

ただし、データ保護法違反の観点からデータ処理に対して意見を表明することはできる（データ保護法第 22 条）。

ICO は官民のシステムに対する監査が行うことができる。通常は、民間のリクエストを

---

[70] Ministry of Justice, "Undertaking Privacy Impact Assessment: The Data Protection Act 1998”,（2010 年 8 月 13 日）
（http://www.justice.gov.uk/guidance/docs/pia-guidance-08-10.pdf）。

[71] ICO 本部がこの田舎町にあるのは、ICO 職員によると、初代コミッショナーが希望したためであるらしい。

[72] 委員会が拒否することも可能だが、今までそのようなケースはない。

[73] オックスフォード大学の Ian Brown 先生。

受けて、政府機関に監査を行う。最近では、リクエストが無くても監査ができる権限を付与されたという。

また、2009 年に ICO の権限が強化されている。データ保護法に新たに 55A 条が追加され、データ侵害によって生じた損害に釣り合った罰金を政府機関や民間企業に課す新たな権限が付加された。罰金の最高額は 50 万ポンド（約 6600 万円）に設定された。

５．３　ICO が PIA において果たす役割

基本的に、ICO が PIA において果たす役割は、PIA の普及啓発のみである。具体的には、ガイドライン（ハンドブック）の作成・提供や、教育（トレーニング）・ワークショップ等を実施している[74]。

PIA は自己評価のツールとしてデザインされているので、PIA の実施方法は実施機関の自主性に委ねられている。ICO は方法論を提供するのみで、PIA の実施方法について細かい指示を行うことはしない。ICO としては、PIA に関して新たに業務を増やすのではなく、既存の枠組み（ex.リスクマネジメント等）の延長上で実施することを推奨しているとのことである。

PIA 実施機関は、ICO に PIA 報告書を提出したり、承認を得る義務はない。ただ、中央省庁に関しては、上述のように内閣府が PIA 実施を義務化しているので、内閣府が PIA 実施状況を管理している。

PIA 報告書の公開は義務ではないが、PIA ハンドブックでは、セキュリティ・センシティブな情報は除いた上で PIA 報告書を公表することを推奨している。

ICO で官民における PIA の実施状況を把握している訳ではないが、ICO への問合せやイベントでの反応から PIA の浸透の度合いを見ると、行政分野では広範囲で利用されている。民間ではあまり利用されていないようである。

５．４　英国における PIA の特徴

英国における PIA の最大の特徴は「コンサルテーション・フェーズ」を重視していることである。

「コンサルテーション」とは、利害関係者との話し合い・意見聴取のことであり、想定される影響やリスクの洗い出しが目的である。システムを利用する職員、システム開発に携わる IT 企業・セキュリティ企業、プライバシーの影響を受ける市民・顧客などが対象となる。コンサルテーションの方法は様々であり、ICO は特にその方法を指定しない。

---

[74] PIA は比較的に新しい概念であり、実施組織に知識がある人が少ないので、どうやって実施するのか、実施することでどんなベネフィットがあるかを説明するためのトレーニングやプレゼンテーションを実施している。プライバシーを保護する以外にも、経済的な利益があることを理解してもらわないといけない。そのため、トレーニングに良い事例の紹介を入れている。ICO は PIA を実施した団体に良い事例を紹介してほしいが、それをしたがらない団体が多いことが課題であるとのことである。

市民に対するコンサルテーションの方法としては、フォーラムの開催、フォーカスグループの形成、市民団体への文書による照会、パブリックコメント等がある。

コンサルテーションの実施によって、プロジェクトの早期の段階で設計に変更を加えることが可能になるため、ICO としてはコンサルテーションが重要なプロセスだと考えている。市民に対しては、コンサルテーションで洗い出したリスク[75]に対して、PIA を通じてこのように解決を図っていると説明することができる[76]ため、これによって反対意見を取り込むことが可能となる。

PIA の具体的方法は、次節に見るように、ICO の PIA ハンドブックにて規定されている。

５．５　ICO の PIA ハンドブックの概要

ICO の PIA ハンドブックは、英国における「監視社会」の進展に対抗する ICO の取組みの一環であり、カナダ・オーストラリアといった他国の取組みの研究に基づき、2007 年 12 月に第 1 版が公表された。これは、英国で初めての PIA に関するガイダンスである。第 1 版の公表後、「分量が長い」「繰り返しの箇所がある」といったいくつかの意見を受けて、2009 年 6 月には第 2 版を公表した。

以下の記述は、PIA ハンドブックの第 2 版をベースとしている。

５．５．１　PIA の実施概要

（１）なぜ PIA を実施するか

PIA は、当該プロジェクトにおいて個人に対するプライバシーリスクを考慮に入れるためのプロセスであり、単に（英国の）データ保護法を順守するために必要となる措置よりもカバーする範囲が広い。PIA は、関係するステークホルダーたちの見解を集め、適宜フィードバックを行う、透明でコンサルティブなプロセスである。

PIA を実施することによって、一般市民を含むステークホルダーの理解やコミットメントを得ることができる。これによって、当該プロジェクトに対する一般市民のプライバシー保護面での信頼を醸成することが可能となる。

PIA は当該プロジェクトの開始（設計等のフェーズ）に先立って、事前に実施するべきである。事前に行うことによって、PIA の実施組織が、起こりうる問題（プライバシーリスク）を予見したり、問題に対する解決策を事前に見出すことが可能となる。プロジェクトの中途や事後に PIA を実施することは避けるべきである。なぜなら、事後にシステムの仕様を変更したりエラーを直すことは、コストがかかるし、更なるエラーを引き起こす恐

---

[75] ICO によれば、「リスクがないと結論付けるのではなく、あらゆる段階でリスクを特定し、それらの最小化を図った上で、残存するプライバシー侵害リスクが正当化できるものであるかを確認することが重要」とのことである。

[76] 「プライバシーの論争は、政府の進めようとすることが正しいか、市民の意見が正しいかという二者択一的な論争にするべきではない」とのことである。

れがあるからである。

（２）PIA の実施体制

PIA 実施の責任は一義的には上級経営層（senior executive）にある。上級経営層が PIA 実施の責任を委任すべき人物としては、以下の選択肢がある。

① プロジェクトチーム内の１人
② プロジェクト外の人
③ 外部コンサルタント

組織内に必要なスキルがない場合、または、組織へ与える影響から可能な限り独立なものとして PIA を実施したい場合には、③の外部コンサルタントを活用することが考えられる。ただ、外部コンサルタントを活用することのデメリットとして、PIA によって得られた結論に対して組織内の人間が抵抗することや、組織のニーズや投資対効果検討書（business case）に対する理解や尊重が欠如する恐れがあることを考慮に入れるべきである。なお、PIA は監査ではないので、独立性に対する強い必要性はない。

ICO は、当該組織の CPO（チーフ・プライバシー・オフィサー）が PIA 実施の責任を委任されるべきとしている。

（３）PIA の成果物

PIA ハンドブックでは、PIA 実施の結果として得られる成果物について、以下のものを挙げている（成果物とは、必ずしもドキュメントに限られるものではない）。

- 当該プロジェクトのプライバシー影響の特定
- 全てのステークホルダーの観点からのプライバシー影響の理解
- 当該プロジェクトやその特徴に対する、影響を受ける組織や人々の受容と理解
- よりプライバシーを侵害しない代替手段の特定と評価
- プライバシーに対する負の影響を防止する方法の特定
- プライバシーに対する負の影響を軽減する方法の特定
- プライバシーに対する負の影響を不可避な場合には、そのことを正当化する業務上のニーズの明確化
- 成果物の文書化と公表

５．５．２　PIA の実施プロセス

ICO の PIA ハンドブックにおいて、PIA の大まかな実施プロセスは、以下のように規定されている。

Ⅰ．イニシャル・アセスメント[77]

・スクリーニングの実施（質問表の利用）

・PIA の実施が必要か否かの決定（さらに、フルスケール版か、小規模版[78]か）

・質問表への回答を全体的に検討して判断する

・利害関係者の特定

Ⅱ．PIA の実施（下記はフルスケール版の場合）[79]

①予備フェーズ（Preliminary Phase）

・プロジェクト概要文書の作成

②準備フェーズ（Preparatory Phase）

・利害関係者とのコンサルテーション計画の作成

・諮問委員会の立ち上げ（利害関係者の代表者で構成）

③コンサルテーションと分析フェーズ（PIA の中核）

・利害関係者（市民を含む）とのコンサルテーションの実施

・プライバシーリスクの特定

・個々のリスクに対する解決策（回避策または軽減策）の検討

・解決策の設計への組み込み（設計内容の変更）

・諮問委員会との相談

④文書化フェーズ（Documentation Phase）

・PIA 報告書の作成

⑤レビューと監査フェーズ（Review and Audit Phase）

・解決策が実装されていることのレビュー

Ⅲ．法令コンプライアンス・チェック（チェックリスト利用）

・プライバシー関連法令へのコンプライアンス・チェック

・データ保護法へのコンプライアンス・チェック

---

77 イニシャル・アセスメントは、個人データを処理する全てのシステムが対象である。

78 例えば、システム改修時に、改修によって既存システムに新たな処理プロセスが追加される場合には、小規模版の PIA が推奨される。また、小規模システムの導入の際には小規模版の PIA が推奨される。

79 予備フェーズ以降は、イニシャル・アセスメントのスクリーニングで残ったシステムが対象となる。

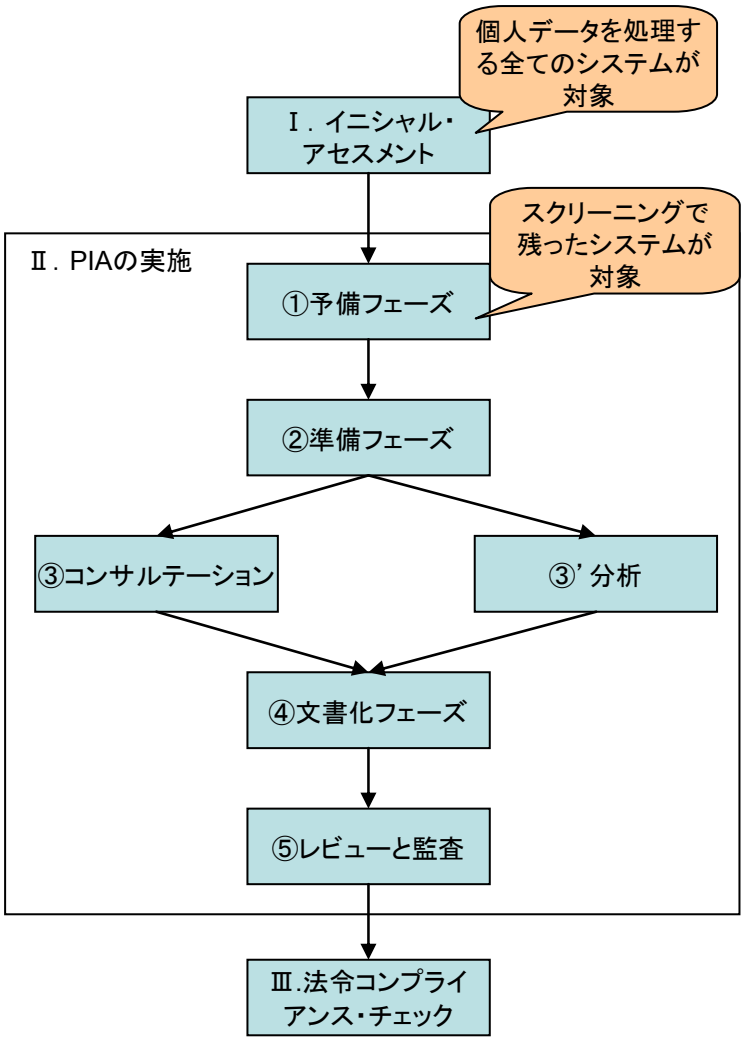


図 17　PIA の実施プロセス[80]

（1）イニシャル・アセスメント

イニシャル・アセスメントは、当該プロジェクトにおいて PIA 実施が必要か否かを決定するプロセスである。

○PIA スクリーニングプロセスの準備

スクリーニングプロセスにおいて質問に回答するのに必要な情報が収集されなければならない。当該プロジェクトに関する十分な情報がないと、明確な結論に到達できない恐れがある。どのレベルの PIA を実施するか（フルスケールか、小規模版か、PIA を実施しないか）を決定するために、本プロセスでは以下の 3 つの情報を集める必要がある。

- プロジェクト概要（project outline）
- ステークホルダー分析

[80] ICO, “Privacy Impact Assessment Handbook Version 2.0”の図に筆者加筆。

・ 環境のスキャン

スクリーニングプロセスの質問は、これらの情報に基づき（少なくとも一時的には）回答できるはずである。

プロジェクト概要の取得または策定

プロジェクトの初期の段階においては、限定された文書しか入手できなかったり、プロジェクトのスコープやシステムの特徴が不明確であったりする。

プロジェクトの目的が何であるかを知り、プロジェクトの潜在的な影響が何であるかを検討し始めるために、プロジェクトの初期のドキュメント（プロジェクトチャーターや付託条項など）のコピーを入手するべきである。

ステークホルダー分析の実施

このことは、プロジェクトに関心があったり、実運用において役割を演じたり、影響を受けたりするグループや組織のリストの作成を含む。このリストは以下を含む。

- プロジェクトを実施する組織や、当該組織内の下位組織
- プロジェクトに直接に関係するその他の組織
- プロジェクトからベネフィットを受けることが想定される組織や個人
- プロジェクトによって影響を受けるかもしれない組織や個人
- プロジェクトを可能にする技術やサービスを提供する組織

ほかに何かないかを調べる

同様な性格の既存プロジェクトについて情報を探すことは価値があるだろう。新たな技術が利用されている場合、またはプロジェクトが既存技術を新たなやり方で応用する場合、当該技術やその応用の記述が集めることによって、イニシャル・アセスメントの評価をサポートすることができるだろう。

