システム管理基準

経済産業省

平成 30 年 4 月 20 日

前文(システム管理基準の活用にあたって)

システム管理基準は、平成 16 年のシステム監査基準の改訂において、それまでの「一般基準」、「実施基準」、「報告基準」で構成されるシステム監査基準の「実施基準」の主要部分を抜き出すとともに、当時の情報技術環境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、監査の効率的・効果的遂行を可能にする判断の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。

今回の改訂の主旨は、前回の改訂の後に生じた情報通信技術環境と情報化実践の大きな変化を踏まえて、さらに次の点を企図している。

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、情報システム化実践に関わる適切な自己診断及び監査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。

本基準は、どのような組織体においても情報システムの管理において共通して留意すべき基本的事項を体系化・一般化したものである。したがって、本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。事業目的、事業分野における特性、組織体の業種・業態特性、情報システム特性などに照らして、適切な項目の取捨選択や各項目における対応内容の修正、情報システムの管理に関連する他の基準やガイドから必要な項目を補完するなど、監査及び管理の主旨が実現できるように独自の管理基準を策定して適用することが望ましい。

なお、情報セキュリティの確保に焦点をおいて情報システムの監査・管理を実施する場合には、当基準でも情報セキュリティの確保に関連する最小限の項目で体系化しているが、それぞれの項目については、「情報セキュリティ管理基準（平成 28 年改正版」(経済産業省)などを活用して独自の管理基準を策定することが望ましい。

さらに、独自に策定する管理基準については、情報システム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、情報システム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、定期的に管理項目の追加・削除などの修正を行うことにより基準の有用性を高めることが必要である。

なお本基準では、「情報セキュリティ管理基準」における要求事項との対応関係の理解を容易にするために、「情報セキュリティ管理基準参照表」を付してある。これを参照して各企業のリスク特性を勘案して独自の管理基準の策定に利用されたい。

本基準で使用した用語は、JIS 及び ISO、その他の標準規格に可能な限り留意するとともに、本基準の理解を容易にするために、理解が困難であったり、意味の特定化が必要と思われたり、やや専門的であったりする基本用語については「用語説明表」として基準の末尾に収録している。適宜、参照されたい。

システム管理基準の枠組み

1. IT ガバナンスの定義

あらゆる組織は、顧客、従業員、取引先、投資家その他を含む、ステークホルダに対して価値を創出することが求められる。一方、IT(情報技術)は事業戦略に欠かせないものとなっており、IT によって実現される情報システムの巧拙が経営に大きな影響を及ぼすようになっている。

情報システムの企画、開発、保守、運用といったライフサイクルを管理するためのマネジメントプロセスが IT マネジメントであり、経営陣はステークホルダに対して IT マネジメントに関する説明責任を有する。

IT ガバナンスとは経営陣がステークホルダのニーズに基づき、組織の価値を高めるために実践する行動であり、情報システムのあるべき姿を示す情報システム戦略の策定及び実現に必要となる組織能力である。また、経営陣は IT ガバナンスを実践する上で、情報システムにまつわるリスク（以下「情報システムリスク」という。）だけでなく、予算や人材といった資源の配分や、情報システム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。

なお、今日では、クラウドサービスやアウトソーシング等、外部の資源を組み合わせる手法が一般化していることから、本基準では情報システムをハードウェア、ソフトウェア、ネットワークに加えて、外部のサービスや業務プロセスを含む概念として用いている。そのため、本基準における IT ガバナンスとは情報システムのガバナンスであり、IT マネジメントとは情報システムのマネジメントである。すでに IT ガバナンス及び IT マネジメントという用語が定着している事を反映して、本基準ではこれらの用語を用いている。

2. IT ガバナンスにおける EDM モデル

本ガイドラインでは、前節の IT ガバナンスの定義における経営陣の行動を、情報システムの企画、開発、保守、運用に関わる IT マネジメントとそのプロセスに対して、経営陣が評価し、指示し、モニタすることとする。また、IT ガバナンスにおける国際標準である ISO/IEC 38500 シリーズ及び日本での規格である JIS Q 38500 より、評価（Evaluate)、指示（Direct)、モニタ（Monitor）の頭文字をとって EDM モデルと呼ぶ。

- 評価とは、現在の情報システム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、想定されるリスクを見積もることである。
- 指示とは、情報システム戦略を実現するために必要な責任と資源を組織へ割り当て、期待する効果の実現と想定されるリスクに対処するよう、IT マネジメントを導くことである。
- モニタとは、現在の情報システムについて、情報システム戦略で見積もった効果をどの程度満たしているか、割り当てた資源をどの程度使用しているか、及び、想定した

リスクの発現状況についての情報を得られるよう、IT マネジメントを整備すると共に、IT マネジメントの評価と指示のために必要な情報を収集することである。

3. IT ガバナンスにおける 6 つの原則

IT ガバナンスを成功に導くため、経営陣は、次の 6 つの原則を採用することが望ましい。

① 責任

役割に責任を負う人は、その役割を遂行する権限を持つ。

② 戦略

情報システム戦略は、情報システムの現在及び将来の能力を考慮して策定し、現在及び将来のニーズを満たす必要がある。

③ 取得

情報システムの導入は、短期・長期の両面で効果、リスク、資源のバランスが取れた意思決定に基づく必要がある。

④ パフォーマンス

情報システムは、現在及び将来のニーズを満たすサービスを提供する必要がある。

⑤ 適合

情報システムは、関連する全ての法律及び規制に適合する必要がある。

⑥ 人間行動

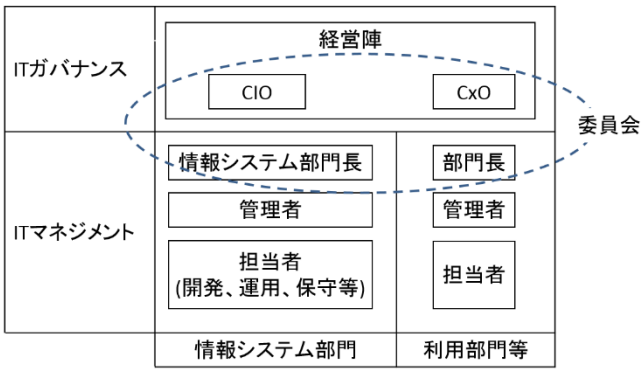
情報システムのパフォーマンスの維持に関わる人間の行動を尊重する必要がある。

4. システム管理基準の前提となる組織体制

本基準は判りやすく具体化したものとするために、モデル化した組織体制を前提とした記述となっている。

そのため、本基準を利用する際に、自らの組織に適合するように読み替える必要がある。

本基準が想定する組織体制を右図に示す。



本基準が想定する組織体制と、自らの組織への適合について以下に述べる。

(1) CIO

情報システム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、経営陣は CIO を任命し、必要な権限を委譲する。そのため、CIO も経営陣に含まれる。

なお、小規模な組織、あるいは経営陣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、本基準において、CIO に関する記述は経営陣として読み替えることとなる。

(2) 委員会（情報システム戦略委員会，プロジェクト運営委員会等）

情報システム戦略の策定や大規模プロジェクト等では組織全体にまたがる利害関係者の調整が必要となる。経営陣は 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。そのため、委員会も経営陣の一部とする。

なお、小規模な組織、あるいは組織内の調整が容易な場合には、委員会を組成しないことがある。その場合には、本基準において、委員会に関する記述は経営陣として読み替えることとなる。

(3) 情報システム部門

IT マネジメントは経営陣の指示に従うと共に、経営陣によるモニタに必要な情報を提供する。

組織内で IT マネジメントを実施する体制を、本基準では、「情報システム部門」と呼ぶ。

情報システム部門は、情報システムに関する「企画」、「開発」、「保守」、「運用」を実施する「担当者」、及び担当者を管理する「管理者」、そして情報システム部門の長である「情報システム部門長」で構成される。

なお、組織によって、経営陣、あるいは CIO が情報システム部門長を兼務することがある。その場合には、本基準において、情報システム部門長に関する記述は経営陣あるいは CIO として読み替えることとなる。

また、小規模な組織では、「担当者」及び「管理者」が少数であり、情報システム部門長を任命しないことがある。その場合には、本基準における情報システムに関する記述は該当する管理者として読み替えることとなる。

(4) 利用部門等

組織内において、「情報システム部門」以外の体制を「利用部門等」と呼ぶ。

情報システム部門と同様、経営陣は必要に応じて CxO 及び「部門長」を任命し、必要な権限を委譲する。CxO あるいは部門長を任命しない場合には、情報システム部門と同様に、本基準の該当箇所を、経営陣、あるいは管理者として読み替えることとなる。

Ⅰ．IT ガバナンス

1．情報システム戦略の方針及び目標設定

(1) 経営陣は、情報システム戦略の方針及び目標の決定の手続を明確化していること。

＜主旨＞

経営戦略に基づく情報システム戦略を策定するために、情報システム戦略の方針及び目標の決定に関する明確な手続を定め、それが機能していることを確認しておく必要がある。

＜着眼点＞

① 経営陣は、情報システム戦略の方針及び目標に影響を与える内的環境要因（既存情報システム資源等）、外的環境要因（技術動向等）、及び利害関係者の要求等を適切に評価していること。

② 情報戦略における方針･目標決定と計画化の手続を明確に規定していること。

③ 情報戦略における方針･目標決定と計画化の手続とその判断基準が適切であるかどうかを適時に点検し、見直しをしていること。

(2) 経営陣は、経営戦略の方針に基づいて情報システム戦略の方針・目標設定及び情報システム化基本計画を策定し、適時に見直しを行っていること。

＜主旨＞

経営目的を実現する情報システムを企画するため、経営陣は情報システム戦略の中長期の方針･目標及び情報システム化基本計画を、経営戦略の方針との整合性を勘案して策定し、適時に見直しを行っている必要がある。

＜着眼点＞

① 組織のビジョン、使命及び経営戦略を評価して、情報システム戦略の目標及び情報システム化基本計画を策定していること。

② 情報システム戦略の目標達成及び情報システム化基本計画の遂行状況を評価するための指標を、可能な限り定量的に、適切に設定していること。

③ 情報システム戦略の目標達成状況を中長期の情報システム化基本計画に照らして適時にモニタリングし、適切な対応に結びつけていること。

(3) 経営陣は、情報システムの企画、開発とともに生ずる組織及び業務の変革の方針を明確にし、方針に則って変革が行われていることを確認していること。

＜主旨＞

経営陣は、情報システム戦略において、情報システムの企画、開発とともに行われる組織及び業務の新設、改変及び廃止の方針を明確にし、方針に則った諸活動が行われているかどうかを確認する必要がある。

＜着眼点＞

① 組織及び業務の変革の方針は、経営戦略に適合することを確認していること。
② 情報システムの企画・開発とともに行われるべき組織及び業務の変革の方針を明確にしていること。
③ 組織及び業務変革の方針を経営陣が承認していること。
④ 設定した変革の方針に則って諸活動が進められていることを確認していること。

2. 情報システム戦略遂行のための組織体制

(1) 経営陣は、CIO（Chief Information Officer）を任命すること。CIO は最高情報責任者 / 情報統括役員としての職務を担うこと。

＜主旨＞

CIO には、経営的な観点から戦略的意思決定を行う経営陣の一員としての役割と情報システム部門の統括責任者としての役割が期待される。

＜着眼点＞

① CIO の指示を、情報システムの企画、開発、運用及び保守業務の責任者に対して迅速かつ正確に伝えるための指揮系統を整備すること。
② 情報システムの企画、開発、運用及び保守業務の現場で発生した問題が、CIO に迅速に伝わる情報網を整備すること。
③ CIO には、経営陣の一員としての役割と情報システム部門の統括責任者としての役割があることを明確にしていること。
④ CIO の職務遂行の状況を、適切にモニタリングしていること。

(2) 経営陣は、情報戦略を統括する役割を明確に規定し、適切な権限及び責任の付与のもとに情報システム戦略委員会等を設置し、適切に機能させていること。

＜主旨＞

経営戦略に基づいた情報戦略の方針･目標と中長期の情報システム化基本計画の策定と実行を推進するため、経営陣は、情報システム戦略委員会等を設置し、その役割と権限、責任を明確にする必要がある。また、設置された情報システム戦略委員会等が適切に機能していることが求められる。

＜着眼点＞

① 情報戦略の策定と実行を推進する情報システム戦略委員会等を設置していること。
② 情報システム戦略委員会等は、CIO、CFO、業務部門の責任者、各情報システムの責任者（オーナ）等、必要な組織の権限者によって構成されていること。
③ 情報システム戦略委員会等の位置付けを明確にし、関係者の合意を得ていること。
④ 情報システム戦略委員会等には、適切な役割、権限及び責任を与えていること。
⑤ 情報システム戦略委員会等の構成は、情報戦略、業務機能及び組織の変更に伴って見直しをすること。

⑥　情報システム戦略委員会等が適切に機能していることを、適時にモニタリングしていること。

(3) 情報システム戦略委員会等は、組織における情報システムに関する活動全般について、モニタリングを実施し、必要に応じて是正措置を講じること。

＜主旨＞

情報システム戦略に基づいた情報システムの企画、開発、運用、保守を実施するため、情報システム戦略委員会等は、全社の情報システムを総括する権能と責任を有し、不適切な状況に対しては、是正のための適切な措置を講ずる必要がある。

＜着眼点＞

①　情報システム戦略委員会等がモニタリング対象とする情報システムの活動を明確にしていること。

②　ビジネス環境の変化に即応できるように、適切かつ適時のモニタリングを行う仕組みを構築していること。

③　障害、事故、プロジェクト進捗、予算執行等のモニタリング項目を明確にしていること。

④　モニタリングによって発見された不具合等に対して、適切な対応を行っていること。

⑤　モニタリングによって発見され是正措置を指示した施行に関して、必要に応じて情報システム戦略への対応、反映を行っていること。

(4)　情報システム戦略委員会等は、情報技術の動向に対応するため、技術採用指針を明確にしていること。

＜主旨＞

変化する情報技術動向に適切かつ迅速に対応し、組織全体としての整合性のとれた情報技術基盤を確立しリスクを低減させるため、情報システム戦略委員会等は、技術採用指針を明確にしている必要がある。

＜着眼点＞

①　組織として関連のある情報技術分野の動向を明確にしていること。

②　情報技術の最新動向等を収集する範囲、担当部門を明確にしていること。

③　技術採用指針を文書化し、定期的に見直していること。

④　必要に応じて、適切で客観かつ公正な外部専門家の助言を得て、これを技術採用指針に反映させていること。

(5) 情報システム戦略委員会等は、活動内容を経営陣に報告していること。

＜主旨＞

情報システム戦略委員会等は、経営活動の意思決定に資するため、情報システム戦略の策

定･実行･評価内容を適時に経営陣に報告している必要がある。
＜着眼点＞
① 情報システム戦略委員会等の活動を経営陣に報告する手続を定めていること。
② 情報システム戦略委員会等の活動内容を報告書として作成していること。
③ 報告書のレビューを実施していること。
④ 報告書を経営陣に提出し、報告していること。

(6) 情報システム戦略委員会等は、経営戦略の計画･実行･評価に関わる意思決定を支援するための情報を経営陣に提供していること。
＜主旨＞
情報システム戦略委員会等は、情報システム戦略にかかわる環境変化、技術動向、組織内情報システムの状況を適切かつ迅速に経営方針に反映させるため、それらの情報を経営陣に適時提供し、意思決定に資するようにしている必要がある。
＜着眼点＞
① 情報システム戦略委員会等は、情報システム化基本計画及びその投資の是非の判断に資する情報を経営陣に提供していること。
② 代替案を評価する判断根拠、基準を適切に提供していること。
③ 経営陣に提供する情報について、事実と意見を区別して提供していること。

3. 情報システム部門の役割と体制
(1) 経営陣は、CIO の配下に情報システム部門をおき、情報システム部門の役割を明確にし、適切な権限及び責任を与えていること。
＜主旨＞
適時に適切な情報システム機能を遂行するために、経営陣は、情報システム部門をおき、統括責任者として CIO をおいていること。情報システム部門長は CIO の配下に位置付けられていることが必要である。さらに、情報システム部門の役割、機能を明確にして、適切な権限と責任を与えている必要がある。
＜着眼点＞
① 情報システム部門の使命や役割を明文化して、経営陣が承認していること。
② 情報システム部門は、ユーザ部門から独立しつつ、協働する体制を取っていること。
③ 情報システム部門長は、情報システム投資、及び情報システムに関わる諸資源を集約して管理していること。
④ 情報システム部門長は、情報システム部門の役割と目的を組織内に周知徹底していること。
⑤ 特定の委託先、業務提携先等に依存していないこと。

(2) 情報システム部門長は、経営陣の承認を得て、組織の規模及び特性に応じて、情報システム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構築していること。

＜主旨＞

情報システム戦略を効果的かつ効率的に実現するために、自社内の資源とともに外部資源も適切に活用し、組織の情報システムのニーズや投資効果に見合った体制である必要がある。

＜着眼点＞

① 情報システム部門長は、作業効率と品質の向上、及び情報セキュリティの確保の観点から適切な職務の分離、及び専門化の推進を行っていること。

② 情報システム部門長は、迅速かつ業務実態に即した承認を実現するため、適切な権限付与を行っていること。

③ 業務活動の状況に即した物理的セキュリティ、論理的セキュリティ、及び環境的セキュリティを適切に確保していること。

④ 情報システム部門長は、業務の活動に効果的な外部委託先を選定し、適切に管理、監督していること。

4. 情報システム戦略の策定の評価・指示・モニタ

(1) 経営陣は、情報システム戦略の策定を情報システム戦略委員会等に、指示していること。

＜主旨＞

情報システム戦略とは、経営戦略に基づき情報システムの中長期計画として策定する必要があるため、経営陣は、情報システム戦略の策定体制を情報システム戦略委員会等として確立している必要がある。

＜着眼点＞

① 情報システム戦略委員会等には、情報システム戦略の策定の際には、情報システムに係るすべての部門が参画していること。

② 参画者の役割を明確にしていること。

③ 能力、経験等を考慮して参画者を選定していること。

(2) 経営陣は、情報システム戦略について利害関係者の合意を得ることを指示していること。

＜主旨＞

円滑に運用できる情報システム戦略とするために、利害関係者の合意を得る必要がある。

＜着眼点＞

① 利害関係者の範囲が明確に定義されていること。

② 情報システム戦略策定のルールが定められ、その中に利害関係者の合意の手順が含まれていること。
③ 利害関係者による合意を書面として残していること。

(3) 経営陣は、情報システムで目指すべき情報システムの将来像を、中長期の情報システム化基本計画として明確にしていること。
＜主旨＞
情報システムは、互いに連携し効率的かつ効果的に組織の事業目的を達成するため、経営陣は、情報システム戦略において、中長期の情報システムで目指すべき事業と情報システムの将来像を明確にする必要がある。
＜着眼点＞
① 事業及び情報システムの内部及び外部環境の変化について、適切に評価を行なっていること。
② 組織のすべての情報システムを各ユーザ部門の業務とともにモデル化する手法を定めていること。
③ 情報システムと事業の現状及び目指すべき将来像をモデル化手法等によって記述していること。
④ 現状の情報システム及び事業における課題を洗い出していること。
⑤ 情報システム及び事業の目指すべき将来像において、現状の課題が解決されることを確認していること。
⑥ 情報システムが目指すべき将来像を達成する具体的な手法及び工程表を、情報システム化基本計画として明らかにしていること。
⑦ 情報システム化基本計画の実行状況を適時にモニタリングしていること。

(4) 経営陣は、経営計画で示した事業の方針及び目標に基づいて、情報システム戦略を評価していること。
＜主旨＞
情報システム戦略は、事業の方針及び目標に基づいて策定され、経営戦略と整合している必要がある。
＜着眼点＞
① 情報システム戦略策定のルールが定められ、その中に承認手続が含まれていること。
② 情報システム戦略には、事業の方針及び目標が簡潔かつ明確に記されていること。
③ 情報システム戦略において、事業の方針及び目標に基づいて、情報システム戦略の目標及び方針が設定されていること。
④ 情報システム戦略の目標の達成をモニタリングするための指標が定められていること。

⑤　情報システム戦略を経営陣が評価し、承認していること。

(5) 経営陣は、情報システム戦略においてコンプライアンスを考慮することを指示していること。

＜主旨＞

関連法規、業界の自主基準等を遵守するように、情報システム戦略は、コンプライアンスを考慮して作成する必要がある。

＜着眼点＞

①　情報システム戦略の策定時点で確定している考慮すべき法規等を全て洗い出していること。

②　今後改定・新設が予想される法規等への対応を講じていること。

③　考慮すべき法規等を定期的及び必要に応じて見直すことを定めていること。

④　情報システム戦略に対するコンプライアンスの面からのレビューに、法務部門等の法律の専門家が参画していること。

⑤　コンプライアンスに関するリスクの対処方法を講じていること。

⑥　組織の構成員に対するコンプライアンス徹底の方法を定めていること。

(6) 経営陣は、情報システムの企画、開発及び運用、保守のための標準化の方針、並びに品質確保の方針を含めたルールを明確にすること。

＜主旨＞

情報システムの企画、開発及び運用、保守を効率的かつ高品質に保つため、情報システムの企画、開発及び運用、保守のための標準化の方針、並びに品質確保の方針を明確にする必要がある。

＜着眼点＞

①　情報システムの企画、開発及び運用、保守のための標準化、並びに品質確保の方針を明文化していること。

②　標準化及び品質確保の方針について周知徹底すべき関係者及び関係者の理解をモニタリングする方法を定めていること。

③　標準化及び品質確保の方針に基づいて明文化すべき企画、開発及び運用、保守にかかわる標準及びその標準について周知徹底すべき範囲を定めていること。

④　環境の変化に対応して標準を見直すことを定めていること。

(7) 経営陣は、個別の開発計画の優先順位及び順位付けのルールを明確にしていること。

＜主旨＞

経営課題の重要性及び緊急性を反映し、開発資源を有効に活用するため、情報システム戦略では、個別計画の優先順位及び順位付けのルールを明確にする必要がある。

＜着眼点＞

① 個別計画の優先順位の決定方法をルールとして定めていること。
② 各個別計画が目的としている経営課題の重要性及び緊急性を明確にしていること。
③ 個別計画の着手の順序、資源配分、開発の期間は、業務との整合性を考慮して検討していること。
④ 個別計画の優先順位の決定理由を説明すべき関係者を明確にしていること。
⑤ 必要に応じて個別計画の優先順位を見直すことを定めていること。
⑥ 決定された優先順位に基づいて個別計画が着手されることを確認するように定めていること。

(8) 経営陣は、情報システム戦略を関係者への周知徹底を指示することと、その結果をモニタすること。

＜主旨＞

情報システム戦略を実行性の高いものとするため、すべての利害関係者に周知徹底し、理解させる必要がある。

＜着眼点＞

① 情報システム戦略を周知徹底すべき関係者のリストが作成されていること。
② 全関係者に情報システム戦略を周知徹底していること。
③ 周知徹底の方法をルールとして定めていること。
④ 経営陣は、全関係者に情報システム戦略を周知徹底して理解させたことをモニタリングしていること。

(9) 経営陣は、情報システム戦略の実行状況について、定期的及び経営環境等の変化に対応して適時モニタリングを行い、必要なアクションをとること。

＜主旨＞

情報システム戦略を硬直化・陳腐化させないために、定期的なモニタリング及び経営環境等の変化に対応したモニタリングを適時行う必要がある。

＜着眼点＞

① 情報システム戦略の実行状況は、定期的及び必要に応じてモニタリングされていること。
② モニタリングの結果、情報システム戦略に対して必要なアクションを行うこと。
③ 情報システム戦略に対してアクションを行う際にはその理由を明確にしていること。
④ 情報システム戦略の変更を経営陣が承認していること。
⑤ 情報システム戦略に対して定期的及び必要に応じてモニタリングとアクションを行うこと、またモニタリングとアクションの手順がルールとして定められていること。
⑥ ルールを遵守したモニタリングとアクションが行われていることを経営陣に報告し

ていること。

5. 情報システム投資の評価・指示・モニタ

(1) 経営陣は、情報システム投資計画を経営戦略との整合性を評価して策定すること。

＜主旨＞

情報システム投資を経営課題の解決に役立たせるため、経営に与える利益効果、業務処理の改善等の情報システム戦略の観点から、経営戦略と整合性をもった情報システム投資計画を策定する必要がある。

＜着眼点＞

① 情報システム投資の対象範囲とその区分が定められていること。
② 情報システム投資の有効性を評価する指標及び目標が定められ、経営戦略の指標及び目標と整合がとれていること。
③ 経営戦略の策定の経営陣が、情報システム投資計画を承認していること。
④ 情報システム投資の優先順位付けは、情報システム戦略の観点を踏まえて、定量的な投資評価等に基づいて行われ、関係者の合意を得ていること。

