【講演レポート】JIPDECセミナー

PIAとは何か？PIAの進め方とポイントを解説

JIPDEC 電子情報利活用研究部 主席研究員
菊地 彰

PIA（プライバシー影響評価）とはなにか

PIAの定義

PIAとは、個人識別可能情報（Personally Identifiable Information　以下、「PII」という。）を取り扱うシステムにおいて、利害関係者に影響を与えるプライバシーリスクに対し、利害関係者とアセスメント及び協議するなどして事前にリスクを明確にする行為と定義されています。リスクを明確にする行為が、その結果責任に対し法的に追うべきか否かを決定する際の判断指標となります。

PIAの根底をなす思想として、以下の３つがあげられます。

1）プライバシー・バイ・デザイン※1

・PII（個人識別可能情報）を処理するプロセス、プログラム、ソフトウェア、モジュール、デバイス又はその他の取組みにおいて初期段階で実施する。

２）利害関係者のエンゲージメント

・PIAの準備段階で利害関係者をエンゲージメント（合意形成を図りその結果を約束）することで、実施するPIAのリスクを多角的に特定する。

・評価結果については利害関係者に対し、公表することが推奨されている。

３）デューデリジェンス

・ある行為者の行為結果責任を、行為者が法的に負うべきかを否かを決定する前に、行為に先んじて払ってしかるべき正当な注意義務及び努力。

※1　「ビジネス・プラクティス」、「物理設計」のデザイン（設計）仕様段階からあらかじめプライバシー保護の取り組みを検討し、実践すること。

PIIの見つけ方

PIAを行う際にはまず、PII（個人を識別できる情報）を正確に捉える必要があります。PIIは、個人情報保護法で言う個人情報よりも広く個人に関連する情報を対象としており、単なるデータとしてではなく、人が相手だと認識することが必要です。

PIA実施のタイミング

新たにシステムの要件定義や基本設計等を行う前の実施が大前提となります。すでにあるシステムやサービスを改変する場合は、従来のPIIの範囲を拡大する、取得方法を変更する、取得・利用等の業務手順に大きな変更があった場合など、それぞれの状況に応じて実施するタイミングを見定める必要があります。

PIAの進め方

PIAの基本的なプロセス

PIAの必要性の決定から、PIAのフォローアップまでおおまかに7段階の手順に沿って進めていくことをお勧めします。（図1）

まずは、特定個人情報保護評価やGDPR（一般データ保護規則）等を参考に、しきい値分析やPIA実施が必要か、また必要な場合の範囲等の判断を行います。実施必要性が決定した後は、利用するPIIが利用者へ与える影響レベルやリスクの起こりやすさをレベル分けする作業、利用者への配慮の分析など各リスク基準を定義することになります。

その後、実施責任者の任命や実施計画書の作成、利害関係者のエンゲージメントなどの準備を経て実行フローへ移行することになります。

利害関係者へのエンゲージメントはとても重要で、企業側は第三者視点を理解することができ、またリスク特定の際も客観性を持たせることができます。

PIA実施後は、報告書を作成し広く広報することが推奨されており、再実施の計画等、フォローアップも重要なステップとなります。利害関係者からのフィードバックもPIA報告書へ記載するとよいでしょう。

