全社的リスクマネジメント（ERM）構築の必要性

The Need for Building Enterprise Risk Management (“ERM”)


矢野 昌彦
Masahiko Yano
三菱UFJリサーチ&コンサルティング
コンサルティング事業本部東京本部
マネジメントシステム部
部長
General Manager
Management System Consulting Dept.
Corporate Strategy Consulting Division


堀口 勉
Tsutomu Horiguchi
三菱UFJリサーチ&コンサルティング
コンサルティング事業本部東京本部
マネジメントシステム部
チーフコンサルタント
Chief Consultant
Management System Consulting Dept.
Corporate Strategy Consulting Division

1992年米国において不正経理をきっかけに内部統制の枠組み（COSO：トレッドウェイ委員会組織支援委員会）が発表され、2004年にはCOSO-ERMとしてERM（ERM：Enterprise Risk Management）のフレームワークが発表された。今、国内外で、リスクマネジメントのフレームワークや手法は進化している段階である。日本においても大手企業が、JIS Q 2001:2001に沿ったリスクマネジメントシステムの導入が進んでいる点やCOSO-ERMとの融合化を進めている点が事例研究から考察できる。今までのリスクマネジメントとERMとの大きな違いは、①グループ会社全体の取り組み、②企業価値創造を目的とする、③戦略リスクを含む、④リスクの統合化などである。各企業は、COSO-ERMのフレームワークとJISのマネジメントシステムを融合化させ、競争力強化につなげる仕組みが必要である。

今後、コーポレートガバナンスや内部統制の強化が高まる中で、企業単体のみでなくグループ会社全体を対象にERM手法の導入が本格化するであろう。

Triggered by improper accounting in the United States in 1992, an integrated framework for internal controls (COSO: Committee of Sponsoring Organizations of the Treadway Commission) was announced and this was followed up by the announcement of an ERM framework as COSO-ERM in 2004. Currently, both domestically and overseas, the framework and tools for risk management are evolving. In Japan also, this can be seen from the fact that large enterprises have been introducing risk management systems that conform to JIS Q 2001:2001, and from case studies of fusion with COSO-ERM. The major differences between the risk management up to now and ERM are: (i) measures for all group companies, (ii) having the objective of creating enterprise value, (iii) the inclusion of strategic risks, and (iv) the integration of risks. For each enterprise it will be necessary to fuse the COSO-ERM framework with the JIS management system and link this to enhancing competitiveness.

In the future, while the strengthening of corporate governance and internal controls are being heightened, the introduction of ERM tools targeting not only enterprises on an unconsolidated basis, but the group companies as a whole will become full-fledged.

1 財務報告に関わる内部統制の意義

2008年4月から財務報告に関わる内部統制の対象年度となり評価が始まった。上場企業にとって、今までの構築（文書化）と同様、評価証跡の作成、文書の見直し・改善など「評価」にかかるコストは相当なものである。財務報告に関わる内部統制の目的は投資家に対して適正な財務諸表であることを証明することである。部分的には業務の見直し、標準化につながるとは言え、単なる証明作業に過ぎず、収益拡大には直接つながらない。COSOの定義する内部統制（財務報告以外の目的も含む）への取り組みは、長期的にはコーポレートガバナンスや社内マネジメントの強化などメリットも大きい。しかし内部統制に大きな問題を抱え、これを期に充実を図ろうという企業以外は、意欲的に取り組む意味合いがなかなか見出せないのである。

内部統制の評価フェーズに入ると、今までの構築フェーズとほぼ同等程度の負担が見込まれている。2年目以降は習熟により運用コストは下がるとはいえ、毎年の評価は必要となる。財務報告に関わる内部統制は、米国同様に見直しが行われると考えられるが、資本市場から調達を行う限りある程度の負担は覚悟する必要がある。経営者としてはこれらのコスト負担を、いかに企業価値に転換させていくのかが大きな課題である。

現状ではいろいろ問題のある内部統制ではあるが、長期的な経営マネジメントの進化から俯瞰すると、極めて大きな意義がある。というのは企業グループとしてのリスクマネジメントの背骨が構築できたことである。会社法により、グループとしてのリスク管理体制の構築が義務づけられたものの、グループ全体で相当と思われるリスク管理体制を構築できている企業は極めて少ない。形式的な対応で済まされている企業が多いことが問題である。会社法が本来求めるリスク管理体制と、今回紹介するERMを比較すると、ERMのほうが従来のリスクマネジメントに比べ、より包括的で少し先を行く概念である（図表1参照）。

今回の財務報告に関わる内部統制の構築作業をベースに、企業グループに一筋通ったリスクマネジメントへと活用し、全グループ的なリスク管理体制（以下ERM）へ発展させていく可能性がある。これにより財務報告に関わる内部統制のコストは、企業価値に転換させることが可能になるのである。

2 日本企業のリスクマネジメントの現状

日本企業におけるリスクマネジメントの現状を述べる。大手企業においては重要と思われる個別のリスクに対して管理体制を構築している。例えば製造物責任に代表される品質リスク、個人情報・機密情報の漏洩、情報システムリスク、品切れ・事業中断などのサプライチェーンリスク、金利・為替変動リスク等だ。しかし取り組み主

図表1　従来のリスクマネジメントとERMの違い

	従来のリスクマネジメント	ＥＲＭ
対象	個別のリスク。オペレーショナルリスクや危機管理が多い。	戦略達成、財務目標達成に関わるリスク。今まで扱いづらかった戦略リスク等も対象。
目的・管理体系	個別のリスクの低減が目的。従って個別のリスクを対象とした管理体系の集合体。	企業グループの戦略達成、財務目標達成を阻害する要因を可視化し、総合的取り組みを行う管理体系。
取り組み主体と意識	各社毎の取り組み。したがって各社の意識によってばらばら。子会社、海外拠点は後手。	企業グループ全体での取り組み。目的・方針を共有した統一的な取り組み。
特徴	①重大なリスクの見落とし。また部門で認識されていても、グループとして認識されていない。 ②収益につながる戦略リスクの管理、モニタリングの弱さ。	①グループ内のリスクの顕在化。また組織横断的な一元管理による、リスクに対する意思決定の迅速化。 ②リスク許容内での戦略立案を行い、企業のリスク許容内でリスクをコントロールし事業目標を達成する。

体は各企業であり、企業の問題意識により取り組みはまちまちである。国内でも子会社になるとリスクマネジメントの水準は一段レベルが下がっており、グローバル化が進展するなか、リスク意識の高い欧米拠点ならいざ知らず、アジア拠点におけるリスクマネジメントは後手に回っているのが現状である。

日本企業の現状を一言でいうならば、個別のリスク管理の集合体で、管理水準もばらばらである。当然重要なリスクの見落としや現場で認識されていても、経営層が認識していないリスクもある。つまり、リスクの集合体であって、リスクの統合化が進んでいない。一方、これらのリスクは企業にマイナス影響をもたらすリスクであり、収益につながる戦略リスクなどは、意思決定時には検討されることはあっても、その後のモニタリングはほとんどされていない。

