JISQ15001　解説補助

「5　リーダーシップ」で気になったこと

（有）中野ソフトウエアサービス

2020/03/10

5　リーダーシップ

- 「4　組織の状況」で、何をターゲットして個人情報保護マネジメントシステムを作り上げるのかの方向性が決まった。
- 実際の個人情報保護マネジメントを作って行くためには、組織全体にその意図を理解させ、適切な方向に導かなければならない。それはトップマネジメントだけができることである。

5.1 リーダーシップ及びコミットメント

- **トップマネジメントは，次に示す事項によって，個人情報保護マネジメントシステムに関するリーダーシップ及びコミットメントを実証しなければならない。**
  - リーダーシップとコミットメントという言葉が出てきますが、用語としては定義されていません。リーダーシップについて、ドラッガーは「リーダーに関する唯一の定義は、つき従う者がいるということである」としており、その言動に信頼と納得をし、部下がついて行くことを確実にできるかに係わります。コミットメントとは、「結果に対する誓約」と言ったところでしょうか？
  - ただし、規格では「リーダーシップ」「コミットメント」とは何かを気にする必要はなく、ａ）からｈ）までを実施することで良いと考えれば善いでしょう。
- **a) 内部向け個人情報保護方針及び個人情報保護目的を確立し，それらが組織の戦略的な方向性と両立することを確実にする。**
  - 「内部向け個人情報保護方針」を明示（文書化）すること。
  - そこには組織の個人情報保護の目的を含めること。戦略的な方向性を示すことになります。
- **b) 組織のプロセスへの個人情報保護マネジメントシステム要求事項の統合を確実にする。**
  - 組織活動の中で個人情報がどう取り扱われているのかを明確にして行く過程で施策を展開すれば自動的に上記を満たすことになります。

（続き）

- **c) 個人情報保護マネジメントシステムに必要な資源が利用可能であることを確実にする。**
  - これは、箇条「7　支援」を満たすことで達成されます。
- **d) 有効な個人情報保護マネジメント及び個人情報保護マネジメントシステム要求事項への適合の重要性を利害関係者に伝達する。**
  - これは、「5.2　方針」や「5.3 組織の役割，責任及び権限」に対応します。
- **e) 個人情報保護マネジメントシステムがその意図した成果を達成することを確実にする。**
  - マネジメントシステム全体の話ではあるが、特に「8　運用」を確実にする過程で実施できる。
- **f) 個人情報保護マネジメントシステムの有効性に寄与するよう人々を指揮し，支援する。**
  - トップマネジメントの役割そのものになる。下記参照。
  - 3.5 トップマネジメント
  - 最高位で組織（3.1）を指揮し，管理する個人又は人々の集まり。
  - 注記 トップマネジメントは，組織内で，権限を委譲し，資源を提供する力をもっている。

（続き）

- **g) 継続的改善を促進する。**
  - 箇条「9.3　マネジメントレビュー」を通して「10　改善」についても責任を持つと云うことになる。
- **h) その他の関連する管理層がその責任の領域においてリーダーシップを実証するよう、管理層の役割を支援する。**
  - 「5.3 組織の役割，責任及び権限」に該当する。

- ここで記載されていることの個々のa)からh)について実施していることを証明する必要はない。しかし、個人情報保護マネジメントシステム自体に対し、委任することは良いとしても「丸投げ」は許されない。最終責任はトップマネジメントが負うことになる。「事務局」に「やっておけ」と云うのは論外になる。

5.2.1 内部向け個人情報保護方針

- **トップマネジメントは，次の事項を満たす内部向け個人情報保護方針を確立しなければならない。**
  - **a) 組織の目的に対して適切である。**
  - **b) 個人情報保護目的（6.2 参照）を含むか，又は個人情報保護目的の設定のための枠組みを示す。**
  - **c) 個人情報保護に関連する適用される要求事項を満たすことへのコミットメントを含む。**
  - **d) 個人情報保護マネジメントシステムの継続的改善へのコミットメントを含む。**
- 個人情報保護方針の要素が記述されている。組織の目的、個人情報保護の目的、要求事項への誓約、継続的改善への誓約になる。
- ただし、上記をそのまま「個人情報保護方針」にすることは望ましくない。例えば、最初のa)に対して、「当社は組織の目的に適切であることを確実にする」と云うことは何も言っていないに等しい。
- 「当社は・・・と言う事業を営んでおり、その事業を進めるに当たっては個人情報の取得を・・・と言う場面で収集しています。それを適切に取り扱うために・・・と言う仕組みを作っています。」といった文脈が必要である。

（続き）

- **内部向け個人情報保護方針は，次に示す事項を満たさなければならない。**
  - **e) 文書化した情報として利用可能である。**
  - **f) 組織内に伝達する。**
  - **g) 必要に応じて，利害関係者が入手可能である。**
- これは、個人情報保護方針の外形的基準になる。文書化していること、組織内外に分かるようにアナウンスしていることが必要になる。

（最初JISQ15001の要求事項）

- 事業者の代表者は、個人情報保護の理念を明確にした上で、次の事項を含む個人情報保護方針を定めるとともに、これを実行し維持しなければならない。
- a)　事業の内容及び規模を考慮した適切な個人情報の取得、利用及び提供に関すること（特定された利用目的の達成に必要な範囲を超えた個人情報の取扱い（以下、“目的外利用"という。)を行わないこと及びそのための措置を講じることを含む。)。
- b)　個人情報への不正アクセス、個人情報の漏えい、減失又はき損の防止並びに是正に関すること。
- c)　苦情対応に関すること。
- d)　個人情報の取扱いに関する法令、国が定める指針及びその他の規範を遵守すること。
- e)　個人情報保護マネジメントシステムの継続的改善に関すること。
- f)　代表者の氏名

- 事業者の代表者は、この方針を文書（電子的方式、磁気的方式その他人の知覚によっては認識できない方式で作られる記録を含む。以下、同じ。)化し、従業者に周知させるとともに、一般の人が入手可能な措置を講じなければならない。

5.2.2 外部向け個人情報保護方針

- **トップマネジメントは，次の事項を満たす外部向け個人情報保護方針を文書化し，一般の人が知り得るようにしなければならない。**
- **a) 5.2.1 で確立した内部向け個人情報保護方針に対して矛盾しない。**
- 外部向け個人情報保護方針を内部向け個人情報保護方針と違うものを作りなさいといっているわけではない。
- 外部向けの個人情報保護方針については、最初JISQ15001の要求事項が参考になるかもしれない。

5.3 組織の役割，責任及び権限

- **トップマネジメントは，個人情報保護に関連する役割に対して，責任及び権限を割り当て，利害関係者に伝達することを確実にしなければならない。**
- **トップマネジメントは，次の事項に対して，責任及び権限を割り当てなければならない。**
- **a) 個人情報保護マネジメントシステムが，この規格の要求事項に適合することを確実にする。**
- **b) 個人情報保護マネジメントシステムのパフォーマンスをトップマネジメントに報告する。**
- **注記 トップマネジメントは，個人情報保護マネジメントシステムのパフォーマンスを組織内に報告する責任及び権限を割り当ててもよい。**
- 用語の定義の中に特別な役割として、「3.40　個人情報保護管理者」と「3.41 個人情報保護監査責任者」が定義されている。a)に個人情報保護管理者に、b)に個人情報保護監査責任者に割り当てても良いだろう。

この動画の問い合わせは下記までどうぞ

中野　康範

ysnakano@nss.watson.jp