JIS

情報技術－セキュリティ技術－
情報セキュリティ管理策の
実践のための規範

JIS Q 27002：2014

（ISO/IEC 27002：2013）

（JSA）

平成 26 年 3 月 20 日　改正

日本工業標準調査会 審議

（日本規格協会 発行）

著作権法により無断での複製，転載等は禁止されております。

日本工業標準調査会標準部会 構成表

	氏名	所属
（部会長）	稲　葉　　敦	工学院大学
（委員）	伊　藤　　弘	公益財団法人住宅リフォーム・紛争処理支援センター
	大　橋　　守	一般社団法人日本鉄鋼連盟
	金　丸　淳　子	公益財団法人共用品推進機構
	河　村　真紀子	主婦連合会
	窪　塚　孝　夫	公益社団法人自動車技術会
	高　久　　昇	一般財団法人日本規格協会
	田　中　護　史	一般財団法人日本船舶技術研究協会
	土　肥　義　治	公益財団法人高輝度光科学研究センター
	中　西　英　夫	一般社団法人ビジネス機械・情報システム産業協会
	野　口　祐　子	グーグル株式会社
	長谷川　英　一	一般社団法人電子情報技術産業協会

主　務　大　臣：経済産業大臣　　制定：平成 18.5.20　　改正：平成 26.3.20
官　報　公　示：平成 26.3.20
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 3-13-12 三田 MT ビル　TEL 03-4231-8530）
審　議　部　会：日本工業標準調査会　標準部会（部会長　稲葉　敦）

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 基準認証ユニット管理システム標準化推進室（〒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，日本工業規格は，工業標準化法第 15 条の規定によって，少なくとも 5 年を経過する日までに日本工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。

著作権法により無断での複製，転載等は禁止されております。

目　次

著作権法により無断での複製，転載等は禁止されております。

ページ

著作権法により無断での複製，転載等は禁止されております。

まえがき

この規格は，工業標準化法第 14 条によって準用する第 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，工業標準原案を具して日本工業規格を改正すべきとの申出があり，日本工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工業規格である。これによって，**JIS Q 27002**:2006 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工業標準調査会は，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。

著作権法により無断での複製，転載等は禁止されております。

白　　紙

著作権法により無断での複製，転載等は禁止されております。

日本工業規格　　JIS
Q 27002：2014
(ISO/IEC 27002：2013)

情報技術－セキュリティ技術－
情報セキュリティ管理策の実践のための規範

Information technology—Security techniques—
Code of practice for information security controls

0　序文

この規格は，2013 年に第 2 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工業規格である。

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。

0.1　背景及び状況

この規格は，組織が，**JIS Q 27001** [10] に基づく情報セキュリティマネジメントシステム（以下，ISMS という。）を実施するプロセスにおいて，管理策を選定するための参考として用いる，又は一般に受け入れられている情報セキュリティ管理策を実施するための手引として用いることを意図している。また，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。

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，情報を収集，処理，保存及び送信する。

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，情報も，情報に関連するプロセス，システム，ネットワーク並びにこれらの運営，取扱い及び保護に関与する要員も，他の重要な事業資産と同様，組織の事業にとって高い価値をもつ資産であり，様々な危険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。

資産は，意図的及び偶発的な脅威の両方にさらされるが，関連するプロセス，システム，ネットワーク及び要員には内在的なぜい弱性がある。事業のプロセス及びシステムに対する変更，又はその他の外部の変更（新しい法令，規制など）によって，新たな情報セキュリティリスクが発生することもある。すなわち，脅威がぜい弱性を利用して，組織に害を及ぼす方法が無数にあることを考え合わせると，情報セキュリティリスクは常に存在する。有効な情報セキュリティは，脅威及びぜい弱性から組織を保護することで，これらのリスクを低減し，これによって，資産に対する影響を低減する。

情報セキュリティは，方針，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。これらの管理策は，組織固有のセキュリティ目的及び事業目的を満たすことを確実にするために，必要に応じて確立，実施，監視，レビュー及び改善をする必要がある。**JIS Q 27001** [10] に規定する ISMS では，一貫したマネジメントシステムの総合的な枠組みに基づいて，包括的な情報セキュリティ管理策集を実施するため，組織の情報セキュリティリスクを

著作権法により無断での複製，転載等は禁止されております。