欧米企業に比べて日本企業はリスクマネジメントで遅れていると言われている。その理由のひとつは、1990年頃までの日本企業のフォロアー戦略思考[1]が原因であり、もう１点は、海外事業拠点に伴う管理体制整備の遅れである。確かに独自の戦略がなければリスクもそう大きい訳ではないし、海外の異なるリスクや、コミュニケーション・ギャップがなければ、リスクも問題なく伝達され、経営者、管理者の感覚的判断も概ね間違っていない。そのような多くの経営者の判断がリスクマネジメントの進展を遅らせてきた原因のひとつであろう。

日本企業の中でも、グローバル企業をはじめ、金融、エネルギー産業など、従来のリスクマネジメントから脱皮し独自のERMを構築しつつある企業もある。今後経済はますますグローバル化し、その中で独自の戦略を打ち出し、収益も含めて目標を確実に達成できる企業が株主にとっても魅力的な企業なのである。

3 ERMとは

ERMは全社的リスクマネジメント、または統合的リスクマネジメントとして紹介されている。ERMとしては、米国内部監査人協会等によるものもあるが、1992年に不正経理をきっかけにCOSO（米国トレッドウェイ委員会組織委員会）が「内部統制の総合的フレームワーク」を発表し、2004年には「全社的リスクマネジメント・フレームワーク」（以下COSO-ERM）として進化した。（図表2参照）現在、ERMフレームワークとして広く普及しつつある。

COSO-ERMでは以下の通りERMを定義している。

「事業体の取締役会、経営者、その他によって遂行され、事業体の戦略策定に適用され、事業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、事業体のリスク許容限度に応じてリスク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。」

上記のERMの定義も参考にしながら企業が導入する上でのERMの特徴・効果を以下に、概説する。

①グループ会社全体でリスクを捉え可視化する

ERMでは、従来の部分的なリスクマネジメントではなく、グループ全体でどのようなリスクを保有しているのかを可視化し、重要なリスクの漏れや認識違いを防止できる。特に子会社や海外拠点で有効である。企業グループで統一的なリスクの抽出・評価の基準により企業グループが保有するリスクを正しく認識し的確に意思決定できることにより、予期せぬリスクが発生することを防止できる。

②企業戦略目的の達成の阻害要因をリスクと捉える

従来のリスクマネジメントの手法は、リスクの種別ごとにアプローチしていた。例えば業界ごとの過去の事件・事故やリスク事例を参考にしながら、オペレーショナルリスクが中心であった点が否めない。リスクを特定する方法も、業務フローを作成しリスクを抽出・評価し、リスク対応計画を策定する手法が一般的であった。この方法は想定外のリスクを抽出する方法としては優れており、安定的な業務には適するものの、戦略リスクなど動的なリスクには対応が難しい。

ERMでは、リスクの定義を「企業における戦略目的の達成を阻害する要因」としている。これにより収益につ

ながる戦略リスクも対象となり、戦略策定の領域も範囲となった。このリスクの定義が、リスクマネジメントの考えを一変させERMへと発展させつつある。事業目的・目標の達成を阻害する要因をリスクとして考えることは、経営活動全てにリスクがあり経営管理活動のひとつの側面としてリスク管理活動があることを意味している。それらのリスクを管理し目的達成に合理的な保証を与える統合的な管理がERMの特徴だ。ERMは、従来の経営計画、目標管理などの経営管理活動と融合・統合化を図りながら進化しつつある。なおCOSO-ERMではマイナス要因を「リスク」、プラス要因を「機会」として整理している。

③安定性な収益確保により株主価値の向上

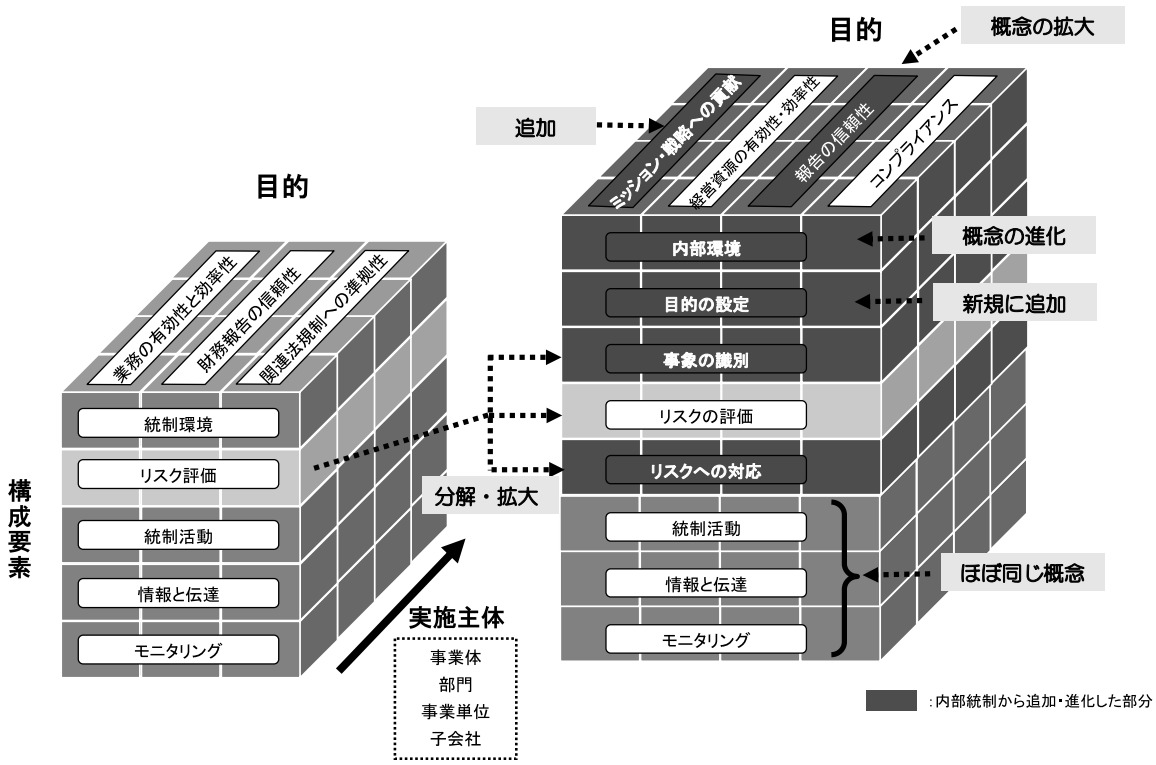
ERMの重要性を株主の立場から見てみよう。企業が毎期掲げる業績予想を確実に達成してくれることは株主にとても大きな魅力である。企業にとって利益に影響する重要リスクを管理することは、株主に対する企業価値としても大変重要である。

COSO-ERMの定義でも「リスク許容限度に応じてリスク管理が実施できるように」とあるが、まず企業としてのリスク許容限度を設定し、リスクの評価を行い、対策を行った後の残留リスクも算定する。そして各事業におけるリスクについてポートフォーリオ的な視点から企業としての最適解を探るのだ。これにより企業のリスク許容度内にリスクを設定しコントロールすることが可能となる。

