

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

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という言葉が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ます。この場を借りて御礼を申し上げます。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す。

2021年11月

島田裕次

個人情報保護法への企業の対応

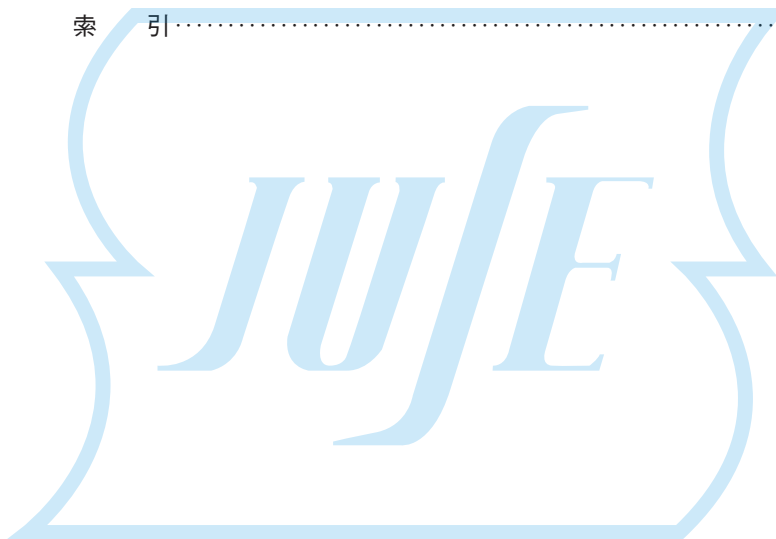
目次

	まえがき	iii
第1章	デジタル社会と個人情報保護	1
	1.1 デジタル社会の進展と個人情報	1
	1.2 個人情報とは何か	4
	1.3 個人情報に関するデータベースの概念	8
	1.4 個人情報保護の考え方	9
	1.5 個人情報保護法に関わる歴史	11
	1.6 個人情報保護法の制定と2015年改正	16
	1.7 2015年個人情報保護法改正と番号法の制定	17
	1.8 2020年改正個人情報保護法	22
	1.9 2021年改正個人情報保護法	25
第2章	2020年・2021年改正個人情報保護法	31
	2.1 改正の考え方	31
	2.2 2020年および2021年改正個人情報保護法の構成	36
	2.3 個人情報取扱事業者等の義務	37
	2.4 仮名加工情報取扱事業者等の義務	48
	2.5 匿名加工情報取扱事業者等の義務	50
	2.6 個人情報取扱事業者等の監督	52
	2.7 民間団体による個人情報保護の推進	55

2.8	個人情報保護に関するガイドライン	59
第3章	安全管理措置（個人情報保護対策）	61
3.1	安全管理措置の概要と意義	61
3.2	基本方針の策定と規律の整備	63
3.3	組織的安全管理措置	64
3.4	人的安全管理措置	67
3.5	物理的安全管理措置	69
3.6	技術的安全管理措置	71
3.7	中小規模企業の安全管理措置の考え方	75
第4章	マイナンバーの概要	77
4.1	番号法の概要	77
4.2	事業者側での対応	80
4.3	マイナンバーカード	81
4.4	マイナンバーに関わるガイドライン	82
4.5	個人情報と特定個人情報（マイナンバー）の保護策の違い	88
第5章	GDPRの概要	101
5.1	GDPRとは	101
5.2	日本企業に及ぼす影響	110
第6章	個人情報に関わるインシデント	113
6.1	インシデントとは	113
6.2	インシデントからの学び方	114
6.3	機密性に関わるインシデント	118
6.4	可用性に関わるインシデント	124
6.5	インテグリティに関わるインシデント	127

