事業リスク評価・管理人材育成システム開発事業

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

平成17年3月

経済産業省

目次

本テキストについて

「事業リスク評価・管理人材育成システム開発事業」と本テキストの位置付け

本テキストは経済産業省「事業リスク評価・管理人材育成システム開発事業」の一環として作成されました。

近年、企業を取り巻く環境の変化のスピードは加速傾向にあり、その結果、各企業が直面するリスクが急速に増加かつ多様化しています。一方で、これらのリスクを適切に管理できる人材が不足していることから、その育成が急務となってきました。

このような状況の下、平成15年度から経済産業省は「事業リスク評価・管理人材育成プログラム」を開始しました。初年度はリスクマネジメントを担う高度専門人材が保有すべき標準的スキルを解説したテキスト『事業リスクマネジメントテキスト』を作成し、理論編として事業リスクマネジメントの理解・知識の習得を目指しました。

本テキストは上記知識を実務の中で活用する方法の提示を求める企業の声を受け、リスクマネジメントの実践に具体的に役立つ実務編として開発されたものです。

本テキストの目的

本テキストを開発するにあたり、リスクマネジメントの取組みにおいて多くの企業がどの段階にあるのかを検討するために、2003年度事業リスク評価・管理人材育成システム開発事業の一環として行われたアンケート結果を再度分析しました。次ページで示す「リスクマネジメントのレベルマップ」はその分析結果を示しています。

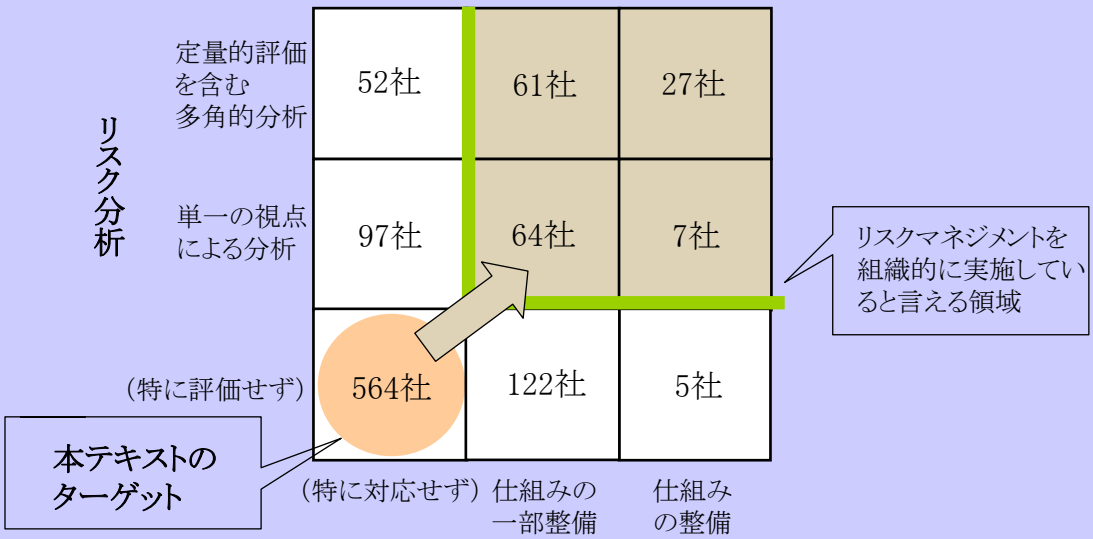
この分析結果から、半数以上の企業がリスクの評価も体制の整備も十分でないことがわかりました。このような企業に必要なのは高度なリスク分析に関する実務指針よりも、リスク評価を含むリスクマネジメントに組織的に取り組むためにまず何をすべきかを示すことです。そこで本テキストは、これからリスクマネジメントに着手しようとしている企業を対象とし、これらの企業がリスクマネジメントに組織的に取り組んでいく際に必要となる知識の提供を目指しました。

またそのための方法として、リスクマネジメントの先進企業における取組みを多く紹介することにより、企業のリスクマネジメント担当者が実務の中で活用できる実践的な内容とすることを目指しています。

これらを踏まえ、本テキストの目的を以下の通りとしました。

先進企業の取組み事例を含む実践的な情報を提供することにより、リスクマネジメントにこれから取り組もうとする企業の実務者が、組織への導入にあたって実施すべき事柄と留意点について具体的なイメージを持てるようにすること

リスクマネジメントのレベルマップ



リスクマネジメントの仕組み

アンケート回答企業の属性:
2003年事業リスク評価・管理人材育成システム開発事業
同年7月～11月に国内有力企業に対して行ったアンケート調査より作成
国内主要株式市場上場企業約3,597社に対して調査票を送付し、1009票の回答を得たもの(無回答10社)

評価軸の説明

リスクマネジメントの仕組み
「貴社で作成または利用されているリスクマネジメントガイドライン等がありますか」
「貴社のリスクマネジメント体制についてあてはまるものをお選びください(複数回答)」より作成

仕組みの整備:充分な体制と自社で作成した体系的なガイドラインがある
仕組みの一部整備:体制またはガイドラインが一部整備されている
特に対応せず:体制もガイドラインも未整備

リスク分析
「具体的にリスクの特性や影響度、発生頻度等について調査、分析したことがありますか(複数回答)」より作成

定量的評価を含む多角的分析:定量的評価、定性的評価、およびリスクの原因、因果関係による分析手法のうち定量的評価を含む複数面からの分析を実施
単一の視点による分析:定量的評価、定性的評価、リスクの原因、因果関係による分析のうちどれか1つの視点で分析を実施
特に評価せず:具体的な調査・分析にまで至っていない

本テキストの特徴

先達に学ぶ

- リスクマネジメント先進企業17社のリスクマネジメント実務担当者にヒアリングを行い、日本企業のリスクマネジメントの現場で実際に行われている取組みを多く紹介しています。また成功要因や乗り越えなければいけないポイント等、これから体制を構築する企業が遭遇すると予想される事に関して道標となるような情報も、貴重な経験談を基に抽出し掲載しています。

全社的なマネジメントシステムの構築ステップをPDCAで解説

- 企業としてリスク情報を集約し対策を講じるためのマネジメントシステムの構築について、そのステップをPlan-Do-Check-ActのPDCAサイクルに従って解説しています。また同じくPDCAサイクルに則った「JIS Q 2001 リスクマネジメントシステム構築のための指針」を整理のためのフレームワークとして参考にしています。

複数の選択肢を紹介

- 企業におけるリスクマネジメントは一つとして同じものがありませんので、企業に合った方法を選択していただくために、なるべく複数の選択肢と、選択の際の留意点を紹介しています。

2003年度テキスト(『事業リスクマネジメントテキスト』)との関係

2003年度に開発された『事業リスクマネジメントテキスト』と本テキストの関係は以下のとおりです。どちらも同じ事業リスクマネジメントを解説していますが、本テキストでは2003年度テキストで得た知識を組織的な取組みの導入に役立てることを意図し、マネジメントシステムに焦点を当てています。

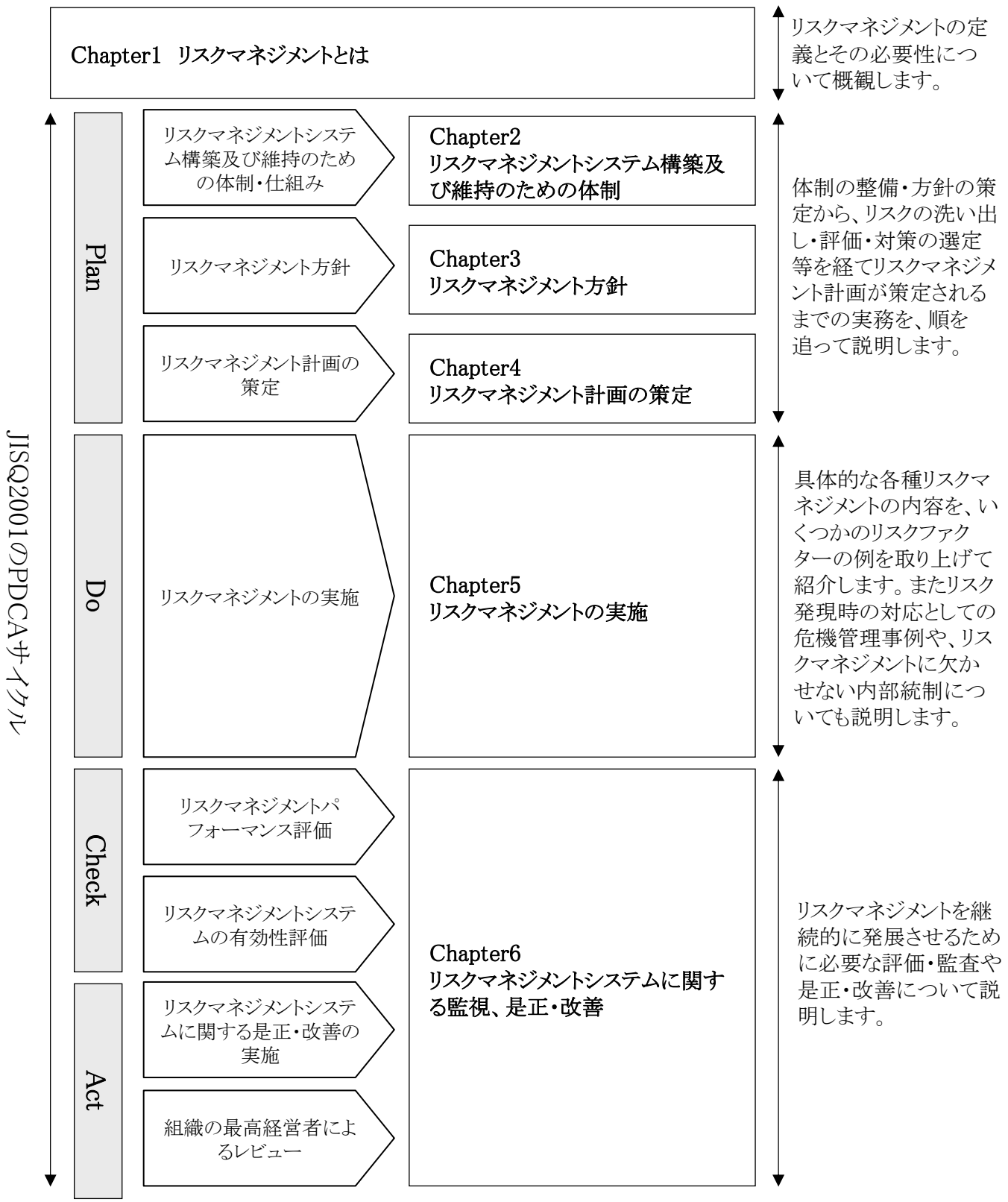
テキストの利用方法としては、2003年度テキストを使った研修等で知識を得た読者が、本テキストを参照しながら実務を行うことを想定しています。ただし本テキストのみでも最低限必要な事項は把握できるようになっています。また2003年度テキストの参照ページを随時示しています。

2003年度テキスト	本テキスト
理論編	実践編
知識の習得が目的	実務での活用が目的
手法に焦点	マネジメントシステムに焦点
基礎から高度な技法まで体系的に紹介	企業の実例に基く留意点を多く紹介

本テキストの構成

本テキストはJISQ2001のPDCAサイクルを参考にした章立てになっています。

Chapter1では導入として定義の説明等を通じてリスクマネジメントそのものについて概説します。その上で、リスクマネジメントシステムの構築・維持の実務をPDCAサイクルに従ってChapter2からChapter6で説明していきます。

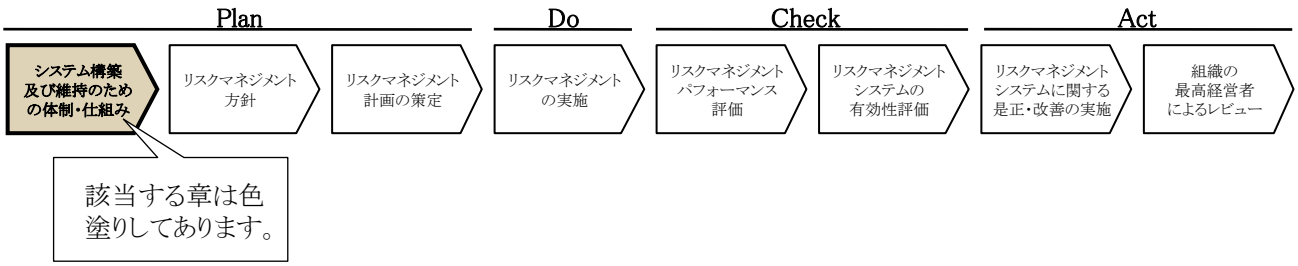


本テキストの読み方

本テキストは前述のようにJISQ2001の規格に沿い、PDCAサイクルをもとに章立てされています。

事業リスクマネジメントに関する主な説明は、2003年度事業リスクマネジメントのテキストを引用しています。2003年度テキストは、経済産業省のホームページより参照が可能です。
（経済産業省ホームページ内白書・報告書「－創業・起業促進型人材育成システム開発等事業－事業リスク評価・管理人材育成システム開発事業」）

章のはじめには、当該章がPDCAサイクルのどこに位置しているかを示す図を入れています。（下図参照）PDCAサイクルを意識しながら、テキストを参照してください。



その他見出しの構成やヒアリングより収集した事例やノウハウは以下のような凡例に基づいて説明しています。

X.X 大項目のタイトル

大項目内で論じる概要を説明しています。

X.X.X 中項目のタイトル

小項目のタイトル

小小項目のタイトル

大　見出しの構成と議論の構造　小

私たちが先進企業に対して実施したヒアリングから得た実例です。

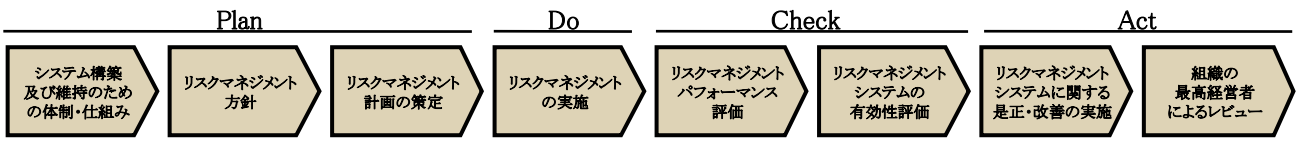
事業リスクマネジメントを実施する上で、私たちが特に重要だと認識する事柄です。

- 事例をもとにした考察や事例を補う説明です。

CHAPTER 1

リスクマネジメントとは

1.1 事業リスクマネジメントシステム構築の意義
1.2 リスクマネジメントの定義



本章では事業リスクマネジメントシステム構築の意義について、まず説明し、次に本テキストにおけるリスク、リスクマネジメント及び事業リスクマネジメントの定義を紹介した上で、その他の規格における定義を説明します。

この中でリスクマネジメントと危機管理の違いについても説明します。

リスクマネジメントにおいては、リスクという言葉の定義やリスクマネジメントのフレームワークについて共通の認識を持つことが必要最低限の要件となります。リスクは形がなく捉えどころがないため、言葉の定義を明確にしておかないと人によって違う意味を想定する場合があるためです。ヒアリングの中でも自社におけるリスクの定義について何度も議論を重ねたという声が聞かれました。

リスクの定義はすべてのリスクマネジメントの原点となるため、非常に重要なものであるといえます。このことはリスクマネジメントに取り組む中で皆様が今後何度も実感されることでしょう。

この章の内容

1.1 事業リスクマネジメントシステム構築の意義

1.1.1 部門別リスクマネジメントから統合的な事業リスクマネジメントへ

経営環境の変化

部門別リスクマネジメントの問題点

事業リスクマネジメントに取り組み始めたきっかけは

1.1.2 事業リスクマネジメントシステムの必要性とメリット

経営トップは事業リスクマネジメントへの関心を高めざるを得ない

事業リスクマネジメントの重要性を見直す動き

事業リスクマネジメントシステム構築のメリット

事業リスクマネジメントシステムを構築する際の費用等

1.2 リスクマネジメントの定義

1.2.1 リスクとは

リスクの定義例

1.2.2 リスクマネジメントとは

リスクマネジメントの定義例

1.2.3 事業リスクマネジメントとは

ERMの定義例

1.2.4 リスクマネジメントと危機管理

1.1 事業リスクマネジメントシステム構築の意義

ここでは「なぜいま全社的なリスクマネジメントシステムが必要とされているのか」に関して
・ 事業リスクマネジメントシステムの必要性とメリット
・ 事業リスクマネジメントシステム構築への関心の高まり
について説明します。なお、リスクマネジメントシステムとは、リスクマネジメントを実施するための体制や手続き等の仕組みを指します。

1.1.1 部門別リスクマネジメントから統合的な事業リスクマネジメントへ

昨今「リスクマネジメント」という言葉を目にする機会が多くなりました。しかし従来より「リスクを管理する」という概念は存在していたため、特に目新しい物ではない、昔から実施している、と感じている企業も多いようです。

こうした従来型のリスクマネジメントは、主に各部門や部署別に実施されてきました。その役割を担う人材が部門の中に存在し、その道の経験側の中で発見したリスクをマネジメントするという形です。多くの場合リスクの発見から対応まで部門の中で完結して遂行され、経営トップや他部門に逐一情報が伝わることはまれでした。

一方事業リスクマネジメントは、リスクを企業として把握し適正に管理することで、リターンを最大にすることを目指すものです。そのためにはリスク情報の集約や明確な管理体制が非常に重要になります。これにより全体最適かつ機動力のあるリスク対応が可能になり、また対外的な説明責任を果たす土台が整うことになります。

経営環境の変化

事業リスクマネジメントの必要性が高まった背景として、『リスク新時代の内部統制』(経済産業省　2003年)は以下の4点の環境変化を挙げています。

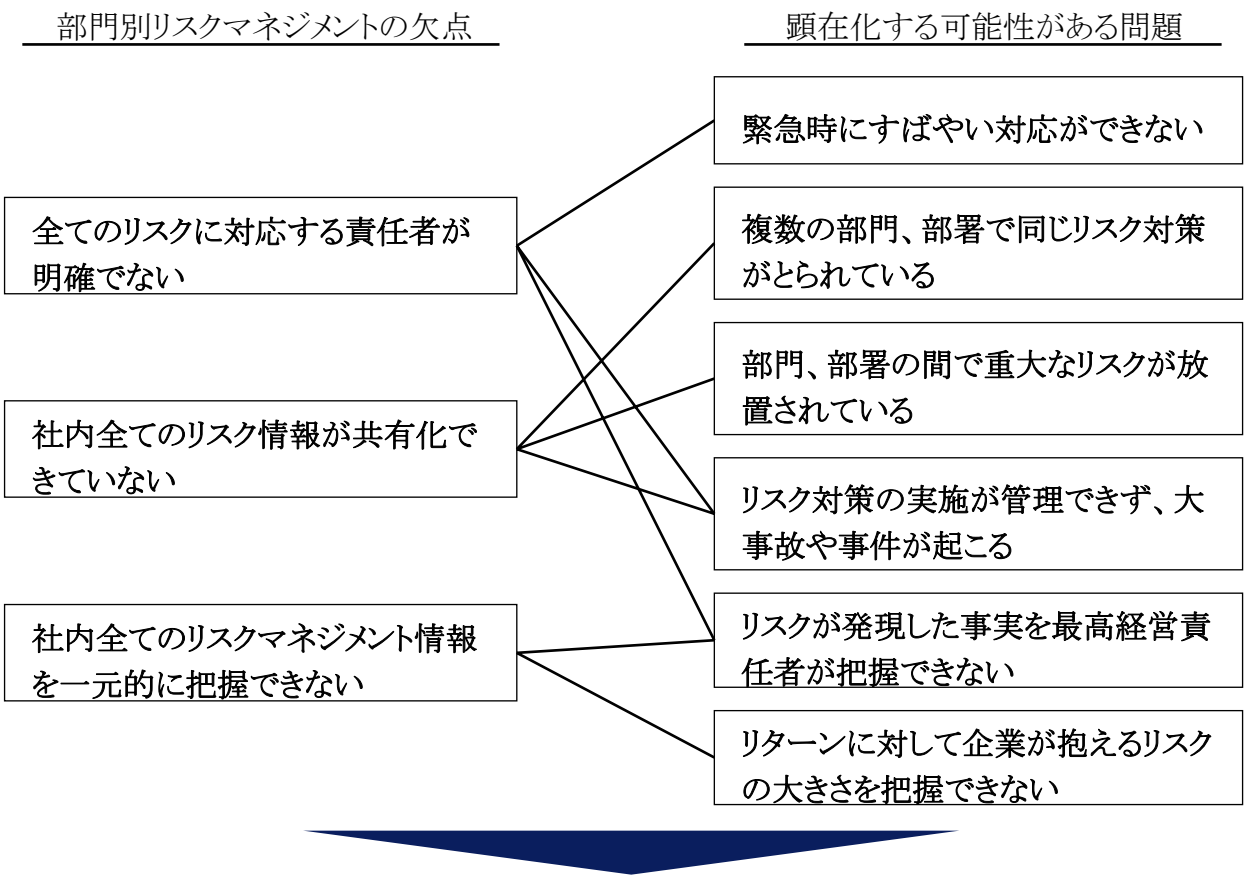
「・ 規制緩和の進展
規制緩和が進み、自己責任に基づく事後規制へと社会的枠組みが変わっていく中で、企業がそれぞれの判断でリスクを管理し、収益を上げていくことが必要となってきている。
・ リスクの多様化
急速な技術進歩、事業の国際化、事業展開のスピードアップ等に加えて、環境問題等の新たな社会規制がリスクをより多様なものとしている。
・ 経営管理のあり方の変化
当事者間の暗黙の了解や信頼関係のみに依存した経営管理のあり方に限界が生じてきている。
・ 説明責任の増大
市場経済が進展していく中で、リスクの特定、評価や対応を怠った場合、広範なステークホルダーに損害を与えるとともに、市場の信頼を失い、企業自らも厳しいペナルティを受けることになる。

つまり、外部環境としてリスクが多様化している中で、各企業には自己責任に基づいたリスクマネジメントの必要性が生じており、そのリスクマネジメントに関しての取組みをステークホルダーに適切に説明する責任が高まっていることが事業リスクマネジメントシステムの普及が望まれる理由です*。」

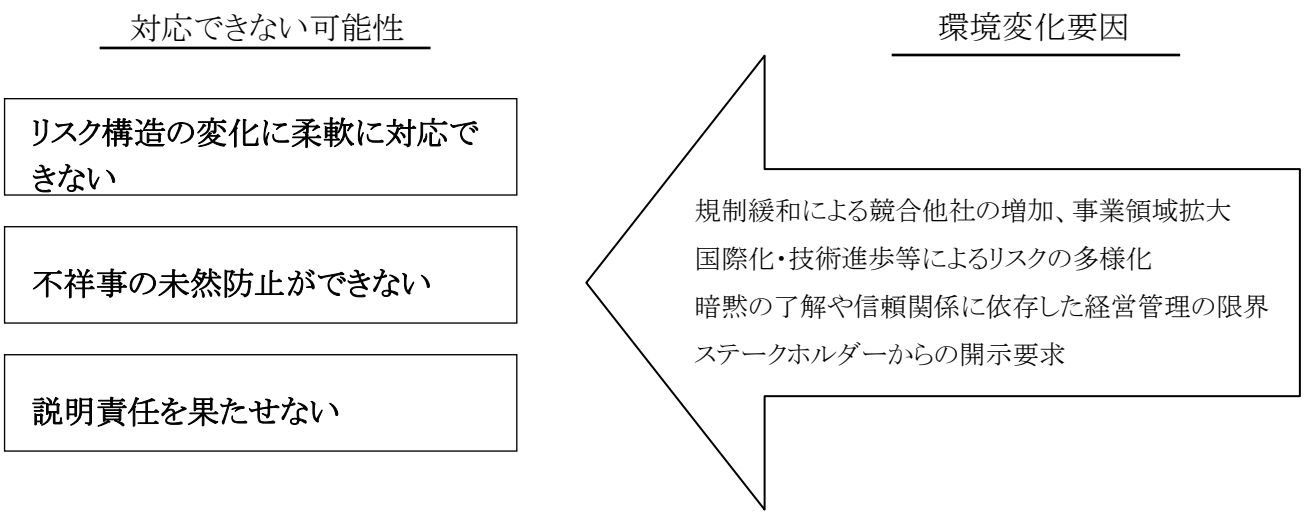
*『事業リスクマネジメントーテキストー 経済産業省 平成16年3月』 24ページより一部修正

部門別リスクマネジメントの問題点

部門別リスクマネジメントでは、企業が組織的にリスクに対応するための体制や情報の流れが整備されていない場合が多く、以下のような問題が顕在化する可能性があります。



これらの問題が顕在化した場合、環境変化への対応が充分にできない可能性も考えられます。



経営環境の変化に対応するためには全社的なリスクマネジメントシステムの構築が必要

事業リスクマネジメントに取り組み始めたきっかけは

多くの企業では以下のような契機で事業リスクマネジメントの実施を決定しています。

◆ 事故や不祥事の懸念

銀行や多くの企業が経営不振、倒産に追い込まれる中でステークホルダーの目を強く意識し始めた

他社の不祥事を他山の石とし、全社的なリスクマネジメント体制に取り組むことを決めた

- 部門で行われていることを経営トップが全く把握しておらず、ある日突然大きな事故や不祥事が発生するというケースが多く見受けられます。またそういった企業には社会からも厳しい目が向けられます。
- 全社的なリスクマネジメントシステムを実施することで、全てのリスクを企業として管理し「知らなかった」というような事態の発生を避けることが期待できます。またリスクが発現してしまった場合にも、そのリスクに対して的確に対応することが望まれます。実際、他社不祥事によって危機感を募らせ、事業リスクマネジメントを実施し始めたという企業が多いようです。

◆ 積極的なリスクテイクの必要性

規制緩和による競争相手の増加や事業範囲の拡大に伴い、新しい分野に挑戦して高いリターンを得る必要性が生まれた

得ようとするリターンに対し、リスクの大きさがどの程度であれば妥当なのか企業の体力を考慮の上、判断する必要性が出てきた

- 規制緩和やグローバル化の進展により、事業領域の拡大等のチャンスが広がる一方、従来は規制等に守られていた領域でも予想される他社の参入に対抗するために自己責任でリスクを取っていく必要が出てきました。
- このような状況に積極的に対応しようとする企業は、未知の事業や競争相手に対応するために、リスクについても多角的な情報を意思決定者がタイムリーに把握する必要があります。

◆ 積極的な情報開示に耐える体制整備の必要性

米国企業改革法への対応を機に、説明責任を充分に果たせるリスクマネジメント体制を構築することにした

- 米国の企業改革法では、上場企業にリスクマネジメント体制の確立を求め、またその情報開示を求めています。事業リスクマネジメントシステムは同法の要求事項よりは範囲が広い概念ですが、法制対応を実質的な企業価値向上の機会とすべく、導入をする企業もあります。
- 当然ながら情報開示のためには社内のすべてのリスク情報を集約する必要があります。
- 日本でも各種の情報開示への要求は高まっており、今後情報開示を一つのきっかけとしてリスクマネジメントシステムを構築する企業が増加すると考えられます。

1.1.2　事業リスクマネジメントシステムの必要性とメリット

部門別リスクマネジメントの限界や経営環境の変化により、事業リスクマネジメントの必要性は高まっていますが、事業リスクマネジメントの実施は企業経営において非常に重要な課題であると考えられます。

ただし実際の日本企業のリスクマネジメントに対する取組みはまだ進んでいないと言えます。「リスクマネジメントの必要性自体は認めるものの、直接収益をもたらす業務とは言いがたいため手が回らない」というのが実情だと思われます。しかし、近年急速にリスクマネジメントの必要性が認識されており、徐々に体制が整備されているのも事実です。

しかし一方で「リスクマネジメントの重要性が認識されるにつれて、全社横断的にリスクを監視、評価したり、リスク対策の窓口となる組織、リスクマネジメント専管部門、部署やリスク管理委員会を設置する企業が増えています。また、近年IR（インベスターリレーション）の観点からリスク情報、リスクマネジメントに関する情報提供、情報開示のニーズが高まっているため、こうした組織でリスク情報の管理を行うようになってきています。*」

*『事業リスクマネジメントーテキストー 経済産業省 平成16年3月』29-30ページ より一部修正

最近では経営トップに求められる責任も変化してきており、事業リスクマネジメントへの関心を高めざるを得ないとも言えます。

経営トップは事業リスクマネジメントへの関心を高めざるを得ない

経営トップに求められる責任は日々変化しており、経営トップを中心とした事業リスクマネジメントシステムの構築に対する要求は高まっています。

大手銀行ニューヨーク支店損失事件に係る株主代表訴訟判決

1995年大手銀行ニューヨーク支店行員が11年間にもわたり無断取引等を行い、銀行に11億ドルもの巨額の損失を負わせていたことが発覚した。本件に関し、当時の取締役に善管注意義務及び忠実義務の違反があったとして、株主による損害賠償請求が行われた。

2000年9月20日大阪地方裁判所では、現・元取締役ら11人に総額7億7500万ドル（約830億円）の賠償命令を下した。

- 本判例は全社のリスクマネジメントに対する最高経営責任者の責任を明確に示した判例となりました。
- 最高経営責任者には社内のリスクに目を配り、対応していくことが求められています。

有価証券報告書のリスクに対する情報開示要求

2003年4月1日以降、有価証券報告書において「リスクに関する情報」、「コーポレート・ガバナンスに関する情報」の開示が原則適用されることになった。

- リスクに関する情報では当該企業の認識するリスクが開示されることになりました。コーポレートガバナンスに関する情報では、リスクに関する企業内の体制も開示されることになりました。
- この情報開示要求はステークホルダーのリスクマネジメント情報の開示に対する関心の高さと、最高経営責任者の責任明確化が求められた結果であるといえます。
- ステークホルダーの理解を得られるような形でリスク情報を開示するためには、社内のリスク情報を把握できる体制が企業内で整備されていることが必要になります。

東京証券取引所による有価証券報告書等確認書提出および、宣誓義務

有価証券報告書の虚偽記載を含む記載や誤りが相次いだため、東京証券取引所では2005年より有価証券報告書と半期報告書について「有価証券報告書等の記載内容の適正性に関する確認書」の提出を義務付けた。また、適時適切な会社情報開示の観点から上場会社に、開示情報の正確性等を宣誓させる旨を決定した。宣誓事項について重大な違反を行った場合には、上場廃止の対象となる。

- 経営に対して今まで以上に最高経営責任者の責任が厳格に求められるようになっています。
- ステークホルダーや社会に対する責任がより具体的に求められています。

上記3つの例から言えることは、不祥事防止や情報開示の大前提として、最高経営責任者自らが自社のリスクや重要事項を的確に把握することが社会から強く求められている、ということです。そのための体制構築は最高経営責任者の責任になります。ここで言う「把握」とは単に「知っているつもり」では不十分で、外部への説明責任が伴うものです。

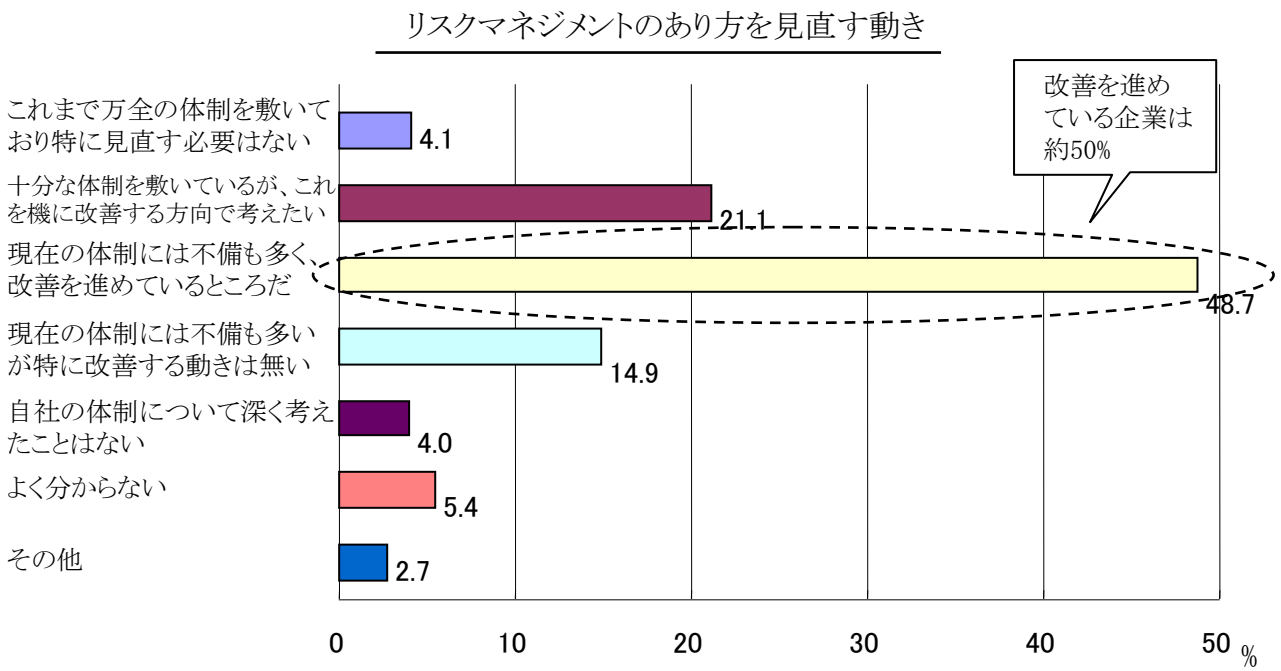
このような体制構築が不十分なために、最高経営責任者が社内の重要事項を把握出来ていないケースは往々にしてあったと考えられますが、今後は大きなペナルティを課される可能性を孕んでいます。

経営トップは全社のリスクについて「知らなかった」では済まされない

事業リスクマネジメントの重要性を見直す動き

リスクマネジメントに関して実施されている様々なアンケートを通じて、事業リスクマネジメントへの関心が高まっていること、事業リスクマネジメントシステムを導入する企業が増えてきていることが明らかになってきました。

参考 リスクマネジメントのあり方を見直す動き

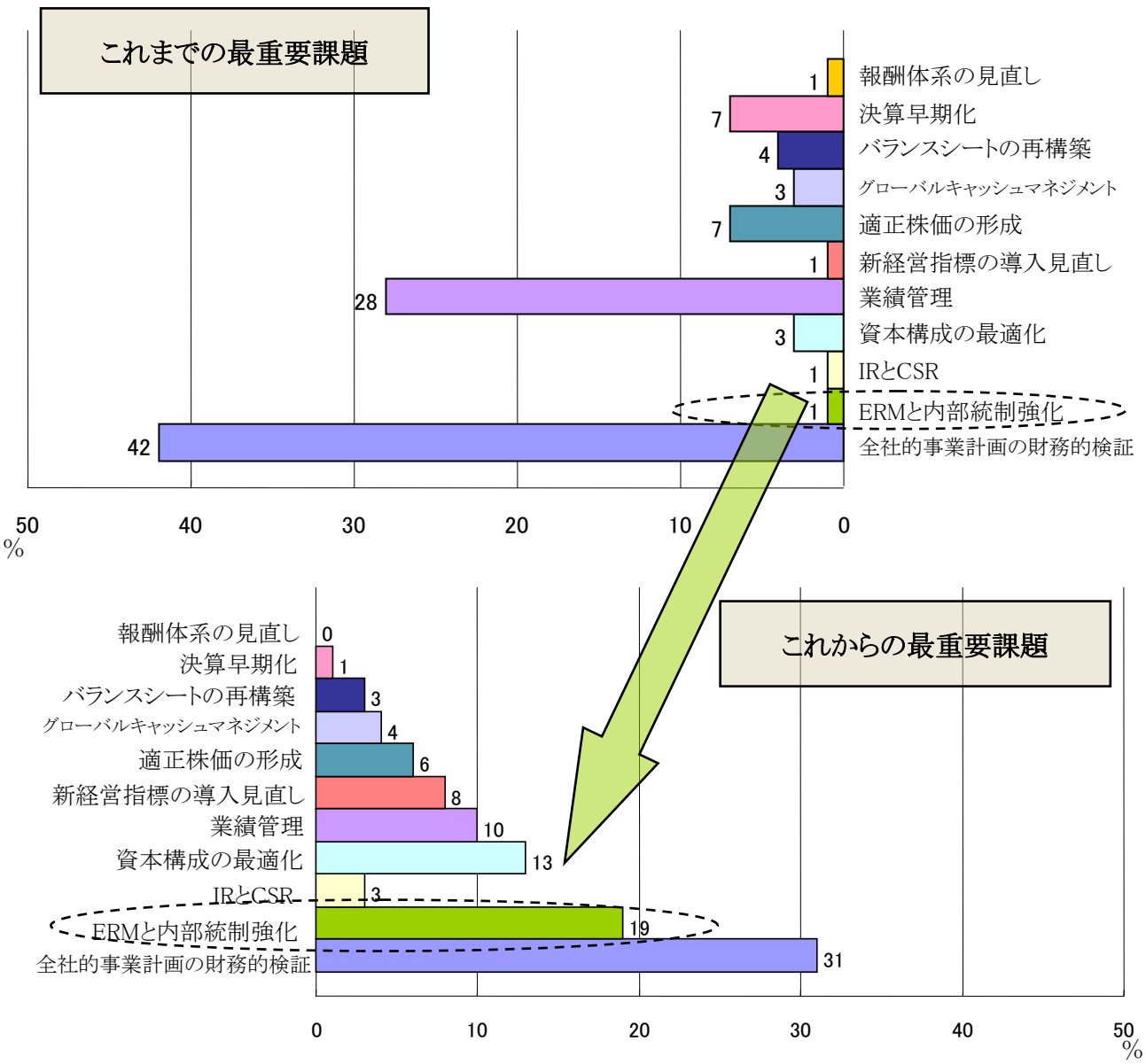


2003年事業リスク評価・管理人材育成システム開発事業
同年7月～11月に国内有力企業に対して行ったアンケート調査より
国内主要株式市場上場企業約3,597社に対して調査票を送付し、1009票の回答を得たもの
「貴社では、リスクマネジメントのあり方を見直すような動きはありますか」(複数回答)

- このアンケート結果からは、現在のリスクマネジメント体制からの改善を図っている企業が約50%を占めることが明らかになっています。
- これは、従来の部門別リスクマネジメントでは管理体制として十分でないという意識の表れであると言えます。

参考 | **事業リスクマネジメントの重要性を見直す動き**

CFO（財務担当役員）の考える今までの最重要課題とこれからの最重要課題

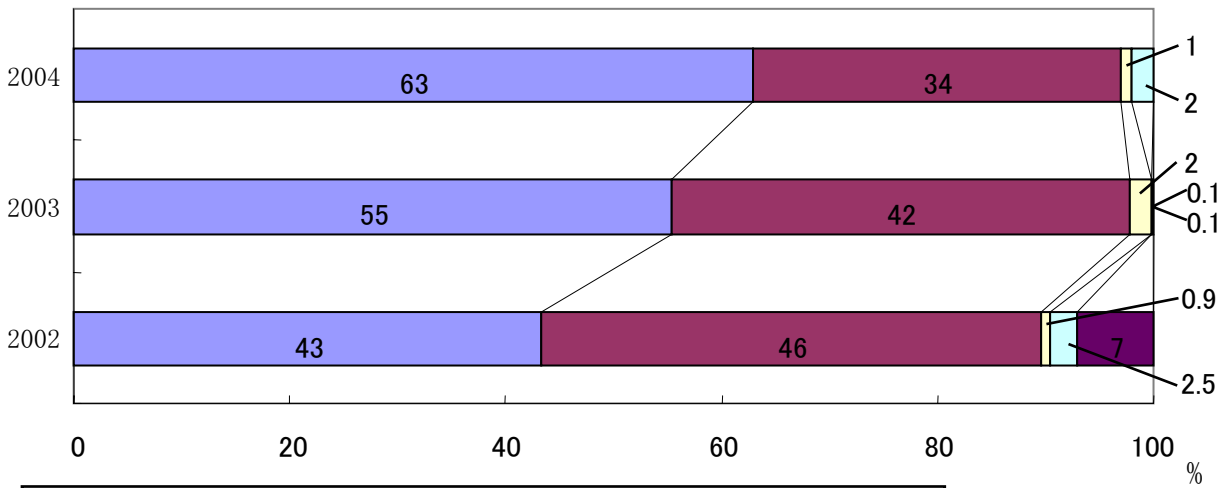


日本ピープルソフト株式会社　2004年12月16日　プレスリリース『日本CFO協会と日本ピープルソフト、上場企業財務担当役員の「財務報告と内部統制」に対する意識調査を発表』より作成
日本CFO協会では、年4回「財務マネジメントサーベイ」を実施。その一環として日本ピープルソフト株式会社企画のもと実施されたアンケート。
無作為に抽出された上場企業500社のCFOに調査票を送付。回答72社。
（回答企業：製造業63%、グループ年商1000億円超が54%、グループ従業員数1000人超が68%）

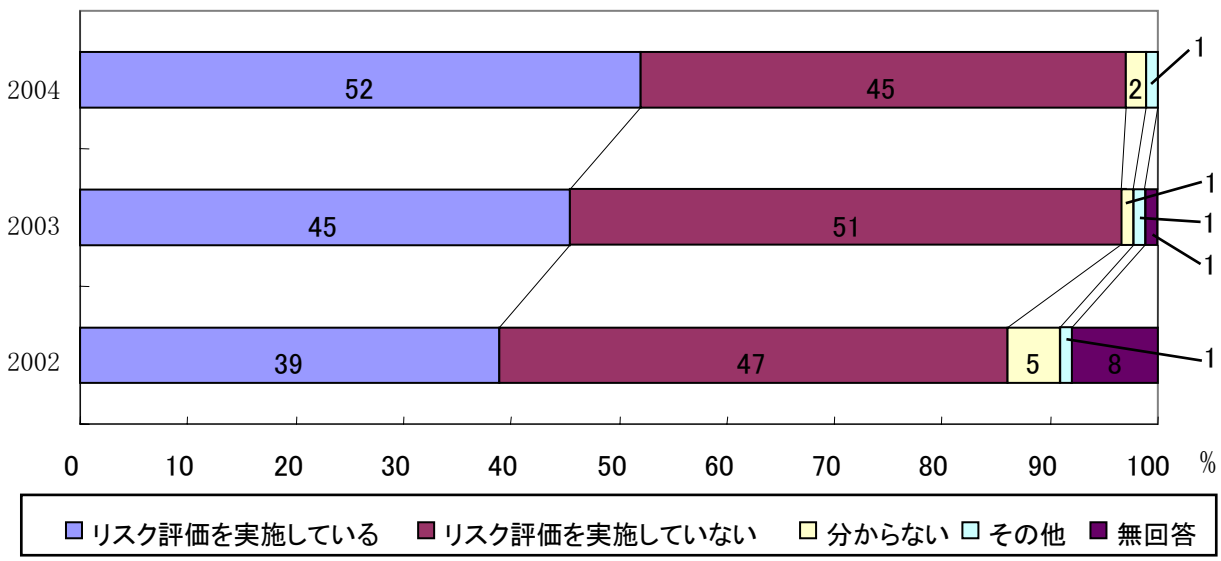
- これからの最重要課題としてERMと内部統制の強化と答えたCFOが著しく増加しました。
- この結果からオペレーション重視からERMと内部統制強化という企業の意識の変化がCFOの意識の変化にも影響したということが考えられます。

参考 | **事業リスクマネジメントの重要性を見直す動き**

リスク管理部署及びコンプライアンス統括部署の有無



リスク評価実施の有無



監査法人トーマツ　エンタープライズリスクサービス部
2002年 「企業リスク対策アンケート調査報告」:東京、大阪、福岡、名古屋の4会場で計6回に開催した「コンプライアンス経営セミナー」において、出席企業に対してリスク対策に関するアンケートを実施。2002年5月～6月にかけて調査実施。561社が回答。
2003年 「企業リスク対策アンケート調査報告-2003年実績及び昨年からの推移-」:東京、大阪、福岡、名古屋の4会場で計6回開催した「コンプライアンス経営セミナー」において、出席企業に対してリスク対策に関するアンケートを実施。2003年3月～6月にかけて調査実施。209社が回答。
2004年 「企業リスクマネジメントアンケート調査報告」:2004年10月同研究所が発行する季刊誌「企業リスク」の読者に対するアンケート調査、2004年9月28日に東京で実施されたセミナー、2004年12月7日・8日に東京・大阪にて実施したセミナー時に行ったアンケート結果を集計。301社が回答より作成

- リスク管理部署またはコンプライアンス統括部署を設置している企業は徐々に増加しており、リスク評価を実施している企業も増加しています。

事業リスクマネジメントシステム構築のメリット

以下に事業リスクマネジメントシステムを構築するメリットを示します。事業リスクマネジメントを実施すれば、以下のような効果を得ることができるでしょう。

ステークホルダーへの信頼性と透明性を確保できる

- 企業の事業リスクマネジメントシステムに対しステークホルダーが高い関心を持っていることは、有価証券報告書のリスクに対する情報開示要求などからも明らかです。全社的なリスクマネジメントシステムを構築して社内外にアピールすることは、企業の信頼性と透明性を確保することにつながります。

格付会社へのアピールが可能になり、企業イメージが向上する

- 格付会社に「御社では事業リスクマネジメントに取り組んでいますか」という質問を受けたことで事業リスクマネジメントに対する意識が高まったという企業がありました。
- 実際、格付会社では、企業のリスクマネジメントへの取組み状況に高い関心を寄せており、格付に際しては当該企業においてどのようなリスクが認識されているのか、そのためにどのようなマネジメントが行われているのかということが考慮され、決定されます。また、この場合市場リスク、為替リスク、金利リスクなどの定量的なリスクのみではなく、コンプライアンスやレピュテーションなどの定性的リスクに関しても判断材料とされます。

リスクを明確に把握、管理することで保険料の削減が可能になる

- 全社のリスクを把握することで、社内で対策を取ることが可能なリスクと、保険によって移転されるべきリスクが明確に判断できるようになります。各部門や部署でのリスク対策で保険によるリスクの移転が行われていたような場合でも、事業リスクマネジメントシステムの運用による明確なリスク対策の策定と社内のリスクに対する意識の向上により、保険を掛ける必要がないという結論になる場合もあるかもしれません。
- 実際、事業リスクマネジメントを実施しロスプリベンション（損害防止の活動）を徹底することで、保険料の削減に成功している企業もあります。

リスク対策にかける費用の配分を適切に行うことが可能になる

- 各部門や部署で独自に実施しているリスク対策の適切性、つまり対策が必要十分で重複がなく、過度でないことを全社の視点から評価することが可能になるため、リスク対策費用の適正配分が可能になります。

リスクとリターンの関係を使い、共通の尺度で意思決定できるようになる

- 想定されるリスクの大きさに対して、企業は十分なリターンを得られるのかに関して、新規事業や投資の決定時に全社的視点で判断を行うことが可能になります。

事業リスクマネジメントシステムを構築する際の費用等

事業リスクマネジメントシステムを構築する場合、費用、つまり、時間・労力・金銭的支出がかなり伴うため実施に踏み出せないという話がありました。しかし実際には様々な進め方があり、懸念されるほど大きな費用がかからず構築できた例もあります。

費用は事業リスクマネジメントシステムの構築の仕方により様々

大きな費用をかけずに構築することも可能

- 当該作業を実施する人材は、リスク管理部署のメンバーと各部門や部署のリスクマネジメントシステム担当者が中心となります。全社的な活動であるため、リスクマネジメントの基本単位とする部署の数や1部署あたりの関与人数によって総時間数は変わってきます。
- 要する時間や労力については、通常、リスクマネジメントサイクルは年単位で実施されるので、リスクの洗い出し、評価、監査など工数のかかるものに関しては、年1回程度の作業になります。
- 特にリスクの洗い出し、評価に関しては、2年目以降は前年の情報の見直しが中心になり、初年度ほどの労力はかかりません。
- 一度にすべてのことをスタートさせるのではなく、できることを一つ一つ確実に実施していくことで作業にかかる負荷を分散することが可能です。
- 全社のリスクマネジメントを統括するリスクマネジメント委員会は、活動報告を受けるため、年二回程度開催されるのが標準的であり、臨時の開催を含めても時間的負担は限定的であると考えられます。
- 金銭的支出に関しては、外部のコンサルタントを利用する場合と自社の人材のみで取り組んだ場合では大きな差が出てきます。それ以外で大きな支出の要素はありません。

1.2 リスクマネジメントの定義

ここではリスクやリスクマネジメントとは何かについて、その定義を説明していきます。
必ずしも確立された定義があるわけではないため、代表的な基準やフレームワークにおける定義を参照しながら、本テキストでの定義を提起します。また先進企業が自社における定義として採用している内容についても紹介していきます。

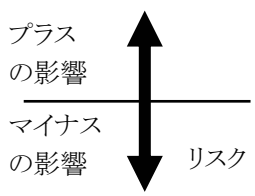
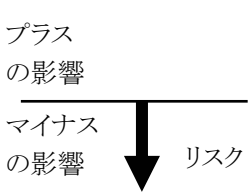
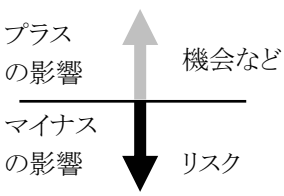
1.2.1 リスクとは

「リスク」という言葉は色々な場面で多様な使われ方をしており、すべてを包括するような定義をすることは難しい状況です。
本テキストでは特に断りの無い限り、昨年度テキストでの定義を継承し、リスクをプラス・マイナス両方あるものとして捉えます。

リスクとは

組織の収益や損失に影響を与える不確実性

「リスク」にはゼロまたはマイナスの結果をもたらす概念と機会創出をもたらすプラスの概念があります。

		
プラスの影響、マイナスの影響どちらも与えるものである	マイナスに影響をするもののみを言い、プラスの影響は視野に入れない	マイナスに影響をするもののみを言い、プラスに影響するものに別の名前をつける
財務関連のリスクや戦略リスクなど、一つの行為がプラス・マイナス両方の結果を生む可能性のあるものが対象である場合考えやすい定義	いわゆるハザード関連のリスクに使われる定義であり、従来より広く使われている。 ただしリターンを増大させるために積極的にリスクテイクする、といった活動に結びつきにくいきらいがある	従来のマイナス方向の影響のみという定義を踏襲しつつ、同時にプラスの影響についても視野に入れ、双方をコントロールすることを前提とする

本文中特に断りの無い限り、「リスク」はプラス・マイナス両面を含めた概念として捉えていることとします。

リスクの定義例

リスクマネジメントの観点から、例えば代表的なリスクマネジメントのフレームワークでは、リスクを以下のように定義しています。

参考 | JIS Q 2001とCOSO ERMにおけるリスクの定義

◆ JIS Q 2001における定義

リスクとは

事態の確からしさとその結果の組み合わせ、又は事態の発生確率とその結果の組合せ

解説によるとそもそもリスクには以下二つの性質があり、当該性質を考慮し上記定義がされています

①その事象が顕在化すると好ましくない影響が発生する

②その事象がいつ顕在化するか明らかでないという発生の不確実性がある*

*『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年より一部修正

◆ COSO ERMにおける定義

リスクとは

組織にとって不利な影響を与え得る事象

COSOERMでは上記のようにマイナスの意味合いでリスクを定義しています*。

また、プラスの機会を創出するリスクに関してはこれとは別に定義されています。

「機会(Opportunities)またはリスクとの相殺(Natural Offsets)組織にとって有利な影響を与え得る事象」*

* COSO Enterprise Risk Management-Integrated Framework, Framework, September 2004 より一部修正

リスクマネジメント先進企業では、リスクマネジメントで管理対象とするリスクの範囲を示す意味で独自のリスク定義が行われている例も多くあります。

事例 | 企業におけるリスクの定義

自社の事業継続を脅かすすべてのもの

事業の目的達成を阻むものすべて

1.2.2　リスクマネジメントとは

リスクマネジメントについても様々な定義がありますが、リスクの定義ほど本質的な意味合いにおける違いはないと考えられます。また当然ながら、リスクの定義によってリスクマネジメントの定義も異なります。

本テキストでは以下のように定義します。

リスクマネジメントとは

収益の源泉としてリスクを捉え、リスクのマイナスの影響を抑えつつ、リターンの最大化を追及する活動

リスクマネジメントの定義例

参考　リスクマネジメントの定義例

◆ JIS Q 2001における定義

リスクマネジメントとは

リスクに関して、組織し管理する、調整された活動*

＊『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年より引用

◆ 経済産業省　リスク管理・内部統制に関する研究会における定義

リスクマネジメントとは

企業の価値を維持・増大していくために、企業が経営を行っていく上で事業に関連する内外の様々なリスクを適切に管理する活動*

＊ 経済産業省「リスク新時代の内部統制　リスクマネジメントと一体となって機能する内部統制の指針」リスク管理・内部統制に関する研究会 2003年6月 より一部修正

リスクマネジメント先進企業では、リスクマネジメントに関しても自社独自の定義が行われている例が多くあります。

事例　企業におけるリスクマネジメントの定義

自社の事業継続を脅かすリスクに対して回避、移転、低減、保有の対策を実施すること

自社の曝されている様々なリスクに対して、リスクを適切に把握し、評価し、減らすための取組み

1.2.3　事業リスクマネジメントとは

本テキストでは、事業リスクマネジメントをERM（Enterprise Risk Management）とほぼ同義で使用しています。

リスクマネジメントを一切行っていないという企業はほとんどありませんが、事業リスクマネジメントを実施している企業は現状ではごくわずかです。

本テキストでは以下のように定義にします。

事業リスクマネジメントとは

リスクを全社的視点で合理的かつ最適な方法で管理してリターンを最大化することで、企業価値を高める活動

ERMの定義例

参考　様々なERMの定義1/2

◆ COSO ERMにおける定義

リスクマネジメントとは

事業体の取締役会、経営者やその他構成員によって実施される一連の行為（プロセス）であり、戦略設定において事業体横断的に適用され、事業体に影響を及ぼす可能性のある潜在事象を識別し、リスクをリスク許容限度（risk appetite)内に収めてマネージし、事業体の目的の達成に合理的な保証を提供するものである*

＊ COSO Enterprise Risk Management-Integrated Framework, Framework, September 2004 より一部修正

◆ その他代表的な定義

リスクマネジメントとは

組織の戦略的、財務的な目的達成に影響を与えるすべてのリスクを評価し、対応するための厳密かつ調整されたアプローチ。ここでは上方リスクと下方リスクの双方がカバーされるものである*

＊ Tillinghast-Towers Perrin(編),Enterprise Risk Management: Trends and Emerging Practices, 2001 Institute of Internal Auditors Research Foundation より一部修正

参考 様々なERMの定義2/2

リスクマネジメントとは

企業全体としての株主価値の最大化を目的とし、財務的なリスクだけでなく、主要なビジネスリスクと機会のすべてを管理するための前向きでプロセス思考のアプローチであり、監督機構の構築によるコーポレートガバナンスの強化、不測の損失への対応、戦略的マネジメントツールの導入などを目的とするマネジメントである*

＊ James Deloach , Enterprise-Wide Risk Management: Strategies for Linking Risk & Opportunity, 2000 Financial Times Managementより一部修正

リスクマネジメント先進企業では、事業リスクマネジメントについて、組織的、統一的などのキーワードを用い、定義しているケースが見られます。

事例 企業における事業リスクマネジメントの定義

企業が晒されているすべてのリスク（不確実性）を統合的に把握・管理し企業経営に活かすための組織的・体系的アプローチ

企業グループ全体で統一的なフレームワークを用いて、重要リスクを一元管理すること

1.2.4　リスクマネジメントと危機管理

「阪神・淡路大震災の後、「リスクマネジメント」という言葉が氾濫したように、日本においては危機管理（Crisis Management）とリスクマネジメントが混同されるケースが見受けられます。

リスクマネジメントを推進する際に、この2つの言葉の認識を明確化しておくことが極めて重要です*1。」

危機管理とは

いかなる危機にさらされても組織が生き残り、被害を極小化するために、危機を予測し、対応策をリスク・コントロールを中心に計画・指導・調整・統制するプロセスのこと*

*『事業リスクマネジメントーテキストー 経済産業省 平成16年3月』キーワード集より引用

危機管理とは

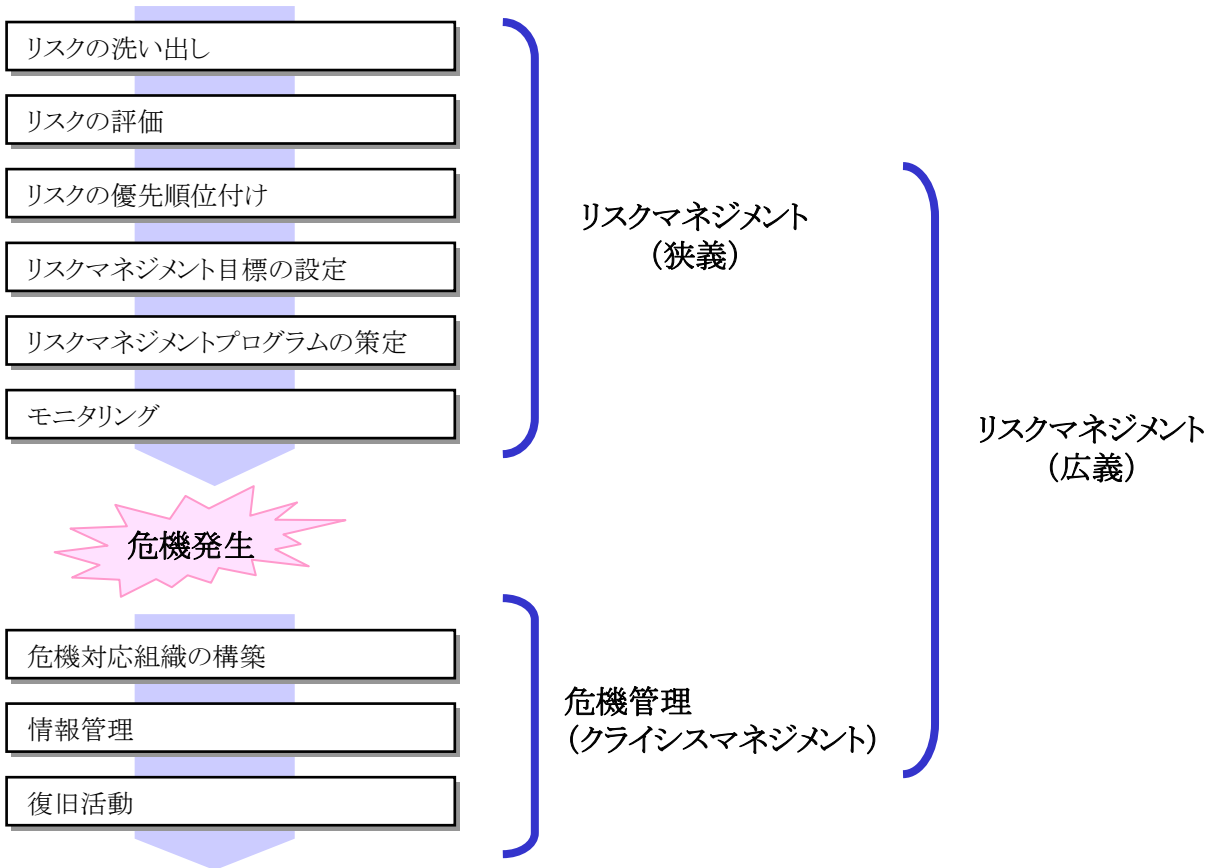
一般により切迫した重大リスクへの対応手法を意味し、緊急事態の回避、危機発生時の対応について、より特化したアプローチを行なうもののこと*1

*1 株式会社インターリスク総研編著『実践リスクマネジメント』経済法令研究会 2002年より引用

下図のように、一旦クライシス(危機)が起こると通常のプロセスではなく危機対応、情報管理、復旧活動という3つのクライシスマネジメントプロセスにて対応することとなります。

本テキストでは広義のリスクマネジメントを対象としています。このうちクライシスマネジメントについては「5.2危機管理(クライシスマネジメント)」で詳しく解説しています。

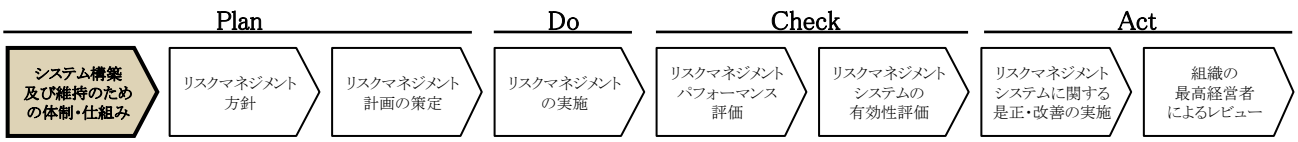
参考　リスクマネジメントと危機管理



CHAPTER 2

事業リスクマネジメントシステム構築及び維持のための体制

2.1 事業リスクマネジメント実施体制
2.2 全社のリスクマネジメント統括体制
2.3 各部門、部署のリスクマネジメント管理体制
2.4 事業リスクマネジメントシステム維持のための仕組み



事業リスクマネジメントを実施していく為には、まずそのための体制や仕組みを整備しなければなりません。そしてその体制や仕組みは、事業リスクマネジメントの性格上、長期間に渡り、安定的に維持・運用される必要があります。

本章では、事業リスクマネジメントを行う上で必要となる体制や仕組みである事業リスクマネジメントシステムを「いかにして構築し、維持していくか」について事例をもとに解説していきます。

事業リスクマネジメント実施のための体制の整備は、システム運用の基礎を整える上で非常に重要です。

米国企業のリスクマネジメントシステムを紹介した書籍では「ケーススタディ企業が、目的を達成するために利用するインフラは多様である*」とされています。

＊トーマス・L・バートン、ウィリアム・G・シェンカー、ポール・L・ウォーカー著 刈屋武昭、佐藤勉、藤田正幸訳『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】』東洋経済新報社 2003年

また日本企業においても、有価証券報告書や各企業のホームページなどを参照する限り、企業における事業リスクマネジメントシステムが実に多様な形態を以って展開されていることが伺えます。

形態に相違があったとしても、リスクマネジメントシステムを構築する目的は

> 企業内のリスクを適正、円滑に管理し、リスクの発現によって被る損害を最小限にするため

という点で共通しています。 この目的を念頭におき、事業リスクマネジメント実施のための体制を説明します。

この章の内容

2.3 各部門、部署のリスクマネジメント管理体制

2.3.1 各部門や部署がリスクマネジメントの実行主体者

2.3.2 リスクをどの単位で管理するか

リスクファクターごとの部会で網羅する

事業本部と職能専門会議で網羅する

社内機能と地域で網羅する

2.3.3 リスクをその性質から分類し、分担して管理する

リスクを分担して管理するメリット

リスクを分担して管理する場合の注意点

業務リスクと戦略リスクに分類する

計測可能リスクと計測不能リスクに分類する

2.3.4 誰が各部門、部署のリスクマネジメントを統括するか

2.4 事業リスクマネジメントシステム維持のための仕組み

2.4.1 事業リスクマネジメントシステム維持のための8つの仕組み

2.4.2 教育

テキストのコンテンツ

いつ教育するのか

だれが教育するのか

だれに教育するのか

どのように教育するのか

2.4.3 シミュレーション

2.4.4 コミュニケーション

社内のリスク情報を共有する

2.4.5 記録

リスクマネジメントガイドライン、管理規程

リスクマネジメントマニュアル

社内のリスク情報を記録管理する

2.4.6 リスクの監視

2.4.7 リスクマネジメントシステム監査

2.1 事業リスクマネジメント実施体制

ここでは「いかにして事業リスクマネジメントシステムを運用するための体制を整えるか」について解説していきます。
具体的には
・ 事業リスクマネジメント体制とはなにか
・ 事業リスクマネジメント体制構築のための準備
に関して説明します。

2.1.1 事業リスクマネジメント体制とは

事業リスクマネジメントを実施しシステムとして運用するためには、まずそのための体制を整える必要があります。

JISQ2001では「組織は、リスクマネジメントに関する役割、責任及び権限を文書によって定めるとともに関連する部署及び部門に伝達することが望ましい*」と体制作りの必要性を示しています。
*『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年 より引用

事業リスクマネジメントシステム構築に際し、まず体制を整えたという企業は実際にも多いようです。特にトップダウンで取組みを始めた企業では、まずリスクマネジメントの体制の構築の着手から入る傾向が見られました。

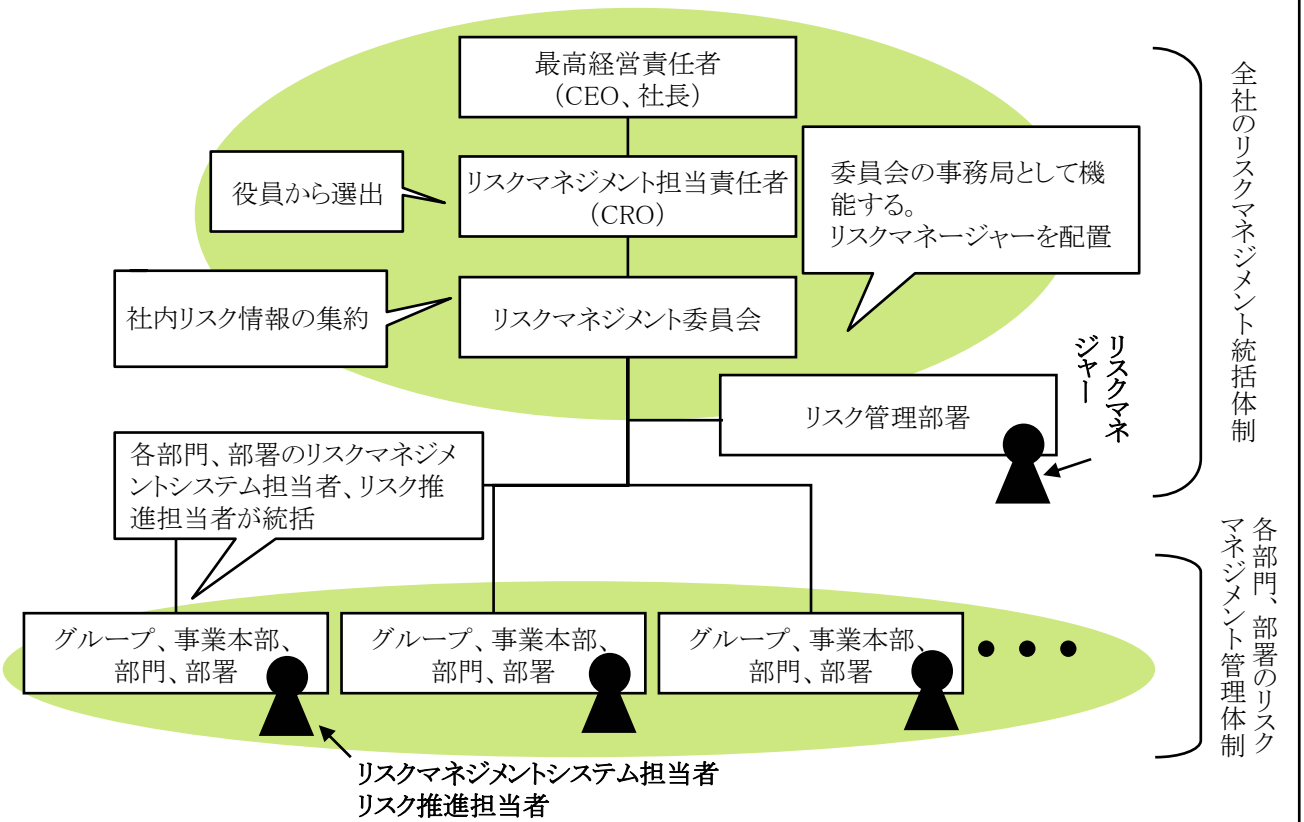
一般的には経営トップ（経営会議メンバー及び取締役会メンバーを指す）の中からCRO（ Chief Risk Officer）が選任され、CROを委員長とするリスクマネジメント委員会を設置します。当該委員会は全社のリスクマネジメントに関する承認、諮問機関として各部門や部署のリスクマネジメントを統括します。

リスクマネジメント活動そのものを実施する主体はあくまでも各部門や部署であり、リスク管理部署や委員会は全社のリスクマネジメントの推進及び統括の役割を担います。

このように、まず体制を整えることによって、全社のリスクマネジメントを統括する仕組みができたことを社内に明確に示すことが可能になります。従って事業リスクマネジメントシステムの体制を整えることは、社内に対するアピールという意味でも重要です。

ここでは、全社のリスクマネジメント統括体制と、各部門や部署のリスクマネジメント管理体制に分けて説明します。

参考　一般的な事業リスクマネジメント体制



2.1.2　事業リスクマネジメント体制構築の準備

事業リスクマネジメント体制を整備するためには、最高経営責任者をはじめとする経営トップと社員一人一人の理解と協力が必要になります。

新たな体制を構築するためには、社内の理解や説得をはじめ、担当者の選定など困難が伴います。
しかしながら、ここでしっかりとした体制を構築しておくことを怠ってしまうと、事業リスクマネジメントへの意識が社内に浸透せず、その後の取り組みや活動が継続しません。社内の各部門や部署を巻き込んだ形で組織作りを行うためにも経営トップの理解と協力を取り付けておくことが重要になってきます。

ここでは、事業リスクマネジメント体制を整備する上で、必須となる経営トップや社員の理解と協力をどのように得るかに関して説明します。

いかに経営トップを巻き込むか

「社内で事業リスクマネジメントの重要性は十分認識されてきているものの、経営トップがなかなか動かず実施に結びつかない」といった話を聞くことがあります。
経営トップの説得には「Chapter1」内「事業リスクマネジメントシステム構築の意義」で紹介した様々なデータが活用できます。しかしこうした数字や他社情勢などのほかに「誰が」「どのように」説得するのかも重要です。

全社を見渡す機能を持つ社内部署や外部コンサルタントによる説得が行われることが多い

監査部が企画部に声をかけ、協同で説得にあたった

総務部が声をかけ、企画部、監査部と協同で説得にあたった

外部コンサルタントに委託し、一気に事を進めた

- 社内を全体的に見渡すことが可能な部門や部署が事業リスクマネジメントシステムに関する高い意識をもつことが多いようです。
- 特に監査部からの警鐘は内部統制への意識の高まりとあわせて、経営トップの危機意識を煽る効果が高いようです。
- 社内のみでの説得が難しいと判断できる場合は外部のコンサルタントに依頼することも効果的です。具体的には経営会議や部長会議などに出席してもらい、事業リスクマネジメントの重要性と他社事例を説明してもらうことがよいと考えられます。

事業リスクマネジメントに取り組もうとする前向きな姿勢が、ボトムアップの説得を成功させる

他社へのヒアリングを積極的に行うと同時に、ターンブルレポートの読み込みなど自ら事業リスクマネジメントに関しての学習を積極的に行った

他社のベンチマーキングと共に、自ら事業リスクマネジメントに関しての学習を積極的に行った

- 事業リスクマネジメントへの高い危機意識と責任感を意識して、自ら勉強にあたる姿勢が必要です。
- また、取組みの進んでいる他社へのヒアリングを行っている企業が多かったことも印象的でした。
- このような積極的な姿勢を以って説得にあたる必要があります。事業リスクマネジメントが及ぼす影響と効果を継続的に説明、報告していくことが必要です。

社内の説得にあたる

事業リスクマネジメントの導入に際し、社内に対してその意味をいかに説得できるかが事業リスクマネジメントが社内にスムーズに受け入れられ、定着するかどうかの鍵となります。特に従来各部門や部署ごとにリスクマネジメントに取り組んでおり、社内でも大きな問題が顕在化していない場合、なぜここで新たに全社的な体制で取組みを進めなければならないのかについて納得してもらうことが必要になります。

社内の説得を進める場合のポイントをいくつか列挙します。

各部門、部署内のキーパーソンを押さえる

- 各部門や部署内で力をもつ人物やオピニオンリーダーの理解を得ることができれば、説得に力を得ることになります。
- 彼らをやる気にさせるためには、経営トップに説明してもらう、もしくは外部コンサルタントなどによって事業リスクマネジメントの重要性を説明してもらうことも有効です。

社内へのスピークアウトに細心の注意を払う

- 社内中堅社員からタスクフォースメンバーを募り、議論を重ね周到に準備を行うことが有効です。
- 彼らは日頃から社内の情報を数多く耳にしていると考えられます。彼らの大半が納得できる内容であれば、同様に社内の大半の同意を得ることができると想定されます。
- 細かな調整に多くの苦労があるかと思いますが、一度着地させることができれば後は進むのみです。

トップが強力なリーダーシップを発揮する

- トップの説得とリーダーシップがあってこそ、円滑なリスクマネジメントシステムが運用されることになります。
- トップによって繰り返し説得、説明が行われることが不可欠です。

トップの説得があっても事業リスクマネジメントに対する意識がなかなか社内に浸透しないという場合は、人事評価制度との連動を図ることもひとつの方法です。

事業リスクマネジメントに関する行動を評価項目に入れることや、個人の目標管理に事業リスクマネジメントに対する目標を盛り込むといった方法によって、事業リスクマネジメントに対する行動を、組織に徹底させることが可能になります。

外部組織を利用する

外部組織とはコンサルタントや保険会社を指します。

事業リスクマネジメントシステム運用全般をサポートしてくれるコンサルタントや保険会社を効率的に利用している企業もあります。

コンサルタントは社内の説得や事業リスクマネジメントシステム運用のためのノウハウを提供してくれる

経営トップや社内の説得に力を貸してくれる

事業リスクマネジメントシステム構築のためのノウハウやツールを提供してくれる

- コンサルタントを利用する場合には、その効果を最大限発揮するために、利用目的をはっきりさせ、社内メンバーとの協力体制を明確にする必要があります。
- コンサルタントは元々企業内の変革や意思決定の手助けを強みにしているため、社内への説得に際して彼らの協力を得ることは、コンサルタントの利用目的に合致していると言えます。
- ただし、コンサルタントの利用は高額になる場合があります。またコンサルタントから提供されたツールや方法論も、結局そのままでは利用出来ず自社に合った独自の方法論を確立したという話もありました。
- 事前にコンサルタントと社内のメンバーの役割分担と協力体制を作りあげておくことで、社内の事情を反映した方法論を作り上げることができます。
- まずは当該テキストを元に社内のリソースで可能な範囲と、外部コンサルタントに委託しなければ実現できない範囲を明確にすることを提案します。

保険会社はリスク対策とリスク評価の実施に力を貸してくれる

膨大な過去の事例から安全管理策などのリスク対策案を提案してくれる

膨大な過去の事例からリスク評価に力を貸してくれる

- 保険会社は従来より個別のリスクをコントロールするための情報を企業に提供してきたところにその強みがあります。彼らの保有する各種安全管理対策を始めとした数多くのリスク対策を参考にすることは、企業にとってリスク発現とその影響の大きさに関する事例を得るという点で多くの利益があるといえるでしょう。
- 保険会社から提供された過去のプラクティスをもとにリスク対策をとることは無駄が少なく、適切な対策がとれる可能性が高いと言う意味で、非常に効率的かつ効果的な手法であるといえます。
- 保険会社にとっても取引企業が事業リスクマネジメントに取り組むことは歓迎すべきことです。リスクマネジメントが行われることによって、不用意なリスクの発現による多額の保険金の支払を迫られる可能性が小さくなるからです。

2.2 全社のリスクマネジメント統括体制

事業リスクマネジメントシステムでは、従来の各部門や部署で行われているリスクマネジメント情報を一元化して管理することが求められています。
ここでは「いかにして各部門や部署単位で実施されるリスクマネジメントを統括するか」について解説していきます。
具体的には
・ 全社のリスクマネジメントを統括する人物
・ 全社のリスクマネジメントを統括する組織
に関して説明します。

2.2.1 最高経営責任者は自身の関与を社内外に明確に示す

最高経営責任者は事業リスクマネジメントへの理解を示し、社内外に向けいかにリスクマネジメントを重視しているかを明確に示す必要があります。

JISQ2001による最高経営責任者の役割

JISQ2001では最高経営責任者の役割を以下のように示しています。

「最高経営責任者はリスクマネジメントに対する責任をもち、方針を策定して表明し、方針どおりのリスクマネジメントが行われているかどうかのレビューを行います。以下にその業務内容を示しています。ただし、リスクマネジメントは経営戦略、法令遵守、環境保全、労務、品質、財務など広範に専門性が必要となるため、取締役会の下にリスクマネジメント委員会のような組織を設け、経営意思決定に資する諮問を行うこともあります*1 。」
また「組織の最高経営責任者は、リスクマネジメントシステムを構築及び維持するために必要な経営資源を用意することが望ましいとされています。

- リスクマネジメントシステムの構築および維持に関する責任をもつ
- リスクマネジメント方針の表明
- リスクマネジメント行動指針の策定
- リスクマネジメントシステムのレビュー*2」

*1『事業リスクマネジメントーテキストー 経済産業省 平成16年3月』412-413ページ より一部修正
*2『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年 より一部修正

しかし現実には最高経営責任者には通常JISQ2001で明文化されている以上の役割が期待されています。全社的なリスクマネジメントを実施している企業での最高経営責任者に実務上求められている役割は、社内へのアピールと社外へのアピールの2つです。

社内に対する役割

社内に向かって最高経営責任者が、事業リスクマネジメントへの関与を明確に示すことによって、事業リスクマネジメントシステムの円滑的な運用が実現します。

また、最高経営責任者が直接リスクマネジメントに関する伝達を行うことは社内のリスクマネジメント意識向上のために非常に効果的です。

・ 最高経営責任者が関与を明確に示す
・ 最高経営責任者から社内に直接リスクマネジメントに対する伝達を行う
ことが事業リスクマネジメントシステムの円滑化が実現につながります

リスクマネジメントへの取組みが全社的なものであることが伝わる

リスクマネジメントへの取組みがいかに重要であるかが伝わる

社内にリスクマネジメント意識が浸透しやすい

- 最高経営責任者の意欲と意識が明確にあらわされることで、社内にはリスクマネジメントに真剣に取り組む雰囲気が醸成されます。
- 最高経営責任者が自らの関与を会社内に直接伝えていくことで、全社的な取組みへの参加意識が高まり、社内のリスクマネジメントシステムの円滑化につながります。

