コンプライアンスのシステム監査について
(第III期報告・最終)

－System Auditing of Information System Compliance
(third term report　The Final)－

2013年7月6日

システム監査学会・日本システム監査人協会　共同
コンプライアンスのシステム監査研究プロジェクト

雑賀　努 (株式会社ニイタカ　監査室)
荒牧　裕一 (京都聖母女学院短期大学)
松田　貴典 (大阪成蹊大学)

「本発表内容は、システム監査学会第27回研究大会（2013年6月7日開催）での発表内容と同じです」

研究会メンバー

【主査】
雑賀　努　（株式会社ニイタカ）
【副主査】
吉田　博一（大阪府）
【メンバー】
荒牧　裕一（京都聖母女学院短期大学）
伊地知裕貴（株式会社ニイタカ）
中田　和男（株式会社エスシーエイエヌ）
林　　裕正（富士通株式会社）
広瀬　克之（株式会社ナレッジ，ヒューマン＆テクノロジーズ）
福本　洋一（弁護士法人　第一法律事務所）
松田　貴典（大阪成蹊大学）
（アイウエオ順）

本研究プロジェクトについて

- 本研究プロジェクトは、２０１０年１月より日本システム監査人協会との共同で開始した。
- 情報通信技術の進歩により、情報システム（ＩＣＴシステム）と密接に関連する法的問題を、コンプライアンス視点で点検・評価することが、重要な課題となっている。
- 本研究プロジェクトでは一般企業（製造業）を対象とした情報システムを対象に、コンプライアンスのシステム監査基準の策定を目標として研究を行った。
- 今回は最終報告であり、実際に使用できるものへのブラッシュアップを目指した。
- 成果物は、次のとおりである。（巻末資料参照）
  ａ．部門・業務別コンプライアンスＭＡＰ
  ｂ．システム管理基準へのコンプライアンス脚注

１．当研究プロジェクトの活動実績（１／３）

【第Ⅰ期（前期）】
・期間　　２０１０年1月～２０１０年８月（８回開催）
・内容　　コンプライアンス確保のため関連法規を一覧化し、
　　それらの法規に関連する情報システム（ＩＣＴ）の
　　マップを作成

【第Ⅰ期（後期）】
・期間　　２０１０年９月～２０１１年２月（５回開催）
・内容　　研究活動の参考のため、有識者による情報提供を
　　受け、研究会メンバーと討議を実施
　　その結果を受け、前期の成果物の見直しを行った。

１．当研究プロジェクトの活動実績（２／３）

【第Ⅱ期】
・期間　　２０１１年６月～２０１２年５月（９回開催）
・内容　　①情報システムのコンプライアンス確保のため関連法規を一覧化
②それらの法規に関連する情報システムＭＡＰを作成
③このＭＡＰをベースにシステム開発を例にシステム管理基準にコンプライアンスに関する脚注を追加
④モデル取引、契約の工程をベースにシステム管理基準の内容についてコンプライアンスの観点からの課題抽出
⑤今後はシステム管理基準に対するシステム監査実践マニュアルでの追記の見直しが必要と認識

１．当研究プロジェクトの活動実績（３／３）

【第III期】
・期間　　２０１２年６月～２０１３年３月（１０回開催）
・内容　　①今期は、システム管理基準の内、企画、開発、運用、保守業務について検討した。
②システム管理基準に加える脚注に関して、一層の充実を図り、マニュアル的な活用を目指した。
ａ．コンプライアンス視点からの具体的な監査ポイントについて議論し、一部を脚注に織り込んだ。
ｂ．課題として挙げられた体系上の位置付けや表現等の整合性について、脚注で可能な限り説明を加えた。

２．①コンプライアンスに関する脚注の作成方針

（基本項目）
- 権利関係を明確化するために契約上で必要な項目
- 法務部門（外部の法律専門家）の参画と連携
- 外部委託を前提に委託業務の内容を明確化するための項目
- コンプライアンスリスクに関する検討項目

（追加項目）
- コンプライアンス視点からの具体的な監査ポイントを追加
- 体系上の位置付けや表現等の整合性に関する説明を追加

２．①検討に際して発見されたシステム管理基準上の問題点

- モデル契約とシステム管理基準の細目との用語の定義ずれ（例：要件定義と要求定義）→本研究プロジェクトはモデル契約にあわせた。（要件定義：技術者向けに要求をまとめたもの、要求定義：ユーザの要求をまとめたもの）

