ISO/IEC 27000 ファミリーについて

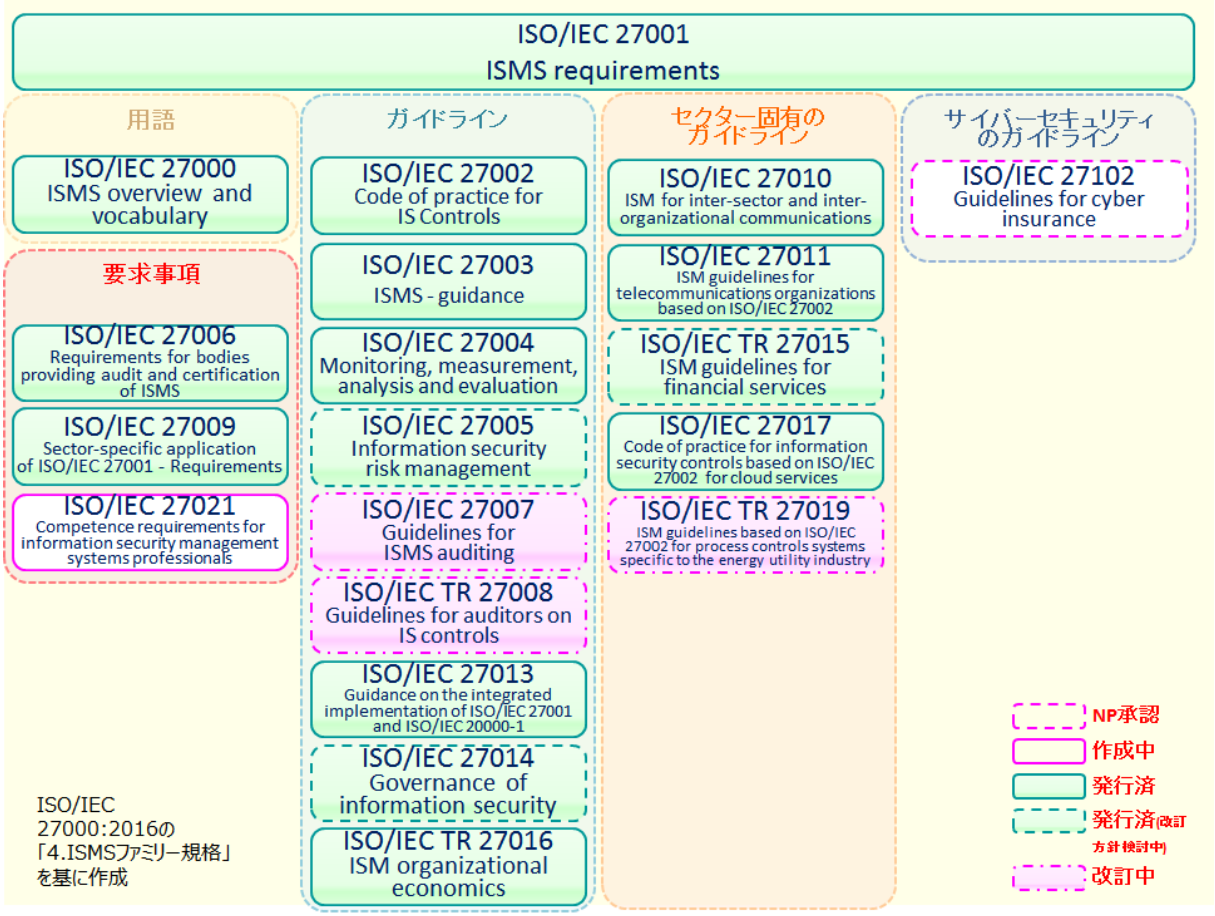
2017 年 5 月 31 日

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、9 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 27000:2016

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

2016 年 2 月発行［第 4 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。

※ 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。

2017 年 4 月ハミルトン会議にて、2016 年 3 月以降に発行された 27000 ファミリー規格（27003 等）に対応するための改訂開始が決定された。

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。

*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［第 2 版］
Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation
2016 年 12 月発行
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 27005:2011
Information technology – Security techniques – Information security risk management
2011 年 6 月発行［第 2 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。
これを受けて、現在、改めて SP（Study Period）を設置し、design specification（今後の改訂の方針、方向性等）を検討中である。

