ISO/IEC 27000 ファミリー規格について

～ ISO/IEC JTC 1/SC 27/WG 1 における検討状況 ～

Contents

2022年7月22日

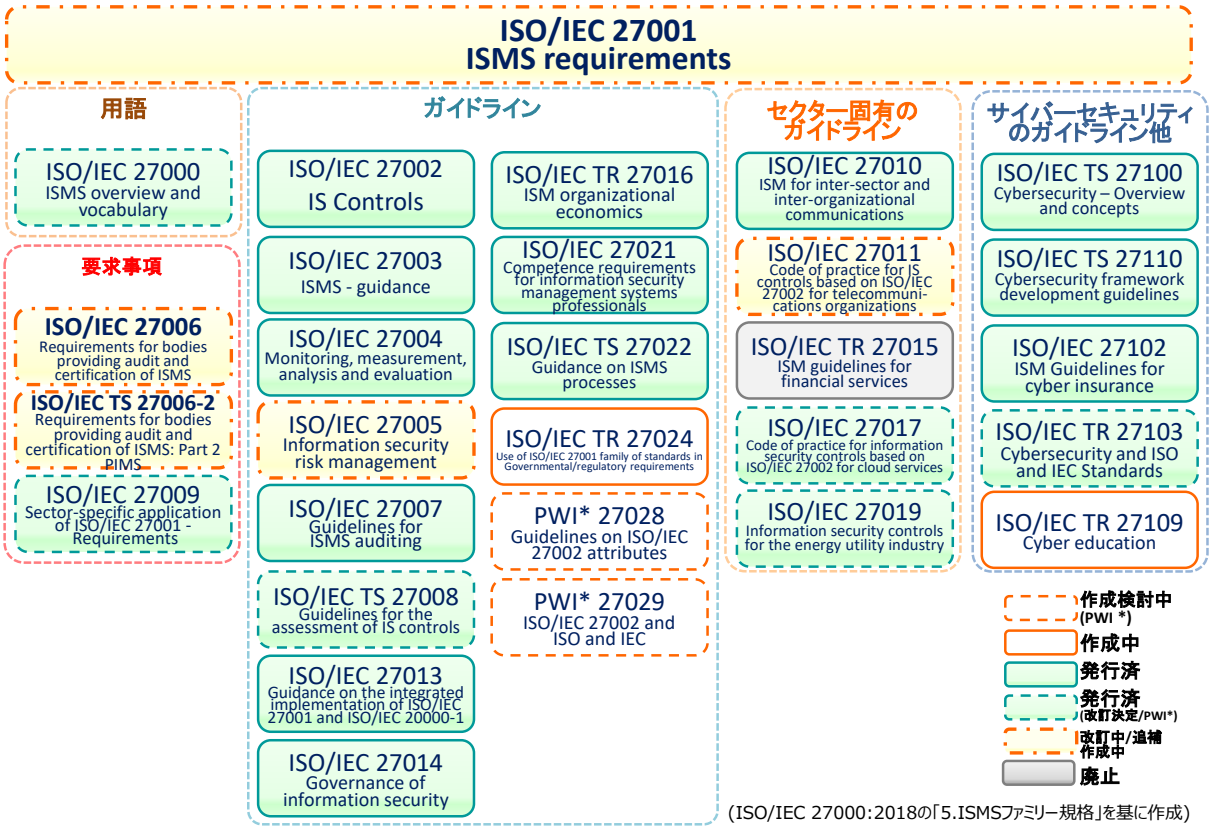
JIPDEC
一般財団法人日本情報経済社会推進協会

1. ISO/IEC 27000 ファミリー規格とは

ISO/IEC 27000 ファミリー規格は、情報セキュリティマネジメントシステム（ISMS）に関する国際規格であり、ISO（国際標準化機構）及び IEC（国際電気標準会議）の合同専門委員会 ISO/IEC JTC 1（情報技術）の分科委員会 SC 27（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）において標準化作業が進められています。

ISO/IEC 27000 ファミリー規格は、要求事項を規定した規格（ISMS 要求事項を規定した ISO/IEC 27001、ISMS 認証機関のための要求事項を規定した ISO/IEC 27006 及びセクター固有の ISMS 実施のための追加の要求事項の枠組みを規定した ISO/IEC 27009）と、ISMS 実施の様々な側面に関する手引を規定した規格（一般的なプロセス、管理策に関する指針及びセクター固有の手引）から構成されています。規格の番号は、現時点では 27000～27040 番台及び 27100～27110 番台の一部が中心となっています。

ISO/IEC 27000 ファミリー規格は、主に SC 27/WG 1（情報セキュリティマネジメントシステム）において作成されています。以下の図は、WG 1 における規格の作成／改訂状況を示しています。



(ISO/IEC 27000:2018の「5.ISMSファミリー規格」を基に作成)

*作成開始（NP 承認）： ISO 規格の作成可否について実施される NP（New work item Proposal）投票の結果、新規作成が決定された規格です。（「作成中」は NP 承認済で作成段階にある規格です。）規格作成の段階については、「2-1 WG1 における ISO/IEC 27000 ファミリー規格の検討状況」をご参照下さい。

※ISO/IEC TS 27006-2 は、SC 27/WG 5 のプロジェクトとして登録されていますが、SC 27/WG 1 と合同で策定され、ISO/IEC 27006 の第 2 部（Part 2）であるため記載しています。

