2005 年 2 月 28 日

日本内部監査協会
CIA フォーラム　ERM 研究会

ERM についてのよくある質問集（FAQ）

当研究会では全社的リスクマネジメント（ERM）に関してよくある質問集（FAQ）を作成いたしました。

海外では ERM についてはここ数年間様々な実験的取り組みがなされその結果が報告されてきました。そしてこれらを集大成する形で 2004 年 9 月には COSO の ERM フレームワーク編およびツール編が公表されました。ERM はいよいよ本格的運用段階を迎えているものといえます。

翻ってわが国でも ERM の重要性は非常に高まっています。

2004 年 6 月提出の有価証券報告書から本格的に開始したリスク情報開示は、グループ全体の視点で統一的にリスクを優先順位付けし開示するものとしないものとを合理的な基準で区分する ERM の仕組みが不可欠といえます。これにより仮に開示されないリスクが後から顕在化しても、開示時点でどのようなルールに基づいて開示リスクと非開示リスクを切り分けたかを合理的に説明でき、虚偽記載等と認定されるリスクを軽減できることになるからです。

2004 年度中に有価証券報告書の虚偽記載等についての民事責任を強化する証券取引法が施行され、2005 年に入って代表者の宣誓書／確認書の導入や非財務情報の虚偽記載等が上場廃止原因に含める等の内容で東京証券取引所規則が改定されました。これらは 2005 年 6 月の有価証券報告書におけるリスク情報作成には前年度以上に ERM の必要性が高まっていると考えられます。

ところが残念ながらわが国では未だ ERM が十分に認知されているとはいえないのが実情です。そこで当研究会では、ERM に関する理解を促進するため、まずは簡易に疑問点に答える形式の FAQ に着目し、その作成を目指して作業を進めてまいりました。その結果が本日公表する運びとなったこの「ERM についてのよくある質問集」です。

コーポレート・ガバナンスおよびリスクマネジメントの有効性評価を責務とする内部監査部門の実務家はもちろん、リスクマネジメント部門の方、ERM 推進の担当者、ERM についての監督責任を負う取締役、あるいは監査役まで、社内で ERM に何らかのかかわりを持ち、様々な困難に遭遇されている方に対して、この FAQ が多少なりともお役に立てれば幸いです。

本報告書についてご意見、ご批判、コメント等ありましたら、座長の眞田（sanada@zac.att.ne.jp）宛に E メールでご連絡いただきますよう、お願いいたします。

なお、富士ゼロックス株式会社　吉田邦雄様他何人かの方には、わが国における先進的 ERM 取り組み事例についての情報をご提供いただき、本研究会は本報告書取りまとめの過程で貴重な示唆を得ることができました。ご協力いただいた皆様方に、この場を借りて御礼を申し上げます。

以上

日本内部監査協会
CIA フォーラム ERM 研究会

座長：　眞田　光昭　（日本内部監査協会 理事（国際担当）、公認内部監査人）
メンバー：　樫原　　忠　（キリンビール株式会社、公認内部監査人）
神田　　浩　（株式会社日本総合研究所、公認内部監査人）
小菅　章裕　（株式会社プロティビティ ジャパン、公認内部監査人）
常橋　直弓　（株式会社ベネッセコーポレーション、公認内部監査人）
村田　　一　（オリックス株式会社、公認内部監査人）
吉野　太郎　（東京ガス株式会社、公認内部監査人）

ERM についてのよくある質問集（FAQ）

CIA フォーラム ERM 研究会

目次

ERM についてのよくある質問集（FAQ）

Ⅰ．そもそも編

１．全般的事項

質問１．リスクは発生の都度対応すれば十分

重要なリスクは、担当部門が明確になっており、本来業務としてしかるべき対応策が打たれている（もしくは打たれつつある）。既にリスクへの対応策が本来業務として行われているのだから、リスクは**発生の都度対応すれば十分**ではないか。費用対効果の観点から、あえて**労力をかけて**リスクマネジメントを**行う必要**があるのか。

＜回答＞

近年、企業を取り巻く事業環境が急激かつ大きく変化しており、その結果、リスクは巨大化すると共に複雑化している。発生の都度の対応では、次第に巨大化し、複雑化しているリスクへの対応が次第に困難になってきている。

このような巨大化し、複雑化している近年のリスクへ対応するためには、リスクを把握･評価し、対応策を策定し、対応策が確実かつ効果的に実行されるようにコントロールする一連のプロセスを事前に策定しておき、リスクに関する情報を適切にコミュニケーションし、それらが適切に遂行されているかをモニターするリスクマネジメントの導入が必要になってきている。

さらに、リスクマネジメントは、**コーポレート・ガバナンスを強化**する有効な手段であり、さらには**企業価値の持続的な向上**へと結びつくものである。

質問２．リスクマネジメントと内部統制との関係

リスクマネジメントと内部統制との関係はどのようなものなのか。

＜回答＞

リスクマネジメントの手法には、リスクの回避、移転、保有、縮減の４つがあり、リスクを受容可能なレベルまで縮減させる手法が内部統制である。内部統制は、リスクを受容可能なレベルまで縮減させるリスクマネジメントの不可欠な手法であり、リスクマネジメントは内部統制を包含する。

ＥＲＭにおいても、内部統制はＥＲＭの不可欠な部分である。ＥＲＭのフレームワークは、内部統制を包含し、マネジメントにとって、従来のリスクマネジメントより一層強固な概念と道具になる。「内部統制の統合的枠組み」全体が、ＣＯＳＯ－ＥＲＭのフレームワークに組み込まれている。

２．そもそも論

質問１－1．何の意味があるのか

リスクを組織的に洗い出してリストアップすること、つまり組織のリスクリストを作成することはかなり大変な作業であるが、各担当者は、担当している業務のリスクの大部分は把握し、管理していると思われる。
個々の担当者が担当する業務のリスクを把握しているのだから、労力をかけて組織的にリスクリストを作成することに何の意味があるのか。担当者が分かっているから不要ではないのか。

質問１－２．ニーズがないのになぜやるのか

今、リスクマネジメントをやらなければならないニーズは現実には感じられないのに、それでも始める必要があるのか。始めなければならないニーズや取っ掛かりがないのにこのような大掛かりなことを始めるのはなぜなのか。

＜回答＞

組織共通の目的に向かう企業活動を進める上では、目標を組織として共有した上で、その目標達成の不確定要素となるリスクを管理することが必要とされてくる。この際、まず始めに必要となることはリスク事象を特定し、組織として共通に把握することである。このような取組はこれまでは通常の業務遂行に於いて担当者が個人的に習得した知識・スキルやノウハウの中で業務の優先順位ごとに活動する中で管理を行なってきていると思われる。

しかし、現在その非効率さが無視できなくなっている。例えば

１． リスク情報開示を求める環境変化への対応
２． 担当者の異動・流出による業務のレベルの変動（雇用環境の変動）
３． 情報、経験蓄積の資産の雲散霧消
４． アウトソーシングの進展による管理外業務への依存度の高まり

など外部からの要求と現在企業が直面している状況は従来の取組では企業としての目標達成の安定性を確保するための管理していく上でのコストの急速な増加を避けられない状況となっている。

このような現実の中では組織的なリスクの洗い出しは、必ずしも非効率ではなく、むしろ組織としてのリスク管理能力の向上に繋がる情報資産蓄積の根源となる。リスクを管理し組織的な対応能力を高めるためには、業務に固有なリスクを洗出し、ステイトメントとして特定した上で、リストとして組織的に保有することが必要である。このリスト化により初めて個人の知識やノウハウが組織共通の言葉で理解されるようになる。通常、リスクの捉え方やその管理をする進め方には個人差がある。これを個人による業務処理能力の差ではなく組織としての認識に変えることで個人差による認識のギャップを低減し、理解を組織としてリスクを共有できるようになる。このため、組織的な活動として優先順位を明確にして管理していくことが可能となる。**リスク情報はこのようなプロ**

セスを通して具体的な対応策につなげることで初めて組織的な管理が可能となる。すなわち、企業として抱えているリスクへの対応策を事前に準備することができるようになる。このようなリスクマネジメントを通して経営者としては目標達成の確実性を高めることを合理的に保証する事が可能とすることができる。

質問２－１．全てのリスクを管理する必要性

事業運営とリスクとは裏腹の関係にあるので、リスクマネジメントとは事業運営そのものである。とすると、リスクマネジメントを行うとは、事業のトップからボトムまで、具体的には、経営判断のリスクから現場の仔細なリスクまで、全てのリスクをマネジメントすることになる。しかし、極めて多岐にわたり、軽重様々なリスクの集合体である会社の業務全部を、オーバーオールに洗い出して管理するなど、不可能だし、意味がないのではないか。

そもそも、業務プロセスリスクを含む全てのリスクを管理する必要性があるのか。（例えばコンプライアンスリスクのように、）現在の枠組みでは対応できないリスクに限定すべきではないか。

質問２－２．全社共通でリスク管理を行う必要性

全社共通でリスク管理を行う必要があるのか。各部門が所管しているリスクを責任を持って管理すればそれで十分ではないのか。つまり、重要なリスクについて、それを所管する部所がそれぞれの責任で管理する従来のやり方で十分なのではないか。

＜回答＞

組織共通の目的に向かう企業活動を進める上では、目標を組織として共有した上で、その目標達成の不確定要素となるリスクを管理することが必要とされる。

この組織的なリスク管理の推進の中では、事業のトップからボトムまで、具体的には、経営判断のリスクから現場の仔細なリスクまで、全てのリスクをマネジメントすることになる。この極めて多岐にわたり、軽重様々なリスクの集合はこれまでそのリスクを所管する部署がそれぞれの責任で管理することが行われてきているが、これを全社共通にてリスク管理行なうことで以下のことが解決される。

１．　全体をリスク管理するため、抜け漏れを防止できる。
２．　全体の中での優先順位付けが可能となり戦略性を持たせることができる。
３．　組織的に一元管理することによりリスク対応のレベルを合わせていくことが可能となる。
４．　継続的なリスク管理レベルの改善が図れるようになる。

この中でも特に重要なことは、これまで業務プロセスに埋め込まれて管理されてきたリスクについての一元管理がおこなわれることである。これによりリスク管理に継続性が生まれ、管理レベルの向上が期待できる。**また、これまでの部門や業務プロセスごとの縦割りのアプローチでは、認識や対応が困難であった複数の部門にまたがるリスクや部門と部門の境界線上にあるリスクに関しても、ERM を導入することがメリットをもたらし、比較的容易に対応が可能となるといった効果が期待できる。**このように１つの組織体としての一定のレベル合わせを行い、リスク全体としての管理レベルを改善していくことは、組織体として永続する上での効率と安定を同時に達成する上で不可欠なことである。

３．現行の経営管理システムとの関係と相違点

質問１．他の新しい経営管理システムとの関係・相違点

品質マネジメントシステム（ＩＳＯ９０００）や環境マネジメントシステム（ＩＳＯ１４０００）、バランススコアカード（ＢＳＣ）、およびＣＳＲマネジメントシステムなど、他の新しい経営管理システムとはどこが違うのか、それらと整合性はあるのか。

＜回答＞

ＥＲＭは、これまでは個別に考えられてきたマネジメントシステムを、リスクという視点で統合的にとらえたものである。

ＩＳＯ９０００や１４０００、様々なステークホルダーの視点をマネジメントに採り入れるＢＳＣや、最近では環境保護も含めた社会貢献・消費者保護・コンプライアンス等々総合的に求めるＣＳＲなどは、品質保証や環境保護への要求を満たすため、あるいは企業に求められる各種ステークホルダーの要請にこたえるため、というように、ひとつひとつの目的に応じて、導入されてきたといえるだろう。

これらと同様、ＥＲＭもまた、ＰＤＣＡの構造を持つマネジメントシステムである。ただしＥＲＭの特徴は、企業や事業体が目指す「目的」そのものから始まり、それを阻害するあらゆるリスクを想定し、対処すべきリスクやその対策を選択する。

従って、ＥＲＭが対象とする範囲は広く、他の経営管理システムもまた、その中に含まれてくるはずである。企業や事業体は、そのようなトータルの視点で、対応すべきリスクをとらえたとき、その対策として、必要な個々のマネジメントシステム導入を選択していくことになるだろう。

質問２．現在使用している既存の経営管理システムとの関係・相違点

たとえば部門業績評価制度や経営管理のための実績報告制度など、現在機能している既存の経営管理システムとどこが違うのか。それらと整合性はあるのか。また、ＥＲＭを導入するためには、現在機能している既存の経営管理システムをどのように変える必要があるのか。

＜回答＞

ＥＲＭは、既存の個々の管理システムにとって代わるものではなく、それらを補完・補強するものとなる。

ＥＲＭとは、リスクという視点の下に統合される、マネジメントのシステムそのものと言える。いま自社や自グループ内で機能している制度やシステムとは異なる何かの事物ととらえるよりも、まずは、一段上で包括するシステムと考えたほうがよいだろう。

ＥＲＭは、企業や事業体における様々なリスクを統合的に把握し、調整し、最適な管理方法を選択できるようにするものである。業績評価制度や報告制度も、マネジメントシステムには不可欠でありその意味ではこれまでとの違いはない。しかし、それらの個々の制度も、より統合的な視点に照らして見ることで、組織にとってより的確な制度へと見直す可能性が広がってくる。

もし、これからＥＲＭを導入しようとするのであれば、まったく新しいものを作るのではなく、事業体が目指そうとする方向性に照らして、既存のマネジメントの方針やシステムを検証し、強み・弱みを評価し、いまあるものはできるだけ活用し、新たに必要と思われるしくみを構築していくのが望ましい。

４．コーポレートの経営管理機能との関係

質問１．コーポレートが行う経営管理との違い・線引き

リスクマネジメントは、コーポレートが行う経営管理そのものであるように見える。コーポレートが行う経営管理とどのような点で違うのか。両者の線引きはどのようなものなのか。
リスクマネジメントはコーポレートが行う経営管理と同じことを、別の方法でやるだけではないのか。二度手間にならないか。

＜回答＞

経営管理もＥＲＭもマネジメントシステムという意味では同じである。従来のシステムとは別の機能、別の方法とみなすより、企業全体を横断するリスクを想定し、それに照らして、従来の管理システムを、発展・強化するものとみるべきだろう。

また、ＥＲＭの考え方では、企業のあらゆる階層、組織の人々がこれに関わることになる。コーポレート以外の組織でも、リスクマネジメントは行われている。コーポレートの役割上、これらの活動をすべて統制し、監督する役割も大きくなってくると思われる。

