プライバシー影響評価（PIA）の実践と現実

池田 美穂[1,*]　亀石 久美子[1]　畑島 隆[1]　藤村 明子[1]　折目吉範[1]

概要：プライバシー影響評価（PIA）は個人に関する情報を適切に取扱うための有効な手段であるが，PIA の適切な実践は容易ではない．例えば，本来 PIA を実施するべき案件であっても，案件担当者が「自身の案件では“案件担当者が考えるところの個人情報”を取扱わないため個人情報保護法とは無関係であり PIA の実施は不要である」と誤って認識した場合には，PIA が実施されないという問題が発生する．筆者らは，自社において PIA を年間 100 件以上の案件に対して数年以上実施してきた．その経験から PIA 実施時の案件担当者の個人情報保護法に関する知識・理解度を分析した結果，PIA 実践のために必要な知識・理解度との間にギャップがあることがわかった．また，PIA 実践の観点での分析から，従来の従業員教育における個人情報保護法全般の基礎解説の内容は案件担当者の知識として定着しておらず，案件担当者からは案件を進める上で必要な個人情報保護法の要点を手短に把握できる方法が求められているという知見を得た．以上を踏まえ筆者らは，円滑な PIA の実践に有効な，個人情報保護法の基礎知識の習得支援方法と PIA 実践支援方法を検討した．支援方法の一部に関してはプロトタイプとして実装し，法務担当や PIA 評価者による予備評価を行い，個人情報保護法・PIA に関する教材としての利用や PIA 実践における有効性を確認した．

キーワード：プライバシー影響評価，PIA，個人情報保護法

Conduct and Facts of Privacy Impact Assessments Based on the Act on the Protection of Personal Information

Miho Ikeda[1,*]　Kumiko Kameishi[1]　Takashi Hatashima[1]　Akiko Fujimura[1]
Yoshinori Orime[1]

Abstract: A privacy impact assessment (PIA) should be conducted to ensure compliance with laws and guidelines related to privacy. However, misunderstanding of the Act on the Protection of Personal Information (APPI) prevents from conducting appropriate PIAs. Analyzing PIA results conducted in our corporation and frequently answered questions, we identify that many people in charge of projects processing personal information do not acquire adequate knowledge of APPI for conducting PIAs and they need concise methods for legal compliance of the projects. In order to assist those people to conduct PIAs, we propose four methods for learning APPI compactly and three methods for conducting PIAs appropriately. We have produced prototypes of some of these methods and examined those effectivity in preliminary evaluation by people in charge of legal affairs and PIA governance.

Keywords: Privacy Impact Assessment, PIA, The Act on the Protection of Personal Information

1. はじめに

個人情報の保護に関する法律（平成 15 年法律第 57 号．略称：個人情報保護法．以下，「法」という．）[1]は，個人情報の有用性と個人の権利利益の保護の両立を図るために策定された法律である．個人に関する情報[a)]を取扱う研究や事業（以下，「案件」という．）を実施する者は，法を遵守して個人に関する情報を取扱わなければならない．

法を遵守しても個人のプライバシーが保護されるとは限らない．例えば，カメラ画像は撮影自体がプライバシー侵害や肖像権の侵害を問われる可能性があり[3]，撮影される住民や施設利用者等の利害関係者の理解を得るためのコミュニケーションが不十分であるなどして，ネットやメディアで問題視され炎上し，案件の中止に追い込まれる事例は絶えない（例えば[4][5]）．

そこで，プライバシー影響評価（Privacy Impact Assessment. 以下，「PIA」という．）への期待が高まっている．PIA は「個人情報等の収集を伴う事業の開始や変更の際に，プライバシー等の個人の権利利益の侵害リスクを低減・回避するために，事前に影響を評価するリスク管理手法」として，個人情報保護に関する監督機関である個人情報保護委員会が重要性を指摘するものである[6]．総務省や経済産業省も，「消費者やステークホルダーとのコミュニケーションを積極的にとり，能動的にプライバシー問題へ対応する」等の企業のプライバシーガバナンスを機能させる際の PIA の有用性に言及しており[7]，PIA の重要性や期待が増している．

NTT では，企業活動における社会的責任を果たすため，PIA を 2013 年から年間 100 件以上実施しており，筆者らは評価者として参画してきた経験から，PIA を適切に実践するのは容易ではないことを把握している．例えば，本来は

1 NTT 社会情報研究所
NTT Social Informatics Laboratories
* miho.ikeda.da@hco.ntt.co.jp / miho.ikeda@ntt.com

a) 本稿における「個人に関する情報」とは，法第 2 条および第 16 条で定義され法の保護対象である，生存する個人に関する情報である個人情報，個人識別符号，要配慮個人情報，個人データ，保有個人データ，個人関連情報，仮名加工情報，匿名加工情報のいずれかに該当するものとする．なお，統計情報は法の保護対象外である[2]．

PIA を実施するべき案件において，案件担当者が法を正しく理解しないまま，「自身の案件では“案件担当者が考えるところの個人情報”を取扱わないため，法とは無関係であり，PIA の実施は不要である」と認識した場合には， PIA が実施されないという問題が発生しうる．

そこで本稿では，PIA 実践を支援する技術の発展を目的に，筆者らが取り組んでいる PIA 実践の問題分析と解決策を述べる．第 2 章では個人情報保護法の概略と PIA ガイドラインの動向を説明する．第 3 章では NTT で実施している PIA 活動の概要を説明する．第 4 章では PIA 実践上の問題を分析し，第 5 章で問題の解決策を検討するとともに，筆者らが実装した PIA 支援ツールを紹介する．第 6 章では本稿のまとめと今後の研究計画について述べる．

