ITSMS ユーザーズガイド

—JIS Q 20000 (ISO/IEC 20000)対応—

ITSMS：Information Technology Service Management System

IT サービスマネジメントシステム

平成 19 年 4 月 20 日

JIPDEC

財団法人　日本情報処理開発協会

はじめに

情報技術（IT）の発展と、IT によって提供されるサービス（IT サービス）の進展によって、個人のレベルでの利用から官公庁・自治体・企業での活用まで、今や IT を抜きに社会を語ることは難しくなっています。

こうした状況は IT サービスの提供者には、IT サービスを一定の品質でどのように提供するかという課題として認識されます。優れた IT サービスマネジメントシステム（ITSMS）を構築・管理・運用する知見に関心が向くのは、趨勢であるといえるでしょう。

ITSMS 適合性評価制度は、2006 年夏からのパイロット期間を経て、2007 年 4 月より本格運用を実施しています。本制度は、わが国の IT サービスマネジメント全体の向上に寄与し、諸外国からも信頼の得られるレベルの IT サービスを達成し、維持することを目的としています。

本制度に適用される認証基準は、JIS Q 20000-1 です。本ガイドは、JIS Q 20000-1 の要求事項について一定の範囲でその意味することを説明していますが、認証のための判断基準を規定することは意図しておりません。認証取得自体を合目的化する活動は、必ずしも IT サービスマネジメントの健全な普及と定着を意味しない場合が考えられます。そのため付録において、いくつかの JIS Q 20000 の利用シーンを想定した記述を入れ、最終的な目的をイメージしやすいようにしました。形骸化を忌避する一助としていただきたい。

本ガイドの主な読者は、ITSMS 認証取得を検討もしくは着手している事業者において、実際に ITSMS の構築に携わっている方及びその責任者を想定しています。JIS Q 20000 を理解する上での一助となり、ITSMS を構築・運用する上で参考となることを期待しています。

本ガイドの作成にあたり、ITSMS 適合性評価制度運営準備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。

2007 年 4 月

ITSMS 適合性評価制度技術専門部会
財団法人日本情報処理開発協会

目　次

0. 序文

0.1. 本ガイドの位置づけ

ITSMS ユーザーズガイド（以下、「本ガイド」という。）は、JIS Q 20000-1（以下、「本規格」という。）によって、情報技術（Information Technology：IT）（以下、「IT」という。）を用いて供される IT サービスマネジメントシステム（IT Service Management System：ITSMS）（以下、「ITSMS」という。）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）向けに作成したものです。

ITSMS で最も重要なことは、健全な IT サービスマネジメントの実現と定着のため、経営陣による関与（コミットメント）と継続的な改善の仕組みを構築することです。

本ガイドでは、本規格に記述された主要な条項を紹介し、要求する内容や意図、コンセプトなどについて解説しています。できるかぎり丁寧な解説を試みましたが、本規格の全てが網羅されているわけではありませんので、留意されたい。

なお、本規格の仕組みは ITIL（Information Technology Infrastructure Library）と補完関係にあり、ITIL 書籍を本ガイドと合わせて参考にされるとよいでしょう。

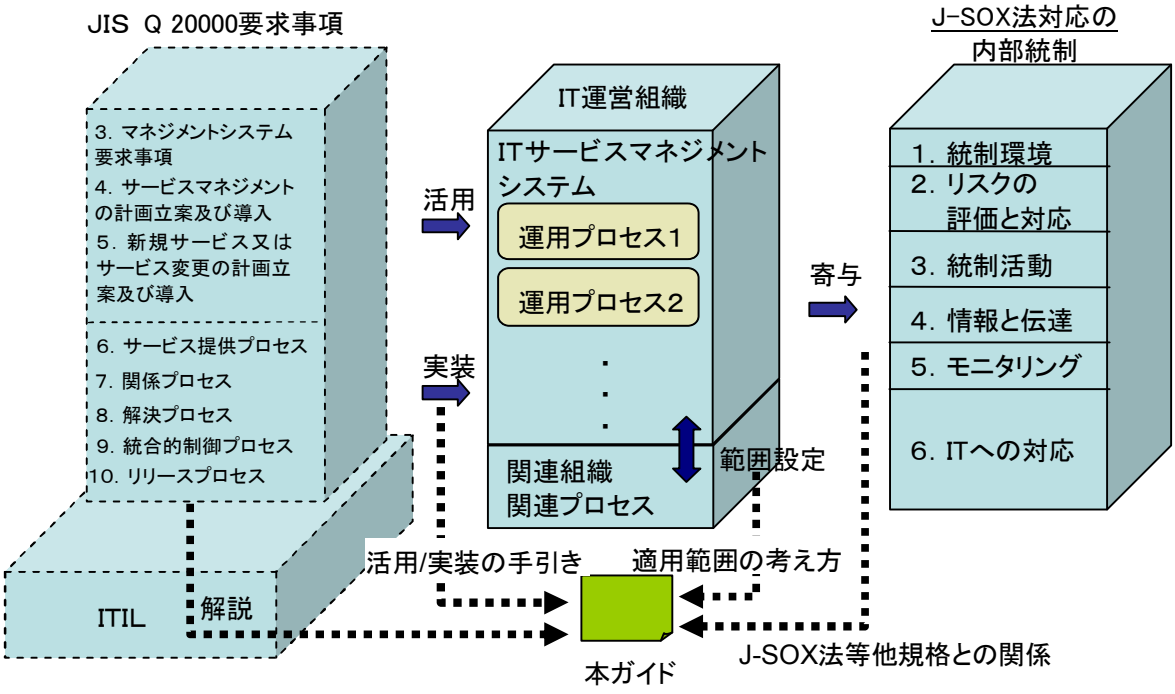


図 0-1　ITSMS ユーザーズガイドの内容

0.2. ITSMS 認証制度

ITSMS 規格化の経緯及び ITSMS 適合性評価制度について説明します。

0.2.1. ITSMS 規格化

ISO（国際標準化機構）と IEC（国際電気標準会議）の合同専門委員会(JTC1)配下の委員会 SC7 で審議が行われ、2005 年 12 月に ISO/IEC 20000 が制定されました。

それまでの経緯は、1989 年に英国政府が ITIL を IT サービスマネジメントプロセスのベストプラクティスとして発表し、その規格として、英国規格協会が、2000 年に英国規格 BS 15000 を制定した後、2004 年に国際規格の迅速化手続き（Fast Track Procedure）により ISO/IEC JTC1 に提出がなされ、国際規格として制定されたものです。日本では、2007 年 4 月 20 日に JIS Q 20000 として、制定されました。

JIS Q 20000 の構成は、次の２部構成になっており、ITSMS 構築には、これら要求事項を満たすことが必要となります。

- JIS Q 20000-1（第１部　仕様）

  事業上の要求事項及び顧客要求事項を満たす、管理されたサービスを効果的に提供するため、統合されたプロセスアプローチの採択を促進するものであり、顧客に受け入れられる品質の管理されたサービスを提供するため、サービス提供者に対する要求事項を規定しており、認証の基準となるものである。

- JIS Q 20000-2（第２部　実践のための規範）

  実践のための規範として、手引き及び推奨のかたちをとり、要求事項に沿った形で IT サービスマネジメントプロセス運営に対する推奨事項を記載したものであり、認証のための基準ではない。

JIS Q 20000 の概要を示します。

章	内容
1. 適用範囲	本規格の目的及び用途について、記述している。
2. 用語及び定義	本規格で用いる用語及び定義を説明している。
3　マネジメントシステム要求事項	ITSMS を支えるための要素（経営陣の責任、文書化、教育・訓練など）について、規定している。
4　サービスマネジメントの計画立案及び導入	ITSMS が備えるべき機能/活動について、PDCA サイクルにより規定している。
5　新規サービス又はサービス変更の計画立案及び導入	新規/変更のサービスを提供する場合に対応すべき事項について規定している。
6　サービス提供プロセス	ITIL のサービス提供に相当するプロセスに加えて、情報セキュリティ管理について規定している。
7　関係プロセス	顧客関係管理と供給者管理の側面を扱っている。
8　解決プロセス	インシデント管理と問題管理について、規定している。
9　統合的制御プロセス	構成管理と変更管理について、規定している。
10　リリースプロセス	リリース管理について、規定している。

0.2.2. ITSMS 適合性評価制度

ITSMS 適合性評価制度は、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です。ITSMS 適合性評価制度については、国際規格 ISO/IEC 20000-1 を基にして、2006 年 7 月にパイロット事業を開始しました。2007 年 4 月からの本格運用には、JIS Q 20000-1（以下、「本認証基準」という。）による認証が行われます。

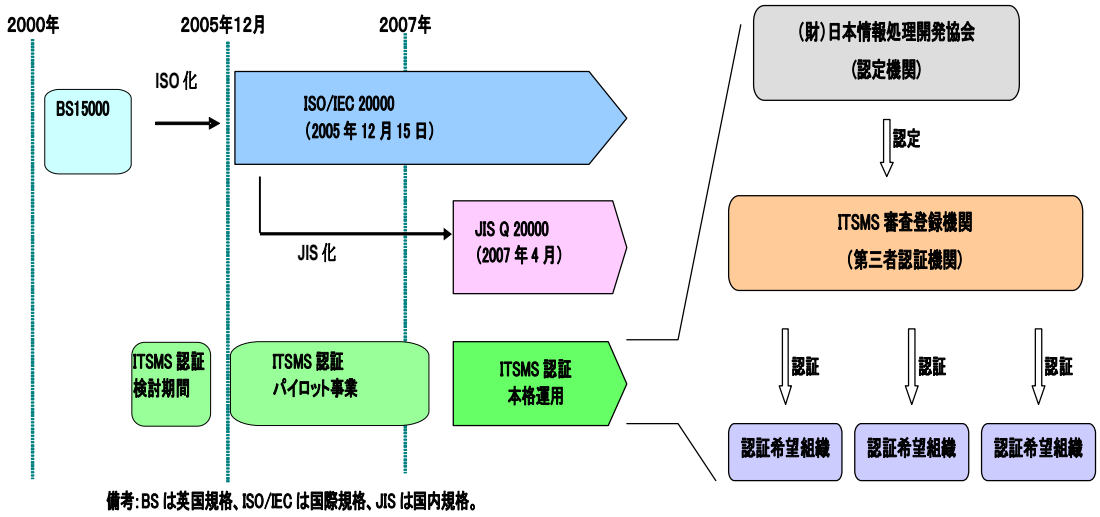


図 0-2 ISO/JIS 規格と認証スキーム

ITSMS 適合性評価制度の実施スケジュールは、図 0-3 に示す通りです。

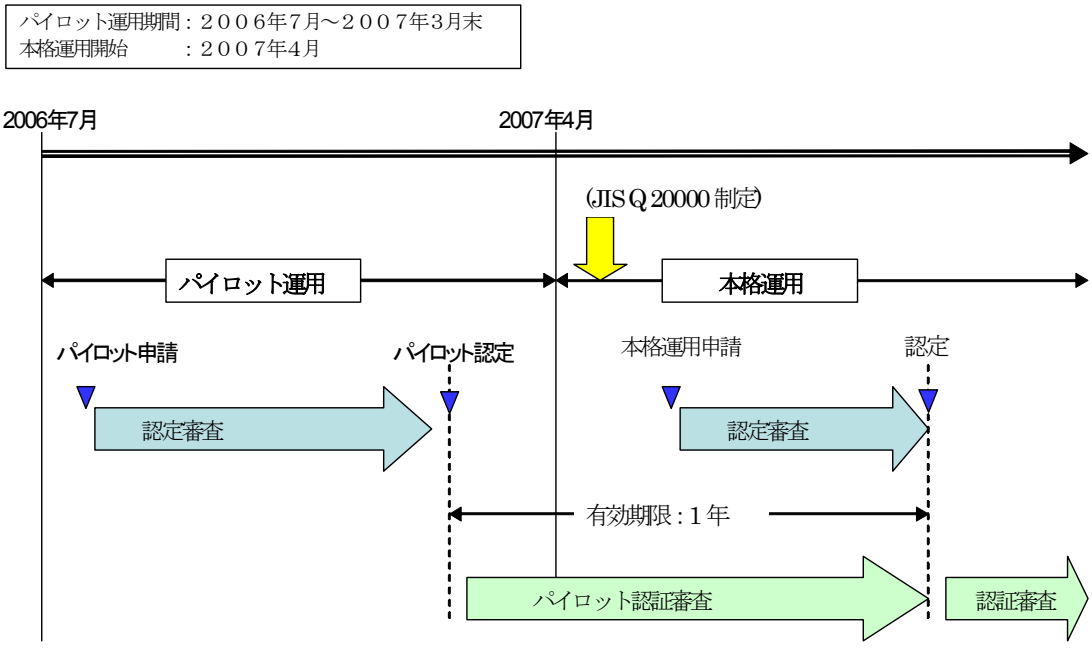


図 0-3　ITSMS 適合性評価制度実施スケジュール

0.3. プロセスアプローチと PDCA モデル

本規格は、組織が ITSMS を確立、導入、運用、監視、維持し、かつその ITSMS の有効性を改善するためのモデルを提供することを目的として作成されています。従って、サービス品質低下を引き起こす潜在リスクや今後のリスク変化に対応できる組織基盤を構築する抜本的な業務改革の目的に適しています。

0.3.1. 一般

一般に、業務改革はベンチマーキング（ベンチマーク基準）を活用すると成果が上がるといわれています。ここでのベンチマーキングとは組織内外のベストプラクティスに学ぶ手法のことを指します。本規格は、ITIL の IT サービスマネジメントプロセスにおけるベストプラクティスを基に規格化しているため、本規格を適用することで、組織におけるサービス品質の向上が期待されます。

ITSMS におけるベンチマーキングの目的は、リスクアセスメントにより明らかになった適用範囲内のサービス品質のリスク（サービス品質目標に対するリスク）に対応することです。そのためには、適用範囲内のプロセスを取り巻く環境を分析し、影響を及ぼすリスクの状態を適切に捉えることが重要です。このリスク及びリスクの変化を的確に認識するためには、管理対象を明確に規定したマネジメントが必要になります。

マネジメントを実施することによって組織のプロセス改革の方向性や方針が明確となり、これにより組織全体に IT サービスマネジメントに対する意識の高揚やその活動状況の測定等が徹底されます。更に、測定した結果をフィードバックすることにより改善が行われ、本質的なプロセス改革へとつながります。このことは、次のプロセスアプローチという考え方を採用することでより明確になります。

0.3.2. プロセスアプローチ

このプロセスアプローチという考え方は、品質マネジメントシステムの規格（JIS Q 9001:2000）等で紹介され、日本においても多くの組織で活用されています。プロセスアプローチでは、インプットをアウトプットに変換するために、経営資源を使用して運営管理されるあらゆる活動をプロセスとみなします。そして、組織内に存在するプロセスを明確にし、それらの相互関係を把握し、これら一連のプロセスをシステムとして適用して、運営管理する考え方のこと（アプローチ）を言います（図 0-4 参照）。このように、組織の IT サービスを管理するため、多くの活動を明確にした「プロセスアプローチ」を採用することを推奨しています。

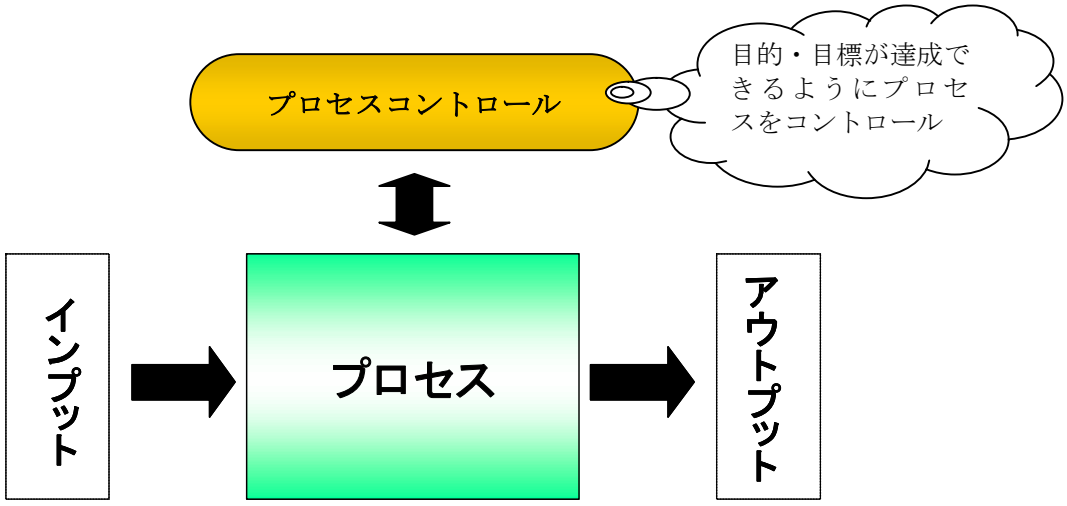


図 0-4 プロセスアプローチ

プロセスアプローチでは、それぞれのプロセスにおいて「インプット」されるものが何で、処理結果として「アウトプット」されるものが何かを多角的に検討し、明確にする必要があります。

ITSMS の構築では、ここで検討され明確にされた IT サービスに関する項目からプロセスに関与するサービス品質のリスクを識別し、適切に対応策を実施し運用していくことに繋がります。

つまり、ITSMS の構築を一連のプロセスとして捉え、各々のプロセスをプロセスアプローチに従って明確化し、その相互関係にあるインプットとアウトプットを把握することで、上記に示した ITSMS の構築に要求される重要な事項が認識できます。さらに、期待されるアウトプットを得るには、KGI（重要目標達成指標）、KPI（重要業績評価指標）などを用いてこのプロセスをコントロールすることが望まれます。

本規格では、他マネジメントシステムと同様に、ITSMS における管理手法としてプロセスアプローチを採用することを奨励し、それを実現するための考え方として「4　サービスマネジメントの計画立案及び導入」に示す「PDCA モデル」を提示しています。ITSMS

プロセスは、この PDCA モデルを採用することで整理され、組織の IT サービスマネジメントの管理体制に継続的な学習と改善の機会を提供します。

0.3.3. ITSMS 構築ステップ

この規格はプロセスについて規定した規格です。ITSMS は運営管理されたサービスを効果的に提供するための、統合されたプロセスアプローチの採用を奨励しています。認証を希望するサービス提供者は、運営管理されたサービスを提供するための、適切な高品質の統合プロセス群を実装しなければなりません。サービス提供者が全面的なマネジメントシステムが実施されていることを証明するためには、全ての必要なプロセスについて次のことを確実にすることが必須となります。

- プロセスを実施している
- 適切にプロセス同士が統合されている
- 効果的であるということを確実にするために管理し、監視されている
- 継続的改善のプロセスが適応されている

マネジメントシステムは規格の中心であり、認証を求めるサービス提供者は包括的なレベルの運営管理が実施されていることを確実にしなければなりません。標準的な、適合したマネジメントシステムは入力、出力、活動、全てのプロセスの関連を含んでいますが、又、ポリシー、計画、報告、継続的な改善、能力と訓練、予算のような高度なレベルの一般的なプロセスも含んでいます。

ITSMS の構築には次のようなステップが考えられます。

STEP1　現状分析
STEP2　マネジメントシステムの構築
STEP3　サービスマネジメントの計画と導入
STEP4　サービスマネジメントプロセスの導入

【STEP1　現状分析】

サービス提供者はまず、自組織の IT サービスマネジメント活動の現状（本規格要求事項への適合性）を分析します。現状を調査する際は、BIP0015（PD0015）などのセルフアセスメントを活用すると良いでしょう。

尚、この現状分析の結果より自組織の活動と本規格の要求事項とのギャップを洗い出し、そのギャップを埋めるための計画を立案します。この計画こそがサービスマネジメントの計画です。

【STEP2　マネジメントシステムの構築】

本規格に関連する標準的なマネジメントシステムとして次のようなものがあります。

- ISO9000 – 品質マネジメントシステム
- ISO27001 – 情報セキュリティマネジメントシステム

それぞれ、品質に関するマネジメントシステム、セキュリティに関するマネジメントシステムです。本規格におけるマネジメントシステムとは、IT サービスの品質に関して、経営陣を含めた組織がサービスを効果的に運営管理し、実施できるようにするものです。

マネジメントシステムの構築には下記の 3 つの領域での要求事項を満たす必要があります。

- 経営陣の責任
- 文書化に関する要求事項
- 力量、認識及び教育・訓練

【STEP3　サービスマネジメントの計画と導入】

品質マネジメントシステムでのデミング・サイクルを用いる、いわゆる PDCA サイクルの採用です。サービスマネジメントの実現に必要なサービスマネジメントプロセスの設計や達成すべき目標、各プロセスや担当するメンバーの役割や責任、サービス品質を管理、監査、改善する方法などを計画、そしてあらゆるプロセスに適応可能なプロセス改善サイクル（ITSMS のフレームワーク）を規定します。これをサービスマネジメントの計画と言います。

【STEP4　サービスマネジメントプロセスの導入】

STEP3 で立案した計画に従い、5 章の「新規サービス又はサービス変更の計画立案及び導入」と、6 章以降の 13 プロセスの導入をします。

尚、それぞれの領域における要求事項はすべてを網羅しているわけではないので、必要であれば目的及び管理策の追加をすることができます。

【ITSMS 構築のポイント】

ITSMS を構築する上でのポイントを以下に記載します。

- 経営者が深く関与する（経営者のリード）
- 組織横断的なプロセスアプローチの実現
  - ・プロセス単位に役割と責任を明確にする
  - ・プロセス間の相互関係（入力情報と出力情報）を明確にする
- サービスマネジメント目標及び各プロセスの KPI 設定と測定
  - ・測定可能な数値目標を設定、測定し、改善のための「きっかけ」とする
- 従来のサービス方法との乖離の極小化
  - ・ダブルスタンダード化を抑制する
  - ・ITIL に拘ることなく自らが一番やり易いやり方、効率的な手順を実装する

0.3.4. 他のマネジメントシステムとの両立性

本規格では、JIS Q 27002（情報セキュリティマネジメントの実践のための規範）が情報セキュリティ管理プロセスで引用されているだけで、他マネジメントシステムとの両立性に触れてはいません。

しかし、情報セキュリティマネジメントシステム（ISMS）や、品質マネジメントシステム（QMS）、環境マネジメントシステム（EMS）は、本規格で推奨する PDCA モデルを適用するマネジメントシステムであり、既存のマネジメントシステムの考え方を踏襲しながら、相互の調和や統合が可能です。

ISMS では、次のように説明されています。

> この規格は,関連するマネジメント規格と矛盾することなく統合して導入及び運用することができるように，JIS 9001:2000 及び JIS Q 14000:2004 との調和がとられている。
> (一部省略)この規格は，組織が自らの ISMS を，関係する他のマネジメントシステムの要求事項に調和させること又は統合することが可能なように設計されている。
> （JIS Q 27001:2006 0.2.3 他のマネジメントシステムとの両立 より引用）

ここでは、JIS Q 27001 規格制定後に本規格が制定されるため、ITSMS について言及されていませんが、本規格が参考文献として、JIS Q 9001:2000 の品質マネジメントシステムを挙げているように他のマネジメント規格と調和がとられているため、他のマネジメントシステムの要求事項に調和させること又は統合することができると言えます。例として、組織において ITSMS、ISMS、QMS を統合させた場合の概念を図に示します。

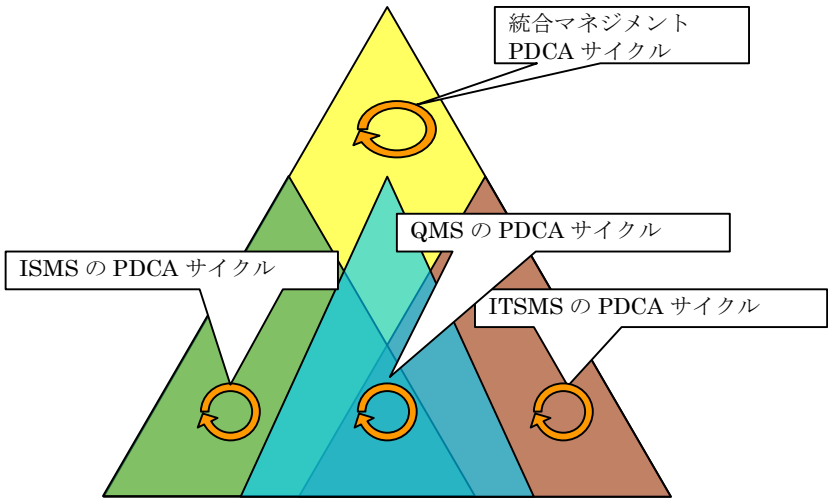


図 0-5　ISMS/QMS/ITSMS の統合（例）

0.4. ITIL とは

ITIL(Information Technology Infrastructure Library)は 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)と呼ばれています。

Library という名が示すように、ITIL は一連の書籍群から構成されます。1980 年代後半に英国 CCTA(Central Computer and Telecommunications Agency)により ITIL V1(Version 1)が制定され、初期は 40 冊程度の書籍から構成されていました。ITIL の策定には多くの公的機関、ベンダ、コンサルタント、ユーザが経験、知識を出し合い開発されています。1990 年代の後半に入ると、書籍群の重複部分の整理、改訂が計画され、7 冊の書籍にまとめられました。これが現在の ITIL V2 と呼ばれる書籍群です。コアになる書籍は、次の 7 冊です。(注 :『ビジネスの観点』は Part 1 と Part2 に分冊されて発行。)

- 『サービスサポート』: 日々の運用業務であるサービスデスク、インシデント管理、問題管理、変更管理、リリース管理、構成管理を含む
- 『サービスデリバリ』: 中長期的な視点の運用に関係するサービスレベル管理、キャパシティ管理、可用性管理、IT サービス継続性管理、IT サービス財務管理を含む
- 『サービスマネジメント導入計画立案』:サービスマネジメントの成熟度評価とそのプロセスの導入と改善の実用的なガイダンス
- 『セキュリティ管理』: IT サービスマネジメントに関わるセキュリティ管理
- 『ビジネスの観点 Part1＆2』: ビジネス関係管理、サプライヤ管理
- 『ICT インフラストラクチャ管理』: インフラストラクチャに関するライフサイクル管理
- 『アプリケーション管理』: アプリケーションに関するライフサイクル管理

ITIL は IT サービスマネジメントにおけるベストプラクティスの集大成ですが、規格ではありません。この ITIL V2 の発行後、ITIL を基に英国規格として BS 15000 と呼ばれる IT サービスマネジメント規格が制定されました。BS 15000 は BSI(British Standard Institute 英国規格協会)により 2000 年に初版が制定され、2002 年から改訂され、現在は 2 部構成となっています。2 部構成の内訳は BS 15000-1:2002 (Specification : 仕様) と BS 15000-2:2003 (Code of Practice : 実施基準) です。この他に補足的な文書として PD0005(Manager's guide)と PD0015(Self-Assessment Workbook) が発行されています。英国規格として BS 15000 が登場後、2003 年には、IT サービスマネジメントの普及・促進を目指す国際的なユーザーフォーラムである *it*SMF (IT Service Management Forum) から、BS 15000 に基づく IT サービスマネジメントの第三者認証制度が発表されています。

BS 15000 の国際規格化に向けて ISO(International Organization for Standardization : 国際標準化機構)と IEC (International Electrotechnical Commission : 国際電気標準会議) は事前調査を 2004 年に開始しました。2005 年にかけて、ISO/IEC に参加する加盟国 24 カ国により、Fast Track と呼ばれる迅速化手続きを経て ISO 化は承認

され、2005 年 12 月に ISO/IEC 20000-1 及び ISO/IEC 20000-2 として発行されました。本規格の大きな特徴は規格ありきではなく、IT サービスマネジメントの現場から生まれたベストプラクティス集が、まず BS 15000 の英国規格になり、ついで国際規格の ISO20000 に制定されていったという点です。

JIS Q 20000 の構成に沿って、ITIL との関連性について概観します。

まず１章にはこの規格が適用される「適用範囲」が、２章には「用語及び定義」が記述されています。ITIL との関係では、２章で定義されている用語は ITIL のそれと同じと考えてよいでしょう。

IT サービスマネジメントを構成するプロセス群を構築し、運営していくために、３～５章において PDCA モデルを採用した ITSMS の構築を定義しています。３章以降の全体図を図 0-6（図中の括弧内はこの規格での項目番号です。）に示します。

<table>
<tr><td colspan="3">適用範囲（１）</td></tr>
<tr><td colspan="3">用語及び定義（２）</td></tr>
<tr><td colspan="3">マネジメントシステム要求事項（３）</td></tr>
<tr><td colspan="3">サービスマネジメントの計画立案及び導入（４）</td></tr>
<tr><td colspan="3">新規サービス又はサービス変更の計画立案及び導入（５）</td></tr>
<tr><td colspan="3">サービス提供プロセス（６）

容量・能力管理
(6.5)
サービス継続及び
可用性の管理（6.3）

サービスレベル管理
(6.1)
サービスの報告（6.2）

情報セキュリティ管理
(6.6)
サービスの予算業務及び
会計業務（6.4）</td></tr>
<tr><td colspan="3">統合的制御プロセス（９）

構成管理（9.1）
変更管理（9.2）</td></tr>
<tr><td>リリースプロセス（１０）

リリース管理（10.1）</td><td>解決プロセス（８）

インシデント管理
(8.2)
問題管理（8.3）</td><td>関係プロセス（７）

顧客関係管理（7.2）
供給者管理（7.3）</td></tr>
</table>

図 0-6　JIS Q 20000 と IT サービスマネジメントのプロセス群の関係

3 章では、マネジメントシステムの要求事項として、経営陣の責任、文書化に関する要

求事項、力量、認識及び教育・訓練があります。この 3 章は、ISO9001:2001 の品質マネジメントシステムあるいは ISO27001:2005 といった他の ISO マネジメントシステム規格でのマネジメントシステム要求事項と整合性があります。本規格の基になっている ITIL V2 書籍の中では、マネジメントシステムの要求事項が 1 つの章立てあるいはコンポーネントとして記述されているわけではありませんが、3 章に関連する ITIL 書籍としては、『サービスマネジメント導入計画立案』が参考になるでしょう。

4 章では、サービスマネジメントの計画立案及び導入として、プロセス改善サイクルに関する要求事項を規定しています。プロセス改善サイクルは、デミング・サイクルの PDCA を次のように規定しています。

- サービスマネジメントの計画(Plan)
- サービスマネジメントの実施及びサービスの提供(Do)
- 監視、測定及びレビュー（Check）
- 継続的改善（Act）

ITIL 書籍『サービスマネジメント導入計画立案』では、IT サービスの供給開始あるいは改善のステップについて説明しています。継続的サービス改善プログラム(Continuous Service Improvement Programme：CSIP)を通じて、サービス供給の品質改善を目指しています。本規格のプロセス要求事項に頻出する“サービス改善計画”を立案する上での参考になります。

5 章においては、新規サービス又はサービス変更の計画立案及び導入の要求事項を規定しています。新規サービス又はサービス変更の導入は、6 章～10 章に含まれている多くのプロセスと密接な関係があります。

例えば、5 章の要求事項のひとつには、「新規サービス又はサービス変更の導入(サービスの終了を含む。)は，正式な変更管理を通して計画し，かつ，承認しなければならない。」（JIS Q 20000-1 5. 新規サービス又はサービス変更の計画立案及び導入より引用）と記述されています。これは 9 章の統合的制御プロセスの中の変更管理プロセスに従うことを要求事項としています。ITIL では新規サービスの導入についてはプロセスとしての明確な記述はありませんが、いくつかのサービスサポート、サービスデリバリのプロセスの中で、新規のサービスに言及していると読み取れる部分もあります。例えば、リリース管理におけるリリースの分類では、大規模なソフトウェアリリースや大規模なアップグレードに言及しています。また 5 章におけるサービス変更の計画立案と 9 章の統合的制御プロセスに含まれている変更管理プロセスの関係を記述している部分は規格の中にはありません。変更管理プロセスでは扱えないような大規模変更あるいは新規サービスについては、5 章のプロセスに沿って実施するか、9 章の変更管理プロセスを一部利用すると読み取れば良いように思えます。この仮定では大規模変更とそれ以外の変更の定義が必要になります。ITIL 書籍で 5 章に対応する部分は、『サービスマネジメント導入計画立案』に加えて『サービ

スサポート』、『サービスデリバリ』のいくつかのプロセスになるでしょう。

6 章以降では、IT サービスを運用管理するために必要不可欠な 13 のプロセスを 5 つのカテゴリに分類して、それぞれのプロセスの要求事項を規定しています。(括弧内はこの規格での項目番号です。)

- サービス提供プロセス（6）
  - サービスレベル管理（6.1）
  - サービスの報告（6.2）
  - サービス継続及び可用性の管理（6.3）
  - サービスの予算業務及び会計業務（6.4）
  - 容量・能力管理（6.5）
  - 情報セキュリティ管理（6.6）
- 関係プロセス（7）
  - 顧客関係管理（7.2）
  - 供給者管理（7.3）
- 解決プロセス（8）
  - インシデント管理（8.2）
  - 問題管理（8.3）
- 統合的制御プロセス（9）
  - 構成管理（9.1）
  - 変更管理（9.2）
- リリースプロセス（10）
  - リリース管理プロセス（10.1）

6～10 章ではITサービスマネジメントを構成している個別のプロセスに対する要求事項が規定されています。3～4 章において規定されているマネジメントシステムがあることで、6 章以降の個別プロセスを効果的に運用していくことができます。5 章の新規サービス又はサービス変更の計画立案及び導入を含めて、広い意味では 3~10 章はプロセスとして論じられていると言えるでしょう。

IT サービスマネジメントのプロセスは互いに密接に関係していますが、規格の中では、プロセス間の相互関係あるいは依存関係は明記されていません。必要に応じて『サービスサポート』、『サービスデリバリ』を参照することをお奨めします。

1. 適用範囲

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、効果的に行うための仕組みです。仕組みを構築するに当たって、提供する IT サービスの品質を、あらかじめ顧客と合意したレベルに維持していくためには、IT サービスマネジメントの全てのプロセスにおいて、要求事項を規定していくことが重要であることを、本規格では以下のように説明しています。

> この規格は，顧客に受け入れられる品質によって運営管理される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する。
>
> （JIS Q 20000-1:2007 1. 適用範囲 より引用）

IT サービスマネジメントを導入することにより、以下のような効果が期待されます。

- ビジネスニーズに対応した IT サービスの提供
- IT サービスの品質の向上
- 長期的視野からの、IT サービスにかかるコスト削減
- ビジネスへの貢献度の向上
- IT サービスの可視化
- 顧客満足度の向上

> この規格は，次の事業，組織又は用途に利用してもよい。
> a) サービス調達を入札に付そうとしている事業
> b) サプライチェーンに属するすべてのサービス提供者に対し，一貫した取組みを求める事業
> c) 自らのサービスマネジメントを比較評価するサービス提供者
> d) 独立したアセスメントのための基盤
> e) 顧客要求事項を満たすサービスを提供する能力をもつことを実証する必要がある組織
> f) サービス品質の監視・改善プロセスを効果的に適用することによって，サービスの改善を目指す組織
>
> （JIS Q 20000-1:2007 1. 適用範囲 より引用）

事業、組織については詳細な説明が無いために、a)～f) 項の例示について、それぞれに想定することが可能です。

a) サービス調達を入札に付そうとしている事業

この規格はサービス提供者に向けられたものですが、顧客にとっても有益なのが、入札に当たってこの規格を活用することです。

顧客は、サービス提供者から受けるサービスの品質を確保するために、入札に際して SLA に盛り込んでいく数値目標などを条件として提示しますが、それ以外に、サービス

提供者としての指針や具体的な実装方法などにも踏み込んだ記載を求める時代に入っています。そのときに、数値化されない指針や具体的な実装方法については、顧客とサービス提供者の間では、共有化された規格が今までは存在しませんでした。本規格を用いることによって、信頼できるサービス提供のプロセスを有していることを評価できるようになります。

b) サプライチェーンに属するすべてのサービス提供者に対し、一貫した取組みを求める事業

顧客が、ビジネスプロセスを実現するに当たって、単独のサービス提供者によって全てを遂行することが出来るとは限りません。むしろ、複数のサービス提供者がその得意とする持ち味を活かして提供しているサービスを組み合わせることで、より効率的で適正な業務処理が可能になることの方が多いとも言えます。こうした場合には、最終の品質を確保するためには、関係する全てのサービス提供者に、一定水準の品質を確保するために要求する数値化された基準及び定性的な必要要件の達成度合いを評価する尺度及びその仕組みが必要になります。この規格は、提供するサービスの内容が異なる複数のサービス提供者に対しても共通に適用可能な基準として、活用できます。

c) 自らのサービスマネジメントを比較評価するサービス提供者

サービス全般にわたって適用可能というこの規格の特性を利用することで、サービス提供者は内部の複数のサービス提供部門のマネジメントを比較検討する際の基準として使うことができます。あるいは事業上競合している他のサービス提供者の、サービスマネジメントとの比較評価に用いることが可能です。

d) 独立したアセスメントのための基盤

サービスの提供プロセスの改善を考えたとき、まずは現状を把握し、しかるべき基準とのギャップを分析し、対策を立てるという手順がとられます。この規格は、ギャップを分析する際の基準として用いることができます。この規格は、客観的な視点からプロセスを規定しているので、プロセスの網羅性や十分性の診断に用いることが可能なのです。

e) 顧客要求事項を満たすサービスを提供する能力をもつことを実証する必要がある組織

今日のビジネス環境において、サービス提供者は、顧客の要求を満足する IT サービスを提供できる能力を実証することが求められています。

この規格を満たす IT サービスを提供することは、サービス提供者として、少なくともこの規格が要求しているプロセス全てを有し、PDCA による改善サイクルを回していることが満たされていると言えます。

更に、認証を取得すれば、中立の第三者によって評価されることから、その重みは一層増します。

f) サービス品質の監視・改善プロセスを効果的に適用することによって、サービスの改善を目指す組織

サービス全般にわたって適用可能ということがこの規格の特性の一つですが、まさにPDCA を回していく品質の改善の標準的な仕組みが、この規格のエッセンスであります。従って、IT サービスを提供者である「サービス提供者」、「ユーザ」、「顧客」、「サプライヤ」など、全ての組織で、適用が可能です。

サービス提供者では、そのサービス提供プロセスのマネジメントに適用することでPDCA の改善サイクルを導入することができ、「顧客」は、サービス提供者から提供されるサービスの品質を監視する際の、網羅性のチェックリストとして活用することなど、その立場によって様々な活用法が考えられます。

今日のビジネス環境において、サービス提供者は、顧客の要求に答えることが出来る IT サービスを提供できる能力を有することを実証する必要があります。本認証基準を満たす IT サービスの提供は IT サービスマネジメントの業界標準を満たすことを表しています。

組織をサービス提供者と仮定すれば、サービス提供者は本認証基準を以下のように利用することが出来ます。

- 提供している IT サービスの品質を監視し、改善する
- ベンチマーキング
- 認証取得への基礎
- 基準を満たす IT サービス提供能力の実証

IT サービスの提供に責任を持つサービス提供者は組織の内部にある場合もあれば、外部組織にアウトソーシングされていることも考えられます。あるいは、IT サービスの提供に必要なプロセスの内のいくつかを外部の組織にアウトソーシングしているケースもあると考えられます。本認証基準の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、全てのプロセスについてコントロールしていることを実証する必要があります。