また、SC 27/WG 1 の他、SC 27/WG 4（セキュリティコントロールとサービス）、SC 27/WG 5（アイデン

ティティ管理とプライバシー技術）においても関連する規格が策定されています。以下は、現在、作成・発行されている規格の一例です。

ISO/IEC 27018:2019

Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 27031:2011

Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity

ISO/IEC 27032:2012

Information technology – Security techniques – Guidelines for cybersecurity

ISO/IEC 27701:2019

Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines

詳細については、ISO の Web サイトをご参照ください。

ISO/IEC JTC 1/SC 27 で作成された規格一覧：

https://www.iso.org/committee/45306/x/catalogue/

2. ISO/IEC JTC 1/ SC 27/WG 1 会議の結果概要

WG 1 会議は、2022 年 4 月 5 日に Web 会議で開催されました（一部のプロジェクトについては、この会期外に Web 会議で審議を実施）。以下に ISO/IEC 27000 ファミリー規格の検討状況を一覧表として示すとともに、主なプロジェクトの進捗状況等を記載します。

2-1 WG1 における ISO/IEC 27000 ファミリー規格の検討状況

*各会議で審議される規格の段階を示しています。既に IS 発行済で現在改訂中のものについては、（）で改訂段階を示しています。
例：（DIS）－IS 発行済だが、現在改訂中で DIS 審議
※下表の色分け：緑色は発行済規格[斜字は改訂決定]、薄黄色は改訂中/追補作成中規格、灰色は中止プロジェクトです（白は作成中）。

ISO/IEC 番号	規格内容	規格策定の段階*	
		2022 年 4 月会議（今回）	2022 年 10 月会議（予定）
27000	*ISMS* 概要及び用語	(*PWI*)	(*PWI*)
27001	ISMS 要求事項	(DAM)	(FDIS 又は IS)
27002	情報セキュリティ管理策	IS	IS
27003	ISMS の手引	IS	IS
27004	ISM － 監視、測定、分析及び評価	IS	IS
27005	情報セキュリティリスクマネジメントに関する指針	(DIS)	(FDIS)
27006	ISMS 認証機関に対する要求事項	(2nd CD)	(DIS)
TS 27006-2	ISO/IEC 27701 認証機関に対する要求事項	(2ndWD)	(CD)
27007	ISMS 監査の指針	IS	IS
TS 27008	*IS* 管理策の評価*(assessment)*のための指針	(*PWI*)	(*PWI*)
27009	セクターへ規格の *27001* 適用－要求事項	(*PWI*)	(*PWI*)
27010	セクター間及び組織間コミュニケーションのための情報セキュリティマネジメント	IS	IS
27011	ISO/IEC 27002 に基づく電気通信組織のための情報セキュリティ管理策の実践の規範	(CD→2ndCD)	(DIS)
27013	ISO/IEC 27001 と ISO/IEC 20000-1 との統合導入についての手引	IS	IS
27014	情報セキュリティのガバナンス	IS	IS
TR 27015	金融サービスに対する情報セキュリティマネジメントの指針	(廃止)	(廃止)
TR 27016	ISM－組織の経済的側面(Organizational economics)	TR	TR
27017	*ISO/IEC 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	(*PWI*)	(*PWI*)
27019	エネルギー業界のための情報セキュリティ管理策	(*PWI*)	(*PWI*)
27021	ISMS 専門家の力量に関する要求事項	IS	IS
TS 27022	ISMS プロセスに関する手引	TS	TS
TR 27023	ISO/IEC 27001 及び ISO/IEC 27002 改訂版のマッピング	TR	TR
TS 27100	サイバーセキュリティの概要及びコンセプト	TS	TS
27102	ISM－サイバー保険のためのガイドライン	IS	IS
TR 27103	サイバーセキュリティと *ISO* 及び *IEC* 規格	(*PWI*)	(*PWI*)
TS 27110	サイバーセキュリティフレームワーク策定の指針	TS	TS

ISO/IEC JTC 1 における規格作成の段階は、以下の通り

*()は、省略可能な場合がある。

国際規格(IS)	(PWI)* → NP → WD → CD → DIS → FDIS → IS
追補（Amendment）	(PWI)* → (NP)* → WD → CDAM → DAM → FDAM → Amendment
技術仕様書(TS)	(PWI)* → NP → WD → DTS → TS
技術報告書(TR)	(PWI)* → DTR → TR

PWI	Preliminary Work Item	**CDAM**	Committee Draft Amendment
NP	New work item Proposal	**DAM**	Draft Amendment
WD	Working Draft	**FDAM**	Final Draft Amendment
CD	Committee Draft	**DTS**	Draft Technical Specification
DIS	Draft International Standard	**TS**	Technical Specification
FDIS	Final Draft for International standard	**DTR**	Proposed Draft Technical Report
IS	International Standard	**TR**	Technical Report

※PWI は、通常、NP に進めるには時期尚早な事項等を審議するために設置される。WG1 では、特に規格の作成／改訂に先立って、その方針(design specification)等を審議するために設置されている。

追補（Amendment）
既存の IS に対して、変更及び／又は追加を行うものであり、部分的な改訂とみなされる。

技術仕様書（TS：Technical Specification）
まだ開発の途上にある等の理由から、将来的に国際規格として合意が得られる可能性があるが現時点では直ちには得られない場合に発行することができる文書。発行後 3 年以内に見直しが行われる。

技術報告書（TR：Technical Report）
IS 又は TS として通常発行されるものとは異なる種類の収集データを含む文書。規定を示すような内容は含まない。

