公表されたエンタープライズ・リスク・マネジメント（ERM）の統合的枠組み

野村　亜紀子

要　約

1. 米国では 2004 年 9 月、トレッドウェイ委員会組織委員会（COSO）により「エンタープライズ・リスク・マネジメント（ERM）の統合的枠組み」（ERM フレームワーク）及び「適用テクニック」が公表された。2003 年 7 月に草案が公開されて以降、1 年余りを経てのことだった。
2. ERM は一般に、企業の個々の組織や部門を超えた全社的なリスク管理を意味する。企業行動を規律付ける仕組みの一つであり、コーポレート･ガバナンスと相互に関連し、補完しあう関係とも言える。
3. COSO の ERM フレームワークの主たる目的は、近年注目の高まっている ERM に関する統一概念の提示にあった。草案に対するコメントでは、例えば「リスク」の定義をめぐって、議論が行われた。
4. COSO の ERM フレームワークは、ERM のグローバル･スタンダードとなる可能性も有しており、わが国企業も意識しておく必要があろう。

Ⅰ．背景

米国で 2004 年 9 月、トレッドウェイ委員会組織委員会（COSO）より、「エンタープライズ・リスク・マネジメント（ERM）の統合的枠組み」（以下、ERM フレームワークとする）が、適用テクニック編と共に公表された[1]。

ERM とは一般に、企業内の部門や組織をまたがる全社的なリスク管理を意味するが、近年、ERM に対する関心が高まるにつれて、統一概念や共通の枠組みの不在が指摘されていた。今回の ERM フレームワークは、この問題に対処すべく、COSO が提示したものである。2003 年 7 月に草案が公表され、3 ヶ月のコメント期間を経て、最終版が作成された。

会計・監査専門家の集まった組織である COSO は、92 年、今やグローバル・スタンダードとなった内部統制の統合的枠組みを提示したことで知られる。COSO によると、内部統制と同様に、ERM フレームワークが企業のリスク管理のベンチマークとなることが期待されている。

折しも、後述するように、米国登録企業は、サーベンス・オクスレー法 404 条により年次報告書の中で「内部統制報告」を行うことが義務づけられ、企業はそのための対応に追われてきた。そのような中で、COSO の提示するフレームワークがどのように受け入れられていくのかも注目されている。

Ⅱ．ERM の位置付け

全社的なリスク管理である ERM は、企業の活動を企業内部において規律付けるためのプロセスと言える。その意味では、法令違反等がないようにするための社内体制である内部統制と同じ範疇に入る。なお、後述するように、COSO のフレームワークでは、ERM は内部統制を内包するものとして位置付けられている。

一方、企業経営者が株主の利益に沿った行動を取っているかどうかを監視するのが、コーポレート・ガバナンスである。ERM、内部統制ともに企業経営者が最終責任者であり、また、経営者のコミットメントが成否を分けるとも言われていることから、この両者は経営者の行動監視の決定打にはなりえない。他方、取締役会にせよ株主にせよ、企業の戦略策定プロセスや日々の業務執行に常時目を光らせることは不可能である。このように、企業行動の規律付けにおいて、コーポレート・ガバナンスと ERM とは相互に関連し、補完し合う関係にあると位置付けられる（図表 1）。

Ⅲ．ERM フレームワークの概要[2]

