12. IT全社統制チェックリスト(サンプル)

要素	領域	内部統制目標	項番	レベル	考慮すべき事項	解説	Cf S2	実施基準の対応項目	会社の統制手続	関連資料	整備状況評価手続					運用状況評価手続							(ロールフォワード評価手続)				
											評価手続	評価部門	評価実施者	評価実施日	評価結果	評価手続	評価部門	評価実施者	評価実施日	母集団数	サンプル数	評価結果	評価手続	評価部門	評価実施者	評価実施日	評価結果
統制環境	ＩＴ計画	経営目標に沿ったIT計画を策定、周知し、進捗状況をモニタリングする。	1	H	経営者は経営目標に沿ったIT計画を作成しているか? IT計画の策定に当たっては、その影響を受ける利害関係者（内部および外部）の要望を反映する仕組みとなっているか?	IT計画の作成に当たっては、企業グループ内の調整結果が反映される仕組みとなっているか。 IT計画とは、IT部門の予算のみならず、新規システム開発計画等、ITに関する事業計画であることに留意する。	1	経営者は、ITに関する適切な戦略、計画等を定めているか	事業計画を策定する際に、IT計画も合わせて策定を行っており、経営目標に沿ったものとなっている。 事業計画は必要に応じて取締役会において、利害関係者の要望を反映する仕組みとなっていることを確認している。	事業計画	取締役への質問を行い、左記の事実を確かめる。 事業計画を閲覧する。	経営管理本部			有効に整備されている。													
			2	L	IT部門は、業務プロセスの責任者や組織内のその他の関係者に、IT計画が周知されていることを確認しているか？	部門横断的な委員会等で計画内容が調整されている等、計画策定プロセスに関係者が関与する体制があればよい。	2	–	IT推進チームをIT部門として配置している。IT推進チームは、経営管理部長に対し情報を伝達し、経営管理部長は経営会議においてIT計画の伝達、確認を行っている。	組織図 業務分掌規程 経営会議議事録	組織図、『業務分掌規程』を閲覧し、○○部○○チームの配置と業務分掌を確かめる。 経営会議議事録を閲覧し、○○部部長がIT計画に関する情報の伝達、確認を行っていることを確かめる。	経営管理本部			有効に整備されている。													
			3	M	IT部門の責任者は、自部門の業務執行状況や課題、リスクを社長や担当取締役に定期的に報告しているか? また、このような情報が取締役会で共有されているか?	直接、取締役会で報告される体制となっていてもよい。	3	–	IT推進チームの活動は、管理部長が必要に応じて取締役会で報告を行っている。	取締役会議事録	取締役会議事録の閲覧及び取締役への質問により、○○部部長（副部長）が必要に応じて取締役会で報告を行うことを確かめる。	経営管理本部			有効に整備されている。													
			4	M	IT部門は、ＩＴ計画の進捗状況をモニタリングし、目標達成に必要な対応をとっているか?	例えば、IT部門内のミーティングが月次で開催され、進捗報告が行われているか。	4	–	IT推進チームは、設定した目標を達成するため、定期的にチームミーティングを行っている。		IT推進チームへの質問により、設定した目標を達成するため、定期的にチームミーティングを行っていることを確かめる。	経営管理本部			有効に整備されている。													
	IT組織とその関わり	IT関連部門とその要員の役割、責任を明確に定義する。	5	L	IT関連部門の責任者には、責務を遂行するのに適切な知識と経験があるか？	IT関連部門の責任者を選任する際に、知識や経験を考慮するプロセスが確立されているか。	5	–	IT推進チームのチームリーダー選任に際し、適切な知識と経験があることを確認している。		IT推進チームのチームリーダーへの質問により、適切な知識と経験があることを確かめる。	経営管理本部			有効に整備されている。													
			6	M	財務情報に関連するシステムとデータが把握され、それらの責任者が明確になっているか?	システムオーナーが明確になっているか。例えば、開発変更案件の承認責任者が明確となっているか。	6	–	当社は「勘定奉行」を用いて財務情報を管理しており、財務情報は経営管理部が把握し、経営管理部内に責任者を置いている。		「勘定奉行」を用いて財務情報が管理されており、財務情報は経営管理部が把握し、経営管理部内に責任者を置かれていることを確かめる。	経営管理本部			有効に整備されている。													
