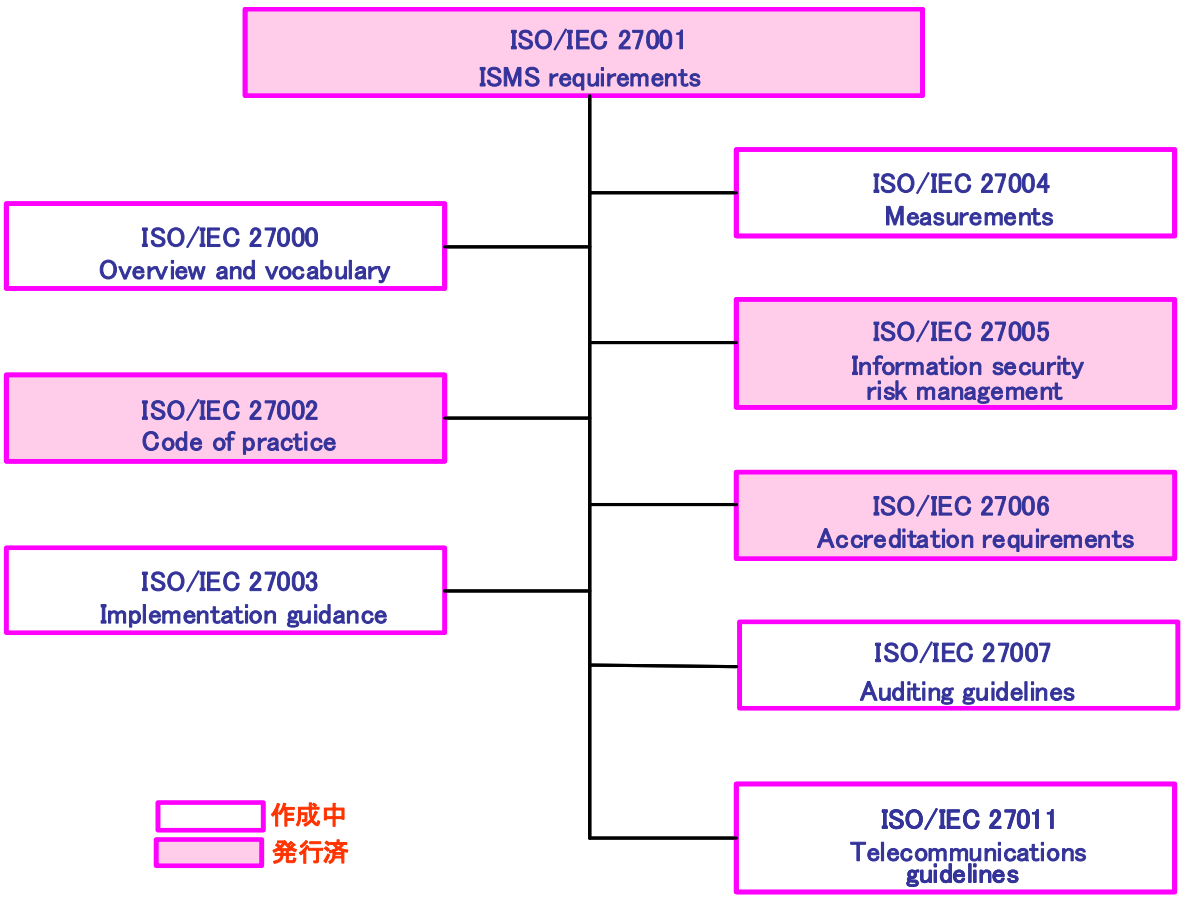
ISO/IEC 27000 ファミリーの概要

2008 年 12 月 16 日

財団法人 日本情報処理開発協会
情報マネジメント推進センター

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。



ISO/IEC 27000（作成中）

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

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

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

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 の設計・導入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の導入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 managements 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－現在全マネジメント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 27011（作成中：近日中に発行予定）

Information technology – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

電気通信組織における、I SO/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。

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 37 回 WG 1 会議は、2008 年 10 月 6 日～10 日にキプロス（リマソール）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、（社）情報処理学会様の Web サイトにて公開されています。