4 内部統制からERMに進化させるフレームワーク

ERMのフレームワークもいくつかあるが、内部統制を発展させていくフレームワークとしては、前述のCOSO-ERMが最適であろう。その概念は、内部統制にリスクマネジメントのコンセプトを盛り込みブラシュアップしたイメージであり、企業が今後構築すべきERMを的確に示している。しかし92年に発表した「内部統制の統合的枠

図表 2　COSOにおける内部統制からERMへの進化



資料：全社的リスクマネジメント　フレームワーク編：東洋経済　を参考に三菱UFJリサーチ＆コンサルティング編集

組み」と同様に、コンセプトを述べただけであり、何を行えば良いのか分かりづらい。COSOがERMを発表した背景としては、「内部統制の統合的枠組み」は企業の実態としては、使い勝手が悪かったためであり、COSO-ERMはその点が改良されている。

COSO-ERMのフレームワークは図表2の通りである。目的は4つとなり、8つの要素から構成されている。目的は「ミッション・戦略への貢献」が追加された。その内容は「事業体の使命と連動し、それを支える高水準な目標への貢献」とあるが、企業の理念、ビジョン達成を目指す事業戦略および目標のことである。経営情報は「報告の信頼性」であり、財務報告の信頼性も含んでいる。業務の有効性は、「経営資源の有効性・効率性」に包含された。構成要素は、「内部環境」、「目的の設定」、「事象の識別」、「リスクへの対応」が大きく追加・変更となっている。実施主体は、事業体、部門、事業単位、子会社となっており、各々の主体で4つの目的に対応する構成要素を構築することを忘れてはならない。これにより重層的な管理体制が必要となるのである。

「内部環境」とは、経営者の理念・哲学、ERMを構築・運営するためのリスクマネジメント観、リスク風土、組織体制、社員の倫理観、教育、リスク許容限度などが含まれている。内部統制における統制環境にリスクマネジメント要素を加えている。特にここでは企業としてのリスク許容限度の設定が求められており、今後のどの程度のリスクを許容できるかの基準となっている。

「目的の設定」とは、実施主体における目的である。企業であれば事業目標、部門なら部門目標のことである。目的は実施主体ごとにブレークダウンされるとともに、目的の設定はリスク許容限界と整合をとって設定される。COSO-ERMで戦略領域まで足を踏み入れており、「目的－リスク－コントロール－指標」の関連で捉えることが求められている。最近企業では戦略立案にバランス・スコアカードが利用されており、その改良が行われているところである。

「事象の識別」とは、設定された目的達成を阻害する要因を識別することで、リスクの抽出およびその内容の識別のことである。リスクは企業にマイナスになるものばかりではなく、戦略リスクのように事業機会となるものもあり、その識別が求められている。

「リスクの評価」はリスクが企業へ与える影響度合いを把握することである。一般的には発生可能性と影響度で評価を行う。企業グループである程度統一された方法が望ましいが、リスクの大きさなど求められる精度を踏まえた評価方法が望ましい。COSO-ERMでは、何も対策を行わない場合の固有リスクと、対策を行った場合の残留リスクの分析が求められている。

「リスクへの対応」は、回避、共有（移転）、低減、受容といった選択肢の中から対応策を練るとともに、費用対効果の検討・評価を行うプロセスである。具体的には各部門から集計されたリスクを事業としてのリスクに積み上げ、事業レベルのリスクの相互関係をポートフォーリオの観点から分析し、企業としてリスク許容限度内か否かの検討が求められている。「目的設定」でブレークダウンされた目的に対して、個別のリスクの抽出・評価を行い、再度事業レベルのリスクに積み上げ、複数の事業リスクが相殺するのか、増幅するのか等の視点から検討するイメージである。COSO-ERMにおける事業リスクをポートフォーリオの視点から分析する考えは大変優れており、企業価値最大化のために効果を発揮すると考えられる。

「統制活動」は、リスクの対応が各階層で確実に行われるための、方針・手続きのことである。対象は異なるが内部統制の概念とほぼ同じである。

「情報と伝達」の概念も、92年版の内部統制とほぼ同じである。しかし実際に企業グループ内のリスク関連のコミュニケーションを構築する場合は課題が多い。企業の各部門のリスクを可視化し、必要な権限者へ適切な加工を施し伝達するとともに、モニタリングの仕組みが必要となる。部分的にはモニタリングを実施しているものの、全社またはグループ横断でということになると、分断されている企業が散見される。やはり、リスクの統合

化やリスク情報を如何につなぎ合わせていくのかが重要である。前述のようにERMを支える経営管理ツールが完全に整備されていないことも踏まえ、理想的な情報と伝達の仕組みの整備は緒についたばかりである。

5 日本における全社的リスクマネジメントの導入

国内においても、1998年から経済産業省を中心にリスクマネジメントシステムに関する研究会が開催され、2001年に日本工業規格JIS Q 2001が制定された。（図表3参照）この規格においてリスクマネジメントは、「リスクに関して、組織を指導し管理する､調整された活動」と定義され、リスクマネジメントシステムは「組織のリスクに関する戦略的な計画策定、意思決定および他の過程を含むマネジメントシステムの諸要素」と定義されている。

企業においては、主要事業の他に補助的な事業や新規事業など事業を中核としたリスクマネジメントを適用すべき範囲はかなり広範となる。特に主要事業においても、認知できていないリスクが存在する。新規事業においては、経験則からでは、測定できないリスクも存在する。事業活動とリスクとの相関関係を明確にし、顕在化するプロセスを構築していくことが重要である。

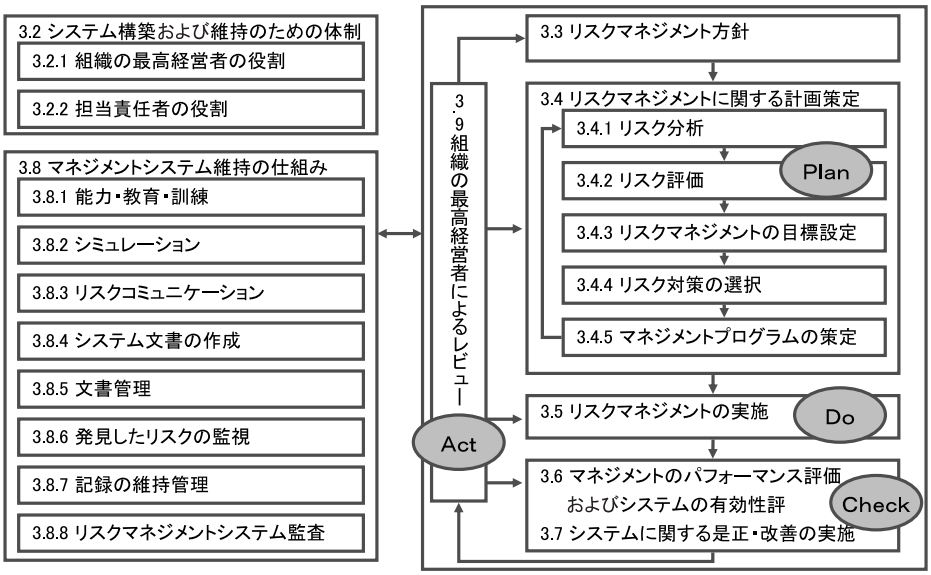
企業においてリスクマネジメントを実施する第一歩は、リスクの存在を認知することである。リスクの認知なしに、対策を打つことができないからである。そのためには、先行事例を知ることが重要になる。リスクが顕在化した事例を図表4に示す。まずは、業界や他社のリスク顕在事例を知り、その経緯や原因を分析することにより、リスク認知に努めることが先決である。

