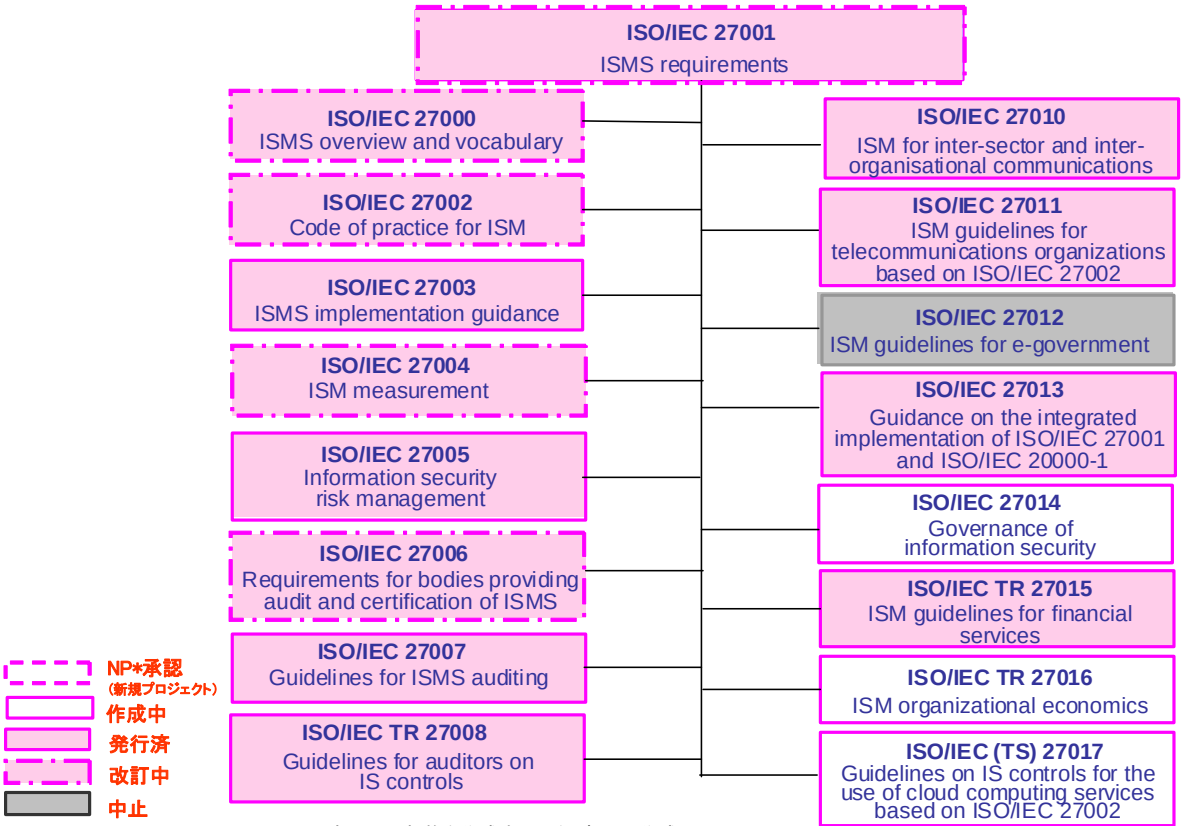
ISO/IEC 27000 ファミリーについて

2012 年 12 月 10 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、5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（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、現在改訂中の 27001、27002 に対応した改訂も並行して審議中である。

ISO/IEC 27001:2005

Information technology – Security techniques – Information security management systems – Requirements

2005 年 10 月発行（現在、改訂審議中）

組織の事業リスク全般を考慮して、文書化した ISMS を確立、導入、運用、監視、レビュー、維持及び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 として制定された。

JIS Q 27001:2006

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 27002:2005 （旧番号ISO/IEC 17799:2005*）

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

2005 年 6 月発行（現在、改訂審議中）

情報セキュリティマネジメントの導入、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 として制定された。

JIS Q 27002:2006

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

ISMS の実装（計画から導入まで）に関するガイダンス規格

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。

ISO/IEC 27005:2011

Information technology – Security techniques – Information security risk management

2011 年 6 月発行
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。

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（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。

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。
※ 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 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 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
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。

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
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。

ISO/IEC 27014（作成中）
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。

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。
2011 年 10 月ナイロビ会議にて、今後の方針として TR（Technical Report）とすることで合意された。この Status 変更（IS から TR）については、会議後に Letter Ballot が実施され、TR とすることになった。

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 (TS) 27017（作成中）
Information technology – Security techniques – Information security management -- Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002
ISO/IEC 27002 に基づくクラウドサービス利用のための情報セキュリティ管理策に関するガイドライン規格　（TS:Technical Specifications）

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 45 回 WG 1 会議は、2012 年 10 月 22 日～26 日にローマ（イタリア）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 45 回SC 27/ WG 1 会議における検討状況（全体）

