システム管理基準（案）

経済産業省

令和５年Ｘ月Ｘ日

目次

前文（システム管理基準の活用にあたって） 1
Ⅰ. IT ガバナンス編 14
Ⅰ.1 IT ガバナンスの実践 15
Ⅰ.1.1 経営戦略とビジネスモデルの確認 15
Ⅰ.1.2 IT 戦略の策定 16
Ⅰ.1.3 効果的な IT パフォーマンスの確認と是正 17
Ⅰ.1.4 実行責任及び説明責任の明確化 18
Ⅰ.2. IT ガバナンス実践に必要な要件 19
Ⅰ.2.1 ステークホルダーへの対応 20
Ⅰ.2.2 取締役会等のリーダーシップ 20
Ⅰ.2.3 データ利活用と意思決定 21
Ⅰ.2.4 リスクの評価と対応 22
Ⅰ.2.5 社会的責任と持続性 23
Ⅱ. IT マネジメント編 25
Ⅱ.1 推進・管理体制 26
Ⅱ.1.1 体制と機能 26
Ⅱ.1.2 システムライフサイクルモデル管理 28
Ⅱ.1.3 IT アーキテクチャ管理 28
Ⅱ.1.4 資源配分管理 29
Ⅱ.1.5 品質管理体制 30
Ⅱ.1.6 知識資産管理 31
Ⅱ.2 プロジェクト管理 32
Ⅱ.2.1 プロジェクト計画の策定と承認 32
Ⅱ.2.2 プロジェクト実行と管理 32
Ⅱ.2.3 プロジェクト意思決定管理 33
Ⅱ.2.4 プロジェクトリスク管理 34
Ⅱ.2.5 調達管理 34
Ⅱ.2.6 外部委託管理 35
Ⅱ.2.7 構成・変更管理 36

Ⅱ.2.8　情報管理 37
Ⅱ.2.9　ドキュメント管理 38
Ⅱ.2.10　プロジェクトの生産性等の測定 39
Ⅱ.2.11　情報システムの品質保証 40
Ⅱ.3　企画プロセス 41
Ⅱ.3.1　ビジネス分析 41
Ⅱ.3.2　業務要件定義 42
Ⅱ.3.3　システム要件定義 42
Ⅱ.3.4　基本設計 43
Ⅱ.3.5　詳細設計 44
Ⅱ.3.6　実現可能性及び効果の分析 44
Ⅱ.4　開発プロセス 46
Ⅱ.4.1　実装 46
Ⅱ.4.2　統合 46
Ⅱ.4.3　検証 47
Ⅱ.4.4　ユーザ受入テスト 48
Ⅱ.4.5　本番環境への移行 48
Ⅱ.4.6　稼動後評価と報告 49
Ⅱ.5　運用プロセス 51
Ⅱ.5.1　運用体制の整備 51
Ⅱ.5.2　運用計画 51
Ⅱ.5.3　運用の実施 52
Ⅱ.5.4　運用における構成・変更管理 53
Ⅱ.5.5　インシデント・問題管理 54
Ⅱ.5.6　サービスレベル管理 55
Ⅱ.5.7　運用の監視と記録 56
Ⅱ.5.8　運用の評価と報告 56
Ⅱ.6　保守プロセス 58
Ⅱ.6.1　保守体制の整備 58
Ⅱ.6.2　保守計画 59

Ⅱ.6.3　保守作業の実施 60
Ⅱ.6.4　保守作業の検証 61
Ⅱ.6.5　本番環境への適用 62
Ⅱ.6.6　実施結果の記録と報告 63
Ⅱ.7.　廃棄プロセス 65
Ⅱ.7.1　廃棄計画 65
Ⅱ.7.2　廃棄の実施 66
Ⅱ.7.3　廃棄結果の検証 66
Ⅱ.8.　外部サービス管理 68
Ⅱ.8.1　外部サービス利用計画の策定 68
Ⅱ.8.2　外部サービスの選定と契約 68
Ⅱ.8.3　外部サービスの運用管理 69
Ⅱ.8.4　外部サービスの評価 70
Ⅱ.8.5　サービスレベル管理 71
Ⅱ.9.　事業継続管理 73
Ⅱ.9.1　リスクアセスメント 73
Ⅱ.9.2　業務継続計画の策定 74
Ⅱ.9.3　業務継続計画の管理 74
Ⅱ.9.4　訓練、演習及びテストの実施 75
Ⅱ.9.5　業務継続計画の評価及び見直し 76
Ⅱ.10　人的資源管理 76
Ⅱ.10.1　人的資源管理計画 76
Ⅱ.10.2　責任と権限の管理 77
Ⅱ.10.3　業務遂行の管理 78
Ⅱ.10.4　教育・訓練の管理 78
Ⅱ.10.5　健康管理 79
Ⅱ.10.6　要員のエンゲージメント向上 79

前文（システム管理基準の活用にあたって）

システム管理基準（以下、「基準」という。）は、平成16年のシステム監査基準の改訂において、システム監査基準の「実施基準」の主要部分を抜き出し、当時の情報技術の進展を踏まえて修正･追加を行うことによって、システム監査基準の姉妹編として策定された。その主旨は、システム監査とシステム管理の実践規範を明確に切り分けることによって、システム監査実践の独立性･客観性を明確に位置づけるとともに、システム監査の効率的･効果的遂行を可能にするための判断尺度として有効活用されることを企図するものであった。

また、平成30年の改訂においては、その後に生じた情報通信技術と情報化に関する大きな変化を踏まえて、第1に大企業のみならず中小企業においても情報システム化戦略、情報システム化の進展に関わる適切な自己診断及びシステム監査の実践を可能にすること、第2に情報システムにまつわるリスクを適切にコントロールしつつ、これまで以上にITガバナンスの実現に貢献することを企図して改訂が行われた。

・改訂の趣旨

今回の改訂においては、様々な組織において、データの利活用を含むITシステムの利活用によって、組織体の価値を向上させるサービス、製品及びプロセスを生み出し、改善する取組が加速するとともに、自社で保有する情報システムだけでなく、広く外部のサービスを利用して事業を推進する組織体が多くを占めるようになっている状況や、ボーダレスなIT環境を踏まえて、ITガバナンス及びITマネジメントに関わる国際規格の考え方や体系を取り入れるとともに、今後の組織体におけるITシステムの利活用の進展状況に対応しやすい内容とすることを企図し、ITガバナンス編とITマネジメント編から構成するようにした。

本基準において、「IT システムの利活用」には、IT の利活用だけではなく、データの利活用も含み、情報システムの計画、調達、外部委託、設計、統合、検証、移行、運用、保守及び廃棄、さらには、外部の IT サービスの利用も含ま

れる。このため、IT ガバナンス編では、これらを一括して「IT システムの利活用」と表現しているが、IT マネジメント編においては、これらの要素の一部について記述する必要もあるため、「情報システム」、「情報システムの構成要素」等の表現も使用している。

・システム管理基準ガイドラインとの関係

改訂前の「基準」は、本文、主旨、着眼点から構成されており、実践的な部分も含めていたが、今後の技術革新や社会情勢の変化等を踏まえて改訂が必要となる実践的な部分については、「基準」と切り離してシステム管理基準ガイドラインとすることにした。同ガイドラインについては、迅速なアップデートが可能とするためには、民間団体が策定し公表することとした。

このため、改訂後の「基準」においては、章及び節の冒頭で目的と範囲を説明し、それについて、「達成目標」と「ガバナンス活動の例」又は「管理活動の例」だけを示すことにした。「基準」を活用するための実践的な着眼点等については、民間団体が策定するシステム管理基準ガイドラインに委ねることとした。

「基準」は、ITシステムの利活用において共通して留意すべき事項を体系化･一般化してまとめたものであり、システム監査における監査人の判断の尺度として活用するだけではなく、取締役会等（監査役、監査（等）委員、理事、監事を含む）や経営者（最高経営執行責任者等）がITシステムの利活用のガバナンスあるいはマネジメントを行う上でも利用できるようにとりまとめたものである。

・「基準」の適用方法

「基準」の適用においては、「基準」に則って網羅的に項目を適用するような利用法は有効ではない。組織体の事業目的、事業分野における特性、組織体の業種・業態特性、ITシステムの利活用の特性などを踏まえて、「基準」で示した項目・内容の取捨選択・修正、関連する他の基準やガイドライン等からの必要項目の追加、用語の修正等を行い、システム監査及びITガバナンスやITマネジメントの主旨が実現できるように組織体に適した形にして、適用すること

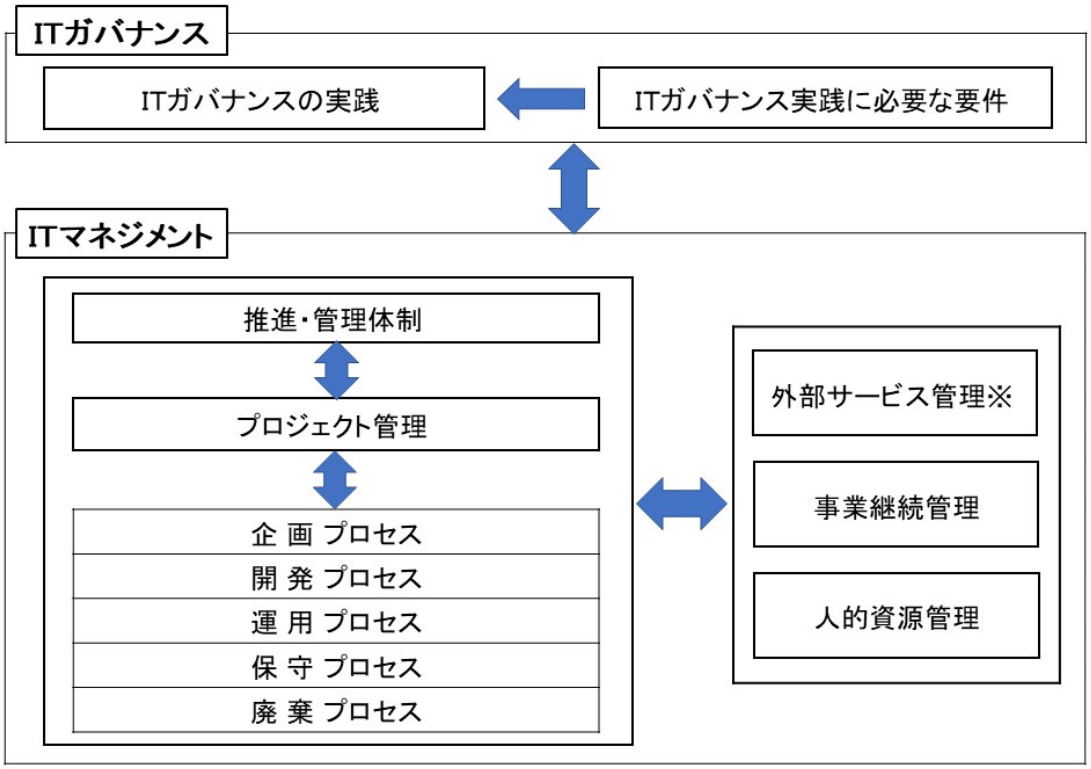
が望ましい。

また、情報セキュリティに関連する項目は、「情報セキュリティ管理基準（平成28年改正版）」（経済産業省）を参照していただきたい。

組織体独自の基準を策定する場合には、ITシステムの利活用に影響を与える情報技術の発展動向、関連する法令や規範の制定･改定状況、ITシステムの利活用の管理プロセスの要員の知識と技能の蓄積度などに絶えず注意を払い、定期的に項目の追加･削除などの修正を行うことによって、基準の有用性を高めることが必要である。

・「基準」の全体構成

本基準は､IT ガバナンス編と IT マネジメント編の 2 編から構成されており、全体構成は、以下に示すとおりである。



※「外部サービス管理」には、クラウドサービスの管理を含む。

・「基準」が想定する組織体の体制

「基準」が想定する組織体の体制を以下の図に示した。ここに､「取締役会等」とは､取締役会､理事会等の組織体のガバナンスを担う機関を意味し､「経営者」

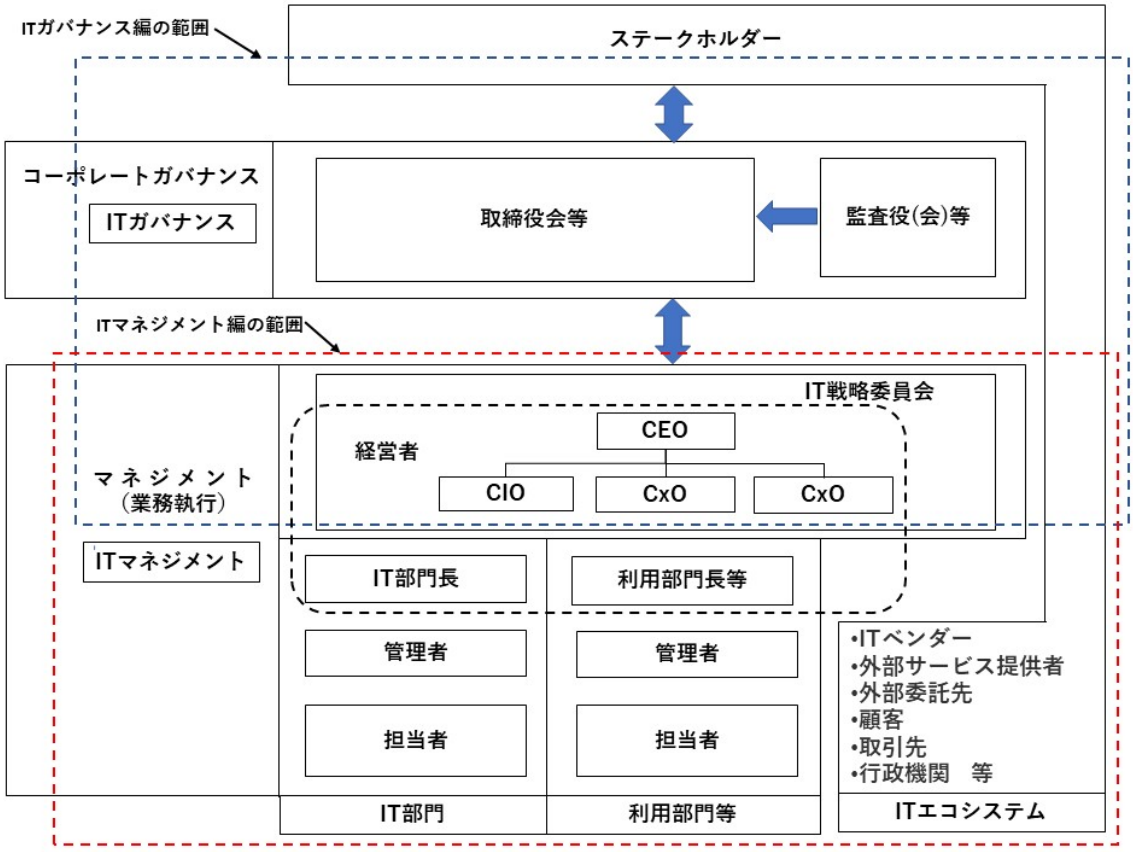
とは、最高経営責任者（CEO)、最高情報責任者（CIO）などの組織の業務執行責任を担う執行役員等を意味する。なお、改訂前の「基準」においては、取締役会等と業務執行責任を担う経営者を一括して「経営陣」と表現していたが、コーポレートガバナンスに関する認識の浸透状況を踏まえて、「取締役会等」と「経営者」を分けて示すこととした。