リスマネジメントシステムの基本ステップは、①「リスクの発見・確認」、②「リスク分析・算定・評価」、③「リスク対応（処理・制御）」、④「リスク受容」、⑤「リスクコミュニケーション」となる。（図表5参照）

「リスクの発見・確認」とは、事業計画や日常活動のどこにどのようなリスクがどのような状態で存在しているかを発見し確認することを意味する。例えば部門別（営業、設計、製造別など）または、ステークホルダー別（顧客、株主、社員など）にリスクを抽出する。例えば、ブレーンストーミングなどを活用すると、参加者の意識づけになり教育効果もある。

「リスク分析・算定・評価」は、リスクの発生頻度、被害の大きさ、形態を分析し、対策の必要度を評価分類別に特定する。リスクの評価は、発生の可能性（頻度）と損害の規模の乗数でリスクの大きさを評価し、リスク課

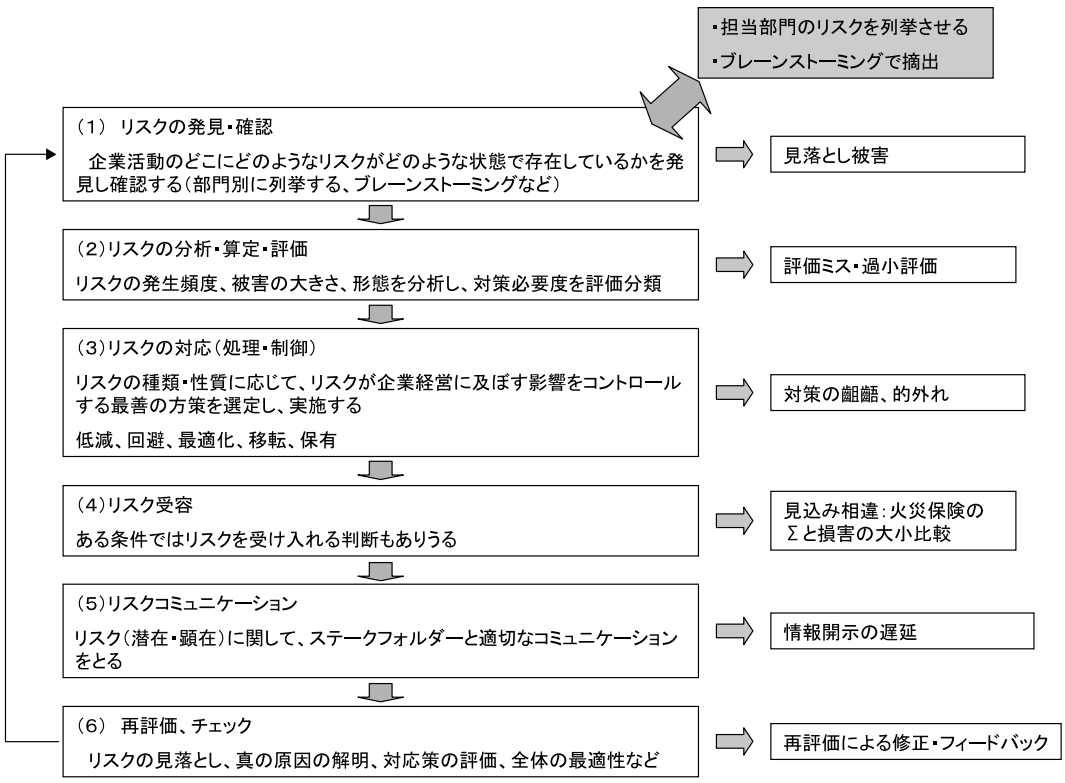
図表 3　リスクマネジメントシステム（JIS Q 2001:2001）



図表 4　リスクマネジメントからみた企業の事件・事故の発生事例

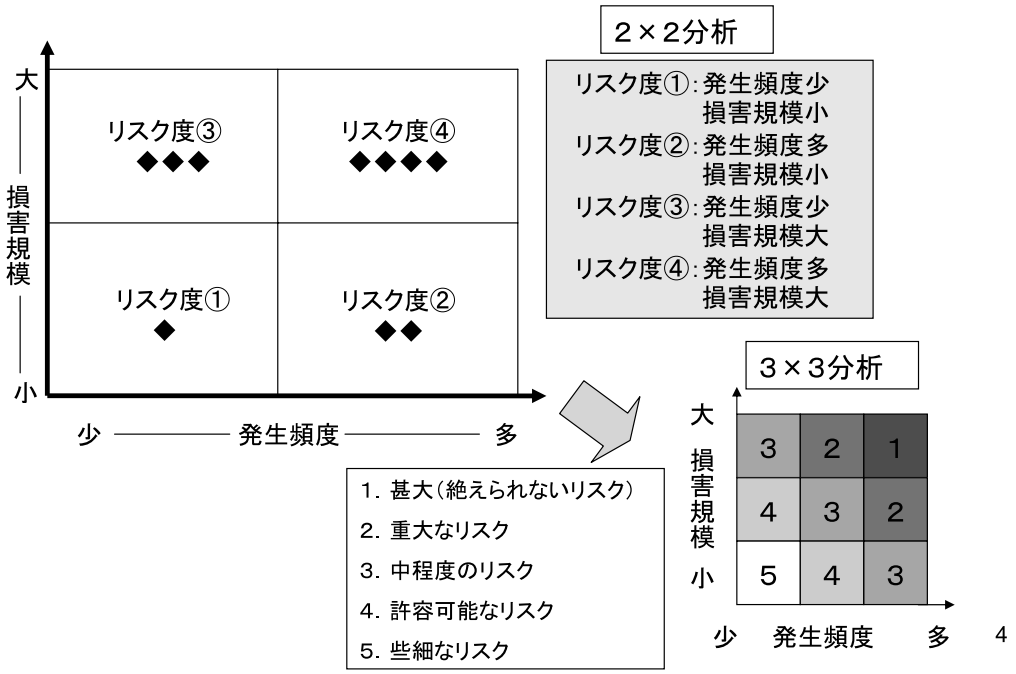
	年月	事　例
1	1997年11月	三菱自動車　総会屋利益供与で社長交代
2	2000年6月	雪印乳業　大阪工場　食中毒　発生　発症者数　14,804人
3	2000年8月	三菱自動車リコール隠し発覚
4	2002年1月	雪印食品　表示内容　偽装発覚　→廃業へ
5	2002年7月	USJで賞味期限切れ食材（最長9ヵ月）の使用発覚
6	2002年7月	USJでアトラクション「ハリウッドマジック」に許可量を超す火薬が使用発覚
7	2002年7月	USJで汚水管破断事故、配管接続ミスによる浄水器汚染など発覚
8	2004年3月	三菱自動車大型車　後輪ハブ欠陥隠し発覚
9	2004年3月	森ビル　六本木ヒルズ　回転扉死亡事故
10	2004年5月	三菱自動車　クラッチ系部品の欠陥　リコール隠し発覚
11	2005年3月	JAL（日本航空）　機体トラブル続発　→業務改善命令
12	2005年4月	JR西日本　福知山線脱線事故
13	2005年11月	松下電器産業　FF式石油温風機　一酸化炭素中毒事故　→機器回収
14	2006年7月	パロマ　屋内瞬間湯沸器　一酸化炭素中毒事故　→社長辞任、機器回収
15	2007年1月	関西テレビ　健康番組における番組情報のねつ造　→番組中止
16	2007年1月	不二家　期限切れ原料使用による洋菓子製造　→社長辞任