- 大規模のウォータフォールモデルの開発を対象としているため、現在の開発方法（オープン系、クラウド、パッケージ、アジャイル、中小規模等）とのかい離→本研究プロジェクトはウォータフォールモデルを対象とした。

- システム管理基準の細目の記載順序の不整合→本研究プロジェクトは現状の記載順序にあわせた。

補足資料①　システム管理基準へのコンプライアンス脚注　－０－

コンプライアンス脚注の対象
コンプライアンス上の課題が多岐にわたるもの

開発区分	開発工程	対　象
企画業務	開発計画	×
	分析	○
	調達	○
開発業務	開発手順	×
	システム設計	○
	プログラム設計	×
	プログラミング	×
	システムテスト・ユーザ受入テスト	×
	移行	×

補足資料①　システム管理基準へのコンプライアンス脚注　－１－

斜体文字がコンプライアンス脚注

システム管理基準と監査のポイント	確認すべき資料、確認方法
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。	開発業務標準
契約上の留意点：要求定義の手順も要件定義作成支援業務に含める場合は明確に規定する。	
契約上の留意点：モデル解約では準委任契約で行うこと。	
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。	開発業務標準 節目でのレビュー実施記録
（ここは要求定義の部分なのでシステム開発は対象としない。）	
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。	要求定義実施経緯（議事録、記録） 要求定義結果 要求定義レビュー実施経緯（議事録、記録）
機密事項に触れる場合もあるので＊外注＊委託業者の作業範囲を＊決定＊明確にする。　ユーザーの理解できる表現で作成するため、＊要件（＊要求＊）＊定義検討会の実施、記録の作成担当を明確に規定する。（後日、開発範囲、開発機能に関する法的問題を防止するため） *開発担当者を明確に規定する。）？*	
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。	要求定義承認記録（印）

補足資料①　システム管理基準へのコンプライアンス脚注　－２－

（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。	開発業務標準 ユーザニーズ調査経緯（議事録、記録）
ユーザーと業務範囲の確認書を取り交わしていること。 ***ユーザーとの議事録を取り交わしていること。***	***ユーザー開発範囲確認書*** ***ユーザー議事録***
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。	ユーザニーズ調査経緯（議事録、記録）
責任者は直接に関係する、間接にしか関係しないに関わらず全てのユーザー部門を網羅していること。	
3）開発の対象、範囲及び方法がユーザニーズを適格に把握できるものであることを確認していること。	ユーザニーズ調査法検討経緯（議事録、記録） ユーザニーズ調査結果 ユーザニーズレビュー実施記録
ユーザー部門が理解できる文書で確認を取ること。	
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。	ユーザニーズレビュー実施記録
定められた開発標準を利用して行っていること	

補足資料①　システム管理基準へのコンプライアンス脚注　－３－

（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。	現状分析実施経緯（議事録、記録）
法的問題に対応する為に法務部門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。	現状分析過程での分析経緯（議事録、記録）
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。	現状分析過程での分析経緯（議事録、記録）
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。	現状分析過程での分析経緯（議事録、記録） 現状分析結果
現状業務の法令順守状況を確認していること。	
5）分析結果を将来展望を考慮して評価していること。	現状分析結果 現状分析結果評価実施経緯（議事録、記録）
6）分析結果を記録していること。	現状分析過程での分析経緯（議事録、記録） 現状分析結果
省略	

補足資料①　システム管理基準へのコンプライアンス脚注　－４－

（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。	ユーザニーズ調査結果 機能要件分析経緯（議事録、記録） 機能要件分析結果
2）調査結果に調査の対象、範囲及び方法等を記録していること。	ユーザニーズ調査結果 機能要件分析経緯（議事録、記録） 機能要件分析結果
ユーザーと業務範囲の確認書を取り交わしていること。 ***ユーザーとの議事録を取り交わしていること。***	
3）十分な内容と詳細度を持った文書としていること。	機能用件分析結果
4）調査結果を、全ユーザに説明していること。	機能要件分析結果説明記録（議事録、記録）
（2）で定めたユーザー部門の責任者およびキーマン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。	ユーザニーズ承認記録（印） 機能要件分析結果承認記録（印）
（2）で定めたユーザー部門の責任者の承認を受けていること。	
省略	

補足資料①　システム管理基準へのコンプライアンス脚注　－５－

（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。	リスク分析実施経緯（議事録、記録） リスク分析結果
コンプライアンスリスクを対象としておくこと	
2）リスクを漏れなく拾いだしていること。	リスク分析結果
特にコンプライアンスリスクについては、外部専門家または法務部門を交えて十分に検討しておくこと	
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。	リスク分析実施経緯（議事録、記録） リスク分析結果
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。	リスク分析実施経緯（議事録、記録） リスク分析結果
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。	リスク分析結果
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。	リスク分析レビュー実施記録
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。	リスク分析結果合意形成状況 リスク分析結果承認記録（印）
省略	

