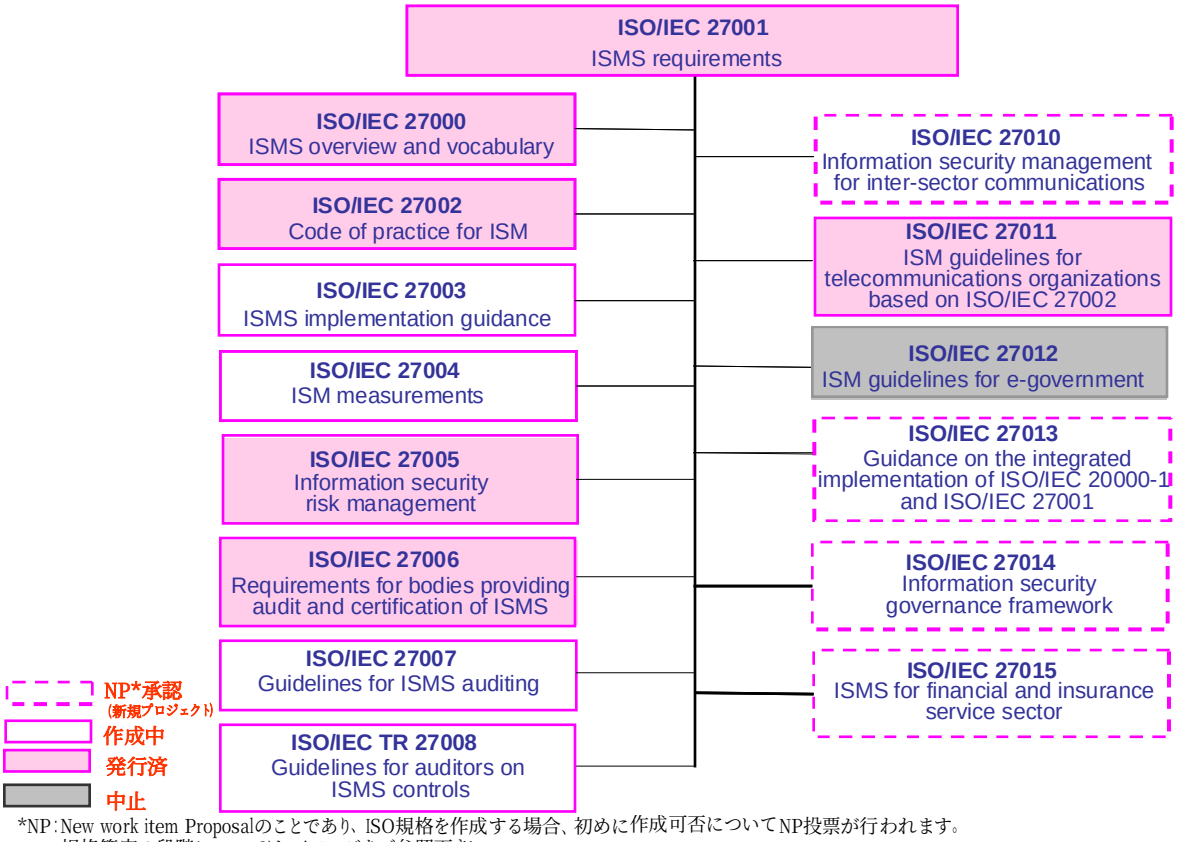
ISO/IEC 27000 ファミリーについて

2009 年 8 月 4 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。

上図の「作成中」及び「発行済」規格の概要は、以下の通りです。

ISO/IEC 27000

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

ISO/IEC 27011

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

2007 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。

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 38 回 WG 1 会議は、2009 年 5 月 4 日～8 日に中国（北京）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 38 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 5 月）	次回 （2009 年 10 月）
ISO/IEC 27000	概要及び用語	FDIS→IS （2009-04-30 発行）	IS
ISO/IEC 27001	要求事項	IS（改定審議） （2005-10-15 発行）	IS（改訂 WD）
ISO/IEC 27002	実践のための規範	IS（改定審議） （2005-06-15 発行）	IS（改訂 WD）
ISO/IEC 27003	導入に関する手引	FCD	FDIS
ISO/IEC 27004	測定	2nd FCD	FDIS
ISO/IEC 27005	リスクマネジメントに関する指針	IS （2008-06-15 発行）	IS
ISO/IEC 27006	認証機関に対する要求事項	IS （2007-03-01 発行）	IS
ISO/IEC 27007	監査の指針	3rd WD	1st CD
ISO/IEC 27008	ISMS 管理策に関する監査員のための指針	1st WD	2nd WD
ISO/IEC 27010	業界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	NP	1st WD
ISO/IEC 27011	電気通信組織のための指針	IS （2008-12-15 発行）	IS
ISO/IEC 27012	電子政府サービスのための ISMS 指針	NP （中止）	―
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	NP	Pre WD
ISO/IEC 27014	情報セキュリティガバナンスフレームワーク	NP	1st 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	NP	1st WD

*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

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

27000 ISMS Overview and vocabulary

FDIS 投票の結果、承認され、2009 年 4 月 30 日に発行された。

27001 及び 27002（改訂）

・**27001 と 27002 の改訂について**

27001、27002 については、個別審議に先立って Joint meeting が開催され、両規格に共通の Strategy、Structure に関して各国から寄せられたコメントをもとに、今回の改訂の基本的な方向性が審議された。日本からは、27001 の改訂は、ISMS 認証取得組織及び ISMS ユーザに多大な負荷を強いる可能性があり、経済的影響も大きいと思われることから、今後とも改訂は慎重であるべきとの旨を説明した。この考えは、一定程度理解が得られたと思われる。

