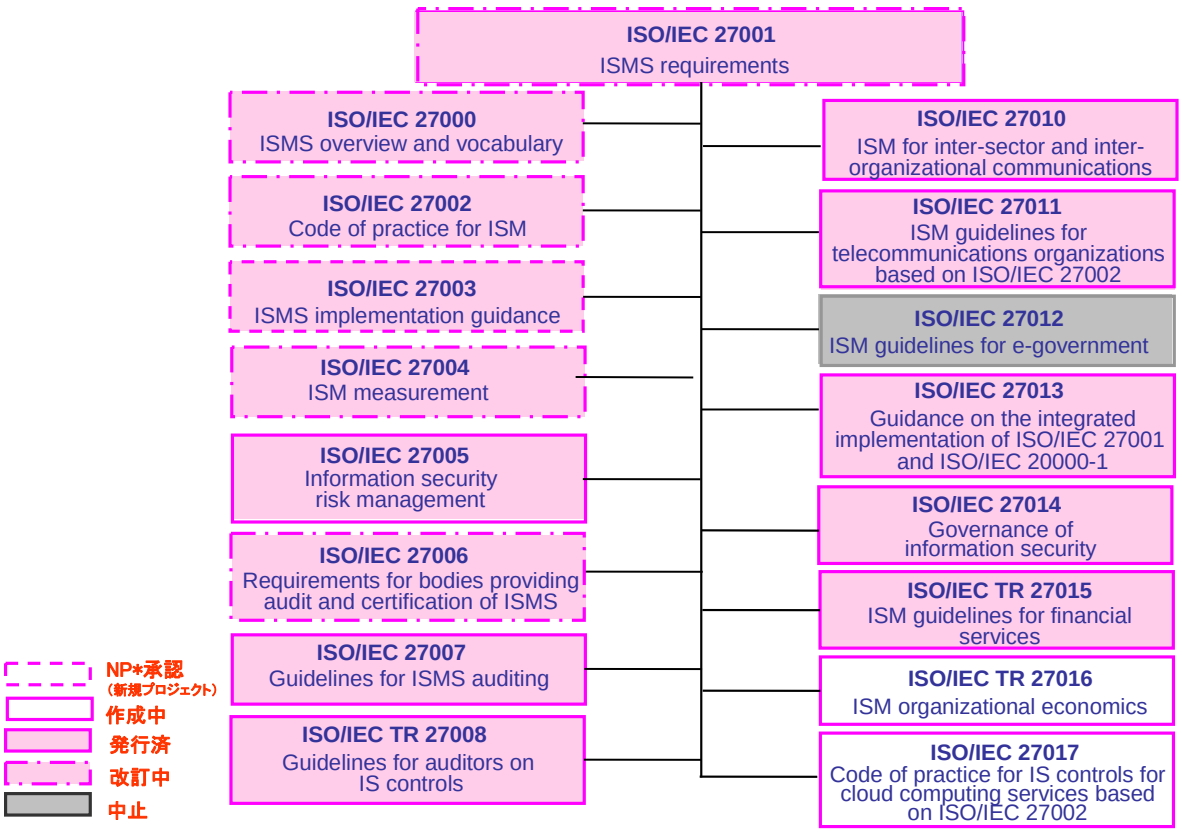
ISO/IEC 27000 ファミリーについて

2013 年 6 月 11 日
（改 2013 年 7 月 1 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 27000:2012

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

2012 年 12 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 及び ISO/IEC 27002:2005 に対応した改訂版が、2012 年 12 月に発行された。なお、現在改訂中の 27001、27002 に対応した改訂も並行して審議中である。

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。

現在実施中の改訂審議の中で、第 2 版では標題が以下に変更されることになった。

Information technology – Security techniques – Code of practice for information security controls

※ 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（改訂決定）

ISMS の実装（計画から導入まで）に関するガイダンス規格

2012 年 10 月ローマ会議後に開始された NP 投票の結果を受けて、2013 年 5 月ソフィアアンティポリス会議にて改訂開始が決定された。

ISO/IEC 27004:2009

Information technology – Security techniques – Information security management – Measurement