実際に多くの企業において最高経営責任者は機会を捉えてリスクマネジメントの重要性を説明し、社内にリスクマネジメントに敏感な雰囲気を作り出すことに努めています。

朝礼や挨拶時など機会あるごとにリスクマネジメントの重要性を説く

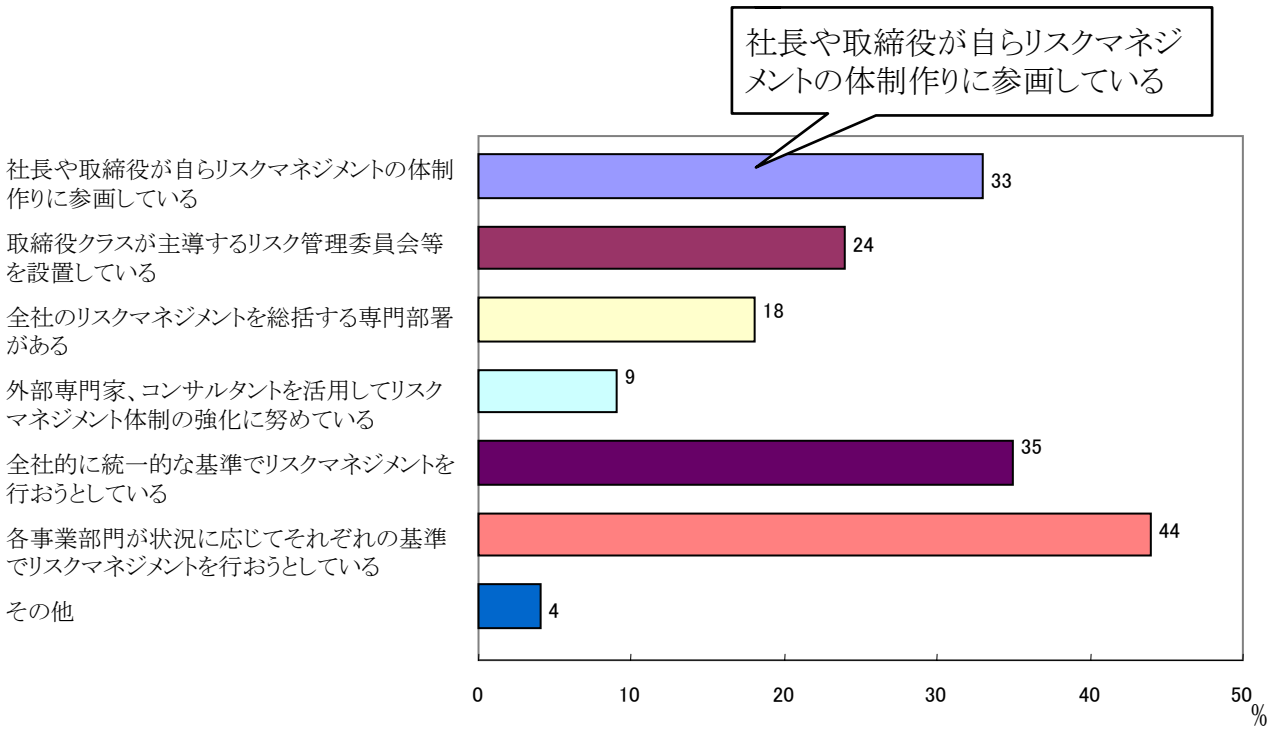
リスクマネジメントの重要性と取組みへの理解を求めるメールを社員全員に送信する

懇談会などの場で社員一人一人とリスクマネジメントに関して直接話し合う

事業リスクマネジメントシステムを構築する上で、最高経営責任者の承認及び協力は必須です。最高経営責任者によってリスクマネジメントへの取組みの重要性が積極的に訴えられることにより、社内にリスクマネジメントへの意識を浸透させることが可能になります。

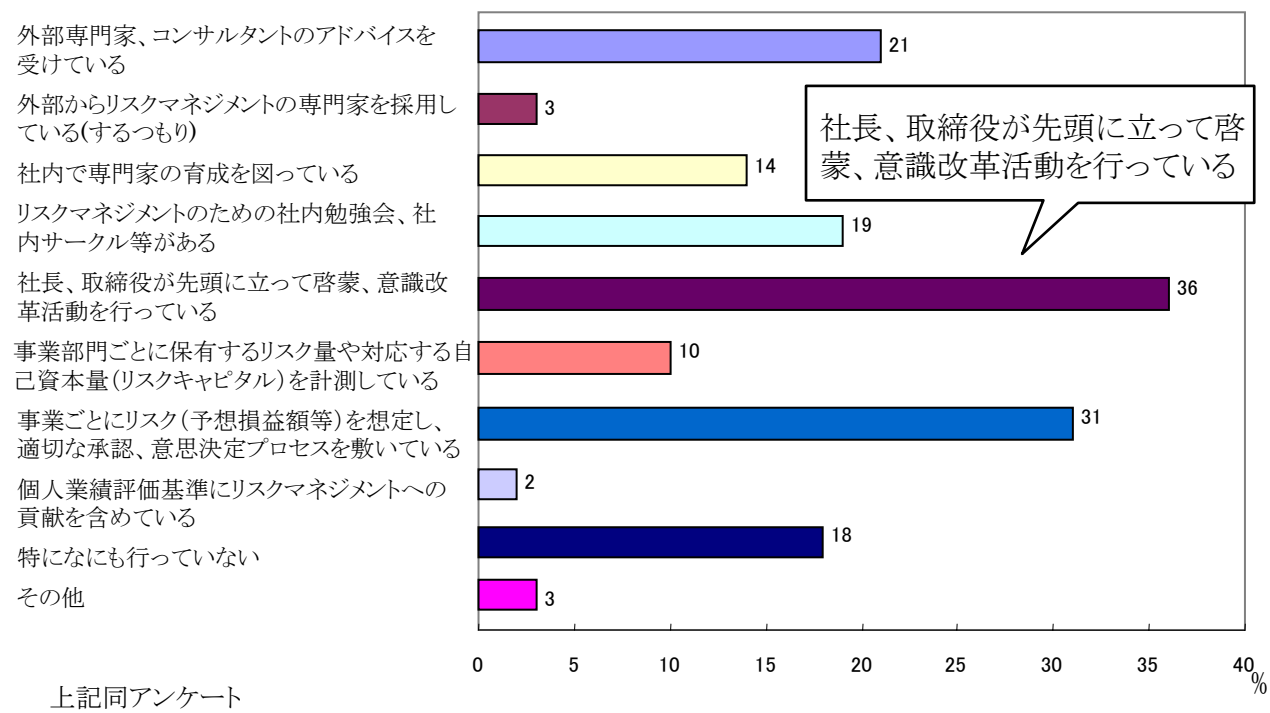
参考　事業リスクマネジメントへの社長、取締役の参画状況

リスクマネジメント体制について



2003年度事業リスク評価・管理人材育成システム開発事業
2003年7月～11月に国内有力企業に対して行ったアンケート調査より抜粋作成
「貴社のリスクマネジメント体制について当てはまるものをお選びください」(複数回答)

リスクマネジメントの取組みについて



上記同アンケート
「貴社ではリスクマネジメント強化のためになんらかの取組みをなさっていますか」(複数回答)

リスクマネジメントに関するアンケート結果からも、社長や取締役が積極的にリスクマネジメントに参画している企業の割合が高いと考えられます。

社外に対する役割

ステークホルダーからの信頼の確保や社会的イメージの向上のために、社外に積極的にリスクマネジメント情報を開示していく必要があります。

最高経営責任者が事業リスクマネジメントへの関与を社外に積極的に開示することが企業イメージの向上につながります

ステークホルダーからの信頼を得られる

格付け会社へのアピールが可能になる

- リスクマネジメントへの取組みとその具体的内容を開示することで、企業活動の透明性が増し、ステークホルダーからの信頼を得ることが可能になります。
- 例えば「トレーサビリティーをこのような方法で実施しています」ということを明確に示すことで、消費者の信頼確保と企業イメージの向上につながります。

◆ 実際に行われている開示方法

有価証券報告書を通し、意識の高さと透明性を開示する

自社のホームページ上で、リスクマネジメントに対する認識の高さと実際に行っている対策を公開する

リスクマネジメントに関する情報誌などの取材を受け、できるだけ多くの目に触れる形で開示する

- 有価証券報告書への情報開示要求などにも見られるように、事業リスクマネジメントシステムに関する情報開示は必須ともいえます。
- 実際にヒアリングを実施した結果、私たちが調査した外部情報（有価証券報告書、インターネット、新聞雑誌記事など）よりも、より的確な事業リスクマネジメントに取り組んでいる企業が多く見られました。開示の機会をチャンスと捉え、より積極的に開示する姿勢を示すことが、ステークホルダーからの信頼確保につながります。

情報開示の方法に関しては他社をリサーチし、ベンチマーキングの上、開示方法を決定した

- 開示方法に関して他社リサーチを行ったという企業もありました。開示の仕方は様々ですが、自社にあった方法を検討の上、積極的に開示していくことが必要です。
- ただし、細かなリスクマネジメントに関する情報の開示は、社内の危機管理体制やネットワーク情報などを社外に公表してしまうことになりかねません。どのような形で情報を開示し、どこまでを開示するのかに関しては十分な注意が必要になります。

2.2.2　CROを核として

事業リスクマネジメントシステムは全社的に実施されるため、CROまたはそれと同等の役割を果たす機能を持った役職には、経営トップである役員が兼務にて当たるケースが多いようです。「CROは経営に携わる立場とリスク管理の責任者としての職務の両方から事業目的の策定にも関与する立場*」にあると言えます。

* 竹谷仁宏『トータル・リスクマネジメント』ダイヤモンド社 2003年 より引用

JISQ2001によるCROの役割

JISQ2001で示されているリスクマネジメントシステム担当責任者はCRO、リスクマネジャーにある人物のことです。リスクマネジメントシステム担当責任者の役割としては、以下のようなものが示されています。

「リスクマネジメント担当責任者は最高経営責任者の指名を受け、リスクマネジメントに関わるすべての業務を統括します*1。」

「リスクマネジメント担当責任者は、経営トップの中から専任または兼任を問わず指名されることが望ましいでしょう。

またリスクマネジメント担当責任者は、発生場所、原因、損害を受ける対象などによってリスクをグループとして扱うことが適切と判断できる場合には、そのグループごとに部門、部署、委員会などの形式でリスクマネジメントシステム担当を定めてもよいとされています*2。」

「以下にその業務内容を示します。

- リスクマネジメントに関わるすべての業務の統括
- リスクマネジメントに関する計画策定
- リスクマネジメントの実施
- リスクマネジメントパフォーマンス評価及びリスクマネジメントシステムの有効性評価
- リスクマネジメントシステムに関する是正及び改善対策の策定並びに実施
- リスクマネジメントシステムに関する最高経営責任者への報告及び提案
- リスクマネジメントシステムに関連する外部の機関との連絡、調整及び連携
- リスクマネジメントシステムに関連する組織内の連絡及び調整
- リスクマネジメントシステムに関連する組織全体の記録の作成及び管理
- リスクの特性*1」

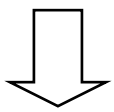
*1『事業リスクマネジメント-テキスト- 経済産業省 平成16年3月』412-413ページ より一部修正
*2『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年 より一部修正

CROを設置するメリット

CROを設置することで、全社のリスク管理に関わる全ての情報を収集することができるようになります。

社内すべてのリスクを経営のトップレベルで把握することが可能になる

全社のリスクマネジメントに対する最終責任者が明確になり、社員からリスクに関する情報が集まりやすくなる



社内に存在する全てのリスクに対してトップダウンの関与が可能になる

社内に存在するリスクに対し部門や部署に特化せず社内横断的な対応が容易になる

- 経営トップより選任されるCROは強力な権限をもって、社内に存在する全てのリスクに対し関与することが可能です。
- 事業リスクマネジメントでは一部門では解決できないリスクを扱います。部門や部署という枠にとらわれずリスクに対応できるように、高度な権限を持ち合わせた人材の関与が不可欠です。

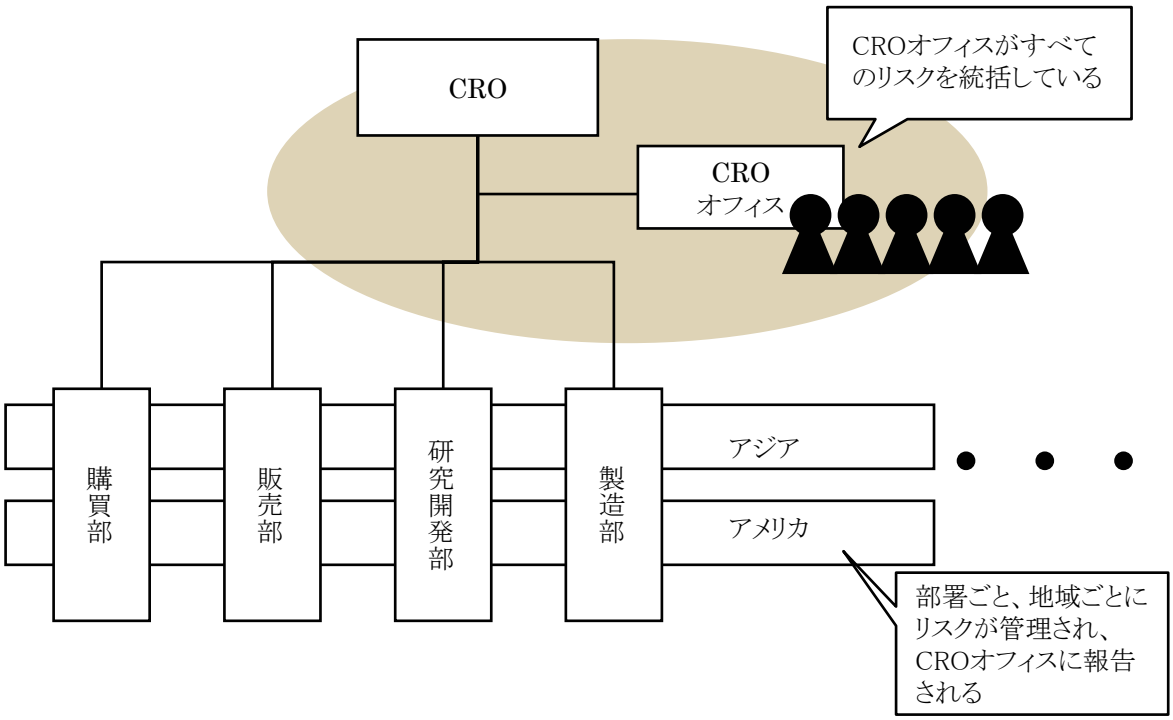
社内に対するリスクマネジメントシステムの権威付けが可能になる

- CROは、社内への広報活動やリスクマネジメントへの継続的な取組みに対する象徴的意味を持ちます。
- リスクマネジメントに関して社内への広報を行う場合、CROから発せられているということが意味を持ちます。
- 社内の全てのリスクに対し、強力な権限を保有するCROが任命されているというだけでも、社内のリスクに対する意識は高まります。

意思決定をすばやく行うことが可能になる

- CROに強力な権限を委譲することにより、意思決定に際し、会議や伺いを立てる必要がなくなり、すばやい意思決定を行うことが可能になります。
- 特に緊急時には、CROの権限が大きな威力を発揮し、すばやい対応と意思決定を可能にします。

事例　ある消費財製造業の組織体系



CROを新たに設置しない場合の注意点

これまで述べてきたように事業リスクマネジメント円滑化のためにはCROを設置することが望ましいですが、CROを設置しない場合には、実質的にCROが担う意思決定、社内情報集約の機能を代替するための仕組みが必要になります。

事業リスクマネジメント担当役員を明確化し、各部門や部署のリスクマネジメントシステム担当者は日ごろから担当役員に報告を行う

- CROという役職として任命を行わない場合でも、リスクマネジメントの報告を受ける担当役員を決定しておく必要があります。
- 担当役員は、有事の意思決定を可能にするため、継続的にリスクマネジメントに関する報告を受けることが必要になります。

社内向け文書に事業リスクマネジメントシステム担当役員名を記載する

- CROの設置は、事業リスクマネジメントへの取組みをアピールすることを可能にします。従ってCROを設置しない場合には、書面上に明確に担当役員名を記載し、事業リスクマネジメントへの取組み姿勢を示す必要があります。

2.2.3　リスクマネジャーは事業リスクマネジメントの要

リスクマネジャーは各部門や部署内で集約されたリスクを全社レベルで統括する役割を担います。まさに、リスクマネジメントにおいて、経営と現場をつなぐ要の役割を担う人物であると言えます。

リスクマネジメント委員会の事務局長、リスク管理部署の部署長などがリスクマネジャーにあたります。また CROが自らその役割を担う場合もあります。

リスクマネジャーの役割

リスクマネジャーはまさに現場と経営をつなぐ役割を担っているといえます。

各部門、部署からあがってきたリスクマネジメント報告の集約を行う

各部門、部署からあがってきたリスクマネジメント報告をリスクマネジメント委員会に報告する

各部門、部署で実施されているリスクマネジメント対策の実施状況を把握する

各部門、部署のリスクマネジメントシステム担当者と密に連絡を取り合う

リスクマネジメントシステム全体の推進役として、教育の実施や情報提供や意識付けなど、各部門への働きかけを行う

- リスクマネジャーの主な役割は、社内の全てのリスクマネジメント情報を集約し、リスクマネジメント委員会や経営トップへの報告を行うことと社員一人一人にリスクマネジメントの意識付けを行うことです。
- リスクマネジメント委員会の主なメンバーは役員クラスであり、情報の集約を行うことは困難です。リスクマネジャーは事務局的な立場で情報を集約し、承認や諮問の手助けをします。
- リスクマネジャーは、社内の全てのリスク情報を集約する役割を負っているため、日頃からリスクマネジメント担当者と密に連絡を取り合っていることが求められるでしょう。

リスクマネジャー設置のメリット

リスクマネジャーを設置することによって得られるメリットを、以下に挙げます。

社内に存在するすべてのリスクに対する情報の集約が容易になる

各部門、部署で発生した問題がすばやく報告される

各部門、部署のリスクマネジメントシステム担当者の相談窓口になる

- リスクマネジャーがいることで、社内のリスクマネジメント情報の集約先が明確になり、情報が集まりやすくなります。
- また問題が発生した場合の報告先も明確になり、迅速な対応が可能になります。

リスクマネジャーは専任か兼任か

リスクマネジャーの設置を考慮する際に問題となるのがリスクマネジャーは専任とするべきか、兼任が可能なのかという点です。

兼任にする場合「負担が大きすぎる」という意見もあります。中には、負担も大きく専門の組織で取り組んだほうが効率がいいという理由で、経営トップに専門の組織の設置を提案したが、承認されなかったという企業もありました。

◆ 専任が望ましいケース

企業規模が大きく、全社のリスクマネジメントを統括することが大きな負担となる場合

過去において各部門や部署単位でのリスクマネジメントが特に行われておらず、各部門や部署からの自発的な報告に頼ることが困難な場合

- 当該組織の責任者の担う業務範囲が著しく大きく、負担を要する場合は、全社のリスクマネジメントを統括する担当者を専任で設置することが望ましいでしょう。

◆ 兼任が可能なケース

初めて事業リスクマネジメントに取り組む企業で、システムが軌道に乗る前の段階にある場合

兼任者がもともと全社的なリスク情報が集まりやすい部門や部署に所属し、全社のリスク情報を事前に理解できている場合

- これから事業リスクマネジメントに着手するという企業では、現時点では最終的な仕組みを想像できない可能性があります。特にそのような場合には、兼任からはじめて、その人物が全社のリスクマネジメント管理を行う人物として相応しいか、業務内容として負担が大きすぎないかなどを検討の上、最終的に専任にすることも考えられます。
- 財務部など従来からリスク移転のための保険を扱っている部門や部署では、社内のリスクにかかわることが多く、当該部員は社内のリスクに関する知識が高いと考えられ、兼任できる可能性もあります。
- まずは柔軟な姿勢で取り掛かってみることが大切です。

リスクマネジメントは業務として負担が大きく、特に有事には機動力の高さが求められています。兼任の場合何かあったときに即座に対応できるとは考えにくく、専任が望ましいでしょう。

リスクマネジャーの資質

リスクマネジャーは全社のリスクマネジメントシステムを管理する上で要にあたる人物です。CROと同一人物であっても、個別にリスクマネジャーにあたる人物を任命してもかまいません。

リスクマネジャーにあたる人物はバイタリティに溢れ、リスクマネジメントに対し高い関心と知識、また使命感を有していることが求められます。

全社を通じ、人的ネットワークをもっている

- 総務部、法務部、財務部など全ての社員とかかわりをもつ可能性のある部門や部署に所属していたことのある人物は、社内に広い人的ネットワークを保有している可能性があります。
- 社内の人的なネットワークの大きさによって社内の説得が容易になることや、各部門や部署のリスクマネジメントシステム担当者の選定も行いやすくなります。

人の話を聞くことができる。相談に乗ることができる

- 粘り強い説得や説明が必要とされるといえるため、コミュニケーション能力に長けた、じっくりと腰を据えて人と話ができる人物が望ましいと思われます。
- 特に相談に乗るということは、リスクマネジメント上重要な要素であるといえます。各部門や部署のリスクマネジメントシステム担当者が重大なリスクを抱え込んでしまい、最終的にリスクが発現してしまうという最悪の事態を防ぐことが重要なのです。

人から信頼を得られる人柄である

- 信頼を得られるような真摯でまじめな人柄であることが期待されます。
- 特に「たとえ些細なことであってもとりあえずこの人に報告しておけば、大丈夫だ」という信頼を各部門や部署のリスクマネジメントシステム担当者から得ていることが重要です。こうした信頼感がリスクの発現防止につながります。

2.2.4　リスクマネジメント委員会を設置する

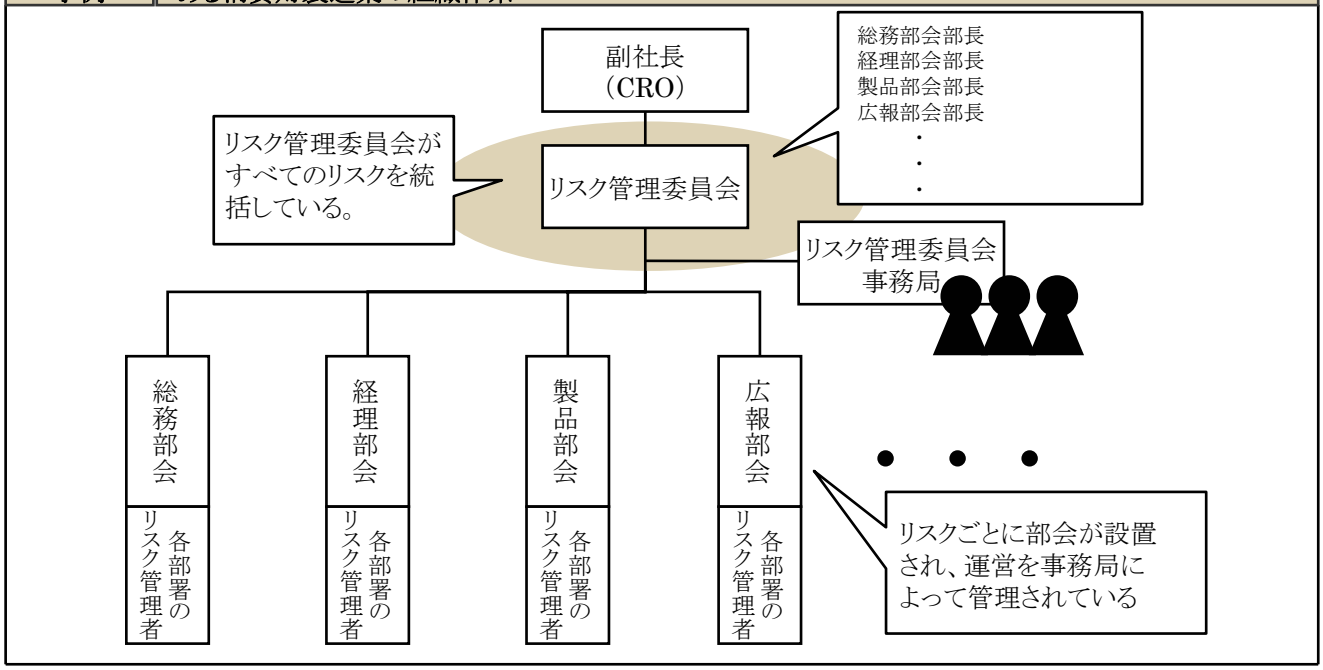
事業リスクマネジメントを実施するために、リスクマネジメント委員会を設置する場合があります。

リスクマネジメント委員会は取締役会や経営会議の中に、その会議のメンバーを委員として設置される場合と、経営の諮問機関としてその下に設置される場合があります。いずれの場合も、委員長には通常CROが就任します。

通常年二回程度開催され、全社のリスクマネジメントに関する中間報告及び結果報告が行われます。その他にも必要に応じ、適宜開催されることがあります。

リスクマネジメント委員会は、社内の各部門や部署が横断的な決定を行うことを容易にし、リスクマネジメントに特化した視点で経営の意思決定を行うことを可能にします。

事例　ある消費財製造業の組織体系



リスクマネジメント委員会のメンバー

リスクマネジメント委員会のメンバーは、その責任と権限の大きさを考慮して、役員クラスを選出するのが基本です。

リスクマネジメント委員には役員クラスを選出する

- リスクマネジメント委員会などの全社リスクマネジメント統括組織は、社内のすべてのリスクを統括するという意味で、役員クラスが責任をもってメンバーを務めるというケースが多いようです。全社レベルの意思決定は社内の全リスクマネジメントの状況を踏まえた上で行われる必要があることからも、役員レベルの人材が全社のリスクマネジメントを統括する組織の一員となる必要があります。
- 役員が積極的にリスクマネジメントに関与していることを示すことで、リスクが企業にとって重要な管理項目であるということを社内にアピールする意味でも、リスクマネジメント委員会に役員が選任されている必要があります。
- またリスクマネジメント委員会には役員だけでなく、社内のリスク対策に直接関係する管理系の部門や部署の室長クラスを入れることがあります。また、管理系スタッフを事務局に入れることで組織の機動性の確保が期待できます。

リスクマネジメント委員会の役割

リスクマネジメント委員会の役割は、各部門や部署からのリスクマネジメントに関する報告をもとに、全社のリスクマネジメントに関する承認と意思決定を行うことです。

各部門、部署からあがってきたリスクマネジメント報告の承認を行う

社内に存在する全てのリスクに対する評価の最終化を行う

全社で対応するリスクの対策を議論し、策定する

リスクマネジメント委員会設置のメリット

リスクマネジメント委員会を設置することによって得られるメリットを、以下に挙げます。

全社横断的な視点でリスクマネジメントに取り組める

- リスクマネジメント委員会は、社内横断的に委員を選任するため、通常の部門や部署単位でのリスクマネジメントと異なり、自部門のリスクや個別リスクへの対応に終始せず、全社にとって意味のあるリスクマネジメントを実行することが可能になります。

リスクマネジメントのためだけに開催されるため、リスクマネジメント方針や重要リスクの認識など重要テーマについて上級管理職が様々な角度から十分に議論を尽くすことができ、最適な意思決定ができる

- 経営会議等と違い、企業にとって重要なリスクに関して話し合いを持つことができるため、上級管理職のリスクマネジメントに対する意識を高めることが可能になります。

委員会に参加することで各委員のリスクマネジメントに対する意識向上に役立つ

- 委員会の開催時期には、委員や委員の属している部門や部署のリスクマネジメントに対する意識の向上を促すことができます。

リスク対策実施状況の報告義務が発生することで、リスクマネジメントシステム担当者のリスク対策促進が可能になる

- 報告義務が生じることにより、必然的に各部門や部署のリスクマネジメントシステム担当者はリスク対策を積極的に実施せざるを得なくなります。
- 報告がなされることで、適宜改善点や問題点を考慮できるというメリットもあります。

有事に対応する部門、部署や責任者が明確になるので、迅速な対応が可能になる（危機管理機能も持つ場合）

- 全社に存在するリスクの情報を日頃から社内横断的に共有し、責任者を明確にし、対応策を策定しておくことで、リスクが発現した場合にも迅速且つ適切な対応が可能になります。

事業リスクマネジメントに注力していることをステークホルダー(含:従業員)が明確に理解できる

- 有価証券報告書や自社のホームページなどにリスクマネジメント委員会の設置を明記し、全社的なリスクマネジメントに注力していることをアピールすることで、ステークホルダーからの信頼を確保できます。

リスクマネジメント委員会設置時の注意点

リスクマネジメント委員会を設置する場合には、そのメリットを最大限発揮させるために注意すべき点もあります。

形だけの承認機関となってしまわないよう、委員の構成や運営に配慮する

- リスクマネジメントに対する高い意識や責任感を持ち合わせた人物を選任することで、組織の形骸化を防ぐことができます。
- 従来から各部門や部署でリスクマネジメントに携わっている人物を選任することで、単なるCRO直轄の承認機関ではなく、社内のリスクマネジメントを司る機関として認識され、実行力をもった委員会にすることが可能になります。

経営会議等上部の会議や、他の委員会との役割分担を整理し、重複感のないようにする

- 同様の上級管理職が出席する他の会議との目的の相違を明確にし、単に出席するという会議ではなく、実際に話し合いを行い、社内に存在する全てのリスクに対応するという目的と意識を持つ委員会にする必要があります。

委員会の果たす役割と各部門、部署で実施されるリスクマネジメント活動との関係を明確にし、社内に浸透させる

- イントラネットや社内報などを活用し、委員会の存在と役割を社内に伝え、各部門や部署で実施されるリスクマネジメントとの関係を明確化することで、委員会の存在意義が伝わります。

リスクマネジメント委員会を新たに設置しない場合の注意点

リスクマネジメント委員会を設置しない場合、委員会制度の代替機能を持つ仕組みが必要です。

経営会議などの場でリスクマネジメントについて議論する時間を充分確保する

- 上級管理職や取締役が集まる場所での議論を確保することで、リスクマネジメントに対する関心と各人の責任感を担保する必要があります。特にリスクマネジメントに関しては「マイナス」な意識が働き、後回しにされる可能性がありますので、やはり個別にリスクマネジメントに関して議論する場を設けることが望ましいでしょう。

CROに対し、意思決定のために必要な情報や意見を伝える仕組みを確立する

- リスクマネジメント委員会の目的である全社のリスクを把握し、社内の意思決定に役立てるという機能を代替する仕組みを作る必要があります。
- 各部門や部署からリスクマネジメントに関する報告を受けるための事務局の設置やイントラネットを利用した方法など全社のリスクを把握するためのパイプを作る必要があります。

社内に対し、リスクマネジメントの各種活動を積極的に広報する

- リスクマネジメント委員会の設置を通じて、日常的にリスクに対する意識を高めることの重要性を理解してもらうことができないため、社員一人一人の意識を高めるための広報活動に力を入れる必要があります。
- リスクマネジメントに対する意識付けに留まらず、特別に委員会は設置しなくとも、全社でリスクマネジメントを重要視していることを伝えていくことが必要です。
- 社内イントラネットを利用したメールマガジンや掲示板なども活用できるかも知れません。

2.2.5　リスク管理部署を設置する

事業リスクマネジメント実施のためにCROやリスクマネジメント委員会の下部組織として、または委員会の代替組織としてリスク管理部門や部署を設置することがあります。一般的にはリスク管理室やリスクマネジメント推進室などと言われます。

この組織にリスクマネジャーにあたる人物を配置し、全社のリスクマネジメントの取りまとめを行います。ここでは事業リスクマネジメントの事務局的役割を担います。

リスク管理部署の役割

リスク管理部署では、各部門や部署で実施されているリスクマネジメントの取りまとめを行います。

全社のリスクマネジメントに関する情報の集約を行う

各部門、部署のリスクマネジメントシステム担当者から報告、相談を受け付ける

全社横断的なリスクに関する対応策やマニュアルを策定する

リスク管理部署設置のメリット

リスク管理部署を設置することによって得られるメリットを、以下に挙げます。

社内に存在するすべてのリスクの一元管理が容易になる

- 事業リスクマネジメントの要となる組織であり、社内に存在する全てのリスクを統括します。当該組織に全社のリスク情報が集約されることになります。
- 全社横断的にリスクを取りまとめるため、社内に存在するリスクを漏れや重複無く、一元管理することが可能になります。

有事の際の報告先が明確になる

- リスクが発現した場合に、どこにどのように報告をあげればいいかということが社内で明確になります。従って、リスクが発現した場合にも、当該組織に情報を収集し、全社横断的に対策を実行することが可能です。

各部門、部署のリスクマネジメントシステム担当者の相談窓口になる

- 各部門や部署のリスクマネジメントシステム担当者は、従来各人が責任をもって自らリスクを回避してきました。リスク管理部署の設置により対応に迷う場合や、改善策が思うようにいかない場合などの相談窓口ができることとなり、各担当者の負担が軽減されるとともに、各担当者の手に余るリスクが放置されるという最悪の事態を回避できます。

社内の誰もが社内に存在するリスクが当該部署に管理されていると明確に理解できる

- 「顔の見える担当者」が全社のリスクを管理している、ということを社員一人一人が意識し、リスクマネジメントに積極的に取り組むことができます。

リスク管理部署を特別に設置しない場合、社内の既存組織で代替することが可能です。社内の既存組織で代替する場合に関しては以下で説明します。

既存の組織で代替する

リスク管理部署というような特別な組織を社内に個別に設置せずに既存の組織を利用して、その機能を代替させる場合があります。
この場合担当者は既存の職務と事業リスクマネジメント業務を兼務することになるために、負担が過大になると言う意見もあります。

しかし、リスクマネジメントシステムが軌道に乗るまでの間、既存の組織で全社のリスクマネジメントを実施する機能を代替することは事業リスクマネジメントシステム構築のための負担を軽減できると言う点でメリットがあります。まずは問題意識を持った部門や部署を中心として取組みを進めてみることが重要でしょう。
ただし、事業リスクマネジメントシステムは社内のすべての部門や部署を対象としたシステムとして機能するべきであることから、独立した組織として設置されることが望ましいことは言うまでもありません。

以下では、既存の組織で代替した例を示します。

社内の保険を取り扱っていた財務部が全社のリスクマネジメントも担当することになった

- 保険を取り扱う部門や部署には、多くのリスク情報があると考えられ、当該部門や部署が引き続き全社のリスクマネジメントの統括に当たることは十分に考えられます。

事業リスクマネジメントに関する取組みを提案した総務部が中心となり、全社のリスクマネジメントを担当している

- 事業リスクマネジメントの必要性を提案した部門や部署が全社のリスクマネジメント統括を行うことは、リスクに対する意識も高く、効率的ともいえるかもしれません。特に総務部など社内の情報に詳しい部署は適切でしょう。総務部がリスクマネジメント担当部署である企業も多いようです。
- ただし監査を担当する部門や部署は、リスクマネジメントを統括する組織と独立している必要があります。
- リスクマネジメントシステム実施後の各部門や部署の役割を明確に想定した上で、柔軟に体制を構築していく必要があります。

2.3 各部門、部署のリスクマネジメント管理体制

事業リスクマネジメントシステムでは、従来の各部門や部署で行われているリスクマネジメント情報を一元化し、管理することが求められています。
ここでは「いかにして各部門や部署単位でリスクマネジメントを実施統括するか」について解説していきます。
具体的には
・ 各部門や部署でリスクマネジメントを統括する人物
・ リスクを管理する方法
に関して説明します。

2.3.1 各部門や部署がリスクマネジメントの実行主体

「リスクマネジメントプログラムを実施するのは組織の各部門や部署の責任者です。実施状況についてはCROに定期報告を行わなくてはなりません。

- リスクマネジメントプログラムの実施
- リスクマネジメントシステム担当責任者への実施状況の定期報告*」

*『事業リスクマネジメントーテキストー 経済産業省 平成16年3月』413ページ より引用

従来の「部門型リスクマネジメント」では、各部門や部署内で実施されたリスクマネジメントが全社として集約、管理されることはありませんでした。
しかし事業リスクマネジメントは、各部門や部署でのリスクマネジメントに留まらず、全社としてリスクが管理される仕組みです。

事業リスクマネジメントは、各部門や部署において実施されているリスクマネジメントを全社として統括する仕組みであり、各部門や部署のリスクマネジメントは非常に重要です。

2.3.2　リスクをどの単位で管理するか

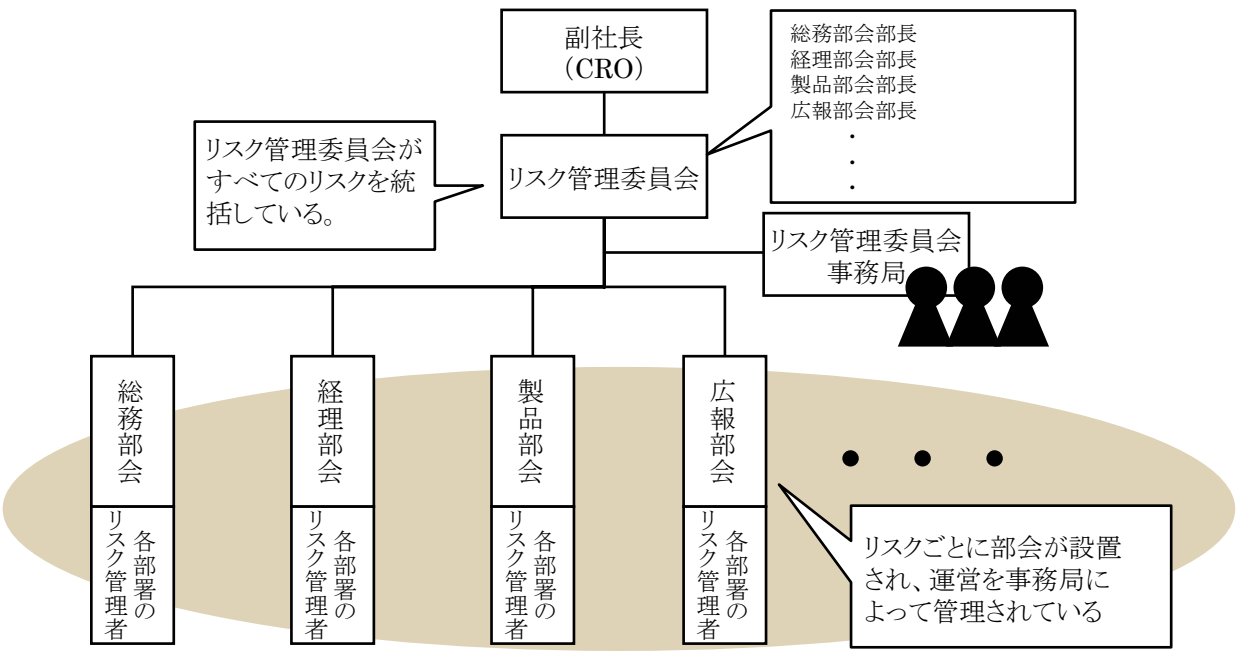
JISQ2001では「発生場所、原因、損害を受ける対象などによってリスクをグループとして扱うことが適切と判断できる場合にはそのグループごとに部門、部署、委員会などの形式でリスクマネジメントシステム担当者を定めてもよい*」とされています。
*『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編　2003年より引用

今回のヒアリングを通し、各企業が実に様々な方法でリスクを管理していることが明らかになりました。

リスクファクターごとの部会で網羅する

この企業では、従来より各部門や部署でリスクマネジメントに取り組んできた担当者を取り込んで、リスクファクター別の組織を作り、リスクマネジメントを実施しています。

事例　**ある消費財製造業の組織体系**



リスクファクターごとに部会を設置してリスクマネジメントを実施している

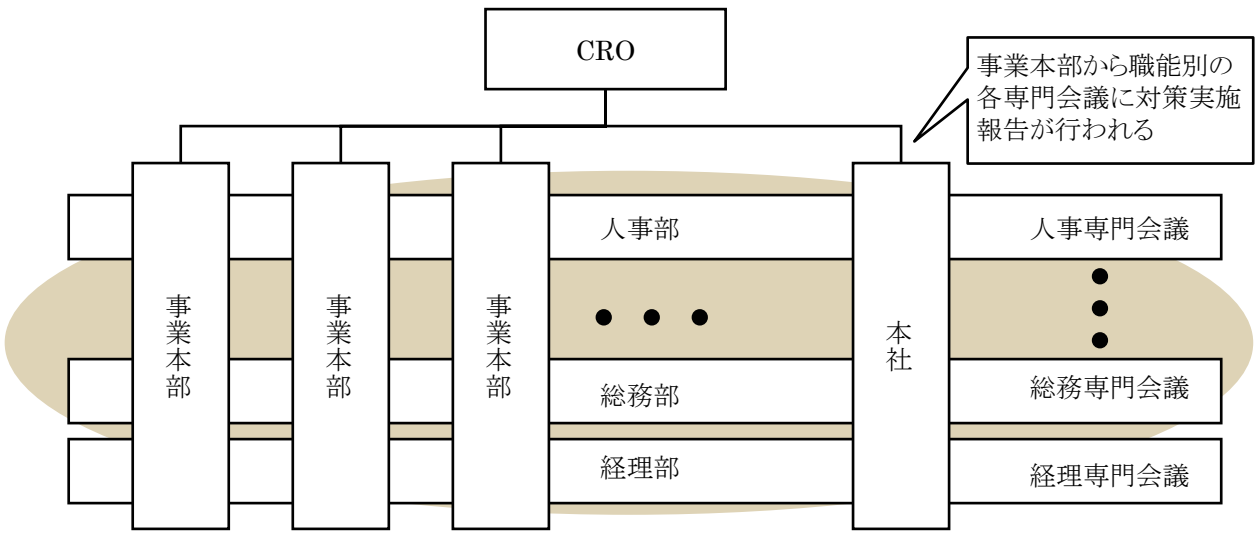
リスクファクター別に担当部門や部署を決定し、部会には担当各部門や部署のリスクマネジメントシステム担当者をメンバーとして配置している

- 社内の部門や部署に捕らわれず、社内に存在するすべてのリスク別に管理を行うという形態です。社内に存在するリスクがある程度明らかな場合には適した方法であるといえます。
- 部会には、各部門や部署で従来よりリスクマネジメントに取り組んできた担当者が選任されており、従来のリスクマネジメントと事業リスクマネジメントシステムを融合させた方法です。従来リスクマネジメントに取り組んできた担当者を事業リスクマネジメントシステムに取り込んでいくことは、地に足のついた事業リスクマネジメントシステム構築を実現可能にする方法であるといえます。

事業本部と職能専門会議で網羅する

この企業では、事業本部別にリスクマネジメントを実施し、全社職能別専門会議で組織横断的なリスクマネジメントを実施しています。

事例 ある消費財製造業の組織体系



リスクマネジメントは経営と密接な課題であるため、各事業本部長が責任を負う

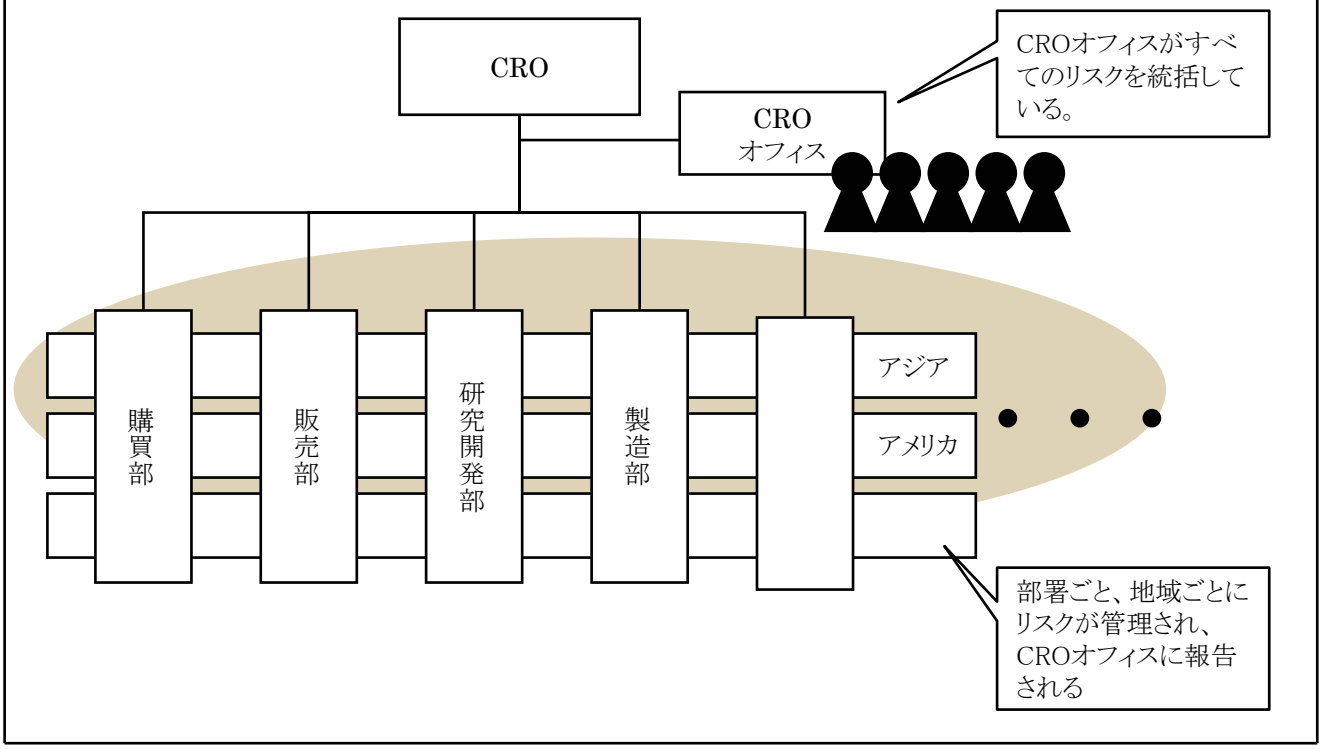
全社共通のリスクに関しては、横軸の職能別専門会議で掌握されている

- 自事業本部内に存在する全てのリスクは各事業本部内で責任をもって管理され、CROと職能別の専門会議に報告されます。事業本部長は自らの責任で自事業本部のリスクに関し、マネジメントを行います。
- 事業本部横断的に管理や対策がなされなくてはならないリスクに関しては職能別専門会議で掌握されます。社内横断的な対策が必要なリスクに対して、適切な管理対策を講じることができる、という事業リスクマネジメントシステムの目的に添った方法であるといえます。
- この方法を取る場合、各事業本部長にはリスクマネジメントに対する責任と意識の高さが要求されます。しかしリスクが発現してしまった場合、すべての責任を当該事業本部長に負わせるような仕組みにしてしまわないように注意が必要です。責任の所在を明らかにすることは重要ですが、事業本部長の「責任を負うのは自分だけなのだ」という意識がリスクに対する隠蔽体質を作ります。なにかあった場合にはすぐにCROに報告相談するという意識を作ることで、リスクの発現と隠蔽を防止することが必要です。

社内機能と地域で網羅する

この企業では、社内の機能別にリスクマネジメントを実施し、同様の機能を持つ地域に展開することで組織横断的なリスクマネジメントを実施しています。

事例 | **ある消費財製造業の組織体系**



縦軸に機能を、横軸に地域を配置して両面から網羅的にリスクを管理している

- この企業では社内の機能別にリスクを管理することが前提になっています。地域を横軸に置く理由は、社内の各機能で想定されるリスクは地域を問わずある程度共通であると想定されるからです。
- 機能ごとにリスクが管理されることで、各地域に同様のリスクに対する警告及び対策を実施することが可能になります。
- 以前より社内の機能にあわせてリスクマネジメントが行われてきた企業では、新たな管理単位を確立するよりもこのような方法が望ましいでしょう。ただしこの場合、地域によって想定されるリスクが異なることや、本社と海外スタッフとのリスクに対する認識の相違に十分な注意が必要になります。

2.3.3　リスクをその性質から分類し、分担して管理する

全社的にリスクマネジメントシステムを運用する場合でも、発見されたリスクの性質そのものを考慮し、その性質ごとに分類の上、分担して管理する方法を取っている企業がありました。

リスク本来の性質を考慮して分類し、同一部門や部署内で分担して管理する場合と、別々の部門や部署で分担して管理される場合があります。

原則として事業リスクマネジメントの基本はリスクの一元管理にあります

しかし現実にはその性質によってリスクを分類し、分担して管理するケースもあります。この場合、リスクを評価する段階で明確な分類基準を設けた上で管理方法を検討する必要があります。

リスクを分担して管理するメリット

リスクを分類し、分担して管理するメリットを以下に挙げます。

リスクをその性質から分類することでリスクの評価を行う際の確実性があがる

定量化できるリスクを明確に分類することで管理が容易になる

- リスクを分類することでリスクの評価を行う際に、その性質を考慮した評価が可能になるため、評価の確実性が増し、全社で対応するリスクの決定に役立ちます。
- リスクはすべて明確な定量評価が可能であるとは言い切れません。例えば、オペレーショナルリスクの発生確率をリスクの発現経験無しに、定量化することは困難であるといえます。このように確実に定量化可能なリスクと定量化することが困難なリスクを分類して評価することは、リスク評価の確実性の向上につながります。

リスクを分担して管理する場合の注意点

リスクを分類し、分担して管理するメリットを最大限に生かすためには注意すべき点もあります。

分担管理体制の狭間で見落とされるリスクがないか入念に確認を行う

- リスクをその性質から考慮し分担して管理する場合、全社としてリスクを発見、分類する際にその分類から漏れて管理から見落とされてしまうリスクが出る可能性があります。
- リスクを分担して管理する場合には、社内のリスクを網羅的に概観してから、分類のフレームに当てはめていく必要があります。分ける、という意識が先に立つ場合、リスクが見落とされる可能性があり非常に危険です。

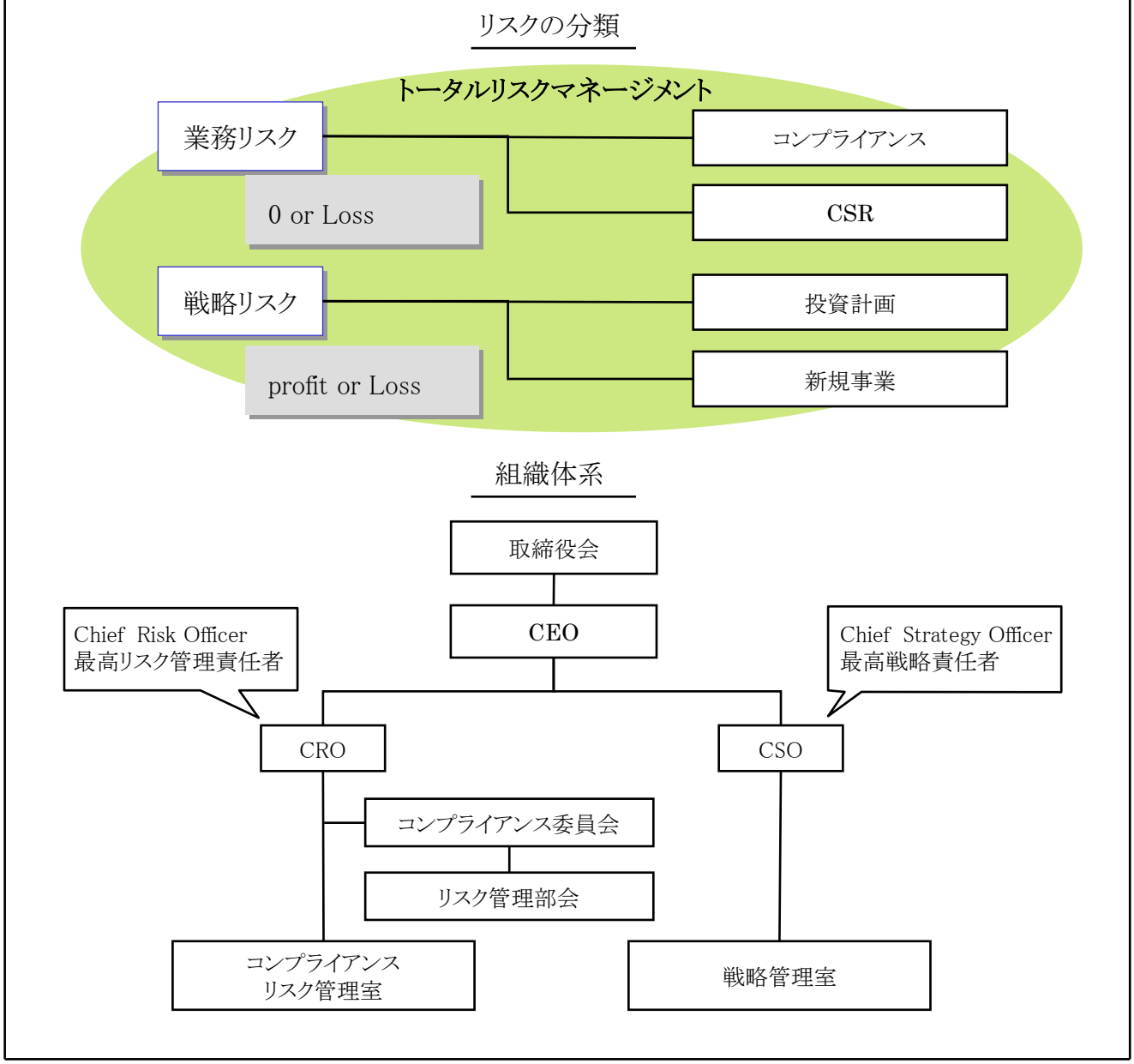
分担した体制の上に、全体を見渡す機能を持たせる

- 本来的には全社のリスクは一元管理される必要があります。従って、日常のリスクマネジメントでは分担して管理されるとしても、分担で管理されているリスクを改めて俯瞰する組織や役割、機能を持たせる必要があります。
- 俯瞰する機能がない場合、従来の個別に管理されていたリスクマネジメントと同じ状態が起こり、社内のリスクを一元管理できていないのと同じ状態になる可能性があります。

業務リスクと戦略リスクに分類する

この企業では、全社のリスクを業務系のリスクと戦略系のリスクに分類して管理しています。
組織もリスク別に構成されています。

事例 | **ある生産財製造業のリスク分類・分担体系**



業務リスク：日常的なリスクの発見、評価、対策、モニタリングによって管理されるもの

戦略リスク：戦略立案、意思決定時のリスク分析、戦略実行時のパフォーマンスモニタリングによって管理されるもの

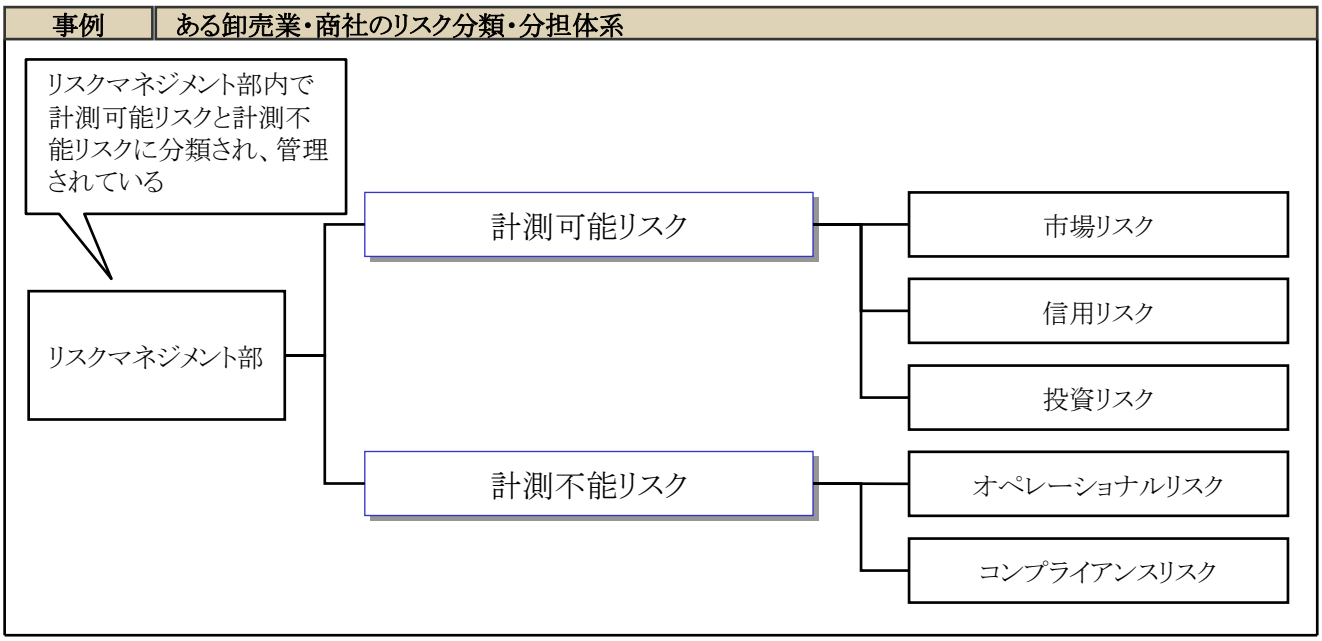
- この企業では、ゼロまたはロスの結果しか生まない日常的に管理されるべきリスクと新規事業等利益を生み出す可能性があるリスクを分類して考えています。
- 多くの企業が「ゼロまたはロスしか生まないもの」をリスクと考えているのに対し、この企業では、利益を得るためにロスを抱える可能性があるリスクを個別に管理していることが特徴です。
- 戦略上のリスクを個別に管理することで、投資計画や新規事業への参入などの際に経営上の意思決定に大きく貢献することが可能になります。

なお、戦略リスクの具体的な扱い方に関しては「Chapter4」内洗い出し対象リスクにて詳しく解説します。

計測可能リスクと計測不能リスクに分類する

この企業では「リスクマネジメント部」が設置され、この一つの部署でリスクマネジメントが統括されています。ただし、このリスクマネジメント部内で計測可能リスクと計測不能リスクという二つの種類にリスクを分類して管理しています。

事例 ある卸売業・商社のリスク分類・分担体系



計測可能リスク:リスクを定量的に評価し、リターンを得るために抱える可能性のあるリスクを評価。リターンを最大化させることを目的として管理されるもの

計測不能リスク:リスクを保険を掛けるなど第三者に転嫁し、リスクの発現可能性を縮小することを目的として管理されるもの

- 計測可能なリスクとは、前掲の戦略リスクに近い概念であるといえます。つまり、正確な数値化が可能であり、経営の意思決定に役立つリスク評価になります。一方、オペレーショナルリスクなどはその発生可能性やインパクトをすべて数値化することは不可能であり、数値化可能なリスクとは区別して管理するという概念です。
- 実際、すべてのリスクを数値化することはほぼ不可能に近いため、このような分類方法はかなり現実のリスクの性質に近い管理方法といえます。
- 計測可能、不可能という分類にすることでリスク対策も策定しやすく、管理そのものも容易になります。

2.3.4　誰が各部門、部署のリスクマネジメントを統括するか

各部門や部署のリスクマネジメントを統括する体制を整備する場合、各部門や部署内の如何なる人物にその中心メンバーになってもらうかを考慮する必要があります。

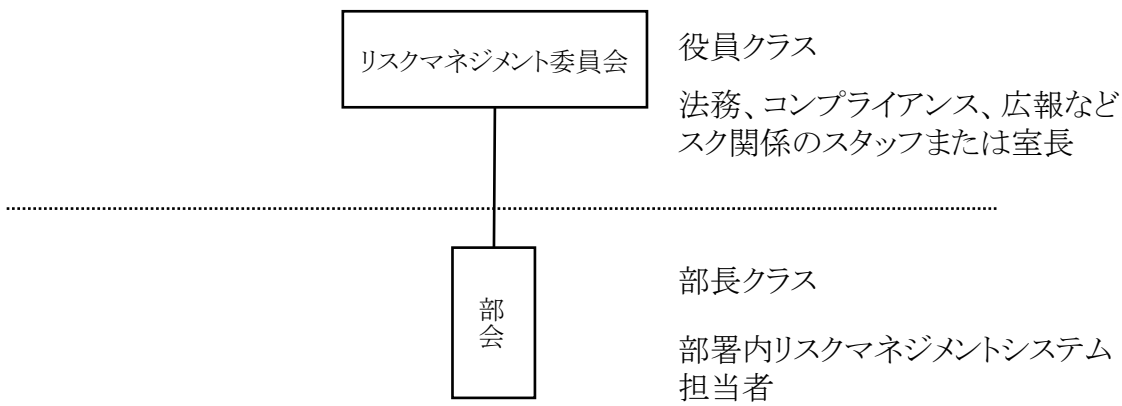
中堅社員や各部門、部署のリスクマネジメントのプロを集める

- ある程度経験を積んだ社員に参加してもらう必要があります。彼らが社内の業務内容を一番よく理解していると考えられるからです。
- また、各部門や部署で従来よりリスクマネジメントに携わっていた人材に参加してもらうことが必要です。彼らはリスクマネジメントに対する意識が高く、また個別のリスクファクターに関しては高い知識を持ち合わせていると考えられます。彼らの納得を得た上で全社的な取組みを行うことは必須条件であるといえます。

各部門や部署のリスクマネジメント統括組織には部長クラスをメンバーとする

- 全社リスクマネジメント統括組織の直下の組織が社内の個別具体的なリスクを話し合う場であることを考えると、現場を俯瞰し、かつ現場について一定の決定権と影響力を持ち合わせている部長クラスがメンバーとして相応しいと言えます。実務上も部長クラスが選任されることが多いようです。

事例　**ある消費財製造業の組織体系**



- この企業では、リスクマネジメント委員会直下の部会に責任者としての部長クラスの人材と、従来各部門や部署でリスク対策責任者を務めてきた社員を選任しています。役員や部長が積極的にリスクマネジメントに関与することの重要性はもちろんですが、一方で、従来リスク対策にあたってきた社員を組織に取り込んでいくことが、リスクを正確に把握する意味でも、また実行性の高い意味のある組織を作るためにも重要なことであるといえます。

次世代の経営幹部候補を選任する

- リスクマネジメントを経営上の重要事項と認識し、次世代の経営幹部候補社員をリスク管理部署のメンバーとして任命している企業もあります。事業リスクマネジメントは、企業経営そのものであり、社内に存在する全てのリスクを理解しておくことや、リスクマネジメント手法を理解することは、経営上の意思決定のためには、非常に重要です。
- 次世代の経営幹部候補をメンバーとして選任することは、企業経営の観点からも、次代の経営を担うという姿勢を彼らの側に作るためにも大きな意味があります。

コラム

体制が先か実施が先か

ヒアリングを行った企業の多くは事業リスクマネジメントを実施するために体制を整え、リスクマネジメントのための手順や役割、責任を明確化してから事業リスクマネジメントを実施し始めていました。
しかし、最初の一年間は暫定的に事業リスクマネジメントに取組み、その結果としてコンプライアンス委員会の設置を決定したという企業がありました。

この企業では、社員からの提案により事業リスクマネジメントシステムの導入が検討されたため、当初は経営層の意識も薄く、取締役会の下部組織において「実際にやってみる」ということだけが決定された状態でした。社内への正式な説明もなく、言い出した部署が事務局となり、コンサルタントの協力を得てとにかく初年度の事業リスクマネジメントを実施しました。

初年度が終了し、事業リスクマネジメントを体感したことで、上層部もその重要性を理解し、何か特別な組織が必要なのではないかという意見が出るようになりました。そこで初めてコンプライアンス委員会を設置することが決定されました。

社内横断的に情報を収集する組織が既にあり、役割と責任が明確であれば必ずしも初めから体制を整える必要はありません。しかしこの企業の場合は体制もなく、経営トップからの説明もまったくなかったため、当初は社内各所から「なぜやるのか」という声が出ました。

体制を整える目的は「組織内のリスクマネジメントを円滑に運営するため」です。体制を整えることは、社内へ事業リスクマネジメントの重要性の認識を広げるために大きな効果があります。事業リスクマネジメントに取り組むのだ、その組織が中心になって取り組むのだ、ということ認識を広めることは、事業リスクマネジメントを実施していく上で非常に有効でしょう。

2.4 事業リスクマネジメントシステム維持のための仕組み

ここでは「いかにして事業リスクマネジメントシステムを維持するか」について解説していきます。
具体的には
・ 事業リスクマネジメントシステムをどのようにして社内に浸透させるか
・ どのようにして仕組みを維持するのか
に関して説明します。

2.4.1 事業リスクマネジメントシステム維持のための8つの仕組み

事業リスクマネジメントシステムは構築するだけでなく、これを維持していくことが必要です。構築するだけに留まらず、社内の継続的な活動にしていかなくては意味がないのです。
継続的な活動にしていくことでリスクが発現した場合にも適切な対処が可能になります。従って、維持のための仕組みは非常に重要といえます。

JISQ2001ではリスクマネジメントシステムを維持するために必要な仕組みとして8つを挙げています*。
*『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年 より作成

教育	能力・教育・訓練
シミュレーション	シミュレーション
コミュニケーション	リスクコミュニケーション
記録	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
リスクの監視	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	リスクマネジメントシステム監査

本テキストではこの8つの仕組みを、教育、シミュレーション、コミュニケーション、記録、リスクの監視、リスクマネジメントシステム監査の5つのカテゴリーに分け、このカテゴリーに沿って説明していきます。

2.4.2　教育

「事業リスクマネジメントシステム維持のためには組織成員全員が、リスク感性を向上させ、そのソリューション能力を身につけていることが必要です。そのために組織内で教育プログラムを作成することが効果的といえます。

教育プログラムを策定する場合には以下の観点に考慮する必要があります。

- 組織の構成員の役割に応じた教育項目を設定する
- 教育および訓練を受ける、部門及び部署をリスクごとに定め、その中から教育を受けるべき要員を指名する
- 教育成果の客観的な評価を可能にする
- 要員の現状の能力*」

*『事業リスクマネジメント-テキスト- 経済産業省 平成16年3月』417ページ、『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年 より一部修正

研修といってもリスクマネジメントに対しより深い知識を身に付けてもらうという性質のものではなく、現在の時点で実行できていないことが何かを識別し、実行するためにリスクマネージャーと共に協力し合おう、というスタンスを取っている社もあります。

この場合の研修目的は、リスクマネジメントを担当者が自分でできるようになることでは無く、リスクマネジメントに対する意識付けと協力を呼びかけることなのです。

平時よりリスクマネジメントの意識付けを行うことが、有事に最大限の効果を生み出すと考えられています。

なお、社員の意識付けには事業リスクマネジメントのスローガンも大いに役立ちます。スローガンに関しては「Chapter3」内「リスクマネジメント方針をスローガンとして掲げる」で説明します。

テキストのコンテンツ

事業リスクマネジメントシステムを維持する上で継続的な研修は重要な位置を占めています。この研修は各部門や部署のリスクマネジメントシステム担当者の能力と意識の向上、また担当者以外のすべての従業員の意識の向上を目的にして行われます。

様々なリスクに囲まれている昨今では、社員一人一人がリスクに対して敏感であることが求められているのです。社員一人一人のリスクマネジメント意識の浸透を主な目的として、多くの企業がテキストを作成して研修を行っています。

参考 一般的なテキストのコンテンツ

リスクマネジメントの定義

- リスクやリスクマネジメントに関する一般的な説明。

自社のリスクマネジメントシステムに関する説明

- 自社で実施するリスクマネジメントはどのようなものか（体制や方針を含む）を説明。

リスクマネジメント実施方法

- リスクマネジメントを実際に行う上で理解しておくべき方法論を解説。
- 自社の方法論を理解してもらう。

リスクマネジメント実施計画

- リスクマネジメントをどのように実施していくのかを自社のスケジュールにあわせて決定し、説明する。

テキストは自社で作成されることが多いようですが、リスクマネジメントの詳細な手法に関しては2003年度事業リスク評価・管理人材育成システム開発事業『事業リスクマネジメントーテキストー 経済産業省 平成16年3月』を参照することもできます。

いつ教育するのか

定期的な機会を設けて、リスクマネジメントに対する意識の喚起を図ることが多いようです。また朝礼の場やイントラネットなど日常のコミュニケーションの中に埋め込むことで大きな啓蒙効果をあげていた企業もありました。

異動に併せて研修を実施

- 社内の研修機会を捕らえてリスクマネジメントに関する研修を組み込むことが効果的です。毎年同じタイミングで研修プログラムを組めば、リスクマネジメントの研修を継続的に実施する体制を確保することが可能になります。

社員が耳を傾ける機会に繰り返し伝える（朝礼や社長の挨拶）

イントラネットを利用して伝える（掲示板、メール）

- 社長や上級幹部からの継続的な伝達はどのようなマニュアルよりも大きな効果を発します。
- 現場の社員にはイントラネットを通しての啓蒙活動が効果的です。ある企業では「メールは必ず本人が目を通すものなので効果的だ」という話が聞かれました。イントラネットが発達している企業ではメールや掲示板などを活用して啓蒙活動を行うことが可能です。

だれが教育するのか

社内講師と社外講師の2つの方法があります。

各部門、部署の研修やセミナー開催時にリスクマネジメント担当者が直接出向いてリスクマネジメントに対する説明を実施

外部講師を招いてセミナーを実施

- リスク管理部署やリスクマネジメント委員会事務局など全社のリスクマネジメント統括担当者が実際に教育を行うことは無駄が無く、またリスクマネジメントの重要性を伝える意味でも意義があると言えます。
- 外部講師によるセミナーに期待される役割は、リスクマネジメントの重要性の伝達です。リスクマネジメントに対する重要性を十分に伝えるために、いかに他の企業で取組みが重要視されているか、なぜ重要視されているのかに関して第三者から語られることも有効です。

だれに教育するのか

事業リスクマネジメントが全社的な取り組みである以上、教育の対象も原則全社員です。ただしその中で行われる教育の内容は、各人の果たす役割に応じて決定されます。

リスクマネジメントに携わる全社員

各部門、部署のリスクマネジメントシステム担当者、推進責任者

対役員：リスクマネジメントの重要性を説くことに重点

対部長、課長：リスクマネジメントの実施、運用方法を伝える

対現場社員：リスクマネジメントの重要性や日頃の心構えを説く

- 教育はリスクマネジメントに携わる全従業員を対象に行われます。しかし、全従業員に同一の教育方針で行われるのではなく、役職や期待する役割に応じて行われます。
- 役員への教育には事業リスクマネジメントの重要性に関する認識と理解を主な目的とします。彼らの理解と協力無しに事業リスクマネジメントを実施することは不可能です。
- 部長や課長は、リスクの発見や対応及び報告の実務に携わることから、リスクマネジメントを実施するための具体的方法に関する研修を実施します。
- 現場の社員にはこの研修を通してリスクの重要性を理解してもらい、以前ならば見逃されていた小さな変化やリスクを見逃さないようにする意識付けを行います。この意識付けがリスクの発現確率を低下させることにつながります。

どのように教育するのか

ここでは、研修のプログラムの例を紹介します。単なる知識の講義ではなく実際にやってみることで、実践的なスキルを開発することができます。

事例	ある消費財製造業の新任課長リスクマネジメント研修の概要

リスクマネジメント管理体制、危機管理体制に関する講義（40分）

リスク発見、評価、対策に関するグループディスカッション（60分）

① 社内に存在するリスクを3つ挙げる
② 当該リスクの影響度と発生頻度を考慮の上、リスクマップを作成
③ リスク評価の妥当性に関して議論
④ 重要リスク一つに関して対応策を策定

- 部長や課長は自部門、部署で実際にリスクマネジメントを実施するため、具体的な手法を理解する必要があります。このように「実際にやってみる」研修は各部門や部署で個別に実施されるリスクマネジメントのレベルを合わせるためにも意義があります。

2.4.3　シミュレーション

「JISQ2001で言うシュミレーションとは、実際にリスクが発現したことを想定して、組織としてどう対処するかをシミュレートし、想定しているリスクに対して必要な判断力や技術の検証、シミュレーションの妥当性、リスクマネジメントシステムの妥当性の検証、要員の教育・訓練効果の向上などを目的として行うものです。」

実際にはリスク管理部署や、リスク対策を担当する部門や部署などが社内で関係する部門や部署に呼びかけて年一度または二度、社内の規程に沿って実施されます。

「シミュレーションの手順には以下の事項を含めることが望ましいでしょう。

- シミュレーションの目的を明確にする
- 特定のリスクが発現していく過程、リスクが発現して緊急時になる過程、緊急時を脱して復旧時となる過程などのシナリオの策定及び環境変化の設定
- 特定のリスクが発現していく過程、リスクが発現して緊急時になる過程、緊急時を脱して復旧時となる過程などにおけるリスク対策及び手順の確認
- シミュレーションの実行計画の策定
- 特定のリスクが発現する過程、緊急時となる過程、復旧時となる過程などにおける緊急時実行組織の編成、適切性及び機能の確認
- 組織内関連部門及び部署、並びに外部機関との調整及協力の確認
- 情報管理、リスクコミュニケーション及び広報の機能検証
- 対応又は手順が不適切な場合に、是正及び改善を実施する基準の設定*」

*『事業リスクマネジメント-テキスト- 経済産業省 平成16年3月』419ページ、『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編　2003年 より一部修正

2.4.4　コミュニケーション

事業リスクマネジメントを実施する上で、コミュニケーションは極めて重要であると言えます。社員一人一人から小さな変化やリスクを報告してもらうことが必要です。また、リスクに対する社内の情報共有が重要です。

また「リスクコミュニケーションとは、意思決定者とステークホルダーとの間でリスク情報を共有し、リスクに対する理解度を高める活動のことを言います。リスクコミュニケーションという言葉が表わしているとおり、リスク情報を開示するだけではなく、ステークホルダーとの間で共に考えていくというプロセスに意味があります。

リスクマネジメントシステムの維持にあたって、リスクコミュニケーションは次を目的として実施されます。

① リスクを発見・特定の情報を収集する
② ステークホルダーが被害を受ける可能性がある場合、それを防止あるいは低減すること
③ 誤解や理解不足のためにリスクが表面化、増幅することを防止すること

リスクコミュニケーションの第一歩としては、リスクの開示の範囲と対象者、開示の手順を決定しておくことが重要です。これは基本的に最高経営責任者が行います*。」

*『事業リスクマネジメントーテキストー 経済産業省 平成16年3月』420ページ、『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編　2003年 より一部修正

社内のリスク情報を共有する

事業リスクマネジメントシステムを維持する上で社内の情報共有化は必須です。
社内で発現したリスク情報を収集し共有化することにより、他の部門や部署で見落とされていたリスクの発見や対応策策定の手助けにつながり、リスクの発現を防止することが可能になります。
ここでは社内のリスク情報共有化のための取組み例を示します。

社内リスク情報の共有化に対する目的を明確に示す

- 社内リスクの情報共有化への目的を明確に示すことで、社内各部門や部署で発現したリスクに対する情報収集が可能になり、対応策策定につながります。また、リスクに関する報告を徹底することで、社内のリスクに関する情報隠蔽を防止できます。

社内のリスクに関するコミュニケーション手段を明確化する

- リスク情報の収集及び発信を誰がどのように行うのかを決定し、社内に明確に示すことにより「如何なる場合」に「誰にどのように報告すればいいのか」を社員が理解することが可能です。コミュニケーション手段の明確化により、社内の情報が一元化され、混乱や誤った情報の錯綜を防止できます。
- 具体的なリスク発現時のコミュニケーション手段は「Chapter5」内「危機管理」の部分で詳しく解説します。

社内のリスクに関する平時及び緊急時の広報手段を確立する

- 平時はリスクマネジメントの重要性を理解し、意識を向上させることが目的となります。イントラネットや朝礼などでトップマネジメントから直接の呼びかけが行われることや、研修を通じての意識の向上が必要になります。
- 緊急時にはすばやい情報収集と適切な対応策がとられ、社員及びステークホルダーに速やかに説明されることが必要になります。正確で速やかな情報収集を元に、責任者の決定及び対応策の策定が行われ、メディアや社内広報を通して説明責任を果たすことが必要です。この場合誰がどのように説明責任を果たすのか、その手段はどうするかを決定しておく必要があります。発現したリスクの大きさにより広報媒体も変化し、責任者も変化します。様々なシナリオを想定し準備しておくことが重要です。

2.4.5　記録

「リスクマネジメント文書は、リスクマネジメント活動の全てのプロセスにおいて必要な文書、記録のことです。たとえば、以下のようなものが考えられます。

① リスクマネジメントマニュアル
② 管理規程・手順書
③ 計画書・記録

JISQ2001では、文書の管理、作成・改定に関して以下の事項に留意する必要があると示しています。

- 文書の作成者及び承認者を明確にする
- 改定担当者及び承認者を明確にする
- 所定の責任者によって文書が定期的にレビューされ、必要に応じて改定され、かつ、所定の責任者によって文書の妥当性が承認される
- 文書の配布先の管理
- 文書の廃止の規程
- 文書の管理
- 機密及びアクセス制限*」

*『事業リスクマネジメントーテキストー 経済産業省 平成16年3月』420-421ページ、『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編　2003年 より一部修正

実際にリスクマネジメントシステムを運用するためにガイドラインや管理規程、マニュアルなどを整備する必要があります。これらは方針をもとにして策定されます。

リスクマネジメントシステム運用時には、これら文書を参考にします。特にマニュアルは、実際に何をするかという手順まで細かく示されたものであり、リスクマネジメントを部門や部署によるばらつきなく全社で実施するためには非常に重要です。

リスクマネジメントガイドライン、管理規程

リスクマネジメントガイドラインや管理規程は、リスクマネジメントを実施する上での方向付けを文書で示したものです。

リスクマネジメントガイドラインでは、事業リスクマネジメント実施のための目的や組織体制、運用、評価などに関する基本的な大枠を文書で示します。

リスクマネジメント管理規程では、リスクマネジメントに携わる各人の役割や組織の役割を規定します。

- 市場リスクや信用リスクに関しては、個別に「市場リスク管理規程」などを策定している企業もあります。「市場リスク管理規程」に関しては「Chapter5」で解説します。
- PDCAサイクルを意識し、漏れや重複の無いガイドライン、管理規程を策定してください。

次ページには管理規定の具体例を示します。実際に管理規定を作成する際の参考にして下さい

参考	リスク管理規程具体例

第一章　総論

　第三条　　全社リスクマネジメント統括組織として、リスクマネジメント委員会を設置しなければならない。

　第四条　　リスクマネジメントシステム運用にあたっては各部門に一名づつリスクマネジメントシステム担当者を設置しなくてはならない。

・
・
・

第五章　報告

　第十五条　　各部門は年一度、リスクマネジメント委員会事務局を通じてリスクマネジメントに関する報告を行わなくてはならない。

・
・
・

- 管理規程には、有事の際の責任者や報告、対応も明記される必要があります。どのような場合、誰が、何をするのか、を明確にします。

リスクマネジメントマニュアル

リスクマネジメントマニュアルでは、リスクマネジメントを具体的にどのように進めるかに関して示します。

参考	一般的なリスクマネジメントマニュアルの構成

- リスクの定義
- リスクマネジメントの必要性
- 当社で実施するリスクマネジメントはどんなものか（体制など）
- リスクマネジメントプロセス（発見、特定、評価、対策）
- リスク評価基準
- リスクマネジメント監査基準

- リスクマネジメント実施方法では、より具体的なリスクマネジメント実施手順を示します。基本的には、各担当者はマニュアルのみ見ればリスクマネジメントに関する業務が可能になります。

