

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|--|-----|-----|-----|
| I. 情報戦略 | | | |
| 1. 全体最適化 | | | |
| 1.1 全体最適化の方針・目標 | | | |
| (1) ITガバナンスの方針を明確にすること。 | | | |
| 1) 組織体の長<以下に共通>は、コーポレートガバナンスに基いたITガバナンス方針を策定させ、承認していること。 | ○ | | |
| 2) ITガバナンスの方針に基づいて、ITガバナンスの重要成功要因CSF(Critical Success Factors)など具体的な内容を明確に定義していること。 | ○ | | |
| 3) ITガバナンスを具体化し、組織内に周知徹底するためのプロセスを明確にしていること。 | ○ | | |
| 4) ITガバナンスを実現するための推進組織体を整備していること。 | ○ | | |
| 5) 推進組織体に、情報化戦略や情報化投資の決定等について最終的な判断を下す部門・責任者を明確に定義していること。 | ○ | | |
| 6) 組織体の長に直結する情報システム担当の最高責任者CIO(Chief Information Officer)を任命していること。 | ○ | | |
| 7) CIOの役割と責任を明確化し、組織内に周知していること。 | ○ | | |
| 8) ITガバナンスの重要成功要因(CSF:Critical Success Factors)としてオフショア開発利用に関する要因を必要性和リスクを含めて考慮すること。 | ○ | ○ | |
| 9) CIOの指示を、受注(オフショア)先の企画、開発、運用、及び保守業務の責任者へ迅速かつ正確に伝えるための指揮系統を整備すること。 | ○ | ○ | ○ |
| 10) 上記の逆ルートとして、受注(オフショア)先責任者からの情報がCIOに迅速に伝わる情報連絡体制を整備すること。 | ○ | ○ | ○ |
| (2) 情報化投資や情報化構想の決定における原則を定めること。 | | | |
| 1) CIO<以下に共通>は、情報化投資及び情報化構想等にかかわる意思決定の区分(システム利用の原則、採用するアーキテクチャー等)を定めていること。 | ○ | | |
| 2) 意思決定区分ごとに、誰が、いつ、どのような頻度で決定するのかを定めていること。 | ○ | | |
| 3) 各決定を行う場合の基準を定めていること。 | ○ | | |
| 4) 情報化投資や情報化構想等の意思決定の基準が有効かどうかを、定期的に検証し、必要な見直しを行っていること。 | ○ | | |
| 5) 投資効果の評価においてオフショア開発に関するリスクマネジメント(文化の違いや政治・経済上の環境変化によるリスク)を考慮すること。 | ○ | | |
| 6) 文化の相違点の例として当該国固有の考え方や国情の相違、生活・組織・勤務形態の相違、休日の相違等を考慮すること。 | ○ | | |
| 7) 国際環境変化に対応して投資における最適化計画を見直すこと。 | ○ | | |
| (3) 情報システム全体の最適化目標を経営戦略に基づいて設定すること。 | | | |
| 1) 組織体の長は、組織体のビジョン、ミッション、経営戦略を明文化していること。情報システム全体の最適化目標は、経営戦略と整合性がとられていること。 | ○ | | |
| 2) CIO<以下に共通>は、最適化目標の設定に先立ち、現行業務及び現行システムの分析、評価を行い、経営上の問題点の抽出、整理を行っていること。 | ○ | | |
| 3) 情報システム全体の最適化の項目及び各項目の目標を明文化していること。 | ○ | | |
| 4) 明文化された最適化目標の達成が経営戦略に貢献することを明確にしていること。 | ○ | | |
| 5) 情報システムの最適化と経営戦略の整合性について検証、検討していること。 | ○ | | |
| 6) 最適化目標の検討に際して組織体全体の調整を行う場合は受注(オフショア)開発固有の要素(外部環境、メリット、輸出入に関する法的リスクや為替リスク等)を考慮すること。 | ○ | | |
| (4) 組織体全体の情報システムのあるべき姿を明確にすること。 | | | |
| 1) CIO<以下に共通>は、組織体のすべてのユーザ部門の業務および情報システムを統一的にモデル化する手法を定めていること。 | ○ | | |
| 2) 企業のビジョン・ミッションを実現するための情報システムにおける現状の課題を洗い出していること。 | ○ | | |
| 3) 情報システムの現状及びあるべき姿(理想型)をモデル化スタンダードによって記述していること。 | ○ | | |
| 4) 情報システムのあるべき姿において、現状の課題が解決されることを検証していること。 | ○ | | |
| 5) あるべき姿を達成する具体的な手法及び工程表(移行計画)を明らかにしていること。 | ○ | | |
| 6) 情報システムのあるべき姿に関する受注(オフショア)開発の影響(維持管理の容易性など)の有無を評価すること。 | ○ | ○ | |
| (5) システム化によって生ずる組織及び業務の変更の方針を明確にすること。 | | | |
| 1) CIOは、組織及び業務の変更の方針について、経営の方針との整合性を検討していること。 | ○ | | |
| 2) CIOは、情報システムの(再)構築と同期をとって行われるべき組織体制及び業務の変更を明確にしていること。 | ○ | | |
| 3) 組織体の長は、経営層がレビューした組織及び業務の変更の方針を、承認していること。 | ○ | | |
| (6) 情報セキュリティ基本方針を明確にすること。 | | | |
| 1) 情報セキュリティ管理責任者<以下に共通>は、全体最適化計画において、保護すべき情報資産を特定していること。 | ○ | | |
| 2) 情報セキュリティ基本方針について、組織体の長の承認を受け、企業内外に周知していること。 | ○ | | |
| 3) 情報セキュリティの基本方針と全体最適化計画との整合性を確保していること。 | ○ | | |
| 4) 業務の重要度及びリスクの内容と影響度について、リスクアセスメントを行い、リスクマネジメントの結果として、情報資産のセキュリティ対策を明確にしていること。 | ○ | | |
| 5) 情報資産のセキュリティ対策の具体策を関係者に教育し、周知徹底していること。 | ○ | | |
| 6) 情報資産のセキュリティ対策策定に当たり、個人情報保護等、関連する法令等の遵守を検討していること。 | ○ | | |
| 7) 基本方針には以下の事項を含めること。 ① 受注(オフショア)当該国組織を含む情報セキュリティマネジメントシステムの目標を設定するための枠組みを含み、全般的な方向性及び行動指針を含めること。 ② 受注(オフショア)を含む事業上の要求事項、法的または規制要求事項、契約上のセキュリティ義務を考慮すること。 ③ 受注(オフショア)を含む情報セキュリティマネジメントシステムを確立し維持するために必要な戦略上の視点からみた組織環境を整備すること。 ④ 受注(オフショア)を含むリスクを評価するための基準を確立し定義すること。 | ○ | ○ | |
| 8) 基本方針の周知先に受注(オフショア)先を含めること。 | ○ | ○ | ○ |
| 9) オフショア開発に伴い技術提供が必要な場合は輸出管理規制の問題がないか検討すること。 | ○ | ○ | ○ |
| 1. 2 全体最適化計画の承認 | | | |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|---|-----|-----|-----|
| (1) 全体最適化計画の立案体制は、組織体の長の承認を得ること。 | ○ | | |
| 1) CIO<以下共通>は、自らの責任において、全体最適化計画の立案体制を明確化のうえ、組織内に周知していること。 | ○ | | |
| 2) 全体最適化計画の立案について、情報システムの運営等に関与、関連するすべての部門の参加を明示していること。 | ○ | | |
| 3) 全体最適化計画の立案に関与する構成員の役割を、明確にしていること。 | ○ | | |
| 4) 全体最適化計画の立案に必要な資源を確保していること。 | ○ | | |
| 5) 全体最適化計画の立案を中核として担う人材を、能力、経験等を考慮のうえ選任し、配置していること。 | ○ | | |
| 6) 上記を通じて、経営戦略に基づき、組織全体として、整合的かつ一貫性のある情報化推進が担保されていること。 | ○ | | |
| 7) 組織体の長は<以下共通>立案体制を確立するにあたって、オフショアの有識者をメンバーに加えること。 | ○ | ○ | |
| (2) 全体最適化計画は、組織体の長の承認を得ること。 | | | |
| 1) 組織体の長<以下に共通>は、全体最適化計画の立案ルール(起案から承認までの手順を含む)を明文化のうえ、承認し、これを組織内に周知していること。 | ○ | | |
| 2) 全体最適化計画の立案ルールには、体制、時期、検討範囲・事項を明示する他、策定・承認・見直し手順を明確化していること。 | ○ | | |
| 3) 全体最適化計画の立案にあたり、経営戦略との整合性を確保していること(整合性が取れない場合の対処方法を含む)。 | ○ | | |
| 4) 策定した全体最適化計画を承認していること。 | ○ | | |
| (3) 全体最適化計画は、利害関係者の合意を得ること。 | | | |
| 1) 組織体の長は、全体最適化計画の策定、承認に際し、利害関係者の合意を得、合意書を入手していること。 | ○ | | |
| 2) 組織体の長は、前項において承認を得るべき、利害関係者の範囲および合意の手順を明確に定義していること。 | ○ | | |
| 3) オフショアが関係することについて利害関係者の合意を得ること。 | ○ | ○ | |
| 1. 3 全体最適化計画の策定 | | | |
| (1) 全体最適化計画は、方針及び目標に基づいていること。 | | | |
| 1) CIO<以下に共通>は、全体最適化計画に総論ないし前文的に位置づけられる部分を設け、そこに経営戦略に基づいた組織全体としての整合性・一貫性を考慮した全体計画策定の方針及び目標を明文化していること。 | ○ | | |
| 2) 全体最適化計画において、計測可能な重要目標達成指標(Key Goal Indicator)、重要業績評価指標(Key Performance Indicator)を定めていること。 | ○ | | |
| 3) 全体最適化計画の項目間、ないしこれに基づいて策定された下位計画において、上記1)で定めた方針、目標との関連付けないし整合性が確保されていること。 | ○ | | |
| 4) 全体最適化計画の達成状況につき、2)のKGI, KPIによるモニタリング方法を明確にしていること。 | ○ | | |
| 5) 全体最適化計画の達成状況につき、前項のモニタリング方法により、定期的に評価していること。 | ○ | | |
| 6) 全体最適化計画において、IT等の技術採用方針(採用基準、留意事項等)を明確にしていること。 | ○ | | |
| 7) 組織体の長は<以下共通>オフショアに関する方針と目標を明確にし全体最適化計画はその方針と目標に基づいて明確に示すこと。 | ○ | ○ | |
| (2) 全体最適化は、コンプライアンスを考慮すること。 | | | |
| 1) CIO<以下に共通>は、全体最適化計画の策定方針において、法令、ガイドライン、基準などコンプライアンス上、考慮すべき外部ルールの遵守、コンプライアンスリスクへの対処、組織体の構成員に対するコンプライアンスの徹底を明文化していること。 | ○ | | |
| 2) コンプライアンスの適切な運営のため、法務部や外部の専門家との顧問契約など、必要な措置を講じていること。 | ○ | | |
| 3) コンプライアンス面からのレビューに、法務部や外部の専門家を関与させていること。 | ○ | | |
| 4) 全体最適化計画の策定時点で法令、ガイドライン、基準などコンプライアンス上、考慮すべき外部ルールをすべて洗い出して、参照可能な状況にしていること。 | ○ | | |
| 5) 全体最適化計画の運営上、今後適用、あるいは将来的に制定が予想される法令等への対応を考慮していること。 | ○ | | |
| 6) 全体最適化計画の運営上、考慮が必要な法令等のリストを、定期的及び必要に応じて見直し、その適用可否を考慮していること。 | ○ | | |
| 7) 全体最適化計画の策定に際し、コンプライアンスリスクをリストアップしたうえ、個別にその対処策を講じていること。 | ○ | | |
| 8) 全体最適化計画の運営に当たり、組織体の構成員に対し、コンプライアンス徹底のための方策を | ○ | | |
| 9) オフショア対象国のコンプライアンスを考慮すること。 | ○ | ○ | ○ |
| 10) オフショア対象国について、例えば中国の場合、中央政府の法令だけでなく、地方の法令の準拠を考慮すること。 | ○ | ○ | ○ |
| 11) 開発課程での国際間の争議・調停等の紛争解決に備えて国内外の管轄裁判所など考慮すること。 | ○ | ○ | ○ |
| (3) 全体最適化計画は、情報化投資の方針及び確保すべき経営資源を明確にすること。 | | | |
| 1) CIO<以下に共通>は、全体最適化計画において、情報化投資の方針を明確にしていること。 | ○ | | |
| 2) 前項の情報化投資の方針には、経営戦略とのリンク付け、環境変化への対応、新技術の採用ルール等を盛り込んでいること。 | ○ | | |
| 3) 情報化投資の実施に当たり、人的・物理的資源や金銭的資源(投資資金の調達)など、確保すべき経営諸資源や、管理すべき情報資産を明確にしていること。 | ○ | | |
| 4) 情報化投資が、全体最適化計画において定めた情報化投資方針に従っているかどうかを、確認する手順を定めていること。 | ○ | | |
| 5) 情報化投資の実施に際し、経営資源の不足や環境変化など、不測の事態が生じた場合の対応手順を定めていること。 | ○ | | |
| 6) オフショアを考慮する場合、経済資源として対象国の人材、設備、技術、費用などを十分調査し、考慮すること。 | ○ | ○ | |
| (4) 全体最適化計画は、投資効果及びリスク算定の方法を明確にすること。 | | | |
| 1) CIO<以下に共通>は、計画採択や修正の判断基準を明確にするため、投資効果及びリスク算定について、その方法(算定のタイミング、対象、手法、実施主体、算定結果の承認者)を明確にしていること。 | ○ | | |
| 2) 前項の投資効果及びリスク算定において、定量的要素と定性的要素の両方を勘案していること。 | ○ | | |
| 3) 投資効果及びリスク算定にあたり、全体最適化計画の策定、個別情報システムの開発計画の策定、情報システム稼働一定期間後など、適切なタイミングで実施していること。 | ○ | | |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|--|-----|-----|-----|
| 4) 投資効果及びリスク算定の結果を、計画の修正、リスクの許容限度の認定、追加的なリスク対策の可否の検討などに活用していること。 | ○ | | |
| 5) 投資効果及びリスク算定の結果に基づき、全体最適化計画修正のトリガーとなる閾値(いきち)を定義していること。 | ○ | | |
| 6) 前項の閾値の妥当性を、事前的あるいは事後的に検証していること。 | ○ | | |
| 7) 投資効果およびリスク算定が適正に実施されているかをモニタリングすることを定義していること。 | ○ | | |
| 8) 投資効果に関するリスク算定のための脅威と脆弱性の評価及び全体評価のための方法についてオフショア当該国の固有のリスクを十分に調査し対策を明確にすること。 | ○ | ○ | |
| (5) 全体最適化計画は、システム構築及び運用のための標準化及び品質方針を含めたルールを明確にすること | ○ | ○ | ○ |
| 1) C10<以下に共通>は、情報システムの企画、開発、運用および保守業務に係る標準化及び品質確保にかかる方針(方針を定める目的を含む)を、全体最適化計画のなかで明文化していること。 | ○ | | |
| 2) 前項の方針を見直す場合の条件(環境変化等)および見直しのポイントを定めていること。 | ○ | | |
| 3) 環境変化等に応じて情報システムの企画、開発、運用および保守業務に係る標準化及び品質にかかわる方針を見直していること。 | ○ | | |
| 4) 情報システムの企画、開発、運用および保守業務に係る標準化及び品質確保にかかる方針を、組織体として承認していること。 | ○ | | |
| 5) 情報システムの企画、開発、運用および保守業務に係る標準化及び品質確保にかかる方針を、周知徹底する関係部門の範囲を明確にしていること。 | ○ | | |
| 6) 前項に基づき、組織内に周知徹底を図っていること。また、関係者の理解を確認する方法を定めていること。 | ○ | | |
| 7) 標準化及び品質確保にかかる方針に基づき、企画、開発、運用および保守業務に係る標準・品質基準(以下、個別業務標準という)を、明文化していること。 | ○ | | |
| 8) 明文化した個別業務標準を、組織体として承認していること。 | ○ | | |
| 9) 明文化した個別業務標準を、関係者に周知徹底していること。 | ○ | | |
| 10) 業務標準の見直しの条件および見直しのポイント、ルールを明文化していること。 | ○ | | |
| 11) 前項のルールに従い、個別業務標準を見直していること。 | ○ | | |
| 12) 品質方針を含めた全体最適化のためのルールを明確にする際には異国への情報伝達の正確性を考慮し、詳細に文書化を行い曖昧性を排除した明確な内容にすること。 | ○ | ○ | ○ |
| (6) 全体最適化計画は、個別の開発計画の優先順位及び優先順位付けのルールを明確にすること。 | ○ | ○ | ○ |
| 1) C10<以下に共通>は、全体最適化計画のなかで、個別の開発計画の優先順位及び優先順位付けの決定方法、優先順位を必要に応じて見直すことを、ルールとして明確に定義していること。 | ○ | | |
| 2) 前項の優先順位付けの設定に際して、経営課題や情報戦略の緊要性(経営課題を解決する情報システムの重要性および緊急性)、業務ニーズ、技術的な実現可能性、投資予算枠との整合性、開発 | ○ | | |
| 3) 個別のシステム開発計画の着手順序、資源配分、開発期間について、業務との整合性を考慮のうえ、決定していること。 | ○ | | |
| 4) 個別のシステム開発計画の優先順位を決定した際に、その理由を説明する関係者を明確にしていること。 | ○ | | |
| 5) 個別のシステム開発計画への着手は、決定済みの優先順位に従っていること。 | ○ | | |
| 6) 決定済みの優先順位に従って、個別のシステム開発計画に着手しているかどうかをモニタリングするよう、ルール化していること。 | ○ | | |
| 7) 前項に基づくモニタリング結果の報告を受け、その内容により適切な対応をしていること。 | ○ | | |
| 8) 部分的なサブシステム開発をオフショアで行う場合は国内側の開発との境界を特に明確にして進めること。 | ○ | ○ | ○ |
| (7) 全体最適化計画は、外部資源の活用を考慮すること。 | ○ | ○ | |
| 1) C10<以下に共通>は、全体最適化計画の実施に当たり、必要に応じ外部資源の活用を考慮していること。 | ○ | | |
| 2) 全体最適化計画の実施に際し、確保が必要な資源を、質・量の両面から適切に評価し、把握していること。 | ○ | | |
| 3) 前項の資源確保に必要なコストの算定方法を適切に定めていること。 | ○ | | |
| 4) 内部資源について、外部資源と比較のうえ、質・量両面からその十分性評価、コストの算定を行い、全体最適化計画の実施に十分かどうかを考慮していること。 | ○ | | |
| 5) 外部資源の活用を柔軟に行うため、平素から情報収集していること。 | ○ | | |
| 6) 全体最適化計画の実施に必要な資源とその確保状況について、関係者(個別のシステム開発計画の優先順位を決定した際に、その理由を説明する関係者)に説明責任が果たせるように、客観性のある評価資料を提示していること。 | ○ | | |
| 7) 前項において、全体最適化計画採択できない、あるいは要望どおり実現できない場合に、資源不足をその理由とする場合には、外部資源の採用を不可とする理由を明確に示していること。 | ○ | | |
| 8) 外部資源の活用が適切に行われているかどうかをモニタリングするよう、ルール化していること。 | ○ | | |
| 9) 前項に基づくモニタリング結果の報告を受け、その内容により適切な対応をしていること。 | ○ | | |
| 10) オフショアにより外部資源(人材・ソフト・ハード)を活用する場合、各国の特徴や強み、弱み、リスクを十分考慮すること。 | ○ | ○ | |
| 1. 4 全体最適化計画の運用 | | | |
| (1) 全体最適化計画は、関係者に周知徹底すること。 | ○ | ○ | |
| 1) C10<以下、本項に共通>は、全体最適化計画のなかで、同計画を組織の構成員に周知徹底することの重要性を明確にしていること。 | ○ | | |
| 2) 全体最適化計画を周知徹底すべき関係者を、リストを作成するなどにより明確化していること。 | ○ | | |
| 3) 全関係者に、全体最適化計画(当初、及び見直し後はその都度)の趣旨と内容を周知徹底し、且つ理解したことを確認していること。 | ○ | | |
| 4) 全体最適化計画の周知徹底状況をモニタリングするルールを定めていること。 | ○ | | |
| 5) 前項に基づくモニタリング結果の報告を受け、その内容により適切な対応をしていること。 | ○ | | |
| 6) 組織体の長は全体最適化計画について受注(オフショア)の開発責任者及びブリッジSEに周知すること。 | ○ | ○ | |
| (2) 全体最適化計画は、定期的及び経営環境等の変化に対応して見直すこと。 | ○ | ○ | ○ |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|--|-----|-----|-----|
| 1)C10<以下に共通>は、全体最適化計画について、定期的および必要に応じて見直すこと、及び適切な見直しの手順(見直しのトリガーやタイミング)を明確化していること。 | ○ | | |
| 2)全体最適化計画を、年度ごとや環境変化による情報戦略の変更に対応して見直していること。 | ○ | | |
| 3)全体最適化計画を見直す場合には、その理由を明確にし、利害関係者その他の了承を得ていること。 | ○ | | |
| 4)全体最適化計画の見直しに当たっては、組織体の長が承認していること。 | ○ | | |
| 5)全体最適化計画の見直し結果を、関係者に周知徹底していること。 | ○ | | |
| 6)全体最適化計画が、1)で定めた手順どおりに見直されているかモニタリングするルールを定めていること。 | ○ | | |
| 7)前項に基づくモニタリング結果の報告を受け、その内容により適切な対応をしていること。 | ○ | | |
| 8)オフショア開発を行う場合、国際環境の変化に即応できるようモニタリング体制を整備すること。 | ○ | ○ | ○ |
| 2. 組織体制 | | | |
| 2.1 情報システム化委員会 | | | |
| (1)全体最適化計画に基づき、委員会の使命を明確にし、適切な権限及び責任を与えること。 | ○ | ○ | |
| 1)組織体の長は、全体最適化計画を推進し、自らの意思決定を支援する組織として、情報システム化委員会(名称は組織体により任意、以下同じ)を設置していること。 | ○ | | |
| 2)C10<以下に共通>は、全体最適化計画の実施に責任を持つ各部門の長を、情報システム化委員会の構成員に含めていること。 | ○ | | |
| 3)委員会の構成員を、経営体制や組織変更、業務機能の変更、情報戦略の変更に応じて、適時に見直していること。 | ○ | | |
| 4)前項の構成員を、自ら任命していること。 | ○ | | |
| 5)情報システム化委員会の役割、組織上の位置づけを明確にし、関係者の合意を得ていること。 | ○ | | |
| 6)情報システム化委員会の権能として、情報システムの諸活動のモニタリングにかかる項目を含めていること。 | ○ | | |
| 7)情報システム化委員会の運営に必要な資源(例えばスタッフ機能)を適切に確保していること。 | ○ | | |
| 8)情報システム化委員会の活動状況につき、適時に報告を受け、全体最適化計画の実施を含む意思決定支援に活用していること。 | ○ | | |
| 9)情報システム化委員会に、その機能を十分に果たせるよう、必要かつ適切な権限および責任を与えていること。 | ○ | | |
| 10)情報システム化委員会もしくは相当する組織にオフショア関係者を加えること。 | ○ | ○ | |
| 11)国際間のコンプライアンスを考慮し国際紛争を専門とする法律家を体制に加えること | ○ | ○ | |
| 12)オフショアに関する権限・責任を明確にすること。 | ○ | ○ | |
| 13)オフショアの元請側独自にも委員会を構成していること。 | | | |
| (2)委員会は、組織体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ずること。 | ○ | ○ | ○ |
| 1)情報システム化委員会<以下に共通>は、自らがモニタリング対象とする情報システムにかかる活動(企画、開発、運用および保守業務等)を明確化していること。 | ○ | | |
| 2)モニタリングの内容(PCDAサイクルやプロシージャー)を明確にしていること。 | ○ | | |
| 3)モニタリングの方針ないし着眼点(全体最適化計画や個別業務計画との整合性、経営戦略や外部環境ほかの与件変化への対応など)を明確にしていること。 | ○ | | |
| 4)モニタリングの方策を制定し、モニタリング対象となる組織、業務部門に明示にしていること。 | ○ | | |
| 5)モニタリング対象項目(障害、事故、プロジェクトや予算執行の進捗、情報化投資の是非に関する情報等)を明確にしていること。 | ○ | | |
| 6)モニタリングの過程で不具合を発見した際の対処(不具合事象への個別対処のほか、必要に応じ、全体最適化計画への反映を行うことを含む)を明確にしていること。 | ○ | | |
| 7)モニタリングの過程で、不具合にはいたらぬものの、トラブルが予見される事象(他社の事例を含む)が発生した場合についても、その対処方法を明確にしていること。 | ○ | | |
| 8)前項<6、7>に基づいた不具合などについて、全体最適化計画への反映などの対処を適切に実施していること。 | ○ | | |
| 9)受注(オフショア)組織全体を包括するモニタリングを実施すること。 | | ○ | ○ |
| 10)受注(オフショア)側技術者に対して開発上の問題点を積極的に上部に提言できるように指導すること。 | | ○ | ○ |
| (3)委員会は、情報技術の動向に対応するため、技術採用指針を明確にすること。 | ○ | ○ | ○ |
| 1)情報システム委員会<以下に共通>は指針として定めるべき内容、全体最適化計画の中での位置づけ、情報システム化委員会による具体的な措置権限を明確にしていること。 | ○ | | |
| 2)技術採用指針を定め、これを文書化していること。 | ○ | | |
| 3)技術採用指針の見直しルール(見直し頻度、その他見直しのトリガーとなる事項)を定めていること。 | ○ | | |
| 4)技術採用指針の中で、組織体に関連する情報技術分野を明確にしていること。 | ○ | | |
| 5)変化する情報技術動向の適切かつ迅速な把握と対処を可能とするため、情報技術の最新動向を収集する役割およびその役割を担う部門を明確にしていること。 | ○ | | |
| 6)技術採用指針を高度化を図るため、必要に応じ外部の識者の助言を得ていること。 | ○ | | |
| 7)技術採用指針の運営実態について、組織体の長に、適時に報告していること。 | ○ | | |
| 8)受注(オフショア)先の技術が関係する場合、当該国及び対象企業の情報技術動向に対応した技術採用指針を明確にすること。 | | ○ | ○ |
| (4)委員会は、活動内容を組織体の長に報告すること。 | ○ | ○ | |
| 1)情報システム化委員会<以下、本項に共通>は、その活動を組織体の長に報告する手続き、頻度、報告書に盛り込むべき内容、レビューの実施要領を定めていること。 | ○ | | |
| 2)委員会の活動報告書について、レビュー会議を開催していること。 | ○ | | |
| 3)委員会の活動内容の報告書を、組織体の長に報告書していること。 | ○ | | |
| 4)報告内容として受注(オフショア)先での開発状況に関する情報を定期的または必要時点で組織体の長に提供すること。 | ○ | ○ | |
| (5)委員会は、意思決定を支援するための情報を組織体の長に提供すること。 | ○ | | |
| 1)情報システム化委員会<以下に共通>は、組織体の長に対し、全体最適化計画や個別業務計画等に関する意思決定を適時に支援するためのための情報を、明確にしていること。 | ○ | | |
| 2)全体最適化計画を実現するためのPDCAサイクルを明確にし、そのサイクルに従った適切な運営を担っていること。 | ○ | | |
| 3)組織体の長に対し、全体最適化計画にかかる意思決定支援のため、適時、かつ適切に情報提供を行っていること。 | ○ | | |
| 4)前項の情報提供を適切に行うため、提供に際しては、代替案の評価基準、判断根拠を含めていること。また、事実と意見の区別に配慮していること。 | ○ | | |
| 5)情報化投資の是非の判断に資する情報を適時に提供していること。 | ○ | | |
| 6)前項の機能を果たすため、モニタリング活動の一環として、情報化投資の是非判断が可能なように、必要な情報収集を行っていること。 | ○ | | |
| 2. 2 情報システム部門 | | | |
| (1)情報システム部門の使命を明確にし、適切な権限及び責任を与えること。 | ○ | | |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|---|-----|-----|-----|
| 1)情報システム部門の長<以下に共通>は、情報システム部門の使命、役割を明文化し、関係者の承認を得ていること。 | | | |
| 2)前項に際しては、利用者部門との区分、エンドユーザーコンピューティングの方針、業務・システムやデータの帰属(オーナーシップ)を盛り込んでいること。 | | | |
| 3)情報システム部門の使命、役割の遂行に必要な権限、責任を付与し、そのために必要な資源を確保していること。 | | | |
| 4)使命、役割を組織内に周知徹底し、ITガバナンスの実現に貢献していること。 | | | |
| 5)情報システム部門の業務運営の各面において、特定のITベンダーに依存していないこと。 | | | |
| (2)情報システム部門は、組織体規模及び特性に応じて、職務の分離、専門家、権限付与、外部委託等を考慮した体制にすること。 | ○ | ○ | |
| 1)情報システム部門の責任者<以下に共通>は、情報システムの特性、規模に応じて、適切に職務を定義し、役割を細分化していること。 | ○ | | |
| 2)迅速かつ業務実態に即して運営が行われるよう、部門内において、前項で定めた役割に応じ適切に権限を付与していること。 | ○ | | |
| 3)前々項で定めた役割が適切に担われるように、専門性を勘案しつつ要員を配置していること。 | ○ | | |
| 4)業務活動の状況に即して、物理的・論理のおよび環境のセキュリティを適切に確保するため、必要な方策を講じていること。 | ○ | | |
| 5)前項の方策を有効ならしめるために、当事者以外の第三者によるセキュリティ監査などを通じて、セキュリティ確保策の有効性を確認していること。 | ○ | | |
| 6)業務活動の一部または全部を外部委託する際には、予め業務委託方針や委託先選定、管理基準等を定めていること。 | ○ | | |
| 7)前項に基づき、外部委託先を選定し、適切に管理、監督していること。 | ○ | | |
| 8)外部委託体制にはオフショアの当該国の専門家を含めること。 | | ○ | |
| 2. 3 人的資源管理の方針 | | | |
| (1)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。 | ○ | ○ | ○ |
| 1)情報システム部門の責任者<以下に共通>は、自組織内で用いる情報技術に求められるITスキル標準を定め、スキルズインベントリーにより人的資源の現状を把握し、その内容を定期的に更新していること。 | ○ | | |
| 2)前項のスキルズインベントリーについて、技術採用指針との整合性を確保していること。 | ○ | | |
| 3)受注(オフショア)側は要求する技術は明確にすること。 | | ○ | |
| 4)受注(オフショア)側は必要な技術を有する人材を明確にすること。 | | | ○ |
| (2)人的資源の調達及び育成の方針を明確にすること。 | ○ | ○ | ○ |
| 1)情報システム部門の責任者<以下に共通>は、自らの情報化に必要な人材確保のため、採用、育成方針あるいは将来計画を明確にしていること。 | ○ | | |
| 2)前項の方針、計画には、外部資源の調達も考慮していること。 | ○ | | |
| 3)前2項の方針、計画を組織内に周知徹底していること。 | ○ | | |
| 4)オフショア開発企業選定基準は人的資源調達条件を明確にすること。 | | ○ | |
| 5)ブリッジSEの力量を評価をすること。 | | ○ | |
| 6)ブリッジSEの評価は、マネジメントスキル、技術スキル、コミュニケーションスキル(対日本だけでなく、中国現地組織とのコミュニケーションを含む)、協調性、積極性、誠実性などを | | ○ | ○ |
| 7)発注側は要員の育成方針を明確にすること。 | | ○ | |
| 8)受注(オフショア)側は要員の育成・補充計画を明確にすること。 | | | ○ |
| 9)受注(オフショア)側は要員育成時は育成費用についてその後の仕事の継続を前提とするなど、育成効果が有効に活用できる対策を講じていること。 | | | ○ |
| 3. 情報化投資 | | | |
| (1)情報化投資計画は、経営戦略との整合性を考慮して策定すること。 | ○ | | |
| 1)CIO<以下に共通>は、情報化投資計画の策定に当たり、情報化投資の対象範囲とその区分、作成や見直し周期を予め定めていること。 | | | |
| 2)情報化投資の有効性を評価する指標および目標を予め定めていること。 | | | |
| 3)前項の指標および目標について、経営戦略と整合性が取れていることを確認していること。 | | | |
| 4)情報化投資計画を見直す場合には、情報システム化委員会の審議に付すとともに、組織体の長に報告していること。 | | | |
| 5)情報化投資計画に盛り込む、個別システム化案件の優先順位付けのため、事前に、定量的な投資価値等に基づく検討を行っていること。 | | | |
| 6)優先順位付けは、関係者の合意を得ていること。 | | | |
| 7)前々項の投資価値等による検証結果を、投資実施から一定期間経過後、再度事後的に検証していること。 | | | |
| 8)組織体の長は、情報化投資計画およびその変更をその都度承認していること。 | | | |
| (2)情報化投資計画の決定に際して、影響、効果、期間、実現性等の観点から、複数の選択肢を検討すること。 | ○ | | |
| 1)CIOは、情報化投資計画の策定に際し、経営戦略所管部門とも協議のうえ、影響、効果、期間、実現性等の観点から、明確にその内容に差がある複数の選択肢を検討・提示し、情報化システム委員会の審議に付していること。 | | | |
| 2)情報システム化委員会は、事務局から提示された複数の選択に対し、予め定めた選択基準に沿って、審議を行っていること。 | | | |
| 3)情報システム化委員会は、審議の結果選択した内容について、その採択理由を利害関係者に説明できるようにしていること。 | | | |
| 4)オフショア開発を選択する場合は外国企業に関連する特徴的な利点と影響を明確にすること。 | | | |
| (3)情報化投資計画に関する予算を適切に執行すること。 | ○ | | |
| 1)CIO<以下に共通>は、情報化投資計画にかかる予算執行の最終決裁者を定めていること。 | | | |
| 2)予算執行の時期、金額、契約形態等を、情報化投資計画に盛り込んでいること。 | | | |
