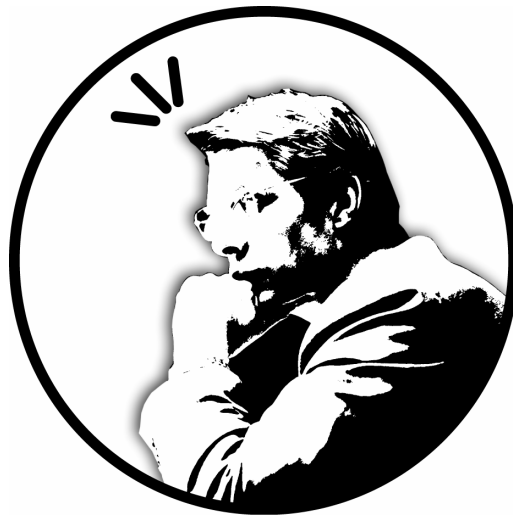


JIS Q

Guidebook for understanding
personal information Protection management systems-Requirements

Privacy mark

15001 要求事項理解のための
2006 **ガイドブック**



まえがき

プライバシーマーク制度の審査においては、JIS Q 15001 への適合はもとより、個人情報保護法、各省庁が発行するガイドラインへの適合が考慮される。

本ガイドブックでは、プライバシーマーク認証制度において適用される基準（JISQ15001:2006）の要求事項と、以下の「参考文献」より、関連する各条項および事例などを並列して掲載することにより、要求事項の意図する内容や審査のポイントなどの解説を試みている。

なお、本ガイドでは、JISQ15001:2006 の要求事項に関して一定の範囲において、その意味する内容を説明しておりますが、必ずしも全てを網羅している訳ではなく、また、プライバシーマーク認証取得を保証するものではありません。

本ガイドは、プライバシーマーク認証取得（JISQ15001:2006）を検討している企業若しくは担当者における、認証規格の理解と共に PMS（Personal information Protection management systems）構築の手助けになることを目的とし、以下の参考文献をもとに作成されたものです。

本ガイドが、これから、プライバシーマーク認証取得を目指される企業及び担当者の方において、JISQ15001:2006 を理解する上での一助となり、PMS を構築する上でのご参考になることを期待します。

■ 参考文献

- ・ JISQ15001:2006 個人情報保護マネジメントシステム—要求事項
- ・ 個人情報保護法（個人情報の保護に関する法律）
- ・ 個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン
- ・ JISQ15001:2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン

目次

1	適用範囲	1
2	用語及び定義	2
3	要求事項	4
3.1	一般要求事項	4
3.2	個人情報保護方針	5
3.3	計画	6
3.3.1	個人情報の特定	6
3.3.2	法令、国が定める指針その他の規範	6
3.3.3	リスクなどの認識、分析及び対策	7
3.3.4	資源、役割、責任及び権限	8
3.3.5	内部規程	9
3.3.6	計画書	10
3.3.7	緊急事態への準備	10
3.4	実施及び運用	12
3.4.1	運用手順	12
3.4.2	取得、利用及び提供に関する原則	12
3.4.2.1	利用目的の特定	12
3.4.2.2	適正な取得	14
3.4.2.3	特定の機微な個人情報の取得、利用及び提供の制限	15
3.4.2.4	本人から直接書面によって取得する場合の措置	16
3.4.2.5	個人情報を3.4.2.4以外の方法によって取得した場合の措置	20
3.4.2.6	利用に関する措置	21
3.4.2.7	本人にアクセスする場合の措置	25
3.4.2.8	提供に関する措置	27
3.4.3	適正管理	34
3.4.3.1	正確性の確保	34
3.4.3.2	安全管理措置	34
3.4.3.3	従業者の監督	50
3.4.3.4	委託先の監督	52
3.4.4	個人情報に関する本人の権利	55
3.4.4.1	個人情報に関する権利	55
3.4.4.3	開示対象個人情報に関する事項の周知など	60
3.4.4.4	開示対象個人情報の利用目的の通知	62
3.4.4.5	開示対象個人情報の開示	64
3.4.4.6	開示対象個人情報の訂正、追加又は削除	66
3.4.4.7	開示対象個人情報の利用又は提供の拒否権	68