以下のようなソースを考慮することができる。

- 同様なプロジェクトにおける既存の PIA。組織内で実施されたもの、他の組織で実施されたもの、他国で実施されたもの。
- 業界団体や技術プロバイダー、リサーチセンターによって公表されたファクトシート、白書、報告書、関連記事。
- 専門家協会とのコンサルテーション。
- プライバシー規制者、とりわけ ICO とのコンサルテーション。
- 他の規制者（例えば消費者権利分野）とのコンサルテーション。
- プロジェクトによって潜在的に影響を受ける人々を代表したり、そうした人々にアドバイスを提供する NGO とのコンサルテーション。

○PIA スクリーニングのための質問

上記の準備を終え、情報を入手したら、スクリーニングプロセスを実施する。

スクリーニングプロセスの目的は、当該組織が行う「投資」がリスクと釣り合ったものであることを保証することである。具体的には、以下の 4 つの質問セットに順次、回答を行う。

①フルスケールの PIA がレコメンドされるか？

- このステップでは、プロジェクトの主要な特徴がフルスケール PIA が必要であることを示唆するかを確認する。
- フルスケール PIA 用のスクリーニング質問に回答する[81]。フルスケール PIA がふさわしいか否かは、質問表への回答を全体的に検討して判断する
- もし Yes であれば、フルスケールの PIA、プライバシー法令コンプライアンス・チェック、データ保護法コンプライアンス・チェックを実施する。
- もしフルスケールの PIA がレコメンドされない場合は、以下に進む。

②小規模版の PIA がレコメンドされるか？

- このステップでは、プロジェクトの主要な特徴が小規模版の PIA が必要であることを示唆するかを確認する。
- 小規模版 PIA 用のスクリーニング質問に回答する。小規模版 PIA がふさわしいか否かは、質問表への回答を全体的に検討して判断する。
- もし Yes であれば、小規模版の PIA、プライバシー法令コンプライアンス・チェック、データ保護法コンプライアンス・チェックを実施する。
- もし小規模版の PIA がレコメンドされない場合は、以下に進む。

③プライバシー法令コンプライアンス・チェックがレコメンドされるか？

- このステップでは、何らかのプライバシー関連法令の影響下にある活動が含まれるかを確認する。
- もし Yes であれば、プライバシー法令コンプライアンス・チェックとデータ保護コンプライアンス・チェックを実施する。
- もしプライバシー法令コンプライアンス・チェックがレコメンドされない場合は、以下に進む。

④データ保護法のコンプライアンス・チェックがレコメンドされるか？

- このステップでは、プロジェクトの活動は「個人データ」の取扱いを含んでいるか

[81] フルスケールの PIA 用のスクリーニング質問表については、２．５．３節に翻訳を記載する。

を確認する。

- もし Yes であれば、データ保護コンプライアンス・チェックを実施する。

○プライバシーリスクのイニシャル・アセスメントの実施

上記で概要を述べたステップを全て実施したら、プロジェクトが直面する可能性があるいくつかの当初のプライバシー影響やリスク、脆弱性をリスト化することでできる立場にある。このことは、いかに PIA を完遂するかや、ステークホルダーに対してどのような質問があるか、プロジェクトの実施の間どのような問題が生じうるかといった情報を提供するための初期見解として利用することができる。

しかし、このことは、プライバシーリスク[82]を特定するための単なる初期の試みにすぎないこと、また、当該組織の視点から検討されたものであることを明確にしなければならない。PIA 実施の間、ステークホルダーは、実施組織が検討しなかった懸念を提起したり、あなたが特定したが却下した懸念に対して大きな重みを与える可能性がある。

（２）PIA の実施（PIA の本体）

ICO の PIA ハンドブックでは、フルスケール版 PIA 用のプロセスとして、以下の 5 つのフェーズが規定されている。

①予備フェーズ（Preliminary Phase）
②準備フェーズ（Preparation Phase）
③コンサルテーションと分析フェーズ（Consultation and analysis phase）
④文書化フェーズ（Documentation phase）
⑤レビューと監査フェーズ（Review and audit phase）

①予備フェーズ（Preliminary Phase）

予備フェーズの目的は、PIA を効果的かつ効率的に実施するための堅固な基盤を築くことである。成果物は、プロジェクト計画、プロジェクト背景ペーパーである。

予備フェーズのタスクとして、以下のものが挙げられている。

- イニシャル・アセスメントの結果と文書をレビューする。必要あれば、PIA 実施にとって有用だが､イニシャル･アセスメントでは作成されなかった文書を用意する。
- イニシャル・アセスメントの際に作成されたプロジェクト概要を発展させる。
- PIA チームに付された権限、スコープ、リソースが適切であることを保証する。
- 関連する組織と予備の議論を行う。これらの議論は、当該組織と主要参加組織に関

[82] なお、ICO の PIA ハンドブックでは、プライバシーリスクの 2 つのカテゴリーとして、①個人に対するリスク（個人情報の紛失・損害・誤用・濫用の結果として生じる、プライバシーに関連した権利の侵害等)、②組織に対するリスク（情報漏えい、評判の低下、法令違反、対策コストの発生等）の 2 つが挙げられている。

連する部分にフォーカスして行われる。ICO を含む、外部の組織との議論も、一定の環境下では推奨される。

- ステークホルダー・グループの代表者と予備の議論を行う。このことは、当該プロジェクトによって外部の特定の組織や人々が大きな影響を受ける場合に重要である。
- プライバシー・イシューに関する予備の分析を実施する。このことは、スクリーニングプロセスの結果についてのより深い再検討を開始することとなるだろう。
- プロジェクト背景ペーパーを準備する。この文書は、ステークホルダーとの議論のベースとなる。

プロジェクト概要（プロジェクト背景ペーパー）の作成

プロジェクト背景ペーパーの作成目的は、次のフェーズ以降の堅固な基盤を作ることである。プロジェクト背景ペーパーは以下の内容を含むべきである。

- プロジェクトの提案が進められた文脈や背景の記述（関連する社会的・経済的・技術的考察を含む）。
- 当該プロジェクトの基本となるモチベーションや動因、機会に関する記述。
- プロジェクトの目標、スコープ、業務上の理由付けに関する記述。
- プロジェクトがどのように具体化するかについての当該組織の現行の理解を反映した、プロジェクトの設計に関する記述。
    - 参加者がプロジェクトの影響を検討することができるように十分に詳細なレベルで説明することが必要である。
    - この詳細は、プロジェクトの開発段階に依存して変わる。もし目立った設計の特徴が決まっていない場合には、設計に関する記述は、概念的かつ大雑把なものとなるかも知れない。
    - もしプロジェクトがすでに要求分析と設計フェーズを経過している場合は、プロジェクト背景ペーパーは、十分に詳細なレベルで個人情報のフローを記述することが可能である。このフローは、プロセス記述を描いたダイアグラムや個人情報項目を含む付録において記載されるかもしれない。
- 潜在的なプライバシー・イシューやリスクに対するイニシャル・アセスメント（プライバシーに対する明確・直接的な影響や、長期的・二次的な影響を含む）。
    - 当該文書が準備される時点で当該組織に認識されるべきもの。
- 当該組織が特定したオプションや対案に関する簡潔な記述（既に却下されたり、検討中であるようなオプションを含む）。
- プライバシーに対して潜在的な影響に与える特徴（機能）についての正当化を説明する投資対効果検討書（business case）。
    - 当該スキームの主要な特徴（機能）がいかに目標を達成するかに関す

る説明。

- 費用対効果の分析。

・ プロジェクト計画全体の記述、計画全体の中での PIA プロセス、PIA プロセスの中でのコンサルテーションプロセス。
・ 関係する組織やステークホルダー、PIA に貢献するために招待された代表者や擁護者のリスト。
・ プロジェクトおよびその潜在的なプライバシー影響を理解するために有益な添付書類。

また、後のフェーズで効果的なコンサルテーションプロセスを実施するために、技術的文書やブリーフィング、デモを準備する必要があるかもしれない。こうしたものが必要になる技術の例としては以下がある。

- 接触型 IC カード
- 非接触型 IC カード、RFID タグ
- アイデンティティマネジメント
- サービスや認証のためのポータル
- データウェアハウス、データマイニング
- 位置特定技術
- バイオメトリクス　など

②準備フェーズ（Preparation Phase）

このフェーズの目的は、重要な③フェーズがスムーズに進行するように必要なアレンジメントを行うことである。成果物は、ステークホルダー分析、コンサルテーション戦略・計画、PIA 諮問グループの設立である。

準備フェーズのタスクとして、以下のものが挙げられている。

・ ステークホルダーとの議論が効果的になるように、コンサルテーション計画を作成する。
・ PIA 諮問グループ（PCG）を組織する。PCG は、ステークホルダー・グループの代表者から成る。
・ プロジェクト背景ペーパーを PCG に配布する。このことは、PCG のメンバーが PIA の提案の内容を理解できることを保証する。

<u>コンサルテーション計画の作成</u>

フルスケールの PIA を必要とするような複雑で潜在的にプライバシーの脅威となるプロジェクトは、多くの組織や人々に影響を及ぼしがちである。コンサルテーションと分析フェーズの実施を保証するため、適切なコンサルテーション計画を立てることは有用である。

コンサルテーションはプロジェクトのスケールやスコープ、性格にふさわしいものであるべきである。重大なプライバシーリスクを伴った大規模なプロジェクトでは、以下に記述するような手段のほとんど全てを利用するかもしれない。小規模なプロジェクトでは、これら全てを利用する必要はないかもしれない。いくつかの組織は、よく練られたコンサルテーション戦略を既に準備しているかもしれないし、こうした戦略内で PIA コンサルテーションが完遂できない理由はない。コンサルテーション戦略を持たない組織については、以下のアドバイスが参考になる。

効果的なコンサルテーションは、プロジェクトに関わる全てのステークホルダーが十分に情報を与えられ、彼らの視点や懸念を伝える機会があり、彼らの視点が設計に反映されているという信頼感を築けることに依存する。

コンサルテーションプロセスによってプロジェクトと設計に変更点が生ずることは、通常のことである。最小限のコストでリスクマネジメントに最大限の効果を挙げるためには、コンサルテーションは早期に開始し、プロジェクトのライフサイクルを通じて継続する必要がある。

効果的なコンサルテーションを保証する有益な手段には、以下のものがある。

- プロジェクトに関するいくつかの情報を提供することによる、議論の呼び水。
- PIA プロセスを通じてコンサルテーション相手との進行形の対話を行うこと。
- 技術やシステム、プライバシー影響に関する適切なバックグラウンドを持った代表者や擁護者、ステークホルダー・グループを参加させること。
- 参加者の間のインタラクションを促進すること。
- 全ての関連する視点が提示され、全ての関連する情報が収集されるように、コンサルテーションを行うグループや個人に十分な多様性を持たせること。
- 各グループが情報やコメントを提供する機会を与えられていること。必要あれば、複数回のコンサルテーション・ラウンドを行うこと。
- コンサルテーション手段が、コンサルテーションを行う当該グループに適合したものであること。例えば、公式な書面によるコンサルテーションの代替として、またはそれに加えて、ワークショップやフォーカスグループを利用すること。
- 全ての組織や個人から提供された情報が、設計や実装のフェーズにフィードバックされるようにすること。
- コンサルテーションプロセスの間に生じた視点や不安、イシューが、PIA プロセスの成果に反映されるようにすること。
- アイデアの効果的な交換を可能とするようなコミュニケーションプロセスを工夫すること。このことは、ワークショップや会合などを含む。

セキュリティ上の配慮や他のプライバシー懸念によってコンサルテーションプロセスをオープンに行うことができない場合には、以下が推奨される。

- PIA は可能な限りオープンに実施する。

- セキュリティ上の懸念がある部分については、機密の別冊として分離したり、クローズな議論のセッションとして分離したりする。
- セキュリティ上の配慮によって情報が開示されない場合には、可能な限り効果的で信用できる近似の手段を工夫する。例えば、セキュリティ・センシティブな情報は信頼された第三者に提供され、当該第三者は PCG のメンバーに評価のコメントを提示するなど。

③コンサルテーションと分析フェーズ

ステークホルダーとのコンサルテーション、リスク分析、問題の特定、解決策（solutions）の検討を含むフェーズである。このフェーズの目的は、問題を早期に特定すること、効果的な解決策を見出すこと、設計にこれらの解決策を組み込むことを保証することである。成果物は、プロジェクト関連文書の変更、「イシュー登録リスト」、「プライバシー設計機能ペーパー」である。

コンサルテーションと分析フェーズのタスクとして、以下のものが挙げられている。

- ②のフェーズで作成されたコンサルテーション計画を実施する。
- プロジェクトにおける設計上のイシューとプライバシー問題とを特定する。
- 設計の選択肢を再検討する。このことは、問題を解決するために利用可能な様々なアプローチに焦点を当てる。
- 問題と解決策とを、「イシュー登録リスト」として文書化する。大きなプロジェクトには、PIA が段階的に実施されると、企業の記憶が徐々に失われていくリスクがある。この問題は、プライバシー諮問グループ（PCG）が利用可能なプロジェクト背景ペーパーの全ての版において「イシュー登録リスト」を付録として付けることで対処することができる。「イシュー登録リスト」は、直接的に対処できないイシューを記載したり、看過される可能性を避けたりする手段としての役割も果たす。
- 到達した結論を「イシュー登録リスト」および／または「プライバシー設計機能ペーパー」に反映させる。「プライバシー設計機能ペーパー」は、以下を文書化したものである。
    - 特定されたイシュー
    - 検討された回避対策と軽減対策（却下されたもの、採用されたもの）
    - 結果として実施された設計の変更点
    - 特筆すべきイシュー
- 「プライバシー設計機能ペーパー」を、PCG とプロジェクトチームに提出する。
- プロジェクトチームからのフィードバックを、PCG に提出する。
- PCG と更なるコンサルテーションを実施する。
- プライバシー設計機能に関する決定を、設計に組み込む。
- 未解決のイシューがあれば、コンサルテーションと分析を継続する。