１．統一概念の提示

上述の通り、ERM フレームワークの主たる目的の一つは、ERM に関する用語の定義、概念の統一にある。その主立ったものを挙げると以下のようになる。

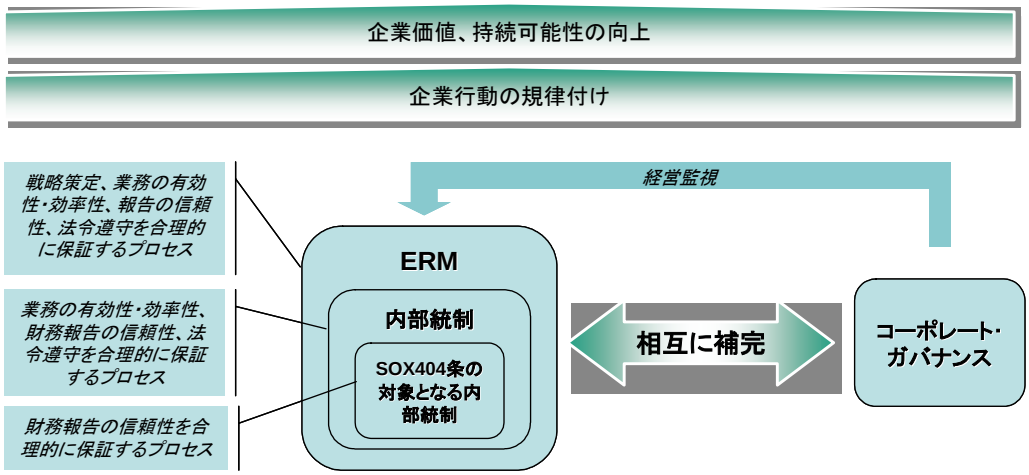
①不確実性（uncertainty）と価値（value）

ERM は、営利組織であれ、非営利組織であれ、ステークホルダーのための価値創造を目的とすることを前提としている[3]。経営陣は、ステークホルダーの価値増大のために、どの程度の不確実性を受け入れられるかを判断しなければならない。

不確実性はリスクと機会の両方を伴う。不確実性は、事象の発生頻度とその重大性を正確に判断できないことによりもたらされる。また、経営判断によりもたらされる場合もある。

価値の創造、維持、減少は、経営陣の決定により起こる。経営陣が、成長とリスクの最適バランスを保つ形で戦略・目的を設定し、

図表 1　ERM とコーポレート・ガバナンス



（注）SOX＝サーベンス・オクスレー法
（出所）野村資本市場研究所

効率的・効果的な資源配分を行う時に、価値の最大化が実現する。

②事象（event）、リスク（risk）、機会（opportunity）

事象とは、組織の目的達成に影響を与えるような企業内外の出来事である。このうち、悪影響を与える事象発生の可能性がリスク、好影響を与える事象発生の可能性が機会である。

悪影響を与える事象は価値創造の妨げや価値の喪失につながる。例えば機械の故障、火事、クレジットの喪失である。顧客の需要が生産力を上回った結果、需要を満たせず顧客の支持を失い、将来の受注減につながるといったことも含まれる。

機会は価値の創造と維持につながるもので、経営陣は機会を戦略または目的設定のプロセスに反映させ、機会を獲得するための行動を決定する。

③ERM とは

ERM とは、「企業の目的の達成に関して、合理的な保証を提供することを意図し、取締役会、経営者およびその他の構成員によって遂行され、戦略策定において企業全体にわたって適用され、企業に影響を与える潜在的な事象の特定とリスクの適正範囲内での管理のために設計されたプロセス」と定義される。

上記の ERM の定義は、以下のような基本的な概念をふまえて行われている。

- ERM は、企業の中で継続的、かつ全社に流れるプロセスである。
- 組織の全レベルの人員により実施される。
- 戦略策定に適用される。
- 全社的に、あらゆるレベルに適用され、リスクのポートフォリオ的視点を伴う。
- 企業に影響をあたえる事象の特定、リスク管理のために設計される。
- ERM は合理的保証を与えるのであり、絶対的保証は提供しない。
- ERM により、単一もしくは複数の目的達成を目指す。そのためのプロセスであり、それ自体が目的ではない。

また、ERM フレームワークでは、「企業の目的」として、次の 4 つのカテゴリーを設けている。

- 戦略：ハイレベルの目的に関するもので、企業のミッションを支える（戦略策定）
- 業務：企業の資源の効果的・効率的な活用に関するもの（業務の有効性・効率性）
- 報告：企業の報告の信頼性に関するもの（報告の信頼性）
- 法令遵守：企業に適用される法規の遵守に関するもの

上記の ERM の定義は、COSO の内部統制の定義を発展させたものである。COSO の内部統制は「①業務の有効性と効率性、②財務報告の信頼性、③法令遵守、のカテゴリーに分けられる目的の達成に関して、合理的な保証を提供することを意図した、企業の取締役会、経営者およびその他の構成員によって遂行されるプロセス」と定義され、これが世界各国の企業により共有されている。

