Computer Security Symposium 2017
23 - 25 October 2017

各国におけるプライバシー影響評価の導入状況の分析

長谷川久美†1　瀬戸洋一†1

概要：
現在，多量の個人情報がシステムに収集，処理，保管されている．官民問わず，個人情報の利活用が盛んである．要配慮個人情報を扱うシステムや国境を越えた個人情報の流通を前提としたシステムもあり，個人情報を安全に管理するための体制の構築が必要とされている．各国では個人情報保護の枠組みが規定されている．例えば，EU では一般データ保護規則が施行され，データ保護影響評価（プライバシー影響評価）の実施が義務化された．日本では，番号法に基づいて特定個人情報保護評価が義務付けられた．本稿では，EU をはじめとする各国のプライバシー影響評価の導入状況を分析する．

キーワード：一般データ保護規則，個人情報，データ保護影響評価，特定個人情報保護評価，プライバシー影響評価

Analysis of adoption of Privacy Impact Assessment in each country

Kumi Hasegawa†1　Yoichi Seto†1

Abstract:
At present, a lot of personal information is collected, processed, and stored in the system. The utilization of personal information is promoted in the public and private sectors. There is also a system that treats Special care-required personal information and a system that premises distribution of personal information across national borders, and it is necessary to establish a system for safely managing personal information. In each country, a framework for protection of personal information is stipulated, for example, General Data Protection regulation were enforced in the EU, and implementation of data protection impact assessment (privacy impact assessment) was mandated. In Japan, the specific personal information protection assessment is required by the National ID Act. In this paper, we analyze the privacy impact assessment of EU and other countries.

Keywords: data protection impact assessment, EU general data protection regulation, privacy impact assessment, personal information, special care-required personal information

1. はじめに

現在，多種多量の個人情報が日常的に収集，蓄積，解析されている．インターネット利用を前提とした電子商取引や SNS（Social Networking Service）では，国境を越えた個人情報の収集を伴うビジネスが展開されている．また，IoT（Internet of Things）の進展により，防犯カメラとして使用されるネットワークカメラの撮影画像など，収集した情報をマーケティングや人流解析などの用途への活用が進んでいる．例えば，日本では，2017 年に全面施行された改正個人情報保護法では，匿名個人情報が定義され，顔認証データ等の利活用を促進する動きがある［1］．

公共分野では，マイナンバー制度により，国民向けに提供されるサービスにおいて，個人を識別可能な情報を用いたシステムが利用されている．

海外の一部の国や地域では，個人情報保護保護に関する法令やガイドラインの制定が行われ，プライバシー影響評価（Privacy Impact Assessment，以下 PIA）の実施体制が整備されている．

EU では，2018 年 5 月に施行される予定の一般データ保護規則（General Data Protection Regulation，以下 GDPR）で，PIA に相当するデータ保護影響評価（Data Protection Impact Assessment，以下 DPIA）の実施が規定されている［2］［3］．

日本では，2015 年に番号法が施行され，マイナンバーを含む個人情報を扱う政府機関や自治体を対象とした特定個人情報保護評価が義務付けられた［4］．

インターネット経由で個人情報が流出すると，情報がインターネット上に拡散するため，回収が困難となる．また，最近のサイバー攻撃の傾向として，ネットワークカメラ等の IoT 機器が標的になっている［5］．日本でも個人情報を扱うシステムの導入において，開発初期の段階で事前にリスク評価を行い，対策を行う必要性の検討が始まっている．

本稿では，各国のプライバシー影響評価について，ガイドラインの整備や実施状況を調査分析する．

†1 公立大学法人首都大学東京　産業技術大学院大学
Advanced Institute of Industrial Technology

2. プライバシー影響評価の概要

2.1 プライバシー影響評価の定義

プライバシー影響評価とは，個人情報に関するリスクアセスメント手法である.「個人情報の収集を伴う新たな情報システムの導入にあたり，プライバシーへの影響度を「事前」に評価し，その回避または緩和のための法制度・運用・技術的な変更を促す」ための一連のプロセスである［6］-［9］.