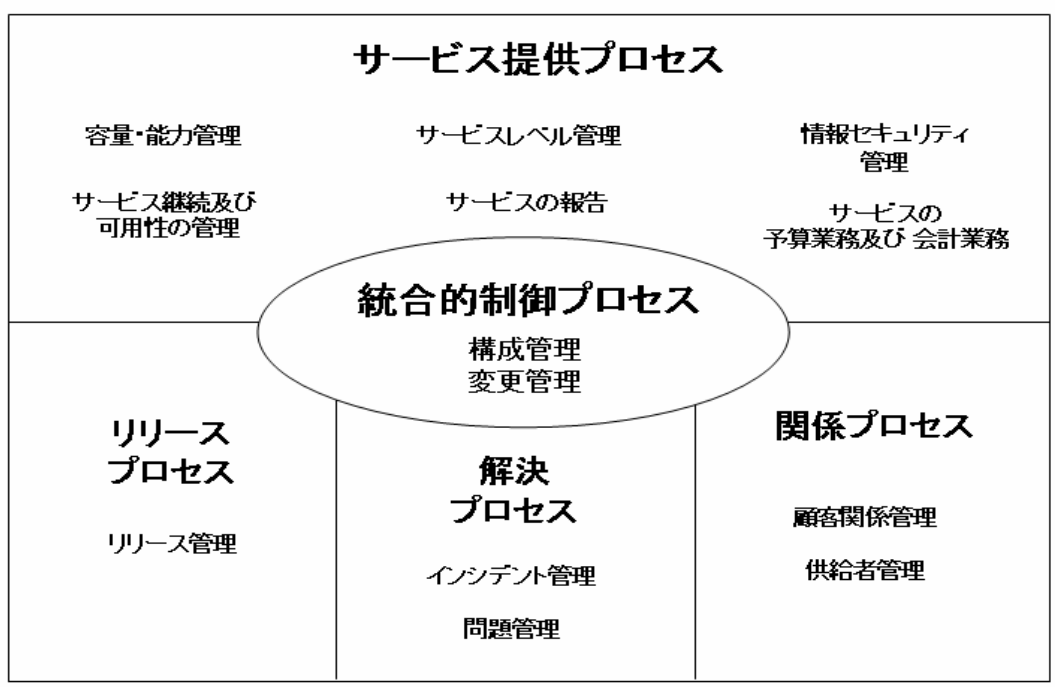


図 1—サービスマネジメントのプロセス

この規格は，図 1 に示すように，互いに密接な関係があるサービスマネジメントの多くのプロセスを規定する。

プロセス間の関係は，組織内での適用によって異なり，モデル化するには複雑すぎるため，図 1 には示していない。

この規格に含まれる目的及び管理策はすべてを網羅してはいないので，組織は，特定の事業上の必要性を満たすために必要であれば，目的及び管理策の追加を考慮してもよい。目的全体を達成するためにこの規格の要求事項をどのように実施するかは，サービス提供者と顧客との関係の性質によって決まる。

この規格は，プロセスについて規定した規格であり，製品アセスメントに用いることは意図していない。しかし，サービスマネジメントのためのツール，製品及びシステムを開発している組織は，最善の慣行（ベストプラクティス）に沿ったサービスマネジメントを支援するツール，製品及びシステムの開発に役立てるために，この規格及び JIS Q 20000-2 を利用してもよい。

（JIS Q 20000-1:2007 1. 適用範囲 より引用）

この規格の理解には、次の理由から ITIL の知識が非常に役立ちます。

- この規格の用語は、ITIL で使われているものと基本的に一致する
  この規格で使われている用語については、2 章に詳説しました。
- この規格が規定するプロセスは、ITIL で説明されるものと基本的に一致する
  図 1 に示され、この規格の 6 章以降に規定されている各プロセスは、ITIL のものと基本的に同じです。本ガイドでは、各プロセスの解説で詳説しました。
- ITIL では、この規格が規定するプロセスの間の関係性について詳しく解説している
  「プロセス間の関係は，組織内での適用によって異なり，モデル化するには複雑すぎるため，図 1 には示していない。」とあります。実際には図 1 だけでなく、この規格の 6 章以降の各プロセスの規定でも、プロセス間の関係性に関する記述は十分なレベ

ルにはありません。この規格と ITIL の基本的内容が同じであることは、この規格に沿ったマネジメントシステムを構築する際には、JIS Q 20000-2 だけではなく ITIL も参考になるということです。またこの規格の認証を取得後、さらなる改善サイクルによってマネジメントシステムに磨きをかける際にも ITIL は非常に有効です。

「この規格に含まれる目的及び管理策はすべてを網羅してはいないので，組織は，特定の事業上の必要性を満たすために必要であれば，目的及び管理策の追加を考慮してもよい。」とあるように、この規格は ITIL に掲載されたプロセスにだけとらわれるのではなく、適宜必要なプロセスを追加することを推奨しています（ただし削除することは求めていない)。

さらに「サービスマネジメントのためのツール，製品及びシステムを開発している組織は，最善の慣行（ベストプラクティス）に沿ったサービスマネジメントを支援するツール，製品及びシステムの開発に役立てるために，この規格及び JIS Q 20000-2 を利用してもよい。」としていて、拡大解釈したこの規格の利用法についても述べています。具体的な利用の方法についての記述はないため、憶測の域をでませんが、以下に例示しました。

- 例 1）製品の開発
  製品を開発する作業を、この規格が想定しているサービスと見立てて、製品開発の際に発生する課題をインシデントとして扱い、これらを処理するプロセスとしてこの規格が規定するプロセス群を活用する。
- 例 2）システムの開発
  システムを構築する作業を、この規格が想定しているサービスと見立てて、システム開発の際に発生する顧客からの要求要件をインシデントとして扱い、これらを処理するプロセスとしてこの規格が規定するプロセス群を活用する。

2. 用語及び定義

IT の世界で使用される用語は、しばしば特殊な意味を持って使われることがあります。この規格で用いられている用語の原典は ITIL にあります。この規格を利用する際は、ITIL の考え方に沿った用語の定義を理解しておく必要があるでしょう。

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。
注記 可用性は，通常，合意したサービス時間中に占める，実際に顧客がサービスを利用できる時間の割合で表される。
（JIS Q 20000-1:2007 2.1 可用性（availability） より引用）

ここで述べるコンポーネントは構成品目(CI: Configuration Item)を示しています。可用性は、信頼性、保守性、サービス性、パフォーマンス、セキュリティといった要素から決定されます。一般的に可用性は%で表され、下記の計算式が使われます。

$$\text{可用性} = \frac{\text{合意されたサービス時間} - \text{ダウンタイム}}{\text{合意されたサービス時間}} \times 100\%$$

2.2 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（2.4 参照）の状態のスナップショット（snapshot）。
（JIS Q 20000-1:2007 2.2 ベースライン（baseline） より引用）

ある時点での構成品目あるいは構成品目を集めたセットを、その状態で凍結して、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。保存されたものがベースラインです。例えば、新しい構成品目を投入するとか、災害復旧などの場合を考えると、構成品目が元の状態から変更されるか、あるいは変更してしまっているということになります。元に戻したければ、変更前の状態を知る必要があります。この変更前の状態を保存しているのがベースラインです。ITIL の中では構成ベースラインという表現も使われています。

2.3 変更記録（change record）
認可された変更によって，どの構成品目（2.4 参照）がどのように影響を受けるかという詳細情報を含む記録。
（JIS Q 20000-1:2007 2.3 変更記録（change record） より引用）

変更記録は認可された変更要求(Request for Change)により生成されます。「変更記録」の“記録”の意味するところは、2.9 記録（record）を参照してください。

2.4　構成品目，CI（configuration item）
　インフラストラクチャのコンポーネント又は品目であって，構成管理の下に置いた又は置く予定のもの。
（JIS Q 20000-1:2007 2.4 構成品目，CI（configuration item）　より引用）

構成品目は他の構成品目と区別できるようにユニークである必要があります。ITIL 書籍では構成項目と訳出されています。構成品目は、構成管理データベース（2.5）で管理されます。構成管理と資産管理の違いについては、2.5 構成管理データベースを参照してください。

2.5　構成管理データベース，CMDB（configuration management database）
　各構成品目に関連するすべての詳細，及びそれら構成品目間の重要な関係の詳細を含むデータベース。
（JIS Q 20000-1:2007 2.5 構成管理データベース，CMDB（configuration management database）　より引用）

IT サービスを提供する為に必要な全ての構成品目を含んでいるデータベースです。構成管理データベースは属性も含みます。構成品目に関するインシデント、問題、変更記録などもリンクされて構成管理データベースに格納されます。構成管理は、資産管理に似た概念ですが、定義にあるように『構成品目間の重要な関係の詳細を含む』という部分に大きな相違があります。資産管理によって管理されている資産と資産の、互いの関係性も含めて管理するのが構成管理です。

2.6　文書（document）
　情報及びそれを保持する媒体。
（JIS Q 20000-1:2007 2.6 文書（document）　より引用）

媒体とは、紙あるいはコンピュータ内のデータを示します。コンピュータ室のレイアウトなども文書に含まれます。規格においては、文書（document）と記録（record）は明確に区別されます。「文書」とは記述されたもの全てを指し、逆に書かれたものは全て「文書」と言えます。2.9 記録（record）を参照してください。

2.7　インシデント（incident）
　サービスの標準的な運用に属さないあらゆる事象であって，サービスの中断若しくはサービス品質の低下を引き起こすもの，又は引き起こす可能性があるもの。
（JIS Q 20000-1:2007 2.7 インシデント（incident）　より引用）

定義の前半では『サービスの標準的な運用に属さないあらゆる事象』と間口を広げていますが、後半では『サービスの中断若しくはサービス品質の低下を引き起こすもの，又は引き起こす可能性があるもの』と限定しています。定義の前後半での差分が、注記にある『問合せを含む場合がある』であると考えてよいでしょう。「問合せ」の扱いについては、ITIL と JIS Q 20000 では温度差があります。ITIL では、インシデントと誤解しやすいもの

にサービス要求(Service Request)があります。例えば、パスワードの再設定、ステータスの問い合わせなどは、ITIL ではインシデントとして扱うのではなくサービス要求として扱っています。JIS Q 20000 の「インシデント」は、サービスの利用及び提供環境全体でみるとランダムに発生する事象全てを指し示す可能性を残した概念であるといえるでしょう。

2.8　問題（problem）
一つ以上のインシデントの未知の根本原因。
（JIS Q 20000-1:2007 2.8 問題（problem）　より引用）

インシデント（2.7）は、サービスの利用及び提供環境全体でみると、利用者及び提供者の意思とは別に発生します。これに対し「問題」は、数あるインシデントの中から、サービスの提供者が“これは「問題」である”と認識するところからスタートします。端的な表現をとれば、「問題」とはコンピュータ・システムの“バグ（不具合)”の存在が認められると判断されたインシデントのことです。根本原因が究明されるか、あるいは回避策（ワークアラウンドと ITIL では呼ばれる。）が見つかった場合に、問題は既知の誤りと呼ばれるようになります。

2.9　記録（record）
達成した結果を記述した，又は実施した活動の証拠を提供する文書。
（JIS Q 20000-1:2007 2.9 記録（record）　より引用）

ITIL ではレコードとして訳出されています。ITIL では、読み取り可能な形式の情報で、コンピュータのデータも含んでいます。規格においては、文書（document）と記録（record）は明確に区別されます。「文書」とは記述されたもの全てであるのに対し「記録」は、例えば題名であるとか、概要や作成日など、文書に付随しうる管理情報を伴ったものを指しています。したがって記録は文書であると言えますが、逆は真ではありません。また、「文書」は書き換えが可能であるのに対し、「記録」の変更は許されません。『記録を，意図の証拠というよりは活動の証拠として扱う』とあるのは、記録が変更不可であることを示しています。

2.10　リリース（release）
新規及び／又は変更された構成品目の集合であって，まとめて試験され，稼働環境へ導入されるもの。
（JIS Q 20000-1:2007 2.10 リリース（release）　より引用）

「構成品目」に着目してリリースを定義すると、このようになります。リリース自体は、そもそも何らかの「変更」を稼働環境に与えようと意図して行われるものですので、ITIL でのリリースの定義は、この定義とは表現を変えて、IT サービスに対する承認された変更の集合となっています。両者に本質的な違いはありません。

2.11　変更要求（request for change）
　サービス又はインフラストラクチャの構成品目を変更する要求の詳細を記録するために用いる，書式又は画面。
（JIS Q 20000-1:2007 2.11 変更要求（request for change）　より引用）

この定義において気をつけなければならないのは、「変更要求」とは『サービス又はインフラストラクチャの構成品目を変更する要求』そのものではなくて、『要求の詳細を記録するために用いる，書式又は画面』としている点です。したがって「変更要求」は具体的には、変更の詳細を記録した“用紙”であったり、変更要求の指示を記した画面の“ハードコピー”であったりします。

2.12　サービスデスク（service desk）
　直接に顧客と接する支援グループであって，支援業務全体の中の多くの割合を担うもの。
（JIS Q 20000-1:2007 2.12 サービスデスク（service desk）　より引用）

サービスデスクは、顧客からのインシデントの受付窓口として機能します。サービスデスクの業務及びその管理も、当然プロセスとして定義されうるのですが、ITIL 及び JIS Q 20000 ではそのようにしていません。プロセスとは、4 章に示されるように、入力を出力に変える処理全体を指しています。そこでインシデントを受け付けるサービスデスクをプロセスで定義してしまうと、そのサービスデスク・プロセスに入力するさらに一つ前のプロセスを想定しなければならず、際限がありません。そこで ITIL 及び JIS Q 20000 では、サービスデスク自体は「機能」として定義し、この機能の結果として得られるインシデントに注目し、以降のプロセスへの入力として扱います。この規格の中にはサービスデスクは含まれていません。それはこの規格が、インシデントを起点としたプロセス群の詳細にのみフォーカスしているためです。

2.13　サービスレベル合意書，SLA（service level agreement）
　書面にしたサービス提供者と顧客との合意であって，サービス及び合意したサービスレベルを記述したもの。
（JIS Q 20000-1:2007 2.13 サービスレベル合意書，SLA（service level agreement）　より引用）

ITIL ではサービス・プロバイダと顧客の間の合意を、サービスレベル合意書（SLA）とし、サービス・組織内の間で顧客に対する IT サービスのサポート及びデリバリに関する合意をオペレーショナルレベル・アグリーメント（Operational Level Agreement：OLA）としています。また、外部サプライヤとの契約は請負契約(Underpinning Contract：UC)とし、明確な区別をしています。しかし、この規格では、“供給者との SLA”という表現が 7 章に見られ、OLA、UC を併せて SLA と記述しているように考えられます。

2.14　サービスマネジメント（service management）
事業上の要求事項を満たすサービスのマネジメント。
（JIS Q 20000-1:2007 2.14 サービスマネジメント（service management）　より引用）

1 章に「この規格は，プロセスについて規定した規格であり」とあるように、この規格及び ITIL ではプロセス主導型アプローチを採用しています。この観点から、サービスマネジメントは､多くの関連するプロセスから形成されるとしています｡この規格においては、「サービス」の明確な定義はありません。したがって「サービスマネジメント」とは『サービスのマネジメント』であるとするこの定義は、心許ないと言わざるを得ないと思われます。本ガイドとして、以下を提案します。

- サービス:顧客に有用な効果をもたらす活動で､人及びシステムによって実現される。
- IT サービス : IT を利用して提供するサービスのこと。IT に対して提供されるサービス（例えばコンピュータ・システムの構築支援サービス)、すなわちサプライヤが提供する IT に関連したサービスは、この規格では「IT サービス」とは呼ばない。
- サービスマネジメント : 提供するサービスを管理すること。サービスがいくつかのプロセスの連携によって提供される場合、個々のプロセスの管理と、総体としての全プロセスの管理、提供されるサービス自体の管理が考えられる。
- IT サービスマネジメント : IT を利用して提供するサービスを管理すること。IT サービスを提供している IT の運用自体ではなく、IT 運用の管理、及びその結果として生まれ顧客に提供される IT サービスを管理することを意味する。そのためこの規格では､「IT サービスマネジメントを構成している個々のプロセス」「IT サービス提供プロセスの全体」「提供される IT サービス自体」が論点として扱われる。

これらの定義案は、2.14 のサービスマネジメントの定義とは矛盾しておらず、本ガイド及びこの規格の理解補助を目的とするものです。

2.15　サービス提供者（service provider）
この規格を満たすことを目指す組織。
（JIS Q 20000-1:2007 2.15 サービス提供者（service provider）　より引用）

2.14 の解説に記した IT サービス及びサービスを、顧客に提供する組織がサービス提供者です。ITIL ではサービス・プロバイダと訳出しています。この規格には、サービスを提供する「サービス提供者」を中心に、サービス提供者からのサービスを直接利用する「ユーザ」、サービス提供者が SLA を締結する相手である「顧客」、サービス提供者にシステムや支援を提供する「サプライヤ」が登場します。1 章に規定されているように、この規格はサービス提供者に向けられたものです。

3. マネジメントシステム要求事項

目的： すべてのサービスを効果的に運営管理し，かつ，実施できるようにするための方針及び枠組みを含むマネジメントシステムを提供するため。 （JIS Q 20000-1:2007　3. マネジメントシステム要求事項 より引用）

本規格の「3. マネジメントシステム要求事項」では、ITSMS を計画、導入、監視、レビュー、及び改善するために重要な要求事項について説明しています。いわゆるマネジメントサイクルである P-D-C-A の具体的な要求事項は、次章の「4. サービスマネジメントの計画立案及び導入」以降で説明することになりますが、ここでは、方針や枠組みを作る上で重要となる「3.1 経営陣の責任」、「3.3　力量, 認識及び教育・訓練」の説明や、各々の活動において基盤となる「3.2　文書化に関する要求事項」について説明します。

3.1. 経営陣の責任

解説

ITSMS の活動のあらゆる段階において、様々な活動が確実に実施されていることについて、経営陣の果たすべき役割は非常に重要です。サービスマネジメントの対象を組織全体ではなく、ある組織階層とし、マネジメントの対象を限定する場合も多いと思われますが、その時でも組織全体としてのマネジメントを意識することが重要です。

経営陣が ITSMS の構築に関与することは、コーポレートガバナンスの視点からも重要です。コーポレートガバナンスとは、株式会社においては経営者による会社の経営責任を株主からの受託責任ととらえ、その遂行責任を問うものです。

コーポレートガバナンスは、「株主による取締役会及びそれを通じた執行者の統治」と、「執行者による企業運営の統治」の 2 つの局面が考えられます。執行者による企業の統治（運営）が行われずして、株主による取締役会及びそれを通じた執行者の統治は意味がありません。従って、まず執行者による企業の統治が重要となります。この統治を行うためにマネジメントが必要となります。

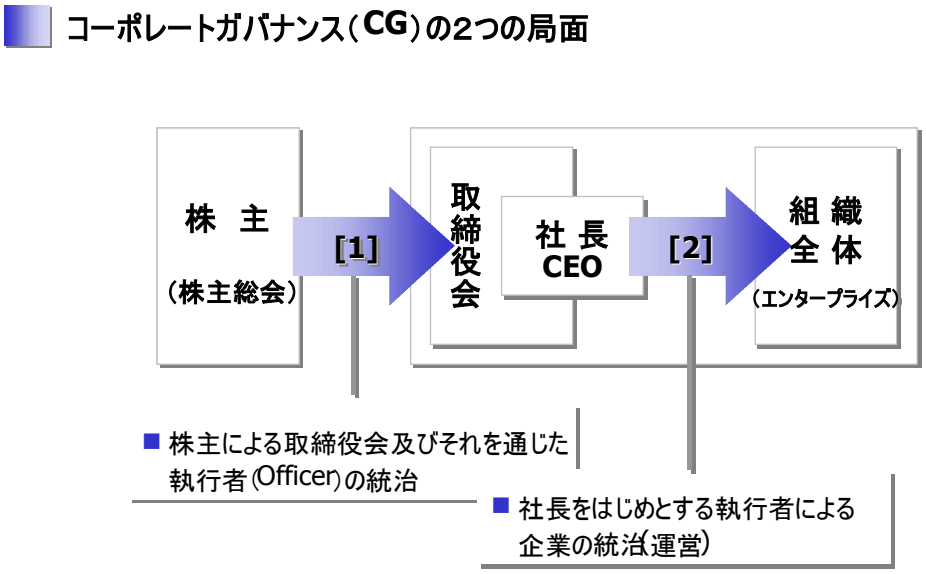


図 3-1　コーポレートガバナンス（ＣＧ）の２つの局面

執行者によるマネジメントの対象は多岐にわたります。マネジメントの対象の１つとして、IT のサービスも考えることができます。その他、品質や環境もマネジメントの対象となります。

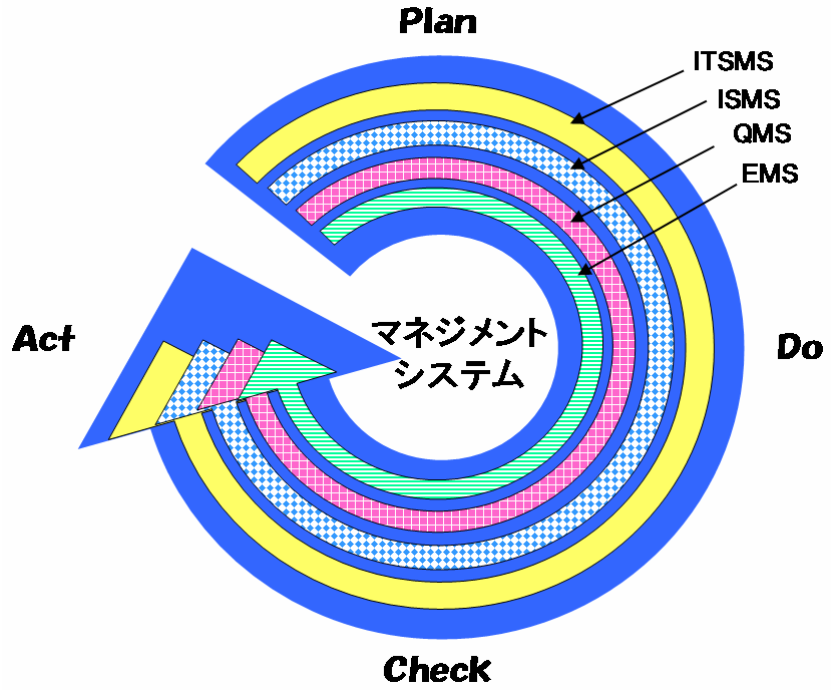


図 3-2　マネジメントシステムの対象

IT サービス、情報セキュリティ、品質、環境のマネジメントプロセスを手順化したものが、それぞれ ITSMS、ISMS、QMS、EMS と言われるものです。これらのマネジメントシ

ステムは事業全体を対象としたマネジメント、とりわけリスクマネジメントの一部として、企業の事業目的達成を側面から支援することになります。このことは組織論的には、事業全体のマネジメントができていないにもかかわらず、その一部にのみ力を入れても高い効果を得られないことを示唆しています。ITSMS は、全体のマネジメントシステムとの関係を考えながら確立していくことが重要です。

また、企業グループ全体を統治することを必要とする組織においては、最近コーポレートガバナンスの観点から、法律上の企業体ではなく、支配力の及ぶ企業グループ全体についての統治、マネジメントの重要性が強調されています。連結経営などはその象徴といえます。ITSMS も企業グループ全体で構築することが、コーポレートガバナンスの観点からは必要となります。

典型的な組織のマネジメントは、図 3-3 のように階層構造を持ち、下位組織階層のマネジメントシステムは上位組織階層のマネジメントシステムと協調して活動します。

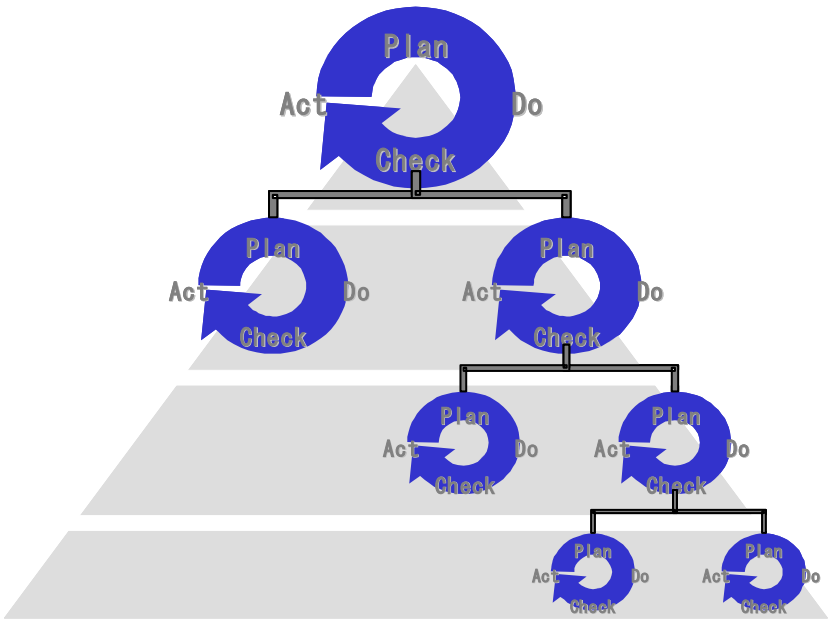


図 3-3　典型的な組織のマネジメントシステム

ITSMS の構築の初期段階においては、適用範囲を限定し、特に効果の高い領域への対策を優先することに注力することもあります。しかし、経営陣はその場合においても前述のマネジメントシステム間の連携を認識し、最終的に想定したゴールに導く責任を負います。

経営陣の果たすべき重要な役割のひとつにコミットメントがあります。ITSMS の確立、

導入、運用及び維持等にリーダシップを発揮し、組織としてIT サービスマネジメントの実施責任を利害関係者に宣言する「コミットメント」は、執行権限を有する経営陣にのみ実施する事が許されるからです。

本規格では、経営陣の責任を次のように規定しています。

> 経営陣は，サービスマネジメントの能力を事業上の要求事項及び顧客要求事項との関連において開発，実装及び改善することへのコミットメントの証拠を，リーダシップ及び活動を通じて示さなければならない。
>
> 経営陣は，次を実施しなければならない。
>
> a) サービスマネジメントの方針，目的及び計画を確立する。
>
> b) サービスマネジメントの目的を達成することの重要性，及び継続的改善の必要性を周知する。
>
> c) 顧客要求事項を決定することを確実にし，その決定が顧客満足の改善という目的に沿っていることを確実にする。
>
> d) すべてのサービスの調整及びマネジメントに責任をもつ者を，経営陣の中から一人指名する。
>
> e) サービスの提供及び運営管理を計画，導入，監視，レビュー及び改善するための資源を決定し，例えば，適切な要員の採用・異動の管理によって，これを提供する。
>
> f) サービスマネジメントの組織に対するリスク及びサービスに対するリスクを管理する。
>
> g) サービスマネジメントが引き続き適切であり，妥当であり，かつ，有効であることを確実にするために，あらかじめ定めた間隔でサービスマネジメントをレビューする。
>
> （JIS Q 20000-1 3.1 経営陣の責任　より引用）

経営陣は、ITSMS の計画、導入、監視、レビュー、及び改善等に最終的な責任を負います。しかし、経営陣は組織のマネジメントシステムに責任を持ちますが、全ての活動に関与することは不可能です。

そこで、経営陣はまずサービスマネジメントの方向性を示す方針を確立します。

次に、サービスマネジメントの目的を設定し、ITSMS の実践のための計画が策定されることを明確に指示し、確実に実施されることに責任を負います。

また、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、サービスの調整上の役割及び責任を持つ者を経営陣の中から定め、サービスの提供及び、運用管理を計画、導入、監視、レビュー及び改善等に十分な経営資源を提供しなければなりません。最終的に経営陣は、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自身が内部監査等を通じて把握し、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が重要となります。

3.2. 文書化に関する要求事項

解説

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。文書の管理について、以下の点を盛り込んだ管理手順を確立し、文書管理する必要があります。JIS Q 20000-1 では、文書管理について、特に明確な要求事項が記載されていないため、その他のマネジメントシステム（JIS Q 27001:2006、JIS Q 9001:2004 など）で要求されている仕様を参照すると良いと思われます。ここでは、JIS Q 27001:2006 の文書管理の要求事項について、記載しておきます。

> ISMSが要求する文書は，保護し，管理しなければならない。次の事項を行うのに必要な管理活動を定義するために，文書化した手順を確立しなければならない。
> a）適切かどうかの観点から，文書を発行前に承認する。
> b）文書をレビューする。また，必要に応じて更新し，再承認する。
> c）文書の改変を特定すること及び現在の改版状況を特定することを確実にする。
> d）使用する必要があるとき，適用する文書の関連する版が使用可能であることを確実にする。
> e）文書は読みやすく，かつ，容易に識別可能であることを確実にする。
> f）文書を，それを必要とする者には利用可能にすることを確実にする。また，文書を，その分類区分に適用される手順に従って受け渡すこと，保管すること，及び最終的には処分することを確実にする。
> g）外部で作成された文書であることの識別を確実にする。
> h）文書配付の管理を確実にする。
> i）廃止文書の誤使用を防止する。
> j）廃止文書を何らかの目的で保持する場合には，適切な識別を施す。
>
> （JIS Q 27001:2006　4.3.2 文書管理　より引用）

また、記録は、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、管理します。

ITSMS では、文書及び記録に関して、以下のものを作成することを要求しています。

文書化したサービスマネジメントの方針及び計画	方針書及び計画書
文書化した SLA	サービス文書
この規格が要求する，文書化したプロセス及び手順	手順書，プロセス記述書
この規格が要求する記録	プロセス制御記録

（JIS Q 20000-1:2007　上記各項　より引用）

記録の管理として、以下の事項の実施などが効果的です。

- 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文書化すること
- 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

3.3. 力量，認識及び教育・訓練

経営陣の重要な役割の一つとして、「人」、「物」、「金」といった経営資源の提供があります。経営陣は、サービスマネジメントの必要性を理解し、そのために必要な経営資源の提供を行わなければなりません。経営陣の掛け声だけでは、サービスマネジメントの計画、導入、運用及び管理等は難しいと思われます。サービスマネジメントの構築に必要な一連のプロセスには、経営資源の割り当てが必要となります。

経営資源の中でも「人」の問題は特に重要です。
本規格では、「人」に関連する力量、認識及び教育・訓練を次の 3 つの事項を挙げて説明しています。

> サービスマネジメントのためのすべての役割及び責任は，それらを効果的に果たすために必要な力量と合わせて定義し，かつ，維持しなければならない。
> 要員の力量及び教育・訓練の必要性を，要員が自らの役割を効果的に果たすことを可能にするために，レビューし，かつ，管理しなければならない。
> 経営陣は，従業員が自らの活動のもつ意味及び重要性を認識し，サービスマネジメントの目的の達成に向けて自分はどのように貢献できるかを認識することを，確実にしなければならない。
>
> （JIS Q 20000-1:2007 3.3 力量，認識及び教育・訓練　より引用）

ITSMS の計画、導入、運用及び管理等を行っているのは、人であるということを忘れてはなりません。組織の各個人が ITSMS に関連する責任を果たし、期待される役割を実行するためには、本人の力量が伴わなければならないことは明らかです。

経営陣には、明確にされた役割を割り当てられた要員すべてが、要求される職務を実施する力量を持つことを確実にするために、教育・訓練を実施させる責任があります。また、実施する教育・訓練の内容は、全ての要員が自らのサービスマネジメントについての活動の意味とその重要性を認識し、サービスマネジメントの目的の達成に向けてどのように貢献できるかを認識できるようなものが理想です。

実施した教育・訓練については、その有効性を評価し、力量を持った要員の確保に役立てることが重要です。必要とされる力量は、それぞれの業務により異なることになります。

ITSMS の計画、導入、運用及び維持等のために必要となる力量としては、表 3-1 のような分野が考えられます。

表 3-1　力量の分野

マネジメントに関連する力量	マネジメント論全般、リーダシップなど
監査に関連する力量	監査理論全般、監査の実務
IT 技術に関連する力量	運用に関する実務経験、トラブルシューティング能力、ネットワーク、アプリケーション、OS、プログラム、開発等に関する知識
セキュリティ技術に関連する力量	ネットワークセキュリティ、サーバアプリケーションセキュリティ、OS セキュリティ、ファイアウォール、侵入検知システム、ウィルス、セキュアプログラミング、暗号等に関する理論や実践

これらの力量を適切に定義し、その達成度を確認することが重要となります。

また、この力量の有無を検討する一つの目安として、資格制度を利用することも有益と思われます。それぞれの力量と関連する資格の例としては表 3-2 のような資格、試験合格者が考えられます。

表 3-2　力量と関連する資格

内部監査	公認内部監査人(CIA)[1]、公認会計士、公認システム監査人[2]、システム監査技術者[3]、公認情報システム監査人(CISA)[4]、ITSMS 主任審査員、ITSMS 審査員、ISMS 主任審査員、ISMS 審査員、公認情報セキュリティ監査人（CAIS）[5]
IT マネジメント	プロジェクトマネージャー[3]、PMP（Project Management Professional）[6]、 IT コーディネータ[7]、ITIL マネージャ資格[8]
IT 技術	テクニカルエンジニア（ネットワーク、データベース、システム管理）[3]、ITIL ファンデーション資格[8]
セキュリティ技術	情報セキュリティアドミニストレータ、上級システムアドミニストレータ、テクニカルエンジニア（情報セキュリティ）[9]、公認情報セキュリティ管理者(CISM)[10]、公認情報システムセキュリティ専門家(CISSP)、公認システムセキュリティ熟練者(SSCP)[11]

また、情報セキュリティについての業務毎に必要とされる力量を決定する際に、情報処理推進機構（IPA）が発表しているセキュリティスキル標準についての報告書などを参考にされるとよいと思われます。[12]

---

[1] 公認内部監査人（Certified internal Auditor）は内部監査人協会（The Institute of Internal Auditors,Inc.(IIA)　http://www.theiia.org）が認定する内部監査人の資格。内部監査人協会は 1941 年に米国で設立され、2006 年現在、全世界で約 122,000 名が内部監査人協会に所属している。

[2] 公認システム監査人は特定非営利活動法人日本システム監査人協会（http://www.saaj.or.jp）が認定するシステム監査人の資格。

[3]独立行政法人情報処理推進機構により行われている、システム監査技術、プロジェクトマネージャー、テクニカルエンジニア（ネットワーク、データベース、システム管理）の技術を有していることを認定するための国家試験。

[4] 公認情報システム監査人は、ISACA（Information Systems Audit and Control Association 情報システムコントロール協会 http://www.isaca.org）により認定されるシステム監査人の資格。情報システムコントロール協会は 1967 年に米国で設立され、2006 年現在、全世界で約 50,000 名が ISACA に所属している。

[5] 公認情報セキュリティ監査人は、特定非営利活動法人日本セキュリティ監査協会により認定される情報セキュリティ監査人の資格。

[6] PMP は、米国 PMI（Project Management Institute）により認定されるプロジェクトマネジメントに関する資格。

[7] IT コーディネータは、特定非営利活動法人 IT コーディネータ協会により認定される IT のコーディネートに関する資格。

[8] ITIL マネージャ、ITIL ファンデーションは、itSMF（特定非営利活動法人 IT サービスマネジメントフォーラム）　及び英国政府 OGC (Office of Government Commerce)により認定される ITIL (IT Infrastructure Library)に関する資格。

[9]情報セキュリティアドミニストレータ、上級システムアドミニストレータ、テクニカルエンジニア（情報セキュリティ）は独立行政法人情報処理推進機構により行われている、情報セキュリティ管理、システム管理、情報セキュリティについての一定の専門的知識・能力を有していることを検定するための国家試験。

[10] 公認情報セキュリティ管理者（Certified information security manager）は、情報システムコントロール協会（Information Systems Audit and Control Association　http://www.isaca.org）により認定されるセキュリティ管理者としての専門的能力を有していることを証明する資格。

[11] 公認情報システムセキュリティ専門家（Certified information system security professional）、公認システムセキュリティ熟練者（System security certified practitioner）は(ISC)[2]（International Information Systems Security Certification Consortium　http://www.isc2.org）により認定される情報セキュリティについての専門的能力を有していることを保証する資格。

[12] http://www.ipa.go.jp/security/fy14/reports/professional/sec-pro-outline.pdf

4. サービスマネジメントの計画立案及び導入

図 2 に示すモデルは，この規格の箇条 4～10 に規定するプロセス及びプロセス間のつながりを表したものである。

注記　“計画(Plan)－実行(Do)－点検(Check)－処置(Act)”（以下，PDCA という。）として知られる方法論は，あらゆるプロセスに適用できる。PDCA を説明すると次のようになる。

a) 計画（Plan）：顧客要求事項及び組織の方針に沿った結果を出すために，目的及びプロセスを確立する。
b) 実行（Do）：それらのプロセスを実施する。
c) 点検（Check）：方針，目的及び要求事項に照らしてプロセス及びサービスを監視し，測定し，かつ,その結果を報告する。
d) 処置（Act）：プロセスのパフォーマンスを継続的に改善するための処置をとる。

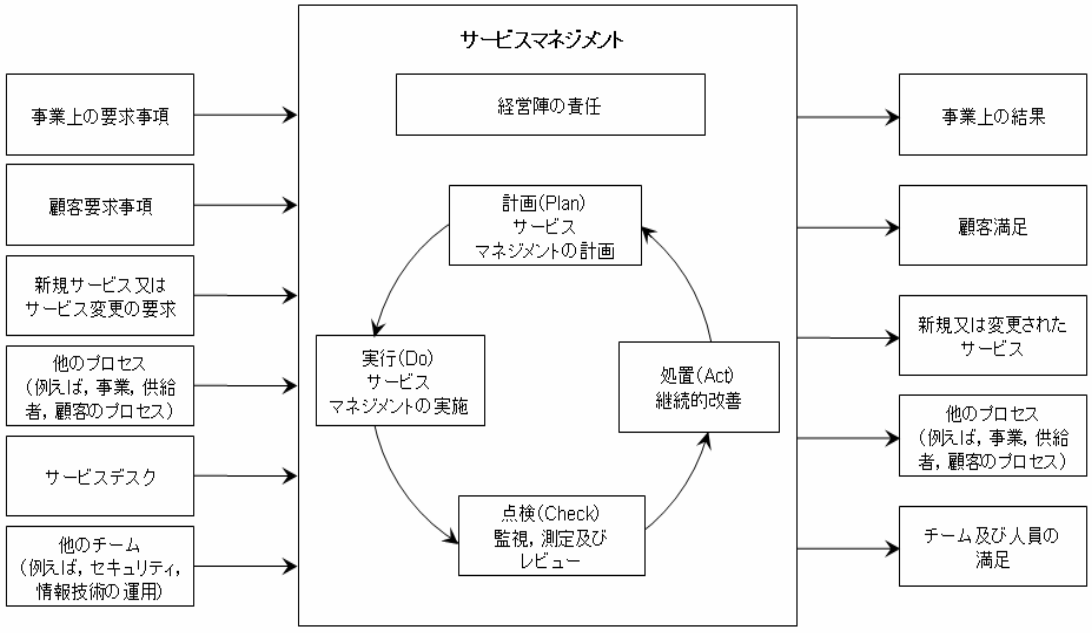


図 2－サービスマネジメントのプロセスのための PDCA 方法論

（JIS Q 20000-1:2007　4 サービスマネジメントの計画立案及び導入 より引用）

解説

JIS Q 20000-1 はサービスを実現するアプローチに、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。プロセスとは、入力された情報を出力に変える活動であり、図 2 に示されている左側が入力、右側が出力、そして中央が JIS Q 20000-1 によってマネジメントされたプロセスを表しています。

左側の入力は、すべてサービスマネジメントへの要求事項であり、事業上の要求や顧客の要求、サプライヤからの要求などが含まれます。その中には新たなサービスの実現を期待する要望や現状のサービスをより良いものに改善するための提案もあります。また、要求は、社会的な或いは事業上の必要性から求められるものや、顧客、サプライヤ、更には、

サービスデスクを通じて得られるエンドユーザからのフィードバックもあります。

それらの入力を組織のサービスマネジメントプロセスを通じて出力、すなわち良質なサービスの提供につなげることを示しています。組織はより良いサービスを実現すべく本規格の 3 章を考慮した上で 5 章から 10 章までの各プロセスを体系化し、実施、監視、改善に結びつけるために 4 章の PDCA サイクルを確立することが求められています。詳細は 4.1 項から 4.4 項に記載されています。