ISO/IEC における規格作成に関しては、ISO/IEC Directives で規定されている。詳細は、以下を参照。

- **ISO/IEC Directives, Part 1** —Consolidated ISO Supplement —Procedure for the technical work — Procedures specific to ISO —（ISO/IEC 専門業務用指針第 1 部—統合版 ISO 補足指針—ISO 専用手順－）
- **ISO/IEC Directives, Part 2** —Principles and rules for the structure and drafting of ISO and IEC documents（ISO/IEC 専門業務用指針第 2 部 ISO 及び IEC 文書の構成及び作成に関する原則と規則）
- **JTC 1 Supplement**（JTC 1 補足指針）

https://www.iso.org/directives-and-policies.html

2-2 主なプロジェクトの進捗状況

27001 （Information security management systems – Requirements）

2021 年 4 月開催の Web 会議の結果*に従って 2021 年 12 月に DAM が発行された。その後、2022 年 2～5 月上旬にかけて DAM 投票が実施された。投票の結果、DAM が承認され、FDIS に進むことになった。

2022 年 7 月現在、ISO 中央事務局にて FDIS 発行に向けて作業中である。

本 FDIS は、承認された DAM とこれまで発行されている正誤票 2 件を、ISO/IEC 27001:2013 に統合して発行される予定。

統合に際して、ISO 中央事務局から ISO/IEC Directives, Part 1 の Annex SL*最新版を適用するように指示があったことから、Annex SL に規定するマネジメントシステム規格の共通要素（共通箇条、共通テキスト、用語等）の最新版と整合させるために本文の変更も行われる見込みとなった。

*Annex SL (normative) Harmonized approach for management system standards：マネジメントシステム規格の共通要素を定めた附属書

※ 2021 年 4 月 Web 会議での検討結果は、【個々の規格の概要】の「ISO/IEC 27001:2013」を参照。

27002 （Information security controls）

2021 年 12 月に終了した FDIS 投票の結果、反対国はなく、FDIS が承認された。
この投票結果を受けて、2022 年 2 月に ISO が発行された。

27004 （Monitoring, measurement, analysis and evaluation）

規格発行から 5 年目の定期レビュー（Systematic review）が、2021 年 10 月から 3 月にかけて実施された。その結果、現行版を維持すべき（Confirm）：21 か国、改訂すべき（Revise/Amend）：4 か国、棄権（Abstain）：25 か国であった。

この定期レビュー結果に関して会議は開催されず、代わりにエディタからの報告書が 4 月下旬に発行された。この報告書によると、改訂を求めている国の主なコメントは、ISO/IEC 27002:2022 への整合が必要というものであった。ISO/IEC 27004 では ISO/IEC 27002 を参照していないが、ISO/IEC 27002 の管理策と整合している ISO/IEC 27001:2013 附属書 A の参照は含まれる。また、ISO/IEC 27001:2013 は、現在、ISO/IEC 27002:2022 との整合のために改訂中である。このような状況から、報告書では、コメントに対応するために ISO/IEC 27004 における ISO/IEC 27001:2013 の参照を、ISO/IEC 27001:2022 に更新するための正誤票（Corrigendum）の発行を提案すると結論づけている。

この報告書に基づき、正誤票（Corrigendum）の発行について書面投票が行われた。投票の結果、賛成多数で正誤票を発行する方向となった。

27005 （Guidance on managing information security risks）

DIS 投票結果は、賛成 29 か国（うちコメント付賛成 10 か国）、棄権 19 か国、反対 1 か国（スウェーデン）で、約 170 件のコメントが寄せられた。本 DIS 審議のために 3 月に Web 会議を開催し、これらのコメントについて審議した。会議にてすべてのコメント審議を終了し、FDIS を発行することになった。

27006-1 （Requirements for bodies providing audit and certification of ISMS - Part1 General）

2nd CD 投票結果は、賛成 25 か国（うちコメント付賛成 4 か国）、棄権 21 か国、反対 2 か国（日本、スウェーデン）で、約 90 件のコメントが寄せられた。
2ndCD 審議のために 2022 年 3 月に Web 会議を開催し、これらのコメントについて審議した。セクター規格認証のための追加の要求事項について、附属書 E に記載していたが、それ以外にも本文に一部追記するかたちで直接記載されている箇所もありわかりにくいというコメントがあり、審議された。その結果、附属書 E に記載の要求事項を本文中の関連する各箇条に移動し、附属書 E には、セクター規格認証のための追加の要求事項が記載されている箇条の一覧を記載することになった。その他、附属書 B に対して多くのコメントが寄せられており、審議された。
会議にてすべてのコメント審議を終了し、DIS を発行することになった。

■ISO/IEC 27006 の規格群として、WG 5 会議において次の規格の改訂について審議された。

TS 27006-2（Requirements for bodies providing audit and certification of information security management systems - Part 2: Privacy information management systems）

2ndWD に対して約 60 件のコメントが寄せられた。これらのコメントについて、3-4 月に開催された WG 5 国際会議において審議した。主に審査工数の計算方法について審議された結果、27006-1 との整合性を保つために要員数を審査工数のベースとする方向となった。

今回の会議にてすべてのコメント審議を終了し、CD を発行することになった。

【個々の規格の概要】

■ ISO/IEC 27000～ISO/IEC 27010

ISO/IEC 27000:2018

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

2018 年 2 月発行［第 5 版］

ISMS ファミリー規格の概要、ISMS ファミリー規格において使用される用語等について規定した規格。

■ **国内規格の発行**：2019 年 3 月に JIS Q 27000:2019 として制定された。

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 の用語及び定義の技術的内容を変更することなく作成した国内規格（ISMS の概要等を示した ISO/IEC 27000:2018 の箇条 4 以降は含まれていない）。

