東京海上日動リスクコンサルティング（株）
情報グループグループリーダー　指田　朝久

リスクマネジメントと事業継続、危機管理の相互関係

本文要約

リスクマネジメントシステム JISQ2001 と ISOGuide73 が制定され考え方が整理されたが、その普及活動を実施していると現状企業等で用いられているリスクマネジメントに関する用語や概念が依然根強いことがわかった。さらにリスクマネジメントシステムに類似する事業継続の概念が普及しはじめ、また危機管理という用語も用いられている。加えて COSO によるＥＲＭ（事業体全体のリスクマネジメント）の提案もなされている。このような現状においてリスクマネジメントの議論を行う場合は、まず当事者と用語や概念の定義および主張点を確認することが不可欠である。ここでは現在様々な用いられ方をされているリスクマネジメントの概念の説明と、リスクマネジメント、事業継続、危機管理の概念の整理をする。また、概念の混同の原因のひとつと考えられるリスクマネジメントシステムとリスクマネジメントプロセスの違いにつき整理をする。

１．リスクマネジメントシステム等の浸透状況の現状把握

（１）アンケート調査による JISQ2001 の浸透度

JISQ2001 リスクマネジメントシステム構築のための指針[1]の浸透度は必ずしも高くない。財団法人日本情報処理開発協会が 2006 年 3 月に発表した「わが国における情報セキュリティの実態」[2]によれば「JISQ2001 を利用している 6.4%」、「知っている 45.1%」、となっており、2004 年 3 月に実施した前回調査[3]の数字である「JISQ2001 を利用している 3.3%」、「知っている 32.3%」、に比較して増加しているがまだ不十分な状況である。調査対象者が情報システム部門に偏っていることを差し引いても普及しているとはいいがたい状況である。

（２）危機管理セミナーにおける現状把握

リスクマネジメントと危機管理の包含関係をどのように捉えるかについて 2005 年 10 月 24 日に実施された特定非営利活動法人危機管理対策機構 D-ＰＡＣプロジェクト 2005 の講演会の出席者約 100 名に対して挙手によるアンケートを主催者が実施したところ、「リスクマネジメントが危機管理を包含する」と「危機管理がリスクマネジメントを包含する」と回答した

©東京海上日動リスクコンサルティング株式会社　2007

数がほぼ同数であった。(もうひとつの選択肢の「リスクマネジメントと危機管理は同じである」という選択はほとんど無かった)(図１参照)

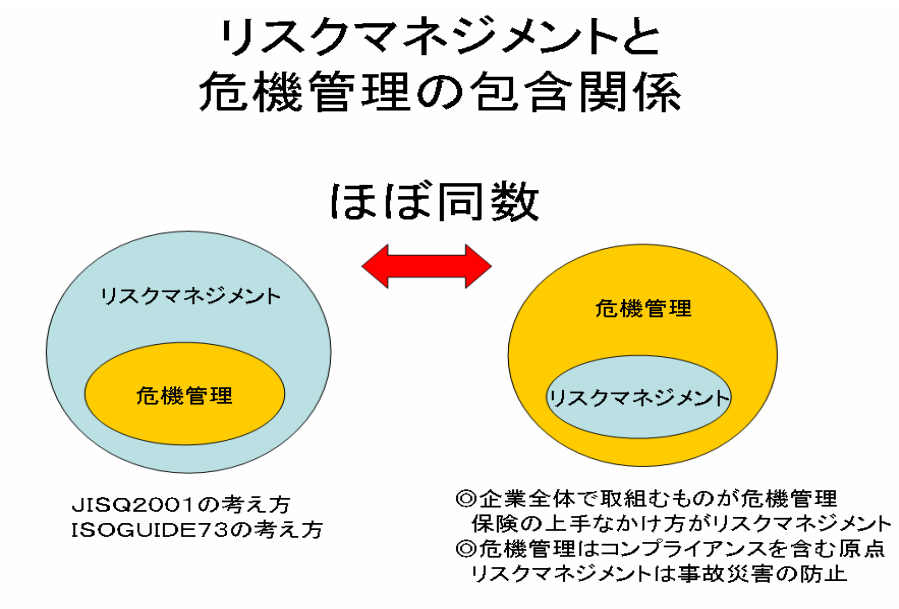


図1 リスクマネジメントと危機管理の包含関係

ここで「危機管理がリスクマネジメントを包含する」と回答した人に筆者がその理由を聞くと以下の回答があった。

① 企業全体で取り組むものが危機管理であり、リスクマネジメントは保険の上手な掛け方を指す。

② 危機管理はコンプライアンスを含む企業活動の原点である。リスクマネジメントは事故や災害の防止活動である。

当該講演会の出席者は主に企業の災害対応や危機管理の実務担当者であるが、このような考え方をみると JISQ2001 や Guide73[4] は浸透しておらず、リスクマネジメントを防災や保険に限定する古典的な捉え方が依然として残っていることがわかる。

