個人情報保護法への企業の対応

リスクマネジメントと事例から見た実務の要点

島田裕次 著

日科技連

まえがき

デジタル技術の進展に伴って、DX(デジタルトランスフォーメーション)が注目を集めており、企業が厳しい競争を勝ち抜くためには、DX を推進することが求められている。DX の推進においては、デジタル技術よりもデータが重要な意味をもっている。例えば、AI(人工知能)を活用したビジネスを行う際には、AI の解析対象となるデータが重要であり、いかにビジネスにとって有益なデータを収集し解析するのかが AI 活用の成否を左右するからである。

データのうち特に重要なものが個人データである。個人データは、営業活動を始め事業活動を行う上でのキーになるからである。しかし、個人データの活用に際しては、個人情報保護法や各種ガイドラインの遵守が必須であることを忘れてはならない。

本書では、企業を対象にして、個人情報保護に関するポイントを解説するとともに、リスクマネジメントの視点から説明している。さらに、個人情報に関わるインシデント(事件・事故)事例を紹介して、理解しやすい内容にしている。

なお、2021 年改正で追加された地方自治体や学術研究団体については、説明から除いている。

本書の構成は、次のようになっている。第 1 章では、個人情報保護の歴史を含めて、デジタル社会における個人情報保護の意義について説明し、第 2 章では、本書の中心となる 2020 年および 2021 年改正個人情報保護法のポイントを解説する。改正の背景、概要などについて説明した後に、同法の具体的な内容について説明する。2021 年改正については、未確定な部分があるので、今後の動向に注意されたい。

第 3 章では、安全管理措置(個人情報保護対策)について、個人情報保護ガイドラインの分類に沿って、組織的安全管理措置、人的安全管理措置、物理的安

全管理措置、技術的安全管理措置について説明する。

第4章では、個人情報と関連が深いマイナンバーについて、マイナンバーに係るガイドラインに沿って説明し、第5章では、個人情報保護に関わる欧州(EU)の取組状況を紹介する。GDPRという言葉を聞かれた方も少なくないと思うが、EUで事業展開する企業は、その内容を理解しておく必要がある。

第6章では、個人情報に関わるインシデント(事件・事故)事例を紹介する。個人情報保護対策を講じる場合には、個人情報に関わるインシデントから学ぶべきことが多いからである。また、経営者を始め個人情報に携わる者に対して個人情報保護の重要性を認識してもらう場合には、実際に起きたインシデント事例を使って説明するとわかりやすいからである。

第7章では、リスクマネジメントの視点から個人情報保護について解説する。個人情報保護法では安全管理措置がポイントになるが、情報セキュリティ対策と類似点が多い。そこで、効率的・効果的な安全管理措置を講じる際には、リスクマネジメントと整合をとる必要がある。

第8章では、外部委託先管理、システム開発・運用管理に加えて、クラウドサービス、SNS、IoTを利用するときや、テレワークを行うときの管理ポイントを説明している。また、第9章では、情報セキュリティ、内部統制などとの関係について説明する。さらに付録として、個人情報保護チェックリストとマイナンバー保護チェックリストを加えたので、実務での参考にされたい。

本書の執筆に際しては、日科技連出版社の鈴木兄宏氏から貴重な御意見や助言をいただいており、この場を借りて御礼を申し上げたい。最後に、本書が企業における個人情報保護の推進に貢献できれば幸いである。

2021年11月

島　田　裕　次

個人情報保護法への企業の対応

目次

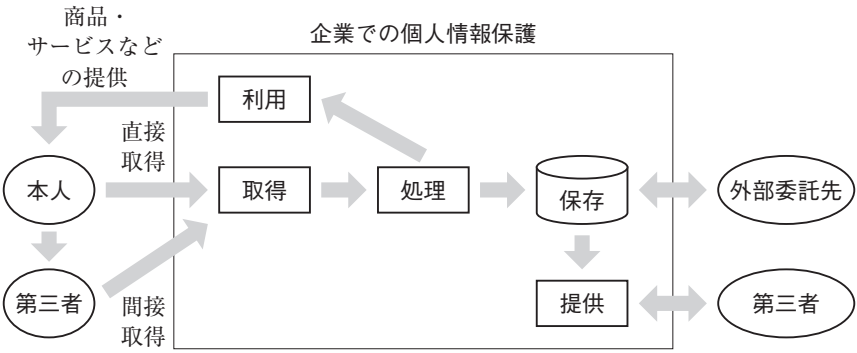

図 7.9　個人情報の取扱いの全体像

大事なリスクを見落とすことにつながりかねない。全体像を考えて、体系的、網羅的にリスク評価することがポイントである。

(3) 個人情報保護リスクの洗い出し方法

個人情報保護リスクは、例えば、以下に述べるように、インシデントから考える方法、個人情報のライフサイクルから考える方法、個人情報のアクセスポイント、法令・ガイドラインから考える方法がある(**図 7.10**)。