５．その他

質問１．既に主管する部が決まっているリスクとの関係は

既に主管する部が決まっているリスクは、今回提案されたリスクマネジメントの対象に入るのか。対象に入るとすれば二重管理になるのではないか。

＜回答＞

既に主管する部が決まっているリスクも、今回提案されたリスクマネジメント（ＥＲＭ）の対象に含まれるが、二重管理になることはない。

それは、ＥＲＭが従来の「分散的なリスクマネジメント」ではなく「総合的なリスクマネジメント」を目指していることによる。ＥＲＭの目指すリスク管理は、リスクを「各部門に任せっきりにする」ことから「会社全体として管理する」という考え方の導入である。これによって、各部門毎に本来業務として行われているリスク管理が相互のつながりをもつことになり、「分散的なリスクマネジメント」では対応が難しい、あるいは不十分な面を補強することが可能となる。つまり、全社の立場から見れば複数部門で二重管理になっているリスクを整理する方向に導いたり、逆にポテンヒットになって管理されていないリスクを明らかにすることになって、全社レベルでのリスク管理体制・機能改善をもたらすのである。

各部門が本来業務の一部として「単独で」行うリスク管理も、各部門の異なる視点で把握されるリスクであり、ＥＲＭの重要な要素といえる。ただし、上述したように、ＥＲＭの考え方に基づくリスク管理はそれぞれの個別のリスク管理にとって代わるものではなく、それらを包含するものであると考えると分かりやすいと思われる。

質問２．誰のために必要なのか

リスクマネジメントは、誰のために必要なのか。コーポレートのためなのか、トップマネジメントのためなのか、それともリスク管理部門のためなのか。

＜回答＞

リスクマネジメントは誰のために必要なのか、ということについて検討するために、ここでは先ずＥＲＭの導入が各部門にとってどういうメリットがあるかについて考えてみる。

メリットとしては次のような事項が挙げられる。

①最適予算配分メリット

・ＥＲＭはリスクを会社全体の立場で管理するという考え方の導入であるから、各部門におけるリスクを全社横並びで比較することが可能になる。その結果を受けて、対策等取組みの優先順位を定めてリスクに応じた資源配分を助成する機能を発揮する。この機能を有効にするため、先ず各部門の重要リスクは、合理的な基準、即ち全社の中での影響度・発生頻度などを基準にした解決に取り組むための優先度検討（リスクの評価・分類）を行う必要がある。各部門にとって自部門だけの負担では解決しにくいリスク対策も、全社ベースでの位置づけが明確になることで、対策取組みの予算もたやすく得ることが可能となる。こうして、全社レベルで考えた最適な予算配分が行われることになる。

②自部門リスクの詳細把握メリット

・自部門リスクについて、全社ベースでの位置づけが明確になるプロセスでリスク要因まで掘り下げた分析が行われることになるので、各部門長は自部門の抱えているリスクの詳細、他部門への影響、全社影響等の詳細把握が可能になる。この結果、各部門長自身が各リスクに対して取組むべき事前の対応策等有効な手段が打ちやすくなる。

ところで、以上の事項について、視点を変えて経営者或は経営管理機能を担う本社部門の立場でみてもメリットとも言えるものである。

このように総合的なリスクマネジメントをめざすＥＲＭの効果は、会社を構成する「トップマネジメント、リスク管理部門、現業部門」等すべての部門、階層を含む「会社全体」で享受できるものである。ここでは社内に視点をおいて説明したが、以上のメリット効果はさらに発展してステークホルダー全体にも影響を及ぼすことにもつながる。ＥＲＭは、リスクマネジメントに関係を持つあらゆる階層のための仕組みであるといえる。

質問３．理解や納得感を得られるのか

リスクマネジメントを導入に着手しても、全社ベースで理解や納得感が選られるのか疑問である。単なる運動論に終わってしまい、結局何も残らなかったということにはならないか。

特に、現場の管理者クラスも巻き込んで行うと言うが、多忙な現場の実状を考えると、「やらされている」として反発を受ける可能性が高く、現場第一線に定着するとは思えない。

＜回答＞

ＥＲM導入のメリットについては、トップマネジメント、リスク管理部門、現業部門等を含む全社で享受できるものであり、単にリスク管理部門の管理のためのツールにとどまるものではない。現場の責任者にとってのメリットも大きい、ということを先ず正しく理解してもらい、本社部門に「やらされている」という誤った考えの上でＥＲM導入への取組みを開始することのないようにする必要がある。このことは、ＥＲM導入活動を継続してゆく上で、つまりＥＲMを有効な存在足らしめるためにも、必要不可欠なことである。

というのも、ＥＲM導入に際しては、全員参加での取組みが無ければ意味が無いからである。ＥＲMへの取組みは、リスクを「各部門に任せっきりにする」ことから「会社全体として管理する」という考え方の導入である。リスクマネジメントを推進するに当たり全社ベースで障害となる事項、或いは促進剤となる事項を認識・分類した上での、全員参加による目標達成に向けた継続的な活動が求められる。これらのことを、全社員に正しく理解してもらうことが、導入後（将来）のリスクマネジメントシステムを成功に導く大きな鍵となるといえよう。

質問４．今までやったことがないのに、本当にできるのか

「全員参加型で、全てのリスクを評価し対応する」といっても、社内の多くの部門は今までそのようなことをやってきていないので、果たしてうまくいくのか不安である。もちろんリスク管理部門などで専門的でやってきているところもあるが、そういう部門とのギャップにも不安を感じる。

＜回答＞

新しい制度、マネジメントシステムを導入するときには、多かれ少なかれ不安や戸惑いが生じるものであるが、ＥＲM導入に際しても同様であると思われる。一方、マネジメントシステムとして期待される意味合いも、これまでに社内で取組んだ事例があれば同様な内容が経験されており、理解はされやすいと思われる。

例えば品質管理のときや、コンプライアンスのときにも経験したように、マネジメントシステムは PDCA サイクルとして日常業務の中に組み込まれていかなくては一時的なキャンペーンに終わってしまい、継続的な機能を有するシステムとは言い難いと感じるのと同じである。したがってこのような流れが浸透するように社員全員の意識を変えていくための継続的な努力も必要である。

特にＥＲMは、「全員参加型で、会社全体として管理する」という状況が継続的に維持されることを前提としており、「自部門で対応している個別リスク対応で精一杯。これ以上のリスク管理には手を染めたくない。」といった従来から良く見られる社員意識からの脱却が必要不可欠となる。

一方、ＥＲM導入にあたって各部門を引っ張ってゆく立場にある部門長にとっても、

①リスクの詳細内容、事前の対応等有益な情報が得られること

②従来属人的に管理されてきたリスクが、組織として管理され、当該リスク管理のノウハウが蓄積されること、

などのメリットをあげることができる。ＥＲM導入スタートに当たっては、部門長から社員にいたるまでの全社的な視点でのメリット理解、或は従来既に取組んだことのある各種マネジメントシステム事例との比較による理解を深めることで、新しいシステム導入取組みへの不安も払拭することが可能となると思われる。

質問５．「一時的なはやり」ではないのか

ＥＲＭは、例えばＥＶＡなどの「一時的なはやり」で、しばらくすると忘れられてしまうものと同類なのではないか。「これからの経営管理に必要な永続的・普遍的な仕組み」であると、どうして言えるのか、本当に言えるのか。

＜回答＞

複雑多様化する社会、経済情勢に対応できるリスク管理プロセスを導入したいという企業、事業体は数多いと思われる。それに応えるのがＥＲＭである。ＥＲＭは必ずこうしなければいけないというような規則・規定ではないが、リスク管理プロセスを導入する際の指針（共通言語）として重要な役割を担うものである。

もともと「内部統制」に焦点をあてた「ＣＯＳＯ９２年レポート」の‘発展型’としてのフレームワーク（枠組み、流れ。実際に動くシステムを作るためには、具体的な手続き、権限といったものを別途制定することが必要。）がＥＲＭである。アメリカではこのような「フレームワーク」がいくつも作成され淘汰されていく過程で、結果的に多くの分野から支持を受けたものだけが残っていくのが現状である。そのような中で、「ＣＯＳＯ」は公認会計士協会、会計学会、内部監査人協会、財務担当経営者協会から構成されており、十分にグローバルスタンダードとして、これからの経営管理に必要な「永続的・普遍的な仕組み」となる資格を有している。１９９２年頃のアメリカでは、企業統治の観点から大きな課題として注目されていた「内部統制上の問題（不正経理問題）」に対処するために設置された委員会が「ＣＯＳＯ」であり、ＥＲＭは時代の流れの中でその必要性から求められて策定されたものといえよう。

一方、実際にいかなる企業も各々の業務活動を行う上でリスクの存在を全く無視することはできない。ＥＲＭは、理想論ではなくむしろマネジメントがリスクに満ちた環境の中で、より効果的に業務活動をおこなうことを可能にするためにどうすべきか、という枠組みを示していることにも注目しておくべきである。理想論では無いが故に、現実的な経営管理に必要な「永続的・普遍的な仕組み」として受け入れられる仕組みであると言えるのである。

以下参考のために、ＥＲＭ導入が企業にもたらすメリットと思われる項目を掲げておく。

①経営目標とのバランスの中で、受け入れ可能なリスクの大きさと戦略の方向性を検討できること
②リスクとリターンを関連付けること
③リスク対応に関する意思決定プロセス・手続きの質を高めること
④業務上の予測できない事象や損失の極小化を図ること
⑤企業全般にわたるリスクを特定し、コントロールすること
⑥複数のリスクに対する総合的な対応策をとること
⑦ビジネス機会をとらえること
⑧経費・予算を合理的に配分すること

質問６．コンプライアンスリスクの方を優先すべきではないか

当面一番重要なリスクはコンプライアンスリスクであるのに、その先を見越したリスク全体を管理しようとするのは、優先順位が逆ではないのか。まず、コンプライアンスリスクを管理する体制を作り、その後にリスクマネジメントに取り組めばよいのではないか。

＜回答＞

ＥＲＭは、コンプライアンスリスクも含めて、他の多くのリスクを個々に単独で管理するのではなく、広く全社的な立場で管理するための考え方である。つまりＥＲＭの考え方に基づくリスク管理のほうは各個別のリスク管理を包含するものであると位置づけられる。

従来型の各部門による「分散的なリスクマネジメント」では把握できなかった、或は相互に関連し合う影響について理解されなかった内容が、企業全般にわたるリスクとして位置づけられることにより、コントロールされやすい状況をもたらす。さらに、複数のリスクに対する統合的な対応策策定が可能になることも認識すべきである。ビジネスプロセスには多くの固有リスクが関係していることについては異論が無いと思われるが、ＥＲＭは、それらのリスクを管理するための統合的な解決策作成への道しるべとなるのである。

質問７．複雑な仕組みが当社にとって本当に必要なのか

ＥＲＭは複雑な仕組みに思える。そんな複雑な仕組みを当社が導入しなければならないのだろうか？当社にとって本当に必要な仕組みなのだろうか？

＜回答＞

ＥＲＭそのものが、到達しなければいけない目標を持っているかのように誤解してしまうと、「質問」のように感じてしまうと思われる。

全ての企業は、リスクの全く無い環境で業務活動を行うことには無理がある。一方ＥＲＭが、そのようなリスクの無い環境を作り出すという「使命」を帯びているわけでもない。むしろ、ＥＲＭはリスクの存在を前提にして、マネジメントがリスクに満ちた環境の中で、より効果的に業務活動を行うことを可能にするための支援ツールとして受け止めるのが適切である。このため、ＥＲＭは、企業の中であらゆる業務活動から独立して運用することは前提にしていない。あくまでも、マネジメントプロセスの支援機能として働く一つのツールなのである。

ＥＲＭ導入により、複数の部門にまたがるリスクや、部門と部門の境界線上にあるリスクへの対応が容易になるというメリットが期待できる。結果的に重要なリスク及びその管理方法を経営層（取締役会等）に提供することで、コーポレートガバナンスと相互に密接に関連することになるし、またリスクを反映させた評価基準を提供する等によって業績評価（業績管理）との関連も生まれる。さらに、業績目標を達成する上での無駄な資源投資・損失防止や業務執行に必要な法律等の準拠への手助けにもなると思われる。

多くの企業がＥＲＭ導入に踏み切っているのは、このようにＥＲＭ導入により、直接効果として見える以上のメリットをさまざまな形で享受することができることが期待されるためである。

質問 8. ＥＲM導入時には現場の作業が増えると反対されないか？

現場では既にいくつかのリスク管理の名の下に、いろいろな作業が発生している。これ以上さらに手間暇をかけなければいけないような仕組みを導入しなければいけないのだろうか？

＜回答＞

確かに、ＥＲMは、これまでの「各部門に任せる」従来のやり方とは異なる「全社的な視点」からのリスク管理への取組みであるため、現場の違和感、従来には無い作業等が増えることもあると思われる。しかし、それは一時的なものであって、その仕組みが継続的な活動として浸透してゆけば、その見返り、効果は現場にも大きく帰ってくるものであることを理解してもらう必要がある。

そのためには、導入時の説明会などは重要視されるべきである。ＥＲMが複雑な仕組みであるという先入観をすて、マネジメントがリスクに満ちた環境の中で、より効果的に業務活動を行うことを可能にするためのひとつのツールであるという考え方を理解してもらうこと、さらに経営層・管理部門のみならず現場部門にとっても導入による効果をさまざまな形で享受できることを理解してもらうことで、ＥＲM導入取組み時の抵抗感は和らぐはずである。導入時の説明会は、全社員の理解を得る絶好の機会である。

Ⅱ．基　本　編

第１部　ＥＲＭ固有の質問

１．ＥＲＭの定義と目的

質問１．ＥＲＭとは何か

＜回答＞

企業や事業体が、その目的を達成するとき、それに影響を与え得るすべての事象をリスクとして想定し、それらを統合的かつ戦略的に管理することで、企業価値の向上に結びつけようという新しいリスクマネジメントの考え方と手法が、ＥＲＭである。

どのような企業でも、何らかの形でリスクマネジメントを行っている。それは多くの場合、生産部門なら品質管理、営業部門は債権管理、情報部門はシステムやハードの保全、そして事故や災害に対する保険というように、企業内のそれぞれの部門で、それぞれの業務推進を阻害するリスクを想定し、回避しようとしてきた。

特に欧米では、長い間、リスクマネジメントといえば安全で安価な保険購入の戦略であった。この、従来のリスクマネジメントは、多くの部門が個々別々に、保険を蓄積しているさまをサイロにたとえ、「サイロ型のリスクマネジメント」と言われる。

これに対して、９０年代以降に開発されたのが、ＥＲＭ（エンタープライズリスクマネジメント）である。ＣＯＳＯ（トレッドウェイ委員会組織委員会）は、ＥＲＭを次のように定義する。

「ＥＲＭは、事業体の取締役会、マネジメント、その他の人たちによって遂行され、事業体全体の戦略策定に適用され、事業体に影響を及ぼす発生可能な事象を特定して事業体のリスク・アピタイトに応じたリスク管理が実施できるように設計された、事業目的の達成に関する合理的な保証を与えるひとつのプロセスである。」（「ＣＯＳＯ-ＥＲＭフレームワーク」（2004 年 9 月）より）

