

JIS

情報セキュリティ，サイバーセキュリティ 及びプライバシー保護— 情報セキュリティ管理策

JIS Q 27002 : 2024

(ISO/IEC 27002 : 2022)

(JSA)

令和 6 年 6 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
	山本 浩司	日本電信電話株式会社
	相蘭 敏子	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
	中越 一彰	総務省国際戦略局
	永沼 美保	日本電気株式会社
	永山 はるみ	一般財団法人日本消費者協会
	西口 周作	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 18.5.20 改正：令和 6.6.20

官 報 掲 載 日：令和 6.6.20

原 案 作 成 者：一般財団法人日本規格協会

(〒108-0073 東京都港区三田 3-11-28 三田 Avanti TEL 050-1742-6017)

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) 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 背景及び状況	1
0.2 情報セキュリティ要求事項	2
0.3 管理策	2
0.4 管理策の決定	2
0.5 組織固有の指針の策定	3
0.6 ライフサイクルに関する考慮事項	3
0.7 関連国際規格	3
1 適用範囲	4
2 引用規格	4
3 用語及び定義並びに略語	4
3.1 用語及び定義	4
3.2 略語	9
4 この規格の構成	11
4.1 箇条	11
4.2 テーマ及び属性	11
4.3 管理策の構成	12
5 組織的管理策	13
5.1 情報セキュリティのための方針群	13
5.2 情報セキュリティの役割及び責任	15
5.3 職務の分離	16
5.4 管理層の責任	17
5.5 関係当局との連絡	18
5.6 専門組織との連絡	18
5.7 脅威インテリジェンス	19
5.8 プロジェクトマネジメントにおける情報セキュリティ	20
5.9 情報及びその他の関連資産の目録	22
5.10 情報及びその他の関連資産の許容される利用	24
5.11 資産の返却	25
5.12 情報の分類	26
5.13 情報のラベル付け	27
5.14 情報の転送	28
5.15 アクセス制御	31
5.16 識別情報の管理	33
5.17 認証情報	34

5.18	アクセス権	36
5.19	供給者関係における情報セキュリティ	37
5.20	供給者との合意における情報セキュリティの取扱い	39
5.21	ICT サプライチェーンにおける情報セキュリティの管理	41
5.22	供給者のサービス提供の監視, レビュー及び変更管理	43
5.23	クラウドサービスの利用における情報セキュリティ	45
5.24	情報セキュリティインシデント管理の計画策定及び準備	47
5.25	情報セキュリティ事象の評価及び決定	49
5.26	情報セキュリティインシデントへの対応	49
5.27	情報セキュリティインシデントからの学習	50
5.28	証拠の収集	51
5.29	事業の中断・障害時の情報セキュリティ	52
5.30	事業継続のための ICT の備え	53
5.31	法令, 規制及び契約上の要求事項	54
5.32	知的財産権	55
5.33	記録の保護	57
5.34	プライバシー及び PII の保護	58
5.35	情報セキュリティの独立したレビュー	59
5.36	情報セキュリティのための方針群, 規則及び標準の順守	60
5.37	操作手順書	61
6	人的管理策	62
6.1	選考	62
6.2	雇用条件	63
6.3	情報セキュリティの意識向上, 教育及び訓練	64
6.4	懲戒手続	66
6.5	雇用の終了又は変更後の責任	67
6.6	秘密保持契約又は守秘義務契約	68
6.7	リモートワーク	69
6.8	情報セキュリティ事象の報告	70
7	物理的管理策	71
7.1	物理的セキュリティ境界	71
7.2	物理的入退	72
7.3	オフィス, 部屋及び施設のセキュリティ	74
7.4	物理的セキュリティの監視	75
7.5	物理的及び環境的脅威からの保護	76
7.6	セキュリティを保つべき領域での作業	77
7.7	クリアデスク・クリアスクリーン	78
7.8	装置の設置及び保護	79
7.9	構外にある資産のセキュリティ	79

