ISO/IEC 29134対応

プライバシー影響評価実施マニュアル

瀬戸洋一［編著］
長谷川久美［著］

日科技連

まえがき

国内外でプライバシー保護強化の流れがある。国際標準化小委員会ISO/IEC JTC 1/SC 27では、2017年、プライバシー影響評価に関するISO/IEC 29134(Guidelines for privacy impact assessment)を発行した。

ISO/IEC 29134は、本書がテーマとするプライバシー影響評価に関する最新の国際標準規格である。ISO/IEC 29134の全訳であるJIS X 9251が、2021年に日本規格協会より発行される予定である。また、2018年5月よりEU一般データ保護規則(General Data Protection Regulation：GDPR)が完全施行された。GPDRでは、個人情報を扱うシステムを構築する際、データ保護影響評価(Data Protection Impact Assessment：DPIA)の実施を義務づけている。日本はEUより十分性認定を受けており、EUと同等の保護体制の構築が必要である。

著者らは、2008年発行のISO 22307(Financial services－Privacy impact assessment)に準拠し、日本の社会制度に合うプライバシー影響評価の実施手順書(マニュアル)を開発済みである。今回ISO/IEC 29134：2017発行を契機に、ISO/IEC 29134に適合するプライバシー影響評価実施手順書を改訂した。

本書は、ISO/IEC 29134あるいはJIS X 9251(2021年3月発行予定)の規格そのものを解説した書籍ではない。本書が提供するのは、著者らが2017年に開発した「プライバシー影響評価実施手順書」について、ISO/IEC 29134規格との相違点を分析し、規格に準拠した「プライバシー影響評価実施手順書」である。読者は、本書を通じて、プライバシー影響評価とは何かを学べるだけでなく、実際にプライバシー影響評価を実践できるようになる。

プライバシー影響評価は、EU(European Union：欧州連合)、APEC

(Asia-Pacific Economic Cooperation：アジア太平洋経済協力)、英国連邦(Commonwealth of England)、米国などで実施され有用性が確認されている一方で、日本では十分に普及しているとはいえない。また、日本では2015年度に改正個人情報保護法が施行され、匿名化された個人情報の利活用ができるようになったが、必ずしも個人の権利を守るフレームワークはできていない。プライバシー影響評価は、Privacy by Design(計画的プライバシー対策)を具現化する重要な手法の一つであり、個人の権利を守る有用な方法論である。本書がプライバシー影響評価を日本に普及させる一助になることを願う。

本書は、以下の3部から構成されている。

- 第1部　プライバシー影響評価(PIA)の概要
- 第2部　プライバシー影響評価(PIA)の実施手順
- 第3部　店舗向け多目的監視カメラシステムのPIAの実施事例

プライバシー影響評価の内容を知りたい場合は、第1部から読むことを勧めたい。プライバシー影響評価について理解し、実施手順のみでよい場合には、第2部から読んでほしい。なお、以下の書籍と併せて学習していただければ、効率的にプライバシー影響評価に関する実践的な力を身につけることができる。

①　プライバシー影響評価の概要

瀬戸洋一、伊瀬洋昭、六川浩明、新保史生、村上康二郎(2010)：『プライバシー影響評価PIAと個人情報保護』、中央経済社。

②　プライバシー影響評価の事例

瀬戸洋一(2016)：『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R&D。

③　プライバシーリスク評価の詳細

瀬戸洋一(2014)：『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。

プライバシー影響評価の研究は、著者が2007年に法務省からの研究受託で開始した。以後10年間、産業技術大学院大学における Project Based Learning(PBL)の教育研究のテーマとして実施してきた。本書はその成果をまとめたものである。

PBLにおいてプライバシー影響評価に関わった学生、特に、リスク分析手法の検討では渡辺慎太郎氏の貢献が大きい。また、ご協力いただいた関係者(省庁、自治体、医療機関、企業)、およびプライバシー影響評価の研究に関与したすべての関係者、および本書の出版にご尽力いただいた日科技連出版社の編集者田中延志氏に対し、ここに感謝の意を表します。

2020年10月

編著者　瀬戸　洋一

目　次

第３部　店舗向け多目的監視カメラシステムの PIA 実施事例

第 1 章
PIA の概要

1.1　PIA の背景

1990 年代から個人情報の電子化の進展に伴い、情報システムにおける個人情報の漏えいやプライバシーの侵害などの問題が顕在化し、その対策としてプライバシー影響評価（Privacy Impact Assessment：PIA）の実施が世界各国で実施された。PIA は 1990 年代中盤以降から、英国連邦であるカナダ、ニュージーランド、オーストラリアや、米国、韓国が導入した。英国連邦は、社会制度として PIA を実施している一方、米国や韓国は、法的に規定し実施している[1][2]。EU では、2018 年 5 月に施行された一般データ保護規則（General Data Protection Regulation：GDPR）で、PIA に相当するデータ保護影響評価（Data Protection Impact Assessment：DPIA）の実施が規定された[2]-[5]。日本では、マイナンバー制度における特定個人情報保護評価が PIA の類似制度として運用が開始され、自治体、行政機関等に法律で実施が義務づけられている[6]。