図表 5　リスクマネジメントの基本プロセス

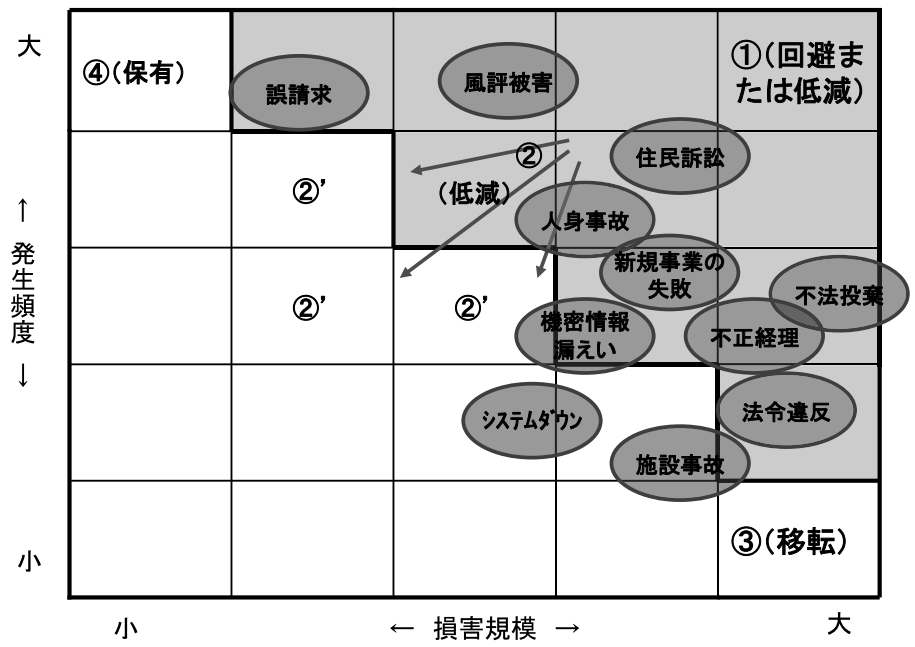


題の優先順位を明確にする。また、実際に着手する場合の経営資源（人・モノ・金）や対策効果を勘案することも必要である。図表6は、リスクマッピング事例で発生頻度と損害金額のマトリクスが一般的である。広く用いられている2×2と3×3の方法である。このリスクを発生頻度とその影響度を整理するのに有効なのが「リスクマップ」である。このリスクマップにより、リスクの「見える化」が可能である。（図表7参照）

図表 6　リスク評価基準（例）



図表 7　リスクマップ活用事例



「リスク対応（処理・制御）」とは、リスクの種類・性質に応じて、リスクが企業経営に及ぼす影響をコントロールする最善の方策を選定し、実施するリスクの回避、低減、移転、受容を決めていく。基本的な対策の順序は、①回避、②低減、③移転、④受容である。回避はその事業の中止等を意味し、リスクはほぼゼロになり、効果は大きいが、一般的には、対応しづらい。そこで主体となるのが、リスク低減策である。その主体は管理策であり、ISO9001やISO14001と同じ継続的な改善の視点で取り組んでいくことができる。

「リスク移転」は、低減と合せて実施する方法である。移転の主流は保険などであるが、アウトソースなど委託先へのリスク移転も重要な要素のひとつとなっている。特に委託契約書の見直し、リスク監査などで、委託先の監督を強化するなどの方法が取られている。

「リスク受容」は、経営判断として、ある条件ではリスクを受け入れる判断をすることである。リスクをそのまま受け入れる場合もあれば、リスク対応策を実施し、残存するリスクに対し、受容を行う場合もある。いずれにしても、リスクはゼロにならないので、重要な決断となる。

「リスクコミュニケーション」は、リスク（潜在・顕在）に関して、ステークホルダーと適切なコミュニケーションをとることである。

リスクコミュニケーションの第一主体はトップであり、社内に浸透させていくことが重要である。トップ自身が、リスクマネジメントシステムの必要性をまず認識することが前提条件である。例えばトップに意見しづらい組織や、トップの考えのみで、経営戦略・計画が立案されている場合は、組織が綱渡り状態であることに気づくべきである。トップの意識変革からスタートし、社員が共有できる体制を構築することが成功の条件である。

6 事例研究

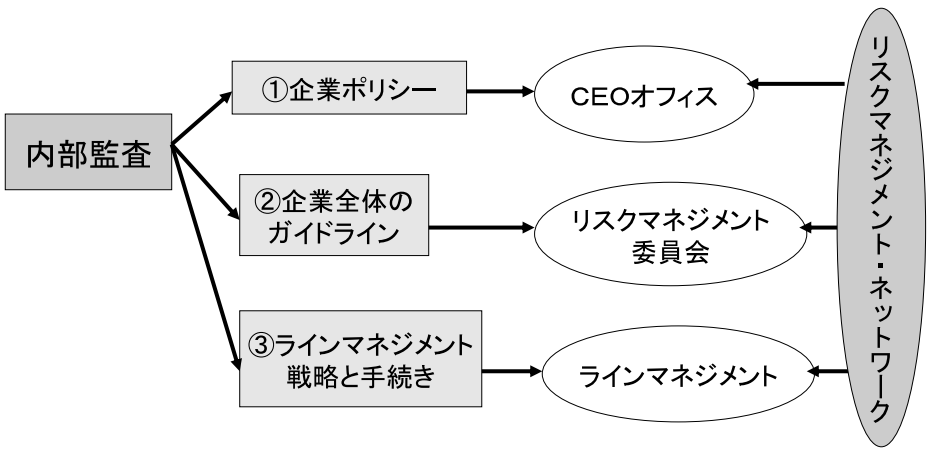
（1）海外の事例

海外におけるERMにおいて先進事例としてデュポンが紹介されている。その内容を以下に述べる。

デュポンは、企業戦略においてリスクマネジメントを上手に活用している。リスクマネジメントの3つの枠組みは、①企業ポリシー、②企業全体のガイドライン、③ラインマネジメント戦略と手続き、となっており企業ポリシーの4つの側面として、①哲学、②リスク目標、③ある特定なリスクを経営するときの権限を与えられた利用法と限度、④リスク委員会としている。特徴的な項目として、リスクマネジメント・ネットワークを構築し、内部監査制度によるモニタリングを実施している（図表8-1参照）。