| 3)情報化投資計画にかかる予算の執行時期、金額を、経営環境の変化に合わせて、調整していること。 | | | |
| 4)情報化投資計画にかかる予算執行の適切性を確保するよう、第三者による検証を実施していること。 | | | |
| 5)前項に関連して、不適切な執行が明白である場合に、それを停止する内部統制の枠組みがあること。 | | | |
| 6)情報化投資計画にかかる予算執行が、適切であるかを評価する体制を設けていること。 | | | |
| (4)情報化投資計画に関する投資効果の算出方法を明確にすること。 | ○ | | |
| 1)CIO<以下に共通>は、情報化投資案件の採否判断に際して、個別案件ごとに、投資予算および投資効果を算出することをルール化していること。 | | | |
| 2)前項のルール化には、予め効果算出の方法を盛り込んでいること。算出方法の適否を見直す仕組みを構築していること。 | | | |
| 3)情報化投資案件について、投資予算および期待される投資対効果を、事前に個別算定していること。 | | | |
| 4)前項の算定が漏れなく、かつ適切に実施されているかを、客観的にモニタリングする内部統制の枠組みを設けていること。 | | | |
| 5)前項の予算、投資効果の算出結果を横断的に検証し、客観性を担保していること。 | | | |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|--|-----|-----|-----|
| 6)投資効果の評価結果を、今後の情報化投資計画にフィードバックする手続きを明確化していること。 | | | |
| (5)情報システムの全体的な業績及び個別のプロジェクトの業績を財務的な観点から評価し、問題点に対して対策を講じること。 | ○ | | |
| 1)C10<以下に共通>は、情報システム全体および個別のプロジェクトにつき、財務的観点からの評価基準を予め定め、モニタリングを実施していること。 | | | |
| 2)1)の結果、財務的な課題が発覚した場合には、予め用意した対応手順等に即し、適切に対処すべき旨ルール化していること。 | | | |
| 3)1)のルールには、財務的な評価を行う際の指標だけでなく、財務的な要請に基づくアラームポイント(閾値)を盛り込んでいること。 | | | |
| 4)1)に定める評価ないしモニタリングの対象、個別情報化投資案件(プロジェクト)については、投資規模等による抽出基準を明確にしていること。 | | | |
| 5)情報システム全体と抽出された個別投資案件(プロジェクト)の各々について、財務的観点からのモニタリングを実施していること。 | | | |
| 6)モニタリングの結果、アラームポイントへの抵触など、発生が予想される財務的な課題につき、予め対応手順(発動権限者を含む)を定めていること。 | | | |
| 7)財務的観点からの評価が実施されないまま、プロジェクトが推進されることを防止する内部統制の枠組を設けていること。 | | | |
| (6)投資した費用が適切に使用されたことを確認すること。 | ○ | | |
| 1)情報システム部門の責任者<以下に共通>は、情報化投資案件について、費用の支払時期、金額、資金使途、支払先の実績記録をルール化し、個別案件ごとに記録し、計画段階の予定費用と突合することをルール化していること。 | | | |
| 2)前項の費用の記録、計画段階の予定費用との都合の結果、大幅なずれが生じた場合の理由を記録していること。 | | | |
| 3)投資内容について、計画対比で大きくズレが生じた場合には、その要因を分析のうえ、補正投資の実施ないし、原投資計画の修正(他の投資案件との比較考量を含む)を行っていること。 | | | |
| 4)承認された計画に計上された予定費用が、計画通り適正に使用されたことを確認する手続きをルール化していること。 | | | |
| 5)前項の確認が行われないまま放置されるのを防止する内部統制の仕組みを構築し、その枠組みの元で適切に運営していること。 | | | |
| 4. 情報資産管理の方針 | | | |
| (1)情報資産の管理方針及び体制を明確にすること。 | ○ | | |
| 1)組織体の長<次項と共通>は、自らの責任において情報資産の管理体制を決定し、情報資産管理責任者を任命していること。 | | | |
| 2)情報資産管理責任者について、組織体の長の代務者として、組織全体及び必要に応じ部門ごとに任命していること。 | | | |
| 3)情報資産管理責任者<以下に共通>は情報資産の管理方針を策定し、組織体制と併せて文書化のうえ、組織体の長の承認を得ていること。 | | | |
| 4)情報資産の管理方針及び体制について、組織内に周知徹底していること。 | | | |
| 5)情報資産の管理方針を周知徹底すべき関係者を、予め明確にしていること。 | | | |
| 6)管理すべき情報資産について、分類および情報資産の定義などを明確化していること。 | | | |
| 7)情報資産管理のPDCAサイクルを明確にし、そのサイクルで情報資産管理業務を運営していること。 | | | |
| 8)情報資産管理業務の全部または一部を外部委託する場合には、予め定めた委託先選定基準に沿って審査のうえ、委託先を選定していること。 | | | |
| 9)情報資産にかかるリスク分析とリスク対策実施の効果等を踏まえ、情報資産管理体制が有効に機能しているかを適時にモニタリングしていること。 | | | |
| 10)上記の管理サイクルが適正かつ効率的に運営するため、統制機能として内部監査体制を構築していること。 | | | |
| 11)受注(オフショア)側の関係する情報資産を含めて全て明確にして、管理方法を明確に規定すること。 | | ○ | ○ |
| (2)情報資産のリスク分析を行い、その対応策を考慮すること。 | ○ | ○ | ○ |
| 1)情報資産管理責任者<以下に共通>は、管理対象となる情報資産を漏れなく洗い出したうえ、変更管理も含め、適切に台帳(ないし目録)として整備していること。 | ○ | | |
| 2)情報資産ごとに、直面するリスク要因とそのインパクトを洗い出し(リスク分析と呼ぶ)、その結果を踏まえ、優先順位付けのうえ、個々に対応策を講じていること。 | ○ | | |
| 3)前項のリスク分析および対応策につき、第3者的な観点から横断的に十分性を検証のうえ、組織体の長の承認を得ていること。 | ○ | | |
| 4)国際取引のインターネット環境を考慮したリスク分析・リスク対応を行うこと。 | ○ | ○ | ○ |
| (3)情報資産の効率的で有効な活用を考慮すること。 | ○ | | |
| 1)情報資産管理責任者<以下に共通>は、情報資産の活用を最大限考慮していること。具体的には効率性(利用率、稼働率、生産性)、有効性(経営戦略・情報戦略、情報化投資、業務完全などの目的達成度向上)の両面にわたる活用を図っていること。 | | | |
| 2)重要業績評価指標や重要目標達成指標などの指標を予め設定のうえ、情報資産の効率性、有効性両面でのモニタリングを可能としていること。 | | | |
| 3)前2項の活用状況を把握するため、定期的なモニタリングの枠組みを導入し、運営していること。 | | | |
| (4)情報資産の共有化による生産性向上を考慮すること。 | ○ | | |
| 1)情報資産管理責任者<以下に共通>は、生産性の向上を図るため、情報資産の共有化を図っていること。 | | | |
| 2)生産性向上の評価のために、重要業績評価指標や重要目標達成指標などの指標を、予め設定していること。 | | | |
| 3)前項の生産性向上の指標を基に、モニタリングしていること。 | | | |
| 5. 事業継続計画 | | | |
| (1)情報システムに関連した事業継続の方針を策定すること。 | ○ | ○ | ○ |
| 1)C10<以下に共通>は、事業継続の方針を策定し、文書化していること。 | ○ | | |
| 2)方針策定の前提となる事業継続の対象範囲を明確にしていること。 | ○ | | |
| 3)自社の事業にかかる潜在的な脅威を洗い出し、情報システムに関連する項目、影響範囲を明確にしていること。 | ○ | | |
| 4)事業継続の体制、関連部門の役割、従業員への教育訓練、関係者の周知徹底、定期的なテストによる有効性検証、事業継続方針の定期的な見直しなどの方針を明確にしていること。 | ○ | | |
| 5)方針に基づいて事業継続計画に盛り込むべき内容・項目を明確にしていること。 | | ○ | ○ |
| (6)事業再開計画に基き最新のソースプログラムの保存を確実にすること。 | | ○ | ○ |
| (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、組織体の長が承認すること。 | ○ | | |
| 1)C10<以下に共通>は、事業継続の方針に従い、事業継続の目的、範囲、実行体制および役割と責任、事業の優先順位、緊急時対応などの項目を明確化した事業継続計画を策定していること。 | | | |
| 2)事業遂行上の利害関係者を含めて、事業継続計画を立案する組織体制を明確にしていること。 | | | |
| 3)事業継続計画の立案の適切性をチェックするモニタリングや内部統制の仕組み(定期的な監査実施を含む)を構築していること。 | | | |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|---|-----|-----|-----|
| 4)組織体の長は、事業継続計画が、事業継続の方針に基づき、利害関係者を含む組織的体制で立案されていることを確認のうえ、承認していること。 | | | |
| (3)事業継続計画は、従業員の教育訓練の方針を明確にすること。 | ○ | | |
| 1)CIO<以下に共通>は、事業継続計画に関する従業員の教育訓練の方針および方針に基づき訓練計画を実施する主体(部門、責任者)を明確にしていること。 | | | |
| 2)従業員に対する教育訓練は、事業継続計画に基づき迅速かつ確実に事業継続にかかる手続きを実施することが目的であることを明確にしていること。 | | | |
| 3)事業継続計画における教育訓練方針の整合性や内容の適切性を確保していること。 | | | |
| 4)教育訓練方針に基づき、適切な教育訓練計画を立案すること。教育訓練の優先順位は、事業継続の優先順位と整合性を確保していること。 | | | |
| 5)教育訓練計画の実施責任者が、教育訓練計画を承認していること。 | | | |
| 6)教育訓練計画に基づき、定期的および必要に応じ、従業員訓練を実施していること。 | | | |
| 7)従業員の教育訓練の結果を、訓練計画や事業継続計画及び事業継続の方針に反映すること。 | | | |
| 8)事業継続計画の推進にかかる責任者および教育訓練の実施責任者は、教育訓練の実施結果とこれを踏まえた対処策の報告を受け、承認していること。 | | | |
| 9)従業員の教育訓練の適切性や十分性をチェックするために、モニタリングや内部統制の仕組み(定期的な監査実施を含む)を構築していること。 | | | |
| (4)事業継続計画は、関係各部に周知徹底すること。 | ○ | | |
| 1)CIO<以下に共通>は、事業継続計画の推進にかかる責任者は、事業継続計画の周知徹底の対象者、周知方法、頻度や時期、計画変更時の取り扱い手続きを明確にしていること。 | | | |
| 2)事業継続計画の策定時や内容変更時、責任者や関係者の交代時、企業の合併時、組織改組時、新規事業開始時など、適時に事業継続計画を周知徹底していること。 | | | |
| 3)事業継続計画を周知徹底の状況を、従業員の研修受講報告や各部署への説明会議事録等により、確認していること。 | | | |
| (5)事業継続計画は、必要に応じて見直すこと。 | ○ | | |
| 1)CIO<以下に共通>は、事業継続計画の見直し手順を、明文化していること。 | | | |
| 2)事業継続計画を見直す必要がある事態をあらかじめ整理のうえ、そうした事態が発生した場合には、遅滞なく計画見直しを指示ないし、実施していること。 | | | |
| 3)事業継続計画の見直しに伴い、計画を変更する場合には、変更内容、および変更の理由を明確にしていること。 | | | |
| 4)事業継続計画を変更する場合には、組織体の長に承認を受けていること。変更内容が軽微な場合には、あらかじめ定めた承認権限者が承認していること。 | | | |
| 5)事業継続計画の変更内容を関係者に周知徹底していること。周知徹底の結果について、報告を受けていること。 | | | |
| 6)事業継続計画の見直し責任者を明確にして、任務を割り当てていること。 | | | |
| 6. コンプライアンス | | | |
| (1)法令及び規範の管理体制を確立するとともに、管理責任者を定めること。 | ○ | ○ | ○ |
| 1)組織体の長は、法令および規範の所管部門を定めていること。 | ○ | | |
| 2)法令および規範の所管部門長は、自部門の管理責任者を定め、その職務および責任者の責務を明確に定めていること。 | ○ | | |
| 3)全社コンプライアンス管理責任者は、組織体における法令および規範の遵守状況、システム管理にかかる法令および規範への準拠状況について、モニタリングないし審査を実施していること。 | ○ | | |
| 4)発注側、受注(オフショア)側関係国双方の法令・規範の管理責任者を明確にしていること。 | ○ | ○ | ○ |
| (2)遵守すべき法令及び規範を識別し、関係者に教育及び周知徹底すること。 | ○ | ○ | ○ |
| 1)組織体の長は、組織体に適用される法令や規範を特定していること。 | ○ | | |
| 2)全社コンプライアンス管理責任者<次項と共通>は、組織体に適用される法令や規範のリストを、定期的及び必要に応じて見直していること。 | ○ | | |
| 3)前項で特定された、組織体に適用される法令や規範を、必要な関係者に周知徹底していること。 | ○ | | |
| 4)全社コンプライアンス管理責任者は、法令や規範を周知徹底するために必要な教育体制を構築し、教育の実施責任者を任命していること。 | ○ | | |
| 5)教育実施責任者は、教育計画を策定し、組織内の関係者に、必要な教育を実施していること。 | ○ | | |
| 6)全社コンプライアンス管理責任者は、教育結果報告等により前項の教育が適切に行われていることを確認していること。 | ○ | | |
| 7)知的財産権に関する取り決めを契約で正式に行っていること。 | | | |
| ①日本側 (あ)工業所有権著作権 (い)ソフトウェア著作権 | | ○ | ○ |
| ②中国側 (あ)中華人民共和国著作権法 | | | |
| 8)ソフトウェア特許の申請・取得などの方法を定めていること。 | | ○ | ○ |
| ①日本特許法 ②中華人民共和国特許法 | | | |
| 9)不正競争防止法を遵守すること。 | | ○ | ○ |
| 10)中国国内のオフショア関連企業(日本企業含む)は中華人民共和国技術輸出入管理条例を遵守していること。 | | ○ | ○ |
| 11)中国企業が外商投資商業領域管理弁法(新)の対象である場合、同法に準拠していること。 | | ○ | ○ |
| 12)ソフトウェア開発マネジメントシステム関連の標準的な基準に準拠していること。 (ISO/9001, CMM) | | ○ | ○ |
| 13)情報セキュリティマネジメントシステム関連の標準的な基準に準拠していること。 (ISO/IEC27001) | | ○ | ○ |
| (3)情報倫理規程を定め、関係者に教育及び周知徹底すること。 | ○ | ○ | ○ |
| 1)組織体の長は、情報管理に関し、業務上適用される法令、規範に基づき、組織体として遵守が求められる事項を、情報倫理規程として明文化していること。同規程の中で、規程の適用を受ける関係者、教育を含む運営体制、見直しルールを定めていること。 | ○ | | |
| 2)組織体の長は、情報倫理規定の内容について、定期的ないし必要に応じ、見直しを実施していること。 | ○ | | |
| 3)全社コンプライアンス管理責任者は、情報倫理規程の内容について、検証していること。 | ○ | | |
| 4)組織体の長は、情報倫理にかかる責任の所在を明確にし、また情報倫理規程の運営体制を確立していること。 | ○ | | |
| 5)全社コンプライアンス管理責任者<以下に共通>は前項の一環として、情報倫理規定を周知徹底するための教育体制を構築していること。 | ○ | | |
| 6)前項に基づき、関係者に必要な教育を実施し、周知徹底を図っていること。 | ○ | | |
| 7)前項の関係者には、組織体内の要員だけでなく、関係会社や協力会社等の要員も含めていること。 | ○ | | |
| 8)組織体の長は、周知徹底結果について報告を受け、結果を確認していること。 | ○ | | |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|---|-----|-----|-----|
| 9) 受注(オフショア)側における情報倫理規定を定め、関係者に教育・周知徹底していること。 | | ○ | ○ |
| (4) 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ること。 | ○ | | |
| 1) 組織体の長<以下に共通>は、個人情報保護法等関係法令に基づき、個人情報取扱方針(プライバシーポリシー)を定め、個人情報に関し、その取扱原則、組織体の義務を明示していること。 | | | |
| 2) 知的財産権保護の観点から、知的財産取扱方針を定め、知的財産権にかかる権利保護等の取扱いルールを明示していること。 | | | |
| 3) 外部へのデータ提供に関する方針を定め、提供に際して準拠すべき事項を明示していること。 | | | |
| 4) 上記の3方針各々について、その業務遂行に必要な、具体的な取扱基準、実施手順書等を整備していること。 | | | |
| 5) 上記の3方針各々について、定期的ないし必要に応じ、見直しを実施していること。 | | | |
| 6) 上記の3方針各々について、その内容を法令および規範の所管部門に検証させていること。 | | | |
| 7) 上記の3方針各々について、責任の所在を明確にし、またその運営体制を確立していること。 | | | |
| 8) 上記の3方針各々について、関係者に必要な教育を実施し、周知徹底を図っていること。 | | | |
| 9) 上記の3方針各々について、その運営責任者より周知徹底結果について報告を受け、結果を確認していること。 | | | |
| 10) 上記の3方針各々について、不適切に運営されることを防ぐため、モニタリングや内部統制の仕組み(定期的な監査実施を含む)を構築していること。 | | | |
| 11) 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に関する方針を定めていること。 | ○ | ○ | ○ |
| (5) 法令、規範及び情報倫理規程の遵守状況を評価し、改善のために必要な方策を講じること。 | ○ | ○ | |
| 1) 組織体の長は、法令および規範、情報倫理規程の遵守状況を定期的に点検するようルール化していること。 | | | |
| 2) 全社コンプライアンス管理責任者は、前項に基づき、定期的な点検を実施していること。 | | | |
| 3) 組織体の長は、点検結果について、報告を受けていること。 | | | |
| 4) 全社コンプライアンス管理責任者は、法令および規範、情報倫理規程の遵守状況を点検・評価の結果、改善が必要な場合には、責任部署を定めた上、改善計画を立案するなど、具体的な改善策を講じていること。 | | | |
| 5) 前項の改善計画については、経営層によりマネジメントレビューを実施し、その結果を組織体の長が承認していること。 | | | |
| 6) 全社コンプライアンス管理責任者は、改善計画の進捗状況は、定期的に責任部署の長および経営層に報告を行っていること。 | | | |
| 7) 組織体の長は、上記のPDCAサイクルが、不適切に運営されることを防ぐため、内部統制の仕組み(定期的な監査実施を含む)を構築し、適切に機能していること。 | | | |
| 1) 受注(オフショア)側における法令・規範及び情報倫理規定の遵守状況を評価し、改善のために必要な方針を講じていること。 | ○ | ○ | |
| II. 企画業務 | | | |
| 1. 開発計画 | | | |
| (1) 開発計画は、組織体の長が承認すること。 | ○ | ○ | |
| 1) 企画の責任者<以下に共通>は、開発計画立案ルールを策定していること。 | | | |
| 2) 開発計画立案ルールを明文化していること。 | | | |
| 3) 開発計画に対する組織体の長の承認を取り付けていること。 | | | |
| 4) 開発計画書を正式文書として、関係部門に配布していること。 | | | |
| 5) 開発計画に対する関係者の合意を取り付けていること。 | | | |
| 6) 開発計画を定期的に見直ししていること。 | | | |
| (2) 開発計画は、全体最適化計画との整合性を考慮して策定すること。 | ○ | ○ | |
| 1) 企画の責任者は、全体最適化計画が存在することを確認していること。 | ○ | | |
| 2) 開発計画を全体最適化計画に基づいて作成させていること。 | ○ | | |
| 3) 開発計画と全体最適化計画との整合性をレビューしていること。 | ○ | | |
| 4) 企画担当者<以下に共通>は、開発計画と関連する他の情報システムとの関連を明確にしていること。 | ○ | | |
| 5) 全体最適化計画と相違している事項について、理由を明確にし、関係者の合意を取得していること。 | ○ | | |
| 6) 開発計画全体においてオフショア開発を考慮しているか確認すること。 | ○ | ○ | |
| 7) オフショア開発を考慮した開発マネジメントサイクル(PCDA)が形成されていること。 | ○ | ○ | |
| 8) オフショア開発を含む開発計画が各組織体の長によって承認されていること。 | ○ | ○ | |
| 9) オフショア開発計画はISO/IEC12207(JIS X 0160)に準拠していること。 | ○ | ○ | ○ |
| (3) 開発計画は、目的、対象業務、費用、スケジュール、開発体制、投資効果等を明確にすること。 | ○ | ○ | ○ |
| 1) 企画担当者<以下に共通>は、開発計画の目的、対象業務、費用、スケジュール、開発体制、投資対効果等を明確にしていること。 | ○ | | |
| 2) 開発する情報システムの目的及び対象業務が、全体最適化計画と整合しているかを確認していること。 | ○ | | |
| 3) 開発効果の算定において、全体最適化計画で定めた方法を使用していること。 | ○ | | |
| 4) 開発費用の算出根拠を明確にしていること。 | ○ | | |
| 5) 開発費用の算出が合理的であることを確認していること。 | ○ | | |
| 6) 開発計画の投資効果の算出根拠を明確にしていること。 | ○ | | |
| 7) 開発計画に採算性があることを確認していること。 | ○ | | |
| 8) 開発スケジュールの妥当性を確認していること。 | ○ | | |
| 9) 開発体制の妥当性を確認していること。 | ○ | | |
| 10) 開発計画を関係者に配布し説明していること。 | ○ | | |
| 11) 企画責任者<以下同様>は開発の目的を明確にしていると同時に、オフショア会社を活用する目的も明確にしていること。 | ○ | ○ | |
| 12) オフショア会社に発注する対象業務は明確になっていること。 | | ○ | |
| 13) オフショア会社の発注に関する費用は明確になっていること。 | | ○ | ○ |
| 14) ソフトウェア規模の見積もり方法を定め、以下の項目を明確にしていること。 ①要求機能 ②使用言語 ③定量的な規模見積もり方法(ファンクションポイント)等 ④開発期間と納期⑤品質レベル(安定性に関する条件など) ⑥ドキュメント条件(上流工程でのドキュメント、保守マニュアルなど付帯するドキュメントなどの条件、ソースへのコメント記入条件など) ⑦ブリッジSE配置、⑧総合費用 | | ○ | ○ |
| 15) 外国一日本間出張費用その他外国に関わる雑費用を含んでいること。 | | ○ | ○ |
| 16) オフショア会社との打合せは、頻度や日取りの他、外国現地で実施するケース、日本に集合して実施するケース、会議電話等で行うケース、メール等で行うケースなど、具体的かつ詳細に定められていること。 | | ○ | ○ |
| 17) 開発体制は開発全体の体制と、そこに組み込まれるオフショア会社の位置、役割が明確になっていること。 | | ○ | ○ |
| 18) オフショア会社内の体制について、特に元請側との連携体制、品質管理体制、進捗管理体制、問題処理体制などについて責任者の氏名は明確になっていること。 | | ○ | ○ |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|---|-----|-----|-----|
| 19)ブリッジSEの責任と権限(役割)を参考図(ブリッジSEの機能)を参照して明確に定義すること。 | | ○ | ○ |
| 20)オフショア会社を活用する投資効果に関して評価していること。 | ○ | ○ | |
| 21)開発に関する固有の用語の定義を明確にすること。 | | ○ | ○ |
| (4) 開発計画は、関係者の教育及び訓練計画を明確にすること。 | | | |
| 1) 企画担当者<以下に共通>は、情報システムの開発、運用及び保守に必要な教育及び訓練の内容を明確にしていること。 | | | |
| 2) 教育及び訓練の対象に漏れがないことを確認していること。 | | | |
| 3) 教育及び訓練の内容に沿った実施計画を明確にしていること。 | | | |
| 4) 教育訓練の実施計画が妥当であることを確認していること。 | | | |
| 5) 教育及び訓練に必要な資源と費用を明確にしていること。 | | | |
| 6) 教育及び訓練のインストラクターの目処をつけていること。 | | | |
| 7) 資源と費用が妥当であることを確認していること。 | | | |
| 8) 元請側の開発責任者やその他直接関係者にオフショア当該国に関して理解を深めるための教育や研修を行っていること。 | | ○ | |
| 9) 受注(オフショア)側の責任者及びブリッジSEと主だった従事者は日本企業の業務の進め方に関する教育を受けていること。 | | | ○ |
| 10) 受注(オフショア)会社に発注する業務に関連して特に必要な教育・訓練がないか検討していること。 | | ○ | |
| 11) 必要な教育・訓練がある場合、訓練内容と計画コスト負担、セキュリティ・著作権などの条件が明確になっていること。 | | ○ | ○ |
| (5) 開発計画は、ユーザ部門及び情報システム部門の役割を明確にすること。 | ○ | ○ | ○ |
| 1) 企画担当者<以下に共通>は、開発、運用及び保守業務におけるユーザ部門と情報システム部門の役割分担を明確にしていること。 | ○ | | |
| 2) 役割が必要かつ十分であることを確認していること。 | ○ | | |
| 3) 開発する情報システムの特性及びユーザ組織の特性を考慮して役割分担を検討していること。 | ○ | | |
| 4) 役割の振り分けが合理的かつ妥当であることを確認していること。 | ○ | | |
| 5) 開発の責任者<以下に共通>は、役割分担をユーザ及び情報システムの両部門の責任者に承認を得たうえで、自部門内に周知徹底していること。 | ○ | | |
| 6) 役割分担を組織及び情報システムの変更に伴い、見直していること。 | ○ | | |
| 7) 企画責任者は<以下同様>開発計画で、ユーザ部門と情報システム部門の役割分担を明確にし、オフショアに関する内容がある場合は受注(オフショア)側への連絡ルートとの関係についても同時に明確にすること。 | | ○ | ○ |
| 8) 上流工程における受注(オフショア)側の作成ドキュメントでユーザ部門に密接に関係する場合、具体的なアウトプット条件を予め詳細に明確にすること。 | | ○ | ○ |
| 9) 受注(オフショア)側に関係する部分におけるユーザ部門からの開発途中での仕様変更や、暫定仕様の場合のその後の仕様確定の場合の周知ルールや費用などの扱いを予め明確にしていること。 | ○ | ○ | ○ |
| (6) 開発計画は、開発、運用及び保守の費用の算出根拠を明確にすること。 | ○ | ○ | ○ |
| 1) 企画担当者<以下に共通>は、開発計画に開発、運用及び保守業務の費用項目を網羅していること。 | ○ | | |
| 2) 費用の算出根拠を明確にし、関係者に承認を取り付けていること。 | ○ | | |
| 3) 費用の算出根拠が合理的でかつ妥当であることを確認していること。 | ○ | | |
| 4) 費用には余裕率を見込んであることを確認していること。 | ○ | | |
| 5) 全体最適化計画の情報化投資方針と相違する費用項目及び費用について、相違の理由を明確にしていること。 | ○ | | |
| 6) オフショアに関係する費用部分を明確にすること。 | | ○ | ○ |
| (7) 開発計画は、システムライフを設定する条件を明確にすること。 | ○ | | |
| 1) 企画担当者<以下に共通>は、設定条件に業務の変化及び技術的制約を考慮していること。 | ○ | | |
| 2) システムライフの設定条件を構成する評価項目に漏れがないことを確認していること。 | ○ | | |
| 3) システムライフの設定条件の根拠を明確にしていること。 | ○ | | |
| 4) システムライフの設定条件を定量的及び定性的評価の両側面から明確にしていること。 | ○ | | |
| 5) 設定条件の前提が合理的でかつ妥当であることを確認していること。 | ○ | | |
| 6) システムライフの設定条件について、関係者の合意を取り付けていること。 | ○ | | |
| 7) システムライフに於けるオフショア関係部分を明確にすること。 | ○ | ○ | ○ |
| (8) 開発計画の策定に当たっては、システム特性及び開発の規模を考慮して形態及び開発方法を決定すること。 | ○ | ○ | ○ |
| 1) 企画担当者<以下に共通>は、開発するシステムはの全体最適化計画における位置づけを明確にしていること。 | ○ | | |
| 2) 情報システムの目的、機能、システム特性及び開発規模を整理していること。 | ○ | | |
| 3) 情報システムの目的、昨日、システム特性及び開発規模の記述が必要かつ十分な詳細度を持っていることを確認していること。 | ○ | | |
| 4) 開発形態及び開発方法の選定基準を明確にしていること。 | ○ | | |
| 5) 選定基準が合理的でかつ妥当であることを確認していること。 | ○ | | |
| 6) 開発形態及び開発方法を開発の規模、開発期間及びシステム特性を考慮して決めていること。 | ○ | | |
| 7) 開発形態及び開発方法を開発要員の能力及び経験を考慮して決定していること。 | ○ | | |
| 8) 開発形態及び開発方法を保守業務を考慮して決定していること。 | ○ | | |
| 9) 企画の責任者は、開発形態及び開発方法が他の情報システムと整合していること。を確認していること。 | ○ | | |
| 10) 開発方式がスパイラル設計方式の場合とウォーターフォール形開発のそれぞれに、ふさわしい開発計画を立てること。(受注(オフショア)側にはプロトタイプ作成の候補、タイミング、繰り返し限度、統合化計画、品質管理計画、要員計画、外注管理計画など詳細な計画を提案すること。) | | ○ | ○ |
| 11) プロトタイプ作成をオフショア受注側が行う場合、迅速な開発の要求に応じるためにソフトウェアのネットワークを介した送受信が行える環境を整備すること。 | | ○ | ○ |
| 12) 上記の場合、技術情報送受に関する当該国の法的制約がないことを確認すること。 | | ○ | ○ |
| 13) スパイラル設計方式の場合、連絡密度が高くなるため、受注(オフショア)側とのコミュニケーション方法を確認すること。 | | ○ | ○ |
| 14) 開発対象がネットワークシステムの場合、ノード単体の開発の後、ネットワーク接続試験が必要であるが、関係システム、関係組織間の試験環境を考慮すること(受注(オフショア)側) | ○ | | ○ |
| 15) 大規模システムの接続試験や総合試験の場合多くの会社が運動するため受注(オフショア)側を含む関係組織のコミュニケーション方法を十分考慮すること。 | ○ | ○ | ○ |
| 16) 計画はオフショア対象国の習慣(休日等)を考慮すること。 | | ○ | ○ |
| (9) 開発計画の策定に当たっては、情報システムの目的を達成する実現可能な代替案を作成 | ○ | | |
| 1) 企画担当者<以下に共通>は、情報システムの目的を達成する複数のシステム案を作成していること。 | ○ | | |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|---|-----|-----|-----|
| 2) 代替案は複数あり、かつ考えられる全てを網羅していることを確認していること。 | ○ | | |
| 3) 情報システム案を比較する評価項目を明確にしていること。 | ○ | | |
| 4) 評価項目が合理的でかつ妥当であることを確認していること。 | ○ | | |
| 5) 評価項目を事前に決めていること。 | ○ | | |
| 6) システム案の検討に関係者を参画させていること。 | ○ | | |
| 7) 最終案の選定理由を明確にしていること。 | ○ | | |
| 8) 最終案に対する運用及び保守の責任者の承認を取っていること。 | ○ | | |
| 9) 最終案に至る検討結果を記録していること。 | ○ | | |
| 2. 分析 | | | |
| (1) 開発計画に基づいた要求定義は、ユーザ、開発、運用及び保守の責任者が承認すること。 | ○ | ○ | ○ |
| 1) 開発の責任者は、システム分析及び要求定義の手順を明確にしていること。 | ○ | | |
| 2) 開発担当者<以下に共通>は、開発計画に基づいてシステム開発を行っていること。 | ○ | | |
| 3) 関係者を参画させて要求定義の分析を行っていること。 | ○ | | |
| 4) ユーザ、運用及び保守の責任者を明確にした上で、関係責任者の承認を取っていること。 | ○ | | |
| 5) 発注者・ブリッジSE(外国側、日本側)の役割・責任分担を明確にすること。 | | ○ | ○ |
| 6) 発注側と受注(オフショア)側の責任者の承認をすること。 | | ○ | ○ |
| 7) 仕様の変更に関する取決めは明確にすること。(仕様記述レベルと製造側の自由度のレベルの取決めは、発注側、受注(オフショア)側で明確にすること) | ○ | ○ | ○ |
| 8) 仕様の打ち合わせ計画は明確に計画され、かつ実行すること(発注側の問題) | ○ | ○ | ○ |
| (2) ユーザニーズの調査は、対象、範囲及び方法を明確にすること。 | ○ | ○ | ○ |
| 1) 開発担当者<以下に共通>は、開発の対象、範囲及び方法を事前にユーザと調整し、明確にしていること。 | ○ | | |
| 2) 参画するユーザ部門には漏れがないことを確認していること。 | ○ | | |
| 3) 開発の対象、範囲及び方法がユーザニーズを適切に把握できるものであることを確認していること。 | ○ | | |
| 4) ユーザニーズの調査を定められた対象、範囲及び方法に基づいて行っていること。 | ○ | | |
| 5) ユーザニーズ内容を受注(オフショア)側に伝えることが好ましい(背景の明確化のため)。 | ○ | ○ | ○ |
| (3) 実務に精通しているユーザ、開発、運用及び保守の担当者が参画して現状分析を行うこと。 | ○ | ○ | ○ |
| 1) 開発担当者<以下に共通>は、現状分析を行うに際し、開発対象業務及び現行情報システムに精通したユーザ、開発、運用及び保守の担当者を参画させていること。 | ○ | | |
| 2) ユーザの参画者が業務に精通していて、かつ部門を代表できるスキルを持っていることを確認していること。 | ○ | | |
| 3) ユーザの参画者に自らの役割を認識しているかを確認していること。 | ○ | | |
| 4) 現状分析を行うに際し、現行情報システムの機能、規模等を設定するために必要な情報を収集していること。 | ○ | | |
| 5) 分析結果を将来展望を考慮して評価していること。 | ○ | | |
| 6) 分析結果を記録していること。 | ○ | | |
