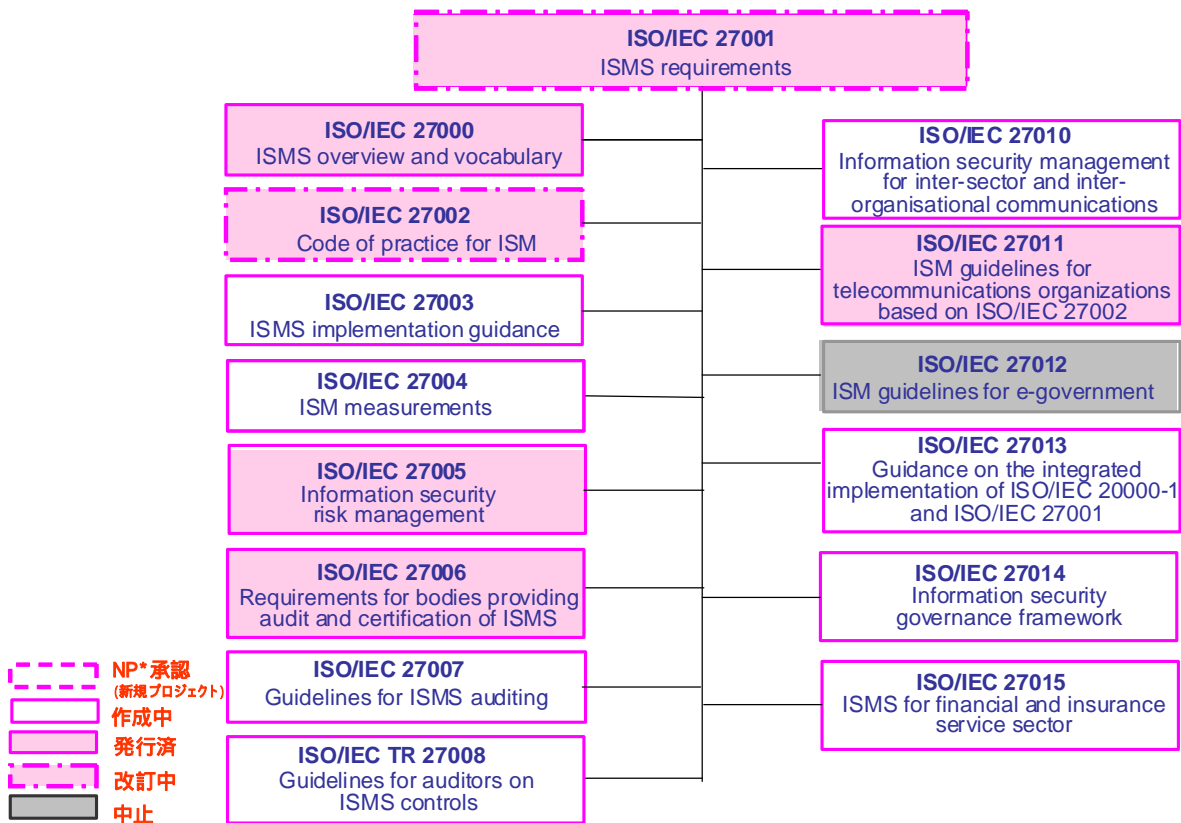


ISO/IEC 27000 ファミリーについて

2009 年 12 月 18 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、4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4月発行

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、定期見直し後、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、定期見直し後、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 (作成中)

Information technology – Security techniques – Information security management system implementation guidance

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 (作成中)

Information technology – Security techniques – Information security management – Measurements

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

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

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 management systems controls

リスクに基づいたアプローチを通して選択したISMS 管理策の導入の適切性及び有効性のレビューに関する規格。

TR (Technical Report) 規格。ISO とするか、TR とするかは、検討中。

ISO/IEC 27010 (作成中 - 今回より WD として審議開始)

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。

("Information technology – Security techniques -- Information security management for inter-sector communications" から名称変更)

