ITSMS ユーザーズガイド
～導入のための基礎～

ITSMS：Information Technology Service Management System

IT サービスマネジメントシステム

平成 25 年 11 月 20 日

一般財団法人日本情報経済社会推進協会

はじめに

IT（情報技術）の高度化により、これを利活用した IT サービスが生活の隅々まで浸透してきました。これまで「サービス」とは、教育、美容、クリーニング、郵便、ホテル、レストランなどに見られるように、通常は人から人に提供される活動を指してきましたが、現代ではこうしたサービスの一部を IT が担う、または全面的に IT に依存したサービス提供の例も出てきています。Web を介した教育、携帯電話を使った電子メール、現金自動預払機（ATM）などでは、私たちは IT システムを通じてサービスを受けています。一方、表面的には人によってサービスが提供されている場合でも、サービスを構成する要素を見ると、例えば予約・発券・販売・履歴管理のところで IT が活躍しています。人のみが担い手であったサービスに、IT が不可欠な時代に入ってきているのです。

IT サービスの最大の特徴は、IT システムによってサービスが提供されていることです。IT システムについて、利用されている技術やハードウェア・ソフトウェアといった製品、開発手法やプロジェクト管理などには、これまでも関心が払われてきました。しかしながら、IT システム運用の局面、IT サービスマネジメントに対する日本での関心は、決して高かったとは言えなかったのではないでしょうか。今や、IT サービスの提供は国境を越え、時間の区切りを消し去ってしまっているという現実があるため、ひとたびトラブルが起こったときに、それが与える社会的な影響の範囲、深刻度、重大性は計り知れません。IT サービスマネジメントに対する無関心は組織や社会にとって致命的になりうるのです。

一般財団法人日本情報経済社会推進協会（JIPDEC）では、2007 年 4 月、JIS Q 20000 の発行と IT サービスマネジメントシステム（以下、「ITSMS」という）適合性評価制度の本格運用開始にあわせて、ITSMS 適合性評価制度技術専門部会の執筆による『ITSMS ユーザーズガイド - JIS Q 20000 （ISO/IEC 20000）対応 -』を発行いたしました。『ITSMS ユーザーズガイド - JIS Q 20000 （ISO/IEC 20000）対応 -』は、ITSMS を効果的に構築しようとするユーザ（例えば、経営者、ITSMS の構築企画者、ITSMS の推進者）向けに、認証基準である JIS Q 20000-1 の解説を中心として作られた冊子です。

これに対して、本ガイドは、『ITSMS ユーザーズガイド- JIS Q 20000（ISO/IEC 20000）対応 -』に対し、次の基礎的な内容を補充する狙いをもって編纂いたしました。

- 基本用語の解説

  次の 3 つのカテゴリから理解が必要な用語を選別し、解説しています。

  - ✓ 基礎的な用語
  - ✓ マネジメントシステムとの関係性が強い用語
  - ✓ IT との関係性が強い用語

- 適用範囲の説明

  JIS Q 20000 適用の際に最初に直面する「適用範囲」の考え方として、「規格の適用範囲」「ITSMS の適用範囲」「認証取得の適用範囲」の 3 つに区別した説明を加えています。

・ 他マネジメントシステムの視点からみた ITSMS

以下のマネジメントシステムユーザが ITSMS を導入しようとする際の留意点、各視点から JIS Q 20000 はどのように解釈されうるのか、その相違および共有可能なプロセスについて説明しています。

- ✓ 品質マネジメントシステム（JIS Q 9001）
- ✓ 情報セキュリティマネジメントシステム（JIS Q 27001）
- ✓ ITIL（IT Infrastructure Library）

また、2011 年 4 月に改訂し、ISO/IEC 20000-3（ITSMS の適用範囲設定に関する手引）及び ISO/IEC TR 20000-5（ITSMS の段階的導入に関する手引）についての解説、さらにはソフトウェア資産管理（SAM: Software Asset Management）と ITSMS との関係についての記述を、それぞれ付録 C、新 4 章、新 8 章として新たに追加いたしました。

さらに、このたび、2012 年 9 月に JIS Q 20000-1:2012 が発行されたことに伴い、また ISO/IEC 20000-3 の改訂版である ISO/IEC 20000-3:2012 発行、ISO/IEC TR 20000-4 発行等、他の関連規格の改訂・発行も考慮して、本ガイドを改訂いたしました。

本ガイドの主な読者は、ITSMS 構築に初めて取組む方、他マネジメントシステム（JIS Q 9001、JIS Q 27001、ITIL）の知識や経験を持ってはいるが ITSMS 構築は初めてという方を想定しています。本ガイドに既刊の『ITSMS ユーザーズガイド- JIS Q 20000（ISO/IEC 20000）対応 -』を併読いただくことで、広く ITSMS を理解する上での一助となり、ITSMS を構築・運用する上で参考になる事を期待しています。

本ガイドの作成にあたり、情報マネジメントシステム運営委員会の委員のみなさまをはじめ、ご協力いただいた関係各位に対し厚く御礼申し上げます。

2013 年 5 月

ITSMS 適合性評価制度技術専門部会
一般財団法人日本情報経済社会推進協会

目　次

1. ITSMS とは

1.1. ITSMS 概要

ITSMS とは、サービス提供者が、提供する IT サービスのマネジメントを効率的、効果的に運営管理するための仕組みです（図 1-1 参照）。

具体的には次のようなことを行い、顧客満足やサービス品質の向上、もしくは費用対効果の増大などの IT サービス提供に関する運営管理上の要求/期待に対応します。

【対顧客】サービス提供者は、提供のサービスレベルを顧客と合意し、合意に基づいたサービス品質を管理し、サービスレベル状況を顧客に報告します。

【対サービス提供の関連プロセス】IT サービスマネジメントは、顧客との合意のサービスレベルを含む各種要求を満たすよう、サービス提供の関連プロセスを統制します。

【対供給者】サービス提供者は、供給者とサービスレベル（顧客合意のサービスレベルとの整合が条件）を合意し、監視します。

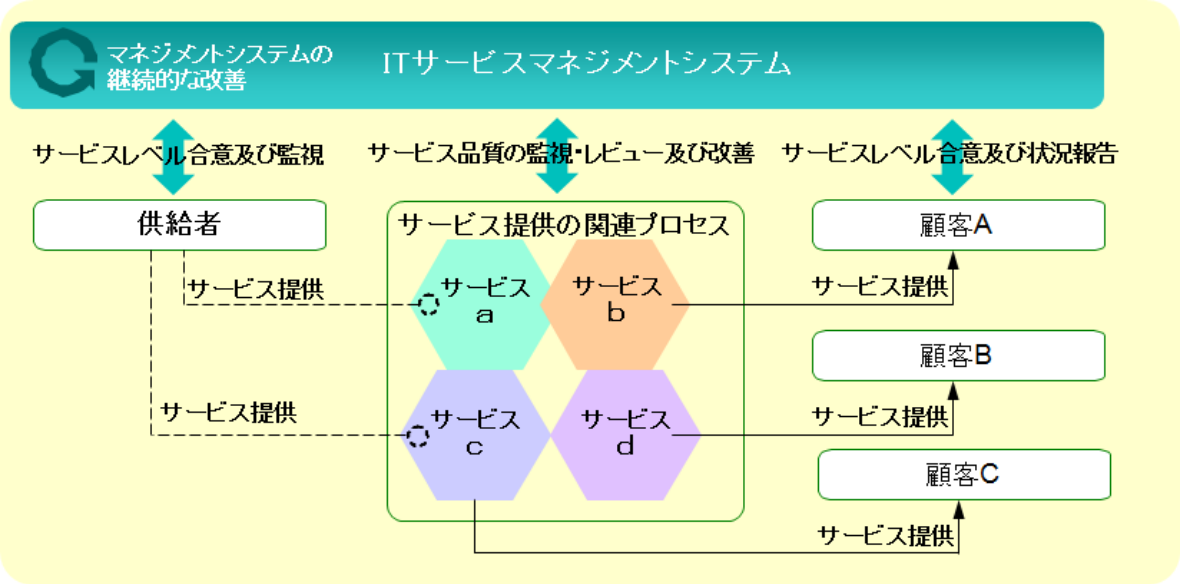


図 1-1　IT サービスマネジメントのイメージ

ITSMS の仕様及び実践のための規範が JIS Q 20000（ISO/IEC 20000）として規格化されたため、ITSMS で実現すべき内容が明確になり、その構築が容易になっています。

ITSMS 構築・運用によるメリットは、次のものが挙げられます。

■目標達成のための指標を監視・レビューし、目標達成に向けた継続的な対応が図れます。

■IT サービスマネジメント活動への経営陣の参画（マネジメントレビューの実施）により、経営の視点に沿った活動及び経営者に認知された活動が行えます。

■IT サービスマネジメントの要求事項を満たすことにより、サービス品質および顧客満足度が向上します。

IT システムの構築が一旦完了すると陳腐化/形骸化が始まります。したがって、ITSMS 構築後の留意点は、如何にマネジメントシステムの改善を行い、その改善をどのように長期的に継続するかが、問われることになります。

（１）IT サービスマネジメントの標準化/規格化

標準化については、英国中央コンピュータ電気通信局（CCTA：Central Computer and Telecommunications Agency）が、IT サービス運用管理における成功事例を基に、1989 年にベストプラクティス集である ITIL（Information Technology Infrastructure Library）として書籍をまとめ、それらを普及促進する団体 *it*SMF が各国で活動することにより、IT サービスマネジメントのデファクトスタンダード（事実上の標準）となりました。

規格化については、ITIL 第２版(ITIL V2)を基に英国規格である BS 15000 が 2000 年に制定されました。さらに、2004 年には BS 15000 の国際規格化に向けた提案がなされ、ISO/IEC JTC 1（合同専門委員会）/SC 7（ソフトウェア技術）から迅速化手続（Fast Track Procedure）で事前調査を開始後、翌年の 2005 年 12 月には、国際規格 ISO/IEC 20000-1（情報技術-サービスマネジメント-第 1 部：仕様）及び ISO/IEC 20000-2（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）として発行されました。

わが国では、これら対応の規格として JIS Q 20000-1（第 1 部　仕様）及び JIS Q 20000-2（第２部　実践のための規範）が 2007 年 4 月 20 日に制定されました。この JIS 化は、「セキュア・ジャパン２００７」施策の一環としても位置付けられています。

第 1 部は、ITSMS を構築・運用するための規格で、認証の基準となるものであり、第 2 部は、IT サービスマネジメントのガイドラインを示すものです。

ISO/IEC 20000-1 の改訂は、2005 年に開始され、2011 年 4 月に ISO/IEC 20000-1:2011 が発行されました。これに伴い、JIS Q 20000-1:2007 も改正が開始され、2012 年 9 月に改訂版である JIS Q 20000-1:2012（情報技術―サービスマネジメント―　第 1 部　サービスマネジメントシステム要求事項）が発行されました。

ISO/IEC 20000-2 についても同様に改訂が開始され、2012 年 2 月に改訂版である ISO/IEC 20000-2:2012 が発行されました。また、JIS Q 20000-2 についても改正が行われ、2013 年 11 月に JIS Q 20000-2:2013 が発行されました。

（２）JIS Q 20000-1（ISO/IEC 20000-1）概要

JIS Q 20000 ではサービスを実現するアプローチとして、PDCA として知られるプロセスアプローチを採用しています。

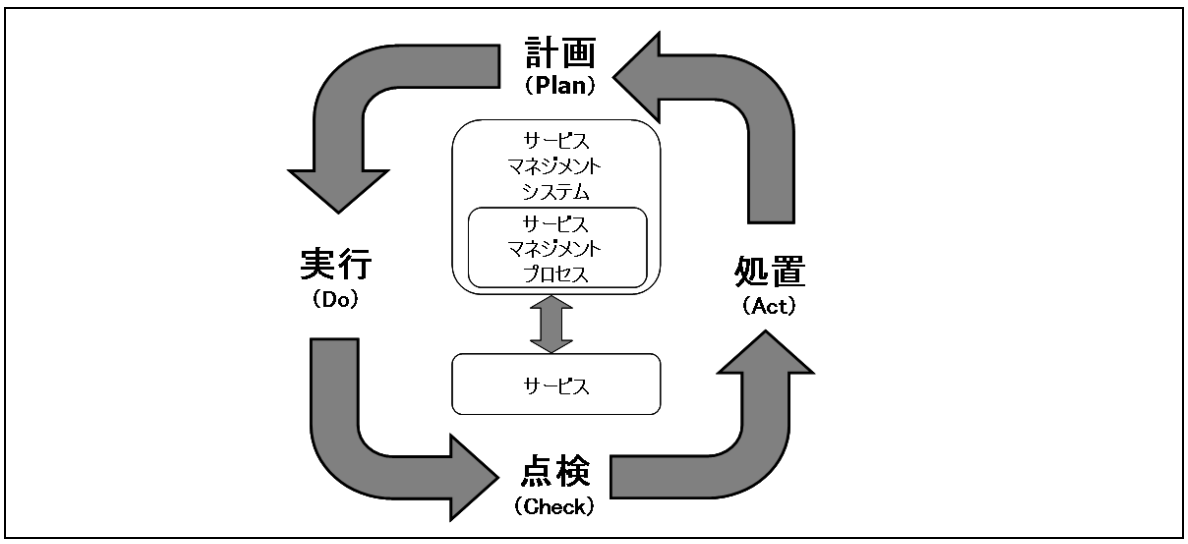


図 1 － サービスマネジメントに適用される PDCA 方法論
（JIS Q 20000-1:2012　0.2 サービスマネジメントシステム要求事項　より引用）

この図が示すように、JIS Q 20000 においては、全体的な視点で管理するサービスマネジメントシステムとサービスマネジメントのプロセス全体に、改善サイクルを回す PDCA の考え方がかかっていると考えてよいでしょう。

JIS Q 20000-1 におけるプロセスは、JIS Q 20000-1　1.1 一般の図 2 に、サービスマネジメントのプロセスを含むサービスマネジメントシステムとして、次のように示されています。

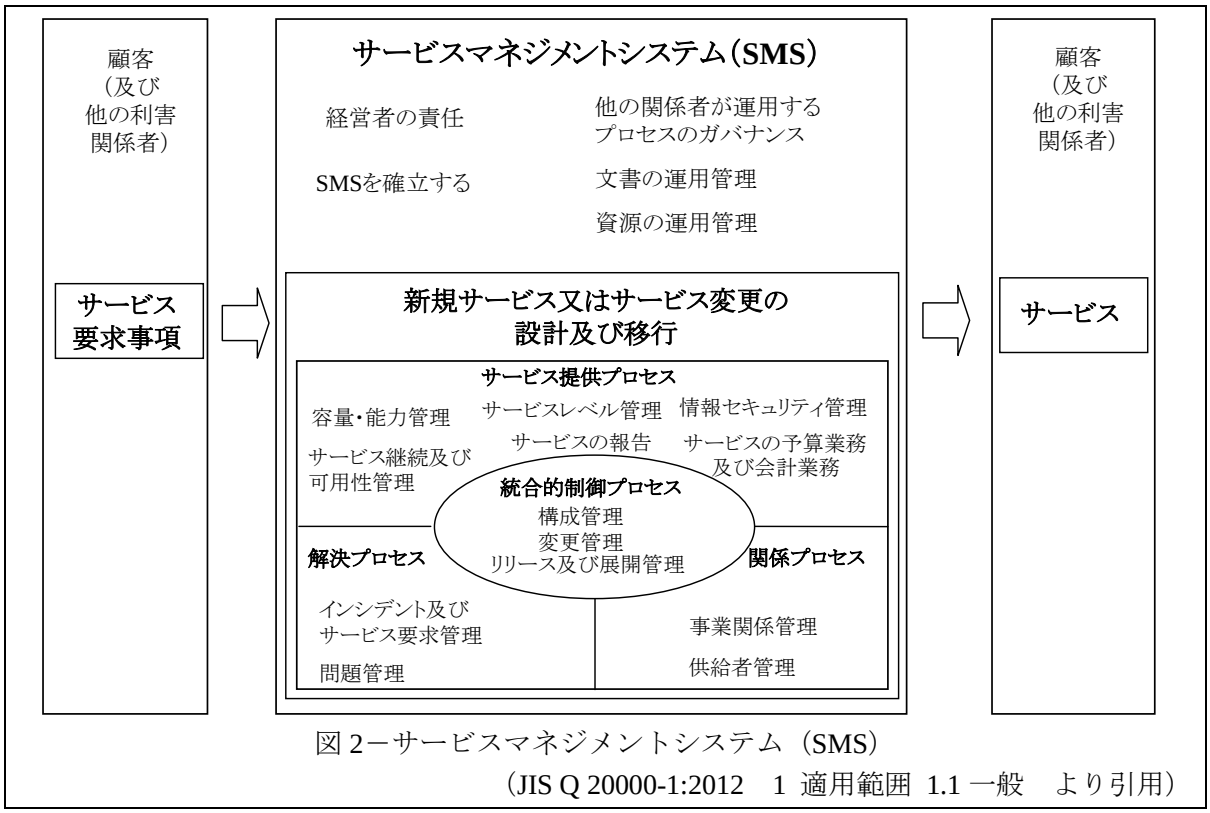


図 2－サービスマネジメントシステム（SMS）
（JIS Q 20000-1:2012　1 適用範囲 1.1 一般　より引用）

このように、規格では、IT サービスを運用管理するために必要不可欠な１３プロセスと「新規サービス又はサービス変更の設計及び移行」のプロセスを含めて、１４のプロセスに分割しています。

次に１４プロセスの一覧を示します（表 1-1 参照)。

表 1-1　IT サービスマネジメントプロセスの一覧と目的

プロセス	目的
5.新規サービス又はサービス変更の設計及び移行	新規サービス又はサービス変更が、事業ニーズ及び顧客要求事項を満たすため、あるいは、サービスの有効性を改善するために、合意した費用及びサービス品質で提供可能であり、かつ、管理可能であることを確実にするため。
6.サービス提供プロセス	
6.1　サービスレベル管理（SLM）	サービスレベルを定義、合意、記録及び管理するため。
6.2　サービスの報告	十分な情報に基づいた意思決定及び効果的な伝達のための、合意に基づく、適時の、信頼できる、正確な報告書を作成するため。
6.3　サービス継続及び可用性管理	合意したサービス継続及び可用性についての顧客に対するコミットメントを、あらゆる状況のもとで満たすことを確実にするため。
6.4　サービスの予算業務及び会計業務	サービス提供費用の予算を管理し、かつ、会計を行うため。
6.5　容量・能力管理	顧客の事業において必要な、現在及び将来の合意された需要を満たすために、サービス提供者が十分な容量・能力を常にもっていることを確実にするため。
6.6　情報セキュリティ管理	すべてのサービス活動内で、情報セキュリティを効果的に管理するため。
7.関係プロセス	
7.1　事業関係管理	顧客及びその事業推進要因に対する理解に基づき、サービス提供者と顧客との間に良好な関係を確立し、かつ、維持するため。
7.2　供給者管理	均質なサービスが確実に提供されるように、供給者を管理するため 。
8.解決プロセス	
8.1　インシデント及びサービス要求管理	顧客へ合意したサービスを可能な限り迅速に回復するため、又はサービス要求に対応するため。
8.2　問題管理	インシデントの原因を事前予防的に識別し、かつ、分析することによって、及び問題の終了まで管理することによって、顧客の事業に対する中断を最小限に抑えるため。
9.統合的制御プロセス	
9.1　構成管理	サービスライフサイクル全体で、特定されたサービス、サービスコンポーネント及び CI に関する情報の完全性を確立し、維持するため。
9.2　変更管理	すべての変更が制御された方法で評価され、承認され、レビューが確実に行われるようにするため。
9.3　リリース及び展開管理	ハードウェア、ソフトウェアおよびサービスコンポーネントの完全性が維持されるように、全てのリリースが稼働環境に効果的に展開されるようにするため。

注：表中のプロセスにおける数字は、規格の箇条を示している。

規格での各プロセスへの要求事項の管理策を実施することで、目的を達成することが ITSMS には要求されます。但し、事業上の必要性を満たすためには、さらに目的及び管理策の追加を考慮することも必要です。また、個々のプロセス以外に ITSMS 全体に関する要求事項が箇条 4「サービスマネジメントシステムの一般要求事項」に示されているので、その要求事項に対応することも必要になります。

【規格改正のポイント】

今回の JIS Q 20000-1:2012 における主な改正点としては、次が挙げられます。

- ISO 9001、ISO/IEC 27001 との整合性の向上
- 国際的な用法を反映するために、用語を変更
- 用語定義の見直しによる、用語定義の大幅な追加（削除は 2 つのみ）
- JIS Q 20000-1:2007 年版の箇条 3 と箇条 4 を合わせて 1 つの箇条にし、マネジメントシステム要求事項を 1 つの箇条に集約
- 他の関係者が運用するプロセスのガバナンスについての要求事項の明確化
- SMS の適用範囲の定義に関する要求事項の明確化
- サービスマネジメントのプロセス及びサービスを含む、SMS に適用される PDCA 方法論の明確化
- 新規サービス及びサービス変更の設計・移行に関する要求事項の導入

JIS Q 20000 の構成の変更点を示します。

JIS Q 20000-1:2007	JIS Q 20000-1:2012
序文	0.1　序文
	0.2　サービスマネジメントシステム要求事項
1　適用範囲	1　適用範囲
	2　引用規格
2　用語及び定義	3　用語及び定義
3　マネジメントシステム要求事項	4　サービスマネジメントシステムの一般要求事項
4　サービスマネジメントの計画立案及び導入	
5　新規サービス又はサービス変更の計画立案及び導入	5　新規サービス又はサービス変更の設計及び移行
6　サービス提供プロセス	6　サービス提供プロセス
7　関係プロセス	7　関係プロセス
8　解決プロセス	8　解決プロセス
9　統合的制御プロセス	9　統合的制御プロセス
10　リリースプロセス	（9　統合的制御プロセスに移動）

（3）規格の適用範囲

適用範囲は、「規格の適用範囲」、「ITSMS の適用範囲」及び「認証の適用範囲」に区分できます。ここでは、規格の箇条 1「適用範囲」について、触れておきます。

> 1.1 一般
>
> この規格は，サービスマネジメントシステム（SMS）の規格である。この規格は，SMS を計画，確立，導入，運用，監視，レビュー，維持及び改善するための，サービスの提供者に対する要求事項を規定する。
>
> 要求事項にはサービスの要求事項を満たすための，サービスの設計，移行，提供及び改善を含む。この規格は，次の組織，サービス提供者又は審査員若しくは監査員が利用してもよい。
>
> a) サービス提供者からのサービスを求め，サービスの要求事項が満たされるという保証を必要とする組織
> b) サプライチェーンに属するものを含め，全てのサービス提供者による一貫した取組みを求める組織
> c) サービスの要求事項を満たすサービスの設計，移行，提供，及び改善に関する能力を実証しようとするサービス提供者
> d) 自らのサービスマネジメントのプロセス及びサービスを，監視，測定及びレビューするサービス提供者
> e) サービスの設計，移行及び提供を，SMS の効果的な導入及び運用を通して改善するサービス提供者
> f) この規格の要求事項に対するサービス提供者の SMS の適合性評価に，基準として用いる審査員又は監査員
>
> （JIS Q 20000-1:2012　1 適用範囲 1.1 一般　より引用）

この箇条 1「適用範囲」では、当規格が IT サービス提供者に対する要求事項を規定したものであり、規格を適用する有効なケースとして、どのようなものがあるかを示しています。
c)では、顧客に対して、サービス提供の能力を説明するために有効であるということです。

すなわち、顧客に対して、“本規格を適用し、IT サービスマネジメントを構築して運用しています”と説明することで、少なくとも規格の要求事項を満たしていること、また、PDCA サイクルで改善がなされ、顧客満足を図るよう努力していることがサービス提供側に期待できるということが、顧客には、理解できるのです。

1.2. ITSMS 適合性評価制度

（1）認証登録スキーム

IT サービスマネジメントシステム（ITSMS）の国際規格 ISO/IEC 20000 に対する国内規格 JIS Q 20000 の制定に伴い、JIS Q 20000-1（ISO/IEC 20000-1）を認証基準とした IT サービスの運用管理に対する第三者認証制度として、IT サービスマネジメントシステム適合性評価制度（以下、ITSMS 制度という）を 2007 年 4 月から開始しました。

ITSMS は、企業における IT サービスの運営管理に特化したマネジメントシステムであり、これによって IT サービスの品質向上及び企業価値の向上につながるだけでなく、対外的にも IT サービスの信頼性をアピールすることができます。

ITSMS 制度は､組織における IT サービス運用管理の品質を継続的に向上させることによって、わが国の IT サービス全体の信頼性の向上に貢献することを目的とし､国際的な整合性を確保しながら、信頼性のある第三者認証制度として確立することを目指しています。

この国際的に整合のとれた活動をするためには、認定機関は、ISO/IEC 17011 に適合し、また、認証機関（審査登録機関）は、ISO/IEC 17021 及び ISO/IEC 27006 をベースに策定した認定基準に適合させる必要があります（表 1-2 参照)。

表 1-2　ITSMS 認証機関の認定にかかわる文書

･ITSMS 認証機関の認定に関連する文書　　**2013 年 5 月現在**

文書名	文書番号	発行・改訂日	内容
ITSMS 認証機関認定基準及び指針	JIP-ITAC100-2.3	2012.3.22	ITSMS 認証機関の認定審査及び登録を行う際の認定基準、及びこの基準の要求事項に適用する指針。
IMS 認証機関認定の手順	JIP-IMAC110-2.4	2012.3.22	認証機関として認定を受けるための手順と、認定を申請する機関及び認定された機関の権利と義務 について規定したもの。
IMS 認証機関認定の手引き	JIP-IMAC111-2.3b	2011.12.26	認証機関が認定を申請して登録されるまで、及び登録維持の標準的な流れと条件を示したもの。
マネジメントシステム認証に関する基本的な考え方 ― 認証範囲及びその表記―	JIP-IMAC121-1.1a	2011.12.26	認証審査を実施するにあたっての認証範囲及びその表記に関する基本的な考え方を示したもの。
IMS 認定シンボル使用規定	JIP-IMAC510-2.3a	2011.12.26	認定シンボルの表示条件及び適用条件を定めたもの。

･ITSMS 要員認証機関に関連する文書

文書名	文書番号	発行・改訂日	内容
ITSMS 審査員の資格基準に関する指針	JIP-ITAC401-1.0	2008.5.1	各審査員（審査員補、審査員、主任審査員）についての資格要件を規定したもの。
ITSMS 審査員研修コースに対する要求事項	JIP-ITAC223-1.0	2007.10.25	審査員研修コースに対する要求事項を纏めたもの。

認定基準には、認証機関が認証サービスを遂行する能力があり、信頼できると承認されるために適合させるべき要求事項が規定されています。すなわち、ITSMS 制度とは、組織が構築・運用した ITSMS が認証基準 JIS Q 20000-1（ISO/IEC 20000-1）に適合しているか否かについて、認定された認証機関が、認証審査を実施し、その審査結果に基づいて組織を認証登録するスキームです。

現在の認証機関及び認証取得組織の詳細は､URL:http://www.isms.jipdec.or.jp/itsms.html の｢ITSMS 認証機関一覧」及び「ITSMS 認証取得組織検索」を参照願います。

（2）審査員資格スキーム

ITSMS 審査員登録及び審査員研修機関の承認（ITSMS 審査員研修コースの承認も含む）は、ISO/IEC 17024 に基づき認定された「要員認証機関」において実施することになります（図 1-2 参照)。ITSMS 審査員資格としては、ITSMS 審査員の資格規準に関する指針に基づいた審査員資格

要件、あるいは ITSMS 研修コース基準が公表されることになります。特に、JIS Q 20000-1（ISO/IEC 20000-1）の規格の解釈に基づき、認証審査を計画、実施、報告及びフォローアップする力量を確保するためには、実際の審査経験を積むことが必要です。現在、ITSMS 審査員資格として、次の指針を公表しています。

・情報技術分野で少なくとも４年以上の実務経験があること、その内 IT サービス関連分野で少なくとも２年以上の実務経験があること。（実務経験）
・ITSMS 審査員研修コースを成功裏に修了し、合格すること。（研修実績）
・ITIL 関連の用語及び知識を有していること。（実務経験）
・審査員としての審査実績は、最低４回延べ２０日間にわたる完全な審査に参加していること。審査チームリーダーとしては、最低３回延べ１５日間を務めていること。（審査実績）

その他に、教育レベル、個人的資質、CPD（Continuing Professional Development）などが要求されています。

なお、ITSMS 審査員研修コース基準、審査員登録要件については、IRCA（国際審査員登録機構）が公表していますので参照願います。

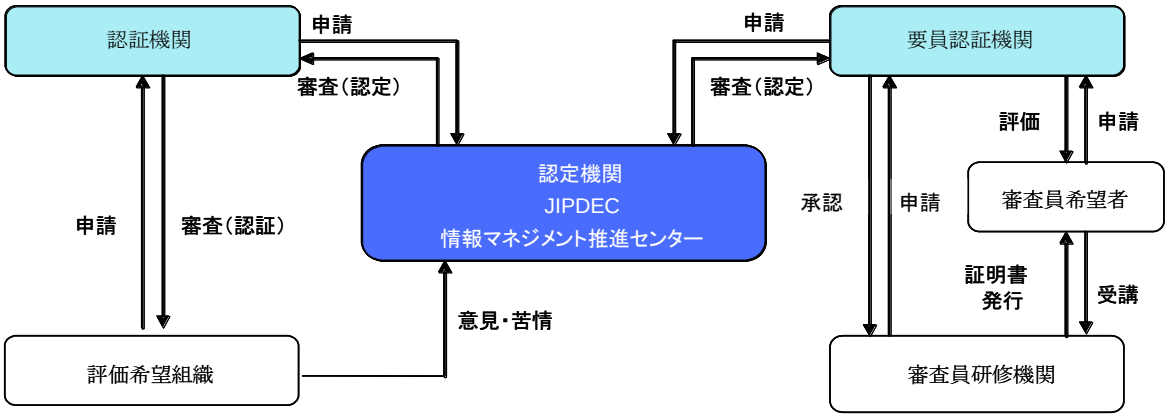


図 1-2　ITSMS 適合性評価制度のスキーム

1.2.1. 審査登録制度の概要

（１）審査登録制度

審査登録制度（「認証制度」ともいう）とは、独立した外部の機関によって実施される第三者による監査（審査）のことをいいます。これは、組織が外部の利害関係者に対して何らかの保証をしたい時に、組織と利害関係にない第三者機関（この機関を総称して「認証機関」という）が認証審査を実施して、その適合性を保証することです。すなわち、ITSMS 制度では、第三者である認証機関が、受審する組織の ITSMS が認証基準（JIS Q 20000-1（ISO/IEC 20000-1））の要求事項に適合しているか否かを審査し、審査結果によって認証を登録・公表（ここでは、「認証登録」という）することです。

認証登録を受けた組織は、自らの ITSMS に対してより一層信頼を置くことができ、認証登録証によって組織における IT サービスマネジメント能力を保有していることを公式に表明でき、情報を共有する取引先からも信頼を得ることができます。

一方、認定機関は、認証機関が行う認証審査に不公平があったり、不正確であったりしては不都合が生じるので、これらの認証機関を評価し、認証審査を遂行する能力があるかを公式に認める役割を持っています。

（2）認証機関の選択

ITSMS 認証取得を希望する組織は、自社の ITSMS を構築・運用した後、認証機関へ申請しますが、その認証審査が信頼できるものであることを保証するために、認定を受けた認証機関を選択する必要があります。認定された認証機関は、受審組織の業種による制限はないので、どの業種も審査することができます。審査において業種特有の専門知識が必要な場合には、技術専門家などを加えて審査チームとしての力量を確保する必要があります。また、認証機関は、組織との利害抵触の可能性のある場合等では申請を受け付けられない、もしくは、審査が実施されないこともあるので事前に十分な確認が必要です。

（3）認証機関への申請

認証機関の選択後、認証登録に関する条件について事前に確認し、組織内において受審の意思決定をしてから申請します。申請に必要な書類や様式等については、それぞれの認証機関から入手することができます。特に、認証審査に関わる審査工数は ITSMS の適用範囲や受審組織の規模、プロセスの複雑さなどによっても異なるので、認証機関から事前に見積りを取るなどして確認しておく必要があります。

（4）認証登録

申請が受理され、認証機関との認証契約等の締結後、審査チームの編成や審査の日程等が調整され、審査が開始されます。認証機関は、組織の IT サービスマネジメントの適用範囲が組織の活動を適切に反映しており、導入及び改善の計画が IT サービスマネジメントプロセスの規定する活動の境界まで含めていることを確認する必要があります。また、審査の開始に先立って、申請者に内部レビュープロセス手順があり、運用の可能性を実証できることが前提となります。次に、審査は第１段階審査（ステージ１）と第２段階審査（ステージ２）の２段階で行われます。

第１段階審査の目的は、組織の IT サービスマネジメントの方針及び目的に照らして当該 ITSMS を理解し、また当該審査に対する組織の準備状況を確認することによって、第２段階審査に計画の焦点を定めることにあります。

第２段階審査の目的は、組織が自ら定めた方針、目的、及び手順を順守していること、並びに当該組織の IT サービスマネジメントの方針及び目的を実現しつつあることを確認することにあります。第２段階審査は、常に組織のサイトで実施します。また、申請から認証登録までの期間は、実際の審査に係る工数のほか審査の不適合（認証基準に適合していないか、システムが運用されていないこと）の状況によっても異なってきます。規模があまり大きくなく、特に問題がない場合には３～４ヶ月程度が一般的です。認証登録の情報は、認証機関から認定機関に報告されますが、報告時期によっては１ヶ月程度ずれる場合があります（図 1-3 参照）。

認証登録された組織は、自らの IT サービスマネジメントプロセスに対して一層の信頼を置くことができます。また認証登録証によって、組織は IT サービスマネジメントの詳細を機密情報とし

て保持する一方で、IT サービスマネジメントプロセスの能力を保有していることを公表することができます。認証登録されたサービス提供者は、効果的な IT サービスマネジメントを運用することによって、高いレベルの顧客サービス及び顧客満足を得ることができます。

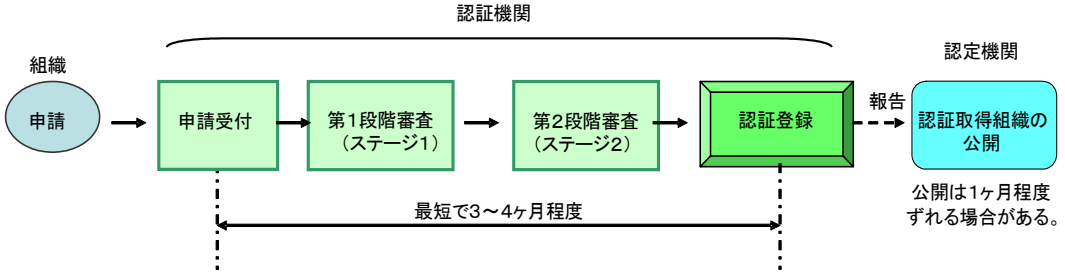


図 1-3　認証登録の流れ

（5）認証登録の適用範囲

組織の IT サービスマネジメントの認証登録の適用範囲は、組織形態、IT サービスの内容や活動など顧客とサービス提供者の関係によっても境界が異なってきます。通常は、サービス提供者が認証を求める対象組織です。そのため、認証を受けようとするサービス提供者は、IT サービスをどのような形態で顧客に提供しているかを認識し、認証基準に規定された全てのプロセスについてマネジメント・コントロールしていることを実証する必要があります。

IT サービスの提供に関与するサービス提供者は、組織全体ではなく組織の内部あるいは外部組織にアウトソーシングされている場合もあります。あるいは IT サービス提供に必要なプロセスのうち、いくつかを外部の組織にアウトソーシングしていることも考えられます。

そのため、適用範囲の記述には次のことを明確に含まなければなりません。

・審査対象となるサービス
・地理的又は場所の境界
・組織又は部署の境界
・アウトソースされた全てのプロセスの要素

審査の範囲内におけるプロセスが、完全に一つの組織単位によって実行されるかは重要ではありません。複数の組織が関係する場合には、認証登録の適用範囲を明確にし、サービス提供者の認証に直接関係のあるプロセスだけが審査の対象となります。審査に複数の供給者（サプライヤ）と顧客が関係している場合、サービスの範囲、審査されるマネジメントプロセスによって支えられたサービスだけを定義する必要があります。

この認証登録の適用範囲の設定の考え方については、本ガイドの 3 章スコーピングを参照願います。

（６）審査の種類

(a)初回審査

認証取得の希望を初回に申請した場合で、組織が構築及び運用している ITSMS が JIS Q 20000-1（ISO/IEC 20000-1）の要求事項に適合しているか否かを審査し、審査結果が適合している場合には、認証登録されます。

(b)サーベイランス審査

認証登録は、初回審査の登録から３年間有効となります。そのため認証登録後、通常１年を超えないサイクルで組織が引き続き ITSMS を有効に維持しているかどうかのサーベイランスが実施されます。サーベイランスでは、前回指摘事項等の是正・改善状況、基準への適合状況、維持状況等により IT サービスマネジメントの有効性を確認します。

(c)再認証審査

初回審査から３年目には、組織が引き続き認証登録を維持する場合に更新審査が実施されます。更新審査では、初回審査とほぼ同様の審査が行われますが、ITSMS に大きな変更がない場合には、審査工数が削減される可能性があります。

(d)特別審査

既に認証登録している組織が、認証登録の範囲を大幅に変更する場合などに実施する審査です。認証登録の範囲を拡大する場合には、通常、サーベイランス審査、更新審査において実施されることが多くあります。

1.3. 本書の活用方法

ITSMS 構築に初めて取組む方（他マネジメントシステム構築済みでも ITSMS 構築は初めての方を含む）向けに、基礎的/基本的なことを理解できることを目的としています。

構成は表 1-3 の通りとなっていますので、読者は、この表を参考に読み進めてください。

表 1-3　各章の対象とする読者

章	ﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑ 初めての方	ISMS ユーザ	QMS ユーザ	ITIL ユーザ
1.ITSMS とは	○	○	○	○
2.用語の解説	○	○	○	○
3.スコーピング	○	○	○	○
4.ITSMS の段階的導入 ～ISO/IEC TR 20000-5 の要点～	○	○	○	○
5.ISMS ユーザのための ITSMS 入門		○		
6.QMS ユーザのための ITSMS 入門			○	
7.ITIL ユーザのための ITSMS 入門				○
8. ソフトウェア資産管理と IT サービスマネジメント				○

また、詳しくは『ITSMS ユーザーズガイド - JIS Q 20000（ISO/IEC 20000）対応 -』を併用してください。

2. 用語の解説

この章は、JIS Q 20000 で使用される用語に関する知識を深め、JIS Q 20000 の理解を助けることを目的としています。具体的には、以下の考え方に基づいて収録する用語を選定し、全体を掴んでもらうことを目指しています。

○ITSMS または JIS Q 20000 に初めて触れる方を対象として、基礎的な用語を解説する。
（IT との関係性が強い用語やマネジメントシステム規格との関係性が強い用語についても、ITSMS または JIS Q 20000 におけるイメージを確認するため、再度解説しています）

○用語が指し示すイメージを伝えることを第一義とする。
（用語に関する厳密な定義は、本章では解説していません）

収録した 22 の用語の大まかなカテゴリは以下の通りです。

○基礎的な用語
- 顧客、ユーザ、事業、サービス提供者、供給者（2.6.）
- リスク（2.11.）
- インシデント（2.12.）
- 情報セキュリティインシデント（2.20.）
- 問題（2.13.）

○マネジメントシステムとの関係性が強い用語
- マネジメントシステム（2.1.）
- サービスマネジメントシステム（2.17.）
- プロセス、プロセスアプローチ（2.3.）
- 適用範囲（2.4.）
- 文書、記録（2.5.）
- 力量（2.7.）
- 要求事項（2.8.）
- 是正処置（2.18.）
- 予防処置（2.19.）

○IT との関係性が強い用語
- サービス（2.22.）
- IT サービスと IT サービスマネジメント（2.2.）
- 内部グループ（2.21.）
- サービスコンポーネント（2.16.）
- サービス改善計画（2.9.）
- サービスレベル、サービスレベル目標値（2.10.）
- 変更とリリース（2.14.）
- ベースライン、構成ベースライン（2.15.）

なお、「マネジメントシステム規格」という表現で対象としているのは、主に以下の範囲を想定しています。

JIS Q 20000　　JIS Q 27001　　JIS Q 9001

2.1. マネジメントシステム

マネジメントシステムとは、ある方針や目標を定めて達成するための仕組みのことです。規格では、マネジメントシステムを IT サービスの運営管理に適用しており、その方法論として「PDCA モデル」を提示しています。なお、「IT サービスマネジメント」を実現するためのマネジメントシステムを「IT サービスマネジメントシステム」と捉えることができます。

規格では、IT サービスマネジメントを実現するための PDCA モデルを以下のように説明しています。

> 計画（Plan）：SMS を確立し，文書化し，合意する。SMS には，サービスの要求事項を満たすための方針，目的，計画及びプロセスが含まれる。
>
> 実行（Do）：サービスの設計，移行，提供及び改善のために SMS を導入し，運用する。
>
> 点検（Check）：方針，目的，計画及びサービスの要求事項について，SMS 及びサービスを監視，測定及びレビューし，それらの結果を報告する。
>
> 処置（Act）：SMS 及びサービスのパフォーマンスを継続的に改善するための処置を実施する。
>
> （JIS Q 20000-1:2012　0.2 サービスマネジメントシステム要求事項　より引用）

非常に簡潔に表せば、「目的と、目的達成のためのプロセスを定め」（Plan）、「定めたプロセスを実行し」（Do）、「目的への達成状況を測り」（Check）、「達成状況に応じて改善をはかる」（Act）ということが PDCA です。目的がなかったり、目的が極端にあいまいであったり、目的への達成状況が測れないような IT サービスマネジメントシステムはマネジメントシステムとしての本来の機能を果たさないでしょう。

IT サービスマネジメントシステムは、この PDCA サイクルを継続的に運用することにより、サービス提供者として提供する IT サービスに関する品質を維持及び向上させていくものになります（イメージは図 2-1 を参照してください）。

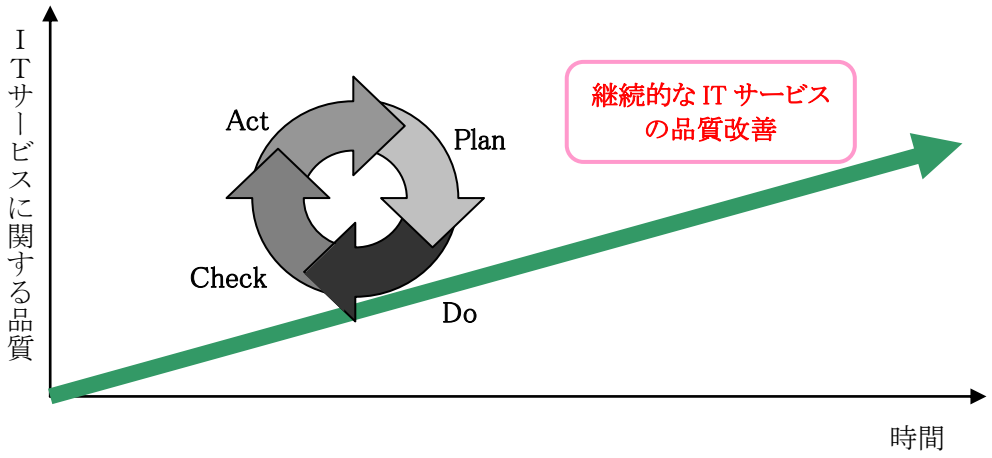


図 2-1 継続的改善のイメージ

2.2. IT サービスと IT サービスマネジメント

規格には「IT サービス」や「IT サービスマネジメント」という用語は登場しません。しかし、以下のように「サービス」については記載があります。「サービス」は「IT サービス」のことですので、「サービス」を「IT サービス」に、「サービスマネジメント」を「IT サービスマネジメント」に読み替えても差し支えないと考えられます。

> この規格は，SMS を計画，確立，導入，運用，監視，レビュー，維持及び改善するための，サービスの提供者に対する要求事項を規定する。
>
> （JIS Q 20000-1:2012　1 適用範囲 1.1 一般　より引用）

「IT サービス」は色々な意味で用いられる用語ですが、規格では明確に定義していません。本ガイドでは、規格の「IT サービス」に対するイメージを図 2-2 に示すように捉えます。

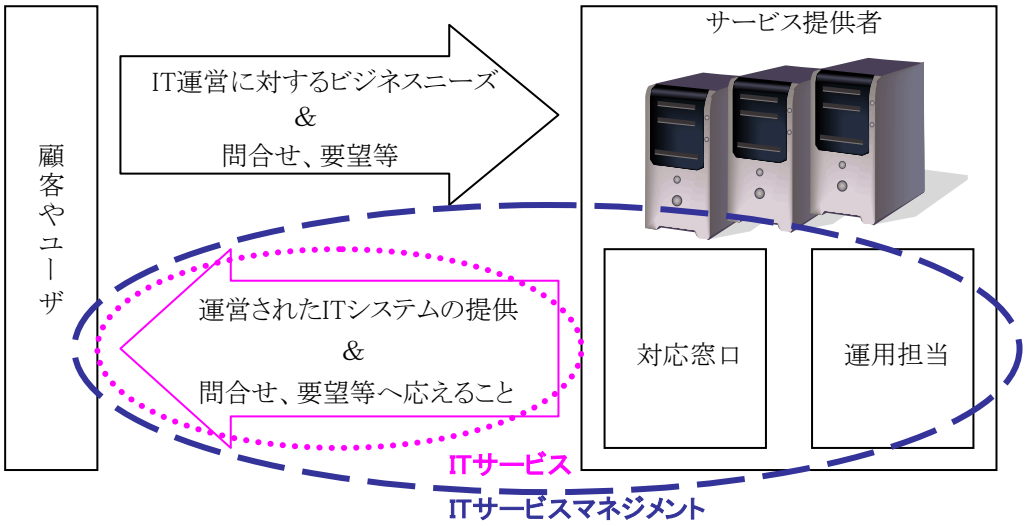


図 2-2「IT サービス」のイメージ

「IT サービス」は、顧客やユーザに対して、運営管理された IT システムを提供すること及び問合せや要望等へ回答することと捉えるとイメージしやすいと思われます。このように考えると、IT サービス提供の中心には IT システムがあり、人がメインとなって提供するサービスは IT サービスとは捉えないと考えることができます。例えば、IT システムそのものに対して人が提供するサービス（IT システムの開発・構築等）は、この規格において IT サービスと呼ぶことは相応しくないでしょう。

「IT サービス」を上記のように捉えると、IT サービスマネジメントは、IT サービスの提供品質を維持・向上させるためにマネジメントすることとなります。したがって、日常的な IT システムの運用管理（オペレーション）そのものだけではなく、IT システムの運用管理業務をマネジメントすることも含めた概念として捉えます。

2.3. プロセス、プロセスアプローチ

JIS Q 20000-1 は用語及び定義の中でプロセスを定義しています。プロセスを次のように述べています。

> 3.21 プロセス（process）
> インプットをアウトプットに変換する、相互に関連する又は相互に作用する一連の活動。
> [JIS Q 9000:2006]
>
> （JIS Q 20000-1:2012　3 用語及び定義　より引用）

図 2-3 はプロセスの一般的なモデルを示します。プロセスはインプットを受け取り、プロセスにおける活動（Activity）あるいはサブプロセス内における活動を通じて、何らかのアウトプットをします。このプロセスのアウトプットは事業の達成目標から導き出された基準に沿うものでなければなりません。JIS Q 9001 においては、プロセスの活動の結果として製品（product）が得られるとしています。

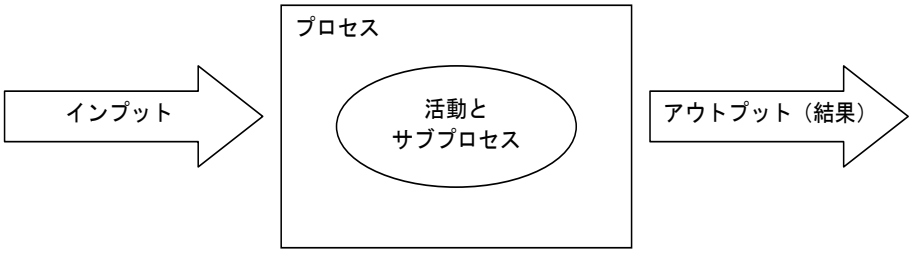


図 2-3　プロセスの一般的なモデル

JIS Q 27001 では ISMS の確立、導入、運用、監視、レビュー、維持及び改善のために、プロセスアプローチを採用しています。プロセスアプローチとは、プロセスを明確にし、かつ、相互作用させることとあわせて、それらのプロセスをシステムとして組織内に適用し、かつ、運営管理することです。では、プロセスが正常に機能し、そのアウトプットが目標に合致し、プロセスが効果的、効率的に実行されていることをどうやって知れば良いのでしょう。JIS Q 20000-1 では PDCA サイクルの C（Check）において、次のように述べています。

> サービス提供者は, SMS 及びサービスの監視及び測定のために適切な方法を用いなければならない。
>
> （JIS Q 20000-1:2012　4.5.4 SMS の監視及びレビュー　より引用）

具体的な測定方法としては、ITIL 等で利用されている CSF（Critical Success Factor：重要成功要因）と KPI（Key Performance Indicator：重要業績評価指標）が役立つでしょう。JIS Q 20000-1 では箇条 5 以降に１４のプロセスが定義されています。

2.4. 適用範囲

ITSMS（または JIS Q 20000）に関連して「適用範囲」という用語が使われる場合には、「ITSMS の適用範囲」を意味する場合が多いでしょう。但し、「適用範囲」と言った場合には、図 2-4 に示すような意味で用いられる場合もあります。

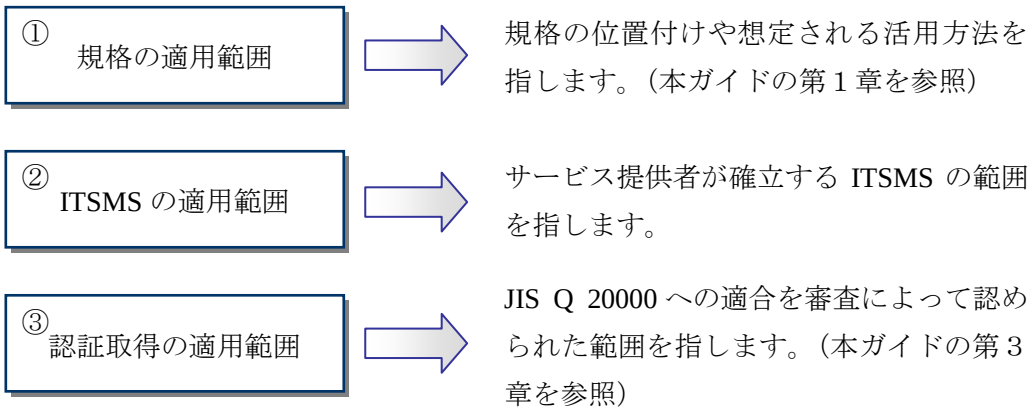


図 2-4 「適用範囲」の用いられ方

図 2-4 に示す①、②及び③は、意味が全く異なります。①は規格自体の位置付けや対象、想定される活用方法を指すのに対し、②や③は規格を活用した ITSMS の範囲や認証の範囲を指します。

②と③は、認証取得を目指すサービス提供者の場合は同一になるでしょう。ITSMS は、2.2 節に示したように IT サービスに関する品質を維持・向上させるための仕組みです。したがって、ITSMS の適用範囲の決定は、管理対象とする IT サービスを決めることから始めることになります。そこから決定した ITSMS の適用範囲において ITSMS 認証を取得すると捉えます。認証取得を目指す場合の適用範囲には要件がありますので、適用範囲の設定に関する考え方は本ガイドの第 3 章を参照してください。

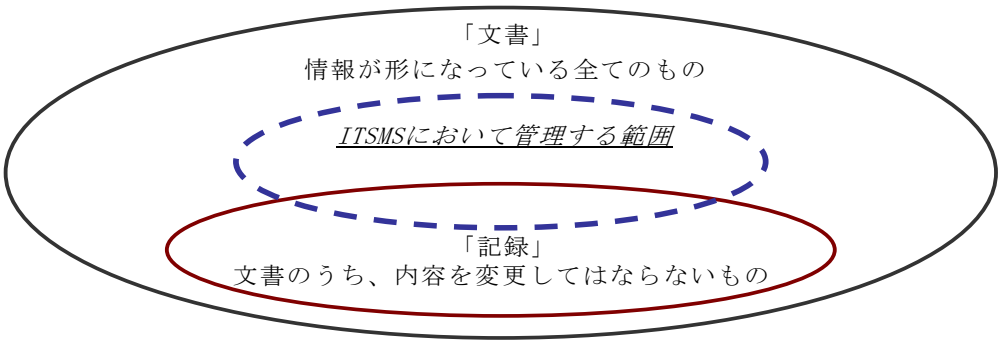
なお、③の認証取得の適用範囲は、サービス提供者の顧客やその他の利害関係者が「どの IT サービスに対して認証を取得しているのか」を把握するためにも参照されます。認証機関が認証したサービス提供者の ITSMS の適用範囲は、JIPDEC のホームページ上で参照できます。

2.5. 文書、記録

文書は、何かしらの情報が記述されたもの全てを含みます。紙の書類はもちろん、ハードディスク上のデータ、テープや CD 等に保存されているデータも文書です。一方、記録は、含まれる情報が証跡として取扱われるものです。なお、規格では文書も記録も様式や媒体はどのようなものでもよい、とされています。

規格には、文書と記録の例として、それぞれ以下のようなものが挙げられています。

> 文書の例：方針文書，計画書，プロセス記述書，手順書，サービスレベル合意書，契約書又は記録。
> 記録の例：監査報告書，インシデント報告書，教育・訓練の記録又は会議の議事録。
> （JIS Q 20000-1:2012　3 用語及び定義 3.8 及び 3.22　より引用）



（JIS Q 9000:2006　3.7 文書に関する用語をもとに作成）

図 2-5　「文書」と「記録」の範囲（イメージ）

文書と記録の違いを直感的に理解するためには、作成後に変更してもよいか・変更してはならないか、を考えるとわかりやすいでしょう。その関係を単純に表したのが図 2-5 です。図 2-5 の中で「ITSMS において管理する範囲」という点線で囲った範囲があります。これは、サービス提供者内には様々な文書や記録がある中で、ITSMS で管理すべき文書や記録の範囲を定める必要があることを意図しています。