内部統制と比較して新たに加わった点としては、ERM が企業の戦略策定にも適用され、したがって、達成すべき企業の目的の一つに戦略策定が含まれると同時に、下記の 8 つの構成要素に目的設定が含まれている点が指摘できる。ERM は全社的に適用されリスクのポートフォリオ的視点を伴うことも新しい点である。

また、企業の目的の一つである「報告の信頼性」には、社内外の関係者に対して出されるあらゆる報告書が含まれる。この点、内部統制では「財務報告の信頼性」とされていた。一見細かな違いだが、内部統制から ERM フレームワークへの発展にあたって、財務報告を中心とする会計・監査の視点からの転換がさらに進められたことが端的に表れている。

図表 2　ERM フレームワークの構成要素

構成要素	概要	適用テクニックの例
内部環境	・ERM の他の要素の基盤を形成し規律をもたらす ・企業の ERM 哲学、リスク選好、取締役会による監視、倫理観、経営者による権限委譲	・経営者がリスク管理哲学に関するステートメントを作成する ・「組織の長は倫理的行動について手本になっているか」などを問うサーベイを定期的に社員に行う ・行為規範の作成
目的の設定	・戦略、業務、報告、法令遵守の 4 つのカテゴリーから成る目的の設定 ・企業のリスク選好とリスク許容度に沿って行われる	・戦略目標設定プロセスにおける、シナリオ分析、モデリング、ストレス・テスト等のリスク評価テクニックの利用 ・リスク選好の定性分析、定量分析（発生頻度と重大性、キャピタル・アット・リスクとリターンなど）
事象の特定	・経営者による、企業に影響を与えうる事象の特定と、リスクか機会かの判定 ・企業全体に関わる企業内外の様々な要因が対象	・事象の一覧リスト（社内で作成、社外調達） ・社内の複数部門にまたがる会合による事象の把握 ・個別インタビューによる率直な意見の把握 ・質問票による調査 ・先行リスク指標、エスカレーション・トリガーの事業部門目的別整理 ・損失につながる事象に関するデータ・トラッキング ・事象の分類によるリスクと機会の把握
リスク評価	・リスクが目的達成に与えうる影響の程度を把握する ・経営者は、発生頻度と重大性の 2 方向から、通常は定性的及び定量的手法を組み合わせて評価 ・内在・残留リスクの両方を評価	・定性分析：発生頻度の序列に応じたリスク分類、重大性の序列に応じた損失の測定 ・定量分析：バリュー・アット・リスク、バック・テスティング、センシティビティ分析、シナリオ分析、ストレス・テスティング等 ・リスク・マップの作成 ・部門ごとのリスク評価に基づく、全社的なリスク・プロフィールの作成
リスク対応	・回避、軽減、分担、保有 ・経営者は発生頻度と重大性への影響、費用対効果を考え、残留リスクを許容度の範囲内に収めるリスク対応を選定 ・残留リスクに対するポートフォリオ的視点	・残留リスクについても、内在リスクと同様の手法を用いて、定量的・定性的に評価。複数のテクニックを併用することもあり得る。 ・回避、軽減、分担、保有のそれぞれについて、販売部門等の費用増と、稼働率・目標 EBIT 増加の可能性を対比 ・地域別と全社的な内在リスク、リスク対応、残留リスクの一覧
統制活動	・リスク対応が実行されるようにする手続き、方針 ・例えば、承認、調整、営業パフォーマンスの確認、資産保全、職務の分離	・統制活動そのものがリスク対応になりうる ・例えば、支払いに関する入力は全て大元の注文の詳細と照合してから初めて次の処理に回される、支払い額を大元の支払い情報に関係するスタッフ以外の人物が確認する、等の統制活動による報告の完全性、正確性、正当性確保。
情報と伝達	・必要な情報が適宜、必要な人に伝達される ・情報テクノロジーの活用 ・情報が組織の上下・横断的に流れる ・顧客、取引先等外部との有効な情報伝達方法も必要	・機能別の各部門が情報テクノロジーを駆使して情報を捕捉・管理・報告し、それが全社的に共有される ・システムのオープン・アーキテクチャ化の進展、ウェブ技術、XBRL、XML 技術の活用、システム統合 ・情報のタイムリーさの確保（例えばダッシュボード・レポーティングとドリルダウン機能） ・ERM の重要性を訴えかける CEO のメッセージ発出、イントラネットの活用
監視活動	・ERM の構成要素が時間を経ても存在・機能することの確認 ・継続的監視活動、独立的評価	・リスクと統制に関するマニュアル、自己評価質問票やワークショップ、社内・業界等のベンチマーク比較 ・欠陥の報告対象者に関するガイドライン、経営上層部に欠陥報告すべきかどうかの判断基準策定