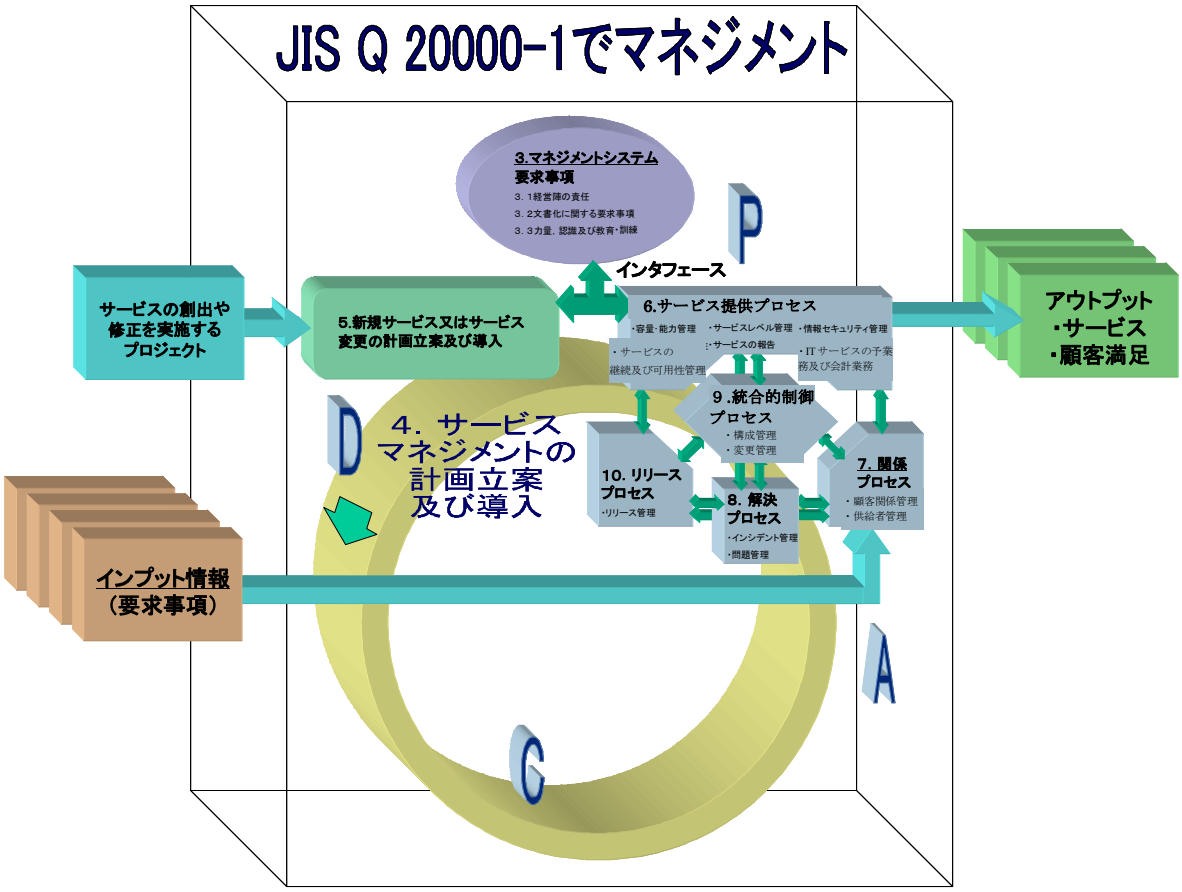


図 4-1　JIS Q 20000-1 でマネジメントするプロセス体系

適用範囲の項でも述べている通り、この規格の 4 章から 10 章までの各プロセスは、必ずしも組織が必要とする管理の目的や管理策をすべて網羅している訳ではありません。JIS Q 20000-2 や ITIL などを参考にし、具体的な管理手法を取り入れることも出来ます。ただし、気をつけなければならないことは、組織のサービスに影響を及ぼすリスクの大きさ以上に管理策を採用してしまうことです。組織の文化や教育の浸透度、管理にかかる費用などについても考慮し、組織にあった ITSMS を構築することが重要です。

4.1. サービスマネジメントの計画（Plan）

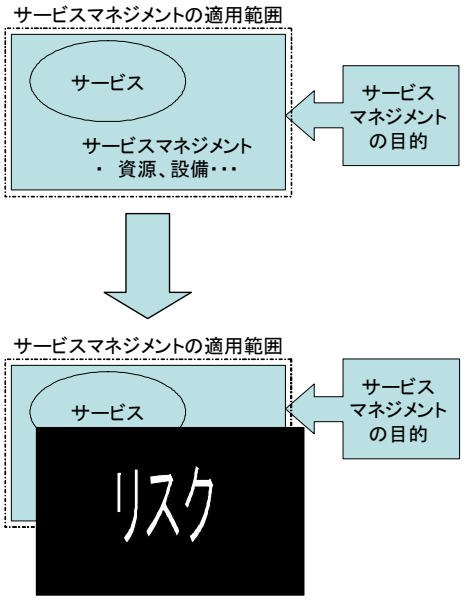
本項ではサービスマネジメントの計画（Plan）に相当する ITSMS の要求事項として、サービスマネジメントのプロセスの骨格を作るために、どのようなプロセスの構造が必要であるかを検討し計画を立てることについて記載されています。

目的： サービスマネジメントの導入・実施について計画するため。 （JIS Q 20000-1:2007　4.1 サービスマネジメントの計画（Plan）　より引用）

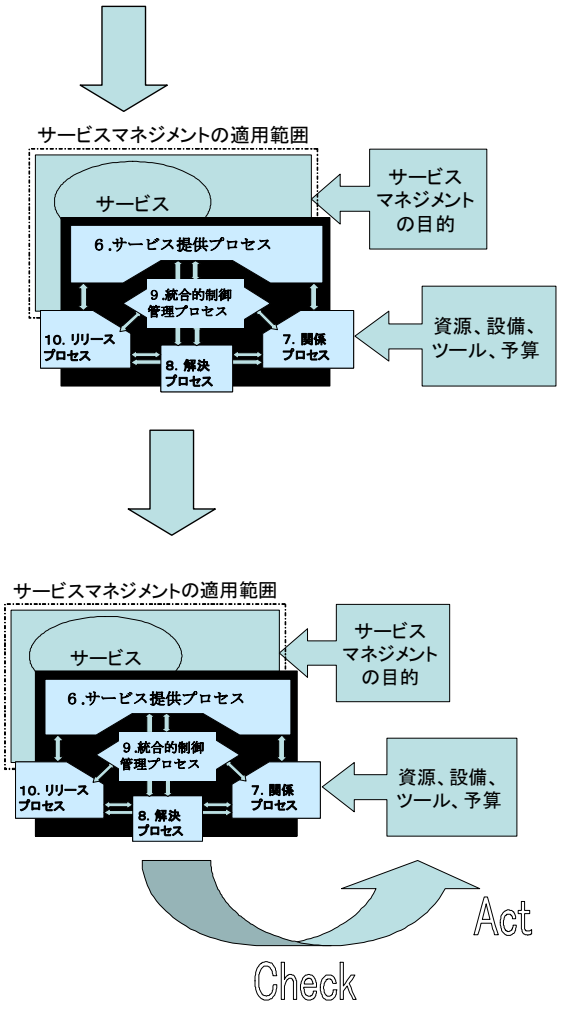
解説

サービスマネジメントを計画する上で、まず考えなければならないのは適用範囲とサービスマネジメントによって達成すべき目的です。適用範囲を適切に保つことは、サービスマネジメントが意味のある活動になるか否かを決定付けるものです。サービスマネジメントの適用範囲は、管理可能な範囲でなければなりません。どのサービスに適用し、そのサービスを実施する場所・建物、組織または組織関係、インフラストラクチャ、サービスレベルを実現するために必要なプロセスについて、サービスへの影響を直接的にまたは間接的に管理可能な範囲を定めなければなりません。

その範囲の中で求められる管理のレベルは、サービスマネジメントの目的を達成するために十分なものでなければなりません。「3.1 経営陣の責任」の記述にもあるように、サービスマネジメントのプロセスを確立する上で、組織に対するリスクやサービスに対するリスクを管理することが求められています。組織は、リスクを特定し、アセスメントによって目的の達成に及ぼす影響の大きさを評価し、それを受け入れ可能なレベルまで低減すべく、必要な資源、設備、予算を投入し、各プロセスが、確実に実施できる環境を与えることが重要です。その過程を図 4-2 に示します。



- サービスマネジメントの適用範囲及び目的を定める
- 目的の達成に対する課題やリスクの特定及びその影響をアセスメントする方法や管理する手段の定義



- サービスマネジメントの中で実行すべきプロセス及びプロセス間のインタフェース、及び各プロセスの活動の調整方法
- サービスマネジメントに対する役割、責任
- 目的を達成するために必要な資源、設備、予算
- プロセスを支援するための適切なツール
- サービス品質を管理、監査及び改善する方法

図 4-2　サービスマネジメントの導入・実施計画

サービスマネジメントの中で実行すべきプロセスは、本規格の 4 章から 10 章のプロセスに示され、サービスを実現するために必要な基本的なプロセスとして採用することになるでしょう。各プロセスは、オーナーを定め、管理の責任を定めることが求められています。組織は採用したプロセス同士の繋がりや、そこで取り交わされる情報及び処理についても考慮に入れ、一連の流れを体系化することが重要です。プロセス同士のつながりを理解するために、例えば、サービスが追加・変更された場合を考えて見ましょう。追加・変更要求は顧客から契約担当部署を通じて 7 章の「関係プロセス」にインプットされます。サービス運用担当部署は変更が及ぼす影響をアセスメントし、5 章の「新規サービス又はサービス変更の計画立案及び導入」を用いて、費用や人員、サービスの導入時期を検討し、SLA や、報告の内容の追加・変更、情報セキュリティに対する新たな管理策の採用、人員増減に伴う予算配分の変更など、6 章の「サービス提供プロセス」全体について見直す必要があります。また、CMDB の修正は、9 章の「統合的制御プロセス」、実環境に投入する際は 10 章の「リリースプロセス」が適用されサービスの運用がスタートします。さらに、

計画されたプロセスが、上手く動いていることを内部監査やマネジメントレビューで見直し、サービスやサービスマネジメントの改善につなげることも忘れてはなりません。サービスの追加・変更以外にも、インシデントの対応など、各場面でプロセス同士が複雑に関係しあうことを知ることが大切です。そのインタフェースは、会議などのコミュニケーションの場であったり、指示書や記録の回覧であったりさまざまです。

また、インタフェースについては、サービスの創出や修正を実施するプロジェクトについても取り上げています（図 4-1 参照)。例えば、開発部門とのインタフェースであれば、ソフトウェアの大規模な改修や、新規のシステムを構築するにあたっての仕様の決定やレビュー、実環境への投入プロセスなど、開発部門とサービス提供部門との間でコミュニケーションを密にとり、相互に情報交換を成すインタフェースを確立することが考えられます。サービスの運用に影響するハードウェア、ソフトウェアの質が高いことは、運用にかかるコストや可用性、サービス継続性にも影響するため、良質なサービスを実現する上で不可欠です。しかしながら、開発プロジェクトのマネジメントについては JIS Q 20000-1 のサービスマネジメントプロセスに含まれていないため、開発プロジェクトのマネジメントについては ISO 9001 や CMM、CMMI を活用することが有効です。サービスの創出や修正を行う上で、確立されたインタフェースを活用し、関わりの深いプロジェクトやプロセスに対し要求を出したり、フォローアップをすることで稼働環境への移行をスムーズに行うことができます。

また本項では、サービス品質を管理、監査及び改善する方法についても定義することが求められています。サービスマネジメントのプロセスの計画に盛り込むものとして、4.2、4.3、4.4 の項目に記述されている実行(Do)－点検(Check)－処置(Act)のプロセスを参照ください。

要求事項

・サービスマネジメントの計画を立案する。

・計画には以下を含める。

a) サービス提供者のサービスマネジメントの適用範囲及びサービスマネジメントによって達成すべき目的及び要求事項

b) 実行すべきサービスマネジメントプロセス及びプロセス間のインタフェースと各プロセスの活動の調整方法

c) 上位の管理責任者、プロセスの管理責任者及び供給者の管理者を含む、管理者層の役割及び責任についての枠組み

d) 定義した目的の達成に対する課題及びリスクの特定、アセスメント及び管理のためにとるべき取組み

e) サービスを創出・修正する複数のプロジェクトにインタフェースをとるための取組み

f) 定義した目的を達成するために必要な資源、設備及び予算

g) プロセスを支援するための適切なツール

h) サービス品質を管理、監査及び改善する方法

留意事項

- サービスマネジメントの適用範囲は、マネジメントの管理可能な範囲を的確に捉えていることが重要です。サービスレベルを実現するために必要なプロセスを考慮し、サービスへの影響を直接または間接的に管理可能な組織範囲、インフラストラクチャ、プロセスなどを決定することをお勧めします。
- サービスマネジメントによって達成すべき目的は、サービスに対するリスクを如何に反映するかが重要です。
- 適用範囲以外の部門、プロジェクトとのインタフェースは、取り扱う問題の影響の大きさや緊急度に適した管理を実現することが重要です。

4.2. サービスマネジメントの実施及びサービスの提供（Do）

本項ではサービスマネジメントの実施（Do）に相当する ITSMS の要求事項として、4.1 で定めたサービスマネジメントの計画を実施に移し、管理状態にあるサービスを確実に提供するためのキーとなるポイントが記載されています。

目的： サービスマネジメントの目的及び計画を実施するため。 （JIS Q 20000-1:2007　4.2 サービスマネジメントの実施及びサービスの提供（Do） より引用）

解説

本項では、4.1 で定めたサービスマネジメントの計画を実施に移す以上のことを要求しているものではありませんが、実施の際に注意すべき基本事項として以下のことが強調されています。

4.1 で計画された通り、リスクを評価し、そのリスクに見合った対応を計画し、計画を現実のものにするために、資金の調達、設備の導入、予算の割り当てなどを確実に実施し、計画が絵に書いた餅にならないよう注意が喚起されています。サービスマネジメントに掛かる費用を把握し、必要な資金を調達することは、最も基本的なことであることは言うまでもありませんが、万が一にも、これが管理されない状況に陥れば、人の採用が滞り、人的資源の不足を招くことになります。悪影響は設備の導入や保守などにも及び、あらゆる管理に影響を与えます。

その他にも、方針の決定や、手順の維持、役割及び責任の割当て、文書化は、人の育成、運用チームの管理についても記載されています。実施に際しては、「3.1 経営陣の責任」や「3.2 文書化に関する要求事項」、「3.3 力量，認識及び教育・訓練」を参照下さい。

計画に対する進捗状況の確認も忘れてはなりません。また、サービスマネジメント実施結果を 4.3 項の点検(Check)－4.4 項の処置(Act)の中で活用することも重要です。

要求事項

・サービス提供者は、サービスを運営管理して提供するために、サービスマネジメントの計画を実施する。

留意事項

・ 健全なサービスマネジメントを実現するためには、適切な資金と予算の割り当て、資源の配分、管理が重要です。
・ また、サービスマネジメントの実施やサービスの提供については、継続維持が重要です。

4.3. 監視，測定及びレビュー（Check）

本項目ではサービスマネジメントの監視、測定及びレビュー（Check）に相当する ITSMS の要求事項として、サービスマネジメントの目的及び計画の達成を、監視、測定及びレビューする方法について記載されています。

目的： サービスマネジメントの目的及び計画の達成を，監視，測定及びレビューするため。 （JIS Q 20000-1:2007　4.3 監視，測定及びレビュー（Check）　より引用）

解説

サービスマネジメントの目的及び計画の達成を、監視、測定及びレビューする方法として、他のマネジメントシステムでも用いられているマネジメントレビューと内部監査について記載されています。マネジメントレビューではサービスマネジメントが計画に沿い、JIS Q 20000-1の要求事項に適合していることや、有効に実施され維持されているかどうかをあらかじめ定めた間隔で見直すことが求められています。サービスマネジメントが有効に機能していることを見極めることは非常に難しいことですが、いくつかの指標は相関関係にあるものとして監視することができ、次の4.4の中で改善が意図されている対象の監視についても考慮されるとよいでしょう。

4.4 d） 品質、費用及び資源利用の改善目標を設定する。

4.4 e） すべてのサービスマネジメントのプロセスからの改善に関する入力を検討する。

サービスの品質にかかわる情報は「6.2 サービスの報告」、「8.2 インシデント管理」、「8.3 問題管理」などが情報源であり、サービスにかかわる費用の情報は、「6.4 サービスの予算業務及び会計業務」、資源の状況は、「6.5 容量・能力管理」プロセスの情報が活用できるでしょう。さらに、4.4 e）に記載しているように、すべてのサービスマネジメントのプロセスからの改善に関する情報を監視の対象と考えれば、サービスに関わるありとあらゆる情報が考慮可能な対象と考えることができます。これらの情報は、例えば次のようなマネジメントレビューの入力情報に含まれ、レビューの結果は、4.4の継続的改善につながります。

✧ サービスレビューや中間会議の結果
✧ 利害関係者からのフィードバック
✧ サービス苦情
✧ サプライヤのパフォーマンスレビューの結果
✧ インシデント情報
✧ サービスマネジメントやサービスに関わるリスク情報
✧ サービスマネジメントやサービスに影響する可能性のある変更及び改善のための提案
✧ 内部監査の結果
✧ 予防処置、是正処置の状況
✧ 過去のマネジメントレビューの結果に対するフォローアップ

内部監査については以下の要求があります。

✧ 監査プログラムの計画
✧ 監査の基準、範囲、頻度及び方法を定義手順の確立
✧ 監査プロセスの客観性及び公平性
  - 監査員は自らの仕事を監査してはならない

マネジメントレビューや内部監査の記録は作成し維持管理の対象として管理されることが求められています。

要求事項

- サービス提供者は、サービスマネジメントのプロセスを監視及び測定し、プロセスが計画した結果を達成する能力があることを明示する。
- 経営陣は、サービスマネジメントの要求事項が、サービスマネジメントの計画に沿っており、この規格の要求事項に適合し且つ有効に実施されているかどうかを判断するために、あらかじめ定めた間隔でレビューを実施する。
- 監査の対象となるプロセス及び領域の状況及び重要性、並びにこれまでの監査結果を考慮して、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、手順の中で定義する。
- 監査員の選定及び監査の実施は、監査プロセスの客観性及び公平性を確実にする。

留意事項

- 「4.3. 監視，測定及びレビュー(Check)」のプロセスは、そのアウトプットの質と量が次の「4.4 継続的改善(Act)」の効果を左右します。
- マネジメントレビューのインプット情報については取り立てて記載はないが、すべてのサービスマネジメントのプロセスからの改善に関する情報を活用することが意図されています。
- 内部監査については、自らの仕事を監査しない程度の客観性が求められています。

4.4. 継続的改善（Act）

本項ではサービスマネジメントの継続的改善（Act）に相当する ITSMS の要求事項として、サービスの提供及び運営管理の有効性及び効率を改善するためのキーとなるポイントが記載されています。

目的： サービスの提供及び運営管理の有効性及び効率を改善するため。 （JIS Q 20000-1:2007　4.4 継続的改善（Act）より引用）

解説

サービスの提供及び運営管理の有効性及び効率を改善する目的を達成するために方針を掲げ、公開することが求められています。参考までに JIS Q 20000-2 では、継続的改善について方針を作成し公開することによって、サービスマネジメントに関わるサービス提供者の全スタッフが、サービスマネジメントプロセスに対して継続的改善がもつ意味を詳細に理解することを推奨しています。ここでいう公開される範囲とは、その方針を知る必要性に見合った範囲であり、サービスマネジメントに関わりを持つ方が対象と考えてよいでしょう。

サービスの改善については提案された変更要求に対しアセスメントを実施することが求められています。アセスメントについては、「9.2 変更管理」の中でもリスク、影響及び事業利益について評価することが求められています。サービスの改善はアセスメントの結果を考慮し、優先順位に応じた実施を計画することが重要です。

サービス改善のための計画の実施に先立って、サービス品質及びサービスレベルのベースラインを記録し、改善を実施する前と後とを比較し評価することは、改善の効果を知る上で重要です。また、改善の効果は、品質面、費用面、資源の活用について予測され、目標として設定することが求められています。改善は、必要に応じてサービスマネジメントの方針、プロセス、手順及び計画を改訂し、その結果は、上記で設定された目標（品質面、費用面、資源の活用）と比較され、サービスの提供及び運営管理の有効性及び効率が実際に改善された程度を測定し、関係者へ報告・周知することが求められています。

要求事項

・サービス改善について、公開した方針を備え、この規格又はサービスマネジメントの計画を順守していない場合には、修正を行う。

・すべての提案されたサービス改善についてアセスメントを行い、記録し、優先順位を決め、認可する。

・サービス提供者は、改善活動を継続的に特定、測定、報告及び管理するためのプロセスとして以下を実行する。

a) サービス提供者の能力のベースラインを決めて比較評価をするために、データを収集・分析する。
b) 改善策を特定し、計画立案の上、実施する。
c) 関係者全員と協議する。
d) 品質、費用及び資源利用の改善目標を設定する。
e) すべてのサービスマネジメントのプロセスからの改善に関する入力を検討する。
f) サービス改善を、測定、報告及び周知する。
g) 必要な場合は、サービスマネジメントの方針、プロセス、手順及び計画を改訂する。
h) 承認した処置すべてが実行され、その活動が意図した目的を達成することを確実にする。

留意事項

・ サービスマネジメントを計画(4.1)し、実施(4.2)し、目的及び計画の達成を、監視、測定及びレビュー(4.3)した結果を、サービスの有効性及び効率を改善することが目的とされています。
・ サービス改善について、公開した方針を備えなければなりません。
・ サービス改善のための計画を作成しなければなりません。
・ サービス品質及びサービスレベルのベースラインは改善の実施に先立って記録されなければなりません。
・ 改善の効果は、品質面、費用面、資源の活用について、目標を設定しなければなりません。
・ その結果は、測定され、関係者へ報告・周知することが求められています。

5. 新規サービス又はサービス変更の計画立案及び導入

ITSMS における変更（新規追加も含みます）は、大きく２つに分類することができます。１つは「9.2　変更管理」プロセスが主体となって取り扱う変更、そしてもう１つは、「5 新規サービス又はサービス変更の計画立案及び導入」に基づき取り扱われる変更です。この両変更の対象をそれぞれ明確に定義し区別することが、「5　新規サービス又はサービス変更の計画立案及び導入」プロセス構築の最初のステップとなります。

それぞれの変更対象の定義は、費用・組織・技術・営業面など、顧客やサービス提供組織への影響を考慮して定義することが重要です。

本章の対象となる変更が生じた場合には、新規サービス及びサービスの変更が、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という目的を達成するために、計画を立案し、その計画に従い導入にあたることになります。

計画実施前の承認及び計画実施後の評価活動である導入後レビューは、「9.2 変更管理」での定義に従い遂行することになります。

目的：新規サービス及びサービス変更が，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。 （JIS Q 20000-1 5. 新規サービス又はサービス変更の計画立案及び導入　より引用）

解説

本章の目的（狙い）は、以下の 2 点を実現することにあると言えます。

- 組織が新規にサービスを立ち上げる場合や既存のサービスを変更する場合に、正当な導入計画を立案すること。
- 新規サービスの立ち上げやサービスの変更が、導入計画通りのコストで運営され、かつ導入の結果、期待通りのサービス品質を得ること。

前述の「正当な導入計画」とは、サービス立ち上げや変更に必要なコストや人的資源、サービス提供組織の事業上の要求事項（ビジネス要求）、各プロセスからの改善提案、顧客の要求事項、技術革新、市場の動向など様々なインプット情報を考慮した結果から得られる導入計画を指しており、組織にとって正しい根拠の下に導入計画を立案することを促しています。

また、立案された導入計画が正しい根拠か否かについて、ビジネスインパクトを考慮の上で判断し、その導入計画をコントロールする事でコストとサービス品質の両側面で計画通り、あるいはそれ以上の効果を得る事を目指しています。すなわち本規格では QCD（クオリティ／コスト／デリバリ）のバランスを担保しつつ新規サービス又はサービス変更の計画立案及び導入を遂行することが求められています。

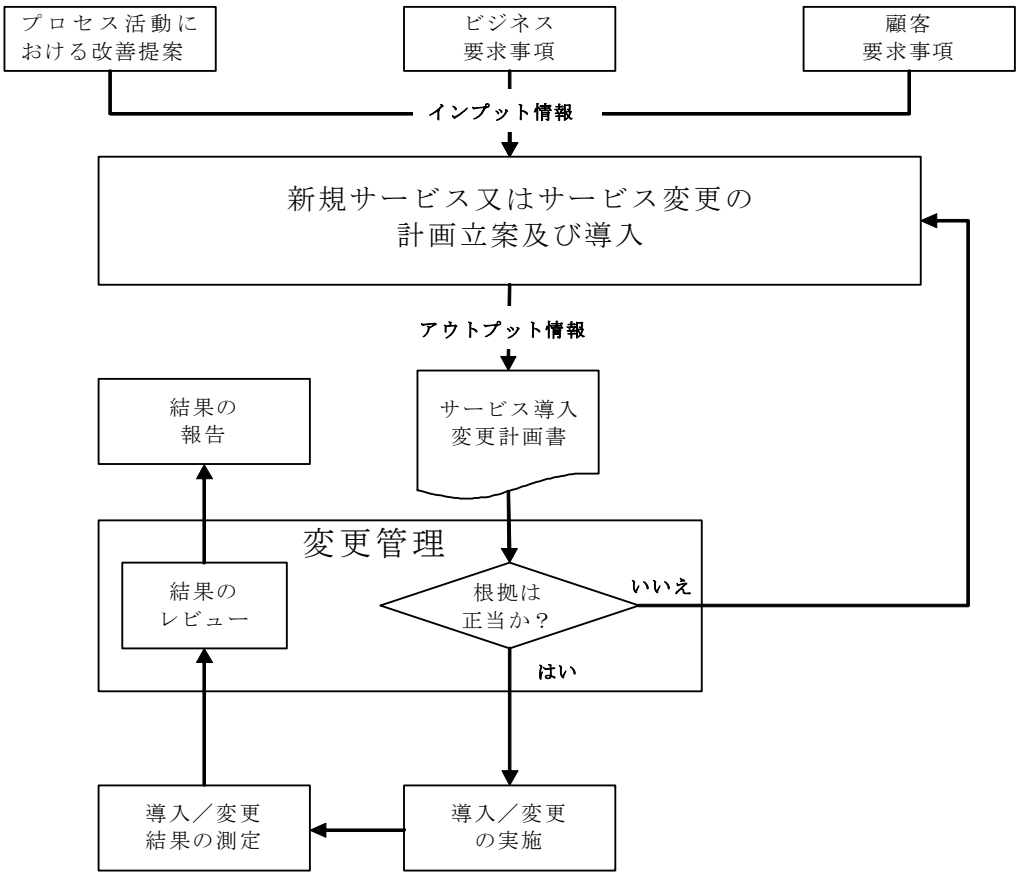


図 5-1　新規サービス又はサービス変更のフロー

サービス提供組織において発生する変更は、顧客やビジネスへの影響度の大小などにより必ずしも一様ではありません。これらを単一の手順により管理した場合、様々な不都合が生じる可能性があります。

例えば、日々発生するような手順が明確かつ単純な変更作業の全てについて、本章で要求されている詳細な計画を立案していては、業務、ひいては顧客へのサービス提供が立ち行かなくなる可能性があります。

また、その反対に、影響度の大きな作業に関して、本章で求められるような計画を立案せずに導入にあたると、予定外の既存システムへの影響、コミュニケーション不足による関係者間の認識の不整合、コストの増大、要員や技術力の不足といったリスクが生じます。

結果として、スケジュールの大幅な遅延やサービス品質の低下、あるいは計画外のコスト増加など、顧客やサービス提供組織に対して大きな損失を与えてしまう可能性が生じます。

そこで、新規サービス及びサービス変更を、「9.2　変更管理」で扱う変更と明確に区別し、計画に従い管理することを求めています。

本章には、計画立案時に盛り込むべき項目が列挙されています。これをチェックリスト

として活用し、計画を立案してください。そして、その計画の実施可否については、変更管理プロセスにて、その内容（リスク、影響、事業利益など）を評価し、承認を受けてください。このように計画は変更承認の場における判断材料としても、とても重要です。

また、サービス受け入れ基準や期待される結果を計画に盛り込むことは、導入後レビューにおいて計画実施結果の分析や成否の判断をするためにも不可欠な項目となります。

要求事項

- 新規サービス又はサービス変更の計画立案時は、費用・組織・技術・営業の面への影響を考慮する。
- 新規サービス又はサービス変更の導入は、変更管理プロセスを通して計画し、承認する。（サービスの終了も含む）
- 新規サービス又はサービス変更の計画には、次を含める。（例）
  - a) 新規サービス又はサービス変更の導入、運用及び維持についての役割と責任
  - b) 人的資源及び人員採用の要求事項
  - c) 技能及び教育・訓練に対する要求事項（例えば、利用者及び技術支援）
  - d) 新規サービス又はサービス変更のための予算及びスケジュール
  - e) サービス受入れ基準
  - f) 新規サービスの運用によって期待される結果（測定可能なもの）
- 新規サービス又はサービス変更は、稼働環境に導入される前に、サービス提供者により承諾を得る。
- サービス提供者は、変更管理プロセスを通して新規サービス又はサービス変更後に計画された結果と実際の結果とを比較しレビューする。

留意事項

- 本章で扱う変更と「9.2　変更管理」で扱う変更を定義し区別して下さい。
- 計画の立案に際しては正しい根拠が必要です。
- 計画は、変更管理のもとリスク、影響、事業利益を評価し承認を得るために必要な判断材料であることが重要です。
- 新規サービスの立ち上げとサービスの変更だけではなく、サービスの終了に関する計画も本章の要求事項に従い実施することが必要です。
- 導入計画は、正式な変更管理プロセスの承認手順にしたがい認可することが必要です。加えて、導入後も変更管理のもとレビューを行い、期待された結果と実際の結果を比較し評価することが必要です。
- 本章で取り扱うような新規サービス追加あるいは大きなサービス変更が生じた場合、そのサービス追加や変更が本認証基準への適合性や認証の適用範囲に影響を与えるものであれば、審査登録機関による差分審査が必要となる場合があります。

6. サービス提供プロセス

6.1. サービスレベル管理（SLM）

サービスレベル管理とは、サービス提供者と顧客の間において、提供する IT サービスの内容やサービスレベルを明確にした上で合意し、サービスレベルを満たしているかどうかを監視し、報告し、必要に応じて改善を行うといった継続的なプロセスのことをいいます。

IT サービスの提供を受ける顧客は、明確な合意（あるいは契約）がなくともある程度のサービスが提供されるものと認識していることがあります。顧客の IT サービスに対する黙示的な要求から、サービス提供者はより広い範囲のサービスを提供しなければならないこともあるでしょう。このような事態は、顧客とサービス提供者の良好な関係の構築を阻害する要因にもなりかねません。サービス提供者と顧客の間で合意済みの IT サービスの内容やサービスレベルを記載したサービスレベル合意書は、顧客との関係の構築・維持向上において中心的な役割を果たすものとなります。

本規格では、サービスレベル管理の目的を以下のように規定しています。

> 目的：サービスレベルを定義，合意，記録及び管理するため。
>
> （JIS Q 20000-1:2007　6.1 サービスレベル管理（SLM）　より引用）

解説

サービスレベル管理を導入する前に、サービス提供者が提供する IT サービス全体とその関係者を明確にすることが重要になります。関係者とは、サービス提供者の組織内の各担当者、IT サービスの提供先である顧客、IT サービスを支援する内部供給者（社内の別組織）や外部供給者等を指します。IT サービスを支援する内部または外部の供給者が存在する場合、顧客と IT サービスについて合意するには、支援を受ける内部または外部の供給者との間で事前の調整が必要である場合があるためです。

これらを明確にした上で、各関係者との間で IT サービスの内容やサービスレベルについて交渉、合意していくことになります。本規格では、IT サービスの内容や求める水準を定義する文書のうち、顧客と合意するものを「サービスレベル合意書（SLA：Service Level Agreement）」、その他の供給者と合意するものを「支援サービスに関する合意」、中でも特に外部供給者と合意して締結するものを「供給者契約」と呼んでいます。

なお、ITIL では内部供給者との合意文書と外部供給者との合意文書を示す用語を以下のように区別して用いています。

オペレーショナルレベル・アグリーメント（OLA）
オペレーショナルレベル・アグリーメント（OLA：Operational Level Agreement）は内部の IT 部門と交わす合意で、ネットワークやプリンタ・サーバの可用性等、特定要素のサービス提供についての合意を詳述したものです。例えば、SLA にて、高い優先度のインシデントの回復目標値を含んでいる場合、OLA は、サポート・チェーンのそれぞれの要素に対する目標値（サービスデスクにおけるコールへの応答やエスカレーション等に対する目標値、ネットワーク・サポートにおける関連するエラーの調査開始と解決に対する目標値等）を含まなければなりません。OLA はサービスを提供する IT 組織をサポートします。

請負契約（UC）
請負契約（UC：Underpinning Contract）は外部のプロバイダと交わす合意で、ワークステーションの問題解決や通信網のリース等、サービスのあるようその提供についての合意を詳述したものです。UC は OLA を外部で実施するようなものです。多くの組織では内部の IT 部門が IT サービスの提供を行っており、SLA や OLA は法的な契約というよりもむしろ内部の部門間で合意したものを記載したものになっています。しかし、外部のプロバイダと結ぶ請負契約（UC）は通常、正式な契約書となります。

（ITIL 入門　10 サービスレベル管理　より引用）

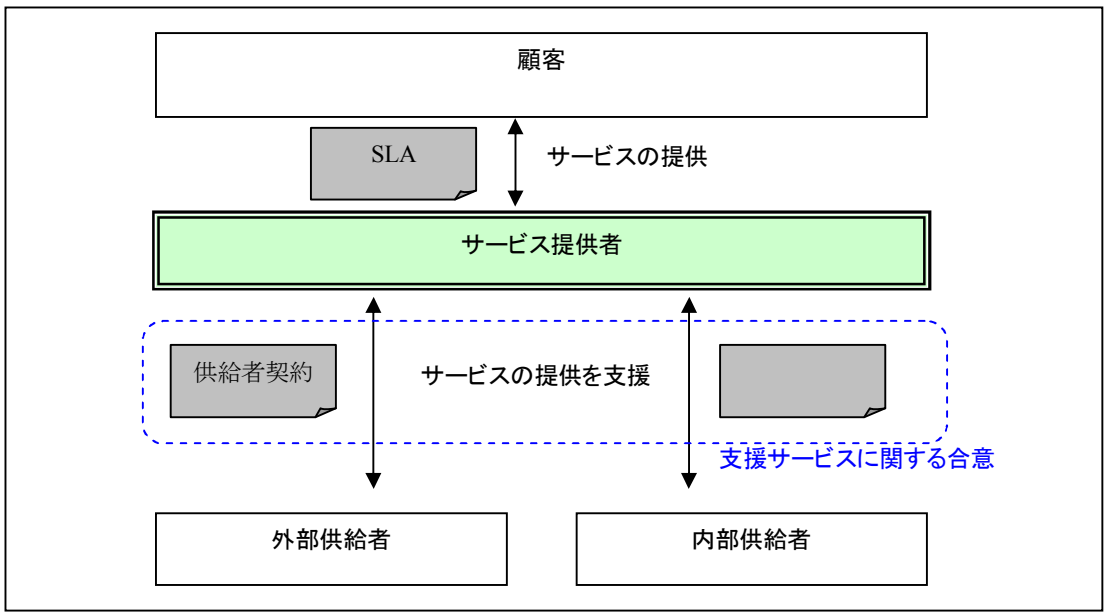


図 6-1　サービス提供者・顧客・供給者の関係（例）

顧客との間に締結する SLA は、必ずしも提供する IT サービスの単位で作成する必要はないでしょう。実際のサービス提供の場では、一つの IT サービスを複数の顧客へ提供するケースや、複数の IT サービスを一つの顧客へ提供するケース等も考えられるためです。SLA の体系には、IT サービス毎や顧客毎及びこれらを組み合わせる体系等がありますが、サービス提供者側の組織体制や提供する IT サービス、支援を受ける供給者などの各要素を考慮し、適切な SLA 体系を検討する必要があります。

サービスレベル管理を導入するためには、SLA の草案を作成し、それを基に顧客と交渉し、合意を得て締結する必要があります。また、SLA の草案作成段階において、関係する支援サービスがあるかどうか確認し、SLA の要求事項を満足するために必要があれば支援サービスに関する合意を見直します。一般に、供給者から支援を受けるサービスより高い水準のサービスを提供することは困難であると考えられるためです。

SLA には、サービス内容やサービスレベル指標とその目標はもちろんですが、緊急時の対処方法、サービスレベルの結果報告内容や頻度等のコミュニケーションの方法等も明記します。SLA を正式に合意した後には、SLA 自体も構成管理の対象文書として取扱い、関係者に周知することになります。SLA の記載内容を修正する場合には、変更管理に従い実施します。SLA を変更することによって、サービス提供者の IT サービス提供能力を超える目標値を設定することがないか等を、変更管理が評価し、確認するためです。

SLA に含める指標のガイドは、経済産業省の「情報システムに係る政府調達への SLA 導入ガイドライン」や総務省の「公共 IT におけるアウトソーシングに関するガイドライン」、電子情報技術産業協会(JEITA)の「民間向け IT システムの SLA ガイドライン」等に記述がありますので、参考にするとよいでしょう。

SLA の内容に基づいた実際の運用においては、サービスレベル指標の監視と、監視結果の報告を行います。顧客への報告は、SLA の定めに従い実施しますが、目標値に達していない場合や、その傾向が見られる場合等も報告を行うことが求められています。報告の内容に関する詳細は、「6.2 サービスの報告」で説明します。

改善策には、SLA に対する不適合等から発見される IT サービス自体の改善、個々の SLA の内容の改善や、サービス提供者組織内の改善、顧客からの要請や苦情に基づいた改善等さまざまなケースが考えられます。このうち、個々の SLA の内容の変更に留まらないような課題については、サービス改善計画の要素として取扱うことにより、組織として統一的な対応を実施することが可能になります。

要求事項

- （サービス提供者が）提供できるサービスの全範囲を、対応するサービスレベル目標及び作業負荷の特性とともに、関係者で合意し、記録すること。
- 提供するそれぞれのサービスを、一つ以上の SLA の中で定義し、合意し、文書化すること。
- SLA は、支援サービスに関する合意内容、供給者契約及び対応する手順とともに、これらの関係者のすべてで合意され、記録されること。
- SLA を、変更管理プロセスの下に置くこと。
- SLA が最新の状態であること及び常に有効であることを確実にするために、関係者による定期レビューによって、SLA を維持すること。

- （IT サービスの）最新情報及び傾向情報を示して、サービスレベルを目標に照らして監視し、報告すること。
- （IT サービスの）不適合の理由を報告し、レビューすること。
- サービスレベル管理で特定した改善策を記録し、サービス改善計画へ入力すること。

留意事項

- サービスレベル管理は、サービス提供プロセス全体において中心的なプロセスとなるため、SLA の変更は他の多くのプロセスに影響を与える可能性があることに留意する必要があります。
- SLA は、顧客と合意した内容を記載したものであるため、達成不可能な目標値や、測定不能な内容を含めることは避けるべきです。また、顧客側の理解を十分に得られるような表現となるように、IT 専門用語の不必要な使用を避ける等の配慮をする必要があります。
- SLA に含むサービスレベル指標及び目標は、顧客の要求とサービス提供者の提供範囲及びレベルを定めるものであるため、顧客及びサービス提供者双方の視点から見て納得感のあるものにすべきです。

6.2. サービスの報告

サービスの報告とは､提供している IT サービスの状況を正確かつ適時に報告することです。報告された情報は、IT サービスに対する適切な意思決定を下すために利用されます。したがって、サービス報告書に含まれる情報は正確かつ信頼できることを合理的に説明できなければならず、また最新の情報である必要があります。

本規格では、サービスの報告の目的を以下のように規定しています。

> 目的：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。
>
> （JIS Q 20000-1:2007 6.2 サービスの報告　より引用）

解説

サービスの報告を実施する目的は、本規格にも規定されているように意思決定及び効果的な伝達をすることにあります。目的から考えると、IT サービスの状況を報告する相手先は、サービス提供者の経営陣や管理者、顧客が考えられます。

サービス提供者の経営陣や管理者に向けたサービス報告書は、SLA に対する遵守状況はもちろんですが、予定されている作業の種類や負荷、必要なリソース、重大なインシデントや変更後の IT サービスの状況、他のプロセスからの重要な情報等の、内部管理に必要な情報を含んでいる必要があります。サービス報告書に含まれるこれらの情報に基づき、経営陣や管理者は、IT サービスの改善の方向性について意思決定を行うことになります。適

切な意思決定を行うためには、当然のことながら報告される情報は信頼性があり正確なものであることが求められ、一般には、日々のサービスレベル監視報告から傾向や問題点をとりまとめて、一定の間隔で報告する方法等が考えられます。また、定期的な報告以外にも、SLA 未達成が発生した場合の報告やその兆候が見られた場合の報告、今後予定しているイベントに関する報告等、随時発生するものもあります。サービス提供者は、報告書を作成するための基礎的な情報を得るため、サービスレベル達成状況の測定や記録を行います。供給者が支援するサービスを利用している場合には、供給者から提出を受ける報告書の内容や頻度についても合意を得て、支援サービスに関する合意にて明らかにしておきます。

また、サービス提供者は、顧客へのサービス報告の内容や頻度を予め SLA の中に記載し、SLA の定めに従い顧客への報告を行う必要があります。顧客へ報告する情報に関しては、サービス提供者として公式なものになるため、前述したような流れで作成した報告書に基づき、サービス提供者の組織内でのレビューを実施する等して経営陣へ報告及び改善の方向性について組織内の合意を得ておくことが必要となります。顧客との関係においては、報告書の提示以外にも、サービス全体や SLA の内容に関するレビュー会議を実施することが求められています（「7.関係プロセス」参照）が、サービス報告書はレビュー会議でも有益な情報の一つとなり得ます。

