JIS

情報技術－セキュリティ技術－
情報セキュリティマネジメントシステム－
要求事項

JIS Q 27001：2014

（ISO/IEC 27001：2013）

（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）

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。

目　次

ページ
0　序文 1
0.1　概要 1
0.2　他のマネジメントシステム規格との両立性 1
1　適用範囲 2
2　引用規格 2
3　用語及び定義 2
4　組織の状況 2
4.1　組織及びその状況の理解 2
4.2　利害関係者のニーズ及び期待の理解 2
4.3　情報セキュリティマネジメントシステムの適用範囲の決定 2
4.4　情報セキュリティマネジメントシステム 3
5　リーダーシップ 3
5.1　リーダーシップ及びコミットメント 3
5.2　方針 3
5.3　組織の役割，責任及び権限 3
6　計画 4
6.1　リスク及び機会に対処する活動 4
6.2　情報セキュリティ目的及びそれを達成するための計画策定 5
7　支援 6
7.1　資源 6
7.2　力量 6
7.3　認識 6
7.4　コミュニケーション 6
7.5　文書化した情報 6
8　運用 7
8.1　運用の計画及び管理 7
8.2　情報セキュリティリスクアセスメント 7
8.3　情報セキュリティリスク対応 7
9　パフォーマンス評価 8
9.1　監視，測定，分析及び評価 8
9.2　内部監査 8
9.3　マネジメントレビュー 8
10　改善 9
10.1　不適合及び是正処置 9
10.2　継続的改善 9

Q 27001：2014 (ISO/IEC 27001：2013) 目次

ページ
附属書 A（規定）管理目的及び管理策 ……10
参考文献 ……21
解　説 ……22

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 27001**: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。

白　　紙

日本工業規格　　JIS
Q 27001：2014
(ISO/IEC 27001：2013)

情報技術－セキュリティ技術－
情報セキュリティマネジメントシステム－要求事項

Information technology—Security techniques—
Information security management systems—Requirements

0　序文

この規格は，2013 年に第 2 版として発行された **ISO/IEC 27001** 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　概要

この規格は，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。ISMS の採用は，組織の戦略的決定である。組織の ISMS の確立及び実施は，その組織のニーズ及び目的，セキュリティ要求事項，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全ては，時間とともに変化することが見込まれる。

ISMS 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情報の機密性，完全性及び可用性を維持し，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。

ISMS を，組織のプロセス及びマネジメント構造（management structure）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情報セキュリティを考慮することは，重要である。ISMS 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，組織自身の情報セキュリティ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も，また，外部関係者が評価するためにも用いることができる。

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されている。

ISO/IEC 27000[1)]は，ISMS ファミリ規格（**ISO/IEC 27003**[2]，**ISO/IEC 27004**[3]及び **ISO/IEC 27005**[4]を含む。）を参照しながら，ISMS の概要について記載し，用語及び定義について規定している。

注 [1)]　ISMS ファミリ規格の用語及び定義については，**JIS Q 27000** が制定されている。

0.2　他のマネジメントシステム規格との両立性

この規格は，ISO/IEC 専門業務用指針 第 1 部 統合版 ISO 補足指針の**附属書 SL** に規定する上位構造（HLS），共通の細分箇条題名，共通テキスト並びに共通の用語及び中核となる定義を適用しており，**附属書 SL** を採用した他のマネジメントシステム規格との両立性が保たれている。

附属書 SL に規定するこの共通の取組みは，二つ以上のマネジメントシステム規格の要求事項を満たす