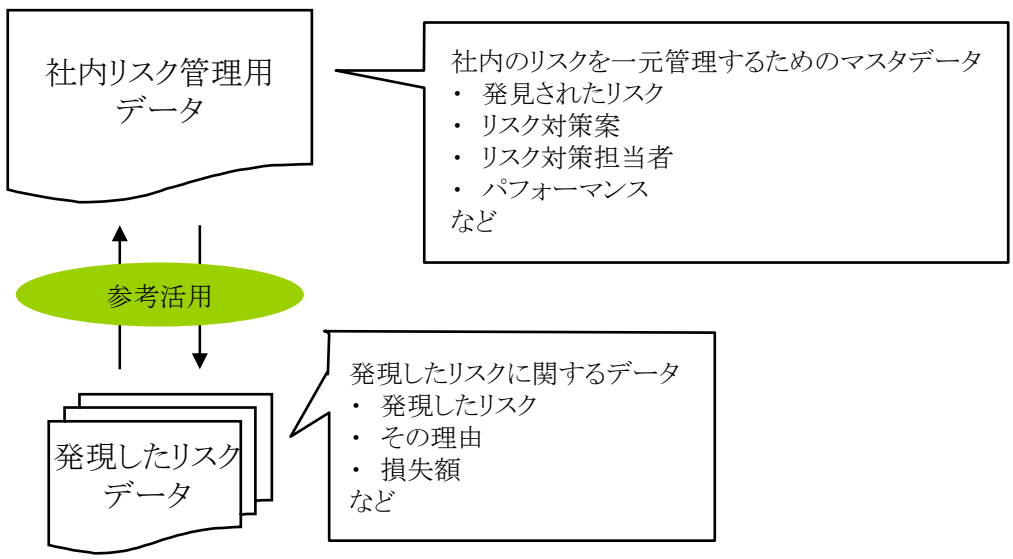
社内のリスク情報を記録管理する

事業リスクマネジメントシステムを維持する上で、社内で把握されたリスクに関するすべての情報を記録し、管理しておくことは非常に重要です。記録しておくことで社内のリスク発見や、対応策の策定に大きく貢献できます。

社内のすべてのリスク情報をデータベース化する

- 社内で発見されたすべてのリスク及び発現したリスクに関しての情報を収集、記録することによって、次年度のリスク発見及び対応策策定に大いに貢献できます。
- データベース化といってもエクセルを利用しての管理で十分です。過去データの分析や対応策に対するパフォーマンスを記載することが重要です。このデータベースを閲覧、分析することにより、現在及び未来のリスクマネジメントにヒントを与えられます。

参考 一般的なリスク情報管理方法



- 通常リスクに関する情報は、このような二重構造で管理されています。マスタデータとしてのリスク一覧と発現したリスクに関する一覧データです。
- 社内で発見された全てのリスクに関する対策や責任者、パフォーマンスに関して毎年加筆、更新され、保管されるものをマスタデータとします。
- 発現したリスクに関する一覧データは発現した事象や取っていた対策、損失の大きさなど発現したリスクに関する全ての情報を記録します。場合によってはリスクが発現した部門や部署の当該リスクに対する評価もここに記録されます。社内で同様のリスクが考えられる他の部門や部署では他部署のリスク評価結果と発現理由を参考に、リスク対策を策定できます。
- すべてのリスクに対しこのようなデータを取ることで、過去から現在までの対策やパフォーマンスを分析することができます。
- このシートは毎年加筆、更新され、過去のデータと紐付けられて活用されることが望ましいでしょう。

2.4.6　リスクの監視

発見されたリスクは、継続的に監視されることが望まれます。なんらかの対策を講じるリスクに対しても、現段階では対策を講じないとされたリスクに対しても、社内では十分なケアが必要になります。

JISQ2001では発見したリスクの変化を継続的に監視するために、リスクに対して変化を与える因子を特定し、情報を収集することが望ましいとしています。リスクの変化に影響を与える因子の特定には以下の事項を考慮します。

「- 法的要求事項及びその他の要求事項
- 社会通念
- 組織の状況
- 関係者の状況
- 組織を取り巻く環境
- 学術的知見の動向
- リスク低減のための対策技術の動向*」

*『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年 より引用

リスク対策を講じないと決定したリスクに関する具体的な監視方法は、4.2.5～～にて詳しく解説しています。

2.4.7　リスクマネジメントシステム監査

事業リスクマネジメントを管理、維持していくためには監査手続を踏むことが必要です。監査手続に沿って行われるモニタリングを通し当該年度の計画や対応策がどのように実施されどのような効果を上げているのか、昨年度との違いはどこか、何がよく、何がいけなかったのかを詳細に分析することが可能です。

JISQ2001ではリスクマネジメントシステム監査の目的を以下にように示しています。

「- その組織のリスクマネジメントシステムが、この規格の要素を考慮して適切に構築され、実施され、維持されているか否かの判断をする
- 最高経営責任者によるレビューに資する*」

またリスクマネジメントシステム監査の手順は、次の次項を含むことが望ましいでしょう。

「- 監査する範囲の決定
- 頻度及び方法の決定
- 監査人の能力の設定
- 監査結果に関する関係者の協議*」

*『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年 より引用

監査を行わない場合事業リスクマネジメントが単に実施されたという事実しか残らず、実際にどのように実施されたのか、今後どのように改善していくのかという視点でのチェックが行われずシステムの維持につながりません。

リスクマネジメントシステム監査に関しては6章にて詳しく解説していきます。

コラム

リスクマネジャーの資質

ヒアリングに伺った際非常に印象深く感じられたのは、リスクマネジャーと言われる方たちの事業リスクマネジメントに対する姿勢でした。
特に印象的だったのは、各部門や部署のリスクマネジメントシステム担当者との接し方に関しての話です。

「現場でリスクに向き合っている各部門や部署のリスクマネジメントシステム担当者からの信頼を得なくては何もできない。どんな些細な変化でも見逃さずに、またどんなことも報告を恐れずにいてもらうことが大切なのだ」
たとえ小さな事故であっても、隠蔽せずにリスクマネジャーに報告する。この変化が些細なものなのか、重大なものなのかは分からないが、あの人に報告しておけばなんとかしてくれる。大丈夫だという信頼を得ることが、なによりもリスクの顕在化を防ぐことになります。

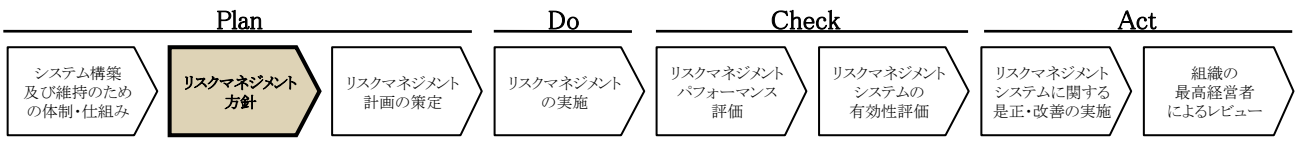
ある企業では「リスクマネジメントの基本は相談。各部門、部署のリスクマネジメントシステム担当者から相談がある間は、大きなリスクが発現することはない」という話もありました。
“リスクマネジメントの基本は相談”。非常に重い言葉に聞こえました。
あの人に相談すればなんでもすぐ上に伝わってしまうから、相談するのは止めよう、という意識が働いてしまえばリスクマネジメントは機能しなくなってしまいます。

リスクマネジャーは社のリスクに対する命運を握る方たちです。リスクに正面から向き合い、真剣に考える人材であるとともに、相談窓口としての資質を見極める必要があります。

CHAPTER 3

リスクマネジメント方針

3.1 リスクマネジメント方針策定の意義
3.2 リスクマネジメント方針策定



本章では「どのようにしてリスクマネジメント方針を策定するか」を事例をもとに解説していきます。

企業はリスクマネジメント方針を通じて、リスクマネジメントの方向を社内外に明確に示します。

方針を策定する上で大切なことは

> 企業にとって最重要視すべきことは何であり、そのために何をするのか

を考慮することです。

方針策定は単なる手順ではなく、企業の方向性を決定するという意味で非常に重要な過程です。

この章の内容

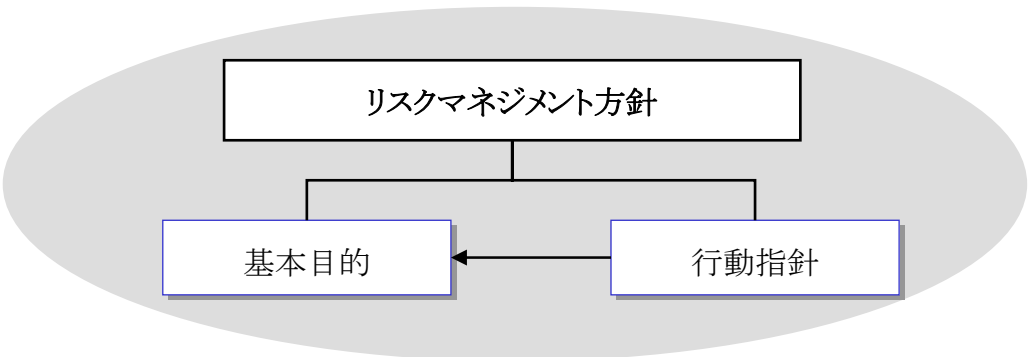
3.1 リスクマネジメント方針策定の意義

ここではなぜリスクマネジメント方針を策定する必要があるのかに関して説明します。
具体的には
・ リスクマネジメント方針とはなにか
・ なぜリスクマネジメント方針が必要なのか
に関して解説していきます。

3.1.1 リスクマネジメント方針とは

リスクマネジメント方針とは、企業が「リスクマネジメント活動において何を目的として、何をどのように実施するのかに関する声明*」です。
* 鈴木敏正&リスクコンソーシアム21『リスクマネジメントシステム』日刊工業新聞社 2002年 より引用

JISQ2001では「リスクマネジメント方針は、リスクマネジメント行動指針及びリスクマネジメント基本目的からなる」と示しています。



鈴木敏正&リスクコンソーシアム21『リスクマネジメントシステム』 日刊工業新聞社 2002年 より作成

つまり「リスクマネジメント方針」そのものは無く、「リスクマネジメント行動指針」と「リスクマネジメント基本目的」を策定することがリスクマネジメント方針の策定になります。

リスクマネジメント行動指針は、具体的にどのようにしてリスクマネジメントのための活動を実施していくかを示すものです。リスクマネジメント基本目的はリスクマネジメント行動指針を受けた上で、具体的なリスクマネジメントの到達点を示すものとなります。

しかし、リスクマネジメント行動指針及び基本目的という分類で厳密に規定している企業は多くないようです。だからといってそのような企業にリスクマネジメント方針がないわけではありません。実際には、リスクマネジメント方針に該当するものがリスクマネジメントポリシーまたはリスクマネジメント目的と呼ばれるものに含まれていることが多いようです。また、リスクマネジメント方針に対する社内の理解を促すことを目的として、リスクマネジメント行動指針及び基本目的を詳細に規定する代わりに、その趣旨を簡潔に要約したスローガンを活用しているところもあるようです。

大切なのは企業にとって戦略や最重要課題などの最重要視すべきことは何かを識別した上でリスクマネジメントの必要性を緻密に検討すること、そしてその結果を踏まえた上で企業が進むべき方向を社内外に対し、具体的な表現で分かりやすく示すことです。

3.1.2　リスクマネジメント方針策定の必要性

リスクマネジメント方針は、組織の構成員に企業や経営トップのリスクマネジメントに対する意識を理解してもらうために策定する必要があります。

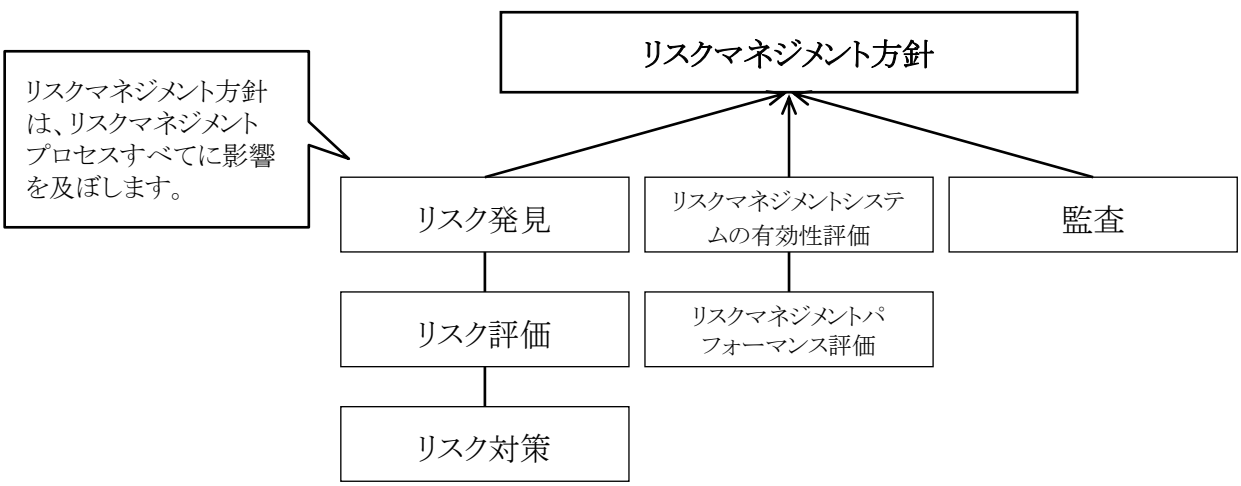
「リスクマネジメントのゴールや目的、管理範囲や制限が明確に定義されておらず、リスクマネジメントシステム担当者にその内容が伝わっていないと、リスクマネジメントシステム担当者は、日常業務活動においてビジネスリスクをきちんと管理できなくなる可能性があります。その結果、経営トップから見て許容しがたく、発生を根本から排除するべきだったリスクを容認してしまったり、これとは反対にリスクを伴ったビジネスチャンスについて、全社的なビジネスポートフォリオの観点からは問題なく許容可能だったにもかかわらず、リスクに過剰に反応してしまいビジネスチャンスを逸してしまったりすることが考えられます*。」

* ベリングポイント株式会社 野村直秀、川野克典、待島克史『内部統制マネジメント』生産性出版 2004年 より一部修正

リスクマネジメントプロセスからの必要性

リスクマネジメント方針に基づいて、リスクマネジメントシステムが運用されます。

リスクマネジメント方針が策定されていないと、社内のリスクマネジメントが迷走してしまいます。方針は必ず言葉で示される必要があります。



- リスク発見：マネジメントすべきリスクを方針から判断し、社内に存在するリスクの洗い出しを行います。
- リスク評価：対策を講じるべきリスクの優先順位を決定するための評価軸を方針を基に決定します。
- リスク対策：重大なリスクであると方針で示されているものが、どのような状態でコントロールされていればいいのかを判断します。
- リスクマネジメントシステムの有効性評価・リスクマネジメントパフォーマンス評価：重大なリスクであると方針で示されているものに関するマネジメント結果の有効性及び活動状況の効率性の評価を通じて、適切なマネジメントがなされているかを評価します。
- 監査：事業リスクマネジメントシステムの整備状況及び運用状況の評価を通じて、重大なリスクであると方針で示されているものに適切なマネジメントがなされているかを評価します。

方針策定によって可能になること

リスクマネジメント方針策定によって、以下のような効果が期待できます。

社内外に分かりやすく明確な言葉で当社でのリスクマネジメントとは何かを説明できる

- 方針を文書として公表することで、社内外にリスクマネジメントに対する意識の高さを示すことができます。
- 方針が明確に示されることで、どのリスクを何のためにマネジメントするのかについての社内外の理解が得られずにリスクマネジメントが失敗するという事態を防止することができます。
- 方針という経営トップの方向指示があることで、リスクマネジメントに対する社内の迷走を防止し、効果的なリスクマネジメントへの取組みが実現できます。
- 方針が示されることで、社内のリスクマネジメントに対する求心力を高め、社内一丸となったリスクマネジメントへの取組みが実現できます。
- ステークホルダーに対しリスクマネジメントに真剣に取り組む姿勢を明確に示すことが可能になり、企業イメージの向上、企業信頼の向上につながります。

リスクマネジメントに関する共通言語を社内に作ることができる

- 全社でのリスクマネジメントが実施されていない場合、各部門や部署、場合によってリスクまたはリスクマネジメントの定義が異なり、各人各様にこれらの用語を使用していることがあります。「リスク」という言葉に関して社内の意識を統一することが非常に難しかった、という企業もありました。
- リスクとは何か、リスクマネジメントとは何か、その目的は何かを明確に示すことで、社内に共通の言語と認識が醸成され、全社でのリスクマネジメントへの取組みに対する効果を高めることができます。

社内にリスクマネジメント意識を定着させやすい

- 何のためにリスクマネジメントに取り組むのかを明確にすることで、社員一人一人がリスクマネジメントの趣旨を理解しやすくなります。その結果、社内のリスクマネジメント意識の向上を期待できます。

3.2 リスクマネジメント方針策定

ここではどのようにリスクマネジメント方針を策定するかに関して説明します。
具体的には
・ リスクマネジメント方針を決定する
・ リスクマネジメント方針を表明する
に関して解説していきます。

3.2.1 リスクマネジメント方針策定手順

「企業のリスクマネジメント方針の策定は、事業形態や最高経営責任者の戦略により、多様な方向が存在すると考えられます。しかし少なくとも以下の要素を考慮の上、策定される必要があります。

- クライシスマネジメント
- 品質マネジメント
- 環境マネジメント
- 労働安全衛生マネジメント
- 内部統制
- コンプライアンス
- コーポレート・ガバナンス

方針の表明はとりもなおさず企業の哲学、文化、使命、価値観を再確認し、組織成員と利害関係者の間で共有化していくために重要なプロセスです*。」
*『事業リスクマネジメントーテキストー 経済産業省 平成16年3月』410ページ より一部修正

リスクマネジメント行動指針を策定する

「組織の最高経営責任者は、リスクマネジメント行動指針をリスクマネジメントシステムの構築の際に定め、それに基づいてシステムの運用を行うことが望ましいでしょう*。」
*『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年 より一部修正

以下にリスクマネジメント行動指針の例を示します。

リスクマネジメントを通じて、リスク対応能力の継続的向上を図る

リスク感性の醸成とリスク情報の共有化を行う

緊急事態発生時には速やかな対応と復旧を図る

精度の高い危機管理体制の構築により有事には自社の素早い復旧のみならず、社会貢献を果たすことも目指し、企業イメージの向上を図る

- 経営トップのリスクマネジメントに対する意識が盛り込まれた言葉になる必要があります。
- リスクマネジメント行動指針を策定する場合、以下の項目が盛り込まれることが望ましいでしょう。

「- 組織の社会的評価を高めること
- 組織を構成する人々の安全・健康と組織の経営資源の保全を図ること
- ステークホルダーの安全、健康および利益を損なわないように活動すること
- 被害が生じた場合には、速やかに回復を図ること
- 事態が発生した場合には、責任ある行動をとること
- リスクに関連する社会的要請を組織のリスクマネジメントシステムに反映すること*」

＊鈴木敏正&リスクコンソーシアム21『リスクマネジメントシステム』日刊工業新聞社 2002年 より引用

リスクマネジメント基本目的を策定する

「組織はリスクマネジメント行動指針に基づき、組織に関連するリスクに対して、リスクマネジメントシステムの運用によってどのような到達点又は結果を目指すのかをリスクマネジメント基本目的として明確に設定することが望ましいでしょう。到達点及び結果は、可能な場合は定量化することが望ましいでしょう*。」

＊『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年 より一部修正

以下にリスクマネジメント基本目的の例を示します。

社員と家族の安全確保

業務の継続

企業資産の保全

ステークホルダーからの信頼性確保

- リスクマネジメント基本目的を策定する場合、以下の内容が盛り込まれることが望ましいでしょう。

「- リスクマネジメントが対象とするリスクの種類あるいは被害種類
- リスク低減の目的およびその低減程度
- リスク低減策の到達点を定量的、定性的に表す
- リスクの低減程度を表す評価軸およびその判定基準
- リスクマネジメントパフォーマンス評価の評価軸と到達レベル*」

＊鈴木敏正&リスクコンソーシアム21『リスクマネジメントシステム』日刊工業新聞社 2002年 より一部修正

3.2.2　リスクマネジメント方針をスローガンとして掲げる

JISQ2001におけるリスクマネジメント方針は、リスクマネジメント行動指針とリスクマネジメント基本目的の両方で構成されています。

しかし実際には多くの企業で全社的リスクマネジメントを実施する上で最重要視すべきことを「スローガン」や「キーワード」として分かりやすい一言で語っていることが多いということが分かりました。

リスクマネジメント方針や最重要視すべきことが一言で表現されなければならない、ということではありませんが、スローガンが示されることで社内のリスクマネジメントへの理解が進み、取組み意識が向上することが期待できることも事実です。

リスクマネジメント方針や最重要視すべきことを表現する上で大事なのは「我が社では、このような方針でリスクマネジメントを行うのだ」ということを明確に示すことであり、必ずしも言葉の長さや形態ではありません。しかしながら、方針を簡潔明瞭に伝達する上でスローガンを決めることには一定の効用があると言えるでしょう。 以下にリスクマネジメントのスローガンの例を示します。

トータルリスクマネジメント戦略

- このケースでは、リスクの発現を防止する「平時のリスクマネジメント」と有事のリスク発現による影響を最小化する「クライシスマネジメント（危機管理）」とを併せて「トータルリスクマネジメント」と表しています。加えて「リスクマネジメントを戦略的に実施していく」というスタンスを強調するために、後ろに「戦略」を付しています。

一人ひとりがリスクマネジャー

その場にいる人がリスクマネジャー

- リスクマネジメントシステムが構築されていても、現場の各人がリスクに対して高い意識で臨まなければ効果的なリスクマネジメントは期待できません。このケースでは、各人が高い意識を持ってリスクマネジメントに臨むことが重要視されていることが表われています。

何かあったら必ず一報を

- このケースでは、問題を識別したらどんなに小さいことであっても、必ず報告しあうことで隠蔽体質を排除し、大事件や大事故を未然に防ぐことが重要視されていることが表われています。

Business　Continuity　－　事業継続

- このケースでは、経営計画の達成を阻害する最大の要因は事業の中断であるとの企業の認識が表れています。結果として、リスクマネジメントを事業継続のために行うという明確な目的が示されていることになります。

3.2.3　リスクマネジメント方針を公表する

リスクマネジメント方針は策定後、社内外に表明する必要があります。

「組織の最高経営責任者は、組織のリスクマネジメント方針を定め、組織の構成員及び必要に応じて関係者に対し、文書で明確に表明することが望ましいでしょう*1。」

「その理由は以下の通りです。
・ 組織全体に最高経営責任者の強い意志を表明すること
・ 組織成員全員にその方針を理解させること
・ 組織成員全員が参加すること
・ ステークホルダー（顧客、株主、地域社会など）に対して方針を明らかにして企業の信用を高めること
・ コンプライアンスの遵守を表明することで社会の信頼を得ること
・ 企業イメージ、ブランドを高める*2」

*1『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年 より引用
*2『事業リスクマネジメントーテキストー 経済産業省 平成16年3月』410ページ より引用

リスクマネジメント方針は例えば下記のようなチャネルを通して社内外に表明されます。

リスクマネジメント方針を社内に表明する

イントラネットを利用し、メールや掲示板で最高経営責任者から表明される

朝礼や全体会議など社員全員が集合する場で、最高経営責任者から表明される

- リスクマネジメント方針は社内に対しては表明されるだけでなく、常に開示されていることが望ましいでしょう。管理職以上の全社員に対し、常に閲覧可能な状態にしているという企業もあります。
- どのような方法であっても方針を確認し、リスクマネジメントへの意識を確認できる状態を作っておくことが大切です。

リスクマネジメント方針を社外に表明する

ホームページを利用して公開する

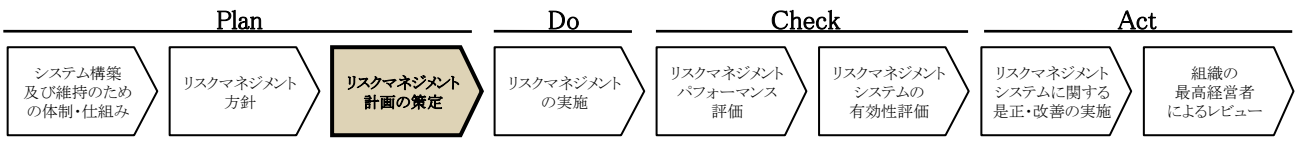
企業情報の開示書類（アニュアルレポート、CSR報告書など）に詳細に記述する

- リスクマネジメント方針を社外に明確に表すことで、ステークホルダーの信頼を得ることにもつながります。

CHAPTER 4

リスクマネジメント計画の策定

4.1 リスクの洗い出し・評価
4.2 リスク戦略、リスクマネジメントの目標、リスク対策の選択



本章ではリスクマネジメント計画策定のための作業について解説します。具体的には、企業に関わるリスクとして何があるのかを把握して、分析を行って、リスクの優先順位付けをした上で、リスクマネジメントの目標を設定して、対応策を策定する、という一連の作業が本章の解説対象となります。

重要なリスクが認識・対応されないでいると、企業はただその脅威に晒されるのみの状態になってしまいます。そうならないように、自社が直面している主要なリスクについて分析をしっかり行い、対応策を立てることが肝要です。

リスクマネジメントではリスクの発現自体を事前に防ぎ、発現してしまった場合にもできるだけ影響が小さくなるように先手を打って管理することが基本です。その意味で、本質的に事前の準備が重要になります。つまり、

> 内容が充実してかつ現実的な計画を立てられるかどうかが、リスクマネジメント全体の成否に非常に大きく影響する

ことになります。

この章の内容

4.2 リスク戦略、リスクマネジメント目標、リスク対策の選択

4.2.1 リスク戦略

リスク戦略の種類

リスク戦略の基本的パターンは

4.2.2 リスクマネジメントの目標設定

リスクマネジメント目標の設定

リスクマネジメントの目標は可能な限り定量化する

4.2.3 リスク対策の選択

時系列リスク対策の分類

機能別リスク対策の分類

どのように具体的なリスク対策を選択すべきか

4.2.4 リスクマネジメントプログラムの策定

リスクマネジメントプログラムを経営計画へ反映させる

日常業務への取組みと同等の優先度

リスクの割当て

リスク対策シート（例）

4.2.5 リスク対策を講じないと決定したリスクへの対応

モニタリングシート（例）

4.1 リスクの洗い出し・評価

ここでは企業にとってのリスクをできる限り漏れなく洗い出した上で、その発生頻度や影響度を検討して、自社で優先的に取り組むリスクを選択する作業について解説します。組織としてこの一連の作業をどのようなプロセスを経て行うべきかについて、自社に適した方式を考え実践することが重要です。

本節ではリスクの洗い出し・評価の進め方について、企業の事例を踏まえながら下記の内容を中心に説明します。

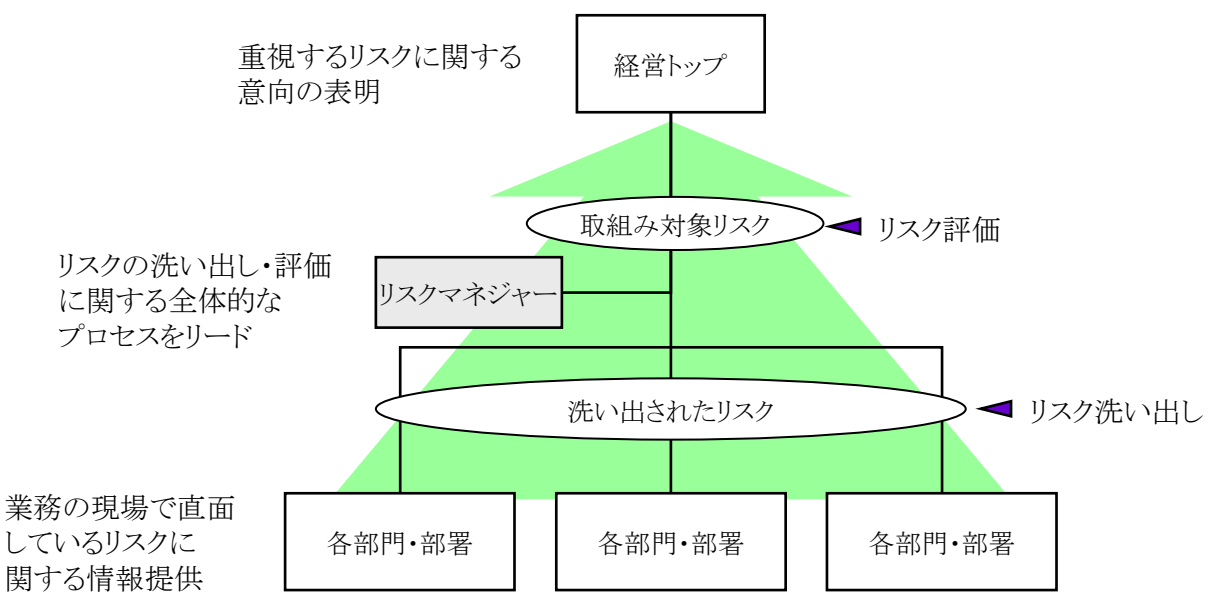
- リスクの洗い出し・評価の全体プロセス
- リスク洗い出しの着眼点
- 調査票の作り方
- リスクの評価方法

4.1.1 リスクの洗い出し・評価プロセスでは何を行うか

リスクマネジャーは各部門や部署からリスクに関する情報を収集・分析し、経営トップの意向も確認しながら取組み対象とするリスクを決定するまでのプロセスに重要な役割を担います。

しかしながら、具体的なリスクの分析作業内容や役割分担となると、あらゆる企業に普遍的に当てはまる特定の優れた方式があるわけではありません。事業リスクマネジメントの先進企業各社でも自社の状況を考慮して、独自の進め方でリスクの洗い出し・評価を行っています。

参考　企業組織におけるリスクの洗い出し・評価

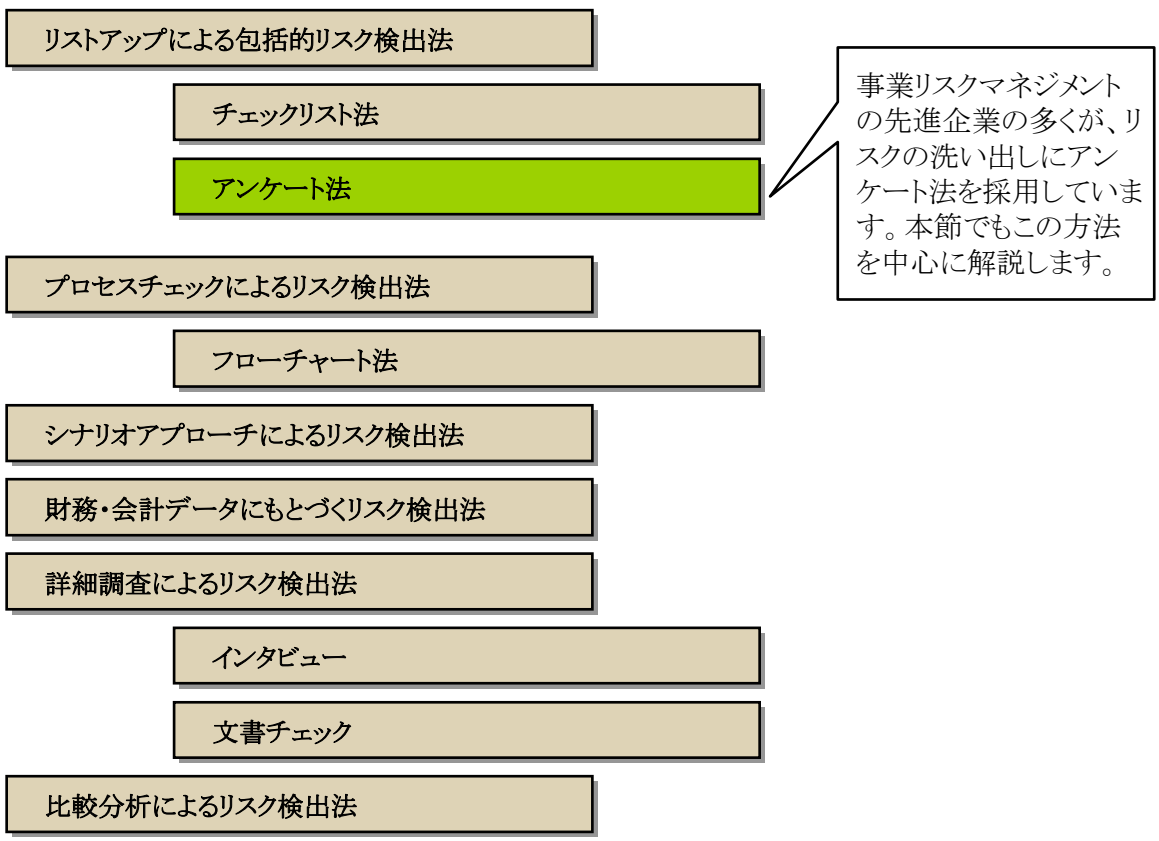


リスク洗い出しのための技法の体系

経済産業省『事業リスクマネジメントーテキストー 経済産業省 平成16年3月』では、企業リスク洗い出しのために活用できる基本的な技法が、6種類8技法に体系化されてまとめられています。各技法に関する解説は、同書の「2.2.1 リスク認知の基本技術」をご参照ください。

事業リスクマネジメントのために多くの先進企業は同書で挙げられた技法のうちで「アンケート法」を活用しています。その理由としては、各部門部署からリスクに関する情報を均質な形式で収集できるというアンケート法の方法の性質によることが大きいと考えられます。本節でもリスク洗い出しの作業プロセスについては、アンケート法を中心に解説します。

参考　リスク洗い出しの主な技法



『事業リスクマネジメントーテキストー 経済産業省 平成16年3月』75-82ページより作成

多くの企業ではアンケート法を中心に用いながらも、他の技法も必要に応じて併用して活用しています。
リスク洗い出しの各技法を組み合わせて、自社に適した仕組みを構築することが効果的です。

リスクの洗い出し・評価の一般的な作業ステップ

ここではリスクの洗い出し・評価の一般的な作業ステップについて概説します。

各作業ステップの詳細について、リスクの洗い出しについては「4.1.2 リスクの洗い出しに関する留意事項」と「4.1.3 リスク洗い出しのための調査票の開発」で、リスク評価については「4.1.4 リスクの評価に関する留意事項」で説明します。

リスクの洗い出しのステップ

ここではアンケート法によるリスクの洗い出しを考えているので、まずリスクマネジャーは調査票（アンケート用紙）を開発します。

全社的なリスクマネジメントですので、多くの事業や職能が広く調査対象となり、調査票への回答が要求されます。地理的にも各地方の事業所や海外拠点で固有のリスクがあることが考えられる場合は、やはり調査対象として調査票への回答を求める必要があります。

リスクマネジャーは、回収した調査票の記載内容について疑問を抱いた場合には、回答内容についての確認作業を行いデータの正確を期すようにします。

これらのステップを経てデータの集計を行い、対象部門ごとのリスク一覧をまとめます。

リスクの評価のステップ

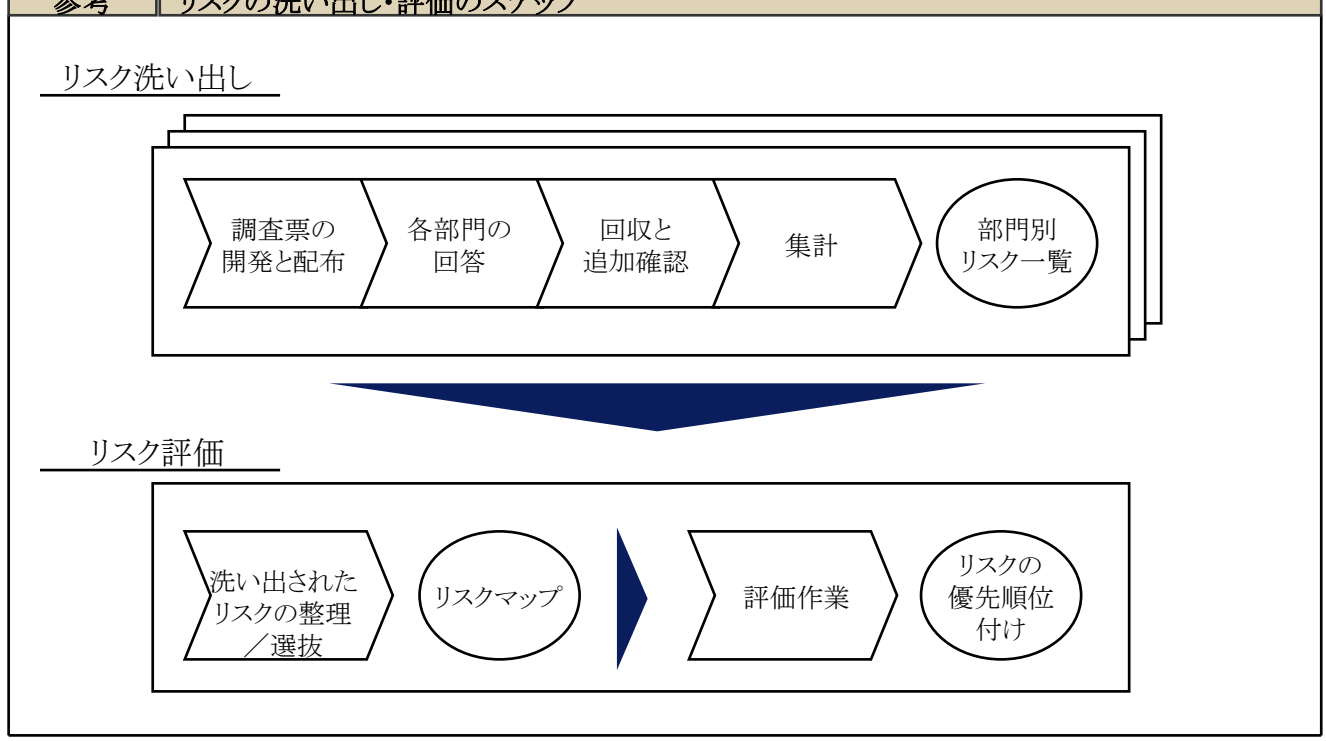
洗い出し作業により収集されたリスクは相当数に上ることが見込まれますが、一方で複数の部門・部署から同じ内容のリスクが挙げられていることが予想されます。また、各リスクの重要度も様々であることが考えられます。

そこで、収集されたリスクを整理します。各リスクを内容別に分類してまとめていきます。

まとめられたリスクについて、何らかの基準を用いて重要度を評価します。多くの企業ではリスクを影響度と発生頻度で評価し、その結果をリスクマップ（次ページ参照）としてまとめています。

こうして作成されたリスクマップをもとに経営トップの意向も反映した上で、自社として優先的に取り組むべきリスクが決定されます。

参考　リスクの洗い出し・評価のステップ



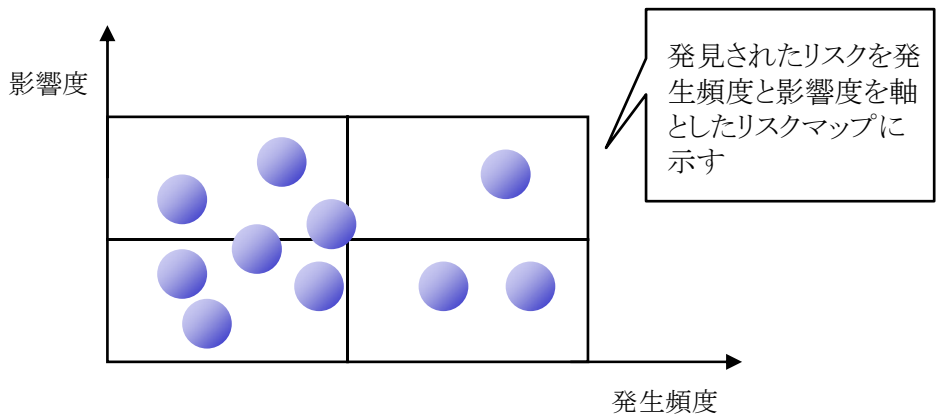
リスクマップとは

リスクは発生の確からしさ(発生頻度)と結果(企業に与える影響度)の2つの要素をもっています。そのため、各リスクを発生頻度の軸と影響度の軸の2次元に表現することができます。それぞれのリスクを、この2次元の図に同時にプロットしたものがリスクマップです。

リスクマップを用いて容易にリスクを相対的に比較することができます。リスクを目に見える形にすることで、多くの関係者との情報の共有が可能になります。

こうして作成されたリスクマップを活用して、自社にとってクリティカルなリスクを見出し対応します。

参考 リスクマップ



「影響度」の範囲と対象リスク

本テキストでは、リスクをプラス・マイナス両方の影響を与える不確実性と捉えていますが、ここで紹介する手法における「影響度」とは、主にマイナス方向の影響であることに注意してください。

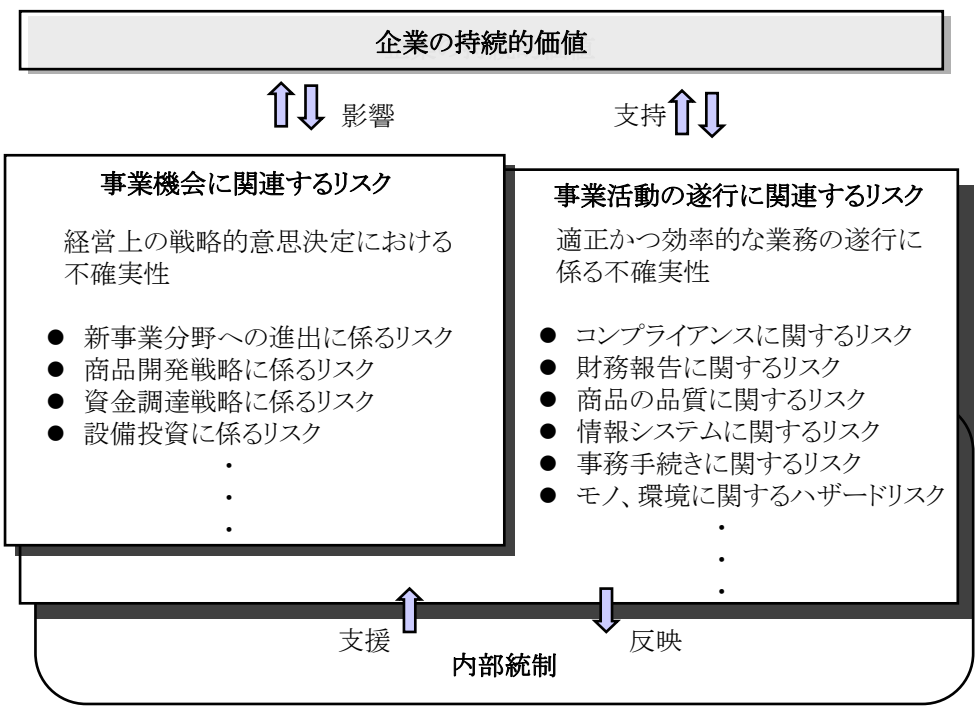
経済産業省『リスク新時代の内部統制』では、リスクを下図のように大きく2種類に分類し、このうち右側の「事業活動の遂行に関連するリスク」について次のように説明しています。

「事業活動の遂行に関連するリスクについては、例えば、コンプライアンスに関して、法令が十分に遵守される等の「良い結果」は当然のことと考えられるため、法令が遵守されない等の「悪い結果」のみが対象と考えられることも多い。この意味においては、事業活動の遂行に関連するリスクのうち、コンプライアンスに関するリスクやハザードリスクなど一部のリスクについては、「事業目的等の達成を阻害する要因」と考えることも可能である*。」

＊ 経済産業省「リスク新時代の内部統制　リスクマネジメントと一体となって機能する内部統制の指針」リスク管理・内部統制に関する研究会 2003年6月 より一部修正

ここで紹介するリスクの洗い出し・評価手法はマイナスの影響を主眼とするため、この「事業活動の遂行に関連するリスク」の洗い出し・評価に適していますが、だからと言って「事業機会に関連するリスク」を取り扱えないというわけではありません。その方法については本章で後述します。

参考　**「事業機会に関連するリスク」と「事業活動の遂行に関連するリスク」**



経済産業省「リスク新時代の内部統制　リスクマネジメントと一体となって機能する内部統制の指針」リスク管理・内部統制に関する研究会 2003年6月 より作成

各社のリスク洗い出し・評価作業の概要

本節の冒頭で述べましたように、リスクの分析・評価は様々な方法が可能です。ここでは、実際の企業での進め方について、数社における概要を紹介します。

事例 | **各社のリスク洗い出し・評価作業 1/2**

洗い出し作業

		消費財製造業A社	エネルギー・鉱業B社
調査対象（調査票送付先）		グローバルに全36ファンクションの全部署	全10部門の企画担当グループマネジャーと全関係会社の総務長
リスク洗い出しの指示		中期計画達成に障害となりうるものを1人当り5～10項目挙げる	事前洗い出しリストを参照して自部門のリスクを挙げる
記載項目 リスクについての評価	影響度	3段階（米ドルで100万以下、100万～1億、1億超）	3段階（相対的大中小）（同じ想定影響額でも部門により評価が違ってよい）
	発生可能性	3段階（1年に1回以上、1～10年に1回、10年に1回以下）	3段階（相対的高中低）（同じ発生可能性でも部門により評価が違ってよい）
	その他	対策実施状況	対応策（現在の実施状況と将来予想の両方記入）、過去顕在化の有無
事務局による支援		特になし（記入マニュアルは作成）	調査票に合わせ事務局が事前に洗い出したリスク250項目のリストと記入見本を提供、部門への説明会の開催
洗い出されたリスク数		約900項目	約400項目

洗い出されたリスク項目の整理／選抜

作業内容	データの集計・整理	数値基準による客観的選抜（足切り）
方法	洗い出された上記900リスクの内容について分類して似た内容のものを集約	洗い出された上記400リスクについて事務局が影響度および発生可能性について評価して、「影響額100億円以上および発生頻度30年に1度以上」という客観基準を満たすリスクを選抜
リスクマップに記載したリスクの数	17項目	数十項目

評価作業

選定事由	1. 影響度および発生可能性が高い 2. 関連部門の数が多い 3. 対応レベルが低い	事務局に総合企画部他を交えセッションにより機械的にプロットされたリスクマップ上の項目位置を修正、上記客観基準に該当しない項目も一部復活選択
取組み決定リスク数	5項目	12項目

事例 | 各社のリスク洗い出し・評価作業 2/2

洗い出し作業

		生産財製造業C社	運輸・物流業D社
調査対象 (調査票送付先)		持株会社傘下のグループ140社 課ごとに洗い出し	リスクマネジメントリーダー100名強 (部門および関係会社から)
リスク洗い出しの指示		シナリオ法を活用して課が抱えるリスクを挙げるフォーム うち重要なリスクについては「リスク対策シート」作成を要求	自部門の業務を洗い出し、それに付随するリスクを挙げる
リスクについての評価 記載項目	影響度	3段階(大中小) (固有リスクと残余リスクの両方記入)	5段階評価 (小数は用いず1～5の何れかに)
	発生可能性	3段階(高中低) (固有リスクと残余リスクの両方記入)	5段階評価 (小数は用いず1～5の何れかに)
	その他	責任者、報告先部署 対策実施状況評価(3段階) 改善課題 フォローアップ時期	リスクに対応する業務の責任者
事務局による支援		リスク洗い出しの記載マニュアル作成とそれに基づいた教育	業務・リスクの洗い出しに支援を必要とする部門にはリスクマネジャーが参画して共同作業で遂行
洗い出されたリスク数		約2,000項目	数百項目

洗い出されたリスク項目の整理／選抜

作業内容	階層別ごとの重要リスク集約・管理	ポイント化
方法	1.課レベルで作成されたリスク一覧を基に部レベルで対策・管理する重要リスクを選出・評価 2.個社レベルで同様の作業 3.事業グループレベルで同様に	1.影響度・発生頻度の各段階について対応する金額・確率を仮置きする 2.両者を掛算した積を各リスクのポイント額とする
リスクマップに記載したリスクの数	数十項目	数十項目

評価作業

選定事由	1. 機械的選定 －残余リスク評価が「高」のもの 2. 自主的判断 －経営戦略達成上阻害要因 －近年社外で発生して問題に	リスク分野別にポイント上位リスク選抜 選抜リスクの合計ポイントを把握
取組み決定リスク数	約15項目	十数項目

企業ごとのリスク・マネジメントへの独自の取組み

ここで挙げた各社の事例を見ても、リスクの洗い出し・評価についてその企業独自の取組みをしていることが分かります。各社の特徴について数点ずつここに記しますが、それぞれに関連したより詳細な説明は本節の以降の部分に盛り込まれておりますのでご参照ください。

消費財製造業A社のリスク洗い出し・評価の特徴

リスクの性格を具体的に示すことで洗い出しをスムーズに実施

- A社ではリスクの洗い出しに当り、回答者に「中期計画達成に障害となりうるもの」を挙げるよう求めています。ただ漠然とリスクを挙げるよう求めるのではなく、このように自社として洗い出すリスクはいかなる性格のものかを具体的に示すことで、自社のリスクマネジメントのニーズに対応した情報を集められるうえ、回答者もスムーズに答えられるようになります。

洗い出されたリスクを的確に整理

- 洗い出された900のリスクを事務局が17にまとめたうえで、リスクマップに載せて評価を行っています。同社ではこれら900リスクを壁に張り出して、内容が重なるものをまとめていく作業を行いました。現場からはそれぞれの業務に関連するリスクが挙げられてきます。これらを的確に整理することもリスクマネジャーの役割です。

全社取組み対象リスクの選定基準を明確化

- リスクマップ上の17リスクから全社的な取組み対象とするものを選抜するときに、同社では3つの基準を設けています。こうした基準によって最終的にどのリスクを残すかを決めるわけですから、ここには自社のリスクに対する価値観が表れるということもできます。ここでは基準のひとつに「関連部門の数が多い」というのがありますが、これは部門間の調整を徹底させないとスムーズな事業運営に支障が生じるという同社が強く抱いている問題意識が反映されています。

消費財製造業A社のリスク洗い出し・評価の特徴

リスクマネジャーによる積極的な準備活動

- B社ではリスクマネジャーが事前にリスクの洗い出しを行って、回答者に調査票と共にリスクのリストと記入見本を配りました。同社では全社へリスクマネジメントを導入するに　当ってリスクといってもどういうものを報告したらよいのかわからないという声が強く、こうしたものを作成したことで、「各人がリスクについて考えていたが、うまくまとめられないでいた」という状況から前進するのに寄与しました。

リスク評価を部門・部署と事務局の二段階で実施

- 同社におけるリスク評価方法は、部門や部署単位での評価と事務局での評価の二段階方式を採っています。
- 部門・部署による洗い出しの段階では相対的評価によることとしています。例えば、想定影響額としては同じ10億円のリスクでも、ある事業部門では影響度を「大」と評価して、他の事業部門では「中」ないし「小」と評価することがあっても構わないとしています。
- この点A社では、どの部門部署でも同じ金額を基準としているのと対照的です。事業部門ごとに投資規模等が異なる等の事情から、まず現場の感覚での評価を求めることにしてB社ではこうした相対評価によることにしました。
- しかし、こうした相対評価結果だけでは全社的にどのリスクが重要かの判断ができないため、同社では洗い出された400のリスクすべてについて事務局が定量評価を行っています。こうすることで各リスクについて同じ評価者の視点による影響度・発生頻度の測定がなされて、一定金額以上の影響（100億円以上等）および一定の頻度以上の発生可能性（30年に一度以上等）という一律の基準による足切りが可能になります。なお影響額の基準は、自社の○○利益（営業利益・純利益等）の何%ないし何年分相当額ということを根拠にしています。

経営企画室の参画

- またB社では取組み対象リスクを選抜するセッションに経営企画室が参画しています同社ではこの部門が参画することで経営トップの見方に近い視点からのコメントが得られたことが有意義であったとしています。

生産財製造業C社のリスク洗い出し・評価の特徴

「固有リスク」と「残余リスク」の双方を回答してもらう

- C社ではリスクの洗い出しに当って「固有リスク」と「残余リスク」の両方を記入することを求めています。詳しくは後述しますが、これはリスクについて対策を講じていない状態で把握する（固有リスク）か、講じている状態つまり現状で把握する（残余リスク）かの違いです。同社では両者を把握することでリスクに関する詳しい情報を集めています。

シナリオ法を活用した調査票とトレーニングの実施

- また同社ではリスク洗い出しのための発想法としてシナリオ法に則って回答ができるよう工夫した調査票を用いています。シナリオ法の説明は後述しますが、ここでは表中の事務局による支援として「記載マニュアル作成とそれに基づいた教育」とあることを確認してください。こうした調査票設計の意図が活かされるように、同社ではトレーニングを行って浸透を図っています。

取組み対象リスクの「機械的選定」と「自主的判断」を組み合わせて判断

- C社では取組み対象リスクの選定に「機械的選定」と「自主的判断」の2つを組み合わせて行っています。前者は洗い出しからのリスク評価の延長にあるもので、残余リスクについての評価結果が「高」となったものを対象とします。これに続いて、更に独自の基準による自主的判断を行います。ここでは機械的選定によって選定されたリスクの吟味に加え、選定漏れとなったリスクについての見直しも行います。同社では自主的判断のために「戦略達成上の阻害要因」とか「近年社外で発生して問題に」といった基準を用いています。

運輸・物流業D社のリスク洗い出し・評価の特徴

業務に基づいたリスクの洗い出しを実施

- D社では、リスクの洗い出しを調査対象部門の業務に基づいて行うようにしています。リスク洗い出しの際に何に着眼して行うのかは本節での重要な論点であり後ほど解説しますが、同社では現場の各部門において実務で中心的な役割を果たしている課長層を中心にリスクマネジメントリーダーを任命しています。そして各リーダーとその部下が担当している業務内容は何か、それに関連するリスクは何かというふうにリスクを洗い出していくことにしました。ですから同社のリスク洗い出し調査票は、業務リストと対応する形式になっています。

リスクマネジャーによる積極的な支援

- ただ、これだけでリスクマネジメントリーダーのもとスムーズに洗い出しが進んだわけではなく、洗い出し作業が滞りがちな部門においてはリスクマネジャーと共に作業を進めました。同社のリスクマネジャーは事務局であると同時にそうした部門における「共同作業者」でもあったとしています。

リスクの大きさをポイントで換算して評価

- またD社では各リスクの一律の定量評価が困難なことからポイント換算の技法を用いています。この技法については後に説明しますが、影響度と発生可能性に関する相対的評価レベルについて、例えばレベル5なら300ポイントなどとポイントを仮置きすることで複数のリスクの重要度に関する相対的な大小の比較が可能なことと、自社が抱えているリスク全体の大きさをポイントで把握して次年度への目標設定に活用できるというメリットがあるとしています。

セッション方式によるリスク洗い出し・評価作業

リスクの洗い出し・評価についてセッション方式を活用して、多人数が参画しながら作業を推進している企業もあります。この場合は、多人数が討議に参加して意見を反映させられるうえ、各人の当事者意識が高まるという効果があります。

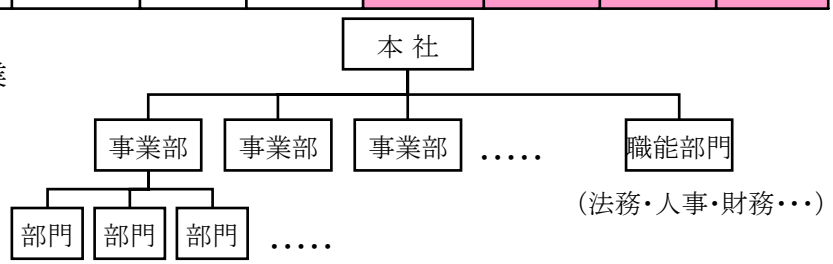
その反面、人数が多くなる分まとめるのが難しくなったり作業が遅くなったりする危険もあります。この企業では図のように部門・事業部・全社の3段階でセッションを開催していますが、セッション開催前にリスク管理担当者（全社については全社リスクマネジャー）がリスクマップの原案を仮作成しておいてセッションの討議で正式なリスクマップを決定するという段取りにすることで、効率化を図っています。

またセッションを充実させるために全社リスクマネジャーは事業部および部門のリスク管理担当者に対して、セッションにおけるファシリテーターとしての役割を果たせるようにセッション運営のための事前トレーニングも行っています。

事例　セッション方式によるリスク洗い出し・評価作業

作業ステップ		部門			事業部		職能部門	本社	
		リスク管理担当者（兼任）	営業・業務マネジャー	部長	リスク管理担当者（専任）	事業部長		全社リスクマネジャー（専任）	経営トップ
1	リスク事前洗い出し				○			○	
2	調査票開発				○				
3	調査票回答	○							
4	部門リスクマップ仮作成				○				
5	部門内リスク評価セッション	○	○	○	○				
6	事業部リスクマップ仮作成				○				
7	事業部リスク評価セッション			○	○	○		○	
8	職能部門リスク洗い出し						○	○	
9	全社リスクマップ仮作成							○	
10	全社リスク評価セッション（経営会議）					○	○	○	○

注）この企業は右図のように各事業部内に複数の部門がある組織構成になっています。またリスク管理担当者が事業部（専任）および部門（兼任）でも任命されています。



4.1.2　リスクの洗い出し時には何に留意するべきか

リスクの洗い出しに関しては、いかに漏れなく行うか、リスクマネジャーは回答者に対してどのような支援ができるか、一部の特殊な性質のリスクについてはどう扱うか、などの論点があります。また、固有リスクと残余リスクという2つの概念の区別も重要なので、説明します。

何に着眼してリスクを洗い出すか

リスクの洗い出しでは、できる限り漏れなく行うことが重要です。そのために、何らかの切り口にしたがって関係するリスクを挙げていくことで、リスクの洗い出しのための発想を促進することが効果的です。リスクマネジャーがこうしてリスクを洗い出した結果は、調査票に添付されるリスク一覧表等に活用されます。

業務別のリスクの洗い出し

業務があるところにリスクがあるとの考えから、各業務ごとに関連するリスクを挙げていくことで網羅的なリスクの洗い出しを図る方法があります。この場合はまず業務の棚卸を行って、自社社員が遂行している業務を把握します。そして、各業務とリスク種類からなるマトリクスを作成して、各セルに該当するリスクを挙げていきます。

この方式の場合は何を参照して業務の洗い出しを行うかが問題になりますが、職務分掌を参照することが近年では広く行われています。業務洗い出しにフローチャートを参照する方式もありますが、実際には必ずしも全ての業務のフローが作成されているわけでないこともあり、職務分掌が用いられることが多くあります。

いずれにせよ、これは個々の部課等の仕事の内容を出発点とするのですから、非常に現場に近いレベルでのリスクの洗い出しに適したアプローチです。

事例　**業務別のリスクの洗い出し**

リスク種類 →

業務	労務	法務	情報システム	・・・・・・・
業務A				
業務B				
業務C				
業務D				
・・・・・・				

ステークホルダー別のリスクの洗い出し

企業には様々なステークホルダーがいます。バリューチェーン上に並ぶ顧客や仕入先を始め、株主や規制当局、更には自社の従業員等もステークホルダーです。

こうしたステークホルダーとの関係に問題が生じ得ることがリスクであるという認識から、ステークホルダーを切り口にしてリスク洗い出し作業を行う方法もあります。

事例　ステークホルダー別のリスクの洗い出し

リスク種類 →

ステークホルダー ↓	労務	法務	情報システム	…….
顧　客				
仕入先				
行　政				
……				
……				

業務・ステークホルダー別のリスクの洗い出し

業務とステークホルダーを両軸にしたマトリクスを作成して、各セルに該当するリスク内容を検討するというアプローチもあります。

アンケート調査票の集計後に挙げられたリスクの網羅性について検討するため、こうしたマトリクスを活用している企業もあります。

事例　業務・ステークホルダー別のリスクの洗い出し

ステークホルダー →

業務 ↓	顧客	仕入先	行政	…….
業務A				
業務B				
業務C				
業務D				
……				

事業目標からのリスクの洗い出し

事業には目標があり、その目標実現の妨げとなり得るものがリスクであるとの考えから、各事業目標に対してリスク種類ごとにどのようなリスクがありうるか整理するアプローチもあります。

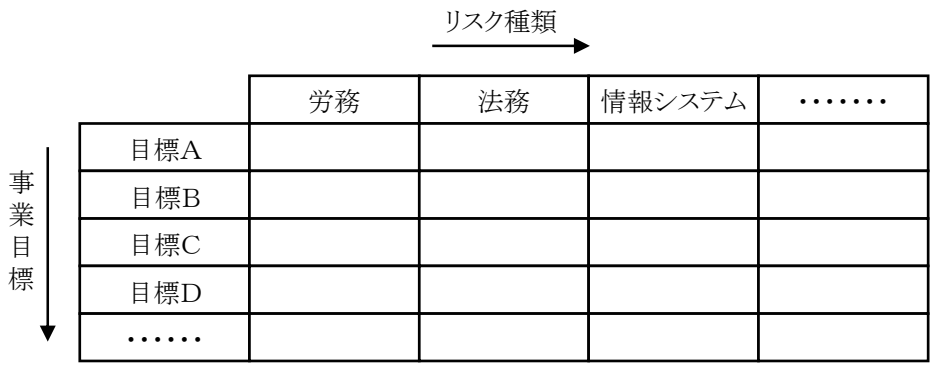
事業の目標との関連がわかるため、事業部として洗い出されたリスクへの対策実施に積極的になるという利点があります。

このアプローチを取る場合は、全社ないし部門の目標が明文化されているか、少なくとも経営トップの明確な意向として確認されている必要があると考えられます。

この方法では期間別の目標のうちで中長期的なものを視野に入れることが有効です。と言うのは、短期的な目標を念頭に洗い出しを行うと、各目標に関係するリスクの範囲も狭くなることが考えられます。その結果、洗い出しに漏れが生じる恐れがあります。

目標実現のためには事業部の当事者には気付きにくい全社のリスク（財務や人事等本社機能に関連するもの）がありますので、全事業部のリスクを集約しただけでは全社のリスクにならないことは注意を要します。

事例 | **事業目標からのリスクの洗い出し**



リスク洗い出しの際は環境変化に考慮を

企業の経営環境は日々変化しています。現時点ではリスクではないか軽微なリスクであっても、将来は重大なリスクになることもあり得ます。したがって将来的な環境要因の動向を考慮して、リスクの洗い出しを行うことが重要です。

参考 | **リスク洗い出し時における環境変化への考慮**

経営環境の変化

✓規制緩和
✓コンプライアンス要求
✓環境問題
✓国際化
✓雇用の流動化

・・・・・・・

これらの動向を考えて、
将来におけるリスクは何か洗い出す

現場でのリスクの洗い出しを支援する

単に調査票を配布しただけでは、必ずしも現場の側でスムーズに記入が進み十分にリスクが洗い出されるとは限りません。事務局として必要に応じて支援策を検討して実行するようにします。

事業リスクマネジメントの先進企業においても制度の導入当初からリスクの洗い出しが自然にスムーズに定着したわけではなくて、事務局側から様々な支援活動を行っています。ここでは、そうした支援施策の幾つかを挙げます

リスクの洗い出し作業に関する事務局による支援の例

◆ 調査票配布前の支援活動例

事前に調査対象者全員を集めて説明会を開催

- こうすることで一度に関係者全員に同じ内容を伝えることができるうえ、会場での質疑応答の内容を全員が共有したことが大きく役に立ちました。

調査票の記入マニュアルだけでなく、Q&A集も開発して全員に配布

◆ 調査票回答中の支援活動例

リスク洗い出し作業担当者一人一人と個別に話をして、作業の方法や意義について疑問点の解消に努めた

人手不足等で作業が滞った部門・部署に対しては、リスクマネジャーが作業の一部を引き取り共同作業として進めることにした

◆ 調査票回収後の支援活動例

調査票の回収後に全部署に対して個別にヒアリングを行い、認識のすり合わせや内容の修正を実施

リスクマネジャーにとって、各部門・部署とのネットワークは仕事の基盤です。
リスク洗い出しの支援活動は基盤構築のチャンスと捉えて積極的な行動を。

洗い出し対象リスクの範囲

リスクは、できる限り漏れなく洗い出すのが原則です。しかしながら、一部の種類のリスクについては、その特性から洗い出し・評価の作業において扱い方に配慮を要するものもあります。

戦略リスクをどう扱うか

企業が重大な投資や企業買収等といった「戦略的」意思決定を適切に行いうるかに関するリスクを戦略リスクと言います。

こうした戦略リスクは意思決定のタイミングで行われる評価とその後のパフォーマンスのモニタリングによって管理されるのが普通であるため、本節で紹介しているようなリスクの定期的な棚卸には馴染みにくい性質のものです。

ただしすべてのリスクを一元的に把握したいというニーズから「○○戦略の失敗」といったリスク名称で洗い出し対象に入れる場合もあります。

損失だけでなく利益もあるリスクをどう扱うか

リスクのなかには、例えば原料の仕入れ値や為替レートに関するリスクのように、損失だけでなく利益をもたらし得るリスクもあります。

リスクマップは軸の一つに「影響度」を取っていますが、これは基本的にどの位の損失を自社にもたらすことがあり得るかという観点で評価されます。そのため、こうした利益もあるリスクについては、リスクマップに載せることが難しくなります。

これについては別途管理してリスクマップの対象外としている企業もありますし、「市場コントロールに失敗して損失を被る限度額」と捉えてマイナス部分だけ評価している企業もあります。

組織体制とリスク洗い出し

ここまで見てきたように、リスクの洗い出しは全社的なリスクマネジメントの一環として組織的に取り組まれるものです。このため、組織構造によってリスク洗い出しのあり方も影響を受けます。

事業部制組織におけるリスク洗い出し

事業部制組織では事業部間で共通のリスクが多いので、リスクの洗い出し作業を「横展開」することがある程度可能です。つまり最初に一箇所で洗い出されたリスク一覧を雛形として他の部署へ配布します。他の部署では、それを叩き台としながら地域による違い等を反映してリスクの追加や削除を行うことで洗い出しをするということです。

最終的に全社のリスク一覧（ないしリスクマップ）を作成する際には、複数の事業部で挙げられた同じリスクをまとめる作業が必要になります。また事業部のリスクだけでは不十分で、職能部門からもリスクを集める必要があります。

職能別組織におけるリスク洗い出し

職能別組織では組織間のリスクの重なりは少なく、基本的に各部門から挙げられたリスクを足し合わせることで全社のリスクとなります。ただし職能の狭間に落ちたリスク（漏れ）がないか、何らかの形で検証することが望まれます。

固有リスクか残余リスクか

リスクというときに、「固有リスク」と「残余リスク」の2つの捉え方があります。

「固有リスク」とは対策を何も講じていない状態でのリスク
「残余リスク」とは対策を講じた後になお存在するリスク

特定のリスク要因について、企業がその時点で講じている対策の効果を考慮に入れるかどうかが両者の違いです。

一般的には「残余リスク」を用いる方が回答しやすい

- 残余リスクは対応策の効果を受けた現時点のリスクの程度を表すので、回答者にとっての実感のリスク程度に近いものになります。
- それに対し固有リスクの場合は、「もし今の施策がなかったらどうなっているのだろう」という推定のための負荷がかかります。また、この推定の部分には回答者の恣意が入る可能性もあります。
- 実務でも現時点での実際のリスク水準を把握することに重点を置く立場で、残余リスクを用いている企業が多く見られます。

「固有リスク」を把握すると多くの情報が得られる

- 幾つかの企業では、まず固有リスクについて評価を求めたうえで、現行の施策の効果を評価して、残余リスクの水準も把握することを回答者に求めています。
- これは施策の効果の定量化を通じ、リスクマネジメントにできるだけ定量的アプローチで臨むという意向のものに行われています。つまり、「固有リスクの水準は10で、今の施策の効果は3だから残余リスクは7である。来期は効果が6となる何らの施策を取り残余リスクの水準を4まで下げよう。」といったアプローチを志向する場合です。
- また、昨年と今年で残余リスクが減少した場合に、それが外部環境が変わったためか（固有リスクの化）、それとも対策が進んだためか（対策実施状況の変化）がわかる等のメリットもあります。
- この方式では、仮定の話になるので上述のように回答者にそれなりの負荷がかかることの認識が必要です。また、固有リスクだけを把握するのは余り意味がなく、現行施策の効果および残余リスクも合わせて把握することが基本です。

調査票ではどちらについて記入を求めているのか明確に

- ある部署は固有リスクを別の部署は残余リスクを念頭に置いて回答したのではデータの価値が損なわれ分析に支障が生じます。どちらについて回答を求めているのか必ず明確にしておくようにします。
- ＜例外＞リスクマネジメントに不慣れな企業で、「固有リスク」と「残余リスク」の概念の説明をすることが却って混乱を招きかねないという配慮から、どちらを用いるとは敢えて言わず、回収されたフォームを見たうえで部門に確認を求めることにした事例もあります。しかし、これはやはり例外的と言えるでしょう。

4.1.3　リスク洗い出しのための調査票をどう開発するか

アンケート法を用いて各部門・部署から現場で認識しているリスクの情報を収集する作業では、調査票をどう作るかが重要です。

良い調査票とは

事業リスクマネジメントの先進企業各社ではリスクの洗い出しがスムーズに行われるように、調査票に関して以下のような点に留意しています。

参考　**良い調査票とは**

良い調査票が備えるべき要件

①調査の重点事項を反映したうえ、回答者が リスクに関して連想しやすい構成になっている

- リスク洗い出しにおいて、重点的に情報収集する内容が盛り込まれるように調査票を設計します。ここでは調査の力点に合わせて構成された調査票の具体例を数件紹介します。
- 回答者がリスクを連想しやすいように、調査票だけでなくて参考としてリスク一覧表を添付することが多くの企業で行われています。またシナリオ法を用いたリスクの連想促進を念頭に構成された調査票の例も紹介します。

②言葉の定義が明確である

- 回答者が迷ったり人によって解釈が違ったりすることを避けるよう調査票上の文言の表現には注意を払う必要があります。

③（特に事業リスクマネジメントの導入初期において）回答者の負担が少ない

- 事業リスクマネジメントの導入初期はできるだけ回答者の負担にならないように、記入事項を選択式にするなどの試みをした企業もあります。
- ただし、この点を過度に意識して情報価値が低下したのでは本末転倒になるので注意が必要です。

調査票紹介

各社では自社のリスク洗い出しに関する方針やニーズを考慮して、自社に適した調査票を開発して活用しています。ここでは、調査票フォームの幾つかを紹介します。

調査票の例(1):リスクに影響する要因の説明を重視

この調査票では、「考えられる増幅要因」「考えられる抑制要因」の欄に大きなスペースを充てています。現在のリスクを考えるだけでなく将来的にリスクがどう変動するかの考察を重視して、この企業ではこうした構成にしました。

事例	リスク影響要因を重視した調査票

＜リスク基本情報＞

リスク名		リスク概要	
リスク分野			

＜リスク評価＞

影響度		発生頻度		総合評価	

考えられる増幅要因
考えられる抑制要因

＜対策＞

管理番号	施策概要	実施状況	責任者	実施期間

調査票の例(2):対策の説明重視、レベル定義とリスク一覧付き

この調査票ではリスクの内容や程度だけでなく、それに対して何をしているか／するべきかに関連して詳しい記載を求めています。現在の対策についての評価欄には、社内で一定の尺度を規程して用いるようにしています。この点は後述する対策実施状況評価の考え方で説明します。更にそうした現状に対して取るべき行動とその時期まで記載を求め、現場としてどう取り組むかまで一貫して記載を求めています。調査票を回収後に事務局で進捗状況を記載できるよう、モニタリングの欄も設けられています。

事例 | **対策の説明を重視した調査票 1/3**

リスク調査票

貴部門に関連するリスクの影響調査を行います。考えられるリスクの事例に基づき、原因、影響度、対策等について記入してください。リスクタイトル名は「リスク一覧表」を参照してください。

リスク名				部門	
リスク種類 (1つに○を)	財務、人命、業務影響、環境、評判			回答者	
発生頻度		影響度		回答日	

リスクの事象	想定されるシナリオと最悪のケース		
損害と影響	影響する部署・機能・範囲や過去の発生データ		
発生要因	発生にいたる内的要因・外的要因		
現在のコントロール	リスク対策の内容	規程の機能状況	評価
今後必要なコントロール	アクション案		スケジュール
モニタリング			

この調査票の記入説明書には、リスクの影響度と発生頻度のレベル定義が含まれています。こうした定義を行うことで、回答者の解釈による不統一をできるだけ回避するようにします。

事例 | **対策の説明を重視した調査票 2/3 影響度と発生頻度のレベル定義**

調査票の記入について

影響度のレベル定義

レベル	定義	影響の出る分野				
		財務	人命	業務影響	環境	評判
1	軽微な影響	100万円以内	応急処置で対応可能	無視できる程度の影響	ごく短期間の汚染	日常の管理で解決する
2	やや軽い影響	～1億円	医師の手当てが必要な障害	特定のプロジェクトのみ／1日程度	軽い汚染	1媒体に記事が出る
3	中程度	～5億円	入院が必要な傷害	数週間の影響	中程度	マスコミに小さく取り上げられる
4	大きな影響	～15億円	1名の死亡／複数名の障害	1ヶ月程度の影響	重篤な害	中程度の範囲で取り上げられる
5	甚大な被害	15億円以上	複数名の死亡	1ヶ月以上の影響	長期に渡る害	マスコミで大々的に騒がれる

発生頻度のレベル定義

レベル	定義レベル	頻度の状況
1	ごくまれに発生	余程例外的な状況でないと発生しない
2	発生しにくい	数年に1回程度発生
3	中程度	1年に1回は発生
4	たびたび発生	年に複数回発生
5	日常的に発生	月に複数回発生

この調査票の記入説明書には、更に付随資料として部署別サンプルリスク一覧があります。回答者はこの一覧を参照することで、リスクの洗い出しが促進されるようになっています。

事例　対策の説明を重視した調査票 3/3　サンプルリスク一覧

部署別サンプルリスク一覧表

部署	リスク内容
総務	株主総会、文書管理、 備品管理、緊急時対応
経営企画	経営戦略、新規事業、企業イメージ、 事業所展開、業務提携
法務	知的所有権、製造物責任、独占禁止法、 環境汚染、インサイダー取引
人事・労務	雇用・昇進差別、セクシャルハラスメント、 労働争議、労働災害、海外駐在員の安全
財務・経理	為替変動、金利変動、敵対的買収、 債権回収、決算書作成、納税申告
製造	設備事故、品質低下、リサイクル、 製造ライン停止、汚染物質流出
営業	競合商品、不買運動、 顧客ニーズの変化、在庫切れ
情報システム	情報漏洩、不正アクセス、 システムダウン、ウイルス進入
研究開発	商品開発失敗、特許戦略、 開発競争、不良製品開発

調査票の例(3):固有リスクも評価

この調査票ではリスクの影響度と発生頻度については固有リスクで評価することを求めています。そのうえで、対策について説明・評価を行い、結果としての残余リスクの水準を評価する形式になっています。

なおこの調査票は先に見た2票と違って、一枚の調査票にその部署部門が抱える複数のリスクについて一覧形式で概要を記述する形式になっています。この企業では、本票に挙げられたリスクのうち回答者が特に重要と考えるものについてより詳細に記述するための別票を用意しています。(右端に「別表有無」を記載する欄があります。)

事例 | **固有リスクについても評価を求める調査票**

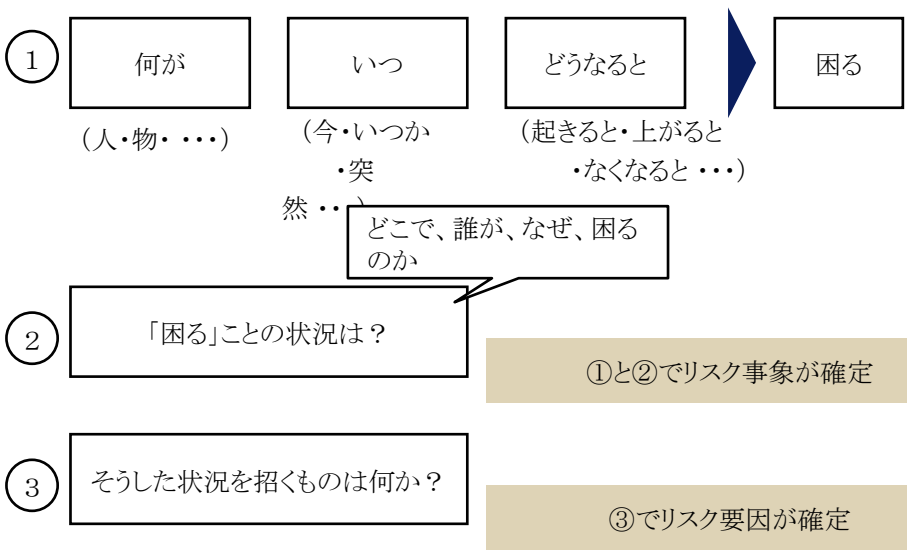
	リスク分野	リスク概要	固有リスク評価			担当者	対策	対策評価	残余リスク評価	別表有無
			影響度	発生頻度	リスク度					
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										

調査票の例(4):シナリオ法によるリスク洗い出しの促進

シナリオ法では、何らかの状況下で何が起きるかそしてその状況を引き起こすものは何かなど、仮想の状況についての考察を手掛かりにしてリスク洗い出しを行います。
回答者がこのシナリオ法の思考を活用してリスク洗い出しを促進できるように、調査票を設計した企業もあります。

事例 | **シナリオ法の考え方を活用した調査票**

シナリオ法の考え方



リスクの例

XX主任に急に退社されると困る。担当の業務はXX主任の知識・経験に依存しており、当人がいなくなると顧客満足度が大幅に低下して幾つかの得意先を失うことがありうる。知識共有や後継者育成をしてこなかったうえ、当人が満足できる処遇をしてきたかも疑問

日経平均株価が1年以内にXX,XXX円を下回ると困る。 ・・・・・・・・

調査票

	「人・物・金・情報」	「～する／している」と	リスク分野	リスク事象	リスク要因	リスク評価		今後の対策
						影響度	発生頻度	
1	が XX主任が	急に退社されると	人事・労務	XX主任がいないと顧客満足度が大幅に低下して、幾つかの得意先を失うことがありうる	担当業務はXX主任の知識・経験に依存しているのに、知識共有や後継育成をしてこなかったうえ、当人が満足できる処遇をしてきたかも疑問			
2	日経平均株価が	1年以内にXX,XXX円を下回ると	財務	・・・・・・・	・・・・・・・			
3								

言葉の定義は明確に

社内には様々な経歴や価値観の人々が集まっているうえに、アンケート調査票は各種の職能・事業の担当者が回答することになります。そのため、人によって異なった受け取り方をする可能性があることは念頭に置く必要があります。

同じ調査票を使っても個々の回答者が異なった意味に解釈して回答したのでは回収データの有効性が損なわれます。それどころか、確認のために膨大な追加作業が発生して収拾がつかなくなったり、甚だしい場合にはリスクマネジャーが信頼を失って全社リスクマネジメントが推進不可能になるといった事態にすら陥りかねません。

回答者による「解釈の違い」は禁物。言葉の定義を明確に。

定義の必要性

誤解を避けるため、調査票に記載される言葉の定義は明確にする必要があります。

特にリスクの発生頻度・影響度の算定欄については、そのレベルの定義は厳密に行い、回答者の解釈による相違が生じないようにする必要があります。先述の調査票事例のひとつにあったレベル定義の例などを参照してください。

