

JIS

個人情報保護マネジメントシステム— 要求事項

JIS Q 15001 : 2023

令和 5 年 9 月 20 日 改正

日本産業標準調査会 審議

(日本規格協会 発行)

日本産業標準調査会標準第二部会 情報技術専門委員会 構成表

	氏名	所属
(委員長)	河合 和哉	国立研究開発法人産業技術総合研究所
(委員)	青木 裕佳子	公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会
	足立 朋子	株式会社東芝
	荒木 則幸	日本電信電話株式会社
	伊藤 雅樹	株式会社日立製作所
	上原 まひる	ソニーグループ株式会社
	高岡 詠子	上智大学
	中里 学	総務省国際戦略局
	永沼 美保	日本電気株式会社
	仲谷 文雄	一般社団法人ビジネス機械・情報システム産業協会
	永山 はるみ	一般財団法人日本消費者協会
	橋本 崇	日本銀行
	福田 健太郎	日本アイ・ビー・エム株式会社
	山崎 朋子	一般財団法人日本規格協会

主 務 大 臣：経済産業大臣 制定：平成 11.3.20 改正：令和 5.9.20

官 報 掲 載 日：令和 5.9.20

原案作成協力者：一般財団法人日本情報経済社会推進協会

(〒106-0032 東京都港区六本木 1-9-9 六本木ファーストビル内 TEL 03-5860-7551)

審 議 部 会：日本産業標準調査会 標準第二部会 (部会長 古関 隆章)

審議専門委員会：情報技術専門委員会 (委員長 河合 和哉)

この規格についての意見又は質問は、上記原案作成協力者又は経済産業省産業技術環境局 国際電気標準課 (〒100-8901 東京都千代田区霞が関 1-3-1 E-mail:jisc@meti.go.jp 又は FAX 03-3580-8625) にご連絡ください。

なお、日本産業規格は、産業標準化法の規定によって、少なくとも5年を経過する日までに日本産業標準調査会の審議に付され、速やかに、確認、改正又は廃止されます。

目 次

	ページ
0 序文	1
0.1 一般	1
0.2 概要	1
0.3 他のマネジメントシステム規格との近接性	2
1 適用範囲	2
2 引用規格	2
3 用語及び定義	2
3.1 マネジメントシステムに関する用語	2
3.2 個人情報保護リスクアセスメント及び対応に関する用語	6
3.3 個人情報保護に関する用語	9
4 組織の状況	11
4.1 組織及びその状況の理解	11
4.2 利害関係者のニーズ及び期待の理解	11
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	11
4.4 個人情報保護マネジメントシステム	11
5 リーダーシップ	12
5.1 リーダーシップ及びコミットメント	12
5.2 方針	12
5.3 役割, 責任及び権限	13
6 計画策定	14
6.1 個人情報の特定	14
6.2 リスク及び機会への取組	14
6.3 個人情報保護目的及びそれを達成するための計画策定	16
6.4 変更の計画策定	17
7 支援	17
7.1 資源	17
7.2 力量	17
7.3 認識	18
7.4 コミュニケーション	18
7.5 文書化した情報	19
8 運用	21
8.1 運用の計画及び管理	21
8.2 個人情報保護リスクアセスメント	22
8.3 個人情報保護リスク対応	22
9 パフォーマンス評価	22

	ページ
9.1 監視, 測定, 分析及び評価	22
9.2 内部監査	23
9.3 マネジメントレビュー	23
10 改善	24
10.1 継続的改善	24
10.2 不適合及び是正処置	24
附属書 A (規定) 個人情報保護に関する管理策	26
附属書 B (参考) マネジメントシステムに関する補足	34
附属書 C (参考) 附属書 A の管理策に関する補足	46
附属書 D (参考) 安全管理措置に関する管理目的及び管理策	63
附属書 E (参考) JIS Q 15001:2023 と JIS Q 15001:2017 との対応	74
参考文献	80
解 説	81

まえがき

この規格は、産業標準化法に基づき、日本産業標準調査会の審議を経て、経済産業大臣が改正した日本産業規格である。これによって、**JIS Q 15001:2017** は改正され、この規格に置き換えられた。

この規格は、著作権法で保護対象となっている著作物である。

この規格の一部が、特許権、出願公開後の特許出願又は実用新案権に抵触する可能性があることに注意を喚起する。経済産業大臣及び日本産業標準調査会は、このような特許権、出願公開後の特許出願及び実用新案権に関わる確認について、責任はもたない。

白 紙

個人情報保護マネジメントシステム—要求事項

Personal information protection management systems—Requirements

0 序文

0.1 一般

この規格は、1999年に第1版が制定され、2006年及び2017年に改正が行われた（以下、旧規格という。）。その後の個人情報の保護に係る法律の改正に伴い、内容の整合性を図るために改正した日本産業規格である。

なお、対応国際規格は現時点で制定されていない。また、この規格と旧規格との対応を**附属書 E**に示す。

0.2 概要

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の全ては、時間とともに変化することが見込まれる。

個人情報保護マネジメントシステムは、リスクマネジメントプロセスを適用することによって個人情報の保護を維持し、かつ、リスクを適切に管理しているという信頼を利害関係者に与える。

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。

この規格は、組織自身の個人情報保護要求事項を満たす組織の能力を、組織の内部で評価するために用いることも、また、外部関係者が評価するために用いることも可能である。

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。本文中の細別符号 [例えば、**a)**, **b)**, 又は **1)**, **2)**] は、参照目的のためだけに付記している。

この規格は、本文のほか、**附属書 A**は“個人情報保護に関する管理策”、**附属書 B**は“マネジメントシステムに関する補足”、**附属書 C**は“**附属書 A**の管理策に関する補足”、**附属書 D**は“安全管理措置に関する管理目的及び管理策”、**附属書 E**は“**JIS Q 15001:2023**と**JIS Q 15001:2017**との対応”で構成されている。