# JISQ15001:2017　規格本文に関するチェックシート　　サンプル

「0.1　概要」は、PMS に対する心構えを記載している。そこの理解を曖昧にしたままでの PMS は、形式化した MS になりかねず、組織への貢献も薄れて行く。まずはこの部分の確認をすること。

## 0　序文　0.1 概要

序文は、この規格を組織に適用する場合の注意点が記載されています。それを確認することをお勧めしています。

・「規格」に規格の記載をそのまま載せます。
・「留意」は規格の中で誤解されやすい箇所や特に注目してほしい内容を取り上げます
・「理解」は組織としてどう理解解釈して対応したのかを記載してください。
・この項番は、正しい正しくないではなく、どう考えるのかの確認にとどまります。

| | |
|---|---|
| 規格 | この規格は，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，継続的に改善するための要求事項を提供するために作成された。**個人情報保護マネジメントシステムの採用は，組織の戦略的決定である。**組織の個人情報保護マネジメントシステムの確立及び実施は，その組織のニーズ及び目的，個人情報保護の要求事項，組織が用いているプロセス，並びに組織の規模及び構造によって影響を受ける。影響をもたらすこれらの要因全ては，**時間とともに変化すること**が見込まれる。 |
| 留意 | まずは、PMS は組織の戦略的な枠組みに含まれる必要がある。すなわち、企業活動の目的遂行の中で PMS はどのような枠割りを持たせるのかを明確にする必要がある。それを支えるのは、経営ビジョンであり、その経営ビジョンを達成するための組織運営である。単に PMS を構築することが目的にならない。<br>また、経営環境が変化する中で、静的なマネジメントシステムでは対応できない。ダイナミックなマネジメントに配慮することが望まれる。 |
| 理解 | |

| | |
|---|---|
| 規格 | 個人情報保護マネジメントシステムを，組織のプロセス及びマネジメント構造全体の一部とし，かつ，その中に組み込むこと，並びにプロセス，情報システム及び管理策を設計する上で個人情報保護を考慮することは，重要である。個人情報保護マネジメントシステムの導入は，その組織のニーズに合わせた規模で行うことが期待される。<br>・・・<br>この規格で示す要求事項の順序は，重要性を反映するものでもなく，実施する順序を示すものでもない。 |
| 留意 | 誤解されるようだが、この規格に合わせてマネジメントシステムを作れといっているのではない。組織の機能は様々であり、規模も異なる。その組織に適したマネジメントがある。<br>便宜上、個人情報保護マニュアルは規格項番にあわせた方が管理しやすいが、実業務プロセスを明確にして対応を考える必要がある。<br>また、用語も自社の固有のものがあればそれを使うことを優先し、規格との相違をまとめて記載しておくことで対応することが望ましい。 |
| 理解 | |

## 規格項番との対応チェック

PMS 構築に当たっては、その戦略的目的に合わせて、組織と機能そして作業手順を明確にしなければならない。基本としての規格の本文について下記の視点で整理することを勧める。

規格・・・規格本文を掲載する
活動・・・組織として対応する活動は何かを示す。誰がどこで何をするのかといった 5W1H で示されることが望ましい
文書・・・その活動を規定する文書の有無を示す。ある場合にはその文書名を示す
記録・・・その活動が行われている証左を何で確認できるかを示す。日常の活動（例えば朝礼）などでもよい
合否・・・このままで十分かどうかの判定
改善・・・十分ではないと判断した場合の施策を示す

なお、未検討や該当するものがわからない場合には、素直に「不明」「未検討」と記載すること。
やってもいないことを記載すると形骸化した PMS を作りかねない。
なお、ここでは規格解釈は載せません。素直に感じるところから始めてください。

