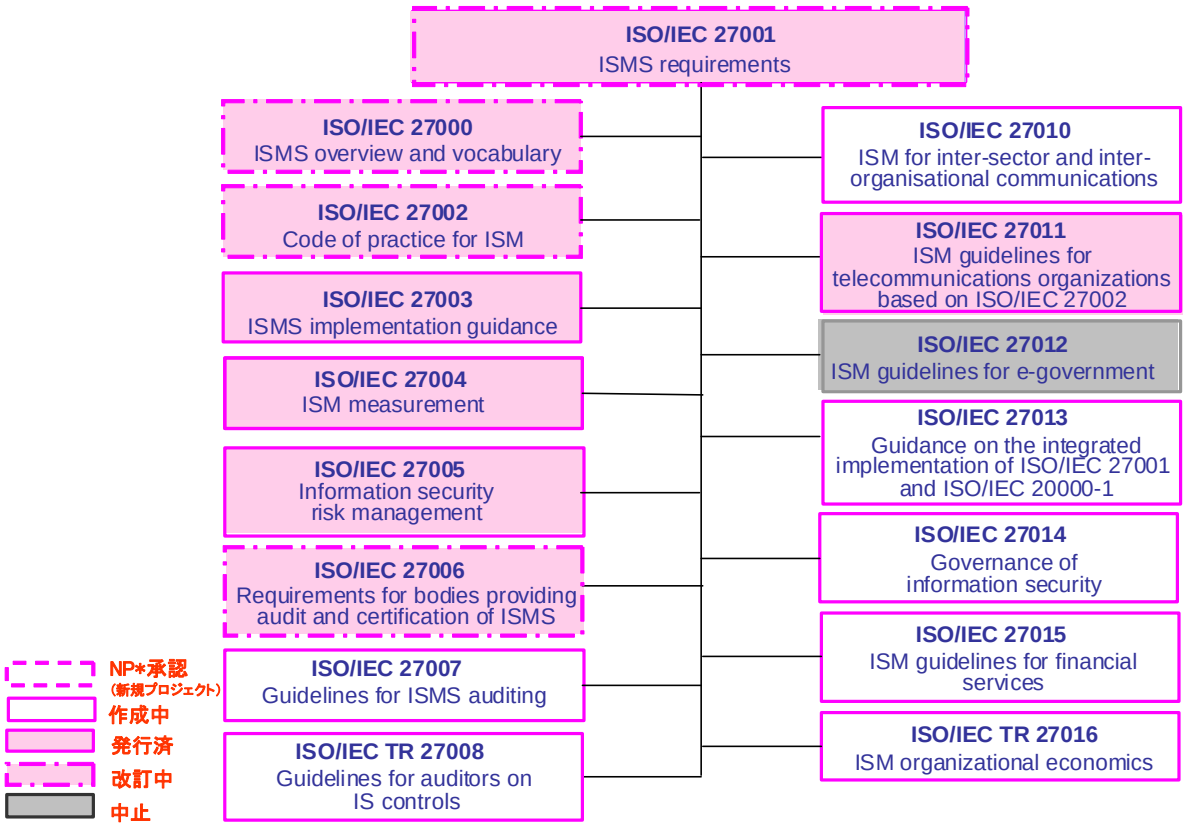
ISO/IEC 27000 ファミリーについて

2011 年 6 月 8 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 27005:2011

Information technology – Security techniques – Information security risk management

2011 年 5 月 19 日発行

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 27006:2007 Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems 2007 年 3 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。 ※ 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ドライン規格。 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。
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ドライン（TR：Technical Report）。
ISO/IEC 27010（作成中） Information technology – Security techniques – 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 – 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。
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）。

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 42 回 WG 1 会議は、2011 年 4 月 11 日～15 日にシンガポール（シンガポール）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 42 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 42 回会議（2011 年 4 月）	第 43 回会議（2011 年 10 月）
ISO/IEC 27000	概要及び用語	IS（改訂: 2nd WD）	IS（改訂 3rd WD）
ISO/IEC 27001	要求事項	IS（改訂 4th WD）	IS（改訂 1st 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 3rd WD）	IS（改訂 4th 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（FDIS）	IS (改訂版)
ISO/IEC 27006	認証機関に対する要求事項	IS（改訂審議）	IS（DIS）
ISO/IEC 27007	監査の指針	FCD	FDIS
ISO/IEC TR 27008	IS 管理策に関する監査員のための指針	DTR	（TR）
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 CD	FCD
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	3rd WD	1st CD
ISO/IEC 27014	情報セキュリティのガバナンス	1st CD	2nd 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	2nd WD	3rd 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)	1st 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

