

IT サービスマネジメントシステム認証機関の パイロット認定の指針

JAB MS308P-2008

制定日：2008年10月24日

財団法人日本適合性認定協会

IT サービスマネジメントシステム認証機関のパイロット認定の指針

序文

この指針は、IT サービスマネジメントシステム (ITSMS) 認証に対して JIS Q 17021:2007(JAB MS100「マネジメントシステム認証機関に対する認定の基準」)を適用するにあたっての指針を示すものである。

この文書は、itSMF*が ISO/IEC Guide 62 及び IAF Guidance to ISO/IEC Guide 62 に沿って作成した itSMF 15/015 (Scheme for Bodies Operating the Certification /Registration of IT Service Management Systems) を参考にして作成した。なお、年版の表示のない引用文書については、最新版を適用する。

*itSMF は英国で 1991 年に非営利団体(NPO)として設立された会員制ユーザ・フォーラムで、1980 年代後半に英国政府の OGC(Office of Government Commerce)が作成した情報システムの運用管理基準 [ITIL (IT Infrastructure Library)] の普及促進を目的として設立された。

備考 1:この指針は、itSMF 15/015 を JAB 認定基準 MS100 適用の指針としており、itSMF 15/015 に示される approval body が「本協会」を指すものと見なして差し支えない。

備考 2:この文書の全体を通して、「...なければならない」という用語は、要求事項を反映した強制規定であることを示すために使用されている。指針中の「...望ましい」という用語は強制ではないが、要求事項を満たすために認められた手段として提供されている指針であることを示すために使用されている。

1. 適用範囲

この指針は、財団法人日本適合性認定協会が JIS Q 17021 に基づき ITSMS 認証業務を行っている第三者機関(以下、ITSMS 認証機関という)の適格性と信頼性について認定審査及び認定を行うために使用する指針である。

この文書では、JIS Q 17021 の項目を太字で示し、各条項に指針を与える場合、参照しやすいように“G”の文字を付けて識別した。また対応する itSMF15/015 の条項を各指針の末尾に“SM”の文字を付けて示した。

2. 引用規格及び関係文書

この項に掲げる規格及び文書のうちで、西暦年を付記してあるものは、記載の年の版を適用し、その後の改正版(追補を含む)には適用しない。西暦年の付記のない引用規格又は文書は、その最新版(追補を含む)を適用する。本協会の文書の最新版は、本協会ウェブサイト(www.jab.or.jp)で閲覧及びダウンロード可能。

2.1 引用規格

次に掲げる規格は、この基準に引用されることによって、この指針の規定の一部を

構成する。

JIS Q 20000-1:2007 (ISO/IEC 20000-1:2005) 情報技術 - サービスマネジメント
- 第 1 部 : 仕様

JIS Q 20000-2:2007 (ISO/IEC 20000-2:2005) 情報技術 - サービスマネジメント
第 2 部 : 実践のための規範

itSMF 15/015 Scheme for Bodies Operating the Certification
/Registration of IT Service Management Systems

JIS Q 17021:2007 適合性評価 - マネジメントシステム認証の審査および認
証を提供する機関に対する要求事項

JIS Q 9000:2006 (ISO 9000:2005) 品質マネジメントシステム - 基本及び用語

JIS Q 17000:2005 (ISO/IEC 17000:2004) 適合性評価 - 用語及び一般原則

JIS Q 19011:2003 (ISO 19011:2002) 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

2.2 関連文書

JAB MS100-2007 マネジメントシステム認証機関に対する認定の基準

JAB MS208P IT サービスマネジメントシステム認証機関のパイロット認
定の手順

3 . 用語及び定義

この指針の目的のために、JIS Q 20000-1、JIS Q 20000-2、JIS Q 17000 及び JIS Q
9000 記載の該当する定義を適用する。

4 . 原則

4.1 一般

4.2 公平性

4.3 力量

4.4 責任

4.5 透明性

4.6 機密保持

4.7 苦情への適切な対応

5 . 一般要求事項

5.1 法的及び契約上の事項

5.2 公平性のマネジメント

5.3 債務及び財務

6 . 組織運営機構に対する要求事項

6.1 組織構造及びトップマネジメント

6.2 公平性委員会

6.2.2

6.2.2 項に対する指針(G.6.2)

