

ISO/IEC 27000 ファミリーについて

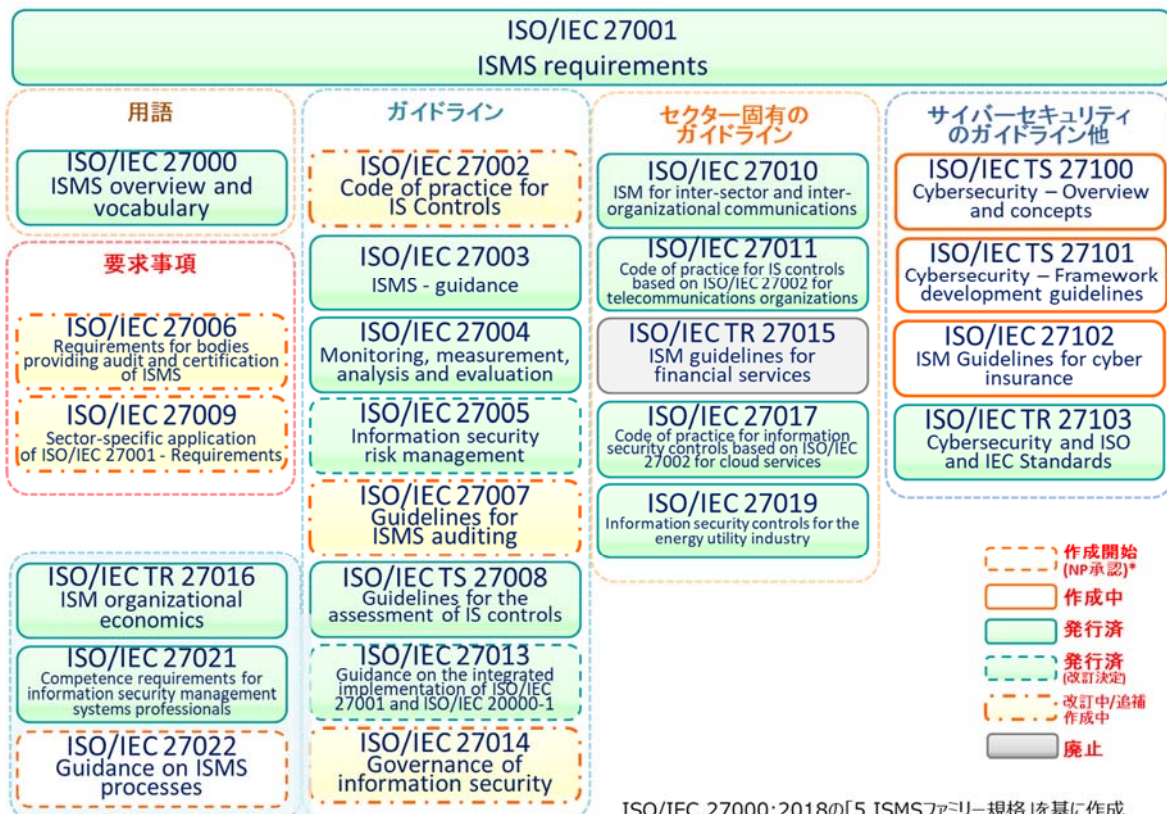
2019年5月20日

1. ISO/IEC 27000 ファミリーとは

ISO/IEC 27000 ファミリーは、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）の設置する合同専門委員会 ISO/IEC JTC 1（情報技術）の分科委員会 SC 27（セキュリティ技術）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 2710X 番台が中心となっています。

ISO/IEC 27000 ファミリーは、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。



*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、11ページをご参照下さい。

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 27018:2014

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 DIS 27552

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：

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45306&published=on

2. 個々の規格の概要

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 27000:2019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。

※ 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。

ISO/IEC 27001:2013

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

2013年10月発行 [第2版]

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 専門業務用指針 第1部 統合版 ISO 補足指針」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（別途、手続中）。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。

ISO/IEC 27002:2013

Information technology – Security techniques – Code of practice for information security controls
2013年10月発行 [第2版] (改訂中)

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月に定期レビュー審議を行い、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月タンパ会議にて定期レビュー審議を行った。その結果、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 審議において標題を以下に変更することになった。

