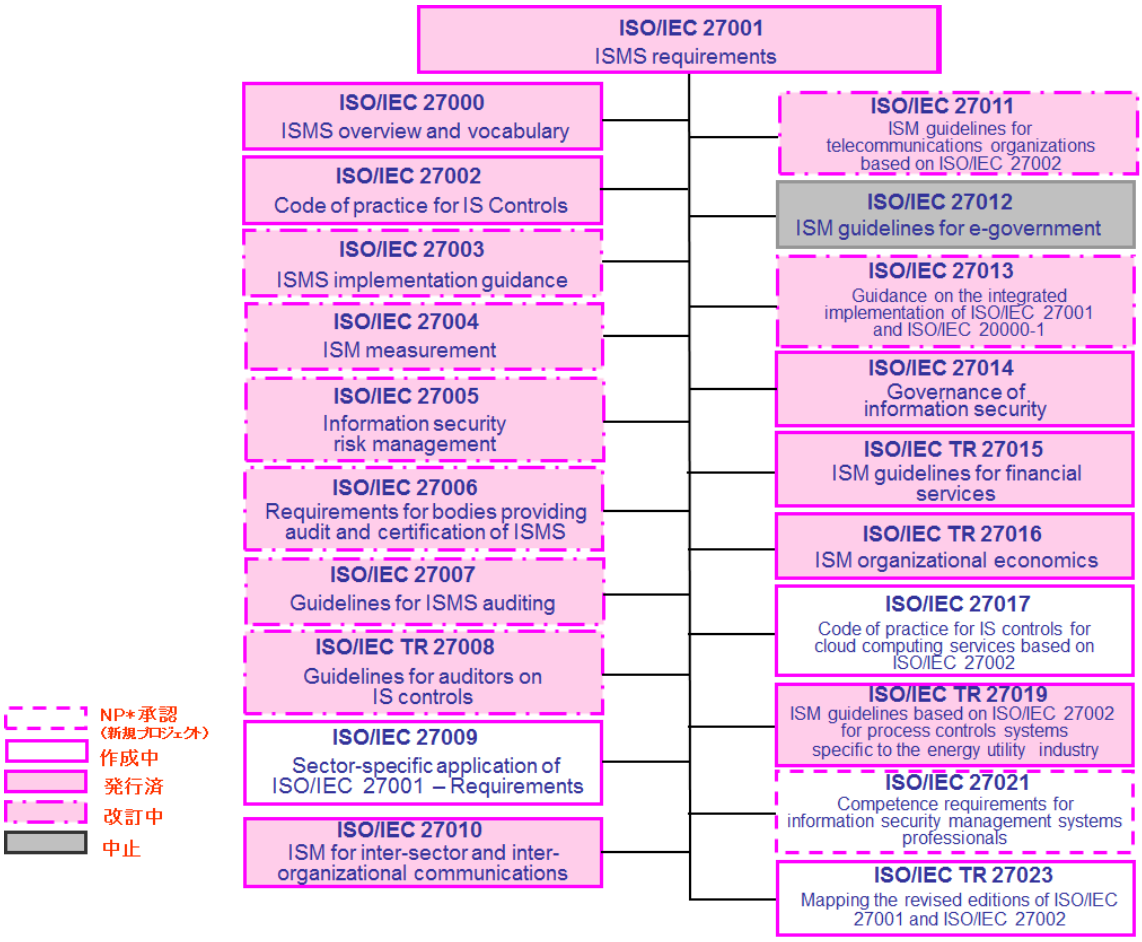
ISO/IEC 27000 ファミリーについて

2014 年 12 月 8 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、7 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 27000:2014

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

2014 年 1 月発行［第 3 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)。

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 正誤票は現在作成中)。

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 月に改訂版が発行された。

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 正誤票は現在作成中)。

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 月に改訂版が発行された。

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。

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（改訂決定）

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（改訂決定）

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。

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 27010:2012

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。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。

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 27013:2012
Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
2012 年 10 月発行（現在、改訂審議中）
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。
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（作成中）
Information technology – Security techniques – 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

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（作成開始） 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 2014 年 4 月香港会議後に開始された NP 投票の結果を受けて、2014 年 10 月メキシコシティ会議にて作成が開始されることになった。
ISO/IEC TR 27023（作成開始－発行予定） Information technology -- Security techniques -- Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002 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。現在、発行に向けて ISO にて準備中。

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 49 回 WG 1 会議は、2014 年 10 月 20 日～24 日にメキシコシティ（メキシコ）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。

※ 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 49 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
※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 49 回会議 （2014 年 10 月）	第 50 回会議 （2015 年 5 月）
ISO/IEC 27000	概要及び用語	IS[第 3 版] （SP）	IS[第 3 版] （SP、改訂決定）
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：3rd WD）	IS[第 1 版] （改訂中：1st CD）
ISO/IEC 27004	測定	IS[第 1 版] （改訂中：3rd WD）	IS[第 1 版] （改訂中：1st CD）
ISO/IEC 27005	リスクマネジメントに関する指針	IS[第 2 版] （2nd WD）	IS[第 2 版] （3rd WD）
ISO/IEC 27006	認証機関に対する要求事項	IS[第 2 版] (改訂中：2nd CD)	IS[第 2 版] (改訂中：DIS)
ISO/IEC 27007	監査の指針	IS[第 1 版] （改訂決定）	IS[第 1 版] （WD）
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] （改訂決定）	TR[第 1 版] （WD）
ISO/IEC 27009	セクター規格への 27001 適用に関する要求事項	CD	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 1 版]	IS[第 1 版] （改訂決定）
ISO/IEC 27011	電気通信組織のための指針	IS[第 1 版] （改訂中：CD）	IS[第 1 版] （改訂中：2nd CD）
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 1 版] （改訂中：CD）	IS[第 1 版] （改訂中：DIS）
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)	TR[第 1 版]	TR[第 1 版]
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	2nd CD	DIS
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 [SP]	TR [SP、改訂決定]
ISO/IEC 27021	ISMS 専門家の力量に関する要求事項	NP	WD
ISO/IEC TR 27023	ISO/IEC 27001 及び ISO/IEC 27002 改訂版のマッピング	DTR (fast track)	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※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 49 回 SC 27/ WG 1 会議における検討状況（詳細）