■ **改訂について**：

- 2009 年：第 1 版発行。2012 年 12 月：第 2 版発行。2014 年 1 月：第 3 版発行（その際に 27001:2013、27002:2013 対応）。2016 年 2 月：第 4 版発行。2018 年 2 月：第 5 版発行。
- 2021 年 4 月 Web 会議にて合意された、ISO/IEC 27002 改訂の影響を受ける 27000 ファミリー規格全体の段階的改訂スケジュールに従って、第 2 段階の改訂として、27000、27008、27019、27103 の改訂検討を開始することが合意された。これを受けて、27000 の改訂方針を検討するために PWI が設置された。

※ 27000 ファミリー規格の策定・改訂に対応する必要があるため、比較的短期間でマイナーな改訂が実施されている。

（2.1 に戻る）

ISO/IEC 27001:2013

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

2013 年 10 月発行［第 2 版］ **（改訂中）**

組織の事業リスク全般を考慮して、文書化した ISMS を確立、実施、維持及び継続的に改善するための要求事項を規定した規格。

■ **国内規格の発行**：2014 年 3 月に JIS Q 27001:2014（JIS Q 27001:2006 の改正版）として制定された。

JIS Q 27001:2014

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

■ **正誤票の発行**：2014 年 9 月に ISO より正誤票が発行された（JIS 正誤票は 2014 年 11 月に発行）。
その後、2015 年 11 月にも ISO より正誤票が発行された（JIS 正誤票は 2015 年 12 月に発行）。

■ **改訂について**：

- 2005 年に第 1 版発行後、2008 年 10 月に規格発行から 3 年目の定期レビュー（Pre-review）審議を行い、改訂開始が決定された。これを受けた改訂作業を経て、2013 年 10 月に第 2 版が発行された。
- 2016 年 4 月タンパ会議にて規格発行から 3 年目の定期レビュー（Pre-review）審議を行った。その結果、現時点では改訂は行わず現行版を維持することになった。
- 2019 年 4 月テルアビブ会議にて規格発行から 5 年目の定期レビュー（Systematic review）審議を行った結果、「ISO/IEC Directives, Part 1 —Consolidated ISO Supplement —Procedure for the technical work — Procedures specific to ISO —（ISO/IEC 専門業務用指針第 1 部—統合版 ISO 補足指針—ISO 専用手順－）」の Annex SL（マネジメントシステム規格の共通要素を定めた附属書）の改訂を考慮して、現時点では維持（confirm）とする方向となった。一方で、この Annex SL 改訂版の発行時期、ISO/IEC 27002 の改訂等を考慮した 27001 次期改訂への対応案がいくつか提示され、次回会議にて審議することになった。
- 2019 年 10 月パリ会議にて上記に関して審議した結果、現時点では改訂を開始しないが、今後 Annex L*や ISO/IEC 27002 の改訂状況をみながら必要に応じて再度検討することになった。
  *2019 年版では Annex SL から Annex L（（規定）マネジメントシステム規格の提案）に附属書番号が変更されたが、2020 年版にて再び Annex SL となった。
- 2021 年 4 月 Web 会議にて、ISO/IEC 27002 の改訂審議が DIS 段階となったことを受けて、27002 改訂の影響を受ける 27000 ファミリー規格全体の改訂スケジュールについて検討した。その結果、第 1 段階の改訂として 27001、27009、27017 を改訂することになった。
  27001 については、附属書 A を ISO/IEC 27002 改訂版に整合させるために限定的な改訂を実施し、Amendment（追補）を作成することになった。なお、すでに正誤票が 2 件発行されていることから、これらの正誤票と Amendment を ISO/IEC 27001:2013 に統合して、ISO/IEC 27001 第 3 版として発行される見込み。
  並行して PWI を設置し、27001 全面改訂を検討することになった。

（2.1 に戻る）

ISO/IEC 27002:2022

Information security, cybersecurity and privacy protection–information security controls

2022 年 2 月発行［第 3 版］

組織の情報セキュリティリスクの環境を考慮に入れた管理策の選定、実施及び管理を含む、組織の情報セキュリティ標準及び情報セキュリティマネジメントを実施するためのベストプラクティスをまとめた規格。ISO/IEC 27001 の「附属書 A 管理目的及び管理策」と整合がとられている。

※ 当初、ISO/IEC 17799 として発行されたが、2007 年 7 月に規格番号が 27002 へ改番された。

■ **国内規格の発行**：2014 年 3 月に JIS Q 27002:2014（JIS Q 27002:2006 の改正版）として制定された。

JIS Q 27002:2014

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

■ **正誤票の発行：**2014 年 9 月に ISO より正誤票が発行された（JIS 正誤票は 2014 年 11 月に発行）。
その後、2015 年 11 月にも正誤票が発行された（JIS Q 27002:2014 では対応済みのため、対応する JIS 規格の正誤票はない）。

■ **改訂について**：

- 2005 年に第 1 版発行後、2008 年 10 月に規格発行から 3 年目の定期レビュー（Pre-review）審議を行い、改訂開始が決定された。これを受けた改訂作業を経て、2013 年 10 月に第 2 版が発行された。
- 2016 年 4 月タンパ会議にて規格発行から 3 年目の定期レビュー（Pre-review）審議を行った。その結果、改訂する方向となり、SP（Study Period）[1]を設置して、design specification（改訂の方針等）について検討することになった。
- 2017 年 11 月ベルリン会議にて SP を終了し正式に改訂プロジェクトを開始するための NP 投票を実施した結果、2018 年 4 月武漢会議より改訂プロジェクトが開始された。
  なお、design specification 審議において規格名称を以下に変更することになった。
  Information technology — Security techniques — Information security controls
- 2022年2月に、数年にわたる審議の後、改訂版が発行された（その後、2022年3月に修正版［Corrected version］が発行された）。
  - ✓ 関連する改訂：2021 年 4 月 Web 会議にて、27002 の改訂審議が DIS 段階となったことを受けて、27002 改訂の影響を受ける 27000 ファミリー規格全体の改訂スケジュールについて、前回の会議にて検討した結果、3 段階に分けて関連規格を改訂することになった。第 1 段階として、27001、27009、27017 改訂検討が 2021 年 4 月に開始され PWI が設置された。
  - ✓ 関連する改訂：2021 年 10 月 Web 会議にて、第 2 段階として、27000、27008、27019、27103 改訂検討が 2021 年 10 月に開始され、PWI が設置された。

