米国・カナダにおけるプライバシー影響評価（PIA）と日本における検討状況

2012年1月31日

国際社会経済研究所
小泉　雄介
y-koizumi@pd.jp.nec.com

目　次

・本資料は、弊社にて2011年11月に実施した米国・カナダ現地調査、および文献調査結果を取りまとめたものです。

1．PIAの概要

PIA（Privacy Impact Assessment：プライバシー影響評価）とは

○ 「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」 －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）より －

○ 「社会保障・税番号大綱」との関係

→ 「情報保護評価」に該当

※ 「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）（略）」

※ 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）の時点では「プライバシーに対する影響評価」と呼ばれていた。

※ 「関係機関」とは日本年金機構や医療保険者等をいう。

各国のPIA導入状況

○ カナダ
  – 1990年代から自主的に実施。
  – 2002年にカナダ財政委員会事務局がPrivacy Impact Assessment Policyにおいて、個人情報を取り扱うITシステムを導入・改修する行政機関にPIA実施を義務化。
  – 上記Policyの付属文書としてガイドライン”PIA Guidelines: A Framework to Manage Privacy Risks”を発行。
  – 2010年にカナダ財政委員会事務局がDirective on Privacy Impact Assessment（PIA指令）を策定。

○ 米国
  – 2002年電子政府法の第208条において、行政機関にPIA実施を義務化（報告書写しを連邦行政予算管理庁OMBの長官に提出する義務）。
  – 2003年9月にOMBがガイダンス ”OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002”を発行。

○ オーストラリア
  – 2006年に連邦プライバシーコミッショナー局が行政機関向けのガイダンス”Privacy Impact Assessment Guide”を発行。
  – PIA実施は義務ではなく、ガイドラインにおける推奨。

※オーストラリアについては、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）等を参照した。

○ ニュージーランド、香港でも実施

○ 英国
  – 先進諸国の取り組みを参考に、2007年頃に導入。
  – 2008年より、内閣府が中央省庁に対してPIA実施を義務化。法令化はされていない。
  – 2007年に情報コミッショナーオフィス（ICO）がPIAハンドブックを発行。
  – 拙稿『欧州におけるプライバシー影響評価（PIA）とEU指令改正の動向』http://www.i-ise.com/jp/study/PIA_20110914.pdf を参照のこと。

各国のPIA導入状況（続き）

○ その他のEU各国におけるPIA導入状況

– フィンランド
  - PIAの利用が一時検討されていた。

– アイルランド
  - データ保護コミッショナーが職場や学校における生体情報利用に関するガイドラインを策定し、その中でPIAの実施を推奨。

– オランダ
  - PIAを導入したが、成果が上がっていない。（英国ICOからの情報）

○ EUにおけるPIA類似の制度

– 欧州では、EUデータ保護指令（95/46/EC）第20条において「Prior checking」（事前評価）を規定。
  - PIAそのものではないが類似。
  - 国内法への反映状況等は国により様々。EU27カ国中、少なくとも16カ国で条文化。
  - 例：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）。

※EUデータ保護指令第20条　Prior checking（弊社訳）

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）

– 2012年1月25日に欧州委員会から提出されたEUデータ保護規則案（現行のEUデータ保護指令を改正）には、センシティブ情報等を取扱う処理について、データ保護影響評価（＝PIA）の実施を義務付ける規定がある。

２．日本における検討状況

社会保障・税番号制度の法律事項に関する概要（案）の要点

（2011年12月16日資料）

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

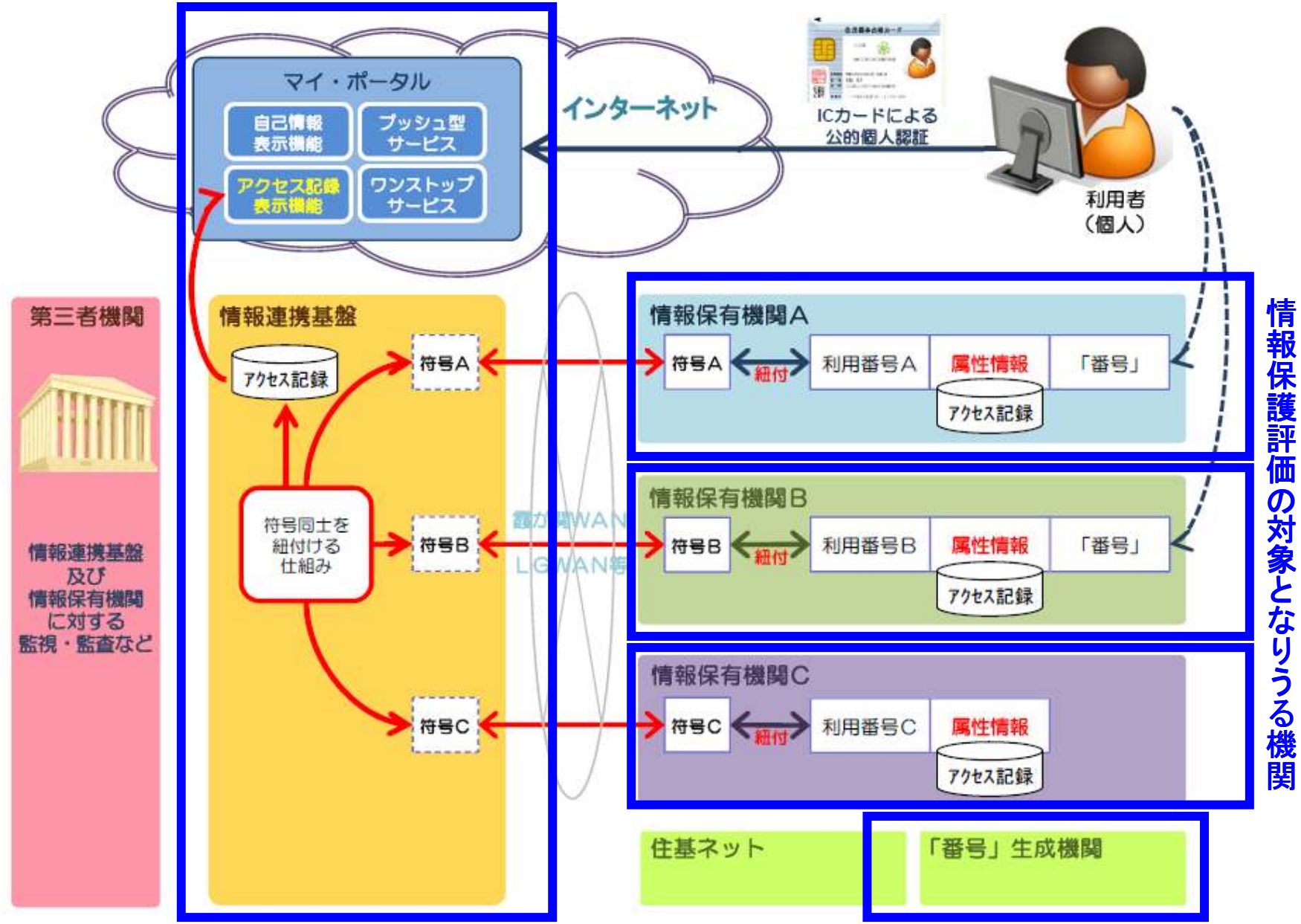
○マイナンバー法の施行後5年を目途として、本法の施行状況等を勘案し、本法の規定について検討を加え、その結果に応じて利用範囲の拡大を含めた所要の見直しを行う