| 7) 仕様は詳細に且つ明確に定義すること。(発注「日本」側の記述方法及び記述内容の問題と受注(オフショア)側での確認の問題) a)外部要求仕様、内部構造仕様、内部詳細仕様などの全体構成及び内容を明確にすること。 b)外部要求仕様には、機能条件、性能条件、信頼性条件、安定性条件、品質条件、コスト条件、納入期日条件、維持管理条件、セキュリティ条件、格別条件を明瞭にすること。 | ○ | ○ | ○ |
| 8) 機能仕様条件は詳細に明文化されていること。 例1: 適用プロトコル仕様で、標準で定められず、任意となっている条件(例えば、具体的なタイミング条件など)は別途仕様書で定めているか。 例2: 画面に関する機能のルール、デフォルト表示、SORT順、表示項目のSORT機能、値をセットする援助機能 等。 | | ○ | ○ |
| (4) ユーザニーズは文書化し、ユーザ部門が確認すること。 | ○ | ○ | ○ |
| 1) 開発担当者<以下に共通>は、ユーザニーズの開発結果を記録し、文書として整理していること。 | ○ | | |
| 2) 調査結果に調査の対象、範囲及び方法を記録していること。 | ○ | | |
| 3) 十分な内容と詳細度を持った文書としていること。 | ○ | | |
| 4) 調査結果を、全ユーザに説明していること。 | ○ | | |
| 5) 調査結果を記録し、全ユーザの承認を取っていること。 | ○ | | |
| 7) ユーザニーズの開発結果は受注(オフショア)側に示すことが好ましい(背景の明確化のため)。 | ○ | ○ | ○ |
| (5) 情報システムの導入に伴って発生する可能性のあるリスク分析を実施すること。 | ○ | | |
| 1) 開発担当者<以下に共通>は、リスク分析の対象を明確にしていること。 | ○ | | |
| 2) リスクを漏れなく拾いだしていること。 | ○ | | |
| 3) 個々のリスクの発生頻度、影響度及び範囲を明確にしていること。 | ○ | | |
| 4) リスクの種類に応じて、損害の内容及び損害額を算出していること。 | ○ | | |
| 5) リスクの種類に応じて、リスク軽減策を検討していること。 | ○ | | |
| 6) リスク分析、対策が妥当であることを確認していること。 | ○ | | |
| 7) リスクの対策に対し関係者の承認を取り、関係部門に周知徹底していること。 | ○ | | |
| (6) 情報システムの導入によって影響を受ける業務、管理体制、諸規程等は、見直し等の検討を行うこと。 | ○ | | |
| 1) 開発担当者<以下に共通>は、影響を受ける業務、管理体制、諸規定等の範囲を明確にしていること。 | ○ | | |
| 2) 業務、管理体制、諸規程類に漏れがないかを確認していること。 | ○ | | |
| 3) 影響を受ける関係者を参画させて、見直し等の検討を行っていること。 | ○ | | |
| 4) 影響の程度及び範囲を明確にし、対応策を講じていること。 | ○ | | |
| 5) 検討結果を文書化していること。 | ○ | | |
| 6) 関係者から対応策に対する承認を取り付けていること。 | ○ | | |
| (7) 情報システムの導入効果の定量的及び定性的評価を行うこと。 | ○ | | |
| 1) 開発担当者<以下に共通>は、情報システムの実現によって得られる効果を明確にしていること。 | ○ | | |
| 2) 評価項目及び評価方法を明確にしていること。 | ○ | | |
| 3) 定量的及び定性的評価を実施していること。 | ○ | | |
| 4) 定量的な評価において、算出項目が必要かつ十分であること。 | ○ | | |
| 5) 計算ロジック及び前提条件が合理的でかつ妥当である方式を用いて計算していること。 | ○ | | |
| 6) 費用対効果を分析していること。 | ○ | | |
| 7) 評価結果に対する合意を関係者から取っていること。 | ○ | | |
| 8) 開発計画と相違する評価結果については、理由を明確にしていること。 | ○ | | |
| 9) 開発計画と相違する評価結果については、合理的でかつ妥当な理由で説明していること。 | ○ | | |
| (8) パッケージソフトウェアの使用に当たっては、ユーザニーズとの適合性を検討すること。 | ○ | | |
| 1) 開発担当者<以下に共通>は、情報システムの処理におけるユーザニーズを整理していること。 | ○ | | |
| 2) 候補となりうるパッケージソフトウェアを漏れなく挙げていること。 | ○ | | |
| 3) 評価・選定基準を事前に確定していること。 | ○ | | |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|---|-----|-----|-----|
| 4) ユーザーニーズに対するパッケージソフトウェアの対応状況を整理し、評価していること。 | ○ | | |
| 5) 関係者を集めて適合性の評価を行わせていること。 | ○ | | |
| 6) 適合性の評価結果に対するユーザー部門の責任者の承認を取り付けていること。 | ○ | | |
| 3. 調達 | | | |
| (1) 調達の要求事項は、開発計画及びユーザーニーズに基づき作成し、ユーザ、開発、運用及び保守の責任者が承認すること。 | ○ | ○ | |
| 1) 企画の責任者は、調達する資源を明確にしていること。 | ○ | | |
| 2) 企画の担当者<以下に共通>は、調達する資源を開発計画及びユーザーニーズに基づいて作成していること。 | ○ | | |
| 3) 調達する資源の種類、数量を明確にしていること。 | ○ | | |
| 4) 調達する資源の条件、必要事項を明確にしていること。 | ○ | | |
| 5) 調達の要求事項をユーザ、開発、運用及び保守の責任者の承認人を取り付けていること。 | ○ | | |
| 6) オフショア開発を行う場合海外への発注を容認することを関係責任者は承認すること。 | ○ | ○ | |
| (2) ソフトウェア、ハードウェア及びネットワークは、調達の要求事項を基に選択すること。 | ○ | | |
| 1) 企画の責任者は、開発計画及びユーザーニーズに基づく情報システムの実現に必要なソフトウェア、ハードウェア、ネットワーク等を明確にして文書化させていること。 | ○ | | |
| 2) 企画の担当者<以下に共通>は、機能、性能、費用、サービス、保守体制等を検討し、ソフトウェア、ハードウェア、ネットワーク等を選択していること。 | ○ | | |
| 3) 評価・選択基準を事前に確定し、企画・開発・保守の責任者の承認を取り付けていること。 | ○ | | |
| 4) 他の関連する情報システムとのインタフェース及び拡張性を考慮し、ソフトウェア、ハードウェア、ネットワーク等を選択していること。 | ○ | | |
| 5) 合理的かつ妥当なロジックで評価・選択をしていること。 | ○ | | |
| (3) 開発を遂行するために必要な要員、予算、設備、期間等を確保すること。 | ○ | ○ | ○ |
| 1) 企画の責任者<以下に共通>は、システム分析に基づき、要員、予算、設備、期間等を確保し、情報システム部門責任者の承認を取り付けていること。 | ○ | | |
| 2) 要員、予算、設備等の投入時期、期間、規模等を考慮していること。 | ○ | | |
| 3) 要員および設備の要求は要求事項を明確にしていること。 | ○ | | |
| 4) 能力及び経験等を考慮し、要員を確保していること。 | ○ | | |
| 5) 要員、設備には数量を確定していること。 | ○ | | |
| 6) 受注(オフショア)側要員の質、量とも満足していることを確認すること。 | | ○ | ○ |
| (4) 要員に必要なスキルを明確にすること。 | ○ | ○ | |
| 1) 企画の責任者<以下に共通>は、開発、運用及び保守業務の各段階において、必要となる作業内容を明確にしていること。 | ○ | | |
| 2) それぞれの作業内容に必要な要員のスキルを明確にしていること。 | ○ | | |
| 3) スキル別の量を明確にしていること。 | ○ | | |
| 4) 必要となる時期を明確にしていること。 | ○ | | |
| 5) 必要なスキルを分野及びスキルの段階を設定して明確にしていること。 | ○ | | |
| 6) 必要なスキルを自情報システム部門責任者内から調達するか、外部から調達するかを明確にし | ○ | | |
| 7) 元請側及び受注(オフショア)側の必要なスキルを明確にすること。 | | ○ | ○ |
| (5) ソフトウェア、ハードウェア及びネットワークの調達はルールに従って実施すること。 | ○ | | |
| 1) 企画の責任者<以下に共通>は、開発に必要な資源の調達部門を定めていること。 | ○ | | |
| 2) 調達のルールを定めていること。 | ○ | | |
| 3) 調達のルールは内部牽制機能が働く内容としていること。 | ○ | | |
| 4) 調達のルールに対する関連部門の承認を取り付けていること。 | ○ | | |
| 5) 調達のルールに沿って調達が行われていることを定期的に確認していること。 | ○ | | |
| 6) 調達のルールを適宜見直していること。 | ○ | | |
| (6) 調達した資源は、ルールに従って管理すること。 | ○ | | |
| 1) 企画の責任者<以下に共通>は、調達する資源を明確にしていること。 | ○ | | |
| 2) 調達した資源を管理するルールを制定し、ルールに従って管理していること。 | ○ | | |
| 3) 調達した資源を漏れなく台帳に登録していること。 | ○ | | |
| 4) 調達品の棚卸しを定期的実施していること。 | ○ | | |
| 5) 調達した資源の活用状況を評価し、有効活用を図っていること。 | ○ | | |
| 6) ルールに従って管理していることを定期的に確認していること。 | ○ | | |
| 7) 管理ルールを適宜見直していること。 | ○ | | |
| III. 開発業務 | | | |
| 1. 開発手順 | | | |
| (1) 開発手順は、開発の責任者が承認すること。 | ○ | ○ | ○ |
| 1) 情報システム部門責任者は、開発の責任者を明確にしていること。 | ○ | | |
| 2) 情報システム部門責任者は、開発の責任者の役割と権限を明確にしていること。 | ○ | | |
| 3) 情報システム部門責任者は、開発計画及び開発方法を明確にしていること。 | ○ | | |
| 4) 開発方法としてはウォーターフォールまたはスパイラル開発など具体的な方法及び付随する条件を定め受注(オフショア)側と確認をとること。 | | | |
| 5) 開発の責任者は、開発計画、開発方法に基づき、開発手順を定めていること。 | ○ | | |
| 6) 開発の責任者は、開発手順を承認していること。 | ○ | | |
| 7) 開発の責任者は、開発手順を関係者に周知徹底していること。 | ○ | | |
| 8) 開発の責任者はブリッジSEを任命すること。(注:ブリッジSEとはオフショア開発に関する受発注間において相互調整業務を行う技術者であり通訳・翻訳能力を有するシステム技術者) | | ○ | ○ |
| 9) 開発の責任者は発注者・ブリッジSE(受発注双方)の連携手順を明確にすること。 | | ○ | ○ |
| 10) 発注者・ブリッジSE(国際取引側、日本側)の相互承認を行うこと。 | | ○ | ○ |
| 11) 発注側と受注(オフショア)側での確認方法を含む開発手順を定義すること | | ○ | ○ |
| (2) 開発手順は、開発方法に基づいて作成すること。 | ○ | ○ | ○ |
| 1) 開発の責任者<以下、本項に共通>は、開発手順を明文化していること。 | ○ | | |
| 2) 開発方法に準拠して、開発手順を定めていること。 | ○ | | |
| 3) 開発作業をする上で必要な要件を明確にしていること。 | ○ | | |
| 4) システム開発手順を明文化していること。 | ○ | | |
| 5) システム開発手順書に開発作業を遂行する上で必要な要件を盛り込んでいること。 | ○ | | |
| 6) 開発責任者は<以下同様>開発方法として、ウォーターフォールモデルと、スパイラルモデルがあるが、それぞれのモデルに適した開発手順を定めること。 | | ○ | |
| 7) 発注元に開発手順に関する方針が有る場合、受注(オフショア)側がそれに準拠することに同意すること。 | | ○ | ○ |
| (3) 開発手順は、開発の規模、システム特性等を考慮して決定すること。 | ○ | ○ | ○ |
| 1) 開発の責任者<以下、本項に共通>は、開発手順の決定理由を明確にしていること。 | ○ | | |
| 2) システム開発手順に盛り込むべき作業項目を明確にしていること。 | ○ | | |
| 3) システム開発手順書に盛り込むべき作業項目を網羅していること。 | ○ | | |
| 4) システム開発手順書に無理及び無駄のない作業の流れ、日程等を記載していること。 | ○ | | |
| 5) 開発上の重点管理項目を明確にしていること。 | ○ | | |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|---|-----|-----|-----|
| 6)開発責任者は<以下同様>ターゲットシステムの性格(ネットワークシステム、業務アプリケーションシステム、データベースシステム、端末、webシステムなど)の特徴に対応した開発方法があるが、それに基づいた開発手順とし、受注(オフショア)側と合意すること。 | | ○ | ○ |
| 7)システムのOS、使用言語、日本語を用いた開発環境に対応した開発手順とすること。 | | ○ | ○ |
| 8)大規模な場合の開発順序、小規模な場合の簡略化など、開発規模に応じた開発手順とすること。 | | ○ | ○ |
| 9)開発の工程(基本設計、詳細設計、コーディング、単体試験、結合試験、総合試験など)を明確にして受注(オフショア)側と合意すること。 | | ○ | ○ |
| 10)開発の工程に対応する開発体制、人数、スキルを受注(オフショア)側も含めて明確にすること。 | | ○ | ○ |
| 11)各工程での品質管理、進捗管理などの報告及び打ち合わせ方法、周期、体制、開催場所、使用言語など詳細な計画を相互に確認すること。 | ○ | ○ | ○ |
| 12)仕様変更の手順を明確にしておくこと。 | ○ | ○ | ○ |
| 13)ハードとソフトの双方に関係する問題や複数社に跨る問題などの対応手順を明確にしておくこと。 | ○ | ○ | ○ |
| 14)納入に必要なドキュメントの種類、形式、時期を明確にし契約内容に含めること。 | ○ | ○ | ○ |
| (4)開発時のリスクを評価し、必要な対策を講じること。 | ○ | ○ | ○ |
| 1)開発の責任者は、開発プロセスの工程の機能を明確にしていること。 | ○ | | |
| 2)開発の責任者は、各工程単位に作業を進める上でのリスクを想定していること。 | ○ | | |
| 3)開発の責任者は、リスクの評価を行い、対策を検討し、重要度の順番を付けていること。 | ○ | | |
| 4)開発の責任者及びユーザの代表者は、リスクの洗い出しに参加していること。 | ○ | | |
| 5)開発の責任者は、主要なリスクを関係者の間での共通認識としていること。 | ○ | | |
| 6)開発の責任者は、2次リスク、残存リスクについても評価し、対策を講じていること。 | ○ | | |
| 7)外部仕様の不完全性のリスクを軽減するため、開発責任者は<以下同様>外部仕様及要求事項を含めて網羅的に完成しているかについてレビューする計画、及び計画に基づいた実行を行うこと。 | ○ | ○ | ○ |
| 8)内部設計仕様不完全性のリスクを回避するためは外部仕様を満足していることをレビューする計画、及び計画に基づいた実行を行うこと。レビューにはブリッジSE及び受注側の各要員は参加すること。 | ○ | ○ | ○ |
| 9)製造段階でのリスクを軽減するため、製造・コーディングの工程の節目でレビューする計画、及び計画に基づいた実行を行うこと。レビューにはブリッジSE及び受注側の各要員は参加すること。 | | ○ | ○ |
| 10)試験不完全のリスクを軽減するため、結合試験、総合試験は、内部設計仕様や外部設計仕様を試験できるよう、試験項目を体系的に作成し、妥当性についてレビューする計画、及び、計画に基づいた実行をすること。レビューにはブリッジSE及び受注側の各要員が参加すること。 | | ○ | ○ |
| 11)ブリッジSEは全ての工程においてリスクマネジメントのためのモニタリングを行うこと。 | | | |
| 12)その他、オフショアによる開発時のリスク(脅威と脆弱性)について検討し、必要な対策を講じること。 | | ○ | ○ |
| 13)開発計画立案に際しては中国の場合、日中間の国情に関わる特異日(満州事変、上海事変、盧溝橋事件、国恥記念日など)に配慮すること。サービス開始などのイベントは避けること。 | ○ | ○ | |
| 2. システム設計 | | | |
| (1)システム設計書は、ユーザ、開発、運用及び保守の責任者が承認すること。 | ○ | ○ | ○ |
| 1)情報システム部門責任者は、システム開発におけるユーザ、開発、運用及び保守の責任者の役割と権限を明確に定めていること。 | ○ | | |
| 2)情報システム部門責任者は、ユーザ、開発、運用及び保守の責任者を明確に定めていること。 | ○ | | |
| 3)ユーザ、開発、運用及び保守の責任者は、システム設計書を承認していること。 | ○ | | |
| 4)ユーザ、開発、運用及び保守の責任者は、関係者にシステム設計書を周知徹底していること。 | ○ | | |
| 5)開発の担当者は、開発手順及びシステム設計マニュアルに基づいてシステム設計書を作成していること。 | ○ | | |
| 6)開発の担当者は、必要な内容をすべて網羅してシステム設計書を作成していること。 | ○ | | |
| 7)開発の担当者は、システム設計書と要求定義との整合性を確認していること。 | ○ | | |
| 8)情報システム部門責任者は、システム設計書を作成することを定めていること。 | ○ | | |
| 9)開発の責任者は、システム設計のレビュー体制を確立していること。 | ○ | | |
| 10)情報システム部門責任者は、システム設計のレビュー責任者およびその役割と権限を明確に定 | ○ | | |
| 11)開発の責任者は、システム設計のレビューにユーザ部門の代表者を参加させていること。 | ○ | | |
| 12)正式な承認を得た仕様書(外部仕様書)に基づいて設計を開始すること。 | | ○ | ○ |
| 13)発注側、元請側、受注(オフショア)側(ブリッジSEを含む)の責任者が承認すること。 | | ○ | ○ |
| 14)設計書の種類を明確にすること。(例:ユースケース図、クラス図、アクティビティ図、概要設計書、詳細設計書、IPOチャートその他) | | ○ | ○ |
| (2)運用及び保守の基本方針を定めて設計すること。 | ○ | ○ | ○ |
| 1)開発の担当者は、有人・無人、24時間連続・定期保守、事業継続計画との整合から、システム運用条件への反映(バックアップなど)、運用体制などの外部条件から運用の基本方針を定め、運用案を検討していること。 | ○ | ○ | |
| 2)開発の責任者は、運用案のレビューには運用部門の代表者も参加させていること。 | ○ | | |
| 3)開発の担当者は、保守の基本方針を定め、保守手順を検討していること。 | ○ | | |
| 4)開発の責任者は、保守手順のレビューには保守部門の代表者を参加させていること。 | ○ | | |
| 5)開発の担当者は、運用及び保守の基本方針を考慮してシステム設計していること。 | ○ | | |
| 6)システムの障害に対する処理の内、システムで自動的に復旧するものと、運用や保守で手動で対応するものを明確にして設計すること。 | | | |
| 7)運用設計条件は製造工程に入る前に必要に応じて受注(オフショア)側を含めてレビューすることが好ましい。 | ○ | ○ | ○ |
| 8)レビュー計画に基づいてレビューすること。 | | ○ | ○ |
| 9)レビュー結果は記録され、誤りは修正し、開発方法自体の改善が必要であれば改善すること。 | | ○ | ○ |
| 10)レビュー結果の効果は確認すること。 | | ○ | ○ |
| (3)入出力画面、入出力帳票等はユーザの利便性を考慮して設計すること。 | ○ | ○ | ○ |
| 1)開発の担当者は、開発方針及びシステム設計マニュアルに基づいて入出力帳票、入出力画面等を設計していること。 | ○ | | |
| 2)開発の担当者は、入出力帳票、入出力画面の設計における考慮点を明確にしていること。 | ○ | | |
| 3)開発の担当者は、入出力帳票、入出力画面の設計する際にユーザの利便性を考慮していること。 | ○ | | |
| 4)開発の担当者は、入出力帳票、入出力画面およびコードをシステム設計書に記載していること。 | ○ | | |
| 5)開発の責任者は、入出力帳票設計のレビューにユーザ部門の代表者が参加させていること。 | ○ | | |
| 6)開発の責任者は、入出力画面設計のレビューにユーザ部門の代表者が参加させていること。 | ○ | | |
| 7)開発の責任者は、コード設計のレビューにユーザ部門の代表者が参加させていること。 | ○ | | |
| 8)入出力画面の詳細な仕様を明確にすること。例:画面レイアウトルール、色使い・ボタン位置・画面遷移等 | ○ | ○ | ○ |
| 9)発注仕様書に画面設計条件を明記すること。 | ○ | ○ | ○ |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|---|-----|-----|-----|
| 10) 受注(オフショア)側は中間段階で画面イメージを提示し発注側にレビューすること。 | ○ | ○ | ○ |
| 11) エラーメッセージ画面内容をレビューすること。 | ○ | ○ | ○ |
| 12) 業務固有の用語は予め定義しておくこと。 | ○ | ○ | ○ |
| (4) データベースは、業務の内容及びシステム特性に応じて設計すること。 | ○ | ○ | ○ |
| 1) 開発の担当者<以下、本項に共通>は、開発方針及びシステム設計マニュアルに基づいてデータベース設計していること。 | ○ | | |
| 2) データベース設計における考慮点を明確にしていること。 | ○ | | |
| 3) 選定したデータモデルの種類と特徴を明確化していること。 | ○ | | |
| 4) 採用するDBMS(Data Base Management System)が十分な機能及び性能を有していることを確認していること。 | ○ | | |
| 5) 業務の特性に基づいて、データベースの利用形態を明確にしていること。 | ○ | | |
| 6) システムライフにおけるデータ量の増加を考慮してデータベース設計していること。 | ○ | | |
| 7) データベース設計の結果及び検討経緯を明文化していること。 | ○ | | |
| 8) 業務の内容から求められるデータベースの設計条件(リアルタイム性・容量等を含む)は詳細にかつ明確に定めること。 | ○ | ○ | ○ |
| 9) 適切なデータモデルを構築し、データベース設計を行うこと。 | | ○ | ○ |
| 10) 用語として「出来高」「売り上げ」などの時点で確定するか、や「通番」「区分」「分類」「種類」など一般的な用語については当該システムとしての明確な定義をするなど、厳密な定義が必要な場合は文書で明確化すること。 | ○ | ○ | ○ |
| 11) データベースの相互の関係、文字の種類、文字数制限、数値の桁数など、関連するあらゆる条件を明確にすること。 | | ○ | ○ |
| (5) データのインテグリティを確保すること。 | ○ | ○ | ○ |
| 1) 開発の担当者<以下、本項に共通>は、開発方針、システム設計マニュアルの基づいてデータのインテグリティ確保の設計をしていること。 | ○ | | |
| 2) データのインテグリティを確保すべきチェックポイントを明確にしていること。 | ○ | | |
| 3) データのインテグリティを確保するためのチェック機能の設計をしていること。 | ○ | | |
| 4) チェック結果を記録する機能を組み込んでいること。 | ○ | | |
| 5) データのインテグリティ確保の設計結果及び検討経緯を明文化されていること。 | ○ | | |
| 6) データのインテグリティを確保するためのリスク評価に基きシステム設計を行うこと。 | | ○ | ○ |
| 7) リスク評価に基づく対策や、確保に必要な条件、手順は明確にすること。 | | ○ | ○ |
| 8) データにアクセスできるネットワークルート、媒体の保存に関する管理策を策定すること。 | ○ | ○ | ○ |
| 9) データにアクセスできる人は制限すること。データの性格によって分類し、対応する制限を明確にすること。 | ○ | ○ | ○ |
| 10) データへのアクセスログなどの記録をとること。 | | ○ | ○ |
| 11) 上記の記録は定期的に検査できるように設計すること。 | | ○ | ○ |
| (6) ネットワークは、業務の内容及びシステム特性に応じて設計すること。 | ○ | ○ | ○ |
| 1) 開発の担当者<以下、本項に共通>は、開発方針及びシステム設計マニュアルに基づいてネットワーク設計していること。 | ○ | | |
| 2) ネットワーク設計における考慮点を明確にしていること。 | ○ | | |
| 3) 利用するネットワークの種類及び選定理由を明確化していること。 | ○ | | |
| 4) 利用するネットワークが適切な性能を有していることを確認していること。 | ○ | | |
| 5) 業務の内容及びシステム性能に基づいて、ネットワークの利用形態を明確にしていること。 | ○ | | |
| 6) システムライフにおけるトラフィック量の増加を考慮してネットワーク設計していること。 | ○ | | |
| 7) 利用するネットワークは、適切なセキュリティを有していること。 | ○ | | |
| 8) ネットワーク設計の結果及び検討経緯を明文化していること。 | ○ | | |
| 9) ネットワークに要求されるトラフィックの量と質に最適なネットワーク設計(容量、速度、許容遅延時間等)を行うこと。 | | ○ | ○ |
| 10) システムの障害発生時の影響を十分考慮すること。 | ○ | ○ | ○ |
| 11) 組織内部と外部と社内ネットワークの非武装ゾーンを明確にし、セキュリティポリシーに基づくネットワークルーティング条件を明確にすること。 | | ○ | ○ |
| 12) 事業継続計画に対応する措置を講じること。 | ○ | ○ | ○ |
| (7) 情報システムの性能は、要求定義を満たすこと。 | ○ | ○ | ○ |
| 1) 開発の担当者<以下、本項に共通>は、開発方針及びシステム設計マニュアルに基づいて情報システムの性能分析・評価を行っていること。 | ○ | | |
| 2) 情報システムの性能分析・評価の方法および考慮点を明確化していること。 | ○ | | |
| 3) 開発対象のシステムを含む情報システム全体として、性能を捉えていること。 | ○ | | |
| 4) 情報システムの性能分析・評価の結果及び検討経緯を明文化していること。 | ○ | | |
| 5) 情報システムの性能分析・評価の結果が要求定義を満たしていることを検証していること。 | ○ | | |
| 6) 要求定義を満たす性能を確保できない場合、要求定義の見直しをユーザに申し入れ、再検討していること。 | ○ | | |
| 7) 要求定義の見直しを技術面及び経済面の両面から行っていること。 | ○ | | |
| 8) 見直された要求定義を明文化されていることを確認する。 | ○ | | |
| 9) 要求定義の見直しの理由を明文化していること。 | ○ | | |
| 10) 要求定義の要求から漏れた機能を明確にし、記録として残していること。 | ○ | | |
| 11) 受注(オフショア)側が全体システムの一部のサブシステムを請け負う場合は、性能に関する要求定義を満足するための各サブシステム単位での性能条件を定めること。 | | ○ | ○ |
| 12) 受注(オフショア)側は上記性能条件を承知していること。 | | ○ | ○ |
| 13) 検収条件に12)の確認を含めること。 | ○ | ○ | ○ |
| 14) 性能条件の種類として、①処理時間、②処理遅延時間、③トラフィック条件など、当該システムとして必要な要素を網羅すること。 | ○ | ○ | ○ |
| 15) 特殊な処理で処理時間を要するものは、処理の上限など、具体的な目標を明確にすること。 | ○ | ○ | ○ |
| (8) 情報システムの運用性及び保守性を考慮して設計すること。 | ○ | ○ | ○ |
| 1) 開発の担当者<以下、本項に共通>は、開発方針及びシステム設計マニュアルに基づいて情報システムの運用の基本方式を検討していること。 | ○ | | |
| 2) 運用における処理のボトルネックを検討していること。 | ○ | | |
| 3) 運用性及び保守性を確保する技術的実現方法を検討していること。 | ○ | | |
| 4) 運用性及び保守性を確保する経済的実現方法を検討していること。 | ○ | | |
| 5) 運用性及び保守性を考慮した設計のレビューに運用部門及び保守部門の代表を参加させていること。 | ○ | | |
| 6) 運用性及び保守性を考慮した設計のレビューは受注(オフショア)側も参加していること。 | ○ | ○ | ○ |
| (9) 他の情報システムとの整合性を考慮して設計すること。 | ○ | ○ | ○ |
| 1) 開発の担当者<以下、本項に共通>は、ITインフラストラクチャとの整合性を評価していること。 | ○ | | |
| 2) 組織体に基本アーキテクチャ(EA)が設定されている場合、EAを遵守して設計していること。 | ○ | | |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|--|-----|-----|-----|
| 3)業務間に共通システムが存在する場合、その共通システムとの整合性、影響度等を評価していること。 | ○ | | |
| 4)データの授受を行う情報システムが存在する場合、データの整合性、データ授受の方式、運用形態、影響度等を評価していること。 | ○ | | |
| 5)ポータルに組み込まれる場合、全体との調和をとって設計していること。 | ○ | | |
| 6)他の情報システムとの整合性を考慮する必要がある場合で、受注(オフショア)側への発注内容に関係する場合、設計の条件を受注(オフショア)側に示すこと。 | ○ | ○ | ○ |
| (10) 情報システムの障害対策を考慮して設計すること。 | ○ | ○ | ○ |
| 1)開発の担当者<以下、本項に共通>は、開発方針及びシステム設計マニュアルに基づいて障害対策機能を設計していること。 | ○ | | |
| 2)情報システムの障害対策の設計の手順および考慮点を明確化していること。 | ○ | | |
| 3)情報システムの可用性(アベイラビリティ)目標を設定していること。 | ○ | | |
| 4)情報システムの障害対策を講じる対象を明確化していること。 | ○ | | |
| 5)明確化した対象障害ごとに、障害対策機能を設計していること。 | ○ | | |
| 6)障害発生後の復旧について、復旧対象、復旧方法の設計を行っていること。 | ○ | | |
| 7)障害対策の設計結果を、明文化していること。 | ○ | | |
| 8)障害の種類を特定していること。 | | ○ | ○ |
| 9) 8)に対応した設計条件は明確にしていること。 | | ○ | ○ |
| 10)オフショアに対応した部分における8)の条件は受注(オフショア)側に示すこと。 | | ○ | ○ |
| (11) 誤謬防止、不正防止、機密保護等の機能を設計しているか。 | ○ | ○ | ○ |
| 1)開発の担当者<以下、本項に共通>は、開発方針及びシステム設計マニュアルに基づいて情報セキュリティ確保の設計をしていること。 | ○ | | |
| 2)開発の責任者は、想定されるリスクを明確化していること。 | ○ | | |
| 3)開発の責任者は、誤謬防止機能を設計していること。 | ○ | | |
| 4)開発の責任者は、不正防止機能を設計していること。 | ○ | | |
| 5)開発の責任者は、機密保護機能を設計していること。 | ○ | | |
| 6)開発の責任者は、プライバシー保護機能を設計していること。 | ○ | | |
| 7)開発の責任者は、リスクコントロール結果を記録する機能を設計していること。 | ○ | | |
| 8)開発の責任者は、リスクコントロール機能の設計結果及び設計経緯を明文化していること。 | ○ | | |
| 9)監護(うっかりミスを含む)、不正防止、機密保護等を考慮して設計すること。 | | ○ | ○ |
| 10)受注(オフショア)側に発注した部分における、上記1)の条件は受注側の注意力や「常識」に期待していることがなく詳細で明確になっていること。 | | ○ | ○ |
| (12) テスト計画は、目的、範囲、方法、スケジュール等を明確にすること。 | ○ | ○ | ○ |
| 1)開発の担当者<以下、本項に共通>は、開発方針及びシステム設計マニュアルに基づいてテスト計画を立案していること。 | ○ | ○ | ○ |
| 2)開発対象の情報システムに対するテスト方針を明確化していること。 | ○ | ○ | ○ |
| 3)テストの種類、目的、体制及び実施方法を明確にしていること。 | ○ | ○ | ○ |
| 4)信頼性、安全性および効率性についてのテスト項目を定めていること。 | ○ | ○ | ○ |
| 5)テストデータ仕様書を作成していること。 | ○ | ○ | ○ |
| 6)性能の測定及び分析方法並びに性能のチューニングポイントを明確にしていること。 | ○ | ○ | ○ |
| 7)テスト実施に必要な期間を設定していること。 | ○ | ○ | ○ |
| 8)テスト結果の検証方法・体制を明確にしていること。 | ○ | ○ | ○ |
| 9)開発側のテストとともに、ユーザ受入れテストも考慮していること。 | ○ | ○ | ○ |
| 10)テスト計画を各工程に対して合理的に計画すること。(単体、結合、ノード全体、ノード間結合、ネットワーク総合、運用など) | ○ | ○ | ○ |
| 11)各工程におけるテスト計画の目的、方法を明確にすること。 | ○ | ○ | ○ |
| 12)各工程におけるテストスケジュールを明確にすること。 | ○ | ○ | ○ |
| 13)オフショアに関する部分で日本の他社との結合試験が必要な場合、試験場所や体制など2国をまたがる場合の配慮をしていること。 | | ○ | ○ |
| (13) 情報システムの利用に係る教育の方針、スケジュール等を明確にすること。 | ○ | | |
| 1)開発の担当者<以下、本項に共通>は、ユーザ教育の対象者、教育の種類、内容、方法、スケジュール等を明確にしていること。 | ○ | | |
| 2)ユーザマニュアル等の作成手順及び承認手続を定めていること。 | ○ | | |
| 3)ユーザ教育に必要な資源を明確にし、確保していること。 | ○ | | |
| 4)ユーザ教育の方針等のレビューにユーザ部門の責任者を参画させていること。 | ○ | | |
| 5)ユーザの情報リテラシーの成熟度を考慮して教育計画を立案していること。 | ○ | | |
| (14) モニタリング機能を考慮して設計すること。 | ○ | ○ | ○ |
| 1)開発の責任者は、開発計画時にモニタリング対象の指標と目標値を選定していること。 | ○ | | |
| 2)開発の責任者は、システムの評価項目についてユーザ部門の責任者、運用部門の責任者、及び保守部門の責任者に確認していること。 | ○ | | |
| 3)開発の担当者は、モニタリング項目のシステム実行上の値を測定・解析できる機能をシステム設計時に組み込んでいること。 | ○ | | |
| 4)開発の責任者は、モニタリング項目を継続的に測定・解析できるようにしていること。 | ○ | | |
| 5)開発の責任者は、モニタリング機能のレビューにユーザ部門の代表者、運用部門の代表者、及び保守部門の代表者を参加させていること。 | ○ | | |
| 6)性能に関する事項以外に、目的業務のデータ(登録・変更・業務評価データ等)に関するモニタリング機能を考慮して設計すること。このとき、データの定義を明確に定めオフショア先に示すこと。 | | ○ | ○ |
| 7)運用状況のデータに関するモニタリング機能を考慮して設計すること。このとき、データの定義を明確に定め、オフショア先に示すこと。 | | ○ | ○ |