ある企業では、自社の社風として定義はできるだけ公式に定めておかないと議論が進み難いという事情も考え、調査票作成時には主要な言葉の定義を念入りに行っています。同社での具体的な定義例の一部として、下記のようなものがありました。なお、この企業ではこうした行いを「議論のための土壌づくり」と呼んでいます。

事例　リスクマネジメントのための言葉の定義の例

品質リスク	品質事故による社会的信用や市場の占有率の低下、経営コストロスを招くリスク
品質事故	社内の次工程の品質管理業務への悪影響、不適合品、取引先・消費者苦情等の発生事実
不適合品	規格・基準に逸脱した原材料・仕掛品・半製品・製品・商品
社内外区分	（商法上の線引きでなく）「出荷コントロールが可能な配送パートナーまでが社内

「リスク」の定義

「リスク」という言葉自体も人によって違う用いられ方をされることがありますので、意味を明確にしておく必要があります。自社では既にリスクの意味を定義・発表されているという場合でも、改めてその定義を調査票に書いておくことが望まれます。

ある企業では「リスクとは事業継続を損なう恐れのある事項」のことと定義しました。同社はこうすることにより、事業目的達成のために本質的な内容のリスクが中心に洗い出され、そうではない細かいリスクが排除されることを狙いました。

「リスク」を定義することにより、洗い出しのフィルターにすることも可能です

事業リスクマネジメント導入初年度の調査票

リスクマネジメントの導入初年度で初めてリスク洗い出しを行う際には、回答者の負担を意識して通常と異なる調査票を設計した企業の事例があります。

事務局が洗い出したリストを載せた調査票の例

ある企業では、事業リスクマネジメントの導入初年度にリスクマネジャーが自ら各部門のリスクを洗い出して、それを記載済みの調査票を部門部署に配りました。

回答者は既にリスクが挙げられている下記のような調査票を受け取り、発生頻度と影響度の評価欄に○を付けていくことになります。

事例　リスクは記載済で回答者は評点をする調査票

リスク	発生頻度					影響度				
取引先倒産	1	2	3	4	5	1	2	3	4	5
金利変動	1	2	3	4	5	1	2	3	4	5
為替変動	1	2	3	4	5	1	2	3	4	5
・・・・・・・	1	2	3	4	5	1	2	3	4	5

- しかし、かなりの小規模企業でない限りリスクマネジャーが現場の業務を全て把握しているということは不可能なので、こうした場合でも調査票には「その他のリスク」として自由記入欄を設けておくようにします。
- 漏れなくリスクを洗い出すという目的からは、社内の大多数が気付いていないリスクで、それがたった1人によって指摘されたものであっても、判断根拠を吟味して妥当な内容なら重要リスクとして取り上げることが必要です。したがって、こうした現場での発想の場を残しておくことは重要です。
- この逆に事業リスクマネジメント導入の初年度でも、アンケート調査票にリスク一覧の添付を行わなかった企業もあります。この企業では、現場でなければ把握できないリスクが漏れることのないように、現場の発意を重視するという考え方から、たとえ回答や事後調整に負荷はかかってもリスクの例示は行わないという方針で臨みました。
- このように、自社のニーズや条件を考えて調査票を設計することが重要です。

リスク評価を行わずリスク項目のみ挙げる純粋な「洗い出し」調査票の例

やはり事業リスクマネジメント導入の初年度における配慮の事例ですが、調査票では部門部署が直面しているリスクを挙げるのみにとどめて、それらの発生頻度や影響度についての記入は求めないことにした企業もあります。この場合は各部門部署から一度集めたリスク項目を事務局が整理して、再度評価のために各部門部署へ配布するという二段階の手続になります。

この企業では不慣れな回答者が初回には適切にリスクを洗い出せない可能性があるため、そのままリスクの評価をして無駄な作業を発生させないよう一旦事務局が整理することにしました。事務局の整理としては、リスクとは言えないものや重複の排除、事務局から見て漏れていると思われるリスクの追加、リスクに適切な名前をつける、等がありました。

4.1.4　リスクの評価時には何に留意するべきか

リスクの評価については、影響度と発生可能性をいかなる指標で評価するか、そのうち定量指標によるものはどのように行うか、また各リスクに対する対策実施状況をどう評価するかといった論点があります。

更に評価をめぐるワークショップを開催する場合はどのように進めるか、そして最終的に自社で優先的に取り組むリスクをどのように選定するかといった内容について、ここでは論じます。

リスク評価指標を決定する

リスクを評価しリスクマップ上に配置するために、影響度と発生可能性の基準を決定する必要があります。

影響度の基準を決定する

影響度の把握のための主要なアプローチとして、以下のようなものがあります。

金銭的損失の大きさにより影響度を把握する

- 金銭的損失に換算した場合、どの程度のインパクトがあるかという視点に基づいてレベル分けします。
- 具体的金額設定の目安として、経常利益から算出している企業が見られます。例えば、過去3年間の平均経常利益の10%を最大レベルに設定するなどです。

非金銭面（回収、人命、企業イメージ、業務停止など）により影響度を把握する

- 金額ではなく、定性的な影響度からレベル分けする方法もあります。
- 回収の範囲であれば【全面回収、小売・店頭単位回収、在庫回収、出荷停止、個別対応】などのレベル分けが考えられます。

金銭的・非金銭的影響を組み合わせて影響度を把握する

- 金額と定性的な影響度を組み合わせて評価レベルを設定します。
- この場合、金額に換算できる場合と必ずしも金額には換算できない場合の両方の場合を加味しながらリスク評価が実施できます。

発生可能性の基準を決定する

発生頻度の単位を設定する

- 30年に一度、毎年一度、月一度、週一度、日常レベルなどの設定が考えられます。

業界固有のサイクルで決定する

- 業界によって事業サイクルには違いがあります。例えば小売業界のサイクルは短い（主に週・月単位）のに対して、造船業界等のサイクルは長い（月・年単位）等の違いがあります。
- 業界のサイクルを考慮して、発生可能性のレベル分けを行う必要があります。

リスクを定量的に評価する

リスクの評価時には、評価を定量的に行うか定性的に行うかに関しての判断が必要になります。実際の企業の対処状況としては、「すべてのリスクを定量的に評価」、「すべてのリスクを定性的に評価」、「定量的なリスクと定性的なリスクを分類して評価」の場合に分かれます。それぞれの立場の企業の意見を紹介します。

◆ すべてのリスクを定量的に評価するという意見

すべてのリスクを定量的に評価しないと評価の公平性が保たれない

定量化することでリスク評価が明確になり、リスク管理が容易になる

◆ すべてのリスクを定性的に評価するという意見

厳密な評価にこだわり時間をかけるよりも、リスク評価プロセスの負荷を軽減することで対策策定により多くの時間を割くことがより実質的なリスクマネジメントにつながる

数値による定量評価が求められる市場リスクや信用リスクは当社においては重大なリスクではなかったため、定量測定よりもコンセンサスに拠る評価を行った

リスクマネジメントの厳密な費用対効果を算定しないことにしたので、定量化に必ずしもこだわる必要はない

◆ 定量的なリスクと定性的なリスクを分類して評価するという意見

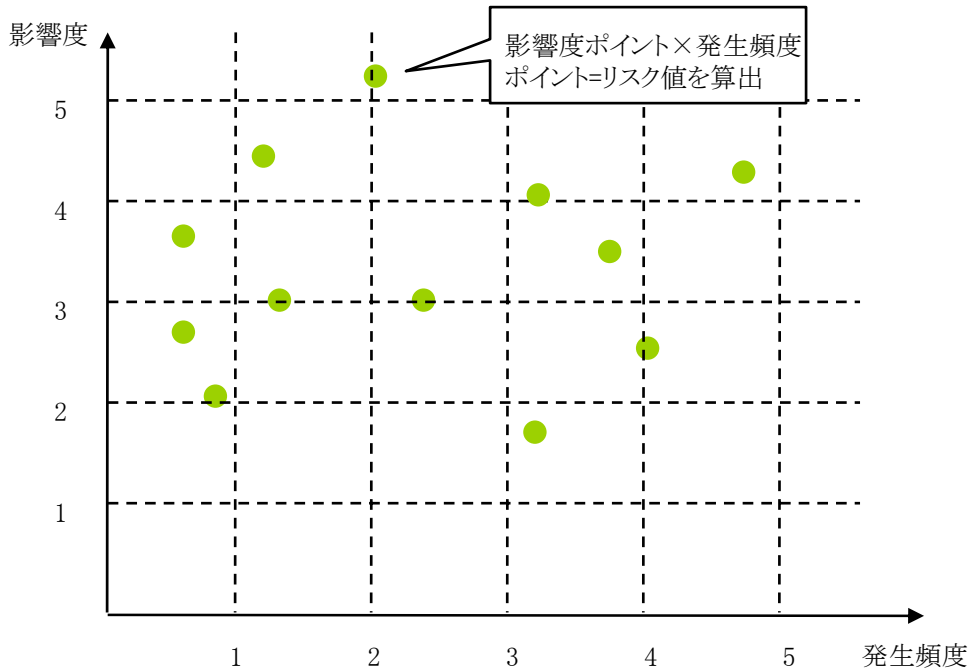
リスクのすべてを定量化することは不可能だが、より厳密な評価が必要とされるリスクは定量化し、その他の定量化が困難なリスクは定性的に評価する

- 原則としてはすべてのリスクを定量化することが望ましく、そうでない事例としてここで紹介しているのは定量化が難しいものの扱いに関する議論であることに注意してください。
- 市場リスクなどは定量化手法も普及しており通常は評価数値に基づいた意思決定が行われることからも、基本的には定量的評価を行うべきと考えられます。ただし、この領域のリスクが自社の事業内容とそれ程密接な関係にない場合には、必ずしも労力を費やして定量化する必要は無い場合もあります。
- 定量化可能なリスクと厳密な定量化が困難なリスクをはっきりと分類し、そのリスクの性質に沿った評価方法を取ることが現実のリスクの性質を考慮した評価方法であると考えられます。
- リスクを定性的に評価するとしている企業でも自社の事情や優先順位からそうしているのであり、リスクの定量評価が無意味であると言っているわけではありません。

◆ リスクの大きさをポイントに換算する

全てのリスクの一律な定量化が困難であることを前提として、ポイントという概念を用い全てのリスクについてリスク値を算出している企業がありました。

事例	リスクのポイント換算



【ポイント化計算の例】
損害額30億円以上なら ⇒ 影響度「5」 ⇒ 40ポイント

影響度・発生頻度について1～5の段階で区分けしてポイント化する

影響度ポイント×発生頻度ポイントからリスク値を算出する

全てのリスクをポイント化して合計値を計算して、次年度リスクマップ作成時には総評価数の減少度合いを検証する

対策実施状況を評価してリスクマップに表示する

リスクについて、その影響度や発生頻度だけでなく、自社ではいかなる対策を実施しているかについての検討も重要です。

対策実施状況を評価する

リスクに対する取組み状況の評価には、企業内で一定の尺度を持って測定することが必要です。ここでは成熟度モデル（マチュリティ・モデル）として経営管理の様々な分野で活用されている考え方をリスクマネジメントに応用した事例を紹介します。

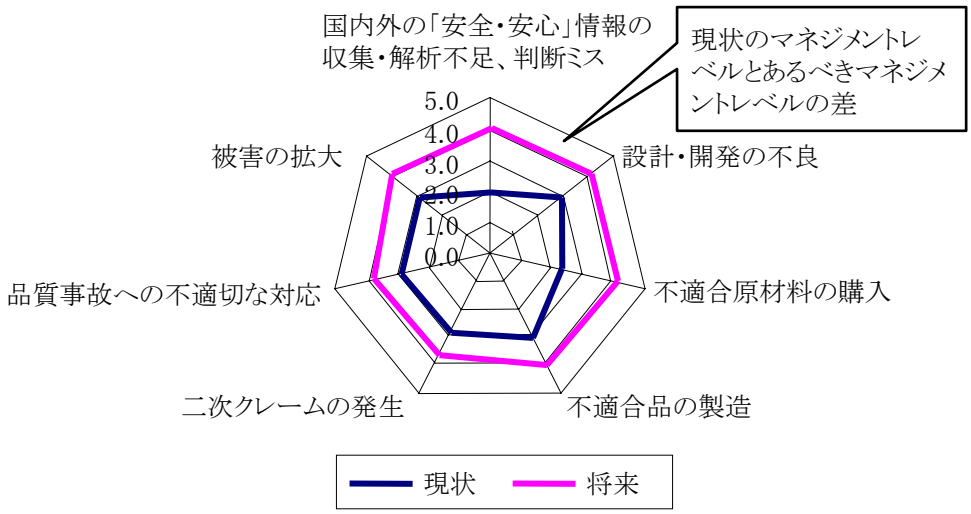
事例 | **成熟度モデルによる対策状況の評価1/2**

マネジメントレベル		マネジメント要素*					
		ビジネス戦略と方針	ビジネス・プロセスとリスクマネジメントプロセス	人	経営報告書	方法論	システムとデータ
		リスクマネジメント能力を用いて達成すべき目標の設定	リスク戦略を達成するためのプロセスの構築	プロセスを実行するための人員の配置	リスクマネジメント報告	リスクマネジメント方法の確立	リスクマネジメントデータの収集・加工
5	最適化	リスク戦略が策定され、リターンにあったリスクをとるための分析を行い意思決定する仕組みがある。					
4	マネジメント	リスクの測定方法と分析方法が確立され、リスクが定量的に測定されており、全社で包括的に管理されている。					
3	定義・制度化	リスクマネジメント方針・プロセス・基準が全社的に標準化されている。					
2	連続・反復	リスクマネジメント担当者が専任・配置され、リスクマネジメントが実施されているが、担当者の能力に大きく依存している。					
1	初期段階	リスクマネジメントの責任・業務が不明確であり、その活動は属人的で場当たり的である。					

- 社内のマネジメント要素がリスクマネジメントのレベルとしてどの段階にあるかを5段階評価で示しています。ただし、社内のマネジメント要素は各社で若干異なることが想定されます。
- この企業では従来は「初期段階」に示されているように属人的で現場任せのリスクマネジメントが実施されており、それが次第に全社的なリスクマネジメントに発展する途上にあります。最終的にはマイナスの意味のリスクだけでなく、プラスの意味のリスクをも想定したリスクマネジメントが実現されるレベルまで到達するというのが理想として、リスクのレベル分けを行っています。
- この基準をもとに重大なリスクに対するリスクマネジメントのレベルを5段階で評価して、次頁に示すデータチャートを使って分析しています。

事例の企業では、各リスクに対する対策実施状況について現在の水準と将来のあるべき水準を一覧できるチャートを開発してリスクマネジメントに役立てています。

事例　成熟度モデルによる対策状況の評価2/2



- この企業では社内の重大なリスクを集め、マネジメントレベルの評価軸に沿って5段階で評価し、上図のようなチャートに落とします。現在の評価ポイントと将来のあるべき評価ポイントを記載し、その差異を明確にしています。
- このような分析を実施することで、重大なリスクがどの程度のレベルでマネジメントされているかということと、あるべきマネジメントレベルとの間にどの程度の差異が生じているかを明確化できます。
- 現状のリスクマネジメントレベルとあるべきリスクマネジメントレベルの差異が大きいほど、対策の策定が急がれると考えられます。従ってこの分析によって取組みの優先順位をつけることも可能になるのです。

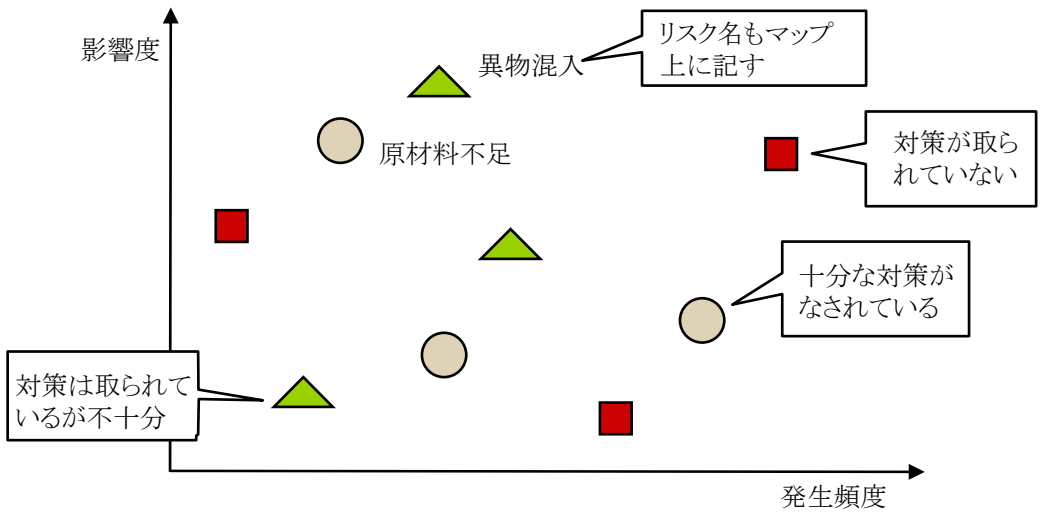
対策実施状況をリスクマップに表示する

対応実施状況をリスクマップでどう表示するかについて、幾つかの事例を紹介します。

リスクマップ上に対策実施状況も表す

- ある企業ではリスクマップ上の各リスクについて対策実施状況を記号で表示することで、当該リスク発生頻度・影響度だけでなく対策の実施程度も把握できるようにしています。

事例　対策実施状況も示したリスクマップ



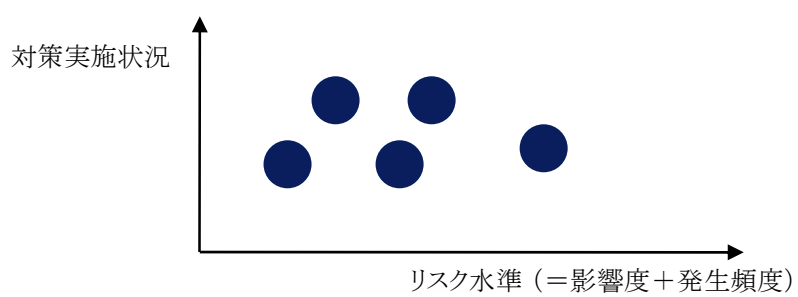
残余リスクのみでリスク評価をまず実施して、その中から重大なリスクを決定のうえ重大リスクについてのみ対策実施状況を評価する

- まず残余リスクで影響度・発生頻度の評価を行い、その中から重大なリスクを決定します。決定された重大なリスクについてのみ対策実施状況を評価します。
- リスクマップ上に表される全てのリスクの対策実施状況を必ずしも確認する必要が無く、重大リスクに関してのみ対策程度を詳細に把握するという場合はこうした方法もあります。

「影響度＋発生頻度」を算出して対策実施状況とのマップを作成する

- ある企業では「影響度＋発生頻度」の軸に用いることで、対策実施状況との一覧ができるマップを作成しています。

事例　対策実施状況を軸に取ったリスクマップ



リスク評価ワークショップを実施する

リスクを洗い出して個別リスクの影響度や発生頻度に関して何らかの観点から評価を行ったとしても、リスクマップ上で各リスクの位置関係はどうあるべきかについては、関係者の認識を反映させて最終化を行うことで社内のコンセンサスを得やすくなります。個別の担当者に意見を確認しても良いですが、そうした意見調整の場としてリスク評価ワークショップを開催することも有効です。

基本的には評価対象組織のリスクを決定する際に、リスクマップを主要なツールとしてワークショップを実施します。ワークショップ参加者がその場でリスクの洗い出しから始めるケースもありますが、一旦アンケート等で洗い出したリスクを基にリスクマップを仮作成しておいて、それに対する検討からワークショップを始める方がスムーズな進行が望めます。

ワークショップの参加者

参加人数は5～10人程度とする

- 参加人数が多すぎるとコンセンサスを取ることに時間がかかり、その煩雑さから以降の実施に対する積極性が失われる可能性もあります。
- 少ない人数で意思決定を行うことによる危険はありますが、人数が多過ぎても意思決定が難しくなると考えられます。人数と参加メンバーには十分な配慮が必要です。

議論を促すファシリテーターを決めておく

- リスクマップを取りまとめる立場no事務局やリスク推進部門から、ファシリテーターを用意します。
- ファシリテーターが各参加者に意見を促して取りまとめることで、ワークショップの運営をスムーズにします。

評価対象リスクに関わる部門・部署の責任者に参画を求める

- 評価対象リスクの洗い出し・評価を行った部門や部署の責任者が出席することにより、ワークショップ参加者は当該部門・部署内での意思決定過程を知ることができます。従って、そうした事情を踏まえてリスクの評価に関する社内の意見調整ができるようになります。
- また、各部門・部署の責任者が出席することにより、最終的な意見調整に対する各部門・部署の意思決定がその場で可能になります。

全社リスク評価のワークショップには、可能であれば経営トップにも参画を依頼する

- こうしたワークショップには、経営トップまたはそれに近い立場の人にも出席してもらうことが望まれます。
- 部門や部署の責任者の意見だけでなく経営トップの意見を踏まえることで、より全社的視点に立った評価が可能になります。
- 経営トップの参画が難しい場合は、例えば経営企画室等、日頃経営に近い視点で業務を行っている部署のメンバーが参加するとより有意義な議論ができるようになります。

ワークショップの実施方法について

ワークショップでの意思決定をどう行うか

- ワークショップの運営として、ある企業では関係部門・部署の担当者が会議室にこもり「ざっくばらん」な議論を丸一日行って検討することを通して、意思決定をしています。別の企業では、投票等による数値化された評点によって決定しています。
- 意思決定の方式については、組織風土やワークショップをめぐる状況などを検討して、自社に適すると考えられるものを採用する必要があります。

個別のリスクに対する認識の相違を埋めるためリスクの定義を行う

- ワークショップの場で議論が正確に行われるためには、討議の対象となるリスクの意味について各参加者が共通の認識をしていることが必要です。
- 各部門・部署で洗い出されたリスクが集められて討議資料に載っている場合、書かれている言葉は違っても内実は同じという可能性もありますし、同じ呼び方をされているリスクでも出席者間で認識が食い違っている可能性もあります。
- リスクマップに表されたリスクに対する認識が出席者によって異なっていることによる議論の紛糾を恐れて、個別リスクの定義を行ったという企業もあります。
- リスクマネジャーはリスク定義のリストを事前に作成しておき、必要ならばワークショップの場で定義の修正も行うようにします。

全社で優先的に対応すべき重大なリスクを選定する

リスクの洗い出しと評価を行ってリスクマップを作成した後に、自社で優先的に取り組むリスクを選定するようにします。事業リスクマネジメントを行う主要な意義の一つは、自社の経営にとって真に重要なリスクを見極め注力した取組みができるようになることです。一方、どれほど詳細な分析をしたリスクであっても、ここでの判断次第では全社的な取組みの対象とならないこともありえます。ですから、この選定をどのように行うかは非常に重要です。

全社で優先的に対応すべきリスクとして、多くの企業では10個前後のリスクを選定して対策を講じています。

優先的対応リスクの選定基準

影響度・発生頻度の大きいリスク

- 一般的にリスクマップ上で右上に位置するリスク、即ち発生頻度が高いうえに企業に及ぼす影響も大きいリスクは優先的に取り組む対象のリスクとして第一候補となります。影響が大きなリスクが始終発現しては、企業の存続すら脅かされ経営が立ち行きません。

対策度が低いリスク

- 自社の現行リスクマネジメントで対策が十分でないリスクも、ここでの選定候補となります。
- 対策が十分でないということは、部門や部署で行われている個別のリスクマネジメントでリスクを十分に低減出来ていない場合だけでなく、各部門や部署で対応はしていても企業全体で見ると断片的な対策になっている場合も考えられます。

社内の複数の組織に関連するリスク

- 社内で部門横断的な対応を必要とするリスクであるかどうかは、全社的対応をすべき重大リスクの選定での重要な観点です。企業活動においては様々な部門や部署が関与しています。このことは製品や原材料が社内の部門間で受け渡されるときには多くの場合に前工程でのリスクも同時に受け渡されているとも言え、前工程・後工程どちらかだけでは完全な対応は不可能です。このようなリスクは、全社で対応すべきリスクとして選定する必要性が高いです。

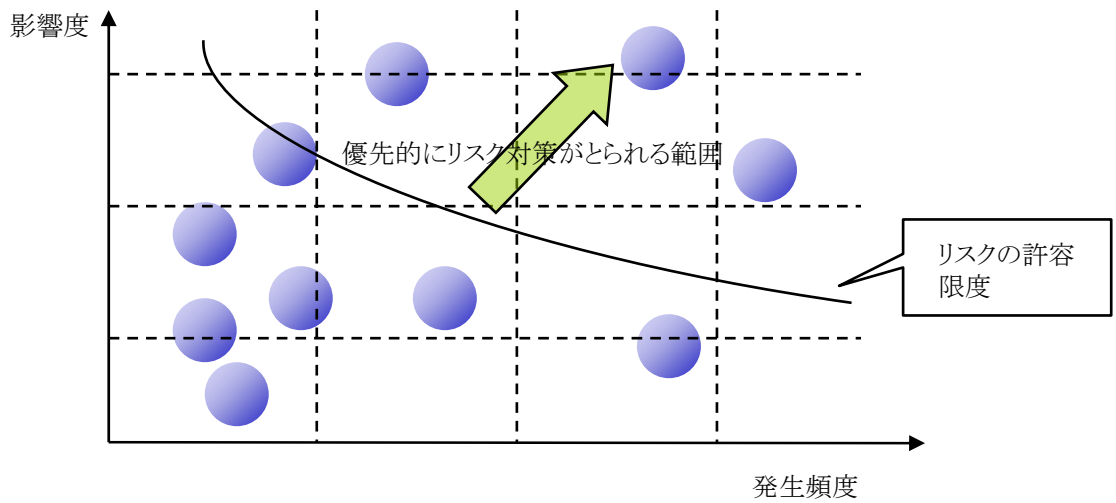
社会的関心事となっており危機感が増大しているリスク、今後社内でも発現の危険度が増大することが見込まれるリスク

- 他社の不祥事などによって当該リスクに対する社会的関心が高まり、社内でも当該リスクの発現に対して危機感が増している場合には、当該リスクを重大なリスクと選定して全社的対応を取るようにします。
- 当該リスクが社内でどのように管理され対策が講じられているのか、その責任者は誰かということを全社で明確化して十分な対応策を取るようにします。

リスクの許容限度を特定する

COSOERMではリスクマネジメント方針策定時にリスクマップ上の許容限度を特定することを示しています。リスクマネジメント方針策定の際には社にとって重大なリスクを決定するのと同時に、リスクマップ上で全社で対応すべき範囲と許容できる範囲を決定しておくことが良いでしょう。

参考 リスクの許容範囲の図示



- 影響度と発生頻度の軸を決定し、リスク値（この企業では、リスクの発生確率×リスクの影響度として算出）で許容限度を決定します。このリスクマップ上では、曲線より上部が発生頻度が高く影響度も高い許容できない範囲と決定されており、優先的にリスク対策が取られるリスクになります。
- またこうした基準を設定することで、洗い出された膨大なリスクから絞り込みを行う一助ともなります。

コラム

リスクマップはコミュニケーションのツール

これまで見てきたように、リスクマップは数多くの調査票の回答の分析や関係者との討議といった作業を経てまとめられます。このため、リスクマップの完成時には「労作」として満足感を抱くのは良いのですが、そこでリスク対応に関する作業を終わりにしてはいけません。

リスクマップは社内に存在する数多くの様々な種類・性格のリスクを一枚の図にまとめたその名の通り「マップ」です。リスクマップを作成することよりも、リスクマップを使っていかなる行動を取るかの方が重要です。

リスクマップは自社における主要なリスクの分布状況に関するその時点での評価結果を共有するためのコミュニケーションのツールと考えるべきものです。リスクマップに対応策の答えが書いてあるわけではありません。社員はリスクマップを見ながら、

- 対策を打つべきリスクの範囲
- リスクに対する対応方針
- 今後各リスクのマップ上の位置はどう動く／動かすべきか

といった事項に関する問題意識を抱き、より効果的なリスクマネジメントを実践することが大切なのです。

4.2 リスク戦略、リスクマネジメントの目標、リスク対策の選択

ここでは企業が対策を講じると決定したリスクをどのようにマネジメントしていくのかについて説明していきます。
具体的には、
- 企業はどのようなリスク戦略を採るのか
- どのようなリスクマネジメントの目標を設定するのか
- どのように実施すべき対策を選択するのか
- どのようにリスクマネジメントプログラムを策定するのか
- 対策を講じないと決定したリスクはどのように対応するのか

ということについて説明していきます。

4.2.1 リスク戦略

企業は対策に取り組むリスクを選定した後、選定された個々のリスクについてリスク戦略を検討する必要があります。リスク戦略とは選定された個々のリスクについて現在の状況（発生確率、影響額等）を分析し、その結果を踏まえて当該リスクに対してとるべき戦略を決定することです。

リスク戦略の種類

企業がとるべきリスク戦略には、「リスク低減」、「リスク回避」、「リスク移転」、「リスク保有」があります。

「リスク低減とは「特定のリスクに関する確からしさもしくは発生確率、好ましくない結果又はその両者を低減する行為です*。」
すなわち、リスクの発生頻度を低減させる「リスクの予防・防止」、影響度を低減する「リスクの軽減」の観点からリスクをコントロールするものです。
リスク低減はリスク戦略の中で最も多く採用される戦略で、企業が自ら積極的にリスクを低減させる戦略です。

「リスク回避とは、リスクのある状況に巻き込まれないようにする意思決定又はリスクのある状況から撤退する行動です*。」
つまり、リスクを伴う業務をすべて中止するということです。リスク回避戦略により、リスクはゼロとなります。リスクをゼロにすることは究極的なリスク戦略ですが、同時に得られるリターンもゼロになる点に注意が必要です。企業が営利を目的として設立されている以上、リスクを回避することで営利活動を阻害してしまう恐れがあります。

「リスク移転とは、特定のリスクに関する損失の負担を他者と分担することです*。」
リスク移転は保険や契約によって行われる場合が多いようです。例えば、リスクの顕在化により被ることが予想される損害額を算出し、その金額と同等の保険をかけるという対応は、保険会社へのリスク移転を意味します。

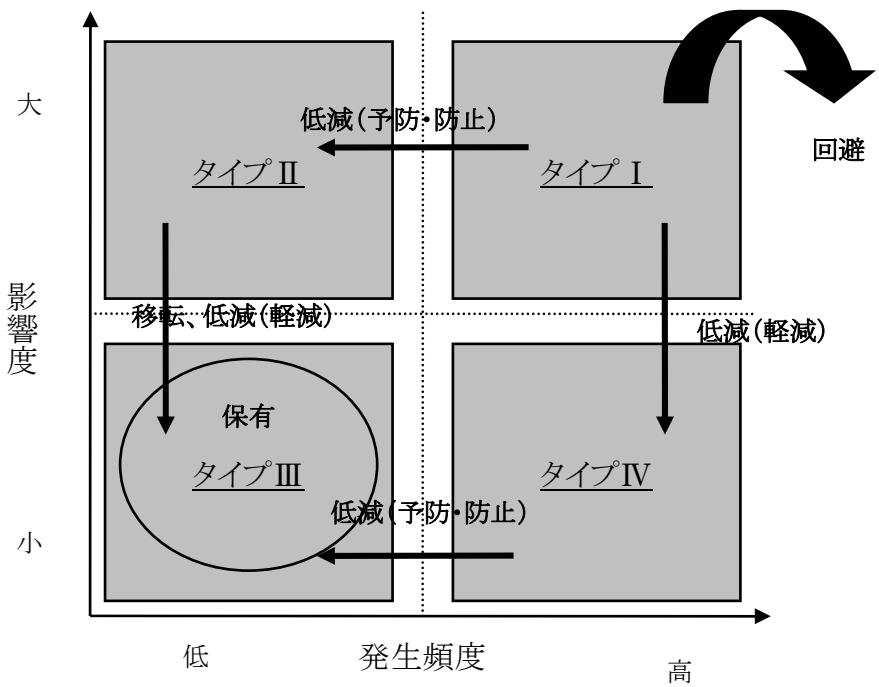
「リスク保有とは、特定のリスクに関する損失の負担の享受です*。」

ここで注意したいのは、リスクを享受することもリスク戦略となることです。つまり、リスクの発生頻度が低く、影響度が小さなリスクについては、何がなんでもリスク対策を講じる必要はないということです。そのようなリスクについては、あらかじめリスクを保有することを宣言し、無駄なコストは発生させないことが費用対効果の観点からも有用となります。

*『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年 より引用

リスク戦略の基本的パターンは

個々のリスクに対してのどのようなリスク戦略を採用するかについて決まったルールは存在しません。企業の状況やリスクの性質を把握し、企業に適合したリスク戦略を選択する必要があります。ただし、リスクマップ上にプロットされる位置によって、一般的に選択されるリスク戦略は下図のように整理できます。



タイプⅠのリスク戦略

タイプⅠの領域にあるリスクは、影響度が大きく発生頻度が高いリスクです。この領域では、影響度を小さくするリスク低減（軽減）、発生頻度を小さくするリスク低減（予防・防止）ことが考えられます。しかし、特に影響額が大きいものについてはリスク回避が考えられます。

タイプⅡのリスク戦略

タイプⅡの領域にあるリスクは、影響度が大きく発生頻度の低いリスクです。この領域ではリスク移転により影響度を小さくすることが考えられます。リスク移転を選択しない場合には、影響度を小さくするリスク低減（軽減）が考えられます。

タイプⅢのリスク戦略

タイプⅢの領域にあるリスクは、影響度が小さく発生頻度の低いリスクです。この領域ではリスクを享受するリスク保有が考えられます。

タイプⅣのリスク戦略

タイプⅣの領域にあるリスクは、影響度が小さく発生頻度が高いリスクです。この領域では発生頻度を低くするリスク低減（予防・防止）が考えられます。

コラム

ある企業の事例

ここまでの説明を通し、個々のリスクに対するリスク戦略検討の必要性を述べてきました。

ある消費財製造業では、「リスクは自分で負って保険をかけない」というリスク戦略をリスクマネジメント方針の中に掲げています。その趣旨は資金は保険会社へ払うのではなく、安全や損失防止のために払うものであるというものです。

また、欧米企業でも全社的なリスク戦略をリスクマネジメント方針として掲げ、リスクマップ上の位置によってシステマティックにリスク戦略を決定するような事例がありました。

いずれの事例も長年リスクマネジメントへ取り組んでいる企業のものであります。全社的なリスク戦略をリスクマネジメント方針として掲げることは、これからリスクマネジメントに取り組もうとする企業にとっては難しいことですが、継続的にリスクマネジメントに取り組むことにより、ノウハウが蓄積され、自社のリスクをより理解した後には、この例のように自社に最適なリスク戦略をリスクマネジメント方針として昇華させることも可能になるでしょう。

4.2.2　リスクマネジメントの目標設定

企業は保有しているリスクについてどのようにマネジメントしていくかというリスクマネジメントの目標を個々のリスクごとに設定していきます。

『JISQ2001 リスクマネジメントシステム構築のための指針』では、「リスクマネジメントの目標とはリスクマネジメント基本目的を達成するために設定される詳細なリスクマネジメントパフォーマンスの要求事項」と定義されています。

また、「リスクマネジメントパフォーマンスとは、リスクマネジメント基本目的及びリスクマネジメントの目標に基づいて、組織が行うリスクマネジメントに関する測定可能な結果」と定義されています。

すなわち、リスクマネジメントの目標には

① リスクマネジメント基本目的を達成するために設定されるもの

② 組織が行うリスクマネジメントに関する測定可能な結果の要求事項の詳細

という特徴があります。

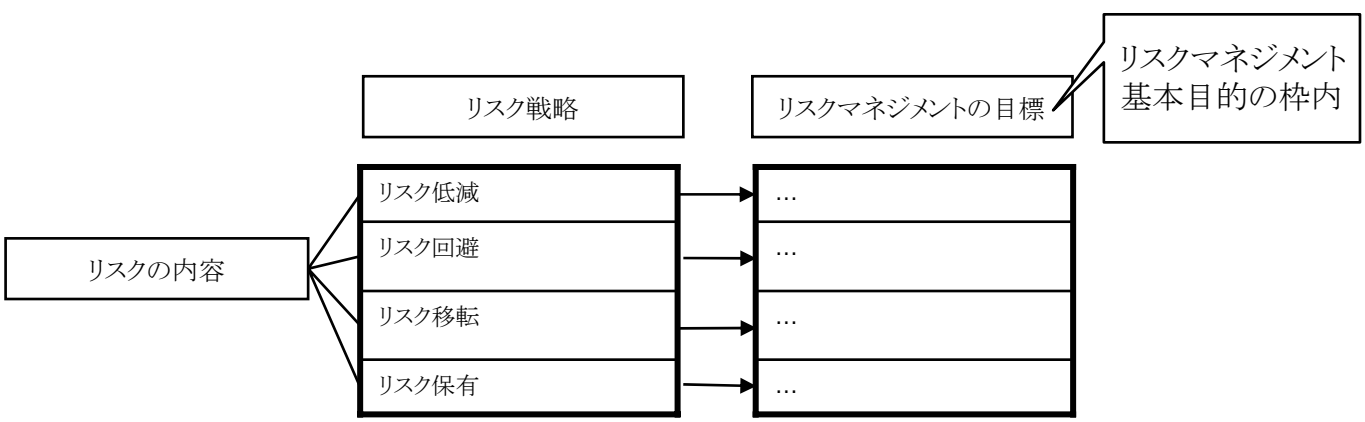
また、JISQ2001では、リスクマネジメントの目標を設定する際の考慮事項として下記を挙げています。

「- 守るべき対象を明確にしておく
- 関係者との約束を守る
- 関係者に悪影響を与えるリスクを低減する
- 法的要求事項
- 社会通念
- 組織内外の関係者が容易に理解できる
- 費用対効果を考慮し最大限に経営資源の活用がなされる
- 実行可能である*」

＊『JISQ2001リスクマネジメントシステム構築のための指針』日本規格協会2003年より引用

リスクマネジメント目標の設定

リスクマップ上で個々のリスクの影響度や発生頻度を把握したら、次に当該リスクに対してとるべき戦略、低減・回避・移転・保有を決定します。すなわちリスク戦略を決定します。その結果を踏まえてリスク戦略に適うリスクマネジメントの目標が決定されます。したがって、リスクマネジメントの目標を決定する前にリスク戦略を決定する必要があります。ある1つのリスクに対してとるリスクマネジメントの目標もリスク戦略によって異なります。ただし、個々のリスクに対するリスクマネジメントの目標は全社的に策定したリスクマネジメント基本目的に適うものである必要があります。



リスクマネジメントの目標は可能な限り定量化する

リスクマネジメントの目標の特徴②「組織が行うリスクマネジメントに関する測定可能な結果の要求事項の詳細」から導かれるポイントについて説明します。

リスクマネジメントの目標は、可能な限り定量化することが望まれます。発生頻度や影響度が定量的に把握されている場合には、リスクマネジメントの目標も定量化することが比較的簡単です。
しかし、定量化することが難しい場合には、定性化することは言うまでもありません。

以下には定量化を行うメリットを示します。

リスクマネジメントの目標がより具体的になるので、目標に向かって邁進しやすくなる

リスク対策実施後のリスクマネジメントパフォーマンス評価及びリスクマネジメントシステムの有効性評価が容易となる

各部門部署で実施すべきリスク対策がより明確になるので、リスク対策への理解が得られやすくなる

リスクマネジメントの目標はリスクの内容、リスク戦略等により多種多様なものとなります。三者の関係を参考として例示します。

参考　リスクマネジメントの目標の具体例

リスクの内容	リスク戦略	リスクマネジメントの目標
工場で労働災害が発生するリスク	リスク低減（予防・防止）	工場での年間労働災害件数を現在の100件から30件に減少させる
製品瑕疵によりリコールが生じるリスク	リスク低減（予防・防止）	製品瑕疵によるリコール件数は現在年間10件あるが、皆無とする
震度6以上の地震が発生するリスク	リスク低減（軽減）	震度6以上の地震が発生しても死者を出さない。また1ヶ月以内に操業を再開させる
火災により工場の製造ラインが停止するリスク	リスク低減（軽減）	1件の火災で停止する製造ラインを全体の50%以内に留める
海外の顧客から巨額の訴訟を起こされるリスク	リスク回避	海外市場から1年以内に撤退し、国内販売に専念する
店舗の商品が盗難や万引きされるリスク	リスク移転	販売店舗の商品に対して付保100%となるような保険契約を締結する
コンプライアンスリスク	リスク低減	法令等の遵守を通じて企業としての社会的責任を遂行するとともに企業価値の向上を図る

コラム

全知（経済）人か？経営人か？

伝統的な経営学で意思決定における人間の能力に対して議論されています。ひとつは人間は全知全能で何でも知っているという、いわゆる「全知（経済）人仮説」です。この仮説では、完全で最適な意思決定ができます。もうひとつは人間の能力には限界があり、全ての完全な情報は得られないという、いわゆる「経営人仮説」です。この仮説では、人間は限られた情報のもとで満足する代替案を選択します。

リスクマネジメントをこれから実践しようとする皆様は、神様のような「全知（経済）人」ではなく「経営人」の立場で考えなくてはなりません。もし、自分は全知（経済）人であると認識している方がおられたらすみません。

「全知（経済）人」ではないのですから、リスクマネジメントの完全な実践を期待すべきではありません。「経営人」として、限定された情報の下で合理的に実践することを目指しましょう。リスクマネジメントサイクルは継続的改善が大前提となります。日々改善していくことによりリスクマネジメントも最適（完全）に近づいていくことでしょう。

4.2.3　リスク対策の選択

リスクマネジメントの目標が設定されたら、具体的なリスク対策を決定します。具体的なリスク対策は一つのリスクマネジメントの目標に対して一つ選択されるケースのみではなく、一つのリスクマネジメントの目標に対して複数のリスク対策を実施するケースや複数のリスクマネジメント目標に対して一つのリスク対策を実施するケースがあります。

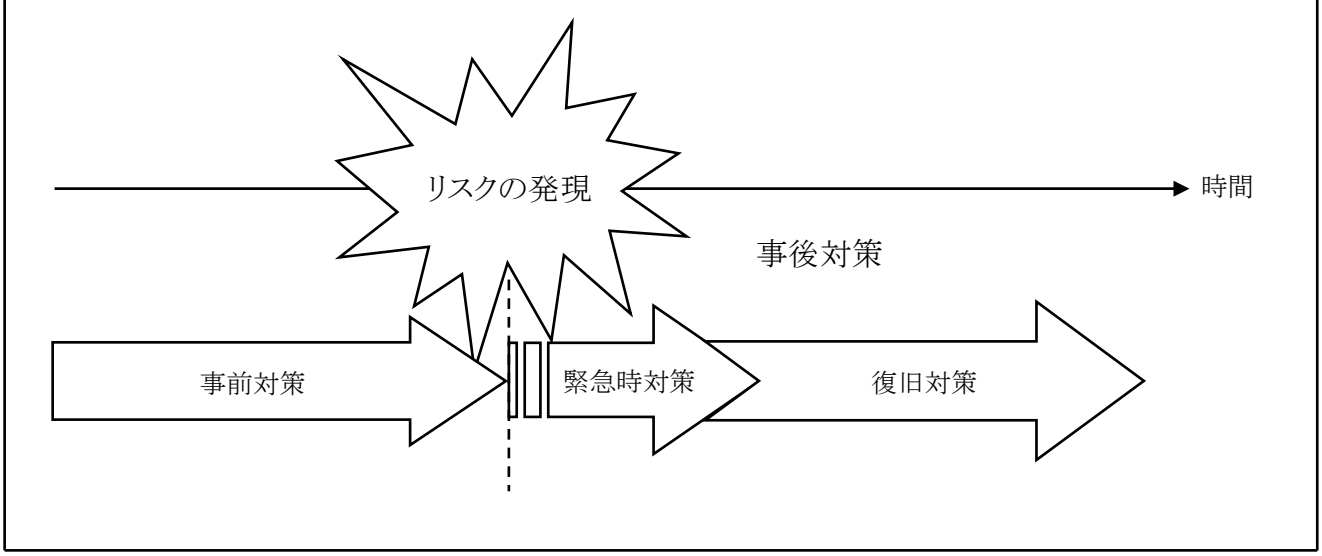
ここで注意したいことは、具体的なリスク対策はリスクマネジメントの目標を達成するために選択されるということです。リスク対策の実行には人、物、金等の経営資源が投入される場合もあります。そのためある一定の経営資源や時間の制約がある中で最適のリスク対策を選択する必要があるのです。

時系列リスク対策の分類

リスク対策を時間軸の観点から分類した場合、予防・防止等の事前対策のみでなく、緊急時対策、復旧時対策の2つの事後対策があります。各対策の意義と目的は下表の通りです。

対策の種類	事前対策	事後対策	
		緊急時対策	復旧対策
意義	リスク発現前、つまり組織が問題なく無事に運営されている平常時において実施するもの	リスク発現直後に実施するもの	緊急時対策に引き続き実施されるもの
目的	・リスクの発現の防止 ・リスクの低減	・被害の最小化 ・被害拡大の防止 ・復旧対策の早期立上げ	・二次被害の防止 ・通常組織活動への早期復旧

参考　時系列リスク対策の分類図



機能別リスク対策の分類

リスク対策はリスクの種類や企業の採用するリスク戦略及び企業の事業内容等により無数にあります。リスク対策を一律に整理、体系化するのは困難ですが、以下のようなものを例として挙げることが可能です。

①設備・装置面での対応	火災に備えてのスプリンクラーや防火壁の設置
	地震に備えての耐震構造への補強
	盗難等に対するセキュリティー設備の設置
	データ保存のためのバックアップセンターの建設
②組織・人材・教育面での対応	リスクに関する責任者とチェック機能を意識した組織作り
	法務スタッフや財務スタッフのような専門性の高い人材の採用・育成
	品質検査部員の増員
	防災訓練
	教育研修の実施
③規律・運用・広報面での対応	リスクマネジメントに関するルールやマニュアルの明確化
	コンプライアンス体制等の充実
	社内外に対するリスクコミュニケーション能力の向上と情報共有
④財務・契約面での対応	リスク発生に備えての保険契約やデリバティブ取引等の金融取引
	引当金の積み増し
	他社との委託契約の締結
	保証契約の締結

『事業リスクマネジメントーテキストー 経済産業省 平成16年3月』 262ページより作成

どのように具体的なリスク対策を選択すべきか

具体的なリスク対策を策定するのは組織にもよりますが、各部門・部署で立案することが多いようです。

いくつかの対策案を比較する

- 対策を決定する前に対策案を多角的に比較する必要があります。対策案ごとにリスクマネジメントの目標達成の有効度、対策を実施した場合の業務量、必要な経営資源の量、実行容易性、他の対策との組み合わせ等を評価します。複数の対策案がある場合は対策案の中から評価結果を総合的に判断した上で、実施すべき対策を決定します。

リスク対策は全社的な視点から考える

- 対策実施に必要な経営資源や時間には一定の制約があります。そのため、リスク対策は個々のリスクごとではなく、企業全体の視点で最適なリスク対策を選定する必要があります。
- 全社的な視点でリスク対策を選択するには、リスクマネジメントシステム担当責任者とリスク対策案を提案した部門・部署との協議が必要となります。

費用対効果を考慮する

- 対策実施の予算には限りがあります。そのなかで費用対効果分析を実施し、費用対効果の高い対策を優先して選択することが重要となります。
- 複数のリスクマネジメント目標の達成に有効な対策は一般的に費用対効果が高いので、なるべく優先して選択すべきです。

4.2.4　リスクマネジメントプログラムの策定

リスク対策の選択後、企業が次に実施すべきことはリスク対策を実践するための具体的な活動計画、つまりリスクマネジメントプログラムの策定です。リスクマネジメントプログラムとはリスク対策の実施そのものを指すのではなく、リスク対策実行に必要な5W1H（誰が、何を、いつ、どこで、どのように）を定めた計画であるとも言えるでしょう。

リスクマネジメントプログラムが策定されたらあとは当該プログラムに沿って行動します。

リスクマネジメントプログラムには事前対策のみならず、緊急時対策、復旧対策が含まれる点にも注意が必要です。

JISQ2001ではリスクマネジメントプログラムの策定時に設定することが望ましい事項を下記のように定めています。

「- リスク対策の具体的内容
- 組織の関連する各部門及び部署におけるリスク対策の日程
- 利用する経営資源
- 責任の範囲及び所在*」

また、JISQ2001ではリスクマネジメントプログラムの策定において考慮すべき事項を下記のように定めています。

「- 継続的に実施できるような内容
- 適切な手順
- 参画すべきすべての責任ある関係者
- 定期レビューのために必要な仕組み
- 利用する経営資源、責任、時期及び対応すべきリスクに対してとるべき対策の優先順位の適切さ
- リスクマネジメント方針及び一般的な計画活動への対応の適切さ
- 監視及びレビューの手順*」

*『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年より引用

リスクマネジメントプログラムを経営計画へ反映させる

リスクマネジメントの取組みをより実行可能にするにはリスクマネジメントプログラムを経営計画等に組み込むと良いでしょう。組み込むことにより下記のようなメリットがあります。

リスク対策の実施に必要な人員、予算、時間等を事前に確保できる

リスク対策の責任部署が明確となる

各部門部署でリスクマネジメントの実施すべきことが明らかとなり、対策への取組みが理解されやすい

日常業務への取組みと同等の優先度

通常業務に追われるとなかなかリスク対策が実行できないことが多いものです。リスクマネジメントを有効に機能させるためには、リスク対策についても日常業務と同等の優先度で実行させることが大切となります。

職務規定の中にリスクマネジメントを明記する

- リスクマネジメントが正式な業務であるという認識をもってもらうことで前向きに取り組んでもらうことができます。

業績評価の中にリスクマネジメントに対する項目を加える

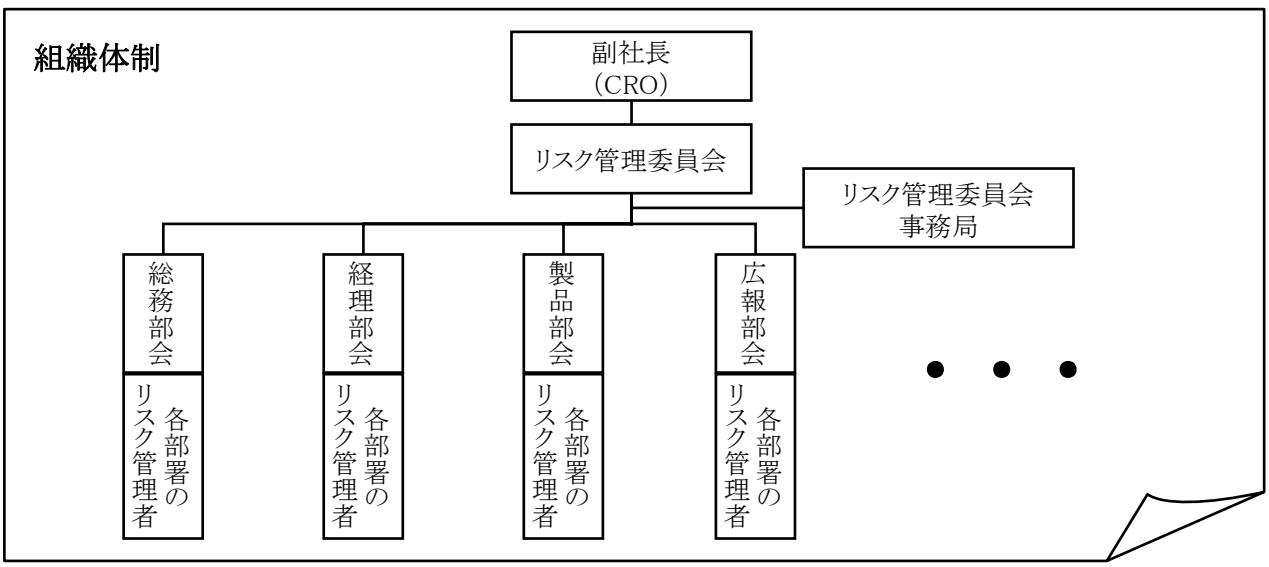
- 業績評価の良し悪しにより昇進や年俸が決定する企業が多いため、リスク対策を積極的に実施する動機付けが得られます。

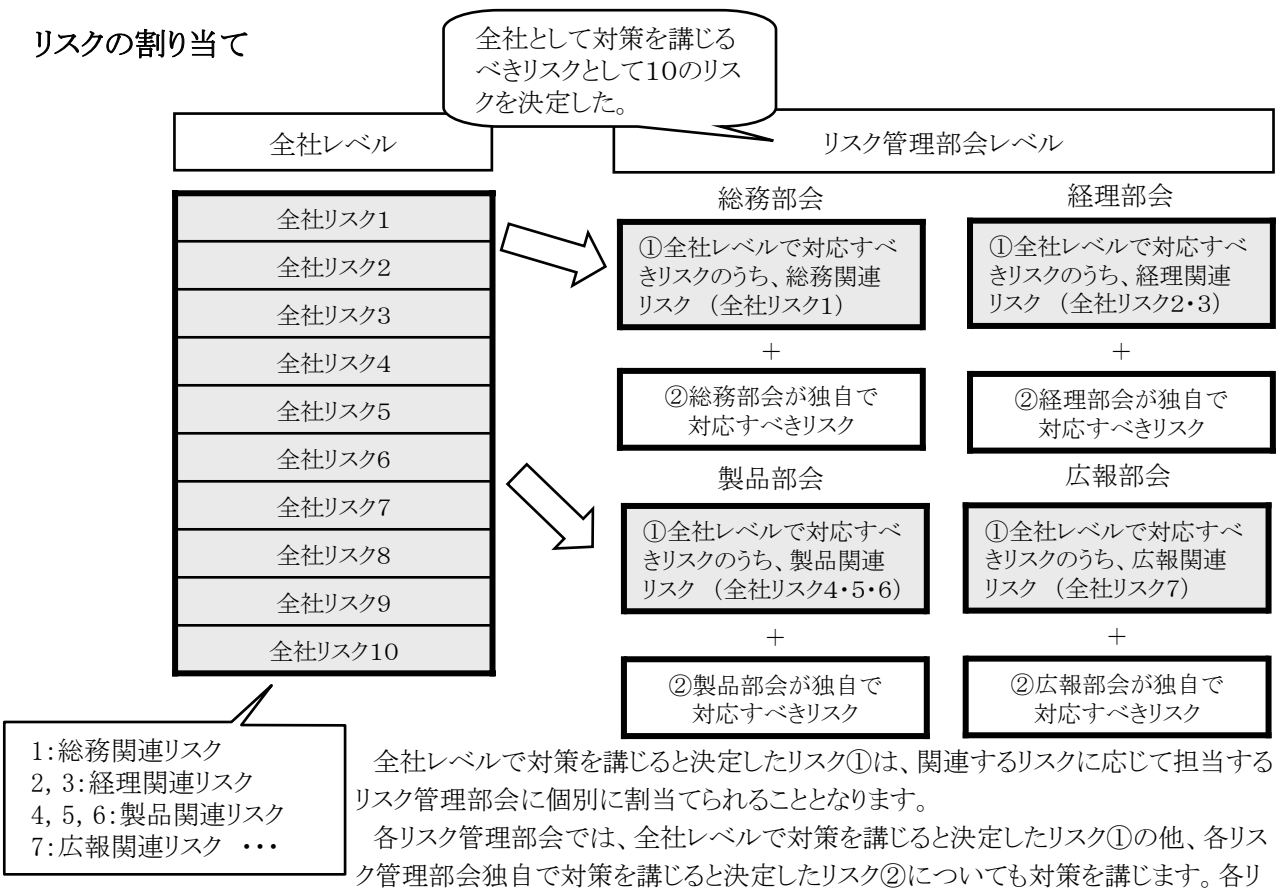
リスクの割当て

対策を講じるべきリスクの割当て方法は、企業が採用しているリスクマネジメントシステム体制及び組織形態により様々です。ここでは、Chapter2「リスクをどの単位で管理するか」のリスクマネジメント体制の参考事例に基づいて対策を講じるべきリスクの割当ての具体事例を紹介していきます。

事例 | **リスクの割当て 1/2**

CROを委員長をとするリスクマネジメント委員会が設置されている場合はリスクマネジメント委員会にて各専門部会にリスクを割り当てを決めるのが一般的です。



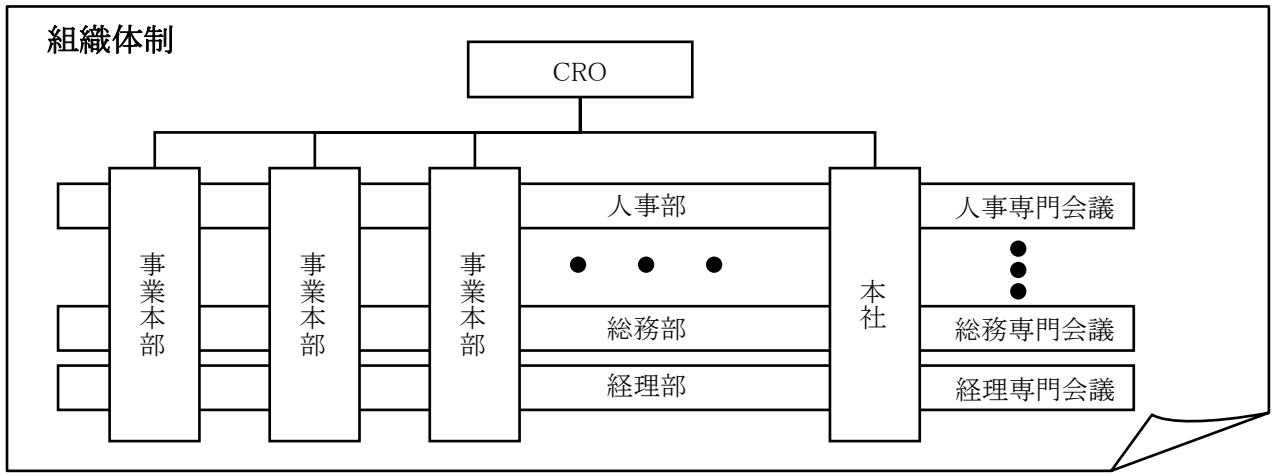


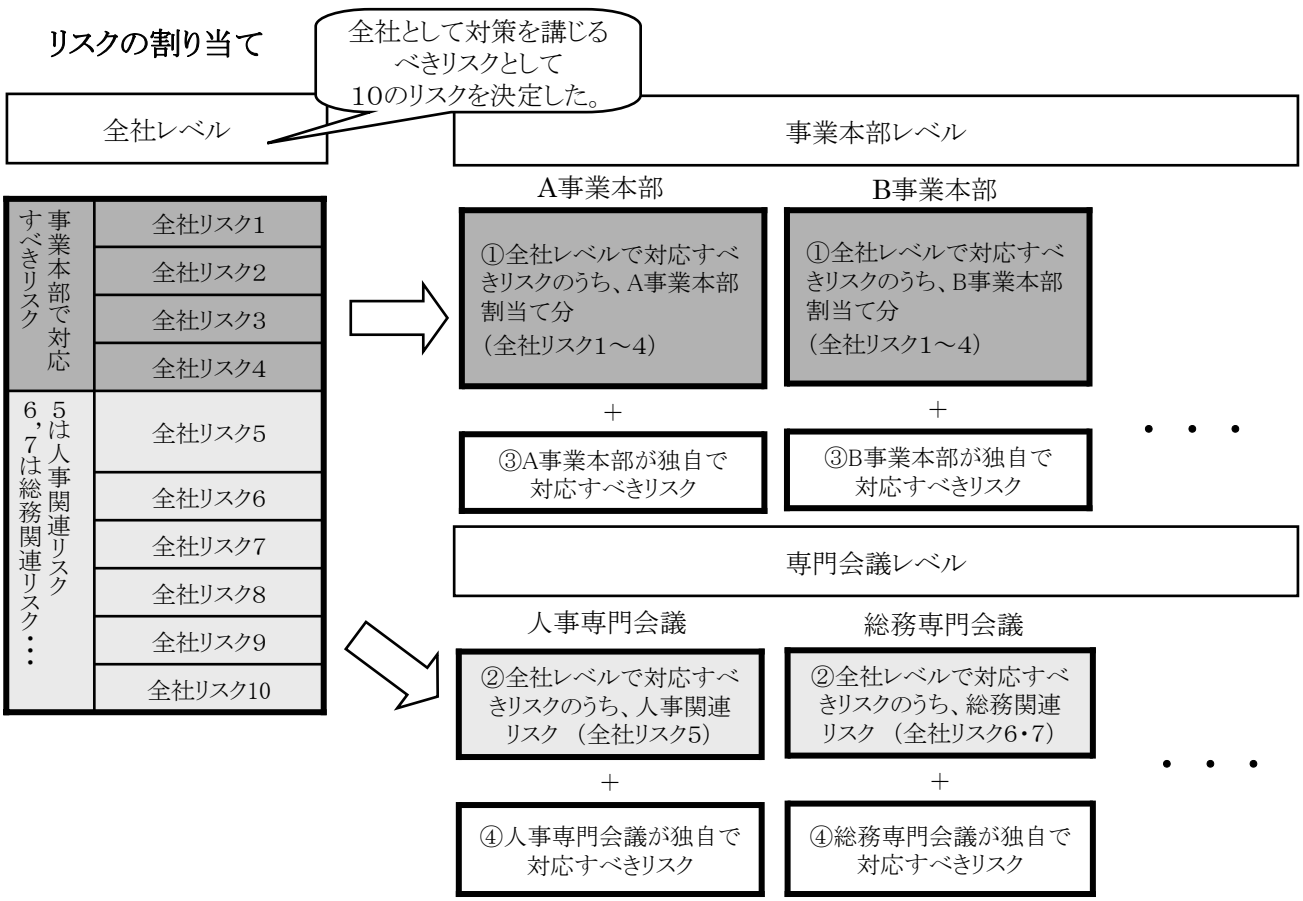
全社レベルで対策を講じると決定したリスク①は、関連するリスクに応じて担当するリスク管理部会に個別に割当てられることとなります。

各リスク管理部会では、全社レベルで対策を講じると決定したリスク①の他、各リスク管理部会独自で対策を講じると決定したリスク②についても対策を講じます。各リスク管理部会のリスク対策責任者は各リスク管理部会長となります。

事例　リスクの割当て 2/2

事業部組織制の場合、リスク対策を講じる主体は基本的には事業部になります。ただし、例えば、人事関連リスク等全社共通のリスクについては、人事部や各事業部の人事担当を集めた専門会議で全社的な方針や施策を策定します。





全社レベルで対策を講じると決定したリスクは①おおむね全ての事業本部が対応すべきリスクと②特定の専門会議が対応すべきリスクに分類されます。

各事業本部では、全社レベルで対策を講じるべきリスクのうち各事業本部分①の他、各事業部独自で対策を講じると決定したリスク③についても対策を講じます。各事業本部のリスク対策責任者は事業本部長となります。

各専門会議では、全社レベルで対策を講じるべきリスク②の他、各専門会議独自で対策を講じると決定したリスク④についても対策を講じます。各専門会議のリスク対策責任者は専門会議長となります。

顧客ニーズの変化等リスクは、事業によって性質も大きさも違うため、事業ごとに対策を講じていきます。

リスク対策シート（例）

リスク対策シートはリスクマネジメントプログラムで定めた各リスクに対する具体的対策の実施方法を示した文書です。リスク対策実施者が作成し、リスクマネジメントシステム担当責任者の承認を得る必要があります。

計画策定時に記入

リスク管理担当部署	A工場	実施責任者	X山　X夫
リスクの内容	工場で労働災害が発生するリスク	承認欄	2004/5/12 CRO　X野　X助　㊞
リスクマネジメントの目標	・A工場での年間労働災害件数を現在の20件から10件に減少させる。		
リスク対策の具体的内容	・工場内で事故が多発する場所10ヶ所にミラーを取り付ける ・労働災害を防止するための教育訓練を実施する。		
リスク対策の日程	上期中にすべてミラーを取り付ける 7月に1回、12月に1回労働災害リスク予防の教育研修を開催する。		
評価指標			

評価時に記入

リスクマネジメントパフォーマンス評価	評価時期	
	評価担当者	
	評価結果	
次年度への留意事項		

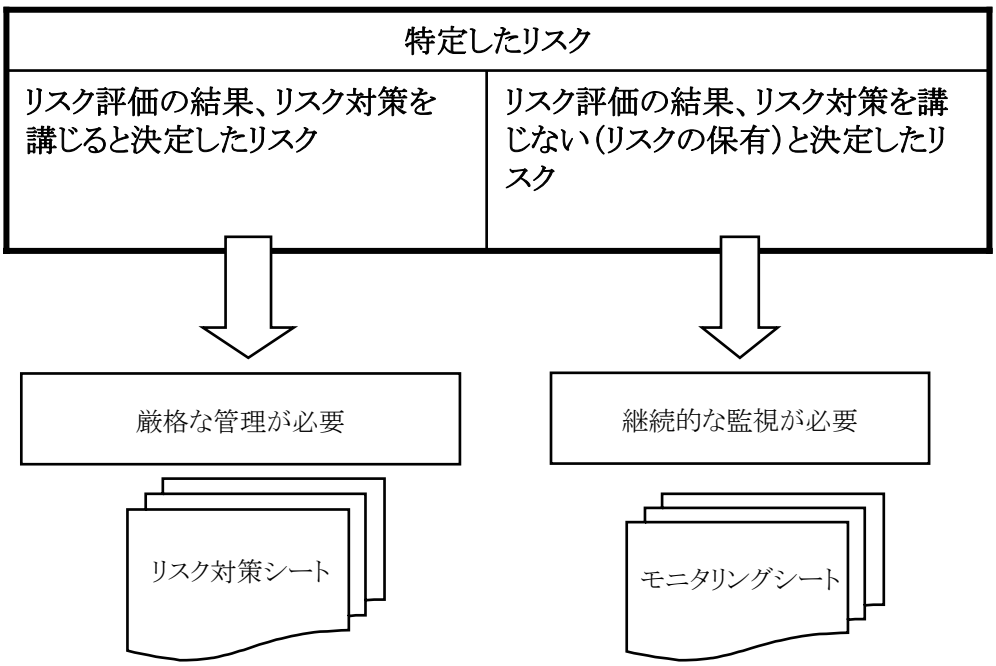
この部分は「6.2.5評価の実施」にて説明しています。

リスクマネジメントに対するパフォーマンス評価時に記入される
(Chapter6、6.2.2 リスクマネジメントパフォーマンス評価「どのようにリスクマネジメントパフォーマンスを評価するのか」にて説明)

4.2.5　リスク対策を講じないと決定したリスクへの対応

リスク評価の結果、リスク対策を講じないと決定したリスクは、単にリスク対策を取らないと決定しただけで、リスクそのものは存在し続けます。また、期中にリスク度合いが変化し重大なリスクとなる可能性や実際にリスクが発現する可能性があります。そのため、これらのリスクについては何もしないということではなく、モニタリング方法を定めて継続的に監視していく必要があります。

参考　特定したリスクへの対応



モニタリングシート（例）

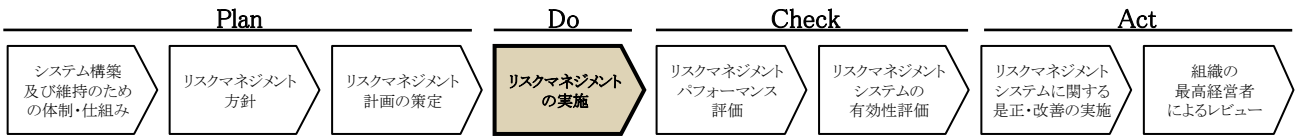
リスク対策を講じないと決定したリスクを継続的に監視するツールがモニタリングシートです。モニタリングシートには、当面対策を講じないとした理由やモニタリング実施の記録がされます。

リスク名	対策を講じないと決定した理由	監視責任者	監視予定日	監視記録	
不動産所有リスク	土地の時価下落により固定資産の減損損失が認識されるおそれがあるが、現在著しい時価の下落がないため	総務部長Y	2004/9/10 2005/3/10	2004/9/15 著しい時価の下落なし	

CHAPTER 5

リスクマネジメントの実施

5.1 リスクファクター別取組み
5.2 危機管理
5.3 内部統制



リスクマネジメントの実施においては、Chapter4で策定されたリスクマネジメント計画を実施していくこととなります。

このChapter5では企業が重視しているリスク、今後重視していくことが必要な代表的なリスクについて経営トップの役割も含めて解説していきます。

リスクマネジメントシステム担当においては、個別のリスクファクターについて対策立案および実行に関わるケースもあるため、リスクファクター別の基本的な理解を深めてこくことも重要です。

この章の内容

5.1.5 信用リスク

信用リスクの仕組み

信用リスク評価を構成する要素

信用リスクマネジメント評価・管理手法

信用リスクマネジメント“簡易編”

信用リスクマネジメント“詳細編”

信用リスクマネジメントにおける検討点

信用リスクマネジメントにおける今後の課題

5.1.6 レピュテーションリスク

リスク評価におけるレピュテーションリスクの扱い

レピュテーションリスクへの対応

5.2 危機管理（クライシスマネジメント）

5.2.1 事業リスクマネジメントにおける危機管理

5.2.2 危機管理マネジメント

エスカレーションルールの策定

危機管理マニュアルの作成

5.2.3 危機発生時の対応

危機対応組織の構築

情報管理

復旧活動

再発防止策の検討

5.2.4 事業継続計画（Business Continuity Plan）

事業継続計画（BCP）の必要性

事業継続計画（BCP）策定の手順

5.3 内部統制

5.3.1 内部統制とは

多くのリスクは内部統制の構築・運用によって低減できる

内部統制の具体例

内部統制のフレームワーク

内部統制の定義

「COSO−内部統制の統合的枠組み」の概要

5.3.2 リスクマネジメントと内部統制

企業の直面するリスク

リスクへの対応と内部統制

リスクマネジメントと内部統制との関係

COSOにおけるリスクマネジメントと内部統制

内部統制の限界

5.3.3 内部統制の継続的見直し

内部統制の継続的見直しの必要性

内部統制におけるPDCAサイクル

内部統制の評価

内部統制の是正・改善

5.1 リスクファクター別取組み

ここではリスクファクター別のリスクマネジメント取組み例および管理上の留意点について実際の企業がどのように対応しているか実例を上げて解説していきます。
具体的には
- 製品要因リスク
- 情報セキュリティリスク
- 市場リスク
- 信用リスク
- レピュテーションリスク

に関して取り上げます。

5.1.1 企業が重視しているリスクファクター

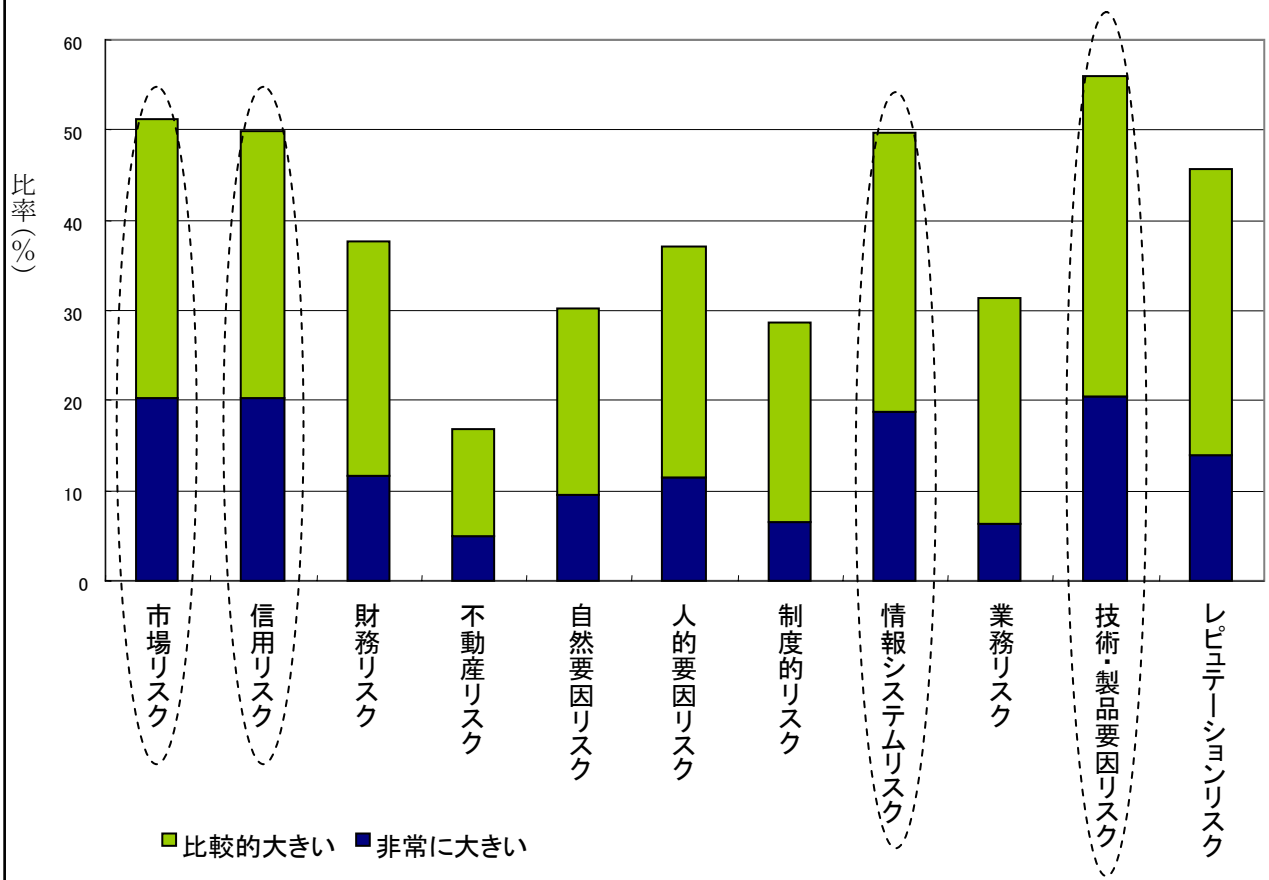
ここでは、企業が実際にどのようなリスクを重視し、マネジメントしているのか、またマネジメントしていこうとしているかにフォーカスを当て、リスクファクター別に実例を挙げて取組みをご紹介します。

企業が事業活動に影響を与えると認識しているリスクファクターについて2003年事業リスク評価・管理人材育成システム開発事業で実施されたアンケートでは市場リスク・信用リスクについて50%超の企業が影響が「非常に大きい」または「比較的大きい」影響があると回答しており、影響度の大きなリスクファクターとして捉えられています。また、情報システムリスク・技術・製品要因リスクにおいても同様に影響度の高いリスクファクターとして認識されています。
また、次ページの企業が今後調査分析対象として捉えているリスクファクターでは情報システムリスク・技術・製品要因リスクを対象として上げる企業が多く、これらのリスクへの意識の高さが伺えます。
この結果に基づき、この章では、製品要因リスク・情報システムリスク・市場リスク・信用リスクを取り上げます。情報システムリスクについては近年特に関心の高い情報セキュリティリスクと事業継続計画(BCP)の観点から取り上げます。(事業継続計画に関しては5.2.3で取り上げます)

近年の製品要因に関わる品質リスクや情報セキュリティに関わる情報漏えいといった企業不祥事の例にみられるようにこれらのリスクは対策を怠ったり、対応を間違うと非常に大きな問題へと発展し企業の信用の失墜、存続にも関わる問題となっています。また、市場リスクによる巨大損失の例は後を絶たず、信用リスクに関しても大手流通業や上場ゼネコンが姿を消すなど先が読めない時代に突入しています。本テキストではこれらのリスクに対する先進企業の取組みを紹介し、先達に学ぶことにより、これら固有のリスク対策はもちろんのことそれだけではなく、これらの事例が様々なリスクに共通して応用ができるものと確信しています。

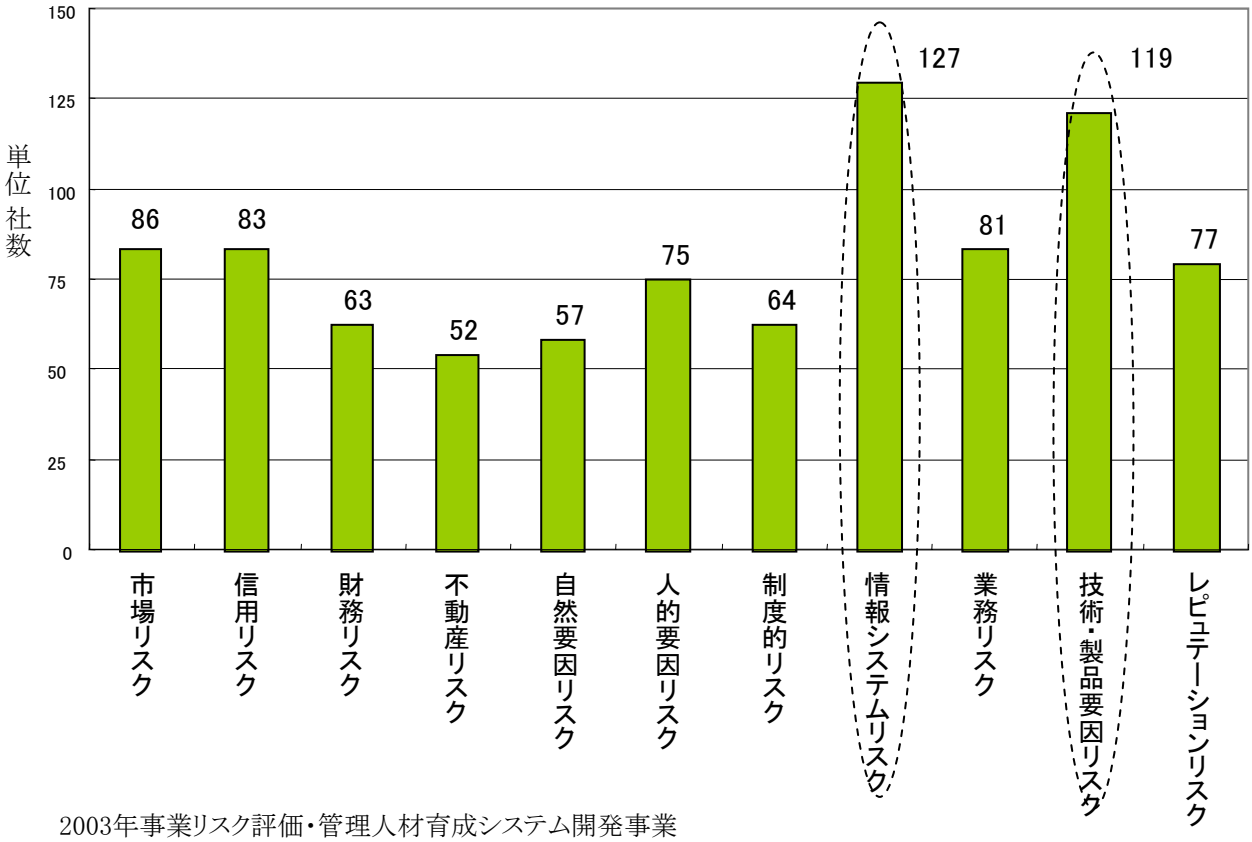
そして最後にこのアンケートでこれら4のリスクに次ぐ影響度があると回答されたものの現状ではなかなか具体的な対策をとりづらく複合的な要因により発生するレピュテーションリスクも合わせて取り上げます。

