日本価値創造 ERM 学会誌

JAVCERM JOURNAL

2018 年度 第 3 回 セミナー報告

改訂版 COSO-ERM の我が国企業での活用の方向性

～社外取締役の視点から

第 1 部：基調講演

第 2 部：パネルディスカッション

開催日：2018 年 11 月 15 日

会場：日本工業大学（神田キャンパス）

第 1 部：基調講演

「改訂版 COSO-ERM の概要 ～我が国企業での活用の視点も含めて」

青山学院大学 大学院会計プロフェッション研究科教授　　橋本　尚（たかし）

第 2 部：パネルディスカッション

「社外取締役の視点から見た改訂版 COSO-ERM の我が国企業での活用の方向性」

〈パネリスト〉

青山学院大学　大学院会計プロフェッション研究科教授　　橋本　尚（たかし）

アジア開発銀行研究所　エコノミスト　　根本直子
（中部電力株式会社　社外取締役）
（株式会社コンコルディア・フィナンシャルグループ　社外取締役）

鈴木総合法律事務所　弁護士　　鈴木洋子
（株式会社ブリヂストン　社外取締役）
（株式会社イトーヨーカ堂　監査役）
（日本ピグメント株式会社　社外取締役）

〈モデレーター〉

日本価値創造 ERM 学会　副会長　　吉野太郎

開会挨拶

（日本価値創造 ERM 学会副会長　吉野太郎）

定刻になりましたので、これから第３回の公開セミナーを開催いたします。本日は、お忙しい中、お集まりくださりありがとうございます。私は当学会の副会長を拝命している吉野と申します。よろしくお願いします。

当学会では、毎年４回程度、公開セミナーを開催し、ERM（全社的リスクマネジメント）についての各種の情報発信を行っています。今回は、皆様のお手元にございますとおり、「改訂版 COSO-ERM の我が国企業での活用の方向性」を社外取締役の視点から考えてみたいと思います。

まず、今回のセミナーの趣旨を説明させていただきます。この 10 年、技術改革の急速な進展とそれに伴う産業構造の転換、保護主義の台頭、地震や台風などの自然災害の頻発およびテロの脅威の深刻化など、リスクは複雑化、巨大化しており、企業に深刻な影響を及ぼす新たなリスクが発生しています。

さらに近年、わが国を代表する企業、競技団体もしくは学校法人などで、まさかと思うような不祥事が頻繁に報道されております。そのような時代においてわが国の企業では、リスクマネジメントがますます重要になっているということは承知のことだと思います。そして、わが国の企業は、このリスクマネジメントを強化するための手段、視点、人材をますます必要としています。

このような時代背景の中で、昨年（2017 年）９月に 13 年ぶりに改訂版が公表され、本年４月に邦訳が公表された改訂版 COSO-ERM は、わが国が必要としているリスクマネジメントの強化に対して、一つの方向性を示すものではないかと考えております。その内容を理解し、各社のリスクマネジメントの強化に活用することが望まれていると思います。

改訂版 COSO-ERM の書名は、「全社的リスクマネジメント　―戦略とパフォーマンスとの統合」でありまして、企業が ERM を戦略およびパフォーマンス統合させることによって、持続的な価値向上を実現するためのフレームワークを提供しています。わが国企業がこの改訂版を活用して、ERM を企業価値向上の手段として活用することが望まれます。

本セミナーの構成ですが、まず最初に、改訂版 COSO-ERM の概要を、邦訳の実務面の取りまとめを担当されました監訳者の青山学院大学の橋本先生に、わが国企業の活用の視点も含めてご説明いただきます。それを踏まえて、ERM を取締役会がどのように監督すべきかについて、複数の企業で社外取締役をご担当されている根本直子様と鈴木洋子先生も交えて議論することを通して、改訂版 COSO-ERM のわが国企業の活用の方向性を展望したいと思い

ます。

それでは、これから基調講演として、「改訂版 COSO-ERM の概要　～我が国企業での活用の視点も含めて」という標題で、青山学院大学の橋本尚先生にお願いします。橋本先生、よろしくお願いします。

第１部：基調講演

（青山学院大学　大学院会計プロフェッション研究科教授　橋本　尚(たかし)）

こんにちは。ただ今ご紹介いただきました青山学院大学の橋本でございます。今日は、「改訂版 COSO-ERM の概要　～我が国企業での活用の視点も含めて」ということで、ERM(全社的リスクマネジメント)の最新動向とわが国企業が得るべき知見というようなことを１時間ほどお話しさせていただきます。どうぞよろしくお願いいたします。

１．当初版 ERM フレームワーク（2004 年 9 月公表）

ERM に関して COSO は、先ほど吉野さんの紹介にもありましたように、2004 年 9 月に「全社的リスクマネジメント　―統合的フレームワーク」というタイトルの報告書を公表しました。当初版の ERM フレームワークは世界中に普及しており、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ました。

当初版フレームワークでは ERM を、「事業体の取締役会、経営者、その他の組織内のすべての者によって遂行され、事業体の戦略策定に適用され、事業体全体にわたって適用され、事業目的の達成に関する合理的な保証を与えるために事業体に影響を及ぼす発生可能な事象を識別し、事業体のリスク選好に応じてリスクの管理が実施できるように設計された、一つのプロセスである」と定義しております。

この ERM の当初の定義は、内部統制の定義と平仄を合わせたもので、すべての者によって遂行される、しかも１つのプロセスである、あるいは合理的な保証を与えるといったところが、内部統制の定義と共通していました。けれども、この ERM の定義では、リスク管理担当者にとっては比較的容易に理解されるものでしたが、経営者をはじめ、それ以外の関係者にとっては分かりにくいものでした。この点、2017 年版の改訂版の定義は、後ほどお示しするとおり、分かりやすく、かつ、読みやすく見直されております。

また、改訂版 ERM フレームワーク作成にあたっては、フレッシュ・キンケイド式読みやすさ判定ツールという英語の文章の読みやすさや解釈のしやすさを判定するツールがある

のですが、それを全部、文書の全体にかけまして、報告書全体にわたって読みやすくなるように改善されております。加えて、実際にリスクマネジメントを担当している実務家の方が下訳を担当されたこともありまして、邦訳はこれまでの翻訳調のものと比べると、かなり読みやすくなっております。

当初版の ERM フレームワーク公表以降の 10 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発生しました。特に、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りました。金融業界は、あらゆる業界の中で最も強力で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、この金融機関が世界的な金融危機によって深刻な影響を受けたことは、ERM 関係者にとって大きなショックでした。

また、当初版の ERM フレームワーク公表当時は、ちょうどアメリカにおいては 2002 年のサーベインズ・オクスリー法（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のばらつきが見られました。そのため、今般の改訂にあたっては、ERM が経営にどのように役立つかを経営者に分かりやすく示すことが大きな課題になりました。

２．2017 年版 ERM フレームワークの公表

企業を取り巻く環境が激変する中で、戦略や事業目標の達成に役立つ新たな ERM フレームワークのニーズに対応するために、COSO は 2017 年、昨年９月（報告書の日付は６月になっていますが）に、「全社的リスクマネジメント－戦略とパフォーマンスとの統合」というタイトルで改訂版 ERM フレームワークを公表しました。

今日、お手元の資料は白黒で印刷されていまして、ちょっと分かりづらい面もあると思いますが、今回の新しい ERM フレームワークはカラー版でできておりまして、５つの構成要素をそれぞれ別の色で色分けしています。スクリーンに投影したパワーポイントは色を付けています。これまで一連の COSO の報告書の邦訳は白黒版で公表してきたのですが、今回はカラーでないと理解がしにくいため、邦訳もカラー版になっております。ERM に関連して、事例の解説編など、さまざまな文書が、そのあと公表されており、それらも今後翻訳をしていく予定ですが、カラー版で出版することを予定しております。

この改訂版のフレームワークは、ERM の最新かつ進化している概念と適用方法を反映したものであり、報告書名にもあるように、統合（integrate）という言葉が強調されております。戦略策定においても、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おります。特に、戦略の策定と実行における戦略及び 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ます。組織は、世界的な規模で、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ものと考えられます。

改訂版のフレームワークは、組織が脅威を管理するだけでなく、より上手に機会（opportunity）を追求するのに役立つように考案されております。具体的には、リスクマネジメントの中心的検討事項として、戦略と事業体のパフォーマンスの重要性を認識しており、内部統制と ERM をより明確に区別し、ERM を意思決定に不可欠なものと位置づけております。

2017 年版の 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」と定義することによって、これまでの 2004 年版の定義からの簡素化を図っております。

今回の翻訳にあたって、パフォーマンスやカルチャーなど片仮名用語が多いのですが、例えばパフォーマンスを「業績」と訳すと、量的な面しか出ないで質的な面の意味合いが出ません。また、カルチャーを「文化」と訳すと、なんとなく古い感じがします。そのため、パフォーマンスやカルチャーといった片仮名で訳して、少し新しい意味や広い意味を込めたものにするべきではないかと考えて、片仮名用語での訳を交えております。

この ERM の新しい定義では、カルチャーを認識すること、能力を開発すること、実務に適用すること、戦略策定およびパフォーマンスと統合（一体化）すること、戦略と事業目標に係るリスクを管理すること、および価値とリンクしていること、このようなことに焦点を当てながらリスクを管理することが強調されております。この改訂版のフレームワークは、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おります。

また、よく内部統制とリスクマネジメントとガバナンスとの関係が問われますが、内部統制は ERM の基盤として位置づけられています。COSO が 1992 年に初めて公表した内部統制のフレームワークを改訂した 2013 年版の内部統制フレームワークと今回の改訂版 ERM フレームワークとの間には、優劣の関係はなく、互いを補完するものとなっております。

さらに、ERM の概念と原則は、内部統制と同様に、営利、非営利などの法的な構造や、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おります。COSO はそもそも、営利、非営利、政府組織といった、いずれの組織もステークホルダーに価値を提供するために存在することを前提にしています。改訂版の ERM フレームワークは、価値の大部分が戦略レベルの意思決定と日常業務レベルの意思決定の両方によって決まることを示しており、それらの意思決定により価値が創造されるか、維持されるか、実現されるか、あるいは損なわれるかが決まります。

（新しい図１：戦略の位置付け）

グラフィックを用いて、このような ERM の考え方が示されておりますが、改訂版の 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を下図のように図示しています。2004 年版の当初版の ERM フレームワークでは、内部統制と同様に「COSO キューブ」と呼ばれる立方体の図が使われていましたが、この図にありますように「COSO キューブ」は踏襲されず、戦略の位置づけが以下のように図示されております。

この図は英語で書かれていますが、図の左の部分が、ミッション、ビジョンおよびコアバリューであります。組織の中核目的と願望は、組織のミッションとビジョンに定められており、期待される行動は、組織のコアバリューに示されております。この図の中央部分は、戦略、事業目標およびパフォーマンスであります。中央の輪は、戦略策定時、事業目標設定時およびパフォーマンス推進時に３種類のリスクが存在することを示しております。それぞれ色分けしてありますけども、戦略と事業目標が整合しない可能性というリスク、それから、選択された戦略からの影響、および戦略とパフォーマンスに係るリスクであります。そして、この図の右はパフォーマンスの向上につながるということが示されております。

