情報ネットワーク法学会
第14回研究大会

第4分科会
プライバシーに関する
国際標準化の動向と課題

村上康二郎
東京工科大学准教授

Copyright © 2014 Yasujiro Murakami, All rights reserved.

会場について

ハッシュタグは
#inlaw4
をお使いください

- 会場内では飲み物をお飲みいただけます。食事はご遠慮ください。

- 会場内での撮影・録音・録画を禁止いたします。報道関係については、それらの許可について受付でお済ませください。

- 本日から1週間以内にインフルエンザなどの感染症の発症があった場合には、学会までお知らせください。全参加者にその旨をお知らせします。

発言の公開について

ハッシュタグは
#inlaw4
をお使いください

- 分科会について学会活動記録のために録画しております。記録については録画内容が公開されます。また、発言を原稿化した文章が学会誌に掲載され、書籍として発刊されます。録画は会場後方から登壇者を主として撮影します。原稿化する文章には、登壇者以外の発言は匿名での記載となります。

- ご自身のご発言であっても、それを非公開・非掲載にするご要望には沿えません。なお、学会が不適切と判断したご発言については、ご本人の了解を得ずに削除する場合があります。あらかじめご承知置きください。

ソーシャルメディアへの投稿

ハッシュタグは
#inlaw4
をお使いください

- ツイッターなど、ソーシャルメディアへの投稿については、特に制約はございません。

- 投稿する場合には、別会場向けの投稿と区別するために、以下のハッシュタグをお使いください。

#inlaw4

- **inlaw（3文字目は小文字のエル）**に続けて、数字の **4**（よん）

全体の進行

Ⅰ　はじめに（村上康二郎）

Ⅱ　プライバシーに関する国際標準化の全体的動向、PIAに関する動向と課題（29134）など（村上康二郎）

Ⅲ　経済産業省における各種プロジェクトの経緯など（森亮二）

Ⅳ　消費者向けオンラインサービスにおける通知または同意・選択に関するガイドライン、今後の国際標準化の予定など（崎村夏彦）

Ⅴ　PII保護のための行動規範（29151）など（佐藤慶浩）

Ⅰ　はじめに　－趣旨説明－

- プライバシー・個人情報保護については、EU一般データ保護規則、米国消費者プライバシー権利章典、OECDガイドラインなどが注目されている。

- ISO/IEC JTC1 SC27WG5において、プライバシー関連の国際標準の作成が行われている。プライバシーフレームワーク（29100）、プライバシー影響評価（29134）など重要なものが多い。

- ISOにおける標準化は、我が国では十分に認知されていない。　→　まずは、プライバシーに関する国際標準化動向に関心を持っていただきたい。

「プライバシー国際規格研究会」について

① 主査

村上康二郎（東京工科大学）

② メンバー

佐藤慶浩（日本HP）
新保史生（慶應義塾大学）
六川浩明（弁護士）
小林慎太郎（NRI）
板倉陽一郎（弁護士）
坂下哲也（JIPDEC）
小堤康史（データ通信協会）
崎村夏彦（NRI）
小向太郎（情報通信総合研究所）
宮内　宏（弁護士）
藤村明子（NTT）
河井理穂子（埼玉工業大学）
黒坂達也（JIPDEC）

Ⅱ プライバシーに関する国際標準化の全体的動向

ISO/IEC 29100
Information technology - Security techniques - Privacy framework

ISO/IEC 29101
Information technology - Security techniques - Privacy architecture framework

ISO/IEC 29134
Information technology - Security techniques - Privacy impact assessment - Methodology

ISO/IEC 29151
Information technology - Security techniques - Code of practice for PII protection

New SP
User friendly online privacy notice and consent

1. ISO/IEC 29100 Privacy framework

1 Scope
2 Terms and definitions
3 Symbols and abbreviated terms
4 Basic elements of the privacy framework
  4.1 Overview of the privacy framework
  4.2 Actors and roles
  4.3 Interactions
  4.4 Recognizing PII
  4.5 Privacy safeguarding requirements
  4.6 Privacy policies
  4.7 Privacy controls