（３）類似概念の普及

2005 年は経済産業省[5]や内閣府[6]が相次いで事業継続ガイドラインを発表し、リスクマネジメントと近接した概念である「事業継続」の概念が浸透してきた。

また、リスクマネジメントそのものもＣＯＳＯ[7]の流れを受けて「リスクマネジメントと内部統制」の概念の普及が見られ、この場合の「リスクマネジメント」の概念は ISO Guide73 とは一致していない。

このように現状では様々な用語[8]が用いられている。ここではどれが正しい等の議論をするのではなく、当事者同士で言葉の定義や概念を確認しないと誤解が生じる恐れが強い現状

©東京海上日動リスクコンサルティング株式会社 2007

にあることを認識する必要があると指摘しておく。

２．概念の整理

リスクマネジメントシステムを中心に据えて「事業継続」「危機管理」および「COSO のリスクマネジメント」の整理を行う。

（１）JISQ2001 リスクマネジメントシステムの概念

JISQ2001 リスクマネジメントシステムの定義では「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；備考　リスクマネジメントには、一般的にリスク算定、リスク評価、リスク対応、リスク受容及びリスクコミュニケーションを含む」と定義されている。企業全体を対象とすることもその中の一部の組織を対象とすることもできる。また、対象とするリスクを限定していない。

（２）事業継続の概念

内閣府事業継続ガイドライン[9]では「事業継続」は「災害時に特定された重要業務が中断しないこと。また万一事業活動が中断した場合に目標復旧時間内に重要な業務を再開させ、業務中断に伴う顧客取引の競合他社への流出、マーケットシェアの低下、企業評価の低下などから企業を守るための経営戦略」としている。（図２参照）

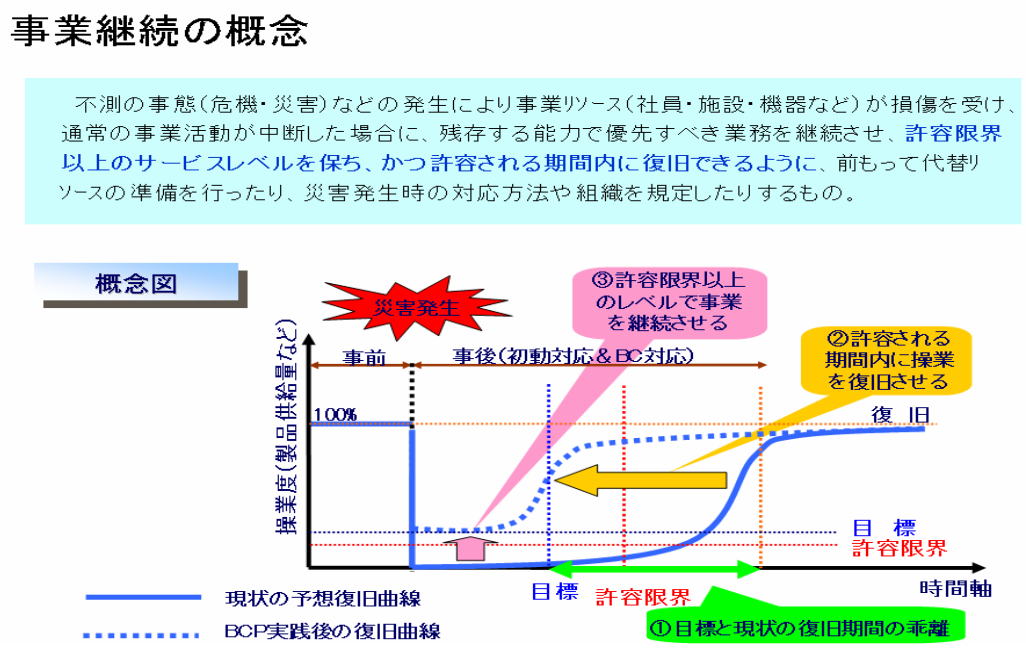


図2　事業継続の概念　（内閣府事業継続ガイドラインより）

事業継続ガイドラインでは継続的改善であるマネジメントシステムを前提としており、また取組みにおいて事前、事後、復旧の時間軸を持ち、JISQ2001 リスクマネジメントシステム