3.4.5	教育	70
3.5	個人情報保護マネジメントシステム文書	71
3.5.1	文書の範囲	71
3.5.2	文書管理	72
3.5.3	記録の管理	73
3.6	苦情及び相談への対応	73
3.7	点検	74
3.7.1	運用の確認	74
3.7.2	監査	75
3.8	是正処置及び予防処置	76
3.9	事業者の代表者による見直し	76

1 適用範囲

この規格は、個人情報事業の用に供している、あらゆる種類、規模の事業者に適用できる個人情報保護マネジメントシステムに関する要求事項について規定する。

事業者は、次の事項を行う場合に、この規格を用いることができる。

- a) 個人情報保護マネジメントシステムを確立し、実施し、維持し、かつ、改善する。
- b) この規格と個人情報保護マネジメントシステムとの適合性について自ら確認し、適合していることを自ら表明する。
- c) 組織外部又は本人に、この規格に対する個人情報保護マネジメントシステムの適合性について確認を求める。
- d) 外部機関による個人情報保護マネジメントシステムの認証／登録を求める。

個人情報保護法

第2条（定義）

3 この法律において「個人情報取扱事業者」とは、個人情報データベース等を事業の用に供している者をいう。ただし、次に掲げる者を除く。

- 一 国の機関
- 二 地方公共団体
- 三 独立行政法人等（独立行政法人等の保有する個人情報の保護に関する法律（平成十五年法律第五十九号）第二条第一項に規定する独立行政法人等をいう。以下同じ。）
- 四 地方独立行政法人（地方独立行政法人法（平成十五年法律第百十八号）第二条第一項に規定する地方独立行政法人をいう。以下同じ。）
- 五 その取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定める者

個人情報の保護に関する法律施行令

第2条（個人情報取扱事業者から除外される者）

法第2条第3項第5号の政令で定める者は、その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数（当該個人情報データベース等の全部又は一部が他人の作成に係る個人情報データベース等であって、次の各号のいずれかに該当するものを編集し、又は加工することなくその事業の用に供するときは、当該個人情報データベース等の全部又は一部を構成する個人情報によって識別される特定の個人の数を除く。）の合計が過去6月以内のいずれの日においても5千を超えない者とする。

審査時のチェックポイント

1. 全従業員を人的適用範囲に含めていること。
全従業者（社長、取締役、執行役員、理事、監査役、監事、正社員、パートタイマー、契約社員、派遣社員）及び全サイト（本社、支店、営業所、工場）が適用範囲とされてなければなりません。
2. 業務の用に供している個人情報を適用範囲対象とするよう定めていること。
事業の用に供している個人情報(電子データ、紙データ、音声、写真など個人が特定できるもの)を適用対象とされてなければなりません。

2 用語及び定義

この規格で用いる主な用語及び定義は、次による。

2.1 個人情報

個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述などによって特定の個人を識別できるもの（他の情報と容易に照合することができ、それによって特定の個人を識別することができることとなるものを含む。）。

2.2 本人

個人情報によって識別される特定の個人。

2.3 事業者

事業を営む法人その他団体又は個人。

2.4 個人情報保護管理者

代表者によって事業者の内部の者から指名された者であって、個人情報保護マネジメントシステムの実施及び運用に関する責任及び権限をもつ者。

2.5 個人情報保護監査責任者

代表者によって事業者の内部の者から指名された者であって、公平、かつ、客観的な立場にあり、監査の実施及び報告を行う責任及び権限をもつ者。

2.6 本人の同意

本人が、個人情報の取扱いに関する情報を与えられた上で、自己に関する個人情報の取扱いについて承諾する意思表示。本人が子ども又は事理を弁識する能力を欠く者の場合は、法定代理人等の同意も得なければならない。