個人情報保護対策には，法律（ハードロー），ガイドライン（ソフトロー），社会倫理，国際標準，対策技術などの理解が必要である．技術的対策，法的対策を効果的に実施するには，事前の評価が必要である．また，ステークホルダーの合意形成（マルチステークホルダーエンゲージメント）が必要である．PIA では，システムの企画・設計段階で包括的なプライバシー問題を事前に把握し，ステークホルダー間の合意形成を行う．

図 1 は PIA の役割を示す.

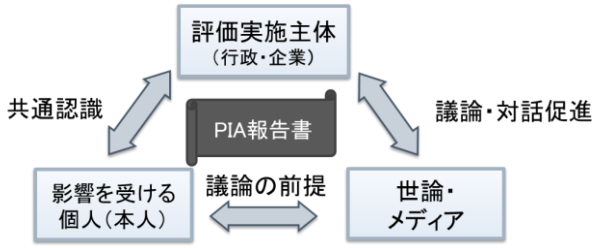

図 1 PIA の役割

PIA の実施目的は，大きく 3 つに分けられる[6].

(1) 個人情報に関するセキュリティ対策

PIA の特徴の 1 つは，情報システムのライフサイクルにおいて，企画段階でプロアクティブ（事前）にプライバシー対策を考慮するという，Privacy by Design のコンセプトが取り入れられていることである[7].システムの企画段階で PIA を実施することで，事前にシステムにおけるプライバシーリスク評価を行い，その結果を開発に反映する．

一般的に，情報システムのセキュリティ対策にかかるコストは,後工程になるほどコストがかかると言われている．システムの企画段階で PIA を実施することは，セキュリティ対策コストに制約がある組織でも，有効な個人情報保護対策の手法となり得る．

(2) ステークホルダー間の信頼構築

PIA を実施することで，ステークホルダー間の信頼構築につなげることができる．例えば，公的機関で個人情報を扱う情報システムを導入する場合，国民（または住民）にとって，そのサービスを利用しないという選択肢は実質無いに等しい．このようなサービスを実施する場合，行政，市民，各種団体，専門家等の各ステークホルダーが対等な立場で円卓会議式に議論する「マルチステークホルダープロセス（Multi-Stakeholder Process)」の手法を用いることが望ましい［10］.

PIA は，このマルチステークホルダープロセスの手法を用いて，新たに導入する情報システムを評価し，その結果を PIA 報告書として Web などで公開することで，住民との対等な議論と対話を促進することが可能となる．PIA はリスクコニュニケーションツールとも言える．

(3) 個人情報保護における相当注意

プライバシー影響評価の国際標準規格 ISO/IEC 29134:2017 では，PIA の実施を Due Diligence の指標として利用することが可能であるとしている[9]．Due Diligence とは，直訳すると「相当の注意」，企業経営では M&A や証券発行に際して，問題点の有無を把握するために行う事前に実施する調査のことである．業務の過程で起こりうる潜在的なプライバシー・リスクを事前に特定し，対処する PIA のプロセスが，Due Diligence に相当する．EU の一般データ保護規則では PIA（DPIA）を実施した場合，罰則の軽減などの措置が取られる［2］［11］.

図 2 は，PIA を実施することによる効果について，各ステークホルダーに対して，Privacy by Design，Multi-Stakeholder Process，Due Diligence の 3 つの視点でステークホルダーとの関係をまとめたものである．

		ステークホルダー		
		個人（データ主体）	民間企業・公的機関（データ保有者・利用者）	PIA実施者・第三者機関（監督者）
Privacy by Design	・リスク保護担保	■	■	
	・コスト削減		■	
	・プライバシー意識喚起		■	
Multi Stakeholder Process	・参加	■		
	・透明化	■	■	■
	・説明責任	■	■	■
Due Diligence	・リスク対応		■	
	・エビデンス		■	■
	・説明責任（相当注意）	■	■	

図 2 PIA と各ステークホルダーの関係

3. 海外におけるプライバシー影響評価の状況

3.1 PIA の動向

(1) PIA を導入しているエリア

図 3 に現在 PIA を実施している国，地域を示す．英国連邦（カナダ，オーストラリア，ニュージーランドなど），米国，韓国では，各国で法律やガイドラインに基づいて PIA が実施されている．EU では 2018 年 5 月 25 日に完全施行する GDPR で PIA の実施を義務付けている．APEC では，実施している国もあるが APEC としての PIA 実施については,検討中の段階である［2］［7］［12］.