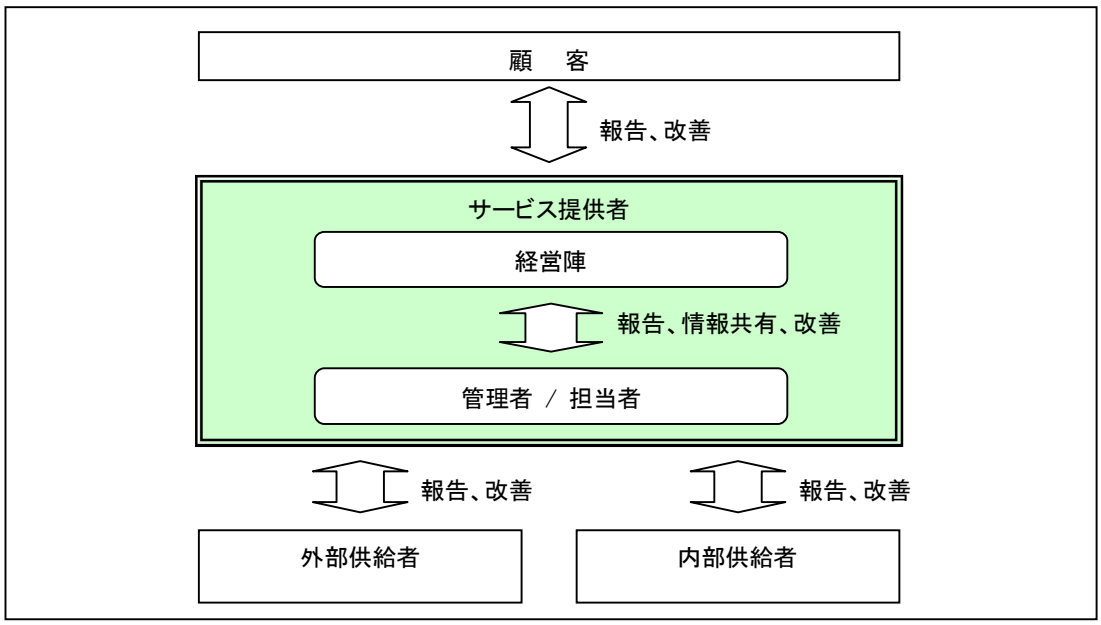


図 6-2　サービスの報告

本規格ではサービスの報告に関して、サービスレベルの達成状況に関係する項目以外にもいくつかの報告を求めています。一つには、IT サービスにおけるコストに影響する事象の報告があります。コストに影響しうる課題については、サービス提供者や顧客、供給者等の関係者間のレビュー会議等で必要に応じて報告することにより、適切な資源配賦を求めることが出来るものと思われます。その他にも本規格では、顧客満足度に関する報告を規定しています。顧客満足度の測定については、「7.関係プロセス」で述べていますが、サービス提供者が意識すべき指標の一つとして必要な関係者に報告し、情報の共有や問題点の改善が求められています。

サービスの報告を行うためには、日常的な監視を行い、その記録を取得する必要があります。この日常の監視記録は、顧客への報告書を取りまとめるための基礎的な情報となります。サービス提供者は組織内のレビュー等により、この記録に最新の情報や見受けられる傾向などを付加し、分かり易い形式で報告書に記載します。また、これらの報告内容や SLA 記載内容の変更の要否を確認するためのミーティングを開催する必要があります。ミーティングの頻度やメンバーは、通常、提供する IT サービスの特性により決定しますが、顧客とのミーティングに関しては、SLA に開催頻度等が記載されている場合には、SLA の記載に従い開催する必要があります。

このようにサービスの報告内容は、ITSMS 全体やサービスレベル管理において改善のきっかけとなるような情報を提示するための重要な役割を果たします。サービス提供者は、適切な報告対象者に適切な方法・時期で、正確な報告が行われるように努める必要があります。

要求事項

- サービス報告書には、その文書の識別、目的、報告先及びデータの出所を含む、明確な説明を記載すること。
- サービス報告書は、明らかになった必要性及び顧客要求事項を満たすために作成すること。サービスの報告には、次の事項を含めること。
  a) サービスレベル目標に対するパフォーマンス
  b) 順守していないこと及びその懸念（例えば、SLA の不履行、セキュリティ違反）
  c) 作業負荷の特性（例えば、作業量、資源の利用程度）
  d) 重大な事象（例えば、重大なインシデント、変更）の後のパフォーマンスの報告
  e) 傾向情報
  f) 満足度の分析
- 経営陣による決定及び是正処置は、サービス報告書の所見を考慮すること。また、この決定及び是正処置を、該当する関係者に伝達すること。

留意事項

- サービス提供者は、本規格で規定されている a)～f)の項目を参考に報告相手毎に報告すべき内容やその詳細さを検討する必要があります。
- サービス報告書に SLA 未達成の情報が含まれる場合は、特に今後講ずる予定の是正処置の内容までを含めておくことが望まれます。
- サービス報告書は、必ずしも IT 部門の関係者のみが参照するとは限りません。特に顧客に提示する報告書は、報告相手に配慮して分かり易い内容となることに留意する必要があります。

6.3. サービス継続及び可用性の管理

サービス継続及び可用性の管理は、IT サービスをどの程度利用可能にするかを特定し、特定された要求を満たすための活動を継続的に行うことです。今や、IT サービスは事業を成功させるための重要な要素となり、IT サービスの停止は直接的に事業の停止を意味することもあるでしょう。24 時間 365 日動き続ける事業の世界では、あらゆる状況下において IT サービスの継続性及び可用性を確保するために、サービス継続及び可用性の管理は常に意識されなければならないのです。

本規格では、サービス継続及び可用性の管理の目的を以下のように規定しています。

> 目的：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。
>
> （JIS Q 20000-1:2007 6.3 サービス継続及び可用性の管理　より引用）

解説

サービス継続の管理と可用性の管理は、どちらも IT サービスが利用可能な状態を保つという目的がありますが、可用性の管理は主に日常的に起こり得る可能性が高い障害（機器障害等）に着目しており、サービス継続の管理は効果的な対策が直接実施できないもの（例えば地震、テロ等）やサービス全体にわたり大きな障害が発生しうる問題等に着目しています。つまり、IT サービスが利用可能であることに対して、可用性の管理は日常的な管理を行い、サービス継続性の管理は重大なサービス障害や災害等の発生時の管理を行うと考えるとよいでしょう。

サービス継続及び可用性の管理の第一歩は、サービス提供者の事業計画（重要視する顧客や IT サービス等）、顧客との SLA、リスクアセスメントの結果に基づき、IT サービスの継続性及び可用性に対する要求事項を明らかにすることです。IT サービスの継続性及び可用性を高めるには、一般的には投資が必要となります。IT サービスの継続性及び可用性に対する要求事項は、IT サービスにどの程度投資をすべきか判断するための材料を提供します。

これらの要求事項を明らかにするための方法の一つとして、ビジネスインパクト分析が

考えられます。ビジネスインパクト分析は、IT サービスの停止が発生した際に事業に与える影響を明らかにすることで、対応の優先度を提供します。優先的に対応すべき IT サービスが明らかになったら、リスクアセスメントにより IT サービスが保有するリスクを識別し、評価します。この結果を受けて、サービス継続及び可用性に対する要求事項を特定していきます。なお、ビジネスインパクト分析及びリスクアセスメントの結果は、IT サービスの変更により影響を受けることが考えられます。これらの結果に変化がある場合はサービス継続及び可用性に対する要求事項にも変化がある可能性があるため、対象とする IT サービスにおいて変更が実施される際には、変更管理において、サービス継続及び可用性の管理に及ぼす影響をよく確認することが求められます。

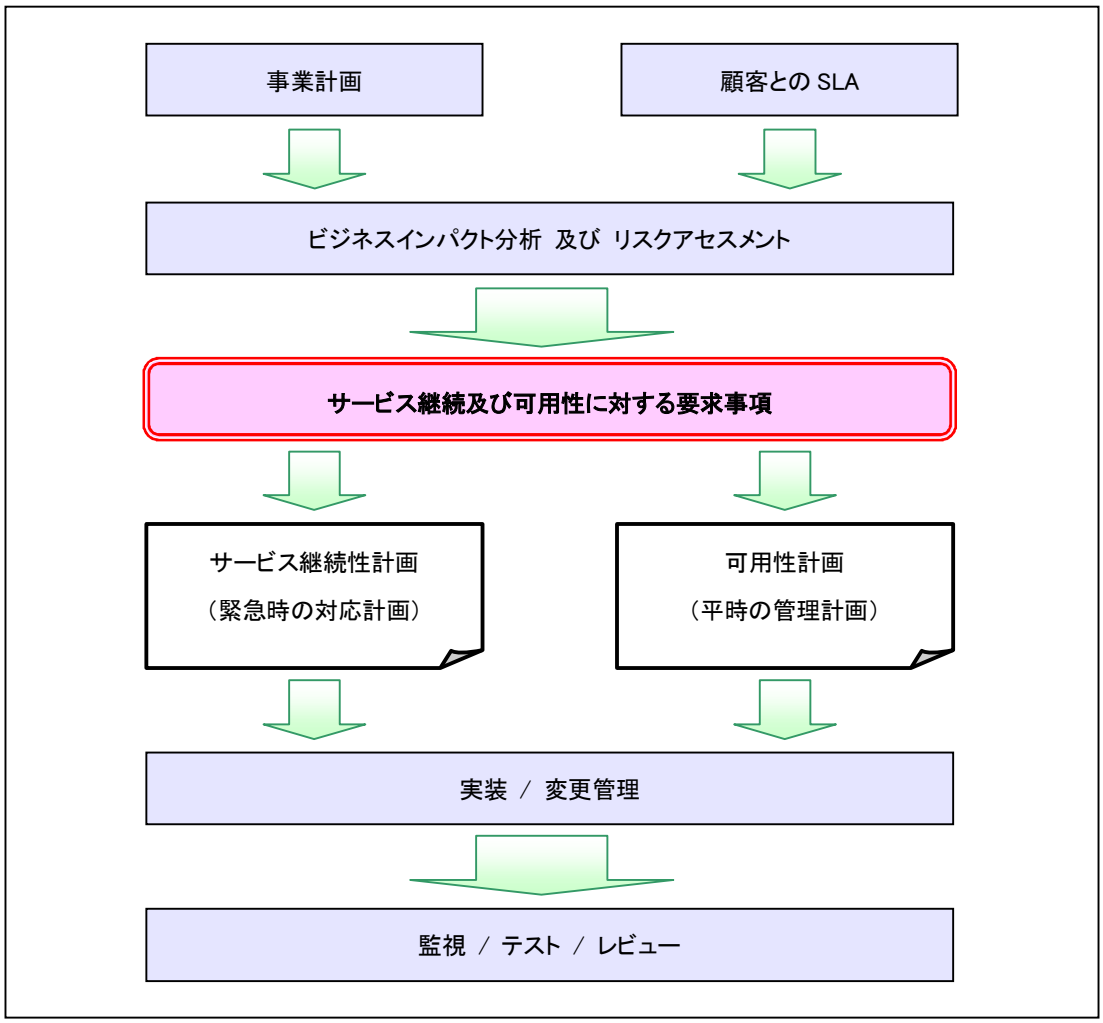


図 6-3　サービス継続及び可用性の管理

サービス継続及び可用性に対する要求事項は、測定の実施や是正処置等のために数値目標として設定することがよいでしょう。少なくとも、IT サービスの応答時間及びシステムコンポーネント全体の可用性について定めることが望まれます。数値目標を定めることで、それを実現するための具体的な可用性計画、サービス継続性計画を策定することができる

ようになります。可用性計画は、特定したサービス継続及び可用性に対する要求事項を満たすために必要な日常的な（平時の）管理の計画であり、サービス継続性計画は、重大なサービス障害や災害等が発生した場合であってもサービス継続性が損なわれないようにするための緊急時の対応計画ということができます。なお、サービス継続性計画では、緊急時の対応計画である性質上、通常のオフィス利用ができない状況も想定しておく必要があります。そのため、サービス継続に必要な情報であるサービス継続性計画や緊急時の連絡先一覧、構成管理データベース等はバックアップサイト等でも使用可能であることをあらかじめ確保しておく必要があります。

可用性及びサービス継続性計画で定めた数値目標は常に監視し、監視データとして記録していきます。常に監視されていなければ、対象サービスの品質が低下した時、気がつくことさえないかもしれません。また、監視データがなければ、数値目標が達成されているのか、現状がどうなのか知る術がありません。監視データを収集するためには、予め数値目標を分析し､数値目標に関わるデータをもれなく収集できるように設計をしておきます。収集した監視データは、少なくとも年に一度はレビューし、数値目標を満たしているか、SLA 等の要求事項を満たしているか、監視設計に問題はないか等を確認します。

策定した可用性及びサービス継続性計画は、定期的にテストすることが望まれます。想定したリスクが顕在化したと仮定し、復旧計画等がうまく機能するか確認するためです。実施の結果は逐次記録し、想定どおり実施されなかった点については、改善しなければなりません。テストは定期的に実施するほかにも、事業環境が大きく変化した場合（企業合併、類似事故の多発等）にも実施します。

要求事項

- 可用性及びサービス継続に関する要求事項を、事業計画、SLA 及びリスクアセスメントに基づいて特定すること。要求事項には、アクセス権、応答時間、及びシステムコンポーネント全体の可用性を含めること。
- 通常状態から重大なサービスの中止にいたるあらゆる状況において合意した要求事項を満たすことを確実にするために、可用性及びサービス継続計画を策定し、少なくとも年 1 回レビューすること。これらの計画は、事業上の必要に基づいて合意した変更が計画に反映されることを確実にするために、維持すること。
- 事業環境に重大な変更があった場合には、そのたびに可用性及びサービス継続計画を再試験すること。
- 変更管理プロセスは、可用性及びサービス継続の計画を変更することの影響について、アセスメントを行うこと。
- 可用性を測定し、記録すること。計画にない可用性の喪失を調査し、適切な処置をとること。
- 通常のオフィスの利用が妨げられた場合でも、サービス継続計画、連絡先一覧及び構成管理データベースは利用可能であること。サービス継続計画には、平常業務への復

帰も含めること。
- 事業上の必要性に沿って、サービス継続計画を試験すること。
- すべての継続試験は、記録すること。試験が不合格の場合は、処置計画を策定すること。

留意事項

- ビジネスインパクト分析を実施する際には、利害関係を考慮し、客観的に分析するために、複数の利害関係者の視点（顧客からの視点、経営からの視点、社内関係者からの視点等）から分析するようにすべきです。

6.4. サービスの予算業務及び会計業務

サービスの予算業務及び会計業務は、サービスの提供において、得られた収入と消費されたコストを継続的に正確かつ適時に把握し、予算との対比を行うことにより、財務面での問題点の早期発見及び対応策の早期実施を実現することです。このような活動を行うことにより、IT サービスの提供に関する投資効果を最大化することを目指し、サービス提供者としての最適な投資配分を行うための情報提供を行うことを目的としています。

本規格では、サービスの予算業務及び会計業務の目的を以下のように規定しています。

> 目的： サービス提供費用の予算を管理し，かつ，会計を行うため。
>
> （JIS Q 20000-1:2007 6.4 サービスの予算業務及び会計業務　より引用）

解説

予算業務では、サービスの提供に必要な資金を予測することで、サービスの提供に関する効率的な予算計画を立案することが求められます。また、予算計画にて配分された予算項目は、会計処理によって算出された実績データとの比較により採算の管理を行うことができるため、予算の超過や著しい不採算状況への迅速な対応が可能となります。したがって、より正確な採算性を把握するためにはサービスの提供に関わる全てのコンポーネント（予算を配分する必要がある要素）ごとに予算費目を定めた上で、予算配分ならびに実績の管理をしていく必要があります。

会計業務では、一定の期間ごとの決算終了後の会計データを用いて、サービスの提供に投入された資金（実績データ）の集計を行うことが求められます。実績データを集計する際には、予算業務にて立案された予算計画との比較によって財務状況を把握することとなります。したがって、会計業務にて実績データを集計する際の費目については、分析精度を高めるために、予算業務にて設定したコンポーネントに関連付けた原価レベルでの管理が望まれます。実績データは、大きく間接費と直接費に区分することができ、直接費については当該費用の発生元に関するコンポーネントに計上することとなります。一方間接費

については、費用の発生源を一意に特定することができない費用（管理部門の人件費、共通インフラの維持・運営費用）ですので、コンポーネントごとに間接費を配賦する必要があります。

サービスの提供に関する財務状況は、予算業務、会計業務からのアウトプットで把握することができるものです。財務状況の管理を効率的に進めていくためには、実績データと予算計画との乖離を適時に検出することが必要となります。したがって、定期的にサービスの提供に関する財務状況を取りまとめ、関係者に周知すること、ならびに問題点の見直しをしていくことが重要です。

サービスの変更には一般的にコストがかかります。サービスの変更が予定されていたものである場合、すでに予算化されている場合が多いでしょうが、予定外のものであった場合には、必要なコストについて承認を得る必要があります。この活動は、変更管理プロセスの中で実施することになります。

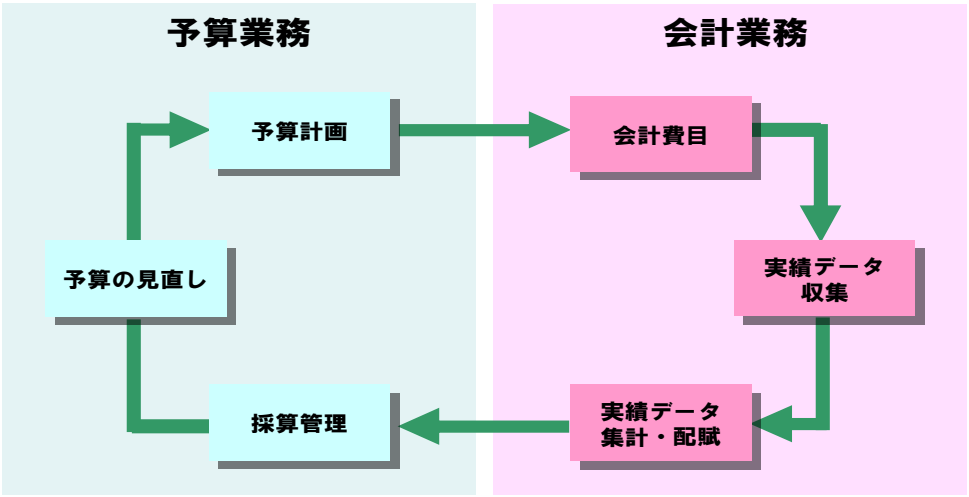


図 6-4　サービスの予算業務及び会計業務

要求事項

- 次の事項に対して明確な方針及びプロセスを備えること。
  - すべてのコンポーネント（例えば、情報資産、共有資源、間接工数、外部提供のサービス、人員、保険、使用許諾）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
  - 効果的な財務管理及び認可
- 費用は、効果的な財務管理と意思決定とができるように十分詳細に予算化すること。
- サービス提供者は、予算と照らして費用を監視し、報告すること。また、財務予測をレビューし、それに応じて費用を管理すること。
- サービスの変更は、変更管理プロセスを通して費用を見積り、承認を得ること。

留意事項

- 予算業務、会計業務による財務状況の管理は、契約単位に管理することが望まれます。
- 財務会計（財務報告に関する会計処理）と本規格が要求している会計業務は目的がことなるため、区別することが望まれます。ただし、全く別の管理を行うことは非効率的であることから、会社全体で実施している予算業務及び会計業務と ITSMS で行う予算業務及び会計業務とを整合しておくことが望まれます。
- 顧客に対する課金業務に関する事項は本規格の対象外です。

6.5. 容量・能力管理

容量・能力管理は、容量・能力に対する計画を立案し維持することで、サービス提供者が IT サービスの提供に必要かつ十分な容量・能力を保有し続けることを可能にします。IT サービスの提供に必要な容量・能力が不足するような事態が発生した場合には、IT サービスのパフォーマンスが低下することが予想され、場合によっては SLA で合意したサービスレベルを達成できない状況に陥ってしまうことも考えられます。したがって、容量・能力管理の目的は、現在または将来の顧客の事業上の要件に沿って、適時かつ適切なコストで必要な IT サービスの提供を可能にすることや、IT リソースに対する顧客の需要に供給を一致させることです。

本規格では、容量・能力管理の目的を以下のように規定しています。

> 目的：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。
>
> （JIS Q 20000-1:2007 6.5 容量・能力管理　より引用）

解説

容量・能力管理は、顧客からの事業上の要求事項（ニーズ）、IT サービス、リソースの 3 つの観点から検討していく必要があります。これは、サービス提供者が提供する IT サービスに対して、顧客からどのような期待や要求がなされているのかを理解し、保有している IT サービス及びリソースが現在どの程度利用されているのかを把握することによって、現在及び将来を通じて過不足のない容量・能力を計画するために必要な観点です。

ITIL では、顧客からの事業上の要求事項に着目する「事業キャパシティ管理」、IT サービスの利用に着目する「サービス・キャパシティ管理」、リソースの利用に着目する「リソース・キャパシティ管理」の 3 つを容量・能力管理のサブプロセスとして位置付けており、以下のように説明しています。

事業キャパシティ管理
このサブプロセスの達成目標は、将来のユーザのニーズを理解することである。これは戦略計画等顧客からの情報を得たり、トレンド分析を実施することによって行う。このサブプロセスは、本質的にプロアクティブである。

サービス・キャパシティ管理
このサブプロセスの達成目標は、IT サービス（顧客へ提供される製品やサービス）の利用を把握、理解することである。適切なサービスの合意を行ってこれを保証するために、パフォーマンスと最大負荷を理解していなければならない。このサブプロセスは、サービスの合意の定義や交渉においてサービスレベル管理と強力に結び付いている。

リソース・キャパシティ管理
このサブプロセスの達成目標は、IT インフラストラクチャの利用を把握、理解することである。リソースの例としては、ネットワークの帯域、処理能力、ディスク容量等がある。これらのリソースを効果的に管理するために潜在的な問題は早く検出しなければならない。また、技術の発展に遅れをとらないようにする必要もある。積極的にトレンドを監視することは、このサブプロセスでは重要な活動である。

（ITIL 入門　12 キャパシティ管理　より引用）

容量・能力管理は、現在の要求を満たすことはもちろん、将来の要求を満たすことも求められるため、顧客にとっての IT サービスはどのような位置付けにあるのか、将来的にどのような拡張が必要になるのか、またサービス提供者としては顧客の要求にどのように応えていくのか、といった事業の観点からの IT サービスの位置付けを理解しなければなりません。つまり、IT サービスに対する顧客からの事業上の要求事項の観点から、サービス提供者としてどのような方針をとっていくのか、具体的にはサービス提供者としての経営方針、事業方針への対応や、外部の変化（法令対応等）といった企業活動方針を理解することが必要です。これらの理解及び現状を踏まえて、容量・能力計画を立案することになります。

IT サービス、リソースに関する容量・能力管理としては、IT サービスが SLA の目標値の達成を確実にし、要求通りに機能するために必要な IT サービス、リソース面での容量・能力の管理をしていきます。IT サービスの容量・能力は、主に IT サービスの利用状況から計測することができます。リソースの容量・能力は、IT サービスを提供していくために必要なハードウェア、ネットワーク機器、周辺機器、ソフトウェア、人的リソース等の使用状況から計測することができます。これらの情報を計測するために、必要となる監視手段及び手順を備えておく必要があります。IT サービス及びリソースの容量・能力の現状を正しく把握することができなければ、容量・能力の調整もできませんし、将来のための計画を立案することもできないためです。

また、容量・能力管理では、事業上の要求事項や IT サービス・リソースの容量・能力に関する情報を蓄積していきます。この情報は、新たな IT サービスを開発する場合や IT サービスを変更する場合に、必要なリソースの情報を提供する等の支援を行うことができま

す。容量・能力管理の支援により、新たな IT サービスの開発や変更におけるコストや所要期間の見積もり等が容易になることが考えられます。

要求事項

- 容量・能力管理は、容量・能力計画を立案し、維持するものであること。
- 容量・能力管理は、顧客からの事業上の必要性に取り組むものであること。
- 容量・能力管理には、次を含めること。
  - 現在及び予測された、容量・能力及びパフォーマンスに対する要求事項
  - サービス拡張のための、明確な、期間、しきい値及び費用
  - 予想されるサービス拡張、変更要求、新技術及び技法が、容量・能力に及ぼす効果の評価
  - 外部の変化（例えば、法令の変更）に関して予測される影響
  - 予測分析を可能にする、データ及びプロセス
- サービスの容量・能力を監視し、サービスのパフォーマンスを調整し、適切な容量・能力を提供するための方法、手順及び技法を明確にすること。

留意事項

- サービス拡張等は、経営方針、事業方針等の事業上の要求事項に従って決定されるようにすべきです。
- 容量・能力管理では、実績データの管理に加えて、将来における予測も行うことが望まれます。

6.6. 情報セキュリティ管理

IT サービスは、LAN・インターネット等のネットワークを介して他の事業や外部と接続されることで利用範囲が拡大する一方、IT インフラストラクチャの複雑化や外部接続先の増加等により内外の様々なリスク（技術的な障害、人為的ミス、不正アクセス、コンピュータ・ウイルス等）に対する脆弱性が多様化し複雑化しています。

情報セキュリティ管理ではこれらのリスクを分析し、管理することで SLA や契約、法律といった外部からの要件を満たすこと、組織が定めるセキュリティレベルを維持することを可能にします。

本規格では、情報セキュリティ管理の目的を以下のように規定しています。

目的： 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。 （JIS Q 20000-1:2007 6.6 情報セキュリティ管理　より引用）

解説

本規格の情報セキュリティ管理は ISMS の要求事項を要約した内容となっています。そ

のため、ITSMS を適用する範囲が ISMS を構築した範囲に含まれる場合には、ISMS の仕組みをそのまま使用して情報セキュリティ管理の活動を実施することができます。一方、ITSMS を適用する範囲において ISMS を構築していない（または一部のみ ISMS を適用している）場合には、ISMS の要求事項を全て網羅する必要はなく、以降に記述する本規格で要求される事項を満たすことで情報セキュリティ管理の活動を実施することになります。

ISMS ユーザーズガイド（JIP-ISMS111-2.0）は、ISMS の構築、維持及び改善に有用な情報を提供します。なお、JIS Q 27001:2006 では、ISMS の構築、維持及び改善を実施するための PDCA モデルの概要を以下のように規定しています。

＜ 表 6-1 ISMSのPDCAモデルの概要＞

計画 （ISMS の確立）	組織の全般的方針及び目的に従った結果を出すための，リスクマネジメント及び情報セキュリティの改善に関連した，ISMS 基本方針，目的，プロセス及び手順の確立
実行 （ISMS の導入及び運用）	ISMS 基本方針，管理策，プロセス及び手順の導入及び運用
点検 （ISMS の監視及びレビュー）	ISMS 基本方針，目的及び実際の経験に照らした，プロセスのパフォーマンスのアセスメント（適用可能ならば測定），及びその結果のレビューのための経営陣への報告
処置 （ISMS の維持及び改善）	ISMS の継続的な改善を達成するための，ISMS の内部監査及びマネジメントレビューの結果又はその他の関連情報に基づいた，是正処置及び予防処置の実施

（JIS Q 27001:2006 0.1 序文 0.2.2.プロセスアプローチ より引用）

情報セキュリティ管理に取組む際の第一歩は、組織の情報セキュリティに係る方向性や行動指針を定めることを目的として、サービス提供者における情報セキュリティ管理の基本的な考え方としての情報セキュリティ基本方針を策定します。策定した情報セキュリティ基本方針は、IT サービスの提供に関わる全ての要員に周知する必要があります。なお、情報セキュリティ基本方針は組織の経営方針や行動指針と整合性が取られていなければならず、経営陣としての考え方を表明するものであるため、しかるべき権限を持つ組織の経営陣により承認されなければなりません。また、目標及び要求事項を達成するために、IT サービスまたはシステムへのアクセスに関連するリスクを識別し評価するためのリスクアセスメントを実施します。ここでは、サービス提供者が保有する情報資産を特定することから始めることになるでしょう。情報資産を特定したら、情報セキュリティを阻害する脅威や、脅威を発生させる要因となる脆弱性を識別してリスクを評価していきます。この結果に基づき、情報セキュリティリスクの発生を予防するための対策を特定していくことになります。情報セキュリティリスクを発生させる脅威及び脆弱性は、IT サービスに変更があった場合には、同様に変化する可能性があります。そのような変化によって、情報セキュリティ対策がうまく機能しない状況が発生することのないように、変更管理プロセスでは変更が情報セキュリティ対策に与える影響についても評価することが求められます。

情報セキュリティを確保するための対策の実施には、必要なリソースを確保するととも

に､対策が確実に実施されるように文書化することが必要になります｡対策の文書化では、対策が形骸化しないために､少なくとも､どのようなリスクを予防するための対策なのか、誰が対策を実施する責任があるのかについて記述しておく必要があります。場合によっては、リスクの発生を予防するために新たな対策を実施する必要もあるでしょう。その場合には対策を実装するためにリスク対応計画を策定し､継続的に進捗管理を行っていきます。

実際の運用段階において、情報セキュリティ管理が意図したとおりに実施され、目標が達成されているかを判断するための監視手順を策定し、実施する必要があります。ここでは、情報セキュリティ対策が実施されていることを定期的に確認するための点検や、セキュリティインシデントの管理を実施します。セキュリティインシデントの管理を実施するためには、インシデント管理に従って報告されることを確実にした上で、原因を調査し是正するための仕組みを備えておく必要があります。

情報セキュリティ管理において発見された問題点については、全て記録し、サービス改善計画へ入力します。

要求事項

- 適切な権限をもつ経営陣は、情報セキュリティ基本方針を承認すること。情報セキュリティ基本方針は、すべての関連する要員に周知され、必要な場合は顧客にも周知されること。
- 次のために、適切なセキュリティ管理策を運用すること。
  - 情報セキュリティ基本方針の要求事項の実施
  - サービス又はシステムへのアクセスに関連するリスクマネジメント
- セキュリティ管理策を文書化すること。この文書は、その管理策が関係するリスク、及び管理策の運用・維持方法を記述すること。
- 変更を実装する前に、変更が管理策に与える影響のアセスメントを行うこと。
- 情報システム及び情報サービスへのアクセス権をもつ外部組織が関与する取決めは、すべての必要なセキュリティ要求事項を定義した、正式な合意に基づいていること。
- 情報セキュリティインシデントは、インシデント管理手順に従って、できる限り速やかに報告し、記録すること。すべてのセキュリティインシデントを調査し、管理処置をとることを確実にするための手順を備えること。
- 情報セキュリティインシデント及び誤動作の種類、数及び影響を定量化、監視できるようにする仕組みを備えること。このプロセスで識別した、改善のための処置を記録すること。また、この改善のための処置は、サービス改善計画に入力すること。

留意事項

- 情報セキュリティ管理の手引きとして、JIS Q 27001:2006 及び JIS Q 27002:2006 が活用できます。
- ISMS をすでに構築している範囲において ITSMS を構築する場合には、既存の ISMS

における活動と変更管理プロセスとの関連性及び整合性、インシデント管理プロセスとの連携に留意するとともに、情報セキュリティリスクアセスメント、教育、内部監査、マネジメントレビュー等の実施時期及び実施内容といった ISMS のフレームワークにも影響が及ぶ可能性があることを意識する必要があります。

7. 関係プロセス

7.1. 一般

関係プロセスでは、「サービス提供者」と、サービス提供者からサービスの提供を受ける「顧客」、サービス提供者の提供するサービスの一部を担っている「供給者」の 3 者が登場します。これら 3 者は、本規格の図 3（「7.3 供給者管理」での引用参照）の中に示されるように、サービス提供のサプライチェーン内におけるそれぞれの役割を果たしています。「顧客」「サービス提供者」間の、サービス提供者側から見た役割とプロセスに関しては「顧客関係管理」に記載されています。「供給者」と「サービス提供者」に関しての、サービス提供者側から見た役割とプロセスについては「供給者管理」に記述されています。

> 関係プロセスでは，顧客関係管理及び供給者管理という，二つの関連する側面を規定する。
>
> （JIS Q 20000-1:2007 7.1 一般 より引用）

本規格の図 3 のサービス提供例では、サービス提供者は、顧客に提供するサービスの一部を供給者 1 及び 2 と、統括供給者 3 から供給を受けています。このケースでは、統括供給者 3 は、サービス提供者に対して提供しているサービスの一部を再請負契約先供給者 4 に依っています。サービス提供者は、供給者 1・2 あるいは再請負契約先供給者 4 からのサービスを含むサービスを提供している統括供給者 3 からのサービスを受け取ります。そしてサービス提供者は、これらのサービスを統合し、付加価値を持ったサービスとして顧客に提供しています。しかしながら、実際の企業の組織に当てはめてみると、供給者、サービス提供者、顧客が独立した組織にそのままマッピングされることは、少ないと言えます。

何故なら、組織自体は、孤立することはなく、何らかのサービス提供のチェーンにおいて、インとアウトを持つ以上、立場が変われば、供給者と顧客の双方の役割を担うことになりますし、供給者がサービス提供者と同じ組織の中に存在することも良くあります。供給と提供の関係自体は相対的であり、図 3 の例でいえば統括供給者 3 の立場からは、自身はサービス提供者を *“顧客”* と見立てた *“サービス提供者”* であり、再請負契約先供給者 4 は *“供給者”* です。 したがって現実には、立場の違いによって供給者と顧客の双方の役割を担うことになる場面があります。さらに、顧客として想定される対象がサービス供給者と同じ組織内に存在する場合や、供給者がサービス供給者と同じ組織内に存在する場合など、複雑で多様な関係者によって構成されることが考えられます。こうした場合には、それぞれの立場で IT サービスマネジメントを構築していく必要がありますが、組織全体でのマネジメントとして全体最適が図られるように留意すべきです。

更に、企業活動を進める上で関係してくる多くの企業または組織が実際には存在するわけで、こうした利害関係も整理しておくことが望まれます

7.2. 顧客関係管理

サービス提供者と顧客の関係を扱います。サービス提供者から見た「顧客」は、実際には個人であったり、企業などの組織体であったりします。「顧客」という呼称は、サービス提供者が提供しているサービスの“対象者”を表現していると表現してもよいかもしれません。一方でサービス提供者とは実際には企業や公共機関などであるので、「顧客」に対する活動とは「事業（ビジネス）」を意味します。関係プロセスの立場からは、「顧客」と「事業」は同一視できます。この規格の原文に当たる ISO/IEC 20000 では、「顧客関係管理」と訳出した本プロセスは、“Business Relationship Management：事業（ビジネス）関係管理”となっています。

目的：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。 （JIS Q 20000-1:2007 7.2 顧客関係管理 より引用）

解説

適切な IT サービスの提供に必要となるビジネスを理解するために、必要なコミュニケーションチャネルが作られ、維持され、活用されていることが重要です。サービス提供者の組織にとって供給者、顧客との関係は組織の外部になる場合もあれば、内部になる場合もあります。外部に対しては契約で正式化され、内部においてはサービスレベル・アグリーメントあるいはオペレーショナルレベル・アグリーメントで正式化されます。

サービス提供者と顧客の良好な関係を確立する為に、次のような活動に応えてゆく必要があります。

- 顧客は誰か？サービスの利害関係者は誰か？
- サービスレビュー会議が開催されているか？
- 苦情処理はなされているか？
- 顧客満足度は測られているか？
- 顧客と利害害関係者

サービス提供者は顧客及び利害関係者の期待と、顧客及び利害関係者はサービスをどのように認識しているかを明確にする必要があります。これらを明確にすることは、良好な関係を築く上での出発点となるからです。サービス提供者は顧客が誰であるか、また、サービスの利害関係者は誰であるかを認識し、文書化しておく必要があります。

サービスレビュー会議の開催

最低でも年に１回、もし、重大な変更が予定されているのであればその前後に、サービス提供者と顧客でサービスレビュー会議を開催します。参加者は利害関係者を含んでも良

いとされています。利害関係者とは、例えば、再請負契約者、利用者グループ、その他の代表団体等です。会議の計画、記録を取り、関係者に周知します。サービスレビュー会議で合意された改善案は記録され、サービス改善計画にインプットされ、変更管理を通じて実施されるべきでしょう。サービスレビュー会議の主要な議題は次のようなものです。

- サービスの適用範囲
- SLA に対する変更
- 契約に対する変更
- 事業上の変更

また、サービス提供者と顧客は進捗状況、達成度、課題に関する中間レビュー会議の開催に合意し、利害関係者に通知することを要求しています。

サービスの苦情処理

サービスにおける苦情とはどのようなものかを定義しておく必要があります。サービス提供者と顧客の間でサービス苦情を定義し、合意しておきます。また、サービス苦情に対する連絡先をサービス提供者、顧客の双方に通知します。サービス提供者は、サービス苦情を処理するプロセスを利用し、そのプロセスで、全てのサービス苦情を記録、調査、対応して、適切な処置を実施します。未解決なサービス苦情についてはエスカレーションのパスを用意しておき、上級管理者が対応し、処理して顧客へ報告することとします。

顧客満足度

顧客の期待、認識、満足度がどのような状態にあるかを知ることは、サービス提供者にとって重要な関心事です。一般的に、サービスの評価は、顧客の主観に基づくものである場合が多いものです。顧客満足度調査は、顧客満足度の目標と現在のサービスのパフォーマンスを比較する指標になります。サービス提供者は顧客満足と顧客関係管理の責任者を 1 名以上指名しておくことが推奨されています。満足度調査を実施する場合は、顧客に負担をかけずに、時間もかからない方法で実施するのが良いでしょう。満足度レベルに大きな変化があった場合は、原因を調査し、理解しておくことは重要です。調査結果は顧客と討議し、その後のアクションプランは顧客と合意しておきます。アクションプランはサービス改善計画への入力とします。顧客満足度調査の結果、悪い評価は改善計画へのインプットとなりますが、好意的あるいは良い結果は文書化して、スタッフへ報告すると良いでしょう。これによりスタッフのモチベーションアップにつながることが期待できます。

<u>要求事項</u>

- サービスの利害関係者及び顧客を識別し、文書化すること。
- 少なくとも年 1 回サービスレビューを行い、サービス・SLA・契約等を見直す。
- サービスの提供状況を把握するため、定期的に会議を行い、議事内容を残すこと。
- 契約・SLA の変更は会議を経て、変更管理プロセスで行うこと。

- サービス提供者は、変更に関して認識しておくこと。
- 苦情処理プロセスを有していること。
  - ✓ 苦情の定義を明確にし、顧客と合意すること。
  - ✓ 苦情の受付から終了までを管理すること。
  - ✓ 通常ルートで解決しない場合の経路を確保しておくこと。
- 顧客関係プロセスに責任を持つこと。
  - ✓ 責任者を置くこと。
  - ✓ 顧客満足度の測定プロセスを有していること。
  - ✓ 改善策はサービス改善計画の入力とすること。

留意事項

- 顧客の苦情の内部処理に関する手引として、“ISO 10002：組織における苦情対応のための指針”、JIS Q 10002（2005/6/20 発行）が参考となる。
- 顧客満足に関する国際標準としてはこの他に、以下が審議中である。
  - ✓ ISO 10001：組織のための行動規範に関する指針
  - ✓ ISO 10003：組織外部の紛争解決に関する指針

7.3. 供給者管理

サービス供給者が顧客に提供するサービスは、複数の供給者から構成されることは一般的なことです。場合によっては再請負契約先供給者が存在し、サービス供給者との間に統括供給者が存在する場合もあるでしょう。供給者管理は次のことを目的としています。

目的：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。 （JIS Q 20000-1:2007 7.3 供給者管理 より引用）

解説

均質なサービスとは、供給者によりサービスを提供されていることを顧客が認識していない状況と言い換えることが出来るでしょう。これは、サービス提供者が供給者を管理下においていることを意味します。サービス提供者の組織にとって供給者、顧客との関係は組織の外部になる場合もあれば、内部になる場合も考えられます。外部に対しては契約で正式化され、内部においてはサービスレベル・アグリーメントあるいはオペレーショナルレベル・アグリーメントで正式化されます。サービス提供者と供給者の関係は本規格の図 3 で示されています。