2. 個人情報保護法と PIA ガイドラインの動向

2.1 個人情報保護法の概略

2022 年 4 月 1 日施行の改正法では，民間事業者を対象としていた旧法に新たな規律が追加されるとともに，官民を通じた個人情報保護制度の見直しがなされ，これまで別の法律で設けていた国の行政機関等と独立行政法人等の規律も合流した法律となっている．2022 年 4 月 1 日施行の改正法は第 1 弾改正であり，民間事業者と国の行政機関等，独立行政法人等を対象とするものである．2023 年 4 月 1 日に施行予定の第 2 弾改正は[8]，地方公共団体の機関および地方独立行政法人を対象とするものである．

法の体系は主に，民間部門・公的部門共通の個人情報保護の基本方針（法第 1 章～第 3 章），民間部門の規律（法第 4 章，第 8 章等），公的部門の規律（法第 5 章，第 8 章等）からなる[9]．本稿では以降，民間部門における個人に関する情報の取扱いを前提に記述する[b), c)]．

法は大まかには，個人情報を定義し，情報の取扱い（取得，加工，他者との情報の授受等）における規律を定める構造となっている．したがって，法を遵守するには，まずは案件で取扱う情報を特定し（例：要配慮個人情報を含む個人情報を取得する），次に情報の取扱い方法を特定する（例：「個人データの取扱いの委託」を実施する）手順を踏むことで，該当する規律と法的要件を特定できる．

2.2 PIA ガイドラインの動向

PIA は，1 章で前述したとおり，プライバシー等の個人の権利利益の侵害リスクを低減・回避するためのリスク管理手法である．PIA は，案件の企画時点と案件の実施前の両方で実施するのが望ましいとされている（図 1）[7]．なお，本稿執筆時点（2022 年 8 月）では，個人情報保護委員会等の国の機関では PIA の実施指針を定めておらず，PIA の実施範囲や実施方法等は各組織に委ねられている．

図 1　PIA の効果的な実施時期（[7]を参考に筆者作成）

PIA 実施を検討する上で参考になるガイドラインとして，国際標準の ISO/IEC 29134:2017[11]や，それを JIS 化した JIS X 9251:2021[12]がある．これらの規格を参照すると，PIA は基本的に，既存の情報セキュリティマネジメントシステム（ISMS）にプライバシーへの影響の観点でのリスクマネジメントを追加して実施すればよいことが読み取れる．

しかし，ISO や JIS に記載の手順を忠実に実施しても，PIA を適切に実施できるとは限らない．例えば JIS X 9251:2021 の「6.3.1 PIA チームの設置及び指示」を参照すると，「PIA の最小要件は，法的若しくは規制上の制約，又は組織がプライバシーリスクとみなす重大さの程度に依存する」とあり，PIA は少なくとも法令遵守とプライバシーリスクの観点から実施するものであることが読み取れる．ただし ISO や JIS には，「6.4.4.1 プライバシーリスク特定」等でプライバシーリスクの観点の記述はあるが，法令遵守の観点での具体的な記述はない．日本国内においては，法は個人に関する情報を取扱う際に遵守しなければならない法規範の一つである．したがって，PIA を適切に実施するには最小でも，ISO や JIS に記載の手順に，法に基づく評価観点を適宜加えて実施する必要がある．

法の観点からは，PIA のアセスメント対象は，自組織での情報の取扱いにとどまらず，個人からの情報取得から利用に至るまでの，情報システムや人・組織等の各アクタの活動全般における情報の取扱いがアセスメント対象となる．

このため，法を理解していない者が PIA を実施した場合には，自組織内での情報の取扱いのみを評価すればよいという過小な見立てをしてしまい，PIA の評価結果は法に適合していない不完全なものとなる可能性がある．

3. NTT の事業活動と個人情報保護の取り組み

NTT の主要な事業内容は，NTT グループ全体の経営戦略の策定および基盤的研究開発の推進である．取扱う個人に関する情報としては主に，株主等のお客様の情報，従業者の情報の他，研究開発の一環で実験を実施し取得した実験参加者の情報等がある．これらの情報を適切に取扱うためのベースラインの取り組みとして，例えば，個人情報等の

b）独立行政機関等のうち国立大学等の一部の法人は，個人情報ファイル，開示等及び匿名加工情報に関しては法第 5 章の適用を受けるが，その他の個人情報等の取扱いに関しては法第 4 章の適用を受ける[10]．

c）第 2 弾改正は，主に公的部門（法第 5 章等）の規律の対象に地方公共団体の機関および地方独立行政法人が加わり，一部の条項が追加されるが，施行済みの第 1 弾改正の内容に大幅な変更が加わるものではない．よって本稿での検討内容は第 2 弾改正の施行後も有効であると考える．

ガバナンスの管理体制の整備，情報セキュリティポリシーおよび個人情報保護方針の策定・公表，個人情報等の取扱いに関する社内規程等の整備，個人情報保護・PIA に関する e ラーニングの定期実施等を実行している．

個人情報保護の取り組みの強化策として，法務担当をはじめとして法やプライバシー保護等に精通した者が PIA を実施する，PIA 活動と呼ぶ取り組みを実施している．この PIA 活動では，大学等との共同研究やプロジェクト等のいわゆる非定型業務の案件を PIA の対象としている．従業者の労務管理や来訪者情報管理等の定型業務は，業務手順書等の作成過程で PIA が実施されるため対象外である．

PIA 活動における PIA の評価観点は，筆者らの組織が企業活動を営む上で社会的責任を果たすために PIA として必要と考える要素からなり，事実上 ISO や JIS の手順をアレンジしている．具体的には，案件における情報の取扱いを，法をはじめとする企業法務全般，プライバシー保護や炎上リスク，企業倫理等の総合的な観点で評価し，リスク対応の方針や具体的な対応方法を案件担当者へ提案している．なお，案件概要のみで評価するのではなく，実験参加者等に提示する説明書等の内容も評価対象である．