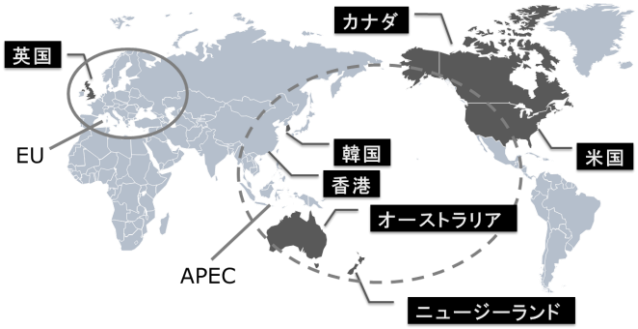

図 3 PIA を導入・検討しているエリア

(2) PIA の実施根拠

図 4 に示すように，PIA の実施は，各国（地域）ごとに規定された個人情報保護に関する法律やガイドラインに基づいて，PIA の実施手順と実施体制が整備されている．

英国および英国連邦では PIA の実施を規定した法律は制定されておらず，社会的慣習に基づき PIA ガイドラインに従い，PIA が実施されている．

米国では電子政府法，韓国では個人情報保護法に基づき PIA が実施されている．日本では番号法に基づき，マイナンバーを含む個人情報である特定個人情報を対象に，特定個人情報保護評価が実施されている［6］［7］．

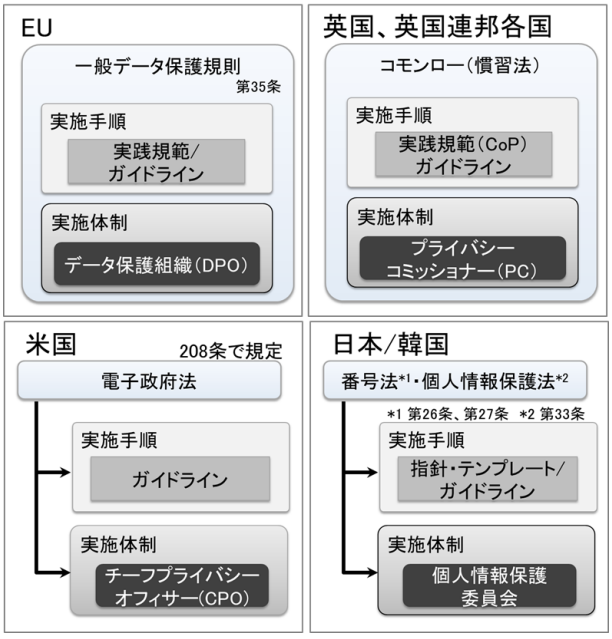

図 4　各国（エリア）の PIA 実施体制

3.2 EU データ保護規則におけるデータ保護影響評価

(1) 一般データ保護規則 GDPR の概要

EU では，欧州委員会が一般データ保護規則 GDPR を 2016 年 1 月 25 日に公開した．GDPR は 1995 年に採択された EU データ保護指令（95/46/EC）に代わるデータ保護制度で，2018 年 5 月 25 日に完全施行する．

EU ではデータ保護に関するルールが「指令（Directive）」から「規則（Regulation）」に格上げされる．これは，加盟国に直接の効力をもち，国内法に優先することを意味する．また，適用の地理的範囲は EU 域内に限定せず，「EU 域内に拠点のない管理者又は取扱者による EU 在住のデータ主体の個人データの取扱いに適用される」とある（第 3 条第 2 項）．EU に居住する個人に対する商品やサービスの提供や行動のモニタリングを行う日本企業，例えばオンラインサービス事業者やオンライン広告事業者も適用対象となる［2］［11］．