（2.1 に戻る）

ISO/IEC 27003:2017

Information technology – Security techniques – Information security management system – Guidance

2017 年 4 月発行［第 2 版］

ISO/IEC 27001：2013 に規定する ISMS の要求事項に対するガイダンス規格。箇条 4 から 10 は、ISO/IEC 27001 の構成に沿っており、各箇条では、要求される活動（Required activity）、説明（Explanation）、ガイダンス（Guidance）、関連情報（Other Information）について記載されている。

■ **改訂について**：

- 2010 年に第 1 版発行後、2013 年 5 月に ISO/IEC 27001:2013 に対応するための早期改訂開始が決

[1]SP（Study Period）：期間を設定して設置される検討プロジェクト。ISO 策定・改訂以外の事項（例：27009 事例集の検討）や、規格の策定・改訂の開始前に必要な方針（design specification）について検討される。なお、2019 年 10 月のパリ会議から、ISO/IEC Directives（ISO/IEC 専門業務用指針）に沿って SP に代わり PWI を設置することになった。

定された。これを受けた改訂作業を経て、2017 年 4 月に第 2 版が発行された。

- 2020 年 4 月 Web 会議にて規格発行から 3 年目の定期レビュー（Periodical pre-review）審議を行った結果、現時点では改訂は行わず現行版を維持することになった。

（2.1 に戻る）

ISO/IEC 27004:2016

Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation

2016 年 12 月発行［第 2 版］

ISO/IEC 27001:2013 に規定する「9.1 監視、測定、分析及び評価」の要求事項を満たすために情報セキュリティのパフォーマンス及び ISMS の有効性の評価を支援することを目的としたガイダンス規格。

■ **改訂について**：

- 2009 年に第 1 版発行後、2012 年 5 月に規格発行から 3 年目の定期レビュー（Periodical pre-review）審議の結果により改訂開始が決定された。これを受けた改訂作業を経て、2016 年 12 月に第 2 版が発行された。
- 2019 年 4 月にテルアビブ会議にて規格発行から 3 年目の定期レビュー（Periodical pre-review）審議を行った。その結果、現時点では改訂は行わず現行版を維持することになった。一方で、英国から編集上の不備による適用への影響が報告され、不備を修正するための正誤票（Corrigendum）を発行する方向となった。
- 2022 年 4 月に Web 会議にて 5 年目の定期レビュー（Systematic review）を行った結果、ISO/IEC 27001:2013 からの参照を ISO/IEC 27001:2022 に更新するための正誤票（Corrigendum）を発行する方向となった。

（2.1 に戻る）

ISO/IEC 27005:2018

Information technology – Security techniques – Information security risk management

2018 年 7 月発行［第 3 版］ **（改訂中）**

情報セキュリティのリスクマネジメントに関するガイドライン規格。

■ **改訂について**：

- 2008 年 6 月に第 1 版発行後、2010 年 4 月に ISO 31000:2009 及び ISO Guide 73:2009 との整合に限定した改訂を行うことが決定され、2011 年に第 2 版が発行された。
- 2013 年 10 月に ISO/IEC 27001:2013 に対応するための早期改訂開始が決定されたが、ISO 規定の期間内に発行に至らなかったため 2016 年 4 月にいったん改訂プロジェクトはキャンセルとなった。そのため、改めて SP（Study Period）を設置して、design specification（今後の改訂の方針、方向性等）を検討することになった。
- 2017 年 4 月ハミルトン会議にて、ISO/IEC 27005:2011 に対して提出された Defect Report（ISO/IEC 27001:2005 対応であり廃止すべきという英国提案）を審議した結果、SP と並行して ISO/IEC 27001:2013 に合わせるための編集上の修正を示した正誤票を発行する手続を実施することになった。
- 2017 年 10-11 月ベルリン会議にて、ISO の手続上の関係から正誤票ではなく改訂版を発行することになった。

そのため、正誤票案の内容を反映した版を迅速化手続によって準備し、2018 年 7 月に第 3 版として発行された（なお、上記の通り ISO/IEC 27001:2013 に合わせるための技術的な修正は行われていない）。

ISO/IEC 27001:2013 対応のための改訂については、2013 年 10 月に開始した SP にて検討した結果、2019 年 4 月テルアビブ会議にて本 SP を終了し、正式に改訂プロジェクトを開始するための NP 投票を実施することになった。2019 年 10 月パリ会議にて、NP 投票結果を受けて改訂プロジェクトを開始することになった。

- 2020 年 4 月 Web 会議にて、規格名称について、2017 年に合意された Design Specification（改訂方針）に従って変更すべきとの提案を受けて、以下に変更することになった。

  Guidance on managing information security risks

（2.1 に戻る）

ISO/IEC 27006:2015［追補 1］

Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems

2015 年 10 月発行［第 3 版］ **（改訂中）**

2020 年 3 月追補 1 発行

ISMS 認証を希望する組織の審査・認証を行う認証機関に対する要求事項を規定した規格。

マネジメントシステム認証機関に対する要求事項としては ISO/IEC 17021-1 が規定されているが、ISMS 認証機関に対しては併せて ISO/IEC 27006 が要求される。