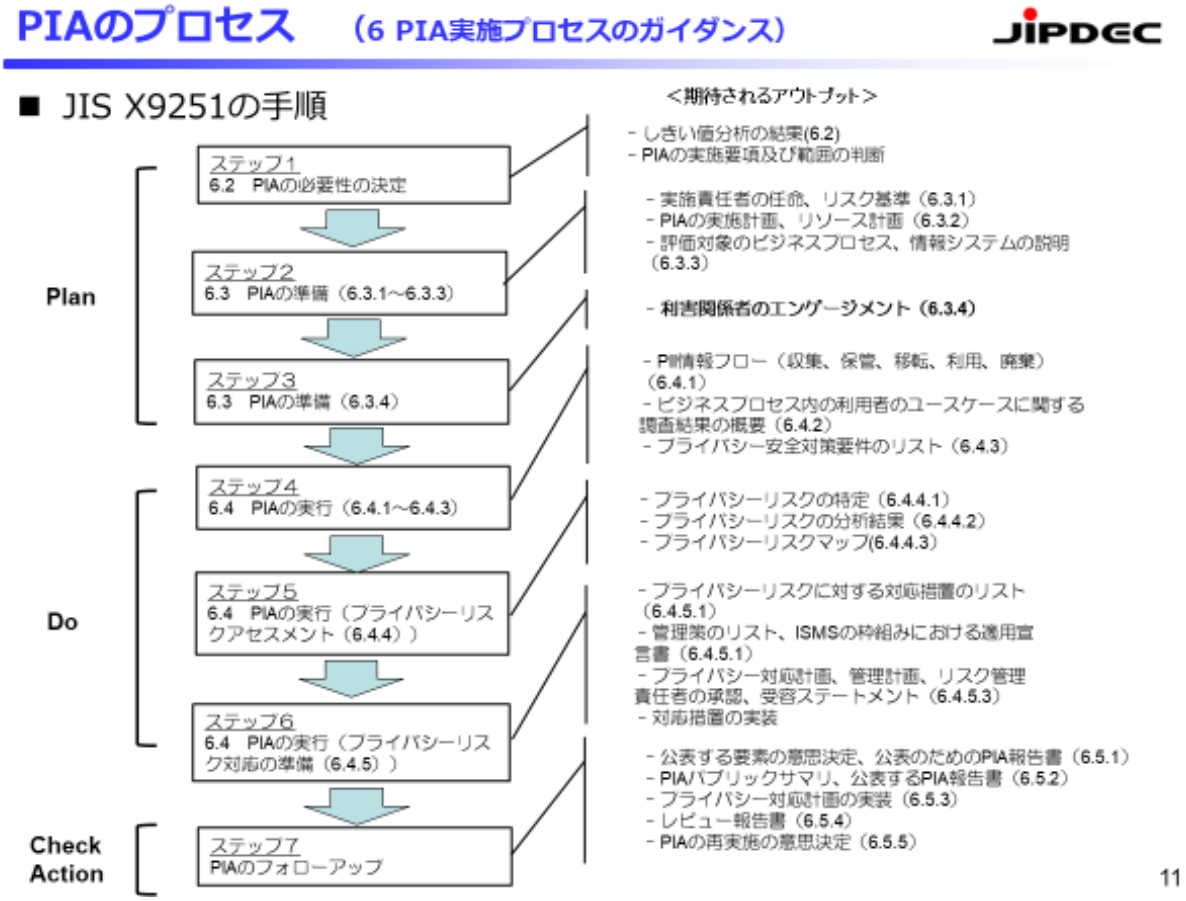

図1.PIAのプロセス

PIAの実行

PIAの実施概観

サービスのフロー図(図2)を「利用者」が見てわかりやすく作成することが重要となります。PIIについても、「誰のPIIが、何のために、どのように使われるのか」を明記してください。

本当に必要なPIIであるのかを精査した上で、PIIのライフサイクルや保有、廃棄の期間なども明記します。また、組織としてのリスクとサービスで起こりうるリスクは分けて考え、その全てにおいて、各事業者のレベルにあったベストエフォートの選択を行う必要があります。

なお、フローにおいては、システム自体の構成をフロー化し分析することもひとつの方法です。この場合、当該システムがどのように構成されているのか、その中でどのようにデータが移動し処理されているのかなどシステム構造を明確に示すことになりますので、企業の技術情報、個人情報の管理に関する情報、対象サービスのノウハウなどが含まれるため、公表することを前提に考えると公表用のPIA報告書に若干手間がかかってしまう点は懸念点としてあげられます。