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

出典：社会保障・税に関わる番号制度に関する実務検討会

番号制度における符号連携のイメージ

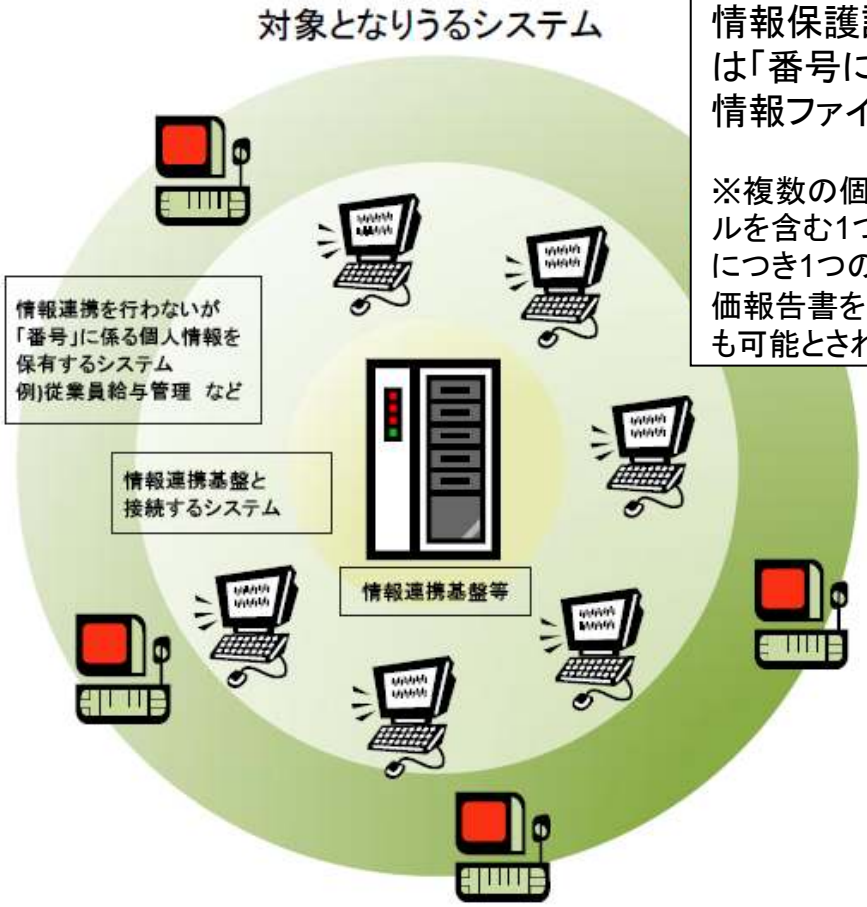


出典：情報連携基盤技術WG資料に加筆

情報保護評価の対象となりうる機関及びそのシステム

○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	



情報保護評価ガイドライン案では、
情報保護評価の対象は「番号に係る個人情報ファイル」と規定。

※複数の個人情報ファイルを含む1つのシステムにつき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。

(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)

出典:情報保護評価SWG資料

現時点で想定されている情報保護評価のプロセス

- 情報保護評価の実施の仕組み（案）

出典：情報保護評価SWG資料

情報保護評価の必要性を判断する

(しきい値評価)

区分	情報保護評価	国民の意見	第三者機関の審査	公開
				
対象外	×	×	×	○
必要性が特に高いとはいえないもの	△ ※重点項目評価を実施	△ ※各機関の裁量により意見聴取	△ ※重点項目評価をサンプリングチェック	○ ※しきい値評価、重点項目評価を公開
必要性が特に高いもの	○ ※全項目評価を実施	○	○ ※全件	○ ※しきい値評価、全項目評価を公開

３．米国の現状

米国のPIA制度概要： 背景と経緯

○ PIA導入の背景と経緯

- 「2002年電子政府法」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。
- 電子政府法第208条（プライバシー条項：PIA含む）は、「1974年プライバシー法」（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、1974年プライバシー法を補完するために策定された。
- 2003年9月にOMB（行政管理予算局）がガイダンス「OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002」を発行。