また当初版では、４つの目的と８つの構成要素の関係が「COSO キューブ」という立方体によって表されていましたが、2017 年版の新しい改訂版のフレームワークでは、５つの構成要素と 20 の原則という形での提示に変わりました。このように、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プリンシプルベースの考え方は、2013 年版の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 の原則と平仄を合わせたものになっております。

（新しい図２：COSO リボン）

また「COSO キューブ」は、1992 年の内部統制のフレームワークと同様、2013 年版として改訂された内部統制フレームワークでも引き続き使用されていますが、改訂版 ERM フレー

ムワークでは、前述の通り「COSO キューブ」は踏襲されず、新たに「COSO リボン」と称される図が導入されております。上の図をさらに展開したものが下の形ですが、DNA の二重らせん構造のようなリボンの形式ですので、「COSO リボン」と呼び、新たにこの形で ERM のフレームワークが提示されております。

この「COSO リボン」というのは、DNA の二重らせん構造から着想を得たもので、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）されていることを分かりやすく図示したものであります。この図は、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との関係を説明したものですが、「戦略と目標設定」「パフォーマンス」「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おります。「ガバナンスとカルチャー」「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おります。

また、「COSO リボン」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おります。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ります。ERM は、最終的に価値を創造し、維持し、実現するために、戦略とパフォーマンスに不可欠なものです。

最初の図を展開したこの「COSO リボン」は、ERM の５つの構成要素を５色のリボンで織りなすように描くことで、統合を説明するとともに、５色のリボンが戦略の策定、事業目標の体系化、実践とパフォーマンスを通り抜けて、最終的に一番右側で価値の向上につながることを示しております。

３．COSO 改訂 ERM の構成要素

改訂版 ERM の５つの構成要素は、このように「ガバナンスとカルチャー」「戦略と目標設定」「パフォーマンス」「レビューと修正」「情報、伝達および報告」の５つであります。

（ガバナンスとカルチャー）

ガバナンスとカルチャーは、ともに ERM の他のすべての構成要素の基礎となるものであります。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ものであります。

カルチャーは、意思決定に反映されるもので、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おります。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ます。

（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ます。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ます。組織は、戦略策定と合わせてリスク選好を設定します。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ものであります。

（パフォーマンス）

３番目のパフォーマンスについては、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、評価します。先ほど、最初の図の説明の中で、３つのリスクの種類があると申し上げましたが、もう１つ、リスクについては３つの側面から捉えられておりまして、これは「新しいリスク」、「エマージングリスク」、および「変化する既存のリスク」という、このような３つのタイプのリスクを示して、リスクの識別、評価を求めております。従って、新しい改訂版の ERM フレームワークは、３つのリスクと５つの構成要素、そして 20 の原則から構成されていると見ることができます。

リスクを識別、評価するために、組織は、戦略と事業目標の達成に影響するかもしれない事象を識別、評価しますが、組織は、この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ことになります。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します。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します。

（レビューと修正）

次のレビューと修正に関しては、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することができます。

（情報、伝達および報告）

最後の、情報、伝達および報告については、内部統制では５つの構成要素の中で「統制

環境」と「情報と伝達」が日本企業にとって重要と言われていますが、ERM では最初の「ガバナンスとカルチャー」のところと、最後のこの「情報、伝達および報告」のところが、特に日本企業にとって重要と言われております。

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とされております。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します。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します。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、カルチャー及びパフォーマンスについての報告を行うことになります。

改訂版 ERM フレームワークでは、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 20 の原則が体系的に提示されております。公開草案では 23 あったのですけれども、最終的には 20 の原則に集約されております。各原則は、関連する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ります。

（１）ガバナンスとカルチャー

ガバナンスとカルチャーに関連する原則は５つあります。「取締役会によるリスク監視を行う」が最初の原則ですが、取締役会は全般的なリスク監督に第一義的責任を負う一方で、経営者はリスクマネジメントに第一義的な責任を負っております。取締役会は、十分なスキル、経験および業務知識を持って、リスク監督の責任を果たします。取締役会は、組織のミッション、ビジョン、戦略と事業目標および関連するリスクを理解する必要があります。取締役会は組織の複雑さを理解して、組織のリスクマネジメントアプローチを戦略と事業目標に合わせます。また、十分に独立しており、客観的に監督責任を果たすことが必要となります。取締役会は、組織バイアスや集団思考を最小限に抑えて、リスクマネジメントに関する意思決定の有効性を確保する必要があります。

２番目の、「業務構造を確立する」関しては、戦略と事業目標を支援するような業務構造と報告経路を組織は定めることになります。また、リスクマネジメント活動は、経営者の意思決定の裏付けとなる適切な情報が伝達されるよう構築されます。

３番目の、「望ましいカルチャーを定義づける」。特にこのカルチャーというものが、改訂版の ERM では重視されておりまして、この原則の３番をどのように具体化するかというのが新しい ERM のフレームワークを導入あるいは活用する際の１つのキーポイントとされております。その他に、「コアバリューに対するコミットメントを表明する」「有能な人材を惹きつけ、育成し、保持する」といった原則が示されております。この５番目の「有能な人材を惹きつけ、育成、保持する」は、サクセッションプランや後継者の養成といったところとも関連しております。

（ポイント①）

この最初のガバナンスとカルチャーの部分についてのポイントと実践上の課題をいつか

挙げてみますと、まず、ERM におけるカルチャーの役割、重要性を認識し、「リスクを認知するカルチャー」を醸成することが重要と考えております。リスク管理の重要性を強調するとともに、リスク情報の適時な伝達、さらには、許容範囲と活動限度の認識、また、リスクに関してのオープンな議論というものを行うことで、組織行動がリスク選好と結びつくことになると考えられております。「リスクを認知するカルチャー」の醸成については、経営者がトップダウンでメッセージを継続的に伝え続けることが重要とされております。

（実践上の課題②）

実務上の課題としては、経営者にとっては明確な意思表示の継続、経営企画部門にとってはカルチャー醸成に必要な事項の継続的推進、内部監査部門については経営企画部門の取組状況の検証と改善提言、取締役会・監査役については経営者の取組状況の監督と改善指示があると考えられております。

（ポイント②）

また、テクノロジーの進化に伴う業務モデルの変化と、それに伴うリスクの変化への対応も重要と考えられております。テクノロジーの進展あるいはグローバル化というのが、現在の企業を取り巻く大きな事業環境の変化の１つと考えられています。標準的な業務モデルはバーチャルとなると考えられますので、業務モデルは複数のテクノロジーの組合せに依存することになります。そのため、業務モデルの変化に伴ってリスクが変化することについて考えていく必要があります。こういった変化にどのように対応するか、あるいは業務モデルが変化することで既存のリスクがどのように変化するかに着目することが必要とされております。

（実務上の課題②）

実務上の課題としては、業務モデルの変化を定期的に確認し、業務モデルの変化に伴うリスクが今後、戦略と事業目標の達成にどのような影響を及ぼすかを検討する体制を構築することであります。リスクが顕在化する前に、対応を予め意思決定しておく、想定内、想定外といった言葉がよく使われますけども、先見の明を持って、先を見越して対応策を予め決めておくことが重要とされております。

（２）戦略と目標設定

次の戦略と目標設定に関する原則は、６番から９番までの４つあります。「事業環境を分析する」「リスク選好を定義する」「代替戦略を評価する」「事業目標を組み立てる」という４つであります。特にこのリスク選好の定義に関しては、さまざまな説明がフレームワークの中でなされておりまして、リスクをどのように表すかについて、新たなリスク概念などの理論的な発展を反映させるのに、かなり精緻化した議論がなされております。

（ポイント）

ここでは事業環境、外部内部要因の分析ということで、組織全体に展開するリスク選好と戦略との整合性、代替戦略のリスクも評価対象とされております。また、戦略と整合し

た各階層の事業目標の体系化といったことも示されております。

このようなリスクに関しては、特にこの戦略と目標設定をカスケードする、落とし込んでいくという概念が示されておりまして、段階的に上の目標から下の目標に落としていくとどうなるかとか、あるいは逆に、下の目標からだんだんと事業体全体の目標に積み上げていくときに、どのようにリスクが変わっていくかとか、そういったことを総合的に検討することが求められております。

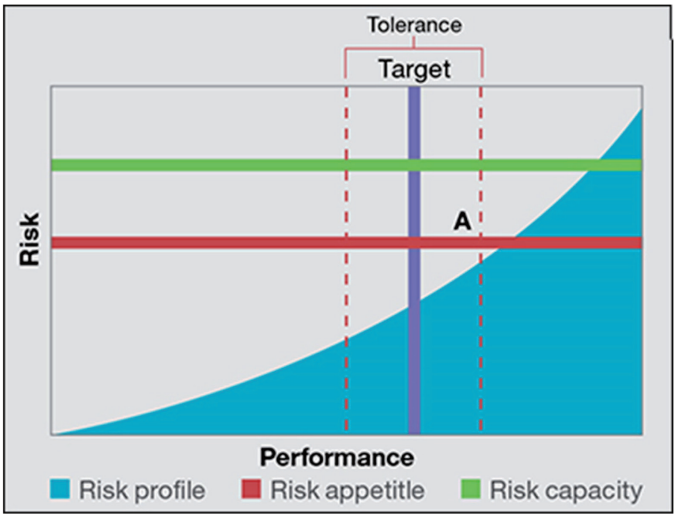
（実践上の課題）

実践上の課題としては、このような事業環境の変更に伴うリスク対応、ダイナミックな戦略変更とリスク対応、許容できる業績の変動幅の設定などがポイントとなります。

リスクプロファイル、リスク選好と許容度といった形で、さまざまなリスクの考え方が示されております。改訂版 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ところが大きな特徴となっております。リスク選好の定義については、従来の、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で、許容度（tolerance）については、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け入れ可能な変動範囲と定義されております。

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とになります。紫の線の部分と赤い線の部分が交わっているところが、この関係を示したところであります。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ります。リスクもパフォーマンスも変化しないもの、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、よりよく評価することが可能となります。

リスクプロファイル、リスク選好と許容度



2017 年版の ERM フレームワークの付録 D において、このような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おりますので、リスクプロファイルのこういった例示については、付録の D の部分を参照していただければと思います。

（３）パフォーマンス

次のパフォーマンスに関する原則は５つ、10 番から 14 番まであります。「リスクを識別する」「リスクの重大度を評価する」「リスクの優先順位づけをする」「リスク対応を実施する」「ポートフォリオの視点を策定する」の５つであります。

（ポイント）

リスクの重大度については、従来、発生可能性と影響度という２つの面から見てきましたけれども、新しい ERM フレームワークでは、これにさまざまな適応性とか、複雑性とか、速度、持続性、回復度といったものを設けて、次のリスクの優先順位づけの基準として位置づけております。また、14 番の「ポートフォリオの視点を策定する」では、ポートフォリオの視点に立って、個々のリスクではなくて全体として見ることの重要性を指摘しております。