G.6.2 6.2.2 項でいう利害関係者とは、産業界及び商業界における顧客及び組織、規制当局、貿易機関、IT サービスマネジメントの専門家及び関連専門家、並びに政府がある。

(SM.2)

7 . 資源に対する要求事項

7.1 経営層及び要員の力量

7.1項に対する指針(G.7.1.1 - G.7.1.2)

G.7.1.1 この指針で重要とすべき項目は、認証プロセスを方向づけ、また管理する認証機関の能力にある。ITSMS認証を実施するために必要な能力の必須事項として、全体的な力量が審査対象の活動及び関連のITサービスマネジメント事項に適切である要員を選択、提供及び管理することである。

(SM.3マネジメントの力量 SM.3.1一般)

G.7.1.2 認証機関が、システムを構築し、それは審査対象の組織のITSMSに関連する技術的及び法的展開に関する知識を確実にするものでなければならない。

認証機関は、ITサービスマネジメントの力量分析のために効果的なシステムをもたなければならない、それが運用されるすべての技術的分野に対して利用できなければならない。

認証機関は、関連の契約内容の確認ができる能力をもたなければならない。また、各顧客に対する契約内容の確認に先立って、関連の産業分野の要求事項についての力量分析(ニーズの評価を行ったうえでそれに対応したスキルの決定)を実施したことを実証できなければならない。特に、認証機関では、次の活動を完了する能力があることを、実証しなければならない

- a) 組織の産業分野の活動領域において、ITサービスマネジメントに関連する固有の事項とその改善を特定する。
- b) 組織の活動領域を定義する。
- c) a)で特定したことに関連し、組織の活動範囲全体から生じる、組織のサービスに固有の事項、改善を確認する。
- d) 特定した活動、及び組織のITサービスマネジメントに関連する事項、改善に関連して、認証を行うために、機関内で必要な能力を明確にする。
- e) 要求される力量が利用できることを確認する。

(SM.3マネジメントの力量 SM.3.2力量分析ならびに契約内容の確認)

7.1.1

7.1.1項に対する指針(G.7.1.3)

G.7.1.3 認証機関の認定範囲は、審査員の力量と密接に関連しており、これは、組織がITSMSを構築及び維持するに当たって実施する実施・改善計画の審査において

特に重要である。認証機関は認定機関に対して、ITSMSが審査及び認証される産業分野で審査員に力量があることを実証することが要求される。

(SM.1)

7.2 認証活動に関与する要員

7.2項に対する指針(G.7.2.1)

G.7.2.1 認証機関は、ITSMS認証の授与、維持、拡大、縮小、一時停止又は取消しに関する決定のプロセスを管理するための能力、プロセス、手順をもたなければならない。

(SM.3 マネジメントの力量 SM.3.4 認証決定プロセスのマネジメント)

7.2.4

7.2.4項に対する指針(G.7.2.2)

G.7.2.2 認証機関は、審査チームが次に関して適切なレベルであることを確実にするために、教育訓練と選定のための基準をもたなければならない。

- a) ITSMS規格又は規準文書の理解
- b) ITサービスマネジメントのプロセス、手順、問題の理解
- c) 実施、サービス改善計画、管理の理解
- d) 審査対象の活動に関する専門的知識
- e) 組織内のITSMSに関連する規制要求事項の知識
- f) マネジメントシステム審査の力量
- g) マネジメントシステムの知識

(SM.3 マネジメントの力量 SM.3.3 審査チームの教育訓練と選定)

7.2.5

7.2.5項に対する指針(G.7.2.3 - G.7.2.6)

