CIA フォーラム第一部会テーマ:「CSR に貢献する内部監査」

【部会構成員(順不同 / 敬称略)】

- (座長)柳澤良文
- 相知義文
- 浦西完次
- 宮内隆行
- 菰池道夫
- 植垣雅則
- 石井秀明

【成果報告書全体構成】

第1章　CSR の意味と内部監査の関わり

第2章　グループ経営における内部監査の役割

第3章　グローバル経営における内部監査の役割

第4章　IT統制に対する内部監査

第 1 章　CSR の意味と内部監査の関わり

1.　CSR とは

CSR（Corporate Social ResponsibilITy）とは一般に企業の社会的責任と訳される。経済産業省が 2004 年9月に公表した「企業の社会的責任（CSR）に関する懇談会」中間報告書では、CSR を、「今日経済・社会の重要な構成要素となった企業が、自ら確立した経営理念に基づいて、企業を取り巻くステークホルダーとの間の積極的な交流を通じて事業の実施に努め、またその成果の拡大を図ることにより、企業の持続的発展をより確かなものとするとともに、社会の健全な発展に寄与することを規定する概念であるが、同時に、単なる理念にとどまらず、これを実現するための組織作りを含めた活動の実践、ステークホルダーとのコミュニケーション等の企業行動を意味するもの」と定義している。

この定義には大きく二つの重要な意味が含まれている。一つは「CSR はあらゆるステークホルダーとの関係を維持しつつ企業を発展させるための具体的な経営活動である」ということ、もう一つは「企業は CSR の取組を積極的にステークホルダーに報告（コミュニケーション）すべきである」ということである。すなわち、企業が自社の活動に係る責任ある対応をいかに行い、その成果をどのように情報開示するかが社会から問われている。

このように CSR は非常に広範な範囲をカバーする。CSR が対象とするステークホルダーは株主・投資家、一般消費者、取引先、監督官庁、社会環境など非常に多岐にわたり、取り扱うテーマもコンプライアンスやリスクマネジメントだけでなく、近年脚光を浴びている内部統制もその範囲に含まれる。当部会では CSR の中でも特に株主・投資家に対する CSR に焦点を当て、内部監査がどのような形で貢献できるかについて考察を深めたい。

2.　株主・投資家にとっての CSR

株主・投資家にとっての CSR とは、第一義的には企業価値を高めることで投資収益を還元することである。加えて、近年株主・投資家は「信頼できる企業情報の開示」を企業に対して強く求めるようになってきている。この風潮は米国での巨額粉飾決算や、日本における有価証券報告書の虚偽記載及び粉飾決算を契機として急速に高まっており、典型的には「金融商品取引法」（仮称：現「証券取引法」）や「（新）会社法」によって、各企業に信頼できる「内部統制」の構築が法的に要請されることに代表される。「金融商品取引法」では単に企業が「内部統制」を構築するだけでなく外部監査人による内部統制監査も要求される。

このように、株主・投資家が「信頼できる企業情報を開示して欲しい」、「そのために信頼できる内部統制を構築して欲しい」という期待を企業に対して抱くようになっている。これは裏を返せば、この期待に対して各企業が適切に応える社会的責任を有していることを意味する。当部会が考える株主・投資家にとっての CSR とは、この「信頼できる企業情報を開示するために適切な内部統制を構築すること」と解釈する。

3. 当部会が考える内部監査と CSR の関わり

それでは内部監査は株主・投資家にとっての CSR の実践において、どのような関わりを有するのであろうか。

内部監査は、企業内の各部門が経営理念及び経営計画並びに社内ルール等に準拠して適性かつ適法な活動を行っていることを保証する機能、あるいはコンサルティング機能を有する。当部会は特に保証機能こそが内部監査の重要な機能であると考える。

前述の「信頼できる企業情報を開示するために適切な内部統制を構築」していることを企業の経営者が株主・投資家に対して意見表明し、その意見に対して外部監査人の内部統制監査が実施される局面において、内部監査は①経営者が安心して意見表明できる保証を与える、②外部監査人に対して企業がいかに適切に内部統制を構築しているかを積極的にアピールする、という役割を果たさねばならない。この役割の遂行を通じて内部監査は CSR に貢献する。

4. 当部会の研究テーマ

以上より当部会では株主・投資家にとっての CSR に貢献する内部監査を研究対象とし、想定される様々な局面における内部監査の課題と改善の方向性を検討・提案する。

ただし、限られた研究時間の中で広範な内部監査全般について研究することは効率性を害するだけでなく有効性をも損なうとの判断のもと、以下の領域に焦点を当てて研究を行うものとする。

- グループ経営における内部監査の役割（第 2 章）
- グローバル経営における内部監査の役割（第 3 章）
- IT統制に対する内部監査（第 4 章）

第２章　グループ経営における内部監査の役割

グループ経営における内部監査には大きく分けて分散型内部監査体制と集中型内部監査体制がある。分散型内部監査はグループ内に複数の内部監査組織を有し現場の実情をより良く把握した上で有効な監査を行うものであり、集中型内部監査は親会社のみが内部監査組織を有し集中的かつ効率的に監査を行うものである。本章では分散型及び集中型のそれぞれについて内部監査の役割を考察する。