（社）情報処理学会： http://www.itscj.ipsj.or.jp/index.html

2-1 第 37 回 SC 27/ WG 1 会議における検討状況（全体）

規格番号	今回*	次回 （2009 年 5 月、北京）
ISO/IEC 27000（概要及び用語）	FCD	FDIS
ISO/IEC 27001（要求事項）	発行済	（改定検討）
ISO/IEC 27002（実践規範）	発行済	（改定検討）
ISO/IEC 27003（導入に関する手引）	1st CD	FCD
ISO/IEC 27004（測定）	FCD	2nd FCD
ISO/IEC 27005（リスクマネジメントに関する指針）	発行済	
ISO/IEC 27006（認証機関に対する要求事項）	発行済	
ISO/IEC 27007（監査の指針）	2nd WD	3rd WD
ISO/IEC 27011（電気通信組織のための指針）	FDIS 投票終了	発行予定

*規格策定の段階は、次の通り

WD → CD → FCD → FDIS

WD： Working Draft

CD： Committee Draft

FCD： Final Committee Draft

FDIS： Final Draft for International standard

2-2 第 37 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

27000

FCD に対して、約 200 件のコメントが寄せられた。当初 4 カ国が反対していたが、審議の結果、1 カ国のみが反対を継続したが他の 3 カ国は賛成となり、次の版は FDIS に進むこととなった。

27003

1st CD に対して、約 540 件のコメントが寄せられた。このプロジェクトについては、ITTF 監査によりプロジェクト進捗に対する指摘を受け、編集会議で FCD に向けた改善、具体的な修正案を検討する等の作業を行った。その結果、次の版は FCD に進むこととなった。

27004

会議前に行われた書面による FCD 投票では賛成国が多い一方で、FCD に対するコメント数は約 450 件であり技術的なコメントも多数に上った。審議の結果、ほぼ全てのコメントについて解決されたが、次版を FDIS とする当初の案についてはスイス、ポーランド、日本等から反対意見が出された。最終的に FDIS に進めるか否かについて投票を行った結果、反対多数により FDIS 化は否決され、次の版は 2nd FCD とすることとなった。

27007

2nd WD に対して、約 130 件のコメントが寄せられた。今回も、ISO 19011 と調和を図りつつ作業が進められたが、ISO 19011 改訂の進捗状況等を考慮し次版も WD とすることとなった。

－その他（定期見直し、新規プロジェクト等）

27001、27002（改定）

27001 については、定期レビューである periodical pre-review の結果、賛成多数で改定に着手することとなった。今後の改定の進め方等について審議された結果、27002 改訂との整合性を保つため、次回会議で 27001、27002 両規格について併せて検討することとなった。

27002 については、前回会議にて改定が決定され、これに基づきコメントが寄せられていたが、コメント審議は次回会議へ持ち越しとなった。

27008（新規）

NP（New Work Item Proposals）投票で可決され、これを受けて審議した結果、WD を作成することとなった。規格タイトルとしては、以下が予定されている。

Title: Guidelines for assessing the implementation of ISMS controls

27010（新規）

NP 投票で可決され、新規プロジェクトとすることになったが、審議の結果、今回は WD の作成は見合わせることとなった。規格タイトルとしては、は以下が予定されている。

