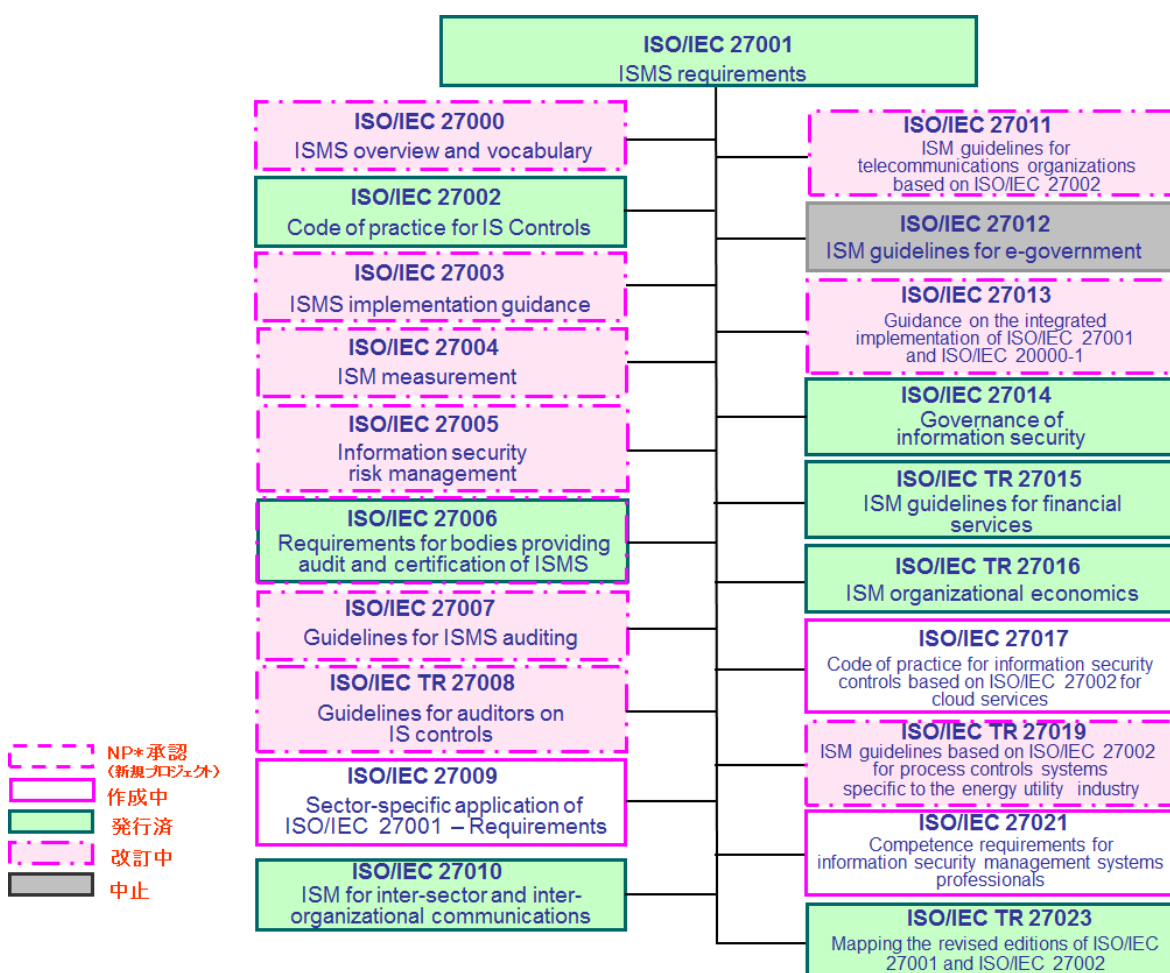


ISO/IEC 27000 ファミリーについて

2015年12月2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）の分科委員会 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、7 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。