取締役会等が組織体の IT システムの利活用に関して責任を負う領域が IT ガバナンスであり、経営者が IT システムの利活用について責任を負う領域が IT マネジメントである。

取締役会等は、ステークホルダーのニーズに基づき IT ガバナンスを実践する実行責任と、ステークホルダーに対する IT ガバナンス全体の説明責任を負っており、組織体の目標を含む IT 戦略（IT ガバナンス方針と IT 基本計画）を示し、必要な実行組織の設置と適切な権限委譲を行い、経営者による実行状況のモニタリングを行う。なお、監査役（会）等は、取締役会等に対する監査を行う。

経営者は、取締役会等が設定した IT 戦略に基づいて目標を達成する実行責任と取締役会等に対する説明責任を負う。

IT ガバナンスの方針と戦略を示す責任は取締役会等にあるが、具体的な IT 戦略の策定等については、取締役会等が経営者に指示し、その内容を検討し承認することが通常と想定されるので、「基準」の IT ガバナンス編に含めて記載している。



なお、上図では、コーポレートガバナンスとマネジメント（業務執行）の役割の分離が行われていることを想定しており、「基準」もこれに従って定めている。そのため、取締役会等と経営者の役割が分離されていない組織の場合には、代表取締役等がITガバナンスとITマネジメントの両者の機能を担うことになるので、「基準」を利用する際に、自らの組織体に適合するように読み替えていただきたい。

(1) CIO

組織のITシステムの利活用から価値を得るためには、ITに関する専門的知識が求められることから、取締役会等はCIOを任命し、必要な権限を委譲する。

なお、小規模な組織、あるいはCEOが十分な専門的知識を有している場合にはCIOを任命しないことがある。その場合には、CEOが自らITマネジメントを統括する。

(2) 委員会（IT戦略委員会、プロジェクト運営委員会等）

IT戦略の策定や大規模プロジェクト等では組織体全体にまたがるステークホルダーの調整が必要となるため、IT戦略委員会、プロジェクト運営委員会等が設置される。CEOはCIOを含む複数のCxO、あるいは後述する部門長を含む委員会を組成し、必要な権限を委譲する。

なお、小規模な組織体、あるいは組織体内の調整が容易な場合には、既存の会議体を活用して、委員会を設置しないことがある。

(3) IT部門

ITマネジメントは取締役会等の指示に従って整備・運用するとともに、取締役会等によるモニタに必要な情報を提供する。組織体内でITマネジメントを担う部門を「IT部門」と呼ぶ。

IT部門は、IT部門長の下に、ITに関する企画、開発、運用、保守、廃棄を実施する管理者及び担当者で構成される。

組織によって、CIOがIT部門長を兼務することがある。

なお、小規模な組織では、マネジャー及び担当者が少数であり、IT部門長を任命しないことがある。

(4) 利用部門等

組織内において、IT部門以外の部門を「利用部門等」と呼ぶ。IT部門と同様、取締役会等は必要に応じてCxO及び利用部門長等を任命し、必要な権限を委譲する。

DX(Digital Transformation)推進のためにCDO(Chief Digital Officer)、DX推進部門等を設置している場合も見られるが、設置形態は様々であるのでCxO及び利用部門等に含むものとする。

(5) ITエコシステム

ITエコシステムは、他の組織と利用する共通のデジタル基盤やITサービス等であり、ITベンダ、外部サービス提供者、外部委託先、顧客、取引先、行政機関等のステークホルダーが関係する。

なお、ITガバナンスを有効に機能させるためには、ITマネジメントとITガバナンスの橋渡し役が必要であり、ISO/IEC TS38501（ITガバナンス：実装ガイド）においてはガバナンス運営グループ（Governance Steering Group）の設置を定めている。当該グループは、取締役会等によって任命されたCIO等のマ

ネジメントの責任者とメンバーから構成されるが、小規模な組織体では個人になることもある。そして、組織体の IT ガバナンスを効果的に推進する管理活動及び組織における変革プログラム活動の進捗の管理に責任を持ち、取締役会等による評価、指示及びモニタのために必要な関連情報を収集・調整し、適時に提供する機能を担う。

IT ガバナンスの枠組み

・IT ガバナンスの定義

IT ガバナンスとは、組織体のガバナンスの構成要素で、取締役会等がステークホルダーのニーズに基づき、組織体の価値及び組織体への信頼を向上させるために、組織体における IT システムの利活用のあるべき姿を示す IT 戦略と方針の策定及びその実現のための活動である。そのためには、データの利活用を含む IT システムの利活用により組織体の価値を向上させるサービスや製品、プロセスを生み出し、改善する組織体の能力（デジタル活用能力）が必要となる。

ここにいうデジタル活用能力とは、IT システムの利活用により組織体の価値を向上させるサービスや製品、プロセスを生み出し、改善する能力をいう。組織体の価値を向上させるサービス等の運用では、組織体内の関連する部門や IT エコシステムによるデジタルサービス等との連携が不可欠である。組織体における既存のデジタル活用能力と強化すべきデジタル活用能力を特定し、維持する継続的なプロセスが必要となる。また、IT エコシステムとは、他の組織体と利用する共通のデジタル基盤や IT サービス等であり、組織体の活動に有効で、顧客に価値を提供するサービスや製品、プロセスを支援するための仕組みである。

また、取締役会等は、IT ガバナンスを実践する上で、IT システムの利活用に係るリスクだけでなく、予算や人材といった資源の配分や、IT システムの利活用から得られる効果の実現にも十分に留意する必要がある。

・IT ガバナンスの達成目標

IT ガバナンスは、組織体のガバナンスの構成要素であるので、組織体のガバナンスの達成目標に関連して IT システムの利活用によって得られる達成目標が設定されることになる。

組織体におけるガバナンスの達成目標は、ステークホルダーに提供する付加価値の生成能力の向上、変化する状況下でネガティブな影響に対するレジリエンス（強靭性／回復力）とパフォーマンスの向上、意思決定効率の向上、ステークホルダーからの信頼の向上等、組織体としての価値向上に寄与することである。

IT ガバナンスの達成目標は、組織体のガバナンスの達成目標に関連させて、以下のような達成目標が設定される。

(1)　効果的な IT パフォーマンスの実現

IT パフォーマンスとは IT システムの利活用による成果のことである。IT システムの利活用によりビジネス成果の達成を効果的に支援するためには、組織体の状況とステークホルダーのニーズに基づく、明確なパフォーマンスの期待値の設定が不可欠である。具体的な達成目標の例は、以下のとおりである。

- 組織体の目標を達成することを可能にする、又は支援するための組織体のデジタル活用能力の整備の程度
- 組織体に必要なデジタル活用能力と変革のレベルに応じた IT システムの利活用への適切な投資
- IT システムの利活用により向上した組織体の価値及び信頼の度合い
- データの利活用によって組織体とそのステークホルダーの意思決定にもたらした改善効果とデータの利活用に要したコストとの度合い
- 獲得した組織体のデジタル活用能力によって実現されたビジネス機会による利益、対処された潜在的なリスク、法律等の新たな義務に対応できるようになった度合い

(2)　責任ある IT 資源管理の実施

組織体が責任ある方法で IT 資源管理を実施することによって、組織体に対するステークホルダーの信頼向上に寄与する。組織体の管理下にある資源には、組織体のデジタル活用能力のほか、組織体が作成したデータや組織体外からのデータが含まれており、自動化された意思決定が合理的かつ公正であること、

データが適切に保護され使用されることへの配慮が必要である。具体的な達成目標の例は、以下のとおりである。

・IT システムの利活用におけるセキュリティと障害等に対するレジリエンスの確保

・組織体のデジタル活用能力によって実現するサービスや製品等において、リスクへの対応や法令遵守等の観点から、適切な意思決定がなされていることの明確化

・透明性、説明可能性、影響評価など、変化するステークホルダーのニーズへの対応

(3)　組織体における倫理的行動の確保

取締役会等が、IT ガバナンスの原則を遵守してガバナンス活動を実施することによって、組織体の倫理的な行動を推進することができる。具体的な達成目標の例は、以下のとおりである。

・データを含む IT 資源に関する所有権、使用権及び機密性の保持、並びに関連する規則等を遵守した行動等

・IT パフォーマンス及び IT 資源の管理等について、IT マネジメントによる正確で適時な報告の徹底

・IT ガバナンスにおける取締役会等の活動

IT ガバナンスにおける取締役会等の活動は、ステークホルダーへの対応及び IT マネジメントとそのプロセスに対する評価、指示、モニタから構成される。各活動の内容は、下表のとおりである。

取締役会等の活動	活動の内容
ステークホルダーへの対応 （Engage Stakeholders）	組織体の IT システムの利活用に関連するステークホルダーを特定し、協議し、そのニーズを明確にして対応すること
評価（Evaluate）	組織体における IT システムの利活用についての現在と将来のあるべき姿を比較分析し、IT マネジメントに期待する効果と必要な資源、想定されるリスク等を評

	価し、判断すること
指示（Direct）	IT戦略と方針を実現するために必要な責任と資源等を組織体内へ割り当て、期待する効果（ITパフォーマンスの期待値を含む）を示し、その実現と想定されるリスクへの対処を指示し、ITマネジメントの実践を指示すること
モニタ（Monitor）	ITシステムの利活用について、IT戦略で設定した目標をどの程度満たしているか、IT方針を遵守しているか、ITパフォーマンスをどの程度達成しているか、また想定したリスクの発現状況及び対処状況について、適切な仕組みを通じて、ITパフォーマンスの情報を収集し、確認すること

・ITガバナンスに関する基準の構成

IT ガバナンスに関する基準は、IT ガバナンスにおける取締役会等の活動と達成目標を踏まえて、以下の 2 種類のプロセスに分類した。

プロセスの分類	プロセスの内容
取締役会等によるITガバナンスの実践のための直接的な活動	1. ITガバナンスの実践 1.1　経営戦略とビジネスモデルの確認 1.2　IT戦略の策定 1.3　効果的なITパフォーマンスの確認と是正 1.4　実行責任及び説明責任の明確化
ITガバナンスの実践を支える活動	2. ITガバナンスの実践に必要な要件 2.1　ステークホルダーへの対応 2.2　取締役会等のリーダーシップ 2.3　データ利活用と意思決定 2.4　リスクの評価と対応 2.5　社会的責任と持続性

IT マネジメントの枠組み

・IT ガバナンス編と IT マネジメント編との関係

既に述べたように、経営者は、取締役会等が設定した IT ガバナンスの方針と戦略に基づいて目標を達成する実行責任と取締役会等に対する説明責任を負っている。そこで、経営者は、経営方針及び IT ガバナンス方針に基づいて策定した IT 戦略の各目標を達成するために、IT システムの利活用に関するコントロールを実行し、その結果としてのパフォーマンス、コスト管理、リスク管理、コンプライアンス管理、社会的責任と持続性等の状況を経営者に報告するための体制を整備・運用することが必要となる。

IT 戦略の策定及び取締役会等から経営者に対して指示する事項については、IT ガバナンス編に記載しており、IT マネジメント編では、これらに基づいて IT システムの利活用に関する統制を実行するための達成目標と管理活動の例を記載している。

・システムライフサイクルプロセスとの関係

IT マネジメントに関する基準は、JIS X 0170（システムライフサイクルプロセス）に記載されているプロセスの区分を参考にして作成した。これは、JIS X 0170 の元となっている ISO/IEC/IEEE 15288：2015 をベースにして、セキュリティ・バイ・デザインの実装、ディペンダビリティマネジメント（開放系総合信頼性）などの規格も作成されており、今後の「基準」の適用領域の拡張性を考慮したものである。

システムライフサイクルプロセスにおけるライフサイクルモデルとは、システムの企画から廃棄までの過程をいくつかの段階に分類し、それぞれの段階で発生する工程を一般化して整理したものである。分類の方法は様々であるが、「基準」では、企画、開発、運用、保守、廃棄の各プロセスに分類し、さらに細分化したサブプロセス毎に基準を示した。改訂前の「基準」においては、「フェーズ」いう表現を用いており、順を追ってフェーズが進行するウォーターフォールモデルをイメージされ易かったが、各サブプロセスの順序は固定されたものではないので、「プロセス」という表現に改めた。

特に情報システムの企画・開発工程の進め方については、実務上様々な方法があるが、プロセスモデルとして、以下の３種類に分類される。

① 定義された要件等に従って順を追って開発するモデル（例：ウォーターフォールモデル）

② 漸進的に進化しつつ開発するモデル（例：スパイラルモデル）

③ 短期開発サイクルの繰り返しによって徐々に開発するモデル（例：アジャイル開発モデル）

また、自ら情報システムを企画・開発するのではなく、パッケージソフトやSaaS（アプリケーションソフトウェアをクラウドサービスによって利用する形態）を利用して情報システムを導入するケースも存在する。

「基準」では、システムライフサイクルにおける基本となる活動に基づいて細分化したプロセス毎に記載しているため、その組み合わせによって、様々なプロセスモデルや情報システムの導入形態に応用可能である。ただし、システム監査の実践においては、これらのプロセスモデルや導入形態に対応した固有の留意点等も存在するため、テーマ別のガイドラインの策定・公表を民間団体で行うことを計画している。

・IT マネジメントに関する基準の構成

IT マネジメントに関する基準は、適用対象の違いにより、下表のとおり、プロセスを 4 種類に分類して記載している。システム監査における判断基準として利用する際には、監査対象とするプロセスの範囲や監査テーマに合わせて、取捨選択・修正して活用していただきたい。

プロセスの分類	プロセスの名称
IT 部門の組織全体に係るプロセス	1.推進・管理体制
システムの企画・開発プロジェクトの管理に係るプロセス	2.プロジェクト管理
システムライフサイクルプロセスの遂行に係るプロセス	3.企画プロセス 4.開発プロセス 5.運用プロセス

	6.保守プロセス 7.廃棄プロセス
IT部門以外の部門のマネジメントとの関連が深いプロセス	8.外部サービス管理 9.事業継続管理 10.人的資源管理

Ⅰ．ITガバナンス編

Ⅰ.1　IT ガバナンスの実践

ステークホルダーのニーズに基づき、組織体の価値及び組織体への信頼度を向上させるために、組織体における IT システムの利活用のあるべき姿を示す IT 戦略を策定し、組織体の IT に関するパフォーマンスを含めた IT ガバナンスの状況を確認して必要な是正措置を指示することによって、組織体の目標を達成する。

