JISQ15001　解説補助

「6　計画」で気になったこと

（有）中野ソフトウエアサービス

2020/03/10

6　計画

- 「0.2 他のマネジメントシステム規格との近接性」には下記の記述がある。
  - この規格は，ISO/IEC 専門業務用指針 第1 部 統合版ISO 補足指針の附属書SL に規定する上位構造（HLS），共通の細分箇条題名，共通テキスト並びに共通の用語及び中核となる定義を参考にしており，附属書SL を採用した他のマネジメントシステム規格との近接性が保たれている。
- 現時点で公開されている上記資料では、「6.1　リスク及び機会への取り組み」と「6.2　XXX目的及びそれを達成するための計画策定」しかない。JISQ15001では6.1が細分化されている。固有の要求事項に展開されているので注意深く読んで行く。
- 参考のために次ページに共通テキストの内容を示す。

共通テキストの「6　計画」について

- 引用　Appendix2（規定）
- 「上位構造、共通の中核となるテキスト、共通用語及び中核となる定義」より

6.計画

6.1　リスク及び機会への取り組み

XXXマネジメントシステムの計画を策定するとき、組織は、4.1に規定する課題及び4.2二規定する要求事項を考慮し、次の事項のために取り組む必要があるリスク及び機会を決定しなければならない。

- XXXマネジメントシステムが、その意図した成果を達成できるという確信を与える
- 望ましくない影響を防止または提言する
- 継続的改善を達成する

組織は、次の事項を決定しなければならない

a)　上記によって決定したリスク及び機会への取り組み

b)　次の事項を行う方法

- その取り組みのXXXマネジメントプロセスへの統合及び実施
- その取り組みの有効性の評価

- 6.2　XXX目的及びそれを達成するための計画策定
- 組織は、関連する機能及び階層において、XXX目的を確立しなければならない。
- XXX目的は、次の事項を満たさなければならない。
- a)　XXX方針と整合している
- b)　（実行可能な場合）測定可能である
- c)　適用される要求事項を考慮に入れる
- d)　監視する
- e)　伝達する
- f)　必要に応じて、更新する
- 組織は、XXX目的に関する文書化した情報を保持しなければならない。
- 組織は、XXX目的をどのように達成するかについて計画するとき、次の事項を決定しなければならない。
- –　実施事項
- –　必要な資源
- –　責任者
- –　達成期限
- –　結果の評価方法

6.1 リスク及び機会に対処する活動

- 6.1は以下の項番に細分化されている
  - 6.1.1 一般
  - 6.1.2 個人情報保護リスクアセスメント
  - 6.1.3 個人情報保護リスク対応
- この中では具体的な施策（付属書A）についても言及がされている。
- この箇条の「リスク及び機会」というのは、ISOの審査員が頭を悩ました用語でもある。用語の定義では「3.9　リスク　目的に対する不確かさの影響」となっているが、ISOと言う枠組みを離れて、経営戦略などを語るときにはリスクとは「未来を左右する出来事」という程度で捉えている。代表的なところでは、「円相場が変動する」だろう。仮に円高進めば輸入業者には利点になり、輸出業は不利になる。
- 例えば個人情報保護マネジメントでいえば、「公共交通機関で個人情報を運搬する」というのがリスクであり、「漏洩」「紛失」は事故（もしくはハザード）という概念になる。しかし、JISの定義はこれとは異なる。
- 「リスクと機会」という言葉からは不確実性（例えば上記で云えば「公共交通機関で個人情報を運搬する」）によってもたらされる好ましい結果と好ましくない結果を意味すると捉える必要がある。
- こうした概念的な違いを配慮に入れてリスク分析を行う必要があるのに注意されたい。

6.1.1 一般

- **個人情報保護マネジメントシステムの計画を策定するとき，組織は，4.1 に規定する課題及び4.2 に規定する要求事項を考慮し，次の事項のために対処する必要があるリスク及び機会を決定しなければならない。**
  - **a) 個人情報保護マネジメントシステムが，その意図した成果を達成できることを確実にする。**
  - **b) 望ましくない影響を防止又は低減する。**
  - **c) 継続的改善を達成する。**
- **組織は，次の事項を計画しなければならない。**
  - **d) 上記によって決定したリスク及び機会に対処する活動**
  - **e) 次の事項を行う方法**
    - **1) その活動の個人情報保護マネジメントシステムプロセスへの統合及び実施**
    - **2) その活動の有効性の評価**
- この内容は共通テキストの内容をそのまま踏襲している。計画の内容はd)及びe)に記載されている。具体的には、個人情報保護の方針の策定や資源の配分、教育や内部監査、マネジメントレビュー、改善活動などが含まれる。

6.1.2 個人情報保護リスクアセスメント

- **組織は，次の事項を行う個人情報保護リスクアセスメントのプロセスを定め，適用しなければならない。**
- **a) 次を含む個人情報保護のリスク基準を確立し，維持する。**
- **1) リスク受容基準**
- **2) 個人情報保護リスクアセスメントを実施するための基準**
- 最初のパラグラフになる。突然、JISQ15001を目にする人は戸惑うことになる。簡単に言えば、そのリスク（例えば、電車の中に個人情報を保管しているパソコンを忘れる）と云うことが、頻繁に起きえるのか、それが起きたときにどの程度の影響があるのかなどを決定し、その組合わせとしての重大性を勘案して対策をとるかどうかを決める基準を設定すると言う文脈になる。
- 具体的には「リスク分析表」を作ることになる。リスク分析表については「JISQ15001:2017　個人情報保護マネジメントシステム　導入・実践ガイドブック　一般社団法人日本情報経済社会推進協会プライバシーマーク推進センター編」（日本規格協会）に記載されており、公式な見解として参照した方が良い。