ISO/IEC 29100 Privacy framework

5 The privacy principles of ISO/IEC 29100

- 5.1 Overview of privacy principles
- 5.2 Consent and choice
- 5.3 Purpose legitimacy and specification
- 5.4 Collection limitation
- 5.5 Data minimization
- 5.6 Use, retention and disclosure limitation
- 5.7 Accuracy and quality
- 5.8 Openness, transparency and notice
- 5.9 Individual participation and access
- 5.10 Accountability
- 5.11 Information security
- 5.12 Privacy compliance

Annex A

PII（Personally Identifiable Information）とは

PII
any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal

EU Data Protection Directive (19951123)
'personal data ' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified , directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

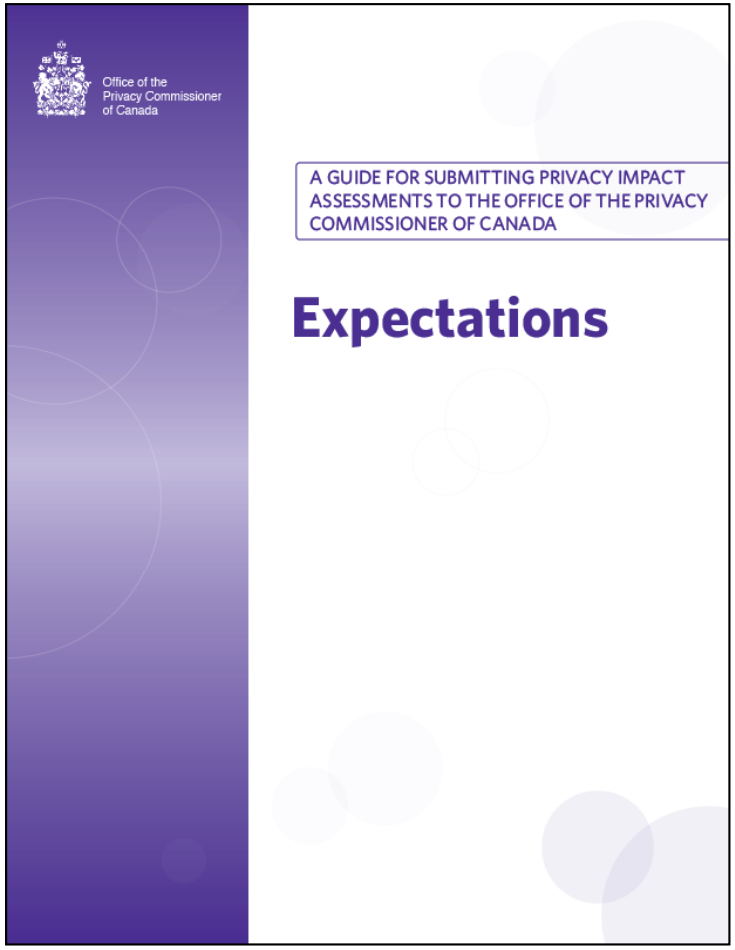
EU General Data Protection Regulation (20140312)
'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, unique identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person