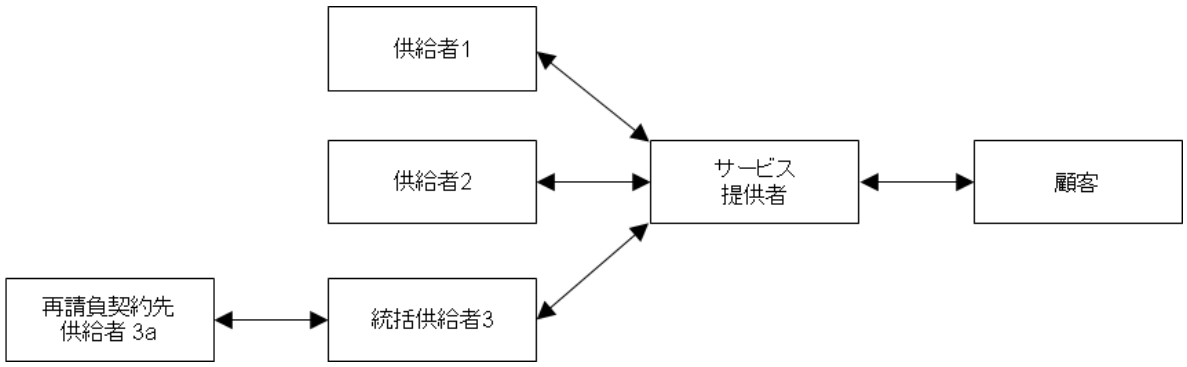
規格では「4.3 文書の運用管理」の中で、ITSMS で管理すべき文書及び記録の範囲とそれらの管理手順を確立することを要求しています。規格にある「文書化した・・・」は、求められている事項がサービス提供者内の全要員の共通認識となっているだけでは足りず、「文書」として形式化・見える化されていることを求めています。例えば、運用支援ツールを用いてインシデントを監視・検知し、対応していたとしても、その手続がどのようになっているか見えるようになっていなければなりません。

2.6. 顧客、ユーザ、事業、サービス提供者、供給者

JIS Q 20000-1 における顧客、サービス提供者、供給者の関係は図 2-6 で示される関係となっています。

事業（business）とは、複数の事業部門から成る企業体または組織の全体を示しています。また、本規格における事業（business）という言葉は、箇条によっては顧客を意味すると読み取れる場合もあります。

ITIL では顧客とユーザは別の意味を持ちますが、規格の中では厳密に定義されていません。顧客とは、サービス提供者により IT サービスの提供を受ける組織または個人を意味します。顧客は IT サービスの提供を受けるためにサービス提供者に IT サービスの提供にかかるコストを支払います。顧客が必ずしも IT サービスを利用するわけではありません。IT サービスを利用する組織または個人がユーザです。サービス提供者が提供する IT サービスの形態により、両者が同一である場合も考えられますが、IT サービスの適用範囲を考える場合には、顧客は誰か？ユーザは誰か？を明確にすることは重要です。



（JIS Q 20000-1:2012　7.2 供給者管理　より引用）

図 2-6 サービス提供者及び供給者間の関係の例

サービス提供者は事業内の顧客に対して IT サービスを提供します。事業内の顧客は、サービス提供者の組織内部の場合もあれば外部組織の場合も考えられるでしょう。今日の IT 環境においては、IT サービスを提供するために必要となる製品またはサービスが単独のサービス提供者によって供給されることは現実的ではないかもしれません。サービス提供者が、単独で IT サービスのすべての構成要素を提供できない場合は、供給者を利用します。供給者は IT サービス提供者に対して製品またはサービスを提供します。サービス提供者は、顧客に提供している IT サービスに供給者からの製品またはサービスを組み込みます。供給者が更に別な供給者からサービスの提供を受けて、サービス提供者へ提供している場合は、統括供給者と再請負先契約者という関係が生じます。供給者の代表的な例としては、ハードウェアやソフトウェアのベンダーなどです。

2.7. 力量

規格で用いられる「力量」は、コンピテンシーや遂行能力と捉えるとわかりやすいと思われます。言い換えれば、何らかの役割や責任に対するコンピテンシーや遂行能力が、規格で用いられる「力量」であるということです。

規格では、以下に引用する箇所に「力量」という用語が用いられています。

> サービスの要求事項への適合に影響がある仕事に従事するサービス提供者の要員は，適切な教育，訓練，技能及び経験を判断の根拠として，力量がなければならない。サービス提供者は次の事項を実施しなければならない。
>
> a) 要員に必要な力量を決定する。
>
> b) 該当する場合，必要な力量がもてるように教育・訓練するか，又は他の処置をとる。
>
> （JIS Q 20000-1:2012　4.4 資源の運用管理　より引用）

「力量」をコンピテンシーや遂行能力に置き換えて捉えると、上記の要求事項では「力量」に関して、「サービスマネジメント（ITSMS）の運営における役割及び責任について、その役割及び責任を果たすために必要な“遂行能力”とともに定義をすること」を要求していると捉えられます（図 2-7）。

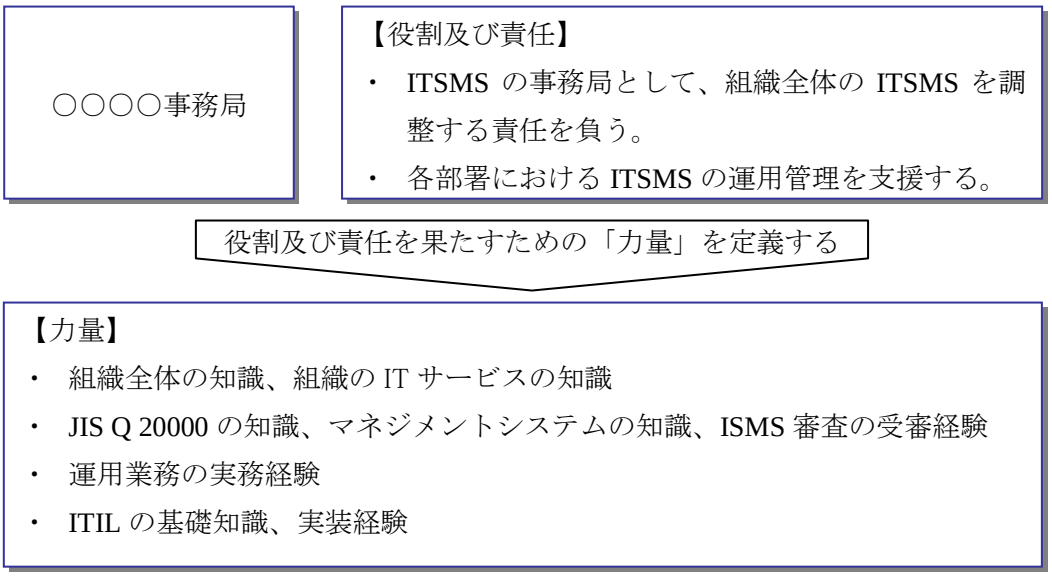


図 2-7 「力量」のイメージ

なお、JIS Q 20000-1：2012 の基となっている ISO/IEC 20000-1：2011 では、「力量」は“Competence”と記述されています。また、JIS Q 9000：2006 では、「力量」を「知識及び技能を適用するための実証された能力」と定義しています。

2.8. 要求事項

要求事項は、一般的には、システム工学とソフトウェア工学で使われる用語ですが、システム開発においては、提供する製品やサービスの在るべき姿を指します。

一方、規格における要求事項は、組織が規格への適合を証明するために達成しなければならない事項を指します。言い換えると、規格への適合を証明するためには、規格要求事項を満足することが必要となります。

要求事項の用語としての定義は、JIS Q 9000:2006 において次のように述べられています。

> 要求事項（requirement）
> 明示されている，通常，暗黙のうちに了解されている若しくは義務として要求されている，ニーズ又は期待。
>
> 注記 1 “通常，暗黙のうちに了解されている”とは，対象となる期待が暗黙のうちに了解されていることが，組織，その顧客及びその他の利害関係者にとって慣習又は慣行であることを意味する。
> 注記 2 特定の種類の要求事項であることを示すために，修飾語を用いることがある。
> 例 製品要求事項，品質マネジメント要求事項，顧客要求事項
> 注記 3 規定要求事項とは，例えば文書で，明示されている要求事項である。
> 注記 4 要求事項は，異なる利害関係者から出されることがある。
>
> （JIS Q 9000:2006 3 用語及び定義 より引用）

JIS Q 20000 は JIS Q 20000-1 と JIS Q 20000-2 の 2 部で構成されます。JIS Q 20000-1 は情報技術サービスを提供するサービス提供者に対する要求事項について規定しています。

要求事項として規定されている文章は、JIS Q 20000-1 の中ではすべて、“～しなければならない。”（英文では shall～）と表現されています。これに対して JIS Q 20000-2 では、要求事項を実現するための実施基準、いわゆるガイドラインが述べられています。表現も、“～することが望ましい”（英文では should～）という表現が取られています。

JIS Q 20000 のような 2 部構成の形をとるマネジメント規格としては、他には、JIS Q 27001・JIS Q 27002（情報セキュリティマネジメント）などがあります。

2.9. サービス改善計画

JIS Q 20000-1:2007 では箇条 5 以降に１４のプロセスの要求事項が規定されており、その多くのプロセスには“サービス改善計画へ入力しなければならない”という要求事項が見られました（下表参照）。サービス改善計画とは、各プロセス群の PDCA サイクルにおいて識別された改善項目を実行に移すための計画のことを指します。

JIS Q 20000 の箇条 5 以降で規定されるプロセスは、単独に活動することは少なく、互いに密接に関連しあい、連携しながら、それぞれの機能を果たしますが、プロセスという観点からすれば、PDCA サイクルを回すことによって、プロセス改善をしてゆく必要があります。サービス改善の要求は JIS Q 20000 の全てのプロセスから発生する可能性があります。下表のプロセス群において、要求事項としてサービス改善計画への入力を要求している理由は、各々のプロセス改善に必要なだけでなく、提供している IT サービス改善にとっても特に重要となるプロセスであるからです。

JIS Q 20000-1:2012 では、“サービス改善計画へ入力しなければならない”という表現は無くなりました。替わりに、“改善の機会（Opportunity for improvement）”という表現が使われています。

比較のための例示として、6.1 サービスレベル管理の 2007 年版と 2012 年版で該当する要求事項を記載しておきます。

表 2-1　サービス改善計画

JIS Q 20000-1:2007	要求事項
6.1 サービスレベル管理	サービスレベルを目標に照らして監視し，かつ，報告しなければならない。不適合の理由を報告し，かつ，レビューしなければならない。このプロセスで特定した改善策を記録しなければならない。この改善策を，サービス改善計画に入力しなければならない。（JIS Q 20000-1:2007） サービス目標に照らして傾向及びパフォーマンスを監視しなければならない。結果は，不適合の原因及び改善の機会を特定するために，記録し，レビューしなければならない。 （JIS Q 20000-1:2012）
6.6 情報セキュリティ管理	このプロセスで識別した，改善のための処置を記録しなければならない。また，この改善のための処置は，サービス改善計画に入力しなければならない。
7.2 顧客関係管理	このプロセスで特定した改善策を記録しなければならない。この改善策を，サービス改善計画に入力しなければならない。
7.3 供給者管理	このプロセスで特定した改善策を記録しなければならない。この改善策を，サービス改善計画に入力しなければならない。
8.3 問題管理	このプロセスで特定した改善策を記録しなければならない。この改善策を，サービス改善計画に入力しなければならない。

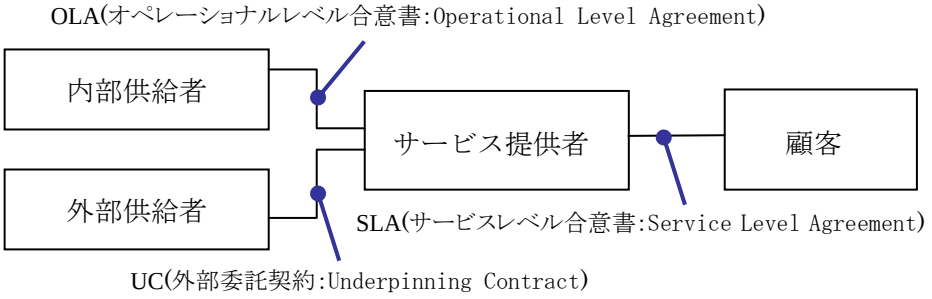
9.2 変更管理	変更管理で特定した改善策を記録しなければならない。この改善策を，サービス改善計画に入力しなければならない。
10.1 リリース管理プロセス	分析には，事業，運用及び支援要員資源に与える影響のアセスメントを含めなければならない。この分析結果は，サービス改善計画に入力しなければならない。

（JIS Q 20000-1:2007 より引用）

2.10. サービスレベル、サービスレベル目標値

サービスレベルは、顧客に対してサービス提供者が提供する IT サービスに関する品質と捉えられます。その品質を測定するための目標がサービスレベル目標値です。サービスレベル目標値を定義して、顧客とサービス提供者の間で合意する文書がサービスレベル合意書（サービスレベル・アグリーメント、以下「SLA」）になります。

サービス提供者が顧客に IT サービスを提供する際には、組織の内部あるいは外部の組織から支援を受ける必要があるかもしれません。サービス提供者は、顧客と合意した SLA の内容を遵守するために、内部あるいは外部の組織に対して一定の品質を確保することを要求する必要が生じることもあります。規格では、サービス提供者が内部あるいは外部の供給者と、支援内容等に関して合意するための文書を「供給者との SLA」としていますが、ITIL では内部の組織との合意を OLA、外部の組織との合意を UC として使い分けています。これらの関係を図 2-8 に示します。



（JIS Q 20000-1:2012 をもとに作成）

図 2-8 SLA、OLA、UC の位置付け

例として、サービス提供者が顧客に対してメールサービスを提供している場合を考えてみます。メールサービスに対する顧客の業務要件が“障害に対して 24 時間以内には復旧する”ことと仮定すると、サービス提供者と顧客はサービスレベル目標値の一つとして、“ダウンタイムが 20 時間以内であること”を SLA に定義するかもしれません。サービス提供者が図 2-8 のように組織の内部及び外部の供給者から支援を受けている場合には、“ダウンタイムが 20 時間以内であること”を確実にするために、障害が発生した場合の目標復旧時間、復旧体制、復旧手順等を供給者と協議して決定し、合意していくことになるでしょう。供給者と合意した内容は、相手に応じて OLA や UC に記載されることになります。

なお、ITIL ではサービスレベル目標値を以下のように説明しています。

> サービスレベル・アグリーメントに文書化された義務。サービスレベル目標値はサービスレベル要件に基づいており、IT サービスの設計が目的に適うようにするために必要とされる。サービスレベル目標値は測定可能であるべきで、通常は KPI に基づいている。
>
> （ITIL V3 用語集 より引用）

2.11. リスク

リスク（RISK）は、“RISICARE”（あえて～する）という古イタリア語から派生したそうですが、様々な定義が唱えられています。

企業にとってのリスクに絞って言えば、『企業にとってのリスクとは、経営資源に対して、不確実性によって影響をもたらすと思われる事態の発生要因およびその影響』と言えます。

また、JIS 規格（JIS Q 31000）でのリスクの定義を見ると「目的に対する不確かさの影響」という表現になっており、その注記 4 で「注記 4　リスクは，ある事象（周辺状況の変化を含む。）の結果とその発生の起こりやすさとの組合せとして表現されることが多い。」と記載しています。これら 2 つに共通するのは影響度（damageability）と発生頻度（frequency）の 2 つの要素で構成されているということです。

ITIL V3 の用語集では、以下の通りとしていますが、同じ事を言っています。

> 組織が影響を受ける可能性のある脅威の尺度。リスクは、業務中断の可能性とその結果発生しうる損失の組み合わせ
>
> （ITIL V3 用語集 より引用）

ITSMS におけるリスクは「IT サービスを正常に提供できなくする事象が発生する可能性と、事象が発生したことによる影響の組み合わせ」と捉えることができます。

なお、リスク管理をシンプルに表現すると、『リスク管理とは、リスクの顕在化による企業活動への影響を抑制するための一連の活動』であると言えます。リスク管理の流れの一例を図 2-9 に示します。

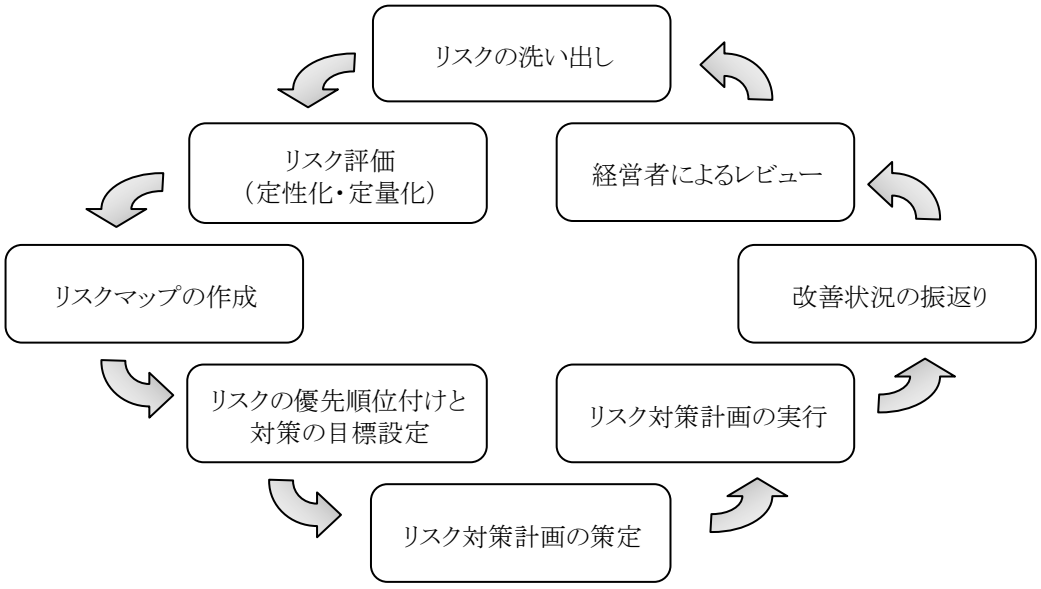


図 2-9 リスク管理の流れの一例

2.12. インシデント

IT 分野では、一般的に、情報資産の管理やシステムの運用における脅威となる事案を指します。情報セキュリティの分野では、以下のように言われています。

> 事業活動又は情報セキュリティを損ねる可能性のある,予期しない又は望んでいない事象。 ①サービス，設備又は施設の停止、②システムの動作不良又は過負荷、③人為的誤り、④方針又は指針への不適合、⑤物理的セキュリティに関する取決めへの違反、⑥管理されていないシステム変更、⑦ソフトウェア又はハードウェアの動作不良、⑧アクセス違反
>
> （JIS Q 13335-1 より引用）

情報セキュリティ以外では、メーカーやベンダーの製品への問い合わせ等の回数・ロードの指標として使われたりしますが、システム運用においては、提供するサービスに関して、以下のように定義することが出来ます。

インシデントとは、「システムが提供するサービスを中断させる可能性がある事案、または顧客が利用するサービスの品質の低下を引き起こす可能性がある事案のこと」を言います。もっと平明な言い方をすれば、『IT サービスを受けたい、あるいは使いたいときに使えないこと、正確な IT サービスを受けられないこと』とも言い直せます。

インシデントは「未遂」も含みますが、インシデントのうち、実際に中断やサービス品質が低下した場合には、一般的なアクシデント（accident : 既遂）として区別します。過去の事故事例を分析してみると、アクシデントが起きる過程には、一見、何の結びつきも無さそうな幾つもの事案が繋がって、最後にアクシデントとして発現することがあります。従って、一つ一つのインシデントが、何処でどのように起きたかを繋いでいき、アクシデントに至るその連鎖を分析した「インシデント・レポート」は、アクシデントを防ぐために重要な情報になります。

インシデントに関連して使われる用語にコメントを加えると以下の通りです。

- インシデント管理　：可能な限り迅速に顧客へのサービスを元に戻すという主要な目標を持って、運用上の不測の事案を管理するサービスマネジメントのプロセス。
- インシデント・コントロール：インシデントを識別、記録、分類し、影響を受けたサービスが回復するまで進行させるプロセス。
- インシデント・ライフサイクル：インシデントの進行過程のこと。インシデントの「発生」、インシデントの「検出」、障害原因の「診断」、CI の「修理」、稼働インフラストラクチャに CI を復元する「復旧」、サービスの「回復」に分解される。

医療や航空などの分野では、事故に至らない「ひやっとした事例」といったニュアンスの用語として使われています。

2.13. 問題

JIS Q 20000-1 において「問題」は、次のように定義されています

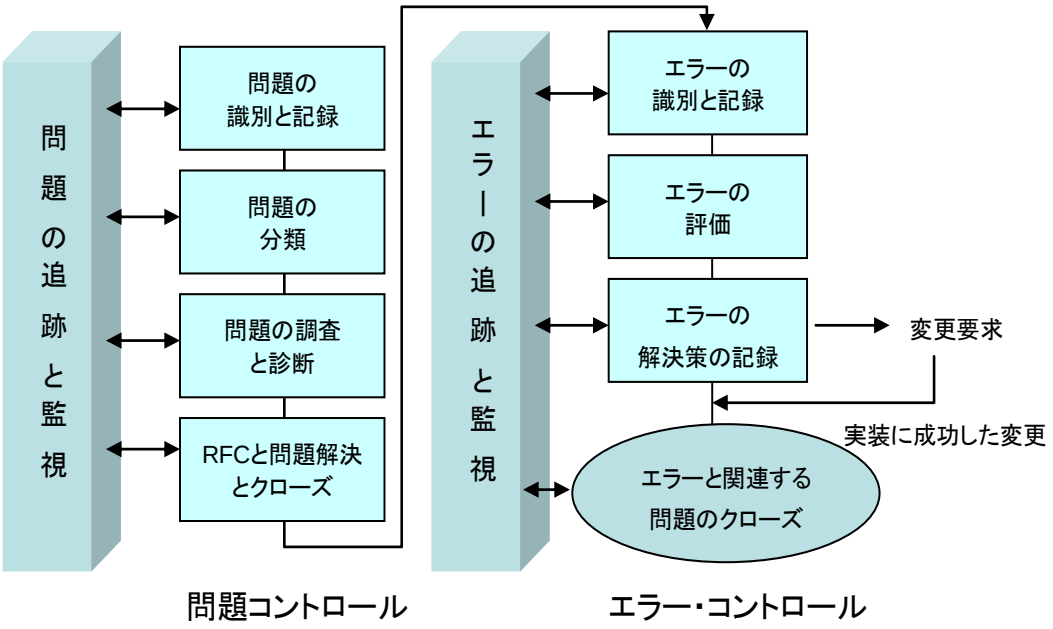
> 3.19 問題（problem）
> 一つ以上のインシデントの根本原因。
> 注記 問題の記録が作成された時点では，通常はその根本原因は不明であり，問題管理プロセスは更なる調査に対して責任をもつ。
> （JIS Q 20000-1:2012　3 用語及び定義　より引用）

規格では解決プロセスとして、IT サービスを阻害する要因を解決するためのインシデント及びサービス要求管理プロセス、問題管理プロセスを規定しています。問題管理プロセスは、インシデント及びサービス要求管理から解決できなかったインシデントを受け取り、その根本原因を調査します。

ITIL V2 の問題管理では、インシデントや問題が事業に対する中断を最小限に抑えることと、インシデントを引き起こした根本原因の検知と、恒久的な解決を提供し、更に、再発を防ぐ予防までを目標としています。ITIL V2 では、図 2-10 に示すように、問題コントロールとエラー・コントロールという 2 つの主要な活動により、問題解決までを管理しています。

問題の根本的な原因が発見され、回避策（ワークアラウンド）が特定されると、問題は、既知の誤りと呼ばれるようになります。問題コントロールの主要な目的は問題を既知の誤りにすることです。リアクティブな活動であり、図 2-10 に示すように、幾つかのフェーズにわかれています。

エラー・コントロールは、既知の誤りが解決されるまでの活動です。エラー・コントロールでは、変更管理に対して変更要求（Request for Change：RFC）を発行します。規格における問題管理での問題の識別から解決までの要求事項は、問題コントロールとエラー・コントロールの活動がカバーしていると言えます。



（ITIL 書籍『サービスサポート』をもとに作成）

図 2-10 問題コントロールとエラー・コントロール

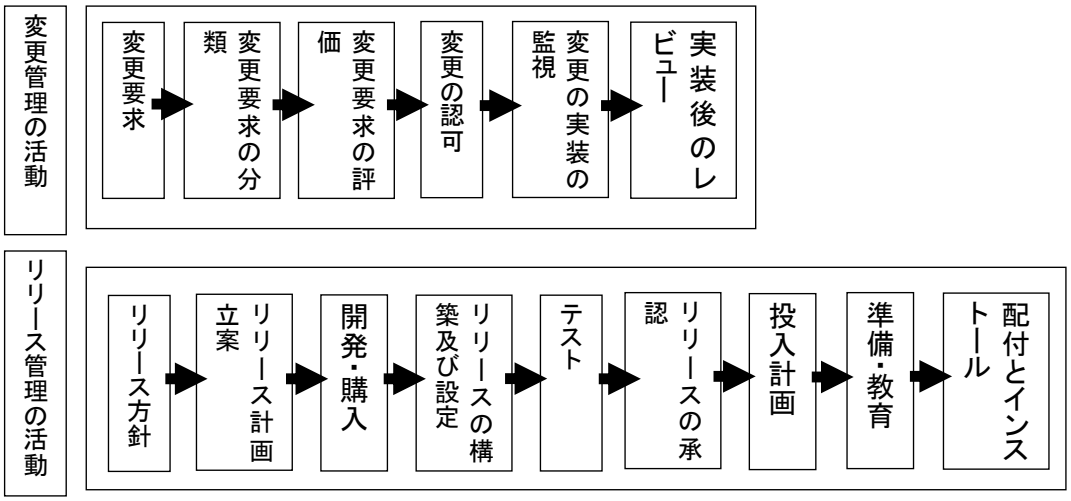
2.14. 変更とリリース

変更は IT サービスを改善するために行う活動です。『IT サービスマネジメントーITIL 入門』書籍において、変更管理の章で次のような格言を紹介しています。

“すべての変更が改善ではないが、すべての改善は変更である。”IT サービスの改善にとって、変更がいかに重要であるかを表現していると言えるでしょう。変更管理プロセスとリリース管理プロセスは、「変更」に密接に関連するプロセスですが、異なる役割を持ちます。変更管理は、すべての変更を扱い、変更の実装をコントロールすることが目的です。変更を稼働環境へ実装することは、リリース管理に責任があります。2 つのプロセスを連携・協調させて活動させてゆくことが求められます。

変更管理で取り扱う変更の対象について考えると、変更の最小単位は、構成品目となります。構成品目を管理しているのは、構成管理ですから、「変更」における関連プロセスは、構成管理を含めた 3 つのプロセスからなることがわかります。

変更管理とリリース管理の主な活動を図 2-11 に示します。



（ITIL サービスサポートをもとに作成）

図 2-11　ITIL 変更管理とリリース管理の活動

2.15. ベースライン、構成ベースライン

JIS Q 20000-1:2007 では用語においてベースラインを次のように定義していました。
ITIL V2 では構成ベースラインとも呼んでいます。

> ベースライン（baseline）
> ある時点における，サービス又は個々の構成品目の状態のスナップショット（snapshot）。
> （JIS Q 20000-1:2007　2 用語及び定義　より引用）

JIS Q 20000-1:2012 では、箇条 3 の用語及び定義において、“ベースライン”の用語は無くなりました。替わって、構成ベースラインとして定義されています。

> 3.2 構成ベースライン（configuration baseline）
> サービス又はサービスコンポーネントの存続期間における特定の時点で，正式に指定された構成情報。
> 注記 1 構成ベースラインに，このベースライン以降に承認された変更を加えたものが，最新の構成情報となる。
> 注記 2 ISO/IEC IEEE 24765:2010 から部分的に採用。
> （JIS Q 20000-1:2012　3 用語及び定義　より引用）

リリース及び展開管理で IT サービスを提供している稼働環境に対して変更の実装を行いますが、いつも変更がうまくゆくとは限りません。例えば、変更の実装途中でインシデントが発生した場合はどうすれば良いでしょうか。インシデントを解決して、変更の実装を続行するか、一旦、止めて、元に戻すか、その時々の条件により判断することになるでしょう。もし、途中まで変更したものを元に戻そうとしても、ハードウェアあるいはソフトウェアには既に変更が加えられていて、元の状態には戻れないかも知れません。

構成品目あるいは構成品目を集めたセットを、特定の目的のために、ある時点で、その時の状態で凍結し、保存しておくことを『スナップショットを取る』と言います。変更の直前に稼働中のインフラストラクチャの状態をそのまま保存しておくというイメージです。これには、ハードウェア、ソフトウェアなどの関連する構成品目の状態が含まれます。

変更は、構成品目（Configuration Item）に対して加えられますので、変更を実施した後で、何らかの理由により構成品目を元に戻したい時には、保存している変更前の構成品目の状態が役立ちます。この「変更前の構成品目の状態」を構成ベースラインと呼びます。

構成ベースラインは変更が失敗した場合あるいは構成品目を再構築する必要があるような場合に利用されます。変更では構成品目が変更されるのは当然ですが、その他にも、システムに新しい構成品目を追加する場合、災害が発生した後のリカバリーを考えると、構成品目が元の状態から変更されてしまうことになります。構成品目を元に戻すことは、変更前の構成品目の状態と比較できなければなりません。アプリケーションやソフトウェアの構成ベースラインは再構築にも利用できます。

このように、構成ベースラインは、インフラストラクチャを確実に、ある時点まで回復することができるようにするために利用されます。

2.16. サービスコンポーネント

IT サービスマネジメントではサービスを構成する要素を表すのに CI（Configuration Item）という用語が使われます。CI は次のように定義されています。

> 3.3　構成品目，CI（configuration item）
> サービスの提供のために管理する必要がある要素。
> （JIS Q 20000-1:2012　3 用語及び定義　より引用）

CI だけで IT サービスを構成する全ての要素を表すことは現実的ではありません。IT サービスを構成する IT インフラストラクチャを取ってみても、ハードウェア、ミドルウェア、アプリケーション、ネットワークと多くの異なる要素があります。JIS Q 20000-1:2007 では、コンポーネントという用語を使用することで、CI 以外の要素を表現していました。例えば、可用性の定義では、次のような使い方をしていました。

> 2.1　可用性（availability）
> あらかじめ決めた時点又は期間にわたって，要求された機能を実行するコンポーネント又はサービスの能力。
> （JIS Q 20000-1:2007　2 用語及び定義　より引用）

残念なことにコンポーネントの用語としての定義は 2007 年版にはありませんでした。加えて、コンポーネントという用語の使い方にも一貫性が欠けていて、規格の中ではコンポーネントを単独として使用する他に、さまざまな組み合わせで使われていました。

・インフラストラクチャのコンポーネント
・ハードウェアコンポーネント
・システムコンポーネント

等々です。

2012 版では、このような一貫性に欠けていた点を改め、サービスコンポーネントを用語として定義し、規格内ではコンポーネントを単独の用語としては使用していません。

> 3.27　サービスコンポーネント（service component）
> サービスの一つの単位であり，他の単位と組み合わされることで完結したサービスを提供する。
> 例 ハードウェア，ソフトウェア，ツール，アプリケーション，文書，情報，プロセス又は支援サービス。
> 注記 サービスコンポーネントは，一つ以上の構成品目で構成し得る。
> （JIS Q 20000-1:2012　3 用語及び定義　より引用）

2.17. サービスマネジメントシステム（SMS）

「情報技術－サービスマネジメント－第 1 部:仕様」

上記は、JIS Q 20000-1:2007 年版のタイトルです。

JIS Q 20000-1:2012 のタイトルは次のように変更になりました。

「情報技術－サービスマネジメント－第 1 部:サービスマネジメントシステム要求事項」

2012 年版では、JIS Q 20000 がサービスマネジメントシステム（以下、SMS とする。）に対する要求事項であることを明確に宣言しています。

JIS Q 20000-1:2012 規格の 0.2 において、次のように述べられています。

> この規格は，サービス提供者がサービスマネジメントシステム（以下，SMS という。）を計画，確立，導入，運用，監視，レビュー，維持及び改善する場合の統合されたプロセスアプローチを要求する。
>
> （JIS Q 20000-1:2012　0.2 サービスマネジメントシステム要求事項　より引用）

では、SMS とは何でしょう？ JIS Q 20000-1:2007 年版で定義されていた用語は 15 ありましたが、その中に SMS はありませんでした。JIS Q 20000-1:2012 年版では大幅に用語の定義が追加され、SMS もその中に含まれています。

> 3.31　サービスマネジメントシステム，SMS（service management system）
>
> サービス提供者のサービスマネジメントの活動を指揮し，管理するためのマネジメントシステム。
>
> 注記 1 マネジメントシステムは，方針及び目的を定め，その目的を達成するための，相互に関連する又は相互に作用する要素の集まりである。
>
> 注記 2 SMS には，サービスの設計，移行，提供及び改善のため，並びにこの規格の要求事項を満たすために必要な，全てのサービスマネジメントの方針，目的，計画，プロセス，文書，及び資源を含む。
>
> 注記 3 JIS Q 9000:2006 の“品質マネジメントシステム”の定義から部分的に採用
>
> （JIS Q 20000-1:2012　3 用語及び定義　より引用）

マネジメントシステムを用いて、サービス提供者のサービスマネジメントを指揮、管理することが SMS のようです。マネジメントシステムは、注記 1 にマネジメントシステムについての記載がありますが、本章に於いても解説を加えていますので、そちらも併せてご参照ください。注記 3 でも触れていますが、いわゆるマネジメント規格とよばれる JIS Q 9001（品質マネジメントシステム）、JIS Q C27001（情報セキュリティマネジメントシステム）などと同様の考え方を取り入れています。

サービスマネジメントは 2012 年版で用語として、次のように定義されています。

3.30　サービスマネジメント（service management）
　サービスの要求事項を満たし，サービスの設計，移行，提供及び改善のために，サービス提供者の活動及び資源を，指揮し，管理する，一連の能力及びプロセス。
（JIS Q 20000-1:2012　3 用語及び定義　より引用）

SMS の用語定義から始まって、“マネジメントシステム”に“サービスマネジメント”と、言葉遊びにみたいになりましたが、これらの関係を端的に表し、SMS への理解を深めさせてくれそうなのが次の図です。

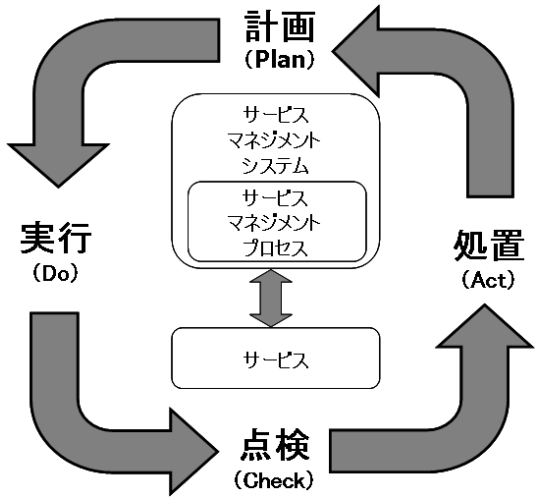


図 1 －サービスマネジメントに適用される PDCA 方法論
（JIS Q 20000-1:2012　0.2 サービスマネジメントシステム要求事項　より引用）

SMS（サービスマネジメントシステム）の中には、箇条 4 のマネジメントシステムと箇条 5～箇条 9 のサービスマネジメントプロセスがあります。

SMS から下にサービスがつながっているのは、サービス提供者が、SMS を運用してサービスを提供する構造を示しています。

そして、SMS とサービスを P-D-C-A が取り囲んでいます。マネジメントシステムの実践における方法論は PDCA です。図では、その PDCA がサービスに対しても提供されることを意味しています。

JIS Q 20000 が他のマネジメントシステムと異なる点は、PDCA がサービスに対しても適用されるという点です。規格の序文においても、SMS 及びサービスのあらゆる場面で P-D-C-A として知られる方法論を要求するとしています。

この規格は，SMS 及びサービスのあらゆる場面で，“計画（Plan）－実行（Do）－点検（Check）－処置（Act）”（PDCA）として知られる方法論の適用を要求する。
（JIS Q 20000-1:2012　0.2 サービスマネジメントシステム要求事項　より引用）

2.18. 是正処置（corrective action）

3.6　是正処置（corrective action）

検出された不適合又はその他の検出された望ましくない状況の原因を除去する, 又はそれらの再発の可能性を低減するための処置。

（JIS Q 20000-1:2012　3 用語及び定義より引用）

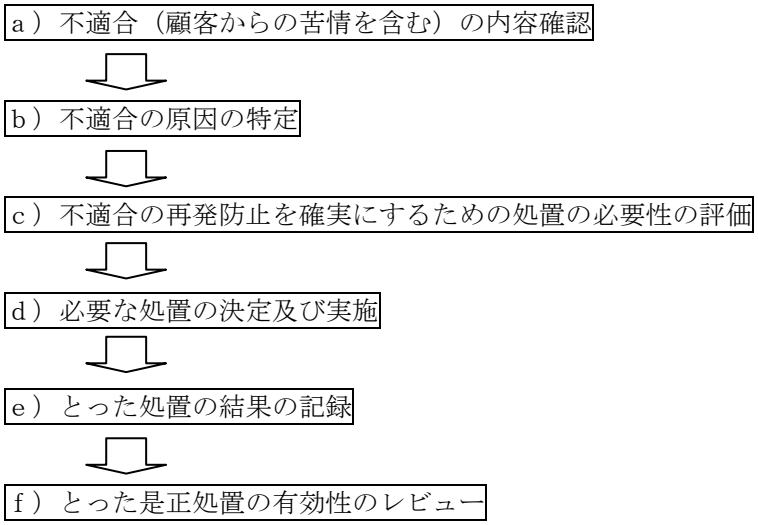
規格の要求事項、組織が定めた要求事項、法令・規制又は契約上により求められる要求事項に対して、適合していない活動の状況や結果を不適合といいます。

IT サービスではインシデントとして取り扱う事象の多くが不適合に該当しますが、内部監査やマネジメントレビューなどの仕組みの見直しからも不適合は検出されます。顧客や利用者からの提供サービスに対する苦情又はクレームも不適合として取り扱います。

マネジメントシステムでは、この不適合が検出された場合には、速やかにその不具合を解消することが要求されますし､場合によっては根本的な原因の除去による改善の活動も求められます。

不適合（障害や苦情を含む）の原因を特定し、その根本的な原因を除去し、再発を防止するための恒久的な処置を是正処置といいます。是正処置は、検出された不適合の持つ影響に応じたものでなければなりません。応急的な復旧のための修正処置と併せて行うことがあります。

JIS Q 20000-1 において参照されている JIS Q 9001:2008　8.5 の是正処置では、次の要求を満たすために文書化した手順を整備することを求めています。



是正処置、予防処置を含む改善の機会には文書化された手順に加えて、活動の文書化及び記録が要求されます。SMS の運用において不適合（障害や苦情を含む）な事象に対する処置を文書で“見える化”し、定めた手順に従って確実に処置又は対処をするためです。

上記の c）及び d）では、責任ある人が再発防止の処置の必要性を評価して、必要な処置を決定し、実施を確実にすることが求められています。

また f）には、実施した是正処置によって“意図した結果”が得られているかの有効性レビューによる検証までが要求されていることに注目ください。

2.19. 予防処置（preventive action）

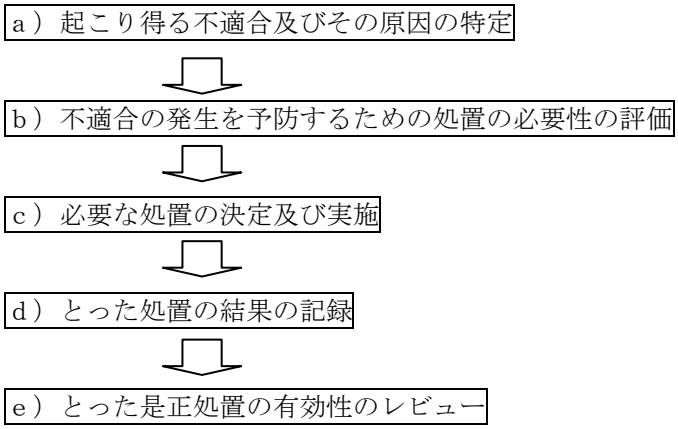
3.18　予防処置（preventive action）
起こり得る不適合又はその他の起こり得る望ましくない状況の発生の原因を回避する若しくは除去する，又はそれらの発生の可能性を低減するための処置。
（JIS Q 20000-1:2012　3 用語及び定義　より引用）

提供する製品やサービスにおいて、不測の事態が想定されるリスクに対応し、そのリスクの影響を把握するリスクアセスメントを行って、その結果から設計し導入される回避策、軽減策、又は移転策などの処置も予防処置に含まれます。

上記の他、マネジメントシステムの運用の中から、以下のような予防処置も行われています。

（1）他社或いは他のサービスにおいて発生したインシデントに対する是正処置を参考にして、SMS に予防処置として導入する。（他事例の水平展開、波及処置などとも呼ばれる）
（2）影響が顕在化していない不測の事象を「ヒヤリハット」として収集し、不足の影響が発生する前にその事象に対して予防処置を実施する。
（3）サービス提供の活動における要求、手順、設備、作業者、提供方法などの構成ベースラインからの変更に対して、その変更による影響を事前に評価し、その影響が回避又は軽減できる予防策を決定し実施する。

JIS Q 20000-1 において参照されている JIS Q 9001:2008　8.5 の予防処置では、次の要求を満たすために文書化した手順を整備することを求めています。



是正処置、予防処置を含む改善の機会には文書化された手順に加えて、活動の文書化及び記録が要求されます。SMS の運用において、不適合の潜在的な事象に対する予防活動を文書で“見える化”し、定めた手順に従って確実に処置又は対処をするためです。

2.20. 情報セキュリティインシデント

> 3.12　情報セキュリティインシデント（information security incident）
> 望ましくない単独若しくは一連の情報セキュリティ事象, 又は予期しない単独若しくは一連の情報セキュリティ事象であって, 事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。
>
> （JIS Q 20000-1:2012　3 用語及び定義　より引用）

この情報セキュリティインシデントには、サービス停止、システムダウン、情報漏洩等の事件や事故が含まれます。

情報セキュリティインシデントの管理として、JIS Q 27002:2006 では 13 章の「情報セキュリティインシデントの管理」において、次のような対応を求めています。

(1) 情報セキュリティ事象及び弱点を検出した場合、適切な管理者への連絡経路を通して、できるだけ速やかに報告するのが望ましい。情報セキュリティ事象及び弱点の報告に加えて、情報セキュリティインシデントを検知するために、システム、警告及び脆弱性の監視を利用することが望ましく、情報セキュリティインシデントの形態、規模及び費用を定量化して監視できるようにする仕組みを備えることが望まれる。

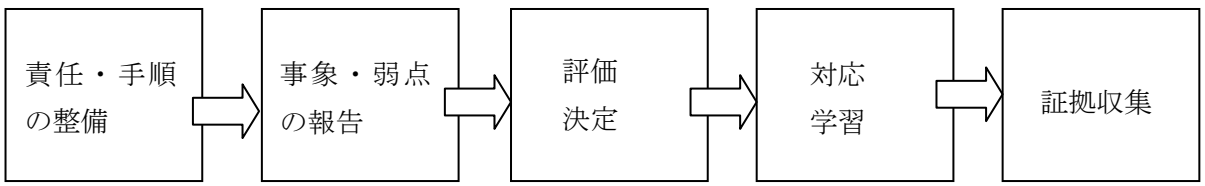
(2) その報告があった時に直ちに、それらを効果的に取り扱える責任体制及び手順を備えることが望ましい。責任体制及び手順では、情報セキュリティインシデントを管理する目的を経営陣が理解していることが望ましく、情報セキュリティインシデントの管理について責任ある人々が、組織が決めた情報セキュリティインシデントの取扱いの優先順位を理解していることを確実にすることが望まれる。

(3) 情報セキュリティ事象の評価、情報セキュリティインシデントへの対応、並びに情報セキュリティインシデントの監視、評価及び包括的管理に対し、継続的改善の手続きを取ることが望ましい。

情報セキュリティ事象を評価し、情報セキュリティインシデントとして分類すべきかどうかを決定する。情報セキュリティインシデントは文書化された手順に従って対応され、分析や解決の結果で得られた知識は、将来の発生頻度、損傷及び費用を抑制するための強化した管理策又は追加の管理策の必要性の提起に使われる。

(4) 証拠が必要な場合には、法的要求事項を順守することを確実にするために、証拠を収集することが望ましい。

情報セキュリティインシデント処理後の個人又は組織への事後処理が法的処置（民事又は刑事）に及ぶ場合には、関係する法域で定めている証拠に関する規則に従うために、証拠となり得る情報を特定、収集、入手及び保護することが望まれる。



2.21. 内部グループ

「内部グループ」は、JIS Q 20000-1:2012 年版で追加された用語で、次のように定義されています。

> 3.14　内部グループ（internal group）
> サービスの設計，移行，提供及び改善に貢献するために，サービス提供者と合意文書を交わす，サービス提供者の組織の一部。
> 注記　内部グループは，サービス提供者の SMS 適用の範囲外である。
> （JIS Q 20000-1:2012　3 用語及び定義　より引用）

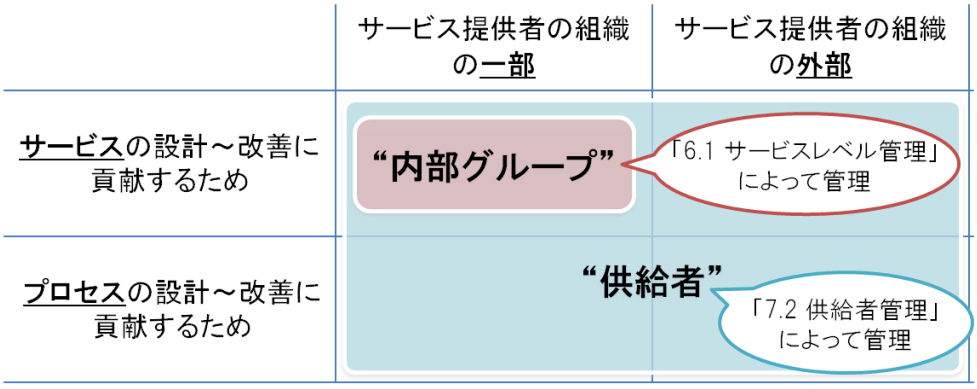
この「内部グループ」は、以下のような箇所で使われており、「供給者」と似たような概念だとわかります。

> 供給者がプロセスの一部を運用している場合，サービス提供者は供給者管理プロセスによって供給者を管理しなければならない。内部グループ又は顧客がプロセスの一部を運用している場合，サービス提供者はサービスレベル管理プロセスによって内部グループ又は顧客を管理しなければならない。
> （JIS Q 20000-1:2012　4.2 他の関係者が運用するプロセスのガバナンス　より引用）

また、「供給者」は、次のように定義されています。

> 3.35　供給者（supplier）
> サービス又はプロセスの設計，移行，提供及び改善に貢献するために，サービス提供者と契約を結ぶ，サービス提供者の組織の外部組織，又は組織の一部。
> （JIS Q 20000-1:2012　3 用語及び定義　より引用）

以上からまとめると、「内部グループ」と「供給者」の違いは下図のように理解すればよいでしょう。なお、組織の一部を「内部グループ」と識別するか「供給者」と識別するかにより、適用される要求事項が異なってきますので、注意が必要です。



2.22. サービス

「サービス」は、JIS Q 20000-1:2012 年版で追加された用語で、次のように定義されています。

> 3.26　サービス（service）
> 顧客が達成することを望む成果を促進することによって，顧客に価値を提供する手段。
> （JIS Q 20000-1:2012　3 用語及び定義　より引用）

これだけ読んでいてもイメージがしにくいですが、規格には以下のようなことを表す図が記載されています。

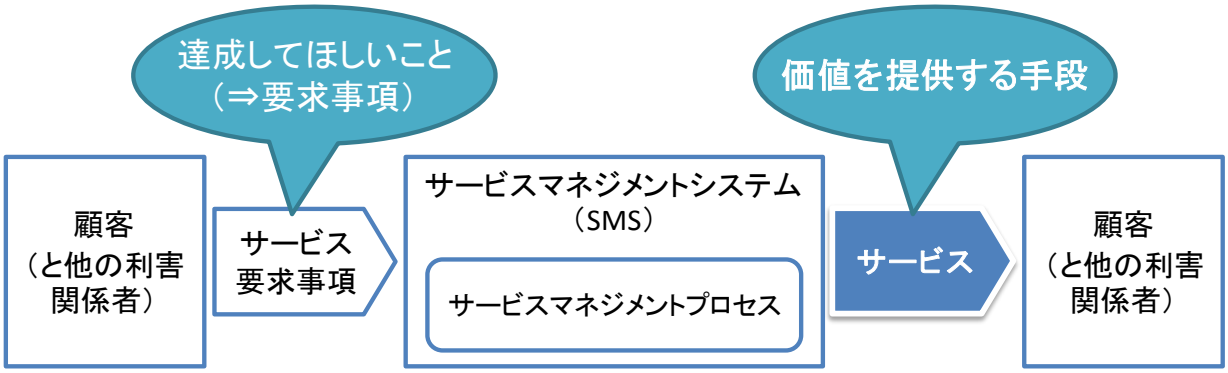


図 2-12　「サービス」の位置付け

上図からは、顧客（他の利害関係者を含む）からの「サービス要求事項」を受けて、顧客へ提供されるものが「サービス」であることがわかります。このように表現すると、接客“サービス”のような一般的に“サービス”と呼ばれていることも含まれるように読めそうですが、この規格が「情報技術（IT）」の規格であることを踏まえると、“IT サービス”のことを暗に意味していると捉えてもかまわないと考えられます。

IT サービスのイメージは、本ガイドの「2.2. IT サービスと IT サービスマネジメント」に示していますので参照してください。

3. スコーピング

3.1. はじめに

本章は、ITSMS 認証取得を目指す組織が、認証取得の適用範囲を特定する際の手引きとして、原則的な考え方を示すものであり、マネジメント・コントロールの程度（深さ）や範囲について事例をあげて解説しています。『ITSMS ユーザーズガイド - JIS Q 20000 (ISO/IEC 20000) 対応 - 「付録 D　認証の適用範囲の考え方」』及び『本書「付録 C ITSMS の適用範囲設定に関する手引き（ISO/IEC 20000-3:2012 の要点）」』の記載内容とあわせてご活用いただくことを推奨します。

3.2. 適用範囲設定時の原則的な考え方

3.2.1. すべての管理プロセスを整備する

ITSMS 認証取得を目指す IT サービス提供者（以下、「組織」）は、その規格である JIS Q 20000-1 における要求事項を原則として全て満たす必要があります。もちろん、組織が特定の事業上の必要性を満たすために、個別の目的や管理方法の追加を妨げるものではありません。また、組織において定める ITSMS の目的や目標を達成するために、この規格をどのように実施するかは、組織内の方針、組織とサービス提供を受ける顧客との関係や相互の合意によって決定されます。

ITSMS は、品質マネジメントシステム（JIS Q 9001:2008）（以下、「QMS」）における 7 章製品実現の適用除外や、情報セキュリティマネジメントシステム（JIS Q 27001:2006）（以下、「ISMS」）における附属書 A の管理策の採用要否のように、要求事項を除外することを明確に定めていません。

ITSMS の適用範囲定義が難しいと言われる理由のひとつは、箇条 6 以降の各管理プロセスを全て整備することにあると考えられます。各管理プロセスは、組織における業務プロセスを意味します。該当する業務が組織に存在するかを確認し、存在しない場合、適用範囲設定の見直しや管理プロセスを組織に導入する意義を検討する必要があります。以下に、各管理プロセスにおいて適用範囲設定を左右する重要な検討事項を解説します。

a）サービスレベル管理と事業関係管理

規格では、提供するサービスを SLA という文書として合意すること、関係者での定期レビューによって維持することが要求されています。適用範囲を定める上で検討すべきは次の 2 点です。

- （提供する各サービスの）SLA の策定と合意
- （提供する各サービスの）SLA の定期レビュー

ITSMS の初回審査時点において、適用範囲のサービスを提供する全ての顧客と SLA を合意していることが望まれます。しかし、データセンタ事業者や ASP 事業者などは数百あるいはそれ以上の顧客へのサービス提供も考えられます。その場合は、全ての顧客と合意がなされていない状態であっても、一定程度の合意実績があり、全範囲の合意に向けた能動的かつ計画的な取組みが認められることが重要です。なお、SLA の記載内容については、具体的な要求事項はありません。また、必ずしも、『サービスレベル合意書』という名称とする必要もありません。

定期レビューは、「事業関係管理」や「サービスの報告」と合わせて考える必要があります。事業関係管理では、あらかじめ定めた間隔でのレビューを要求しています。よって、適用範囲とす

るサービスにはこの要求事項に対して何らかの対応が必要となります。ここでも多数の顧客を抱える組織では対応が難しくなりますが、サービスレビュー等は相対だけではなく、企業ホームページ（顧客別専用サイトの開設等）、TV 会議、電話会議、電子メールでの資料受送信など様々なコミュニケーション手段を活用することができ、顧客やサービスの特性などに応じて対応の軽重を組織の方針として定義することができます。いずれにしても、顧客との良好な関係を確立し、顧客の事業上のニーズの変化などに対応できる態勢構築が重要であることは言うまでもありません。

b）構成管理と変更管理

構成管理の要求事項には「変更要求のアセスメントを支援するために、変更管理プロセスに提供しなければならない」とあります。また、変更管理の要求事項としては、「変更要求は定義された適用範囲をもたなければならない。」とされています。このように、構成管理の対象範囲は変更管理プロセスが適用できる範囲として構築することが求められています。すなわち、構成情報は全て変更管理プロセスによって追加・更新されることを意味します。但し、変更管理プロセスは同一の統一されたプロセスとすることまでは要求していません。リスクに応じて承認手順の一部を省略したり、変更要求に必要な申請書類を簡素化したりできます。

構成管理及び変更管理の目的は、サービスに係わる変更を制御された方法で実施し、正確な構成情報を維持することです。対象とするサービスが構成管理もしくは変更管理の範囲外の場合、適切な構成情報や変更を管理するプロセスが欠落してしまい、ITSMS の適用範囲としては相応しくないということになります。

