全社的統制とIT統制に関する留意点

1．全社的統制に関する留意点

（1）[統制環境]

	留意点	（対応が不十分な場合）発生しうる問題例	具体的な対応例
1	信頼性のある財務報告のための基本方針を社内に対して明確に示さなければならない	社内各部署で財務報告への対応にばらつきが発生し、結果として財務報告の品質がマネジメントの期待したものにならない	財務報告の重要性の認識を経営理念や倫理規定に明記し周知する
			取締役会等で経理規程を定め社内に周知する
			必要に応じ経理規定を改定し、これを周知する
			決算等を契機として、経理部門から定期的に決算上の留意事項について周知する
2	経営理念や倫理規定に合致しない行動が是正される仕組みがなければならない	幹部、社員が倫理規定に反した行動をとっても放置され、解決への行動が取られない	経営理念/倫理規定に反した状況に接した場合のルールを定める
			第三者からなる内部通報対応窓口を設置する
			不正行為に対する罰則規定を設ける
3	会計処理の原則は適切であり、客観的な実施過程を持っていなくてはならない	会計処理において、処理担当者の恣意が影響し数値が客観性を失う	経理規程、マニュアルを整備することで、経理処理から主観を極力排除する
			財務内容を適切に表示する会計方針を採用する
4	企業の問題の指摘を阻む組織構造や慣行をなくす努力が図られていなければならない	企業の収益性を損なう問題、不正が発生しても、安易に現状が維持されてしまう	利害が相反する部門間での兼務禁止や遵法性のチェックなど牽制が働く組織設計とする
			倫理研修への不参加やアンケートへの未回答の状況を把握し、その比率が高い場合には再度マネジメントからの徹底を図る
			社外取締役、社外監査役の選定に当たっては、出身企業と自社の取引額などもふまえ中立性・独立性が確保できるか確認する

	留意点	（対応が不十分な場合）発生しうる問題例	具体的な対応例
5	企業内の組織には適切に役割分担をしなければならない	チェック機能が働かず、不当な決定、行動が放置されてしまう	業務の企画、実施機能とそれに対する遵法性・経済性・効率性等の観点からの審査、モニター機能が極力別の組織に属するよう組織設計を行う
			分掌規定等を設け、必要な業務執行の割り当ての漏れや重複等がない合理的な組織構造を担保する
6	信頼性のある財務報告の作成に必要とされる能力を持つ人材を配置しなければならない	経理担当者が十分な経理能力を持たず、経理品質が劣化する	経理スキルを持つ社員をデータベース化し、適正配置を行う
			経理担当者については、その採用・育成に関して長期的な視野から計画を立案し、実施する
			アウトソーシング、中途採用等多様なバックアッププランを検討する
7	信頼性のある財務報告の作成に必要とされる能力の内容は常に見直さなければならない	当初は十分な経理能力をもった経理担当者であったが、経理制度の変更等に対応できず、経理品質が劣化してしまう	制度改正などの環境変化に対応した社内勉強会、外部研修会を活用する
			能力検定等を利用して経理担当社員の能力を定期的にチェックする
8	全ての社員が責任と権限の範囲を明確に割り当てられているか	権限を逸脱した意思決定・承認行為が行われる	責任規程等の文書で責任範囲を明示し、これを周知する
			責任規程の内容については環境変化等を踏まえて定期的に見直す
9	社員の権限と責任の割りあての範囲は適切か	過大な権限委任がなされた結果、意思決定が本来なされるべき職位より経験・能力が劣る担当者によってなされる	組織内規による権限の委任に対しては、全社としてのガイドラインを設け歯止めをかける
10	社員は業務上必要な訓練等を受けていなければならない	社員の業務知識が不足したため処理を誤り、結果として経理数値に誤りが生じる	社員の訓練については、その内容、頻度、対象について包括的な計画を立案し、実施する
			訓練に対する参加者を把握し、未参加者に対するフォローアップを実施する

