中小企業におけるリスクマネジメントの考え方と導入プロセスとは

2021.03.19

- コンプライアンス・リスクマネジメント
- 経営戦略

- リスク管理

社会情勢や環境が大きく変化し、企業内外にさまざまなリスクが顕在化する現在、リスクマネジメントの重要性が高まっています。リスクをマネジメントするとはどういうことか、企業が行うべきプロセスをやさしく解説します。

目次

そもそもリスクとは何か

ビジネスにおけるリスクとは

「リスク(risk)」という言葉は、従来はさまざまな定義が混在していましたが、昨今は国際標準化機構（ISO）による国際的なガイドライン「ISO31000：2009, Risk management – Principles and guidelines」で定められた、以下の定義が定着しつつあります。

「目的に対する不確実性の影響（Effect of uncertainty on objectives）」

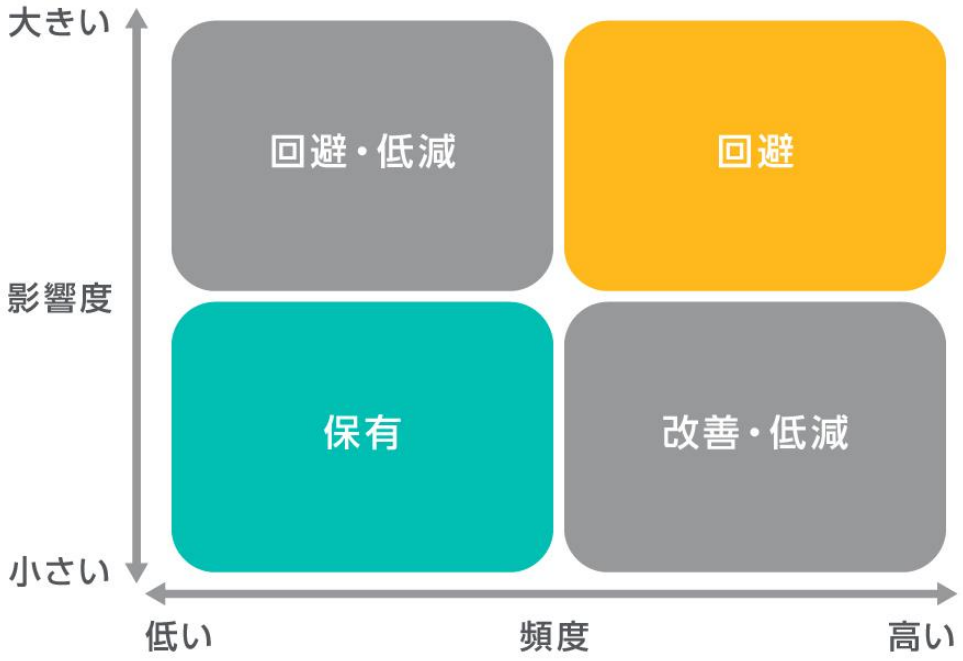
つまり、あらゆる組織は目的が達成できるかどうか、いつ達成できるか、という不確実性に直面しています。その不確実性は組織の内部にも外部にも存在します。リスクという言葉は「危険」「危機」の意味で用いられることが多いようですが、企業におけるリスクは、「起こる可能性のある事象の分布」といった統計学的な意味合いに近い意味で使われています。

たとえば、製造業の場合、原料の市場や製品、サービスを販売する市場の不確実性、売り上げが低下した場合の回復能力、営業力の不確実性など事業に関わるものや、資本調達に関する不確実性、コンプライアンス違反などに起因するリスクがあります。これらのほとんどは事前の調査・分析により影響を予測することができるリスクに分類できます。そして事前に予測することでリスクを回避、低減、ときにはリスクテイクするのが、リスクマネジメントです。

リスクの評価・算定方法

リスクの程度は誰にとっても同様に認識されるかというと、そうではありません。まったく同じ状況に対しても、人それぞれ感じ方や評価も異なります。つまりリスクの程度に対する評価は絶対的なものでなく、相対的なものであるといえます。そこで、「発生した場合の影響度×発生する頻度」という考え方でリスクを評価・算定します。そしてその結果によって、リスクに対してどのように対応するかを決定していきます。

リスク評価・算定の例



リスクマネジメントは、不確実性の管理です。しかし、不確実性とは、事件や事故が起こるかどうかではなく、必ず起こると仮定し、リスクの顕在化や影響の軽減策を平常時に準備、実行していきます。