このフェーズは通常、何回も繰り返される。最も効果的なアプローチは、プロジェクトの開始段階でこのフェーズを実施し、プロジェクトの後のフェーズ（例えば、新たなシステムの要求分析、論理設計、物理設計、開発、インテグレーション、実装）に対応したリハーサルを準備してしまうことである。

プロジェクト背景ペーパーは、プロジェクトを通じた発展を反映させるために段階的に変更する必要があるだろう。PIA によって、プライバシー侵害を軽減したり回避したりするために設計が変更されることは通常のことである。遅い時点での変更は当然、コストが高くつく。そのため、早い時点での PIA の実施が必要である。

プライバシー解決策の特定

特定したプライバシーリスク（イシューやプライバシー問題）に対して、どのような解決策を実施するかを検討する必要がある。取りうる解決策は、以下の 3 つに分類できる。

- (a)リスク、影響、不利益を受容する。
- (b)リスクを回避する方法を特定する。
- (c)リスクを軽減する方法を特定する。

(a)は、リスクが実現する可能性が極めて低いか、実現した際の影響が極めて少ない場合に取りうる選択肢であるが、あくまでもオプショナルな選択肢だと考えるべきである。この選択肢を取る場合には、リスクを受容することの理由付けを明確化する必要がある。

(b)のプライバシー影響回避策（privacy impact avoidance measures）の例としては、以下の解決策が挙げられている。

- 個人情報の収集を必要最低限のものに抑える。
- 賛否両論のあるようなデータ項目を収集しない。
- 意思決定において特定の情報の利用を取り止める（ex.就職活動時の履歴書における民族欄の削除）。
- 個人の身体的自己を侵害するという論議を避けるために、生体情報は採用しない。

(c)プライバシー影響軽減策（privacy impact mitigation/reduction measures）の例としては、以下の解決策が挙げられている。

- 個人情報を記録しないことで、その保持を最低限に抑える。
- 個人情報が必要なトランザクションが完了したら、速やかにそれを消去する。
- 個人情報の消去スケジュールを定め、そのスケジュールを監査できるようにする。
- 特定の目的で取得した個人情報の利用を、強力な法的・組織的・技術的安全手段によって制限する（目的外利用を防ぐ）：苦情処理システムの設計・導入・運用、厳格な罰則と執行能力による担保など。

④文書化フェーズ

PIA は 1 つのプロセスである。組織が PIA を実施するベネフィットは、一部はステークホルダーによる、一部は当該組織やプロジェクトチームによる学習や適応という形で、主にプロセスの中から生じてくる。しかし、PIA プロセスの目標に向けた最終文書を作成することにはメリットがある。

文書化フェーズの目的は、PIA プロセスとその成果を文書化することである。成果物は、PIA 報告書である。

文書化フェーズのタスクとして、以下のものが挙げられている。

- 「イシュー登録リスト」および／または「プライバシー設計機能ペーパー」の最終版において、回避対策と軽減対策についての意思決定を確定する。
- PIA 報告書を作成する。
- PIA 報告書を PCG に提供する。
- PIA 報告書を公表する。（セキュリティ・センシティブな情報は差し引いて。）

PIA 報告書を準備する理由は、以下のものである。

- 説明責任の 1 要素として、PIA プロセスが適切に実施されたことを示す。
- 実施後のレビューの基盤を提供する。
- 監査の基盤を提供する。
- 元のスタッフが異動した場合、新たな PIA の実施の際に、プロジェクトを通じて得られた経験が利用可能となるように、「企業の記憶」を提供する。
- プロジェクトを通じて得られた経験が、将来の PIA チームや組織外の他の人々に共有されるようにする。

PIA 報告書に含めるべき主要な内容は、以下のものである。

- プロジェクトの記述
- プライバシー・イシューの分析
- プライバシー侵害やプライバシーへの影響を正当化する投資対効果検討書（business case）
- 検討された代替案と決定に至った合理的理由
- プライバシー侵害を軽減したり回避したりするために採用されたプライバシー設計機能の記述と、これらのプライバシー設計機能の影響
- 当該スキームやその活用に対する国民の受容性の分析

PIA 報告書にはその他、以下の内容も含めてよいかもしれない。

- 実施されたコンサルテーションプロセスの概要
- コンサルテーションを実施した組織や個人の連絡先

- コンサルテーションを実施した相手に提示したプロジェクト背景ペーパー
- PIA プロジェクト計画
- 「イシュー登録リスト」および／または「プライバシー設計機能ペーパー」
- 関連法令や規約、ガイドラインの参照

後の段階で、法令コンプライアンスがチェックされた後には、PIA 報告書の付録に以下のものを追加することが適切であるかもしれない。

- プライバシー法令コンプライアンス検討
- データ保護法コンプライアンス検討

PIA 報告書は公表されること、さもなくば少なくとも広範に配布されることを予期して作成されるべきである。その場合、PIA 報告書は上記に挙げた機能を果たすことができる。すなわち、説明責任、実施後のレビュー、監査、将来の PIA 実施へのインプット、将来に PIA を実施する人々のための背景情報としての機能である。

PIA プロセスを通じて得られた情報のいくつかは、セキュリティ・センシティブもしくは商業的にセンシティブなものである可能性がある。そのような場合には、詳細情報を機密もしくはクローズな別冊の形にすることが適切であるかもしれない。そのような情報の非開示は、そのことが正当化される場合に限定される必要がある。議論とアセスメントが完全で、情報豊かで、理解できるものであることを保証するために、PIA 報告書には十分な情報が含まれている必要がある。

⑤レビューと監査フェーズ

このフェーズの目的は、コンサルテーションと分析フェーズで達成された成果が、システムの運用またはプロジェクトの実施に反映されていることを保証することである。

レビューと監査フェーズのタスクとして、以下のものが挙げられている。

- 「イシュー登録リスト」および／または「プライバシー設計機能ペーパー」に文書化された軽減対策や回避対策の実装に関するレビューを実施する。
- プライバシーレビューレポートを作成する。
- プライバシーレビューレポートを PCG に提出する。
- プライバシーレビューレポートを国民が利用できるようにする。

他のフェーズと同様、プロジェクト全体のライフサイクルの中の適切な段階でこのフェーズを実施することはベネフィットがある。例えば、詳細設計のレビューのようなマイルストーンで実施することがありうる。

組織の標準や、定期的・抜き打ち的内部監査や、外部監査プロセスにレビューを組み込むことの適切性や費用効率性を検討するアプローチも可能かもしれない。

（３）法令コンプライアンス・チェック

本プロセスでは、プライバシー関連法令へのコンプライアンス・チェックとデータ保護法へのコンプライアンス・チェックを実施する。詳細は割愛する。

５．５．３　イニシャル・アセスメントのスクリーニング質問表

ICO の規定する PIA のプロセスでは、イニシャル・アセスメントにおけるスクリーニングが、PIA を実施するか否かを決定する上で重要な位置を占めている。

以下は、フルスケール版のスクリーニング質問表の抄訳（弊社訳）である。PIA の実施企業は、この 11 の質問への回答を全体的に判断して、フルスケール版の PIA を実施するか否かを決定する。

○プロジェクトの主要な特徴に関する 11 の質問（フルスケール版 PIA 用）

技術

（１）プロジェクトは、プライバシー侵害に実質的な可能性を持つ新たなもしくは追加的な情報技術を利用しているか？

- 例えば、（これらに限定されないが）IC カード、RFID タグ、バイオメトリクス、位置情報技術（携帯電話の位置、GPS アプリケーション、ITS など）、視覚監視、デジタル画像・ビデオ記録、プロファイリング、データマイニング、電子トラフィックの記録など。

アイデンティティ

（２）プロジェクトは、新たな識別子、既存の識別子の再利用、侵害的な識別（身元確認）・アイデンティティ認証・アイデンティティマネジメントのプロセスを含むものか？

- 例えば、デジタル署名、多目的の識別子、登録手続きの一環としての窓口来所と身分証明書の提示、バイオメトリクスのような侵害的な識別子など。こうした特徴を持ったスキームは、プライバシーへの影響にかなりの可能性を持ち、国民の懸念や、ひいてはプロジェクトにとってのリスクを引き起こす。

（３）プロジェクトは、匿名性や偽名性を否定したり、従来は匿名・偽名で実施可能だったトランザクションを本人を特定するトランザクションに変更したりするものであるか？

- 多くの行政機能は、市民のアイデンティティにアクセスすることなく効果的に実行することができない反面、アイデンティティを必要としないようなものも存在する。プライバシー保護の重要な側面は、自分のアイデンティティを告げることなく組織とやり取りをする権利を維持することである。

複数の組織

（4）プロジェクトは、政府機関か民間企業かに関わらず、複数の組織を巻き込むものであるか？

- こういった性質のスキームは、個人データ「サイロ」やアイデンティティ「サイロ」の「破壊」を伴う。そして、いかにデータ保護法制を遵守するかについての疑問を生じさせる可能性がある。この「破壊」は、詐欺の検知や防止にとって、また一定のケースでは業務プロセスの効率化にとって望ましいかもしれない。しかし、データ「サイロ」やアイデンティティ「サイロ」は昔から続くものであり、多くのケースにおいて効果的なプライバシー保護を提供している。それゆえ、複数の組織を巻き込むようなプロジェクトにおけるプライバシーの侵害を正当化するような投資対効果検討書を準備することに関連して、特定のケアが必要とされる。それを補償するような保護措置が検討されるべきである。

データ

（5）プロジェクトは、個人に特定の不安を与えるような個人データの新たな取扱いや、取扱いに関する重大な変更を伴うものであるか？

- データ保護法の第 2 条では、特別なケアが必要となる「センシティブな個人データ」のカテゴリーを特定している。これらには、人種や民族、政治的見解、宗教的信仰、労働組合への加入、医療状態、性生活、犯罪、法廷手続きが含まれる。
- 個人データの、不安を与えるようなその他のカテゴリーには、金融データ、税弱な個人に関する特定のデータ、ID 窃盗を可能とするようなデータが含まれる。
- さらなる例には、特定の環境において適用される。ある少数の個人に関する住所や電話番号は、少なくとも彼らの生活の特定の期間については、伏せられる必要がある。なぜなら、このような「リスク状態にある個人」は、発見された場合に物理的な危害を被る恐れがあるからである。

（6）プロジェクトは、データベース内にある各個人に関する個人データのかなりの量について新たな取扱いや、取扱いに関する重大な変更を伴うものであるか？

- 例えば、プロファイルに基づく、福祉、医療、消費者信用、消費者マーケティングのような大量のデータ処理など。

（7）プロジェクトは、大量の数の個人に関する個人データの新たな取扱いや、取扱いに関する重大な変更を伴うものであるか？

- この手の類のデータ処理は、個人の居場所を特定しようとしたり、個人のプロファイルを構築したり、それらを更新しようとする組織や個人にとって魅力的である。

（8）プロジェクトは、複数のソースからの個人データの新たな連結や相互リンク（紐付け）、相互参照、マッチング、あるいはそれらの重大な変更を伴うものであるか？

- このことはとりわけ重要な要因である。イシューは、データの品質や、表面的には類似したデータ項目の多様な意味や、非常に短い期間を超えたデータの保持に関連して発生する。

適用除外と例外

（9）プロジェクトは、法令上のプライバシー保護の適用除外となるような仕方で、データ処理を行うか？

- 例えば、一部のまたは全てのプライバシー保護が法令上の適用除外または例外によって無効となるような、法執行機関の情報システムやナショナルセキュリティ情報システム、その他のスキームなど。

（１０）プロジェクトの正当化（理由）には、公共のセキュリティ安全保護対策における重要な寄与を含むものであるか？

- 重要なインフラストラクチャや人々の物理的な安全に対する不安に対処するような対策は、通常、プライバシーに対する重大な影響を持つ。近年ではプライバシーに重みが与えられない傾向がある。このことはプライバシー上の利益との緊張関係を生み出し、当該プログラムやスキームに対する国民の反対や不採用のリスクを生み出す。

（１１）プロジェクトは、相当のプライバシー法制の影響下にない第三者への個人データのシステマティックな提供や、それらの第三者によるアクセスを伴うものであるか？

- 提供は、販売や交換、ハードコピーや電子アクセス可能な形態における保護されていない公開、契約事業者へのデータ処理のアウトソーシングなどを通じて発生する。
- 第三者は、データ保護法の条項や他の関連する法令条項の影響下にないがために、適切なプライバシー法制の影響下にないかもしれない。例えば、第三者が外国の法制化にある場合である。英国内の組織であっても、それが英国外に本社を持つ組織の子会社であるような場合には、不安が発生するかもしれない。

以下は、スクリーニング質問票を用いた分析に関する追加のガイダンスである。

早期に事実に直面すること

上記で言及したような主要な特徴は、プロジェクトの重大なリスク要因を代表するものであり、これらの重大性は軽く扱われるべきではない。問題に対処するのが遅くなればなるほど、それらに対処するためのコストは高くなることを忘れるべきではない。

検討するための視点

様々なステークホルダーのグループがこれらの要因に関して異なる視点を持つことを評価することは重要である。もし分析が組織自体の視点のみから実施されてしまうと、リスクが見過ごされる可能性が高い。それゆえ、各質問への回答において、ステークホルダーの視点も考慮に入れられていることを推奨する。

プロジェクトによって影響を受ける個人の観点からは、単なる市民や住民一般、もしくは人口全体のものよりも、焦点をより正確に絞る必要がある。プロジェクトに興味のある、もしくは影響を受ける国民の様々なセグメントの完全な理解を保証するためには、準備フェーズの一環で実施されるステークホルダー分析をリファインする必要がある。例えば、遠隔地に居住する人々や、教育的に不利な人々、移動労働者、第一言語が英語でない人々、民族的・宗教的マイノリティーなどに対しては、しばしば異なる影響が存在する。