個人情報を洗い出したら、洗い出した個人情報について、どのようなリスクがあるのかを検討する。個人情報保護におけるリスクには、例えば、次のようなリスクが考えられる。

- 個人情報の不適切な取得
- 個人情報の不適切な利用
- 個人情報の不適切な第三者提供
- 個人情報の漏洩
- 個人情報の誤廃棄

(a) インシデント(事件・事故)から洗い出す方法

個人情報に関わるさまざまなインシデント(事件・事故)を参考にして考える

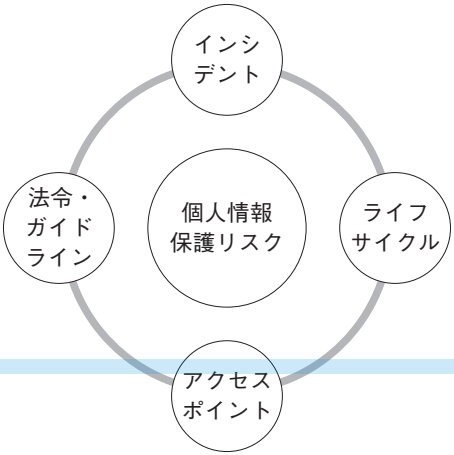

図 7.10　個人情報保護リスクの洗い出し方法

方法がある。しかし、このようなアプローチでリスクを洗い出すと、リスクを網羅的に把握することが難しいので、リスクの把握漏れが生じるおそれがある。

なお、インシデント事例については、**第 6 章**を参照されたい。

(b) ライフサイクルから洗い出す方法

個人情報に関わるライフサイクル(業務フロー)に沿ってリスクを洗い出す方法がある。つまり、個人情報の取得から廃棄までのライフサイクルから、個人情報についてどのようなリスクがあるのかを洗い出す方法である(**図 7.11**)。

例えば、販売業務プロセスを考えてみると、まず、顧客から個人情報を取得する時点から、最後に個人情報を廃棄する時点までの一連のプロセスを把握する。次に、個人情報の取得するときに情報の記入ミスが発生するリスク、個人情報が記載された書類を紛失してしまうリスク、業務に関係のない者が顧客の情報を閲覧してしまうリスク、などを販売業務プロセスのどこにどのような個人情報保護に関わるリスクがあるかどうかを洗い出す。このような手順で個人情報保護に関わるリスクを洗い出せば、リスクの全体像を把握しやすい。

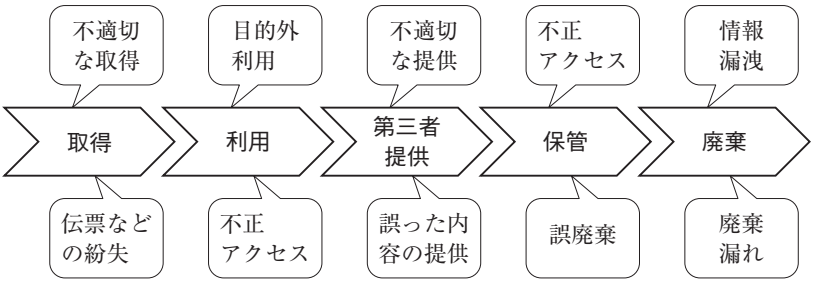

図 7.11　ライフサイクルから見たリスク

(c) 個人情報のアクセスポイントから洗い出す方法

個人情報保護に関わるリスクは、当然のことながら個人情報が存在している場所に存在する。リスクの洗い出しでは、個人情報がどこにどのように利用・保管されているか把握することが重要である。例えば、次のような個人情報へのアクセスポイントを考えるとよい。