Ⅰ.1.1　経営戦略とビジネスモデルの確認

組織体の目的（パーパス）を実現するためのビジネスモデルと、それを実現するための経営戦略を支援するための IT 戦略ビジョンを策定する。

なお、ビジネスモデルとは、組織体が、顧客や社会に価値を提供し、持続的に価値を向上させていくビジネスの仕組みのことをいう。

＜達成目標＞

1. 組織体を取り巻く自然環境、社会的・経済的な状況に応じて、組織体の目的を達成するための経営戦略とビジネスモデルと達成すべきビジネス成果が明確にされ、組織体全体に周知されている。
2. 経営戦略とビジネスモデルを実現するための IT の役割と重要性が認識されている。
3. 経営戦略とビジネスモデルを実現するための IT 戦略ビジョンが策定されている。
4. IT ソリューションや新技術等が経営戦略とビジネスモデルに及ぼす影響が定期的に評価され、経営戦略とビジネスモデルについて、必要な見直しを行っている。

＜ガバナンス活動の例＞

1. （IT 戦略ビジョンの策定）経営戦略とビジネスモデルにおける IT の役割を明確にし、組織体の IT 戦略ビジョンを策定する。
2. （ビジネス成果の設定）IT 戦略ビジョンでは、経営戦略とビジネスモデルにより達成すべきビジネス成果を設定する。

3. （ステークホルダーのニーズの反映）IT 戦略ビジョンには、ステークホルダーのニーズを反映する。
4. （新技術等の定期的評価）新しい IT ソリューションや新技術が IT 戦略ビジョンに及ぼす影響を定期的に評価する。
5. （市場変化の定期的評価）市場の変化が経営戦略とビジネスモデルに及ぼす影響を定期的に評価する。
6. （IT 戦略ビジョン等の見直し）事業環境等の評価を実施し、その結果に基づいて、ビジネスモデルと IT 戦略ビジョンの見直しを行う。

Ⅰ.1.2 IT 戦略の策定

組織体における IT システムの利活用のあるべき姿を示す IT 戦略を策定し、それに基づいて IT マネジメントの責任者に指示する。

＜達成目標＞

1. 取締役会等の意図と期待を明確にした IT 戦略（IT ガバナンス方針と IT 基本計画）が策定されている。
2. IT ガバナンス方針には、ビジネス成果を実現するための IT 戦略の達成目標が設定されている。
3. IT 戦略の実現に必要となる組織体のデジタル活用能力を確保するための戦略と計画が策定されている。
4. IT 戦略において、IT ソリューションの劣化や陳腐化に対処するための戦略と、将来に向けた IT に関する適切な方向性が示されている。

＜ガバナンス活動の例＞

1. （IT 戦略の策定）IT 戦略に関する取締役会等の意図と期待を明確にした IT ガバナンス方針と IT 基本計画を策定する。
2. （IT 戦略策定の権限委譲）経営者に権限委譲して IT 戦略を策定する。
3. （IT 戦略の評価と承認）策定された IT 戦略は、取締役会等が内容を評価し承認する。
4. （IT 戦略の見直し）組織体を取り巻く環境変化を評価し、その結果に基づ

いて、IT 戦略を見直す。

5. （IT ガバナンス方針）IT ガバナンス方針では、次の事項を明確にする。
   (1) ビジネス成果の実現と結び付けられた IT 戦略の達成目標の設定
   (2) IT ガバナンスの体制、責任及び権限
   (3) IT 投資の方針
   (4) IT 資源の調達と IT 人材の育成・確保に関する方針
   (5) IT システムの利活用に関わるリスク評価に基づく IT リスクマネジメントの方針
   (6) データ利活用の役割と意思決定に関する方針
   (7) 新しいソリューションや新技術の定期的な影響評価に基づく、技術の陳腐化等に対処するための方向性
6. （IT 基本計画）IT 基本計画では、次の事項を明確にする。
   (1) 組織体の現在のニーズと将来的なニーズへの対応
   (2) IT システムの利活用に関わるステークホルダーの特定と、そのニーズの反映
   (3) 組織体のデジタル活用能力の駆使による組織体の価値の向上
   (4) IT 戦略の目標達成状況を評価するための開発計画等におけるパフォーマンスの期待値と IT エコシステムの選定基準の設定

Ⅰ.1.3 効果的な IT パフォーマンスの確認と是正

組織体の IT パフォーマンスが、取締役会等の意図や期待、倫理的行動、コンプライアンス上の義務を満足していることを確認するために、IT パフォーマンスの状況を適時確認して、必要な是正措置を指示する。

＜達成目標＞

1. 取締役会等によって組織体の IT パフォーマンスが評価され、必要な是正措置が指示され、IT パフォーマンスが管理されている。
2. 取締役会等の意思決定を支援するとともに、意思決定の透明性を確保するための取締役会等への情報提供のプロセスが整備されている。
3. 組織体の活動において、IT に関連する法令・規制・ガイドライン、契約、

組織体の倫理規程、社内規程などが計画的に遵守されている。

4. IT に関連した法令・規制・ガイドライン、契約、組織体の倫理規程、社内規程など遵守において重大な違反があった場合には、取締役会等に適時に報告されている。

＜ガバナンス活動の例＞

1. （IT ガバナンスの実践状況の確認）IT ガバナンス方針に従って、IT ガバナンスが実践されていることを確認する。
2. （IT ガバナンス方針遵守の確認）新たな技術を利活用することに伴う権限委譲と責任の割り当てが、IT ガバナンス方針に従って実施されていることを確認する。
3. （IT パフォーマンス管理の仕組みの構築）組織体の IT パフォーマンスの管理の仕組みを構築するよう指示する。
4. （外部の専門家による評価）組織体の IT パフォーマンスの評価が直接確認できない場合には、外部の専門家等による第三者評価を利用するよう指示する。
5. （コンプライアンス違反等の報告）IT に関連した規制、契約及びコンプライアンスの遵守における重大な違反があった場合は、取締役会等にその情報を報告する。
6. （ビジネスリスクの報告）IT に関連して発生しうるビジネス上のリスクについて、正確な情報を把握し、取締役会等に報告する。
7. （IT 戦略の達成状況の評価及び是正）IT 戦略の達成目標の状況を評価したうえで、IT 戦略の内容について適宜是正措置を指示する。
8. （技術のライフサイクル管理）新しい技術の導入から、古くなった技術やデータの破棄まで、技術のライフサイクルにわたって評価し管理するよう指示する。

Ⅰ.1.4　実行責任及び説明責任の明確化

組織体全体及びステークホルダーに対する実行責任及び説明責任は取締役会等が有しており、これらの責任を果たすために、取締役会等は主体的に責任を

もって行動する。

＜達成目標＞

1. IT ガバナンスに関する実行責任及び説明責任は、権限委譲の有無にかかわらず、取締役会等にあることを明確にしている。
2. ITに関連する意思決定の構造及びパフォーマンスの確認体制は、経営者、IT 部門及び利用部門が関与しており、権限はそれを行使するのに最適な立場にある者に委譲されている。
3. IT ガバナンスの実践が適切であり、IT システムの利活用に関する統制が適切であることを、取締役会等が評価している。
4. 経営者は、取締役会等が設定した IT 戦略に従って、目標を達成する実行責任と取締役会等に対する説明責任を負っている。

＜ガバナンス活動の例＞

1. （権限委譲における責任の所在）権限を委譲しても、委譲した者に責任があることを認識し、委譲された者の責任の範囲について明確にする。
2. （権限を委譲された者の責任）権限を委譲された者が、実行責任及び説明責任を果たせるように権限委譲を行う。
3. （情報開示）組織体の目的及び経営戦略とビジネスモデルに関連させて、IT 戦略ビジョン、IT 戦略について、外部に情報を開示する。
4. （IT ガバナンスの保証）内部監査や外部監査等を用いて、IT ガバナンスの仕組みが有効に機能していることを評価することにより、IT ガバナンスの妥当性を保証する。
5. （IT システムの利活用に関する責任の明確化）IT サービスの提供と利活用に関する実行責任と説明責任を明確にする。

Ⅰ.2. IT ガバナンス実践に必要な要件

IT ガバナンスの実践により、優れた成果を挙げるためには、IT ガバナンス活動を支えるための、ステークホルダーへの対応、取締役会等のリーダーシップ、データ利活用と意思決定、リスクの評価と対応、社会的責任と持続性等の要件

を整える必要がある。

Ⅰ.2.1　ステークホルダーへの対応

ステークホルダーのニーズを考慮した IT ガバナンスを実践するために、ステークホルダーと良好な関係を構築する。

＜達成目標＞

1. ステークホルダーに対して、計画的で適切な対応が実践されている。
2. 組織体のビジネスモデル及び IT 戦略は、ステークホルダー中心のアプローチによって、ステークホルダーのニーズと整合がとられている。
3. 組織体の IT 戦略に対するステークホルダーの満足度が高い。

＜ガバナンス活動の例＞

1. （ステークホルダーの特定及び対応）組織体の IT システムの利活用に関連するステークホルダーを特定して、ステークホルダーと協議し、適切に対応する。
2. （ステークホルダーのニーズの把握及び対応）ステークホルダーのニーズをビジネスの目標に結び付け、さらに望ましい IT 投資に反映させる。
3. （ステークホルダーの満足度の評価）主要なステークホルダーの満足度を評価する仕組みの構築を指示する。

Ⅰ.2.2　取締役会等のリーダーシップ

組織体の変革や倫理規範の遵守のために、取締役会等が率先して倫理的な行動を実践するとともに、効果的な指導を通じてリーダーシップを発揮する。

＜達成目標＞

1. リーダーシップの発揮によって、組織体変革のレベル、複雑さ及び変革のスピードに対応した IT による変革能力が備わった組織づくりが行われている。
2. リーダーシップの発揮によって、IT サービスの取得や変更に柔軟に対応

し、IT システムを利活用した組織体の変革が推進されている。

3. リーダーシップの発揮によって、組織体の目標を達成するために、将来ニーズに対応した新たな技術やスキルを獲得する学習文化が醸成されている。

＜ガバナンス活動の例＞

1. （パフォーマンスの目標値の設定）組織体全体としてのパフォーマンスの目標値の設定について、リーダーシップを発揮する。
2. （倫理的規範の策定と遵守）取締役会等がリーダーシップを発揮して、倫理規範を策定するとともに、取締役会等が率先して倫理規範を遵守する。
3. （組織体の変革の推進）組織体の変革に必要なビジネス及びデジタル活用能力を向上するようにリーダーシップを発揮する。
4. （IT 知識の継続的改善）社会や組織体からの要求に応えられるように、取締役会等が自らの IT 知識を継続的に向上させ、リーダーシップの発揮につなげる。
5. （新たな技術等への対応）戦略的な意思決定とそのパフォーマンスについて、ステークホルダーに対する説明責任を果たすために、継続的に新たな技術やスキルに対応するようにリーダーシップを発揮する。

Ⅰ.2.3 データ利活用と意思決定

データが、意思決定のための価値のある経営資源であることを組織体に認識させるために、データ利活用に関する方針等を策定し、周知する。

＜達成目標＞

1. データが製品、サービス、価値の創出など、組織体のあらゆる側面で利活用され、組織体の目標に対する価値の提供について、組織体全体に周知されている。また、データ利活用に際して考慮すべきリスク及び遵守すべき法規制等が明らかにされている。
2. IT ガバナンス方針で示されたデータの利活用の意義、役割及び管理方針が組織体全体に周知されている。

3. データが、プライバシーや著作権等の遵守、利活用目的への適合、必要な品質要件等を満足し、盗難、破損、不正使用から保護されている。
4. 必要なデータの品質要件が理解され、データがその要件に適合するための仕組みが整備されている。

＜ガバナンス活動の例＞

1. （データ利活用の周知及び関連法規の明確化）データが価値ある経営資源であることを組織体内に周知し、データの利活用を推進するとともに、データ利活用に関わる法規制を明らかにする。
2. （データ利活用のリスクへの対応）データ利活用に関するリスクは、組織体のリスク管理のフレームワークの範囲に収まるよう指示する。
3. （意思決定のための適切なデータ利活用）意思決定において、データを適切に利活用するために、データの適切な分類、分類に従った配付、保護、処理するよう指示する。
4. （倫理的なデータ利活用のための方針の策定）データを倫理的に利活用するための方針等を策定する。

Ⅰ.2.4　リスクの評価と対応

組織体の目的及び IT 戦略の目標を達成するために、達成に及ぼす影響についてリスクを評価し、対応を行う。

＜達成目標＞

1. IT システムの利活用に関連する重要なリスクが認識され、速やかに対応されている。
2. IT システムの利活用に関して、組織体が受容できるリスクのレベルが明確にされ、管理されている。
3. 組織体内外の障害等に対応し、IT サービス等のレジリエンスが確保できるよう対策されている。
4. IT システムの利活用に関する事業継続に関する方針が策定されている。

＜ガバナンス活動の例＞

1. （リスクの認識及び管理プロセスの確認）IT システムの利活用に関する重要なリスクを常に認識し、リスク管理が実施されていることを確認する。
2. （リスク対応とステークホルダーへの伝達）組織体が継続的にリスクを検知し、それに対応し、必要な対応策を関係するステークホルダーに伝える。
3. （IT リスク管理方針の開示及び IT サービスのレジリエンスの確保）組織体の目的を果たし、戦略的目標を確実に達成するために、IT リスク管理に関する組織体の方針を示すとともに、提供している IT サービス等のレジリエンスの確保を指示する。
4. （事業継続方針の策定）IT システムの利活用に関する事業継続の方針を策定する。

Ⅰ.2.5　社会的責任と持続性

組織体が存続し、長期に成果を挙げ続けるために、IT システムの利活用に関する組織体の意思決定の透明性を確保し、より広範な社会的期待に応え、現在及び将来のステークホルダーのニーズを満足させるように組織体のデジタル活用能力を維持・向上させる。

＜達成目標＞

1. IT に関する意思決定を適切に行うため、本編に示した基準と整合する方針が策定され、意思決定の結果に対して組織体内での責任者が明確にされている。
2. IT を用いた自動的な意思決定のリスクを評価し、それに基づいて対策が講じられている。
3. ステークホルダーのニーズに応える上で有効な IT エコシステムが構築されている。
4. IT ガバナンス方針とその実践により、IT に関するリスクが増大する環境であっても、事業活動とデータが確実に保護されている。