参考　企業が事業活動に影響を与えると認識しているリスクファクター



2003年事業リスク評価・管理人材育成システム開発事業
同年7月～11月に国内有力企業に対して行ったアンケート調査より作成
国内主要株式市場上場企業約3,597社に対して調査票を送付し、1,009票の回答を得たもの
「以下のような事象（リスクファクター）は貴社の事業活動にどの程度影響を与えるとお考えですか。
市場性リスク、信用リスク、財務リスク、不動産リスク、自然要因リスク、人的要因リスク、制度的リスク、情報システムリスク、業務リスク、技術・製品要因リスク、レピュテーションリスク」
（単一回答：非常に大きい/比較的大きい/影響はある/ほとんどない/無視できる/分からないより影響度が非常に大きい、比較的大きいと回答した企業数の比率を算出）

参考　企業が今後調査分析対象として捉えているリスクファクター



2003年事業リスク評価・管理人材育成システム開発事業
同年7月～11月に国内有力企業に対して行ったアンケート調査より作成
国内主要株式市場上場企業約3,597社に対して調査票を送付し、1009票の回答を得たもの
「今後調査・分析を行う必要性を感じているリスクファクターはありますか」

5.1.2　製品要因リスク

製品要因リスクとは、企業が製品を生産するという活動における原材料や部品の調達から最終顧客までの全ての工程に存在するリスクを言います。

「まず製品を生産する過程で労働者が災害に遭遇するリスクがあります。こうした労働災害が発生すると、当該労働者の補償、ラインの停止による生産低下などの損失が考えられます。
また、欠陥製品を販売したために消費者に被害を与えるリスクも、製品要因リスクの一つと考えられます。欠陥製品を販売して消費者に被害を与えた場合には、製造物責任法により、過失の有無にかかわらず、損害賠償を請求される場合もあり得ます。製品の安全性の確保という観点から、厳重なる品質管理が求められています*。」
*『事業リスクマネジメントーテキストー 経済産業省 平成16年3月』72ページ より一部修正

特に製造物責任を負担する場合、企業の被る損失は直接的な損失、間接的な損失ともに大きなものになります。

「－ 損害賠償金
－ 紛争解決費用　　直接的損失
－ 事後措置費用
－ 利益損失
－ 企業イメージ　　間接的損失
－ 従業員の士気* 」

* 東京海上火災保険 企業リスクコンサルティング室『企業リスクのすべて　その事例と対策』東洋経済新報社 2001年より作成

製品要因リスクのうち主要な具体的リスクとしては以下のようなものが挙げられます。

－ 品質リスク
－ 調達リスク
－ 工場事故リスク
－ 製品瑕疵リスク

これらのうち、ここでは、品質リスク及び調達リスクに関する取組み例とリスク対策取組み例を紹介します。

製造業は複数の工程に分けた上で製造作業を行うことから、リスクの因果関係を分析しやすい業態であると言えます。また工場などの現業部門を抱えており、現場での作業の質がリスクの発生頻度に大きく影響を与えます。
こうした製造業の特徴を踏まえ、品質リスクについてはリスク発見及び分析方法を紹介します。

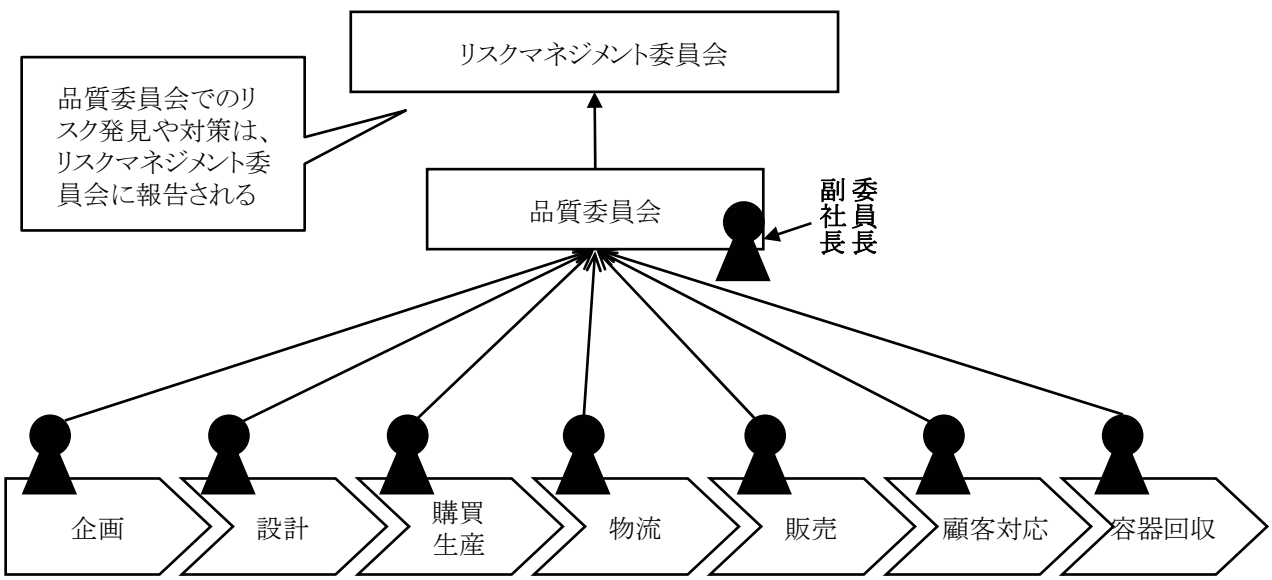
また調達リスクについては、取引先の財務分析を行うことにより調達上のリスクを低減する方法を紹介します。これは信用リスクの管理の際に用いられる手法に近い方法です。

リスク対策取組み例としては、リスク対策意識を現場に浸透させるための方法を二つ紹介します。

品質リスク – 製品製造サイクルからのリスク発見

この企業では「品質委員会」で製造の全工程を視野にリスクの発見、評価、対策を行う仕組みを採用しています。この仕組みによって、部門や部署の狭間で見落とされがちなリスクの発見が可能になります。

事例 ある消費財製造業の組織体系



- 品質委員会では年二回、副社長を委員長として製品製造サイクルに関係する部門や部署のリスクマネジメントシステム担当者が集まり、リスクの発見を行います。
- 通常は、例えば企画工程であれば企画部などのような、各工程の担当部署においてリスクの発見作業が実施され、リスクマネジメント委員会に報告されることが多いと考えられます。しかしこのような方法では、部門や部署の狭間でリスクが抜け落ちてしまう可能性があります。
- この企業では工程ごとに組織横断的にリスクを発見することによって、リスク発見の漏れを補完しています。
- 品質委員会では各工程担当部署の責任者が集まり、ディスカッションによってリスクを洗い出します。
- 実際には当該工程を担当している部署よりも前後の工程を担当している部署の方が、当該工程担当部署のリスクに関して詳しいという話がありました。従って製品製造サイクルを意識したリスクの発見は非常に有効と言えます。

品質委員会を通じて発見された各工程のリスク例

品質委員会では各工程を通したすべてのリスクを発見します。この作業を通じ、企画から容器回収に至る各段階で発見されたリスクの例を挙げます。

企画段階でのリスク

- ✓ 商品企画が顧客のニーズに沿っていないリスク
- ✓ 表示内容が誤っているリスク
- ✓ パッケージが顧客のニーズに沿っていないリスク
- ✓ 市場調査が十分に行われていないリスク

設計段階でのリスク

- ✓ 法律に違反しているリスク
- ✓ 社内基準に沿っていないリスク
- ✓ 消費者の使用テストが十分に行われていないリスク

購買・生産段階でのリスク

- ✓ 社内品質基準に沿っていないリスク
- ✓ 手法、容器基準に沿っていないリスク
- ✓ 原材料が調達できず、生産できないリスク
- ✓ 不良品の発生による製品回収のリスク

物流段階でのリスク

- ✓ 輸送条件が悪く、品質が悪化するリスク
- ✓ 発注、受注タイミングが間違っているリスク

販売段階でのリスク

- ✓ 在庫過多による長期保管で品質が悪化するリスク
- ✓ 正しい説明がなされないまま商品が販売されてしまうリスク

顧客対応段階でのリスク

- ✓ 顧客からのクレームに適切に対応できないリスク
- ✓ 重大なクレームを見逃してしまうリスク

容器回収段階でのリスク

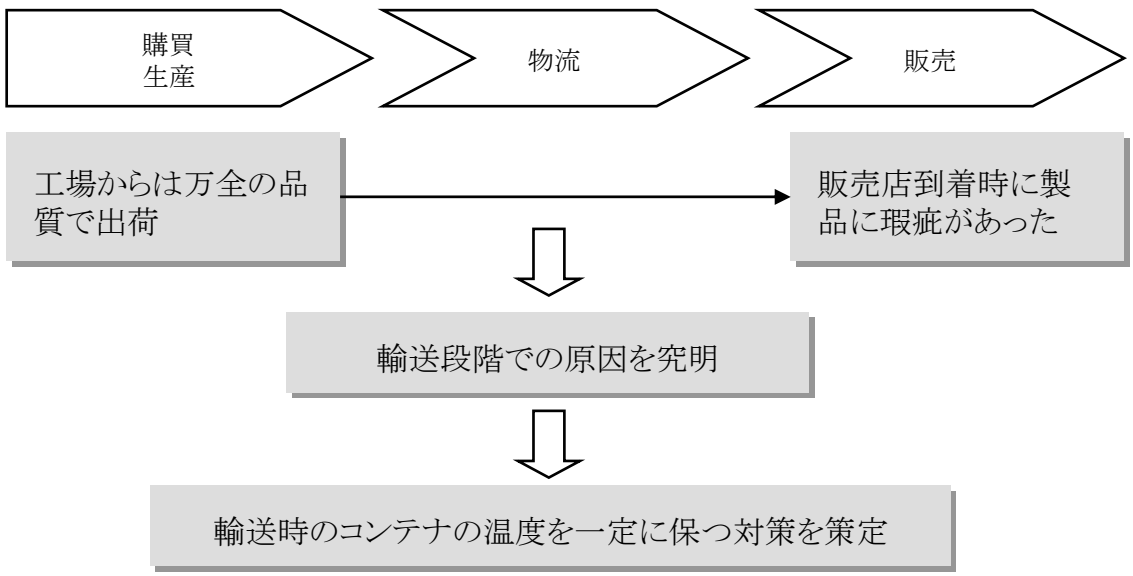
- ✓ 容器の不法投棄などでブランドイメージを損なうリスク
- ✓ 顧客に適切な説明が行われないリスク

組織横断的なリスク発見と対策

品質委員会を通して全工程のリスクの発見がなされることで、自工程のみでのリスク発見作業では発見できなかったリスクが発見されます。例えば物流工程で発見されている「輸送条件が悪く、品質が悪化するリスク」は下記のような前後工程からの指摘により発見されたリスクです。

販売工程に届いた製品に瑕疵があった場合、その前工程で何らかの不備が生じていることが想定されます。
品質委員会を通じて関係工程のリスクマネジメント責任者が話し合うことで、どこにリスクがあるのかを発見でき、適切な対策を講じることが可能です。

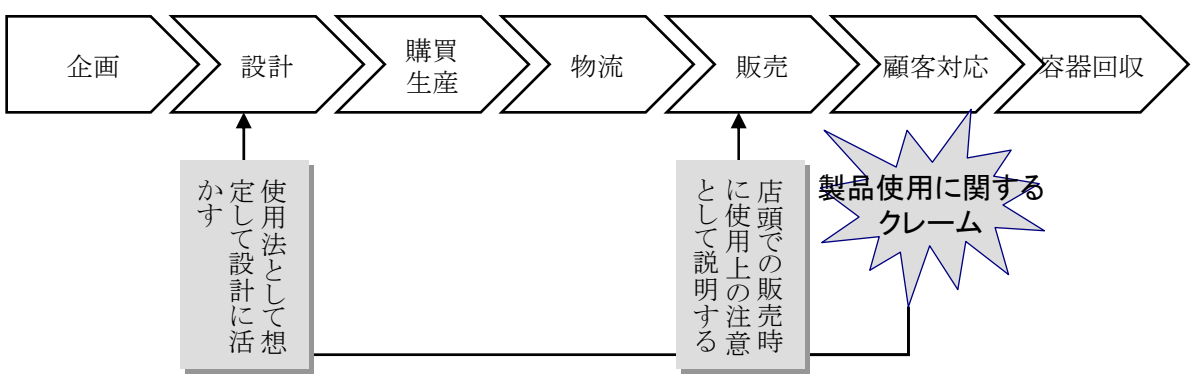
事例　前後工程からの指摘により、対応されたリスク



品質委員会という組織横断的な活動を通し、リスクの発見機能が強化されただけでなく、工程間の結びつきが強化され、リスクへの対応のスピードも高まりました。

顧客対応で設計時には予期できなかった使用法によるクレームが発生した場合、速やかに関係工程のリスクマネジメント責任者に当該情報が伝わり、すぐに反映されるような情報共有の仕組みも品質委員会を通じて確立されました。

事例　顧客対応時に発見され、対応されたリスク

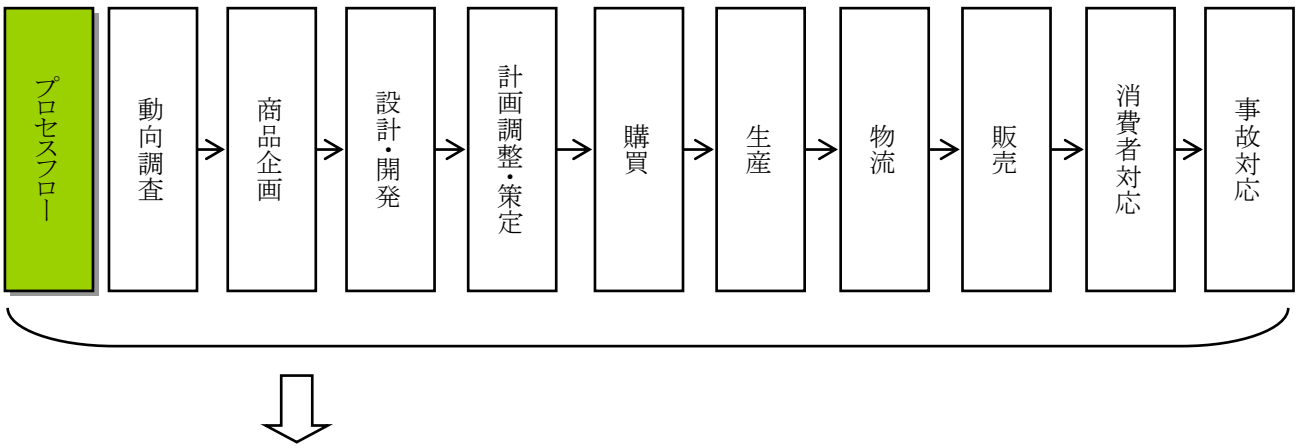


品質リスク – リスク発生のシナリオからリスク要因を特定する

品質リスク発生のシナリオを整理し、品質リスクの発生源となり得るリスクを特定している企業がありました。このように一つのリスクをより深く掘り下げることによってその原因を特定し、より詳細な対応策を策定することが可能になります

(1) プロセスフローの各工程内のリスクを発見する

プロセスフローから洗い出されたリスクをグルーピングし(KJ法などを利用)因果関係で整理していきます。



動向調査工程で考えられるリスク

商品企画工程で考えられるリスク

●

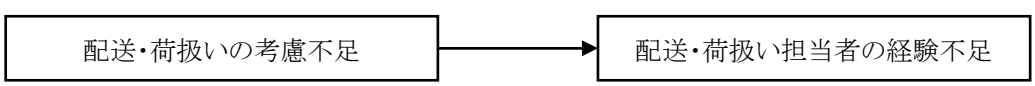
●

●

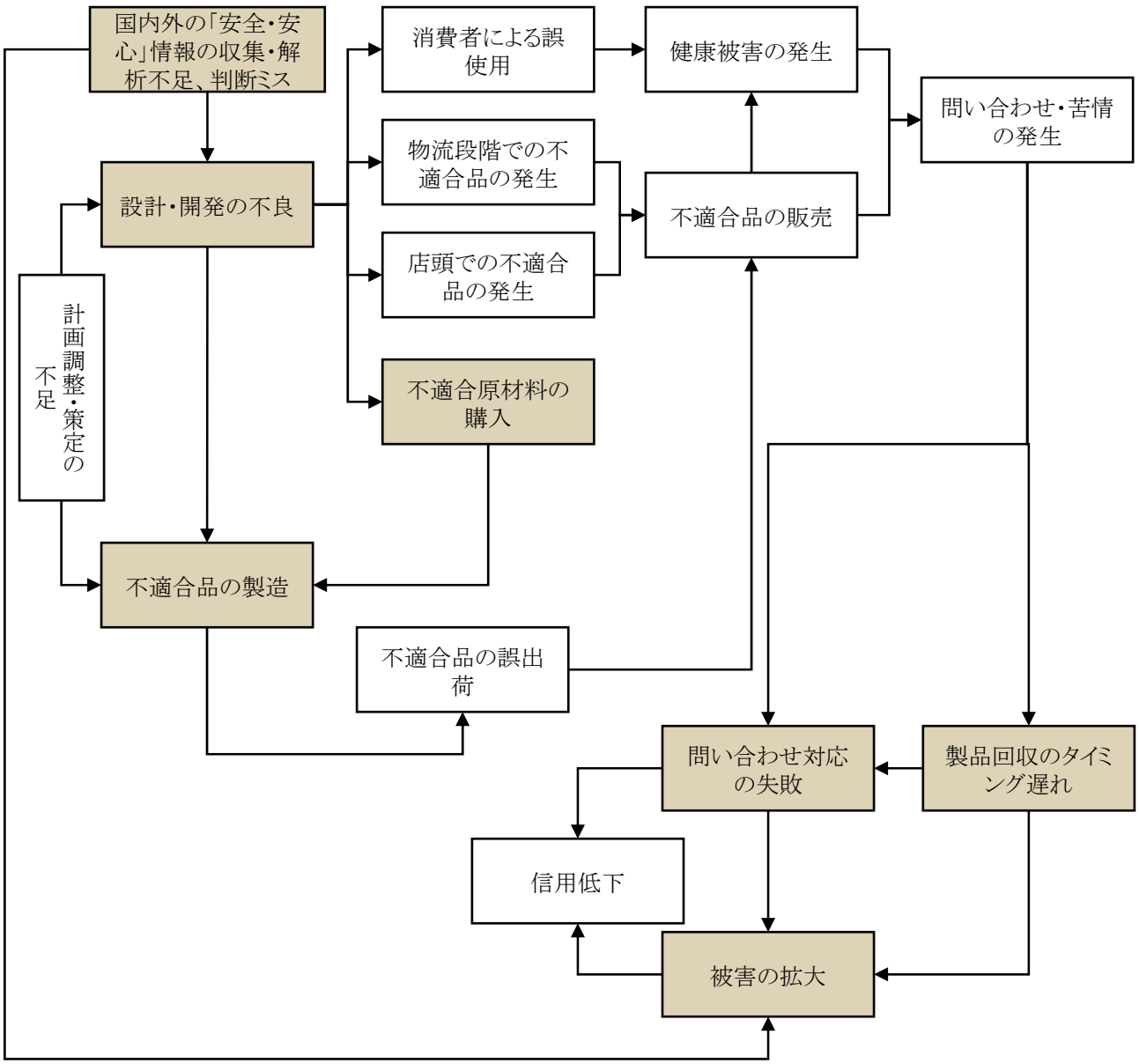
(2) リスクをグルーピングして、因果関係を示す

発見されたリスクはグルーピング(リスクカテゴリー化)して、因果関係を探します。グルーピングは仮決めで、大きなリスクも小さなリスクもまとめて因果関係を整理します。

グルーピング後、因果関係を整理したものが、次ページの関係図になります。



事例　ある消費財製造業の品質リスク発生シナリオの因果関係図



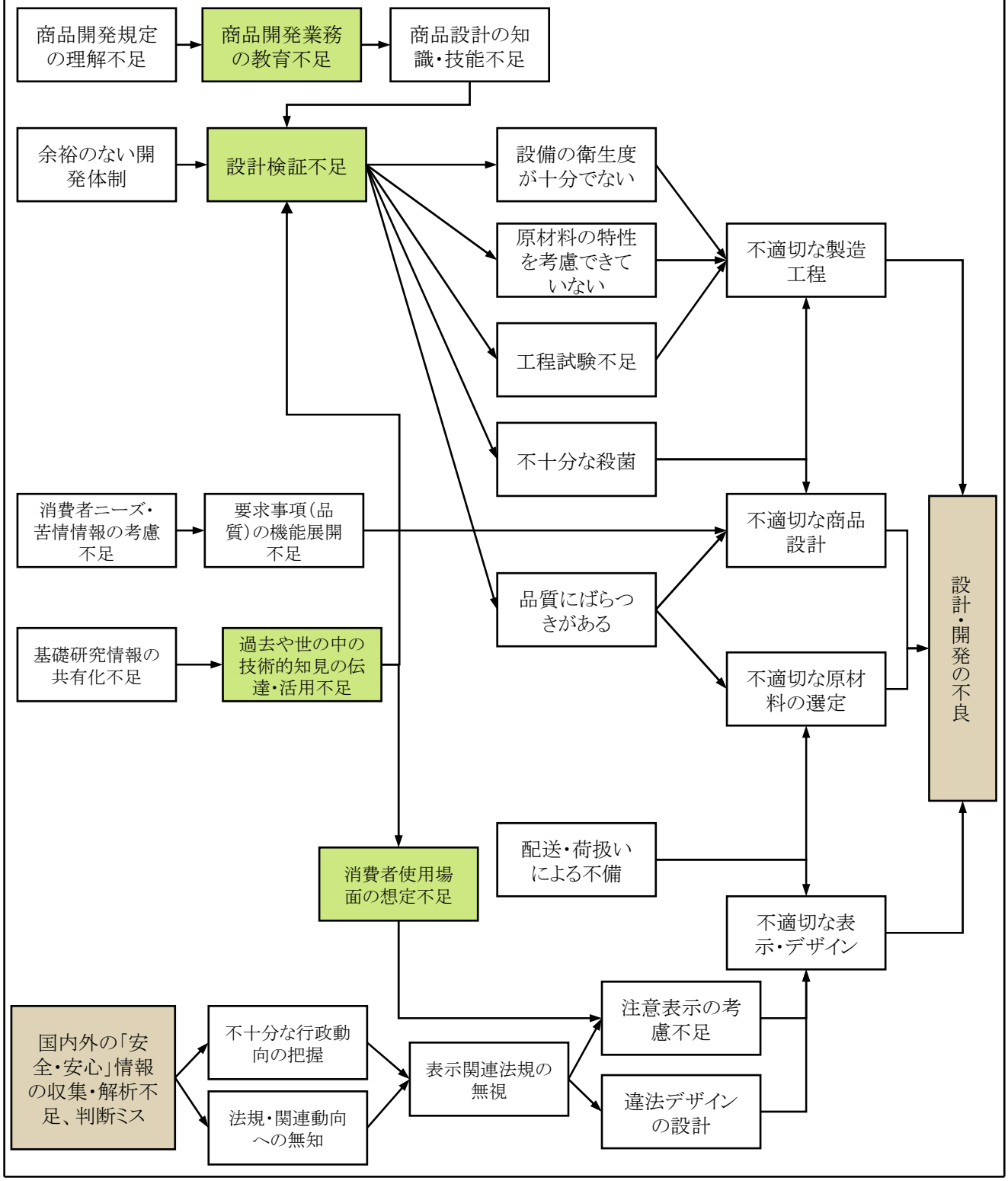
- この企業では品質リスクが発現するシナリオをワークフローから導出し、どの時点での不具合がリスクの発現を生むのかを分析しています。
- 因果関係の整理を繰り返すことで、
  - 国内外の「安全・安心」情報の収集・解析不足、判断ミス
  - 設計・開発の不良
  - 不適合原材料の購入
  - 不適合品の製造
  - 二次クレームの発生
  - 品質事故への不適切な事故対応
  - 被害の拡大

  の7点を主要なリスクとして特定しました。（図中は網掛けしています）
- この分析結果をもとに、当該リスクのより根本的な原因を特定します。

（3）個々のリスクカテゴリーのキーリスクを特定する

個々のリスクカテゴリーの原因を分析して、主要な原因であるキーリスクを特定します。

事例　**ある消費財製造業の『設計・開発の不良』リスク源泉分析図**



- ここでは先の分析で明らかになった『設計・開発の不良』という主要リスクのさらに根本的な要因を探し出すための分析を行っています。
- 『設計・開発の不良』というリスクは漠然としており、具体的な対策を明確にすることが困難です。当該リスク要因をさらに詳細に分析して「商品開発業務の教育不足」「設計検証不足」が源泉であると特定することで、さらに具体的な対策を講ずることが可能になります。

調達リスク – 財務分析から取引先を判別

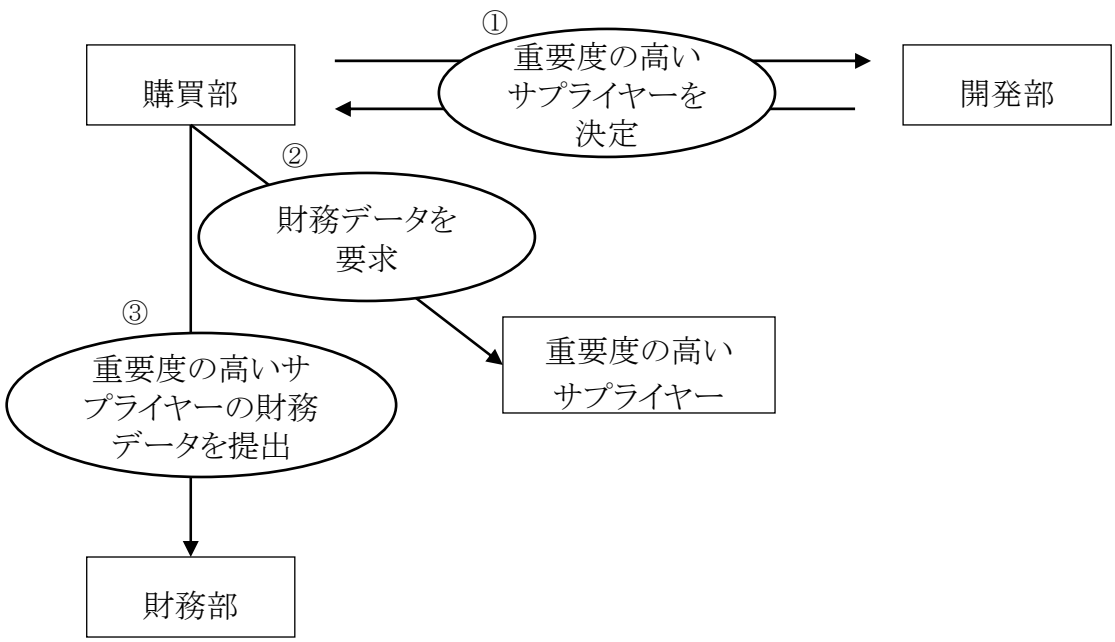
製造業には部品調達のリスクが伴います。安定的に部品や原材料が調達できなければラインが停止してしまい、業務の継続に影響を与えます。

こうした調達上のリスクには様々な要因が考えられます。例えば原材料を調達している海外との取引が何らかの原因でできなくなった場合や原材料が尽きてしまった場合などもその要因にあたります。ここで取り上げるのは取引先の倒産等により調達ができなくなるリスクです。

この企業では現在取引をしているサプライヤーの財務状態を独自のモデルを使って分析し、継続的な取引先として適正かどうかを判断しています。サプライヤーの財務状態を分析することで取引先として適正かどうかを判断し、安定して部品が調達できなくなるリスクを低くします。サプライヤーの信用評価を行うことで安定的な調達が可能になり、安定的な製造が可能になります。

なお、この企業では現在の取引先に対するリスク判断として当該方法を用いていますが、新規取引先や見積相手先の選定においても、条件が揃えば同じ方法論を使用することが可能です。

(1) 重要度の高いサプライヤーを決定する



① サプライヤーの窓口である購買部が主になり、開発部と協力して重要度の高いサプライヤーを決定します。

- 取引金額
- 技術的な優位性(例えば特殊な技術などを持っており他に代替がきかない、など)
- 品質
- アフターサービスのレベル
- 納期

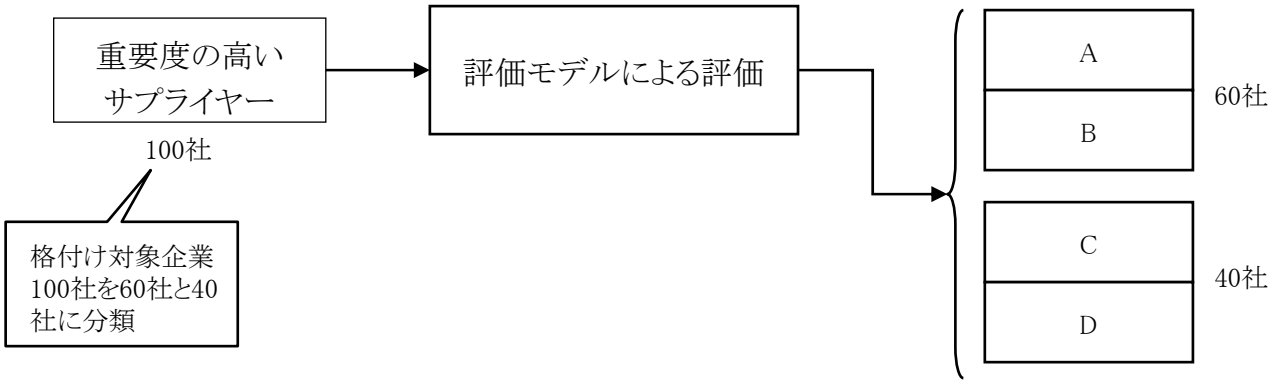
などの項目から重要なサプライヤーが決定されます。

② 購買部は重要なサプライヤーに対して、財務データの提出を求めます。

③ サプライヤーから届いた財務データは財務部に渡され、社内独自の評価モデルに沿って格付けされます。

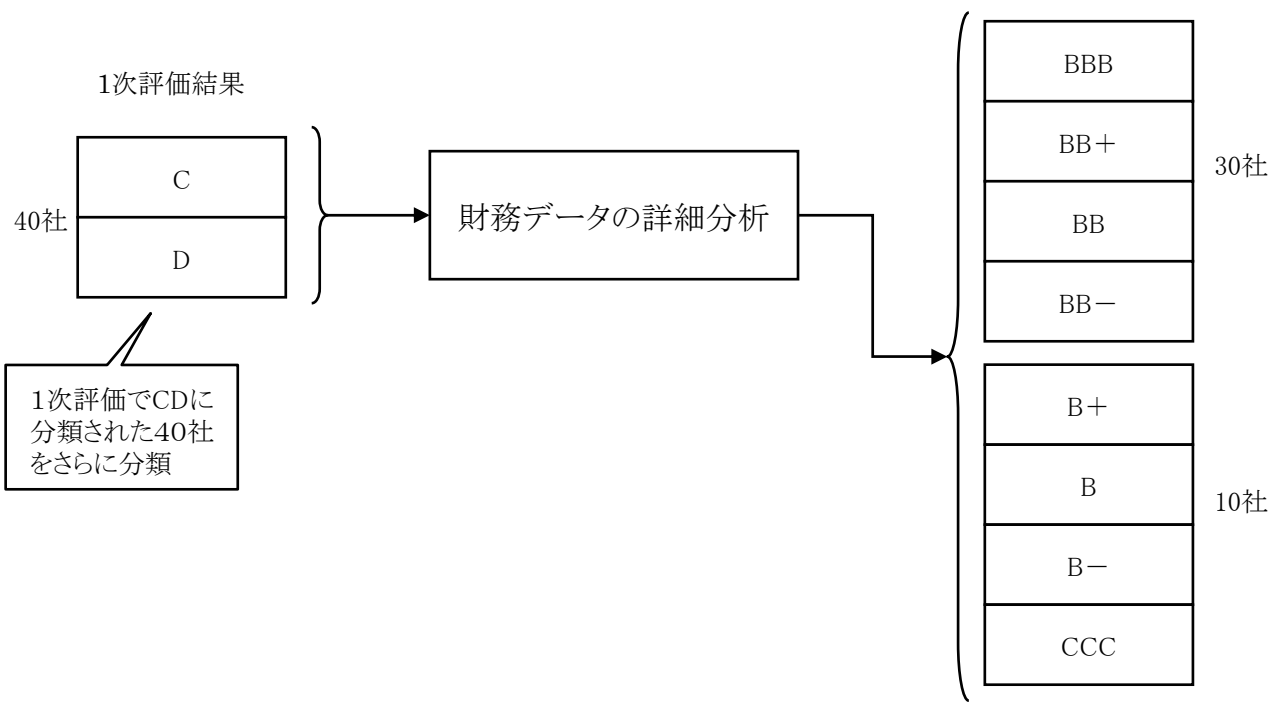
- 全てのサプライヤーの評価を個別に行うことが理想ですが、重要なサプライヤーに絞って評価を実施してもよいでしょう。

（2）1次評価を実施する



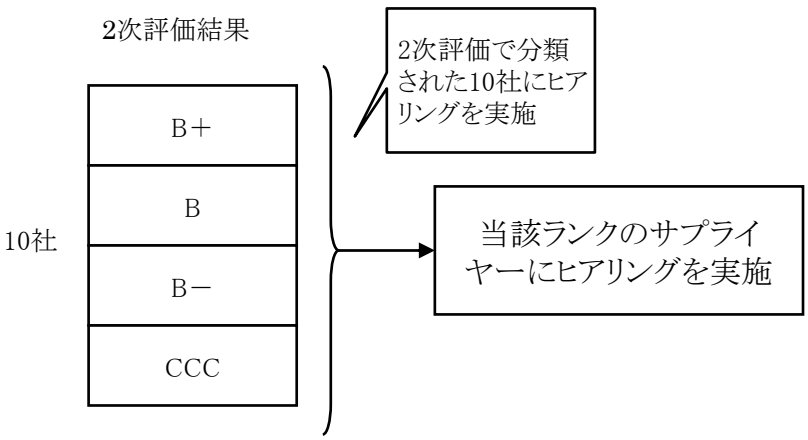
- 社内独自の評価モデルに沿って、サプライヤーから提供された過去1年間の財務データを参考にA、B、C、Dに格付けします。具体的な評価方法に関しては「5.1.5の信用リスク」内で説明します。
- 一律の評価モデルでは国別の事情や企業規模の大小に個別に対応できないため、財務データが良好と言い切れないものは全てC、Dに格付けし、2次評価で個別企業を細かく査定します。

（3）2次評価を実施する



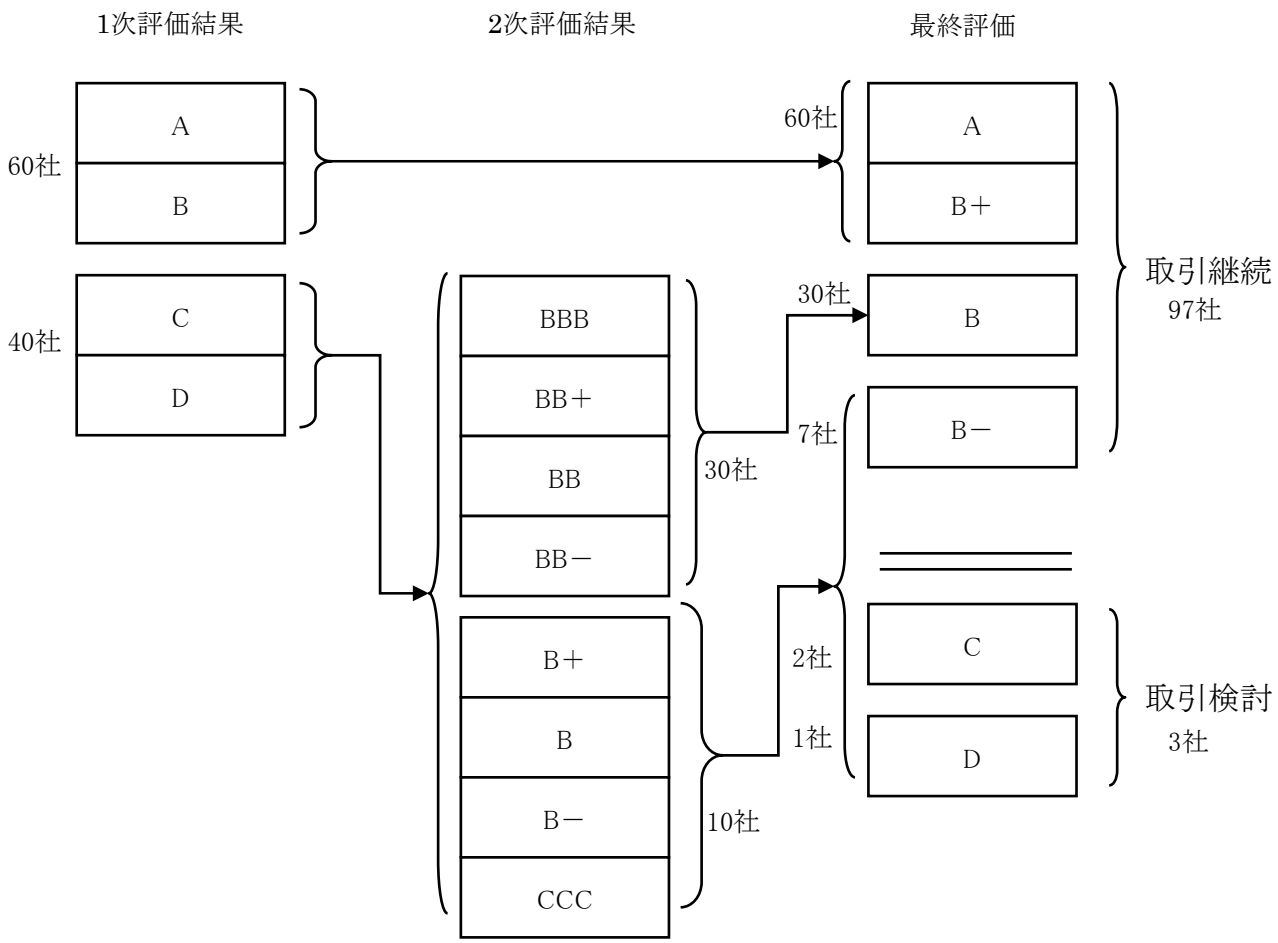
- 1次評価でC、Dに格付けされた企業の財務データを詳細に分析し、再度格付けを行います。
- 2次評価では3期分の財務データ（貸借対照表、損益計算書、キャッシュ・フロー計算書、銀行取引状況、借入推移表、株主構成、事業計画など）を入手し、分析します。
- 1次評価では、評価モデルに沿った定量的な分析になってしまうため、2次評価では定性的な側面も加味し、評価します。
- 分析の過程で問題がある値が確認された場合には、ヒアリングの実施を決定します。

（4）2次評価でB+以下に分類された企業にはヒアリングを実施



- 2次評価でB+以下の格付けがされた場合、当該サプライヤーの経営者や財務部長などに対しヒアリングを実施します。
- ヒアリングの結果を考慮の上、最終的な格付けを決定することになります。

（5）最終評価を決定する



- 最終評価でA、B+、B、B-に格付けされたものに関しては、取引の継続に問題がないと判断されます。
- 最終評価でCに格付けされた企業に関しては、財務部として取引継続の是非の再検討を購買部に提案します。
- 最終評価でDに格付けされた企業に関しては、取引を停止します。
- ただし、サプライヤーとして極めて重要であり財務評価以外に問題がないというような場合には再度総合的に再度評価を行うことになります。

（6）最終評価でCにランクされた企業への対応

① 財務部からの取引継続是非の提案をもとに、開発部、購買部（担当バイヤー）、財務部、サプライヤーでリスクコミッティーを実施。アクションプランを策定します。
② アクションプランを役員報告会で報告し、承認を得ます。
③ サプライヤーと財務部、購買部が協同してアクションプランを実施していきます。
④ アクションプラン実施状況を把握するために、月1度はサプライヤーと会合を持ちます。

- アクションプランが計画通りに実施されている場合には、取引先として問題ないと判断します。
- 本評価は取引を停止するかどうかを目的とするのではなく、サプライヤーとの安定的な取引実現のためのものなので、共にアクションプランを実施し財務体質の改善を図ることで安定的な取引を実現させます。
- この企業では、サプライヤーと非常に密接な関係を持っているため、ここまでの綿密且つ詳細な改善策を協同で実施することにしています。

注） この事例内で使用した社数とその割合は架空であり、目安となるものではありません。

製品要因リスク対策 – 現場作業員にリスク意識をもたせる

現場作業員が作業時に利用するマニュアルにリスク要素を盛り込むことで、リスクに対する高い意識を日常的に持たせることが可能になります。

A工場作業手順書 / 梱包作業手順		
・エプロン　・懐中電灯　・ゴーグル ・手袋　・トランシーバー ・マスク	作業上のチェックポイント	リスク要素
トランシーバーで指示の出た缶詰を確認する	ゆがみや凹みが無いか確認する	品質異常につながる
段ボールに梱包していく	賞味期限が同じか確認する	一部商品に賞味期限切れが起きる
製造場所、タンク名の入ったラベルを貼る	記載が正しいか確認する	不具合が生じても、直ぐに確認が取れない
● ● ●	作業時に確認すべき内容を記載すると同時に、その確認がなぜ行われなくてはならないのか＝リスクにつながるという意味を手順書に記載する	

- このような作業手順書にリスク要素を盛り込むことで、作業時のチェックひとつひとつに「なぜそれを実施するのか」という意味付けが可能になり、リスクに対する理解と認識が深められます。
- このような「なぜ」を伝達することで作業を行う社員一人一人のリスクに対する意識が高まり、ひとつひとつの作業に責任をもって取り組むことができるようになります。このような取組みの姿勢がリスクの発現を防止します。
- 昨今では雇用形態の変化により、正社員の減少、属人的スキルが伝承されていないなどの問題が顕在化してきています。こうした変化に伴い、従来では属人的なスキルによって未然に防がれていたリスクの発現可能性が拡大しています。従って属人的なスキルに頼らず、詳細に作業上のチェックポイントとその理由を明文化し示すことには大きな意味があるといえるでしょう。

製品要因リスク対策 – 管理・監督者による現場へのリスク意識醸成

ある企業では工場事故リスクの要因を分析した結果、工場で発現する事故の根本的な原因は不安全行動によるものだとの結論に達しました。

管理・監督者が社の規定や常識に沿わない不安全な行動をひとつひとつ観察し、問題があれば是正していくことが工場事故リスクの発現を予防するために必要であると言えます。

以下ではデュポン株式会社で安全対策のために運用されている「行動災害防止プログラムSTOP」の中の管理・監督者用STOPを紹介します。デュポン株式会社では不安全行動を是正し、再発防止することをこのプログラムの目的としています。

管理・監督者は現場に足を運んで観察する

管理・監督者は必ずこまめに現場に足を運んで、安全に関する観察を行う必要があります。

観察上注意すべきポイントを決める

工場内のルールが守られているか観察する

- 管理・監督者は現場を観察する責任があることをまず自覚する必要があります。必ず現場に出向き、自らの目を通して観察を行う必要があるのです。
- 現場で観察すべきポイントを決定しておきます。そうすることで工場内の安全管理上最も重要なポイントを確実に観察することができます。
- 保護具、作業位置、作業標準、工具などに関して工場内のルールが遵守されているかどうかをポイントに観察します。

不安全行動には質問で措置を行う

現場での甦安全行動には、管理・監督者から質問を行うことで、現場作業員に自ら問題意識を持つように促します。

質問1:今行われている不安全行動によって、予期しない事態が起こった場合、どのような結果をもたらすか

質問2:もっと安全に仕事をするためには、何をすればいいか

- 質問1によって相手のリスク意識を高め、続けて質問2によって相手に自律的な行動改善を促すことができます。

なぜ直接的に改善要求をするのではなく、このような方法を取る必要があるのでしょうか。その理由は以下3点にまとめられます。

管理者側の一方的な改善要求だけでなく、現場の理解・納得が伴うことでより効果的な改善が期待できる

- 世代ギャップや雇用環境の変化などにより、管理者側からの一方的な改善要求がとおりにくくなりつつあります。

作業者自身の言葉で語らせることで、作業者のリスクマネジメントに対する関与を引き出すことができる

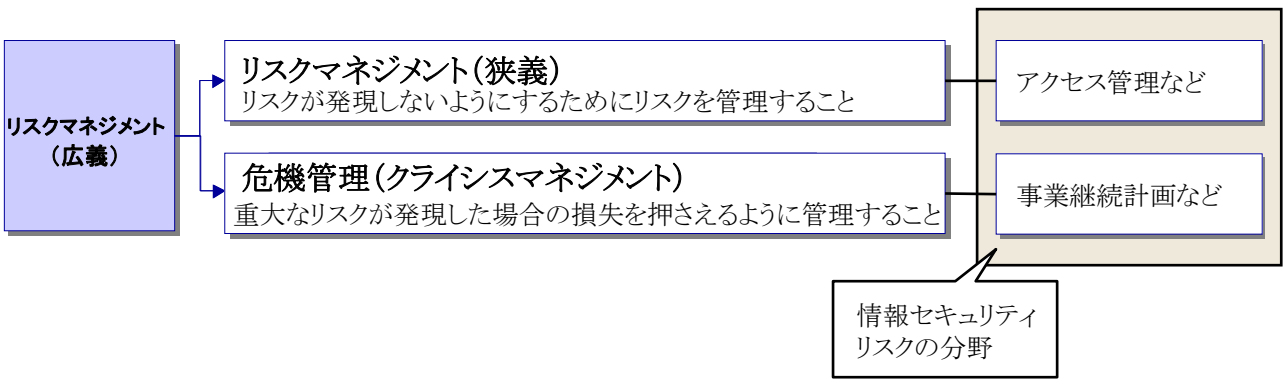
管理・監督者が想定している以上の意見やアイディアを作業者から出してもらうことができる

こうした管理・監督者による日常的な現場へのリスク意識醸成努力が、工場事故リスクの防止に役立ちます。

5.1.3　情報セキュリティリスク

一般にリスクマネジメントを広義にとらえると、リスクが発現しないようにするために実施する管理（狭義のリスクマネジメント）と重大なリスクが発現した場合の損失を押さえるための管理（クライシスマネジメント、以下 危機管理）の2つの側面からなりたっています。

情報セキュリティにもこの枠組みは当てはまります。例えば日々の運用に関わってくるアクセス管理などはリスクが発現しないようにするために実施する管理にあたり、災害発生時などにおける事業継続計画などは重大なリスクが発現した場合の損失を押さえるための管理に該当します。



危機管理はリスクが発現しないようにするために実施する管理（狭義のリスクマネジメント）に比べ情報セキュリティという軸だけでとらえることが難しく、むしろ危機（発現したリスク。例えば地震、社会インフラの停止など。）に対して会社の事業継続のためにどう対応していったらよいか、という軸で捉えたほうが適切な場合が一般的です。
このようなことから危機管理と狭義のリスクマネジメントは分けて検討されるべきことではありますが、これらふたつが不整合を起こさないように検討され、両方の管理が統合的になされるような体制を構築しておくことに留意する必要があります。

なお、情報セキュリティのリスクを考える場合には、以下の3つの視点からのリスクを想定するのが一般的です。

①機密性の欠如
「機密性」とは「アクセスを認可された者だけが情報にアクセスできることを確実にすること」です。機密性の欠如は情報漏洩につながります。
②完全性の欠如
「完全性」とは「情報及び処理方法が、正確であること及び完全であることを保護すること」です。完全性が欠如してしまうと情報の内容の正確性が保てなくなります。
③可用性
「可用性」とは「必要なときに情報及び関連する資産にアクセスできることを確実にすること」です。可用性が欠如してしまうと使いたいときに必要な情報が使えなくなってしまいます。

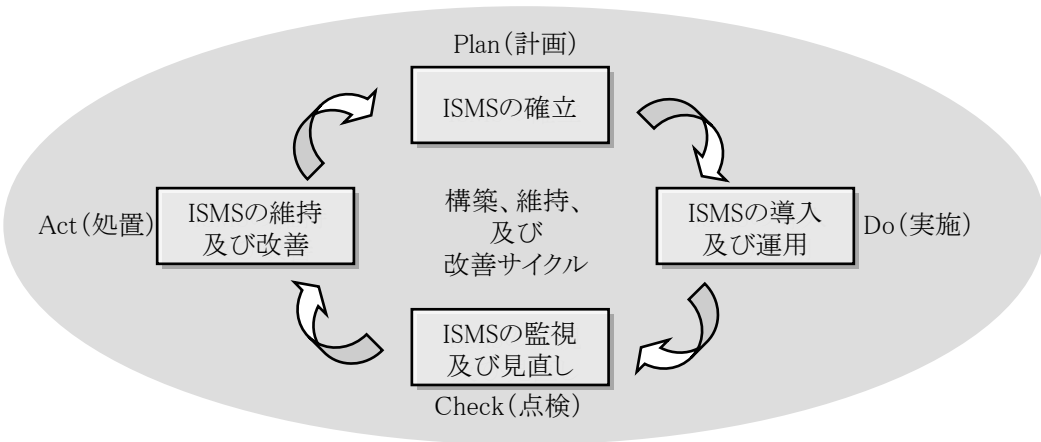
情報セキュリティマネジメントのPDCAサイクル

情報セキュリティについてのリスクマネジメントの枠組みとしては、やはりこれも一般のリスクマネジメント同様に、PDCA(Plan-Do-Check-Act)の管理サイクルに基づく管理を実施していく、と言えます。

実際ISMS認証基準などにおいても、情報セキュリティ・マネジメントはPDCAモデルにて実施されるべきことが示されています。

ISMS認証基準とは財団法人 日本情報処理開発協会が実施している情報セキュリティマネジメントシステム(Information Security Management System:ISMS)適合性評価制度で使用している情報セキュリティに関する認証規格です。

この基準は、ワールドワイドで情報セキュリティマネジメントシステムの規格として広く活用されているBS7799をベースとして作成されており、情報セキュリティの管理に関わる事項が広く網羅的に示されております。



『情報セキュリティマネジメントシステム適合性評価制度 -ISMS認証基準(Ver.2.0)-JIP-ISMS100-2.0 』 より作成

Plan:ISMSの確立

情報セキュリティについて組織としての方針を確立(情報セキュリティポリシーの策定)

リスク分析を実施しどのようなリスクが存在しているのかを把握する

リスク対策を策定する

- 「組織の全般的な基本方針及び目標に沿った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連する情報セキュリティ基本方針、目標、対象、プロセス及び手順を確立します*。」

Do:ISMSの導入及び運用

リスク対策を実装・運用

社員への教育

- 「Planで策定された情報セキュリティ基本方針、管理策、プロセス及び手順を導入し運用します*。」

Check:ISMSの監視及び見直し

日々の活動や偶発的な事態に関する事項を監視

定期的な監査

- 「情報セキュリティ基本方針、目標及び実際の経験に照らしてプロセスの実施状況を評価し、可能な場合これを測定し、その結果を見直しのために経営陣に報告します*。」

Act:ISMSの維持及び改善

Check結果を反映した是正措置

再発防止のための予防策の実施

- 「ISMSの継続的な改善を達成するために、マネジメントレビューの結果に基づいて是正処置及び予防処置を講じます*。」

＊『情報セキュリティマネジメントシステム適合性評価制度 - ISMS認証基準(Ver.2.0)- JIP - ISMS100-2.0 』より一部修正

以降においては、情報セキュリティに関するリスクマネジメントのPDCAサイクルにかかるいくつかの事項について説明します。

具体的には、Planフェーズにかかる事項としてリスク分析について、Doフェーズにかかる事項として運用管理および教育について、Check/Actフェーズにかかる事項として監査・点検について、説明します。

Plan ー 情報セキュリティにおけるリスク分析

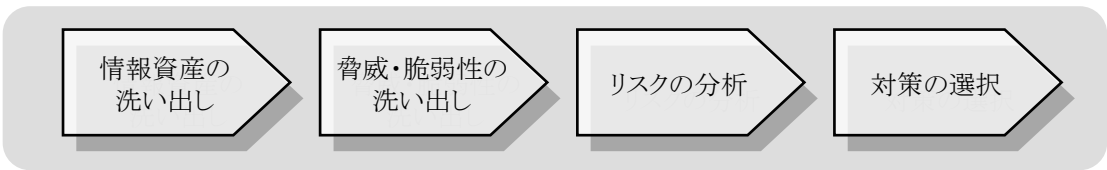
ひとくちにリスクマネジメントを行う、といってもその管理すべき対象が何であるかをきちんと把握しないことには始まりません。これを行う作業がリスク分析です。情報セキュリティのリスクマネジメントにおいてもリスク分析を実施することで、どのようなリスクがあるのかということをまず識別します。その後に対策を講じるべきリスクのレベル（残存するリスクの許容レベル）を設定し、しかるべき対策を講じ、その対策の有効性をモニタリングします。

リスクの対策の種別としては、一般にリスクの回避、リスクの予防・軽減、リスクの分散・集中、リスクの移転、リスクの保有がありますが、情報セキュリティ対策もこの分類の形態のどれかに属する形に整理できます。これら対策の種別のうちどの対策を選択するかを、リスクの影響度、発生可能性、コストなどを勘案し検討します。

情報セキュリティにおけるリスク分析の流れ

ここでは情報セキュリティにおけるリスク分析についてイメージを持てるように、その作業のおおまかな流れとポイントについて簡単に説明します。具体的な詳細については、既にISMS適合評価制度やBS7799などに関する書籍で多くとりあげられていますので、そちらの書籍をご参照下さい。

情報セキュリティにおけるリスク分析はおおむね次の流れで実施されます。



(1) 情報資産を洗い出す

リスク分析の最初には、リスクの対象となる資産の洗い出しを行います。情報セキュリティで保護する対象は“情報資産”となりますので、まずはこの情報資産の洗い出しを行う必要があります。

◆ 情報資産の例

電子化されコンピュータに格納されているデータ

紙の上に印刷された文字や絵などの情報

電子化されたデータを供給する仕組みである情報システム

情報資産の洗い出しにおいて、どこまで細かく作業を行うか、ということが疑問として上がるかもしれません。その場合には、リスク分析の目的に立ち返って考えると良いでしょう。この段階で行うリスク分析は、事業体全体としてどのような種類の情報を扱っていて、それがどのような価値を有していて、どのような脅威・脆弱性に曝されているのか、をあぶりだすのが目的であるのが一般的です。従って、日常作業における扱われ方、有する価値、などを考慮し同じようなものに対してはある程度の大きな単位でくくってしまってもその結果に大きな差異はでない、と考えられます。伝票1枚1枚を情報資産の単位ととらえ、それらについて具体的な脅威が何であるか、を検討しだすととてつもない作業量となり、情報資産の洗い出し時点で息切れしてしまうということにもなりかねません。

(2) 脅威・脆弱性を洗い出す

情報資産が洗い出されたら各情報資産について脅威・脆弱性を検討します。もちろんすべての脅威・脆弱性を完璧に洗い出すことは不可能ですが、なるべく漏れのないように行う必要があります。そのためには、情報セキュリティの3要素と脅威の種別を考慮するとよいでしょう。

すなわち、「人」「自然が引き起こす事象」「情報システム」が「情報の漏洩(機密性の欠如)」、「情報の改ざん(完全性の欠如)」、「情報が使えない状態の継続(可用性の欠如)」を引き起こすのはどのような場合か、という視点で洗い出していくことは漏れを小さくする上で有効です。

(3) リスクの分析を行う

情報資産についての脅威・脆弱性が洗い出されたら、次にそれらについてのリスクの大きさを分析します。

一般に資産価値・脅威・脆弱性の程度はその企業の環境などを考慮した基準値を設けた上で数値で表し、その後評価された資産価値・脅威・脆弱性の程度を表す数値を勘案してリスク値を判定します。この基本的な考え方は、情報セキュリティ以外の一般的なリスク分析と同じです。すなわち

情報セキュリティのリスク値は、以下の関数で表されます。

リスク値 ＝ f (資産価値の程度、脅威の程度、脆弱性の程度)

リスク値を求める数式としては以下の方法が一般的です。

資産価値・脅威・脆弱性の値を乗じる方法:
リスク値 ＝ 資産価値の程度 × 脅威の程度 × 脆弱性の程度

資産価値、脅威、脆弱性の値を足し合わせる方法:
リスク値 ＝ 資産価値の程度 ＋ 脅威の程度 ＋ 脆弱性の程度

資産価値、脅威、脆弱性の値を乗じる方法は、足し合わせる方法に比べ、リスクの大きさの度合いの違いが顕著に現れるという特徴があるので、特にリスクの大きなものを絞り込みたい場合に有効です。

ここで判定されたリスク値が一定以上のものについて追加の対策を検討していく、という方針で対応しているのが一般的です。

(4) 対策の選択を行う

各情報資産についてリスクの評価が終わった後には、その内容にあわせた適切な対策を選択します。すなわちリスクとの付き合い方(このリスクは回避するのか、移転するのか、保有するのか等)を検討することになります。

対策の検討においては、ISMS認証基準などの基準を参考にすることも可能です。

事例 情報セキュリティのリスク分析シートの例

情報資産はデータ・紙・その他の形態など意識して洗い出します。

情報資産の管理状況を把握するため、情報資産の開示範囲や保管場所などについて記述します。

実務担当者の方が認識している機密性・可用性・完全性の観点からの想定脅威を記述します。
その脅威に対し現状の対策が不十分である程、脆弱性は大きくなります。

脅威・脆弱性・情報資産価値をその大きさに応じて順番に「3(大きい)、2(中程度)、1(小さい)」などの数値で表し評価します。
ここで決められた数値をもとに現状のリスク値を判定します。

No.	情報資産	具体例	開示(利用)範囲		保管(保存)場所	保管(保存)状況	想定脅威		リスク評価		
			社内	社外			具体的内容	現状対策	脅威	脆弱性	資産価値
1	見積依頼	見積依頼書 見積依頼済みDB 御見積書	○○部	社内のみ	紙は○○部キャビネ 電子データは○○システム	キャビネは鍵がない ○○システムは作業グループごとにID・パスワードでアクセス制限している	部内の人間が故意に見積関連データを複製/持ち出すことにより、競争相手に製商品価格情報が流出する	特に無し。	1	2	2
2	受注(販売)	月次販売実績DB 月別販売予測DB 販売申請書	○○部	申込書のパンチ会社	紙は○○部キャビネ 電子データは○○システム	キャビネは鍵がない ○○システムは作業グループごとにID・パスワードでアクセス制限している	部内の人間が故意に販売データファイルにアクセス権を設定することにより、ファイルが利用出来なくなる。	管理者以外には各種設定が不可能な設定としている。	3	1	3
3							月次で販売データを取引先に送信している為、誤って送信して販売データが他の取引先に漏洩する。	特に無し。	1	2	3
4	業務手順書	稟議書回覧手順書(ファイル) 作業標準書(ファイル) 業務フロー(ファイル)	△△部	社内のみ	△△部部門サーバ	アクセス制御なし	xxxからの依頼に基づき関係書類を送付する際、誤って送信することによる情報の漏洩。	特に無し。	2	3	1
5							関連書類を誤ったディレクトリに保存することによる情報の書き換え。	参照のみの設定にしている。	3	1	1
6							誤ってフォルダのアクセス権を設定してしまうことにより、部内の他の人が利用出来なくなる。	管理者以外には各種設定が不可能な設定としている。	1	2	1

情報セキュリティにおけるリスク分析の留意点

ここでは情報セキュリティにおけるリスク分析の留意事項についていくつか列挙します。

バランスを考える

- 特に初めてリスク分析を行う場合には、どの程度のことを行えばよいのかがわからない、という不安感からか、完全主義を目指した作業に陥る傾向が強いようです。しかしながら前述の情報資産の洗い出しにおいて触れたように、すべてにおいて詳細な部分にまで検討を行いだすと膨大な期間と作業量を要することになってしまいます。
- リスク分析もいくつかのレベルがあります。事業の方向性を決めるために全体感をもって行う場合とある具体的な対策の実装方法を決定するために行う場合とでは、掘り下げるレベルや詳細度は当然違ってきます。特にPlan段階で行うリスク分析の目的は「事業の方向性を決めるため」となりますので、幅広く全体的に行う必要はあるかもしれませんが、個々の対策の具体的な実装要件を導き出すわけではないのでそこまで深堀した形で行う必要はありません。幅広く全体をとらえた上で、特にリスクの高そうな部分を必要に応じて掘り下げる、という方法もとれるでしょう。
- リスク分析はこの辺りに留意しながら、適切なバランス感覚を持って実施していく必要があります。

リスク分析の機会を有効に活用する

- リスク分析においては、情報資産を扱う現場の人々の関与が必要です。なぜならば、その情報資産がどんな風に扱われていてどんな脅威にさらされているか、は現場の人でないとわからないからです。しかしながら別な観点からいえば、このリスク分析は全体的に行われるので、現場の人を巻き込むということは非常に大掛かりなイベントになることが想像されます。
- これを考えるとリスク評価の遂行ではプロジェクト管理をきちんと行っていかないと最後まで完遂できない、という側面に留意する必要があります。しかしながら反面こういう場をうまく利用していくという観点で捉えることもできます。すなわち、リスク分析を行う事を、現場に情報資産の価値を再認識してもらう絶好の機会、と考えるわけです。“情報セキュリティを確保できる風土”を作り上げるための足がかりのひとつ、という視点で教育的な要素を取り込んでリスク分析プロジェクトを設計する、ということも一案かもしれません。

組織体として承認された結論を導き出す

- リスク分析の結果は、施される対策の要件となります。その要件は、組織体全体で一様に同じ対策で守られなければなりません。同じ情報資産なのに、部門によって守り方のレベルが違ってくる、というようなことは本来あってはなりません。なぜなら情報資産の価値は組織体全体としての見解であるべきで、それが部門によって違うということはありえないからです。
- 組織体としてどういう情報資産が価値のあるものなのか、どういう守り方をしていかなければならないのか、という認識を統一するためにも、リスク分析の結果は組織体全体として承認されたものでなくてはなりません。その意味において、リスク分析の結果はトップマネジメントによる承認がなされるべきです。

Do ー 情報セキュリティにおける運用管理

情報セキュリティの運用管理の全体像の捉え方はさまざまなものがあり、必ずしもこうでなければならない、といった定説があるものではありません。

ここでは情報セキュリティの運用管理の領域を、人的管理、情報資産管理、物理的管理、情報システムの開発に関する管理、情報システムの運用に関する管理、規程類の管理、事故管理に区分し、それぞれどのような管理が必要なのかについて紹介します。

情報セキュリティ運用管理

ここでは情報セキュリティの運用管理の領域を、人的管理、情報資産管理、物理的管理、情報システムの開発に関する管理、情報システムの運用に関する管理、規程類の管理、事故管理に区分し、それぞれどのような管理が必要なのかについて紹介します。

人的な管理を行う

人的管理とは、情報セキュリティの保護の対象となる情報資産を扱う人間の管理を指します。例えば次のようなものがあげられます。

内部の人的管理

- 情報資産を扱う人間ひとりひとりが与えられた教育を受けているかどうか、あるいはその理解度は望まれるレベルに達しているのか、などの管理がこれにあたります。

外部の人的管理

- 業務の外部委託やアウトソースなど第三者に情報資産を扱わせる場合に必要となる管理がこれにあたります。ここでの管理項目としては、当該第三者との契約事項としてどういうことを盛り込むべきか、についても含まれます。

情報資産の管理を行う

情報資産管理とは、情報資産そのものの管理を指します。例えば次のようなものがあげられます。

紙や電子データなどの情報そのものの管理

情報が格納されている様々な媒体の管理

電子データを取り扱うIT資産の管理

- 情報資産管理で大切なことは、上で示された情報資産が分類されており、管理の対象として認識できる単位が明確になっていることです。こうした分類がなされることにより、はじめてその単位ごとの重要度に応じた管理を実践していくことが可能になります。管理の対象が不明確なまま管理を実践することはできません。例えば、顧客情報か否かという分類があってこそ、顧客情報の重要度を勘案したうえで“施錠可能な場所に保管する” という管理要件があきらかになります。（これはあくまでも例であり、顧客情報が施錠保管されなければならない、という意味ではありません）
- 情報資産管理でもうひとつ大切なことは、情報資産のライフサイクルという視点を取り入れることです。情報資産も生まれてから消滅するまでいくつかのプロセスを経ることになります。例えば、企画部門の担当者が作成する企画書であれば、作成した企画書を会議で発表するため複写したり、関連部門に配布したり、自部門のキャビネに保管したり、あるいは廃案になった場合には廃棄したり、というようないくつかのプロセスを経ることになります。こういったライフサイクルの要所において、どんな管理を行えばよいのか、ということが検討され明確化される必要があります。

物理的な管理を行う

物理的管理には、例えば次のようなものがあげられます。

情報資産を扱う場所に関する管理

- 例えば、施錠が必要とされる部屋がきちんと施錠されていることの確認やかぎの管理がどのように行われているか、などが管理の対象となります。

入退館や入退室に関する管理

- これには入退館（室）の記録の管理や入館（室）証の発行・取り消しの管理などが含まれます。

情報資産やそれに関わるものの移動の管理

- 特にセキュリティ上重要度が高い場所へ持ち込まれるもの、あるいは持ち出されるものが正当なものであることや、持ち込み・持ち出しが正当な手続を経たものであること、などの管理が対象となります。

情報システムの開発に関する管理を行う

情報システムの開発に関する管理は、開発される情報システムに必要なセキュリティ機能が組み込まれるようにするための管理で、具体的には例えば開発のフェーズごとにセキュリティ機能の組み込みに対するレビューを行うことなどがあげられます。

情報システムの運用に関する管理を行う

情報システムの運用に関する管理には、例えば次のようなものがあげられます。

情報システム上で使用されるユーザの登録・変更・削除の管理や、これらユーザによる情報システム上のデータへのアクセスの管理

- ここでいうアクセスの管理とは、例えば情報にアクセスできる権限の付与・除去をタイムリーに行うことや、アクセスログを取得して異常がないかの監視、あるいはアクセスログの定期的な監査、さらにはアクセス権限の付与の承認ルートの明確化、などが含まれます。最近ではこのようなアクセス管理やユーザ管理をまとめて、アイデンティティ・マネージメントと呼ぶことがあります。アイデンティティ・マネジメントは情報システムというバーチャルな世界で、情報資産を保護するための手法といえます。例えば物理的な世界では、機密書類は鍵のかかるキャビネに保管し、許可された人だけがキャビネの鍵を開けることができる、などの管理を行いますが情報システム上に格納された電子データにも似たような管理が必要です。
- すなわち、電子データを触る人が誰であるかをバーチャルな世界で正しく識別し、その当人が本当にその電子データにさわっていいのかどうか、をきちんと管理していく必要があります。これを成すための考え方として、最近提唱され始めているのがアイデンティティ・マネジメントなのです。アイデンティティ・マネジメントを取り入れることにより、情報システム上での情報資産たる電子データがより確実に保護されるようになると考えられます。

不正アクセスに対する管理

- これには、ハッカーなどの攻撃の監視、情報システムへのログイン状況の監視、情報システム上の資源へのアクセス違反が起きていないかの監視、などの各種の監視があげられます。
- また、定期的に情報システムのセキュリティ対策が妥当であることを確認するために、擬似的に情報システムへの侵入を試みたり、脆弱なパラメータ設定がされていないかをチェックしたりすることもこの管理のひとつです。
- さらには、そのような脆弱性の情報や製品などのセキュリティホールの情報を収集したりその内容を検討したりすることも、この管理に含まれます。

規程類の管理を行う

規程類の管理とは、言い換えれば文書化されたルールの管理といえるかもしれません。情報セキュリティのルールはセキュリティポリシーを核とし、様々な規程の中に盛り込まれることになりますが、このルールは企業の内的環境や外的環境に応じて変化します。このような変化にタイムリーに対応していく必要があります。規程類の管理には、例えば次のようなものがあげられます。

各種ルールの定期的な評価

必要に応じた内容の改訂

各種規程類の改廃の管理

改訂部分の周知

事故管理を行う

事故とは、日常の業務に組み込まれた情報セキュリティのあるべき運用から逸脱した事象、といえるかもしれません。ここで情報セキュリティにかかわる事故となる事象をすべて列挙するのは困難ですが、イメージを描いていただくためにいくつかの例をあげます。

◆ 情報セキュリティ事故例

ハッカーの攻撃によりホームページが書き換えられた

ウィルスに感染した

Webアプリケーションソフトにバグがあり扱っている個人情報が漏洩した

建物への入館カードをかねている社員証を紛失した

電車に機密書類を置き忘れた

ノート型パソコンを盗まれた

このような事象は、もちろん起こらないことが望ましいのですが、100％起こらないようにすることは困難かつ非現実的です。情報セキュリティに関する事故管理としては、例えば次のようなことがあげられます。

◆ 事前管理事項例

できるだけこのような事象が起こらないような事前の対策を試みること

起こってしまったときに速やかに、かつ適切に対応できる体制を整えておくこと

◆ 事後管理事項例

タイムリーに対処し2次的な事象の発生や被害の拡大を避けること

再発防止のための手段を講じること

情報セキュリティにおける人的管理と教育

ここでは、特に前述の人的管理のひとつである教育についてもう少し触れます。なぜならば結局のところ運用を実践するのは人間であり、人間に適切な運用を行わせるにはまずそれを教育する必要があるからです。運用を成功させるための第一歩は教育にあるといえます。

ひとくちに教育といっても、“情報セキュリティ”ということで何を教えるべきなのでしょうか。

何をなぜ守るのか：情報セキュリティを運用することの理由を伝える

- “何をなぜ守るのか”の教育は、情報を扱うすべての人間に一様に実施する必要があります。
- この教育におけるポイントは、まず事業において情報がいかに大切であるか、を認識してもらうことであり、これがすべての出発点になると考えられます。「情報は第4の経営資源である」といわれるようになって久しいですが、残念ながら一般的な日本人の感覚としては、まだまだ情報の価値に対する認識は薄いのではないか、と思われます。例えば机上に百万円を放置する人はいないと思いますが、同じ価値を有すると思われる情報の扱いとなるとぞんざいであったりしないでしょうか。
- “何をなぜ守るのか”の教育は、“情報セキュリティ”というような難しそうなイメージを抱かれる話ではなく、事業における情報の価値を説くことから始めるのがよいでしょう。価値が伝われば、おのずと良心のある人間であればぞんざいな扱いはしなくなり、ひとりひとりがそういう意識を持つようになればそこから“情報を守る”というカルチャーが生まれてくることが期待できます。

どうやって守るのか、どういうことを実施するのか：情報セキュリティを運用するための技巧を伝える

- “どうやって守るのか”の教育は、必ずしも情報を扱うすべての人間に実施する必要はないかもしれません。なぜならば、この内容は各自の業務によって変ってくる可能性が高いからです。（中には、“ウィルス対策ソフトの使い方”のようなおよそ全員に対し実施すべき事項ももちろんあります）

では、こういった教育はどのように実施していけばよいのでしょうか？すべての情報を扱う人をターゲットに教育を実施することは容易ではありません。

階層型で実施する

- 例えば情報セキュリティ委員会の事務局などが現場部門の先生となる人に教育し、教えを受けた先生がこんどは現場の人を教育していく、というような階層型に実施していく方法です。場合によっては、これは2階層ではなく、3階層以上になることもあります。

eラーニングを活用する

- 人数が多い場合に使われるやり方としては、いわゆるeラーニングの活用があげられます。特に集中管理が可能なツールを活用すれば、受講や修了の管理やテストによる理解度のチェックなども可能です。

このようにいくつかの方法がありますが、忘れてはならないのはこの教育は“時間をかければいい”というものではないということです。あくまで目的は、受講する人が“日常の業務の中で情報セキュリティを守れる”ようにする下地を作ることなので、これを達成する合理的な方法や計画を検討する必要があります。

Check、Act ー 情報セキュリティにおける監査・点検

情報セキュリティの要求事項は日常の業務の中に組み込まれて様々な形で日々運用されます。しかしながら気になるところは、決められたルールが実際に現場で守られているかどうかです。情報セキュリティも他のリスクマネジメント同様、何かルールを決めればそれでおしまい、というものではありません。むしろルールが決まった時点が出発点であり、そこから日々決められたことを守っていく、という果てしない継続が始まるのです。この継続は大変根気のいる作業となります。放っておくといつのまにか形骸化し、ルールはあるが実践されない、ということになってしまいがちです。こうならないように、点検(Check)し必要に応じ処置(Act)を施す必要があるわけです。

情報セキュリティにおける監査・点検

ここでは監査・点検の具体的方法に関して説明します。

情報セキュリティ監査を実施する

- 情報セキュリティ監査については、情報セキュリティ監査基準などを参考に自社内の内部監査人が実施していく方法が考えられます。あるいは、特に専門性が求められる領域については外部の情報セキュリティのノウハウを有する企業に委託する、という方法もあるでしょう。
- いずれにしても監査は実施するだけでなく、監査後に監査の結果見つかった課題についてどう対応していくかを検討し、改善計画を立てて確実にフォローアップしていくことが重要です。

自己点検を実施する

- 現場レベルの自己点検では、隣の部門同士などで相互にチェックしあうクロスチェックの方法があります。例えば、あらかじめ用意されたチェックリストに基づき、ルールが実践されているかどうか、を現場のチェック担当者が確認していくやり方です。このチェックリストは難しいものである必要はありません。むしろ現場でなじみのあるような、「機密の書類は帰宅時に机の上に放置されていないか」のようなもので十分です。こういう自己点検を例えば四半期ごとに行っていけば、現場レベルでルールが再確認されるとともにその遵守が徹底されていくようになります。
- なお、こういった自己点検で違反者が発見された場合、違反したものと違反しなかったものでは、なんらかの違いがでてこないと点検した意味がないので、違いをつける必要があります。ただし、違反といってもこのレベルのチェックで見つかるものは軽微な過失程度であるため、就業規則にあるような罰則をあてはめる必要はないでしょう。(もちろん不幸にして重大な過失などが発見された場合はそれなりの罰則が必要と考えられます)例えば上のチェックリストの例の場合であれば、放置していた機密書類は一旦上長に預けられ、上長への申し出なしには返却されない、というレベルでも構わないかもしれません。
- また、違反者に直接目をむけるのではなく、違反が少なかった部門を表彰するなど社内キャンペーン的な対応をする方法もあります。このあたりは組織の風土を考慮して、その組織に適した対応を検討するのがよいでしょう。

（参考）情報セキュリティに関する情報収集

インターネット上にはセキュリティ対策や事故事例等の情報を掲載したサイトが各種存在します。ISMS導入時の参考にするとともに、導入後も適宜参照して常に最新の情報を把握しておくと良いでしょう。

参考	情報セキュリティ関連ウェブサイト

- 内閣官房情報セキュリティ対策推進室
  http://www.bits.go.jp/
- 経済産業省／情報セキュリティに関する政策、緊急情報
  http://www.meti.go.jp/policy/netsecurity/index.html
- 総務省／国民のための情報セキュリティサイト
  http://www.soumu.go.jp/joho_tsusin/security/index.htm
- IPAセキュリティセンター
  http://www.ipa.go.jp/security/
- 情報セキュリティマネジメントシステム(ISMS)適合性評価制度
  http://www.isms.jipdec.jp/
- 特定非営利活動法人　日本セキュリティ監査協会
  http://www.jasa.jp/index.html
- 警察庁サイバー犯罪対策HP
  http://www.npa.go.jp/cyber/

5.1.4　市場リスク

ここでは、2003年度のテキストで紹介された市場リスクの定義、および市場リスク管理の仕組みを構成する要素、測定手法の定義を確認し、共通の前提知識のもとで説明をすすめていきます。

市場リスクとは
金利や為替、有価証券の価格など、金融市場における様々な要因が変化することにより、保有する資産・負債の価値が変動して損失が発生するリスク

なお、金融市場に限らず市場を広く含める場合もあります。

主な市場リスク

以下に主な市場リスクを挙げます。

主な市場リスク	定義や内容
金利リスク	金利が変動することで、保有する資産のポジション価値が変化して損失を被るリスク
為替リスク	為替レートの変動により、保有する資産ポジションの価値が変化して損失を被るリスク
商品価格リスク	コモディティの現物や先物価格が変動して、保有するポジションの価値が低下することで損失を被るリスク

『事業リスクマネジメントーテキストー 経済産業省 平成16年3月』57-59ページ より作成

市場リスク管理の仕組み

市場リスクを管理する仕組みを挙げます。

主な管理の仕組み	定義や内容
リスク管理体制	リスク管理の組織、フロント・ミドル・バック*という役割分担と相互牽制等管理体制 * フロント・ミドル・バックとは・・・フロントは取引執行部門、ミドルはリスク管理部門、バックは事務部門を意味するのが一般的である
リスク管理方針	デリバティブについては投機は行なわない等の基本的な方針を定めたリスク管理方針
リスク管理規則 関係会社管理規則	子会社においては、金額（最大リスク額）によって親会社の事前承認を受けることを義務づけている等を定めて管理規則

市場リスクの測定手法

市場リスクの測定方法を以下に挙げます。

主な測定手法	定義や内容
感応度分析	ある特定の項目について、その値を変化させたら採算性がどう変化するかを測定する手法。例えば金利1%変化したら損益にどの程度の影響が生じるのかを測定する
ストレステスト	予想するのが困難な通常では考えられない状況や統計的に極めて発生しにくい状況などを想定し、こうしたシナリオのもとでポートフォリオが被る損失を推計すること
VaR (Value at Risk) バリュー・アット・リスク	保有している資産について、保有期間内に特定の確率（例えば1%など)の範囲で生じる最大損失額を統計的に計測する方法
バックテスト	推計されたリスク量と実際の市場変動による損益とを比較することにより、リスク量算出モデルの信頼性を検証するテストのこと