○国土安全保障省における経緯

- 国土安全保障省（DHS）については、「2002年国土安全保障省設立法」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。同法に基づき、DHSのプライバシーオフィスが設立された。
- 2004年、2006年、2007年にDHSプライバシーオフィスがPIAに関するガイダンスを発行。
- 2008年12月にDHSのCPOが「プライバシーポリシーガイダンス覚書」を発行。どのような場合にPIAが必要か等を規定。
- 2010年6月に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」を発行。

米国のPIA制度概要： DHSのプライバシー遵守プロセス

①プライバシー閾値分析（PTA）　※PTAのみはDHS独自の制度

- 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
- 3年ごとにレビューが必要

②プライバシー影響評価（PIA）

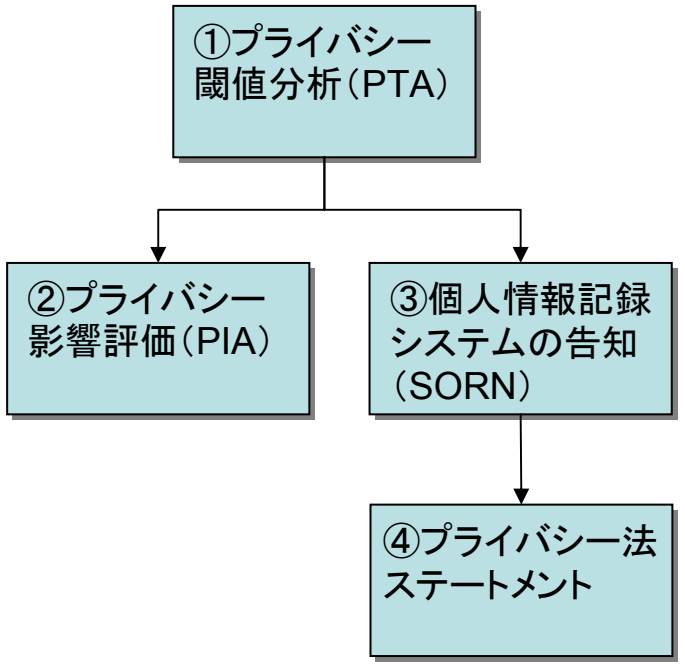
- 事前にプログラムやシステムのプライバシーリスクを特定し、軽減するための意思決定ツール
- どんな個人識別情報（PII）をどのような目的で収集し、どのように利用するか等について、一般市民に理解してもらう
- また、FIPPs（公正な情報取扱い8原則）に則ってプライバシーへの影響を評価し、軽減する

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
- プライバシー法のe項（4）号で規定　※日本の「個人情報ファイル簿」に相当

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
- プライバシー法のe項（3）号で規定



米国のPIA制度概要： PIAにおける各機関の役割分担

〇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
- 連邦行政機関向けのPIAガイダンスの作成・発行
- 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

〇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
- CPO（チーフプライバシーオフィサー）によるPIAの承認
- PIAに限らない一般的な任務
  - 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

〇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するPIAの実施
- 各部門ごとにプライバシーオフィサーが存在

※DHSにおけるPIAに関係する機関のみを記載。

PTA(Privacy Threshold Analysis:プライバシー閾値分析) 1/3

〇概要

- 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。
- DHS独自の制度。DHSの「プライバシーポリシーガイダンス覚書」で規定。

〇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。
- DHSプライバシーオフィスの決定を記録する。

〇PTAの実施対象

- 新たなプログラム(日本での「制度」に近い)、システム、技術、規則制定(rule-making)。
- 既存のプロジェクト(プログラム、システム、技術、規則制定の総称)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
  - PIIを異なる目的で利用する
  - PIIを削減する
- 3年ごとにレビューと再認定が必要。

〇PTAの実施件数

- DHSでは年間に600～700件程度のPTAを実施。

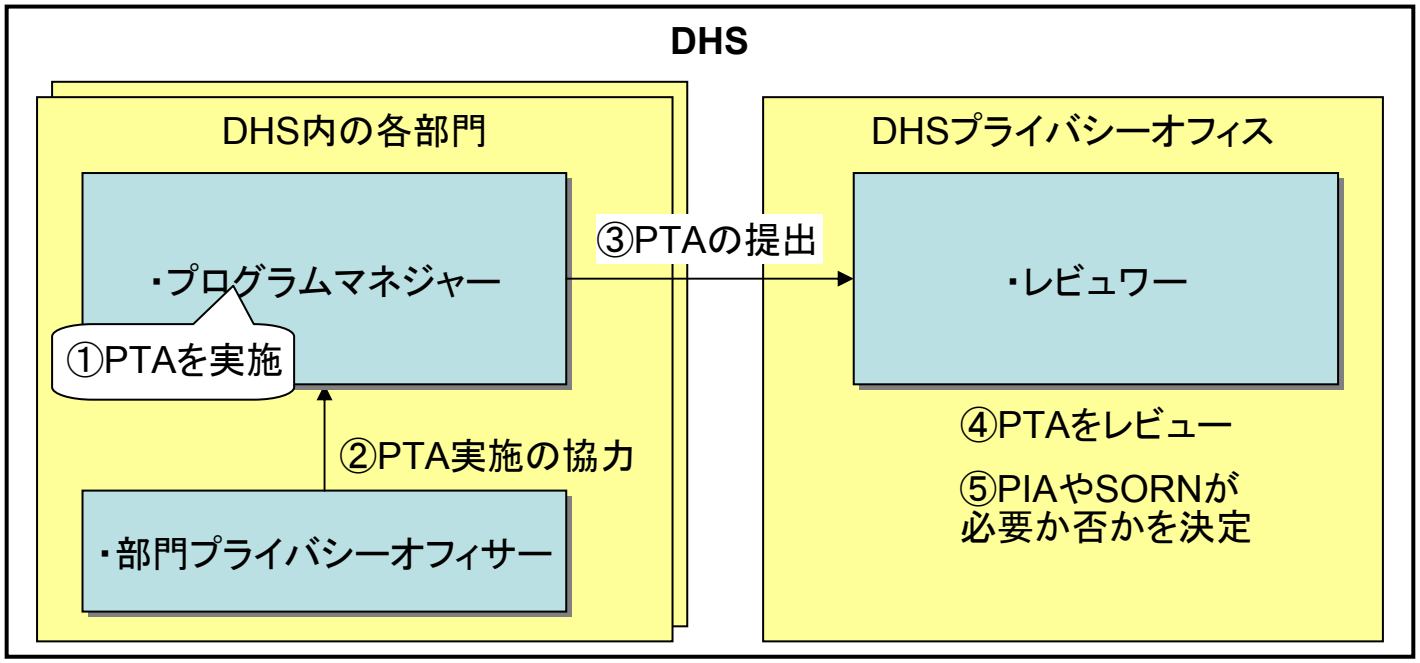
PTA(Privacy Threshold Analysis:プライバシー閾値分析) 2/3

