エンタープライズ・リスク・マネジメントと経営者にとっての保証とは

ＫＰＭＧビジネスアシュアランス株式会社
シニアコンサルタント
三宅 弘子

はじめに

エンタープライズ･リスク･マネジメント（以下ERM）ということばは、日本でも広く知られるようになってきた。“リスク”を、保険や財務の領域、あるいは金融機関だけの話と考えている経営者はいないだろう。将来は常に不確実性をはらんでいるものであり、複雑で絶え間ない内外環境の変化にさらされながら会社の舵取りを行っている企業の経営者にとっては、収益、成長、リスクのバランスをいかに取るかということはまさしく経営そのものである。したがってERMは企業経営上の中核的な要素であって、トップマネジメントが積極的に関与していかなければならない課題であることは、誰しも異論のないところと思われる。

企業の社会的責任（CSR）やコンプライアンスの問題が注目を集めていることからも分かるように、現代の企業は増大する法的･社会的責任のプレッシャーの中に置かれている。同時に、資本主義経済の中で、企業が競争に勝ち抜き、成長を続けていくためには、効率的経営は至上命題である。こうした現実の中、多くの経営者はERMに少なからぬ関心を持ち、何かしなければならないとは思いながらも、「どこまでやれば十分なのか」を明確にできず、遵法と効率のジレンマに直面することが多いのでないだろうか。その一因としては、ERMについての議論が、経営者として“何をすべきか”ということに偏り、ERMが経営者にとって“何を意味するのか”、経営者はERMによって“何を得るのか”、という視点が欠落しがちなためではないかと考えられる。

そこで本稿では、ERMから経営者は何を得るのか（何を得るべきか）を改めて問い直し、ERMの意味とあり方を考えてみたい。具体的には、「ERMは経営者に対して保証（assurance）を提供するプロセスである」とするCOSO（注1）の定義に着目し、経営者にとってERMは「保証」の根拠であるととらえた上で、経営者にとっての保証とはどのようなものであるかを考察する。そして実際に保証の根拠とはどのようなところに求められるのか、英国におけるリスク･マネジメントと内部統制の実行指針を参考に見ていくこととしたい。

ERMと経営者の責任

ERMについては種々の定義やフレームワークが研究･発表されているが、基本的な考え方は、企業の目標や戦略の遂行に（主としてマイナスの）影響を与える将来の潜在的可能性（＝リスク）について、個別にではなく組織全体で体系的に把握し対応するというものである。ERMを経営に取り入れることについては、企業価値の維持･増大、競争力の強化、持続的発展等、企業としての使命やステークホルダーに対する責任を果たすという効果が強調されることが多い。ERMがコーポレート･ガバナンスや企業戦略における重要なテーマに位置づけられるようになってきているのは、このためである。

他方、企業の不祥事によって広範なステークホルダーが損失を被る事件が後を絶たず、国際的にコーポレート･ガバナンス改革の機運が高まり、経営者自身によるERMへの真剣な取り組みがますます強く求められるようになってきた。海外に目を向けると、企業の財務･会計を巡る大規模なスキャンダルが多発した反省から、内部統制の構築、適切な情報開示についての経営者責任の明確化･厳格化が急速に進んでいる。最もよく知られるのが米国の『企業改革法（サーベインス･オックスレー法）』（2002年7月成立）である。このほか英国『統合規範（コンバインド･コード）』の制定（1998年6月公表、2003年7月改訂）およびそのロンドン証券取引所上場規則集への添付があり、フランスでも『ファイナンシャル･セキュリティー法』（2003年8月成立）により内部統制の強化と情報開示の充実が義務づけられた。