PIA 活動の流れを図 2 に示す．PIA 活動では，週 1 回の頻度で開催する PIA 会議において，個人に関する情報を取扱う案件の PIA を実施する．会議には案件の担当者，PIA を実施する評価者，会議進行等を担う事務局が参加する．PIA の効果的な実施時期を踏まえ，基本的には実験開始前や契約締結前の企画・設計の段階で案件を PIA 会議へ付議することとしている．案件担当者は，自主確認シート（図 3）を用いて PIA 会議への付議要否を自主確認し，付議必要と判定された場合には PIA 会議への付議希望のメールを事務局宛てに送信する．事務局は，メールに記載または添付の案件概要を参考に，エントリーシートの草案（表 1）を作成し案件担当者へ提示する．案件担当者は，PIA 会議に必要な資料を作成または用意して期日までに事務局へ提出する．会議資料は PIA 会議前に評価者に共有され，評価者は会議資料内容に基づき PIA の予備評価と案件担当者への質問事項や参考情報の整理を行う．PIA 会議当日は，(1)案件担当者による案件概要の説明，(2)案件担当者と評価者の間での質疑応答，(3)評価者による PIA の実施とリスク対応案の提示，(4)案件担当者の法や PIA に関する理解向上のための質疑応答，という流れで進行する．評価者が指摘した，法への法的適合性，プライバシーリスク対応，知的財産等のその他の法的リスク対応の観点で必要な会議資料の修正は宿題として管理される．すべての宿題対応が完了したことを事務局が確認後，事務局にて当該案件の PIA に関する一連の記録として PIA 報告書を作成し保管する．なお，業務推進および PIA の簡素化のため，PIA 会議での評価内容の範囲で案件を進めるかぎりは運用前の PIA 会議での再評価は不要とし，評価内容の範囲から外れる場合には改めて PIA 会議に付議し評価者が評価するとしている．

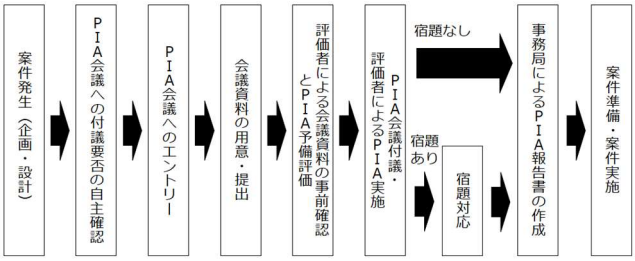

図 2　筆者らの組織における PIA 活動の流れ

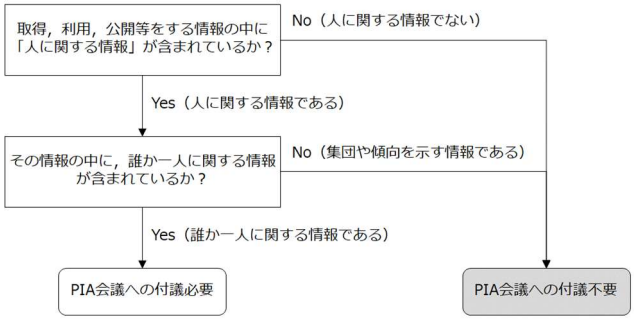

図 3 自主確認シートの概要

表 1　筆者らの組織における PIA 会議で使用する資料

資料分類	資料内容	PIA会議における主な参照目的
説明書(案)*	情報の取扱いなど本人への説明事項を記述した文書の案	・取得するデータ項目，取得方法，利用目的，利用する者の範囲，取扱い方法（誰がどのように利用（保管・加工・提供・削除等）するか），プライバシーへの配慮などの説明内容を確認する． ・PIAを実施した結果，必要に応じて修正する対象．
同意書(案)*	情報の取扱いなどに関して本人からの同意取得が必要な場合に用いる文書の案	・PIAを実施した結果，必要に応じて修正する対象．
契約書(案)*	法人間で締結する契約書および付属書（仕様書，覚書等を含む）の案	・PIAの実施において考慮するべき情報の取扱いに関する事項を確認する． ・PIAを実施した結果，必要に応じて修正する対象．
サービス利用規約，プライバシーポリシー	案件で利用するサービスの利用条件や個人情報の取扱方針を定めた文書	・PIAの実施において考慮するべき情報の取扱いに関する事項を確認する．
エントリーシート	PIA会議で案件概要を説明するための資料． 案件の目的，実施内容，各案件関係者の役割，データフロー図（案件関係者間での情報の流れを整理したもの．図4参照）などが含まれる．	・案件の概要を把握する． ・法令順守，プライバシー保護，炎上リスク，企業倫理等の観点から，案件が適切であるか評価する． ・各案件関係者における情報の利用目的等を踏まえて，案件で取扱う情報や情報の取扱い方法を特定し，案件に関係する個人情報保護法の規律を特定する． ・規律内容に基づき現状の説明書・同意書・契約書等の修正要否を判断し，必要な修正内容を検討する． ・その他，プライバシー保護，炎上リスク等の観点から，現状の説明書・同意書・契約書等の修正要否を判断し，必要な修正内容を検討する．

