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－用語

JIS Q 27000：2019

(JSA)

平成 31 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)

2019年7月1日の法改正により名称が変わりました。
まえがきを除き、本規格中の「日本工業規格」を「日本産業規格」に読み替えてください。

日本工業標準調査会標準第二部会 構成表

	氏名	所属
(部会長)	大　崎　博　之	東京大学
(委員)	青　柳　恵美子	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
	伊　藤　　智	一般社団法人情報処理学会情報規格調査会（国立研究開発法人新エネルギー・産業技術総合開発機構）
	岩　渕　幸　吾	一般社団法人電子情報技術産業協会
	内　田　富　雄	一般財団法人日本規格協会
	江　崎　　正	IEC/SMB 日本代表委員（ソニー株式会社）
	酒　井　祐　之	一般社団法人電気学会
	住　谷　淳　吉	一般財団法人電気安全環境研究所
	高　村　里　子	全国地域婦人団体連絡協議会
	田　中　一　彦	一般社団法人日本電機工業会
	橋　爪　　弘	一般社団法人ビジネス機械・情報システム産業協会
	平　田　真　幸	IEC/CAB 日本代表委員（富士ゼロックス株式会社）
	水　本　哲　弥	東京工業大学
	山　根　香　織	主婦連合会

主　務　大　臣：経済産業大臣　　制定：平成 26.3.20　　改正：平成 31.3.20
官　報　公　示：平成 31.3.20
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　標準第二部会（部会長　大崎　博之）

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　この規格の目的 1
0.3　この規格の内容 1
1　適用範囲 2
2　引用規格 2
3　用語及び定義 2
参考文献 13
附属書 JA（参考）JIS と対応国際規格との対比表 15
解　説 16
索　引 21

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 27000**: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。

日本工業規格　　JIS
Q 27000：2019

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－用語

Information technology—Security techniques—Information security management systems—Overview and vocabulary

0　序文

この規格は，2018 年に第 5 版として発行された **ISO/IEC 27000** を基とし，箇条 **3** の用語及び定義については技術的内容及び構成を変更することなく作成し，情報セキュリティマネジメントシステム（以下，ISMS という。）の概要などを示した箇条 **4** 以降を削除して編集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。変更の一覧表にその説明を付けて，**附属書 JA** に示す。

0.1　概要

マネジメントシステム規格は，マネジメントシステムの導入及び運用において従うモデルを提供する。このモデルは，当該分野の専門家が国際的に最新のものとして合意した特性を取り入れている。**ISO/IEC** JTC1（情報技術）/SC 27（セキュリティ技術）には，情報セキュリティのためのマネジメントシステム規格の開発を担当する作業グループがあり，それらの規格は，ISMS ファミリ規格とも呼ばれる。

ISMS ファミリ規格を用いることによって，組織は，財務情報，知的財産，従業員情報，及び顧客又は第三者から委託された情報を含む，情報資産のセキュリティを管理するための枠組みを策定し，実施することができる。また，これらの規格は，情報の保護に適用した，組織の ISMS について独立した評価のための準備に用いることもできる。

0.2　この規格の目的

ISMS ファミリ規格には，次の規格が含まれる。

a)　ISMS 及び ISMS を認証する機関に対する要求事項を規定する規格

b)　ISMS を確立し，実施し，維持し，改善するためのプロセス全体に関する直接的な支援，詳細な手引及び／又は解釈を提供する規格

c)　ISMS に関する分野固有の指針を取り扱う規格

d)　ISMS に関する適合性評価を取り扱う規格

0.3　この規格の内容

この規格では，次のような表現形式を用いる。

－　“～しなければならない（shall）”は，要求事項を示す。

－　“～することが望ましい（should）”は，推奨を示す。

－　“～してもよい（may）”は，許容を示す。
－　“～することができる”，“～できる”，“～し得る”など（can）は，可能性又は実現能力を示す。

“注記”に記載している情報は，関連する要求事項の内容を理解するための，又は明確にするための手引である。箇条 **3** に記載している“注記”は，用語上のデータを補足し，用語の使用に関連する規定を含むことがある追加情報を提供する。

1　適用範囲

この規格は，ISMS ファミリ規格で共通して用いている用語及び定義について規定する。この規格は，あらゆる形態及び規模の組織（例えば，営利企業，政府機関，非営利団体）に適用できる。

この規格で対象とする用語及び定義は，次のとおりである。

－ ISMS ファミリ規格で共通して用いている用語及び定義を対象とする。
－ ISMS ファミリ規格内で適用している全ての用語及び定義を対象としてはいない。
－ ISMS ファミリ規格において，新しい用語を定義することを制限するものではない。

注記 1　対応国際規格では，ISMS の概要に関する記載も含めて規定しているが，**JIS** では，これに該当する箇条を削除したため，標題及び適用範囲から ISMS の概要に関する記載を削除した。

注記 2　この規格の対応国際規格及びその対応の程度を表す記号を，次に示す。

ISO/IEC 27000:2018，Information technology － Security techniques － Information security management systems－Overview and vocabulary（MOD）

なお，対応の程度を表す記号“MOD”は，**ISO/IEC Guide 21-1** に基づき，“修正している”ことを示す。

2　引用規格

この規格に引用規格はない。

3　用語及び定義

ISO 及び **IEC** は，次の URL において，標準化に用いる用語上データベースを維持する。

－ ISO Online browsing platform：https://www.iso.org/obp
－ IEC Electropedia：https://www.electropedia.org/

3.1

アクセス制御（access control）

資産へのアクセスが，事業上及びセキュリティ要求事項（**3.56**）に基づいて認可及び制限されることを確実にする手段。

3.2

攻撃（attack）

資産の破壊，暴露，改ざん，無効化，盗用，又は認可されていないアクセス若しくは使用の試み。

3.3

監査（audit）

監査基準が満たされている程度を判定するために，監査証拠を収集し，それを客観的に評価するための，体系的で，独立し，文書化したプロセス（**3.54**）。

注記 1　監査は，内部監査（第一者）若しくは外部監査（第二者・第三者）のいずれでも，又は複合

監査（複数の分野の組合せ）でもあり得る。

注記 2　内部監査は，その組織自体が行うか又はその組織の代理で外部関係者が行う。

注記 3　“監査証拠”及び“監査基準”は，**JIS Q 19011** に定義されている。

3.4

監査範囲（audit scope）

監査（**3.3**）の及ぶ領域及び境界。

（**JIS Q 19011**:2012 の **3.14** を変更。**注記**を削除した。）

3.5

認証（authentication）

エンティティの主張する特性が正しいという保証の提供。

注記　エンティティは，“実体”，“主体”などともいう。情報セキュリティの文脈においては，情報を使用する組織及び人，情報を扱う設備，ソフトウェア及び物理的媒体などを意味する。

