

全社的リスクマネジメント（ERM）の新展開

橋 本 尚

【キーワード】 ガバナンス、カルチャー、環境・社会・ガバナンス（ESG）関連リスク、全社的リスクマネジメント（ERM）、トレッドウェイ委員会支援組織委員会（COSO）

I はじめに

トレッドウェイ委員会支援組織委員会（Committee of Sponsoring Organizations of the Treadway Commission：COSO）は、2017年9月（報告書の日付は同年6月）、『全社的リスクマネジメント—戦略およびパフォーマンスとの統合』（Enterprise Risk Management—Integrating with Strategy and Performance）（2017年版ERMフレームワーク）¹⁾を公表した。これは、2004年9月に初めて公表された『全社的リスクマネジメント—統合的フレームワーク』（Enterprise Risk Management—Integrated Framework）」（当初版ERMフレームワーク）²⁾を13年ぶりに改訂したものである。

当初版ERMフレームワークは、世界中に普及し、経営者や取締役会が、不確実性を管理する組織の能力を向上し、また、ステークホルダーの価値向上を追求する中で、どの程度のリスクを受け入れるべきかを検討する際に役立ってきた。しかしながら、当初版ERMフレームワーク公表以降の十数年で、2008年秋のリーマンショックに象徴されるように、リスクは一層複雑化し、深刻なリスクも新たに生じてきた。全社的リスクマネジメント（ERM）を導入してもリーマンショックを防げなかったことから、結果的に機能しなかったERMに経営者は見向きもしなくなってしまうという。とりわけ、最も強力に成熟したリスクマネジメント能力があると広く認識されていたにもかかわらず、世界的な金融危機によって金融業界が深刻な影響を受けたことは、ERM関係者にとって大きな衝撃となった。また、当初版ERMフレームワーク公表当時は、2002年サーベインズ・オックスリー（SOX）法への対応が最重要課題とされていたこともあり、ERM導入に際してギャップや適用レベルのばらつきが見られたことから、今般の改訂にあたっては、ERMが経営にどのように役立つのかを経営者にわかりやすく示すことが課題の1つとされ、企業を取り巻く状況が激変する中で、

戦略や事業目標の達成に役立つような新たな ERM フレームワークのニーズに対応し、ERM の最新かつ進化している概念と適用方法を反映すべく、報告書名にもあるように、戦略策定プロセスにおいても、パフォーマンス促進においても、リスクを検討することの重要性が強調されている。特に、戦略の策定と実行における戦略および ERM の役割により深い知見を提供し、組織のパフォーマンスと ERM の一体性を高めるとともに、ガバナンスと監督への期待にも応えるものとなっており、組織は、世界的規模で、ERM からさらなる価値を獲得することができるようになるであろう。

本稿においては、2017 年版 ERM フレームワークを起点とする ERM の新展開を概観していく。

Ⅱ 2017 年版 ERM フレームワークの概要

2017 年版 ERM フレームワークでは、ERM を「組織が価値を創造し、維持し、および実現する過程において、リスクを管理するために依拠する、戦略策定ならびにパフォーマンスと統合されたカルチャー、能力、実務」と定義している³⁾。この ERM の新しい定義では、次のようなことに焦点を当てながらリスク管理を行うことが強調されている。

- ①カルチャーを認識すること
- ②能力を開発すること
- ③実務に適用すること
- ④戦略策定およびパフォーマンスと統合すること
- ⑤戦略と事業目標に係るリスクを管理すること
- ⑥価値とリンクしていること

2017 年版 ERM フレームワークは、戦略および組織のパフォーマンスと ERM との統合的、一体的な関係を重視している。また、内部統制は、ERM の基盤として位置づけられており、2013 年 5 月に改訂された内部統制フレームワーク（2013 年版内部統制フレームワーク）⁴⁾ と 2017 年版 ERM フレームワークとの間に優劣はなく、互いを補完するものである。さらに、ERM の概念と原則は、内部統制と同様、営利、非営利などの法的な構造、規模の大小、業種または地域に関係なく、すべての組織に適用されることが意図されている。