*PIA会議で修正の指摘がなければそのまま使用する予定のものを提出することとしている．

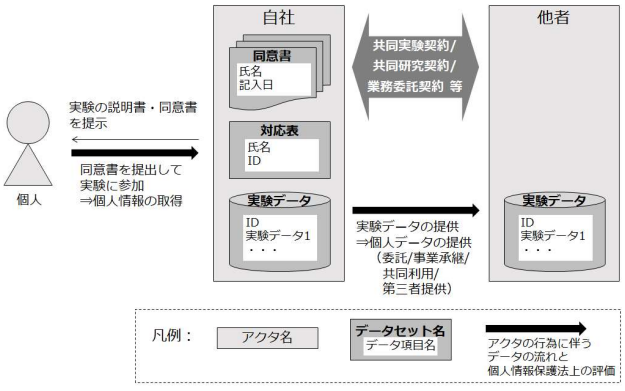

図 4 データフロー図のイメージ

表 2　2021 年度 PIA 会議の評価案件（全 102 案件）における評価者からの指摘状況

	①宿題が発生した案件	①の内訳：宿題観点別の該当案件数(延べ件数)			②の内訳：	
		②法的適合性に問題あり	③プライバシーリスク対応に問題あり	④その他権利関係等に問題あり	②-A：情報や情報の授受について誤りがある（それ故説明書等の記述が不適切）	②-B：情報や情報の授受について誤りはないが説明書等の記述が不適切
全案件（w: 102件）	78	②-w: 78	5	16	②-A-w: 30	②-B-w: 48
新規案件（i: 71件）	55	②-i: 55	4	13	②-A-i: 22	33
類似案件がある案件（ii: 31件）	23	②-ii: 23	1	3	②-A-ii: 8	15

4. PIA 実践の問題分析

4.1 案件担当者の個人情報保護法の理解・知識の現状

2021 年度に PIA 会議で PIA を実施した全 102 案件における，会議資料に対する評価者からの指摘状況を表 2 に示す.「情報や情報の授受の誤り」とは，評価者は法に照らして各アクタが取得・加工・授受する情報や授受の形式を識別しており，会議資料に記載してある案件担当者によるそれらの識別が誤っていると評価者が指摘したものをいう.「類似案件がある案件」とは，案件担当者が関与している過去に PIA 会議で評価済みの案件がある場合をいう. また，宿題観点について,「法的適合性」とは法への適合性（法に係るプライバシーリスク対応を含む),「プライバシーリスク対応」とは法を超えた範囲のもの,「その他権利関係等」とは知的財産等のその他の法的リスクに関するものをいう.

表 2 のように, 情報や情報の授受の誤りは全 102 案件(w)中 30 案件（②-A-w）で発生した．サンプル数が少ないため参考値となるがその発生確率は，新規案件（31.0%＝(②-A-i) / i）と類似案件がある案件（25.8%＝(②-A-ii) / ii）との間で大きな差はない．法的適合性の観点での宿題は全 102 案件中 78 案件（②-w）で発生し，こちらもその発生確率は，新規案件（77.5%=(②-i) / i）と類似案件がある案件（74.2%＝(②-ii) / ii）との間で大きな差はない.

表 3 のように，情報や情報の授受の誤り（30 案件（②-A-w）で計 42 個）を詳細分析すると，最も多く発生した誤りは，情報と情報の授受の両方の誤りのうち加工後の情報の誤りに起因するもの（18 件）であった．具体的には,「データから氏名や ID 等の識別子を削除し，個人情報に該当しなくなったデータを他者へ提供する」という認識誤りである．これは，PIA を実施せずにそのまま案件を実施した場合には法令違反となる可能性が極めて高い，評価者が最も憂慮する認識誤りである．なお，これが認識誤りである理由は，加工後のデータに含まれる ID や複数のデータ項目の値の組み合わせ等を照合キーとして，加工前の個人データ（簡単に説明すると，個人情報（氏名，顔画像等の特定の個人を識別できる情報や個人識別符号（生体認証情報や運転免許証番号などの公的番号）を含むもの）をデータベース化し，そのデータベースから一部のデータ項目を抽出

表 3 情報や情報の授受の誤りの内訳
（表 2 の②-A-w の詳細分析）

誤りの分類	誤りの個数（30案件計42個中）
情報のみ	4
取得した情報の誤り	3
加工後の情報の誤り*	1
情報および情報の授受	26
取得した情報の誤りに起因するもの	8
加工後の情報の誤り*に起因するもの	18
情報の授受のみ	12

＊ 具体的には、加工後も個人データのままであるものを、個人情報保護法の保護対象外のもの、もしくは匿名加工情報と誤って識別している

したもの）と容易に照合できる場合には，加工後も個人データのままであり，当該データの他者との授受は個人データの取扱いの委託／事業承継／共同利用／第三者提供のいずれかと評価されるためである（図 4 参照）. 次に多く発生した誤りは情報の授受の誤り（12 件）であった．具体的には，案件の実施内容を考慮すると，個人データの取扱いの委託／事業承継／共同利用／第三者提供の中から明らかに該当しないものを誤って選択するというものであった.

なお，情報や情報の授受の誤りは，案件担当者が PIA 会議へ付議希望をした初期状態では表 2 や表 3 の件数よりも多い．表 2 や表 3 は，PIA 会議で使用した会議資料に基づく分析であり，案件担当者が会議資料を作成する過程で事務局が発見した誤りは会議資料では既に訂正されている．仮に初期状態で PIA 会議に臨んだ場合には，表 2 や表 3 に示した各種誤りは 2~3 倍以上になると推測する．事務局が発見できなかった誤りが残存し，表 2 や表 3 の結果となっている理由は，会議資料から読み取れる範囲では評価上の不確定要素があり，PIA 会議で案件担当者に質問して評価に必要な材料を引き出す必要がある案件が多いためである.

表 2 に戻ると，情報や情報の授受に誤りはないが法的適合性の観点で宿題が出された案件（48 件(②-B-w)）が宿題を出された案件(78 件(②-w))の半数以上を占めることは，注意を払うべき現象である．これは案件担当者が，情報や情報の授受を正しく識別できたとしても，そのときに満たすべき法的要件を十分に理解しておらず，説明書・同意書・契約書等の記述が不適切な状態であることを意味する.