補足資料①　システム管理基準へのコンプライアンス脚注　－６－

（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。	業務見直し実施経緯（議事録、記録） 法律・制度・ガイドライン調査経緯（議事録、記録）
外部専門家または法務担当部門を交えて以下の確認を行うこと。 *法律・制度・ガイドライン調査経緯（議事録、記録）* *法律・制度・ガイドライン準拠性評価経緯（議事録、記録）* *法律・制度・ガイドライン準拠性合意形成状況（議事録、記録）* *法律・制度・ガイドライン準拠性評価報告書*	法律・制度・ガイドライン準拠性評価経緯（議事録、記録） 法律・制度・ガイドライン準拠性合意形成状況（議事録、記録） 法律・制度・ガイドライン準拠性評価報告書
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。	業務、管理体制、規程類見直し結果報告書
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。	業務見直し実施経緯（議事録、記録）
コンプライアンスについては外部専門家または法務担当部門を参画させること	
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。	業務見直し結果
5）検討結果を文書化していること。	業務、管理体制、規程類見直し結果報告書
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。	業務見直し合意形成状況 業務見直し結果承認記録（印）
コンプライアンスについては外部専門家または法務担当部門が承認していること	
省略	

補足資料①　システム管理基準へのコンプライアンス脚注　－７－

（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。	情報システム実現効果評価経緯（議事録、記録）
コンプライアンスについてはシステムで実現するか、運用等他の手段で実現するかを明確にすること。	
例：タバコの販売業務における未成年確認	
2）評価項目及び評価方法を明確にしていること。	情報システム実現効果評価経緯（議事録、記録）
例：オンラインレスポンスタイム、事後処理の処理時間、定例処理の処理時間	
3）定量的及び定性的評価を実施していること。	情報システム実現効果評価経緯（議事録、記録）
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。	情報システム実現効果評価経緯（議事録、記録）
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。	評価結果
6）費用対効果を分析していること。	費用対効果分析実施経緯（議事録、記録）
要件定義の内容が実現された場合の費用と計画上の費用を対比しておく	
7）評価結果に対する合意を関係者から取っていること。	情報システム実現効果・費用対効果分析合意形成状況
マイルストーンとしてアクセプタンステストを盛り込んでおく。	
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。	情報システム実現効果評価経緯（議事録、記録）
マイルストーンとして開発計画に対する相違と責任を明確化を盛り込む。	
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。	情報システム実現効果評価経緯（議事録、記録）

補足資料①　システム管理基準へのコンプライアンス脚注　－８－

（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。	ユーザニーズ調査結果
ＲＦＰを明確にする。	
ＲＦＰの中でコンプライアンスの問題について網羅していることを確認していること	
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。	パッケージソフト評価報告書
ＲＦＰをベンダーに提示して対応可能なパッケージの提案を受ける	
ＲＦＰは各ベンダーに同時に開示して説明する。（公平性を保つ）	
3）評価・選定基準を事前に確定していること。	評価・選定基準
カスタマイズは原則しない。営業部門との調整	
カスタマイズする場合は、その範囲を明確にする	
4）ユーザ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。	パッケージソフト評価報告書
複数のパッケージソフトウェアを比較検討し対応可能状況を評価する。	
5）関係者を集めて適合性の評価を行わせていること。	パッケージソフト評価報告書
ベンダー報告会には関係者を集めて実施すること	
6）適合性の評価結果に対するユーザ部門の責任者の承認を取り付けていること。	パッケージソフト評価報告承認記録（印）

補足資料①　システム管理基準へのコンプライアンス脚注　－９－

システム管理基準と監査のポイント	確認すべき資料、確認方法
３．調達　（1）　調達の要求事項は、開発計画及びユーザ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。	調達品要求定義書
調達品が法的要件に適合していることを確認すること。（例：納税用のイメージがパッケージが勝手に圧縮している場合）	
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ニーズに基づいて作成していること。	調達品要求定義書 ユーザニーズ要求定義書
開発計画からの納期を意識する	
3）調達する資源の種類、数量を明確にしていること。	調達品要求定義書
4）調達する資源の条件、必要事項を明確にしていること。	調達品要求定義書
関連する法令を検討する。	
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。	調達品要求定義書
法務部門の責任者の承認を取り付けること。	