(2) 情報システム投資計画の決定に際して、経営陣は、影響、効果、期間、実現性等の観点から複数の選択肢を評価すること。

＜主旨＞

情報システム投資計画を利害関係者の合意の上で決定するために、影響、効果、期間、実現性等の観点から複数の選択肢を挙げて評価し、適切なものを選択する必要がある。

＜着眼点＞

① 影響、効果、期間、実現性等の観点において明確な差がある複数の選択肢が挙げられていること。
② 選択基準が定められていること。
③ 具体的な選択肢を選択した理由を利害関係者に説明できるようにしていること。

(3) 経営陣は、情報化投資に関する予算を適切にモニタしていること。

＜主旨＞

情報システム化投資計画の実行のために、経営陣は、適切な時期、金額、契約形態等で予算の執行状況をモニタする必要がある。

＜着眼点＞

① 予算執行の最終決裁者が定められていること。
② 予算執行の時期、金額、契約形態等が計画されていること。
③ 経営環境の変化に合わせて予算執行の時期、金額が調整されていること。
④ 不適切な執行を防止するための内部統制が存在していること。

⑤　予算の執行が適切であったかを事後に評価する体制が整備されていること。

(4)　経営陣は、情報システム投資の方針及び確保すべき経営資源を明確にすることと、その投資状況及び経営資源の状況をモニタリングしていること。

＜主旨＞

情報システム化投資計画では、情報システム投資及び確保すべき経営資源を評価して明確にし、適切な状態に維持する必要がある。

＜着眼点＞

①　情報システム投資の内容を明確にしていること。

②　確保すべき経営資源を明確にしていること。

③　計画に従った投資が行われることをモニタリングする手順を定めていること。

④　経営資源に不足が生じた場合の対応手順を定めていること。

(5)　経営陣は、情報システム投資に関する投資効果の算出及びリスク算定の方法を明確にしていること。

＜主旨＞

情報システム投資の効果を客観的に評価し、計画の採択基準及び修正を検討すべき判断基準を明確にするため、さらには今後の情報システム化投資計画にフィードバックするために、投資効果の算出及びリスク算定方法を事前に明確にしておく必要がある。

＜着眼点＞

①　各情報システム投資案件について、その効果の算出及びリスク算定方法を事前に定めていること。

②　各情報システム投資案件について、その予算を個別に定めていること。

③　投資効果の期待値を事前に算定していること。

④　投資効果の算出方法を事前に明確にすることがルールとして定められていること。

⑤　投資効果が不明確なまま情報システム投資が行われることを防止する内部統制があること。

⑥　投資計画の修正の検討が必要となる閾値(いきち)が定義されていること。

⑦　投資効果及びリスク算定が適正に行われることをモニタリングすることを定めていること。

(6)　経営陣は、情報システムの全体的な実績及び個別プロジェクトの実績を財務的な観点からモニタリングして、問題点に対して対策を講じること。

＜主旨＞

情報システムの全体的な業績及び個別プロジェクトの業績の財務的な課題を早期に発見し適切な対策を講ずるために、財務的な観点からのモニタリングを行うとともに、想定され

る課題については事前に対応手順を準備しておく必要がある。
＜着眼点＞
① 情報システムの全体的な実績及び個別プロジェクトの実績について、財務的な観点からのモニタリングを行っていること。
② モニタする指標及びアラームを立てる閾値(いきち)を定義していること。
③ 投資規模等に応じて、重点的に、モニタリングすべき個別プロジェクトを明らかにしていること。
④ 想定される財務的な課題について事前に対応手順を準備していること。
⑤ 情報システムの全体的な業績及び個別プロジェクトの実績を財務的な観点からモニタリングして、問題点に対しては対策を講ずることがルールとして定められていること。
⑥ 財務的な観点から評価が行われないまま個別プロジェクトが推進されることを防止する内部統制があること。

(7) 経営陣は、投資した費用が適正な使用であったかについてモニタリング及び評価をすること。
＜主旨＞
情報システム投資が計画通りなのか、適正な使用なのか、また計画とのずれがあった場合に適切に修正されたのかについて、投資金額、用途等をモニタリングして評価する必要がある。
＜着眼点＞
① 各投資案件について、投資金額、用途等を記録していること。
② 各投資案件について、投資金額、用途等をモニタリングし、計画と突合していること。
③ 計画とのずれがあった場合には、その理由を明確にしていること。
④ 計画との大きなずれがあった場合には、元の計画に戻すための補正投資を行うか、又は投資計画自体を修正していること。
⑤ 投資した費用が適正に使用されたこと及び妥当性を評価することがルールとして定められていること。
⑥ 投資した費用が適正に使用されたこと及び妥当性の評価が行われないまま放置されることを防止する内部統制があること。
⑦ 投資の評価にあたっては、情報システムの資産価値や減損についても確認すること。

6. 情報システムの資源管理の評価・指示・モニタ
(1) 経営陣は、情報システムに関する資源管理の対象を明確にしていること。
＜主旨＞
組織として情報システムの資源である情報資産、人的資産、外部資源の活用等を明確にす

る必要がある。
＜着眼点＞
① 情報システムの資源である情報資産、人的資産、外部資源の活用等を明確にする部門が定まっていること。
② その部門でどのように情報資産、人的資産、外部資源の活用等を把握することができるかをルール化しておくこと。

(2) 経営陣は、情報資産に対する管理方針及び体制を明確にしていること。
＜主旨＞
組織の経営上重要な資産である情報資産を適切に管理し、有効利用するため、管理の方針を定め、その体制を明確にする必要がある。
＜着眼点＞
① 情報資産の管理方針及び体制は、文書化され、経営陣が承認していること。
② 情報資産の管理方針及び体制について、関係者に周知徹底していること。
③ 管理すべき情報資産を明確にしていること。

(3) 経営陣は、情報システム戦略において外部資源の活用を考慮していること。
＜主旨＞
情報システム戦略において資源面の制約事項を排除するためには、組織内部の資源だけでなく、外部資源の活用を考慮する必要がある。
＜着眼点＞
① 内部資源の量及び質を正しく把握して検討を行っていること。
② 内部資源のコストを常に外部資源のコストと比較していること。
③ 代替案の検討において資源の不足を制約事項とする際には、外部資源の採用が困難である理由が明確にされていること。

(4) 経営陣は、情報資産の効率的で有効な活用を指示し、その結果をモニタすること。
＜主旨＞
経営戦略や情報システム戦略の目的を達成するため、情報システム投資の方針に基づき、情報資産を効率的かつ有効に活用する必要がある。
＜着眼点＞
① 情報資産の効率的かつ有効な活用方法を指示していること。
② 情報資産が効率的かつ有効に活用されているかどうかをモニタリングしていること。

(5) 経営陣は、情報資産の共有化による生産性向上を考慮し、その結果をモニタすること。
＜主旨＞

経営戦略や情報システム戦略の目的を達成するため、情報資産の共有化による生産性向上を図る必要がある。

＜着眼点＞

① 情報資産の共有化を図っていること。

② 情報資産の共有化による生産性向上の指標を設定していること。

③ 情報資産の共有化による生産性向上をモニタリングしていること。

(6) 経営陣は、人的資源に関する現在及び発展するニーズを考慮し、人間行動を尊重することを指示し、その結果をモニタすること。

＜主旨＞

情報システムの方針、指針及び決定において、人的資源の現在及び将来のニーズを考慮し、人間行動を尊重することを指示し、その結果をモニタする必要がある。

＜着眼点＞

① 情報システムに関する人間行動が特定され、適切に考慮されていること

② 人間行動に対するリスクが、方針及び手順に従って管理されていること

③ 管理されている事項が適切な管理者に適時報告されていること

④ 人間行動に対して適切な注意が払われていることを確実にするために、人間行動に関する管理をモニタリングしていること

(7) 経営陣は、情報技術に関する人的資源の現状及び必要とされる人材を明確にすること。

＜主旨＞

情報システム戦略の目標を達成するために、組織における情報技術に関する人的資源の現状を適切に把握し、必要とされる人材、能力を明らかにする必要がある。

＜着眼点＞

① 経営陣は、組織内のスキルズインベントリを文書化し、定期的に更新していること。

② 人材のスキルズインベントリは、組織の技術指針と整合性がとれていること。

③ 必要とされる人材の持つべき能力や経験を明確化していること。

(8) 経営陣は、人的資源の調達及び育成の方針を明確にしていること。

＜主旨＞

組織の情報システムに必要な人材の現状及び将来計画に従って、人的資源の採用、育成の方針を明文化し、これを周知徹底する必要がある。

＜着眼点＞

① 経営陣は、情報システム化人材の採用方針、計画を明確にしていること。

② 経営陣は、内部人材の育成の方針、計画を明確にしていること。

③ 経営陣は、外部資源の調達の方針を明確にしていること。

7. コンプライアンスの評価・指示・モニタ

(1) 経営陣は、情報システムに関する法令及び規制の遵守のための管理体制を確立するとともに、管理者を定めていること。

＜主旨＞

情報システムに関する法令及び規制を遵守し適切に管理していくためには、組織として、法令及び規制の所管部門を明らかにし、管理体制を確立するとともに、管理者を定めてモニタする必要がある。

＜着眼点＞

① 組織内において、法令及び規制の所管部門を定めていること。
② 法令及び規制の所管部門において、管理責任者を定め、責任の所在を明確にしていること。
③ 該当部門の職務分掌として、法令及び規制の所管を明確に位置付けていること。
④ 法令及び規制の管理責任者は、組織内において法令及び規制の遵守状況をモニタリングしていること。

(2) 経営陣は、情報システムに関して遵守すべき法令及び規範を識別し、関係者への教育及び周知徹底を指示し、その結果をモニタしていること。

＜主旨＞

法令及び規制を遵守し適切に管理していくためには、組織として遵守すべき法令及び規制を明確に識別し特定することが必要である。その上で、特定した法令及び規制を関係者に知らせるための体制を確立し、関係者に周知徹底する必要がある。

＜着眼点＞

① 組織内において、遵守することが求められる関係法令や規制を識別し特定すること。
② 特定した関係法令や規制について、経営陣は、組織内外の必要な関係者に周知徹底するために必要な教育体制を確立していること。
③ 関係法令及び規制についての教育の実施責任者を定め、必要な教育を実施し、関係者に周知徹底していること。
④ 関係法令及び規制について必要な教育を実施し関係者に周知徹底していることをモニタリングしていること
⑤ 特定した関係法令及び規制については、定期的に見直しを行っていること。

(3) 経営陣は、情報倫理規程を定め、関係者への教育及び周知徹底を指示し、その結果をモニタしていること。

＜主旨＞

組織として、法令及び規制を遵守し適切に管理していくためには、組織内の遵守すべきル

ールとして、情報倫理規程を定めるとともに、組織内外の関係者に教育し、周知徹底する必要がある。

＜着眼点＞

① 業務遂行上必要となる関係法令や規制に基づき、組織が遵守すべきルールを情報倫理規程として定めていること。

② 情報倫理規程を周知徹底するための教育体制を確立するとともに、必要な関係者に教育を実施していること。

③ 情報倫理規程を周知徹底するための教育体制の確立と必要な関係者に教育を実施していることをモニタリングしていること。

④ 経営陣は、情報倫理規程について定期的に見直しを行っていること。

(4) 経営陣は、個人情報の取扱い、知的財産権の保護、外部へのデータ提供等に関する方針を定めて指示し、その結果をモニタしていること。

＜主旨＞

法令及び規制を遵守していく上で、組織内外の各種権利保護の観点から、個人情報の取扱い、知的財産権の保護、外部へのデータ提供等に関して、組織としての考え方を明確にした方針を定める必要がある。

＜着眼点＞

① 経営陣は、個人情報保護の観点から個人情報取扱方針を定めていること。

② 経営陣は、知的財産権の保護の観点から知的財産取扱方針を定めていること。

③ 経営陣は、各種権利保護とデータ取扱いの観点から、外部へのデータ提供に関する方針を定めていること。

④ 経営陣は、定めた方針を実行するため、業務遂行に必要な手順書、マニュアルを定め、組織内外の関係者に周知徹底していること。

⑤ 経営陣は、業務遂行に必要な手順書、マニュアルを定め、組織内外の関係者に周知徹底した結果をモニタリングしていること。

8. 情報セキュリティの評価・指示・モニタ

(1) 経営陣は、情報セキュリティの現在及び予想される環境変化を考慮し評価すること。

＜主旨＞

情報セキュリティにおいて、現在の状況と予測される環境変化に基づいて、その変化がもたらすリスクを考慮して、適切な対応策を評価する必要がある。

＜着眼点＞

① 経営陣は、情報システム戦略において、保護すべき情報資産を明確にしていること。

② 経営陣は、情報資産に係るリスクを幅広く評価していること。

③ 経営陣は、情報セキュリティ対策の有効性の評価結果に対応して、必要な処置の優先

順位を決定していること。

(2) 経営陣は、情報セキュリティの目的及び戦略を明確にして指示すること。
＜主旨＞
不正防止、機密保護、個人情報保護等について、健全な経営活動推進の基盤であるため、情報セキュリティ対策の方針を情報システム戦略で明確にする必要がある。
＜着眼点＞
① 業務の重要度及びリスクに応じて、情報資産のセキュリティ対策の方針を明確にしていること。
② 経営陣は、情報資産のセキュリティ対策の方針を関係者に周知徹底することを指示していること。
③ 個人情報保護等の法令等への遵守を指示すること。
④ 情報システム戦略には、情報セキュリティ対策の方針が明確に示されていること。

(3) 経営陣は、情報セキュリティ対策の有効性をモニタしていること。
＜主旨＞
不正防止、機密保護、個人情報保護等について、講じられている情報セキュリティ対策が、健全な経営活動推進の基盤となっていることをモニタリングしている必要がある。
＜着眼点＞
① 情報セキュリティ対策の有効性、及び内外部の要求事項への適合性をモニタリングしていること。
② 変化する事業、法制度、規制、及びそれらの情報資産に対するリスクの潜在的影響を考慮していること。

9. リスクマネジメントの評価・指示・モニタ
(1) 経営陣は、情報システムリスクについて、情報システム戦略と情報システムに関わるリスクを管理する体制と役割を明確にしていること
＜主旨＞
情報システム戦略と情報システムに関わるリスクを組織として管理する役割と体制を明確にする必要がある。
＜着眼点＞
① 情報システム戦略と情報システムに関わるリスクの発生する対象を明確にしていることにより、組織におけるリスク管理体制を設置していること。
② リスク管理体制の役割、責任及び権限を明確にしていること。

(2) 経営陣は、情報資産に対するリスクの抽出とその対策についてモニタリングし、評価

すること。
＜主旨＞
情報資産の信頼性、安全性を確保するため、情報資産がもっているリスクについて洗い出し、その大きさと対応策を評価する必要がある。
＜着眼点＞
① 管理すべき情報資産の目録を作成していること。
② 情報資産ごとにリスクを洗い出していること。
③ リスクが顕在化した場合の対応策が明確になっていること。
④ 環境変化に応じてリスクの再洗い出しと、対応策の見直しが行われていること。

(3) 経営陣は、情報資産に対するリスクマネジメントの方針を明確に指示すること。
＜主旨＞
情報資産のリスク評価に基づいて、そのリスクへの対応レベルと対応策を指示する必要がある。
① 情報資産のリスクごとに対応策のマネジメントの方針を設定していること。
② 情報資産のリスクへの対応策の検討を指示していること。

(4) 経営陣は、策定したリスクマネジメントの方針を、関係各部門への周知徹底を指示することと、その結果をモニタすること。
＜主旨＞
リスクマネジメントの対応力を高めるため、経営陣は関係者に周知徹底する必要がある。
＜着眼点＞
① 経営陣は、リスクマネジメントの方針を周知徹底する方法を明確にしていること。
② 経営陣は、周知徹底されたことをモニタリングしていること。

10. 事業継続管理の評価・指示・モニタ
(1) 経営陣は、情報戦略及び情報システムに関連した事業継続の方針を策定していること。
＜主旨＞
組織の事業継続性を確保するため、情報戦略や情報システムに関連した事業継続の方針を定める必要がある。
＜着眼点＞
① 経営陣は、情報戦略や情報システムに関連した事業継続の対象範囲を明確にしていること。
② 経営陣は、情報戦略や情報システムに関連した事業継続の方針を策定し、文書化していること。
③ 事業継続の対象範囲には、災害時対応計画等も含むこと。

(2) 事業継続計画は、利害関係者を含んだ組織的体制で立案し、経営陣が評価して承認していること。

＜主旨＞

事業継続にかかわる事象が発生した場合にすべての利害関係者が円滑に対応できるようにするため、利害関係者を含んだ組織体制で実行性の高い事業継続計画を立案し、経営陣が評価をして承認する必要がある。

＜着眼点＞

① 事業継続計画は、利害関係者を含んだ組織体制で立案していること。

② 事業継続計画を経営陣が評価して承認していること。

(3) 経営陣は、事業継続計画を、関係各部門への周知徹底を指示することと、その結果をモニタすること。

＜主旨＞

事業継続計画の実行性を高めるため、経営陣は事業継続計画を関係者に周知徹底する必要がある。

＜着眼点＞

① 経営陣は、周知徹底の方法を明確にしていること。

② 経営陣は、周知徹底されたことをモニタリングしていること。

Ⅱ.企画フェーズ

1. プロジェクト計画の管理

(1) 経営陣は、プロジェクト運営委員会を設置すること。

＜主旨＞

経営陣は、プロジェクト運営委員会に、プロジェクトの開始、計画変更、終了、及び重要事項にかかる意思決定に責任を持たせるために、権限を委譲する必要がある。

経営陣は、利害関係者のニーズが確実にプロジェクトに反映されるようにプロジェクト運営委員を選定する必要がある。

＜着眼点＞

① プロジェクト運営委員は、プロジェクトに利害関係を有していること。

② プロジェクト運営委員は、IT 投資に対する責任を有していること。

(2) プロジェクト運営委員会は、プロジェクトマネージャ(PM)を任命すること。

＜主旨＞

プロジェクト運営委員会は、PM に、プロジェクトの企画立案、運営管理等の責任を持たせるために、権限を委譲する必要がある。

＜着眼点＞

① PM は、プロジェクトの対象となる業務に関する知見を有していること。

② PM は、プロジェクト管理に関する体系的な知識・経験を有していること。

③ PM は、プロジェクト管理に関する資格を取得する等、継続的なスキル向上に取り組んでいること。

(3) PM は、プロジェクト計画を策定し、プロジェクト運営委員会の承認を得ること。

＜主旨＞

PM は、情報システム戦略を達成するために、適切かつ実現性のあるプロジェクト計画を策定する必要がある。また、プロジェクト運営委員会は、利害関係者のニーズが反映されていることを確認し、承認する必要がある。

プロジェクト計画には少なくとも以下の内容を含める必要がある。

① プロジェクトの目的

② 対象業務

③ プロジェクト体制

④ スケジュール

⑤ 投資額（予算）

⑥ 期待される効果

＜着眼点＞

① プロジェクトの目的が情報システム戦略と整合していること。

② 対象業務が明確に定義されていること。
③ プロジェクト体制において、利用部門及び情報システム部門の役割が明確になっていること。
④ システムリリースの時期が適切に設定されていること。
⑤ スケジュールに利用部門への教育及び情報システム部門への訓練が含まれていること。
⑥ 既存システムを更改する場合は、既存システムの評価を行うこと。

(4) PM は、要件定義に必要な体制を確保すること。
＜主旨＞
PM は、要件定義を遺漏なく進めるために、必要な要員を確保するようプロジェクト運営委員会に要請し、必要な体制を確保する必要がある。
＜着眼点＞
① 実務に精通している利用部門の担当者が参画すること。
② 開発、運用及び保守の担当者が参画すること。

2. 要件定義の管理
(1) プロジェクト運営委員会は、要件定義の作業内容を定めるよう PM に指示すること。
＜主旨＞
システム開発において実装すべき機能や満たすべき要求が漏れないようにするために、PM は要件定義の作業内容を予め明確にする必要がある。
＜着眼点＞
① 要件定義書に記載すべき項目を明確にしていること。
② 要件定義書に対する変更を追跡する仕組みが存在すること。

(2) PM は、利害関係者の要求を収集・分析・調整すること。
＜主旨＞
システム開発において手戻りが発生することを防ぐために、PM は全ての要望を確実に収集し、分析・調整する必要がある。
＜着眼点＞
① PM は、利害関係者の全ての要求を記録すること。
② PM は、要求を分析し、システムとして実現する要件とすること。
③ PM は、要件を機能要件と非機能要件に分類すること。
④ PM は、要求を出した利害関係者に要求の必要性及び重要性を確認し、機能要件、非機能要件毎に優先順位を付けること。
⑤ 新規にパッケージソフトを導入する場合は、パッケージソフトの機能と業務のフィ

ットアンドギャップ分析を行うこと。また、既存システムをパッケージソフトで更改する場合は、既存システム及び業務とのフィットアンドギャップ分析を行うこと。

⑥　情報セキュリティに関する要件は、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

(3) プロジェクト運営委員会は、優先順位付けの適切性を検証すること。

＜主旨＞

プロジェクト運営委員会は、情報システム戦略から逸脱しないようにするために、要件に対する優先順位付けが適切に行われていることを検証する必要がある。

＜着眼点＞

①　全ての要件に対して定量的及び定性的評価を実施していること。

②　評価の尺度又は根拠が明確になっていること。

③　費用対効果を明らかにしていること。

(4) PM は、開発方針を策定すること。

＜主旨＞

PM は、プロジェクト計画を踏まえ、検証された要件に基づき、適切かつ実現性のある開発を行うために、開発方針を策定する必要がある。

開発方針には、開発手法が含まれる。開発手法とはプロジェクトの作業内容を類型化したものであり、代表的なものとしてウォーターフォール開発やアジャイル開発がある。プログラミングを伴わないパッケージソフトの導入や外部サービスの利用も開発手法に含まれる。

一つの開発方針につき、複数の開発手法を組み合わせることが可能である。その場合は、作業が重複しないよう適用範囲を明確にする必要がある。

＜着眼点＞

①　複数の開発方針を策定すること。

②　開発方針毎に機能要件・非機能要件への適合性を明らかにすること。

③　開発方針毎に開発期間、コストを明らかにし、効果を定量的に評価すること。

④　開発方針において、複数の開発手法を組み合わせる際は、開発手法毎の適用範囲を明確にすること。

(5) PM は、プロジェクトのリスクを分析し、対策を検討すること。

＜主旨＞

PM は、プロジェクトのリスクが発現しないようにするために、予めプロジェクトのリスクを洗い出し、対策を検討しておく必要がある。

＜着眼点＞

①　リスクの特定にあたって利害関係者の協力を求めること。

② 機能、技術、品質、情報セキュリティ等の観点からリスクの一覧を作成すること。
③ リスクの一覧に対して、発生確率と影響度から優先順位を付けること。
④ リスクの高い順に、リスク対応策を検討すること。

(6) PM は、要件定義書を作成し、プロジェクト運営委員会の承認を得ること。
＜主旨＞
システム開発において手戻りが発生しないようにするために、プロジェクト運営委員会は要件定義書の内容が適切であることを確認し、承認する必要がある。
＜着眼点＞
① 全ての要件が利害関係者によって検証されていること。
② 要件の優先順位に利害関係者が合意していること。
③ 開発方針が適切であること。
④ プロジェクトのリスク及び対策が適切であること。
⑤ パッケージソフトを使用する際は、パッケージソフトでは実現できない要件について利用部門の管理者の承認を得ること。
⑥ システム開発によって影響を受ける業務を明らかにし、管理体制、諸規程等の見直しを検討すること。

3. 調達の管理
(1) プロジェクト運営委員会は、システムにかかる調達方法を明確にするよう PM に指示すること。
＜主旨＞
調達とは、システムの実現に必要となる社内外の全ての資源が対象であり、ソフトウェア、ハードウェア、ネットワークだけでなく、人的資源及びサービス等も含まれる。
情報システム戦略及び要件定義書と整合した調達を行うために、予め調達の対象及び要求事項を明確にする必要がある。
ただし、外部サービスを利用する際は、Ⅶ. 外部サービス管理で記載するために、本項は対象外となる。
＜着眼点＞
① PM は、情報システム部門の協力を仰ぎ、調達に必要な情報を収集すること。
② PM は、要件定義書に基づき、調達の要求事項を明確にすること。
③ PM は、調達先を客観的に評価できるよう評価基準を策定し、評価すること。
④ PM は、調達に際して、複数の調達先を比較することが望ましい。
⑤ パッケージソフトの調達の際は、禁止事項、附帯サービスの内容、及びバージョンアップの条件を明確にすること。
⑥ 人的資源として、開発、テスト、保守、運用の担当者が含まれていること。