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 - 今回より WD として審議開始)

Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001

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 - 今回より WD として審議開始)

Information technology – Security techniques – Information security governance framework

情報セキュリティガバナンスの枠組みに関する規格。ITU-T との共同開発で作成が進められている。

ISO/IEC 27015 (作成中 - 今回より WD として審議開始)

Information technology – Information security management guidelines for financial and insurance services

金融及び保険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39回 WG 1 会議は、2009年11月2日～9日に米国（レドモンド）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、（社）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。

（社）情報処理学会 情報規格調査会：<http://www.itscj.ipsj.or.jp/index.html>

2-1 第39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	今回 (2009年10月)	次回 (2010年4月)
ISO/IEC 27000	概要及び用語	IS	IS
ISO/IEC 27001	要求事項	IS (改訂 1st WD)	IS (改訂 2nd WD)
ISO/IEC 27002	実践のための規範	IS (改訂 1st WD)	IS (改訂 2nd WD)
ISO/IEC 27003	導入に関する手引	FDIS (12/9投票終了予定)	(FDIS/IS)
ISO/IEC 27004	測定	FDIS (10/27投票終了)	(FDIS/IS)
ISO/IEC 27005	リスクマネジメントに関する指針	IS	IS
ISO/IEC 27006	認証機関に対する要求事項	IS	IS
ISO/IEC 27007	監査の指針	1st CD	2nd CD
ISO/IEC 27008	ISMS 管理策に関する監査員のための指針	2nd WD	3rd WD
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	1st WD	2nd WD
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	-	-
ISO/IEC 27013	ISO/IEC 20000-1 と ISO/IEC 27001 との統合導入についての手引き	Pre WD	2nd WD
ISO/IEC 27014	情報セキュリティガバナンスフレームワーク	1st WD	2nd WD
ISO/IEC 27015	金融及び保険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
<p>*規格策定の段階は、次の通り</p> <p>NP WD CD FCD FDIS IS (発行済)</p> <p>NP : New work item Proposal WD : Working Draft CD : Committee Draft FCD : Final Committee Draft FDIS : Final Draft for International standard IS : International Standard</p>			

2-2 第 38 回 SC 27/ WG 1 会議における検討状況（詳細）

- 各プロジェクト進捗状況

27001 Information security management systems – Requirements

1st WD に対して、全 298 件のコメントが寄せられた。特に、米国から対象を情報システムに限定した要求事項にすべきという大幅な改定を要求する一連のコメントが提出されたが、エディタ及び出席者の反対があり、そのほとんどが却下された。

また、全コメントのうち、Technical コメントは 233 件であり、全て審議され、次回は 2nd WD を作成することになった。

前回の北京会議に引き続き、ISO/TMB (Technical Management Board) JTCG (Joint Technical Coordination Group) にて進められている management systems standards (MSS、全ての Management System 規格の標準化) についても議論され、最上位の章単位での共通化について JTCG で作成されている MSS 案に従って記述されることが合意された。

27002 Code of practice for information security management

前回の北京会議にてカナダから提案された、管理目的・管理策の分類体系の大幅な見直し案については、影響分析の結果、顧客に与える影響が大きすぎるとして、正式に却下された*。

今回のコメントは相当な数に上り (全 211 ページ) 全ては処理できなかったため、残ったコメントについてはエディタ預かりで処理を進めることになり、次回は 2nd WD を作成することになった。

*一方で、カナダ提案の活用方法について言及した他国のコメントがいくつか提出されており、これらのコメントについて議論された結果、新たに 27002 とは別途 Study Period (研究期間) が設置され、活用方法を検討することになった。

27003 Information security management system implementation guidance

10 月 9 日から 12 月 9 日間で、FDIS 投票中。

27004 Information security management – Measurements

8 月 27 日から 10 月 27 日間で FDIS 投票が行われ、正式に承認された。現在、ISO にて発行準備中。

27007 Guidelines for information security managements auditing

1st CD に対して約 210 件のコメントが寄せられた。ニュージーランドから、必要とされる文書の確認表の追加を提案するコメントがあったが、Audit の作業に制限を与えることになると懸念されるという理由で却下された。