補足資料①　システム管理基準へのコンプライアンス脚注　－１０－

（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。	システム環境選択経緯（議事録、記録） システム環境選択結果 ソフトウェア選定経緯（議事録、記録） ハードウェア選定経緯（議事録、記録） ネットワーク選定経緯（議事録、記録）
コンプライアンスの項目を明確にした文書化を行うこと	
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。	システム環境選択経緯（議事録、記録） システム環境選択結果 ソフトウェア選定経緯（議事録、記録） ハードウェア選定経緯（議事録、記録） ネットワーク選定経緯（議事録、記録）
機能にはコンプライアンス項目を明記する。	
選定経緯にはコンプライアンス項目への対応を明確に記載する。	
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。	評価・選択基準
法務部門の責任者の承認を含めること。	
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。	システム環境選択経緯（議事録、記録） システム環境選択結果 ソフトウェア選定経緯（議事録、記録） ハードウェア選定経緯（議事録、記録） ネットワーク選定経緯（議事録、記録）
将来の法的問題の拡張性を考慮しておくこと	
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。	選択経緯（議事録、記録）

補足資料①　システム管理基準へのコンプライアンス脚注　－１１－

（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。	開発資源洗い出し経緯（議事録、記録） 開発資源承認記録（印）
要員、予算、設備、期間等を明確にする。	
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。	開発資源確保計画 開発資源確保計画レビュー実施記録
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。	開発資源確保計画
4）能力及び経験等を考慮し、要員を確保していること。	開発資源確保計画 開発資源確保実績
開発規模に応じた能力を明確にする。	
5）要員、設備には数量を確定していること。	開発資源確保計画

補足資料①　システム管理基準へのコンプライアンス脚注　－１２－

（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。	開発資源洗い出し経緯（議事録、記録） 開発資源洗い出し結果
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。	開発資源洗い出し結果
3）スキル別の量を明確にしていること。	開発要員確保計画
対象業務別、開発方法別、規模別、プロジェクトリーダー、ＳＥ、プログラマの体制を明らかにする。	
4）必要となる時期を明確にしていること。	開発要員確保計画
開発の進捗に応じた開発要員の山積みを機動的に行う。	
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。	開発資源洗い出し結果
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ていること。	開発要員確保計画 開発要員スキル一覧
本来は予算計上の前提条件として検討される。	

補足資料①　システム管理基準へのコンプライアンス脚注　－１３－

（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。	購買標準
2）調達のルールを定めていること。	購買標準
調達のルールにコンプライアンス、契約上の問題を明確にしていること。（下請法に注意）	
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。	購買標準
要件定義と発注とは分離し透明性を確保する。	
ベンダーへの見積依頼の同時開示等も考慮して競争見積もりの公平性を確保する。	
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。	調達承認記録（印）
発注担当者は関連部門の承認が取れていることを確認して発注する。	
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。	内部監査報告書
6）調達のルールを適宜見直していること。	購買標準改訂履歴
法規制への対応、会社の方針の変更、調達の不備の顕在化に合わせて見直す。	

補足資料①　システム管理基準へのコンプライアンス脚注　－１４－

（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。	開発資源洗い出し結果
プロジェクト独自のものと全社のものを明確にすること	
プロジェクトの独立的管理が認められている場合だけは２）以降を実施することが可	
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。	調達品管理標準 調達品管理記録
3）調達した資源を漏れなく台帳に登録していること。	資産管理台帳 調達品発注書
ハードウェア、ソフトウェア、ライセンス契約の管理（特に同時使用ライセンスの場合にベンダー指定の管理ソフトが必要）	
期間を区切ったシステムリソースの管理（レンタル、リース、不動産賃貸借）	
4）調達品の棚卸しを定期的に実施していること。	棚卸し結果
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。	調達品管理標準 調達品評価記録
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。	資産管理状況報告書
7）管理ルールを適宜見直していること。	調達品管理規定改定履歴