（出所）COSO, *Enterprise Risk Management －Integrated Framework*、同 *Application Techniques*, Sep. 2004.

２．8 つの構成要素

ERM フレームワークは、内部環境、目的の設定、事象の特定、リスク評価、リスク対応、統制活動、情報と伝達、監視活動の 8 つの構成要素から成る。これらは、「多方向（multidirectional）で相互に作用する（interactive）プロセス」であり、1 つの要素が残りの 7 つのいずれにも影響を与えうる。また、ERM フレームワークが機能するためには、8 つの構成要素の全てが揃う必要はあるものの、個々の企業による ERM の適用方法は、企業規模、業界、経営哲学等に応じて多様であり、具体的な手法は企業によって大いに異なるはずだとされている。具体的な手法については、105 ページから成る「適用テクニック編」で、上記 8 つの構成要素に沿った形で事例が紹介されている（図表 2）。

３．草案からフレームワークに至る議論

ERM フレームワークは、2003 年 7 月に公表された草案の内容を基本的に踏襲している。ただ、以下で紹介するように、草案に対するコメント・レターを受けて議論が喚起された点もあった。

１）リスクと機会

前述の通り、ERM フレームワークの草案では、リスクの定義は、企業をめぐる事象の中で、悪影響を与えるものとされており、好影響を与えるものは機会として区別された。これに対しコメントでは、リスクの定義を拡げて機会の概念も含む形にすべきだという意見が出された。機会の概念を含まないリスクということで ERM フレームワークを論ずると、機会も ERM の一部であることが伝わらず、ERM フレームワークの妥当性が損なわれるという指摘だった。一方で、逆に、機会への言及を全て削除すべきであるという意見も出された。

このような意見が出される背景として、「リスク管理のリスクには何が含まれるのか」という議論が指摘できる。例えば、自然災害等のクライシスをリスクと捉えるのか、収益の源泉たる不確実性をリスクと捉えるのかによって、管理方法の議論も自ずと変わってくる。昨今の潮流は、後者も含めた幅広いリスク概念の下で、統合的なリスク管理を目指す方向にあると言えるが、そのような中で、「悪影響はリスク、好影響は機会」という ERM フレームワークの定義が議論を喚起したとしても不思議はない。繰り返しになるが、統一概念の欠如ゆえに COSO は ERM フレームワークを提示したのであり、本フレームワークの概念が議論を呼ぶのはむしろ当然のことと言える。

結局のところ、ERM フレームワークでは、リスクの定義は草案通り機会の概念を含まない形になり、その代わりに、機会への対応も ERM の中に組み込まれていることが明確に記述された。図表 3 は ERM フレームワークで提示された事象とそのカテゴリーの具体例だが、自然災害やテロリズムが含まれる一方で、流動性や資本市場の環境、買収合併といったものも含まれている。これらの事象が、個々の企業の事情に応じて、リスクもしくは機会となりうるわけである。リスクの定義はさておいても、幅広い事象が ERM の対象となっているのは確かである。

２）有効性評価

ERM フレームワークの草案では、ERM の有効性評価は、「8 つの構成要素が存在し、有効に機能しているかどうかの評価からもたらされる主観的な判断」であるとされた。この点について、ERM の有効性評価は、プロセスの成果を測定し、その結果に基づき行われるべきだというコメントがなされた。