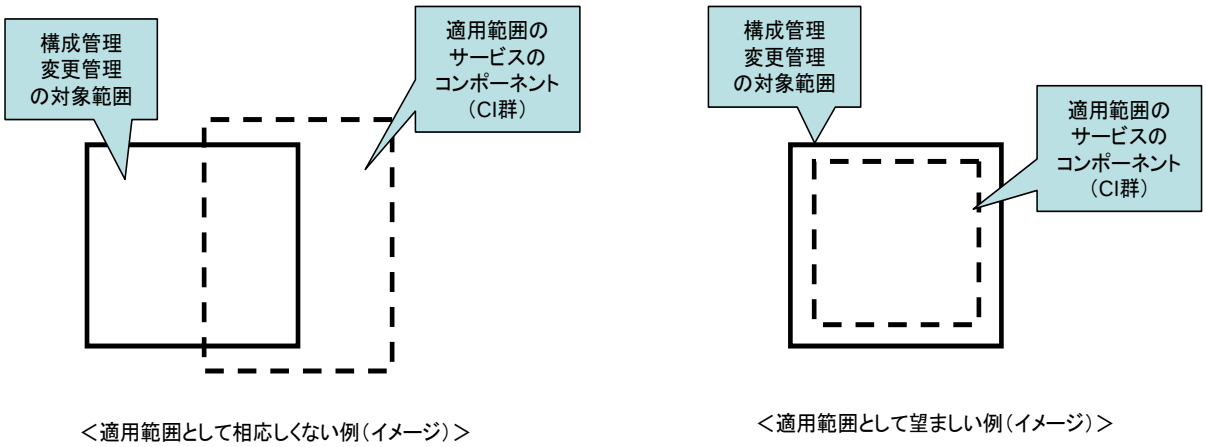


図 3-1　構成管理・変更管理の範囲設定（イメージ）

管理すべき構成品目の詳細さも論点のひとつになりますが、規格では具体的な要求はありません。組織として、どこまで詳細に管理するか（どのような構成品目を記録するか）が明確に定義されていることが重要です。

また、構成情報を格納する構成管理データベースは物理的に単一のデータベースである必要はありません。複数のデータベースであっても、それら全体を構成管理データベースとして位置付け、管理すればよいのです。但し、構成品目は一意に識別可能であることが規格上求められていますので、この場合、全体としての情報の正規化、もしくは、同一の構成品目の識別と更新の同

期などに留意しなければなりません。

c）情報セキュリティ管理

規格では、情報セキュリティ基本方針の策定と経営陣による承認、サービス及びシステムへのアクセスに関連するリスクマネジメントのために、セキュリティ管理策の文書化と適切な運用を要求しています。また、管理策が関係するリスクと管理策の運用・維持まで文書に記述することを求めています。ISMS 認証を取得している場合など、組織に備わっている情報セキュリティ基本方針や管理策を定めた文書などが範囲を限定している場合は、ITSMS の適用範囲検討時において、情報セキュリティに関する取組みの一部拡大、ITSMS の適用範囲とするサービスの縮小などの検討・調整が必要となります。

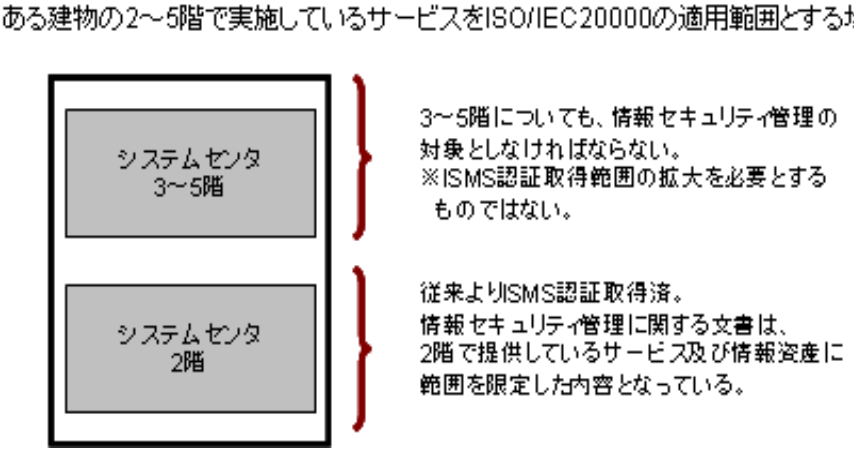


図 3-2　情報セキュリティ管理の対象範囲が限定されている場合の対応例

d）その他の留意事項

ITSMS 適用範囲を定義する場合は、前述の a）～c）の他、以下の点についても留意してください。

①サービス継続及び可用性管理

可用性及びサービス継続計画は、組織の方針や IT 環境、サービスの内容等により作成単位が異なります。複数のサービスを適用範囲とする場合において、組織の決定により個々のサービスごとの計画策定は相応しくない、もしくは過剰であると判断される場合などは、複数のサービスを包含するような計画を策定すること自体に問題はありません。

また、規格では試験の実施を求めています。全ての範囲の試験を実施することが望ましいと言えますが、「事業上の必要性」を鑑みた方針を定め、計画的に実施することを、組織内の方針、顧客との合意などをもとに合理的に説明できれば問題ありません。

②供給者管理

事業関係管理の要求事項と同様に、あらかじめ定めた間隔で、供給者のパフォーマンスをレビューすることを要求しています。組織が適用範囲とするサービスに影響を与え得る供給者（委託先等）を全て特定し、当該供給者とレビュー実施できるか否かが適用範囲設定の判断材料のひとつになります。

③リリース及び展開管理

規格では、制御された受入れ試験環境を確立することが求められています。制御の度合いは組織により異なるものの、組織の方針、顧客からの要求、その他サービス固有のリスク等を踏まえた環境を整備することが必要です。

しかし、全てにおいて試験環境を整備することが困難な場合も想定されます。整備する「試験環境」は、本番環境との近似性や独立の度合いなどについて、規格要求事項には具体的に明記されていません。したがって、組織における定義が重要になります。そのような意味において、環境整備できうる（整備する用意のある）サービスを適用範囲として選択するのがよいでしょう。

④その他管理プロセス

インシデント及びサービス要求管理や問題管理では、適用範囲としたサービスの「インシデント」及び「問題」を管理しなければなりません。また、容量・能力管理、予算業務及び会計業務などについても、カバーされている必要があります。

3.2.2. 各マネジメントプロセスの管理すべき対象が一貫している

サービス提供者は JIS Q 20000-1 に含まれるサービスマネジメントプロセスすべてが、例外なく網羅されている必要があります。但し、適切なサービスマネジメントプロセスが存在しても、それぞれのマネジメントプロセスが管理すべき対象（システムやサービス）に一貫性がないと意味を持たないサービスマネジメントと成りかねない恐れがあり、注意が必要です。

図 3-3 に示すサービス提供者が IT サービスＡ、Ｂ、Ｃ、Ｄという 4 つの IT サービスを提供していたと仮定します。

このサービス提供者は、組織全体としては JIS Q 20000-1 に含まれるサービスマネジメントプロセスすべてを実装しており、またそれぞれサービスマネジメント計画に則り活動（コントロールされた状態）も行っているため IT サービスＡ、Ｂ、Ｃ、Ｄすべてを適用範囲として認証取得を目指しています。

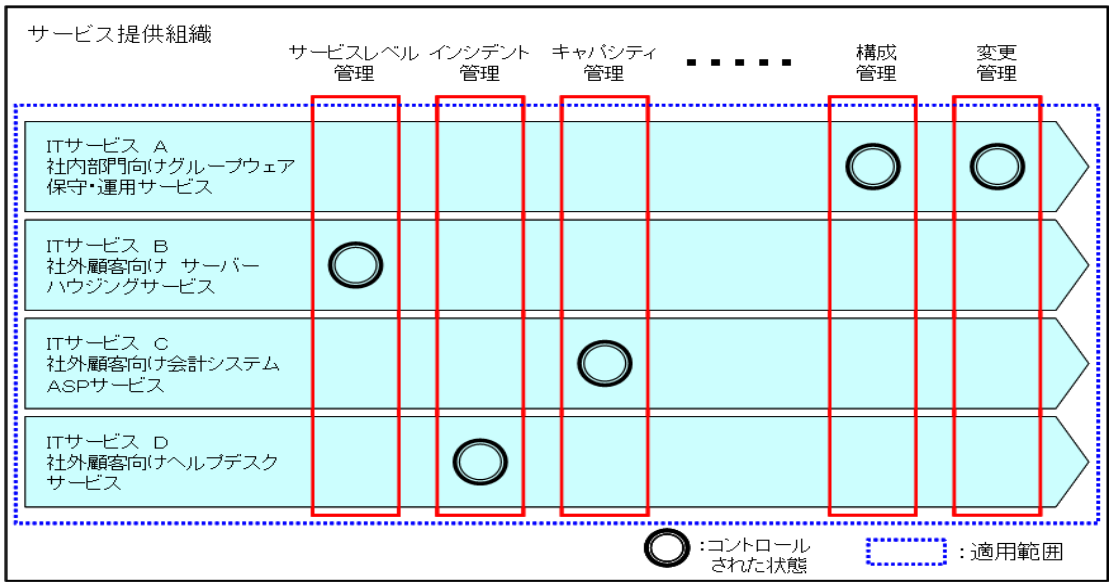


図 3-3　提供サービスとサービスマネジメントプロセスの関係

このようなケースでは、組織全体として見れば確かにサービスマネジメントプロセスすべてを実装しコントロールされた状態で活動しているわけですから問題はないように思われますが、図 3-3 で示すようにマネジメントプロセスで管理している対象のシステムやサービスがバラバラな状況で、果たしてこの活動が効果的なサービスマネジメントと言えるのでしょうか。

幾つか例をあげてみると、例えば IT サービスＡ（社内部門向けグループウェア保守・運用サービス）における構成管理では社内用グループウェアシステムが管理の対象となっているでしょうし、IT サービスＣ（社外顧客向け会計システムの ASP サービス）におけるキャパシティ管理の対象システムは ASP で提供している会計システムが該当します。また、IT サービスＤ（社外顧客向け IT ヘルプデスクサービス）においては、おそらく顧客の IT 資産に関するインシデントをインシデント及びサービス要求管理で取り扱っているでしょう。図 3-3 で示すような状況では、効果的で且つ一貫した IT サービスマネジメントは望めません。

そもそも JIS Q 20000-1 において「SMS を調整のとれた形で統合し、かつ、実施することによって、継続的な管理、並びに継続的改善の機会、より高い有効性及び効率性が得られる。」としています。すなわち、各マネジメントプロセスが管理すべき対象（システムやサービス）に一貫性を持ち、ひとつの管理対象を各マネジメントプロセスが相互に密接な関連性を持って、はじめて効果的なサービスマネジメントが実現できることを意味しています。

したがって、例え組織全体で JIS Q 20000-1 が要求する管理プロセスをすべて実装していたとしても図 3-3 で示すような状況では JIS Q 20000-1 の適用の宣言は出来ません。当然 IT サービスＡ～Ｄ個々のサービスにおいても、すべての管理プロセスの活動が認められないので個々のサービス単位でも適用の宣言は出来ないと考えてください。

JIS Q 20000-1 における適用範囲の考え方としては、例えば図 3-4 に示すように、ある 1 つの管理対象（システムやサービス）において、JIS Q 20000-1 に含まれるサービスマネジメントプロセスすべてが実装されており、コントロールされた環境で活動されていることが望ましいと言えます。

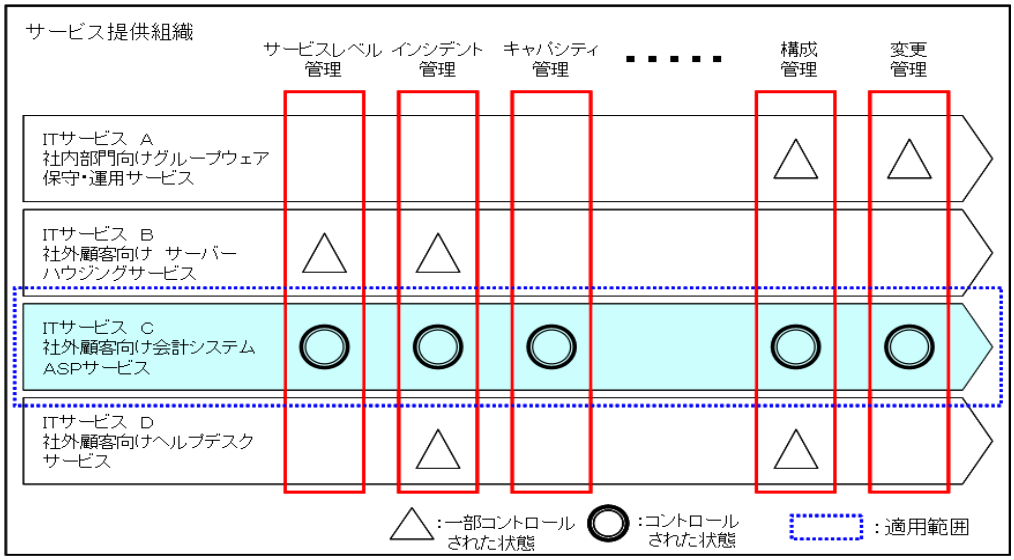


図 3-4　ITSMS 適用を宣言する場合の望ましい状態

理想としては、図 3-5 に示すようにサービス提供者が提供する全てのサービスを適用範囲として、各マネジメントプロセスの共通的な管理基準に則り、それぞれのサービスの内容は異なっていても一貫したサービスマネジメントが実施され、サービス品質の均一化を図ることが望ましいと思われます。

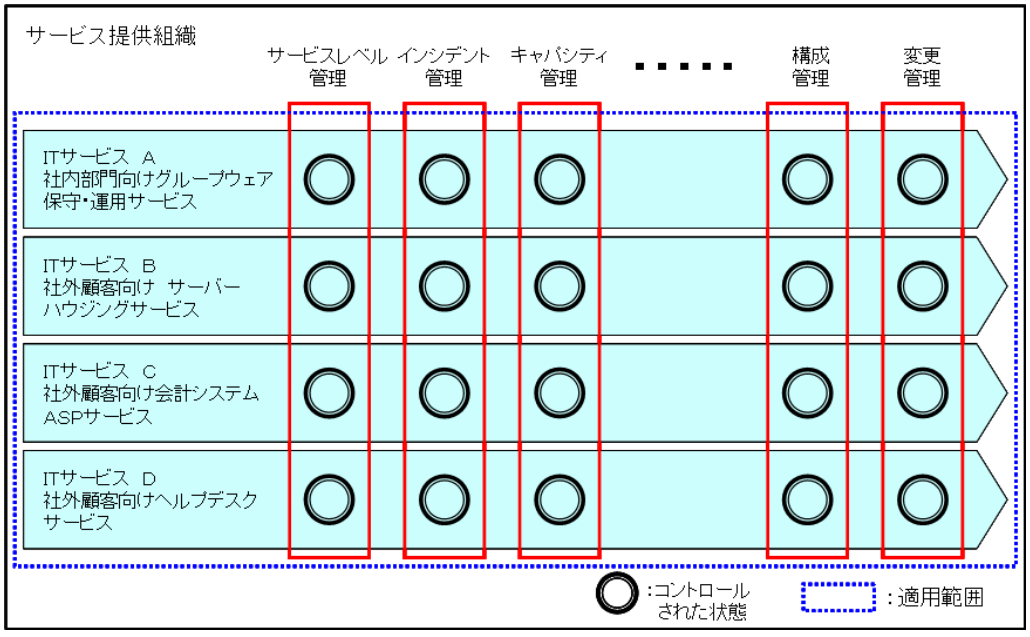


図 3-5　ITSMS 適用の理想型

しかし、適用となる対象や範囲が大きければ大きい程、サービス毎の手順や方針の調整に時間

を要す可能性があることから、サービスマネジメントシステム構築の初期段階においてはある程度、対象や範囲を限定した構築を進め順次、これを成功事例として他の対象（システムやサービス）へ横展開していき、最終的にサービス提供者が提供する全てのサービスに適用範囲を拡大していくような進め方も良いのではないでしょうか。

3.2.3. 組織階層、組織関係、対象サービスの責任の所在の整理

前の 3.2.1 項では、サービスをマネジメントするために必要なプロセスとして、JIS Q 20000-1 の箇条 6 から箇条 9 に示されている全てのプロセスを実装することの必要性にふれています。この規格の適用範囲を特定するために、最初に考えなければならないことが、適用すべきサービスを決めることであり、そのサービスマネジメントがこの規格の適用を宣言できる状態とは箇条 6 から箇条 9 の全プロセスが実装されている状態であることを示しています。

ここでもう 1 つ考えなければならないことはそのプロセスを誰（どの組織）が担当しているかであり、必ずしもその組織構造は単純ではありません。

1 つの組織の中ですべてのプロセスが完結しているケースもあれば、複数の部門に跨って実装されているケースもあります。1 つのサービスをマネジメントする ITSMS が、1 つであることは基本であり、方針、目的の組織内での一本化に始まり、意思決定の構造も一元化されていなければなりません。すなわち、3.2.1 項、3.2.2 項に続く ITSMS の 3 つ目の原則は、どのように複雑な組織体であってもマネジメントシステムが 1 つでなければならないと言うことです。

図 3-5 の 1 つのサービスを取り出し、いくつかのパターンの中で“1 つのマネジメントシステム”とはどのような状態を示すかを考えて見ましょう。

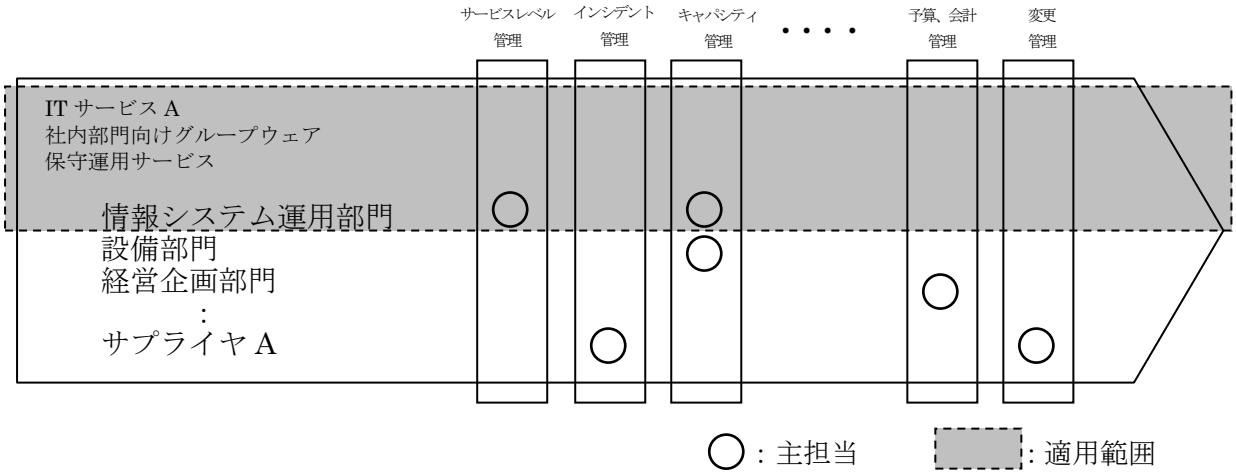


図 3-6　情報システム運用部門に JIS Q 20000-1 を適用した事例

図 3-6 は、代表的な JIS Q 20000-1 の適用事例です。

JIS Q 20000-1 を適用する組織は、インシデント及びサービス要求管理と変更管理をサプライヤ Aに委託し、また、予算・会計管理は別の部門が担当しているケースです。ITSMS のトップマネジメントは情報システム運用部門長が担い、他の部門には、その責任があるプロセスについて協力を要請し、OLA（Operational Level Agreement）が存在する場合も在ります。

この組織構造における 1 つのマネジメントが、どのような条件を満たした場合であるかと言うと、情報システム運用部門長の責任のもと、全てのプロセスがコントロールされていると言うこ

とに他なりません。ここで扱う全てのプロセスとはマネジメントシステムのプロセスも含む箇条 4 から箇条 9 全てを対象としています。情報システム運用部門長のコミットメントが、すべてのプロセスに対し影響を行使し、それに従って設備部門や経営企画部門が動き、社内に対し提供するグループウェア保守運用サービスを一連のプロセスによって適切な状況を保つことが必要です。また、情報システム運用部門以外の組織が運用する全てのプロセスの実施状況や事業上のリスクについては、情報システム運用部門の中で把握し、その責任を保有していなければなりません。ITSMS の構築範囲を最初はできるだけ小さくしたいと言う要望を良く聞きますが、他部門のプロセスの責任までも保有することは、容易ではありません。OLA のような部門間の取り決めが存在している場合を除き、1 つのサービスに関わる社内の組織については、機能的に関わる範囲（部門または個人）を特定し、必要な範囲として含むことをお勧めします（図 3-7 参照）。

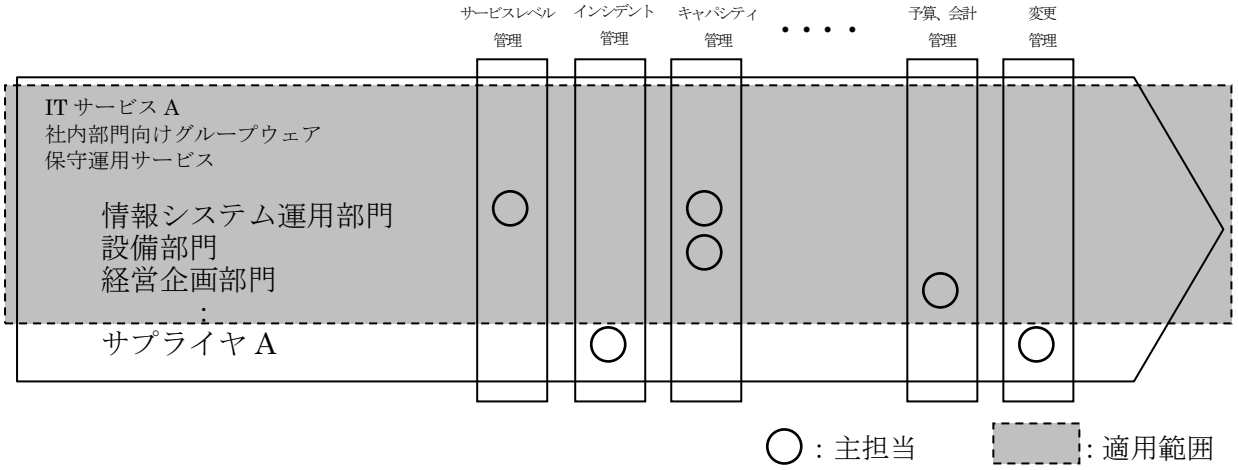


図 3-7　機能的に関わる範囲（部門または個人）を特定し、JIS Q 20000-1 を適用した事例

サプライヤAについては、別企業であり、業務を遂行する上での企業理念などは必ずしも同じではなく、1 つのマネジメントの中に組み入れるには困難な場合が多くあります。しかし、委託元のサービスをマネジメントする上で不可欠と考え、また要求事項と報告の流れを、内部インタフェースと同様に見立てて含むケースも考えられます。このような場合、サプライヤAは企業としての独立性を宣言すべきではありませんが、組織の 1 機能として組み入れることは十分考えられます。（グループ認証）（図 3-8 参照）

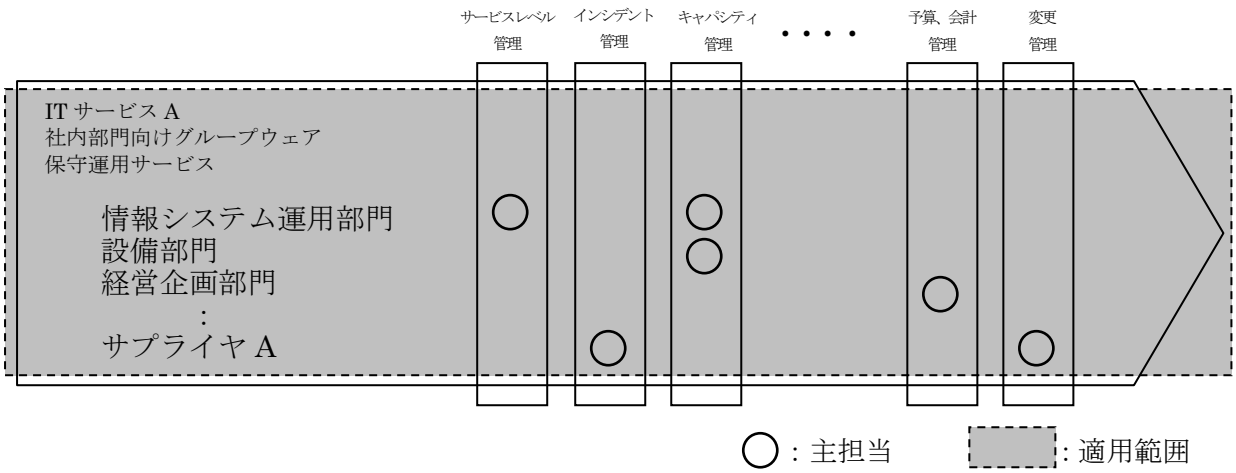


図 3-8　サプライヤAを組織の 1 機能として組み入れた事例（グループ認証）

図 3-9 の場合は情報システム運用部門とサプライヤAとの間に契約が存在し、インシデント及びサービス要求管理と変更管理のみを情報システム運用部門に対し提供しています。一見、“社内部門向けグループウェア保守運用サービス”の一部を担い、直接委託先のある部門にサービスをしているかのように見えますが、サプライヤAはあくまでも情報システム運用部門に対しサービスを行っているにすぎません。インシデント及びサービス要求管理と変更管理については委託先のある部門に対する管理責任が情報システム運用部門側にあり、“社内部門向けグループウェア保守運用サービス”についてサプライヤA が JIS Q 20000-1 の適用を宣言することは適切ではありません。但し、インシデント及びサービス要求管理と変更管理を、情報システム運用部門に対して行う 1 つのサービスとして、取り交わされた SLA に従い、全ての ITSMS のプロセスをインシデント及びサービス要求管理と変更管理サービスのレベルを保証するために駆使するのであれば、インシデント及びサービス要求管理と変更管理のための ITSMS として宣言は可能です。

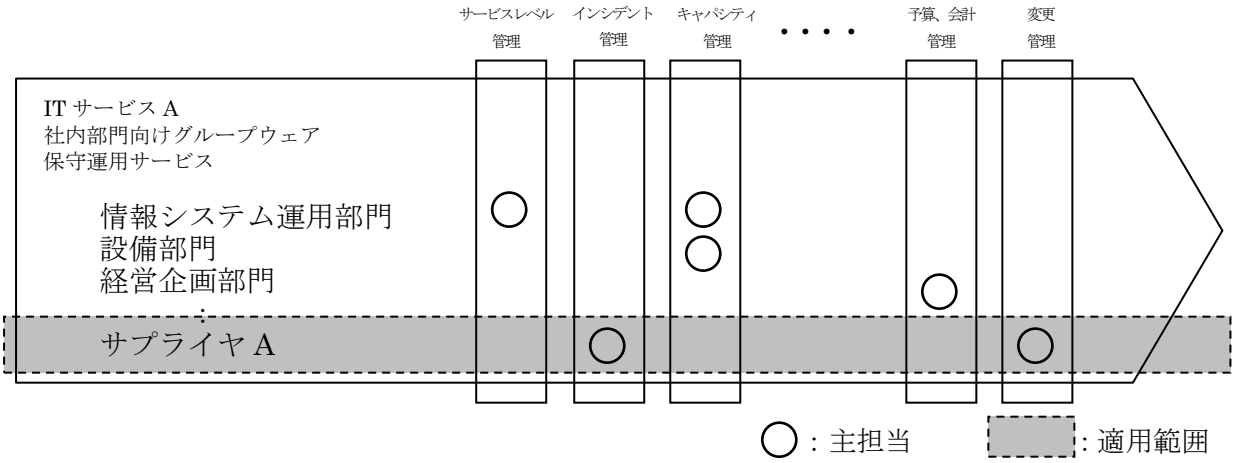


図 3-9　サプライヤに JIS Q 20000-1 を適用した事例

3.2 章は、適用範囲設定時の原則的な考え方について記載しました。3.3 章の適用範囲に関する事例解説を読むに当たっては、上記解説を参照ください。

3.3. 適用範囲に関する事例解説

3.3.1. データセンタ事業者における適用範囲設定

データセンタ事業者（情報システムの運用業務やサービスを受託する企業等）は、規格の要求事項に相当する業務やプロセスが既に存在していることも多く、あるいは適合しやすい業務があり、JIS Q 20000 との親和性の高い業態であると考えられます。

また、第三者認証取得を公表することにより、自らの組織の管理態勢やサービスレベル及びサービス品質などが、顧客やマーケットに対するアピール材料のひとつになります。その点においては、データセンタ事業者は JIS Q 20000 の認証制度を活用することが有効であると言えます。

一方で、データセンタ事業者は、多くの顧客に対して各種のサービスを提供し、複数のデータセンタ拠点を運営していることもあり、適用範囲を設定する際には検討が必要です。

a）対象となるサービス

データセンタ事業者は、多種多様なサービスを提供しており、様々なサービスの呼称があります。データセンタ施設・設備・電力資源等を提供するコロケーション（ハウジング）、データセンタの所有するサーバ機器等を提供するホスティング及びそれに関連する各種保守・監視サービスなどがあります。個別のオプションなどもサービスとして用意されている場合もあるでしょう。データセンタ事業者が提供するサービスは、多くの場合、JIS Q 20000 における IT サービス（注：規格上は「サービス」）として捉えることができます。

しかし、情報システムの運用設計等に関するコンサルティングサービスや、PC 利用についてのヘルプデスクサービス、情報システムの導入を請負うサービスを提供している場合、それらのみを対象とすることは、JIS Q 20000 における各管理プロセスを整備するうえで規格要求事項の解釈に無理が生じます。その場合は認証適用範囲を見直すべきです。

b）顧客とサービス提供者の位置づけ

規格を解釈するうえでは、どのような組織を「顧客」として位置付けるかが重要になります。認証取得を目指す組織は「顧客」と SLA について合意しなければなりませんし、サービスレビューなどを実施しなければなりません。

データセンタ事業者は、基本的には受託事業ですので、委託元が顧客に該当します。IT サービスの利用者（エンドユーザ）や委託元にとっての顧客を想定するなど、複雑に考える必要はありません。

また、認証取得を検討する組織によっては、「○○株式会社向け XX システムの運用・保守サービス」のように、特定の顧客向けのサービスのみを適用範囲とすることも考えられますが、特に問題はありません。

c）認証取得の取組みにおける留意事項

データセンタ事業者は、数多くの企業等に対してサービス提供していることが想定されます。一部の顧客のみとは合意された SLA により運用されているが、他の顧客に対しては契約書やサー

ビス標準約款などは存在していても、いわゆる「サービスレベル合意書」として詳細な性能表示やペナルティなどを記載した書面はないという場合もあります。このような場合、規格要求事項には顧客との合意事項については具体的な定めはありませんので、何を SLA として位置付けるかを見極め、組織として定義することが重要です。

同様に、顧客とのサービスレビューは、すべての顧客とあらかじめ定めた間隔でレビューするのは不可能という場合もありますが、顧客ごとにログインできる専用の Web サイトを設け、稼働状況や障害対応結果等を報告している好事例もあります。

3.3.2. 企業等の IT 部門及びシステム子会社における適用範囲設定

企業等における IT 部門（以下、「IT 部門」）は、当該組織内のユーザが利用する情報システムの運用・保守などを行っています。この場合は、情報システムの仕様を決定するとか、主に利用する部門（以下、「オーナー部門」）に対するサービス提供として捉えることができます。また、IT 部門の機能を別会社（以下、「システム子会社」）としていることもあります。この場合は親会社に対するサービス提供と捉えることができます。このように、広く一般から受託するようなサービス提供者ではなくとも、ある組織に対して IT サービスを提供し、その品質の維持・向上を実践する組織は、JIS Q 20000 の認証取得に対して効果的に取組むことができます。

IT 部門やシステム子会社の多くは、自らの業務を「サービス」として捉える文化や習慣がなく、どのような単位をサービスとして捉えるべきか悩ましいところです。認証取得の活動を機に、サービスとして再認識することにより、その品質維持・向上に寄与することでしょう。また、前述のデータセンタ事業者など外部のサービス提供者と比較した場合、親会社やオーナー部門と直接的かつ緊密な関係を維持できます。このことからも、「顧客」の事業に大きく貢献する効果的な IT サービスマネジメントの実践が可能であると言えます。

a）対象となるサービス

IT 部門及びシステム子会社などは、情報システムの企画・開発業務から運用・保守まで、幅広く業務を行っていることが考えられます。しかし、JIS Q 20000 及びそのベースとなっている ITIL においては、運用・保守を IT サービスとして捉えていることから、基本的には運用・保守を適用範囲とし、自らの IT サービスを定義するのがよいでしょう。

昨今では、IT ガバナンスや情報セキュリティの観点から、開発担当と運用担当の職務を分離することが望ましいとされています。比較的規模の大きな組織では、開発部門と運用部門とに組織が分かれていることがあり、開発部門（業務）を認証の適用範囲に含めることの要否を議論されることもあります。基本的には必須ではありませんが、開発部門が IT サービスの提供においてどのような役割を担っているかを確認する必要があります。具体的には、規格要求事項の「新規サービス又はサービス変更の設計及び移行」「リリース及び展開管理」などに注意してください。

b）顧客とサービス提供者の位置づけ

IT 部門は、適用範囲とする情報システムのオーナー部門を顧客として位置付け、規格要求事項を解釈します。もちろん、実際のビジネスにおいては、その企業が販売・取引対象とする顧客（個人・法人）が存在するはずですが、規格要求事項を理解するうえでは、オーナー部門が IT サービ

スを享受する「顧客」であると捉えます。なお、定義したあるひとつのサービスに対して、当該サービスを利用する部門が複数にわたる場合、代表となる組織（主管する組織）をオーナー部門と位置付けることにより、効果的かつ効率的に対応できます。

一方、システム子会社については、親会社の IT 部門を顧客として位置付けると、規格要求事項を解釈しやすくなります。逆に、IT 部門以外のオーナー部門を顧客として考える場合、日常業務において直接的な接点が少なく、通常は IT 部門を介して業務を行っていることが多いと想定されるので、規格要求事項上の「サービスの報告」「事業関係管理」など、いくつかの要求事項においては対応に注意が必要です。

但し、最近では EUC システムなど、オーナー部門が直接的にシステム子会社に運用・保守業務を委託し、IT 部門が全く介在しないケースなどもあります。このような情報システム（IT サービス）を適用範囲とする場合もありますので、必ずしも一概には言えません。組織形態やサービス提供形態に適した定義が必要となります。

c）認証取得の取組みにおける留意事項

IT 部門が認証取得を目指す場合は、特にサービスレベル管理に注意が必要です。「顧客」とは同じ企業内であるため、基本的には契約行為はなく、サービスレベルを定めた合意文書がないことが考えられます。このような場合、新たに SLA に相当する文書を作成することが必要となります。但し、最初から厳格かつ詳細な SLA を用いる必要はありません。優先順位の高いいくつかの目標のみを簡潔に定めるのがよいでしょう。

この点は、システム子会社の場合もほぼ同様です。受託業務全体の包括的な委託契約書は存在するものの、サービスレベル目標などは設定していないケースが考えられます。認証取得の取組みを機に、親会社（顧客）との関係を見直す、または然るべき目標を設定する良い機会として検討するのがよいでしょう。

いずれの場合も、合意した何らかの記録は必要となりますので、責任者の捺印やサインまでは必須ではありませんが、ミーティングを開催するような場合は議事録作成が望まれます。

また、上述の内容に関連し、「サービスの予算業務及び会計業務」についても注意が必要です。規格要求事項では、すべてのコンポーネントのための予算業務及び会計業務、間接費の配賦及び直接費の割当て等についての明確な方針やプロセスを備えることを求めています。特に、間接費については明確な配賦方針が設定しにくい場合があります。適用範囲を定義する際に、配賦方針を明確にしやすい IT サービスの選定なども適用範囲検討のポイントとなります（なお、規格の注記にあるとおり、顧客に対して実際に課金することまでは求めていません）。

3.3.3. コールセンタ事業者における適用範囲設定

a）対象となるサービス

まずコールセンタ事業者が JIS Q 20000-1 を適用する場合の標準的な考え方について考えてみましょう。

○○コールセンターサービス(株)は CTI（Computer Telephony Integration）システムを活用してホテルの予約サービスを提供している事業者です。このようなケースにおいては、「ホテルの予約サービス」そのものを IT サービスと呼ぶには少々抵抗があるので、ホテルの予約サービスを支える

「CTI システムの保守・運用サービス及びその IT ヘルプデスクサービス」を IT サービスと設定すると効果的な IT サービスマネジメントシステムが構築できると思われます。

b）顧客とサービス提供者の位置づけ

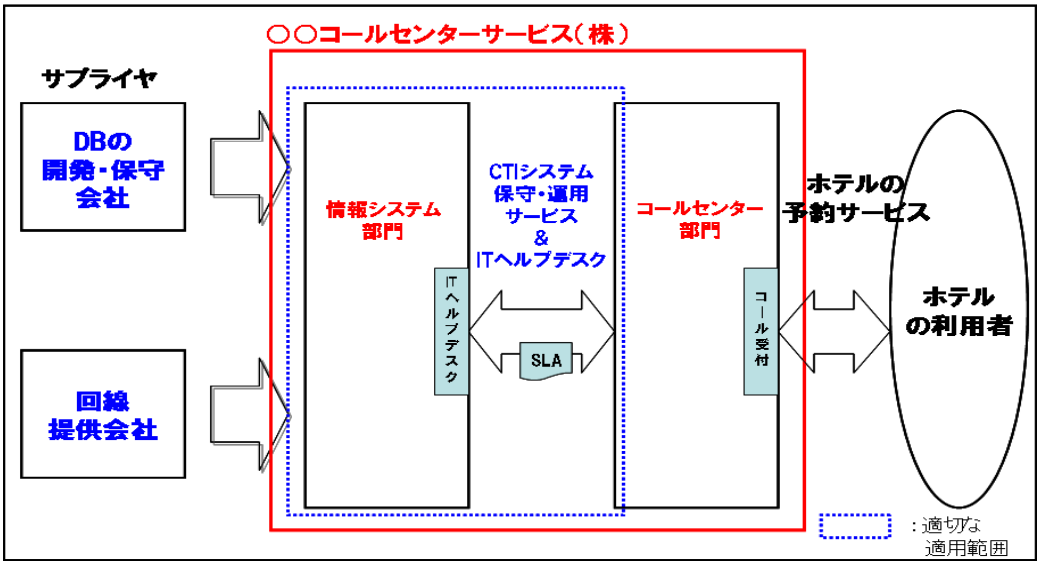


図 3-10　○○コールセンターサービス社の適用事例

図 3-10 に示すようなコールセンタ事業者が JIS Q 20000-1 を適用する場合には、以下のような適用範囲の考え方がスタンダードと言えるでしょう。

【適用範囲の記述例】
『東京都○○○区』に所在する、『○○コールセンターサービス(株)の情報システム部門』が『社内コールセンタ部門』向け『CTI システムの保守・運用サービス及びその IT ヘルプデスクサービス』の提供をサポートするための、IT サービスマネジメントシステムを適用範囲とする。

このような適用範囲を設定した場合に、CTI システムが安定稼動することによって、結果として○○コールセンターサービス(株)の本業であるホテルの予約サービスの品質の向上につながるという考え方となります。

c）認証取得の取組みにおける留意事項
図 3-11 に示すようなケースでは注意が必要です。

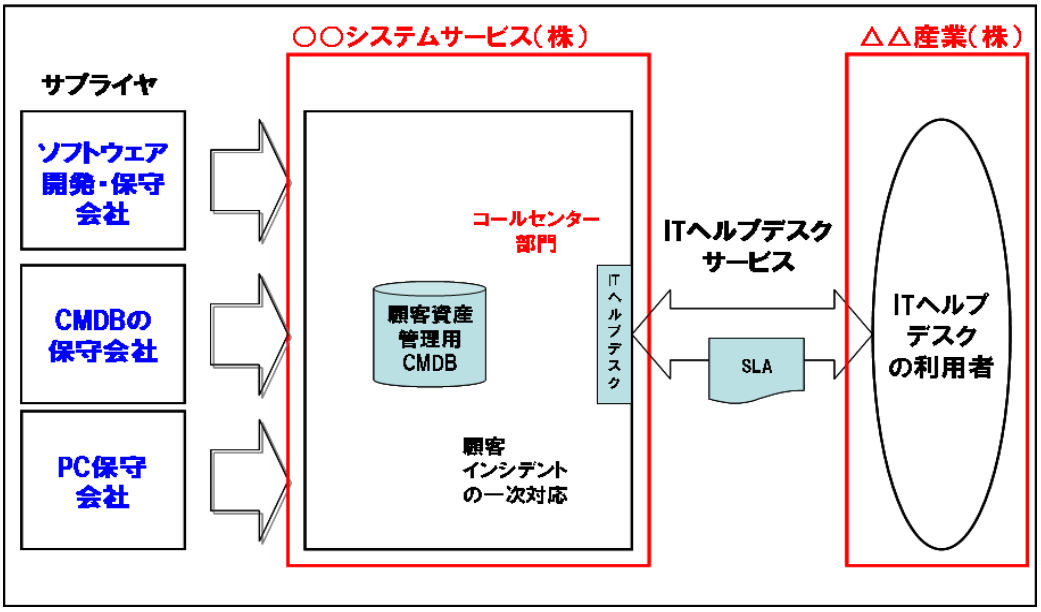


図 3-11　○○システムサービス社の提供サービス

図 3-11 に示す、○○システムサービス(株)は CMDB を利用して△△産業(株)という顧客の IT 資産を管理し、その IT 資産、例えばパソコンやサーバ、ソフトウェアなどの操作支援・故障対応・保守業者の手配などをサービスとして提供している IT ヘルプデスク事業者です。

このようなケースにおいて「△△産業(株)向け IT ヘルプデスクサービス」を JIS Q 20000-1 における IT サービスとして設定することが適切なのでしょうか。客観的に見るとこの「△△産業(株)向け IT ヘルプデスクサービス」は△△産業(株)の IT 資産に関わるインシデント及びサービス要求管理、問題管理や構成管理、加えて IT ヘルプデスクサービスに関するサービスレベル管理等が実装されているだけで、例えば IT ヘルプデスクサービスにおける容量・能力管理やリリース及び展開管理プロセスで扱う対象は何になるのか、コントロール権限を持った変更管理プロセスの活動が存在するのかなど、幾つかの疑問が残ります。

JIS Q 20000-1 では規格要求事項を原則として全て満たし、且つコントロールされた状態で各管理プロセスが活動されていることが必須です。だからといって、無理やり要求事項を満たすために一貫性を持たない管理対象を設定（例えばインシデント及びサービス要求管理は IT ヘルプデスクで受け付ける顧客 IT 資産に関するもので、容量・能力管理や変更管理の対象は○○システムサービス(株)が保有する CMDB を対象とするなど）することやそもそもサービスの特性上、活動自体必要としない管理プロセスを実装することは、効果的な IT サービスマネジメントシステムの活動を阻害する可能性もあり、無駄な工数を費やす結果になりかねません。

このようなケースの場合には、規格要求事項を満たすために『SE 部門がコールセンタ部門に提供する顧客資産管理用 CMDB の運用サービス』を適用範囲として設定し認証取得に臨むことも可能ですが、認証取得に拘らないのであれば、JIS Q 20000-1 をフレームワークとして採用し、実装することでサービス品質の向上が期待できる一部の管理プロセスを ITIL（ベストプラクティス）を参考としながら、部分的に実装するという構築方法をお勧めします。但し当然、この方法では管理プロセスの部分的な実装となるので要求事項を満たすことはできず認証取得には至らないことになります。こうなると QMS における適用除外や、ISMS における附属書 A の管理策の採用要否のような考え方の採用も今後、検討の余地は大いにありそうです。

3.3.4. Web システムを利用したサービス提供者における適用範囲設定

インターネット上での情報検索、株式や各種商品などの売買、チケットの購入、予約など Web システムを利用したサービスが急増しています。このような Web システムを利用したサービス提供者も Web システムという IT を利用して顧客にサービスを提供しているわけですからデータセンタ事業者と同様に、JIS Q 20000 との親和性の高い業態であると言えます。但し、適用範囲を設定する際には、「IT サービス」と「IT を利用したサービス」という違いに注意が必要です。

a）対象となるサービス

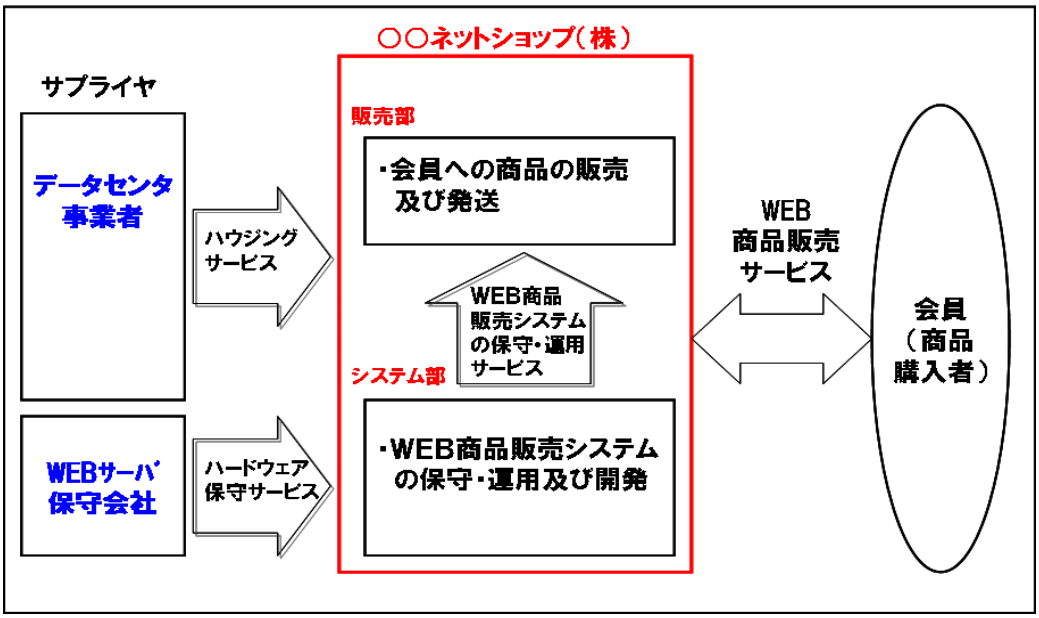


図 3-12　○○ネットショップ社の提供サービスと組織の関係

例えば、インターネット上で様々な商品の販売を行っているサービス提供者を例に、考えてみましょう。

図 3-12 に示すように○○ネットショップ(株)は、Web システムで会員登録制の商品販売を行っています。このようなケースにおいては、インターネット商品販売サービスが「IT サービス」と思われがちですが、インターネット商品販売サービスは「IT を利用した商品の販売サービス」と考え、適用範囲設定における対象となるサービスとしては、○○ネットショップ(株)システム部が提供する Web 商品販売システムの運用・保守サービスと設定するべきでしょう。

b）顧客とサービス提供者の位置づけ

○○ネットショップ(株)のケースにおいては、認証の適用範囲決定における「顧客」の設定には 2 通りの考え方があると思われます。1 つは「顧客」を○○ネットショップ(株)の販売部とし、会員を「システム利用者あるいはエンドユーザ」とするケースです。

もう 1 つは「顧客＝システム利用者」と捉えるケースです。すなわち「会員」を「顧客」と設定します。会員はサービス利用に関して会員登録（一種の契約行為が成立している）を行っていることから顧客とも位置づけることが出来ます。

本書 3.3.1　b)でも述べたように認証取得を目指す組織は「顧客」と SLA について合意しなければなりませんし、サービスレビューなどを実施しなければなりません。1 つ目のケースであれば、

顧客である販売部とサービス提供者であるシステム部が SLA について合意し両者でサービスレビューを実施すれば良いという、いたってシンプルな考え方ができます。2 つ目のケースでは顧客、すなわち会員は多数の個人であることが想定され SLA についての合意やサービスレビューの実施方法など、幾つか考慮すべき事項が発生します。

どちらを選択しても良いと思いますが、顧客をどのように設定するかは、認証取得を目指す組織の戦略やサービスの性質などを十分に考慮し決定することをお勧めします。

c）認証取得の取組みにおける留意事項

Web システムを利用したサービスは多種多様であり、一般的な考え方として顧客が不特定多数の個人であるケースが多く見受けられます。認証取得の適用範囲設定において顧客を不特定多数と設定しなければならないケースもあります。JIS Q 20000 では顧客が法人か個人か、単一か複数か、ということは問いませんが、顧客が不特定多数の場合には、サービスレベルの合意やサービスレビューの方法、インシデントのクローズ、顧客満足の調査など、留意が必要です。顧客は可能な限り特定することをお勧めします。

3.3.5. 人材提供事業における適用範囲設定

人材提供事業については、大きく分けて2つのパターンが存在します。一つは、派遣事業で、もう1つは請負により行われる事業です。請負とは、労働の結果としての仕事の完成を目的とするもの（民法632条）で、派遣事業との違いは「労働者派遣事業と請負により行われる事業との区分に関する基準」（昭和61年労働省告示37号）に定められているように、請負は、業務の遂行に関する指示その他の管理を自ら行うなどの特徴を有しています。

一方、派遣事業は、業務の遂行に関する指示その他の管理を発注者側が行うもので、JIS Q 20000-1の適用は発注者側が行うべきものであることは、疑う余地はありません。

ここでは、お客様の情報システムの運用業務を、そこに常駐し請け負っている組織が、JIS Q 20000-1の第三者認証取得を目指されているケースについて述べます。

a） 対象となるサービス

情報システムの運用業務そのものは、JIS Q 20000-1との親和性が非常に高い業態ですが、その一方で業務請負の仕方によっては、JIS Q 20000-1の要求事項に適さない場合もあり注意が必要です。人材派遣については、その指揮命令系統が発注者側にあるため、派遣事業主が、客先で行う業務についてJIS Q 20000-1の第三者認証を取得することが困難であることは先に述べた通りです。お客様の情報システムの運用業務を、請負っている場合に限り、自らの業務遂行のマネジメントをJIS Q 20000-1でマネジメントすることの意義があります。

b） 顧客とサービス提供者の位置づけ

お客様の情報システムの運用業務を、常駐し、請負っている場合の例を一つ挙げると、お客様が情報システムを保有し、障害対応やバックアップ、システムのアップデートなどの保守作業を協力会社（第三者認証の対象組織）に委託し、SLAに記載されたサービスレベルを要求する場合が考えられます。協力会社は情報システムこそ自分たちの資産ではありませんが、運用業務については、

JIS Q 20000-1に記載された全てのプロセスの責任を保有していることで、JIS Q 20000-1への適合を宣言する価値が生まれてきます。ちなみに、お客様と協力会社の関係が、親会社とシステム子会社の場合であれば、本ガイドの3.3.2項を参照することができます。

c) 認証取得の取組みにおける留意事項

お客様の情報システムの運用業務を、請負っている組織が、第三者認証取得を目指す上で、留意しなければならない事があります。JIS Q 20000-1は、要求された全てのプロセスを箇条4のマネジメントシステムの管理下に置き、箇条5から箇条9で扱われているサービスマネジメントのプロセスをバランスよく計画、実施、監視、見直しする中で、常に最適なバランスを維持するために改善を行う、いわゆるP-D-C-Aのサイクルを回すことを目的としています。

プロセス同士は、運用上起こり得るさまざまな事象に対処するため、強い関係を有しています。一つのプロセスに変化が生じれば他のプロセスとも影響しあい、最適なバランスを常に維持しようとするため、もし、影響を及ぼす先のプロセスが存在しない或いは、プロセスに対する責任を保有していなければ、PDCAサイクルを回す上で、ITSMSの効果を発揮できないことにつながります。例えば変更管理については全てお客様先で行い、インシデントが発生しても常駐し、作業を請負う組織側では、何の影響も行使できない場合があります。その他にも「サービスの予算業務及び会計業務」、「インシデント及びサービス要求管理」、「問題管理」、「構成管理」などは、同様のケースを良く見かけます。仮に、それらの情報の管理をお客様側で実施している場合であっても、サービスを請負う組織側で情報を利用できたり、分析したり、必要に応じてプロセスに修正をかけるなどの責任を保有できていなければなりません。お客様の情報システムの運用業務を、請負っている組織が、第三者認証取得を目指す上では、このようなことに留意する必要が在ります。

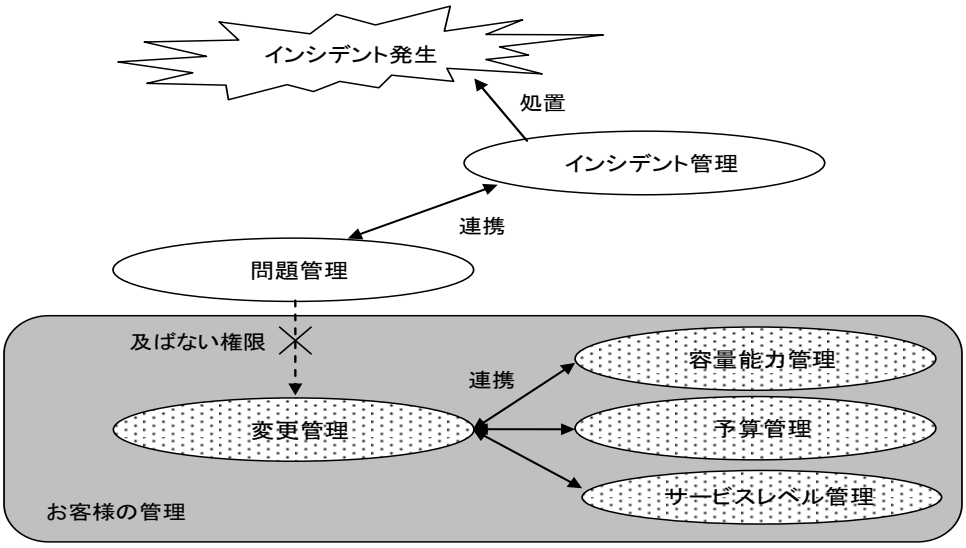


図 3-13　お客様先が変更管理を行い、インシデント対応時、請負組織の管理が及ばない事例

3.3.6.　ソフトウェアハウス

ソフトウェアを開発している組織が、JIS Q 20000-1 の第三者認証取得を希望する場合、ソフトウェアの開発そのものをマネジメントするために JIS Q 20000-1 を用いることはふさわしくあり