補足資料①　システム管理基準へのコンプライアンス脚注　－１５－

システム監査基準と監査のポイント	確認すべき資料、確認方法
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。	職務権限規程
コンプライアンスに関する権限がそれぞれの責任者に明確に割り当てられていること。	
例：開発から本番移行時のライセンス管理は開発、運用、保守の責任者が認識しているのか？	
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。	組織図、プロジェクト憲章
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。	承認済みシステム設計書
コンプライアンスの視点を含めてシステム設計書を承認しているか？	
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。	承認済みシステム設計書、システム設計書説明状況（議事録、記録等）
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。	開発手順書、システム設計マニュアル、システム設計書
システム設計マニュアルにはコンプライアンスの要求事項を順守することを盛り込んでいること。	
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。	システム設計書
コンプライアンス項目は第一優先で対応すること。	
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。	要求定義書、システム設計書
コンプライアンス項目の整合性は最優先で確認すること。	
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。	開発規程
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。	システム設計レビュー体制図（表）
レビュー体制には法務担当者をメンバーにしておくこと	
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めていること。	職務権限規程
コンプライアンスの視点を含めてレビュー責任者にその責任を説明しているか？	
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。	システム設計レビュー体制図（表）、レビュー実施記録
代表者がコンプライアンスを含めてレビュー可能であること。	

補足資料①　システム管理基準へのコンプライアンス脚注　－１６－

(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、運用の基本方針を定め、運用案を検討していること。	運用の基本方針、運用案
運用で必要なコンプライアンスを組み込んでいるか？	
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。	レビュー実施記録
代表者がコンプライアンスを含めてレビュー可能であること。	
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。	保守の基本方針、保守手順
保守で必要なコンプライアンスを組み込んでいるか？	
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。	レビュー実施記録
代表者がコンプライアンスを含めてレビュー可能であること。	
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。	システム設計書

補足資料①　システム管理基準へのコンプライアンス脚注　－１７－

(3) 入出力画面、入出力帳票等はユーザの利便性***およびコンプライアンス***を考慮して設計すること。	
1)開発の担当者は、***ユーザー要求定義、***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。	開発方針、システム設計マニュアル、システム設計書
ユーザー要求定義にシステム対応項目として記載されたコンプライアンス項目を全て取り込むこと	
開発方針にコンプライアンス項目を組み込むこと	
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。	システム設計マニュアル、システム設計書
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。	入出力インターフェイス基準、アクセシビリティ基準、システム設計書
コンプライアンスの視点を犠牲にして利便性を追求しないこと。	
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。	システム設計マニュアル、システム設計書
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。	ユーザ部門代表者へヒアリング、レビュー実施記録、レビュー体制図
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。	ユーザ部門代表者へヒアリング、レビュー実施記録、レビュー体制図
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。	ユーザ部門代表者へヒアリング、レビュー実施記録、レビュー体制図

補足資料①　システム管理基準へのコンプライアンス脚注　－１８－

(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。	開発方針、システム設計マニュアル、データベース設計書
ユーザー要求定義にシステム対応項目として記載されたコンプライアンス項目を全て取り込むこと	
開発方針にコンプライアンス項目を組み込むこと	
データの追加・変更・削除の操作履歴を、適切に取得・保存する機能を備えること	
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。	データベース設計書、システム設計マニュアル
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。	データベース設計書、検討経緯
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。	データベース設計書、ＤＢＭＳ説明書、検討経緯
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と。	データベース設計書、検討経緯
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。	データベース設計書、データ量予測
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。	データベース設計書、検討経緯
(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ウ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。	システム設計マニュアル、データベース設計書
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。	データベース設計者にヒアリング
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。	データベース設計書
4)チェック結果を記録する機能を組み込んでいること。	データベース設計書
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。	データベース設計書、検討経緯

補足資料①　システム管理基準へのコンプライアンス脚注　－１９－

(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。	開発方針、システム設計マニュアル、ネットワーク設計書
コンプライアンスの視点でネットワークを設計すること。	
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。	システム設計マニュアル、ネットワーク設計書
国際的なネットワークの場合に注意	
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。	ネットワーク設計書、検討経緯
選定理由にはコンプライアンスの視点を考慮すること	
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。	ネットワーク設計書、ネットワーク説明書、検討経緯
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。	ネットワーク設計書、検討経緯
6)システムライフにおけるトランザクション量の増加を考慮してネットワーク設計していること。	ネットワーク設計書、トランザクション量予測
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。	セキュリティポリシー、ネットワーク設計書
コンプライアンスの視点でセキュリティとの整合性を確保していること。特に法的セキュリティに留意する。	
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。	ネットワーク設計書、検討経緯

