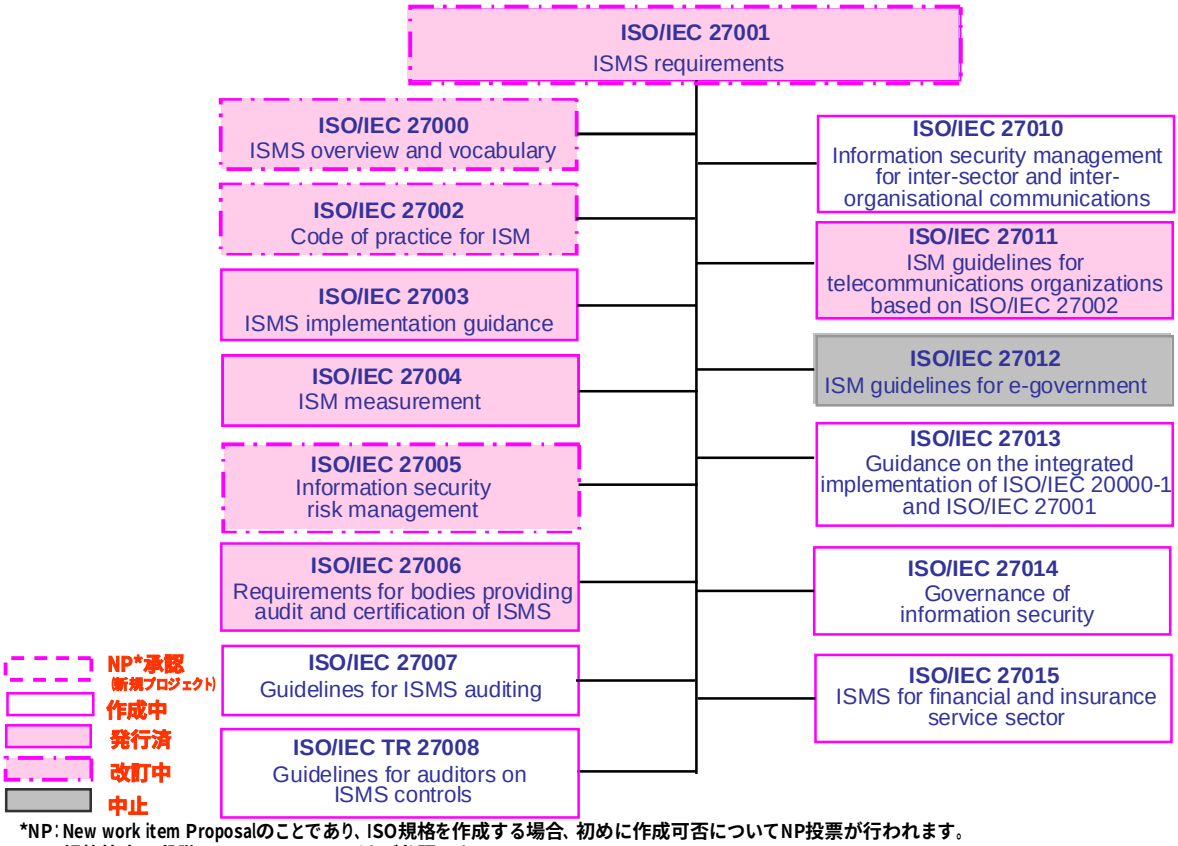
ISO/IEC 27000 ファミリーについて

2010 年 6 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（**2010 **年** 4 **月開催のマラッカ会議で改訂開始が決定された）**

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 27003:2010

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（**2010 **年** 4 **月開催のマラッカ会議で改訂開始が決定された）**

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）

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 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）

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。（2010 年 4 月開催の第 40 回会議にて、”Information technology – Security techniques -- Information security governance framework”から名称変更になった。）

ISO/IEC 27015（作成中）

Information technology -- Security techniques – Information security management system for financial and insurance services sector

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 40 回 WG 1 会議は、2010 年 4 月 19 日～23 日にマレーシア（マラッカ）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 40 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 40 回会議（2010 年 4 月）	第 41 回会議（2010 年 10 月）
ISO/IEC 27000	概要及び用語	IS	IS（改訂開始予定）
ISO/IEC 27001	要求事項	IS（改訂 2nd WD）	IS（改訂 3rd WD）
ISO/IEC 27002	実践のための規範	IS（改訂 2nd WD）	IS（改訂 2nd 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	IS（改訂開始予定）
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	2nd CD	3rd CD
ISO/IEC TR 27008	ISMS 管理策に関する監査員のための指針	3rd WD	PDTR
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	2nd WD	3rd 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	ー	ー
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	1st WD	2nd WD
ISO/IEC 27014	情報セキュリティのガバナンス	2nd WD	3rd 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	2nd WD	(2nd 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

2-2 第 40 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

27001 Information security management systems – Requirements
1st WD に対して、全 225 件のコメントが寄せられた。特に、ISO 31000（リスクマネジメントの原則及び指針-2009.11 発行）、measurement に関する要求事項の見直し・明確化、asset、information asset の定義について議論された。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）対応についても議論された。
Technical コメントの処理は、Annex A に関連するものを除き、すべて終了した。今回はアイスランドの火山噴火の影響で欠席国が多いことから、Annex A に関するコメントの審議を次回に延期し、また CD には進めず次も WD とし、従って次回は 3rd WD を発行することになった。

27002 Code of practice for information security management
コメント総数は 797 件であった。欠席者が多かったため、用語の定義の追加や管理策の追加を求める等、大幅変更を求めるコメントについては今回会議では審議保留とし、次回ベルリン会議で議論することになった。また、コメント数が多く、処理できたコメントは全体の 3 分の 1 程であった。従って、今回の会議では Meeting Report（会議報告）を発行し、3rd WD は発行しないことになった。次回のベルリン会議にて、引き続き 2nd WD 27002 に対する残りのコメント処理を行った後に 3rd WD 27002 を発行予定である。

27007 Guidelines for information security management systems auditing
2nd CD に対して約 160 件のコメントが寄せられた。このうち、本文に対する Technical コメントは約 40 件と少なく、これらはすべて処理された。Annex C（Audit practice guide）については、日本から新 Annex C 提案を提出しており、これと併せてコメント約 70 件も提出していた。日本の新 Annex C 提案については、各 NB に対して次回会議までに内容を確認しコメントを提出することが要請され、次回議論することになった。
今回の審議の結果、次回は 3rd CD を作成することになった。

27008 Guidance for auditors on information security management systems controls
3rd WD に対して約 80 件のコメントが寄せられた。このうち、日本からは適用範囲（Scope）について、Technical Compliance Checking をおこなうためのガイダンスという位置付けにすべきという提案を行ない、ほぼ受け入れられた。また、文書名の変更、及び TR から IS への変更については、今回の会議は出席国が少なかったことから、審議は次回保留となった。
2nd WD に対するコメントの審議を行った結果、次回は PDTR（Proposed Draft Technical Report）を発行することになった。

以上