1.　分散型内部監査体制

(1) 現状と課題

分散型内部監査体制では監査テーマごとに親会社監査部がグループ全体を監査、あるいは親会社監査部門と主要子会社の監査部が分担してグループ全体を監査する。具体的には、親会社の監査部は各組織と主要子会社の監査を行い、孫会社（傘下会社）は主要子会社の監査部（あるいは事業部監査人）が担う。

この際、親会社監査部がグループ全体の監査計画の立案・推進を行うとともに各組織や主要子会社の監査人材の育成を行うことでグループ全体の監査水準の均一化を図っている。一方で、主要子会社の監査部（事業部監査人）は、自社各組織及び傘下会社（孫会社）の監査を行うとともに親会社監査部監査のフォロー、自己点検の推進を行う。

このような分散型内部監査体制に関して以下の課題が挙げられる。

①　監査リソースの課題（特に要員面）

近年、日本の企業組織においてはグループ経営の重要性が叫ばれているが、内部監査機能に対する人員問題について必ずしも特定の方針または戦略が設定されているとはいえない状況にあると思われる。

実際、「監査白書（2000 年度）」によると、内部監査担当部門の人員数は「3 名以下」が66.5%（1 名は 35.1%)である一方で 10 名以上はわずか 9.4%にとどまっていることがそのことを示しているとも言える。

②　業務内容の理解不足（社内の各部門、本業と関係の薄い関係会社の業務）

全社的な共通業務（購買・経理業務、情報管理等）の場合は比較的容易に単一のチェックリストで監査を実施できるが、各部門、各社に固有の業務の場合は業務内容の理解（監査設計）に時間がかかる上に、作成したチェックリストに汎用性がなく他の監査テーマに応用がきかないという問題点がある。

また、本業とは関係の薄い事業を展開している関係会社の場合は、「一品一様」の監査となり、限られた人員で監査を実施する場合の制約となる。関係会社といっても規模がさまざまであり、経理・購買業務であっても同じチェックリストで監査を行うのが困難な場合も多い。

③　自主監査（自己評価）の課題（レベルの違い、マンネリ･形骸化）

上記の課題を解決する方法として自主監査の活用が考えられるが、自主監査にも問題がある。自主監査実施レベルの違い（範囲・深さ）である。また、自主監査の実施状況を評価する仕組が確立していないため、ベクトルを合わせることもできていないのが実情である。また、自主監査の実施状況を評価する仕組が確立していないことに関連するが、自主監査（自己評価）は、とかく「実施することに意味がある」という状況に陥りがち（形式的な自主監査）で、毎年継続して同じテーマ、同じチェックリストをやっていることからマンネリ感も強い。

(2) 改善の方向性

①　自主監査（自己評価）のレベルアップ

各組織･関係会社への監査人設置（専任、兼務、臨時）とともに、チェックリストを工夫し、該当業務の主管部署による定期的な見直しを実施する。また、情報交換･相互啓発の仕組を作り、自主監査の機能を単なるチェックではなく継続的な PDCA サイクルである Control Self-Assessment（以下「CSA」）に昇華する。

②　親会社監査部のサポート機能強化

親会社監査部が関係会社監査人への継続的な教育を行うとともに、関係会社の監査テーマ設定や監査計画立案時及び往査におけるレビューを実施するなど必要な支援と助言を行う。

また、マニュアル類の整備と提供を促進するために、全体フレームの明確化・監査対象業務の定量化指標の設定・評価基準の策定・各種文書の書式の統一等の施策を講じる。

③　外部戦力活用

監査法人などの企業外部の専門家の活用を検討することも選択肢として挙げられる。

④　監査テーマの工夫

統一テーマや中期計画の設定を行う。

⑤　「財務報告に係る内部統制」の文書化・自主検査との連携

実施要領の作成等の自主検査の仕組をつくり、該当組織と連携した自主監査の実施を行

う。

⑥　モニタリング業務の導入

内部監査部門が被監査組織や一般管理部門からの情報入手を通じて監査対象業務を継続的に評価するとともに、必要に応じて監査を行う。

・アンケート形式での実態調査（ポイントを絞った情報収集）

・アクションレベルの設定（発信元に確認～関係者と協議～監査実施）

・アラームポイント（アクションを起こす判断基準）の設定

2.　集中型内部監査体制

(1) 現状と課題

内部監査体制の確立は、企業規模にかかわらず、全企業に求められる。特に、昨今の上場企業における不祥事の増加に伴い、その社会的要求は強まるばかりである。

しかし、実態としては、上場企業であっても、相対的に小規模の企業においては、理想的な内部監査体制の確立を一足飛びに実現することは、人材確保・コスト面などの種々の問題が大きな障害となって実現が困難になっている。さらに、グループ企業として子会社が存在する場合に、その子会社に内部監査組織を擁することは、さらに困難な状況にある場合が多いと推測される。

