

ISO/IEC 27000 ファミリーについて

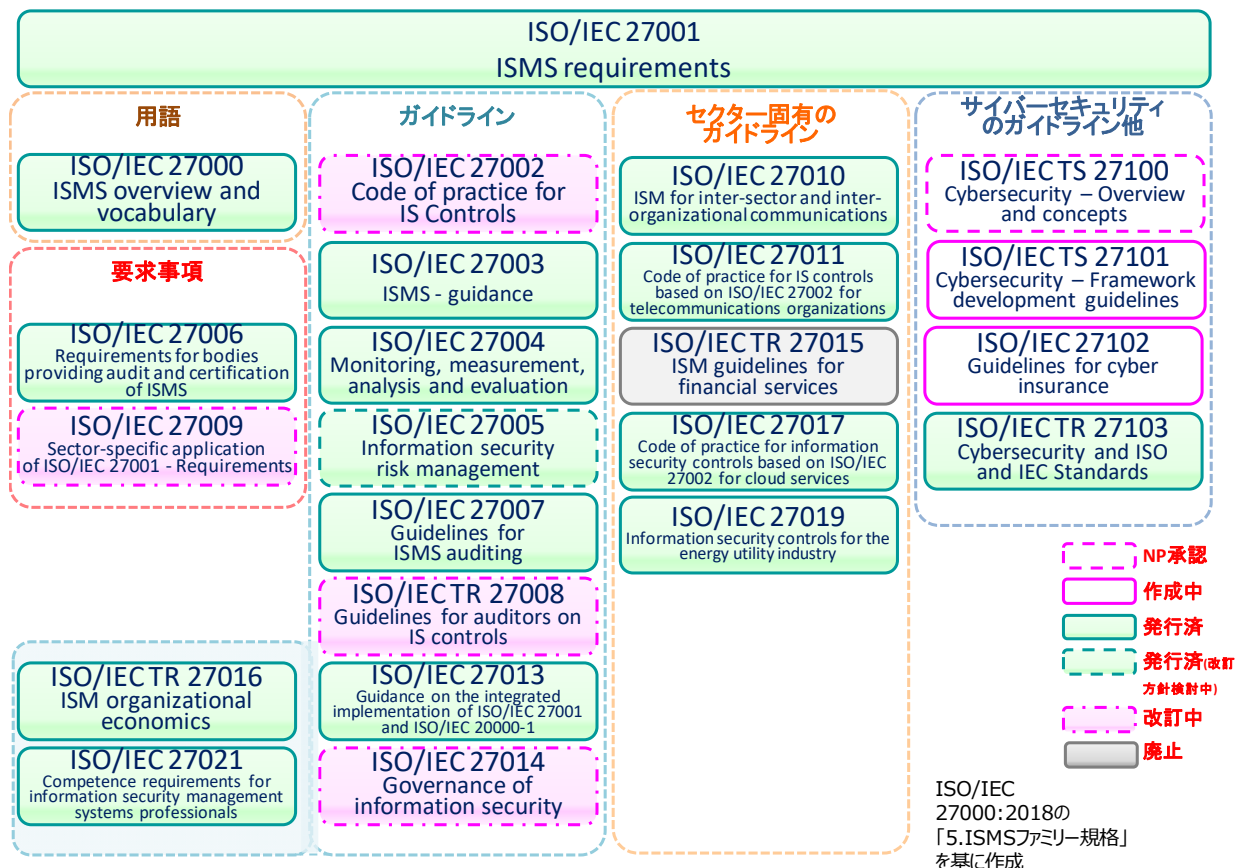
2018 年 12 月 12 日

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。



*NP：New work item Proposal のことであり、ISO 規格を作成する場合、初めに作成可否について NP 投票が行われます。規格策定の段階については、10 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

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

※ 国内規格としては、2014 年 3 月に JIS Q 27000:2014 として制定された。

JIS Q 27000:2014

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－用語

ISO/IEC 27000:2014 の箇条 2 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 の概要などを示した ISO/IEC 27000:2014 の箇条 3 以降は含まれていない)。

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

※ 国内規格としては、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

なお、2014 年 9 月に、ISO より正誤票が発行されている (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 正誤票は 2015 年 12 月に発行)。

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、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 27002:2013

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

2013 年 10 月発行 [第 2 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。

※ 国内規格としては、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

なお、2014 年 9 月に、ISO より正誤票が発行されている（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 規格の正誤票はありません）。

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（DS）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。

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

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。

ISO/IEC 27005:2018

Information technology – Security techniques – Information security risk management

2018 年 7 月発行 [第 3 版]（現在、改訂審議中）

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

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) を検討後、現在この design specification に沿って Working Document を作成中である。

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、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ための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 (正誤表発行ではなく) 早期改訂を実施して正誤票案の内容を反映した第 3 版を迅速化手続によって発行することになり、2018 年 7 月に第 3 版が発行された。

なお、ISO/IEC 27001:2013 対応のための改訂は上記 SP にて実施中であり、改訂終了後に第 4 版として発行予定である。

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]

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。

※ 国内規格としては、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

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 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]

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。

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 TR 27008:2011

Information technology – Security techniques – Guidelines for auditors on information security controls

2011 年 10 月発行（現在、改訂審議中）

組織の情報セキュリティの管理策のレビューに関する技術報告書（TR：Technical Report）

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た。

改訂審議の中で、第 2 版では適用範囲の変更とともに標題を以下に変更することになった。

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

また、TR（Technical Report：標準報告書）から TS（Technical Specification：標準仕様書）に変更することになった。

ISO/IEC 27009:2016

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

2016 年 6 月発行（現在、改訂審議中）

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。

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。

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。

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。

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]