VUCA 時代のリスク保有＝リスクをとる時代へ

VUCA（ブーカ）とは、Volatility（変動性）、Uncertainty（不確実性）、Complexity（複雑性）、Ambiguity（曖昧性）の 4 つの単語の頭文字をとった造語です。VUCA ワールド、VUCA 時代と呼ばれることもあり、社会環境が複雑化し、将来予測が困難な時代を意味する言葉です。もともとは冷戦時代からより複雑で混沌とした時代を迎えることを予想した軍事用語でしたが、2010 年代にダボス会議や ASTD （米国人材開発機構）などで使われたことがきっかけで、徐々にビジネスシーンにも広まりました。

VUCA の時代となり、リスクマネジメントの考え方も変化しました。時代の変化を事前に予測できないため、重要なのは環境の変化に素早く対応することです。そのためにすべきことは 2 つあります。

1.時代に合わせたリスクマネジメント体制の構築

スマートフォンが普及して以来、情報のスピードは格段に変化しています。PC でしか作業できなかったものがスマートフォン 1 つで完結してしまう。そんな時代に応じたリスクマネジメント体制の構築が必要です。

2.スピーディーな意思決定

SNS などの発達で世界はより緊密につながり、日本で起きたリスク事象は瞬く間に世界に拡散され、さまざまな影響を与えます。１分１秒の対応の差が企業の命運を大きく左右してしまう時代になったといえます。そんな時代のリスク対策は「明日やる」では通用しません。リスクが発生した際、誰が意思決定を下すのかを明確にしてスピーディーに決定できる体制が必要です。

リスクマネジメントの考え方

「リスクマネジメント」は「危機管理」とも言われることがあります。しかし「危機管理」は、英語では「Crisis Management（クライシスマネジメント）」であり、両者は異なる概念です。

日本語で「危機管理」という時は、「クライシスマネジメント」と「リスクマネジメント」の２つのプロセスをあわせた管理の概念として一般的に使われます。つまり、危機が発生する前の活動であるリスクマネジメントと、危機が発生した後に行うクライシスマネジメントの両者をあわせた概念である「危機管理」として認識されています。

リスクアセスメント、リスクヘッジ、クライシスマネジメントとの違い

リスクマネジメントを行う上で知っておきたい用語に「クライシスマネジメント」以外にも「リスクアセスメント」「リスクヘッジ」などがあります。ここで、それぞれの言葉を簡単に説明しておきましょう。

１．リスクアセスメント

リスク特定、リスク分析およびリスク評価をするプロセスを指します。 リスクアセスメントは、ステークホルダーの知識と見解を生かし、体系的、協力的そして反復的に行われるプロセスです。必要に応じて追加調査で補完し、利用可能な最善の情報を使用して実行することが必要です。

２．リスクヘッジ

考えられる危険に対して、何らかの対策・工夫を行うことです。リスクという言葉には、危険を表す意味以外に、「予想通りにいかない可能性」という意味もあります。思わぬ事態や避けられない危機的状況に関して、その影響を最小限に抑える対策・軽減させるような工夫も「リスクヘッジ」です。

３．クライシスマネジメント

「既存のマニュアルでは対応できない重大事故に備えて対応する」行動のことです。リスクマネジメントより重大な事象、例えばテロや自然災害など、日常レベルの想定を凌駕する事案が発生した場合、その影響を回避し、被害を最小限に抑えるためにさまざまな対策を講じる行動のことです。

リスクマネジメントをどう行うか

従来のリスク対処の４手法

従来、リスクに対応する方法には「回避・低減・移転・受容」の４つがあるとされていました。これが先述した「ISO31000：2009」やその後継によって、現在は拡充されています。まず従来の４手法から見ていきましょう。

１．回避：リスクを発生させない

リスクに対して前もって何らかの対策を行うことでリスク発生の確率を低くするのが「回避」策です。ビジネスにおいては、ノートパソコンの紛失、盗難、情報漏えいなどのリスクに備えて、保存する情報を暗号化しておく、サーバ―ルーム室に不正侵入できないように二重三重の認証を必要とする入退室管理を実施する、従業員に情報セキュリティ教育を実施して、セキュリティに対する知識を充実させ、認識を新たにさせるなどがあります。

２．低減：リスクの影響を小さくする

リスクが発生したときの影響を少なくするのが「低減」策です。自動車を運転するケースでいえば、万が一事故が起きたときに備えて、被害を抑えるために後部座席でもシートベルトを締める、高くて質のいいチャイルドシートを使うなどの対策を行い、リスクが発生した場合のダメージコントロールをするといった対処に当たります。