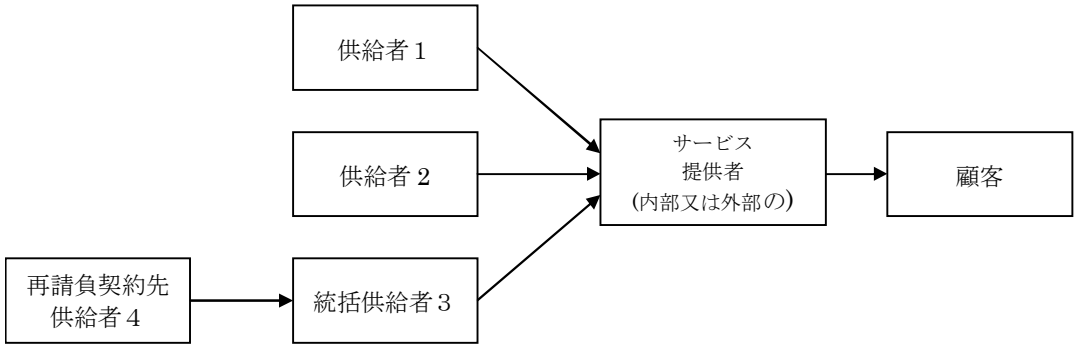


図 3－サービス提供者及び供給者間の関係の例

（JIS Q 20000-1:2007 7.3 供給者管理 より引用）

ITIL では供給者の管理レベルを下記の 3 つに分類しています。

- 戦略レベル
  重要な提携関係
- 戦術レベル
  営利上の活動及びビジネスのやりとりが関与する関係
- 運用レベル
  価値が低く、代替の入手が容易な製品あるいはサービスを供給する関係

サービス提供者は、ビジネスの達成目標に合致した供給者との関係と種類を選択する必要があります。ITIL ではいくつかの供給者関係の種類を挙げています。サービス提供者は、適切な供給者との関係を確立し、維持していく必要があります。

- 内部供給者
  多くの組織では、組織内部に供給者としての役割を持つ部分を備えています。
- 単一または複数の供給者からの供給
  サービスを単一供給者(シングルソース)から入手するか、複数の供給者(マルチソース)から入手します。
- 提携関係
  役員レベルで確立された供給者との関係。
- アウトソーシング
  サービスの一部あるいは全部を外部供給者に、オーナーシップまで含めて移管します。

どの関係においても、契約、あるいは OLA によって支えられるべきです。本規格では、供給者管理手順において次のことを確実にすることが望ましいとしています。JIS Q 20000-2 の 7.3.1 章を参照すると良いでしょう。

a) 供給者が，サービス提供者に対する自らの義務を理解している。
b) 合意されたサービスレベル及び適用範囲において，正規の合意した要求事項が満たされている。
c) 変更が管理されている。
d) すべての関係者間の商取引が記録されている。
e) すべての供給者のパフォーマンスに関する情報が観察可能で，また，これに対して処置をとることができる。

（JIS Q 20000-2:2007 7.3.1 はじめに より引用）

契約管理

サービス提供者と供給者との契約あるいは合意は SLA を満たすために必要な内容でなければなりません。別の表現をすれば、顧客に提供するサービスレベルを支える内容が供給者との契約あるいは合意に記載されていることになります。これには供給者が提供するサービスの範囲、サービスレベル、コミュニケーションプロセス、レビューの予定などが含まれます。本規格では、文書化し、全ての関係者の合意を得ることとしていますので、顧客を含めた、サービス提供者、供給者での合意が必要となります。サービス提供者は、各供給者毎に管理者を置き、必要な場合は共通のプロセスを定め、連絡先を決めておきます。供給者毎の契約を管理し、契約修正があった場合に利用するプロセスを定義しておきます。プロセスではレビューを少なくとも年一回は実施し、契約内容に変更がある場合は変更管理プロセスに従います。

サプライヤ関係の形式化

サービス提供者と各供給者との関係を形式化します。ITIL では、これを下記の、「合意」により形式化しています。

- 基本的なサービス上の合意
  - 基本的な条件
  - サービスの説明
  - サービス標準
  - 作業負荷
  - 管理情報
  - 責任及び依存性
- 広範なサービス合意
  - 報奨と罰則
  - 業績の基準
- 契約上の合意
  - 供給されるサービスの適用範囲
  - サービスのパフォーマンス要件
  - 責任の分担

- 契約のレビューと争議解決のプロセス
- 価格構造
- 支払い条件
- 変更と投資に対するコミットメント
- 合意を変更するプロセス

サービスの定義

本規格では、サービス提供者により各サービス及び供給者ごとに、次の項目を維持することを要求しています。

> a) サービス，役割及び責任の定義
> b) サービスの適用範囲
> c) 契約管理プロセス，権限レベル及び契約解除の計画
> d) 適切な場合は，支払い条件
> e) 合意された報告のパラメタ及び達成したパフォーマンスの記録
>
> （JIS Q 20000-2:2007 7.3.3 サービスの定義 より引用）

複数の供給者の管理

供給者がサービスあるいは製品をさらに再委託している先を再請負契約先供給者とし、その時の供給者を統括供給者としています。サービス提供者は、供給者あるいは統括供給者のいずれと契約しているかを明確にしておく必要があります。供給者はサービス提供者によって管理されますが、再委託先の再請負契約先供給者は統括供給者によって管理されます。統括供給者は全ての再請負契約先供給者の名称、責任、関係を記録し、サービス提供者が利用できるようにしておきます。また、サービス提供者は統括供給者が再請負契約先供給者を管理していることの実証を得ることとします。

契約紛争の管理

サービス提供者と供給者の間で発生する、業務上の紛争を解決するプロセスを持っていることが必要です。このプロセスは紛争を記録、調査、処置、正式に終了させます。契約書の中で、プロセスの内容について定義しておきます。

契約の終了

契約管理プロセスには、供給されるサービスの終了、打ち切り、あるいは他の供給者へサービスを譲渡する場合の対処について規定しておきます。

要求事項

- 供給者管理プロセスを文書化し、責任者を任命すること。
- 供給者が提供するサービスについての詳細は、顧客との SLA と整合を取り、合意しておくこと。
- プロセス間のインタフェースは文書化し、合意しておくこと。
- 統括供給者、再請負契約先供給者に関する役割と関係を文書化すること。
- 統括供給者は、再請負契約先供給者が契約を満たすプロセスを有していることを実証できること。
- 契約・合意についてのレビューを年 1 回実施すること。
- 契約・合意の変更はレビューを経て、変更管理プロセスで行うこと。
- 紛争処理プロセスを有していること。
- サービスの終了・打ち切り・移管プロセスを有していること。
- サービスのパフォーマンスの監視プロセスを有し、改善策はサービス改善計画の入力とすること。

留意事項

- 供給者管理においても、顧客の苦情の内部処理に関する手引である“ISO 10002：組織における苦情対応のための指針”、JIS Q 10002（2005/6/20 発行）が参考となる。
- この他に、以下が審議中である。
  - ✓ ISO 10001：組織のための行動規範に関する指針
  - ✓ ISO 10003：組織外部の紛争解決に関する指針

8. 解決プロセス

8.1. 背景

解決プロセスは、大きくは、インシデント管理と問題管理の 2 つのプロセスから構成されています。

> インシデント管理と問題管理とは，密接に関連しているが，別々のプロセスである。
> （JIS Q 20000-1:2007 8.1 背景 より引用）

インシデント管理は本規格の 13 あるサービスマネジメントのプロセスの中で、唯一、リアクティブなプロセスであり、発生したインシデントによるサービスへの影響を最小限に抑えることが目的です。

一方、問題管理は、インシデント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が、インシデントの再発を防ぐというプロアクティブな活動も目的としています。

8.2. インシデント管理

インシデントの定義は、用語の解説で述べたとおり、「サービスの標準的な運用に属さないあらゆる事象であって、サービスの中断若しくはサービス品質の低下を引き起こすもの、又は引き起こす可能性があるもの」です。

> 目的：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。
> （JIS Q 20000-1:2007 8.2 インシデント管理 より引用）

解説

インシデント管理は、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ています。インシデント管理はインシデントだけでなくサービス要求も処理します。サービス要求とは、例えば、パスワードの再設定などはサービス要求として扱われます。インシデント管理プロセスは図 8-1 に示すプロセス・フローに沿って処理されます。この図はインシデント・ライフサイクルとも呼ばれています。インシデントの処理に関係するスタッフは、このフロー中の各活動が意味する所を充分に理解しておく必要があります。

インシデントの検知と記録

インシデントの検知に関しては、そのサービスを利用しているユーザである場合が多いでしょうが、その他にもインシデントを検知できるケースがあります。例えば、予めシス

テムにアプリケーション等で想定される閾値(許容限界)を設定しておいて、越えた場合にインシデントとして検知することも出来ます。インシデントの報告は電話、メール等が利用されますが、直接、インシデント記録に入力することも可能です。全てのインシデントを記録することが必要です。また、インシデントは報告があった時点で記録します。このためにも、報告のルートを関係者に周知徹底させ、可能な複数の手段（電話、メール等）も確保しておくことが大切です。上記のように、システムに組み込まれた自動検知の仕組みでは、システム的にインシデント管理の仕組みに情報が書き込まれて、管理番号なども振られる仕組みを併せて構築することで、網羅性の確保、大幅な省力化が図られます。

初期の分類とサポート

検出されたインシデントに対していくつかの観点からインシデントの分類をします。例えばハードウェアとソフトウェアといった大きなカテゴリ分けから、ネットワーク、PC、アプリケーションなどの詳細なカテゴリに分けることもできます。また、インシデント管理はインシデントに対して優先度をつけます。これは、そのインシデントにより引き起こされるであろうサービスへの影響とそのサービスが持っている緊急度により決定されます。一般的に緊急度はインシデントが検知されてから、サービスが影響を受け、顧客の事業に影響を与え始めるまでの時間に基づいて設定されます。こうしてインシデントを分類した後、インシデントに対するサポートを行います。１次サポートは通常サービスデスクが行います。サポートはその機能により 2 次サポート、3 次サポート…N 次サポートと分類されます。例えば、2 次サポートは管理部門、3 次サポートは開発者や設計者などです。

調査と診断

サービスデスクだけではインシデントが SLA で合意されている時間内に解決できない場合は、別のサポートグループからより深い技術面や解決のサポートを受ける必要が出てきます。こうした、サポートの階層を、第 2 次、第 3 次、・・第 N 次などと、区分することもあります。そして、このようなサポートの組織的な連携を、エスカレーションと呼びます。SLA で合意した時間内に解決できないインシデントはエスカレーションの対象となります。エスカレーションは優先度と解決時間によって決定されます。優先度はそのインシデントにより引き起こされる事業への影響と、緊急度により決定されます。

解決と復旧

インシデントが解決され、サービスが復旧すれば、活動中のイベントや処置を含んだ対処方法をインシデント記録に残します。インシデントの解決策がワークアラウンドの場合は、変更要求を提起するケースも考えられます。

インシデントのクローズ

通常は 1 次対応者であるサービスデスクがインシデントをクローズします。この場合、

根本原因がわかっていなくて、ワークアラウンドで対処したとしても、インシデントはクローズされます。また、インシデントのクローズ前には、インシデント報告者に確認を得てからクローズします。

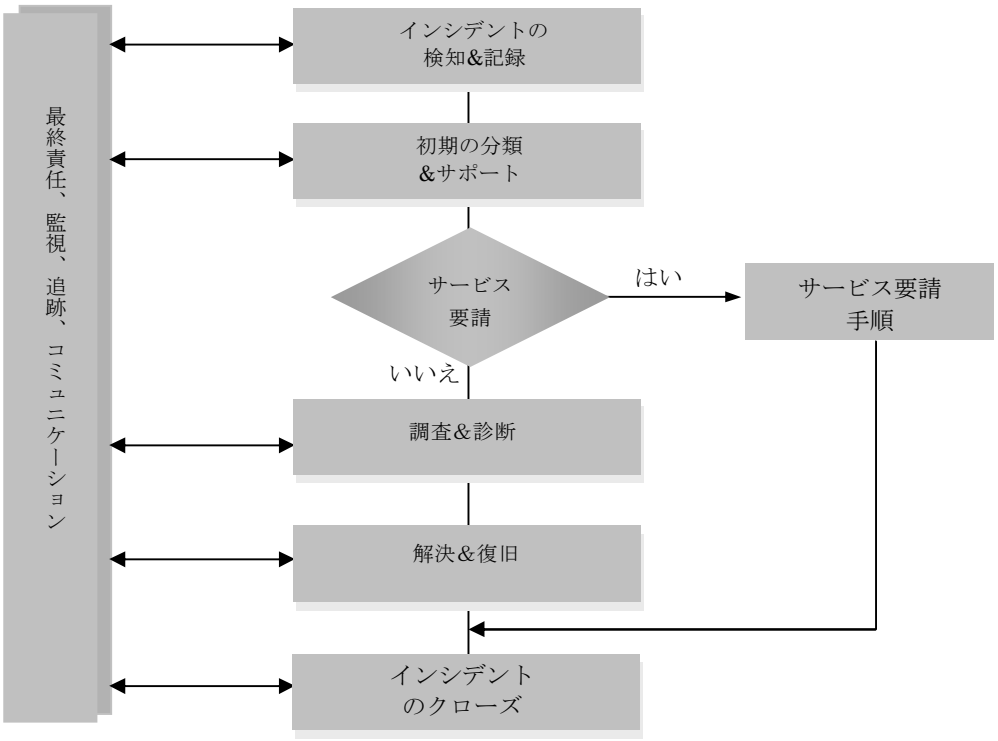


図 8-1 インシデント・ライフサイクル（出典：ITIL 書籍『サービスサポート』）

重大なインシデントへの対応

インシデントのライフサイクルで全てのインシデントに対応できない場合があります。ユーザに対して深刻な影響があり、現場の混乱が度を越しているようなケースでは、インシデント管理では特別な手順を取ります。IT サービスを提供している関係者を招集し、善後策を検討してゆきます。関係者は社内とベンダのサポートスタッフ、IT サービス・マネージャ、サービスデスクの代表者等です。対策と活動を記録し、インシデントの一部として記録に残します。

要求事項

- インシデントの影響を管理する手順を用意すること。
  - ✓ 手順には、記録、優先度付け、影響度、分類、更新、エスカレーション、解決、終了の定義を含むこと。

・ インシデント（サービス要求）の進捗状況を継続的に通知すること。
・ サービスレベルや処置の合意が得られない場合は、あらかじめ警告すること。
・ インシデント管理のスタッフは、全ての関連情報にアクセスできること。
・ 重大インシデントに関するプロセスを有していること。

留意事項

・ サービスデスク機能との連携が本規格では触れられていませんが、ITIL を参考にインタフェースを整備する必要があります。

8.3. 問題管理

問題管理はインシデントを引き起こした根本原因を特定するリアクティブな活動と、インシデントが発生する前に問題を識別して、解決するという事前予防的な活動の二つの側面を持っています。

> 目的：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。
>
> （JIS Q 20000-1:2007 8.3 問題管理 より引用）

解説

インシデントを引き起こす、未知の原因を問題と定義しています。原因が認識され、対策あるいはワークアラウンドが特定されると、問題は既知の誤りとなります。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 の問題管理では、問題コントロールとエラー・コントロールの 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。問題コントロールの活動は問題の識別と調査を行います。問題を既知の誤りにすることが問題コントロールの目的です。リアクティブな活動であり、図 8-2 に示すように、幾つかのフェーズからなり、目的は問題の根本的な原因を突き止めることにあります。根本的な原因が発見され、ワークアラウンドが特定されると、問題は、既知の誤りとなります。既知の誤りはエラー・コントロールの活動に引き継がれます。エラー・コントロールとは、問題コントロールから引き継いだ、既知の誤りが解決されるまでの関連する活動です。エラー・コントロールでは変更管理プロセスに対して変更要求（RFC）を出し、変更実装後の導入後のレビュー（PIR）で変更を評価します。エラー・コントロールの活動を図 8-3 に示します。本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るでしょう。本規格では予防処置を取ることを要求しています。

問題と既知の誤りをインシデント発生前に識別し、解決することが予防処置の活動です。インシデントと問題の分析レポートを利用して、トレンド分析を行うことで、「壊れやすい」コンポーネントを識別することが可能になります。これには、変更後に発生する特定のタイプの問題、特定タイプの故障の前兆、特定のタイプもしくは個々の項目で再発する問題、顧客トレーニングの強化もしくは文書の改良の必要性などが含まれています。

要求事項の中に、“問題解決の有効性を監視、レビュー、及び報告しなければならない。”とありますが、これはプロセス管理における一般的な概念でもあります。ITIL の問題管理では、監視、レビュー、及び報告に対して、明確に記述している部分は少なく、サービスサポートの問題管理の章「6.10 測定基準」が相当すると思われますが、充分な内容となっていません。

本規格の 4.3 章にある監視、測定及びレビューの要求事項と併せて検討すると良いでしょう。

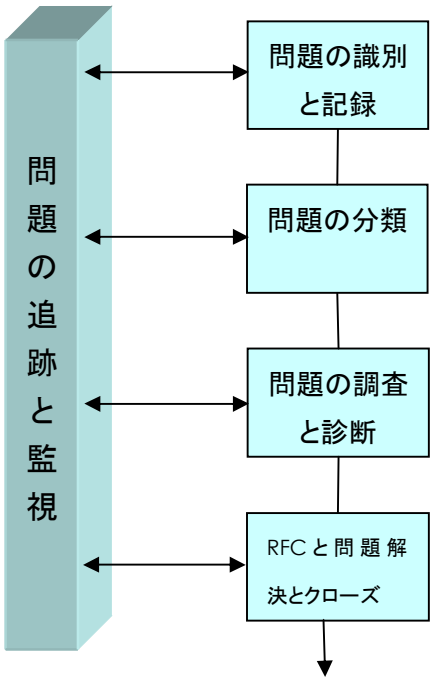


図 8-2 問題コントロール（出典：ITIL 書籍『サービスサポート』）

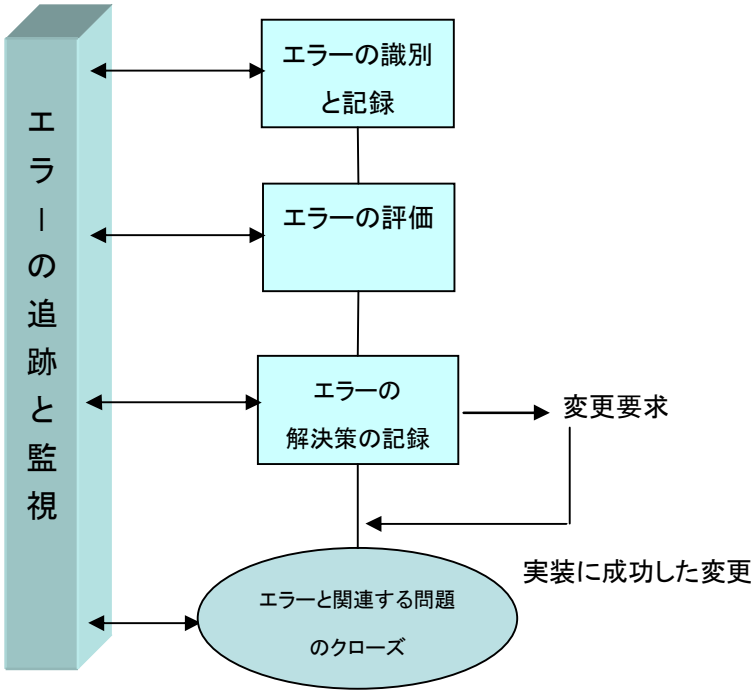


図 8-3 エラー・コントロール（出典：ITIL 書籍『サービスサポート』）

要求事項

- 問題は全て記録すること。
- インシデント・問題の影響を識別し、影響の最小化または回避する手順を用意すること。
  - ✓ 手順には、問題の記録、分類、更新、エスカレーション、解決、終了の定義を含むこと。
- 予防処置をとること。
- 問題の根本原因を修正する変更は、変更管理プロセスで行うこと。
- 問題解決の有効性を監視・レビュー・報告すること。
- 既知の誤り・是正情報を利用可能とすること。
- 改善策を記録し、サービス改善計画に入力すること。

留意事項

- 回避策は ITIL でワークアラウンドと呼ばれています。
- 根本原因が究明されるか回避策が見つかった問題は、既知の誤りと呼ばれます。
- 問題が発生した後にとるリアクティブな処理だけでなく、問題を事前予防的に発生させないためのプロアクティブな活動が重要です。

9. 統合的制御プロセス

9.1. 構成管理

構成管理プロセスとは、品質の高いITサービスを効率的・効果的に提供するために、ビジネスに影響を与える可能性があり、管理すべきと判断した構成品目（CI）であるサービスやインフラストラクチャを管理するプロセスです。そして、これらの信頼できる最新情報を他のプロセスに提供し、他のプロセスの活動を支援します。この構成管理プロセスによって、ビジネスをサポートするために必要な全てのIT資産などが把握できるようになります。

目的：サービス及びインフラストラクチャのコンポーネントを定義し，制御し，かつ，正確な構成情報を維持するため。 （JIS Q 20000-1:2007 9.1 構成管理 より引用）

解説

構成管理プロセスは、サービス及びインフラストラクチャの構成品目（CI）を管理するプロセスです。構成管理プロセスが提供する構成情報を活用して、他のプロセスはそれぞれの活動を確実に実施します。構成管理プロセスは他のプロセスの活動を支援します。

構成品目とはビジネスにおいて管理すべき要素のことであり、ハードウェア、ソフトウェア、文書などがあります。構成管理プロセスは、組織が所有するIT資産を正確に把握し、組織が許可していない構成品目の使用を防止することを目指します。また、正確な構成情報を維持するために、構成品目が実際の状況と一致しているかチェックが必要です。

構成品目（CI）の例をいくつか紹介します。

- ソフトウェアと関連する文書（要求仕様書、設計書、リリース文書）など
- 標準ハードウェアやセキュリティコンポーネント（ファイアウォール）など
- サービス関連文書（SLA、契約書）など

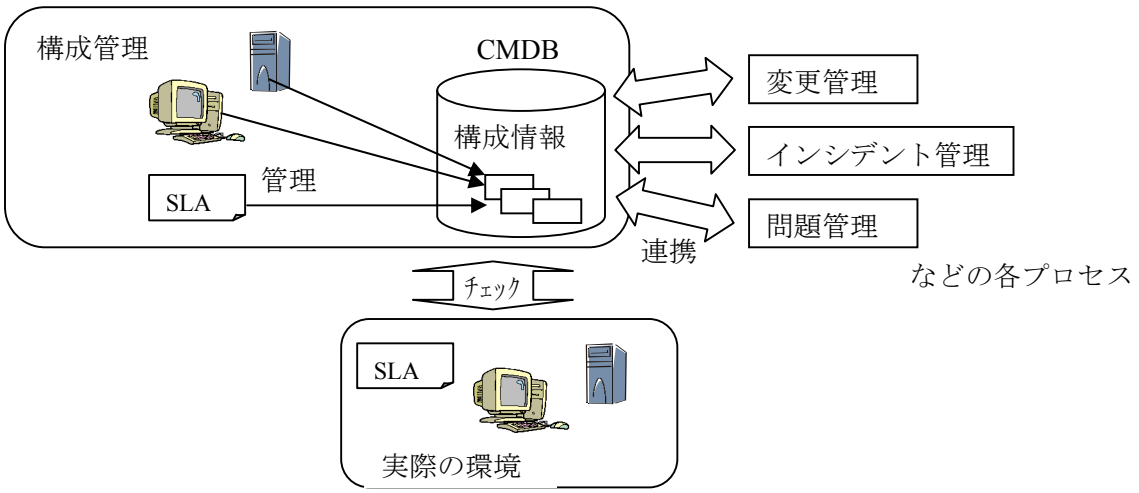


図 9-1　構成管理の概要

構成管理の活動は以下のとおりです。

- 構成管理の計画及び導入
- 構成識別
- 構成コントロール
- 構成ステータスの説明及び報告
- 構成の検証及び監査

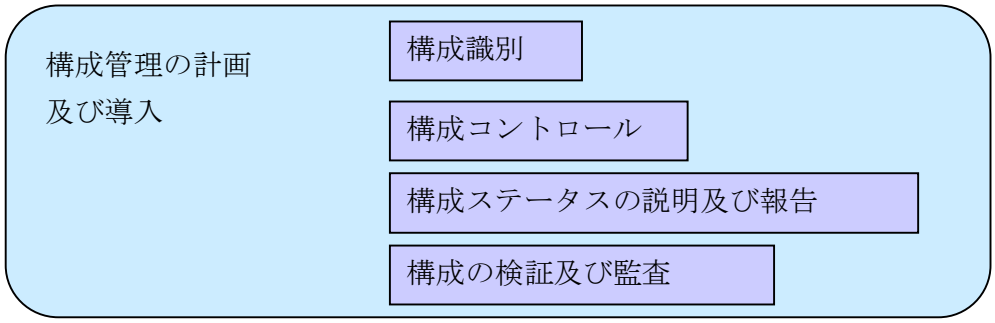


図 9-2　構成管理の活動

構成管理の計画及び導入

構成管理の目的、適用範囲、達成目標、ポリシーと手順、組織的要素と技術的要素を考慮した計画を立案し、定義づけを行います。例えば、「構成の検証及び監査」の実施タイミングや「構成ステータスの説明及び報告」の報告頻度、報告内容などもこの活動で決定します。計画は、なるべくシンプルにし、常に必要な最新情報が提供できるようにしましょう。

構成識別

CI を効果的にコントロールし、記録、報告するために、ビジネスが必要とするレベルで全ての CI を一意に識別します。どこまでを構成管理でコントロールする範囲・レベルとするかを決定する活動で、変更管理で扱う最小単位に影響するため、CI の分解レベルは変更が起こるレベルと一致させる必要があります。また、管理する CI の属性情報が多すぎる・詳細すぎると工数・コストに大きく影響します。その CI にとって本当に必要な情報のみ管理対象としましょう。

構成コントロール

許可された CI のみを CMDB 上に記録します。そのため、「許可」をコントロールする変更管理との連携が大変重要になります。CI の情報を管理する CMDB を常に最新状態に更新し、他のプロセスに情報を提供します。

CMDB を最新状態に更新するために、例えば以下のタイミングで本活動が必要になります。

- 新規 CI の登録
- 既存 CI の更新・廃棄
- RFC と関連する CI のステータス情報

など

構成ステータスの説明及び報告

それぞれの CI のライフサイクル全体を管理します。CI のステータスに関する履歴データを記録し、報告することでソフトウェアの変更などを追跡できるようにします。

また、この活動はリリース管理の活動をサポートします。

構成の検証及び監査

物理的に存在する CI が、CMDB に記録されている内容と一致しているかどうかをレビューし、監査します。CMDB の CI 情報と実際の状態が一致していない場合、その CI 情報を利用している他のプロセスに大きな影響を与える可能性があるため、CMDB が常に最新の状態であることをこの活動によって確認します。

例えば、大規模なリリースを実施する前には、この活動を実施し CMDB の整合性を確認します。その他、災害復旧後や重大な変更後などにも、実施します。そして、定期的なタイミング、不定期なタイミングでも実施しましょう。特に不定期なタイミングで実施することで、この活動を迂回していないかどうかがチェックできます。

検証と監査の結果、一致していない情報が確認できた場合には、対処手順に従い処置を行います。

要求事項

- 変更管理プロセスと連携し、構成品目の変更に対する CMDB への反映を確実にする手順を作成すること。
- 財務資産の会計業務プロセスとのインタフェースを定義すること。
- 構成品目（CI）とそのコンポーネントの定義に関するポリシーの設定し文書化すること。
- それぞれの構成品目（CI）に関する記録すべき情報を、効果的なサービスマネジメントに必要な関係と文書も含め定義し文書化すること。
- 構成管理は、サービス及びインフラストラクチャの識別可能なコンポーネントのバージョンを識別、コントロールし追跡するための仕組みを提供する。ビジネスニーズ、失敗のリスク、サービスの重要性に見合うコントロールを行うこと。
- 構成管理は、要求されたサービス及びインフラストラクチャの構成に関する変更の影響に関する情報を、変更管理プロセスに提供する。構成品目（CI）に対する変更（例えば、ソフトウェアやハードウェアの変更や移動）は、追跡可能とし、必要に応じて監査できること。
- 構成のコントロールの手順は、システム、サービス及びサービスコンポーネントの完全性（正確であり、完全であること）を確実にするために手順化（文書化）し、確実に順守すること。
- 構成品目（CI）のベースラインは、稼働環境へリリースする前に決定すること。
- ソフトウェアやテスト製品、サポート文書などの電子的構成品目（CI）のマスターコピーは、セキュリティが保たれた保管庫（確定版ソフトウェアの保管庫（DSL））で管理すること。このマスターコピーの構成記録が追跡可能であること。
- 全ての構成品目（CI）は一意に識別でき、更新アクセスが厳重にコントロールされた CMDB に記録されること。信頼性と正確性を確実にするために、管理し、検証すること。構成品目（CI）の、バージョン、場所、関連する変更及び問題、関連文書のステータスは可視化できること。
- 構成監査の手順には、結果の記録方法、是正処置の対処方法、成果に関する報告を含むこと。

留意事項

- 構成管理プロセスは変更管理プロセス、リリース管理プロセスと連携することで、IT 資産や構成を効果的に管理できるようになります。構成管理プロセスの成果は関連プロセスとの連携に大きく影響されますのでご注意ください。
- ソフトウェアに関する手引きとして、ISO/IEC 19770-1(ソフトウェア資産管理のプロセス)が参考になります。
- CI となる文書は、フォーマルなものであり、構成品目（CI）として登録・管理しているサービスやインフラストラクチャに影響する文書が構成品目（CI）となります。全

ての文書が構成品目（CI）となるわけではありません。そして、これら構成品目（CI）として登録した文書は文書のライフサイクルで管理できます。

9.2. 変更管理

変更管理プロセスは、全ての構成品目（CI）の変更を管理・コントロールするプロセスです。そのために、全ての変更に標準プロセスや手順を用います。そして、変更が原因で発生するインシデントによるサービス品質へのインパクトを極力抑えます。

目的：すべての変更を，制御された方法で，アセスメント，承認，実装及びレビューすることを確実にするため。 （JIS Q 20000-1:2007 9.2 変更管理 より引用）

解説

変更管理プロセスは、構成品目（CI）の全ての変更を効率的かつ迅速に取り扱うための標準化された方法、手順を確立し、変更に起因するインシデントがサービス品質へおよぼす影響を最小限にします。

IT インフラストラクチャなへ変更は、以下の場合に発生します。

- 問題を解決するため
- 法律改正に対応するため
- 効率性改善のため
- 有効性改善のため
- サービス改善のため

など

そして、変更した後に、インシデントが発生する場合が多いことも周知の事実です。だからこそ、変更管理プロセスがそれら全ての変更を管理・コントロールすることで、変更が原因で発生するインシデントを抑えるのです。この活動により、日々の運用が改善できます。

また、変更には、通常の変更、緊急変更、標準的な変更など、様々なパターンがあります。そしてそれぞれに手順が異なります。変更のパターンに応じた手順を準備しましょう。

緊急変更とは、早急に対処しなくてはならない変更のことであり、迅速にその変更処理に対応します。緊急変更が発生すると、その作業に対応するためリソースを割り当てるため、その他の変更に関する作業が中断してしまう場合があります。よって、なるべく緊急変更が発生しないようにしましょう。

標準的な変更とは、あらかじめ決まった手順で処置できる変更のことであり、事前に変更の手順を準備し対応します。標準的な変更のパターンを多数用意することで、効率的かつ確実な変更が行えます。

変更に対して、評価、認可、実装、レビューを確実に行うためにコントロールされた方法・手順を作成します。

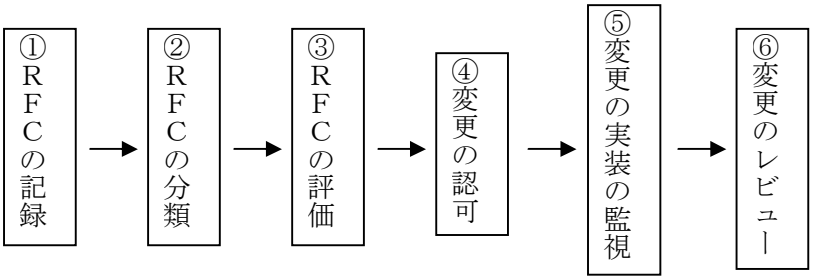


図 9-3　変更管理の活動

ITIL における変更管理の活動は以下のとおりです。

①RFC の記録（RFC の登録とフィルタリング）

受け付けた RFC は全て記録します。記録する項目（必須項目、オプション）については、事前に決定しておきます。変更管理で取り扱う変更の最小単位は、構成品目（CI）毎です。必須記録項目の例としては、RFC に関連する構成品目（CI）情報があります。

②RFC の分類（優先度の割り当て、変更のカテゴリ化）

受け付けた RFC は、インパクトと修正の緊急度に基づいて優先度を設定します。そして、IT 組織に対する変更に必要なリソースの観点から、カテゴリを決定します。また、緊急変更（非常時の変更）の場合には、特別な手順を用意します。

③RFC の評価

変更がビジネスに耐えるインパクトや、変更対象の構成品目（CI）と関係する他のサービスなどへのインパクト、リリースに必要となるリソース（人、IT など）、リスク、利益などを評価します。この評価では、ビジネスと技術（IT）のそれぞれの観点から評価を行います。

④変更の認可

変更諮問委員会（変更許可委員）が、変更を認可するかどうかを決定します。実装を認可された変更は全てスケジュール化します。そのスケジュールには変更の詳細と実装期日予定日などを記述します。そして、このスケジュールに関する情報は、関係者が参照できるようにすべきです。

⑤変更の実装の監視（変更の構築、テスト、実装）

変更管理は、変更の構築、テスト、実装を行うのではなく、変更をコントロールし、スケジュール通りにそれぞれの活動が実施されるよう、監視・調整・コントロールを行います。変更の構築では、失敗した変更を元に戻す／修正するための切り戻し計画も作成します。変更のテストでは、全ての変更が確実にテストされるよう、監視します。

緊急変更の場合には､テストが省略される場合もあります｡また省略されない場合でも、全ての変更をテストするのではなく緊急のテストとして項目が簡略化されます。

⑥変更のレビュー

全ての変更は、実装後にレビューし、改善すべき項目は記録をとり、関係者にフィードバックし、サービス改善の計画に反映します。レビューのポイントとしては､「顧客が満足しているか」「予期せぬ出来事が起こらなかったか」「変更がその目標を達成したか」などがあります。レビューのタイミングは、変更した構成品目（CI）の利用頻度によって異なります。

その他の活動として、変更管理の報告、分析及び処置があります。これらの活動では、記録している変更を定期的に分析します。そしてその分析結果をもとに、必要な処置を明確にし、改善活動計画に反映します。例えば、頻繁に発生する変更の種類を見つけ、その原因を突き止め頻繁に変更が発生しないよう改善を行うなどです。

要求事項

- サービス及びインフラストラクチャの変更（に対応する）範囲は、文書化し明確に定義する。
- 全ての変更要求（RFC）は記録し分類すること。分類区分は、至急、非常時、重大、軽微などが考えられる。変更要求（RFC）は、リスク、影響、ビジネス上の利点などで評価すること。
- 変更管理プロセスは、変更が失敗した場合に元に戻す、または修正する方法を用意すること。
- 変更は、認可を得た後にチェックを行い、そしてコントロールされた方法で実装すること。
- 全ての変更は、成功かどうかを確認するために（実装後に）レビューを行うこと。また、実装後に行った全ての処置についてもレビューを行うこと。
- 緊急変更の、認可と実装をコントロールするためのポリシーと手順を用意すること。
- 既にスケジュールされている変更実装の予定日をベースに、変更とリリースの実装予定を計画すること。実装の認可を得た全ての変更の詳細と実装予定日を明記したスケジュール（将来的な変更スケジュール（FSC））を維持し、関係者に伝えること。

- 変更記録を定期的に分析し、変更の増大レベル、頻発する変更の種類、新しい傾向、その他の関連情報を検知すること。変更の分析による結果や結論は記録すること。
- 変更管理プロセスで判明した改善策を記録し、サービス改善計画への入力にすること。

留意事項

- 変更管理プロセスはリリース管理プロセスと連携（分担）して変更に対応します。それぞれのプロセスの責任範囲、作業範囲を明確に定義する必要があることに留意してください。
- 変更管理プロセスが取り扱うのは、構成品目（CI）の変更に対してです。
- サービスに対する変更は「５． 新規サービス又はサービス変更の計画立案及び導入」が取り扱います。それぞれの対象範囲を明確にしておく必要があります。
- いかなる緊急変更に対しても、変更管理プロセスがコントロールすることを忘れないでください。また、その緊急変更に対応した変更手順は事前に作成しておきましょう。
- 変更要求（RFC）には、バグ修正パッチ適用や機能強化など様々なパターンがあります。
- 変更要求（RFC）を発行できる窓口を限定したほうがよい場合があります。
- 変更諮問委員会は定期的に開催し、委員会で取り扱う変更要求（RFC）については、事前に関係者に通知しましょう。この通知により関係者は、その委員会に参加するか代理者を参加させるか、参加しないかという判断ができるようになります。

10. リリースプロセス

10.1. リリース管理プロセス

リリースの定義は、「２．用語及び定義　」で述べたとおり「新規及び／又は変更された構成品目の集合であって、まとめて試験され、稼働環境へ導入されるもの」です。

目的： リリースにおける一つ以上の変更を，稼働環境に配送し，配付し，かつ，追跡するため。 （JIS Q 20000-1:2007 10.1 リリース管理プロセス より引用）

解説

リリース管理プロセスは、IT サービスにおける変更を包括的に見渡し、リリースに関するあらゆる面、すなわち技術と技術以外の視点双方を一緒に検討することを保証します。

リリース管理プロセスを導入することで大規模、もしくは重要なハードウェアやソフトウェアにおけるリリースの成功率が高まるため、事業（ビジネス）に対して提供するサービス品質を向上させることができます。稼働環境を安全に保つ、すなわち、不適切な対応に伴う誤りや作業漏れ、更に、許可されていない変更がされることを防ぐといった内部統制上重要や役割を担う活動がリリース管理プロセスです。

コントロールされる主なコンポーネントは以下の通りです。

・ 組織内で開発されたアプリケーションプログラム ・ 組織外で開発されたソフトウェア（市販ソフトウェア、顧客作成ソフトウェアを含む） ・ ユーティリティソフトウェア ・ サプライヤから提供されたシステム・ソフトウェア ・ ハードウェア及びハードウェアの仕様書 ・ 組み立て指示書と、ユーザマニュアルを含む文書 （出典：ITIL 書籍『サービスサポート』）

リリース管理活動は、以下に示す「リリース方針の策定」から「配布とインストール」までの手順からなります。

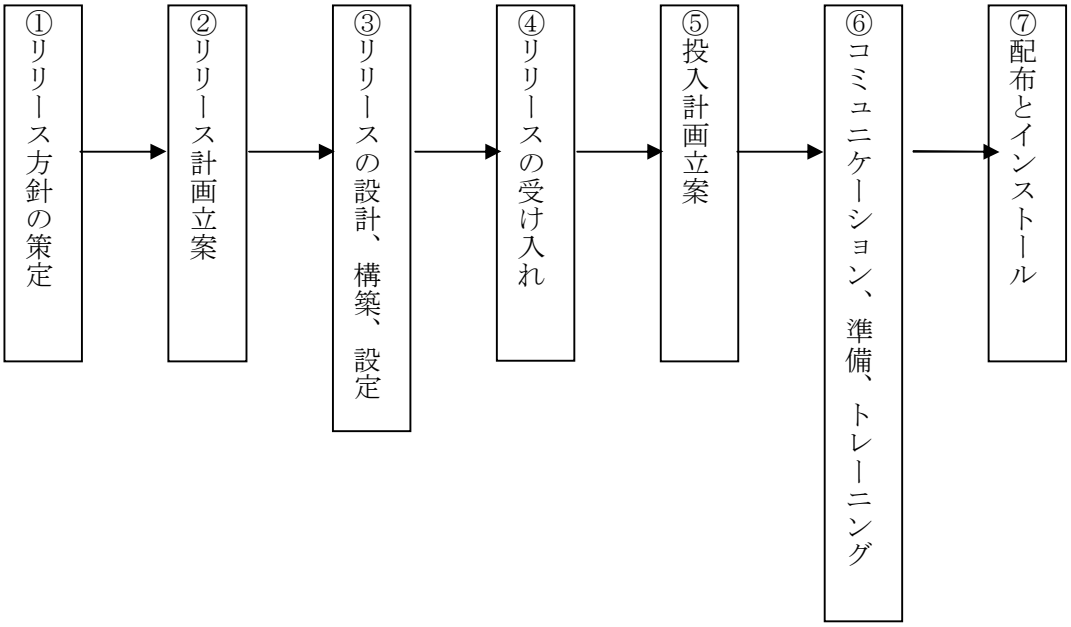


図 10-1　リリース管理の活動

① リリース方針の策定

リリース管理の役割と責任を明確にするため、リリース名称や番号付けのルール、大規模／小規模リリースの定義、緊急修正の方針、切り戻し計画の作成とテストのレベルに関する方針などを定めます。

② リリース計画立案

リリース方針にもとづいて特定リリース計画やリリースに対する概要レベルのテストと受け入れ基準を作成します。また、リリース失敗時の回復手段として切り戻し計画を作成し、リリースによる事業（ビジネス）への不要なインパクトを受けないようにします。

