特定個人情報保護評価ガイドラインの開発

永野　学†　畠山智美†　寺田佳代子†　瀬戸洋一†

†産業技術大学院大学
140-0011　東京都品川区東大井 1-10-40
seto.yoichi@aiit.ac.jp

あらまし　個人情報の漏えいを防ぐため，欧米では個人情報を扱うシステムの構築にあたり，漏えいリスクを事前評価するプライバシー影響評価が実施されている．日本でも 2013 年施行の番号法で行政機関等を対象に特定個人情報保護評価の実施が規定され，同保護評価指針が発行されている．しかし，同指針ではリスク評価の実施手順は明示されず，国際標準 ISO22307 への適合も不明確である．評価に実効性をもたせるためには，リスクを可視化し共有する統一的な手順が必要である．

今回，民間対応で開発した個人情報影響評価ガイドラインをベースに，特定個人情報保護評価ガイドラインを開発した．開発したガイドラインでは，国際標準と特定個人情報保護評価指針の手続に準拠し，リスク項目の分析方法などを明確にした．

Development of Guideline for Specific Personal Information Protection Assessment

Satoru Nagano† Tomomi Hatakeyama† Kayoko Terada† Yoichi Seto†

Advanced Institute of Industrial Technology
1-10-40, Higashi Ohi, Shinagawa ku, Tokyo 140-0011, JAPAN
seto.yoichi@aiit.ac.jp

Abstract　The Privacy Impact Assessment to evaluate in advance the risk of leakage of personal information have been conducted in Europe and the United States. Implementation of Specific Personal Information Protection Assessment is specified in the national ID number law in 2013 in Japan. The SPIPA procedure has been issued, but the implementation of risk assessment procedure is not explicitly, conform to ISO22307 is also unclear. In order to provide an effective evaluation procedures unified to visualize the risk is required. This paper describes the development of SPIPA guideline based on the PIA guidelines.

1.　はじめに

IT 技術の進歩により、電子化された個人情報の蓄積・利用が進み、市民生活や企業活動に利

便性をもたらす一方、個人情報漏えい・プライバシー侵害のリスクが増えた。ネットワーク上に一度漏洩した個人情報を取り戻すことは事実上不可能である。従来、P マーク（JISQ15001）など、運用面から個人情報保護を行う内部統制的な対策は実施されていたが、システムが適正に構築されていなければ、運用面での対策はコストがかかるうえ、本質的な問題解決にならない。個人情報を扱うシステムを構築する際、企画設計段階から個人情報の保護を考慮するプライバシー影響評価（Privacy Impact Assessment）の実施が北米、豪州を中心に広がり、2008 年には、PIA の実施手順および実施体制に関して具体的な 6 項目が定められた国際標準規格 ISO22307 が発行された［1］［2］.

日本では民間分野が先行して自主的に PIA を試行してきた. 2013 年 5 月に施行された番号法にて特定個人情報保護評価の行政システムへの実施が義務化された［3］-［5］。同保護評価では、評価の手続きや報告書のテンプレートなどを明記した指針が発行されているが、リスク評価の実施手順は明示されず、PIA の国際標準 ISO22307 への適合も不明確である。評価の質を確保するには、リスクを可視化する統一的な手順が必要である。

本稿では、先に開発した民間対応の個人情報影響評価実施ガイドラインをベースに、新たに特定個人情報保護評価ガイドラインを開発した。開発したガイドラインは、国際標準と特定個人情報保護評価指針の手続に準拠し、リスク項目の分析方法などを明確にした。

欧米ではプライバシー影響評価と呼ばれるが、機微な個人情報だけでなく、個人情報全般を保護の対象にするため、本稿では個人情報影響評価(Personal information Impact Assessment、以下 PIA)と呼ぶ。

2. 個人情報影響評価の概要

PIA は，個人情報の収集を伴う情報システムに対し，個人情報の漏えい防止とプライバシーリスクの回避または緩和のための法的・運用的・技術的な変更を促すリスク管理手法である［2］［3］.