ません。開発プロジェクトのマネジメントであれば、JIS Q 9001 や CMM、CMMI のような他の規格の適用をお勧めします。ソフトウェアを開発している組織の JIS Q 20000-1 の適用についても、他の産業分野で適用を考慮するのと同様に、IT サービスマネジメントの範囲に限定されることを理解しなければなりません。

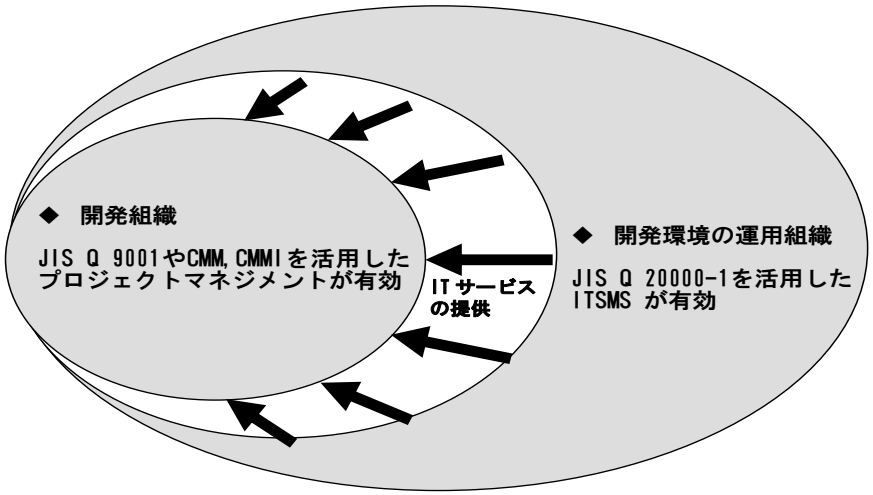


図 3-14　ソフトウェアを開発している組織の JIS Q 20000-1 の適用イメージ

a) 対象となるサービス

ソフトウェアを開発している組織が、JIS Q 20000-1 でマネジメントすべき IT サービスが何であるかについては、ソフトウェアの開発と IT インフラとの関わりを考えることが重要です。ソフトウェアの開発も、CAD などの開発環境、テスト環境の運用・保守やライブラリの管理、バックアップ、リリースなど多くの IT サービスに支えられています。その関係において、ソフトウェアを開発するプロセスへの IT サービスの可用性や継続性への影響を考慮して、どのサービスを対象として JIS Q 20000-1 を適用するかを決めることが重要です。

b) 顧客とサービス提供者の位置づけ

ソフトウェアを開発している組織と種々の開発環境の運用・保守をしている組織を分けて考えた場合、ソフトウェアを開発している組織に対し、開発環境の運用・保守をITサービスの提供として位置づけることは、容易に理解できる内容です。基本的な考え方は、本ガイドの3.3.2項をそのまま活用することができます。

c) 認証取得の取組みにおける留意事項

認証取得の取組みにおいて留意すべき事項についても、本ガイドの 3.3.2 項と同様に、ソフトウェアを開発している組織と開発環境の運用・保守をしている組織との間には、契約行為はなく、サービスレベルを定めた合意文書がないことも考えられますが、双方の関係を見直す、または然るべき目標を設定する良い機会として、可用性や継続性への影響を考慮して検討するのがよいでしょう。また、「サービスの予算業務及び会計業務」についても同様に注意が必要です。すべてのコンポーネントのための予算業務及び会計業務、間接費の配賦及び直接費の割当て等についての明確な方針やプロセスを備えることが重要です。

3.3.7. クラウドサービス（SaaS 型）における適用範囲設定

昨今のクラウドサービスの普及にも裏付けられるように、ITは「所有」から「利用」の時代へと移り変わっています。クラウドサービスを利用する顧客（利用者）はサービスの利用により、コスト削減効果／ビジネススピードの向上／開発・導入作業の短期化／スケーラビリティの向上などの恩恵を受ける一方で、データの所在、セキュリティ、可用性・継続性、性能、採用するフレームワークや標準などが、見え難いことに対する懸念も抱いているようです。本項ではこのクラウドサービスを提供する組織がJIS Q 20000-1の第三者認証取得を目指されているケースについて述べます。

a) 対象となるサービス

本項で取扱うクラウドサービス（SaaS）とは「インターネットを経由して何らかのアプリケーション機能を提供するサービスの形態」と定義します。顧客（利用者）は、どの施設から提供しているか、どの機器の提供を受けているかについて、意識する必要がなく情報処理機器や情報処理機能を利用することのできるサービスです。まさに「ITサービス」を代表するサービス提供形態と言っても過言ではなく、JIS Q 20000-1との親和性が非常に高いサービス提供形態と言えます。

b) 顧客とサービス提供者の位置づけ

クラウドサービス（SaaS）そのものが、スコープの対象となるので、他のケースに比べれば顧客とサービス提供者の関係はシンプルだと言えます。SaaS型ではオフプレミス（組織の業務システムを、サービス提供者が提供するアプリケーションを利用し運用委託することで、サービス、活動の優先順位は、公共性や社会性、契約に基づきクラウドベンダが決定します）としてサービス提供されるケースが多く、サービス提供者がサービス全体をコントロールしやすい一方で責任も重大です。

c) 認証取得の取組みにおける留意事項

顧客はクラウドサービスに対して、データの所在、セキュリティ、可用性・継続性、性能、採用するフレームワークや標準などが見え難いことに対して不安を抱いている傾向にあるようです。サービス提供者はこの不安を払しょくするためにサービス品質の見える化や信頼性確保の表明が必要であり、その1つの方法としてJIS Q 20000-1の認証取得が大いに貢献すると考えられます。

ここでサービス提供者はサービスの性質上、アプリケーションからインフラストラクチャまでの管理を実施する必要があることから、サプライチェーンの構造は複雑化することが予測され、他の関係者が運用するプロセスのガバナンスの実証が重要となります。顧客も同一サービスでありながら法人（B to Bの形態）と個人（B to C形態）が混在するケースが考えられ、SLAの合意方法や顧客とのコミュニケーション方法など留意が必要です。

また、顧客はクラウドサービス（SaaS）に不安を抱く一方で、ビジネススピードやスケーラビリティの向上に高い期待をよせている傾向にあり、容量・能力管理の充実は不可欠と言えるでしょう。

4. ITSMS の段階的導入 ～ISO/IEC TR 20000-5 の要点～

4.1. はじめに

JIS Q 20000-1 の要求事項を満たす IT サービスマネジメントシステム（ITSMS）※1）を導入する方法についてまとめた「ISO/IEC TR 20000-5（技術報告書）」について、重要なポイントを中心に解説します。このガイド（「ISO/IEC TR 20000-5」）により、サービス提供者（サービスプロバイダ）は ITSMS の一つの導入方法を学ぶことができます。このガイドでは、ITSMS を導入するための活動に優先順位をつけ、3 つの段階に分けて導入を進める方法を紹介します。このガイドは、ITSMS を効率的に導入していく手助けとなるでしょう。

※注記の説明：

1）ISO/IEC TR 20000-5 では SMS（サービスマネジメントシステム）と表記していますが、本ユーザーズガイドの本文中では ITSMS としています。

4.2. 段階的に導入する際のポイント

JIS Q 20000-1 の要求事項に基づく ITSMS の導入は、段階的な取組みが可能です。段階的な導入は、導入時の影響範囲を極小化することにより、関係者の理解が得られやすい場合が多く、各種資源の投入も一度に多くの資源配賦を必要としなくなります（各種資源の投入も長期に分散されるため、見直しや抑制がしやすくなります）。そのほか、小規模な取組みを通じて組織内外の関係者が成功体験を得られやすい、一定期間の継続的な取組みを通じて顧客・供給者との信頼関係を築きやすいなどのメリットがあります。

段階的に導入するためには、JIS Q 20000-1 の要求事項に対する深く正しい理解と各段階の目標・目的を明確にした方針と計画が必要です。そして、各組織の状況に応じた適切なアプローチを検討しなければなりません。その際、ITSMS 及びプロセスの現在の状態だけではなく、事業上の必要性や契約上の義務、法規制などの社会的要請等を考慮して取組むことが重要です。

段階的な導入としては、JIS Q 20000-1 の要求事項を特定のサービスや特定の組織・拠点等に適用範囲を限定する場合などが考えられますが、ここでは JIS Q 20000-1 の各要求事項の成熟度や到達レベルを組織自らが設定する取組みについて述べていきます。以降、導入プロジェクトの重要ポイントと各段階の実施事項とあわせて解説していきます。

4.3. 重要ポイント１：ビジネスケースの策定

JIS Q 20000-1 の要求事項に基づく ITSMS の導入に際し、最初に事前の検討・準備を行います。具体的には、JIS Q 20000-1 の要求事項の原則、目的、及び内容等の理解、自組織のサービス及び ITSMS の概要（特徴、既存資源、要求レベル、改善計画等）の理解に努めます。さらに、ギャップ分析の実施方法、実施体制、スケジュール、費用等の検討とあわせ、段階的な導入に際しての目標設定と導入プロジェクト実行計画を立案します。特に早い段階でのマネジメントのコミットメント、各種活動と役割などを事前に確立しておくことがポイントです。ここでは、次のような検討・準備の結果が成果となるでしょう。

導入プロジェクトの検討事項　－ビジネスケース－（例）

- IT サービスマネジメントシステム導入目標
- IT サービスマネジメントシステムの適用範囲案
- サービスレベルの改善目標
- 実施事項と各段階の達成目標
- 導入による影響度・影響範囲（負荷及び資源の増減、各種変更点、ビジネスの発展、リスク、利害関係者等）
- 直接的/間接的なメリット及びデメリット
- プロジェクト体制、スケジュール、費用　　など

（出典：ISO/IEC TR 20000-5:2010）

4.4. 重要ポイント２：コミットメントと方針

JIS Q 20000-1 の要求事項に基づく ITSMS を導入する場合、一般的にはプロジェクトを組成することになります。この ITSMS 導入プロジェクトには、実施するための資源（例えば、適切な力量を持った要員、必要な調達をするための資金）が必要になります。また、利害関係者に対する協力の要請等も含む指示、命令、報告等が必要となります。したがって、ITSMS 導入の際には、適切な組織決定（例えば、稟議）を実施し、トップマネジメントの支援及びコミットメントを得た上でプロジェクトを進めることが肝要です。このような進め方をすることにより、プロジェクトの遂行に必要な資源や利害関係者の協力を得ることができます。トップマネジメントを含む、すべての利害関係者の理解を得た上でプロジェクトを進めることによって、プロジェクトの過程で生じる様々な課題（例えば、複数のタスクの中から優先順位をつける）を解決することができるようになります。

今回紹介する ITSMS 導入アプローチ方法は 3 つの段階に分けて ITSMS を実現するものです。そこには全体を通して一貫した方針（全体方針）が必要であるとともに、それぞれの段階においての方針も必要です。また、それぞれの段階の各活動における方針も必要です。これら個々の方針は全体方針に従っており、方針に矛盾がないことが大切です。ある組織で策定された方針は、その組織にとっては効果的ですが、他の組織にとっても同様であるとは限りません。自組織において何が要求されているのかを適切に理解し、方針を決定していく必要があります。

4.5. 重要ポイント３：ギャップ分析の考え方

JIS Q 20000-1 の要求事項を満たすマネジメントシステムを構築することを達成すべきゴールと考えた場合、JIS Q 20000-1 の要求事項に対して、現状のマネジメントシステムがどの程度一致しているかを分析することはゴールへ到達するための大変重要な活動です。いわゆるギャップ分析です。

このギャップ分析は様々な詳細さで行うことができます。一般的には、サービス提供者のニーズ、そのサービス提供者の顧客基盤のニーズに合わせて調整することが望ましいといえます。

ISO/IEC TR 20000-5 では、ギャップ分析する項目が以下のとおり例示されています。

a）既に確立及び導入されているマネジメントシステム。これには、それぞれの適用範囲を含む。
b）次を含む、文書及び記録の両方が存在していること及びその品質。
　1）方針
　2）プロセス文書
　3）手順
　4）サービスレベル合意書
　5）供給者契約書
　6）サービス提供者及び供給者による実際の成果（achievement）の記録
c）実際の業務慣行。
d）有用な情報をもたらすサービスレビュー、内部監査、適合性評価。
e）作業負荷の特性及び実際のサービスレベル。
f）最近の又は現在のサービス改善計画。
g）役割、責任及び権限の定義の正確さ、利用可能な要員の技能及び力量。
h）サービス提供者の（企業）文化のアセスメント。
i）構成、サービス及び／又は技術に対して計画される、あらゆる重大な変更。
j）関連する法令及び規制要求事項、並びに契約上の義務。

（出典：ISO/IEC TR 20000-5:2010）

ISO/IEC TR 20000-5 の附属書 D には、文書に関する一般的な不備が例示されていますので、参考になるでしょう。

・
・
・
h）文書の履歴の中に変更理由に関する記載がなく、又は変更の承認者に関する記録がない。
i）文書及び記録の数が過剰である。
j）文書が過度に詳細なため、読むのに時間がかかるか、又は理解しづらい。
k）非常に多くの種類の様式、構成、媒体がある。
l）計画、目的、方針、プロセス、手順、サービスレベル合意書、及びサービス記録などに関する文書で欠けているものがある。
m）プロセス及び手順に不要な派生版（variations）がある。
n）方針、プロセス及び手順が、論理的な階層構造（hierarchy）のとおりに関連していない。
0）方針、プロセス及び手順がそれぞれ重複しているか、又は SMS の重要コンポーネントが文書化されていない。
p）成果（achievements）の記録が不足しているか、不完全である。
q）現在の文書又は記録が、実際には、実態及び期待と何ら関係がない。

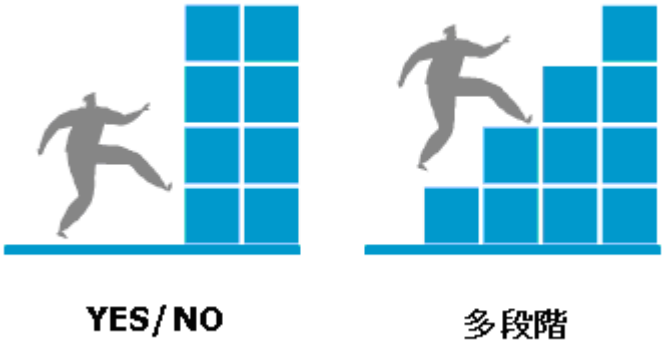
（出典：ISO/IEC TR 20000-5:2010）

また、JIS Q 20000-1 の要求事項に従ったマネジメントシステムを目指す場合は、JIS Q 20000-1 の要求事項の一つひとつそれぞれを検討するという方法も考えられます。また、要求事項とのギャップの状況を「適合している」、「適合していない」や YES/NO で判断するのではなく、ギャップの程度を複数の段階で判断するという方法もあります。段階のつけかたにはいろいろな考え方がありますが、例えば、実際に実施されているかどうかに焦点をあてて、次のように 4 つの段階にわけて評価する方法も考えられます。

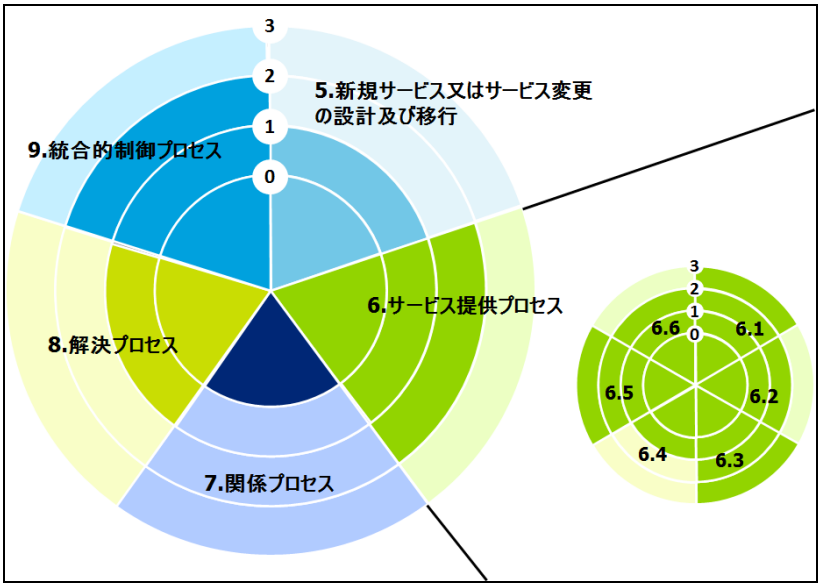
０：実施されていない。
１：一部実施されている。
２：実施されているが、正式に文書化された手続がない

３：正式に文書化された手続が存在し、実施されている。

ギャップを段階別に把握することにより適合への道筋を明確にすることができ、目標（ゴール）達成の助けとなります。



また、段階別に把握することによって、プロジェクトをより細かく管理することができ、プロジェクト成功の可能性を高めるでしょう。下記の図は、JIS Q 20000-1 の箇条 5 から箇条 9 までの達成度の段階評価のダッシュボード図の例です。要求事項ごとの達成度を集約してダッシュボードにつなげるように設計することにより、各要求事項の達成度の評価から全体感を把握することができるようになります。下図ではマネジメントの要求事項を含めていませんが、これらも段階的に把握することができます。



4.6. 重要ポイント４：導入プロジェクトのガバナンスとマネジメント

導入プロジェクトを始めるにあたり、プロジェクトチームを組成する必要があります。組織はプロジェクトが開始される前にこのプロジェクトチームの役割や権限と責任を明確にするとともに、プロジェクトリーダーを特定する必要があります。プロジェクトチームにはプロジェクトを成功に導くための強いリーダーシップが求められます。それはそのままプロジェクトリーダーにも求められます。プロジェクトリーダーには、サービスマネジメントの理解のみならずプロジェ

クトマネジメントに関する力量をもつ要員を任命することが望まれます。プロジェクトを成功させるためには、プロジェクトメンバー、とりわけプロジェクトリーダーは組織のガバナンスの原則や方針、組織文化等を理解しておくことが重要です。

プロジェクトリーダーは、プロジェクト計画を立案します。プロジェクト計画を立案する際には、プロジェクト期間、プロジェクトメンバーの力量や関与度合い、プロジェクト予算、プロジェクトリスク、他のプロジェクトとの関係、プロジェクト内外のコミュニケーション、プロジェクトの品質管理等を考慮することが重要です。プロジェクトメンバーは日常業務との兼務でプロジェクトの役割を担っている場合もあります。このような場合、プロジェクトリーダーは、プロジェクトメンバーの日常業務の負荷状況も把握し、プロジェクト計画を調整するという重要な役割を担っています。また、複数地域や多数の部署にまたがるような大規模プロジェクトの場合は、特にコミュニケーション等に留意し、プロジェクトを進めることが肝要となります。

4.7. 段階的導入の例

IT サービス提供者が、効果的に段階的な取組みをするために、ここでは、ISO/IEC TR 20000-5 に基づき、段階的な取組みについて具体的な例を示し、また、各段階の目的について説明します。

まず ISO/IEC TR 20000-5 では、各段階の一般的な目的をつぎのように示しています。

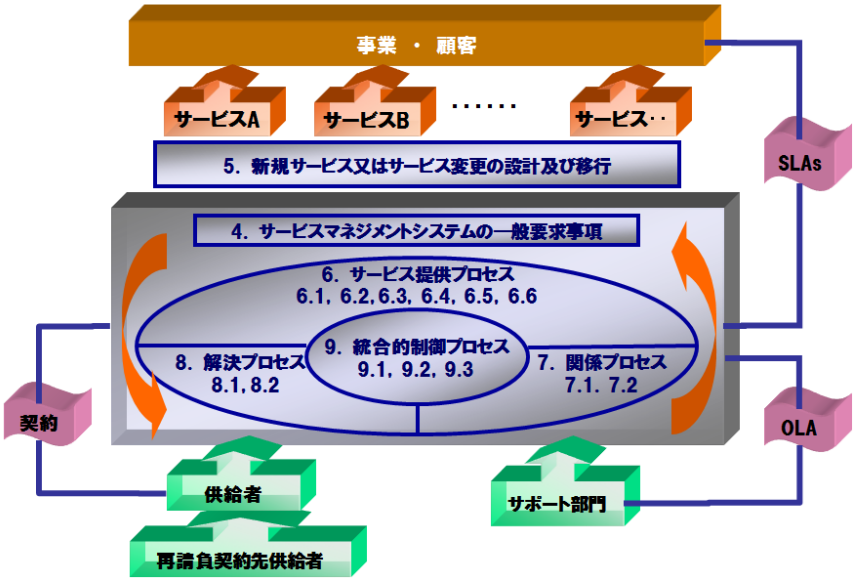
表 4-1 各段階の目的

第１段階	第２段階	第３段階
ギャップ分析の結果（findings）及びビジネスケースの取り込み。	第１段階終了時の成果分析（achievement analysis）に基づく、計画の調整。	第２段階終了時の成果分析に基づく、計画の調整。
確立・導入された SMS の構成。これには、サービスマネジメントの計画、初期方針、コミットメント／説明責任、危機管理／事後対応的プロセスを含む。	方針の改訂、追加のプロセス、既存プロセスの統合、手順、その他の支援文書。	方針の改訂、（事前対応的な）最終プロセス、すべてのプロセスの統合、基盤となる手順及び他の支援文書の文書化。
第１段階の完了時には、サービス提供者は、サービスの中断及び要求に対して迅速かつ有効に対応することに重点を置くとともに、基本的な SMS について ISO/IEC 20000-1 の要求事項を満たす、方針・プロセス・手順を導入しているようになる。サービス提供者は、すべてのサービスと関連するコンポーネントとについての知識をもち、この知識によってこうしたサービスの中断又は要求に対応できるようになる。	サービス提供者は、第２段階完了時には、サービスの中断及び要求の予測・回避を可能にする、活動・プロセス・手順・コンポーネントの管理を導入しているようになる。サービス提供者は、より信頼できるサービスを顧客に提供するために、自らのプロセス及び活動を安定化させているようになる。また、顧客のニーズを計画に組み込むために、将来のサービス要求事項について顧客との話し合いを開始しているようになる。	サービス提供者は、サービス文化を築き、かつ、顧客の事業/業務及びサービス要求事項について十分に理解を深めているようになる。また、サービスとプロセスの有効性及び効率の測定が行われるようになる（これには、顧客満足と提供したサービスの継続的改善とを含む）。サービス提供者は、供給者及び顧客の両方との取引関係を理解し、確立しているようになる。結果として、サービス提供者は、ISO/IEC 20000-1 のすべての要求事項に適合するようになる。
第１段階終了時の状況（status）の分析。	第２段階終了時の状況の分析。	第３段階終了時の状況の分析。これには、完全な内部監査を含む。また必要な場合には、ISO/IEC 20000-1 への適合のための準備を含む。
第１段階の終了までに、SMS が第２段階の基盤を提供するようになる。	第２段階の終了までに、SMS が第３段階の基盤を提供するようになる。	第３段階の終了までに、SMS が安定化のための基盤と継続的改善とを提供するようになる。

（出典：ISO/IEC TR 20000-5:2010）

上記各段階の目的を踏まえて、それぞれの段階をさらに具体的に説明いたします。各組織は、これらの例を参考に組織の活動に沿った計画を持つとよいでしょう。

JIS Q 20000-1の要求事項



JIS Q 20000-1 の要求事項では、ITSMS の構築に必要な PDCA サイクルの形成を最重要視しています。ISO/IEC TR 20000-5 では、以下のようなプロセスの導入が段階 1 から必要であるとして、記載しています。

【段階 1】

段階 1 で導入が必要なプロセス・活動：

計画（Plan）

- ITSMS の計画を確立する
- 文書化する

実行（Do）

- 導入する
- 運用及び管理する

点検（Check）

- 監視する（適切な測定システムによって）
- レビュー／監査する

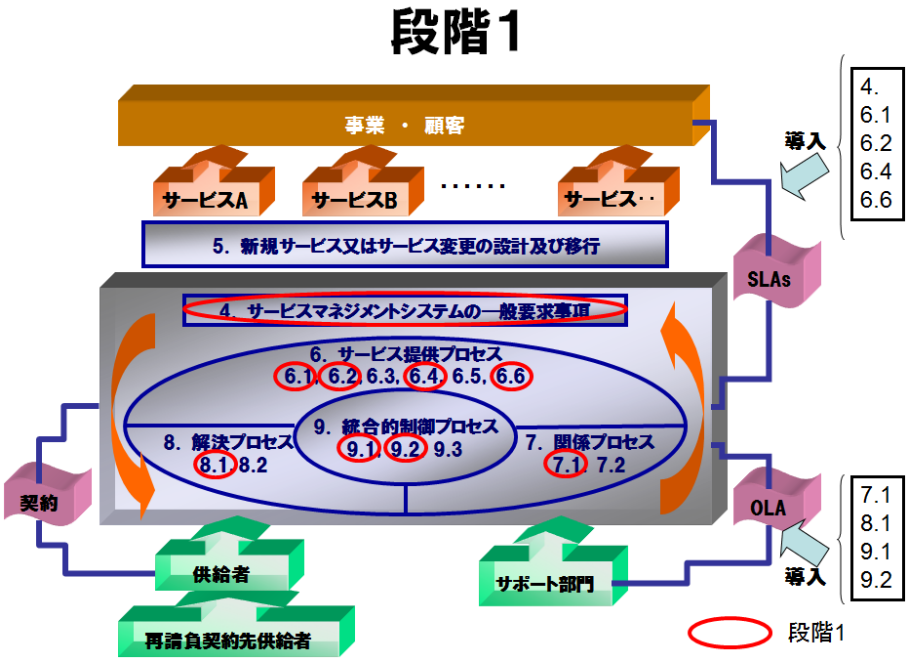
処置（Act）

- レビューによってその必要性が特定された場合には、改善する

これらは、JIS Q 20000-1 の要求事項と照らし合わせると、以下のようなプロセスを導入することになります。

- マネジメントプロセス（箇条 4　マネジメントシステムの一般要求事項）
- PDCA（箇条 4　マネジメントシステムの一般要求事項）
- サービスレベル管理（箇条 6　サービス提供プロセス（6.1））
- サービスの報告（箇条 6　サービス提供プロセス（6.2））
- サービスの予算業務及び会計業務（箇条 6　サービス提供プロセス（6.4））
- 情報セキュリティ管理（箇条 6　サービス提供プロセス（6.6））
- 事業関係管理（箇条 7　関係プロセス（7.1））
- インシデント及びサービス要求管理（箇条 8　解決プロセス（8.1））
- 構成管理（箇条 9　統合的制御プロセス（9.1））
- 変更管理（箇条 9　統合的制御プロセス（9.2））

段階 1 で注力すべきことは、IT サービスの中断及びビジネスニーズなどからの要求事項を速やかに且つ効果的に適応することです。また、これらに対応可能な方針、プロセス、手順などを確立し、関連する各々のコンポーネントについての知識を持つことが段階 1 の目的となります。



上図の〇で囲まれたプロセスが段階 1 で導入する項目です。

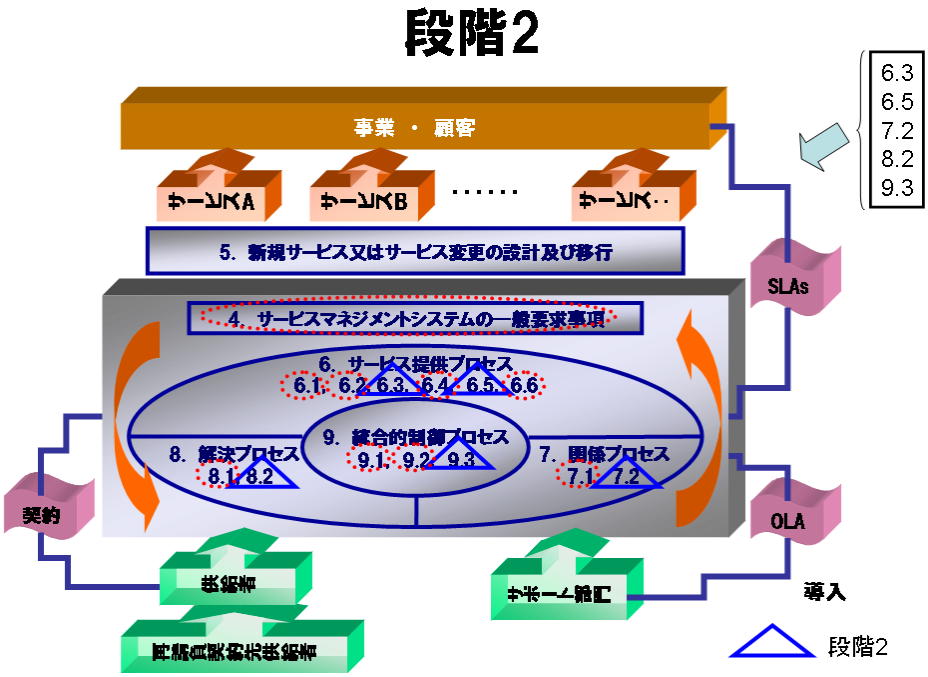
【段階２】

次に、段階２では、段階１で整った基盤に加え、IT サービスの中断を予測し、回避できる及びビジネスニーズを予測できる態勢を整えることを目指します。

段階２で導入が必要なプロセス：

- サービス継続及び可用性管理（箇条 6　サービス提供プロセス（6.3））
- 容量・能力管理（箇条 6　サービス提供プロセス（6.5））
- 供給者管理（箇条 7　関係プロセス（7.2））
- 問題管理（箇条 8　解決プロセス（8.2））
- リリース及び展開管理（箇条 9　統合的制御プロセス（9.3））

これらに対応可能な活動、プロセス、手順及び管理について確立し、より信頼性の高いサービスを顧客に提供することに注力することがポイントとなります。また、顧客のニーズを計画に組み込むためにも、将来のサービス要求事項について顧客との話し合いを開始する必要があります。



上図の△で囲まれたプロセスが段階２で導入する項目です。

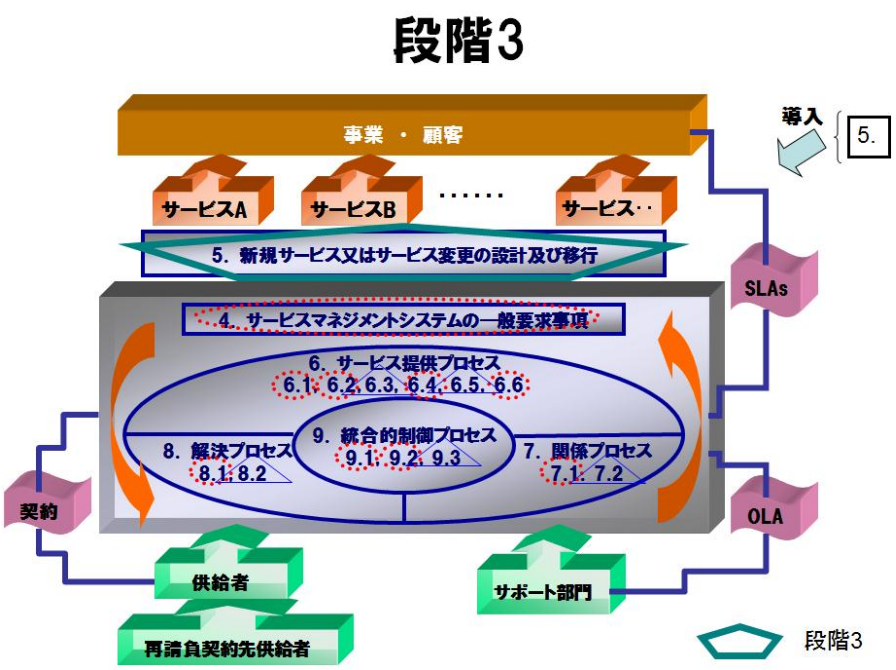
【段階３】

段階３では、段階２で整った基盤を基に、サービスとプロセスの有効性及び効率の測定が実施されることがポイントになります。また、顧客満足の向上及びサービスの継続的改善のため手法の確立に注力することになります。

段階３で導入が必要なプロセス：

- 新規サービス又はサービス変更の設計及び移行（箇条 5）

この段階においては、サービス提供者は、供給者及び顧客の両方との取引関係を理解し、確立している状況が期待されます。また、結果として、サービス提供者は、JIS Q 20000-1 のすべての要求事項に適合していることとなります。



上図の ⬠ で囲まれたプロセスが段階３で導入する項目です。

さて、ISO/IEC TR 20000-5 に記載されている事例を基に、3 段階に分けて JIS Q 20000-1 のすべての要求事項に適合していく過程について紹介しましたが、各々の段階で導入したプロセスは、次の段階に進んだときには、さらにそのプロセスを向上させる必要があることに留意してください。次の段階に進んだので、前段階のプロセスが終了したということではありません。

ISO/IEC TR 20000-5 では、ある段階で導入されたプロセスが次の段階においても継続的に活動している様子を下図のように示しています。

（出典：ISO/IEC TR 20000-5:2010）

この図は、例えば段階１で導入を始めたプロセスは、段階２、３と進むにつれ、中断することなく向上させていくことを示しています。

情報セキュリティ管理を例にとって、具体的にその内容を見ていきましょう。

前述したように段階１の目標が IT サービスの中断及びビジネスニーズなどからの要求事項を速やかに且つ効果的に適応することとした場合、段階１における情報セキュリティ管理においては、まず情報セキュリティ基本方針を策定し、IT サービス中断などに対応するための役割、責任などを明確にし、IT サービス提供者、顧客及び供給者の該当する要員全員に伝達し、同意を得る、などのプロセス、手順などを確立することになります。

段階２になりますと、IT サービスの中断を予測し、回避できる態勢及びビジネスニーズを予測できる態勢を整えることが目標になりますので、段階２における情報セキュリティ管理では、IT サービスの中断を引き起こす脅威やぜい弱性を識別し、リスク分析・評価などを確実に実施し、予防、検知、復旧などのために必要な対策を施すことが期待されます。

さらに段階３においては、段階２で投じた管理策や情報セキュリティ管理体制などを改善するために内部監査や専門家などによる監査や助言を受け、同意した改善項目を確実に実施し、情報セキュリティ管理を向上させることが期待されます。

ISO/IEC TR 20000-5　附属書 B　では、各々の活動、例えば情報セキュリティ管理について段

階１～３においてどのような活動が必要であるかを下表のように纏めてありますので、参考にされるとよいでしょう。

活動	段階			責任
	1	2	3	
情報セキュリティ管理				
a)セキュリティ方針及び管理策の導入ための、情報セキュリティ管理の目的及び計画が合意される。	・			プロジェクト（又はチームメンバー）
b)サービス提供者、顧客及び供給者の該当する要員全員に、情報セキュリティの要求事項が伝達されている。	・	・	・	
c)情報セキュリティリスクのアセスメント基準及びリスクの受容可能なレベルについて合意されている。	・	・		
d)情報セキュリティのリスクアセスメントが定期的に実施される。		・	・	セキュリティ管理
e)情報セキュリティ内部監査が実施され、結果がレビューされ、特定された改善が記録、合意、及び実施される。			・	
f)情報セキュリティ関連のリスクの管理のために導入及び運用されている適切な情報セキュリティ管理策が、情報セキュリティ基本方針の要求事項を満たす。		・	・	プロジェクト（又はチームメンバー）セキュリティ管理

（出典：ISO/IEC TR 20000-5:2010）

この表には、各々の段階で実施すべく活動内容とその活動に係る責任者の例が記載されています。

4.8. 導入後のポイント

段階的取組みを実施した場合においても、JIS Q 20000-1 の導入後に、要求事項が継続的に満たされることを確実にする必要があります。

4.8.1. ITSMS のガバナンスの維持及びサービスの改善

JIS Q 20000-1 の要求事項が引き続き満たされていることを確実にするための一つの方法は、ガバナンスの維持と継続的改善に対するコミットメントを確実にすることです。また、継続的な改善の対象には、ITSMS、提供したサービスなどにおいて、改善に必要なあらゆるプロジェクトが含まれます。従って、組織の ITSMS におけるガバナンスを維持し、継続的な改善を実施していくことが、ポイントとなります。また、そのための具体的な方法として、利害関係者のグループを任命することが挙げられます。このグループには、ITSMS を用いて提供するサービスに対する説明責任をもつ上級管理者とプロセス管理責任者及びサービス管理責任者などを含め、提案されたサービスの改善要求に対して、リスクや影響（他のグループへの影響なども含まれる）、事業損益などをアセスメント（評価）することが期待されます。

4.8.2. Plan-Do-Check-Act

JIS Q 20000-1 の導入後、最も重要な活動の一つは、JIS Q 20000-1 に規定された Plan-Do-Check-Act の適用からもたらされる、継続的改善のサイクルを維持することです。このことは、JIS Q 20000-1 の要求事項を継続して満たしていることを、サービス提供者がどのようにして確実にするのかという活動でもあります。

JIS Q 20000-1 の要求事項を引き続き満たすことを確実にするためには、次の活動を継続的に行い、強化していくことが重要です。

a）サービス及びプロセスのパフォーマンスの監視
b）内部監査及びマネジメントレビュー
c）サービス及びプロセスの改善

4.8.3. 新規サービス及びサービスの変更のためのプロジェクトとのインタフェース

サービス提供者は、新規または変更するサービスのための計画や展開が要求される基準を維持していることを確実にする必要があります。そのため、サービス提供者は、顧客の事業計画に対する変更又はその他の変更で、自組織で提供するサービスと供給者又は再請負契約先供給者から受けるサービスとの両方に影響を与え得る変更に関する情報を要求することが望ましいといえます。その上で、新規サービス又はサービス変更を提案する際は、サービスの提供及び運営管理から生じるかもしれない費用、組織、技術、営業の分野への影響を考慮する必要があります。また、実際の導入に際しては正式な変更管理を通して計画し、承認されなければなりません。

4.9. まとめ

ご紹介した通り、ITSMS の構築には段階的に取組むことが可能です。ITSMS の効果的な導入には、ビジネスケースの策定やギャップ分析、組織としての方針やコミットメント、ガバナンスといった要素がポイントになります。これらのポイントを押さえて ITSMS 導入を確実なものとしましょう。

また、JIS Q 20000-1 の要求事項を満たすためには、自組織のみならず、供給者や顧客ともその関係を確立する必要があります。自組織の態勢が不十分であった場合、供給者や顧客とのより良い関係を築くことは困難です。まずは、自組織の IT サービス提供を確実にした上で、段階的に強化していきましょう。

5. ISMS ユーザのための ITSMS 入門

5.1. はじめに

ここでは、ITSMS、ISMS の両基準の異なる点、共通点について触れます。お互いの基準の目的が「IT サービスマネジメント」と「情報セキュリティマネジメント」といったように異なる以上、大きな視点（統制目標、リスク管理）から両者をみれば、異なる領域の内容になりますが、基準の中に同様な事柄を要求している箇所もあり、両基準を満たす活動をする上では、必ずしも全て異なる組織を構築しなければならないわけではありません。小さな視点（態勢、手法、手順など）については、共有可能な点もありますので、これらについての考察を行っていきます。

考察する上で、ISMS と ITSMS の関連性についての概要を図に示していきます。図 5-1 は、ISMS に適用される PDCA モデルと ITSMS の「6.1 サービスレベル管理」と「6.2 サービスの報告」プロセスを統合させたものです。ISMS は、ITSMS の「サービスレベル管理」という顧客からの期待に対する一連の情報セキュリティに係る管理を担い、その結果として、運営管理された情報セキュリティの状況を「サービスの報告」として顧客に提供することに役立ちます。

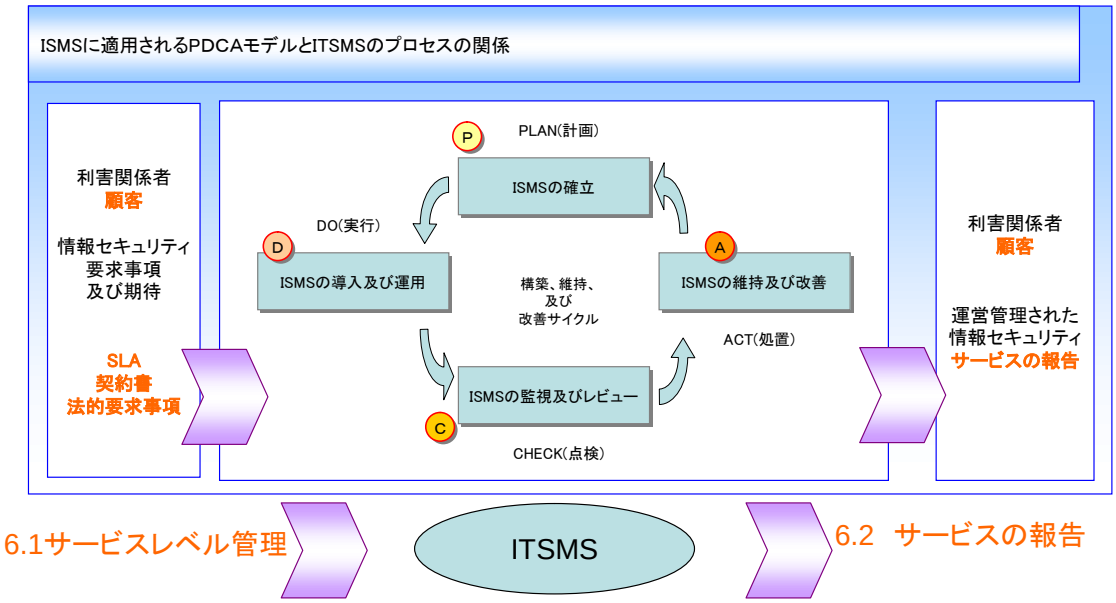


図 5-1　ISMS に適用される PDCA モデルと ITSMS のプロセスの関係

具体的には、図 5-2 に示すように組織内で多様に展開される「顧客サービス」、「販売管理サービス」等といったサービスが、「顧客」、「取引先」といった利害関係者に対し、それらの運用状況を報告する際、ISMS は、運用管理、リスク管理といった側面からそれらの活動を支援しているといえます。

このような関連性を踏まえ、次項に両基準を活用する場合の留意点について触れていきます。

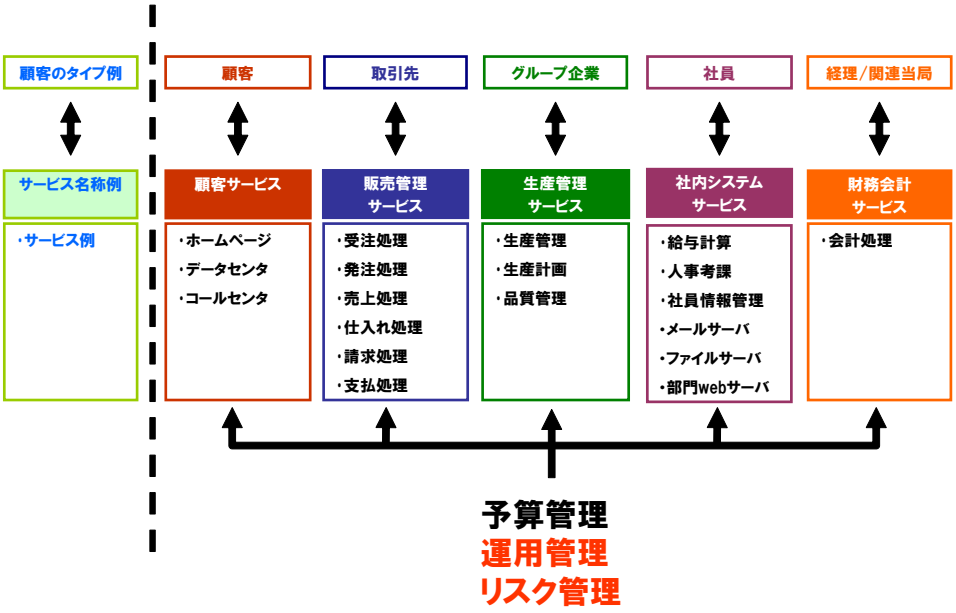


図 5-2　各サービスを「運用管理」、「リスク管理」の視点で支援する ISMS 活動

5.2.　両基準を活用する場合の留意点

ITSMS は、サービスマネジメントを主眼として考えられているため、同一組織内の複数サービスが必ずしも同じプロセス構成から成り立たない場合もあります。情報セキュリティでは、一般的に組織にとって最も弱い箇所から、そのぜい弱性が露呈し、ウィルス蔓延に繋がる事故や、個人情報の漏洩に繋がる事件が多く見受けられることから、可能な限り適用範囲を広め、組織の共有インフラとして活用することが効果的ですが、サービスマネジメントを行う場合、サービス間が独立していることも多く、その場合は個々のサービスに応じたプロセスを適切に組合せて構築していく必要があります。

従って、ISMS を構築された企業は、図 5-3 に示す図のように、ISMS 全般の内、ITSMS に関連する組織や活動を ITSMS のインフラとして位置付け、その上位に各サービスに必要なプロセスを適切に管理しながら ITSMS を構築していくことが、効果的だと考えられます。またこのことは、最終的には、ITSMS を統制するにあたり、関連する ISMS の部分を包含していくことと同意です。

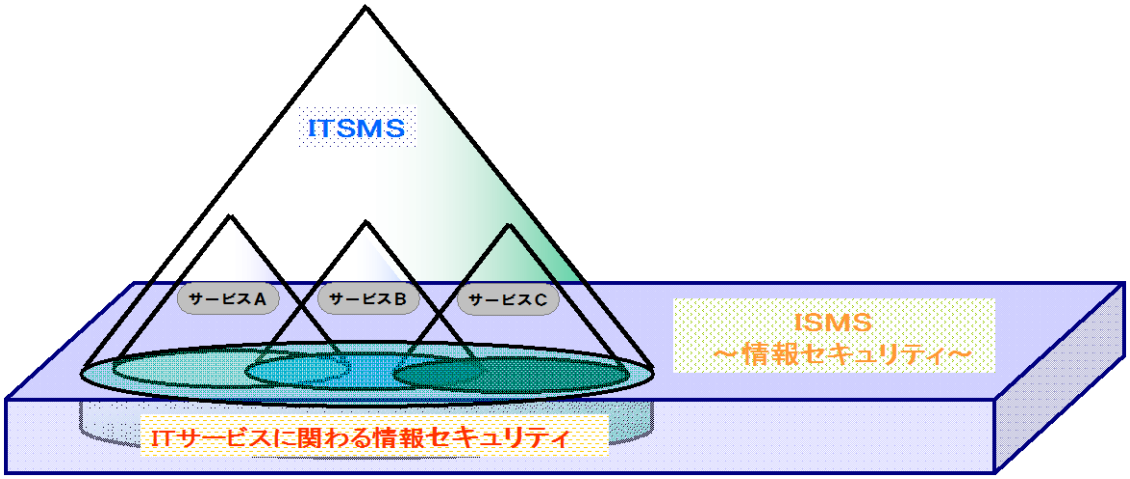


図 5-3　IT サービスの情報セキュリティ部分を担う ISMS

この視点から、ISMS を構築した組織は、ITSMS を構築する上で留意しなければならないことがあります。

【全般的な活動】

統制・管理目標の違いから、自ずと活動内容や点検業務などの頻度は異なります。

ISMS の活動ではリスク管理を中心に、識別された脅威・ぜい弱性に対し、適切な管理策を講じ、様々な視点からそれらの管理策の有効性を評価し、改善に繋げていきます。

一方、ITSMS の場合は、以下のような視点で提供するサービスに対し評価し、改善に繋げていきます。

- サービスの品質：「6.2 サービスの報告」、「8.1 インシデント及びサービス要求管理」、「8.2 問題管理」などのプロセスを展開し、評価する。
- サービスに係る費用：「6.4 サービスの予算業務及び会計業務」などのプロセスを展開し、評価する。
- リソース（資源）の運用状況：「6.5 容量・能力管理」などのプロセスを展開し、評価する。

また、改善活動などの頻度に関しても、ITSMS の PDCA サイクルの周期の方が、ISMS と比較すると早いといわれています。一概には言えませんが、ISMS では、概ね月単位で情報セキュリティに関する報告が上げられ、半期または年間に一回程度の ISMS 全体の見直しが行われることが考えられます。一方、ITSMS では、概ね週単位で IT サービスに関する報告が上げられ、月毎に利害関係者に対しサービスの報告が行われ、四半期または半期に一回程度の ITSMS 全体の見直しが行われることが考えられます。

【報告内容の開示】

ISMS では、情報セキュリティに係る内容の開示はその性質上、適用宣言書やそれと同等の比較的、抽象的な情報に留めています。一方、ITSMS の場合、サービス内容を他社との差別化に活用するためにカタログや提案書を介して積極的に展開する場合が想定されます。このような場合、情報システム部門などによって改善・向上した IT サービスに関わるパフォーマンスや品質を遅延することなく、正確に伝達することが必要と考えられます。このためには、カタログなどの版管理に加え、古い版のカタログの撤収の徹底などが効果的であると考えられます。

【組織】

ISMS の組織を活用することは、可能であると考えられます。但し、個人情報保護などを目的に ISMS を構築する組織においては、管理部門（総務、法務、情報システム等）が主体となり、各サービス部門等を指導していく場合が多く見受けられます。一方、ITSMS では、IT サービスのオーナーである各サービス部門を中心とした活動が期待されます。各サービス部門は、管理部門に対し、顧客に期待されるサービスを提供するために、様々な活動を依頼・指示し、各管理部門で検討した事項について、承認するなどの仕組みが必要になると考えられます。

【資産】

ISMS としてとらえている資産の内、特にサービスや IT（ハードウェア、ソフトウェア等）に留意して、IT サービスにおいて考慮される資産との整合を図ることが必要と考えられます。

ここで、IT サービスにおいて考慮される資産と記載しましたが、JIS Q 20000-1 では用語及び定義の中で「資産」を定義していません。これについて、ISO/IEC 27013:2012（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）では、JIS Q 20000-1 で用いられる資産は、一般的に用いられる用語の‘資産’として考えて良いとしています。一方、JIS Q 20000-1 では、‘構成品目（CI：Configuration Item）’をサービスの提供のために管理する必要がある要素として定義しており、「9.1 構成管理」において、「（CI の）原本には少なくとも、文書、ライセンス情報、ソフトウェア、及び入手可能な場合は、ハードウェア構成の配置図を含めなければならない」としています。従って、ISMS で定義付けられた‘資産’は‘構成品目（CI：Configuration Item）’に包含されることになります。

JIS Q 20000-2 では、CI の種類について、以下のように記載しています。

> 9.1.3.4　CI の種類
>
> CI の種類には，次の事項を含めることが望ましい。
>
> a) サービスカタログに記載されるサービス及びその関連情報，並びに文書（SLA，合意書，契約，サービスの要求事項，サービス設計の仕様など）
> b) ハードウェア，ソフトウェア及びライセンス，ツール，アプリケーション，文書，支援サービスなどを含むサービスコンポーネント
> c) サービス，システム，ソフトウェア構成ベースライン又は構築記述書の全ての版及びリリース。その構築記述書は，各々の構築文を適用可能な環境，及びハードウェア構成図のような標準的なハードウェア構築に対するものである。
> d) 物理的及び／又は電子的な格納庫に保管されるCIの原本，CMDB及び使用ツール
> e) 情報セキュリティ資産
> f) セキュリティが保たれた磁気媒体，機器など，財務資産管理又は事業上の理由で追跡する必要のある資産
> g) 方針，プロセス文書，手順，計画などのSMS文書
>
> 各CIの種類は，CMDB又は統合された文書若しくは記録に関連情報をもつことが望ましい。
>
> （JIS Q 20000-2:2013　9.1.3.4　CIの種類　より引用）

上記の e)　情報セキュリティ資産が、ISMS としてとらえている資産と考えることができます。その上で、ISO/IEC 27013:2012 では、一概にはいえませんが、例えば、通常のデータ送信のためのケーブルは CI に含まれるが、ISMS の資産には含まれないことがあります。同様に、要員は、ISMS の資産に含むが、CI には含まないなどの例示が記載されています。

ISO/IEC 27013 については、本章末の【参照情報】を参照してください。

【リスクアセスメント】

リスクアセスメントの手法自体を共有することは可能と考えられます。ITSMS では、リスクアセスメント手法に関する詳細な要求が記載されていないため、ISMS で利用しているリスク

アセスメント手法を基調にすることは有用であると考えられます。但し、ITSMS ではサービスに係るリスクを評価するわけですから、サービスの機密性、完全性、可用性の喪失が事業に与える影響の度合いを評価するにあたり、サービス契約の不履行、サービス中断、誤情報の配布等について、想定される被害損失額を実際の売上げや顧客数などを基に、より具体的かつ明確に（定量的に）把握しておくことが、効果的と考えられます。

JIS Q 20000-2 では、リスクアセスメントの実践について、以下のように記載しています。

6.6.3.3　リスクアセスメント

ISMプロセスは，稼働環境の情報セキュリティリスクを特定するために，定期的にリスクアセスメントを実施することが望ましく，次にそれを文書化し，特定されたリスクの影響を予防又は最小化するための具体的な管理策を実施することが望ましい。また，ISMプロセスは，新規サービス又はサービス変更の設計及び移行の一部として，適切なリスクアセスメントを行うか，又は行われることを確実にすることが望ましい。

情報セキュリティ方針は，情報セキュリティリスクアセスメントが，次のとおりであることを確実にすることが望ましい。

a) 新規サービス又はサービス変更に対するものを含めて，合意した間隔で実施される。
b) 記録し，承認された要員だけに可視的であるようにする。
c) 事業ニーズ，プロセス及び構成の変更の間も維持される。
d) サービスに影響を及ぼすものについての理解を助ける。
e) 情報セキュリティ監査に関する要求事項を定義する。
f) 運用する管理策の種類に関する決定を通知する。

情報資産のリスクは，リスクの性質及び事業に与える潜在的な影響に応じてアセスメントを行うことが望ましい。

注記　情報セキュリティの専門家としての役割を担う要員は，ISO/IEC 27005に精通していると役に立つ。

6.6.3.4　情報セキュリティリスクの管理

情報セキュリティ管理策は，サービス提供者が，サービスマネジメントの目的及びセキュリティ方針の要求事項を達成できることを確実にすることが望ましい。また，管理策は，サービス提供者が特定された全ての情報セキュリティリスクを管理できるようにすることが望ましい。