一方で、グループ内に複数の子会社が存在する場合や、支店において複数の事業部門が存在する場合には、監査体制のコンフリクトや洩れ（監査対象とならない部門が残る）が発生するというリスクを抱えており、これらの課題を克服することが求められる。

(2) 改善の方向性

監査体制を構築する場合、監査資源の分散化と集中化の 2 つの方法があると考えられるが、上記のような比較的小規模企業においては、監査資源を分散するよりも、親会社（本社内部監査部門）に内部監査スタッフを集約することが得策であり、最も効率化を図ることができると考える。具体的な運営のポイントは以下の通りである。

①　グループ監査計画の策定及び中期監査計画の策定

本社集中型監査体制をとることにより、監査体制のコンフリクトやモレを排除することが可能となる。そして、その基本となるのが監査計画である。グループ全体の監査計画を集中的

に本社の内部監査部門で立案し、それに従い監査を実施することにより、監査体制のコンフリクトやモレを排除することが可能となる。

また、中期的なリスクベースの監査計画を策定することにより、限られた監査資源で、より優先順位の高い監査テーマに取組むことが可能になるとともに、中期的な監査体制の強化目標（量と質のアップ）を明らかにすることができると考える。

② 専門分野別スタッフの確保

監査テーマを分類する場合、大きく 2 つの切り口が存在すると考えられる。

つまり、購買・製造・営業・経理・総務・情報システムなどの『業務機能別』分類、商品を軸とした『事業別』分類の 2 つである。複数の事業を抱えるグループ企業における内部監査スタッフは、基本的な内部監査のスキルを持ち、業務機能別のスキルとともに、さらに、商品・事業別の知識を備えなければならない。

これらの全ての分野に精通することは、非常に困難なことではあるが、この『業務機能別』分類、商品を軸とした『事業別』分類のマトリクスにおいて、少人数でも網羅できるように人材の獲得・育成計画を持つことが重要であると考える。

③ CSA の導入

少数の監査スタッフで、グループ企業内の全部の内部監査を実施することは、監査部門長及び監査スタッフにとって、非常に多忙な状況となり、各監査テーマに十分な時間をかけることができないために監査品質が低下するという弊害をもたらす危険がある。これを解決するためには、CSA の導入が不可欠である。この場合、被監査部門における自己評価用のアンケートを作成することが必要となるが、職務機能別視点からの質問だけでなく、事業部門毎のリスク特性を考慮した自己評価用質問テンプレートを作成することにより、効果的な CSA の導入が実現できると考えられる。

前述のリスクベースの監査計画の活用により、優先順位の高い監査テーマについては重点的に内部監査を実施し、一方、定型化が比較的容易で、かつ、広範囲に活用できる監査対象に対しては CSA を導入していくことがポイントになると考えられる。

第 3 章　グローバル経営における内部監査の役割

1.　グローバル(海外拠点・関係会社)監査における内部統制の評価について

(1)　現状の課題

1990 年代以降、経済・市場のグローバル化に伴い、グローバル市場参加企業数は急激な拡大を見せている。こうした経営環境下、継続的な内部統制評価のため毎年グループ全体に対して内部監査を実施することは、経営資源に限りがあることから困難なものとなってきている。

そこで、企業監査におけるリスクアセスメントと CSA を活用したグローバル監査について考察する。

ただし、本社及びグループ各社の財務報告に関わるルール及び業務手順の標準化を同時に進める必要がある。なぜなら、ばらつきが顕著にみられると、内部統制の整備・強化が困難になるためである。もちろん、各社で業務内容が完全に一致しているわけではないため、財務報告に関わるルール及び業務手順を完全に統一することは不可能だろうが、可能な限り標準化を進める必要があると考える。

そのうえで投入資源が比較的少ない CSA をグループ全体に実施し、一方で内部監査の必要性が高い拠点・関係会社を特定して重点的に内部監査を実施するというリスクアプローチの採用により、内部統制評価の費用対効果を最大限に高めることが可能となると思われる。

2.　対応策としてのリスクアセスメント(リスク評価)及び CSA(統制自己評価)の活用

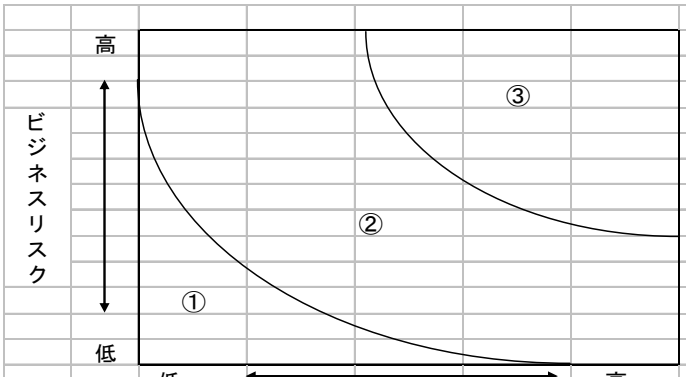
（1）リスクアセスメント(リスク評価)の活用

①　リスクアセスメントの内容及び目的

リスクの定義は「経営目的の達成を脅かすあらゆる不確実性」とされている。そして、リスク評価とは「効率的かつ実効性のある内部監査を実施するために、被監査部門に内在するリスクを定期的に分析し評価し、監査の頻度や優先度を決めること」と言われている。ここでは、被監査部門のリスク評価の対象とするリスク分類をビジネスリスク(固有リスク：内部管理を考慮する前のリスク)とコントロールリスク(管理リスク：ビジネスリスクが内部管理によりコントロールされない可能性)に分類する。そして、被監査部門のビジネスリスクの種類・程度、コントロールリスクの程度を、可能な限り正確に把握することによって、残存リスク(ビジネスリスクが内部管理によりコントロールされず残存するリスク)の程度を評価する。