	留意点	（対応が不十分な場合）発生しうる問題例	具体的な対応例
11	社員の勤務評価は公平で適切でなくてはならない	不公正な評価の結果、社員のモラルが悪化し、不正の原因となる	短期の業績目標を極端に報酬・昇格に反映させない
			評価の基準、手順を定め、社員に周知する
			職能/職位に対して求められるスペックを規定し、明示する
12	企業の業務執行にあたっては、適切にスケジューリングを行わなくてはならない	無理なスケジュール設定により事故、誤りが多発する	施策実施にあたっては、事前に投下するリソースと負荷に配慮して合理的なスケジュール計画を作成する
			施策が予定に対し、遅滞が生じた場合に対する対応策をあらかじめ定めておく

（2）[リスクの評価と対応]

	留意点	（対応が不十分な場合）発生しうる問題例	具体的な対応例
1	経営者、管理者を適切に組み込んだリスク評価の仕組みを設けなくてはならない	リスクが存在したにもかかわらず経営者がこれを認知せず適切な行動を取らなかった結果、これが放置される	マニュアル等によりリスク評価、対応のためのプロセス、役割分担を定め、周知する
			内部監査部門等は内部統制検証を実施し、その結果及び対応状況についてマネジメントへ報告する
			マネジメントは外部監査人と緊密なコミュニケーションを保持して、その指摘改善事項への取り組みを主導し、結果を確認する
2	企業の内外の諸要因を適切に考慮して財務報告へのリスクを評価しなくてはならない	リスクが顕在化し財務報告へ重大な影響を与えるまでこれに気づかず結果として誤った報告をしてしまう	マニュアル等により内外のリスクを定義し、それぞれの対応策を設定し、周知する
			リスク管理のための専任組織（委員会等）を設置し、一元的な対応を行う
			月次分析などにより経営状況を分析し、リスクの早期検知、評価、対応を行う

	留意点	（対応が不十分な場合）発生しうる問題例	具体的な対応例
3	大きな組織変更等重大な変化が発生した時にはリスクを再評価する仕組みを設けなくてはならない	組織変更等重大な変化の際にそれに伴うリスクの発生が見過ごされ、適切なコントロールが設定されない	リスク対応の規程の中で、重大な変化の際のリスクの再評価を義務付け、どのような変化がこれにあたるかを定義づける
4	不正リスクの評価の際には、その動機、背景等を考慮しなくてはならない	不公正な評価制度が不正を誘発させていたことを見過ごした結果、社員のモラルが悪化し、不正リスクが増大する	報酬水準、労働時間が妥当なものとなっているか確認する
			評価制度が、公正なもので社員から納得感を得られているか確認する
			適切な役割分担など不正を防止するチェック機能に留意した組織構造になっているか確認する

（3）[統制活動]

	留意点	（対応が不十分な場合）発生しうる問題例	具体的な対応例
1	財務報告作成上のリスク軽減のためのコントロールを確保する方針、手続きを定めなくてはならない	リスク軽減に対する対応が部門ごとにばらばらになり、包括的な対応ができない	該当のコントロールを確保する方針、手続きの骨子については経理規定の中でこれを定め、必要に応じてマニュアル類で補足する
			内部監査部門を中心に、リスクの洗い出し、コントロールの設定、コントロールの運用状況の確認についての具体的な手順を決定、周知する
2	財務報告作成上の職務分担、権限分担を適切に行い、明確化しなくてはならない	財務報告上必要な特定の業務について、分担に漏れが生じ、対応が遅れる	責任規程、経理規程等の中で、財務報告上の職務分担等についても明確化し、必要であれば更に細目を定めたマニュアルを整備する
			期末決算作業を開始する前に、会議等を通じ業務分担等を再確認する