■ **国内規格の発行**：2018 年 3 月に JIS Q 27006:2018（JIS Q 27006:2012 の改正版）として制定された。

JIS Q 27006:2018

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

■ **改訂について**：

- 2007 年に第 1 版発行後、ISO/IEC 17021 の改訂版 ISO/IEC 17021:2011 が発行されたことを受けて、2011 年 4 月に ISO/IEC 27006 も ISO/IEC 17021:2011 との整合に限定した早期改訂を行うことが決定され、2011 年に第 2 版が発行された。
- その後、2012 年 5 月に ISO/IEC 17021:2011 整合以外の内容も含む改訂開始が決定された。これを受けた改訂作業を経て、2015 年に第 3 版が発行された。
- 2018 年 4 月武漢会議にて規格発行から 3 年目の定期レビュー（Pre-review）審議を行った。その結果、6 か月間の SP（Study Period）を設置し、追補の発行が必要か検討することになった。
- 2018 年 9-10 月イエビク会議において、追補発行の可能性について検討した結果、追補を発行することになり、2020 年 3 月に追補 1 が発行された。
- 2020 年 9 月 Web 会議にて、ISO/IEC TS 27006-2 発行に伴い、ISO/IEC 27006-1 への番号変更が必要になったこと、及び今後の ISMS セクター規格認証（例：ISO/IEC 27701）の認定への共通的な対応を検討する必要が生じたことから、27006 改訂について検討するために PWI を設置することになった。
- PWI27006 審議のために実施された 2021 年 2 月 Web 会議にて、ISMS セクター規格認証対応のため、及

びニューノーマルに関連する事項を検討するための改訂開始が決定された。なお、規格番号は 27006-1 へ、これに伴いタイトルを以下に変更するための手続きを進めることになった。

Requirements for bodies providing audit and certification of information security management systems – Part1: General

■ISO/IEC 27006 の規格群

ISO/IEC TS 27006-2:2021

Requirements for bodies providing audit and certification of information security management systems - Part 2: Privacy information management systems

2021 年 2 月発行 **（改訂中）**

ISO/IEC 27701 認証を希望する組織の審査・認証を行う認証機関に対する要求事項を規定した規格。

ISO/IEC 27701 の認証機関に対しては、ISO/IEC 27006 と併せて ISO/IEC TS 27006-2 への適合が要求される。

■ 改訂について：

- 2021 年 4 月 Web 会議にて、TS から IS へ変更するための改訂について審議された。その結果、改訂を開始（ISO/CASCO の承認要）することになった。本改訂は、ISO/IEC JTC 1/SC 27/WG 5 にて審議される。

（2.1 に戻る）

ISO/IEC 27007:2020

Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing

2020 年 1 月発行［第 3 版］

ISMS 監査の実施に関するガイドライン規格。ISO 19011:2018（マネジメントシステム監査のための指針 – 2018 年 07 月発行）に加えて、ISMS 固有のガイダンスを提供する。

■ 改訂について：

- 2011 年に第 1 版発行後、2014 年 4 月に規格発行から 3 年目の定期レビュー（Periodical pre-review）を実施した結果、改訂開始が決定され、2017 年 10 月に第 2 版が発行された。
- 2018 年 9-10 月イエビク会議にて、ドイツ提案による ISO 19011:2018 対応のための早期改訂について審議した結果、ISO 19011:2018 対応に限定したマイナーな早期改訂開始が決定され、2020 年 1 月に第 3 版が発行された。

（2.1 に戻る）

ISO/IEC TS 27008:2019

Information technology – Security techniques – Guidelines for the assessment of information security controls

2019 年 1 月発行

情報セキュリティの管理策のレビューに関する技術仕様。

■ 改訂について：

- 2011 年に第 1 版発行後、2014 年 4 月に規格発行から 3 年目の定期レビュー（Periodical pre-review）を実施した結果、改訂開始が決定され、2019 年 1 月に第 2 版が発行された。改訂審議の中で、TR

（Technical Report：標準報告書）から TS（Technical Specification：標準仕様書）となり、さらに適用範囲の変更とともに標題も変更された。

- 2021 年 4 月 Web 会議にて合意された、ISO/IEC 27002 改訂の影響を受ける 27000 ファミリー規格全体の段階的改訂スケジュールに従って、第 2 段階の改訂として、27000、27008、27019、27103 の改訂検討を開始することが合意された。これを受けて、27008 の改訂方針を検討するために PWI が設置された。

※TS への変更に伴い、2019 年が（ISO/IEC TS 27008 としての）第 1 版となった。

（2.1 に戻る）

ISO/IEC 27009:2020

Information security, cybersecurity and privacy protection – Sector-specific application of ISO/IEC 27001 - requirements

2020 年 4 月発行

ISO/IEC 27001 を各セクターに適用した規格を作成する際の、規格の記述方法、様式等を定めた規格であり、セクター規格を作成する組織を対象としている。

■ **改訂について**：

- 2017 年 4 月ハミルトン会議にて早期改訂を開始することが決定され、2020 年 4 月に第 2 版が発行された。
- 2021 年 4 月 Web 会議にて、ISO/IEC 27002 の改訂審議が DIS 段階となったことを受けて、27002 改訂の影響を受ける 27000 ファミリー規格全体の段階的改訂スケジュールについて検討した。その結果、第 1 段階の改訂として 27001、27009、27017 を改訂することになり、27009 改訂検討のための PWI を設置することになった。