クライテリアの提供

11 の質問に個別に回答した後、フルスケール版の PIA が必要が否かの結論に到達するために、回答は全体として検討される必要がある。もし必要であれば、PIA のスコープが広範なものであるかそれともプロジェクトの特定の側面のみに焦点を当てたものであるかを決定する必要がある。

５．６　PIA 実施プロジェクトの例

５．６．１　スコットランド国民資格カード（NEC）

（１）国民資格カードの概要

スコットランド国民資格カード（National Entitlement Card: NEC）は、スコットランド政府、スコットランド各地方政府（32 の県）、公共サービス提供者等の共同プロジェクトである。行政が発行する様々なカードを 1 枚に統合し、市民が資格を持つサービスに 1 枚のカードで容易にアクセスできるようにすることを目的としている。

2006 年に開始し、2011 年 3 月現在 160 万人が利用している。国民資格カードの利用は希望者制（任意）である。なお、スコットランドの人口は 509 万人であるので、利用率は約 31% である。

国民資格カード配布による調達コスト削減額は、400 万ポンド（約 5.3 億円）とのことである。

なお、国民資格カードプロジェクトは「カスタマーファースト（CF）」プログラムの一環である。この CF プログラムは、スコットランド政府が支援する総額 3450 万ポンドのプログラムである。同プログラムは、以下のことを目的としている。

- より便利でニーズに応えた公共サービスの提供
- サービスへのオンラインアクセス
- 少なくとも 75%の主要なサービスリクエストを、1 つのコンタクトポイントで対処できるようにする

（２）券面記載情報と IC チップ格納情報

国民資格カードは、RFID の入った非接触 IC カードである。券面記載情報と IC チップ格納情報は以下の通りである。

券面記載情報

- 氏名
- 生年月日
- 写真
- NEC 番号[83]
- 有効期限
- PASS ホログラム
- ITSO[84]や OneScotland[85]、地方政府（県）のロゴ

[83] NEC 番号は 16 桁の番号である。初めの 6 桁は当該カードを発行した県の番号、次の 8 桁は個人に対する番号（番号に生年月日等の意味はない）、最後の 2 桁は何回目に発行を受けたカードかを示す。NEC 番号を図書館や交通機関など、公共サービス提供者側で保存することはない。あくまで市民アカウントシステム（CMS）における管理上の番号として付いている。券面に記載する必然性はないが、見た目が良いように載せているとのことである。

・特定サービスの資格を示すロゴ（SPT[86]、交通、Young Scot[87]、sQuid[88]など）

図 18　スコットランド国民資格カード（NEC）

IC チップ格納情報

・ITSO 用のセクション（乗車券情報）
・割引乗車券情報
・民間の乗車券情報
・氏名・住所・生年月日・性別等
・図書館会員番号、スポーツジム会員番号等

（３）国民資格カードで利用できるサービス

以下は提供サービスの例である。

- 公共交通機関の割引乗車（子ども、高齢者、障害者）
- 図書館やレジャー施設の会員カード
- 商店での割引
- 学校飲食施設での支払い[89]

---

84 統合交通 IC カード機構（Integrated Transport Smartcard Organisation）。ITSO は、政府支援を受けた英国の非営利団体であり、英国におけるスマート発券のための技術仕様を開発している。
85 スコットランド政府のアクセシビリティに関するブランド。
86 Strathclyde Partnership for Transport（ストラスクライド県交通連盟）。スコットランド西部のストラスクライド県における地域的な交通連盟。
87 11 歳から 26 歳の全てのスコットランド市民が対象。交通機関や店舗等で各種の割引を受けられる。
88 電子マネーのサービス。
89 学校の飲食施設では、生徒がお金を払う場合と、払わない場合（フリーミール）とがあ

・ sQuid（電子マネー） など

サービス提供者によるカード読取

サービス提供者によるカード読取は、バスのカードリーダによる読取、図書館内のカードリーダによる読取等の場合がある。プライバシー保護対策として、サービス提供者は、チップ内の自分のセクションにしかアクセスできない。カードリーダ側から相互認証のためのユニークコードの提示が必要となる。例えば、バスの運用者はチップ内の図書館セクションにアクセスすることはできない。

プライバシー上の課題

市民が資格を持つサービスに容易にアクセスできるように個人情報を有効活用することと、個人情報のプライバシーを保護することのバランスを確保することが課題であるという。具体的には、1 枚のカードを多目的利用するために、市民から取得した個人情報を他の地方政府や公共サービス提供者に提供することのバランスが必要となる。

また、本人同意も重要な要素である。PIA は市民からの信頼を築く上で重要な手段であるという。

（4）国民資格カードの運用

国民資格カードおよび後述の市民アカウントシステムは、スコットランド政府等の各種資料より、図 19 のようなスキームで運用されていると考えられる。

る。低所得世帯の場合は、お金を払わない。国民資格カードは、学校がいくらスコットランド政府からお金をもらえばいいかの計算に使われる。従来はフリーミールの場合、レジでお金を払わないので低所得世帯だと分かってしまったが、国民資格カードでは全員が同じように使用するので、フリーミールかどうか分からないという利点がある。

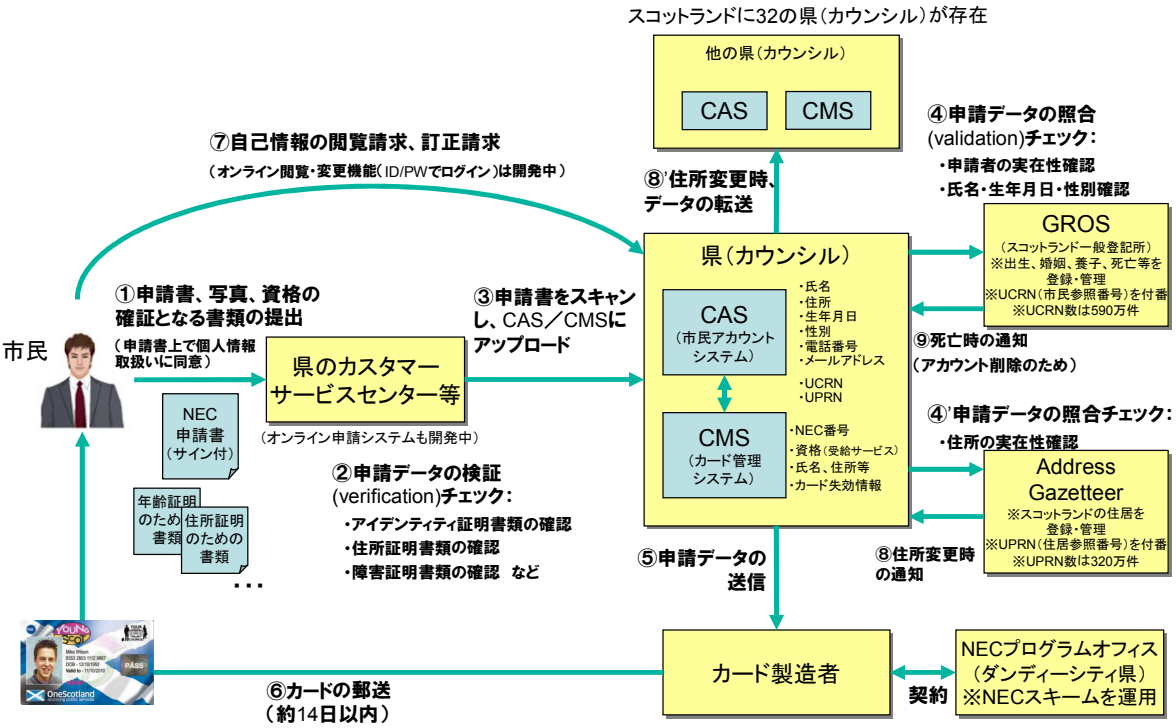


図 19　スコットランド国民資格カード（NEC）の運用

①スコットランド市民は、申請書（本人のサイン付き）、写真、資格の確証となる書類（年齢証明のための書類、住所証明のための書類、障害証明のための書類等）を、居住する地方政府（県）のカスタマーサービスセンター等に提出する。市民は申請書上で、個人情報取扱方針に同意する。

②地方政府（県）のカスタマーサービスセンター等は、申請されたデータの検証（verification）チェックを行う。具体的には、アイデンティティ証明書類の確認、住所証明書類の確認、障害証明書類の確認等を行う。

③地方政府（県）のカスタマーサービスセンター等は、申請書をスキャンし、地方政府（県）で管理する市民アカウントシステム（CAS）／カード管理システム（CMS）[90]にアップロードする。

④申請データが CAS／CMS に登録されるにあたって、申請データの照合(validation)チェックが行われる。具体的には、GROS（スコットランド一般登記所）[91]に対して、申請者の実在性確認と、氏名・生年月日・性別の照合を行う。また、Address Gazetteer[92]に対して、住所の実在性確認を行う。

---

90 CMS には、NEC 番号、国民資格カードの資格（受給できるサービス。例えば、交通チケットの割引、図書館会員番号など）、氏名、住所、カード失効情報等が登録されている。
91 スコットランドにおいて出生、婚姻、養子、死亡等を登録・管理する役所。
92 スコットランドにおいて住居を登録・管理する役所。下記の UPRN（住居参照番号）を付番する。

⑤地方政府（県）は、カード製造者に申請データを送信する。
⑥カード製造者は、約 14 日以内に、市民にカードを郵送する。
⑦市民は、地方政府（県）に対して、自己情報の閲覧請求や訂正請求を行うことができる。
（オンライン閲覧・変更機能（ID/PW でログイン）は開発中である。）
⑧住所変更時は、Address Gazetteer から地方政府（県）に通知がなされ、CAS や CMS のデータが変更される。また、他の県に引越す場合には、転出元の地方政府（県）から転入先の地方政府（県）にデータが転送される。
⑨死亡時は、GROS から地方政府（県）に通知がなされ、アカウントが削除される。

（５）市民アカウントシステム（CAS）

市民アカウントシステム（Citizen Account System：CAS）とは、市民とスコットランド政府・地方政府（県）が連絡を取り合う際のコンタクトポイントである。CAS への登録は希望者制であるが、上記の国民資格カードを発行する際には、CAS への登録も必要となる。

CAS への登録に際しては、市民は「氏名」「住所」「生年月日」「性別」「電話番号」「メールアドレス」「UCRN（Unique Citizen Reference Number：市民参照番号）[93]」「UPRN（Unique Property Reference Number：住居参照番号）[94]」等を登録する。申請は、オンラインもしくは対面で申請が可能である。

- オンラインでの申請は、市民が提示した個人データと行政側で保持するデータとの照合によって本人確認が行われ、レベル 1 のアカウントを取得することができる。
- 対面での申請は、住所およびアイデンティティの証明（本人確認）によって行われ、レベル 2 のアカウントを取得できる。

[93] UCRN は個人に割り当てられた 18 桁の番号であり、生年月日等の意味のある情報は入っていない。出生番号を一定のアルゴリズムで変換して作成する。生涯不変の番号であり、通常は出生時に割り当てられる。出生番号はセンシティブなので、これから生成した UCRN を使っている。スコットランド一般登記所（GROS：General Register Office for Scotland）が出生時に UCRN を付番し、維持している。スコットランドに移住した住民については、住民が NHS（国民保健サービス）に登録することによって、GROS が UCRN を付番してくれる。UCRN の件数は 590 万件。GROS では、出生・婚姻・養子・死亡時などに登録を行っており、10 年に 1 回の国勢調査も実施する。

[94] UPRN は住所の確認に用いる番号である。スコットランドでは Address Gazetteer において住居の DB が管理されており、住居 1 つ 1 つに番号が付いている。UPRN の件数は 320 万件である。

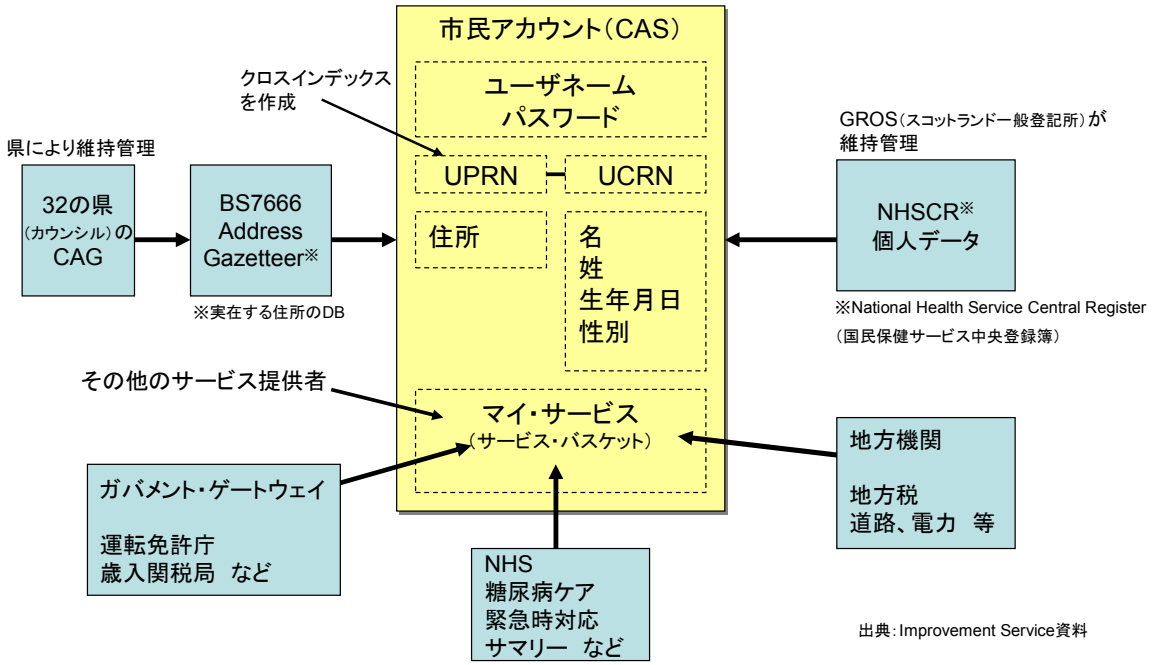


図 20　スコットランドの市民アカウントシステム（CAS）

（６）市民アカウントシステム（CAS）で利用できるサービス

登録内容の変更通知

CAS を利用して、登録内容の変更通知を一括で行うことができる。例えば住所変更時、市民は CAS に届け出れば、接続する全ての公共サービス提供者に対して住所変更の通知が転送される。