⑦　PM は、競争入札を用いて、複数の調達先を比較すること。

(2) PM は、プロジェクト計画に基づき、調達の要求事項を作成すること。

＜主旨＞

PM は、情報システム戦略から逸脱しないようにするために、プロジェクト計画及び要件定義書に基づき、調達の要求事項を作成する必要がある。

＜着眼点＞

①　人的資源を調達する際、求めるスキル、人数、期間を明確にすること。

②　ソフトウェア、ハードウェア、ネットワークを調達する際、必要な仕様を明確にすること。

③　資源が必要となる時期・予算が明確になっていること。

④　プロジェクト運営委員会によって承認されること。

Ⅲ．開発フェーズ

1. 開発ルールの管理

(1) 情報システム部門長は、事前にシステム開発部署とシステム運用部署の責任を分離すること。

＜主旨＞

システム開発業務において不正を防止するために、開発と運用の責任を分離する必要がある。

＜着眼点＞

① システム開発部署の職務及び責任が明確に定められていること。

② システム開発部署の職務及び責任には、システム運用、システム利用を含めないこと。

(2) PM は、プロジェクト標準を策定し、文書化し、プロジェクト運営委員会の承認を得ること。

＜主旨＞

プロジェクトの品質を確保するためには、プロジェクトの担当者が遵守すべきガイドラインとしてプロジェクト標準を定める必要がある。プロジェクト標準には以下の内容が含まれる。

① 成果物に関する標準

② 作業に関する標準

③ プロジェクト支援ツール

＜着眼点＞

① PM は、プロジェクト標準の策定に必要な資源を確保すること。

② PM は、開発の規模、開発手法、システムの特性、スキルレベルに適合したプロジェクト標準を策定すること。

③ プロジェクト担当者が遵守すべき項目を明確に記載すること。

④ プロジェクト支援ツールの選択にあたっては、適用可能性や効果を評価すること。

⑤ プログラムのコーディング標準を定めること。

⑥ 品質、コスト、進捗に関する測定指標を定義すること。

⑦ 他のシステムとの整合性を確保すること。

⑧ 外部委託を行う場合は、「Ⅶ．外部サービス管理」に準ずること。

⑨ プロジェクト標準に関わる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

2. 基本設計の管理

(1) PM は、基本設計を作成し、文書化すること。

＜主旨＞

要件が充足されるようにするために、要件定義から、実装を考慮した基本設計を作成する必要がある。

基本設計は、業務プロセスの全体像及びシステムの実装方針を決定し、アプリケーションに共通する機能を定義する工程である。

基本設計の対象は、アプリケーション、ハードウェア、ソフトウェア、ネットワークだけでなく、業務プロセス及びサービスが含まれる。

＜着眼点＞

① プロジェクト標準を充足した文書を作成し、レビューを実施すること。
② システム運用及びシステム保守が容易になるよう、システム運用及びシステム保守の基本方針を定めること。
③ 入出力画面、入出力帳票について、ユーザの利便性を考慮するために、利用部門が参画すること。
④ データのインテグリティを確保すること。
⑤ データベース及びネットワークが業務内容及びシステムの特性に適合していること。
⑥ システムが充足すべき性能を明確にすること。
⑦ システムの運用及び保守を容易にすること。
⑧ 接続が必要な他のシステムの仕様が明確になっていること。
⑨ 障害対策を考慮した設計とすること。
⑩ 誤謬防止、不正防止、機密保護等を考慮すること。
⑪ テスト計画として、テストの目的、範囲、体制、方法、スケジュールを明確にすること。
⑫ ユーザへの教育方針、スケジュールを明確にすること。
⑬ ログ等の監査証跡を確保できるよう考慮すること。
⑭ 情報セキュリティに関する基本設計は、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

(2) プロジェクト運営委員会は、基本設計を承認すること。

＜主旨＞

基本設計が十分な品質を満たしていることを確認するために、プロジェクト運営委員会は、レビュー等を実施し、基本設計を承認する必要がある。

＜着眼点＞

① プロジェクト標準を充足していること。
② 情報セキュリティ管理基準を充足していること。
③ 要件定義から遺漏が無いこと。

3. 詳細設計の管理

(1) PM は、詳細設計を作成し、文書化すること。

＜主旨＞

個別具体的な要件が充足されるようにするために、基本設計から、実装に必要な詳細設計を作成する必要がある。

詳細設計とは、基本設計で定義されたシステムの構成要素に対して、実装に繋がる仕様又は詳細を定義する工程である。

＜着眼点＞

① プロジェクト標準を充足した文書を作成し、レビューを実施すること。
② 新しい業務プロセスにおけるユースケースが定義されていること。
③ 新しい業務プロセスの手順、業務処理上のルールが明確になっていること。
④ 新しい業務処理上のリスクに対するコントロールは可能な限り自動化すること。
⑤ 連携するシステムが洗い出され、インターフェースが明確になっていること。
⑥ データの入力方法、定義、検証方法が明確になっていること。
⑦ データの保管方法、保管場所が明確になっていること。
⑧ システムの冗長性、復旧、バックアップについて考慮されていること。
⑨ ユーザにとって使いやすいユーザインタフェースとなっていること。
⑩ 情報セキュリティに関する詳細設計は、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

(2) PM は、テストの要件を検討すること。

＜主旨＞

詳細設計の品質を高めるために、詳細設計に基づき、テストに必要となる要件を特定する必要がある。

＜着眼点＞

① ハードウェア及びネットワークにおける制約を明確にすること。
② ユーザにおけるパフォーマンス要件を定量化すること。
③ 運用担当者及び保守担当者の観点から、設計上の弱点を明らかにすること。
④ ログ等の証跡によってエラーの原因を特定できること。
⑤ 情報セキュリティに関するテストの要件は、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

(3) プロジェクト運営委員会は、詳細設計を承認すること。

＜主旨＞

プロジェクト運営委員会は、レビュー等によって、基本設計が十分な品質を満たしていることを確認する必要がある。

＜着眼点＞

① プロジェクト標準を充足していること。

② 情報セキュリティ管理基準を充足していること。

③ 基本設計から遺漏がないこと。

④ 詳細設計時に発見した基本設計の矛盾は、基本設計に遡って解決していること。

4. 実装の管理

(1) PM は、プロジェクト計画、プロジェクト標準に従い、プログラミング及び実装を実施すること。

＜主旨＞

プログラミングは、アプリケーションのプログラムコードを記述する作業であり、実装は、アプリケーション以外のハードウェア、ソフトウェア、ネットワーク、サービスを導入し、必要な設定を行う作業である。

要件定義で定義された要件を正確にプログラムに反映及び実装し、品質を確保するために、開発担当者は、プロジェクト標準に従い、詳細設計に基づき、プログラミング及び実装を実施するよう開発担当者に指示する必要がある。

＜着眼点＞

① 詳細設計に基づいてプログラミング及び実装を行うこと。

② 外部に委託する場合は、外部委託先の役割を明確にし、プロジェクト標準を遵守していることを定期的に点検すること。

③ プログラミング及び実装中に判明した基本設計・詳細設計の不備について、修正及び承認の手続を定めておくこと。

④ 成果物は、プロジェクト標準に従って文書化し、レビューを受けること。

⑤ 成果物に対するバージョン管理を維持すること。

⑥ 外部システムとの相互運用性をレビューすること。

⑦ 情報セキュリティの要求事項が厳しいデータについては、利用責任を明確にすること。

⑧ プログラムコードは、コーディング標準に適合していること。

(2) PM は、単体テスト計画を作成し、単体テストを実施すること。

＜主旨＞

プログラミング及び実装された機能が、過不足なく正確に稼動することを検証するために、全ての機能に対して単体テストを実施する必要がある。

＜着眼点＞

① 単体テスト計画には、テストの目的、範囲、体制、テストケース、スケジュールを明記すること。

② 重要プログラムはプログラム作成者以外によってテストされること。
③ 利害関係者は単体テスト計画をレビューすること。
④ 単体テスト計画に基づき、単体テストを実施すること。
⑤ 単体テストで発見されたバグは修正が完了していること。
⑥ 単体テストの結果は、プロジェクト運営委員会の承認を得ること。

5. システムテスト（総合テスト）の管理

(1) PM は、システムテスト計画を作成し、文書化すること。

＜主旨＞

本番稼動後にシステム上の不備が発現しないようにするために、PM は、網羅的なテストケースを想定し、システムテスト計画を作成する必要がある。

システムテストには結合テスト及び総合テストがある。結合テストとは単体テストが完了したプログラムに対して、プログラム間インターフェースの適切性を検証するテストである。総合テストは性能、運用、操作性といった総合的な観点から、システムの完全性を検証するテストである。

システムテスト計画には以下の観点が含まれる。

① システムテストの目的、範囲、体制、スケジュール
② 本番運用手順
③ 性能・キャパシティ
④ 情報セキュリティ要求事項(個人番号・個人情報の取り扱いに関する要件を含む)
⑤ 内部統制
⑥ データ品質

＜着眼点＞

① 基本設計及び詳細設計に基づき、テストケースを策定すること。
② 本番環境との差異等、システムテスト環境を明確にすること。
③ システムテスト環境は本番環境と隔離し、本番環境に影響を与えないこと。
④ 運用担当者もシステムテストに参加すること。
⑤ テスト手法、進捗、結果に対する目標値、及び報告方法を明確にすること。
⑥ テストデータとして本番データを使用しないこと
⑦ システムテスト計画は、利害関係者のレビューを受けること
⑧ システムテストに関わる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

(2) プロジェクト運営委員会は、システムテスト計画を承認すること。

＜主旨＞

システムテストが有効に機能するようにするために、プロジェクト運営委員会はシステ

ムテスト計画を承認する必要がある。
＜着眼点＞
① テストケースは基本設計・詳細設計に基づいて網羅的に洗い出されていること
② 結合テストではプログラム間インターフェースの適切性を検証すること
③ 総合テストでは性能、運用、操作性といった総合的な観点から完全性を検証すること。
④ テストに必要な人的資源(開発担当者、テスト担当者、運用担当者等)が確保可能であること。
⑤ システムテスト環境が確保されていること。
⑥ システムテストにおける作業単位、役割、実行責任が明確になっていること。
⑦ システムテストの開始基準、及び終了基準が明確になっていること。
⑧ 情報セキュリティ管理基準を充足していること。

(3) PM は、情報システム部門に、システムテスト環境を準備させること。
＜主旨＞
システムテスト環境の構築は、プロジェクトとは別にするために、情報システム部門が準備する必要がある。
＜着眼点＞
① システムテスト計画に基づき、スケジュール内に準備すること。
② 総合テストにおいては、性能、運用、操作性、情報セキュリティといった観点毎に検証環境を検討すること。

(4) PM は、システムテストの状況を収集し、結果を評価し、文書化すること。
＜主旨＞
システムテスト結果を検証可能とするために、PM はシステムテストの進捗状況及び品質を収集し、テスト結果を評価し、文書化する必要がある。
＜着眼点＞
① システムテスト計画に基づき、進捗及び品質を管理すること。
② 進捗及び品質上の問題に対して、適切な対策を実施すること。
③ 判明したバグは速やかに修正し、利害関係者の承認を受けること。
④ システムテストの結果について、関係者によりレビューが行われ、評価が実施されること
⑤ システムテストの結果、及びレビュー結果を文書化すること。

(5) プロジェクト運営委員会は、システムテストの結果を承認すること。
＜主旨＞
本番稼動後にシステム上の不備が発現しないようにするために、プロジェクト運営委員

会は、システムテストの結果を承認する必要がある。
＜着眼点＞
① システムテスト結果は記録され、文書化されていること。
② システムテストの終了基準を充足していること。

6. ユーザ受入テストの管理
(1) PM は、ユーザ受入テスト計画を作成すること。
＜主旨＞
ユーザ受入テストを円滑に実施するために、あらかじめ、必要な資源、スケジュールを明確にする必要がある。
ユーザ受入テスト計画には、以下の観点が含まれる。
① 業務フローの検証
② 本番移行及びフォールバック（移行が失敗した場合の復旧）・バックアップ手順の確認
③ 現行システムとの処理結果の比較
＜着眼点＞
① 要件定義に基づき、ユーザの目線でテストケースを策定すること。
② ユーザ受入テスト環境を明確にすること。
③ ユーザ受入テスト環境は本番環境と隔離すること。
④ ユーザ及び運用担当者がテストに参加すること。
⑤ テスト手法、進捗、結果に対する目標値、及び報告方法を明確にすること。
⑥ パッケージソフトを使用する場合は、開発元による品質テストの結果を確認すること。
⑦ ユーザ受入テストに関わる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

(2) プロジェクト運営委員会は、ユーザ受入テスト計画を承認すること。
＜主旨＞
ユーザ受入テストに必要な資源を確保するために、ユーザ受入テスト計画はプロジェクト運営委員会によって承認される必要がある。
＜着眼点＞
① ユーザにとって業務上重要であり、本番運用を想定したテストケースを網羅していること。
② テストに必要な人的資源(開発担当者、テスト担当者、運用担当者、ユーザ等)が確保可能であること。
③ ユーザ受入テスト環境が確保されていること。

④　ユーザ受入テストにおける作業単位、役割、実行責任が明確になっていること。
⑤　ユーザ受入テストの開始基準、及び終了基準が明確になっていること。
⑥　情報セキュリティ管理基準を充足すること。

(3) システム部門は、ユーザ受入テスト環境を準備すること。
＜主旨＞
ユーザ受入テスト環境は、システム部門が準備する必要がある。
＜着眼点＞
①　システムテスト計画に基づき、スケジュール内に準備すること。
②　ユーザ受入テスト環境は本番環境と同等のものであること。

(4) PM は、ユーザ受入テストを実施し、経過を報告し、結果を文書化すること。
＜主旨＞
ユーザ受入テストの進捗及び品質を管理するために、適宜、経過を報告し、テスト結果は検証可能なように文書化する必要がある。
＜着眼点＞
①　ユーザ受入テスト計画に基づき、進捗・品質を管理すること。
②　進捗・品質上の問題に対して、適切な対策を実施すること。

(5) プロジェクト運営委員会は、ユーザ受入テストの結果を承認すること。
＜主旨＞
ユーザ受入テストの結果はプロジェクトの関係者（ユーザ、開発、運用及び保守）によって承認される必要がある。
＜着眼点＞
①　ユーザ受入テスト結果は記録され、保管されていること。
②　ユーザ受入テストの終了基準を充足していること。

7. 移行の管理
(1) PM は、移行計画を作成し、文書化すること。
＜主旨＞
円滑な移行を実現するために、予め必要な資源、リスク、対策を明確にする必要がある。
＜着眼点＞
移行計画には以下の内容を含めること
①　移行における進捗・完了の検証方法
②　業務プロセスの変更に伴う、役割と責任の変更箇所
③　事業継続計画（BCP)の変更箇所

④　情報システム部門及び外部のサービス提供事業者の協力体制
⑤　移行対象となるデータの変換方式と変換手順
⑥　移行対象となるインフラストラクチャー、アプリケーション、サービスの変更箇所と変更手順
⑦　パイロット移行、平行移行の場合の新旧のシステム環境
⑧　運用・保守に必要なドキュメント・ツール
⑨　移行作業におけるリスク及びその対策
⑩　移行に必要な予算及び設備
⑪　移行計画に関わる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

(2) プロジェクト運営委員会は、移行計画を承認すること。
＜主旨＞
運用・保守の管理者の協力を得て、移行に必要な要員、予算、設備等を確保する。
＜着眼点＞
①　移行スケジュールがプロジェクト関係者に周知されていること。
②　移行期間中のデータが必要十分であることが検証されていること。
③　移行データのバックアップが必要十分であることが検証されていること。
④　情報セキュリティ管理基準を充足していること。

(3) プロジェクト運営委員会は、移行結果を承認すること。
＜主旨＞
移行が適切に実施され、本番運用を開始できることを確認する。
＜着眼点＞
①　移行作業の結果が適切に保存されていること。
②　移行計画に即して移行作業が完了していることが検証されていること。
③　移行作業中に発見された問題が解決されていること。

8. プロジェクト管理
(1) PM は、プロジェクトの進捗をモニタリングする手法を定義すること。
＜主旨＞
プロジェクトの進捗は計画された手法で実施する必要がある。
＜着眼点＞
ルール又はガイドラインを制定すること。

(2) PM は、プロジェクトの進捗管理を継続的に実施すること。

＜主旨＞
プロジェクトの進捗管理を円滑に進めるために、進捗状況をプロジェクト運営委員会と共有する必要がある。
＜着眼点＞
① プロジェクト標準に即して、定期的に進捗状況を測定すること。
② 計画からの逸脱があれば、影響を評価し文書化すること。
③ 定期的にプロジェクト運営委員会へ進捗状況を報告すること。

(3) PM は、プロジェクトのリスクを管理すること。
＜主旨＞
プロジェクトのリスク管理を円滑に進めるために、リスクをモニタリングし、一元的に管理する必要がある。
＜着眼点＞
① プロジェクト標準に即して、定期的にプロジェクトのリスクを測定すること。
② 期待値からの逸脱があれば、影響を評価し文書化すること。
③ 定期的にプロジェクト運営委員会にリスク管理状況を報告すること。

(4) プロジェクト運営委員会は、プロジェクト終了時にレビューを実施すること。
＜主旨＞
プロジェクト終了時には期待通りの成果が得られたことを確認する必要がある。
＜着眼点＞
① プロジェクトの目標への未達に対して、対応方針が定められていること。
② プロジェクトから得られた教訓や知識を文書化すること。

9. 品質管理
(1) CIO は、開発・運用で求められる品質目標を定めること。
＜主旨＞
品質を確保するために、予め全社的に共通の品質目標を定める必要がある。
なお、品質管理の対象は、アプリケーションソフトウェアだけでなく、ネットワークやサービスも含まれる。
＜着眼点＞
① 品質目標として、計測可能な品質指標と測定方法を定めること。
② 品質指標を用いて品質目標を定義すること。
③ アジャイル開発では、個別の品質目標を定めることも可能とする

(2) CIO は、品質管理に責任と権限を明確にすること。

＜主旨＞

品質管理の有効性を高めるために、責任を明確にする必要がある。

開発における品質の責任はプロジェクト運営委員会にあり、運用における品質は運用部門の管理者にある。

＜着眼点＞

① プロジェクト運営委員会は、PM に品質管理状況を報告させること。

② PM は、品質上の問題が発生した場合は、問題毎に原因、解決策を検討すること。

③ 原因について、他のシステムやプロジェクトに類似する問題が無いか確認すること。

④ 解決策には、必要な資源、作業工数、費用見積を含めること。

⑤ 報告は、文書で行い、記録を残すこと。

⑥ アジャイル開発ではツールを用いて報告を自動化することも可能とする

⑦ プロジェクト運営委員会は、必要に応じてプロジェクト計画の見直しを PM に指示すること。

(3) CIO は、品質維持・向上に関する活動を周知すること。

＜主旨＞

品質管理は、全社的に取り組む必要がある。

＜着眼点＞

① 品質維持・向上に関する活動の重要性を組織内に周知すること。

② 品質維持・向上に関する活動の実施状況について、品質管理者から定期的に報告を受けること。

Ⅳ. アジャイル開発

従来のウォーターフォール型の開発だけでなく、アジャイル開発による開発手法も増加しており、その必要性に鑑みて、従来の取扱いに加えて、特にアジャイル開発において留意するべき取扱いについて示すものである。

1. アジャイル開発の概要

(1) 利用部門と情報システム部門・ビジネス部門が一体となったチームによって開発を実施すること。

＜主旨＞

従来型開発は、計画を確実に実行することに適した開発手法である。一方、アジャイル開発は、変化に迅速かつ柔軟に対応するための開発手法である。よって、利用部門と情報システム部門・ビジネス部門が一体となって、コミュニケーションの頻度と質を高めることを重視している。

＜着眼点＞

① アジャイル開発は、利用部門を代表するプロダクトオーナーと情報システム部門・ビジネス部門による開発チームで組成されていること。

② プロダクトオーナーと開発チームは、情報システムの目標を達成する上で対等な関係にあること。

③ プロダクトオーナーと開発チームは、双方向のコミュニケーションを随時行える環境にあること。

(2) アジャイル開発では、反復開発を実施すること。

＜主旨＞

アジャイル開発は、変化に迅速かつ柔軟に対応するために、『計画、実行、及び評価』(イテレーション)を複数回繰り返す反復開発が前提となる。

＜着眼点＞

① アジャイル開発は、開発作業を反復して実施していること。

② 各イテレーションでは、リリースを実施すること。

③ 各イテレーションでは、開発対象の要件の範囲・優先順位の見直しを実施していること。

2. アジャイル開発に関係する人材の役割

(1) プロダクトオーナーは、開発目的を達成するために必要な権限を持つこと。

＜主旨＞

アジャイル開発では、従来型開発のように予め計画した要件や品質基準を満たすことが

完了条件とはならない。プロダクトオーナーは、情報システムを開発する目的を明確に定め、その達成のための要件を開発チームに提示し、開発の完了を一意に判断する必要がある。

＜着眼点＞

① 情報システムの利用者、顧客、及び経営者の観点から、情報システムの目的を決定できる権限を持っていること。

② 情報システムの目的と、その時点での達成状況をもとに、情報システムに対する要求の範囲や優先順位の変更・見直しを決定できる権限を持っていること。

③ 情報システムの目的と、その時点での達成状況をもとに、開発の継続、完了、撤退を決定する権限を持っていること。

(2) 開発チームは、複合的な技能と、それを発揮する主体性を持つこと。

＜主旨＞

アジャイル開発では、従来型開発のように予め計画した組織体制、及び工程に基づく分業制はとらない。開発チームは、分析・設計・プログラミング・テストといった複数の技能を備え、開発作業全般を自律的に推進する必要がある。

＜着眼点＞

① イテレーション終了毎に見直された情報システムの目的や要求に基づき、分析・設計・実装・テストといった開発作業全般を自律的に計画すること。

② イテレーション終了毎に見直された情報システムの目的や要求に基づき、分析・設計・実装・テストといった開発作業全般を自律的に遂行するチーム構成及び環境であること。

③ イテレーション終了毎に見直された情報システムの目的や要求に基づき、分析・設計・実装・テストといった開発作業全般の完了条件を自律的に策定すること。

④ 情報システムの要求について、要求の範囲や優先順位をプロダクトオーナーに提言すること。

3. アジャイル開発のプロセス（反復開発）

(1) プロダクトオーナーと開発チームは、反復開発によって、ユーザが利用可能な状態の情報システムを継続的にリリースすること。

＜主旨＞

アジャイル開発では、従来型開発のように工程毎の完了基準に沿って、開発プロセスを逐次的に進めることはない。情報システムをイテレーション毎にユーザ利用可能な機能を段階的にリリースする開発プロセスである。アジャイル開発は、イテレーションを反復し、情報システムをリリースする。

＜着眼点＞

① プロダクトオーナー及び開発チームは、イテレーションの開始時に協力してイテレ

ーション計画を策定すること。

② プロダクトオーナー及び開発チームは、イテレーション計画において、イテレーションの範囲を合意すること。

③ プロダクトオーナーは、イテレーション計画において、達成すべき要求の範囲と優先順位を最新化すること。

④ 開発チームは、イテレーション計画において、開発可能な規模を見積もること。

⑤ 開発チームは、イテレーション毎に必ずテスト完了済みの利用可能な情報システムをリリースすること。

(2) プロダクトオーナーと開発チームは、反復開発を開始する前にリリース計画を策定すること。

＜主旨＞

反復開発は、従来型開発のように網羅的、不変的な要求が存在する前提に基づいていない。状況の変化に迅速に対応できるよう、複数回のイテレーションによるリリース計画を策定する必要がある。イテレーション終了ごとにリリース計画を見直す必要もある。

＜着眼点＞

① プロダクトオーナー及び開発チームは、リリース計画をイテレーション開始前に策定し、イテレーション終了ごとに見直すこと。

② プロダクトオーナーは、達成すべき要求、予算、全体スケジュール、開発範囲を明らかにし、イテレーション終了毎に見直すこと。

③ 各イテレーションの期間を定めること。各イテレーションは同じ期間(1～数週間)であること。

④ プロダクトオーナーは、イテレーション終了毎に見直したリリース計画についてプロジェクト運営委員会の承認を都度得ること。

(3) プロダクトオーナー及び開発チームは、緊密なコミュニケーションの構築ためのミーティングを実施すること。

＜主旨＞

問題を早期に対処するため、プロダクトオーナー及び開発チームは、緊密なコミュニケーションを必要とする。プロダクトオーナー及び開発チームの全員が毎日顔を合わせるなどにより必要な情報を共有することが重要である。

＜着眼点＞

① 毎日時間を決めるなど、プロダクトオーナー及び開発チームの全員が顔を合わせること。

② 短い時間(15 分が目安)で済むように共有する情報を絞ること。共有する情報の例として、作業の進捗、当日の予定、課題などがある。課題の共有を超えた解決策の議論

等は関係者のみで別途ミーティングをもつこと。

(4) プロダクトオーナー及び開発チームは、イテレーション毎に情報システム、及びその開発プロセスを評価すること。

＜主旨＞

反復開発では複数回のイテレーションを繰り返すため、イテレーション終了毎に開発プロセスを評価し、改善することが重要となる。

＜着眼点＞

① プロダクトオーナー及び開発チームは、イテレーションの終了時に情報システム及び開発プロセスについてふりかえりを行うこと。
② プロダクトオーナーは、リリース計画に対する達成状況を評価すること。
③ 開発チームは、開発プロセスの課題を洗い出すこと。
④ プロダクトオーナー及び開発チームは、全員で、次のイテレーションに向けた改善策を決定すること。