<p>ISO/IEC 27000:2014 Information technology – Security techniques – Information security management systems – Overview and vocabulary 2014年1月発行〔第3版〕（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</p> <p>※ 国内規格としては、2014年3月に JIS Q 27000:2014 として制定された。</p> <p>JIS Q 27000:2014 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－用語 ISO/IEC 27000:2014 の箇条 2 の用語及び定義の技術的内容を変更することなく作成した国内規格（ISMS の概要などを示した ISO/IEC 27000:2014 の箇条 3 以降は含まれていない）。</p> <p>2014年10月メキシコ会議にて 27006 等の DIS 段階以降となった規格の用語掲載のための早期改訂、及び DIS 投票開始の承認のための手続きを実施することが決定された。この結果、DIS から開始する迅速法による、早期改訂が決定された。</p>
<p>ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements 2013年10月発行〔第2版〕 組織の事業リスク全般を考慮して、文書化した ISMS を確立、実施、維持及び継続的に改善するための要求事項を規定した規格</p> <p>※ 国内規格としては、2014年3月に JIS Q 27001:2014（JIS Q 27001:2006 の改正版）として制定された。</p> <p>JIS Q 27001:2014 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</p> <p>なお、2014年9月に、ISO より正誤票が発行されている（JIS 正誤票は 2014年11月に発行）。その後、2015年11月にも正誤票が発行された。</p> <p>2008年10月リマソール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。これを受けた改訂作業を経て、2013年10月に改訂版が発行された。</p>
<p>ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls 2013年10月発行〔第2版〕 組織の情報セキュリティリスクの環境を考慮に入れた管理策の選定、実施及び管理を含む、組織の情報セキュリティ標準及び情報セキュリティマネジメントを実施するための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。</p> <p>*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。</p> <p>※ 国内規格としては、2014年3月に JIS Q 27002:2014（JIS Q 27002:2006 の改正版）として制定された。</p> <p>JIS Q 27002:2014 情報技術－セキュリティ技術－情報セキュリティ管理策の実践のための規範</p>

なお、2014年9月に、ISOより正誤票が発行されている（JIS正誤票は2014年11月に発行）。その後、2015年11月にも正誤票が発行された。

2008年10月リマソール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。これを受けた改訂作業を経て、2013年10月に改訂版が発行された。

ISO/IEC 27003:2010

Information technology – Security techniques – Information security management system implementation guidance

2010年2月発行（現在、改訂審議中）

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早期改訂開始が決定された。

現在実施中の改訂審議の中で、第2版では適用範囲の変更とともに標題が以下に変更されることになった。

Information technology – Security techniques – Information security management system – Guidance

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。

現在実施中の改訂審議の中で、第2版では適用範囲の変更とともに標題が以下に変更されることになった。

Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation

ISO/IEC 27005:2011

Information technology – Security techniques – Information security risk management

2011年6月発行〔第2版〕（現在、改訂審議中）

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（第2版）が発行された。

2013年5月ソフィアアンティポリス会議後に開始されたNP投票の結果を受けて、2013年10月インチョン会議にて早期改訂開始が決定された。

ISO/IEC 27006:2015

Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems

2015年10月発行〔第3版〕

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、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。（ISO/IEC 27006:2015に対応したJIS改正については未発行。）

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 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年に第2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。これを受けた改訂作業を経て、2015年に第3版が発行された。

ISO/IEC 27007:2011

Information technology – Security techniques – Guidelines for information security management systems auditing

2011年11月発行（現在、改訂審議中）

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。

2014年4月香港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 TR 27008:2011

Information technology – Security techniques – Guidelines for auditors on information security controls

2011年10月発行（現在、改訂審議中）

組織の情報セキュリティの管理策のレビューに関する技術報告書（TR：Technical Report）。

2014年4月香港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 27009（作成中）

Information technology – Security techniques – Sector specific application of ISO/IEC 27001 - requirements

セクター規格を作成する組織に対する、27001適用について規定する規格。

ISO/IEC 27010:2015

Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications

2015年11月発行〔第2版〕

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。情報共有コミュニティの中で情報セキュリティマネジメントを実施するためのガイダンスや、セクター間及び組織間コミュニケーションにおける情報セキュリティに関する管理策及び手引を提供する。

2014年10月メキシコ会議にて27001:2013対応のための早期改訂、及びDIS投票開始の承認のための手続きを実施することが決定された。この結果、DISから開始する迅速法による、早期改訂が決定された。これを受けた改訂作業を経て、2015年に第2版が発行された。

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（現在、改訂審議中）

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。

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

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（現在、改訂審議中）

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。

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

ISO/IEC 27014:2013

Information technology – Security techniques – Governance of Information security

2013年4月発行

情報セキュリティのガバナンスに関する規格であり、情報セキュリティガバナンスの原則及びプロセスの手引を提供する。

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に関する技術報告書。

ISO/IEC TR 27016:2014

Information technology – Security techniques – Information security management – Organizational economics