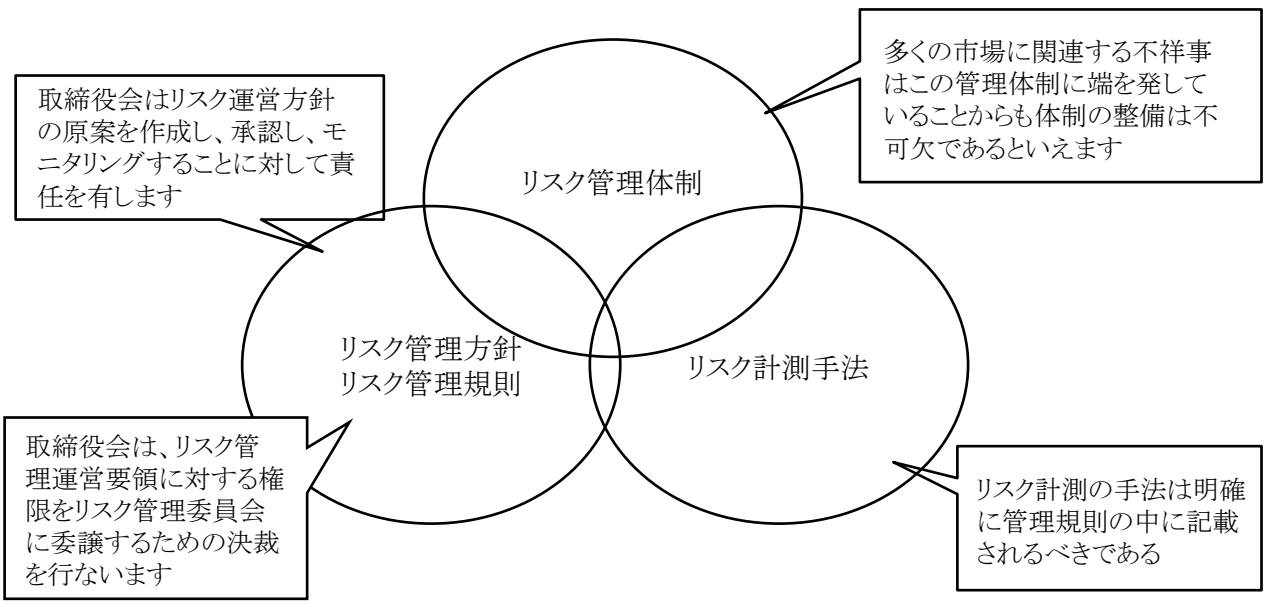
『事業リスクマネジメントーテキストー 経済産業省 平成16年3月』121-122ページ より作成

これらの管理のしくみ、測定手法等について具体的に次ページ以降にて実例を紹介していきます。

市場リスクマネジメント3つの柱

リスク管理体制、リスク管理方針・規則、リスク計測手法、これら3つの重要な柱のどれかが欠けていた場合、重大な損失が発生する可能性があります。

市場リスクマネジメント3つの柱



市場リスクマネジメントにおけるポイント

リスク管理体制－取引執行部門と管理部門を分離してチェック機能を効かせる

リスク管理方針－投機目的、実需に関係のない取引に関する方針を示す

リスク管理規則－リミットや計測手法（ストレステスト・VaR・バックテスト）についても規定する

リスク計測手法－個社のリスク特性にあった手法を選択

- リスク管理体制については定期的な自己評価の実行により有効性を確認します。
- リスク管理方針・リスク管理規則については内部監査の情報の活用をして有効性を確認することが重要です。
- リスク計測手法については外部監査の情報の活用をして有効性を確認することが重要です。

これら3つの柱の点検には自己評価、内部および外部監査の活用も考えられます。

最先端のリスク測定手法を提供するリスクメトリクス グループ（Risk Metrics Group）でも「リスク測定よりもリスク管理に時間を増やすべき」であるとの認識のもと、管理面での重要性を強調しています

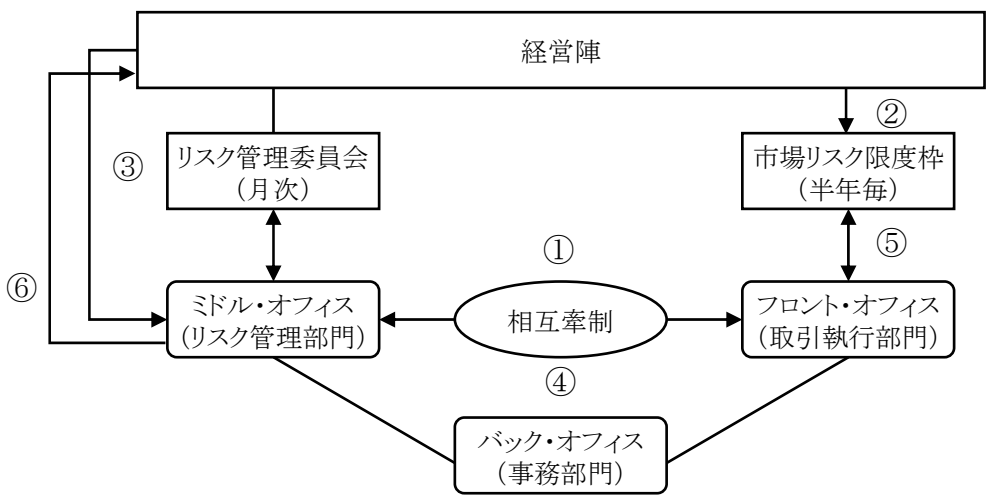
リスク管理体制

市場リスクマネジメントにおいては経営陣の積極的な関与と実務者の日々の管理双方がお互いの役割を果たすときにはじめて有効となります。そのためには以下のようなリスク管理体制に基づき、相互が監視しあう仕組みが必要となります。

市場リスクは経営陣が注意深く、監視し、管理していかなければいけないリスクです

- 相互牽制システムを作り、実行するのがトップの責任です。不祥事が起きた場合、その責任が問われるのも企業のトップです。
- 経営陣は自ら組織のとる市場リスクの限度枠に関心を持ち決定すべきです。
- 経営陣は定期的にレポートされる内容に自ら関心を持ち、理解すべきです。

リスク管理体制(例)



市場リスク管理体制における経営陣の役割

相互牽制
①構築　取引執行部門と管理部門を分離した体制　④実行

取引限度
②決定　市場リスクの限度枠　⑤遵守

レポート
③検証　経営陣への定期レポート　⑥報告

市場リスク管理体制における実務者の役割

取引限度の設定（例）

金融機関においては以下のような取引限度の設定を実施しています。

ロスリミットの80%時点で一度、リスク管理部門に警告が届くシステムになっている

リスク管理部からは80%超の部署、個人の記録が経営陣にレポートされる

一度ロスリミットの80%を越えた部署や個人に対してリスク管理部は今度80%を超えるようなケースにはいつでも取引停止権を発動することができる

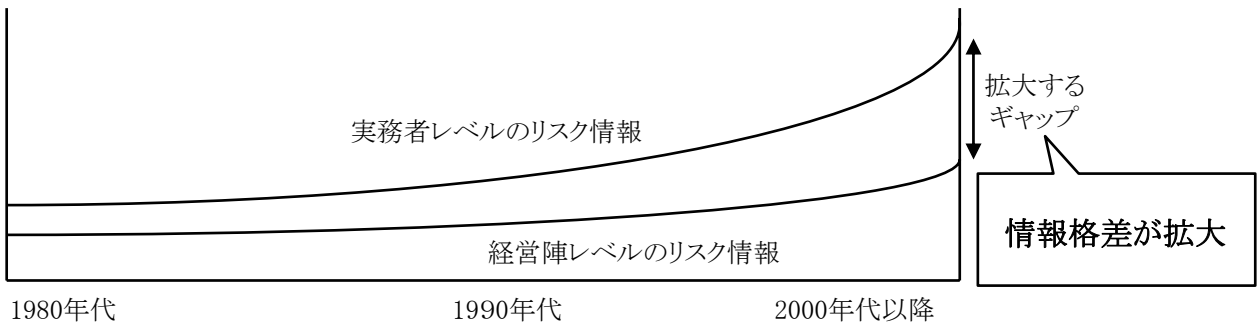
- このようにロスリミットに届く前、何らかの牽制が効く仕組みが必要です

リスクレポートの役割

リスクレポートとは、市場リスク管理部門から、経営陣に市場リスクのマネジメント状況について報告するレポートです。具体的には、株式や債券の時価評価額や、金利、為替リスク等について取っているポジションの最大損失額を報告するといった形で行なわれています。頻度については、金融機関では毎日、事業会社では月1回、四半期に1回等、業種により様々です。また最近では、ステークホルダーに対してのリスク情報の開示もリスクレポートと呼ばれることがあります。

リスクレポートに関する取組み(例)

金融市場・商品の急激な発展により、実務者と経営陣にリスク情報に対するギャップが生まれてきています。



フューチャーシステムコンサルティング株式会社ホームページ　セミナー資料より作成

以下の事例は、このギャップを実務者が認識し、市場リスクのレポートについて経営陣と実務者の双方が共通の認識を持ち意見交換しなければいけないとの発想から生まれた取組みです。

ある企業の市場リスク担当の実務者は市場リスクに関係する金融商品やリスク計測手法等の急速な発展の真っ只中に身を置いていた。そんな中で何とか自分達はかろうじてそれらを理解しているものの、経営陣は本当に理解しているのだろうかという疑問が湧いてきた。

経営陣には定期的な市場レポートをE-mail にて報告していたが、いつも質問もなく反応がなかった。そこで、実務者はE-mailにて報告後、経営陣に連絡をとり確認をとることとした。その結果は予想したとおり、実はレポートを見ていない、何を意味するかわからないといった声が上がったため、毎回簡単な説明を実施し、相互理解を図ることとした。

実務者はリスクレポートに関して、提出するだけではなく、トップの反応を注意深く見て、必要に応じてリスクの状況を説明すべきです

実務者から経営陣へのレポートチェックポイント

トップがレポート内容を理解しているか（報告される数字が何を意味しているか）

トップが本当に知りたいことは何か（常に意識する）

トップからの監視の目を感じるか（感じていないようでは危ない）

- 逆に経営陣からもリスク・レポートに関して、提出を受けるだけではなく、内容については自ら理解し、リスクがどう変化しているのか把握する必要があります。

E-mailや電子掲示板等の電子媒体による報告スタイルが一般化したことで、報告自体は手軽に出来るようになりました。しかし一方で経営陣にレポートを直接持参して口頭で説明するような、直接的なコミュニケーションを持つ機会が減りつつあります。

相互理解の必要性を双方が意識し、確認し合うためのコミュニケートすることが求められています。

リスク管理方針・規程

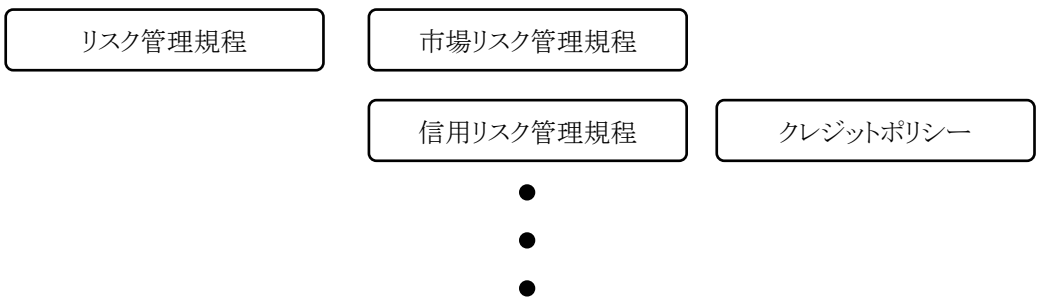
先に述べた管理体制とともに大事なのが管理方針・管理規程です。

市場リスクマネジメントは管理体制と管理方針・管理規程を元に運営されるべきであり、二つが揃ってはじめて正しい運営が可能となります。管理体制も含めて管理規程に記載されるのが理想的です。

また、市場リスク関してはその専門性、および頻繁な変動から、その他のリスクと独立した管理規程が必要です。

以下の管理規程体系（例）を参考にしてください。

管理規程体系（例）



管理方針および管理規程には以下のような違いがあり、双方を考慮の上、作成します。

リスク管理方針の特徴	リスク管理規程の特徴
より経営的な視点：経営戦略	より実務的な視点：実務的詳細
責任の所在：取締役会	責任の所在：リスク管理委員会
やるべきこととやらざるべきことの記述	作業過程や事前対策の記述
管理枠（リミット）	具体的計測手法や実効性を高める仕組みの設定
権限の所在の明確化	職責とその範囲の明記

ジョン・ウェングラー『電力取引とリスク管理』 エネルギーフォーラムより作成

また管理規程には以下のような項目を盛り込むことが必要です。

- 市場リスクの範囲
- 経営基本方針
- 所管
- 社員の責務
- 管理体制・管理上の留意点等

具体的には、次ページの例を参考にしてください。

市場リスク管理規程（例）

（総則）
第1条　この規程は、会社の市場リスク管理について定める。
（市場リスクの範囲）
第2条　この規程において「市場リスク」 とは、金利リスク、為替リスク、商品・コモデティリスク等をいう。
（経営基本方針）
第3条　会社は、市場変動により保有するポジションが被るリスクを最小限となるよう対処する。
（所管）
第4条　市場リスク管理および対策は、リスク管理部の所管とし、その総括責任者はリスク管理部長とする。
（社員の責務）
第5条　社員は、会社の市場リスク管理について、次の債務を負う。
　　(1)　市場リスクが会社の経営において重大な損害を与える可能性があることを正しく認識すること。
　　(2)　市場リスクを管理し、ポジション、評価損益、BPV・VaR等のリスク指標を日次、ないし月次で把握、測定し、経営陣に報告する。
（管理体制の分離）
第6条　取引を実施する部署（フロント）と事務処理を実施する部署（バック）を分離し、リスク管理担当者（ミドル）を配置することにより、相互牽制体制を明確にする。
（管理上の留意点）
第7条　市場リスク管理にあたる社員は、次の点に留意しなければならない。
　　(1) 迅速、かつ、正確に取引を執行すること
　　(2) 具体的、かつ、総合的に管理を行なうこと
　　(3) モデルの有効性を毎月確認すること
　　(4) 取引の進捗状況を適宜適切にリスク管理部長に報告すること
　　(5) 管理の実施において判断に迷ったときは、独断専行せず、リスク管理部長に指示を求めること
（付則）
第8条　この規程は、　年　月　日から施行する。

巨額損失事件からの教訓

市場リスクに関わる巨大な損失は一度発生してしまうと莫大な被害をもたらし、企業の存続さえおびやかす存在です。代表例においても解散に追い込まれた企業があり、影響の大きさを物語っています。

参考　過去の代表的な巨額損失事件

年月	件名	概要	損害額
1998.3	飲料メーカー	デリバティブ	1057億円
1995.9	大手銀行ニューヨーク支店	米国債の売買	11億ドル
1995.3	ガス会社	金利スワップ	119億円
1995.2	英商業銀行	日経平均先物取引	10億ポンド
1994.12	米地方自治体	デリバティブ濫用	17億ドル
1994.12	独エネルギー会社	原油先物取引	30億マルク
1994.4	石油会社	為替取引失敗	1600億円
1993.7	化学会社	為替取引失敗	139億円
1993.2	石油会社	通貨先渡取引の含み損	1663億円
1987.9	化学会社	債券先物取引失敗	286億円

これら近年の金融事故に共通して言えることは、一貫したリスク管理方針・規程というものが欠如していたことです。これらの損失事件を契機に、規制当局の動きが活発になり、一般企業の側でも顕著な反応が見られ、JP.モルガンのリスクメトリクスやバンカーズ・トラストのRAROCなどのリスク管理ツールが表れました。

英商業銀行&大手銀行NY支店からの教訓

- トレーダーがフロントオフィスとバックオフィス双方の権限を持っていた
- 取引所において過大なポジションに対する注意が払われなかった
- 運用担当者はポジション限度を超過して取引していた
- トップは前年の内部検査の結果を黙殺した

米地方自治体&独エネルギー会社からの教訓

複雑な仕組み債を理解していなかった。金利動向の読み違い

簿価で自らのポートフォリオをレポートしていた（損失を認識できなかった）

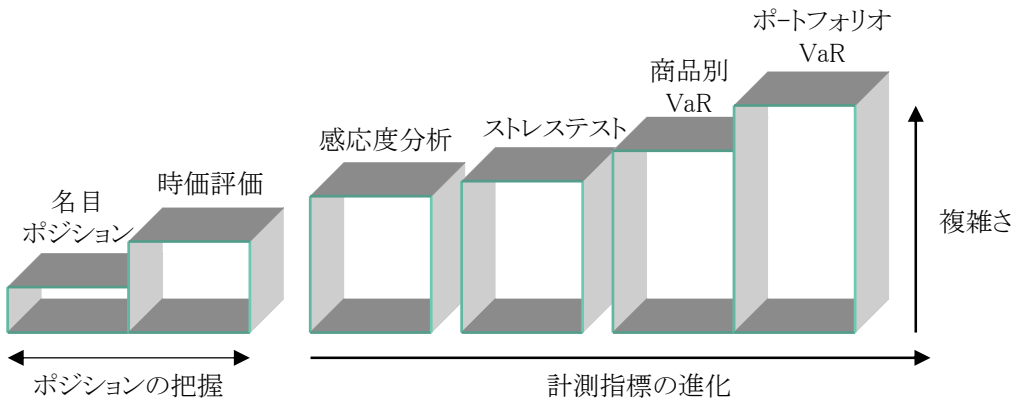
当時は長期（10年間）にわたる先渡契約の市場が存在しなかったため短期の先物市場を利用経由して短期契約を組み合わせてヘッジを行なった。しかしながら短期先物市場が長期価格から乖離したため 損失が発生した

これらの事件は取引執行部門と管理部門の権限分離の重要性やデリバティブ商品利用時の商品知識の確実な理解といった点を教訓として残してくれています。

リスク計測指標の進化

市場リスク計測手法は以下のような進化を遂げてきました。金融機関では既にポートフォリオVaRの活用が始まっています。しかしながら、金融機関以外の事業会社では時価評価や感応度分析(ストレステスト)が一般的な計測手法となっています。

参考　リスク計測指標の進化



三菱信託銀行オペレーショナルリスク研究会編『オペレーショナルリスクのすべて』東洋経済新報社 2002年より作成

- 上図のようにリスク管理指標の進化とともに管理も複雑さを増しています。毎日トレーディングを行なっており、大きなリスクを取っている場合と月に1回、年に1回取引をする場合ではおのずと使用する管理指標も違ってきます。
- 最も大事なことはそれぞれの取引にあったリスク管理指標を使うことです。リスク管理方針、規程を守っていること等が重要です。

事業会社における時価評価管理の特徴

「資産、負債、オフバランス商品などを、その時々の市場の価格で評価する方法が時価評価で、取得原価で評価する方法に比べて、リスクの状況や資産価値を正確に表すという特徴を持っています*。」

＊ 野村アセットマネジメントホームページ用語集より引用

時価評価は計測手法としては、非常にシンプルなものですが、事業会社においては、金融機関ほど大きなポジションを持たない、また取引の回数が少ないという特性から一般的な計測手法となっています。たとえ、自社のポートフォリオに大きな変動があっても機動的に対応はせずに時価評価で十分だとの意識がある企業も多いようです。

我が国では、2001年3月期より金融商品の時価会計が導入されて おり、一定の要件を満たした有価証券とデリバティブ取引が時価評価の対象となっていることで、多くの企業で定期的な時価評価が行なわれるようになったことも時価評価で十分との認識につながっているようです。

デリバティブの中には少ないポジション・取引であってもレバレッジが効いているなど市況の変動以上に価値が変動し、大きな損失をもたらすものもあるため、時価評価だけでは十分とはいえません。

大きな損害をもたらすケースの有無を分析し、想定されるケースに対して対策を検討することは有意義であるといえます。

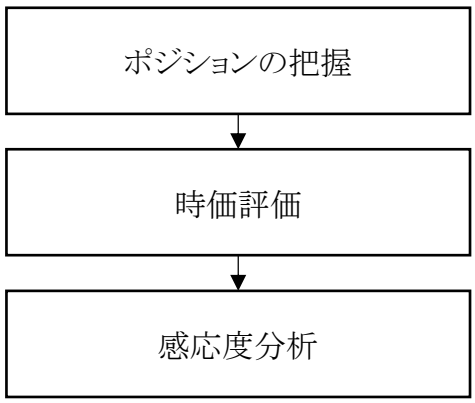
このような観点から、自社の市場リスク評価指標として時価評価を用いている場合、マーケットの変動により自社の取引、ポジションがどのような影響を受けるのかストレステストを並行して実施し、検証していくことが重要です

感応度分析

次にあげる感応度分析は市場リスク管理において非常に重要な計測、管理手法です。前ページの管理指標の進化のうち、今回も多くの企業で最もよく使われていた手法です。

感応度分析のステップ

感応度分析を行なうためには以下のようなステップが必要です。まず、自社の持っているポジションを把握します。次にそのポジションの時価評価をおこないます。この時価評価をもとに例えば、金利が1%変動すれば時価が1億円変動するといったようにポジションの感応度を分析します。



事例	感応度分析

海外から原油を輸入しているため感応度分析により、為替と原油価格に対する変動の影響を分析している。

為替や商品価格の変動をそのままリスクファクターとして設定。

円/ドル為替の1円/ドルの変動:	約20,00百万円
原油価格の1ドル/バレルの変動:	約4,000百万円

- この企業においては、為替に1ドル当たり1円の変動がある際、20億円の影響があると分析しています。また、原油価格に関しては、1バレル当たり1ドルの変動がある際、40億円の影響があると分析しています。

なぜ感応度分析か

直感的に理解しやすい

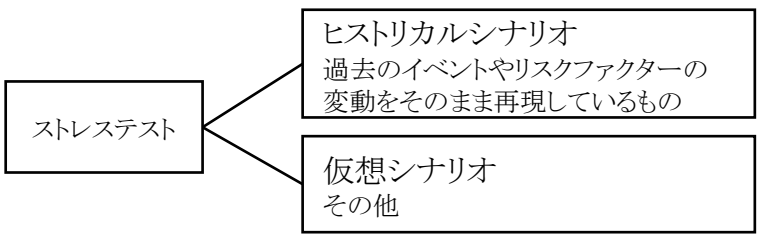
自社特有のリスク特性の把握が可能である

ストレステスト

次にあげるストレステストは感応度分析によって得られた自社の感応度を使い、さまざまなシナリオの想定によりポートフォリオが被る損失を推計します。ストレステストは経営者にも直感的に理解しやすく、個社のリスク特性に応じた設定がし易い特徴があります。また、統計的にとらえることのできない例外的な損失についても検証ができます。

ストレステストの分類

ストレステストにはヒストリカルシナリオを使用する場合と仮想シナリオを使用する場合に分類できます。



ストレステストのシナリオ例

ヒストリカルシナリオを使用する場合には過去のイベント時に起こった変動をそのまま使用する場合とイベント時のリスクファクターの変動を参考に調整を加えて使用する場合があります。

ヒストリカルシナリオ
1987 ブラックマンデー
1994 世界的金利上昇
1997 アジア危機
1998 ロシア危機、LTCMの破綻

仮想シナリオ
景気の上ブレ（金利の上昇等）
景気の下ブレ（株価の下落等）
企業の信用力の低下
テロの発生

事例 | **仮想シナリオを使ったストレステスト**

保有株式について仮想シナリオを使ったシナリオテストを実施。
景気の下ブレ時の株価の下落を20%とするシナリオを想定。
感応度分析により、既に株価1%の変動に対して、時価は2億円変動するとの分析済。
景気の下ブレ時の保有株式の株価の変動を最大20%と推定。
影響は40億円であると推定。

景気の下ブレ（株価の下落等）	影響
1%	2億円
20%	40億円

なぜストレステストか

経営陣が理解しやすい

- 経営者は最大損失がいくらになるかということに非常に関心が高い。ストレステストは過去のイベントや仮想シナリオから最大損失予想額を算出できます。

自社特有のリスク特性の把握が可能

- 自社のポジションやポートフォリオに基づいて推計するため自社のリスク特性を反映することが可能です。

時価評価、VaRでは把握できない例外的で重大な損失を検証可能

- シナリオの設定に制限がなく、自由なので例外的なイベントに関しても対応可能です。

VaRの特徴

市場リスク計測、管理手法はここ数年飛躍的な進歩を遂げ、特に金融機関においては2003年度テキストにて紹介されたVaR等を使い統合的なリスク管理を行なうのが一般的です。

VaRは非常に洗練された計測手法ですが、万能ではなく長所も短所もあり注意が必要です。

VaRの長所

概念的なわかりやすさ

計算の簡便さ

ポートフォリオ分析への応用可能性の高さ

VaRの特徴と短所

VaRは、その概念的なわかりやすさ、計算の簡便さ、およびポートフォリオ分析への応用可能性の高さなどから、金融機関のリスク管理実務で最も標準的に使用されるリスク指標となっています。

しかしながら、VaRのリスク指標としての妥当性に関しては、損益額分布の形状によっては、VaRが信頼区間外のリスクを捉えられないといった定義上・理論上の問題点が指摘されており、実務でもこうした問題点が意識され始めています。

ストレステストによる補完

例外的な環境下で起こり得る状況を正確に把握するためには、VaRのような統計的モデルには限界があります。こうした限界が存在する理由は、一部にはVaRの算出を容易にするための仮定の設定方法にあります。

ストレステストは、起こり得る極端なイベント下でのエクスポージャーを定量的に示すことによって、このギャップを部分的に埋めることによりVaRを補完するといえます。こうした極端なイベントの発生確率を捕捉することができるような信頼性のある統計手法は現在、存在しません。

バックテスティングの必要性

VaRモデルについては、モデルから算出されたVaRと損益との関係を検証するバックテスティングを実施し、VaRモデルが十分な精度を有していることを検証する必要があります。また、定期的に監査法人の監査を受ける等、外部によるモデルの評価を受けることも有効です。

VaRの計測方法

VaRは大きく分けて以下の3つの計測方法があり、それぞれ相違点があります。

分散/共分散VaR

- 計算負担が少なくてことから最もよく使われています。保有資産が債権、株式、スワップ、先物など線形のリスクを持つ場合に有効です。

ヒストリカルVaR

- オプションなど、非線形のリスクを持つ資産にも対応できますが、計算負荷は高くなります。また、過去データが十分な期間にわたって調達できない可能性や、その中に異常データが存在してしまう可能性も指摘されています。

モンテカルロVaR

- シナリオを自動生成するため、十分なシナリオ数を利用することができます。しかし、シナリオ生成のためのパラメーターの与え方によっては、ヒストリカルVaRに比べて、制限的になってしまう可能性もあります。また、計算負荷が非常に高いのが欠点です。

それぞれの特徴を知った上で、目的にあった計測方法を選ぶ必要があります。

事業会社におけるVaRの活用

VaRはある時点での最大損失額を示すのに非常に便利な手法であるので事業会社でも活用が出始めました。

ではその例を見てみましょう。

VaRの活用例

全社リスクの影響度分析時の活用

経営陣への決裁承認時の活用

ステークホルダーへの情報開示時の活用

全社リスクの影響度分析時の活用(社内)

ある事業会社では全社におけるそれぞれのリスクの影響度を分析する際に市場リスクに関して最大損失95%VaRで影響額を算出しました。

経営陣への決裁承認時の活用(経営)

経営陣にデリバティブによるヘッジの決裁をもらう際、最初のデリバティブ商品説明に続き、VaRを用い「期末VaR－ヘッジ後の期末VaR＝ヘッジによる効果」という説明を行ないました。

期末VaR	ヘッジ後の期末VaR	ヘッジによる効果
10億円	6億円	4億円

ステークホルダーへの情報開示時の活用(社外)

VaRによる最大損失額をリスク量として株主や監督官庁に開示しています。

統合VaRの活用

以下のレポート例ではそれぞれのVaRを算出した上で、商品間の価格変動の相関を考慮し、ポートフォリオのVaRを算出しています。

これは、VaRの長所の1つであるポートフォリオ分析への応用可能性の高さを示している実例と言えます。

参考 ポートフォリオVaRによる市場リスクレポート

【VaRの範囲と前提】
信頼水準:片側99%
保有期間:1日
商品間の価格変動の相関を考慮

億円

(月末)	02/3	02/6	02/9	02/12	03/3	03/6	03/9	03/12	04/3
株式	10.1	12.2	8.7	5.3	7.5	10.5	11.3	8.4	7.3
金利	2.1	4.5	3.2	4.2	5.5	4.7	2.5	3.3	2.7
為替	0.3	0.3	0.2	0.3	0.2	0.3	0.3	0.2	0.3
小計	12.5	17.0	12.1	9.8	13.2	15.5	14.1	11.9	10.3
分散効果	−1.4	−3.5	−2.6	−2.2	−4.8	−5.3	−3.6	−3.8	−2.4
VaR	11.1	13.5	9.5	7.6	8.4	10.2	10.5	8.1	7.9

2002年度最大値:18.0億円最小値:6.2億円平均値:9.3億円
2003年度最大値:16.5億円最小値:4.6億円平均値:9.8億円

5.1.5　信用リスク

ここでは、信用リスクの定義、および信用リスクに関わる言葉、手法の定義をご紹介し、共通の知識のもと説明をすすめていきます。

信用リスクとは
与信供与先がデフォルトしたり、信用状態が悪化したりすることで、貸付金の回収ができなくなるなどの損失を被るリスク

信用リスク管理の仕組み

信用リスクを管理する仕組みを挙げます。

主なリスク管理の仕組み	定義
リスク管理規則 (クレジットポリシー)	経営理念、行動規範を踏まえ与信業務の普遍的かつ基本的な理念・指針・規範等を明示したもの
独立した審査部門	各部門から独立した審査部門による格付・信用リスク管理が実施するのが望ましい
ポートフォリオ管理	ポートフォリオを分析・管理するためには信用リスクの計量化が不可欠。計量化には与信金額、デフォルト率、回収率のデータが必要となり、データ整備等が必要となります

『事業リスクマネジメントーテキストー 経済産業省 平成16年3月』57-59ページより作成

信用リスク評価を構成する要素

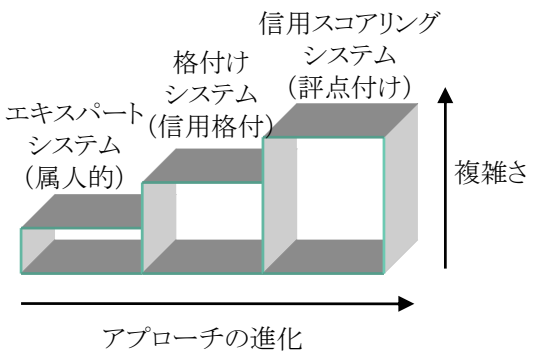
構成要素	内容
与信	一般的に「商取引において取引相手に信用を供与すること」を指します
定量評価	数値化できる情報に基づく評価。例えば財務データ、登記事項、株価等
定性評価	数値化できない情報に基づく評価。事業の見通し、業界内の風評、経営者の人物等
信用格付	信用リスクを統一的な尺度で評価し、簡潔な記号で分類表示するのが信用格付です。格付け付与におけるグループ各社間での尺度統一、外部格付けとの整合性確保といった客観性も問題となります
倒産確率（デフォルト率）	将来の一定期間に債務不履行等の事象が発生する確率
回収率	回収率はモデルにより、一定と仮定される場合もあるし、変動すると仮定される場合もあります
信用VaR	一定期間後に一定確率のもとで、貸出債権や債券等の種々の信用リスク資産で構成されたポートフォリオに発生しうる最大予想損失額。市場VaRの考え方を応用

信用リスクマネジメント評価・管理手法

信用リスク評価手法はエキスパート・システム（専門家による判断）、格付けシステム、信用スコアリング（評点付け）・システムと発展してきました。

ここではまず、それぞれの特徴や一般の事業会社と商社や金融機関の信用リスクに対する考え方、取組みの違いを説明し、次頁でそれぞれの実例を紹介します。

参考 信用リスク評価の伝統的アプローチ



- 信用リスク評価アプローチのうち、事業会社ではエキスパート・システムや簡易な格付システムを使用しているのが一般的です。例えば製造業では、長いスパンで継続的に安定した取引を基本とするので定性的な情報を重視する傾向があります。また、格付システムを使用する場合でも、与信金額の算出や貸倒引当金率の設定に直接連動しているケースは少ないようです。

エキスパート・システム（専門家による判断） 担当者の専門知識 主観的な判断 特定の重要ファクターのウェイト付け	5つのCが基本的なチェック項目である 1.借手の特徴（Character） 2.資本（Capital） 3.能力（Capacity） 4.担保（Collateral） 5.景気循環（Cycle）
格付システム（信用格付） 低格付け 高格付け 貸倒引当金率	貸倒引当金の妥当性を評価するために誕生したシステム 例えば、格付Aは0%, Bは20%,、Cは50%の引当金を設定するなど
信用スコアリング（評点付け）システム 倒産企業 非倒産企業 非線形性	消費者ローンから商業ローンに至るあらゆるタイプの信用分析で用いられており、返済に対するデフォルト確率を決定する上で重要なファクターをまず探し出し、それらを組み合わせてあるいは加重平均して定量的なスコア（評点）にする

- 商社や金融機関では詳細な格付システムや信用スコアリングを使用しているのが一般的です。例えば、商社では格付システムに応じて与信金額の算出や貸倒引当金率の設定をするなど、直接連動しているケースも見受けられます。また、倒産確率や回収率を使い、信用リスクの総量を計量化する動きが見られます。

業種別信用リスク評価のアプローチ

一般事業会社等	商社・金融機関等
目的	**目的**
売掛債権の回収	貸付金回収
新規取引先の決定	貸倒引当金設定
取引継続可否判断	新規融資先審査
格付分類の数	**格付分類の数**
少ない	多い
取引先	**取引先**
少ない	多い
情報源	**情報源**
主に定性情報＋定量情報	主に定量情報＋定性情報

- 事業会社においては、信用リスク評価による情報は主に定性情報＋定量情報を使用しているケースが多く見受けられます。特に原材料や部品の調達先といったケースではその特殊な技術を持ったその企業としか取引できないといったケースもあり、持っている技術や業界の評判といったことをまず、評価しその後に財務内容をチエックするといった形も多く見られます。
- 一方、商社や金融機関の場合は先に財務内容を定量的に評価し、その後定性的な情報をプラスし、総合的に判断するのが一般的のようです。

信用リスク審査方法別の特徴

信用リスク管理ツールによる自動審査	担当者による審査
自動審査によるスピードの向上	時間的制約
複数企業間での相対的な比較が可能	企業ごとに絶対的判断
共通の基準による判断	状況に応じた柔軟な判断
微妙な要素の判断が難しい	ツールに反映されない要素を加味した判断
例）倒産確率0.8%と0.9%では何が違うのか	担当者ごとに独自の判断基準

帝国データバンク 企業評価モデルプロジェクトチーム『企業評価と信用リスク』清文社 2002年 より作成

- 評価対象が多い企業の場合には担当者が全案件を評価するには時間が足りません。また、担当者ごとに独自の判断基準が存在することにもなります。
- そこで評価の最初のプロセスを自動化し、審査のスピードアップを図り、担当者は判断の難しいボーダーにある企業等の審査に時間をかけようとの動きが進んできました。
- また、インターネット等の発展により、リアルタイムの審査が必要になってきましたが、データベースやモデルの構築には多額の費用と時間がかかるため、以下のように業界や官公庁が中心となって共同で信用リスク分析データベースを構築する動きも活発になっています。

参考 日本における信用リスク分析データベースおよび運用者

『しんきん情報システムセンター』 信用金庫
『日本リスクデータバンク（RDB）』 都市銀行、地方銀行、商社
『信用リスクデータベース（CRD）』 中小企業庁

前述で一般事業会社と商社や金融機関の信用リスク評価には大きな違いがあることを説明しました。目的が違うので当然、評価するプロセスや使用するモデルも違ってくることとなります。

ここではそれぞれを簡易編(事業会社で多く見られる方法)と詳細編(商社・金融機関等で多く見られる方法だが、事業会社にも取り入れられている)という2つに分類をしました。簡易編では信用格付を4段階に分類している一般事業会社(製造業)での実例をご紹介します。

信用リスクマネジメント“簡易編”

製造業における信用リスクは主に売掛債権と原材料調達先に分けられます。評価プロセスとしてはまず、財務データ等を使った定量評価と数値化できない情報による評価である定性評価を行なった結果より、あらかじめ決めてあった信用格付けと照らし合わせます。

信用格付例(4段階)

参考　ある消費財製造業の信用格付け

評価	定義	対応策
A	財務上の問題点は少ない 且つ、問題点に深刻な要素を含まない	年1回の定期的な評価を行なう
B	財務上の問題点はAより多いが、問題点に深刻な要素を含まない	年1回の定期的な評価を行なう
C	財務上の問題点が多く、近い将来深刻な財務状況の悪化が予想される	現状の取引は一時停止することを提案。関連部署共同で今後の対応策を検討する
D	財務状況は悪く、近い将来、倒産の確率が高い	即時取引の停止を提案する

信用格付時の財務上のチェックポイント

財務上の問題点は以下のような財務データをもとに判断をします。

貸借対照表、損益計算書表、財務比率の比較

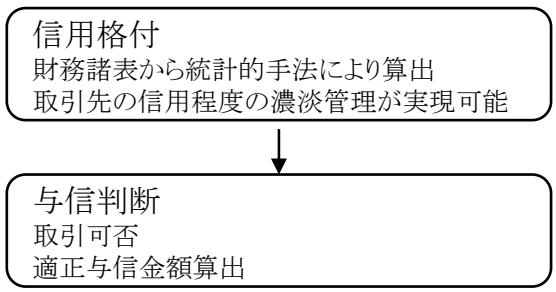
- 貸借対照表は一定時点の企業の財政状態を明らかにする書類です。資本をどのように調達し、どのように運用しているかのチエックをします。
- 損益計算書表では、売上高や利益の推移をはじめ、本業で利益を計上しているのか、その企業の損益体質がどのようなものかを見ることが重要です。
- 財務比率の比較では評価対象企業の属する業界の平均値や標準偏差などを把握した上で比較をします。

支払い能力の判定

- 手元資金
- 売上債権・買入債務の回転期間
- 借入返済額
- 経費支払

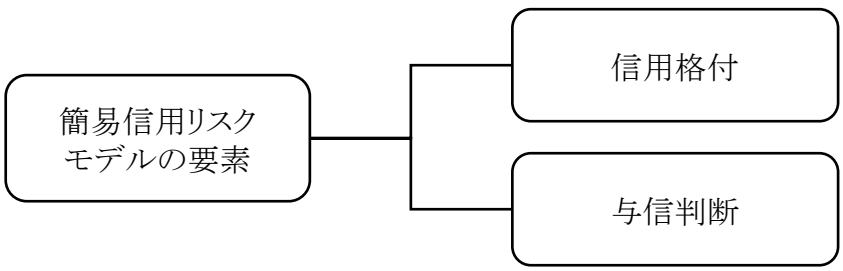
信用リスク評価プロセス例(簡易編)

簡易編では、4つの信用格付の基準に照らし合わせ、対象企業を分類し、主にC、Dに分類された企業を中心に評価を進め、取引をするのか否か、また、適正な取引額に関して決定を行います。



信用リスクモデルの要素(簡易編)

簡易評価のプロセスをモデル化する際は信用格付と与信判断に分け、モデル化することとなります。初期段階においては、信用格付のみをモデル化することも選択枝の一つです。



評価モデルに使用する候補データ

定性データ
信用情報
業歴
規模
資本構成
損益
資金現況
経営者
企業活力
加点
減点
経営者情報
業界経験
経営経験
得意分野
就任経緯
経営者人物像ほか

定量(財務データ)
総資本経常利益率
総資本企業収益率
自己資本経常利益率
売上高営業費用比率
売上高原価率
売上高販売管理比率
売上高営業外収益率
売上高経常利益率
売上高当期利益率
売上高金融収支比率
売上高金利負担率
有利子負債平均金利
売上高原価償却率
原価償却率
利益留保率
総資本回転率ほか

信用格付モデル構築

信用格付のモデルを構築する場合には左記のような、定量(財務データ)を使い簡易にモデル化が可能である。

定性データも非常に有益な情報であるが、主観的な要素が入るため評価モデルに使うデータとしては注意が必要である。

帝国データバンク 企業評価モデルプロジェクトチーム『企業評価と信用リスク』清文社 2002年 より作成

信用リスクマネジメント簡易編におけるポイント

定性情報により多角的な評価を行うことが可能

定量情報である財務データの有効性に問題がある場合には注意が必要

定性情報と定量情報の組み合わせにより総合的に評価

- 定性情報の内容には資本構成、損益、経営者、支払能力、資金需要動向、資金調達余力、担保設定状況等有益な情報が含まれます。
- 財務データは必ずしも入手できるとかぎりませんが、可能な限り入手します。財務データの有効性に問題がる場合には定性情報をより重視し、財務データを参考程度とすることも考えられます。
- 可能であれば経営者、財務責任者へのインタビュー等も含む数字に表れない情報の入手、定性評価、財務情報を中心とした定量評価、そして最終的にはこれら評価を総合的に判断することができれば、精度の高い評価が可能です。
- 取引先によっては、販売目標達成や営業利益確保のために取引せざるを得ない場合もあるかもしれませんが、最終評価後も常にクレジットポリシーや信用格付と照らし合わせ監視していくことが重要です。

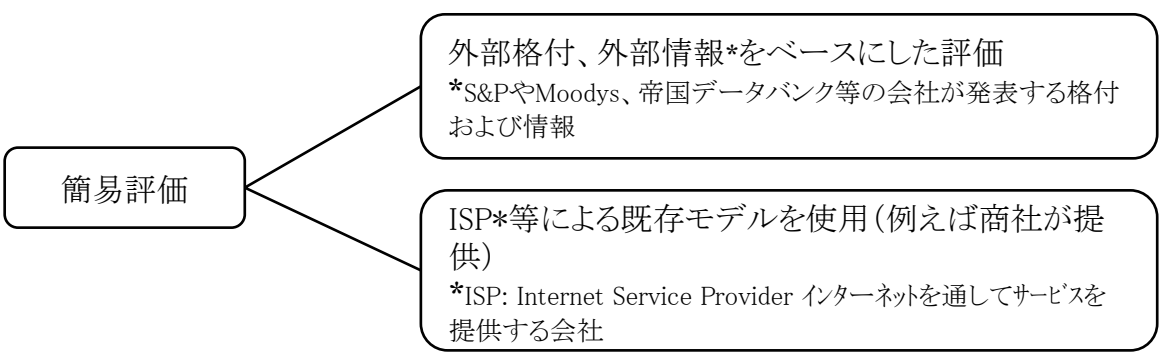
製造業における調達先のリスク管理に信用リスクの管理手法を使った例については「5.1.2 製品要因リスク」内調達リスクのパートで詳しくご紹介しています。

すぐに始められる信用リスク評価

今まで統一された信用リスクに関する明確な基準がなく、これから始めようといった企業においては、出来ることから始めることが肝要です。

最初の簡易評価モデルは例えば、Excelベースの簡単なものでも対応可能です。実際、まずはとても簡易な評価モデルからスタートし、段階的に改善することで、緻密な自社信用モデルを作り上げた企業もあります。

すぐに始められる信用リスク評価方法としては、以下のように外部格付をそのまま利用する方法や、既存のモデルとデータベースを利用する方法があります。



信用リスクマネジメント“詳細編”

取引先が多岐にわたる、リスクの大きい取引先の割合が高いといったような企業の場合にはより詳細な信用格付を設定した上で、評価をすすめることが必要となります。

以下の例では評価区分を9つに区分することによって企業の変化をより細かく捉えることができます。また、この評価モデルでは、取引先の財務状況に基づく定量評価及び各種定性評価に基づき格付する仕組みとなっています。またこれと連動し、取引先に対する与信枠も設定されます。取引先の格付に応じて与信枠設定の決裁権限に差をつけることにより、格付の低い取引先に対する与信管理を相対的に強化する仕組みとしています。

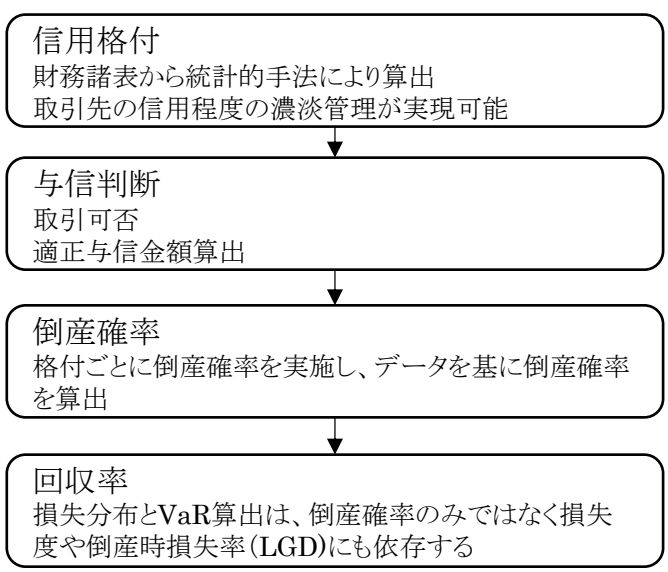
信用格付例(9段階)

参考 | 信用格付け

格付	区分	定義
1	超優良	企業規模も相応にあり、財務内容も非常に良好な企業
2	優良	1ランクには劣るが、概ね財務内容も良好な企業
3	良好	標準企業の中でも比較的良好な企業
4	標準1	平均的企業
5	標準2	要注意企業には入らないが、平均に達していない企業
6	注意1	注意が必要な企業
7	注意2	多大な注意が必要な企業
8	警戒	警戒を要する企業
9	問題	債務超過、または極めて警戒を要する企業

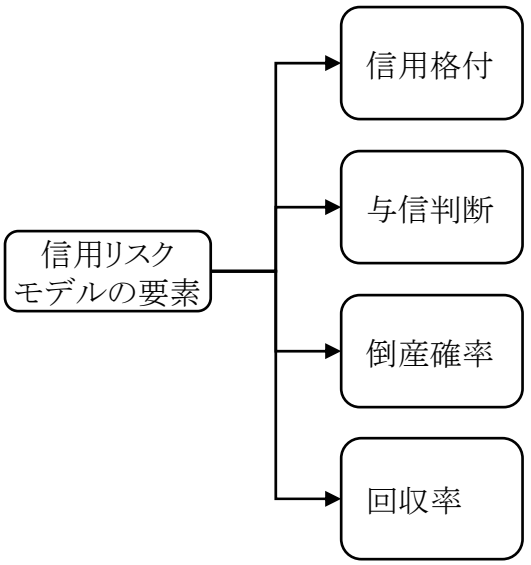
信用リスク評価プロセス例(詳細編)

詳細編では、9つの信用格付の基準に照らし合わせ、対象企業を分類し、さらに倒産確率、回収率を加味し、信用リスクを計量的に捉えていくこととなります。回収率を加味すれば信用VaRの算出も可能となります。



信用リスクモデルの要素（詳細編）

詳細評価のプロセスをモデル化する際は下記のように信用格付と与信判断に加え、倒産確率、回収率についても考慮にいれます。これにより、損失見込を算出することが出来るようになり、ポートフォリオ管理が可能となります。



倒産確率別損失見込				
格付	倒産確率	与信額	回収率	損失見込
1	0.01%	1000	50%	0.05
2	0.05%	700	50%	0.175
3	0.10%	500	50%	0.25
4	0.50%	300	50%	0.75
5	1.00%	200	50%	1.0
6	2.00%	100	50%	1.0
7	5.00%	50	50%	1.25
8	7.0%		50%	
9	10.0%		50%	
合計		2850		4.475

帝国データバンク 企業評価モデルプロジェクトチーム『企業評価と信用リスク』清文社 2002年 より作成

ポートフォリオ管理

前述のように倒産確率や回収率を算出できるようになると与信額を参考にして格付ごとの損失見込みを算出できるようになります。

この企業の許容最大損失が10.だとすると例では合計が4.475なので許容最大損失まであと5.525余裕があることになります。例えば、格付5与信のケースでは、与信額100に対して0.5の損失見込となるので1105の与信枠があることになります。

このように損失見込の全体の合計を見ながらどの格付の企業にいくら与信が可能かを全体のバランスを見ながら決める管理手法をポートフォリオ管理といいます。これにより、どんな場合でも許容最大損失内に与信を収めるといった戦略をとることが可能となります。

信用リスクマネジメント詳細編におけるポイント

実際に先進企業の中にはJPモルガンが開発したクレジットメトリクスのメソドロジーを参考に自社独自の要素を加え、信用リスクモデルを開発し、信用VaRを算出し、個別の案件、全体としての最大損失の把握に役立てているケースもあります。但し、そこに至るまでにはいくつもの過程があり、一歩一歩の進化があってのことです。

社内独自のモデルを持つ企業においても外部格付との関係を重視し、社内格付が外部格付を上回ることがないよう定めています。

先進企業ではモデルの精緻化および信頼あるデータの蓄積が進むにつれ、市場リスク同様リスク・リターンの発想で格付に応じたリスクウェイトを用いて必要なリターンを算出し、管理することが始まっています。

社内信用格付けごとのデフォルトレートあるいは信用の推移確率行列をベースに信用VaRを計算する算出ロジックを研究しシステム化する

格付毎にリスクウェイトを設定して信用リスクのリスクアセットを算出する

信用リスクも考慮してリターンをあげるインセンティブが働く仕組みを確立する

信用リスクマネジメントにおける検討点

評価の過程ではあらかじめ決めた評価プロセスにより評価をしますが、以下のような点もプロセスを進める上での重要な点です。

事業リスクマネジメントの観点から評価プロセス・基準を統一する場合、子会社および海外拠点において独自のプロセスや基準を使用していることが考えられます。これらを統一、または整合性を持たせることは予想以上に手間がかかるので一旦、整理をした上で今後の対応課題とすることも可能です。

その次に各データの有効性や信頼性を確認の上、どのように格付に反映させていくのかを検討していくこととなります。財務情報に基づく信用格付プロセスは格付ごとにその後の審査にかけるウェイト・時間・プロセスを決定するためのものであることから、基本を押さえた上で自動化、簡易化をすることが望まれます。自動化、簡易化することにより詳細な判断が必要な次ステップ以降により多くの時間を費やすことができます。

子会社および海外拠点との格付および格付基準の整合性
－　ローカル特有の問題を整理する

モデルとデータの有効性
－　最新情報や、特定のイベント等を反映する

格付プロセスの自動化と簡易化
－　リスクの小さい与信先には省力化し、大きい与信先には採算性や取引の意義を十分考慮する

信用リスクマネジメント今後の課題

信頼できる大量のデータと詳細なモデルにより以下にあるように算出された期待損失の値を経営判断や取引事後のモニタリングに活用することも、今後の課題として視野に入ってきます。

モデルによる評価により全てが完結するのではなく、企業の状況は刻々と変化するので、最終的な判断では経験を積んだ人間の判断が必要となります。

期待損失(Expected loss)の貸倒引当金への適用

取引の事後モニタリングにも格付利用

信用リスク定量化、モデル依存への警告

『最強のリスクマネジメント』の中でスタンダード&プアーズのマネジング・ディレクター、三次啓之氏は以下のように述べています。

「どんなに優れた数量的分析手法が現れようと、信用リスクを管理するに当たっての留意すべき重要な点があります。「それは技術的に進んだからこそ陥りやすい誤解です。信用リスクの管理は決して信用モデルや技術的な基盤作りのみで達成できるものではありません。それらは非常に有用な道具立てですが、それら自身が優れたリスク管理をしてくれるわけではないのです。むしろ過剰に依存してしまうリスクの方が重大な結果を招くのです。優れた洞察を得るために、信用リスクをダイナミックに変化するものととらえる必要があります*。」

*『週刊東洋経済　臨時増刊　最強のリスクマネジメント　東洋経済新報社　2003年 7月』より引用

5.1.6　レピュテーションリスク

レピュテーションとは、肯定的及び否定的な評価、評判のことをいいます。

レピュテーションリスク(レピュテーショナルリスク)とは、企業に関する否定的な評価・評判が世間に周知されることで企業の信用やブランド価値等が悪化し、結果的に損失を被るリスクをいいます。企業に関する否定的な評価・評判は、企業の信用やブランド価値等の悪化につながるので、顧客や取引先離れを引き起こし、社員の不安を増大させます。それが更なる顧客離れや取引先離れ、社員の不安の増大を加速させ、ついには企業の社会的信用の失墜、業績の悪化につながるのです。

当該リスクは、不祥事とうの発生など評判の基となる事実が存在する場合のみならず、単なる噂など事実に基づかない場合も発現する可能性があります。

企業が長年で築き上げてきたレピュテーションは不祥事等の発生により簡単に崩壊し、元の状態に回復させるには長い年月と莫大な費用を費やすことが必要な場合もあります。更には結局回復できず企業が崩壊してしまう場合さえもありえます。その意味でレピュテーションリスクは最終的にビジネス全体に影響すると言うことができ、その対応が大変重要となります。

リスク評価におけるレピュテーションリスクの扱い

リスクの影響度を評価する際に、例えば事故などのリスクがあったとして、物の損害や損害賠償金など直接的に受ける損害の他に、その後のレピュテーションが傷つくことで生じる売上低下などの間接損害があります。レピュテーションが傷つくことで生じる売上低下などの損害は特定が難しいため、多くの企業では直接損害のみを評価対象としているようです。

しかし、昨今はコンプライアンス関連リスク等、直接的な損害は大きくないがレピュテーションの低下による損害が大きいリスクが増えているため、レピュテーションの低下を評価対象とする企業が増えてきています。ただし、その場合でも、具体的な金額に換算することが難しいため、報道等で取り上げられる大きさを5段階で表すなど定性的に評価していることが多いようです。(詳しくは「Chapter4」リスク評価基準例を参照下さい。)

レピュテーションリスクへの対応

レピュテーションリスクを予防・低減するためには、一次的に発現する各種のリスク発現を予防・低減するのは当然ですが、リスク管理の企業文化を社内に浸透させること、情報を管理すること、ステークホルダーと良好な関係を保つことが有効となります。

企業文化の浸透

企業がリスク管理や倫理、法令、規程等を遵守する企業文化を確立し全社的に浸透させ、従業員が正しい行動をすることでレピュテーションリスクが予防・低減されます。企業文化を浸透させるには従業員へ対する経営トップの意思伝達や教育研修を実施することが有効です。企業が正しい行動をしているということが世間に周知されることで、企業に関する否定的な情報から企業の信頼やブランド価値が保護されることが期待できます。

企業がリスク管理や規程等を遵守する企業文化を浸透させるためには、以下のようなコンプライアンスプログラムの立案と実施が有効となります。

- 倫理綱領や行動指針の策定と周知徹底
- 経営トップの率先垂範
- オープンなコミュニケーションの確立
- 正しい行動が正当に評価される評価制度　など

情報管理

情報の収集と迅速な対応が求められる

- 企業の信用やブランド価値の低下を防ぐためには日頃から企業に関する評判等の情報を収集する必要があります。情報源には下記のようなものがあります。
  - お客様相談室などに集まる顧客の声
  - 営業や渉外など、外部と接点がある担当者からの報告
  - 新聞や雑誌等の報道内容
  - インターネットの掲示板や個人サイトに書かれる情報（監視ソフトウェアを使った社名などの特定キーワードの監視）
  - 内部通報窓口に集まる従業員の声（企業に関する悪い評判の多くが内部者の告発に端を発することからも、こういった窓口に集まる従業員の声に適切に対応すること　は重要）
- これらで得た情報に対し、その内容の重要度に応じた適切な報告や迅速な対応ができるように、エスカレーションルールを整備します。（詳しくは5.2危機管理内エスカレーションルールを参照下さい。）
- リスクの兆候となる情報をいかに早い段階で発見し、適切に対処できるかがカギとなります。

参考 | **クレームとレピュテーションリスク**

ハインリッヒの法則*をクレームに当てはめると、1件のレピュテーションの低下につながる「重大なクレーム」の裏には29件の顧客から寄せられたレピュテーションの低下につながりかねない「軽微なクレーム」が存在していたことになります。さらにその裏には、300件の従業員が「しまった」と思っているが外部からのクレームがないため見逃したケース、つまり「認識された潜在的な失敗」が存在していたはずです。

このことは、レピュテーションの低下につながるような重大なクレームを発生させないためには「軽微なクレーム」や「認識された潜在的な失敗」を見逃さず、その原因に対し適切に対処することが必要かつ重要であるということを意味します。

＊「ハインリッヒの法則」とは、米国のハインリッヒ氏が労働災害の発生確率を分析したもので1:29:300の法則とも呼ばれます。1件の重大労働災害の裏には29件のかすり傷程度の軽災害があり、さらにその裏にはケガはないがひやっとした300件の体験があるというものです。

情報開示体制の整備が求められている

- 企業はレピュテーションに関する情報を日頃から積極的に開示することが必要となります。その上で万一、レピュテーションを低下させるような事象が発生した場合の危機管理体制を整備することも必要です。企業自身が事態の最新情報をすばやく適切に把握し、現状や企業の対処内容、社会へのメッセージを適切な方法で発信できるよう、あらかじめ体制やマニュアルを整えます。例えば同じ不祥事等を起こした場合でも、その後の対処方法によってレピュテーションの低下度合いを大きく変えることができます。（詳しくは5.2危機管理内危機発現時の対応を参照ください。）

ステークホルダーとの友好的な関係

ステークホルダーとは、当該企業にとっての利害関係者のことです。企業には株主、従業員、取引先、顧客等企業内外に多数のステークホルダーが存在します。

企業の信用やブランド価値はステークホルダーが感知するものです。したがってレピュテーションリスクを防止・低減するにはステークホルダーと友好的な関係を構築し保持していくことが重要となります。ステークホルダーと友好的な関係を保持するために、企業は重要なステークホルダーグループ内に支持者を積極的に見つけ、共通する関心事項について支持者たちと定期的に交流することが有効となります。交流によって企業は企業に関する情報を収集できるのみならず、危機に際した場合に必要な情報を効果的に発信することが可能となります。

最近CSR（企業の社会的責任）という言葉が注目を集めています。CSRを果たすためには、ステークホルダーとの適切なコミュニケーションにより企業への期待を把握することが重要です。このような活動自体がリスクマネジメントであると捉える企業もあります。

ステークホルダーはそれぞれ当該企業との関わりにおける利害が異なるため、ステークホルダー別にリスク情報についてのコミュニケーション戦略を策定することが望まれます。不祥事等が発生した場合の主要なステークホルダー別の具体的なリスクコミュニケーション戦略は次ページの通りです。

参考　不祥事等が発生した場合の主要ステークホルダー別コミュニケーション戦略

ステークホルダー	不祥事等が発生した場合の具体的なコミュニケーション戦略
株主	株主は多くの場合企業の株価に関心を持ちます。不祥事等が発生した場合は、機関投資家等の大株主に対して個別に状況の説明や謝罪を直接行います。また、それ以外の株主にはマスメディアやダイレクトメール等を通して状況の説明や謝罪を行います。株主ではありませんが、証券アナリストからのインタビュー要請には誠実に対応し株式市場での当該会社の価値等の意見をもらうことも有効です。
従業員	不祥事等の発生は従業員に大きな動揺を与えます。企業のイメージやブランド価値を実際に創造するのは企業の従業員です。不祥事等が発生した場合には、会議やアンケート等で不祥事等の原因や事後対応についての理解について意見を収集するとともに、勤労意欲が低下しているか否かの調査も行います。
取引先	不祥事等が発生した場合には、企業との取引が中止され売上が低下する可能性があります。主要な取引先を個別に訪問して状況の説明や謝罪を直接行い、取引の継続を要請していきます。
顧客	最終消費者である顧客は企業の売上に大きな影響を与えます。不祥事等が発生した場合には電話調査、インターネット調査などで反応を確かめることが有効です。またマスメディアを通して謝罪や不祥事等の情報を発信することも重要です。

コラム

ジョンソン・アンド・ジョンソン社のタイレノール事件

1982年9月に、全米を震撼させる「タイレノール」事件が発生しました。これは、ジョンソン・アンド・ジョンソン社（J&J社）の医薬品部門で全米の主力商品だった家庭用鎮痛剤「タイレノール」にシアン化合物が混入され、シカゴを中心に7名が死亡するというものでした。

J&J社と「タイレノール」を扱うグループカンパニーのマクニール社は重大な危機に直面しました。これに対しJ&J社は全「タイレノール」商品の回収、マスコミを通じた積極的な情報公開、新聞への警告広告の掲載、対策チームの設置など素早い対応を行いました。陣頭指揮をとった当時のJ&J社のバーク会長は、単なる危機管理として対応することに終わらず、「消費者への責任」を第一に考えた体制をとりました。これは、J&J社の企業理念である「我が信条」の第一の責任に立ち返った意思決定でした。

事件終結後、J&J社のこの事件における対応は、一般消費者をはじめ政府・産業界からも、これまで以上に高く評価されました。そして、全社員が一丸となった努力の結果、予想をはるかに越える速さで市場での信頼や業績が回復していきました。

ジョンソン・アンド・ジョンソン社ホームページ　J&Jヒストリーより一部引用

5.2 危機管理(クライシスマネジメント)

ここでは重要リスク発現時の危機管理について、下記事項を中心に説明します。
- 組織的な危機対応のためのエスカレーションルールの設定
- 危機管理マニュアルの作成
- 危機発生時の対応に関する主要な考慮点
- 再発防止策の検討
- 事業継続計画の策定

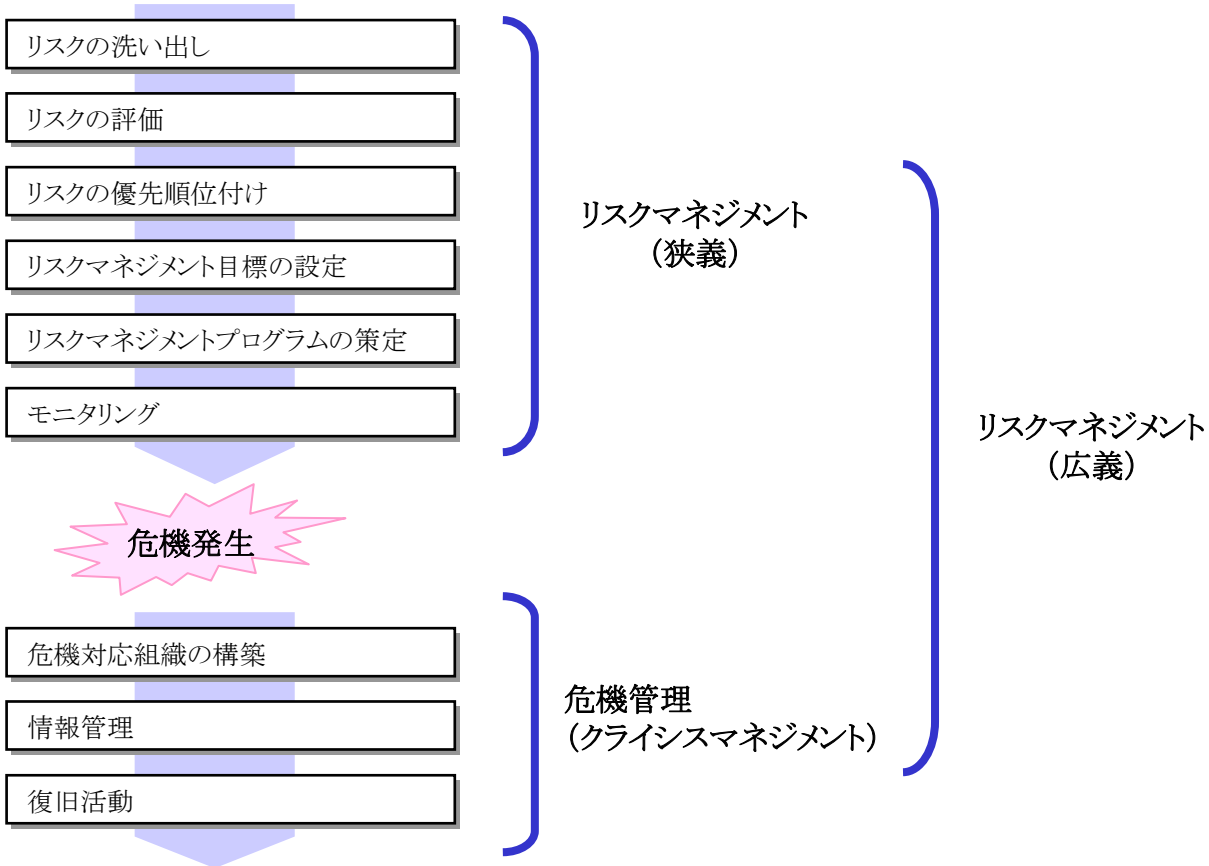
5.2.1 事業リスクマネジメントにおける危機管理

ここまで説明してきた各事項を入念に遂行し、リスクの発現可能性をできるだけ小さくすることは事業リスクマネジメントの基本であるといえるでしょう。しかしながら、いかに基本に忠実であってもリスクが絶対に発現しない仕組みを構築することは、いかなる企業においても不可能です。危機的な事態が生じるのは地震や台風などの自然災害による場合もあれば、火災や情報システムダウン等の事故による場合もあり、更には業務上のミスや不祥事による場合もあります。いずれにせよ、重要なリスクが発現してしまった際にどのような対応をするかということは、リスクの発現自体をどう防ぐかということと同様に、リスクマネジャーにとっての最重要課題の一つです。

通常のリスクマネジメントはリスクの発現防止を中心とした範囲を対象とします。現実に危機が発生した場合には、通常のプロセスではなく a.危機対応組織の構築、b.情報管理、c.復旧活動という3つのプロセスにて対応することとなります。これらについては次項「5.2.2 危機発生時の対応」で個別に説明します。

しかしながら、通常のプロセスに拠らないで対応するということが即ち危機管理について事前の準備が不要ということではありません。どのような事態になったらどの階層の誰が責任者となる等のエスカレーションルールの策定と、危機発生時の対応ノウハウをまとめた危機管理マニュアルの作成は事前に行う必要があります。

参考 | **リスクマネジメントと危機管理**



5.2.2　危機管理マネジメント

有事に適切な対応を行うためには、平常時からいつ発生するか分からない危機に備えておく必要があります。

エスカレーションルールの策定

有事の際、迅速な情報収集と対応指示を行うため、どのような事態になったらどの階層の誰に情報を収集し、誰が責任者となるのかを定めておく必要があります。

エスカレーションルールの必要性

危機が発生した際には責任ある者が事態を正しく把握していることが、企業組織として正しい行動を取るための必要条件になります。

「どのような事態の時に組織のどの階層にまで報告を上げるのか」というエスカレーションルールを定めておくことが必要です

- 危機管理においては、いかに早い段階で危機の認識をし、組織としての対応が取れるかが重要なので、エスカレーションルールによって然るべき判断のできる人に素早く情報が届くようにすることが大切です。
- 事件や事故が企業に与える影響の大きさに応じて報告レベルを決めておきましょう。危機の重大度により報告先（社長・執行役員・部長など）と報告内容を決めておくことは、誰が対策本部長となり実行の責任を持つかという意思決定・命令系統の明確化を図る上で重要です。
- また、エスカレーションルールに従って、誰は誰に報告することになるといった情報伝達の道筋をエスカレーションルートと呼びます。

実際に危機が発生したときは第一報が迅速にエスカレーションルートに乗って報告されることが促進されるように、報告に関する原則を定めておくようにします

- 危機が発生した時の第一報は不完全な情報であっても迅速さが大切です。後で誤報とわかった場合でも、そのことについて通報者が責められることはないと決めておくことは特に重要です。そうしないと、次から部下は叱られることを恐れる余り本当の危機のときに連絡が遅れて、企業として致命傷を負うことにもなりかねません。

ある企業ではエスカレーションに関し以下のような原則を掲げて、迅速な情報伝達を図っています。

先ず上司に一報

複数のルートが可

精緻より迅速

第一報は訂正可能

事例1： 緊急時対応レベルの設定

ある消費財製造企業では緊急時対応レベルとして、下図のように3段階を設定しています。

事例　ある消費財製造業の緊急時対応レベルの設定

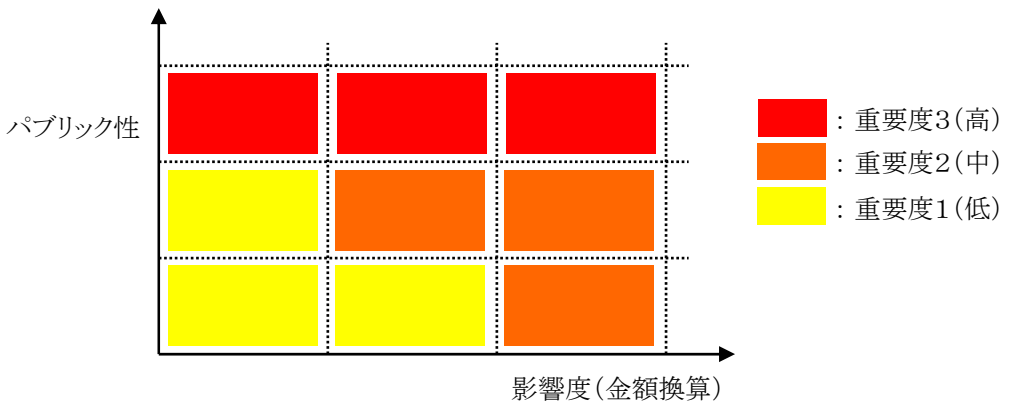
	レベルA	レベルB	レベルC
有事の程度	全社的に経営上の影響が大きく、全社挙げての対応が必要	経営上の影響はレベルAほどではないが、マスコミ対応ないし複数部門での対応が必要	経営への影響は小さく、マスコミ対応も必要でない。主管部門対応で解決可能
該当する有事の例	大規模地震・火災、テロ、大規模リコール　等	中規模以上の事故・事件、大規模クレーム、特許係争、得意先倒産　等	小規模な火災・事故、事務ミス　等
責任者	社長	主管部門担当取締役	主管部門長

- 緊急事態の発生現場から事務局や所属部門に連絡が入ると、事務局では事態把握のための情報収集、関連部門への連絡、緊急調整のための下準備等を行います。事務局だけではあらゆるリスクの緊急対応はできないため、関連部門のキーマンに緊急打ち合わせへの出席を求め調整を行います。そこで事態の対応レベルと主管部門を決めます。
- 同社では、緊急時対応は手間がかかり業務への負担が大きいことから主管部門がなかなか決まらないという問題が従来から認識されていました。しかし、それでは経営トップに報告するまでに時間がかかってしまいます。例えば最初は数件だった商品クレームが2～3日後には100件となり、そして200件になって慌ててトップに報告するということにもなりかねません。そのため、関連部門のキーマンとの緊急調整に基づいて主管部門を決定することにしています。どうしても決まらないときは、臨時委員会を開いて経営トップの判断を仰ぐ、あるいは事務局が主管部門を決めることとなります。
- このように同社では緊急打ち合わせによって、対応レベル、主管部門、責任者が決まる仕組みにしています。

事例2： 重大度マトリックス作成とエスカレーションルート

あるサービス業企業では危機管理に関するエスカレーションルールとして、横軸に金額換算された「影響度」、縦軸に「パブリック性」をとったマトリックスを作成して、重大度管理をしています。「影響度」はリスクマップでの「影響度」と同じ基準に拠っています（影響度に関しては「4.1.4 リスクの評価に関する留意事項」を参照ください）。各危機内容がこのマトリックス上でどこに位置するかは、過去のトラブル事例を参照して決めています。

事例	ある消費者向サービス業におけるマトリックスによる重大度管理



危機発生によって深刻な影響を被る要因について検討した結果、危機内容の「パブリック性」を重視してエスカレーションルールを定めることにしました

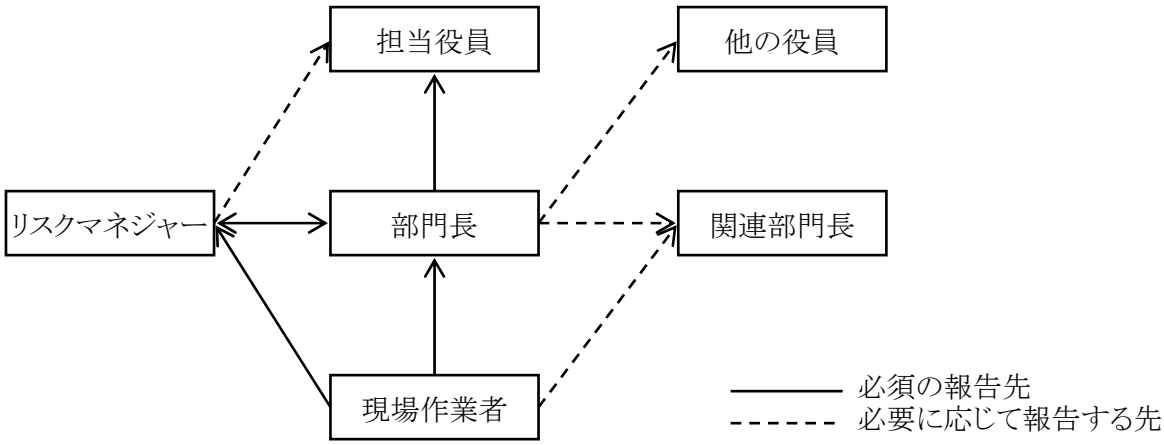
- 同社におけるパブリック性とはメディア報道等による自社のイメージの破壊とそれによる企業価値低下に関するおそれを意味します。パブリック性が「大」の場合は、影響度の水準に拘わらず、重大度が最も高い「3」としています。パブリック性が「中」で影響度が「大」または「中」の場合と、パブリック性が「小」でも影響度が「大」の場合は重要度が中程度の「2」としています。こうして危機の内容に応じて、エスカレーションルールを定めています。

同社では危機発生時の報告ルートについても原則を定めています。

エスカレーション対象となる事業と危機の重要度に応じてエスカレーションルートを定めており、必須の報告先と必要に応じて報告する先を特定しています

- 報告を受ける側が判断しやすいよう、具体的記述をして可能な限り定量指標を含めるよう求めています。

事例　ある消費者向サービス業におけるエスカレーションルートの例



エスカレーションルールが効果的に機能するために

エスカレーションルートにリスクマネジャーを組み込む

- エスカレーションルールによって危機の内容によって報告を上げる先の階層が規程され、多くの場合にその報告対象となっている人物が危機対応のために中心的な役割を担います。しかし、リスクマネジャーも事業リスクマネジメント推進の中心人物として、危機対応に関する情報を把握する必要があります。Eメールの“CC”のような形で、危機対応についての全ての連絡はリスクマネジャーにも届く仕組みを作っておくことが有効です。
- また実際に発生している事態は、エスカレーションルールで想定しているうちのどの事態に該当するのか不明確なこともあります。こうしたときは、リスクマネジャーに対して報告を行い、重大性の判定はリスクマネジャーが行うと決めておくことも迅速な対応のために効果的です。

エスカレーションルートにリスクマネジャーを組み込む

- エスカレーションルール自体は平常時に作成しておくものですが、実際に危機が発生した時にルールが機能するように風化させない工夫が必要です。定期的に予行演習を行って、危機発生についての現実感を抱かせることや、人事異動や組織変更のタイミングでエスカレーション対象とする事象や報告先の見直しをすることが有効です。
- 更に、重大危機だけでなく業務の中で比較的頻繁に発生するような事象もこのルール体系の中で扱う（例えば課長まで報告するものもこのルールの中で特定する）ことで、日頃からルールが目に触れるようにします。こうすることで、このルールで情報を報告することに抵抗感をなくして、リスクに関してオープンな風土を作るようにします。

危機管理マニュアルの作成

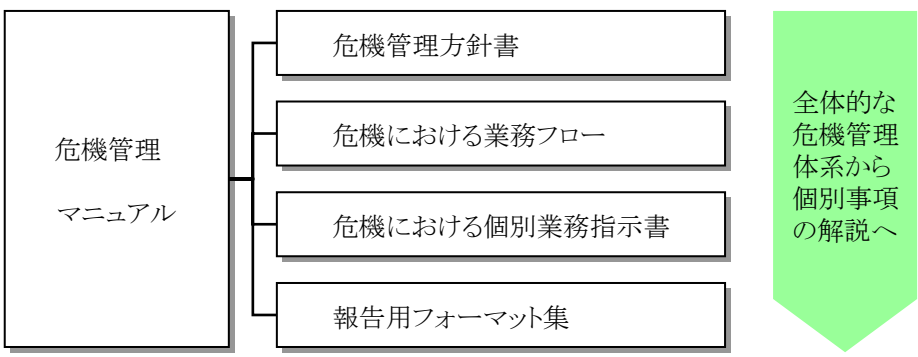
企業として特に対応を要するリスクについては被害状況を想定して対応目標を決めたうえで（例えば○○日以内に復旧する等）、緊急時の組織体制を定め然るべき対応が取れるようにします。

こうした事項に関するノウハウをまとめて解説した危機管理マニュアルを作成しておき、関係者は平常時にそれを読んでおくことで、危機発生時に取るべき施策を理解して実践できる体制を確保します。

マニュアルは階層構造を持たせ読みやすく記載する

- 危機管理関係者は平常時にマニュアルを読んで理解しておき、危機発生時に指示や進捗チェックを行うのに役立つようにします。図の例のようにマニュアルは階層に分けて作成して、最上位マニュアル（図の例では「危機管理方針書」）以外は一階層上位のマニュアルに対する「各論」として詳細事項が記述されるようにして、各部分が全体体系のなかで整然と位置付けられるようにします。このように内容を整理しておくと、各人が平常時に全体の体系を理解して熟知したうえで、危機発生時には必要な部分だけを参照するという実践的な活用法が可能になります。

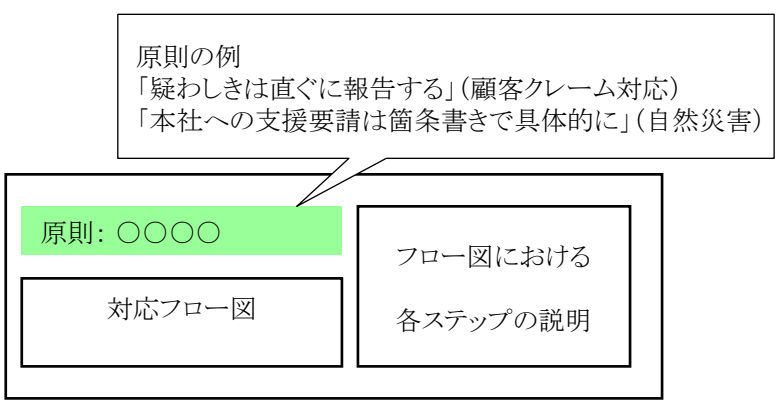
事例　階層構造化されたマニュアルの例



非常にシンプルでわかりやすい作りにすることを重視して、各項の最初の1行を見れば何をすれば良いのかほぼ伝わる

- そして各部門が取るべき行動もフロー図で視覚的に分かりやすくまとめています。

事例　行動原則を1行で示したシンプルさ重視のマニュアル



危機が業務に及ぼす影響を検討して、マニュアル記載内容を決定する

- マニュアルに記すべき内容は、危機の内容や企業の業種・業態によって異なります。自社の業務基盤に重要な影響を及ぼす事態は何で、それがどのような状況下に発生すると考えられ、その場合に優先的に確保されねばならないことは何か、などを考えて実際に役に立つものを作成する必要があります。
- ある企業では1995年の神戸淡路大震災で実際に被災した社員の声をマニュアルに反映させています。こうすることで、読み手により強く訴える内容にしています。
- ある企業の震災対策マニュアルは下記の構成となっています。震災が生じるのが、勤務時間内であるか否か、被災するのが本社(同社の場合は首都圏)か支店か、などで被害と対応策が異なるという認識から同社ではこうした構成のマニュアルを開発しています。

