

リスクマネジメントシステム
ガイドライン
(初級編)

目 次

1. はじめに	
(1) 社会環境とリスクマネジメントシステム	1
(2) 本ガイドラインの目的と構成	3
2. リスクとリスクマネジメント	
(1) 正しいリスクの理解	4
(2) 正しいリスクマネジメントの理解	5
(3) リスクマネジメントの原則	6
3. Plan - 計画	
(1) リスクマネジメントシステム	7
1 リスクマネジメント方針の決定	8
2 リスクマネジメント組織体制の決定	9
3 リスクマネジメント規程の策定	10
(2) リスクマネジメント用語の定義	11
(3) 緊急事態の定義とレベルの判断	12
1 エスカレーションルール	12
2 対策本部の設置	13
3 対策本部の役割、責任、権限	14
4. Do- リスクマネジメントプロセス	
(1) リスクを認識する	15
(2) リスクを分析する	16
(3) リスクを評価する	19
(4) リスクへの対応	20
(5) 対策の立案	21
(6) 対策の実施	22
1 目標の設定	22
2 ガイドラインまたはマニュアルの策定	22
3 コミュニケーション方法の策定	23
5. Check- モニタリング	
(7) モニタリング	24
6. Action- 是正・改善	
(8) 是正・改善	25

1. はじめに

(1) 社会環境とリスクマネジメントシステム

近年、営利目的組織（企業）及び非営利目的組織（公的機関や団体）（以下、まとめて「組織」という）には、コンプライアンス、リスクマネジメント、内部統制といった、業務の適正を確保する体制が求められています。同時に、多くの組織では、取引先から「CSRアンケート」と称し、環境や製品の安全、労働環境や人権の尊重といった課題に、組織としてどのように対応しているかの「説明」を要求されるようになりました。

お取引CSRアンケート

- 法令遵守
- 製品の安全
- 労働者の安全と人権の尊重
- 公正な取引
- 情報管理
- 反社会的勢力への対応
- 環境
- 災害（事業継続計画）

ここがポイント！

このようなアンケートに、どのように回答したらよいのか、悩んでいる経営者も多いようです。このアンケートにある項目は、CSR（企業の社会的責任）として、一般的に組織に対応が求められているものですが、現代社会ではこれらの課題への対応不備は、組織の信用を喪失する「リスク」なのです。各項目に「リスク」という言葉を追加する、例えば「法令遵守リスク」のように考えると、その対応方法がわかりやすくなります。

このアンケートへの回答として、「まだ、取組んでいない。近いうちに取組みます」で済まされるでしょうか？答えは、「No」です。このアンケートは、発注元の企業が「取引先に関するリスク」を管理することを目的に実施しているもので、単なるアンケート調査ではありません。つまり、御社に対し「説明責任」を求めているのです。

説明責任 Accountability

アカウンタビリティは、英語で会計を意味する Accounting と Responsibility という責任を意味する言葉を合成した単語で、もともとは企業が決算報告をする責任として使用されていました。しかし、現在では意味の範囲が大幅に拡大し、企業や組織が、その活動に関する事項をステークホルダーに報告する責任として使われています。また、説明責任は、ただ単に「説明する責任」ではなく、顧客や消費者に対し約束した内容を嘘、偽りなく実行していること、そして説明する内容が全て事実であることへの責任も含みます。さらには一方的に説明するのではなく、ステークホルダーからの質問に答えながら、相互が意見を交換し、ステークホルダーが納得する説明をするという、非常に重大な責任です。



しかし、ここで誤解してはいけないことがあります。それは、「取引先は、各課題に対し、完璧な管理ができている、という回答を望んでいるわけではない」ということです。日本社会の文化は、これまで「完璧」を追求し、技術やサービスが発展してきました。しかし、組織運営において「完璧」はほぼありえません。それは、質問を投げかけている取引先が、一番よく理解しています。では、なぜこのようなアンケート調査を実施するのでしょうか？それは、「取引先の信頼性の高さを把握する」ことが目的です。重要なリスクを認識し、組織として管理しようとしているか？それらリスクを管理するために、組織としてどのような体制や仕組みを構築しているか？組を把握することにより、自社の商品やサービスの信頼性を高めるために行っている活動なのです。