その上で、Annex A（管理目的及び管理策）を現状通り 27001 の附属書とすること、27001 と 27002 の関連についても現状通りとすること等が確認された。

・**27001** Information security management systems – Requirements

今回の審議では、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、WG1 にも対応が求められたため、審議時間の大半が本件への対応に充てられた。

そのためコメントの審議は全ては終了しなかったが、今回審議した内容を反映して 1st WD を作成することになった。

・**27002** Code of practice for information security management

27001 との関連は、前述のとおり現状通り維持されることとなった。また、カナダから管理目的・管理策の分類体系の大幅な見直しが提案され、論議が紛糾し、その採否については先送りとなった（1st WD 27002 に合わせてカナダが分類体系を修正し、再提出したうえで次回会議にて再検討される予定）。

コメントの審議は、8 章までしか進まなかったが、今回審議した内容を反映して 1st WD を作成することになった。

27003 Information security management system implementation guidance

FCD に対して、約 690 件（日本 160 件）のコメントが寄せられた。当初の投票結果は、投票総数 34 カ国、賛成 17 カ国、コメント付賛成 5 カ国、反対 7 カ国（日本、英国、オランダ、フィンランド、スイス、マレーシア、ポーランド）、棄権 5 カ国であったが、編集会議にて全てのコメントを検討し、会合中に追加案を作成する等の作業の結果、次の版は FDIS に進むことで合意された。

27004 Information security management – Measurements
2nd FCD に対して、約 660 件（日本 405 件）のコメントが寄せられた。投票結果は、投票総数 34 カ国、賛成 17 カ国、コメント付き賛成 4 カ国、反対 4 カ国、棄権 9 カ国であった。技術的なコメントも多数寄せられたが、2nd FCD としては今回、賛成国が多数であり、（その為大きな変更は再投票で問うことはできずプロジェクトの中止につながることから）大幅な変更を求めるコメントは採用せず、技術的な議論も行わないとするエディタの方針を WG1 委員長が支持したため、次回は FDIS に進むことで合意された。

27007 Guidelines for information security managements auditing
3rd WD に対して、約 150 件のコメントが寄せられた。ISO 19011 の改訂作業及び ISO/IEC 17021-2（仮題：マネジメントシステム認証機関に対する要求事項及びマネジメントシステムの第三者認証審査に対する要求事項）策定作業と調和を図りつつ作業が進めることを前提にコメント審議を行い、次回は 1st CD に進むことになった。

27008 Guidance for auditors on information security management systems controls
1st WD に対して約 110 件のコメントが寄せられた。複数の NB（National Body）から、本課題を TR から IS に上げるよう提案があったが、2nd WD 及び次回の会議結果を見てから判断することで合意され、次回は 2nd WD に進むことになった。