事例　マニュアル構成の例

○○社　震災対策マニュアルの目次

Ⅰ. 本マニュアルで想定する災害状況
Ⅱ. 対策実施計画と運営体制
Ⅲ. 業務手順書(勤務時間中首都圏被災の場合)
Ⅳ. 業務手順書(夜間・休日等の発生への対応)
Ⅴ. 業務手順書(支店被災時)
Ⅵ. 非常用物資の準備
Ⅶ. 教育・訓練

業務手順書
－初期動作
－連絡手段
－被害把握
－お客様窓口設置
－行政への報告
などについて記載

マニュアルに則った訓練を実施する

- マニュアルを作成したうえで、それに則った危機対応訓練を実施することも有効です。
- 訓練を行うことで実際の危機発生時に組織の対応能力が高まるうえ、マニュアルの内容の実行可能性についてもある程度検証することができます。
- 大幅なマニュアル改訂があったときや年一回の定期的な人事異動のときが、訓練を実施する時期として適しています。

5.2.3　危機発生時の対応

危機発生時の行動として、危機対応組織の構築・情報管理・復旧活動の3つのプロセスに関する留意点を説明します。また危機を脱した後に再発防止策を検討することが非常に重要であることから、この点についても解説します。

危機対応組織の構築

危機発生時には対策本部となる組織を設けて対策にあたります。

緊急対策組織体制の構築

エスカレーションルールで定められた責任者が中心になり関係者を集めて、緊急対策討議のための組織を設置します。

招集対象となる部門としては危機の内容に直接関わる部門はもちろんのこと、多くの場合に広報・法務・営業等が含まれます。危機が顧客にどのような影響を及ぼしうるか、従ってどのような対応を取るべきかについて的確な判断をできるように、営業部門の関与を求めることが多くの場合に必要です。

災害時における危機対応組織構築

自然災害などで拠点が損傷を受ける場合は、対策本部について更に物理的な支援体制についての考慮も必要です。

ある企業では、被災地域に隣接する地域の支店が基本的に臨時対策本部となって支援を行うことにしています。ただし、隣接地といっても多くの場合に数ヶ所存在するので、該当すると考えられる支店では先ず対策本部を作ってしまうことにしています。時間が経過して複数支店で対策本部が設けられていることが明らかになれば、そのうえで機能統合を図ることにしています。こうすることで同社では迅速な対応を図っています。

情報管理

危機発生時に的確な行動を取るためには、現実に起きていることについての情報を正確に把握することが必要です。

情報管理の留意点

対策本部では実際に発生したことや時々刻々変化する状況に関する情報を収集し分析していきます。各担当者は分担して任務を行っていることが多いため、必ずしも全体的な情報を把握しているわけではありません。また、危機状況下のプレッシャーから誤報・誤解も生じがちです。何月何日何時現在の情報として起こっている状況を取りまとめて、関係者全員でその情報を共有することが大切です。

具体的な情報の内容としては、

①現在までに判明した事件事実の概要
②自社で現在実施している対応策の内容と状況
③今後の見通し
④依然不明な点
⑤次回の状況連絡予定時刻

等を含むことが多くの場合に有効です。

最重要事項はヘッドライン（見出し）として大書したり、前回発表からの変更があった点についてはアンダーラインを引く等、受け手にとって分かりやすく伝えるようにします。

ステークホルダー向けに情報を発信する

情報がある程度集まった段階で、顧客・従業員・社会といったステークホルダーごとに伝えるべき情報を整理して、情報発信を適切に行う必要があります。こうすることで、ステークホルダーと事態についての情報を共有化し、かつ今後の自社の対応体制について支持を取り付けるようにします。不祥事等により記者会見を開くこともこの作業に含まれます。

情報発信の基本はタイミングと透明性です。危機事態が発生してから相当の時間が経過するまで何も発表を行わなかったり、限られた情報しか開示しなかったりすると、企業姿勢が問われ不信感が募る原因となります。ステークホルダーに対する説明責任を果たすことが重要です。（情報開示と企業の評判・信用等に関する問題については、本書の「5.1.5 レピュテーションリスク」の説明も参照してください。）

復旧活動

事態の収束に向けて、誰が何をするかというアクションプラン（行動計画）を立て実行するようにします。アクションプランでは危機管理マニュアルで想定されている対応プロセスを基本として、当該の危機の状況を勘案しながら具体的な行動内容を明らかにします。

アクションプランの策定と実行

実践的なアクションプラン策定のために、各組織の長が意思決定するにあたり必要となるチェックポイントを洗い出してまとめておくようにします。

例えば、何らかの事由で受注システムが一定期間停止した事態における営業部門の取るべき行動としては、以下のようなことが考えられるでしょう。

参考　対応アクション表の例

受注管理システム停止時における営業部門の行動例

初期対応	1. 在庫の確認 2. 手書き注文処理への切り換え準備 3. 顧客への説明準備
応急処置	1. 賠償事案の有無検出 2. 緊急案件について手書き注文処理実施
暫定業務による稼動	1. 緊急注文品の発注管理・出荷確認 2. 顧客からの照会への応答 3. 復旧見込みについての顧客への連絡 4. 復旧後発送の受注および注文ストック管理
収束期の活動	1. 注文ストック分の手配管理 2. システム受注の再開と正常稼動の確認 3. 顧客への謝罪方針の決定と実行

アクションプラン策定時の検討事項

アクションプランの策定は以下のような事項について検討しながら進めるようにします。

- どのような選択肢があるか
- プランはどの程度効果的と考えられるか
- プラン実行のために社内外の誰の協力を必要とするか
- いつまでに本格実施できるか
- 進捗状況をどのように把握するか
- プランについていつどこまで情報開示する
- プランが失敗時のリスクおよび成功しても残るリスクは何か

等

再発防止策の検討

危機的な状況が過ぎ去って通常の業務に戻ることができても、同様の事態が発生することのないように危機発生に至った原因を徹底的に分析して、抜本的な対策を講じるようにします。

対策は全社レベルで行う

- ある部門で発生した危機について当該部門だけの問題として終らせるのではなく、他の部門でも生じうる可能性を検討します。リスクマネジャーは危機発生に関する原因分析結果をもとに、他部門についても調査・ヒアリングを行い、類似の事象が発生する可能性があれば問題点を指摘して改善を求めます。
- こうすることで会社全体で以降に同様の危機が発生する可能性を事前に排除することができるので、リスクにより強い会社になることが可能になります。

組織風土の問題も含めて検討する

- 危機に至った原因の調査では、危機を引き起こした直接的な原因だけではなく、「危機を食い止められなかった原因」や「危機を大きくしてしまった原因」などの間接的な原因ないし遠因まで明らかにすることが重要です。
- 危機発生の現場を調査すると、組織風土の問題、つまり「以前から警告する声はあったが聞き入れられなかった」「一部の従業員は危険性に気付いていたが言いにくい雰囲気があった」などの問題が明らかになることがあります。危機発生を機会にこうした問題も改めるようにしないと抜本的な解決にはなりません。
- 組織風土の問題は、当該部門だけでは発見・解決することが難しい場合も多くありますので、リスクマネジャーが主体的に関与して積極的な取組みをすることが望まれます。

危機対応をナレッジ化する

- 特定部門で発生した危機は多くの場合に他部門でも起こり得るものであるため、自社が危機を収束させた際に取った行動とそこから得た教訓をナレッジとして全社的に共有されるようにします。危機管理マニュアルを更新して内容を反映させるのはもちろんのこと、トレーニング等を実施して危機発生時の対応だけでなく事前予防に関するナレッジも共有化するようにします。Z

再発防止策を社外に開示する

- 危機を乗り越え再発防止策を策定したら、その取組み内容を社外に開示することも検討すべきです。危機発生後の記者会見で「今後こうした事態が二度と生じないよう社員一同全力を尽くします」という言葉が発せられることはよくありますが、危機を起こしたいと願っている企業などあるはずありません。また、残念ながら、そうした企業が類似の危機の発生を繰り返した事例もありました。
- 再発防止の決意を示すことも大切ですが、真に社外に対して訴えるべきなのは自社の苦い経験から同様の危機を起こさないために何をこれからしていくかということです。再発防止策の内容については、社外の疑問を想定して徹底的に検討したうえで発表することです。

5.2.4　事業継続計画(Business Continuity Plan)

ここではまず、事業継続計画とは何かについて説明し、具体的に導入検討のステップをどのように進めていくかを順を追って解説していきます。

今回はITシステムの例をご説明していきます。

事業継続計画（BCP / ビジネス・コンティニュイティ・プランニング）とは

災害や事故等の発生に伴って通常の事業活動が中断した場合に、可能な限り短い期間（時間）で事業活動上最も重要な機能を再開できるように、事前に計画・準備し、継続的メンテナンスを行う1つのプロセスのことです。重要な事業活動の再開にフォーカスをあてている点が大きな特徴です。

わが国では、「ビジネス・コンティニュイティ・プランニング」という用語自体は、ビジネス用語としてまだ一般的ではないものの、事業中断への備えという点では、危機管理やリスクマネジメントの一環として、あるいはその他の枠組みの中で、すでに多くの企業が取り組んでいます。重大リスクが顕在化し、図らずも事業中断に至ってしまった場合であっても、いち早く重要な機能を再開・復旧し、事業を継続していく上で、「ビジネス・コンティニュイティ・プランニング」は企業経営にとって、不可欠なものといえます。

今日の事業活動においては、ITシステムへの依存度が飛躍的に高まっており、システム面から見た事業継続計画が不可欠になっているため、ITシステムにおける事業継続計画（BCP)を主に取り上げます。

事業継続計画(BCP)の必要性

ビジネスの情報システムへの依存度が増加したことにより企業のプロセスは劇的に変化し、複雑化の一途をたどっています。こうした背景から災害などの緊急事態により事業が中断した場合の、事業の復旧までに見込まれるコストを算出することは非常に困難なっています。ここでは、アメリカでの事業継続計画のアンケート・停止期間費用の例を参考にして、事業中断時のコストを大まかに把握する基準を例示します。

参考　停止期間費用の算出

停止期間費用の内訳	
費用	**種類**
生産性損失 (Productivity Loss)	多数の従業員による時間報酬の超過
収益損失 (Revenue Loss)	直接収益損失 賠償の支払い 将来収益の損失 支払い済みの損失 投資収益損失
毀損されたファイナンシャルパフォーマンス (Impaired Financial Performance)	収益認識 キャッシュフロー ディスカウントの損失 (未払い金) 支払い保証 クレジット レーティング 株価
ダメージを受けたレピュテーション (Damaged Reputation)	顧客 サプライヤー 金融市場 銀行 ビジネスパートナー
その他費用 (Other Expenses)	臨時雇用従業員 機器のレンタル オーバータイムコスト

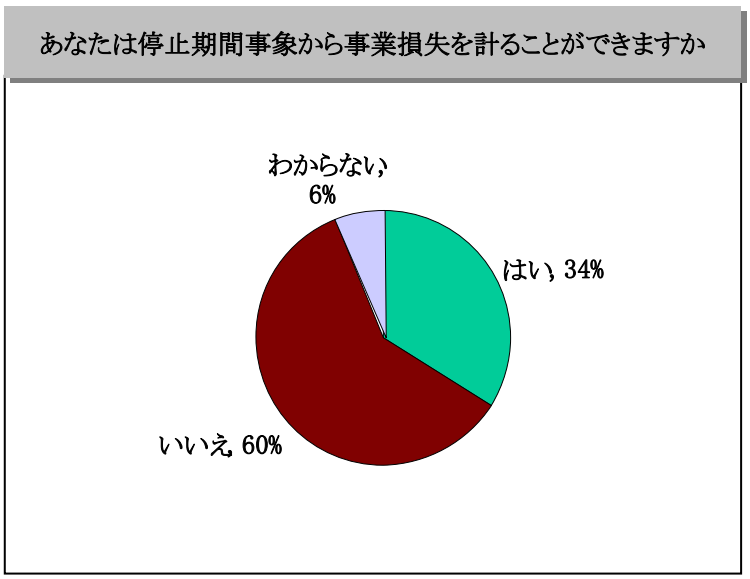
Gartner, High Availability Networking , September 2002 より作成

停止期間費用	
アプリケーション	**停止期間費用**
ファイナンシャル/トレーディング	$40,000 / 分
サプライチェーン	$10,000 / 分
ERP	$10,000 / 分
CRM	$8,000 / 分
E-コマース	$8,000 / 分
E-ビジネス	$8,000 / 分
ビジネス アプリケーション	$5,000 / 分
データベース	$5,000 / 分
メッセージング(Messaging)	$1,000 / 分
インフラストラクチャ(Infrastructure)	$700 / 分

DRJ, How Much Is Enough, Winter 2003 Issue より作成

以下のアンケートは、自社が事業損失を計測できるかどうかわからない企業が存在することを示しています。また別の調査は、企業が事業継続計画を持たない理由に高額すぎる、複雑すぎるといった必要性とは違う理由を挙げている企業が多いことを示しています。これらの企業はどこまで真剣に事業継続計画について検討をしたのか疑問が残ります。

参考　停止期間費用の算出



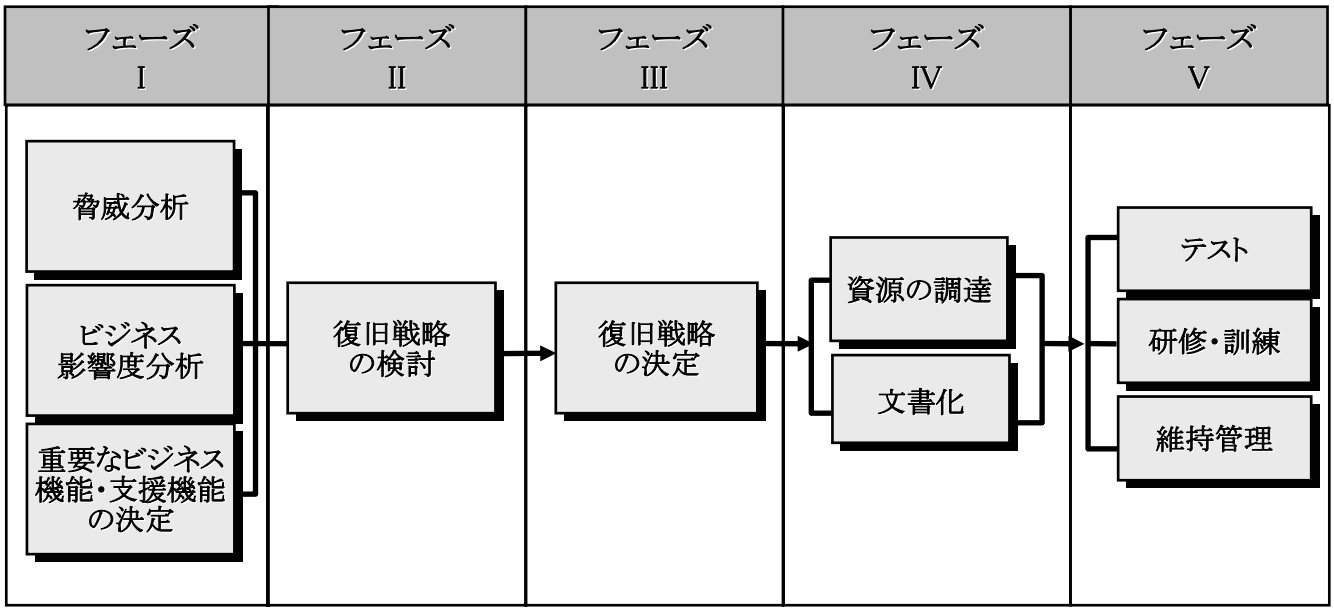
Forrester Research Inc.より作成

事業継続計画欠如のトップ理由	
無計画の理由	%
高額すぎる(Too Expensive)	29%
複雑すぎる(Too Complex)	25%
必要でない(Not Needed in Our Business)	10%
他のサービスが役割を果たしている (Not Needed – Other Service Fulfills Role)	5%
セキュリティの関係で(Security Concerns)	2%
事業エリアでサービスがない (No Service in Our Geographic Area)	2%
その他(Other)	27%

Gartner Dataquest, Survey of 205 professional responsible for BCDR planning, 2003　より作成

事業継続計画(BCP)策定の手順

事業継続計画(BCP)策定の手順は以下のフェーズ1:影響度分析、フェーズ2:戦略の検討、フェーズ3:戦略の決定、フェーズ4:計画の文書化、、フェーズ5:テスト、研修・訓練、維持管理の5つのフェーズがあります。



フェーズⅠ-1 脅威分析(シナリオの検討)

事業継続計画を検討するにはまず、被害のシナリオを作成しなければなりません。どのような被害があった時に、組織がどのように影響を受け、その結果何がおこるのかについてあらかじめ最悪事態として想定しておかなければなりません。以下の例では大地震の災害が発生したシナリオを考えていきます。

参考 脅威分析

災害シナリオの想定	考慮している事象
地震災害	直下型地震、東海地震 震度6以上の地震
2次災害	火災、爆発

脅威分析

1.シナリオづくりに必要なもの
事業継続計画(BCP)におけるシナリオは、組織の弱みと組織に対する脅威の2つを組み合わせることによって、危機のシナリオをつくります。

2.「脅威」の分析
第1に、脅威はどこからくるか、脅威の種類を列挙しなければならない。例えば下記の3つが壊滅的被害をもたらす脅威として挙げられます。
①大地震
②火災・爆発
③津波

3.「弱み」の分析
第2に、組織の弱みを考慮します。
①事業継続計画の欠如
②主要業務のシステムへの依存
③データバックアップ・ルールの未整備

4.「脅威」×「弱み」＝最悪シナリオ
そして第3段階では、脅威と弱みが組み合わさったときに、どのような損失と影響が生ずるかを予測し、優先順位をつけます。
①長期間の操業停止
②財務上の莫大な損失
③組織の信頼性の喪失

危機マネジメント研究会『実践 危機マネジメント』ぎょうせい 2002年より作成

- この分析により、被災時にどのような損失と影響がでるかを把握し、事業継続計画を検討する上での最悪シナリオとして活用していくこととなります。

フェーズⅠ-2 ビジネス影響度分析

脅威分析にて起こりうる最悪のシナリオを検討した後、次にビジネス影響度分析により、時間による影響度を分析します。

ビジネス影響度分析(BIA、Business Impact Analysis)とは
重大なインシデントがビジネス活動に及ぼす影響度を分析し、それぞれのビジネス活動に関する時間的重要度(タイム・クリティカリティ)を特定することです

通常業務別に売上等の直接損失と経費等の間接損害に分け、時間の経過による影響を以下の図のように分析します。

参考　ビジネス影響度分析表

主要業務とリソース等	

	1時間後	8時間後	24時間後	48時間後	72時間後	1週間後	1ヶ月後
売上への影響							
経費への影響							

経費、間接費においては以下の分類のようにさらに具体的なそれぞれの1時間当たりのコストに要する時間をかけることによって総コストを見積もるのが一般的です。

業務機能の停止		1時間	8時間	24時間
a	直接収益損失 (販売損失、配送や請求の遅延)			
b	スタッフへの影響 (スタッフの損失時間×ビジネスの時間コスト)			
c	外部修理技術者のコスト (1時間当たり単価×時間)			
d	内部修理技術者のコスト (1時間当たりプラスビジネスインパクト)			
e	業務機能停止の総費用 (aからdの合計)			
f	予測される事象件数			
	業務機能停止コストの総合計 (e×f)	¥	¥	¥

SEMI 日本地区BCM 研究会編『事業継続マネジメント入門』 共立出版 2005年 より作成

以上、脅威分析とビジネス影響度分析(BIA)の結果をもとに、次に具体的な重要なビジネス機能の決定を行います。

フェーズⅠ-3 重要なビジネス機能の決定

ここでは実例に基づき重要なビジネス機能の決定について解説していきます。対応業務、対応範囲等を決定していきます。

事例 | **事業継続計画**

信販会社における事業継続計画(ITシステム版)

新システムの導入計画に伴い、ITシステムの事業継続計画を検討することとなった。
検討にあたってまず、業務を分類し、影響度を分析した。
例えば、災害時に延滞管理は長期延滞の人は2週間程度は問題ないが初期延滞はすぐに督促しないと延滞になるという統計があるのですぐ対応する必要がある等。
大きなカテゴリーでまず必要性を判断。しかし大分類だと全部重要ということになるので細分化して再度どの業務を残すか検討した。

対応業務

優先度が高くこの企業が選択したもの	この企業にとって優先度が低いもの
非常に影響が大きく中断できない業務 (中枢業務) ①返済管理(初期延滞) ②回収 ③利用停止	影響はあるが優先度が低い業務 (その他業務) ①審査 ②長期延滞 ③貸し倒れ ④業務オペレーション

- この企業ではまず対応業務についての中枢業務とその他業務に分類し影響度を検討しました。
- 信販会社の場合、回収が新規獲得より優先度が高いと言えます。
  - 業務停止可能期間を業務別に検討。「システムが何日使えなくても耐えられるか？」という質問を関連部署におこない重要性が大きく、停止可能期間が短いものに焦点をあわせた。
  - 大きく停止可能期間が2～3日、1週間、1ヶ月といった目安で検討した。
  - なかには日にちによって当日復旧でなければだめなものもある。利用停止は顧客に迷惑をかけるので即時とした。
  - 他社への影響も検討する。提携カードなどの相手先とどういう契約上の約束をしているかも考慮した。

対応範囲

本社と主事業所中心 中枢業務のみ	すべての事業所 その他業務

- 対応範囲についての検討を行い、本社を中心に対応範囲としました。
- この企業は東京に本社機能もシステムも集中しており、社員の8割は東京本社勤務であるため、東京本社とシステムの機能がそこなわれた場合の対処を中心にを検討することにしました。

フェーズⅡ-1　復旧戦略の検討（必要な対策の検討 ）

復旧戦略の検討ステップでは、フェーズ1で決定した重要な業務に対してどのようなシステム資源が必要かを検討します。

事例　**事業継続計画**

必要なアプリケーション

ITにおける事業継続は、対象業務の重要性と共に必要なシステム資源（ハード、ソフト）を特定する必要があります。以下のようなマトリックスを使って、業務Aに関連するアプリケーションを洗い出した後、業務への関与度、必要性を判断します。ここでは業務Aを継続するにあたってアプリケーションAが必須であり対応が必要だと認識されました。

業務	業務の重要性	アプリケーションシステムA	アプリケーションシステムB	アプリケーションシステムC
業務A	High	○		△
業務B	Low		△	
業務C	Low			△

○：業務遂行に必須　　△：利用しているが必須ではない

必要なインフラ資源

また、先に必須とされたアプリケーションシステムAについて稼動に関連するサーバ、回線、マシンセンター等について必要な要素につき、検討をしました。その結果回線a.b という2回線がアプリケーションAの業務を支えているとの分析結果より、対応すべきシステム資源を特定しました。

アプリケーション	サーバー			回線			マシンセンター	
	a	b	c	a	b	c	東京	大阪
A	○			○	○		○	
B		○				○		○
C			○		○		○	

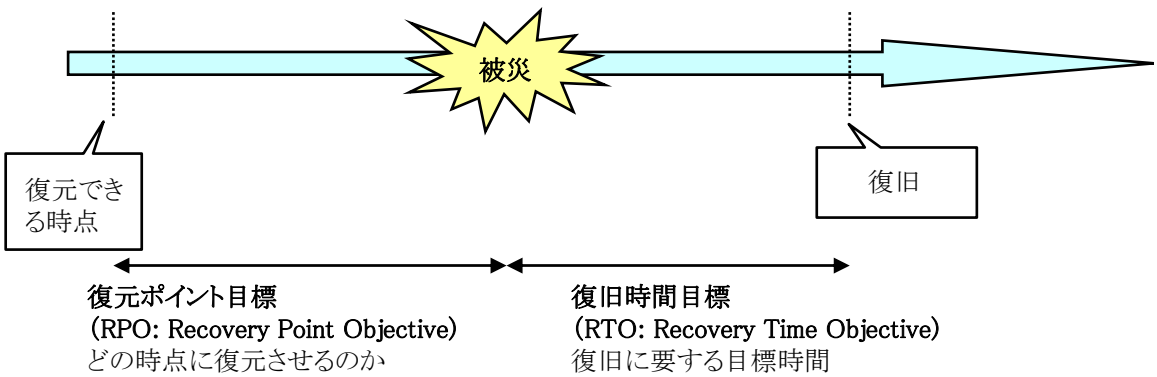
○：業務遂行に必須

フェーズⅡ-2　復旧戦略の検討(ITシステム復旧レベル)

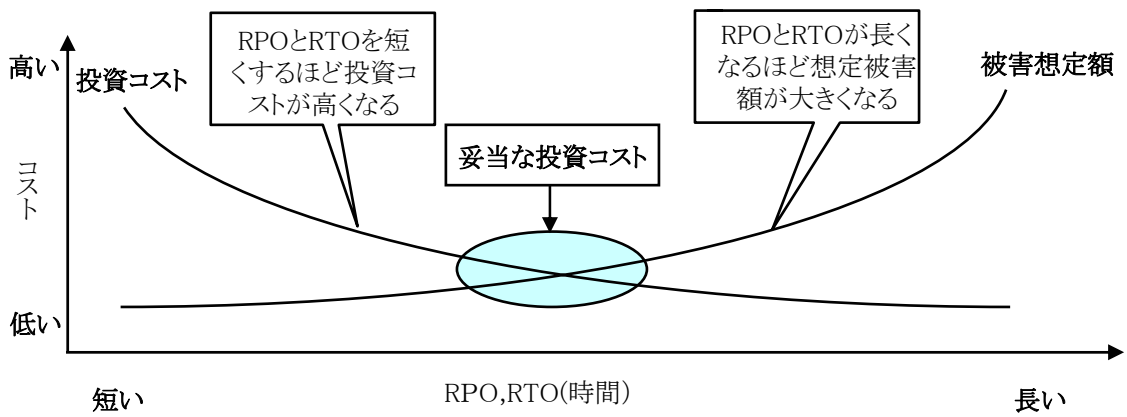
復旧戦略の検討においては、ITシステム復旧レベルについてRPO(復旧ポイント目標)、RTO(復旧時間目標)に基づく投資効果を考慮します。最も投資コストがかかるのは被災の直近の状態にすぐ復旧させる場合でありますが被害額は最小で済むと想定されます。また逆に、被災の起こるかなり前の時点の状態に時間をかけてITシステムおよびデータを復旧させる場合では投資コストは少なくてすみますが、被害額は膨らむと想定されます。

参考　**ITシステム復旧レベル**

RPO, RTOの考え方(ITシステム)においては以下のポイントも考慮します。



RPO, RTOに基づく投資効果の考え方



『日経システム構築』日経BP社 2005年2月号より引用一部修正

ITシステムにおけるポイント*

復旧時間目標(RTO: Recovery Time Objective)は復旧に要する目標時間を検討しますが、主にバックアップサイトの作り方に影響します。RTOが長くてもよければ、バックアップ・サイトではテープを保管するだけでよいかもしれません。一方RTOを短くするためには、ホットスタンバイ等の対応が必要になる可能性があります。

復旧ポイント目標(RPO: Recovery Point Objective)はどの時点に復旧させるのかを検討しますが、バップアップの頻度に影響します。RPOが1時間なら1時間に1回、1日なら1日に1回バックアップを取ることになります。

*『日経システム構築』日経BP社 2005年2月号を参考に作成

フェーズⅢ　復旧戦略の決定

前頁において識別された業務について、重要なデータのバックアップやデータ・センターの体制などの適切な対策レベルについて検討しました。

ハード・ソフト両面からの対策が必要ですが、ハード対策に比べてもれがちなデータ管理も含めたソフトのバックアップを重視し、例えばOSまわりのバックアップなどを追加検討しました。

事例	事業継続計画

リスク対応レベル（IT復旧レベル）

優先度が高くこの企業が選択したもの	その他の選択肢

RTO−当日もしくは翌日 RPO−被災前日の状態 対策−日次データバックアップ	RTO−1週間以内復旧 RPO−最長1週間 対策−週次データバックアップ	RTO−当日復旧（4時間） RPO−被災直前の状態 対策−リアルタイムバックアップ

- 必要なIT復旧レベル
  - オンラインによる重要業務は当日もしくは1週間以内に復旧すればよい。（RTO）
  - オンラインによる重要業務は被災前日の状態に復旧すればよい。（RPO）
  - 必要な対策を日次、週次データのバックアップと判断した。

①二重回線 ②データの保管ルールの徹底 ③環境整備 バックアップセンターなし	①代替拠点 ②リアルタイムデータバックアップ ③環境維持 バックアップセンターあり

- 必要な対策

  ー対応する業務を決めたあと、サーバーの場所が分散しているので回線の二重化を検討した。またバックアップ追加対象やバックアップ保管期間を検討した。データセンターは耐震性を備えた強固なビルにあるためバックアップセンター機能の構築は見送った。

プライマリの強化 プライマリを守るのに費用をかける。建物を補強する等	**非常時のノンスタンバイ契約** 非常時には一定のサービスを受けられる契約	**コールドスタンバイ** 主系と待機系の同期を行なわずに、主系に障害が発生してから待機系を作動させる方式	**ホットスタンバイ** 待機系は主系と常に同じ状態を保っておき、主系に障害が発生すると即座に待機系に処理が引き継がれる

- データセンターの対応

  ー　主に以下の4つの対応形態があるが、バックアップ機能の構築を見送ったかわりに現在のデータ・センターについて建物内部の補強を図ることとした。

事業継続計画のレベル

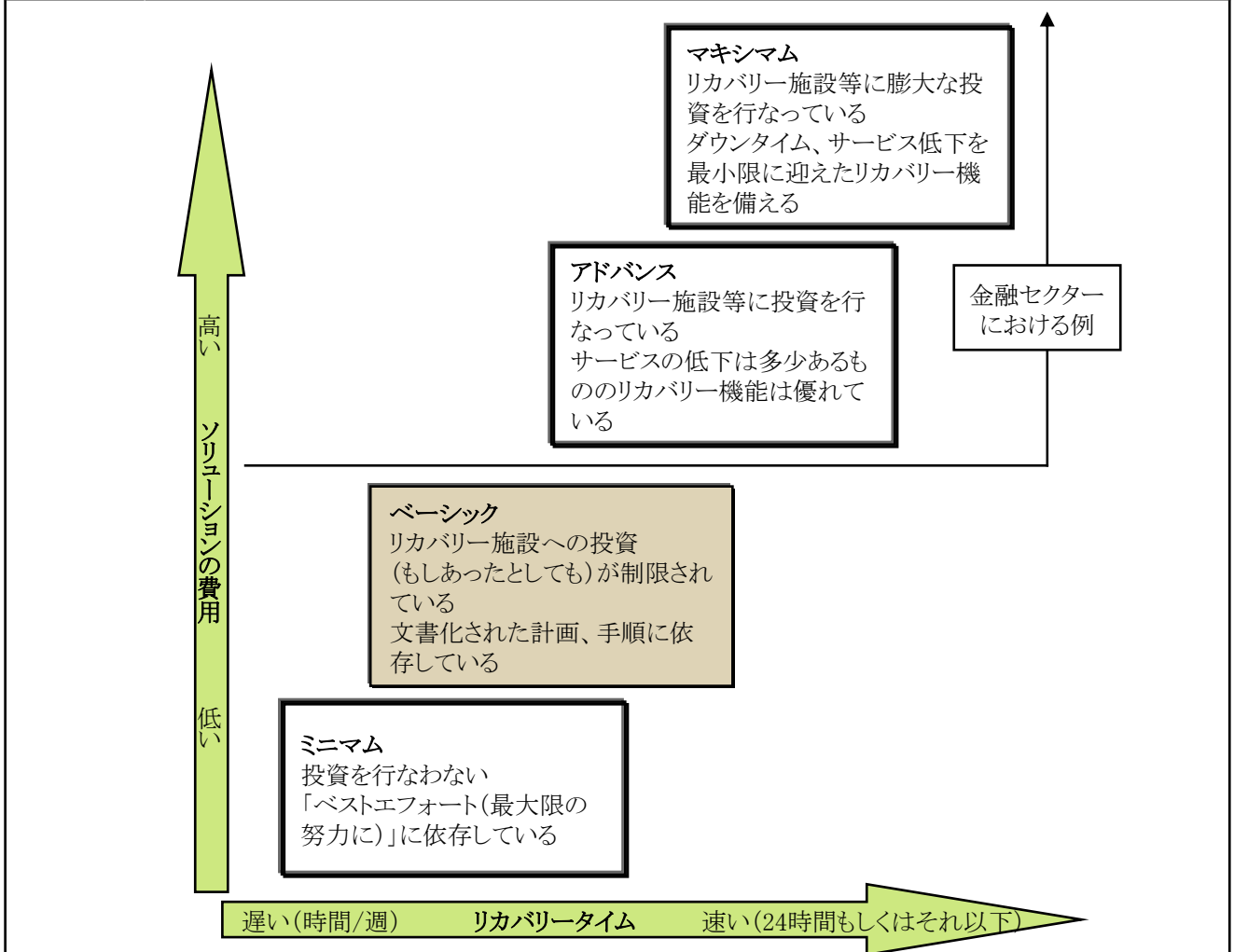
今回の検討はベーシックレベル（下図参照）を基本として進められました。

ソリューション費用およびリカバリー時間をマトリクスにする考え方から事業継続計画のレベルを大きく4つにわけることができます。投資金額の順にミニマム、ベーシック、アドバンス、マキシマムとするという考え方です。 投資費用が少なく、リカバリータイムが遅いものをミニマム。投資費用が多く、リカバリータイムが速いものをマキシマムとしています。

上の2つは主に金融セクターでの取り組みとなっています。これらレベルは、業種や企業の特性により選ばれるべきであり、それらに合ったレベルであることが必要です。おのずから金融機関や公共性の高い企業とそれ以外の企業ではレベルも変わってくるでしょう。

先にも述べたように事業継続計画にどの程度の費用を投資すべきかを判断することが、企業にとって最大の課題となっていますが、本事例ではリカバリー施設に限られた投資を行なうベーシックな対応を行いました。

参考　事業継続計画のレベル



英国銀行協会（著）『ビジネス継続マネジメントガイド』中央経済社 2004年 より作成

対策とコストのバランスがとれているか
ベーシック事業継続計画（BCP）採用：
最終的に経営トップが関与し、意思決定

フェーズⅣ-1　資源の調達

フェーズⅣ資源の調達では決定された復旧戦略について実際のシステムやデータ復旧に必要な資源を調達します。具体的には、バックアップセンターの手配やオフサイトストレージプログラム等の契約等が挙げられます。

◆ 事業継続計画（BCP）資源調達についてのチェックポイント

- 通信、伝達手段の確保
- バックアップセンターやオフサイトストレージプログラム等の契約
- プライマリーデータセンターの強化作業
- 非常用電源の確保
- 空調施設稼動用水源の確保

◆ 事業継続計画（BCP）IT以外の資源調達チエックポイント

IT関連以外の資源とサービスの確保

- 事業中断保険の調達
- 移動手段の確保（バイク等）
- 非常時の作業人員の確保

事業継続プランを発動するケースでは停電や交通手段の障害といったことを視野に入れ、あらかじめ必要とされる資源を準備しなければなりません。たとえば移動手段がない場合バックアップセンターを持っていても動かす人員がそこまでたどり着けないというケースも考えられます。

- 昨今ではサプライチェーンのつながりは複雑になってきているので、そのことを考慮に入れた資源調達を考える必要がある。
- できる限り、1つではなく、複数の手段、調達先を確保し、計画書に盛り込むことが必要である。

フェーズⅣ-2 文書化

フェーズⅣでは決定された復旧戦略について詳細な手順およびマニュアルを作成します。ここでの注意点はシステムやデータ復旧の手順と共に、ITが使えないことを想定した手作業時の業務手順マニュアルを作成し整備しておくことも必要となります。

◆ 事業継続計画(BCP)文書化のチエックポイント

重要業務の優先順位付けがしっかりなされているか

業務手順が詳細に記載されているか

アウトソーシング先のサービスレベルを考慮し作成がなされているか

作業手順だけではなく、計画の目的やゴールも記載されているか

それぞれの役割や責任、権限が明記されているか

◆ 事業継続計画(BCP)手作業についてのチェックポイント

ITに頼らない復旧手段の文書化

ITに頼らないマニュアル・手順の作成

通常時に比べさまざまな制約があることを考慮の上作成すること

事業継続プランを発動する多くのケースでは何らかインフラの障害やまた、予期せぬトラブルが発生することがあり、システムやデータの復旧にすぐに取りかかれないことも考えられます。また、システムが稼動するまでの間は手作業で業務を行なうことが不可欠になってきます。その時に手作業での業務マニュアルを用意していないといざという時に混乱をきたすこととなります。システム停止時の手作業業務遂行の段取りをあらかじめまとめておくことはシステム対応と共に非常に重要なポイントです。

以下、手作業時業務マニュアル作成・運用のポイントを挙げましたのでご参考ください。

手順・マニュアルにおいて、中枢業務に必要なスタッフ、データ、文書、帳票、事務用品、通信手段を明記する必要があります

手順・マニュアルによる、訓練を十分おこない不備がないか確認をしておく必要があります

障害復旧に必要となる期間と事業継続の緊急性から、手作業が必要になるシナリオをあらかじめ複数想定しておく必要があります

フェーズⅤ　テスト、研修・訓練、維持管理

フェーズⅤでは作成された事業継続計画についてテスト、研修・訓練を行います。実際のテストや訓練の中で手順およびマニュアルに不備がないか。計画は有効に機能するかといったことを確認します。また、テストや訓練時に発見された不備に関して改定をおこない計画をより完全なものに近づけます。

◆ 事業継続計画(BCP)テスト・訓練についてのチエックポイント

訓練計画の立案がなされているか

訓練計画のチエックリストに漏れはないか

テスト・訓練の頻度は妥当か(最低年1回)

テスト・訓練の実行がなされているか

テスト・訓練後に検証と不備の改善がおこなわれているか

- 実際の事業継続計画策定時にはシステムインフラとともに、対応体制整備・訓練実施が重要となります。(緊急時連絡網、復旧時の要員・場所等)
- 事業継続計画においては、緊急事態経験後、訓練の実施後には必ず、計画の有効性を検証し、是正・改善を行います。

金融機関を対象とした日本銀行の考査においては事業継続計画の以下のような点も重要な点とみられています。

リスクシナリオをしっかりと考えているか

ロストデータ対策が考慮されているか(切り替え時)

バックアップ後のシステムを元に戻すプランを考慮しているか

5.3 内部統制

ここでは内部統制について、下記事項を中心に説明します。
- 内部統制の意義
- リスクマネジメントと内部統制
- 内部統制の継続的見直し

5.3.1 内部統制とは

昨今、内部統制という言葉が色々な場面で使われるようになってきました。しかし言葉を目にしたことはあっても、内部統制とは一体何なのかを理解している人はまだあまり多くないようです。

企業を目的地へ向かって走る自動車に例えると、販売や生産等の機能はエンジンに当たります。それに対し内部統制は、車を安全に効率良く走らせるための各種制御装置と言えるでしょう。

内部統制は企業の制御装置です

ドライバーがハンドルを切った方向に素早く曲がる、異常発生時に警告ランプがつく、各種の安全装置等の様々な仕組みによって、車はドライバーの意図に従って安全に走ります。企業においても同様です。ドライバーである経営者の意図が従業員に浸透する、問題が適切に経営者に伝わる、各部署でミスや不正を予防する、というような様々なことが常に確実に行われないと、安定した事業運営ができません。そのために企業に構築された様々な体制やルール、手続などが内部統制です。

これは特に目新しい仕組みなどではなく、各種規程や職務分掌、管理職の承認行為など、従来からある管理の仕組み全般が内部統制に該当します。

多くのリスクは内部統制の構築・運用によって低減できる

例えば現金の盗難や持ち出しというリスクに対する対策を講じる場合、金庫に保管するだけでは十分ではありません。鍵の管理方法や責任者の役割、出納の手続などの各種ルール（内部統制）を定めて適切に運用することで初めて、今後も継続的にリスクの発現を防ぐことができます。

企業を取り巻くリスクのうち多くは、そのリスクに応じた内部統制を社内に構築・運用することで継続的に低減することが可能です。その意味では内部統制は、汎用的なリスク対策手段であると言うことができます。

どのようなリスクについて内部統制が有効な対策になり得るかについては、「5.3.2 リスクマネジメントと内部統制」で詳述します。

内部統制の具体例

内部統制についてもう少し具体的なイメージを持てるようにするために、実際の業務プロセスである購買業務を例に個別の手続や体制を示していきます。

日常的な管理手続(内部統制行為)における具体例

承認、権限付与、査閲(チェック)、調整、業務結果のレビュー などが実際の内部統制における手続となります。これらの内部統制における手続を内部統制行為といいます。参考として購買業務における具体例を示すと下記のようになります。

購買業務プロセスに含まれる内部統制(一部)

承認:購買依頼書は、製造部の部長の承認を得ている

権限付与:購買依頼書の作成は、製造部の特定担当者のみが実施できる

査閲(チェック):購買部が購買依頼書が製造部長の承認を得たものか査閲(チェック)する

調整:購買部が買掛金残高について仕入先と残高の確認・調整を行う

業務結果のレビュー:購買部長が月次で仕入高や買掛金残高の内訳をレビューしている

体制等における具体例

上記の日常的な管理手続以外にも、下記にあげる体制などが内部統制の具体例として考えられます。

経営者の正しい姿勢や倫理観の周知徹底
(社長のメッセージ、中期経営計画、倫理綱領 など)
明確な相互牽制機能の確立や特定者への権限集中の回避
(職務権限・責任の明確化、職務分掌 など)
経営上必要な社内外の情報を入手・活用する手段の確立
(定例報告・会議、内部通報制度、顧客窓口 など)
経営上のリスクを識別し、適切な対応を検討する仕組み
(リスクマップ、リスク管理部署設置 など)
業務執行部門から独立した立場でのモニタリングの確立
(内部監査部門、クロス・チェックなど)

内部統制のフレームワーク

リスクマネジメントの一環として内部統制を構築し運用しようとする場合、参考となるフレームワークは以下の通り複数存在します。この中でも最も有名であり、ディファクトスタンダードとしての位置づけにあるといえるのが「COSO-内部統制の統合的枠組み」です。

フレームワーク	説明
COSO-内部統制の統合的枠組み	トレッドウェイ委員会組織委員会が発表し、米国公認会計士協会（AICPA）、財務担当経営者協会（FEI）、内部監査人協会（IIA）その他の団体によって支持されています。米国で最も有力なフレームワークです。当該フレームワークに関しては、次項にて詳しく説明します。
CoCo -統制モデル	カナダ勅許会計士協会の統制基準委員会（Criteria of Control Committee of the Canadian Institute of Chartered Accountants）が発表したモデルです。
ターンブル・レポート （Turnbull Report）	ロンドン証券取引所の上場規則に基づくディレクター・ガイダンス（Guidance for Directors on the Combined Code）：イギリス・ウェールズ勅許会計士協会のコーポレートガバナンス委員会がロンドン証券取引所と協力して制定したもので、1999年に発表されています。ターンブルレポートは企業が重要なリスクを認定、評価、管理し、関連する内部統制システムの有効性を評価することを要求しています。
ACC-オーストラリア統制基準	オーストラリア統制基準（Australian Criteria of Control）：オーストラリア内部監査人協会（Institute of Internal Auditors - Australia）が1998年に発表した基準です。
キング・レポート	The King Report：コーポレートガバナンスに関するキング委員会（King Committee on Corporate Governance）が1994年に発表したキング・レポートは、南アフリカにおいて高度なコーポレートガバナンスの基準を推進するものです。
リスク新時代の内部統制	経済産業省は、産業界、学会、会計プロフェッション、法曹界等を代表する委員が集まる「リスク管理・内部統制に関する研究会」を設けて、COSOレポートを参考としつつ検討を行うことによって、内部統制に関する指針「リスク新時代の内部統制　～リスクマネジメントと一体となって機能する内部統制の指針～」を2003年6月に策定しました。

内部統制の定義

内部統制の定義は、内部統制に関する各種フレームワークごとにそれぞれ決められています。
以下は内部統制フレームワークの中でもディファクトスタンダードともいえる「内部統制の統合的枠組み」（トレッドウェイ委員会組織委員会：Committee of Sponsoring Organizations of Treadway Commission、以下COSO）及び「リスク新時代の内部統制」（経済産業省、リスク管理・内部統制に関する研究会）における内部統制の定義です。

「COSO-内部統制の統合的枠組み」による定義

内部統制は、以下の範疇に分けられる目的の達成に関して合理的な保証を提供する事を意図した、事業体の取締役会、経営者およびその他の人々によって遂行される一つのプロセスである
- 業務の有効性と効率性
- 財務報告の信頼性
- 関連法規の遵守*

＊「内部統制の統合的枠組み」トレッドウェイ委員会組織委員会 1992年

「リスク新時代の内部統制」による定義

内部統制とは、企業がその業務を適正かつ効率的に遂行するために、社内に構築され、運用される体制及びプロセスである。その構築・運用の水準は、業務の適正かつ効率的な遂行に合理的に保証を与えることのできる程度まで高められなければならない
（内部統制の目的）
- 事業経営の有効性と効率性を高めること
- 財務報告の信頼性を確保すること
- 事業運営に関わる法規や社内ルールの遵守を促すこと*

＊「リスク新時代の内部統制　リスクマネジメントと一体となって機能する内部統制の指針」リスク管理・内部統制に関する研究会 2003年6月

「COSO－内部統制の統合的枠組み」及び「リスク新時代の内部統制」の内部統制の定義から共通するポイントを抽出すると以下のように表すことができます。

内部統制の定義におけるポイント

内部統制は社内に構築された体制及びプロセスである

内部統制は3つの目的を達成するために構築される

内部統制は合理的な保証を提供する（完全な保証は提供しない）

「COSO - 内部統制の統合的枠組み」の概要

数ある内部統制フレームワークの中でも最も有名であり、ディファクトスタンダードとしての位置づけにある「COSO-内部統制の統合的枠組み」の概要として、COSO誕生の背景やCOSOキューブについて示していきます。

COSOとは

COSOは、本来、トレッドウェイ委員会組織委員会（Committee of Sponsoring Organizations of Treadway Commission）の略称ですが、COSOの発行したレポートで提示された内部統制のフレームワークがあまりにも有名であるため、この内部統制フレームワークそのものを表す言葉として用いられることもあります。

COSOの内部統制フレームワークは、各国の様々な規制のなかにも組み込まれており、広く受け入れられた枠組みとなっています。

COSO誕生の背景

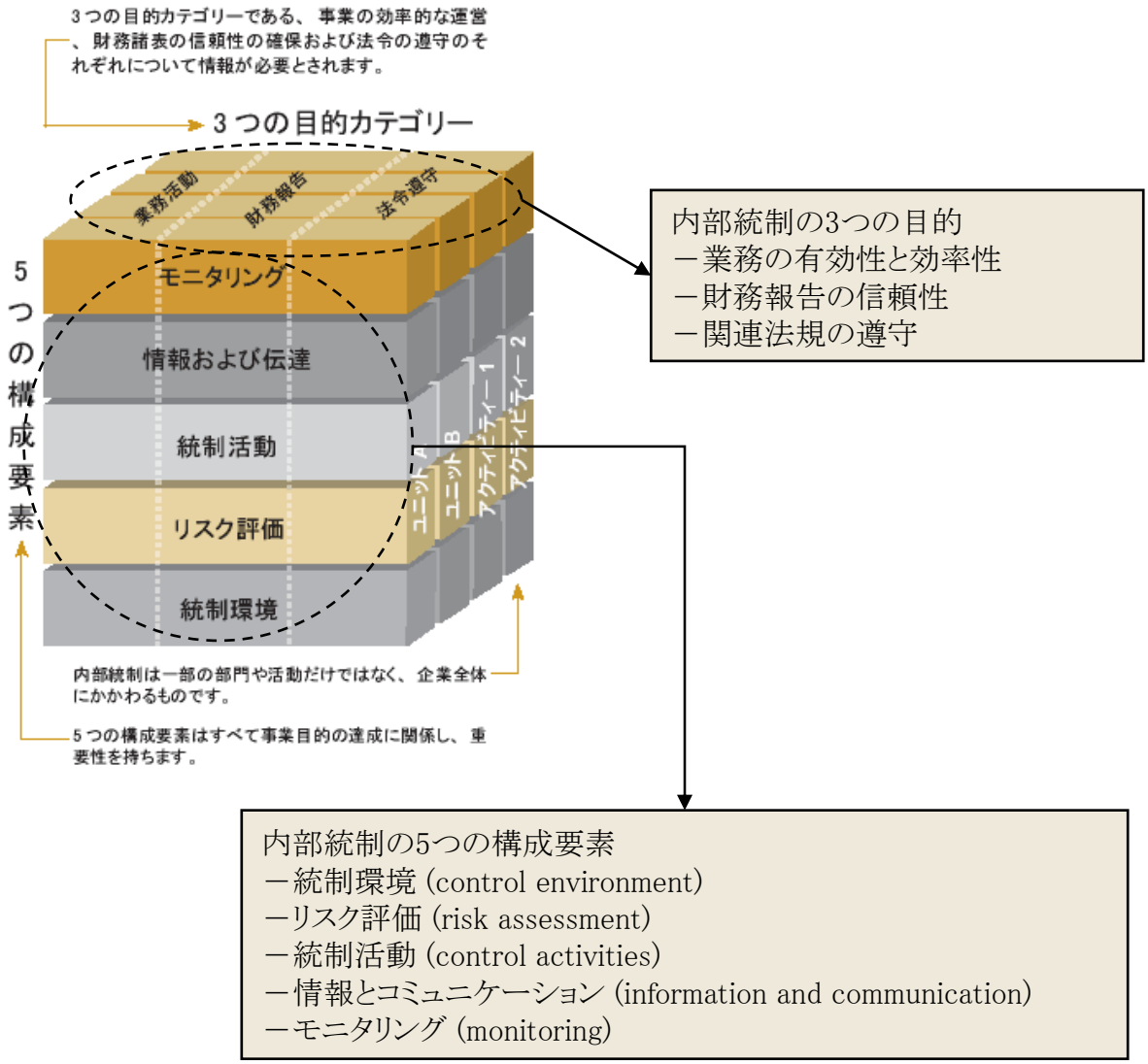
アメリカにおいて、1980年代前半に金融機関を含む多くの企業の経営破綻が大きな社会・政治問題となりました。これに対処するため、1985年にアメリカ公認会計士協会（AICPA）は、アメリカ会計学会、財務担当経営者協会、内部監査人協会、全米会計人協会に働きかけ、「不正な財務報告全米委員会（The National Commission on Fraudulent Financial Reporting）」（委員長J.C.Treadway, Jr.の名前を付してトレッドウェイ委員会と呼ばれた。）を組織しました。

トレッドウェイ委員会は、多方面にわたる検討を行って1987年に「不正な財務報告」と題するレポートを公表して、不正な財務報告を防止し発見するためのフレームワークとその方策を勧告しました。その中で、トレッドウェイ委員会は、内部統制の重要性を指摘し、特にその評価に関する基準の設定を勧告したことから、内部統制のフレームワークを提示することを目的として、トレッドウェイ委員会組織委員会を組織しました。

COSOキューブとは

COSOキューブとは、内部統制においてのポイントをまとめた図のことです。

COSOキューブは、内部統制の3つの目的カテゴリー、5つの構成要素によって表現されるとともに、内部統制は、一部の部門や活動だけではなく企業全体にかかわるものであることも示しています。



トーマツ企業リスク研究所ホームページ、キーワード「COSO」より作成

詳しくはCOSOホームページを参照ください。
http://www.coso.org/

5.3.2　リスクマネジメントと内部統制

リスクマネジメントと内部統制の関係を考える際には、まず企業の直面するリスクを整理する事が必要となります。

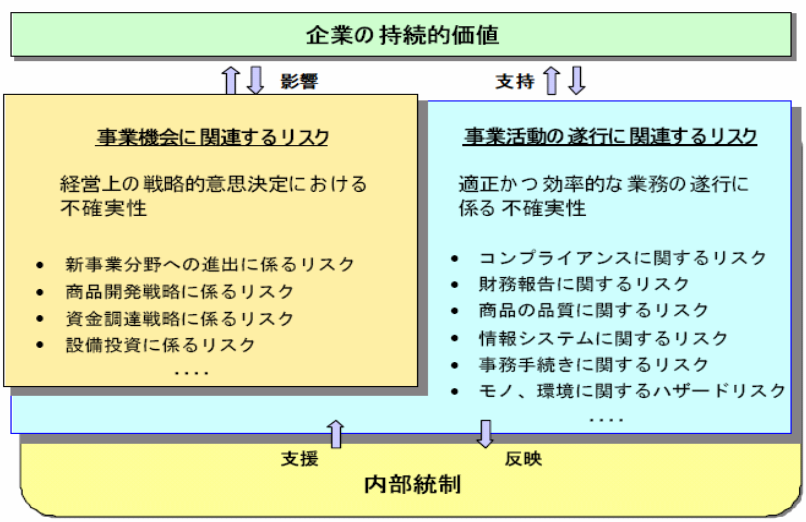
経済産業省「リスク新時代の内部統制」リスク管理・内部統制に関する研究会では、企業の直面するリスクを①事業機会に関連するリスクと②事業活動の遂行に関連するリスクの二つに分類する事を前提に説明しています。

これら二種類のリスクは、どちらも全社的なリスクマネジメントの対象ですが、内部統制との関係はそれぞれ異なります。

企業の直面するリスク

①事業機会に関連するリスク
事業機会に関連するリスクとは、経営上の戦略的意思決定に係るリスクをいう。具体的には、下記の図に記載されているようなものを挙げることができる。

②事業活動の遂行に関連するリスク
事業活動の遂行に関連するリスクとは、適正かつ効率的な業務の遂行に係るリスクをいう。具体的には、下記の図に記載されているようなものを挙げることができる*。



＊リスク新時代の内部統制　リスクマネジメントと一体となって機能する内部統制の指針」リスク管理・内部統制に関する研究会 2003年6月 より作成

リスクへの対応と内部統制

1. 事業活動の遂行に関連するリスクと内部統制
リスクへの対応のうち「事業活動の遂行に関連するリスク」への対応は、内部統制のプロセスの中で直接的に実施される。したがって「事業活動の遂行に関連するリスク」を適切に管理するためには、内部統制を適切に構築し運用することが必要である。

2. 事業機会に関連するリスクと内部統制
「事業活動の遂行に関連するリスク」を内部統制の適切な構築・運用によって管理することにより、経営者は、より適切かつ大胆に判断を行うことができ事業機会に関連するリスク」を含むリスク全体を管理することがはじめて可能となる。

＊リスク新時代の内部統制　リスクマネジメントと一体となって機能する内部統制の指針」リスク管理・内部統制に関する研究会 2003年6月 より作成

また、リスク及びリスク対策を例示して企業の直面するリスクと内部統制の関係を説明したものが下記の表です。

リスクの種類	リスク	リスク対策例	リスク対策と内部統制の関係
事業活動の遂行に関するリスク	顧客の倒産で代金を回収できなくなるリスク	与信管理ルールを定めて適切に運用する	内部統制の構築・運用そのものがリスク対策となっている
	火災により特定の資産が焼失するリスク	火災保険の付保	保険の付保自体は内部統制ではない。ただし重要な資産に適切な保険が付保されることが担保されるように、責任者を決めたり業務ルールを作成することは内部統制の構築となる
事業機会に関するリスク	新商品の発売に伴う不確実性	事前のリサーチ、商品企画、宣伝等、当該商品に関るすべての事業活動	個々の事業活動の遂行に関するリスクを内部統制によって管理する

リスクマネジメントと内部統制の関係

前述の二つのリスクへの対応という意味で、内部統制は、全てのリスクに対応するための前提となり、ひいては、内部統制が、事業に関連する内外の様々なリスクを適切に管理する活動であるリスクマネジメントを支えているといえます。リスクマネジメントと内部統制との関係は以下のようにまとめることができます。

リスク評価と内部統制評価

- リスクマネジメントにおけるリスク対策の多くは内部統制の構築によって達成されます。そのためリスクマネジメントにおけるリスク評価で、リスク対策の実施状況評価の一環として内部統制の整備・運用状況の評価を実施する場合があります。
- なお、内部統制の整備・運用状況の評価については、「5.3.3　内部統制の継続的見直し」で詳述します。

リスク評価結果に応じた内部統制の継続的な見直し

- 「内部統制は「事業活動の遂行に関連するリスク」のみならず、あらゆるリスクの評価及び対応のあり方を踏まえ、ダイナミックに構築・運用されなければなりません。経営者は、リスクマネジメントによるリスクの評価と対応方針に応じて、内部統制のあり方の見直しを継続的に行うことが必要です*。」

リスクマネジメント組織へのフィードバック

- 「内部統制のプロセスの中で対応される「事業活動の遂行に関連するリスク」は、リスクマネジメント組織へフィードバックされ、全体的なリスクマネジメントの中で評価され、対処されなければなりません。すなわち、リスクマネジメントは、「事業機会に関連するリスク」と「事業活動の遂行に関連するリスク」を両方含むかたちで、統合的に行われることが必要なのです*。」

＊リスク新時代の内部統制　リスクマネジメントと一体となって機能する内部統制の指針」リスク管理・内部統制に関する研究会 2003年6月 より一部修正

COSOにおけるリスクマネジメントと内部統制

内部統制フレームワークを策定したCOSOが、2004年9月に今度はERMのフレームワーク（COSO Enterprise Risk Management Flamework ）を発表しました。このフレームワークは従来の内部統制フレームワークをすべて包含し、更に目的の設定やリスク評価の高度化等、全社的な視点であらゆるリスクに対応するための要素が追加されたものになっています。COSO-ERMの説明や内部統制フレームワークとの比較については、巻末の付録を参照してください。

これにより、リスクマネジメントに内部統制は不可欠なものであることや、特に個々のリスクへの対応は基本的に内部統制に委ねられる部分が大きいといった見解が伺えます。

内部統制の限界

内部統制の限界とは、内部統制が機能しない状況のことです。言い換えれば、内部統制自体に内在すリスクそのものと言えます。リスクマネジメントの一環として内部統制を構築・運用する場合には、内部統制の限界について十分に留意する必要があります。

企業構成員の判断の誤りや不注意により内部統制からの逸脱が生じた場合

- 「内部統制は、企業構成員の判断の誤りや不注意等を看過することのないよう、上位者や他部門等による社内記録等の照合、定量的分析などのコントロールやモニタリングを通じて、組織的にリスク低減を図るものですが、コントロールやモニタリングの過程における判断の誤りや不注意等が発生する可能性までをゼロにすることはできません*。」

企業構成員が共謀して、内部統制を無効にした場合

- 「内部統制においては、多くの場合、企業構成員間の相互牽制を通じて適切なコントロールやモニタリングが行われますが、例えば、企業構成員が共謀して社内記録を改ざんしたり、コントロールやモニタリングを意図的に行わないことがあり得ます。この場合、コントロールやモニタリングはその意図したとおりに機能せず、内部統制が無効となってしまうことになります*。」

経営者等が内部統制を無視した場合

- 「内部統制が適切に構築・運用されていれば、重大な法令違反や不適切な社内報告があった場合、このような情報が経営者等に伝達されることが期待できます。しかしながら、この情報が適切に報告されていても、例えば、経営者等がこれを無視して適切な施策を講じなかったり、意図的に法令違反等を放置するなどした場合、内部統制はその構築・運用の目的を果たせないことになります*。」

内部統制の構築当初は想定していなかった環境の変化や新たな事象が発生した場合

- 「内部統制を構築した後に、情報技術の進展などの外部環境や企業規模の拡大などの内部環境の変化が生じることで、構築当初に期待した効果を維持できなくなる可能性や、構築当初にはなかった新たな事象に対して内部統制が機能しない可能性があります*。」

＊リスク新時代の内部統制　リスクマネジメントと一体となって機能する内部統制の指針」リスク管理・内部統制に関する研究会 2003年6月 より一部修正

5.3.3　内部統制の継続的見直し

内部統制の継続的見直しについて、その必要性を説明します。また、内部統制の継続的見直しにおいて最も重要となる内部統制の評価の方法についても、具体的な例を示しながら説明していきます。

内部統制の継続的見直しの必要性

内部統制のもつ動態的な性質及びリスクマネジメントとの関係から、内部統制は継続的に見直される必要があります。

内部統制の動態的な性質

内部統制は、以下の3つの目的を通じて事業目的の達成を支援する仕組みであり、事業活動がダイナミックに遂行されることを支援する動態的な体制及びプロセスであるため、静態的なものと理解してはならない。
（内部統制の目的）
- 事業経営の有効性と効率性を高めること
- 財務報告の信頼性を確保すること
- 事業運営に関わる法規や社内ルールの遵守を促すこと*

＊リスク新時代の内部統制　リスクマネジメントと一体となって機能する内部統制の指針」リスク管理・内部統制に関する研究会 2003年6月 より一部修正

内部統制は、事業活動の変化に応じた体制及びプロセスの見直しが必要である

リスクマネジメントとの関係

内部統制は、リスクマネジメントを適切に行うために不可欠であり、したがって、内部統制はリスクマネジメントを支えるものということができる。一方で、内部統制が有効であるためには、それがリスクマネジメントによる総合的なリスクの評価等を踏まえて、体制及びプロセスを構築し、運用される必要がある*。

＊リスク新時代の内部統制　リスクマネジメントと一体となって機能する内部統制の指針」リスク管理・内部統制に関する研究会 2003年6月 より一部修正

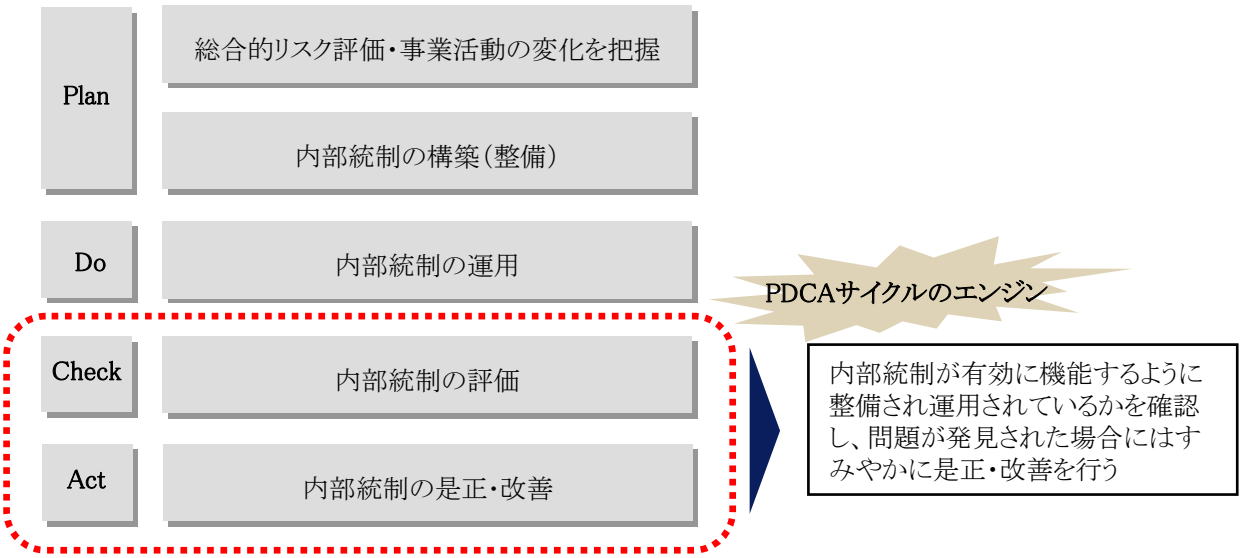
内部統制の有効性を確保するため、総合的なリスク評価に応じた体制及プロセスの見直しが必要である

内部統制におけるPDCAサイクル

内部統制の継続的な見直しは、リスクマネジメントサイクルと同様にPDCAサイクルによって行われます。PDCAサイクルのうち、実務上特に重要になるのが、内部統制が有効に機能するように整備され運用されているかを確認する内部統制の評価（Check）及び内部統制の是正・改善（Act)となります。

内部統制の評価（Check）及び内部統制の是正・改善（Act)は、内部統制におけるPDCAサイクルのエンジンといえます。

内部統制におけるPDCAサイクル



内部統制の評価

内部統制の評価において、実務上実施する場合に留意すべきポイントは複数存在します。

- 評価の実施者
- 評価の方法
- 総合的評価の実施
- 内部統制の評価と内部監査

評価の実施者（誰が評価を行うべきか）

プロセスオーナーによる評価が原則

- 確認の対象となる業務を理解し、現状を把握しているプロセスオーナーが実施する方法が考えられます。具体的には、購買プロセスであれば購買部長、製造プロセスであれば製造部長等が各業務プロセスのプロセスオーナーといえます。
- しかし、実務ではプロセスオーナー（購買部長や製造部長）がひとつひとつの内部統制を確認し評価するのは現実的ではないため、実際は購買プロセスの中でも「発注」や「検収」というようにさらに細分化したレベル（例えば課長やチームリーダ等）で評価を行い、その評価結果に基づいてプロセスオーナーが総合的評価を行う事になります。

評価の方法（どのような方法で評価を行うべきか）

内部統制の評価とは、個々の内部統制行為や体制が内部統制を構築した目的に適ったものかを整備状況(ルールや体制が存在するか、またその内容は妥当か)と運用状況（ルールが実際に遵守されているか）の観点から判断することです。

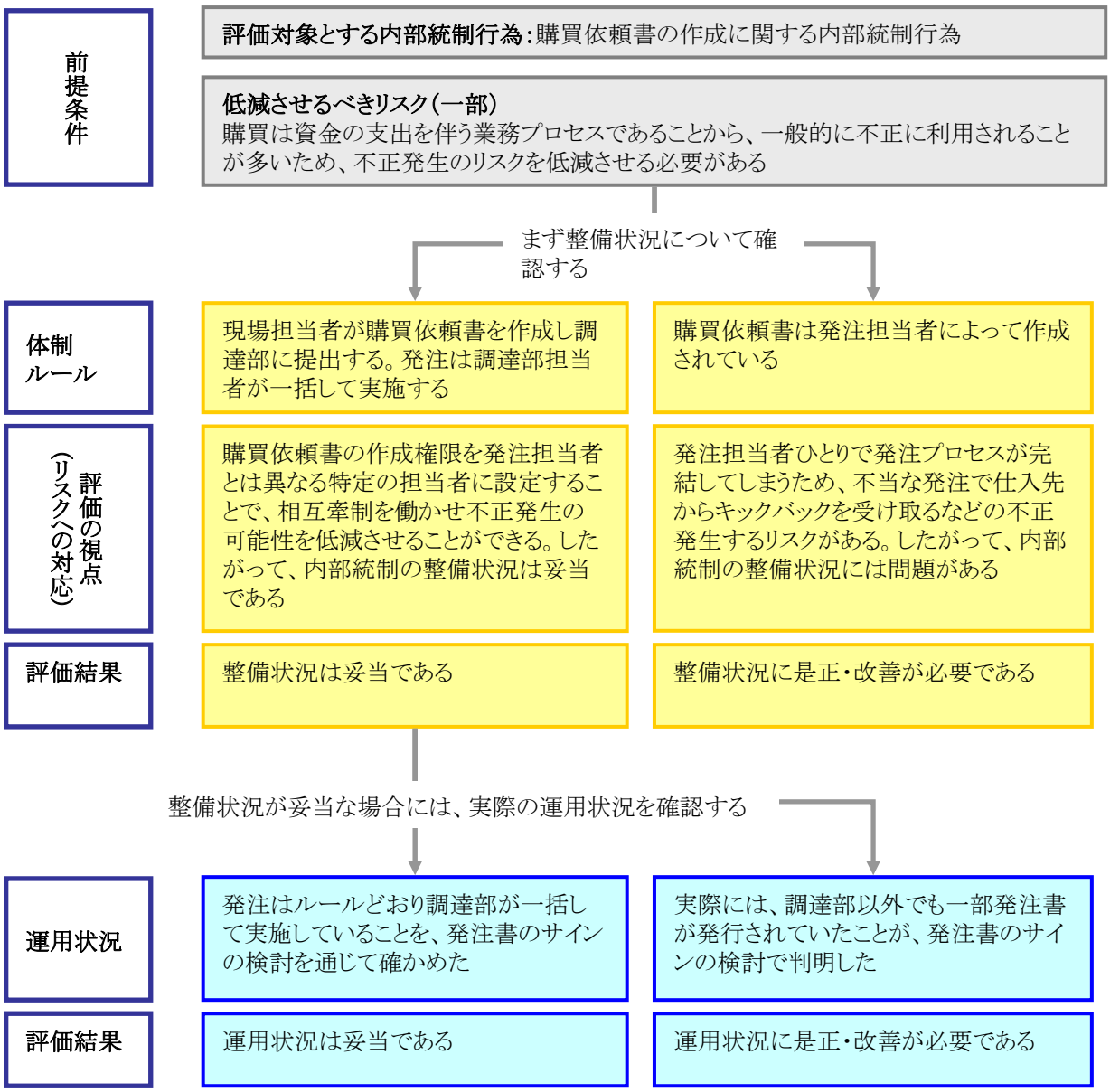
内部統制の評価については、2つの考え方があります。

①リスク分析に基づく評価：特定の業務におけるリスクを把握し、それを予防及び適時に発見することのできる内部統制が整備・運用されているかを評価する方法
②ベストプラクティスとの比較による評価：ベストプラクティス（あるべき内部統制）と現状の内部統制との比較（ギャップ分析）により整備状況を評価し、それが適切に運用されているかを評価する方法

リスク分析に基づく評価を実施する

リスク分析に基づく評価の流れについて、購買プロセスのうち発注サブプロセスを例に説明します。

参考　内部統制の評価の流れ



内部統制のベストプラクティスとの比較による評価を実施する

それぞれの業務におけるリスクを把握し、それを予防及び適時に発見することのできる内部統制が整備・運用されているかを評価する方法は理論的である反面、実務上では作業負荷が高くなり評価者の負担が大きくなるといった問題が生じます。

そこで、企業の標準的な業務を前提とした内部統制のベストプラクティス（あるべき内部統制）を実際の業務と比較し、ギャップを把握することで整備状況を評価し、それが適切に運用されているかを評価する方法も考えられます。

ただし、内部統制のベストプラクティスとの比較は、企業の規模や業態を勘案したうえで比較しなければならないため、内部統制に精通した担当者が必要になる点に留意する必要があります。

総合的評価の実施

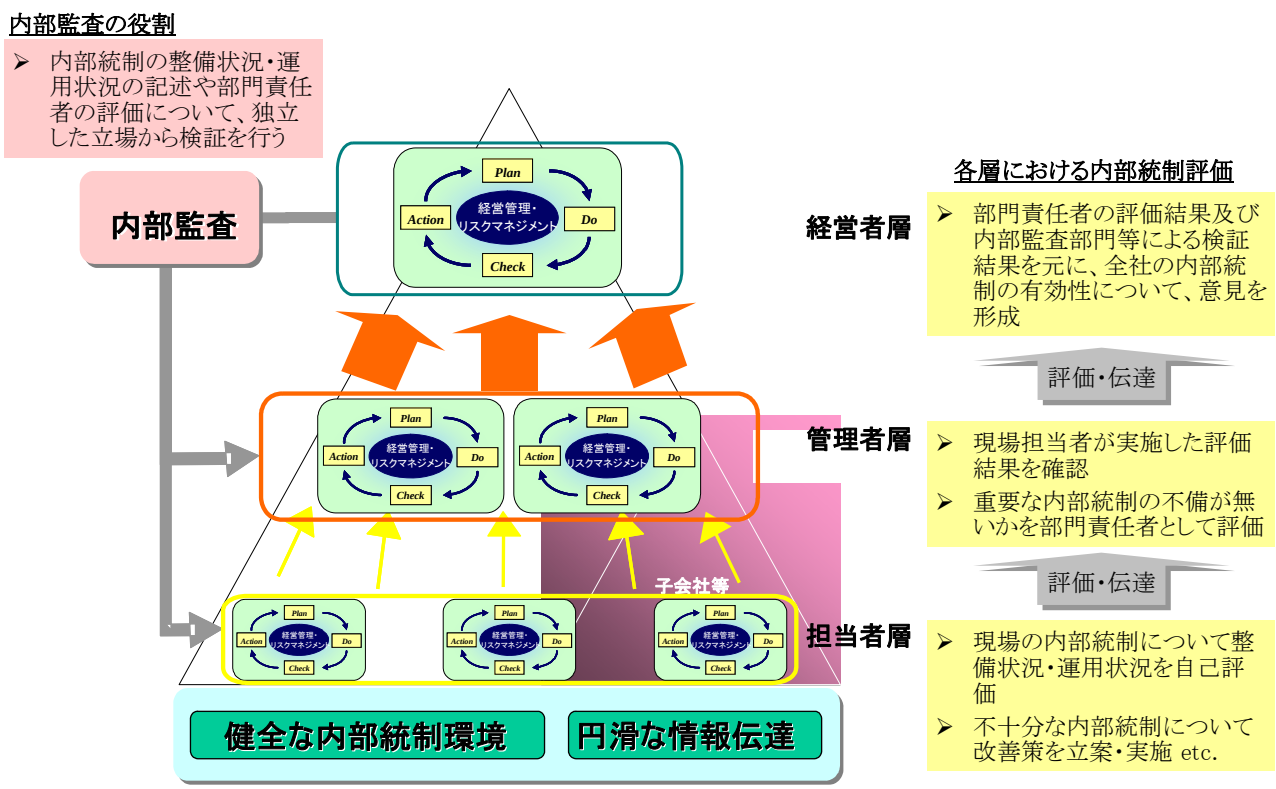
内部統制の評価は、業務プロセス(販売プロセス、購買プロセス等)ごとの評価を集計し、全社的な内部統制の評価として統合(総合的評価)する必要があります。

ある業務プロセスに問題が発見された場合、問題の重要性によっては、全社的には内部統制が機能していないという総合的評価となる可能性があります。一方で、発見された内部統制上の問題が、それ程重要でない場合や、他の内部統制がその問題をカバーしているような場合には総合的評価としては、全社的には内部統制が機能していると結論づけられることとなります。

総合的評価の実施のイメージ

総合的評価の一環として、経営者層(取締役等)、管理者層(営業部長、購買部長、経理部長等)、担当者層(課長、チームリーダー等)が実施する内部統制評価を図を用いて説明すると以下のようになります。各層における内部統制評価は独立して実施されるのではなく一連の流れとして実施されます。

また、内部統制の評価においては内部監査の果たす役割が重要です。独立した立場から各層における内部統制評価結果を検証することで、内部統制評価の客観性を高めることが可能となります。



＊経済産業省「リスク新時代の内部統制　リスクマネジメントと一体となって機能する内部統制の指針」リスク管理・内部統制に関する研究会 2003年6月より作成

内部統制の評価と内部監査

①自己評価と内部監査の組み合せ

プロセスオーナーによる内部統制の評価は、いわゆる自己評価であるため客観性は低くなってしまいますこの問題を解決する方法として、社内の独立した第三者である内部監査部門が内部統制の評価に関与することが考えられます。

実務的には、自己評価と内部監査の組み合わせを検討することになります。具体的には以下のケースが考えられます。

ケース1:内部統制の整備状況・運用状況についてプロセスオーナーが自己評価したうえ、内部監査部門がその評価結果を監査する。

ケース2:内部監査部門が整備状況及び運用状況の全てを評価し、プロセスオーナーによる自己評価は実施しない。

ケース3:内部統制の整備状況についてのみプロセスオーナーによる自己評価を実施し、内部監査部門が運用状況を評価する。

②内部監査の実施上の留意点(例示:ケース1を前提)

内部統制の評価結果に対する内部監査実施で留意すべき事項の例としては、以下のことが考えられます。

監査対象の決定:内部監査を実施するうえで、企業の行う全てのプロセスを監査するのは困難です。そのため、リスク評価に基づいて重要なプロセスを識別し、監査対象とするべきプロセスを決定する必要があります。

監査手続の確立:内部統制の評価に関する監査は、従来の内部監査で実施されていた監査手続とは異なります。特に運用状況の監査においては適切な監査結果を得るためのサンプリング数を決定すること等が求められます。

③内部監査に期待されるその他の機能

上記の他に内部統制のPDCAサイクルにおける内部監査部門の機能として以下の事項が考えられます。

内部統制のPDCAサイクルが適切に機能していることを経営者に対し保証する。

- 内部統制の是正・改善策をプロセスオーナーに提案する
- 内部統制の是正・改善策の妥当性を確認する
- 内部統制の是正・改善の進捗状況について確認する

内部統制の是正・改善

内部統制の評価の結果、問題が発見された事項については適切な是正・改善を行うことが必要となります。

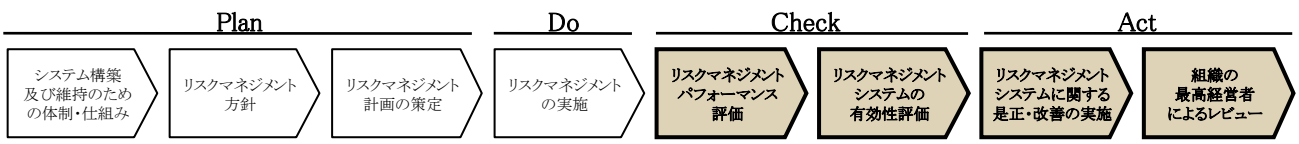
内部統制の是正・改善における留意事項

内部統制の評価の結果発見された問題点については、改善案を作成し実行する必要があります。その際、決定すべき事項と留意すべき事項は以下のとおりです。

決定すべき事項		留意すべき事項
是正・改善の優先順位の決定	→	重大な問題から順次対応していく
是正・改善策の決定	→	現状の業務を無視せず、実現可能な方策とする
是正・改善期限の決定	→	実現可能な期日とする
是正・改善責任者の決定	→	改善のための十分な権限をもった責任者とする
是正・改善状況のモニタリング	→	第三者による進捗状況の確認を行う

CHAPTER 6

リスクマネジメントシステムに関する評価、是正・改善



本章ではリスク対策を実施した後の評価と、その評価結果に基づいて実施される是正・改善について説明していきます。

いかに綿密で最適なリスクマネジメント計画を策定しても計画通りに実行されなければ、その計画は形骸化してしまう可能性があります。特にリスクマネジメントが業務の一環として浸透するまでは日常業務が優先され、リスクマネジメントの取組みが疎かになりがちです。リスクマネジメント計画に沿ってリスク対策を実行することを担保するためには事後の評価が有効となります。

また、評価で不適合が発見された場合、その性質によって速やかに追加の対策を講じたり、次のPDCAサイクルで是正・改善していく必要があります。

事業リスクマネジメントシステムを継続的に運用していくためには、評価・改善は不可欠

次のPDCAサイクルで是正・改善していくには組織の最高経営責任者がその必要性を認識する必要があります。そのために最高経営責任者はリスクマネジメントシステムの適切性と有効性が継続されていることを確認するためのレビューを行います。レビューのための情報はリスクマネジメントシステム監査の結果から入手します。