日本では，「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、第 27 条において，PIA に相当する「特定個人情報保護評価」が定められた. 内閣総理大臣のもとに，特定個人情報保護委員会を設置し「特定個人情報保護評価」を実施することが定められているが，同法で規定する「個人付与の番号に関する特定個人情報」の保護が対象であり，現時点で「特定個人情報保護評価」に関する具体的な手順は明らかにされておらず，国際標準 ISO22307 への適合についても言及されていない.

3. 個人情報影響評価の実施手順

図 1 に個人情報影響評価実施手順の全体フローを示す［3］［6］. 以下，PIA 実施体制，実施計画，影響評価の実施，PIA 報告の順に解説する.

	予備PIAの実施	PIA実施計画書の作成	PIA評価の実施				PIA報告書の作成
	予備PIA報告書の作成	PIA実施計画書の作成	評価準備	個人情報リスクの識別	個人情報リスクの分析	個人情報リスクの評価	PIA報告書の作成
評価手順	・実施体制の構築	・目的の明確化	・評価関連資料の収集 ・参照法令や規格、ガイドラインなどの特定	・個人情報の識別	・影響度の評価	・評価シートによる評価 ・必要なリスク対応の検討	・PIA報告書の作成
	・対象範囲の特定 ・対象システムの概要	・対象範囲の特定	・対象システムの分析	・リスクシナリオの識別	・脆弱性の評価	・影響評価（双方向ギャップ分析）	
	・予備評価根拠資料の特定	・個人情報の扱いに関する確認	・（業務）データフローの分析	・既存または計画済み対策の識別	・発生可能性の評価		
	・予備PIA報告書の作成	・PIA実施計画書の作成	・評価シートの作成				
成果物	・予備PIA報告書	・PIA実施計画書	・システム分析書 ・個人データフロー分析書 ・評価シート	・個人情報管理台帳 ・リスク分析表	・リスク分析表	・影響評価結果書 ・評価シート	・PIA報告書

図１　個人情報影響評価実施手順の全体フロー図

3.1　実施体制

日本においてはPIAの実施対象を「公的分野」「公共性の高い民間分野」「一般的な民間分野」に分け，実施体制を構築することが適切である．行政機関など公的分野では，対象情報システムが要件を満たしているかを判断する監査的要素が強い．一方，民間分野では，PIA 実施過程において，PIA 評価者の助言を得て PIA 実施依頼組織が個人情報保護対策を図っていくコンサルテーション的な要素が強い。PIA は，実施対象により評価目的が異なることを考慮すべきであり、実施依頼組織のシステム開発プロジェクトチームの協力の下，評価組織により実施される．

3.2　予備評価

予備 PIA（以下，予備評価）では，情報システムで取り扱う個人情報の有無により，PIA 本評価実施の要否を判定し報告書にまとめる．主に公的機関において実施される．例えば，番号法における特定個人情報保護評価では，しきい値判断に相当する．一方，情報システムが個人情報を取り扱わない場合には，PIA は実施不要と判定される．

予備評価の結果が PIA 実施要の場合，実施スケジュールおよび体制（人員）確保，実施形態の決定，予算，対象範囲など，PIA を効率よく行うための情報を報告書に記載する．

3.3　実施計画

予備評価実施後，PIA 実施計画を策定し，PIA 実施体制を整備する．PIA の対象範囲，評価基準としての参照すべき法令や規格，ガイドラインなどの参照規定文書，組織の内部規程を特定し，スケジュールと共に PIA 実施計画書に記載する．

特に対象範囲に関して，プライバシーリスクに関するシステムと運用との責任範囲を明確にする．評価の対象は，システム構成図，システムを運用する組織体制，システムの運用管理に関する設計資料等のシステムに関する設計資料である．

PIA はシステム構築前に実施するため，システムにおける個人情報の扱いを定義した設計書が存在しない場合があり得る．この場合は，業務に関する個人情報フロー分析も評価の対象とし，計画に組み込む．

3.4　評価準備

(1) システム分析

影響評価を行う前に，評価対象であるシステムのハードウェア，ソフトウェアに関する機能と構成を明確に把握する．

PIA 評価チームは実施依頼組織から資料等の提供を受け，評価対象の範囲，システムの目的と機能を特定する．運用設計書・手順書をもとに安全管理措置について物理的対策，技術的対策，組織的対策を明確にし、システム分析，続いてリスク分析を行い、システム分析報告書にまとめる．