なお、オンラインでの届出機能は開発中である。

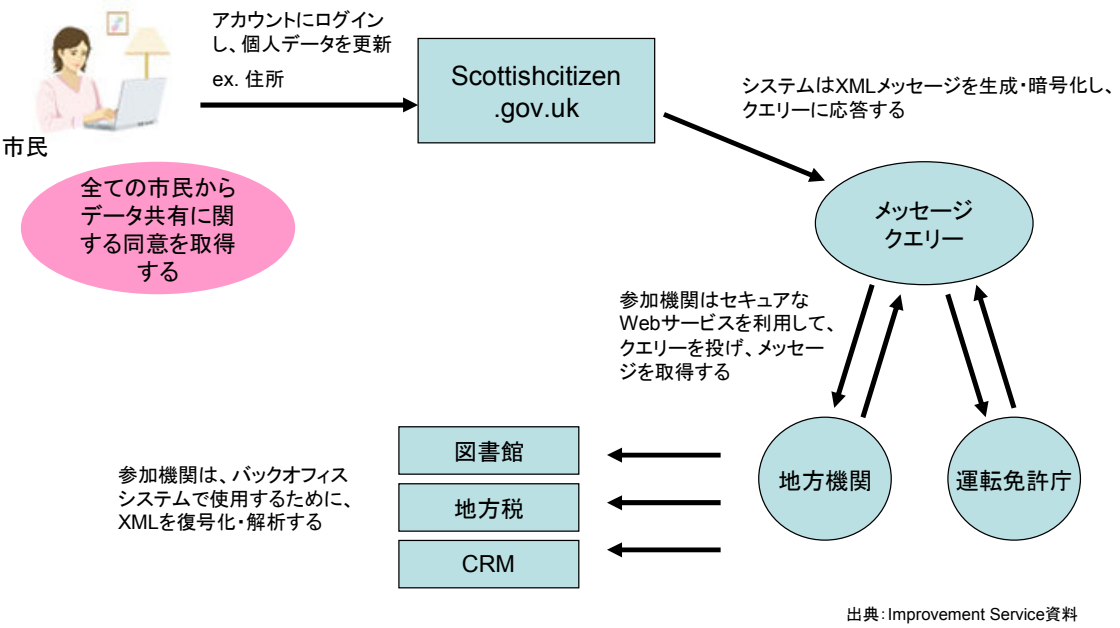


図 21　市民アカウントシステムを用いた登録内容の変更通知

ログイン認証（シングルサインオン）

CAS のサイトからサービス提供者のサイトへのシングルサインオン機能もある。CAS の「マイ・サービス機能（サービス・バスケット）」から各サービス提供者へのリンクが張られている。各サービス提供者は、どのオンラインサービスがどのレベルの認証を必要とするかを特定する必要がある。

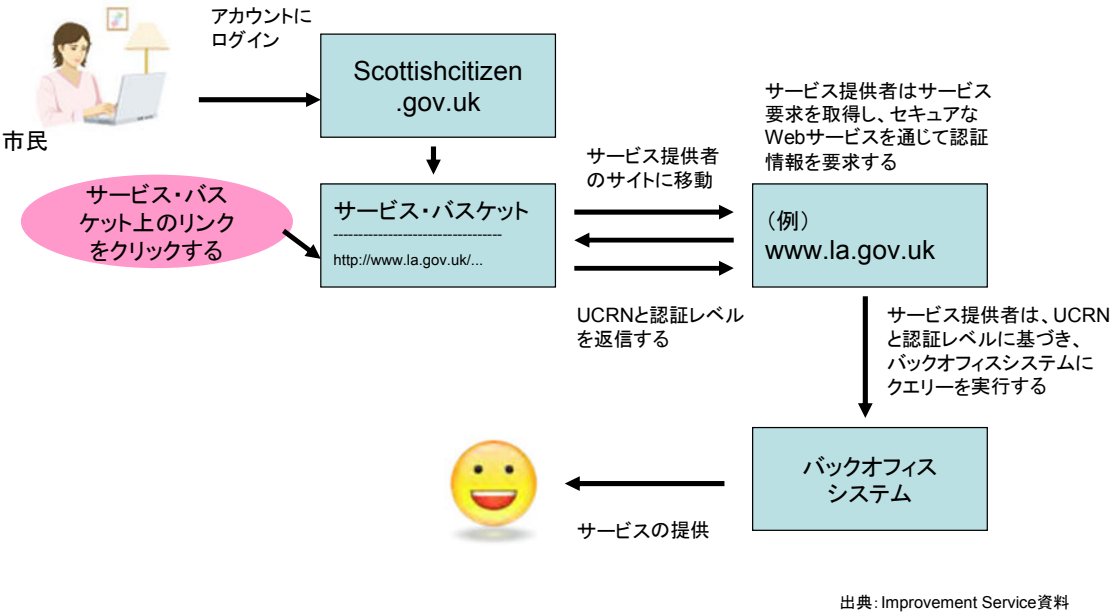


図 22　市民アカウントシステムを用いたログイン認証（シングルサインオン）

（7）国民資格カード／CAS の PIA

コンサルテーション・フェーズ

コンサルテーション・フェーズの対象者は、システム利用者（スコットランド政府・地方政府職員、公共サービス提供者の職員）と一般市民であった。

市民へのコンサルテーションは、市民パネルに対して実施し、「国民資格カード／CAS の導入によってどのような問題が懸念されるか？」「そのような懸念に対して、どのように対処したらよいか？」ということに対する意見を求めた。市民からの代表的意見としては、以下のようなものが挙げられた。

「国民資格カード管理システムや CAS に市民の情報が集積され過ぎるのではないか（政府がビッグブラザーになるのではないか)」

「英国政府（特に ID カードシステム）と個人情報が共有されるのではないか」

「カードのチップに個人情報を入れ過ぎるのはないか」

実施体制・期間・コスト

PIA チームは 1 名であり、セキュリティ会社に委託した。スコットランド政府国民資格カード担当者が PIA チームの監督を行った。

約 6 ヶ月で PIA 報告書ドラフトを作成し、スコットランド政府国民資格カード担当者が査閲・修正した。修正した報告書をシステム利用者（職員等）に提示し、フィードバックを受けた。正式な PIA 報告書発行に至るまでの PIA 実施期間は 1 年間程度だが、上記のスコットランド政府国民資格カード担当者の多忙による遅延があった。

PIA 実施コストはスコットランド政府が負担した。

PIA 実施後にシステムに加えた機能等

CAS において、オンラインで住所変更を行った場合、変更情報はすぐに反映されずに、電話等での確認を行うようにした。これは、他人のなりすましによる虚偽の情報変更や、本人の虚偽の申請による税金逃れ等を防止するためである。

コンサルテーション・フェーズで挙げられたその他のリスクに対しては、国民資格カード／CAS のシステムの中に既に反映済みであった。

PIA 報告書において市民にアピールしたこと

スコットランド政府国民資格カード担当者によると、PIA 報告書において読者である市民にアピールしたことは、以下の内容である。

- 国民資格カードは（廃止になった）英国の ID カードとは別スキームであり、情報が共有されることもない。
- 国民資格カード／CAS において市民の情報（特にカード利用履歴）を一元管理するこ

とはない。また、市民から取得する情報は、サービス提供に必要最小限なものである。
・ 国民資格カード／CAS の利用は任意であり、公共サービス提供者への情報提供については必ず事前に本人の同意を取得する。

また、報告書作成時の苦労としては「PIA 報告書を一般市民に読んでもらえるように極力簡潔なものとした」ことだという。

PIA 報告書の構成

スコットランド国民資格カード／CAS の PIA 報告書[95]は、以下のような構成となっている。

・ イントロ： PIA レポートの目的、位置づけ
・ 概要： PIA レポートのサマリー
・ NEC スキーム： 国民資格カードの目的、ステークホルダー
・ NEC スキームの運用： 国民資格カードの運用主体等
・ データ保護／データ管理者： データ保護 WG、参照ガイドライン、データ管理者の責務、本人同意の取得
・ データ処理／データ保有： 国民資格カードの申請手続き、紛失・盗難手続き、システム保有情報
・ NEC に保存される情報： カード券面情報、チップ格納情報、セキュリティ対策
・ その他の保存情報： 資格確証文書の保存等
・ データへのアクセス： システム保有情報やカードチップ格納情報へのアクセス権限
・ データ保持と廃棄： データの保存期間等
・ 結論
・ 付録（FAQ の要約）

５．６．２ 警察全国データベース

警察全国データベース（Police National Database : PND）とは、イングランドとウェールズの 43 の警察機関でローカルに管理されている情報へのリンクを提供する DB のことである。

PIA 実施概要、教訓等

95 Improvement Service, “National Entitlement Card (NEC) Privacy Impact Assessment Report”,（2011 年 1 月）（http://www.entitlementcard.org.uk/docs/PIAJan2011.pdf）。

2008 年 2 月にイニシャル・アセスメント（スクリーニング）を行い、フルスケール版 PIA を実施するという決定をした。2008 年 4 月まで、コンサルテーションとして、関連機関・団体に対して文書による照会を行った。本 PIA の特徴的なプロセスとしては、分析フェーズ後に、報告書ドラフトを用いて再度、関係機関・団体に対するコンサルテーションを実施した。2009 年 4 月に PIA 報告書[96]を公表した。

PIA 実施後にシステムに加えた機能や運用

PIA 実施の結果として、当該システムに加えた機能や運用は、以下のようなものである。

- アクセス者の限定とトレーニング
- 職務に必要なデータや機能のみにアクセス可能とすること（アクセスコントロール）
- 利用ログの保存と監査
- プライバシー要件（プライバシー原則）を考慮した機能設計
  ex. PND から警察機関へのデータ移転に対する一定の制限や安全保護措置　等
- システムおよびデータ利用規則の策定

５．７　英国におけるその他の個人情報保護関連の動向

（１）BS10012

英国規格協会（BSI）は、2009 年に「BS 10012:2009 データ保護。個人情報マネジメントシステムのための仕様[97]」を開発した。個人情報マネジメントのための最初の仕様であり、英国の 1998 年データ保護法への遵守をサポートし、ベストプラクティスを確立するために開発された。背景には、上記の歳入関税局での 2500 万人分のデータ入り CD-R 紛失事件など、官民における漏えい事件が相次いだことがある。

BS 10012 は、組織における個人情報マネジメントシステム（PIMS）に対する要求事項を特定している。PIMS は、とりわけ、1998 年データ保護法への遵守を維持し、改善するための基盤を提供するものである。BS 10012 は、いかに運用を行うべきかを正確に記述するものではなく、むしろ個人情報を効率的にマネジメントすることを可能にするフレームワークを提供する。同基準は、行政および民間分野のあらゆる規模の組織が、教育や意識向上、リスクアセスメント、データ共有、データの保有と廃棄、第三者提供等における手続きを含むカスタマイズされたマネジメントシステムを構築するために利用できる。BS 10012 は、個人情報のマネジメントに信頼性を提供したり、内部監査人及び外部監査人が

---

96 National Policing Improvement Agency, “IMPACT Programme: Police National Database – Privacy Impact Assessment Report”,（2009 年 4 月）（http://www.npia.police.uk/en/docs/Privacy_Impact_Assessment.pdf）。

97 British Standards Institution, “BS 10012:2009 Data protection. Specification for a personal information management system”,（2009 年 5 月）（http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030175849）。

とりわけデータ保護法への遵守を効率的にアセスメントすることを可能とするための共通の土台を提供することを目的としている。

BS 10012 は、産業界や政府、学界、消費者団体の代表者を含む専門家委員会によって開発された。3 ヶ月間のパブリックコメントによって沢山のコメントが寄せられ、これらのコメントは同基準の第 1 版を策定する前に専門家委員会によって吟味された。

BS10012 の中では、PIA に言及していない。なぜなら、BSI は政府機関や民間企業が誰でも利用できるフレームワークを提供するものであり、民間企業等には、PIA を必ずしも必要としないような、複雑でない、あるいは ICT を使っていない個人情報マネジメントシステムも存在するからである[98]。

BS10012 における ICO の役割

ICO は BS10012 を支援しているが、それを使っていることによって、その組織にデータ保護のお墨付きを与えるわけではない。ICO はいわば一歩下がったところから支援している。ある組織から個人情報が漏洩した場合、その組織がどれだけデータ管理を適切に行っていたか、BS10012 に沿って行ってきたという過去の実績を当該組織が証明できれば、ICO が罰則を少なくすることはありうる。そうした、組織が自らのデータ取り扱いの適切性を証明するための便利なツールとして、ICO も BS10012 を推奨している。

BS10012 の認証スキーム（第三者認証制度）について

現時点では、BS10012 の認証スキームは存在しない。BSI では、標準を発行してから市場に根付かないと、認証事業に移ることができない。また、BSI の関係者（株主等）がやる気がないといけない。ICO の権限を強化したばかりなので、政府は認証スキームにあまり関心がない。BSI 自身は認証スキームをやる気があるが、全体の見通しが立ってからでないと立ち上げられない。

BSI のデータ保護領域での取組みについて[99]

BSI はデータ保護の領域で長い実績があり、2004 年にはデータ保護のための詳細ガイダンス文書” Data Protection Pocket Guide”を ICO と協働して開発し、発行したりしている。BSI はデータ保護実施者向けの補完的な訓練も提供している。このガイダンス文書は、BS10012 に合わせて更新されており（2009 年に第二版を発行）、組織が自らアセスメント

