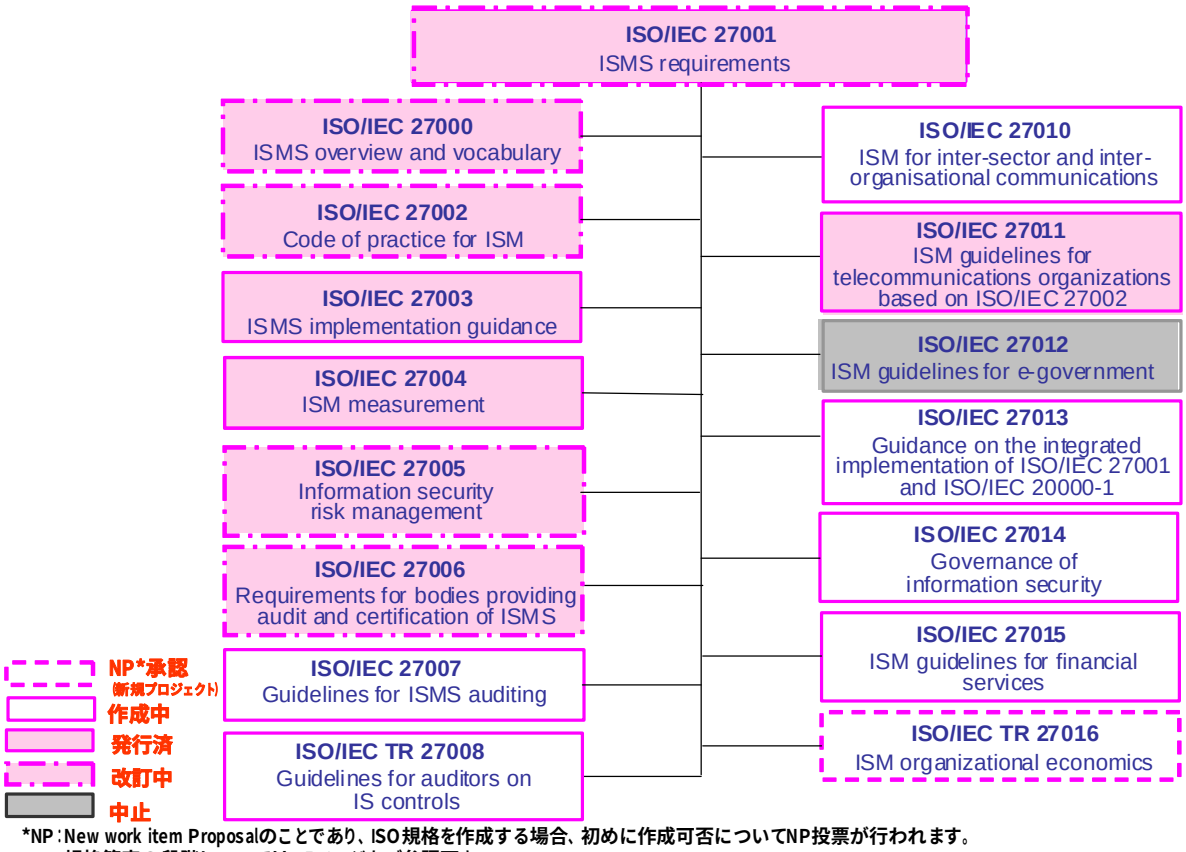
ISO/IEC 27000 ファミリーについて

2010 年 12 月 3 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

上図の「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**

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**

ISO/IEC 27005:2008

Information technology – Security techniques – Information security risk management

2008 **年** 6 **月発行（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

ISO/IEC 27006:2007

Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems

2007 年 3 月発行（2010 年 10 月開催のベルリン会議で改訂開始が決定された）

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、2008 年 9 月に JIS Q 27006:2008 として制定された。

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（作成中）

Information technology – Security techniques – Guidelines for information security management systems auditing

ISMS 監査の実施に関するガイダンス規格。

ISO 19011（品質及び／又は環境マネジメントシステム監査のための指針－現在マネジメントシステム監査のための指針として改訂中）に加えて、ISMS 固有のガイダンスを提供する内容となる予定。

ISO/IEC TR 27008（作成中）

Information technology – Security techniques – Guidelines for auditors on information security controls

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ダンス規格。

TR（Technical Report）規格。

ISO/IEC 27010（作成中）

Information security management for inter-sector and inter-organisational communications

業界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 – 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る予定。

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 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。

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 41 回 WG 1 会議は、2010 年 10 月 4 日～8 日にドイツ（ベルリン）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 41 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