(5) プロダクトオーナー及び開発チームは、利害関係者へのデモンストレーションを実施すること。

＜主旨＞

アジャイル開発では状況に柔軟に対応するため、利害関係者にとっては、情報システムの現状が判りにくくなる。プロダクトオーナー及び開発チームは、顧客や利用者を含む利害関係者へのデモンストレーションを実施することでプロジェクトの成果を伝え、次のイテレーションに向けたフィードバックを得る必要がある。

＜着眼点＞

① プロダクトオーナー及び開発チームは、イテレーション計画にデモンストレーションの計画を含めること。
② プロダクトオーナーは、デモンストレーションの内容に合わせて利害関係者に参加を依頼すること。
③ プロダクトオーナーは、デモンストレーションの参加者からのフィードバックを収集し、次のイテレーション計画に活用すること。

Ⅴ．運用・利用フェーズ

所定の運用環境で、情報システム及びソフトウェア製品を運用し、情報システム及びソフトウェア製品の利用部門への支援を運用管理者が提供するフェーズである。運用管理手順書は、開発管理者より引継ぎを受けて、運用管理者及び情報システム部門長が承認している。その際、リスクの高い情報システムについては、運用部門と開発部門等との職務が分離されていることを確認する。但し、開発部門と運用部門等が協働してソフトウェアのリリースを迅速かつ頻繁に、あるいは反復的･継続的に実施する方法等を駆使する場合は、各部門は各々の職務遂行について常に情報を共有し、意思疎通及び相互チェックが可能な仕組みを確立して、透明性を実現する。

運用・利用フェーズで情報システムの運用を円滑に行うための活動には、情報システム運用部門が主体となる活動に限らず、情報システムの利用部門が主体となる活動を含む。

1. 運用管理ルール

(1) 運用管理者は、運用管理ルールを、開発フェーズで作成した運用設計に基づいて作成すること。

＜主旨＞

運用管理ルールと運用設計の整合性を取り、運用を円滑かつ効率的に行うために、運用管理ルールを運用設計に基づいて作成する必要がある。

＜着眼点＞

① 開発フェーズで作成した運用設計を入手していること。
② 運用設計に基づいて運用管理ルールを作成していること。
③ 運用ルールが、技術や社会的要求などの環境変化に適応していることを確認していること。

(2) 情報システム部門長は、運用管理ルールを承認すること。

＜主旨＞

運用管理ルールは、運用を円滑かつ効率的に行うために必要なものであるため、情報システム部門長が承認をする必要がある。

＜着眼点＞

① 運用管理ルールを明文化していること。
② 運用管理ルールを関係者に周知徹底していること。
③ 定期的に運用管理ルールの有効性を確認し、改善していること。

(3) 運用管理者は、運用手順を承認すること。

＜主旨＞

運用業務を効率よく実施するため、運用設計及び運用管理ルールに基づき、さらに規模、

期間、システム特性から運用手順を決定する必要がある。
＜着眼点＞
① 運用手順を明文化していること。
② 運用管理ルールに基づき、さらに規模、期間、システム特性から運用手順を決定していること。
③ 運用担当者と、その役割と責任を決定していること。

(4) 運用管理者は、作業手順を標準化し、明文化すること。
＜主旨＞
運用手順と指示書により作業品質を向上させ安定化させるため、運用手順に含まれる個別の作業の手順を標準化し、文書化する必要がある。
＜着眼点＞
① 実行ジョブ名、使用設備、資源などを具体的に明示した指示書（オペレータに対する作業指示書のこと）を作成すること。
② 作業手順を標準化し、明文化し、承認していること。
③ 例外処理の処理内容と処理方法を明文化し、承認していること。
④ 計画外の緊急処理が必要な場合の対応方法を定めて、明文化していること。

2. 運用管理
(1) 運用管理者は、年間運用計画を策定すること。
＜主旨＞
情報システムの運用を IT 戦略計画に沿って実施するため、年度単位で実行可能な運用計画を策定し、関係者の合意の上、情報システム部門長が承認し、関係者に周知徹底する必要がある。
＜着眼点＞
① 各システム予定作業項目を考慮した情報システムの年間運用計画を策定していること。
② 各イベントは、スケジュールの重複が無いように、関係者によって調整を行っていること。
③ 年間運用計画は、情報システム部門長が承認していること。
④ 年間運用計画を関係者に周知徹底していること。

(2) 運用管理者は、年間運用計画に基づいて、月次、週次、日次等の運用計画を策定すること。
＜主旨＞
情報システムの運用を円滑かつ効率的に進めるため、IT 戦略計画に沿った年間運用計画

に基づいて月次、週次、日次などの運用計画を策定する必要がある。
＜着眼点＞
① 年間運用計画に基づき、月次運用計画を策定していること。
② 月次運用計画に基づき、週次や日次運用計画を策定していること。
③ 各運用計画を関係者に周知徹底していること。

(3) 運用管理者は、運用管理ルールの遵守状況を確認すること。
＜主旨＞
運用の標準化を図り、情報システムにかかわる誤り及び不正を防止するため、運用管理ルールに従って運用管理を行う必要がある。
＜着眼点＞
① 運用の関係者が、運用管理ルールに関する教育訓練を受けていること。
② 運用の手続を運用管理ルールによって実施していること。
③ 承認されたデータのみを運用で取り扱うこと。
④ 運用記録があり、運用のモニタリングを行い、結果の分析と評価を行っていること。

(4) 運用管理者は、ジョブスケジュールを、業務処理の優先度を考慮して設定すること。
＜主旨＞
資源を有効利用し、利用部門ニーズに対応した運用を行うため、業務の優先度を考慮して処理のタイミングと順序を示したジョブスケジュールを設定する必要がある。
＜着眼点＞
① ジョブスケジュールは、運用管理ルールと利用部門からの依頼に基づき、作成していること。
② 優先度は、業務の重要性、緊急性、機密度、操作上の誤り防止、不正防止等を考慮し、設定していること。
③ オペレーションがジョブスケジュール及び指示書に基づいて行われること。
④ オペレーションの実施結果が記録されていること。

(5) 運用管理者は、例外処理のオペレーションを、運用管理ルールに基づいて行うこと。
＜主旨＞
操作上の誤り及び不正を防止し、運用を円滑に行うため、例外処理は、運用管理ルールに基づいて的確に行う必要がある。
＜着眼点＞
① 例外処理が、他の業務に及ぼす影響を調査していること。
② 例外処理の頻度及び理由を分析し、ジョブスケジュールに反映していること。

③　例外処理の定期的見直しを行い、減らすようにしていること。

(6) 運用管理者は、運用管理ルールに基づいてオペレータの交代を行うこと。
＜主旨＞
業務処理を正確かつ円滑に遂行するため、オペレータの交代は、運用管理ルールに基づいて行う必要がある。
＜着眼点＞
①　引継ぎ内容が記録されていること。
②　オペレータの引継ぎの状況を運用管理者が定期的に把握していること。

(7) 運用管理者は、指示書とオペレーション実施記録の差異分析を実施すること。
＜主旨＞
操作上の誤り及び不正を防止し、業務処理を円滑に遂行するため、指示書とオペレーション実施記録の差異分析を行う必要がある。
＜着眼点＞
①　指示書とオペレーション実施記録の差異分析を定期的に行っていること。
②　差異分析は、例外処理を含めて実施していること。
③　差異分析の結果をジョブスケジュールに反映していること。

(8) 運用管理者は、オペレーション実施記録を、運用管理ルールに基づいて一定期間保管すること。
＜主旨＞
操作上の誤り、不正、事故及び障害の原因を究明するため、オペレーション実施記録は、運用管理ルールに基づいて一定期間保管する必要がある。
＜着眼点＞
①　オペレーション実施記録及び引継記録を、定められた期間保管していること。
②　オペレーション実施記録を破棄した場合、破棄の記録をとっていること。

(9) 運用管理者は、利用部門の情報システム利用を支援すること。
＜主旨＞
購入ソフトの利用、外部の処理サービス利用、EUC など、利用部門が直接情報システムを利用する機会が増加しており、業務への貢献と円滑な処理のために、利用部門を支援する必要がある。
＜着眼点＞
①　利用部門が情報システムを利用するための基本ルールを定めていること。
②　利用部門が直接情報システムを利用することを支援する窓口を設置していること。

③　情報システム部門と利用部門で定期的に話し合う場を設けていること。

(10) 運用管理者は、情報システムの稼動実績を把握し、性能管理、リソース管理、及び資源の有効活用を図ること。

＜主旨＞

情報システムの信頼性、安全性、効率性、有効性、リソース等を確認し、費用対効果を高めるため、情報システムの稼動実績の把握と分析を行い、性能管理及び資源の有効利用を図る必要がある。

＜着眼点＞

①　情報システムのモニタリングの仕組みを有していること。
②　性能評価の指標、危機対応レベルの評価の指標、及びシステム利用の程度と利用効果測定指標を明確にしていること。
③　稼動実績を分析し、評価し、評価結果を関係者に報告していること。
④　評価に基づいて情報システムの性能管理、リソース管理、資源の有効利用を図るための対策をとっていること。

3. 情報セキュリティ管理

3. 1 情報セキュリティ管理ルール

(1)　運用管理者は、組織の情報セキュリティ方針に基づいて運用の情報セキュリティ管理ルールを作成し、遵守状況を確認すること。

＜主旨＞

情報セキュリティに関するリスクを管理するため、また情報処理設備及びシステムの正確かつセキュリティを保った運用を行うために、情報セキュリティ管理ルールを作成する必要がある。

＜着眼点＞

①　物理的、実務管理的、及び技術的な情報セキュリティ管理ルールを作成し、文書化すること。
②　情報システム部門長が承認し、関係者に周知徹底すること。
③　情報処理設備及びシステムにアクセスする外部組織を特定し、情報セキュリティ管理ルールについて合意し、適用すること。
④　情報セキュリティ管理ルールの有効性をレビューし、改善を図ること。

(2) 運用管理者は、サイバー攻撃への対処策を作成し、有効性を保つこと。

＜主旨＞

情報セキュリティに関するリスクを管理するため、データを保護するため、また情報処理設備及びシステムの正確かつセキュリティを保った運用を行うために、サイバー攻撃への

対策及び発覚後の対応策を整備し、適宜見直して有効性を保つ必要がある。
＜着眼点＞
① サイバー攻撃にかかわる物理的、実務管理的、及び技術的な対策を作成し、文書化すること。
② 情報システム部門長が承認し、関係者に周知徹底すること。
③ サイバー攻撃に関わる情報を収集し、対策を見直すこと
④ サイバー攻撃発覚後の対応策を作成すること。
⑤ 訓練によりサイバー攻撃発覚後の対応策を見直すこと。

(3) 上記以外の情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

3.2 アクセス管理
(1) 運用管理者は、情報セキュリティ方針に基づいて、運用システムへのアクセス管理ルールを作成し、情報システム部門長の承認を得て、適切に運用すること。
＜主旨＞
情報処理設備及びシステムの正確かつセキュリティを保った運用を実施するために、認可された利用者が運用システムにアクセスし、認可されていないアクセスを防止するアクセス管理ルールを作成し、関係者に周知徹底し、変更管理、定期的な見直し、特権管理などの運用を適切に行う必要がある。
＜着眼点＞
① 運用システムのアクセス管理ルールの適用範囲を明確にすること。
② 情報システム部門長が承認し、関係者に周知徹底すること。
③ 運用要員の採用・異動・退職や職務変更の際には、速やかにアクセス権の設定・変更・削除を行い、運用管理者が承認すること。
④ アクセス権付与及びアクセス権設定について、定期的に見直しを実施すること。
⑤ 一般より高い権限レベルを持つ特権的アクセス権については、設定・変更・削除について厳格に運用管理すること。
⑥ 特権的アクセス権の適用範囲を確認し、定期的な監視を行うこと。

(2) 運用管理者は、データへのアクセスコントロール及びモニタリングを、実施すること。
＜主旨＞
データへの不正アクセスの防止、不正利用の防止、機密保護及び個人情報保護のために、アクセスコントロール及びモニタリングを実施する必要がある。
＜着眼点＞
① 無資格者による情報システムの利用を定期的に調査していること。

② 特定のファイルへの偏った利用、異常な時刻での利用等を調査していること。
③ 不正利用、不正アクセスの検出時に運用管理者へ通知する手順を定めて周知していること。
④ 不正利用、不正アクセスの再発防止策を講じていること。
⑤ 業務内容、組織、基本ソフトウェア等の変更に伴い、アクセスコントロールを見直していること。

(3) 上記以外のアクセス管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

4. データ管理

(1) 運用管理者は、データ管理ルールを定め、遵守状況を確認すること。

＜主旨＞

データの誤処理防止、機密保護及び個人情報保護のために、データ管理ルールを明文化する必要がある。

＜着眼点＞

① 使用するデータを網羅した体系的なデータ管理ルールを作成すること。
② データ管理ルールを情報システム部門長が承認していること。
③ データの管理者、検証者等の役割を定め、情報システム部門長が承認していること。
④ 機密情報及び個人情報の取扱い方法を、データ管理のルールに定めていること。
⑤ データ管理ルールで定める機密度の高いデータの交換については、暗号化等の安全対策を講じていること。
⑥ データ管理ルールを関係者に周知徹底するとともに、ルールが遵守されていることを検証していること。
⑦ データ管理ルールを定期的にまた状況変化に応じて見直していること。

(2) 運用管理者は、データの知的財産権を、管理すること。

＜主旨＞

構築したデータの知的財産権の保護及び外部から導入したデータの知的財産権の侵害を防止するために、知的財産権を管理する必要がある。

＜着眼点＞

① 知的財産権の教育を実施し、著作物に対する認識をもっていること。
② 知的財産権の保護の対象とするデータを明確にしていること。
③ 外部からのデータを、定められた手続で導入していること。

④　外部から導入したデータの知的財産権を侵害していないことを定期的に調査していること。

(3) 運用管理者は、データのインテグリティ（完全性）を、維持すること。
＜主旨＞
データが正確かつ完全であり、正常である状態を保つために、データが正しく更新される必要がある。
＜着眼点＞
①　データが正常であることを検証していること。
②　データを登録・更新する場合は、正しく処理されたことを確認していること。
③　データに不具合が発生した場合の回復手段を用意しておくこと。

(4) 運用管理者は、データの利用状況を記録し、定期的に分析すること。
＜主旨＞
データの利用を予想し、不正利用を防止するために、データの利用状況を記録し、定期的に分析する必要がある。
＜着眼点＞
①　分析結果に基づき、データベース、ファイル、記録媒体等のデータ保管領域の有効利用を図ること。
②　分析結果に基づき、将来のデータ量の変化への対応を考慮していること。
③　不正利用の調査を行い、対策を講じていること。
④　不正利用を検知した場合の通報先を明確にしていること。

(5) 運用管理者は、データのバックアップの範囲、方法及びタイミングを、業務内容、処理形態及びリカバリの方法を考慮して決定すること。
＜主旨＞
データの記録媒体の障害、誤操作、コンピュータウイルス等による影響を最小にするために、データのバックアップの範囲、方法及びタイミングを、業務内容、処理形態及びリカバリの方法を考慮して決定する必要である。
＜着眼点＞
①　バックアップの範囲、タイミング、記録媒体、保管方法等を、業務内容、処理形態及びリカバリの方法に応じて定めていること。
②　バックアップ方法を、情報システムの変更に伴い、見直していること。

(6) 運用管理者は、データのバックアップの処理単位をデータ構造に基づいて定めること。
＜主旨＞

データのバックアップからの再利用を確実にするために、データのバックアップの処理単位をデータ構造に基づいて決める必要がある。

＜着眼点＞

データのバックアップの処理単位を、情報システムの変更に応じて見直していること。

(7) 運用管理者は、データの授受、保管、確認及び返却を、データ管理ルールに基づいて行わせること。

＜主旨＞

データの誤使用、不正利用、改ざん等を防止するために、データの授受は、データ管理ルールに基づいて行う必要がある。

＜着眼点＞

① データの授受を記録し、運用管理者が承認していること。

② データの授受記録を一定期間保管していること。

(8) 運用管理者は、データの交換の形態に応じた、不正防止及び機密保護の対策を講じること。

＜主旨＞

不正利用の防止、機密情報の漏えい及び個人情報保護のために、データの交換の形態に応じて、不正防止及び機密保護の対策を講ずる必要がある。

＜着眼点＞

① データの交換を運用管理者が承認していること。

② データの交換記録を定期的に分析し、改善を図ること。

(9) 運用管理者は、データの保管、複写及び廃棄に、誤びゅう防止、不正防止及び機密保護の対策を講じること。

＜主旨＞

データの不正利用、漏えいの防止及び個人情報の侵害等を防止するために、データの保管、複写、不要データの廃棄に、不正防止及び機密保護の対策を講ずる必要がある。

＜着眼点＞

① 保管、複写、廃棄に、データの記録媒体に応じた不正防止、機密保護及び個人情報保護の対策を講じていること。

② 保管、複写、廃棄を、運用管理者が承認していること。

③ データを、所定の場所、期間及び方法で保管していること。

④ データの重要度に応じて、複写を制限する対策を講じていること。

⑤ 重要なデータについては、複写履歴を記録していること。

⑥ 重要なデータの廃棄には、運用管理者が立ち会っていること。

(10) 利用部門の管理者は、データの入力管理ルールを作成し、遵守状況を管理すること。

＜主旨＞

データの正確性を期すために、入力管理ルールに基づいたデータ入力が必要である。

＜着眼点＞

① 利用部門の管理者は、入力管理ルールを明文化すること。
② 利用部門の部門長が、入力管理ルールを承認すること。
③ 利用部門の管理者が承認した担当者は、入力管理ルールに基づいて、入力を漏れなく、重複なく、正確に行うこと。
④ 利用部門の管理者は、入力データの作成手順、取扱い等で、誤びゅう防止、不正防止、機密保護等の対策を講じること。
⑤ 利用部門の管理者は、データの入力の誤びゅう防止、不正防止、機密保護等の対策を、有効に機能させること。
⑥ 利用部門の管理者は、入力データの保管及び廃棄を、入力管理ルールに基づいて行うこと。

(11) 利用部門の管理者は、出力管理ルールを作成し、遵守状況を管理すること。

＜主旨＞

出力情報の正確性を期し、機密保護及び個人情報保護のために、出力管理ルールに基づいた出力が必要である。

＜着眼点＞

① 利用部門の管理者は、出力管理ルールを明文化すること。
② 利用部門の部門長が、出力管理ルールを承認すること。
③ 利用部門の管理者は、出力情報が漏れなく、重複なく、正確であることを確認していること。
④ 利用部門の管理者は、出力情報の作成手順、取扱い等で、誤びゅう防止、不正防止及び機密保護の対策を講じること。
⑤ 利用部門の管理者は、出力情報の引渡し、保管及び廃棄を、出力管理ルールに基づいて行うこと。
⑥ 利用部門の管理者は、出力情報の利用状況及びエラー状況を、記録し、定期的に分析すること。

(12) データ管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

5. ログ管理

(1) 運用管理者は、ログを取得し、定期的に分析すること。

＜主旨＞

情報システムで発生した問題を識別するために、ログを取得し、分析することが必要である。

＜着眼点＞

① 通常の運用範囲を超えたアクセスや違反行為を含めて、運用の作業ログ、利用部門の活動ログを記録し、保管すること。

② 情報セキュリティインシデント、障害の内容ログ及び原因ログを記録し、保管すること。

③ 取得したログを、認可されていないアクセスから保護し、内容が改ざんされないように保管すること。

④ 保管したログを定期的に分析し、分析結果に応じて必要な対策を講じること。

⑤ 一定期間保管したログを、適切に廃棄すること。

⑥ 特権的アクセスのログは、その重要性から、多頻度で厳密に分析するなど特別に厳格な管理をすること。

⑦ 組織の関連する全ての情報システムのクロックを、単一の参照時刻源と同期させること。

(2) 運用管理者は、情報セキュリティ方針に基づいて、適切なツールを利用するなどして、全てのログを一元管理し、即時に分析して、可及的速やかにセキュリティインシデントの予兆や痕跡を取得し、対策を講じること。

＜主旨＞

サイバー攻撃などのセキュリティインシデントの対策を可及的速やかに講じるために、適切なツールを利用するなどして、セキュリティインシデントの予兆や痕跡を可及的速やかに取得することが必要である。

＜着眼点＞

① ログ取得の仕組みを更新する場合は、ログの管理策を更新し、明文化し、情報システム部門長の承認を得て、運用すること。

② ログの管理、分析は、訓練された実務管理者が実施すること。

(3) ログ管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

6. 構成管理

6. 1 機器の構成管理

(1) 運用管理者は、構成管理ルールを作成し、遵守状況を確認すること。

＜主旨＞

情報システムの正常かつ効率的な稼動のために、構成管理ルールを定め、遵守する必要がある。

＜着眼点＞

① 管理対象を効率的に管理するための構成管理ルールを作成すること。

② ソフトウェアのライセンス管理者を定めていること。

(2) 運用管理者は、管理するソフトウェア、ハードウェア及びネットワークを明確にして管理すること。

＜主旨＞

管理するソフトウェア、ハードウェア及びネットワークについて、二重管理及び管理の漏れが生じないようにするために、管理の対象範囲を明確にして、効率的に管理する必要がある。

＜着眼点＞

① ソフトウェア、ハードウェア等、管理対象をグループにまとめ、グループごとに構成管理の手続を明文化すること。

② 情報システムを新規開発あるいは変更して運用する際には、構成管理の手続に従うこと。

③ ハードウェア構成やネットワーク構成を変更して運用する際には、構成管理の手続に従うこと。

④ 構成変更時の影響を検討して、要求されるセキュリティのレベル、性能、可用性等の劣化を予防すること。

(3) 運用管理者は、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を作成して構成を管理すること。

＜主旨＞

情報システムの機能維持及び障害時の早期回復を図るために、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する必要がある。

＜着眼点＞

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を作成していること。

(4) 運用管理者は、ソフトウェア、ハードウェア及びネットワークの導入及び変更について、影響を受ける範囲を検討して決定すること。

＜主旨＞

情報システムの停止、機能低下等を防止し、安定稼動を図るために、ソフトウェア、ハードウェア及びネットワークの導入及び変更の際には、影響を受ける範囲を検討して決定する必要がある。

＜着眼点＞

① 影響を受ける範囲を検討していること。

② ソフトウェア、ハードウェア及びネットワークの導入及び変更を運用管理者が承認していること。

③ 構成変更の作業中、作業後の問題発生の対処の手続を定めていること。

(5) 運用管理者は、ソフトウェア、ハードウェア及びネットワークの導入及び変更について、計画を作成して実施すること。

＜主旨＞

情報システムに与える影響を最小にするために、ソフトウェア、ハードウェア及びネットワークの導入及び変更を計画的に実施する必要がある。

＜着眼点＞

① ソフトウェア、ハードウェア及びネットワークの導入及び変更の計画を作成していること。

② 計画を情報システム部門長が承認していること。

③ ソフトウェアについては、情報システム保守部門が実施すること。

④ ソフトウェア、ハードウェア及びネットワークの変更履歴を記録していること。

⑤ 計画実施後に計画実施状況を評価して、評価結果を今後の計画の作成にフィードバックしていること。

(6) 機器の構成管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

6.2 ハードウェア管理

(1) 運用管理者は、ハードウェア管理ルールを作成し、遵守状況を確認すること。

＜主旨＞

ハードウェアの適切な利用を図り、障害を防止し、不正行為等から保護するために、ハードウェア管理ルールを作成する必要がある。

＜着眼点＞

① ハードウェア管理ルールを明文化し、情報システム部門長が承認していること。

② ハードウェア管理ルールを関係者に周知徹底するとともに、ルールが遵守されていることを検証していること。

③　定期的にハードウェア管理ルールの有効性を確認し、必要に応じて見直していること。

(2) 運用管理者は、ハードウェアの保管、移設及び廃棄の際の、不正防止及び機密保護の対策を講じること。

＜主旨＞

ハードウェアの盗難、紛失等による権限者以外のハードウェア利用の防止、及びデータ等の情報資産保護のために、ハードウェアの保管、移設及び廃棄の際には、不正防止及び機密保護の対策を講ずる必要がある。