[98] ただ、BSI が策定した RFID に関するガイダンスには、PIA のテンプレートも含まれているという。

[99] BusinessStandards.com 記事（2009 年 6 月 2 日）（http://www.businessstandards.com/Articles/090603_BS27_Governance?print_only=1）を参考にした。

を行えるようにオンラインで利用可能とする予定である[100]。BS10012 は組織による自己評価用の基準であるが、需要があれば、BSI は第三者認定スキームを立ち上げるかもしれない。

BSI の ICT 部門向け市場開発部長の Breda Corish 氏は、BS10012 が疑いもなく英国のビジネスにベネフィットになるとしている。「BS10012 は、より良い顧客サービスをもたらし、組織が顧客をより良く知ることを可能にし、個人情報を注意深く取り扱っていることを示すことで顧客のロイヤリティを高めることができる。」

（２）Privacy by Design

Privacy by Design（PbD）とは、「設計段階からプライバシー保護を組み込む」というシステム開発の 1 つの「哲学」であり、実践手段として PIA や PET（Privacy Enhancing Technology：プライバシー強化技術）を伴うものである。カナダのオンタリオ州情報・プライバシーコミッショナーである Ann Cavoukian 博士によって提案された概念である。

ICO は 2008 年 11 月発行の”Privacy by Design”[101]において、「プライバシー・バイ・デザインの目的は、新たなシステム等の開発に先立って、プライバシーニーズに十分に配慮することである。換言すれば、当該システムやプロセスが個人のプライバシーに及ぼす影響（impact）について考慮に入れ、そのことを当該システムのライフサイクル全般に渡って行い、それにより、適切なコントロールが実施され維持されることを保証することである」と規定している。

PbD については、ICO がデータ保護法に盛り込むことを提案しているという。

なお、EU データ保護指令については 2011 年内に欧州委員会が改正案を提出する予定であり、EU 各国の国内法もそれに合わせて改正される見込みである。

---

100 http://www.bsigroup.com/en/About-BSI/News-Room/BSI-News-Content/Disciplines/Information-Management/Data-protection-tool/のことを指すと思われる。

101 Information Commissioner’s Office, “Privacy by design”,（2008 年 11 月）（http://www.ico.gov.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf）。

６．ドイツの状況

６．１　ドイツにおける事前評価

ドイツでは、連邦データ保護法[102]の第 4d 条第 5 項でデータ保護のための Prior checking（事前評価）を規定している。同条項の日本語訳（弊社訳）は以下の通りである。

連邦データ保護法　第 4d 条第 5 項

自動化されたデータ処理が、本人（データ主体）の権利および自由に対する特別なリスクにつながる場合、そのようなデータ処理は開始に先立つ段階における評価（事前評価）の対象となる。事前評価は、特に以下のような場合に実施すること。

1. 特別な種類の個人データ（第 3 条 9 項）（＊註 1）の処理を行う場合

2. 個人データの処理が、本人の能力を含む、個人的特徴、実績、または行動を評価するためのものである場合

ただし、以下のような場合は事前評価の対象とはならない：

法的な義務または本人の許可が存在し、もしくは本人との法的行為または法的行為に類する債務関係の証明、実行、または完了のために、（個人　データの）収集、処理もしくは利用が必要である場合。

（＊註 1）人種・民族、政治的見解、宗教・哲学的信条、労働組合への加盟、医療、性生活に関する個人データ

図 23　ドイツの連邦データ保護法第 4d 条第 5 項 事前評価

官民の機関・組織が個人データの自動処理を行う場合には、事前評価が必要となる。紙での取り扱いのみの場合は必要ない。事前評価は、当該機関・組織によって自主的に実施され、事前評価の実施責任者は、当該組織のデータ保護担当者である。

なお、連邦データ保護法の第 4f 条 1 項において、個人データの自動処理を行う組織（官および民）はデータ保護担当者を任命しなければならないと規定されている。

実施機関は、事前評価結果をデータ保護監察官（データ保護のための監督機関）に報告する義務はない。ただ、事前評価を行うことは連邦データ保護法上の義務であるため、データ保護監察官による監査時に、事前評価の未実施が判明すると、当該機関には罰金が課される。

ドイツにおいては、事前評価に関する詳細規定やガイドラインは存在しない。データ保護担当者の資格基準があり、これによって各機関は事前評価の水準を担保している。事前評価のやり方や結果の妥当性について、データ保護担当者からデータ保護監察官への問合せは多いとのことである。

---

[102] Bundesdatenschutzgesetz(BDSG)（http://bundesrecht.juris.de/bdsg_1990/index.html）。

６．２　データ保護監察官の概要

データ保護監察官は、行政・民間における個人データの取扱いを監督する第三者機関であり、EU 指令第 28 条の「監督機関」に該当する。連邦、16 の各州に存在する。

連邦と州の役割分担については、連邦政府機関、電気通信・郵便・鉄道事業者については連邦データ保護監察官が所轄し、各州・自治体の機関、各州の民間企業については、週のデータ保護監察官が所轄する。

連邦のデータ保護監察官は、連邦政府が推薦し、連邦議会が選任し、連邦大統領が任命する。連邦データ保護監察官の任期は 5 年間であり、この間は解任されない。再任は可能であるが、再再任は不可である。また、連邦データ保護監察官事務所のスタッフは元々は内務省の職員である。ただし、監察官事務所に来ている間（任期期間中）は、内務省の指示は受けない。内務省が監察官事務所の人事に口を出すことはできない。連邦データ保護監察官事務所の予算については、予算項目上は内務省の外局の扱いだが、予算額やその使途の決定権は監察官にある。

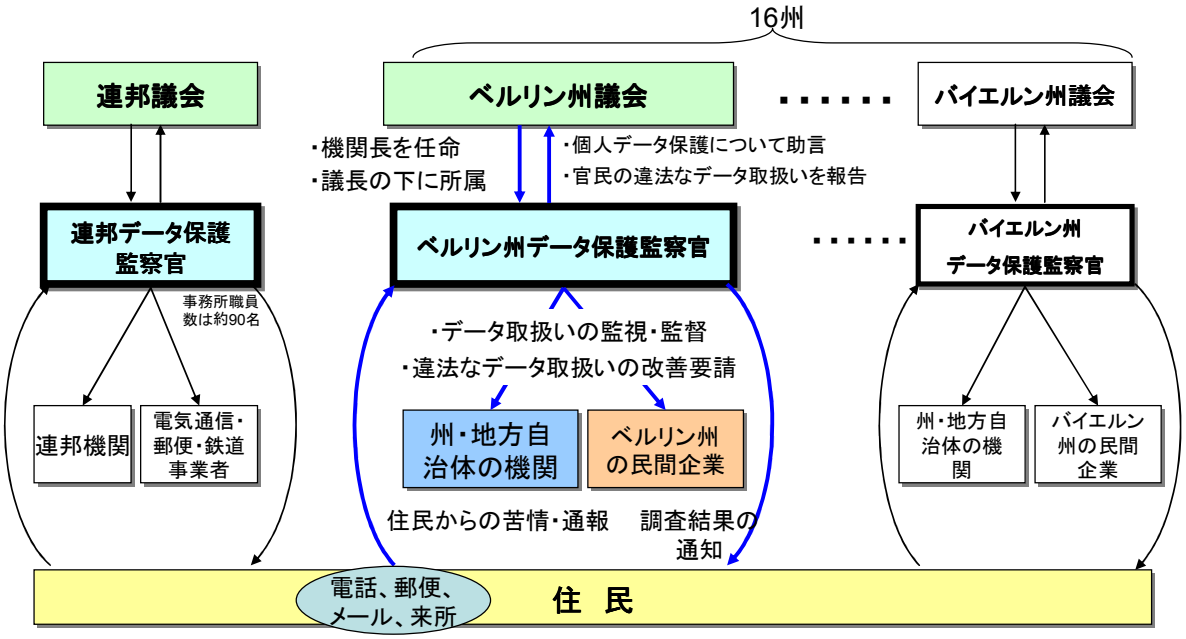


図 24　ドイツのデータ保護監察官

６．３　eID カードについて

ドイツの eID カードについては、2010 年度報告書に詳述しているが、本年度上期に追加調査を行ったので、下記に記載する。

eID カードは 2010 年 11 月から、既存の身分証明書に替えて順次発行を開始しており、2011 年 4 月現在で 370 万枚程度発行済みとのことである。

「Restricted ID」の利用状況

eID カードの利用者をサービス提供者が識別する方法は、以下の 2 つがある。

- eID カード内の個人情報を用いる方法　（初回認証時、一過性のトランザクションの場合など）
- 「Restricted ID」を用いる方法　（継続的なトランザクションの場合など）

オンライン認証では、「Restricted ID」を用いるサービスが大半とのことである。とりわけ匿名サービス（インフォメーションポータル等）では「Restricted ID」を用いる。保険会社での口座開設等の場合は、窓口で手続きを行い、その後のオンラインサービスでのログイン認証には「Restricted ID」の方法で行う。

eID カードで利用できる官民サービス

2011 年 4 月現在で、40～50 のサービスが提供されているとのことである[103]。そのうち 3 分の 2 は民間サービスである。民間サービスの多くは保険会社のサイトであり、他にインフォメーションポータル、オンラインショップ等がある。行政サービスは児童手当の申請、州・自治体ポータル等が存在する。間もなく使える行政サービスとしては、交通違反の点数確認、納税申告がある。

eID カードに対するデータ保護監察官の意見

データ保護監察官は新しい法律の制定段階で、連邦データ保護法の第 26 条 2 項に基づき意見書（答申書）を提出することができる。

eID カード導入に際しては、「身分証明書改正法案」への意見書として、連邦および 16 州合同で提出を行った。意見書に拘束力はないが、連邦議会の専門委員会で審議され、法案修正のインプットとなるとのことである。

この意見書は、上述の「事前評価」とは異なるものであり、eID カードの事前評価は各機関で実施しているとのことである。

eID カード（法案段階）に対する連邦・16 州合同意見のうち、主なものは以下の通りである。

---

103 なお、eID カードで利用できる官民サービスの一部は、
http://www.ausweis-portal.de/index.php/live-testanwendungen/live-test-anwendungen
に掲載されている。

① eID カードのチップへの指紋情報の格納は任意とすべきであり、指紋情報を格納しないことによって、当人が何らかの差別を受けるべきではない。(→この意見は採用された。)
② 指紋情報は eID カードの中のみに格納するべきであり、DB で管理するべきではない。(→この意見は採用された。)
③ eID カードの認証機能は、チップの中の情報をサービス提供者に提供することが要求され、そのことはリスクとなりうる。不正なプログラムによってカードの PIN が読み出されるおそれもある。そのため、eID 機能の利用はオプショナルであり、オプトアウト可能とするべきである。(→この意見は採用された。)
④ (少なくとも署名機能を使う場合は) テンキー付きの最もセキュリティレベルの高いカードリーダーのみを利用可能とするべきである。(→この意見は採用された。)

７．日本での導入に向けた課題

日本で予定されている情報保護評価制度、本事業で調査した米国、カナダ（連邦、オンタリオ州）及び英国の PIA 制度について、比較表としてまとめると、表 1 のようになる。

表 1　PIA 制度各国比較表[104]