－その他（定期見直し、新規プロジェクト等）
27010 Information security management for inter-sector communications
（前回より継続審議）
現状に関して議論が分かれたが、結果的に英国とカナダとがエディタとなり、1st WD を作成することになった。

27012 ISM Guidelines for e-government（前回より継続審議）
前回のキプロス会議で NP が承認されたが進展が無く、今回の会議中にも意見が分かれたため、本プロジェクトを継続するか否かの投票が行われた。その結果、8 対 2 でキャンセルとなり、WG1 及び SC27 の総会でキャンセルが認められた。

27013 Guidance on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001
今回の会議前に実施された NP 投票において賛成多数で本プロジェクトは承認されたが、エディタ立候補・寄稿等はなく、本会議では特に進展はなかった。そのため、今回、臨時のエディタを務めた英国がアウトライン文書を作成することになり、それと同時にエディタと寄稿とを募集することになった。なお、本プロジェクトは、ISO/IEC 20000-1 担当の SC7/WG25（IT Service management）と連携して進められる予定。

27014 Information security governance framework

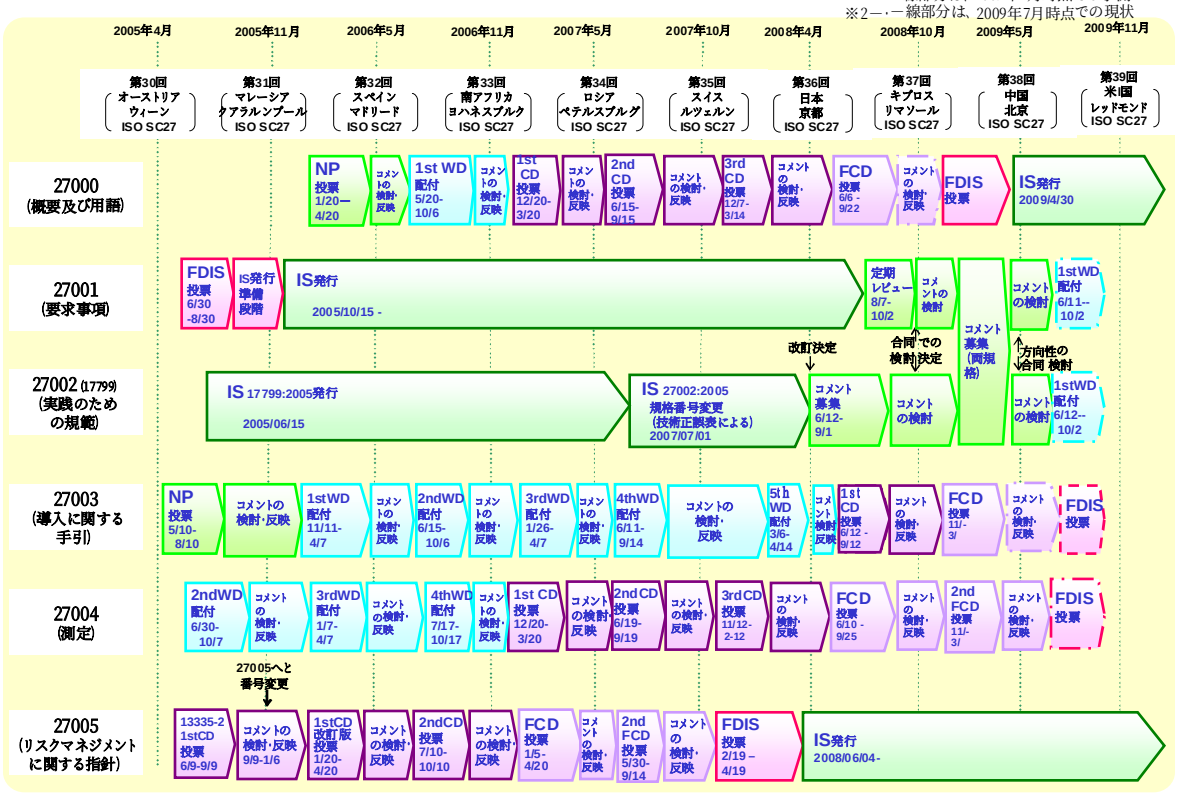
今回の会議前に実施された NP 投票において賛成多数で本プロジェクトは承認された。カナダ、日本、韓国からエディタの立候補があり、投票の結果、日本と韓国とがエディタとなった。本会議期間中に Draft WD を日本、韓国、ISACA（情報システムコントロール協会）の寄稿をベースに作成し、ISO JTC1/ WG6-CGIT（Corporate Governance of IT）に入力することになった。