ここには、ＥＲＭのいくつかの基本的な考え方が示されている。

- ＥＲＭは、それ自体が目的ではなく、目的のための手段、プロセスである。
- 事業体のすべての人がこれに関わる。
- 事業戦略策定にも利用される。
- 事業体のあらゆる階層や組織単位でリスク認識を共有する。
- 事業体が許容できる範囲内で、リスクをコントロールすることができる。

ここから思い描かれるのは、かなり広範な“リスクマネジメント”であるが、重要なのは、ＥＲＭは「リスク」の概念を新たにし、そのマネジメント目的を、組織目標の達成、企業価値の向上に置くところにある点といえよう。

質問２．ＥＲＭは何のために導入し、何を解決するものなのか。

導入することでこれまでの経営管理と比べて何が変化するのか。
どのような問題の解決に適しているのか。

＜回答＞

今日、企業をとりまく環境は不確実性に満ちている。ＥＲＭが注目されるのは、そうした不確実性に対処し、企業の目的達成の確度を上げるための手法と考えられるためである。

欧米でＥＲＭが導入され始めた背景には、９０年代に入って相次いだ金融不祥事から、企業に対するリスクマネジメントの強化と開示の要請が強化されてきたことがあげられる。ただ、それだけではなく、企業の側にも、従来のような個別のリスク管理では、複雑化、多様化する事業環境に対応しきれなくなり、より高度なリスクマネジメント戦略が必要になってきたためとも言えるだろう。

ＥＲＭのプロセスでは、組織目標を策定し、それに照らしてあらゆるリスクを識別し、分析・評価し、対応策を選択し、管理する。そのプロセスを踏むことで、次のようなメリットを提供すると言われる。

１．組織目標と結びつけることで、戦略的なリスク管理ができる。
（１）ＥＲＭでは、事業体が受入可能なリスク範囲を考え、その中で戦略目標に沿って、コントロール可能なリスクを受け入れることになる。
（２）「リスク」を軽減し、「機会」を最大化するという考え方に立つので、ビジネス機会も逃さず把握することができる。
２．意思決定の質を高める
（１）様々な事象を想定するので、リスクの相互関連や連鎖を把握できる。
（２）様々なステークホルダーの立場でリスクを認識できる。
（３）様々な事象に対して、考えられるリスク対応策を検討し評価するので、可能な限り最適な対応策を選択できる。
（４）組織内のすべての関係者に、リスクマネジメントに関する共通言語を提供する。
３．効率的かつ費用効果の高いリスク管理ができる。
（１）上記から、リスクと機会に対して、最適な資源配分が可能になる。

ここで、より具体的な例として、日本においてすでにＥＲＭ活動をはじめている東京ガス㈱での、導入目的をあげてみる。

１．グループ全体の統一的なリスク・マネジメントの仕組みを構築すること。
２．リスクを全社的視点で把握し、経営資源の最適配分等の経営判断へ活用すること。
３．リスク対応状況を継続的にフォローするモニタリングの仕組みを制度として構築すること。
４．他社事例を他山の石として、自主的に点検し対応策を実施するリスク・レスポンスのいっ

そうの向上。

５．リスク・マネジメント体制構築に対する司法、行政、株主等ステークホルダーからの要請への対応を向上させること。

６．自由化進展や事業領域拡大に伴う新たなリスクに適切に対応する基盤を構築すること。

同社でのＥＲM導入の背景には、規制緩和による競争激化への対応、新規事象の進出計画などに伴い、予測されるリスクは大きくかつ複雑で、その対応のためには、新たに、グループ全体としての統合的なリスクマネジメントシステムが必要との認識があった。（「東京ガスグループにおける統合的リスクマネジメントへの取組みについて」月刊監査研究２００４年６月）

すなわち、ＥＲMは、企業や企業グループが自らの置かれる環境を客観的にとらえ、かつどのような環境にあっても企業価値を上げようとする強い欲求のもと、そのための明確な戦略・目的を持つことによって始動し、推進されるものと言えよう。少なくとも、それぞれの企業や企業グループにとっての、何らかのリスク意識とその克服という能動的な意志なしには、マネジメントそのものが意味のないものとなる。

ＥＲMは、業績管理や経営管理システムのひとつのトレンドとして、最先端企業の証明のごとく、とりあえず導入してみせて終わるものではない。組織のすべての人々のリスクに対する認識を変え、プロセスを構築し、マネジメントシステムとして恒常的に機能させるには、経営の明確な意思と強力な推進力が必要となる。これから ERM を導入しようというときには、自社・自グループの目指す姿をはっきりと認識した上で着手すべきであろう。

２．ＥＲＭのメリットと必要性

質問１－１．ＥＲＭのメリット

ＥＲＭはどのようなメリットをもたらすのか。また、ＥＲＭ導入により期待する効果は何か。
➢導入によりどのようなメリットや効果が得られるのかを明示することが必要。

質問１－２．これまでＥＲＭに取組んでいたといえるのか否か

これまでもＥＲＭに取組んでいたと言えるのではないか。それとも、これまではＥＲＭに全く取組んでいなかったということなのか。
➢我が社では、中期計画では「ＳＷＯＴ分析」を行ってリスクを認識し、優先順位を決めて取組んでいるし、新たな脅威を認識した場合には毎年計画を見直して取組んできている。このように、リスクマネジメントにはそれなりに取組んできたつもりなのだが、どうしても場当たり的になってしまって、継続性がなく、堂々巡りになっているような点が気になっている。

＜回答＞

ＥＲＭは、まだ生まれて間もないが、既に導入したいくつかの企業では、収益の安定性を確保することを目的に、競争優位の確立を目指すツールとして熱烈な支持を受けている。これらの取組は以下のようなＥＲＭのもたらすメリット及びそれにより得られる効果によるものである。

ＥＲＭは、ＣＯＳＯの新しいフレームワークの中で、以下の能力を助成するとされている。

- リスク・アピタイトと戦略を整列させる
- リスク対応意思決定を強化する
- 業務上のサプライズや損失の抑制
- 複合リスクや企業間リスクの識別と管理
- 機会の活用
- 資本運用の改善

（「ＣＯＳＯ-ＥＲＭフレームワーク」（2004 年 9 月）エグゼクティブ・サマリより）

上記のように ERMの導入はさまざまなメリットをもたらし、これにより期待される効果は大きいと考えられる。

これまでの取り組みとＥＲＭ導入によるリスクマネジメントへの取り組みの違いは、以下の点があげられる。

『ＥＲＭは「伝統的な」リスクマネジメントとは大きく異なる。リスクマネジメントは伝統的にリスクの範囲や、リスクマネジメント戦略のタイプ、リスクの影響と性質に関してより狭い範囲に焦点を当ててきた。範囲は伝統的に純粋な危険や、資産･負債、リスクに限定されており、戦略は

主に保険による解決策に集中していた。結果として、従来のアプローチはリスクを厳密に下方現象として取り扱う傾向があり、組織が達成を目指す目的への影響度合いではなく、重要性とは無関係に保険によって解決される性質のリスクに焦点がおかれていた。』

（全社的リスクマネジメント―近年の動向と最新実務―、ティリンガスト-タワーズ・ペリン編、眞田光昭訳　より抜粋）

また、これまでの単年度ごとの対応を主体とする個別の取組みと違って全社的に取り組むことにより、これまでどちらかというと場当たり的な対症療法となっていた取組が、組織的に共有され、リスク管理ノウハウの蓄積にすることが可能となる。また、この展開を進めることはリスク管理レベルを継続的に改善することにつなげることを可能とする。

一例だが、ウォルマート社ではリスクマネジメントの伝統的アプローチとＥＲＭの概念を比較し以下の利点を見出している。

『伝統的リスクマネジメントのフレームワークの下では、リスクは一般に機能（すなわち、流通、業務、給料計算、物流、法務）やリスク専門領域で分割した「サイロ」の中で扱われる。このサイロ・アプローチにおける問題はその焦点の当て方が縦割りで、複雑な問題の限られた視野だけが提示されるということである。

もう１つの限界は、情報の各機能横断的な共有は容易なことではなく、また各リスクは独立して優先順位付けされることである。ウォルマート社のマネジャーは、サイロ・アプローチが長い目で見ればより高いリスクマネジメント・コスト結果として跳ね返ってくる傾向があると感じた。

他方、ＥＲＭフレームワークは、水平と垂直の両方から焦点を当てる機能横断的なアプローチをとる。ウォルマート社は、ＥＲＭがリスクのより包括的な視点を提供し、より統合化された解決策を生み出すことができると感じた。ＥＲＭフレームワークはまた機能横断的な情報交換を容易にし、リスクの優先順位付けの調整にも役立つ。この結果、彼らは種々のリスクの相互関係を識別し、活用できるようになり、最終的により費用対効果の高いリスクマネジメント戦略を持つこととなるだろう。ＥＲＭが約束するものは伝統的フレームワークより優れているように思われた。』

（全社的リスクマネジメント―近年の動向と最新実務―、ティリンガスト-タワーズ・ペリン編、眞田光昭訳　より抜粋）

参考までに、ＥＲＭの導入による企業を取り巻く各ステークホルダーへのメリットの一例を以下に示す。

ステークホルダー別にみたＥＲＭの有効性とは

	ＥＲＭとは何か？	なぜＥＲＭは必要か？
顧客	商品･サービスの企業としての全社的改善活動	商品の品質の信頼性、安全性及び企業の提供する商品に対する保証が明確になる。
取引先	取引に於ける自社活動の安定性を保証する上での合理的な判断材料	取引に際しての契約履行の確実性を向上させ、自社活動の安定性が向上する。
従業員	企業活動における目標到達までの不確実性の要因を管理し、確実性を継続的に向上させるプロセス	組織としての目標到達への不確実性が共通の尺度にて継続的に改善され、信頼性と安定性が向上する。
債権者･株主	企業が活動推進に於ける不確実性を管理し、継続的に改善する全社的活動	融資先、投資先の資本回収可能性リスクが管理され、資産運用の安全性と効率性が向上する。
地域社会･国家	固有の企業が独自に活動を管理、改善する上で共通の基準	組織的な活動の信頼性と安全性が向上し、社会･国家としての経済効率が向上する。

質問２．ＥＲＭは「なぜ今」また「誰にとって」必要とされているのか

なぜ今ＥＲＭが必要なのか。また、ＥＲＭは誰にとって必要なのか。経営者にとって必要なのか、あるいは、実務担当者にとって必要なのか。

＜回答＞

ＥＲＭは、大規模なものから小規模なものまで、様々な業種を横断して非常に多くの組織が着手している。それらの動機付けは、環境変化への対応としてやむを得ずというものから、競争優位を目指す合理的ビジネスモデルとしてというものまで多岐にわたる。

環境変化の要因としては、特に近年の米国における動きが契機となっている。２００１年９月１１日に生じた同時多発テロ事件および１２月に露呈したエンロン社の会計不正事件は、会社にかかわるリスクマネジメントの重要性が再認識させた。その後のワールドコムの巨額不正事件を経て、一段と企業への不信が強まる中で各国企業に対してガバナンスメカニズムを改善し、主要リスク要因と課題を全面的に開示させようとする圧力が増大している。

また、市場要因も組織にＥＲＭを検討させる上で重要な役割を演じている。包括的な株主価値の管理とＥＲＭは複雑に関係している。今日の金融市場は一貫して利益予想を満たすことに対して相当なプレミアムを与える。逆にこうした期待に答えないと、金融市場から株主価値への手厳しい罰を受ける可能性がある。ある調査によると他の条件を一定とした場合に、競合他社より安定した利益を達成した組織は非常に高い市場評価を得られることが判明している。このように、いまや企業経営は、あらゆるリスクに対処可能なように、全社的なリスク・マネジメントを設計しておくことが不可欠となっており、今後、ERM がそのための指針となることは間違いないであろう。

次に、ＥＲＭが誰にとって必要とされているかについては、ＣＯＳＯのフレームワークより企業内の各構成員との係わり合いにも明示されているが、以下のようなトップダウンのアプローチである。

１．取締役会

取締役会には、ＥＲＭを監視する役目があり、ＥＲＭの重要な要素を理解し、リスクについて経営管理者に質問をし、経営判断に同意することが求められる。しかし、経営管理者に代わって意思決定することはできないし、ＥＲＭに対する経営管理者の責任を軽くすることもできない。

２．ＣＦＯおよび財務管理部門

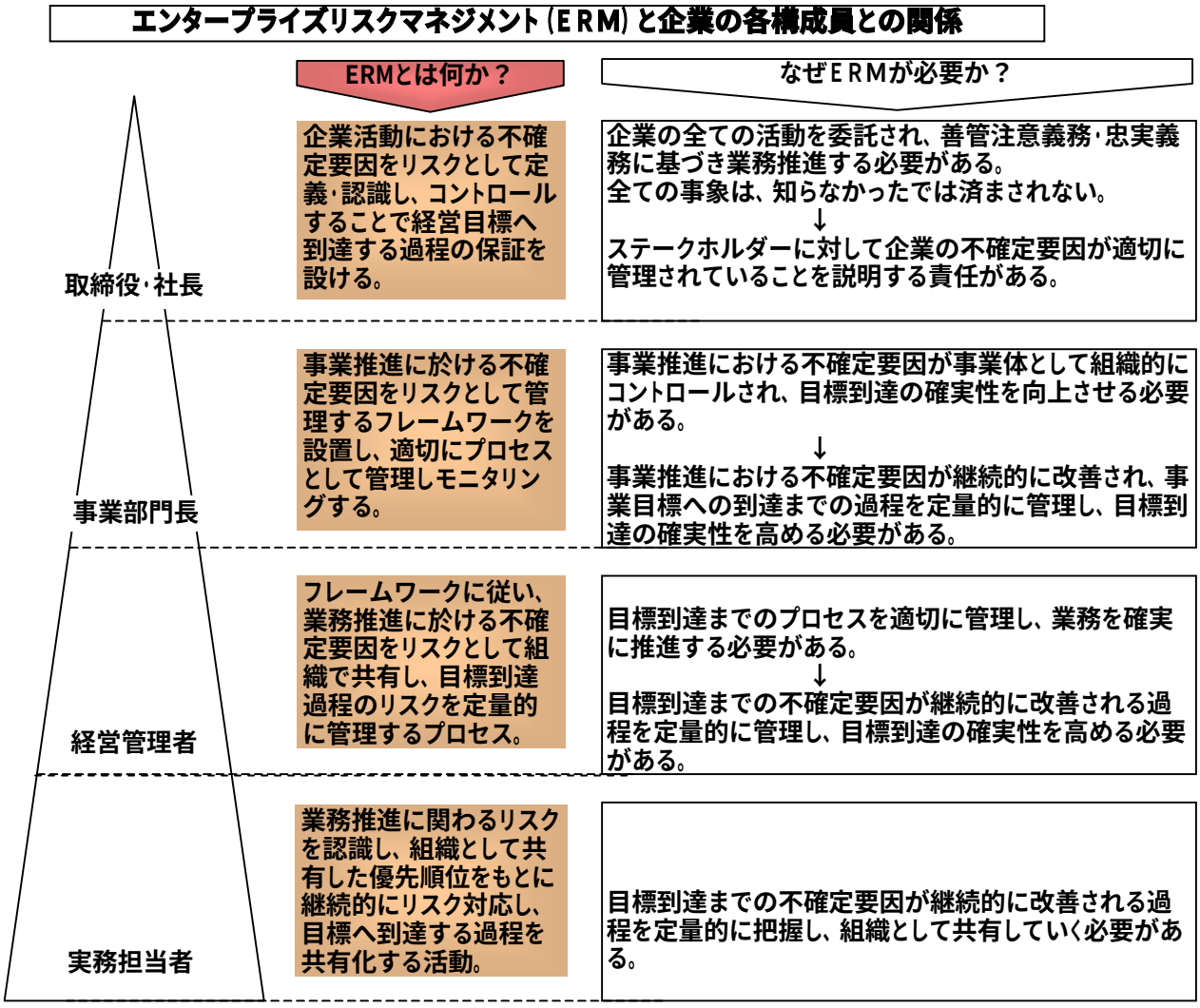
ＣＦＯと財務管理部門は、戦略立案プロセスの欠くべからざる一部分としてのリスク・マネジメントに必要な、規定や手続の策定に重要な役割を果たす。ＣＦＯは、リスク選好および許容の決定のための分析ツールを作り、会社全体のリスク・ポートフォリオの構築と管理をする。また、リスク評価が、経営管理プロセスの中で継続的かつ不可分な部分となっており、また取締役会で決定しているリスク・マネジメント方針とも一致しているように、必要な統制を構築する経験と知識を持っているのもＣＦＯである。

