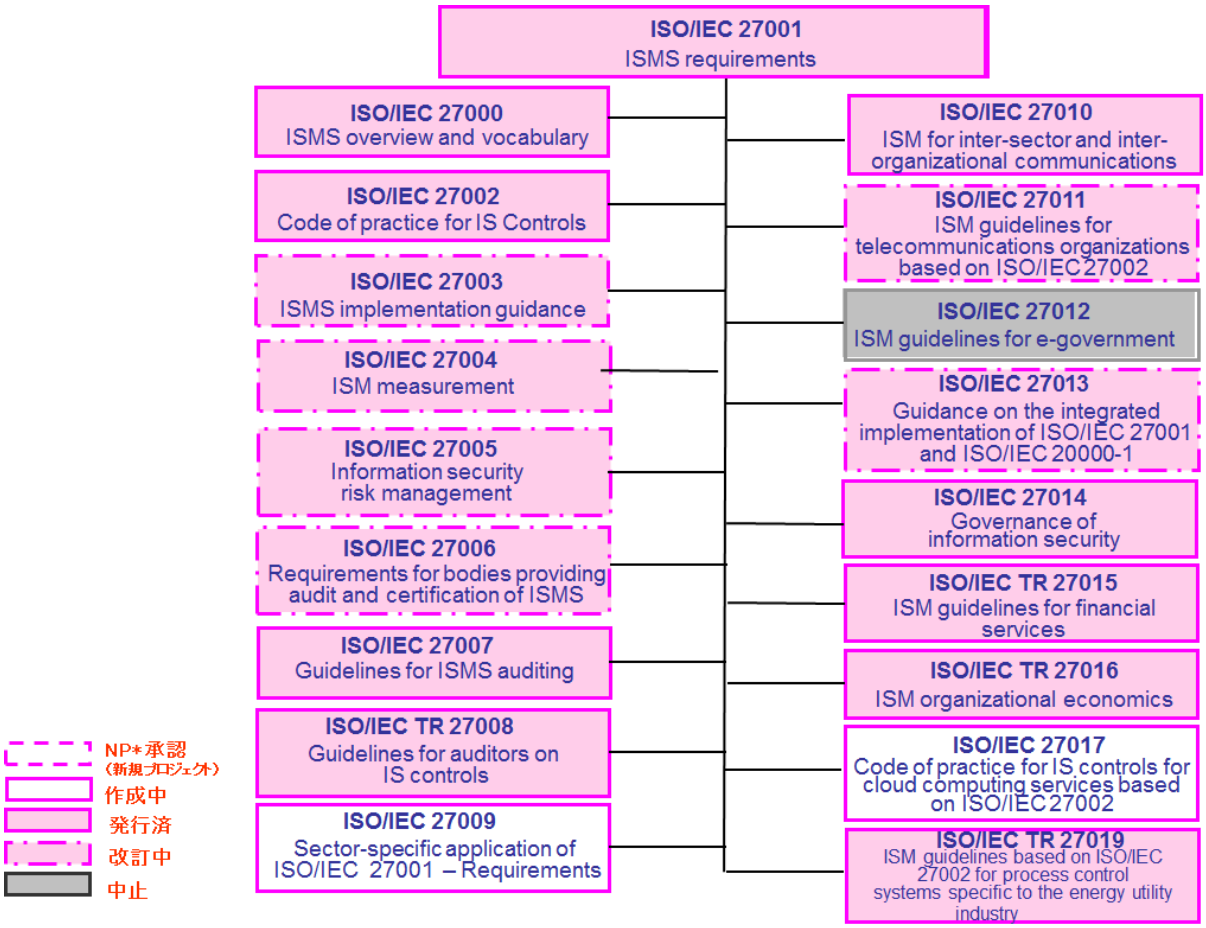
ISO/IEC 27000 ファミリーについて

2014 年 6 月 4 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 27000:2014

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

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

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

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 48 回 WG 1 会議は、2014 年 4 月 7 日～11 日に香港（中国）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 48 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 48 回会議（2014 年 4 月）	第 49 回会議（2014 年 10 月）
ISO/IEC 27000	概要及び用語	IS[第 3 版] [SP]	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：2nd WD）	IS[第 1 版] （改訂中：3rd WD）
ISO/IEC 27004	測定	IS[第 1 版] （改訂中：2nd WD）	IS[第 1 版] （改訂中：3rd WD）
ISO/IEC 27005	リスクマネジメントに関する指針	IS[第 2 版] （WD）	IS[第 2 版] （2nd WD）
ISO/IEC 27006	認証機関に対する要求事項	IS[第 2 版] (改訂中：CD)	IS[第 2 版] (改訂中：2nd CD)
ISO/IEC 27007	監査の指針	IS[第 1 版]	IS[第 1 版] （改訂決定）
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] （改訂決定）
ISO/IEC 27009	セクター規格への 27001 適用に関する要求事項	2nd WD	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]
ISO/IEC 27011	電気通信組織のための指針	IS[第 1 版] （改訂中：WD）	IS[第 1 版] （改訂中：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：WD）	IS[第 1 版] （改訂中：CD）
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	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	CD	2nd 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 [SP]	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 48 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

スウェーデンからの寄書及び，日本及び英国からのコメント処理を行い，27000 の今後の改訂方法等に関する課題の整理を行った結果、SP（Study Period）を延長し、引き続き 27000 の運用管理等について検討していくことになった。

27001、27002 Defect Report

2013 年 10 月に発行された 27001 の 8.1.1（管理策）、及び 27002 の 8.1.1（管理策）、8.1.3（実施の手引）、7.1.2（実施の手引）について、オーストラリアより Defect Report が提出されており、審議を行った。その結果、オーストラリアの提案に基づき、該当箇所の"Assets associated with information and information processing facilities"という表現に Information が含まれるように修正を行うこととし、Technical Corrigenda（技術修正票）を発行することになった。