2. ISO/IEC 29134 PIA methodology

前提知識：PIAとは

PIAには各種の定義がある。

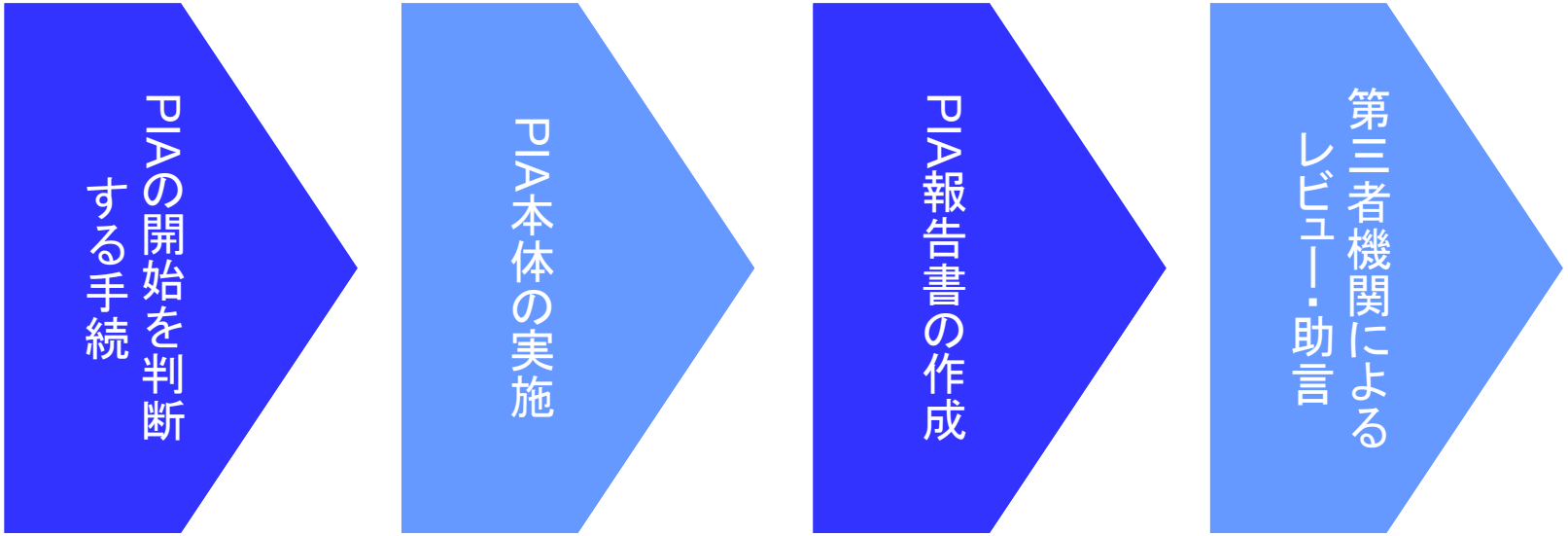
「個人情報を伴うイニシアティブがプライバシーリスクをもたらすかどうかを判断するのに役立ち、そのようなリスクを計測し、記述し、数量化し、プライバシーリスクを除去するか受け入れ可能なレベルまで緩和するための解決策を提案するもの」
（Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada）



http://www.priv.gc.ca/information/pub/gd_exp_201103_e.pdf

PIAの一般的な手続の流れ

PIAの内容、手続などは国ごとに異なっているが、ある程度共通している部分もある



しきい値評価、
スクリーニング
質問など

・プライバシーリスクの特定、分析、評価
・パブリックコンサルテーションなど

報告書は後に
公開されること
が多い

レビューはなく
助言だけの場合
もある

PIAの対象となる情報の範囲
ーPIAの対象となるプライバシーとは何かー

- PIAの対象領域

  国際的に、公的部門から民間部門に拡大する傾向が見られる

- PIAの保護対象

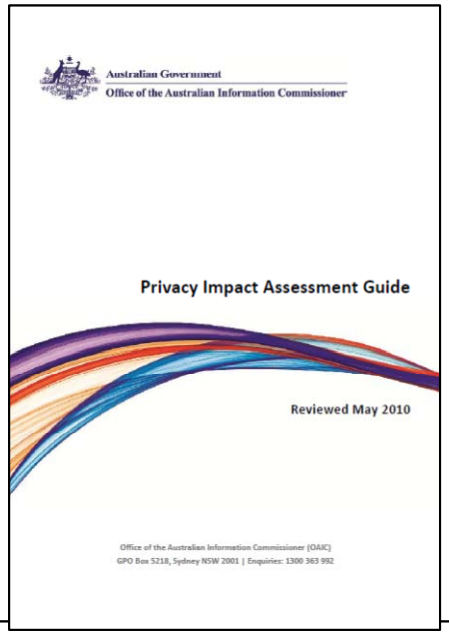
  多くの国において、PIAは情報プライバシーまたはデータ・プライバシーの保護を主たる目的にしている