③ リリースの設計、構築、設定

正確な操作順序を含む詳細なリリースの構築指示書、テスト計画、インストール指示書、切り戻し手順などを作成します。社内開発コンポーネント（CI）と社外サプライヤから購入した CI では手順が異なるので、それぞれ標準的な手順を作成します。

切り戻し計画の作成は「変更管理プロセス」の責任ですが、リリース管理ではリリースに含まれる個々の変更に関する切り戻し計画が確実に行えることを確認します。

④ リリースの受け入れ

リリース全体の完全性と正確性に関して承認を得る活動です。これには「テスト」と

「リリースの承認」が含まれています。

「テスト」では、独立したスタッフによって、すべての変更に関する手順と切り戻し手順がすべてテストされます。テストの各段階では承認が必要です。

「リリースの承認」は、リリースを稼働環境に投入する前の最終受け入れ及び承認（リリース実装許可）を「変更管理プロセス」を通して行うための活動です。「変更管理プロセス」はユーザの正式な変更の受け入れと承認があることを確認します。テスト結果などによりリリースが却下される場合には「変更管理プロセス」を通じて再スケジュールします。

⑤ 投入計画立案

作成されたリリース計画を拡張して、正確なインストール手順・活動と合意済みの実装計画情報を追加します。実装計画情報により、日付、時間、誰が何を行うかを詳細化します。ユーザへの情報伝達内容を明確にし、コミュニケーション計画立案を行います。

⑥ コミュニケーション、準備、トレーニング

リリースに関する情報として、何が計画され、業務にどのような影響があるかなどを、顧客、ユーザやサービスデスクなどの関係者全員に連絡し、トレーニングを含むリリースの準備を行います。すべての関係者がリリースに関する情報を常に持っていて、リリースに対する適切な対応ができるようにします。また、ミーティングなどにより顧客やサポートスタッフとのコミュニケーションを図ります。(コミュニケーションは一般的に「サービスデスク」が行います。)

⑦ 配布とインストール

稼働環境へリリースを行います。リリース準備が整い、必要なトレーニングすべてが終了した後に実施します。

ソフトウェアの配布については、取り扱い、こん包及び配送中にソフトウェアの完全性を維持しなければなりません。ネットワーク経由でのソフトウェアの自動配布が利用できると、リソース節約、配布時間の短縮ができますが、配布後の完全性の確認も必要です。

CMDB 内の CI の情報更新を行うために「構成管理プロセス」に情報を渡します。

要求事項

- リリース方針を文書化し合意する。リリース方針には、リリース頻度や種類及びリリースの役割や責任を定義する。
- サービス提供者と顧客がいっしょに、サービス、システム、ソフトウェア及びハードウェアのリリースを計画する。投入方法に関する計画はすべての該当関係者（顧客、利用者、運用者、支援要員など）の合意及び許可を得る。
- リリースの計画ではリリースが失敗した場合の切り戻し方法又は修正方法を含める。
- リリースの計画にはリリース期日及び提出書類の記録と、関連する変更要求、既知の誤り及び問題を言及する。
- リリース管理プロセスは「インシデント管理プロセス」に適切な情報を伝えるようにする。
- アセスメントにより変更要求のリリース計画への影響を把握する。リリース手順には、変更記録の更新と変更を含める。
- 緊急リリースは緊急の「変更管理プロセス」とインタフェースを取っている定義されたプロセスに従って管理する。
- 受入れ試験環境を確立し、配布前にすべてのリリースを構築、試験する。
- ハードウェア及びソフトウェアの導入、取扱い、こん包及び発送の間その完全性が維持されるようにリリース及び配布は設計し、実施する。
- リリースの成功及び失敗を測定する。測定にはリリース後のリリースに関するインシデントを含む。
- リリースの分析には事業、情報技術運用者及び支援要員の資源に及ぼす影響のアセスメントを含む。この分析結果は、サービス改善計画に入力する。

留意事項

- リリース管理は、内部統制における IT 全般統制でも重要な位置づけにあります。本番環境に対して、不正な変更・改ざん、破壊、消滅などが行われることは財務報告の信頼性を損なう重大な問題を引き起こす可能性が高いからです。「職務分離」ということで、コンポーネントの作成、変更を行う者と、本番環境へのリリースを行う者を分けるのは、これらのリスクのコントロールとして有効です。

参考文献

規格

1) JIS Q 9000:2006 品質マネジメントシステムー基本及び用語
(ISO 9000:2005, Quality management systems－Fundamentals and vocabulary)

2) JIS Q 9001:2000 品質マネジメントシステムー要求事項
(ISO 9001:2000, Quality management systems－Requirements)

3) JIS Q 20000-2:2007 情報技術ーサービスマネジメントー第 2 部：実践のための規範
(ISO/IEC 20000-2:2005, Information technology－Service management－Part 2: Code of practice)

4) JIS Q 27002:2006 情報技術―セキュリティ技術―情報セキュリティマネジメントの実践のための規範(ISO/IEC 17799:2005, Information technology － Security techniques－Code of practice for information security management)

5) JIS X 0160:1996 ソフトウェアライフサイクルプロセス
(ISO/IEC 12207:1995, Information technology－Software life cycle processes)

6) JIS X 0170:2004 システムライフサイクルプロセス
(ISO/IEC 15288:2002, Systems engineering－System life cycle processes)

7) TR X 0027:2000 プロジェクト管理に JIS X 0160 を適用するためのガイド
(ISO/IEC TR 16326:1999, Software engineering－Guide for the application of ISO/IEC 12207 to project management)

8) ISO 10007:2003 Quality management systems － Guidelines for configuration management

9) ISO/IEC TR 15271:1998 Information technology－Guide for ISO/IEC 12207 (Software Life Cycle Processes)

10) ISO/IEC 15504-1:2004 Information technology － Process assessment － Part 1: Concepts and vocabulary

11) ISO/IEC 15504-2:2003 Software engineering － Process assessment － Part 2: Performing an assessment

12) ISO/IEC 15504-3:2004 Information technology － Process assessment － Part 3: Guidance on performing an assessment

13) ISO/IEC 15504-4:2004 Information technology － Process assessment － Part 4: Guidance on use for process improvement and process capability determination

14) ISO/IEC 15504-5:2006 Information technology－Process Assessment－Part 5: An exemplar Process Assessment Model

15) ISO/IEC TR 19760:2003 Systems engineering－A guide for the application of ISO/IEC 15288 (System life cycle processes)

16) ISO/IEC 90003:2004 Software engineering－Guidelines for the application of ISO 9001:2000 to computer software

規格について

ISO（International Organization for Standardization：国際標準化機構）は、電気及び電子技術分野を除く産業分野に関する標準化機関です。IEC（International Electrotechnical Commission：国際電気標準会議）も同じく標準化機関で、電気及び電子技術分野の国際規格の作成を行っています。情報技術の分野は、これら両者に関係するとして合同専門委員会（JTC 1：Joint Technical Committee 1）によって規格化の検討が行なわれています。JTC 1 で規格化されたものは“ISO/IEC”という規格名が付けられます。略して例えば“ISO20000”と書かれることがありますが、正式には“ISO/IEC 20000”となります。ただし ISO 9000 などは JTC 1 で規定された国際標準ではないため、略号ではなく“ISO 9000”となります。

日本における国家規格として JIS（Japanese Industrial Standard：日本工業規格）は、工業標準化法に基づいて、全ての工業製品に関して規定されます。規格名の“JIS”に続く 1 文字は、その規格の分野を示しており、例えば以下のようになります。

- 情報処理：JIS X xxxxx
- 管理システム：JIS Q xxxxx

また ISO/IEC も JIS も、どの版であるかを示すため、設定年あるいは改訂年が添えられています。（例：ISO/IEC 20000-1:2005、JIS Q 20000:2007）

ISO/IEC 20000-1 で参照されている文献について、関連する規格ごとに分類し、簡単な解説を記載します。

品質マネジメントに関連した規格

1) JIS Q 9000:2006　品質マネジメントシステム－基本及び用語
(ISO 9000:2005, Quality management systems－Fundamentals and vocabulary)

2) JIS Q 9001:2000　品質マネジメントシステム－要求事項
(ISO 9001:2000, Quality management systems－Requirements)

16) ISO/IEC 90003:2004　Software engineering－Guidelines for the application of ISO 9001:2000 to computer software

ベンダが提供する製品について一定以上の品質が確保されるためには､顧客の視点から､しかるべきマネジメントシステムが構築されているはずであろうという期待があります。ISO9000 シリーズは、品質マネジメントシステムに関する国際標準であり、ISO 9001 は品質マネジメントシステムについての要求事項が記述されています。内容は、マネジメントシステム自身に対する要求、責任者が果たすべき責任、確保されなければならない資源の

管理、製造、マネジメントシステムの監視・測定といったものが網羅されています。

ISO/IEC TR 90003 は，ISO 9001 の要求事項をソフトウェア開発、供給及び保守の分野に適用する際に ISO 9001 の要求事項をどのように読み替えればよいのかについての指針を示したものです。

なおソフトウェアのライフサイクルについては JIS X 0160（ISO/IEC 12207）に、ソフトウェアを含むシステム全体のライフサイクルについては JIS X 0170（ISO/IEC 15288）に記述があります。

IT サービスマネジメントに関連した規格

3) 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(ISO/IEC 20000-2:2005, Information technology－Service management－Part 2: Code of practice)

JIS Q 20000-1:2007 情報技術－サービスマネジメント－第 1 部：仕様(ISO/IEC 20000-1:2005, Information technology－Service management－Part 1: Specification)が ITSMS に対する要求事項を記載しているのに対し、JIS Q 20000-2 は JIS Q 20000-1 の要求事項の範囲に限定した ITSMS の推奨項目を記述しています。JIS Q 20000-1 の要求事項を満たすために、JIS Q 20000-2 に書かれている内容をすべて実装する必要はありません。逆に JIS Q 20000-2 が実装できていれば、JIS Q 20000-1 の要求事項を満たしているということが期待できます。

ITIL は、IT サービスマネジメントに関するベストプラクティスであると言われています。包含関係で言えば ITIL のもつ広がりが一番大きく、JIS Q 20000-1 は ITIL の網羅範囲を最も絞り込んだエッセンスであり、それ故に「要求事項」と呼ばれます。JIS Q 20000-2 は、JIS Q 20000-1 のためのベストプラクティスです。

情報セキュリティマネジメントに関連した規格

4) JIS Q 27002:2006 情報技術―セキュリティ技術―情報セキュリティマネジメントの実践のための規範(ISO/IEC 17799:2005, Information technology－Security techniques－Code of practice for information security management)

JIS Q 27002 は、情報セキュリティマネジメントシステム（ISMS）に関するベストプラクティスであり、ISMS 実現のための管理策を詳説しています。ちなみに JIS Q 27001 は、ISMS に対する要求事項です。

ライフサイクルプロセスに関連した規格

システム及びソフトウェアの開発モデルの規格であり、発注者と受注者間の意思疎通のための共通言語的な意味合いを持っています。

ソフトウェアライフサイクルプロセス

5) JIS X 0160:1996　ソフトウェアライフサイクルプロセス
(ISO/IEC 12207:1995, Information technology－Software life cycle processes)

7) TR X 0027:2000　プロジェクト管理に JIS X 0160 を適用するためのガイド
(ISO/IEC TR 16326:1999, Software engineering－Guide for the application of ISO/IEC 12207 to project management)

9) ISO/IEC TR 15271:1998　Information technology－Guide for ISO/IEC 12207 (Software Life Cycle Processes)

ISO/IEC 12207 はソフトウェアの取得、供給、開発、運用、保守のプロセスを主に、これを支援するライフサイクルプロセスと組織に対するライフサイクルプロセスに関する推奨事項を記述したものです。

TR X 0027 は、JIS X 0160 のマネジメントプロセスをソフトウェアプロジェクトマネジメントへ適用する際のガイドラインです。

ISO/IEC 12207 はソフトウェア開発に必要なプロセス･アクティビティを定めていますが、実際の適用に関する記述(時間軸に沿った実行の順序など)については記述していません。そのためプロジェクトへの適用の際には、組織やプロジェクトごとに規定していく必要があります。ISO/IEC TR 15271:1998 では、Annex C に 3 つのライフサイクルモデル（“Waterfall”“Incremental”“Evolutionary”）とその組み合わせ（“Hybrid”）を紹介し、ISO/IEC 12207 適用のガイドとなっています。

なお TR X 0027 や ISO/IEC TR 16326 に現れる“TR”とは、”Technical Report”の略です。標準報告書と呼ばれ、JIS や ISO ではないが標準に関連している情報類（標準化関連情報、データ集など）を指します。

「共通フレーム 98　SLCP-JCF98」は、ソフトウェア（システム）の開発及び取引の明確化を目的として、JIS X 0160 と整合をとりつつ規定された日本における標準です。JIS X 0160 とともに役に立つ資料として特記したいと思います。

参考：http://www.meti.go.jp/policy/it_policy/si_so/si98.pdf

システムライフサイクルプロセス

6) JIS X 0170:2004 システムライフサイクルプロセス(ISO/IEC 15288:2002, Systems engineering－System life cycle processes)

15) ISO/IEC TR 19760:2003 Systems engineering－A guide for the application of ISO/IEC 15288 (System life cycle processes)

JIS X 0170 は、JIS X 0160（ソフトウェアライフサイクルプロセス）をシステムに拡張したものです。システムのライフサイクルを記述するための共通の枠組み、プロセスを規定しています。

ISO/IEC TR 19760 は、ISO/IEC 15288 をシステム及びプロジェクトへ適用する際のガイドラインです。

構成管理に関連した規格

8) ISO 10007:2003 Quality management systems－Guidelines for configuration management

ISO 10007 は、組織における構成管理の使用に関する方針を規定しており、製品の構想から処分までに適用されます。内容は責任及び権限のほか、構成管理プロセスとして構成管理計画、構成識別、変更管理、構成状況会計、構成監査について記載しています。

プロセスアセスメントに関連した規格

10) ISO/IEC 15504-1:2004 Information technology－Process assessment－Part 1: Concepts and vocabulary

11) ISO/IEC 15504-2:2003 Software engineering－Process assessment－Part 2: Performing an assessment

12) ISO/IEC 15504-3:2004 Information technology－Process assessment－Part 3: Guidance on performing an assessment

13) ISO/IEC 15504-4:2004 Information technology－Process assessment－Part 4: Guidance on use for process improvement and process capability determination

14) ISO/IEC 15504-5:2006 Information technology－Process Assessment－Part 5: An exemplar Process Assessment Model

ISO/IEC 15504 は、CMM などの各種アセスメントモデルを統合して規格化した、ソフトウェア開発における品質・信頼性、生産性などに関するプロセスレベルを評価する手法についての規定です。

本ユーザーズガイドの参考文献

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.jp/doc/uguide/ugall.pdf
  情報セキュリティマネジメントシステム構築方法

ITIL 関連

- ITIL 書籍『サービスサポート』（TSO 刊）
- ITIL 書籍『サービスデリバリ』（TSO 刊）
- ITIL 書籍『サービスマネジメント導入計画立案』（TSO 刊）
- ITIL 書籍『ビジネスの観点 サービス提供における IS からの視点』（TSO 刊）
- ITIL 書籍『アプリケーション管理』（TSO 刊）
- ITIL 書籍『ICT インフラストラクチャ管理』（TSO 刊）
- ITIL 書籍『ITIL 入門』（TSO 刊）

SLA 関連

- 『情報システムに係る政府調達への SLA 導入ガイドライン』（情報処理推進機構）
  http://www.meti.go.jp/policy/it_policy/tyoutatu/sla-guideline.pdf
- 『公共 IT におけるアウトソーシングに関するガイドライン』（総務省）
  http://www.lasdec.nippon-net.ne.jp/rdd/OS-guide/OS-guide-sum.pdf
  http://www.lasdec.nippon-net.ne.jp/rdd/OS-guide/OS-guide.pdf
- 『民間向け IT システムの SLA ガイドライン』　JEITA・ソリューションサービス事業委員会 編著（日経 BP 社 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®は、英国、欧州連合各国、及び米国における英国政府 Office of Government Commerce の登録商標であり、共同体商標です。
- “COBIT”と COBIT のロゴは、米国及びその他の国で登録された 情報システムコントロール財団（Information Systems Audit and Control Foundation, 本部：米国イリノイ州）及び IT ガバナンス協会（IT Governance Institute 本部：米国イリノイ州）の商標（trademark）です。COBIT ®の内容に関する記述は、情報システムコントロール財団及び IT ガバナンス協会に著作権があります。
- 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。

付録 A 内部統制を実現するための JIS Q 20000 の活用の仕方

付録 A.1 財務報告に係る内部統制の評価及び監査の制度の概要

「証券取引法等の一部を改正する法律」が 2006 年 6 月 7 日に成立し、証券取引法は金融商品取引法としてより幅広いリスク商品を対象とすることとなりました。この金融商品取引法では、財務報告に係る内部統制の評価及び監査の制度が規定されています。この制度が規定された背景には、粉飾決算を含む有価証券報告書の虚偽記載等の事件が続き、適正な証券市場の確保のために開示情報の適正性の確保が重要と認識されたことがあります。

財務報告に係る内部統制の評価及び監査制度の法制化をにらみながら、金融庁は 2005 年 2 月に企業会計審議会に内部統制部会を設置し、財務報告に係る内部統制の評価及び監査の制度の枠組み及び経営者評価及び監査の基準等の検討を行いました。約 10 ヶ月に及ぶ検討の結果、内部統制部会は、2005 年 12 月に「財務報告に係る内部統制の評価及び監査の基準のあり方について」を公表し、財務報告に係る内部統制の評価及び監査の制度の枠組みと基準案を示しました。その後、この制度を実務に適用するための詳細な規定である実施基準の策定に向けて作業ワーキングを設置し、検討を重ねました。約 1 年にわたる検討の結果、2007 年 2 月に「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の設定について（意見書）」を公表しました。この意見書では、財務報告に係る内部統制の評価及び監査の基準（以下、「内部統制基準」という）と財務報告に係る内部統制の評価及び監査の実施基準（以下、「内部統制実施基準」という）が示されています。

この財務報告に係る内部統制の評価及び監査の制度では上場企業等は、財務報告に係る内部統制の整備状況及び運用状況の有効性を評価し、その結果を内部統制報告書として公表し、監査人がその内部統制報告書の内容の適正性についての意見表明を行うことになっています。なお、この制度は、上場企業等の財務情報の信頼性の確保を目的にしているため、経営者の評価及び監査人の監査の対象となる内部統制は財務情報の信頼性に関係する部分のみとなります。

参考　金融商品取引法

第 24 条の 4 の 4
第二十四条の四の四第二十四条第一項の規定による有価証券報告書を提出しなければならない会社（第二十三条の三第四項の規定により当該有価証券報告書を提出した会社を含む。次項において同じ。）のうち、第二十四条第一項第一号に掲げる有価証券の発行者である会社その他の政令で定めるものは、事業年度ごとに、当該会社の属する企業集団及び当該会社に係る財務計算に関する書類その他の情報の適正性を確保するために必要なものとして内閣府令で定める体制について、内閣府令で定めるところにより評価した報告書（以下「内部統制報告書」という。）を有価証券報告書（同条第八項の規定により同項に規定する有価証券報告書等に代えて外国会社報告書を提出する場合にあっては、当該外国会社報告書）と併せて内閣総理大臣に提出しなければならない。

第 193 条の 2 第 2 項
金融商品取引所に上場されている有価証券の発行会社その他の者で政令で定めるものが、この法律の規定により提出する貸借対照表、損益計算書その他の財務計算に関する書類で内閣府令で定めるものには、その者と特別の利害関係のない公認会計士又は監査法人の監査証明を受けなければならない。ただし、監査証明を受けなくても公益又は投資者保護に欠けることがないものとして内閣府令で定めるところにより内閣総理大臣の承認を受けた場合は、この限りでない。

付録 A.2　内部統制と IT への対応

マネジメントプロセスと内部統制

内部統制基準による内部統制の定義。

内部統制とは、基本的に、業務の有効性及び効率性、財務報告の信頼性、事業活動に関わる法令等の遵守並びに資産の保全の４つの目的が達成されているとの合理的な保証を得るために、業務に組み込まれ、組織内のすべての者によって遂行されるプロセスをいい、統制環境、リスクの評価と対応、統制活動、情報と伝達、モニタリング（監視活動）及び IT（情報技術）への対応の６つの基本的要素から構成される。

内部統制はマネジメントプロセスの一部です。内部統制基準によれば、内部統制が達成しようとする目的は、

- 業務の有効性及び効率性
- 財務報告の信頼性
- 事業活動に関わる法令等の遵守
- 資産の保全

の 4 つです。このうち、金融商品取引法により評価及び監査の対象となるのは財務報告の信頼性という目的を達成するための内部統制です。

これらの目的が達成されていることを合理的に保証するために、業務に組み込まれ、組織内のすべての者によって遂行されるプロセスが内部統制となります。ただし、内部統制は、マネジメントプロセス全体ではありません。マネジメントプロセス全体のうち、経営者の判断や、目的の設定、計画の立案、リスク管理そのもの、是正措置といった目的を達成するための直接的な行為は含まれないというのが一般的な考え方です。したがって、JIS Q 20000-1 により構築されるマネジメントシステムには、内部統制ではない領域も存在することになります。

なお、COSO 内部統制報告書では、マネジメントプロセスと内部統制の関係について以下のように整理しています。

	マネジメントプロセス	内部統制	関連する内部統制の構成要素
1	事業体レベルの目的の設定		
2	戦略的経営計画		
3	統制環境要因の設定	✓	統制環境
4	活動レベルの目的の設定		
5	リスクの識別と分析	✓	リスクの評価
6	リスク管理		
7	統制活動の実施	✓	統制活動
8	情報の識別，捕捉と伝達	✓	情報と伝達
9	監視活動	✓	モニタリング
10	是正措置		

内部統制の基本的要素としての IT への対応

財務諸表等の作成には、IT の活用が不可欠なことから、内部統制基準及び内部統制実施基準では、COSO 内部統制報告書で規定されている内部統制の５つの構成要素に加えて、「IT への対応」を追加しています。「IT への対応」は、内部統制の他の基本的要素と必ずしも独立に存在するものではありません。したがって、「IT への対応」と他の基本的要素との関係については、以下のとおりとなることに留意してください。

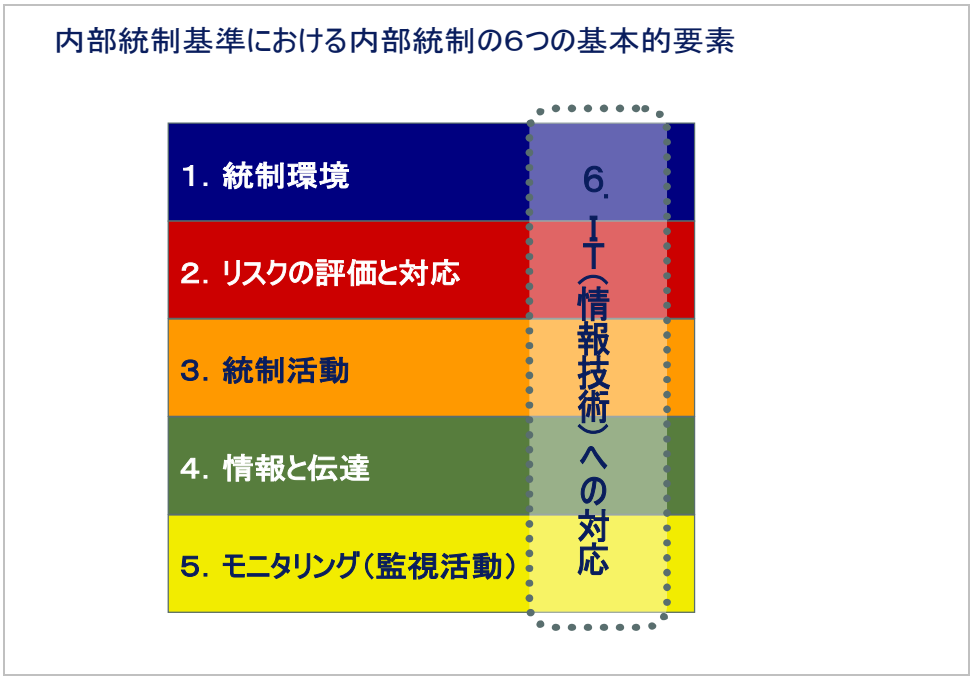


図 A-1 内部統制基準における内部統制の６つの基本的要素

さて、「IT への対応」について、その詳細をみていきましょう。「IT への対応」は、「IT 環境への対応」と「IT の利用及び統制」からなります。「IT への対応」について、内部統制基準の定義等を整理し示すと以下の図のようになります。

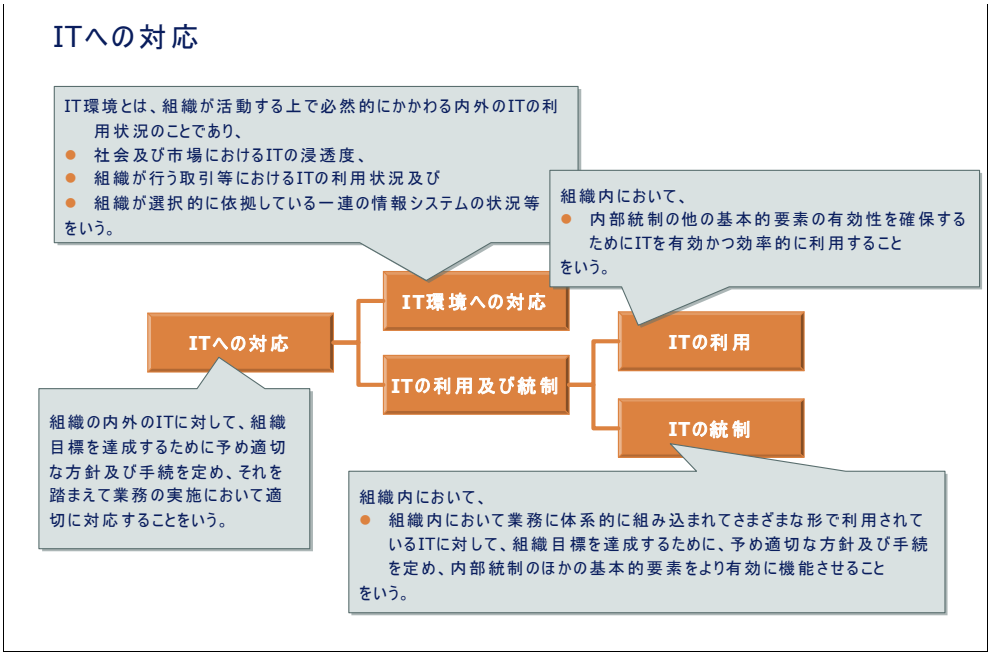


図 A-2 IT への対応

「IT の統制」はさらに、IT を利用した統制である IT に係る業務処理統制（以下、「IT 業務処理統制」という）と IT 業務処理統制を含む IT 業務処理が適切に機能することを保証する IT に係る全般統制（以下、「IT 全般統制」という）に分類されます。IT 業務処理統制と IT 全般統制の説明を示すと以下の図のようになります。

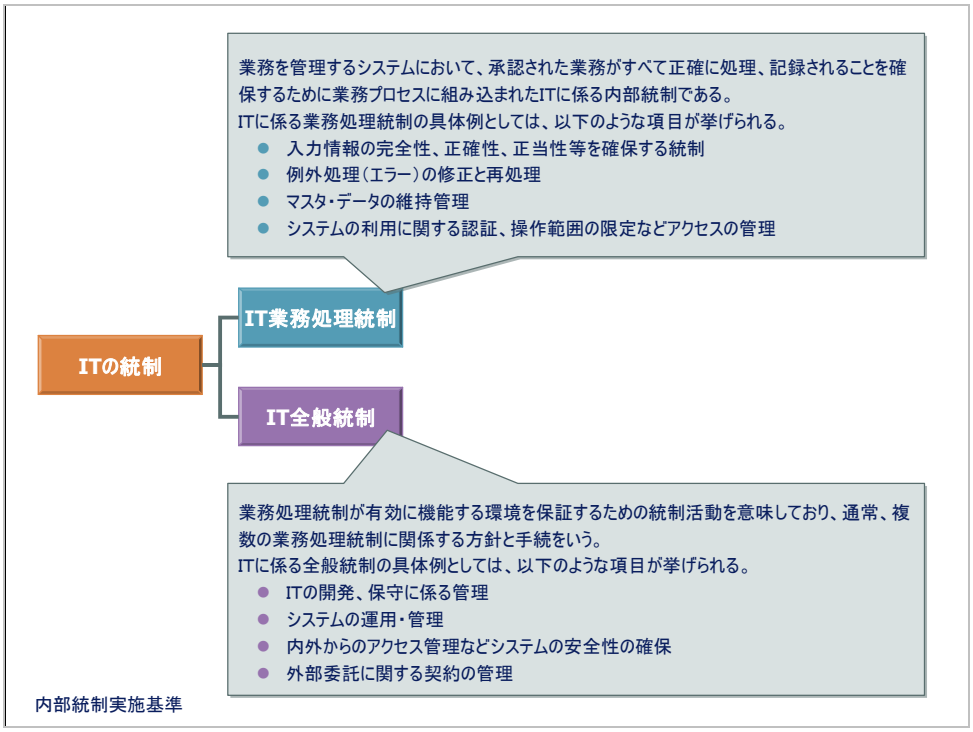


図 A-3 IT 業務処理統制と IT 全般統制

IT 全般統制

ここでは、さらに内部統制実施基準にもとづいて IT 全般統制について詳細にみていきましょう。内部統制実施基準では監査人が IT 全般統制の有効性を評価する際の視点として以下の項目を挙げています。

a．システムの開発，変更・保守	監査人は、企業が財務報告に関連して、新たにシステム、ソフトウェアを開発、調達又は変更する場合、承認及び導入前の試験が適切に行われているか確認する。 その際、監査人は、例えば、以下の点に留意する。 • システム、ソフトウェアの開発、調達又は変更について、事前に経営者又は適切な管理者に所定の承認を得ていること • 開発目的に適合した適切な開発手法がシステム、ソフトウェアの開発、調達又は変更に際して、適用されていること • 新たなシステム、ソフトウェアの導入に当たり十分な試験が行われ、その結果が当該システム、ソフトウェアを利用する部門の適切な管理者及びIT部門の適切な管理者により承認されていること • 新たなシステム、ソフトウェアの開発、調達又は変更について、その過程が適切に記録及び保存されるとともに、変更の場合には、変更前のシステム、ソフトウェアに関する内部統制の整備状況に係る記録が更新されていること • 新たなシステム、ソフトウェアにデータを保管又は移行する場合に、誤謬、不正等を防止する対策が取られていること • 新たなシステム、ソフトウェアを利用するに当たって、利用者たる従業員が適切な計画に基づき、教育研修を受けていること
b．システムの運用・管理	監査人は、財務報告に係るシステムの運用・管理の有効性を確認する。その際、例えば、以下の点に留意する。 • システムを構成する重要なデータやソフトウェアについて、障害や故障等によるデータ消失等に備え、その内容を保存し、迅速な復旧を図るための対策が取られていること • システム、ソフトウェアに障害や故障等が発生した場合、障害や故障等の状況の把握、分析、解決等の対応が適切に行われていること
c．システムの安全性の確保	監査人は、企業がデータ、システム、ソフトウェア等の不正使用、改竄、破壊等を防止するために、財務報告に係る内部統制に関連するシステム、ソフトウェア等について、適切なアクセス管理等の方針を定めているか確認する。
d．外部委託に関する契約の管理	企業が財務報告に関連して、ITに係る業務を外部委託している場合、監査人は、企業が適切に外部委託に関する契約の管理を行っているか検討する。

JIS Q 20000-1 との関係で言えば、IT 全般統制のうち、「システムの開発」を除く IT 全般統制は概ね JIS Q 20000-1 にも関係してくることになりますが、財務報告に係る内部統制の評価及び監査の制度においては、財務報告に係る内部統制のみが経営者評価及び監査の範囲となることに留意しなければなりません。また、JIS Q 20000-1 の認証そのものが、直ちに財務報告に係る内部統制の評価及び監査の代替にはなりません。ただし、JIS Q 20000-1 の認証を取得することにより、経営者評価及び監査手続の軽減につながることはありえます。

付録 A.3　JIS Q 20000 を利用した IT への対応

JIS Q 20000-1 に適合したマネジメントシステムを構築することは、財務報告に係る内部統制の構築にも寄与することができます。すなわち、適用範囲とするマネジメントシステムが財務報告に係る内部統制の要求に従うことを目的とし運営することにより、財務報告に係る内部統制が有効に機能するようにすることが可能となります。

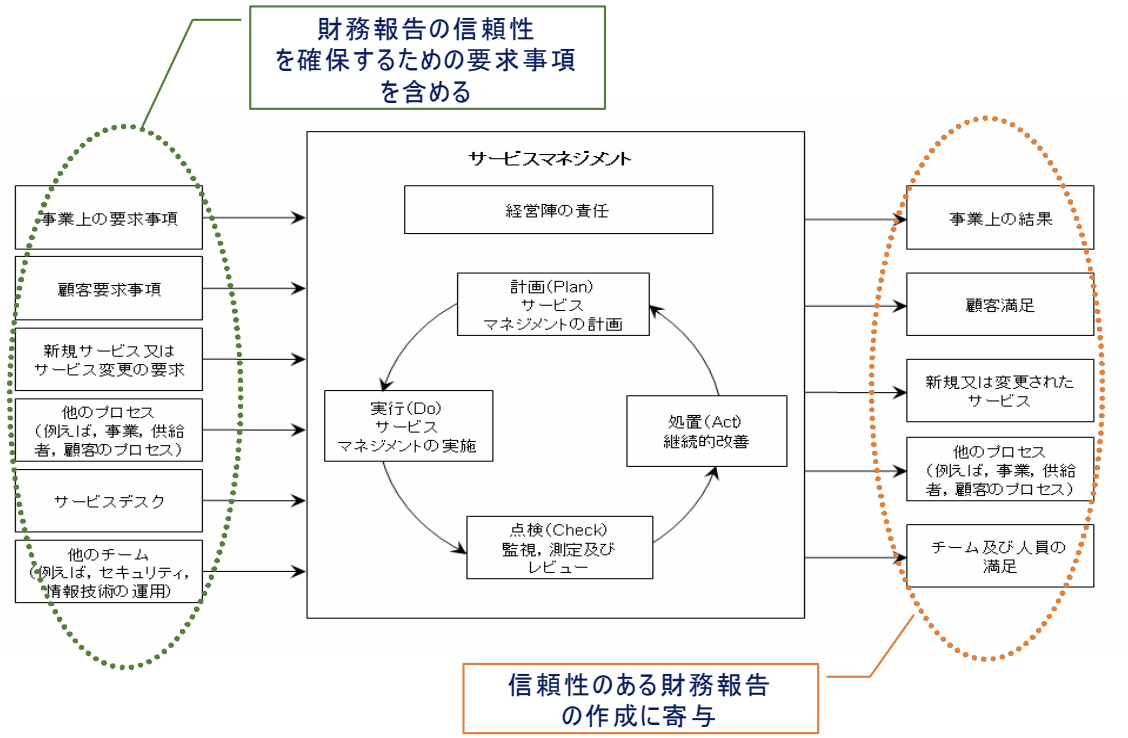


図 A-4 サービスマネジメントプロセスとの対応

以下に、JIS Q 20000-1 の要求事項の目的を抜粋します。

	目的
3 マネジメントシステム要求事項	すべてのサービスを効果的に運営管理し、かつ、実施できるようにするための方針及び枠組みを含むマネジメントシステムを提供するため。
3.1 経営陣の責任	
3.2 文書化に関する要求事項	
3.3 力量，認識及び教育・訓練	
4 サービスマネジメントの計画立案及び導入	
4.1 サービスマネジメントの計画（**Plan**）	サービスマネジメントの導入・実施について計画するため。
4.2 サービスマネジメントの実施及びサービスの提供（**Do**）	サービスマネジメントの目的及び計画を実施するため。

4.3 監視，測定及びレビュー（**Check**）	サービスマネジメントの目的及び計画の達成を、監視、測定及びレビューするため。
4.4 継続的改善（**Act**）	サービスの提供及び運営管理の有効性及び効率を改善するため。
5 新規サービス又はサービス変更の計画立案及び導入	新規サービス及びサービス変更が、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性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 IT 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、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 一般	
7.2 顧客関係管理	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、維持するため。
7.3 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 背景	
8.2 インシデント管理	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。
8.3 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	サービス及びインフラストラクチャのコンポーネントを定義し、制御し、かつ、正確な構成情報を維持するため。
9.2 変更管理	すべての変更を、制御された方法で、アセスメント、承認、実装及びレビューすることを確実にするため。
10 リリースプロセス	
10.1 リリース管理プロセス	リリースにおける一つ以上の変更を、稼働環境に配送し、配付し、かつ、追跡するため。

JIS Q 20000-1 の要求事項はマネジメントシステムに関する要求事項と具体的な統制に関する要求事項の２つに大きくわけることができます。これを JISQ 20000-1 の要求事項の項番と対比させると次のようになります。

要求事項の種別	要求事項の項番
マネジメントシステムに関する要求事項	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
統制に関する要求事項	6 サービス提供プロセス
	7 関係プロセス
	8 解決プロセス
	9 統合的制御プロセス
	10 リリースプロセス

「3 マネジメントシステム要求事項」は、マネジメントシステム全体に関する事項であるため、内部統制の基本的要素すべてに関係することになりますが、とりわけ、統制環境、リスクの評価と管理、情報と伝達に関連することになります。

「4 サービスマネジメントの計画立案及び導入」も、概ね内部統制の基本的要素すべてに関係することになります。詳細にみると「4.1 サービスマネジメントの計画（Plan）」は統制環境、「4.2 サービスマネジメントの実施及びサービスの提供（Do）」は統制活動、モニタリング（とりわけ継続的監視業務）、「4.3 監視，測定及びレビュー（Check）」はモニタリング、「4.4 継続的改善（Act）」はリスクの評価と管理、情報と伝達が関係してくることになります。なお、JIS Q 20000-1 のマネジメントシステムは、内部統制実施基準で統制環境の一部として重要視されている経営者の「誠実性及び倫理観」については規定されていません。

統制に関する要求事項は、おもに IT 全般統制に関係します。システムの開発に関する事項を除けば、JIS Q 20000-1 の要求事項は概ね IT 全般統制に関係することになります。内部統制実施基準における IT 全般統制の分類と JIS Q 20000-1 の章の間の関係は概ね以下の図のようになります。

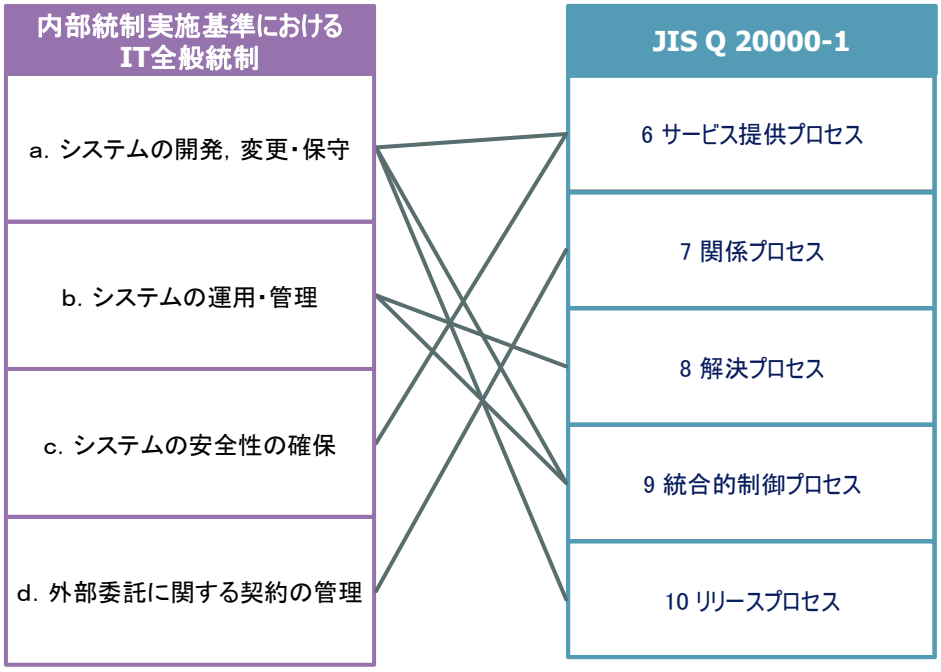


図 A-5 内部統制実施基準における IT 全般統制と JIS Q 20000-1 のプロセスとの関係

ただし、内部統制実施基準の「a. システムの開発，変更・保守」は、JIS Q 20000-1 の「6 サービス提供プロセス」、「9 統合的制御プロセス」、「10 リリースプロセス」に対応させていますが、JIS Q 20000-1 のこの 3 つのプロセスが全て適合していることが「a. システムの開発，変更・保守」に準拠していることにはならないと、同時に、JIS Q 20000-1 の「6 サービス提供プロセス」は、内部統制実施基準の「a. システムの開発，変更・保守」、「c. システムの安全性の確保」に対応させていますが、内部統制実施基準のこの 2 つの項目に準拠していることが「6 サービス提供プロセス」に適合していることにはならないことに留意してください。