ここの部分では、新しいリスクおよび変化するリスクの識別が取り上げられていますが、最近では、これまでにないような新しいタイプのリスクが発生しております。また、エマージングリスク、こういった既存のリスク以外のリスクにどのように対応していくかとともに、これまでの既存のリスクも変化していますので、そのような３つのリスク、すなわち新しいリスク、エマージングリスクおよび変化するリスクに対応することが必要であります。

（実践上の課題）

実践上の課題としては、事業内容の変化に伴うリスクの変化、例えば M&A をしますと、これまでと違った形でのリスクテイクが必要になることもありますし、違った業種への展開をしますとそれに伴って、リスクも変容してくるものと思われます。それから、リスク選好と許容度の測定、組織レベルと全社レベルの調整、こういったところも１つの課題であります。下の階層ではそれほどでもないリスクが、それを積み重ねることによって大きなリスクになる場合もありますし、あるいは、目標との関連でどこまでリスクを取るかも検討していく必要があります。

（４）レビューと修正

次が、レビューと修正に関する原則が、15 番から 17 番の３つとなります。ここでは、「重大な変化を評価する」「リスクとパフォーマンスをレビューする」「ERM の改善を追求する」といった３つが挙げられております。

（ポイント）

ポイントとしては、持続的な変化そのものよりも、それらが戦略、リスクに与える影響の評価が重要となります。全社的リスクマネジメントについて、継続的な改善のための見直しを行っていくことがポイントであります。

（実務上の課題）

実務上の課題としては、「変化」が組織の戦略、リスクに与える「影響」が組織のリスク感応度・対応力、リスク選好度等によって一様ではないので、影響度の計測が難しいという点が挙げられるかと思います。社内外の重大な変化を捉えた上で、それらが組織のリスク、パフォーマンスに与える影響をレビューするという構成でありますので、ここでは重要な「変化」そのものよりも、それらが戦略、リスク、およびパフォーマンスに与える「影響」を評価するという点がポイントとなります。

（５）情報、伝達および報告

最後の、情報、伝達および報告に関する原則は、18 番から 20 番までの３つであります。「情報とテクノロジーを有効活用する」「リスク情報を伝達する」「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」という３つであります。

特にこの部分では、内部統制のフレームワークではないものとして、情報システムについての言及がなされている点が ERM の新しいフレームワークの特徴であります。テクノロジーの進展とともに、いろいろとこういった情報とか伝達、報告の手段も変わってきておりますので、効率的に適時に対応していくためにどのようにしたらいいか、全社にわたって、このような情報伝達および報告の経路を確保することが重要とされております。

（ポイント）

このポイントといたしましては、情報の「品質」の維持つまり、増大するデータ量の中

で、情報の品質を確保、維持することが１つのポイントになります。そのためには、新たなテクノロジー、情報システムの活用もさることながら、既存システムの情報を活用することで、関連性／適切性、利用しやすさ、信頼性／正確性、最新性といった情報の品質を確保し、リスクへの理解が深めることが必要になります。

次のポイントは、リスク情報の中身についてであります。価値あるリスク情報は、戦略、事業目標、パフォーマンスと深く関連するものでなければなりません。ここでは、KPI とか KRI、リスクカルチャー、リスクアペタイトの影響を受けるという点が示されております。

（実務上の課題）

実務上の課題としては、情報過多の環境の中で、情報量の絞り込み、質の確保をどう確保するのか、また、ソーシャルメディアなどの伝達手段が多様化する中で、報告相手を意識した対応が求められます。一歩間違えると効果がなかったり、また、悪い影響を及ぼしたりしかねませんので、この点は留意が必要であります。

また、「カルチャー」については、定性的で、その分析・計測というものは複雑かつ難易度が高いということが挙げられます。こういった点に実務では留意する必要があるかと思われます。

４．内部統制との関係

内部統制と ERM は、今回のフレームワークで明確に線引きがなされております。その中で、内部統制は ERM の基盤として位置づけられております。原則 10 から 14、とりわけ原則 13 によって両者はリンクづけられております。2013 年版の内部統制のフレームワークと、改訂版 ERM フレームワークは相互補完関係にありますので、両フレームワークに共通の構成要素である統制活動などについては、改訂版 ERM フレームワークでは特に言及されておりません。他方、ガバナンスなどの幾つかの概念については、敷衍、発展させて説明がなされております。

５．ERM の最新動向から我が国企業が得るべき知見

（主要な変更点）

以上、2017 年版の ERM フレームワークの、当初版のフレームワークからの主要な変更点としては､以下の 10 項目にまとめることができます｡①構成要素と原則の構造を採用した、５つの構成要素と 20 の原則で説明しているという原則主義的、プリンシプルベース的な思考であります。②ERM の定義が簡素化され、リスク担当者以外の人たちにも分かりやすいものとなっております。さらには、③リスクと価値との関係の強調、④新たに ERM の統合（一

体化）というところに焦点を当てている点、⑤カルチャーの役割を考察している点、⑥戦略の議論を高めている点、⑦パフォーマンスと ERM の連携の強化を図っている点、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の明確化、⑩リスク選好と許容度に関する考え方の精緻化といったところに主な変更点を見ることができます。

（プラスのリスクも対象とする）

ERM はもともと保険論やファイナンス論の領域の概念であることから、マイナスの影響を与える事象をリスクとして捉えてきました。2004 年の当初版 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て、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ました。

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両方のリスクを視野に入れる必要があることは言うまでもありません。改訂版の ERM フレームワークでは、ERM の定義の最新化と同様に、リスクについても、事象が発生し、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を示すとともに、先ほどの３つの種類のリスク、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つのリスクの識別のためのアプローチが提示されております。

このように、プラスのリスクとマイナスのリスクという両方を視野に入れたことで、リスク対応としても、従来のマイナスリスクへの対応としての回避、低減、共有、受容といったリスク対応に加えて、活用（pursue）という、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とか、積極的にリスクを取っていこうというような、ERM 固有の内部統制のリスク対応にはない対応策を講じる道が開かれました。むしろ、事業機会があるところにおいては、そういったリスクを積極的に取っていこうというような対応も示されております。

（リスクの重大度の評価）

従来、リスクの重大度は、発生可能性と影響度ということで評価されてきましたが、改訂版フレームワークでは、①適応性、複雑性、速度、持続性、および回復度といったものを考慮すること、②リスクをポートフォリオの視点によって評価すること、および、③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とその重要度を評価することを重視しております。

（リスク評価におけるバイアス）

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ります。これに関して、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という理論を紹介して、フレーミングのバイアスによってリスクが正確に記述されないリスクを念頭に置くべきとしています。

人間は損失を被る場合には積極的に回避することを優先するが、利益を得る場合には確実に手に入れることを優先する傾向があるというプロスペクト理論においては、自分が儲かる状況になったときの選択の仕方と、自分が損する状況になったときの選択の仕方が違

うことが示されています。こういったことを利用して、リスクを識別する際のバイアスについても注意するように促しております。

（情報とテクノロジー）

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て、データの有効かつ効率的な管理・分析方法や、最新のテクノジーの活用方法が詳細に検討されております。人工知能やデータマイニング、機械学習といったコグニティブコンピューティングの進化についても触れておりますし、ビッグデータの管理、分析についても言及されております。利便性と脆弱性を併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ことを求めております。

（戦略およびパフォーマンスとの一体化）

このように、2017 年版の新しい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、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おります。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ころに、改訂版の ERM フレームワークの最大の特徴があります。

このように、分かりやすい 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、しかも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、新しい改訂版のフレームワークでは明確かつ体系的に示されております。

（わが国の長寿企業のカルチャーから学ぶこと）

改訂版の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おります。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ですが、長期的、持続的な企業価値向上の観点からは、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」、フェアプレーに徹することといった、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ります。

わが国は非常に、100 年を超えるような長寿企業が世界で一番多いといわれております。金剛組という建設業の会社は、飛鳥時代の 578 年創業で、四天王寺なども建設し、今年は 2018 年ですから 1,440 年続いている会社となります。池坊華道会、旅館やホテル、出版、飲食、あるいはデパートといった老舗の企業が多いのが日本での特徴でありまして、日本には創業 100 年を超える企業が３万 3,000 社余りあるといわれており、世界一であります。

これはアジアの特徴かというと、そうでもなくて、中国や韓国には 100 年以上続いている会社はあまりないようであります。国が変わったり、あるいは政争とかのない安定的な状況でないと、なかなか長期にわたって会社を維持することは難しいものといえます。また、長寿企業であっても、いろいろ新しいビジネスの波が押し寄せてきますので、それに対応できるかどうかというのも１つの鍵であります。

このような、日本の企業に長寿企業が多いということは、特別の技術を持っていたりとか、あるいは経営のノウハウがあったりという面もありますけども、この ERM でいうところのガバナンスとカルチャーの部分が大きく影響しているのではないかということで、今、当日本内部統制研究学会では、このような日本の長寿企業のガバナンスの研究をしようと研究チームを立ち上げております。

（我が国企業が求められること）

また、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といわれております。

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ります。その際には、経営者の交替といった組織内部の変化、そして M&A といった外部からの影響により、組織のカルチャーに変化が生じることにも留意する必要があります。

改訂版の ERM フレームワークは、事業目標の達成のために戦略的活動の一環として組織に組み込むべき ERM のフレームワークを提示したものであり、ERM を通じた経営の指南書と言うこともできます。ERM 関係者は、経営者との対話において大いに活用できるでしょうし、経営者にとっても必読の書といえます。組織の戦略やパフォーマンスと一体的な活動の一部として ERM を有効かつ効率的に実践していくためには、経営者の資質が改めて問われることになるでしょうし、ある意味では経営者の意識改革も必要とされるかもしれません。

（COSO 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　事例の解説篇）

これまで、去年の９月に公表されました 2017 年版の改訂版 ERM フレームワークについての概要と、特に日本企業の持続的な発展のために、どのような点がポイントかということに触れてきましたが、この ERM の改訂版フレームワークの他に、COSO は ERM に関して、「事例の解説篇」（Compendium of Examples）という文書を今年の６月に公表しております。

この文書は 100 ページぐらいの文書でありますが、さまざまな、地方規模、全国規模、国際規模の会社について、どのように 20 の原則を適用すべきかについての事例を全部で９つ挙げており、金融機関から消費財メーカー、政府機関、テクノロジー会社、あるいはガス会社、学校など様々な事業体についての事例を紹介しております。

この「事例の解説篇」についても翻訳を進めておりまして、今年の 12 月には日本内部監

査協会から、『COSO 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　事例の解説篇』の書名で刊行される予定です。おそらく 11 月の末、26 日ごろには Amazon で出るのではないかと思われます。

（不確実な時代のリスクマネジメント－COSO 新フレームワークの活用）

また、この改訂版 ERM フレームワークは、内部監査人が活躍する場を広げると言われていますが、内部監査や内部監査人についてはあまり触れられていません。そのため、今年の２月から COSO の新しい会長に就任した内部監査人として非常に有名なポール・ソーベルさんが、内部監査人向けの改訂版 ERM フレームワークの解説書を出しております。これはすでに今年の８月に邦訳が出されておりまして、『不確実な時代のリスクマネジメント－COSO 新フレームワークの活用』(日本内部監査協会)という書名です。非常に短い本ですが、内部監査人がどのように改訂版 ERM フレームワークを活用したらよいかということについて分かりやすく示されているので、参考になるのではないかと思います。