- 情報機器(サーバー、パソコンなど)
- キャビネット、倉庫など
- 外部委託先
- クラウドサービス

(d) 法令・ガイドラインでの要求事項に沿って洗い出す方法

個人情報保護に関わるリスクのオーソドックスな洗い出し方法は、個人情報保護法、番号法の要求事項について、それを遵守しているかどうかをチェックする方法である。個人情報保護法や番号法では、具体的な内容がわかりにくいので、実務上は、個人情報保護やマイナンバーに関するガイドラインを参照してリスクを洗い出すことになる。

そこで、個人情報やマイナンバーの管理部門は、法令やガイドラインを十分に理解しておく必要がある。

表 8.1　クラウドサービスの管理ポイント

項目	管理ポイント
個人情報に関わるシステムでのクラウド利用方針が明確になっているか	• 導入してよいサービスの明確化(例：個人情報に関わるシステムについてのクラウドサービスを導入可否) • 個人情報の利用目的の明確化(例：自社の競争優位の確保との関係) • 自社開発、パッケージ調達との比較基準(個人情報の保護の視点)
クラウド利用における個人情報保護リスクを分析したか	• リスクの網羅性 • リスクの把握手順(誰が、いつ、どのようにして行ったのか？) • リーガル部門やコンプライアンス推進部門の参画
リスク分析の結果、どのようなリスクを把握したか	• クラウドサービス自体に関するリスク • クラウドサービスと自社システムとのインターフェースに関するリスク • 自社システムに及ぼすリスク
把握したリスクの大きさをどのように評価したか	• クラウドが利用できなくなった場合の個人情報に関わる社内業務や顧客への影響 • 世界各地で発生した障害などによるクラウドサービスへの影響 • 復旧までの手順の明確化(障害復旧目標時間を含む)
クラウドサービス・ベンダーの選定をどのように行ったか	• 複数案(機能・価格・継続利用性、認証取得、個人情報保護体制など)の比較・検討 • 利用規約の確認 • ベンダーの評価 • 提供機能とクラウド化する自社業務の F&G(フィットアンドギャップ)分析 • 自社業務プロセスの見直し
リスクへの対応策(コントロール)を検討したか	• リスクとコントロールの整合性 • コントロールの費用対効果 • 暗号化ツールは何を利用しているか？ • 暗号化クラウドサービス・ベンダーが提供する暗号化ツールではなく完全な第三者の暗号化ツールの利用
クラウドサービスに関するモニタリングを行っているか	• ベンダーの経営状況 • ベンダーの社会的な評判 • 従業員などの監督・教育(特に個人情報保護)の実施状況
クラウドの BCP を策定しているか	• クラウドのレスポンスが低下したとき、利用ができなくなったとき • 自社システムおよび顧客への影響

著者紹介

島田裕次（しまだ　ゆうじ）　博士(工学)
東洋大学総合情報学部教授。東洋大学産学協同教育センター センター長
川越市個人情報保護審議会会長(2019 年～)

[略歴]

1979 年早稲田大学政治経済学部卒業。同年東京ガス株式会社入社。情報通信部、経理部などで勤務し、2000 年から監査部で勤務(情報システム監査グループマネージャー、業務監査グループマネージャー、会計監査グループマネージャーを歴任)。2009 年 4 月より現職。日本大学商学部非常勤講師(コンピュータ会計論)を兼務

[資格]

公認内部監査人(CIA)、公認情報システム監査人(CISA)、経済産業省システム監査技術者

[主な著書]

『はじめての内部監査』(単著)、『内部監査の実践ガイド』、『内部監査人の実務テキスト［基礎知識編］』、『同［業務知識編］』(編著、いずれも日科技連出版社)、『よくわかるシステム監査の実務解説(第 3 版)』(同文舘出版)、『内部監査入門』(翔泳社)、ほか多数

個人情報保護法への企業の対応

リスクマネジメントと事例から見た実務の要点

2021 年 12 月 28 日　第 1 刷発行

著　者　島田裕次
発行人　戸羽節文

検　印
省　略

発行所　株式会社 日科技連出版社
〒151-0051　東京都渋谷区千駄ケ谷 5-15-5
DS ビル
電話　出版 03-5379-1244
営業 03-5379-1238

Printed in Japan

印刷・製本　㈱三秀舎

ISBN 978-4-8171-9749-8

URL　https://www.juse-p.co.jp/