2019年度　東京都
個人情報保護制度説明会

個人情報保護法に関する事業者の心構えと対応

2019年9月27日

JIPDEC（（一財）日本情報経済社会推進協会）
認定個人情報保護団体事務局　坂本　誠
sakamoto-makoto@jipdec.or.jp
（JIPDEC法人番号：1 0104 0500 9403）

本講義の概要

- 概要
  - コンプライアンス（法遵守）
  - プライバシーマーク制度とISMS
- 到達目標
  - コンプライアンスに対する考え方やアプローチを理解する
  - マネジメントシステムについて理解する
- キーワード
  - コンプライアンス、マネジメントシステム
- 受講推奨対象
  - 一般職員、管理職、IT開発

アジェンダ

1．コンプライアンスについて考える

2．個人情報保護の取り組み例

「コンプライアンス」について考える

弊社は、お客様の権利利益を第一に考え、
お客様の個人情報を適切に扱います。

そのために、
個人情報保護法をはじめとした各種法令を遵守します。

「コンプライアンス」について考える

魚屋さんは、なぜ腐った魚を売らないのか？

腐った魚の販売は法で禁止されている？

魚とは？イカは？タコは？豚肉なら腐っていても良い？

腐るとは？

「法令遵守」とは？

例えば、

個人情報の保護に関する法律
第二十七条　個人情報取扱事業者は、保有個人データに関し、次に掲げる事項について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。
一　当該個人情報取扱事業者の氏名又は名称
二　全ての保有個人データの利用目的（第十八条第四項第一号から第三号までに該当する場合を除く。）
三　次項の規定による求め又は次条第一項、第二十九条第一項若しくは第三十条第一項若しくは第三項の規定による請求に応じる手続（第三十三条第二項の規定により手数料の額を定めたときは、その手数料の額を含む。）
四　前三号に掲げるもののほか、保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの
２　個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの利用目的の通知を求められたときは、本人に対し、遅滞なく、これを通知しなければならない。ただし、次の各号のいずれかに該当する場合は、この限りでない。
一　前項の規定により当該本人が識別される保有個人データの利用目的が明らかな場合
二　第十八条第四項第一号から第三号までに該当する場合
３　個人情報取扱事業者は、前項の規定に基づき求められた保有個人データの利用目的を通知しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

一見すると手続きを詳細に規定しているように見える。

実際は、あらゆる事業者のあらゆる取り扱いを対象とできるように、
最低限のルールを定めたに過ぎない。

「法律に書いてあること」を守るだけで十分か？

保護の対象となる個人情報とは？

「〇〇は個人情報か？」という議論

個人情報保護法で定める「個人情報」を限定的に捉え、対象情報のみを保護するという手法はリスクが高いのではないか？

参考（JIS X9250 プライバシー保護の枠組みと原則）：

個人識別可能情報，PII（personally identifiable information, PII）

a）その情報に関連するPII主体を識別するために利用され得る情報，又は

b）PII主体に直接若しくは間接に紐付けられる又はその可能性がある情報。

事例

大手就職情報サイトの事例

2019年8月 就職情報サイト「リクナビ」が、就活活動中の学生が内定を辞退する可能性を予測して企業に提供していた問題が報道される。その後、同サービス（「リクナビDMPフォロー」）の廃止が発表される。