表 4 案件担当者からのよくある質問や疑問

分類	案件担当者からのよくある質問や疑問
情報	個人データとは何か？　個人情報との違いは何か？
	氏名のデータ項目を削除すれば個人データに該当しなくなるか？
	匿名加工情報とは何か？　統計情報との違いは何か？
	“匿名化”（氏名やID等の識別子を削除した場合をいう）しているので匿名加工情報に該当するのではないか？
	自社は氏名を削除したデータの提供を受けて取扱うため，個人情報保護法は関係しないのではないか？
情報の授受	委託／共同利用／第三者提供とは何か？　それぞれの違いは何か？
	業務委託契約であれば個人情報保護法における「委託」か？
	共同研究契約や共同実験契約であれば「共同利用」か？

また，案件担当者から寄せられるよくある質問や疑問を表 4 に示す．法に関する知識・理解不足に起因する質問が多く寄せられており，これらは表 2 や表 3 に示した案件担当者の誤りに関連していることがわかる．

以上を踏まえると，案件担当者の法に関する理解・知識には 3 つの傾向があると指摘できる．

一つ目は，法が定義する情報に関する理解不足である．例えば，加工後も個人データのままであるデータを他者から受け取る案件において,「個人に関する情報に該当しないデータ」を他者から受領すると案件担当者が誤って認識し，「自社は個人に関する情報を取扱わないので，案件は法に関係しない，よって PIA の実施は不要である」と考える案件担当者が PIA 活動で多くみられる．実際には，そのようなデータの授受は個人データの取扱いの委託／事業承継／共同利用／第三者提供のいずれかに該当することが大多数であり，法に従って情報を取扱う法的義務が発生する．

二つ目は，法が定義する情報の授受に関する理解不足である．例えば，共同研究契約や共同実験契約を締結する場合に，契約名称に含まれる「共同」という単語に引きずられて,「個人データの共同利用を実施する」と考える案件担当者がみられる．実際には，個人情報の取得時の説明内容や契約条件等を考慮した結果，個人データの取扱いの委託／事業承継／共同利用／第三者提供のうち，個人データの取扱いの委託しか取りえない場合もある．

三つ目は，情報の取扱いに関する法の規律内容の理解不足である．例えば，個人データの共同利用を検討している案件において，実験参加者に提示予定の説明書に「共同利用します」の文言のみを記載している場合がある．実際には法的要件を満たすには，法第 27 条第 5 項第 3 号で定められた 5 項目（①共同利用をする旨，②共同して利用される個人データの項目，③共同して利用する者の範囲，④利用する者の利用目的，⑤当該個人データの管理について責任を有する者の氏名又は名称及び住所並びに法人にあっては，その代表者の氏名）を記載する必要がある．

このような案件担当者の法に関する理解・知識の傾向は，筆者らの会社に限らずどの組織でも普遍的に観察される現象であると考える．筆者らは研究活動の一環として，NTT グループの一部の会社に対し PIA の実践支援を実施しており，その NTT グループ会社の社員からも PIA 会議の案件担当者と同様の質問や疑問（表 4）が寄せられている．また，PIA 会議で評価する案件は，NTT グループ外の組織も関与する案件が半数近くを占め，表 2 や表 3 に示した誤りが PIA 会議で指摘されるということは，社外関係者も法を正しく理解していない可能性を示唆していると考える[d]．

また，案件担当者の法に関する誤った知識・理解は，PIA の実践を妨げる要因となる．前述の例と同様に，案件内容を最も理解している案件担当者が，法の不正確な理解・知識に基づき,「自身の案件は個人に関する情報を取扱わないため PIA は不要である」と誤って認識した場合には，案件担当者による PIA は実施されない．PIA に通じた評価者が PIA を実施する運用体制を整備しても，案件担当者が PIA は不要と認識しているかぎり，案件担当者は評価者に対し PIA を依頼しないため PIA は実施されない．この問題に対する予防策として，筆者らの組織では「案件全体において個人に関する情報を取扱う案件は PIA 会議への付議対象である」と定め，確実に PIA が実施されるよう図っている．

筆者らは，案件担当者の法に関する知識・理解不足は，PIA の適切な実践を実現するために最優先で解決するべき問題であると考えており，この問題解決に向け筆者らが取り組んでいる解決策の検討を以降で論じる．

4.2 PIA を適切に実践するための要件

案件担当者の法に関する知識・理解不足の解決策を検討する前に，PIA を適切に実践するための要件，要件を満たしている状況と現状とのギャップ，およびギャップが生じている原因を整理・分析する．

PIA を適切に実践するための要件は，業務の流れを踏まえると次のように整理できる．

(1) 個人に関する情報を取扱う案件が発生すること
(2) 案件担当者が PIA 実施の必要性を認識すること
(3) PIA を適切な評価観点で実施すること
(4) PIA の評価結果を踏まえ，案件担当者が必要なリスク対応を実施すること

(1)は PIA 実践の大前提である．(2)は，案件で何らかのデータを取扱うが，個人に関する情報に該当するか該当しないかを識別することを含めて，PIA の実施の必要性を案件担当者が認識することをいう．(3)は，案件の性質（分野，データ項目，データの利用目的等）によって参照する法令・ガイドライン等は変化するが，法への法的適合性の観点では，大まかには次の観点・流れで評価を実施する．

a) 案件における情報の取得・利用が各種法令に違反しないか，不適切な行為を助長しないかを評価する．
b) 法の適用対象であるかを識別する（例：生存する個人

d) 契約先の法務担当等による確認対象が契約書のみの場合は，案件における情報の取扱いの実態を把握していないために契約条件の一般的な確認に留まり，PIA 会議での指摘事項が残存することは容易に想像できる．

に関する情報であるか).

c) 適用される規律が民間部門（法第 4 章等）と公的部門（法第 5 章等）のどちらであるかを識別する.

d) 各アクタが取得・加工する情報，およびアクタ間における情報の授受を特定し，適用される規律を特定する.

e) 適用される規律内容に照らして案件の法的適合性を評価し，案件が満たしていない法的要件を特定する.

f) 案件が満たしていない法的要件を是正するための対応方法の案を検討する.