JIS Q 20000-1 の規格に従って、IT サービスマネジメントシステムを構築することは、財務報告に係る内部統制の評価と監査制度への対応そのものになるわけではありませんが、IT サービスマネジメントを実施することにより、この制度への対応のための評価及び監査の手続を軽減することにつながることになります。

付録 B 入札条件としての利用

付録 B.1 サービスの一般的特徴と入札条件化

本規格の「1 適用範囲」には、本規格の用途として入札に関する記載があります。

> この規格は，次の事業，組織又は用途に利用してもよい。
> a) サービス調達を入札に付そうとしている事業
> （JIS Q 20000-1:2007 1. 適用範囲 より引用）

入札条件として本規格を利用することは、サービス提供者に対するインパクトが大きいと考えられるため、まずは「入札」という日本語訳の正当性を確認しておくことにします。

> It may be used:
> a) by businesses that are going out to tender for their services;
> （ISO/IEC 20000-1:2005 1. 適用範囲 より引用）

JIS Q 20000-1 では、“tender”を「入札」と訳しています。“tender”には「差し出す」「提出する」などの意味がありますので、より一般的に“提供”と訳出できるはずですが、規格の他の箇所で「提供」の意味で“provide”などの単語を用いていること、ここだけが“tender”という単語を特に用いていることから、より明確な例示となる“入札”が採用されました。

本 ITSMS ユーザーズガイドでは、この一文を次のように解説しています。

> 事業、組織については詳細な説明が無いために、a）～f）項の例示について、それぞれに想定することが可能です。
> a）サービス調達を入札に付そうとしている事業
> この規格はサービス提供者に向けられたものですが、顧客にとっても有益なのが、入札に当たってこの規格を活用することです。
> 顧客は、サービス提供者から受けるサービスの品質を確保するために、入札に際して SLA に盛り込んでいく数値目標などを条件として提示しますが、それ以外に、サービス提供者としての指針や具体的な実装方法などにも踏み込んだ記載を求める時代に入っています。そのときに、数値化されない指針や具体的な実装方法については、顧客とサービス提供者の間では、共有化された規格が今までは存在しませんでした。本規格を用いることによって、信頼できるサービス提供のプロセスを有していることを評価できるようになります。

近藤隆雄著『【新版】サービスマネジメント入門』によると、サービスには一般に以下の特徴があります。

① 無形性：サービスは活動であり物理的な「形」を取ることができない
- ✓ 流通させることができない
- ✓ 作り置きし、在庫にしておくことができない
- ✓ 顧客に見せたり、試しに使わせたりすることができない

② 生産と消費の同時性：サービス活動の対象が人である場合には、サービスは生産と同時に消費が発生する（例：電車での移動は、電鉄会社からはサービスの提供であり、乗客からはサービスの消費となる）
- ✓ やり直しがきかない（サービスの付可逆性）
- ✓ サービスの生産過程が重要視される
- ✓ 顧客はサービスが生産されている場所に出向く必要がある（顧客が必要とする場所と時間においてサービス生産が行われる必要がある）

③ 顧客との共同生産：サービスの生産者と顧客が共同して作り出される（コ・プロダクション）
- ✓ 自分自身にサービスすることがある（例：セルフサービス）
- ✓ サービス提供者に協力することがある（例：レストランまで出かけてサービスを受ける）
- ✓ サービスには時間の経過を伴うので、顧客も対応活動を行わざるを得ない

④ 結果と過程の重要性：結果を得るために活動の過程を経験する必要があるため、結果ばかりでなく過程も同程度に重要性を持つ
- ✓ 結果が出るまでの間の活動過程が快適であることが望まれる
- ✓ 結果と過程の両方が顧客にとって重要である
- ✓ サービスの過程は不安定で標準化が難しく振れ幅が大きい（モノ製品の消費過程は、組み込まれた機能との関係で予定された範囲内でのみ発生する）

特徴①から、利用者はサービス利用に先立ってその品質を事前チェックすることは不可能です。対抗策として考えられるのは、これから提供されるサービスの内容や程度について、提供者と使用者の間であらかじめ合意しておくことです。サービスの契約書にはサービス内容が、サービスレベルアグリーメント（SLA）にはサービス水準に関する合意が盛り込まれます。SLA に記載される内容は、システムの可用性を数値化した値などの定量的な記述だけでなく、サービス提供者がサービスの提供に際してとる指針や方針など定性的な側面の記載も含む可能性があります。

しかしここまでの手当てでも、そもそもサービス提供者が SLA に記載された内容を実現するに足るサービス提供プロセスを有しているのかということについては、顧客は知る手立てがありません。しかも特徴②のサービスの不可逆性は、ひとたび劣ったサービスを提供してしまうと、サービス提供者のビジネスに負のインパクトを与えてしまうことを暗示しています。「入札」に言及しているこの条項は、こうした顧客側の視点に立った本規格の利用法と言えるでしょう。顧客の側からサービス提供者に対して以下のような要求を、入札の条件として求めることで、サービスの提供プロセスまで踏み込んだ安心を、サービスの提供より前に得ることができる可能性があります。

a) 本規格や ITIL を元に IT サービスマネジメントに取り組んでいる状況について、説明を受ける。

b) サービス提供者が実行している IT システム運用についての説明を、本規格や ITIL に沿った形で求める。
c) 本規格の認証取得を求める。

このうち a)及び b)がサービス提供者の自己申告であるのに対し、c)は適合性認定制度に則った第三者による審査を経たものであるので、信頼性は格段に違うと言えます。本 ITSMS ユーザーズガイドはいたずらに本規格の認証取得を求めるものではなく、まして入札条件に認証取得を規定することを希求しているわけではないのですが、より厳格な IT サービスマネジメントの履行を事前に要望する場合には、活用も視野にいれると良いでしょう。

本規格の存在意義の一つは、特徴④の「過程の標準化は困難」を軽減するための手段の提供にあると考えられます。本規格は SLA 等に記載される定量的数値が示す「結果」だけでなく、サービス提供がプロセスまでを視野に入れた活動に昇華させようとする時、また良質なサービスを受けたいと希求する顧客にとって参考となる考え方や施策の基本となるでしょう。

参考：『【新版】サービスマネジメント入門　［商品としてのサービスと価値づくり］』
近藤隆雄 著 生産性出版 2004 年 1 月刊

付録 B.2 産業構造審議会資料にみる本規格の活用法

経済産業省の産業構造審議会・報経済分科会・情報サービス・ソフトウェア小委員会が発行している『情報サービス・ソフトウェア産業維新　～魅力ある情報サービス・ソフトウェア産業の実現に向けて～』(以下、「産業維新報告」と略す。)では、従来からの問題に加え到来しつつある問題を鑑み、情報サービス産業のあるべき姿として次の(1)～(3)を挙げています。

(1) 多様な機能を発揮するベンダが活躍できる産業構造の確立
(2) ユーザとベンダの合意・共同作業の実現
(3) ベンダ間の競争的市場環境の整備

これらの課題を解決するため、大きく 2 つの「可視化」を提案しています。

- 可視化 1：情報サービス産業の可視化
- 可視化 2：情報システムの価値の可視化

可視化1:情報サービス産業構造の可視化

情報サービス産業が抱える構造的課題に関して、産業維新報告が重要であるとしていることは次の 2 点です。

a) 情報サービス産業の多様な機能の分節化：能力のあるプレイヤーが多様な機能をユーザ企業に対して提供できるような産業構造を確立すること
b) 提供形態の多様性及び柔軟性の確保：各種の機能が IT プラットフォーム（パッケージ型、請負開発型、サービス型、アウトソース型）の多様性に応じて、柔軟に提供されるビジネス構造を確立すること

a)に関して、複数の機能を包括的に提供しうる企業においても、従来のように各機能の内容を曖昧にした一括請負という形態ではなく、個々の内容を個別に切り出して提供（分節化）するというプロセスが盛り込まれることが必要であるとしています。また b)では特に、最近の IT の進展とグローバル展開によって、オンサイト、オフサイト、オフショアなどさまざまな形態での機能提供が可能になっていることから、この選択の柔軟性確保が重要であるとしています。

このために産業維新報告が着目するのは、以下です。

- 情報サービスの品質や成果を定量化
- プロセスの標準化・定量化の推進

具体的な解決策として産業維新報告は「機能」と「役割」の可視化を中心に 5 つ挙げています。

(1) 情報サービスの可視化
(2) 「ユーザ・ベンダ間の取引関係・役割分担」の可視化

(3) 「下請け取引関係・役割分担」の可視化

(4) ベンダ間の競争環境の整備

(5) ユーザ企業の発注コーディネーション能力の強化

この 5 項目の中から、ISO/IEC 20000 の活用について言及した(1)を引用します。

> （1）情報サービスの可視化
>
> 情報サービス産業全体の「機能」と「役割」の明確化と柔軟化に結び付けるために、活用が進んできているSLA（Service Level Agreement）をより有効に活用するためのSLM（Service Level Management）のさらなる標準化と普及を進めることが必要である。具体的には、昨年秋に国際規格化されたITILを元に作成されたISO/IEC 20000の適合性評価制度を創設し、普及を促進する。それとともに、既存の政府・民間レベルのSLAガイドラインを必要に応じて改訂し、普及を促進する。
>
> ＜参考＞これまでの情報サービス標準化の動き
>
> ●ITIL（Information Technology Infrastructure Library）・ISO/IEC 20000
>
> ITILは、英国OGC（Office of Government Commerce）が開発したITサービスに関するベストプラクティスであり、世界的に活用されている。日本では、itSMF Japan(IT Service Management Forum Japan)により普及活動が行われてきた。ITILにおいては、サービスレベル管理の基盤としてSLAを位置づけている。ITILをもとに、英国規格BS 15000が作られ、さらに、2005年12月にはISO/IEC 20000として国際規格となった。ITILがベストプラクティスであり、プロセスを定義しているのに対し、ISO/IEC 20000はプロセスが組織に導入されているかを判断する。
>
> ●「情報システムに係る政府調達へのSLA導入ガイドライン」（経済産業省）
>
> 電子政府の取組の一つとして、情報システムにおける政府調達の手続きの合理化や透明化の向上、調達費用の提言などを目的として2004年に経済産業省が策定した。政府調達のSLA導入手順や検討方法、SLM（Service Level Management）の運営方法に関するポイント等を提示している。
>
> ●「公共ITにおけるアウトソーシングに関するガイドライン」（総務省）
>
> 地方公用団体が連携して進める協同利用型アウトソーシングについて、プロジェクトの進め方、SLA等に関する指針を示すことを目的として総務省が策定した。
>
> ●「民間向けITシステムのSLAガイドライン」（電子情報技術産業協会）
>
> 民間におけるSLAの共通的な指標として、情報サービスの利用者と提供者の間で適切なサービスレベルの選択を可能とすることを目的として電子情報技術産業協会が策定した。
>
> また、ベンダの側では個別機能ごとのサービス提供（個別機能提供で他社に差別化を図れるベンダ）及び複数機能の統合的提供（バリューチェーン全体を提供することで差別化を図れるベンダ）の両者のビジネスモデルを確立し、多様なビジネスモデルの間で競争が起きる環境が整うことが重要である。
>
> このような情報サービスの機能分化・ビジネスモデルの多様化をスムーズに進めるためには、第一に業界内の情報交換を円滑化すべきであり、母体企業の業態や、経緯的な要因から分化している業界団体の垣根を越えた「対話の場」を作るべきである。第二に、政府調達等を利用して、ベンダの各種機能を適切に評価するような仕組みを整備していくことが重要である。
>
> （情報サービス・ソフトウェア産業維新　～魅力ある情報サービス・ソフトウェア産業の実現に向けて～
> 第二章 第二節：解決方策①情報サービス産業構造の可視化　より引用）

ポイントとされているのは以下のとおりです。

- SLA/SLM のさらなる標準化と普及の推進
- ISO/IEC 20000 適合性評価制度を創設し、普及を促進
- 既存の政府・民間レベルの SLA ガイドラインの改訂、普及の促進
- 個別機能提供で他社に差別化を図れるベンダと、バリューチェーン全体を提供するこ

とで差別化を図れるベンダの両者のビジネスモデルを確立し、多様なビジネスモデルの間で競争が起きる環境を整備

- ✓ 業界内の情報交換を円滑化、業態・業界団体の垣根を越えた対話の場の用意
- ✓ 政府調達等を利用して、ベンダの各種機能を適切に評価するような仕組みの整備

この文章からは、SLA/SLM を重視する姿勢と、ISO/IEC 20000 適合性認定制度に対する期待の大きさ、ベンダ間の健全な競争を促すための「情報交換の場の設置」「政府調達等の利用」が目につきます。

本規格の 6.1 章がサービスレベル管理（SLM）であることに、付録 B.1 にみたように適用例として「サービス調達を入札に付そうとしている事業」が想定されていることを織り込むと、少なくとも IT サービスマネジメント領域においては本規格がベースとして機能することが求められている解釈してもよいでしょう。政府調達に本規格が利用される可能性も、ゼロではないでしょう。

可視化 2:情報システムの価値の可視化

「政府調達に本規格が利用される可能性も、ゼロではない」ということを示す論拠として、産業維新報告の「第二章 第三節：解決方策②情報システムの価値の可視化」で『「人月工数単価」から脱却し情報システムの「価値の可視化」を実現』するための方策の一つ、「信頼性に関する価値表示機能の創設」を引用します。

> （ｉ）信頼性に関する価値表示機能の創設
> そもそも、「高信頼性」の実現のためには、ユーザ・ベンダの共同関係の構築、経営トップが責任をもったシステム構築体制の実現、事前予防と事後措置、保守・運用プロセスの重視といった考え方に基づき、今回制定された「情報システムの信頼性向上のためのガイドライン」（以下、信頼性ガイドライン）を遵守すること、並びに当該システムの信頼性レベルをユーザ企業がしっかり認識することが重要である。具体的な実施に当たっては、信頼性ガイドラインを踏まえて策定されるモデル契約・契約プロセス及び改訂 SLCP の遵守が必要である。
> このための具体的ステップとして、以下の措置を検討する。まず、第一段階として、例えば、信頼性ガイドラインに基づき、各種ベンチマーク、モデル契約等の採用状況等も勘案して、客観的な「信頼性評価指標」を整備し、民間の認証メカニズム等を活用しつつ、保険制度などの利用のためのメリットを活用するための環境を整備する。次に、第二段階として、産業界への浸透状況を見極めつつ、主にベンダ企業を対象に、当該企業の信頼性実現レベルを公的な第三者機関（独立行政法人情報処理推進機構など）による客観的な評価が可能な体制を整備し、政府システムの調達や重要なシステム構築等において広く活用を図る（図２－３－１）。
> このことにより、ベンダの高信頼性という観点からの情報システム構築力の「可視化」が進み、ベンダ間の競争を通じて業界全体で高信頼性情報システムの構築能力の向上が期待される。なお、実際の指標構築に当たっては、企画段階と開発段階以降を分割する等のきめ細かな設計が必要である。
>
> （情報サービス・ソフトウェア産業維新　～魅力ある情報サービス・ソフトウェア産業の実現に向けて～
> 第二章 第三節：解決方策②情報システムの価値の可視化　より引用）

この文面に産業維新報告の図 B-1 の内容を加えて整理すると、第一段階から第二段階への昇華パスのポイントは以下のようになります。

第一段階：客観的な「信頼性評価指標」と活用体制の整備・浸透

- 『情報システムの信頼性に関するガイドライン』を参照
- 各種ベンチマークの整備と活用
  - ✓ ISO 9001:2000、ISO/IEC 20000、システム管理基準等の活用
- モデル契約・モデル契約プロセスの採用状況等の勘案
- 民間の認証メカニズム等を活用
- 産業界への浸透状況の見極め
- 保険制度などの利用のためのメリットを活用するための環境を整備

第二段階：保険制度、政府調達での活用

- 保険制度での利用
- 政府システムの調達や重要なシステム構築等において広く活用
- 信頼性実現レベルの公的な第三者機関による客観的な評価体制を整備

「政府調達での活用」に向けた基本となるベンチマークの具体例として、本規格が参照されていることを特記しておきます。

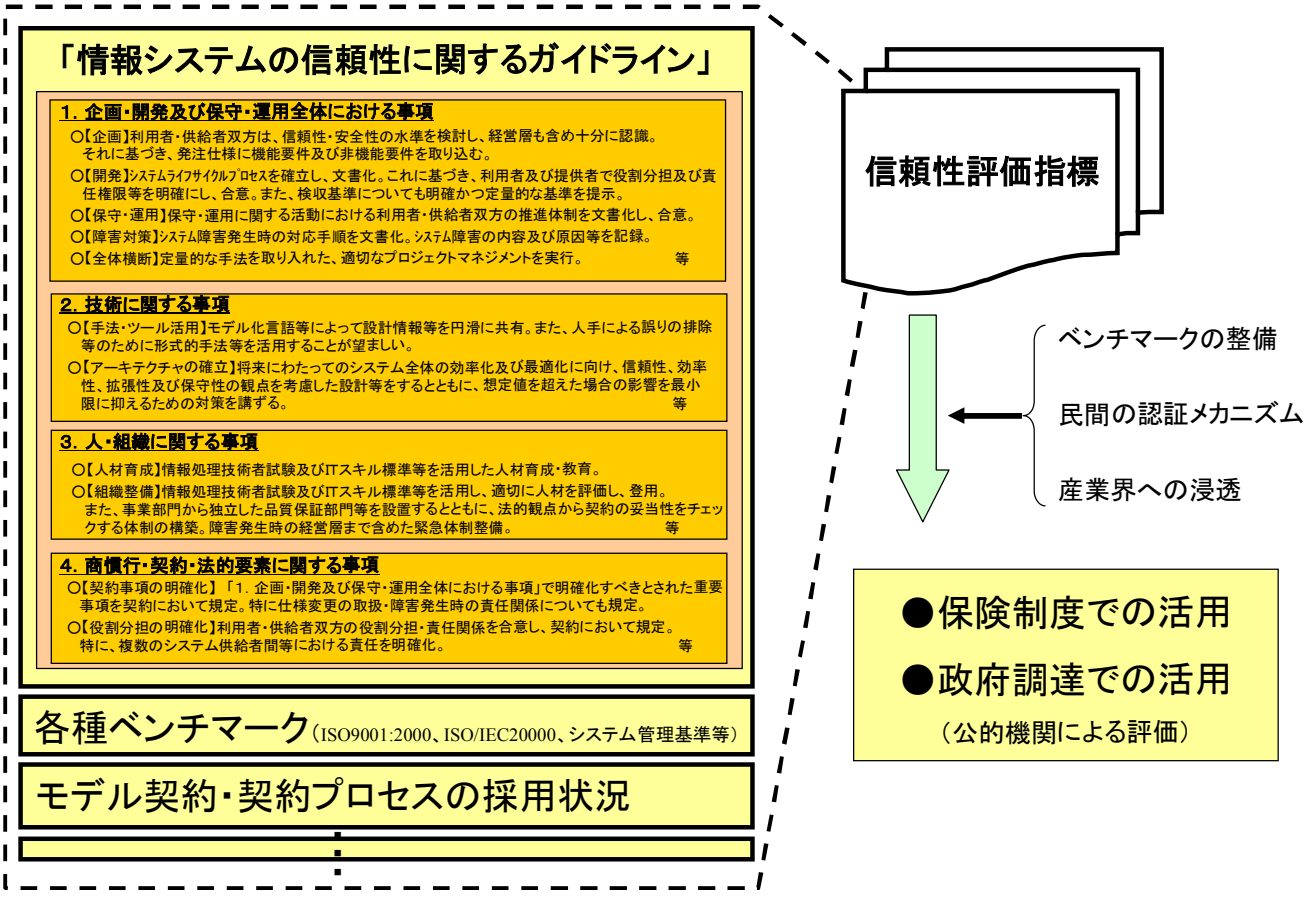


図 B-1 信頼性評価指標の策定とその活用（出典：産業維新報告 図 2-3-1）

※1：この他に産業維新報告では、ビジネス改革提案機能を担うサービス、会計・人事等のエンドユーザ業務を含むケースについて考察している。

参考：『情報サービス・ソフトウェア産業維新　～魅力ある情報サービス・ソフトウェア産業の実現に向けて～』産業構造審議会　情報経済分科会　情報サービス・ソフトウェア小委員会　中間とりまとめ（平成 18 年 9 月 14 日）

付録 C 組織内での利用

付録 C.1「IT サービスマネジメント」確立の必要性

システムトラブルが社会的な問題となり、システムリスクの顕在化が世間を騒がせています。また、近年、個人情報保護法や SOX 法、政府セキュリティガイドラインなど、IT サービスを提供していく中で、留意・遵守すべきルールも急速に増加しており、これらのルール違反に対する市場の反応も厳しくなっています。

一方、IT 技術の進展、ビジネスへの IT 技術利活用の推進などにより、ビジネスのシステムへの依存度が高まり、システムリスクが即ビジネスリスクに直結する事態が顕在化する時代を迎えており、社会的なルールの遵守も含め、大きなシステムリスクを惹起させないように、これまで以上にシステムの安定稼働やセキュリティ維持・確保などシステムリスクの徹底したコントロールが求められています。

このように、IT への期待と一方で脆弱性に対する懸念からか、ビジネスへの IT の適正・的確な利活用や IT に係わる業務運営の適正化が強く求められるようになって来ており、IT に係わるマネジメントの成熟度を今までの延長線ではなく飛躍的に高めていく必要のある時代になって来ています。

今日的に求められるマネジメントは、自己責任の原則に則って業務の健全かつ適切な運営を実現していく必要があり、それを自ら証明していくことが求められます。そのため、業務運営にあたっては網羅性と妥当性の確保されたプロセスの明確化とその確実な実施を組織担保しておく必要があります。

こう言った状況の中で、「IT サービスマネジメントスキーム」を構築し、正のスパイラルを回し、継続的な改善活動に資する JIS Q 20000-1 の認証取得することは意味があります。

付録 C.2　認証取得のメリット（何故、JIS Q 20000 認証取得なのか）

ただ、認証取得をすればいいと言うわけではありません。認証取得することが目的ではなく、この規格が提唱・推奨する PDCA サイクルを組織の内部統制のスパイラルと一体化して、継続的な改善活動にしていけるようにすることが大切です。それにより、「顧客・株主等ステークホルダーへの説明責任を全うする」ことが可能となります。

また、組織の成熟度を向上させるだけではなく各メンバーの「人材育成」にも大きく寄与すると考えられます。

【顧客・株主等への説明責任を全うする】

社会の成熟度が高まってきたのに伴い、自己責任の下での適正な業務・組織運営が強く求められる時代になってきています。適正な業務・組織運営について、客観的・合理的な方法によった説明責任（自己証明）の必要性が生じています。それを実現していくため（顧客への説明責任を全うしていくため）には、各組織の独自のやり方から脱却していく必要

があります。

JIS Q 20000 の認証を取得するということは、認証を取得する組織が

① JIS Q 20000（及びそのベースとなる ITIL）で定義されている IT サービスマネジメントの各プロセスを備えていること

② 経営陣がコミットする継続的に改善されるしくみ（マネジメントシステム）を備えていることを公正な第三者機関が証明してくれることです。

IT サービスマネジメントの標準的なフレームワークである ITIL（Information Technology Infrastructure Library）をベースにした規格である JIS Q 20000 の認証を取得することにより、プロセスの網羅性、妥当性が確保され、お客様への説明責任をより一層全うすることができます。

【人材の育成・人材の確保】

また、ITSMS（JIS Q 20000）などの規格や認証の取得は、組織の成熟度を向上させるだけではなく各メンバーの成長にも大きく寄与すると考えられます。標準的なフレームワークの中に自分の経験・実績をマッピングすることで、経験や実績を「知識」に変換することが出来、各メンバーのスキルの幅や奥域を広げることに役立つことが出来ます。「知識」に変換し蓄積させていくことで、SE としてのプロフェッショナリズムにも磨きがかかり、また他の人への知識伝承・移転も容易になってきます。

付録 C.3　IT サービスマネジメント構築上の考慮点

～　各組織にとって JIS Q 20000 をより実効性のある規格とするために　～

【システム運用を「IT サービス」として捉える】

「システム運用」は、情報システムが業務で有効に活用できるように、情報システムを適正なコストで日々稼働させ、またシステムの安定性や継続性、正確性を妨げるあらゆる脅威を排除し続けることが求められますが、当該業務を単なるコンピュータの運行・運用として捉えるのではなくて、情報システムがビジネスに有効に活用できるよう情報システムの機能を安定的・正確に提供し続ける「IT サービスの提供」として捉えサービスの内容を明確化、定義することが重要です。

「IT サービスの提供」は、①毎日の確実なシステムの稼働、②トラブルの監視と検知及び対処、③トラブルを未然に防ぐ予防活動、④サービスレベルに応じたコストの適正化　を行うことが求められますが、これらの活動の原点には、①ビジネスとシステムの関係の明確化、②ビジネスの中におけるシステムリスクを十分認識、評価しそれらを最小化すると言う考えの下で活動する必要があると考えられます。

さらに、社会動向を考慮すれば、「何事も起こさないこと」に努め、何か起きたら迅速的確な対処・対策・報告を行うといった従来の発生事象対応型の業務運営ではなく、自己責任の下で「何事も起こしていない」ことの証明をし続けることと、その説明責任が強く求められるようになってきているとの認識に立つべきです。

これらを考慮すれば、明確・的確なガバナンスとマネジメントの下において、各プロセスの明確化とその透明性や公開性の確保、各プロセスの妥当性や網羅性で問題がないことを示し、またその確実な実施状況を常にモニタリングしコントロールし続ける必要があり、これら全体を含めてリスクコントロールベースの「IT サービスマネジメント」活動としていく必要があると考えられます。

【「守るべきもの、守り方」を明らかにする】

（リスクコントロールベースの IT サービスマネジメント）

あらゆる脅威を排除し的確なコントロールを行うためには、リスクコントロールベースでの IT サービスマネジメントが有効です。

この実現を図るためには、まず「守るべきもの、守り方」を明確にする必要があります。

「守るべきものは何か（対象の明確化）」「脅威は何か」「どこにリスクが存在するか」「リスクが顕在化した場合、どのような影響をビジネス（利用者の）に及ぼすか」を明らかにし、それらを評価し、最小化策を明確化するなどリスクシナリオを作成していきます。リスクの洗い出し、最小化策の策定にあたっては、「漏れなく重複なく（MECE：Mutually Exclusive Collectively Exhaustive）」行うことが重要です。COBIT の考え方（「データ、アプリケーション、テクノロジー、設備、人」を対象に、「有効性、効率性、機密性、完全性、可用性、準拠性、信頼性」の観点で分析する）や、「SOX 法」「個人情報保護法」に係わるガイドラインや、金融庁・通商産業省の「監査基準」、金融情報システムセンター(FISC)「安全対策基準」などが参考になります。

検討した結果を、「脅威」「リスク」「リスク最小化策」「モニタリング」として整理しガイドとして取りまとめることにより、IT サービス活動の原点とし、以下のように活用できます。

- 新たなシステムを開発する際のガイド（運用設計、非機能要件ガイド）
- システム稼働可否判断時の評価基準
- システム稼働後のモニタリング基準（リスク監視、コンテンジェンシー発動基準）

【IT サービスに係わるプロセスの明確化、マネジメントシステムの構築】

上記ガイドを起点に、IT サービスに係わる作業をリスク管理の実践に向けた作業として定義、明確化し、それを規定体系として整理します。

組織としての基本的なリスク方針（「リスク管理ポリシー」など）、IT サービスに関するより具体的な取組み指針（「システムリスク管理スタンダード」など）の基本文書の中で「ガ

バナンス」や「モニタリングの視点」の明確化、「マネジメントによる監理」などを明らかにするとともに、どのような管理プロセスを備えるべきかを定義していきます。

管理プロセスの構築にあたっては、JIS Q 20000 の規格だけでなく、ITIL や IT の分野における内部統制の標準的なフレームワークである COBIT との整合性を確保しておくことも重要です。

これらのスタンダードを使用し組織の現状とのギャップ分析を行い、組織にとって不十分なプロセスを強化していくとともに、その網羅性、内容の妥当性を確保していきます。

マネジメントシステムの観点では、各組織が従来から持っている PDCA サイクルと整合性をとり、組織にとって有効かつ効率的なマネジメントシステムにすることが重要です。それにより継続的な正のスパイラルアップを実現させていきます。

これにより、明確・的確なガバナンスとマネジメントの下において、各プロセスの明確化とその透明性や公開性の確保、各プロセスの妥当性や網羅性で問題がないことを示すことが出来ます。

管理されたプロセスと、その実施状況の評価基準を明らかにし、日々の業務遂行状況をモニタリングし続けることで業務運営適正化の組織担保が図れます。

【プロセスの確実な実施とそのモニタリング（IT サービスに係わるサービスレポート)】

モニタリングは、「認識・評価」されることが重要であるとともに、継続的に同じ視点で確実に行われるべきものでもあります。モニタリング結果をどのようにレポートにまとめ、経営陣やお客様へ、どのようなタイミングで報告しレビューを受けるかが、内部統制の観点から重要になります。以下参考例です。

「パフォーマンスレポート」

各プロセス単位の正確性、妥当性の確保を行うために作成し、発生した事象と事前に策定してある評価指標と比較評価しながら作業の確実性や改善点の確認を行うとともに、変化するリスクへ確実な対応を図れるようにプロセスそのものの妥当性や網羅性の保障を行うことを目的とします。

例えば、サービスレベル管理については、各サービスレベル指標について達成状況（達成・非達成、達成率など)、インシデント管理・問題管理については、インシデントの発生状況やお客様への影響度の把握、原因究明や再発防止策実施状況、性能管理については、各種リソースの使用予測とその結果の状況などの詳細状況をレポートします。また、各プロセスについて以下の基準で繰り返し確認し、正当性を確保し続けます。

- 各プロセスの目的は明確か？
- 目的は全員に周知徹底されているか？
- プロセスは明確か？
- プロセスは遵守されているか？

- 評価できる指標は明確か？
- 指標は達成できているか？（正確性・効率性）
- ドキュメントは整備されているか？
- プロセスは現状に即しているか？
- 必要な変更は行われているか？
- 何らかの予兆は？

なお、各プロセスの実施は、「作業（行為）が“信頼”されている形で行われているならそれを信ずる」と言う意識を改め、「“記録”がなければ、（行為を）チェックできない」との認識に立って、「作業（行為）が行われていること」の証明“記録”（エビデンス）の確保を確実に行うことにします。

「リスクベースレポート」

「パフォーマンスレポート」の中から、リスクの観点で認識しておくべき内容を、「サービス品質に係わるリスク」「サービス継続性に係わるリスク」「セキュリティに係わるリスク」等の切り口で分析、評価した結果を取りまとめます。

これをエグゼクティブ・サマリーレポートとして経営陣やお客様と共に、COBIT の掲げる IT の内部統制のフレームワークをベースに据え、相互に認識・評価しリスク管理の実効性を高めます。

付録 C.4 実効性ある IT サービスマネジメントを実現させるための組織、人材

【開発・運用の分離・牽制　～IT 組織の運営・権限を明確にすることの重要性～】

システムの開発部門は、システムを企画・開発し、リリース後はそのメンテナンスを行い、運用部門は開発部門が作成した運用手順に従いオペレーションを行う。従来からの、開発と運用の役割分担はこのようなものであり、現在でも、運用部門は運行に徹している組織があるのではないでしょうか。しかしながら、システムが提供するサービスを IT サービスとして捉えると、運用部門は IT サービスのプロバイダそのものであり、本番稼働する IT サービス全般について責任を負うべき時代になってきていると認識すべきです。IT 統制管理、資産管理、開発戦略、設計開発、導入変更、運用管理、支援のプロセスについての責任範囲と権限を明確にすることが重要です。

開発担当者はプロジェクトのスケジュール通り完遂することを最大の目標としており、極端な場合はスケジュール通りにリリースするためには手段を選ばないというほど情熱的になることがあります。ビジネスの IT への依存が高まっている中、システムリスクを適切にコントロールすることが求められていますが、リスクを適切に評価しコントロールする

ためにはITサービス全体を俯瞰し判断できる冷静な目が必要です。「新しいサービスや機能を反映したい」と考えるパワーに対して、「IT サービスを安定的に提供し続ける」ことを考える冷静なパワーが牽制する態勢を作ることが重要です。これが、開発と運用の分離・牽制です。

開発と運用の分離・牽制を確実に行うためには、以下の3つの要素も考慮する必要があります。

① 職責の分離
システムの開発と運用の組織を明確に分離し、職責を明確にすることで、社内で相互牽制を実現する。
② 環境の分離
開発と運用（本番）の環境を分離し、開発担当者が運用環境にアクセスすることを原則禁止とする。
③ アクセスの制限と管理
運用環境の変更は、運用部門で評価・承認し、変更作業は基本的に限られた運用担当者が実施する。また、変更作業操作のログを残し、作業の妥当性、安全性を確認する。

【人材の育成・確保】

今日的なITサービスマネジメントを実現し、維持、進化させ続けるためには、それを支える人材の育成・確保が不可欠です。ITの基本的な知識をベースに、ITIL（JIS Q 20000）やCOBIT、リスク管理、マネジメント手法などの知識をベースに、各人がそれぞれの分野で真のプロフェッショナルとして活躍できる人材の育成、確保を計画的に行っていく必要があります。そのためには標準的なフレームワークの知識の研修、習得、標準的なフレームワークをベースにした実践が組み合わされて行く必要があります。

参考

COBIT 関連

- 『COBIT 4.0 日本語版』　http://www.itgi.jp/download.html
- 『COBIT for SOX 2nd Edition 日本語版』サーベインズ・オクスリー法(企業改革法)順守のための IT 統制目標　http://www.itgi.jp/download.html

SOX 法関連

- 『財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の設定について（意見書）』
  http://www.fsa.go.jp/singi/singi_kigyou/tosin/20070215.pdf
- 『システム管理基準 追補版(財務報告に係る IT 統制ガイダンス)」』
  http://www.meti.go.jp/press/20070330002/20070330002.html

個人情報保護法関連

- 『個人情報の保護に関する法律』(平成 15 年 5 月 30 日法律第 57 号)
  http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/

FISC 関連

- 金融情報システムセンター　http://www.fisc.or.jp/

付録 D 認証の適用範囲の考え方

本付録では認証取得を目指す組織（サービス提供者）の認証における適格性の考え方について解説します。

サービス提供者は認証取得のための審査に先立ち、審査対象となるサービスや組織の範囲（以下、認証の適用範囲）を特定し、審査員あるいは審査登録機関の承認を得る必要があります。また、認証の適用範囲の記述は、客観的に曖昧性がなく、その記述が実際のサービス提供者の能力を超えるような表現にならないよう正確に特定し記述する必要があります。

尚、本付録はサービス提供者が認証の適用範囲を特定、記述する際の考え方について、原理原則として記述したものです。したがって、実際の認証の適用範囲の決定に際しては、その範囲と有効性について本認証基準の審査登録機関と協議するか、あるいはコンサルタントと相談の上、決定することをお勧めします。

付録 D.1　認証の対象

本認証基準は、サービス提供者が IT サービスを提供するためのサービスマネジメントプロセスの本認証基準への適合性及び有効性に対して認証されるものであり、製品やサービスそのものの品質を保証するものではありません。

付録 D.2　認証の適用範囲の考え方

- 認証取得は、認証の適用範囲となるサービスの提供に責任を持つサービス提供者が対象となります。
- 適合性を審査する上で IT サービス提供の対象となる IT システムの存在は必須です。但し IT サービス提供組織がサービス提供における責任を負うことができれば、その IT システムの所有者が誰であるかは重要ではありません。
- サービス提供者が提供しているサービスが商用であるか非商用であるか、あるいは社内の利用者向けのサービスであるのか社外顧客向けのサービスであるのかは重要ではありません。
- サービス提供者は本認証基準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。ただし、適切なサービスマネジメントプロセスが存在しても、それぞれが単独で運用されていれば、そのサービス提供者は認証を得る十分な資格があるとはいえません。それぞれのサービスマネジメントプロセス間のインタフェースや相互のやり取りが明確であり、サービス提供者によって管理されていることが非常に重要です。
- サービス提供者が本認証基準に適格か否かは、本認証基準に定めるすべてのサービスマネジメントプロセスに関して実施している「マネジメント・コントロール

※」の程度（深さ）と範囲に基づいて判断されます。したがって、一部のプロセスを同一社内の他の部門や社外のサプライヤにアウトソーシングしていたとしても本認証基準で定めるすべてのプロセスについてマネジメント・コントロールを実施していることを証明できればサービス提供者は本認証基準に適格であるといえる訳です。

- サービス提供者は直接実施しているサービスマネジメントプロセスとサプライヤにアウトソーシングしているサービスマネジメントプロセスに関して役割と責任を明確にする必要があります。

※マネジメント・コントロールとは

マネジメント・コントロールとは、戦略的に立案された計画を、組織的にオペレーションしていくためのシステム及びプロセスのことです。すなわち目標を実行レベルにつなげていくための活動の推進に責任を持っていることを指しています。

一般的にマネジメント・コントロールは以下のプロセスで構成されます。

- インプットに関する知識及びその管理
- アウトプットに関する知識、その使用と実装
- 測定基準の定義及び測定
- 本認証基準に従ったプロセス機能の責任を客観的に証明する
- プロセス改善の定義、測定、レビュー

付録 D.3　適用範囲（スコープ）特定時の考慮点

認証の適用範囲の記述は、顧客がその範囲の表現で誤解（その記述が実際のサービス提供者の能力を超えるような表現になっているなど）を招かないよう、客観的に曖昧性がなく、正確に特定し記述する必要があります。サービス提供者が認証の適用範囲を決定する際は、以下の点を考慮し認証の適用範囲を特定すると良いでしょう。

- 地理的条件（1 つのオフィス、複数のオフィスからなる組織、地域、国など）
- IT サービスを提供する組織の構成（単一の部門　or　複数の部門　or　全部門など）
- IT サービスの構成（1 つのサービス　or　複数のサービス）
- IT サービスを受ける顧客の構成（単一顧客 or 複数顧客 or 不特定多数の顧客など）

【認証の適用範囲の記述例】

『サービス提供場所』に所在する、***『サービス提供組織名』***が***『顧客の定義』***向け***『サービス名あるいはサービス概要』***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認証の適用範囲とする。

付録Ｅ　「顧客満足」関連３規格について

「顧客満足」関連３規格とは、本付録においては以下を指します。

- ISO 10001 Quality management - Customer satisfaction - Guidelines for codes of conduct for organizations
- ISO 10002:2004 Quality management - Customer satisfaction - Guidelines for complaints handling in organizations
  JIS Q 10002:2005 品質マネジメント－顧客満足－組織における苦情対応のための指針
- ISO 10003 Quality management – Customer satisfaction – Guidelines for dispute resolution external to organizations