  → 情報プライバシーや個人情報保護に関する法律・ガイドラインを遵守しているかというコンプライアンスチェックが基本になっていることが多い

PIAの対象となるプライバシーとは①

Australia : Privacy Impact Assessment Guide

- 情報のプライバシー
- 身体のプライバシー
- 領域のプライバシー
- 通信のプライバシー



UK : Privacy Impact Assessment Handbook

- 個人情報のプライバシー
- 身体のプライバシー
- 行動のプライバシー
- コミュニケーションのプライバシー

PIAの対象となるプライバシーとは②

David Flaherty

Privacy Impact Assessments: an essential tool for data protection, in THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT 265 (2001)

http://tobaccotrial.blogspot.jp/2013/05/day-145-four-seasosn-later-david.html

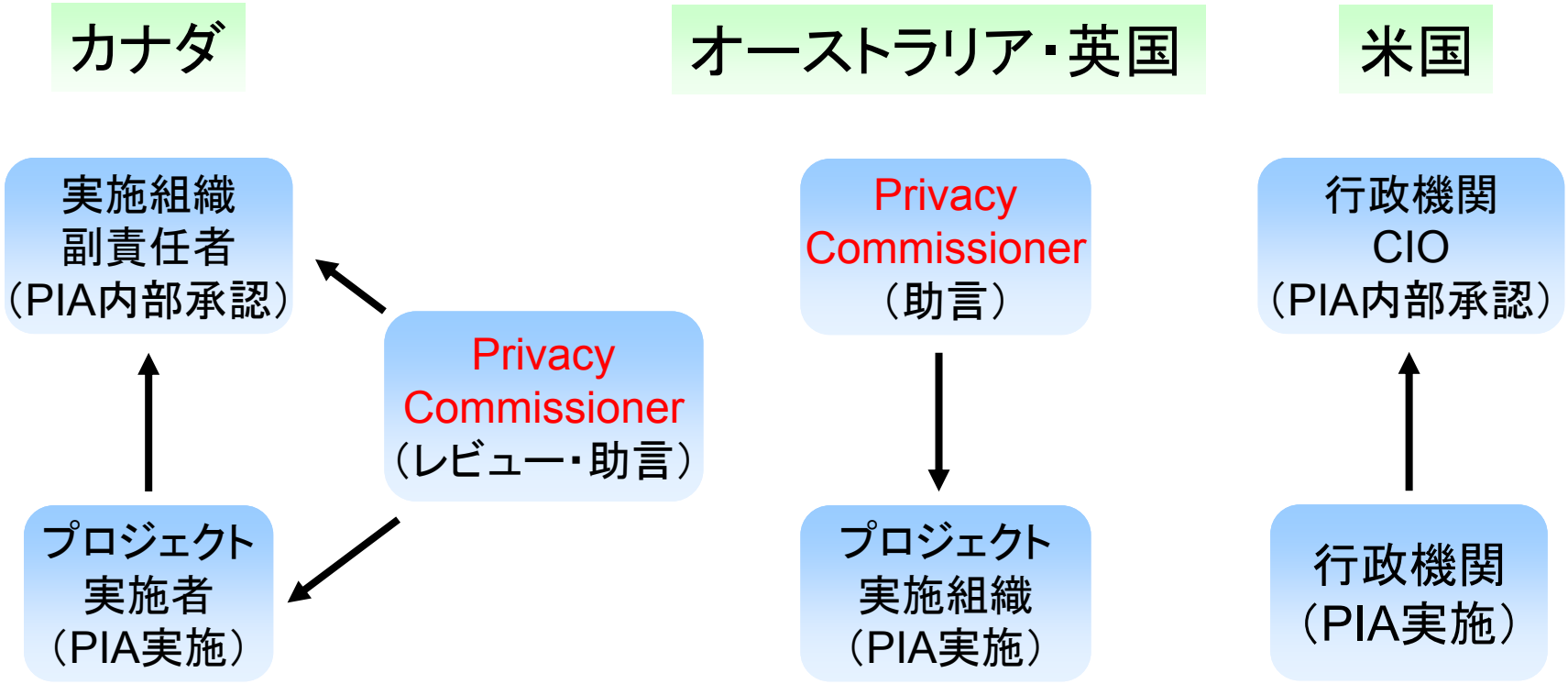
An important secondary goal is to meet the privacy expectations of the public with respect to moral and ethical considerations.