©東京海上日動リスクコンサルティング株式会社　2007

と親和性がある。事業継続を構築する対象は何らかの理由で企業の主要な機能が停止した場合であるが、先進企業の実例では地震、火災、情報システム停止、取引先の事故、テロ、ライフラインの停止、疫病が発生した場合等つまり災害を対象としている。逆に、法令違反による営業停止処分への対応などは対象としていない。結論として、事業継続はリスクマネジメントシステムに内包されると考えてよい。

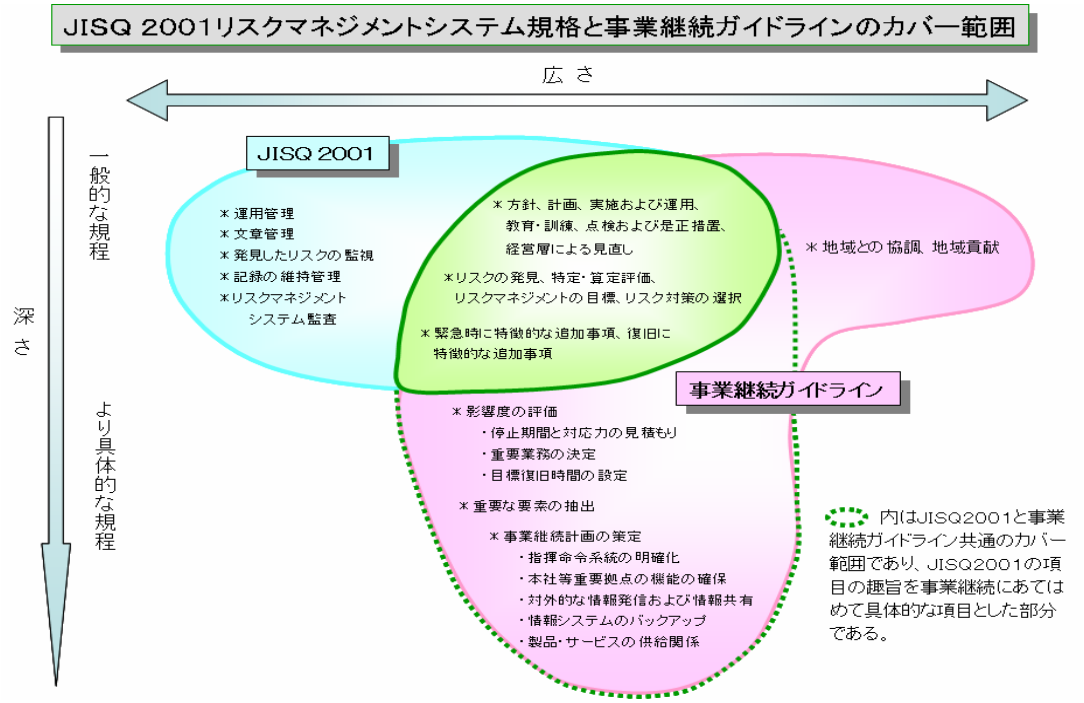


図3　JISQ2001 と事業継続ガイドラインのカバー範囲

実際に JISQ2001 と内閣府事業継続ガイドラインの要求事項を比較したものが図３である。この図のように内閣府事業継続ガイドラインは JISQ2001 を、事業継続を目的として具体的に展開したものと考えてよい。唯一内閣府の事業継続ガイドラインの要求事項が JISQ2001 のカバー範囲を超えているものと考えられるものに「地域との協調、地域貢献」がある。

「事業継続」の異説に企業の存在目的そのものに「自らの製品供給を通じて組織を発展させるゴーイングコンサーン」があり、倒産しないための最上位の取組みが事業継続であり、リスクマネジメントは防災や保険の取組みに限定とするものがある。この場合は「事業継続」が企業全体を対象としたリスクマネジメントシステムに該当し、ここでいう「リスクマネジメント」は後述の「リスクマネジメントプロセス」のひとつの適用に該当する。ここで「リスクマネジメント」と「危機管理」と同様の概念の包含関係の混乱が生じている。例えば中小企業庁ではホームページで公開している、「中小企業ＢＣＰ策定運用指針」[10]の中でＢＣＰの定義を「緊急時企業存続計画または事業継続計画」と翻訳し、企業が倒産しない仕組みを事業継続の概念と位置づけている。このためリスクマネジメントを防災・保険の手法と位置づけ、事業継続をリスクマネジメントより上位の概念に位置づけている。（図４参照）