３．内部監査人

取締役会および監査委員会は、適切なリスク・マネジメント・プロセスが整備され、適切かつ有効であるかどうか判断する監督の役割を負う。内部監査人は取締役会および監査委員会に対し、リスク・マネジメント・プロセスの適切性と有効性について調査、評価、報告、改善助言を行う。ＣＯＳＯ－ＥＲＭフレームワークは、会社のリスク・マネジメントへの取り組みを内部監査人が評価するときのベンチマークとして活用できる。

以上、トップダウンのアプローチではあるが、このフレームワークは、ＩＴ、財務、経理、内部監査、そしてリスクの専門家等、あらゆる組織のすべての分野で使用できるが、企業が全社的に、継続してリスクに取り組む力を強化するように作られている。

ＥＲＭの全ての企業構成員への必要性に関する妥当性については次の図のように整理することができる。



３．従来のリスクマネジメントとＥＲＭとの違い

質問１．従来型のリスクマネジメントとＥＲＭとの違い

従来からリスクマネジメントはやってきた。各部門が責任を持って、「ＳＷＯＴ分析」を行いリスクを認識し、優先順位を決めて取組んできたし、新たなリスクを認識した場合にはその都度計画を見直して対応策を実施してきている。このように、従来からリスクマネジメントには**それなりに取組んできた。**

従来行ってきたリスクマネジメントとＥＲＭとの**相違点は何**なのか。また、従来行ってきたリスクマネジメントでは**どのような点が不十分**であり、それに対してＥＲＭは**どのような点で優れているのか。**

＜回答＞

従来型のリスクマネジメントとＥＲＭとの主な相違点や、その不十分な点や優れている点は以下のとおり。

視点	従来型のﾘｽｸﾏﾈｼﾞﾒﾝﾄ	Ｅ　Ｒ　Ｍ
実施主体	**断片的** ・社内各部門が**断片的・専門的・独立的**にリスクを管理（注）。 ・ﾘｽｸﾏﾈｼﾞﾒﾝﾄは社内の**一部、限られた人達だけ**が行っている。主に財務、審査・与信、内部監査部門だけが行っている場合が多い。 ・**縦割り**で行われる。 ⇒リスクの**全社的視点での把握**と、それに基づく**経営資源の最適配分**等の**経営判断**が効率的に行いにくい。 ⇒ﾘｽｸﾏﾈｼﾞﾒﾝﾄの実施水準が部門により**バラつき、最低限の水準**を担保できない部門が発生する可能性がある。当該部門でリスクが顕在化した場合、ブランド価値毀損の影響が全社へ波及する。 ⇒有価証券報告書、決算短信、ＩＲ、株主総会などでのステークホルダーへの**情報開示**に際して、全社レベルでのリスク情報の適切な開示が行いにくい。	**統合的** ・経営レベルで**統合的・全社的**にリスクを管理（注）。 ・ﾘｽｸﾏﾈｼﾞﾒﾝﾄは**社内全員**で行われている。組織の誰もが、ﾘｽｸﾏﾈｼﾞﾒﾝﾄを自分の仕事の一部と考えている。 ・**全社横断的**に行われる。 ⇒リスクの**全社的視点での把握**と、それに基づく**経営資源の最適配分**等の**経営判断**が効率的に行いやすい。 ⇒部門によるﾘｽｸﾏﾈｼﾞﾒﾝﾄの実施水準の**バラつきが減り**、社内全体で**最低限の水準**が担保でき、一部部門でのリスク顕在化による全社ブランド価値毀損のリスクが減少する。 ⇒有価証券報告書、決算短信、ＩＲ、株主総会などでのステークホルダーへの**情報開示**に際して、全社レベルでのリスク情報の適切な開示が行える。
情報・認識	**断片的** ・リスク情報は**各部門内**に止まる（縦割り）。 ・リスクに対する**社内の認識**（捉え方や考え方）が部門により異なる。 ⇒社内各部門の**境界線上**にあるリスク	**統合的** ・リスク情報は**全社横断的**に共有される（横串機能）。 ・リスクに対する**社内の認識**は全社で共通。 ⇒社内各部門の**境界線上**にあるリスク

	や**部門を横断的にまたがる**リスクへの対応が行いにくい。 ⇒リスクやその対応策についての**全社的な共通認識・共通行動**が生まれにくい。 ⇒他部門でのリスク事例（失敗）を**「他山の石」**と受け止めることが少ない。	や**部門を横断的にまたがる**リスクへの対応が行いやすい。 ⇒リスクについての**全社的な共通認識・共通の行動**が生まれやすい。 ⇒他部門でのリスク事例（失敗）を**「他山の石」**と受け止めることが容易。
時間軸	**アドホック** ・ﾘｽｸﾏﾈｼﾞﾒﾝﾄはそれを行なう必要がある時に行なわれる。取組みが**単発的**であり、継続性に乏しい。 ・**短期**に焦点 ⇒ﾘｽｸﾏﾈｼﾞﾒﾝﾄの**ＰＤＣＡサイクル**が機能しにくい。	**継続的** ・ﾘｽｸﾏﾈｼﾞﾒﾝﾄは**継続的**に行なわれる。 ・**中長期**にも焦点 ⇒ﾘｽｸﾏﾈｼﾞﾒﾝﾄの**ＰＤＣＡサイクル**が機能しやすい。
対象範囲	**狭い焦点** ・危機・災害・不祥事や、資産・負債に関する損失など（起きて欲しくない）**特定のリスク**に限定。 ・（短期的な）損失防止が主な関心事。したがって、**下方リスク**が中心。 ・**金額換算が容易**な保険可能なリスクと金融的リスクが主な対象。 ⇒**企業価値の向上**への貢献が限定的。	**広い焦点** ・**全てのリスクと機会**が対象。 ・（短期的な）損失防止と（中長期的な）機会拡大の両方に関心。したがって、**下方リスクと上方リスクの両方**が対象。 ・**金額換算が困難**なオペレーショナルなリスクも対象。 ⇒**企業価値の向上**への貢献が大。
経営環境	**変化小** ・経営環境の**変化が少ない場合**に適している。 ⇒経営環境の変化が激しくなり、**リスクが大きく複雑化**した場合には、**全社レベルでリスクを把握し、対応戦略を経営判断**する必要に迫られるが、そのための手段としては限界がある。	**変化大** ・経営環境の**変化が激しい場合**に適している。 ⇒経営環境の変化が激しくなり、**リスクが大きく複雑化**した場合でも、**全社レベルでリスクを把握し、対応戦略を経営判断**するための手段として有効。

（注）リスク管理とは、ここでは、リスクの把握、評価、優先順位付け、対応策の策定・実施、モニター、対応策改善の一連のプロセスを意味する。

質問2．旧ＣＯＳＯとＣＯＳＯ－ＥＲＭとの違い

ＣＯＳＯが今回（２００４年）に提唱したＥＲＭと、１９９２年に提唱した内部統制フレームワークとはどこがどう違うのか。

＜回答＞

1. 両者の関係

ＣＯＳＯが今回（２００４年）に提唱したＥＲＭ（ＣＯＳＯ－ＥＲＭ）は、ＣＯＳＯが１９９２年に提唱した内部統制フレームワーク（旧ＣＯＳＯ）を**代替するものではない**。ＣＯＳＯ－ＥＲＭは、旧ＣＯＳＯの内部統制フレームワークの考え方をそのまま受け入れるとともに、それを**全て包含**しており、経営全体を対象としたより広範囲な視点を提供しているフレームワークである。すなわち、ＣＯＳＯ－ＥＲＭは、個々のリスクを個別的に管理するのではなく、組織全体のリスクを対象として、全ての重要なリスクを組織全体で統合的に管理するものである。

また、旧ＣＯＳＯの内部統制フレームワークは、ＣＯＳＯ－ＥＲＭの不可欠な部分であり、依然として内部統制のフレームワークとして位置付けられている。事実、ＣＯＳＯ－ＥＲＭには、旧ＣＯＳＯの内部統制フレームワークを参照せよと記載しており、ＣＯＳＯ－ＥＲＭを理解するためには、旧ＣＯＳＯの内部統制フレームワークを理解する必要がある。

旧ＣＯＳＯは内部統制に焦点を当てた「内部統制のフレームワーク」であったが、ＣＯＳＯ－ＥＲＭはそれを包含し、かつ、大きく経営全体を対象とした「統合的なリスクマネジメントのフレームワーク」である。

２．主な相違点

（1）「目的」の概念の拡大

ＣＯＳＯ－ＥＲＭ	旧ＣＯＳＯ	変更点
①戦略		新目的の追加
②オペレーション	①業務	変更なし
③レポーティング	②財務報告	概念の拡大
④コンプラアンス	③法規の遵守	変更なし

（2）「構成要素」の拡張し・精緻化

ＣＯＳＯ－ＥＲＭは、旧ＣＯＳＯの内部統制フレームワークの構成要素を拡張し、精緻化している。具体的には以下のとおり。

ＣＯＳＯ－ＥＲＭ	旧ＣＯＳＯ	変更点
①内部環境	①統制環境	概念の拡大
②目的設定	―――	新構成要素の追加
③事象の特定	②リスク評価	分割と内容の高度化
④リスク評価		
⑤リスクへの対応		
⑥統制活動	③統制活動	変更なし
⑦情報とコミュニケーション	④情報とコミュニケーション	概念の拡大
⑧モニタリング	⑤モニタリング	変更なし

（3）ＣＯＳＯ－ＥＲＭで新たに明確にされた主な概念

旧ＣＯＳＯの内部統制フレームワークでは明確にされず、ＣＯＳＯ－ＥＲＭで明確にされた主な概念は以下のとおり。

①戦略

戦略の策定を通してリスクを検討している。

②リスクと機会の区別

「リスク」を組織体の目的達成にマイナスの影響を及ぼす事象が発生する可能性と定義し、「機会」を組織体の目的達成にプラスの影響を及ぼす事象が発生する可能性と定義。

③リスク・アピタイト（リスク許容限度、リスク選好）

組織体が受け入れようとするリスクの大きさ。経営者はリスクアピタイトを定めた上で、戦略から期待されるリターンを、リスク・アピタイトと整合性を持たせることが必要であるとする。

④ポートフォリオの観点

個々のリスクそれぞれに焦点を当てて個別的に管理することの他に、組織体が負っている全てのリスクを集合体として捉え、全体としてのポートフォリオの観点からも管理することを提唱している。

４．日本企業におけるＥＲＭ導入事例

質問１．ＥＲM導入のきっかけ

当社では、新しい仕組みを導入する場合にトップの理解がないとなかなか前に進められない場合が多い。ＥＲM導入に成功した日本企業は、どのようなきっかけから導入に至るのだろうか。

＜回答＞

ＥＲM導入のきっかけは、主として次に示すような事象が影響しているようである。従来は、自然災害・業務災害が実際に発生したことを受けて導入検討を開始するという動きが主流であったようだが、今後は、各社・各部門におけるニーズに沿った形で予防的な見地から導入されるケースが増えると思われる。

[導入へのきっかけ分類]

①災害発生型	：大地震、台風などによる経営への打撃、業務上のトラブル発生等
（自然災害	→エネルギー・公共事業企業体など
・業務災害）	→食品事業等
②他社参考型	：同業他社導入の実例、新聞報道による触発等
③ニーズ対応型	：自社本来業務を遂行する上で必要性等

今後事業規模が拡大するなかで、企業全般にわたるリスクのコントロールや複数リスクに対する総合的な対応策をとる必要性が明らかになってきた企業は、上記「①、②」をきっかけとした導入に先進的な役割を果たした企業の成功事例を確認しつつ、自らのニーズに対応する形でＥＲM導入に踏み切ってゆくことになると思われる。

質問２．ＥＲＭ導入の手順

導入の手順に関していくつかの事例を知っておきたい。
（１） 本格的実施までの流れ
（２） 準備すべき項目
（３） 具体的なリスク評価方法・定量化方法

＜回答＞

「Ⅱ．基本編『４』は、３社（「Ｔ社（公共事業)」「Ｆ社（メーカー)」「Ａ社（商社)」のヒヤリング等で得た内容をベースに記述する。各項目以下の通りである。

（１）本格的実施までの流れ

①Ｔ社（公共事業）の事例

Ｔ社では、大きく三段階のステップを踏みながら導入に取り組んでいるところである。グループ全体での理解を得ることに注力しているために各ステップ最低１年はかけており、確実に各部門への浸透を図ろうとしている。今後は第三ステップである本格実施に向けて取組中である。