- b) 繰り返し実施した個人情報保護リスクアセスメントに，一貫性及び妥当性があり，かつ，比較可能な結果を生み出すことを確実にする。
- c) 次によって個人情報保護リスクを特定する。
- 1) 個人情報保護マネジメントシステムの適用範囲内における個人情報の不適切な取扱いに伴うリスクを特定するために，個人情報保護リスクアセスメントのプロセスを適用する。
- 2) これらのリスク所有者を特定する。
- d) 次によって個人情報保護リスクを分析する。
- 1) 6.1.2 c) 1) で特定されたリスクが実際に生じた場合に起こり得る結果についてアセスメントを行う。
- 2) 6.1.2 c) 1) で特定されたリスクの現実的な起こりやすさについてアセスメントを行う。
- 3) リスクレベル（リスクの大きさ）を決定する。
- e) 次によって個人情報保護リスクを評価する。
- 1) リスク分析の結果と6.1.2 a) で確立したリスク基準とを比較する。
- 2) リスク対応のために，分析したリスクの優先順位付けを行う。
- 組織は，個人情報保護リスクアセスメントのプロセスについての文書化した情報を保持しなければならない。

- いずれもリスク分析の仕方を規定する要素になっている。
- リスク分析に当たっては明確な手順や書式を作ってこれを実施することが必要になる。
- 高度なリスク分析という側面では、インシデント情報（例えば、サーバーへのアクセスの状況）の分析なども考えられるが、過度な対応は望ましくない。ごく自然に情報が収集できるならいざ知らず、専門家や専門の仕組みが必要なら、それがないことを前提に考えれば善い。

6.1.3 個人情報保護リスク対応

- 組織は，次の事項を行うために，個人情報保護リスク対応のプロセスを定め，適用しなければならない。
- a) リスクアセスメントの結果を考慮して，適切な個人情報保護リスク対応の選択肢を選定する。
- b) 選定した個人情報保護リスク対応の選択肢の実施に必要な全ての管理策を決定する。
- 注記 組織は，必要な管理策を設計するか，又は任意の情報源の中から管理策を特定することができる。
- c) 6.1.3 b) で決定した管理策を**附属書A** に示す管理策と比較し，必要な管理策が見落とされていないことを検証する。
- 注記**1 附属書A** は，管理目的及び管理策の包括的なリストである。この規格の利用者は，必要な管理策の見落としがないことを確実にするために，**附属書A** を参照する。
- 注記2 管理目的は，管理策に暗に含まれている。**附属書A** に規定した管理目的及び管理策は，全てを網羅してはいないため，追加の管理目的及び管理策が必要となる場合がある。

- 「個人情報保護リスク対応」というのは、具体的な“個人情報”を適切に取り扱うための個人情報保護マネジメントで実施すべき管理策を指しているのだろう。
- 何度も出てくる「付属書A」とは、この規格の後ろについてくる「附属書A（規定）管理目的及び管理策」のことである。
- 実質的に、企業がすべき具体策がここに記述されている。

- **d) 個人情報保護リスク対応計画を策定する。**
- **e) 個人情報保護リスク対応計画及び残留している個人情報保護リスクの受容について，リスク所有者の承認を得る。**
- **組織は，個人情報保護リスク対応のプロセスについての文書化した情報を保持しなければならない。**
- **注記 この規格の個人情報保護リスクアセスメント及びリスク対応のプロセスは，JIS Q 31000 に規定する原則及び一般的な指針と整合している。**
- 文書か要求が含まれている。
- リスク分析の前提となる業務プロセスの明確化、リスク分析表、これに基づく管理策の一覧表などは、対策のもれ抜けなどがないように図や表にしておくことを勧める。

6.2 個人情報保護目的及びそれを達成するための計画策定

- 組織は，関連する部門及び階層において，個人情報保護目的を確立しなければならない。
- 個人情報保護目的は，次の事項を満たさなければならない。
  - a) 内部向け個人情報保護方針と整合している。
  - b) （実行可能な場合）測定可能である。
  - c) 適用される個人情報保護要求事項，並びにリスクアセスメント及びリスク対応の結果を考慮に入れる。
  - d) 伝達する。
  - e) 必要に応じて，更新する。
- 組織は，個人情報保護目的に関する文書化した情報を保持しなければならない。
- 組織は，個人情報保護目的をどのように達成するかについて計画するとき，次の事項を決定しなければならない。
  - f) 実施事項
  - g) 必要な資源
  - h) 責任者
  - i) 達成期限
  - j) 結果の評価方法

- 共通テキストのXXXに単純に「個人情報保護」という言葉を入れてしまったのでこういう文言になってしまったのだろう。
- ここでは、「目的」を「の目的達成のためにすべき活動」と置き換えた方が自然になるだろう。個人情報保護マネジメントシステムが有効に機能するために各階層・部門では何をすべきかを明らかにし、その活動がうまくいっているのかを何で見て行くのかという議論の中で、自然に計画が決まってくる。一般的には「目標管理」と云うことが該当する。
- 少しわかりにくいのが「b) （実行可能な場合）測定可能である。」かもしれない。一般的には定量可能な数値を求めることが多いが、これにこだわる必要はない。要は目的が達成されたかどうかの判断ができれば良い。
- 「ISO9001　何をなすべきか　ISO/TC176からの助言には下記の記述があります。
  - 例えば、達成の必要がある期間または所定の量を測定する方法があります。品質目標は定量的な方法だけでなく、定性的な方法（例えば、サービスのパフォーマンスレベル）を併用することで測定可能なものにすることができます。
- たとえばコールセンターでは呼び出し音3回以内に受話器を取ることでも良い。あるいは、10月末までに全社員に個人情報保護マネジメントに関する教育を受けさせるでも良いだろう。

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