(4)は, PIA 実施後のリスク対応に関するものであるが, 1 章で前述した PIA の実施目的を考慮すると，PIA を適切に実践するための要件の一つとして含める必要があると考える.

(2),(3),(4)は，法に関する知識・理解を要するものである. しかし案件担当者の知識･理解には段階があると考えられ, 4.1 節で分析したように, 法における情報の定義を知らない人，情報の定義は知っているが具体的な規律内容までは把握していない人，規律内容を把握して案件準備を適切に進められている人など，様々である.

そこで，個々人の法に関する知識・理解と PIA 実践の段階を，人材開発・教育支援分野等で用いられる学習の 4 段階モデル[13][14]を参考にレベル分けした（図 5）. なお，ソフトウェア業界では CMMI（Capability Maturity Model Integration. 能力成熟度モデル統合）[15]を用いることが多いが，CMMI は組織の成熟度を測るものであり，個々人の能力・スキルを測るものではなく，本稿が意図する分類には不向きであるため採用しなかった.

このレベル分けに基づくと，PIA を適切に実践するには, 案件担当者に求められるレベルは，自ら PIA を実施する場合はレベル 3 以上，PIA を実施できる人物に PIA 実施を依頼する場合はレベル 2 以上が必要である.

しかし, 4.1 節の分析を踏まえると, 案件担当者は概ねレベル 1～レベル 2 の段階にあると推測される. PIA 活動における PIA の評価結果を例にとると，情報や情報の授受の誤りをした案件担当者はレベル 1，情報や情報の授受は識別できても宿題を出された案件担当者はレベル 1～レベル 2 と推測される.

ここで，案件担当者はなぜとりわけレベル 1 の段階にあるのかという疑問が生じる. 従業者をはじめとする何らかの人物の個人情報を取扱う法人等は個人情報取扱事業者であり，安全管理措置の一つとして従業者の教育を実施することが法で義務付けられている（法第 23 条）. 筆者らの組織における個人情報保護・PIA に関する e-ラーニングも，法令遵守の一環として定期的に実施しているものであり，PIA 会議で案件担当者の誤りを指摘している情報や情報の授受の説明は学習内容に含まれており，学習内容の理解度を測る確認テストも実施している. それにも関わらず，案件が発生した際に，法の保護対象である情報を取扱うにもかかわらず保護対象ではないと案件担当者が誤って認識するのはなぜだろうか. この疑問に対して以下に考察する.

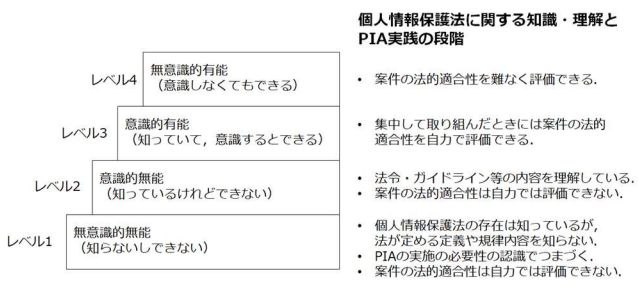

図 5　個人情報保護法に関する知識・理解と PIA 実践の段階

4.3 個人情報保護に関する既存の教育手法の限界

筆者らは，個人情報保護に関する既存の教育手法は，個人情報保護の重要性や法令違反した場合の影響を知らせる等の一定の効果はあるものの，PIA の適切な実践に求められる知識・理解やその実践の段階にまで引き上げるものにはなっていないと推測している.

既存の教育手法は，自前の教材を組織で用意する方法（例 : 業務委託して特注の教材を作成する），市販の教材を利用する方法（例：一般書籍や教育用コンテンツを購入・配布する，外部講師を招いて講習会を実施する）等が考えられ，いずれも個人情報取扱事業者に課せられる安全管理措置の義務履行のために法全般を一通り解説しているために，応分の大量な文章量になっていると想定される.

しかし，法務担当や総務担当，PIA 評価者等の一部の人を除き，多くの人にとって法は馴染みのないものであるとみられる. さらにそれらの人々は法に興味や関心を示さず, また法を正確に理解していなくても，組織が定める運用手順等を遵守すれば担当業務は滞りなく進めることができると考えられる. これらの理由により，個人情報保護に関する学習は担当業務との関連が薄く, 担当業務で多忙なため, 学習は短時間で済ませたい心理が働くと考えられる.

そのため案件担当者の状況を時系列に沿って推測すると，次のいずれかの段階に陥っていると考えられる.

(A) 学習内容を記憶する気がない.

(B) 業務で利用しないため知識が定着しない.

(C) 担当業務で個人に関する情報を取扱う案件が発生したとき, 手間であるため法の定義や規律内容を確認しない.

(D) 教材や法令・ガイドライン等[16]を参照して法の定義や規律内容を確認したものの, 知識と実践との間にはギャップがあり, 法に照らして案件における情報の取扱いを評価できない.

