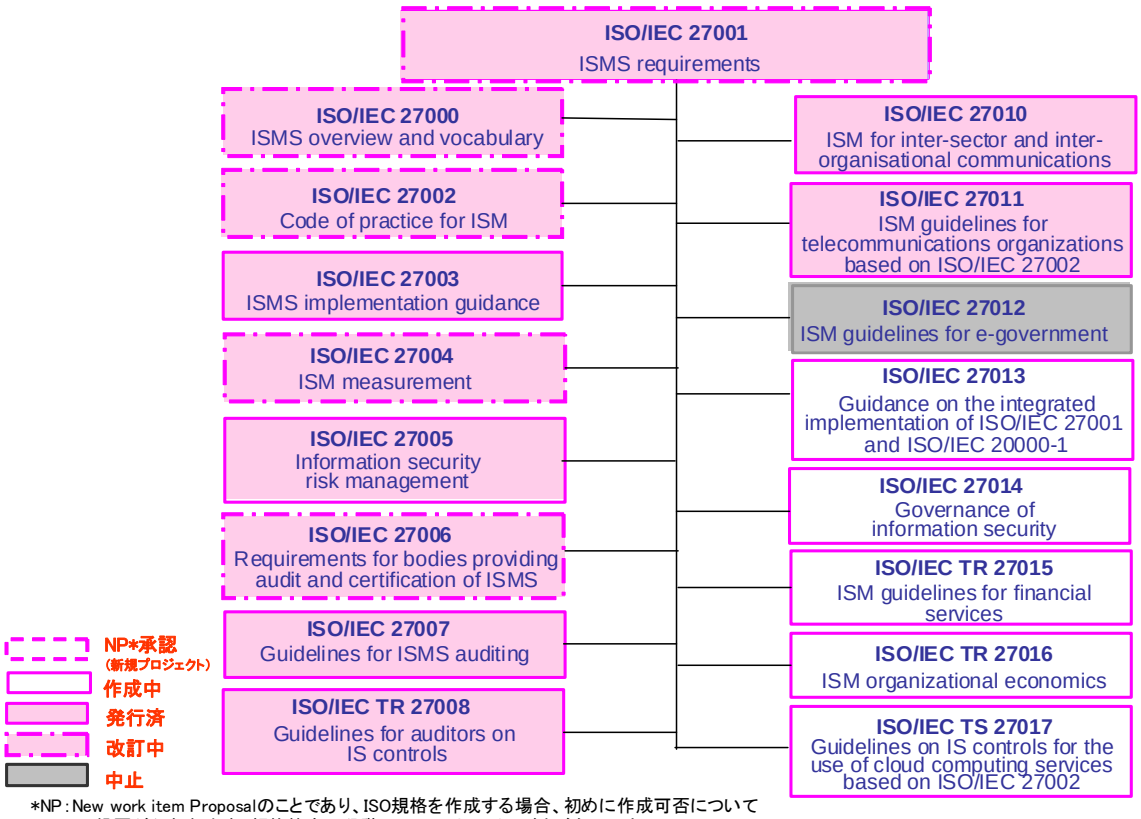
ISO/IEC 27000 ファミリーについて

2012 年 6 月 27 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 27000:2009

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

2009 年 5 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

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（定期レビュー審議後、改訂決定）

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

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。

※（ISO/IEC 27006:2007 の）国内規格としては、2008 年 9 月に JIS Q 27006:2008 として制定された。ISO/IEC 27006:2011 については、現在、JIS 化が行われている。

JIS Q 27006:2008

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（作成中）
Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
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）と連携して進められている。

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（作成中）
Information technology – Security techniques – Information security management guidelines for financial services
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

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 44 回 WG 1 会議は、2012 年 5 月 7 日～11 日にストックホルム（スウェーデン）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 44 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 44 回会議 （2012 年 5 月）	第 45 回会議 （2012 年 10 月）
ISO/IEC 27000	概要及び用語	IS （改訂中:1st CD）	IS （改訂中:DIS）
ISO/IEC 27001	要求事項	IS （改訂中:2nd CD）	IS （改訂中:3rd CD）
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:1st CD）
ISO/IEC 27003	導入に関する手引	IS	IS
ISO/IEC 27004	測定	IS	IS （改訂開始）
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 （第 2 版）	IS (改訂中:1st 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	DIS	FDIS
ISO/IEC 27014	情報セキュリティのガバナンス	DIS	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	PDTR	DTR
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)	3rd WD	4th WD
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	2nd WD	3rd 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 44 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

CD 投票では、賛成 20 カ国、コメント付賛成 6 カ国、反対 2 カ国（日本、英国）、棄権 12 カ国であり、コメント総数は約 60 件であった。

編集会議では、これまで現行版の ISO/IEC 27001：2005、ISO/IEC 27002:2005 に基づく改訂に関するもの（Rev.1）と、改訂版 27001/27002（現在改訂作業中）に基づく改訂（Rev.2）に関するものとに区別して審議されたが、今回それぞれの発行時期についても検討された。