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、2012 年 9 月に JIS Q 27006:2012（JIS Q 27006:2008 の改正版）として制定された。（ISO/IEC 27006:2015 に対応した JIS は、現在改正中。）

JIS Q 27006:2012
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。

ISO/IEC 27007:2011

Information technology – Security techniques – Guidelines for information security management systems auditing
2011 年 11 月発行（現在、改訂審議中）
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。

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。

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。

現在実施中の改訂審議の中で、第 2 版では適用範囲の変更とともに標題が以下に変更されることになった。
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

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。

ISO/IEC 27011:2016

Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

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。

ISO/IEC 27014:2013

Information technology – Security techniques –Governance of Information security

2013 年 4 月発行

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。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 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 投票を実施することになった。

ISO/IEC TR 27015:2012

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

2012 年 11 月発行

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ることになった。

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

クラウドサービスにおける ISO/IEC 27002 に基づく情報セキュリティ管理策の実践のための規範を提供する規格

ISO/IEC TR 27019:2013

Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

2013 年 7 月発行（現在、改訂審議中）

エネルギー業界向けプロセス制御システムのための ISO/IEC 27002 に基づく情報セキュリティマネジメントに関する技術報告書

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 に変更することになった。

ISO/IEC 27021（作成中）

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

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（作成決定）
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。

3. 第 54 回 ISO/IEC JTC 1 SC 27/WG 1 会議の結果概要

第 54 回 WG 1 会儀は、2017 年 4 月 18 日～22 日にハミルトン（ニュージーランド）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 審議中。
※行の色分け：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*	
		第 54 回会議 （今回：2017 年 4 月）	第 55 回会議 （次回予定：2017 年 10-11 月）
ISO/IEC 27000	概要及び用語	IS[第 4 版] （IS）	IS[第 4 版] （改訂開始）
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]* *（SP）*	*IS[第 2 版]* *（SP）*
ISO/IEC 27003	ISMS の手引	IS[第 1 版] （改訂中：FDIS）	IS[第 2 版] （IS）
ISO/IEC 27004	監視、測定、分析及び評価の手引	IS[第 2 版] （IS）	IS[第 2 版] （IS）
ISO/IEC 27005	*リスクマネジメントに関する指針*	*IS[第 2 版]* *（SP）*	*IS[第 2 版]* *（SP）*
ISO/IEC 27006	認証機関に対する要求事項	IS[第 3 版]	IS[第 3 版]
ISO/IEC 27007	監査の指針	IS[第 1 版] （DIS）	IS[第 1 版] （FDIS）
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] （2nd PDTS）	TR[第 1 版] （2nd PDTS）
ISO/IEC 27009	セクター規格への 27001 適用に関する要求事項	IS	IS （改訂開始）
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	電気通信組織のための指針	IS[第 2 版] （IS）	IS[第 2 版] （IS）
ISO/IEC 27012	電子政府サービスのための ISMS 指針	ー	ー
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]	IS[第 2 版]
ISO/IEC 27014	情報セキュリティのガバナンス	IS[第 1 版] （SP）	IS[第 1 版] （NP）
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	TR[第 1 版] （廃止）	TR[第 1 版] （廃止）
ISO/IEC TR 27016	情報セキュリティマネジメントー組織の経済的側面(Organizational economics)	TR[第 1 版]	TR[第 1 版]
ISO/IEC 27017	クラウドサービスにおける ISO/IEC 27002 に基づく情報セキュリティ管理策の実践のための規範	IS	IS
ISO/IEC TR 27019	エネルギー業界向けプロセス制御システムのための ISO/IEC 27002 に基づく ISM の指針	TR[第 1 版] （DIS）	TR[第 1 版] （FDIS）
ISO/IEC 27021	ISMS 専門家の力量に関する要求事項	DIS	FDIS
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 27102	サイバー保険のための指針	NP	WD

ISO 規格策定の段階は、次のとおり
NP → WD → CD → DIS → FDIS → IS（発行済）
NP： New work item Proposal
WD： Working Draft
CD： Committee Draft
DIS： Draft International Standard
FDIS： Final Draft for International standard
IS： International Standard