わが国においては、経営者がリスク管理体制の構築義務を負っていることを初めて法律の面から明らかにしたのは、大和銀行株主代表訴訟一審判決（2000年9月大阪地裁）であった。また神戸製鋼所の総会屋利益供与事件株主代表訴訟（2002年4月神戸地裁）でも、取締役は内部統制システムを構築すべき法律上の義務があるとの所見が示された。しかしその後も、企業による虚偽の情報開示等の不祥事が相次いで発覚し、かねてより問題視されていた日本企業の情報開示への意識の低さ、財務報告の信頼性の薄弱さが改めてクローズアップされることとなった。これに対する具体的な対応策としては、2003年4月に証券取引法上の開示制度の改訂（いわゆる代表者確認制度の導入等）（注2）、今年に入ってからは同法の民事責任規定の整備および有価証券届出書の虚偽記載に対する課徴金制度の導入（注3）、そして東京証券取引所の上場規則見直し（注4）等が行われた。金融審議会では引き続き、米国企業改革法に倣った内部統制に係る外部監査の義務化や、継続開示（有価証券報告書）の虚偽記載に対する課徴金制度の導入等を模索している。さらに法制審議会にて現在検討が進められている会社法制の現代化においても、内部統制の整備義務が法律に明記される方向にある。

経営者にとってのERMの意味

このように、企業経営者の責任が一層重く厳しいものになっていく中で、経営者は、ERMに必要な経営資源（人、情報、時間、金）とそれによって得られる効果のバランスに従来以上に注意を払う必要がある。なぜならこれまでは、ERMへの積極的な取り組みは先進的あるいは優良な企業としての評価につながっていたが、いまや情報開示も内部統制も企業として当然行うべき義務と見なされ、怠れば罰則さえ受けかねない時代だからである。では、どこまでどのようなERMを実行すれば経営者として十分な責任を果たしたといえるのだろうか？　その答えを考えるには、経営者にとってのERMの意味を改めて問うてみることが有意義であると思われる。

ここで注目したいのが、2004年9月29日にCOSOが公表した『エンタープライズ・リスク・マネジメント：統合的枠組み（Enterprise Risk Management- Integrated Framework、以下COSO ERM）』におけるERMの定義である。COSO ERMでは、ERMとは「経営者（management）および取締役会（board of directors）に対し、目標の達成について合理的な保証（reasonable assurance）を提供するためのプロセス」であると定義しているのである。これはつまり、経営者および取締役会にとってのERMは「保証」の意味があり、逆にいえばERMは、経営者や取締役会にとって「保証」となるような形で行われるべきであると解することができる。

また、英国の『統合規範』に関連して作成された『ターンブルの実行：取締役会への説明（Implementing Turnbull: A Boardroom briefing）』（注5）にも、「取締役会はどこに保証を見出すことができるか？」という項目があり、経営者と取締役会にとっての保証はリスク・マネジメントと内部統制の運用に根拠を求めることができるとしている。

「保証」の概念

では「保証」とは何であろうか。ここでいう「保証」は保証書や債務保証などのguaranteeの意ではなく、assuranceを原語とする。assuranceということばは、生命保険の意味で使われる以外にリスク・マネジメントの世界ではあまり馴染みがないが、監査論および監査実務においては従来より用いられている用語である。そこでまず、監査の世界における保証の概念を確認しておきたい。

監査での保証の概念ないし公認会計士による保証業務については、統一的な定義はないとされる。そこで代表的なものとして次の2つを挙げる。

■国際監査基準（ISA）による「保証」の定義：
　ある者が他者の利用に供する目的で行う主張の信頼性に関する監査人の満足に関係している。このような保証を提供するためには、監査人は、実施された手続によって収集された証拠を評価し結論を表明する。したがって、満足の度合い、および提供される保証水準は実施された手続とその結果によって決定される。

■米国公認会計士協会（AICPA）の保証業務特別委員会（通称エリオット委員会）による「保証業務」の定義：
　意思決定者のために、情報の質、あるいはその内容の質を向上させる、独立した専門的職業家の業務。

これらをもう少し一般化すると、保証とは“ある情報の質や内容について、客観的な手続と基準によって評価・判断し、その情報の利用者にとっての信頼性を高めること”と表現することができる。そして上述したERMの定義の文脈にこの概念を当てはめるならば、企業のリスクを一定のフレームワークや基準に基づき、ある程度の（合理的な）確信をもって評価・判断する仕組みがERMであり、その情報に基づいて企業の経営者と取締役会が意思決定を行うことによって、企業目的を達成する可能性を高めることができるわけである。なおERMが与えることのできる保証が、絶対的でなく「合理的」水準にとどまるのは、リスクは本質的に将来に関わることであり、人間にとって将来は正確に予測しきれないこと、そしてERMは人間によって実行されるため自ずと限界があることが前提となるからである。

