Quality Agent Co.,Ltd.

プライバシーマーク
はじめてハンドブック

Ver. 1.00.00

株式会社クオリティ・エージェント編

目　次

1. はじめに

本書は、プライバシーマーク制度を理解してもらうと共に、プライバシーマーク制度の審査基準である JIS Q 15001:2006（「個人情報保護マネジメントシステム―要求事項」）の規格を分かりやすく理解していただけるよう、出来る限り、平易な言葉と具体的な表現での解説を心がけています。

このため、はじめてプライバシーマークに触れる方を中心に、プライバシーマークに対して疑問をお持ちの方、あるいは、プライバシーマークにすでに取り組んでいる方であっても「今さら聞けないなぁ」とお悩みの方など多くの方に、正しくプライバシーマークを理解していただき、また、それを生かすためのヒントになればと考えて文章を構成しています。

また、プライバシーマークは、個人情報を守るための仕組みを、その企業に合う形で導入していくものであり、決して難しいものではありません。しかし、セキュリティ強化のために、多くのルール作りや、設備を充実させなければいけないと誤解し、そのために多くの費用がかかってしまうのではないかと、どうしても、難しく捉えてしまう方も少なくありません。このような誤解についても、本書の中での解説を通して、解けていくことを願っています。

1.1 プライバシーマークに対する印象は？

皆さんは、「プライバシーマーク」に、どのような印象を持っているでしょうか？

もちろん、本書を読む方の中で、初めてプライバシーマークに触れる方であれば、「そもそもプライバシーマークって何？」という方もいると思いますが、プライバシーマークという言葉を知っている方の中には、次のようなことを思っている方もいるのではないでしょうか？

「個人情報を守ってくれる会社でしょ？」

まずは、そこまで分かっていれば十分です。（詳しくは、この後に、順次説明していきますね）

その他にも、プライバシーマークについては、次のような印象を持っている方もいることでしょう。

「セキュリティを上げるために、たくさんのお金がかかりそう」

「文書とか記録とか、いっぱい作らなきゃいけないから大変そう」

「個人情報の管理が大変になりそう」

「専門的な部分が多くて難しそう」

確かに、個人情報という非常に重要な情報を取り扱うのですから、その管理を行うことは決して簡単なものではありませんし、コストは少なからず考えなければいけません。しかし、皆さんが考えているよりも、難しく大変なものではありませんし、少ないコストでプライバシーマークは取得することも出来ます。

「それが知りたいんじゃないか？」

という声が聞こえそうですが、それは、本書の中で順次説明させていただきますね。
少なからず誤解からも、「お金がかかる」、「難しい」、「大変だ」と思われている部分については、本書を読み終えたときに、これらの誤解が解けると思っています。

また、単に「取引先から取得するように言われているから取得したいだけだよ」という方もいることでしょう。しかし、プライバシーマークの審査基準である JIS Q 15001 は、2006 年度版から「個人情報保護マネジメントシステム」となりました。マネジメントシステムの詳細は、次章で説明しますが、会社の仕組みを整備していくことにより、強力な経営ツールとして活かすことも十分に出来るものとなっているのです。せっかくプライバシーマークを取得するのですから、会社の中に、有効に活用出来る仕組み作りが出来るようにしてみませんか？

2. 基礎知識を学ぼう

この章では、プライバシーマークについての基礎的なことを学びます。
「いや、基礎的なことなら分かっているよ」という方は、この章は、読み飛ばして構いません。ただ、プライバシーマークの基礎的なことを、キチンと理解することで、何かのヒントになるかも知れませんので、ご興味のある方は、この章も、是非、じっくりと読んで貰えればと思います。

2.1 プライバシーマークって何？

プライバシーマークとは、正式には、プライバシーマーク認定制度と言い、以下のような制度のことを言います。

> 個人情報の取り扱いが適切であることを第三者機関が認定して、
> その証として「プライバシーマーク」の使用を認める制度

例えば、プライバシーマークを持っていない会社が、「うちの会社は、個人情報をキチンと守っています！」と言ったところで、本当に守っているのかは分かりませんし、その会社の人たち以外には、その会社内の状況を見ることはなかなか出来ません。また、「キチンと」というものが、どの程度のものなのかも分かりませんよね？

このため、第三者機関が、一定のルールに則り、その会社を評価した上で、「この会社は、確かに個人情報を守るための仕組みがある」と認めた会社に対し、そのお墨付きとして「プライバシーマーク」の使用を許しているのです。