○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。

○PTAの結果、PIAが必要とされないケース

- PTAにおいてPII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(Privacy Threshold Analysis:プライバシー閾値分析) 3/3

○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」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)
  - 「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」

PIA(Privacy Impact Assessment:プライバシー影響評価) 1/5

○概要
- 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。
  - 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。
  - 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、軽減する。
- 電子政府法で連邦行政機関の実施義務を規定。

○PIAの実施目的(DHSのPIAガイダンスより)
- 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。
- 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。

○PIAの実施対象(DHSの「プライバシーポリシーガイダンス覚書」より)
- 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
- 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

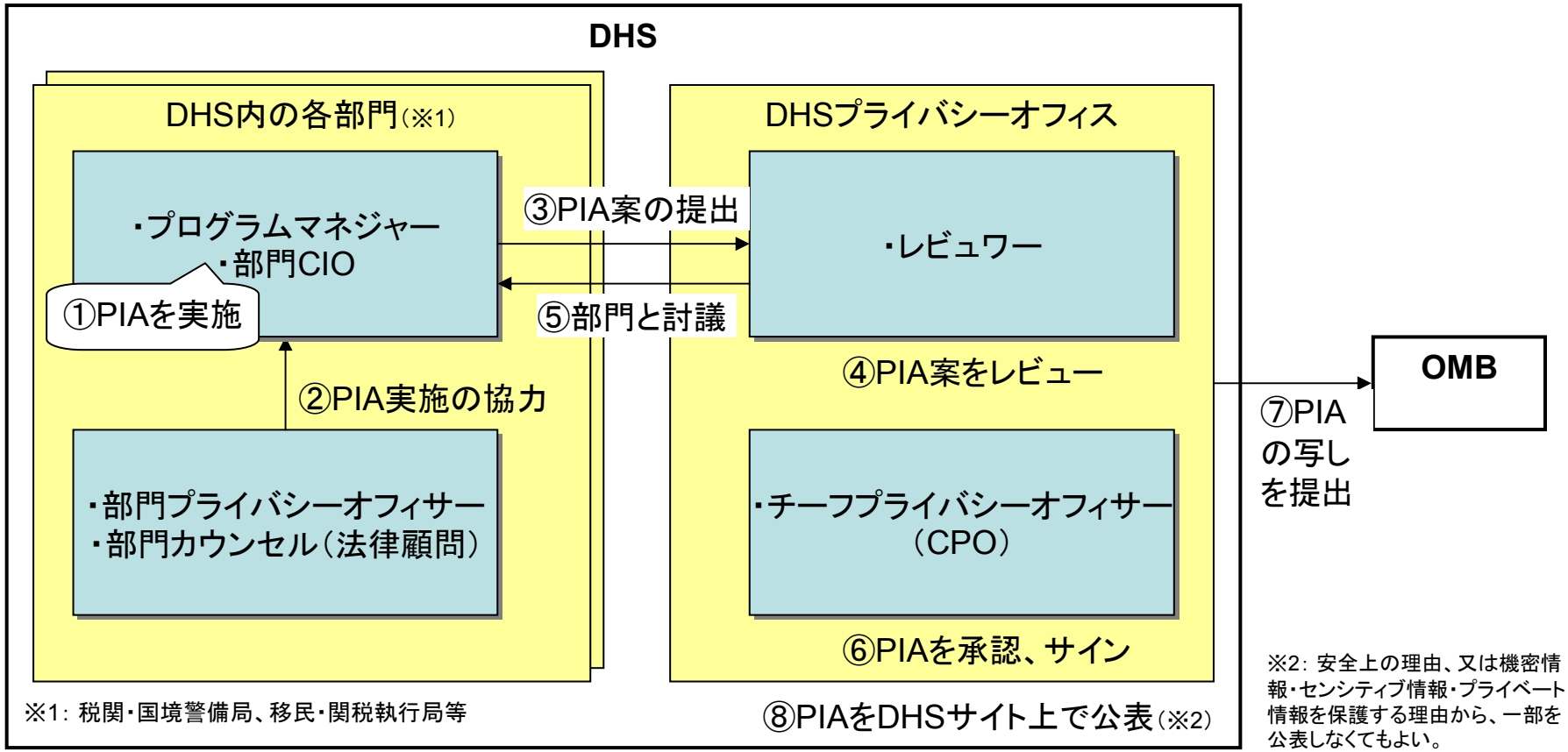
○PIAの実施件数
- DHSでは年間に100件程度のPIAを実施。

○PIAの実施期間
- 通常はPTA開始からPIA承認まで3~6ヶ月。
- 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(後述)。

