1ZA-4

プライバシー影響評価実施における リスクアセスメントの検討

前島 肇† 鶴田 亜由美† 渡辺 慎太郎† 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 ISO 22307 を基に各国の事情に合わせた実施体制・手順を考慮し，プライバシーリスクの評価（アセスメント）を行う必要がある．

ISO 22307 では，PIA に関する要求事項は規定されているが，リスク分析の具体的方法は明記されていない．

本発表では，PIA におけるリスク分析の考え方を報告する．

2. プライバシー影響評価の概要

PIA の定義は，「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．

つまり，PIA は，以下の 2 点に特徴がある．

(1) 守るべき要求事項に対し，その適合性を評価する．

(2) リスクを軽減するための，技術的な対策のみならず，法整備などを促す．

PIA では，実施結果を踏まえ，必要に応じて構築システムに対して仕様の変更を促す．システム稼働前に変更を行うことにより，稼働後のプライバシー問題の発覚による稼動停止や，それに伴って発生するビジネス上のリスク，システム改修コストを軽減することができる．

また，システムを構築運用する組織（以下 PIA 実施依頼組織）が PIA 報告書を公表することで，プライバシーや個人情報の取り扱いに関して PIA 実施依頼組織，個人，マスメディアの三者で議論する共通の土俵を提供することができる．組織が個人の権利保護に留意している姿勢を関係者に示すことにもなる．すなわち，PIA はプライバシーに関するリスクコミュニケーション手段である．

PIA に関する国際標準規格は，国際標準化委員会 ISO TC68/SC7（金融サービス）が 2008 年 4 月に発行した ISO 22307 Financial services - Privacy Impact Assessment である．

3. プライバシー影響評価実施におけるリスクアセスメントの課題

図 1 は，ISO 22307 に準拠した PIA の手順を示す．

	PIA計画	PIA評価				PIA報告
	プロジェクト計画	評価準備	プライバシーリスクの識別	プライバシーリスクの分析	プライバシーリスクの評価	報告
評価手順	実施体制の整備	評価関連資料の収集	個人情報の識別	影響度の評価	必要なリスク対応の検討	PIA報告書の作成
	スコープの確定	対象システムの分析	リスクシナリオの識別	発生可能性の評価	プライバシー影響評価	
	参照法令や規格、ガイドライン、社内規程、契約類の特定	評価シートの作成	既存または計画済み対策の識別			
	PIA実施計画書の作成					
成果物	PIA実施計画書	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	リスク分析表	リスク分析表 評価シート	PIA報告書

図 1 PIA 実施手順

ISO 22307 は，①PIA 計画，②PIA 評価，③PIA 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の 6 項目を PIA 実施の要求事項としている[2]．

PIA のリスク分析は，②PIA 評価のフェーズで実施する．実施の方法は，システム構成の分析，データフロー分析などにより，対象システムの脅威脆弱性を把握した上で，法律やガイドラインから作成した評価基準である評価シートにおける準拠性をチエックすることで行う．

この場合の問題として以下の 2 点がある．

(1) 文書化したリスク分析を実施しないため，評価が属人的になる．

(2) 基準の適正性が評価できない．このため法制度の変更を促すことができない．

A Study of Risk Assessment for Privacy Impact Assessment
Hajime MAEJIMA†, Ayumi TSURUTA†,
Shintaro WATANABE† and Yoichi SETO†
†Advanced Institute of Industrial Technology

4. プライバシー影響評価実施におけるリスクアセスメントの提案

3 章の問題について以下の対応が必要である．
(1)個人情報にあったリスク分析の実施．プラバシーマークで実施されている，個人情報のライフサイクルにそったリスク評価方法を採用した．
(2)評価基準の準拠性のみでなく，リスク分析結果から得られる，技術的な側面および法的・運用的な側面の改善策を求める．