3.6

真正性（authenticity）

エンティティは，それが主張するとおりのものであるという特性。

3.7

可用性（availability）

認可されたエンティティが要求したときに，アクセス及び使用が可能である特性。

3.8

基本測定量（base measure）

単一の属性とそれを定量化するための方法とで定義した測定量（**3.42**）。

注記　基本測定量は，他の測定量と機能的に独立した測定量をいう。

（**ISO/IEC/IEEE 15939**:2017 の **3.3** を変更。**注記 2** を削除した。）

3.9

力量（competence）

意図した結果を達成するために，知識及び技能を適用する能力。

3.10

機密性（confidentiality）

認可されていない個人，エンティティ又はプロセス（**3.54**）に対して，情報を使用させず，また，開示しない特性。

3.11

適合（conformity）

要求事項（**3.56**）を満たしていること。

3.12

結果（consequence）

目的（**3.49**）に影響を与える事象（**3.21**）の結末（outcome）。

注記 1　一つの事象が，様々な結果につながることがある。

注記 2　結果は，確かなことも不確かなこともある。情報セキュリティの文脈において，結果は，通常，好ましくないものである。

注記 3　結果は，定性的にも定量的にも表現されることがある。

注記 4　初期の結果が，連鎖によって，段階的に増大することがある。

（**JIS Q 0073**:2010 の **3.6.1.3** を変更。**注記 2** の“不確かなこともあり，目的に対し…”以降を変更した。）

3.13

継続的改善（continual improvement）

パフォーマンス（**3.52**）を向上するために繰り返し行われる活動。

3.14

管理策（control）

リスク（**3.61**）を修正（modifying）する対策。

注記 1　管理策には，リスク（**3.61**）を修正するためのあらゆるプロセス（**3.54**），方針（**3.53**），仕掛け，実務及びその他の処置を含む。

注記 2　管理策が，常に意図又は想定した修正効果を発揮するとは限らない。

（**JIS Q 0073**:2010 の **3.8.1.1** 参照）

3.15

管理目的（control objective）

管理策（**3.14**）を実施した結果として，達成することを求められる事項を記載したもの。

3.16

修正（correction）

検出された不適合（**3.47**）を除去するための処置。

3.17

是正処置（corrective action）

不適合（**3.47**）の原因を除去し，再発を防止するための処置。

3.18

導出測定量（derived measure）

複数の基本測定量（**3.8**）の値の関数として定義した測定量（**3.42**）。

（**ISO/IEC/IEEE 15939**:2017 の **3.8** を変更。**注記 1** を削除した。）

3.19

文書化した情報（documented information）

組織（**3.50**）が管理し，維持するよう要求されている情報，及びそれが含まれている媒体。

注記 1　文書化した情報は，あらゆる形式及び媒体の形をとることができ，あらゆる情報源から得ることができる。

注記 2　文書化した情報には，次に示すものがあり得る。

- 関連するプロセス（**3.54**）を含むマネジメントシステム（**3.41**）
- 組織（**3.50**）の運用のために作成された情報（文書類）
- 達成された結果の証拠（記録）

3.20

有効性（effectiveness）

計画した活動を実行し，計画した結果を達成した程度。

3.21

事象（event）

ある一連の周辺状況の出現又は変化。

注記 1　事象は，発生が一度以上であることがあり，幾つかの原因をもつことがある。

注記 2　事象は，何かが起こらないことを含むことがある。

注記 3　事象は，“事態（incident）”又は“事故（accident）”と呼ばれることがある。

なお，“事態”は，“インシデント”とも表現される。

（**JIS Q 0073**:2010 の **3.5.1.3** を変更。**注記 4** を削除した。）

3.22

外部状況（external context）

組織が自らの目的（**3.49**）を達成しようとする場合の外部環境。

注記　外部状況には，次の事項を含むことがある。

- 国際，国内，地方又は近隣地域を問わず，文化，社会，政治，法律，規制，金融，技術，経済，自然及び競争の環境
- 組織（**3.50**）の目的に影響を与える主要な原動力及び傾向
- 外部ステークホルダー（**3.37**）との関係並びに外部ステークホルダーの認知及び価値観

（**JIS Q 0073**:2010 の **3.3.1.1** 参照）

3.23

情報セキュリティガバナンス（governance of information security）

組織（**3.50**）の情報セキュリティ（**3.28**）活動を指導し，管理するシステム。

注記　これは，**JIS Q 27014**:2015 における用語及び定義である。

3.24

経営陣（governing body）

組織（**3.50**）のパフォーマンス（**3.52**）及び適合性について説明責任を負う個人又はグループ。

注記 1　経営陣は，法域によっては，取締役会でもあり得る。

注記 2　これは，**JIS Q 27014**:2015 における用語及び定義である。

3.25

指標（indicator）

見積り又は評価を示す測定量（**3.42**）。

3.26

情報ニーズ（information need）

目的（**3.49**），目標，リスク及び問題点を管理するために必要となる見解。

（**ISO/IEC/IEEE 15939**:2017 の **3.12** 参照）

3.27

情報処理施設，情報処理設備（information processing facilities）

あらゆる情報処理のシステム，サービス若しくは基盤，又はこれらを収納する物理的場所。

3.28

情報セキュリティ（information security）

情報の機密性（**3.10**），完全性（**3.36**）及び可用性（**3.7**）を維持すること。

注記　さらに，真正性（**3.6**），責任追跡性，否認防止（**3.48**），信頼性（**3.55**）などの特性を維持することを含めることもある。

3.29

情報セキュリティ継続（information security continuity）

継続した情報セキュリティ（**3.28**）の運用を確実にするためのプロセス（**3.54**）及び手順。

3.30

情報セキュリティ事象（information security event)

情報セキュリティ（**3.28**）方針（**3.53**）への違反若しくは管理策（**3.14**）の不具合の可能性，又はセキュリティに関係し得る未知の状況を示す,システム,サービス若しくはネットワークの状態に関連する事象。

3.31

情報セキュリティインシデント（information security incident）

望まない単独若しくは一連の情報セキュリティ事象（**3.30**），又は予期しない単独若しくは一連の情報セキュリティ事象であって，事業運営を危うくする確率及び情報セキュリティ（**3.28**）を脅かす確率が高いもの。

3.32

情報セキュリティインシデント管理（information security incident management）

情報セキュリティインシデント（**3.31**）を検出し，報告し，評価し，応対し，対処し，更にそこから学習するための一連のプロセス（**3.54**）。

3.33

ISMS 専門家［information security management system （ISMS） professional］

一つ又は複数のセキュリティマネジメントシステムプロセス（**3.54**）を確立し，実施し，維持し，継続的に改善する人。

3.34

情報共有コミュニティ（information sharing community）

情報を共有することに合意した組織（**3.50**）のグループ。

注記　組織は，個人であることもある。

3.35

情報システム（information system）

アプリケーション，サービス，IT 資産，又は情報を取り扱う他の構成要素等の組合せ。

3.36

完全性（integrity）

正確さ及び完全さの特性。

3.37

利害関係者（interested party）（**推奨用語**）

ステークホルダー（stakeholder）（**許容用語**）

ある決定事項若しくは活動に影響を与え得るか，その影響を受け得るか，又はその影響を受けると認識している，個人又は組織（**3.50**）。

3.38

内部状況（internal context）

組織（**3.50**）が自らの目的を達成しようとする場合の内部環境。

注記　内部状況には，次の事項を含むことがある。

－　統治，組織体制，役割及びアカウンタビリティ

- 方針（**3.53**），目的（**3.49**）及びこれらを達成するために策定された戦略
- 資源及び知識としてみた場合の能力［例えば，資本，時間，人員，プロセス（**3.54**），システム及び技術］
- 情報システム（**3.35**），情報の流れ及び意思決定プロセス（公式及び非公式の両方を含む。）
- 内部ステークホルダー（**3.37**）との関係並びに内部ステークホルダーの認知及び価値観
- 組織の文化
- 組織が採択した規格，指針及びモデル
- 契約関係の形態及び範囲