＜ガバナンス活動の例＞

1. （ステークホルダーのニーズに関するリスクの特定）ステークホルダーのITに関するニーズに影響を与えるリスクを特定し、リスクの内容とITシステムの利活用によるビジネスチャンスを明確にする。
2. （IT エコシステムへの適切な対応）組織体が長期にわたって持続的発展を行うために、組織体が利用しているITエコシステムのニーズを理解し、適時かつ効果的に対応する。
3. （自動的な意思決定への対応）ITを用いた自動的な意思決定については、その透明性を確保し、意図しない結果が生じた場合には、適切に対処する仕組みを構築して、社会的責任を果たすようにする。
4. （サービス品質の維持）IT システムの利活用によって必要な品質要件を満たすサービスの提供を維持し、組織体の目的と目標の達成に貢献する。
5. （ITサービスのレジリエンス確保）ビジネス機能がITに依存していることを認識して、提供するITサービスのレジリエンスを確保する。
6. （倫理的行動）組織体の IT システムの利活用は、倫理規範を遵守して行うとともに、ステークホルダーや経済・自然環境に悪影響を与えることがないように配慮する。

Ⅱ．ITマネジメント編

Ⅱ.1　推進・管理体制

Ⅱ.1.1　体制と機能

経営方針及びITガバナンス方針に基づいて策定したIT戦略の各目標を達成するために、ITシステムの利活用に関するコントロールを実行し、その結果としてのパフォーマンス、コスト管理、リスク管理、コンプライアンス管理、社会的責任と持続性等の状況を経営者に報告するための体制を整備・運用する。

＜達成目標＞

1. 経営者の承認を得て、組織体の規模及び特性に応じたIT部門の体制が構築されている。
2. IT戦略に関わる意思決定を支援するための情報を経営者に提供されている。
3. ITシステムの利活用に関する技術の動向に対応するための体制が整備・運用されている。
4. ITシステムの利活用に関するパフォーマンスとコストに関する実行状況をモニタリングし、必要な是正措置が講じられている。
5. データ利活用の推進と管理のための体制が整備・運用されている。
6. ITシステムの利活用に関するリスク管理のための体制が整備・運用されている。
7. ITシステムの利活用に関する法令及び規制の遵守のための体制が整備・運用されている。
8. ITシステムの利活用に関する社会的責任を果たし、持続性を維持するための体制が整備・運用されている。
9. ITシステムの利活用に関わるパフォーマンス、コスト管理、リスク管理、コンプライアンス管理、社会的責任と持続性等の状況が経営者に報告されている。

＜管理活動の例＞

1. （IT 部門の体制整備）経営者の承認を得て、組織体の規模及び特性に応じて、IT 部門における職務の分離、専門化、権限付与、外部委託等を考慮した体制を整備する。
2. （委員会等の設置）経営者の IT 戦略の計画･実行･評価に関わる意思決定に必要な情報を提供するために、組織体内の部門をまたがる委員会等を設置し運営する。
3. （関係者の満足度調査）経営者の IT 戦略に関する組織体内外の関係者に対する満足度調査を実施する。
4. （技術採用指針等）IT システムの利活用に関する技術の変化に対応するため、技術情報を収集・分析し、技術採用指針等を明確にする。
5. （IT システムの利活用の目標設定と実績評価）組織体における IT システムの利活用に関わるパフォーマンスとコストに関する目標設定と実績評価の方法を定め、その実行状況をモニタリングすることによって、必要な是正措置を講じる。
6. （データ利活用の推進と管理）データ利活用の推進、リスクへの対応、倫理的なデータ利活用等の方法を定め、定期的な見直しと改善を行う。
7. （IT システムの利活用のリスク管理）IT システムの利活用に関するリスク管理の方法を定め、リスクの識別・評価とリスクへの対応を行い、定期的な見直しと改善を行う。
8. （IT システムの利活用のコンプライアンス管理）IT システムの利活用に関する法令及び規制等の遵守のための方針と手続を定め、遵守状況をモニタリングし、必要な是正措置を講じる。
9. （IT システムの利活用の行動基準等）行動基準等において IT システムの利活用に関する遵守事項を定め、関係者への教育及び周知を行い、遵守状況を確認する。
10. （IT システムの利活用の経営者への報告）IT システムの利活用に関わるパフォーマンス、コスト管理、リスク管理、コンプライアンス管理、社会的責任と持続性等の状況について、報告の内容と頻度を定め、経営者へ状況を報告する。

Ⅱ.1.2　システムライフサイクルモデル管理

IT 戦略に従って、目標に適合した手順と方法で情報システムを構築、運用するためのシステムライフサイクルモデルを作成、適用するとともに、そのモデルを評価し改善する。

＜達成目標＞

1. システムライフサイクルモデルに従って管理するための方針と体制が確立され運用されている。
2. システムライフサイクルモデルの適切性の評価方法が確立され、これに基づいて評価が行われている。
3. 評価の結果明らかになったシステムライフサイクルモデルの課題は、優先順位を付けて改善されている。

＜管理活動の例＞

1. （システムライフサイクルモデルに従った管理の方針と体制）システムライフサイクルモデルに従った管理の方針、手続及び管理体制を定めて、関係者に周知する。
2. （プロセスモデルの選択適用）企画・開発プロセスの進め方に関するウォーターフォールモデル、スパイラルモデル、アジャイル開発モデル等の選択適用の方針、手続及び管理体制を定めて、関係者に周知する。
3. （システムライフサイクルモデル等に従った管理の定期的評価）システムライフサイクルモデル及びプロセスモデルに従った管理の状況を定期的に評価する。
4. （システムライフサイクルモデル等に従った管理の改善措置）システムライフサイクルモデルに従った管理の評価結果から明らかになった課題を、優先順位を付けて改善する。

Ⅱ.1.3　IT アーキテクチャ管理

組織体の情報システム全体の整合性を保って、情報システムを構築・運用するために必要な IT アーキテクチャを定め、IT 基盤を利用可能にする。

＜達成目標＞

1. 組織体の情報システム全体の整合性を確保できる IT アーキテクチャが定められている。
2. 構築・運用する情報システムの目的に基づいて IT 基盤に対する要求事項が定義されている。
3. 要求事項を満たすための IT 基盤の構成要素が明らかにされている。
4. IT 基盤の各要素が必要な時期に利用可能な状態になっている。

＜管理活動の例＞

1. （IT アーキテクチャの管理)組織体全体の IT アーキテクチャを明確にし、周知する。
2. （IT 基盤の構成要素）対象とする情報システムの目的に適した IT 基盤の構成要素を、種類や用途等の要件を基に漏れなく明らかにする。
3. （IT 基盤の導入計画）IT 基盤の導入計画を策定し、これに従って IT 基盤を利用可能にする。
4. （IT 基盤の定期的評価）IT 基盤が情報システムの目的どおり利用されているかについて、定期的に評価する。
5. （IT 基盤の変化に応じた更新）運用開始後の情報システムの目的や環境の変化に応じて、必要な更新を行う。

Ⅱ.1.4 資源配分管理

経営資源を有効に活用するために、プロジェクトに優先順位を付けて資源配分を行う。

＜達成目標＞

1. プロジェクトの評価方法が定められ、これに従ってプロジェクトが定期的に評価されている。
2. 評価結果に基づいてプロジェクトに優先順位が付けられ、それに応じて資源配分が管理されている。

＜管理活動の例＞

1. （プロジェクトの評価方法の確立）IT戦略に従ってプロジェクトの時期、投資額、必要性等を評価するための方法を確立する。
2. （プロジェクト全体の定期的評価）プロジェクトの開始前を含めて、組織体におけるプロジェクト全体を定期的に評価して、優先順位を見直す。
3. （優先順位に応じた経営資源の配分）プロジェクトの優先順位に応じて経営資源を配分する。
4. （貢献度や利用度による判断）組織体の価値創出への貢献度や利用度による評価が低い情報システムに関する廃止プロジェクトの検討を行う。

Ⅱ.1.5　品質管理体制

利用者が満足する製品やサービスを提供するために、最適な品質管理体制を整備・運用する。

＜達成目標＞

1. 情報システムの品質目標を定め、これを達成するための体制が確立されている。
2. 情報システムの品質評価の基準、測定方法及び実施手順が定められている。
3. 情報システムの品質評価結果が分析されている。
4. 評価結果に基づいてシステムが改善されている。

＜管理活動の例＞

1. （品質目標の設定）情報システムの品質目標を設定する。
2. （品質管理の役割と責任）品質管理の体制における役割と責任の所在を明確にし、評価対象部門から独立した専門性のある人員を配置する。
3. （実施手順等の制定）品質評価の基準、測定方法及び実施手順を定める。
4. （品質評価の定期的実施と改善）品質評価を定期的に実施し、必要な改善を行う。

Ⅱ.1.6　知識資産管理

個別に得た知識、技能を基に、組織体として知識資産を蓄積し有効利用するために、知識資産を再利用可能な状態で管理する。

＜達成目標＞

1. 知識、技能等を知識資産として蓄積し、利用可能な状態になっている。
2. 蓄積した知識や技能等の利用状況を分析して利用を促進するために再編成されている。
3. 対象とする知識、技能、及び知識資産の管理方法を定期的に見直されている。

＜管理活動の例＞

1. （知識管理対象の整理）管理対象とする知識、技能を漏れなく特定し、知識資産として利用しやすい形に整理する。
2. （知識管理対象の保護）管理対象とする知識、技能を保護する。
3. （知識等の活用体制）蓄積した知識、技能等の知識資産を組織体として利用する体制を整備する。
4. （知識等の定期的棚卸）管理されている知識、技能等の知識資産の棚卸を定期的に行い、管理方法について必要な見直しを行う。

Ⅱ.2　プロジェクト管理

Ⅱ.2.1　プロジェクト計画の策定と承認

プロジェクト目標を確実に達成するために、効果的・効率的で実行可能なプロジェクト計画を策定し、権限者の承認を得るとともに、プロジェクトの関係者と情報共有する。

＜達成目標＞

1. IT戦略に従ってプロジェクトの目標が設定され､計画が策定されている。
2. プロジェクトの関係者の役割、責任及び権限が定められている。
3. プロジェクトの実施に必要な内部資源及び外部資源が確保されている。
4. プロジェクト計画の承認後､適時に実施を開始するための準備が行われている。

＜管理活動の例＞

1. （プロジェクトの目的､対象業務､効果）IT戦略に従ってプロジェクトの目的、対象業務、期待される効果を明確にする。
2. （プロジェクトの体制）プロジェクトマネージャ（PM）等、プロジェクトに必要な体制を整備する。
3. （プロジェクト計画）プロジェクトのスケジュール、リソース（要員スキル・作業工数、予算）等を定めたプロジェクト計画を整備する。
4. （プロジェクトの実行の準備）プロジェクト計画の承認後に、適時にプロジェクトを開始できるよう準備する。

Ⅱ.2.2　プロジェクト実行と管理

プロジェクト計画に基づいて、プロジェクトの品質、納期、予算を守りながら､プロジェクトを実行する｡また､プロジェクト進捗状況をモニタリングし、プロジェクトを確実に遂行する。

＜達成目標＞

1. プロジェクトの進捗や品質等のモニタリング手法及び評価手法が明確にされている。
2. プロジェクトの責任者にプロジェクトの進捗や品質等のモニタリング及び評価状況が報告されるとともに、必要に応じて関係者と情報共有されている。
3. プロジェクトの進捗状況等の評価に基づいて、必要な対応が行われている。
4. プロジェクト目標の達成状況が評価されている。

＜管理活動の例＞

1. （プロジェクト管理標準）プロジェクトをモニタリング・管理するための体系化されたプロジェクト管理標準を定める。
2. （プロジェクトのモニタリングと評価）プロジェクト標準に基づき、定期的及び重要なマイルストーンにおける実績をモニタリング・評価する。
3. （プロジェクトの是正処置、再計画）定期的又は重要なマイルストーンにおける実績の評価結果に基づき、必要な是正処置に関する方向づけやプロジェクト計画の見直しを実施する。
4. （プロジェクトの終結の確認）プロジェクト計画における全てのプロセスの完了を確認することによって、プロジェクトの終結を確認する。

Ⅱ.2.3　プロジェクト意思決定管理

組織体にとって最も有益なプロジェクトを選択するために、プロジェクトの開始、中止、変更、続行の意思決定を管理する。

＜達成目標＞

1. 意思決定のために必要な評価方針や評価基準が明確にされている。
2. 評価基準、評価方針に従って代替案を比較・評価し、意思決定が行われている。
3. 思決定の根拠及び前提が明確にされている。

＜管理活動の例＞

1. （意思決定の方針と手続）意思決定のために必要な評価項目、選定基準等を定めて、意思決定に関する組織体の方針及び手続を確立する。
2. （情報の比較と分析）意思決定に関する組織体の方針及び手続に従って、代替案を含めて比較、分析する。
3. （意思決定結果の記録とその活用）意思決定の根拠、前提及び結果を記録して、今後の意思決定に活用する。

Ⅱ.2.4 プロジェクトリスク管理

プロジェクトの円滑な遂行のために、プロジェクトリスクを継続的に評価して必要な対応を行う。

＜達成目標＞

1. プロジェクトリスクが特定され、リスク評価結果に基づいて優先順位付けされた対応策が実施されている。
2. プロジェクトリスクの変化及び対応策の実施状況が継続的にモニタリングされ、必要な対応が行われている。

＜管理活動の例＞

1. （リスクの特定）プロジェクトリスクを特定する。
2. （リスク評価）プロジェクトリスクを評価し、優先順位付けして対応する。
3. （リスクのモニタリング）プロジェクトリスクをモニタリングし、リスクの変化に応じて必要な対応を行う。

Ⅱ.2.5 調達管理

プロジェクトの要求内容を満足する製品・サービスを取得するための調達手続を明確にし、それに基づいて調達を実施する。

なお、外部委託を行う場合は「Ⅱ.2.6 外部委託管理」を、クラウドサービスを含む外部サービスを利用する場合は「Ⅱ.8 外部サービス管理」の項を参照のこと。

＜達成目標＞

1. IT 戦略に基づいて、製品・サービスが調達されている。
2. 調達の実施に関する判断基準が明確にされている。
3. プロジェクトの要求内容（品質・コスト・納期）を満足する製品・サービスが選定されている。
4. 調達先との間で調達内容に関する契約が締結されている。
5. 契約に基づいて製品・サービスを納入されている。
6. 契約に基づいて支払等の調達先に対する義務が果たされている。

＜管理活動の例＞

1. （IT 戦略との整合）製品・サービスの調達計画が IT 戦略と整合していることを確認する。
2. （調達管理手続）調達する製品・サービスに関する選定基準・選定方法を含む調達手続を定める。
3. （調達先選定）調達手続に基づいて、プロジェクトの要求内容（品質・コスト・納期）を満たした製品・サービスが選定され、履行能力を満たした調達先が選定されていることを契約前に確認する。
4. （契約の締結）調達手続に基づいて、調達先と契約が締結されていることを確認する。
5. （実施状況のモニタリング）契約内容の実施状況をモニタリングし、必要な対応を実施する。
6. （検収手続）契約に基づいた製品・サービスが納品されたことを検収する。