以上の方法を採用し，具体的には以下のような手順で実施した．

4.1 リスクアセスメントための基準

PIA におけるリスクの分析において，基準となる要求事項が必要である．これは評価シートとして作成する．評価シートは，OECD のプライバシー保護と個人データの国際流通についてのガイドライン，プライバシー・ポリシー，個人情報保護法，民法および刑法の関連条文，事業分野毎に所管省庁や業界団体が定めるガイドライン，契約，社内規程などをもとに作成する．個人情報保護法などコアとなる部分と業界毎あるいは社内規定などで定められた部分を追加するなどしてアセスメントのための基準を明確にし，評価シートを作成する．

4.2 対象システムのリスク分析

システム構成，業務プロセス概要，データフロー図，システムが取り扱う個人情報の台帳などをもとに対象システムのリスクを洗い出す．リスク分析では，リスクマネジメントの国際標準規格の ISO 31000:2009，情報セキュリティリスクマネジメント規格の ISO/IEC 27005:2011 などを参照し，また，個人情報保護マネジメント規格の JIS Q 15001:2006 が定める個人情報のライフサイクルを踏まえた評価を行う．個人情報について，取得・移送・利用・保管・廃棄の各ライフサイクルにおけるリスクの原因と結果，影響を検討する．

特定したリスクに対して定量的または定性的な評価を与え，必要とされるリスク対応を検討し，PIA 実施依頼組織で計画されたリスク対応策を確認の上，リスク分析表を作成する．

4.3 ギャップ分析

評価シートとリスク分析表を用いて基準（要求事項）へ合致しているかを分析する．

ギャップ分析はプライバシーの影響評価分析に相当する．図 2 で示すように，評価項目に該当するリスクがあり，その対策が計画されていない場合は，プライバシー適合性判定は不適合とし，評価対象システムに対して技術設計の見直しを促す．

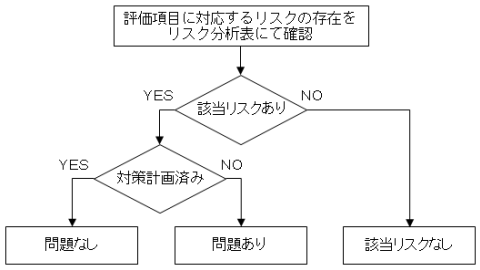

図 2 ギャップ分析の流れ

ギャップ分析において，対象システムが保有するリスクが基準として設定されていない場合がある．この場合は，基準（要求事項）に不備がないか確認し，規定自体を整備するか，運用においてリスクを軽減するような対策を講ずるか明確にし，必要に応じて制度設計を見直す．

図 3 で示すように，ギャップ分析により，要求事項，法令やシステムの逆分析および技術設計と制度設計の整備促進が可能である．

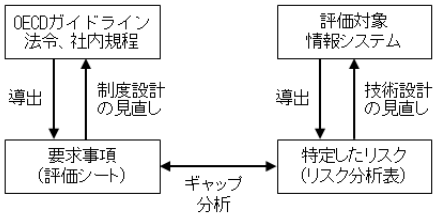

図 3 要求事項とシステムの逆分析

5. おわりに

ISO 22307 は PIA の要求事項が規定されているが，リスク分析の方法は明記されていない．本発表は PIA のリスク分析の方法を検討した．

PIA におけるリスク分析は，対象システム毎に作成する評価基準（評価シート）と対象システムに対し実施するシステム分析結果のギャップ分析により，評価基準への適合性評価と同時に評価基準に対する過不足が評価可能となる．この結果，新たな法整備などの提案も可能となる．

提案したリスク分析手法は，今回の発表では触れなかったが，実際の PIA 実施に採用し，その有効性を確認できた［2］－［4］．

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，瀬戸洋一ほか：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，ISEC，2011.11
[3] 渡辺慎太郎，瀬戸洋一ほか：プライバシー影響評価の健康診断総合システムへの適用，CSS2012，2012.11
[4] 鶴田亜由美，瀬戸洋一ほか：プライバシー影響評価の有効性評価に関する一考察，SCIS2013，2013.1