## 4　組織の状況

### 4.1 組織及びその状況の理解

| | |
|---|---|
| 規格 | 組織は，組織の目的に関連し，かつ，その個人情報保護マネジメントシステムの意図した成果を達成する組織の能力に影響を与える，外部及び内部の課題を決定しなければならない。 |
| 活動 | |
| 文書 | |
| 記録 | |
| 合否 | □ 適合・合格　□ 不適合・不合格　□ 適合ではあるが改善の余地がある |
| 改善 | |

### 4.2 利害関係者のニーズ及び期待の理解

| | |
|---|---|
| 規格 | 組織は，次の事項を決定しなければならない。<br>a）個人情報保護マネジメントシステムに関連する利害関係者<br>b）その利害関係者の，個人情報保護に関連する要求事項<br>注記 利害関係者の要求事項には，法的及び規制の要求事項並びに契約上の義務を含めてもよい。 |
| 活動 | |
| 文書 | |
| 記録 | |
| 合否 | □ 適合・合格　□ 不適合・不合格　□ 適合ではあるが改善の余地がある |
| 改善 | |

### 4.3 個人情報保護マネジメントシステムの適用範囲の決定

| | |
|---|---|
| 規格 | 組織は，個人情報保護マネジメントシステムの適用範囲を定めるために，その境界及び適用可能性を決定しなければならない。<br>この適用範囲を決定するとき，組織は，次の事項を考慮しなければならない。<br>a）4.1 に規定する外部及び内部の課題<br>b）4.2 に規定する要求事項<br>c）組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係<br>個人情報保護マネジメントシステムの適用範囲は，文書化した情報として利用可能な状態にしておかなければならない。 |
| 活動 | |
| 文書 | |
| 記録 | |

| | |
|---|---|
| 合否 | □ 適合・合格　□ 不適合・不合格　□ 適合ではあるが改善の余地がある |
| 改善 | |

4.4 個人情報保護マネジメントシステム

| | |
|---|---|
| 規格 | 組織は，この規格の要求事項に従って，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，継続的に改善しなければならない。 |
| 活動 | |
| 文書 | |
| 記録 | |
| 合否 | □ 適合・合格　□ 不適合・不合格　□ 適合ではあるが改善の余地がある |
| 改善 | |

中略

## 10 改善

### 10.1 不適合及び是正処置

| | |
|---|---|
| 規格 | 不適合が発生した場合，組織は，次の事項を行わなければならない。<br>a）その不適合に対処し，該当する場合には，必ず，次の事項を行う。<br>1）その不適合を管理し，修正するための処置をとる。<br>2）その不適合によって起こった結果に対処する。<br><br>b）その不適合が再発しないように又は他のところで発生しないようにするため，次の事項によって，その不適合の原因を除去するための処置をとる必要性を評価する。<br>1）その不適合をレビューする。<br>2）その不適合の原因を明確にする。<br>3）類似の不適合の有無，又はそれが発生する可能性を明確にする。<br><br>c）必要な処置を実施する。<br>d）とった全ての是正処置の有効性をレビューする。<br>e）必要な場合には，個人情報保護マネジメントシステムの変更を行う。<br>是正処置は，検出された不適合のもつ影響に応じたものでなければならない。<br>組織は，次に示す事項の証拠として，文書化した情報を保持しなければならない。<br>f）不適合の性質及びとった処置<br>g）是正処置の結果 |
| 活動 | |
| 文書 | |
| 記録 | |
| 合否 | □ 適合・合格　□ 不適合・不合格　□ 適合ではあるが改善の余地がある |
| 改善 | |

### 10.2 継続的改善

| | |
|---|---|
| 規格 | 組織は，個人情報保護マネジメントシステムの適切性，妥当性及び有効性を継続的に改善しなければならない。 |
| 活動 | |
| 文書 | |
| 記録 | |
| 合否 | □ 適合・合格　□ 不適合・不合格　□ 適合ではあるが改善の余地がある |
| 改善 | |

以上

2019 年 12 月 10 日　作成

（有）中野ソフトウエアサービス　中野康範