（2.1 に戻る）

ISO/IEC 27010:2015

Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications

2015 年 11 月発行［第 2 版］

セクター間及び組織間コミュニケーションのための情報セキュリティマネジメントに関する規格。情報共有コミュニティの中で情報セキュリティマネジメントを実施するためのガイダンスや、セクター間及び組織間コミュニケーションにおける情報セキュリティに関する管理策及び手引を提供する。

■ **改訂について**：

- 2012 年に第 1 版発行後、2014 年 10 月に ISO/IEC 27001:2013 対応のための早期改訂が決定され、2015 年に第 2 版が発行された。
- 2018 年 4 月武漢会議にて規格発行から 3 年目の定期レビュー（Periodical pre-review）審議を行った。その結果、現時点では改訂は行わず現行版を維持することになった。

（2.1 に戻る）

■ ISO/IEC 27011～ISO/IEC 27019

ISO/IEC 27011:2016

Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations

2016 年 12 月発行［第 2 版］ **（改訂中）**

電気通信業界内の組織における、ISO/IEC 27002 に基づいた情報セキュリティマネジメント導入を支援するガイドライン規格であり、SC 27 と ITU-T が共同で作成したものである。

■ **改訂について**：

- 2008 年に第 1 版発行後、2013 年 10 月に（ISO/IEC 27001:2013 対応のための）改訂開始が決定され、2016 年に第 2 版が発行された。
- 2019 年 4 月テルアビブ会議にて規格発行から 3 年目の定期レビュー（Pre-review）審議を行った。その結果、改訂プロジェクトを開始するための NP 投票を実施することになった。なお、規格の標題を変更することになった。
- 2019 年 10 月パリ会議にて NP 投票結果を受けて改訂プロジェクトを開始することになった。

（2.1 に戻る）

ISO/IEC 27013:2021

Information security, cybersecurity and privacy protection – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

2021 年 11 月発行［第 3 版］

ISO/IEC 20000-1 及び ISO/IEC 27001 の統合実践に関するガイダンス規格。

ISO/IEC 20000-1 担当の SC 7/WG 25（IT Service management）*と連携して作成された。

*現在の SC 40/WG 2 Service management - Information technology

■ **改訂について**：

- 2012 年に第 1 版発行後、2013 年 10 月に（ISO/IEC 27001:2013 対応のための）改訂開始が決定され、2015 年に第 2 版が発行された。
- 2018 年 4 月武漢会議にて規格発行から 3 年目の定期レビュー（Pre-review）審議を行った。その結果、現時点では改訂は行わず現行版を維持することになった。一方で、ISO/IEC 20000-1 の改訂版が 2018 年に発行される見込みのため、12 カ月間の SP（Study Period）を設置し、今後改訂が必要か検討するために ISO/IEC 20000-1 との違いを検証することになった。
- 2018 年 9-10 月イエビク会議にて ISO/IEC 20000-1:2018 が 2018 年 9 月に発行されたことに伴い、SP を終了して正式に改訂プロジェクトを開始するための NP 投票を実施することになった。
- 2019 年 4 月テルアビブ会議にて NP 投票結果を受けて改訂プロジェクトが開始され、2021 年 11 月に第 3 版が発行された。

（2.1 に戻る）

ISO/IEC 27014:2020

Information security, cybersecurity and privacy protection –Governance of Information security

2020 年 12 月発行［第 2 版］

情報セキュリティのガバナンスに関する規格であり、情報セキュリティガバナンスの原則及びプロセスの手引を提供する。

■ 国内規格の発行：2015 年 7 月に JIS Q 27014:2015 として制定された。

JIS Q 27014:2015

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

■ **改訂について**：

- 2016 年 4 月タンパ会議にて規格発行から 3 年目の定期レビュー（Pre-review）審議を行った結果、改訂する方向となり、SP（Study Period）を設置して、design specification（改訂の方針等）について検討することになった。
- 2017 年 4 月ハミルトン会議にて SP を終了し正式に改訂プロジェクトを開始するための NP 投票を実施した結果、2017 年 10 月ベルリン会議より改訂プロジェクトが開始され、2020 年に第 2 版が発行された（その後、2022 年 4 月に修正版［Corrected version］が発行された）。

（2.1 に戻る）

ISO/IEC TR 27015:2012

Information technology – Security techniques – Information security management guidelines for financial services

2012 年 11 月発行（2017 年 7 月廃止）

金融サービスのための情報セキュリティマネジメントに関する技術報告書

2016 年 10 月アブダビ会議にて改訂について審議された結果、TC 68/SC 2（Financial Services, security）等からも改訂の支持が得られず廃止を求める国が多かったため、廃止の手続きを進め、2017 年 7 月に廃止された。

（2.1 に戻る）

ISO/IEC TR 27016:2014

Information technology – Security techniques – Information security management – Organizational economics

2014 年 2 月発行

組織の情報資産の保護に対して経済学的な視点を適用し、モデル及び例示の使用を通して情報セキュリティに関する組織の経済性を適用する方法の手引を提供する技術報告書。

■ **改訂について**：

- 2019 年 4 月テルアビブ会議にて規格発行から 5 年目の定期レビュー（Systematic-review）審議を行った。その結果、現時点では改訂は行わず現行版を維持することになった。

（2.1 に戻る）

ISO/IEC 27017:2015

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

2015 年 12 月発行

ISO/IEC 27002 に基づいて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を提供する規格。

■ **国内規格の発行**：2016 年 12 月に JIS Q 27017:2016 として制定された。

JIS Q 27017:2016

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

■ **改訂について**：

- 2018 年 4 月武漢会議にて規格発行から 3 年目の定期レビュー（Pre-review）審議を行った。その結果、現時点では改訂は行わず現行版を維持することになった。
- 2021 年 4 月 Web 会議にて、ISO/IEC 27002 の改訂審議が DIS 段階となったことを受けて、27002 改訂の影響を受ける 27000 ファミリー規格全体の改訂スケジュールについて検討した。その結果、第 1 段階の改訂として 27001、27009、27017 を改訂することになり、27017 改訂検討のための PWI を設置することになった。