PIA(Privacy Impact Assessment:プライバシー影響評価) 2/5

○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。



※2: 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。

PIA(Privacy Impact Assessment:プライバシー影響評価) 3/5

○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、OMBにPIA報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。
- 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)。
  - 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。

○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
  - 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。
  - 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が必要である。
  - 以下、規則制定のプロセス

    ①DHS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。

    ②パブリックコメントが来る。

    ③DHS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。)

    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。

PIA(Privacy Impact Assessment:プライバシー影響評価) 4/5

○PIA報告書の概要

- PIA報告書は、以下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プライバシーオフィスにおけるPIAレビューの方法

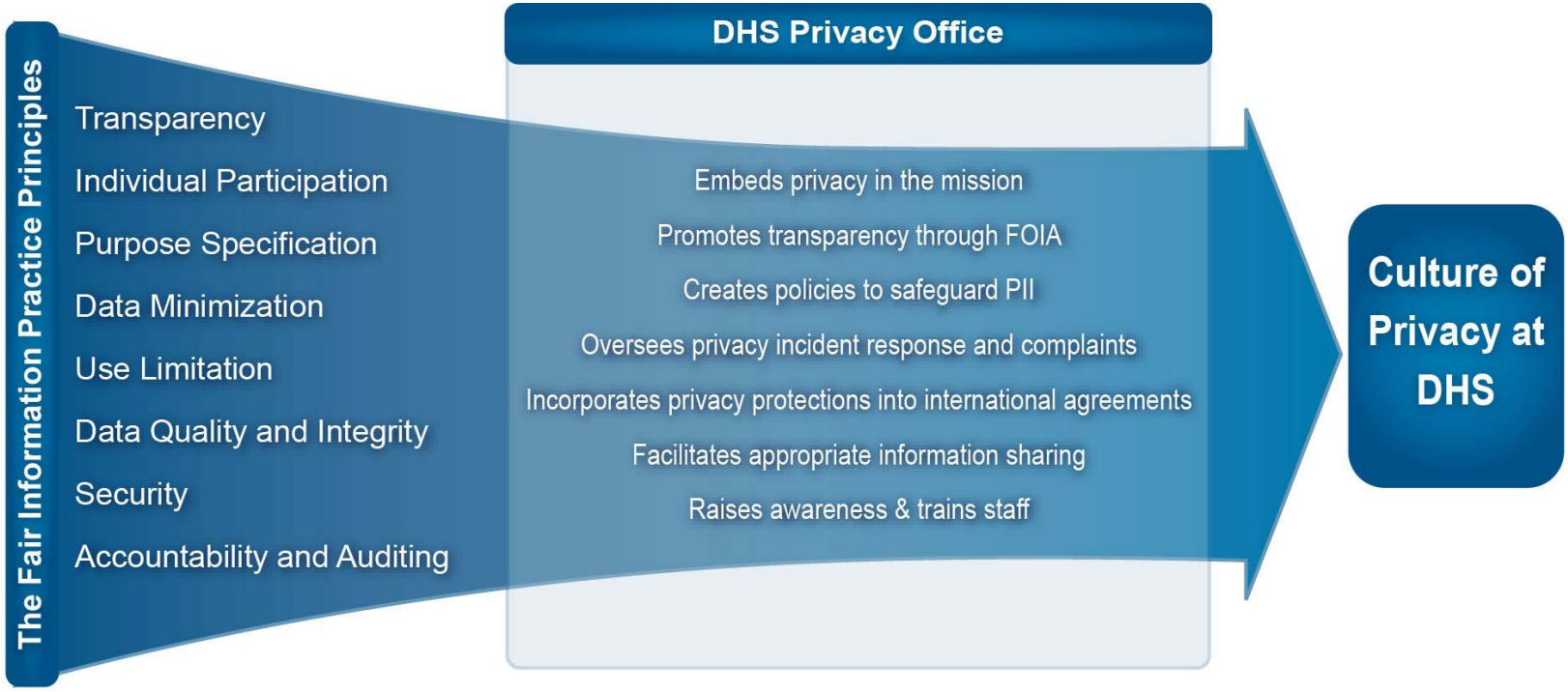
- PIA報告書のセクションごとに、下記FIPPsの各原則に合致しているかという観点から、システマティックに評価する。
- プログラムやシステムを具体的にイメージして、情報収集等が適切か等について、当該部門も交えながら、非常に長く議論する。
  - 例えば、後述のセクション2については、収集する情報がなぜ必要か、何のベネフィットがあるのか、収集する情報を減らしても目的を実現できるのではないかといった観点からレビューする。
- プライバシーとは何かといった、そもそも論には立ち返らない。

PIA(Privacy Impact Assessment:プライバシー影響評価) 5/5

○FIPPs(公正な情報取扱い8原則)

– プライバシー法を貫く8原則をベースに、DHSプライバシーオフィスがDHS用に再定義したもの。

- 透明性(Transparency)
- 目的明確化(Purpose Specification)
- 利用制限(Use Limitation)
- セキュリティ(Security)
- 個人参加(Individual Participation)
- データ最小化(Data Minimization)
- データ正確性と完全性(Data Quality and Integrity)
- 説明責任と監査(Accountability and Auditing)



PIA報告書の構成1/2 （DHSのPIAガイダンスより）

〇プログラムの概要
- 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。

〇セクション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。

〇セクション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。
  - 収集する情報を減らせば、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。
- 情報の収集源の特定。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。
- プライバシー影響分析：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。
  - 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。