4つの側面の1つである哲学は、「リスクマネジメントは、サイロの中で経営するのではなく、ビジネス戦略の脈絡の中で経営することである。」と明記している。戦略ビジネスユニット（SBU）はリスクを経営する責任があり、リスクチャンピオン（リスクマネジメントの専門家）がそのチームをサポートする体制をとっている。SBUの責任者はリスクをとることが役割であり、その役割が、報酬の源泉となる考え方を明確にしている。リスクマネ

図表 8 - 1　デュポン社のリスクマネジメントプロセス



資料：収益を作る戦略的リスクマネジメント～米国優良企業の成功事例～
トーマス・Ｌ・バートン、ウィリアム・Ｇ・シェンカー、ポール・Ｌ・ウォーカー

ジメント・ネットワークは、部門横断的にリスク統合の結果を「見える化」することに寄与している。さらにデュポンの大きな特徴は、「アーニングアットリスク(Earnings at Risk)」[2]にある。SBUは、自分たちの事業のリスク水準をよりよく理解し、収益のばらつきを識別し、各階層でコミュニケーションを生まれるとしている(図表8-2、8-3参照)。

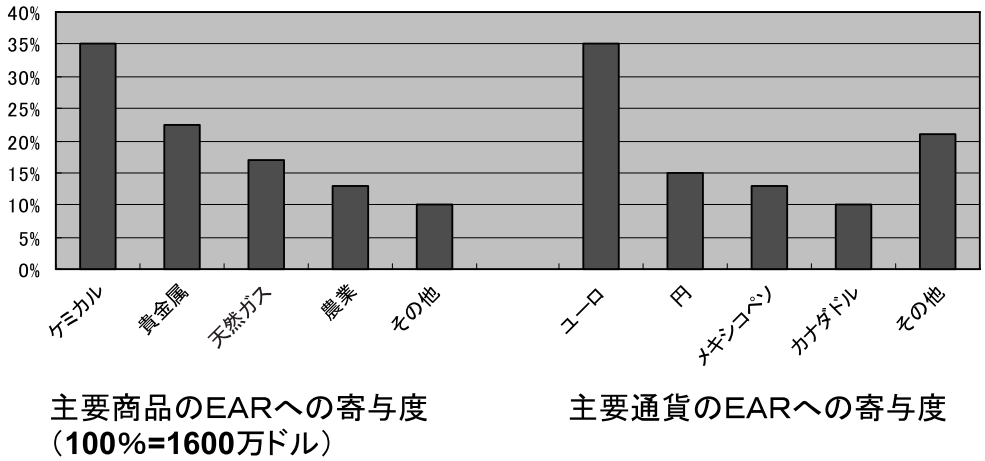
(2)日本の事例

日本におけるERM導入事例としては、「日本価値創造ERM学会」で発表された4社のERM導入事例をまとめた(図表9参照)。

各社ともにリスクマネジメントの統合的管理については、2000年前後からの取り組みであり、海外に比べて歴史が浅い点が特徴的である。導入のきっかけは、阪神・淡路大震災を契機とした事業継続管理(BCM)の必要性、企業不祥事の増加、CSR(企業の社会的責任)の高まりなどである、「トータル　リスクマネジメント」の体制整備に取り組んできた。

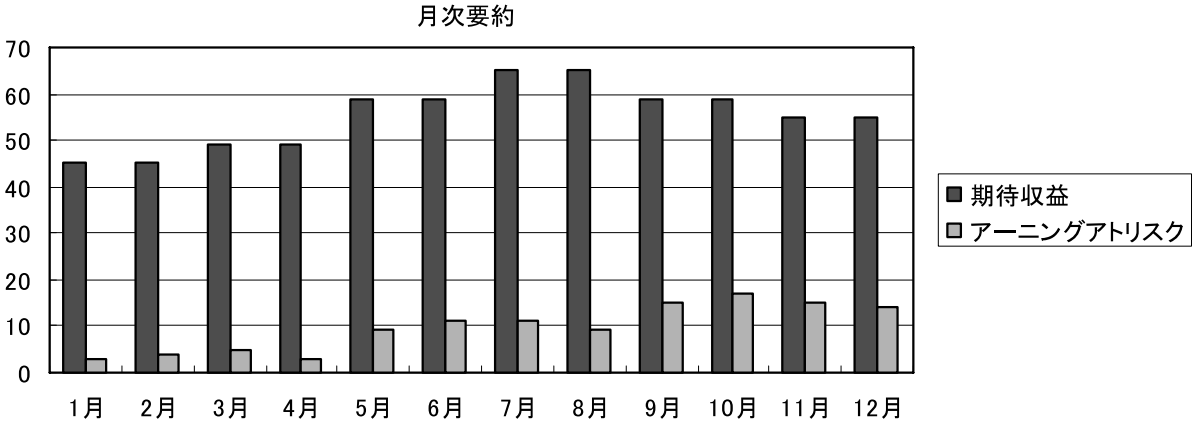
各社の比較項目としては、リスク識別、リスク評価手法、リスク管理体制、ERMの特徴などを整理した。

図表 8 - 2　アーニングアットリスク(EAR)の測定結果



資料:収益を作る戦略的リスクマネジメント～米国優良企業の成功事例～
トーマス・L・バートン、ウィリアム・G・シェンカー、ポール・L・ウォーカー

図表 8 - 3　会計年度2000年の期待収益アーニングアットリスク(EAR)