(2) データ保護影響評価 DPIA

EU における PIA 導入に関して，1995 年に採択された EU データ保護指令（95/46/EC）では，第 20 条「Prior checking」（事前評価）が規定された．「Prior checking」については，「データ主体に特定の危険をもたらす可能性のある作業を事前に指定し，作業開始前に調査しなければならない」としている．PIA 実施の義務，体制や実施手順についての規定はない．

一方，GDPR ではデータ管理者の新たな義務について，第 35 条ほかでデータ保護影響評価 DPIA（Data Protection Impact Assessment）について規定している［3］．

- 第 35 条　データ保護影響評価 DPIA
  特に新たな技術を用いるなどのある種の取り扱いがその性質，範囲，文脈及び取り扱いの目的を考慮して，自然人の権利や自由に高リスクを生じさせる可能性がある場合，管理者は，取り扱いの前に，予定された取り扱い作業の個人データ保護への影響評価を実施しなければならない．
- 第 36 条　事前協議
  取り扱い対象の情報が機微であるなどリスクが高い場合の監督期間への事前協議を行う手続きを規定
- 第 37 条　データ保護オフィサーDPO の指名
  Data Protection Officer の指定を必要とする場合について規定
- 第 38 条データ保護オフィサーの地位
  DPO が個人データの保護に関連するすべての問題において，適切かつ適時に関与することを保証することについて規定

図 5 に GDPR の条文から把握できる DPIA の実施体制を示す［3］．

- DPIA の実施における責任者は，管理者（controller）や処理者（processer）であり，実施時にデータ保護官の助言を受け，実施する．
- 監督機関は対象リストを作成し，国民に公開し，また，欧州データ保護委員会にリストを通知する．
- 監督機関は DPIA の実施責務者に，DPIA に問題ある場合は，勧告する．

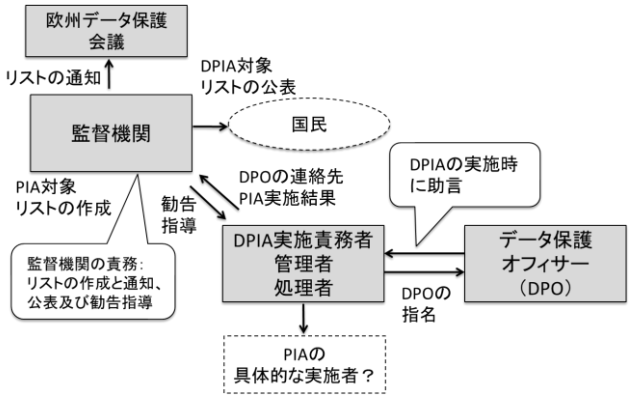

図 5 DPIA の実施体制

(2) PIA の実施フロー

図 6 に DPIA の実施フローを示す [13]. 図 6 の DPIA は 3 つの段階から構成される.

A. 準備段階
- 必要性判断
- 評価実施計画
- ステークホルダーの識別
- 評価対象資料の収集

B. 評価段階
- 保護の目標特定（システム，業務フロー）
- 攻撃者の特定（システムおよびデータフローにおけるリスク分析）
- 影響評価

C. 報告・対策段階
- 安全管理策の特定
- 評価結果の報告書作成（DPIA 報告書）
- DPIA 報告書の公開

なお，DPIA には，安全管理策の実施とその評価も考慮されている. ISO22307 では,PDCA の P 段階での対応であるが，ISO/IEC29134 および DPIA は PDCA 全てを対象としている.

(3) PIA ガイドライン

EU あるいは EU 各国で，PIA ガイドラインが発行されている. GDPR に大きく齟齬がないガイドラインである. 表 1 は PIA ガイドラインの一例である.

3.3 その他の国における状況

表 2 に各国での PIA 実施状況について，法的根拠，ガイドライン，第三者機関，実施事例の観点でまとめた.

(1) 英国および英国連邦

英国では，1998年に施行したデータ保護法に基づき，独立した監督機関であるICO（Information Commissioner’s Office）が設置された. 設置当初はEUデータ保護指令28条の「監督機関」に相当し，個人や団体などからの苦情受付と対応，データ保護法への遵守に向けたベストプラクティスの提供を行っている.