第一ステップ（準備期間１年）平成１５年度
(ｲ)重要リスクの把握、評価、分類
(ﾛ)リスクマネジメントの具体的運用方法の策定
(ﾊ)「リスク管理規則」の作成
第二ステップ（施行期間１年）平成１６年度
(ｲ)グループ全体でのリスク・マネジメントを試行実施
(ﾛ)各部門、関係会社は自主的に推進
(ﾊ)リスクの見直し、再評価
(ﾆ)リスク管理指標の設定（可能な場合）
第三ステップ（本格実施２年）平成１７～１８年度
(ｲ)グループ全体でリスク・マネジメントを本格実施

②Ａ社（商社）の事例

Ａ社では、従来からの「計測可能なリスク」を対象として発展してきたリスク管理を基礎にして、「計測不能なリスク」への対応プロセスとしてＥＲＭ導入に取組んでいる。

商社固有の特性により業務内容が多岐に亘っているため、リスク分散型の事業本部制を導入し、業務上の戦略的なリスク（リスクポートフォリオ）は適度に分散されている環境下でのリスク管理体制を取っていた。しかし、ビジネス環境の変化に伴い、全社レベルでのリスク管理

体制・機能改善の必要性が求められることになり、大きく三段階・４年計画でのＥＲM導入に取組んでいる。

前段階（「計測可能なリスク」を対象としたリスク管理体制の浸透）
(ｲ)リスクアセットの算出
(ﾛ)リスクリターンの算定
第一ステップ（「計測不能リスク」への対応：１年かけて取組み）平成１４年度
(ｲ)リスクの洗い出しと評価（頻度と影響度で算定）
(ﾛ)リスクマップの作成
第二ステップ（優先対応リスク区分の設定：１年かけて取組み）平成１５年度
(ｲ)三つのリスク区分の設定
①金銭的な不正・架空取引リスク等
②環境関連リスク・危険物取扱関連リスク等
③文書作成に関するリスク等
(ﾛ)改善策策定・実行の推進
第三ステップ（本格実施：２年かけて取組み）平成１６～１７年度
(ｲ)現場意識の改革（現場リスクオーナーへの浸透）
(ﾛ)制度定着化（ＰＤＣＡサイクルの実施と定着化）

③外国の事例

「全社的リスクマネジメント－近年の動向と最新実務」（ティリンガスト-タワーズ・ペリン編　眞田光昭訳 日本内部監査協会刊、以下「最新実務」）の第Ⅱ部には、外国企業の「全社的リスクマネジメントについての代表的事例の研究」レポートが収められていて興味深い。この中には、これからＥＲM導入を検討しようとしている部門・会社等にとって有益な教訓（各社取り組み実績を踏まえたもの）が示されている。

導入取組み時の留意事項として共通に指摘されている項目を以下に整理した。

＜導入取組み時の留意事項＞

（イ） ＥＲM導入から定着には時間(数年ターム)が必要であることを認識する必要がある。
（ロ）ＥＲM導入には現場部門の理解を得ることが前提である。
（ハ）社員の意識改革にはかなりの時間を要することを認識しておく必要がある。

（２）準備すべき項目

①リスクマネジメントの位置づけ・目的の理解
・全社的視点で把握、経営判断に使用するもの（Ｔ社）
・クライシスマネジメントとの違いでの理解（Ｆ社）
・従来管理されていなかったものを統合リスク管理の一環で管理するもの（Ａ社）
②仕組みの構築（Ｔ社、Ｆ社、Ａ社）
・継続的にフォローできる仕組みであること

・リスクレスポンスの一層の向上につながる仕組みであること
・ステークホルダーからの要請に対応が可能であること
・新たなリスクに対応する基盤が構築できること
・現場のリスクオーナーが自ら対応できる仕組みであること

③リスクのリストアップ

リスクのリストアップにあたっては、プロジェクトチームが構成されて推進役になり、現場を巻き込んでゆく事例（T社)、リスク分類を予め行ってその分類別に担当部門が確認し確定する事例（F社)、現場営業部門に近い営業統括部門にリスクマネジメントグループを設置して推進してもらう事例（A社）などがある。

この中でいずれにも共通なことは、本社部門或はリスク管理担当部門（プロジェクトチームも含む）がリスクを調査するのではなく、各現業部門・関係会社に自分たちで議論して作業してもらうというプロセスを導入していることである。この過程によって、今後のリスク管理は「やらされる」のではなく、自ら対応してゆくものであるという感覚が浸透してゆく効果を期待しているようである。

＜分類の事例：T社＞

・大分類、中分類（小分類）…リスク要因を選別する区分として

・	大分類	中分類
	（イ）災害・事故リスク	自然災害、原料調達、製造・供給支障事故
	（ロ）市場リスク	市場リスク、天候の変動
	（ハ）事業戦略リスク	規制緩和、新規事業への進出
	（ニ）情報リスク	情報漏洩、期間システム停止・誤作動
	（ホ）社会的責任リスク	環境、コンプライアンス、顧客対応

（4） 具体的なリスク評価方法・定量化方法

・リスク評価方法としては、各社とも＜発生確率（頻度）×　影響度＞で求めている。

①T社：リスクの定量化にあたっては、中分類の単位で集計する。発生頻度と影響度のうち影響度をより重視する。定量評価の難しいリスクについては、社会的な影響度・ブランドイメージへの影響などを考慮して評価する。

②F社：リストアップされたリスクの当該社（部門）におけるレベルを認識する目的で実施。

③A社：計測可能なリスクと計測不可能なリスクに分けて対応。

（イ）計測可能なリスクについては、リスクアセット（項目別にリスク度を定めておきリスク度を積算する）を求めて、リスクリターンをみながら、予め定められた年度内で目標値との関係をフォローしてゆく。

＜リスクアセット…例えば、キャッシュのリスクはゼロ＞

（ロ）計測不可能なリスクについては、頻度と影響度で算定する。

＜頻度　　×　影響度　＞

質問３．具体的なＥＲM活動の管理方法

ＥＲMを導入した日本企業は、具体的にどのような管理方法をとっているのか、またＥＲMの継続性維持のための仕組みはどうなっているのか。

＜回答＞

具体的な活動について、（１）担当部（セクション）、（２）フォロー体制　の区分で事例を見ていく。

（１）担当部（セクション）

①Ｔ社　　：リスク管理推進セクションを、推進当初（準備期間後の施行期間）は「監査部」に設置。但し固定的ではなく、実績を考慮しつつ担当セクションは柔軟に対応する方針で臨む。

②Ｆ社　　：経営管理部、経営監査部が対応する。

③Ａ社　　：現場営業部門内の総括部、ＲMグループが旗を振る。

（２）フォロー体制

①Ｔ社の事例

・各部門関係会社　　：毎年１回、リスク対策実施状況の確認及びリスク項目・対策の見直しを実施し、リスク管理セクション宛報告

・社長宛報告　　：リスク管理セクションは、受領した報告に基づいてヒヤリングを実施し、結果を社長宛に報告する。

・監査部　　：各部門、各関連会社への監査において、リスクマネジメントの遂行状況全般を監査（報告内容、実施状況、対応策見直し内容の有効性、適切性の監査）し、社長に報告する。

②Ｆ社の事例

・Ｆ社では、プロセスモデルＪＩＳ Ｑ ２００１（ＪＩＳ規格）に則った体制の構築を目指している。

・各部門関係会社　　：リスク項目別に「リスクマネジメント年間計画・実施状況レビュー書」を作成。毎月定例の「RM推進会議」に報告する。

・情報の共有　　：「RM会議」を経営企画会議開催時に実施。実施回数は適宜。

・経営監査部　　：ＰＤＣＡのマネジメントサイクルが機能する体制のチェック機能を担って対応。

↓

＜リスクマネジメントシステム維持のための仕組み＞

・能力・教育・訓練　　・シミュレーション

・リスクコミュニケーション　　・リスクマネジメントシステム文書の作成

・文書管理
・記録の維持管理
・発見したリスクの監視
・リスクマネジメントシステム監査

③A社の事例（計測不能リスクへの対応状況）

A社では、ＣＯＳＯによるＥＲＭをめざしており、全社ベースでのＰＤＣＡ勿論のことながら、現場のリスクオーナーによる現場でのＰＤＣＡサイクル実施の定着化を目指している。

・各部門関係会社	：現場ＷＥＢを使用したセルフアセスメントの活用を中核にしてリスク対策実施状況の確認、リスク管理セクション宛報告及びリスク項目・対策の見直しに結び付けようとしている。
・総括部	：リスク管理セクションである現場の総括部は、受領した報告内容の適切性を調査、チェックする。結果は内部監査部門にも報告され、監査部門による現場指導（報告内容の管理体制指導）に連携させている。
・監査部	：ＰＤＣＡのマネジメントサイクルが機能する体制のチェック機能を担って対応。

質問４．導入時の留意事項

導入時の留意事項について、予め把握しておきたいと思っている。

＜回答＞

（１）Ｔ社の事例

①トップ・マネジメントの理解と支持

・トップ・マネジメントの理解と支援を得ることは導入の必須の条件である。しかし、実際にリスク・マネジメント導入の必要性をグループ内に浸透させるのは、プロジェクトチームの役割である。

②社内各部門の理解と協力

・リスク・マネジメントを実際に行うのは各部門、関係会社であるため、最低限、各部門の理解と協力を得ることは導入に際して不可欠である。

・そのため、全部門のキーパーソン（企画担当マネージャークラス）全員の理解と協力を得るように心がけている。

③総合企画部との共同実施

・Ｔ社の「参謀本部」である総合企画部の影響力、情報力、経営感覚を導入に十分活用。

④段階的導入と十分な個別説明

・次の２点に対処するため、Ｔ社では、ステップを踏んだ段階的な導入及び各部門のキーパーソンの理解と協力を得るために個別に十分な説明（体面式）を実施。平成 15 年度（導入初年度の準備期間として位置づけられた年度）では 79 回の説明をおこなった。

（イ）ＥＲＭノ導入は、リスクを「各部門に任せる」ことから、「全社全体として管理する」と言う点でパラダイムシフトを伴うものである。そのため、すぐには理解されにくい面がある。

（ロ）リスクに対する考え方や認識は人により異なっており、「リスクは管理すべき」という一般論ではだれでも同意するが、「リスクをどのように管理すべきか」という具体論になると意見が必ずしも一致しない面がある。

⑤その他

・導入時に３つの基本方針を定め、この基本方針に従って検討を進めた。

（イ）実際に稼動し、継続して機能するよう通常業務の一環として定着させる。

（ロ）可能な限り実施部門の負荷を軽減するとともに、組織は新設せず既存の組織やシステムをできるだけ活用するなど費用対効果を重視。

（ハ）グループ全体の経営管理やコーポレート・ガバナンスへの活用。

（２）Ａ社の事例

①リスクマネジメントの「現場化」が課題

・リスクに向き合っている「リスクオーナー」の自主的な管理意識なくしてＥＲMは浸透しないとの考えに基づいて推進している。リスク管理は、本社部門から「やらされる」のはなく、現場のリスクオーナーが自ら対応していく必要があるという感覚を持ってもらうことを最大の推進目的、課題としている。

②リスクオーナーによるＰＤＣＡサイクル実施の定着化が課題

・リスクマネジメントの「現場化」が推進され定着化することで、本社部門・リスク管理部門・内部監査部門による全社ベースでのＰＤＣＡサイクルに加えて、現場内でのＰＤＣＡサイクル実施、機能の定着化が課題となってくる。

（３）外国企業の事例の事例

「最新実務」（前掲：207 頁）には、８社の事例研究を踏まえた上で、ＥＲM導入を成功させるための「成功要因」として整理した項目を次の通り掲げている。

＜ＥＲM導入の重要な成功要因＞

・上級経営陣（たとえば、ＣＥＯ、ＣＦＯ、ＣＲＯ）から強く、目に見える支持を得ている。
・ＥＲM導入を推進し、運用段階でも後押しし続けるための献身的な機能横断的なスタッフのグループがいる。
・ＥＲMを組織のカギとなる戦略的目的、財務的目的、ビジネスプロセスにしっかりと関連付けている。
・ＥＲMを新規の独立プロセスより、むしろ組織内で既に強固でよく受け入れられたプロセスに対する強化策の１つとして取り入れる。
・社外からの意見を取り込む。
・一歩一歩着実に前進し、「初期の成功」を次のステップへの足掛かりとして活用する。

６．用語

質問１．フレームワークの意味

ＣＯＳＯ－ＥＲＭには、最初に「フレームワーク」という言葉が出てくるが、どういう意味なのか。

・規定なのか。守らないと罰則を伴うのか。規定でないならなぜ「参考に」「準拠」しなくてはならないのか。
・すでに「規定・規則」整っているので、「いまさらそのフレームワークを参考にする必要はない」といわれる可能性がある。
・フレームワークを参考にすることでどんな得があるのか。

＜回答＞

フレームワークはＥＲＭの共通言語、そして導入時の手引きである。

ＣＯＳＯによれば、ＥＲＭプロセスの原則的な考え方やその構成要素を説明するのが、「フレームワーク」である。これを定めることで、ＥＲＭを推進しようとする経営者層から従業員までが、共通の認識と言語をもって、正しくコミュニケーションすることを可能にする。

ＣＯＳＯのフレームワークは、同委員会が１９９２年に公表した「内部統制の統合的枠組み」（Ｉｎｔｅｒｎａｌ　Ｃｏｎｔｒｏｌ－Ｉｎｔｅｇｒａｔｅｄ　Ｆｒａｍｅｗｏｒｋ）に始まる。この報告書では、「統合的枠組み」の意図を次のように述べている。

「内部統制が意味するところは人によって異なる。そして、内部統制についてはさまざまな特徴づけや意味づけが行われ、このことが内部統制についての共通理解を妨げている。かくして、本研究の重要な目標とは、内部統制に関するさまざまな考え方を一つの枠組みに統合し、その枠組みのもとで内部統制についての共通の定義を下すとともに、内部統制を構成する要素を識別することである。」（「内部統制の統合的枠組み　理論編」Ｐ１７ 白桃書房１９９６年）

２００４年、このフレームワークを拡張する形で公表されたのがＣＯＳＯ-ＥＲＭフレームワークであるが、これについても同様の位置づけが述べられている。

このように、フレームワークはＥＲＭ活動を規定または規制する決まりとしてではなく、円滑に進めるための共通の指針として、事業体の実情に応じて柔軟に活用するものと考えるのが本来であろう。ＥＲＭという概念は、従来のリスクマネジメントよりも広く深い。全社で一斉に取りかかるのはよいが、新しい概念の導入には往々にして認識や解釈の違い、理解不足や誤解といった混乱が生じ、それが推進を阻害することにもなりかねない。フレームワークはそのような「リスク」を低減し、推進にあたっておさえるべき観点、踏むべきステップを紹介するものである。

なお、「フレームワーク」という語そのものは、「枠組み」という意味合いどおり、様々な概念や考え方に一定のまとまりを持たせる型のようなものと言える。従って、「ＣＯＳＯ-ＥＲＭフレームワーク」に限らず、欧米のＥＲＭ先進企業では、それぞれ独自の「ＥＲＭフレームワーク」を持ち、