©東京海上日動リスクコンサルティング株式会社　2007

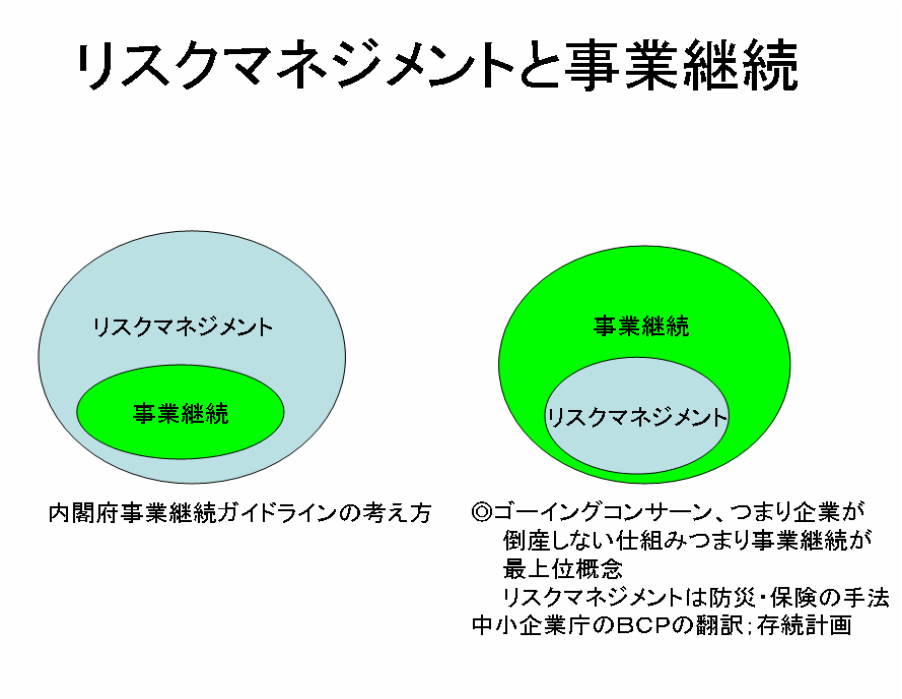
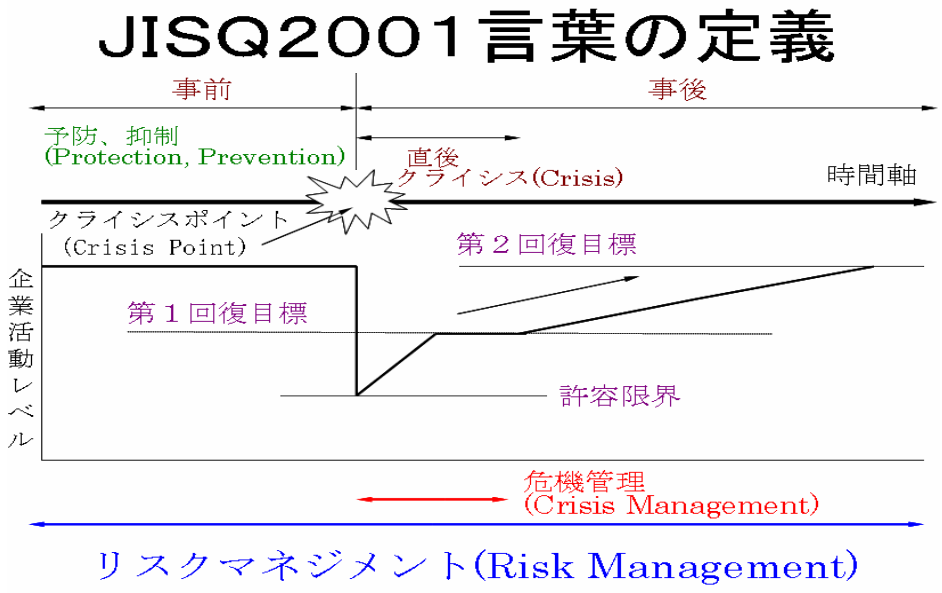