PIAの重要な第2の目的は、道徳的・倫理的観点から、プライバシーに対する公衆の期待を満たすことである

→ 法律の対象となる「個人情報」だけではなく、パーソナルデータや準個人情報のようなものもPIAの対象に含めるという案

第三者機関の関り方

多くのPIA実施国で、プライバシーコミッショナーのような第三者機関が何らかの形でPIAに関わっている。第三者機関がPIAのガイドラインやハンドブックを作成したり、PIAに対するレビュー・助言を行っている。

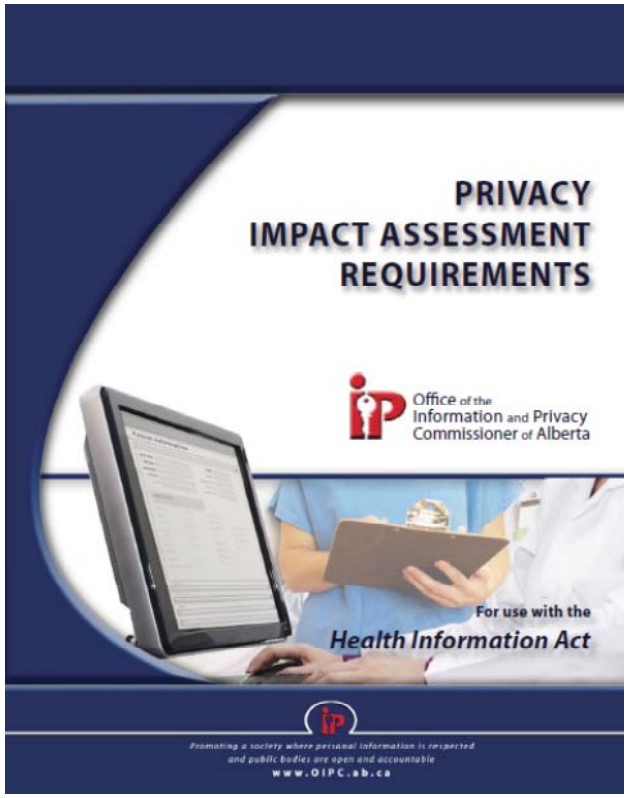


PIAに対する第三者機関の承認

主要なPIA実施国では第三者機関はPIAの「承認」を行っていない。

カナダのブリティッシュコロンビア州・アルバータ州では、「受諾（accept）」をしているが「承認（approve）」はしていない。

Because the onus always remains on the organization to ensure adequate levels of privacy protection, as required in the applicable legislation, a PIA will not be "approved". (Office of the Information and Privacy Commissioner of Alberta, PIA Requirements)



http://www.oipc.ab.ca/Content_Files/Files/PIAs/PIA_Requirements_2010.pdf

PIAに関する国際標準化の動向

ISO/IEC JTC1 SC27WG5において、PIAに関する国際規格の作成が進行中。PIAに関する複数の国際標準を策定する予定で、現在は、PIA Methodology（ISO29134）について検討。当初、リスクマネジメント規格（ISO31000）をもとにWDが作成されたが、その後方向転換をした。

1.) PIA– the methodology
2.) PIA – requirements on the system description
3.) PIA – protection baseline
4.) PIA – for governmental systems
5.) PIA – for Finance systems (replacing ISO 22307:2008)
6.) PIA – for RFID technology systems
7.) PIA – for Cloud computing systems
8.) PIA – for Social Network community systems
9.) PIA – for Smart Metering systems

Rapporteur's Report on WG 5 Study Period on Privacy impact assessment (2012)

ISO 31000 Risk management

http://www.kinokuniya.co.jp/f/dsg-01-9784542402386

http://www.kinokuniya.co.jp/f/dsg-01-9784542701625

PIAとISO31000の関係

Summary of National Body comments on SC 27 N12550 -- Text for ISO/IEC 2nd WD 29134 (GB1)

The reader might assume that PIA and privacy risk management are one and the same thing. However, they are not, nor are they understood that way. PIA, ・・・, is a process for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts. Privacy risk management, ・・・, is a methodology for assessing and managing privacy risks. The methodology does not particularly focus on stakeholder engagement (unlike PIA).・・・

Indeed, the term PIA includes a set of steps or policy actions that have much to do with stakeholder consultation, publication and third-party review. PIAs are policy-oriented, whereas privacy risk management is focused on ascribing numbers to particular threats, vulnerabilities and consequences.

