ISO/IEC 27000 ファミリーについて

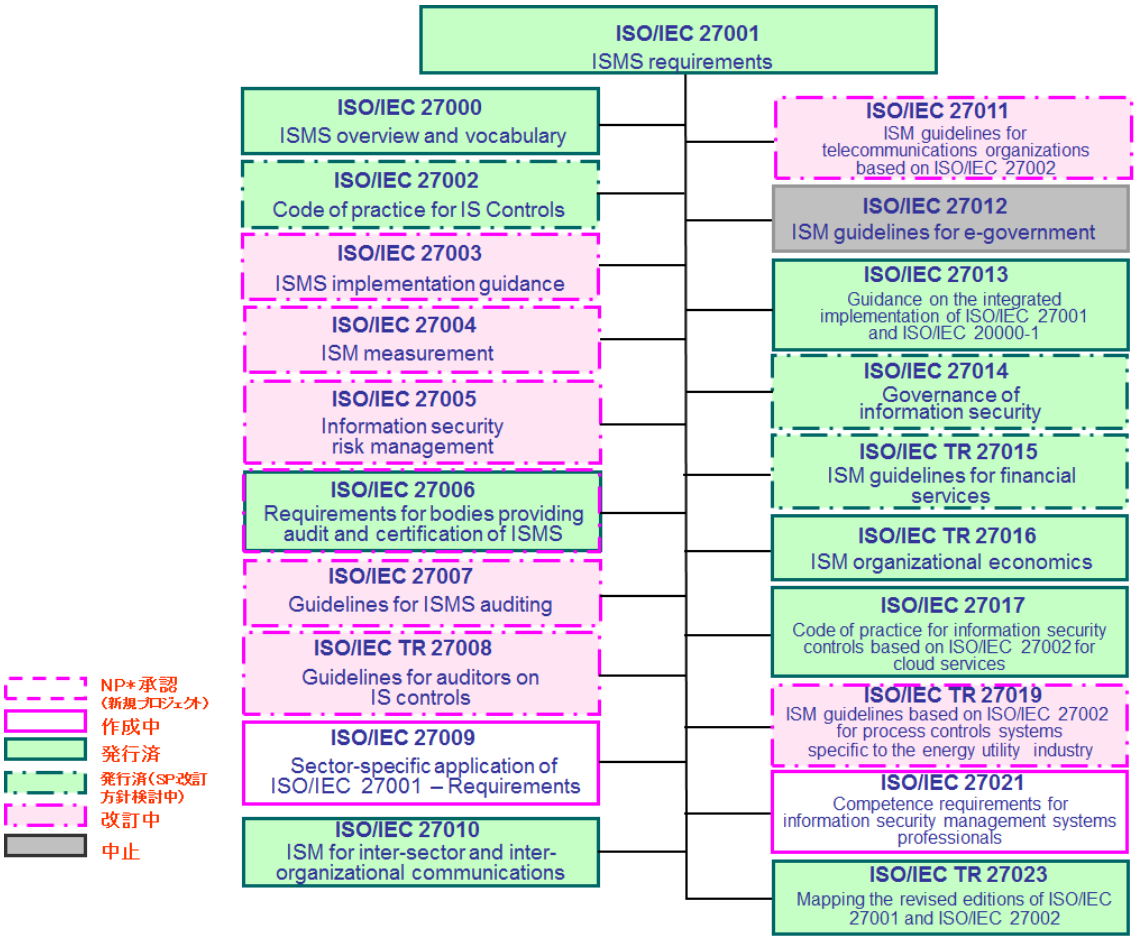
2016 年 6 月 13 日
(改 2016 年 6 月 17 日)

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分野固有の手引）から構成されています。

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。それらの名称等を下記に示します。



*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、8 ページをご参照下さい。
*SP：Study Period のことであり、SP では新プロジェクトの設置等が検討されます。

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

なお、SC 27 で作成されている 27000 ファミリーは、現時点では 27000～27040 番台となっております。

・規格の概要

前図の「作成中」及び「発行済」(「改訂中」含む）規格の概要は、以下の通りです。

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)。

2010 年 4 月開催のマラッカ会議で改訂開始が決定され、第 2 版として 2012 年 12 月に発行された。なお､その際に 27001 改訂､27002 改訂に対応した改訂も並行して審議され､2014 年 1 月に ISO/IEC 27001:2013 及び ISO/IEC 27002:2013 に対応した第 3 版として発行された。