図4　リスクマネジメントと事業継続の関係

（３）危機管理の概念の整理

危機管理については日本工業規格標準情報 JISTRZ0001 危機管理システムを発展的に解消し JISQ2001 を制定する際に、「危機管理」は事後対応に限定して位置付け、リスクマネジメントは事前、事後、復旧のすべてを包含する、つまり危機管理を含むと整理した。　Guide73 の用語の定義でも危機管理はリスクマネジメントに包含されると解釈されている。(図５参照)



出典：　JISTRZ0001（Q2001の原案）より

図5　JISQ2001 の言葉の定義

©東京海上日動リスクコンサルティング株式会社　2007

http://www.tokiorisk.co.jp/

「危機管理はコンプライアンスを含む企業活動の原点である。リスクマネジメントは事故や災害の防止活動である」という主張は、「危機管理」の定義が JISQ2001 の定義とは異なっており好ましくない。またここでいう「リスクマネジメント」は後述する「リスクマネジメントプロセス」にあたる。

（４）ＣＯＳＯの概念

内部統制や内部監査を検討しているトレッドウェイ委員会の進める全社的リスクマネジメント（ERM；Enterprise Risk Management）では「リスクマネジメントの考え方」として「事業体としてあらゆる局面で、事業体がリスクをどのように考慮するかを特徴づける共有化された信念と姿勢を表したもの」としている。どの分野に進出するか、新製品のコンセプトなどの戦略的なリスクを主対象に災害や法令違反なども視野にいれた概念を構成している。この考え方はグループ会社全体を捉えたリスクマネジメントシステムと同じであると解釈される。なお、重要視されている内部監査も JISQ2001 に明記されている。（図６参照）

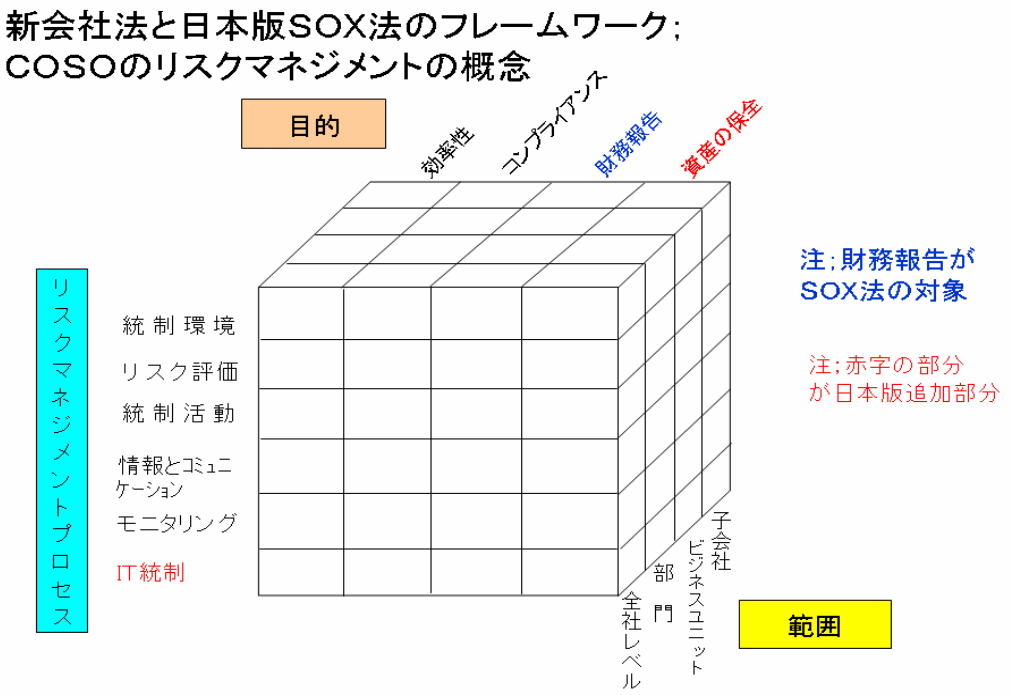


図6　COSOのフレームワーク（「財務報告に係る内部統制の評価及び監督の基準案」金融庁企業会計審議会内部統制部会 2005 年 12 月 18 日公表より作図）

３．JISQ2001 の主張点と限界および課題

先ほどＪＩＳQ2001 のリスクマネジメントの定義をみたが、この定義は組織を前提としていること、また「保険」や「事故対策」などの言葉は一切ない特徴がある。また、セミナーのヒアリングなどで明らかになったように一般的には「リスクマネジメント」は保険や、製品安全