G.7.2.3 ITSMS審査を実施するために認証機関に雇用される要員は、JIS Q 19011に基づき、次の基準に適合していなければならない。

ITSMS審査を実施するために人材を雇用する場合、チームメンバー内で、(G 7.2.5 SM 5.3)に記載される特質を分け合うこともありうる。

- a) 教育：大学卒業レベル(広範な経験と補足的な専門教育および訓練は、当該レベルと同等とみなす)
- b) 4年以上のフルタイムでの情報技術の分野での実務経験。このうち2年以上はITサービスマネジメントに関係する役割又は職務を経験したものであること。
- c) ITSMS審査、およびITSMS審査の管理に関する5日間の研修を成功裏に修了していること。
- d) 審査員としての責任を負う前に、候補者はITSMS全審査過程を経験しておくことが望ましい。この経験は、書類審査、改善プログラム、現地審査、審

査報告書の作成を含む、4回以上延べ20日にわたる審査への参加によって得られたものであることが望ましい。

- e) これらの経験はすべて合理的に最新のものであることが望ましい。
- f) JIS Q 19011 7.2項に示されている個人的特質を備えていることが望ましい。候補者は、複雑な業務を広い視野に置き、より大きな組織における個々の部門の役割を理解できることが望ましい。
- g) ITサービスマネジメント及び審査に関する知識及び技能および専門を維持していること。

主任審査員として審査を遂行する審査員の場合は、上記に加えて次の要求事項を満たすことが望ましい。

- h) 評価プロセスを管理するための知識および特性をもつ
- i) 少なくとも3回のITSMS審査に対して、審査チームリーダーとして参加している。
- j) 審査プロセスを管理する知識及び特質をもっている。
- k) 口頭及び文書の両方で効果的な意思疎通ができる能力を実証している。
(SM.3 マネジメントの力量 SM.4 審査員の力量)

G.7.2.4 技術専門家を除く、審査チームの各員に、次の要求事項が適用される。

審査チームの全員が次の事項について適切な経験理解をもっていることを実証できなければならない。

- a) ITSMS規格又は規準文書
- b) マネジメントシステムの一般的概念
- c) ITサービスマネジメントへの各分野に関連した問題
- d) 実施、サービス改善計画、及び管理に関連した原則及びプロセス
- e) 審査の原則
(SM.5 審査チームの力量 SM.5.2)

G.7.2.5 次の要求事項が審査チーム全体に適用される。

- a) 次の各分野で、少なくとも1人の審査チームメンバーが、チーム内で責任をもつことについて、認証機関の基準を満足することが望ましい。
 - i) チームの管理
 - ii) ITサービスマネジメントの事項に関連する法規制要求事項及び法的適合の知識
 - iii) ITサービスマネジメントプロセス関連事項の特定
 - iv) 組織の脆弱性の特定、並びにその影響、その軽減及び制御の理解
 - v) 当該分野の現在の最新技術の知識
 - vi) ITサービスマネジメントに関連する実施、サービス改善計画活動の知識
- b) 審査チームは、組織のITSMSにITサービスマネジメントインシデントを示唆するものを見出した場合、その示唆するものをITSMSの適切な要素にたどり着くまで追跡できる力量があることが望ましい。

c) 上記a)に示されている要求事項全てを満足するならば、審査チームは一人でもよい。

(SM.5 審査チームの力量 SM.5.3)

G.7.2.6 プロセス及びITサービスマネジメントの問題に係り組織に影響のある法規制に関して特定の知識のある技術専門家を、上記の基準をすべて満たさなくとも、審査チームの一部としてよい。技術専門家は、単独で機能させないことが望ましい。

(SM.5 審査チームの力量 SM.5.4 技術専門家の起用)

7.2.9

7.2.9項に対する指針(G.7.2.7 - G.7.2.8)

G.7.2.7 認証機関において認証の授与/取消しの決定を行う者（一個人の場合もあり得る）は、審査プロセスおよび審査チームによる関連の推薦を評価するのに十分な水準の知識や経験をもっていることが望ましい。

(SM.13 認証に関する決定)

G.7.2.8 認証決定を行う者は、通常、審査チームによる否定的な推薦を覆すことは望ましくない。そのような状況が起きた場合、認証機関は、推薦を覆す決定の基礎を文書に残し、その正当性を示さなければならない。

(SM.11 認証の決定)

