6E-1

プライバシー影響評価実施における社会制度の相違を考慮したハンドブックの開発

高坂 定† 石田 茂† 横山 完† 瀬戸 洋一†

†産業技術大学院大学

1. はじめに

個人情報の電子化が進み，プライバシーリスク管理の重要性が増している．プライバシー影響評価（PIA：Privacy Impact Assessment）は，個人情報の収集を伴うシステムの導入，改修の際に，プライバシー問題の回避あるいは低減を目的としてプライバシーリスクを「事前」に評価するリスク管理手法である[1]．PIA を実施する上では，国際標準 ISO22307 を基に各国の事情に合わせた実施体制・手順の明確化が必要である．本発表では，日本で PIA を実施する際に利用する諸外国との社会制度の相違を考慮した，PIA ハンドブックの概要について報告する．

2. プライバシー影響評価の概要

プライバシー影響評価の国際標準である ISO22307 は，プライバシー保護の目的では金融業界に限定していないため，他の業種にも適用可能である．ISO22307 の PIA への要求事項は，以下の 6 項目がある．

①PIA 計画，②PIA 評価，③PIA 報告が PIA の実施手順に相当し，④十分な専門知識，⑤独立性と公共性の程度，⑥対象システムの意思決定時の利用は，PIA の実施体制に関する要求である．

①PIA 計画： 適用範囲の定義，実施者に必要な専門知識分野の特定，適用されるプライバシーについての法令，規格の特定等と対象システムの調査を行い，実施計画書を作成する．

②PIA 評価： PIA 計画で定義した PIA の実施対象範囲について，プライバシーリスクを洗い出し，指摘事項とその指摘事項に対する推奨案を作成する．この作業は，プライバシーに関する専門知識を持ったメンバーが行う．

③PIA 報告： 対象システムについて関係者間でレビューを行うため，評価，分析した事項と必要であれば提案事項を文書化する．

Development a Privacy Impact Assessment handbook for social system in Japan

Sadamu TAKASAKA†, Shigeru ISHIDA†, Mamoru YOKOYAMA† and Yoichi SETO†

†Advanced Institute of Industrial Technology

④十分な専門知識： PIA を実施するためには，PIA 実施プロジェクトのメンバーに対して十分な専門知識を求めている．最低でも，法律分野，IT インフラストラクチャ，業務プロセスについての専門知識を求めている．

⑤独立性と公共性： PIA を実施するにあたって PIA の実施者に対して，対象システムに関する利害関係者に対し独立性と公共性を保ち，中立性の確保を求めている．

⑥対象システムの意思決定： PIA 実施結果はリスク対策時の対象システムの意思決定における利用を求めている[2]．

3. プライバシー影響評価ハンドブックの分析

日本版プライバシー影響評価ハンドブックを開発するに当たり，諸外国(英国，米国，ニュージーランド，カナダ，オーストラリアの 5 ヶ国)の公的機関から発行されたハンドブックの構成項目を比較したものが表 1 である．

表 1 PIA ハンドブック構成項目比較表

構成項目/PIAガイド	英国/ICO	米国/DHS	NZ/PCO	カナダ/PCO	豪州/PCO
発行日	Jun-09	Jun-10	Oct-07	Aug-02	May-10
①PIAプロセス	■	■	■	■	■
②プライバシーリスクに関わる質問	■	■	■	■	■
③PIA実施組織（民間企業、政府機関）	■		■		■
④プライバシーのタイプ（情報他）					■
⑤リスク管理	■	■		■	■
⑥リスクの特定	■		■	■	■
⑦リスク対策			■		
⑧PIAの効果	■		■	■	■
⑨外部ステークホルダーとの協議	■				■
⑩PIA報告書公表	■	■	■	sumary	■
⑪予備PIA	■	■		■	■
⑫PIA報告書の推奨構造	■	■	■	■	■
⑬プロジェクトライフサイクルで実施	■	■	■		■
⑭コンプライアンスチェック	■			■	■
⑮審査と監査		■	■	■	
⑯PIAと予算の関係	■	■		■	
⑰PIA報告書の説明責任		■		■	
⑱ISO22307要求事項	■	■	■	■	■

凡例 ICO:Information Commissioner's Office PCO:Ofice of Privacy Commissioner

3.1 各国のハンドブック構成と特徴

5 カ国のハンドブックの構成項目は 18 項目であった．全ての国で共通の構成項目は，①PIA プロセス，②プライバシーリスクに関わる質問，⑩PIA 報告書公表，⑫PIA 報告書の推奨構造，⑤リスク管理（⑥プライバシーリスクの特定，⑦リスク対策含めて），⑱ISO22307 要求事項 であ

