【講演レポート】

民間におけるPIAの取組（企業におけるプライバシー保護の勘所）

株式会社日立コンサルティング
スマート社会基盤コンサルティング第2本部
ディレクター　美馬　正司氏

プライバシーガバナンスのためのPIA

2011年に世界経済フォーラムのレポートで「パーソナルデータは新たな原油である」と言われてから約10年、ビジネスの世界においてパーソナルデータ活用の取組みが進められてきました。その検討の中で、匿名加工情報化しての二次利用や、本人同意のもとで活用する情報銀行のような検討もなされてきています。

さらに、新型コロナの影響により社会環境全般が変化し、私たちの活動の場がオンライン主流となる中で、様々な手続きがデジタル化し、パーソナルデータのデジタル化も急速に進んでいますが、一方で、新型コロナ対策アプリの開発等を通じて、プライバシーと公益の両立という課題も顕在化しており、ビジネスを進める上でもプライバシーガバナンス実施の重要性を実感しています。

実際にプライバシーガバナンスを業務プロセスの中で回していく際、考え方の基盤となるのがPrivacy by Designで、それを実践するためのツールがプライバシー影響評価（PIA）です。PIAに関しては標準化が進んでおり、今回、国際規格（ISO/IEC29134）をJIPDECが原案作成しJIS化（JIS X 9251）されました。

日立におけるプライバシー保護の事例

IoTやAI、ドローン等、日立のビジネスを支える技術革新とパーソナルデータ活用・保護は切り離すことができないので、事業リスクを最少化させるための取組みが不可欠です。このため、日立製作所では以前から、博報堂と共同で消費者意識調査を実施したり、情報システム部門においてPIAに取り組んできました。さらに現在では、単にリスクヘッジのためだけでなく、企業ブランド向上という攻めの点からもプライバシー保護への取組みを重要視しています。

プライバシー保護体制

日立では、パーソナルデータ責任者である情報通信システム関連部門CIOの下に、プライバシー保護諮問委員会という組織を設置して、実務の中でのプライバシー保護について助言・支援を行っています。

PIA

新たなパーソナルデータを扱う業務の検討に際し、チェックリストによりPIAを実施、高リスクの場合にはプライバシー保護諮問委員会でリスク低減策の検討・適用を行ったうえで、実業務を開始するという流れになっています。

私たちが行っているPIAでは、対象を単に個人情報だけでなくパーソナルデータ全体としているところが特徴的です。ビジネスにおいてパーソナルデータ全般の扱いに配慮する必要性は、経済産業省のプライバシーガバナンスガイドブックでも指摘されています。また、改正個人情報保護法でも”個人関連情報”という定義で追加されるなど、今後対応が求められるものと思われます。

企業におけるPIA試行事例

PIA試行の背景と実施手順

2019年に公表された個人情報保護法　制度改正大綱では、PIAに対する民間の自主的な取組みが推奨されており、今後プライバシーガバナンスの必要性が高まることが想定されます。また、ISO/IEC29134のJIS化の動きも出てきたため、ある企業においてPIAを試行を行いました。試行の実施手順と各段階での作業項目は以下のとおりです。

PIA試行の実施手順

HITACHI
Inspire the Next

	作業項目
実施方針の検討	評価対象とする事業の選定
	PIAの実施手法の精査
PIAの対象となる事業の整理	PIAの対象範囲の設定
	対象とする事業に係るビジネスプロセス、情報システム、組織等の整理（取り扱われるパーソナルデータを特定した上で整理）
	評価対象となるビジネスプロセス、情報システム等の詳細化（PIIの収集方法、処理方法、処理目的、利用方法、管理・変更方法、廃棄方法、責任者等）
	ユーザーのユースケースの設定
プライバシーリスクの分析、整理	コンプライアンス要件等の整理
	プライバシーリスクの特定
	プライバシーリスクの分析、評価
	プライバシーリスク対策の検討
	プライバシーリスク管理策の検討
PIA報告書等のとりまとめ	プライバシーリスク対応計画の作成
	PIA報告書の作成