＜着眼点＞

①　ハードウェアの保管、移設及び廃棄に関するルールを定め、情報システム部門長が承認していること。

②　保管、移設及び廃棄の際には、ハードウェアの特性及び保有する情報資産に応じた不正防止、機密保護及び個人情報保護の対策を講じていること。

③　ハードウェアを、所定の場所、期間及び方法で保管していること。

④　重要なハードウェアの移設、廃棄には、運用管理者が立ち会っていること。

(3) 運用管理者は、ハードウェアを、想定されるリスクに対応できる環境に設置すること。

＜主旨＞

障害、不正行為等が情報システムに及ぼす影響を最小にするために、ハードウェアを想定されるリスクに対応できる環境に設置する必要がある。

＜着眼点＞

①　ハードウェアに関するリスク分析を計画的に行っていること。

②　リスク分析の結果に基づき、リスクに対応できる環境条件を明確にしていること。

③　リスクへの対応として設定した環境条件を維持していること。

④　リスクに対応した管理を行うこと。

(4) 運用管理者は、ハードウェアの、定期的保守を行うこと。

＜主旨＞

ハードウェア障害による情報システムの停止、機能低下を未然に防止するために、定期的に保守を実施する必要がある。

＜着眼点＞

①　保守対象、保守内容及び保守サイクルを明確にしていること。

②　保守の実施時にデータ等の漏えいを防止していること。

③　保守の結果を記録し、情報システム部門長に報告していること。

(5) 運用管理者は、ハードウェアの障害対策を講じること。

＜主旨＞

情報システムの稼動停止及び機能低下を防止し、障害発生時の早期復旧のために、ハードウェアの障害対策、を講じる必要がある。

＜着眼点＞

① 障害時の連絡体制を整備していること。

② 障害対策の現状を把握し、必要に応じてレビューしていること。

③ 障害発生のリスクを分析し、必要な障害防止策を講じていること。

④ 障害の早期復旧措置を講じていること。

⑤ 障害対策の機能を確認していること。

(6) 運用管理者は、ハードウェアの利用状況を記録し、定期的に分析して改善を図ること。

＜主旨＞

ハードウェアの有効利用を図り、不正利用を防止するために、利用状況を記録し、定期的に分析する必要がある。

＜着眼点＞

① 利用状況を記録していること。

② 利用状況の記録を分析していること。

③ 分析結果に基づき、ハードウェア利用の改善を図っていること。

(7) ハードウェア管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

6.3 ネットワーク管理

(1) ネットワークの管理者は、ネットワーク管理ルールを定め、遵守状況を確認すること。

＜主旨＞

ネットワークの正常かつ効率的な稼動のために、ネットワーク管理ルールを定める必要がある。

＜着眼点＞

① ネットワーク管理ルールを明文化し、情報システム部門長が承認していること。

② ネットワーク管理の範囲を明確にしていること。

③ ネットワークの稼動状況を常時監視できる体制を作っていること。

④ 定期的にネットワーク管理ルールの効果を確認し、必要に応じて見直していること。

(2) ネットワークの管理者は、ネットワークを利用した外部サービスを、ネットワーク管

理ルールに基づいて管理すること。

＜主旨＞

ネットワークを利用した適切な外部サービスの提供を受けるために、ネットワークを利用した情報提供等の外部サービスについて、ネットワーク管理ルールに基づいて効率的に外部サービスを利用する必要がある。

＜着眼点＞

① ネットワークを利用した情報提供等の外部サービスとそのサービスを提供する組織体を評価する手順を明確にしていること。

② 有料サービスの費用の支払手続を明確にしていること。

(3) ネットワークの管理者は、ネットワークへのアクセスコントロール及びモニタリングを実施すること。

＜主旨＞

ネットワークへの侵入及び不正使用を未然に防止し、早期に発見するために、ネットワークへのアクセスコントロール及びモニタリングを実施する必要がある。

＜着眼点＞

① ネットワークをセグメントに分割してアクセスコントロールを行っていること。

② 不正アクセスの検出時にネットワークの管理者へ通知する手順を定めて周知していること。

③ モニタリング記録の分析結果に基づいて、必要な対策を講じていること。

④ ネットワーク管理用のユーザ ID の管理を適切に行っていること。

⑤ リモートアクセスサービスとそのユーザを適切に管理していること。

⑥ 遠隔保守用のポートを適切に管理していること。

⑦ ペネトレーション（侵入）テストを行い、ネットワークへのアクセスコントロールが有効に機能していることを確認していること。

⑧ 高いセキュリティレベルが要求されるネットワーク環境では、ネットワークの利用状況を常に収集して監視し、異常が発生した場合の原因究明手続を定めていること。

(4) ネットワークの管理者は、ネットワーク監視ログを定期的に分析すること。

＜主旨＞

ネットワークへの侵入及び不正利用を検出して必要な対策を講ずるために、ネットワーク監視ログを定期的に分析する必要がある。

＜着眼点＞

① ネットワーク監視を行うために、監視ログ分析の対象となるネットワーク機器を適切に識別していること。

② ネットワーク機器の監視ログの出力に関する設定を有効にしていること。
③ 監視ログ分析作業の効率化に関する対策を検討し、実施していること。
④ 監視ログへのアクセスコントロールを行っていること。
⑤ 監視ログを適切に管理し、一定期間保存後に適切に廃棄していること。
⑥ 監視ログの分析結果についての対応を検討し、選択していること。

(5) ネットワークの管理者は、ネットワークの障害対策を講じること。
＜主旨＞
情報システム及び電子メールやWeb等の各種サービスの可用性を確保するために、ネットワークの障害対策を講ずる必要がある。
＜着眼点＞
① 重要なネットワーク機器や伝送路について、最長許容障害復旧時間を定め、最長許容障害復旧時間内に復旧するための措置を講じていること。
② 障害発生後、発生原因や対処等を記録した障害報告書を作成して、再発防止策を講じていること。
③ ネットワーク障害の発生時の対応手順を明文化していること。
④ 必要に応じて、代替の伝送路を設定していること。
⑤ ネットワークの可用性を評価して、ネットワークの障害対策を見直していること。

(6) ネットワークの管理者は、ネットワークの利用状況を記録し、定期的に分析すること。
＜主旨＞
ネットワークの効率的で安定した稼動を図るために、利用状況を記録し、定期的に分析する必要がある。
＜着眼点＞
① ネットワークの利用状況の収集、分析及び評価の手順等を明確にしていること。
② 分析結果に基づき、ネットワークの新設、変更等の改善を図っていること。

(7) ネットワーク管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

7. ファシリティ管理
(1) ファシリティの管理者は、建物及び関連設備を、想定されるリスクに対応できる環境に設置すること。
＜主旨＞
情報システムの停止、破壊等による被害を最小にするために、建物及び関連設備は、想定されるリスクを回避できる環境に設置する必要がある。

＜着眼点＞

① 想定するリスクとその対策を明確化していること。

② 自然災害の影響が最小になる場所に設置していること。

③ 侵入を防止する設備を設置していること。

④ 情報システムの設置場所を表示していないこと。

⑤ セキュリティエリアを層別に管理していること。

(2) ファシリティの管理者は、建物及び室への入退の管理について、不正防止及び機密保護の対策を講じること。

＜主旨＞

情報システムを不正行為から保護するために、建物及び室の入退管理に不正防止及び機密保護の対策を講ずる必要がある。

＜着眼点＞

① 入退館、入退室にかかわるルールを明文化していること。

② 入退館、入退室の資格を明確にしていること。

③ 検知した異常をファシリティの管理者へ連絡する方法を明確にしていること。

④ 物品の持込み及び持出しを監視していること。

(3) ファシリティの管理者は、関連設備について、適切な運用を行うこと。

＜主旨＞

電気、空調などの関連設備を継続的・安定的に運用するために、関連設備の管理・運用を行う上でのルールを定め、遵守する必要がある。

＜着眼点＞

① 関連設備を運用するためのルールを定めていること。

② ファシリティの管理者は、運用ルールの順守状況を確認していること。

(4) ファシリティの管理者は、関連設備について、定期的に保守を行うこと。

＜主旨＞

関連設備の障害による情報システムの停止、機能低下等を未然に防止するために、定期的に保守する必要がある。

＜着眼点＞

① 保守の内容及び点検項目を明確にしていること。

② 保守を定期的に行っていること。

③ 保守結果を記録し、ファシリティの管理者が承認していること。

④ 保守結果及び障害の原因に基づき、改善措置を講じていること。

(5) ファシリティの管理者は、関連設備について、障害対策を講じること。

＜主旨＞

電気、空調などの関連設備の障害を未然に防止し、あるいは早期に回復させるために、障害対策を講じる必要がある。

＜着眼点＞

① 関連設備の稼動状況を監視していること。

② 瞬断及び停電対策を講じていること。

(6) ファシリティの管理者は、建物及び室への入館及び入室を記録し、定期的に分析すること。

＜主旨＞

事故発生時に入館及び入室者を特定し、追跡調査を可能とするために、建物及び室への入管及び入室の状況を記録するとともに、ファシリティの管理者が定期的に分析する必要がある。

＜着眼点＞

① 建物及び室への入館及び入室の状況を記録していること。

② 入館（室）者を特定するとともに、事故発生時にトレース可能にしていること。

③ 建物及び室の入退の記録を定期的に分析していること。

(7) ファシリティ管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

8. サービスレベル管理

(1) 運用管理者は、提供するサービスについて、サービスの要求事項に基づいて実行可能なサービスメニューを作成し、実施すること。

＜主旨＞

提供するサービスの品質を維持向上するために、適切な管理指標に基づいてサービスの提供を実施する必要がある。

＜着眼点＞

① サービスの要求事項に基づいて、サービス目標を定めること。

② サービスの構成要素、及び作業負荷の特性を明確にして効率化を図ること。

③ サービス目標のもとに実行可能なサービスメニューを文書化し、利用部門と合意すること。

④ 情報システム部門長はサービスメニューを承認すること。

(2) 利用部門の管理者は、定期的にサービスをレビューし、変更を管理すること。

＜主旨＞

変更に伴うリスクを低減させながらサービスの品質を維持するために、サービスの変更を迅速にかつ適切に行う必要がある。

＜着眼点＞

① 運用部門の管理者は、利用部門のレビューとサービス目標に基づいて、サービスを変更すること。

② 運用部門の管理者は、サービスの変更後、サービスメニューを更新し、維持すること。

(3) 運用管理者は、サービスを継続的に改善すること。

＜主旨＞

情報システム運用部門及び利用部門の生産性を維持向上させるために、サービスの継続的な改善が必要である。

＜着眼点＞

① 運用管理者は、サービス目標に基づいた利用部門の利用状況を定期的に監視すること。

② サービスデスクは、サービスデスクの活動を運用管理者に報告すること。

③ 運用管理者は、サービスの質についての利用部門の満足度をモニタリングすること。

④ 運用管理者は、サービスの活動と成果を分析し、傾向や再発性のある問題を特定し、その対応を検討してサービスの継続的な改善に努めること。

9. インシデント管理

9. 1 インシデント対応の管理

(1) 運用管理者は、すべてのインシデントを、優先度をつけて、またインシデント管理手順を用いて、効率的かつ効果的に体系的な管理をすること。

＜主旨＞

インシデントの解決を、インシデントの影響を最小限に抑制し、利用部門と合意したサービス目標内及び時間内で迅速に達成するために、優先度を定めて効率的かつ効果的に体系的な管理をする必要がある。

＜着眼点＞

① インシデントの、事業及び利用部門への影響、及び緊急度のアセスメントに基づいて優先度を決定すること。

② インシデントを受付けてから可能な限り早く、優先度を利用部門と合意すること。

③ インシデントの影響度に応じた報告体制及び対応手順を明確にすること。

④ インシデントの内容を記録し、分析すること。

⑤ インシデントの潜在的な影響の評価に基づいて、外部の法的機関に連絡するなどのインシデント対応手順を実施すること。
⑥ 適切なログ管理機能により、インシデントの原因を究明すること。
⑦ インシデントを解決し、再発防止の措置を講じること。

(2) 運用管理者は、インシデントのエスカレーションの手続を定めること。
＜主旨＞
情報システム運用部門、サービスデスク、利用部門等関係部局で適切なコミュニケーションを行い、インシデントへの適切な対処をするために、サービスデスクのインシデントエスカレーションの手続を定める必要がある。
＜着眼点＞
① サービスデスクは、速やかに回答できない利用部門からの問合せ、要求及びインシデントを適切にエスカレーションすること。
② サービスデスクは、インシデントの対応状況をモニタリングし、常に利用部門に通知すること。
③ インシデントエスカレーションの手続は、関係者に周知徹底していること。
④ インシデントエスカレーションの手続は、環境の変化に応じて見直しを行っていること。

(3) 運用管理者は、インシデントの終了の手続を定めること。
＜主旨＞
インシデントの解決の不正確な判断を避けるために、手続を定める必要がある。
＜着眼点＞
① 利用部門からの問合せ、要求への対応完了を適時に確認し、記録を更新すること。
② インシデントの解決を利用部門と合意し、記録を更新した後に終了すること。
③ インシデントが解決した段階で、問題解決に向けて講じたステップを記録し、利用部門と合意した対応が取られていることを確認すること。
④ 回避策を取った未解決のインシデント又は既知のエラーによる再発インシデントについては、適切な問題管理に関する情報を提供できるように、記録し、運用管理者へ報告すること。
⑤ インシデントの段階的な解決策を取る場合は、利用部門と合意し、その問題がサービスに及ぼす影響を低減又は除去すること。

(4) 運用管理者は、重大なインシデントを専用に取り扱うための手順を文書化すること。
＜主旨＞
重大なインシデントは、一般に影響が大きく、その解決には特別な注意が必要となるため

に、専用の手順を定める必要がある。
＜着眼点＞
① 何が重大なインシデントに当たるかを定めていること。
② 誰が重大なインシデントであると宣言する権限を持ち、どのようにして宣言するかを定めていること。
③ 誰が活動の調整及び管理を行い、誰が関与するかを定めていること。
④ どのようにして解決作業を実施するかを定めていること。
⑤ 重大なインシデントの進行中及び終了後に誰にどのような連絡を行うかを定めていること。
⑥ 重大なインシデントの解決後のレビューを誰とどのタイミングでどのように行うかを定めていること。

(5) 運用管理者は、インシデント管理プロセスの体系的な記録を作成し、報告すること。
＜主旨＞
インシデントを迅速に解決してサービスの品質を維持向上するため、インシデント管理プロセスの体系的な記録が必要である。
＜着眼点＞
① インシデント管理の手順書及び記録を作成し報告すること。
② 重大なインシデント管理の手順書及び記録を作成し報告すること。
③ 必要に応じて速報版の報告書を発行すること。
④ 所定の期間中のインシデントに関する報告書を発行すること。
⑤ インシデント解決に要した時間及びリソースを記録し、報告すること。
⑥ インシデントの原因、再発防止策及びその効果目標を記載した報告書を発行すること。

(6) 運用管理者は、インシデント管理プロセスで必要となる要員と、その権限及び責任を適切に割り当てること。
＜主旨＞
インシデントを確実に解決するために、解決に関与する要員を特定し、要員の知識及び能力を反映して適切に割り当てる必要がある。
＜着眼点＞
① 重大なインシデントの場合は、重大なインシデント管理プロセスの発動、インシデント対応要員の動員、及び重大なインシデントに必要となる役割及び要員の特定に責任をもつ、重大なインシデントの対応管理者を適切に割り当てること。
② サービスデスクに、初期症状のデータの収集及び利用部門との継続的コミュニケーションの役割を与えること。

③　一次サポート要員を超える専門的技能及び経験を持つインシデント解決要員を、二次サポート及び三次サポートして指名すること。
④　情報システム運用部門の担当者に、インシデントの解決を補佐するための作業を割り当てること。
⑤　要員の知識及び能力を反映して作業の割当てを行っていること。

(7)　利用部門の管理者は、インシデント発生後可能な限り早く、インシデント対応の優先度を運用管理者と合意すること。
＜主旨＞
インシデントの影響を最小限に抑制し、あらかじめ定めたサービス目標内及び時間内で迅速に解決するために、優先度を定めて効率的かつ効果的に体系的な管理をする必要がある。
＜着眼点＞
①　インシデントが発生してから可能な限り早く、優先度を情報システム運用部門と合意すること。
②　インシデントを発見した場合には、速やかにサービスデスクに通知すること。

(8) 利用部門の管理者は、インシデントの終了を判断すること。
＜主旨＞
インシデントの解決の不正確な判断を避けるために、インシデントを利用部門の判断のもとで終了する手続を定める必要がある。
＜着眼点＞
①　インシデントへの適切な対応が取られて解決したことを確認し、終了を判断すること。
②　インシデントの段階的な解決策を取る場合は、その問題が利用部門に及ぼす影響を低減又は除去すること。

(9)　インシデント管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

9.2 問題管理
運用管理者は、問題を識別し、問題管理手順を整備して問題を適切に管理し、再発防止の措置を講じること。
＜主旨＞
インシデントの影響を最小化又は回避するために、問題を識別し、インシデントの根本原因を特定して恒久的な対策を講じ、また傾向分析及び予防処置を実施してインシデントの

発生を予防する必要がある。
＜着眼点＞
① 問題を識別し、記録すること。
② 問題の、事業及び利用部門への影響及び緊急度を評価して優先度を決定すること。
③ 問題の原因を究明し、解決すること。
④ 問題が解決したことについて利用部門と合意し、記録を更新し、終了すること。
⑤ 根本原因の特定及び潜在的な予防処置のために、問題のデータ及び傾向を分析すること。
⑥ 根本原因が特定されたが問題が恒久的に解決されていない場合、その問題がサービスに及ぼす影響を低減又は除去するための処置を講じること。
⑦ 問題管理手順に従って問題を管理し、必要に応じて見直すこと。

9.3 変更管理
(1) 運用管理者は、変更計画を作成して変更を適切に管理すること。
＜主旨＞
変更を確実に実施するために、全ての変更を制御された方法で体系的な管理をする必要がある。
＜着眼点＞
① 重大な影響を及ぼす変更、緊急度の高い変更、変更の成功又は失敗、を判断する基準を定めること。
② ソフトウェアの変更については、情報システム運用部門では行わず、情報システム保守部門に依頼すること。
③ 緊急変更の定義を明文化し、利用部門と合意して、管理すること。
④ 変更要求を記録すること。
⑤ 変更要求を、適用範囲、有効性、リスク、サービス及び利用部門への潜在的影響、サービスの要求事項、技術的実現可能性、事業への影響及び財務的な影響等を考慮して評価し、変更計画を作成すること。
⑥ 変更が失敗した場合に、失敗した変更を元に戻す又は修正するために必要な手順を作成し、事前に確認すること。
⑦ 変更計画を運用管理者が承認すること。
⑧ 承認された変更を、実施し、結果を確認すること。
⑨ 変更計画と実績を定期的に分析し、適切な改善の処置を講じること。

(2) 利用部門の管理者は、変更管理を情報システム運用部門と合意し、変更を適切に管理すること。
＜主旨＞

変更を確実に実施するために、全ての変更を制御された方法で体系的な管理をする必要がある。

＜着眼点＞

① 運用部門の定義する緊急変更に該当するかを判断すること。

② 変更による利用部門への潜在的影響、サービスの要求事項、技術的実現可能性、事業への影響及び財務的な影響について運用部門と合意すること。

③ 変更結果を確認すること。

9.4 リリース管理

運用管理者は、リリース計画を策定し、リリース管理手順を作成してリリースを適切に管理すること。

＜主旨＞

リリースを確実に実施するために、リリース計画を策定し、リリース管理手順を整備してリリースを適切に管理する必要がある。

＜着眼点＞

① リリース計画を策定し、利用部門と合意すること。

② リリース計画に基づいたリリース管理手順を作成し、明文化すること。

③ リリースが失敗した場合には、元に戻すか又は修正し、原因を調査して合意した処置をとること。

④ 緊急のリリースは緊急変更との整合性が取られている明文化された手順に従って管理すること。

⑤ リリースを分析し、分析結果を記録し、レビューして適切な改善の処置を講じること。

10. サービスデスク管理

(1) 運用管理者は、情報システム運用部門と利用部門とをつなぐ単一窓口(SPOC ： Single Point of Contact)のサービスデスクを設置すること。

＜主旨＞

利用部門からの問合せ及び発生した問題に対して、タイムリーかつ効果的に対応するために、適切に構成、運用されているサービスデスクが必要である。

＜着眼点＞

① 運用管理者は、合意されたサービスレベルに基づくサービスデスクのモニタリングとエスカレーションの手続を整備すること。

② サービスデスクは、利用部門からの全ての問合せ、報告されたインシデント、及びサービスと情報に関する要求を受付、登録、処理すること。

③　サービスデスクは、利用部門からの要求を、合意されたサーベスレベルに基づき、エスカレーションすること。
④　サービスデスクは、インシデントを、事業及びサービスの優先度に基づいて分類し、必要に応じて運用管理者にエスカレーションすること。
⑤　サービスデスクは、利用部門への情報発信などの積極的なコミュニケーションを行うこと。
⑥　サービスデスクは、サービスデスクの質についての利用部門の満足度をモニタリングすること。

(2) サービスデスクは、利用部門からの問合せ及び対応を記録し、レビューし、文書化すること。
＜主旨＞
サービスデスクとサービスの質の向上のために、利用部門からの問合せ、インシデント、サービス要求及び対応を記録し追跡するための機能とシステムを確立する必要がある。
＜着眼点＞
①　利用部門からの問合せ、インシデント、サービス要求、情報要求と、その回答を記録すること。
②　定期的に記録をレビューして文書化すること。
③　利用部門に対して、それぞれの問合せへの対応状況を常に通知すること。

(3) 利用部門は、情報システム運用部門への連絡にサービスデスクを活用すること。
＜主旨＞
問合せ及び発生した問題に対して、タイムリーかつ効果的に解決を得るために、サービスデスクを適切に活用する必要がある。
＜着眼点＞
全ての問合せ、インシデント連絡、及びサービスと情報に関する要求をサービスデスクに連絡すること。

Ⅵ. 保守フェーズ

1. 保守ルール

(1)情報システム部門長は、保守フェーズにおける保守対象を明確にすること。

＜主旨＞

情報システム部門長は、保守対象についての認識を統一するために、保守対象を明確にする必要がある。

＜着眼点＞

① 保守対象は、自社で開発したアプリケーション、Web サイト、データベース、外部のソフトウェアメーカから調達した OS、ミドルウェア、パッケージソフト及びサービス提供事業者から調達したクラウドサービスなどを含めること。

② 保守対象について、自社で保守管理するものと外部事業者に管理を委託するものを区分すること。

(2) 情報システム部門長は、保守を実施する体制とその役割を明確にすること。

＜主旨＞

情報システム部門長は、保守を実施する体制についての認識を統一するために、保守を実施する体制を明確にする必要がある。

＜着眼点＞

① 保守実施体制として、保守管理者を定めること。

② 保守管理者に保守の方針及び基本手順の作成、保守計画の作成、保守の実施及び実施管理を行う役割を与えること。

③ 保守管理者に保守依頼を提出する部門の管理者を、保守依頼部門管理者として明確にすること。

(3) 保守管理者は、自社開発ソフトの保守に必要な開発の成果物を、開発フェーズから引き継ぐこと。

＜主旨＞

保守管理者は、自社開発ソフトの保守を確実に行うために、保守に必要な開発の成果物を開発フェーズから確実に引き継ぐ必要がある。

＜着眼点＞

① 引き継ぐ成果物には、次のものを含むこと。

・開発フェーズで作成されたソースコードやドキュメント

・開発フェーズのテスト段階で作成されたドキュメントやデータ

② 引き継いだものの一覧を作成・維持すること。

③ 引き継いだものを安全性の確保された状態で保管すること。

(4)保守管理者は、保守フェーズ全体の基本的枠組みをまとめた「保守手順書」を作成し、最新状態に維持すること。

＜主旨＞

保守管理者は、保守を確実かつ円滑に実施するために、保守フェーズ全体についての基本方針や基本手順を明確にする必要がある。

＜着眼点＞

① 「保守手順書」には、次の事項を記載すること。

- 保守の基本方針
- 保守対象
- 保守実施体制
- 保守依頼の受領からソフトウェアの修正を実施するかの判断、修正実施、修正したソフトウェアの本番システム環境へのリリースに至る基本手順
- 変更管理手順（仕様変更に伴う修正の実施手順）
- 保守において想定されるリスクと対応策

② 情報システム部門長は、「保守手順書」を承認すること。

③ 保守手順書」の内容は、定期的及び必要に応じて見直すこと。

(5) 保守管理者は、「保守手順書」の基本手順を詳細化した「保守作業マニュアル」を作成し、最新状態に維持すること。

＜主旨＞

保守管理者は、ソフトウェア修正作業を確実かつ円滑に実施するために、「保守作業マニュアル」を作成する必要がある。

＜着眼点＞

① 「保守手順書」に記載されている基本手順について、保守対象ソフトウェアの特性（アジャイル開発されたものである、パッケージソフトをカスタマイズしたものであるなど）、保守の規模や期間を考慮し詳細化すること。