資料:収益を作る戦略的リスクマネジメント～米国優良企業の成功事例～
トーマス・L・バートン、ウィリアム・G・シェンカー、ポール・L・ウォーカー

図表 9　ERM事例研究

	資生堂	帝人
規格準拠	JISQ2001	COSO＆JISQ2001
戦略リスク	有（経営企画の一部）	有
業務リスク	有	有
危機管理	有	有
リスク識別	部門別リスク区分・識別 ■法務リスク　法務部 ■労務リスク（人権啓発部会）　人事部 ■財務リスク財務部 ■経営戦略リスク　経営企画部（05/5） ■広報リスク　広報部 ■お客さまニーズ対応リスク　お客さまセンター ■海外事業リスク　グローバル事業企画部 ■中国リスク　中国事業部（06/4） ■環境リスク（品質・環境部会）技術部 ■国内事業リスク　事業企画部 ■商品リスク（品質・環境部会）技術部 ■情報システムリスク　情報企画部（05/5） ■災害事故セキュリティリスク　総務部 ■情報セキュリティ部会　総務部	トータルリスクマネジメント区分 1．業務運営リスク（①企業に悪影響のみを及ぼす有害事象によるリスク②発生時は業務執行（事業運営）の段階で的確な対応と意志決定を迫られるリスク） 1．1 業務リスク 1．2 コンプライアンスリスク 2．経営戦略リスクマネジメント（①経営戦略・経営計画策定、重要投資案件審議等、経営の戦略的意志決定に伴うリスク（将来結果の不確実性によるリスク）②期待値（見通し）と結果の差は、プラスにもマイナスにもなりうるリスク） 2．1 経営計画 2．2 個別投資案件
リスク評価手法	「JISQ2001ガイドライン」に則った手法 リスク担当部会ごとに「リスクの洗い出し」を継続実施 ①洗い出したリスクを優先順位付け ②優先順位上位リスクを重点実施項目として「年度予防計画」を立案 ③予防計画に基づき部会ごとに年度の予防対策を推進 ④監査結果を次年度計画に反映	①リスクの評価作業は、リスクの大きさ（リスクが顕在化した場合の影響度合）並びにリスクの発生可能性を評価し、「本源的リスク」の評価（リスク度の算出）をする。 ②内部統制の評価も実施し「残存リスク」を評価します。 ③リスクの評価結果をリスク度に応じて色分けして表示する（「リスク・ヒートマップ」）。
リスク管理体制	5つの委員会（総合リスク対策委員会、CSR委員会、企業倫理委員会、技術・品質委員会、個人情報保護委員会）を2007年4月からCSR委員会に統合し、下部組織として企業価値創造委員会、コンプライアンス委員会の2つでCSR委員会を構成	CSRO（CSR責任者） グループCSR委員会（CSR室、環境・安全室） グループコンプライアンス・リスクマネジメント部会 グループESH部会 グループPL・品質保証部会 グループ安全保障輸出管理会議 グループCSRスタッフ部会
ERMの特徴	資生堂のリスクマネジメントポリシー 「社員と家族の安全確保（人命尊重）」を第一義とし、次いで「会社資産を保全」して「事業を継続」するとともに、被災時における社会貢献等を通じて「ステークホルダーからの信頼を確保する」ことにより当社のブランド価値を高めていくことを基本方針としている。4つの優先順位が明確であることが特徴	トータルリスクマネジメント（TRM）を導入 ◎包括的・全社的に対応 ◎経営者を含む全社員の認識 ◎プロアクティブ（予防的）コントロール ◎戦略的位置付け ◎継続的な対応 ◎対象リスクは複雑化・多岐化

	全日空	住友商事
規格準拠	JISQ2001	COSO
戦略リスク	有（内部リスクの一部）	ウエイト大
業務リスク	有	有（計測不能リスクの一部）
危機管理	ウエイト大	無
リスク識別	リスク分類表 ＜外部リスク＞ ①災害リスク②航空保安リスク③政治・カントリーリスク ④財務リスク⑤経営外部環境リスク ＜内部リスク＞ ①運航リスク②業務プロセスリスク③経営戦略リスク④コンプライアンスリスク⑤システム（IT）リスク⑥環境リスク	事業リスク＝事業価値の変動要因 ＜計測可能リスク＞ ①ビジネス・リスク 市場の成長性・需要等、数量面での変動 ②市場リスク 仕入・販売商品の価格面での変動 ③財務リスク 為替・金利の変動 ＜計測不能リスク＞ オペレーショナルリスク等
リスク評価手法	STEP 1 リスク分析ワークシートにてリスクの洗い出し STEP 2 洗い出したリスクをリスク分析表に集約 STEP 3 リスク管理担当者がヒアリングし、リスク評価・転記 リスク管理規程のリスク評価基準に従って、リスク評価を実施する。	Earnings at Risk手法を採用 Earnings at Risk手法により長期的なリスク評価および分析的なリスク評価が可能 Value Driver＝Risk Factorが事業全体のキャッシュフロー変動に与える影響度がわかり、事前に事業価値最大化のための対応策、事後の改善策を講ずることが可能
リスク管理体制	CSR推進会議（総括：社長） 安全保障輸出管理部会 チーフCSRプロモーションオフィサー（CSR推進室担当役員） コンプライアンス委員会 リスクマネジメント委員会（リスクマネジメント部会、航空保安・危機管理部会、情報セキュリティ部会、安全保障輸出管理部会）	コンプライアンス委員会スピークアップ制度 インターナルコントロール委員会インターナルコントロールプロジェクト 全社一律のリスクマネジメントフレームワーク構築／運用
ERMの特徴	事故・ハイジャック等への緊急対応マニュアル（ERM）を策定 本マニュアルは、会社の航空機に係る事故又はハイジャックなどの事態の対応に必要な組織および業務内容を明確に定め、対応を迅速かつ適切に実施し、損害の極小化を図るとともに、原因を調査究明し将来の安全かつ安定的な運航を確保することを目的とする。併せて、会社以外の航空機事故などの支援対応に必要な組織および業務を定めることにより、迅速かつ適切な支援を開始するとともに被害の拡大を防止することを目的とする。	統合リスク管理TFの立ち上げ（2002年） グローバル連結ベースでの「業務品質」の向上を目的としている。従来制度を統合し、リスク管理機能を強化し、従来個別に導入されていた自己監査、統合リスク管理等を統合した。自己評価結果よりも、プロセスを重視し定期的かつ網羅的なフォローアップ。全ての部署で、全ての子会社で、全世界で、現場自らが振り返ることを重視。マイナス情報は即報告する。

1）リスク識別

資生堂は、個別リスクを分類し、部門別リスク区分を明確にしている。リスク主管部署を決めて統括管理体制を整備している。帝人では、リスクを大別し、業務運営リスクと経営戦略リスクに区分し、業務運営リスクは、業務リスクとコンプライアンスリスクに区分されている。全日空では、外部リスクと内部リスクに区分され、内部リスクの1部に経営戦略リスクを位置づけている。特に危機管理を主体とした事業継続管理（BCM）に力点が置かれている。

住友商事では、事業価値の変動要因を事業リスクと定義し、計測可能リスクと計測不能リスクに大別し、前者では①ビジネスリスク、②市場リスク、③財務リスクに分類しており、計測不能リスクとしてオペレーショナルリスクを位置づけている。商社らしい事業リスクの識別となっている。

2）リスク評価手法

住友商事はアーニングアットリスク手法により戦略的なリスク評価を実施している。長期的な事業リスクとしてリスク評価が可能Value Driver＝Risk Factorが事業全体のキャッシュフロー変動に与える影響度を分析し 事業機会としてのリスクマネジメントを実践している。

その他の3社は、各社ごとに、リスク分類を異なるもののJIS Q 2001に沿った標準的な方式で、①リスクの洗い出し、②リスク分析（リスクの大きさ×影響度)、③優先順位づけ、④残存リスクの評価、⑤対応策の実施、⑥レビューの実施となっている

3）リスク管理体制

各社共通の要素としては、リスクマネジメントを管理する委員会が設置され、委員長にはトップまたは役員が就任している。また各種委員会の統合を推進し、近年整備されたばかりであることも特徴的である。例えば資生堂は、企業価値創造委員会を組成し、住友商事は、グローバル連結ベースでの「業務品質」の向上を目的としたインターナルコントロール委員会を組成するなど、前向きなリスクマネジメントが特徴的である

帝人は、CSRとの連携を図り、経営戦略の立案から業務活動、事業継続管理までをトータルに管理するTRMを導入している。

全日空は、経営戦略よりも、オペレーショナルリスクや事業継続管理（BCM）に重点が置かれており、事故・ハイジャックなどへの緊急時対応マニュアルの策定が特徴となっている