Title: Information security management for inter-sector communications

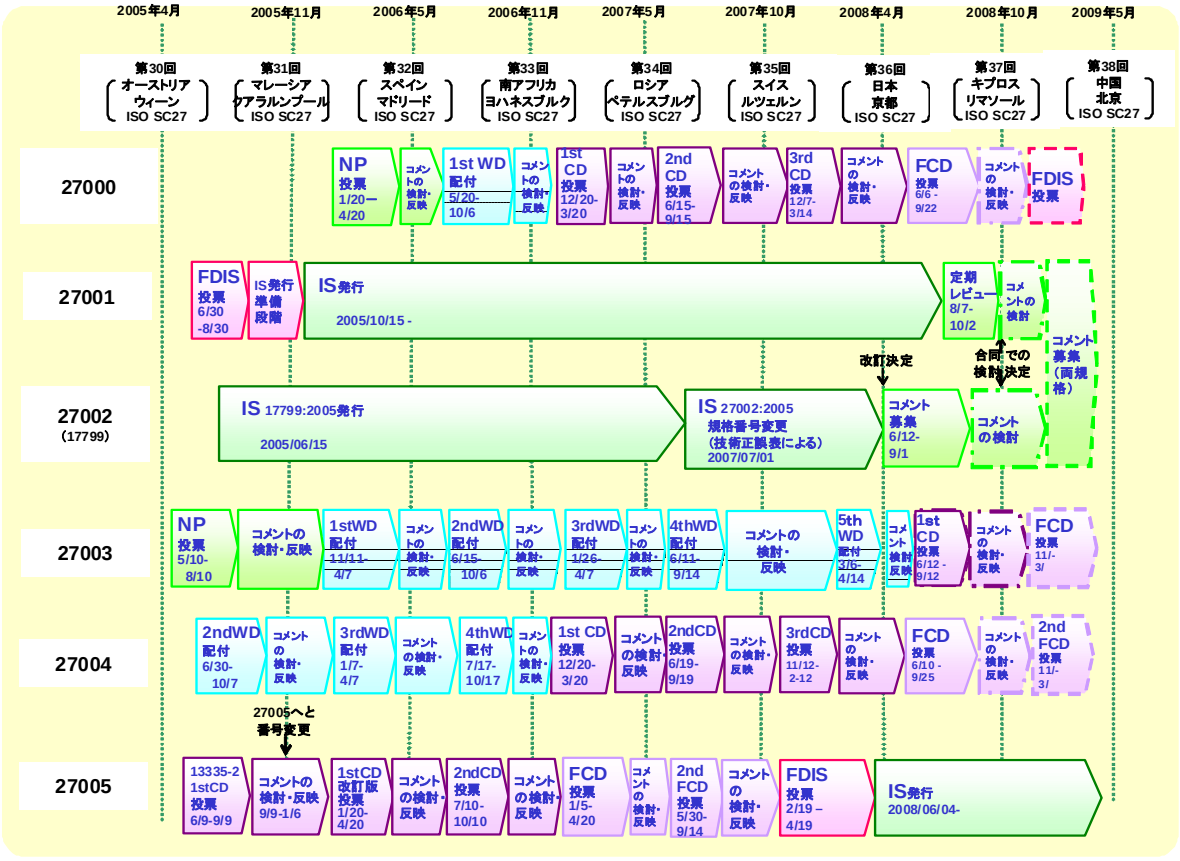
27012（新規）

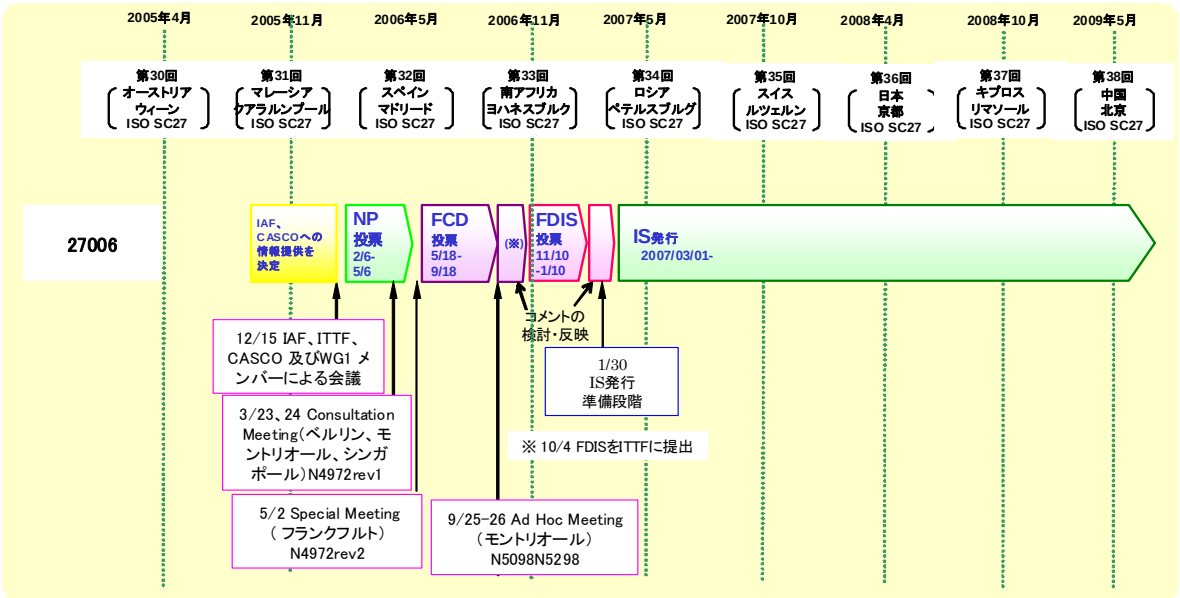
NP 投票で可決され、これを受けて審議した結果、WD を作成することとなった。規格タイトルとしては、以下が予定されている。