② 「保守作業マニュアル」を保守部門のメンバーに周知すること。

2. 保守計画

(1) 保守管理者は、保守依頼部門管理者から提出された保守依頼の内容について確認、調査及び分析を行うこと。

＜主旨＞

保守管理者は、確実な保守作業を行うために、保守依頼の内容について十分な確認、調査及び分析を行う必要がある。

＜着眼点＞

① 保守依頼の内容が次のどれに該当するかを確認すること。
・不具合を解決するための修正
・障害の発生が想定される要因を事前に除去するための修正
・操作性、性能、情報セキュリティなどの改良を目的とする修正
・仕様変更に伴う修正
② 不具合を解決するための修正については、不具合の再現性を確認すること。
③ 修正範囲、修正量、修正にかかる時間を調査・分析すること。
④ 修正の重要性を確認すること。
⑤ 修正による影響（他のソフトウェアへの影響、業務への影響、情報セキュリティ面での影響など）を調査・分析すること。
⑥ 確認、調査・分析にあたって、必要であれば保守依頼部門管理者に改めてヒアリングを行い、誤解・漏れのないようにすること。
⑦ 確認、調査・分析の結果を記録すること。
⑧ 確認、調査・分析結果を承認するとともに、保守依頼部門管理者に伝えること。

(2) 保守管理者は、保守依頼に対してソフトウェアの修正を実施するかどうかを決定すること。
＜主旨＞
保守管理者は、保守依頼についての確認、調査・分析結果を踏まえて、修正を実施するかどうかを決定する必要がある。
＜着眼点＞
① (1)の確認、調査・分析結果を基に決定すること。
② 修正に係る投資対効果も考慮し決定すること。
③ 決定した内容及びその理由を記録すること。
④ 決定した内容及びその理由を承認するとともに、保守依頼部門管理者の了解を得ること。

(3) 保守管理者は、修正を実施することを決定した場合、保守フェーズに従うのか、開発フェーズに従うのかを決定すること。
＜主旨＞
保守管理者は、適切かつ効率的なソフトウェア修正を行うために、保守フェーズ、開発フェーズのいずれに従ってソフトウェア修正を行うのかを決定する必要がある。
＜着眼点＞
① 修正対象範囲、修正量、修正による影響などを考慮し決定すること。
② 仕様変更に伴う修正は、開発フェーズに従うことを原則とすること。
③ 決定した内容及びその理由を記録すること。

④　決定した内容及びその理由を承認するとともに、保守依頼部門管理者の了解を得ること。

(4) 保守管理者は、修正を実施することを決定した場合、「修正計画」を作成すること。
＜主旨＞
保守管理者は、保守依頼に合致した適切なソフトウェア修正を行うために、「修正計画」を作成する必要がある。
＜着眼点＞
①　「修正計画」には、次の事項を盛り込むこと。
・修正対象ソフトウェア
・修正箇所と修正内容
・修正を行うことによる影響（他のソフトウェアへの影響、業務への影響、情報セキュリティ面での影響など）
・修正に対するテストの方針と内容
・修正実施体制及びテスト実施体制
・修正実施スケジュール及びテスト実施スケジュール
②　修正対象ソフトウェア、修正箇所と修正内容の検討に当たっては、いくつかの選択肢を比較検討し、最善の方法を選択すること。
③　テスト内容の策定に当たっては、修正箇所だけでなく、修正が影響を及ぼすと考えられる部分をテスト範囲に含めること。修正内容によっては、レグレッションテスト（退行テスト）の実施を検討すること。
④　修正実施スケジュールの作成に当たっては、保守依頼部門管理者による受入テストの実施や本番システム環境へのリリース時期を考慮すること。

(5) 保守管理者は、「修正計画」を承認するとともに、保守依頼部門管理者の了解を得ること。
＜主旨＞
保守管理者は、修正の実施について合意形成を図るために、「修正計画」について保守依頼部門管理者の了解を得る必要がある。
＜着眼点＞
必要に応じて、保守依頼部門管理者への説明又は協議の場をもつこと。

(6) 保守依頼部門管理者は、修正されたソフトウェアの「受入計画」を作成すること。
＜主旨＞
保守依頼部門管理者は、修正されたソフトウェアが保守依頼に合致していることを確認し、修正されたソフトウェアを本番システム環境に確実にリリースするために、「受入計画」

を作成する必要がある。
＜着眼点＞
① 「受入計画」には、次の事項を盛り込むこと。
・受入テスト実施体制及び実施スケジュール
・データ移行実施体制、実施方法及び実施スケジュール
・本番システム環境へのリリース実施体制及び実施スケジュール
② 受入テストは、保守依頼部門管理者が保守依頼に合致した修正が行われていることを利用者の立場で確認することを目的とすること。
③ 修正されたソフトウェアの本番システム環境へのリリースに関連してデータ移行が必要な場合には、移行対象、移行方法、移行検証方法を計画すること。
④ 本番システム環境へのリリーススケジュールの設定に当たっては、リリース対象システム環境の利用時期、利用時間を考慮すること。
⑤ 本番システム環境へのリリースに当たって、リリース作業中に問題が発生した場合の対処方法を計画すること。
⑥ 保守管理者は、保守依頼部門管理者による「受入計画」の作成に協力すること。
⑦ 保守依頼部門管理者は、「受入計画」を承認するとともに、保守管理者の了解を得ること。

3. 情報セキュリティ管理
(1) 保守管理者は、外部調達ソフトに関するぜい弱性情報及び修正コード情報の収集に努めること。
＜主旨＞
保守管理者は、自社で使用している外部調達ソフトのセキュリティ確保のために、外部調達ソフトのぜい弱性情報及び修正コード情報の収集に努める必要がある。
＜着眼点＞
① ソフトウェアメーカやサービス事業者から提供される情報の収集に努めること。
② セキュリティ情報提供機関から公表される情報の収集に努めること。
③ 保守のアウトソーシング先事業者から提供される情報の収集に努めること。

(2) 保守管理者は、収集したぜい弱性情報及び修正コード情報について、自社システム環境への適用の必要性を調査・分析し、適用の是非を決定すること。
＜主旨＞
保守管理者は、ぜい弱性による自社システムへの影響、修正コードを適用した場合のリスクを併せて調査・分析し、適用の是非を決定する必要がある。
＜着眼点＞
① ぜい弱性による自社システムへの影響を調査・分析した上で、適用の是非を決定する

こと。

② 併せて、修正コードを適用した場合のリスクについても調査・分析すること。

③ パッケージソフトやクラウドサービスについては、提供元事業者から提供される最新バージョンの使用を基本とすること。

(3) 保守管理者は、OS などの自動適用可能なソフトウェアの修正コードについて、適用方針を決め確実な適用を行うこと。

＜主旨＞

保守管理者は、OS などのぜい弱性が情報セキュリティ攻撃の温床になることを防ぐために、ぜい弱性に速やかかつ確実に対応する必要がある。

＜着眼点＞

① 自動適用するか否かを決定すること。

② 自動適用する場合には、ソフトウェアに自動適用の設定を行うこと。

③ 自動適用しない場合には、個別適用の計画として次のことを明確化すること。

・適用するか否かの判断基準

・修正コードの事前検証方法

・適用スケジュール

・修正コードを適用したソフトウェアの本番システム環境へのリリース手順

④ 計画に従って、修正コードの事前検証、適用、適用結果の確認を行うこと。

⑤ 計画に従って、修正コードを適用したソフトウェアを本番システム環境にリリースすること。

⑥ 本番システム環境へのリリース結果（リリース日、リリースしたバージョン、適用した修正コード）を記録すること。

(4) 保守管理者は、コンピュータウイルス対策ソフトウェア（以下「ウイルス対策ソフト」という。）及びパターン定義ファイル（以下「パターンファイル」という。）の更新の適用を実施すること。

＜主旨＞

保守管理者は、コンピュータウイルスによる被害を防ぐために、ウイルス対策ソフト及びパターンファイルを最新状態に維持する必要がある。

＜着眼点＞

ウイルス対策ソフト及びパターンファイルの更新の適用は、自動適用を基本とすること。

(5) 上記以外の情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

4. 変更管理

保守管理者は、仕様変更に伴うソフトウェアの修正に対応すること。

＜主旨＞

保守管理者は、仕様変更に伴うソフトウェアの修正に確実に対応する必要がある。

＜着眼点＞

① 仕様変更に伴うソフトウェアの修正手順は、開発フェーズに従うこと。

② 仕様変更に伴うソフトウェアの修正においては、修正が及ぼす他のソフトウェアや業務に対する影響範囲及び影響度合いに、特に留意すること。

5. 保守の実施

(1) 保守管理者は、「修正計画」を再確認し、必要であれば詳細化すること。

＜主旨＞

保守管理者は、確実な修正作業を行うために、「修正計画」の内容を十分に理解する必要がある。

＜着眼点＞

① 「修正計画」の内容を再確認すること。

② 必要に応じて、「修正計画」の内容を詳細化すること。

(2) 保守管理者は、「修正計画」に従って修正作業を実施し、実施状況を管理すること。

＜主旨＞

保守管理者は、確実かつ効率的にソフトウェア修正を行うために、「修正計画」に従って修正作業を実施し、その実施状況を管理する必要がある。

＜着眼点＞

① 修正作業の実施状況を記録すること。

② 修正作業の実施状況を確認すること。

③ 進捗面や品質面で「修正計画」と修正作業実施状況に差異が発生した場合には、原因を調査し対策を講じるとともに、必要であれば「修正計画」の変更を行うこと。

(3) 保守管理者は、「修正計画」に従って、修正したソフトウェアのテストを実施すること。

＜主旨＞

保守管理者は、ソフトウェアの修正が適切であることを確認するために、「修正計画」に従ってテストを実施する必要がある。

＜着眼点＞

① テスト結果を記録すること。

② テスト結果の検証を行うこと。

③ テストで使用したデータを保管すること。

(4) 保守管理者は、ソフトウェアの修正に伴って関連するドキュメントの修正が必要かどうかを調査し、必要なドキュメントの修正を行うこと。

＜主旨＞

保守管理者は、ソフトウェアと関連ドキュメントとの内容の整合性を確保するために、ソフトウェアの修正に対応してドキュメントの修正を行う必要がある。

＜着眼点＞

① 関連するドキュメントの抽出に漏れのないよう、留意すること。

② 関連するドキュメントの修正箇所の抽出に漏れのないよう、留意すること。

③ ドキュメントの修正にあたっては、ドキュメント管理フェーズに従うこと。

(5) 保守管理者は、修正実施結果、テスト結果、最終的な修正内容、及びドキュメント修正内容を承認すること。

＜主旨＞

保守管理者は、修正内容が保守依頼に合致していることを確実にするために、「修正計画」に対して実施した内容を承認する必要がある。

＜着眼点＞

① 承認する内容を整理し文書化すること。

② 承認方法は、報告書による承認、報告会の開催などの方法を採ること。

③ 承認した内容を保守依頼部門管理者に伝えること。

(6) 保守依頼部門管理者は、「受入計画」に従って、修正されたソフトウェアの受入テストを実施すること。

＜主旨＞

保守依頼部門管理者は、ソフトウェアの修正が保守依頼に合致しており、業務で使用する上で問題のないことを確認するために、「受入計画」に従って受入テストを実施する必要がある。

＜着眼点＞

① 「受入計画」の内容を再確認すること。

② 必要に応じて、「受入計画」の内容を詳細化すること。

③ 必要なドキュメント修正が行われていることを確認し承認すること。

④ 受入テストのテストケース、テスト項目は業務手順を基に設定すること。

⑤ 受入テストのテストケース、テスト項目の設定に当たっては、必要に応じて保守管理者の協力を得ること。

⑥ 受入テストの実施に当たっては、業務でシステムを利用する利用者を参加させること。

⑦　受入テストの実施結果を記録すること。
⑧　受入テストの実施結果を承認すること。
⑨　受入テストの実施結果を踏まえて、修正されたソフトウェアの受入可否を決定すること。
⑩　受入テストの実施結果及び受入可否を保守管理者に伝えること。

(7) 保守依頼部門管理者は、受入を決定したソフトウェアの修正について、運用管理者に本番システム環境へのリリースを依頼する。
＜主旨＞
保守依頼部門管理者は、本番システムの運用に影響を及ぼさないために、「受入計画」に従って修正されたソフトウェアを本番システム環境にリリースする必要がある。
＜着眼点＞
①　運用管理者のリリース計画に合わせて、本番システム環境へのリリースを依頼すること。
②　データ移行が必要な修正については、「受入計画」に従ってデータ移行を行うこと。
③　本番システム環境へのリリースの過程で問題が発生した場合には、「受入計画」で策定した対処方法に従って対処すること。
④　本番システム環境へのリリースに当たっては、本番システム環境への影響が少ない時期を考慮すること。
⑤　本番システム環境へのリリースについての記録を残すこと。

6. ソフトウェア構成管理
(1) 保守管理者は、ソフトウェア構成管理として管理する項目を決定すること。
＜主旨＞
保守管理者は、システムの信頼性・保守性・効率性を高めるために、本番システムで使用しているソフトウェアの構成情報を正確に管理する必要がある。
＜着眼点＞
①　本番システム環境で使用しているソフトウェアについて、ソフトウェアの種類、自社開発ソフトか外部調達ソフトかの区分、ソフトウェア名称、バージョン、関連するドキュメントとの対応、保守サポート委託先などを明確にすること。
②　本番システムを構成しているソフトウェアのうち、対象とするソフトウェアを決めて使用状況を調査し、その結果をソフトウェア構成管理項目の１つとして管理すること。

(2) 保守管理者は、ソフトウェア構成管理実施体制を確立すること。
＜主旨＞

保守管理者は、ソフトウェア構成管理を確実に実施するために実施体制を確立する必要がある。

＜着眼点＞

① ソフトウェア構成管理担当者を定め、ソフトウェア構成情報を変更できる権限を付与すること。

② ソフトウェア構成管理担当者は、ソフトウェア構成情報の更新・維持管理を行うこと。

(3) 保守管理者は、ソフトウェア構成管理の実施手順を定めること。

＜主旨＞

保守管理者は、ソフトウェア構成管理を確実に実施するために手順を定める必要がある。

＜着眼点＞

① ソフトウェア構成情報に対する変更情報の収集手順及び変更情報の検証手順を定めること。

② ソフトウェア構成情報に対する変更情報の反映手順及び反映結果の検証手順を定めること。

(4) 保守管理者は、本番システムで使用しているソフトウェアについて、修正コードの本番システム環境へのリリース履歴を管理すること。

＜主旨＞

保守管理者は、システムの保守性を高めるために、ソフトウェアに加えた修正コードを必要な時に容易に確認できるように管理する必要がある。

＜着眼点＞

① リリース履歴情報として、保守依頼との対応、修正計画との対応、修正結果との対応、本番システム環境にリリースした修正コード、リリース日、リリースしたバージョンなどを管理すること。

② ソフトウェア構成管理情報との関連付けを考慮すること。

③ リリース履歴情報を安全性の確保できる状態で保管すること。

④ リリース履歴情報にアクセスできる者を限定すること。

(5) 保守管理者は、ソフトウェアのバージョンアップを行った場合における、ソフトウェアの旧バージョンの扱いを明確にすること。

＜主旨＞

保守管理者は、システムの保守性を確保するために、旧バージョンの扱いを明確にする必要がある。

＜着眼点＞

① ソフトウェアの旧バージョンの扱いに関して、保管する世代数、保管期間、保管方法、

世代管理を終えたソフトウェアの廃棄方法などを明確にすること。

② 廃棄方法、廃棄時期の設定においては、機密保護対策を考慮すること。

(6) ソフトウェア構成管理にかかわる情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

7. ライフサイクル管理

(1) 保守管理者は、外部調達ソフトについて、ソフトウェアメーカのバージョンアップ計画、サポート計画に関する情報を収集すること。

＜主旨＞

保守管理者は、外部調達ソフトの保守を確実に行うために、ソフトウェアメーカのバージョンアップ計画、サポート計画に関する情報を収集する必要がある。

＜着眼点＞

① 不明点があれば、外部調達ソフトメーカに問合せを行い、正確な情報収集に努めること。

② 把握した情報を整理し、関係者で共有すること。

(2) 保守管理者は、(1)で収集した情報に基づいて、自社における外部調達ソフトの保守計画を作成すること。

＜主旨＞

保守管理者は、外部調達ソフトの保守を確実に行うために、外部調達ソフトメーカの保守・サポート計画を基に、自社における外部調達ソフトの保守計画を作成する必要がある。

＜着眼点＞

① 計画には、バージョンアップ、他のソフトウェアへの移行などの選択肢を考慮すること。

② 計画が、外部調達ソフトメーカの保守・サポート計画と整合していることを確認すること。

(3) 保守管理者は、外部調達ソフトの保守計画に従って保守を実施し、実施結果を記録すること。

＜主旨＞

保守管理者は、外部調達ソフトの保守を確実に行うために、手順を確立する必要がある。

＜着眼点＞

保守計画、実施、記録、検証の手順を基本にすること。

(4) 保守管理者は、バージョンアップや他のソフトウェアへの移行を行った後の旧ソフト

ウェアの廃棄計画を立て、廃棄を行い、記録を残すこと。

＜主旨＞

保守管理者は、不要になった旧バージョンのソフトウェアを確実に処分するために、手順を確立する必要がある。

＜着眼点＞

① 廃棄計画、廃棄実施、記録、検証という手順を基本にすること。

② 旧バージョンのソフトウェアの廃棄に当たっては、最新バージョンのソフトウェアの信頼性が確保されるまで一定期間は保管すること。

③ 廃棄方法、廃棄時期の設定においては、機密保護対策を考慮すること。

Ⅶ. 外部サービス管理

1. 外部サービス利用計画

(1) 外部委託元部門長は、情報システム戦略計画にもとづき、外部サービス利用計画を策定し、情報システム戦略委員会が承認すること。

＜主旨＞

外部委託元部門長（情報システム部門長及び利用部門長等）は、外部委託の対象と内容を明確にするため、情報システム戦略計画と整合のとれた外部サービス利用計画を策定し、情報システム戦略委員会が承認する必要がある。

＜着眼点＞

① 外部サービス利用計画は、情報システム戦略計画に基づいて策定していること。
② 外部サービス利用計画は、情報システム戦略委員会の承認を受けること。
③ 状況の変化に応じて、外部サービス利用計画を見直していること。

(2) 外部委託元部門長は、外部サービス利用計画で、目的、対象範囲、予算、体制等を明確にすること。

＜主旨＞

外部委託元部門長は、委託業務の内容を明らかにし、業務を円滑に遂行するため、外部委託の目的、内容、効果などを明確にする必要がある。

＜着眼点＞

① 外部委託の目的、対象範囲、予算、期待できる効果、リスク、委託先の体制、セキュリティ対策及び委託先の選定条件等を明確にしていること。
② 外部委託の目的、対象範囲、予算、期待できる効果、リスク、委託先の体制、セキュリティ対策及び委託先の選定条件等を関係者が合意していること。

2. 委託先選定

(1) 外部委託元部門長は、委託先の選定基準を明確にすること。

＜主旨＞

委託先の選定が外部サービス利用計画と整合性がとれ、客観的な評価ができるようにするため、選定基準を定めておく必要がある。

＜着眼点＞

① 委託先の選定基準を明文化し、情報システム戦略委員会が承認していること。
② 選定基準は、外部サービス利用計画と整合性がとれていること。
③ 選定基準は、客観的な指標を定めておくこと。
④ 選定基準は、外部委託業務の特性を考慮していること。
・総合評価（技術点＋価格点）
・最低価格（資格審査＋最も価格が低いもの）

・企画競争（技術審査＋価格は一定）等

⑤ 選定基準には、委託先の安定性、実績、技術レベル、セキュリティ対策状況、品質管理体制等について盛り込んでいること。

⑥ クラウドサービスやデータセンタの利用等の場合、委託先の事業継続対策についても考慮すること。

(2) 外部委託元管理者は、委託候補先に対して必要な要求仕様を提示し、その内容を合意すること。

＜主旨＞

外部委託元管理者は、契約後に委託先とトラブル等を生じさせないようにするため、事前に要求仕様を合意しておく必要がある。

＜着眼点＞

① 外部サービス利用計画にもとづき、要求仕様を作成すること。情報システム開発の場合は、Ⅱ.企画フェーズの要求定義書に基づくこと。

② 外部委託の目的を明確にしていること。

③ 外部委託の範囲、要求するサービスの内容、サービスのレベルを明確にしていること。

④ 要求仕様の内容について、関係者が合意すること。

(3) 外部委託元管理者は、可能な限り、複数の候補先が提示した提案内容の比較検討を行ったうえで、委託先を選定すること。

＜主旨＞

委託先を公正に選定するため、選定基準にもとづき、複数の候補先を総合的に評価する必要がある。

＜着眼点＞

① 可能な限り複数の委託候補先が提示した提案内容の比較検討を行ったうえで、委託先を選定すること。（最低価格方式以外の場合）

② 項目ごとに点数化した選定基準にする等、選定理由を明確にすること。

③ 選定の結果については、外部委託元部門長の承認を受けていること。

3. 契約と管理

3. 1 契約

(1) 外部委託元管理者は、「外部サービス利用計画」に基づき、契約を締結すること。

＜主旨＞

委託先との契約内容が外部サービス利用計画から逸脱しないようにするため、契約を締結する必要がある。

＜着眼点＞

① 関係部署による契約内容のチェックを受けるなどして、契約書を作成すること。
② 外部委託元部門長の承認を得ること。

(2) 外部委託等契約書には、必要な事項を盛り込むこと。
＜主旨＞
委託先との問題が生じないようにするため、契約書に必要事項を盛り込む必要がある。
＜着眼点＞
① 外部委託等契約書には、委託業務内容・範囲及び責任分担、委託方法、委託期間又は納期、特約条項・免責条項、損害賠償条項、守秘義務条項、暴力団排除条項、瑕疵担保責任（不具合時の責任)、知的財産権や使用権等の権利の帰属、再委託の可否（再委託を認める場合は、再委託先が外部委託先と同等の義務を負うこと等責任の所在、再委託時の手続（委託元への届出、委託元の承認等）を明確にすること）等を含むこと。
② コンプライアンスに関する条項を明確にすること。

(3) 契約締結後の委託業務内容に追加及び変更が生じた場合、外部委託元管理者は契約内容の再検討を行うこと。
＜主旨＞
外部委託元管理者は、委託契約の内容が実態と乖離しないようにするため、委託業務内容に追加や変更が生じた場合には、契約内容の見直しをする必要がある。
＜着眼点＞
① 委託業務内容に変更がないかどうか、定期的に確認すること。
② 委託業務内容に変更がある場合は、契約内容の見直しを検討すること。
③ 契約内容を変更する場合は、外部委託元部門長の承認を得ること。

(4) システム監査に関する方針を明確にすること。
＜主旨＞
委託先の委託業務内容の信頼性、安全性、効率性の確保を担保するために、委託契約にシステム監査に関する方針を明確にする必要がある。
＜着眼点＞
① 契約でシステム監査の実施の方針を定めていること。
② システム監査の対象範囲、適用する基準を明確にしていること。
③ システム監査の結果の取扱いを明確にしていること。

3.2 委託先管理
(1) 外部委託元管理者は、委託業務の実施内容が、契約内容と一致することを確認するこ

と。
＜主旨＞
委託業務の内容を過不足なく実施するため、委託先が契約に定められたとおりに委託業務を遂行しているか、外部委託元管理者は、委託業務の実施内容を確認する必要がある。
＜着眼点＞
① 委託業務の実施内容が、契約内容と一致することを定期的に確認すること。
② 委託業務の実施内容を把握していること。
③ 委託業務の実施内容と契約内容の相違点について、適切な措置を講じていること。

(2) 外部委託元管理者は、契約に基づき、必要な要求仕様、データ、資料等を提供すること。
＜主旨＞
委託業務を委託計画どおりに遂行するため、契約に基づき、必要な要求仕様、データ、資料等を委託先に提供する必要がある。
＜着眼点＞
① 委託契約書、仕様書に基づき、必要な要求仕様、データ、資料を提供していること。
② 資料、機材等提供の責任者、担当者を明確にしていること。
③ 資料等提供ルールを定め、提供、変換、廃棄等の方法を明確にしていること。
④ 委託先の情報セキュリティ管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。

(3) 外部委託元管理者は、契約に基づき、委託先より業務報告書に基づく報告を定期的に受けていること。
＜主旨＞
委託先が契約どおりに委託業務を実施しているかどうかを確認するため、外部委託元管理者は、委託先より業務報告書に基づく報告を定期的に受ける必要がある。
＜着眼点＞
① 委託先より業務報告書に基づく報告を定期的に受けていること。
② 業務報告書には、委託業務の進捗状況又は稼動状況、品質管理状況、発生した問題点と対策状況、セキュリティ対策の実施状況及び今後の予定等の必要な事項が記載されていること。

(4) 外部委託元管理者は、業務報告書の内容を分析・評価し、必要な対策を講ずること。
＜主旨＞
外部委託元管理者は、委託業務が計画どおりに遂行するため、進捗や問題点に対してリスク対策を講ずる必要がある。
＜着眼点＞

① 業務報告書の内容から進捗状況を定期的に把握していること。
② 遅延やその他の問題点の原因を追究し、適切な措置を講じていること。
③ 進捗の状況及び不正防止、セキュリティ対策等のリスク対策の実施状況について、外部委託元部門長に報告すること。

(5) 外部委託元管理者は、情報システム戦略委員会で定めた「委託先に対する立入監査又はモニタリングの実施対象の選定基準」に該当する場合、立入監査又はモニタリングを実施すること。