る．4 カ国で記述されている構成項目は⑧PIA の効果，⑪予備 PIA，⑬プロジェクトライフサイクルで実施 である．

各国の構成項目の特徴は以下のとおりである．

・英国は，14 項目を網羅的に記述し，PIA プロセスの詳細やプライバシー関連事項の記述もしており、内容が充実している．

・ 米 国 は ， DHS(Department of Homeland Security)のハンドブックで，PIA の実施が法律で義務化されている．PIA のテンプレート作成から始まり，具体的な評価項目の記述が中心で、省庁の事情を考慮したものとなっている．

・ニュージーランドは，プライバシー法を遵守するための評価項目と報告内容を詳細に記述している．その他は英国に類似しているが，関連事項の記述はない．

・カナダは，米国に類似しているが，PIA 実施組織を限定していない．

・オーストラリアは，英国と同じ 14 項目を記述しているが，⑯PIA と予算の関係がなく④プライバシーのタイプ（情報他）が含まれている．

③PIA 実施組織は，対象組織として民間企業と政府機関があるが実施手順は無く，日本にあるような公共性の高い民間企業の記述はない．

3.2 日本における PIA 実施の課題

日本で PIA を実施するためには，実施組織を考慮した実施手順が必要で，以下の課題がある．

①中立的な立場で助言，勧告できる組織が存在しない．

②個人情報保護法は存在するが，PIA の実施を義務付け，実施体制を規定する法律がない．

③マニュアルが未整備なため実施者の評価能力や志向に左右され，評価の中立性が保証されない等の問題が生じることが考えられる．

4. プライバシー影響評価ハンドブックの提案

前述の課題に対応するために，日本における社会制度を考慮し ISO22307 に準拠した，「公的分野」，「公共性の高い事業分野」，「民間分野」の 3 つのパターンの実施体制で，PIA を実施するためのハンドブックの開発が必要となる．

日本版ハンドブックの構成は，諸外国の構成項目を参考として，日本の社会状況に合わせた以下の構成を提案する．

・１章 はじめに～ハンドブックの目的，適用分野，利用者と各章の概説

・2 章 プライバシー影響評価 PIA とは～PIA の概要，プライバシーリスク，プライバシー保護の関わる規格と法制度

・3 章 プライバシー影響評価実施のための法的根拠と体制～法的根拠と体制，ISO22307 の実施要求事項

・4 章各国におけるプライバシー影響評価 PIA 実施例～実施状況，実施課題と対策，PIA 実施体制

・5 章 プライバシー影響評価 PIA 実施フレームワーク～実施フレームワーク，実施プロセス，全体フロー，予備 PIA，簡易 PIA，詳細 PIA

・6 章 おわりに

・添付資料～個人情報保護ガイドライン，諸外国の PIA 実施状況，PIA に関係するセキュリティ標準規格，評価シート例，プライバシー影響評価実施マニュアル

今後は，実施体制が「公的分野」では厳密な評価判定と監視，「公共性の高い事業分野」では中立的評価とコンサル，「民間分野」では経営判断とコンサル を考慮し，本ハンドブックを基に PIA 実施マニュアルを作成してゆく．

5. おわりに

本発表は，諸外国で PIA 実施において利用されているハンドブックを分析し、日本の PIA 実施組織で利用する PIA ハンドブックの構成について検討した．その構成項目として，PIA プロセスに加えて PIA の理解を助けるためプライバシー関連事項についても記述した．さらに，PIA の実施手順は，実施の法的根拠と実施体制により異なるため，実施体制が「公的分野」，「公共性の高い事業分野」，「民間分野」による実施手順についても記述を加えた．

日本では，社会保障・税番号制度に関連して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として情報影響評価（PIA 相当）の実施が予定されている．

しかし，PIA が十分に認知されておらずなじみが薄いものと考えられるため，新しいシステムの導入や既存システムの改変などの際に，本ハンドブックが PIA 実施の手助けになる．

参考文献

[1] 瀬戸洋一，六川浩明，新保史生，村上康二郎，伊瀬洋昭，プライバシー影響評価 PIA と個人情報保護，中央経済社，2010.3

[2] 石田 茂，高坂 定，横山 完，瀬戸 洋一，日本におけるプライバシー影響評価の実施に関する提案 信学技報 2011.11

[3] PIAF， A Privacy Impact Assessment Framework for data protection and privacy rights :Prepared for the European Commission Directorate General Justice，2011.9