情報セキュリティ管理策の例を次に示す。

a) 情報セキュリティ方針を確立し，導入し，要員，供給者及び顧客に周知させることが望ましい。
b) 情報セキュリティ管理プロセスの権限及び責任を定義し，割り当てることが望ましい。
c) 情報セキュリティ方針の有効性を監視し，測定し，アセスメントを行うことが望ましい。
d) 重要な情報セキュリティの役割を担う要員は，情報セキュリティに関する教育・訓練を受けることが望ましい。
e) リスクアセスメント及び管理策の導入について，専門家の助けが得られるようにしておくことが望ましい。
f) 変更によって，管理策の効果的な運用が損なわれないほうがよい。
g) 情報セキュリティインシデントは，インシデント及びサービス要求管理プロセスに従って報告し，適切な優先度を割り当てられることが望ましい。
h) 情報セキュリティインシデントは，その優先度及びセキュリティインシデント記録にアクセスするために必要な権限のレベルに応じて，それを解決する権限をもつ要員への段階的取扱いをすることが望ましい。

i) 情報セキュリティインシデントの詳細は，適切な権限をもつ要員だけに可視的であるようにすることが望ましい。
j) 定期的なリスクアセスメントは，組織のリスク耐性への準備状況の変化を特定するために完了することが望ましい。
k) 定期的な監査は，確立された情報セキュリティ方針及び管理策の適合性を確認するために実施することが望ましい。
l) 情報セキュリティのベースラインは，定義され，効果的に適用されることが望ましい。
m) 情報セキュリティ監査の所見は，分析して，優先度付けされた行動計画に集約することが望ましい。
n) 情報セキュリティの教育・訓練計画及び教育・訓練記録を作成し，最新に保つことが望ましい。

サービス提供者は，サービス提供者の情報にアクセスするか又はそれを利用する外部組織とともに，情報セキュリティ管理策を特定し，文書化し，管理することを確実にするために，供給者管理プロセスと連携することが望ましい。

（JIS Q 20000-2:2013　6.6.3.3 リスクアセスメント，
6.6.3.4 情報セキュリティリスクの管理　より引用）

【リスク対応】

リスクアセスメントの結果、リスクが受容できないプロセスに対して実施するリスク対応の態勢を共有することは可能と考えられます。ITSMS では、リスク対応に関する詳細な要求が記載されていないため、ISMS で利用しているリスク対応の考え方【　1）適切な管理策の適用、2)組織の方針及びリスク受容基準を明確に満たすリスクの、意識的、かつ、客観的な受容、3)リスクの回避、4)関連する事業上のリスクの、他者（例えば、保険業者、供給者）への移転　JIS Q 27001:2006 4.2.1 f）参照　】を基調にすることは有用であると考えられます。リスクを低減するための管理策について、ITSMS では附属書などを用意していませんが、JIS Q 20000-1　6.6 情報セキュリティ管理のプロセスでは、参照する規格として、ISO/IEC 27000 ファミリー規格を挙げています。

可用性、完全性に関する管理策として、JIS Q 27002:2006 には、「10.5　バックアップ」、「12.2 業務用ソフトウェアでの正確な処理」等が特に有効であると考えられます。

一方、例えば、IT サービスの可用性を維持するためによく採用される、冗長化（例えば二重化）、負荷分散などの分野に関する対策の例示が詳細にはないため、ITSMS に必要な管理策を追加し、補完する必要があると考えられます。追加する際、ISMS の適用範囲内であれば、それらを追加の管理策として、ISMS の維持・管理にも有用であれば、追加し、適用宣言書に反映させていくと ISMS の改善に効果的と考えられます。

【リスクマネジメントの態勢】

リスクアセスメントの手法や、関連する基準（クライテリア）などを承認する組織や態勢を ISMS と共有化することは可能だと考えられます。特に、ISMS は ITSMS のリスク管理部分を担う役割を果たすので、基準などを統合し、管理することが効果的だと考えられます。但し、リスクアセスメントの手法自体に対しては、前述したように、より定量的にリスクを把握するような手法を用いる方が、サービス部門にとって効果的だと思われます。

【外部委託先管理】

特に、個人情報、機密情報保護の視点から ISMS を構築した組織の場合、外部委託先選定基準を明確にした上で委託先業者を特定し、個人情報や機密情報を取扱う外部委託先担当者を限定し、預託または委託したそれらの情報の運用に関し、アクセス制御や暗号化など情報漏えいのために必要と考えられる管理策の実施について監視する、または報告を要求する傾向があります。

一方、ITSMS の場合、サービスの継続性、可用性の視点からサービスを保護することを目的として、外部委託先管理を行うことから、コストを考慮しながら、サービス停止などの脅威に対応するために、複数の外部委託先（サービス提供者）と契約し、必要に応じて代替手段を投じていくことが考えられます。また、預託または委託したそれらの情報や運用に関し、パフォーマンスや冗長化機能、バックアップ/リスト機能など、サービスの継続性の維持のために必要と考えられる管理策の実施について監視する、または報告を要求する傾向があります。

従って、外部委託をする場合、個人情報等の機密性に係る資産なのか、サービスなどの可用性に係る資産なのかを分類し、適切な外部委託先管理をすることが重要です。情報が双方の領域にまたがることも当然ありますので、情報セキュリティ及びサービスの適切なレベルを実現し、維持するための管理策を施し、委託先やサービス提供者と契約を締結し、その内容について、SLA などを顧客と同意しておくことが必要です。

【外部委託先管理組織（法務、総務部あたりを想定）】

ITSMS の外部委託先やサービス提供者に係るリスクの考え方の違いについては、前述しましたが、それらを踏まえた上で、実際に外部委託先を管理する組織（法務、総務部あたりを想定）は、ISMS の仕組みを ITSMS で併用することは可能であると考えられます。また、情報セキュリティに関係する内容の SLA を締結する上において、JIS Q 27002:2006 の

- 6.1.5 秘密保持契約
- 6.2.1 外部組織に関係したリスクの識別
- 6.2.2 顧客対応におけるセキュリティ
- 6.2.3 第三者との契約におけるセキュリティ
- 10.2 第三者が提供するサービスの管理
- 8　人的資源のセキュリティ（契約社員などを含む）

等は、有用な情報であると考えられます。

【コンプライアンス管理組織（法務、総務部あたりを想定）】

構築するマネジメントシステムが法や規制に準拠していることは、ISMS、ITSMS を問わず重要なことです。関連する法令、規制を整理し、それらの遵守状況を確認する組織や態勢は、両マネジメントシステムで共有することは可能であると考えられます。

【事件・事故（インシデント）報告態勢　/　苦情処理窓口】

ISMS で採用している情報セキュリティインシデントや苦情処理窓口などの仕組みを

ITSMS で併用することは可能であると考えられます。情報セキュリティ要件や期待に対し、障害となり得る事象をセキュリティインシデントとして認識し、対応することは、ITSMS を構築する上においても重要です。但し、ITSMS では、インシデントを、「サービスに対する計画外の中断、サービスの品質の低下、又は顧客へのサービスにまだ影響していない事象」と定義しています。自組織内や外部委託先で発生するインシデント以外にも、例えばサービス提供者の態勢や周辺の情勢の変化などを、サービスの中断もしくは品質の低下を引き起こすインシデントと捉え、事前に何らかの対応をとることも重要です。

インシデントが発生した場合、ISMS、ITSMS とも発生したインシデントに対して、出来るだけ速やかに通常サービスに復旧させることを目的とした活動が重要です。

特に、ITSMS では、インシデント及びサービス要求管理の目的を以下のように定義しています。

8.1.2　概念

インシデント及びサービス要求プロセスは，全てのインシデント及びサービス要求を，事業及び顧客の優先度に従って，効果的かつ効率的に管理できることが望ましい。インシデント及びサービス要求の一環として収集したデータは，該当するサービス目標を基準にしたパフォーマンスの監視に使用することが望ましい。このデータは，顧客に渡すサービス報告書に含めることができる。

インシデントは，計画外のサービスの中断，サービスの質の低下，又はまだサービスに影響を及ぼしていない構成品目の障害と考えられる。サービス要求の例には，低リスクで，十分に定義され，事前に承認を受けた変更などの標準変更，情報の要求，手引の要求，標準的サービスへのアクセスの要求などが含まれることがある。

インシデント及びサービス要求管理プロセスは，二つの別々の文書化された手順で支援することが望ましい。一つはインシデントの管理用であり，もう一つはサービス要求の管理用である。二つの手順は，次の事項を定義することが望ましい。

a) インシデント及びサービス要求の一貫した記録
b) 合意し，文書化されたサービス目標に基づく，インシデント及びサービス要求の優先度付け及び分類
c) 8.1.3～8.1.6に詳述する，インシデントの解決及びサービス要求の実現に必要な活動
d) インシデントが解決したか，又はサービス要求が実現されたことについての利用者からの確認に関する，インシデント及びサービス要求記録を更新し，終了するために必要な処置
e) 該当する場合，合意したサービスレベルに従って，各インシデント又はサービス要求の解決又は実現を確実にするための段階的取扱い

インシデント及びサービス要求の手順は，既知の誤り及び問題とインシデントの比較，並びにサービスカタログとサービス要求との比較を含むことが望ましい。

（JIS Q 20000-2:2013　8.1.2 概念　より引用）

インシデント及びサービス要求管理プロセスに含めることが望ましいものとして、「情報の要求」、「記録」、「優先度付け及び分類」などが挙げられているところが特徴的です。ITSMS では、サービスの品質管理の視点から、情報の要求としての問合わせに対する対応も、インシデント及びサービス要求管理プロセス内で処理することが期待されています。

【内部監査員の態勢】

サービスマネジメントの実効性を担保するために、組織における様々な活動、サービスの調整など、構築したサービスマネジメントが意図した通り有効に機能していることを、内部監査を通じて把握し、改善のための意思決定等を行うためにマネジメントレビューを実施することは、重要です。

ISMS で採用している内部監査の仕組みや態勢、実施のための有益な手引きとなる JIS Q 19011:2012 を参照することは有用な手段であると考えられます。

ITSMS では、独立した項目として「4.5.4.2 内部監査」があり、その中で

- 監査プログラムを計画する
- 監査の基準、範囲、頻度及び方法を文書化する
- 監査の客観性及び公平性を確実にする
- 監査員は自らの仕事を監査してはならない

などが記載されており、JIS Q 27001 と整合がとられています。

【文書管理・記録管理】

サービスマネジメントの効果的な計画立案、運用及び管理を確実にするために、文書類は、版管理され適切な文書を必要とする人が必要なときに使用可能な状態で管理されている必要があります。JIS Q 20000-1 では、文書管理について、以下のものを作成することを要求しています。

> 4.3.1　文書の作成及び維持
>
> サービス提供者は，SMS の効果的な計画立案，運用及び管理を確実にするために，記録を含む文書を作成し，維持しなければならない。これらの文書には次を含まなければならない。
>
> a) サービスマネジメントについての文書化した方針及び目的
> b) 文書化したサービスマネジメントの計画
> c) この規格で要求する特定のプロセスのために作成された，文書化した方針及び計画
> d) 文書化したサービスカタログ
> e) 文書化した SLA
> f) 文書化したサービスマネジメントのプロセス
> g) この規格で要求する，文書化した手順及び記録
> h) SMS の効果的な運用及びサービスの提供のために，サービス提供者が必要と判断した，付加的な文書。
>
> これには外部で作成されたものを含む。
>
> （JIS Q 20000-1:2012　4.3.1 文書の作成及び維持　より引用）

また、記録管理に関しても、ISMS の記録管理同様、組織の ITSMS が要求事項へ適合していること及び、運用の効果を示す証拠として作成、維持、管理する必要があります。

JIS Q 20000-1 では、記録の管理として、以下の事項が要求されています。

4.3.3　記録の管理

記録は，要求事項への適合及び SMS の効果的運用を実証するために保管しなければならない。

記録の識別，保管，保護，検索，保管期間及び廃棄に関して必要な管理を規定するために，文書化された手順を確立しなければならない。記録は，読みやすく，容易に識別可能で，検索可能にしておかなければならない。

（JIS Q 20000-1:2012　4.3.3 記録の管理　より引用）

また、以下の事項の実施などが効果的です。

- 運営管理プロセスで記録の必要性及び記録の範囲を定めること
- 会社法等により保管期間が定められている場合には、法的要求事項に適合した保存期間を決定すること

JIS Q 20000-2:2013 では、情報セキュリティに関する文書及び記録に関して、以下のように記載しています。

6.6.4　文書及び記録

ISMプロセスによって作成し，保持することが望ましい文書及び記録は，次の事項を含めることが望ましい。

a)　情報セキュリティ戦略
b)　情報セキュリティ方針
c)　情報セキュリティ計画
d)　情報セキュリティ管理手順
e)　情報セキュリティ報告書
f)　ISMプロセスの有効性及び効率性に関する報告書
g)　情報セキュリティインシデントの記録
h)　情報セキュリティリスクアセスメント
i)　情報資産台帳

文書及び記録は，経営者に情報セキュリティ方針の有効性に関する情報を提供するために，定期的に分析することが望ましい。その他に役立つ側面としては，情報セキュリティインシデントの傾向，サービス改善計画へのインプット，並びに情報，資産及びシステムへのアクセス管理がある。

（JIS Q 20000-2:2013　6.6.4 文書及び記録　より引用）

【ISMS の管理策】

ISMS の管理策である JIS Q 27001:2006　附属書 A は､ITSMS のプロセスとの関連性が強く、共有化することが可能であると考えられます。

図 5-4 は、ITSMS のプロセスと ISMS の管理策全般の関係を例示したイメージです。「ISMS の領域」に包含された ITSMS のプロセスほど、ISMS の管理策を共有することが可能であると考えられます。ITSMS では、JIS Q 27001:2006　附属書 A のような管理策が特に用意されていないため、図 5-4、図 5-5 または表 5-1 を参考にしてください。図 5-5 は、ISO/IEC 27013 から引用した、ISO/IEC 27001 と ISO/IEC 20000-1 の対比に関する概要図です。

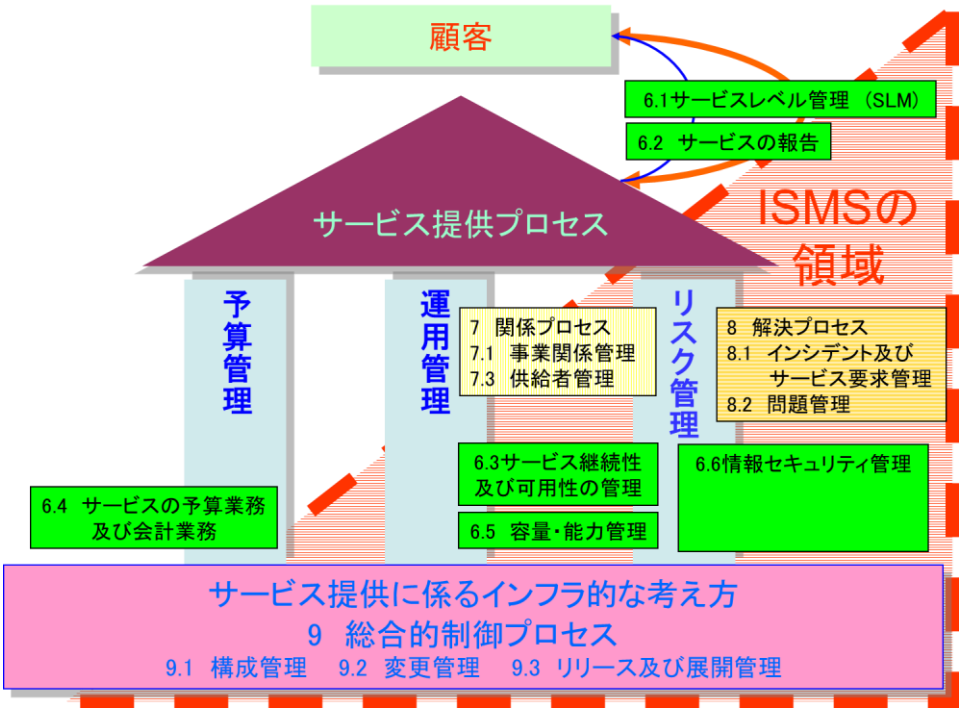


図 5-4　ITSMS のプロセスに関連する ISMS の管理策

ISO/IEC 27001 固有部分	共有部分（一部に重複又は相違あり）		ISO/IEC 20000-1 固有部分
・情報の分類	・容量・能力管理	・資源の運用管理	・サービスの予算業務及び会計業務
・情報資産の管理	・変更管理	・リスクアセスメント	・事業関係管理
	・構成管理	・役割及び責任	・新規サービス又はサービス変更の設計及び移行
	・インシデント及びサービス要求管理	・情報セキュリティ管理	
	・問題管理	・サービス継続及び可用性管理	・サービスレベル管理
	・リリース及び展開管理	・供給者管理	

共通部分（両規格で同じ内容のもの）	
・継続的改善	・PDCA
・法律及び規制の順守	・教育・訓練及び意識向上
・経営者の責任	・文書管理

図 5-5　ISO/IEC 27001 と ISO/IEC 20000-1 の対比（出典：ISO/IEC 27013:2012）

表 5-1　ISMS の管理策と ITSMS のプロセスとの関連

JIS Q 27001:2006　附属書 A ※（全般）は、管理目的配下の管理策全般を意味する	JIS Q 20000-1:2012	備考
A.10.2.3 第三者が提供するサービスに変更に対する管理	5.2 新規サービス又はサービス変更の計画	新規サービス又はサービス変更の計画立案について、顧客及び利害関係者と合意を得る
A.5.1.1 情報セキュリティ基本方針文書 A.6.1.5 秘密保持契約 A.6.2 外部組織（全般） A.10.2.1 第三者が提供するサービス A.11.3 利用者の責任（全般）	6.1 サービスレベル管理	顧客のセキュリティに関するニーズを識別し、SLA や契約を介し、保証するセキュリティレベルや、請負契約を締結している第三者との関係などを明らかにする
A.5.1.1 情報セキュリティ基本方針文書 A.6.1.5 秘密保持契約 A.6.1.6 関連当局との連絡 A.6.2.2 顧客対応におけるセキュリティ A.10.2.3　第三者が提供するサービスに変更に対する管理 A.10.10 監視（全般）	6.2 サービスの報告	提供している IT サービスの状況を正確かつ適時、経営陣や管理者、顧客に報告する
A.10.5 情報のバックアップ（全般） A.14 事業継続管理（全般）	6.3 サービス継続及び可用性管理	サービスの事業継続計画を作成し、試験、維持、及び再評価をし、顧客との SLA などで合意した範囲内に緊急事態の影響を抑える
A.10.3.1 容量・能力の管理 A.10.10.2 システム使用状況の監視	6.5 容量・能力管理	サービスの可用性を維持する上において、容量・能力の管理を徹底する
附属書 A　（全般）	6.6 情報セキュリティ管理	情報セキュリティ管理の実施及び、変更によって、管理策の効果的な運用が阻害されないようにする
A.5.1.2 情報セキュリティ基本方針のレビュー A.6.2.2 顧客対応におけるセキュリティ A.10.9.1 電子商取引 A.11.2.4 利用者アクセス権のレビュー A.11.3 利用者の責任　（全般）	7.1 事業関係管理	顧客の良好な関係を確立する為に、顧客のセキュリティに関するニーズを識別しサービスの適用範囲、SLA、顧客からの事業上の必要性の変更などをレビューする
A.5.1.2 情報セキュリティ基本方針のレビュー A.6.1.5 秘密保持契約 A.6.1.8 情報セキュリティの独立したレビュー A.6.2.1 外部組織に関係したリスクの識別 A.6.2.3 第三者との契約におけるセキュリティ A.10.2 第三者が提供するサービスの管理（全般） A.12.5.5 外部委託によるソフトウェア開発	7.2 供給者管理	顧客に提供するサービスレベルを維持するため供給者（内部組織、提携会社、第三者（外部委託先））を管理する
A.6.1.6 関連当局との連絡 A.8.2.2 情報セキュリティの意識向上、教育及び訓練 A.10.4.1 悪意のあるコードに対する管理策 A.13 情報セキュリティインシデントの管理（全般）	8.1 インシデント及びサービス要求管理	セキュリティインシデントを報告し、内容に応じて適切な処置を投じる

A.5.1.2 情報セキュリティ基本方針のレビュー A.6.1.7　専門組織との連絡 A.10.4.1 悪意のあるコードに対する管理策 A.10.10.5 障害のログ取得 A.12.6 技術的ぜい弱性の管理（全般） A.13.2　情報セキュリティインシデントの管理及びその改善　（全般）	8.2 問題管理	情報セキュリティ上の弱点を識別し、既知及び未知の問題が発生しないよう、解決策を見出す
A.7.1 資産に対する責任（全般） A.7.2 情報の分類（全般） A.15.1 法的要求事項の順守（全般）	9.1 構成管理	SLA や、関連する法的要求事項（個人情報、知的財産の取扱い等）等の要件に応じ、資産（情報、システムなど）を識別、分類し、どのように管理するかの構成について設計し、管理する
A.10.1.2 変更管理 A.10.2.3 第三者が提供するサービスの変更に対する管理 A.12.5.1 変更管理手順 A.12.5.3 パッケージソフトウェアの変更に対する制限	9.2 変更管理	変更管理手続きに従い、変更後も顧客に対して、合意したセキュリティレベルのサービスを提供する
A.10.3.2 システムの受入れ A.12.5.2 オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー	9.3 リリース及び展開管理	新規のシステム（ソフトウェア、ハードウェア、通信機器など）リリースに際し、各々のセキュリティテストなどを介してサービスを提供する、またはそれらのシステムを受入れる

注意：この表は、ISMS の管理策と ITSMS のプロセスとの関連性を示したもので、ISMS を構築していれば、該当する ITSMS のプロセスの要求事項を全て満たしていることを示すものではないことに十分留意してください。

表 5-1 の JIS Q 20000-1:2012　6.6 情報セキュリティ管理では、JIS Q 27001:2006　附属書 A　全般として表記しました。但し、下記に示すように 6.6.2 情報セキュリティ管理策では、以下の通り記載しています。

6.6.2　情報セキュリティ管理策

サービス提供者は，次のために物理的，実務管理的，及び技術的な情報セキュリティ管理策を導入し，運用しなければならない。

a)　情報資産の機密性，完全性及びアクセス性を保つ。

b)　情報セキュリティ基本方針の要求事項を満たす。

c)　情報セキュリティ管理の目的を達成する。

d)　情報セキュリティに関連するリスクを管理する。

これらの情報セキュリティ管理策を文書化し，管理策が関連するリスク，管理策の運用及び維持について記述しなければならない。

サービス提供者は，情報セキュリティ管理策の有効性をレビューしなければならない。サービス提供者は，必要な処置をとり，とった処置について報告しなければならない。

サービス提供者は，サービス提供者の情報又はサービスにアクセスし，利用又は管理する必要がある外部組織を特定しなければならない。サービス提供者は，情報セキュリティ管理策について，これらの外部組織と文書化し，合意し，実施しなければならない。

（JIS Q 20000-1:2012　6.6.2 情報セキュリティ管理策　より引用）

注意：上記のアクセス性において、対応国際規格の“accessibility”に対して“アクセス性”の

訳語を当てていますが、これはJIS Q 27001:2006の“情報セキュリティ”の定義に用いられている“可用性（availability)”と同じ意味です。詳細は、「ITSMSユーザーズガイド –JIS Q 20000（ISO/IEC 20000）対応 -」を参照してください。

また、上記以外にも、「A.10　通信および運用管理」全般、「A.11アクセス制御」全般、「A.12　情報システムの取得、開発及び保守」全般等、比較的、技術的な要素を多く含む項目は、共有化が計りやすいと考えられます。

5.3. まとめ

前述のように、各々の基準の差を認識された上で、可能な限り、ISMS 構築時に培ったノウハウやリソースを最大限に生かしながら、ITSMS を構築することは、双方のマネジメントシステムに相乗効果をもたらすことが期待されます。負のリスクを最小限に抑える ISMS のいわば守備側の側面と展開するサービスの信頼性、品質に貢献する ITSMS のいわば攻撃側の側面が一体となることは、IT サービス事業者にとって、最大限の利益を得ることに繋がります。従って、ISMS、ITSMS を車の両輪に見立て、バランスよく運用していくことが重要です。

一方、両基準を効果的に満たすマネジメントシステムの構築は確かに重要ではありますが、そもそも個人情報、機密情報保護のような目標だけを掲げて ISMS 構築をした組織であれば、容易に ITSMS との統合化を設計できるものではありません。当初からあまり合理化のための設計に捉われることで、ISMS 担当者の業務負荷を高め、モチベーションを低下させるよりは、ある程度、両マネジメントシステムが形になってから、共通項などを整理された方が、良い結果を得ることに繋がることにも留意していただきたいと思います。

また、統合する場合、マネジメントサイクルの同期をとることを推奨いたします。ISMS の監査後に、ITSMS の監査を行い、マネジメントレビュー等を別々に行うというよりは、可能な限りタスクを一元化し、効果的なマネジメントシステムを構築することを推奨します。企業、組織によっては、サービスは最低限、四半期に一度見直すが、情報セキュリティは、年に一度である、とか、情報セキュリティは一度構築しても、日々、強度が弱まる傾向にあるため、毎週のように見直すが、サービスは、新規サービスでも立ち上げない限り、本質的な見直しを行わないなど、考え方は様々であると思いますが、前述したように双方のマネジメントシステムを車の両輪のように一体化した仕組みで運用することが効果を発揮すると思います。従って、作業を低減する上においても双方の PDCA サイクルの周期の同期を図ることを推奨します。

【参照情報】　ISO/IEC 27013:2012 について

ISO/IEC 27013:2012 は、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として、2012 年 10 月に発行されました（2013 年 5 月現在、本ガイダンス規格は、JIS 化される予定はありません。）。本ガイダンス規格は、タイトルが示す通り、ISO/IEC 20000-1 及び ISO/IEC 27001、すなわちサービスマネジメントと情報セキュリティマネジメントは、比較的近い関係にあり、多くの組織・企業が両方の規格を採用することのメリットを感じていることから、両規格を取り入れる、またはいずれかの規格の要求事項を満たしている場合、それらをさらに向上させるためにもう一方の規格の要求事項を取り入れ、統合的なマネジメントシステムを構築する際、役

立ちます。また、本章を記載する際、ISO/IEC 27013:2012 を参考にしています。

参考として、本ガイダンス規格の目次を記載します。

表 5.2　ISO/IEC 27013:2012 の目次

項番			ISO/IEC 27013:2012 のタイトル（仮訳）
1			適用範囲
2			引用規格
3			用語，略語及び定義
4			ISO/IEC 27001 及び ISO/IEC 20000-1 の概要
	4.1		国際規格の理解
	4.2		ISO/IEC 27001 の概要
	4.3		ISO/IEC 20000-1 の概要
	4.4		類似点及び相違点
5			統合された実装へのアプローチ
	5.1		一般
	5.2		両規格の適用範囲の考慮事項
	5.3		実装前の組織の状況
		5.3.1	一般
		5.3.2	マネジメントシステムの基礎として両規格を現在利用していない場合
		5.3.3	どちらかの規格の要求事項を満たしているマネジメントシステムが存在している場合
		5.3.4	各規格の要求事項を満たすマネジメントシステムが別々に存在している場合
6			統合された実装に関する考慮事項
	6.1		一般
	6.2		考えられる課題
		6.2.1	資産という用語の利用及び意味
		6.2.2	サービスの設計及び移行
		6.2.3	リスクアセスメントとリスクマネジメント
		6.2.4	リスク受容レベルの違い
		6.2.5	インシデント管理及び問題管理
		6.2.6	変更管理
	6.3		考えられる効果
		6.3.1	PDCA サイクルの活用
		6.3.2	サービスレベル管理及びサービスの報告
		6.3.3	経営者のコミットメント
		6.3.4	容量・能力管理
		6.3.5	第三者のリスクの管理
		6.3.6	継続及び可用性管理

6. QMS ユーザのための ITSMS 入門「JIS Q 9001 から見た JIS Q 20000」

6.1. はじめに

既に JIS Q 9001（ISO9001）規格の QMS は製造業及びサービス業の産業分野において、多くの認証が登録されています。一方、IT サービスにおいては、JIS Q 20000（ISO/IEC 20000）が発行され、ITSMS の認証登録が 2007 年から国内で新たに開始されました。

JIS Q 9001 は提供する製品（物やサービス）の品質向上と顧客満足の継続的な向上を目指していくマネジメントシステムであり、そのプロセスは広汎な業種に対応できるように、最小限の基本的な要求で構築され、組織固有の部分は自らが定義したプロセスや手順を付加して構築・運用する規格であります。

一方、JIS Q 20000 は提供するサービスの品質向上を目指すもので、この目的は JIS Q 9001 と同じですが､提供するサービスを IT サービスに特化している品質マネジメントシステム規格であります。2012 年 9 月に ITSMS の規格である JIS Q 20000 が改訂されました。この改訂では、使用する用語などに QMS の JIS Q 9001 や ISMS の JIS Q 27001 との整合が配慮されていますから、これらの規格間の共通性が一段と増しています。

本ガイドでは、既に JIS Q 9001 を導入している QMS ユーザのために、JIS Q 9001 規格からみた JIS Q 20000 の規格の違いや共通点を紹介して ITSMS への理解を促すものであり、QMS から ITSMS への展開をも考察しています。

6.2. 両規格の相違点

JIS Q 9001 の規格を基準として、JIS Q 20000 の規格の比較をこの 6 章末の図 6-1 に示しています。

規格全体は、①の適用範囲、②のマネジメントシステム、③の製品実現プロセスに分けることができます。2012 年の JIS Q 2000 規格の改訂から、①の適用範囲や②のマネジメントシステムは規格の要求事項の対比から、JIS Q 9001 と JIS Q 20000 はほぼ同じ要求になりました。一方、③の製品実現は ITSMS の JIS Q 20000 の方が詳細な要求となっています。両規格の相違点を以下に明らかにします。

6.2.1. 適用範囲の相違点

JIS Q 9001 の 1 章「適用範囲」では、適用除外に違いがあります。JIS Q 9001 は 7 章「製品実現」での要求プロセスや要求項目が該当しない場合には適用除外にできますが､JIS Q 20000 で定義された箇条 5、箇条 6、箇条 7、箇条 8、及び箇条 9 の設計と運用に関する１４のプロセスは除外が認められません。

6.2.2. マネジメントシステムの相違点

JIS Q 9001 及び JIS Q 20000 はマネジメントシステムに関係するプロセスはマネジメントレビュー、内部監査などほぼ共通ですが、上記したように JIS Q 20000 では１４のプロセスの適用除外が認められないことから、そのプロセスの一部或いは全部を内部グループ、顧客又は供給者に

委託している場合には、4.2 項「他の関係者が運用するプロセスのガバナンス」に示すように、プロセスの説明責任やプロセスの順守を要求する権限などを実証することが求められています。QMS の管理の方法や程度を定めて運用するアウトソースの管理より一段強いガバナンスの要求であることに注目ください。以下に JIS Q 9001 の要求に対比した JIS Q 20000 の要求の違いを示します。

「4.2　文書化に関する要求事項：JIS Q 9001」

今回 JIS Q 20000 が改訂され、文書管理、記録の発行・配布・保管等の要求に対する管理を文書管理手順書などで管理することになりました。また、文書化した手順、契約（SLA）等の文書、変更要求（RFC）の画面記録、構成管理における構成要素データ等の文書・記録の管理の確立が要求されています。

・JIS Q 20000 のサービス改善方針は、「品質方針」、又は全体の「品質目標」に相当します。

「5.1 経営者のコミットメント、5.6 マネジメントレビュー：JIS Q 9001」

経営者の責任に関係するコミットメントなどの要求はほぼ同じです。今回 JIS Q 20000 が改訂され、マネジメントレビューのインプット及びアウトプットの要求もほぼ同じとなりました。

「6.　資源の運用管理：JIS Q 9001」

資源の提供には、コスト管理とあわせて、教育・訓練、インフラ、作業環境（労働衛生）の考慮が必要です。JIS Q 20000 のサービス要員の教育・訓練の要求事項は JIS Q 9001 と同じですが、サービスデリバリ、コントロールのそれぞれのプロセス定義との結びつけが必要です。

「8.2.2 内部監査：JIS Q 9001」

JIS Q 20000 が改訂され、内部監査の要求が同じになりました。

「5.2 顧客重視、8.2.1 顧客満足：JIS Q 9001」

JIS Q 20000 では「7.1 事業関係管理」で顧客満足の実現のための要求を明らかにしています。顧客とのコミュニケーションや顧客満足度測定に加えて、苦情の定義を顧客と同意し、エスカレーションの経路を含む苦情処理手順を整備することを求めています。

「8.5.2 是正処置、8.5.3 予防処置：JIS Q 9001」

JIS Q 20000 では「4.5.5 SMS の維持及び改善」で継続的改善、是正処置及び予防処置が要求され、これら詳細は JIS Q 9001 を参照する注記となっています。

6.2.3. 製品実現プロセスの相違点

特に、製品（サービス含む）実現のプロセス構成に対しては、JIS Q 9001 が広汎な事業活動を許容するため最小限の要求となっているのに比べて、JIS Q 20000 は IT サービス提供に不可欠な箇条 5「新規サービス又はサービス変更の設計及び移行」のプロセス、及び箇条 6～箇条 9 の運用に関する１３のプロセスを特定し、そのプロセス特有の要求事項を詳細に規定しているところに大きな違いがあります。JIS Q 9001 のプロセスから見た JIS Q 20000 のプロセスの相違を以下に示します。

「7.1 製品実現の計画：JIS Q 9001」

図 6-1 の③に、JIS Q 9001 製品実現の計画における基本的なプロセス構成と JIS Q 20000 の IT サービスに関する設計のプロセスと運用に関する１３のプロセスの違い及びその関係を示しています。

「7.2 顧客関連プロセス：JIS Q 9001」

「7.2.1 製品に関連する要求事項の明確化、7.2.2 製品に関連する要求事項のレビュー、7.2.3 顧客とのコミュニケーション」については、JIS Q 20000 における「7.1 事業関係管理」で詳細に要求事項が定められており、「6.1 サービスレベル管理（SLA）」の協議、苦情の定義と対応の手順化、「6.2 サービスの報告」でのレポートの義務化などが関係します。

「7.3 設計・開発：JIS Q 9001」

JIS Q 20000 では「5 新規サービス又はサービス変更の設計及び移行」のプロセスが関係し、計画、設計及び開発、移行に対しての要求があります。設計・開発のプロセスにおける要求は JIS Q 9001 程は具体的でなく、詳細は JIS Q 9001 を注記で参照しています。設計・開発後の移行に当たっては、試験し、稼働環境への展開のためにリリース及び展開管理プロセスを使用することになります。また、新規サービス又はサービス変更は JIS Q 20000 の変更管理プロセス・構成管理プロセスを通して実施することが要求されています。

「7.4 購買：JIS Q 9001」

JIS Q 9001 の要求は一般的な購買を対象としていますが、JIS Q 20000 では IT サービスでよく見られる委託関係を考慮して、「7.2 供給者管理」に供給者との契約締結、顧客との契約（SLA）との整合、再委託先の管理などが追加されています。

「7.5 製造及びサービス提供：JIS Q 9001」

「7.5.1 製品及びサービス提供の管理」、「7.5.2 製品及びサービス提供のプロセスの妥当性確認」に関しては、IT サービス提供はリアルタイムの連続サービスが多いために、JIS Q 9001 の妥当性確認のプロセスの考え方が大事になります。容量・能力管理、可用性管理、などのサービスデリバリを継続する具体的な要求事項、及びサービス提供プロセスにおける要員の IT スキルの確保のための教育訓練等が要求されます。

「7.5.3 識別及びトレーサビリティ」に関しては、JIS Q 9001 でも構成管理を要求していますが、JIS Q 20000 では「9.1 構成管理」として、管理ツール（CMDB）の用意などの資源の提供とあわせてサービス提供を構成する要素に関して詳細な要求がされています。

「7.5.4 顧客の所有物」に関しては、顧客からの情報資産が対象になり、JIS Q 20000 の「6.6 情報セキュリティ管理」が関係します。

「7.5.5 製品の保存」はサービスの内容によりますが、JIS Q 20000 では「9.1 構成管理」における構成ベースラインの維持が該当し、「9.2 変更管理」「9.3 リリース及び展開管理」をサポートしています。

「7.6 監視及び測定機器の管理：JIS Q 9001」

監視機器、測定機器の管理に関しては、JIS Q 9001 では単独の要求がされています。一方、JIS Q 20000 では単独の要求はありませんが、サービス提供の構成要素である電気通信設備の監視、測定機器の管理はシステムの維持に不可欠でありますから、JIS Q 9001 と JIS Q 20000 の要求内容はあまり変わらないと言えます。JIS Q 9001 ではソフトウェアの意図した監視測定

機能の確認だけの要求ですが、JIS Q 20000 におけるサービスの監視には監視用ソフトウェアが不可欠のため、ソフトウェアを含む監視システム全体の管理が必要になります。

但し、監視カメラのような、要員の行動（サービス活動）を監視・記録する場合は、個人情報保護法などの法的な要求事項の考慮が必要です。

「8.2.3 プロセスの監視測定：JIS Q 9001」

JIS Q 20000「4.5.4 SMS の監視及びレビュー」では、(a)JIS Q 9001 の 8.2.3 プロセスの監視及び測定、(b)5.6 マネジメントレビュー、(c)8.2.2 内部監査の目的が記載されています。

また、JIS Q 20000「9.1 構成管理」では構成の監査として欠陥の記録、是正処置の開始、及び結果報告の手順が必要になります。

JIS Q 20000 の「6.2 サービスの報告」では a)～f)の活動状況を報告することが要求されていて、これにはシステム及びプロセスの監視測定が必要になります。

「8.2.4 製品の監視及び測定：JIS Q 9001」、「8.3 不適合製品の管理：JIS Q 9001」

提供するサービスの監視測定に関して、JIS Q 20000 では「5 新規サービス又はサービス変更の設計及び移行」において試験を要求しており、「4.5.4 SMS の監視及びレビュー」でも SMS の要求事項、又はサービスの要求事項に対して不適合を特定する要求があります。

JIS Q 9001 の不適合には、JIS Q 20000 では「8.1 インシデント及びサービス要求管理」の“インシデント”が該当しますが、“インシデント”はサービスに対する計画外の中断、サービスの質の低下、又は顧客へのサービスにまだ影響していない事象と定義されています。利用者からの“障害”だけでなく“サービスの要求”も含めて、このプロセスで取り扱います。また“内部で発見された障害”もこのプロセスで扱うことが求められます。インシデントの処理は JIS Q 20000 の「8.1 インシデント及びサービス要求管理、8.2 問題管理、9.1 構成管理、9.2 変更管理、9.3 リリース及び展開管理」で詳細に定められています。

「8.4 データの分析：JIS Q 9001」

JIS Q 20000 の「4.5.5 SMS の維持及び改善」に改善のマネジメントを要求しています。改善の機会は優先度を付け、承認された改善について計画実行することが要求されています。個々のプロセスにおいては、改善の機会を特定するために結果を測定し、評価し、レビューすることが求められています。

6.2.4. **JIS Q 9001** にない規格概念による相違点

JIS Q 9001 の QMS には“リスク管理”及び“予算管理”に関する概念がなく、JIS Q 20000 の ITSMS ではこの概念から QMS には無い下記のプロセスが新たに要求されています。

「6.3　サービス継続及び可用性管理：JIS Q 20000」

JIS Q 9001 では障害によるサービス中断を防止するため、設備に冗長性を持たせる“可用性”までは、適用されている例がありますが、災害等の発生を想定したサービス停止に対する事業継続の要求はありません。JIS Q 20000 ではこれが要求されます。

「6.4　サービスの予算業務及び会計業務：JIS Q 20000」

サービス提供費用の予算を管理し、会計を行います。対象範囲外である財務管理プロセスとのインタフェースの明確化も必要です。運用コスト（施設、エネルギー、ライセンス費用）、インフラ（冗長化など含む）、要員（外注費含む）などにかかるコストは、リスク評価ととも

に考えなければなりません。

「6.5 容量・能力管理：JIS Q 20000」

現在及び将来に予想されるサービス拡張に対してキャパシティを管理します。

「6.6　情報セキュリティ管理（事業リスク評価）：JIS Q 20000」

IT サービス提供の事業リスクに対して情報セキュリティを実施します。

6.3. まとめ

JIS Q 9001 の QMS と JIS Q 20000 の ITSMS はマネジメントシステムの基本的な形態でほぼ同じ構造を持っていますが、ITSMS では IT サービスの提供管理に不可欠なプロセスを特定して、そのプロセスに対する要求事項が詳細に規定されているところに違いがあります。

既に QMS を導入している IT サービス事業者においては、図 6-2 に示すように、JIS Q 9001 の QMS で構築した製品実現プロセスにおいて、JIS Q 20000 の「新規サービス又はサービス変更の設計及び移行」のプロセスと運用に関する１３のプロセスを併せた１４のプロセス要求を付加していくことにより、QMS から ITSMS へシステムを円滑に変えて行くことができます。特に、QMS で構築したマネジメントシステム部分をシステムの基礎として、その上に ITSMS 固有の設計と運用のプロセスが付加できるので、効果的に ITSMS のシステムが構築できます。また、IT サービスに限らず事業活動が広い場合にはより広範な活動を対象とする JIS Q 9001 の QMS と JIS Q 20000 の ITSMS との共有のマネジメントシステムにすることで会社全体の管理を統合化できます。

以上からも、JIS Q 9001 規格の QMS と JIS Q 20000 規格の ITSMS は互いに補完し合える親和性の高いマネジメントシステムであります。QMS から ITSMS への展開は IT サービス特有のプロセスを付加することで容易に実現可能であり、顧客からの ITSMS 認証取得の要求に対しても、QMS ユーザは JIS Q 9001 で培ったシステムの基盤と運用の実績が無駄にはならないことに注目しましょう。

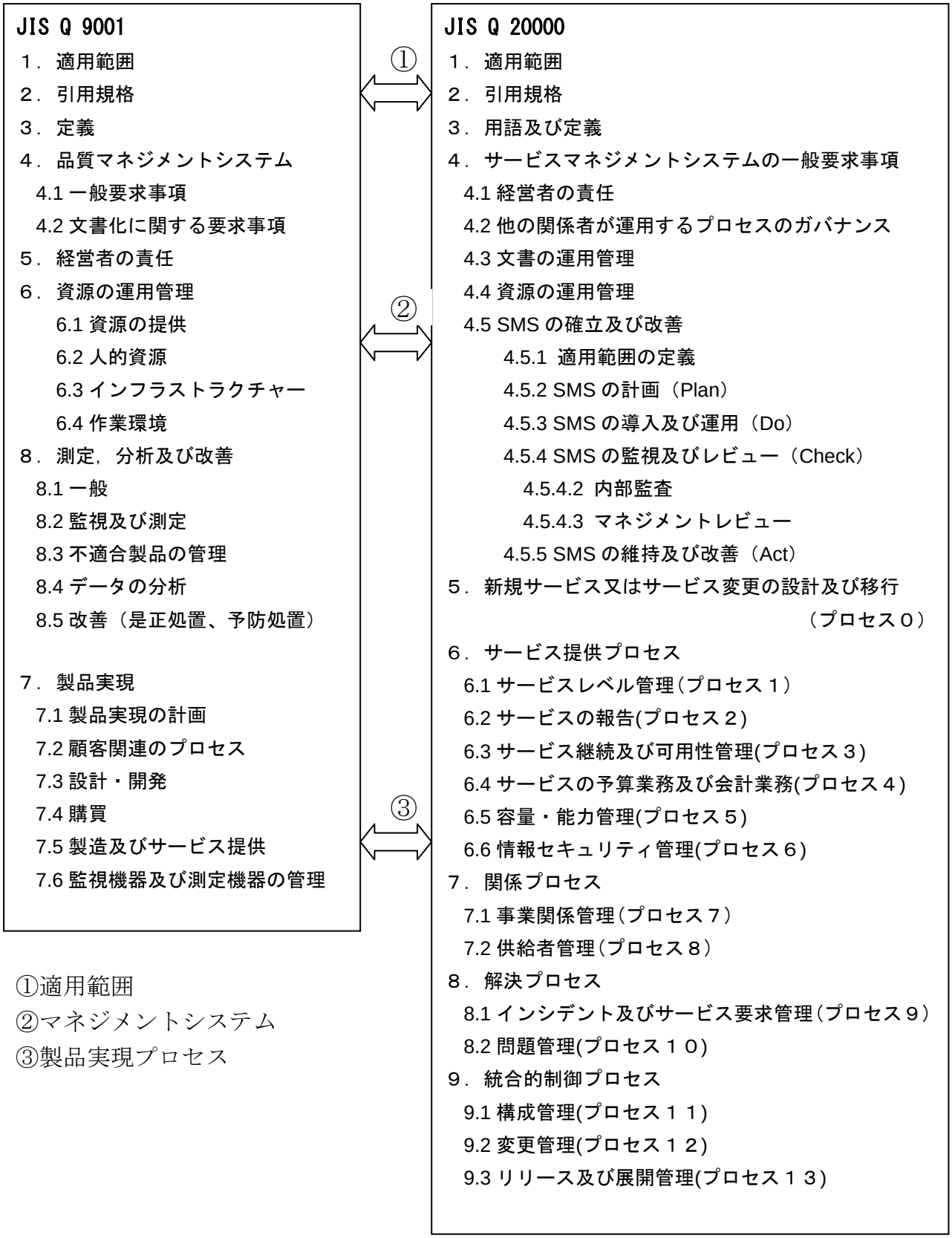


図 6-1　JIS Q 9001 と JIS Q 20000 の規格要求事項の対比図

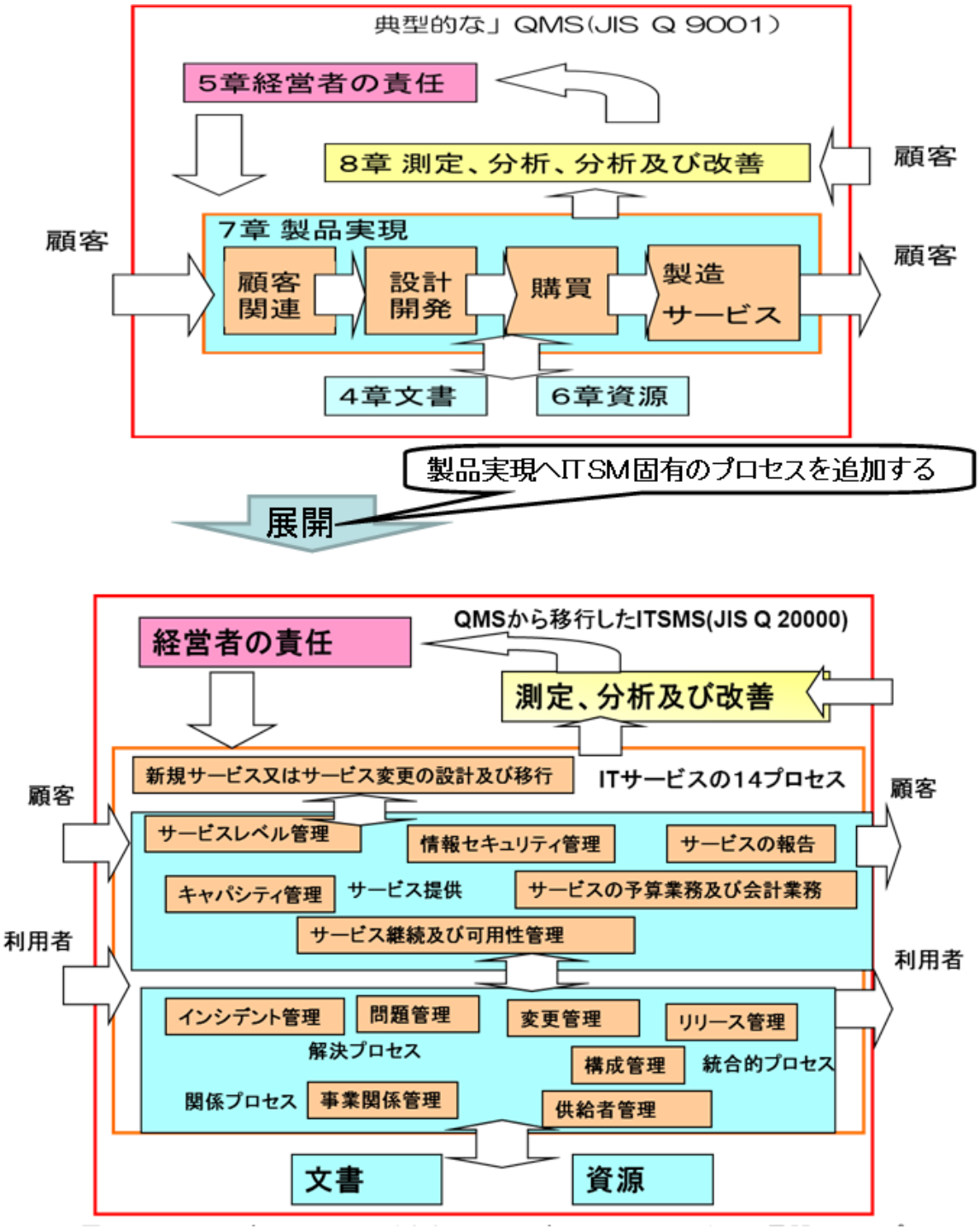


図 6-2　QMS(JIS Q 9001)~ITSMS(JIS Q 20000)への展開ステップ

7. ITIL ユーザのための ITSMS 入門

7.1. はじめに

ITIL（IT Infrastructure Library：IT インフラストラクチャライブラリ）は 1980 年代から英国で、IT サービスを効率的に管理・運営していくための方法論の模索として興りました。初版は 1989 年、当時の英国政府機関 CCTA（Central Computer and Telecommunications Agency）、現在の OGC（Office of Government Commerce）によって発行されています。

1990 年代の後半に入ると ITIL の第 2 版（以下、ITIL V2）として、書籍群の重複部分の整理や改訂が行われ、7 冊の書籍に整理されました（図 7-1）。日本への上陸を 2003 年の *it*SMF Japan（IT サービスマネジメントフォーラム）の設立時と考えると、今年（2008 年）で足掛け 11 年目となります。この間に既に多くの企業や団体に導入され、さまざまな効果や工夫が報告されています。ITIL で採用されている IT サービスマネジメントプロセスの呼称は、全国の IT システム運用の現場のどこでも通用する共通言語になりました。

日本における ITIL の隆盛を追いかけるように、2005 年 12 月に ITIL V2 をベースとした国際規格 ISO/IEC 20000 が制定されています（JIS 化は 2007 年 4 月）。ここに至って、ITIL 導入から始めて IT サービスマネジメントの整備を進めてきた組織は、ITIL→JIS Q 20000→ISO/IEC 20000 という読み替えを行うことによって海を越えて通用する IT サービスマネジメントの認識基盤を手中にしたわけです。このことはグローバルな IT サービス提供体制を確立・推進している企業、もしくはグローバルに IT サービスを利用している企業にとって大きな意味を持つといえるでしょう。

その後、ITIL と ISO/IEC 20000 はそれぞれを推進している組織によって改訂を加えられてきました。ITIL は 2007 年に ITIL V3 として改訂版が発表されました。それまでのプロセスベースと称される構造から、IT サービスのライフサイクルアプローチという構造を取ることで、ビジネスを意識した IT サービスの提供を目指しました。ITIL V3 ではライフサイクルのステージを 5 段階に分類し、それぞれの段階をコア書籍として纏めています（図 7-2）。

ITIL V3 は、2007 年に出版後に、更にもう一段階改訂が加えられ、ITIL V3 2011 Edition※1）として 2011 年に発行されました。

※注記の説明：

1）2013 年から、ITIL V3 2011 Edition は ITIL 2011 Edition と表記されることになっていますが、ITILV2, V3 との比較表などを考慮し、ITIL V3 2011 Edition としました。

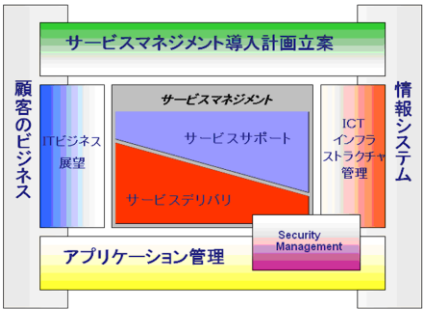


図 7-1：ITIL V2 フレームワーク

出展：OGC（Office of Government Commerce）

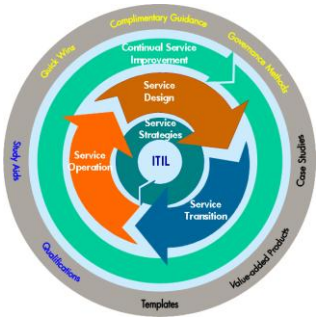


図 7-2：ITIL V3 フレームワーク

出展：OGC（Office of Government Commerce

本章では、ITIL 導入に取組んでいる組織の読者を対象に、ISO/IEC 20000 への道筋を示したいと考えています。

7.2. ベストプラクティスと規格

7.2.1. ベストプラクティス

ITIL V2 は、IT サービスマネジメントのベストプラクティスとして知られる次の 7 冊の書籍群です。

表 7-1　ITIL V2 コア書籍の概要

サービスサポート	ユーザに対するサービスのサポートを供給することに関連した 5 つのコア・サポート・プロセス（インシデント管理、問題管理、変更管理、構成管理、リリース管理）と、他の全プロセスが利用するサービスデスク機能について説明
サービスデリバリ	情報システムサービスの供給の将来的な計画立案と改善により関連した、5 つのコア・デリバリ・プロセス（サービスレベル管理、IT サービス財務管理、キャパシティ管理、IT サービス継続性管理、可用性管理）について説明
サービスマネジメント導入計画立案	組織内でのサービスマネジメント･プロセスの計画立案、導入、および改善に関連する課題とタスクを考察し、IS 組織と、関連するサービスマネジメントプロセスの両方について現在の成熟度レベルを評価する際の実用的な手引きを提供
ビジネスの観点	ビジネスまたは事業（ビジネス）組織とその運営の主要な原則と要件が、情報システムサービスの開発、提供、サポートにどのように関係しているかについて、IT 実践者の認識形成を支援
アプリケーション管理	アプリケーションに対する初期のビジネスニーズから廃棄までを含むアプリケーションのライフサイクルを通して、アプリケーションの管理について説明
ICT インフラストラクチャ管理	ICT のコンポーネントとサービスの計画立案、設計、展開、および継続的な技術サポートと管理に関して説明
セキュリティ管理	情報および情報システムサービスに関する定義済みのセキュリティレベルにおける計画立案と管理のプロセスについて説明

国内においては、サービスサポートとサービスデリバリで取り上げられているプロセス群が、運用管理のベストプラクティスとして注目され多くの企業において取り組みがなされました。

2007 年に発表された ITIL V3 では、ITIL V2 で唱えられていた、IT サービスとビジネスの整合から、IT サービスとビジネスの統合を目指しました。

ITIL V3 では、IT サービスの戦略から運用までをサービスのライフサイクル視点で捉えることで、5 つのステージを定義しています。各ステージは、それぞれ 5 冊のコア書籍として纏められました。