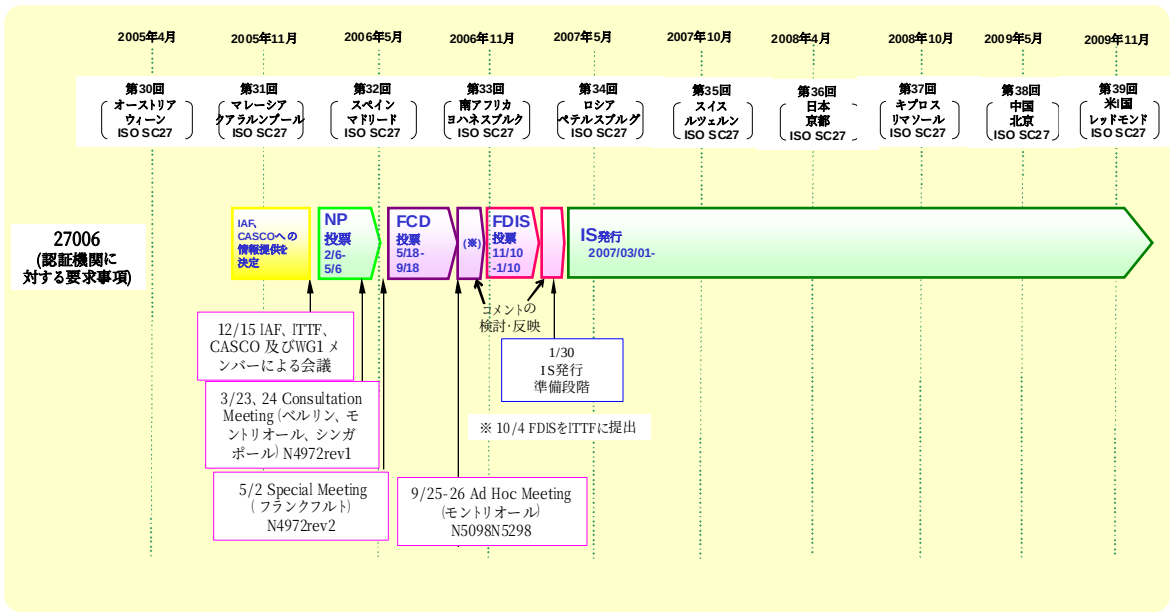
27015 Information security management for financial and insurance service sector