TR/TS 規格策定の段階は、次のとおり。
TR： PDTR → TR
TS： NP → WD → PDTS → TS
TR：Technical Report（技術報告書）
TS：Technical Specification（技術仕様）
PDTR/PDTS：Proposed Draft Technical Report/ Specification
※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に先立って、改訂方針等について検討されます。

3-2 主なプロジェクトの進捗状況

27002 （SP Design specification for the revision of ISO/IEC 27002:2013）

27002 改訂に先立って Design specification（改訂方針）を策定するために 2016 年 4 月に設置された 12 か月間の SP である。
主に構成について審議された。会議に先立って様々な構成案が提出されており、審議されたが結論に至らず、最終的に残った 2 つの構成案をもとに次回会議にて改めて検討することになった。そのため、SP を 6 か月間延長することになった。

27003 （Information security management system – Guidance）

前回タンパ会議後に開始された FDIS 投票の結果、IS に進むことが承認され、2017 年 4 月に第 2 版として発行された。

27005（SP Design specification for the revision of ISO/IEC 27005:2011）

27005 改訂に先立って Design specification（改訂方針）を策定するために 2016 年 4 月に設置された 12 か月間の SP である（2013 年 10 月に開始された改訂プロジェクトはいったんキャンセルされた）。
審議の結果、SP を 6 か月間延長し、引き続き改訂方針について検討することになった。

27005：2011（Defect Report）

前回タンパ会議における Defect Report 審議の結果を受けて発行された Draft Corrigendum（正誤票案）について、事前に実施された投票では、反対国は 2 か国（英国、日本）※だけであった。審議の結果、賛成多数で正誤票案を若干更新し発行することになった。

※正誤票の元々の主旨は、現行規格の ISO/IEC 27001:2005 に関連する記述を、ISO/IEC 27001:2013 に沿って修正することだった。
一方で、正誤票案の中では ISO/IEC 27001:2005 に関連する記述について編集上の削除・更新（例：箇条名称の更新）などは行われているが、内容については追加・更新されておらず、ISO/IEC 27001:2013 対応の修正としては不十分なことから日本としては反対した。

27007 （Guidelines for information security management systems auditing）

事前に実施された DIS 27007 に対する投票では、反対国は 3 か国（オーストラリア、英国、日本）であり、コメントは約 160 件だった。編集会議ではこれらのコメントに基づいて審議し、最終的に各国のコメントの主旨が反映されたことから、オーストラリア、英国、日本とも賛成に転じ、FDIS に進むことになった。

27008 （Guidelines for the assessment of information security controls）

事前に実施された 2nd PDTS に対する投票では、反対は 3 か国（オーストラリア、ニュージーランド、日本）であり、コメントは約 280 件であった。編集会議ではこれらのコメントに基づいて審議し、最終的に各国のコメントの主旨が反映されたことから、オーストラリア、ニュージーランド、日本とも賛成に転じ、コメントを反映したテキストを確認することになった。

27009 （Draft Corrigendum／Defect Report）

前回タンパ会議の結果を受けて発行された Draft Corrigendum（正誤票案）について事前に実施さ

れた投票では、反対国は 3 か国（オーストラリア、フランス、米国）であった。このうち、オーストラリア、米国からは別途寄書（Defect Report など）が提出されていた。

まず正誤票案について審議されたが、コメントの一部が Defect Report の内容とも関連していたことから、Defect Report 審議も統合して実施した。このなかで、ISO/IEC 27009 の意図を読みとりやすくし、また、テンプレート（Annex A）を使いやすくする必要があるとのコメントがあった。

こうしたコメントを受けて、審議の結果、正誤票の発行はとりやめ、早期改訂を実施するための手続を実施することになった。

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、国際規格の必要性について議論されました。その結果、以下の文書を作成することになりました。

・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

・各国サイバーセキュリティ関連の基準等と ISO・IEC 規格の関連を示す参考文書
名称： SD 27103 Cybersecurity and ISO and IEC Standards
※ SD は SC 27 の内部文書であるため、今後 TR 27103 として作成予定。

上記の他、サイバーセキュリティについて幅広く検討するための SP が設置され、サイバーセキュリティの定義、概念、要件などについても検討が進められています。
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