2017 年版 ERM フレームワークでは、ミッション、ビジョンおよびコアバリューと戦略との関係、組織の全体的な方向性、ならびにパフォーマンスの原動力としての戦略の位置づけが図表 1 のように示されている⁵⁾。

図表 1 戦略の位置づけ



当初版 ERM フレームワークでは、4つの目的と8つの構成要素の関係が「COSO キューブ（立方体）」によって表されていたが、2017年版 ERM フレームワークでは、ERM の5つの構成要素と20の原則が提示されている。フレームワークを構成要素と原則を用いて説明する原則主義的な考え方は、2013年版内部統制フレームワークの3つの目的、5つの構成要素および17の原則と平仄をあわせたものである。これに対して「COSO キューブ」は、内部統制に関しては、1992年9月の『内部統制の統合的フレームワーク』（Internal Control Integrated Framework）（当初版内部統制フレームワーク）と同様に、2013年版内部統制フレームワークでも引き続き使用されているが、2017年版 ERM フレームワークでは、リスク、戦略およびパフォーマンスとの結びつきをより良く説明するために、「COSO キューブ」は踏襲されず、「COSO リボン」と称される新たな図表が導入されている（図表2参照）⁶⁾。「COSO リボン」は、DNAの二重らせん構造から着想を得たものであるが、DNAが生物と一体のものであるように、ERMが組織に統合（一体化）されていることをわかりやすく図示したものといえよう。

図表 2 ERM の構成要素
全社リスクマネジメント



図表2は、ERMの構成要素ならびに各構成要素と組織のミッション、ビジョン、およびコアバリュー⁷⁾との関係を説明したものであるが、戦略と目標設定、パフォーマンス、およびレビューと修正の構成要素を示す3つのリボンは、組織の中にある共通のプロセスを表している。ガバナンスとカルチャー、ならびに情報、伝達および報告の構成要素を示す他の2つのリボンは、ERMの支援的な側面を表している。また、図表2は、ERMが戦略の策定、事業目標の体系化、実践とパフォーマンスを貫いて統合される際に、価値の向上が実現できることも示している。ERMは静的なものではなく、日々の意思決定を通して、戦略策定、事業目標の体系化およびそれらの目標の実現に統合されていくものである。

2017年版ERMフレームワークの5つの構成要素は、以下の通りである。

- ①ガバナンスとカルチャー：ガバナンスとカルチャー⁸⁾はともに、ERMの他のすべての構成要素の基礎となる。ガバナンスは、ERMの重要性を強調し、それに対する監督責任を確立する事業体の気風を醸成する。カルチャーは、意思決定に反映される。
- ②戦略と目標設定：ERMは、戦略と事業目標の策定プロセスを通じて、事業体の戦略計画に統合される。事業環境を理解することにより、組織は、内外の要因とそれらがリスクに及ぼす影響についての知見を得ることができる。組織は、戦略策定と合わせてリスク選好を設定する。事業目標は、戦略の実行を可能にし、事業体の日常活動とその優先順位を形づくる。
- ③パフォーマンス：組織は、戦略と事業目標を達成する事業体の能力に影響を及ぼすかもしれないリスクを識別し、評価する。そのために、組織は戦略と事業目標の達成に影響するかもしれないリスクを識別し、評価する。組織は、リスクの重大度に応じて、また事業体のリスク選好を考慮して、リスクを優先順位づけする。そして、組織は、リスクへの対応を選択し、パフォーマンスの変化の動向を監視する。このように、組織は、戦略と全社レベルの事業目標を追求する中で受け入れたリスク量に対するポートフォリオの視点を構築する。
- ④レビューと修正：ERMの能力と実務、およびその目標に対する事業体のパフォーマンスをレビューすることにより、組織は、ERMの能力と実務が、どの程度まで長期的に価値を向上させてきたのか、さらに、大きな変化に直面した場合でも価値を向上させ続けられるかを検討できる。
- ⑤情報、伝達および報告：伝達は、事業体全体を通して情報を収集し、共有する継続的で反復的なプロセスである。経営者は、ERMを支援するために、内外の情報源から関連性のある情報を利用する。組織は、データと情報を入手し、処理し、管理するために、情報システムを活用する。すべての構成要素に関連する情報を利用して、組織は、リスク、カルチャーおよびパフォーマンスについての報告を行う。