３．移転：リスクの影響を他に移す

リスクが起きたときに影響を第三者に移そうと考えるのが「移転」策です。保険で損失を補てんしたり、社内の情報システムの運用を他社に委託したり、不正侵入やウイルス感染の被害に対して損害賠償の形でリスクを他社などに移すことです。ただし、すべてのリスクが移転できるとは限らず、金銭的なリスクなど、一部のみ移転可能です。

４．受容：リスクを受け入れる

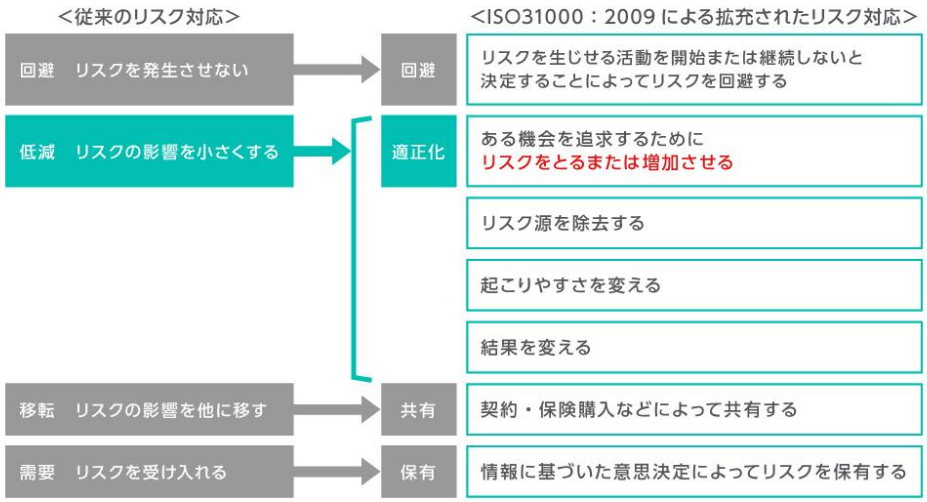
リスクの発生を認め、何もしないのが「受容」策です。リスクの影響力が小さいため、特にリスクを低減するための対策を行わず、許容範囲内としてリスク

を容認します。現状そのリスクにおいて実施すべきセキュリティ対策が見当たらない場合や、コスト（ヒト、モノ、カネ等）に見合うリスク対応効果が得られない場合などにも、リスクを容認することがあります。

リスクへの新しい対処方法

これに対して、新しい国際規格ではリスクへの対処法が拡充され、従来の対応法との対比は以下のようにまとめることができます。

従来のリスク対応と「ISO31000：2009」によるリスク対応



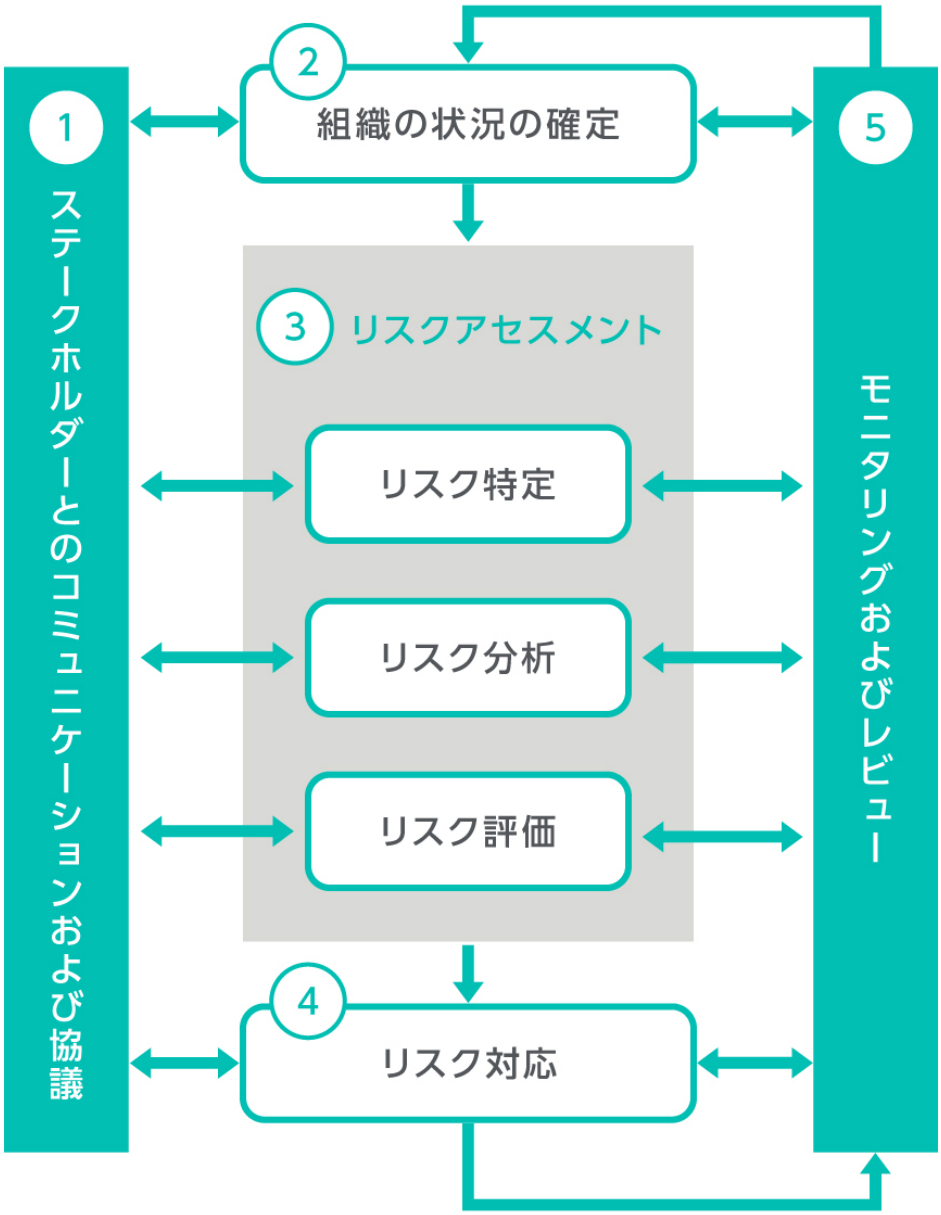
もっとも注目すべき点は、リスクは必ずしも低減されるのではなく、リスクはとるもの、または増加させるものとしても認識されていることでしょう。また、リスク適正化（低減）の方法がより詳細になっています。