	留意点	（対応が不十分な場合）発生しうる問題例	具体的な対応例
3	リスクが存在する組織の責任者がそのコントロールの責任ももたなくてはならない	リスクの実態に精通しない担当者によってコントロール設定がなされ、適切な対応ができない	リスクの検出、評価、コントロールの設定とその報告に関する第一次責任は事業主管組織（リスクの存在する組織）が負うルールとする
			各業務のリスクの検出、評価、コントロールの設定とその報告に関する責任者については、定期的にこれを確認する
4	全社を網羅した職務規程や個々の業務マニュアルを適切に作成しなくてはならない	マニュアルが存在しない業務について担当者によって、処理方法が異なり、結果にも差異が生じる	職務分掌、責任規程作成にあたっては、全ての組織・業務を包括し定義を行い、極力客観的解釈が可能なものとする
			反復性、継続性のある業務に関してはマニュアルを作成し、業務実施の方法に再現性を確保する
5	業務全体にわたってコントロールを誠実に実施しなくてはならない	コントロールが設定されたもののこの実施が不完全でリスクに十分対応できない	コントロールの設定、運用の状況については、これを定期的にモニターし、報告する
6	統制活動の実施の中で検出された問題には、必要な対応を取らなくてはならない	検出されたリスクに対し、コントロールの設定が決められたが、その実施が送れ結果的にリスクが放置される	検出されたリスクに対してはコントロールを設定し、このときその実施時期についても明示する
			コントロールの設定、運用の状況については、これを定期的にモニターし、報告する
7	統制活動はその実施状況を踏まえて、定期的に見直し、改善しなくてはならない	組織、環境等が変化し、統制活動のプロセスが実態に合わなくなり、リスクが見逃される	統制活動の具体的な方針、プロセスについては毎年再検討し、必要に応じ修正を加える
			組織、環境等が大きく変化した場合には、随時見直しを実施する

（4）[情報と伝達]

	留意点	（対応が不十分な場合）発生しうる問題例	具体的な対応例
1	財務報告作成に関するマネジメントの方針、指示が適切に伝達される体制がなくてはならない	経営者の指示が経理担当者に伝わらず経営者の意図と異なる経理処理が行われる	マネジメントは取締役会、幹部会議等で決算方針等財務報告作成に関する重要な決定を行う
			経理規程等の作成、修正には取締役会、幹部会議等の承認を必要とすることとする
			財務報告作成に関するマネジメントの指示については、その伝達方式を定め（文書通達、ウェブ掲載等）、社員が確認できるようにする
2	財務に関する情報が、関連の業務プロセスから適切に伝達され利用される体制となっていなくてはならない	業務プロセスから経理システムへの接続時にエラーが生じ、決算を誤る	業務システムの設計、改造時に経理システム等との接続に支障が生じないよう、システムの導入、運用には一元的ポリシーを設け、全体の整合を図る責任部門を設置する
3	内部統制に関する情報が円滑にマネジメント及び適切な管理者に伝わる体制でなくてはならない	監査結果等の情報のマネジメントへの伝達が意図的に阻害され適切な対応が取られない	定期的なコントロールの設定、運用状況に関する監査結果は、取締役会、幹部会議等でマネジメントに伝達され、適切な関係者に共有されるようルールを設ける
			内部監査部門はマネジメントと直接のリポートラインを持ち、直接のコミュニケーションが持てる体制とする
			内部監査部門の人事、評価はマネジメント直結とし、社内の第三者の影響を排除する
4	マネジメント、監査役等の間で情報を適切に伝達しなくてはならない	監査役に十分な内部情報が伝達されず、監査役が十分責務を果たせない	内部統制に関する監査結果は取締役会、監査役会で報告され、情報が共有される
			内部監査部門長の選任に監査役が関与する制度とする
5	内部通報などについて独立した伝達経路を設定しなくてはならない	内部通報の通報先が通常の業務を扱う部門の場合、通報者が情報漏れを怖れ、率直な情報提供が滞る	内部通報の通報先は社外の第三者による独立組織とする

	留意点	（対応が不十分な場合）発生しうる問題例	具体的な対応例
6	内部統制に関する外部からの情報はマネジメント、監査役等に適切に伝達し、利用しなくてはならない	外部からリスクの指摘があったにもかかわらず、これがマネジメントに伝達されず対応に反映できない	IR担当、お客様窓口等を設け、外部からの情報を集約、マネジメント等に報告する
			緊急性のある情報に対してはどのようにマネジメントに伝達するかあらかじめ伝達ルートを定めておく
			会計監査人の指摘事項に関しては、マネジメント、監査役が直接伝達されるルールとする

（5）[モニタリング]