2017年版ERMフレームワークでは、上記の相互に関連する5つの構成要素別に、これらの構成要素を支える以下の20の原則が体系的に提示されている。各原則は、各構成要素に関連する基本的な概念を示したものであり、それらの適用において普遍的なものであり、ERMの一部を形成するものである。

構成要素1 ガバナンスとカルチャー

- 原則1. 取締役会によるリスク監視を行う—取締役会は、戦略を監視し、ガバナンスの責任を果たすことにより、経営者が戦略と事業目標を達成できるよう支援する。
- 原則2. 業務構造を確立する—組織は、戦略と事業目標を達成するために、業務構造を確立する。
- 原則3. 望ましいカルチャーを定義づける—組織は、事業体の望ましいカルチャーを特徴づける望ましい行動を定義づける。
- 原則4. コアバリューに対するコミットメントを表明する—組織は、事業体のコアバリューに対するコミットメントを表明する。
- 原則5. 有能な人材を惹きつけ、育成し、保持する—組織は、戦略と事業目標にふさわしい人的資本の形成にコミットメントする。

構成要素2 戦略と目標設定

- 原則6. 事業環境を分析する—組織は、リスクプロファイルに対する事業環境の潜在的影響を検討する。
- 原則7. リスク選好を定義する—組織は、価値の創造、維持、実現の観点からリスク選好を定義する。
- 原則8. 代替戦略を評価する—組織は、代替戦略とリスクプロファイルに対する潜在的影響を評価する。
- 原則9. 事業目標を組み立てる—組織は、戦略と結びつき、かつ、戦略を支える事業目標をさまざまな階層において設定する際にリスクを検討する。

構成要素3 パフォーマンス

- 原則10. リスクを識別する—組織は、戦略および事業目標のパフォーマンスに影響を及ぼすリスクを識別する。
- 原則11. リスクの重大度を評価する—組織は、リスクの重大度を評価する。
- 原則12. リスクの優先順位づけをする—組織は、リスク対応選択の基礎として、リスクの優先順位づけを行う。
- 原則13. リスク対応を実施する—組織は、リスク対応を識別し、選択する。
- 原則14. ポートフォリオの視点を策定する—組織は、リスクのポートフォリオの視点を策定し、評価する。

構成要素4 レビューと修正

原則 15. 重大な変化を評価する一組織は、戦略や事業目標に重大な影響を与え得る変化を認識し、評価する。

原則 16. リスクとパフォーマンスをレビューする一組織は、事業体のパフォーマンスの結果をレビューし、リスクを考慮する。

原則 17. ERM の改善を追求する一組織は、ERM の改善を追求する。

構成要素5 情報、伝達および報告

原則 18. 情報とテクノロジーを有効活用する一組織は、ERM をサポートするために、事業体の情報とテクノロジーシステムを有効活用する。

原則 19. リスク情報を伝達する一組織は、ERM をサポートするために、コミュニケーション経路を利用する。

原則 20. リスク、カルチャーおよびパフォーマンスについて報告する一組織は、リスク、カルチャーおよびパフォーマンスを複数の階層に、また、全社にわたって報告する。

内部統制は、ERM の基盤として位置づけられており、上記原則 10 から 14、とりわけ、原則 13 によって両者は関連づけられている。2013 年版内部統制フレームワークと 2017 年版 ERM フレームワークは、相互補完関係にあるので、両フレームワークに共通の構成要素（例えば、統制活動）については、ERM フレームワークでは言及されていない。他方、ERM のガバナンスなどのいくつかの概念については、敷衍、発展させている。

2017 年版 ERM フレームワークの当初版 ERM フレームワークからの主要な変更点は、以下の 10 項目である。

- ①構成要素と原則の構造の採用
- ②ERM の定義の簡素化
- ③リスクと価値の関係の強調
- ④新たに ERM の統合にフォーカス
- ⑤カルチャーの役割を考察
- ⑥戦略の議論を高める
- ⑦パフォーマンスと ERM の連携の強化
- ⑧意思決定への ERM の明確な関連づけ
- ⑨ERM と内部統制との線引き
- ⑩リスク選好と許容度の精緻化