7.3 個々の外部審査員及び外部技術専門家の起用

7.4 要員の記録

7.5 外部委託

8 . 情報に関する要求事項

8.1 公にアクセス可能な情報

8.2 認証文書

8.3 被認証組織の登録簿

8.4 認証の引用及びマークの使用

8.5 機密保持

8.6 認証機関とその依頼者間の情報交換

8.6.1 認証活動及び要求事項に関する情報

8.6.2 認証機関による変更の通知

8.6.3 依頼者による変更の通知

9 . プロセス要求事項

9.1 一般要求事項

9.1 項に対する指針(G.9.1.1 - G.9.1.2)

- G.9.1.1 認証機関は、申請者は、審査の開始に先立ち、内部監査のプロセスが計画されていること、並びにそのプログラム及び、プロセス/手順が運用され、その運用を示すことができることを実証できるように申請者に対して要求するプロセス/手順をもっていることが望ましい(注：審査については JIS Q 17021 の 5.2 も参照)。

認証機関は、ITSMSの設計に関する文書を入手することが望ましい。この文書には、少なくとも組織が実施したITサービスマネジメント関連の問題と計画に関する分析、ITサービスマネジメントの方針、ITSMSの核となる要素を含む。上記のITサービスマネジメント文書から、審査員は次を実施することが望ましい：

- a) 組織が自らの方針、目的及びプロセスを守っていることの確認
 - b) ITSMSがITSMS規格又は規準文書のすべての要求事項に適合していること及び組織の方針・目的を達成しつつあることの確認
- これを行うために、審査では組織の次の点に焦点を絞ることが望ましい。
- a) ITサービスマネジメントに関連する問題のアセスメント及びその結果に基づくITSMS設計
 - b) ITサービスマネジメントの方針
 - c) このプロセスから導き出された目的および目標
 - d) 目的および目標に照らしたパフォーマンスの監視、測定、報告、及び見直し
 - e) プロセス及びマネジメントのレビュー
 - f) ITサービスマネジメントの方針に対する経営層の責任
 - g) 方針、ITサービスマネジメントのインパクト及びリスクアセスメントの結果、目的及び目標、プロセス、責任、計画、プロセス/手順、パフォーマンスデータ、見直し、及び継続的改善計画との対応
- (SM.9 審査の方法論)

- G.9.1.2 ITSMS認証の分野における多数サンプリングの決定は、品質システムに対する同様の決定よりさらに複雑である。多数サイトの審査にサンプルをベースにした方法を採用することを希望する認証機関は、サンプリングプログラムを構築するに当たって、下記問題の全範囲にわたる手順を維持する必要がある。サンプリングにより第一回目の審査を行う前に、認証機関は、使用する方法及びプロセス/手順を認定機関に示し、多数サイトITSMS審査を管理するために下記の問題をどう考慮するのかを具体的に示さなければならない。

認証機関のプロセス/手順は、最初の契約内容の確認で最大限可能な限りサイト間の違いを明確にし、下記規定に従ってサンプリングの適正なレベルが決定されるようにすることが望ましい。組織は単一のITSMSでカバーされる多くの類似サイトをもっている場合、次の条件を満たしていれば、その組織に、それらすべてのサイトをカバーする認証文書を発行してもよい。

- a) すべてのサイトが同一のITSMSのもとに運営されていること。そして、そのITSMSは中央で管理され、監査され、かつ、中央の経営層による見直しに付されていること
- b) 組織の内部審査プロセス/手順に基づいてすべてのサイトが監査を受けていること
- c) 下記の要求事項を考慮して、代表し得る数のサイトを認証機関がサンプルとして取上げていること。
 - i) 本社及びサイトの内部審査結果
 - ii) マネジメントレビューの結果
 - iii) サイトの大きさの違い
 - iv) サイトの業務目的の違い
 - v) ITSMSの複雑度
 -) 異なるサイトでの情報システムの複雑度
 -) 作業慣例の違い
 -) 異なるサイトで行われているITSMS活動の違い
 - ix) 重要な情報システム又は機密情報を処理する情報システムとの潜在的相互作用
 - x) 法的要求事項の違い
- d) サンプルは、上記c)項に基づき一部は選択可能で、一部は必須であることが望ましい。その結果、サイト選定のランダムな要素を失うことなく、広い範囲の異なるサイトが選ばれることが望ましい。
- e) 認証機関は、認証に先立ち、資産に対する著しい脅威、ぜい弱性、又は影響の対象となるITSMSに含まれるすべてのサイトを審査することが望ましい。
- f) サーベイランス・プログラムは、上記の要求事項に照らして作成され、妥当な期間内に、当該組織又はITサービスマネジメント方針に含まれるITSMSの認証範囲の中にあるすべてのサイトをカバーすることが望ましい。
- g) 本部又はどこか一つのサイトで不適合が見つかった場合は、本部及びその認証がカバーしているすべての該当するサイトにその是正処置手順を適用することが望ましい。