（**JIS Q 0073**:2010 の **3.3.1.2** 参照）

3.39

リスクレベル（level of risk）

結果（**3.12**）とその起こりやすさ（**3.40**）の組合せとして表現される，リスク（**3.61**）の大きさ。

（**JIS Q 0073**:2010 の **3.6.1.8** を変更）

3.40

起こりやすさ（likelihood）

何かが起こる可能性。

（**JIS Q 0073**:2010 の **3.6.1.1** を変更。**注記**を削除した。）

3.41

マネジメントシステム（management system）

方針（**3.53**），目的（**3.49**）及びその目的を達成するためのプロセス（**3.54**）を確立するための，相互に関連する又は相互に作用する，組織（**3.50**）の一連の要素。

注記 1　一つのマネジメントシステムは，単一又は複数の分野を取り扱うことができる。

注記 2　システムの要素には，組織の構造，役割及び責任，計画及び運用が含まれる。

注記 3　マネジメントシステムの適用範囲としては，組織全体，組織内の固有で特定された機能，組織内の固有で特定された部門，複数の組織の集まりを横断する一つ又は複数の機能，などがあり得る。

3.42

測定量（measure）

測定（**3.43**）の結果として値が割り当てられる変数。

（**ISO/IEC/IEEE 15939**:2017 の **3.15** を変更。**注記 1** を削除した。）

3.43

測定（measurement）

値を決定するプロセス（**3.54**）。

3.44

測定の関数（measurement function）

複数の基本測定量（**3.8**）を結合するために遂行するアルゴリズム又は計算。

（**ISO/IEC/IEEE 15939**:2017 の **3.20** 参照）

3.45

測定方法（measurement method）

特定の尺度に関して属性を定量化するために使う一連の操作の論理的な順序を一般的に記述したもの。

注記　測定方法の類型は，属性を定量化するために使う操作の性質による。これには，次の二つの類型がある。

－　主観的　人間の判断を含んだ定量化

－　客観的　数値的な規則に基づいた定量化

（**ISO/IEC/IEEE 15939**:2017 の **3.21** を変更。**注記 2** を削除した。）

3.46

監視（monitoring）

システム，プロセス（**3.54**）又は活動の状況を明確にすること。

注記　状況を明確にするために，点検，監督又は注意深い観察が必要な場合もある。

3.47

不適合（non-conformity）

要求事項（**3.56**）を満たしていないこと。

3.48

否認防止（non-repudiation）

主張された事象（**3.21**）又は処置の発生，及びそれらを引き起こしたエンティティを証明する能力。

3.49

目的（objective）

達成する結果。

注記 1　目的は，戦略的，戦術的又は運用的であり得る。

注記 2　目的は，様々な領域［例えば，財務，安全衛生，環境の到達点（goal）］に関連し得るものであり，様々な階層［例えば，戦略的レベル，組織全体，プロジェクト単位，製品ごと，プロセス（**3.54**）ごと］で適用できる。

注記 3　目的は，例えば，意図する成果，目的（purpose），運用基準など，別の形で表現することもできる。また，情報セキュリティ目的という表現の仕方もあり，さらに，同じような意味をもつ別の言葉［例えば，狙い（aim），到達点（goal），目標（target）］で表すこともできる。

注記 4　ISMS の場合，組織は，特定の結果を達成するため，情報セキュリティ方針と整合のとれた情報セキュリティ目的を設定する。

3.50

組織（organization）

自らの目的（**3.49**）を達成するため，責任，権限及び相互関係を伴う独自の機能をもつ，個人又は人々の集まり。

注記　組織という概念には，法人か否か，公的か私的かを問わず，自営業者，会社，法人，事務所，企業，当局，共同経営会社，非営利団体若しくは協会，又はこれらの一部若しくは組合せが含まれる。ただし，これらに限定されるものではない。

3.51

外部委託する（outsource）

ある組織の機能又はプロセス（**3.54**）の一部を外部の組織（**3.50**）が実施するという取決めを行う。

注記　外部委託した機能又はプロセスは，マネジメントシステムの適用範囲内にあるが，外部の組織は，マネジメントシステム（**3.41**）の適用範囲の外にある。

3.52

パフォーマンス（performance）

測定可能な結果。

注記 1　パフォーマンスは，定量的又は定性的な所見のいずれにも関連し得る。

注記 2　パフォーマンスは，活動，プロセス（**3.54**），製品（サービスを含む。），システム又は組織（**3.50**）の運営管理に関連し得る。

3.53

方針（policy）

トップマネジメント（**3.75**）によって正式に表明された組織（**3.50**）の意図及び方向付け。

3.54

プロセス（process）

インプットをアウトプットに変換する，相互に関連する又は相互に作用する一連の活動。

3.55

信頼性（reliability）

意図する行動と結果とが一貫しているという特性。

3.56

要求事項（requirement）

明示されている，通常暗黙のうちに了解されている又は義務として要求されている，ニーズ又は期待。

注記 1　“通常暗黙のうちに了解されている”とは，対象となるニーズ又は期待が暗黙のうちに了解されていることが，組織及び利害関係者にとって，慣習又は慣行であることを意味する。

注記 2　規定要求事項とは，例えば，文書化した情報の中で明示されている要求事項をいう。

3.57

残留リスク（residual risk）

リスク対応（**3.72**）後に残っているリスク（**3.61**）。

注記 1　残留リスクには，特定されていないリスクが含まれ得る。

注記 2　残留リスクは，“保有リスク”ともいう。

3.58

レビュー（review）

確定された目的（**3.49**）を達成するため，対象となる事柄の適切性，妥当性及び有効性（**3.20**）を決定するために実行される活動。

（**JIS Q 0073**:2010 の **3.8.2.2** を変更。**注記**を削除した。）

3.59

レビュー対象物（review object）

レビュー（**3.58**）される特定のもの。

3.60

レビュー目的（review objective）

レビュー（**3.58**）の結果として何を達成するのかを説明したもの。

3.61

リスク（risk）

目的（**3.49**）に対する不確かさの影響。

注記 1　影響とは，期待されていることから，好ましい方向又は好ましくない方向にかい（乖）離することをいう。

注記 2　不確かさとは，事象，その結果又はその起こりやすさに関する，情報，理解又は知識に，たとえ部分的にでも不備がある状態をいう。

注記 3　リスクは，起こり得る“事象”（**JIS Q 0073**:2010 の **3.5.1.3** の定義を参照），“結果”（**JIS Q 0073**:2010 の **3.6.1.3** の定義を参照），又はこれらの組合せについて述べることによって，その特徴を示すことが多い。