ERM は、もともと保険論やファイナンス論の領域の用語であることから、マイナスの影響を与える事象をリスクとして捉えてきた。当初版 ERM フレームワークでも、リスクをネガティブ・リスクに限定し、目標達成にプラスの影響を及ぼす事象が生じる可能性である「事業

機会」を視野に入れつつも、用語上はリスクと明確に区別されてきた。しかしながら、ERMの特徴を最大限に発揮するためには、プラスとマイナスの双方のリスクを視野に入れる必要があることはいうまでもない。2017年版ERMフレームワークでは、ERMの定義の最新化・簡素化と同様に、リスクについても「事業が発生し、戦略と事業目標の達成に影響を及ぼす可能性」という新たな定義⁹⁾を示すとともに、新しいリスク、エマージングリスク、変化するリスクという3つのリスクを識別するためのアプローチが提示されている¹⁰⁾。このように2017年版ERMフレームワークでは、リスク選好の範囲内でリスクを受け入れて価値の向上を実現するという観点から許容されるリスクとパフォーマンスの向上との最適なバランスを図る価値向上のための意思決定に資する情報を経営者に提供する機能が重視されている。

プラスとマイナスの双方のリスクを視野に入れたことで、リスク対応についても従来の回避、低減、共有（移転）、受容に加えて、活用（さらに高いパフォーマンスを達成するために、より多くのリスクを許容する対策を講じること）というERM固有の対応策を講じる道が開かれた。また、リスクの重大度は、発生可能性と影響度で評価されるが、2017年版ERMフレームワークでは、これに加えて適応性、複雑性、速度、持続性、回復度をリスクの優先順位づけの規準として位置づけている。さらに、リスクをポートフォリオの視点によって評価することと、リスクが及ぼす影響範囲に着目しつつ事業体全体や各階層といった異なる階層におけるリスクおよびその重大度を評価することを重視している。

リスクを識別する際には、リスク自体を正確に記述することが何よりも重要である。これに関連して、リスク評価におけるバイアスについても、人間の意思決定を解明するプロスペクト理論¹¹⁾について言及する中で、フレーミングリスク（フレーミング（心的構成）のバイアスによりリスクが正確に記述されないリスク）を念頭に置くべきであるとしている¹²⁾。

2017年版ERMフレームワークでは、リスク選好と許容度の概念も精緻化されている。リスク選好については「組織が価値追求において受け入れる、幅広いリスクの種類と量」という定義を堅持する一方、許容度は、リスク選好のより厳密あるいは詳細な形の表現ではなく、パフォーマンスという用語を使って「事業目標達成にあたり、パフォーマンスの受入れ可能な変動範囲」と定義されている。リスクプロファイルにおいて、この関係性は、リスク選好とパフォーマンス線の垂直な交差で表される。

こうして許容度の定義を精緻化することによって、所与のパフォーマンスのために許容できるリスク量に焦点が当てられ、組織は、パフォーマンスの要素の中で許容可能なリスクの領域を明確に示すことができるようになる。リスクもパフォーマンスも、変化しない、別々のものと認識されるのではなく、むしろ絶えず変化して互いに影響を及ぼすものと認識され、これらの領域の決定によって、組織は、パフォーマンスレベルの変化が、許容可能な変動幅の範囲に収まっているかどうかをより良く評価することが可能となる。なお、2017年版ERMフレームワークの付録Dには、リスクプロファイルの作成方法と、組織がERMフレ

ームワークの諸原則を適用する際のリスクプロファイルのさまざまな活用方法が図示されている。このように2017年版ERMフレームワークは、リスクプロファイルを活用することにより、リスクとパフォーマンスの最適なバランス（組合せ）を可視化し、関係者が議論する際の共通のツールを提供することで、意思決定プロセスの改善に資するものとなっている。