＜主旨＞

外部委託元管理者は、委託先の進捗状況、稼動状況、情報セキュリティ対策の取組み状況等により、情報資産の安全性が損なわれるリスク等を確認するため、リスクの大きさに応じ、委託先への立入監査などを実施する必要がある。

＜着眼点＞

① 立入監査等では、契約で取り決めた事項に対する遵守状況、情報セキュリティ管理態勢、事故等(サイバーセキュリティ事案を含む)への対応態勢や再委託先（再々委託先以降も含む）の管理状況等を確認すること。
② 委託先において再委託が行われている場合は、契約に基づき、再委託（再々委託以降も含む）先の業務の実施状況を把握すること。
③ 立入監査等の実施結果については、外部委託元部門長及び情報システム戦略委員会に報告すること。

(6) 委託業務において事故等が発生した場合は、外部委託元管理者は、委託先に対して速やかに報告を求めること。

＜主旨＞

委託先で発生した事故等については、外部委託元部門の管理責任も問われるため、速やかに委託先に対して報告を求める必要がある。

＜着眼点＞

① 報告には、発生した事象、業務への影響、原因、対策、復旧の見込み、再発防止策等について求めること。
② 報告の内容により、外部委託元部門としての対応を決定していること。
③ 事故等の重要度に応じて、速やかに外部委託元部門長及び情報システム戦略委員会に報告していること。

(7) サービスや成果物の検収は、契約に基づいて外部委託元管理者が実施し、検収結果は外部委託元部門長が承認すること。

＜主旨＞

委託の目的の達成状況を確認するため、サービスや成果物の検収は、契約に基づいて行う必要がある。

＜着眼点＞

① 検収方法を明確にしていること。

② サービスや成果物の検収は、検収方法に基づいて実施していること。

③ 検収結果は、外部委託元部門長が承認していること。

(8) 外部委託元管理者は、業務終了後、委託業務で提供したデータ、資料等の回収及び廃棄の確認を行うこと。

＜主旨＞

委託先で情報漏えい等が起きないようにするため、外部委託元管理者は、業務終了後、委託業務で提供したデータ、資料等の回収及び廃棄の確認を行う必要がある。特にクラウドサービスでは、注意を要する必要がある。

＜着眼点＞

① 委託業務で提供したデータ、資料等の回収及び廃棄の確認方法を明確にしていること。

② 業務終了後、委託業務で提供したデータ、資料等の回収及び廃棄の確認を行うこと。

③ クラウド事業者が委託元の情報を取扱う場合でデータ消去を実施する場合は、データ消去証明書等を受領すること。

(9) 外部委託元管理者は、外部委託終了後、委託業務の結果について、評価すること。

＜主旨＞

今後の委託計画の策定、委託先の選定等に活用するため、委託終了後、委託した業務の結果を分析及び評価する必要がある。

＜着眼点＞

① 委託計画に基づいてその目標の達成状況を評価していること（費用対効果への評価を含む。）。

② 委託先については、引続き委託を継続すべきかどうかを評価していること。

③ 委託業務の実施結果を分析及び評価結果を記録し、外部委託元部門長が承認していること。

(10) 外部委託元管理者は、労働者派遣法等関連法規を遵守して、委託先の管理を行うこと。

＜主旨＞

労働者派遣と請負等の区分を明確にするため、労働者派遣法等関連法規を遵守して、委託先の適正な管理を行う必要がある。

＜着眼点＞

① 派遣契約の場合は、労働者派遣法に従うこと。
② 請負契約・（準）委託契約の場合は、厚生労働省のガイドライン等に従い、適正化を図ること。

4. サービスレベル管理(SLM)

(1) 外部委託元管理者は、サービスの品質を維持するために、外部委託契約に SLA (Service Level Agreement：サービスレベル合意）の締結を検討すること。

＜主旨＞

委託先から提供を受けるサービスの品質を維持・評価するために、委託する業務内容に応じて、SLA 条項を盛り込むことを検討する必要がある。

＜着眼点＞

① 提供を受けるサービスの内容により、SLA を締結することのメリット・デメリットを検討していること。
② サービスレベルに影響を及ぼす前提条件を明確にしていること。
③ SLA の内容は要件定義の内容と整合性がとられていること。

(2) SLA 締結の場合は、外部委託元管理者は必要な事項を盛り込むとともに、外部委託元部門長の承認を得ていること。

＜主旨＞

外部委託元管理者は、サービスのレベルを維持と品質を評価するため、必要な項目を SLA に項目を盛り込み、外部委託元部門長の承認を得ている必要がある。

＜着眼点＞

① 運用サービスの場合は、SLA 条項の項目として運用時間、稼動率、障害発生率、障害対応時間等について検討すること。
② 保守サービスの場合は、故障率（ハードウェア)、障害復旧時間、保守員到着時間等について検討すること。

(3) 外部委託元管理者は、外部委託業務が SLA を満たしているかを定期的に確認し、その結果を外部委託元部門長に報告すること。

＜主旨＞

外部委託元管理者は、サービスの品質が維持されるようにするため、委託先が SLA の条件を遵守しているかを定期的に確認する必要がある。

＜着眼点＞

① 委託先から定期的に、サービルレベルについての報告を受けること。
② 報告内容に基づき、委託先がサービスレベルを達成しているかどうかを確認すること。

③　情報セキュリティに関する合意レベルの維持管理策については、情報セキュリティ管理基準参照表を利用して、情報セキュリティ管理基準の該当箇所を参照すること。
④　確認の結果を、外部委託元部門長に報告すること。

(4)　外部委託元管理者は、サービスレベル未達成の場合に備え、リソース増強や代替手段の適用など具体的な対応方法を検討していること。

＜主旨＞

サービスレベル未達成の場合に備えるため、代替手段の適用など具体的な対応方法や契約解除条件を設定しておく必要がある。

＜着眼点＞

①　サービスレベル未達成の場合に備え、リソース増強や代替手段の適用など具体的な対応方法を検討しておくこと。
②　SLA の未達成による契約解除条件を設定しておくこと。

(5) 外部委託元管理者は、委託業務内容に変更が生じた場合は、必要に応じて SLA の内容の見直しを行うこと。

＜主旨＞

委託業務内容に変更が生じた場合は、サービスレベルの内容に影響を及ぼす可能性があるため、必要に応じて SLA の内容の見直しを行う必要がある。

＜着眼点＞

①　委託業務内容に変更が生じた場合は、SLA の内容の見直しの検討を行うこと。
②　見直しを実施した場合は、外部委託元部門長の承認を得ていること。

Ⅷ. 事業継続管理

IT ガバナンス及び情報システム戦略委員会の方針に基づく。

1. リスクアセスメント

(1) 情報システム部門長は、自然災害等のリスク及び情報システムに与える影響範囲を明確にすること。

＜主旨＞

情報システム部門長は、情報システムにかかわる災害時、テロによる破壊行為発生時及びサイバー攻撃の情報システムの対応策を具体化するため、地震、洪水、テロ及びサイバー攻撃等のリスク及び情報システムに与える影響範囲を明確にする必要がある。

＜着眼点＞

① 自然災害は、すべて想定するとともに、テロ等による破壊及びサイバー攻撃も含めていること。
② 被災の規模は、業務継続が困難となる規模を含めて想定していること。
③ 被災の想定は、地理的、組織的､物理的及び業務的視点から検証していること。
④ 想定した影響範囲について、将来を考慮していること。
⑤ 事業継続に関わる情報セキュリティ管理基準の該当事項を参照し確認すること。

(2) 情報システム部門長は、情報システムの停止等により組織体が被る損失を分析すること。

＜主旨＞

情報システム部門長は、情報システムに係る被災の程度に応じた業務の復旧の重要性及び緊急性を明確にするため、情報システムの停止等によって組織体が被る損失について利害関係者を入れ、分析する必要がある。

＜着眼点＞

① 情報システムの停止及び機能縮退によって組織体が被る損失を分析する対象範囲には、影響を受ける業務を網羅していること。
② 利害関係者の合意を得ること。
③ 損失の分析は、組織体の損害及び社会的損害を明確にしていること。
④ 業務の復旧の重要性及び緊急性を明確にしていること。
⑤ 事業継続に関わる情報セキュリティ管理基準の該当事項を参照し確認すること。

(3) 情報システム部門長は、業務の復旧許容時間及び復旧優先順位を定めること。

＜主旨＞

情報システム部門長は、情報システムにかかわる被災による業務の停止及び影響を最小限にとどめ、効率的に復旧するため、業務の復旧許容時間及び復旧優先順位を定める必要がある。

＜着眼点＞

① 復旧許容時間及び復旧優先順位の設定は、業務の重要性、緊急性、影響範囲及び他の業務との整合性及び実現可能性を考慮していること。

② 復旧許容時間及び復旧優先順位の設定理由を明確にしていること。

③ 復旧許容時間及び復旧優先順位を関係者が合意していること。

④ 事業継続に関わる情報セキュリティ管理基準の該当事項を参照し確認すること。

2. 業務継続計画の管理

(1) 情報システム部門長は、リスクアセスメントの結果に基づき、経営陣が定めた事業継続計画と整合を取った情報システムの業務継続計画を策定すること。

＜主旨＞

情報システム部門長は、災害及び重大事故発生時に混乱することなく、適切な措置を迅速に確実に実行するために、事業継続計画と整合した情報システムにかかわる業務継続計画を策定する必要がある。

＜着眼点＞

① 情報システム部門長は、業務継続計画の策定ルールを明文化すること。

② 情報システム部門長は、関係者と協議し、事業継続計画と整合した業務継続計画を作成すること。

③ 情報システム部門長は、業務継続計画に、バックアップ、代替処理対策、復旧対策等を記載されることを確保すること。

④ 情報システム部門長は、将来の経営環境及び情報システムにかかわる業務の変化を考慮して業務継続計画を作成すること。

(2) 情報システム部門長は、情報システムに係る災害及び重大事故発生時に対応した業務継続計画を作成し、承認を得ること。

＜主旨＞

情報システム部門長は、災害及び重大事故発生時に混乱することなく、情報システムに係る適切な措置を迅速に実行するため、経営陣が定めた災害及び重大事故発生時に対応した情報システムの業務継続計画を関係者に周知徹底する必要がある。

＜着眼点＞

① 情報システムに係る災害及び重大事故発生時に対応した業務継続計画が作成され、承認されていること。

② 経営陣が業務継続計画を承認していること。

③　情報システム部門長は、業務継続計画を関係者に周知徹底していること。
④　事業継続に関わる情報セキュリティ管理基準の該当事項を参照し確認すること。

(3)　情報システム部門長は、情報システムに係る業務継続計画の実現可能性を確保すること。
＜主旨＞
情報システム部門長は、被災の程度に応じて情報システムにかかわる業務の継続性を確保し、確実にシステム復旧するため、業務継続計画の実現可能性を確認すること。
＜着眼点＞
①　実現可能性を検証する計画を策定していること。
②　検証する計画は、被災の程度に応じた内容となっている。
③　情報システム部門長は、検証結果を記録し、業務継続計画に反映していること。
④　事業継続に関わる情報セキュリティ管理基準の該当事項を参照し確認すること。

(4)　情報システム部門長は、業務継続計画の中で、従業員の教育訓練及びリスクコミュニケーションの方針を明確にすること。
＜主旨＞
情報システムにかかわる業務継続計画に定めた具体策を習熟し、確実に実行するため、従業員の教育訓練及びリスクコミュニケーションの方針を明確にし、訓練を定期的に行う必要がある。
＜着眼点＞
①　情報システムにかかわる業務継続計画に基づいて、教育訓練の方針を明確にしていること。
②　教育訓練の方針を踏まえた教育訓練計画を策定していること。
③　災害及び重大事故発生時におけるリスクコミュニケーションの方針を明確にすること。
④　事業継続に関わる情報セキュリティ管理基準の該当事項を参照し確認すること。

(5)　情報システム部門長は、業務継続計画を関係各部に周知徹底すること。
＜主旨＞
情報システム部門長は、情報システムにかかわる業務継続計画に定めた具体策を習熟し、確実に実行するため、従業員の教育訓練の方針及び計画を明確にし、業務継続計画の教育訓練を定期的に行う必要がある。
＜着眼点＞
①　業務継続計画に対応した訓練に基づいて、教育訓練を定期的に実施していること。
②　教育訓練の結果を記録し、業務継続計画に反映していること。

③　事業継続に関わる情報セキュリティ管理基準の該当事項を参照し確認すること。

(6) 情報システム部門長は、業務継続計画を必要に応じて見直すこと。

＜主旨＞

情報システム部門長は、情報システムにかかわる業務継続計画について、経営環境及び業務の変化等に対応して、実現可能性を保持するため、適時に見直しを行う必要がある。

＜着眼点＞

①　見直しのルールを明文化していること。

②　見直しによる変更は、理由が明確であること。

③　変更した計画を経営陣が承認し、関係者に周知徹底させていること。

④　事業継続に関わる情報セキュリティ管理基準の該当事項を参照し確認すること。

3. システム復旧計画の管理

(1)　情報システム部門長は、情報システム、データ及び関連設備のバックアップ方法及び手順を業務の復旧目標に対応して定めること。

＜主旨＞

情報システム部門長は、情報システムにかかわる復旧作業の効率及び経済性を考慮して、確実に復旧させるため、業務の復旧目標に対応して、バックアップ方法及び手順を定める必要がある。

＜着眼点＞

①　業務別にバックアップの対象を明確にし、関連業務のバックアップとの整合を図っていること。

②　業務の復旧許容時間及び復旧順位に対応して、バックアップ方法及び手順を定めていること

③　バックアップ要員及び予算を確保していること。

(2)　情報システム部門長は、情報システムにかかわるバックアップ方法及び手順を検証すること。

＜主旨＞

情報システム部門長は、定められたバックアップ方法及び手順の実現の可能性を確認するために、運用の責任者とバックアップ方法及び手順を検証する必要がある。

＜着眼点＞

①　情報システム部門長は、実現可能性を検証する計画を策定していること。

②　情報システム部門長は、検証結果を記録し、バックアップ方法及び手順に反映していること。

(3) 情報システム部門長は、復旧までの代替処理手続及び体制を定め、検証すること。
＜主旨＞
停止した情報システムを復旧するまでの間、業務を継続するため、代替処理手続及び体制を定める必要がある。また、その実現可能性を確認するため、ユーザ及び運用の責任者と検証する必要がある。
＜着眼点＞
業務の復旧許容時間及び復旧優先順位に対応して、代替処理手続及び体制を明確にしていること。
① 代替処理の要員及び予算を確保していること。
② 代替処理の責任者及び指揮命令系統を明確にしていること
③ 実現可能性を検証する計画を策定していること
④ 検証結果を記録し、代替処理手続及び体制に反映していること

(4) 情報システム部門長は、復旧手続及び体制を定め、検証すること。
＜主旨＞
停止した情報システムを円滑かつ確実に復旧までの手続及び体制を定める必要がある。その実現可能性を確実にするため、ユーザ及び運用の責任者が検証する必要がある。
＜着眼点＞
① 業務の復旧許容時間及び復旧優先順位に対応して、復旧処理手続及び体制を定めていること。
② 復旧の推進状況を関係者に周知徹底する体制を定めていること。
③ 復旧の要員及び予算を確保していること。
④ 実現可能性を検証する計画を策定していること。
⑤ 検証結果を記録し、復旧手続及び体制に反映していること。

4. 訓練の管理
(1) 情報システム部門長は、情報システムにかかわる適切な業務継続手順・計画が、事業継続目的に合致していることを確かにするために、手順に基づき訓練を実施すること。また、訓練は、策定後の維持管理のために、定期的に訓練の目的に応じて適切な訓練を実施、継続していること。
＜主旨＞
情報システム部門長は、目的や効果に応じて適切な業務継続手順・計画の訓練を実施し、実効性を高めていく必要がある。
＜着眼点＞
① 情報システムの事業継続マネジメントシステムの適用範囲及び達成目標と合致していること。

② 明確に定められた狙いと達成目標をもって、周到に計画された適切なシナリオに基づいていること。
③ 該当する利害関係者を含めた業務継続の取り組み全体について、長期にわたる総合的な妥当性を確認すること。
④ 業務の中断・阻害のリスクを最小限に抑えること。
⑤ 訓練実施結果、提案、及び改善するための処置を含めた正式な訓練実施報告書を作成すること。
⑥ 継続的な改善を促進する観点からマネジメントレビューを行うこと。
⑦ 定期的に実施され、また組織内又は組織が活動する事業環境に大きな変化があった場合、実施すること。

(2) 情報システム部門長は、訓練の実施手順に則り実施し、マネジメントレビューを行い、マネジメントサイクル（PDCA）を回すこと。

＜主旨＞

情報システム部門長は、国内外の状況変化や時間の経過により陳腐化させないために、業務継続計画策定後も、定期的に訓練を繰返し実施する必要がある。 また、業務継続計画は、訓練により常に最新の状態に更新をする必要がある。

＜着眼点＞

① 業務継続計画の訓練の実施手順は、次の手順及び実施項目を含めること。
- 訓練計画の策定
- 訓練評価項目の策定
- 訓練シナリオの策定
- 訓練の実施
- マネジメントレビュー
- 業務継続計画の改善/更新

② 訓練結果を反映すること。
- 実施の優先順位
- 情報システム/予算/体制/備蓄
- サプライチェーンマネジメント　等

5. 計画の見直しの管理

(1) 情報システム部門長は、情報システムにかかわる業務の中断・阻害を引き起こす事故が発生し、業務継続計画の発動に至った場合、事故発生後に業務継続計画の評価及び見直しを行うこと。

＜主旨＞

情報システム部門長は、情報システムにかかわる業務に影響を与える重大な事故が発生した場合、事故後に業務継続計画を評価し、見直す必要がある。

＜着眼点＞

① 業務継続手順及び能力の適切性、妥当性及び有効性の継続を確保するために、それらの評価をすること。

② 計画の見直しを、定期的なレビュー、訓練、試験、事故発生後の報告、及びパフォーマンス評価を通して行うこと。

③ 適用される法令及び規制の要求事項の順守、業界のベストプラクティスとの適合、並びに業務継続計画方針及び目的との適合を定期的に評価すること。

④ あらかじめ定められた間隔で、また大きな変更があった場合にも、評価を実施すること。

(2) 情報システム部門長は、業務継続計画が、引き続き、適切かつ有効であることを確実にするために、あらかじめ定められた間隔で、業務継続計画の評価及び見直しを行うこと。

＜主旨＞

情報システム部門長は、業務継続計画が適切かつ有効であることを、あらかじめ定められた間隔で評価し、見直す必要がある。

＜着眼点＞

① 前回の見直しの結果と取られた処置の状況を確認すること。

② 業務継続計画に関連する外部及び内部の課題に変化による、見直しを実施すること。

③ リスクアセスメント、事業影響度分析、業務継続計画及び関連する手順の更新を実施すること。

④ 情報システムにかかわる業務継続計画に影響を与える可能性のある組織内外の環境変化に対応するための手順及び管理策を修正すること。

Ⅸ. 人的資源管理

IT ガバナンス及び情報システム戦略委員会で定められている方針に基づく。

1. 責任と権限の管理

(1) 情報システム部門長は、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ること。

＜主旨＞

情報システム部門長は、情報システムにかかわる企画、開発、運用及び保守業務を効率的に遂行し、誤びゅう及び不正を防止し、機密を保護するため、各業務にかかわる管理者・担当者の責任及び権限を明確に定める必要がある。

＜着眼点＞

① 情報システム部門長は、情報システムにかかわる企画、開発及び保守業務の遂行に必要な責任及び権限を明文化するとともに、運用にあたって具体的な担当者・管理者を明確にしていること。

② 情報システム部門長は、情報システムにかかわる責任及び権限を定めるにあたって、情報システムの職務分掌、指揮命令系統、独立性等を踏まえ、各役割、担当者、管理者などの関係に矛盾がないことを確認すること。

③ 明文化した責任と権限の運用にあたって、情報システム部門長は各担当者、管理者等の能力及び経験を評価し割り当てること。

④ 情報システム部門長は、情報システムにかかわる企画、開発及び保守業務にかかわる責任及び権限を定めるにあたって、責務の分離を明確にしていること。

⑤ 人的資源のセキュリティに関する情報セキュリティ管理基準の該当事項を参照し、確認すること。

(2) 情報システム部門長は、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こと。

＜主旨＞

情報システム部門長は、業務環境及び情報環境の変化に適応させるため、情報システムにかかわる要員の責任及び権限は定期的又は適切なタイミングで見直す必要がある。

＜着眼点＞

① 見直しにあたっては、情報システム部門長は見直しの範囲を明確にしていること。

② 見直しにあたっては、情報システム部門長は見直しの判断基準・根拠を明確にしていること。

③ 見直しの結果を組織体として、承認していること。

④ 見直しにあたっては、情報システム部門長は見直しの手続を明確にしていること。

(3) 情報システム部門長は、要員の責任及び権限を関係者に周知徹底すること。

＜主旨＞

情報システムにかかわる企画、開発、運用及び保守業務を効率的かつ確実に遂行し、人的資源相互の連携を図るため、責任及び権限を個々の要員をはじめ関係者に周知徹底する必要がある。

＜着眼点＞

① 情報システム部門長は、適切な方法及び時期を踏まえ、必要な要員及び関係者に周知徹底を行うこと。

② 情報システム部門長は、情報システムに係る責任と権限について、必要な個々の要員及び関係者の理解を確認すること。

2. 業務遂行の管理

(1) 要員は、責任を果たし、権限を遵守すること。

＜主旨＞

企画、開発、運用及び保守業務を効率的かつ確実に遂行するため及び誤びゅう、不正を防止するため、要員は責任を果たし、権限を遵守する必要がある。

＜着眼点＞

① 企画、開発、運用及び保守業務の責任者は、要員の職務遂行状況を把握する仕組みを確立し、把握していること。

② 情報システム部門長は、要員間の相互牽制の仕組みを構築し、それを適切に運用すること。

③ 要員は作業報告書を作成し、管理者がそれを確認していること。

④ 人的資源のセキュリティに関する情報セキュリティ管理基準の該当事項を参照し、確認すること。

(2) 管理者は、作業分担及び作業量を、要員の知識、能力等から検討すること。

＜主旨＞

企画、開発、運用及び保守業務を計画に基づき遂行し、目的とした成果物の品質を確保するため、管理者は、作業分担及び作業量を要員の知識、能力等から検討する必要がある。

＜着眼点＞

① 情報システム部門長は、要員のスキル、能力を定義していること。

② 管理者は、要員の知識及び能力を反映して作業の割当てを行っていること。

③ 企画、開発、運用及び保守業務の管理者は、要員の作業遂行能力を評価していること。

④ 管理者は、評価に基づき、作業分担及び作業量を見直していること。

(3) 管理者は、要員の計画的及び不測な交替に備え、交替要員の育成をすること。

＜主旨＞

管理者は、業務の適切な遂行のために、計画的及び不測の事態への対応のために、日常的に交替要員の育成をする必要がある。

＜着眼点＞

① 管理者は、業務計画、システム化計画に基づき、中長期的視野も含めた要員計画を策定すること。

② 管理者は、システム化計画に関わる不測の事態を整理し、その対応の要員計画を策定すること。

③ 管理者は、中長期定な観点を含めた要員のスキル向上計画を策定し、実施すること。

(4) 管理者は、要員の交替にあたっては、業務の適切な遂行、誤謬防止、不正防止及び機密保護を考慮すること。

＜主旨＞

要員の交替に際しては、業務の円滑な継続、引継ぎミス等による誤びゅう発生の防止、担当を外れた要員による不正の防止、機密保護を考慮する必要がある。

＜着眼点＞

① 管理者は、交替時の引継ぎルールを明確にしていること。

② 管理者は、引継ぎの期間を考慮した交替を行うこと。

③ 管理者は、業務分担、業務内容に応じて、適宜、アクセス資格を見直し、管理していること。

④ 管理者は、利用技術等の変化に伴い機密保護の方法を。適宜、定めていること。

⑤ 交替者は、引継ぎ内容を文書に作成し、管理者はそれを確認していること。

⑥ 人的資源のセキュリティに関する情報セキュリティ管理基準の該当事項を参照し、確認すること。

(5) 管理者は、不測の事態に備えた代替要員を日常的に確保すること。

＜主旨＞

企画、開発、運用及び保守業務の継続性を維持するため、管理者は不測の事態に備えた代替要員の確保を検討し、育成しておく必要がある。

＜着眼点＞

① 管理者は、代替要員を必要とする作業を明確にし、代替要員の育成をしていること。

② 管理者は、代替要員を確保するまでの臨時措置を検討していること。

3. 教育・訓練の管理

(1) 管理者は、教育及び訓練に関する計画及びカリキュラムを、システム化計画及び人的資源管理の方針に基づいて作成及び見直しを行うこと。

＜主旨＞

情報システム部門長は、情報システムにかかわる一貫した教育及び訓練を行うため、管理者は、システム化計画及び人的資源管理の方針に基づいたカリキュラムを作成し、情報技術の進歩等に応じて見直す必要がある。