また，実際に個人に関する情報を取扱う案件が発生した際には，案件担当者は手間をかけずに案件で実施するべき法的対応を知りたいだろうと推測される. 案件で進めるべき作業は多岐にわたり，PIA や法的対応だけに時間を割くわけにもいかないため，業務効率化のために例えば法的対応ができている優良事例を真似るなどして，法的対応をな

るべく短時間で済ませたいと考えるだろう．実際に，筆者らの組織における PIA 活動でも，案件担当者から事務局や評価者に対し，空欄に案件依存の事項を入力するだけでよい説明書･同意書の雛形を用意してほしいとの要望がある．

このような案件担当者の心理を考慮すると，PIA 実践の観点からは，案件を進める上で必要な法的要点を手短に把握できる方法が求められており，従来の教育手法で実施していると想定される法の規律内容全般の基礎解説に係る資料は，PIA 実践時の利用に難があるものであると考察する．

5. PIA 実践の支援方法

本章では，4.3 節の考察を踏まえ筆者らが検討および一部実践している，PIA 実践に直結する支援方法を紹介する．

5.1 個人情報保護法の基礎知識の習得支援

4.2 節で検討したように，PIA 実践のためには案件担当者への法の基礎知識の習得支援は必須である．

また，4.3 節の考察を踏まえると，習得支援の要件として，案件担当者が必要とする／知りたい内容へ容易にアクセスできること，容易に理解できるよう内容がコンパクトにまとめられていることが挙げられると考える．

これらの要件を満たす支援方法としては，例えば次の方法が考えられる．

方法１：法の内容を損なわず，法令遵守のために必要な要点の理解が可能となる限界まで要約したコンテンツを用意し，案件担当者が自ら学習する方法

方法２：FAQ を充実させ，案件担当者が学習時に疑問を抱えると想定される事項を解説したコンテンツを閲覧可能にしておく方法

方法３：チャットボットを用意し，案件担当者にインタラクティブに疑問点を解決させる方法

方法４：自社サービス事例等の案件担当者が理解しやすい事例を用いて解説したコンテンツを用意する方法

例えば，文献[17]は方法１や方法２を実現している．

5.2 案件担当者による PIA 実践の支援

案件担当者による PIA 実践を支援するには，法の知識と実践との間にはギャップがあることを前提に，案件担当者の法の知識・理解の程度でも適切に PIA を実践できるよう適宜誘導することが要件として求められると考える．

この要件を満たす PIA 実践の支援方法として，例えば次のようなものが考えられる．

方法１：早見表を用意する方法

この方法は，自社の既存サービスで新規取得する情報または既に取得した情報について，予めサービス利用規約等で定めた情報の利用目的等の範囲内で利用するかどうかの判断に有効である．早見表で設ける確認観点としては例えば，データ項目，データ項目毎の利用目的，他者との情報の授受の可否等が考えられる．

方法２：事例に当てはめさせる方法

この方法は，個人に関する情報を取扱う新規の研究やサービス等を検討する際に有効である．事例は，自組織における個人に関する情報を取扱う案件を類型化するなどして複数用意するとよい．なお，案件が事例に当てはまるかぎりは問題ないが，不適切な当てはめが発生しないようにする工夫を要する．

方法３：実際の PIA と同じ手順で PIA をガイドする方法

この方法は，最も汎用性が高くすべての案件に対応できる．ただし，案件担当者の法に関する知識・理解を最も要求する難易度の高い方法であるため，一つ一つのステップで案件担当者のあいまいな知識・理解を適宜訂正して誘導する工夫を要する．

5.3 PIA 支援ツールの開発

筆者らは，5.1 節で述べた基礎知識の習得支援の方法１，5.2 節で述べた PIA 実践支援の方法２および方法３を実装したプロトタイプ（以下，「PIA 支援ツール」という．）を開発した．基礎知識の習得支援の方法１に関しては，図を多用して文章での説明量を減らし，直感的にわかりやすいように解説したガイドブックを作成した（図 6 右）．PIA 実践支援の方法２に関しては，同ガイドブック内に，筆者らが評価した PIA 会議の過去の PIA 評価案件をもとに，組み合わせ可能な頻出事例を全 11 例抽出し（図 7），各事例の前提条件を文章と図を用いて明記し，事例ごとに情報や情報の授受に関しての評価者の考え方を記述することで，案件と事例との対比を容易にしている．また，PIA 実践支援の方法３に関しては，法への法的適合性の確認順序に基づき設問を構成し（図 8），案件で実施する情報の取扱いに関して，設問に対し与えられた選択肢から選んで回答していくだけで該当する情報や情報の授受を特定し，案件が満たすべき法的要件を表示する Web アプリケーションを実装した（図 6 左）．同アプリケーションの画面上部にはガイドブックを表示し，選択肢の選択誤りを減らせるよう工夫している．なお，PIA 支援ツールは現時点では民間部門（法第 4 章等）のみに対応している．

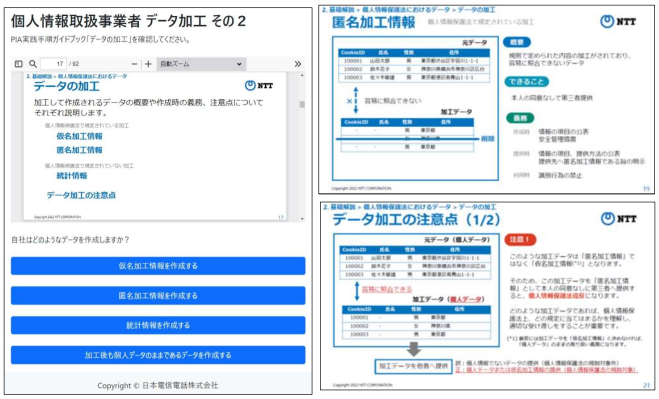

図 6　Web アプリケーション（図左）および同アプリケーションで表示されるガイドブック（図右）のイメージ

図 7 ガイドブックに掲載している事例のイメージ

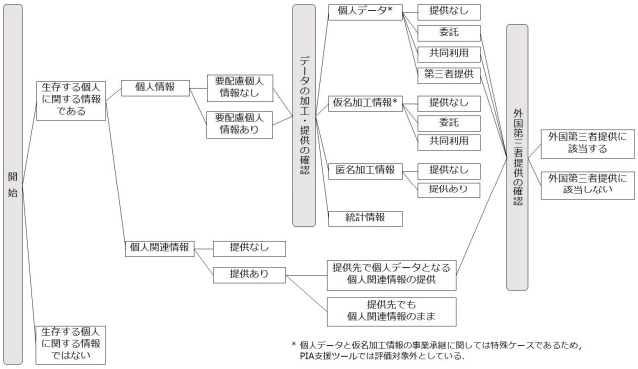

図 8　法的要件の導出に用いる判定内容（抜粋）

5.4 PIA 支援ツールの予備評価

PIA 支援ツールの予備評価として，NTT グループ数社の法務担当や PIA 評価者が試用し，社内での法・PIA に関する教材としての利用や，PIA 実践の効率化が期待されるとのコメントを得ている．また，本研究による PIA 支援ツールは現在，実際の PIA 活動において試験導入しており，評価案件の評価状況を分析して有効性を評価予定である．