| (15) システム設計書をレビューすること。 | ○ | ○ | ○ |
| 1)開発の責任者は、システム設計書のレビュー時期を開発計画書に明確にし、レビュー時までシステム設計書を適切に作成していること。 | ○ | | |
| 2)開発の責任者は、システム設計書のレビューにはユーザ部門、開発部門、運用部門及び保守部門が参加していること。 | ○ | | |
| 3)開発の責任者は、システム設計書のレビュー項目の妥当性を確認していること。 | ○ | ○ | |
| 4)開発の責任者は、システム設計書のレビューの終了条件を明確にしていること。 | ○ | ○ | |
| 5)開発の担当者は、システム設計書のレビュー結果をルールに基づいて記録し、適切なフィードバックと処理を行っていること。 | ○ | ○ | |
| 6)開発責任者はシステム設計書のレビュー計画は開催場所(外国&日本)を含めて明確にしていること。 | | ○ | ○ |
| 7)レビューの目的、要領、計画について、オフショア側との共通認識が出来ていること。 | | ○ | ○ |
| 8)レビューに必要なリソースを確保していること。 | | ○ | ○ |
| 9)レビュー要領について、受注(オフショア)側が了承していること。 | | ○ | ○ |
| 3. プログラム設計 | | | |
| (1) プログラム仕様書は、開発の責任者が承認すること。 | ○ | | ○ |
| 1)情報システム部門責任者は、プログラム設計書を承認する責任者として、開発の責任者を任命していること。 | ○ | | |
| 2)開発の責任者は、プログラム設計書を承認し、関係者に周知徹底していること。 | ○ | | |
| 3)開発の担当者は、開発手順及びプログラム設計マニュアルに基づいてプログラム設計書を作成していること。 | ○ | | |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|--|-----|-----|-----|
| 4) 開発の担当者は、プログラム設計書の必要な記載項目を全て網羅していること。 | ○ | | |
| 5) 元請側の責任者が承認していること。 | | ○ | ○ |
| 6) 受注(オフショア)側責任者の承認があること。 | | ○ | ○ |
| 7) プログラム設計書では設計内容として何を記述するか、詳細に定めること(発注・元請(日本)側と受注(オフショア)側での確認の問題) | | ○ | ○ |
| (2) システム設計書に基づいて、プログラムを設計すること。 | | ○ | ○ |
| 1) 開発の担当者<以下、本項に共通>は、開発手順及びプログラム設計マニュアルに基づいて、プログラム設計書を作成していること。 | | ○ | ○ |
| 2) プログラム機能をシステム機能に対して追跡可能であるように設計していること。 | | ○ | ○ |
| 3) プログラム設計で定義された機能をシステム設計で定義された機能に対して必要十分であることを確認していること。 | | ○ | ○ |
| 4) プログラム設計についてシステム設計で定義されたシステムの構造を反映していることを確認していること。 | | ○ | ○ |
| 5) システム設計書とプログラム仕様書との整合性確認結果の記録を確認していること。 | | ○ | ○ |
| 6) プログラム設計書はシステム設計書またはソフトウェアの基本設計書に基づいて作成していることをレビュー等で確認していること。 | | ○ | ○ |
| 7) 国内のメーカーと分担設計している場合、プログラム間の問題の調整の場は明確になっていること。 | | ○ | ○ |
| 8) 元請側から提供されたサンプルプログラムを検討せずそのまま流用しないこと。 | | ○ | ○ |
| 9) 設計書変更管理方法を明確に定めること。 | | ○ | ○ |
| (3) テスト要求事項を定義し、文書化すること。 | ○ | ○ | ○ |
| 1) 開発の担当者<以下、本項に共通>は、開発手順及びプログラム設計マニュアルに基づいて、テスト要求事項を作成していること。 | ○ | ○ | ○ |
| 2) プログラム設計のためのテスト基本方針を作成していること。 | ○ | ○ | ○ |
| 3) プログラム設計に関するテスト要求事項をすべて洗い出していること。 | | ○ | ○ |
| 4) 洗い出したテスト要求事項を文書化していること。 | | ○ | ○ |
| 5) テスト要求事項は設計段階の各段階に対応して階層的に整理体系付けられていること。 | | ○ | ○ |
| 6) テスト段階として、少なくとも、単体試験、結合試験、総合試験をそれぞれ計画すること。 | | ○ | ○ |
| 7) それぞれのテスト段階におけるテストの観点を明確にし重複を避け、全体として試験の全てを網羅するよう、要求事項を定義すること。 | | ○ | ○ |
| 8) テスト要求事項には性能に関する事項が含まれていること。(規定しない場合のリスクを評価し、対策を講じていること) | | ○ | ○ |
| (4) プログラム設計書及びテスト要求事項をレビューすること。 | ○ | ○ | ○ |
| 1) 開発の責任者は、プログラム設計の品質目標を明確にしていること。 | ○ | ○ | ○ |
| 2) 開発の責任者は、プログラム仕様書及びテスト要求事項のレビュー方針、レビュー手順、レビューポイント等を定めていること。 | ○ | ○ | ○ |
| 3) 開発の責任者は、プログラム仕様書及びテスト要求事項のレビュー体制を明確にしていること。 | ○ | ○ | ○ |
| 4) 開発の責任者は、プログラム仕様書及びテスト要求事項のレビューメンバーの人数、能力面の妥当性を確認していること。 | ○ | ○ | ○ |
| 5) 開発の責任者は、プログラム仕様書及びテスト要求事項のレビュー結果の記録を確認していること。 | ○ | ○ | ○ |
| 6) 開発の責任者は、プログラム設計書及びテスト要求事項のレビューにおいてシステム設計との整合性を確認していること。 | ○ | ○ | ○ |
| 7) レビュー計画にオフショア側設計者及びブリッジSEが含まれていること。 | | ○ | ○ |
| 8) レビューの範囲、稼働量、など、品質管理の条件に対応して明確な基準を設けていること。 | | ○ | ○ |
| 9) レビュー計画は基本設計、詳細設計、コーディング単体試験、結合試験、総合試験など、各工程ごとに計画すること。 | | ○ | ○ |
| 10) レビュー対象(設計書のほか、ソースコード、テスト手順、ユーザマニュアルなど、出力ドキュメント)を明確にすること。 | | ○ | ○ |
| 11) レビューで検出された問題点は問題の発生要因(途中仕様変更、教育不足等)、技術的要因(異常処理、排他制御など)、日本語表現要因(以上、未済など)の要因を分析し、追加試験措置 | | ○ | ○ |
| 12) レビュー結果の反映方法は明確になっていること。 | | ○ | ○ |
| (5) プログラム設計時に発見したシステム設計の矛盾は、システム設計の再検討を行って解決すること。 | ○ | ○ | ○ |
| 1) 開発の責任者は、プログラム設計の過程でシステム設計の矛盾を発見した場合の報告手続を明確にしていること。 | ○ | ○ | ○ |
| 2) 開発の責任者は、システム設計の矛盾が発見された場合に報告手続に従って報告されていることを確認していること。 | ○ | ○ | ○ |
| 3) 開発のシステム設計担当者は、システム設計の矛盾が発見された場合システム設計の再検討を行っていること。 | ○ | ○ | ○ |
| 4) 開発の責任者は、システム設計の再検討の結果について関係者の合意を確認していること。 | ○ | | |
| 5) 開発の責任者は、システム設計担当者自身によるシステム設計書の変更を確認していること。 | | ○ | |
| 6) 開発の責任者は、システム設計の再検討結果の記録を確認していること。 | | ○ | ○ |
| 7) 開発の責任者は、公式なレビュー結果を確認しシステム設計書の変更を承認していること。 | ○ | ○ | ○ |
| 8) 解決はブリッジSEを含む会議で対策を決定すること。 | ○ | ○ | ○ |
| 4. プログラミング | | | |
| (1) プログラム設計書に基づいてプログラミングすること。 | | ○ | ○ |
| 1) 開発の責任者は、システム開発手順やプログラミングマニュアルに基づいて、プログラミングすることを定めていること。 | | ○ | ○ |
| 2) 開発の責任者は、プログラミングの具体的手順をまとめたプログラミングマニュアルを定めていること。 | | ○ | ○ |
| 3) 開発の責任者は、プログラミングの検証手順を定めていること。 | | ○ | ○ |
| 4) 開発の責任者は、プログラミングの検証手順として、プログラム設計書とコーディングの突合を行うことを定めていること。 | | ○ | ○ |
| 5) 開発の担当者は、システム開発手順およびプログラミングマニュアルに基づいてプログラミングしていること。 | | ○ | ○ |
| 6) 開発の担当者は、プログラミング検証手順に基づいて、プログラミングの検証を行っていること。 | | ○ | ○ |
| 7) 開発の担当者は、プログラミングの検証結果を記録していること。 | | ○ | ○ |
| 8) 最速に計画されたソースコードレビューの計画があること。 | | ○ | ○ |
| 9) レビュー項目はプログラム設計書に基づいて選定されていること。 | | ○ | ○ |
| 10) 受注(オフショア)側担当分のソースコードレビューについて受注(オフショア)側内部で周知されていること。 | | | ○ |
| 11) ソースコードレビューに発注側の設計者やブリッジSE及びオフショア側の設計者は参加していること。 | | ○ | ○ |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|--|-----|-----|-----|
| (2) 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。 | | ○ | ○ |
| 1) 開発の責任者は、プログラムのコーディング標準を定めていること。 | | ○ | ○ |
| 2) 開発の責任者は、プログラマに対してコーディング標準の提示や教育を行っていること。 | | ○ | ○ |
| 3) 開発の責任者は、プログラマに対して、コーディング標準に適合してプログラミングすることの重要性を指導していること。 | | ○ | ○ |
| 4) プログラマは、コーディング標準の適合の重要性を認識していること。 | | ○ | ○ |
| 5) 開発の責任者は、プログラミングの検証手順として、プログラムコードがコーディング標準に適合していることを検証することを定めていること。 | | ○ | ○ |
| 6) プログラマは、プログラムコードをコーディング標準に適合して作成していること。 | | ○ | ○ |
| 7) 開発の担当者は、プログラマがコーディング標準に適合してプログラミングしていることを検証していること。 | | ○ | ○ |
| 7) 受注(オフショア)側のコーディング標準の解釈は発注者側の解釈と合っていることを確認していること。 | | | ○ |
| 8) 受注(オフショア)側のプログラミング要員はコーディング標準に準じてコーディングしていることを途中で確認すること。 | | | ○ |
| 9) コーディング標準との整合性チェックツールを用いてチェックする場合、当該のチェックツールの機能はコーディング標準を満足していること。(単なる形式的なコーディング方法のみが「コーディング標準」となっている場合は標準そのものの見直しが必要) | | | ○ |
| 10) 日本語のコメントを挿入する場合の書体やフォント、挿入基準や用語など必要な事項は全て規定されていること。 | | | ○ |
| (3) プログラムコード及びプログラムテスト結果を評価し、記録及び保管すること。 | | ○ | ○ |
| 1) 開発の責任者は、プログラムテスト計画を作成するシステム開発手順を定めていること。 | | ○ | ○ |
| 2) 開発の責任者は、システム開発手順に基づきプログラムテスト計画やプログラムテスト手順を作成していること。 | | ○ | ○ |
| 3) 開発の責任者は、プログラムテスト結果の検証の責任者を明確にしていること。 | | ○ | ○ |
| 4) 開発の担当者は、プログラム設計書に基づいて具体的なプログラムテスト計画を作成していること。 | | ○ | ○ |
| 5) 開発の担当者は、プログラム設計書に基づいて、プログラムテストのテストケースを想定していること。 | | ○ | ○ |
| 6) 開発の担当者は、想定したテストケースを検証するテストデータを、洩れなく作成していること。 | | ○ | ○ |
| 7) 開発の担当者は、プログラムテスト結果の検証手順、検証ポイントを定めていること。 | | ○ | ○ |
| 8) 開発の担当者は、プログラムテストの検証手順、検証ポイントに基づき、プログラムテスト結果の検証を行っていること。 | | ○ | ○ |
| 9) プログラムテスト結果の検証の責任者は、開発の担当者がプログラムテスト結果の検証手順に従ってプログラムテスト結果の検証を行っていることを、確認していること。 | | ○ | ○ |
| 10) 開発の担当者は、プログラムコードの評価及びプログラムテスト結果を記録し、保管していること。 | | ○ | ○ |
| 11) テスト結果の評価基準は受発注双方で明確になっており、合意していること。 | ○ | ○ | ○ |
| (4) 重要プログラムは、プログラム作成者以外の者がテストすること。 | | | |
| 1) 開発の責任者<以下、本項に共通>は、プログラム重要度の設定基準を定めていること。 | | | ○ |
| 2) 重要プログラムのプログラムテスト担当者の選定基準を定めていること。 | | | ○ |
| 3) 重要プログラムのプログラムテスト担当者をプログラム作成者以外の者がテストする基準として定めていること。 | | | ○ |
| 4) 開発の責任者は、基準に基づいてプログラムに重要度を設定していること。 | | | ○ |
| 5) 基準に基づいて重要プログラムのプログラムテスト担当者を選定(プログラム作成者以外の者)していること。 | | | ○ |
| 6) 重要プログラムのプログラムテスト担当者の能力の適格性を確認していること。 | | | ○ |
| 7) 重要プログラムのプログラムテストについては、プログラム作成者以外のものに対応させていること。 | | | ○ |
| 5. システムテスト・ユーザ受入れテスト | | | |
| (1) システムテスト計画は、開発及びテストの責任者が承認すること。 | ○ | ○ | ○ |
| 1) 開発の責任者<以下、共通>は、システム開発手順にシステムテスト計画を作成するよう定めていること。 | | ○ | ○ |
| 2) システムテスト計画の方針を定めていること。 | | ○ | ○ |
| 3) 開発の担当者がシステム開発手順に基づきシステムテスト計画書やシステムテスト手順書を作成していることを検証していること。 | | ○ | ○ |
| 4) 開発の担当者が必要な内容をすべて網羅したシステムテスト計画書を作成していることを検証していること。 | | ○ | ○ |
| 5) システムテストにおける開発及びテストの責任者を明確にしていること。 | | ○ | ○ |
| 6) 開発及びテストの責任者は、システムテスト計画を承認していること。 | | ○ | ○ |
| 7) 開発及びテストの責任者は、システムテスト手順およびシステムテスト計画の内容を関係者に周知徹底していること。 | | ○ | ○ |
| 8) システムテスト計画は発注・元請側と受注(オフショア)側の双方の承認があること。 | ○ | ○ | ○ |
| 9) システムテストは結合試験、複数複合試験・総合試験など、階層化して計画すること | | ○ | ○ |
| 10) 項目数の妥当性を確認すること。 | | ○ | ○ |
| 11) 試験項目一覧表を作成すること | | | ○ |
| 12) 試験手順書を作成すること。 | | | ○ |
| 13) システムテスト計画はネットワーク構成、システム構成、サブシステム構成、サブシステム内部のモジュール構成など重要な観点で体系化されていること。 | | ○ | ○ |
| 14) ユーザ受け入れテストの前の段階(総合試験段階等)で重要仕様(機能・性能)についてユーザの確認を得ることが好ましい。 | ○ | ○ | ○ |
| (2) ユーザ受入れテスト計画は、ユーザ及び開発の責任者が承認すること。 | ○ | ○ | ○ |
| 1) 開発の責任者は、システム開発手順にユーザ受入れテスト計画を作成するよう定めていること。 | | ○ | ○ |
| 2) 開発の担当者は、システム開発手順に基づきユーザ受入れテスト計画書やユーザ受入れテスト手順書を作成していること | | ○ | ○ |
| 3) 開発の担当者は、必要な内容をすべて網羅したユーザ受入れテスト計画書を作成していること。 | | ○ | ○ |
| 4) 開発の責任者は、ユーザ受入れテストにおけるユーザ及び開発の責任者を明確にしていること。 | | ○ | ○ |
| 5) 開発及びテストの責任者は、ユーザ受入れテスト計画を承認していること。 | | ○ | ○ |
| 6) 開発及びテストの責任者は、ユーザ受入れテスト手順およびユーザ受入れテスト計画の内容を関係者に周知徹底していること。 | | ○ | ○ |
| 7) 受注(オフショア)側が関連する場合、必要に応じて受注(オフショア)側も開発の責任者として含まれていること。 | | ○ | ○ |
| (3) システムテストに当たっては、システム要求事項を網羅してテストケースを設定して行うこと。 | | ○ | ○ |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|--|-----|-----|-----|
| 1) システムテストの担当者は、システム要求事項を網羅してテストケースを設定していること。 | | ○ | ○ |
| 2) 開発の責任者及び開発の担当者は、システムテストケースのレビューを実施していること。 | | ○ | ○ |
| 3) テスト内容はシステムの機能、性能、信頼性条件の確認を含んでいること。 | | ○ | ○ |
| 4) システムテストの計画はシステムの性格(小規模アプリケーション、大規模ネットワークシステムなど)に対応して最適に実現していること。 | | ○ | ○ |
| 5) システムテストで出たエラーについて分析し、前段階のテストで検出されるべきエラーがある場合には、類似の問題についてテストケースを再検証すること。 | | | ○ |
| (4) テストデータの作成及びシステムテストは、テスト計画に基づいて行うこと。 | | ○ | ○ |
| 1) 開発の責任者は、開発の担当者がシステムテスト計画に基づいて、具体的なシステムテストの計画を作成していることを検証していること。 | | ○ | ○ |
| 2) 開発の責任者は、開発の担当者がシステムテストの担当者に、システムテストの計画を周知徹底していることを検証していること。 | | ○ | ○ |
| 3) 開発の責任者は、システムテストの担当者がシステムテストのケース想定書に基づいて、システムテストデータを作成していることを検証していること。 | | ○ | ○ |
| 4) 開発の責任者は、不具合が生じた場合のフォローの方法・体制を明確にしていること。 | | ○ | ○ |
| 5) システムテストの担当者は、具体的なシステムテストの計画に基づいて、システムテストを実施していること。 | | ○ | ○ |
| 6) 開発及びテストの責任者は、システムテスト計画に基づいてシステムテストが行われていることを確認していること。 | | ○ | ○ |
| 7) テストデータの作成及びシステムテストはテスト計画に基づいて擬似データもしくは本番データなどの性格、及びデータ量について吟味して行っていること。 | | ○ | ○ |
| 8) テストデータの管理責任は受注(オフショア)側に対して明確になっていること。 | | ○ | ○ |
| 9) システムテストの完了条件は明確になっており、国際取引先と合意できていること。 | | ○ | ○ |
| (5) システムテストは、本番環境と隔離された環境で行うこと。 | | ○ | ○ |
| 1) 開発の責任者<以下、本項に共通>は、システムテストを実施する環境を本番環境と物理的に隔離していること。 | | ○ | ○ |
| 2) システムテストを実施する環境を本番環境と論理的に隔離していること。 | | ○ | ○ |
| 3) システムテストを実施する環境をテスト効果の観点から本番環境と相違ない環境としていること。 | | ○ | ○ |
| 4) システムテストを実施する環境を承認していること。 | | ○ | ○ |
| 5) システムテストを本番環境と隔離された環境で行う場合、2国間の何れで行うか合意できていること。 | | ○ | ○ |
| 6) 本番データを用いる場合、その管理は厳重になされていること。 | | ○ | ○ |
| 7) 本番データを扱う場合機密管理の契約はあること。 | ○ | ○ | ○ |
| (6) システムテストは、開発当事者以外の者が参画すること。 | | ○ | ○ |
| 1) 開発の責任者<以下、本項に共通>は、システムテストの実施体制を確立していること。 | | ○ | ○ |
| 2) システムテストの責任者を明確にしていること。 | | ○ | ○ |
| 3) システムテストの体制に開発当事者以外の者の参画させていること。 | | ○ | ○ |
| 4) システムテストに参画する者のシステムの目的、システムテストの目的を理解度を確認していること。 | | ○ | ○ |
| (7) システムテストは、適切なテスト手法及び標準を使用すること。 | | ○ | ○ |
| 1) 開発の責任者は、システムテスト実施に当たって、システムのタイプ、システム開発の形態、アプリケーションシステムの種類等によって、適切なテスト手法を採用していること。 | | ○ | ○ |
| 2) 開発の責任者は、システムテスト実施にあたって、システムテストの目的に即した適切な標準を使用していること。 | | ○ | ○ |
| 3) 本番環境と異なる場合、テスト負荷を擬似するための試験環境やテスト技法を用意していること。 | | ○ | ○ |
| 4) テスト実施範囲を把握する手法を用いていること。 | | | ○ |
| (8) ユーザ受入れテストは、本番同様の環境を設定すること。 | | ○ | ○ |
| 1) 開発の責任者<以下、本項に共通>は、ユーザ受入れテスト実施にあたって、確認すべきユーザ要求事項をすべて洗い出して、ユーザ受入れテスト計画に反映していること。 | | ○ | ○ |
| 2) ユーザ受入れテスト実施にあたって、確認すべきユーザ要求事項をテストする環境を定義していること。 | | ○ | ○ |
| 3) 定義されたユーザ受入れテストの環境が本番環境と同様であることを確認していること。 | | ○ | ○ |
| 4) ユーザ受入れテストの実施環境を本番環境と隔離していること。 | | ○ | ○ |
| 5) ユーザ受入れテストを実施する環境を承認していること。 | | ○ | ○ |
| 6) 本番環境と異なる条件とその影響についてリスク評価を行っていること。 | | ○ | ○ |
| 7) 上記のリスク評価は開発側と発注側双方の合意はできていること。 | | ○ | ○ |
| (9) ユーザ受入れテストは、ユーザマニュアルに従い、本番運用を想定したテストケースを設定して実施すること。 | | ○ | ○ |
| 1) 開発の責任者<以下、本項に共通>は、ユーザ受入れテストに実務に精通したユーザが参画させていること。 | | ○ | ○ |
| 2) ユーザ受入れテストにおいて、要件定義書とユーザマニュアルの内容を確認していること。 | | ○ | ○ |
| 3) ユーザ受入れテストにおいて、本番運用を想定したテストケースを設定していること。 | | ○ | ○ |
| 4) ユーザ受入れテストのテストケースについて、実務に精通したユーザによるレビューが実施されていることを確認していること。 | | ○ | ○ |
| (10) ユーザ受入れテストは、ユーザ及び運用の担当者もテストに参画して確認すること。 | | ○ | ○ |
| 1) 開発の責任者は、ユーザ受入れテストの実施体制を確立していること。 | | ○ | ○ |
| 2) 開発の責任者は、ユーザ受入れテストの責任者を明確にしていること。 | | ○ | ○ |
| 3) 開発の責任者は、ユーザ受入れテストの体制に、ユーザ及び運用の担当者を参画させていること。 | | ○ | ○ |
| 4) 開発の責任者は、ユーザ受入れテストに参画する者のシステムの目的、ユーザ受入れテストの目的を理解度を確認していること。 | | ○ | ○ |
| 5) ユーザ受入れ手テストの担当者は、ユーザ受入れテスト計画に基づいて、ユーザ受入れテストを | | ○ | ○ |
| 6) 開発及びテストの責任者は、ユーザ受入れテスト計画に基づいてユーザ受入れテストが行われていることを確認していること。 | | ○ | ○ |
| (11) システムテスト及びユーザ受入れテストの結果は、ユーザ、開発、運用及び保守の責任者が承認すること。 | | ○ | ○ |
| 1) 開発の責任者は、システムテストやユーザ受入れテストのテストの計画で定めた目的の達成を検証していること。 | | ○ | ○ |
| 2) ユーザ、開発、運用及び保守の責任者は、システムテストやユーザ受入れテストの結果を承認していること。 | | ○ | ○ |
| 3) 受注(オフショア)側の責任者も承認していること。 | | ○ | ○ |
| (12) システムテスト及びユーザ受入れテストの経過及び結果を記録及び保管すること。 | | ○ | ○ |
| 1) 開発の責任者<以下、本項に共通>は、システムテスト及びユーザ受入れテストの経過及び結果を記録及び保管することを定めていること。 | | ○ | ○ |
| 2) システムテスト及びユーザ受入れテストの環境、データ、結果の保管方法、保管期間が定めていること。 | | ○ | ○ |
| 3) システムテスト及びユーザ受入れテストの環境、データ、結果の保管責任者を明確にしていること。 | | ○ | ○ |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|--|-----|-----|-----|
| 4) システムテスト及びユーザ受入れテストのテストデータ、テスト結果及びテスト環境が、記録されていることを確認していること。 | ○ | ○ | |
| 5) システムテスト及びユーザ受入れテストのテストデータ、テスト結果及びテスト環境が、保管されていることを確認していること。 | ○ | ○ | |
| 6) 受注(オフショア)側に通知し、受注(オフショア)側でも経過及び結果を記録、保管すること。 | ○ | ○ | ○ |
| (13) パッケージソフトウェアを調達する場合、開発元が品質テストを実施したことを確認すること。 | ○ | ○ | |
| 1) 開発の責任者は、パッケージソフトを調達する場合、開発元によるパッケージソフトの品質テストの実施とその結果を確認していること。 | | ○ | |
| 2) 開発の責任者は、パッケージソフトを調達する場合、品質テストの実施結果の開示を調達条件に入れていること。 | ○ | ○ | |
| 6. 移行 | | | |
| (1) 移行計画を策定し、ユーザ、開発、運用及び保守の責任者が承認すること。 | ○ | ○ | |
| 1) 開発の責任者<以下、本項に共通>は、移行までに、開発、導入・テストが終了していることを確認していること。 | ○ | ○ | |
| 2) 移行までに、開発、導入・テストの作業の記録が作成されていることを確認していること。 | ○ | ○ | |
| 3) 移行までに、開発、導入・テストの作業の記録を承認していること。 | ○ | ○ | |
| 4) 移行までに、開発、導入・テストの作業の記録を保管していること。 | ○ | ○ | |
| 5) 移行計画の策定手順を定めるとともに、移行計画策定にあたってはユーザ、開発、運用、保守の各部門を参加させていること。 | ○ | ○ | |
| 6) 移行計画において、移行に必要な書類(運用、保守の引継書を含む)を整理していること。 | ○ | ○ | |
| 7) 移行計画において、移行に必要なリソースを明確にしていること。 | ○ | ○ | |
| 8) 移行計画において、並行移行、段階的移行、一括移行などの移行方法を明確にしていること。 | ○ | ○ | |
| 9) 移行全体のプロセスの承認を行うとともに、各ユーザ、運用、保守の責任者の承認を得ていることを確認していること。 | ○ | ○ | |
| 10) 受注(オフショア)側は発注元の責任者あるいは、ユーザ、開発、運用・保守の責任者から移行計画の提示を受け、承認すること。 | ○ | ○ | ○ |
| (2) 移行作業は文書に記録し、責任者が承認すること。 | ○ | ○ | |
| 1) 開発の責任者<以下、本項に共通>は、移行概要作成時に、作成すべき移行作業に係る記録文書の種類とタイミングを検討し、移行計画書に明記していること。 | ○ | ○ | |
| 2) 移行計画書に基づき、移行に係る作業の実施記録、実施報告書、懸案事項等が作成し、各ユーザ、運用、保守の責任者の承認を受けていること。 | ○ | ○ | |
| 3) 移行に係る作業の実施記録、実施報告書、懸案事項等の記録を保管していること。 | ○ | ○ | |
| 4) 移行に係る各種の作業記録を、移行計画書に基づき遅滞なく作成していること。 | ○ | ○ | |
| 5) 移行作業終了後もデータの移行が継続される場合は、作業を分けて定義し、終了報告書も個別に作成していること。 | ○ | ○ | |
| 6) 受注(オフショア)側は移行作業の概要、日程等について、責任者の承認のある文書、記録を確認すること。 | ○ | ○ | ○ |
| (3) 移行完了の検証方法を移行計画で明確にすること。 | ○ | ○ | |
| 1) 開発の責任者<以下、本項に共通>は、移行計画書において、検証対象を明確にしていること。 | ○ | ○ | |
| 2) 移行計画書において、検証手順、検証方法及び検証体制を明確にしていること。 | ○ | ○ | |
| 3) 移行計画書において、移行完了の評価基準を明確にし、関係者の同意を得ていること。 | ○ | ○ | |
| 4) 受注(オフショア)側は開発を終了し、正式稼働に到るまでの移行完了の検証方法(作業計画、分担、ドキュメント、テスト結果、各種ツール類・操作マニュアル等の提示、引継ぎ等)について、発注元の責任者と協議し、明確化すること。 | ○ | ○ | ○ |
| (4) 移行計画に基づいて、移行に必要な要員、予算、設備等を確保すること。 | ○ | ○ | |
| 1) 開発の責任者<以下、本項に共通>は、移行計画において、移行に必要な要員、予算、設備等の見積り結果を明確にしていること。 | ○ | ○ | |
| 2) 移行計画において、移行に必要な要員、予算、設備等の投入時期を明確にしていること。 | ○ | ○ | |
| 3) 移行計画に記述されている移行に必要な要員、予算、設備等の見積りおよび投入時期について、その妥当性を検証していること。 | ○ | ○ | |
| 4) 移行計画に記述されている移行に必要な要員、予算、設備等の見積りおよび投入時期について、その妥当性の検証結果を記録していること。 | ○ | ○ | |
| 5) 移行計画に記述されている移行に必要な要員、予算、設備等の見積りおよび投入時期について関係部門の責任者に説明し、合意を得ていること。 | ○ | ○ | |
| 6) 移行計画に基づいて、移行に必要な要員、予算、設備などの確保を行っていること。 | ○ | ○ | |
| 7) 移行に必要な要員、予算、設備などの確保状況を確認していること。 | ○ | ○ | |
| 8) 受注(オフショア)側は発注元責任者との間で協議、明確化した移行に関する役割分担に従って、必要な要員・体制、予算、設備等を確保すること。 | | ○ | ○ |
| (5) 移行は手順書を作成し、実施すること。 | ○ | ○ | |
| 1) 開発の責任者<以下、本項に共通>は、移行計画書において、移行の作業定義を行っていること。 | ○ | ○ | |
| 2) 移行の作業定義に基づき、移行作業手順書を作成していること。 | ○ | ○ | |
| 2) 移行手順書において、移行作業の内容を明確にしていること。 | ○ | ○ | |
| 3) 移行作業を行う要員に対して、移行手順書を事前に配布し、事前確認を行っていること。 | ○ | ○ | |
| 4) 移行作業が移行手順書通り、実施されていることを確認していること。 | ○ | ○ | |
| 5) 受注(オフショア)側は、移行作業に必要な手順書を手入または作成・承認を受け、合意した役割分担に従って実施すること。 | | | ○ |
| (6) 移行時のリスク対策を検討すること。 | ○ | ○ | |
| 1) 開発の責任者<以下、本項に共通>は、設計段階、導入・テスト段階で、本番移行時のリスク想定を実施していること。 | ○ | ○ | |
| 2) 本番移行時のリスク想定作業に、ユーザ、開発、運用、保守の各部門を参加させていること。 | ○ | ○ | |
| 3) リスクに対する重要度の基づく対応策を検討し、対応の優先順位付けを行っていること。 | ○ | ○ | |
| 4) リスク評価において、最悪の事態も評価の対象としていること。 | ○ | ○ | |
| 5) 本番移行時のリスク評価・対応策の検討結果を、関係者に周知徹底していること。 | ○ | ○ | |
| 6) 受注(オフショア)側は、移行に伴うリスクについて分析を行い、発注元と協議し、必要な対策を検討すること。 | | ○ | ○ |
| (7) 運用及び保守に必要なドキュメント、各種ツール等は開発の責任者から引き継いでいること。 | ○ | ○ | |
| 1) 開発の責任者は、運用・保守作業計画書等において、運用・保守に必要なドキュメント・各種ツール類を明確にしていること。 | ○ | ○ | |
| 2) 開発の責任者は、本番稼働前に、運用・保守に必要なドキュメントが全て作成されていることを確認していること。 | ○ | ○ | |
| 3) 開発の責任者は、本番稼働前に、運用・保守に必要な各種ツール類等の機能確認が終了していることを確認していること。 | ○ | ○ | |
| 4) 開発の責任者は、本番稼働前に、運用・保守に必要なドキュメント・各種ツール類について、運用及び保守の関係者に対して、引渡しや説明を実施していること。 | ○ | ○ | |
| 5) 運用及び保守の責任者は、開発の責任者から受領した文書類を元に、稼働前までに現行の文書類を適切に修正していること。 | ○ | ○ | |
| 6) 運用及び保守の責任者は、修正済み文書類を担当者に周知徹底していること。 | ○ | ○ | |
| 7) 受注(オフショア)側は、移行、運用、保守に必要なドキュメント、操作説明書、関連ツール等について、発注元の責任者に確認し、必要な引継ぎを行うこと。 | | | ○ |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|---|-----|-----|-----|
| (8) 移行は関係者に周知徹底すること。 | ○ | | |
| 1)開発の責任者<以下、本項に共通>は、移行作業と移行に係る評価を完了していること。 | ○ | | |
| 2)関係者による本番稼働の承認を確認していること。 | ○ | | |
| 3)本番稼働予定日を明確にしていること。 | ○ | ○ | ○ |
| 4)移行の概要を、関係者に周知徹底していること。 | ○ | ○ | ○ |
| 5)受注(オフショア)側も移行作業を行う場合は発注元責任者との間で、移行に関する、承認済文書を交換、関係者に配布確認するなど周知徹底を図ること。 | | ○ | ○ |
| IV 運用業務 | | | |
| 1. 運用管理ルール | | | |
| (1) 運用管理ルール及び運用手順は、運用の責任者が承認すること。 | ○ | | |
| 1)運用の責任者は、運用管理ルール及び運用手順を明文化させ、承認していること。 | ○ | | |
| 2)運用管理担当者は、情報システムの運用形態を考慮して運用管理ルールを作成していること。 | ○ | | |
| 3)運用管理担当者は、運用管理ルールに基づき運用手順を作成していること。 | ○ | | |
| 4)情報システム部門責任者は、運用の責任者を定めていること。 | ○ | | |
| 5)運用管理担当者は、運用管理ルール及び運用手順を関係者に周知徹底していること。 | ○ | | |