表 7-2　ITIL V3 コア書籍の概要

サービスストラテジ（SS: Service Strategy）	サービスマネジメントを戦略的資産として 開発､導入するためのガイダンス

サービスデザイン（SD: Service Design）	事業の要求を満たすサービスとプロセスを 設計するためのガイダンス
サービストランジション（ST: Service Transition）	新規または変更されたサービスを運用に 移行させるガイダンス
サービスオペレーション（SO: Service Operation）	サービスの提供における有効性と効率性を達成するためのガイダンス
継続的サービス改善（CSI: Continual Service Improvement）	サービスの品質や運用上の効率性を維持し改善するためのガイダンス

ITIL V3 は 2007 年に発表された後、いくつかの課題に対処するために、全面的な改訂が決定されました。結果として、2011 年に ITIL V3 2011 Edition が発表されています。ITIL V3 ではサービスのライフサイクルに関連するプロセス群が定義されています。ライフサイクルを意識しているために、プロセスによっては複数のステージにまたがって活動をします。ITIL V3 2011 Edition では次のように、26 のプロセスと 4 つの機能が定義されています。

表 7-3　ITIL V3 2011 Edition のプロセス

事業関係管理	SS	リリース管理および展開管理	ST
需要管理	SS	サービス妥当性確認及びテスト	ST
サービス・ポートフォリオ管理	SS	移行の計画立案およびサポート	ST
IT サービス戦略管理	SS	変更管理	ST
IT サービス財務管理	SS	変更評価	ST
サービス・カタログ管理	SD	サービス資産管理および構成管理	ST
サービスレベル管理	SD	ナレッジ管理	ST
キャパシティ管理	SD	要求実現	SO
可用性管理	SD	問題管理	SO
IT サービス継続性管理	SD	アクセス管理	SO
デザイン・コーディネーション	SD	インシデント管理	SO
情報セキュリティ管理	SD	イベント管理	SO
サプライヤ管理	SD	7 ステップの改善プロセス	CSI

注：SS（Service Strategy）、SD（ Service Design）、ST（Service Transition）、SO（Service Operation）、CSI（Continual Service Improvement）

表 7-4　ITIL V3 2011 Edition の機能

サービスデスク	SO	IT 運用管理	SO
技術管理	SO	アプリケーション管理	SO

7.2.2. 規格

ベストプラクティスの ITIL に対し、ISO/IEC 20000 は 2 部からなる国際規格です。2005 年に国

際規格として制定されました。

・ISO/IEC 20000-1:2005
　Information technology - Service Management - Part 1: Specification
・ISO/IEC 20000-2:2005
　Information technology - Service Management - Part 2: Code of Practice

JIS Q 20000 は ISO/IEC 20000 を翻訳した JIS 規格であり、次のように訳出されています。

・JIS Q 20000-1:2007
　情報技術－サービスマネジメント－第 1 部：仕様
・JIS Q 20000-2:2007
　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

規格は 5 年ごとに見直しが行われます。ISO/IEC 20000:2005 も同様の経緯を経て、2011 年に、次のように改正された規格として置き換えられました。

・ISO/IEC 20000-1:2011
　Information technology - Service Management - Part 1: Service management system requirements
・ISO/IEC 20000-2:2012
　Information technology - Service management - Part 2: Guidance on the application of service management systems

ISO/IEC 20000 の JIS 化に関しては、Part1 は 2012 年に JIS Q 20000-1:2012 として、Part2 は、2013 年に JIS Q 20000-2:2013 として制定されました。

・JIS Q 20000-1:2012
　情報技術－サービスマネジメント－第 1 部：サービスマネジメントシステム要求事項
・JIS Q 20000-2:2013
　情報技術－サービスマネジメント－第 2 部：サービスマネジメントシステムの適用の手引

2005 年版と 2011 年版の表題が、Part1 の Specification から Service management system requirements の表記に変わり、Part2 は Code of Practice から Guidance on the application of service management systems に変わっていることを留意ください。

日本語表記では、Part1 が 2007 年版の仕様（Specification）から、2012 年では、サービスマネジメントシステムの要求事項（Requirements）に変更になっています。単なる仕様の表記のみであったものが、対象を「サービスマネジメントシステム」と明確化した要求事項となっています。

Part2 は、JIS の 2007 年版では、実践のための規範（Code of Practice）という表記でしたが、2013 年版では、サービスマネジメントシステムの適用の手引（Guidance on the application of service management systems）という表記になりました。

JIS Q 20000 は ISO/IEC 20000 の国際一致規格として作成されていますので、両者は同等な規格とみなされます。本章では、ISO/IEC 20000 の説明に JIS Q 20000 での日本語訳を使用し、表記に関しては、2007 年版と 2012 年版があることから、必要に応じて“JIS Q 20000”で統一します。

また ITIL も ITIL V2 と ITIL V3 の 2 つの版があり、さらに ITIL V3 においては、最新の 2011 Edition が存在しますので、こちらも必要に応じて、ITIL V2、ITIL V3、ITIL V3 2011 Edition とわけて表記します。

この後に、単に JIS Q 20000 と表記する場合は JIS Q 20000-1:2012 を意味します。

JIS Q 20000 は、序文に続いて 9 つの箇条からなる構成をとっています。

表 7-5　JIS Q 20000-1:2012 構成

序文 1. 適用範囲 2. 引用規格 3. 用語及び定義 4. サービスマネジメントシステムの一般要求事項 5. 新規サービス又はサービス変更の設計及び移行 6. サービス提供プロセス 6.1 サービスレベル管理 6.2 サービスの報告 6.3 サービス継続及び可用性管理 6.4 サービスの予算業務及び会計業務 6.5 容量・能力管理 6.6 情報セキュリティ管理	7. 関係プロセス 7.1 事業関係管理 7. 2 供給者管理 8. 解決プロセス 8.1 インシデント及びサービス要求管理 8.2 問題管理 9. 統合的制御プロセス 9.1 構成管理 9.2 変更管理 9.3 リリース及び展開管理 参考文献

JIS Q 20000 は、次の 4 部に分けて読むと理解し易いでしょう。

- 箇条 1：JIS Q 20000 が適用される対象を記述
- 箇条 3：JIS Q 20000 で使用される用語を説明
- 箇条 4：マネジメントシステムに必要な要件と、PDCA について記述
- 箇条 5 以降：JIS Q 20000 で必要とされるプロセス群を記述

表 7-6 で、JIS Q 20000 の箇条の概要を示します。箇条 1 と箇条 3 については、既にそれぞれ本ガイドの 3 章と 2 章で解説されていますので、本章では「箇条 4 サービスマネジメントシステム」と「箇条 5 以降：IT サービスマネジメントのプロセス」について、ITIL V3 との違いを述べることにします。

表 7-6　JIS Q 20000 の概要

箇条		題	概　　要
1		適用範囲	JIS Q 20000 の適用範囲（スコープ）や補足的説明
2		引用規格	
3		用語及び定義	JIS Q 20000 の用語と定義（37 項目）

4		サービスマネジメントシステムの一般要求事項	経営陣／文書化／力量、認識及び教育・訓練の視点で、効果的なマネジメントシステム構築の方針や枠組み。他の関係者が運用するプロセスのガバナンス。
5		新規サービス又はサービス変更の設計及び移行	サービス又は事業に重大な影響を与える可能性のある新規サービス又はサービス変更に対する計画、設計、開発、移行を担うプロセス。サービスの廃止、移管も対象。
6	6.1	サービスレベル管理	サービスレベルの管理（サービスレベル設定、レビュー、変更）
	6.2	サービスの報告	サービスマネジメントに対するサービス実施に関する報告書を作成
	6.3	サービス継続及び可用性の管理	平常時における可用性に関係する「可用性の管理」と災害等発生時の管理を行う「サービス継続の管理」
	6.4	サービスの予算業務及び会計業務	IT サービスに関するコストと予算、会計処理を管理
	6.5	容量・能力管理	顧客からの事業上の要求事項、IT サービス、リソースの 3 つの視点で容量・能力を管理
	6.6	情報セキュリティ管理	IT サービスのリスクを分析し管理（ISMS の要求事項を要約）
7	7.1	事業関係管理	サービス提供者と顧客の関係をサービスレベル、苦情処理、顧客満足度の 3 つの視点で管理
	7.2	供給者管理	サービス提供者（プロバイダ）と供給者（サプライヤ）の管理
8	8.1	インシデント及びサービス要求管理	インシデント及びサービス要求を管理し、事業及び顧客の優先度に従って管理
	8.2	問題管理	インシデントの根本原因を特定するリアクティブな活動とインシデント発生前に解決するプロアクティブな活動で問題を管理
9	9.1	構成管理	サービスおよびインフラストラクチャを構成品目（CI）として管理
	9.2	変更管理	全ての構成品目（CI）の変更をレビュー、承認することにより、変更を管理・コントロール
	9.3	リリース及び展開管理	全ての構成品目（CI）のリリースを管理

ITIL V2 の利用者にとってなじみの深いプロセス群は箇条 5 以降（特に箇条 6 以降）に配置されています。

箇条 5 以降の目次構成を見ただけで、直ちに ITIL V2 との対応関係を読み取れる読者も多いでしょう。実際、ISO/IEC 20000:2005（JIS Q 20000:2007）は、BS 15000 として知られていた英国規格が国際標準化されたものですので、ITIL V2 も ISO/IEC 20000:2005（JIS Q 20000:2007）も同じ英国出身と考えてよいでしょう。ITIL V2 と JIS Q 20000:2007 においては、両者の親和性はよく、図 7-3 に示す対応関係をつけることができます。

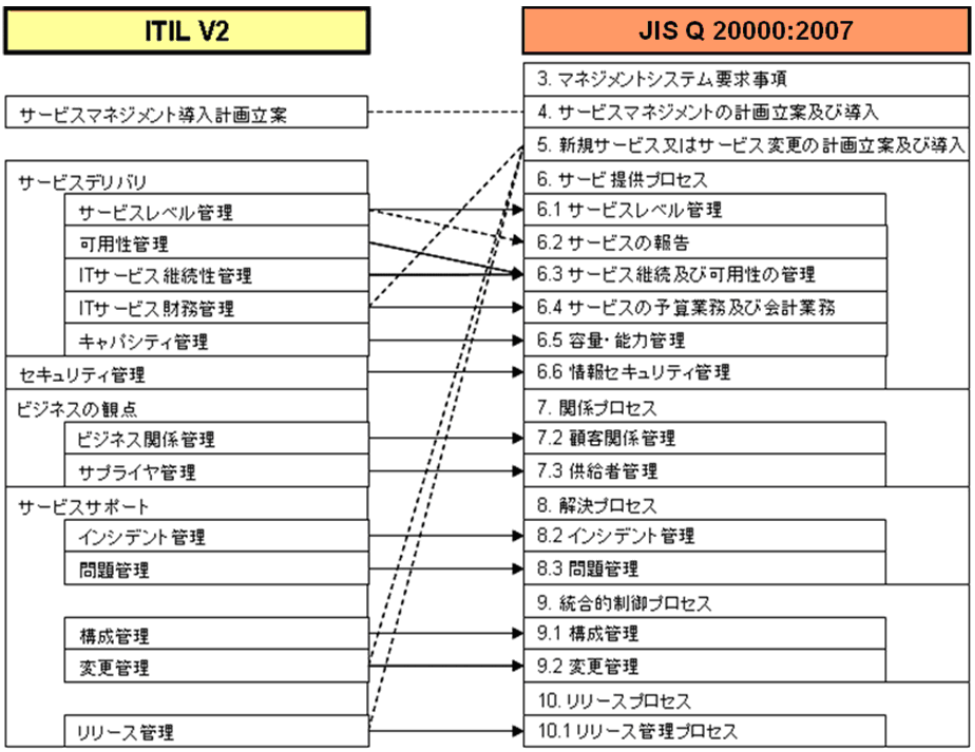


図 7-3　ITIL V2 と JIS Q 20000:2007 の対応

次は、現行の最新版である JIS Q 20000:2012 を中心に、こちらも最新版である ITIL V3 2011 Edition との関係を見ておくことにしましょう。JIS Q 20000 では箇条 5 から箇条 9 までに 14 のプロセスが定義されています。前掲の表 7-3 に示したように、ITIL V3 2011 Edition ではサービスのライフサイクルに沿って 26 のプロセスが定義されています。ITIL V2 で馴染みのプロセスは全て包含されていますが、多くのプロセスが追加されています。図 7-3 の JIS Q 20000:2007 と ITIL V2 の対応表では直接的に関連づけされる代表的なプロセスをあげています。実装の場においては、ある箇条の要求事項を実現するプロセスとしては、ここに挙げているプロセスだけでなく、他のプロセスも必要とする場合があることに留意しておく必要があります。

表 7-7　JIS Q 20000 と ITIL V3 2011 Edition との関連

JIS Q 20000（ISO/IEC 20000:2011 年版）と ITIL V3 2011 Edition との関連		
箇条	**JIS Q 20000**	**ITIL V3 2011 Edition**
4	サービスマネジメントシステムの一般要求事項	ITIL V3 は、サービスのライフサイクルに焦点をあてていますが、マネジメントシステムに関する記述は少なく、箇条 6 以降のように直接に対応づけられるプロセスはありません。箇条 4 と強い関連を持つプロセスとしては、IT サービス戦略管理（SS）、サプライヤ管理（SD）、サービスレベル管理（SD）などがあります。

5	新規サービス又はサービス変更の設計及び移行	ITIL V3 には箇条 5 に直接に該当するプロセスはありません。さまざまなプロセスが箇条 5 を担当しますが、その中でも、デザイン・コーディネーション（SD）や変更管理（ST）とリリース管理および展開管理（ST）をはじめとするサービストラジションに含まれるプロセスの多くが、箇条 5 の要求事項の実現に役立ちます。
6.1	サービスレベル管理	サービスレベル管理（SD）
6.2	サービスの報告	対応するプロセスとしてはありません。ITIL V3 ではすべてのプロセスに測定と報告は組み込まれているという考え方です。
6.3	サービス継続及び可用性管理	IT サービス継続性管理（SD） 可用性管理（SD）
6.4	サービスの予算業務及び会計業務	IT サービス財務管理（SS）
6.5	容量・能力管理	キャパシティ管理（SD） 需要管理（SS）
6.6	情報セキュリティ管理·	情報セキュリティ管理（SD）
7.1	事業関係管理	事業関係管理（SS）
7.2	供給者管理	サプライヤ管理（SD）
8.1	インシデント及びサービス要求管理	インシデント管理（SO） 要求実現（SO）
8.2	問題管理	問題管理（SO）
9.1	構成管理	サービス資産管理および構成管理（ST）
9.2	変更管理	変更管理（ST）
9.3	リリース及び展開管理	リリース管理および展開管理（ST）

7.3. サービスマネジメントシステム（SMS）と PDCA

JIS Q 20000 においては、箇条 5～箇条 9 で示されるサービスマネジメントのプロセス群と箇条 4 で定義されるサービスマネジメントシステムに PDCA の方法論を適用します。次の図で示されるように、全体的な視点で管理するサービスマネジメントシステムとサービスマネジメントのプロセス全体に、改善サイクルを回す PDCA の考え方がかかっていると考えてよいでしょう。

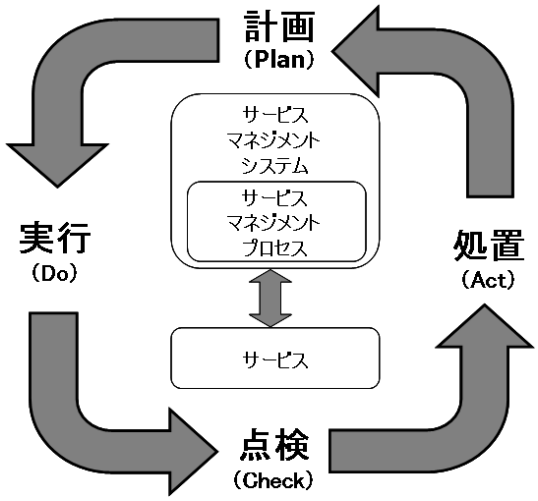


図 1 － サービスマネジメントに適用される PDCA 方法論
（JIS Q 20000-1:2012　0.2 サービスマネジメントシステム要求事項　より引用）

既にみたように、箇条 4 に明示的に対応する記述は ITIL V2 にも ITIL V3 にもありません。このことは ITIL ではマネジメントシステムや改善サイクルが軽視されているということを意味しているのではありません。ITIL では ISO/IEC 20000 のように、まとまった記述がされていないと考えた方がよいでしょう。一方、箇条 6 以降の IT サービスマネジメントのプロセス（箇条 5 については明確な対応付けがみられない）の規定内容は、ITIL V2 あるいは ITIL V3 において明確に対応するプロセスがあります。ITIL ユーザは、箇条 4 をじっくり読むことで JIS Q 20000 と ITIL の端的な違いを理解することが出来るでしょう。

サービスマネジメントシステム（SMS）

箇条 4 は、『サービスマネジメントシステムの一般要求事項』と題されています。

マネジメントシステムの「規格」であるという点では、JIS Q 9001（品質）も JIS Q 27001（情報セキュリティ）もそうであり、あるいは JIS Q 14001（環境）とも共通します。その共通部分が、JIS Q 20000 の場合には箇条 4 に書かれていると考えてよいでしょう。JIS Q 20000 ではサービスマネジメントシステム（SMS）を新たに用語（3.31）として定義しています。

箇条 4 では、PDCA“計画（Plan）－実行（Do）－点検（Check）－処置（Act)”について述べています。

計画（Plan）： SMS を確立し，文書化し，合意する。SMS には，サービスの要求事項を満たすための方針，目的，計画及びプロセスが含まれる。
実行（Do）：サービスの設計，移行，提供及び改善のために SMS を導入し，運用する。
点検（Check）：方針，目的，計画及びサービスの要求事項について，SMS 及びサービスを監視，測定及びレビューし，それらの結果を報告する。
処置（Act）： SMS 及びサービスのパフォーマンスを継続的に改善するための処置を実施する。
（JIS Q 20000-1:2012　0.2 サービスマネジメントシステム要求事項　より引用）

PDCA の各フェーズに対応した箇条 4 内の細分箇条は表 7-8 のとおりです。

表 7-8　PDCA と箇条 4

PDCA の各フェーズ	箇条 4 の細分箇条
計画（Plan）	4.5.2 SMS の計画
実行（Do）	4.5.3 SMS の導入及び運用
点検（Check）	4.5.4 SMS の監視及びレビュー
	4.5.4.1 一般
	4.5.4.2 内部監査
	4.5.4.3 マネジメントレビュー
処置（Act）	4.5.5 SMS の維持及び改善
	4.5.5.1 一般
	4.5.5.2 改善のマネジメント

IT サービスマネジメントのプロセス

箇条 5 以降で記述されている合計１４のプロセスのうち、箇条 5 の新規サービスまたはサービス変更の設計及び移行を除けば、ITIL ユーザにとってはなじみの深いものでしょう。

箇条 5 から箇条 9 までの規格の概要は、付録Ａに掲載しました。ITIL ユーザにとって付録Ａは、自身の ITIL 知識を背景に JIS Q 20000 を読み取る助けとなるでしょう。

ITIL に関する一般的な解説および、JIS Q 20000 のより詳細な説明は『ITSMS ユーザーズガイド- JIS Q 20000 （ISO/IEC 20000）対応 -』をご参照ください。

7.4. ITIL と JIS Q 20000 の利用

ITIL および JIS Q 20000 に取組む際の、利用の違いを整理します。

ITIL の利用

ITIL はベストプラクティスですので、適用を考えている組織に合わせて、必要と思われるところから取組むというスタイルが一般的であり、取組みの深さ自体も自分で決めることが出来ます。

ITIL は V2 であれ V3 であれ、IT サービスマネジメントに必要となる基本のプロセスに変わりがあるわけではありません。ITIL への取り組みには、次のような特徴があることになります。

- 何に取組むかを決めることができる
- どれくらいの深さまで取組むか、決めることができる

この特徴を逆に表現すると、「必ずしも全てのプロセスを同時に、しかも ITIL 書籍に書かれていること全てを完璧に実施する必要はない」ということになります。そのため ITIL では、取組みの次ステップでは「深掘り」と「横展開」がテーマになります。

またこれらの特徴から、ITIL では「ITIL に取組んでいる」という表明では、“ITIL の何をどこの深さまでやっているか”についての補足をする必要が出てきます。

JIS Q 20000 の利用

JIS Q 20000 で規定されるプロセスを組織に適用する際には、以下の 2 つが考えられます。

① あくまでも JIS Q 20000 を参考として使用する

② JIS Q 20000 に対する適合を宣言する

①の場合は、これは ITIL と同じ利用と言えます。JIS Q 20000 に書かれた内容の中から、組織の事情に合ったものを適用していきます。但し JIS Q 20000 は、ITIL のサブセットであると言うこともできますので、①の方法は ITIL への取組みと何ら変わらないとも言えるでしょう。

一方の②の利用では、最初から規定された全ての内容に取組むことが求められます。ITIL の利用では、適用の対象としていないプロセスが ITIL に沿っていなくても、あるいはあえて ITIL に沿っていないプロセスを残したとしても、問題にはなりません。ところが JIS Q 20000 ではそういうわけにはいかないのです。②を目指すのであれば、JIS Q 20000 の全ての要求事項に従わなければ、目的を叶えること（すなわち JIS Q 20000 認証を受けること）は出来ません。ここで JIS Q 20000 には、必要最小限のことが書かれているということを思い出してください。要求事項を満たしてさえいれば、それ以上のことは求められません。

- 全てに取組んでいなければならない
- 規定を満たしている限りにおいて、それぞれの取組みは深くても浅くてもよい

このような特徴から、JIS Q 20000 の②の利用では、最初は薄皮のように全て取組みます。そして PDCA サイクルを回す過程で、改善していくことになります。その改善のステップでは「深掘り」がテーマになります。

ITIL と JIS Q 20000 の利用の補完

ITIL の利用では、クィック・ウィンの得られる領域に対して自分たちのペースで取組むことができます。IT 部門などで IT システム運用を地道に改善する場合に向いている方法と言えるでしょう。ITIL においては、現場に合わせてベストプラクティスベースの IT システムを実現することを第一に考えます。その先に、ITIL の全範囲をカバーするという全体像が見えてきます。この方法においては、積み重ねた実績を元に、最終的にはその証明となる JIS Q 20000 認証に取組むという道筋が望ましい姿でしょう。

しかし気をつけるべきことは、認証取得のための活動だけがメインになってしまうと、現場の運用が取り残される危険性もあるということです。IT システムは、ITIL 書籍の最初に説明されているように「IT こそがビジネスであり、ビジネスは IT そのものである」ことから、現場との乖離は致命傷になりかねません。「認証」取得に振り回されすぎないようにしたいものです。

一方の JIS Q 20000 利用では、その特徴である「網羅性」をうまく活用できる一つの可能性がクローズアップされてきています。

財務報告に関する不正行為を根本的な方法で防止するために、会計データ等が IT システム上で扱われている段階からコントロールしようという動き、いわゆる「内部統制」という取組みがあります。こうした要請に対しては、漏れなくコントロールしているということを証明するために、何はともあれまず「網羅性」を確保するということが重要視されるものです。

以上をまとめると、IT システム運用の改善というテーマで、2 つのルートを設定することができそうです。第一は「クィック・ウィン」重視型であり、もう一つは「網羅性」重視型です。

IT システム運用上の問題がはっきりしているようなケースでは、「クィック・ウィン」重視型が向いています。例えば IT サービスにおける問い合わせ対応で、問い合わせがきちんと質問者に戻っていないというような状況が発生している場合は、問題の発生箇所が比較的明確なため、窓口業務に絞って改善活動を進めれば大きな効果が得られると考えられます。このような場合には、現場の改善活動の延長からスタートさせることが可能な ITIL を用いた利用が適しています。

一方の「網羅性」重視型に取組む動機としては、内部統制対応のようなケースが考えられます。IT システム運用の統制について、どういった考えで行っているのか、漏れなくカバーしているかどうかということが問題となります。このケースでは、JIS Q 20000 を考え方の中心にすえた利用が適しています。特に海外展開を果たしている企業・組織にとっては、JIS Q 20000 が「国際規格」であることが有利にはたらくでしょう。

ここで「教科書的用法」と「参考書的用法」というものを考えてみましょう。「教科書的用法」とは、対象文献（JIS Q 20000 の規格書や、ITIL 書籍）を“教科書”とみなして使い、極力これに沿った運用環境を構築していくことと定義します。一方、「参考書的用法」は対象文献を“参考書”として扱い、困った時に参照するだけにとどめようとする方法としてみましょう。

「教科書的用法」では、対象文献に書かれたこと全部がそっくりそのまま実現されることを目指します。「参考書的用法」は対象文献をあくまでも参考にするだけですから、部分的に実現されるだけです。

- 教科書的用法：教科書として読み砕き、現実に合わせて適用していく方法
- 参考書的用法：問題が発生した時に参考書として使い、その部分の改善に適用する方法

教科書的用法は、トップダウンで仕組みを導入する時には向いていると言えるでしょう。JIS Q 20000 の利用に適した方法と考えてよさそうです。ITIL でももちろん教科書的用法は使えますが、書籍のボリュームが膨大であるため、簡単にはいかない可能性が高いと考えられます。特に、ITIL V3 のライフサイクルアプローチでは、V2 の 10 のプロセスと 1 つの機能から 26 のプロセスと 4 つの機能へと、大幅にプロセス、機能が追加されています。教科書的用法を取ろうとしても、どこから手をつけて良いのかを判断するのに迷うかもしれません。

一方の参考書的用法は、ある意味日本的な、現場主導のやり方と言えます。大きなコストはかからないという利点が考えられますが、この方法で ITIL の全プロセスをやり抜くのは難しいかもしれません。それは IT システム運用が、要員の業務定義や組織の変更を伴う場合が考えられるからです。こうしたケースでは参考書的な用法でスタートし、成果を少しずつ出すことでトップの理解を得、いずれどこかの時点でトップダウン的な利用に移行するのが現実的と考えられます。

8. ソフトウェア資産管理と IT サービスマネジメント

8.1. はじめに

IT サービスマネジメントを実践している組織が、そのプロセス中にソフトウェア資産管理（以下 SAM とする） を統合して、運用しているケースは少ないように思われます。同様に、SAM の全体あるいはライセンス管理のプロセスを実装している組織が、IT サービスマネジメントのプロセスを意識して活動しているケースも多くないように思われます。この章では、IT サービスマネジメントと SAM の関係を解説する事で、IT サービスマネジメントを実践されているサービス提供者に、SAM を統合してゆく一助になることを目的としています。

8.2. SAM の定義

IT サービスマネジメントのデファクトスタンダードとして知られる ITIL では、資産を管理するプロセスとして IT 資産管理を備えています。IT 資産管理は、ITIL V2 および V3 においては、プロセスとして存在していますが、SAM は明確な形で扱われていません。

SAM は、ITIL V2 の 7 冊のコア書籍に対する補完書籍という位置付けで、単独の書籍として存在していました。SAM 書籍は、ITIL V2 フレームワークを補完する書籍としながらも、ITIL のコア書籍であるサービスサポート （2000 年発行）、サービスデリバリ （2001 年発行）、アプリケーション管理（2002 年発行）、サービスマネジメント導入計画立案（2002 年発行）の中核書籍に遅れることなく、2003 年に発行されています。

ITIL の SAM 書籍では、ソフトウェア資産管理を次のように定義しています。

> SAM の定義
> SAM（ソフトウェア資産管理）は、組織内のソフトウェア資産のライフサイクル全ステージを通じて、効果的な管理、制御、および保護のために必要なインフラストラクチャとプロセスの全てである。
>
> 出典：ITIL 書籍 『Software Asset Management』 TSO 刊を基に作成）

定義における、“管理、制御、および保護”の意味するところは、ソフトウェア資産の持っている特徴をよく表しているでしょう。すなわち、ソフトウェア資産を管理する上での重要なテーマの一つであるライセンス管理を想起させます。ライセンス管理を実践することはコンプライアンス（法令遵守）につながることから、ソフトウェア資産をライフサイクルにわたり“管理、制御、および保護”することは必須といえます。

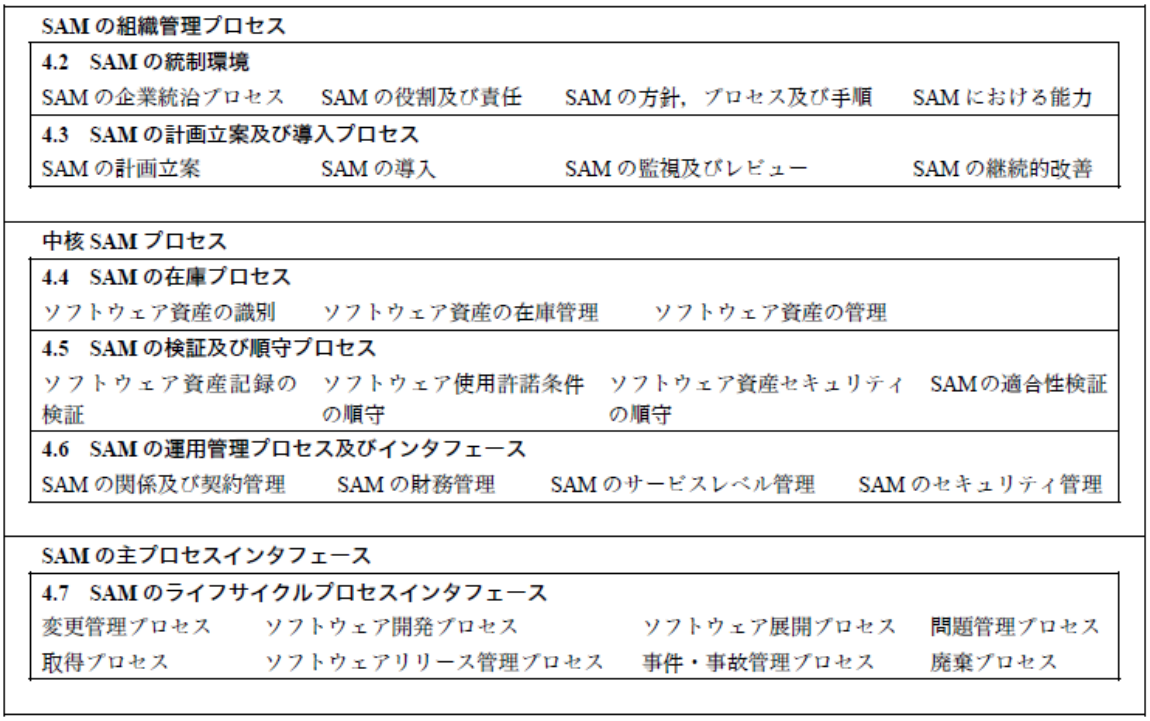
ITIL V2 のコア書籍においては、IT サービスを顧客/利用者に提供するために必要なプロセス群のベストプラクティスが中心であり、ソフトウェア資産について、ライフサイクルを通じて“管理、制御、および保護”するためのプロセス群は扱われていません。SAM の定義では、必要なインフラストラクチャも含まれるので、SAM はソフトウェア資産の管理に係るハードウェアと、（ライセンスを含んだ）ソフトウェアを扱うプロセス群のすべてを指していることになります。

8.3. SAM のプロセス

SAM の国際規格である ISO/IEC 19770-1 （以下 SAM 規格とする） は 2006 年に制定されまし

た。SAM 規格は、ソフトウェア管理に必要とされる一連のプロセス群を規定しています。ソフトウェア資産をプロセスのもとで管理する ITIL V2 の SAM 書籍と目的は同じです。SAM 規格の発行を受けて、我が国において JIS 化が推進され、2010 年に JIS X 0164-1 の国内規格として発行されました。JIS X 0164-1 では SAM のプロセス群を次のように 3 つの領域に分類しています（図 8-1 参照）。

a) SAM の組織管理プロセス
b) 中核 SAM プロセス
c) SAM の主プロセスインタフェース



（JIS X 0164-1:2010 ソフトウェア資産管理　より引用）

図 8-1　SAM プロセスの枠組み

8.4. IT サービスマネジメントと SAM の関係

JIS X 0164-1 の解説には次のような表現があります（ISO/IEC 19770-1:2006 では序文にあります）。

> この規格は，JIS Q 20000 規格群と緊密な整合をとり，また，それを支援するように意図されている。
>
> （JIS X 0164-1:2010 ソフトウェア資産管理　より引用）

独立した規格が他の規格を支援するというのは、少々違和感を覚えますが、規格の箇条において、次のように上記の序文を補足しています。

4.1.1 定義及びサービスマネジメントとの関係
ソフトウェア資産管理とは，組織内のソフトウェア資産の有効な管理，制御及び保護をいう。
この規格が定義する SAM のプロセスは，JIS Q 20000 規格群が定義している情報技術（IT）サービスマネジメントとよく両立するように構成されており,それを適切に支援することを意図している。
（JIS X 0164-1:2010 ソフトウェア資産管理　より引用）

SAM のプロセス群が、JIS Q 20000 規格の定義する IT サービスマネジメントとよく両立するように構成されており、それを適切に支援することを意図していると述べています。

JIS Q 20000 は ISO/IEC 20000 を基に制定された国内規格です。また、ISO/IEC 20000 は IT サービスマネジメント（ITIL）と整合し、補完している規格とされています。このことから、SAM 規格で定義されるプロセス群が JIS Q 20000 規格で定義している IT サービスマネジメントのプロセスと緊密に整合する事は、ITIL にも整合していると考えても良いでしょう。

とりわけ、下記の箇条 4.7 の 4.7.1 一般において、SAM 規格の中で定義されている SAM のライフサイクルプロセスインタフェース は、明示的に JIS Q 20000 のプロセスと整合が取られているとしています。

4.7 SAM のライフサイクルプロセスインタフェース
4.7.1 一般
“SAM のライフサイクルプロセスインタフェース”は，SAM との関連では，JIS X 0160 での主ライフサイクルプロセス及び JIS Q 20000 規格群のプロセスとほぼ整合がとられている。
（JIS X 0164-1:2010 ソフトウェア資産管理　より引用）

SAM 規格でのライフサイクルプロセスとは、次のプロセス群です。

a) 変更管理プロセス
b) 取得プロセス
c) ソフトウェア開発プロセス
d) ソフトウェアリリース管理プロセス
e) ソフトウェア展開プロセス
f) 事件・事故管理プロセス
g) 問題管理プロセス
h) 廃棄プロセス

変更管理、リリース管理、展開、問題管理などのプロセスと JIS Q 20000 の同名のプロセス群が緊密に整合する関係があることは容易に想像できるでしょう。

SAM 規格は Asset （資産） を扱う事から、IT サービスマネジメントのプロセスの中で最も関連が深いプロセスは構成管理であることは明白ですが、SAM 規格では構成管理との関係について、

次のように述べています。

> “SAM の在庫プロセス”は，SAM の基本であるだけでなく，すべての構成管理の基本である。すべての IT 資産（ソフトウェア及び関連資産だけではない。）及びこれらの資産すべての間の関係を対象にする限りにおいて，更に非 IT 資産も含んでよいことから，構成管理は，SAM の適用される範囲を超える。IT サービスマネジメントのすべてを含むプロジェクトでは，“SAM の在庫管理プロセス”が構成管理の一部とみなされることもある。
>
> （JIS X 0164-1:2010 ソフトウェア資産管理　より引用）

構成管理の適用範囲は “SAM 在庫プロセス”における適用範囲を包含することを述べています。“SAM の在庫プロセス”とは、次のプロセスで構成されています。

a) ソフトウェア資産の識別
b) ソフトウェア資産の在庫管理
c) ソフトウェア資産の管理

8.5. SAM と ITIL V3

2007 年に ITIL V2 はそれまでのプロセスベースのガイダンスから、サービスのライフサイクルに焦点を当てた ITIL V3 へ改訂されました。ITIL V3 はライフサイクルアプローチを取ることで、SAM に必要なプロセス群の多くを包含した形となっています。

また、ITIL V2 では、セキュリティ管理は別の書籍として存在していましたが、ITIL V3 ではプロセスの一つとして取り込まれています。ITIL と SAM の関係は、主として、資産と構成管理にあります。ITIL V3 のプロセスの中では、サービス資産および構成管理プロセス （Service Assent and Configuration Management: 以下 SACM とする） 、リリース管理および展開管理プロセス、財務管理プロセスの 3 つのプロセスが SAM と重要な関係にあります。

3 つのプロセスの中で注目すべきプロセスは SACM です。SACM は適用範囲としてサービス資産を扱います。ITIL V3 用語集によれば、サービス資産は次のように定義されています。

> サービス資産
>
> サービス・プロバイダのあらゆる能力またはリソース。サービスの提供に寄与する可能性があるすべてのものが含まれる。
>
> 資産
>
> 任意のリソースまたは能力。資産は、マネジメント、組織、プロセス、知識、人材、情報、アプリケーション、インフラストラクチャ、金融資本のいずれかのタイプになりうる。
>
> （ITIL V3 用語集　より引用）

ITIL V3 の SACM は、 “サービス資産”を“あらゆる資産”と読み替えることができるので、“SAM の在庫プロセス”の適用範囲であるソフトウェア資産を超えるものであることが理解できるでしょう。

SACM は次のような特徴を持っています。

- SACM はサービストランジションの主要プロセスのひとつ。資産とそれに関連するライフサイクルを管理するだけではなく、資産間のリンクと関係も管理する。
- インシデント、問題と変更、サービスと SLA のような、他のサービス管理に関連する問題と資産との関連を管理する。
- SACM の主要な役割は物理的なソフトウェア資産の管理である。
- メディア、ライセンス及び真正性を示す文書類の制御。

SACM プロセスでは SAM を抱合している事が、より明白に述べられていることが理解できるでしょう。SAM は ITIL V3 のライフサイクルのすべての段階とインタフェースを持っていますが、資産と構成情報の管理は、ライフサイクルのサービストランジションとサービスオペレーションのステージにおける役割の一部として考えることができます。

SACM はサービストランジションの主要なプロセスの一つですが、SAM にとって重要な意味を持ちます。SCAM は資産とそれに関連するライフサイクルを管理するだけでなく、資産間のリンクと関係も管理します。また、SACM は、これらの資産と、インシデント、問題、変更、サービスおよび SLA のような、サービスマネジメントに関連する課題との関係を管理することも含んでいます。

組織の物理的な資産管理は、SACM の重要な役割の一つであると考えられます。従って、メディア、ライセンス及び真正性の文書のコントロールが、このプロセスに与えられています。ITIL では、資産管理の財務的側面は IT 財務管理プロセスの適応範囲内であり、別けて論じられます。

SAM 内の資産管理はこれらのすべての側面を含みます。SAM に含まれる一般的な資産管理プロセスには次のものを含んでいます。

- ソフトウェア資産のすべての側面の管理
- 関連するハードウェア資産の管理、SAM に必要不可欠な拡張
- ライフサイクルの全てのステージを通じたソフトウェアコンポーネントのコントロールと管理
- ソフトウェア真正性文書とライセンスの管理
- 調達とソフトウェア契約文書の管理
- すべてのマスターソフトウェアメディアの保管と管理
- すべての設置済みのソフトウェアコピーのコントロールと管理
- 全ての上記側面の間の関係の管理
- CMDB の内容で、何が現実世界で利用されているのか、つまり、実際の稼働環境で使用されているのものと、DML の内容との定期的な調整

注：CMDB（Configuration Management Data Base：構成管理データベース）

DML（Definitive Media Library：確定版メディアライブラリ）

8.6. SAM に関連する ITIL プロセス

ITIL V3 の主要な段階とプロセスにおいて、SAM に関連し支援する役割を持つプロセスには、次のようなものがあります。

■サービスストラテジ

SAM 戦略は、組織の全体的なサービス戦略の必須部分を形成します。ソフトウェアのソーシングとソフトウェアパートナーの選別は、ICT 組織における全体的な戦略の重要な要素です。

他の重要な戦略的な領域は、資産管理プロセスです。資産管理プロセスは、ICT に関連したファイナンスとコストの管理とコントロールに責任があります。すべてのソフトウェアの調達と実際の支出の詳細は、資産管理プロセスにより収集され、解析されなければなりません。これには、財務コストモデルへの組み込みのために、すべてのサポートとメンテナンス契約が含まれます。

■サービスデザイン

サービスライフサイクルのこの段階の主要なプロセスはつぎのとおりです。

サービスレベル管理プロセス：

このプロセスでは、すべての顧客とユーザの役割と責任が SLA で合意され文書化されることを確実にしなければなりません。条件はすべての SLA の詳細に含まれていなければなりません、すなわち、すべての ICT システムのユーザは、ICT システムを利用し ICT サービスにアクセスする前に、ソフトウェア、セキュリティ、インターネット利用の組織のポリシーにより、受け入れて、合意して、署名して、従わなくてはなりません。

可用性管理プロセス：

可用性管理プロセスは、サービス、コンポーネントの可用性あるいは非可用性の問題を起こすことに対して関係する、すべてのソフトウェア資産に関与するかもしれません。

IT サービス継続性管理プロセス（ITSCM）：

このプロセスでは次の事を確実にする必要があるでしょう。すなわち、すべての回復及び継続性の計画が、組織中で利用しているすべてのソフトウェアにたいして実施されています。そのため、SAM プロセス群は、ITSCM のプロセスに、すべての新規あるいは変更されたソフトウェアを通知すべきです。

また、ITSCM は、すべてのスタンバイ及びリカバリーサイトとシステムにおける SAM の問題が対処されたことを確実にするべきです。

セキュリティ管理プロセス：

このプロセスでは、リスクのアセスメント、軽減処置と対策の実装を支援するでしょう。また、セキュリティ管理プロセスでは、すべてのソフトウェアの例外と法令違反の検出、アラート、エスカレーションを支援するべきです。

サプライヤ管理プロセス：

このプロセスでは、ソフトウェア、ソフトウェアパートナー及びベンダーに関連する契約とサプライヤに関するすべての課題の管理を支援します。

■サービストランジション

SACM プロセスに加えて、サービスライフサイクルの段階の主要なプロセスはつぎのとおりです。

変更管理：

ITIL に対応している組織においては、ICT 環境におけるすべての変更の管理とコントロールに関して責任があります。

ソフトウェアを含むすべての変更は、SAM のプロセスに対する影響を分析すべきです。変更においては、SAM のプロセスのすべての要求事項が満足されていて、CMDB の更新とライセンス遵守に関しては、ライフサイクルの段階を通して確実に管理されるべきです。効果的な変更管理のオペレーションは、SAM プロセスの成功には極めて重要です。

リリース管理プロセスおよび展開管理プロセス：

このプロセスは、ITIL に対応している組織において、実環境へのソフトウェアの物理的なコントロール、展開及び実装に責任があります。

■サービスオペレーション

サービスライフサイクルのサービスオペレーションの段階における主要なプロセスは、次のようなものです。

サービスデスク、インシデント管理プロセス、要求実現プロセス：

ITIL に対応している組織においては、ICT サービスとシステムのすべてのユーザに単一窓口の提供をする責任があります。

サービスデスクとインシデント管理においては、すべてのインシデント、課題、問い合わせ、要求、案内を管理し、解決と修正あるいはエスカレーションのために、すべてのソフトウェア資産、ライセンスとそれらの利用に関連するすべての例外的な事が、ただちに SAM プロセス群に報告されることを確実にしなければなりません。

イベント管理プロセス：

ITIL に従う組織では、このプロセスは効果的な SAM プロセスのための、すべてのタイプのイベント管理に対する責任と、重要な支援を提供する事ができます。

問題管理プロセス：

ITIL に対応している組織においては、インシデントの根本原因を分析し、問題とそれに続く予防に対して責任があります。

SAM は問題管理プロセスと共に、すべての SAM に関する例外が、予防的に再発防止のために解析されることを確実にするために活動すべきです。

■継続的サービス改善

ライフサイクルのこの段階では、SAM プロセスの継続的改善のためのフレームワークとアプローチを提供するべきです。SAM がサービスマネジメントプロセスの効果的な測定と改善の主要な統合部分として捉える事は必要不可欠です。

8.7. ISO/IEC 19770-1 の改訂

2012 年 6 月に SAM 規格が改訂され第 2 版と置き換えられました。SAM 規格で扱われている 27 プロセスの成果（outcome）を 4 段階（Tier）にマッピングしています。こうすることで、組織が SAM の導入に際して、段階的なアプロ―チを取ることを可能にしています。（図 8-2）

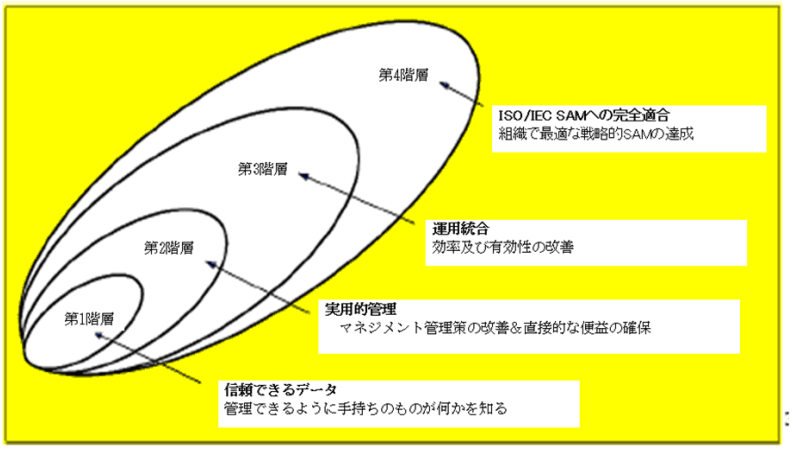


図 8-2　SAM の 4 つの段階

各段階は次のように定義されています。

- 第 1 段階：信頼できるデータ

  この段階では、管理できるようにするデータは何かを知ることを意味しています。“知らないことは管理できない”ということであり、ライセンスの順守を実証するための基礎となります。

- 第 2 段階：実用的管理

  この段階の達成は、マネジメント管理策の改善及び直接的な利点の確保を意味します。方針、役割及び責任など、基本的なマネジメント統制環境を扱います。

- 第 3 段階：運用統合

  この段階では効率及び有効性の改善を意味します。この段階では、前の 2 つの段階を基礎として SAM の運用プロセスへの統合を推進します。結果として、効率及び有効性が改善されます。

- 第 4 段階：SAM への完全適合

  この段階の達成は、最高の戦略的 ISO/IEC SAM の達成を意味します。組織の戦略計画への完全統合を含めて、完全な SAM のうち、より高度な、過大な労力を要する側面を取り扱います。

8.8. まとめ

IT サービスマネジメントを実践しているサービス提供者にとっては、SAM を構築する場合、新たにプロセスを導入する必要はありません。既存の運用プロセスを SAM に合わせて変更し、改善を加えてゆけば良いでしょう。

ITIL V2 での基本的な原則とプロセスは ITIL V3 に包含されています。ITIL V2、V3 の SAM 書籍から SAM 規格にいたるまで、一貫して IT サービスマネジメントと SAM で定義されているプロセス群は密接に関係し、整合しているのです。

- SAM は IT サービスマネジメントと緊密に整合が取られている。
- SAM が対象とする適応範囲は、IT サービスマネジメント（ITIL V3）のサービス資産および構成管理プロセスにおける適応範囲に含まれる。
- SAM を実践・構築する事は、ソフトウェアの管理性を高めると共に、IT サービスマネジメントへの貢献となる。

IT サービスマネジメントを実践されているサービス提供者の方々にとって、SAM を身近なプロセスとして感じていただき、SAM のプロセス群を構築する際の一助となれば幸いです。

付録Ａ　JIS Q 20000-1 細分箇条の概要

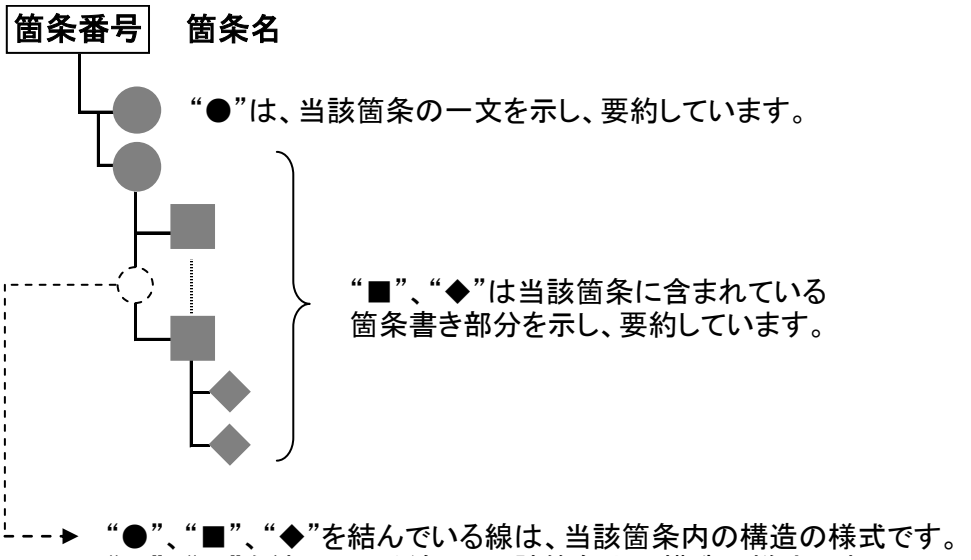
箇条 5 以降の各プロセスの細分箇条を、凡例に記載の項目に沿って説明しています。

凡例：

箇条の名称（箇条の番号）

- 各箇条でのポイント（プロセスとしてみた時の活動項目）を列挙
- ：

※各箇条を大づかみに理解するため、箇条ごとの構造を図示しています。



【インプット】	【アウトプット】
・プロセスとしてみた時の、各箇条から読み取れる、プロセスに対する「入力」を列挙	・プロセスとしてみた時の、各箇条から読み取れる、プロセスからの「出力」を列挙

特記

・ITIL ユーザが注意すべき留意点など

：

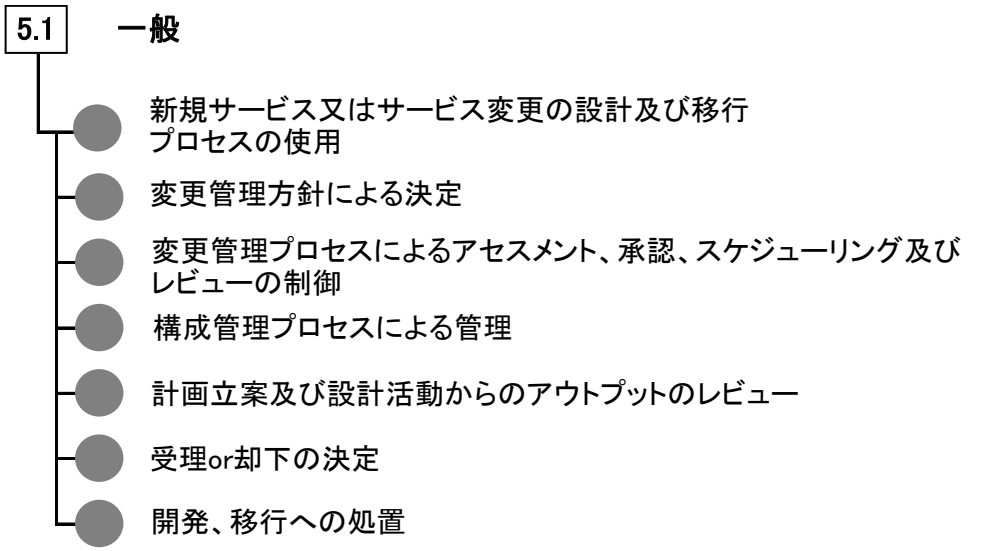
<u>注意</u>

一般にプロセスは繰り返し実施されるので、初回のみに生成されるアウトプットが次回以降はインプットの項目に挙げられることが起こります。規格の箇条では、こういった時間推移まで考慮した記述でないため、インプット／アウトプットにおいて一見奇妙に思われる箇所があります（例えば、サービスの存在が前提となるサービスレベル管理のアウトプットに「サービス定義文書」と書かれている）。読者は付録 A の参照に当たっては、実際のプロセスの動きを思い描きながら読み進まれると良いでしょう。

新規サービス又はサービス変更の設計及び移行（5）

一般（5.1）

- 新規サービスまたはサービス変更の設計及び移行プロセスと変更管理プロセスの強い連携
- 変更管理、構成管理とのインタフェース
- 新規サービス又はサービス変更の計画立案、設計活動のレビュー、受理 or 却下



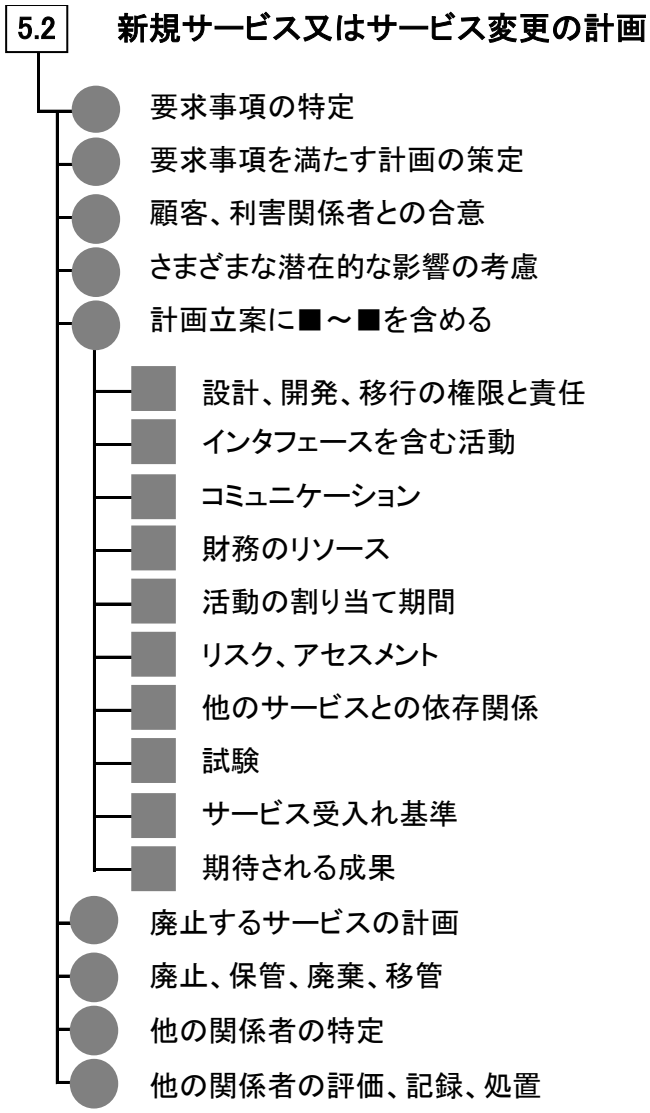
【インプット】	【アウトプット】
・新規サービス提案 ・サービスの変更案	・承認された新規サービス・サービス変更 ・新規サービス・サービス変更へのリスクアセスメント結果 ・計画立案及び設計活動のレビュー結果 ・受理 or 却下の決定 ・開発移行への処置