また異なるシーンでも、「フレームワーク」の語は使われる。たとえば「リスクフレームワークは、組織のすべてのリスクを突きとめ分類することを可能にするマスター・リストなのである」（「戦略的事業リスク経営」ポール・Ｌ・ウォーカー他、東洋経済社２００４年）。

質問２．用語の解説

１．事象の識別

⇒企業が、その目的達成の途上で起こり得る様々な事柄を想定し、それらを「リスク」と「ビジネス機会」とに分類、評価すること。

ＣＯＳＯのＥＲＭモデルでは、まず「目的の設定」というプロセスがあり、次に「事象の特定」というプロセスが続く。ここでは、事業体がその戦略を実行したり、目的を達成したりしようとするときに、それらに影響を与え得る様々な潜在的な事象を、内部要因・外部要因あわせて特定する。そしてそれぞれの事象は、さらにマイナスの影響をもたらすもの（いわゆるリスク）と、プラスの影響をもたらすもの（ビジネス機会）とに識別される。この考え方が、ＥＲＭを従来のリスクマネジメントとは大きく異なる、企業価値向上のためのリスクマネジメントたらしめている。

２．上方リスクと下方リスク

⇒リスクは、損失にもなればチャンスにもなる。

「リスク」と言えば、「危機」あるいは「会社にとっての損失」というイメージがこれまでは一般的であった。リスクマネジメントが、自然災害や労働災害、事件・事故の発生に対する「クライシスマネジメント」を指す企業も多いのではないだろうか。

これに対して、最近の概念では、リスクはリターンの源泉にもなるととらえられる。たとえばＩＴの革新スピードに乗り遅れれば、既存のサービスモデルや業務プロセスはきわめて非効率なものとなるが、先行すれば競争優位を得ることにもなる。

しばしば、企業トップは「危機をチャンスに」と言う。企業が存続の危機にあれば、事業体の縮小というリスクを負ってでも存続可能な強固な経営体質を求める。より成長を目指すなら、新たな分野への投資のリスクを負って新規事業を立ち上げる。リスクは放置すれば企業の存続をおびやかす一方、新たなチャンスを産み出す源泉ともなる。これを「事象の不確実性」といい、厳密には、事業活動にマイナスの影響を持つものをリスク、プラスの影響を持つものはビジネス機会として区別する。

３．リスク選好

⇒リスクは、とるもの。

前記のようなリスク概念の変化によって、リスクは回避すべき危機から、むしろ選択してリターンを追求すべきものとなった。

企業は戦略目的に沿って、事業目的に照らして、数あるリスク（上方リスクも下方リスクも

ある）の中から、どれを選ぶかが、リスク選好である。

ただし、無制限にリスクを抱えるわけにはいかない。そこで企業は、どれだけのリスクを許容できるかを測定し、その範囲内でリスクをコントロールする。その範囲の限界は、リスク許容度という。

ちなみに保険業界でいう「リスク選好度」とは、顧客が「どれだけのリスクをもつ投資を好むか」であり、「リスク許容度」とはその顧客が「どの程度のリスクを負えるか」である。

４．固有リスクと残存リスク

⇒固有リスクーＥＲＭ＝残存リスク

固有リスクとは、企業が「何もしない状態で抱えているリスク」、つまり、どのような影響度を持つリスクが、どのような発生頻度で存在するかを分析し、その結果に応じて対策を検討し、実施するというプロセスを何もとっていないものとして存在するであろうリスクをいう。他方、残存リスクとは、それらのプロセスを経て対応してもなお残っているリスクを指す。

ＥＲＭでいう「事象」には、日常的に識別されているものもあれば、潜在的に存在するものもあり、どのような影響をもたらすか予測し難い。経営は、これらからくる不確実なリスクも想定しなければならない。そこで、まず固有のリスクを、後には残存リスクを、両方ともに検討していくことになる。

５．ポートフォリオ

⇒リスクとリターンのトレードオフ

資産運用の世界では、様々な金融商品の中から、自己の目的に応じて各種を組み合わせ、全体でリスクを抑えつつ、高収益を目指そうとする。この「組み合わせ」がポートフォリオである。

企業は、価値創造のため、また価値の保全のためにリスクを受け入れ、リスクには相応のリターンを期待する。ＥＲＭは、リスクを相互関連性や連鎖の関係もとらえ、トータルとして、リスクを軽減し、また機会をとらえようとするものである。

７．その他

質問１．ＥＲＭの限界

ＥＲＭの限界について教えてほしい。

＜回答＞

ＥＲＭは、事業目的達成の精度を上げる。しかし、それは正確には「合理的な保証を与える」ものとされる。つまり、絶対的に保証するものではない。

ＥＲＭはすでに述べたとおり、事業体の目標に照らし、リスクを特定し、測定し評価し、管理し、監視して見直されるというステップを経ていく。このプロセスが機能しているとき、何も行わない場合に比べて、事業体の目的達成の確率はまちがいなく高くなる。

しかしリスクを「不確実性」と見ることは、誰もがそれを完全には予測し得ないという考え方を示すものである。また、ＥＲＭは経営者や取締役会の誤謬までを管理できない。

たとえば、リスクの識別や評価・分析での選択や判断の誤りにより、意志決定そのものを誤ってしまうこともあれば、費用の制約から初めから不十分な管理方法を選択することもあり得る。また実際の管理（コントロール）の段階では、関わる人間の単純ミスやまちがいも起こり、あるいは複数の人間が共謀すれば違反や不正はそれだけたやすい。さらには、いかなるリスクマネジメントシステムを構築しようが、経営者や取締役会がこれを無視することもできる。

ＥＲＭの効用は、これらの事情に左右される。ただ、これらはＥＲＭの限界であると同時に、企業風土や経営理念の問題であると言えよう。

第２部　リスクマネジメント全般に共通する質問

１．リスクの定義

質問１．リスクの定義

リスクマネジメントで対象としている「リスク」とは何か。

＜回答＞

リスクとは、**目的達成にマイナスの影響を及ぼす事象が生じる可能性**である。

なお、目的達成へのマイナスの影響を相殺したりビジネス機会をもたらすなど、目的達成にプラスの影響を及ぼす事象が生じる可能性は「機会」と呼ぶ。

☞参考：様々なリスクの定義

①リスクとは、**経営目的、事業目的の達成を妨げる可能性がある要因**である。

【A社「リスク管理マニュアル」】

②リスクとは、事業**目的の達成に影響を与える要因**のことである。上向きな（チャンスをもたらす）積極的なリスクと、下向きな（好ましくない結果をもたらす）消極的なリスクがある。

【B社「リスク管理の方針とガイドライン」】

③**事態の確からしさとその結果の組合せ**、または、**事態の発生確率とその結果の組合せ**。ある状況では、**予想との乖離**のこと。

【日本工業標準調査会「ﾘｽｸﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑ構築のための指針ＪＩＳ Ｑ ２００１」】

④リスクとは、**目的を達成**することを**妨げる**かもしれない**もの**。

【Larry Hubbard「統制自己評価：実践的ガイド」】

⑤リスクとは、組織の**目的達成を妨害するかもしれないもの**である。

【Larry Hubbard「統制自己評価：実践的ガイド」】

⑥リスクは、**不確実性（可能性）の尺度**としての概念である。ビジネス･プロセスの脈略において「不確実性」という場合には、組織**目的達成がどのように左右されるか**が問題となる。

【David McNamee「ビジネスリスク評価の実務」】

⑦リスク：**不確実性の尺度**。ビジネス･プロセスでは、不確実性は、組織的な**目的の達成に関係**する。

【眞田光昭訳、David McNamee「ビジネスリスク評価の実務」】

２．リスクと関連領域との関わりや相違点

質問１．危機対応との違い

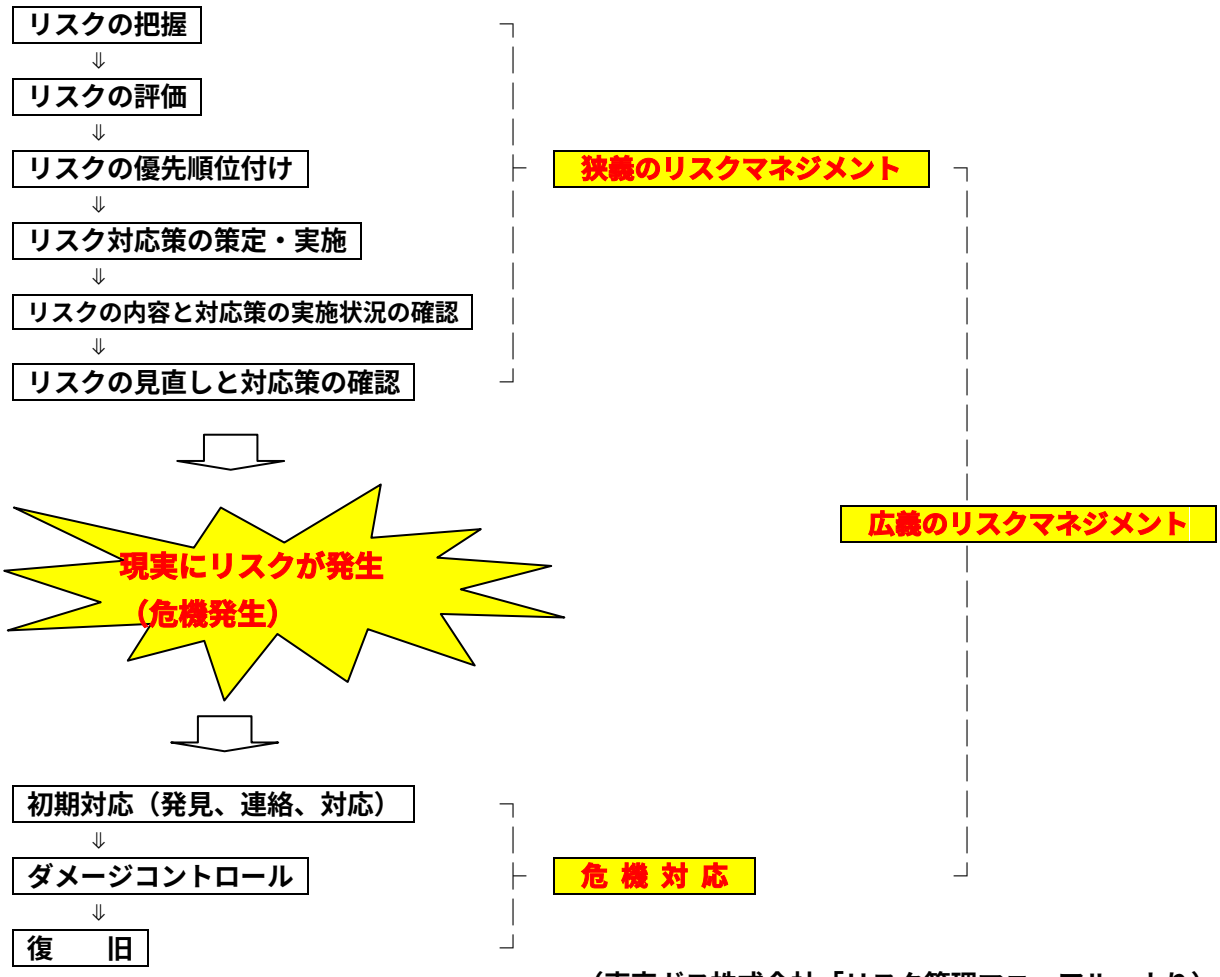
「リスクマネジメント」と「危機対応（クライシスマネジメント）」との違いは何か。

＜回答＞

本来、リスクマネジメントはリスクに関するあらゆる事象を取り扱う広い概念であるため、現実にリスクが発生した時の対応（アクション）である危機対応（クライシスマネジメント）**を**当然**含む**。

しかし、ＥＲＭではリスクマネジメントを所管する部署が必ずしも、危機対応を所管する部署ではない場合もあることから、**リスクの発生防止までの段階とリスク発生時の対応策の事前検討**を扱うことを（狭義の）リスクマネジメントとし、**現実にリスクが発生した時の対応（アクション）**を扱うものを危機対応とする場合もある。

具体的には以下のとおり。



（東京ガス株式会社「リスク管理マニュアル」より）

質問２．リスクマネジメントと日常の業務管理や目標管理との違い

リスクは「目的達成にマイナスの影響を及ぼす事象が生じる可能性」であるから、リスクマネジメントは日常の業務管理や目標管理と同じことを目指しているように見える。なぜ、日常の業務管理とは別にわざわざ手間をかけてリスクマネジメントを行なう必要があるのか。同じことを２度行うことになり、無駄なように思える。リスクマネジメントと日常の業務管理や目標管理との違いは何か。

またリスク対応策は、各部門の政策課題そのものである場合も多く、リスクマネジメントと政策課題推進との違いが解りにくいが、社内でどのように説明すればよいのか。

＜回答＞

リスクマネジメントと、日常の業務管理や目標管理との違いは、以下の３点である。

①企業全体の経営に重大な影響を及ぼす**重要リスクを整理してハッキリ**させたこと。

②リスクマネジメントの**ＰＤＣＡサイクル**が確実にかつ継続的に回るよう**定期的にフォロー**する仕組みを作ったこと。

③リスク管理水準のバラツキを小さくし、**企業全体として一定の管理水準**となるよう**全社統一のルール**を作ったこと。

それによって、目標達成に向けたビジネス活動が、企業全体として一定の水準を保ちつつ、確実に行なわれるようにすることを目指している。つまり、リスクマネジメントは、**日常の業務管理や目標管理が確実に行なわれることを補完し、助けるための全社統一の仕組み**なのである。

質問３．「リスクマネジメントのモニタリング」と「リスクマネジメントの監査」との関係

リスク管理部門が行う「リスクマネジメントのモニタリング」と内部監査部門が行う「リスクマネジメントの監査」との違いは何か。

＜回答＞

（１）原則的には

主な相違点は、**実施主体**が、「リスク管理部門」であるか、それともリスク管理部門から独立した「内部監査部門」であるかの違いである。

実施内容は、様々であるが、元来は、両者の実施事項は基本的には同一である。一例を述べると、①各部門における「リスク内容の確認と見直しの状況」、および、「リスク対応策の実施状況の確認と改善の状況」について報告を受け、内容を確認し、②それらの適切性および有効性を検証・評価し、③結果を改善のために各部門にフィードバックすると共に、④経営に報告する、というプロセスを実施することが多い。