Ⅱ.2.6　外部委託管理

プロジェクトの要求内容を満たす外部委託業務の提供を受けるために、外部委託管理手続を明確にし、それに基づいて外部委託を実施する。

＜達成目標＞

1. IT 戦略に基づいて外部委託業務が利用されている。
2. 外部委託業務の調達に関する判断基準が明確にされている。

3. プロジェクトの要求内容（品質・コスト・納期）を満足した外部委託サービスが選定され、履行能力を満たした調達先が選定されている。
4. 調達先との間で契約が締結されている。
5. 契約に基づいて外部委託業務が提供されている。
6. 契約に基づいて支払等の外部委託先に対する義務が果たされている。

＜管理活動の例＞

1. （IT 戦略計画との整合）IT 戦略に基づいて外部委託利用計画を策定する。
2. （外部委託管理手続）外部委託先の選定基準・方法を含む外部委託管理手続を定める。
3. （外部委託先の選定）外部委託管理手続に基づいてプロジェクトの要求内容（品質・コスト・納期）を満足する外部委託業務を複数の外部委託先候補から選定する。
4. （契約の締結）外部委託管理手続に基づいて外部委託管理先と契約を締結する。
5. （外部委託契約の維持）外部委託契約の実施状況を評価し、外部委託契約に基づいて外部委託が行われるように維持する。
6. （検収手続）外部委託契約に基づいて検収を実施し、成果物を受け入れる。

Ⅱ.2.7　構成・変更管理

プロジェクトの手戻りや中断を最小限に抑えるために、情報システムの構成要素（ハードウェア、ソフトウェア、ネットワーク、外部サービス、施設・区域、公開ドメイン等）の変更について、構成要素間の整合性を確保するとともに、変更履歴を管理する。

＜達成目標＞

1. 情報システムの構成要素として管理する対象範囲を定め、ルール化されている。
2. 変更前後の情報システムの構成要素を構成管理情報として明確にし、管理されている。

3. プロジェクトの関係者が構成管理情報を検索・閲覧できるように管理されている。
4. 構成管理情報の正確性が検証されている。
5. 情報システムの構成要素の変更は、承認に基づいてリリースされている。

＜管理活動の例＞

1. （構成管理の計画）情報システムの構成要素に関する情報の収集・保存・管理計画を策定する。
2. （構成管理台帳等の作成）情報システムの構成要素について、管理台帳等を作成し、閲覧できるようにする。
3. （変更管理）情報システムの構成要素の変更について、承認等の管理を行う。
4. （管理台帳等の更新）変更内容に基づいて、管理台帳等を更新する。
5. （検証と是正措置）管理台帳等の内容と、本番環境等（実環境）との整合性を検証し、必要な是正措置を行う。
6. （変更手続）情報システムの構成要素の変更は、定められた手続に則り、本番環境等へリリースする。

Ⅱ.2.8 情報管理

プロジェクトの関係者が必要とするタイミングで必要な情報を利用できるように、管理対象の情報を維持管理する。

＜達成目標＞

1. 管理対象の情報や情報項目が明確にされている。
2. 情報の管理体制及び管理手続が明確にされている。
3. 情報の重要性や機密性に応じた情報セキュリティ対策が講じられている。
4. 情報は、指定されたプロジェクトの関係者だけが利用可能になっている。

＜管理活動の例＞

1. （管理対象明確化）管理対象とする情報や情報項目を明確にする。

2. （情報の管理体制）情報の管理体制を整備する。
3. （情報の管理手続）情報の管理手続を定める。
4. （情報の維持管理）情報の管理手続に従って、情報を維持、保管、廃棄する。
5. （情報セキュリティ対策）情報セキュリティ対策を講じて、その実施状況及び有効性を確認する。
6. （体制手続の見直し）情報の管理体制及び管理手続は、定期的又は環境変化等に対応して見直しを行う。

Ⅱ.2.9　ドキュメント管理

プロジェクト全般でドキュメントを円滑に利用可能にするために、管理対象とするドキュメントを明確にして、整備・維持管理する。

＜達成目標＞

1. 管理対象ドキュメントが明確にされている。
2. 管理対象ドキュメントの形式及びドキュメントの状態を識別する方法が明確にされている。
3. 管理対象ドキュメントの整備・維持管理に関する体制及び手続が定められている。
4. 管理対象ドキュメントについて、その重要性及び機密性に応じたセキュリティ対策が講じられている。
5. 管理対象ドキュメントは、指定されたプロジェクトの関係者だけが利用可能な状態になっている。

＜管理活動の例＞

1. （管理対象明確化）管理対象とするドキュメントを明確にする。
2. （ドキュメントの管理体制）ドキュメントの管理体制を整備する。
3. （ドキュメントの管理計画）ドキュメントの管理計画を策定する。
4. （ドキュメントの管理手続）ドキュメントの管理手続を定め、それに従って整備する。

5. （ドキュメントの改訂）ドキュメントの管理手続に従って、ドキュメントを改訂する。
6. （ドキュメントの保管）ドキュメントの管理手続に従って、ドキュメントを保管する。
7. （ドキュメントの廃棄・消去）不必要となったドキュメント（改訂等に伴い無効となったドキュメント、妥当性が確認できないドキュメントを含む）は適切に廃棄・消去する。
8. （情報セキュリティ対策）ドキュメントに関する情報セキュリティ対策の実施状況及び有効性を確認している。
9. （計画及び手続の見直し）ドキュメントの管理体制、管理計画、管理手続は、定期的又は環境変化等に対応して見直しを行う。

Ⅱ.2.10 プロジェクトの生産性等の測定

IT ガバナンス及び情報システムの開発・運用・保守の将来に役立てるため、生産性、ユーザ満足度、リスク管理等に関する客観的なデータ及び情報を収集・分析し、関係者に報告する。

＜達成目標＞

1. IT 戦略、関係者の要請等を踏まえて、組織体の情報ニーズ（測定の目的、目標、必要性）と、それに基づく測定の対象が明らかにされている。
2. 必要なデータが収集・分析・蓄積されている。
3. 分析結果がわかりやすく説明されており、意思決定に役立てられている。

＜管理活動の例＞

1. （測定活動の方針及び手続）組織体の情報ニーズに基づいて、測定活動の方針及び手続を定め、関係者へ周知する。
2. （測定結果の伝達）測定活動を適切な作業工程へ組み込んで実施し、その結果を文書で関係者へ伝える。
3. （測定活動の評価及び改善）測定活動の方針及び手続等を評価し、必要な測定活動の改善を図る。

Ⅱ.2.11　情報システムの品質保証

情報システムに求められる品質を確保するために、定められた品質管理手順に従って品質を管理し､プロジェクトにおける情報システムの品質を保証する。

＜達成目標＞

1. 品質保証のための評価の基準及び手順が定められている。
2. 評価の基準及び手順に従って情報システムの品質を評価することによって、品質が保証されている。
3. プロジェクトの関係者へ評価結果が伝えられている。
4. 品質が満足できない場合には、必要な是正措置が実施されている。

＜管理活動の例＞

1. （品質保証計画）品質管理方針・手順に基づいて、プロジェクトに合わせて調整した品質保証計画を策定する。
2. （要件への適合性の評価）業務要件及びシステム要件への適合性を評価し、必要な対応を行う。
3. （システム開発業務の評価）システム開発の手順に基づいて、システム開発業務を適切に進めているかどうかについて評価する。
4. （品質保証の記録と報告）品質保証の結果をプロジェクトの関係者へ報告するとともに、必要な対応を行い、品質保証の記録を保管する。

Ⅱ.3　企画プロセス

経営戦略及び IT 戦略で定められた目標を達成するため必要な情報システムの開発体制を整備し、ビジネスモデル及び業務要件を明確にして、設計作業を行う。

Ⅱ.3.1　ビジネス分析

利用部門等及び IT 部門が連携して、利用者の立場からビジネス分析を実施して、あるべきビジネスモデルを設定する。ビジネス分析の結果明らかになった問題を解決し、分析結果を有益に生かすことができるような、システムソリューション(業務要件を満たすためのシステム導入による解決策)を選定する。

＜達成目標＞

1. あるべきビジネスモデル及び業務プロセスが明確にされている。
2. あるべきビジネスモデル及び業務プロセスによって生じる問題やメリットが明確にされている。
3. システムソリューションの候補が特定されている。
4. あるべきビジネスモデルの実現可能性及び効果を分析して、システムソリューションの候補が選定されている。

＜管理活動の例＞

1. （現状分析）現状のビジネスモデル及び業務プロセスを分析する。
2. （将来像の明確化）あるべきビジネスモデル及び業務プロセスを明確にする。
3. （システムソリューション候補の特定）あるべきビジネスモデル及び業務プロセスに対応するためのシステムソリューションの候補を特定する。
4. （システムソリューション候補の評価）特定したシステムソリューションの候補を評価する。
5. （ビジネス分析の文書化と承認）ビジネス分析の結果を文書化し、承認を得る。

Ⅱ.3.2　業務要件定義

あるべきビジネスモデル及び業務プロセスを踏まえて選定したシステムソリューションを実現し、利用者及び関係者の要求を満足するシステムを提供できるように、業務要件を明確にする。

＜達成目標＞

1. 情報システムの利用者及び関係者が特定されている。
2. 利用者及び関係者のシステム機能に対する要望が明確にされ、優先順位付けされている。
3. 優先順位付けされた要望が業務要件として明確にされ、利用者及び関係者と合意されている。

＜管理活動の例＞

1. （業務要件定義の準備）利用者及び関係者を特定し、業務要件定義の準備をする。
2. （要望の整理）利用者及び関係者のシステム機能に対する要望を収集・分析・調整する。
3. （業務要件の優先順位付け）業務要件の優先順位付けの適切性をレビューする。
4. （業務要件定義の文書化と承認）業務要件定義の成果を文書化し、承認を得る。

Ⅱ.3.3　システム要件定義

業務要件を満たすために必要となる技術的な検討事項を明確にする。

＜達成目標＞

1. システム要件（範囲、機能、遂行能力・性能、運用要件、プロセス、非機能及びインターフェース要件）及び設計上の制約が明確にされている。
2. 重要な情報システムの遂行能力・性能・稼動率等の実績の測定量が明確にされている。

3. 必要に応じて実現可能性及び効果の分析を実施し、システム要件の実現可能性が立証されている。

＜管理活動の例＞

1. （システム要件定義の計画）システム要件定義の範囲と内容を明確にして、スケジュールを調整する。
2. （システム要件の整理）システム要件を整理するための業務要件を収集・分析・調整する。
3. （開発方針の策定）システム要件の優先順位付けの適切性をレビューし、開発方針を策定する。
4. （システム要件定義の文書化と承認）システム要件定義の結果を文書化し、承認を得る。

Ⅱ.3.4 基本設計

システム要件を満たすために必要なシステムアーキテクチャを決定し、具体化する。

＜達成目標＞

1. 全てのシステム要件がシステムアーキテクチャに対応付けられている。
2. システムアーキテクチャの決定のために重要な機能又は制約が明確にされている。
3. 関連する情報システム及び情報システムの構成要素間のインターフェースが特定されている。
4. システムアーキテクチャの候補が分析・評価され、適切なものが選定されている。

＜管理活動の例＞

1. （基本設計の計画）基本設計の範囲と内容を明確にし、スケジュールを調整する。

2. （システムアーキテクチャの整理）システムアーキテクチャの概念、性質、特性、振る舞い、インターフェースを分析・整理する。
3. （システムアーキテクチャの選定）システムアーキテクチャの選定結果の適切性をレビューする。
4. （基本設計の文書化と承認）基本設計の結果を文書化し、承認を得る。

Ⅱ.3.5 詳細設計

基本設計に基づいた実装を可能にするために、情報システムの構成要素を具体化する。

＜達成目標＞

1. 情報システムの全ての構成要素が明確にされている。
2. 全てのシステム要件が情報システムの構成要素に割り当てられている。
3. 関連する情報システム及び情報システムの構成要素間のインターフェースが具体化されている。
4. 情報システムの構成要素に関する代替案が評価されている。

＜管理活動の例＞

1. （詳細設計の計画）詳細設計の範囲と内容を明確にして、スケジュールを調整する。
2. （詳細設計の整理）情報システムの全ての構成要素を分析・調整し、レビューする
3. （詳細設計の文書化と承認）詳細設計の結果を文書化し、承認を得る。
4. （テスト要件の文書化と承認）テスト要件を文書化し、承認を得る。

Ⅱ.3.6 実現可能性及び効果の分析

システムライフサイクル全体を判断するための根拠情報とするために、概念実証（PoC)、技術実証（PoT）の他、各種の分析を実施する。

＜達成目標＞

1. 実現可能性及び効果の分析の実施目的が明確にされている。

2. 実現可能性及び効果の分析の前提条件及び結果の妥当性が確認され、その結果が経営者に報告されている。

＜管理活動の例＞

1. （評価基準）実現可能性及び効果の分析の評価手法及び判断基準を定める。

2. （文書化）実現可能性及び効果の分析結果を文書化し、承認を得る。

Ⅱ.4　開発プロセス

利用者及び関係者の要望に沿った情報システムを実現するために、情報システムの構成要素の開発作業を行い、稼動後評価及び報告を行う。

Ⅱ.4.1　実装

設計に沿った情報システムを実現するために、全ての情報システムの構成要素を導入し、必要な設定を実施する。

＜達成目標＞

1. 情報システムの構成要素の実装に必要な作業及び制約が明確にされている。
2. 情報システムの全ての構成要素が動作可能になっている。

＜管理活動の例＞

1. （実装の計画）実装に必要な作業を明確にし、スケジュールを調整する。
2. （実装結果のレビュー）情報システムの全ての構成要素が設計を満足していることを示す裏付けを入手し、レビューする。
3. （実装結果の記録と不具合の改善）実装の結果及び実装に際して発生した不具合及びその改善結果を記録し、不具合の改善状況をフォローアップする。
4. （構成・変更管理への情報提供）構成・変更管理プロセスに、情報システムの全ての構成要素に関する情報を連携する。

Ⅱ.4.2　統合

システム要件及びシステムアーキテクチャを満たす情報システムを実現するために、情報システムの全ての構成要素を段階的に組み立て、利用可能にする。

＜達成目標＞

1. 情報システムの全て構成要素の統合に必要な作業及び制約が明確にされている。

2. 情報システムの全ての構成要素が段階的に統合され、一体として動作可能になっている。

＜管理活動の例＞

1. （統合の計画）統合に必要な作業を明確にし、スケジュールを調整する。
2. （統合結果のレビュー）統合された情報システムが設計を満足することを示す裏付けを入手し、レビューする。
3. （統合結果の記録と不具合の改善）統合の結果及び統合に際して発生した不具合及びその改善結果を記録し、不具合の改善状況をフォローアップする。
4. （構成・変更管理への情報提供）構成・変更管理プロセスに、情報システムの全ての構成要素に関する情報を連携する。