経営者にとって必要な保証の水準

COSO ERMでは、事業体の目的（entity's objectives）として、戦略（strategic）、業務（operations）、報告（reporting）、遵法（compliance）の4つを挙げている。これは、企業の目的を分類してみるとこの4つのいずれか（1つとは限らない）にあてはまるということであり、当然ながら優先順位や重みづけはその企業の置かれた環境、持っている能力、企業戦略などにより異なる。経営者が目的をどのように設定し、重要性や難易度をどう考えるかによって、必要とする保証の範囲および程度も変わり、したがって保証を得るための取り組みも違ってこよう。重要かつ困難な目的であればそれだけ高い水準の保証を求めるであろうから、当該目的に関わるリスクの特定や評価、統制、モニタリングといった一連の活動に、より多くの労力やコストをかけることになる。

端的にいえば、経営者が必要とする保証の水準とは、ある意思決定を行うに際して自分が必要とする情報が得られるという確信の持てるレベルであって、それは経営者判断の範疇ということである。

たとえば、先に触れた代表者確認制度を例にとって考えてみよう。同制度は証券取引法に導入されたもので、企業の代表者が自社の有価証券報告書などの記載内容が適正であることを確認した旨の文書を、その有価証券報告書等の添付書類として提出するものである（2003年4月1日以後開始する事業年度について任意）。確認書に記載すべき事項についてのガイドラインはあるが（注6）、確認の方法や手順、適正性を判断する基準、報告の要件等についての規定はない。その意味するところは、何をどこまでやって「適正であることを確認」したことになる

のかを判断するのは経営者であり、とりもなおさず経営者が求める保証の程度との関係で決まるということである。実際、2004年3月期は約50社が確認書を提出したが、確認の方法も程度も企業によって差が見られた。とはいえ、経営者としての説明責任を考えれば、確認の方法や根拠は客観的に見て妥当で合理的であることが必要であり、保証を得るための具体的手法や範囲については社内外の専門家の助言を仰ぐことが望ましいといえよう。

どのように保証を得るか

保証は、まさにERMを構成する諸活動から得られる。COSO ERMでいえば8つの構成要素（内部環境、目的設定、事象識別、リスク評価、リスク対応、統制活動、情報と伝達、モニタリング）がこれに該当する。また、前述の『ターンブルの実行：取締役会への説明』では、取締役会にとっての保証の源泉（sources of assurance）になりうるとして以下のものを挙げている。

■リスク･マネジメント･プロセスの取締役会でのレビュー
■業績およびリスク指標に関する月次報告
■管理職による確認
■早期警告メカニズム
■独立的なモニタリング活動（内部監査等）
■財務諸表の監査
■特定の研究、リスクの見直し
■主要な従業員の意見と確認
■執行役員の意見
■業務担当役員の意見
■財務担当役員の意見

また、リスクの特定に利用される手法である自己査定（CSA）のためのワークショップや、面談、円卓会議等での意見収集も、保証を得る方法として有効であるとしている。ただし、これらの根拠の有効性レベルは、以下の要素によって変わると述べている。

■プロセスが実施されている範囲
■役員までの情報伝達速度
■残余リスクの管理能力
■主要な事業目標に対する重点
■リスク認識のタイミング

これらの保証の根拠は、互いに補完的であり、また継続的に見直しが必要なものと考えるべきである。たとえば財務諸表監査は、保証を得る一つの根拠にはなりうるが、外部監査人による法定監査だけでは経営者にとって十分な保証とはいえない。なぜなら監査人は、企業の業務を日常的に監視しているわけではなく、ある時点におけるプロセスや財務報告しか見ないからである。日常的かつ継続的に業務を実行･管理している執行役員、管理職、および従業員から、信頼できる情報を得る仕組みがあってこそ、経営者にとって安心できる、質の高い保証を得ることが可能になるのである。

上に掲げた例からも分かるように、保証源の信頼性は組織構成員のリスクに対する意識によるところが大きい。COSO ERMや、ターンブル･ガイダンスの手引きが共通して強調しているのは、ERMに全従業員を参加させ、それぞれに何らかの責任を持たせることである。それがERMの成功に結びつくには、従業員に会社の状況、目標、直面しているリスク等を十分に伝達し、ERMの目的と、経営者意識を理解させることがポイントである。これはCOSO ERMでいうところの「内部環境」という構成要素であり、ERMの構成要素の中でも最も基礎であるとされ、経営者はこの内部環境をできるだけ良好なものにすることについて重要な役割を担うとされている。つまり経営者にとっては、内部環境の整備と強化によって、ERMによって自分が得る保証の質を高めることになるのである。