その結果等に基づき効率的かつ有効な内部監査の前提として以下を決定する。

- 残存リスクの程度に応じて内部監査の頻度
- 監査投入資源の濃淡



② リスクアセスメントの実施方法

リスクアセスメントは前回監査結果等を踏まえ、被監査部門のリスクの種類・程度を、ビジネスリスク及びコントロールリスクに区分して定性的・定量的な指標等を参考に把握し、残存リスクを総合的に評価する。

バーゼル銀行監督委員会で引用されているリスクを参考に、ビジネスリスクとコントロールリスクの具体的項目のサンプルを示してみる。

	ビジネスリスク		コントロールリスク
1	信用リスク	1	マネジメント
2	カントリーリスク	2	リスクの認識および評価
3	トランスファーリスク	3	リスク管理業務
4	マーケットリスク	4	情報とコミュニケーション
5	金利リスク	5	モニタリング業務と問題点の是正
6	流動性リスク		
7	オペレーショナルリスク		
8	法務リスク		
9	レピュテーショナルリスク(評判リスク)		

※グローバル監査においてはカントリーリスクを海外拠点特有のリスクとして注目しておく必要がある。すなわち、言語・社会環境等本邦との違いにより損失を被るリスク、海外特有の状況から各個別ビジネスリスクに対して損失を増加させるリスク及びこれに類するリスクである。

※経営資源として活用が可能であれば、現地IAの採用は有効な手段となりうる。

(2) CSA(統制自己評価)の活用

① CSA の内容及び目的

CSA とは「統制自己評価」という内部統制評価手法の一つである。

内部統制を評価するためには、大きく分けて 2 つの方法がある。一つは内部監査部門のような独立的な部門が監査対象部門の内部統制の整備状況についてチェックする方法で、もう一つは監査対象部門自らが自己点検する方法である。CSA は後者にあたる(前者はいわゆる内部監査)。

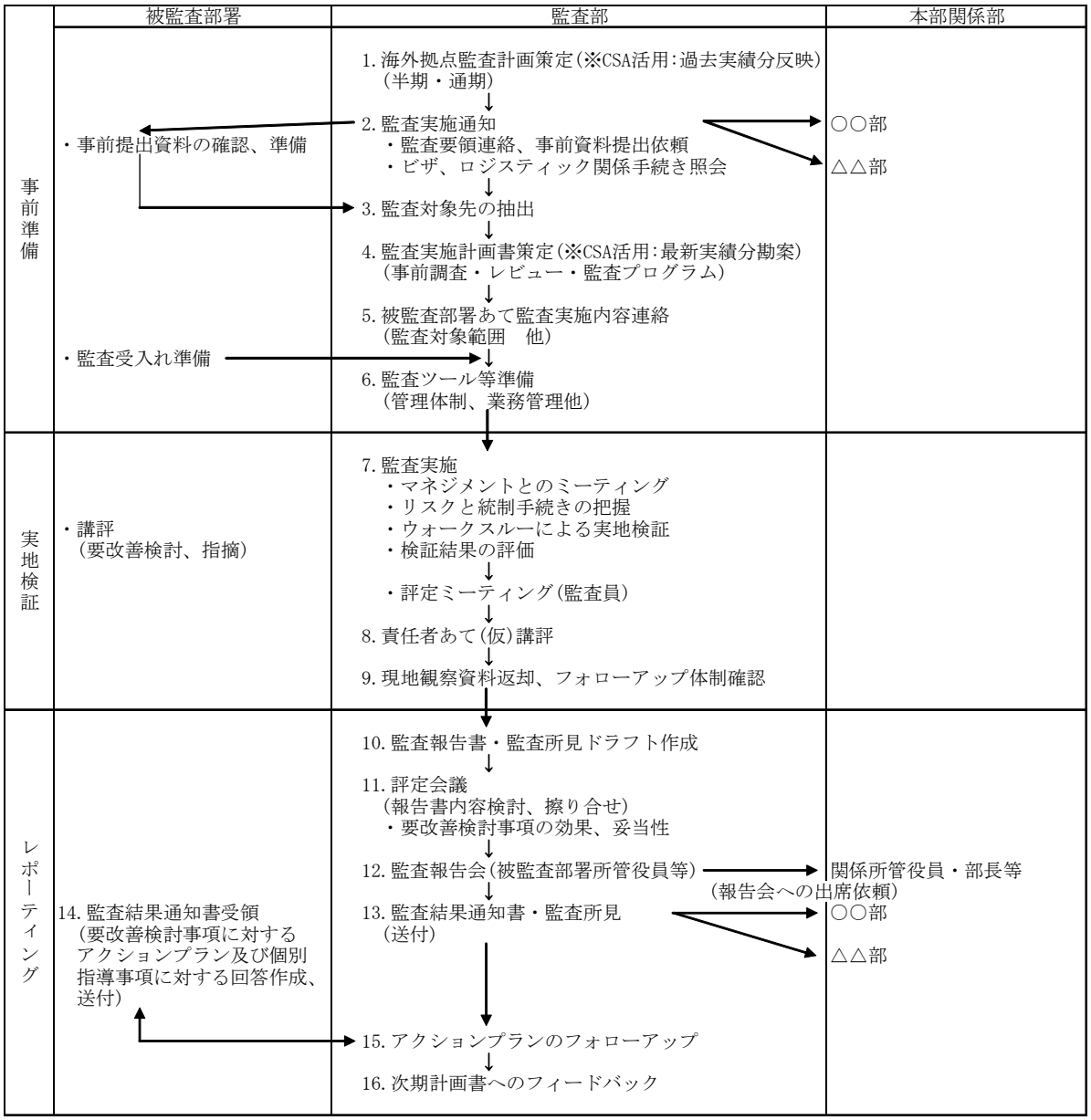
CSA を行う目的は、「ビジネス目的が達成」される「保証」を評価することにある。CSA は、監査手法の一つとして、欧米の内部監査部では比較的利用されているようである。特に最近では米国企業改革法(以下「SOX 法」)の影響もあり、内部監査部のみならず業務部門でも自己検証の手段として使う企業もある。また、「ビジネス目的が達成」される「保証」を評価することは、コーポレート・ガバナンスや財務諸表の開示強化及びリスク管理能力を向上できると考えられており、業務の担当者に内部統制の需要性を認識させて、同時に問題点とその具体的な改善活動を起こす手段として活用されている。