Ⅱ.4.3　検証

情報システム及び情報システムの全ての構成要素が、システム要件を適切に反映していることを確認するために、中間成果物も含めてレビューする。

＜達成目標＞

1. 実装及び統合された情報システムについて、システム要件が満足されている。
2. 検証で発見された不具合が適切に管理されている。

＜管理活動の例＞

1. （検証の計画）検証の範囲、手順、関連システム及びサービス、及び制約を明確にし、スケジュールを調整する。
2. （検証結果のレビュー）システム要件を反映していることを示す裏付けを入手し、レビューする。
3. （検証結果の文書化と承認）検証結果を文書化し、承認を得る。
4. （不具合の改善）検証で発見された不具合及び改善結果を記録し、不具合の改善状況をフォローアップする。

Ⅱ.4.4　ユーザ受入テスト

業務要件を情報システムに適切に反映していることを確認するために、利用者の立場からテストする。

＜達成目標＞

1. 実装及び統合された情報システムについて、業務要件が満足されている。
2. ユーザ受入テストで発見された不具合が適切に改善されている。

＜管理活動の例＞

1. （ユーザ受入テスト計画）ユーザ受入テストの範囲、手順、関連システム及びサービス、及び制約を明確にし、スケジュールを調整する。
2. （ユーザ受入テスト結果のレビュー）情報システムが業務要件を充足していることを示す裏付けを入手し、レビューする。
3. （ユーザ受入テスト結果の文書化と承認）ユーザ受入テストの結果を文書化し、承認を得る。
4. （不具合の改善）ユーザ受入テストで発見された不具合及び改善結果を記録し、不具合の改善状況をフォローアップする。

Ⅱ.4.5　本番環境への移行

利用者が情報システムを利用できるようにするために、情報システムを本番環境で稼動させる。

＜達成目標＞

1. 本番へ移行するために、必要な全ての作業、データ、制約、関連システムが利用可能な状態になっている。
2. 移行で発見された不具合が適切に改善されている。

＜管理活動の例＞

1. （移行の計画）移行の対象となる情報システム、関連システム及びサービス、データ、施設について、必要な変更箇所、手順、制約を特定し、判定基準及びスケジュールを調整する。
2. （移行結果のレビュー）移行が完了したことを示す裏付けを入手し、レビューする。
3. （移行結果の文書化と承認）移行結果を文書化し、承認を得る。
4. （不具合の改善）移行で発見された不具合及び改善結果を記録し、改善状況をフォローアップする。
5. （構成・変更管理への情報提供）構成・変更管理プロセスに、移行で変更された全てのシステムの構成要素に関する情報を提供する。

Ⅱ.4.6 稼動後評価と報告

情報システムがIT戦略における目標を達成していることを確認するために、客観的な情報を提供する。

＜達成目標＞

1. 情報システムがあるべきビジネスモデル及び業務プロセスを実現していることを示す客観的な情報が提供されている。
2. 期待される目標を達成していない場合、改善策が明確にされている。
3. 定量的な目標だけでなく、定性的な目標についても客観的な証拠が提供されている。

＜管理活動の例＞

1. （稼動後評価の計画）稼動後評価の範囲、手順、関連システム及びサービス、及び制約を明確にし、スケジュールを調整する。
2. （稼動後評価結果のレビュー）情報システムが目標を達成していることを示す裏付けを入手し、レビューする。
3. （稼動後評価結果の文書化と承認）稼動後評価結果を文書化し、承認を得る。

4. （問題の改善）稼動後評価で発見された問題及び改善結果を記録し、問題の改善状況をフォローアップする。

Ⅱ.5　運用プロセス

組織体の方針及び要求事項に沿ったサービスを提供するために、情報システムの運用体制を整備して運用を実施し、その監視、検証及び報告を行う。

Ⅱ.5.1　運用体制の整備

運用に必要なリソースを提供できるようにするために、情報システムの運用管理の方針及び体制を整備する。

＜達成目標＞

1. 運用管理の方針が確立され、利用者及び関係者に周知されている。
2. 運用管理者の役割、責任が明確にされている。
3. 必要かつ十分な力量を備えた要員を運用に従事させている。

＜管理活動の例＞

1. （運用管理の方針）組織体の方針に従った運用管理の方針を明確にする。
2. （運用管理の考慮事項）運用を実行するために必要な方法、スケジュール、リソース等の考慮事項を明確にする。
3. （運用管理者の役割と責任）運用管理者の役割と責任を明確にする。
4. （運用管理の情報の文書化）運用管理に必要な情報を文書化し、周知する。
5. （運用担当者に必要な力量）運用担当者に必要な力量を明確にする。
6. （運用担当者の選定基準）運用担当者の選定基準を明確にする。
7. （運用担当者の育成プログラム）運用担当者が必要な力量を得るための育成プログラムを作成する。

Ⅱ.5.2　運用計画

運用管理の方針及び運用設計に基づいて運用するための運用計画を策定する。

＜達成目標＞

1. 運用管理の方針及び運用設計に基づいて運用計画が策定されている。
2. 運用計画において、管理すべきリスクが明確にされている。

3. 運用の実施に必要な情報システム又はサービスが識別され、利用可能な状態になっている。

＜管理活動の例＞

1. （運用計画）運用管理の方針、目的及び開発プロセスで作成した運用設計に基づいて、年次、月次、週次、日次等の運用計画を策定する。
2. （リスク及び制約の識別）運用計画において、対策が必要なリスク及び制約が明確にされている。
3. （運用支援システムの導入計画）運用に必要な運用支援システムを明確にして、導入する。
4. （運用の継続計画）システムの可用性が低下した場合に備えて、運用の継続計画を策定する。

Ⅱ.5.3　運用の実施

情報システムを安定稼動させるために、運用計画に従って、品質を確保した運用を実施する。

＜達成目標＞

1. 運用計画に従って情報システムが運用されている。
2. 運用の品質を低下させるおそれのあるインシデント、変更等に対して、計画的かつ適時に対処されている。
3. 運用に必要なリソースが確保されている。
4. 情報セキュリティ基本方針に従った運用管理ルールが作成され、運用されている。
5. 情報セキュリティ基本方針に従ったデータ管理ルールが作成され、運用されている。
6. 建物及び関連設備がリスクを考慮した適切な場所に設置され、管理されている。

＜管理活動の例＞

1. （運用の実施）運用管理の方針及び運用計画に従って運用を管理する。
2. （緊急時の運用）インシデント等の情報システムの有事発生時には、緊急時の運用を実施する。
3. （外部サービス管理）運用で外部サービスを利用する場合は、「Ⅱ.8.外部サービス管理」も参照して、外部サービスの利用を管理する。
4. （運用リソースの供給能力の管理）運用に必要なリソースの供給能力を管理する。
5. （しきい値外への対応）システムの稼動状況が許容可能な範囲にあるか、しきい（閾）値を設定して管理する。
6. （情報セキュリティ管理ルール）情報セキュリティ基本方針に従って運用に関する情報セキュリティルールを作成する。
7. （情報セキュリティ管理策）「情報セキュリティ管理基準」等を参照して、情報セキュリティ管理策を講じる。
8. （データ管理）データの不正利用及び漏えいの防止、個人情報保護のために、データ管理ルールを作成して管理する。
9. （建物及び関連設備管理）情報システムを設置する建物及び関連設備に関する管理ルールを定め、それに基づいて管理する。

Ⅱ.5.4　運用における構成・変更管理

情報システムを正常かつ効率的に稼動させ、構成要素間の整合性と全ての変更を適切に管理するために、プロジェクトで定めた構成・変更管理手続を実施する。

＜達成目標＞

1. プロジェクトで定めた構成・変更管理手続が適用され、遵守されている。
2. 管理対象のソフトウェア、ハードウェア及びネットワークの構成、調達先、サポート条件等を明確にした管理台帳が作成され、更新されている。
3. 変更計画が策定され、それに従って変更が実施されている。
4. リリース計画が策定され、計画に従って本番環境へのリリースが実施されている。

＜管理活動の例＞

1. （構成・変更管理手続）プロジェクトで定めた構成・変更管理手続の遵守状況をモニタリングする。
2. （構成管理台帳）構成管理台帳を作成し、構成管理の対象を明確にし、構成要素の変更内容に基づいて更新する。
3. （変更計画）運用の追加、廃止、変更、移管等の変更の依頼及び緊急度に従って、変更計画を策定し、優先順位を決定する。
4. （変更の実施）決定された変更計画に従って変更を実施する。
5. （利用部門との合意）IT部門と利用部門との間で変更について合意する。
6. （移行の管理）新規運用又は運用変更では、移行の管理手順を作成して移行を管理する。
7. （リリース計画）新規運用又は運用変更、及び運用の構成要素の稼動環境への展開についてリリース計画を策定する。
8. （リリースの実施）リリース計画に従ってリリースを実施する。

Ⅱ.5.5　インシデント・問題管理

利用部門と合意した目標内でインシデントを解決し、根本原因を特定して恒久的な対策を講じるために、インシデント管理及び問題管理の手順を定めて体系的に管理する。

＜達成目標＞

1. インシデント管理手順及び問題管理手順が作成され、それに従って対応されている。
2. インシデント管理に必要な要員と、その権限及び責任が割り当てられている。
3. インシデントの根本原因となる問題が識別されている。
4. インシデントの発生防止策又は再発防止措置が講じられている。

＜管理活動の例＞

1. （インシデント管理手順）インシデント管理手順を定め、体系的かつ適時に対処する。
2. （重大なインシデント管理手順）重大なインシデントに対応する手順を定め、体系的に管理する。
3. （インシデント対応要員の割り当て）インシデント対応に必要な要員とその権限及び責任を明確にする。
4. （利用部門との合意）利用部門と IT 部門の間で、インシデントの影響度及び緊急度を評価し、インシデント対応の優先度について合意する。
5. （インシデント対応の完了）利用部門の判断の下でインシデント対応を完了する手続を定める。
6. （根本原因の究明）インシデントの根本原因を究明する。
7. （問題管理手順）問題管理手順を作成して、問題を適切に管理し、インシデントの発生防止又は再発防止の措置を講じる。

Ⅱ.5.6　サービスレベル管理

サービスの品質を維持向上するために、適切な管理指標を設定してサービスの提供を管理する。

＜達成目標＞

1. 提供するサービス一覧が作成されている。
2. サービスの範囲及びサービスレベルが IT 部門及び利用部門の間で合意されている。
3. サービスデスクが設置され、利用部門からの問合せや発生した問題が適時かつ適切に対応されている。

＜管理活動の例＞

1. （サービス一覧）サービスの要求事項に基づいてサービス一覧を作成する。
2. （サービスレベルの合意）サービスの範囲及びサービスレベルを IT 部門及び利用部門の間で合意する。

3. （サービスのレビュー）定期的にサービスの実績をレビューし、サービスレベルの変更を管理する。
4. （サービスデスクの設置）利用部門を支援するためのサービスデスクを設置する。
5. （問合せの記録とレビュー）利用部門からの問合せ及び対応結果を記録し、その記録をレビューして、必要な改善を行う。

Ⅱ.5.7　運用の監視と記録

情報システムで発生した問題を把握し、対応が適時・適切に行われていることを確認するために、運用状況を監視して記録し、分析する。

＜達成目標＞

1. 運用計画に従った運用が実施されているか監視されている。
2. 情報システムの稼動実績が記録され、分析されている。
3. ログが取得、保管、分析され、適時に必要な対応がされている。
4. 運用の結果が記録、分析され、必要な改善が行われている。

＜管理活動の例＞

1. （監視の方法）運用を監視する対象、方法及び時期を定める。
2. （運用の監視）情報システムが適切に運用されていることを監視する。
3. （稼動実績の記録と分析）システムの稼動実績を定期的に監視し、記録し、分析する。
4. （ログの管理）情報システムで発生した問題を識別するためのログを取得、保管及び分析し、適時に必要な対応を行う。
5. （運用結果の記録）発生した不具合も含めて運用の結果を記録し、分析して、必要な改善を行う。

Ⅱ.5.8　運用の評価と報告

組織体の方針及び要求事項に従って運用が実施されていることを検証するために、運用の実績を評価し、報告する。

＜達成目標＞

1. 組織体の方針及び要求事項に従って運用が実施されているかが評価され、関係者に報告されている。
2. 利用部門と合意したサービスレベルの達成度が評価され、利用部門へ報告されている。
3. 利用部門の満足度が測定され、評価され、関係者に報告されている。
4. 運用が継続的に改善されている。

＜管理活動の例＞

1. （組織体の方針及び要求への適合性）組織体の方針及び要求に従った運用が実施されているかを定期的に評価し、関係者に報告する。
2. （サービスレベルの達成度評価）サービスレベルの達成状況を定期的に評価し、関係者に報告する。
3. （運用リソースの供給能力の評価）運用に必要なリソースの供給能力を定期的に評価し、関係者に報告する。
4. （利用部門の満足度の評価）利用部門の満足度を定期的に評価し、関係者に報告し、必要な改善を行う。
5. （運用の継続計画の評価）定期的及び運用環境に重大な変更があった場合に、運用の継続計画の有効性を評価し、必要な改善を行う。
6. （問題解決の有効性の評価）問題の傾向と解決策を分析し、問題解決の有効性を評価する。
7. （情報システムの稼動評価）情報システムの稼動実績を定期的に評価し、関係者に報告する。
8. （継続的な改善）運用の適切性、効率性及び有効性を継続的に改善する。

Ⅱ.6　保守プロセス

利用者の業務活動を支援する情報システムの能力・機能を維持するために、保守体制を整備し、保守依頼に応じた保守計画を策定して、それに基づいて保守作業を実施し、その検証、本番環境への適用、記録及び報告を行う。

Ⅱ.6.1　保守体制の整備

情報システムの性能・機能を維持するために、保守に関する方針、手順を定め、保守体制を整備する。

＜達成目標＞

1. 保守方針及び保守手順が定められ、周知されている。
2. 保守対象が明確にされている。
3. 保守実施体制が整備されている。
4. 開発プロセス及び運用プロセスから保守に必要な情報が連携されている。
5. 保守の実施に必要なシステム環境や保守用ツールが整備されている。
6. 保守業務を外部委託する場合、外部委託先との間で契約が締結されている。