なお，PIA 支援ツールによる判定結果は，組織内における PIA の予備評価の位置づけであり，法的適合性の担保はせず，正式な PIA は PIA 評価者等が実施するものとしている．理由は主に，(1)PIA 支援ツール利用者が選択肢を誤って回答する可能性が考えられること，(2)法の各条項の例外条件を考慮していないこと，(3)本来 PIA は法への法的適合性の他，プライバシー保護等の観点でも評価するものであり，PIA 支援ツールでは後者を実装していないことが挙げられる．

6. おわりに

本稿では，PIA 会議における評価状況に基づき，案件担当者の法に関する知識・理解の現状を分析し，案件担当者の法に関する知識・理解不足は PIA 実践を妨げる要因となることを示した．また，従来の従業員教育で実施している法全般に関する基礎解説の内容は案件担当者の知識として定着しておらず，案件担当者は個人に関する情報を取扱う案件の発生時には，法の要点を手短に把握できる方法を求めていると考察した．この考察に基づき，PIA 実践に直結する法の基礎知識の習得支援方法と PIA 実践支援方法を検討した．一部に関してはプロトタイプを実装し，教材としての利用や PIA 実践の効率化が見込まれるとの予備評価を得た．今後の研究計画としては，PIA 活動を通じてプロトタイプの有効性を評価し，また公的部門（法第 5 章等）にも対応した PIA 支援ツールを開発予定である．

最後に，筆者らの組織の PIA 活動では我々の組織に留まらず，多くの組織で発生すると想定される問題が顕在化し，本稿で述べた筆者らの研究に繋がっている．本稿の内容が，PIA 実践支援技術の発展と普及に貢献できれば幸いである．

参考文献

[1] “個人情報の保護に関する法律（平成十五年法律第五十七号）”. https://elaws.e-gov.go.jp/document?lawid=415AC0000000057, (参照 2022-07-25).
[2] “個人情報の保護に関する法律についてのガイドラインに関する Q&A Q1-17”. https://www.ppc.go.jp/personalinfo/faq/APPI_QA/#q1-17, (参照 2022-07-25).
[3] “カメラ画像利活用ガイドブック v3.0”. https://www.meti.go.jp/press/2021/03/20220330001/20220330001.html, (参照 2022-07-25).
[4] “映像センサー使用大規模実証実験検討委員会：調査報告書”. https://www.nict.go.jp/nrh/iinkai/report.pdf, (参照 2022-07-29).
[5] “日本弁護士連合会：鉄道事業者における顔認証システムの利用中止を求める会長声明”. https://www.nichibenren.or.jp/document/statement/year/2021/211125.html, (参照 2022-07-29).
[6] “PIA の取組の促進について―PIA の意義と実施手順に沿った留意点―”. https://www.ppc.go.jp/personalinfo/legal/, (参照 2022-07-25).
[7] “DX 時代における企業のプライバシーガバナンスガイドブック ver1.2”. https://www.meti.go.jp/press/2021/02/20220218001/20220218001.html, (参照 2022-07-25).
[8] “令和３年 改正個人情報保護法について（官民を通じた個人情報保護制度の見直し）”. https://www.ppc.go.jp/personalinfo/minaoshi/, (参照 2022-07-25).
[9] “個人情報保護に関する法律・ガイドラインの体系イメージ”. https://www.ppc.go.jp/files/pdf/personal_framework.pdf, (参照 2022-07-25).
[10] “個人情報の保護に関する法律についてのガイドライン（行政機関等編）”. https://www.ppc.go.jp/personalinfo/legal/guidelines_administrative/#a4-1-1, (参照 2022-07-25).
[11] “ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment”. https://www.iso.org/standard/62289.html, (参照 2022-07-25).
[12] “JIS X 9251:2021 情報技術―セキュリティ技術―プライバシー影響評価のためのガイドライン”. https://webdesk.jsa.or.jp/books/W11M0090/index/?bunsyo_id=JIS+X+9251%3A2021, (参照 2022-07-25).
[13] Broadwell, Martin M. "Teaching for learning (XVI)". The Gospel Guardian. 20 February 1969. http://www.wordsfitlyspoken.org/gospel_guardian/v20/v20n41p1-3a.html, (参照 2022-08-01).
[14] “The Four Stages of Learning: They’re a Circle, Not a Straight Line”. https://www.gordontraining.com/leadership/four-stages-learning-theyre-circle-not-straight-line/, (参照 2022-08-01).
[15] “CMMI”. https://cmmiinstitute.com/cmmi, (参照 2022-07-25).
[16] “個人情報保護委員会：法令・ガイドライン等”. https://www.ppc.go.jp/personalinfo/legal/, (参照 2022-08-23)
[17] “ビッグデータ時代の研究の個人情報保護ルールの全体像を説明～「オープンサイエンスのためのデータ管理基盤ハンドブック」を発行～”. https://www.nii.ac.jp/news/release/2022/0727.html, (参照 2022-07-28).