（ESG 関連の報告書）

また、一番新しいところで、このスライドを作る時には出ていなかったのですが、COSO は今年 10 月に、ERM を環境、社会およびガバナンス関連のリスクに適用することに関する報告書も公表しております。これが表紙です。106 ページぐらいの報告書ですが、これが今一番、企業の皆様は関心が高いようです。特にガバナンス関連の ESG に取り組んでいる方は、非常に注目しています。これは WBCSD（持続可能な開発のための世界経済人会議）という機関との共作です。COSO は翻訳権にうるさいのですが、こちらはガバナンスに関する国連の機関なので、翻訳権についてあまりうるさくなく、おそらく無料で翻訳できるのではないかと思われます。100 ページちょっとなので、来年の春ぐらいまでにはなんとか翻訳を出そうと考えています。これは統合報告とか全部そういったものも含まれていて、統合報告書との関連で、いろいろ示唆に富む内容となっております。

このように、ERM を巡る最新の議論から、わが国企業は様々な知見が得られるものと思われます。各組織の価値の創造、維持、さらにはその実現に向けた有効かつ効率的な ERM の実践がなされることを期待して、簡単ではありますが私の基調講演とさせていただきます。どうもご清聴ありがとうございました。

第 2 部：パネルディスカッション

１．課題認識

吉野：皆さんこんにちは。これからパネルディスカッションを始めます。今回のテーマは、お手元のパンフレットに記載してありますとおり、「社外取締役の視点から見た改訂版 COSO-ERM の我が国企業での活用の方向性」であります。

冒頭の挨拶で申し上げましたとおりこの 10 年、技術改革の急速な進展とそれに伴う産業構造の転換や地震や台風などの自然災害の頻発などリスクが複雑化、巨大化していること、および近年、わが国を代表する企業などで不祥事が頻繁に報道されていることから、わが国企業ではリスクマネジメントがますます重要になっております。このような状況下でわが国企業が、改訂版の COSO-ERM を活用して、ERM を不祥事防止や損失防止を含む企業価値向上の手段として活用することが、わが国企業のリスクマネジメント強化にとって望まれていると思います。

企業価値向上のために ERM を活用するということは､取締役会マターの事項が多いため、取締役会による監督が重要です。この点は、改訂版 COSO-ERM の構成要素の１番目の「ガバナンスとカルチャー」の最初の原則、つまり 20 ある原則の最初の原則として、「取締役会によるリスク監視」が取り上げられていることからもご理解いただけると思います。

そこで、最初に「社外取締役による ERM の監督」という点を踏まえて議論の前提となる事項を固めた上で、社外取締役による ERM の監督をどのように行うべきかについて議論を進めていくことを通して、わが国企業での ERM の活用の方向性を展望したいと思います

２．パネリストからの報告

吉野：それでは最初に、パネリストの３名の方を紹介させていただきます。皆さまに向かって右側から、アジア開発銀行研究所エコノミストの根本直子さんでございます。根元さんは、お手元のパンフレットにありますとおり、中部電力株式会社の社外取締役ならびに株式会社コンコルディア・フィナンシャルグループの社外取締役をご担当されております。その隣、中央に座っていらっしゃるのが、鈴木総合法律事務所の弁護士の鈴木洋子先生でございます。鈴木先生は、株式会社ブリヂストンの社外取締役ならびに株式会社イトーヨーカ堂の社外監査役、さらに日本ピグメント株式会社の社外取締役をご担当されております。その隣に座っていらっしゃるのが、ただ今ご講演いただいた青山学院大学の橋本先生でございます。

それでは、最初に根本さんから５分間、改訂版 COSO-ERM の企業経営の活用についての課題認識についてご報告をお願いいたします。根本さん、よろしくお願いします。

根本：アジア開銀の根本と申します。本日はよろしくお願いいたします。私はリスク管理の専門家でもないので、ご専門家を前に非常にあがってしまうのですけども、社外取締役の立場から見た課題ということで、お話をさせていただければと思います。ちょっと座らせていただきます。

１）世界金融危機：ゴールドンマン・サックスとリーマン・ブラザーズ　ー何が違いをもたらしたのか

改訂版 COSOーERM についての橋本先生のお話で、グローバル金融危機が改訂の契機になったと伺いましたので、ちょっと振り返りというか、2008 年のリーマンショックは何だったのか考えてみたいと思います。私は、もともと日本銀行に入って、そのあと S&P という格付け会社で金融機関の格付けをしておりまして、どちらかというと金融が専門でございまして、そちらの方面のお話になってしまいます。

ゴールドマン・サックスは今も非常に栄えている投資銀行ですが、同じ投資銀行のリーマン・ブラザーズは破綻し、救うと思われていたところが破綻して、あれだけのショックが世界中で起きました。では何がその違いだったのか。

（共通点）

両社の共通点として、①まず、トレーディング業務のウエートが高いということです。②それからリスクテイク意欲も高い。かなり複雑な商品もいろいろ扱っていた。そしてグローバルに事業を展開していた。リスクエクスポージャーがは非常に高い会社だった。③さらに資金調達は市場に依存していた。預金基盤とかそういうものはないわけですから、すべて市場で調達していたという状況だったと思います。

（相違点）

一方で金融危機の前に、ゴールドマン・サックスは、リスク管理部門をかなり強化していた。海外の金融機関の場合、リスク管理部門があって、いろいろとリスクを指摘してもそれが経営に取り入れられないことが往々にありました。日本の銀行危機のときもそうだったと思います。しかしゴールドマン・サックスの場合は、経営者がそれを非常に気にしていた。

そして、さっきお話にもあったリスク・リターンですね、この事業のリスク・リターンはどうなのかを常にモニターしていた。住宅ローン・モーゲージとか、サブプライムとか、こういったところの事業のリスクが高まっていて、リスク調整後のリターンが上がってないという判断から、金融危機が深刻化する前にかなり削減をしていた。当然、その部門が抵抗するわけですが、これはもうトップダウンでやったわけですね。

さらに、危機が起きて、その対応がゴールドマン・サックスは非常に早かった。2008 年

９月にリーマンが破綻したわけですけど、すぐにバークシャー・ハサウェイという、ウォーレン・バフェットの率いる会社に普通株を受けてもらった。それにより、あの人が引き受けたのだからこの会社は大丈夫だ、というような大きな効果があった。また、市場での資金調達が困難なことを予測して、ともかく長期の資金をたくさん取って、さらに現金など流動性を 11 兆円積み上げました。

さらに、投資家、顧客、あるいは政府とのコミュニケーション能力に優れており、こうしたリスク管理能力が功を奏して、ゴールドマンはあまり大きな傷を受けずに、危機を乗り切りました。

２）世界金融危機後の金融機関の対応

（組織の見直し）

世界金融危機後の金融機関の対応については、先ほどの橋本先生のお話で、カバーされていますが、まとめてみたいと思います。反省としては、組織として、リスク管理部門があってもステータスが低かった。

それについての、反省と対応として、①チーフリスクオフィサーというような方を置いたり、さらに、②リスク管理部門が、営業部門に属するのではなく取締役会とか社長にレポートしていく。また、③企業として重要性を認識し、非常に優秀な人を配置していった。そういったことで、取締役会が適切なモニタリングを行えるようになった、つまり、リスク管理部門に任せ、かつ、取締役会はその実効性を適宜見ていくということができるようになりました。

（リスク選好の明確化）

また、リスク選好ですね、リスクアペタイトとも言われていますが、これが明確ではなくて、金融機関の収益とか資本力に対して、適切なリスク量がはっきりしていなかった。かつ、企業の戦略を考える場合もリスク部門がそこに口出し、関与をしなかったという状況でした。

それに対して、さっきもお話に出たリスク選好を明確化し、どういうリスクをとるべきか、どういうリスクは回避すべきか、また取るべきリスクはどの程度とっていけるのかをはっきりさせました。それから、共通の評価尺度を設定して、リスク・リターンを計測しました。

（リスク計測手法の改善）

リスク計測手法ですが、金融機関では、たぶん他の業界に比べると若干進んでおり、定量的なモデルというのがあって、バリュー・アット・リスクなど共通の尺度で、全社的なリスクも随時把握していました。ただし、モデルの計測する数値に依存し過ぎていたことが反省点です。例えば、①バリュー・アット・リスクは株式や為替などのパラメータの平常時の分布を前提として推計した最大の損失ということですから、テールリスクの把握が不十分となり、非常時になった時は、予想を超える損失が出てしまった、②また、過去の

レコードをベースとしていたので、過去にないような動き方をした市場とか、新しい局面ではリスクを過少に見ていたというようなこともありました。

それに対しては、①１つの指標にこだわらず、多様な指標を見ていく、②バックワード・ルッキングではなく、将来を見て、ストレステストや多様なシナリオ分析で補強するという対応がされました。さらに、③商品間の相関の変化を織り込んだり、１つの部門だけのリスクを見ずに、様々な部門への波及効果を織り込むなど、分析手法の高度化もとられました。

（リスク情報の統合）

統合については、かつてはそれぞれのビジネスラインがリスクをそれぞれの立場で個別に見ており、情報共有があまりされていない、サイロ型だったということがありました。

それに対しては、リスクを横断的、包括的に見ることと情報共有が進みました。リスク管理部門、経営企画、監査部、また現場が、いろんなコミュニケーションを持って連携していこうということです。

３）金融機関はリスク・アペタイト・フレームワークを設定

リスク選好については、日本企業では必ずしも明確化されていないものの、個人的には非常に重要だと思っています。リスクをコントロールするだけではなく、攻めのリスク管理というか、リスクを管理しつつ収益をどうやって上げていくのかということが、多くの企業の課題でありそのためにも重要な課題だと思います。

（方針：とるリスク・とらないリスクの明確化）

ある地方銀行の例を取らせていただいたのですが、地方銀行の間では進んでいる事例ではないかと思います。１つは、とるリスク、とらないリスクの明確化で、この資本の範囲内で、地元の企業、個人の信用リスクをとり、資金調達を助けていく。そういうリスクをもっととっていきましょう、逆に地元を助けることにつながらない貸出の信用リスクや市場リスクなどはあまりとらない、というのが方針です。

（定量的な目標の設定）

それから、定量的な目標の設定です。例えば、①リスク調整後の自己資本がどのくらいあるかとか。あるいは、②貸し倒れとなるようなリスクを考慮して利益がどのくらい上がるのか、そういったリスク調整後利益率。あるいは、③重要な事務リスクについて、その発生をどのくらいの水準に抑えるのかなどを設定する。

（変動幅の設定）

利益のレンジとか、あるいは、この間この確率で、このぐらいのロスは出るかもしれないとか、そういう変動幅の目安をある程度決めておくということです。

（リスクリミットの設定）

リスクの限度については、①バリュー・アット・リスク（VAR）だけではなくて、②例えばよりストレスをかけた状態でのストレスVAR、あるいは、③絶対的なポジションの枠など

