JIS Q 15001:2017 附属書 A（規定）管理目的及び管理策のポイント

JIS Q 15001:2017 附属書 A の管理目的及び管理策のポイントを理解するために、規定内容の概要と共に一覧で示したものです。規定の詳細は、JIS Q 15001:2017 にてご確認下さい。

A.3.1 一般

個人情報保護マネジメントシステムの運用を行うため。

A.3.1.1 一般

管理策に規定する事項 は，権限を与えられた者が定めた手段に従い承認する。

A.3.2 個人情報保護方針

個人情報保護の理念を明確にし，公表するため。

A.3.2.1 内部向け個人情報保護方針

内部向け個人情報保護方針を文書化し組織内に伝達。利害関係者が入手可能にする。

A.3.2.2 外部向け個人情報保護方針

外部向け個人情報保護方針を文書化し一般の人が入手可能な措置を講じる。

A.3.3 計画

個人情報の取扱いに関する計画を策定するため。

A.3.3.1 個人情報の特定

個人情報を特定するための手順の確立と維持。を管理するための台帳の整備。

A.3.3.2 法令，国が定める指針その他の規範

関連する法令，国が定める指針その他の規範を特定し参照できる手順を確立し維持する。

A.3.3.3 リスクアセスメント及びリスク対策

個人情報保護リスクを特定し，分析し，必要な対策を講じる手順を確立し，維持する。

A.3.3.4 資源，役割，責任及び権限

個人情報保護管理者および個人情報保護監査責任者を指名する。

A.3.3.5 内部規程

内部規程を文書化し，維持する。

A.3.3.6 計画策定

必要な計画を立案し，文書化し，かつ維持する。

A.3.3.7 緊急事態への準備

緊急事態の特定及びどのように対応するかの手順を確立し，実施し，かつ維持する。

A.3.4 実施及び運用

運用段階において個人情報の取扱いを行うため。

A.3.4.1 運用手順

運用の手順を明確にする。

A.3.4.2 取得，利用及び提供に関する原則

A.3.4.2.1 利用目的の特定

個人情報の利用目的を特定し，必要な範囲内においてを取り扱う。

A.3.4.2.2 適正な取得

適法かつ公正な手段によって個人情報を取得する。

A.3.4.2.3 要配慮個人情報

あらかじめ書面による本人の同意を得ないで，要配慮個人情報を取得してはならない。

A.3.4.2.4 個人情報を取得した場合の措置

速やかに，その利用目的を，本人に通知するか，又は公表する。

A.3.4.2.5 A.3.4.2.4 のうち本人から直接書面によって取得する場合の措置

本人から書面に記載された個人情報を直接取得する場合，書面によって本人に明示し本人の同意を得る。

A.3.4.2.6 利用に関する措置

特定した利用目的の達成に必要な範囲内で個人情報を利用する。

A.3.4.2.7 本人に連絡又は接触する場合の措置

本人に連絡又は接触する場合，本人に対し本人の同意を得なければならない。

A.3.4.2.8 個人データの提供に関する措置

個人データを第三者に提供する場合には，本人に対し本人の同意を得なければならない。

A.3.4.2.8.1 外国にある第三者への提供の制限

外国にある第三者に個人データを提供する場合，本人の同意を得なければならない。

A.3.4.2.8.2 第三者提供に係る記録の作成など

個人データを第三者に提供したときは，記録を作成し，保管しなければならない。

A.3.4.2.8.3 第三者提供を受ける際の確認など

第三者から個人データの提供を受けるに際しては，確認を行わなければならない。

A.3.4.2.9 匿名加工情報

匿名加工情報の取扱いを行うか否かの方針を定め，取り扱う場合は，適切な取扱いを行う手順を確立し，維持する。

A.3.4.3 適正管理

A.3.4.3.1 正確性の確保

個人データを，正確，かつ，最新の状態で管理しなければならない。必要がなくなったときは，消去する。

A.3.4.3.2 安全管理措置

個人情報の安全管理のために必要かつ適切な措置を講じなければならない。

A.3.4.3.3 従業者の監督

個人データの安全管理が図られるよう，従業者に対する必要かつ適切な監督を行う。

A.3.4.3.4 委託先の監督

個人データの取扱いを委託する場合，保護水準を満たしている者を選定し，委託契約を締結し，監督を行う。

A.3.4.4 個人情報に関する本人の権利

A.3.4.4.1 個人情報に関する権利

保有個人データに関して，本人から開示等の請求等を受け付けた場合，遅滞なくこれに応じる。

A.3.4.4.2 開示等の請求等に応じる手続

開示等の請求等に応じる手続を定める。

A.3.4.4.3 保有個人データに関する事項の周知など

保有個人データに関し，苦情の申出先等の事項を本人の知り得る状態に置く。

A.3.4.4.4 保有個人データの利用目的の通知

保有個人データについて，利用目的の通知を求められた場合，遅滞なくこれに応じる。

A.3.4.4.5 保有個人データの開示

保有個人データの開示の請求を受けたとき，本人に対し，遅滞なく，当該保有個人データを書面によって開示する。

A.3.4.4.6 保有個人データの訂正，追加又は削除

保有個人データの訂正，追加又は削除の請求を受けた場合，遅滞なく必要な調査を行い，訂正等を行い，本人に通知する。

A.3.4.4.7 保有個人データの利用又は提供の拒否権

保有個人データの利用の停止，消去又は第三者への提供の停止の請求を受けた場合，これに応じ，措置後，本人に通知する。

A.3.4.5 認識

従業者が認識をもつため，関連する各部門及び階層における認識させる手順を確立し，維持する。

A.3.5 文書化した情報

文書化した情報を作成・維持するため。

A.3.5.1 文書化した情報の範囲

個人情報保護マネジメントシステムの基本となる要素を書面で記述する。

A.3.5.2 文書化した情報（記録を除く。）の管理

文書化した情報（記録を除く。）を管理する手順を確立し，実施し，かつ維持する。

A.3.5.3 文書化した情報のうち記録の管理

個人情報保護マネジメントシステム及びこの規格の要求事項への適合を実証するために必要な記録を作成し，維持する。

A.3.6 苦情及び相談への対応

苦情及び相談に対応するため。
本人からの苦情及び相談を受け付けて，適切かつ迅速な対応を行う手順を確立し，維持する。

A.3.7 パフォーマンス評価

パフォーマンス評価を実施するため。

A.3.7.1 運用の確認

個人情報保護マネジメントシステムが適切に運用されていることが確認されるための手順を確立し，実施し，かつ維持する。

A.3.7.2 内部監査

個人情報保護マネジメントシステムの JIS 規格への適合状況及び個人情報保護マネジメントシステムの運用状況を監査する。

A.3.7.3 マネジメントレビュー

少なくとも年一回，適宜に個人情報保護マネジメントシステムを見直す。

A.3.8 是正処置

不適合に対する是正処置を確実に実施するための責任及び権限を定める手順を確立し，実施し，かつ維持する。

©2018 ISM Web store