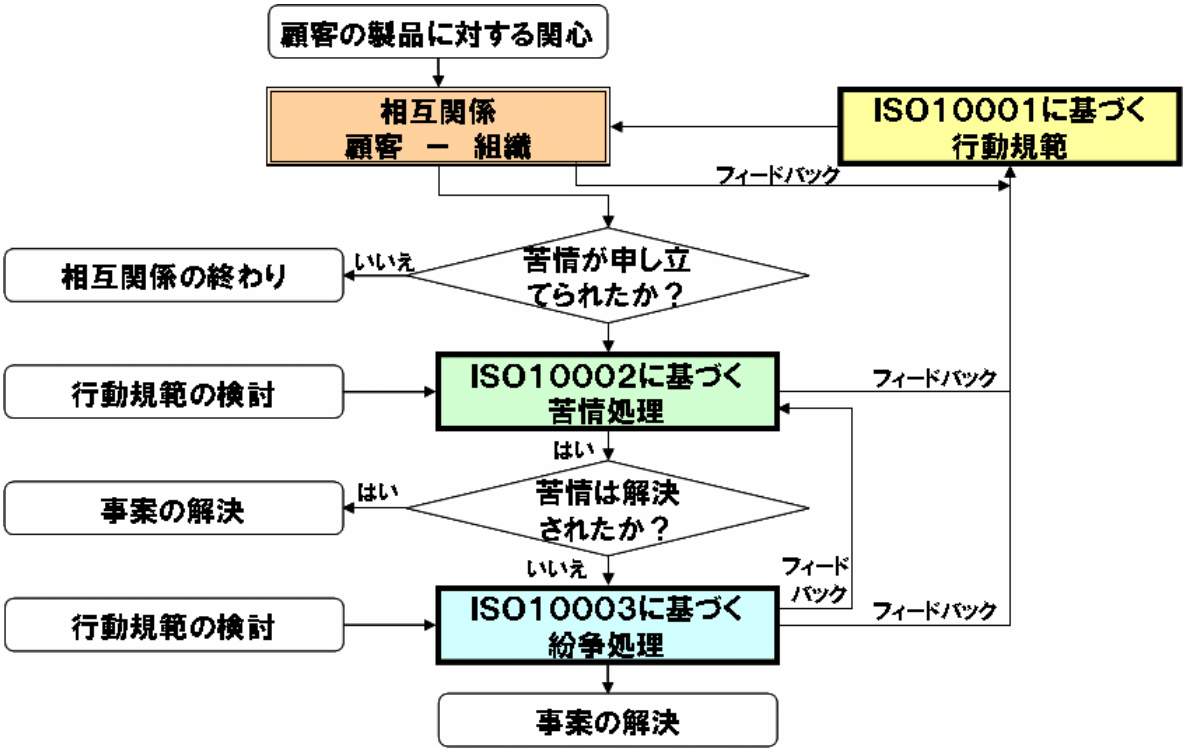
ご注意

「顧客満足」関連３規格のうち、ISO 10002 のみが正式な国際標準及び JIS 規格として発行されていますが、残りの 2 つ（ISO 10001 と ISO 10003）は国際標準化に向けた審議の途中です。したがって本付録における ISO 10001 と ISO 10003 に関する内容は、今後変更される可能性がありますのでご注意ください。本付録は情報提供が目的です。あくまでも正式発行された原文（JIS を含む）のみが有効です。

本付録では、「顧客満足」関連３規格を以下のように表記いたします。

- ISO10001：組織のための行動規範に関する指針
  組織の顧客満足行動規範の手引が記載されている
- ISO10002：組織における苦情対応のための指針
  顧客の苦情の内部処理に関する手引が記載されている
- ISO10003：組織の外部紛争解決に関する指針
  内部的に十分に解決できない製品関連の苦情に関する紛争の解決に関する手引が記載されている

ISO10001、10002、10003 の相互関係を、図 E-1 に示します。二重線で囲んだ四角の中「相互関係　顧客－組織」を JIS Q 20000 における「顧客関係管理」もしくは「供給者管理」と見立てることが可能です。



参考：ISO10001 付属書 B より

図 E-1　ISO10001、10002、10003 の相互関係

付録 E.1　ISO10001：組織のための行動規範に関する指針

顧客満足行動規範の計画、設計、開発、実施、維持及び改善のための手引を提供しています。顧客満足を高めることを目指した組織の行動に関して、組織が顧客に対して行う約束を含む製品に関する規範に適用します。

図 E-2　ISO10001 のフロー

計画、設計及び開発

- 達成する目標の設定
- 課題、課題の発生状況、取り組み方、他組織への影響、他組織の取り組み状況、資源、関連法規を評価
- 利害関係者から規範の内容や使用に関するインプットを入手し、評価
- 範囲・目標、約束・制限、用語定義、対応窓口、未達成時の措置を含む規範を作成
- 定量または定性的パフォーマンス指標を作成
- 規範を実施・維持・改善する手順を作成

- 規範・支援情報を入手可能にする計画を策定
- 約束・救済措置を果たす資源を明確化

実施

- 計画通り実施活動を運営管理
- 関連手順、内外コミュニケーション計画を適用
- 顧客に適切な救済策を提供
- 規範の規定が満たされない場合に措置
- 資源、教育、コミュニケーション計画の適用、苦情処理、救済措置を記録

維持及び改善

- 記録、パフォーマンス評価に必要な情報を定期的・体系的に収集
- パフォーマンスを評価
- 顧客満足を定期的・体系的に判定
- 定期的・体系的に規範及び枠組みを見直す
- 顧客満足を高めるために、規範及び枠組みを継続的に改善

ISO10001 で注意を要する用語として、以下があります。

- 顧客満足行動規範：顧客満足を高めることを目指す行動に関する、組織の顧客に対する約束及び関連規定
- 顧客：製品を受け取る組織又は人
- 顧客満足：顧客の容共事項が満たされている程度に関する顧客の受け止め方
- “製品”という用語は、サービス、ソフトウェア、ハードウェア及び加工された原料に及ぶ

付録 E.2　ISO10002：組織における苦情対応のための指針

組織内部における製品に関連する苦情対応プロセスについての指針を規定しています。指針には、プロセスの計画、設計、実施、維持及び改善を含みますが、組織外の紛争解決や雇用関連の紛争には適用しません。

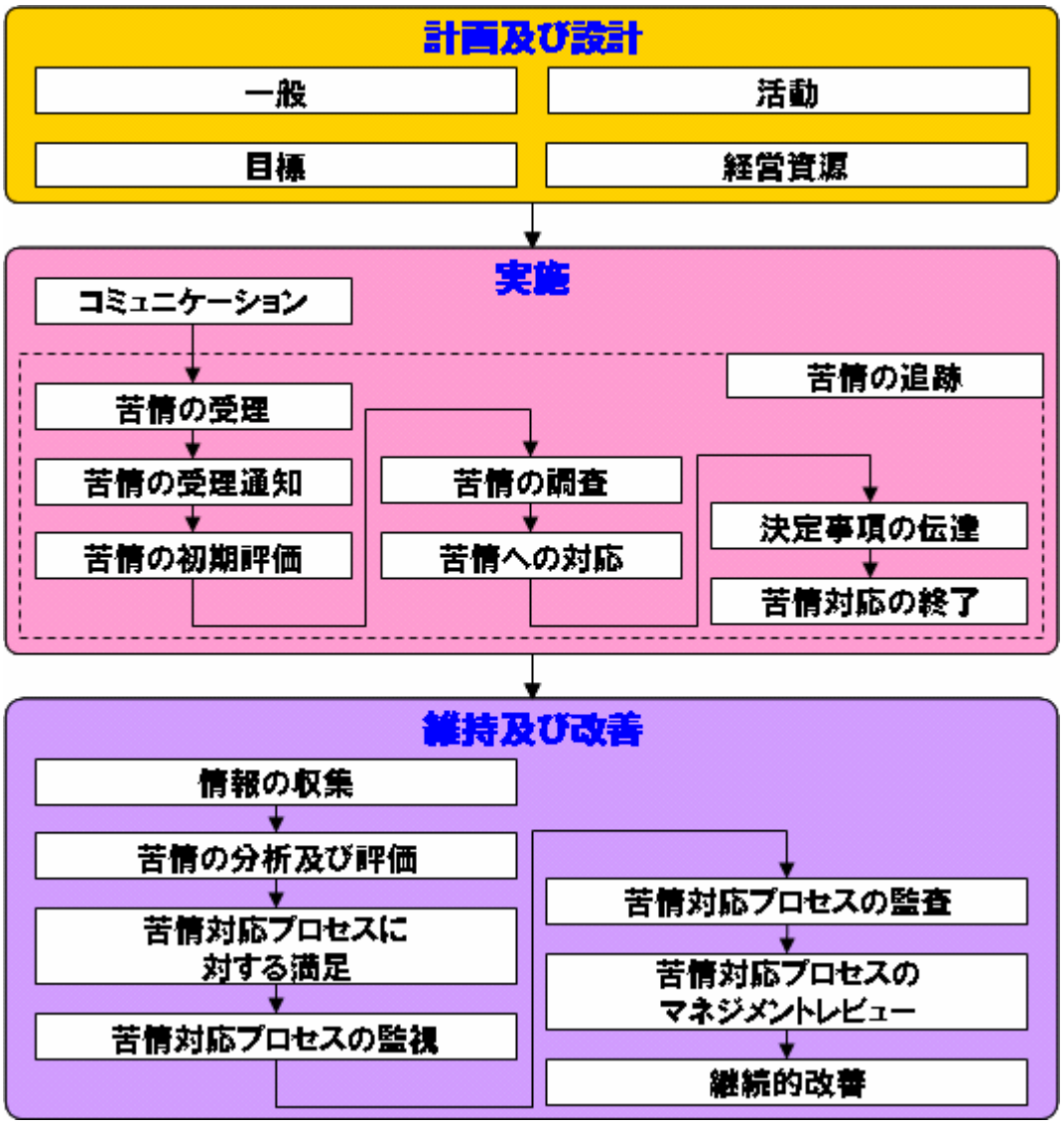


図 E-3　ISO10002 のフロー

計画及び設計

- 苦情対応プロセスを計画・設計し、経営資源を活用し、苦情対応方針への適合と目標を達成
- 苦情対応方針に合った、測定可能な目標を設定
- 苦情対応プロセス計画を確実に遂行
- 必要な経営資源を評価し、提供

実施

- 苦情対応プロセスに関する情報を顧客、苦情申出者、その他利害関係者に告知
- 最初の報告時点で、情報・認識コードを記録
- プロセス全体に亘って苦情を追跡
- 各苦情の受理を直ちに苦情申出者に通知
- 各苦情は重大性・安全性・複雑性・インパクト・緊急性・可用性等の基準で初期評価
- 苦情の状況・情報の調査を実施
- 問題の是正、予防対処を実施
- 苦情対応に関する決定事項・処置を連絡
- 苦情申出者が決定事項・処置を受け入れた場合に、その決定事項・処置を遂行し、記録

維持及び改善

- 苦情対応プロセスのパフォーマンス及び苦情の内容・対応を記録し、利用・管理手順を個人情報・機密保持をしつつ確立し、実施
- 全苦情を分類し、傾向を分析
- 苦情対応プロセスの満足度を定期的に調査
- 苦情対応プロセス、経営資源、収集すべきデータを継続的に監視
- 監査を定期的に実施
- 定期的に苦情対応プロセスをレビュー
- 有効性・効率性を継続的に改善

ISO10002 で注意を要する用語として、以下があります。

- 苦情申出者：苦情を申し出ている人、組織又はその代表者
- 苦情：製品又は苦情対応プロセスに関して、組織に対する不満足の表現で、その対応又は解決が、明示的又は暗示的に期待されているもの
- 利害関係者：組織のパフォーマンス及び成功に利害関係をもつ人又はグループ

付録 E.3　ISO10003：組織外部の紛争解決に関する指針

組織が、製品関連の苦情に対する効果的かつ効率的な外部紛争の解決を計画、設計、構築、実施、維持及び改善するための手引を提供します。

ISO10003 は特に、組織と「個人用又は家庭用の目的で、製品を購入若しくは使用する個人」または組織と「小規模企業」との間の紛争解決を対象としていると注記しています。JIS Q 20000 における紛争処理に参考となると考えられますが、ISO10003 が想定している範囲を超えている可能性がありますので、ご注意ください。

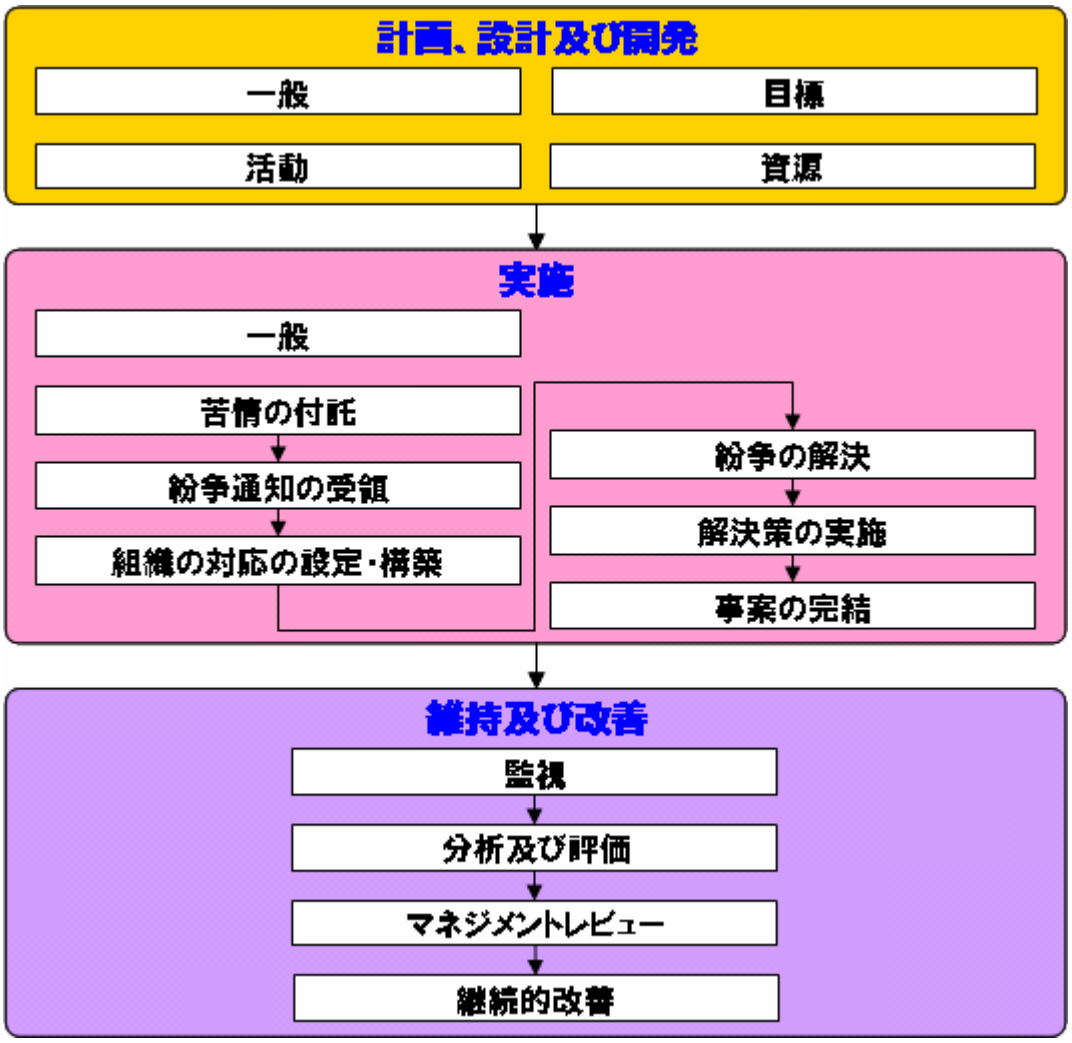


図 E-4　ISO10003 のフロー

計画、設計及び開発

- 有効かつ効果的な紛争解決プロセスを計画、設計、開発
- 現在の取り組みを評価、苦情処理・紛争解決活動・資源・紛争解決方針の分析に基づき紛争解決プロセスを設計し、苦情申出者全体に適用する前に、一部に試用
- 紛争解決の目標を決定、定期的にレビュー

- 要員・情報・資材・資金・インフラ等を入手・配備

実施

- 組織の手順を紛争解決に適用
- 苦情申出者が提供者に紛争を提起していない場合、組織が紛争付託手順を適用
- 紛争解決開始時点で、組織は該当要員に通知
- 紛争を評価するための苦情記録等を収集し、スタッフで協議し、それらの情報を提供者の手順に従って提供し、初期の立場を確立
- 交渉・助言・決定的判断・調停・勧告等により紛争を解決
- 調停・勧告・決定的判断に一致した方法で解決策を遂行
- 紛争の解決が十分に実施された場合に完結

維持及び改善

- 全紛争の性質・進捗状況・結果の情報を収集し、記録
- 収集・入手した紛争解決情報を定期的に分析
- 定期的に紛争解決プロセスをレビュー
- 有効性・効率性を継続的に改善

ISO10003 で注意を要する用語として、以下があります。

- 紛争：提供者に対して申し立てられた苦情に起因する意見の不一致
- 紛争解決者：紛争解決に当たる上で当事者を支援するため、提供者によって任命される個人
- 組織：責任、権限及び関係が取り決められている人々又は施設の集まり
- 提供者：外部の紛争解決プロセスを提供し、運用する人又は組織

付録Ｆ　ソフトウェア資産管理について

『ソフトウェア資産管理』（SAM：Software Asset Management、以降 SAM と訳す場合がある）は、ITIL の書籍群において副読本的な位置づけをされています。ITIL の主要プロセスが ISO/IEC 20000 として国際標準化されたのと同様に、SAM は 2005 年に ISO/IEC 19770-1 として発行されました。SAM が ITIL のコア書籍との関係が強いことを反映して、ISO/IEC 19770-1 は ISO/IEC 20000 と深いつながりがあります。

付録 F.1　ITIL 書籍『ソフトウェア資産管理』概説

ITIL では資産管理というくくりで HW/SW/NW の全てを扱うような、そういうカテゴリ分けはありません。形の上では、資産の多くは構成管理の中で扱い、この『ソフトウェア資産管理』という書籍に書かれるソフトウェアだけがとりわけクローズアップされているという感じです。

■定義

ソフトウェア資産管理（SAM）は、組織内のソフトウェア資産のライフサイクルを通じて、効果的な管理、コントロール、及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と定義しています。

■SAM の目的

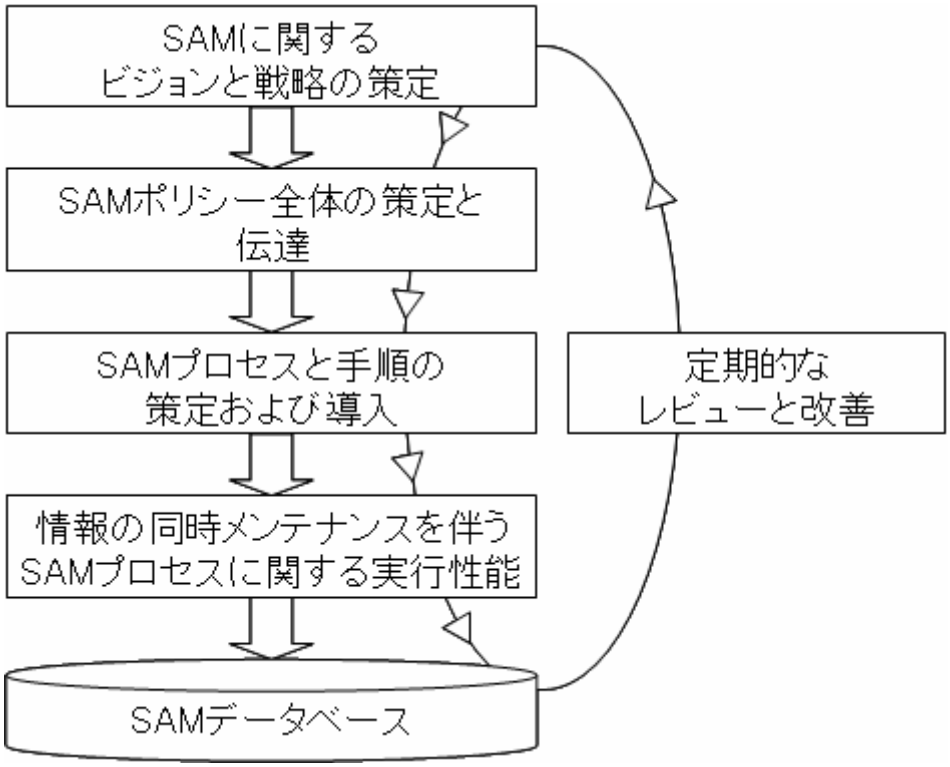
SAM の目的は、ソフトウェア資産の利用によって起きるリスクの管理を含む、組織の持つソフトウェア資産を管理、制御、保護することです。

例えばソフトウェア資産利用で発生するリスクには、不法コピーあるいはソフトウェアライセンスの不正利用があります。こういった問題が発生すると、法的に問題であるという直接の影響に加えて、昨今では企業の姿勢そのものにまで疑いの目が向けられます。SAM の目的に書かれているのは、こうした問題を起こさないということを視野に入れながら、ソフトウェア資産を管理しましょうということです。

この目的を達成するために適用されるアプローチは、下図のような動きがとられます。

- **SAM に関するビジョンと戦略の策定**：上級管理職によって、明確なビジョンと戦略を持つことが最も重要です。
- **SAM ポリシー全体の策定と伝達**：全体ポリシーの確立と伝達が、組織の全体に対して、効果的に行われなければなりません。
- **SAM プロセスと手順の策定および導入**：書き下された手順を含む、詳細なプロセスが定義され、導入される必要があります。
- **情報の同時メンテナンスを伴う SAM プロセスに関する実行性能**：ひとたび SAM プロセスが実装されたら、SAM データベースの情報を並行してメンテナンスします。

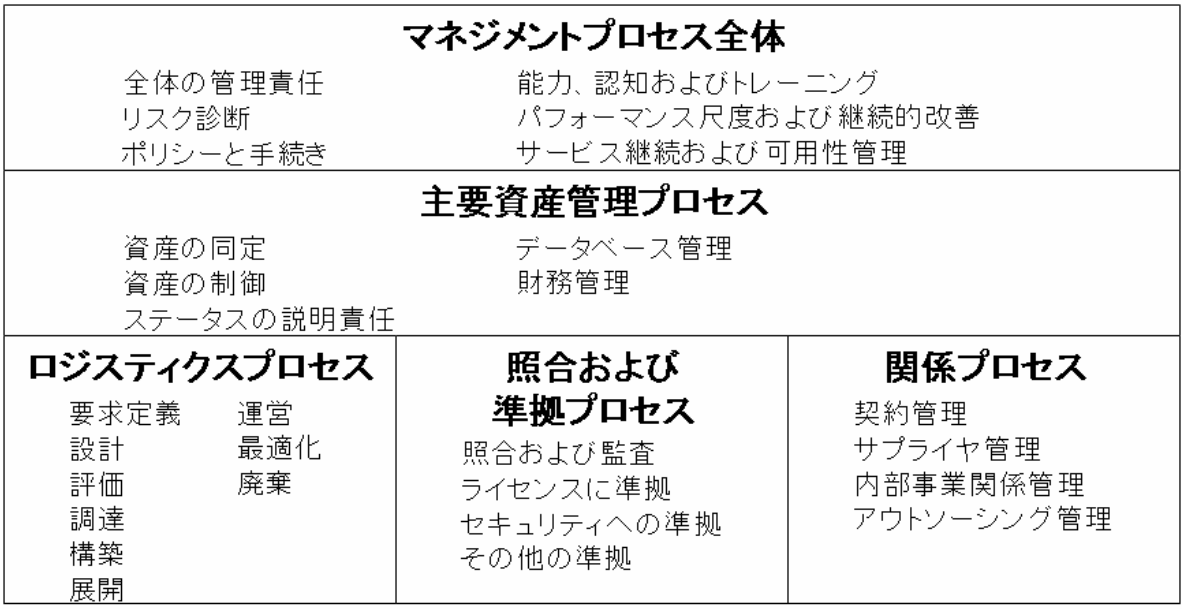
- **SAM データベース**：構成管理データベース（CMDB の一部）で、SAM 情報は正確で最新の状態を保つようにします。
- **定期的なレビューと改善**：定期的なレビューを実施し、影響する全てに対して改善活動を行います。



参考：Software Asset Management

図 F-1 SAM のアプローチ

ソフトウェア資産管理（SAM）は、図 F-2 のように大きく５つのプロセス領域で構成されています。



参考：Software Asset Management

図 F-2　SAM のプロセス

■マネジメントプロセス全体

他の SAM プロセスが導入されているところに、管理のインフラを確立し、維持する

■主要資産管理プロセス

ライフサイクル全体を通じて、ソフトウェア資産に関する情報を識別及び維持し、物理的な資産をソフトウェアに関連付けて管理する

■ロジスティクスプロセス

ライフサイクルに沿ったソフトウェアの推移に影響するすべての活動を制御する

■照合および準拠プロセス

SAM のポリシー、プロセス、手続き及びライセンスの使用権にかかる全ての例外を検知し、エスカレーションし、管理する

■関係プロセス

合意した契約、法的及び文書化したサービス期間と対象に対して、ビジネス内部及びパートナやサプライヤとの、全ての関係を管理する

参考：Software Asset Management　（TSO 刊）

付録 F.2　ISO19770 概説

ソフトウェア資産管理の国際標準 ISO/IEC 19770 は、以下の 2 つが検討されています。

- ISO/IEC 19770-1 Information technology - Software asset management - Part 1 Processes
- ISO/IEC 19770-2 Information technology - Software asset management - Part 2 Tagging

これらのうち ISO/IEC 19770-1 だけが、2006 年 5 月に国際標準として発行されました。ISO/IEC 19770-2 は現在審議中です。

ご注意

- 以降、特に断りのない限り ISO/IEC 19770-1 を ISO19770 と表記します。
- 以下は、規格の一部翻訳あるいはその要約を含みますが、情報提供を目的としたものであり、規格としての正確さを欠くものとお考えください。あくまでも原文のみが有効であり、本冊子での記述内容は参考にとどめてください。

ISO19770-1（プロセス：Processes）を取り上げ、その構成を見ていくことにしましょう。

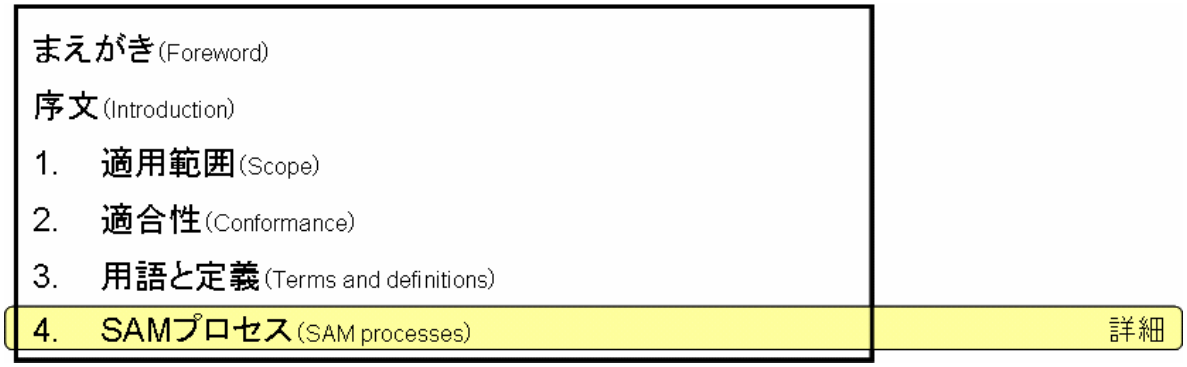


図 F-3　ISO197770 全体構成

ISO19770 の序文には、『この ISO/IEC 19770 第 1 部は ISO/IEC 20000 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。』とあります。つまり、ISO20000 ベースの IT サービスマネジメントが導入された企業に、ISO19770 のソフトウェア資産管理プロセスが矛盾なく導入できることを示しています。

1 章は適用範囲、2 章は適合性、3 章は用語とその定義、4 章が各プロセスについて書いてあります。4 章を中心に ISO19770 の SAM を概説します。

ソフトウェア資産管理のプロセスは、大きく以下の３つのカテゴリに分かれます。

a) SAM の組織管理プロセス
  - SAM の制御環境
  - SAM の計画立案及び導入プロセス

b) 中核 SAM プロセス
  - SAM の目録管理プロセス
  - SAM の検証及び順守プロセス
  - SAM の運用管理プロセス及びインタフェース

c) SAM の主プロセスインタフェース
  - SAM のライフサイクルプロセスインタフェース

カテゴリごとに、定義されているプロセスの目的を、表 F-1～表 F-3 に掲載します。

表 F-1　a) SAM の組織管理プロセスの概要

プロセス			目的
a) SAM の組織管理プロセス	SAM の制御環境	SAM の企業統治プロセス	SAM の管理責任を認識し、仕組みを作る
		SAM の役割及び責任	役割と責任が定義、維持、理解される
		SAM の方針，プロセス及び手順	有効な計画、運用、管理のためにポリシー、プロセス、手順を持つ
		SAM の能力	SAM における能力及び専門知識を確保、応用する
	SAM の計画立案及び導入プロセス	SAM の計画立案	SAM の有効で効率的な目的達成のための準備と計画を行う
		SAM の導入	SAM の目的及び計画全体を達成する
		SAM の監視及びレビュー	SAM の管理目的を達成する
		SAM の継続的改善	プロセスにおける改善点を特定し、措置をとる

表 F-2　b）中核 SAM プロセスの概要

プロセス			目的
b) 中核 SAM プロセス	SAM の目録管理プロセス	ソフトウェア資産の識別	資産が選択、分類され、効率的な管理のため適切な特性で定義する
		ソフトウェア資産の目録管理	ソフト資産を保管し、構成情報を記録し、情報活用のために提供する
		ソフトウェア資産の管理	コントロールの仕組みを提供し、状況の変化と許可を記録、保持する
	SAM の検証及び順守プロセス	ソフトウェア資産記録の検証	記録されるべきことが正確かつ完全に記録される
		ソフトウェアのライセンスの順守	他人所有の知的財産のライセンスが適切にライセンスされる
		ソフトウェア資産のセキュリティの順守	ソフト資産の使用に関するセキュリティ要件を守る
		SAM の適合性検証	ポリシーと手順への準拠と、継続的コンプライアンスを確保する
	SAM の運用管理プロセス及びインタフェース	SAM の関係及び契約管理	関連する全ての契約の管理のため、他組織との関係を管理する
		SAM の財務管理	ソフト資産の予算、会計、財務、税務、TCO、ROI などを準備する
		SAM のサービスレベル管理	SAM に関するサービスレベルを定義、記録、管理する
		SAM のセキュリティ管理	SAM 活動での情報セキュリティを管理し、承認要件を支援する

表 F-3　c) SAM の主プロセスインタフェースの概要

プロセス			目的
c) SAM の主プロセスインタフェース	SAM のライフサイクルプロセスインタフェース	変更管理プロセス	SAM に影響を及ぼす全変更を評価、承認、導入、レビュー、記録する
		取得プロセス	取得し、適切に記録する
		ソフトウェア開発プロセス	SAM の要件を考慮してソフトウェアを開発する
		ソフトウェアリリース管理プロセス	SAM の要件を満たすようリリースを計画し、実施する
		ソフトウェア展開プロセス	SAM の要件を満たすようソフトウェアを展開または、再展開する
		インシデント管理プロセス	ソフト資産の継続的運用におけるインシデントを監視し、対応する
		問題管理プロセス	根本問題の特定、インシデント原因のプロアクティブな識別と分析を行い、ソフト資産を最新及び運用に適した状態に保つ
		廃棄プロセス	ソフト資産の使用を中止する（リサイクルを含む）

参考：ISO/IEC 19770-1:2006　英和対訳版　（日本規格協会 刊）

付録 F.3　『ソフトウェア資産管理基準』『ソフトウェア資産管理評価規準』

『ソフトウェア資産管理基準』及び『ソフトウェア資産管理評価規準』は、ソフトウェア資産管理コンソーシアム（以下、SAMCon と略す）が策定する、ソフトウェア資産管理に関するガイドラインであり、以下を目的としています。

- 導入ソフトウェア資産の正確な把握や評価
- ライセンスコンプライアンス
- システムのセキュリティ対策
- IT 投資の有効活用

『ソフトウェア資産管理基準』

ソフトウェア資産管理基準とは、組織においてソフトウェア資産の管理をするために必要となる管理体制及び管理項目など「管理の枠組み」を定める基準です。この基準により組織におけるソフトウェア資産について何をどのように管理すべきか、という管理要件が明確になります。

『ソフトウェア資産管理評価規準』

ソフトウェア資産管理評価規準とは、ソフトウェア資産管理基準に基づき、成熟度モデルを利用して管理レベルを段階分けすることにより、適切に管理状態の把握と目標設定をするための指標となるものです。ソフトウェア資産管理基準によって明らかになった管理目標がどのレベルまで到達しているかについて、標準的な規準を示すものです。

『ソフトウェア資産管理基準』『ソフトウェア資産管理評価規準』は SAMCon のサイト（URL は参照に掲載）からダウンロードできます。これらの基準は、ISO20000 に関連してソフトウェア資産管理プロセスを構築する際の強力なガイドとなります。

参考：ソフトウェア資産管理コンソーシアム　http://www.samconsortium.org/

付録 G　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 G-1　ITIL と JIS Q 20000 用語比較

ISO/IEC 20000 原文	ITIL 用語	相違	JIS Q 20000
accounting	会計	⇔	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
back-out plan	切り戻し計画	⇔	リリース前の状態に戻す計画
baseline	ベースライン		ベースライン
budgeting	予算管理	⇔	予算業務
build	構築		構築
business objectives	事業達成目標	⇔	事業目的
business process	ビジネス・プロセス	⇔	事業プロセス
business relationship management	事業関係管理	⇔	顧客関係管理
business unit	事業単位		事業単位
capacity	キャパシティ	⇔	容量・能力
capacity management	キャパシティ管理	⇔	容量・能力管理
capacity plan	キャパシティ計画	⇔	容量・能力計画
categorization	カテゴリ化	⇔	分類
change	変更	⇔	変更、変化
change authority	変更許可委員	⇔	変更を認可する権限をもつ者
change control	変更コントロール	⇔	変更を制御する方法
change management	変更管理		変更管理
change record	変更レコード	⇔	変更記録
charging	課金	⇔	課金業務
classification	分類		分類
closure	クローズ	⇔	「終了」
code of practice	実施基準	⇔	実践のための規範
compliance	遵守性	⇔	順守
configuration	構成		構成
configuration audit	構成監査		構成監査
configuration baseline	構成ベースライン	⇔	構成(の)ベースライン
configuration control	構成コントロール	⇔	構成の管理
configuration identification	構成識別		構成識別
configuration item	構成アイテム	⇔	構成品目

configuration management	構成管理		構成管理
configuration management database	構成管理データベース		構成管理データベース
configuration management plan	構成管理計画	⇔	構成管理の計画
configuration status accounting	構成ステータスの説明	⇔	構成状態の説明
configuration verification	構成検証	⇔	構成の検証
contingency plan	緊急事態計画	⇔	不測の事態に対応する計画
contract	契約		契約
contract managers	契約マネージャ	⇔	契約の担当者
control	コントロール	⇔	制御、管理策、管理、統合的制御
cost	コスト	⇔	費用
cost effectiveness	費用対効果	⇔	費用と効果
cost model	原価モデル		原価モデル
customer	顧客		顧客
definitive software library	確定版ソフトウェアの保管庫	⇔	確定版ソフトウェアライブラリ
deliverable	成果物	⇔	提出書類
dependency	依存性		依存性
diagnosis	診断		診断
direct cost	直接費		直接費
disaster recovery	災害復旧		災害復旧
document	文書		文書
effectiveness	有効性		有効性
efficiency	効率性	⇔	効率
emergency change	非常時の変更	⇔	緊急の変更
environment	環境		環境
error	エラー	⇔	誤り
escalation	エスカレーション	⇔	段階的取扱い、経路
failure	障害		障害
fault	故障		故障
function	機能		機能
identification	識別	⇔	識別、(リスクの)特定、把握
impact	インパクト	⇔	影響
incident	インシデント		インシデント
incident categorization	インシデントのカテゴリ化	⇔	インシデントの分類
incident management	インシデント管理		インシデント管理
incident record	インシデント・レコード	⇔	インシデント記録
incident report	インシデント・レポート	⇔	インシデント報告書
indirect cost	間接費		間接費
information system	情報システム		情報システム
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
interface	インタフェース		インタフェース
job description	職務定義書		職務定義書
knowledge	ナレッジ	⇔	知識
knowledge base	ナレッジ・ベース	⇔	知識ベース
known error	既知のエラー	⇔	既知の誤り
known error record	既知のエラー・レコード	⇔	既知の誤りの記録

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	管理システム	⇔	・IT サービスマネジメントシステムを指す場合 「マネジメントシステム」 ・各項のシステムを指す場合 「～管理のシステム」 例： configuration management system = 構成管理のシステム
method	手法	⇔	方法
objective	目標	⇔	目的
operational	運用	⇔	運用(他訳有り)
operational level agreement	オペレーショナルレベル・アグリーメント	⇔	運用レベル合意書
overheads	オーバヘッド	⇔	間接工数
people	人材	⇔	人材、人員、要員
performance	パフォーマンス		パフォーマンス
post implementation review	導入後のレビュー		導入後のレビュー
priority	優先度		優先度
proactive problem management	プロアクティブな問題管理	⇔	事前予防的な問題管理
problem	問題		問題
problem management	問題管理		問題管理
problem record	問題レコード	⇔	問題に関する記録
procedure	手順		手順
process	プロセス		プロセス
process control	プロセス・コントロール	⇔	プロセス制御
process owner	プロセス・オーナ	⇔	プロセスの管理責任者
production environment	本番環境		本番環境
program	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	レコード	⇔	記録
recovery	復旧		復旧
relationship	関係		関係
release	リリース		リリース
release acceptance	リリースの受け入れ	⇔	リリースの受入れ
release management	リリース管理		リリース管理
release plan	リリース計画		リリース計画
release policy	リリース・ポリシー	⇔	リリース方針
release processes	リリース・プロセス	⇔	リリースプロセス
release record	リリース・レコード	⇔	リリース記録
reliability	信頼性		信頼性
request for change	変更要求		変更要求
request for service/service request	サービス要求		サービス要求
resolution	解決		解決
resolution process	解決プロセス		解決プロセス
restoration of service	サービスの回復		サービスの回復
review	レビュー		レビュー

risk	リスク		リスク
risk assessment	リスク評価	⇔	リスクアセスメント
role	役割		役割
roll-out	投入		投入
roll-out planning	投入計画立案	⇔	投入計画の立案
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	サービス受け入れ基準	⇔	サービス受入れ基準
service catalog	サービスカタログ		サービスカタログ
service definition	サービス定義	⇔	サービスの定義
service delivery	サービスデリバリ	⇔	サービス提供
service desk	サービスデスク		サービスデスク
service hours	サービス時間		サービス時間
service level agreement	サービスレベル・アグリーメント	⇔	サービスレベル合意書
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 provider	サービス・プロバイダ	⇔	サービス提供者
service support	サービスサポート	⇔	サービス支援
stakeholders	利害関係者		利害関係者
status accounting	ステータスの説明	⇔	状態の説明
strategic	戦略的		戦略的
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
task	タスク	⇔	業務
threshold	しきい値		しきい値
throughput	スループット	⇔	情報処理量
trend analysis	トレンド分析	⇔	傾向の分析
urgency	緊急度		緊急度
user	ユーザ	⇔	利用者
variant	バリアント	⇔	その派生
variance	差異		差異
verification	検証		検証
version	バージョン	⇔	版
work-around	ワークアラウンド	⇔	回避策
workloads	作業負荷		作業負荷

ITIL 用語出典『IT サービスマネジメント用語集　用語、頭字語、略語』（itSMF Japan 発行）

ＩＴＳＭＳ適合性評価制度技術専門部会

氏　名	所　属／役職
メンバー	
大畑　毅 【委員長】	日本電気㈱　マーケティング本部 グループマネージャ
黒崎　寛之 【副委員長】	㈱ヒルアビット 取締役
今井　政行	新日本監査法人　アドバイザリーサービス部 TSRS　シニアコンサルタント
熊谷　堅	KPMG ビジネスアシュアランス㈱ マネージャー
古賀　和子	NEC ラーニング㈱　IT・NW 研修本部 エキスパート
駒瀬　彰彦	㈱アズジェント 取締役　技術本部長
小山　明美	日本電気㈱　コンサルティング事業部 マネージャー
塩田　貞夫	日本ヒューレット・パッカード㈱ アドバンスソリューション部 ビジネスクリティカルコンサルタント
高橋　秀敏	(社)日本情報システム・ユーザー協会 主席研究員
土屋　慶三	ビーエスアイジャパン㈱　認証事業本部 ISMS/ITSM 技術部長
牧野　敬一朗	KPMG ビジネスアシュアランス㈱
丸山　満彦	監査法人トーマツ　エンタープライズ リスク サービス部 パートナー
オブザーバ	
荒川　博史	㈱ヒルアビット　営業部 部長
石川　浩	経済産業省　商務情報政策局 情報処理振興課　課長補佐
大石　知広	経済産業省　商務情報政策局 情報処理振興課　係長
小田　宏行	経済産業省　産業技術環境局 管理システム標準化推進室　工業標準専門職
島田　洋之	東京海上日動システムズ㈱ 常務取締役
金井　秀紀	経済産業省　商務情報政策局 情報セキュリティ政策室　技術係長
片山　博	ISMS 審査登録機関協議会（JISR） JISR 技術委員会　副委員長
郡司　明	経済産業省　産業技術環境局 標準企画室　工業標準専門職
三好　幸一	ISMS 審査登録機関協議会（JISR） JISR 技術委員会　委員長