©東京海上日動リスクコンサルティング株式会社　2007

や労働安全、災害対策などを意味する事も多い。さらに、リスクマネジメントシステムはＰＤＣＡの概念を取り入れた継続的改善の手法であるが、ある課題を解決するためにリスクの発見、リスク評価、リスク対応、などをする１回限りのリスクマネジメントも存在する。例えば事件事故が発生して事後対応・危機管理対応をしている時、その対応策の各ステップそれぞれに成功する場合、失敗する場合が存在し、代替策との比較などを合理的に検討するために次のリスクマネジメントプロセスの考え方が適用できる。

従ってリスクマネジメントシステムの普及を行うには、それと平行して「リスクマネジメントプロセス」という「組織を前提とせず、1 回限りでも有効である、何らかの行為をするための意思決定を支援する共通の手順」が存在すべきであるという主張が専門家からなされ、2005 年から ISO で議論が開始された。[11]

４．リスクマネジメントプロセスの概念

（１）リスクマネジメントプロセス例

リスクマネジメントプロセスの考え方は古典がすでに存在している。代表的なものに以下のものがある。

① リスク発見、リスク評価、リスク対策

② リスク発見、予知、予防、対処、復旧[12]

またオーストラリア・ニュージーランド規格リスクマネジメント AS/NZS4360[13] はリスクマネジメントプロセス規格として考えて良い。

（２）リスクマネジメントプロセスの留意点

事業を営み目標を達成できるか否かという企業全体を見渡すＥＲＭ、部門毎のリスクマネジメント、製品開発、自然災害・防火、医療過誤等の事故防止活動、製品や食品の安全性確保、労働安全活動、また、危機管理対応実施中の判断等のどの局面でも活用でき、組織としての意思決定、責任者、担当者の個人また家庭での意思決定にも活用できる「リスクマネジメントプロセス」として以下に AS/NZS4360 を基本とした試案を述べる。なお、現在ＩＳＯの議論に向けて日本案の作成が進行中である。

＜＜リスクマネジメントプロセスの要素＞＞（＊が小生の追加意見）

①＊課題の設定（目的を含む）；達成したい目標や解決したい課題を設定する。

②＊課題の保有者（オーナー）；目標や課題の所有者である。企業全体への適用に関しては株主が課題のオーナーにあたる。また部門に目標や課題を委託した場合は経営者や部門長などにあたる。個人の場合は課題の保有者と課題解決の責任者は同一となる。

©東京海上日動リスクコンサルティング株式会社　2007

③＊課題のガバナンス（責任者とオーナーとの関係）；課題解決にあたる責任者が定められる。責任者は課題の保有者から委任をうけて目標達成や課題の解決にあたる。そのためオーナーへの報告や重要な意思決定にあたり承認・レビュー過程が必要となる。企業全体のリスクマネジメントでは株主によるガバナンスの対象となり、コーポレートガバナンスを構成する。階層構造をとる企業内部では、各階層の責任者は上位階層のガバナンスを受ける。

④課題の解決のための環境；課題解決のための外部環境や内部資源の制約条件である。

⑤リスク分析（リスクの発見・特定およびリスク算定）

⑥リスクアセスメント（リスク評価）

⑦リスク対策計画策定（回避、低減、移転、保有）；保険等リスクファイナンスはこの一部である。リスク顕在化の未然防止策およびリスク顕在化後の事後対応策の準備も含む。

⑧対策の実施；統制活動の実施。リスク顕在化後の事後対応・危機管理を含む

⑨実施結果の監視（モニタリング）；自己点検、実施状況、結果の確認などを含む

⑩実施結果の評価（責任者の評価）；目標達成や課題解決のための責任者によるレビュー

⑪その他の項目；状況によっては必須となる可能性のある重要項目

オーナー・責任者、関係者との情報共有を諮るリスクコミュニケーション、外部からの助言をもらうコンサルティングがある。＊AS/NZS4360 ではひとつの項目であるがこの２つを別項目とする。（なお、内部統制では必須である監査は、組織を前提とした場合には必要となるプロセスであるが、個人の場合は必須ではないため要求事項としない）。（図７参照）