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おり、IoT 機器からの個人情報の流出が懸念されている[7]。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、対策を行う必要性がある。

PIA を有効に実施するには、国際標準あるいは日本産業規格（Japanese Industrial Standards：JIS）に適合したマニュアル（実施手順書）と中立的・専門的な監督機関の設置が必要である。2008 年に PIA に関す

第２章
PIA に関連する国際規格および法令

2.1　ISO 22307：2008

ISO 22307（Financial service—Privacy Impact Assessment）は、国際標準化委員会ISO TC68/SC7（金融サービス）により 2008 年 4 月に発行された、初めてプライバシー影響評価を規定した国際標準規格である。この内容は金融業界以外の他の業種にも適用できる[8]。

ISO 22307 は、以下の 6 項目を PIA 実施における要求事項としている。

① PIA 計画
② PIA 評価
③ PIA 報告
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

このうち、前 3 項（①～③）が PIA の実施手順に相当し、後 3 項（④～⑥）が PIA の実施体制に相当する。これらの要求事項の記述は shall（～するべきである）であり強制表現である。

2.2　ISO/IEC 29134：2017

ISO/IEC JTC1/SC27 より ISO/IEC 29134（Information technology—Security techniques—Guidelines for Privacy Impact Assessment）が 2017 年 7 月に発行された。ステークホルダの特定・協議やリスク対応

第７章
PIA 実施手順の概要と実施体制

7.1　PIA 実施手順の概要

図 7.1 は PIA を実施する場合の全体フローである。

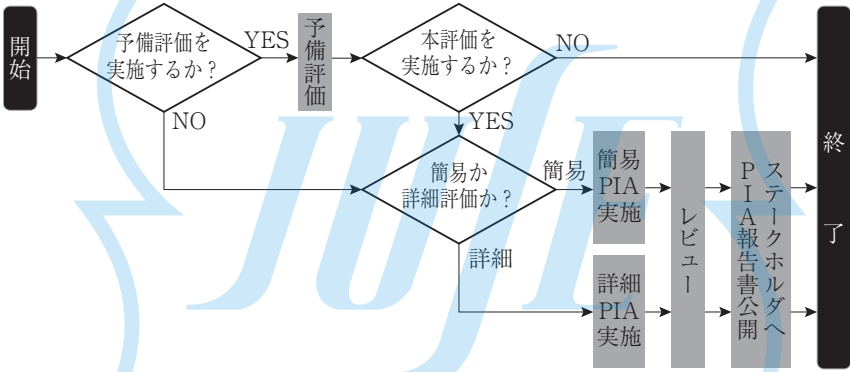

図 7.1　PIA 実施の全体フロー

評価は、予備評価と本評価から構成される。予備評価は、PIA（本評価）を実施するか否かを決定するプロセスである。本評価を実施する場合は、簡易評価を実施するか詳細評価を実施するか判断する。また、必要なドキュメントや実施体制に関する基本情報を収集する。

図 7.2 は、PIA の実施手順を示す。入力（参照するドキュメント等の例）、実施の手順および出力（作成すべきドキュメント）を示す。詳細は**第 9 章**以降で説明する。

添付　店舗向け多目的監視カメラシステム向け評価シート（文書番号：20161104_004）

評価		区分説明
○	適合	適切な安全管理措置が計画されている
×	不適合	安全管理措置が未計画または不十分である
△	評価不能	安全管理措置の計画状況が不明である
−	評価対象外	対象システムにおいては評価対象外である