	留意点	（対応が不十分な場合）発生しうる問題例	具体的な対応例
1	日常的モニタリングは、業務活動に適切に組み込まなければならない	日常業務の中にモニター機能が不足したため、リスクへの対応が遅れる	業務の企画、実施機能とそれに対するモニター機能が極力別の組織に属するよう組織設計を行う
			月次の対計画差分析、対前年度実績差分析等を通じ、異常値の検出を実施する
2	リスク評価の範囲と頻度は、リスクの重要性、コントロール、モニタリングの状況から適切に調整しなくてはならない	既存のリスク評価の範囲、頻度を環境の変化にもかかわらず見直さなかったため、新たに発生したリスクへの対応が見逃される	リスク評価の範囲と頻度に関しては、企業自体の変化、事業環境の変化等に応じ、リスクの重要性、リスクの実現可能性、既存のコントロールの有効性、日常的モニタリングの有効性を勘案し、定期的に見直しを実施する
			内部監査部門は、リスクの評価と頻度の見直しを踏まえた監査計画を立案し、マネジメント、監査役等の承認を得る
3	モニタリングの実施責任者は適切な知識、能力を持たなくてはならない	内部監査部門に十分な能力を持った社員がいないため、適切な監査業務が行えない	内部監査担当者の訓練については、その内容、頻度、対象について包括的な計画を立案し、実施する
			訓練に対する参加者を把握し、未参加者に対するフォローアップを実施する
			必要に応じアウトソーシング等の補足措置を講じる

	留意点	（対応が不十分な場合）発生しうる問題例	具体的な対応例
4	経営者はモニタリングの結果をタイムリーに受け取り、対応しなくてはならない	マネジメントへの情報伝達が遅れたため、必要なリスク対応が間に合わない	定期的なコントロールの設定、運用状況に関する監査結果は、取締役会、幹部会議等でマネジメントに伝達され、適切な関係者に共有されるようルールを設ける
			緊急性のある情報に対してはどのようにマネジメント、監査役に伝達するかあらかじめ伝達ルートを定めておく
5	内部統制の不備情報はコントロールの実施責任者及びその上位者に適切に報告しなくてはならない	内部統制の不備情報が実際の実施責任者に伝達されず、適切な改善が講じられない	定期的なコントロールの設定、運用状況に関する監査結果は、取締役会、幹部会議等でマネジメントに伝達され、適切な関係者に共有されるようルールを設ける
			個々の業務に関するモニタリング結果については、その業務の実施責任者とその上位者に直接フィードバックを実施する
6	内部統制に関わる重要な欠陥はマネジメント、監査役等に適切に伝達しなくてはならない	内部統制に関わる重要な欠陥がマネジメントに意図的に伝えられず、適切な対応がなされない	定期的なコントロールの設定、運用状況に関する監査結果は、取締役会、幹部会議等でマネジメントに伝達され、適切な関係者に共有されるようルールを設ける
			内部通報制度を設ける
			内部監査部門長の選任に監査役が関与する制度とする
7	リスクに対してコントロールの設定が立案された場合には、その実施についてその後の進捗をモニターしなくてはならない	検出されたリスクに対し、コントロールの設定が決められたが、その実施が遅れ結果的にリスクが放置される	コントロールの設定、運用の状況については、これを定期的にモニターし、報告する

（6）[ITへの対応]