Information technology — Security techniques — Information security controls

*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。

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。

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

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 月に定期レビュー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定期レビュー審議を行った。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）を発行することになった。

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 月開催のハミルトン会議において、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 月に開催されたベルリン会議において、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。

ISO/IEC 27006:2015

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] (追補作成中)

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月武漢会議にて定期レビュー審議を行った。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月イェビク会議において、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った。

ISO/IEC 27007:2017

Information technology – Security techniques – Guidelines for information security management systems auditing

2017年10月発行 [第2版] (改訂中)

ISMS監査の実施に関するガイドライン規格。ISO 19011:2011（マネジメントシステム監査のための指針-2011年11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：2014年4月香港会議にて定期レビュー審議を行い、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月イェビク会議にて、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を開始することになった。

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：2014年4月香港会議にて定期レビュー審議を行い、改訂開始が決定され、2019年1月に発行された。

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。

ISO/IEC 27009:2016

Information technology – Security techniques – Sector-specific application of ISO/IEC 27001 - requirements

2016年6月発行 (改訂中)

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た。

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月武漢会議にて定期レビュー審議を行った。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。

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]

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（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。

ISO/IEC 27013:2015

Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

2015年11月発行 [第2版] (改訂開始)

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 Maintenance and development of ISO/IEC 20000 - Information technology - Service management

■ 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月武漢会議にて定期レビュー審議を行った。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月イェピク会議にて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を開始することになった。

ISO/IEC 27014:2013

Information technology – Security techniques – Governance of Information security

2013年4月発行 (改訂中)

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月タンパ会議にて定期レビュー審議を行った結果、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た。

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。

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月にテルアビブ会議にて定期レビュー（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。

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。

※国内規格としては、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月武漢会議にて定期レビュー審議を行った。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。

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月イェピク会議にて附属書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。

ISO/IEC 27021:2017

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

2017年10月発行

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月に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。

ISO/IEC 27022:2017 (作成開始)

Information technology – Security techniques – Guidance on ISMS processes

ISMSのプロセスについてのガイダンスを提供する規格。

2019年4月テルアビブ会議にて新規プロジェクトとして承認され、規格を作成することになった。

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。

■ 改訂について：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として発行することになった。

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。

ISO/IEC TS 27100 (作成中)

Information technology – Cybersecurity – Overview and Concepts

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。

2018年9-10月イエビク会議にて新規プロジェクトとして承認され、規格を作成することになった。

ISO/IEC TS 27101 (作成中)

Information technology — Cybersecurity – Framework development guidelines

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。

2018年4月武漢会議にて新規プロジェクトとして承認され、規格を作成することになった。

ISO/IEC 27102 (作成中)

Information technology – Security techniques – Information security management guidelines for cyber insurance

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。

2017年4月ハミルトン会議にて新規プロジェクトとして承認され、規格を作成することになった。

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。

2018年9-10月イエビク会議にて、サイバーセキュリティフレームワークと既存規格の関係を示す有益な文書であり（標準化作業での活用を前提とした）無償配布のための手続を進めることが決定された。

3. ISO/IEC JTC 1 SC 27/WG 1 会議の結果概要

WG 1 会議は、2019 年 4 月 1 日～5 日にテルアビブ（イスラエル）にて開催されました。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。