G.9.1.1 (SM.9)に記載した審査では、組織の本部の活動を取り上げ、単一のITSMSがすべてのサイトに適用され、運用レベルで中央の管理が行き渡っていることを確保することが望ましい。審査では、上記で述べたすべての問題を扱わなければならない。

(SM.8.1 多数サイト)

9.1.1

9.1.1項に対する指針(G.9.1.3 - G.9.1.5)

G.9.1.3 ITサービスマネジメントに関する資産に対する脅威、ぜい弱性、組織に及ぼす影響、重要だと思われるものに対する管理策：認証機関の役割

ITサービスマネジメントに関する脅威、脆弱性、及び組織に及ぼす影響を特定、検討、評価を行うためのプロセス/手順に一貫性をもちながら確立し、維持していることについての信頼性を確保するために、認証機関は、次の要因を考慮することが望ましい。

- a) ITサービスマネジメントのプロセスが組織に妥当でありかつ適切であるとみなされ、その重要性を特定するための基準を設定し、これを行うための手順を開発するのは組織の仕事である。
- b) 認証機関は、ITサービスマネジメントのプロセスの範囲の分析と適切な対策が、次のプロセス内において組織の運用のために実施されたことを実証するよう組織に要求することが望ましい。
 - サービスデリバリプロセス（サービスレベル管理、サービスの報告、サービス継続性及び可用性管理、ITサービスの予算管理及び会計、キャパシティ管理、情報セキュリティ管理）
 - 関係プロセス（事業関係管理、サプライヤ管理）
 - 解決プロセス（インシデント管理、問題管理）
 - コントロールプロセス（構成管理、変更管理）
 - リリースプロセス（リリース管理）
- c) 組織の方針、目的及び目標、プロセス/手順又はその適用結果との間の矛盾点

認証機関は、重大性の分析に用いられるプロセス/手順が妥当なものであり適切に実施されているかどうかを確認することが望ましい。ITサービスマネジメントのインシデントで、組織に及ぼす影響が重大であると認識されている場合、ITSMS内で管理されていることが望ましい。

(SM.10 ITSMS審査の個別の要素 SM.10.1)

- G.9.1.4 法的適合の維持及びは、組織の責任である。認証機関は、ITSMSがこの点において機能しているかどうかの信頼性を確実にするために必要なチェック及びサンプリングにとどめるのが望ましい。

ITSMSの認証を受けた組織は、その組織に適用される規制上の要求事項に継続して適合すべきマネジメントシステムを保有しているということである。認証機関は、要求事項が遵守され得るシステムが完全に実施されていることを確認する。

(SM.10.2 規制への適合：認証機関の役割)

- G.9.1.5 ITSMS文書とその他のマネジメントシステム（品質、安全衛生、環境などのような）とで文書を併せたものにしてもよいが、ITSMSが、その他のシステムとの適切なインタフェースとともに、明確に識別できることが前提になる。

(SM.10.3 ITSMS文書とその他のマネジメント文書との統合)

9.1.10

9.1.10項に対する指針(G.9.1.6)

