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
（委員会長）	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 薗 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 﨑 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（委員会長　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

ページ

ページ

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

日本産業規格　　JIS
Q 27002：2024
(ISO/IEC 27002：2022)

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