27003 Information security management system – Guidance

今回の会議に先立って、2nd WD 27003 に対して約 350 件のコメントが寄せられた。
編集会議では、適用範囲の変更が採用された。その他、全てのコメント審議を行い、これらのコメントに基づいて内容的な修正も多く採用された。

今回の編集会議の結果、内容的な変更も多かったことから、次回は 3rd WD 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、2nd WD 27004 に対して約 80 件のコメントが寄せられた。
編集会議では、5.3 Meeting 27001 Requirements について、スウェーデンから提案された 27001 の 9.1 と 27004 の実施事項をマッピングした概要図と、日本提案のテキスト変更を合わせて検討し、これに基づき 2nd WD 27004 の 5.3 を変更することになった。また、27004 内での measure、measurement、metrics の使用方法について各国からコメントがあり、整理されることになった。
今回の編集会議の結果、多くのコメントが採用されたが、エディタ預かりとなったものも多かったことから、次回は 3rd 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、1st WD 27005 に対して約 100 件のコメントが寄せられた。
編集会議では、前回に引き続き適用範囲について審議され、その結果、27005 は 27001 だけでなく、27000 ファミリー全般を対象としたものにする方向とすることで合意された。また、ISO 31000 との整合をとることについても基本的に合意された。なお、一部のコメントの審議が終了せず、次回会合で審議されることになった。

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。

27006 Requirements for bodies providing audit and certification of information security management systems
今回の会議に先立って、1st CD 27006 に対して（これまでの会議からの持越し分も含め）約 230 件のコメントが寄せられた。
編集会議では、主に附属書 C について審議された。スウェーデンからの提案をもとに審議を行った結果、審査工数表*、審査工数算出時に考慮すべき要因、その要因を必ず考慮して審査工数を算出すること、及び審査工数表からの削減の割合を Normative（必須）とすることとし、一方でその具体的な算出方法については、例示（Informative）とすることになった。
*審査工数表は、まずは 2011 年版を出発点とし、内容は今後検討予定。
また、本文については、DIS 17021 との整合化はエディタが対応することとなり、テキストの記載箇所の移動を求めるコメントなど多くのコメントもエディタ預かりとなった。編集会議では、それ以外のコメントについて審議を行った。
今回の編集会議の結果、附属書 C（審査工数）を 1st CD 27006 から大幅に変更したため、次回は 2nd CD 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、2nd WD 27009 に対して約 120 件のコメントが寄せられた。
編集会議では、適用範囲に対してコメントが複数寄せられており、前回会議に引き続き再度審議、変更された。また、4 章と 5 章についてコメントも多く、審議された結果、箇条 4 は 27001 要求事項（本文）の拡張等についての規格開発者向け要求事項及び指針を、箇条 5 は 27001 附属書 A／27002 の管理策の拡張等についての規格開発者向け要求事項及び指針を示すことになった。また、箇条 4、箇条 5 に対応するセクター別規格作成に際してのテンプレートを、それぞれ別の附属書として含めることになった。
今回の編集会議の結果、すべてのコメント審議が終了し、次回は 1st CD を発行することになった。

以上