があります。たとえば不動産セクターへのエクスポージャーはいくらまでとか、全体の資産の何割とか、そのような形でリスクリミットをつくるということです。

（リスク・アペタイト・フレームワークの明確化・共有）

今申し上げたリスク・アペタイト・フレームワークの各項目が明確に定義され、社内で共有されているかは非常に重要ですが、私の印象では、なかなかまだそこまではいっていないと。

ただ、例えば金融機関でいえば、この貸出を決定するのに、このぐらい利ざやを取れるけど、でも、リスクを見るとこのぐらいですよね、みたいな、そういう判断は現場でされていると思います。リスクを明確に意識し、日常業務に浸透させることかと思います。

４）重要なリスク（トップリスク）の洗い出しと対応

それから、重要なリスク（トップリスク）の洗い出しというのが重要だというお話もさっきありました。企業に大きな影響を与えるリスクは、従来見てないところから新たに出てくることがあります。社内だけで見ていると、ある意味マネージ可能なことだけを見ていることもあるので、社外取締役や外部の意見なども取り入れ、想定外のリスクも考える。ただ、これもあまりとっぴ過ぎると、出してきても、「そんなこともありますか」というので終わってしまうので、バランスが難しいと思います。

以下は、東京海上ホールディングスが公表しているトップリスクです。災害リスクとか、サイバーリスクなどは業務の内容から想定できますが、８番目にあるコンダクトリスクは注目される点ではないかと思います。

重要なリスク（2018年度）		
1 国内外の経済危機、金融・資本市場の混乱	4 国内巨大地震（含む富士山噴火）	8 コンダクトリスク*
2 日本国債に係るリスク	5 海外巨大自然災害	9 海外規制への抵触
3 国内巨大風水災	6 サイバーリスク	10 テロ・暴動
	7 革新的新技術による産業構造の転換	11 パンデミック

*不正行為、不適切な対応、社内や業界慣行の世間との乖離等により、顧客保護、市場の健全性、有効な競争、公益等に対して悪影響を及ぼした結果、企業価値の毀損に繋がるリスク

コンダクトリスクは、不正行為、不適切な対応、もしくは社内や業界の慣行が世間と乖離していること、それにより顧客保護や有効な競争に対して悪影響を及ぼすというリスクです。最近の品質管理問題などもそれに該当すると思います。「ちょっとぐらい緩めてもいいじゃないか」、「赤信号でも、渡っても、誰もいないんだからいいじゃないか」など、そんなに悪いことをされているという気持ちがなくても、それが結果として大変な企業価値の損失になってしまうという事例が、問題となっています。

日本は長寿企業が多い、企業文化がそれを支えているというお話があり、全くそうだと思います。ただ一方で、その成功体験が、マイナスとなる懸念もあります。日本の企業は

従業員の質も高く、大丈夫だ、といった過信が背景となって、コンダクトリスクが起きているケースもあるようです。

それに対しては、こういうことをしてはいけませんという、リストをつくって配っても、それだけでは防げないと思います。さっき橋本先生のお話にもありましたが、ミッション、ビジョンおよびコアバリュー、そういうものを明確に示して、かつ、経営者が率先して示していく、背中を見せていく、そういうカルチャーを醸成することが非常に重要だと思います。

５）日本企業が不十分な点：全体の連携

最後に、日本企業がまだ改善の余地がある点として、全体の連携があります。例えばリスク選好、リスク管理の強化、事業継続、あるいはコーポレートガバナンスの改革とか、それぞれにおいては非常に真面目に取り組んでいるんですけど、まだその全体の連携というのが十分ではない点もあるように思います。

例えば、報酬制度とガバナンスについては、日本人はそんなに報酬にこだわらないという見方もあり、実際に、私利私欲のために不祥事を起こしたというケースは比較的少ないようです。しかし不祥事の起きた原因の中には、評価、報酬制度の設計に問題があった例もあるようです。従って、例えば、①営業成績だけではなく、リスクを勘案して、あるいは行動を勘案して評価をしましょうとか、あるいは、②業績に連動した報酬については、あまりに業績連動が高すぎないかチェックしましょうとか、そういうリスクを勘案したバランスのある制度が重要ではないかと思います。

また、リスク管理に取り組んでいくのはリスク管理部門だけではない、さっきお話があったフロントラインというか現場の役割も必要ですし、監査部門、経営陣、全体がオーナーシップを持っていく必要があります。それをつないでいくのは、こういった企業カルチャーとかリスクカルチャーの育成ではないかと思います。以上が、私のご報告というか意見でございました。

吉野：どうもありがとうございます。では、続きまして、鈴木先生、よろしくお願いします。

鈴木：皆さんこんにちは。先ほどご紹介にあずかりました弁護士の鈴木洋子と申します。私は 12 年間セブン&アイ・ホールディングスの社外監査役を務めまして、現在はイトーヨーカ堂の監査役とあと、ブリヂストンの社外取締役監査委員会委員、そして、日本ピグメント株式会社の社外取締役監査等委員というところで、主に監査業務を通じて実務家としての仕事をやっておりますので、実務家という観点から今日はお話をさせていただきたいと思っております。どうぞよろしくお願いいたします。座らせていただきます。

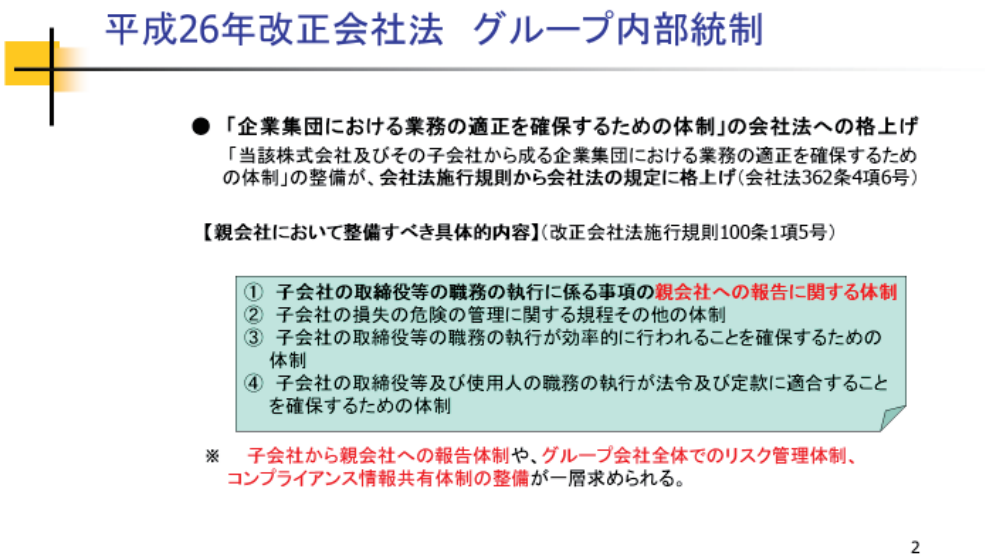
１）社外取締役の役割

社外取締役の役割というところなんですが、これは一言で申し上げると、企業の持続的な成長と中長期的な企業価値の向上のために尽くすということになろうかと思います。先ほどお話がございました、ERM をどのように活用するかというところでご説明いただきました５つの構成要素、20 の原則というのは、実務上いずれも有用だというふうに感じております。特に、社外の目を活かすためには、「情報、伝達および報告」というところが大変重要になるかと思います。これをちょっと実務的なところに触れさせていただきながらご説明したいと思います。

２）グループ内部統制（平成 26 年会社法改正）

こちらの情報伝達統制というところは、グループの内部統制、グループでのガバナンスとして、近年大変重要視されているというふうに理解しております。まず１つには、平成 26 年改正会社法で、「企業集団における業務の適正を確保するための体制」について、会社法への格上げがなされたということで、グループ全体でのガバナンス、コンプライアンス、リスク管理というところが非常に重要になったというふうに受け止めております。

特に、「親会社において整備すべき具体的内容」として、会社法の施行規則で定められました、①のところでございますが、「子会社の職務の執行に係る事項の親会社への報告に関する体制」というのをきちっと定めるようにというふうに新設されております。このような会社法の改正を受けて、一番下に書かせていただきましたとおり、子会社から親会社への報告体制、グループ会社全体でのリスク管理体制、コンプライアンス情報共有体制の整備というのが、親会社として一層求められるという法律上の建付けにもなっております。



３）監査を支える体制の充実・内部統制運用状況の開示（平成 26 年会社法改正）

内部統制関連に関しましても、監査を支える体制の充実というところで、新たに会社法施行規則の定めが増えまして、赤で表示をさせていただいておりますように、子会社の取締役等からの親会社監査役への報告体制、報告者が不利益な取り扱いを受けないことを確保する体制というものが追加されております。

また、内部統制システムの運用状況の概要に関する開示につきましても、以前は基本方針の内容を決定すればいいという立て付けだったのが、「運用状況の概要」についても、事業報告の内容として記載をすべきということが追加されております。そのため、内部統制の運用状況についてもモニタリングをする体制を構築することが必要となっております。

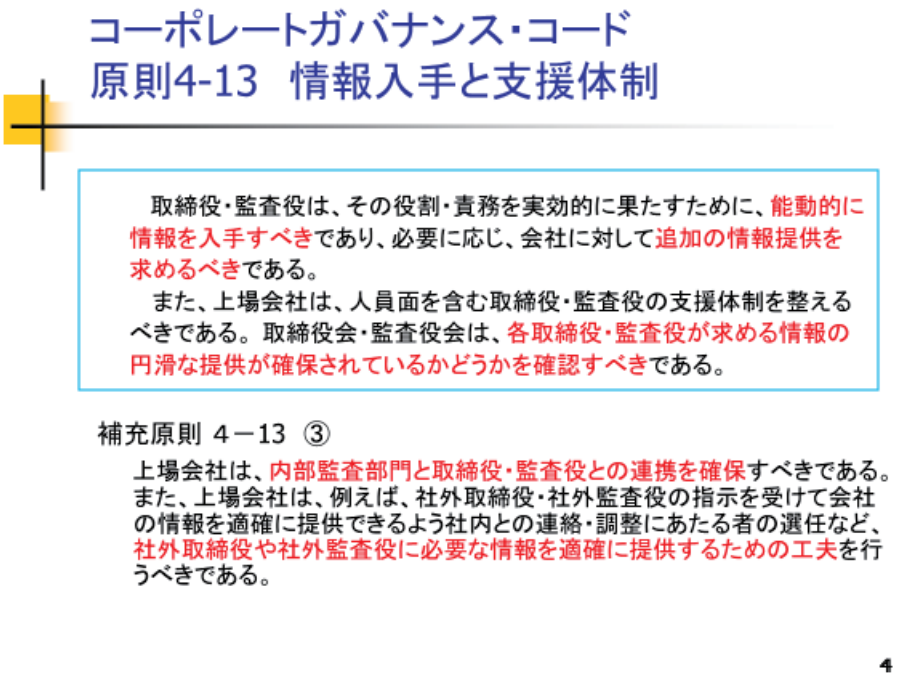
４）情報入手と支援体制（コーポレートガバナンス・コード）

この情報入手と支援体制につきましては、コーポレートガバナンス・コードでも、原則４－13 で定められているところでございます。①社外も含めて取締役・監査役は、その責務を実効的に果たすために、能動的に情報を入手すべきであるということ、そして、②必要に応じ、会社に対して追加の情報提供を求めるべきというふうに定められております。そして、③上場会社は、取締役・監査役の支援体制を整えるべきであり、④取締役会・監査役会は、各取締役・監査役が求める情報の円滑な提供が確保されているかというところを確認すべきであるということで、これを満たすためには、こういう体制をきちっととらなければいけないということになっております。