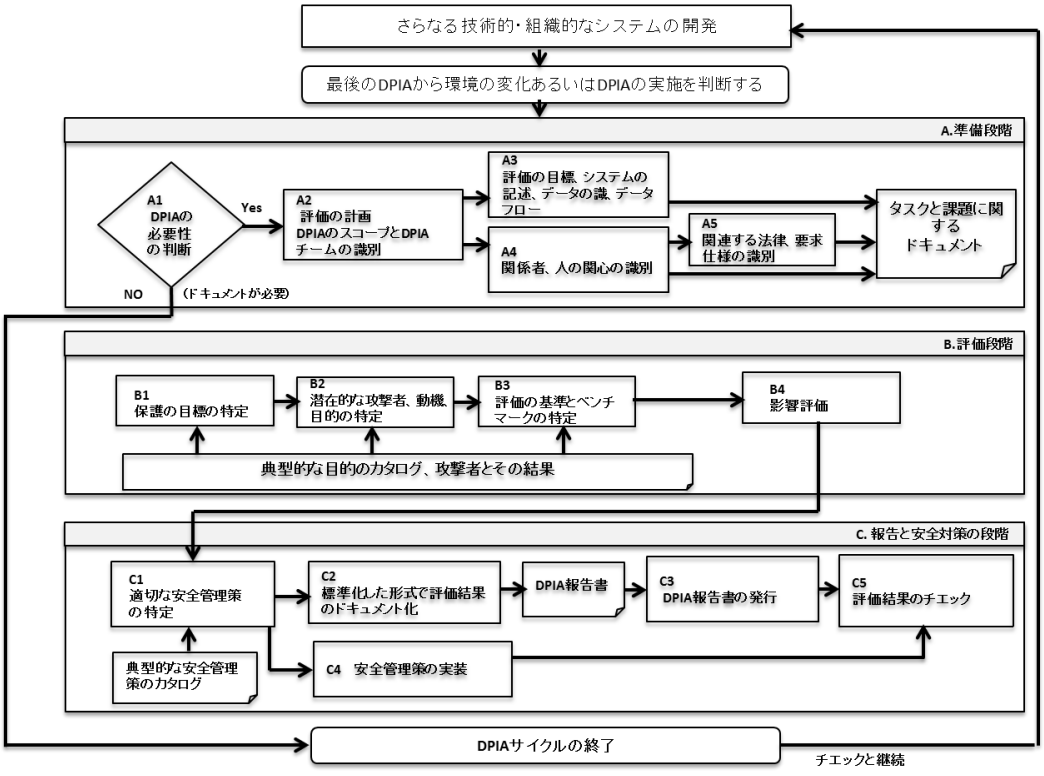

図 6 DPIA の実施フロー

表 1 PIA ガイドラインの一例

ガイドライン	内 容	発行年	発行組織	URL
Test phase of the Data Protection Impact Assessment (DPIA) Template for Smart Grid and Smart Metering Systems 2015	スマートグリッド、スマートメーターを対象にしたDPIA実施のためのテストサンプル 委員会により種々のドキュメントが発行	2015年	European Commission	https://ec.europa.eu/energy/en/test-phase-data-protection-impact-assessment-dpia-template-smart-grid-and-smart-metering-systems
Privacy and Data Protection Impact Assessment Framework for RFID Applications 2011.1	RFIDを対象としたDPIAのフレームワーク 英国ICOベース？	2011年	European Commission	http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf http://www.piawatch.eu/node/413
Conducting Privacy Impact Assessments code of practice 2014.2	データ保護指令を受けてICOにより作成された一般的PIA手順書	2014年	ICO	https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
Privacy Impact Assessment Guideline 2011	ドイツの標準化組織で作成された、RFIDを念頭にいれた一般的PIA手順書	2011年	Bundesamt fur Sicherheit der Informations-technik	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Kurzfasssung.html