補足資料①　システム管理基準へのコンプライアンス脚注　－２０－

(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。	開発方針、システム設計マニュアル、システム設計書
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。現状分析のコンプライアンスを踏襲していること	要求定義結果、システム設計書
例：電子帳簿保存における解像度の指定、暗号方式	
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。	システム設計マニュアル、システム設計書
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。	開発の責任者へヒアリング
システムの設計ミスにより情報システム全体がコンプライアンスに対する影響を考慮すること。	現状分析結果、性能分析結果、システム設計書
例：銀行システムの振込サブシステムのピーク設計のミスによる停止	
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。	性能分析・評価結果、検討経緯
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。	性能分析・評価結果、検討経緯、要求定義書
要求定義におけるコンプライアンス問題を検証しているか？	
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。	性能分析実施経緯、要求定義書、要求定義書の見直し申し入れ（議事録、申入れ文書等）、ユーザへヒアリング
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。	要求定義見直し経緯
技術面、経済面ではコンプライアンスに関する事項が確保できない場合は、運用その他の方法で実現すること。	
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。	要求定義見直し経緯
9)要求定義の見直しの理由を明文化していること。	要求定義の見直し理由
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。	要求定義から漏れた機能一覧

補足資料①　システム管理基準へのコンプライアンス脚注　－２１－

(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。	開発方針、システム設計マニュアル、システム設計書
	運用の基本方針、保守の基本方針
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。	ボトルネックの検討経緯
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。	技術的実現方法の検討経緯
実現するための技術がコンプライアンスに問題があるかどうか検討していること。	
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。	経済的実現方法の検討経緯
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。	運用部門代表者へヒアリング、保守部門代表者へヒアリング、レビュー実施記録、レビュー体制図
法的問題にも留意し、関連部門の代表を参加させていること	

補足資料①　システム管理基準へのコンプライアンス脚注　－２２－

(9)他の情報システムとの整合性*およびコンプライアンスとの関連*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*を含む全体システム*との整合性を評価していること。	情報統括責任者へヒアリング、ＩＴインフラストラクチャのHW構成図・SW構成図・NW構成図、システム設計書
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。	情報統括責任者へヒアリング、ＥＡのＴＡ、システム設計書
ＥＡにコンプライアンス項目がある場合は特に留意して設計すること	
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。	共通システムの仕様書、システム設計書
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。	データの授受を行う情報システムの仕様書、システム設計書
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。	ポータルの説明書、システム設計書

補足資料①　システム管理基準へのコンプライアンス脚注　－２３－

(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。	開発方針、システム設計マニュアル、システム設計書
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。	システム設計マニュアル、システム設計書
考慮点にコンプライアンス関係を明確化する。（ＷＥＢ売買の場合）	
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。	障害対策設計経緯
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。 *対象としてコンプライアンス関連事象も考慮すること。* *例えば、個人情報の漏洩、会計帳簿のデータ化が認められたものの喪失。*	障害対策設計経緯
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。	障害対策設計経緯
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。 *コンプライアンスに関係する対応については、法務部門の確認を取ること。*	障害対策設計経緯
7)障害対策の設計結果を、明文化していること。	システム設計書、障害対策設計経緯

補足資料①　システム管理基準へのコンプライアンス脚注　－２４－

(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。 サイバーリスクに関する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。~~ 上流で帳票が未定義	開発方針、システム設計マニュアル、システム設計書
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。	リスク一覧表
サイバーリスクにおけるコンプライアンス課題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。	リスクコントロール機能設計経緯
4)開発の責任者は、不正防止機能を設計していること。	リスクコントロール機能設計経緯
5)開発の責任者は、機密保護機能を設計していること。	リスクコントロール機能設計経緯
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。	リスクコントロール機能設計経緯
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。	リスクコントロール機能設計経緯
予防、防止、発見（拡大防止）、修復を機能として考慮していること。	
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。	システム設計書、設計経緯

補足資料①　システム管理基準へのコンプライアンス脚注　－２５－

(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。	開発方針、システム設計マニュアル、テスト計画書
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。	開発の責任者へヒアリング、テスト方針
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。	テスト計画書
~~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。~~	~~テスト計画書、システム設計書~~
4)信頼性、安全性、効率性及び必要な場合にはコンプライアンス関連機能についてのテスト項目を定めていること。	テスト計画書、システム設計書
5)テストデータ仕様書を作成していること。	テストデータ仕様書
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。	テスト計画書、システム設計書
7)テスト実施に必要な期間を設定していること。	テスト計画書
8)テスト結果の検証方法・体制を明確にしていること。	テスト計画書、テスト体制
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。	テスト計画書、テスト体制

補足資料①　システム管理基準へのコンプライアンス脚注　－２６－

(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。	教育計画書、システム開発計画書
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。	教育計画書、ユーザマニュアル作成手順、ユーザマニュアル承認手続き
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。	教育計画書
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。	教育計画書、レビュー実施記録
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。	教育計画書
サイバーリスク、コンプライアンスを考慮しているか？	