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

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。

ISO/IEC 27014:2013

Information technology – Security techniques – Governance of Information security

2013 年 4 月発行 (現在、改訂審議中)

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。

※ 国内規格としては、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

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) など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

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

2018 年 4 月武漢会議にて定期レビュー（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。

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

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 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。

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

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 27102（作成中）

Information technology -- Security techniques -- Guidelines for cyber insurance

組織のリスクマネジメントの枠組みの中で、サイバー保険をリスク低減の対策に用いる場合のガイドラ

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、2018 年 9 月 30 日～10 月 4 日にイエビク（ノルウェー）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*	
		2018 年 10 月会議 (今回)	2019 年 4 月会議 (次回予定)
ISO/IEC 27000	概要及び用語	IS[第 5 版]	IS[第 5 版]
ISO/IEC 27001	要求事項	IS[第 2 版]	IS[第 2 版]
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] (WD)	IS[第 2 版] (2nd WD)
ISO/IEC 27003	ISMS の手引	IS[第 2 版]	IS[第 2 版]
ISO/IEC 27004	監視、測定、分析及び評価の手引	IS[第 2 版]	IS[第 2 版]
ISO/IEC 27005	リスクマネジメントに関する指針	IS[第 3 版] (SP)	IS[第 3 版] (SP)
ISO/IEC 27006	認証機関に対する要求事項	IS[第 3 版] (SP:追補検討)	IS[第 3 版] (追補案作成:PDAM)
ISO/IEC 27007	監査の指針	IS[第 2 版] (早期改訂決定)	IS[第 2 版] (DIS)
ISO/IEC TR 27008	IS 管理策に関する監査員のための指針	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] (CD)	IS[第 1 版] (2nd CD)
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]	IS[第 2 版]
ISO/IEC 27013	ISO/IEC 27001 と ISO/IEC 20000-1 との統合導入についての手引	IS[第 2 版] (SP)	IS[第 2 版] (改訂開始)
ISO/IEC 27014	情報セキュリティのガバナンス	IS[第 1 版] (WD)	IS[第 1 版] (2nd WD)
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	情報セキュリティマネジメント組織の経済的側面(Organizational economics)	TR[第 1 版]	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]	IS[第 2 版] (正誤案作成)
ISO/IEC 27021	ISMS 専門家の力量に関する要求事項	IS	IS
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	NP	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	WD	2nd WD
ISO/IEC 27102	サイバー保険のための指針	CD	DIS
ISO/IEC TR 27103	サイバーセキュリティと ISO 及び IEC 規格	TR	TR (無償化手続の実施)
ISO 規格策定の段階は、次のとおり			
NP → WD → CD → DIS → FDIS → IS (発行済)			
TR/TS 規格策定の段階は、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

27002 (Information security controls)

今回の会議に先立って 1st WD が発行されており、この WD について審議した。主に既存の管理策の統合、削除、新規追加について議論した結果、全体的に複数の管理策を統合する方向となり、新規管理策としては約 15 個を追加することになった。一方で、今回は個々の管理策の名称や内容については議論に至らなかった。

今回の審議の結果、次回は 2nd WD を発行し、引き続き管理策の構成や扱う属性など、全体構成の審議を優先して進める予定。

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 12 か月間の 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、作業文書が未成熟であることを理由に SP を延長し、作業文書 (Working Document) の充実を図ることになった。その後、正式な改訂プロジェクトを開始する見込み。

27006 (SP for Development of a possible PDAM for ISO/IEC 27006:2015)

■Periodical Review (定期レビュー)

前回の武漢会合にて ISO/IEC 27006 定期レビュー (Pre-review) を審議した結果、追補発行の可能性について検討するための 6 か月間の SP が設置された。本 SP の目的は、定期レビューと併せて改訂審議用に提出されたコメントをもとに作成した修正提案について審議し、追補を発行するか、改訂を開始するか、あるいは現行版を維持するかについて決定することであり、今回のイェビク会議では主にこの点について審議された。

会議の冒頭に、ラポータから追補として発行する場合には 27006 適用に重大な問題がある修正に限るべきという方針の提案があり、合意された。この方針に基づいて審議した結果、修正提案 38 件のうち、5 件が追補案に含めるべき重大な修正として合意され、追補を発行することで合意された。

次回会議では、追補発行に向けてこの 5 件を含めた追補案を審議予定。

なお、今回含まれなかった修正提案の多くは、次回改訂に持ち越しとなった。

27007 (Guidelines for information security management systems auditing)

会議に先立って ISO 19011:2018 が 2018 年 7 月に改訂されたことを受けて、ドイツより ISO 19011:2018 に整合させるための早期改訂が提案されていた。内容的には現行版は有効であるため、ISO 19011:2018 との整合に限定したマイナー改訂を行うことになった。

審議の結果、改訂を開始するための手続を開始し、DIS を発行することになった。

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

今回の会議に先立って実施された CD 投票結果は、賛成 17 か国、コメント付賛成 3 か国(仏、独、日)、反対 1 か国(英)であった。

投票とともに約 100 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。特に、附属書(セクター規格作成のためのテンプレート)について審議した結果、今回の審議結果を反映したドラフトを慎重に確認するために、次回は 2nd CD 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。

- ・サイバー保険に関するガイドライン規格
名称： ISO/IEC 27102 Guidelines for cyber insurance
今回のイエビク会議で 1st CD について審議された結果、次回は DIS 発行の予定。
- ・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。
今回のイエビク会議において 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 – 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
今回のイエビク会議において NWIP が承認され作成が開始された文書。
サイバーセキュリティの定義を含む概要等を規定する。

※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。

今回のイエビク会議で、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