本件については、同意取得に不備があったといわれているが、それだけの問題か？

個人情報保護法を遵守するとは？

「コンプライアンス」の目的は、権利主体の権利利益の保護。

「コンプライアンス」の「遵守」の対象には、自社で定めた方針等を含む。

自社で取り扱っている個人情報を保護するために、「具体的に何をするか？」を考える必要がある。

「私の会社」の「私の顧客」の個人情報を保護するために、、、

※個人情報保護法は、個人情報取扱事業者の自主的な取組みを推進することを目的として認定個人情報保護団体制度を規定している（第47条他）

リスクベースアプローチ

■ リスクベースアプローチ

リスクアセスメントに基づいて意思決定をする考え方。

目的の達成を危うくする要因を洗い出し、それらの影響を分析し、必要な対策を実施する。

・何をすれば（しなければ）個人情報を保護できるか？

・何をすれば（しなければ）顧客の信頼を得られるか？

個人情報保護の取り組み例

1. 方針の明確化
2. 体制の整備
3. 個人情報、取り扱い状況の洗い出し
4. リスク分析
5. 内部規定、及び規定の定着化
6. 点検・見直し

■ マネジメントシステムの構築

1．方針の明確化

■ 方針の作成

どのような情報をどのように扱うか方針を定める

■ 内部方針と外部方針

定めた方針で公開できるもの、必要があるものは公開する

（外部向け方針※）

※一部の外部向け方針は公開が義務付けられている

2．体制の構築

■ 体制の構築

- 責任者：組織としての責任（Accountability） を有する者
- 担当者：実効性のある実施体制

「絵に描いた餅」にならないようにするためには？

3．個人情報、取り扱い状況の洗い出し

■ 個人情報、取り扱い状況の洗い出し

- 業務フローを明らかにする

  自社の事業における個人情報を取り扱う業務について、個人情報の取得から廃棄までのライフサイクルを明らかにする

- 取り扱う個人情報を漏れなく洗い出す

  個人情報の種類、利用目的、取り扱いの状況（取得、利用、第三者への提供、保管、消去等）、委託状況等を文書化する（いわゆる、個人情報管理台帳）

- 個人情報を処理・保管する、システム・媒体等を洗い出す

  使用する業務システム、ネットワーク、データベース、紙資料等

- 上記に関連した安全管理策を確認する

  人的、組織的、技術的な安全管理策

4．リスク分析

■ リスク分析

- 取扱いに応じたリスクの分析

  3 で洗い出した内容についてリスクを分析する

  ・リスクの特定

  採用済みの安全対策を踏まえ、具体的な脅威・脆弱性を洗い出す

  ・リスクの分析

  発生の可能性と影響度を分析する

  ・リスクの評価

  対応の優先順位を決定する※

  ※組織に関するリスクは受容可能であるが、個人に関するリスクは事業者の判断で自由に受容できるものではないことに注意を要する。

- 法令等への適合状況の確認

5．内部規定、及び規定の定着化

■ 内部規定

４の実施結果について、必要に応じて規程を作成、改定する。

■ 内部規定の定着化

作成した規定を組織に定着させる

・教育

・罰則など

6．点検・見直し

■ 点検

５の実施内容が、組織内で正しく運用されていることを監査などによって確認する。

・内部監査

・外部監査

■ 見直し

点検や日常の運用において生じた問題等について、１から６の見直しを

適宜及び定期的に実施する。

※組織内における個人情報の取扱い、法令や、個人の権利意識等は常に変化する。

１から６の活動は反復・継続して実施することが重要。

個人情報保護マネジメントシステムの構築

■ マネジメントシステムの構築

１から６の活動を組織に根付かせるために、個人情報保護に関するマネジメントシステム※を構築することが望ましい。

※個人情報保護の取り組みを実施するための体制を整え、取り組みの実行・確認、定期的な見直し・改善を図るための一連の仕組みを構築すること。参考情報としてJIS Q 15001:2017等がある。

参考：プライバシーマーク制度

■ プライバシーマーク制度の概要

事業者の個人情報を取り扱う仕組みとその運用が適切であるかを評価し、その証として、事業活動においてプライバシーマークの使用を認める制度。

審査基準は、JIS Q 15001:2017「個人情報保護マネジメントシステム－ 要求事項」をベースにしており、個人情報保護法等、法令への遵守も包含。
法令等への適合性はもちろんのこと、自主的に、より高いレベルの個人情報の管理体制を確立し運用していることを、取引先や消費者に分かりやすく示すことができる制度として活用可能。

参考：ISMSおよびISMS認証

■ ISMSの概要

ISMSは、Information Security Management Systemの略で、情報の「機密性」、「完全性」、「可用性」を保護するためのマネジメントシステム。

ISMSの要求事項を定めた規格として、JIS Q 27001（ISO/IEC 27001）がある。
また、組織が構築したISMSが、JIS Q 27001（ISO/IEC 27001）に基づいて適切に運用されているかを認証する、「ISMS認証」がある。

一般財団法人日本情報経済社会推進協会
電子情報利活用研究部　坂本　誠
sakamoto-makoto@jipdec.or.jp