| 6)運用管理担当者は、定期的に運用管理ルール及び運用手順の効果を確認し、必要に応じて見直していること。 | ○ | | |
| (2) 運用管理ルールは、運用設計に基づいて作成すること。 | ○ | | |
| 1)運用の責任者は、運用設計書を作成していること。 | ○ | | |
| 2)運用管理担当者は、運用設計書に基づき運用管理ルールを作成していること。 | ○ | | |
| 3)運用管理担当者は、情報サービス等で基本運用管理方式が定められている場合、それらも考慮して運用管理ルールを作成していること。 | ○ | | |
| 4)運用管理担当者は、現在の運用環境を考慮して運用管理ルールを作成していること。 | ○ | | |
| 5)運用管理担当者は、運用管理ルールの改訂手順を明確にしていること。 | ○ | | |
| 6)運用管理担当者は、運用管理ルールを改定した場合、関係者に周知徹底していること。 | ○ | | |
| (3) 運用手順は、運用設計及び運用管理ルールに基づいて、規模、期間、システム特性等を考慮して作成すること。 | ○ | | |
| 1)運用管理担当者は、運用設計及び運用管理ルールに基づき運用手順を作成していること。 | ○ | | |
| 2)運用管理担当者は、運用手順に情報システムの規模、期間、システム特性等を考慮していること。 | ○ | | |
| (4) 運用設計及び運用管理ルールに基づいて、担当責任者を定めること。 | ○ | | |
| 1)運用の責任者<以下、本項に共通>は、運用設計に運用管理の基本的事項が設定されていることを確認していること。 | ○ | | |
| 2)運用管理ルールに、運用担当別の役割と責任を定めていることを確認していること。 | ○ | | |
| 3)システム機能等の単位で運用管理担当者を定めていること。 | ○ | | |
| 2. 運用管理 | | | |
| (1) 年間運用計画を策定し、責任者が承認すること。 | ○ | | |
| 1) 運用管理担当者<以下、本項に共通>は、各システムの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作成していること。 | ○ | | |
| 2) 年間運用計画の各イベントのスケジュールが衝突しないよう、関係者によって調整を行っていること。 | ○ | | |
| 3) 運用の責任者に、年間運用計画書の承認を受けていること。 | ○ | | |
| 4) 年間運用計画書を関係者に周知徹底していること。 | ○ | | |
| (2) 年間運用計画に基づいて、月次、日次等の運用計画を策定すること。 | ○ | | |
| 1) 運用管理担当者<以下、本項に共通>は、情報システムの年間運用計画を作成していること。 | ○ | | |
| 2) 年間運用計画に基づき、月次運用計画を作成していること。 | ○ | | |
| 3) 月次運用計画に基づき、日次運用計画を作成していること。 | ○ | | |
| 4) 運用の責任者に月次運用計画及び日次運用計画の承認を受けていること。 | ○ | | |
| 5) 月次運用計画及び日次運用計画を関係者に周知徹底していること。 | ○ | | |
| (3) 運用管理ルールを遵守すること。 | ○ | | |
| 1) 運用管理担当者は、運用管理ルールを明文化し、運用の責任者の承認を受けていること。 | ○ | | |
| 2) 運用の関係者は、運用管理ルールに関する教育訓練を受けていること。 | ○ | | |
| 3) 運用管理担当者は、運用管理ルールに基づいて運用手続きを行っていること。 | ○ | | |
| 4) 運用管理担当者は、データを取扱う場合には、運用管理ルールに則り、企業として正当に承認されたデータのみを対象に取扱っていること。 | ○ | | |
| 5) 運用管理担当者は、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。 | ○ | | |
| 6) 運用管理担当者は、運用管理ルール及び運用手順に関する是正処置を行っていること。 | ○ | | |
| (4) ジョブスケジュールは、業務処理の優先度を考慮して設定すること。 | ○ | | |
| 1) 運用管理担当者<以下、本項に共通>は、ジョブスケジュールを所定の処理依頼に基づき作成していること。 | ○ | | |
| 2) ジョブの優先度を、業務の重要性、緊急性、機密度等を考慮し設定していること。 | ○ | | |
| 3) ジョブスケジュールを、ユーザと調整を図っていること。 | ○ | | |
| 4) ジョブスケジュールを、運用の責任者に承認を受けていること。 | ○ | | |
| (5) オペレーションは、ジョブスケジュール及び指示書に基づいて行うこと。 | ○ | | |
| 1) 運用管理担当者<以下、本項に共通>は、運用の責任者に指示書の承認を受けていること。 | ○ | | |
| 2) 指示書に、オペレーションを実施するのに必要十分な情報を網羅していること。 | ○ | | |
| 3) オペレータに、オペレーション実施結果を記録させていること。 | ○ | | |
| (6) 例外処理のオペレーションは、運用管理ルールに基づいて行うこと。 | ○ | | |
| 1) 運用管理担当者<以下、本項に共通>は、運用の責任者に例外処理の承認を受けていること。 | ○ | | |
| 2) 例外処理が他の業務に及ぼす影響を調査していること。 | ○ | | |
| 3) 例外処理の頻度及び理由を分析していること。 | ○ | | |
| 4) 例外処理の分析結果をジョブスケジュールに反映していること。 | ○ | | |
| 5) 例外処理を定期的に見直し、減らすようにしていること。 | ○ | | |
| (7) オペレータの交替は、運用管理ルールに基づいて行うこと。 | ○ | | |
| 1) 運用管理担当者<以下、本項に共通>は、オペレータの引継ぎの手順を定めていること。 | ○ | | |
| 2) オペレータの引継の状況を定期的に運用の責任者に報告していること。 | ○ | | |
| 3) 引継ぎの内容に、引き継ぎを受けるオペレータにとって必要十分な情報を盛り込ませていること。 | ○ | | |
| (8) ジョブスケジュール及びオペレーション実施記録を採り、ジョブスケジュールとの差異分析を行うこと。 | ○ | | |
| 1) 運用管理担当者<以下、本項に共通>は、ジョブスケジュール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) 差異分析に例外処理を含めていること。 | ○ | | |
| 3) 差異分析の結果を、運用の責任者に報告していること。 | ○ | | |
| 4) 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。 | ○ | | |
| (9) 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こと。 | ○ | | |
| 1) 運用管理担当者<以下、本項に共通>は、オペレーション実施記録の保管期間を定めていること。 | ○ | | |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|---|-----|-----|-----|
| 2)オペレーション実施記録を定められた期間保管していること。 | ○ | | |
| 3)オペレーション実施記録を廃棄した場合、廃棄の記録をとっていること。 | ○ | | |
| (10) 事故及び障害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。 | ○ | | |
| 1)運用管理担当者<以下、本項に共通>は、影響度に応じたエスカレーションフロー及び体制等を定めていること。 | ○ | | |
| 2) エスカレーションフローを、運用の責任者及び利用部門の責任者に承認を受けていること。 | ○ | | |
| 3)エスカレーションフローを、関係者に周知徹底していること。 | ○ | | |
| 4)エスカレーションフローを、環境に応じて見直しを行っていること。 | ○ | | |
| (11) 事故及び障害の内容を記録し、情報システムの運用の責任者に報告すること。 | ○ | | |
| 1)運用管理担当者<以下、本項に共通>は、事故及び障害の発生時に報告書を作成していること。 | ○ | | |
| 2) 事故及び障害の報告書を、運用の責任者に承認を受けていること。 | ○ | | |
| 3)報告書に、事故及び障害の状況、原因等を記載していること。 | ○ | | |
| 4)事故・障害発生時に、あらかじめ定めた連絡体制が機能することを確認していること。 | ○ | | |
| (12) 事故及び障害の原因を究明し、再発防止の措置を講じていること。 | ○ | | |
| 1)運用管理担当者<以下、本項に共通>は、事故及び障害の原因を分析していること。 | ○ | | |
| 2) 事故及び障害の再発防止処置を講じていること。 | ○ | | |
| 3)再発防止処置を関係者に周知徹底していること。 | ○ | | |
| (13) 情報システムのユーザに対する支援体制を確立すること。 | ○ | | |
| 1)情報システム部門の責任者<以下、本項に共通>は、ユーザ部門が利用するための基本ルールを定めていること。 | ○ | | |
| 2)ユーザ部門が利用するための組織化を図っていること。 | ○ | | |
| 3) 情報システム部門を中心としたユーザ利用のための支援体制を確立していること。 | ○ | | |
| 4) 情報システム部門とユーザ部門で定期的話し合う場を設けていること。 | ○ | | |
| (14) 情報セキュリティに関する教育及び訓練をユーザに対して実施すること。 | ○ | | |
| 1)運用の責任者<以下、本項に共通>は、情報セキュリティ教育の内容を明確にしていること。 | ○ | | |
| 2) 教育及び訓練を定期的実施していること。 | ○ | | |
| 3)情報環境の変化に対応して、教育及び訓練の内容を見直していること。 | ○ | | |
| (15) 情報システムの稼働に関するモニタリング体制を確立すること。 | ○ | | |
| 1) 運用の責任者は、情報システムのモニタリングを実施する社内合意を形成していること。 | ○ | | |
| 2)運用管理担当者は、アプリケーションのモニタリングを行う機能を組み込んでいること。 | ○ | | |
| 3)運用管理担当者は、インフラストラクチャのモニタリングを行う機能を組み込んでいること。 | ○ | | |
| 4)運用の責任者は、モニタリング結果を評価する体制を有していること。 | ○ | | |
| 5) 運用の責任者は、評価結果を計画的に改善に結び付ける仕組みを有していること。 | ○ | | |
| (16) 情報システムの稼働実績を把握し、性能管理及び資源の有効利用を図ること。 | ○ | | |
| 1)運用の責任者は、情報システムのモニタリングの仕組みと体制を有していること。 | ○ | | |
| 2)運用管理担当者は、性能評価の指標を明確にしていること。 | ○ | | |
| 3)運用管理担当者は、モニタリング結果を把握し、分析し、評価していること。 | ○ | | |
| 4)運用管理担当者は、評価結果を討議する体制を有し、問題点や対策を討議していること。 | ○ | | |
| 5) 運用管理担当者は、評価結果を関係者に報告していること。 | ○ | | |
| 6) 運用管理担当者は、評価結果に基づき、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。 | ○ | | |
| 7) 運用管理担当者は、稼働実績データをその後の情報システムの構成管理等に活用していること。 | ○ | | |
| 8)情報システムの変更、業務処理の変更等に対し、操作手順の更新を適切に行っていること。 | ○ | | |
| 3. 入力管理 | | | |
| (1) 入力管理ルールを定め、遵守すること。 | ○ | | |
| 1) 入力管理担当者<以下、本項に共通>は、入力管理ルールを明文化し、入力の責任者の承認を受けていること。 | ○ | | |
| 2)入力管理ルールに、不正、誤謬、漏洩等の防止、データの正確性を期すための牽制機能を明記していること。 | ○ | | |
| 3)データの入力者を明確にし、入力の責任者の承認を受けていること。 | ○ | | |
| 4)入力管理ルールを関係者に周知徹底していること。 | ○ | | |
| 5)関係者が入力管理ルールを遵守していることを検証していること。 | ○ | | |
| 6)入力管理ルールを見直していること。 | ○ | | |
| (2) データの入力は、入力管理ルールに基づいて漏れなく、重複なく、正確に行うこと。 | ○ | | |
| 1) 入力管理担当者<以下、本項に共通>は、データの入力を管理者が承認した担当者に行わせていること。 | ○ | | |
| 2) 入力データの照合を行っていること。 | ○ | | |
| 3) 入力データについて、入力の責任者の承認を得ていること。 | ○ | | |
| 4)入力記録及び端末操作記録を一定期間保管していること。 | ○ | | |
| 5)入力管理ルールを関係者に周知徹底していること。 | ○ | | |
| 6)関係者が入力管理ルールを遵守していることを検証していること。 | ○ | | |
| 7)入力管理ルールの効果を定期的に確認し、必要に応じて見直していること。 | ○ | | |
| (3) 入力データの作成手順、取扱い等は誤謬防止、不正防止、機密保護等の対策を講じていること。 | ○ | | |
| 1) 入力管理担当者<以下、本項に共通>は、入力データの作成手順に、誤謬及び不正を防止する仕組みを入れていること。 | ○ | | |
| 2) 入力データの作成手順に、機密保護や個人情報保護を取り入れていること。 | ○ | | |
| 3) 入力データの授受を記録していること。 | ○ | | |
| 4) 入力データの授受には、データの暗号化等の搬送時の保護策を講じていること。 | ○ | | |
| 5)入力データの機密度に応じて取扱者を限定していること。 | ○ | | |
| 6)データ入力に係る事故・障害記録を取得し、適切な対策を講じていること。 | ○ | | |
| (4) データの入力の誤謬防止、不正防止、機密保護等の対策は有効に機能すること。 | ○ | | |
| 1) 入力管理担当者<以下、本項に共通>は、入力時のデータ照合が機能していることを確認していること。 | ○ | | |
| 2) プログラムに、誤謬及び不正を発見するチェック機能を含ませていること。 | ○ | | |
| 3) 機密保護及び個人情報保護の対策を実施していること。 | ○ | | |
| 4)誤謬防止、不正防止、機密保護及び個人情報保護の対策の効果を測定し、見直していること。 | ○ | | |
| (5) データの保管及び廃棄は、入力管理ルールに基づいて行うこと。 | ○ | | |
| 1) 入力管理担当者<以下、本項に共通>は、入力データの保管及び廃棄手順を、業務の責任者から承認を得ていること。 | ○ | | |
| 2) 入力データの保管及び廃棄を、業務の責任者の承認を得て適切に行っていること。 | ○ | | |
| 3)重要な入力データを廃棄する場合、入力の責任者を立ち合わせていること。 | ○ | | |
| 4)重要な入力データを廃棄する場合、磁気媒体からの消去を確実にしていること。 | ○ | | |
| 5)廃棄を外部に委託する場合、契約条件、業者の信頼性、具体的な廃棄方法等により委託先を決定していること。 | ○ | | |
| 6) 廃棄の記録を残していること。 | ○ | | |
| 4. データ管理 | | | |
| (1) データ管理ルールを定め、遵守すること。 | ○ | | |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|---|-----|-----|-----|
| 1) データ管理担当者<以下、本項に共通>は、データ管理ルールを明文化し、データの責任者に承認を受けていること。 | ○ | | |
| 2) データの管理者、検証者等の役割をあらかじめ定め、データの責任者の承認を受けていること。 | ○ | | |
| 3) データ管理の対象を、組織体で使用しているデータを網羅して設定していること。 | ○ | | |
| 4) データ管理の体系を、組織体として一貫性をもって作成していること。 | ○ | | |
| 5) 機密情報及び個人情報の取扱い方法をデータ管理ルールに定めていること。 | ○ | | |
| 6) データ管理ルールに、アクセスコントロール、バックアップ、リカバリ、データの授受等を定めていること。 | ○ | | |
| 7) 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。 | ○ | | |
| 8) データ管理ルールの見直しを行っていること。 | ○ | | |
| (2) データへのアクセスコントロール及びモニタリングは、有効に機能すること。 | ○ | | |
| 1) データ管理担当者<以下、本項に共通>は、データへのアクセスコントロールの機能を有効にしていること。 | ○ | | |
| 2) アクセスコントロールの機能が、対象データの重要性・機密性を考慮した場合、過不足ない内容になっていることを確認していること。 | ○ | | |
| 3) データへのアクセスについてモニタリングし、モニタリング機能の稼働状況を確認していること。 | ○ | | |
| 4) 無資格者が情報システムを使用していないかどうかを定期的に調査していること。 | ○ | | |
| 5) 特定のファイルへの偏った利用はないか、異常な時刻での利用はないか等を調査していること。 | ○ | | |
| 6) 不正利用、不正アクセスを調査し、それらに対し再発防止策を講じていること。 | ○ | | |
| 7) 組織、基本ソフトウェア、業務内容等の変更に伴い、アクセスコントロール機能を見直していること。 | ○ | | |
| (3) データのインテグリティを維持すること。 | ○ | | |
| 1) データ管理担当者<以下、本項に共通>は、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・更新する場合に、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いること。 | ○ | | |
| (4) データの利用状況を記録し、定期的に分析すること。 | ○ | | |
| 1) データ管理担当者<以下、本項に共通>は、データの利用状況を記録する機能を設けていること。 | ○ | | |
| 2) データの利用状況を定期的に分析していること。 | ○ | | |
| 3) 分析結果に基づき、データベース、ファイル、記録媒体等の有効利用を図り、将来のデータ量の変化への対応を考慮していること。 | ○ | | |
| 4) 不正利用の調査を行い、対策を講じていること。 | ○ | | |
| 5) 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) データのバックアップの範囲、方法及びタイミングは、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。 | ○ | | |
| 1) データ管理担当者<以下、本項に共通>は、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) データの授受は、データ管理ルールに基づいて行うこと。 | ○ | | |
| 1) データ管理担当者<以下、本項に共通>は、データの授受を、データ管理ルールで定める担当者に行わせていること。 | ○ | | |
| 2) データ管理ルールに基づいて、データの授受、保管、確認及び返却を行っていること。 | ○ | | |
| 3) データの授受を記録し、データの責任者の承認を受けていること。 | ○ | | |
| 4) データの授受記録を、一定期間保管していること。 | ○ | | |
| (7) データの交換は、不正防止及び機密保護の対策を講じること。 | ○ | | |
| 1) データ管理担当者<以下、本項に共通>は、データの交換形態に応じた不正防止、機密保護及び個人情報保護の対策を講じていること。 | ○ | | |
| 2) データの交換について、データの責任者の承認を受けていること。 | ○ | | |
| 3) データ管理ルールで定める機密度の高いデータ交換には、暗号化等の処置を講じさせていること。 | ○ | | |
| 4) データの交換記録を定期的に分析していること。 | ○ | | |
| (8) データの保管、複写及び廃棄は、誤謬防止、不正防止及び機密保護の対策を講じること。 | ○ | | |
| 1) データ管理担当者<以下、本項に共通>は、保管、複写、廃棄を、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、廃棄について、データの責任者の承認を受けていること。 | ○ | | |
| 3) 所定の場所、期間及び方法でデータ保管していること。 | ○ | | |
| 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) 重要なデータには複写履歴を記録させていること。 | ○ | | |
| 6) 重要なデータの廃棄に当たって、データの責任者が立ち合っていること。 | ○ | | |
| 7) 廃棄を外部に委託する場合、契約条件、業者の信頼性、具体的な廃棄方法等により委託先を決定していること。 | ○ | | |
| 8) 廃棄の記録を残していること。 | ○ | | |
| (9) データに対するコンピュータウイルス対策を講じること。 | ○ | | |
| 1) データ管理担当者<以下、本項に共通>は、情報システムの環境に適合したコンピュータウイルス対策を講じていること。 | ○ | | |
| 2) コンピュータウイルス対策を、関係者に周知徹底していること。 | ○ | | |
| 3) 被害を被った場合は、関係機関への報告やウイルス駆除等回復を実施する体制を有していること。 | ○ | | |
| (10) データの知的財産権を管理すること。 | ○ | | |
| 1) データ管理担当者<以下、本項に共通>は、データ取扱い関係者に対し、知的財産権の教育を実施し、著作物に対する認識をもたせていること。 | ○ | | |
| 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導入する場合、定められた手続きで導入していること。 | ○ | | |
| 4) 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。 | ○ | | |
| 5. 出力管理 | | | |
| (1) 出力管理ルールを定め、遵守すること。 | ○ | | |
| 1) 出力管理担当者は、出力管理ルールを明文化し、出力の責任者の承認を受けていること。 | ○ | | |
| 2) 出力管理担当者は、出力管理ルールに、誤謬防止、不正防止を含め、機密保護、個人情報保護を考慮していること。 | ○ | | |
| 3) 出力の責任者は、情報システム部門の責任者によって定められていること。 | ○ | | |
| 4) 出力管理担当者は、出力管理ルールを関係者に周知徹底しているとともに、ルールが遵守されていることを検証していること。 | ○ | | |
| 5) 出力管理担当者は、定期的に出力管理ルールの効果を確認し、必要に応じて見直ししていること。 | ○ | | |
| (2) 出力情報は、漏れなく、重複なく、正確であることを確認すること。 | ○ | | |
| 1) 出力管理担当者<以下、本項に共通>は、網羅性、正確性確保のための確認ルール、手順を定めていること。 | ○ | | |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|---|-----|-----|-----|
| 2)出力業務を、出力の責任者の承認した担当者に行わせていること。 | ○ | | |
| 3)出力記録及び端末操作記録を一定期間保管していること。 | ○ | | |
| (3) 出力情報の作成手順、取扱い等は、誤謬防止、不正防止及び機密保護の対策を講じること。 | ○ | | |
| 1)出力管理担当者<以下、本項に共通>は、出力情報の作成手順に、誤謬及び不正を防止する内容を含めていること。 | ○ | | |
| 2)不正な複写、複製等を防止する対策を講じていること。 | ○ | | |
| 3)出力情報の機密密度に応じて取扱者を限定していること。 | ○ | | |
| (4) 出力情報の引渡しは、出力管理ルールに基づいて行うこと。 | ○ | | |
| 1)出力管理担当者<以下、本項に共通>は、出力情報の引き渡し状況を記録していること。 | ○ | | |
| 2)引渡し方法を適切に選択していること。 | ○ | | |
| (5) 出力情報の保管及び廃棄は、出力管理ルールに基づいて行うこと。 | ○ | | |
| 1)出力管理担当者<以下、本項に共通>は、出力情報の保管及び廃棄の責任者を定めていること。 | ○ | | |
| 2)出力情報を、適切に保管していること。 | ○ | | |
| 3)出力情報の廃棄方法を定めていること。 | ○ | | |
| 4)重要な出力情報の廃棄には、出力の責任者を立ち合わせていること。 | ○ | | |
| 5)廃棄を委託している場合、契約条件、廃棄方法、業者の信用等を調査し、委託先を決定していること。 | ○ | | |
| 6)出力情報の保管及び廃棄を行う場合、業務の責任者の承認を得ていること。 | ○ | | |
| (6) 出力情報のエラー状況を記録し、定期的に分析すること。 | ○ | | |
| 1)出力管理担当者<以下、本項に共通>は、出力情報のエラー状況を記録していること。 | ○ | | |
| 2)出力情報のエラーの原因を究明し、改善措置を図っていること。 | ○ | | |
| (7) 出力情報の利用状況を記録し、定期的に分析すること。 | ○ | | |
| 1)出力管理担当者<以下、本項に共通>は、出力情報の利用状況を定期的に分析及び評価していること。 | ○ | | |
| 2)分析結果に基づいて、出力情報の改善を図っていること。 | ○ | | |
| 6. ソフトウェア管理 | | | |
| (1) ソフトウェア管理ルールを定め、遵守すること。 | ○ | ○ | ○ |
| 1)ソフトウェア管理担当者<以下、本項に共通>は、ソフトウェア管理ルールを明文化し、ソフトウェアの責任者の承認を得ていること。 | ○ | | |
| 2)ソフト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)ソフトウェア管理の対象を、組織体で使用しているソフトウェアを網羅して設定していること。 | ○ | | |
| 4)管理の体系を、組織体として一貫性を持って作成していること。 | ○ | | |
| 5)定期的にソフトウェア管理ルールの効果を確認し、必要に応じて見直ししていること。 | ○ | | |
| 6)ソフトウェア管理ルールを発注側と受注側の責任者は相互に承認すること。 | ○ | ○ | ○ |
| 7)受注(オフショア)側責任者は担当者に上記管理ルールを周知・教育すること。 | ○ | ○ | ○ |
| 8)管理ルールは維持管理の具体的な内容を詳細に定めること。 | | | |
| (a)ソフトウェアの種類と機密度 (b)ソフトウェア管理者(責任と権限) (c)ソフトウェア授受手順 (d)ソフトウェアの変更管理 (e)バックアップの採取基準方法・管理 (f)ソフトウェア保管方法・保管場所・期間 (g)ソフトウェアの廃棄方法 (h)ソフトウェアの複写方法 (i)機密密度に対応したアクセスコントロールの方法 (j)ソフトウェアの利用状況の記録と定期的検査 (k)ソフトウェアの格納媒体と容量及び余裕領域の管理方法 (l)機能追加要領(有償・無償範囲) (m)コーディング規約 (n)性能評価方法 (o)問題処理要領 (p)品質評価方法、品質判定条件 (q)打ち合わせ体制・頻度・場所 (r)用語定義その他 | | ○ | ○ |
| (2) ソフトウェアへのアクセスコントロール及びモニタリングは、有効に機能すること。 | ○ | ○ | ○ |
| 1)ソフトウェア管理担当者<以下、本項に共通>は、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。 | ○ | | |
| 2)アクセス状況のモニタリング機能の稼働状況を確認していること。 | ○ | | |
| 3)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。 | ○ | | |
| 4)不正利用、不正アクセスの調査を行い、再発防止策を講じていること。 | ○ | | |
| 5)組織、基本ソフトウェア、業務内容等の変更に伴い、アクセスコントロール機能を見直していること。 | ○ | | |
| 6)ソフトウェアへのアクセス制御は利用権限に対応して制限すること。 | ○ | ○ | ○ |
| 7)ソフトウェアのユーザID及びパスワードの登録・削除のルールを定めること。 | ○ | ○ | ○ |
| 8)各個人の利用可能なソフトウェアは管理すること。 | ○ | ○ | ○ |
| (3) ソフトウェアの利用状況を記録し、定期的に分析すること。 | ○ | ○ | ○ |
| 1)ソフトウェア管理担当者<以下、本項に共通>は、ソフトウェアの利用状況を記録する機能を設けていること。 | ○ | | |
| 2)ソフトウェアの利用状況を定期的に分析していること。 | ○ | | |
| 3)分析結果に基づき、情報システムの運用改善を図り、不要ソフトウェアの廃棄を行っていること。 | ○ | | |
| 4)ソフトウェアの利用状況を記録すること。 | ○ | ○ | ○ |
| 5)ソフトウェアの利用状況の記録は定期的に分析すること。 | ○ | ○ | ○ |
| 6)利用上の問題点の対策を実施し、評価すること。 | ○ | ○ | ○ |
| (4) ソフトウェアのバックアップの範囲、方法及びタイミングは、業務内容及び処理形態を考慮して決定すること。 | ○ | ○ | ○ |
| 1)ソフトウェア管理担当者<以下、本項に共通>は、バックアップの範囲、記録媒体、保管方法等を、業務内容及び処理形態に応じて定めていること。 | ○ | | |
| 2)バックアップしたソフトウェアと運用中のソフトウェアとの整合性・同期性について、考慮していること。 | ○ | | |
| 3)バックアップ方法及びリカバリーの方法を、情報システムの変更に伴い、見直していること。 | ○ | ○ | ○ |
| 4)バックアップの方法は発注側条件を満足させること。 世代管理条件、バックアップファイル条件(運転ファイル、ソースファイル、管理ファイル等) | ○ | ○ | ○ |
| 5)業務の重要性を考え、レベル分けしてバックアップ方法を定めること。 | ○ | ○ | ○ |
| 6)バックアップしたソフトウェアの試験方法(正常にバックアップできているか)は定めること。 | ○ | ○ | ○ |
| (5) ソフトウェアの授受は、ソフトウェア管理ルールに基づいて行うこと。 | ○ | | |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|--|-----|-----|-----|
| 1) ソフトウェア管理担当者<以下、本項に共通>は、ソフトウェアの授受を、ソフトウェア管理ルールに定める担当者が行っていること。 | ○ | | |
| 2) ソフトウェア管理ルールに基づいて、ソフトウェアの授受、保管、確認及び返却を行っていること。 | ○ | | |
| 3) ソフトウェアの授受を記録し、ソフトウェアの責任者が承認していること。 | ○ | | |
| 4) ソフトウェアの授受記録を、一定期間保管していること。 | ○ | ○ | ○ |
| 5) 組織間のソフトウェア交換(電子的又は人手によるもの)については、必要のある場合には正式な契約として合意を取り交わすこと。 | ○ | ○ | ○ |
| 6) インターネットその他の電子的な手段を介してのソフトウェアの送受信は当該国の法律上問題ないことを確認すること。 | ○ | ○ | ○ |
| (6) ソフトウェアの保管、複写及び廃棄は、不正防止及び機密保護の対策を講じること。 | ○ | ○ | ○ |
| 1) ソフトウェア管理担当者<以下、本項に共通>は、ソフトウェアの保管、複写、廃棄について、機密度及び記録媒体に応じた不正防止、機密保護の対策を講じていること。 | ○ | ○ | |
| 2) 保管、複写及び廃棄について、ソフトウェアの責任者に承認を得ていること。 | ○ | ○ | |
| 3) ソフトウェアの複写を、使用許諾条件に基づいて行っていること。 | ○ | ○ | |
| 4) ソフトウェアの保管、複写及び廃棄の履歴を記録していること。 | ○ | ○ | |
| 5) 重要なソフトウェアの廃棄を、ソフトウェアの責任者の確認を得て行っていること。 | ○ | ○ | |
| 6) ソフトウェアの保管のルールを定め、誤謬防止、不正防止、及び機密保護の対策を講じること。 (サーバ内部、媒体、取り扱い説明書類など性格に応じた対策はあるか) | ○ | ○ | ○ |
| 7) ソフトウェアの複写のルールを定め、誤謬防止、不正防止、及び機密保護の対策を講じること。 (複写の禁止、不能化、すかし挿入、著作権による請願など) | ○ | ○ | ○ |
| 8) ソフトウェアの廃棄のルールを定め、誤謬防止、不正防止、及び機密保護の対策を講じること。 (廃棄の徹底の程度、不正利用防止対策) | ○ | ○ | ○ |
| (7) ソフトウェアに対するコンピュータウイルス対策を講じること。 | ○ | ○ | ○ |
| 1) ソフトウェア管理担当者<以下、本項に共通>は、情報システムの環境に適合したコンピュータウイルス対策を講じていること。 | ○ | | |
| 2) コンピュータウイルス対策を、関係者に周知徹底していること。 | ○ | | |
| 3) 被害を被った場合は、関係機関への報告やウイルス駆除等回復を実施する体制を有していること。 | ○ | ○ | ○ |
| 4) 悪意のあるソフトウェアの検出及び防止の対策を実施すること。 | ○ | ○ | ○ |
| 5) 悪意のあるソフトウェアに対する利用者の認識の教育を実施すること。 | ○ | ○ | ○ |
| 6) 予防又は定常の作業としてコンピュータ及び媒体を走査するためのウイルス検出ソフトウェアや修復ソフトウェアの導入・運用を考慮すること。 | ○ | ○ | ○ |
| 7) セキュリティ事故発生時の連絡系統は定められているか。 当該国の現地の基準と整合をとること。 | ○ | ○ | ○ |
| (8) ソフトウェアの知的財産権を管理すること。 | ○ | ○ | ○ |
| 1) ソフトウェア管理担当者<以下、本項に共通>は、ソフトウェアを取扱う関係者に対し、知的財産権の教育を実施し、著作物に対する認識をもたせていること。 | ○ | ○ | |
| 2) 知的財産権の保護の対象とするソフトウェアを明確にしていること。 | ○ | ○ | ○ |
| 3) 外部からのソフトウェアを導入する場合、定められた手続きで導入していること。 | ○ | ○ | ○ |
| 4) 導入したソフトウェア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。 | ○ | ○ | ○ |
| 5) 当該国の著作権保護法などの整合をとること。 | ○ | ○ | ○ |
| 6) 受注(オフショア)側職員全員への知的財産権に関する教育を実施すること。 | ○ | ○ | ○ |
| (9) フリーソフトウェアの利用に関し、組織体としての方針を明確にすること。 | ○ | ○ | ○ |
| 1) ソフトウェアの責任者<以下、本項に共通>は、フリーソフトウェア及びシェアウェアに対する組織体の方針を定めていること。 | ○ | | |
| 2) 方針を、情報システム部門の責任者の承認を得ていること。 | ○ | | |
| 3) 方針が、組織体のすべてに遵守されていることを検証していること。 | ○ | | |
| 4) フリーソフトウェア及びシェアウェアの利用状況を管理していること。 | ○ | | |
| 5) フリーソフトウェア及びシェアウェアの利用の基準を具体的に定めること。違反のときの罰則を含むこと。 | ○ | ○ | ○ |
| 7. ハードウェア管理 | ○ | | |
| (1) ハードウェア管理ルールを定め、遵守すること。 | ○ | | |
| 1) 情報システム部門の責任者は、ハードウェアの責任者及び管理担当者を定めていること。 | ○ | | |