(2) 業務分析

システム分析同様，業務に関する個人情報フロー分析を行う．システム構築前で，個人情報の扱いを定義した設計書が存在しない場合は，個人情報の取扱いをシミュレーションする．

PIA 評価チームは，提供された資料をもとに，評価対象の範囲，および業務における個人情報を特定し，業務毎に個人情報管理台帳を作成する．作成した個人情報管理台帳をもとに，取り扱う個人情報の重要度，および個人情報に対する脅威と脆弱性のリスク分析を行い，業務分析報告書にまとめる．

(3) 評価シート作成

表１に示すように，評価シートは，評価基準として参照すべき法令や規格，参照規定文書から導出した要求事項を評価項目として一覧にし，チェックリスト形式でまとめたものである．評価シートには「評価項目」，「根拠規程」，「評価結果」，「指摘・推奨事項」，「査閲資料」の記入欄を作成する．

作成時に記入するのは，評価対象のシステムに対する要求事項を質問形式で表した「評価項目」，および参照規程文書名，条項番号などを表した「根拠規程」の 2 点であり，以降の欄は実際の評価実施時に記入する．

表1　評価シート作成例

大分類（OECD8 原則）		法令・規格					
	評価項目	法律	根拠規定	評価結果	指摘・推奨事項	査閲資料	備考
＜4＞ データ内容の原則							
1.	評価対象システムは、評価対象システムの利用目的達成に必要な範囲において、診療録、診療諸記録を電子保存する場合、個人データの真正性を保つため、以下の①～③の項目を満たす仕組みを備えているか。	個人情報保護法第十九条(データ内容の正確性の確保)	医療安全ガイドライン 7.10　電子保存における真正性の確保　【医療機関等に保存する場合】				
	①（認証管理）作成の責任の所在を明確にするための利用者の識別、認証の仕組みを備えているか。認証手段はバイオメトリクス、セキュリティデバイス、パスワード等の利用者しか持ちえない２つ以上の独立した要素を用いて行う方式を採用しているか。認証要素がユーザ ID とパスワードの単独の場合、それらの情報が本人しか知りえない状態に保つよう対策が行われているか。	-	医療安全ガイドライン 6.5C1 医療介護ガイドライン III 4(2)7.				
	②　（権限管理）評価対象システムは、医療従事者の職種やシステム管理者などの利用区分に応じて、システムに対する権限や役割を割り当て、管理する仕組みを備えているか。また、読み取り、変更、削除の等の操作権限を利用区分	-	医療安全ガイドライン 6.5B(2)C5. 情報の区分管理とアクセス権限の管理				

3.5　影響評価

図 2 に従い，評価の有する 2 つの観点から双方向ギャップ分析を行う．

(1) リスク対策計画の評価：評価シートの各評価項目に対してリスク分析表を確認し，評価対象システムのリスクの存在や対策の計画状況を評価する．

(2) 要求事項の完備性の評価：検出したリスクに対応する評価項目の存在を確認し，要求事項のリスク検討漏れの可能性を評価する．

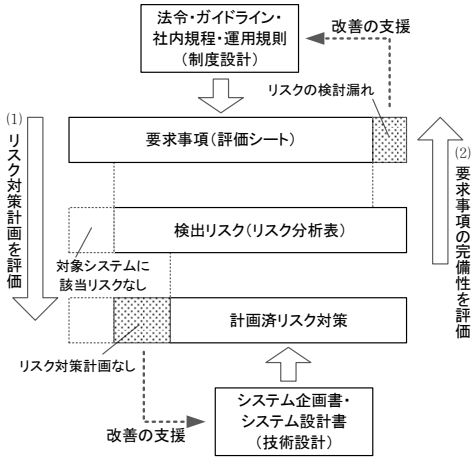

図2　双方向ギャップ分析

各評価項目について，対応するリスクの存在を，システム分析及び業務分析報告書のリスク分析表を利用して判定する．対応するリスクが存在しなければ，その評価項目に関して「該当リスクなし」という評価を与える．対応するリスクが存在する場合には，対策の計画状況について確認し，検証結果欄に記載する．その対策が適切であれば問題なし（適合），不十分また計画されていない場合には問題あり（不適合）の判定を行う．