有効性評価については、ERM のベースである内部統制をめぐって議論されてきた点でもある。また、次章で触れるように、サーベ

図表 3　ERM フレームワークの「事象カテゴリー」の例

外部要因		内部要因	
経済	・ 立法	**インフラ**	**テクノロジー**
・ 資本の入手可能性	・ 公共政策	・ 資産の利用可能性	・ データのインテグリティ
・ 負債、債務不履行	・ 規制	・ 資産の能力	・ データ及びシステムの利用可能性
・ 集中	**社会**	・ 資本へのアクセス	・ システム選定
・ 流動性	・ 人口動態	・ 複雑さ	・ 開発
・ 資本市場	・ 消費者行動	**人員**	・ 配置
・ 失業	・ 企業市民権	・ 従業員の能力	・ メンテナンス
・ 競争	・ プライバシー	・ 詐欺的行為	
・ 買収合併	・ テロリズム	・ 健康と安全	
自然環境	**テクノロジー**	**プロセス**	
・ 排出・廃棄物	・ 障害	・ 容量	
・ エネルギー	・ E コマース	・ 設計	
・ 自然災害	・ 外部データ	・ 執行	
・ 持続的発展	・ エマージング・テクノロジー	・ 供給者・依存度	
政治			
・ 政権交代			

（出所）COSO, *Enterprise Risk Management － Integrated Framework,* Sep. 2004

ンス・オクスレー法 404 条の内部統制報告には、財務報告に係る内部統制の有効性評価も含まれることから、自ずと ERM の有効性評価に対する注目は高まっていた。

最終的に ERM フレームワークでは、プロセスたる ERM の成果を測定して評価するような方法は採用されず、「8 つの構成要素が存在し、有効に機能しているかどうかの評価からもたらされる判断」とされた。ただ、ERM フレームワークの原則に基づく客観的判断もありうるということで、草案と比較して「主観的な」という文言が削除された。

Ⅳ．サーベンス・オクスレー法 404 条対応と ERM

１．内部統制報告の義務づけ

ERM フレームワークは、サーベンス・オクスレー法 404 条の適用開始直前に公表されたこともあり、時宜を得ていると評されている[4]。

サーベンス・オクスレー法 404 条により企業は、年次報告書の中に、①企業経営者が、財務報告に係る適切な内部統制の仕組みと手続きを維持する責任を負うことを記述し、②財務報告に係る内部統制の有効性に関する定期的な評価を含まなければならないとされた。また、②の内部統制の有効性評価について、外部監査人による確認書（アテステーション・レポート）の受領と当該確認書の年次報告書への掲載が義務づけられることとなった。いわゆる内部統制報告の義務づけである[5]。

内部統制報告の義務づけは、米国大企業（時価総額 7500 万ドル以上）については 2004 年 11 月 15 日以降終了の事業年度から、それ以外については 2005 年 7 月 15 日以降終了の事業年度から適用される[6]。適用第一陣の企業の中には、自社の内部統制に重大な弱点がありうることを早々に発表するものも出てきており、内部統制報告の株価、格付け、貸付条件などへの影響が注視されているところである[7]。

ERM フレームワークでは、サーベンス・オクスレー法により、公開企業に対し内部統制システムの維持の義務づけ、経営陣による宣誓と外部監査人によるアテステーションが導入されたこと、COSO の内部統制フレームワークは同法の基準を満たすものであること

が指摘された[8]。その上で、企業はERMフレームワークの活用により、内部統制のニーズを満たすと同時に、より広範なリスク管理に着手することができるとされた。

また、サーベンス・オクスレー法404条により、外部監査人は財務報告に係る内部統制報告のアテステーションを求められることとなったが、ERMについては通常、外部監査人が財務報告書の監査に際して意見表明を行うことはない点が確認された。

２．ERMへの展開の可能性

サーベンス・オクスレー法404条は、財務報告に係る内部統制に関する規定なので、財務報告の信頼性に加えて、事業の有効性と効率性及び法令遵守をも対象とするCOSOの内部統制よりも適用範囲が狭い。しかし、経営者に対する内部統制報告の義務づけが70年代にすでに提案されたものの、産業界からの反対で実現せずに来たことなどを考えあわせると、画期的な制度改正と言える。また、404条対応のコストも相当な金額に上ると見られており、当初の対応だけで1社当たり平均510万ドルという試算も出されている[9]。