| 2) ハードウェア管理担当者<以下に共通>は、運用設計と情報資産の管理方針に基づきハードウェアの購入、導入、運用、監視、廃棄等ハードウェアの管理に必要な項目についてハードウェア管理ルール及び手順を明文化すること。 | ○ | | |
| 3) ハードウェア管理ルール及び手順において、セキュリティを考慮していること。 | ○ | | |
| 4) ハードウェア管理ルール及び手順について、ハードウェアの責任者の承認を受けていること。 | ○ | | |
| 5) 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。 | ○ | | |
| 6) 組織体で使用しているハードウェアを識別し、重要度に応じた管理の対象としていること。 | ○ | | |
| 7) 定期的にハードウェア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) ハードウェアは、想定されるリスクに対応できる環境に設置すること。 | ○ | | |
| 1) ハードウェア管理担当者<以下に共通>は、ハードウェアに関する自然災害、不正行為、障害等のリスク分析を計画的に行っていること。 | ○ | | |
| 2) リスク分析結果を踏まえて、ハードウェアの設置環境を明確にし、ハードウェアの責任者の承認を受けていること。 | ○ | | |
| 3) ハードウェアの設置環境に関して、「情報システム安全対策基準」を考慮すること。 | ○ | | |
| 4) ハードウェアの設置環境を維持・改善していること。 | ○ | | |
| 5) 情報資産の管理方針に基づきリスクに対応したハードウェア管理を行っていること。 (注) 「情報システム安全対策基準」は、平成7年8月作成された基準で、平成3年に作成された「電子計算機システム安全対策基準」を改訂したものである。 | ○ | | |
| (3) ハードウェアは、定期的に保守を行うこと。 | ○ | | |
| 1) ハードウェア管理担当者<以下に共通>は、保守対象、保守内容及び保守サイクルを明確にし、ハードウェアの責任者の承認を受けていること。 | ○ | | |
| 2) 保守の実施に関して、データなどの漏えい防止策を施していること。 | ○ | | |
| 3) 保守結果を記録し、ハードウェアの責任者に報告していること。 | ○ | | |
| 4) 日常の点検項目を明確にし、点検状況を記録していること。 | ○ | | |
| 5) 障害情報を収集し、適切な臨時保守を実施していること。 | ○ | | |
| (4) ハードウェアは、障害対策を講じていること。 | ○ | | |
| 1) ハードウェア管理担当者<以下に共通>は、障害時の連絡体制を整備し、関係者に周知していること。 | ○ | | |
| 2) 障害対策の現状を把握し、必要に応じてレビューし改善していること。 | ○ | | |
| 3) 障害発生時のリスクを分析し、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、必要な訓練を実施していること。 | ○ | | |
| (5) ハードウェアの利用状況を記録し、定期的に分析すること。 | ○ | | |
| 1) ハードウェア管理担当者<以下に共通>は、利用状況の記録項目を明確にし、記録を確認していること。 | ○ | | |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|---|-----|-----|-----|
| 2)分析項目を定め、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、情報システムの方針に沿って、ハードウェア利用の改善を図っていること。 | ○ | | |
| (6) ハードウェアの保管、移設及び廃棄は、不正防止及び機密保護の対策を講じていること。 | ○ | | |
| 1)ハードウェア管理担当者<以下に共通>は、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、ハードウェアの責任者の承認を受けていること。 | ○ | | |
| 2)保管、移設及び廃棄に関して、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、機密保持及び個人情報保護の対策を講じていること。 | ○ | | |
| 3)ハードウェアの保管ルールに従い、所定の場所、期間及び方法で保管していることを定期的に確認していること。 | ○ | | |
| 4)ハードウェアの移設及び廃棄がルールに従って実施されていることを確認していること。 | ○ | | |
| 5)重要なハードウェアの移設、廃棄に立ち会っていること。 | ○ | | |
| 8. ネットワーク管理 | | | |
| (1) ネットワーク管理ルールを定め、遵守すること。 | ○ | ○ | ○ |
| 1)情報システム部門の責任者は、ネットワークの責任者及び管理担当者を定めていること。 | ○ | ○ | ○ |
| 2)ネットワーク管理の担当者<以下に共通>は、障害対策、性能監視、セキュリティ対策、保守管理、コスト管理等必要な項目が網羅したネットワーク管理ルールを明文化すること。 | ○ | ○ | ○ |
| 3) 災害復旧計画との整合性を考慮して、ネットワーク管理ルールを作成していること。 | ○ | ○ | ○ |
| 4)ネットワーク管理ルールに関して、ネットワークの責任者の承認を受けていること。 | ○ | ○ | ○ |
| 5)ネットワーク管理の範囲を明確にしていること。 | ○ | ○ | ○ |
| 6)ネットワークの稼働状況を常時監視できる体制を確立し、責任者の承認を受けていること。 | ○ | ○ | ○ |
| 7)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。 | ○ | ○ | ○ |
| 8)ネットワーク利用のルールを作成し、関係者に周知し遵守状況を確認していること。 | ○ | ○ | ○ |
| (2) 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は、有効に機能すること。 | ○ | ○ | ○ |
| 1)ネットワーク管理担当者<以下に共通>は、ネットワークの重要性、機密性を考慮し、リスク分析を実施し、アクセスコントロール及びモニタリングに関する基本方針を定めていること。 | ○ | ○ | ○ |
| 2)アクセスの基本方針に基づき、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。 | ○ | ○ | ○ |
| 3)アクセスコントロールの基本方針に基づき、アクセスコントロールの方法を検討し、選択していること。 | ○ | ○ | ○ |
| 4)アクセスコントロールの有効性を定期的に確認し、見直していること。 | ○ | ○ | ○ |
| 5)モニタリングの方法を検討し、選択していること。 | ○ | ○ | ○ |
| 6)モニタリングによる不正アクセスの検出時の通知体制を確立し、確認していること。 | ○ | ○ | ○ |
| 7)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。 | ○ | ○ | ○ |
| 8)ネットワーク管理用のユーザIDの管理が適切に行われていることを確認していること。 | ○ | ○ | ○ |
| 9)アクセス権の付与に関して適切に実施されていることを確認していること。 | ○ | ○ | ○ |
| 10)利用者のネットワーク利用ルールの遵守状況を確認していること。 | ○ | ○ | ○ |
| 11)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を確認していること。 | ○ | ○ | ○ |
| 12)遠隔保守用のポートが適切に管理されていることを確認していること。 | ○ | ○ | ○ |
| 13)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及びモニタリングが有効に機能していることを確認していること。必要に応じて改善策を実施していること。 | ○ | ○ | ○ |
| 14)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における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明確にしていること。 | ○ | ○ | ○ |
| (3) ネットワーク監視ログを定期的に分析すること。 | ○ | ○ | ○ |
| 1)ネットワーク管理担当者<以下に共通>は、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が有効になっていることを確認していること。 | ○ | ○ | ○ |
| 3)監視ログ分析作業の効率化に関する対策を検討し、選択していること。 | ○ | ○ | ○ |
| 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を確認していること。 | ○ | ○ | ○ |
| 5)監視ログを適切に管理していることを確認していること。 | ○ | ○ | ○ |
| 6)定期的に監視ログの分析を行い、分析結果についての対応を検討し、選択していること。 | ○ | ○ | ○ |
| 7)ネットワーク監視の有効性を評価し、必要に応じて改善していること。 | ○ | ○ | ○ |
| (4) ネットワークは、障害対策を講じていること。 | ○ | ○ | ○ |
| 1)ネットワーク管理担当者<以下に共通>は、重要なネットワーク機器や伝送路について、リスク分析を行い、業務への影響に配慮して、最長許容障害復旧時間を定めていること。 | ○ | ○ | ○ |
| 2)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内に復旧するための措置を講じていること。 | ○ | ○ | ○ |
| 3)重要なネットワーク機器や伝送路についての障害対策および復旧に関して、ネットワークの責任者の承認を受けていること。 | ○ | ○ | ○ |
| 4)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ネットワークの責任者及び関係者に報告し、再発防止策を講じていること。 | ○ | ○ | ○ |
| 5)ネットワーク障害の発生時の対応手順書を作成し、関係者に周知徹底をしていること。 | ○ | ○ | ○ |
| 6)必要に応じて、代替の伝送路を設定していること。 | ○ | ○ | ○ |
| 7) ネットワーク障害の発生時の対応手順に基づきシミュレーションや訓練を行い、最長許容障害復旧時間を満たしていることを確認していること。 | ○ | ○ | ○ |
| 8)定期的に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や障害発生時の対応手順を見直していること。 | ○ | ○ | ○ |
| (5) 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。 | ○ | ○ | ○ |
| 1)ネットワーク管理担当者<以下に共通>は、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)定期的にネットワークの分析を実施し、分析結果に基づき、ネットワークの新設、変更などの改善措置を図っていること。 | ○ | ○ | ○ |
| (6) ネットワークを利用したサービスについて、組織体としての方針を明確にすること。 | ○ | ○ | ○ |
| 1)ネットワークの責任者は、ネットワークを利用した情報提供等のサービスの利用について方針を明確にしていること。 | ○ | ○ | ○ |
| 2)ネットワーク管理担当者<以下に共通>が、ネットワークを利用した情報提供等のサービスと、サービスを提供する組織体を評価する手順を明確にし、定期的に評価を実施していること。 | ○ | ○ | ○ |
| 3)有料サービスの費用の支払い手続きを明確にしていること。 | ○ | ○ | ○ |
| 9. 構成管理 | | | |
| (1) 管理すべきソフトウェア、ハードウェア及びネットワークの対象範囲を明確にし、管理すること。 | ○ | ○ | |
| 1)情報システム部門の責任者は、構成の責任者及び管理担当者を定めていること。 | ○ | ○ | |
| 2)情報システム部門の責任者は、ソフトウェアのライセンス管理者を定めていること。 | ○ | ○ | |
| 3)構成管理担当者は、構成管理の方針を定め、構成管理の対象を明確にしていること。 | ○ | ○ | |
| 4)構成管理担当者は、導入並びに変更に関する手順書を明文化し、構成の責任者の承認を受けていること。 | ○ | ○ | |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|---|-----|-----|-----|
| 5) 構成管理担当者は、定期的に導入並びに変更に関する手順書の効果を確認し、必要に応じて見直していること。 | ○ | ○ | |
| 6) ソフトウェアのライセンス管理者は、違法コピーのソフトウェアを使用していないことを確実にしていること。 | ○ | ○ | |
| 7) ソフトウェアの構成管理方法を明確にし受注側と合意すること。 | | ○ | ○ |
| (2) ソフトウェア、ハードウェア及びネットワークの構成、調達先、サポート条件等を明確にすること。 | ○ | | |
| 1) 構成管理担当者<以下に共通>は、ソフトウェア、ハードウェア及びネットワークの管理台帳等を作成していること。 | ○ | | |
| 2) 管理台帳の項目については、情報資産の管理方針や各管理手順書との整合性を図り、定期的に見直していること。 | ○ | | |
| 3) 管理台帳が最新の状態を反映していることを検証していること。 | ○ | | |
| 4) 開発に関係する全てのソフトウェアの動作環境条件を明確にし受注(オフショア)側と合意すること。 | | ○ | ○ |
| (3) ソフトウェア、ハードウェア及びネットワークの導入並びに変更は、影響を受ける範囲を検討して決定すること。 | ○ | | |
| 1) 構成管理担当者<以下に共通>は、導入並びに変更に関して、影響を受ける範囲を検討しリスク分析を実施していること。 | ○ | | |
| 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に関して、運用の責任者及び構成の責任者の承認を受けていること。 | ○ | | |
| 3) 導入及び変更作業に際して、関係する部門と事前に調整し、周知徹底をしていること。 | ○ | | |
| 4) 構成変更の作業中及び作業後の問題発生への対処方法を確立する手続きを定めていること。 | ○ | ○ | |
| 5) 仕様変更及びバグ修正項目とファイル版数の対応を明確にすること。 | | ○ | ○ |
| (4) ソフトウェア、ハードウェア及びネットワークの導入並びに変更は、計画的に実施すること。 | ○ | | |
| 1) 構成管理担当者<以下に共通>は、システムとの整合性に考慮し、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) 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書に関して、運用の責任者及び構成の責任者の承認を受けていること。 | ○ | | |
| 3) 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。 | ○ | | |
| 4) 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。 | ○ | | |
| 10. 建物・関連設備管理 | | | |
| (1) 建物及び関連設備は、想定されるリスクに対応できる環境に設置すること。 | ○ | | |
| 1) 情報システム部門の責任者<以下に共通>は、情報システムを運用する場所に関して、自然災害、不正侵入等のリスクを全て想定して選定すること。 | | ○ | |
| 2) 情報システムを運用する場所に関して、事業継続の方針に基づき、可能な範囲で自然災害の影響が最小になるところを選定していること。 | ○ | | |
| 3) 情報システムを運用する場所に関して、不正侵入を防止する設備を設置していること。 | ○ | | |
| 4) 情報システムの設備を設置する場所の表示及び設置状況の公開をしていないこと。 | ○ | | |
| 5) 建物・関連設備の運用に関して、「情報セキュリティ管理基準」「情報システム安全対策基準」を参考にしていること。 | ○ | | |
| (2) 建物及び室への入退の管理は、不正防止及び機密保護の対策を講じること。 | ○ | | |
| 1) 情報システム部門の責任者は、建物及び室の入退管理担当者を定め、入退館、入退室の資格を明確にしていること。 | ○ | | |
| 2) 建物及び室の入退管理担当者<以下に共通>は、入退館、入退室に関するルールを明文化し、関係者に周知していること。 | | ○ | |
| 3) 入退館、入退室に関するルール及び対策に関して「情報セキュリティ管理基準」を参考にし、不正防止及び十分な機密保護対策を実施していること。 | ○ | | |
| 4) 検知した異常を責任者へ連絡する方法及び体制を確立していること。 | ○ | | |
| 5) 物品の持ち込み及び持出しを監視する手順を定め、監視状況を確認していること。 | ○ | | |
| 6) 入退管理の状況を把握していること。 | ○ | | |
| (3) 関連設備は、適切な運用を行うこと。 | ○ | | |
| 1) 情報システム部門の責任者は、建物・関連設備の責任者と管理担当者を定めていること。 | ○ | | |
| 2) 建物・関連設備の責任者は、管理担当者が作成した関連設備を運用するためのルールを承認していること。 | | ○ | |
| 3) 建物・設備管理担当者<以下に共通>は、関連設備について運用ルールを遵守していることを確認していること。 | ○ | | |
| 4) 運用の状況を把握していることを確認していること。 | ○ | | |
| (4) 関連設備は、定期的に保守を行うこと。 | ○ | | |
| 1) 建物・設備管理担当者<以下に共通>は、保守の内容及び点検項目を明確にしていること。 | | ○ | |
| 2) 保守が定期的に行われ、異常がないことを確認していること。 | ○ | | |
| 3) 保守結果が記録され、内容が適切であることを確認していること。 | ○ | | |
| 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) 関連設備は、障害対策を講じること。 | ○ | | |
| 1) 建物・設備管理担当者<以下に共通>は、関連設備の管理および稼働状況の監視ルールを作成し、建物・関連設備の責任者の承認を受けていること。 | | ○ | |
| 2) 建物・関連設備に関するリスク分析を行い、事業継続の方針に基づき障害対策(バックアップ)を実施していること。 | ○ | | |
| 3) 関連設備の稼働状況を監視していること。 | ○ | | |
| 4) 事業継続の方針、機器の重要度に応じて、瞬断及び停電対策を講じていること。 | ○ | | |
| 5) 空気調和設備の能力に余力を持っていることを確認していること。 | ○ | | |
| 6) 監視設備が、検知状況を記録し、異常を警報する機能を有していることを確認し、定期的な動作確認を実施していること。 | ○ | | |
| 7) 定期的に関連設備の障害対策の有効性を評価し、必要に応じて見直していること。 | ○ | | |
| 8) 建物・関連設備の障害対策に関して、「情報セキュリティ管理基準」「情報システム安全対策基準」を参考にしていること。 | ○ | | |
| (6) 建物及び室への入退の管理を記録し、定期的に分析すること。 | ○ | | |
| 1) 建物及び室の入退管理担当者<以下に共通>は、建物及び室への入退館及び入退室の記録について関係者に周知し、遵守状況を確認していること。 | | ○ | |
| 2) 入退館(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) 入退館(室)の記録を定期的に分析し、手順及び対策の有効性を評価し、必要に応じて改善していること。 | ○ | | |
| V. 保守業務 | | | |
| 1. 保守手順 | | | |
| (1) 保守ルール及び保守手順は、保守の責任者が承認すること。 | ○ | ○ | ○ |
| 1) 保守の責任者<以下に共通>は、保守のルールを定めていること。 | ○ | ○ | |
| 2) 保守の実施決定及び保守業務実施のプロセスを標準化していること。 | ○ | ○ | |
| 3) 保守のルールを明文化していること。 | ○ | ○ | |
| 4) 保守の担当者は、保守ルール及び保守実施手順に関して、保守及び運用の責任者の承認を取り付けていること。 | ○ | ○ | |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|---|-----|-----|-----|
| 5) 保守の責任者<以下に共通>は、保守ルール及び保守手順を情報システム部門とユーザの関係者に周知していること。 | ○ | ○ | |
| 6) 保守ルール及び保守手順が遵守されていることを定期的に確認していること。 | ○ | ○ | |
| 7) 保守ルール及び保守手順を定期的に見直していること。 | ○ | ○ | |
| 8) 保守ルール及び保守手順を文書化すること。 | ○ | ○ | ○ |
| 9) 受注(オフショア)側は保守ルール及び保守手順を文書で確認すること。 | | | ○ |
| (2) 保守手順は、保守の規模、期間、システムの特性等を考慮して決定すること。 | ○ | ○ | |
| 1) 保守担当者<以下に共通>は、保守の手順を保守ルールに沿って決めていること。 | ○ | ○ | |
| 2) 個別保守案件の規模、期間、システム特性を分析していること。 | ○ | ○ | |
| 3) 個別保守計画を保守の規模、期間、システム特性を反映したものとしていること。 | ○ | ○ | |
| 4) 保守の規模、期間、システム特性等を文書で明確にすること。 | | | ○ |
| 5) 受注(オフショア)側は保守の規模、期間、システム特性等を文書で確認すること。 | | | ○ |
| (3) 保守時のリスクを評価し、必要対応策を講じること。 | ○ | ○ | |
| 1) 保守担当者<以下に共通>は、保守の実施に当たっては、想定されるリスクを漏れなく洗い出していること。 | ○ | ○ | |
| 2) 洗い出した個々のリスクの発生頻度、影響度及び範囲を明確にしていること。 | ○ | ○ | |
| 3) 想定されたリスクに対して最適な管理策を講じていること。 | ○ | ○ | |
| 2. 保守計画 | | | |
| (1) 保守計画はユーザ及び保守の責任者が承認すること。 | ○ | ○ | ○ |
| 1) 保守責任者は、保守計画を個別保守案件ごとに作成させていること。 | ○ | ○ | |
| 2) 保守担当者<以下に共通>は、個別保守計画に必要なかつ十分な内容を記述していること。 | ○ | ○ | |
| 3) 個別保守計画は組織の要員配置計画と整合させていること。 | ○ | ○ | |
| 4) 保守の反映時期を関連システムの計画と整合させていること。 | ○ | ○ | |
| 5) 個別保守計画をユーザ、運用及び保守の責任者の承認を取り付けていること。 | ○ | ○ | |
| 6) 保守計画は文書で明確にすること。 | ○ | ○ | ○ |
| 7) 受注(オフショア)側の責任者は保守計画内容の内のオフショア側責任部分を文書で確認すること。 | | ○ | ○ |
| (2) 変更依頼等に対し、保守の内容及び影響範囲の調査並びに分析を行うこと。 | ○ | | |
| 1) ユーザ部門責任者は、保守ルールに基づいて、変更依頼等を提出していること。 | ○ | | |
| 2) 保守担当者<以下に共通>は、変更依頼等をユーザ及び保守の責任者が承認したものであることを確認していること。 | ○ | | |
| 3) 保守対象システムのドキュメント、プログラム、データ等の分析を行い、結果を記録していること。 | ○ | ○ | |
| (3) 保守のテスト計画は、目的、範囲、方法、スケジュール等を明確にすること。 | ○ | ○ | ○ |
| 1) 保守担当者<以下に共通>は、テスト計画について要求事項を明確にしていること。 | ○ | ○ | |
| 2) テスト計画についてユーザ、運用及び保守の責任者の承認を取り付けていること。 | ○ | ○ | |
| 3) テストデータの準備を計画に含めていること。 | ○ | ○ | |
| 4) テストの検証方法、求められる処理結果、検証担当者等をテスト計画に含めていること。 | ○ | ○ | |
| 5) テスト環境として、開発業務から引き継いだテスト環境利用の可能性を考慮していること。 | ○ | ○ | |
| 6) 保守テスト計画は文書で明確にすること。 | ○ | ○ | ○ |
| 7) 受注(オフショア)側の責任者は保守テスト計画内容で受注(オフショア)側責任部分を文書で確認すること。 | | | ○ |
| 3. 保守の実施 | | | |
| (1) システム設計書、プログラム設計書等は、保守計画に基づいて変更し、ユーザ及び保守の責任者が承認すること。 | ○ | ○ | |
| 1) 保守担当者<以下に共通>は、システム設計書、プログラム設計書等の保守対象システムのドキュメントの変更を保守計画に基づいて行っていること。 | ○ | ○ | |
| 2) システム設計書、プログラム設計書の変更は変更箇所を明示していること。 | ○ | ○ | |
| 3) システム設計書、プログラム設計書の旧版を文書管理規定に基づき、 所定 の期間保存しておくこと。 | | ○ | ○ |
| 4) 保守対象システムのドキュメントの変更をユーザ及び保守の責任者の承認を取り付けていること。 | ○ | ○ | |
| 5) 変更内容を文書で明確にすること。 | ○ | ○ | ○ |
| 6) 受注(オフショア)側の責任者は変更内容を文書で確認すること。 | | | ○ |
| (2) プログラムの変更は、保守手順に基づき、保守の責任者の承認を得て実施すること。 | ○ | ○ | |
| 1) 保守担当者<以下に共通>は、プログラムの変更を保守手順に基づいて行っていること。 | ○ | ○ | |
| 2) プログラムの変更を個別保守計画書に基づいて行っていること。 | ○ | ○ | |
| 3) 変更するプログラムは本番に使用しているバージョンのソースをテストライブラリーにコピーしていること。 | ○ | ○ | ○ |
| 4) プログラムの変更について保守の責任者の承認を取り付けていること。 | ○ | | |
| 5) プログラムの変更手順、承認、記録の手順を文書で明確にすること。 | | ○ | ○ |
| 6) 受注(オフショア)側責任者はプログラムの変更手順、承認、記録の手順を文書で確認すること。 | | | ○ |
| (3) 変更したプログラム設計書に基づいてプログラミングしていることを検証すること。 | ○ | ○ | ○ |
| 1) 保守担当者<以下に共通>は、変更が必要なプログラムを漏れなく特定していること。 | ○ | ○ | ○ |
| 2) 変更プログラム設計書を作成していること。 | ○ | ○ | ○ |
| 3) 変更箇所を明示していること。 | ○ | ○ | ○ |
| 4) 変更前のソースを保存していること。 | ○ | ○ | ○ |
| 5) 変更するプログラムの検証手順を事前に明確にしていること。 | ○ | ○ | ○ |
| 6) 変更するプログラムを変更プログラム設計書に基づいてプログラミングしていること。 | ○ | ○ | ○ |
| 7) 変更したプログラム設計書に基づいてプログラミングを検証する手順を確立すること。 | | ○ | ○ |
| 8) 受注(オフショア)側責任者はプログラム設計書に基づいてプログラミングしていることを確認すること。 | | | ○ |
| 4. 保守の確認 | | | |
| (1) 変更したプログラムのテストの実施は、保守のテスト計画に基づいて行うこと。 | ○ | ○ | |
| 1) 保守担当者<以下に共通>は、変更するプログラムを保守のテスト計画に基づいてテストしていること。 | ○ | ○ | |
| 2) テストが保守作業に要求されている変更点を満たしていることを確認していること。 | | ○ | ○ |
| (2) 変更したプログラムは、影響範囲を考慮しテストを行うこと。 | | | |
| 1) 保守担当者<以下に共通>は、変更するプログラムが影響を及ぼす範囲を把握して、関係するソフトウェアとの結合テストを実施していること。 | ○ | ○ | |
| 2) 変更するプログラムの影響範囲外に影響が及んでいないこと。を確認していること。 | ○ | ○ | ○ |
| 3) 保守責任者は、テストマニュアルを保守担当者に周知徹底していること。 | ○ | ○ | ○ |
| 4) 影響範囲として、機能面だけでなく、性能面、信頼性面について考慮すること。 | | ○ | ○ |
| (3) 変更したプログラムのテストは、ユーザが参画し、ユーザマニュアルに基づいて実施すること。 | | | |
| 1) 保守担当者<以下に共通>は、テストに業務に精通したユーザを参画させていること。 | | | |
| 2) ユーザ部門責任者は、テストに参画するユーザにテストの目的を理解させ、自己の役割を十分認識させていること。 | | | |
| 3) ユーザマニュアルに変更が及ぶ場合は、テストに先立ちユーザマニュアルを改訂していること。 | | | |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|--|-----|-----|-----|
| 3) テストをユーザマニュアルに基づいて実施していること。 | | | |
| 4) テスト結果について、ユーザの了承を取っていること。 | | | |
| (4) 変更したプログラムのテストの結果は、ユーザ、運用及び保守の責任者が承認すること。 | | | ○ |
| 1) 保守担当者<以下に共通>は、テスト結果を検証していること。 | | | |
| 2) テスト結果に対するユーザ、保守及び運用の責任者の承認を取り付けていること。 | | | |
| 3) 受注(オフショア)側が関係している場合は受注(オフショア)側の責任者は確認すること。 | | | ○ |
| (5) 変更したプログラムのテストの結果を記録及び保管すること。 | | | |
| 1) 情報システム部門責任者は、テストデータ及びテスト結果の保管期間を定めていること。 | | | |
| 2) 保守責任者<以下に共通>は、テスト時のシステム環境を保管していること。 | | | |
| 3) 保管責任者を定めていること。 | | | |
| 4) 保管責任を負っている保守の担当者は、テストデータ、テスト結果及びテスト環境を所定の期間において保管していること。 | | | |
| 5. 移行 | | | |
| (1) 移行手順は、移行の条件を考慮して作成すること。 | ○ | ○ | ○ |
| 1) 保守の責任者は、移行ルールを定めていること。 | ○ | ○ | |
| 2) 保守担当者<以下に共通>は、移行に当たって、期間、方法、体制等の条件を明確にしていること。 | ○ | ○ | |
| 3) 移行の条件を踏まえた移行手順を移行手順書としてまとめていること。 | ○ | ○ | |
| 4) 移行手順書について、ユーザ、保守及び運用の責任者の承認を取り付けていること。 | ○ | ○ | |
| 5) 受注(オフショア)側は移行手順を十分理解し、責任分担に従って、ソフトウェアの機能面で問題のないことを確認、報告すること。 | ○ | ○ | ○ |
| 6) 受注(オフショア)側は、保守における責任分担に基づいて、移行に伴う関連するシステムへのアクセス権が設定され、承認を経ていること。 | ○ | ○ | ○ |
| (2) 変更前のプログラム及びデータのバックアップを行うこと。 | | | |
| 1) 保守担当者<以下に共通>は、変更前のプログラム、データ及び運用のための諸設定のバックアップを取っていること。 | ○ | ○ | |
| 2) バックアップした内容の戻し方をあらかじめ定めていること。 | ○ | ○ | |
| 3) 旧プログラムに戻す判断基準(フォールバックライテリア)を事前に定めていること。 | ○ | ○ | |
| 4) バックアップの保管期間を定めていること。 | ○ | ○ | |
| 5) 受注(オフショア)側は、保守における責任分担に従って、移行時に必要となる変更前のシステム基盤、システムソフトウェア、プログラム及びデータのバックアップを行うこと | | ○ | ○ |
| (3) 運用及び保守の責任者は、他の情報システムへ影響を与えないことを確認すること。 | ○ | ○ | ○ |
| 1) 保守担当者<以下に共通>は、移行前と移行後の情報システムの機能及び性能を明確にしていること。 | ○ | ○ | |
| 2) 移行時に他のシステムへの影響を運用及び保守の責任者に確認してもらっていること。 | ○ | ○ | |
| 3) 受注(オフショア)側は、運用・保守における責任分担に基づいて、保守移行が他の情報システムへ影響を与えないことを確認、報告すること。 | | ○ | ○ |
| 6. 情報システムの廃棄 | | | |
| (1) 旧情報システムは、リスクを考慮して廃棄計画を策定し、ユーザ、運用及び保守の責任者の承認を得て廃棄すること。 | ○ | | |
| 1) 保守担当者<以下に共通>は、旧情報システムを廃棄すること。によるリスクを評価していること。 | ○ | | |
| 2) 1) で評価したリスクを踏まえて廃棄計画を策定していること。 | ○ | | |
| 3) 廃棄計画を、ユーザ、運用及び保守の責任者の承認を取り付けていること。 | ○ | | |
| 4) 廃棄計画及び廃棄作業をあらかじめ関係者に連絡していること。 | ○ | | |
| (2) 旧情報システムの廃棄方法及び廃棄時期は、不正防止及び機密保護の対策を考慮して決定すること。 | ○ | | |
| 1) 保守担当者<以下に共通>は、廃棄方法及び廃棄時期を明確にしていること。 | ○ | | |
| 2) 廃棄方法を情報システムの機密度や重要性を考慮していること。 | ○ | | |
| 3) 廃棄対象物には、ソフトウェアのみならず、システムドキュメント及びユーザマニュアルも含めていること。 | ○ | | |
| 4) 保守責任者は、廃棄が確実に実行されたことを確認していること。 | ○ | | |
| VI. 共通業務 | | | |
| 1. ドキュメント管理 | | | |
| 1. 1 作成 | | | |
| (1) ドキュメントは、ユーザ部門及び情報システム部門の責任者が承認すること。 | ○ | ○ | ○ |
| 1) 情報システム部門責任者<以下に共通>はドキュメントのレビュー部門、レビュー体制を明確化していること。 | ○ | ○ | |
| 2) ドキュメントのレビュー責任者を明確化していること。 | ○ | ○ | ○ |
| 3) ドキュメントのレビュー部門に、ユーザ部門を含めていること。 | ○ | | |
| 4) ドキュメントレビュー責任者<以下に共通>はドキュメントのレビュー手順およびレビューポイントを明確にしていること。 | ○ | ○ | ○ |
| 5) ドキュメントのレビューを、手順に基づいて行っていること。 | ○ | ○ | ○ |
| 6) ドキュメント作成責任者はドキュメントのレビュー結果を基に、ドキュメントの更新を行っていること。 | ○ | ○ | ○ |
| 7) 情報システム部門およびユーザ部門責任者はドキュメントの内容およびレビュー結果を承認していること。 | ○ | ○ | ○ |
| 8) ドキュメント管理責任者<以下に共通>はドキュメントを、配布リストに基づいて配布していること。 | ○ | ○ | ○ |
| 9) ドキュメント条件及びドキュメントは受発注双方の開発責任者が承認するという規約があること。 | ○ | ○ | ○ |
| 10) 規約に基づき、ドキュメントは受発注開発責任者が承認していること。 | ○ | ○ | ○ |
| (2) ドキュメント作成ルールを定め、遵守すること。 | ○ | ○ | ○ |
| 1) 情報システム部門責任者<以下に共通>はドキュメント管理体制、ドキュメント作成体制を確立していること。 | ○ | | |