注記 4　リスクは，ある“事象”（その周辺状況の変化を含む。）の結果とその発生の“起こりやすさ”（**JIS Q 0073**:2010 の **3.6.1.1** の定義を参照）との組合せとして表現されることが多い。

注記 5　ISMS の文脈においては，情報セキュリティリスクは，情報セキュリティ目的に対する不確かさの影響として表現することがある。

注記 6　情報セキュリティリスクは，脅威が情報資産のぜい弱性又は情報資産グループのぜい弱性に付け込み，その結果，組織に損害を与える可能性に伴って生じる。

3.62

リスク受容（risk acceptance）

ある特定のリスク（**3.61**）をとるという情報に基づいた意思決定。

注記 1　リスク対応（**3.72**）を実施せずにリスク受容となることも，又はリスク対応プロセス（**3.54**）中にリスク受容となることもある。

注記 2　受容されたリスクは，監視（**3.46**）及びレビュー（**3.58**）の対象となる。

（**JIS Q 0073**:2010 の **3.7.1.6** 参照）

3.63

リスク分析（risk analysis）

リスク（**3.61**）の特質を理解し，リスクレベル（**3.39**）を決定するプロセス（**3.54**）。

注記 1　リスク分析は，リスク評価（**3.67**）及びリスク対応（**3.72**）に関する意思決定の基礎を提供する。

注記 2　リスク分析は，リスクの算定を含む。

（**JIS Q 0073**:2010 の **3.6.1** 参照）

3.64

リスクアセスメント（risk assessment）

リスク特定（**3.68**），リスク分析（**3.63**）及びリスク評価（**3.67**）のプロセス（**3.54**）全体。

（**JIS Q 0073**:2010 の **3.4.1** 参照）

3.65

リスクコミュニケーション及び協議（risk communication and consultation）

リスク（**3.61**）の運用管理について，情報の提供，共有又は取得，及びステークホルダー（**3.37**）との対話を行うために，組織が継続的に及び繰り返し行う一連のプロセス（**3.54**）。

注記 1　情報は，リスクの存在，特質，形態，起こりやすさ（**3.40**），重大性，評価，受容可能性及び対応に関係することがある。

注記 2　協議とは，ある事柄に関する意思決定又は方向性の決定に先立って，組織（**3.50**）とそのステークホルダーとの間で行われる，その事柄についての情報に基づいたコミュニケーションの双方向プロセスである。協議とは，次のようなものである。

－　権力によってではなく，影響力によって，意思決定に影響を与えるプロセスである。
－　共同で意思決定を行うことではなく，意思決定に対するインプットとなる。

3.66

リスク基準（risk criteria）

リスク（**3.61**）の重大性を評価するための目安とする条件。

注記 1　リスク基準は，組織の目的，外部状況（**3.22**）及び内部状況（**3.38**）に基づいたものである。

注記 2　リスク基準は，規格，法律，方針（**3.53**）及びその他の要求事項（**3.56**）から導き出されることがある。

（**JIS Q 0073**:2010 の **3.3.1.3** 参照）

3.67

リスク評価（risk evaluation）

リスク（**3.61**）及び／又はその大きさが受容可能か又は許容可能かを決定するために，リスク分析（**3.63**）の結果をリスク基準（**3.66**）と比較するプロセス（**3.54**）。

注記　リスク評価は，リスク対応（**3.72**）に関する意志決定を手助けする。

（**JIS Q 0073**:2010 の **3.7.1** 参照）

3.68

リスク特定（risk identification）

リスク（**3.61**）を発見，認識及び記述するプロセス（**3.54**）。

注記 1　リスク特定には，リスク源，事象（**3.21**），それらの原因及び起こり得る結果（**3.12**）の特定が含まれる。

注記 2　リスク特定には，過去のデータ，理論的分析，情報に基づいた意見，専門家の意見及びステークホルダー（**3.37**）のニーズを含むことがある。

（**JIS Q 0073**:2010 の **3.5.1** 参照）

3.69

リスクマネジメント（risk management）

リスク（**3.61**）について，組織（**3.50**）を指揮統制するための調整された活動。

（**JIS Q 0073**:2010 の **2.1** 参照）

3.70

リスクマネジメントプロセス（risk management process）

コミュニケーション，協議及び組織の状況の確定の活動，並びにリスク（**3.61**）の特定，分析，評価，対応，監視及びレビューの活動に対する，運用管理方針（**3.53**），手順及び実務の体系的な適用。

注記　**ISO/IEC 27005** においては，リスクマネジメント全体を示すために“プロセス”（**3.54**）という用語を用いている。リスクマネジメント（**3.69**）プロセス内の要素は，“活動（activities）”と呼ばれる。

（**JIS Q 0073**:2010 の **3.1** を変更。**注記**を追加した。）

3.71

リスク所有者（risk owner）

リスク（**3.61**）を運用管理することについて，アカウンタビリティ及び権限をもつ人又は主体。

（**JIS Q 0073**:2010 の **3.5.1.5** 参照）

3.72

リスク対応（risk treatment）

リスク（**3.61**）を修正するプロセス（**3.54**）。

注記 1　リスク対応には，次の事項を含むことがある。

- リスクを生じさせる活動を，開始又は継続しないと決定することによって，リスクを回避すること
- ある機会を追求するために，リスクをとる又は増加させること
- リスク源を除去すること
- 起こりやすさ（**3.40**）を変えること
- 結果（**3.12**）を変えること
- 一つ以上の他者とリスクを共有すること（契約及びリスクファイナンシングを含む。）
- 情報に基づいた選択によって，リスクを保有すること

注記 2　好ましくない結果に対処するリスク対応は，“リスク軽減”，“リスク排除”，“リスク予防”及び“リスク低減”と呼ばれることがある。

注記 3　リスク対応が，新たなリスクを生み出したり，又は既存のリスクを修正したりすることがある。

（**JIS Q 0073**:2010 の **3.8.1** を変更。**注記 1** の“意思決定”を“選択”に置き換えた。）

3.73

セキュリティ実施標準（security implementation standard）

セキュリティを実現するための認可された方法を規定した文書。

3.74

脅威（threat）

システム又は組織（**3.50**）に損害を与える可能性がある，望ましくないインシデントの潜在的な原因。

3.75

トップマネジメント（top management）

最高位で組織（**3.50**）を指揮し，管理する個人又は人々の集まり。

注記 1　トップマネジメントは，組織内で，権限を委譲し，資源を提供する力をもっている。

注記 2　マネジメントシステム（**3.41**）の適用範囲が組織の一部だけの場合，トップマネジメントとは，組織内のその一部を指揮し，管理する人をいう。

注記 3　トップマネジメントは，ときに業務執行幹部（executive management）と呼ばれることもあり，最高経営責任者，最高財務責任者，最高情報責任者及び類似の役職が含まれることがある。