3.6　影響評価報告書の作成・提出

報告書は，以下の記載区分によって構成する．

導入区分：　実施対象を以下の項目について記載する．

- 目的
- 期間，スケジュール
- 適用範囲
- 体制（PIA 評価チーム，PIA 実施依頼責任者）

概要区分：　業務・システム分析とリスク評価を記載する．

- 対象システムに関する記述（システム構成，取り扱う個人情報など）
- リスク評価実施手順およびリスク評価基準
- 実施にあたり使用した専門知識

意見区分：　評価結果（指摘事項および推奨事項）を記載する．

- 評価区分別の指摘・推奨事項数
- 対象システムが計画する安全管理措置に対する評価
- 法令やガイドライン，組織内規程の整備などに関する評価

民間における実施依頼組織は，評価結果の公開の義務はないが，個人情報提供者の理解を得るために，報告書を公開することを推奨する．一方行政や公共的な分野の PIA は，評価結果の公開が義務つけられる．

4. 特定個人情報保護評価ガイドライン

4.1 特定個人情報保護評価ガイドラインへの展開

特定個人情報保護評価ガイドライン作成にあたり、ポイントは次の 2 点である。

・影響評価の具体的かつ統一的な手順

・対象システム及び対象業務のリスク分析手順

特定個人情報保護評価指針は，報告書のフォーマットは定義されているが，影響評価に関する具体的な実施手順が明記されていない．また、特定個人情報保護評価（全項目評価）におけるプライバシーリスクの評価はリスク対策の有無の記述であり、リスク評価基準・分析手順が明記されていない。従って、影響評価のプロセスについては、評価者に委ねられてしまい、評価の中立性や専門性に問題が残る。

先に開発した民間対応個人情報影響評価ガイドラインにおける影響評価のプロセスは，特定個人情報保護評価（全項目評価）に対しても基本的に利用可能である［8］．

4.2 特定個人情報影響評価実施手順

図３に特定個人情報影響評価の実施フローを示す．個人情報影響評価のプロセスをベースに特定個人情報保護評価の報告書を作成する．

ハッチング部分が個人情報影響評価のプロセス，白抜き部分が特定個人情報保護評価指針で示されたプロセスである．また，表 2 に特定個人情報保護評価実施手順案を示す．

特定個人情報保護評価計画管理書を作成する場合，対象システムの分析が必要である．表 2 に示すように，ガイドラインの予備評価を実施し，作成した個人情報影響評価実施計画書をもとに特定個人情報保護評価計画管理書を作成する．

特定個人情報保護評価指針には，評価対象とするデータ数，扱う職員数などから基本項目，重点項目，全項目評価が決定されることが記述されているが，リスク評価の具体的な手順が明記されていない．このため，個人情報影響評価ガイドラインのシステム及び業務に関するリスク分析該当部分を利用しリスク評価を行い，双方向ギャップ分析により影響評価を実施する．

そして，個人情報影響評価報告書を作成した上で，全項目評価報告書などを作成することが適切である．パブリックコメントを求める際，全項目評価報告書では，結果しか記述されないため、その内容を理解することは困難である。このため、個人情報影響評価報告書を併せて公開することが適切である．

将来，民間組織，例えば金融機関などへの接続を考慮すると，国際標準に準拠した影響評価を実施することが重要であり，ガイドラインをベースに特定個人情報保護評価を実施することで，評価者によらない PIA の中立性や評価の質を維持する事が可能である．