－主要プロジェクト進捗状況

27000 Information security management systems – Overview and vocabulary

これまでの会議から継続して議論されている、27000 の今後の改訂方法等に関する課題の解決に向けて、SP（Study Period）を延長することになった。

また、27006 及び 27010 の用語を掲載するための短期間での改訂を SP と並行して行うことになり、DIS から開始する方向となった。ただし，これら 2 つの規格が所有する用語の追加を検討するだけの限定改訂とする見込みである。

27001、27002 Defect Report

前回会議で 27001、27002 ともに、Technical Corrigenda（正誤票）を発行することになったため、前回会議終了後にこの発行に係る投票を行った。その結果、発行について可決され、９月末に Technical Corrigenda が発行された。

関連 URL：　http://www.isms.jipdec.or.jp/27001_27002_seigo.html

27003 Information security management system – Guidance

今回の会議に先立って、3rd WD 27003 に対して約 500 件のコメントが寄せられた。

編集会議では、コメントに基づいて記述内容の大幅な改善が図られた。

今回の編集会議の結果、文書の構成が安定したこと、及び開発スケジュールを考慮して、次回は CD を発行することになった。

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

今回の会議に先立って、3rd WD 27004 に対して約 100 件のコメントが寄せられた。

今回の会議では構成を変更しない方針で審議を進めたため、結果として構成は安定し、また各国コメントも前向きに審議されたことから、次回は CD 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、2nd WD 27005 に対して、約 390 件のコメントが寄せられた。

エディタの提案により、主要（Major）な論点約 60 件と却下（Reject）対象約 10 件を中心に審議が進められた。編集会議では、構成の変更も含めて審議された。また ISO 31000 との整合については、現在 TC 262 で ISO 31000 を改訂中であり（現在、CD 31000）、TC 262 会議が 12 月に開催予定のため、その結果を待って対応を図ることになった。

今回の編集会議の結果、次回は 3rd WD を発行することになった。

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

今回の会議に先立って行われた 2nd CD 27006 に対する CD 投票では、賛成 14 か国、コメント付賛成 6 か国（日本含む）、反対 4 か国（スウェーデン、オーストリア、スイス、オランダ）、棄権 16 か国であり、コメント総数は約 200 件であった。

編集会議では、Annex B～F に（反対国の）主要なコメントが多く寄せられたことから、まずこれらの Annex について審議された。その結果、Annex の整理統合が行われた。

附属書 C（審査工数）については、前回の審議結果に基づき normative（必須）部分と informative（参照）部分の両方が含まれていることに対して、別々の附属書にすべきというコメントがあり審議した結果、附属書 C を 2 つに分割し、normative（必須）部分の附属書（審査工数表含む）と informative（参照）部分の附属書（算出方法の例示等）として、2 つの附属書にすることになった。
全てのコメント処理が終了し、審議での改善を受けて反対国のうちスイス、オーストリアは賛成に転じた（オランダは欠席）。
今回の編集会議の結果、次回は DIS を発行することになった。

27007 Guidelines for information security management systems auditing
2011 年に第 1 版が発行されており、前回会議にて 3 年ごとの定期レビューにより改訂の可否を審議した結果、改訂を開始することになった。
これに基づき、今回の会議に先立って実施された現行版に対する寄書募集に対して、ドイツからコメントが提出されており、基本的にはこのコメントを受け入れることで、次回は WD を発行することになった。

27008 Guidelines for auditors on information security controls
2011 年に第 1 版が発行されており、前回会議にて 3 年ごとの定期レビューにより改訂の可否を審議した結果、改訂を開始することになった。
これに基づき、今回の会議に先立って現行版に対する寄書募集が実施されたが、特にコメントはなかった。今回の会議では、改訂の主旨等や進め方について審議された結果、エディタが WD を作成し、改訂に着手することになった。

27009 Sector specific application of ISO/IEC 27001 - requirements
今回の会議に先立って行われた 1st CD 27009 に対する CD 投票では、賛成 14 か国、コメント付賛成 5 か国（日本含む）、反対 2 か国（イギリス、ルクセンブルク）、棄権 19 か国であり、コメント総数は約 160 件であった。
コメントに基づき審議を進めた結果、本文、附属書（分野別規格作成のためのテンプレート）とともに内容がより明確になった。また、この改善を評価して、反対国は 2 か国とも賛成に転じた。
一方で全体的に大幅な内容変更となったため、DIS には進まず、次回は 2nd CD に進むことになった。これに伴い、スケジュール延長の手続きを実施することになった。

以上