2014年2月発行

組織の情報資産の保護に対して経済学的な視点を適用し、モデル及び例示の使用を通して情報セキュリティに関する組織の経済性を適用する方法の手引を提供する技術報告書。

ISO/IEC 27017（作成中）

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

クラウドサービスにおける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を提供する規格。

ISO/IEC TR 27019:2013

Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

エネルギー業界向けプロセス制御システムのためのISO/IEC 27002に基づく情報セキュリティマネ

<p>ジメメントに関する技術報告書。 2013年7月発行（現在、改訂審議中）</p> <p>2014年10月メキシコ会議にて、1年間の Study Period での審議結果を経て、早期改訂の開始が決定された。</p>
<p>ISO/IEC 27021（作成中）</p> <p>Information technology -- Security techniques -- Competence requirements for information security management systems professionals ISMS 専門家の力量に関する要求事項について規定した規格</p>
<p>ISO/IEC TR 27023</p> <p>Information technology -- Security techniques -- Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002</p> <p>2015年7月発行</p> <p>ISO/IEC 27001 及び ISO/IEC 27002 新旧対応表をまとめた技術報告書。</p> <p>2013年に10月に発行された ISO/IEC JTC 1/SC 27 N13143「JTC 1/SC 27/SD3 – Mapping Old-New Editions of ISO/IEC 27001 and ISO/IEC 27002」の内容をそのまま取り込んだものである。SD3（Standing Document 3）は ISO の内部文書であるため、より正式な ISO 文書である TR として発行することになった。</p> <p>2014年7月～10月に早期発行のための DTR 投票が行われ、可決された。これを受けた手続を経て、2015年に発行された。</p>

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51回 WG 1 会儀は、2015年10月26日～30日にジャイプール（インド）にて開催されました。この会合での検討状況は次の2-1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：

<https://www.itsci.ipsj.or.jp/>

2-1 第 51 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

※下表の色分け：緑色は発行済規格、薄黄色は改訂中規格、灰色は中止プロジェクトです（白は作成中）。

ISO/IEC 番号	規格内容	第 51 回会議 (今回：2015 年 10 月)	第 52 回会議 (次回予定：2016 年 4 月)
ISO/IEC 27000	概要及び用語	IS _[第 3 版] (SP、DIS)	IS _[第 4 版] (IS)
ISO/IEC 27001	要求事項	IS _[第 2 版]	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 2 版]	IS _[第 2 版]
ISO/IEC 27003	導入に関する手引	IS _[第 1 版] (改訂中：2nd CD)	IS _[第 1 版] (改訂中：DIS)
ISO/IEC 27004	測定	IS _[第 1 版] (改訂中：2nd CD)	IS _[第 1 版] (改訂中：DIS)
ISO/IEC 27005	リスクマネジメントに関する指針	IS _[第 2 版] (4th WD)	IS _[第 2 版] (5th WD)
ISO/IEC 27006	認証機関に対する要求事項	IS _[第 2 版] (改訂中：FDIS)	IS _[第 3 版]
ISO/IEC 27007	監査の指針	IS _[第 1 版] (2nd WD)	IS _[第 1 版] (3rd WD)
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] (2nd WD)	TR _[第 1 版] (3rd WD)
ISO/IEC 27009	セクター規格への 27001 適用に関する要求事項	DIS	FDIS
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] (DIS)	IS _[第 2 版]
ISO/IEC 27011	電気通信組織のための指針	IS _[第 1 版] (改訂中：DIS)	IS _[第 1 版] (改訂中：FDIS)
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 との統合導入に関する手引	IS _[第 1 版] (改訂中：FDIS)	IS _[第 2 版]
ISO/IEC 27014	情報セキュリティのガバナンス	IS _[第 1 版]	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)	TR _[第 1 版]	TR _[第 1 版]
ISO/IEC 27017	クラウドサービスにおける 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	FDIS	IS
ISO/IEC TR 27019	エネルギー業界向けプロセス制御システムのための ISO/IEC 27002 に基づく ISM の指針	TR _[第 1 版] [WD]	TR _[第 1 版] [2nd WD]
ISO/IEC 27021	ISMS 専門家の力量に関する要求事項	2nd WD	3rd WD
ISO/IEC TR 27023	ISO/IEC 27001 及び ISO/IEC 27002 改訂版のマッピング	IS	IS

*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
※SP : Study Period

2-2 第 50 回 SC 27/ WG 1 会議における検討状況（詳細）

ー主要プロジェクト進捗状況

27000 Information security management systems – Overview and vocabulary

6 月 19 日に終了した DIS 27000 に対する DIS 投票では、賛成 29 か国、コメント付賛成 5 か国、反対 0 か国、棄権 13 か国であり、コメント総数は約 100 件であった。DIS に対する反対投票がなかったことにより、FDIS をスキップして IS 発行に進むことが可能な状況であった。