4）リスクマネジメントの特徴

各社のリスクマネジメントは個別リスクからの統合化へと進展してきている。国内において主流とされてきたJIS Q 2001は、危機管理からスタートしているためか、個別リスクの集合体である要素が否めなかったが、COSOモデルの導入により、組織の戦略目的や事業機会としてのリスクマネジメントに変化しつつある。言い換えるとオペレーションリスク主体から戦略リスク主体にパラダイムシフトしていると考えられる。

組織の事業継続の本質は、①戦略策定段階、②業務運用、監視段階、③危機発生段階に区分され、過去の経験から学ぶ②、③のリスクマネジメントから、将来の不確実性を「見える化」する①の段階に変化しているといえる。この①、②、③の各段階の連結機能が、重要になると予想される。

5）事例研究の考察

今回の4社の先進事例に共通するのは、COSO-ERMを参照しつつ、実務的にはJIS Q 2001の手法を活用し、リスクの統合化に着手している点である。さらに、会社法で本来求めわれているコーポレートガバナンスの強化と整合を取りながら、いかにリスクマネジメントの独自性を出していくかを模索している段階であるといえる。

各社に共通的な取り組み事例を以下に示す。

①経営理念・事業目的・行動規範の明示と伝達

②コンプライアンス統括部やCSR委員会などの統括部署や委員会の設置

③内部監査部など独立的な評価部門の設置

④全社統一的な業績管理指標（KPI）の設定とモニタリングの実施

⑤リスクを分類・識別し、リスク評価およびリスク対応の実施
⑥人材育成に力点をおいたコンプライアンス体制構築
⑦コンプライアンスおよび財務報告の順守などについて関係会社から部門宣誓書の入手
⑧業務執行部門から独立した通報ライン（ヘルプライン）の設置
⑨EラーニングなどITを活用したコンプライアンス教育の実施
⑩経営者によるトラブル関連情報の入手と利用
⑪経営者による内部監査情報の入手と利用

これらの取り組みを参考に、日本の企業の多くがベースラインとして採用し、今後、中堅・中小企業まで普及させることが必要な項目といえる。

また、今回の事例研究を通じて、ERMの進展を阻害する課題は以下の通りである。

①事業計画と関連付けてリスクマネジメントを実践している企業が少ない。
②広範なリスクに対してリスクの概念およびリスク評価指標について、必ずしも統合化されていない。
③経営層自ら、関与すべき重要事項としての認識が薄いケースもある。

7 まとめ

全社的なリスクマネジメントを具体的に整備するためには、COSO-ERMモデルを鳥瞰図としながら、ブレークダウンし、戦略リスクも含めて、リスクを識別し、統合化することが重要である。その後、マネジメトシステムとしてPDCAサイクルをまわしていくことで定着・改善を継続的に実施していくことが必要であろう。いわゆるCOSO-ERMとJIS Q 2001の融合化の推進である。

まずは、リスクの統合的な体系を整理し、リスク許容限度を把握することが事業戦略上の重要課題である。さらに環境・社会・経済の視点からみた「バランス経営」が重要であり、CSR（企業の社会的な責任）の実現に向けた取り組みであることを忘れてはならない。

ERMのリスクマネジメントの成功要因を以下に示す。

①**価値**：創造すべき価値・守るべき資産を明確化。
②**組織力強化**：リスクマネジメント体制（リスク委員会等）を整備し、有用な人材をメンバーとする。また、失敗は、個人的なものではなく組織的なものと認識する。
③**現場**：現場情報の収集、現場の取り組みを主体とする。
④**マネジメントシステム**：方針・目標・管理策・マニュアルを整備し、教育と共考（共に考える）を通じて、人々のリスク感性（意識）を高める。
⑤**情報公開**：社内外に企業風土や企業の置かれている情勢を情報公開（デイスクローズ）する。
⑥**変化と継続的改善**：社会環境、事業条件は絶えず変化する。リスクマネジメントも絶えざる進化が不可欠である。

8 今後の課題

企業は内部統制を基礎に企業リスクをその許容限度内で最適に管理するというERMに発展させていくことは間違いない。その際に利用されるフレームワークとしてのCOSO-ERMとマネジメントシステムとしてのJIS Q 2001の統合化が有望である。しかし、現段階で2つの課題があると考えられる。

最初の課題は、経営者の意識である。残念ながら経営者の中で、ERMの本質とは何か、どのように活用していくかを明確に理解している人は少数派である。現実的には、実際に運用しながらERMの理解を深めつつ、その活用を検討していくことになる。その中で自社およびグループのリスクマネジメントに対する考えが整理されて、次なる一歩が展開されていくことを期待したい。

もうひとつの課題は、ERMに対応する経営管理手法の開発である。前述の通り、ERMはリスクの統合化が進展している一方、JISベースのリスクマネジメントは、オペレーションリスクが中心である側面がある。戦略リスクを含めた先進事例はあるものの、これがERMの定番手法

図表10　リスク統合への３つのステップ

ステップ	行動	方法
1	全ての有意なリスクの識別	リスクをリスト化、評価し、マップ化する。
2	リスクの測定、ベストプラクティスと道具の統合	ＶａＲ、ストレステスト、アーニングアットリスク（ＥＡＲ）
3	企業グループ全体としてみる	非整合性、自然相殺、移転、機会に対するファイナンス

資料：収益を作る戦略的リスクマネジメント～米国優良企業の成功事例～
トーマス・Ｌ・バートン、ウィリアム・Ｇ・シェンカー、ポール・Ｌ・ウォーカー

であるというところまでは至っていない。企業価値創造に結びつく、デファクトスタンダードの開発が必要である。

図表10にリスク統合への3つのステップを示した。収益に中核をおいたアーニングアットリスク（EAR）など各事業の組織横断的リスクの統合化や全社的なマネジメントを「科学」できる仕組みが今、求められている。

【注】

[1] フォロアーの戦略思考：業界トップ企業のビジネスモデルを参考に、追従型の戦略を採用する２番手、３番手企業の志向を示す。具体的には、先行する欧米企業のビジネスモデル、戦略を研究し、追いつけ、追い越せ型の日本企業の戦略であり、先行事例があるためリスクは少ない。

[2] アーニングアットリスク：Earnings at Riskとは、金利や市況などの外部環境が動いた場合に、ある一定期間において一定の確率で起こる期間損益（金利差益）ベースでの予想最大変動額を示すもの。Earnings at Riskが高いとは、企業の収益のぶれが大きいことを意味する。

【参考文献】

・先進企業から学ぶ事業リスクマネジメント実践テキストー企業価値の向上を目指してー経済産業省　平成17年３月
・収益を作る戦略的リスクマネジメント～米国優良企業の成功事例～　トーマス・Ｌ・バートン、ウィリアム・Ｇ・シェンカー、ポール・Ｌ・ウォーカー　東洋経済新報社　2003年12月23日
・*The Institute of Internal Auditors“Applying COSO’s ERM — Integrated Framework”
・http://www.theiia.org/bookstore.cfm?fuseaction=product_detail&order_num=521
・財務報告に係る内部統制の評価及び監査基準のあり方について平成17年12月　企業会計審議会　内部統制部会
・日本価値創造ERM学会（The Japanese Association of Value-Creating ERM）研究会、年次大会