PIA については，英国では 2008 年以降，内閣府の報告書“Data Handling Procedures in Government”に基づき中央省庁での PIA 実施を義務付けている．PIA 実施状況は内閣府が管理し，ICO には PIA 報告書の提出義務はない．PIA の実施開始に伴い，ICO は実施規範である「Privacy Impact Assessment Handbook」（2007 年），「Conducting Privacy Impact Assessment Code of Practice」を提供している[11]．英国での PIA 実施例は，2006 年に導入したスコットランド国民資格カード，2007 年に導入した警察全国データベースをはじめとした PIA 実施実績がある．

その他の英国連邦諸国では，カナダ，オーストラリア，ニュージーランドで PIA が実施されている．いずれの国においても，個人データに関する独立した監督機関であるプライバシーコミッショナーが設置され，PIA ガイドラインを発行している．

(2) 米国

米国では，2002 年に施行した電子政府法 208 条に基づき，各行政機関が個人情報を直接的または間接的に推定可能な方法で収集する場合，または配信するための情報技術を開発または調達する場合，事前に PIA を実施することを義務付けている．また，国土安全保障法第 222 条に基づき，省ごとに CPO（Chief Privacy Officer）の任命を義務付けている．CPO は PIA を承認する権限を有する．

米国での PIA 実施例は，2004 年に導入した，米国に入国する外国人を対象としたバイオメトリクスを用いた個人認証プログラムである US-VISIT（United States Visitor and Immigrant Status Indicator）等で実施実績がある［6］．

(3) 韓国

韓国では，2011 年に施行した個人情報保護法第 33 条に基づき，個人情報影響評価（以下 PIA）の実施を義務付けている．PIA 実施体制としては，個人情報保護委員会が独立した監督機関の役割を果たしている．また，安全行政部，KISA（韓国インターネット振興院）が民間企業向け個人情報影響評価遂行ガイドを発行している．PIA の実施は，認定された評価機関によって行われている．

韓国での PIA 実施例は，2007 年に導入した外交部の新電子パスポート，教育部の NEIS（教育行政システム）等をはじめとした PIA 実施実績がある．民間企業でも PIA が実施されている［6］．

4. 日本における状況

4.1 特定個人情報保護評価

日本では，2015 年に施行された番号法に基づき，マイナンバー（個人番号）を含む個人情報を「特定個人情報」と定義し，マイナンバーを管理する各自治体に対し，特定個人情報保護評価の実施を義務付けた．

特定個人情報保護評価の目的は，住民および本人の権利利益の侵害を未然に防止し，信頼を確保することである［14］．評価の実施結果については，特定個人情報保護評価書の形で公表する．また，対象自治体の規模等によっては，特定個人情報保護評価書について，専門性を有する第三者で構成される点検委員会による第三者点検を受ける必要がある．

特定個人情報保護評価は，評価の対象がマイナンバーのみであり，個人情報は対象外である．また，いくつかの点において，特定個人情報保護評価は海外で実施されている PIA とは異なる［15］．

表 2　各国における PIA の実施状況

	EU	英国	英国連邦（カナダ）	米国	韓国	日本	
						民間	マイナンバー
法的根拠	・GDPR35条で、「データ保護影響評価（DPIA）」について定めている。 ・36条において取り扱い対象の情報が機微であるなどリスクが高い場合の監督機関への事前協議を行う手続きを規定	・法的根拠はないが、ICOが主導で、ガイドラインやハンドブックを発行	・法的根拠はないが、連邦政府機関において義務付けられ予算承認プロセスに組み込まれている。（ISO22307適合）	・米国電子政府法第208条 ・（ISO22307適合）	・個人情報保護法第33条	・ISO22307適合	・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第26条
ガイドライン	・GDPRに完全準拠のガイドラインはまだ発行されていない	・ICOからPIA code of practic（2014）を発行	・Office of the Privacy Commissioner of CanadaによるPIA指令 ・報告書は、場合によっては公開	・実施組織のCPOにより発行 ・報告書は原則公開	・行政安全部・韓国インターネット振興院により実施ガイドを発行 ・報告書は非公開	・ハンドブック、マニュアルを開発公開（産業技術大学院大学） ・報告書は公開	・特定個人情報保護評価指針 ・報告書は原則公開
第三者機関	・GDPR38条では、コントローラ（管理者）とプロセッサ（処理者）は、DPOが「個人データの保護に関連するすべての問題において、適切かつ適時に関与する」ことを保証すると規定	・ICO（Information Commissioner's Office）	・Office of the Privacy Commissioner of Canada	・US・VISITなどのシステム構築においてはCPOの設置を義務付け	・個人情報保護委員会	・CPOの設置を推奨	・特定個人情報保護委員会（三条委員会） ・点検委員会/個人情報審議会
実施事例	・GDPR/DPIAということではまだない。	・公共的なシステムで実施実績あり. 例えば警察全国データベースの導入にあたり実施	・行政機関の実施義務あり、複数の実施事例あり	・政府機関のPIAの実施が義務付け ・複数の実施事例あり	・公共機関にPIA実施 ・複数の実施事例あり	・公共性のある民間機関の複数のPIA実施例あり ・報告書の公開あり	・自治体での実施
その他			・州レベルでは社会習慣として自主的に実施		・事例集の公開	・リスク分析手法を具体的に提案	