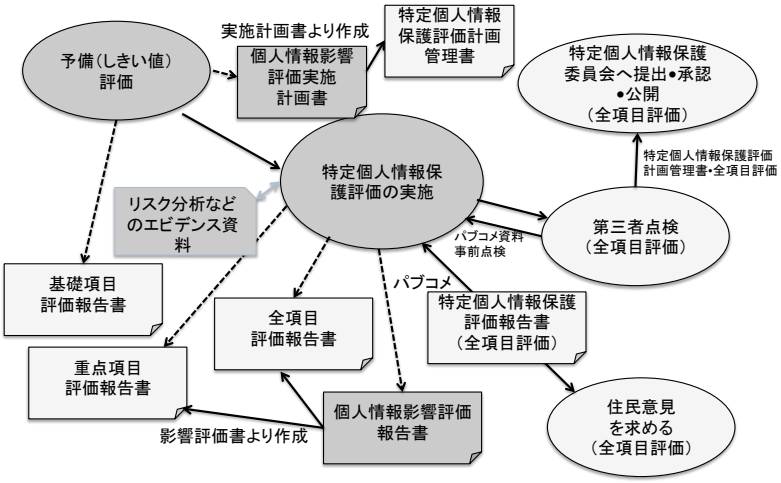

図３特定個人情報保護評価の実施フロー

表２　特定個人情報保護評価実施手順案

	予備PIA評価		影響評価(特定個人情報保護評価)				特定個人情報保護評価報告書の作成
	評価	しきい値評価	評価準備	リスクの識別	リスクの分析	影響評価	PIA報告書/特定個人情報保護評価報告書の作成
評価手順	•実施体制の構築 •目的の明確化	•しきい値判断	•参照法令や規格、ガイドラインなどの特定	•個人情報の識別	•影響度の評価	•評価シートによる影響評価 (双方向ギャップ分析)	•PIA報告書の作成
	•対象範囲の特定 •内部規定文書の特定		•(業務)データフローの分析 •システム構成の分析	•リスクシナリオの識別	•脆弱性の評価	•要求事項の完備性分析 (双方向ギャップ分析)	•ステークホルダーへの報告書の説明
	•対象システムの概要		•リスク分析	•既存または計画済み対策の識別	•発生可能性の評価		・特定個人情報保護評価報告書への転記
	•評価シート(テンプレート)による影響評価	•基礎項目報告書への転記	•評価シートの作成				
	•予備PIA報告書の作成 •実施計画書の作成	•計画管理書への転記					
成果物	•実施体制図 •WBS •システム構成図 •実施計画書 •予備PIA報告書	•基礎項目評価報告書 •計画管理書	•個人データフロー分析書 •システム分析書 •評価シート	・個人情報管理台帳 ・リスク分析表(個人情報フロー分析書) •リスク分析表(システムリスク分析書)	•リスク分析表	•影響評価結果 ・評価シート	•PIA報告書 •特定個人情報保護評価報告書(全項目、重点項目)

５．　おわりに

2016 年より番号法に定義される個人番号を取り扱いが開始する．個人番号を扱うシステムに対し特定個人情報保護評価の実施も義務づけられ，ますます個人情報の電子化，利用が増し，機微情報を含む個人情報保護の意識が高まる事が考えられる．

今回，特定個人情報保護評価の実施担当者の手引きとなるガイドラインを開発した．ガイドラインを参照することで，評価準備から実施，報告に至るまで統一した手順のもと，実施者の評価能力に左右されない「中立性」や「専門性」を確保した影響評価の実施が可能となり，特定個人情報保護評価の意義を明らかにすることができる．

今後、ますます個人情報影響評価に対する重要性が注目され，より詳細な分野別の実施ガイドラインの必要性が生じるものと考えられる．

参考文献

[1] 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
[2] 高坂定, 石田茂, 横山完ほか: 各国におけるプライバシー影響評価とハンドブックの整備に関する分析, 日本セキュリティ・マネジメント学会誌, Vol.27, No.1, pp.17-26 ,2013 年
[3] ISO22307 Financial services - Privacy impact assessment,2008 年
[4] 大類優子, 瀬戸洋一: プライバシー影響評価 ISO22307 の要求事項の分析, SCIS2010, 2010 年
[5] 前島肇, 瀬戸洋一ほか: プライバシー影響評価におけるリスクアセスメントの検討, IPS Japan, 2013 年
[6] 産業技術大学院大学: プライバシー影響評価ハンドブック, 2013 年
[7] 産業技術大学院大学: 個人情報影響評価　事例集, 2013 年, および産業技術大学院大学: 医療分野個人情報ガイドライン, 2013 年
http://aiit.ac.jp/master_program/isa/professor/y_seto.html, （参照 2014-04-01）
[8] 行政手続きにおける個人を識別するための利用等に関する法律, 平成 25 年 5 月 31 日公布
[9] 特定個人情報保護委員会 : 特定個人情報保護評価指針, 平成 26 年 4 月 20 日