補充原則４－13 のほうでは、上場会社は、内部監査部門と取締役・監査役との連携を確保すべきというところでございまして、最後の行にありますとおり、特に、社外取締役や社外監査役に必要な情報を適確に提供するための工夫を行うべきというふうにいわれてお

ります。

このように、会社法ですとかコーポレートガバナンス・コードでも、情報の入手とか支援体制、情報伝達体制については、非常に重要視されているというふうに位置づけられていると思っております。



５）全社的リスクマネジメントの課題

（問題の背景）

それでは、私の実務経験も踏まえまして、全社的リスクマネジメントの課題と思われることについて、幾つかコメントしていきたいと思います。

問題の背景といたしまして、まず、環境、社会規範の変化によるコンプライアンス・リスクの増大というのが挙げられると思います。ご案内のとおり、独禁法・下請法リスク、労務リスク、情報管理リスクというのは非常に高まっておりまして、特に今、働き方改革といわれている中で、労務リスクにつきましては、本当に全社的なリスクマネジメントの大きな課題になっているところだろうというふうに思われます。

そして、先ほどグループガバナンスの紹介をさせていただきましたけれども、子会社で生じた不祥事による業績や社会的信用への影響というのも高まるばかりで、グローバル経営の中で、海外子会社における会計不正、減損リスクというのも増大しているところでございます。それと、先ほど根本様からもお話がありました品質不正問題についても社会的に注目されているところでございます。

（行うべき事項）

このような、環境、社会規範の変化に対応して、各企業さまはリスクマネジメントの強化に取り組んでおられるところですが、これについては、業種によるリスクの種類や大き

さの問題ですとか、それと各企業の規模ですとか、そのような各企業の実情に応じたリスク管理体制、コンプライアンス体制というのをしっかり議論して、その企業さんに応じた形で魂を入れていく必要があるのかなというふうに考えております。特に情報管理体制につきましては、適切な情報伝達体制がなければ正しい情報が上がってこず、適切な対応もとれないため、非常に重要なところだと思っております。

また、企業集団としてのリスクマネジメント、先ほど会社法の改正に触れさせていただきましたが、ますますこの重要性も高まっており、海外子会社まで含めたグループとしてのリスク管理体制の構築が求められているところでございます。

そして、リスク管理部門ですが、リスクがこれだけ注目されて社会的影響も大きいことから、リスク管理部門の組織体制について、現状で足りているのかというところをしっかり確認して、必要な整備をしていく必要があると思っております。

それから、先ほどお話にございました、リスクが増大し、変化しているというところで、未知のリスク、変化するリスクというところも見た、将来を見据えたリスク管理というのが求められるんだろうというふうに認識しております。

６）全社的リスクマネジメントの強化

そこで、全社的リスクマネジメントの強化のために何が重要かというところで、後ほど詳しいお話もさせていただくかと思うのですが、まず１つには、根本様もおっしゃいましたとおり、経営者の姿勢や倫理観が組織に浸透しているかというところが大きなポイントだと思います。

そして、先ほど来申し上げております、リスク情報の伝達、共有というところで、社内で円滑なコミュニケーションがとれているのか、風通しのよい職場環境になっているのかというところ。

それから、やはり内部通報制度の体制を利用しやすく、また利用した方が不利益を被ることなく、素朴に現場で起こっていることを相談できるような内部通報制度の体制整備も必要になっております。これについては、コーポレートガバナンス・コードでも「取締役会がこうした体制整備を実現する責務を負うとともに、その運用状況を監督すべきである。」と定められており、体制はもう整っている会社さんが多いと思いますので、その運用状況を社外取締役が監督していく必要があるのかなというふうに思っております。

７）社外取締役・監査役によるモニタリング

それでは、具体的に社外取締役や監査役がどういうモニタリングをしていくのかといいますと、まずは、経営トップの意識について、取締役会や各種会議への出席とか、代表取締役との意見交換というような機会を通じて、経営者の意識をしっかり確認していくということが極めて重要だと感じております。

それから、内部統制や全社的リスクマネジメントが全社的に構築、運用されているかと

いうところで、①リスク管理部門などからきちっとヒアリングの機会を設けるとか、あと、②内部監査部門との情報共有を通して、先ほど申し上げました内部通報制度の運用状況のモニタリング、特に内部監査で上がってきたり、内部通報で上がってきた問題点について、改善状況をしっかり確認していく必要があると思っております。

そして、カルチャーの問題でいいますと、従業員の方々とか取引先にアンケート調査をなさっている会社さんも多いと思います。そういう調査結果をしっかり取締役会が受け止めて、モニタリングをしていくことができるかというのも、カルチャーの面では非常に重要だと思っております。

以上が、雑ぱくではございますが、私からのご報告になります。ご清聴ありがとうございました。

吉野：ありがとうございました。それでは最後に、橋本先生、お願いいたします。

橋本：特に付け足すことはないと思いますけども、①やはり取締役会がどういうふうに機能するかというのが、ERM に非常に重要だということ、②取締役会がカルチャーをどう位置づけるか、そしてステークホルダーの意向を反映した形で、カルチャーを取締役会が経営者にあるいは、関連する会議体を通して社内に、どういうふうに浸透させていくかということが重要かと思います。そんなところです。

３．議論の前提について

吉野：どうもありがとうございました。では、続きまして、これからパネルディスカッションを開始したいと思います。先ほど申し上げましたとおり、今回のテーマは、「社外取締役の視点から見た改訂版 COSO-ERM の我が国企業での活用の方向性」ということでございます。議論の前段として、１つ目に社外取締役が ERM を監督するために必要なこと、２つ目にどこまでわが国企業で改訂版の ERM を取り入れるべきかという、この２点について議論をしたいと思います。

論点１：社外取締役が ERM を監督するために必要なこと

最初に、社外取締役の ERM に対する監督は、現状を見て、将来の中長期的な価値創造を実現する体制になっているかどうかを見るものだと思われます。最初に、社外取締役が ERM を監督するためにどのようなことが最も必要なのかについて、まず皆さんのご意見をお聞きしたいと思います。最初に根本さん、お願いします。

根本：情報と組織の２つの面があると思います。情報に関しては、リスク情報がリスク管理部門などに早く確実に伝わってくることが大切だと思います。営業現場で、「これはここで解決する問題です」みたいに、現場で終わってしまい、リスク管理部門などに報告されていないことがあるように思います。社内内部で、情報伝達が速く行われており、リスク管理部門が、それを責めないで聞いて、サポートしていくというような良好な関係があるかというのが関心があるところです。

あと、組織についてですが、鈴木先生もおっしゃっていましたが社外取締役というのは、月に１日しかいなくて、正直な話をすると、会社の非常に細かいことは分からないんです。そうすると、リスク管理部門とか内部監査の方々を信頼していくしかないんですね。そこの方がしっかりした方で、トップにも物言えるぐらいなのか、そういうところは気にしています。

そのために、いろんな質問を投げかけてみて、あるいは何かをこちらでお願いして、リスクについてどういう意識を持っていらっしゃるのかを判断します。仮に不安の材料になると組織のあり方について、経営トップに進言をしなくてはいけない場合もあると思っています。

吉野：ありがとうございます。鈴木先生、お願いします。

鈴木：私も今、根本様がおっしゃったとおり、リスク情報が適時に早く社外取締役に報告されるというところが不可欠だと思っております。先ほど申し上げましたグループガバナンスの観点から、子会社で発生した不祥事についても早くグループ全体で情報共有できる体制を作っていただかないと、なかなか対応が難しくなる。早めの対応ができれば被害も小さくなるし、逆に後手、後手に回ってしまうと、レピュテーションリスクも大きくなってしまいます。そのため、子会社で起こっていることも含めて、早くグループ全体でリスクを情報を共有し、連携しながら、自発的な対応をしていくということが大事なのかなというふうに思っております。

吉野：ありがとうございます。では、橋本先生、お願いします。

橋本：今話のあった情報伝達は、テクノロジーの進展でいろんな手段があるので、常に適時、タイムリーに情報が共有されるような、そういう経路をつくっておくことが重要だと思います。特に日本の場合には、悪い情報がなかなか上に伝わらないとか、知らなかったとか、そういうのが多いですから、そういうことがないような体制にしないといけないと思います。

それとやっぱり事後対応ですね。最初のリスク対応を間違うと、より大きなことになってしまい、レピュテーションにも関わってきますので、確実な事後対応を行うことが重要

だと思います。

根本：今思い出したのが財務省の対応ですけれども、ああいう問題が明るみになったら、まず調査をしますというスタンスですよね。やっぱりあれはまずいということですか。

橋本：そうですね。財務省とか、あるいは大学もそうでしたけど、何も出てこないという、対応を一切しないという、いろんな対応の仕方がありますけど、やはりこれは ERM からいうと、リスクマネージの仕方が間違っているのではないかと思いました。

論点２：リスク情報の社外取締役への報告の現状の課題と解決に必要なこと

吉野：ありがとうございました。鈴木先生、今の点で何かございますか。よろしいですか。皆さん共通しているのが、やっぱり社外取締役にとってはリスク情報の伝達が非常に重要であるということかと思います。逆に、リスク情報の伝達というのは、私が思うに、わが国企業のリスクマネジメントの一番脆弱なところだと思っています。

そこで次に、お話がありましたとおり、社外取締役は必ずしも社内の事情、情報に通じているわけではなく、報告されたリスク情報に基づいて判断するため、必要なレベルのリスク情報が適時に報告されるということが社外取締役が ERM を監督するために欠かせないと考えられます。そこで、２つ目の論点といたしまして、リスク情報の社外取締役への報告の現状について、課題と考えておられること、ならびに、その解決に必要と考えておられることについて、ご意見をお聞きしたいと思います。最初に鈴木先生、お願いします。

鈴木：まず、現場から経営に報告されないリスク情報が存在するんじゃないかということが大きな課題だと思います。特に経営が現場とちょっと乖離しているというようなことが、今起こっている不祥事の多くの原因としてあるかというふうに思います。

現場から経営に報告されないという場合には、いろんな要因があると思うのですが、第一に、現場がリスク感覚に弱いというところが挙げられると思います。先ほど新しいフレームワークで、リスクに気付くカルチャーというお話がございましたが、これを醸成することが必要だと思います。従業員の方への教育、研修を通じて、リスクに気付くカルチャーというのをしっかり醸成していくことが必要なのかなと思います。

第二に、リスクに気付いていても、やはり上には言えないというような、風通しの悪さといいますか、そういうところで情報がなかなか上がってこないというところがあると思います。この場合も、カルチャーの改善を地道にやっていくしかないかと思います。