情報とテクノロジーについてもERMの一環として、データのより大きな役割と進化するテクノロジーを重視し、データの有効かつ効率的な管理・分析方法や最新のテクノロジーの活用方法が詳細に検討されている。そこでは、人工知能（AI）、データマイニング、機械学習などのコグニティブ・コンピューティングの進化やビッグデータの管理・分析について言及しつつ、利便性と脆弱性を合わせ持つテクノロジーは、時として、組織に新しいリスクをもたらしかねず、戦略と事業目標の達成に致命的な影響を与えかねない点にも留意するように求めている¹³⁾。

このように2017年版ERMフレームワークでは、フレームワークを全体像の中で捉えて本質を実感すべく、長期的、持続的な企業価値の向上にERMをどのように活用するかという観点から、ERMを巡る最新の議論が展開されている。従来、ERMの中での統合、リスクモデルの中でのPDCAとして捉えてきたERMを、事業モデルのPDCAの中で捉え、戦略およびパフォーマンスとの統合（一体化）を視野に捉えていく、DNAのように組織に一体化されたものとして、ビジネスそのものとしてERMを捉えていこうとするとともに最大の特徴があるといえよう。わかりやすいERMの定義が示されたことで、リスク管理部門、内部監査部門といった隔離された中での閉鎖的な、限られた範囲内での議論から、経営企画部、経営会議なども巻き込んだ形で組織内のコミュニケーションが促進するような、経営に役立つ、経営者にも伝わるような方法で戦略およびパフォーマンスと一体となった（内部統制とは線引きされた）ERMのあるべき姿や目指すべき方向性が明確かつ体系的に示されている。これにより、サイロ型と批判されてきた分散的な各種リスクマネジメントを事業体全体で統合し、各部門・各階層がそれぞれの役割を果たしつつ、連携しながらリスクを横断的・総合的に識別・評価して情報を共有する、いわゆるリスク情報の統合が促進されよう。

2017年版ERMフレームワークでは、カルチャーをERMの重要な柱と捉えている。不祥事が起きると企業体質が問われるなど、カルチャーのマイナスの側面が強調されることが多いが、長期的、持続的な企業価値の向上の観点からは、わが国に長寿企業が多いということは、「三方よし」や「処事光明」といったわが国に古くからある企業経営の形、わが国企業のカルチャーの特質から学ぶべきことが多いことを示唆するものでもある。近年の環境・社会・ガバナンス（ESG）への配慮や持続可能な開発目標（SDGs）の推進に照らして、エクセレント・カンパニーとしてのあるべき姿を目指してわが国企業に求められることは、企業市民としてステークホルダーのカルチャーとの整合性を図りながら、ERMを通じて、事業目標の達成に向けてとるべきリスク、とってはならないリスクを戦略的に識別することである。

各組織の価値の創造、維持、さらにその実現に向けた有効かつ効率的な ERM の実践が大いに期待されるところである。その際には、組織内部の変化（経営者の交替など）と外部からの影響（M&A など）により、組織のカルチャーに変化が生じ得ることにも留意する必要がある。

Ⅲ 『事例の解説篇』の公表と ERM の環境・社会・ガバナンス（ESG）関連リスクへの適用

COSO は、2018 年 6 月（報告書の日付は同年 1 月）、2017 年版 ERM フレームワークを補完する『事例の解説篇』（Enterprise Risk Management — Integrating with Strategy and Performance : Compendium of Examples）¹⁴⁾ を公表した。2017 年版 ERM フレームワークの構成要素に係るすべての原則の適用方法が具体的に示された各事例では、さまざまな種類、規模、業界、および地域の事業体に関連する特定の原則が取り上げられている（図表 3 参照）¹⁵⁾。