2.7 個人情報保護マネジメントシステム

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。

2.8 不適合

本規格の要求を満たしていないこと。

個人情報保護法

第2条（定義）

1 この法律において「個人情報」とは、生存する個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。

2 この法律において「個人情報データベース等」とは、個人情報を含む情報の集合物であつて、次に掲げるものをいう。

- 一 特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの
- 二 前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの

- 3 この法律において「個人情報取扱事業者」とは、個人情報データベース等を事業の用に供している者をいう。ただし、次に掲げる者を除く。
- 一 国の機関
 - 二 地方公共団体
 - 三 独立行政法人等（独立行政法人等の保有する個人情報の保護に関する法律（平成十五年法律第五十九号）第二条第一項に規定する独立行政法人等をいう。以下同じ。）
 - 四 地方独立行政法人（地方独立行政法人法（平成十五年法律第百十八号）第二条第一項に規定する地方独立行政法人をいう。以下同じ。）
 - 五 その取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定める者
- 4 この法律において「個人データ」とは、個人情報データベース等を構成する個人情報をいう。
- 5 この法律において「保有個人データ」とは、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの又は一年以内の政令で定める期間以内に消去することとなるもの以外のものをいう。
- 6 この法律において個人情報について「本人」とは、個人情報によって識別される特定の個人をいう。

個人情報の保護に関する法律施行令

第2条（個人情報取扱事業者から除外される者）

法第2条第3項第5号の政令で定める者は、その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数（当該個人情報データベース等の全部又は一部が他人の作成に係る個人情報データベース等であって、次の各号のいずれかに該当するものを編集し、又は加工することなくその事業の用に供するときは、当該個人情報データベース等の全部又は一部を構成する個人情報によって識別される特定の個人の数を除く。）の合計が過去6月以内のいずれの日においても5千を超えない者とする。

第3条（保有個人データから除外されるもの）

法第二条第五項の政令で定めるものは、次に掲げるものとする。

- 一 当該個人データの存否が明らかになることにより、本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの
- 二 当該個人データの存否が明らかになることにより、違法又は不当な行為を助長し、又は誘発するおそれがあるもの
- 三 当該個人データの存否が明らかになることにより、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利を被るおそれがあるもの
- 四 当該個人データの存否が明らかになることにより、犯罪の予防、鎮圧又は捜査その他の公共安全と秩序の維持に支障が及ぶおそれがあるもの

第4条（保有個人データから除外されるものの消去までの期間）

法第2条第5項の政令で定める期間は、6月とする。

審査時のチェックポイント

規程 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8 のように定義していること。

- ① 「個人情報」には、死者の情報も含まれますが、歴史上の人物までを対象とするものではありません。
- ② 「事業者」には取り扱う個人情報の量及び利用方法に関わらず、個人情報を事業の用の供している全ての事業者が含まれます。
- ③ 「個人情報保護管理者」は、個人情報の取扱いに関する安全措置の管理面だけではな

く、組織全体の個人情報保護マネジメントシステムのマネジメントを含む全ての管理をする必要があります。

- ④ 「本人の同意」は、本人の署名や同意欄へのチェックや HP 上での同意ボタンの押下などの明示的な方法によって本人の意思で行われるものであり、メール、書面などでの通知後一定期間内に返信(返事)が無い場合などは同意があったとは見なすことはできません。また、法廷代理人等の同意を必要とする子供（12 歳から 15 歳までの年齢以下）や成人であっても同意に対しての理解・判断力に懸念のある者については法廷代理人等による同意が必要となります。

3 要求事項

3.1 一般要求事項

事業者は、個人情報保護マネジメントシステムを確立し、実施し、維持し、かつ、改善しなければならない。その要求事項は、簡条 3 で規定する。

個人情報保護法

無し。

審査時のチェックポイント

個人情報保護マネジメントシステムは、PDCA モデル（Plan：計画-Do：実施-Check：確認-Act：見直し）が採用されており、この PDCA サイクルをスパイラル的に継続することにより、事業者の個人情報の保護レベルを上げて行くことが期待されています。