② CSA のリスクベース監査への応用

CSA を実施することで、その実施結果に基づき監査対象を決定するリスクベース監査手法の導入が可能となる。すなわち、CSA の実施結果とあるべき統制とのギャップをただちに修正を要する欠陥と考えず、ギャップから発生する残存リスクをリスク評価した上で、修正すべき欠陥かどうかの判断を行い、監査対象のリスクのポジショニングを実施するのである。

3.　監査フローの紹介

監査フロー(予告監査)



4. 海外関係会社監査についての事例紹介

(1) 各拠点における内部統制部門の状況

① 北米事業(車両の輸入販売)

米国子会社に独立した内部監査部門を設置し、カナダ、米国、メキシコを監査範囲としてカバーしている。

② 欧州事業(車両の輸入販売)

ベルギーの地域統括子会社に内部監査部門を設置し、欧州全域の販売子会社を監査範囲としてカバーしている。

③ 豪州事業(車両の輸入販売)

豪州子会社に内部監査部門を設置し、豪州事業を監査範囲としてカバーしている。

④ 中米事業(車両の製造販売)

コロンビアの子会社に内部監査部門を設置している。

⑤ アジア事業(車両の製造販売)に関しては現状、内部監査部門は設置していない。

(2) 本社と地域統括会社

各地域統括会社の監査部門は、組織的には本社監査本部とは独立した存在となっている。本社監査本部には海外監査チームがあり、これら地域統括会社での内部監査実施状況や発見事項に関する改善状況についての進捗管理を行っている。

本社監査部門が担当する役割は

① 各社監査部門の活動状況(監査計画、実施状況及び各社の統制状況)を集約し、本社担当役員及び経営会議に報告する。
② 本社担当役員及び経営会議からの要望を各社監査部門に伝達、調整を図る。
③ 各社の監査活動を支援する。
④ 年次のミーティングを実施し、各社内部監査部門の交流を促進する(日本／米国／欧州で分担、主催は本社)。

また、担当役員及び経営会議には下記内容を集約、報告している。

1) 各社が作成する中期監査計画
2) 各社からの定期的な監査実施状況/発見事項の改善状況についての報告

なお、発見事項の改善状況については、必要に応じて、月次で各社から報告を受領し、集約・報告する。

(3) 現状の課題

諸般の事情により、弊社にはグローバルなツール（監査プログラム、実施規程、発見事項の評価基準等）の整備が未だ完全ではない為、各社による監査実施レベル（評価基準、対象スコープ等）が十分に統一できていない。

グローバルに統一的なレベルでリスクを適切に評価できているかという点について、未だ十分満足できるレベルに達していない。

適切な内部統制が効果的に運用されていること、あるいは財務諸表上の開示が適切であることについての保証という点では、改善の余地が多大である。

(4) 改善の方向性

① グローバルなツール（監査プログラム、実施規程、発見事項の評価基準等）の整備

各社による監査の実施レベル（対象スコープの選定、実施手順、発見事項についての評価基準等）を統一し、グローバルに統一的なレベルで、リスクの状況を評価できる体制を構築する。なお、各地域の特性により対応できない部分については別途考慮する。