			7	M	IT関連部門の役割と責任を明文化し、周知しているか?	IT全般統制の評価単位として識別されると想定される部門すべてについて該当することに留意する。	7	–	業務分掌規程及び決裁権限規程を策定しており、これに基づきIT関連部門の役割と責任を周知している。	業務分掌規程 決裁権限規程	業務分掌規程及び決裁権限規程を閲覧し、IT関連部門の役割と責任が記載されていることを確かめる。	経営管理本部			有効に整備されている。													
			8	L	財務報告目的内部統制に関する自らの役割・責任を、IT関連部門のメンバーに理解させているか？	IT関連部門が内部統制報告制度で実施しなければならない業務がマニュアル化され周知されているか。	8	–	決算業務で行う業務及び担当者を経営管理部で決めており、役割・責任を理解させている。	業務分掌規程 決裁権限規程	決算業務で行う業務及び担当者を経営管理部で決めており、役割・責任を理解させていることを確かめる。	経営管理本部			有効に整備されている。													
			9	L	各種データの管理責任者が明確に定義され、データの完全性が維持される体制になっているか？	データオーナーが明確になっているか（システムオーナーと一致していることも多い）。例えば、データベースを直接修正する場合に影響の調査、実施結果の確認を行う体制が明確となっているか。	9	–	情報セキュリティ基本規程にて、情報セキュリティ統括責任者を定めている。完全性および可用性の確保を目的としたデータ管理を定めている。	情報セキュリティ基本規程	情報セキュリティ基本規程を閲覧し、情報セキュリティ統括責任者、完全性および可用性の確保を目的としたデータ管理について定めていることを確かめる。	経営管理本部			有効に整備されている。													
			10	M	経営者は、ＩＴ関連部門内で分掌させるべき業務を理解し、適切に分掌させているか?	職務分掌の状況が確認できる職務分掌規程や体制図等が作成されているか。 例えば、システム運用業務とシステム開発保守業務は通常分掌することが必要である。	10	–	業務分掌規程及び決裁権限規程を策定しており、これに基づき経営者はIT関連部門内で分掌させるべき業務を理解し、適切に分掌させている。	業務分掌規程 決裁権限規程	業務分掌規程及び決裁権限規程を閲覧し、IT関連部門内で業務が適切に分掌されることが定められていることを確かめる。	経営管理本部			有効に整備されている。													
	人的資源の管理	IT業務に要求される知識と技能をもった人材を確保し、維持する。	12	M	IT関連部門メンバーの異動や退職に際して、内部統制が損なわれないように、適切に管理されているか?	人材確保・育成の視点も含む。	–	–	IT関連部門のメンバーの異動や退職に際して、内部統制が損なわれないように適切な人事異動を行っている。		IT関連部門のメンバーの異動や退職に際して、内部統制が損なわれないように適切な人事異動が行われていることを確かめる。	経営管理本部			有効に整備されている。													
	教育と研修	ＩＴに関する教育・研修を実施する。	14	M	セキュリティ方針や具体的なセキュリティ対策等に関する教育を実施しているか？	IT関連部門のみならず、全社を対象としていることに留意する。	12	–	内部、外部を問わず勉強会やセミナー等への参加することにより、情報セキュリティ意識向上、情報セキュリティ管理規程等の遵守、情報セキュリティ活動の適切な取組みを目的とした情報セキュリティ教育・啓発活動を定期的に実施している。	情報セキュリティ基本規程	内部、外部を問わず勉強会やセミナー等への参加することにより、情報セキュリティ意識向上、情報セキュリティ管理規程等の遵守、情報セキュリティ活動の適切な取組みを目的とした情報セキュリティ教育・啓発活動を定期的に実施されていることを確かめる。	経営管理本部			有効に整備されている。													

12. IT全社統制チェックリスト（サンプル）

要素	領域	内部統制目標	項番	レベル	考慮すべき事項	解説	CfS2	実施基準の対応項目	会社の統制手続	関連資料	整備状況評価手続					運用状況評価手続							（ロールフォワード評価手続）				