（２）実務上は、

ａ）リスク管理部門が行う「リスクマネジメントのモニタリング」

しかし、実務上では、は、①リスクマネジメントが有効に機能するよう促進する立場であり、リスクマネジメントを推進することをミッションとするリスク管理部門が、自ら推進したミッションの結果を「監査」することは、監査の独立性を損なう可能性があること、②リスクマネジメントのＰＤＣＡサイクルが確実にかつ継続的に機能させるために、モニタリングを年１回程度は全部門で行うことが求められることが多く、そのため時間的・人員的制約が厳しいこと、および、③監査部門ではないリスク管理部門がどこまで報告内容に立ち入った検証を行うことが可能であるかという権限上の問題があること等の問題がある。

そのため、リスク管理部門が行う「リスクマネジメントのモニタリング」は、各部門からの報告内容が正しいことを前提として受け入れることが多く、リスクマネジメントの**適切性および有効性を検証・評価することまでには踏み込むことは少ない**のが現状である。

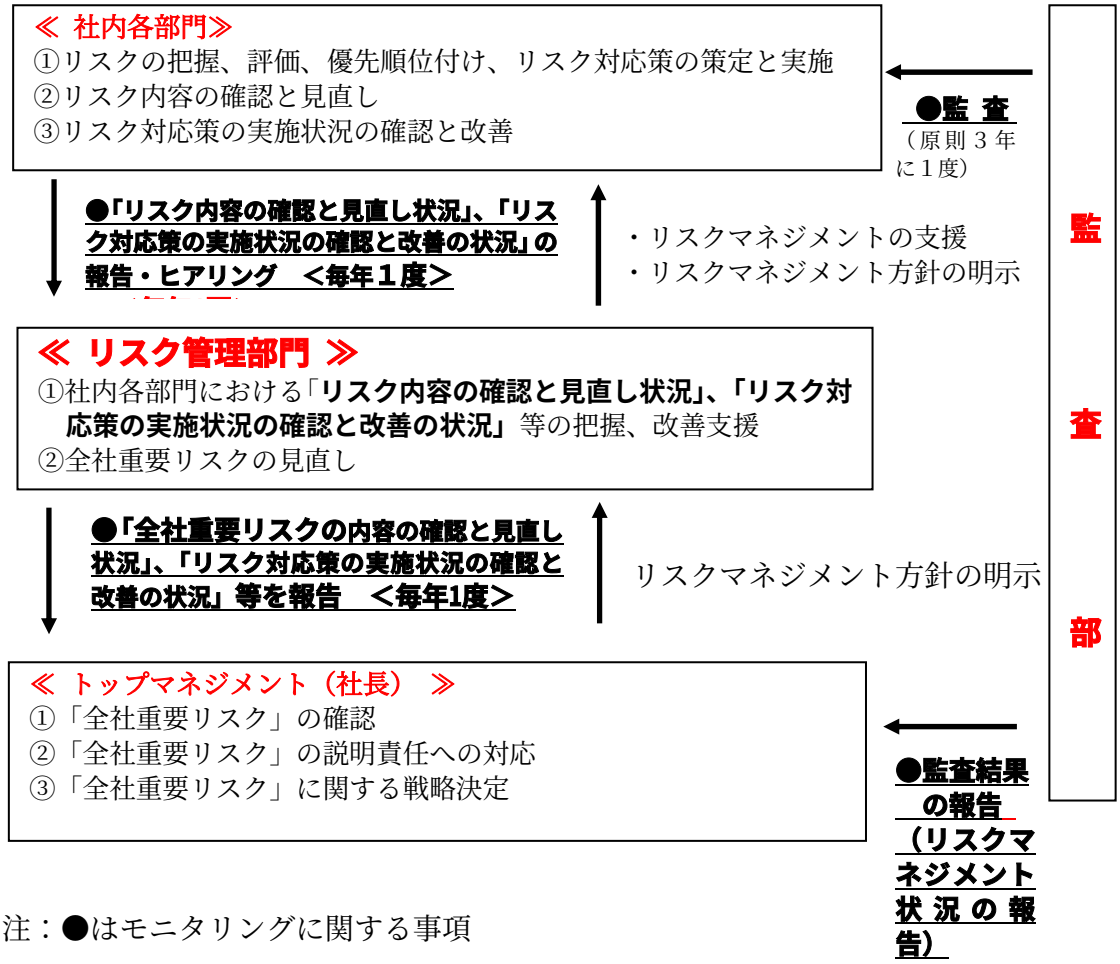
ｂ）内部監査部門が行う「リスクマネジメントの監査」

他方、内部監査部門は、実施は数年に一度である場合が多く、一定の監査能力を有した監査人により実施される。そのため、内部監査部門が行う「リスクマネジメントの監査」は、報告内容について独自の立場で確認・検証を行い、リスクマネジメントの**適切性および有効性について独立した第三者の立場で検証・評価を行う。**

＜参考＞

「リスクイマネジメントのモニタリング」と「リスクマネジメントの監査」との関係（リスクマネジメントのＰＤＣＡサイクルのイメージを含む）

概要を、東京ガス株式会社２００４年３月期有価証券報告書で『内部統制システム及びリスク管理体制整備の状況』として開示。



注：●はモニタリングに関する事項

３．リスクの評価・分類の手法

質問１．リスクの分類方法

リスクを調査した結果、数多くのリスクが報告されたが、当社にとって重要なリスクをどのような形で分類・整理すればよいのか。
各種書籍で紹介されているリスクの分類方法を使ってみたが、どうも自社の事業特性にフィットした分類が見つからない。自社の事業特性に応じたリスクの分類方法を教えて欲しい。

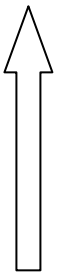
＜回答＞

リスクの種類や重要度は業種、企業により様々であるため、一般的な分類方法では適切な分類は適用できない場合が多く、**自分達で作り上げるより他はない**のが実情である。

一例として、まず、**報告された個別リスクから、小分類⇒中分類⇒大分類へと分類**し、いわば「報告ベースでの分類」を実施し、次に、試行錯誤と議論を重ねながら、自社に適した分類を探求する方法がある。ポイントは、**経営上の重要度合、業務特性とのつながり、社内での理解のしやすさ**等である。

＜参考＞　リスク分類のイメージ

＜例＞大　分　類：　災害・事故等リスク
中　分　類：　自然災害リスク
小　分　類：　地震リスク
報告件名①：　地震による工場設備の損壊リスク
報告件名②：　地震による輸送設備の損壊リスク
報告件名③：　地震による事業用建物の損壊リスク



報告された個別件名のリスクから、小分類⇒中分類⇒大分類へと分類して行く。

質問２．リスクの大きさの評価方法

リスクは、その大きさによって、重要かどうか判断される。それでは、リスクの大きさはどのように評価するのか。

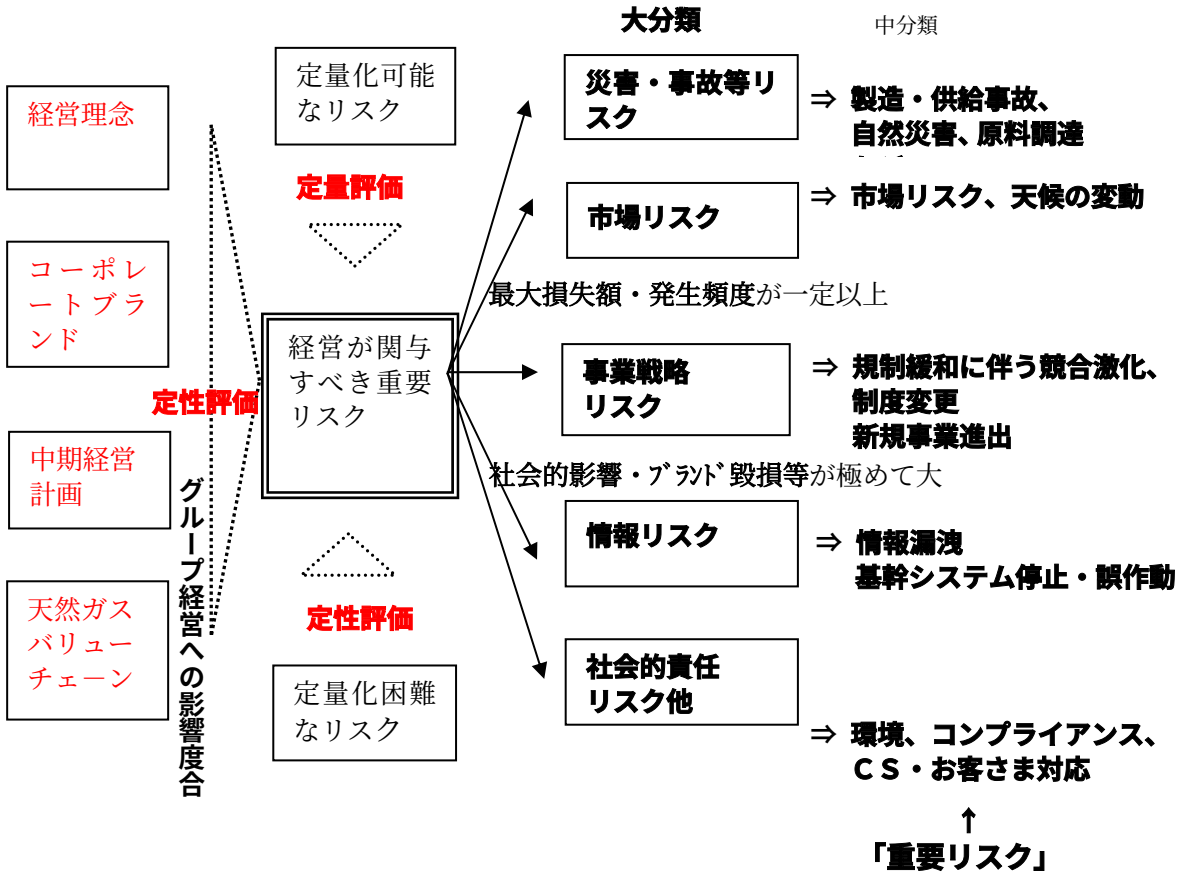
＜回答＞

一般的には、「リスクの大きさ」＝「影響度（損失の大きさ）」×「発生確率」で考え、縦軸＝影響度、横軸＝発生頻度としたリスクマップ上にプロットして評価する。

まず、**定量評価可能なリスク**は可能な限り**定量化**し、定量化結果に基づくリスクマップを作成する。

次に、**定量化が困難なリスクや、定量評価のみでは不十分なリスク**は、社会的な影響度（風評等）、ブランドイメージの毀損度合、経営理念・経営計画・ブランド戦略への影響度などを**定性評価**し、リスクマップの位置を修正する。修正の際には、各リスクの相対的な位置関係を考慮する。

＜参考＞　リスク評価のイメージ　（重要リスク抽出フローのイメージ）
重要リスクは、東京ガス株式会社２００４年３月期有価証券報告書で『事業等のリスク』として開示。



III．応用編

１．リスク管理部門の役割

質問１．実施状況をモニターする方法

リスク管理部門がグループ全体（本社を含む社内各部門および関係会社）のリスクマネジメントの実施状況をモニターする方法として、どのようなことが考えられるのでしょうか。

＜回答＞

外部環境や組織自体の変化に伴いリスクは不断に変化しています。リスクマネジメントの有効性も時々刻々変化するものであり、これを適切なレベルに維持するためにはモニタリングが必要です。

COSO の ERM フレームワークによれば、リスクマネジメントのモニタリングは次の２つの方法を通じて実施されます。

- 日常的に実施される継続的モニタリング
- 独立の評価活動

日常的に実施される継続的モニタリングは、予測と実績報告との乖離、外部関係者とのコミュニケーション、内部／外部監査人の活動、社内ミーティング等による情報共有、等を通じて、リスクマネジメントの適切性を検証するプロセスです。例えば月次の延滞債権の状況をモニタリングは与信手続変更が引き起こす問題点の適時な把握に役立つでしょう。また顧客クレームのレビューは、会社が提供する製品やサービスの品質変化の適時な把握に役立つでしょう。これらは日常業務に埋め込まれた手続であるため、問題点の摘出と対応がより迅速に実施されます。

しかし日常的モニタリングだけで何もかもが解決するわけではありません。例えば全社を挙げて国内の競合他社との間での売上順位争いとこれに関連するモニタリングに集中している間に、ひょっとしたら市場において海外や異業種からの参入といった重大な変化がしょうじているかもしれません。会社がこうした変化を見過ごしてしまったならば、近い将来に深刻な事態に直面することになります。

日常的に実施される継続的モニタリングが、その時々に全ての重要な問題点をカバーしているかを確かめるためには、独立の評価活動を随時実施することが必要となります。具体的な内容としては、自己評価／内部監査、実際の ERM 実施担当者との討議を通じて実態を把握し有効性を評価する、チェックリスト／質問書／フローチャート／ベンチマーキング等の利用、等があります。

質問２．モニター結果を経営トップへ報告する方法

リスク管理部門がモニターした結果を経営トップに報告する方法として、どのようなことが考えられるのでしょうか。

＜回答＞

経営トップは組織のリスクマネジメントの有効性について最終責任を負う立場です。その責任を遂行していくためには、これに役立つ情報の供給が不可欠です。こうした情報のとりまとめと報告は、リスク管理部門の重要な役割です。

経営トップに報告する場合には、短時間に全体像を把握できるように、できるだけ要約され、図表化されていることが求められます。例えば、ＣＯＳＯのＥＲＭツール編では、リスクの大項目毎に許容度との相対的大きさと前四半期からの増減とを矢印の向きと色使いにより簡便に示すダッシュボード報告について紹介されています。（COSO ツール編図表 8.11 ダッシュボードレポーティングより）。この例では気になるリスク項目について更にドリルダウンできる仕組みも提供しており、これらは併せて短時間に必要な情報を入手したい経営陣にとって有効なアイデアといえます。

２．リスクの数値化

質問１．リスクを測定・評価する基準や尺度は？

金融リスクや市場リスクを除いた事業会社におけるオペレーショナルなリスクの影響の大きさを測定･評価する共通の基準や尺度として、どのような基準や尺度が考えられるのでしょうか。

＜回答＞

ポイント

- リスク評価の目的によって基準や尺度は様々である
- リスク事象発現の影響度、例えば経済的な損失額や、対応組織のレベル、顧客、風評に対するインパクト、許認可を受けるビジネスであれば、行政からのペナルティーの程度、といった視点により３～5 段階の基準を設けるケースがある

金融リスクや市場リスクについては、VaR などの計量手法が一般的に利用されている。一方でオペレーションマネジメントの一部は良品率、稼働率の観点から客観的な計量が可能であろう。このようなリスクは、定量可能リスクとして、事業会社でも取扱われている。しかしながら、経営意思決定プロセスに関わるリスクやコンプライアンス、競合他社や顧客の嗜好の変化など多くは、金融リスクや市場リスクのように客観的に計量することは困難である。このような定量不可能リスクとして認識されるリスクについては、計量困難なリスクとして何もしない、ということは企業経営に与える影響度が、計量可能なリスクを超えるケースが多い点からも望ましいことではない。現在では、CSA（コントロールセルフアセスメント）や RCSA（リスクコントロールセルフアセスメント）というプロセスを通じて、計量困難なリスクに対し、リスク定義やリスクシナリオの共有化を組織的に図り、企業価値に与えるインパクトを３～５段階の基準に従って評価する、という手法が定着しつつある。欧米の金融機関においても、オペレーショナルリスク計量手法の一つとしてこのようなアプローチを採用し始めている。