＜管理活動の例＞

1. （保守方針）保守方針（外部委託方針を含む）を定めて、周知する。
2. （保守対象）保守方針に従って、情報システム、ハードウェア、ソフトウェア等の保守対象を明確にする。
3. （保守体制）保守方針に従って、保守専任部署の設置又は開発部署との共同体制等の保守体制（外部委託先を含む）を整備する。
4. （保守契約）保守業務を外部委託する場合、外部委託先との間で契約（以下、保守契約という）を締結する。
5. （保守手順書）保守方針に従って、保守手順書を作成し、周知する。
6. （情報セキュリティ対策）情報セキュリティ管理基準等を参考にして、保守方針に、保守作業に係る情報セキュリティ対策を構築することを明確にする。

7. （必要情報の連携）保守対象のハードウェアやソフトウェアの構成管理情報、システム構成図、プログラム一覧等含む保守で必要な情報を、開発プロセスや運用プロセスから連携する。
8. （保守環境等の整備）保守の実施に必要な保守環境、保守支援システム、保守用ツール等を整備し、使用可能な状態に維持する。

Ⅱ.6.2 保守計画

保守依頼を満足する保守作業を実施するために、保守依頼の内容と整合した保守計画を策定する。

＜達成目標＞

1. 保守依頼の内容が明確に把握され、保守依頼部門と合意されている。
2. 保守依頼に対する保守の実施の可否が、検討・決定されている。
3. 保守の区分（是正保守、適応保守、完全化保守及び予防保守）が設定され、保守プロセスで対応するのか開発プロセスを適用するのかが決定されている。
4. 保守計画に盛り込む必要のある事項が調査され、明確にされている。
5. 保守計画が策定され、承認されている。
6. 保守の実施結果が保守依頼の内容に合致していることを保守依頼部門が確認するための受入テスト計画が策定され、承認されている。

＜管理活動の例＞

1. （保守依頼内容の合意）保守依頼部門から提示された保守依頼の内容について、保守依頼部門と合意する。
2. （計画的な保守）組織体として計画されている保守の場合（可用性確保のためのシステム定期保守等）には、計画的な保守依頼として扱い、その計画の内容を確認する。
3. （保守実施可否の決定及び通知）保守依頼に対する保守の実施の可否を検討し、その結果を適切な期間内に決定し、保守依頼部門に通知する。
4. （保守区分）保守依頼で要求されている保守の区分を明確にする。

- 是正保守：インシデントの原因を取り除くための保守
- 適応保守：システム環境の変更に対応し、システムの正常稼動を維持するための保守
- 完全化保守：情報システムの能力・機能・使用性等に関する改良・拡張要求に対応する保守
- 予防保守：インシデントの未然防止、再発防止の観点からの保守

5. （適用プロセスの決定）保守区分及び保守依頼の内容に従って、保守プロセスで対応するのか開発プロセスで対応するのかを決定する。
6. （保守計画に盛り込む事項の調査）保守計画に盛り込む次のような事項について、調査し明確にする。
   - 保守作業実施スケジュール
   - 保守作業実施体制（外部委託先との連携を含む）
   - 保守対象の詳細化
   - 保守依頼に関する情報・データの入手
   - 保守実施状況のモニタリング計画　等
7. （保守計画の策定・承認・合意）保守区分、保守プロセスで対応するのか開発プロセスで対応するのかの判断、保守作業内容、保守作業実施スケジュール、保守作業実施体制等を記載した保守計画を策定し、承認を受け、保守依頼部門等の関係部門と合意する。
8. （受入テスト計画の策定・承認・合意）保守の実施結果が保守依頼の内容を満足していることを保守依頼部門が確認するための受入テスト計画を策定し、承認を受け、関係部門間で合意する。

Ⅱ.6.3　保守作業の実施

保守依頼を満足する保守を確実に実施するために、保守計画に従って保守作業を実施し、実施状況を管理する。

＜達成目標＞

1. 保守作業を実施する上で、必要に応じて、保守計画を詳細化した保守実施計画が策定されている。

2. 保守計画及び保守実施計画に従って保守作業が実施され、実施状況が管理されている。
3. 保守作業中に発生するインシデントが記録され、適切かつ迅速な解決が図られている。
4. 保守内容に対応したドキュメントの修正が適切に行われている。
5. 保守作業の実施状況が、適時に保守依頼部門に報告されている。

＜管理活動の例＞

1. （保守実施計画）必要に応じて、保守計画の実施スケジュール、実施体制・役割、実施項目・手順等を詳細化した保守実施計画を策定する。
2. （保守作業実施状況の管理）保守計画及び保守実施計画に従って保守作業が実施されているか、進捗や品質等の視点からモニタリングを行って、計画との差異が生じている場合には必要な対応を行う等、実施状況を管理する。
3. （インシデントの解決）保守作業を実施する中でインシデントが発生した場合、保守作業への影響を最小化するように、適切かつ迅速に解決する。
4. （ドキュメントの修正）保守内容に対応するドキュメントの修正を確実かつ漏れなく行い、保守内容とドキュメント修正内容が整合していることを確認する。
5. （保守作業実施状況の報告）定期的な連絡会議を設置して進捗報告を行う等によって、保守作業の実施状況を適時に保守依頼部門に報告する。

Ⅱ.6.4　保守作業の検証

保守作業の実施結果が保守依頼の要件を満足しているかを確認するために、保守計画に従って実施結果を検証する。

＜達成目標＞

1. 保守計画に基づいて保守結果検証計画が策定され、管理されている。
2. 保守結果検証計画に従って、保守結果が検証されている。
3. 検証の結果発見された問題点が記録され、適切かつ迅速に解決されている。

4. 検証結果が、適時に保守依頼部門に報告されている。
5. 保守依頼部門の受入テストによって、保守依頼の要件が満足されているか確認されている。

＜管理活動の例＞

1. （保守結果検証計画）保守計画及び保守実施計画に基づいた保守結果検証計画で業務への影響・検証評価基準等を明確にし、承認する。
2. （検証結果の確認）保守結果検証計画に従って実施した検証結果が、保守依頼の要件を満足させる結果であること、事前に検討した業務影響の範囲内であることを確認する。
3. （インシデント及び問題点の解決）保守結果検証計画に従って検証した結果、発生したインシデントや発見された問題点を記録し、適切かつ迅速に解決する。
4. （作業実施状況の報告）保守作業の実施状況を適時に保守依頼部門に報告する。
5. （依頼要件への充足）保守結果検証計画に従って実施した検証の結果が保守依頼の要件を満足していることを確認する。
6. （性能及び機能の充足）保守の結果、想定していた性能及び機能が要件を満足していることを確認する。

Ⅱ.6.5　本番環境への適用

情報システムの性能・機能を維持するために、保守作業の実施によって、本番環境の情報システムの構成要素に対する変更を実施する。

＜達成目標＞

1. 保守作業で変更した情報システムの構成要素について、本番環境に適用するための本番環境適用計画が策定・承認され、保守依頼部門と合意されている。
2. 本番環境適用計画に従って、変更された情報システムの構成要素が本番環境へ適用されている。

3. 本番環境適用計画に従って、本番環境へ適用された結果が確認されている。

＜管理活動の例＞

1. （本番環境適用計画）情報システムの性能・機能を継続的に維持するため情報システムの構成要素の変更を行うための本番環境適用計画を策定、承認し、保守依頼部門と合意する。
2. （本番環境への適用）本番環境適用計画に従って、変更された情報システムの構成要素を本番環境へ適用する。
3. （本番環境適用手続及び情報システムの構成要素）本番環境への適用に必要な手続、及び情報システムの構成要素を明確にする。
4. （本番環境への適用結果の確認）本番環境適用計画に従って、情報システムの構成要素を本番環境へ適用した結果を確認する。

Ⅱ.6.6　実施結果の記録と報告

情報システムの性能･機能を維持するために､保守作業の実施結果を記録し、報告する。

＜達成目標＞

1. 保守計画又は保守実施計画に従って、情報システムの構成要素の変更の実施結果が記録され、報告されている。
2. 本番環境への適用後、保守計画及び保守実施計画に従って、情報システムの性能及び機能の満足度が記録され、保守依頼部門へ定期的に報告されている。

＜管理活動の例＞

1. （情報システムの構成要素の記録）本番環境へ適用後、情報システムの性能及び機能の確認のために、情報システムの構成要素が定期的に記録されていることを確認し、報告する。
2. （性能及び機能の満足状況）本番環境へ適用した一定期間後に、情報システムの性能･機能について､保守依頼の要求を満足していることを確認し、定期的に報告する。

3. （貢献度の評価）保守作業によって、情報システムの性能及び機能の向上にどの程度貢献しているかを定期的に評価し、報告する。

Ⅱ.7. 廃棄プロセス

組織体の方針及び廃棄に関する要求事項に従って情報システムの利用を適切に終了するために、不要になった情報システムの構成要素を適切に廃棄する。

Ⅱ.7.1 廃棄計画

組織体の方針及び廃棄に関する要求事項に従って、不要となった情報システムの利用を適切に終了するために、廃棄計画を策定する。

＜達成目標＞

1. 不要となった情報システムの廃棄計画が策定されている。
2. 廃棄に関する制約が、要求事項、IT アーキテクチャ、設計及び実装の観点から利用者及び関係者に共有されている。
3. 廃棄に必要な全ての関連システム又はサービスが利用可能になっている。

＜管理活動の例＞

1. （廃棄計画）情報システムの構成要素及び結果として生じる廃棄物を含めた、情報システムの廃棄計画を策定する。
2. （技術要件）廃棄に関する要求事項、IT アーキテクチャ及び設計特性、実装における技術的制約を明確にする。
3. （関連システム又はサービス）廃棄を実施するために必要な関連システム又はサービスを明確にする。
4. （支援システム又はサービス）廃棄作業で利用する支援システム又はサービスを取得する、又はそれらへのアクセス権を取得する。
5. （情報システムの保管方法）廃棄作業が終了するまで情報システムを保管する場合には、格納施設、保管場所、情報システムの構成要素の棚卸等の保管方法及び保管手順を作成する。
6. （廃棄資源の不正利用防止）廃棄された情報システムの構成要素又は廃棄物を、不正にサプライチェーンに再投入することを防止するための方法を定義する。

Ⅱ.7.2　廃棄の実施

不要となった情報システムの利用を適切に終了するために、廃棄計画に従って情報システムの構成要素を適切に廃棄する。

＜達成目標＞

1. 不要となった情報システムの構成要素が廃棄計画に従って適切に廃棄されている。
2. 特に重要なデータについては、データの記録媒体に応じた廃棄の結果が記録され、保管されている。
3. データの記録媒体の特性に応じて、不正防止、機密保護及び個人情報保護の対策が講じられている。

＜管理活動の例＞

1. （廃棄資源の不正利用防止）情報システムの構成要素及び廃棄物を再利用できない方法で廃棄する。
2. （情報システムの構成要素の破壊）廃棄物処理量の削減、廃棄物の資源化等のために、必要に応じて情報システムの構成要素の破壊を実施する。
3. （廃棄作業への立会）重要なデータの廃棄には、運用管理者が立ち会う。
4. （データの保護対策）データの記録媒体の特性に応じた不正防止、機密保護及び個人情報保護の対策を講じる。
5. （中間保管施設の管理）最終廃棄処理まで中間保管施設（組織体内の保管施設を含む）に保管する場合は、盗難、紛失、重要情報の漏えい等が発生しないように管理する。

Ⅱ.7.3　廃棄結果の検証

廃棄計画に従って、不要となった情報システムの構成要素が適切に廃棄されていることを検証する。

＜達成目標＞

1. 情報システムの構成要素及び廃棄物が、廃棄計画に従って廃棄されている。

2. 廃棄後の情報システム環境が元の状態又は合意された状態に戻されている。
3. 廃棄作業が記録・分析され、記録が利用可能な状態になっている。

＜管理活動の例＞

1. （廃棄結果の検証）情報システムの構成要素及び廃棄物が、組織体の方針、廃棄に関する要求事項等に従って、消去、破壊、保管、再利用又は資源化されていることを検証する。
2. （廃棄後の情報システム環境）廃棄後の情報システム環境が元の状態又は合意された状態に戻されていることを確認する。
3. （産業廃棄物管理）産業廃棄物管理の法令等に従って廃棄物が処分されていることを確認する。
4. （廃棄作業の記録と分析）廃棄作業を記録、分析、管理する。

Ⅱ.8. 外部サービス管理

IT 戦略に基づいて外部サービス（クラウドサービスを含む）を利用するために、外部サービスの利用計画を策定し、外部サービス提供者を選定、契約、管理及び評価する。

Ⅱ.8.1 外部サービス利用計画の策定

IT 戦略に基づいて外部サービスを利用するために、外部サービスの利用対象及び内容を明確にした外部サービス利用計画を策定する。

＜達成目標＞

1. IT 戦略に基づいて外部サービス利用計画が策定されている。
2. 外部サービス利用計画において、外部サービスの利用対象及び内容が明確にされている。

＜管理活動の例＞

1. （外部サービス利用計画）IT 戦略に基づいて、外部サービス利用計画を策定し、承認を得る。
2. （外部サービス利用計画の記載内容）外部サービス利用計画において、外部サービスの利用目的、範囲、予算、体制、リスク評価、リスクへの対応方針等を明確にする。

Ⅱ.8.2 外部サービスの選定と契約

外部サービス選定基準を策定して、外部サービス利用計画に従った外部サービス提供者を選定し、契約を締結する。

＜達成目標＞

1. 外部サービスを選定するための外部サービス選定基準が作成されている。
2. 外部サービス利用計画に基づいて、外部サービスの利用対象業務が決定されている。

3. 外部サービス選定基準に基づいて、複数の外部サービスが比較・検討され、外部サービス提供者が選定されている。
4. 外部サービス利用計画に基づき、外部サービス提供者との契約が締結されている。

＜管理活動の例＞

1. （外部サービス選定基準）外部サービス利用計画に基づいた外部サービス選定基準を作成する。
2. （要求仕様の作成）外部サービス利用の対象となる業務要件及びシステム要件（機能要件及び非機能要件）を確認し、要求仕様を取りまとめる。
3. （外部サービス選定基準と要求仕様の整合性）外部サービス選定基準と要求仕様との間に不整合がないことを確認する。
4. （外部サービス提供者の選定）要求仕様と外部サービスの提供内容の整合性を確認して、外部サービス提供者を選定する。
5. （外部サービス提供者との合意）外部サービス提供者と契約（約款、サービスレベル合意（SLA）を含む）を締結する。

Ⅱ.8.3 外部サービスの運用管理

外部サービスの提供が契約どおりに履行されていることを管理するために、外部サービスの提供状況を適切に管理し、不整合や不具合が発生した場合は、外部サービス提供者に対して適時・適切な対応を要求する。

＜達成目標＞

1. 外部サービス利用計画に変更が発生した場合、外部サービス提供者との契約内容に影響のないことが確認され、必要に応じて契約の変更が行われている。
2. 外部サービスに関するシステム監査の取扱いについて、外部サービス提供者と合意がされている。
3. 外部サービスが契約に従って提供されていることが確認されている。