2009 年 12 月発行（現在、改訂審議中）

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（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。

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。

※ 国内規格としては、2012 年 9 月に JIS Q 27006:2012（JIS Q 27006:2008 の改正版）として制定された。

JIS Q 27006:2012

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 27013:2012
Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
2012 年 10 月発行
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）と連携して作成された。

ISO/IEC 27014:2013
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。
2013 年 4 月発行

ISO/IEC TR 27015:2012
Information technology – Security techniques – Information security management guidelines for financial services
2012 年 11 月発行
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 27017（作成中）
Information technology – Security techniques – Information security management -- Code of practice for information security controls for cloud computing services based on ISO/IEC 27002
クラウドコンピューティングサービスにおける ISO/IEC 27002 に基づく情報セキュリティ管理策の実践のための規範

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 46 回 WG 1 会議は、2013 年 4 月 22 日～26 日にソフィアアンティポリス（フランス）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 46 回 SC 27/ WG 1 会議における検討状況（全体）

*各会議で審議される規格の段階を示しています。
既に IS 発行済で現在改訂中のものについては、（）で改訂段階を示しています。
例：IS（改訂中：DIS）－IS 発行済だが、現在改訂中で DIS 審議
※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です。

ISO/IEC 番号	規格内容	第 46 回会議*（2013 年 4 月）	第 47 回会議（2013 年 10 月）
ISO/IEC 27000	概要及び用語	IS[第 2 版] (改訂 NP 投票/CD)	IS[第 2 版] （改訂中：DIS）
ISO/IEC 27001	要求事項	IS[第 1 版] （改訂中:DIS）	IS[第 1 版] （改訂中:FDIS／ IS[第 2 版]）
ISO/IEC 27002	情報セキュリティ管理策の実践のための規範	IS[第 1 版] （改訂中:DIS）	IS[第 1 版] （改訂中:FDIS／ IS[第 2 版）
ISO/IEC 27003	導入に関する手引	IS [第 1 版]（改訂 NP 投票）	IS[第 1 版] （WD）
ISO/IEC 27004	測定	IS[第 1 版] （改訂中:WD）	IS[第 1 版] （改訂中:WD）
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]（改訂 NP 投票）
ISO/IEC 27006	認証機関に対する要求事項	IS[第 2 版] (改訂中:2nd WD)	IS[第 2 版] (改訂中:3rd WD)
ISO/IEC 27007	監査の指針	IS [第 1 版]	IS [第 1 版]
ISO/IEC TR 27008	IS 管理策に関する監査員のための指針	TR [第 1 版]	TR [第 1 版]
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 [第 1 版]	IS [第 1 版]
ISO/IEC 27011	電気通信組織のための指針	IS [第 1 版]	IS [第 1 版]（改訂検討）
ISO/IEC 27012	電子政府サービスのための ISMS 指針	－	－
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	IS [第 1 版]	IS [第 1 版]（NP 投票）
ISO/IEC 27014	情報セキュリティのガバナンス	FDIS	IS [第 1 版]
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	TR [第 1 版]	TR [第 1 版]
ISO/IEC TR 27016	情報セキュリティマネジメント－組織の経済的側面(Organizational economics)	PDTR	DTR
ISO/IEC 27017	クラウドコンピューティングサービスにおける ISO/IEC 27002 に基づく情報セキュリティ管理策の実践のための規範	4th WD	5th 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 46 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

前回会議後、ISO/IEC 27001：2005、ISO/IEC 27002:2005 に基づく改訂版である ISO/IEC 27000:2012-12-01（2nd edition）が、2012 年 12 月に発行された。