企業にとって負担感が拭い去れない中で、404条対応の過程で、実は、企業は本格的なERMの導入に必要な改革の多くに着手しており、次なるステップは、404条対応のための投資を活かして本格的なERMを実施することだという指摘も出始めている。「サーベンス・オクスレー法の義務づけは、実はCOSOのERMの部分集合」であり、ERMの実施には通常2～3年はかかると言われるが、「サーベンス・オクスレー法対応ゆえに多くの作業がすでに済んでおり、今やERM実施のための時間が大幅に短縮されている」というわけである[10]。

COSOのERMフレームワークは、企業が採用を強制されるものではない。したがって、同フレームワークが現実のERMに関するニーズをいかにくみ取っているかが、最終的には普及の決め手になる。他方、内部統制がそうであったように、COSOのERMフレームワークがグローバル・スタンダードとなる可能性もあり、投資家がERMを基準に企業行動の規律付けが十分かどうかを判断するようになることも考えられる。

わが国でも、2002年改正監査基準により会計監査についてはCOSOの内部統制フレームワークが全面的に導入され、また、同年の商法改正により、委員会等設置会社については、取締役会に対して内部統制の整備を求める規定が導入された。さらに、経済産業省から、2003年にリスク管理と内部統制に関する報告書が出されるなど、様々な動きがある[11]。COSOのERMフレームワークが公表された今、わが国企業も同フレームワークへの意識を高めることが求められよう。

---

[1] The Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management －Integrated Framework: Executive Summary, Framework*, Sep. 2004及び同 *Application Techniques*, Sep. 2004.

[2] ERMフレームワークの草案については、野村亜紀子「内部統制から事業リスク管理へ―トレッドウェイ委員会組織委員会（COSO）の報告書案―」『資本市場クォータリー』2003年秋号で紹介した。本章では、重複する部分も含めてフレームワークの全体像を示すこととする。

[3] ERMフレームワークは、このように、企業に限らず多様なタイプの組織を想定しているが、本稿では、企業への適用を前提に記述する。

[4] もっとも、ERMフレームワーク作成は2001年に開始されており、エンロン、ワールドコム等のサーベンス・オクスレー法制定の契機となった不正会計事件への対応というわけではなかった。

[5] わが国でも、2004年10月以降の大手企業による有価証券報告書等への虚偽記載問題を契機に、ディスクロージャー制度への信頼性確保に向けた対策の検討が進められ、2004年12月24日、金融審議会第一部会より報告書が出された。同報告書には、①財務報告に係る内部統制の有効性に関する経営者による評価と公認会計士等による検証の基準の明確化を早急に図るべきである、②会社代表による確認書制度の活用促進とともに、同制度の義務化の範囲や方法等が適切に判断されるべきである、という提言が盛り込まれた。

[6] ただし、証券取引委員会（SEC）は 2004 年 11 月 30 日、事業年度末が 2004 年 11 月 15 日から 2005 年 2 月 28 日の間にある、時価総額 7 億ドル未満の企業については、内部統制報告提出の 45 日間の期限延長を認めた。期限遵守の見通しの立たない企業が多いという認識から、そうすることが公益に資するという判断だった。（SEC, Release No. 34-50754, "Order under Section 36 of the Securities Exchange Act of 1934 Granting an Exemption from Specified Provisions of Exchange Act Rules 13a-1 and 15d-1, " Nov. 30, 2004).

[7] "The 404 Maelstrom," *Investment Dealers' Digest*, Dec. 13, 2004.

[8] SEC がサーベンス・オクスレー法 404 条関連の規則を採択したリリースの中でも、COSO の内部統制フレームワークが例として挙げられている。SEC, Release No. 33-8238, "Final Rule: Management's Report on Internal Control over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports," June 5, 2003.

[9] "Average US group faces $ 5 million compliance bill Sarbanes-Oxley," *Financial Times*, Nov. 12, 2004. なお、Financial Executives International が 8 月に行ったサーベイでは、1 社当たり平均 314 万ドルという結果だった。

[10] George Matyjewicz and James R. D'Arcangelo, "Beyond Sarbanes-Oxley," *Internal Auditor*, Vol. 61, Issue 5 (Oct. 2004).

[11] わが国での動向については、前掲脚注 2 を参照のこと。