この章の内容

6.1 リスクマネジメントシステムに関する評価、是正・改善の全体像

6.1.1 評価、是正・改善の各フェーズの相関関係

6.2 リスクマネジメントの評価

6.2.1 リスクマネジメントパフォーマンス評価

緊急対策や復旧対策に関しても評価が必要

日常的な監視・測定の結果に基づき評価する

6.2.2 リスクマネジメントシステムの有効性評価

6.2.3 誰が評価をするか

リスクマネジメントシステム担当による自己評価のメリットは

6.2.4 評価指標をどう設定するか

JISQ2001における評価指標の説明

結果指標と行動指標

どのように評価指標が使われるのか

結果指標をどう設定するか

6.2.5 評価の実施

どのようにリスクマネジメントパフォーマンスを評価するか

どのようにリスクマネジメントシステムの有効性を評価するか

評価結果への対応

6.3 リスクマネジメントに関する是正・改善の実施

6.3.1 リスクマネジメントに関する是正・改善の継続的実施

いつリスクマネジメントシステムの不適合を是正・改善を実施するか

6.4 組織の最高経営責任者によるレビュー

6.4.1 組織の最高経営責任者によるレビュー

6.5 リスクマネジメントシステム監査

6.5.1 リスクマネジメントシステム監査の目的

6.5.2 リスクマネジメントシステム監査の実施

いつリスクマネジメントシステム監査を実施するか

誰がリスクマネジメントシステム監査を実施するか

内部監査とリスクマネジメント

リスクマネジメントの評価と監査の関係

リスクマネジメントシステム監査の実施例

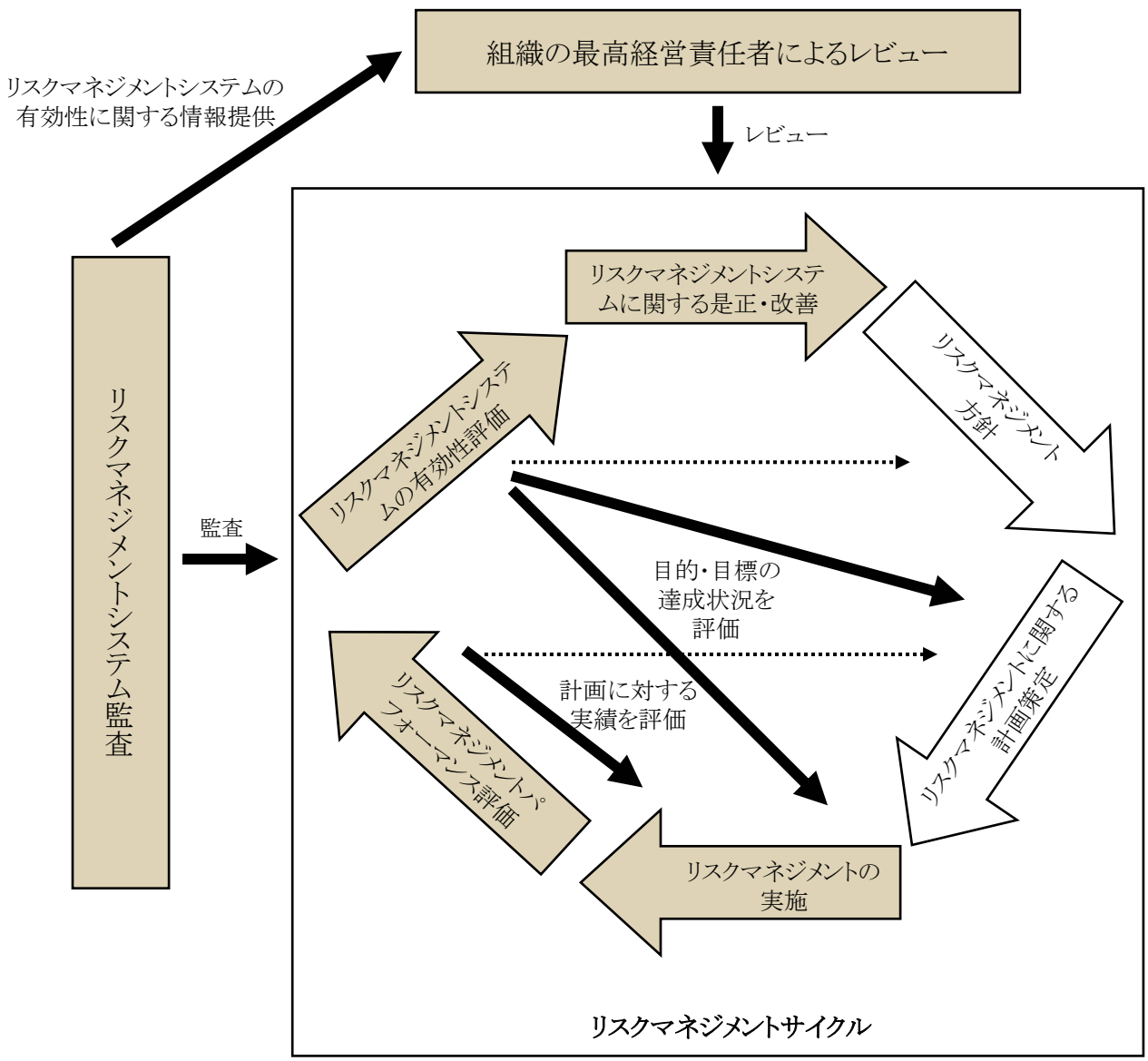
6.1 リスクマネジメントシステムに関する評価、是正・改善の全体像

ここではリスクマネジメントシステムに関する評価、是正・改善の全体像を解説していきます。

6.1.1 評価、是正・改善の各フェーズの相関関係

リスクマネジメントシステムに関する評価、是正・改善フェーズには、リスクマネジメントパフォーマンス評価、リスクマネジメントシステムの有効性評価、リスクマネジメントシステムに関する是正・改善の実施、組織の最高経営責任者によるレビュー、リスクマネジメントシステム監査があり、それぞれの関係をイメージ図で表わすと以下のようになります。

6.2以降で、各フェーズごとに事例を交えて詳細を説明していきます。



6.2 リスクマネジメントの評価

ここではリスクマネジメントの評価について説明していきます。
具体的には、
・ リスクマネジメントパフォーマンス評価とは何か。
・ リスクマネジメントシステムの有効性評価とは何か。
・ どのように評価を実施するか。
ということについて説明していきます。

6.2.1 リスクマネジメントパフォーマンス評価

リスクマネジメントパフォーマンスとは、リスクマネジメント基本目的及びリスクマネジメントの目標に基づいて、企業が行うリスクマネジメントに関する測定可能な結果です。リスクの方針、リスクの特定結果、リスク算定の結果、対策の決定結果などのように具体的に形で示されます。リスクマネジメント計画で策定された具体的な対策がどの程度実施されたかを評価することが、リスクマネジメントパフォーマンス評価です。

例えば、工場で労働災害が発生するリスクに対し、事故が多発する場所10ヶ所にミラーを取り付けるというリスク対策を計画したが、実際に5箇所しか取り付けなかった場合には、パフォーマンスは未達成と評価されます。

リスクマネジメントパフォーマンス評価の目的は、不適合是正のトリガー機能を果たすことであり、パフォーマンス評価の結果に基づいて、次のステップの是正・改善が実施されます。

目的	リスクマネジメント計画で策定された対策がどの程度実施されたかを評価することにより、不適合是正のトリガー機能を果たすこと
対象	・活動計画に対する実績（計画の実施程度） ・リスク対策を実施したあとのリスク算定 ＊ ただし、対策実施後のリスク算定は困難な場合や不要な場合もある
実施時期	計画時に評価時期をあらかじめ定めておき、その時期に実施する。対象となるリスクの発生頻度、影響度および変化の度合いを考慮して時期を設定する

『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年より作成

緊急時対策や復旧対策に関しても評価が必要

リスクマネジメントパフォーマンス評価は、事前対策に関してだけでなく緊急時対策や復旧対策に関しても適宜行うことが必要です。
緊急時対策に関するリスクマネジメントパフォーマンス評価は緊急時対策の終了後に行うことが必要です。事態の拡大の可能性についても評価すべきです。
復旧対策に関するリスクマネジメントパフォーマンス評価は復旧直後に行う必要があります。

日常的な監視・測定の結果に基づき評価する

リスクマネジメント活動の結果を具体的に評価する前に、リスクマネジメントシステム担当者はリスクマネジメント活動プロセスを確認する必要があります。リスクマネジメント計画の策定やリスク対策の実施に関与している担当者が予め企業として定めた手順で実施されていることを確認します。手順を省略していないか、一部の担当者だけが実施しているにとどまっていないかなどの確認を行います。このような監視やパフォーマンス指標の測定は、パフォーマンス評価の直前だけでなく、日常業務の中で都度行われるのが望ましいとされています。例えば障害発生件数等、日頃からデータを蓄積しておく必要のある指標もあります。

この監視・測定の結果に基づいてリスクマネジメントパフォーマンス評価を行います。そのため、監視・測定の結果は記録され適切に保存される必要があります。

6.2.2 リスクマネジメントシステムの有効性評価

リスクマネジメントシステムの有効性評価の目的は、リスクマネジメント基本目的やリスクマネジメントの目標の達成度合いを管理することです。

リスクマネジメントパフォーマンス評価が100点であっても、当初計画していたリスクマネジメントの目標が達成されないこともあります。このような場合にはリスクマネジメントサイクルのどこかに問題があるはずです。この段階でその問題点を分析しActで次の対策につなげていきます。

目的	リスクマネジメント基本目的やリスクマネジメントの目標の達成度合いを管理すること
対象	リスクマネジメントシステムの個別機能と全体機能を対象とする ・個別機能の有効性評価：個別に設定したリスクマネジメントの目標の達成度合を評価すること ・全体機能の有効性評価：全社で設定したリスクマネジメント基本目的の達成度合を評価すること
実施時期	・定期的なリスクマネジメントシステム監査結果を受けて実施する組織の最高経営責任者によるレビューのとき ・リスクマネジメントシステムに疑義が生じたとき ・自らの企業や他企業でリスクが発現化し、重大な被害を受けたとき

『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年より作成

6.2.3 誰が評価をするか

リスクマネジメントパフォーマンス評価、リスクマネジメントシステムの有効性評価はリスクマネジメントシステム担当者によって実施されます。すなわち、リスクに対する当事者により評価が行なわれます。しかし、時には以下の例のように専門家や第三者と協力して評価を行なうこともあります。

リスクマネジメントシステム担当による自己評価

- 一般的には、各部門のリスクマネジメントシステム担当が自己評価をします。またリスクマネジメントシステムの有効性評価で全体機能（全社のリスクマネジメントシステム）を評価する場合は、全社のリスクマネジメントを統括するリスクマネジャーやリスク管理部署が自己評価を実施します。

企業内の専門家の協力を得ての評価

- 技術的なリスクに関わる評価など、リスクマネジメントシステム担当者のみで自己評価することが困難な場合や企業内の専門家の協力を得たほうが評価が有効かつ効率的である場合には、企業内のマネジメントシステムもしくは個々のリスクに関する知識をもつ専門家の協力を得て評価が実施されます。

第三者による評価

- 企業内部でリスクマネジメントシステムに関する評価を行なうことが困難な場合には、コンサルタント会社等の外部の第三者へ外注し評価することも考えられます。

リスクマネジメントシステム担当による自己評価のメリットは

リスクに対する実施当事者が自分自身の評価を行う自己評価には多くのメリットがあります。具体的には以下のようなものがあげられます。

◆ 自己評価することのメリット

自らが事業リスクマネジメントに取り組んでいるという意識が強くなり、リスクマネジメント計画の形骸化やリスク対策の未実施を防止できる

自己評価で自ら課題を発見することにより、次の是正改善にスムーズにつながる

リスクの実態を現状把握することも自己評価と同時に実施できるため環境の変化にも柔軟に対応できる

リスクに対する実施当事者以外の者による評価よりも、より詳細で具体的な状況が把握できる

具体的に自己評価はどのように実施されるのでしょうか。各社の事例を紹介します。

◆ 自己評価の実施方法例

個々のリスク担当部門部署内のリスクマネジメント作業担当者が自ら評価チェックリストに基づいて評価を実施する

- 評価チェックリストではリスクごとに項目を設定して評価していきます。チェック項目には、リスクマネジメント目標の達成の有無、前回の自己評価での不備事項の改善状況、リスクに関する具体対策の実施状況の把握等があります。

リスクマネジメント作業担当者のチェック後にリスクマネジメントシステム担当が二次評価を実施する

- リスクマネジメント作業担当者の評価結果を基礎として、リスクマネジメントシステム担当者により二次評価が実施されます。二段階で評価することでより詳細な評価が可能となり、同一リスクマネジメント部門部署内での作業担当者間の実施結果のばらつきも把握できます。

6.2.4　評価指標をどう設定するか

リスクマネジメントの評価を実施するにあたり、評価指標の設定をどうしたらよいのかという声が多く聞かれます。評価指標として考慮すべき要件や、実際の評価指標の例について以下に説明していきます。

JISQ2001における評価指標の説明

JISQ2001では、リスクマネジメントパフォーマンス評価およびリスクマネジメントシステムの有効性評価における評価指標について、以下のように説明しています。

リスクマネジメントパフォーマンス評価指標で重視される性質

「- 客観性があること
- 再現性があること
- 検証可能性があること
- 経済上、事実上の実行可能性があること*」

リスクマネジメントパフォーマンス評価指標で使用される代表的な指標

「- リスクマネジメントの実施状況（リスクマネジメントに関する計画策定及びリスク対策の実施）に関する進捗度
- 教育及び訓練の進捗度
- 関連する法規制及び規格
- リスクコミュニケーションの実行度*」

リスクマネジメントシステムの有効性評価の評価指標

「リスクマネジメントシステムの有効性評価の指標として、リスクマネジメント基本目的及びリスクマネジメントの目標の達成度をとる*。」

*『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年より一部修正

結果指標と行動指標

評価指標には結果指標と行動指標という2つの考え方があります。それぞれの具体例をあげて説明します。

結果指標

結果指標とは、活動の結果実現された状態を金額、パーセンテージ、件数等数値で示して指標とするものです。リスクマネジメントシステムの有効性評価でリスクマネジメントの目標と結果を比較するときに用いられることが多いようです。

労働災害の件数削減目標を何％達成できたか

行動指標

行動指標とは、目標を達成するために実施する行動そのものを指標とするものです。
この指標はリスクマネジメントパフォーマンス評価で具体的な対策の計画と実際の実施状況を比較するときに用いられることが多いようです。

年度中に教育訓練の実施ができたか

どのように評価指標が使われるのか

リスクマネジメントパフォーマンス評価、リスクマネジメントシステムの有効性評価と評価指標との関係を事例で説明します。

リスクの内容	リスク戦略	リスクマネジメントの目標・・・①	具体的リスク対策計画・・・②	リスクマネジメントの目標結果・・・③	リスクマネジメントパフォーマンス・・・④
工場での労働災害リスク	リスク低減	工場での年間労働災害発生件数を現在の20件から10件に減少させる	・工場内で事故が多発する場所10ヶ所にミラーを取り付ける	年間労働災害件数は15件となった	工場内で5ヶ所にミラーを取り付けた
コンプライアンスリスク	リスク予防	コンプライアンスの欠如による不祥事事件の発生を皆無とする	・従業員へコンプライアンス研修を年2回実施 ・コンプライアンス遵守の冊子を従業員全員へ配布	コンプライアンスの欠如による不祥事事件は発生しなかった	・コンプライアンス研修を年2回実施した。 ・コンプライアンス遵守の冊子を従業員全員へ配布した

結果指標　行動指標

有効性評価指標　パフォーマンス評価指標

事例　パフォーマンス評価指標（行動指標を用いた例）

リスクマネジメントパフォーマンス評価は、対策の実施という行動を評価指標として具体的リスク対策計画②とリスクマネジメントパフォーマンス④との比較によって行われます。行動指標を評価指標として用いる場合でも、実施結果との比較を容易にするため測定可能な単位を用います。この例ではミラーの取り付け場所数、コンプライアンス研修回数、コンプライアンス遵守の冊子の配布従業員数が測定可能な単位として採用されています。

事例　有効性評価指標（結果指標を用いた例）

リスクマネジメントシステムの有効性評価は、年間労働災害発見件数、コンプライアンス欠如による不祥事事件数という結果を評価指標としてリスクマネジメントの目標①とリスクマネジメントの目標結果③との比較によって行われています。この例では結果指標を有効性評価の指標として用いています。

結果指標をどう設定するか

行動指標は、評価対象期間に何を実施したかが指標となるため、比較的設定しやすい指標です。一方結果指標については、対策を実施した結果の測定が難しいケースが多く、必ずしも有効な指標が設定できるとは限りません。しかしリスクマネジメントシステムの有効性評価には結果指標の方が適しているため、できる限り結果指標を設定する努力が必要です。

リスク対策実施後の残余リスクについて、その影響度や発生頻度を的確に測定できれば、その値を結果指標にすることができます。しかし例えば以下に示すようにリスクの性質によってはそれが難しい場合があります。

－　発生頻度が元々小さく、予防対策が有効かどうか発生件数から判断できないもの。（情報漏洩等）
－　人の意識に関るものなど、変化が目に見えにくいもの。（従業員のモチベーション低下等）

このような場合の評価指標設定の考え方としては、①リスク対策の整備・運用レベルが向上すれば結果的に残余リスクが減少すると考え、リスク対策のレベルを何らかの方法で測定する　②間接的な方法で残余リスクの大きさを評価または推定する、等が考えられます。

上記の考え方で設定した評価指標の例を示します。

参考　評価指標の例

評価指標の種類	説明	評価指標の例	対応するリスク
内部統制評価結果	特定のリスクの発現を予防するための内部統制について、ベストプラクティスをチェックリスト化し、各部署で自己評価（または第三者評価）する。 （内部統制評価については「5.3内部統制」参照）	情報セキュリティチェックリストによる評価結果	情報漏洩、コンプライアンス違反等、内部統制によって予防するタイプのリスク全般
		コンプライアンスチェックリストによる評価結果	
リスクマネジメントの組織能力評価結果	特定のリスクに対応するためのリスクマネジメントのPDCAサイクルが、組織の中で適切に構築運営されているかを評価する。	リスクマネジメント能力レベル評価 （「4.1.4リスクの評価に関する留意事項」参照）	リスク全般
		リスクマネジメント実施状況の自己評価 （「6.5.2リスクマネジメント監査の実施」に自己評価チェックシートの事例を掲載）	
定期的な調査結果	定期的に実施される各種調査の中に、評価指標として直接・間接に利用できるものがある。	顧客アンケート結果	顧客離れ
		従業員満足度調査結果	従業員のモチベーション低下
リスク先行指標	発生頻度が小さいリスクについて、特定の事象が増えるとそのリスクの発生可能性が増すようなものがある場合、それを代替的に指標とする。	特定のミスや不具合の発生件数、返品の内容別内訳	製品リコール
		顧客のクレーム件数やその内容別内訳	顧客離れ、ブランド価値低下、レピュテーションリスク

6.2.5　評価の実施

以下では実際にどのようにして評価が実施されるかを見ていきます。

どのようにリスクマネジメントパフォーマンスを評価するか

この会社ではあるリスクへの具体的な対策に関するパフォーマンス評価をリスク対策シートで行なっています。

計画策定時に記入	リスク管理担当部署	A工場	実施責任者	X山　X夫
	リスクの内容	工場で労働災害が発生するリスク	承認欄	2004/5/12 CRO　X野　X助　㊞
	リスクマネジメントの目標	・A工場での年間労働災害件数を現在の20件から10件に減少させる。		
	リスク対策の具体的内容	・工場内で事故が多発する場所10ヶ所にミラーを取り付ける ・労働災害を防止するための教育訓練を実施する。		
	リスク対策の日程	上期中にすべてミラーを取り付ける 7月に1回、12月に1回労働災害リスク予防の教育研修を開催する。		
	評価指標	ミラーの取り付けヶ所数 教育訓練の実施		
評価時に記入	リスクマネジメントパフォーマンス評価	評価時期	2004/2/20	
		評価担当者	工場長A	
		評価結果	ミラーは5ヶ所にしか取り付けられなかったため、パフォーマンスは×（未達成）です。 8月に労働災害リスク予防の教育研修を開催した、パフォーマンスは○（達成）です。	
	次年度への留意事項	ミラーの取り付けについてのパフォーマンスは×（未達成）のため、「ミラーを取り付ける」という具体的対策の実施が不十分だったことがわかります。 パフォーマンス評価の結果から、対策の実施を妨げる何らかの要因があった可能性があり、その要因を是正、改善することとなります。 このようにパフォーマンス評価が是正、改善へのトリガー機能を果たすのです。		

この部分は「4.2.4　リスクマネジメントプログラムの策定」にて説明しています。

リスクマネジメントパフォーマンス評価として記入する

どのようにリスクマネジメントシステムの有効性を評価するか

下表は前ページ同じ労働災害リスクへの対応計画です。ただし対策計画を1つに絞っています。

リスクの内容	リスク戦略	リスクマネジメントの目標	具体的リスク対策計画
工場での労働災害リスク	リスク低減	工場での年間労働災害発生件数を現在の20件から10件に減少させる	・工場内で事故が多発する場所10ヶ所にミラーを取り付ける

個々のリスクにおけるリスクマネジメントの場合、リスクマネジメントの目標の達成度が有効性の評価指標になります。この例ではリスクマネジメントの目標、つまり、工場での年間労働災害の発生件数を10件にすることに対して、リスクマネジメントの実施結果、つまり、実際の件数がどうなったのかをケースごとに示し、各ケースの有効性を評価します。

ケース	実施結果(年間労働災害発生件数)	評価結果
1	年間労働災害件数5件	目標以上の結果達成のため有効
2	年間労働災害件数10件	目標通りの結果達成のため有効
3	**年間労働災害件数15件**	**件数は減少したが目標に実施結果が達していないため有効性に問題がある**

ケース1と2ではリスクマネジメントの目標以上の結果が得られたため、リスクマネジメントシステムは有効と評価されました。しかし、ケース3ではリスクマネジメントの目標に実施結果が達していないので、リスクマネジメントシステムは有効性に問題があることになります。ケース3については、具体的なリスク対策計画、つまり、ミラーの取付け計画に対してリスク対策の結果、つまり、ミラーの取付け実績がどうであったかを更にケースごとに示し、ケースごとに評価を実施します。

ケース	具体的リスク対策の結果	今後の対応
A	ミラー取り付け場所は計画未満の8ヶ所であった。	リスクマネジメントパフォーマンス評価が80点のケース。計画通りに具体的リスク対策を実施しなかったため目標は達成されませんでした。今後は予算や責任体制などについて見直す必要があります。
B	ミラー取り付け場所は計画通り10ヶ所であった。	リスクマネジメントパフォーマンス評価が100点、120点のケース。計画通りに具体的リスク対策を実施しても目標は達成されませんでした。具体的リスク対策の計画がリスク目標に対して力不足であったり、リスク評価が間違っていた等の可能性があります。リスクマネジメントサイクルのどこかで不備な点があり、次のステップである是正を実施していく必要があります。
C	ミラー取り付け場所は計画以上の12ヶ所であった。	

評価結果への対応

リスクマネジメントシステムの有効性評価結果に対し、企業は下記のような対応をとるべきであるとされています。

「－ 結果を記録し、文書管理規程に従って適切に管理する
－ 結果をリスクマネジメントシステム担当責任者に報告する
－ 有効性の向上が必要と判断される場合には、リスクマネジメントの計画、リスク対策並びにリスクマネジメント維持のための体制及び仕組みを見直して、是正及び改善を要する領域を確定する*」

「是正、改善の実施後、リスクマネジメントシステム担当責任者が、その有効性に関する検証を必要と判断したものについては、関係各部門部署の協力を得てその評価を行います。*」

*『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年より一部修正

6.3 リスクマネジメントシステムに関する是正・改善の実施

ここでは、リスクマネジメントに関する是正・改善の実施について解説していきます。
具体的には、「いつリスクマネジメントシステムの不適合を是正・改善するのか」と
いうことについて説明していきます。

6.3.1 リスクマネジメントに関する是正・改善の継続的実施

企業はリスクマネジメントパフォーマンス評価リスクマネジメントシステムの有効性評価の結果に基づいて、必要に応じてリスクマネジメントの各要素を是正及び改善していきます。

リスクマネジメントシステムに不適合があれば、今行っているサイクルの中で速やかに是正・改善を実施するか、もしくは次回のサイクルから是正・改善を実施するかを総合的に判断する必要があります。
例えば、リスクそのものが大きくなっている場合やリスク対策が不十分でリスクの発現が切迫している場合には今行っているサイクルの中で速やかに他のリスク対策を実施するよう、補正予算を組む等の対応が必要となってきます。

リスクマネジメントサイクルは一回限りでなく、今後も継続して繰り返されるものです。今回のリスクマネジメントサイクルで不具合や問題点があれば、今回もしくは次回のサイクルで是正・改善していくというようにサイクルを繰り返すことによって、リスクマネジメントの有効性はだんだんと高くなります。

リスクマネジメントに関する是正・改善を継続的に実施することは、「6.3リスクマネジメントシステムの有効性評価」で説明したリスクマネジメント担当部門による自己評価及び不適合な点がある場合における是正・改善にあたります。

リスクマネジメントの評価で不適合が生じていることが発見された場合に行なうべきこととして以下の手続きが考えられます。

- リスクマネジメントシステムの不適合の原因を調査・究明
- リスクマネジメントシステムの不適合の原因に対応した是正・改善案の提示と実施
- 潜在するリスクを考慮した再発防止策の実施
- 再発防止策の有効性の確認
- 手順書、規定類及び記録書式の変更

いつリスクマネジメントシステムの不適合を是正・改善するか

リスクマネジメントシステムの是正時期は重要となります。場合によっては速やかに是正・改善を実施しなければならないことがあるからです。

『JISQ2001 リスクマネジメントシステム構築のための指針』では、リスクマネジメントシステムの是正・改善の実施時期として下記を挙げています。

継続的に是正・改善を実施する

- リスクマネジメントパフォーマンス及び運用管理の状況の継続的な監視、測定及び評価結果に基づいて実施する。これには日常的な評価を実施して不備があれば改善することが含まれます。

リスクマネジメントシステム監査時

- 定期、不定期に実施されるリスクマネジメントシステム監査で重大な問題点等が指摘された場合などに是正・改善を実施します。

緊急事態経験後

- リスクが発現化したとき、及びその直後に行われる緊急時対策の監視とリスクマネジメントシステムパフォーマンス評価の結果に基づいて是正・改善を実施します。
- リスクが発現化したときを想定した訓練及びシュミレーション評価の結果に基づいて是正・改善を実施する場合もあります。

リスクに関する情報の監視結果に基づく要請時

- リスク対策を講じないと決定したリスクは継続的に監視する必要があります。必要な場合には、そのリスクに関する情報の監視結果に基づいて、リスクマネジメント活動とリスクマネジメントシステムを点検し、見直します。

6.4 組織の最高経営責任者によるレビュー

ここではリスクマネジメントサイクルの最終ステップの組織の最高経営責任者によるレビューについて解説していきます。

6.4.1 組織の最高経営責任者によるレビュー

組織の最高経営責任者は、リスクマネジメントシステム全体について最終的な責任を負います。最高経営責任者はリスクマネジメントサイクルのスタート時点において、リスクマネジメントシステム担当者を任命し、リスクマネジメント方針を表明します。最終時点ではリスクマネジメンシステム全体をレビューし1サイクルを終了させます。そして、レビューの結果を次のリスクマネジメントサイクルでリスクマネジメント方針に反映させることで、サイクルが組織の最高経営責任者の責任でスタートするのです。このように組織の最高経営責任者のレビューによってリスクマネジメントシステムの継続的改善が、異なるサイクルを通じて実現されるのです。

組織の最高経営責任者がリスクマネジメントシステムサイクルのすべての段階においてレビューという形で関与し、経営の意思を確実に反映することは、最高経営責任者の責任として極めて重要となります。

組織の最高経営責任者によるレビューの目的は、リスクマネジメントシステムが継続して適切であり、有効性であることを確認し、必要があればリスクマネジメントシステムとその要素の改善を指示することです。レビューの実施間隔（通常は1年ですが、半期や四半期でもよい）は最高経営責任者が決めるべき事項であり、必ずしも定期的である必要はありません。

「組織の最高経営責任者はすべてのリスクマネジメント活動にわたり、全体との関連性を勘案しつつ包括的なレビューを実施します。

- リスクマネジメント方針
- リスクマネジメントに関する計画策定
- リスクマネジメントの実施
- リスクマネジメントパフォーマンス評価及びリスクマネジメントシステムの有効性評価
- リスクマネジメントシステムに関する是正・改善の実施
- リスクマネジメントシステム構築のための体制・仕組み*」

*『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年 より一部修正

レビューした結果は、指示書にまとめてリスクマネジメント担当責任者に伝えられ、是正・改善に反映されます。

6.5 リスクマネジメントシステム監査

ここでは、リスクマネジメントシステム担当者から独立した第三者によるリスクマネジメント監査について解説していきます。
具体的には、
・ いつリスクマネジメントシステムを監査するか
・ 誰がリスクマネジメントシステムを監査するか
・ どのようにリスクマネジメントシステムを監査するか
ということについて説明していきます。

6.5.1 リスクマネジメントシステム監査の目的

リスクマネジメントシステムでは基本的にリスクマネジメントシステム担当者が、リスクマネジメントのパフォーマンス評価、リスクマネジメントシステムの有効性評価を行い、日常的な監視・測定、評価、是正・改善活動を行います。ただしそれだけではリスクマネジメント活動そのものが形骸化する恐れがあります。そのため、リスクマネジメントシステム担当から独立した第三者による監査が必要となります。

リスクマネジメントシステム監査の主な目的は下記の通りです。

組織の最高経営責任者によるレビューの際の情報を提供するため

- 一般的にはこれが主目的です。組織の最高経営責任者はリスクマネジメントに関する課題のすべてを把握しているわけではありません。そのため、リスクマネジメント監査の結果を最高経営責任者へ伝達し、レビューの際の情報を提供するのです。

企業のリスクマネジメントシステムが、適切に構築され、実施され、維持されているか否かの判断をするため

- 具体的には、
  - リスクマネジメント計画の内容に適合しているのか
  - 規定・手続書等に従って実施され、維持されているのか
  - 法的およびその他の要求事項を遵守しているのか

  について判断します。

リスクマネジメントシステムの継続的な是正・改善を実施するため

- リスクマネジメントシステム監査結果に基づいてリスクマネジメントシステムの是正・改善を実施します。

6.5.2　リスクマネジメントシステム監査の実施

リスクマネジメントシステム監査を効果的・効率的に実施するためには、リスクマネジメントシステム監査の年度計画、実施計画、監査のチェックリスト等の規定・手続書等を準備する必要があります。規定等は、通常の業務監査の手順書と統合される場合や独自に定める場合があります。

リスクマネジメントシステム監査に先立って検討しておかなければならない事項は下記の通りです。

監査する範囲の決定（被監査部門の決定など）
頻度と方法（準拠性監査、部門別監査、テーマ別監査など）の決定
監査の優先順位
監査の実施通知
被監査部門の準備
監査結果の評価基準
監査結果の報告
監査人の能力・資格の設定
監査結果に関する関係者の協議

いつリスクマネジメントシステム監査を実施するか

リスクマネジメントシステム監査実施者はどのようなときに監査を実施しているのでしょうか。

内部監査部門の通常業務と合わせて実施した

- リスクマネジメントシステム監査を実施するには、監査に必要な書類の提出やヒアリングが必要となります。リスクマネジメントシステム担当者の負担を軽減するために中長期経営計画の進捗状況の確認、予算投資案件の状況、予算と実際との差異内容の説明等通常の監査業務と同時にリスクマネジメントシステム監査のヒアリングが実施されています。

組織の最高経営責任者の指示により実施した

- リスクマネジメントシステム監査の主目的は組織の最高経営責任者によるレビューの際に必要な情報を提供するためです。そのため組織の最高経営責任者によるレビューをする前にリスクマネジメント監査が実施されます。多くの会社では年に一回実施されているようです。

誰がリスクマネジメントシステム監査を実施するか

通常、リスクマネジメントシステム監査は内部監査部門で実施されます。企業によっては内部監査部門がない場合はもちろんですが、内部監査部門がある場合でも内部監査部門以外で監査している事例がありました。

いずれにしても、組織の最高経営責任者がレビューする際の情報を提供する人が、リスクマネジメントシステム監査の主体と言えます。

内部監査部門で実施

- 内部監査部門は他の部門部署から独立した最高経営責任者直系の部門であるため、独立性という観点から最も適任です。しかし、内部監査部門がない企業や、内部監査部門があっても内部監査部門のリスクマネジメントシステム監査に必要な経営資源が不足しリスクマネジメントシステム監査が実施できない企業もあります。

CRO主導で組織した監査チームで実施

- CROはリスクマネジメントシステム担当責任者です。リスクに精通したCROによってリスクマネジメントシステム監査を実施した方が効果的であるとした企業で実施されています。厳密に言えば、CROもリスクマネジメントシステムの関係者であるため、監査組織は最高経営責任者直轄が望ましいですが、運用面の実を取った形です。

各リスクを統括している部署相互でチェック

- 各リスクを統括して部署が自己に責任のあるリスクについて評価を行うのは当然です。しかし、他のリスクを統括している部署相互でチェックしている事例がありました。一部署が監査するのに比べ、一度に多くの部署を監査できるメリットがあります。ただし監査担当者は日常業務を抱えながら監査するため、作業負荷の大きなものや専門知識を必要とするものは実施できない可能性があります。

企業外部者が実施

- 例えば、情報リスクに対する内部監査を実施するには情報セキュリティや情報システムについての専門的な能力が要求されます。企業内で能力のある人員を確保できない場合は企業外部者へ内部監査業務を委託します。

内部監査とリスクマネジメント

内部監査とリスクマネジメントの関係はどうなっているのでしょうか。IIA（The Institute of Internal Auditors)が発表している「内部監査の専門職的実施の国際基準」では、内部監査の業務内容として以下を挙げています。

「内部監査部門は、組織体のリスク・マネジメント・システムの有効性を監視し、評価しなければならない＊。」
＊『内部監査の専門職的実施の国際基準』IIA より

このように、リスクマネジメントシステムの有効性は内部監査の主要な監査対象であると言えます。

一方、内部監査は客観的な立場から公正な監査意見を提出することが求められているため、リスクマネジメントの実施そのものに直接携わることは望ましくありません。

これらの原則を踏まえ、IIAの発表している「ERMにおける内部監査の役割（The Role of Internal Auditing in Enterprise-wide Risk Management)」では、全社的なリスクマネジメント体制の中で内部監査の果たす主な役割と、担当すべきでない役割を以下のように示しています。

ERMにおける内部監査の主な役割

「－リスクマネジメントプロセスが有効に機能していることを保証する
－リスクが正しく評価されていることを保証する
－リスクマネジメントプロセスを評価する
－重要リスクに関する報告を評価する
－重要リスクの管理状況をレビューする*」

＊″The Role of Internal Auditing in Enterprise-wide Risk Management″ IIA 2004年より一部修正

内部監査が担当すべきでないこと

「－リスク許容限度を決める
－リスクマネジメントプロセスを自ら構築する
－経営者に代わってリスク評価をする
－リスク対策を決定する
－経営者に代わってリスク対策を導入する
－リスクマネジメントに関する説明責任を果たす*」

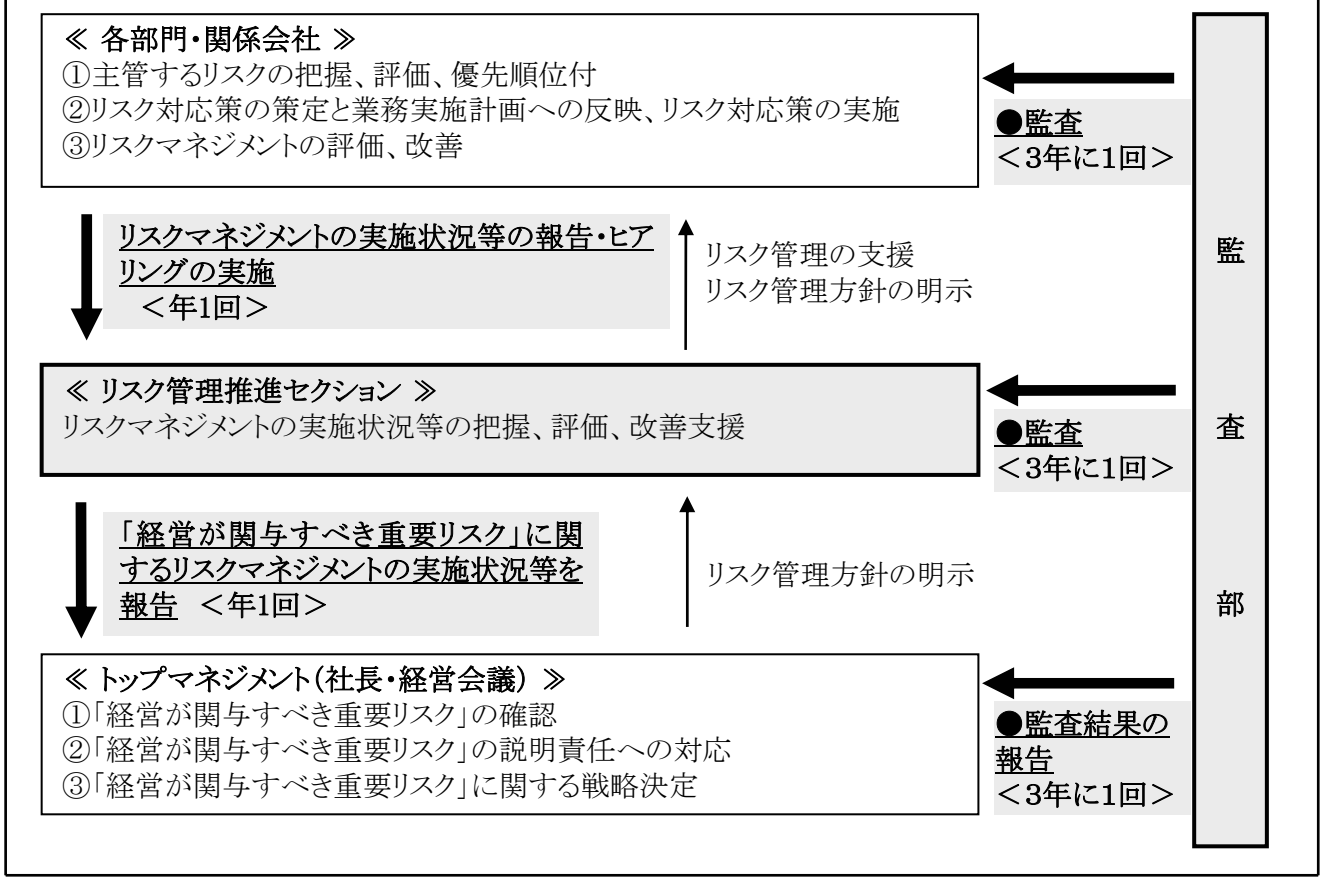
＊″The Role of Internal Auditing in Enterprise-wide Risk Management″ IIA 2004年より一部修正

リスクマネジメントの評価と監査の関係

リスクマネジメントの評価と監査の最も大きな違いは、その実施主体の違いです。評価はリスクマネジメントを実施している当事者が自ら是正・改善のために実施するものであるのに対し、監査は第三者が客観的に検証し、最高経営責任者に対し情報を提供するものです。監査の結果も監査を受けたリスクマネジメントの当事者にフィードバックされ、是正・改善に役立てられます。

以下で実際の組織における役割分担の例を紹介します

事例　あるエネルギー企業におけるリスクマネジメント管理体制の全体像



上記事例企業おけるリスク管理推進セクションと監査部の役割について説明します。

リスク管理推進セクションによるリスクマネジメントの推進と評価

- 各部門部署、関連会社のリスクマネジメントシステム担当者はリスクを見直し、対応策の実施状況を評価して、リスク管理推進セクションへ報告します。
- リスク管理推進セクションでは報告の内容をレビューし、リスクの状況や対策の実施状況をヒアリングにより把握します。報告内容に問題点がある場合には改善策の提案をします。このヒアリングは年に1回実施します。
- リスク管理推進セクションではこれらの評価結果を取りまとめた上で、特に重要な「経営が関与すべき重要リスク」については経営トップへ年1回報告します。

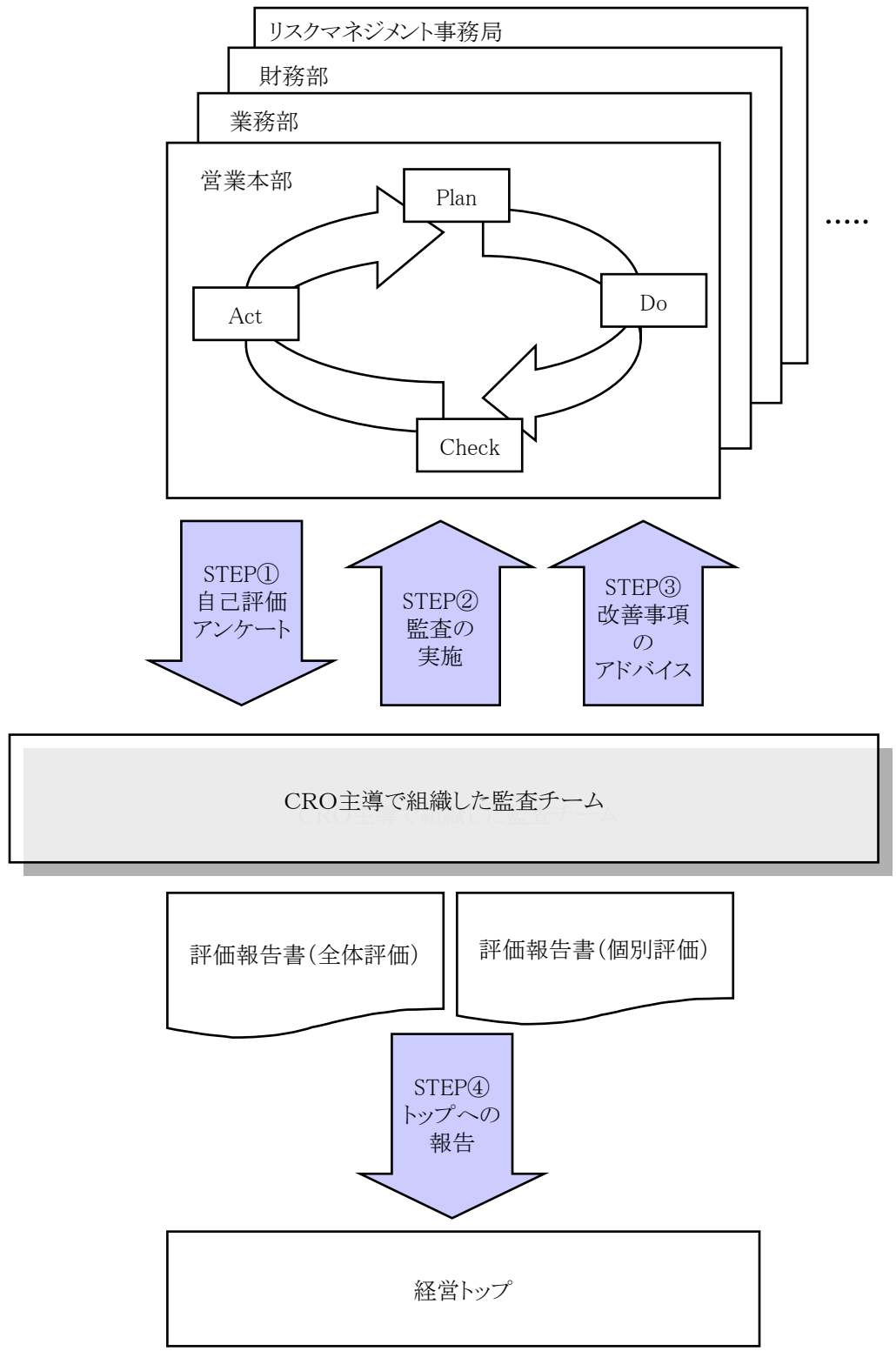
内部監査部門による監査

- 内部監査部門では3年に1度のローテーションで各部門部署、関連会社のリスクマネジメントの実施状況を監査します。当年度に監査の対象となった部門部署・関連会社はリスク管理推進セクションによる例年のヒアリングも同時に受けることとなります。
- 内部監査部門はリスク管理推進セクションが実施した評価レビュー状況や、「経営が関与すべき重要リスク」の選定プロセスについても監査します。
- 内部監査部門は監査対象部門の監査結果を経営トップに報告します。

リスクマネジメントシステム監査の実施例

ある企業で実施されているリスクマネジメントシステム監査を以下で順に説明していきます。ここでは内部監査部門以外による監査の例を紹介していますが、内部監査部門で実施する場合でも同様の手順で実施している例が見られます。

事例　消費財製造業リスクマネジメントシステム監査



前ページの図について、具体的な内容を以下に説明します。

各部門から選任された監査チーム

- 年に1回、監査の時期に各部門から監査担当者を選任し、10数名の監査チームを編成します。この企業には内部監査部門がありますが、業務量等の観点から、このような監査チームを別途編成することにしています。また監査手続等のノウハウを得るために外部のコンサルタントを監査チームに入れ、OJTでのノウハウ習得を目指しています。
- 監査対象部署ごとに、監査担当者2名とコンサルタントでチームを組み、計画立案から報告のまとめまでを実施しています。
- 監査担当者は兼任であるため、アンケートの配布・回収・集計等の事務作業は全社リスクマネジメントの統括部署であるリスクマネジメント事務局が担当しています。リスクマネジメント事務局は監査を受ける立場でもあるため、厳密には監査実施側とは一線を画すことになりますが、限られた資源で円滑に監査を進めるために敢えてこのような分担にしています。

自己評価と組み合わせた監査手続

- STEP① リスクマネジメントサイクルの実施状況をアンケートで自己評価
  各リスクマネジメント担当者がリスクマネジメントサイクルが適切に運用されているか否かをアンケートで確認します。アンケート項目はリスクマネジメントサイクル全般（PDCA）にわたります。アンケートの具体的な内容は次ページで紹介します。
- STEP② 監査の実施
  各リスクマネジメント担当者が記入したアンケートを回収し、監査チームがアンケート結果をレビューします。レビュー結果とこの部門のリスク評価結果、前年度の監査結果等から初期所見を作成し、インタビューの項目や事前に準備して欲しい資料等をリストアップして監査対象部署に渡します。また全社のリスクマネジメント推進体制や活動状況も監査の対象となるため、全社統括組織であるリスクマネジメント事務局も監査対象部署となります。
  インタビューでは監査チームは監査対象部署のリスクマネジメント担当者に対して質問を行い、文書等で裏づけを取る必要のある事項を特定します。特定された事項は関連する資料等の文書により裏づけを行います。
- STEP③ 改善事項のアドバイス
  リスクマネジメントシステム監査は客観的な保証のみならずコンサルティング活動も実施します。そのため、アンケート結果やリスクマネジメントシステム監査の監査対象項目で改善が必要な事項については監査チームでアドバイスを行います。アドバイス結果は次回のリスクマネジメントサイクルに反映されます。
- STEP④ 経営トップへの報告
  監査チームはリスクマネジメントシステム監査結果を評価報告書にまとめ経営トップに報告します。評価報告書はリスクマネジメント基本目的への達成度に関するもの（全体評価）とリスクマネジメントの目標への達成度に関するもの（個別評価）があります。

前ページで触れた自己評価アンケートの内容は①組織と運営、②リスクの洗い出し・評価・被害想定、③日常活動・事前準備、④緊急時の活動、⑤組織能力向上・人材育成、⑥重点リスク対策推進状況の6つに分類され、各分類ごとに20～30の質問項目があります。以下に質問項目の一部を紹介します。

事例　リスクマネジメントの自己評価アンケート例

3. 日常活動・事前準備		
Q3-1 ○○部に関連するリスク情報を組織的に収集していますか？		A 担当者が決められ、定期的に収集し責任者に報告されている
		B 気づいた人が情報を収集し、責任者へ報告している
		C 特段収集していない
Q3-2 ○○部の活動上の問題点、改善点等を社員が気軽に報告できる体制（しくみ）になっていますか？		A 体制がとられており、社員から頻繁に提案がある
		B 体制はとられているが、社員からあまり提案がない
		C 特段把握していない

4. 緊急時の活動		
Q4-1 ○○部に関連する危機が発生した場合の対応方針が明確になっていますか？		A 明確な方針がある
		B 方針施策を検討している
		C 特段方針はない
Q4-2 ○○部に関連する危機が発生した場合の実施項目（対応・対処項目）の優先順位が明確になっていますか？		A 明確に決めている
		B 今後明確化する予定である
		C 特段決めていない

6. 重点リスク対策推進状況		
Q6-1 200×年度○○部の重点リスク対策の推進方針は明確になっていますか？		A 推進方針が明確に定められている
		B ある程度推進方針は定められている
		C 推進方針は定められていない
Q6-2 重点リスク対策の主旨は部の要員に説明されていますか？また、それは要員に認識されていますか？		A 年度当初に要員に説明し、要員全員が認識している
		B 要員に説明はしたが、あまり認識されていない
		C 要員に説明されていない

コラム

リスクマネジメントと監査役監査

現行の日本型経営の仕組みでは、取締役が代表取締役を監視し、監査役が取締役を監視します。会社機関の構造や会社規模にもよりますが、監査役は業務監査権と会計監査権をもっています。また、監査役の業務監査権には、取締役の職務執行の監査、取締役等の意思決定の監査のみならず内部統制システムの整備状況の監査も含まれます。

監査役による内部統制システムの整備状況の監査は、企業の内部統制に関して取締役が企業の規模・事業内容等に即した適切な内部統制システムを構築、運用しているか否かを監査することであり、内部統制システムには、法令等遵守体制（コンプライアンス体制）、リスク管理体制及び企業情報の適正かつ適時名開示のための体制が含まれます。
したがって、監査役はリスク管理体制の整備状況を監査する権限をもちます。また、監査役は取締役の職務執行の監査権をもつため、取締役がリスクマネジメントを忠実に実施しているのかというリスクマネジメントの実施状況についても監査権があります。

リスクマネジメントシステム監査の主目的は組織の最高経営責任者によるレビューの際の情報を提供するためです。そういった意味では取締役の職務執行の範疇でリスクマネジメントシステム監査が実施されています。監査役が独立した立場で最高経営責任者の活動を含めたリスクマネジメントシステム全体を監査することにより、すべてが完結するのです。

参考資料

リスクマネジメントのフレームワーク

ここでは、参考資料としてリスクマネジメントのフレームワークを4つ紹介します。
まず、本テキストの構成上も参考としたJIS Q 2001におけるリスクマネジメントを紹介します。
その上で代表的なリスクマネジメントのフレームワークとして COSO ERMを紹介します。
その他経済産業省『リスク新時代の内部統制』、ターンブル・レポートで示されているリスクマネジメントの概念に関しても紹介していきます。

これらにはISO 9000シリーズ等のような認証制度があるわけではありませんが、自社で体制を構築する際の参考書として大変有用です。

内容

JIS Q 2001リスクマネジメント構築のための指針
- JIS Q 2001とは
- なぜJIS Q 2001なのか
- リスクマネジメントシステム構築のためのPDCAサイクル

COSO Enterprise Risk Management – Integrated Framework
- COSO ERMとは
- COSO ERMにおいて用いられている重要な概念について

「リスク新時代の内部統制～リスクマンジメントと一体となって機能する内部統制の指針～」
- 「リスク新時代の内部統制」からみるリスクマネジメント

ターンブル・レポートにみる英国のコーポレートガバナンス
- ターンブル・レポートの特徴

JIS Q 2001 リスクマネジメント構築のための指針

2001年3月に日本工業規格（JIS規格）として「リスクマネジメント構築のための指針」（JIS Q 2001）が制定され、現在この規格に従ってリスクマネジメントシステムを導入する企業が増えています。

本規格の適用方法について解説した書籍は数多く市販されています。こういった書籍によって理解を深めるのも良いでしょう。

JIS Q 2001 とは

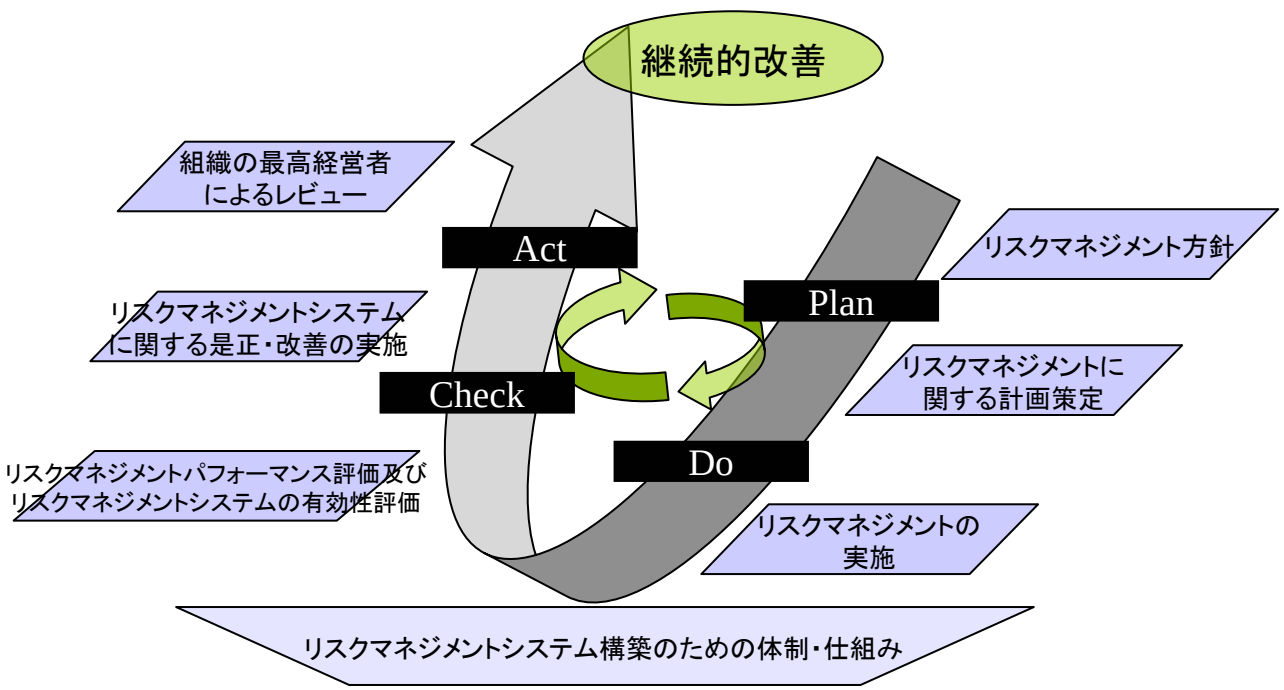
JIS Q 2001は、1995年の阪神・淡路大震災がきっかけとなって企業や自治体などのリスクマネジメントのあり方が問われた中で、地震、災害のほか、コンプライアンス、環境問題、情報漏えいなど、さまざまな危機に対応して、組織体が管理体制を構築するための指針として制定されたものです*。」

*『事業リスクマネジメントーテキストー 経済産業省 平成16年3月』400ページより引用

JIS Q 2001 におけるリスクマネジメントシステム構築のステップは以下の通りです

リスクマネジメント方針の策定
リスクマネジメントに関する計画作成
リスクマネジメントの実施
リスクマネジメントのパフォーマンス評価及びリスクマネジメントシステムの有効性評価
リスクマネジメントに関する是正・改善の実施
組織の最高経営者によるレビュー
継続的改善

参考　JIS Q 2001におけるリスクマネジメントシステムのプロセスモデル



『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年 より作成

なぜJIS Q 2001なのか

JIS Q 2001 リスクマネジメントシステムには以下のような狙いがあります。

JIS Q 2001はリスクマネジメントを組織的に実行していくためのリスクマネジメントの枠組みを提供するとともに、さまざまなリスクに共通なリスクマネジメントシステム構築のための原則及び諸要素の提供を意図して作られており、どのような種類及び規模の組織にも適用できるように作成されている。何よりも大事なのはこの規格によって、リスクに関する用語及び概念の共通基盤をもつことができることである*

「この規格に規定するリスクマネジメントシステムの要素を、既存のマネジメントシステムの要素と独立して設定する必要はありません。場合によっては既存のマネジメントシステムの要素を適用することによって、規定した事項を満たすことが可能になります*。」

*『JISQ2001 リスクマネジメントシステム構築のための指針』日本規格協会編 2003年 より一部修正

リスクマネジメントシステムとして優れている点

PDCAサイクルを採用しているため他のマネジメントシステムと同様にマネジメントが可能である

危機管理に対しても特徴的な事項に関して包含している

検証・評価(Check)、是正(Act)を重視した継続的改善システムである

導入の際、考慮すべき点

指針を自社の組織や文化に合わせて柔軟に解釈することが必要である

指針のすべてに取り組む場合には相当の労力、負担が必要である

指針は実際にどう取り組むべきか具体的な例を示していない

リスクマネジメントシステム構築のためのPDCAサイクル

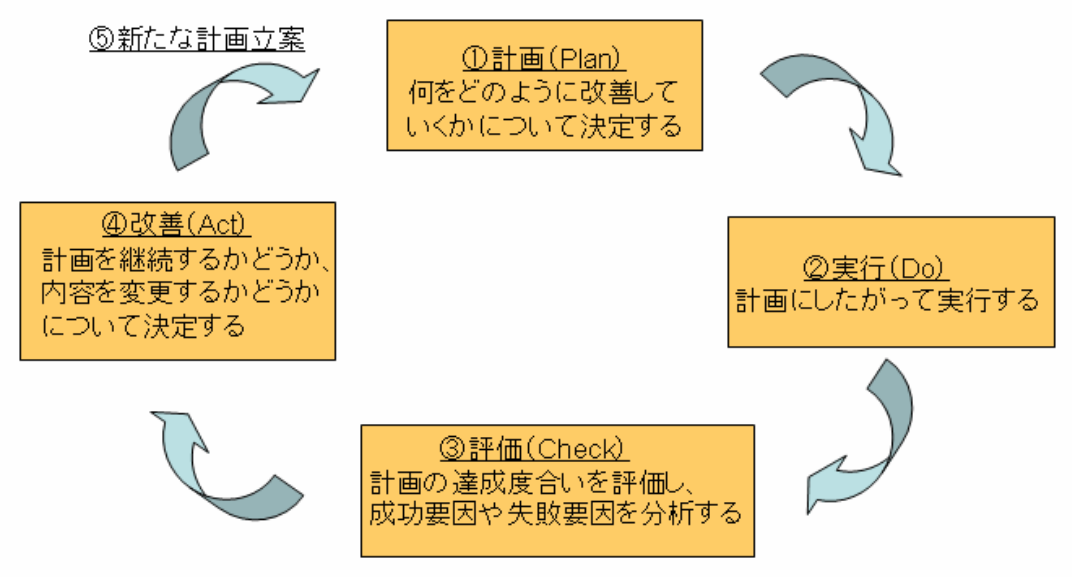
PDCAサイクルの生い立ち、特徴について説明していきます。

「PDCAサイクルとは、計画(Plan)を実行(Do)し、評価(Check)して改善(Act)に結びつけ、その結果を次の計画に活かすプロセスのことです。欧米ではこの考え方を体系化したデミング博士(Dr. W. Edwards Deming)の名前をとって、デミングサイクルとも呼ばれています。

PDCAサイクルの考え方は、民間企業が製品の品質向上や経費削減などを検討する際に広く用いられてきました。一つのプロジェクトについて計画から改善までのプロセスを継続することによって、より良い成果を上げることが期待できるからです。
プロセスを具体的にあらわしたのが下の図です。PDCAサイクルの最大の特徴は、計画から改善に至るプロセスを、さらに次の計画に結びつけることにあります*。」
* 日経BPネットワーク ホームページ キーワード「PDCAサイクル」よりI一部修正

リスクマネジメントにおいてもリスクマネジメントパフォーマンス評価といった評価(Check)の後、リスクマネジメントシステムに関する是正・改善の実施といった改善(Act)が次年度のリスクマネジメント計画の策定に結びつきます。

参考　リスクマネジメント体制構築のためのPDCAサイクル



日経BPネットワーク ホームページ キーワード「PDCAサイクル」より引用

リスクマネジメントサイクルとして優れている点

計画から改善に至るプロセスを次の計画に結びつけることが可能

他のマネジメントシステムに組み込んで同様にマネジメントすることが可能

通常業務の中でよく使われているマネジメントサイクルであり馴染みがある

COSO Enterprise Risk Management – Integrated Framework (ERM)

リスクマネジメントに関する諸説は、多くの経営者・管理者が共有して理解する一般的なものとなっていませんでした。

こうした状況を踏まえ、経営者・管理者が共有しうるリスク・マネジメントの考え方、ガイダンスを提供することを目指し、2004年9月に米国トレッドウェイ委員会組織委員会（the Committee of Sponsoring Organizations of the Treadway Commission: COSO）はEnterprise Risk Management Framework（以下、COSO ERM）を公表しました。

COSO ERMとは

COSO ERMは従来より公表されていたCOSO内部統制フレームワークの概念をその周縁に拡張し、精緻化したものと言われています。内部統制概念の事実上の標準として各国に浸透しているCOSO内部統制概念との親和性ゆえに、COSO ERMは有力なリスク・マネジメントのフレームワークとなる可能性を秘めています。

COSO ERMに則りERMを導入した場合に強化される点

リスク許容限度及び戦略の検討（Aligning risk appetite and strategy）

リスク対応の意思決定の強化（Enhancing risk response decisions）

業務上の予期しない事象及び損失の抑制（Reducing operational surprises and losses）

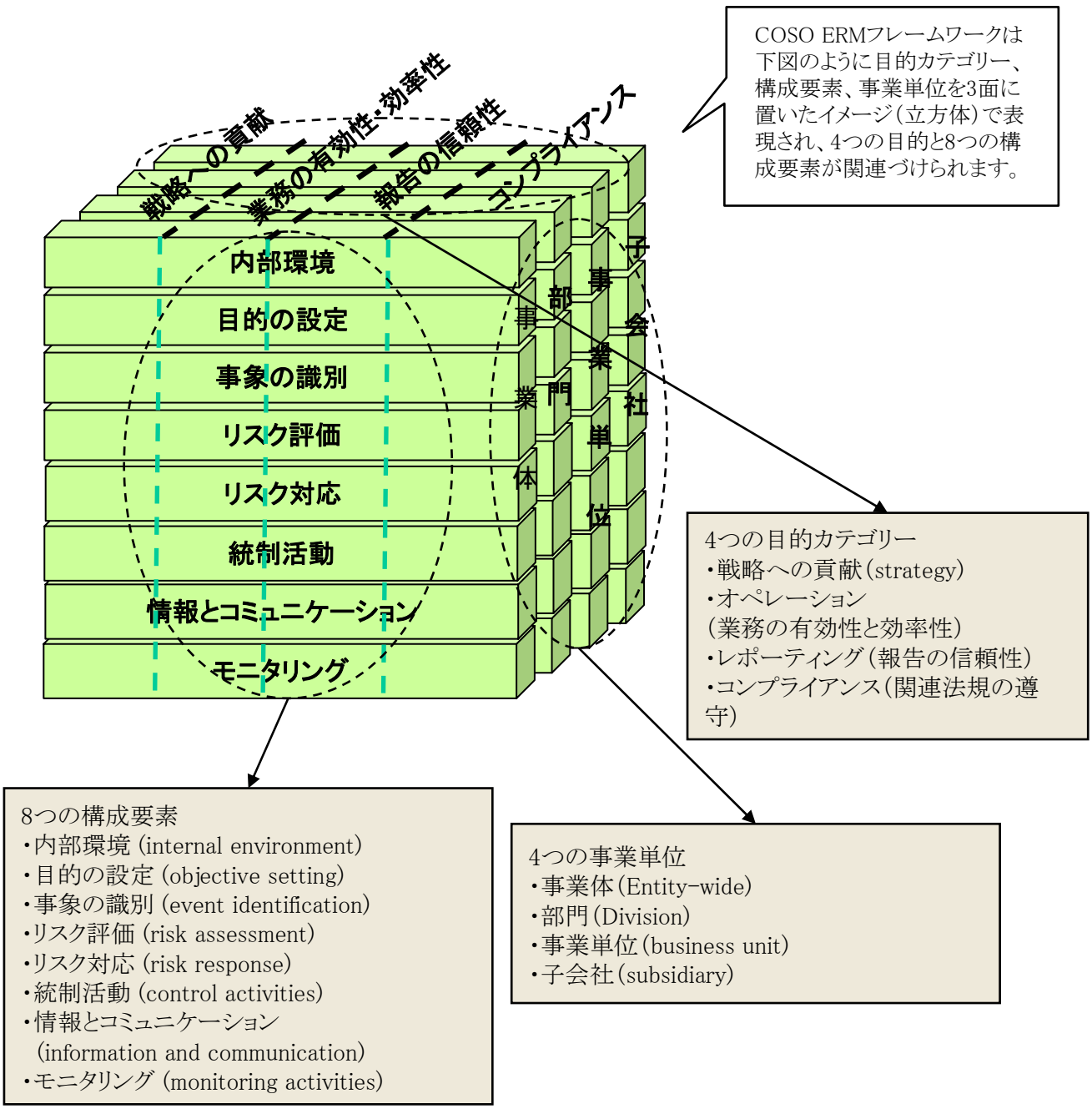
複数のかつ組織横断的なリスクの識別と管理(Identifying and managing multiple and cross- enterprise risks)

機会の獲得（Seizing opportunities）

資本配分の向上（Improving deployment of capital）

COSO ERM キューブ

COSO ERMはERMを3つの基礎概念で整理しています。この概念枠組みは立方体イメージ(Cube)で表現されます。個々の活動は、ERMのどこに属するか分類されることで、その意義を把握することができます。



中央青山監査法人ホームページ リスクマネジメント・内部監査 連載『COSO「エンタープライズ・リスク・マネジメント」のポイントとその日本企業における展開』 より作成

詳しくはCOSOホームページを参照ください。
http://www.coso.org/

COSO ERMにおいて用いられている重要な概念について

COSO ERMでは「ERM」の説明に先立ち「内部統制の統合的枠組み」の中では明確にされていなかった、いくつかの重要な概念について以下のように説明しています。

「リスク(Risk)」:ある事象が発生した場合、それが事業体の目的達成に悪影響を与える可能性
「機会」:ある事象が発生した場合、それが事業体の目的達成に好影響を及ぼす可能性

- 従来リスクについては、色々な場面で様々な捉え方がされており、統一的な考え方が定着していたとはいえない状態にありました。
- ここでは「リスク」を、ビジネスリスクを対象にしたものと限定した上で、ある事象が発生した場合、それが事業体の目的達成に悪影響を与える可能性と定義し、また、「機会」をある事象が発生した場合、それが事業体の目的達成に好影響を及ぼす可能性と定義づけています。
- 事業体の目的を達成するという観点から、起こり得る事象のプラスとマイナスの両側面をそれぞれ「リスク」と「機会」として捉えています。

潜在的な事象(Potential Events):事業体の内部・外部のそれぞれの要因から発生し、戦略と諸目的の達成に影響を与える可能性がある事象

- 事業体の内部・外部のそれぞれの要因から発生し、戦略と諸目的の達成に影響を与える可能性がある事象のことを言います。

リスク選好度(Risk Appetite):事業体がそのミッション・ビジョン、つまりその価値創造の追求のために、受け入れようとする「リスク」の大きさ

- 事業体がそのミッション・ビジョン、つまりその価値創造の追求のために、受け入れようとする「リスク」の大きさのことです。
- 事業体の戦略から期待されるリターンは、この「リスク選好度」と整合性を持っていることが必要という点で、「リスク欲求」は事業体の戦略に直接的に関わるものです。

リスク受容度(Risk Tolerances):事業目的達成のために、事業体が受け入れ可能なリスクの大きさ

- 事業目的達成のために(つまり、事業体のミッション・ビジョンに基づく価値創造のために)、事業体が受け入れ可能なリスクの大きさ(水準)を意味しています。
- 経営者は事業体の「リスク選好度」と整合性を取るように、様々な事業目的の相対的な重要性を検討して、個々の「リスク受容度」を設定することが求められます。

リスクをポートフォリオの観点から捉えること(Portfolio View of Risk):事業体がその事業目的の達成を考えるに当たって、事業体が負っている全ての「リスク」を集合体として捉え、それを「リスクのポートフォリオ」という観点からも検討する必要がある

- 事業体がその事業目的の達成を考えるに当たって、個々の「リスク」にそれぞれ焦点を当て検討するばかりでなく、事業体が負っている全ての「リスク」を集合体として捉え、それを「リスクのポートフォリオ」という観点からも検討する必要があるということです。

以上全て中央青山監査法人ホームページ リスクマネジメント・内部監査『COSO「エンタープライズリスクマネジメントフレームワーク」の公開草案』より一部修正

COSO 内部統制概念との関係

COSO内部統制(内部統制の統合的枠組み)との関係下図のようになっており以下のことがいえます。

参考　COSO内部統制概念(内部統制の統合的枠組み)との関係

COSO ERM	COSO	相違点
1.内部環境	1.統制環境	概念の拡大
2.目的設定	―	新構成要素追加
3.事象認識 4.リスク評価 5.リスクへの対応	2.リスク評価	分割と内容の高度化
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.情報と伝達	概念の拡大
8.モニタリング	5. モニタリング	変更なし

- ✓ 有効なERMには有効な内部統制が不可欠である
- ✓ COSO　ERMは既存のCOSO内部統制概念を廃棄するものではなく、COSO内部統制の外縁にERM概念、枠組みを構築したものであり、COSO内部統制概念をその一部として含む(incorporate)ものである
- ✓ COSO　ERMは、COSO内部統制の構成要素を拡張し、精緻化した
- ✓ COSO内部統制は目的の設定は内部統制にとって与件(Prerequisite)としたのに対し、COSO　ERMは目的の設定を独立した構成要素として含むものとしている
- ✓ COSO　ERMにおける目的分類のうち、「報告」は、COSO内部統制の「財務報告」目的を拡張したものである
- ✓ COSO　ERMはCOSO内部統制のリスク評価概念を拡張し、かつ、事象の識別、リスク評価、リスク対応に細分した

「リスク新時代の内部統制
～リスクマネジメントと一体となって機能する内部統制の指針～」

経済産業省は、産業界、学会、会計プロフェッション、法曹界等を代表する委員からなる「リスク管理・内部統制に関する研究会」を設置し、COSOレポートを参考としつつ検討を重ねた結果として、内部統制に関する指針「リスク新時代の内部統制　～リスクマネジメントと一体となって機能する内部統制の指針～」を2003年6月に策定しました。

「リスク新時代の内部統制」からみるリスクマネジメント

この指針ではリスクマネジメントおよび内部統制について以下のように説明しています。

リスクマネジメントとは「企業の価値を維持・増大していくために、企業が経営を行っていく上で事業に関連する内外の様々なリスクを適切に管理する活動」である

内部統制とは「企業がその業務を適正かつ効率的に遂行するために、社内に構築され、運用される体制及びプロセス」である＊

＊経済産業省「リスク新時代の内部統制　リスクマネジメントと一体となって機能する内部統制の指針」リスク管理・内部統制に関する研究会　2003年6月より一部修正

重要なポイント

この指針における重要なポイントは以下の2点です

リスクマネジメントと一体となって機能する内部統制を構築することが大切

内部統制はリスクマネジメントを支えるものである

内部統制が適切に機能するための基盤

内部統制が適切に機能するための基盤として下記5つの事項を説明しています。

健全な内部統制環境

円滑な情報伝達

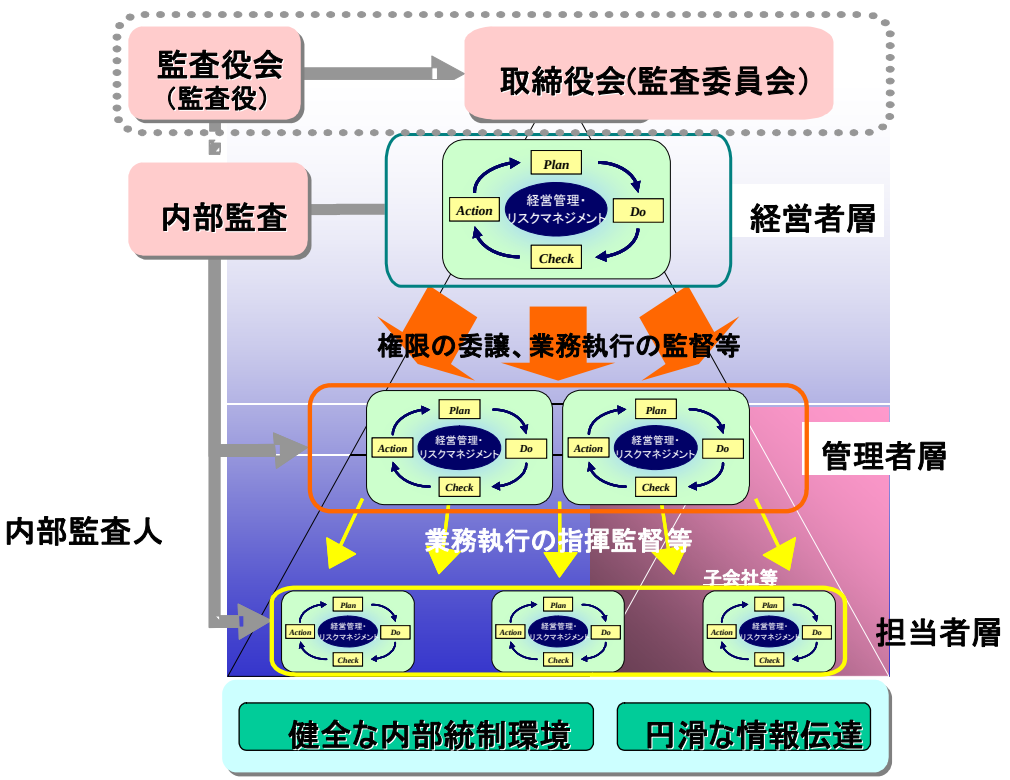
リスクに対応した内部統制の構築

日常的なコントロールとモニタリング

独立したモニタリング(内部監査)

内部統制とリスクマネジメントの関係

この指針中では、「内部統制はリスクマネジメント全体を支えるものであり、経営者は、リスクマネジメントによるリスクの評価と対応方針に応じて、内部統制のあり方の見直しを継続的に行うことが必要」とされています。また内部統制のプロセスの中で対応される「事業活動の遂行に関連するリスクは、リスクマネジメント組織へのフィードバックを通じて統合的に対処がなされる必要がある」とされています。これらを確保することでリスクマネジメント及び内部統制が一体的に機能し、その役割を最大限に果たすことができるとされています。
これらのことを示したのが以下の図となります。



- 内部統制の整備状況・運用状況の記述や部門責任者の評価について、独立した立場から検証を行う

経済産業省「リスク新時代の内部統制　リスクマネジメントと一体となって機能する内部統制の指針」リスク管理・内部統制に関する研究会　2003年6月より作成

経済産業省「リスク新時代の内部統制　リスクマネジメントと一体となって機能する内部統制の指針」リスク管理・内部統制に関する研究会は経済産業省ホームページより閲覧が可能です。

内部統制に関しては「5.3 内部統制」で詳しく触れています。

ターンブル・レポートにみる英国のコーポレートガバナンス

ロンドン証券取引所では、上場企業を対象に1999年12月23日以降の決算期からターンブル・レポートの遵守を義務付けましたが、これは企業自らが適切にリスクマネジメントを行うことにより、健全な事業の実施・発展を図ることを目的としています。

ターンブル・レポートの特徴は、内部統制についての取締役会の責任を明示することにより、その実効性を担保した点であるといえます。

ターンブル・レポートの概要は以下の通りです。

健全な内部統制の維持

- 健全な内部統制の維持に関する責任は取締役会が負い、企業の置かれている環境と組織目的を十分理解した上で適切な方針を設定し、また有効に運用されてるかについて継続的に確かめなければならないとされています。
- また、リスクと統制に関する取締役会の方針を受けて具体的な導入作業を行うのは、経営者の役割であるとされています。
- さらに、全ての従業員はそれぞれの与えられた領域において、目的達成のために内部統制を適切に運用することについて責任を負うとされています。なおここでは、健全な内部統制の要素についても言及されています。

内部統制の有効性の評価

- 内部統制の有効性の評価は、取締役会の基本的な職務であるとされています。内部統制の有効性の評価プロセスには、経営陣より定期的に報告を受けることのほか、実効性を継続的にレビュー・評価すること、さらに年次報告において説明することが含まれます。
- 経営者の報告には、リスクと内部統制の有効性とに関するバランスのとれた評価が示されていることが必要であり、取締役会は適切に全体状況と重要なリスク・統制が捕捉され、重大な統制の欠陥に手当てが施され、更に突っ込んだレビューが必要であるかを検討することとされています。

取締役会の内部統制についての意見書

- 取締役会は、企業の重要なリスクを識別し、評価し、対応するための継続的プロセスがあること、および年次報告書の承認の日まで取締役会が定期的にレビューしていることを最低限記載する必要があるとされています。

内部監査

- 内部監査部門を有していない会社においては、毎年のリスク状況の変化を勘案して、その必要性について継続的に再検討しなければならないとされています。内部監査部門は、上級経営者や取締役会にとって、リスクと統制の客観的評価機能として有用です。そのため、こうした内部監査部門が無い場合には、経営者は自らと取締役会のために、何らかの代替的な内部統制の有効性の監視手続を持たねばならないとされています。また、取締役会はその手続の適切性を検証しなければならないとされています。
- なお、内部監査部門がある場合にも、会社はその範囲、権限、資源配分等を十分に再検討する必要があるとされています。

以上全てトーマツ企業リスク研究所ホームページ キーワード「英国のコーポレートガバナンス」より引用

詳しくはイングランド・ウェールズ公認会計士協会ホームページを参照ください。
http://www.icaew.co.uk/

テキスト開発にご協力頂いた企業

本テキストを開発するにあたり、事例の提供やテキスト内容への助言等で以下の企業に多大なる御協力をいただきました。深くお礼申し上げます。

なお、本テキストに掲載されている事例は、必ずしも特定企業の実例をそのまま記載しているわけではなく、テキスト用に一部変更、または複数社の例を折衷しているものがあります。

テキスト開発協力企業

＊社名掲載を御了承いただいた企業のみ　五十音順

株式会社イトーヨーカ堂
カゴメ株式会社
鹿島建設株式会社
株式会社資生堂
シャープ株式会社
住友商事株式会社
全日本空輸株式会社
帝人株式会社
デュポン株式会社
東京ガス株式会社
日産自動車株式会社
株式会社日立製作所
松下電器産業株式会社

他4社

調査事務局　　監査法人トーマツ エンタープライズリスクサービス部

索引

リ

レ

ロ