図表 3 『事例の解説篇』の事例で示された原則

◆主に説明されている原則

★関連して副次的に説明されている原則

	業 界								
	2 章	3 章	4 章	5 章	6 章	7 章	8 章	9 章	10 章
	高等教育	政府	金融	エネルギー	非営利	消費財	テクノロジー	工業製品	医療
	国際規模	全国規模	地方規模	全国規模	国際規模	地方規模	全国規模	国際規模	全国規模
	ガバナンス	カルチャー	カルチャー	戦略と目標 設定	戦略と目標 設定	パフォーマンス	パフォーマンス	レビューと 修正	リスク情報
原則									
1	◆								
2	◆								
3		◆	◆						
4		◆	◆						
5		◆	◆						
6			★	◆	◆				
7				◆	◆			★	
8	★			◆	◆		★		
9				◆	◆				
10						◆	◆		
11						◆	◆		
12						◆	◆		
13						◆	◆		
14	★					◆	◆	◆	
15								◆	
16								◆	
17								◆	
18									◆
19									◆
20	★	★				★	★		◆

各事例はそれぞれに独立した事例となっている。これらは、ハウツーを提供したり、ベストプラクティスを示すことを意図したものではないが、9つの事例全体として、2017年版ERMフレームワークで提示された5つの構成要素と20の原則のすべてをカバーするものとなっている。

各事例では特定の業界に焦点が当てられているが、他の業界関係者も、そこに示された内容から多くの知見を得ることができるであろう。同様に、さまざまな事業体が原則を調整して適合させた方法が述べられた各事例には、他の事業体が参考とすべき内容も豊富に示されているものと思われる。

各事例では、同一の形式で以下の内容が示されている。

- ①例示した事業体が活動する業界の（外部環境と内部環境の両方の）状況
- ②例示した事業体の背景情報
- ③適用可能な原則
- ④組織がそれらの原則を適用している方法
- ⑤全社的リスクマネジメントが事業に組み込まれている仕方
- ⑥全社的リスクマネジメント実務の主なメリット

また、2018年10月、COSOは、持続可能な開発のための世界経済人会議（World Business Council for Sustainable Development：WBCSD）と共同で『全社的リスクマネジメント—全社的リスクマネジメントの環境・社会・ガバナンス関連リスクへの適用』（Enterprise Risk Management — Applying enterprise risk management to environmental, social and governance-related risks）¹⁶⁾を公表した。本ガイダンスは、リスクマネジメントとサステナビリティの担当者が、ERMの概念とプロセスを、環境・社会・ガバナンス（ESG）関連リスク¹⁷⁾に適用できるようにすることを目的としたものであり、事業体が以下のことを達成する上で役立つものである¹⁸⁾。

- ①レジリエンスの強化：事業体の中長期的な存続とレジリエンスは、戦略と目標を脅かす複雑で相互に関連する一連のリスクを予測し、それに対応する能力にかかっている。
- ②ESG関連リスクを明確にするための共通語：ERMは、戦略および事業目標への潜在的な影響に対するリスクを識別し、評価する。このようにESG関連リスクを明確にすることで、ESGの問題を主流のプロセスや評価で取り上げることができる。
- ③資源配置の改善：ESG関連リスクに関する確実な情報を入手することで、経営者は、資源のニーズを総合的に評価し、資源配分を最適化することができる。
- ④ESG関連機会の追求の強化：ESG関連リスクのプラス面とマイナス面の両方を考慮することで、経営者は新たな機会につながるESGの傾向を識別することができる。
- ⑤規模の効率化の実現：ESG関連のリスクを一元的に管理し、他の事業体レベルのリスクと並行して管理することで、冗長性を排除し、事業体のトップリスクに対処するための

資源をより適切に割り当てることができる。

- ⑥開示の改善：ESG 関連リスクに対する経営者の理解を向上させることにより、投資家が期待する水準の透明性と開示を実現し、規制上の報告要件の遵守を達成することができる。

本ガイダンスは、COSO の 2017 年版 ERM フレームワークの 5 つの構成要素を反映した 5 つの章から構成されている。すなわち、ガバナンスとカルチャー、戦略と目標設定から始まり、次にパフォーマンスに重点を置いた ERM プロセス（ESG 関連リスクの識別、評価、優先順位づけ、および対応）へと進み、そして最後に、レビューと修正、ならびに ESG 関連リスクに関する情報、伝達および報告について、概略以下のように述べられている¹⁹⁾。