Furthermore, a privacy impact assessment should address all types of privacy, whereas the privacy risk management methodology described here, based on the CNIL privacy risk management Methodology, is focused on the protection of data and not on all (seven) types of privacy・・・

（補足） 我が国におけるPIAの課題
（1） 公的部門におけるPIAの課題

特定個人情報保護評価

行政機関の長等（行政機関の長、地方公共団体の機関など）は、特定個人情報ファイルを保有しようとするときは、当該**特定個人情報ファイルを保有する前**に、**特定個人情報保護評価を実施**することが原則義務付けられる。（番号法第27条第1項）

特定個人情報保護評価とは

- 特定個人情報ファイルの保有・変更にあたり、プライバシーや特定個人情報へ及ぼす影響を事前に評価し、その保護のための措置を講じる仕組みをいい、米･加･豪･英等の諸国で行われているプライバシー影響評価（Privacy Impact Assessment）に相当するもの。
- 具体的には、特定個人情報を保有することでどのようなリスクがあり、そのリスクをどのようにして軽減・緩和しているかを、自ら所定の様式の評価書に記載し、公表するもの。

特定個人情報保護評価の対象

- 特定個人情報ファイル（個人番号をその内容に含む個人情報ファイル）を保有する業務･システム

内閣官房「社会保障･税番号制度の概要」（平成25年11月）

① 対象となる領域、情報の範囲

- 情報保護評価の対象は基本的に公的機関に限られる（例外的に、情報提供ネットワークシステムを使用する事業者が対象となるのみ）。
- 対象となる情報は、「特定個人情報ファイル」（個人番号を内容に含む個人情報ファイル）のみ（番号法27条）。個人情報一般を対象とする諸外国のPIAと大きく異なる。
- 番号法の附則6条2項によって、特定個人情報保護委員会の権限拡大（特定個人情報から個人情報一般）に関する検討が予定されている。