2014 年 10 月メキシコ会議にて DIS 段階以降に進んだ規格(27006 等)の用語掲載のための早期改訂、及び DIS 投票開始の承認のための手続きを実施することが決定された。この結果、DIS から開始する迅速法による早期改訂が決定され、2016 年 2 月に第 4 版として発行された。

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)。

2008 年 10 月リマソール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。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。）

2008 年 10 月リマソール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。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、まずは 12 か月間の Study Period（SP：新プロジェクトの設置等の検討）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。

ISO/IEC 27003:2010
Information technology – Security techniques – Information security management system implementation guidance
2010 年 2 月発行（現在、改訂審議中）
ISMS の実装（計画から導入まで）に関するガイダンス規格

2012 年 10 月ローマ会議後に開始された NP 投票の結果を受けて、2013 年 5 月ソフィアアンティポリス会議にて早期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 – Information security management system – Guidance

ISO/IEC 27004:2009
Information technology – Security techniques – Information security management – Measurement
2009 年 12 月発行（現在、改訂審議中）
導入された ISMS 及び管理策（群）の有効性を評価するための測定に関するガイダンス規格

2012 年 5 月ストックホルム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 – Information security management －Monitoring, measurement, analysis and evaluation

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 月に発行後、2010 年 4 月マラッカ会議にて、ISO 31000:2009 及び ISO Guide 73:2009 との整合に限定した改訂を、（ISO/IEC 27001:2005 対応版として）通常よりも早い改訂プロセスを適用

して行うことが決定された。これを受けた改訂作業を経て、2011 年に改訂版（第 2 版）が発行された。
2013 年 5 月ソフィアアンティポリス会議後に開始された NP 投票の結果を受けて、2013 年 10 月インチョン会議にて早期改訂開始が決定された。
2016 年 4 月タンパ会議にて、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、12 か月間の SP（Study Period）を設置し、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。

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 改正については未発行。）
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

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 月シンガポール会議にて 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た。これを受けた改訂作業を経て、2011 年に第 2 版が発行された。
その後、2012 年 5 月ストックホルム会議にて、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

ISO/IEC 27009（作成中）
Information technology – Security techniques – Sector specific application of ISO/IEC 27001 - requirements
セクター規格を作成する組織に対する、27001 適用について規定する規格。

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。

2014 年 10 月メキシコ会議にて ISO/IEC 27001:2013 対応のための早期改訂、及び DIS 投票開始の承認のための手続きを実施することが決定された。この結果、DIS から開始する迅速法による、早期改訂が決定された。これを受けた改訂作業を経て、2015 年に第 2 版が発行された。

ISO/IEC 27011:2008
Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
2008 年 12 月発行（現在、改訂審議中）
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。

2013 年 5 月ソフィアアンティポリス会議後に開始された NP 投票の結果を受けて、2013 年 10 月インチョン会議にて改訂開始が決定された。

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 SC7/WG25（IT Service management）と連携して作成された。

2013 年 5 月ソフィアアンティポリス会議後に開始された NP 投票の結果を受けて、2013 年 10 月インチョン会議にて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 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、まずは 12 か月間の Study Period（SP：新プロジェクトの設置等の検討）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。

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。

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
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。
2013 年 7 月発行（現在、改訂審議中）

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。

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 年に 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。

2. ISO/IEC 27000 ファミリー規格の検討状況

前図に示す ISO/IEC 27000 ファミリーの検討は、年 2 回（春・秋）開催される SC 27 の WG 1（情報セキュリティマネジメントシステム）において進められています。
第 52 回 WG 1 会議は、2016 年 4 月 11 日～15 日にタンパ（米国）にて開催されました。
この会合での検討状況は次の 2-1 のとおりです。

2-1 第 52 回 SC 27/ WG 1 会議における検討状況（全体）

*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、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	第 52 回会議（今回:2016 年 4 月）	第 53 回会議（次回予定 : 2016 年 10 月）
ISO/IEC 27000	概要及び用語	IS[第 4 版]（IS）	IS[第 4 版]（IS）
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]	IS[第 2 版]（SP）
ISO/IEC 27003	導入に関する手引	IS[第 1 版]（改訂中：DIS）	IS[第 1 版]（改訂中/6 月会議）
ISO/IEC 27004	測定	IS[第 1 版]（改訂中：DIS）	IS[第 1 版]（改訂中/6 月会議）
ISO/IEC 27005	リスクマネジメントに関する指針	IS[第 2 版]（5th WD）	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]（3rd WD）	IS[第 1 版]（CD）
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]（3rd WD）	TR[第 1 版]（PDTS）
ISO/IEC 27009	セクター規格への 27001 適用に関する要求事項	FDIS	IS
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 1 版]（改訂中：FDIS）	IS[第 1 版]（改訂中：FDIS）
ISO/IEC 27012	電子政府サービスのための ISMS 指針	－	－
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]	IS[第 1 版]（SP）
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]	TR[第 1 版]（SP）
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	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] [2nd WD]	TR[第 1 版] [CD]
ISO/IEC 27021	ISMS 専門家の力量に関する要求事項	3rd WD	CD
ISO/IEC TR 27023	ISO/IEC 27001 及び ISO/IEC 27002 改訂版のマッピング	IS	IS