特記

・新規サービス又はサービスの変更の提案は、顧客，サービス提供者，内部グループ又は供給者によって提起される可能性があります。

新規サービス又はサービス変更の計画（5.2）

- 新規サービス又はサービス変更の計画と顧客、利害関係者との合意
- 財務、組織、技術、SMS に対する潜在的な影響を考慮
- 計画立案へ含める項目
- サービス廃止の計画
- 関与する他の関係者の特定。評価

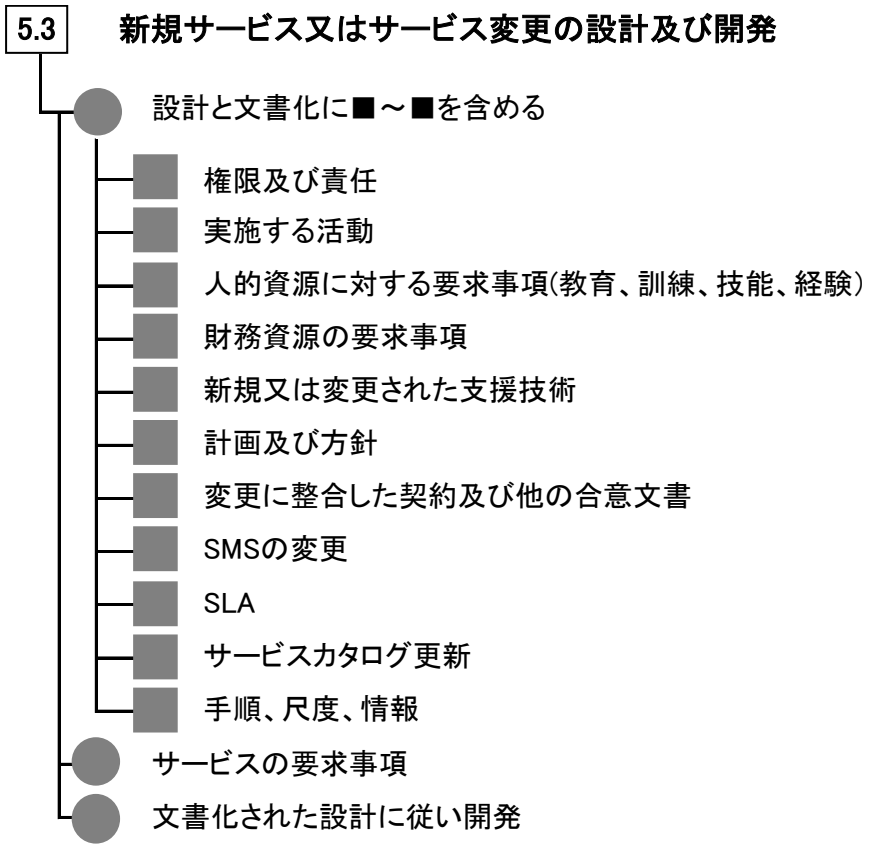


【インプット】	【アウトプット】
・新規サービス提案 ・サービス変更案 ・サービス停止・移行案	・新規サービス又はサービス変更の計画 ・顧客・利害関係者との合意 ・潜在的影響の考慮結果 ・サービス移行・廃止計画 ・他の関係者の評価結果、記録、処置

特記
・廃止 （終了でもリタイアでも同じ）・移行するサービスについても計画することを要求しています。
・他の関係者はサービスコンポーネントの提供に関与します。

新規サービス又はサービス変更の設計及び開発（5.3）

- 新規サービス又はサービス変更の設計と文書化
- サービス要求事項を満たす設計
- 設計に従って開発



【インプット】	【アウトプット】
・新規サービス提案計画 ・サービスの変更計画 ・サービス廃止・移行の計画	・文書化された設計による開発

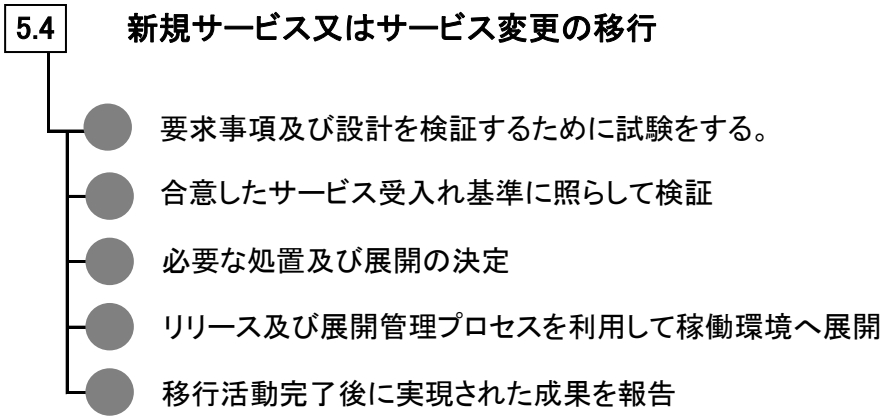
特記

・設計についての詳細は、JIS Q 9001:2008 の 7.3 に記載の設計・開発のプロセス、又は ISO/IEC 15288:2008 の 6.4.3 に記載のアーキテクチャ設計プロセスを参照することを奨めています。

・JIS Q 9001:2008 では、7.3.1 設計・開発の計画～7.3.7 設計・開発の変更管理までの 7 つのステップにおける要求事項があります。

新規サービス又はサービス変更の移行（5.4）

- 新規サービスまたはサービス変更の検証と試験、サービス受入れ基準
- 稼働環境への展開
- 成果の報告



【インプット】	【アウトプット】
・新規サービスの開発 ・サービスの変更の開発	・試験・検証結果 ・サービス受入れ基準の結果 ・実現された成果の報告

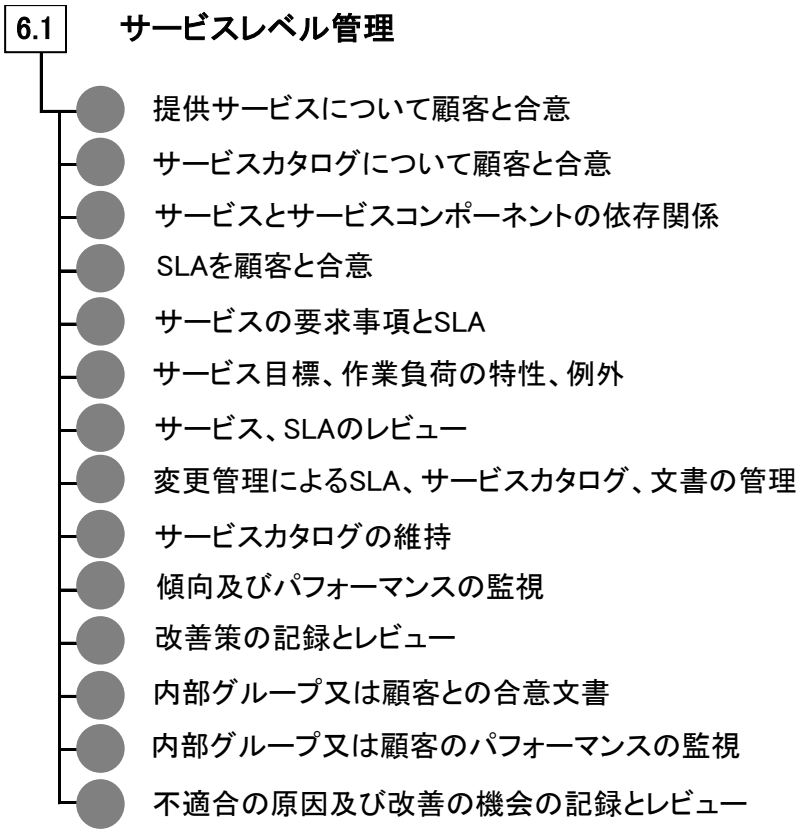
特記

・設計を検証するために試験をし、サービス関係者と利害関係者の間であらかじめ合意した受入れ基準を基に検証します。稼働環境への展開はリリース及び展開管理プロセスを利用します。

サービス提供プロセス（６）

サービスレベル管理（6.1）

－　サービスレベル管理の活動（サービスレベルの設定、レビュー、変更）を行う



【インプット】	【アウトプット】
・サービス ・サービスの要求事項 ・SLA 及び他の合意文書 ・サービスの実施状況 ・サービスコンポーネント合意文書 ・内部グループ、顧客のパフォーマンスデータ	・SLA、SLA の合意記録 ・サービスカタログ ・サービスの要求事項 ・OLA、UC、対応手順書 ・サービス・SLA 履行状況の記録 ・不適合項目の記録 ・内部グループ、顧客のパフォーマンス記録 ・不具合、改善策の記録

特記

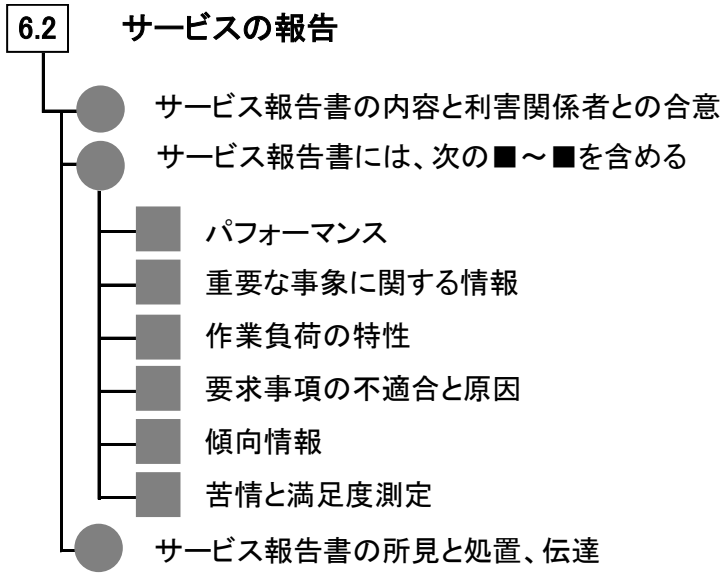
・サービスカタログが定義されました。

・規格の中で、OLA、UC に触れていませんが、記載されている内容から判断して OLA、UC としています。

- OLA（Operational Level Agreement：オペレーショナルレベル合意書）サービス提供者と内部グループとの支援協定。
- UC（Underpinning Contract：外部委託契約）はサービス提供者と供給者との支援取決め。

サービスの報告（6.2）

－　サービスマネジメントに対するサービス実施の報告を行う



【インプット】

・サービスの実施状況

【アウトプット】

・サービス報告書
  - 文書識別
  - 目的
  - 報告先
  - データの出所
  - 目標に対するパフォーマンス
  - 不順守事項・その懸念
  - 作業負荷の特性
  - 重大事象後のパフォーマンス
  - 傾向情報
  - 満足度の分析

・経営陣による決定・是正処置

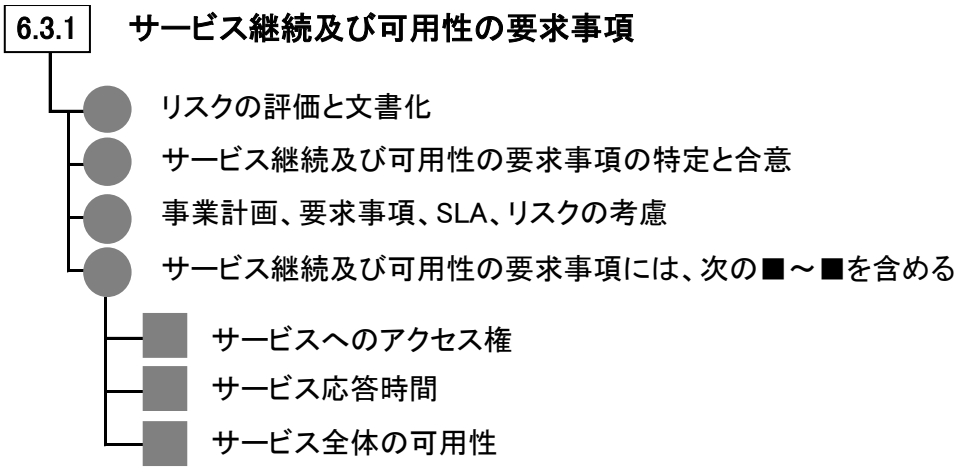
特記

・ISO/IEC 20000 では、サービスの報告として、サービス、プロセス群を対象としています。ITIL V3 ではサービスの報告はプロセスとして扱われていましたが、ITIL V3 2011Edition には、サービス報告だけを取り扱ったプロセスはありません。

サービス継続及び可用性管理（6.3）

サービス継続及び可用性の要求事項（6.3.1）

－　サービス継続性管理と可用性管理の要求事項（リスクの評価）を行う

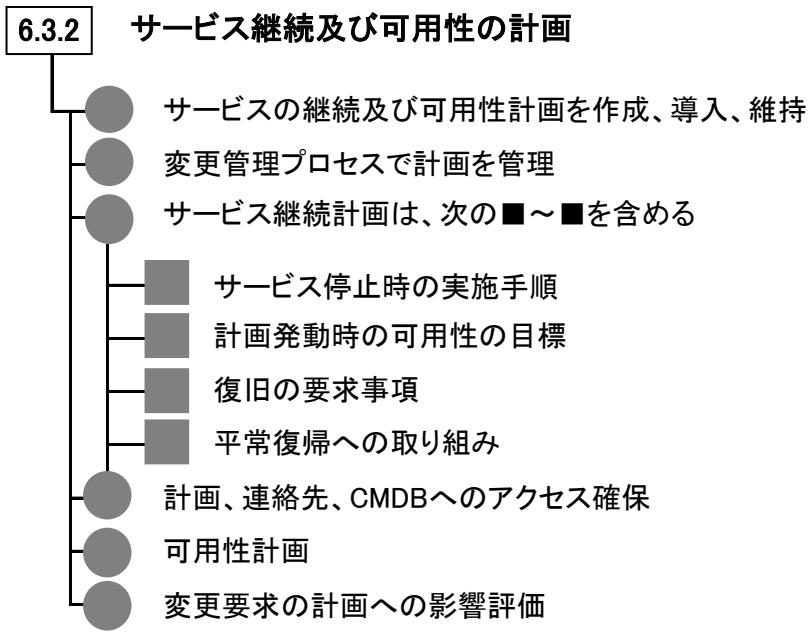


【インプット】	【アウトプット】
・サービス継続及び可用性の要求事項 ・リスクアセスメント ・サービスの実施状況	・可用性及び継続性に対する合意した要求事項

サービス継続及び可用性管理（6.3）

サービス継続及び可用性の計画（6.3.2）

－　サービスの継続と可用性の計画を作成、導入、維持を行う

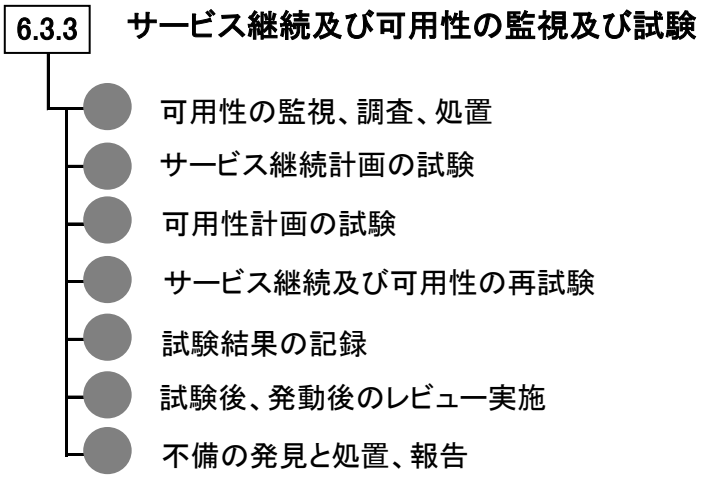


【インプット】	【アウトプット】
・サービス停止時の手順 ・計画発動時の可用性目標 ・復旧の要求事項 ・平常時への復帰の取り組み	・サービス継続計画 ・可用性計画 ・変更要求の計画への影響評価

サービス継続及び可用性管理（6.3）

サービス継続及び可用性の監視及び試験（6.3.3）

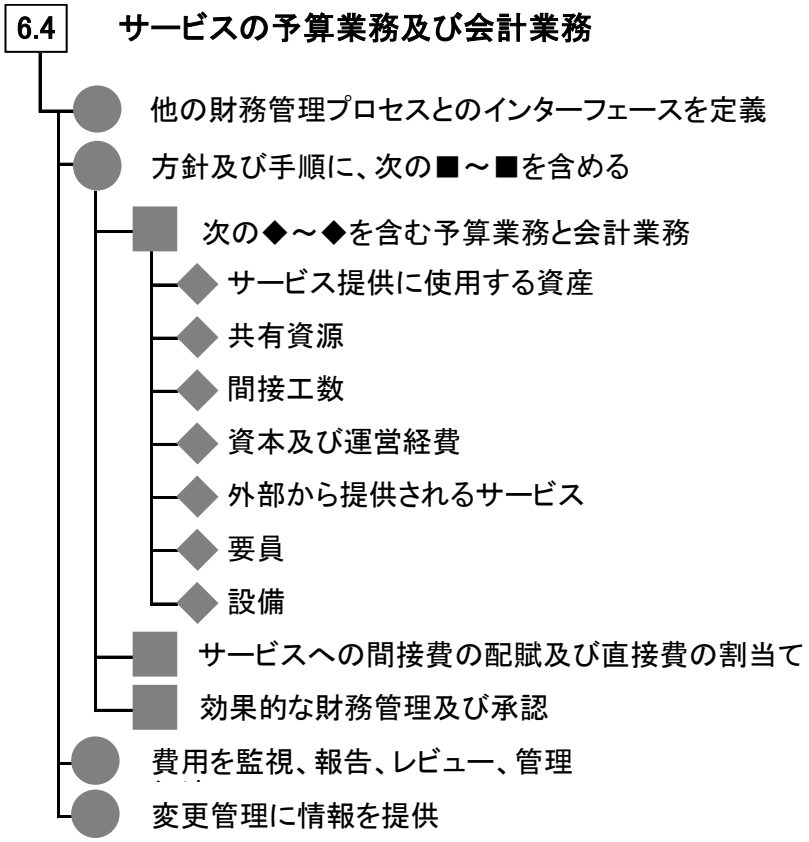
－　サービスの継続性管理と可用性管理の監視、記録、処置



【インプット】	【アウトプット】
・事業計画 ・SLA ・リスクアセスメント ・サービスの実施状況	・可用性・継続性に対する要求事項 ・サービス継続計画 ・レビュー記録 ・試験記録 ・可用性の測定記録 ・試験不合格の際の処置計画

サービスの予算業務及び会計業務（6.4）

- IT サービスのコストと予算を管理する
- 会計処理を管理する



【インプット】

- 全コンポーネントの情報
  - 資産（ライセンス）
  - 共有資源
  - 間接工数
  - 外部サービス
  - 要員
  - 設備
- 費用

【アウトプット】

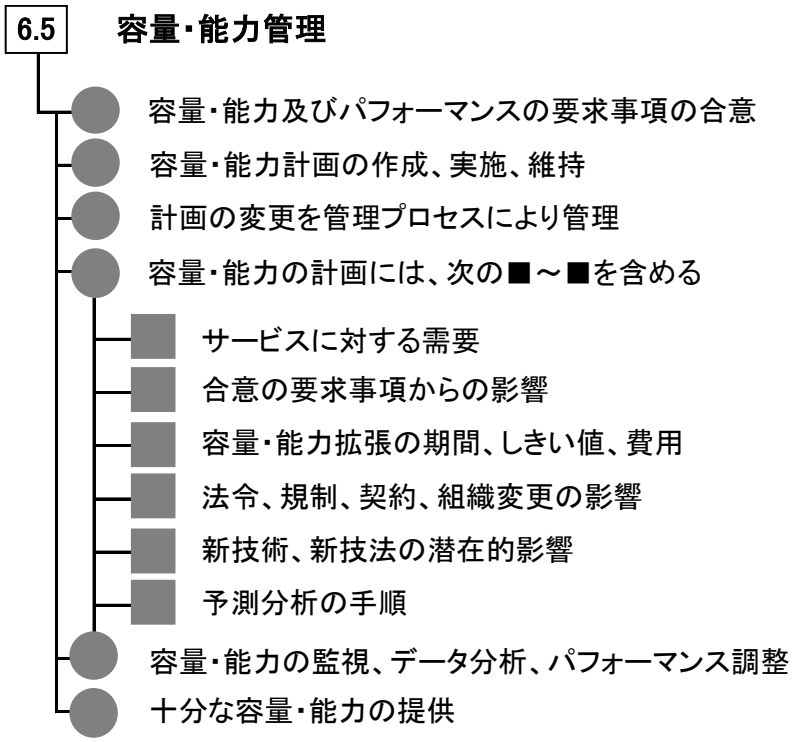
- 他の財務管理とのインタフェース
- 方針及び文書化された手順
  - 予算業務及び会計業務
  - 間接費の配賦、直接費の割り当て
  - 財務管理と許可
- 予算化
- 費用の管理（監視報告、レビュー）

特記

- 課金業務は含まれません。

容量・能力管理（6.5）

- 顧客の事業に必要な容量・能力を保持する
- 現在と将来の合意された需要を満たす十分な容量・能力を保持する



【インプット】

- キャパシティに対する顧客からの事業上の必要性
- 現在のキャパシティとパフォーマンスに対する要求事項
- 予想されるサービス拡張・変更要求
- 予想される新技術・技法
- 外部変化の情報
- 予測分析

【アウトプット】

- キャパシティ計画
- サービス拡張に必要な期間・しきい値・費用
- 予想されるサービス拡張が及ぼす効果の評価
- 予想される新技術・技法が及ぼす効果の評価
- 外部変化で予想される影響
- 適切なキャパシティを提供する方法・手順・技法

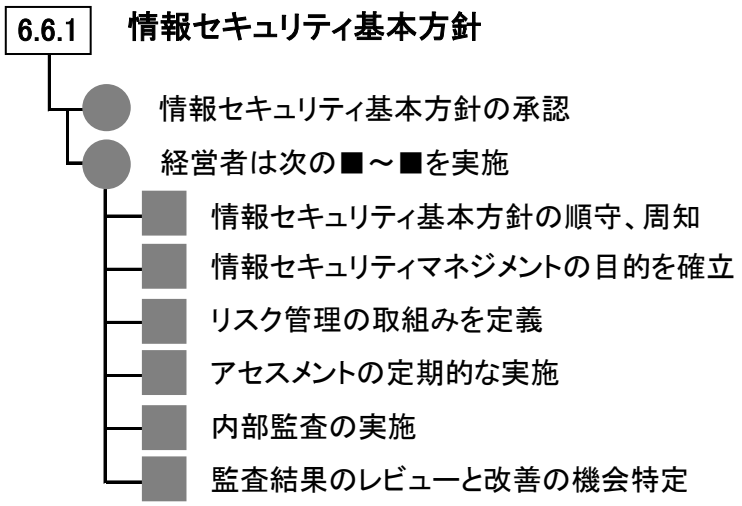
特記

- JIS Q 20000 の容量・能力管理では、ITIL のように「ビジネスキャパシティ」「サービスキャパシティ」「リソースキャパシティ」まで詳細化した記述を盛り込んでいません。

情報セキュリティ管理（6.6）

情報セキュリティ基本方針（6.6.1）

－　経営者による情報セキュリティ基本方針の承認



【インプット】	【アウトプット】
・サービスの要求事項 ・法令・規制要求事項 ・契約上の義務 ・情報セキュリティリスク	・情報セキュリティ基本方針 ・情報セキュリティリスクアセスメント結果 ・内部監査結果とレビュー結果 ・改善策

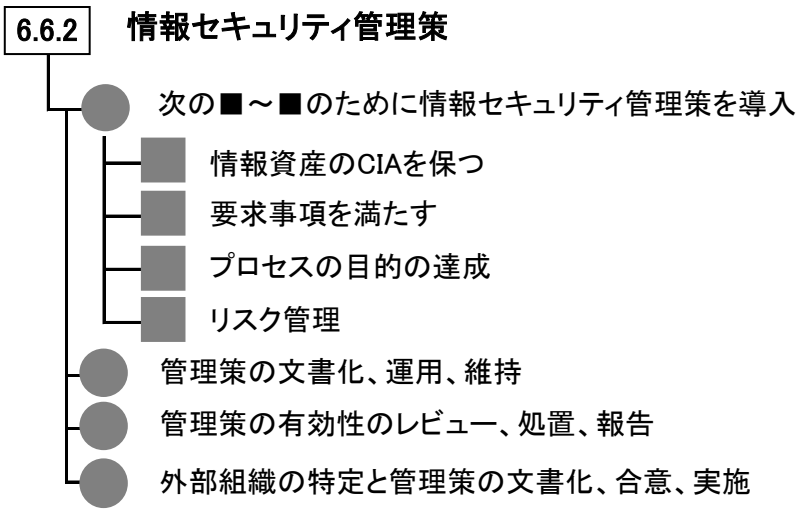
特記

・ISO/IEC 27000 ファミリー規格を必要に応じて参照することで、情報セキュリティ管理プロセスの導入、運用に役立てることが出来るでしょう。

情報セキュリティ管理（6.6）

情報セキュリティ管理策（6.6.2）

- 情報セキュリティ管理策の導入と運用
- 管理策の有効性レビュー、処置、報告
- 外部組織の特定、管理策の文書化、合意、実施



【インプット】	【アウトプット】
・情報資産の CIA ・情報セキュリティ基本方針 ・情報セキュリティ管理目的 ・関連リスク ・サービス ・サービス提供者の情報	・情報セキュリティ管理策 ・有効性のレビュー結果、報告 ・外部組織とのセキュリティ管理策

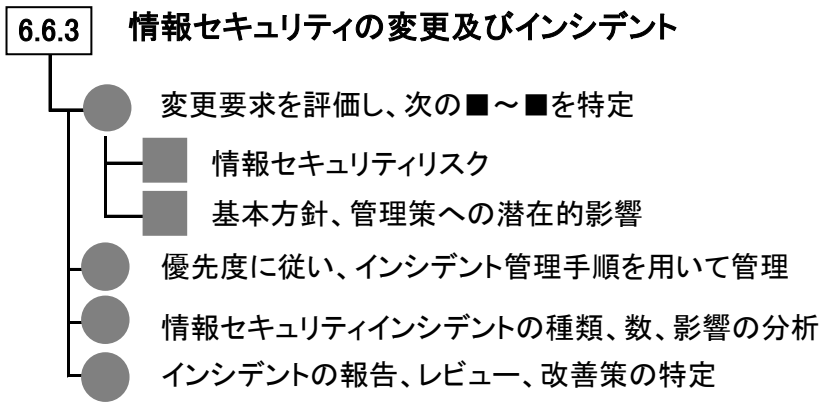
特記

・ISO/IEC 27000 ファミリー規格を必要に応じて参照することで、情報セキュリティ管理プロセスの導入、運用に役立てることが出来るでしょう。

情報セキュリティ管理（6.6）

情報セキュリティの変更及びインシデント（6.6.3）

- 変更要求の評価
- 情報セキュリティインシデントを管理



【インプット】	【アウトプット】
・変更要求 ・インシデントの管理手順 ・情報セキュリティインシデントの種類、数、影響	・変更が管理策に与える影響のアセスメント結果 ・情報セキュリティインシデント分析・記録 ・改善策の特定

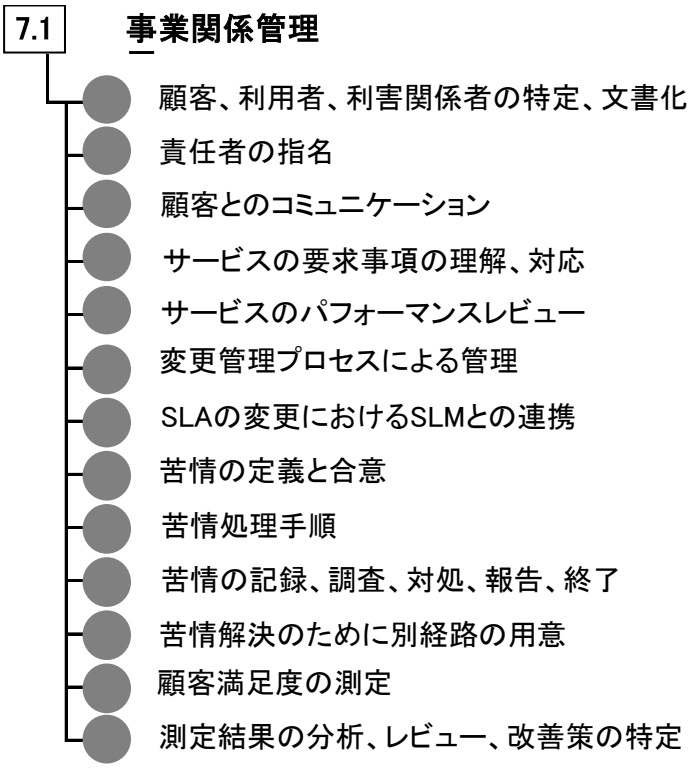
特記

・ISO/IEC 27000 ファミリー規格を必要に応じて参照することで、情報セキュリティ管理プロセスの導入、運用に役立てることが出来るでしょう。

関係プロセス（７）

事業関係管理（7.1）

- サービスレビュー会議を開催する
- サービスの苦情処理を行う
- 顧客満足度測定を行う



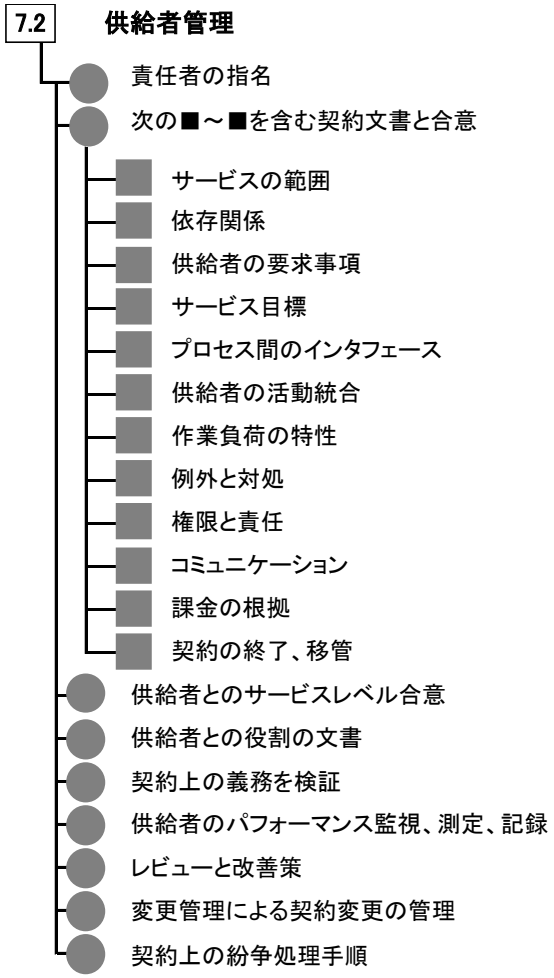
【インプット】	【アウトプット】
・事業環境 ・サービスの要求事項 ・SLA ・苦情 ・顧客満足度調査結果	・サービスのパフォーマンスレビュー ・契約・SLA 変更要求の検討結果 ・苦情についての合意事項 ・苦情処理の報告 ・改善処置

特記

・細分箇条 7.2 と 7.3 は、ISO 10001～10003 が参考になります。ISO 10001～10003 については、『ITSMS ユーザーズガイド - JIS Q 20000 （ISO/IEC 20000）対応 -』の付録を参照ください。

供給者管理（7.2）

- 契約管理を行う
- 複数の供給者の管理を行う
- 契約紛争の管理を行う



【インプット】		【アウトプット】
・供給者の要求事項 ・供給者のサービス実施状況 ・関係者の間の依存関係 ・サービス目標 ・プロセス間のインタフェース ・供給者の活動 ・作業負荷の特性 ・契約の例外と対処法 ・権限、責任の文書	・報告、コミュニケーション ・課金の根拠 ・サービスの終了・移管活動、責任 ・SLA ・改善処置 ・供給者のパフォーマンス ・契約上の義務 ・契約の変更 ・契約上の紛争	・供給者との契約文書 ・サービスレベル合意 ・統括供給者と再請負契約先供給者との役割・関係の文書 ・供給者のパフォーマンス測定結果 ・レビュー ・改善策 ・紛争の処理手順 ・契約担当者の指名

特記

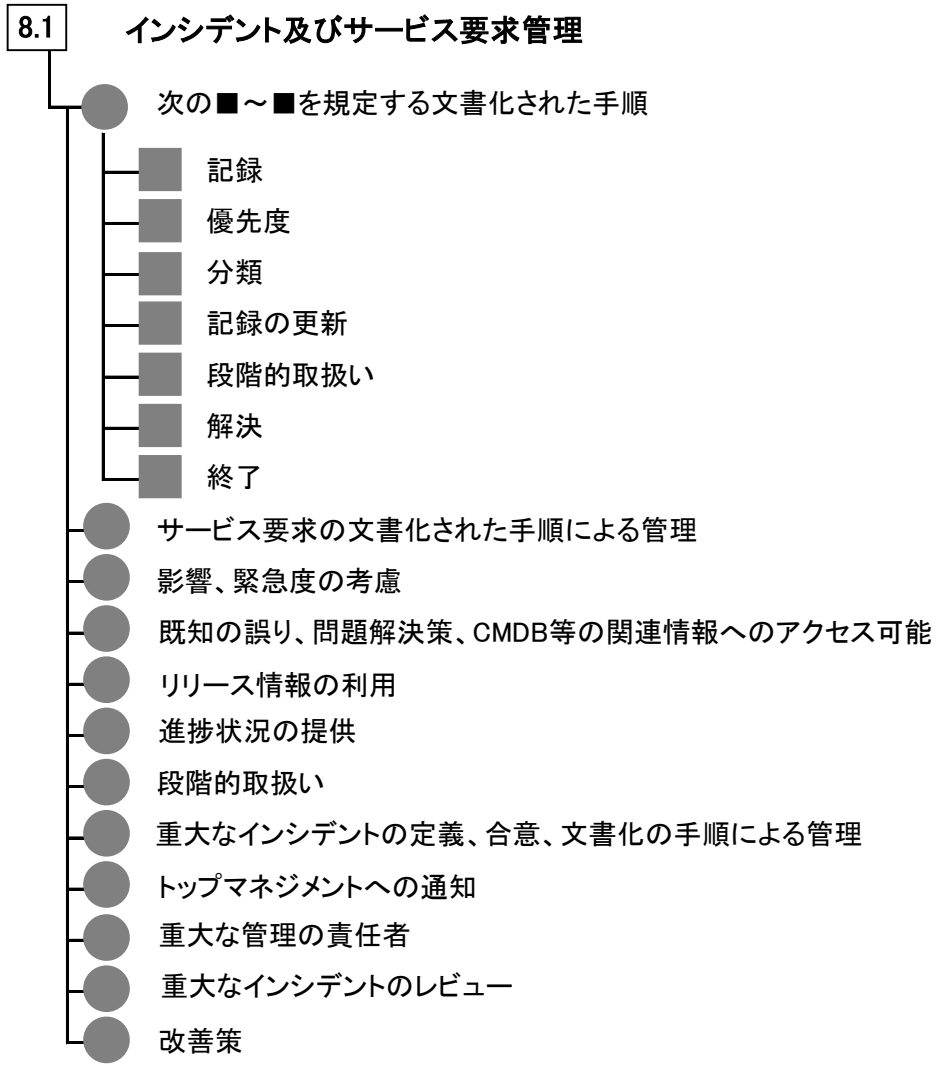
・細分箇条 7.2 と 7.3 は、ISO 10001～10003 が参考になります。ISO 10001～10003 については、『ITSMS ユーザーズガイド - JIS Q 20000 （ISO/IEC 20000）対応 -』の付録を参照ください。

・供給者管理プロセスの適用範囲には、供給者の選定、サービスの調達は含まれません。

解決プロセス（８）

インシデント及びサービス要求管理（8.1）

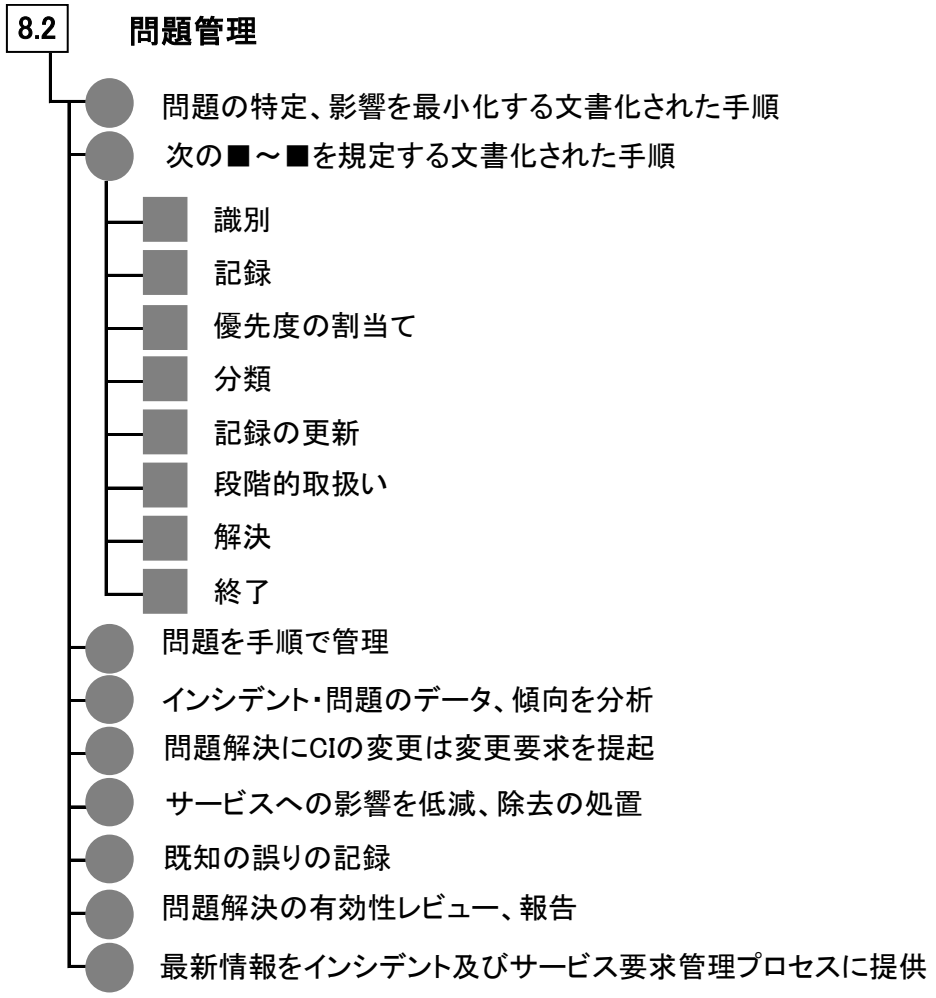
- インシデント管理により合意済みサービスの迅速な回復を行う
- サービス要求に対応する



【インプット】	【アウトプット】
・全てのインシデント ・サービス要求 ・重大インシデント ・インシデント、サービス要求関連情報、進捗状況 ・既知の誤り ・問題解決策 ・CMDB ・リリース期日、リリース情報 ・サービス目標 ・緊急度	・文書化された手順 ➢ 記録 ➢ 優先度 ➢ 分類 ➢ 記録の更新 ➢ 段階的取扱い ➢ 解決 ➢ 終了 ・全インシデントの記録 ・インシデントの影響管理手順 ・進捗状況報告 ・サービスレベル未達の場合の事前警告

問題管理（8.2）

- インシデントを引き起こした根本原因を特定する
- 問題解決後に予防処置等によりプロアクティブに対応する

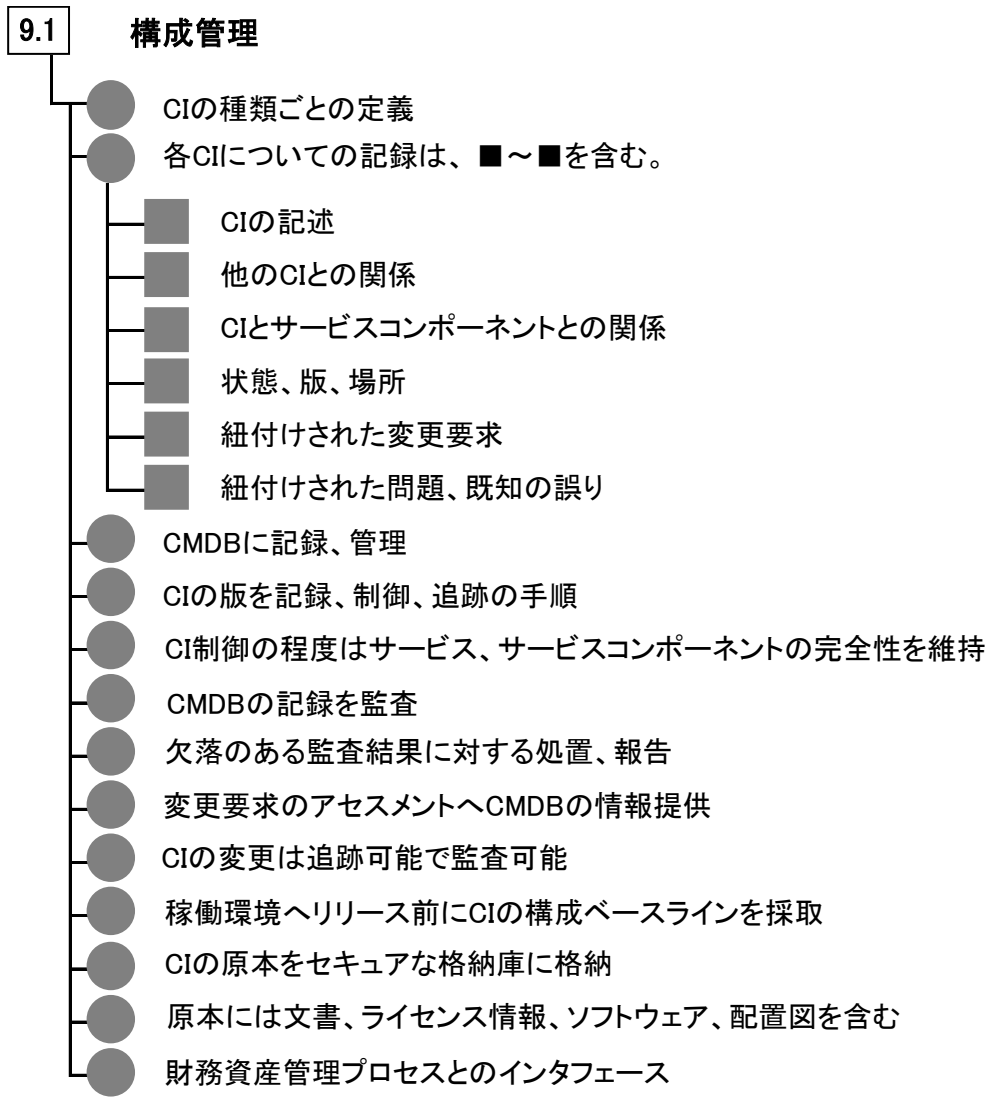


【インプット】	【アウトプット】
・問題 ・インシデントデータ、傾向	・問題の記録 ・インシデント・問題の文書化された手順 ➢ 識別 ➢ 記録 ➢ 優先度の割当て ➢ 分類 ➢ 記録の更新 ➢ 段階的取扱い ➢ 解決 ➢ 終了 ・変更要求 ・既知の誤り・問題解決策の最新情報 ・予防処置

統合的制御プロセス（9）

構成管理（9.1）

- CI を定義する
- CI の正確で最新の情報を維持する



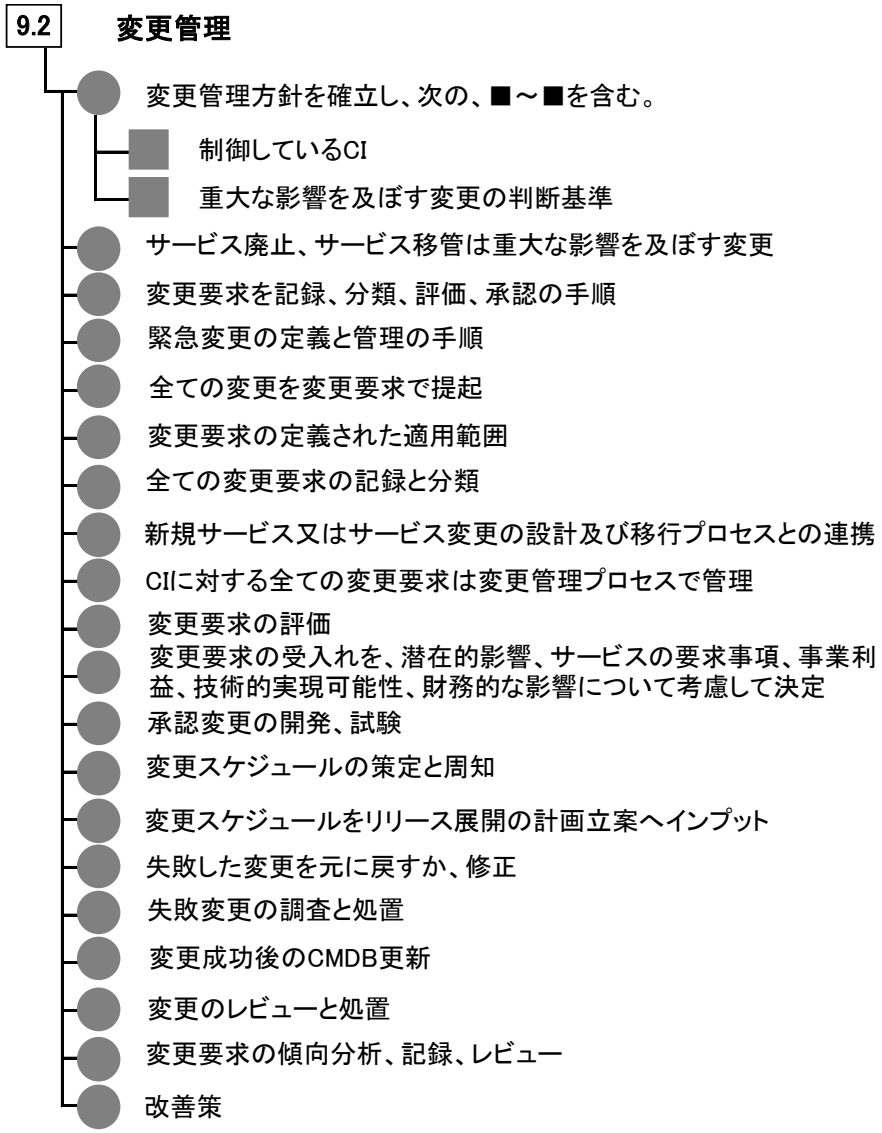
【インプット】	【アウトプット】
・CI の情報 ・サービス ・サービスコンポーネント ・リリース情報 ・CI の原本	・CI の種類ごとの定義 ・CMDB ・CI の版を記録、制御、追跡する文書化された手順 ・CMDB 監査手順 ・CMDB の監査結果 ・変更管理との統合的連携の仕組み ・CI の構成ベースライン ・CI の原本を保管するセキュアな書庫 ・財務資産管理とのインタフェース

特記

・構成管理プロセスの適用範囲には、財務資産管理を含みません。

変更管理（9.2）

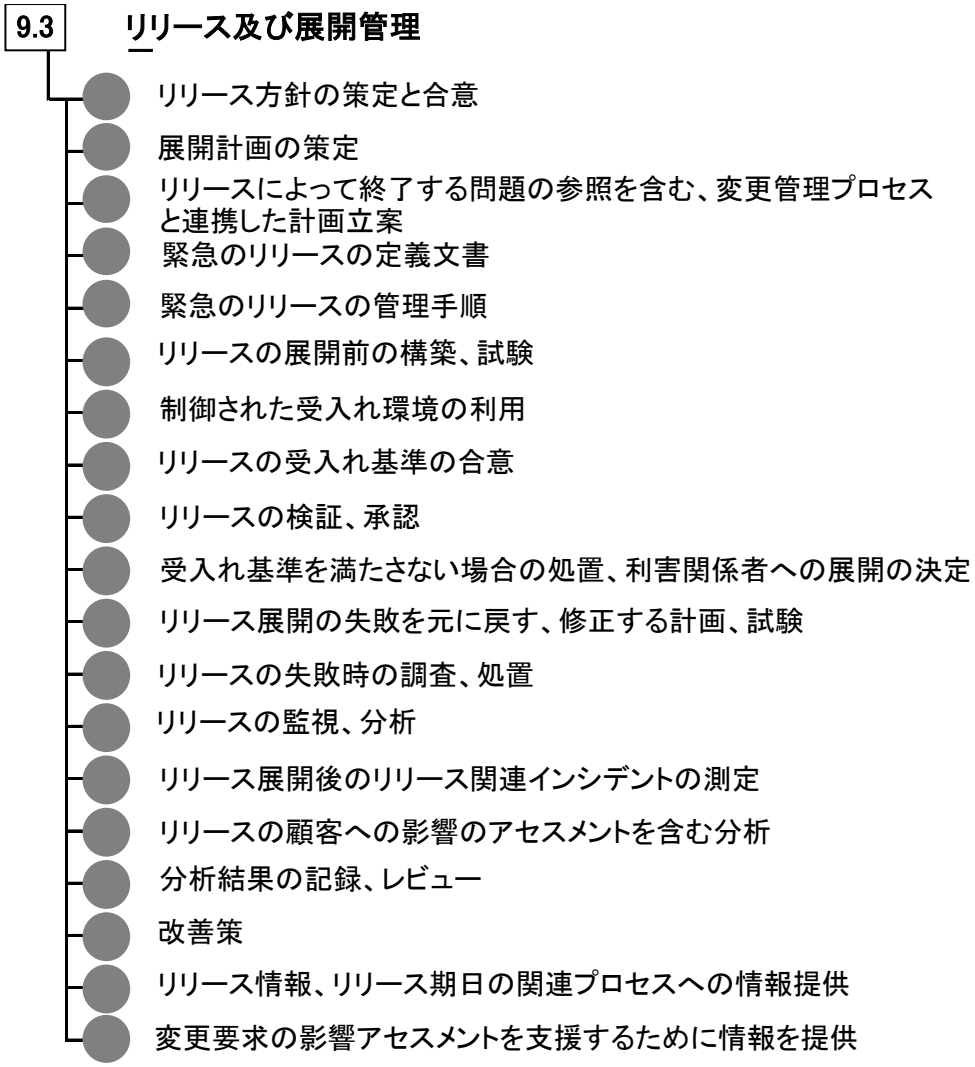
- 変更管理方針を定める
- 全ての変更をアセスメント、承認、実装、レビューする



【インプット】	【アウトプット】
・サービス変更 ・サービス廃止 ・サービス移管 ・新規サービス ・変更要求	・変更管理方針を定義した文書 ・全変更要求の記録、分類、評価、承認の手順 ・緊急変更の許可・実装制御のための方針と手順 ・変更要求をリスク・サービス及び顧客への潜在的影響、サービスの要求事項、事業利益、技術的実現可能性、財務的な影響について考慮した意思決定 ・変更スケジュールの策定 ・失敗時の戻す方法または修正の計画 ・失敗した変更の調査結果、処置 ・更新された CMDB ・変更のレビュー結果、処置 ・変更要求の傾向分析結果、記録 ・変更分析の結果 ・改善策

9.3 リリース及び展開管理（9.3）

- リリース方針
- IT サービスの変更を稼働環境にリリースし、展開を管理する



【インプット】	【アウトプット】
・リリース要求情報	・リリース方針 ・新規サービス又はサービス変更、サービスコンポーネントの稼働環境への展開計画 ・計画立案 ・緊急リリースの定義文書 ・リリース受入れ手順 ・リリース展開時の失敗を元に戻す、または修正の方法 ・リリース展開の失敗の調査、処置の結果 ・リリースの監視、測定、分析、顧客への影響アセスメント ・リリースの記録、レビュー結果 ・改善策 ・リリース情報 ・影響のアセスメントの支援情報

JIS Q 20000 と ITIL ではプロセスの区分の仕方、プロセスの呼称が一部違い、訳の違いも見られます。

- JIS Q 20000 における「新規サービス又はサービス変更の設計及び移行」と「サービスの報告」は、ITIL V3 2011 Edition では明示的な対応プロセスがありません。
- JIS Q 20000 における「サービス継続及び可用性管理」は、ITIL V3 2011 Edition では「IT サービス継続性管理」と「可用性管理」の２プロセスに分類されます。
- JIS Q 20000 における「構成管理」は、ITIL V3 2011 Edition では「サービス資産管理および構成管理」となりますが、財務資産管理は JIS Q 20000 の構成管理では扱われません。

表 A-1　JIS Q 20000 と ITIL でのプロセス名の違い

JIS Q 20000	ITIL V3 2011 Edition
サービスの予算業務及び会計業務	IT サービス財務管理（SS）
サービス継続及び可用性管理	IT サービス継続性管理（SD） 可用性管理（SD）
容量・能力管理	キャパシティ管理（SD）
供給者管理	サプライヤ管理（SD）
構成管理	サービス資産管理および構成管理（ST）
インシデント及びサービス要求管理	インシデント管理（SO） 要求実現（SO）
リリース及び展開管理	リリース管理および展開管理（ST）