3-1 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：IS（改訂中：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*	
		2019 年 4 月会議 (今回予定)	2019 年 10 月会議 (次回予定)
ISO/IEC 27000	ISMS 概要及び用語	IS[第 5 版]	IS[第 5 版]
ISO/IEC 27001	ISMS 要求事項	IS[第 2 版] (定期レビュー審議)	IS[第 2 版] (改訂に関する審議)
ISO/IEC 27002	情報セキュリティ管理策の実践のための規範	IS[第 2 版] (2nd WD)	IS[第 2 版] (3rd WD)
ISO/IEC 27003	ISMS の手引	IS[第 2 版]	IS[第 2 版]
ISO/IEC 27004	ISM - 監視、測定、分析及び評価の手引	IS[第 2 版] (定期レビュー審議)	IS[第 2 版] (正誤票案作成)
ISO/IEC 27005	情報セキュリティリスクマネジメントに関する指針	IS[第 3 版] (SP)	IS[第 3 版] (NP)
ISO/IEC 27006	ISMS 認証機関に対する要求事項	IS[第 3 版] (追補案作成:PDAM)	IS[第 3 版] (追補案作成:DAM)
ISO/IEC 27007	ISMS 監査の指針	IS[第 2 版] (DIS)	IS[第 2 版] (DIS/FDIS)
ISO/IEC TS 27008	IS 管理策の評価(assessment)のための指針	TR[第 1 版] (TS)	TR[第 1 版] (TS)
ISO/IEC 27009	セクター規格への 27001 適用に関する要求事項	IS[第 1 版] (2nd CD)	IS[第 1 版] (DIS)
ISO/IEC 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[第 2 版]	IS[第 2 版]
ISO/IEC 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	IS[第 2 版] (定期レビュー審議)	IS[第 2 版] (NP)
ISO/IEC 27013	ISO/IEC 27001 と ISO/IEC 20000-1 との統合導入についての指針	IS[第 2 版] (改訂開始)	IS[第 2 版] (WD)
ISO/IEC 27014	情報セキュリティのガバナンス	IS[第 1 版] (2nd WD)	IS[第 1 版] (CD)
ISO/IEC 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)
ISO/IEC TR 27016	ISM-組織の経済的側面(Organizational economics)	TR[第 1 版] (定期レビュー審議)	TR[第 1 版]
ISO/IEC 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	IS	IS
ISO/IEC 27019	エネルギー業界のための情報セキュリティ管理策	IS[第 2 版] (正誤票案作成)	IS[第 2 版] (正誤票発行)
ISO/IEC 27021	ISMS 専門家の力量に関する要求事項	IS	IS (追補案の検討開始)
ISO/IEC 27022	ISMS プロセスに関する手引	NP	WD
ISO/IEC TR 27023	ISO/IEC 27001 及び ISO/IEC 27002 改訂版のマッピング	TR	TR
ISO/IEC TS 27100	サイバーセキュリティの概念及びコンセプト	WD	2nd WD
ISO/IEC TS 27101	サイバーセキュリティフレームワーク策定の指針	2nd WD	3rd WD
ISO/IEC 27102	サイバー保険のための ISM 指針	DIS	FDIS
ISO/IEC TR 27103	サイバーセキュリティと ISO 及び IEC 規格	TR (無償化手続の実施)	TR (無償化/手続の実施)
ISO 規格作成の段階は、次のとおり			
NP → WD → CD → DIS → FDIS → IS (発行済)		TR/TS 規格作成の段階は、次のとおり。	
		TR : PDTR → TR	
		TS : NP → WD → PDTS → TS	
NP :	New work item Proposal (NWIP)	TR :	Technical Report (技術報告書)
WD :	Working Draft	TS :	Technical Specification (技術仕様)
CD :	Committee Draft	PDTR/PDTS :	Proposed Draft Technical Report/ Specification
DIS :	Draft International Standard	※SP : Study Period のことであり、上記表内の SP では改訂プロジェクト設置	
FDIS :	Final Draft for International standard	に先立って、改訂方針等について検討されます。	
IS :	International Standard		

3-2 主なプロジェクトの進捗状況

27001 (ISMS Requirements)

今回の会議に先立って実施された、規格発行から 5 年目の定期レビュー (Systematic review) の投票結果は、改訂すべき (Review/Amend) : 13 か国、現行版を維持 (Confirm) : 20 か国、棄権 (Abstain) : 4 か国、廃止すべき (Withdraw) : 0 であった。

会議では、昨年秋に改訂が開始された「ISO/IEC 専門業務用指針 第 1 部 統合版 ISO 補足指針」の Anenx SL*の改訂等を考慮して審議した結果、今回は現行版を維持 (Confirm) とする方向となった。一方で、会議の中で Annex SL 改訂版の発行時期及び現在改訂中の 27002 に関連して、27001 次期改訂への対応についての案がいくつか提示されたことを受けて、これらの案に対するコメントを募集し、次回会議にて検討することになった。

*ISO のマネジメントシステム規格 (MSS: Management System Standard) に共通の要素 (構成、定義、テキスト) を規定した Annex (附属書)。全ての MSS はこの Annex XL を適用することが必須となっている。

27002 (Information security controls)