補足資料①　システム管理基準へのコンプライアンス脚注　－２７－

(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。	システム設計書
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。	ユーザ部門の責任者へヒアリング、運用部門の責任者へヒアリング、保守部門の責任者へヒアリング、システムの評価項目
法務部門の責任者も入れておくこと	
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。	システム設計書
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。	システム設計書
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。	レビュー実施記録、システム設計書
法務部門の責任者も入れておくこと	

補足資料①　システム管理基準へのコンプライアンス脚注　－２８－

(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、レビュー時までにシステム設計書を適切に作成していること。	システム設計書、開発計画書
要件定義書で設定されたコンプライアンス項目を適切にシステム設計書に網羅して作成している	
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。	レビュー実施記録、レビュー体制図
法務部門の責任者も入れておくこと	
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。	開発責任者へヒアリング
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。	レビュー実施手順書、レビュー実施記録
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。	レビュー実施手順書、レビュー実施記録

補足資料②　部門・業務別コンプライアンスＭＡＰ　－１－

大部門：本社管理部門（コーポレート部門）

部署	業務	関連法令	関連ICTシステム
総務部	定款管理	会社法	文書管理
	役員会･総会関連	会社法 商業登記法	文書管理　スケジュール管理 総会管理システム（証券代行側）
	株式･株主管理	会社法 金融商品取引法 会社情報適時開示ガイドブック（東証）	電子株式管理 株主優待管理システム
	広報、IR	景品表示法　著作権法	電子媒体 ＨＰ
	建物･物品･固定資産管理	法人税法　固定資産税法	会計システム 固定資産管理、リース資産管理 IT資産管理
		建築基準法　消防法　不動産登記法	
	契約管理	民法　商法　電子署名･認証法	ＥＤＩ
	社内稟議	会社法　刑法	稟議システム
	渉外	民法　商法　著作権法　暴力団対策法 国家公務員倫理法	電子メール
人事部	人事制度･人事企画	公益通報者保護法	人事情報管理システム
	人事評価･考課･昇給	個人情報保護法	人事システム
	採用	労働基準法　障害者雇用促進法 男女雇用機会均等法　個人情報保護法	採用管理システム　ＨＰ
	労務管理･給与	労働基準法　雇用保険法　厚生年金法	就業管理システム
		職安法　労働者派遣法	
		じん肺法	
		ストーカー行為等の規制等に関する法律	
		育児･介護休業法	
		介護保険法　　健康保険法	
	安全衛生（労働環境の整備）	労働安全衛生法	
		感染症の予防及び感染症患者に対する医療に関する法律	
		建築物における衛生的環境の確保に関する法律（ビル衛生管理法）	
	組合	労働組合法　　労働調整法	
	給与処理	所得税法　各種社会保険法規	給与システム

補足資料②　部門・業務別コンプライアンスＭＡＰ　－２－

大部門：本社管理部門（コーポレート部門）

部署	業務	関連法令	関連ICTシステム
人事部	給与処理	地方税法	
	社員教育　　能力開発	著作権法	e－ラーニング　教育管理システム
経理部	予算管理	会社法　金融商品取引法	会計システム
	伝票処理	手形法･小切手法　電子記録債権法	経理システム
	会計監査･税務監査対応	会計基準　電子帳簿保存法 金融商品取引法	会計システム
	環境会計	環境関連法	文書管理システム
	決算処理	会社法　金融商品取引法　法人税法	会計システム
財務部	資金運用･資本調達	金融商品取引法　外為法　金融商品販売法	資金管理システム
	決済･資金繰り	手形法･小切手法　電子記録債権法	資金管理システム
情報システム部	情報化企画（情報化戦略）	情報処理の促進に関する法律 不正競争防止法	
	要求･要件定義･プロジェクト管理	民法　著作権法　不正競争防止法	提案書管理
	システム開発	民法　著作権法	プロジェクト管理システム
	インフラ構築	不正アクセス禁止法	認証システム ログ管理システム
	情報システム保守･運用	情報システム安全対策基準	システム運用管理システム
	ソフトウェア資産管理	著作権法	ソフトウェア管理システム
	メール管理（情報セキュリティー）	個人情報保護法　刑法	メールシステム ウィルス対策ソフト
	データ保存･ＢＣＰ	e－文書法　電子帳簿保存法	文書管理システム
経営企画部	経営戦略　経営目的　経営計画	個人情報保護法	販売管理、生産管理、物流システム等の個別システム
	組織管理	会社法	
	関係会社管理	会社法　金融商品取引法	連結会計システム
	海外会社管理	外為法、出資法	
	顧客対応･渉外窓口	個人情報保護法	顧客情報管理システム
知財部	特許管理	特許法	ナレッジマネジメントシステム 特許管理システム
	実用新案管理	実用新案法	知財管理システム
	意匠管理	意匠法	知財管理システム
	著作権管理	著作権法	知財管理システム