この結果、現行版の ISO/IEC 27001：2005、ISO/IEC 27002:2005 に基づく 27000 改訂版（Rev.1）を早期に発行するために、DIS に進むことになった。
改訂版 27001/27002（現在改訂作業中）に基づく改訂（Rev.2）については、改訂版 27001 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 Rev.1 と並行して審議を行うことになった。

上記のとおり、今回の編集会議の結果、DIS を発行することになった。

27001 Information security management systems – Requirements

CD 投票では、賛成 16 カ国、コメント付賛成 12 カ国、反対 7 カ国（オーストラリア、フィンランド、日本、ポーランド、南アフリカ、スイス、英国）、棄権 6 カ国であり、コメント総数は約 330 件であった。
ISO/TMB JTCG TF1 で作成されていたマネジメントシステム共通化規格（MSS）については、2012 年 3 月に ISO/IEC Directives（ISO/IEC 専門業務用指針）の Supplement（ISO 補足指針）［2012 年第 3 版］※の Annex SL（附属書 SL）として公開された。

このため、27001 編集会議に先立って、WG1 全体で MSS への対応について検討された。その結果、27001 ではこの Supplement（ISO 補足指針）［2012 年第 3 版］の Annex SL（附属書 SL）版を適用し、その適用ルールに従って、必要な場合には MSS に deviation（変更）を加えることを認める方向で合意された。

27001 編集会議では、この WG1 での決定に従って、これまで保留されていた MSS テキストに対するコメントも含めて審議が進められた。審議の中では、リスクアセスメント・リスク対応について箇条 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、投票により箇条 6 に記載することになった。

今回の編集会議ではすべてのコメント審議には至らず、5 月 31 日～6 月 1 日の 2 日間にわたって、interim meeting（virtual meeting で実施）を開催することになった（この interim meeting にて、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 3rd CD を発行することになった。

※ 次の URL で公開されています。

http://www.iso.org/iso/standards_development/processes_and_procedures/iso_iec_directives_and_iso_supplement.htm

この中の”ISO Supplement, Procedures specific to ISO” （Supplement - Procedures specific to ISO (the "ISO Supplement") 3rd edition）です。

この文書の”Annex SL(normative) Proposals for management system standards”が該当箇所です。

MSS（マネジメントシステム規格）の共通構成については、Annex SL の” Appendix 3

(normative) High level structure, identical core text, common terms and core definitions”をご参照ください。27001 改訂版も、原則この構成となる予定です。
（今後、9001、14001 等、他の MS 規格も、原則としてこの枠組みが適用される見込みです。）

27002 Code of practice for information security management
CD 投票では、賛成 14 カ国、コメント付賛成 11 カ国、反対 6 カ国（オーストラリア、日本、ポーランド、スイス、英国、米国）、棄権 9 カ国であり、コメント総数は約 720 件であった。

今回の会議では、管理目的及び管理策の構成について集中的に審議を行い、この結果、構成についての議論を収束することが合意された。すべてのコメント審議には至らず、多くのコメントが未処理となったことから、次回は次の CD を発行せずに、今回の審議結果を反映した暫定的なドラフトを発行し、次回会議で継続して今回未処理のコメント審議を行うことになった。

そのため、次回会議に向けてのドラフトの版の更新は行われず、1st CD の未処理コメントについて引き続き審議されることになった。

27004 Information security management – Measurement
今回の会議に先立って、5 年毎の ISO 定期レビューの一環である Pre-review（改訂の可否に関する）投票が行われ、これを受けて WG1 Plenary にて審議された。この結果、改訂を開始することとなった（日本としては、現在 ISO/IEC 27001 及び ISO/IEC 27002 が改訂中であり、その確定を待つべきあるとして反対した）。

27006 Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27006:2007 は、IAF によって ISO/IEC 17021:2011 の移行期間が 2012 年 2 月までと定められたことを受けて、ISO/IEC 17021:2011 との整合に限定した早期改訂を行った。
なお、改訂方針として、27006 改訂版の発行後、ISO/IEC17021 の systematic review に合わせて、27006 も systematic review を開始することが盛り込まれた（コメント審議では、ISMS 固有部分に関するコメントは systematic review で審議することし、今回は保留となった）。
この結果、ISO/IEC 27006:2011（Second edition 2011-12-01）が発行された。

この後、今回のストックホルム会合に先立って、上記 systematic review（改訂）を開始するか否かについての 60 日間投票が行われた。
60 日間投票の結果は、賛成 24 カ国、反対 1 カ国（日本）、棄権 15 カ国であった（日本は、改訂自体には賛成だが、17021 改訂がまだ開始されていないことから、改訂開始を 17021 改訂開始後とすべき（従って、現時点での改訂開始には反対）というコメントを提出した）。

編集会議では、今回の投票で賛成多数であったため systematic review（改訂）を開始するが、27006 改訂スケジュールについては、27006 改訂版発行が 17021 改訂版発行後となるよう調整をとることになった。

この改訂開始の決定を受けて、ナイロビ会議にて保留となった ISMS 固有部分に対するコメント、及び今回新た寄せられたコメント約 60 件の審議を行った。
今回の編集会議の結果、WD を発行することになった。

以上