											評価手続	評価部門	評価実施者	評価実施日	評価結果	評価手続	評価部門	評価実施者	評価実施日	母集団数	サンプル数	評価結果	評価手続	評価部門	評価実施者	評価実施日	評価結果
リスク評価	リスク評価と管理	ITに係るリスクを識別、評価し、必要な対策をとる。	15	H	財務報告目的内部統制の一環として経営者が定期的にITリスクを評価する際に用いる、全社レベル、業務レベルのリスク評価のフレームワークがあるか?	内部統制報告制度のリスク評価フレームワークにITの視点が含まれているか。 リスク評価結果が、IT全社統制およびIT全般統制、IT業務処理統制のRCMに反映されているか。	16	・経営者は、信頼性のある財務報告の作成という目的の達成に対するリスクを低減するため、手作業及びITを用いた統制の利用領域について、適切に判断しているか ・ITを用いて統制活動を整備する際には、ITを利用することにより生じる新たなリスクが考慮されているか	経営者が定期的にITリスクを評価する際に用いる全社レベル、業務レベルのリスクの評価については、チェックリストを策定し評価を行っている。	チェックリスト（本チェックリスト）	本チェックリストによって、経営者が定期的にITリスクを評価していることを確かめる。	経営管理本部			有効に整備されている。														
			16	H	IT部門がリスク評価を行うに当たっては、外部、内部の様々な環境を考慮しているか？	考慮すべき事項の例としては、IT環境、経営陣のブレーンストーミング、戦略的な計画、過去の監査やその他の評価結果が挙げられる。	17	経営者は、内部統制を整備する際に、IT環境を適切に理解し、これを踏まえた方針を明確に示しているか （ＩＴ環境の具体例） イ．社会及び市場におけるＩＴの浸透度 ロ．組織が行う取引等におけるＩＴの利用状況 ハ．組織が選択的に依拠している一連の情報システムの状況 ニ．ＩＴを利用した情報システムの安定度 ホ．ＩＴに係る外部委託の状況	リスクに関しては、リスク管理規程に基づき、リスク管理委員会で報告、審議、評価等されている。 リスク管理委員会で評価されたリスクについては、議事録に取りまとめられ、必要に応じて取締役会に報告される。	リスク管理委員会議事録 取締役会議事録	リスク管理委員会議事録を閲覧し、リスクに関してリスク管理委員会で報告、審議、評価等されていることを確かめる。 取締役会議事録を閲覧し、リスク管理委員会で評価されたリスクについて必要に応じて取締役会に報告されていることを確認する。	経営管理本部			有効に整備されている。														
			17	M	受容可能と評価したリスクは、当該リスクの内容とその理由を文書化し、正式な承認を受けているか？	内部統制目標のレベルで該当なしとする場合は、その判断根拠を明記する。	18	－	同上	リスク管理委員会議事録 取締役会議事録	同上	経営管理本部			有効に整備されている。														
情報と伝達	マネジメントの意図と指針の周知	IT業務管理、ＩＴ業務手続に関する全社的な方針と手続が明確になっている。	18	H	統制目標を実現するために、経営者はIT部門の業務を統括する方針と手続を文書化し、周知しているか？	例えば、IT業務管理規程やセキュリティポリシー等が定められている。	－	経営者は、ITに係る全般統制及びITに係る業務処理統制についての方針及び手続を適切に定めているか	情報セキュリティ基本規程にて重要情報の定義付けと、情報セキュリティ事故を未然に防止するための管理について定めている。また、業務分掌規程及び決裁権限規程を策定し、IT部門の業務統括について周知している	情報セキュリティ基本規程 業務分掌規程 決裁権限規程	情報セキュリティ基本規程を閲覧し、重要情報の定義付けと、情報セキュリティ事故を未然に防止するための管理について定めていることを確かめる。 業務分掌規程及び決裁権限規程を閲覧し、IT部門の業務統括について周知していることを確かめる	経営管理本部			有効に整備されている。														
			20	M	経営者は、ITに関連する方針、手続、基準を定期的に見直し、ビジネス環境の変化に対応させているか?	実態に合わない方針や手続、基準が放置されていないか。	13	－	部門ミーティング及び経営会議にて必要に応じて検討しており、ビジネスの変化に対応させている。	経営会議議事録	経営会議議事録を閲覧し、ITに関連する方針、手続、基準を定期的に見直し、ビジネス環境の変化に対応させていることを確かめる。	経営管理本部			有効に整備されている。														