 71

評価対象事業の整理

最初に、業務フロー図を用いてビジネスの流れを把握するとともに、使用するシステムの機能や構成を図示して整理しました。ここで非常に重要視したのが、ユーザー・消費者目線を取り入れるということです。実際には、サービスデザインの際に用いられるジャーニーマップ等の手法を用いて、利用者がどのような行動の時にどのように感情が変化するか、という点まで検討を行いました。

コンプライアンス要件の整理

次に、リスクの洗い出し・分析の際に配慮すべきコンプライアンス要件を整理しました。個人情報保護法の準拠はあくまでもベースラインであり、その他、様々な規格や業界ごとのガイドライン等ソフトローと呼ばれるものも踏まえて、リスクを洗い出していく必要があります。

加えて、私たちがこれまでのビジネスの中で蓄積したノウハウをもとにチェック項目（以下の表は一部抜粋）を作成し、コンプライアンス要件と併せてプライバシーリスクをチェックしました。注意いただきたい点は、これらのチェック項目は汎用的なものではなく、ビジネスの内容に応じて変えていく必要があるということです。

プライバシーリスクの特定

HITACHI Inspire the Next

● コンプライアンス要件以外のプライバシーのチェック項目を踏まえ、プライバシーリスクをチェックする。

プロセス	確認項目
収集	• 個人情報を収集する対象、取得方法、取得する内容、取得する目的 • 本人から収集する際の通知や同意の方法 • 収集する主体がどのようになっているか（個社か共同利用か等）
保管・管理	• 委託先等も含めて個人情報の安全管理 • 個人に対する適切な情報の開示 • 個人からの請求等への対応 • 個人情報に関する記録 • 正確性が担保とID管理
利用	• 個人情報を利用する目的や利用主体 • 加工や分析の内容、方法 • 個人に対してフィードバックする仕組みの有無 • 加工された情報が二次利用される可能性 • 他のデータと結合したり、新たなデータが生成される可能性
移転	• 提供先の第三者の利用範囲や管理 • 加工した個人情報の第三者提供の有無 • 移転先で他の個人情報と結合される、あるいは個人情報に戻る可能性
削除	• 保存期間の設定 • 適切に廃棄・削除