3.76

信頼できる情報コミュニケーションエンティティ（trusted information communication entity）

情報共有コミュニティ（**3.34**）内での情報交換を支援する，自立した組織（**3.50**）。

3.77

ぜい弱性（vulnerability）

一つ以上の脅威（**3.74**）によって付け込まれる可能性のある，資産又は管理策（**3.14**）の弱点。

参考文献

[1] **JIS Q 9000**:2015　品質マネジメントシステム－基本及び用語

注記　対応国際規格：**ISO 9000**:2015，Quality management systems－Fundamentals and vocabulary（IDT）

[2] **ISO/IEC/IEEE 15939**:2017，Systems and software engineering－Measurement process

[3] **JIS Q 17021**　適合性評価－マネジメントシステムの審査及び認証を行う機関に対する要求事項

注記　対応国際規格：**ISO/IEC 17021**，Conformity assessment－Requirements for bodies providing audit and certification of management systems（IDT）

[4] **JIS Q 19011**:2012　マネジメントシステム監査のための指針

注記　対応国際規格：**ISO 19011**:2011，Guidelines for auditing management systems（IDT）

[5] **JIS Q 20000-1**:2012　情報技術－サービスマネジメント－第 1 部：サービスマネジメントシステム要求事項

注記　対応国際規格：**ISO/IEC 20000-1**:2011，Information technology－Service management－Part 1: Service management system requirements（IDT）

[6] **JIS Q 27001**　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

注記　対応国際規格：**ISO/IEC 27001**, Information technology－Security techniques－Information security management systems－Requirements（IDT）

[7] **JIS Q 27002**　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

注記　対応国際規格：**ISO/IEC 27002**, Information technology－Security techniques－Code of practice for information security controls（IDT）

[8] **ISO/IEC 27003**，Information technology－Security techniques－Information security management systems－Guidance

[9] **ISO/IEC 27004**，Information technology－Security techniques－Information security management－Monitoring, measurement, analysis and evaluation

[10] **ISO/IEC 27005**，Information technology－Security techniques－Information security risk management

[11] **JIS Q 27006**　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の審査及び認証を行う機関に対する要求事項

注記　対応国際規格：**ISO/IEC 27006**，Information technology－Security techniques－Requirements for bodies providing audit and certification of information security management systems（IDT）

[12] **ISO/IEC 27007**，Information technology－Security techniques－Guidelines for information security management systems auditing

[13] **ISO/IEC TR 27008**，Information technology－Security techniques－Guidelines for auditors on information security controls

[14] **ISO/IEC 27009**，Information technology－Security techniques－Sector-specific application of ISO/IEC 27001－Requirements

[15] **ISO/IEC 27010**，Information technology－Security techniques－Information security management for inter-sector and inter-organizational communications

[16] **ISO/IEC 27011**，Information technology－Security techniques－Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations

[17] **ISO/IEC 27013**　Information technology－Security techniques－Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

[18] **JIS Q 27014**　情報技術－セキュリティ技術－情報セキュリティガバナンス

注記　対応国際規格：**ISO/IEC 27014,** Information technology－Security techniques－Governance of information security（IDT）

[19] **ISO/IEC TR 27016,** Information technology－Security techniques－Information security management－Organizational economics

[20] **JIS Q 27017**　情報技術－セキュリティ技術－JIS Q 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範

注記　対応国際規格：**ISO/IEC 27017,** Information technology－Security techniques－Code of practice for information security controls based on ISO/IEC 27002 for cloud services（IDT）

[21] **ISO/IEC 27018,** Information technology－Security techniques－Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

[22] **ISO/IEC 27019,** Information technology－Security techniques－Information security controls for the energy utility industry

[23] **ISO/IEC 27021,** Information technology－Security techniques－Competence requirements for information security management systems professionals

[24] **ISO 27799,** Health informatics－Information security management in health using ISO/IEC 27002

[25] **JIS Q 0073**:2010　リスクマネジメント－用語

注記　対応国際規格：**ISO Guide 73**:2009, Risk management－Vocabulary（IDT）

附属書 JA
（参考）
JIS と対応国際規格との対比表

JIS Q 27000:2019　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－用語	**ISO/IEC 27000**:2018，Information technology － Security techniques － Information security management systems－Overview and vocabulary

(I) **JIS** の規定		(II) 国際規格番号	(III) 国際規格の規定		(IV) **JIS** と国際規格との技術的差異の箇条ごとの評価及びその内容		(V) **JIS** と国際規格との技術的差異の理由及び今後の対策
箇条番号及び題名	内容		箇条番号	内容	箇条ごとの評価	技術的差異の内容	
1 適用範囲	ISMS ファミリ規格の用語及び定義		1	ISMS の概要並びに ISMS ファミリ規格の用語及び定義	変更	**JIS** では，ISMS の概要に関する記載を削除した。	ISMS 及び ISMS ファミリ規格の概要に該当する対応国際規格の箇条 4 及び箇条 5 は，参考情報を提供するもので **JIS** として規定する必要性が認められず，削除したため。
2 引用規格							
3 用語及び定義			3		一致		
－	－		4	ISMS の概要	削除	－	この箇条の内容は，参考情報を提供するもので **JIS** として規定する必要性が認められないため。
－	－		5	ISMS ファミリ規格の概要	削除	－	この箇条の内容は，参考情報を提供するもので **JIS** として規定する必要性が認められないため。

JIS と国際規格との対応の程度の全体評価：**ISO/IEC 27000**:2018，MOD

注記 1　箇条ごとの評価欄の用語の意味は，次による。
- －　一致 ……技術的差異がない。
- －　削除 ……国際規格の規定項目又は規定内容を削除している。
- －　変更 ……国際規格の規定内容を変更している。

注記 2　**JIS** と国際規格との対応の程度の全体評価欄の記号の意味は，次による。
- －　MOD ……国際規格を修正している。

JIS Q 27000：2019

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－用語
解　説

この解説は，規格に規定・記載した事柄を説明するもので，規格の一部ではない。

この解説は，日本規格協会が編集・発行するものであり，これに関する問合せ先は日本規格協会である。

1　制定の趣旨

1.1　ISO/IEC 27000 の制定及び改正の趣旨

ISO/IEC 27000 の第 1 版制定の趣旨は，情報セキュリティマネジメントシステム（以下，ISMS という。）ファミリ規格で共通して使用する用語及び定義を提供すること，また，ISMS ファミリ規格に対するユーザーの関心を広く得るためのマーケティング文書となるような概要書を提供することの 2 点であった。

第 2 版への改正の趣旨は，第 1 版制定以後に発行された ISMS ファミリ規格において定義された用語のうち，ISMS ファミリ規格において共通して使用される用語及び定義を記載することであった。第 2 版の改正作業中に，第 2 版発行後に直ちに第 3 版への改正作業が開始されることが既に決定していたため，第 2 版への改正は，上記の内容に限定された。

第 3 版への改正の趣旨は，**ISO/IEC 27001**:2013 及び **ISO/IEC 27002**:2013 の用語及び定義を記載することであった。これら 2 規格は，**ISO/IEC 27000** を引用規格とし，自身の規格中には用語及び定義を規定しないため，これら 2 規格と時期を同じくしての発行が，第 3 版においては最重要事項とされた。