今回の編集会議では、約 10 件の technical (te) コメントの処理を行った後、IS に進むことについて編集会議参加者からの反対は特になかった。

このため今回の会議の結果、(FDIS をスキップして) IS 発行に進むことになった。

27001、27002 Defect Report

前回会議で 27001、27002 とともに、Technical Corrigenda（正誤票）を発行することになったため、前回会議終了後にこの発行に係る投票を行った。その結果、発行について可決され、11 月に Technical Corrigenda が発行された。

関連 URL：http://www.isms.jipdec.or.jp/topics/27001_27002_2013_Cor2.html

27003 Information security management system – Guidance

今回の会議に先立って行われた 2nd CD 27003 に対する CD 投票では、賛成 20 か国、コメント付賛成 4 か国、反対 3 か国（スイス、日本、英国）、棄権 20 か国であり、コメント総数は約 600 件であった。

審議の中で、特にスイス及び英国のコメントによって多くの改善が加えられることになった。

今回の審議の結果、次回は DIS へ進むことになった。

27004 Information security management systems – Monitoring, measurement, analysis and evaluation

今回の会議に先立って行われた 2nd CD 27004 に対する CD 投票では、賛成 19 か国、コメント付賛成 7 か国、反対 2 か国（スイス、日本）、棄権 18 か国であり、コメント総数は約 90 件であった。編集会議では、主に反対国のコメントを中心に審議を行った。その結果、2nd CD 27004 では内容が全体的に measurement 偏重となっていた点について解消され、また文章自体も大幅に変更された。

今回の審議の結果、次回は DIS へ進むことになった。

27005 Information security risk management

今回の会議に先立って、4th WD 27005 に対して、約 300 件のコメントが寄せられた。

編集会議では、te コメントの処理が終了し、この結果テキスト全体に変更が加えられることになった。特に、リスクアセスメント手法の記述の risk identification の記事では、Scenario based approach と Asset based approach を併記し、かつ、Scenario based approach を先に置くことになった。

一方で、プロジェクトスケジュールがひっ迫しており、次の段階について WG1 会議最終日の Plenary にて投票が行われた結果、プロジェクトキャンセル（SP に差し戻し）には至らなかったものの、次回は（CD ではなく）5th WD に進むことになった。

27007 Guidelines for information security management systems auditing

今回の会議に先立って、2nd WD に対して約 30 件のコメントが寄せられており、これらのコメントに基づいて審議した。

その結果、本文については大幅な変更はなかったが、附属書 A (ISMS 監査実施の手引)について日本及び英国提案により大幅に変更することになった。

今回の編集会議の結果、次回は、3rd WD に進むことになった。

27008 Guidelines for auditors on information security controls

今回の会議に先立って、2nd WD に対して約 50 件のコメントが寄せられており、これらのコメントに基づいて審議した。

特に audit の用語について審議され、27007 との相違を明確にするとの主旨は理解するが、assessor は欧米では専門職業を意味するため、内部監査人が排除されるという影響があることを考慮し、assessor は Information security auditor に統一することになった。なお、audit は assess に変更することになり、標題も以下の通り変更することになった。これを受けて標題変更に関する投票が開始されることになった。

新タイトル: Guideline for assessment for information security controls

27009 Sector specific application of ISO/IEC 27001 - requirements

今回の会議に先立って行われた DIS 27009 に対する DIS 投票では、賛成 21 か国、コメント付賛成 4 か国、反対 5 か国 (オーストラリア、フランス、ドイツ、日本、英国)、棄権 12 か国であり、コメント総数は約 200 件であった。

なお、今回、DIS 27009 の投票期限がジャイプール会議中の 10 月 27 日 (火) であったため、N 文書として Draft disposition of comments を事前配布する時間はなく、(会議中にエディタがコメントを取り纏め) 10 月 29 日 (木) の会議当日に、Draft disposition of comments が配布された。

編集会議では、反対国のコメントを中心に審議した結果、DIS 27009 で不明確だったテキストの改善が行われた。また、今回のコメントの多くは附属書 A (27001/27002 に基づくセクター別規格のテンプレート) に対するものであり、これらのコメントを審議した結果、附属書 A は大幅に変更された。

今回の会議の結果、次回は FDIS に進むことになった。

なお、テンプレート (27009 の附属書 A) の使い方に関する事例が必要性和のドイツコメントを受けて、12 か月間の SP を設置し、事例の必要性を検討することになった。

以上