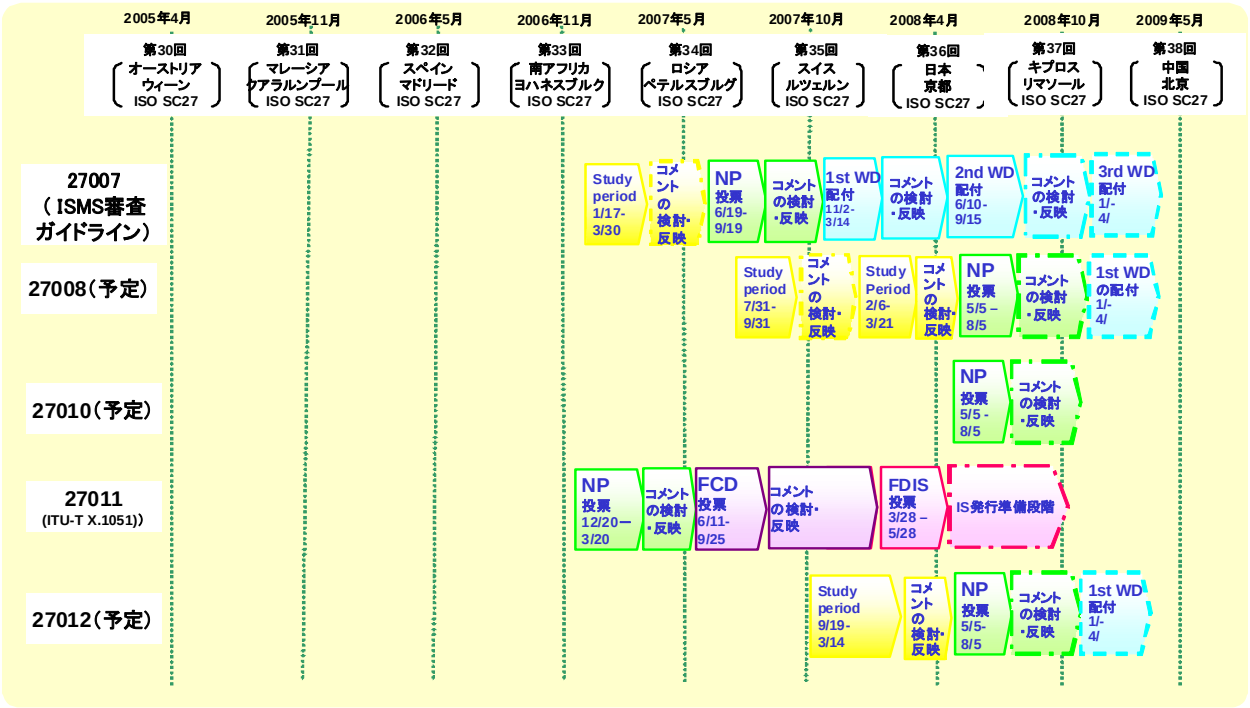
Title: ISM guidelines for e-government services

ーISO/IEC 27000 ファミリー規格作成の進捗状況一覧

※1---- 線部分は、2008年10月時点での予測
※2ー・ー線部分は、2008年10月時点での現状






2005年4月
2005年11月
2006年5月
2006年11月
2007年5月
2007年10月
2008年4月
2008年10月
2009年5月
第30回 オーストリア ウィーン ISO SC27
第31回 マレーシア クアラルンプール ISO SC27
第32回 スペイン マドリード ISO SC27
第33回 南アフリカ ヨハネスブルク ISO SC27
第34回 ロシア ペテルスブルグ ISO SC27
第35回 スイス ルツェルン ISO SC27
第36回 日本 京都 ISO SC27
第37回 キプロス リマソール ISO SC27
第38回 中国 北京 ISO SC27
27007 （ISMS審査ガイドライン）
27008（予定）
27010（予定）
27011 (ITU-T X.1051))
27012（予定）
Study period 1/17-3/30
コメントの検討・反映
NP 投票 6/19-9/19
コメントの検討・反映
1st WD 配付 11/2-3/14
コメントの検討・反映
2nd WD 配付 6/10-9/15
コメントの検討・反映
3rd WD 配付 1/-4/
Study period 7/31-9/31
コメントの検討・反映
Study Period 2/6-3/21
コメントの検討・反映
NP 投票 5/5 – 8/5
コメントの検討・反映
1st WD の配付 1/-4/
NP 投票 5/5 - 8/5
コメントの検討・反映
NP 投票 12/20ー3/20
コメントの検討・反映
FCD 投票 6/11-9/25
コメントの検討・反映
FDIS 投票 3/28 – 5/28
IS発行準備段階
Study period 9/19-3/14
コメントの検討・反映
NP 投票 5/5-8/5
コメントの検討・反映
1st WD 配付 1/-4/