海外で実施しているPIAは実施者（評価者）の要件について，原則として厳密な専門性，中立性を有する者と規定している［6］．しかし，特定個人情報保護評価には実施者の要件についての規定がなく，自己評価（評価と宣言）をベースとしている．また，自治体ごとに設置した，第三者で構成された点検委員会が評価書の点検を行なっているが，点検委員会の構成要件や権限が明確に規定されておらず，PIAにおけるプライバシーコミッショナーの位置づけとは，機能的に異なる．

4.2 PIA

日本では現在，法的根拠に基づくPIA実施体制は整備されておらず，研究・試行段階である［6］［7］［16］．2006年に法務省の依頼により，顔，指紋を扱う入国管理システムに対して，産業技術大学院大学（以下本学）でPIAを実施したのが初めてである［16］．以来本学にて，認証サービス，グループウェアシステム，健診データHERシステム，監視カメラシステム等でPIAを実施した．PIA実施と並行し，各組織でのPIA導入支援として，PIAハンドブック・PIAマニュアルを作成し，PIAにおけるリスク分析手法を具体的に提案した．

また，産官学連携でのPIA導入支援の一環として，（一社）日本画像認識協会に「次世代ネットワーク型監視カメラのプライバシー保護研究専門委員会」（委員長：瀬戸洋一）を設置した．防犯カメラの高性能化，多目的化に対応し，防犯カメラの設置・運用におけるPIA実施体制の整備と，PIAマニュアル作成に向けた取り組みを行っている［17］．

図7は，マニュアルに掲載したPIA実施手順である．PIA実施手順は3つの段階からなる．

(1)　PIA実施の準備
- 予備評価：　評価を実施するか否かの判断
- 評価準備：　ステークホルダーの特定，必要な資料の収集，実施計画書の作成，評価シートの作成

(2)　PIA評価の実施
- リスク分析：　システムおよび業務フロー分析，システムリスク分析，業務フローリスク分析の実施
- 影響評価：　影響評価の実施

(3)　PIA報告
- 報告書作成・レビュー：　PIA報告書の作成およびステークホルダーレビュー

図6に示すDPIAのフローと基本的に同じであるが，リスク分析などをより具体的に記述している．

5. おわりに

本稿では，プライバシー影響評価に関し，各国のPIAの特徴と導入状況について調査分析を行った．

EU，英国連邦諸国や米国では，第三者機関による監督のもとにPIAの実施体制が整備されている．特にEU一般デー

	PIA実施の準備		PIA評価の実施		PIAの報告
	予備評価	評価準備	リスク分析	影響評価	報告・レビュー
入力	・システム設計書 ・業務概要書 ・運用管理規定	・対象システム関連文書 ・参照規定文書	・システム分析書 ・業務フロー分析書	・システムリスク分析書 ・業務フローリスク分析書 ・評価シート	・システム分析書 ・業務フロー分析書 ・評価シート ・リスク分析書
手順	・評価関連資料の収集	・評価関連資料の収集 ・実施体制の整備			・成果物の最終確認
	・対象範囲の確定	・対象範囲の確定			
	・対象システム、個人情報フローの分析 ・保護すべき個人情報の抽出 ・影響評価	・参照法令や規格、ガイドライン、社内規程、契約類の特定	・システムリスク分析 ・業務フローリスク分析		
	・詳細/簡易PIA実施判定	・PIA実施計画書の作成 ・システム分析 ・業務フロー分析 ・評価シート作成	・リスク分析書の作成	・影響評価	・PIA報告書の作成
出力	・予備PIA報告書	・PIA実施計画書 ・システム分析書 ・業務フロー分析書 ・評価シート	・システムリスク分析書 ・業務フローリスク分析書	・影響評価報告書	・PIA報告書