*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

*なお、TR/TS 規格策定の段階は、次のとおり。
NP → WD → PDTR/PDTS → DTR/DTS → TR/TS
※Technical Report：技術報告書

NP：	New work item Proposal
WD：	Working Draft
PDTR：	Proposed Draft Technical Report
DTR：	Draft Technical Report
TR：	Technical Report
TS:	Technical Specification
※SP	Study Period

2-2 第 52 回 SC 27/ WG 1 会議における検討状況（詳細）

ー主要プロジェクト進捗状況

27000 Information security management systems – Overview and vocabulary

前回会議の検討結果を受けて、ISO/IEC 27000:2016（4th edition）が、2016 年 2 月に発行された。

27001 Defect Report

今回の会議に先立って、イタリアから２件の defect report が提出されおり、審議を行った。その結果、27001 の不正確な適用につながるような重要な内容ではないことから、Technical Corrigenda（正誤票）は発行しないことになった。一方で、今回のように修正について議論された箇所については、次回改訂のためのインプットとして記録を残していくことになった。

27001 Periodical Review（定期レビュー）

ISO のルールに従って、規格発行から 3 年後の periodical review（定期レビュー）が実施され、今回の会議にて審議された。その結果、改訂した場合、（まだ 27001 移行終了後から間もないため）市場に混乱をきたす可能性があること等が考慮され、全会一致で今回は confirm（維持ー改訂は見送り）することになった。

27002 Periodical Review（定期レビュー）

ISO のルールに従って、規格発行から 3 年後の periodical review（定期レビュー）が実施され、今回の会議にて審議された。その結果、技術の進歩に対応するため等の理由から改訂する方向となった。そのために、まず 12 か月間の SP（Study Period）を設置して、design specification（改訂の方針・方向性等）について検討し、その後改訂プロジェクトを開始することになった。

27003 Information security management system – Guidance

今回の会議に先立って行われた DIS 27003 に対する DIS 投票は、投票期限が 5 月 11 日であり、まだ投票期間中だったため、審議はなかった。

そのため、6 月下旬にロンドンで DIS 審議のための BCM 会議（Ballot Consulting Meeting）が開催される予定である。

27004 Information security management systems ー Monitoring, measurement, analysis and evaluation

今回の会議に先立って行われた DIS 27004 に対する DIS 投票は、投票期限が 5 月 5 日であり、まだ投票期間中だったため、審議はなかった。

そのため、6 月下旬にロンドンで DIS 審議のための BCM 会議が開催される予定である。

27005 Information security risk management

今回の会議に先立って、4th WD 27005 に対して、約 300 件のコメントが寄せられた。
編集会議の初日において、出席者による多数決を行った結果、（技術的なコメント数が依然として多くテキストがまだ不十分である等の理由から）賛成多数でプロジェクトキャンセルとなった。

これを受けて、12 か月間の SP（Study Period）を設置し、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。

27007 Guidelines for information security management systems auditing

今回の会議に先立って、3rd WD に対して約 110 件のコメントが寄せられており、編集会議ではこれらのコメントに基づいて審議した。なお、附属書 A（ISMS 監査実施の手引）については、前回会議の結果に従い、日本及び英国提案による修正案が採用されており、これについての審議となった。

今回の編集会議の結果、次回は、CD に進むことになった。

27008 Information technology - Security techniques - Guidelines for the assessment of information security controls

今回の会議に先立って、2nd WD に対して約 160 件のコメントが寄せられており、これらのコメントに基づいて審議した。

今回の審議の結果、文書の種類を 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り、これに伴い適用範囲変更の手続も実施することになった。

今回の編集会議の結果、次回は PDTS（Proposed Draft Technical Specification）が発行される見込みである。

27009 Sector specific application of ISO/IEC 27001 - requirements

今回の会議に先立って行われた FDIS 投票では、反対 1 か国（オーストラリア）のみであった。
編集会議では、エディタの準備したコメント対処案に基づいて審議を行った。
今回の編集会議の結果、IS が発行されることになった。

以上