このような調査には、「本音と建前」で回答してはいけません。また、さまざまな課題（リスク）に対し、「取組んでいます」または「これから取組みます」というあいまいな回答では、取引先の自社に対する信頼性を高めることはできません。回答内容と事実が乖離している場合、取引停止になる可能性もあります。

要請されたアンケートにおいて求められる回答は、全ての項目に関し以下の4つの観点から組織の現状を報告することです。

- ① 認識 — それぞれの項目について何が課題であると考えているか？
- ② 方針 — その課題に対し、どのような目標をもっているか？
- ③ 対応 — その目標に対し、何をやっているか？
- ④ 確認 — 対応状況を把握しているか？

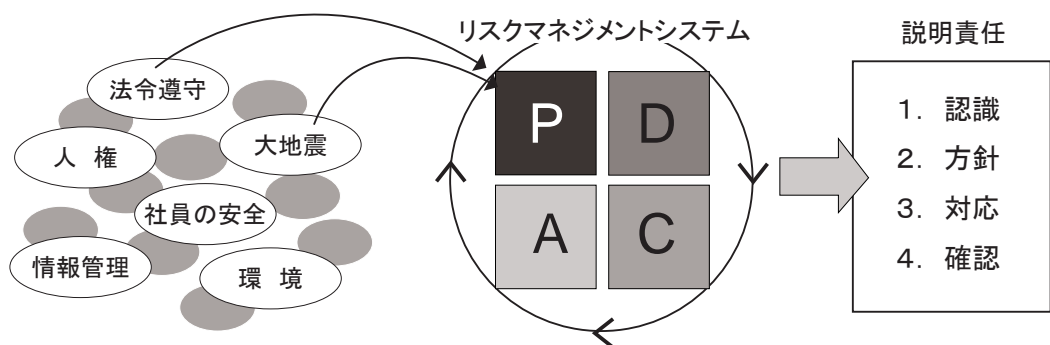
《コンプライアンスの項目に対する回答例》

① 組織としてどのように考えているか？	② どのような目標をもっているか？	③ 目標に対し、何をやっているか？	④ 対応状況を把握しているか？
コンプライアンスはもとより社会通念や道徳といった、社会から求められるより高いレベルの倫理に従って行動することと捉えている。	役員、社員一人ひとりが高い倫理意識をもって活動するとともに、法令違反ができない社内環境を整備する。	コンプライアンス方針、社員コードを明確にするとともに、違反発生確率が高い業務や社内環境を認識し、管理を強化している。	全社員に対し定期的にコンプライアンス教育を行うとともに、意識調査を実施、内部通報制度、自主監査を充実させている。

(2) 本ガイドラインの目的と構成

目的

本ガイドラインは、これまでリスクマネジメントを実施していない組織に、リスクマネジメントの基本システムを構築していただくことを目的としています。リスクマネジメントシステムは、組織に潜在するリスクを、経済的且つ効果的に管理するためのマネジメントシステムです。実効性の高いリスクマネジメントシステムを組織に構築することができれば、組織に求められるさまざまなリスクや課題への対応方法が明確になり、要請される課題への説明責任に対応することが可能になります。



構成

本ガイドラインでは、組織が実効性の高いリスクマネジメントシステムを構築するための手順として、マネジメントシステムといわれている PDCA の各プロセスで何をするのかを解説します。

また、重要なポイント、着目すべきポイントは、以下の記号を用いて、強調しています。



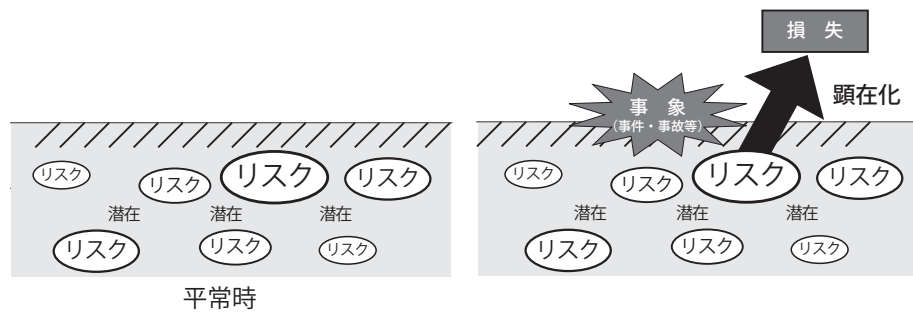
2. リスクとリスクマネジメント

(1) 正しいリスクの理解

リスクマネジメントとは、リスクを管理することです。では、リスクとは何でしょう？リスクとは、「危険」や「危険性」ではありません。リスクマネジメント協会では、リスクを以下のように定義しています。