7.10	記憶媒体	81
7.11	サポートユーティリティ	82
7.12	ケーブル配線のセキュリティ	83
7.13	装置の保守	84
7.14	装置のセキュリティを保った処分又は再利用	85
8	技術的管理策	86
8.1	利用者エンドポイント機器	86
8.2	特権的アクセス権	88
8.3	情報へのアクセス制限	90
8.4	ソースコードへのアクセス	91
8.5	セキュリティを保った認証	93
8.6	容量・能力の管理	94
8.7	マルウェアに対する保護	96
8.8	技術的ぜい弱性の管理	97
8.9	構成管理	101
8.10	情報の削除	103
8.11	データマスキング	104
8.12	データ漏えい防止	106
8.13	情報のバックアップ	107
8.14	情報処理施設・設備の冗長性	109
8.15	ログ取得	110
8.16	監視活動	113
8.17	クロックの同期	115
8.18	特権的なユーティリティプログラムの使用	116
8.19	運用システムへのソフトウェアの導入	117
8.20	ネットワークセキュリティ	118
8.21	ネットワークサービスのセキュリティ	119
8.22	ネットワークの分離	121
8.23	ウェブフィルタリング	122
8.24	暗号の利用	123
8.25	セキュリティに配慮した開発のライフサイクル	125
8.26	アプリケーションセキュリティの要求事項	126
8.27	セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則	128
8.28	セキュリティに配慮したコーディング	130
8.29	開発及び受入れにおけるセキュリティテスト	133
8.30	外部委託による開発	134
8.31	開発環境、テスト環境及び本番環境の分離	135
8.32	変更管理	137
8.33	テスト用情報	138

	ページ
8.34 監査におけるテスト中の情報システムの保護	139
附属書 A (参考) 属性の使用	141
附属書 B (参考) この規格と JIS Q 27002:2014 との対応	155
解 説	166

まえがき

この規格は、産業標準化法第 16 条において準用する同法第 12 条第 1 項の規定に基づき、一般財団法人日本規格協会（JSA）から、産業標準原案を添えて日本産業規格を改正すべきとの申出があり、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 27002:2014** 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

情報セキュリティ、サイバーセキュリティ及び プライバシー保護—情報セキュリティ管理策

Information security, cybersecurity and privacy protection— Information security controls

0 序文

この規格は、2022年に第3版として発行された **ISO/IEC 27002** を基に、技術的内容及び構成を変更することなく作成した日本産業規格である。

なお、この規格で点線の下線を施してある参考事項は、対応国際規格にはない事項である。

この規格には、同じ細分箇条内、同じラテン文字の細別符号を繰り返して用いている箇所があるが、対応する国際規格の技術的内容及び様式との整合を最大限に保つことを優先するため、国際規格どおりに細別を付番したものであり、それらの細別の引用・参照に当たっては、どの段落の細別を指定しているかが特定可能となるよう注意が必要である。

0.1 背景及び状況

この規格は、全ての形態及び規模の組織を対象としている。この規格は、**JIS Q 27001** に基づく情報セキュリティマネジメントシステム (ISMS) において、情報セキュリティリスク対応の管理策を決定し、実施するための参考として用いる。この規格はまた、一般に受け入れられている情報セキュリティ管理策を組織が決定し、実施するための手引として用いることも可能である。さらに、この規格は、それぞれに固有の情報セキュリティリスクの環境を考慮に入れて、業界及び組織に固有の情報セキュリティマネジメントの指針を作成する場合に用いることも意図している。必要に応じて、この規格にある管理策以外に、組織又は環境に固有の管理策をリスクアセスメントを通じて決定することも可能である。

形態及び規模を問わず、全ての組織（公共部門及び民間部門、並びに営利及び非営利を含む。）は、電子的形式、物理的形式及び口頭（例えば、会話、プレゼンテーション）を含む多くの形式で、情報を作成、収集、処理、保存、送信及び破棄する。

情報には、書かれた言葉、数字及び画像そのものを上回る価値がある。知識、概念、アイデア及びブランドは、そのような無形の情報の例である。相互につながった世界では、情報及びその他の関連資産は、自然現象、偶発的又は意図的なもののいずれであれ、様々なリスク源から保護するに値するものであり、又は保護する必要がある。

情報セキュリティは、方針、規則、プロセス、手順、組織構造、並びにソフトウェア及びハードウェアの機能を含む、一連の適切な管理策を実施することで達成される。組織は、固有のセキュリティ目的及び