図7　日本におけるPIA実施手順

タ保護規則GDPRでは，個人データの扱いには，厳しい罰則規定が設けられ，データ保護影響評価DPIAが規定された．

一方，日本において，2015年より実施している特定個人情報保護評価は，PIAに近い制度ではあるが，自己評価を基本とし，中立性，専門性に課題がある．

日本では,2017年5月に全面施行された改正個人情報保護法による匿名加工情報の規定により，個人データの利活用が可能となった．防犯目的から人流解析まで幅広く活用されるネットワークカメラをはじめ，今後，PIAの実施を必要とするシステムが多くなることが予想される．したがって，海外のPIA実施体制に近い,第三者機関による監督に基づいた個人情報保護評価制度と実施ガイドラインの整備が必要であると考える．

謝辞

調査分析のレビューにおいて，本学 Project Based Learning 活動のメンバーである大舘瞳氏，佐藤直子氏，中田亮太郎氏，山川吉雄氏の協力を得た．

参考文献

[1] 岡村久道： 個人情報保護法の知識第 4 版,日経文庫, 2017 年.
[2] 日本貿易振興機構　ブリュッセル事務所： 「EU 一般データ保護規則(GDPR)」に関わる実務ハンドブック(入門編), 2016 年 11 月
https://www.jetro.go.jp/ext_images/_Reports/01/dcfcebc8265a8943/20160084.pdf
[3]個人データの取扱いに係る自然人の保護及び当該データの自由な移転に関する欧州議会及び欧州理事会規則(一般データ保護規則)（仮日本語訳),
https://www.jipdec.or.jp/archives/publications/J0005075.
[4] 特定個人情報保護評価の概要
https://www.ppc.go.jp/files/pdf/20160101hyoukasyousai.pdf.
[5] 平成 28 年中におけるサイバー空間をめぐる脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/H28cyber_jousei.pdf
[6] 瀬戸洋一　他： 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.
[7] 瀬戸洋一： 実践的プライバシーリスク評価技法 プライバシーバイデザインと個人情報影響評価, 近代科学社, 2014 年.
[8] ISO 22307:2008 Financial services - Privacy impact assessment
https://www.iso.org/standard/40897.html
[9] ISO/IEC 29134:2017 Information technology - Security techniques -- Guidelines for privacy impact assessment.
[10] 浦田有佳里, 瀬戸洋一他： マルチステークホルダープロセスにおけるプライバシー影響評価の考察, コンピュータセキュリティシンポジウム 2016.
[11] 小泉雄介： プライバシー影響評価（PIA）の海外動向と日本への応用. 日本データ通信, p.10-12, No.214, 2017 年.
[12] 諸外国における PIA の目的・役割
http://www.cas.go.jp/jp/seisaku/jouhouwg/hyoka/dai1/sankou1.pdf
[13] http://europrivacy.info/2017/01/17/pia-and-proposals-from-isoiec-29134-and-ico/
[14] 特定個人情報保護評価の概要
https://www.ppc.go.jp/files/pdf/20160101hyoukasyousai.pdf.
[15] 佐々木真由美, 瀬戸洋一他： 特定個人情報保護評価における課題分析, コンピュータセキュリティシンポジウム 2015, 2015 年 10 月.
[16] 瀬戸洋一： プライバシー影響評価ガイドライン実践テキスト. インプレス, 2016 年.
[17] 白石敬典, 瀬戸洋一他： ネットワーク対応監視カメラの設置・運用ガイドラインの課題分析とその対策, SCIS2017, 2017