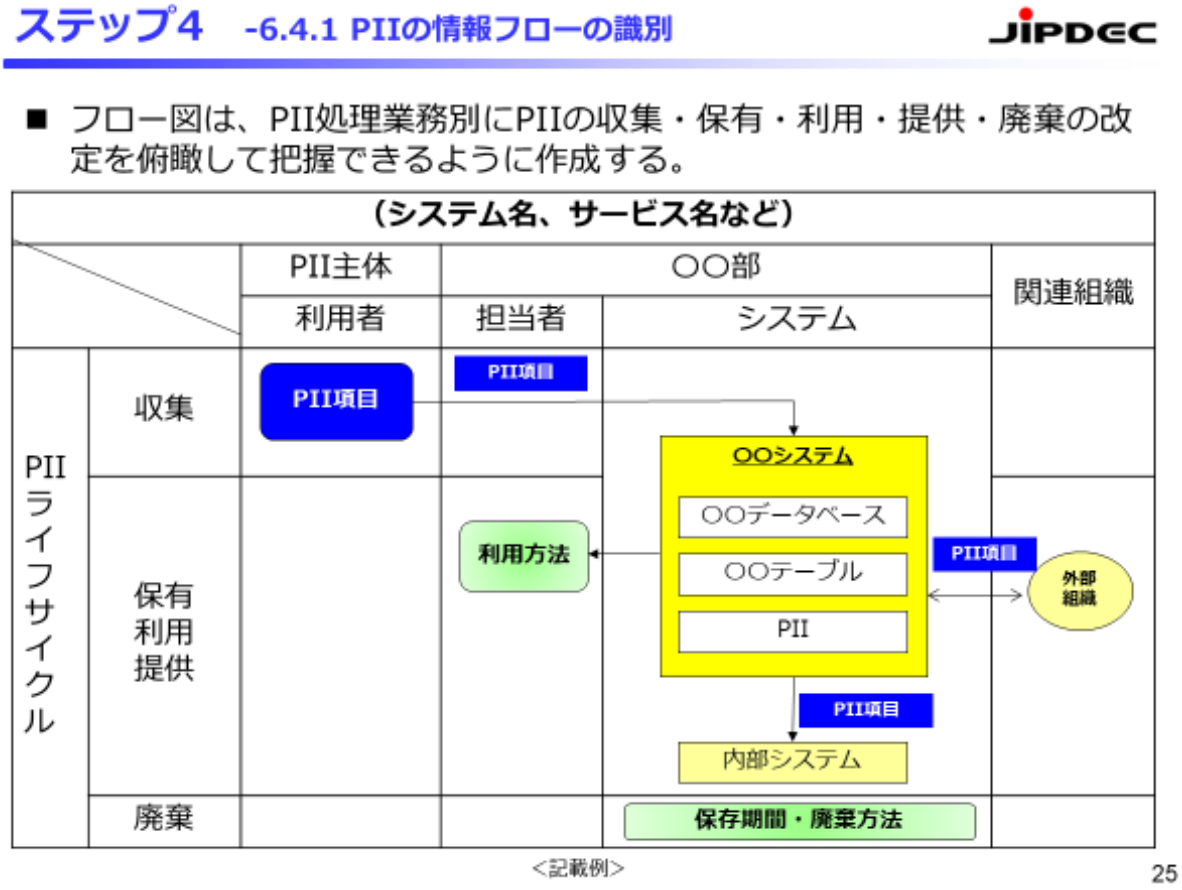

図2. PII実施フロー図（例）

リスク分析の考え方

プライバシーリスクの特定

プライバシーリスクは、「PII主体の観点に基づくプライバシーリスク」と「組織の観点に基づくプライバシーリスク」のふたつに分けて分析することが必要となります。

プライバシーリスクであると特定する際の判断基準は、利用者の基本的権利が守られているかどうかという点になります。その上で、PIIへの認可されていないアクセスがあるか、認可されていない変更がなされていないか、PIIの紛失・盗難等がないかなどをJIS X 9251に記載されている項目に沿って確認を行ってください。

プライバシーリスクの分析

JIS X 9251に記載されている、利用するPIIが利用者に与える影響レベルやリスクの発生のしやすさを推定するレベルを用いて、プライバシーリスクマップを作成します（図3）。