1. ESG 関連リスクに関するガバナンスとカルチャー：ガバナンスまたは内部監視により、決定が行われる方法およびこれらの決定がどのように実行されるかが決まる。ESG 関連リスクへの ERM の適用には、取締役会および上級経営者の ESG 関連リスクに対する意識を高めることが含まれる。これは、ESG 問題のリスクマネジメントに責任を負う人々が連携するカルチャーを醸成する。
2. ESG 関連リスクに関する戦略と目標設定：すべての事業体は自然と社会に影響を及ぼすとともに、依存している。したがって、事業環境、戦略、および目標を深く理解することは、すべての ERM 活動、およびリスクの効果的な管理における拠り所として役立つ。ESG 関連リスクへの ERM の適用には、短期、中期、長期的にこれらリスクの影響と依存関係を理解するための価値創造プロセスの検討が含まれる。
3. ESG 関連リスクに関するパフォーマンス：
 - a) リスクを識別する：組織は ESG 関連リスクを識別するために複数のアプローチを使用する。すなわち、ESG 関連リスクについてのメガトレンド分析、SWOT 分析、影響と依存関係のマッピング、ステークホルダー・エンゲージメントおよび ESG の重要性評価である。これらのツールは、リスクが事業体の戦略や事業目標の達成をどのように脅かしているかという観点から、ESG の問題を識別し表現するのに役立つ。リスクマネジメント担当者とサステナビリティ担当者との連携によるこれらのアプローチの適用は、ESG 関連リスクをリスク一覧表に掲載させ、それらのリスクへの適切な評価と対応を可能にする。
 - b) リスクを評価し、優先順位づけする：企業が有する資源は限られているため、企業全体で識別されたすべてのリスクに等しく対応することはできない。そのため、優先順位づけのためにリスクを評価する必要がある。ESG 関連リスクへの ERM の適用には、用語の定義を含むリスク重大度の評価が含まれ、評価結果はリスクの優先順位づけに使用できる。ESG に関する専門知識を活用することは、ESG 関連の新たなリスクや長期的なリスクが無視されたり過小評価されたりせずに、適切に評価および優先順位づ

けされることを保証するために重要である。

- c) リスク対応を実施する：事業体が識別されたリスクにどのように対応するかによって最終的に、事業体が長期にわたって価値をどの程度効果的に維持または創造するかが決定される。各アプローチの費用と便益だけでなく、リスクの原因を考慮した革新的で協調的な一連のアプローチを採用することは、これらの対応を成功に導く。
4. ESG 関連リスクに関するレビューと修正：ERM 活動のレビューと修正は、その有効性を評価し、必要に応じてアプローチを修正するために重要である。組織は、リスクの識別、評価、および対応に反映させる必要がある変更事項について警告を発する具体的な指標を作成できる。この情報は、社内外のさまざまなステークホルダーに報告される。
5. ESG 関連リスクに関する情報、伝達および報告：ESG 関連リスクへの ERM の適用には、リスク情報に基づいた意思決定を支援するために、内部および外部に伝達および報告される最も適切な情報を識別するためのリスクオーナーとの協議が含まれる。

IV むすび

2018 年 2 月から COSO の新会長に就任したソーベル氏（Paul J. Sobel）は、2017 年版 ERM フレームワークの内部監査人向けの解説書²⁰⁾を公表している。また、ERM に関しては、2019 年 1 月、国際会計士連盟（International Federation of Accountants：IFAC）から『有効な ERM において会計士の果たすべき役割』（Enabling the Accountant's Role in Effective Enterprise Risk Management）²¹⁾という文書も公表されている。