これと並行して、改訂版 27001/27002（現在改訂作業中）に基づく改訂（3rd edition）についても審議するために、早期改訂開始の可否についての NP 投票が行われ、併せて CD が発行された。
NP 投票で反対国はなく、早期改訂の開始が決定された。また、並行して発行された CD についても、反対は 2 カ国（オーストラリア、日本）だけであった。審議の中で、27001、27002 の用語については 27001 編集会議及び 27002 編集会議にて審議され、その結果をインプットとして得ることができ、27000 の用語及び定義に反映することができた（このため日本も賛成に変更した）。なお、その他の規格で使用されている用語は、次回以降の改訂にて審議されることになった。

今回の編集会議の結果、次回は DIS を発行することになった（もし DIS 投票で反対国がない場合、FDIS が省略され、IS が発行されることになる）。

27001 Information security management systems – Requirements

DIS 投票では、賛成 22 カ国、コメント付賛成 10 カ国、反対 6 カ国（オーストラリア、オーストリア、フィンランド、日本、ポーランド、南アフリカ）、棄権 8 カ国であり、コメント総数は約 200 件であった。

今回は DIS のため、（通常の編集会議ではなく）Ballot resolution meeting ということで、まず反対国のコメントから審議され、その後、賛成国のコメントが審議された。今回の審議では、これまで大きく議論となったことについては繰り返しの審議をしない傾向となったため、全体的に（DIS に対する）テキストの大幅な変更はなかった。また、用語に関するコメントについても審議され、27000 プロジェクトにインプットされた。

今回の編集会議の結果、次回は FDIS を発行することになった。
なお、FDIS 投票により可決された場合には、国際会議にて審議することはないため、次回の国際会議に先立って IS（国際規格）が発行されることもある。

27002 Code of practice for information security controls

DIS 投票では、賛成 23 カ国、コメント付賛成 4 カ国、反対 6 カ国（オーストラリア、ブラジル、日本、ポーランド、スウェーデン、スイス）、棄権 12 カ国であり、コメント総数は約 970 件であった。

今回は DIS のため、27001 と同様に（通常の編集会議ではなく）Ballot resolution meeting ということで、まず反対国のコメントの中で（各国が）優先度が高いと判断したコメントについて審議を実施した。この中で、用語及び定義についても審議された。審議の結果、（DIS に対する）構成については大きな変更はなかったが、記述について改善された。

今回の編集会議の結果、次回は FDIS を発行することになった。

なお、FDIS 投票により可決された場合には、国際会議にて審議することはないため、次回の国際会議に先立って IS（国際規格）が発行されることもある。

27003 Information security management system implementation guidance

今回の会議に先立って、27003 の可否に関する NP 投票が実施された。この NP 投票では、反対国はなく、早期改訂が決定された。そのため、編集会議では、1st WD の方向性について議論され、27003 の改訂は 27001 改訂版をサポートするためにできるだけ早い発行を目指すことになった。

今回の編集会議の結果、WD を発行することになった。

27004 Information security management – Measurement

今回の会議に先立って寄せられた各国コメントを集約した文書が発行されており、編集会議では、この文書に基づいて進められ、規格標題、適用範囲等について議論された。

今回の編集会議の結果、次回は WD を発行することになった。

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

今回の会議に先立って、2nd WD 27006 に対して約 160 件のコメントが寄せられた。

編集会議では、特に 7 章 Resource requirements（資源に関する要求事項）の力量部分と Annex C Audit time（附属書 C 審査工数）に関して議論された。

7 章については、スウェーデンから 2nd WD 27006 の構成案をさらに変更するよう提案があったが、まずは現在改訂中の 17021 の関連する内容について改訂の方向性を確認し、その結果を受けて検討することになった。

Annex C Audit time（附属書 C 審査工数）については、他のマネジメントシステム規格（QMS、EMS 等）との整合についても検討され、その結果、Normative とする方向となった。内容の更新については、関連する IAF 文書（MD1、MD5、MD11 等）※を踏まえて次回検討することになった。

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。

※ IAF（国際認定フォーラム）が発行している文書。詳細は、以下の URL を参照ください。
http://www.iaf.nu/articles/Mandatory_Documents_/38

以上