※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

ISO/IEC 番号	規格内容	第 45 回会議（2012 年 10 月）	第 46 回会議（2013 年 4 月）
ISO/IEC 27000	概要及び用語	IS（改訂中:DIS）	IS（IS、次期改訂検討）
ISO/IEC 27001	要求事項	IS（改訂中:3rd CD）	IS（改訂中:DIS）
ISO/IEC 27002	情報セキュリティマネジメントの実践のための規範	IS（改訂中:1st CD）	IS（改訂中:DIS）
ISO/IEC 27003	導入に関する手引	IS	IS
ISO/IEC 27004	測定	IS（改訂開始）	IS（WD）
ISO/IEC 27005	リスクマネジメントに関する指針	IS（第 2 版）	IS（第 2 版）
ISO/IEC 27006	認証機関に対する要求事項	IS (改訂中:1st WD)	IS (改訂中:2nd WD)
ISO/IEC 27007	監査の指針	IS	IS
ISO/IEC TR 27008	IS 管理策に関する監査員のための指針	TR	TR
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	IS
ISO/IEC 27011	電気通信組織のための指針	IS	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き	FDIS	IS
ISO/IEC 27014	情報セキュリティのガバナンス	FDIS	FDIS
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	DTR	TR
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)	4th WD	PDTR
ISO/IEC (TS) 27017	ISO/IEC 27002 に基づくクラウドサービス利用のための情報セキュリティ管理策に関する指針	3rd WD	4th 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

*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

2-2 第 45 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

前回会議の結果、現行版の ISO/IEC 27001：2005、ISO/IEC 27002:2005 に基づく 27000 改訂（今回の改訂）版を早期に発行するために、DIS に進むことになった。
これと同時に、改訂版 27001/27002（現在改訂作業中）に基づく改訂（次期改訂）については、改訂版 27001/27002 発行（現在作業中）と同時期に発行できるよう、Study Period を開始して今回の改訂作業と並行して審議を行うことになった。

この結果を受けて行われた DIS 投票では、賛成 38 カ国、コメント付賛成 2 カ国、反対 1 カ国（スウェーデン）、棄権 9 カ国であり、コメント総数は約 21 件であった。
編集会議では、反対国（スウェーデン）が自国の投票について次期改訂に対するものであったことから投票訂正の意を表したため、反対国は 0 となった。コメント処理でも、technical なものは今回の改訂ではなく次期改訂に関するものであったため、次期改訂で処理することとなった。その結果、今回の改訂については反対につながるコメントがないことを確認し、編集会議では全 NB の承認を得た。
WG1 全体会議では、この編集会議の結果を受けて、FDIS を省略して IS を発行することが承認された。この結果、ISO/IEC 27001：2005、ISO/IEC 27002:2005 に基づく改訂（今回の改訂）版である ISO/IEC 27000:2012-12-01（2nd edition）が、2012 年 12 月に発行された。

また、次期改訂の Study Period（SP）に寄せられたコメントについては、別途セッションが開催された。この改訂については、27001/27002 改訂版発行と同時に発行できるよう、引き続き SP にて検討することになった。

27001 Information security management systems – Requirements

CD 投票では、賛成 17 カ国、コメント付賛成 10 カ国、反対 5 カ国（オーストラリア、フィンランド、日本、南アフリカ、英国）、棄権 7 カ国であり、コメント総数は約 320 件であった。
前回のストックホルム会議と同様に、今回の編集会議でも、リスクアセスメント・リスク対応を、箇条 6（6 Planning）と箇条 8（8 Operation）のどちらに記載するかについて大きく議論が分かれた。最終的には、箇条 6 に記載することになり、この議論についてはこれで収束することが合意された。

マネジメントシステム共通化規格（MSS）（ISO 補足指針［2012 年第 3 版］の附属書 SL 版）については、主にオーストラリアから寄せられた、テキストを ISMS に沿った明確・正確なものにするよう求める提案により、いくつかの deviation（変更）が加えられた。これらの deviation（変更）は、その理由(justification)とともに ISO/TMB に報告することとなった。

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。

27002 Code of practice for information security management

今回の会議では、前回のストックホルム会議での 1st CD 27002 に対する未処理コメントについて引き続き審議された。

編集会議では、ISO の規格作成期間に関するルール上の制約もあり、DIS 向けテキスト作成を目標に作業が行われた。この中で、主に審議すべき重要な事項を中心に議論され、構成を含めてテキスト全体の作成作業が行われた。

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。

27004 Information security management – Measurement

次回会議に向けて、エディタから各国に対して ISO/IEC 27004:2009 との互換性や測定対象に関する質問表が発行されることになった。この質問表に寄せられる各国コメントをエディタが集約し、次回会合に向けての文書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 WD 27006 に対して約 60 件のコメントが寄せられた。
編集会議では、特に Annex C Audit time（附属書 C 審査工数）に関して議論され、Annex C を更新する必要があることについて合意された。また、構成上、細分箇条（X.X.X）のレベルで 17021 と整合していないため混乱が生じていることから、細分箇条も 17021 に合わせるというコメントについて審議され、合意された（主に 7 章と 9 章）。
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