| 2) ドキュメント管理責任者、ドキュメント作成責任者およびその役割と権限を、明確化していること。 | ○ | ○ | ○ |
| 3) ドキュメント作成責任者<以下に共通>はドキュメント作成ルールを明文化していること。 | ○ | ○ | ○ |
| 4) ドキュメント作成ルールを、情報戦略に基づいて定めていること。 | ○ | | |
| 5) ドキュメントの作成に必要な体系、作成部門と利用部門、作成手順、レビュー手順、作成要領などをドキュメント作成ルールに定めていること。 | ○ | ○ | ○ |
| 6) 情報システム部門責任者はドキュメント作成ルールを承認していること。 | ○ | | |
| 7) ドキュメント作成責任者<以下に共通>はドキュメント作成ルールを、ドキュメント作成担当者および関係者に周知していること。 | ○ | ○ | ○ |
| 8) ドキュメント作成ルールに従ってドキュメントが作成されていることを確認していること。 | ○ | ○ | ○ |
| 9) 情報システム部門責任者はドキュメント作成ルールの見直しについて、ルール化していること。 | ○ | | |
| 10) ドキュメント作成責任者はドキュメントを磁気ファイルとして作成する場合の機密性、完全性、可用性、見読可能性を確保していること。 | ○ | ○ | ○ |
| 11) ドキュメントの作成条件(日本語の使用などの条件を含む)は明確になっていること。(画面や紙票の表現含む) | ○ | ○ | ○ |
| 12) プログラムソースへの日本語コメントの挿入条件は明確になっていること。 | ○ | ○ | ○ |
| 13) ドキュメントの作成環境は定められていること。(OS、ドキュメント作成ツール等) | ○ | ○ | ○ |
| (3) ドキュメントの作成計画を策定すること。 | ○ | ○ | ○ |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|--|-----|-----|-----|
| 1)ドキュメント作成責任者<以下に共通>はドキュメント作成ルールに基づいて、企画、開発、運用および保守業務に係るドキュメント作成計画を策定していること。 | ○ | | |
| 2)ドキュメント作成計画に、作成するドキュメントの一覧とその作成目的を明記していること。 | ○ | | |
| 3)ドキュメント作成計画に明記されている作成ドキュメントについて、各業務の作業手順と整合させていること。 | ○ | ○ | ○ |
| 4)ドキュメント作成計画に、ドキュメント作成に必要な要員、環境、予算および期間などを明記していること。 | ○ | ○ | ○ |
| 5)ドキュメント作成計画の内容を、開発計画と整合させていること。 | ○ | ○ | ○ |
| 6)企画、開発、運用および保守の責任者はドキュメント作成計画を承認していること。 | ○ | | |
| 7)ドキュメント作成責任者はドキュメント作成計画を、ドキュメント作成担当者および関係者に周知徹底していること。 | ○ | ○ | ○ |
| 8)ドキュメントそれぞれについて、作成する時期、担当者、管理方法、管理ツール、レビューなどの詳細計画を確定すること。 | ○ | ○ | ○ |
| (4)ドキュメントの種類、目的、作成方法等を明確にすること。 | ○ | ○ | ○ |
| 1)ドキュメント作成責任者<以下に共通>はドキュメント作成ルールに基づいて、ドキュメント作成方法(種類、目的、作成方法等)を定めていること。 | ○ | | |
| 2)ドキュメント作成方法を情報システムの形態、作成費用、保守作業、及び再利用などを考慮して定めていること。 | ○ | ○ | ○ |
| 3)ドキュメント作成方法をドキュメント作成担当者に周知徹底していること。 | ○ | ○ | ○ |
| 4)ドキュメント作成ルールに基づいて、作成するドキュメントの種類、体系、目的を明確化し、ドキュメント作成計画に明記していること。 | ○ | ○ | ○ |
| 5)作成するドキュメントの種類およびその作成スケジュールを、開発計画と整合させていること。 | ○ | ○ | ○ |
| 6)ドキュメントの目的に応じて、その配布先、配付形態を明確化していること。 | ○ | | |
| 7)ドキュメント作成ルールで作成が規定されているドキュメントを作成しない場合、その理由を明確にしていること。 | ○ | | |
| 8)ドキュメント体系は定められ、オフショア受注側を含めて周知されていること。 | ○ | ○ | ○ |
| 9)プログラムソースに日本語コメントを含む場合、コメント作成要領や用語は定義されていること。 | | ○ | ○ |
| 10)要求定義、設計仕様、GUI、ソースコードコメント、テスト要領、進捗管理、品質管理、レビュー、検収条件などのドキュメントの種類、目的、作成方法について、元請側と受注(オフショア)側の役割分担は明確になっていること。 | | ○ | ○ |
| (5)ドキュメントは、作成計画に基づいて作成すること。 | | | |
| 1)ドキュメント作成責任者<以下に共通>はドキュメント作成ルールおよび作成計画に基づいて、ドキュメントを作成し | ○ | ○ | ○ |
| 2)ドキュメント作成状況を作成計画に基づいて管理していること。 | ○ | ○ | ○ |
| 3)作成したドキュメントの種類、内容が作成計画と一致しているか確認していること。 | ○ | ○ | ○ |
| 4)ドキュメント作成計画で計画されていたが作成されなかったドキュメントについて、その理由を明確にしていること。 | ○ | | |
| 5)ドキュメント作成計画に対して作成時期の大幅遅延、作成中止、内容変更などがあった場合、その理由を明確にしていること。 | ○ | ○ | ○ |
| 6)ドキュメント作成計画に対して作成時期が大幅に遅延した場合、対応策を講じていること。 | ○ | ○ | ○ |
| 7)ドキュメント作成実績を記録、分析し、次の作成計画の立案の参考にしていること。 | ○ | | |
| 8)作成計画に基づいて作成されていることを元請側及び受注(オフショア)側で途中でモニタリングして確認していること。 | | ○ | ○ |
| 9)工程の区切りごとにレビューを実施していること。 | | ○ | ○ |
| 1.2 管理 | | | |
| (1)ドキュメントの更新内容は、ユーザ部門及び情報システム部門の責任者が承認すること。 | ○ | ○ | ○ |
| 1)情報システム部門責任者<以下に共通>はドキュメントの更新に対するレビュー体制を確立していること。 | ○ | | |
| 2)ドキュメントの更新に対するレビュー体制に、ユーザ部門を含めた関連部門をすべて含めていること。 | ○ | ○ | ○ |
| 3)ドキュメントレビュー責任者<以下に共通>はドキュメントの更新に対するレビュー手順、レビューポイントを明確化していること。 | ○ | ○ | ○ |
| 4)手順に基づいて、ドキュメントの更新に対するレビューを行っていること。 | ○ | ○ | ○ |
| 5)ドキュメントの更新に対するレビュー結果を記録、保管していること。 | ○ | ○ | ○ |
| 6)情報システム部門および利用者部門責任者は更新したドキュメントの内容およびレビュー結果を承認していること。 | ○ | | |
| 7)ドキュメント管理責任者<以下に共通>は変更したドキュメントを、定められた配布リストに基づいて配布していること。 | ○ | | |
| 8)ドキュメントの更新に関する手順は定められ受注(オフショア)側と合意していること。 | | ○ | ○ |
| 9)構成管理プロセスと使用ツールは受注(オフショア)側と発注側とで合意していること。 | | ○ | ○ |
| 10)受注(オフショア)側が実施したドキュメントの更新内容は元請側及び必要に応じてユーザ側の責任者に伝えられ、各責任者が承認していること。 | ○ | ○ | ○ |
| (2)ドキュメント管理ルールを定め、遵守すること。 | ○ | ○ | ○ |
| 1)情報システム部門責任者<以下に共通>はドキュメント管理体制を確立していること。 | ○ | | |
| 2)ドキュメント管理責任者およびその役割と権限を明確化していること。 | ○ | | |
| 3)ドキュメント管理責任者<以下に共通>はドキュメント管理ルールを明文化していること。 | ○ | | |
| 4)ドキュメント管理ルールを、情報戦略と整合させていること。 | ○ | | |
| 5)ドキュメント管理ルールに、ドキュメントの管理責任部署、管理方法、更新・廃棄手順などを明記していること。 | ○ | | |
| 6)情報システム部門責任者はドキュメント管理ルールを承認していること。 | ○ | | |
| 7)ドキュメント管理責任者<以下に共通>はドキュメント管理ルールを、ドキュメント管理担当者および関係者に周知徹底していること。 | ○ | ○ | ○ |
| 8)ドキュメント管理台帳を作成・管理することをルール化していること。 | ○ | ○ | ○ |
| 9)ドキュメント管理台帳に、ドキュメントの最新状況を記録していること。 | ○ | ○ | ○ |
| 10)ドキュメント管理ルールの遵守状況を確認していること。 | ○ | ○ | ○ |
| 11)情報システム部門責任者はドキュメント管理ルールの見直しについて、ルール化していること。 | ○ | | |
| 12)ドキュメント管理責任者はドキュメントを磁気ファイルとして管理する場合の機密性、完全性、可用性、見読可能性を確保していること。 | ○ | | |
| 13)ドキュメントの管理ルールはユーザ側、元請側、受注(オフショア)側を含めて定めていること。 | ○ | ○ | ○ |
| 14)ドキュメントの管理ルールに従い管理されていることをモニタリングで確認していること。 | | ○ | ○ |
| (3)情報システムの変更に伴い、ドキュメントの内容を更新し、更新履歴を記録すること。 | ○ | ○ | ○ |
| 1)ドキュメント管理責任者<以下に共通>は情報システムの変更に伴い影響を受けるドキュメントを明確化していること。 | ○ | | |
| 2)ドキュメントの更新手順および更新時の留意点を明確化していること。 | ○ | | |
| 3)ドキュメントの更新を、ドキュメント管理ルールに基づいて行っていること。 | ○ | | |
| 4)ドキュメントの更新を遅滞なく行っていること。 (情報システムの変更作業が先行し、ドキュメントの更新が後追いになっていないことなどを含む) | ○ | | |
| 5)ドキュメントの更新状況を確認していること。 | ○ | | |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|--|-----|-----|-----|
| 6)ドキュメントの更新履歴を、作成・管理していること。 | ○ | ○ | ○ |
| 7)十分なドキュメント更新履歴をとっていること。 | ○ | ○ | ○ |
| 8)情報システムの変更の影響を受けるドキュメントで受注(オフショア)側が関係するドキュメントを明確にしていること。 | | ○ | ○ |
| 9)ドキュメントが変更になった場合ドキュメントの内容を更新すると共に更新履歴を記録していることを、受注(オフショア)側で確認していること。 | | ○ | ○ |
| (4)ドキュメントの保管、複写及び廃棄は、不正防止及び機密保護の対策を講じていること。 | ○ | ○ | ○ |
| 1)ドキュメント管理責任者<以下に共通>はドキュメントの利用、保管および廃棄についてのルールを明文化していること。 | ○ | | |
| 2)ドキュメントの利用、保管および廃棄ルールを、ドキュメントの種類、形態などを考慮して決めていること。 | ○ | | |
| 3)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を承認していること。 | ○ | | |
| 5)ドキュメントの保管状況、利用状況を定期的に確認していること。 | ○ | | |
| 6)ドキュメント保管場所および保管方法を、セキュリティを確保する上で問題のないものにして | ○ | ○ | ○ |
| ること。 | | | |
| 7)廃棄したドキュメントについて、ドキュメント管理台帳に記録していること。 | ○ | ○ | ○ |
| 8)重要なドキュメント、機密性の高いドキュメントの廃棄方法を、セキュリティを確保する上で問題のないものとして | ○ | ○ | ○ |
| ること。 | | | |
| 9)重要なドキュメント、機密性の高いドキュメントの廃棄に際し、立ち会っていること。 | ○ | ○ | ○ |
| 10)ドキュメントの複写についてのルールを、明文化していること。 | ○ | ○ | ○ |
| 11)複写禁止、複写制限のドキュメントを明確にしていること。 | ○ | ○ | ○ |
| 12)機密性の高いドキュメントの複写を承認していること。 | ○ | ○ | ○ |
| 13)不正複写が発見された場合の処置について、明文化していること。 | ○ | ○ | ○ |
| 14)ドキュメントの複写についての記録をとっていること。 | ○ | ○ | ○ |
| 15)ドキュメントの複写記録、複写状況を定期的に確認していること。 | ○ | ○ | ○ |
| 16)電子ファイル、書類、媒体それぞれに、重要度に応じた管理方法(アクセス権限、責任者、対象者など)を定めていること。 | ○ | ○ | ○ |
| 17)定期的にまた、必要に応じて任意に監査していること。 | ○ | ○ | ○ |
| 18)ドキュメントの複写は不正防止及び機密保護の対策を講じていること。 | | | |
| ①媒体の持ち出し申請と検査、インターネット環境での情報流失の制限をしていること。 | ○ | ○ | ○ |
| ②特に重要な情報は暗号化、透かし等の手段を講じていること。 | | | |
| 19)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じていること。 | | | |
| ①業者に廃棄を依頼する場合、業者の与信調査を実施し、確実な業者を選定していること。 | ○ | ○ | ○ |
| 2. 進捗管理 | | | |
| 2. 1 実施 | | | |
| (1)進捗計画に基づいて方法、体制等を定め、ユーザ、企画、開発、運用及び保守の責任者が承認すること。 | ○ | ○ | ○ |
| 1)進捗管理責任者は進捗管理計画に基づいて進捗管理の実施体制を明確化していること。 | ○ | ○ | ○ |
| 2)ユーザ、企画、開発、運用および保守の責任者は進捗管理の実施体制を承認していること。 | ○ | | |
| 3)情報システム部門責任者はユーザ、企画、開発、運用および保守の進捗管理責任者を定めていること。 | ○ | | |
| 4)進捗管理責任者は進捗管理計画に基づいて進捗管理の方法を明確化していること。 | ○ | ○ | ○ |
| 5)ユーザ、企画、開発、運用および保守の責任者は進捗管理の方法を承認していること。 | ○ | | |
| 6)進捗管理責任者<以下に共通>は進捗管理の方法として、各業務担当者が進捗報告を定期的に行うことを規定していること。 | ○ | ○ | ○ |
| 7)進捗管理の方法として、進捗管理責任者が進捗レビューを定期的に行うことを規定していること。 | ○ | ○ | ○ |
| 8)作業開始時に、進捗管理の体制、方法等を関係者に説明し、周知徹底を図っていること。 | ○ | ○ | ○ |
| 9)進捗管理の体制、方法等を、クリティカルパスを識別し定めていること。 | ○ | ○ | ○ |
| 10)大規模開発の進捗管理では、EVM(EarnedValueManagement)法等による管理も検討していること。 | ○ | | |
| 11)進捗管理要領・使用ツールを明確にし、各責任者が承認していること。 (例えば進捗管理ソフト利用や、進捗度合い評価方法など) | ○ | ○ | ○ |
| 12)進捗管理の対象が明確になっていること。(要件定義書、基本設計書、詳細設計書、ソースコード、試験項目、マニュアル等) | ○ | ○ | ○ |
| 13)進捗管理方法の詳細を受注(オフショア)側が把握していること。 (打ち合わせルール、頻度、内容など) | | | ○ |
| 14)開発プロセスは十分詳細に分類されていること。 | ○ | ○ | ○ |
| 15)開発プロセスに時間要素を含んでいること。 | ○ | ○ | ○ |
| 16)開発プロセス間の順序関係が明確になっていること。 | ○ | ○ | ○ |
| 17)開発管理のドキュメント形式は定められて各責任者で合意されていること | ○ | ○ | ○ |
| 18)開発手順を定めた要領書が出来ていること。 (1)受注管理(発注管理) (2)開発工程管理要領 (2-1)要件定義 (2-2)方式・基本設計 (2-3)詳細設計 (2-4)製造 (2-5)単体テスト (2-6)結合テスト (2-7)総合テスト | ○ | ○ | ○ |
| 19)納入・検収の手順は明確になっていること。 | ○ | ○ | ○ |
| 20)バグ管理方法、バグの定義、件数の定義など詳細に規定されていること。 | ○ | ○ | ○ |
| 21)他のソフトウェアモジュール、特に他社のモジュールに関するバグのカウント方法は明確になっていること。 | | ○ | ○ |
| 22)ハードウェアを含む問題処理管理方法は定義されていること。 | | ○ | ○ |
| 23)進捗を阻害する下記のリスクを考慮していること。(a)スケジュール遅延(b)対象ソフトウェア理解不足(c)コミュニケーション不足(d)対象ソフトウェア品質(e)改造・挿入ソフトウェア品質(f)開発環境整備(g)スキル不足 | | ○ | ○ |
| 24)上記リスクの対応策を進捗管理要領書に明確にしていること。 | | ○ | ○ |
| 25)開発コストを管理し、開発計画全体に影響する場合速やかな対応方法を明確にすること。 (2)ユーザ、企画、開発、運用及び保守責任者は、進捗状況を把握すること。 | ○ | ○ | ○ |
| 1)各業務担当者は定められた方法に基づいて進捗報告を行っていること。 | ○ | ○ | ○ |
| 2)進捗管理責任者<以下に共通>は定められた方法に基づいて進捗レビューを行っていること。 | ○ | ○ | ○ |
| 3)管理項目について進捗状況の目標と実績との差異を分析していること。 | ○ | ○ | ○ |
| 4)ユーザ、企画、開発、運用及び保守責任者に進捗状況の報告を行い、各責任者はその内容を承認していること。 | ○ | | |
| 5)ユーザ、企画、開発、運用及び保守の責任者<以下に共通>は作業の終了の確認方法・判断基準を明確にしていること。 | ○ | | |
| 6)確認方法・判断基準に基づいて作業の終了確認を行っていること。 | ○ | ○ | ○ |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|---|-----|-----|-----|
| 7) 進捗管理責任者<以下に共通>はクリティカルパス上の作業について進捗状況を重点的に把握していること。 | ○ | ○ | ○ |
| 8) 進捗状況に応じてクリティカルパスの変化を認識していること。 | ○ | ○ | ○ |
| 9) 進捗管理方法に従い受発注の責任者は進捗状況を把握し問題あれば対応するなど、具体的に管理していること。 | ○ | ○ | ○ |
| (3) 進捗の遅延等の対策を講じていること。 | ○ | ○ | ○ |
| 1) 進捗管理責任者<以下に共通>は進捗遅延や進捗上の問題が発生した場合の対処体制、対処方法を定めていること。 | ○ | ○ | ○ |
| 2) 進捗遅延や進捗上の問題が発生した場合、定められた体制と手順によって、対処策を検討・策定していること。 | ○ | ○ | ○ |
| 3) 複数の対策案を評価し、最適な対策案を選択していること。 | ○ | ○ | ○ |
| 4) クリティカルパス上の作業進捗の遅延等の対策の優先順位を上げていること。 | ○ | ○ | ○ |
| 5) ユーザ、企画、開発、運用及び保守責任者は対策を承認していること。 | ○ | ○ | ○ |
| 6) 進捗管理責任者<以下に共通>は対策の実施状況を管理していること。 | ○ | ○ | ○ |
| 7) 問題の発見から解決までの過程を記録していること。 | ○ | ○ | ○ |
| 8) 進捗遅延や進捗上の問題への対処策の実施状況および結果を各業務の責任者に報告し、承認を得ていること。 | ○ | ○ | ○ |
| 9) 進捗遅延のチェックは少なくとも週に1回は実施していること。 | ○ | ○ | ○ |
| 10) 遅延の対策について、各責任者及びブリッジSE間で文書を通じて意思の疎通は図られていること。 | ○ | ○ | ○ |
| 11) 遅延の対策は、遅延の原因(稼働不足、技術不足、連絡系統不備、病気など)を分析し、対応する対策を講じていること。 | ○ | ○ | ○ |
| 12) 遅延の原因について、各責任者及びブリッジSE間で合意できていること。 | ○ | ○ | ○ |
| 13) 遅延対策として要員配置など変更する場合、当該要員の現在の業務との関係を明確にし、以降の工程計画への影響を評価すること。 | ○ | ○ | ○ |
| 14) 未完了部分の内容と要因を把握していること。 | ○ | ○ | ○ |
| 15) 未完了部分の内容と状況が次の工程に及ぼす影響を評価していること。 | ○ | ○ | ○ |
| 16) 国際取引先の休日条件を考慮すること。(中国の場合、毎年国务院から休日情報が発表される。元日、春節、清明節、労働節、端午節、国慶節など)但し、企業によっては実際の適用の方法が異なるため、具体的な日にちを確認すること。 | ○ | ○ | ○ |
| 17) 遅延の要因が仕様条件など基本的な問題に起因する場合は全体計画や費用に影響するため速やかに責任者が対応を協議すること。 | ○ | ○ | ○ |
| 2.2 評価 | | | |
| (1) 業務の工程終了時に、計画に対する実績を分析及び評価し、責任者が承認すること。 | ○ | ○ | ○ |
| 1) 情報システム部門責任者は企画、開発、運用及び保守の各工程の終了時点で、計画と作業実績との差異分析および評価を行うことを規定していること。 | ○ | ○ | ○ |
| 2) 進捗管理責任者<以下に共通>は企画、開発、運用及び保守の各工程の終了時点における計画と作業実績との差異分析および評価のための項目を設定していること。 | ○ | ○ | ○ |
| 3) 企画、開発、運用及び保守の各工程の終了時点で、計画と作業実績との差異分析および評価を、規定に基づいて行っていること。 | ○ | ○ | ○ |
| 4) 企画、開発、運用及び保守の各工程の終了時点における計画と作業実績との差異分析および評価の結果を記録していること。 | ○ | ○ | ○ |
| 5) 企画、開発、運用及び保守の各工程の終了時点における計画と作業実績との差異分析および評価の結果を、各業務の責任者に報告し、承認を得ていること。 | ○ | ○ | ○ |
| 6) 企画、開発、運用及び保守の各工程の終了時点における計画と作業実績との差異分析および評価の結果を、関係者に説明していること。 | ○ | ○ | ○ |
| 7) 工程を終了し、次の工程に進める状態が判断基準を明確に定めること。 | ○ | ○ | ○ |
| 8) 次の工程に進める条件を明確に文書で合意すること。 | ○ | ○ | ○ |
| 9) 基本設計、詳細設計、コーディング、単体試験、結合試験、総合試験など、各工程終了時点でレビューを行い、品質の評価を行うこと。 | ○ | ○ | ○ |
| 10) 計画に対する実績の分析評価結果を各責任者が承認していること。 | ○ | ○ | ○ |
| 11) 次の工程に進める場合の条件が有る場合、条件を文書で明確にすること。 | ○ | ○ | ○ |
| (2) 評価結果は、次工程の計画に反映すること。 | ○ | ○ | ○ |
| 1) ユーザ、企画、開発、運用及び保守の責任者<以下に共通>は、前工程の終了時点における計画と作業実績との差異分析および評価結果の内容を理解していること。 | ○ | ○ | ○ |
| 2) 前工程の終了時点における計画と作業実績との差異分析および評価結果から次工程への影響を把握する作業を行っていること。 | ○ | ○ | ○ |
| 3) 前工程の終了時点における計画と作業実績との差異分析および評価結果を基に、次工程の作業計画の見直しを行っていること。 | ○ | ○ | ○ |
| 4) 上記の作業計画の見直しを、明文化していること。 | ○ | ○ | ○ |
| 5) 情報システム部門責任者、及びユーザ部門責任者は作業計画の見直しの報告を受け、承認していること。 | ○ | ○ | ○ |
| 6) ユーザ、企画、開発、運用及び保守の責任者は上記の作業計画の見直しを、関係者に説明し、周知徹底していること。 | ○ | ○ | ○ |
| 7) 受注(オフショア)側責任者は評価結果を次工程の計画に反映する内容を承認していること。 | ○ | ○ | ○ |
| (3) 評価結果は、進捗管理の方法、体制等の改善に反映すること。 | ○ | ○ | ○ |
| 1) 進捗管理責任者<以下に共通>は、各工程終了時点における計画と作業実績との差異分析および評価結果を基に、進捗管理体制、進捗管理の進め方などに関する問題点の明確化を行っていること。 | ○ | ○ | ○ |
| 2) 上記で明確化した問題点に基づいて、進捗管理体制や進捗管理の進め方の改善策を作成し、その有効性を検証していること。 | ○ | ○ | ○ |
| 3) 進捗管理体制や進捗管理の進め方の改善内容を、明文化していること。 | ○ | ○ | ○ |
| 4) 進捗管理体制や進捗管理の進め方の改善内容を、ユーザ、企画、開発、運用及び保守の責任者に報告し、承認を得ていること。 | ○ | ○ | ○ |
| 5) 進捗管理体制や進捗管理の進め方の改善内容を、関係者に周知徹底していること。 | ○ | ○ | ○ |
| 6) 進捗管理体制や進捗管理の進め方の改善内容を、次プロジェクトに役立てるようノウハウとして蓄積していること。 | ○ | ○ | ○ |
| 7) 評価結果は品質強化方法、開発体制改善、進捗管理の方法の改善等に反映すること。 | ○ | ○ | ○ |
| 8) 評価結果に基づく改善は各責任者で合意されていること。 | ○ | ○ | ○ |
| 9) 計画の見直しで費用の変更を伴う場合は所定の手続きにより契約変更を行うこと。 | ○ | ○ | ○ |
| 3. 品質管理 | | | |
| 3.1 計画 | | | |
| (1) 品質目標に基づいて品質管理の計画を定め、ユーザ、企画、開発、運用及び保守の責任者が | ○ | ○ | ○ |
| 1) 情報システム部門責任者は品質管理の責任者を定めていること。 | ○ | ○ | ○ |
| 2) 品質管理責任者<以下に共通>は品質管理計画を明文化していること。 | ○ | ○ | ○ |
| 3) 品質目標が達成されるように品質管理計画を作成していること。 | ○ | ○ | ○ |
| 4) 品質管理計画を情報システムの企画、開発、移行、運用及び保守等の各プロセスに整合させていること。 | ○ | ○ | ○ |
| 5) 品質管理計画を結果の測定が可能な形態で作成していること。 | ○ | ○ | ○ |
| 6) 品質管理計画を全体最適化計画の中で策定される組織体の品質方針と整合させていること。 | ○ | ○ | ○ |
| 7) ユーザ、企画、開発、移行、運用及び保守の責任者は品質管理計画を承認していること。 | ○ | ○ | ○ |
| 8) 品質管理責任者<以下に共通>は品質管理計画を関係者に周知徹底していること。 | ○ | ○ | ○ |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|--|-----|-----|-----|
| 9) 品質管理計画を内外の環境変化に合わせて見直していること。 | ○ | | |
| 10) 品質目標を定量的に定め、各責任者及び受注(オフショア)側で合意されていること。 | ○ | ○ | ○ |
| 11) レビューの方式や体制を明確にすること。 | | ○ | ○ |
| 12) インспекション、レビュー、ウォークスルーなど用語の定義を明確にすること。 | | ○ | ○ |
| 13) 品質目標は、設計、製造、単体試験、結合試験、総合試験などの各工程で具体的に客観的に進捗管理できるレベルで定められていること。 | | ○ | ○ |
| 14) 品質管理の計画を定め、ユーザ、企画、開発、運用、及び保守の責任者及び各責任者とも承認していること。 | | ○ | ○ |
| 15) 各工程終了時点でレビューの十分性を合意するため、レビュー密度(上限と下限)を予め定めること。 | | ○ | ○ |
| 16) レビューの工数を評価し目標と比較して十分性を確認すること。 | | ○ | ○ |
| 17) 工程終了時点の評価では、レビュー密度の結果を評価し、十分なレビューを実施できたか判定すること。 | | ○ | ○ |
| 18) 品質の評価尺度(ソフトウェアの難易度などの特徴を考慮した規模あたりのエラーの上限下限等)を明確にし、判定根拠を客観的に評価すること。 | | ○ | ○ |
| (2) 品質管理計画は、方法、体制等を明確にすること。 | ○ | ○ | ○ |
| 1) 品質管理責任者<以下に共通>は品質管理計画において各段階での管理が有効になるように必要な判断基準及び方法を明確にしていること。 | ○ | | |
| 2) 品質管理計画において各段階での管理の責任と権限を明確にしていること。 | ○ | ○ | ○ |
| 3) 品質管理計画において品質管理のプロセスを監視、測定、分析していること。 | ○ | ○ | ○ |
| 4) 品質管理に必要な資源と情報を配分していること。 | ○ | ○ | ○ |
| 5) 受注(オフショア)側品質管理体制において元請側との連携体制・責任分担を明確にすること | | ○ | ○ |
| 3.2 実施 | | | |
| (1) 業務の工程終了時に、計画に対する実績を分析及び評価し、責任者が承認すること。 | ○ | ○ | ○ |
| 1) 品質管理責任者<以下に共通>は品質目標、評価の基準を明文化していること。 | ○ | | |
| 2) 業務の工程終了時に、計画に対する実績を分析及び評価していること。 | ○ | ○ | ○ |
| 3) ユーザ、企画、開発、移行、運用及び保守の責任者は計画に対する実績の分析及び評価の結果を承認していること。 | ○ | | |
| 4) 品質管理責任者は品質管理記録を作成していること。 | ○ | | |
| 5) 各工程終了時に計画に対する実績を次工程への移行の可否判断の点から分析、評価していること。 | | ○ | ○ |
| 6) 工程終了時点で計画が延長する場合、費用の変更及び契約変更の有無を確認すること。 | | ○ | ○ |
| 7) 契約変更がある場合所定のルールに従い速やかに契約変更を行うこと。 | ○ | ○ | ○ |
| (2) 評価結果は、品質管理の基準、方法、体制等の改善に反映すること。 | ○ | ○ | ○ |
| 1) 品質管理責任者<以下に共通>は評価結果に基づく改善を実施していること。 | ○ | ○ | ○ |
| 2) 改善の責任者、担当者の役割と責任を決めていること。 | ○ | ○ | ○ |
| 3) 改善の責任者から改善結果の報告を受けていること。 | ○ | ○ | ○ |
| 4) 評価結果に基づき品質管理の基準、方法、体制等を見直していること。 | ○ | ○ | ○ |
| 5) 受注(オフショア)側見直し結果について受注側責任者は承認をしていること。 | | | ○ |
| 4. 人的資源管理 | | | |
| 4.1 責任・権限 | | | |
| (1) 要員の責任及び権限は、業務の特性及び業務遂行上の必要性に応じて定めること。 | ○ | ○ | ○ |
| 1) 情報システム部門の責任者<以下、共通>は、企画、開発、運用、保守の責任者を規程等で明文化していること。 | ○ | | |
| 2) 職務分担を定めるのに先立ち、業務の特性、業務遂行上の必要性など、職務分析を適切に実施していること。 | ○ | | |
| 3) 各管理責任者の職務分担を明確に定め、相互の整合性を確保していること。 | ○ | | |
| 4) 要員の責任及び権限を、能力及び経験を踏まえて定めていること。 | ○ | ○ | ○ |
| 5) 定めた職務分担、権限を、組織的に承認していること。 | ○ | ○ | ○ |
| 6) 各責任者、ブリッジSE、各チームのリーダーなどの責任と権限は明確になっていること。 | ○ | ○ | ○ |
| 7) 要件定義、基本設計、詳細設計、製造、試験、総合試験などの各工程の責任者と権限が明確になっていること。 | ○ | ○ | ○ |
| (2) 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。 | ○ | ○ | ○ |
| 1) 情報システム部門の責任者<以下、共通>は、どのような場合に要員の責任及び権限を見直すのか、見直しのルールを定めていること。 | ○ | | |
| 2) 見直しの判断基準を、業務環境及び情報環境の変化に対応するように、明確にしていること。 | ○ | ○ | ○ |
| 3) 見直し範囲、見直し時期を明確にしていること。 | ○ | ○ | ○ |
| 4) 見直しがルールに基づいて行われることを明確にしていること。 | ○ | ○ | ○ |
| 5) 見直しの結果を、組織的に承認していること。 | ○ | ○ | ○ |
| 6) 要員に変化があった場合、その原因について検討し今後の再発の評価・対策を検討すること。 | | ○ | ○ |
| (3) 要員の責任及び権限を周知徹底すること。 | ○ | ○ | ○ |
| 1) 情報システム部門の責任者<以下、共通>は、要員の責任及び権限の周知徹底の方法をルールに定めていること。 | ○ | | |
| 2) 周知方法、周知対象、周知時期を明文化していること。 | ○ | ○ | ○ |
| 3) 要員交替時や組織変更時など適切な時期に周知徹底していること。 | ○ | ○ | ○ |
| 4) 個々の要員の理解を確認していること。 | ○ | ○ | ○ |
| 5) 変更する場合、関連する要員に連絡していること。 | ○ | ○ | ○ |
| 4.2 業務遂行 | | | |
| (1) 要員は、権限を遵守すること。 | ○ | ○ | ○ |
| 1) 企画、開発、運用、保守の責任者<以下、共通>は、要員の職務遂行状況を把握するルールを定めていること。 | ○ | | |
| 2) 要員の職務遂行状況報告書式を定めていること。 | ○ | ○ | ○ |
| 3) 要員が権限を遵守するよう相互に牽制が機能するようにしていること。 | ○ | ○ | ○ |
| 4) 要員がルールに基づいて職務遂行状況の報告書を作成するようにしていること。 | ○ | ○ | ○ |
| 5) 要員からの報告書をもとに職務遂行状況をレビューしていること。 | ○ | ○ | ○ |
| 6) 受注(オフショア)側責任者は要員の業務実行について、日報、週間報告、月報告など文書を通じて明確に把握を行うこと。 | | | ○ |
| (2) 作業分担及び作業量は、要員の知識、能力等から検討すること。 | ○ | ○ | ○ |
| 1) 企画、開発、運用、保守の責任者<以下、共通>は、要員の作業分担及び作業量を定めるルールを定めていること。 | ○ | | |
| 2) 要員の知識、能力等を評価していること。 | ○ | ○ | ○ |
| 3) 評価に基づき、作業分担及び作業量を見直していること。 | ○ | ○ | ○ |
| 4) 特定要員への作業集中の有無について見直していること。 | ○ | ○ | ○ |
| 5) 作業内容・質・量に関する要員の不満や悩みがないかモニタリングすること。 | | | ○ |
| (3) 要員の交替は、誤りや防止、不正防止及び機密保護を考慮して行うこと。 | ○ | ○ | ○ |
| 1) 企画、開発、運用、保守の責任者<以下、共通>は、要員の交替時の引継ぎルールを定めていること。 | ○ | | |
| 2) 要員の交替時は、アクセス権限を管理し、誤りや防止、不正防止の方法を定めて運用していること。 | ○ | ○ | ○ |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|---|-----|-----|-----|
| 3) 要員の交替時は、機密保護及び個人情報保護の方法を定めて運用していること。 | ○ | ○ | ○ |
| 4) 要員が引継ぎ内容を文書で確認するように業務引継書を定めて運用していること。 | ○ | ○ | ○ |
| 5) 要員の交替に関する誤謬防止、不正防止及び機密保護のための国際取引を考慮した契約があること。 | | | ○ |
| (4) 不測の事態に備えた交替要員の確保を検討すること。 | ○ | ○ | ○ |