＜着眼点＞

① 管理者は、システム化計画及び人的資源管理に基づき教育及び訓練の方針を定めていること。

② 管理者は、組織体の要員育成方針を考慮したスキルスタンダードを定めていること。

③ 管理者は、情報技術の進歩及び多様性を反映し、キャリアパスに基づいてカリキュラムを作成し、それを組織体として承認していること。

④ 管理者は、情報技術の動向及び教育の実績を反映して、カリキュラムを見直していること。

⑤ 人的資源のセキュリティに関する情報セキュリティ管理基準の該当事項を参照し、確認すること。

(2) 管理者は、教育及び訓練に関する計画及びカリキュラムについて、技術力の向上、業務知識の習得、情報システムの情報セキュリティ確保等から検討すること。

＜主旨＞

要員のスキル向上及び業務への参画意識の向上を図るため、教育及び訓練のカリキュラムは、技術力の向上、業務知識の習得及び情報セキュリティの確保等から検討する必要がある。

＜着眼点＞

① 管理者は、情報技術全般及び業務アプリケーション分野について、情報処理技術者として必要な知識、能力を組織体として体系化していること。

② 情報システム部門長の全関係者をも対象にした情報セキュリティにかかわる教育を実施していること。

③ 情報システム部門長は、情報倫理にかかわる教育を実施していること。

(3) 情報システム部門長は、教育及び訓練を、計画及びカリキュラムに基づいて定期的かつ効果的に行うこと。

＜主旨＞

要員が、企画、開発、運用及び保守業務の遂行に必要な知識、能力等を習得するため、情報システム部門長は、教育及び訓練をカリキュラムに基づいて定期的かつ効果的に行う必要がある。

＜着眼点＞

① 情報システム部門長は、教育及び訓練を計画的に実施していること。

② 管理者は、教育及び訓練の実施の効果を評価していること。

③　管理者は、カリキュラムの有効性を定期的に評価していること。
④　情報システム部門長は、教育及び訓練の実施に必要な教材を整備していること。
⑤　教育及び訓練のインストラクタは、必要な経験及び知識を備えていること。

(4)　情報システム部門長は、要員に対するキャリアパスを確立し、業務環境及び情報環境の変化に対応した見直しを行うこと。

＜主旨＞

情報システム部門長は、企画、開発、運用及び保守業務の遂行に必要な知識、能力等を習得させるため、キャリアパスを確立し、業務環境及び情報環境の変化に対応した見直しを行う必要がある。

＜着眼点＞

①　情報システム部門長は、情報戦略、業務環境及び情報環境に基づいてキャリアパスを確立していること。
②　情報システム部門長は、情報戦略、業務環境及び情報環境の変化に対応して、キャリアパスを見直していること。
③　管理者は、キャリアパスを要員に周知徹底していること。
④　管理者は、要員自身によるキャリアパス策定・実施を支援すること。

4. 健康管理

(1) 管理者は、身体的及び精神的に健康を保ち、企画、開発、運用及び保守業務を健全に遂行するため、健康管理を考慮した作業管理を整えること。

＜主旨＞

情報システム部門長は、情報システムにかかわる全ての要員の健康管理を実施し、システムの企画、開発、運用及び保守業務を円滑に実施する必要がある。

＜着眼点＞

①　管理者は、情報システムの構築計画及び人的資源管理に基づき健康管理の方針を定めていること。
②　管理者は、法令等を遵守し、組織体の内部の規約等を定めていること。
　例示：労働基準法、労働安全衛生法等
③　管理者は、組織の方針、規約に基づき、作業環境を整備すること。
　・採光、照明器具
　・騒音対策
　・温度・湿度対策
　・電磁的対策
　・気圧対策
　・換気対策

・休憩設備
・喫煙室
・空調設備の有無

④ 管理者は、組織の方針、規約に照らして、作業時間、休日取得状況等を把握し、適正な作業状況であるかをモニタリングすること。
・作業に必要な要員は確保されているか。
・特定の個人に作業が集中していないか。
・規定以上の残業はないか。
・休暇は取れているか。
・長期の休職者はいないか。
・体調不良による遅刻や欠勤はないか。
・サービス残業はないか。
・残業申請管理は適正か。
・適切な休職の規定が存在するか。

⑤ 人的資源のセキュリティに関する情報セキュリティ管理基準の該当事項を参照し、確認すること。

(2) 管理者は、システム関連する業務の従事者の健康を維持する対策を講ずるため、健康診断及びカウンセリングを行うこと。

＜主旨＞

情報システム部門長は、組織体としてシステムに関わる全ての従事者の健康診断、カウンセリング等を実施し、従事者の健康を管理し、システムの企画、開発、運用及び保守業務を円滑にする必要がある。

＜着眼点＞

① 情報システム部門長は、組織は健康管理の方針に基づき、健康診断、カウンセリングの計画を立てること。

② 情報システム部門長は、健康管理計画に基づき、必要な体制を整備すること。
・産業医の配置や契約医療機関
・休憩室の配置
・定期的な健康診断
・感染症に対する予防管理体制（予防接種燈）
・休業後の復帰体制の整備

(3) 情報システム部門長は、職業病、成人病等、要員の物理的、肉体的管理のみならず、メンタルヘルスケアとして、精神的ないしは心の側面における健康管理を行うこと。

＜主旨＞

情報システム部門長は、システムにかかわる全ての人員のメンタルヘルスを実施し、システムの企画、開発、運用及び保守業務を円滑にする必要がある。

＜着眼点＞

管理者は、メンタルヘルスが内面の問題であることを認識し、相談し易い環境を整え、健康被害を事前に防止すること。

① 組織は、パワーハラスメント等のハラスメント相談窓口を設置すること。

② 産業医は、健康診断結果、残業時間等をモニタすること。

・健康を害する予備軍の把握

・必要な休暇取得の指示

(4) 情報システム部門長は、重大な疾病や災害につながらないようにするために、予防管理体制として、健康診断やカウンセリングも結果に基づいて、作業量の軽減、職種の変更、配置転換等、適切な予防管理体制がとられなければならない。

＜主旨＞

情報システム部門長は、システム関連業務にかかわる労働環境の整備をして健康管理を実施する必要がある。

＜着眼点＞

管理者は、作業従事者の個人的努力のみでは、職場での健康維持が困難であることを認識し、組織として環境を改善すること。

① 労働環境の改善

・空調等の作業環境の改善

・必要な要員の確保

・必要な機器等の支給

② 人事との連携

・ハラスメントある部署からの配置転換

・残業の多い部署からの配置転換

・必要なスキルのある職員の採用

・採用計画、配置計画の見直し

③ ストレスチェック制度に基づくストレスチェックの実施

・ストレスチェック義務事業所は、すべての要員に受けさせることが望ましい。

・義務事業所以外の事業所も受けさせることが望ましい。

X. ドキュメント管理

1. ドキュメントの作成

(1) 利用部門長及び情報システム部門長は、情報システム戦略委員会で定めた方針に従い、ドキュメントの作成ルールを定めること。

＜主旨＞

組織として一貫したドキュメントを作成するために、情報システム戦略委員会で定めたドキュメントの作成方針に従い、体系、記述形式、記述内容等をルールとして定め、利用部門及び情報システム部門が遵守する必要がある。

＜着眼点＞

① ドキュメント作成ルールを明文化し、情報システム戦略委員会が承認していること。

② ドキュメント作成ルールは、ドキュメントの作成者、利用者及び管理の関係者に周知徹底していること。

③ ドキュメント作成ルールの遵守状況をドキュメントの作成者、利用者及び管理の関係者が確認していること。

④ ドキュメントの作成ルールは、利用する情報サービスや情報システムの開発方法、運用形態に応じて見直していること。

⑤ ディジタルファイルを含むドキュメントの機密性、完全性、可用性等の確保のための対策を立てていること。

(2) 利用部門及び情報システム部門の管理者は、ドキュメントの作成計画を策定すること。

＜主旨＞

利用部門及び情報システム部門の管理者は、必要なドキュメントを確実に作成するため、ドキュメント作成計画を策定する必要がある。

＜着眼点＞

① ドキュメント作成ルールに基づいて、IT ガバナンス、企画、開発、運用、保守、外部サービス管理、事業継続管理、及び人的資源管理業務にかかわるすべてのドキュメントの作成計画を策定し、部門長が承認していること。

② 作成するドキュメントは、IT ガバナンス、企画、開発、運用、保守、外部サービス管理、事業継続管理、及び人的資源管理業務の作業手順と整合性を図っていること。

③ 作成するドキュメントの一覧及び作成に要する要員、予算、期間、承認者等を作成計画に反映していること。

(3) 利用部門及び情報システム部門の管理者は、ドキュメントの種類、目的、作成方法等を明確にすること。

＜主旨＞

利用部門及び情報システム部門の管理者は、ドキュメントの種類の過不足を防ぎ、使用目的に応じ効率よく作成するため、ドキュメントの種類、目的、作成方法等をドキュメントの作成計画で明確にする必要がある。

＜着眼点＞

① ドキュメントの種類、目的、作成方法等をドキュメント作成ルールに基づいて定めていること。
② 作成するドキュメントの種類、作成スケジュール等は、開発計画等と整合性を図っていること。
③ ドキュメントの目的に対応した配布先、配布形態を明確にしていること。
④ ドキュメントの作成方法は、利用する情報サービスや情報システムの形態、費用、保守等を考慮していること。
⑤ ドキュメントの作成方法は、再利用を考慮していること。

(4) 利用部門及び情報システム部門の管理者は、ドキュメントの作成計画に基づいて作成すること。

＜主旨＞

ドキュメントは、必要な内容を網羅し、必要な時期までに用意するために、作成計画に基づいて作成する必要がある。

＜着眼点＞

① 作成したドキュメントの種類、内容、作成時期等は作成計画と一致していること。
② ドキュメントの作成計画に基づいて、ドキュメントの作成状況を管理していること。
③ 作成の遅延、中止及び追加並びに内容が変更となったドキュメントを把握し、その理由を明確にし、関係者へ周知徹底していること。
④ 作成の遅延に対する対策を講じていること。
⑤ ドキュメントの作成に要した要員、費用、期間等の実績を把握し、作成計画と対比して次の工程もしくは次の計画立案時に反映していること。

(5) 利用部門長及び情報システム部門長が、作成したドキュメントを承認すること。

＜主旨＞

ドキュメントの品質を確認し、組織体の共有物とするため、ドキュメントは、利用部門長及び情報システム部門長が承認する必要がある。

＜着眼点＞

① ドキュメントの作成にあたり、関係者がレビューしていること。

② 作成するドキュメントの内容等を利用部門長及び情報システム部門長が承認していること。
③ 作成したドキュメントを計画に基づいて配布していること。
④ ドキュメントの作成を関係者に周知徹底していること。

(6) 利用部門長及び情報システム部門長は、定期的にドキュメント作成ルールの見直しをすること。
＜主旨＞
一度定めた作成ルールが形骸化しないため、定期的に作成ルールの見直しをする必要がある。
＜着眼点＞
① 作成ルールの定期的な見直しを明文化し、情報システム戦略委員会が承認していること。
② 作成ルールの見直しを実施していること。

2. ドキュメントの管理
(1) 利用部門長及び情報システム部門長は、情報システム戦略委員会で定めた方針に従い、ドキュメント管理ルールを定め、遵守すること。
＜主旨＞
情報システムの内容と整合したドキュメントを維持し、利用を円滑にするため、原本及び配布されたドキュメントの管理ルールを定め、遵守する必要がある。
＜着眼点＞
① ドキュメント管理ルールを明文化し、情報システム戦略委員会が承認していること。
② ドキュメント管理ルールをドキュメントの作成者、利用者及び管理の関係者に周知徹底していること。
③ ドキュメント管理ルールの遵守状況をドキュメントの作成、利用の管理者が確認していること。
④ ディジタルファイルを含むドキュメントの機密性、完全性、可用性等の確保のための対策を立てていること。

(2) 利用部門及び情報システム部門の管理者は、利用する情報システムや情報サービスの変更に伴い、ドキュメントの内容を更新し、更新履歴を記録すること。
＜主旨＞
利用する情報システムや情報サービスの内容と整合したドキュメントを維持し、最新の状態を明確にするため、利用する情報システムや情報サービスの変更時に関連ドキュメン

トの内容を更新し、更新履歴を記録する必要がある。
＜着眼点＞
① 利用する情報システムや情報サービスの変更の影響を受けるドキュメントを明確にしていること（変更の種類とドキュメントの種類）。
② ドキュメントの更新を遅延なく行っていること。
③ ドキュメントの更新は、ドキュメント管理ルールに基づいて行っていること。
④ 作業内容を指定する位置づけにあるドキュメントは、その作業開始以前に更新されていること（例：プログラムの変更前に、当該変更を指示するプログラム設計書が変更されていること）。
⑤ ドキュメントの更新作業の進捗状況を管理していること。
⑥ 変更の理由、範囲等を記録し、更新履歴として管理していること。

(3) 利用部門長及び情報システム部門長が、ドキュメントの更新内容を承認すること。
＜主旨＞
変更したドキュメントの品質を確認し、組織体の共有物とするため、ドキュメントは、利用部門長及び情報システム部門長が承認する必要がある。
＜着眼点＞
① 変更したドキュメントを関係者がレビューしていること。
② ドキュメントの変更内容等を利用部門及び情報システム部門の管理者が承認していること。
③ 変更したドキュメントをドキュメントの作成計画に基づいて配布していること。
④ ドキュメントの変更を関係者に周知徹底していること。

(4) 利用部門及び情報システム部門の管理者は、ドキュメントの保管、複写及び廃棄の際の不正防止及び機密保護の対策を講じること。
＜主旨＞
ドキュメントの不正利用、漏えい等を防止するため、ドキュメントの保管、複写及び不要ドキュメントの廃棄は、不正防止及び機密保護の対策を講ずる必要がある。
＜着眼点＞
① ドキュメントの保管、複写及び廃棄は、ドキュメントの形態及び重要度（機密度）に応じた不正防止及び機密保護の対策を講じていること。
② ドキュメント管理者を定め、定期的に保管の状況を把握していること。
③ ドキュメント管理ルールに基づいて、ドキュメントの利用状況を記録していること。
④ 機密性の高いドキュメントの利用及び複写は、ドキュメント管理者が承認し、管理台帳へ記録すること。

⑤　機密性の高いドキュメントの廃棄は、溶解、裁断等で行い、ドキュメント管理者が実施の状況を確認していること。

(5)　利用部門長及び情報システム部門長は、定期的にドキュメント管理ルールの見直しをすること。

＜主旨＞

一度定めた作成ルールが形骸化しないため、定期的に管理ルールの見直しをする必要がある。

＜着眼点＞

①　管理ルールの定期的な見直しを明文化し、情報システム戦略委員会が承認していること。

②　管理ルールの見直しを実施していること。

用語定義

章	用語	定義・説明
	情報システム	組織体の活動を支えるデータ･情報の収集、蓄積、処理、伝達、利用に関わる仕組み･体系の総称である。情報通信技術、人間、制度･ルールなどで構成される。
	経営陣	業務執行に責任を有する経営者を含むガバナンスに責任を有する者。具体的には、取締役（会）、経営者、非営利法人の理事等のことを指し、経営者は一人とは限らないため、このような表現を用いた。
Ⅱ	プロジェクト運営委員会	経営者からの権限移譲を受け、開発プロジェクトに対する IT ガバナンスの職務（指示、モニタリング、評価）の遂行責任を有する。プロジェクトの立ち上げ、進捗、完了について経営者への説明責任を有する。調整を容易にするため、プロジェクトの利害関係者及び専門家を構成メンバーに加えることが望ましい。
Ⅱ	プロジェクトマネージャー（PM）	プロジェクト運営委員会からの権限移譲を受けて、プロジェクトの企画立案、運営管理の遂行責任を有する。 自らが担当するプロジェクトの進捗状況についてプロジェクト運営委員会に説明責任を有する。
Ⅱ	フィットアンドギャップ分析	情報システムを導入する際に、情報システムに対するニーズと、情報システムの機能がどれだけ適合(フィット)し、どれだけ乖離(ギャップ)しているかを分析すること。
Ⅲ	プロジェクト標準	プロジェクトの品質を確保するため、プロジェクト担当者が順守すべきガイドライン
Ⅲ	プロジェクト支援ツール	プロジェクトの管理を支援するために用いられるソフトウェアの総称。 主要なものとして以下のものがあり、PM はプロジェクトに適したプロジェクト支援ツールを購入又は開発する必要がある。 ・進捗管理ツール プロジェクトの進捗状況を収集し、見える化するためのツール ・テスト支援ツール テスト計画から実施までを効率化し、品質・進捗・問題管理を容易にするためのツール ・バージョン管理ツール プログラムやドキュメントの変更箇所を管理するためのツール ・デプロイツール 開発環境・テスト環境・本番環境へのプログラム配布を自動化するため

		のツール ・問題管理ツール
Ⅲ	インフラストラクチャー	情報システムにおいて、アプリケーションを実行するために必要なハードウェア、ネットワーク、及びソフトウェアの総称
Ⅲ	CIO（最高情報責任者）	経営者によって任命された、組織全体の情報化推進の最高責任者であり、経営戦略と情報システム戦略の整合性を確保し、その実現に関する統括責任を持つ。 IT 要員の確保や、情報システムに関する組織共通のルールの策定を情報システム部門またユーザ部門に対して指示する必要がある。
Ⅳ	プロダクトオーナー	情報システムの総責任者(ないしは実権限を委譲された代行者)であり、プロジェクトの対象情報システムの利用者・ユースケース・機能・品質・リリース等の決定権をもち、名目ではなく実際に開発チームと一体となってイテレーションに参加できることが必要。
Ⅳ	イテレーション	1～数週の期間を設け、その期間分の計画・分析・設計・実装・テストを実施して、その期間分の情報システムをリリースする活動。1 プロジェクトの中でこの活動を複数回反復する。
Ⅳ	フィードバック	利用者や利用部門からの情報システムに対する改善及び提案要望。
Ⅴ	利用部門	情報システムの利用部門（従来のユーザ）。
Ⅴ	アクセスコントロール	アクセスできるシステムや機能、データなどを利用者の属性に応じて設定して、認可された利用者がアクセスし、認可されていないアクセスを防止するなど、システムの利用を制御すること。
Ⅴ	特権的アクセス権	システム上のあらゆる作業を可能にする、高いレベルの操作権限。
Ⅴ	ログ	システムの利用状況の履歴の記録。例えばシステム作動記録のシステムログ、情報システム運用部門の作業ログ、利用者の活動ログ、アクセスログなど。情報セキュリティインシデント管理の観点からは、イベントログ、障害の内容ログ、原因ログ等となる。
Ⅴ	情報セキュリティインシデント	情報セキュリティを脅かす事件や事故、及びセキュリティ上好ましくない状況。
Ⅴ	ペネトレーション（侵入）テスト	ネットワークに接続されているシステムに対して実際に既知の技術を用いて侵入を試みることで、システムに脆弱性がないかどうかをテストする手法のこと。侵入テスト。
Ⅴ	ファシリティ	情報システムが稼動する機器を格納する設備や施設、建物など。
Ⅴ	サービスレベル管理	運用管理サービスの品質や成果を、サービス利用者とサービス提供者の双方が適切な管理指標に基づいて具体的、定量的に把握することで、コストや要求に見合ったサービスを維持する管理手法。SLM(Service Level Manegement)と略す。

Ⅴ	インシデント管理	インシデント(事故や事件に繋がる不測の事態）に対応するプロセスには、問題を識別し、原因を特定する問題管理、問題を解決するための変更管理、変更結果を適用するリリースのプロセスを含む。
Ⅴ	エスカレーション	利用部門からの連絡、問合わせや要求にサービスデスクでは対応できないときに、運用管理者などの上位者やインシデント対応管理者等の専門家に連絡して対応してもらう、又は上位者の指示を仰ぐこと。
Ⅵ	レグレッションテスト（退行テスト）	システムに修正や機能の追加を行ったことで、関連する他のシステムに影響が及んでいないか確認するためのテスト
Ⅶ	アウトソーシング	企業の事業戦略の達成を支援し、業務及び管理の有効性と効率性をより高めるために、外部組織のリソースを活用し、企業内業務の遂行を外部組織に委託することをいう。
Ⅶ	クラウド	共用可能なコンピューティングリソース（ネットワーク、サービス、ストレージ、アプリケーション、サービス）の集積に、どこからでも、簡便に、必要に応じて、ネットワーク経由でアクセスして利用することを可能とする形態の総称である。クラウドコンピューティングを略した表現である。
Ⅶ	ASP	アプリケーションソフトウェアをインターネットを介してユーザに提供するサービス形態。(Application Service Provider）の略語。
Ⅶ	データ消去証明書	データが消去されたことを証明する書類（作業場所、消去方法、作業期間、作業担当者名等を記載）のこと。
Ⅶ	（ソフトウェア）エスクロー	委託先の倒産等に備え、ソフトウェアのソースコードや技術情報等を第三者（エスクロー・エージェント）に預託すること
Ⅶ	SLA	委託元（サービス利用者）と委託先（サービス提供者）の間で結ばれたサービスレベルに関する書面による合意。Service Level Agreement の略語
Ⅶ	立入監査	委託元が、委託業務を実施している委託先の作業場所、又は委託元のデータを保管している委託先のデータセンタ等に立ち入って、必要な監査を実施すること。
Ⅷ	復旧許容時間/目標復旧時間	復旧許容時間/目標復旧時間（RTO：Recovery Time Objective）は、インシデント発生後、次の処理/事業までに要する時間。①製品又はサービスの事業が再開されなければならない、又は②事業活動が事業が再開されなければならない、又は③資源が復旧されなければならない。
Ⅷ	事業継続（BC）	事業の中断・阻害を引き起こすインシデントに対応し、事前に定められた事業の許容水準/レベルで製品/商品又はサービスの提供/供給を継続する組織/企業の能力/事業力。
Ⅷ	インシデント	事業の中断・阻害、損失、非常事態、危機となり得るか、又はこれらを導き得る状況。

Ⅷ	事業継続マネジメント（BCM）	組織/企業への潜在的な脅威、及びそれが顕在化した場合に引き起こされる可能性がある事業活動への影響を特定し、主な利害関係者の利益、組織の評判、ブランド力、及び価値創造を保護する効果的な対応のための能力/組織力を備え、組織のレジリエンス*を構築するための枠組みを提供するマネジメントプロセス。 （* レジリエンス：情報システムがあらゆるレベルにおいて備えておくべきリスク対応能力・危機管理能力）
Ⅷ	事業継続計画（BCP）	事業の中断・阻害に対応し、事業を復旧、再開し、あらかじめ定められた事業水準に復旧するように導く文書化された手順。
Ⅷ	業務継続計画	IT ガバナンスの事業継続計画に基づき、情報システム部門の長などが作成する情報システムを復旧、再開するための手順。
Ⅷ	事業影響度分析	事業または業務の中断・阻害の与える影響を分析する手順/プロセス。
Ⅷ	リスクコミュニケーション	あるリスクについて利害関係者間で情報交換をしたり、対話をすることによって意思疎通をはかり、相互理解や信頼を構築すること。
Ⅸ	人的資源管理	情報システムの利活用は、組織にとって重要課題であり、組織全体の人的資源の活用とも密接な関係を有している。情報システムに係る人的資源管理として、情報システムの適切な利活用を推進する上で必要な事項を定める。

参考文献

- 一般財団法人日本情報経済社会推進協会(JIPDEC)，ITSMS ユーザーズガイド　JIS Q 20000(ISO/IEC 20000)対応，2012 年
- 経済産業省，情報セキュリティ管理基準（平成 28 年度改正版），2016 年
- 経済産業省商務情報政策局，新版 システム監査基準／システム管理基準解説書－平成 16 年度基準改訂版，2005 年
- 独立行政法人情報処理推進機構(IPA)，アジャイル型開発におけるプラクティス活用事例調査 調査報告書 ガイド編，2013 年
- 独立行政法人情報処理推進機構(IPA)，共通フレーム 2013，2013 年
- 独立行政法人情報処理推進機構(IPA), 情報システムに係る政府調達への SLA 導入ガイドライン，2004 年
- NPO 日本システム監査人協会，情報システム監査実践マニュアル（第 2 版），2005 年
- ISACA，COBIT 5 Framework(日本語訳)，2012 年
- ISACA，COBIT 5 Enabling Processes(日本語訳)，2012 年
- ISACA，Self-Assessment Guide：Using COBIT 5(日本語訳)，2013 年

- JIS Q 38500:2015，情報技術－IT ガバナンス
- JIS Q 22301:2013，社会セキュリティー事業継続マネジメントシステム－要求事項
- JIS X 0161:2008，ソフトウェア技術－ソフトウェアライフサイクルプロセス－保守
- JIS Q 20000-1:2012，情報技術－サービスマネジメント－第 1 部：サービスマネジメントシステム要求事項
- JIS Q 20000-2:2013，情報技術－サービスマネジメント－第 2 部：サービスマネジメントシステムの適用の手引