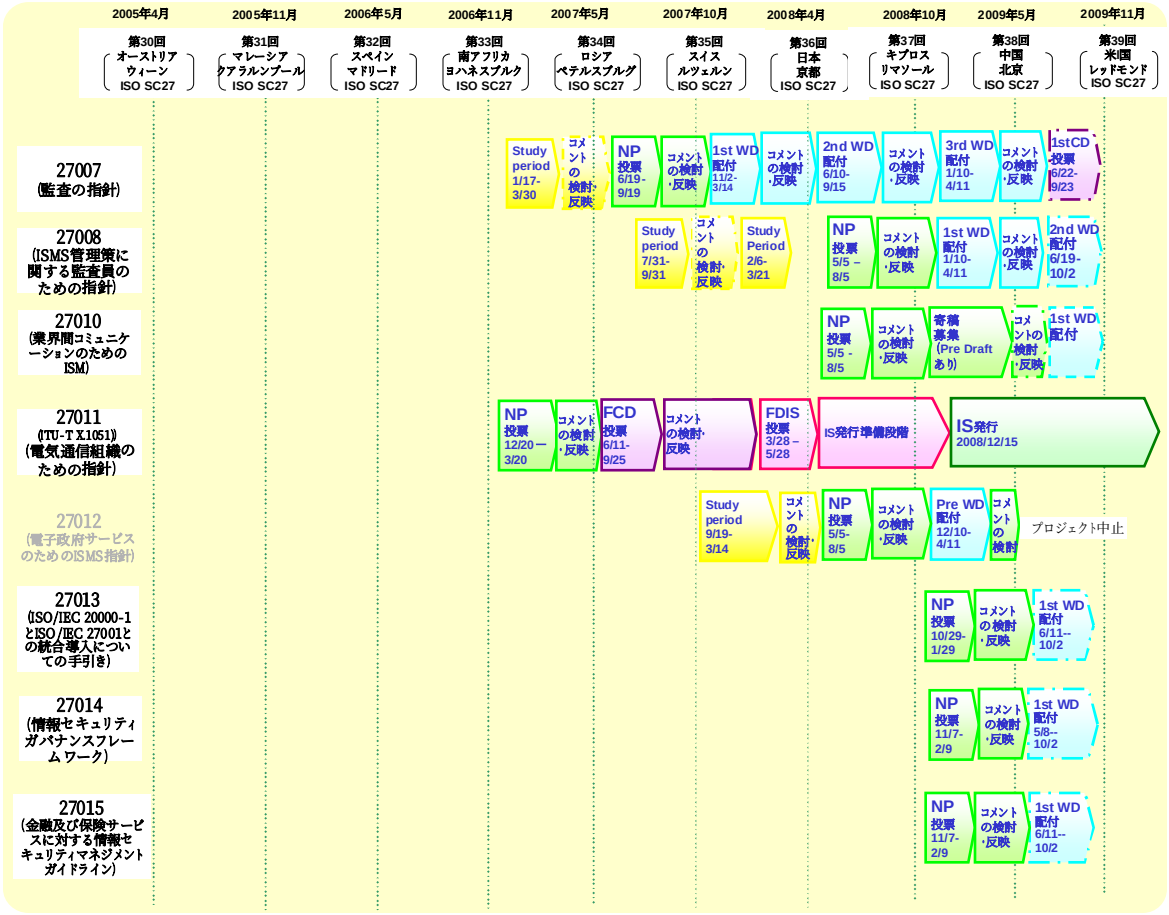
今回の会議前の NP 投票において賛成多数で本プロジェクトは承認された。ただし、英国、日本、スイス、南アフリカ、ロシアから ISO TC68（Financial services）との協調を第一にすべきとのコメントがあり、コメント対応にて、ISO TC68 と連携をとる必要があることが確認され、リエゾン文書を作成することとなった。米国とルクセンブルクとがエディタとなり、1st WD を作成することになった。

－ISO/IEC 27000 ファミリー規格作成の進捗状況一覧

※1---- 線部分は、2009年7月時点での予測
※2－･－線部分は、2009年7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
2009年11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
第39回 米国 レッドモンド ISO SC27
27007 (監査の指針)
27008 (ISMS管理策に関する監査員のための指針)
27010 (業界間コミュニケーションのためのISM)
27011 (ITU-T X.1051) (電気通信組織のための指針)
27012 (電子政府サービスのためのISMS指針)
27013 (ISO/IEC 20000-1とISO/IEC 27001との統合導入についての手引き)
27014 (情報セキュリティガバナンスフレームワーク)
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)
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 1/10-4/11
コメントの検討・反映
1stCD 投票 6/22-9/23
Study period 7/31-9/31
コメントの検討・反映
Study Period 2/6-3/21
NP 投票 5/5 – 8/5
コメントの検討・反映
1st WD 配付 1/10-4/11
コメントの検討・反映
2nd WD 配付 6/19-10/2
NP 投票 5/5 - 8/5
コメントの検討・反映
寄稿募集 (Pre Draft あり)
コメントの検討・反映
1st WD 配付
NP 投票 12/20 – 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
IS発行 2008/12/15
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
Pre WD 配付 12/10-4/11
コメントの検討
プロジェクト中止
NP 投票 10/29-1/29
コメントの検討・反映
1st WD 配付 6/11--10/2
NP 投票 11/7-2/9
コメントの検討・反映
1st WD 配付 5/8--10/2
NP 投票 11/7-2/9
コメントの検討・反映
1st WD 配付 6/11--10/2