「第三者機関ってどこのこと？」
「一定のルールって何？」

という言葉が聞こえそうなので、もう少し詳しく説明しますね。

プライバシーマーク制度は、日本情報処理開発協会（以下 **JIPDEC**）が管理している個人情報の取り扱いに関する認定制度のことです。個人情報について、JIPDECの定める基準を満たして適正に管理していると認定されれば、使用許諾を得ることが出来るのです。審査基準は、基本的に、**JIS Q 15001（個人情報保護マネジメントシステム―要求事項）に準拠**しており、**有効期間は 2 年間**となっています。

JIS Q 15001 では、個人情報を保護するにあたり、組織が具体的にどのようなことをしなければいけないかを、個人情報保護法よりも詳細に要求していますので、個人情報保護法において要求される事項も JIS Q 15001 の要求事項の中に含まれています。このため、JIS Q 15001 に合わせた対策を行なっていけば、結果的に個人情報保護法よりも一段上の個人情報保護対策を行なえることになります。

2.2 JIS について

プライバシーマークの審査基準として、JIS Q 15001（個人情報保護マネジメントシステム－要求事項）があります。要求事項そのものは、この後の章で、詳しく説明していきますが、ここでは、JIS について、簡単に説明したいと思います。

「ジス」と読みます。JIS は、日本工業規格（JIS:Japanese Industrial Standards）のことで、日本における工業標準化の促進を目的とした工業標準化法という法律があるのですが、この法律に基づいて制定される国家規格のことを言います。

JIS の後に続くローマ字 1 文字は、部門記号と呼ばれ、JIS の部門を表しています。「A：土木及び建築」、「B：一般機械」、「C：電子機器及び電気機械」、「D:自動車」など 19 の部門に分かれおり、「Q」は、管理システムを表しています。（「表 1　JIS 部門記号一覧」参照）

部門記号に続く数字は、各部門で一意な番号となっています。

なお、JIS 規格は、日本工業標準調査会（JISC）（JIS の策定などを行っている機関です）のサイト（http://www.jisc.go.jp）から、JIS 規格を参照することが出来ます。このサイトでは、各規格の番号をもとに、データベース検索すると、規格を閲覧することが可能です。（JIS Q 15001 ならは、「Q 15001」と入力します）著作権の問題があるため、印刷やコピーなどは行うことが出来ませんが、閲覧するだけで十分という方は、ここで閲覧するようにしましょう。

なお、プライバシーマーク取得にあたり、コンサルティングの方に依頼したときなど、規格をまったく見ない方もいますが、さまざまな誤解は、規格を見ないことにより起こることも多々ありますので、可能な限り、規格を読み解

部門記号	部門
A	土木及び建築
B	一般機械
C	電子機器及び電気機械
D	自動車
E	鉄道
F	船舶
G	鉄鋼
H	非鉄金属
K	化学
L	繊維
M	鉱山
P	パルプ及び紙
Q	管理システム
R	窯業
S	日用品
T	医療安全用具
W	航空
X	情報処理
Z-1	包装
Z-2	放射線
Z-3	溶接
Z-4	リサイクルその他

表 1　JIS 部門記号一覧

き、理解するようにしましょう。（もちろん、本書にて、規格の内容そのものは詳しく説明していきます）

2.3　個人情報保護マネジメントシステム

個人情報保護マネジメントシステムは、その略称として、**PMS（Personal information protection Management System）**とも呼ばれ、JIS Q 15001では、以下のように定義されています。

> 事業者が、自らの事業の用に供する個人情報について、
> その有用性に配慮しつつ、個人の権利利益を保護するための
> 方針、体制、計画、実施、点検及び見直しを含むマネジメントシステム

マネジメントシステムの用語の説明で、マネジメントシステムという言葉が出てくるのはいかがなものかとは思いますが、ここでは、その議論は避けておきましょう。

さて、上記の定義をそのまま読み解くと、事業者（「2.9.3 事業者」参照）が、自分たちが使用する個人情報を、その有用性（役に立つこと）に配慮しながら、個人の権利や利益を保護するための様々な仕組み（方針、体制、計画、実施、点検及び見直し）を含めたマネジメントシステムのことであると言っています。

マネジメントシステムは、JIS Q 9000 で、以下のように定義されています。

> 方針及び目標を定め、その目標を達成するためのシステム

マネジメントシステムというのは、方針と目標を定め、その目標を達成するために、どのように振る舞うべきなのかを求められているようですね。いわゆる**目標達成のシステム**のことを指しているようです。

それでは、最後にシステムも調べてみましょう。同じく JIS Q 9000 では、以下のように定義されています。

> 相互に関連する又は相互に作用する要素の集まり

システムについては、ちょっと分かり難いですよね。ここは、単純に「仕組み」のことだと思ってもらって構いません。