2014.4

「個人情報保護マネジメントシステム実施ハンドブック」簡易版　第 24 章

個人情報保護監査研究会

第24章　マネジメントシステムの統合化

24.1　マネジメントシステム規格（MSS 規格：Management System Standard)

個人情報保護マネジメントシステム（JIS Q15001:2006）では、「マネジメントシステム規格の正当性及び作成に関する指針」（ISO Guide 72:2001）に基づき、他のマネジメントシステム規格との構造の整合性に配慮するよう求めています。

また、2012 年 5 月 1 日には、ISO/IEC Directives（専門業務用指針）の「統合版 ISO 補足指針」として、マネジメントシステムの統合化のための「MSS 共通テキスト」が取りまとめられました。

※ご参考（一般財団法人日本規格協会）：http://www.jsa.or.jp/itn/pdf/shiryo/iso_supplement_sl234.pdf

24.2　統合マニュアルを作成する場合の基本事項

マネジメントシステムの統合化では、「3.4.5 教育」、「3.5.2 文書管理」、「3.5.3 記録の管理」、「3.7.2 監査」、「3.8 是正処置及び予防処置」、「3.9 事業者の代表者による見直し」の統合を主眼として行うことをお勧めします。共通項目として実施することで、従業者にとっても、理解しやすく年間スケジュール、研修講師、内部監査員の手配についても、高いパフォーマンスを得られる結果となります。

24. 3　統合マニュアルの構造

ＰＭＳにおける、１．適用範囲～　3.4.4 個人情報に関する本人の権利、までは、ＰＭＳ個別のマニュアルとします。保護対象である個人情報の特定、リスク分析については個別の要求事項に従うためです。ここでは、「統合版 ISO 補足指針」、JISQ27001:2014(**ISO27001:2013**)を参考に、個人情報保護マネジメントシステム（**PMS**）を含める場合の事例をご紹介します。

PMS:3.4.5　教育　(ISO27001:2013：7.2 力量)

事業者は、次の事項を行う。

a) 事業者の PMS／その他 MS に関連する業務を行う従業者に必要な、力量を決定する。
b) 従業者が、適切な教育、訓練、経験に基づいて、力量を備えることを確実にする。
c) 該当する（教育対象）には必ず、必要な力量を身につけるための処置をとり、処置の有効性を評価する。
d) 力量の証拠の情報は、文書化して保持する。

PMS:3.4.5　教育　(ISO27001:2013：7.3 認識)

事業者は、事業者の管理下で働く従業者に次の事項に関して認識を持たせる。

a) PMS／その他 MS 方針
b) PMS／その他 MS の有効性に対する自らの貢献
c) PMS／その他 MS 要求事項に適合しないことの意味

PMS:3.5.2 文書管理　(ISO27001:2013：7.5　文書化した情報、7.5.1 一般)

事業者の PMS／その他 MS には、次の事項を含める。

a) PMS／その他 MS の要求事項

b) PMS／その他 MS の有効性のために必要であると事業者が決定した事項

PMS:3.5.2 文書管理、3.5.3 記録の管理　(ISO27001:2013　7.5.2 作成及び更新)

文書化した情報を作成及び更新する際、事業者は、次の事項を確実にする。

a) 適切な識別及び記述　(例：タイトル、日付、作成者、参照番号)

b) 適切な形式　(例：言語、ソフトウエアの版、図表)　及び媒体(例：紙、電子媒体)

c) 適切性及び妥当性に関する、適切なレビュー及び承認

PMS: 3.5.2 文書管理、3.5.3 記録の管理 (ISO27001:20137.5.3 文書化した情報の管理)

文書化した情報の管理に当たって、事業者は、該当する場合には、必ず、次の行動に取り組む。

PMS／その他 MS の計画及び運用のために、事業者が必要と決定した外部からの情報は、必要に応じて特定し、管理する。

a)文書化した情報は、必要なときに入手可能かつ利用に適した状態に置く。

b)文書化した情報が十分に保護されている(例：機密性の喪失、不適切な使用及び完全性の喪失からの保護)

c)配付、アクセス、検索及び利用。

d)読み易さが保たれることを含む、保管及び保存。

e)変更の管理(例：版の管理)

f)保持及び廃棄

PMS:3.7.2 監査　(ISO27001:2013　9.2　内部監査)

事業者は、PMS／その他 MS が次の状況にあるか否かに関する情報を得るために、あらかじめ定められた開隔で内部監査を実施する。

a) PMS／その他 MS に対して事業者自体が決定した要求事項、及び規格が要求する要求事項に適合する。

b) 有効に実施され、維持されている。

c) 頻度、方法、責任及び計画に関する要求事項及び報告を含む、監査プログラムの計画、確立、実施及び維持されている。監査プログラムは、関連するプロセスの重要性及び前回までの監査の結果を考慮に入れる。

d) 各監査について、監査基準及び監査範囲を明確にする。

e) 監査プロセスの客観性及び公平性を確保する監査員を選定し、監査を実施する。

f) 監査の結果を関連する事業者の管理層に報告することを確実にする。

g) 監査プログラムの実施及び監査結果の証拠として、文書化した情報を保持する。

PMS:3.8 是正処置及び予防処置　(ISO27001:2013　10.1 不適合及び是正処置)

不適合が発生した場合、事業者は、次の事項を行う。

a) その不適合に対処し、該当する場合は次の事項を行う。

1) その不適合を管理し、修正するための処置をとる。

2) その不適合によって起こった結果に対処する。

b) 不適合が再発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。
1) その不適合をレビューする。
2) その不適合の原因を明確にする。
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。

c) 必要な処置を実施する。
d) とった全ての是正処置の有効性をレビューする。
e) 必要な場合には、PMS／その他 MS の是正処置を行う。 是正処置は、検出された不適合のもつ影響に応じたものとする。
f) 不適合の性質及びとった処置の文書化した情報を保持する。
g) 是正処置の証拠として、文書化した情報を保持する。

PMS:3.9 事業者の代表者による見直し　(ISO27001:2013　9.3 マネジメントレビュー)

代表者は、事業者の PMS／その他 MS が、引き続き、適切、妥当かつ有効であることを確実にするために、あらかじめ定めた間隔で、PMS／その他 MS をレビューする。
マネジメントレビューは、次の事項を考慮する。

a) 前回までのマネジメントレビューの結果とった処置の状況
b) PMS／その他 MS に関連する外部及び内部の課題の変化
c) 次に示す傾向を含めた、PMS／その他 MS のパフォーマンスに関するフィードバック
1) 不適合及び是正処置
2) 監視及び測定の結果
3) 監査結果
4) 各目的の達成
d) 利害関係者からのフィードバック
e) リスクアセスメントの結果及びリスク対応計画の状況
f) 継続的改善の機会

事業者の代表者による見直しからのアウトプットには、継続的改善の機会、及び PMS／その他 MS のあらゆる変更の必要性に関する決定を含む。
事業者は、事業者の代表者による見直しの結果の証拠として、文書化した情報を保持する。

2015 年には個人情報保護法の改定が予定されています。ビッグデータに象徴されるパーソナルデータ利活用や、個人情報保護のグローバル化に対応する見直しに向けて、保護と活用の観点から、各法令の整備も行われます。マネジメントシステムの統合化による、パフォーマンス向上へのニーズはますます高まっていくことでしょう。

次回は、「第 25 章　システム管理基準　個人情報保護コントロール」をご紹介します。＞目次へ

個人情報保護監査研究会　http://www.saaj.or.jp/shibu/kojin.html　以上