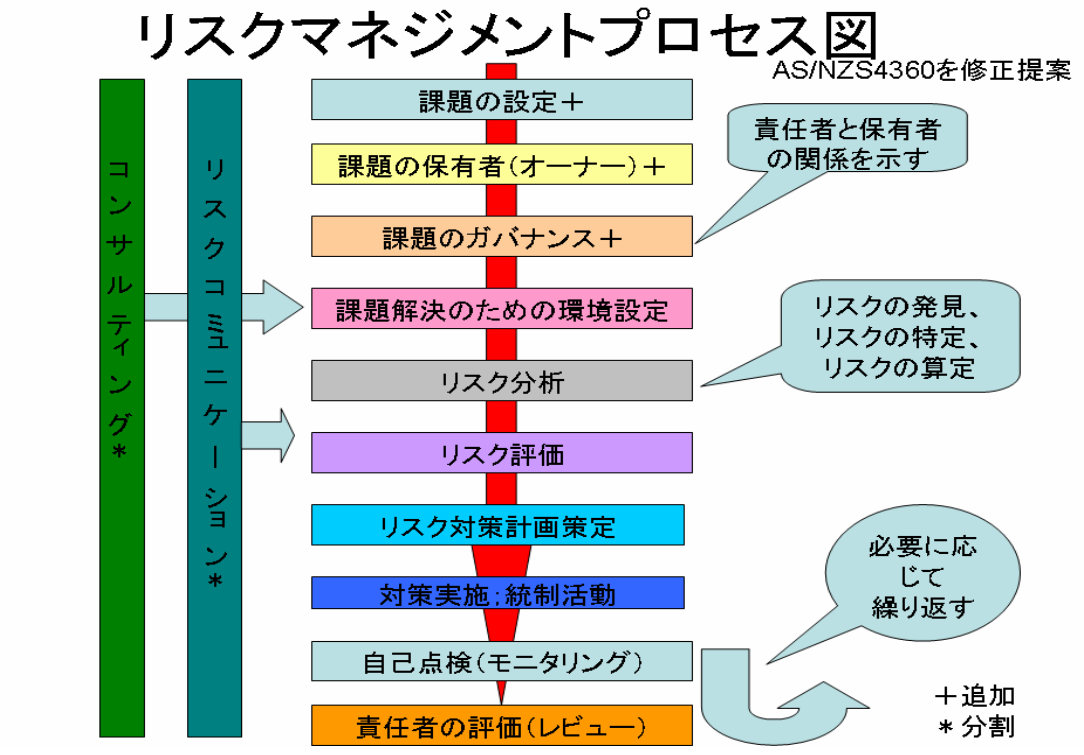


図7　リスクマネジメントプロセス図

©東京海上日動リスクコンサルティング株式会社　2007

（３）リスクマネジメントプロセスとリスクマネジメントシステムの解説

リスクマネジメントシステムはリスクマネジメントプロセスのうち組織を前提とし、日常の予防活動を中心とした継続的な活動における応用例と捉える。グループ経営を含む企業に適用する場合は企業の階層構造に合わせ、一番大きな枠組みが企業グループ全体の継続的発展を目的とした ERM であり、その場合「課題」が「企業の事業目的の遂行を阻害する要因の排除」であり、課題の保有者は法的に言えば株主である。課題の解決の責任者として経営者は株主から委任されており、ここにコーポレートガバナンスが存在する。リスクマネジメントシステムは企業全体から、各組織毎、各部門毎、グループ会社等企業の階層構造に伴って階層化される。各下位組織で実施されるリスクマネジメントシステムは課題の設定や責任者の委任などについて上位階層のガバナンスを受ける。（図８参照）