〇セクション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の特定。
- プライバシー影響分析：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。
  - 透明性の原則、利用制限の原則を考慮する。

PIA報告書の構成2/2 （DHSのPIAガイダンスより）

○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：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。
  - 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：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。
  - 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：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：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。
  - 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。
- 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。
- 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。

SORN（System of Records Notices：個人情報記録システムに関する告知）

〇概要

- 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。
  - 1974年プライバシー法（合衆国法典第5編552a条）が準拠法令。具体的には、552a条のe項（4）号で規定。
  - 日本の行政機関個人情報保護法の「個人情報ファイル簿」に対応。
- SORNは連邦官報で公表される。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。

〇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）

〇SORNでの通知事項（DHSのSORNガイダンスより）

- 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

〇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。
- 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。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

- 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。
- 適用除外事項：個人への通知（SORN）、開示・訂正請求への対応、記録情報を目的達成に必要なものに限定すること。

４．カナダ（連邦）の現状

カナダ（連邦）のPIA制度概要： 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」（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）において、連邦政府機関にPIA実施を義務化。
  - TBSはPIAポリシーの付属書類として、「PIA Guidelines: A Framework to Manage Privacy Risks」を発行。
- 2010年にTBSが「Directive on Privacy Impact Assessment」（PIA指令）を策定、同年4月から施行。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PIA指令を策定した。
- 2011年3月に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）を発行。
  - 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。
  - 「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。
- 2011年12月現在、PIA指令に対応したTBSのガイドラインは未策定。

○PIAの目的（OPCへのインタビューより）

- 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。
- 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。

カナダ（連邦）のPIA制度概要： 連邦・州コミッショナーの所轄範囲

〇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」（※1）と、「個人情報保護及び電子文書法」（PIPEDA：※2）の運用を監督する。
- すなわち、連邦政府機関と、連邦・州の民間企業等を監督。

〇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。

※1：プライバシー法：1982年に制定。連邦政府機関に適用される。
※2：個人情報保護及び電子文書法（PIPEDA）：2000年に制定。連邦・州の民間分野に適用される。
また、1991年の銀行法など、民間の個別分野を規制する連邦法も別途、存在する。

カナダ（連邦）のPIA制度概要： 連邦における各機関の役割分担

〇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。指令やポリシーの策定も行う。
- PIAポリシー（2002年）やPIA指令（2010年）を策定。
- 連邦政府機関からPIA（後述のコアPIAのみ）の提出を受ける。
- コアPIAに対するコメントや承認は行わない。

〇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。
- ポリシー策定において、TBSに協力する。
- 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。政府機関にPIAに関する助言や勧告を行う。PIAの承認は行わない。

〇連邦政府機関

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

カナダ連邦におけるPIAの実施手順　1/3

〇PIAの実施手順

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、追加的なPIA（フルPIA）が必要かを決定する。

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。

⑤ TBS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。

⑥ TBSは、PIBのレビューを行い、承認し、登録する。

⑦ プログラムマネジャーは、コアPIAをOPCに提出する。

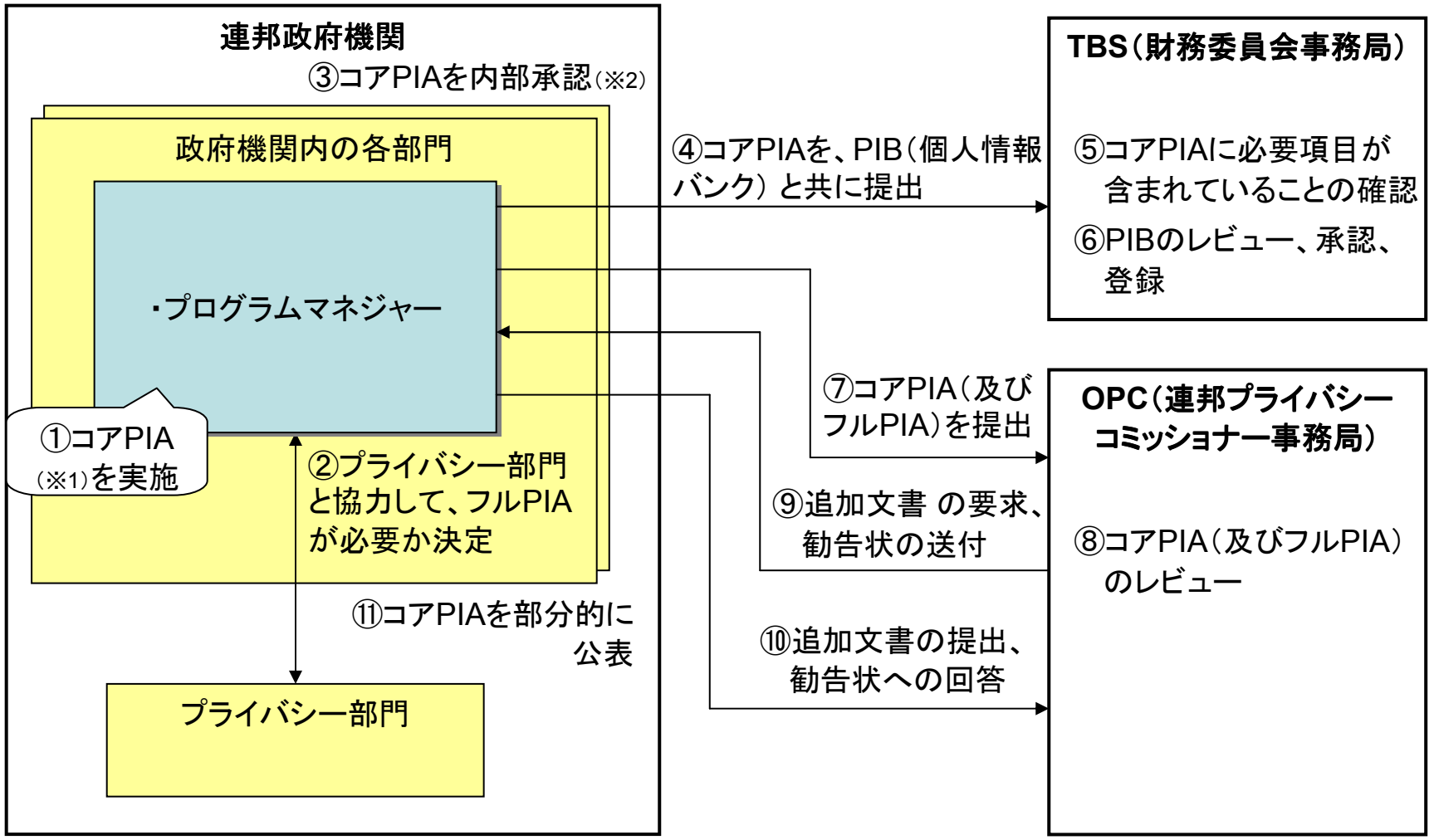
⑧ OPCは、コアPIAをレビューする。
- レビューの間、政府機関に電話やメールで相談・質問をしたり、会合を開いたり、追加的な文書を求める場合がある。