用語
定義

リスク = 事象の発現により、結果的に組織が損失や影響を受ける、又はその結果が組織の目標達成を阻害する可能性がある状態。



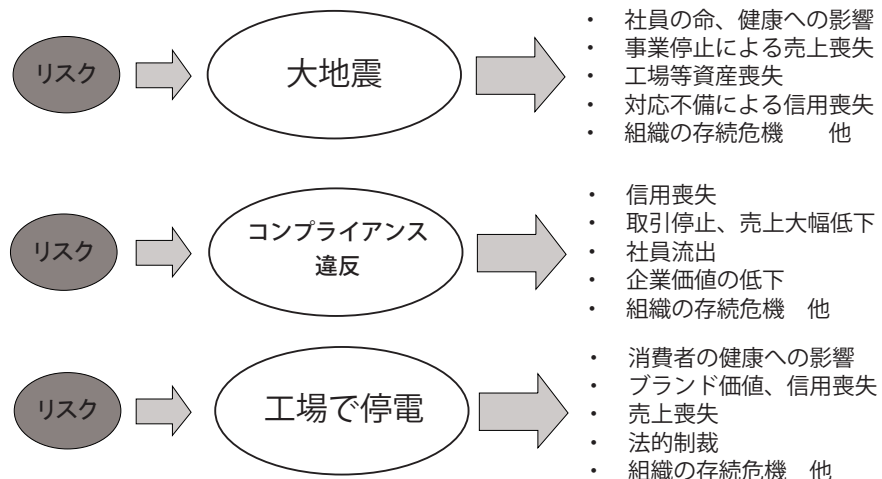
(解説)

リスクは、組織が事業活動が続ける限り、必ず潜在しています。リスクが潜在していることは、組織にとって恥ずかしいことでも、信用を失墜する要因でもありません。リスクは、ある「キッカケ」によって「損失」または「影響」へと発展します。これを、「リスクが顕在化する」といいます。「キッカケ」とは、定義にある「事象の発現」です。リスクは、この「事象の発現」の発生確率と結果として自社が受ける「損失・影響」の大きさで、そのリスクの大きさを判断します。事象の発現と損失・影響の関係は、以下のような例で表すことができます。

ここが
重要!

キッカケ (事象の発現)

結果 (損失・影響)



(2) 正しいリスクマネジメントの理解



多くの方は、リスクマネジメントとは、「事件や事故の発生を防止すること」だと理解しています。実はこの考えは、リスクマネジメントの本来の意義とは、多少異なります。前述のとおり、リスクとは「何かのキッカケにより、組織が損失や影響を被る前の状態」です。リスクマネジメントは、「事件や事故の発生を防止すること」よりも、どちらかという「組織が被る可能性がある「損失」や「影響」を管理する（最小化する）」ことを重視する経営手法なのです。組織が被る損失や影響を最小化するために、それが顕在化するキッカケ（事象の発現）が発生する確率を低減することも含まれるのですが、それが全てではありません。

