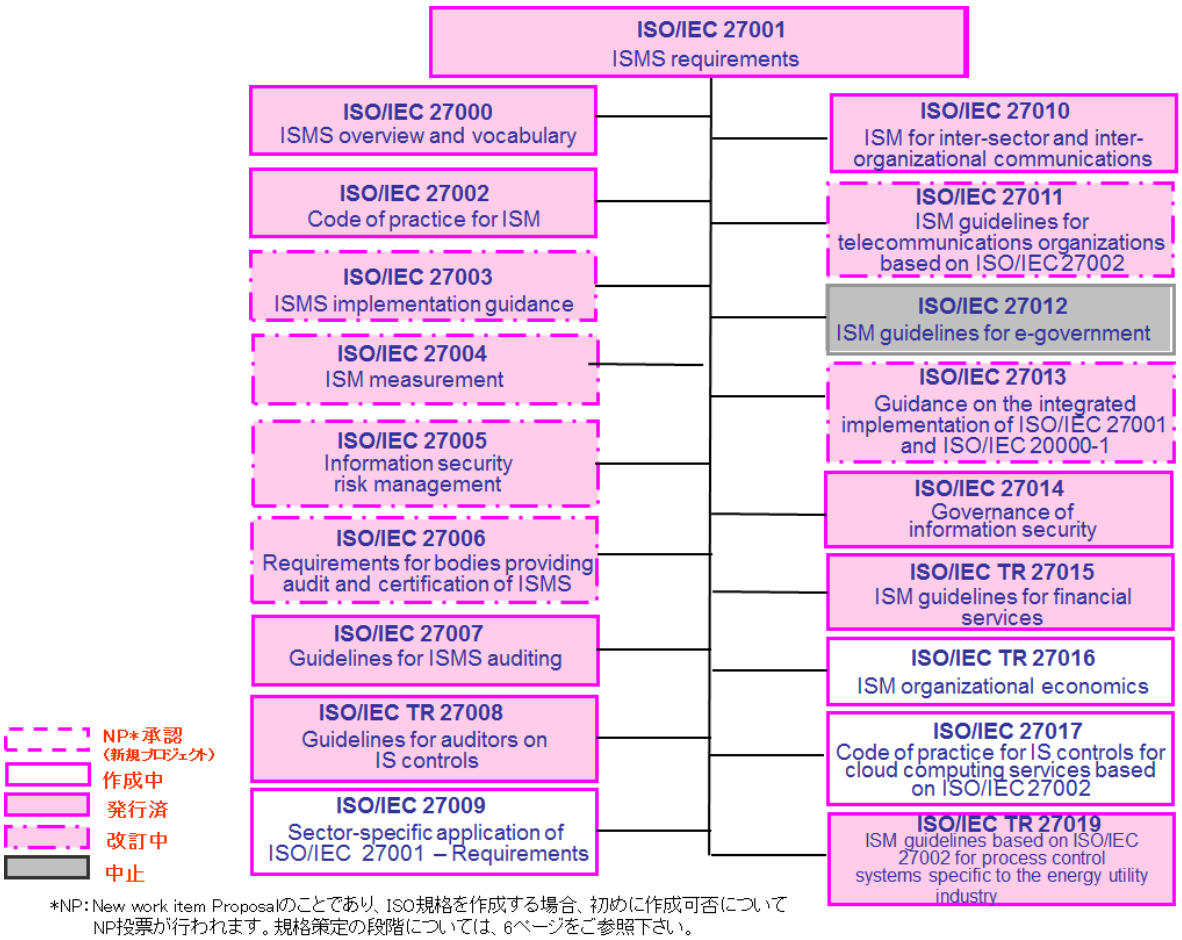
ISO/IEC 27000 ファミリーについて

2013 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 JTC1（情報技術）の分化委員会 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。以下に示すように、要求事項である ISO/IEC 27001 をはじめ、ISO/IEC 27000 ファミリーとして様々な規格が検討され、発行されています。



*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、6ページをご参照下さい。

・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 27000:2012

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

2012 年 12 月発行［第 2 版］（現在、改訂審議中）

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

ISO/IEC 27001:2005 及び ISO/IEC 27002:2005 に対応した改訂版が、2012 年 12 月に発行された。なお、ISO/IEC 27001:2013、ISO/IEC 27002:2013 に対応した改訂版については、2013 年 10 月に審議が終了し、近日中に第 3 版として発行予定である。

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､2006 年 5 月に JIS Q 27001:2006 として制定されており､ISO/IEC 27001:2013 発行に伴い、現在改正中である。

JIS Q 27001:2006（現在、改正中）

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

ISO/IEC 27002:2013

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

2013 年 10 月発行［第 2 版］

情報セキュリティマネジメントの確立、実施、維持及び改善に関する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､2006 年 5 月に JIS Q 27002:2006 として制定されており､ISO/IEC 27002:2013 発行に伴い、現在改正中である。

JIS Q 27002:2006（現在、改正中）

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の実践のための規範

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 systems －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］（改訂決定）
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改訂開始が決定された。