⑨ OPC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。

カナダ連邦におけるPIAの実施手順　2/3



※1：2010年のPIA指令において新たに導入された制度。
従来の「Preliminary PIA」に相当。

※2：内部承認プロセスは各政府機関で策定する。

カナダ連邦におけるPIAの実施手順　3/3

〇PIA実施手順に関する補足

- ②の補足:
  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)
- ④の補足:
  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。

〇パブリックコンサルテーションについて

- 2002年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、2010年PIA指令ではTBSによって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。

〇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。」

〇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。(米国のSystem of recordsに相当。)
- 同法の下では、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。

コアPIA（Core Privacy Impact Assessment）

〇コアPIA

- 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。
- コアPIAにおいて、さらなるPIA（フルPIA）が必要か否かを判断。

〇コアPIAの実施対象

- 新たなプログラムやアクティビティ、又は重要な変更のあるプログラムやアクティビティ
- 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（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
- 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が必要になる場合もある。

〇コア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。
  - 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。

※「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
※「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。
ex.学生に関する統計調査、退職者に関する統計調査等

コアPIAの記載内容

〇セクション1：概要とPIA開始

〇セクション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

〇セクション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）

〇セクション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

〇セクション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

〇セクション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

〇セクション7：添付文書のリスト

〇セクション8：公式な承認

PIA(コアPIA含む)の実施体制、実施期間等

○PIAの実施体制

- 理想的には以下のメンバー(OPCの意見)
  - 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、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。

○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)

- 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
  - 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。

OPCにおけるPIAのレビュー方法

〇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。
- 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
- レビュー用テンプレートを使ってレビューをする。（次頁参照）

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」に対応
- 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？
- Threat and Risk Assessmentも併せて実施されているか？
- プロジェクトの記述は完全なものか？
- どんな個人情報の要素が含まれているか？
- 情報はセンシティブなものであるか？
- 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？
- 全てのプライバシーリスクが特定されているか？
- リスクの軽減策は適切なものか？
- PIAは内部で実施されたものか？
- 十分なエグゼクティブサマリーがあるか？
- プロジェクトの根拠又はニーズは明確なものか？
- 取扱われる情報は十分に記述されているか？
- プロジェクトには具体的な法的権限付けがあるか？
- 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？
- 全てのリスクは管理可能なものか？
- 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
- カナダ規格協会の公正な情報取扱い10原則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ガイドで指定されたPIA報告書のフォーマット

〇PIA報告書のフォーマット

- 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
- 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、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

〇添付書類（PIA報告書と一緒にOPCに提出すべきもの）

- 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

複数機関が関与するPIAについて

〇連邦プライバシーコミッショナー事務局（OPC）の見解

- 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。これを「アンブレラPIA」と呼んでいる。
- アンブレラPIAを推奨する理由は、OPCガイド（2.4節）に記載。
  - 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。 等
- 必要に応じて、アンブレラPIAの下で、各機関が個別のPIAを行うこともある。
- TBS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。

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

〇ロビン・ベイリー氏（Linden Consulting代表）の見解

- 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。
  - 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。

５．カナダ（オンタリオ州）の現状

カナダ（オンタリオ州）のPIA制度概要： PIAの根拠規定

〇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。

〇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。

〇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。

カナダ（オンタリオ州）のPIA制度概要： 各機関の役割分担

〇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）

- 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。
- 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。
- 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。
- 「オンタリオ州公共サービスのためのPIAガイド」を策定。

〇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）

- 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。
- 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。

〇州の政府機関

- 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。
- プライバシーに重大な影響のある事柄についてIPAに相談。
- PIAの公開義務はない。

カナダ（オンタリオ州）のPIA制度概要： PIAの構成要素

○PIAの実施対象

- 「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
- 該当するプロジェクトの例（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

①Preliminary Analysis（準備分析）

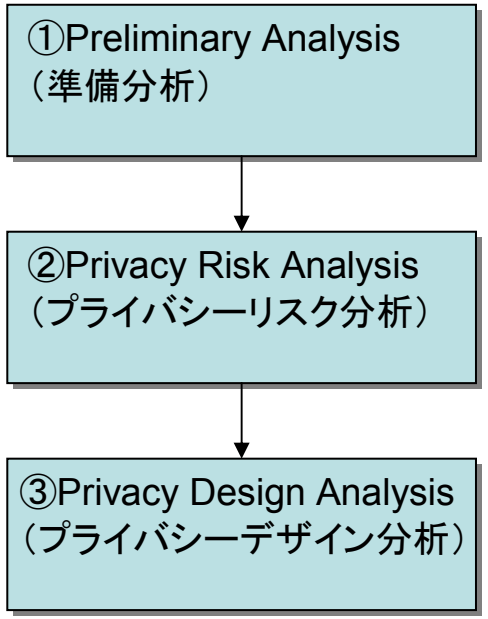
- PIA実施対象となる全てのプロジェクトに対して実施し、さらなる分析が必要か否かを判断するためのツール。