今回の審議の結果、次回は 2nd CD を作成することになった。

27008 Guidance for auditors on information security management systems controls

2nd WD に対するコメントの審議を行った結果、次回は 3rd WD に進むことになった。

また、前回の北京会議からの検討事項となっている、Technical Report (TR) から IS への

変更については、議論の末、次の WD まで待ってから検討することとなった。

27010 Information security management for inter-sector communications

名称変更：“Information security management for inter-sector and inter-organisational communications”

1st WD に対するコメントの審議を行った。エディタは CD に進む意向であったが、日本から認証時の問題点を指摘した結果、今回は 2nd WD を作成することになった。

また、議論の結果、文書名を “Information security management for inter-sector and inter-organisational communications” に変更することになった。

27013 Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001

エディタ募集中であったが、今回 SC27(ISO/IEC 27001 担当)と SC7(ISO/IEC 20000-1 担当)から 1 名ずつエディタが指名された。

1st WD に対するコメントの審議を行った結果、今回は 2nd WD を作成することになった。

27014 Information security governance framework

1st WD に対するコメントの審議を行い、文書構造について議論された。その結果、新しい文書構造について合意され、文書の内容については今回のコメント及び寄書をベースにして新規に作成することになった。

今回は、2nd WD を作成することになった。

27015 Information security management for financial and insurance service sector

1st WD に対するコメントの審議を行ったが、現在の 27015 はまだ目次レベルのものでしかなく、コメントも合計で 15 個という状況であった。

今後の本文の作成については、文書作成を行うグループメンバを募集し、2nd WD を作成することになった。

- その他（定期見直し、新規プロジェクト等）

27000 ISMS Overview and vocabulary 早期改訂について

前回会議後に Study Period（研究期間）が開始された。今回の会議では、早期改訂に関する投票実施の可否について議論された。

結果として、Study Period が 6 ヶ月間延長され、これと並行して早期改訂に関する投票を行うことになった。

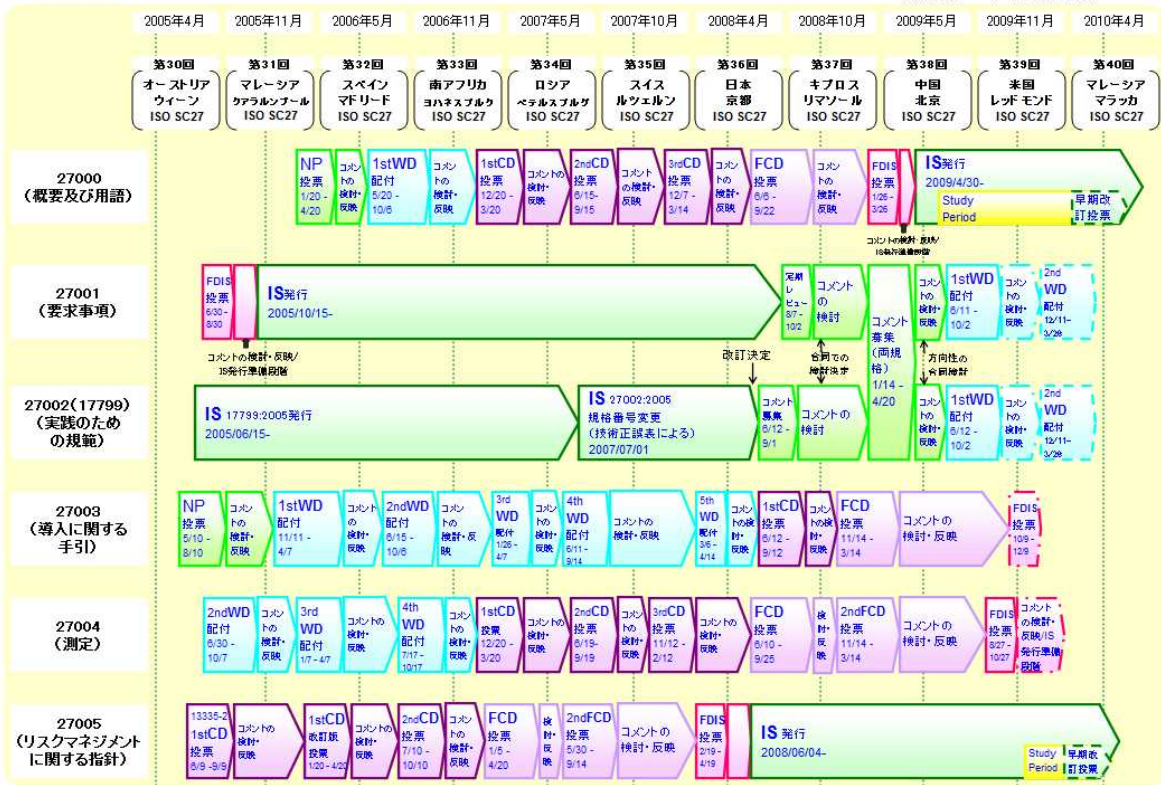
27005 ISM Risk management 早期改訂について

ISO 31000(リスク管理 - 原理とガイドライン)が発行されたことを受けて、今回の会議直前にオーストラリアより ISO 31000 との整合性を保つために早期改訂が必要との提案がなされた。

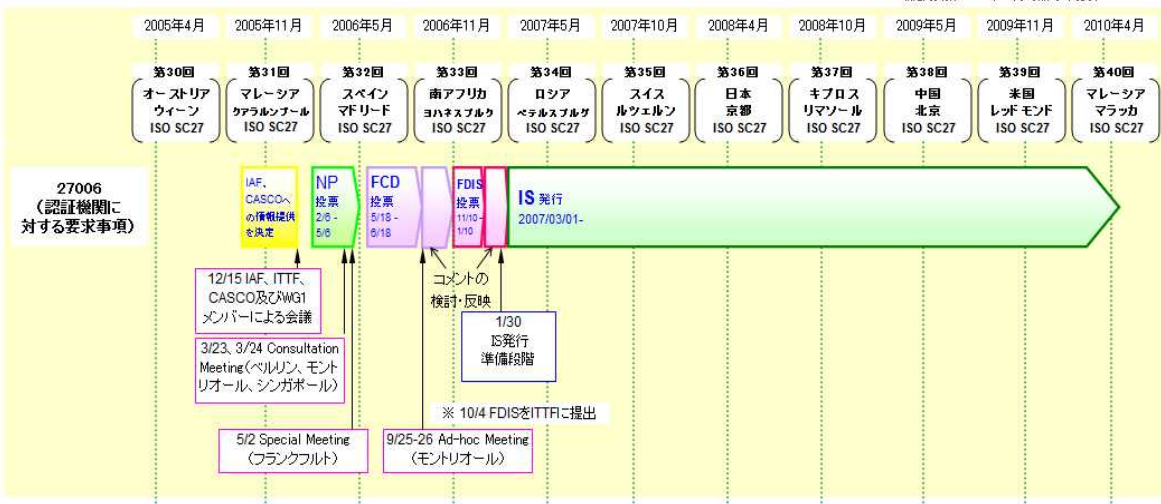
議論の結果、今回の決議では Study Period（研究期間）を開始し、これと並行して早期改訂に関する投票を行うことになった。

- ISO/IEC 27000 ファミリー規格作成の進捗状況一覧

※1 --- 緑部分は、2009年12月時点での予測
 ※2 --- 緑部分は、2009年12月時点での現状



※1 --- 緑部分は、2009年12月時点での予測
 ※2 --- 緑部分は、2009年12月時点での現状



※1 --- 調査分は、2009年12月時点での予測
 ※2 --- 調査分は、2008年12月時点での現状