最後に、調査などをなさっていて、その報告が遅れるようなケースです。まずは第一報を上げていただいて、詳しい調査は、その後で構わないということとし、まずおかしいと思ったら、報告、相談するという、そういうカルチャーづくりというのが課題かと思って

おります。

吉野：ありがとうございます。続きまして、根本さん、お願いします。

根本：第一に、鈴木先生がおっしゃった、現場のリスクに気付くカルチャーの重要性はそのとおりだと思います。例えば、スルガ銀行のシェアハウスへの融資の問題では、ともかく営業目標を達成するので貸さなきゃと、お客さんの預金口座の預金情報を改ざんして収支表を作って融資して、目標を達成するということが行われていました。そういうことをやっても、現場の方から、これは問題だという声があまり上がらなかったと聞いています。金融庁への通報とか、若干退職した人はあったようですが、大きな声になっていなかったと調査報告書に書いてありました。

これほど大きな問題ではなくても、「これはおかしい、このままやってしまうと、社会的に問題が起きるんじゃないのか」など、そういう感覚を持つことは重要だと思います。そのためには、研修も必要ですし、また現場の管理職の方がいろいろと対話をすることも重要だと思います。ぜひやっていただきたいと思います。

第二に、もう少し可視化とか、定量的な情報とか、そういうのがあるといいと思います。金融機関は統合的なリスク指標があると申し上げましたが、事業会社、特にいろんな事業部門がある場合には難しいことですが、工夫の余地もあると思います。社外の目から見ると、KPI などの指標、時系列的な変化を追えるものがあると非常にいいと思います。

これは、社外取締役だけではなく、経営トップにとっても必要かと思います。

第三に、教育です。リスク管理は本当に複雑で、年々進歩していて、キャッチアップするのも大変です。ある会社では、リスクについての勉強会をしてくださっており、これは助かっております。リスク管理部署の人だけではなく、リスクに関係しない他の取締役の方にも、そういう研修が必要なのかなと思います。

吉野：ありがとうございます。では最後に、橋本先生、お願いします。

橋本：いろんなところからリスクが生じます。成功している事業からもリスクが生じます。例えば、あまりに注文が多く来てしまったため応じられなくて、かえって評判を落とすなど、いろんなところにリスクがあります。やはり、リスク情報の円滑な伝達にはカルチャーが重要ですね。例えば、現場に大きなプレッシャーがかかっている場合には、そういう情報を社内で共有するカルチャーがあれば、わりとリスク情報は円滑に流れるんじゃないかと思います。

吉野：ありがとうございます。このリスク情報の伝達は非常に重要だと思いまして、私もちょっと簡単に申し上げますと、リスク情報の伝達には２段階あり、第１段階が現場から

そのリスクを主管する本社統括部門への伝達ですが、だいたいそこが詰まっている場合が多い。

それを防ぐためには、①リスク情報の伝達の意味や重要性をひたすら言い続けて、文化になるまで昇華させること。②悪い情報を受けたときに嫌な顔をしない、あるいは責任を問わないで一緒に解決するスタンスをとること、また、過度の質問、更問をしないこと。③現場の迅速な対応と迅速な報告を両立させること。この３つが必要だと考えています。

リスク情報の伝達の第２段階がリスクを主管する本社統括部門から経営者への伝達です。現場からの報告を受けた本社統括部門は、リスク事案への対応を統括部門で判断すればよいのか、それとも経営者の判断を仰ぐべきかを判断する必要があります。しかし、事案が社会に及ぼす影響や社会からどのように受け取られるかなど、事案がもたらす影響の重大さは、当事者である主管部門だけでは必ずしも的確に判断できない場合があります。そのため、リスク管理部門は、リスクに関係する主要な本社スタッフ部門、すなわち広報部門（マスコミ対応）、法務部門（法的対応）、総務部門（行政対応）、経営企画部門（経営としての対応）の部長もしくはマネジャーによる対策会議を開催して、社内で情報を共有すると共に、事案を多様な視点で検討して、主管部門に対応をアドバイスするという体制が必要だと思っております。

論点３：改訂版 COSO-ERM の諸原則をどこまで取り入れるべきか

では、３つ目の論点に入っていきたいと思います。わが国では、この改訂版の ERM が示すような形で ERM を行っている会社は、金融機関はともかくとして、事業会社ではそれほど多くないのではないかと思いわれます。多くの事業会社では、COSO-ERM のすべてを取り入れているわけではなくて、一部を取り入れているというのが現状だと思います。このようなわが国の事業会社の現状を踏まえて、改訂版 COSO-ERM の諸原則をどこまで取り入れるべきかということについて、皆さんのご意見をお願いしたいと思います。最初は、根本さんよろしくお願いします。

根本：これは非常に難しい話で、私が担当だったら、これを全部やるというのは難しいと思いますので、たぶん重要なことからまず取り組むということになると思います。どこの会社でも、何か重要な問題とか、懸念点がおありだと思いますが、その根本原因は何なのか、企業カルチャーの問題なのか、あるいは、その他の問題なのか、そこに対してどう対応していくのかというところから始められたらいいのかと思います。

あと、現場も含めての全社的なリスクに対する防衛線というか、会社全体にリスクマネジメントの浸透を図るということが大事だと思います。先のグローバル金融危機で、その重要性がフォーカスされました。しかし日本は、この危機の発生源ではなかったので、私が見ている範囲では、欧米の金融機関が定性面を含めて、リスクマネジメントを改善して

きたのに比べると、日本が手薄になっているという印象があります。そこもぜひ取り組んでいただきたいと思います。

吉野：ありがとうございます。どこの会社でも同じようなことがいえるのではないかと思えますが、それでは鈴木先生、お願いします。

鈴木：私も、いずれも大変有用で、全部取り入れられると理想なのでしょうけれども、やはりそれぞれの企業さんの業態だったり、規模だったり、経営戦略上の大きなリスクだったりというところを踏まえて、自社で役に立つような ERM を作っていただくというのが一番いいんじゃないかと思います。また、取締役会レベルで、社外取締役も含めて、この ERM の在り方を戦略とともに議論するようなことも必要なのではないか思っております。

吉野：ありがとうございます。では、橋本先生、お願いします。

橋本：今回の改訂版 ERM フレームワークは、ベストプラクティスを示した水準が高いものので、まず 20 の原則を見てみて、評価ツールとして、自社の今の現状はどの辺なのかというのを見て、それでいいヒントがあったらやってみるとか、そういうトライアンドエラーみたいなのを最初に試行錯誤的にやってみて、その後に全社的に取り組んでいくのがよいと思います。単にリスク管理部門だけに任せているんじゃなくて、これはやっぱり取締役会とか経営者とか、全員参加の下にやっていくということが重要かなと思います。

吉野：根本さん、一言お願いします。

根本：ひとつ申し上げたいのは、リスク選好と攻めのリスク管理についてです。私は以前、こういったパネルを自分で主催して、オリックスの宮内チェアマンに来ていただいたのですが、その中で印象に残ったコメントがありました。宮内さんは「日本の企業は、コーポレートガバナンスを強化し過ぎると、全くリスクを取らなくなってしまう。日本の経営者は、イノベーターではなくてコストカッターなので、コーポレートガバナンスというブレーキばかり強化すると企業は成長しなくなってしまう。」とおっしゃっていました。

リスクをとらなければ、リターンもないわけなので、バランスをとることが重要かと思います。リスク選好を明確にすると、例えば新しい分野に進出するときにも、社外取締役として判断しやすくなります。よく分からないことがあると「この資産を持つとこういうリスクもありますね、こういうリスクもありますよ。」などと、不毛な議論を重ねてしまうことがあります。リスク選好を決めておけば、「これはリスク選好フレームワークからはこうなんだ、これぐらいの影響であり、リスクを取っても収益の変動幅の範囲に収まる」とか、そういうより建設的な議論ができると思います。

吉野：ありがとうございました。どの会社もある程度自社なりの ERM は構築していること、また、橋本先生が今おっしゃった通り改訂版 ERM は水準が高いことから、改訂版 ERM フレームワークを自社の現在の ERM と比較して足りないところを補うという使い方がいいのではないかと思います。

４．我が国企業での活用の方向性

論点４：戦略およびパフォーマンスとの統合を強調している背景と ERM に対する取締役会の監督の在り方

吉野（続き）：では、続きまして、次のテーマに入りたいと思います。COSO-ERM の標題が「戦略およびパフォーマンスとの統合」という名前になっております。それについて、最初に橋本先生にお願いしたいのですが、改訂版の COSO-ERM で、戦略およびパフォーマンスとの統合を強く強調している背景と、また、改訂版に記載されている ERM に対する取締役会の監督の在り方について、かいつまんでご説明いただきたいと思います。

橋本：この改訂版フレームワークの最初の序の部分に、非常に印象的な文章があります。すなわち、「組織全体にわたって全社的リスクマネジメントの実務を統合していくことにより、ガバナンス、戦略および目標の設定、ならびに日々の業務、それぞれの分野における意思決定が改善されていくことになる。戦略と事業目標をリスクにより密接に結び付けることによって、パフォーマンスの向上につながる」というくだりです。

全社的リスクマネジメントを統合する上で必要な努力を積み重ねていくことにより、事業体の価値の創造、維持、さらにその実現に向けた明確な道筋が見えてくる。これはほとんど ERM の改訂版の心だと書かれているのですが、全社的リスクマネジメントを組織の価値の重要な要素というふうに考えるべきだというのが１つのメッセージであります。

実際には、「統合」ということが重要でありまして、意思決定はリスクの検討から切り離せないというメッセージが伝わってくるものであります。こういった全社的リスクマネジメントをビジネス活動とかプロセスに統合することで、意思決定を改善し、パフォーマンスの拡大を推進する上でのより重要な情報につながっていく。価値をどのように創造し実現するかというのは組織ごとに異なるわけですけども、経営者と取締役会が、事業モデル、ビジネスモデルという観点から価値を理解することが重要であるというのが、統合の一つのポイントではないかと思います。

その上で、①どんな形の組織構造をとるのか、あるいは取締役会の構成をどのようにするのか、組織のカルチャーをどうやってモニターするのかを考えていくことが重要です。

また、②取締役会の全体として維持すべき監督とか助言の責任など他の委員会とか、他の取締役に移譲できないようなそういうコアとなる部分を定めたり、最終的には組織のリスクカルチャーを定めたりする上で、取締役会がどういう役割を果たすべきか、そういうことを考えていくことが重要です。そして、③そういうコミュニケーションを社内でとっていくために、どうやったらいいかというのも重要で、その際には、やはりどういう頻度で、どんな情報を、どんな質の情報を伝達するのかということを考えることが重要かと思います。

論点５：社外取締役は ERM の監督をどのように行うべきか

吉野：どうもありがとうございました。今の橋本先生のお話を踏まえまして、鈴木先生と根本さんにお聞きしたいと思います。これは今回の本題ですけども、わが国企業が改訂版 ERM フレームワークを活用することに対して、社外取締役は ERM の監督をどのように行うべきかということについて、鈴木先生と根本さんから話を伺いたいと思います。最初に、鈴木先生、お願いします。