4. 外部サービス提供者の報告内容が外部サービス利用計画と整合していることを確認し、不整合が発生している場合は必要な対策が講じられている。
5. 外部サービス提供者に対して、発生したインシデント等について原因究明を行うとともに、再発防止策を講じることが要求されている。

＜管理活動の例＞

1. （契約内容の変更）外部サービス提供者との契約内容を変更する場合、変更された外部サービス利用計画と変更後の契約内容との間の整合を取る。
2. （システム監査に関する事項）外部サービス提供者との間で合意したシステム監査に関する事項を文書化する。
3. （履行状況の確認方法）外部サービス実施内容を管理するために、外部サービス実施内容が契約どおりに履行されていることを確認する方法を定める。
4. （履行状況の確認）外部サービス提供者から提示される報告書等について、外部サービスが契約どおり履行されていることを確認する。
5. （外部サービス利用計画との整合）外部サービス提供者からの報告内容を分析し必要な対応を行うために、外部サービス提供者からの報告書と外部サービス利用計画との整合性を確認する。
6. （インシデント報告）外部サービスにおけるインシデント等の発生時に適切内対応を行うために、インシデント報告書を受領し、業務影響度を分析するとともに、原因究明及び再発防止策を外部サービス提供者に要請する。

Ⅱ.8.4　外部サービスの評価

IT 戦略に基づいて外部サービスが利用されていることを評価するために、定期的及び契約終了時に外部サービスを評価し、報告する。

＜達成目標＞

1. 外部サービス提供者との契約（約款を含む）に基づいて、外部サービスの検収が行われている。

2. 外部サービス終了時に、外部サービス提供者に対して提供した情報が確実に回収又は廃棄（消去）されたことが確認されている。
3. 外部サービスを評価して、対象業務の目標の達成状況を評価し、経営者に報告されている。

＜管理活動の例＞

1. （検収の実施）契約（約款を含む）に基づいて、外部サービスの提供状況を評価し、外部サービスの検収を実施する。
2. （終了時の情報の回収又は廃棄）外部サービス利用終了時の対応を適切に行うために、情報の回収又は廃棄・消去を確実に実施する。
3. （終了時の評価）外部サービス終了時までに、外部サービス提供者との契約の内容が達成されていることを評価する。
4. （評価結果の報告）利用を終了した外部サービスの評価を行い、IT 戦略に基づいた外部サービス利用の目標達成状況を報告する。

Ⅱ.8.5　サービスレベル管理

提供される外部サービスの品質を確保するために、サービスレベル合意(SLA)を締結し、外部サービスの品質を評価し、問題が発生した場合には適切な対処を行うように外部サービス提供者に要請する。

＜達成目標＞

1. 外部サービス提供者が提供するサービスレベルが明らかになっている。
2. 外部サービス提供者との間で SLA が締結されている。
3. SLA に基づいて外部サービスが継続的に提供されていることが確認されている。
4. サービスレベル未達成の場合に備えて、具体的な対応方法が検討されるとともに、契約解除の条件が設定されている。
5. 業務内容が変更された場合には、必要に応じて SLA が見直しされている。

＜管理活動の例＞

1. （サービスレベルの合意）外部サービス利用計画に基づいて、外部サービス提供者と SLA を締結する。
2. （外部サービス利用計画との整合）SLA と外部サービス利用計画との間に不整合がないことを確認し、外部サービス提供者と合意する。
3. （サービスレベル達成状況の報告）サービスレベルの達成状況について、外部サービス提供者から定期的に報告を受ける。
4. （サービスレベル未達成時の対応策）外部サービスにおけるサービスレベル未達成の場合に備えた具体的な対応策を講じる。
5. （SLA の見直し）業務内容に変更が生じた場合は、サービスレベル合意（SLA）の内容の見直しを行い、必要な SLA の変更を行う。

Ⅱ.9. 事業継続管理

組織体の事業継続計画に基づいた情報システムの業務継続を実現するために、情報システムの業務継続計画を策定し、訓練、検証、報告及び改善を行う。

Ⅱ.9.1 リスクアセスメント

情報システムに影響を与える重大事故、サイバー攻撃、災害、テロ等に対する対応策を具体化するため、影響範囲、業務の重要性及び緊急性を明確にし、復旧優先度を設定する。

＜達成目標＞

1. 情報システムに影響を与える脅威が洗い出され、リスク事象が特定されている。
2. リスク事象の発生時に、情報システムに生じる影響度が想定されている。
3. 事業の優先順位を踏まえて、優先して復旧する業務と情報システムの関連性が明らかにされている。
4. 優先して復旧する業務で利用する情報システムに対して、最大許容停止時間及び目標復旧時間が定められている。

＜管理活動の例＞

1. （リスク事象の特定）重大事故、サイバー攻撃、災害、テロ等の脅威を洗い出し、リスク事象を特定する。
2. （影響範囲の特定）リスク事象の発生時に情報システムに与える影響度を特定する。
3. （事業が被る影響度の分析）情報システムの停止等によって事業が被る影響度を分析し、それを踏まえて業務の復旧の重要度及び緊急度を分析する。
4. （優先業務と情報システムの関連性）業務復旧の優先順位と情報システムの復旧の優先順位の整合を取る。
5. （最大許容停止時間及び目標復旧時間の設定）業務復旧の優先度を踏まえて、効率的に業務を復旧するために、業務の最大許容停止時間及び目標復旧時間を定める。

Ⅱ.9.2　業務継続計画の策定

重大事故、災害等の発生時に、適切な措置を迅速、円滑かつ確実に実行するために、情報システムの業務継続計画を策定する。

＜達成目標＞

1. リスクアセスメントの結果を踏まえて設定した復旧目標に基づいて、組織体の事業継続計画と整合が取れた情報システムの業務継続計画が策定され、承認されている。
2. 情報システムの業務継続計画の実効性が確保されている。
3. 情報システムの業務継続計画において、従業員の教育、訓練、関係者及び一般利用者に対するコミュニケーション等の方針が明確にされている。
4. 情報システムの業務継続計画が関係者に周知されている。

＜管理活動の例＞

1. （業務継続計画の策定）事業継続計画と整合が取れた情報システムの業務継続計画を策定する。
2. （業務継続計画の周知）情報システムの業務継続計画を関係者に周知する。
3. （業務継続計画の実現可能性）情報システムの業務継続計画の実現可能性を検証する。
4. （教育・訓練計画）関係者（外部委託先を含む）の教育・訓練計画を策定する。
5. （利用者及び関係者に対するコミュニケーション）関係者及び一般利用者に対するコミュニケーションの方針を明確にする。

Ⅱ.9.3　業務継続計画の管理

業務継続計画で定めた復旧目標を実現するために、情報システムのバックアップ及び代替処理を含む復旧手続及び体制の実現可能性を検証する。

＜達成目標＞

1. 業務の復旧目標に対応した、情報システムの構成要素についてバックアップ方法及び手順が定められている。
2. 代替処理を含む復旧手続及び体制の実現可能性が検証されている。
3. 情報システムの運用状況に対する監視機能が設けられ、情報システムの可用性が維持されている。
4. 情報システムの運用に要求される稼動率が確保され、情報システムの可用性が維持されている。

＜管理活動の例＞

1. （バックアップ手順の策定）情報システムを確実に復旧させるための業務の復旧目標に対応したバックアップ手順を定める。
2. （バックアップ手順の検証）定められたバックアップ手順の実効性を検証する。
3. （代替処理手続及び体制）情報システムが停止した場合、復旧するまでの間に業務を継続させるために必要な代替処理及び体制を定め、その実効性を検証する。
4. （復旧手続及び体制）停止した情報システムを円滑かつ確実に復旧させるための手続及び体制を定め、その実効性を検証する。
5. （運用状況の監視機能）情報システムの運用状況の監視機能を設ける。
6. （可用性の維持）情報システムの運用に要求される稼動率を確保し、可用性を維持する。

Ⅱ.9.4　訓練、演習及びテストの実施

事業継続計画に基づいた情報システムの業務継続計画を最新の状態にして実効性を高めるために、定期的に訓練を実施し、実現可能性を検証する。

＜達成目標＞

1. 代替処理を含む復旧手続の訓練が実施されている。
2. 訓練を定期的に実施し、復旧手続が最新の状態に維持されている。
3. 訓練結果がレビューされ、必要な改善が実施されている。

＜管理活動の例＞

1. （訓練の実施）目的や効果に応じて適切な業務継続計画の手順の訓練を実施し、その実効性を維持、向上させる。
2. （訓練の定期的実施）外部及び内部環境の変化に伴い業務継続計画の実効性が低減することのないように、定期的に訓練を実施する。
3. （業務継続計画の最新化）業務継続計画は、常に最新の状態に維持する。

Ⅱ.9.5　業務継続計画の評価及び見直し

情報システムの業務継続計画を適切かつ有効なものとするために、定期的（業務継続計画の発動時を含む）に業務継続計画の評価、見直し及び改善を行う。

＜達成目標＞

1. 業務継続計画を発動した場合、対処が完了した後に業務継続計画の評価及び見直しが実施されている。
2. 定期的に業務継続計画の評価及び見直しが実施されている。

＜管理活動の例＞

1. （リスク事象発生後の業務継続計画の評価及び見直し）情報システムに関わる業務に影響を与える重大なリスク事象が発生した場合、対処が完了した後に業務継続計画を評価し、見直しを行う。
2. （業務継続計画の定期的評価及び見直し）業務継続計画が適切かつ有効であることを、定期的に評価し、見直しを行う。

Ⅱ.10　人的資源管理

組織体の人的資源に関する方針に基づいて、IT に関する人的資源を管理し、IT 組織の能力を維持向上させる。

Ⅱ.10.1　人的資源管理計画

適切な IT システムの利活用を行うために、人的資源管理計画を策定、運用す

る。

＜達成目標＞

1. IT に関する人的資源の現状及び必要なスキルが人的資源管理計画で明確にされている。
2. IT に関する人的資源の調達及び育成の方針が人的資源管理計画で明確にされている。
3. IT に関する人的資源の活用等が人的資源管理計画で明確にされている。
4. 定期的又は状況の変化に伴い人的資源管理計画が見直され、人的資源管理計画の評価、検証が行われている。

＜管理活動の例＞

1. （IT ガバナンス方針との整合）IT ガバナンス方針に基づいて、人的資源管理計画を策定する。
2. （現状とスキルの明確化）IT に関する人的資源の現状及び必要なスキルを明確にする。
3. （調達及び育成の方針）IT に関する人的資源の確保及び育成の方針を明確にする。
4. （活用）IT に関する人的資源の活用等を明確にする。
5. （評価、検証及び見直し）人的資源管理計画に基づいて、IT に関する人的資源の定期的又は状況の変化時に評価、検証及び見直しを行う。

Ⅱ.10.2　責任と権限の管理

IT 業務を適正かつ効率的に行うために、要員の責任及び権限を定める。

＜達成目標＞

1. IT に関する企画、開発、運用及び保守業務に関わる管理者・担当者の責任及び権限が明確に定められ、文書化されている。
2. 職務分掌、指揮命令系統、独立性等を踏まえ、各役割、担当者、管理者等の関係に矛盾がないことが確認されている。

＜管理活動の例＞

1. （責任及び権限の設定）業務の特性及び業務遂行上の必要性に応じて、要員の責任及び権限を定めて周知する。
2. （責任及び権限の見直し）要員の責任及び権限は、業務環境及び情報環境の変化に対応した見直しを行う。

Ⅱ.10.3　業務遂行の管理

IT に関する業務が、各種計画に基づいて遂行され、作業品質を確保するために、要員の作業分担及び作業量を管理する。

＜達成目標＞

1. 業務を遂行するために必要な要員が確保されている。
2. 定められた責任が果たされ、権限が遵守されている。
3. 作業分担及び作業量が、要員の知識、能力に応じて割り振られている。
4. 要員の計画的及び不測の交替に備え、交替要員の育成が図られている。

＜管理活動の例＞

1. （責任及び権限）責任が果たされ、権限を遵守していることを確認する。
2. （作業分担及び作業量）作業分担及び作業量を、要員の知識、能力等から割り振る。
3. （交替要員の育成）要員の計画的及び不測の交替に備え、交替要員の育成を行う。
4. （勤務形態）リモートワークとオフィスワークの最適な組み合わせを行う。

Ⅱ.10.4　教育・訓練の管理

必要な IT に関する人材を確保するために、IT に関する人的資源管理計画及び教育カリキュラムに基づいて、要員の教育・訓練を管理する。

＜達成目標＞

1. 教育・訓練により技術力の向上、業務知識の習得、情報セキュリティの確保が実現されている。
2. 教育・訓練が人的資源管理計画及び教育カリキュラムに基づいて定期的かつ効果的に行われている。

＜管理活動の例＞

1. （教育・訓練の計画）人的資源管理計画に基づいて、教育・訓練の計画及びカリキュラムを作成する。
2. （スキルズインベントリ）技術力の向上、業務知識の習得、情報セキュリティ確保等の観点から、スキルズインベントリを作成する。
3. （教育・訓練の実施）人的資源管理計画及び教育カリキュラムに基づいて、教育・訓練を行う。
4. （見直し）業務環境及び情報環境の変化に対応した見直しを行う。

Ⅱ.10.5　健康管理

IT に関する業務の特性を踏まえて、一般的な要員の身体面及び精神面での健康を維持できる作業環境を整備する。

＜達成目標＞

1. 企画、開発、運用及び保守業務の特性を考慮した健康診断、カウンセリング等、要員の健康を維持する対策が講じられている。
2. 身体面の健康管理だけでなく、精神面の健康管理も行われている。

＜管理活動の例＞

1. （健康診断、カウンセリング）企画、開発、運用及び保守業務の特性を考慮した健康診断、カウンセリング等の健康管理の仕組みを整備・運用する。
2. （精神面の健康管理）精神面の健康管理の仕組みを整備・運用する。

Ⅱ.10.6　要員のエンゲージメント向上

IT に関する業務を適切に実施するために、これらの業務に対する要員のエン

ゲージメント（業務に対する前向きで活動的な心理）レベルを向上させるための取組を行う。

＜達成目標＞

1. 要員の採用、昇進・昇格、報酬、表彰等を公正かつ公平に実施する仕組みが整備・運用されている。
2. エンゲージメントレベルを測定するための項目が整理され、要員のエンゲージメントレベルが定期的に測定されている。

＜管理活動の例＞

1. （要員の採用・人事評価）要員の採用、人事評価、表彰等の仕組みを整備し、エンゲージメントレベルを向上させる。
2. （エンゲージメントレベルの測定）エンゲージメントレベルを測定するための項目及び方法を整備し、それに基づいて要員のエンゲージメントレベルを測定する。
3. （見直しと改善）エンゲージメントレベルを向上させるための施策の見直し・改善を行う。