補足資料②　部門・業務別コンプライアンスＭＡＰ　－３－

大部門：本社管理部門（コーポレート部門）

部署	業務	関連法令	関連ICTシステム
知財部	商標管理	商標法、不正競争防止法	知財管理システム
	営業秘密	不正競争防止法	知財管理システム
CSR･監査部	品質管理	ISO9001等	生産管理システム（一部機能）
	プロセス管理		生産管理、工程管理システム、制御システム
	業務管理		個別業務の管理システム
	環境対応	省エネ法	
		化学物質審査規制法　　騒音規制法	
		土壌汚染対策法	
		大気汚染防止法　水質汚濁防止法	
		廃棄物処理法　　悪臭防止法	
		リサイクル法	
		環境基本法　ISO14001	
		環境配慮促進法	
		循環型社会形成推進基本法	
		温対法	
	内部統制	会社法　金融商品取引法	会計システム

補足資料②　部門・業務別コンプライアンスＭＡＰ　－４－

大部門：工場・物流・研究部門

部署	業務	関連法令	関連ICTシステム
研究開発部	研究開発管理	著作権法、特許法、不正競争防止法	
	企画		
	設計･デザイン	意匠法	CAD／CAM
	試作･テスト	下請法	
	シミュレーション･解析		
製造部	生産計画･統制	不正競争防止法	生産管理システム
	製造	製造物責任法、下請法	生産管理システム
	品質表示	計量法　JIS法、JAS法、食品衛生法、健康増進法、薬事法	生産管理システム
	原材料管理	計量法　JIS法、JAS法、食品衛生法、健康増進法、薬事法	在庫管理システム
	消耗品管理		消耗品管理システム
	原価管理	金融商品取引法	原価管理システム
	廃棄物管理	廃棄物処理法、環境関連法規	
品質保証部	計測、検査	計量法　JIS法、JAS法、食品衛生法、健康増進法、薬事法	品質管理システム
	不具合対策	製造物責任法	
施設部	設備資産管理		設備資産管理システム
	点検･修繕		設備資産管理システム
	衛生･清掃	環境衛生関連法	設備資産管理システム
	保安警備	労働安全衛生法	設備資産管理システム
	防災	消防法	設備資産管理システム
業務（物流）部	在庫管理	食品衛生法、健康増進法、（下請法）	在庫管理システム
	入荷確認	（下請法）	入荷（検品）システム
	配送、出荷	道路交通法 自動車NOx･PM法、排ガス抑制法	配送システム
	輸出	輸出入取引法、関税法、外為法	
購買部	発注手配･購買企画		発注システム
	契約業務･発注	民法、商法	
	未払金管理		
	輸入	輸出入取引法、関税法、外為法	

補足資料②　部門・業務別コンプライアンスＭＡＰ　－５－

大部門：営業部門

部署	業務	関連法令	関連ICTシステム
営業部	直接営業･販売活動	消費者契約法、特定商取引法 個人情報保護法 刑法（詐欺、横領、背任）	営業支援システム
	パートナー営業	独占禁止法、下請法	営業支援システム
	グローバル営業	外為法、関税法、通則法、現地法規制	営業支援システム
	通信販売･コールセンター	個人情報保護法、不正競争防止法、刑法、不正アクセス禁止法、著作権法、特定商取引法、割賦販売法、消費者契約法、民法特例法、特定メール適正化法、景品表示法，食品衛生法　JAS法　薬事法、古物営業法、	ネット販売システム 顧客管理システム HP
営業管理部	営業計画･需要予測･販売計画	不正競争防止法、独占禁止法	営業管理システム
	実績管理･販売予算管理	会社法　金融商品取引法	営業支援システム
	債権管理	民法、金融商品取引法	債権管理システム
	契約管理	民法、会社法、金融商品取引法	契約管理システム
営業企画部	商品企画	知財関連法規、不正競争防止法	特許管理システム
	市場調査、マーケティング	個人情報保護法	
	販売促進、広告宣伝	景品表示法	
ＣＳ部	顧客サービス	個人情報保護法	顧客管理システム
	アフターサービス	個人情報保護法、民法（瑕疵担保）、製造物責任法 特定消費生活用品安全法	製品ユーザー管理システム