② 内部統制自己診断（CSA）の整備

日本版 SOX 法の施行に向けて、各社において自己診断の積極的な活用を検討している。海外地域という、本社から遠く離れた地域であること、本社のように監査部門を充実できない可能性が高いことを考えると、「オペレーション」が主体となって実施される自己診断の活用はきわめて有効といえる。問題は、いかにして「実効性」のある CSA システムを構築するかにあるといえる。

本来内部統制に関する自己診断のプロセスは、オペレーションが自らの事業目的を達成する上で、これを阻害するリスクに適切に対応するものとして位置づけられている。日常の事業活動の中に組み込まれ、適宜継続的に適用されるものとされている。そして内部監査部門等による、「第 3 者」の定期的なモニタリング活動が、オペレーション部門における内部統制活動（統制状況の評価と改善）を補完することとなる。

この理想形を達成する為にとられるひとつの形が、オペレーション部門を巻き込んだ形で自己診断プロセス及びプログラムを構築することとされているが、その具体的な展開には検討すべき点が多々ある。具体的には、オペレーション部門をどのように巻き込んでいくか、シ

ニアマネージメントからどのようなサポート得るべきか、教育はどうするか、これら一連の活動に内部統制部門はどのように関与すべきか、等々。

今後の監査実務、自己診断プロセスの改善及び日本版 SOX 法への対応施策の検討等の過程を通じて、この課題に継続的に取組んで行きたい。

第４章　IT統制に対する内部監査

1.　ＩＴ統制とは

第１章で述べたように、「金融商品取引法」（仮称：現「証券取引法」）や「（新）会社法」によって、各企業に信頼できる「内部統制」の構築が法的に要請されている。「財務報告に係る内部統制の評価及び監査の基準のあり方について（金融庁 2005 年 12 月 8 日)」によれば、“内部統制は、、基本的に、業務の有効性及び効率性、財務報告の信頼性、事業活動に関わる法令等の遵守並びに資産の保全の４つの目的が達成されているとの合理的な保証を得るために、業務に組み込まれ、組織内のすべての者によって遂行されるプロセスをいい、統制環境、リスクの評価と対応、統制活動、情報と伝達、モニタリング（監視活動）及びＩＴ（情報技術）への対応の６つの基本的要素から構成される。”とされている。今後、企業が内部統制を構築する際には「ＩＴへの対応」も考慮していく必要があり、企業における重要な業務プロセスや基幹業務に関するシステムに対しては、自己点検、内部監査、外部監査人による監査が必要となっていく。「ＩＴへの対応」とは、“組織目標を達成するために予め適切な方針及び手続を定め、それを踏まえて、業務の実施において組織の内外のＩＴに対し適切に対応すること”とされており、「ＩＴ環境への対応」と「ＩＴの利用及び統制」からなっている。

ＩＴ統制とは、広義には「ＩＴへの対応」を指すが、狭義には「ＩＴの利用及び統制」を指す。すなわち“組織内において、内部統制の他の基本的要素の有効性を確保するためにＩＴを有効かつ効率的に利用すること、並びに組織内において業務に体系的に組み込まれてさまざまな形で利用されているＩＴに対して、組織目標を達成するために、予め適切な方針及び手続を定め、内部統制の他の基本的要素をより有効に機能させること”と理解して差し支えない。

2. 業務処理統制と全般統制

ＩＴ統制は、業務処理統制と全般統制から構成されている。「財務報告に係る内部統制の評価及び監査の基準（公開草案）（金融庁 2005 年 7 月 13 日）によれば、「業務処理統制」とは、“個々のアプリケーション・システムにおいて、承認された取引がすべて正確に処理され、記録されることを確保する、コンピュータ・プログラムに組み込まれた統制”とされている。言い換えると、企業の活動が適切に行われるようにするための統制活動のうち、コンピュータシステムによって実現している部分のことである。例えば、購買部署の社員でなければ発注画面を表示することが出来ないとか、発注承認権限のある役職者でないと承認オペレーションが出来ない、といったものが業務処理統制にあたる。

一方、「全般統制」とは、“ＩＴを利用した業務処理統制が有効に機能する環境を保証する間接的な統制”とされている。全般統制には、通常、ハードウェアやネットワークの運用管理、ソフトウェアの開発、変更、運用並びに保守、アクセス・セキュリティ及びアプリケーション・システムの取得、開発並びに保守に対する統制を含む。例えば、発注画面を表示するプログラムに不正な変更が加えられないようにするとか、利用者のＩＤやアクセス権の管理を行う仕組みの維持などが全般統制にあたる。

全般統制と業務処理統制は、完全かつ正確な情報の処理を確保するために一体となって機能するものであり、どちらか一つだけが信頼できれば良いというものではない。特に全般統制の不備は、直接的には重大なリスクに繋がるものではないが、全般統制に重要な不備があった場合には、たとえ業務処理統制が有効に機能するようにデザインされていたとしても、その継続的な運用を支える情報システムの内部統制は有効に機能せず、リスクが高まることとなる。