 17

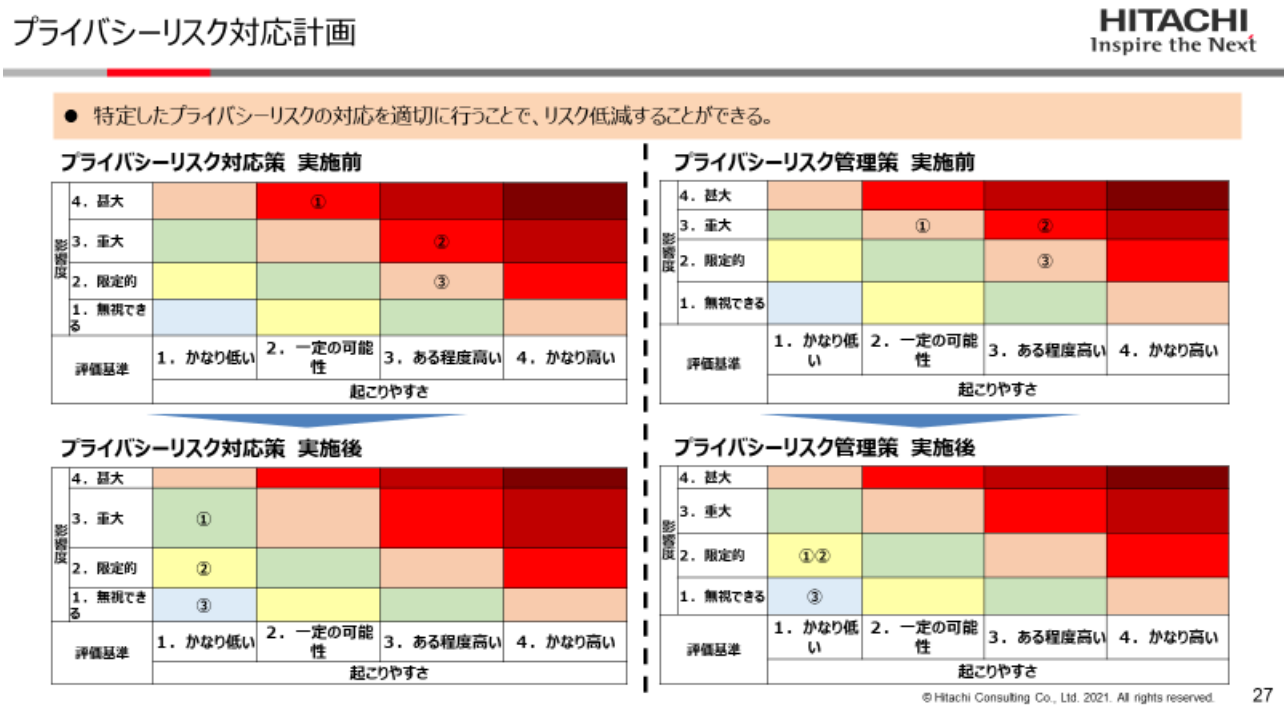
プライバシーリスクの分析、評価、対応策の検討

プライバシーリスクを特定後、それぞれの影響の大きさ、起こりやすさのレベルを推定し、プライバシーリスクマップにプロットし優先度をつけた上でリスク対応を検討します。通常、PIAは事業開始前に行うため静的なものとなりますが、私たちは、事業は事業や社会の環境が変化する中で5年10年と継続する可能性が高いので、変動要因も想定して管理策を検討しておくことが有効だと考えています。変動要因には、法制度や事業目的の変化だけでなく、技術の変化も含まれます。技術が進化すれば生成されるデータが異なり解析結果も異なるため、技術変化がデータ品質に及ぼす影響等も定期的にモニタリングする必要が出てきます。

プライバシーリスク対応計画

次に、検討した対応策を実施するため、対応策と対応期限、管理策と実際にモニタリングするタイミング等を決定し、プライバシーリスク対応計画、管理計画として報告書に取りまとめます。この報告書の内容を情報公開する必要があるかどうかについては、現在、明確な解がありません。報告書を公表することで、別のリスクを生む可能性もあるため、対外的な取り扱いのあり方は今後の検討課題だと感じています。

上記計画をもとに、管理責任者が対応策・管理策を実施した後は、実施前と実施後のリスク評価を行い、リスクが低減したことを確認してPIAは終了となります。



先ほど、リスク評価は影響度と起こりやすさを基準とするとお伝えしましたが、実際の対応場面で、例えば情報漏えいに関して言えば、「データの内容」が変わらない限り、漏えいした場合の影響の深刻度を変えることは困難です。一方、情報漏えいの起こりやすさは、実際にリスク対応することで劇的に下げることが可能なので、こちらでリスク低減を行うことになります。

まとめ

日々のビジネスを通じて、プライバシーガバナンスのニーズは今後ますます高まってくると感じています。これまではリスクヘッジという守りの姿勢で行われてきましたが、今後は「プライバシー保護に真摯に向き合っている」こと自体を企業の競争力に変える、競争力の源泉としてPIAの取り組む、そういった攻めの姿勢で取り組んでいくことが非常に重要になってくると考えられます。

日立でも、情報通信システム関連部門でプライバシー保護の仕組みを運用しており、その一環でPIAも実施していますが、ISO/IEC29134をフルスペックで実施することはそれなりに労力もかかるため、

すべての案件に実施することは現実的とは言えません。また、ISO/IEC29134、JIS X 9251はプロジェクトマネジメントで言うところのPMBOKであり、必ずしもその内容をすべて行う必要があるものでもないので、ビジネスや取り扱うデータの種類・量、企業規模に応じて、PIAの実施対象や内容を調整することが重要になってきます。

以上

株式会社日立コンサルティング
スマート社会基盤コンサルティング第2本部
ディレクター　美馬　正司氏
慶應義塾大学　政策・メディア研究科　特任教授
シンクタンク等を経て、2007年から日立コンサルティングに入社。情報大航海プロジェクト等、国の大規模プロジェクトのプロジェクトマネジメントを経験するとともに、プライバシー等、関連する制度面の検討に従事。匿名化、プライバシー保護、AI倫理等に関するコンサルティングを展開

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～取組みの必要性とビジネスへの生かし方～」での講演内容を取りまとめたものです。