第 4 版及び第 5 版への改正の趣旨は，第 2 版への改正の趣旨と同様に，前の版制定以後に発行された ISMS ファミリ規格において定義された用語のうち，ISMS ファミリ規格において共通して使用される用語及び定義を記載すること，及び概要部分に発行された規格に関する情報を反映することであった。

1.2　JIS Q 27000 の制定の趣旨

この規格は，ISMS ファミリ規格，特に **JIS Q 27001**:2014 及び **JIS Q 27002**:2014 の用語及び定義を規定する規格として **ISO/IEC 27000**:2014 を基に制定された。**ISO/IEC 27000**:2014 は，用語及び定義に加え，ユーザーの関心を広く得ることを目的としたマーケティング文書として，ISMS の概要についても示しているが，これらの内容は参考情報であること，並びに解説の **2.1** に示す制定及び改正の経緯から国際での議論が不十分な内容もあることから，該当する箇条以降は削除し，**JIS** には含めなかった。一方，用語及び定義については，**ISO/IEC 27000**:2014 と一致させるために，技術的内容を変更することなく作成した。

第 5 版にあたる **ISO/IEC 27000**:2018（以下，対応国際規格という。）は，先の版から用語の定義が多く修正されたため，対応する **JIS Q 27000** についても改正を行った。ただし，**JIS Q 27001**:2014 及び **JIS Q 27002**:2014 の用語及び定義に変更はない。

2　制定の経緯

2.1　ISO/IEC 27000 の制定及び改正の経緯

対応国際規格の制定及び改正の経緯を，次に示す。

a)　第 1 版の制定　**ISO/IEC 27000** の制定活動は，**ISO**（国際標準化機構）及び **IEC**（国際電気標準会議）の設置する **ISO/IEC JTC1**（情報技術）/**SC27**（セキュリティ技術）/**WG 1**（情報セキュリティマネジメントシステム）が担当した。

制定活動は，2005 年 4 月のウィーン会合において，**ISO/IEC 13335-1**，Information technology－Security techniques－Management of information and communications technology security－Part 1: Concepts and models for information and communications technology security management の適用範囲を見直す研究期間（Study Period）の開始が合意されたことに始まる。研究の結論として，ISMS に関する規格が増えている状況において，これら ISMS ファミリ規格の調和を促進し，また，ファミリに含まれる規格の適用範囲についての十分な理解を促進するために，ISMS ファミリ規格の全体的な枠組み並びに ISMS ファミリ規格において共通して使用される用語及び定義のリストを作ることの必要性が確認された。

この結論に基づき，2006 年 1 月に新作業項目提案“Proposal for a new work item for Information security management system fundamentals and vocabulary”が提出され，投票の結果，スペイン，スウェーデン及び米国が反対したが，17 か国の賛成を得て，**ISO/IEC 27000** の開発が開始された。この開発プロジェクトには，我が国からも共同執筆者として参画した。

その後，2007 年 11 月の南アフリカ会合において，ISMS ファミリ規格の全体的な枠組みを示すという当初の目的が変更され，ISMS ファミリ規格に対するユーザーの関心を広く得るためのマーケティング文書とすることとなった。これに伴い，開発当初の規格名称（Information technology－Security techniques－Information security management systems fundamentals and vocabulary）の fundamentals が overview に変更となった。また，無償で配布する文書とすることについても合意された。

上記を経て，**ISO/IEC 27000** の第 1 版は，2009 年 5 月に制定された。

b)　第 2 版の発行　**ISO/IEC 27000** は，ISMS ファミリ規格で使用する用語及び定義を規定するため，新規に制定又は改正された ISMS ファミリ規格で規定された用語及び定義を，できるだけ早い周期で反映させることが必要となる。この考えに基づき，早期改正が必要と判断され，2009 年 11 月のレドモンド会合において，第 2 版発行に向けた改正プロジェクトを開始するか否かを問う投票を行うことを決定した。投票の結果，韓国だけが反対したが，その他 27 か国の賛成を得て，2010 年 4 月のマラッカ会合において改正プロジェクトが開始された。

活動を進める中で，**ISO/IEC 27000** の改正プロジェクト自体は，いずれの用語についても定義する権限をもたず，その権限は，各用語を使用する規格の開発又は改正プロジェクトが所有することが確認された。また，一つの用語を複数の規格が使用する場合には，その用語を主に定義する規格の開発又は改正プロジェクトを，その用語の“所有者（Owner）”とし，その他の規格の開発又は改正プロジェクトは，“影響を被るプロジェクト（Impacted Project）”とすることになった。例えば，“リスク（risk）”という用語については，**ISO/IEC 27001** の改正プロジェクトが所有者となり，**ISO/IEC 27005** が影響を被るプロジェクトとなった。これは，**ISO/IEC 27001** が要求事項を定める規格であるため，**ISO/IEC 27005** より優先して用語を定義すべきとの考えによって決定された。このようにして定められた各所有者が各用語の定義を確定し，第 2 版は，2012 年 12 月に発行された。

c)　第 3 版の発行　第 2 版の作成が進められていた一方，2008 年 10 月のキプロス会合から開始されていた **ISO/IEC 27001** 及び **ISO/IEC 27002** の改正プロジェクトにおいて，**ISO/IEC 27000** を引用規格とし，

用語の定義は全て **ISO/IEC 27000** に規定することが確定された。すなわち，従来，**ISO/IEC 27001** 及び **ISO/IEC 27002** の中で必要な用語を定義していたが，これらの規格中では，用語及び定義を個別に規定しないことになった。これを受けて，**ISO/IEC 27000** を **ISO/IEC 27001** 及び **ISO/IEC 27002** と同時期に改正する必要性が認識され，2011 年 4 月のシンガポール会合で改正作業の開始に合意した。

第 2 版が 2012 年 12 月に発行されてから，第 3 版を発行するまでの期間が限られていたため，改正の目的は，当時改正作業中だった **ISO/IEC 27001**:2013 及び **ISO/IEC 27002**:2013 の用語を記載することに絞られた。その結果，2013 年 10 月付で発行された **ISO/IEC 27001** 及び **ISO/IEC 27002** より 3 か月遅れて，**ISO/IEC 27000** の第 3 版が発行された。

d) **第 4 版の発行**　第 4 版発行に向けた改正プロジェクトは，2015 年 4 月のクチン会合にて開始された。主に第 3 版の編集上の誤りを正すことを目的に限定的な改正を行うこととした。概要部で引用されている **ISO/IEC 27000** ファミリ規格のタイトルが違っている，ある用語の定義に，本国際規格で定義されている用語が使用されている場合に，当該用語を定義する細分箇条番号が付されていないなどの誤りを修正することが目的とされた。誤りは各々を見ると大きな問題ではないが，誤り箇所が多かったため，規格全体の品質を下げていると判断し，改訂が行われた。