リスクマネジメント協会では、リスクマネジメントを以下のように定義しています。

用語
定義

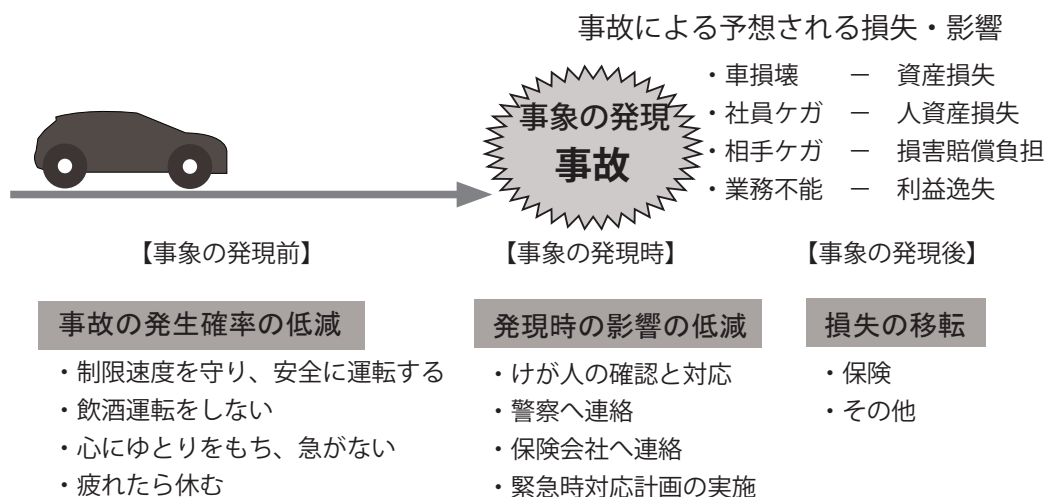
リスクマネジメント = 組織の資源を有効的に活用し、リスクを組織が設置した許容範囲内まで継続的に最小化することにより、組織を目標達成に導く活動。

(解説)

組織におけるリスクマネジメントは、組織にとって悪い結果を可能な限り予防、又は縮小することです。日本企業の多くの経営者は、事故を起こさなければ良いと考え、社員に対し、「事故は起こすな」と命令します。しかし、残念ながら事故や損失、悪い影響の発生を完全に防止することは不可能です。

リスクマネジメントでは、リスクの内容にもよりますが、リスクに対し下図のように、事象の発現前・発現時・発現後の3段階で対策を考えます。

- ① 事象の発現の可能性を低減する努力
- ② 事象の発現時の対応をあらかじめ準備し、速やかに対応することにより、発生する悪い影響を最小化する。
- ③ 発生してしまった損失や影響を、なんらかの形で縮小する努力



(3) リスクマネジメントの原則

ここまで、リスクマネジメントは単なる危険管理ではないことを説明しましたが、日本では多くの方がリスクマネジメントを誤解されているので、ここでリスクマネジメントの原則として、誤解されやすい項目を解説します。



用語
定義

① リスクマネジメントは一時的なプロジェクトではない。

ISOの認証を取得するために、多くの組織ではプロジェクトチームを結成し、認証が取れた段階でチームを解散しています。本来、ISOの認証も、マネジメントシステムが実際に運用されなければ意味がないのですが、残念ながら「認証を取ること」が目的になっているようです。

現在、リスクマネジメントに関する認証制度はありませんが、このガイドラインは、全社的にリスクを管理するために、リスクを管理する仕組みである「リスクマネジメントシステム」を組織文化に定着させることが目的です。

② 全社的なリスクマネジメントとは、全社員がリスクオーナーとなり、各自の責任範囲におけるリスクを管理する体制である。

リスクオーナーとは、「組織が認識したリスクを対象に、各リスクの管理責任と説明責任をもつ人またはグループ」です。全社的にリスクを管理するためには、全社員がそれぞれの職域でリスクマネジメントを行う必要があります。

③ リスクマネジメントは、費用対効果のバランスをとりながら、リスクを組織の許容範囲内へ縮小する活動である。

リスクが顕在化することを100%防止することはできません。100%に近づけることは可能なケースもありますが、通常大規模な経営資源を投入することになります。リスクマネジメントは、費用対効果のバランスをとり、潜在するリスクを組織が許容できる範囲内まで縮小することにより、顕在化した場合においても、組織を存続させるための経営手法です。

④ リスクマネジメントは、全てのリスクに対応する活動ではない。

リスクを認識する作業をすると、100、200のリスクはリストアップされます。しかし、リスクマネジメントはこれら全てのリスクに対応するわけではありません。組織の存続や目標の達成に大きな影響を及ぼすリスクを、経営資源とのバランスを取りながら管理することが目的です。