（2.1 に戻る）

ISO/IEC 27019:2017

Information technology – Security techniques – Information security controls for the energy utility industry

2017 年 10 月発行

エネルギー業界のための情報セキュリティ管理策。

■ **改訂について**：

- 2013 年 7 月に TR として発行後、2014 年 10 月メキシコ会議にて 1 年間の SP（Study Period）での審議結果を経て、早期改訂の開始が決定された。この改訂中に、TR から IS に変更し、名称も変更された。その後、2017 年に IS として発行された。
- 2018 年 9-10 月イエビク会議にて附属書 A（表 A の 11.7）内の表記（should -> shall）の指摘があり、正誤表を発行することになったが、ISO の手続き上、正誤票は発行されず、2019 年 7 月に規格本体にこの修正が加えられた。
- 2021 年 4 月 Web 会議にて合意された、ISO/IEC 27002 改訂の影響を受ける 27000 ファミリー規格全体の改訂スケジュールに従って、第 2 段階の改訂として、27000、27008、27019、27103 の改訂検討を開始することが合意された。これを受けて、27019 の改訂方針を検討するために PWI が設置された。

※TR から IS への変更に伴い、2017 年が（ISO/IEC 27019 としての）第 1 版となった。

（2.1 に戻る）

■ ISO/IEC 27021～ISO/IEC TR 27023

ISO/IEC 27021:2017［追補 1］

Information technology – Security techniques – Competence requirements for information security management systems professionals

2017 年 10 月発行［第 3 版］

2021 年 12 月追補 1 発行

ISMS 専門家の力量に関する要求事項について規定した規格。

■ **改訂について**：

- 2019 年 4 月テルアビブ会議にて韓国から修正提案があり、追補を発行する方向となった。
- 2020 年 4 月 Web 会議にて規格発行から 3 年目の定期レビュー（Periodical pre-review）審議を行った結果、規格の改訂は行わず現行版を維持することになった。
- 2021 年 11 月に ISO/IEC 27021:2017 に対する追補 1 が発行された。

（2.1 に戻る）

ISO/IEC TS 27022:2021

Information technology– Guidance on ISMS processes

2021 年 3 月発行

ISMS のプロセスについてのガイダンスを提供する規格。

（策定中に、規格のタイプが IS（International Standard）から TS（Technical Specification)へ変更された。）

(2.1 に戻る)

ISO/IEC TR 27023:2015

Information technology – Security techniques – Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002

2015 年 7 月発行

ISO/IEC 27001 及び ISO/IEC 27002 新旧対応表をまとめた技術報告書。

2013 年 10 月に発行された ISO/IEC JTC 1/SC 27 N13143「JTC 1/SC 27/SD3 – Mapping Old-New Editions of ISO/IEC 27001 and ISO/IEC 27002」の内容をそのまま取り込んだものである。SD3（Standing Document 3）は ISO の内部文書であるため、より正式な ISO 文書である TR として発行された。

■ **改訂について**：

- 2014 年 7 月～10 月に早期発行のための DTR 投票が行われ、可決された。これを受けた手続を経て、2015 年に発行された。
- 2020 年 4 月 Web 会議にて規格発行から 5 年目の定期レビュー（Systematic review）審議を行った結果、現時点では改訂は行わず現行版を維持することになった（ISO/IEC 27001、ISO/IEC 27002 の改訂後に改訂予定）。

(2.1 に戻る)

■ ISO/IEC TS 27100～ISO/IEC TS 27110

ISO/IEC TS 27100:2020

Information technology – Cybersecurity – Overview and Concepts

2020 年 12 月発行

サイバーセキュリティの概要（用語の定義を含む）を提供する規格。

(2.1 に戻る)

ISO/IEC 27102:2019

Information security management — Guidelines for cyber-insurance

2019 年 8 月発行

組織の情報セキュリティリスクマネジメントの中で、サイバーインシデントの影響を管理するためのリスク対応の選択肢の 1 つとしてサイバー保険を採用する場合のガイドラインを提供する規格。

(2.1 に戻る)

ISO/IEC TR 27103:2018

Information technology – Security techniques – Cybersecurity and ISO and IEC Standards

2018 年 2 月発行

サイバーセキュリティフレームワークにおいて、既存の ISO 及び IEC 規格を活用する方法についての手引を提供する規格。

サイバーセキュリティのためのフレームワークの背景と概要について説明し、ISO/IEC 27000 ファミリーをはじめとする既存の ISO 及び IEC 規格とのマッピングを提供している。

■ **改訂について**：

- 2021 年 4 月 Web 会議にて合意された、ISO/IEC 27002 改訂の影響を受ける 27000 ファミリー規格全体の改訂スケジュールに従って、第 2 段階の改訂として、27000、27008、27019、27103 の改訂検討を開始することが合意された。これを受けて、27103 の改訂方針を検討するために PWI が設置された。

（2.1 に戻る）

ISO/IEC TS 27110:2021

Information technology, cybersecurity and privacy protection – Cybersecurity framework development guidelines

2021 年 2 月発行

サイバーセキュリティの枠組みを構築するためのガイドラインを提供する規格。

（発行準備段階で、規格番号が 27101 から 27110 へ変更された。）

（2.1 に戻る）

以上