なお，本改訂においては，用語の新規追加や定義内容の変更などは発生しなかった。

e) **第 5 版の発行**　第 5 版発行に向けた改正プロジェクトは，2017 年春のハミルトン会合で開始された。**ISO/IEC 27001**:2013 に対応した **ISO/IEC 27003**:2017 及び **ISO/IEC 27004**:2016 の改訂，**ISO/IEC 27021**:2017 の新規発行に伴い，ISMS ファミリ規格で共通的に使用される用語の見直しが行われたことによる。特に **ISO/IEC 27004**:2009 の用語については，**ISO/IEC 27004** に固有であり，ISMS ファミリ規格での共通的な使用に相当しないものが多く **ISO/IEC 27000** に記載されており，誤解を生じないように **ISO/IEC 27004**:2009 固有の用語である旨の注記を入れるなどの対応をしていた。**ISO/IEC 27004**:2016 の改訂に伴い，こうした用語の削除や変更が行われた。

2.2　JIS Q 27000 の制定の経緯

ISO/IEC 27000 の第 1 版及び第 2 版は **JIS** 化されていない。しかし，解説の **2.1 c)** にも記載したとおり，**ISO/IEC 27000** の第 3 版が，**ISO/IEC 27001**:2013 及び **ISO/IEC 27002**:2013 の用語及び定義を記載することになり，これらの国際一致規格である **JIS Q 27001** 及び **JIS Q 27002** もこれに合わせて改正することから，**ISO/IEC 27000** の **JIS** 化が必要となった。このため，2013 年 3 月に，一般財団法人日本規格協会に情報セキュリティマネジメントシステム **JIS** 原案作成委員会を設置し，対応国際規格を基に **JIS** 原案を作成した。

ISO/IEC 27000 の第 4 版では用語の定義内容に変更がなかったことから，**JIS Q 27000**:2014 の改訂は行わなかった。第 5 版については，**JIS Q 27001** 及び **JIS Q 27002** に関する用語については変更がなかったものの，解説の **2.1 e)** にも記載したとおり，**ISO/IEC 27004** に関する用語を主に，多くの用語が修正されたことから 2018 年 6 月に，対応国際規格を基に **JIS** 原案の改正作業を実施した。

3　審議中に特に問題となった事項

3.1　対応国際規格の審議中に特に問題となった事項

対応国際規格の改正作業で特に問題となった事項はない。

3.2　JIS Q 27000 の審議中に問題となった事項

翻訳作業段階で議論になった表現の解釈及び／又は採用した訳を，次に示す。

a) **外部関係者（external party）（3.3 の注記 2）**　**ISO/IEC** 業務指針第 1 部の**附属書 SL**（Annex SL）の表現に合わせ，“外部関係者”の訳をあてた。

b) **管理策（control）（3.14 の注記 2）の定義**　対応国際規格では，“it is possible that”（～する可能性がある）が加わったが，すでに“～するとは限らない”という限定を含む定義になっていたため，この箇所は訳さず従来どおりのままとした。

c) **情報セキュリティガバナンス（governance of information security）（3.23）**　**JIS Q 27014** の用語及び定義であるため，その旨注記に加えた。

d) **情報システム（information system）（3.35）の定義**　“set of～”の訳に関して，“一連の”という訳があげられたが，“or（又は）”の訳を正しく理解するため，文末に“～等の組合せ”を追加することとした。

e) **業務執行幹部（executive management）（3.75 の注記 3）**　**JIS Q 27014** と整合させた。

4　規定項目の内容

ISMS ファミリ規格で共通して用いる用語及び定義について，箇条 **3** に規定している。対応国際規格では，種類又は性質による用語の分類は行わず，全ての用語をアルファベット順に並べており，この規格においても，その順番を変えていない。

ここで，解説の **2.1 c)** にも記載したとおり，**ISO/IEC 27001**:2013 及び **ISO/IEC 27002**:2013 は，自身の中には用語及び定義をもたず，全て対応国際規格に規定している。この規格に規定している用語のうち，**ISO/IEC 27001** 及び **ISO/IEC 27002** の用語について，次に示す。

a) **ISO/IEC 27001:2013 の用語**　**ISO/IEC 27001** の用語は，次の三つに分類される。

1) **情報セキュリティに関する用語**　ISMS ファミリ規格において用いる用語を定義するものである。

2) **リスクマネジメントに関する用語**　**ISO/IEC 27001**:2013 のリスクマネジメントに関する要求事項は，**ISO 31000**:2009 と整合を保ち規定されている。したがって，対応国際規格では，リスクマネジメントに関する用語については **ISO 31000**:2009 の用語に関する引用規格である **ISO Guide 73**:2009 の用語を引用した。**ISO Guide 73**:2009 の国際一致規格として **JIS Q 0073**:2010 が制定されており，この規格では，**JIS Q 0073** の用語及び定義を引用した。

3) **マネジメントシステムに関する用語**　**ISO/TMB**（技術管理評議会）/**TAG13**（専門諮問グループ）**JTCG**（合同技術調整グループ）において，**ISO** における全てのマネジメントシステム規格（Management System Standards：MSS）の整合性を確保するための検討が行われ，MSS の上位構造，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が開発された。開発結果は，**ISO/IEC** 専門業務用指針 第 1 部 統合版 **ISO** 補足指針に**附属書 SL** として含められており，対応国際規格では，この**附属書 SL** で定められた共通用語を引用している。**附属書 SL** については，**ISO/TMB/TAG** 対応国内委員会が共通和訳を作成しており，この規格では，この共通和訳に定められた用語及び定義を引用した。

なお，原則，**附属書 SL** 及びその共通和訳をそのまま引用しているが，情報セキュリティの文脈において修正が必要な場合には，修正を加えた。具体的には，“risk”の定義において，対応国際規格は，**附属書 SL** の定義ではなく，**ISO Guide 73** の定義を引用している。これは，解説の箇条 **4 a) 2)** にも記載したとおり，**ISO Guide 73** が **ISO 31000** の用語を規定しており，情報セキュリティの文脈において，**ISO 31000** との整合をより重視した結果である。これに沿って，この規格も“リスク（risk）”の定義は，**JIS Q 0073** の定義を引用した。

b) **ISO/IEC 27002:2013 の用語**　**ISO/IEC 27002**:2013 の改正の主たる目的が，**ISO/IEC 27002**:2005 からの継続性の確保，組織における技術及び環境の変化への対応，及び規格の使いやすさの改善であったこ

とから，**ISO/IEC 27001**:2013 の用語とは異なり，情報セキュリティに特化した用語のリストとなっている。

5　懸案事項

対応国際規格は，**ISO/IEC 27001**:2013 及び **ISO/IEC 27002**:2013 の用語及び定義だけでなく，ISMS ファミリ規格で共通して使用する用語及び定義を記載することを目的としている。これに対応して，国際会合では，ISMS ファミリ規格で使用する用語をどのように管理するか，また，共通して使用する用語をどのように決めるかといった検討が継続的に進められている。しかし，ISMS ファミリ規格の広がりとともに扱う用語が増加していること，また，既存規格の改訂などに伴う見直しも多く発生することなどから，用語の管理に関する課題は非常に多い状況にある。