→ ・委員会の権限拡大に伴って情報保護評価の対象も拡大されるのかがよく分からない

② しきい値評価の基準

情報保護評価の実施の仕組み

参考資料2

情報保護評価の必要性を判断する

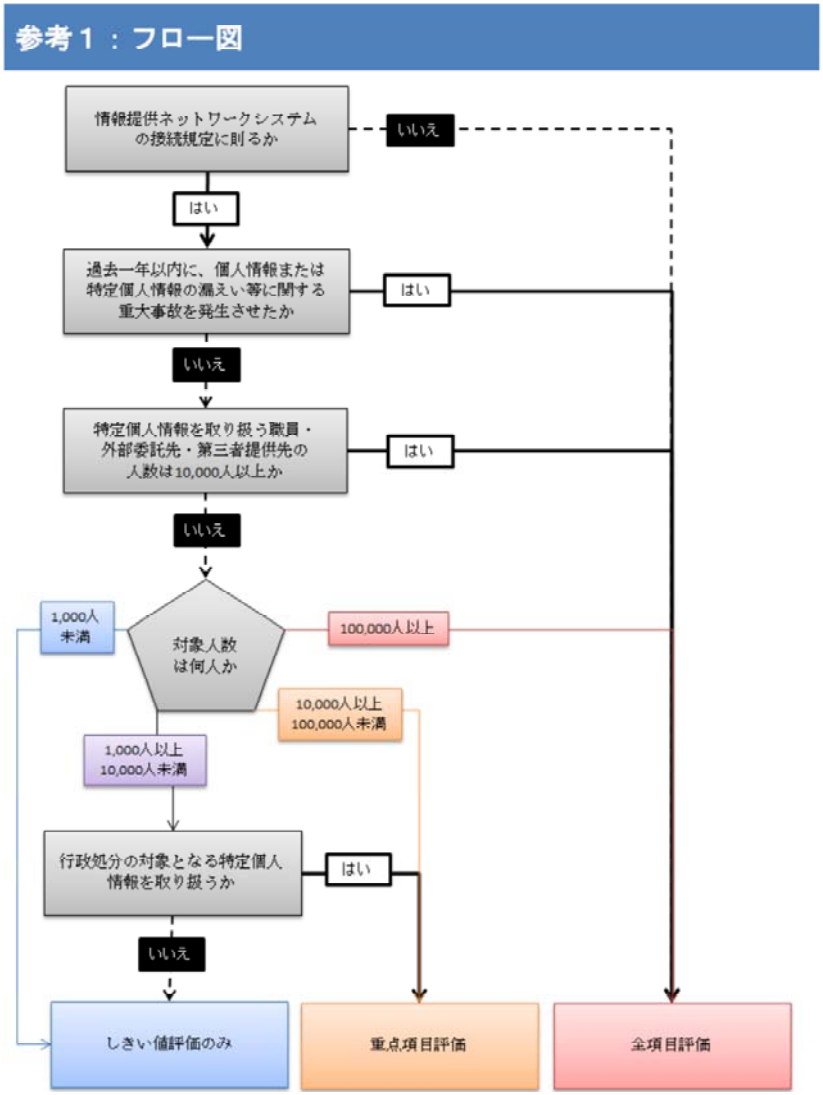
(しきい値評価)

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

内閣官房「情報保護評価サブワーキンググループ」配布資料

情報保護評価（しきい値評価）書

- 現状の「情報保護評価（しきい値評価）書」では、評価基準が特定個人情報を扱う者の人数（10000人以上か）や、対象人数（10000人以上か、100000人以上か）などの量的基準に偏っている。
- 諸外国のPIAでは個人情報の機微性など質的基準も重視されているため、この点については検討の余地が残されているものと考える



http://www.cas.go.jp/jp/seisaku/jouhouwg/hyoka/pdf/sisin_siryou1.pdf

③ 特定個人情報保護委員会の承認権限

特定個人情報保護委員会

※設置時期→2014年（平成26年）1月1日

任務

個人番号その他の特定個人情報の有用性に配慮しつつ、その適正な取扱いを確保するために必要な措置を講じること

組織

○委員長1名・委員6名（合計7名）の合議制
（個人情報保護の有識者・情報処理技術の有識者・社会保障又は税制の有識者・民間企業の実務に関する経験者・地方六団体の推薦者を含む）
○委員長・委員は独立して職権を行使 （独立性の高い、いわゆる3条委員会）
○任期5年・国会同意人事

主な所掌事務

監視・監督	特定個人情報保護評価に関すること	広報・啓発	苦情処理	意見具申
○指導・助言 ○法令違反に対する勧告・命令（命令違反には罰則） ○求報告・立入検査（検査妨害には罰則） ○情報提供ネットワークシステムの構築等に関する措置要求	○特定個人情報保護評価に関する指針の作成・公表 ○評価書の承認	特定個人情報の保護についての広報・啓発	苦情の申出についてのあっせん	内閣総理大臣に対する意見具申

監視・監督 → 行政機関・地方公共団体・独立行政法人等
指針 → 行政機関・地方公共団体・独立行政法人等
評価書 ← 行政機関・地方公共団体・独立行政法人等
広報・啓発 → 民間事業者
あっせん → 個人
苦情 ← 個人
意見 → 内閣総理大臣

18

内閣官房「社会保障・税番号制度の概要」（平成25年11月）

第三者機関の承認権限の是非

- 番号法では、特定個人情報保護委員会は、情報保護評価書に対する承認権限を有することになっている。
- 主要なPIA実施国で第三者機関が承認を行っている例は存在しない。市民から苦情が来たり、何か問題が発生したりした場合に、追加措置を要求したり、勧告を行ったりすることが難しくなるのではないか。
- 情報保護評価SWGは、諸外国の第三者機関が行政から独立しているのに対し、日本の特定個人情報保護委員会は行政機関の一部であるといった理由づけを行っている。