	留意点	（対応が不十分な場合）発生しうる問題例	具体的な対応例
1	ITに関する全社的な戦略、計画等を定める必要がある （ITに係わる全般統制、業務処理統制についての方針もこれに含める）	各部署がITに対し個別に対応した結果、全体として非効率な体系となってしまう	全社を包括したIT戦略立案、実行の責任者（CTO等）を定める
			IT戦略立案、実行責任者（CTO等）と既存のスタッフ・ラインとの責任関係を明確にし、周知する
			ITの導入、運用・利用、統合、撤廃に係わるルールとその運用方針について明確にし、これを周知する
2	IT環境を適切に勘案して、内部統制整備の全社方針を定めなくてはならない	進んだIT環境を活用しない統制整備計画となり、正確性・効率性が本来あるべき水準に達しない	内部統制に関する基本方針の策定、変更等の際には、CTO等のIT統括機関と十分な協議を行う
			CTO等のIT統括機関はITの整備状況及びその利用・運用実態について把握する
3	財務報告の信頼性確保の見地から手作業とITを用いた統制を適切に使い分けなくてはならない	過度にITに依存したプロセスとしたために、整備に時間がかかり、必要な導入時期に間に合わない	ITと手作業の使い分けの基準については、CTO等のIT統括機関がガイドラインを定め、周知する。小規模なIT事案については、これに基づき各業務責任者が判断する。
			大規模な事案については、CTO等のIT統括機関と協議、判断する
4	統制活動にITを利用する際には、そのリスクについても考慮しなくてはならない	顧客のオーダー処理にITを利用した結果、顧客データのネットを通じた流出リスクが発生する	ITの導入、運用・利用、統合、撤廃に係わるルール設定に際しては統制にかかわるリスクも評価し、これに適切に対応するものとする
			各業務の実施責任者はITの利用にあたって全社方針に則ってリスクを評価し、必要に応じてCTO等全社のIT統括機関と協議する

2. IT統制に関する留意点

	留意点	（対応が不十分な場合）発生しうる問題例	具体的な対応例
1	IT/システムの仕様（容量、性能など）は、業務上の必要性との整合を確保しなくてはならない	システムが必要な処理量を行えない、もしくは必要な時間内に処理が終わらない	各業務の実施責任者は全社方針に則って、開発要望を（必要に応じIT統括機関を通じ）開発部門へ提出し、最終的な導入まで協働する
			システムの仕様の設定に関しては、口頭での連絡は補助的な役割に限定し、文書による関係者間の確認を行う
			開発部門は、仕様依頼書、要求条件書、開発のログ等を保管、管理する
2	システムの開発（購入）・変更は必要な承認プロセスを経なくてはならない	システムに対して未承認の開発や変更が行われる	システムの開発（購入）・変更について必要なプロセスについてのルールを定め、これを周知する
			CTO等全社のIT統括機関はIT/システムの開発スケジュールを定め、これを周知する
3	開発（購入）・変更にあたっては、実際の導入の前に十分なテストを実施しなくてはならない	実際の業務に導入後、バグが発見され業務に支障をきたす	システム/開発部門は受け入れ試験を実施し、要求した仕様どおり作動するか確認する
			データ移行作業が発生する場合、予め作成した移行手順書に基づきデータ品質を確認する
			本番移行作業は、試験環境とは別個に設定された本番環境へのアクセスの職務分掌をふまえ、移行計画書に定められた担当者が行う
4	新システム導入後の運用については十分な準備をしておかなくてはならない	社員が導入されたシステムの操作で混乱し、業務に支障をきたす	導入前に十分なユーザ習熟研修を実施する
			該当のシステム業務処理マニュアルを事前に、作成・変更する

	留意点	（対応が不十分な場合）発生しうる問題例	具体的な対応例
5	アカウント管理は適切に処理しなくてはならない	異動・退職した社員のアカウントが残存し、アクセスが可能なままとなる	ユーザーアカウントの登録・変更・削除のルールを定め、周知する
			人事異動の際の手順にユーザーアカウントの登録・変更・削除確認作業を組み込む
			ユーザーアカウントの状況については、定期的に社員情報との突合等の検証を行い、現状に即したものになっているか確認を行う
			ユーザーアカウントの管理者権限の付与についてはあらかじめルールを定め、付与者は最小限に限定し、必要がなくなれば確実に削除する
6	アカウントが不正に利用されないようしなくてはならない	第三者が社員のパスワードを使用し、なりすまして不正アクセスする	パスワード設定にはセキュリティ強度を考慮したガイドラインを設ける
			最初のログイン時にパスワードの変更を強制する
			パスワードには有効期限を設ける
			ログイン時に一定回数を越えるユーザ認証エラーをした場合、該当ユーザIDの使用を禁止する
7	システム管理担当者による不正や誤謬を防止しなくてはならない	システム管理担当者がデータを誤って、もしくは不正に修正してしまう	システム管理責任者と作業者を別個に設定し、システム管理責任者は作業者・作業内容を確認してアクセスを許可する
			システム管理責任者はアクセスログを記録し、不正なアクセスがないか確認する
8	サーバルームのセキュリティー構造を適切に構成しなくてはならない	第三者がサーバに物理的にアクセスし、データに損傷を与える	サーバルームへの入室メンバーを限定し、セキュリティーカード、パスワード等によって運用する
			登録メンバー以外の入退室の際には、登録メンバが同行し、記録を取る