6　原案作成委員会の構成表

原案作成委員会の構成表を，次に示す。

情報セキュリティマネジメントシステム JIS 原案作成委員会　構成表

	氏名	所属
(委員長)	中　尾　康　二	国立研究開発法人情報通信研究機構
(委員)	相　羽　律　子	株式会社日立製作所
	畔　津　布　岐	一般財団法人日本情報経済社会推進協会
	中　村　良　和	日本マネジメントシステム認証機関協議会 (BSI グループジャパン株式会社)
	西　尾　秀　一	独立行政法人情報処理推進機構
	平　野　芳　行	IT・標準化コンサルタント
(関係者)	三　島　　崇	経済産業省産業技術環境局
	堀　坂　和　秀	経済産業省産業技術環境局
	四ツ釜　直　哉	経済産業省産業技術環境局
(事務局)	中　川　　梓	一般財団法人日本規格協会
	嶽　北　慎　子	一般財団法人日本規格協会
	石　川　茉　耶	一般財団法人日本規格協会

(執筆者　相羽 律子)

用語索引（五十音順）

用語	番号	英語
【あ】		
ISMS 専門家	3.33	information security management system (ISMS) professional
アクセス制御	3.1	access control
【お】		
起こりやすさ	3.40	likelihood
【か】		
外部委託する	3.51	outsource
外部状況	3.22	external context
可用性	3.7	availability
監査	3.3	audit
監査範囲	3.4	audit scope
監視	3.46	monitoring
完全性	3.36	integrity
管理策	3.14	control
管理目的	3.15	control objective
【き】		
基本測定量	3.8	base measure
機密性	3.10	confidentiality
脅威	3.74	threat
【け】		
経営陣	3.24	governing body
継続的改善	3.13	continual improvement
結果	3.12	consequence
【こ】		
攻撃	3.2	attack
【さ】		
残留リスク	3.57	residual risk
【し】		
事象	3.21	event
指標	3.25	indicator
修正	3.16	correction
情報共有コミュニティ	3.34	information sharing community
情報システム	3.35	information system
情報処理施設，情報処理設備	3.27	information processing facilities
情報セキュリティ	3.28	information security
情報セキュリティインシデント	3.31	information security incident
情報セキュリティインシデント管理	3.32	information security incident management
情報セキュリティガバナンス	3.23	governance of information security
情報セキュリティ継続	3.29	information security continuity
情報セキュリティ事象	3.30	information security event
情報ニーズ	3.26	information need
真正性	3.6	authenticity
信頼性	3.55	reliability
信頼できる情報コミュニケーションエンティティ	3.76	trusted information communication entity
【す】		
ステークホルダー	3.37	stakeholder
【せ】		
ぜい弱性	3.77	vulnerability
セキュリティ実施標準	3.73	security implementation standard
是正処置	3.17	corrective action
【そ】		
測定	3.43	measurement
測定の関数	3.44	measurement function
測定方法	3.45	measurement method
測定量	3.42	measure
組織	3.50	organization
【て】		
適合	3.11	conformity
【と】		
導出測定量	3.18	derived measure
トップマネジメント	3.75	top management
【な】		
内部状況	3.38	internal context
【に】		
認証	3.5	authentication
【は】		
パフォーマンス	3.52	performance
【ひ】		
否認防止	3.48	non-repudiation
【ふ】		
不適合	3.47	non-conformity
プロセス	3.54	process
文書化した情報	3.19	documented information
【ほ】		
方針	3.53	policy
【ま】		
マネジメントシステム	3.41	management system

用語	番号	英語
【も】		
目的	3.49	objective
【ゆ】		
有効性	3.20	effectiveness
【よ】		
要求事項	3.56	requirement
【り】		
利害関係者	3.37	interested party
力量	3.9	competence
リスク	3.61	risk
リスクアセスメント	3.64	risk assessment
リスク基準	3.66	risk criteria
リスクコミュニケーション及び協議	3.65	risk communication and consultation
リスク受容	3.62	risk acceptance
リスク所有者	3.71	risk owner
リスク対応	3.72	risk treatment
リスク特定	3.68	risk identification
リスク評価	3.67	risk evaluation
リスク分析	3.63	risk analysis
リスクマネジメント	3.69	risk management
リスクマネジメントプロセス	3.70	risk management process
リスクレベル	3.39	level of risk
【れ】		
レビュー	3.58	review
レビュー対象物	3.59	review object
レビュー目的	3.60	review objective

★**JIS** 規格票及び **JIS** 規格票解説についてのお問合せは，規格開発ユニット標準チームまで，電子メール（E-mail:sd@jsa.or.jp），又は **FAX**［(03)4231-8660］，**TEL**［(03)4231-8530］でお願いいたします。お問合せにお答えするには，関係先への確認等が必要なケースがございますので，多少お時間がかかる場合がございます。あらかじめご了承ください。

★**JIS** 規格票の正誤票が発行された場合は，次の要領でご案内いたします。

（**1**）当協会ホームページ（https://www.jsa.or.jp/）の Webdesk に，正誤票（PDF 版，ダウンロード可）を掲載いたします。

なお，当協会の **JIS** 予約者の方には，予約されている **JIS** の部門で正誤票が発行された場合，お送りいたします。

（**2**）当協会発行の月刊誌“標準化と品質管理”に，正・誤の内容を掲載いたします。

★**JIS** 規格票のご注文は，

（**1**）当協会ホームページ（https://www.jsa.or.jp/）の Webdesk をご利用ください。

（**2**）**FAX**［(03)4231-8665］でご注文の方は，出版情報ユニット販売サービスチームまで，お申込みください。

JIS Q 27000
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－用語

平成 31 年 3 月 20 日　　第 1 刷発行

編集兼
発行人　揖 斐 敏 夫

発 行 所

一般財団法人　日 本 規 格 協 会
〒108-0073　東京都港区三田 3 丁目 13-12 三田 MT ビル
https://www.jsa.or.jp/

名古屋支部　〒460-0008　名古屋市中区栄 2 丁目 6-1　RT 白川ビル内
TEL (052)221-8316(代表)　FAX (052)203-4806

関 西 支 部　〒541-0043　大阪市中央区高麗橋 3 丁目 2-7　ORIX 高麗橋ビル内
TEL (06)6222-3130(代表)　FAX (06)6222-3255

広 島 支 部　〒730-0011　広島市中区基町 5-44　広島商工会議所ビル内
TEL (082)221-7023　FAX (082)223-7568

福 岡 支 部　〒812-0025　福岡市博多区店屋町 1-31　博多アーバンスクエア内
TEL (092)282-9080　FAX (092)282-9118

Printed in Japan　NH

JAPANESE INDUSTRIAL STANDARD

Information technology—Security techniques—Information security management systems—Overview and vocabulary

JIS Q 27000：2019

（JSA）

Revised 2019-03-20

Investigated by

Japanese Industrial Standards Committee

Published by

Japanese Standards Association

Price Code 07

ICS 01.040.35;03.100.70;35.030

Reference number：JIS Q 27000:2019(**J**)