リスクマネジメントのプロセス

ビジネスを遂行するうえで発生するリスクの内容や規模は、状況によってさまざまです。そして、リスクの内容や企業の規模、事業環境によって、その対応策もさまざまです。一つの方法を準備しておけばすべてに適応可能というものでは必ずしもありません。それだけにリスクマネジメントでは「プロセス」が重要になってきます。

ここでもやはり、国際規格 ISO31000：2009 が標準的なリスクマネジメントのプロセスを明らかにしていますので、見ていきましょう。

「ISO31000：2009」による具体的なリスクマネジメントプロセス



基本的なプロセスは（1）ステークホルダーとのコミュニケーションおよび協議、（2）組織の状況の確定、（3）リスクアセスメント（リスク特定・リスク分析・リスク評価）、（4）リスク対応、（5）モニタリングおよびレビューという順番に沿います。組織の活動には当然リスクが伴うため、まずリスクを特

定・分析し、そのリスクは修正されるべきか評価することによって管理していきます。注目すべきはリスクマネジメントプロセスのすべての段階で、ステークホルダーとのコミュニケーションおよび協議をおこなうべきとしていることでしょう。ステークホルダーとの対話と情報共有なくして、企業によるリスクマネジメントは不可能だと考えているわけです。

一般的な使われ方とは少し異なる「リスク」という考え方と、リスクマネジメントの考え方、対応法、プロセスなどを見てきました。企業行動はすべてリスクを伴うため、リスクの概念やリスクマネジメントの考え方、実践のプロセスを経営層・管理層がしっかりと身につけることは重要です。リスクは企業目的に対する不確実性の影響であるため、逆にいえば目的をはっきり定めなければリスクも定まらないことになります。

考え得るリスクの一覧が膨大になり、対応に至るまでが大変になってしまう例がよくあります。明確な経営目標の策定、確実なリスク評価をおこなって優先度合いを適切に算定し、上手にリスク管理を行っていきたいものです。

リスクマネジメントは企業目的に対する不確実性への対応。標準的なプロセスが確立しており、各企業の実態に即して実践しよう

リスクマネジメントを行うことで、予測できるビジネスリスクを回避、あるいはその影響を削減することが可能となります。特に VUCA 時代のビジネスでは「リスクをとる」という形でリスク対策を行う必要もあり、従来からリスク対応の考え方は変化しています。すべてのプロセスでステークホルダーとの対話と情報共有を欠かさず、適正にリスクを評価し、プロセスに沿って管理する自社の実情に合ったリスクマネジメントを心がけましょう。

【今すぐできるチェック】

- リスクマネジメントの規定を 1 年以内にチェックしたか？
- リスク発生時の意思決定権の範囲と所在を明確に定めているか？
- マニュアルでなく、守るべきことの原理原則を理解し、意思決定できているか？