鈴木：リスクマネジメントがある程度浸透していて、取締役会で戦略についてリスク情報に基づいて議論を行ったり、M&A の議案などについて多方面からの様々なリスク情報が上がってきて、それらを踏まえて議論を行っている企業さんも多いと思います。今回この新しいフレームワークの中で、私がすごく、これはなかなか難しいけれども重要だなと思いましたのが、「レビューと修正」というところで、戦略を議論したり、M&A の実行を議論することにはすごく熱心でも、なかなかその後の検証が行われていないというところがあると思います。

M&A 実行後の PMI（Post Merger Integration： M&A 成立後の統合プロセス）の状況については、皆さん結構、意識的に聞かれるようになっているとは思います。しかし、M&A に限らず、１回作った戦略について、その後の事業環境の変化により策定した当時は分からなかった新しいリスクが出てきていないかとか、変化したリスクに対してきちっと対応できているかというところをしっかりレビューすることが取締役会として重要ではないかと思います。その時に、リスクとパフォーマンスの「レビューと修正」いう改訂版フレームワーク新フレームワークの構成要素に関する原則が活用できるのではないかと強く感じたところでございます。

吉野：どうもありがとうございました。続きまして、根本さん、お願いします。

根本：わが国の金融機関や保険会社ですが、私の知っている範囲になりますが、海外の大手と比べると、リスク管理について戦略への活かされ方が不十分だと思います。鈴木先生

がおっしゃったように、㋐リスクの観点からみた M&A や新規事業、事業再編の評価、そして、㋑それが事後的にどうなっているのか、㋒当初狙ったようなリスク・リターンが実現されたのか、事業ポートフォリオの検証について改訂版 ERM をぜひ使っていただきたいと思います。

日本の企業にありがちなのは、戦略の失敗を戦術でカバーしようとする。目先のことを一生懸命やるのですが、そもそも戦略の方向性が違っていないかなど、大きなところに目が向けられていないことがあるかと思います。社外取締役が存在する意義といえば、そういうところを指摘できることだと思うので、それに資するような情報の提供があればいいと思います。

吉野：ありがとうございます。今、根本さんと鈴木先生のお二方とも、戦略の事後の検証が不十分であるということを共通しておっしゃっていました。それに対して、根本さんから、そういうことについて社外取締役が指摘すべきだというようなお話がございました。これについて、事後検証に対する社外取締役の指摘、助言、問題提起、これについてもう少し議論を深めてみたいと思います。

鈴木先生、その辺はいかがでしょうか。社内だと、なかなか事後検証するといっても、前につくった会長だとか社長など前任の方の顔もあってなかなか言えませんが、社外の方だと比較的言いやすいと思うんですよね。そういう面で、事後検証をきちんとやらせる、事後検証を進めていくことについて、何かご意見があればお願いしたいと思います。

鈴木：そうですね。やっぱり社外は言いやすいというところがあるので、「あの案件は、その後、どうなりましたか」というような質問で、気になっている案件についてその後の報告をお願いすることは、権限で十分にできるのではないかと思っております。特に重要な案件や実行後の変化が大きい案件であれば、取締役会でしっかりした報告を求めるということも、社外取締役として積極的に行っていくことが必要かなというふうに私も思います。

吉野：ありがとうございます。根本さん、何か付け加えることがございましたら。

根本：事後検証も、誰かに責任を取らせるというものではなく、そこからもっと前向きなものに発展していかなければいけないと思います。

あと、リスクカルチャーについては、失敗の経験やそこから得た教訓を組織内で共有することが大切です。失敗したことを、なんとなくうやむやにしてしまわないで、失敗の経験や教訓の共有はぜひやっていくべきだと思います

私が今社外取締役をやっている中部電力では、原発に行くと、いろいろな事故の経歴とか、その原因や対応などが展示されています。これは非常にいいですねとメディアの方も言ったらしいのですが、そういう振り返りから、いろいろな改善がなされることが望まし

いと思います。

論点６：社外取締役による ERM の監督の在り方

吉野：ありがとうございます。橋本先生、最後に、社外取締役による ERM の監督のあり方についてご意見をお願いします。

橋本：私は某監査法人の社外の委員をやっていますが、やはりステークホルダーといいますか、企業を取り巻く人たちの目から見た意見を社外役員が伝えることが大切だと思います。会社の内部にいたのではなかなか聞こえてこない外の声を届けることによって、いろんな角度からリスクを見ていくという、そういう新しい目といいますか、フレッシュ・アイを提供することが、社外の役員に求められると思います。

吉野：ありがとうございます。私は、社外取締役が機能するためには、社外取締役にリスク情報を提供する内部監査部門やリスク管理部門の充実というのが重要ではないかと考えています。

先ほど根本さんから、金融危機で破綻したリーマン・ブラザーズと生き延びたゴールドマン・サックスの差として、このリスク管理部門の位置づけが、リーマンは低くて、ゴールドマンは高かったという話がありました。内部監査部門やリスク管理部門といったリスク関連部門の充実ということについて、何かお話があれば伺いたいのですが。

根本：本当にその点が重要で、社外取締役がガバナンスのキーというよりは、やっぱり会社内部で整備された各種の仕組みや規定・規則、相互牽制というのが本当のガバナンスのキーであって、社外というのは、それがワークしているかを見るというのが私の考え方なんです。責任転嫁するわけではないですが、一つ一つの案件を見ていくなんていうのは無理なものですから。

最近の不祥事などから、そこを強化する動きがあるのはよい点です。私が関わっている企業ですが、トップが以前、内部監査やリスク管理を経験され、それらの部門の重要性も分かっていて、共通の言葉も分かっている。それはいいことだと思います。ただ、金融機関は国際的なプレッシャーもあって、改善が進みましたが、事業会社においては、人員の面などが足りていない、そういう面はあるかと思います。

吉野：鈴木先生、お願いします。

鈴木：社外の目からみると、管理部門や内部監査部門の人員ちょっと足りないんじゃないかなと感じる時があり、そのような時には、率直に、もうちょっと人員をリスクに見合っ

たものにした方がいいのではないかと提言することも必要だと思っています。

あと、やっぱり内部監査部門とのコミュニケーションがすごく大事だと思っております。せっかく内部監査部門で問題を発見していただき、原因分析もなされて、改善策まで示されても、その改善策が徹底できなくて同じような事案が起こってしまうというようなケースも見受けられます。やはり、しっかり改善できたかというところまでを含めて確認できる実効性のある内部監査体制を、社外として求めていくのも大事なことかなというふうに感じております。

吉野：どうもありがとうございました。それでは、橋本先生、今の根本さんと鈴木先生のご意見を踏まえて、ERM に対する監督の在り方について、何かご意見があれば、お願いします。

橋本：最近はいろいろ新しいリスクも生じていますので、そういう新たな視点に立って、もう一度、会社が有効にリスクを識別、評価できているかどうか、これをもう一度検討してみることが必要だと思います。

また、不正とか不祥事というのは 10 年スパンで起きると言われていますが、日本もカネボウ、ライブドアの事件から、さらにオリンパス、東芝の事件と様々な事件が起きています。会社が常に、緊張感を持って、そういった経験とか、これまでのいろんな事案を踏まえて、リスクマネジメントの強化に取り組んでいるかを監督していただきたいと思います。

５．最後に一言

吉野：どうもありがとうございました。議論も尽きないのですが、そろそろ時間になりましたので、今回の議論を振り返って、最後に一言ずつ、お話をお願いしたいと思います。最初に鈴木先生、お願いします。

鈴木：本日は新しい ERM のフレームワークのお話をお伺いして、社外の目から、しっかりと必要なリスク情報を把握して、いろんな種類のリスクに向けて、多角的なリスク管理、パフォーマンスというのを意識していただくような働きかけをしていきたいなというふうに感じました。今日あまりお話には出なかったんですけども、特にやっぱり ESG の観点は重要だと思いますので、社外の新しい目からということで尽力していきたいなと思っております。

吉野：根本さん、一言お願いします。

根本：私は、吉野さんが以前から高い意識を持たれて、リスク管理業務や内部監査業務に取り組み、経営に提言をされていらっしゃるので、吉野さんのコメントも是非聞きたいと思います。

あとは、リスク情報の伝達については、トップが、「情報をより早く上げることを自分は希望しているし、やらない人は駄目なんだ」ということを強くおっしゃっていただきたい。また、リスク情報のための仕組みや組織が実質的に機能するように、魂を入れていただきたい。

社外取締役としては、トップの方に働きかけると共に、トップの選任に際しても重要な資質として考える、そのようにしていきたいと思います。

吉野：ありがとうございます。最後に、橋本先生、一言お願いします。

橋本：吉野さんが最後、一言くださいよ。

吉野：じゃあ私のほうで、根本さんからのご質問で、どうやってリスク管理部門や内部監査部門が経営トップにアピールしていくかということにつきましては、どうもやはり日本は、例えば ERM を作るとか、あるいは BCP を作るとか、あるいは情報伝達のルールとか、エスカレーションルールを作るとか、経営者がその時その時に気にすることってあるんですね。リスク管理について。それについて、パッチを当てて、経営者のニーズに応えていく、それを実現すという実現力が経営にアピールする一番大きな要因ではないかと思います。逆に言えば、経営者の役に立つということが、実はリスク管理部門でも、内部監査部門でも、私は少なくともわが国の一般的な事業会社では、一番求められることではないかと考えています。

また、内部監査部門につきましては、金融機関ですと、当局からの監督の一環として内部監査部門が位置づけられているため、ガバナンス上、一定の枠組みが実質的にあるわけですね。ところが、わが国の事業会社の場合、そういう枠組みがございませんので、どうしても経営者のニーズによって、重要視されたり重要視されなかったりということが出てきます。例えば、極端なことを言うと、精鋭が来るのか、姥捨山行きみたいな人が来るのか、あるいは、40 歳前半の人も半分ぐらいいるのか、平均年齢が 50 歳後半なのかとか。経営者のニーズが体制に大きく影響することがあります。

そのため、社外取締役の方が、リスク管理部門や内部監査部門の重要性を取締役会で積極的にご発言いただく、あるいはご助言いただくということが、おそらくわが国の事業会社にとっては重要なのかなと思います。

今回のまとめですが、私としては、リスク管理部門、内部監査部門、社内の情報伝達体制、およびリスク管理体制について、社外取締役の方が、社外の客観的な目で、こういう

部門や体制の強化に経営者が取り組んでいることを監督することが求められていると思います。経営者にとって、一番怖いのは、独立した社外取締役ではないかと思われます。この人にだけは言われたくないっていうのがあると思います。

特に女性の社外取締役ですと、厳しいことを言っても柔らかく聞こえるため、後に引きにくく、皆がそうかなと思うというところがあるのではないかと思うんですよ。そういった面で、社外取締役として適任な方は、権威のある財界の大御所的な方や名経営者の次には、企業経営のご経験をお持ちの女性の方ではないかと私は個人的に思っております。

社外取締役の方には、こういう部門や体制の強化について、社外の目から経営者に対して強化するよう働きかけていただきたいということで、時間になりましたので、これで今回のパネルを終了したいと思います。どうもありがとうございました。

以　上