規格番号	規格内容	第 41 回会議（2010 年 10 月）	第 42 回会議（2011 年 4 月）
ISO/IEC 27000	概要及び用語	IS（改訂: WD）	IS（改訂 2nd WD）
ISO/IEC 27001	要求事項	IS（改訂 3rd WD）	IS（改訂 4th WD）
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 2nd WD）	IS（改訂 3rd WD）
ISO/IEC 27003	導入に関する手引	IS	IS
ISO/IEC 27004	測定	IS	IS
ISO/IEC 27005	リスクマネジメントに関する指針	IS（早期改訂:FCD）	IS（FDIS）
ISO/IEC 27006	認証機関に対する要求事項	IS（改訂開始決定）	IS（改訂審議）
ISO/IEC 27007	監査の指針	3rd CD	FCD
ISO/IEC TR 27008	IS 管理策に関する監査員のための指針	PDTR	DTR
ISO/IEC 27010	業界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	3rd WD	1st CD
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	2nd WD	3rd WD
ISO/IEC 27014	情報セキュリティのガバナンス	3rd WD	1st CD
ISO/IEC 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ガイドライン	(1st WD)	2nd WD
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)	(NP)	1st WD

*ISO 規格策定の段階は、次の通り
NP → WD → CD → FCD → FDIS → IS（発行済）

NP： New work item Proposal
WD： Working Draft
CD： Committee Draft
FCD： Final Committee Draft
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

◆ISO JTC1 Directives（ISO JTC1 専門業務用指針）の改訂について
ISO JTC1 の規格策定プロセスを定めた ISO JTC1 Directives（ISO JTC1 専門業務用指針）が改訂された。
これに伴い、今後の規格策定プロセスに対し、移行期間を設けて新指針を適用することとなった。

2-2 第 41 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

前回のマラッカ会議にて、通常の期間による改訂を行うことが決定された。これを受けて WD が発行されており、今回の編集会議ではこの文書に対する審議を行った。
なお、WG4 の規格を含めるか否かについては、まずは WG4 内での検討結果を待つことになった。
今回の編集会議の結果、次の版は 2nd WD を発行することになった。

27001 Information security management systems – Requirements

1st WD に対して、約 200 件のコメントが寄せられた。前回、審議延期となった Annex A に関するコメントについても審議された。Annex A を現状通り維持することに関して議論となったが、最終的には投票を行い、賛成多数で維持されることとなった。
また、JTCG TF1 で作成中のマネジメントシステム共通化規格（MSS）を今回の改訂で採用することが決定された。今回の会議ではこの MSS 案についても検討を行い、検討結果をコメントとして JTCG へ提出することになった。
ISO 31000（リスクマネジメントの原則及び指針-2009.11 発行）対応についても議論され、より一層の整合化が検討された。今回、すべてのコメント処理には至らなかったため、未審議のコメントはエディタ預かりとなった。
今回の編集会議の結果、CD には進まず、次回は 4th WD を発行することになった。

27002 Code of practice for information security management

前回のマラッカ会議に引き続き 2nd WD 27002 に対するコメント処理を行った。標題の変更提案が他国により提出されていたが、議論となり、最終的に”Code of practice for information security controls”とすることになった。また、すべてのコメント処理には至らなかったため、未審議のコメントはエディタ預かりとなった。
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。

27005 Information security risk management

前回のマラッカ会議にて、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。これを受けて FCD が発行されており、今回の編集会議では FCD に対する審議を行った。
FCD 投票結果は、投票総数 37 カ国、賛成 23 カ国、反対 7 カ国、棄権 7 カ国であり、反対国を中心に約 100 件のコメントが寄せられた。その多くが、ISO 31000:2009 及び ISO Guide 73:2009 との整合性に関するものであり、今回の審議においてこれらのコメントを検討した。
今回の編集会議の結果、次回は FDIS に進むことで合意された。

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

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）投票について、この規格の背景*を説明する Notes 文書がマラッカ会議後に発行されており、今回の会議にて改訂を開始することが決定された。これを受けて、"call for contribution（寄書募集）”を発行することになり、次回の会議から改訂について検討する予定である。
* ISO/IEC 27006 は、ISO/IEC 17021 を基に情報セキュリティマネジメントシステム固有の要求事項･指針を追加

した規格であり、ISO/IEC 17021 と整合がとられている。現在、ISO/IEC 17021 は改訂中であり、この規格との整合を維持する必要がある。
ISO/IEC 17021:2006 Conformity assessment – Requirements for bodies providing audit and certification of management systems（JIS Q 17021:2007 適合性評価－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）

27007 Guidelines for information security management systems auditing
3rd CD に対して約 60 件のコメントが寄せられた。今回の審議では、特に 3rd CD 27007 発行後に発行された DIS19011 との整合を図ることが重要であり、コメント処理を通して DIS19011 との整合が図られた。今回の編集会議の結果、19011 が DIS となりほぼ安定したこと、及び 27007 の内容も安定してきたことから、次の版は FCD に進むことで合意された。

27008 Guidance for auditors on information security controls
PDTR に対する投票結果は、投票総数 36 カ国、賛成 21 カ国、反対 3 カ国、棄権 12 カ国であり、コメント総数は 152 件であった。コメント審議では、主にスコープの変更に伴う修正と構成整理に関する修正について議論された。今回の編集会議の結果、賛成多数で次の版は DTR に進むことになった。
また、本プロジェクトについては（IS ではなく）TR ということが確認された。なお、標題も”Guidelines for auditors on information security management systems controls”から標記のとおり変更された。

以上