| 1) 企画、開発、運用、保守の責任者<以下、共通>は、不測の事態に備えた交替要員確保のルールを定めていること。 | ○ | | |
| 2) 不測の事態における交替要員の確保のルールを定めていること。 | ○ | ○ | ○ |
| 3) 交替要員を確保するまでの臨時措置を定めていること。 | ○ | ○ | ○ |
| 4) 交通経路、宿泊施設を検討していること。 | ○ | ○ | ○ |
| 5) 不測の事態に備えた国際取引先の代替要員の確保に関する配慮があることを契約で明記すること。 | | | ○ |
| 4. 3 教育・訓練 | | | |
| (1) 教育及び訓練に関する計画及びカリキュラムは、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。 | ○ | | |
| 1) 教育及び訓練の責任者<以下、共通>は、教育及び訓練に関する計画及びカリキュラム策定ルールを定めていること。 | ○ | | |
| 2) 計画及びカリキュラムについて、人的資源管理方針やキャリアパスに基づき、作成及び見直しを行っていること。 | ○ | | |
| 3) 情報戦略の策定に必要な知識及び能力の習得を、計画及びカリキュラムに反映していること。 | ○ | | |
| 4) カリキュラムが組織的に承認されるようにしていること。 | ○ | | |
| 5) 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。 | ○ | ○ | ○ |
| 6) 開発に必要な特殊技術が受注(オフショア)側に必要な場合その教育の計画を立てていること。 | | ○ | ○ |
| 7) 品質管理や進捗管理のルールに関する教育計画を考慮すること。 | | ○ | ○ |
| 8) 受注(オフショア)側要員に対するコミュニケーション教育の環境が整っていること。 | | | ○ |
| 9) 受注(オフショア)側要員に対するコミュニケーション研修に技術日本語を含むこと。 | | | ○ |
| (2) 教育及び訓練に関する計画及びカリキュラムは、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。 | ○ | ○ | ○ |
| 1) 教育及び訓練の責任者<以下、共通>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必要な技術力の向上、業務知識の習得をカリキュラムに体系化していること。 | ○ | | |
| 2) カリキュラムにおいて、情報システムの情報セキュリティ確保にかかわる教育を行っていること。 | ○ | ○ | ○ |
| 3) カリキュラムにおいて、個人情報保護にかかわる教育を行っていること。 | ○ | ○ | ○ |
| 4) カリキュラムにおいて、情報倫理にかかわる教育を行っていること。 | ○ | ○ | ○ |
| 5) ソフトウェア開発スキル、SEスキル、マネジメントスキルなど、各分野の力量は分類整理されていること。 | | ○ | ○ |
| (3) 教育及び訓練は、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。 | ○ | ○ | ○ |
| 1) 教育及び訓練の責任者<以下、共通>は、教育及び訓練を定期的かつ効果的に行っていること。 | | | |
| 2) 教育及び訓練の実施の効果を評価していること。 | ○ | ○ | ○ |
| 3) カリキュラムの有効性を定期的に評価していること。 | ○ | ○ | ○ |
| 4) 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ーを、必要な経験及び知識を備えている者としていること。 | ○ | ○ | ○ |
| 6) 進捗管理手順、品質管理規程、報告形式など十分教育すること。 | | ○ | ○ |
| 7) 要員変更に伴う新人が配属された場合、当該新人への教育を行うこと。 | | | ○ |
| 8)ブリッジEに対して異文化間のコミュニケーション方法の教育を行うこと。 | | | ○ |
| (4) 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。 | ○ | ○ | ○ |
| 1) 教育及び訓練の責任者<以下、共通>は、情報戦略、業務環境及び情報環境に基づいたキャリアパスを確立していること。 | ○ | | |
| 2) キャリアパスを要員に周知徹底していること。 | ○ | | |
| 3) 情報戦略や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。 | ○ | | |
| 4) 教育を行う場合、受講生の受講後の業務遂行に関して、例えば3年間は関連業務を行うこと、行わない場合は教育経費の返還を行うことなどのアフターフォローの考慮はあること。 | | | ○ |
| 5) 職員の流動性や定着性に対する考慮や契約があること。 | | ○ | ○ |
| 6) 研修終了後の待遇措置などキャリアパスを考慮していること。(研修後の戦力期間確保対策) | | | ○ |
| 4. 4 健康管理 | | | |
| (1) 健康管理を考慮した作業環境を整えること。 | ○ | ○ | ○ |
| 1) 健康管理の責任者<以下、共通>は、健康管理を考慮した作業環境が適切に維持されるようにしていること。 | ○ | | |
| 2) オフィススペースが適切に確保され什器及び備品が適切に配置されるようにしていること。 | ○ | ○ | ○ |
| 3) VDT作業対策や採光・照明、換気・空調等が講じられるようにしていること。 | ○ | ○ | ○ |
| 4) 休憩のための施設が確保されるようにしていること。 | ○ | ○ | ○ |
| 5) 受動喫煙防止の対策が立てられているようにしていること。 | ○ | ○ | ○ |
| (2) 健康診断及びメンタルヘルスクアを行うこと。 | ○ | ○ | ○ |
| 1) 健康管理の責任者<以下、共通>は、要員の担当業務の特性を踏まえた健康診断やメンタルヘルスクアが定期的に行われるようにしていること。 | ○ | ○ | ○ |
| 2) 必要な予防管理体制を確立していること。 | ○ | ○ | ○ |
| 3) 要員がカウンセリングを受けやすくしていること。 | ○ | ○ | ○ |
| 4) 健康診断又はカウンセリングの結果に基づいた必要な対策が講じられるようにしていること。 | ○ | ○ | ○ |
| 5. 委託・受託 | | | |
| 5.1 計画 | | | |
| (1) 委託又は受託の計画は全体最適化計画に基づいて策定し、責任者が承認すること。 | ○ | ○ | ○ |
| 1) 情報システム部門責任者は委託又は受託の責任者を定めていること。 | ○ | | |
| 2) 委託又は受託の責任者<以下に共通>は委託又は受託計画の立案手順を定めていること。 | ○ | ○ | ○ |
| 3) 委託又は受託計画を外部資源の活用方針など全体最適化計画に基づいて策定していること。 | ○ | | |
| 4) 委託又は受託計画について関係者の合意を得ていること。 | ○ | | |
| 5) 状況の変化に応じて、委託又は受託計画を見直していること。 | ○ | | |
| 6) 情報システム部門責任者は委託又は受託の計画を承認していること。 | ○ | | |
| 7)発注側、元請側、受注(オフショア)側それぞれの責任者が計画を承認すること。 | ○ | ○ | ○ |
| (2) 委託又は受託の目的、対象範囲、予算、体制等を明確にすること。 | ○ | ○ | ○ |
| 1) 委託又は受託の責任者<以下に共通>は委託又は受託の目的、対象範囲、予算、体制等を明確にしていること。 | ○ | ○ | ○ |
| 2) 委託又は受託の目的、対象範囲、予算、体制等について関係者の合意を得ていること。 | ○ | ○ | ○ |
| 3) 委託範囲を委託先に対し書面などにより正確に伝えていること。 | ○ | ○ | ○ |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|--|-----|-----|-----|
| 4)発注側、元請側、受注(オフショア)側それぞれ目的、対象範囲、予算、体制等を明確にすること。 | ○ | ○ | ○ |
| 5)発注側と元請側は目的、対象範囲、費用、体制を相互に承認すること。 | ○ | ○ | ○ |
| 6)元請側と受注(オフショア)側は目的、対象範囲、費用、体制を相互に承認すること。 | ○ | ○ | ○ |
| 7)元請側は国際取引に関連するリスクを分析し対応策を検討し決定すること。 | ○ | ○ | ○ |
| (3) 委託又は受託は、具体的な効果、問題点等を評価して決定すること。 | | | |
| 1)委託又は受託の責任者は委託又は受託の効果、問題点、リスク等を外部資源の活用方針など全体最適化計画に照らし検討していること。 | | | |
| 2)関係者は上記検討に参画していること。 | | | |
| 3)委託又は受託の責任者は上記検討結果を委託又は受託計画等に反映していること。 | | | |
| 5.2 委託先選定 | | | |
| (1) 委託先の選定基準を明確にすること。 | ○ | ○ | ○ |
| 1)委託の責任者<以下に共通>は委託先の選定基準を明文化し、企画、開発、運用及び保守の責任者の承認を得ていること。 | ○ | ○ | ○ |
| 2)委託計画と整合性をとって選定基準を定めていること。 | ○ | ○ | ○ |
| 3)選定基準として客観的な指標を定めていること。 | ○ | ○ | ○ |
| 4)委託業務の特性を考慮し選定基準を定めていること。 | ○ | ○ | ○ |
| 5)事業継続計画を考慮し選定基準を定めていること。 | ○ | ○ | ○ |
| 6)選定基準を満たす企業等から委託候補先を選定していること。 | ○ | ○ | ○ |
| 7)選定基準の中に国際取引に関する経験や実績の評価を加えること。 | ○ | ○ | ○ |
| 8)ブリッジSEの能力を評価すること。 | ○ | ○ | ○ |
| 9)評価項目として、ヒューマンスキル、技術スキル、コミュニケーションスキル、文化理解を含めることが好ましい。 | ○ | ○ | ○ |
| 10)会社選定の評価項目としてオフショア開発管理規準に対応したチェック項目を選定することが好ましい。 | ○ | ○ | ○ |
| (2) 委託候補先に必要な要求仕様を提示すること。 | ○ | ○ | ○ |
| 1)委託の責任者<以下に共通>は委託目的、対象範囲、予算、体制等委託方針に基づいて要求仕様を作成していること。 | ○ | ○ | ○ |
| 2)要求仕様において、委託目的、委託範囲、委託業務に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。 | ○ | ○ | ○ |
| 3)提案依頼書(RFP:Request for Proposal)を候補ベンダーに提示すること。 | ○ | ○ | ○ |
| 4)RFPにはシステムの目的、開発期限、ハードウェア条件、機能条件、依頼事項、契約事項などを明記すること。 | ○ | ○ | ○ |
| 5)新たなプロジェクトに取り組む場合で直ちにRFPの作成が困難な場合に、必要な情報を求めるためRFI(Request for Information)の発出を考慮すること。 | ○ | ○ | ○ |
| (3) 委託候補先が提示した提案書の比較検討を行うこと。 | ○ | ○ | ○ |
| 1)委託の責任者<以下に共通>は委託先選定基準に基づいて、委託候補先の提案書を比較検討していること。 | ○ | ○ | ○ |
| 2)委託先選定基準に基づき委託先の決定理由を明確にしていること。 | ○ | ○ | ○ |
| 3)ユーザ、企画、開発、運用、保守、災害対策の責任者など関係者は比較検討の結果を承認していること。 | ○ | ○ | ○ |
| 5.3 契約 | | | |
| (1) 契約は、委託契約ルール又は受託契約ルールに基づいて締結すること。 | ○ | ○ | ○ |
| 1)委託又は受託の責任者は委託契約ルール又は受託契約ルールを定めていること。 | ○ | ○ | ○ |
| 2)委託又は受託の担当者は委託契約ルール又は受託契約ルールに基づいて契約書を作成していること。 | ○ | ○ | ○ |
| 3)委託又は受託の責任者<以下に共通>は法的要件を満たしていることも確認し契約書を承認していること。 | ○ | ○ | ○ |
| 4)契約書の内容を関係者に周知徹底していること。 | ○ | ○ | ○ |
| (2) コンプライアンスに関する条項を明確にすること。 | ○ | ○ | ○ |
| 1)委託又は受託の責任者<以下に共通>は委託契約又は受託契約に情報セキュリティ条項として不正防止、機密保護等の対策を定めていること。 | ○ | ○ | ○ |
| 2)委託契約又は受託契約に委託者、受託者の責任範囲を明確に規定していること。 | ○ | ○ | ○ |
| 3)委託元の組織体の社内規程に準ずる管理が委託先でも実施されることの必要性を検討し、その結果を契約に反映していること。 | ○ | ○ | ○ |
| 4)受注(オフショア)側と日本側の両国で関連する法律、基準、ガイドライン、契約など、明確にすること。 | ○ | ○ | ○ |
| 5)国際紛争解決に備え、調停裁判所を明記すること。 | ○ | ○ | ○ |
| (3) 再委託の可否について明確にすること。 | ○ | ○ | ○ |
| 1)委託又は受託の責任者<以下に共通>は委託契約書又は受託契約書で再委託の可否を明確にしていること。 | ○ | ○ | ○ |
| 2)再委託先に対する監督責任を明確にしていること。 | ○ | ○ | ○ |
| 3)再委託先の機密保持、再々委託の可否等セキュリティ上の制約条件等を明確にしていること。 | ○ | ○ | ○ |
| (4) 知的財産権の帰属を明確にすること。 | ○ | ○ | ○ |
| 1)組織体の長は知的財産権の管理の責任者を定めていること。 | ○ | ○ | ○ |
| 2)委託又は受託の責任者は知的財産権の保護方針に基づきプログラム、データ及びドキュメントの知的財産権の帰属を明確にしていること。 | ○ | ○ | ○ |
| 3)委託の責任者は著作権等知的財産権の侵害についての委託元の委託先に対する管理責任について委託契約書に明確にしているか。 | ○ | ○ | ○ |
| (5) 特約条項及び免責条項を明確にすること。 | ○ | ○ | ○ |
| 1)委託又は受託の責任者<以下に共通>は問題の発生が想定される事項を明確にしていること。 | ○ | ○ | ○ |
| 2)想定した問題事項に対する対応策を、委託方針・受託方針等に基づき明確にしていること。 | ○ | ○ | ○ |
| 3)想定した問題事項に対する必要な特約条項及び免責条項を契約書で明確にしていること。 | ○ | ○ | ○ |
| (6) 業務内容及び責任分担を明確にすること。 | ○ | ○ | ○ |
| 1)委託又は受託の責任者<以下に共通>は委託又は受託業務の内容、責任分担を契約書、又は仕様書に明記していること。 | ○ | ○ | ○ |
| 2)作業の変更、追加についての取扱いを契約書、又は仕様書に明記していること。 | ○ | ○ | ○ |
| 3)内容に疑義が生じた場合の取扱いを契約書、又は仕様書に明記していること。 | ○ | ○ | ○ |
| (7) 契約締結後の業務内容に追加及び変更が生じた場合、契約内容の再検討を行うこと。 | ○ | ○ | ○ |
| 1)委託又は受託の責任者<以下に共通>は追加される作業、変更される作業内容を明確にしていること。 | ○ | ○ | ○ |
| 2)追加される作業、変更される作業内容を変更契約書、変更仕様書に明確にし、管理していること。 | ○ | ○ | ○ |
| (8) システム監査に関する方針を明確にすること。 | ○ | ○ | ○ |
| 1)委託又は受託の責任者<以下に共通>は委託元の委託先監督の一環として、契約でシステム監査実施の方針を定めていること。 | ○ | ○ | ○ |
| 2)システム監査の実施方針に対象範囲、適用する基準、実施時期、コスト負担、協力義務等を明確にしていること。 | ○ | ○ | ○ |
| 3)システム監査の結果の取扱いに関する責任、義務を明確にしていること。 | ○ | ○ | ○ |
| 5.4 委託業務 | | | |
| (1) 委託業務の実施内容は、契約内容と一致すること。 | ○ | ○ | ○ |
| 1)委託先の責任者、担当者は契約で定めた委託業務の内容を実施していること。 | ○ | ○ | ○ |
| 2)委託の責任者<以下に共通>は委託業務の実施内容を把握していること。 | ○ | ○ | ○ |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|---|-----|-----|-----|
| 3)委託業務の実施内容と契約内容の整合を確認し、相違点について適切な措置を講じていること。 | ○ | ○ | ○ |
| (2) 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。 | ○ | ○ | ○ |
| 1)委託の責任者<以下に共通>は委託契約書、委託仕様書に基づき、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、担当者を定めていること。 | ○ | ○ | ○ |
| 3)資料等提供のルールを定めていること。 | ○ | ○ | ○ |
| 4)資料等提供のルールに提供、変換、廃棄等の方法を明確にしていること。 | ○ | ○ | ○ |
| 5)提供資料は記録として管理すること。 | ○ | ○ | ○ |
| 6)提供形態(紙、ディスク等の使用メディア)を明確に定めること。 | ○ | ○ | ○ |
| 7)ネットワークを介して国際転送する場合、暗号化など、転送手段を明確にすること。 | ○ | ○ | ○ |
| (3) 委託状況の進捗状況を把握し、遅延に対する措置を講じていること。 | ○ | ○ | ○ |
| 1)委託の責任者<以下に共通>は委託業務の進捗状況を定期的に把握していること。 | ○ | ○ | ○ |
| 2)問題点の原因を究明し、適切な措置を講じていること。 | ○ | ○ | ○ |
| 3)遅延の原因を分析し再発防止対策を明確にすること。 | ○ | ○ | ○ |
| 4)対策を講じた場合の他の開発作業への評価を行ない、全体的な影響がないことを確認すること。 | ○ | ○ | ○ |
| 5)受発注双方の合意を確認すること。 | ○ | ○ | ○ |
| (4) 委託先における誤謬防止、不正防止、機密保護等の対策の実施状況を把握し、必要な措置を講 | ○ | ○ | ○ |
| 1)委託先の責任者は誤謬防止、不正防止、機密保護等の対策の実現方法を明確にしていること。 | ○ | ○ | ○ |
| 2)委託の責任者<以下に共通>は委託先での誤謬防止、不正防止、機密保護等の対策の実現方法を把握していること。 | ○ | ○ | ○ |
| 3)誤謬防止、不正防止、機密保護等の対策の実現状況に応じて、必要な改善措置を講じていること。 | ○ | ○ | ○ |
| 4)委託先の責任者が不正防止、機密保護にかかわる担当者との誓約書を取り交わしていることを確認していること。 | ○ | ○ | ○ |
| 5)情報セキュリティ対策内容を合意すること。 | ○ | ○ | ○ |
| 6)情報セキュリティ国際標準のISO/IEC27001を取得していることが望ましい。 | ○ | ○ | ○ |
| (5) 成果物の検収は、委託契約に基づいて行うこと。 | ○ | ○ | ○ |
| 1)委託の責任者<以下に共通>は委託物の検収方法を定めていること。 | ○ | ○ | ○ |
| 2)委託契約との関係から判断し妥当な内容の検収基準を定めていること。 | ○ | ○ | ○ |
| 3)委託の担当者は検収方法に基づいて成果物の検収を実施していること。 | ○ | ○ | ○ |
| 4)委託の責任者<以下に共通>は検収結果が検収基準を満たしていない場合の対応を明確にしていること。 | ○ | ○ | ○ |
| 5)再納品が行われた場合の再検収の手続きを定めていること。 | ○ | ○ | ○ |
| 6)検収結果を承認していること。 | ○ | ○ | ○ |
| (6) 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。 | ○ | ○ | ○ |
| 1)委託の責任者<以下に共通>は委託業務で提供したデータ資料等の回収、廃棄の方法・手順を定めていること。 | ○ | ○ | ○ |
| 2)委託業務で提供したデータ資料等の回収、廃棄の確認方法を定めていること。 | ○ | ○ | ○ |
| 3)回収、廃棄の報告を承認していること。 | ○ | ○ | ○ |
| (7) 委託した業務の結果を分析及び評価すること。 | ○ | ○ | ○ |
| 1)委託の担当者は委託業務の実施結果を分析及び評価していること。 | ○ | ○ | ○ |
| 2)委託の責任者<以下に共通>は委託業務の実施結果を分析及び評価結果を承認していること。 | ○ | ○ | ○ |
| 3)関係者に委託業務の実施結果の評価を報告していること。 | ○ | ○ | ○ |
| 5.5 受託業務 | | | |
| (1) 受託業務の実施内容は、契約内容を遵守すること。 | ○ | ○ | ○ |
| 1)受託の担当者は契約の定めに従って受託業務を実施していること。 | ○ | ○ | ○ |
| 2)受託の責任者<以下に共通>は受託業務の遂行状況を把握していること。 | ○ | ○ | ○ |
| 3)受託業務の実施内容と契約内容に相違がある場合、適切な措置を講じていること。 | ○ | ○ | ○ |
| (2) 受託内容の進捗状況を把握し、リスク対策を講じていること。 | ○ | ○ | ○ |
| 1)受託の責任者<以下に共通>は、進捗状況を把握していること。 | ○ | ○ | ○ |
| 2)進捗が遅延している場合、原因を究明し適切な措置を講じていること。 | ○ | ○ | ○ |
| 3)対策を講じた場合の他の開発作業への評価を行ない、全体的な影響がないことを確認すること。 | ○ | ○ | ○ |
| (3) 成果物の品質管理を行うこと。 | ○ | ○ | ○ |
| 1)受託の責任者<以下に共通>は成果物の品質基準を受託契約に基づき明確にしていること。 | ○ | ○ | ○ |
| 2)品質基準を満たすように受託側の品質管理方針に基づいて成果物の品質を管理していること。 | ○ | ○ | ○ |
| 3)成果物の品質管理結果を改善に反映していること。 | ○ | ○ | ○ |
| 4)品質管理は本基準の共通業務「品質管理」に準じて行うこと。 | ○ | ○ | ○ |
| (4) 契約に基づき、受託業務終了後、提供されたデータ、資料、機材等を返却又は廃棄すること。 | ○ | ○ | ○ |
| 1)受託の責任者<以下に共通>はデータ、資料等の返却、廃棄の方法を明確にしていること。 | ○ | ○ | ○ |
| 2)受託業務で提供されたデータ資料等の返却、廃棄の確認の方法を明確にしていること。 | ○ | ○ | ○ |
| 3)返却、廃棄の報告を承認していること。 | ○ | ○ | ○ |
| 6. 変更管理 | | | |
| 6.1 管理 | | | |
| (1) 変更管理ルールを定め、ユーザ、開発及び保守の責任者が承認すること。 | ○ | ○ | ○ |
| 1) 変更の責任者<以下、共通>は、変更管理ルール及び変更手順書等を規定し、ユーザ、開発及び保守の責任者の承認がなされるようにしていること。 | ○ | ○ | ○ |
| 2) 変更管理ルールにおいて、情報システムの運用形態が考慮されるようにしていること。 | ○ | ○ | ○ |
| 3) 変更手順書が変更管理ルールに基づいて作成されるようにしていること。 | ○ | ○ | ○ |
| 4) 変更担当者を定めていること。 | ○ | ○ | ○ |
| 5) 変更管理ルール及び変更手順書を関係者に周知徹底していること。 | ○ | ○ | ○ |
| 6) 変更管理のレビューを行い、変更管理ルール及び変更手順書を見直していること。 | ○ | ○ | ○ |
| 7) 変更管理の対象を明確に定めること。 | ○ | ○ | ○ |
| 8)変更管理の対象は、仕様書、基本設計書、詳細設計書、ファイル、試験項目など、ドキュメントとして明確にしているもの全てを対象とすることが好ましい。 | ○ | ○ | ○ |
| 9)変更管理の記録を保持すること。 | ○ | ○ | ○ |
| (2) 仕様変更、問題点、ペンディング事項等の変更管理案件が生じた場合、他システムの影響を考慮して決定すること。 | ○ | ○ | ○ |
| 1) 変更の責任者<以下、共通>は、仕様変更、問題点、ペンディング事項等の変更管理案件を決定していること。 | ○ | ○ | ○ |
| 2) 変更管理案件の対処を、他システムの影響を考慮して決定していること。 | ○ | ○ | ○ |
| 3) 変更管理案件が、変更管理ルールや手順書に基づき処理されるようにしていること。 | ○ | ○ | ○ |
| 4) 開発途中の変更管理は、仕様、設計書、ソースコード、試験項目など、関連する事項とのトレーサビリティを有すること。 | ○ | ○ | ○ |
| (3) 変更管理案件は、提案から完了までの状況を管理し、未完了案件は定期的に分析すること。 | ○ | ○ | ○ |
| 1) 変更の責任者<以下、共通>は、提案から完了までの状況を管理していること。 | ○ | ○ | ○ |
| 2) 未完了案件を、定期的に分析していること。 | ○ | ○ | ○ |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|--|-----|-----|-----|
| 3) 変更管理ルールに基づいて進捗管理を実施していること。 | ○ | | |
| 6. 2 実施 | | | |
| (1) 変更管理案件は、変更管理ルールに従って実施すること。 | ○ | | |
| 1) 変更の責任者<以下、共通>は、変更管理ルールや変更手順書に従って変更管理及びレビューを行っていること。 | | | |
| 2) 変更手順書によりスケジュールを作成し、進捗管理を行っていること。 | ○ | | |
| (2) 変更管理案件を実施した場合に、関連する情報システムの環境も同時に変更すること。 | ○ | | |
| 1) 変更の管理責任者<以下、共通>は、変更管理案件を実施した場合に、関連する情報システムの環境も同時に変更されるようにしていること。 | ○ | | |
| 2) 変更手順書により、関連する情報システム環境の変更スケジュールを作成し、進捗管理を行っていること。 | ○ | | |
| 3) 変更管理案件の規模、システム特性等を確認していること。 | ○ | | |
| (3) 変更の結果は、ユーザ、開発、運用及び保守の責任者が承認すること。 | ○ | | |
| 1) 変更の責任者<以下、共通>は、変更の結果が、ユーザ、開発、運用、保守の責任者の承認を得られるようにしていること。 | ○ | | |
| 2) 変更管理ルール及び変更手順書により、変更担当者の役割と責任を定めていること。 | ○ | | |
| 3) 変更の担当者を定めていること。 | ○ | | |
| 4) 変更を実施し、変更結果は、ユーザ、開発、運用及び保守の責任者の承認を得るようにしていること。 | ○ | | |
| 7. 災害対策 | | | |
| 7. 1 リスク分析 | | | |
| (1) 地震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 | ○ | | |
| 1) 情報システム部門責任者<以下、本項に共通>は、リスク分析を行っていること。 | ○ | | |
| 2) リスク分析の範囲として立地条件や業種、業態およびシステム化レベルを勘案していること。 | ○ | | |
| 3) 地震、台風、豪雨、豪雪、竜巻、洪水、高潮等、すべての自然災害を想定するとともに、テロ等による破壊も含めていること。 | ○ | | |
| 4) 被災の規模は、最大規模(例えば、地震の場合は、震度7レベル)を想定していること。 | ○ | | |
| 5) 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。 | ○ | | |
| 6) 次回見直しタイミングを含む将来を考慮した影響範囲を想定していること。 | ○ | | |
| (2) 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 | | | |
| 1) 情報システム部門責任者<以下、本項に共通>は、情報システムが停止したときにどのような影響があるかを損害状況の程度に応じて分析していること。 | ○ | | |
| 2) 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。 | ○ | | |
| 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。 | ○ | | |
| (3) 業務の回復許容時間及び回復優先順位を定めること | ○ | | |
| 1) CIOまたは情報システム部門責任者<以下、本項に共通>は、業務の回復許容時間及び回復優先順位を定めていること。 | ○ | | |
| 2) リスク分析の結果から判断して妥当な回復許容時間及び回復優先順位の設定をしていること。 | ○ | | |
| 3) 回復許容時間及び回復優先順位の設定は、業務の重要性、緊急性、影響範囲を考慮していること。 | ○ | | |
| 4) 回復許容時間及び回復優先順位の設定は、他の業務との整合性並びに実現可能性を考慮していること。 | ○ | | |
| 5) 回復許容時間及び回復優先順位の設定理由を明確にしていること。 | ○ | | |
| 6) 回復許容時間及び回復優先順位を関係者が合意していること。 | ○ | | |
| 7. 2 災害時対応計画 | | | |
| (1) リスク分析の結果に基づき、事業継続計画と整合をとった災害時対応計画を策定すること | ○ | | |
| 1) CIOは、災害時対応計画の策定ルールを明文化していること。 | ○ | | |
| 2) 情報システム部門責任者<以下、本項に共通>は、事業継続計画と整合のとれた災害時対応計画を策定していること。 | ○ | | |
| 3) 災害時対応計画に、バックアップ、代替処理対策、復旧対策等を記載していること。 | ○ | | |
| 4) 将来の経営環境及び業務の変化を考慮していること。 | ○ | | |
| (2) 災害時対応計画は、組織体の長が承認すること | ○ | | |
| 1) 組織体の長またはCIOは、災害時対応計画を承認していること。 | ○ | | |
| 2) 情報システム部門責任者は災害時対応計画を関係者に周知徹底していること。 | ○ | | |
| 3) 組織体のメンバは、災害時対応計画の存在および概要を理解していること。 | ○ | | |
| (3) 災害時対応計画の実現可能性を確認すること | | | |
| 1) 情報システム部門責任者<以下、本項に共通>は、災害時対応計画の実現可能性を検証する計画を策定していること。 | ○ | | |
| 2) 被災の程度に応じた実現可能性を検証する計画を策定していること。 | ○ | | |
| 3) 災害時対応計画が、人的、ファンクショナル、時間的、コスト的、技術的等の観点から実現可能性のあることを検証していること。 | ○ | | |
| 4) 災害時対応計画の実現可能性の検証結果は妥当かどうかを確認していること。 | ○ | | |
| 5) 災害時対応計画の実現可能性の検証結果を記録し、災害時対応計画に反映していること。 | ○ | | |
| (4) 災害時対応計画は、従業員の教育訓練の方針を明確にすること | ○ | | |
| 1) 情報システム部門責任者<以下、本項に共通>は、災害時対応計画に基づいて、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。 | ○ | | |
| (5) 災害時対応計画は、関係各所に周知徹底すること | | | |
| 1) 情報システム部門責任者<以下、本項に共通>は、災害時対応計画に基づいて、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、災害時対応計画に反映していること。 | ○ | | |
| (6) 災害時対応計画は、必要に応じて見直すこと | | | |
| 1) CIOは、災害時対応計画に関する見直しのルールを明文化していること。 | ○ | | |
| 2) 情報システム部門責任者<以下、本項に共通>は、見直し理由を明確にしていること。 | ○ | | |
| 3) 見直しのルールに従い、災害時対応計画の見直しをしていること。 | ○ | | |
| 4) 見直した災害時対応計画は、組織体の長またはCIOが、承認していること。 | ○ | | |
| 5) 情報システム部門責任者は、見直した災害時対応計画を関係者に周知徹底していること。 | ○ | | |
| 7. 3 バックアップ | | | |
| (1) 情報システム、データ及び関連設備のバックアップ方法並びに手順は、業務の回復目標に対応して定めること | ○ | ○ | ○ |
| 1) 情報システム部門責任者<以下、本項に共通>は、災害時対応計画に対応した形で、バックアップ方法並びに手順を準備していること。 | ○ | | |
| 2) 業務別にバックアップの対象を明確にしていること。 | ○ | | |
| 3) バックアップ方法並びに手順は、関連する業務との整合を図っていること。 | ○ | | |
| 4) 業務の回復許容時間及び回復優先順位に対応して、バックアップ方法及び手順を定めていること。 | ○ | | |
| 5) バックアップの要員及び予算を確保していること。 | | | |
| 6) バックアップ対象を明確に定めること。開発途中の設計書、ソースコード、テストデータなど | | ○ | ○ |
| 7) バックアップの周期、保存版数などの条件を明確に定めること。 | ○ | ○ | ○ |

| システム管理(監査)基準と監査のポイント | 発注側 | 元請側 | 受注側 |
|---|-----|-----|-----|
| (2)運用の責任者は、バックアップ方法及び手順を検証すること | ○ | | |
| 1)情報システム部門責任者または運用管理の責任者<以下、本項に共通>は、定められたバックアップ方法及び手順の実現可能性を検証する計画を策定していること。 | ○ | | |
| 2)定められたバックアップ方法及び手順の実現可能性を検証していること。 | ○ | | |
| 3)実現可能性の検証結果を記録し、バックアップ方法及び手順に反映していること。 | ○ | | |
| 7. 4 代替処理・復旧 | | | |
| (1)ユーザ及び運用の責任者は、復旧までの代替処理手続き及び体制を定め、検証すること | ○ | | |
| 1)情報システム部門責任者または運用管理の責任者<以下、本項に共通>は、業務の回復許容時間及び回復優先順位に対応して、復旧までの代替処理手続き及び体制の必要な業務を明確にしていること。 | ○ | | |
| 2)災害時対応計画と対比して妥当な内容の復旧までの代替処理手続き及び体制を策定していること。 | ○ | | |
| 3)復旧までの代替処理の要員及び予算を確保していること。 | ○ | | |
| 4)復旧までの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。 | ○ | | |
| 5)復旧までの手続き及び体制の実現可能性を検証する計画を策定していること。 | ○ | | |
| 6)実現可能性の検証結果を記録し、代替処理手続き及び体制に反映していること。 | ○ | | |
| (2)ユーザ及び運用の責任者は、復旧手続き及び体制を定め、検証すること | ○ | | |
| 1)情報システム部門責任者または運用管理の責任者<以下、本項に共通>は、業務の回復許容時間及び回復優先順位に対応して、復旧処理手続き及び体制の必要な業務を明確にしていること。 | ○ | | |
| 2)災害時対応計画と対比して妥当な内容の復旧処理手続き及び体制を策定していること。 | ○ | | |
| 3)復旧の進捗状況を関係者に周知徹底する体制を定めていること。 | ○ | | |
| 4)復旧の要員及び予算を確保していること。 | ○ | | |
| 5)復旧処理手続き及び体制の実現可能性を検証する計画を策定していること。 | ○ | | |
| 6)実現可能性の検証結果を記録し、復旧手続き及び体制に反映していること。 | ○ | | |