	留意点	（対応が不十分な場合）発生しうる問題例	具体的な対応例
9	ネットワークセキュリティーを確保しなくてはならない	第三者がインターネット等を通じネットワークに不正アクセスし、データを剽窃する	責任者を定め、ファイアウォールのフィルタリングルールを常時見直す
			ファイアウォールのアラート機能等を利用して不正なアクセスがないか確認する
			内部監査等特定の業務のサーバは他のものから独立した構成とする
10	バックアップ処理を正確・完全に実施しなくてはならない	データが損傷した際に、データのバックアップがなく現状復帰ができない	定期的・自動的なバックアップが行われる設定とし、正しく実行されていることを確認する
			システムの変更などで手順が変更になった際にはバックアップが適切に実施できることを確認する
			バックアップ媒体は個別識別可能な状態で安全な場所に保管する
11	各アプリケーションの機能が所期の役割を果たしていることを常時担保しなくてはならない	アプリケーションシステムにバグが発生し、処理にエラーが生じる	定期的にテストデータを使用した検証を行い、システムが所期の機能を果たしていることを確認する
			関連するシステムが更改される際には、接続性を事前に確保し、本番環境への移行を前にテストを実施する
12	システム障害に対する対応方法をあらかじめ定めておかなくてはならない	システム障害が発生した際に対応が混乱し、復帰に時間がかかる	システムごとに障害受付、対応の一元的対応主管及び対応プロセスを定めておく
			緊急連絡表を常時現行化しておく
			故障の傾向を分析し、予防措置をほどこす

	留意点	（対応が不十分な場合）発生しうる問題例	具体的な対応例
13	入力情報の完全性、正確性、正当性を確保する手段を取らなくてはならない	キーボード操作ミスのために入力を誤る	あらかじめ、文字種別、入力桁数設定等の入力制限を行い、想定外の投入はできない設定としておく
			入力が必要な項目が漏れなく入力されない限り次の処理に進めない仕組みとする
			適切な権限を持った承認者によって承認されたデータのみが処理される仕組みとする
14	例外処理（エラー）の修正と再処理は適切に管理しなくてはならない	エラーが修正されず出力データが不完全なものとなる	エラーが発生した場合は、エラー内容が出力され、データの再入力が行われない限り処理が完了しない仕組みとする
			エラーリストにはエラーとなった処理が全て出力される仕組みとする
15	取引先等参照されるマスタデータの維持・管理を適切に行わなくてはならない	マスタデータが古いものであったため処理が誤ったものとなる	マスターデータの情報について定期的に検証を行い、適切に管理されているか確認を行う
			マスターデータと他システムとのデータ授受は、正確に、即時に行われるシステム設計とする
16	システムの利用に関しては適切なアクセス管理をしなくてはならない	権限のない人間がシステムにアクセスし、不正な操作・承認を行う	パスワード、生体認証、IDカード等によりアクセス認証を行い、許可された者のみがアクセスできる仕組みとする
			アクセス者別に、業務の必要性に応じた操作範囲及び承認権限を設定する
			システム・データベースの重要度によっては、アクセスの際にはその都度管理者の許可が必要な仕組みとする
			いつ誰がシステムへアクセスし、どのような業務処理を行ったかという記録を残す仕組みとする

（注）上記の留意点で述べられている「システム」については、社内の情報システム（IT）部門がその構築・運用管理に関わる全社的なシステムの他、EUC（エンドユーザコンピューティング）やスプレッドシート等、情報システム（IT）部門の積極的な関与を受けずに主にユーザ側によって構築・運用管理が実施されるアプリケーションシステムを含んでいる。