→ 理論面のみの検討になっており、実質面の検討が不十分ではないか

小泉雄介「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）33頁も参照

（2） 民間部門におけるPIAの課題

一部の事業者などによる自主的な取組みがあるが、単なる自主的な取組みでは信頼性の点で限界がある

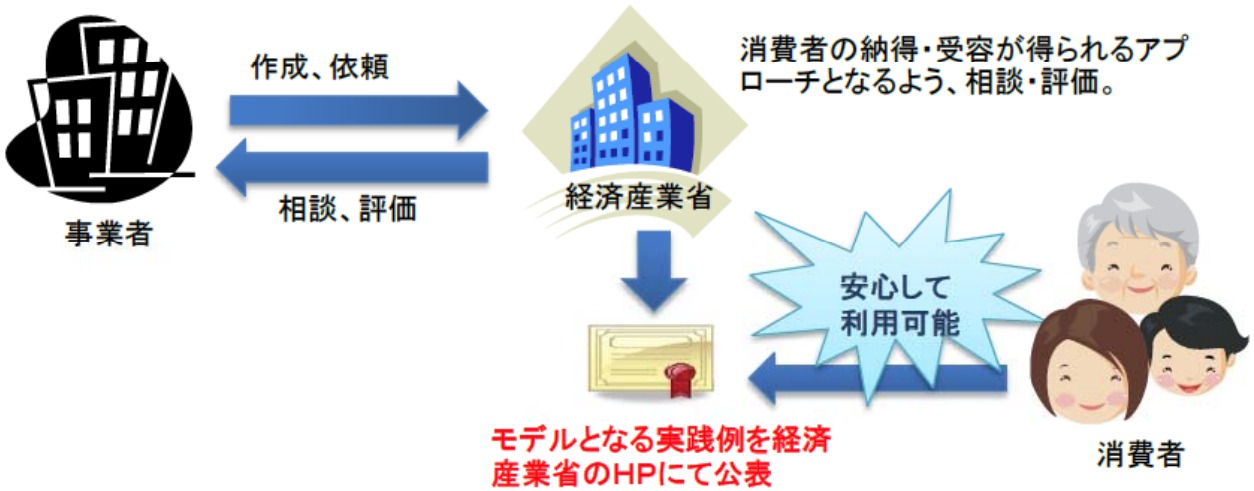
① ISOなどの国際標準に準拠して実施する方法

→ 何らかの形で公的機関が関与した方が信頼が得やすいのでは

② 各省庁が関与してPIAの実施を推奨する方法

経産省「パーソナルデータの利活用に関する事前相談評価」（日本版PIA）

→ PIAとは異なるが、将来的に日本版PIAを実現しようとする一つの試み



経産省「パーソナルデータの利活用に関する事前相談評価」ニュースリリース

③ 権限を拡大された個人情報保護委員会が関与する方法

- 個人情報保護委員会の権限を民間部門にも拡大する
- 個人情報保護委員会が民間用のPIAガイドライン（情報保護評価指針）を作成し、公表する
- 個人情報保護委員会は場合によってPIAに対する評価や助言を行う
- 諸外国におけるPIAの動向からすると、個人情報だけでなくパーソナルデータや準個人情報も対象に含めるという案が考えられる

パネルの論点

1　プライバシーの規格をISO/IEC JTC1 SC27WG5で策定することの是非

2　プライバシーとセキュリティの関係（プライバシーをセキュリティの一部と考えてよいか）

3　日本の特定個人情報保護評価を国際的視点で見た場合の問題（諸外国の一般的なPIAと日本の情報保護評価の相違）

4　消費者向けオンラインサービスにおいて実質的な本人同意をいかにして実現するか（情報共有標準ラベルやアイコンの課題）

→　分かりやすさと正確性、煩雑か、消費者の意見、記載の順序

5　取得ではなく、利用について本人同意をとればよいと考えるか