ISO/IEC 27006:2011

Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems
2011 年 12 月発行［第 2 版］（現在、改訂審議中）
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。

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 年に改訂版が発行された。
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。

ISO/IEC 27007:2011

Information technology – Security techniques – Guidelines for information security management systems auditing
2011 年 11 月発行
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。

ISO/IEC TR 27008:2011
Information technology – Security techniques – Guidelines for auditors on information security controls
2011 年 10 月発行
組織の情報セキュリティの管理策のレビューに関するガイドライン（TR：Technical Report）。

ISO/IEC 27009（作成中）
Information technology – Security techniques – The use and application of ISO/IEC 27001 for sector/service-specific third-party accredited certifications
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。
2013 年 10 月インチョン会議にて、規格標題を以下に変更することになった。
Sector specific application of ISO/IEC 27001 - requirements

ISO/IEC 27010:2012
Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications
2012 年 4 月発行
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。

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（改訂決定）
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 27013:2012
Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
2012 年 10 月発行（改訂決定）
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。

ISO/IEC 27014:2013
Information technology – Security techniques –governance of Information security
情報セキュリティのガバナンスに関する規格。
2013 年 4 月発行

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のガイドライン規格。

ISO/IEC TR 27016（作成中） Information technology – Security techniques – Information security management – Organizational economics 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（Technical Report）。
ISO/IEC 27017（作成中） Information technology – Security techniques – Information security management -- Code of practice for information security controls for cloud computing services based on ISO/IEC 27002 クラウドコンピューティングサービスにおける 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

2. ISO/IEC 27000 ファミリー規格の検討状況

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 47 回 WG 1 会議は、2013 年 10 月 21 日～25 日にインチョン（韓国）にて開催されました。この会合での検討状況は以下のとおりです。

※ SC 27 総会は年 1 回開催されており、この総会の報告については、一般社団法人 情報処理学会 情報規格調査会様の Web サイトにて公開されています。
一般社団法人 情報処理学会 情報規格調査会：http://www.itscj.ipsj.or.jp/index.html

2-1 第 47 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）ーIS 発行済だが、現在改訂中で DIS 審議
※緑色の網掛けセルは発行済規格、灰色の網掛けセルは中止プロジェクトです。

ISO/IEC 番号	規格内容	第 47 回会議（2013 年 10 月）	第 48 回会議（2014 年 4 月）
ISO/IEC 27000	概要及び用語	IS[第 2 版]（改訂中：DIS）	IS[第 3 版] [SP]
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]
ISO/IEC 27003	導入に関する手引	IS[第 1 版]（改訂中：1st WD）	IS[第 1 版]（改訂中：2nd WD）
ISO/IEC 27004	測定	IS[第 1 版]（改訂中：1st WD）	IS[第 1 版]（改訂中：2nd WD）
ISO/IEC 27005	リスクマネジメントに関する指針	IS[第 2 版]（改訂検討）	IS[第 2 版]（WD）
ISO/IEC 27006	認証機関に対する要求事項	IS[第 2 版] (改訂中：3rd WD)	IS[第 2 版] (改訂中：CD)
ISO/IEC 27007	監査の指針	IS[第 1 版]	IS[第 1 版]
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]	TR[第 1 版]
ISO/IEC 27009	セクター規格への 27001 適用に関する要求事項	1st WD	2nd WD
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 1 版]	IS[第 1 版]
ISO/IEC 27011	電気通信組織のための指針	IS[第 1 版]（改訂検討）	IS[第 1 版]（改訂中：WD）
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き	IS[第 1 版]（改訂検討）	IS[第 1 版]（改訂中：WD）
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]
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]
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)	DTR	TR
ISO/IEC 27017	クラウドコンピューティングサービスにおける 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	5th WD	CD
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：Fast Track	TR [SP]

*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※規格策定の段階は、次のとおり。
NP → WD → PDTR → DTR → TR
※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
※SP	Study Period

2-2 第 47 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

前回会議を受けて、27001:2013 及び 27002:2013 対応のための 27000 改訂（3rd edition）文書である DIS について投票が行われた。この DIS 投票では、賛成 32 カ国、反対 0 カ国、棄権 7 カ国であり、技術的なコメントは 1 件であった。

今回の編集会議の結果、反対投票がなく、また技術的なコメントについても次回改訂に対するコメントと確認されたことを受けて、FDIS を省略して IS を発行することになった。

なお、27000 の今後の改訂方法等については、引き続き SP（Study Period）で検討予定。

27001、27002 新旧対比表（SC27/WG1 SD3）

27001、27002 改訂版が 2013 年 10 月に発行された。その新旧対比表について WG1 内で審議されており、このたびこの対比表を SC27 のウェブサイトで閲覧可能とすることになった。