第7章	個人情報保護とリスクマネジメント	129
7.1	個人情報保護マネジメント	129
7.2	プライバシーポリシーなどの策定	137
7.3	個人情報保護リスクの分析・評価	139
7.4	個人情報に関わるリスク(個人情報保護リスク)評価	143
7.5	個人情報保護リスクの対応策	148
7.6	情報セキュリティ対策の構築	150
7.7	個人情報保護リスクの管理体制	153
7.8	個人情報の取扱いに関する教育	154
7.9	個人情報保護マネジメントの監査(個人情報保護監査)	157
7.10	個人情報保護リスクマネジメントの継続	159
第8章	実務上の管理ポイント	163
8.1	外部委託先の管理	163
8.2	クラウドサービスの利用と管理	166
8.3	システム開発の管理	168
8.4	SNS 利用の管理	170
8.5	IoT の管理	171
8.6	テレワークの管理	174
第9章	効率的な個人情報保護を目指して	177
9.1	情報セキュリティと個人情報保護	177
9.2	IT ガバナンスと個人情報保護	178
9.3	IT 統制と個人情報保護	179
9.4	ERM と個人情報保護	183
9.5	システム監査と個人情報保護監査	185
9.6	3 ラインモデルと個人情報保護	186

9.7 DXの推進と個人情報保護	188
9.8 新技術と個人情報保護	190
9.9 個人情報保護リスクの動向	191
付録1 個人情報保護チェックリスト	195
付録2 マイナンバー保護チェックリスト	199
参考文献	205
索引	209



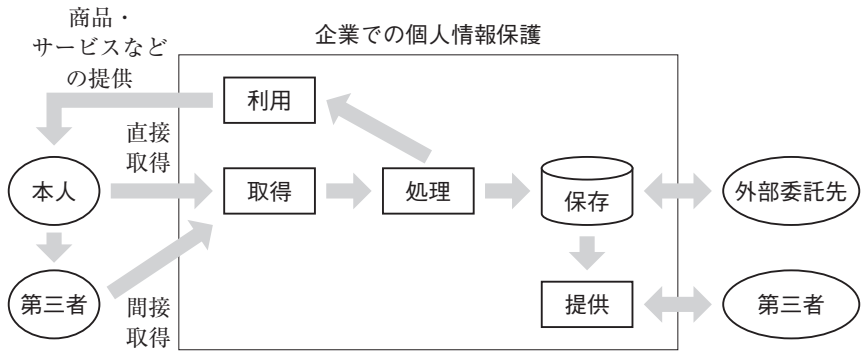


図 7.9 個人情報の取扱いの全体像

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

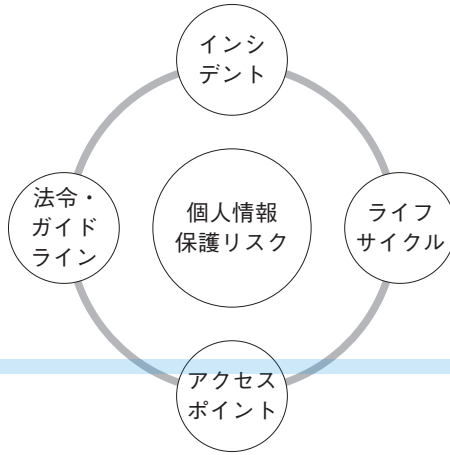


図 7.10 個人情報保護リスクの洗い出し方法

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。

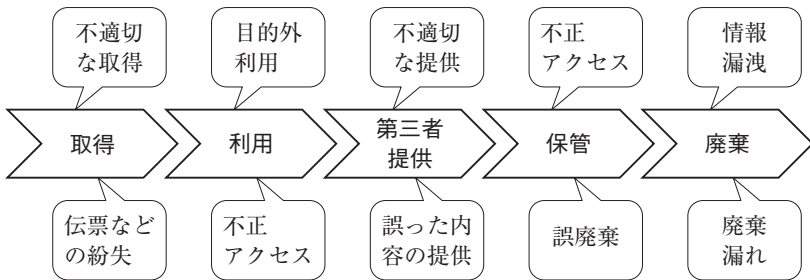


図7.11 ライフサイクルから見たリスク

(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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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)』(同文館出版)、『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 東京都渋谷区千駄ヶ谷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

© Yuji Shimada 2021

ISBN 978-4-8171-9749-8

URL <https://www.juse-p.co.jp/>

本書の全部または一部を無断でコピー、スキャン、デジタル化などの複製をすることは著作権法上の例外を除き禁じられています。本書を代行業者等の第三者に依頼してスキャンやデジタル化することは、たとえ個人や家庭内での利用でも著作権法違反です。