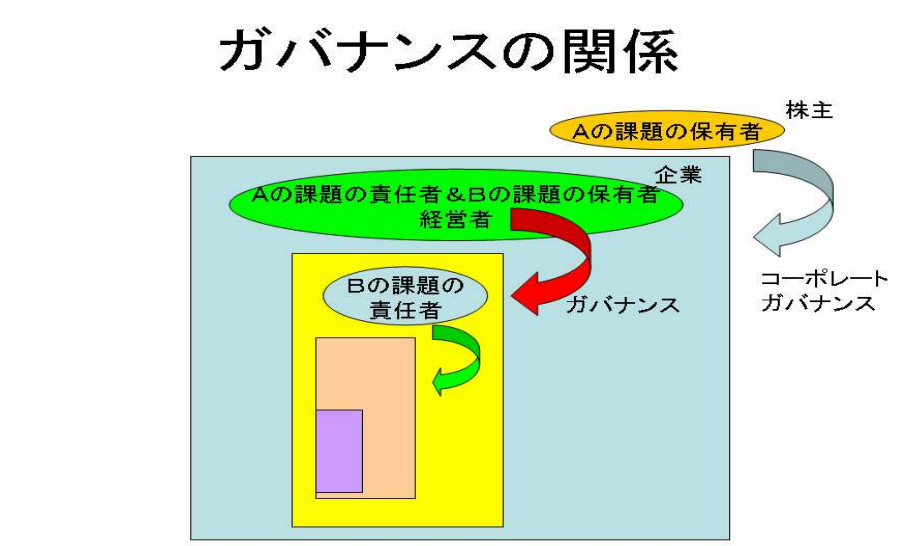


図8　リスクマネジメントシステムのガバナンス

５．まとめ

リスクマネジメントについて JISQ2001 や Guide73 の定義は必ずしも浸透していないため、当事者間で必ず用語と概念の確認をしてから議論をすべきである。リスクマネジメントはリスクマネジメントシステムとリスクマネジメントプロセスを区別すべきである。リスクマネジメントシステムはリスクマネジメントプロセスを組織に適用した応用形態である。リスクマネジメントシステムに事業継続と危機管理は内包される。またリスクマネジメントシステムを企業グループ経営に適用させた概念が全社的リスクマネジメント（ＥＲＭ）にあたる。一方、リスクマネジメントプロセスはすべての意思決定に適用できるモジュールであり、製品開発や事業継続や危機管理の各行動にも適用できる。

©東京海上日動リスクコンサルティング株式会社　2007

http://www.tokiorisk.co.jp/

追記

本論文を執筆中恩師である東京大学廣井脩教授が亡くなられた。図３「JISQ2001 と事業継続ガイドラインの関連図」は亡き廣井先生から整理するように宿題を投げかけられて作成したものであったが、生前説明する事が出来なかった。この場を借りて公表するとともに先生のご冥福をお祈りいたします。

参考文献

1）日本工業標準調査会；リスクマネジメントシステム構築のための指針 JISQ2001（2001 ）

2）財団法人日本情報処理開発協会；わが国における情報セキュリティの実態―「情報セキュリティに関する調査」集計結果―平成１８年；p4（2006）

3）財団法人日本情報処理開発協会；わが国における情報セキュリティの実態―「情報セキュリティに関する調査」集計結果―平成１６年；p4（2004）

4）財団法人日本規格協会；JISTRQ0008 リスクマネジメント―用語―規格に使用するための指針 2003 年　＜ISO／IECGUIDE73；2002＞（ 2003）

5）経済産業省商務情報政策局情報セキュリティ政策室編；事業継続計画（ＢＣＰ）策定ガイドライン；財団法人経済産業調査会（2005）

6）内閣府；事業継続ガイドライン（第一版）（2005）；
http://www.bousai.go.jp/MinkanToShijyou/guideline01.pdf

7）八田進二監訳；全社的リスクマネジメント、フレームワーク編（東洋経済新報社 2006）

8）東京海上日動リスクコンサルティング；リスクマネジメントがよ～くわかる本；p31-32（秀和システム 2004）

9）丸谷浩明、指田朝久編著；中央防災会議「事業継続ガイドライン」の解説と Q&A（日科技連 2006）

１０）経済産業省中小企業庁；中小企業ＢＣＰ策定運用指針；http://www.chusho.meti.go.jp/bcp/

１１）野口和彦；リスクマネジメントの今日を読む　始まった ISO 規格への議論；標準化と品質管理 Vol59　No2；p4-p12（2005）

１２）徳谷昌勇；リスクマネジメントと内部監査； CUC（view&vision）第９号千葉商科大学経済研究所　2000 年 3 月号

１３）オーストラリア、ニュージーランド規格協会 Risk　Management；AS/NZS4360:1995：(1995)

（本論文は２００７年５月２６日に危機管理システム研究学会；危機管理システム研究学会ＡＲＩＭＡＳＳ研究年報第５号に報告文として掲載されました）

©東京海上日動リスクコンサルティング株式会社　2007