大項目		法律	参照規程	内容（先生指摘内容）	評価結果		指摘・推奨事項	査閲資料	備考
同意及び選択									
1-1	選択の機会	個人情報保護法第17条（適正な取得）	民間の防犯カメラの設置及び利用に関する留意事項（新潟県）（防犯カメラ設置の明示）	被撮影者に撮影していることを知らせているか。また、設置区域に入らないという選択の機会を与えているか	△	カメラ設置表示に関する規程がない。撮影を避ける方法が確認できない。	カメラが設置されていることを店舗（撮影区域）に立ち入る前にわかりやすく表示する。		
1-2	本人の同意	個人情報保護法第16条（利用目的による制限）	個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（本人の同意）		○	査閲資料によると、同意書による本人同意を取得している。また、未成年者に対しては保護者の同意を必要としている。		PIAの実施計画店舗向け多目的ビデオシステム基本設計書	
目的の正当性及び明確化									
2-1	利用目的の特定	個人情報保護法第15条（利用目的の特定）	個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（利用目的の特定）	利用目的を単に抽象的、一般的に特定するのではなく、可能な限り具体的に特定しているか	△	カメラの設置目的表示に関する規程がない。	カメラの設置目的表示に関する規程を定め、利用目的をできる限り具体的に特定する。		
収集制限									
3-1	必要最低限のデータ収集	個人情報保護法第16条（利用目的による制限）	防犯カメラの設置及び運用に関するガイドライン（相模原市）（第2-2 撮影範囲の限定）	不必要な画像が撮影されないように撮影範囲を設定しているか。	×	根拠規程なし	店舗外の映像など、不必要な映像が撮影されないようにすることを推奨する。		
		個人情報保護法第15条（利用目的の特定）	JIS Q 15001：2006をベースにした個人情報保護マネジメントシステム実施のためのガイドライン　第2版（3.4.2.1 利用目的の特定）	個人情報の取得は目的達成に必要な限度であるか。	×	再来店時の通知を目的とするのであれば、取得する万引き者の個人情報のうち、住所、職業は不要である。	個人情報の取扱は利用目的達成に必要最小限のものとする。	業務フローリスク分析（個人情報台帳）	
3-2	適正な取得	個人情報保護法第17条（適正な取得）	個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（適正取得）	不正の手段により個人情報を収集していないか	○	−	−	業務フローリスク分析（個人情報台帳）	
3-3	要配慮個人情報	個人情報保護法第17条（適正な取得）	個人情報保護法第17条2項	要配慮個人情報を取得するに当たり、あらかじめ本人の同意を得ているか	○	−	−	業務フローリスク分析（個人情報台帳）	

■編著者紹介

瀬戸 洋一(せと　よういち)　(担当箇所：第 1 部、第 3 部)

1979 年慶應義塾大学大学院修士課程修了(電気工学専攻)、同年日立製作所入社、システム開発研究所にて、画像処理、情報セキュリティの研究に従事。2005 年 4 月から 2020 年 3 月まで、公立大学法人首都大学東京 産業技術大学院大学(現 東京都立産業技術大学院大学) 教授。2020 年 4 月より東京都立大学システムデザイン学部およびシステムデザイン研究科非常勤講師、東海大学情報理工学部コンピュータ応用工学科研究員、(一社)情報サービス産業協会プライバシーマーク審査会 会長、情報セキュリティ、プライバシー保護技術の教育研究に従事。工学博士(慶大)、技術士(情報工学)、個人情報保護士、情報処理安全確保支援士、ISMS 審査員補、2009 年電子情報通信学会　功労顕彰を受賞、2010 年経済産業省 産業技術環境局長賞を受賞、著書に『バイオメトリックセキュリティ入門』(ソフトリサーチセンター、2004 年)、『実践的プライバシーリスク評価技法』(近代科学社、2017 年)等多数。

■著者紹介

長谷川 久美(はせがわ　くみ)　(担当箇所：第 2 部)

1999 年津田塾大学学芸学部国際関係学科卒業、2018 年産業技術大学院大学(現 東京都立産業技術大学院大学)産業技術研究科修了(情報アーキテクチャ専攻)。現在、学校法人岩崎学園 情報科学専門学校にて、情報処理、情報セキュリティを中心とした教育の企画、開発および教科教育に従事。情報処理安全確保支援士、情報処理技術者(ネットワークスペシャリスト)、JASA 情報セキュリティ内部監査人。情報システム学修士(専門職)。著書に『改訂版情報セキュリティ概論』(日本工業出版、2019 年)、『サイバー攻撃と防御技術の実践演習テキスト』(日本工業出版、共著、2019 年)。

ISO/IEC 29134 対応　プライバシー影響評価実施マニュアル

2020 年 11 月 28 日　第 1 刷発行

検　印
省　略

編著者　瀬 戸 洋 一
著　者　長谷川　久美
発行人　戸 羽 節 文

発行所　株式会社　日科技連出版社
〒 151-0051　東京都渋谷区千駄ヶ谷 5-15-5
DS ビル
電話　出版　03-5379-1244
営業　03-5379-1238

Printed in Japan

印刷・製本　㈱三秀舎

URL　https://www.juse-p.co.jp/

ISBN 978-4-8171-9723-8