付録B　ITIL 用語と JIS Q 20000 用語の対比表

ITIL と JIS Q 20000 での用語の対比を次の表に示します。
用語に相違がある場合は、相違欄に“⇔”で示しています。

表 B-1　ITIL と JIS Q 20000 用語比較

ISO/IEC 20000 原文	JIS Q 20000-1:2012	相違	ITIL 用語 ITILV3_Glossary_Japanese_ v3.1.24
accounting	会計業務		会計業務
agreement	合意		合意
asset	資産		資産
asset management	資産管理		資産管理
assurance	保証		保証
attribute	属性		属性
audit	監査		監査
availability	可用性		可用性
availability management	可用性管理		可用性管理
baseline	ベースライン		ベースライン
budgeting	予算業務	⇔	予算管理
business relationship management	事業関係管理		事業関係管理
capacity	容量・能力	⇔	キャパシティ
capacity management	容量・能力管理	⇔	キャパシティ管理
capacity plan	容量・能力計画	⇔	キャパシティ計画
change	変更、変化	⇔	変更
change management	変更管理		変更管理
charging	課金		課金
classification	分類		分類
closure	終了	⇔	クローズ
compliance	適合	⇔	遵守性
configuration	構成		構成
configuration baseline	構成ベースライン		構成ベースライン
configuration item	構成品目 CI	⇔	構成アイテム
configuration management	構成管理		構成管理
configuration management database	構成管理データベース CMDB		構成管理データベース
continual improvement	継続的改善		
contract	契約		契約
control	制御、管理策、管理、統合的制御	⇔	コントロール
corrective action	是正処置		
cost	費用	⇔	コスト
customer	顧客		顧客
deliverable	成果物		成果物
dependency	依存関係	⇔	依存性
direct cost	直接費		直接費
document	文書		文書

effectiveness	有効性		有効性
efficiency	効率性		効率性
emergency change	緊急変更	⇔	非常時の変更
environment	環境		環境
escalation	段階的取扱い、経路	⇔	エスカレーション
failure	失敗	⇔	障害
function	機能		機能
identification	識別、(リスクの)特定	⇔	識別
impact	影響	⇔	インパクト
incident	インシデント		インシデント
incident management	インシデント管理		インシデント管理
incident report	インシデント報告書	⇔	インシデント・レポート
indirect cost	間接費		間接費
information security	情報セキュリティ		
information security incident	情報セキュリティインシデント		
information technology	情報技術		情報技術
infrastructure	インフラストラクチャ		インフラストラクチャ
integrity	完全性		完全性
interested party	利害関係者		
interface	インタフェース		インタフェース
internal group	内部グループ		
known error	既知の誤り	⇔	既知のエラー
live environment	稼働環境		稼働環境
major incident	重大なインシデント		重大なインシデント
management system	マネジメントシステム	⇔	管理システム
method	方法	⇔	手法
nonconformity	不適合		
objective	目的	⇔	目標
organization	組織		組織
overheads	間接工数	⇔	オーバヘッド
people	人々	⇔	人材
performance	パフォーマンス		パフォーマンス
preventive action	予防処置		
priority	優先度		優先度
problem	問題		問題
problem management	問題管理		問題管理
problem record	問題の記録	⇔	問題レコード
procedure	手順		手順
process	プロセス		プロセス
programme	プログラム		プログラム
project	プロジェクト		プロジェクト
quality	品質		品質
record	記録	⇔	レコード
recovery	復旧		復旧
relationship	関係		関係
release	リリース		リリース
release policy	リリース方針	⇔	リリース・ポリシー
release and deployment management	リリース及び展開管理	⇔	リリース管理および展開管理
reliability	信頼性		信頼性
request for change	変更要求		変更要求

resolution	解決		解決
resolution process	解決プロセス		解決プロセス
review	レビュー		レビュー
risk	リスク		リスク
risk assessment	リスクアセスメント	⇔	リスク評価
role	役割		役割
scope	適用範囲		適用範囲
security	セキュリティ		セキュリティ
service	サービス		サービス
service acceptance criteria	サービス受入れ基準	⇔	サービス受け入れ基準
service component	サービスコンポーネント		
service continuity	サービス継続		
service delivery	サービス提供	⇔	サービスデリバリ
service level agreement	サービスレベル合意書 SLA	⇔	サービスレベル・アグリーメント
service level management	サービスレベル管理	⇔	サービスレベル・管理
service management	サービスマネジメント		サービスマネジメント
service management system	サービスマネジメントシステム SMS		
service provider	サービス提供者	⇔	サービス・プロバイダ
service request	サービス要求		サービス要求
service requirement	サービスの要求事項		
supplier	供給者	⇔	サプライヤ
supply chain	サプライチェーン	⇔	サプライ・チェーン
system	システム		システム
threshold	閾(しきい)値		しきい値
top management	トップマネジメント		
transition	移行		移行
urgency	緊急度		緊急度
user	利用者	⇔	ユーザ
verification	検証		検証
version	版	⇔	バージョン
working around	回避策	⇔	ワークアラウンド
workload	作業負荷		作業負荷

付録C　ITSMS の適用範囲設定に関する手引き（ISO/IEC 20000-3:2012 の要点）

C.0. はじめに

本手引き（付録 C）では、『ISO/IEC 20000-3:2012』について独自に翻訳し、その要素を引用又は整理した内容をご紹介しています。

『ITSMS ユーザーズガイド「付録 D　認証の適用範囲の考え方」』及び『本書　3. スコーピング』の考え方の基礎を提供するものです。

C.1. ISO/IEC 20000-3:2012 の構成

ISO/IEC 20000-3:2012 は以下の内容で構成されています。

【目次】

C.2. ISO/IEC 20000-3:2012 の対象範囲

ISO/IEC 20000-1 を用いたサービスマネジメントシステム（SMS※1)）の確立を検討している、又は適合性評価のための準備を行うサービス提供者、及び自組織に適用可能かについて具体的な助言を必要としているサービス提供者に対して、SMS の適用範囲の定義及び適用に関する手引きを提供します。

C.3. ISO/IEC 20000-1 認証への適合

ISO/IEC 20000-1 に規定する要求事項への適合の実証を希望するサービス提供者は、以下を実証することが望まれます。

a) ISO/IEC 20000-1 で要求されるすべてのプロセスが文書化及び運用されている。これには、他社による運用のプロセスへのガバナンスも含まれる
b) プロセス間のインタフェースが文書化及び運用され、望ましい結果をもたらしている
c) サービスマネジメントの機能が、顧客ニーズや顧客要求に沿う結果をもたらしている
d) SMS が顧客と合意された結果を達成するため、供給者及び内部グループと連携が取られている

適合性評価には第一者（内部監査）、第二者（顧客による監査）、第三者（認証機関による監査）の種類があり、以下の国際規格が適用できます。

第三者による適合性評価のための監査の規格は ISO/IEC 17021 であり※2)、それ以外の監査の一般的指針は ISO/IEC 19011 であり、一般的な適合性評価の用語及び定義は ISO/IEC 17000 であります。サービス提供者が第一者監査で適合を自己宣言する場合の要求事項は ISO/IEC 17050-1 を参照することが望まれます。

第三者認証機関は適合性評価で行う認証の授与に関する規則を確立することが要求されます。例えば、その規則には、登録証の発行対象がコンソーシアムではなく、単一の法人とすることも要求可能です※3)。

※注記の説明：

1）SMS としていますが、規格のタイトルには Information Technology（情報技術）が付いているため、ITSMS からの変更はありません。

2）第三者認証の認定基準 ISO/IEC 17021 が 2011 年 1 月に改訂され、ISO/IEC 19011 と分離されたため、本表記としました。

3）認証機関が定める規則において、登録証の発行対象を単一の法人のみにすべきであると言及している訳ではありません。複数の法人の集まりであっても、認証取得における主たるサービス提供組織（代表の法人）と他の支援組織（別法人）との関係や役割、さらに統制環境の整備状況を明確に示すことができれば、1 つの登録証の発行対象として認められる場合があります。

但し、複数法人での認証取得を希望される場合は、事前に認証機関へご相談下さい。

C.4. ISO/IEC 20000-1 の適用に関して

C.4.1 ISO/IEC 20000-1 適用の原則

様々な種類のサービス提供者が ISO/IEC 20000-1 に基づく SMS を活用することができます。

顧客又は供給者が ISO/IEC 20000-1 への適合を実証した場合でも、サービス提供者に ISO/IEC 20000-1 を適用することは可能です。ただし、サービス提供者が SMS の一部のプロセスに対してだけガバナンスを行っている場合は、ISO/IEC 20000-1 への適合が適切でないと評価者が判断することもあります。

C.4.2 他のマネジメントシステムとの統合への考慮

ISO/IEC 20000-1 は PDCA モデルを包含しているので、他の関連マネジメントシステム（ISMS 及び QMS など）と統合又は調整できます。

しかしながら、各マネジメントシステムは異なる目的をもっているため、それぞれ要求事項には違いがあり、各マネジメントシステム規格の特定の要求事項を満たすために、適用範囲内で違いをもたせる必要があり得ることを認識する必要があります。

C.4.3 プロセスのガバナンス

ISO/IEC 20000-1 への適合を希望するサービス提供者は、他の当事者によって運用されるプロセスも含め、すべてのプロセスのガバナンスを要求されます。

※以下、本手引きの『5.5 SMS の適用範囲において一部のサービス又はプロセスを委託している場合の考え方』も合わせてご確認下さい。

ISO/IEC 20000-1 の適用範囲内にある SMS の一部のプロセスは、他の当事者（サービス提供者と同じ組織の中の内部グループ、顧客又は供給者）によって運用することが可能です。この場合、サービス提供者が、他の当事者の責任の定義及び合意を含む、プロセスのガバナンスを持つことが要求されます。

サービス提供者は、次の方法によってプロセスのガバナンスを実証することが求められます。

a) プロセスの説明責任を果たす、またはプロセスの順守を要求する権限を行使する
b) プロセスを定義し、かつ他のプロセスとのインタフェースを管理する
c) プロセスの実施状況を測定・記録・分析することでプロセスパフォーマンスを改善する
d) プロセス改善の計画を立て、評価し、優先順位を付けて実施する

サービス提供者がプロセスの一部を供給者に外部委託している場合、サービス提供者は、供給者とのサービス契約によってサービス提供者が SMS の適用範囲内のすべてのプロセスのガバナンスを持つことを妨げられないようにすることを、確実にすることが望まれます。

プロセスガバナンスは、サービス提供者の適用範囲内に含まれるプロセスのみについて実証する必要があります。他の当事者の管理下にあるプロセスを、サービス提供者の適用範囲に含めることはできません。

C.4.4　ISO/IEC 20000-1 の適用とサービス提供に使用される技術の関係

ISO/IEC 20000-1 の適用は、サービスマネジメントプロセスの自動化のために使用する技術を含め、サービス提供が使用する技術による影響を受けません。ただし、プロセス活動の技能、ツール、及びデータの要求事項に直接的な影響を及ぼします。

サービス提供に使用される技術の代表的なものを以下に示します。(これがすべてではありません。)

> 5.3 サービス提供に使用される技術の範囲
>
> サービス提供者は、ISO/IEC 20000-1 について、次の事項を認識することが望ましい。
>
> a) 適用は、サービスの提供に使用する技術、又は SMS におけるプロセスの自動化による影響を受けない。
> b) 使用する技術によって、ISO/IEC 20000-1 の要求事項に変更を加えることはできない。
> c) 技術は、ツール及びデータの要求事項、並びにプロセス活動の支援に必要な要員の技能に影響を与える可能性がある。
>
> （出典：ISO/IEC 20000-3:2012）

C.5.　SMS の適用範囲

C.5.1　SMS 適用の基本概念

ISO/IEC20000-1:2011 の 4.5.1 では、SMS の適用範囲を決定するための要求事項を提供しています。

サービス提供者は、SMS を確立する前に、SMS の適用範囲を定義する必要があります。

サービス提供者のトップマネジメントは、サービスマネジメントの計画が作成され、SMS の適用範囲が含まれていることを確実にする必要があります。SMS と適用範囲の定義は維持してゆくことが必要です。トップマネジメントは、有効性及び妥当性を可能にする、SMS の適用範囲のレビューに責任を持ちます。

C.5.2　SMS の適用範囲決定時の考慮事項

サービス提供者は、適用範囲の記述について評価者（認証機関など）と検討し、適用範囲の有効性を実証することが望まれます。

SMS の適用範囲外の顧客向けのプロセス及びサービスは、ISO/IEC 20000-1 に規定する要求事項を満たす必要はなく、またアセスメントにも影響や作用を及ぼしません。この除外について適用範囲の記述では言及する必要はありませんが、言及することで適用範囲の記述をより明確なものとするのに役立ちます。

サービス提供者が事業領域全体を SMS に含めようとする場合は、SMS の適用範囲の定義は比較的単純です。しかし、適合性の実証が、サービス提供者の一部のサービスの場合や、一つの顧客に対する一つの小規模サービスの場合などは、適用範囲を単純な用語で定義することや適用範囲の表現の不明瞭さを回避することは難しくなります。このようにサービスの一部を SMS に含めようとする場合には、適用範囲の記述が誤解を招くリスクを避けるために、適用範囲の記述に”

サービスの一部である旨”を明確に記載する必要があります。

サービス提供者は、SMS の適用範囲に複数の顧客に対する複数のサービスを含むことがあります。この場合、各顧客向けのプロセス活動の詳細は異なることもあると思いますが、各プロセスに対する規格の要求事項は満たす必要があります。

C.5.3 サービスの契約が SMS の適用に与える影響

顧客に対して法的に拘束力のある契約条件によってサービスを提供していても、この契約が ISO/IEC 20000-1 で規定する要求事項をすべて満たすというサービス提供者の義務が軽減されることはありません。同じく、すべての要求事項への適合性を十分な証拠に基づき評価するという評価者（認証機関など）の義務が削除されることもありません。これは、契約で提供するサービスやプロセスが制限されている場合でも、例外ではありません。すなわち、顧客との契約内容が「規格要求事項を全て満たす」という義務に影響を与えるものではないことを意味します。

C.5.4 SMS の適用範囲の定義と維持

サービス提供者は、SMS の適用範囲が不明瞭にならないよう、SMS の適用範囲を以下のパラメータを用いて定義することが望まれます。

a) サービスを提供する組織の単位（例えば、単一の部門、部門のグループ又はすべての部門）
b) 提供されるサービス（例えば、単一のサービス、サービスのグループ又はすべてのサービス、財務サービス、小売サービス、電子メールサービスなど）

（出典：ISO/IEC 20000-3:2012）

適用範囲の記述では、サービス提供に貢献している他の当事者の名称は記載してはいけません。

6.4.2 他のパラメタ

情報を追加することによって適用範囲の定義の曖昧さを避けることができる場合には、サービス提供者は他のパラメタを考慮することが望まれます。他のパラメタの使用については、この項の例、及びこの規格の附属書 B に示されています。

例：適用範囲の記述の構成

「<サービス提供者の場所>から<顧客組織の場所>の<顧客>に対して<技術><サービス>を提供する<サービス提供者の組織単位名>の SMS」

これらのパラメタは、サービス提供者が適切とみなすものであれば、どのような順序で用いてもかまいません。また、他のパラメタを用いることもできます。

SMS の適用範囲の定義には、個々の顧客を明確に記載することなしに、複数の顧客を含めることができます。例えば、場所を明記したデータセンターから提供されるすべてのサービスを参照する、あるいは、すべてのデータ保管サービスを参照することによってこれが可能になります。

サービス提供者は、他の当事者又は外部組織については、たとえ SMS 及びサービスに貢献しているとしても、その名称を含めないことが望まれます。

（出典：ISO/IEC 20000-3:2012）

適用範囲の記述で使用されているパラメータは、時間の経過と共に有効でなくなる可能性があります。SMS の適用範囲及び適用範囲の記述はサービス名やサービスの内容、顧客の追加・解約などの変化によって、曖昧又は無効とならないよう定期的に有効性をレビューすることが望まれます。

サービス提供者は、適用範囲の変更※4) を行うことがあります。当初一部のサービスのみに適用していた SMS のサービスを増やしたり、これまで供給者によって提供されていた新たなサービスを含めることで適用範囲を拡大したり、サービスの終了など、SMS の適用範囲の縮小を行うことも考えられます。サービスの変更に際しては、SMS 及び適用範囲記述書の両方の改訂が必要です。SMS の適用範囲への重大な変更※5) は、改善プロセスやその他変更のためのプロジェクト又はプログラムを用いて管理することによって、当該サービスについて ISO/IEC 20000-1 の要求事項への適合を確実なものにします。改訂した SMS に対しては、通常、初回に行われる SMS のアセスメントと同様に再アセスメントを実施する必要があります。

※注記の説明：

4）適用範囲の変更は、戦略的であれ、契約上の変更（サービスの拡大や終了など）であれ、“重大”とされる変更については、サービスの規模、数に対する“増”と“減”の両方を考える必要があります。

それに伴う実際の変化は、サイトの移転や人員削減、増員、資産の追加、減却等、事業・サービスの拡大、縮小に伴い様々であり、認証取得だけを考えた場合には、「ISO/IEC 20000-1 の適用サービスを増やす」という表現を用いることもあります。

5）“重大な変更” 時の考慮事項は、次の三つに整理できます。

ⅰ． JIS Q 20000-1 の箇条 5 による管理を用いてサービスリスクを最小にし、JIS Q 20000-1 の適合を確実にする

ⅱ． 変更範囲においてアセスメントを新たに行う（再アセスメント）
これは上記 i に対するチェック機能（内部監査、その他の評価）と考えると良いでしょう

ⅲ． 結果を踏まえて SMS 及び適用範囲記述書の改訂を適切に行う

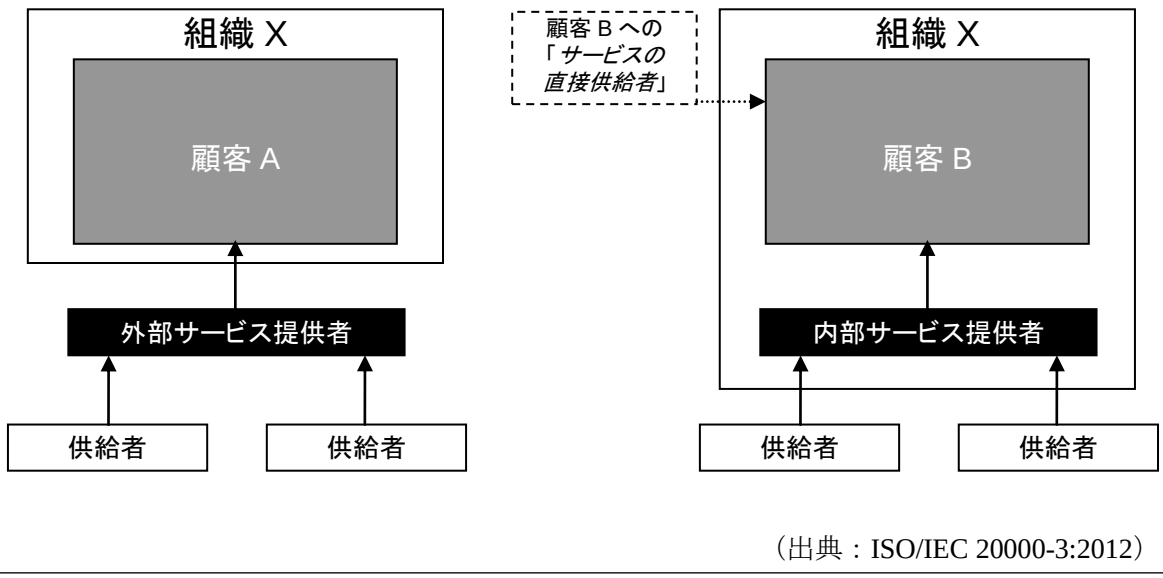
SMS の適用範囲が文書化後も有効であることを確実にするのは、サービス提供者の責任です。これは計画された間隔でレビューを実施し、実際の適用範囲と記述された適用範囲との不一致が無いように適用範囲の記述書を修正しなければなりません。相違が大きい場合は、再アセスメントが必要です。サービス提供者の適用範囲の正確性及び有効性を検証するのは評価者の責任です。

C.5.5　SMS の適用範囲において一部のサービス又はプロセスを委託している場合の考え方

顧客に提供するサービスの一部を供給者又は内部グループに委託している場合であってもISO/IEC 20000-1 に基づく SMS の導入に問題はありません。

効果的な SMS の適用範囲の確立及び有効な適用範囲記述書の定義を行うためにサービス提供者は、サプライチェーン内の組織間の関係が、影響することを認識されることが望まれます。サプライチェーンに関わる 2 つの例が図 C-1 に示されています。

1 つは、顧客 A と組織外部のサービス提供者との単純な関係を示しています。組織外部のサービス提供者は、ISO/IEC 20000-1 の規格の 4.2 項「他の供給者が運用するプロセスのガバナンス」への適合を実証する必要があります。もう 1 つは、顧客 B と同じ組織に属するサービス提供者（内部サービス提供者）と顧客 B に直接サービスを提供する供給者（直接供給者）との関係を示しています。この場合、直接供給者は、顧客 B の直接管理下にあり内部サービス提供者が直接供給者のガバナンスを持たないため、内部サービス提供者の SMS の適用範囲記述において適用外を明示する必要があります。



（出典：ISO/IEC 20000-3:2012）

図 C-1 供給者との関係

サービス提供者が複数の供給者をもつ場合、そのうち 1 社を統括供給者に指定することが一般的です。図 C-2 には、このような統括供給者を含めた 4 段階のサプライチェーンが示されています。サービス提供者の SMS の適用範囲を定義するためには、プロセスの運用を行う統括供給者とプロセスのガバナンスを行うサービス提供者との責任区分を明確にすることが望まれます。SMS の適用範囲は、サービス提供者が次を理解することによって簡単に定義することが出来ます。

a）プロセスガバナンスに何が必要か
b）どの組織が、各プロセスのどの部分を運用するか
c）統括供給者はどの組織か　（出典：ISO/IEC 20000-3:2012）

サービス提供者は、サービスがサプライチェーンのどこから始まるかにかかわらず、サービスの全般的な責任をもつことが求められます。

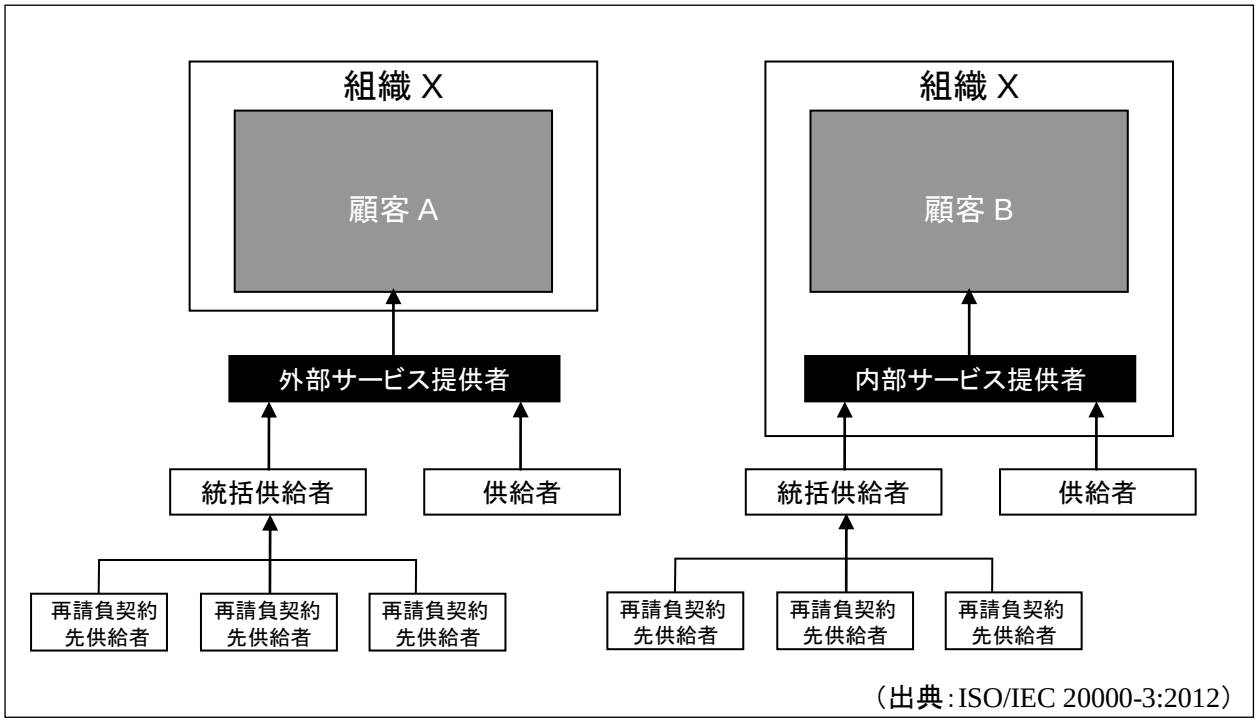


図 C-2 統括供給者と再請負契約先供給者の関係

サービス提供者は、ISO/IEC 20000-1 に規定する供給者管理の要求事項への適合を実証することが求められます。その際、サプライチェーン内の他の組織が ISO/IEC 20000-1 へ適合しているか否かは関係ありません。

重要なことは、サービス提供者が、他者の責任の定義及び合意を含む、当該のプロセスのガバナンスをもっていることであり、1 つのプロセスが複数の組織で実行される場合であっても、そのプロセスのガバナンスはサービス提供者が保有していなければならないと言うことです。

C.5.6 供給者、統括供給者及び、再請負契約先供給者

サービス提供者が複数のサービス供給者に委託する場合、サービス提供者はその内の 1 つの供給者を統括供給者に指名することが出来ます。

このような場合、図 C-2 に描かれているように、（図 C-1 の）3 階層のサプライチェーンは、4 階層のサプライチェーンになり、サービス提供者と統括供給者が直接の契約を有する関係になります。

統括供給者は、この契約の配下のチームとして、再請負契約先供給者管理をサービス提供者に代わってすることが望まれます。

再請負契約先供給者は、統括供給者との契約であり、サービス提供者との契約ではありません。そこには、サービス提供者の SMS の適用範囲に従った明確な責任が統括供給者にあります。

図 C-2 は、サービス提供者によって運営され、統制されるプロセスの内、いくつかを統括供給者が運用するケースを示しています。

統括供給者によって運用されるプロセスに関するサービス提供者のガバナンスが、統括供給者との契約によって妨げられる場合、サービス提供者は、ISO/IEC 20000-1:2011 の 4.2 項（他の関係者が運用するプロセスのガバナンス）の確認ができないことになります。

C.5.7　複雑なサプライチェーンの為の要求事項

サービス提供者は、しばしばサプライチェーンが図 C-2 に描かれている 4 階層のサプライチェーンより複雑であることに気付くでしょう。

その際､サービス提供者が以下のことを理解することによって SMS の適用範囲は明確になります。

a）各プロセスのガバナンスに何が必要か

b）どの組織が、各プロセスのどの部分を運用するか

c）統括供給者はどの組織か

サービス提供者は、サービスの起点がサプライチェーンのどこから始まろうとも、サービスに関する全体の説明責任を求められます。

C.5.8　内部サービス提供者および外部サービス提供者の両方としてのサプライヤ

図 C-3 は、顧客 G の内部サービス提供者が、インフラストラクチャ管理サービスについての ISO/IEC 20000-1 への適合を実証したシナリオを示しています。

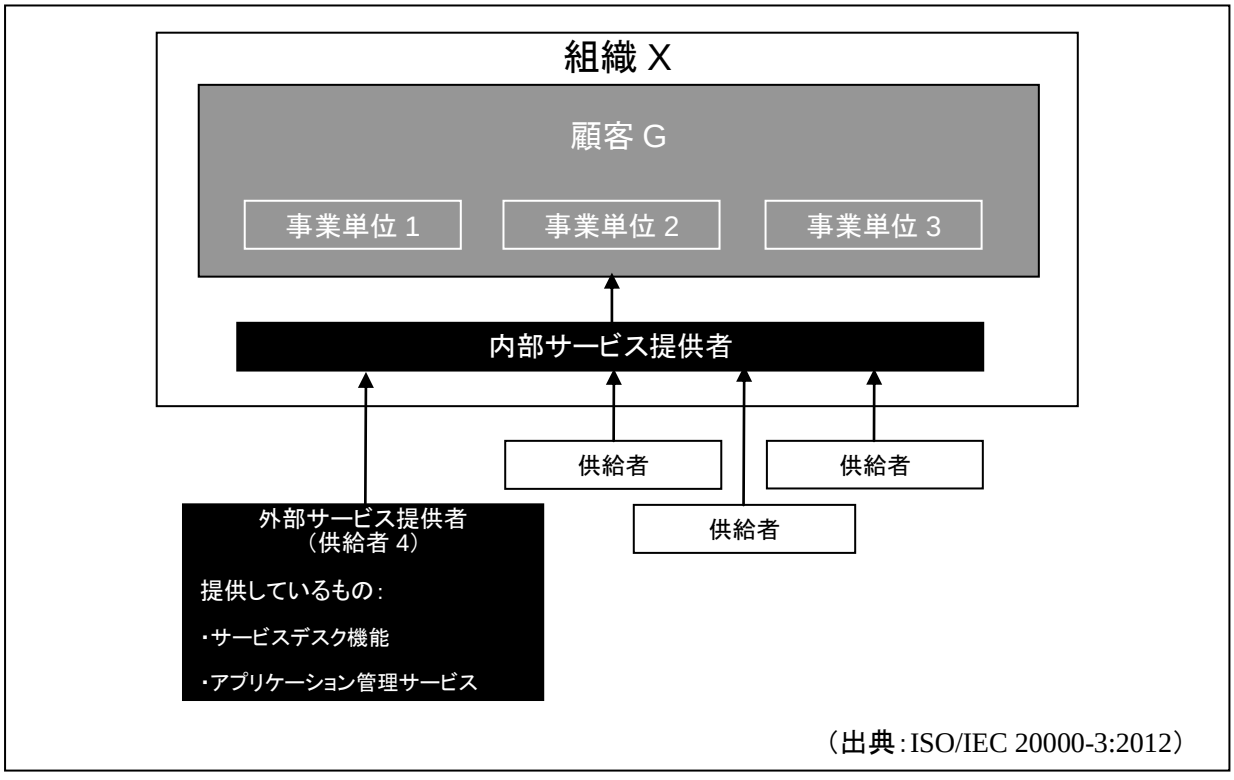


図 C-3 シナリオ 1

顧客 G の内部サービス提供者が ISO/IEC 20000-1 への適合を実証済である場合に、供給者 4 は ISO/IEC 20000-1 への適合を実証できるでしょうか？

特定の条件を満たす場合、可能です。

供給者 4 が、他の顧客又は供給者 4 自らの組織に提供するサービスについての適合を実証することは可能です。

ISO/IEC 20000-1 への適合を実証済のサービス提供者への供給者であることは、その供給者が ISO/IEC 20000-1 への適合を実証できないことを意味するわけではなく、供給者 4 が顧客 G に提供しているサービスのみに基づいて適合を実証することはできないことを意図しています。

図 C-3 及び図 C-4 に示す供給者 4 は、より大きな組織である組織 V に属しています。組織 V の一部は、顧客 H の外部サービス提供者です。組織 V のこの部分は、ISO/IEC 20000-1 への適合を実証可能です。組織 V のこの部分はまた、「他の顧客」への外部サービス提供者、及び組織 V の内部利用者への内部サービス提供者でもあり、これを図 C-4 に示しています。

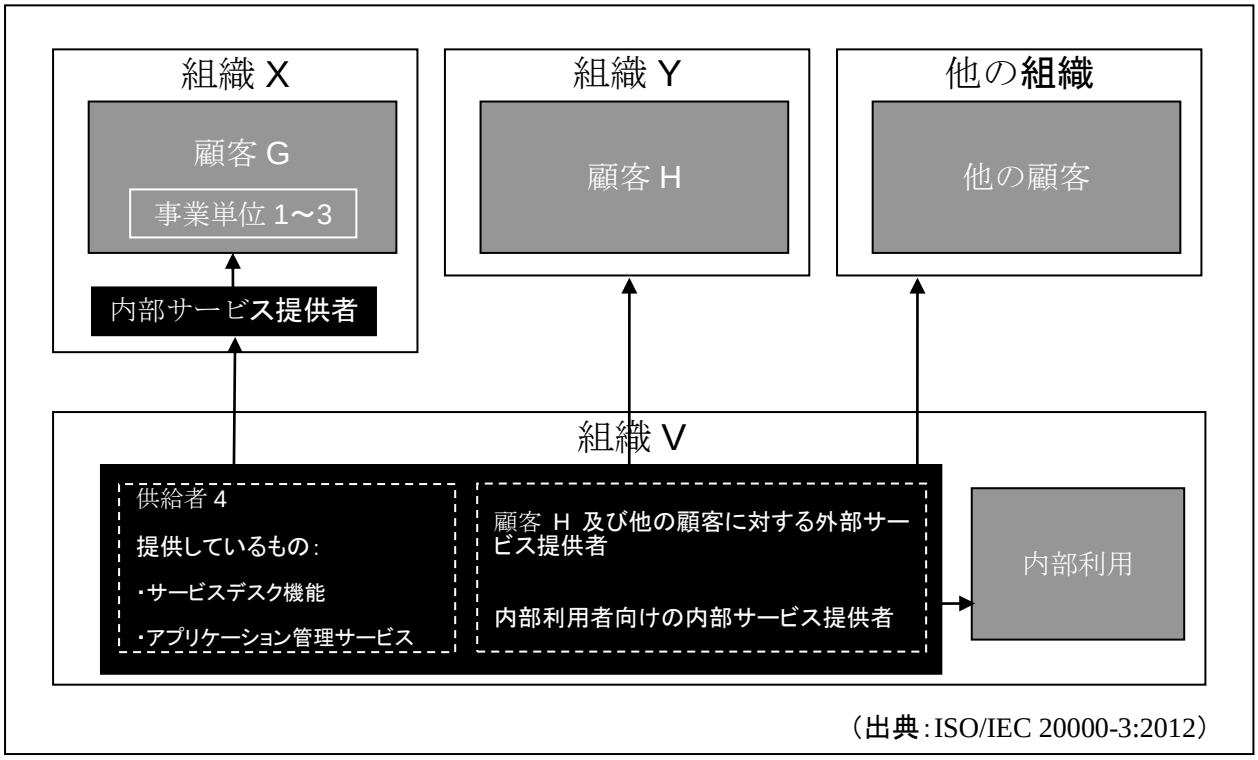


図 C-4 組織 V に属する供給者 4

顧客 H にサービスを提供する組織 V のこの部分は、有効な適用範囲の記述書を含む、SMS を定義し、確立することが求められます。その適用範囲は、すべての要求事項が満たされていること、及びプロセスガバナンスが実証される場合にのみ反映することができます。

【供給者組織 V の適用範囲の記述書例】

例：組織 V による、顧客 H 向けの全てのサービス提供を支援する SMS

上述の適用範囲の記述書の例は、比較的シンプルです。実際のサービスは変化するものである

ため、通常「サービス」という語のみで表すのではなく、はっきりと一覧によってサービスを示すことが推奨されます。顧客 H に言及することで、SMS の適用範囲が顧客 G、他の顧客又は内部利用者を含まないことが明らかになります。

この適用範囲の記述書の例には、地理的場所又は所在地の参照がないため、すべての所在地が含まれることを示唆しています。これが正確ではない場合、明確な所在地の参照を含むことが望まれます。サービス提供者の要員が多くの所在地に配備されている場合、「すべての所在地」と明記することが推奨されます。

C.5.9　複雑なサプライチェーンとプロセスのガバナンス

図 C-5 は、より複雑なサプライチェーンのシナリオを示しています。組織 W の一部であるこのサービス提供者は、外部顧客である顧客 K、L、M について、ISO/IEC 20000-1 の一部のプロセスのみの要求事項を満たすことが可能です。

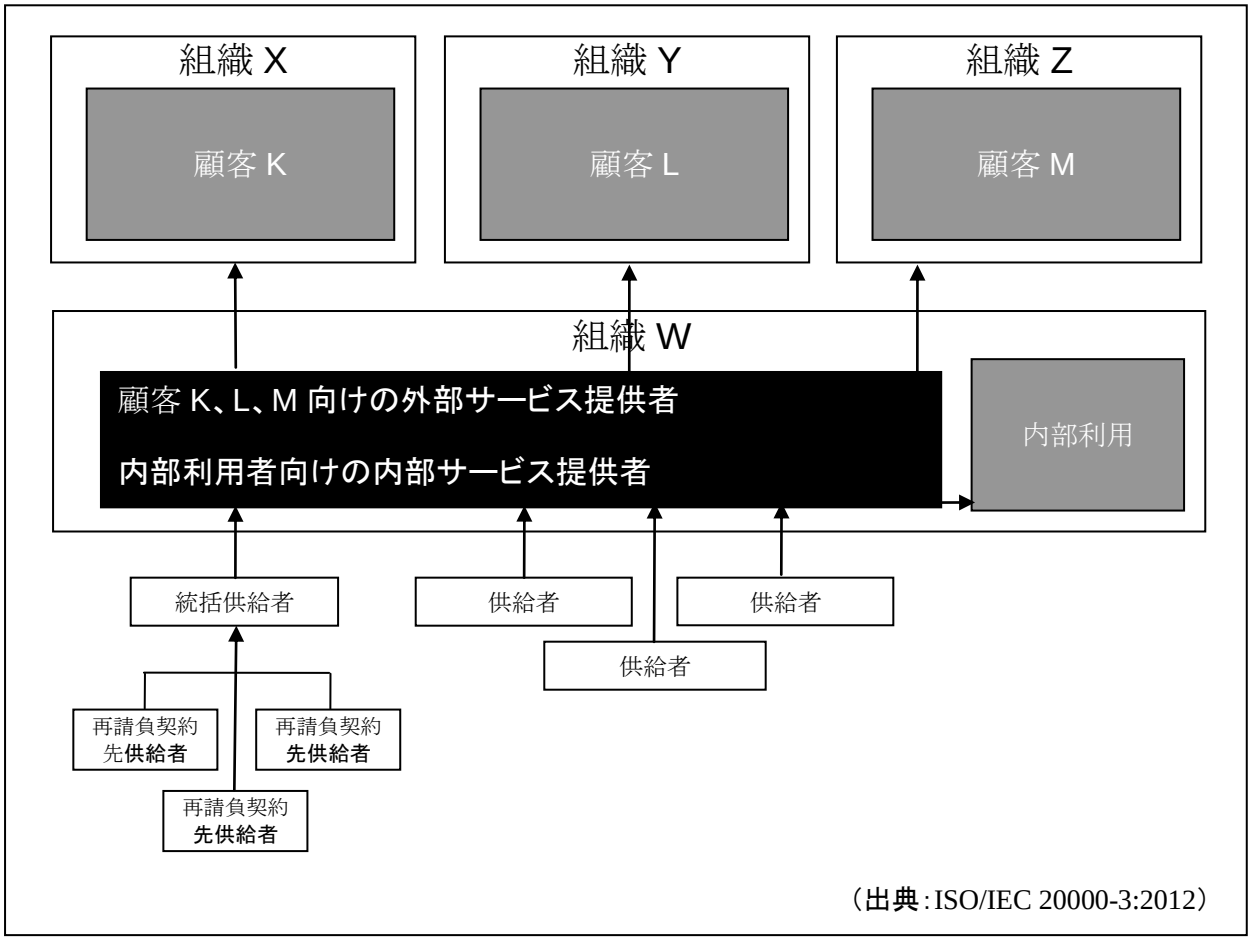


図 C-5 シナリオ 2

サービス提供者は、ISO/IEC 20000-1 への適合の実証を可能にする適用範囲を定義できるでしょうか？

サービスマネジメントの適用範囲及び適用範囲の記述書が、外部顧客に提供されるサービスだけに関係している場合は、できません。

サービス提供者自身の内部サービスが、ISO/IEC 20000-1 の全範囲のプロセスによって支えられている場合には、サービス提供者は、内部サービス提供者としてその SMS の有効な適用範囲を定

義できますが、適用範囲の記述書では、これが内部サービスのみに基づいていることを明確にする必要があります。

このサービス提供者は、顧客と合意したサービスと、供給者と合意したサービスとの間の調整が不十分である可能性があります。通常、これを確認し、計画された改善の初期段階で是正する必要があります。

組織 W は、適用範囲内のすべての顧客を支援するための SMS をもっていることを実証可能な場合、認証の対象となる可能性があります。

すべてのプロセスが内部利用者全体にわたって運用される場合、適用範囲は次のようになる可能性があります。

【組織 W が内部サービス提供者として活動する場合の適用範囲の記述例】

例：組織 W による、内部利用者向けの全ての IT サービスの提供を支援する SMS

付録D　サービスマネジメントのためのプロセス参照モデル
（ISO/IEC TR 20000-4:2010 の要点）

D.0. はじめに

ここでは、『ISO/IEC TR 20000-4:2010』を独自に翻訳し、その要点を引用又は整理した内容を紹介します。

D.1. ISO/IEC TR 20000-4:2010 の構成

ISO/IEC TR 20000-4:2010 は以下の内容で構成されています。

【目次】

D.2. ISO/IEC TR 20000-4:2010 の適用範囲

ISO/IEC TR 20000-4:2010 は、ISO/IEC 20000 規格群の一部であり、ISO/IEC 20000-1 の要求事項の範囲を明示するプロセス目的及び成果の観点から記述した、一連のプロセスから成るプロセス参照モデル（PRM：process reference model）を定義しています。

D.3. ISO/IEC TR 20000-4:2010 の目的

この規格は、ISO/IEC TR 15504-8 に規定されているプロセスアセスメントモデル（PAM）の開発を促進することを目的としています。

この PRM は、ISO/IEC 20000-1 で示されているサービスマネジメントシステム（SMS）のプロセスについて、構成要素を論理的に表現しており、各プロセスは目的及び成果の観点から抽象的なレベルで記述しています。なので、実際に PRM を用いる場合は、環境及び状況に適した追加の構成要素が必要となるかもしれません。

この PRM は、ISO/IEC 20000-1 の要求事項を満たすために必要なプロセスの能力レベルを事前に決定するものではありません。また、適合性評価審査のために用いることを意図したものではなく、プロセス導入の参照ガイドのために用いることを意図したものでもありません。さらには、ISO/IEC 20000-1 が要求する証拠を提供するものではなく、プロセス間のインタフェースを規定するものでもありません。

図 D-1 は、ISO/IEC 20000-1、ISO/IEC TR 24774、ISO/IEC TR 20000-4、ISO/IEC TR 20000-8、ISO/IEC TR 15504-8、及び ISO/IEC 15504-2 の関係を示したものです。

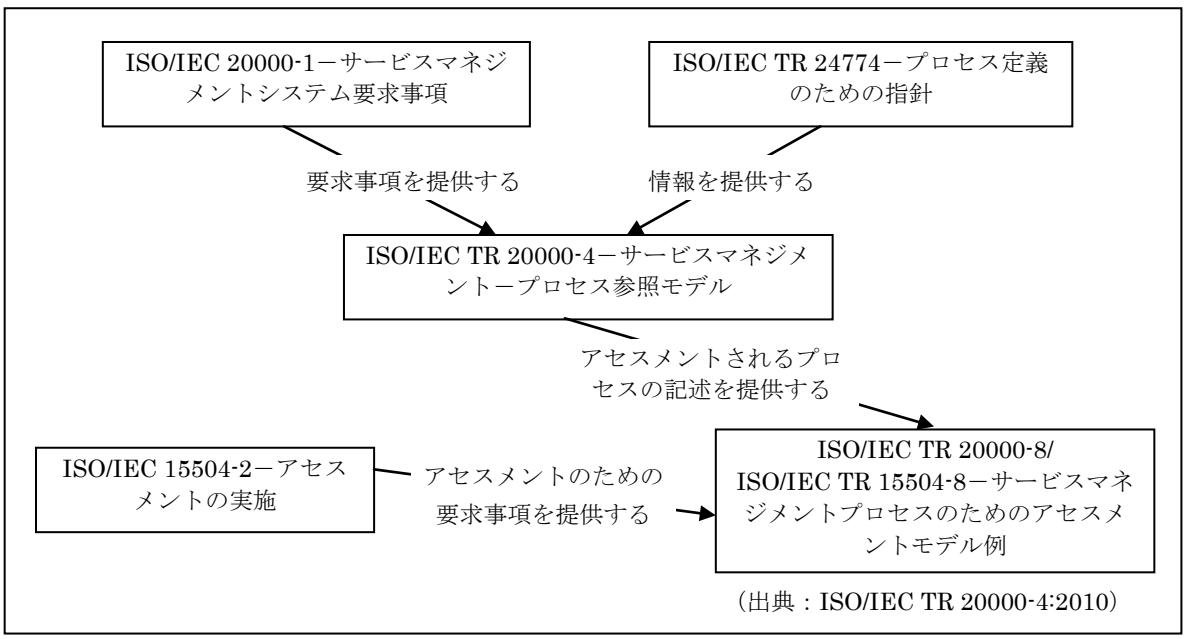


図 D-1－関連する規格間の関係

D.4. 引用されている規格

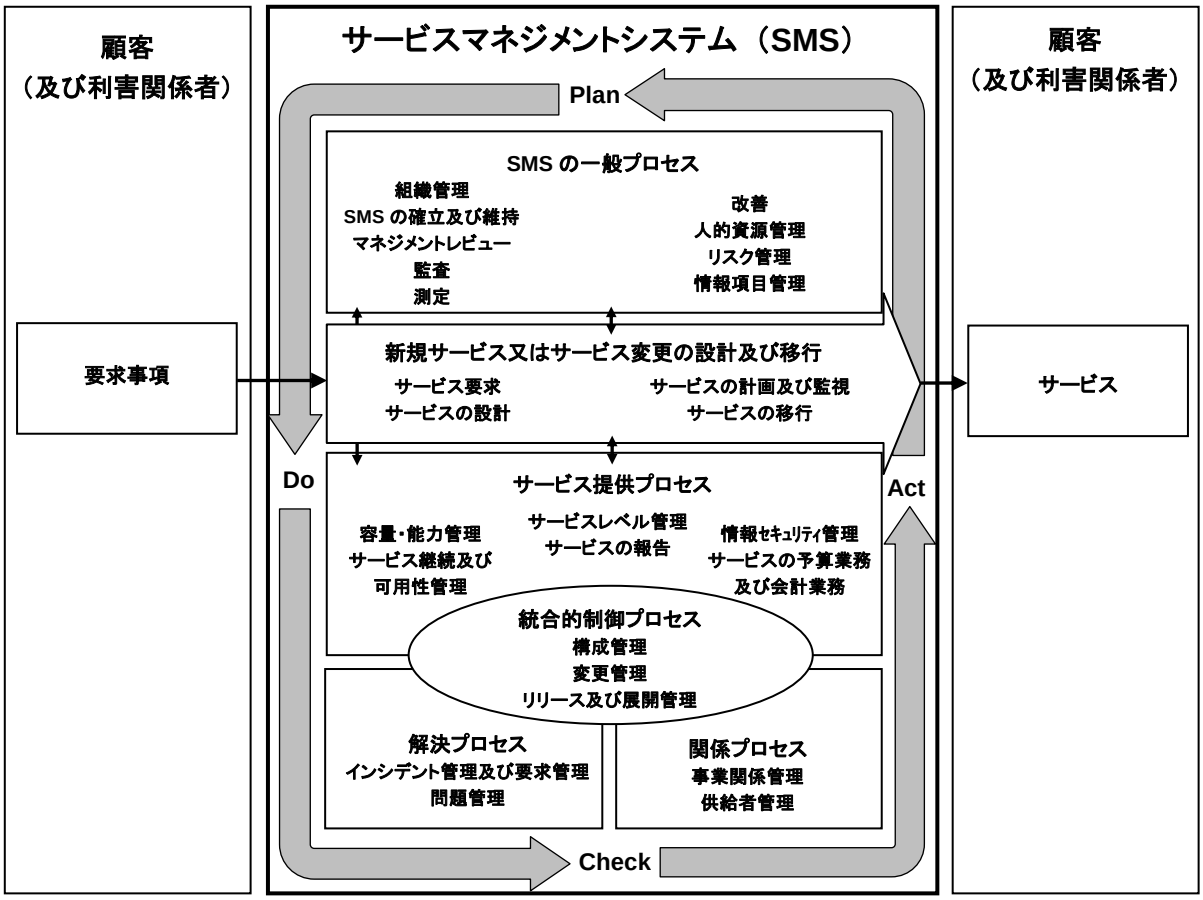
次に示した規格は、この規格から引用されており、規定の一部となっています。

・JIS Q 20000-1 情報技術－サービスマネジメント－第 1 部：サービスマネジメントシステム要求事項（ISO/IEC 20000-1）

・JIS X 0145-1:2008 情報技術―プロセスアセスメント－第 1 部：概念及び用語（ISO/IEC 15504-1）

D.5. サービスマネジメントのためのプロセス参照モデル

図 D-2 に、サービスマネジメントのための PRM に含まれる、ISO/IEC 20000-1 の要求事項に基づくプロセスを示します。



（出典：ISO/IEC TR 20000-4:2010）

図 D-2－プロセス参照モデルにおけるプロセス

D.6. プロセス記述の構成

PRM の各プロセスは、以下の記述項目で構成されています。

a) 名称：プロセスの名称は、そのプロセスの主要な事項を特定し、プロセスの適用範囲を要約したものです。

b) 状況：プロセスの適用について意図している状況です。
c) 目的：プロセスを実施することで達成する目標です。
d) 成果：プロセスの目的を達成した際の目に見える結果です。成果は、測定可能、有形、技術的、又は事業上の結果です。
e) 要求事項の追跡性：この欄には、ISO/IEC 20000-1 の該当する箇条（例：4.1）、箇条の標題、及び成果を示しています。

この規格の 5.2 から 5.27 では、「要求事項の追跡性」欄のすべての行の最後に、角括弧で括った数字（[n]）が記述されています。この角括弧内の数字は、成果欄の番号と対応しています。これらの成果は、ISO/IEC 20000-1 の要求事項と直接結び付けられています。

「成果」欄の中で、角括弧で示されているものは、ISO/IEC 20000-1 の要求事項とは間接的にしか結びつかないものです。これらの成果は、この規格の PRM が PAM（ISO/IEC 15504-8）の基礎としての機能を果たすために必要なので記載されています。これらの追加的な成果によって、このプロセスは完全なものとなり、プロセスの目的を達成することができます。同様の理由から、ISO/IEC 20000-1 の第 1 版（1ED）と第 2 版（2ED）の相互参照関係も記載しています。

D.7. プロセス記述の内容

ISO/IEC TR 20000-4:2010 では、5.2 から 5.27 に PRM の各プロセスについて、上述の記述項目にしたがって、記載されています。ここでは、「5.2 監査」と「5.3 IT サービスのための予算業務と会計業務」について、以下に示します。

監査

名称	監査
状況	監査は、SMS が効果的に確立され維持されているかどうか、及び SMS とサービスがサービス提供者によって確立された要求事項に適合しているかどうかを査定する。監査のための計画は、サービス、プロセス及び監査される領域の重要性と前回の監査結果を考慮に入れる。
目的	監査プロセスの目的は、選択されたサービス、製品、及びプロセスの要求事項、計画及び合意への適合性が第三者機関によって決定されること。
成果	このプロセスの導入に成功したときの成果 1. 適用範囲と目的が定義され[合意される] 2. 監査のやり方と監査員の選定についての客観性と公平性が保証される 3. 選択されたサービス、製品、及びプロセスの要求事項、計画及び合意への適合性が決定される 4. 不適合が記録される 5. 不適合は是正処置と解決に責任を持つ者に伝えられる 6. 不適合に対する是正処置が検証される
要求事項の追跡性	20000-1 1ED IS 04.3　監視、測定及びレビュー（Check）[1,2,4,5] 20000-1 1ED IS 04.4.1　継続的改善（Act）[5] 20000-1 2ED DRAFT 4.5.5.1　一般[4] 20000-1 2ED DRAFT 4.5.5.2　内部監査[1,2,5,6] 20000-1 2ED DRAFT 6.6.1　情報セキュリティ方針[3] 20000-1 2ED DRAFT 9.1　構成管理[4]

（出典：ISO/IEC TR 20000-4:2010）

IT サービスの予算業務及び会計業務

名称	IT サービスの予算業務及び会計業務
状況	予算業務は、費用の支出を予測及び制御し、予算を監視及び調整する。会計業務は、予算化された費用と比較し、予算からの差異を管理しながら、IT サービスの提供費用を明らかにする。すべての会計実務は、サービス提供者の組織全体のより広範囲の会計実務に整合させる必要がある。
目的	IT サービスの予算業務及び会計業務プロセスの目的は、サービス提供のために予算を編成し会計処理すること。
成果	このプロセスの導入に成功したときの成果 1. サービス提供の費用が見積もられる 2. 費用見積もりを使って予算が作成される 3. 予算からの逸脱と費用は制御される 4. 予算からの逸脱は解消される 5. 予算からの逸脱と費用は利害関係者に伝えられる
要求事項の追跡性	20000-1 1ED IS 06.4　IT サービスの予算業務及び会計業務[1,2,3,4,5] 20000-1 2ED DRAFT 6.4　サービスの予算業務及び会計業務[1,2,3,4,5]

（出典：ISO/IEC TR 20000-4:2010）

参考文献

ITSMS（IT サービスマネジメントシステム）関連

・ ITSMS ユーザーズガイド -JIS Q 20000（ISO/IEC 20000）対応-（JIPDEC）
http://www.isms.jipdec.or.jp/itsms/doc/JIP-ITSMS112-11.pdf

ISMS（情報セキュリティマネジメントシステム）関連

・ ISMS ユーザーズガイド（JIPDEC）
http://www.isms.jipdec.or.jp/std/index.html

ITIL 関連

・ ITIL 書籍『サービスストラテジ』（TSO 刊）
・ ITIL 書籍『サービスデザイン』（TSO 刊）
・ ITIL 書籍『サービストランジション』（TSO 刊）
・ ITIL 書籍『サービスオペレーション』（TSO 刊）
・ ITIL 書籍『継続的サービス改善』（TSO 刊）

特記事項

・ “®”（Registration symbol）は紙面と編集の都合上、省略いたします。本ガイドにおけるこの省略は、いかなる意味においても表示上の規約を無視し、登録商標の無断使用を容認するものではありません。
・ ITIL(R) is a Registered Trade Mark of the Cabinet Office.
・ その他、引用された社名、製品名は各社の商標もしくは登録商標です。

ＩＴＳＭＳ適合性評価制度技術専門部会

（順不同）

氏　名	所　属
メンバー	
熊谷　堅	KPMG ビジネスアドバイザリー株式会社
黒崎　寛之	㈱ヒルアビット【副主査】
小林　浩史	NEC ラーニング㈱
駒瀬　彰彦	㈱アズジェント
岡田　雄一郎	日本電気㈱
塩田　貞夫	洛ＩＴサービス・マネジメント株式会社【主査】
新川　敬郎	日本マネジメントシステム認証機関協議会
土屋　慶三	㈱日本シーエスアール認証登録機構
牧野　敬一朗	KPMG ビジネスアドバイザリー株式会社
丸山　満彦	デロイト　トーマツ　リスクサービス㈱
栗本　浩	㈱日立システムズ
オブザーバ	
監物　英樹	経済産業省　商務情報政策局
板屋　一嗣	経済産業省　商務情報政策局
宮尾　健	経済産業省　産業技術環境局

一般財団法人日本情報経済社会推進協会

〒106-0032 東京都港区六本木1丁目9番9号 六本木ファーストビル内

TEL 03-5860-7570　FAX 03-5573-0564

URL http://www.jipdec.or.jp/