各組織の価値の創造、維持、さらにその実現に向けた有効かつ効率的な ERM の実践を通じて、健全かつ強靱な組織が構築・維持されることを願うものである。

注

- 1) COSO, *Enterprise Risk Management — Integrating with Strategy and Performance*, June 2017. (一般社団法人日本内部監査協会・八田進二・橋本 尚・堀江正之・神林比洋雄監訳、日本内部統制研究学会 COSO-ERM 研究会訳『COSO 全社的なリスクマネジメント—戦略およびパフォーマンスとの統合』同文館出版、2018 年 4 月。)
- 2) COSO, *Enterprise Risk Management — Integrated Framework*, September 2004. (八田進二監訳 中央青山監査法人訳『全社的なリスクマネジメント フレームワーク篇』東洋経済新報社、2006 年 3 月。)
- 3) 原書 p.10、訳書 51 頁。当初版 ERM フレームワークで示された ERM の定義は、リスク管理担当者にとっては比較的容易に理解できるものであったが、それ以外の者にとってはわかりにくいものであったので、わかりやすく、かつ、読みやすくなるように見直された。また、フレッシュ・キンケイド式読みやすさ判定ツールを活用して、報告書全般にわたって読みやすくなるように改善されている。
- 4) COSO, *Internal Control — Integrated Framework, Executive Summary, Framework and Appendices, Illustrative*

Tools for Assessing Effectiveness of a System of Internal Control, Internal Control over External Financial Reporting (ICEFR): A Compendium of Approaches and Examples, May 2013. (八田進二・箱田順哉監訳 日本内部統制研究学会新 COSO 研究会訳『内部統制の統合的フレームワーク フレームワーク篇／ツール篇／外部財務報告篇』日本公認会計士協会出版局、2014 年 2 月。)

- 5) 原書 p.13、訳書 58 頁。
- 6) 原書 p.21、訳書 71-72 頁。
- 7) ミッションとビジョンは、戦略と事業目標の策定と実践との関係で、コアバリューは、事業体が尊重したいと願うカルチャーとの関係で検討されている。
- 8) カルチャーは「経営者や職員の判断に影響を与え、組織のミッション、ビジョンおよびコアバリューを反映した、ポジティブおよびネガティブ両面のリスクに対する姿勢、行動およびリスクの理解」と定義されている。また、組織のカルチャーのスペクトル（位置づけ）は、リスクテイクに対する慎重な姿勢から中立的な姿勢を挟んで積極的な姿勢までの間のどこに位置しているかという形で示されている。
- 9) 原書 p.9、訳書 49 頁。
- 10) 原書 p.67、訳書 149 頁。
- 11) 人間は利益を得る局面では、確実に手に入れることを優先し、反対に、損失を被る局面では、最大限に回避することを優先する傾向があるという行動心理に関する理論。
- 12) 原書 p.71、訳書 158 頁。
- 13) 原書 pp.99-101、訳書 211-217 頁。
- 14) COSO, *Enterprise Risk Management — Integrating with Strategy and Performance: Compendium of Examples*, January 2018. (八田進二・橋本 尚・堺 咲子訳『COSO 全社リスクマネジメント—戦略およびパフォーマンスとの統合：事例の解説篇』一般社団法人日本内部監査協会、2018 年 12 月。)
- 15) 図表 3 は、原書 p.3、訳書 5 頁の表 1.1 を補筆したものである。
- 16) COSO and WBCSD, *Enterprise Risk Management — Applying enterprise risk management to environmental, social and governance-related risks*, October 2018. (<https://www.coso.org/Documents/COSO-WBCSD-ESGERM-Guidance-Full.pdf>, visited at January 23, 2019.)
- 17) ESG 関連リスクとは、事業体に影響を及ぼし得る環境、社会、およびガバナンスに関連するリスクおよび／または機会であり、サステナビリティ、非財務リスク、または財務以外のリスクとも呼ばれる。
- 18) COSO and WBCSD (2018), p.7.
- 19) COSO and WBCSD (2018), pp.8-9.
- 20) Paul J. Sobel, *Managing Risk in Uncertain Times — Leveraging COSO's New ERM Framework*, IAF, February 2018. (ポール・J・ソーベル著、八田進二監訳、堺 咲子訳『不確実な時代のリスクマネジメント—COSO 新 ERM フレームワークの活用』一般社団法人日本内部監査協会、2018 年 8 月。)
- 21) IFAC, *Enabling the Accountant's Role in Effective Enterprise Risk Management*, (<https://www.ifac.org/system/files/publications/files/Enabling-The-Accountants-Role-In-Effective-ERM.pdf>, Visited at January 23, 2019.)

(はしもと たかし・青山学院大学大学院会計プロフェッション研究科教授)