3. ＩＴ統制に対する内部監査

(1) ＩＴ利用環境の理解

ＩＴ統制の有効性を評価しようとする内部監査人は、まずＩＴ利用環境を理解する必要がある。ＩＴ利用環境を理解するためには、次表のＡからＧで示す事項を把握しなければならない。外部監査人が行う監査でも、被監査部門はこれらの事項に関して説明をする必要があるので、日頃から整理しておくことが重要である。

項目	理解すべき内容
A. ＩＴインフラの概要	ハードウェア構成、基本ソフトウェア構成、 ネットワーク構成
B. アプリケーション・システムの構成	アプリケーション･システムの機能の内容、 主要な入力データ・データファイル・出力情報、 データの流れ、システム間のインターフェース
C. 電子商取引の利用状況	情報提供のみ、メール注文程度、 Web 注文・決済可能、基幹システムと連動
D. 情報システムに対する投資	ハードウェア関連費用、ソフトウェア関連費用、 システム関係人件費、外部委託費、IT 担当人員、 組織構成
E. 情報システムの変更	業務要件の変更有無と内容、 不具合修正の変更有無と内容
F. 情報システムの安定度	重要な障害・トラブルの概要、原因と対応、 再発防止策
G. 外部委託の利用状況 （アウトソーシング）	開発委託、常駐委託、情報処理の外部委託
H. 業務提携の状況 （アライアンス）	支配関係のない業務提携先の IT の信頼性

(2) 全般統制の評価

全般統制を評価するに際に重要なことは、まず対象となる全般統制の数と管理部署を把握することである。

従来は、大型汎用コンピュータを中心とするホスト系システムを中心に考えられてきたので、アプリケーションの共通基盤としての全般統制は、単純にいえば一つであった。管理部署についても、例えば情報システム部といったＩＴに関する専門部署が担当していることが多いため、全般統制を容易に識別することができた。

昨今は、クライアント・サーバ型のシステムが多く利用されており、業務担当ごとにシステムを管理していることも少なくない。このようなケースでは、全般統制は情報システム部のみが担当するだけでなく、業務アプリケーションごとに担当が異なっている可能性がある。全般統制の数も一つではなく、複数の全般統制が存在することも多い。さらに、全般統制と業務処理統制との区別が明確にできず、情報システム部以外の複数のユーザ部署を全般統制の範囲に含めることがあるので注意が必要となる。

また、Web アプリケーションを利用するシステムであれば、個々のアプリケーション・システムに対する、開発、変更、運用及び保守といった全般統制だけではなく、ネットワーク全体の運用・管理まで一体とした統制活動としての全般統制となる。EDIやインターネットを通じてデータが入出力される環境であれば、従来、企業が管理できていたハードウェアやソフトウェアも、他の企業や個人の支配下にあることになるため、企業外における全般統制の適用状況について、直接的ないし間接的に把握する必要がある。

全般統制は、ＩＴの企画･開発から運用や外部委託まで幅広く関係しているが、大きく以下の 4 つに分類することが出来る。

「情報システムに関する企画・開発・調達業務の統制活動」

「情報システムに関する運用・管理業務の統制活動」

「セキュリティに関する統制活動」

「アウトソーシングの統制活動」

各々の統制活動と評価のポイントについて説明する。

「情報システムに関する企画・開発・調達業務の統制活動」では、情報システムの新規開発やパッケージソフトの導入、並びに情報システムの運用・管理のための内部統制がデザインされているかについて評価する。

情報システムに適切な内部統制を組み込むためには、企画・開発・調達段階で組み込むべき内部統制の内容を検討する必要がある。企業が情報システムに関する企画・開発・調達の過程を適切に管理していない場合には、例えば未承認の発注取引を防止する機能を組み込んでいないなど、完成した情報システムの信頼性が期待できないことがある。このように、情報システムに関する企画・開発・調達は、他の内部統制の整備状況や運用状況に影響を与える。特に、ユーザ部門の参画による十分なテストの実施・検収や、適切なプログラム等の移行・変更管理は、情報システムの信頼性に影響を与えるので十分に評価することが重要である。

「情報システムに関する運用・管理業務の統制活動」では、企業が適切なデータを適切なプログラムで処理し、信頼できる処理結果を得るための内部統制をデザインしているかについて評価する。

この内部統制には、例えば、運用・管理業務のコントロールとして次の事項が含まれるので評価する際の参考にするとよい。

・オペレータによる手動又は自動実行ツールによるプログラム等の運用手順
・プログラムによる処理結果の確認手続
・実行スケジュール管理
・エラーが発生した場合の再処理の方法を含めた対応手順
・不具合が発生した場合のプログラムの修正手順
・適切なプログラムの使用のためのライブラリ管理

「セキュリティに関する統制活動」では、データ、ソフトウェア、ハードウェア及び関連設備等の不正使用、改竄、破壊等を防止するために、アクセス管理や自然災害等への対策のための内部統制をデザインしているかについて評価する。