	日本（予定されているもの）	米国（国土安全保障省）	カナダ（連邦）	カナダ（オンタリオ州）	英国
導入の背景	番号制度導入によって国家により様々な個人情報が一元管理されるのではないか、「番号」に係る個人情報が不正に追跡・突合されるのではないかなどの懸念を踏まえ、国民の「番号」に係る個人情報が適切に取り扱われる安心・信頼できる番号制度を構築するために情報保護評価を導入	1974年プライバシー法は連邦行政機関の個人データ保護を規定するが、旧い法律であるため情報時代における技術進歩に対応できなくなったので、これを補完するために2002年電子政府法においてPIAが導入された	1990年代後半、プライバシー法を効果的かつ体系的に遵守するための1つのツールとして、PIAが検討され、2002年のTBS（カナダ財務委員会事務局）のPIAポリシーにおいて、連邦政府機関にPIA実施が義務化された	（未調査）	ICO（情報コミッショナーオフィス）の「監視社会に関する報告書」（2006年）の中で、英国における監視社会（CCTV、IDカード等）の進展に対処するための手段としてPIAに言及しておりPIA導入の1つの契機となった。2007年頃の省庁における度重なるデータ漏洩事件を受けて、中央省庁に対してPIA実施が義務化された
根拠法令等	マイナンバー法（予定）	・2002年電子政府法第208条 ・2002年国土安全保障省設立法第222条（国土安全保障省（DHS）が対象）	TBSのPIA指令（2010年）	・オンタリオ州行政サービス省の調達指令 ・オンタリオ州行政サービス省の個人情報保護に関する共同ポリシー	内閣府の2008年6月報告書"Data Handling Procedures in Government"
ガイドライン	・行政機関及び関係機関向け情報保護評価ガイドライン（仮称） ・地方公共団体向け情報保護評価ガイドライン（仮称） ・法令に基づき「番号」を取り扱い得る事業者向け情報保護評価ガイドライン（仮称）	・OMB（行政管理予算局）ガイダンス（2003年9月） ・DHSプライバシーオフィスのPIAガイダンス（2010年6月）（DHSが対象）	OPC（カナダ連邦プライバシーコミッショナー事務局）のガイド（2011年3月）	・IPA（オンタリオ州行政サービス省の情報・プライバシー・アーカイブ部門）のPIAガイド ・IPC（オンタリオ州情報プライバシーコミッショナー事務局）の医療分野PIAガイドライン	・ICOのPIAハンドブック（2009年6月） ・法務省の省庁向けPIAガイダンス（2010年8月）
準拠するプライバシー原則	（特になし）	FIPPs（公正な情報取扱い8原則）	カナダ規格協会の公正な情報取扱い10原則	IPCのプライバシー・デザイン8原則	データ保護8原則
義務付け対象機関	・行政機関の長 ・地方公共団体の長その他の執行機関 ・独立行政法人等 ・地方独立行政法人 ・マイナンバー生成機関 ・情報連携基盤を使用する事業者（日本年金機構、医療保険者等）	連邦行政機関	連邦政府機関	・州政府機関 ・州内の医療機関（民間を含む）	中央省庁機関
実施対象、単位	「番号」に係る個人情報ファイルを新規に保有する場合、及びその取扱いを変更する場合 （制度・施策に対する任意の情報保護評価についても想定）	新たなプログラム、システム、技術、規則制定、及び既存のそれらに重要な変更がある場合	新たなプログラムやアクティビティ、及び重要な変更のあるプログラムやアクティビティ	新たなプログラム、既存のプログラムへの大きな変更、新たな技術の使用等	個人データの処理を伴うプロジェクト（システム、データベース、プログラム、アプリケーション、サービス、それらの改修、及び制度等を含む）
実施タイミング	・原則として、システムの要件定義段階（システム用ファイル） ・手作業処理の設計段階（手作業用ファイル）	・プログラムやシステムの開発・改修・調達の前 ・OMBへの予算提出前	・プログラムやアクティビティの開始前 ・特に調達時には、入札の前	プロジェクトの概念段階	プロジェクトの設計段階より前
実施手順の概要	①「番号」に係る個人情報ファイルを保有しようとする場合は、「しきい値評価」を実施する ②しきい値評価の結果、プライバシー等に対する影響を与える可能性があると認められる場合、「重点項目評価」を実施する ③しきい値評価の結果、プライバシー等に対する影響を与える可能性が高いと認められる場合、「全項目評価」を実施する	①新たなプログラムやシステム等に対し、プライバシー閾値分析（PTA）を実施する ②PTAにおいて必要と判断された場合には、PIAを実施する。	①新たなプログラムやアクティビティ等に対し、コアPIAを実施する ②追加的なPIA（フルPIA）が必要であれば、それを実施する。	①新たなプロジェクト等に対して準備分析を実施する ②準備分析で必要と判断されれば、プライバシーリスク分析を実施する ③準備分析で必要と判断されればプライバシーデザイン分析を実施する	①個人データを処理するプロジェクトに対してイニシャル・アセスメントを実施し、PIAの実施が必要か否か、またフルスケール版PIAが必要かスモールスケール版PIAでよいかを判断する ②フルスケール版PIA又はスモールスケール版PIAを実施する
報告書のレビュー	・重点項目評価報告書については、第三者機関がサンプリングして点検 ・全項目評価報告書については、第三者機関の審査が必要	DHSプライバシーオフィスがPTAとPIAをレビュー	OPCがコアPIAとフルPIAをレビュー	・IPAがレビュー ・ハイリスクなものについてはIPCがレビュー	ICOは報告書のレビューを行っていない
報告書の承認	・重点項目評価報告書については、特に承認は必要ない ・全項目評価報告書については、第三者機関の承認が必要	DHSプライバシーオフィスのCPOがPIAを内部承認	実施機関内で定めた承認プロセスに従い、コアPIAを内部承認 （OPCは承認を行わない）	実施機関で内部承認	ICOは報告書の承認を行っていない
報告書の提出義務	全ての報告書は、第三者機関への提出義務がある	OMBへの報告書写しの提出義務がある	・コアPIAは、TBSとOPCへの提出義務あり ・フルPIAは、OPCへの提出義務あり	準備分析については、IPAへの提出義務がある	ICOへの報告書の提出義務はない
報告書の公表	全ての報告書は、情報セキュリティや安全保障上のリスクとなりうる箇所を除き、公表する義務がある	公表義務がある （安全上の理由や機密情報・センシティブ情報等を保護する理由から、一部を公表しなくてもよい）	コアPIAの一部を公表する義務がある	公表義務はない	公表義務はない
パブリックコンサルテーション（パブコメ等）	・重点項目評価については実施機関の裁量でパブコメを実施 ・全項目評価についてはパブコメ実施が必要	PIAの過程に組み込まれている	PIAの過程に組み込まれていない （2002年PIAポリシーの時代には組み込まれていた）	特に市民への影響が大きいプロジェクトについては実施	PIAの過程に組み込まれている
第三者機関の役割	●番号情報保護委員会が相当 ・ガイドラインの策定 ・実施機関から情報保護評価報告書の提出を受ける ・重点項目評価報告書のサンプリング点検 ・全項目評価報告書の審査と承認 ・報告書に虚偽記載等がある場合に、助言・勧告・立入検査	（第三者機関は存在しない）	●OPC（連邦プライバシーコミッショナー事務局）が相当 ・ポリシーや指令の策定において、TBSに協力 ・連邦政府機関からPIAの提出を受け、レビュー ・連邦政府機関にPIAに関する助言や勧告	●IPC（オンタリオ州情報プライバシーコミッショナー事務局）が相当 ・ハイリスクと考えられるプロジェクトに対して、PIAのレビューを実施 ・医療分野におけるPIAガイドラインを策定	●ICO（情報コミッショナーオフィス）が相当 ・PIAの普及啓発 ・具体的には、ガイドラインの作成・提供や、教育・ワークショップ等の実施
実施期間	（未定）	3～6ヶ月程度 （PTA開始からPIA承認まで）	3ヶ月～1年程度	（未調査）	3ヶ月～1年程度
複数機関を跨るPIA	複数機関を跨る情報保護評価についての規定はない （複数ファイルを含むシステムに対する情報保護評価の規定は有り）	OMBガイダンスで「複数の行政機関が共同で個人情報の新たな利用や交換を伴う共用機能を導入する際には、主導する機関がPIAを実施するべき」と規定	・PIA指令で、プログラムやアクティビティが複数機関を跨る場合は1つの機関がリーダーになり、他の機関を取りまとめてPIAを実施することを規定 ・OPCは、ある新たなイニシアティブが複数機関を跨るものである場合、1つのPIAを実施することを推奨	IPCは、複数機関が1つのイニシアティブとしてシステムを導入するような場合、当該イニシアティブに対して包括的なPIAを実施することを推奨。ただし、既存のシステムに与える影響が各政府機関で異なると考えられる場合には、個別のPIAも実施	ICOは、以下のような場合、複数のシステムに対して1つのPIAを実施することが合目的的かつ経済的であると推奨。 (1)複数のシステムに実装されるようなパッケージ・アプリケーションに対して、当該アプリケーションの開発企業がPIAを実施する場合 (2)複数の政府機関が共通のプラットフォームを導入する際にPIAを実施する場合 (3)ある業界内における共通のアプリケーション（信用情報アプリケーション等）に対してPIAを実施する場合

104　日本の欄は、2011 年 12 月 22 日の情報保護評価ガイドライン案の時点で予定されているものである。

既に PIA 制度を導入している先進諸国、とりわけ行政分野の個人情報保護法制の一環として PIA をいち早く導入し、PIA に関して 10 年近い実績と経験のある米国及びカナダと比べると、日本で予定されている情報保護評価制度は、以下のようないくかの点で課題がある。

１．情報保護評価の実施対象範囲の狭さ

日本で検討中の情報保護評価制度は、社会保障・税番号制度導入に当たっての個人情報保護措置の一環という位置付けであるため、「番号」に関係するシステム（「番号」に係る個人情報ファイル）だけが情報保護評価の実施対象とされている。しかし、行政分野には、他にも国民のセンシティブな情報やプライバシーリスクの高い情報を取扱う行政システムがあるにもかかわらず、番号に関係するシステムのみは情報保護評価の対象とするのは突出しており、バランスが悪いと考えられる。

すなわち、入国管理関係、監視カメラ関係、健康医療情報関係のシステムや、その他いわゆる特定機微情報[105]や生体情報、位置情報等を取扱うシステムなど、プライバシーリスクが高いと思われる行政システムは他にも存在する訳であり、PIA 本来の趣旨から言えば、むしろそれらも情報保護評価制度の実施対象に含めるべきと考えられる[106]。

２．情報保護評価が準拠するプライバシー原則の不在

情報保護評価ガイドライン案においては「情報保護評価の評価対象を、個人情報保護にとどまらない国民のプライバシー保護とする」と謳われている。しかし、「プライバシー」や「プライバシーの権利」は日本の法律上で明文化された概念ではなく[107]、ガイドライン案等においては準拠すべきプライバシー原則（OECD プライバシーガイドラインの 8 原則的なもの）も特に挙げられていない。そのため、現在のガイドライン案は、各機関が情報保護評価を実施するにあたって、何に依拠して「プライバシー保護の観点から」自らの対応策の妥当性を判断すればよいか分からない構成となっている（図 25 参照）。

---

105 JISQ15001:2006（個人情報保護マネジメントシステム-要求事項）では、以下に示す内容を含む個人情報は「特定の機微な情報」として、個人情報保護上の格別な扱いが要求されている。「思想、信条又は宗教に関する事項」「人種、民族、門地、本籍地（所在都道府県に関する情報を除く）、身体・精神障害、犯罪歴その他社会的差別の原因となる事項」「勤労者の団結権、団体交渉その他団体行動の行為に関する事項」「集団示威行為への参加、請願権の行使その他の政治的権利の行使に関する事項」「保健医療又は性生活に関する事項」。

106 また、情報保護評価制度そのものではないが、予定されている第三者機関（「個人番号情報保護委員会」）についても、個人情報保護全般を監督するものではなく、番号に関係する個人情報の保護を監督するものにすぎない。諸外国（とりわけ EU）から、国際水準を満たす第三者機関とみなされない可能性が高い。

107 1964 年の「宴のあと」東京地裁判決等、プライバシーの権利を認めた判例が存在するにすぎない。

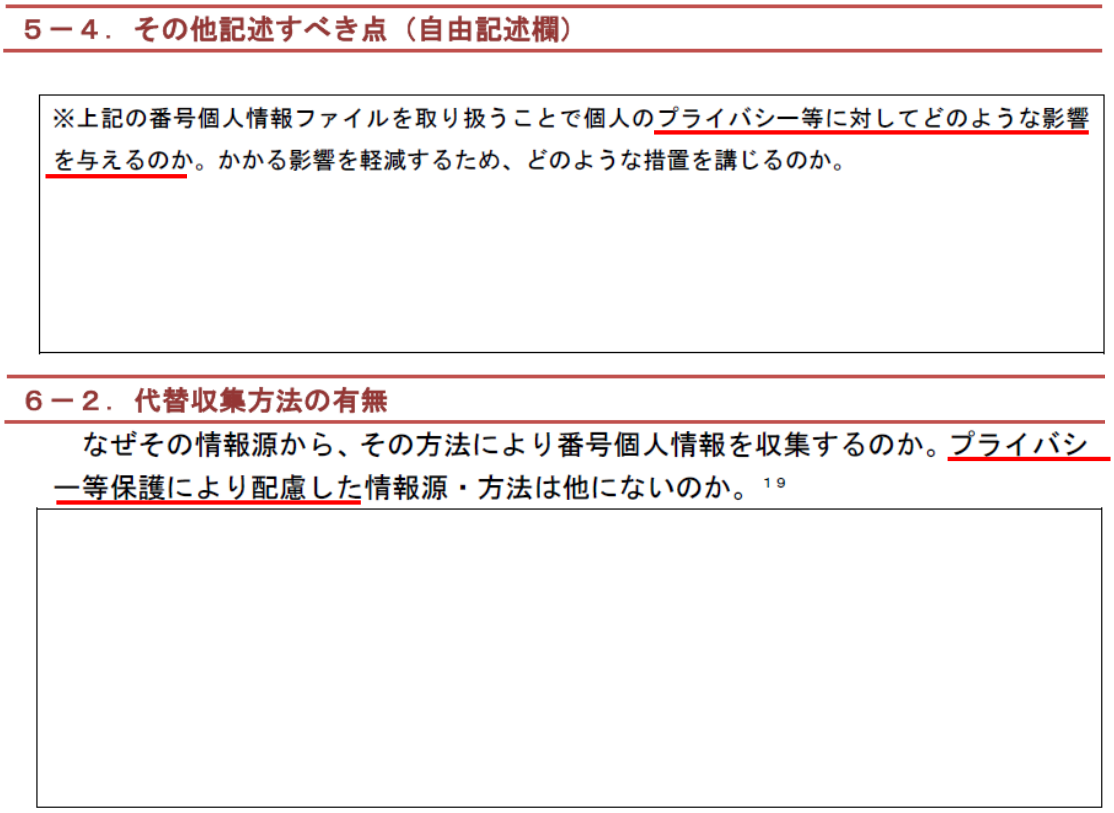


図 25　情報保護評価報告書の記載事項例

ちなみに、米国 DHS では FIPP s（公正な情報取扱い 8 原則）、カナダ連邦ではカナダ規格協会の公正な情報取扱い 10 原則、カナダ・オンタリオ州では IPC のプライバシー・デザイン 8 原則など、それに基づきプライバシーリスクの評価とリスク軽減を行うべき原則がガイドライン中で明記されている。

日本の情報保護評価ガイドライン等においても、各機関が情報保護評価を実施するに当たって依拠すべきプライバシー原則について、明示するべきである。

３．複数機関を跨る情報保護評価に関する規定の不在

社会保障・税番号大綱では、行政機関及び関係機関（日本年金機構や医療保険者等）が情報保護評価の義務付け対象者であり、地方公共団体及び法令に基づき「番号」を取扱い得る事業者（金融機関や源泉徴収義務者など）が非義務付け対象者とされている。義務付け対象者だけでも、医療保険者である健康保険組合は約 1450 団体あるなど、数千の単位に上る。もちろん、情報保護評価ガイドライン案でもこれら全ての機関が全ての「番号に係る個人情報ファイル」に対して情報保護評価を本実施するのではなく、まず「しきい値評価」を実施した上で、プライバシー等に対する影響を与える可能性があると認められる場合に限って、重点項目評価または全項目評価を実施する流れとなっている。