今回の会議に先立って 2nd WD が発行されており、この WD に対して 600 件を超えるコメントが寄せられた。

会議では、このうち約 400 件はエディタが会議前に対処案 (採用、修正して採用等) を示していることから審議しないことを合意し、残りの 200 件について審議した。

会議では、事前にエディタが準備した資料により、これらのコメントを、管理策の構成、管理策の統廃合・新規管理策の追加、管理策の名称・内容等の点から 4 つに分類して審議を進めたが、一部は次回に持ち越しとなった。また、他の WG (WG 4、WG 5) に関連する管理策については、各 WG に確認し、用語や表現の整合をとることになった。

今回の審議の結果、3rd WD を発行することになった。

27004 (Monitoring, measurement, analysis and evaluation)

今回の会議に先立って実施された、規格発行から 3 年目の定期レビュー (Pre-review) 投票の結果は、維持 (Confirm) : 7 か国、改訂 (Revise) : 3 か国であった。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) を発行することになった。

27005 (SP for the development of working document for the 4th edition of ISO/IEC 27005)

ISO/IEC 27001:2013 対応の 27005 改訂案を作成するために設置された SP である。今回の会議に先立って作業文書 (Working Document) が発行されており、この文書に対するコメントに沿って検討した。

審議の結果、作業文書の内容が成熟してきたことから 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。

27006 (Requirements for bodies providing audit and certification of ISMS Amendment 1)

今回の会議に先立って発行された PDAM (Proposed Draft Amendment: 追補案) 投票の結果は、賛成 18 か国、コメント付賛成 2 か国、反対 1 か国 (日本)、棄権 26 か国であった。

会議では、主に反対国のコメントを中心に審議され、日本コメントは概ね採用されたが、反対理由の 1 つである審査員になるために必要な審査の経験に関するコメントは採用されなかったため、最終

的に日本は反対に留まった。

審議の結果、次回は DAM(Draft Amendment – DIS に相当)を発行することになった。

27007 (Guidelines for information security management systems auditing)

前回会議での審議結果を受けて、マイナーな改訂を開始するための投票が実施された。この投票結果により早期改訂が決定され、DIS が発行されたが、DIS 投票期限が 6 月下旬のため今回の会議では審議されなかったため、8 月に Web 会議を実施することになった。

27009 (Sector-specific application of ISO/IEC 27001 – Requirements)

今回の会議に先立って実施された 2nd CD 投票結果は、賛成 18 か国、コメント付賛成 5 か国、反対 0 であった。

投票とともに約 30 件のコメントが寄せられており、会議ではこれらのコメントに基づいて審議した。また、附属書に規定しているセクター規格作成のためのテンプレートについて、ISO/IEC Directives Part 2 に合わせて修正する必要が生じたことから、エディタが修正することになった。

今回の会議の結果、次回は DIS を発行することになった。

3-3 その他

昨今のサイバーセキュリティに関する動向を踏まえて各国から様々な提案がなされたことを受けて、現在、以下の規格の策定が進められています。

- ・サイバーセキュリティ – 概要及びコンセプト(TS:技術仕様書)
名称: ISO/IEC TS 27100 Cybersecurity – Overview and concepts
今回のテルアビブ会議において 1st WD が審議された結果、次回は 2nd WD 発行の予定。
サイバーセキュリティの概要や関連する定義等を規定する。
- ・サイバーセキュリティフレームワークを策定するためのガイドライン(TS:技術仕様書)
名称: ISO/IEC TS 27101 Cybersecurity – Framework development guidelines
前回の武漢会議において作成が開始された文書。米国から提案された文書をもとにしている。
今回のテルアビブ会議において 2nd WD が審議された結果、次回は 3rd WD 発行の予定。
- ・サイバー保険に関するガイドライン規格
名称: ISO/IEC 27102 Information security management guidelines for cyber insurance
今回のテルアビブ会議で DIS について審議された結果、次回は FDIS 発行の予定。

※サイバーセキュリティフレームワークと ISO・IEC 規格の関連を示す技術報告書

名称: ISO/IEC TR 27103 Cybersecurity and ISO and IEC Standards

2018 年 2 月発行。

2018 年 9-10 月イェビク会議において、米国提案により(標準化作業での活用を前提に)無償で入手可能にするための手続を開始することになった。

上記の通り、サイバーセキュリティ関連規格の番号は、2710X 番台となる予定です。

以上