G.9.1.6 認証に関する決定の基礎として、認証機関は、その決定を行うために十分な情報を含む明確な報告書を審査チームに要求する。

a) 審査チームから認証機関への報告書は、審査プロセスのさまざまな段階で必要となる。既にファイルされている情報を組み合わせて、この報告書には、少なくとも次を含めることが望ましい。

i) 文書審査の要約を含めた審査の詳細

ii) 組織のITサービスマネジメントのプロセス、活動、見直しに関する評価の詳細

iii) 審査時間の合計、並びに書類審査、プロセスの評価、実施状況の審査及び審査報告書の作成にかかった時間の内訳

iv) 不適合の明確な記述、使用した調査項目及びそれらを選択した根拠並びに採択した手法

v) 審査チームによる認証機関への認証に関する推薦

b) サーベイランス報告書には、特に、以前に指摘された不適合事項の是正に関する情報を含めることが望ましい。また、サーベイランス報告書には、少なくとも上記a)の要求事項を全体として包めることが望ましい。

(SM.12 審査チームによる認証機関への報告)

9.2 初回審査及び認証

9.2項に対する指針(G.9.2.1)

G.9.2.1 申請組織は、ITSMS規格又は規準文書のどの部分が組織のITSMSに関連し適用されるかを記述したITサービスマネジメント方針を準備しなければならない。ITサービスマネジメント方針は、審査チームに提供される作業文書の一部としなければならない。

(SM.7 ITサービスマネジメント方針)

9.2.1

9.2.1項に対する指針(G.9.2.2)

G.9.2.2 組織は、ITSMSの範囲を明確にすることが望ましい。認証機関の役割は、組織が本来適正にITSMSに入れておくべき活動の要素を認証の範囲から除外していないことを確実にすることに一貫性を提供することである。

したがって、認証機関は、組織のITサービスマネジメントの範囲が組織の活動を適切に反映しており、実施・改善計画がITSMS文書で規定されている活動の境界にまで及んでいることを確実にすることが望ましい。

ITSMSの範囲内とは必ずしもいえないサービス又は活動とのインタフェース

は、認証の対象となっているITSMSの範囲の中で扱われ、組織のITサービスマネジメントの活動に含まれることが望ましい。このような状況の一例には、他の組織との施設（例えば、コンピュータ、電気通信システムなど）の共有がある。

(SM.8 認証範囲)

9.3 サーベイランス活動及び9.4 再認証

9.3項及び9.4項に対する指針(G.9.3.1)

G.9.3.1 認証機関によるサーベイランスでは、年次、最低限、次の検討について含めることが望ましい。

- i) 組織のITサービスマネジメントの方針に対する目的への達成度に関するITSMSの効果
- ii) 定期的な評価、重要性の高いITサービスマネジメントに関連する法規制への遵守のレビューのためのプロセス、手順の機能
- iii) 前回の審査で検出された不適合事項に対する処置

また報告書には、少なくとも、次の項目を含めることが望ましい。

- i) 面談した組織側職員の資格、経験及び権限
- ii) ITSMSに対する信頼を与えるために組織が採用している内部の組織及び手順の適切性

明らかになった不適合を是正するために組織がとった処置。これには、該当する場合には、以前の審査で明らかになった不適合についての処置も含む。

- a) 認証機関は、組織のITサービスマネジメントのもつ脅威を含めて、サーベイランス計画に適用でき、また、その計画に十分な根拠を示すことができることが望ましい。
- b) 認証機関のサーベイランス計画は、認証機関によって決定されることが望ましい。その実施日は、認証組織と合意の上、定めることができる。
- c) 認証機関は、認証文書と報告書の適切な使用を監督しなければならない。
- d) 再認証の審査方法は、審査と同様であることが望ましい。

(SM.14 サーベイランス審査と更新審査)

9.5 特別審査

9.6 認証の一時停止、取消し、又は認証範囲の縮小

9.7 異議申し立て

9.8 苦情

9.9 申請者及び依頼者に関する記録

10 認証機関に対するマネジメントシステム要求事項

10.1 マネジメントシステムに関する選択肢

10.2 選択肢1：JIS Q 9001(ISO9001)に従ったマネジメントシステムの要求事項

10.3 選択肢 2：一般マネジメントシステムの要求事項

財団法人日本適合性認定協会

〒141-0022 東京都品川区東五反田 1 丁目 22-1
五反田 AN ビル 3F

Tel. 03-3442-1214 Fax. 03-5475-2780

著作権法により無断での複製、転載等は禁止されております。