ただ、ガイドライン案のしきい値評価の基準では、対象人数が 10 万人の場合は全項目評価、1 万人以上の場合は重点項目評価という振分けになっている。各行政機関が保有する個人情報ファイル数の資料[108]を見ると、例えば国税庁では全項目評価に相当する対象人数 10 万人以上の個人情報ファイルが約 6,000、重点項目評価に相当する対象人数 1 万人以上の個人情報ファイルが約 18,000 存在する[109]。

国税庁または各税務署は、これらの全件について情報保護評価（重点項目評価または全項目評価）を実施し、全項目評価についてはパブコメを実施し、また第三者機関はこれら全ての全項目評価報告書に対して審査と承認を行わなければならない。

ガイドライン案では一応、複数の「番号に係る個人情報ファイル」を含む 1 つのシステムについて 1 つの情報保護評価報告書を作成することも可能とされている。しかし、複数のシステムや機関を跨るような情報保護評価の実施についての規定はない。

そもそも情報保護評価は（それが「しきい値評価」のみに結果的に留まったとしても）、番号に関係する各機関が個別に行うべきものなのだろうか。「情報連携基盤[110]」や「マイポータル」、「番号生成機関」など、新たに構築するシステムについては個別に情報保護評価を行うことも必要と考えられるが、個々の情報保有機関（上記の行政機関や関係機関など）については番号制度導入に伴う受動的なシステム改修にすぎない訳であるから、情報保有機関の種類ごと（医療保険者、地方公共団体など[111]）にグルーピングした上で、それらの各グループについて統一的な情報保護評価を行い、その結果を受けた共通的なシステム設計ガイドライン（要求仕様）を作成して各グループの情報保有機関に配布する方法もありうるのではないか。

米国の OMB ガイダンス[112]では「複数の行政機関が共同で個人情報の新たな利用や交換を伴う共用機能を導入する際には、主導する機関が PIA を実施するべきである」と言われている。また、3.5 節で述べたように、カナダ連邦では PIA 指令で、プログラムやアクティビティが複数機関を跨る場合は 1 つの機関がリーダーになり他の機関を取りまとめて PIA を実施することが規定されており、OPC は、ある新たなイニシアティブが複数機関を跨る

---

108 http://www.cas.go.jp/jp/seisaku/jouhouwg/hyoka/dai4/sankou1.pdf

109 これらのファイルの多くは国税庁の地方組織である税務署で保有されていると考えられる。また、これら全てのファイルが「番号に係る個人情報ファイル」に該当する訳ではないと考えられる。

110 マイナンバー法案では「情報提供ネットワークシステム」と呼ばれている。

111 あるいは、それらのシステムの納入ベンダーごとにグルーピングすることも考えられる。地方公共団体や医療保険者などは、自前で情報保護評価を実施することは現実問題として困難である。これらの機関はベンダーに情報保護評価を実施させるか（設計・開発と一緒に調達等）、外部コンサルタントを雇うしかないが、その費用は誰が負担するのか。例えば地方公共団体で番号制度導入によって改修が入るのは、情報連携基盤とのインターフェース部分や、情報連携で用いる記号・符号の変換機能の部分、既存システム／ファイルへのマイナンバー追加部分である。これらは、各地方公共団体でシステム構成や運用が大きく異なることは考えにくく、システムの納入ベンダーごとにかなり共通化されるはずである。

112 http://www.whitehouse.gov/omb/memoranda_m03-22/

ものである場合、1 つの PIA を実施することを推奨している。カナダのオンタリオ州でも、IPC は、複数機関が 1 つのイニシアティブとしてシステムを導入するような場合、当該イニシアティブに対して包括的な PIA を実施することを推奨している[113]。また、英国の PIA ハンドブックでも、複数の政府機関が共通のプラットフォームを導入するような際には、包括的な PIA を実施することが合目的的かつ経済的として推奨している。上期の報告書で PIA 実施プロジェクト事例として挙げたスコットランド NEC（国民資格カード）では、関係する複数の機関に対して横断的に 1 つの PIA を実施していた。

我が国でも、「行政の効率化」という番号制度の導入目的の一つに鑑みれば、番号に関係する個々の機関や（評価結果を審査する）第三者機関に過度な負担をかけることのない効率的な PIA 実施の仕組みが必要である。

[113] ただし、既存のシステムに与える影響が各政府機関で異なると考えられる場合には、個別の PIA も実施すべきとしている。

参考文献

（１）全般

- 瀬戸・伊瀬・六川・新保・村上著『プライバシー影響評価 PIA と個人情報保護』（中央経済社、2010 年）
- 内閣官房の「社会保障・税に関わる番号制度」に関する資料、（http://www.cas.go.jp/jp/seisaku/bangoseido/index.html）
- 消費者庁「諸外国等における個人情報保護制度の監督機関」（2010 年 11 月 19 日）、（http://www.kantei.go.jp/jp/singi/it2/denshigyousei/dai4/siryou1_4.pdf）
- Loughborough University, 'APPENDIX H: Broad Jurisdictional Report for the European Union', "Privacy Impact Assessments: International Study of their Application and Effects",（2007 年 10 月）（ http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/lbrouni_piastudy_apph_eur_2910071.pdf）

（２）米国

- 1974 年プライバシー法 "Privacy Act of 1974"（合衆国法典第 5 編第 552a 条に該当する）、http://www.law.cornell.edu/uscode/usc_sec_05_00000552---a000-.html
- 2002 年電子政府法 "E-Government Act of 2002"、（http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf）
- 2002 年国土安全保障省設立法 "Homeland Security Act of 2002"、（http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf）
- Office of Management and Budget, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (E-Government Act Section 208 Implementation Guidance)（OMB ガイダンス）"（2003 年 9 月）（http://www.whitehouse.gov/omb/memoranda/m03-22.html）
- Department of Homeland Security, "PRIVACY POLICY GUIDANCE MEMORANDUM（プライバシーポリシーガイダンス覚書）: Memorandum Number: 2008-01",（2008 年 12 月）（http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf）
- Department of Homeland Security, "PRIVACY POLICY GUIDANCE MEMORANDUM（プライバシーポリシーガイダンス覚書）: Memorandum Number: 2008-02",（2008 年 12 月）（http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-02.pdf）
- Department of Homeland Security, "Privacy Impact Assessments: The Privacy Office Official Guidance（PIA ガイダンス）",（2010 年 6 月）（http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf）

- Department of Homeland Security, “Privacy Impact Assessment Template（PIA テンプレート）”
  （http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_template.pdf）
- Department of Homeland Security, “PRIVACY THRESHOLD ANALYSIS（PTA テンプレート）”,（2010 年 6 月）
  （http://www.dhs.gov/xlibrary/assets/privacy/privacy_pta_template.pdf）
- Department of Homeland Security, “DHS PRIVACY OFFICE: Guide to Implementing Privacy”,（2010 年 6 月）
  （http://www.dhs.gov/xlibrary/assets/privacy/privacy_implementation_guide_june2010.pdf）
- Department of Homeland Security, “System of Records Notices Official Guidance（SORN ガイダンス）”,（2008 年 4 月）
  （http://www.dhs.gov/xlibrary/assets/privacy/privacy_guidance_sorn.pdf）
- 平野美恵子「米国の電子政府法」『外国の立法 217』（2003 年 8 月））
  （http://www.ndl.go.jp/jp/data/publication/legis/217/21701.pdf）
- 消費者庁「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」（2008 年 3 月）（http://www.caa.go.jp/seikatsu/kojin/h21report3.pdf）

（３）カナダ（連邦）

- プライバシー法 “Privacy Act”、
  （http://laws-lois.justice.gc.ca/eng/acts/P-21/index.html）
- Treasury Board of Canada Secretariat, “Privacy Impact Assessment Policy（PIA ポリシー）”,（2002 年 5 月）（http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450）
- Treasury Board of Canada Secretariat, “Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks（PIA ガイドライン）”,（2002 年 5 月）
  （http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld01-eng.asp）
- Treasury Board of Canada Secretariat, “Directive on Privacy Impact Assessment（PIA 指令）”,（2010 年）
  （http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?section=text&id=18308）
- Office of the Privacy Commissioner of Canada, “Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada（OPC ガイド）”,（2011 年 3 月）
  （http://www.priv.gc.ca/information/pub/gd_exp_201103_e.cfm）
- Canadian Standards Association, “Privacy Code”,（1996 年 3 月）
  （http://www.csa.ca/cm/ca/en/privacy-code/publications/view-privacy-code）
- 消費者庁「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」

（2008 年 3 月）（http://www.caa.go.jp/seikatsu/kojin/h21report4.pdf）

（４）カナダ（オンタリオ州）

- Information, Privacy and Archives Division, “Privacy Impact Assessment Guide for the Ontario Public Service（PIA ガイド）”,（2011 年 7 月改訂）（Web 公開は無し）
- Information, Privacy and Archives Division, “OPS PIA – Part1: Preliminary Analysis”,（2011 年 7 月改訂）（Web 公開は無し）
- Information, Privacy and Archives Division, “OPS PIA – Part2: Privacy Risk Analysis”,（2011 年 7 月改訂）（Web 公開は無し）
- Information, Privacy and Archives Division, “OPS PIA – Part3: Privacy Design Analysis”,（2011 年 7 月改訂）（Web 公開は無し）
- Office of the Information and Privacy Commissioner of Ontario, “The New Federated Privacy Impact Assessment (F-PIA) : Building Privacy and Trust-enabled Federation”,（2009 年 1 月）
  （http://www.ipc.on.ca/images/Resources/F-PIA_2.pdf）

（５）英国

- Information Commissioner’s Office, “Privacy Impact Assessment Handbook Version 2.0”,（2009 年 6 月）
  （http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html）
- Information Commissioner’s Office, “Privacy by design”,（2008 年 11 月）
  （ http://www.ico.gov.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf）
- Information Commissioner’s Office, “Privacy Impact Assessments Project - Invitation to bid”,（2007 年）
  （http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/piap_inv_to_tenderfinal.pdf）
- Information Commissioner’s Office, “A Report on the Surveillance Society: For the Information Commissioner’s by the Surveillance Studies Network”,（2006 年 9 月）
  （ http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf）
- ICO Privacy by Design conference の資料（2008 年 11 月）
  （http://www.ico.gov.uk/news/current_topics/privacy_by_design_conference.aspx）
- Cabinet Office, “Data Handling Procedures in Government: Final Report”,（2008 年 6 月）（http://www.cabinetoffice.gov.uk/sites/default/files/resources/final-report.pdf）
- Cabinet Office, “Protecting Information in Government”,（2010 年 1 月）

（http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/caboffprotectinfo.pdf）
- Ministry of Justice, "Undertaking Privacy Impact Assessment: The Data Protection Act 1998”,（2010 年 8 月 13 日）
（http://www.justice.gov.uk/guidance/docs/pia-guidance-08-10.pdf）
- Improvement Service, “National Entitlement Card (NEC) Privacy Impact Assessment Report”,（2011 年 1 月）
（http://www.entitlementcard.org.uk/docs/PIAJan2011.pdf）
- Improvement Service, “National Entitlement Card Scheme and Scottish Citizen’s Account: National Terms & Conditions”,（2008 年 12 月）
（http://www.entitlementcard.org.uk/docs/TsandCs.pdf）
- Customer First (CF)の Data Protection Workshop（2009 年 10 月 5 日）の資料集、（http://www.improvementservice.org.uk/library/download-document/2757-collection-of-cf-conference-workshop-slides/）
- National Policing Improvement Agency, “IMPACT Programme: Police National Database – Privacy Impact Assessment Report”,（2009 年 4 月）
（http://www.npia.police.uk/en/docs/Privacy_Impact_Assessment.pdf）
- British Standards Institution, “BS 10012:2009 Data protection. Specification for a personal information management system”,（2009 年 5 月）
（http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030175849）。
- BusinessStandards.com 記事（2009 年 6 月 2 日）
（http://www.businessstandards.com/Articles/090603_BS27_Governance?print_only=1）
- David Tancock, Siani Pearson, Andrew Charlesworth, “The Emergence of Privacy Impact Assessments”,（2010 年 5 月）
（http://www.hpl.hp.com/techreports/2010/HPL-2010-63.html）
- Adam Warren, “Privacy Impact Assessments: the UK experience”,（2009 年 11 月）（http://www.privacyconference2009.org/program/Presentaciones/common/pdfs/adam_warren_speech_en.pdf）
- 石井夏生利「英国におけるインフォメーション・コミッショナーの組織と権限～わが国の第三者機関創設への示唆～」（堀部政男情報法研究会第 1 回シンポジウム、2010 年 8 月 21 日）（http://www.horibemasao.org/6.ishii.pdf）
- 内閣府「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」（2009 年 3 月）（http://www.caa.go.jp/seikatsu/kojin/index_en3.html）

（６）ドイツ

- 国際社会経済研究所「海外住民データベースの状況と地域情報化の進展に関する調査研究報告書」（2008 年 3 月）
  （http://www.candc.or.jp/cyosa_kenkyu/pdf/2007/2007report_01.pdf）
- 連邦データ保護法 “Bundesdatenschutzgesetz(BDSG)”、
  （http://bundesrecht.juris.de/bdsg_1990/index.html）
- ベルリン州データ保護及び情報公開監察官ホームページ、
  （http://www.datenschutz-berlin.de/）
- 連邦内務省ホームページ、
  （ http://www.bmi.bund.de/cln_165/DE/Themen/Sicherheit/PaesseAusweise/ePersonalausweis/ePersonalausweis_node.html）
- 連邦情報セキュリティ庁ホームページ、
  （https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/Personalausweis/personalausweis_node.html）
- 連邦印刷局ホームページ、
  （http://www.bundesdruckerei.de/de/produkte/produkte_dokument/dok_personala/dok_sicherheit/）

以　上

国民 ID とそれぞれの情報社会
に関する調査研究報告書

2012 年 3 月

株式会社国際社会経済研究所

〒108-0073　東京都港区三田 1-4-28 三田国際ビル 26 階
TEL　03-3798-9711
FAX　03-3798-9719