◆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（新プロセス：NP →WD →CD →DIS* →FDIS →IS。*DIS：Draft International Standard）。

2-2 第 42 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

2nd WD に対して、約 50 件のコメントが寄せられた。今回の方針として、現在改訂中の版ではなく、ISO/IEC 27001：2005 に基づいて改訂を実施することになった。

今回の編集会議の結果、全てのコメント処理が終了し、次の版は 3rd WD を発行することになった。

27001 Information security management systems – Requirements

前回のベルリン会議に引き続き、ISO/TMB JTCG TF1 で作成中のマネジメントシステム共通化規格（MSS）に対応するための規格の再構成、及びリスクマネジメント規格である ISO 31000 との整合を実施中である。

今回の編集会議の結果、次回は 1st CD を発行することになった。

27002 Code of practice for information security management

3rd WD に対して、約 1000 件のコメントが寄せられた。今回の会議では、General コメントの一部を審議した後に、これまでの会議では審議に至っていなかった 10～15 章を中心に審議を行った。すべてのコメント処理には至らなかったため、未審議のコメントについては、メール等を使用してオンラインで審議を実施することになった。

今回の編集会議の結果、次回は 4th WD を発行することになった。

27005 Information security risk management

ベルリン会合の決議を受けて、FDIS 投票が 2011 年 3 月 22 日～4 月 21 日にて実施された。

この FDIS 投票の結果、賛成多数にて 2011 年 5 月 19 日付で、ISO/IEC 27005:2011 が発行された。

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

今回の改訂では ISO/IEC 17021:2011 と整合をとるための更新を行うことを目的とし、17021 改訂に関わる以外のコメントで長期検討を要するものは 27006 改訂 IS 発行後に systematic review を行い、この systematic review での審議事項とする方向となった。これは、ISO/IEC 17021:2011 の発行に伴い、IAF（International Accreditation Forum：国際認定機関フォーラム）が ISO/IEC 17021 の移行期間を 2 年間と定めたことから、この ISO/IEC 17021 を包含する ISO/IEC 27006 の改訂も急ぐ必要が生じたことによる。

なお、Call for Contribution に対して寄せられたコメントは全て、会議中に審議された。

今回の編集会議の結果、DIS を発行し、併せて Strategy 文書を発行することになった。

* ISO/IEC 27006:2007 は、ISO/IEC 17021:2006 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 17021:2006 と整合がとられている。このたび、ISO/IEC 17021 が改訂され、ISO/IEC 17021:2011 が発行され、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） 27006JIS 化文書よりもってくる。
  IAF ID 2:2011 “IAF Informative Document for the Transition of Management System Accreditation to ISO/IEC 17021:2011 from ISO/IEC 17021:2006”（マネジメントシステム認定の ISO/IEC 17021:2006 から ISO/IEC 17021:2011 への移行に関する IAF 参考文書）

27007 Guidelines for information security management systems auditing

FCD 投票では、賛成 24 カ国、コメント付賛成 5 カ国、反対 2 カ国、棄権 6 カ国であり、コメント総数は約 210 件（ISO/TC 176/ SC 3/WG 16 及び ITTF コメント含む）であった。コメントのうち半数以上が 19011 改訂案の最新版との整合を求める編集上のものであり、今回の審議では、本文についてすべてのコメント処理が終了し、27007 自体のテキストは安定していることが確認された。一方で、19011 の FDIS 版が本会議の時点で未発行だったため、現段階で 27007 を FDIS に進めるかどうかについて議論となった。

結果として、会期中に FDIS 19011 案（発行前：5〜6 月頃発行予定）を入手し、主に competence について規定している 7 章を中心に確認を行った。また、27007 の Annex A については、WG 16 からの提示案があり、これをレビューし WG16 へフィードバックすることになったことから、ISO 19011 改訂版に含まれる見込みである。

今回の編集会議の結果、次回は FDIS に進むことになった。

27008 Guidance for auditors on information security controls

DTR 投票の投票結果は、賛成 16 カ国、コメント付賛成 1 カ国、反対 1 カ国、棄権 12 カ国であり、コメントは約 120 件であった。この投票結果を受けて、今回の会議では、DTR から Publication に進むことは投票にて承認されているため、編集上の修正以外の見直しは行なうべきではないという説明がエディタからあり、決議された。このため、編集上のコメント以外のものは、次回改訂まで議論を持ち越すという形となった。

結果として、DTR 投票結果により、27008 の発行が決定された。

以上