この結果を受けて、ISO/IEC JTC 1/SC 27 N13143「JTC 1/SC 27/SD3 – Mapping Old-New Editions of ISO/IEC 27001 and ISO/IEC 27002」が、以下で公開されている。なお、この文書の Introduction にあるとおり、この中で示されている対応は、2005 年版と 2013 年版の内容が同一であることを意味するわけではない（1 対 1 の対応ではない）ことに留意が必要である。

http://www.jtc1sc27.din.de/cmd?level=tpl-bereich&languageid=en&cmsareaid=wg1sd3

27003 Information security management system implementation guidance

今回の会議に先立って、1st WD 27003 に対して約 140 件のコメントが寄せられた。
編集会議では、適用範囲、規格構成、規格標題などについて議論された。審議の結果、適用範囲については、網羅性のある文書にすべきという日本の主張が受け入れられ、（導入・実施[implementation]だけでなく）確立、実施、維持及び継続的改善（establishing, implementing, maintaining and continually improving）すべてを対象とすることが合意された。規格の構成については、27001 の構成に合わせるべきとの方向で次の WD を作成することになった。こうした議論に多くの時間を費やし、コメント審議は行われなかったため、Meeting Report を発行することが決定された。

なお、適用範囲の変更を受けて、規格標題も「Information security management systems ー guidance」に変更することになった。

今回の編集会議の結果、次回は 2nd WD を発行することになった。

27004 Information security management – Measurement

今回の会議に先立って、1st WD 27004 に対して約 100 件のコメントが寄せられた。
編集会議では、寄せられた各国コメントを集約した文書が発行されており、この文書に基づいて進められた。特に、適用範囲、規格標題等について議論された結果、適用範囲については 27001 の 9.1 監視、測定、分析及び評価（monitoring, measurement, analysis and evaluation）を対象とすることで合意された。この適用範囲の変更を受けて、規格標題も「Information security management systems ーmonitoring, measurement, analysis and evaluation」に変更すること

になった。

今回の編集会議の結果、次回は 2nd WD を発行することになった。

27005 Information security risk management

今回の会議に先立って、早期改定の可否に関する NP 投票が実施された。この NP 投票では、賛成 23 カ国、反対 2 カ国（スイス、米国）、棄権 13 カ国であり、この結果を受けて早期改訂が決定された。今回の会議では、主に適用範囲について審議されたが結論が出ず、次回会議にて再度審議することになった。

今回の編集会議の結果、次回は WD を発行することになった。

27003、27004、27005 合同会議（Coordination meeting）

今回、27005 の改訂開始も決定されたことを受けて、27003、27004、27005 合同会議を開催した。この会議では、主に 27003、27004、27005 の適用範囲について審議され、各規格の適用範囲を明確にする必要性があることが合意された（適用範囲の詳細については、上記の各規格の項目を参照）。また、この 3 規格が 27001 を支援する文書であることについて合意された。

今回の審議の結果、このような場は必要であり、今後も継続して実施することになった。

27006 Requirements for bodies providing audit and certification of information security management systems

今回の会議に先立って、3rd WD 27006 に対して約 230 件のコメントが寄せられた。
編集会議では、前回に引き続き、7.資源に関する要求事項の力量部分と附属書 C 審査工数、及び 17021 と重複すると思われる部分に加えて、27001、27002 との整合に関して議論された。
7 章については、9 章、附属書 B、附属書 E にも散見している力量に関する内容の整理を求めるコメントが多く寄せられ、これらのコメントに基づいて力量の要求事項を 7 章に集約して再構成することになった。

附属書 C 審査工数については、主に審査工数の算定の起点について審議され、その結果、ドイツ提案を出発点として複数の要因とその係数を考慮したアプローチで再検討することになった。そのため、前回決定された Normative への変更については、いったん informative へ戻し、内容によってどちらとするかを今後検討していくことになった。

17021 と重複すると思われる部分に関しても議論され、コメントに基づいて審議した結果、重複部分は削除し、また、17021 にはないが IS 固有ではない部分については 17021 改訂 WG に提案することになった（提案が受け入れられれば、27006 から削除予定）。
また、27001:2013、27002:2013 が発行されたことから、コメントに基づいて関連する要求事項が更新された。

今回の編集会議の結果、本文の構成が安定していることから、次回は CD を発行することになった。

27009 The use and application of ISO/IEC 27001 for sector/service-specific third-party accredited certifications

前回の会議にて NP 投票が承認されたことを受けて、1st WD 27009 が発行されており、この WD に対して約 90 件のコメントが寄せられた。
編集会議では、この規格の適用範囲（対象）について大きな議論となり、この規格の対象は 1）ISMS を導入する組織、2）認証機関・認定機関、3）セクター規格を作成する組織、のいずれであるかについて審議された。この 3 択について投票となり、その結果、対象は 3）セクター規格を作成する組織となった。

また、規格標題についても適用範囲に合わせて「Sector specific application of ISO/IEC 27001 - requirements」に変更することになった。
その後、コメントに基づきテキストを改善する審議が行われ、すべてのコメント審議が終了した。

今回の編集会議の結果、次回は 2nd WD を発行することになった。

以上