この内部統制には、アクセス管理用のソフトウェアを導入し、ＩＤとパスワードの組合せをプログラムでチェックするような論理的なものだけでなく、コンピュータルームへの入室を制限して、ハードウェアの物理的な破壊や盗難を防止するような物理

的な対策も含まれる。セキュリティに関する方針を、情報システムの企画・開発・調達段階においても検討し、文書化することが必要である。

「アウトソーシングの統制活動」では、情報システムの開発業務や運用業務等につきアウトソーシングを利用している場合には、委託業務を管理するための内部統制をデザインしているかについて評価する。

受託会社の選定基準、成果物等の検収体制、受託会社の内部統制を理解し、自社の内部統制に与える影響等を評価しているかどうかは重要な評価ポイントである。また、企業がその製品の物流・保管につきアウトソーシングを利用している場合のように、企業の基幹業務の一部を受託会社が担っている場合には、受託会社のシステム障害が、企業の業務の運営に支障をきたす可能性があるので、企業と受託会社との間で合意されているサービスレベルにも留意する必要がある。

(3) 業務処理統制の評価

業務処理統制は、業務プロセスに様々な形で組み込まれているが、大きく分けて 2 種類の統制活動がある。

・アプリケーション・システムに組み込まれた統制活動（自動化された統制活動）

・人とＩＴが一体となって機能する統制活動（ＩＴによる情報を使用した統制活動）

いずれの統制活動であっても業務プロセスを把握し、業務処理統制がどのように貢献しているかについて内部監査人は把握する必要がある。

また、アプリケーション・システムは、業務プロセスごとに作成されることが多いため、内部監査人は、企業の実態に応じてアプリケーション・システムを分析することが重要である。アプリケーション・システムは、企業の業務プロセスを支え、会計に関連する情報及びデータを提供しているが、その業務処理統制を評価するための指針として、例えば、次のＩＴのコントロール目標が挙げられる。

会計データの網羅性

・会計データが漏れなく、重複なく記録され、残高更新され、未決済及びエラーとなった会計データは、期間内に全て適切に処理されていること

会計データの正確性

・会計データは、正確に適時に適切な勘定に記録されていること

・エラーとなった会計データは、期間内に全て適切に処理されていること

会計データの正当性

・会計データは、当該企業に財務的影響を及ぼす取引その他の事象を表し、かつ当該企業に承認されたものだけが入力され、処理されていること

・適切な職務権限に応じて、アクセス権限が設定され、適切な担当者により処理されていること

ファイルの維持継続性

・マスタ・ファイルは、常に最新の状態に保たれ、正しく維持及び継続されていること

・異なるＩＴ間で利用される分散マスタ・ファイル間の整合性が保たれていること

(4) 改善の方向性

従来、内部監査人はいわゆる業務監査を行うことが多く、情報システムを対象とした監査については大きく踏み込めていなかったと思われる。しかしながら、昨今、企業のＩＴ依存度はますます増加しており、過失や故意による不適切な情報処理、システム障害や情報漏洩などのセキュリティ事故が企業やステークホルダーに与える損害は計り知れない。内部監査人は、単なる財務報告目的だけでなく、業務の有効性や効率性を高め、ひいては企業価値を高めるようなＩＴの利用に向けて、有意義なチェックと助言を行っていくべきであろう。

情報システムの監査は専門性が高いと敬遠されがちであるが、情報システム部門に対する業務監査という理解で、全般統制の評価から取り組んでいけば、少しでも負担が少ないのではないだろうか。リスクを低減させるための統制活動について被監査部門から説明を受け、運用されている記録を確認することから始めるといった方法でも十分にスタートが切れると思われる。また、外部の専門家を活用する際にも、丸投げにすることなく一緒に参加していくことで、情報システムの監査に関するスキルもアップしていくと思われる。

以上

＜参考文献＞

- 「CSR マネジメント及び情報開示並びに保証業務の基本的考え方について」
  （日本公認会計士協会　経営研究調査会研究報告第 26 号 2005 年 7 月 20 日）
- 「これが金融機関の内部監査だ」
  （先端内部監査研究会 金融財政事情研究会 2005 年）
- 「内部統制の実践的マネジメント」
  （KPMG ﾋﾞｼﾞﾈｽｱｼｭｱﾗﾝｽ 東洋経済新報社 2005 年）
- 「財務報告に係る内部統制の評価及び監査の基準のあり方について」
  （金融庁 2005 年 12 月 8 日）
- 「財務報告に係る内部統制の評価及び監査の基準（公開草案）」
  （金融庁 2005 年 7 月 13 日）
- 「財務諸表監査における情報技術（IT）を利用した情報システムに関する重要な虚偽リスクの評価及び評価したリスクに対応する監査人の手続について」
  （日本公認会計士協会 IT 委員会報告第 3 号 2005 年 7 月 6 日）
- 「内部監査部門としてのホールディングス体制対応（関係会社自己監査とモニタリング業務の導入）」
  （日本内部監査協会主催セミナー「企業価値経営と内部監査の実践」
  ㈱ＣＳＫホールディングス　播磨 昭彦氏 2006 年 3 月 9 日）

以上