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。

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。



Preliminary Analysis(準備分析)とPrivacy Risk Analysis(プライバシーリスク分析)

○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)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。
- Preliminary Analysisは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。

○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。
- 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。
- 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。
- 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。

Privacy Design Analysis（プライバシーデザイン分析）

○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。
- 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。
- 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。

※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

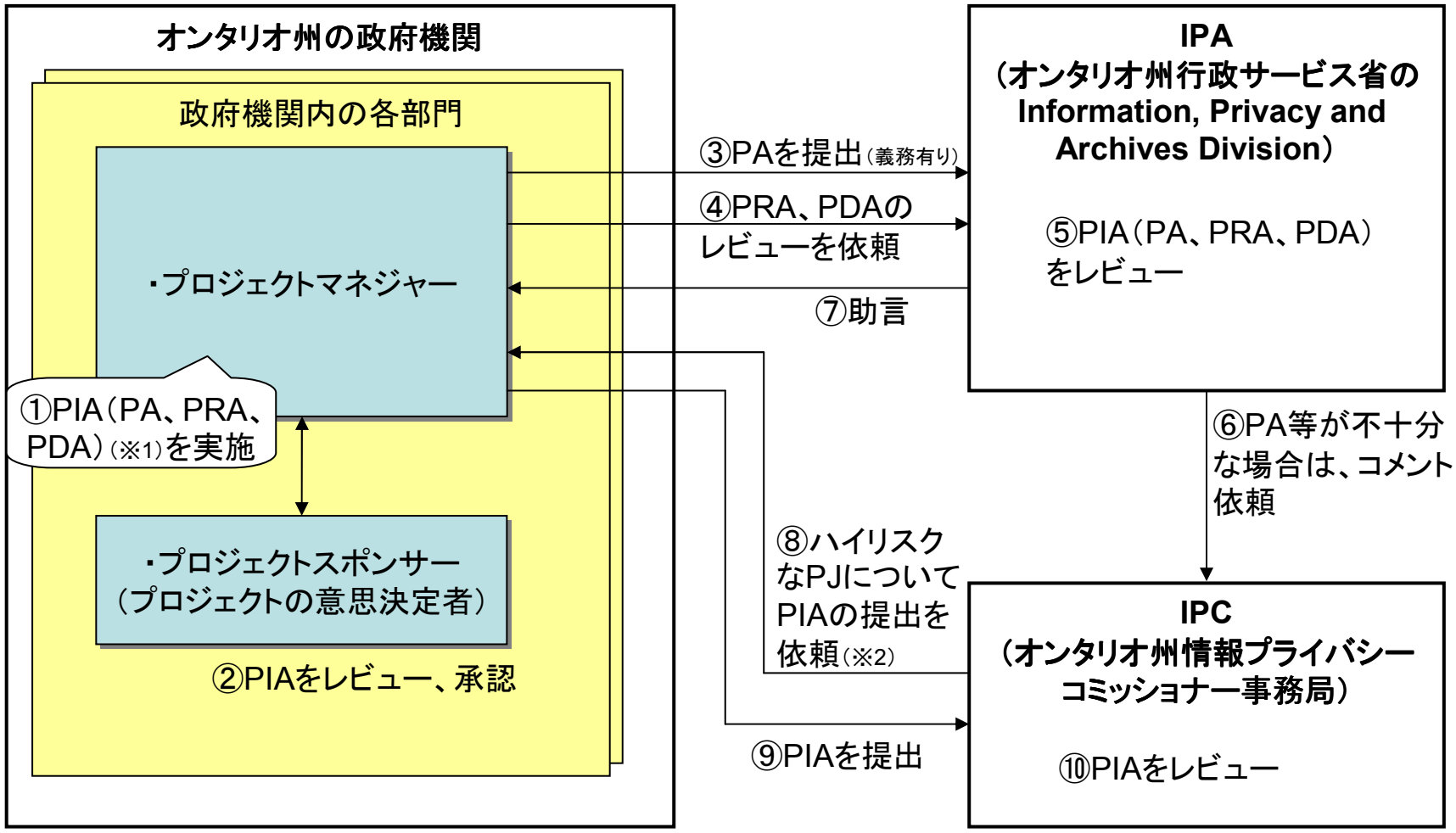
「概念（Concept）」→「定義（Definition）」→「計画（Planning）」→「実施（Implementation）」→「完了（Close-Out）」の5つのフェーズから成る。

①Preliminary Analysis（準備分析）

②Privacy Risk Analysis（プライバシーリスク分析）

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

カナダ・オンタリオ州におけるPIAの実施手順



※1

PA： Preliminary Analysis
PRA： Privacy Risk Analysis
PDA： Privacy Design Analysis

※2：IPCには命令権限もある。

PIAの承認、パブリックコンサルテーション等

○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（※）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。

※ゲーティッドファンディング ：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している。

○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。
  - ex. トロント郊外への監視カメラの設置、オンタリオ州のIC運転免許証等

○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（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。

プライバシー影響評価(PIA)各国比較表　1/2

	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等の懸念を踏まえ、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

※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

プライバシー影響評価(PIA)各国比較表　2/2

	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
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

※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