			21	L	経営者は、ITに関連する方針や手続、基準の遵守状況を評価するプロセスを定めているか？	内部統制報告制度のITに係る内部統制の評価の手続が明確になっている。	14	－	同上	経営会議議事録	同上	経営管理本部			有効に整備されている。														
			22	M	経営者は、金融商品取引法に基づく、財務報告に係る内部統制の評価及び監査の制度において、IT統制に対する自己の役割と責任を理解しているか？	例えば、役員向け研修会や開示委員会等でITに関連するテーマが取り上げられている。 IT単独ではなく、他の全社統制評価項目と合わせて評価される。	15	－	経営者は金融商品取引法に基づく財務報告に係る内部統制の評価及び監査の制度において、取締役会で財務報告に関する報告を行う際に自己の役割と責任を理解していることを確かめる	ヒアリングメモ	質問により、経営者が金融商品取引法に基づく財務報告に係る内部統制の評価及び監査の制度において、取締役会で財務報告に関する報告を行う際に自己の役割と責任を理解していることを確かめる	経営管理本部			有効に整備されている。														
モニタリング	モニタリング	ＩＴ関連業務の実施状況をモニタリングし、必要な改善を行う。	23	M	重要なITプロセス、コントロールに関する記録の管理方針（作成・更新・保管・廃棄等）が定められているか?	各関連規程の中に定めることも可能。 保管対象・期間を定めるにあたっては、内部統制報告制度対応の観点が考慮されているか。	19	－	文書管理規程を策定し、記録の管理方針について定めている。	文書管理規程 情報セキュリティ規程	文書管理規程を閲覧し、記録の管理方針について定めていることを確認する。	経営管理本部			有効に整備されている。														
			26	M	経営者は、ITサービスの提供状況をモニタリングしているか？ 重大なシステム障害やシステム資源の不足など、問題が識別された場合、IT部門は行動計画を立て、改善に取り組んでいるか？	IT全般統制RCMのDS1.5.1は当項目でカバーされる場合もある。	22	－	ITサービスの提供状況、重大なシステム障害、システム資源の不足など、問題が識別された場合は、管理部長の指示のもとIT推進チームが行動計画を立て、改善に取り組んでいる。 上記問題が発生から解決に至るまで、適宜経営会議で報告され、経営者はITサービスの提供状況をモニタリングしている。	経営会議議事録	経営会議議事録を閲覧し、ITサービスの提供状況、重大なシステム障害、システム資源の不足などの問題が発生から解決に至るまで、適宜経営会議で報告され、経営者はITサービスの提供状況をモニタリングされていることを確かめる。	経営管理本部			有効に整備されている。														
	内部統制評価	自己評価、内部監査等により内部統制を評価する。	28	L	内部監査部門は、IT全社統制、IT全般統制、IT業務処理統制の検証に対しても業務責任を果たしているか？	ITスキルのある要員を内部監査部門に確保しているか、あるいは外部調達しているか。	24	－	内部監査室は、ITスキルのある要員を配置し、IT統制の検証に対して監査を行い、業務責任を果たしている。		内部監査室は、ITスキルのある要員を配置し、IT統制の検証に対して監査を行い、業務責任を果たしていることを確かめる。	経営管理本部			有効に整備されている。														
			29	M	自己評価や内部監査により、内部統制の運用状況を定期的に評価しているか?	内部統制報告制度対応として実施する内部統制の評価で代替可能。	－	－	「財務報告に係る内部統制構築基本方針」記載の「内部統制報告書の作成プロセス」に基づき、各部より提出される自己点検シート及び内部監査報告書から内部統制報告書を作成し、内部統制の運用状況を定期的に評価している。	自己点検シート 内部監査報告書 内部統制報告書	自己点検シート及び内部監査報告書から内部統制報告書を閲覧し、内部統制の運用状況を定期的に評価していることを確かめる。	経営管理本部			有効に整備されている。														