マッピングした上で、レベルの高いものから順に対策を講じてください。

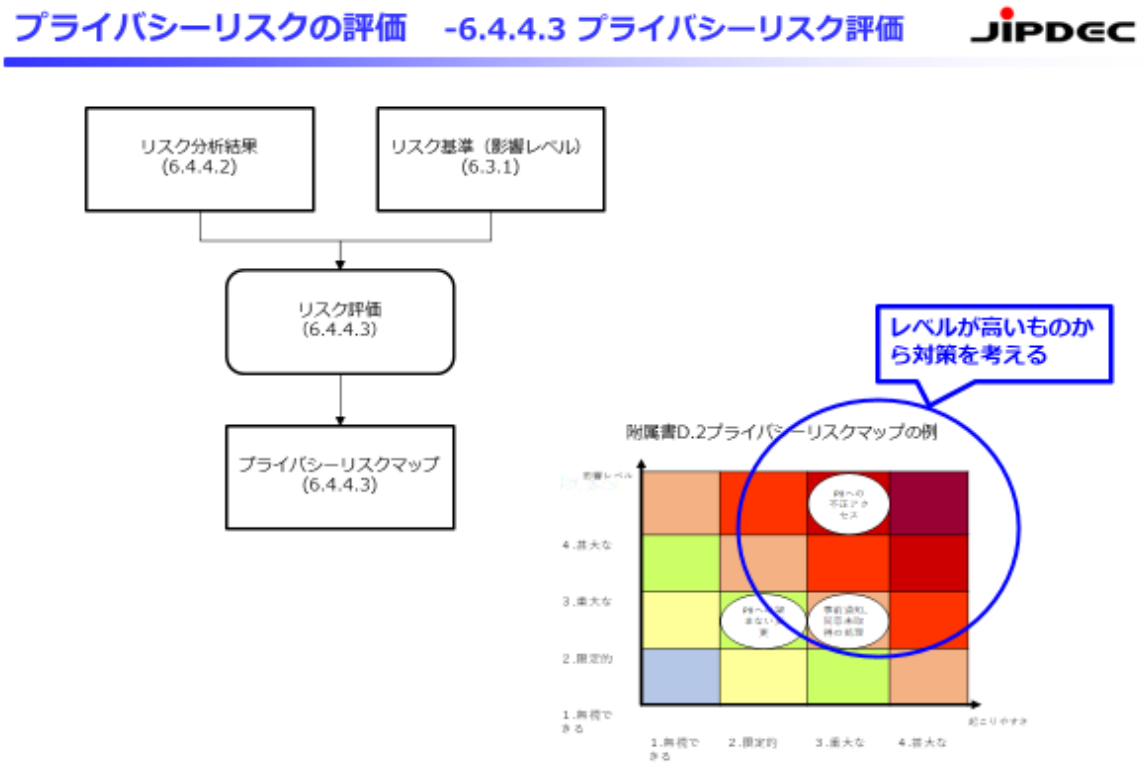

図3. プライバシーリスク評価（プライバシーリスクマップの例）

プライバシーリスクの対応

リスク対応措置の選択肢としては、4段階（低減、保有、回避、移転）があります。以前、JIS化の委員会において、「リスク保有」については、個人のリスクを企業側が勝手に評価し保有してもよいものかという議論がありました。その際は、利害関係者のエンゲージメントという工程の中で保有の可否について協議ができている場合は、企業側がリスクを保有する判断ができるという結論に至りました。

PIA報告書

現在、PIA報告書のフォーマットはないので、日本においては特定個人情報保護評価の形式を用いる方法が考えられます。今後は、民間で活用できるフォーマットのニーズが高まっているので、ぜひ、個人情報保護委員会等から近く公表されることを期待しています。JIPDECもその一翼を担えれば幸いです。

PIAの公表

PIAの結果は、利害関係者への通知が推奨されています。現状、民間においては、事業の機密情報、セキュリティ情報等が含まれていることもあるため国内外含め公表されないケースが多いと認識しています。

ただし、今後の流れとしてデータを利活用する組織はプライバシー保護の説明責任を確保するためにもPIAレポートを作成し、公表することで、当局からの照会に対して迅速に対応することができると思います。

また、PIAレポートの公表は企業の信用獲得にもつながります。ぜひPIAの実行・公表に取り組んでいただければと思います。

以上

JIPDEC 電子情報利活用研究部 主席研究員
菊地 彰

前職にて、Pマーク取得を推進し個人情報保護監査責任者を経験。
昨年度JIS X 9251作成の事務局を担当し、その後、東京都、団体の特定個人情報保護評価委託作業を担当する。

本内容は、2021年2月25日に開催されたJIPDECセミナー「プライバシー影響評価（PIA）のススメ」講演内容を取りまとめたものです。