まとめ

冒頭に述べたように、企業の経営者は今までにも増して、自覚と積極性と責任をもってERMの構築と実践を推し進めていくことが、ステークホルダー、社会、そして監督官庁からも期待されている。その際、ERMのために何をしなければならないか、ということよりも、ERMを行うことによって何を得たいか、という視点で取り組むことが必要と思われる。なぜなら、ERMは目的ではなく手段であるにもかかわらず、それを法律や規制によって背負わされた必要条件としてとらえてしまうと、形式主義や不要なコスト増を招き、本来のERMの意義を見失う恐れがあるからである。現実に企業が置かれた環境、事業体としての成熟度や競争力を無視したお仕着せのERMでは、事業活動や目標とかけ離れたところでただ煩雑な作業が増すだけである。その意味で、COSOやターンブル･ガイダンスは、その通りに実行しなければならない“To-doリスト”ではなく、自社のリスクを網羅的かつ体系的に整理･分析し、対応の弱点を発見するためのツールとして活用してこそ有効である。企業が抱えるリスクは個々に異なるはずであり、また企業の使命、事業目標もさまざまなのだから、ERMへの取り組み方も保証の質についても、画一的な基準を教科書的なフレームワークに求めることはできないし、すべきではない。

公認会計士による財務情報に関する保証が、企業が開示する情報の質を向上させ、投資家や株主が正しい投資意思決定を助けることを第一義的意義としているのと同様に、優れたERMによる保証は、経営者および取締役会にとってのリスク関連情報の質を高め、それがより適切な、あるいは迅速な意思決定や経営判断を可能にする。だからこそ、ERMを通じ、リスクを適切に管理し事業会に生かすためのPDCAを組織と業務の中に組み込み、継続的なモニタリングとフィードバックによってその仕組みを強化することが、経営者にとっての保証の質を高め、もって企業価値の増大やステークホルダーに対する責任を果たすことにつながるといえるのである。

（注1）米国トレッドウェイ委員会組織委員会（The Committee of Sponsoring Organizations of the Treadway Commission）の略称。
（注2）2004年3月11日金融庁発表『企業内容等の開示に関する内閣府令等の一部を改正する内閣府令案の公表について』

（http://www.fsa.go.jp/news/14_news.html）参照。

（注3）第159回国会における金融庁関連法律案『証券取引法等の一部を改正する法律』（2004年3月15日提出、同年6月2日成立）（http://www.fsa.go.jp/houan/houan.html）参照。

（注4）東京証券取引所2004年11月16日社長会見資料（http://www.tse.or.jp/guide/interview/index.html）参照。

（注5）英国『統合規範Committee on Corporate Governance；The Combined Code』における内部統制要件を実行するための指針『内部統制：統合規範に関する取締役のためのガイダンスInternal Control；Guidance for Directors on The Combined Code』（通称『ターンブル・ガイダンス』、1999年9月公表）を実行するための、実務的な手引き。

（注6）『企業内容等の開示に関する留意事項について（開示ガイドライン）』（http://www.fsa.go.jp/guide/guidej/kaiji/01.pdf）5-29-2参照。

【主要な参考文献（順不同）】

・日本公認会計士協会・次世代会計士保証業務研究会『公認会計士保証業務～基礎概念、実務、および責任の研究～』日本公認会計士協会（2000年）

・KPMG著・KPMGビジネスアシュアランス株式会社訳・八田進二監訳『企業価値向上の条件－ターンバル・ガイダンス』白桃書房（2002年）

・経済産業省・リスク管理・内部統制に関する研究会『リスク新時代の内部統制～リスクマネジメントと一体となって機能する内部統制の指針～』（2003年）

・Enterprise Risk Management- Integrated Framework, The Committee of Sponsoring Organizations of the Treadway Commission, 2004.

・Implementing Turnbull: A Boardroom Briefing, The institute of Chartered Accountants in England & Wales, 1999.