企業価値に与えるインパクト、つまり、影響度や重要性と認識される程度に対しどのような基準を用いるかは、リスク評価の目的に応じて様々である。リスク評価の目的は、全社単位、部門単位、ビジネス単位、といった組織のレベルの差や、特定のリスク、例えば、業務プロセス、コンプライアンス、財務といった特定のテーマに対するリスク毎での評価、商品や製品の安全性、のようにプロダクトベースでの評価が考えられる。統合的リスクマネジメントにおいては、リスクの影響度や発生可能性に応じて、優先度の高いリスクを特定し、特定されたリスクに対し、更に細分化された観点でリスク評価を実施する、というプロセスを辿るため、影響度の軸は、リスク評価の目的に応じて、具体的な基準の記述は異なる。一方で、このような目的の違いはあるものの、経済的な損失額や、対応組織のレベル、顧客、風評に対するインパクト、許認可を受けるビジネスであれば、行政からのペナルティーの程度、といった視点により検討すべきであろう。

リスクの測定・評価において注意する点は、洗練度の高低に関わらず、測定結果は常に何らか

の仮定やシナリオに基づいていることを忘れないことである。例えば最も洗練された計量手法の一つである VaR も、エクスポージャーの前後にエクスポージャーの認識を誤らせるようなオペレーショナルリスクを抱えている場合には、VaR として認識されているリスク額に留まらない損失をもたらす事は、大和銀行事件やベアリングス証券などから明らかである。一方で、オペレーショナルリスクを必要以上に厳密に計量することは、リスク管理上の費用対効果を悪化させるリスクがあるため、目的の明確化をした上で充分に検討する必要がある。リスクの測定・評価手法の選択すらも企業経営戦略の一つであると理解することが企業の有機的な ERM に向けたステップとして重要である。

質問 2. 前提条件やシナリオの設定の仕方

数値化するためには、前提条件を作ったり、一定のシナリオを描くことが必要だと思いますが、前提条件やシナリオの作り方によって、リスクの計算結果は大きく変化すると思われます。シナリオを作る時の考え方と、使用するシナリオについてどのように相手と合意しているのでしょうか。

＜回答＞

ポイント

- リスクシナリオは、紐つけられたリスクが発現するシナリオを、リスクの原因と結果に具体的に記述し作成する
- リスクは「点」でなく「範囲（レンジ）」で認識する必要がある
- リスク評価プロセス、つまり「リスクの網羅的洗い出し」「プロセスの把握」「シナリオ作成」「リスク評価の実施」等の手順を踏むことでリスクの共通言語化が進みシナリオに対する合意が図られる
- 影響度と発生可能性の要因を総合的に評価することで、相手との合意が得られやすくなるケースもある

リスクに対して漠然とシナリオを作成する、ということは非常に非効率な作業であり、かつ期待された効果はほとんど得られないだろう。一般的に、組織全体のリスク評価のためには、リスクの網羅的な洗い出しと、プロセスの把握、シナリオ作成といった手順を経由する。

リスクの網羅的な洗い出しは、コンサルタントから提供されるリスクモデルや監督官庁のガイドライン、チェックリストが参考になるが、あくまでも網羅性を確保するための参考とし、企業独自のモデルと定義をすべきである。また、このモデルと定義を組織の共通言語とする意識で合意形成を行うことが重要である。

プロセスは業務プロセスに留まらず意思決定プロセスについて組織としての認識を共有することが必要である。リスクの定義作成とプロセスの認識の共有は、リスクの共通言語化と適切なリスクシナリオ作成の鍵となる。

シナリオ作成は、評価対象のリスク毎に実施されるケースが多いと思われるが、留意点としては、リスク毎にできるだけ多くのシナリオを、多数のリスク評価者から募ることとシナリオはリスクの原因と結果を明示した形で作成することである。プロセスの認識を共有することでリスクシナリオの水準は向上し、計量の際、必要となるリスクドライバー特定も容易になる。

このような過程を経てリスク評価を実施した場合には、リスクの共通言語化が進むため個々人のリスク評価の違いに対し、効果的、効率的な意見交換が可能となるケースが多いようだ。しかしながら、ワークショップによるリスク評価やアンケート形式による場合、統計的な計量手段による場合、どのような手段を利用しても、特定のリスク中の複数のシナリオが全く異なる評価となってしまう、ということは生じ得る。リスク評価において重要なのは、リスクはそもそも１点で認識するものではなく範囲や分布で認識すべきものである、ということである。従って、例えば 5 段階で評価されたリスクのポジショニングを示すリスクマップで、重要性が 4.5 で発生可能性が 2.5 と評価

されたリスクであっても、その数値は分布の平均値に過ぎない、ということである。その分布のどのレベルで評価すべきか、について絶対的な正解はない。そもそも、優先対応が必要とされるリスクの抽出においては、影響度と発生可能性を総合的に判断することが求められるからだ。

それでは、リスクマップ上で分布として表現されるべきリスクを一つの点で表現する場合はどのように考えるべきであろうか。一つの考え方として、外部環境に大きく依存し、自社が積極的にコントロール困難なリスクは、最悪の状況を想定する、という評価のアプローチは金融機関が VaR を 99%の信頼区間を利用するケースが多い点で妥当な判断ではないかと考えられる。重要な点は、特定の個人ではなく、組織がそのような評価の前提となる仮説を充分認識していることと、その仮説が有する評価結果の限界を理解していることである。一方、企業内部でコントロール可能なリスクは、必ずしも最悪のケース、と考える必要はないと思われる。企業が自社内でコントロール可能なリスクであるかそうでないか、という側面に加え、リスク管理能力や内部統制状況を合わせて分布上のどの点で考えるかについて検討をするべきであろう。COSO ERM においては、リスクを固有リスクと残存リスクの双方で評価することを前提としている。つまり、残存リスクを評価する際に、リスクに対するコントロール状況評価は必要不可欠なプロセスである、という点を認識した上でリスク評価を実施することが求められる。

質問 3. リスクの影響度合いをどの範囲まで見るか

・ リスクの影響度合を数値化するためには、直接的な影響までなのか、評判など間接的な影響まで含むのか等、リスクの影響度合をどの範囲まで見るかによって、リスクの計算結果は大きく変化すると思われます。(悲観的に考えていたら無限大になることさえあります。) リスクの影響度合をどの範囲まで見るかについてお考えを教えてください。

＜回答＞

ポイント

- リスクの影響度はリスク定義やリスクシナリオに忠実に計量されるべきである
- リスクシナリオが重層的に原因と結果を有している等、シナリオ作成上の問題が生じないよう、論理的かつ具体的なシナリオ作成が求められる
- リスク間の因果関係分析等が別途実施される等リスクマネジメントの PDCA サイクルを評価者に充分説明し、過度な因果関係の取り込みは不要であることを理解させることが求められる

リスク評価がリスクシナリオから導き出される、という点から考えると、影響度合いの範囲を特定する際にシナリオの巧拙が大きく影響してくることは容易に想像されえることである。リスクシナリオはリスクの源泉とリスク発現（事象）との組み合わせで作成されるが、仮に、リスクの源泉とリスク発現（事象）の間にいくつかのリスクの源泉と発現が暗黙のうちに内在している場合には（つまり、風が吹けば桶屋が儲かる、の状況）このような問題が生じる。この場合には、源泉として想定されているリスクによって直接の影響となるリスク事象がどのような影響を持つのか、という、観点で影響度を評価すべきであろう。つまり、リスク評価はリスクシナリオや複数のリスクシナリオの代替であるリスク定義に忠実に計量されるべきである、ということである。リスク定義やシナリオは、リスクの原因とその結果生じる事象が直接の因果関係を有した形で作成され、事象が生じたときの影響度や重要性、発生可能性を評価する。もし、リスクの原因とその結果生じる事象の間に、更に様々な原因と結果が重層的に存在してしまうと、質問のような問題が顕在化する。

もう一つの考慮すべき点として、リスク評価を実施する際、リスク評価がリスクマネジメントの PDCA サイクルの一部であることを評価者に理解してもらう点が重要である。リスク評価実施後に、リスクに対しては、どのようなケースで発生し、他のリスクとどのような関連が生じるのか、そして、効果的な対策を採るには (つまり、複数のリスクの源泉となるプロセスに対する効果的な対処) どのようなアクションプランを立てるべきなのか、というプロセスが待ち構えていることを理解してもらう必要がある。リスクが有する相互関連性を、インフルエンス・ダイアグラムや特性要因図等を利用して分析し、複数のリスクの源泉について理解する、というプロセスは一般的にリスク評価の後に実施されるため、リスク評価の段階では、リスク定義やリスクシナリオから乖離しない程度にリスクの影響度合いを考える、ということが賢明なアプローチであろう。

質問 4. 金額換算する対象や範囲

金額換算するリスクは、保険を含めた金融面でのリスクや市場リスクなどもともと金額換算が馴染むリスクに限定されているのでしょうか。それとも、競争相手や業務の中断など金額換算が行ないにくいと思われるリスクも含めた企業を取り巻く全てのリスクを金額換算されているのでしょうか。もし、そうであればどのような方法で金額換算されているのでしょうか。

＜回答＞

金額換算がリスク評価基準の全てではないが、できるだけ金額的イメージを持つことはリスクマネジメントに対するモチベーションを向上させる上で有効である。計量のアプローチは、想定可能なリスクシナリオをいくつか作成し、シミュレーションを実施する、というのが一般的手法と思われる。計量結果の評価への適用は必ずしも精緻である必要はなく、一桁単位の違い、つまり、1 億以上、10 億以上... を認識できれば充分としているケースが多いようである。いずれにせよ、計量に利用したリスクドライバーの仮説を文書化し、組織的な理解を共有することや、継続的にリスクシナリオの適用や状況変化に応じた見直しができるプロセスを有することが重要である。

質問 5.「数値化したリスク」と「通常の経営目標数値・経営指標」との関係

「数値化したリスク」は、「通常の経営管理で用いられる主要な経営目標数値や経営指標」と同じものとなり、結局、「リスクマネジメント」は「通常の経営管理」と同じことを二重に行なっていると言われる可能性があります。前者（数値化したリスク）と後者（主要な経営係数）との関係はどのように考え、区別すればよいのでしょうか。

＜回答＞

「数値化したリスク」は会計上の項目、例えば信用リスクであれば売上債権、といったように財務諸表上の数値がベースになるケースがあることは事実である。しかしながら、財務諸表上の数値が、例えば引当金のように損失や発生することが合理的に見積もられるものでなければ財務諸表上表面化しないのに対し、倒産確率などを基礎とした社内格付けによってリスクウェイトを特定し加重平均した信用リスク額は、信用リスクの大小を合理的に判断することを可能とする。例えば、これまでは、業界トップ企業に対し 10 億円の売上債権とその他、低格付け企業に 5 億円を有していたが、競合他社に抜かれ業界トップ企業の売上債権は 5 億円に低下、その穴埋めとして低格付け企業に裾野を広げて 7 億円まで売上債権を拡大した、といった場合を想定する。仮に業界トップ企業のリスクウェイトが 0.1%であった場合には、この企業の信用リスクは売上債権額の減少とは裏腹に高まったことになるだろう。

これまでの経営指標は往々にして財務会計や管理会計上の限界の上で成り立ってきた。もちろん、今後将来も重要な経営情報である点では変わらない。しかし、経営環境に対する不確実性が高まる中、企業戦略実現のための「高い能力水準」が求められる時代である。前述の信用リスクのように、より経済的に価値のある情報を入手することは、「高い能力水準」達成の一つの成功要因となる。一方で、従業員の活動ベース、顧客の満足度調査等のように、財務的な調査からは入手困難な情報収集により、企業活動の方向性と実績の乖離を検証することも、「高い能力水準」達成の成功要因として重要である。これらの中には、企業が既に対応済みの活動も含まれるが、「機会」の探索のために利用するだけでなく「リスク」管理のために利用することが ERM において必要となるだろう。財務諸表の数値自体や、数値に表れづらい情報にもリスクの側面から「高い能力水準」を意識して経営管理に当たることは、従来からの企業の改善、改革の活動の延長線上にあるものと考えるべきであろう。

３．「各部門における自主的なリスク管理のＰＤＣＡサイクル」の設定方法

質問 1. 自主的なＰＤＣＡサイクルを設定・維持する方法

ＥＲＭの目的の一つとして、「自社の全域の日々の業務の中で各部門の管理者（部長・マネージャークラス）が自主的に、リスクを見つけ、評価し、対応策を策定し、モニターし、改善し、その結果を上層部へ報告するというリスクマネジメントの自主的なＰＤＣＡサイクルを設定し、機能するように維持する」ことが言われていますが、各部門の管理者がどのようにしたら自主的にこのような活動を遂行できるようになるのでしょうか。

＜回答＞

ERM の全社レベルの取組みを、組織の個別部門へ落とし込むには、トップのコミットメントが不可欠である。リスクマネジメントに限らず、TQM（Total Quality Management）等全社での取組みにおいて、トップの明確なコミットメントは必要不可欠かつ最大の成功要因であるといえる。過去 TQM 活動が、年月を経た結果、現場の分散的な QC 活動になってしまった、という話を聞くことがある。全社的な取組みは継続的かつ膨大なエネルギーを要するため、いったん定着したといっても、トップが継続的に支援しない限り継続することは困難である。

各部門の管理者がリスクマネジメントに自主的に取組むためには、その必要性を認識することが第一歩であるが、リスクに対する気づき、「感性」は、個人差が大きいため、啓蒙活動が重要になる。リスクシナリオ作成のプロセスは、シナリオライティングの手法を用いることで、リスクに対し能動的に思考する過程で気づきを促す効果があるため、啓蒙活動に組み込むことも有効である。日々の業務に忙殺される現場の管理者は、組織が意識的にこのような時間を取らせる必要があろう。また、リスクマネジメント上の問題点の提起や、改善活動の成果に対する、人事的インセンティブ、具体的には、人事考課項目への取りこみも組織が支援するリスクマネジメントに対する個人的リスク感性向上に寄与する。このような組織的支援が無ければ、個人のリスク感性の向上を長続きさせることは困難であろう。

個人の鋭敏なリスク感性とトップのイニシャチブによる組織的な取組みはリスクマネジメントの組織内部の人的側面の両輪であり、自主的な活動への動機付けを促す基礎といえよう。