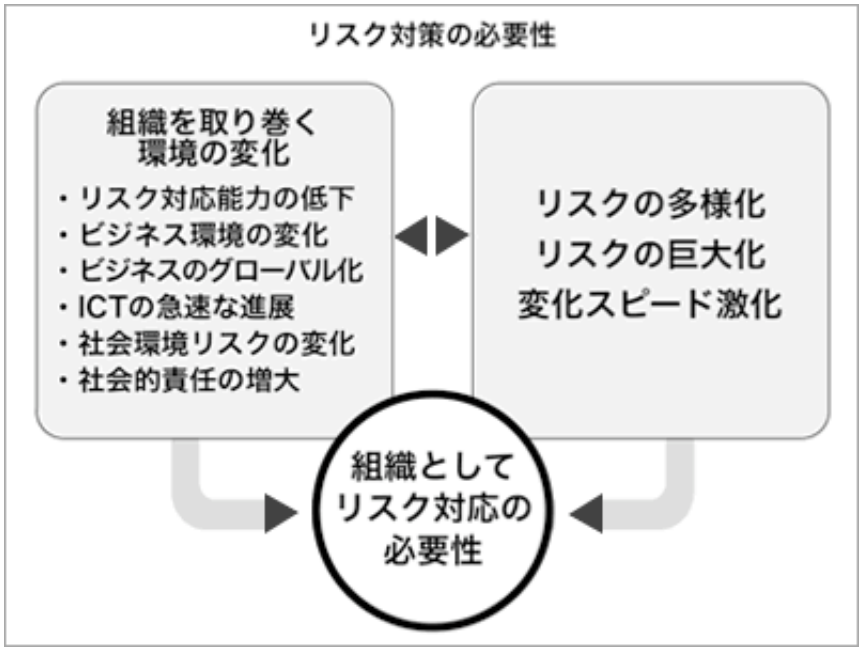
1　CSR（企業の社会的責任）としてのリスクマネジメント

今、なぜリスク対策が必要なのでしょうか。
また、リスクマネジメント（ISO31000）の取組みは、組織に何を提供してくれるのでしょうか。

多様なリスクが、様々な側面・場所で発生しています。またその変化のスピードはあまりにも早く、変化への対応が遅れることで、損害をさらに大きくしてしまう可能性もあります。

近年、組織は顧客やサプライチェーンからリスクに対してその発生を予防し、被害を最小限に留めるための仕組みの構築と実践が要求され続けてきました。

しかし、これからは受け身な姿勢だけではなく、ポジティブにリスクとその変化を予知し、ビジネスに活かしていくための強靭かつ柔軟な組織へと変革していくことが望まれています。リスクを考える上で重要なのは、マネジメントの活用でリスクのプラス面に関する期待に応えるということです。



【さまざまな要請】

○ 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。

○ リスクを回避、移転、低減という負（マイナス）の側面だけでとらえる考え方か

ら、リスクを戦略的機会ととらえ活用（プラス）することへと変化している。

○ リスクマネジメントプログラムの導入によって、組織の改革の仕組み（マネジメントシステム）として強化していくことが求められている。

○ 組織におけるリスクマネジメント能力を本当に高めるためには、経営トップがリスクマネジメントの目的（目標）を明確にし、リスクコントロールの役割を新たな視点で捉え、その期待が実現できるよう全社的活動にコミットメントしなければならない。

○ リスク管理者やリスク所有者は自らの役割として、組織がどのような期待をしているかを十分に理解し、スキルを向上させ、事業戦略として、成長のためのアプローチを心がける必要がある。

○ 活動のためには、組織の全ての階層に対し、リスクに関する情報を適確に伝え、適切にコミュニケーションしていく必要がある。

このような状況下、ISO 31000（ERM：エンタープライズリスクマネジメント）は以下の側面で支援することで、リスクに強い組織づくりを支援します。

1. **価値を創出し、受け入れられない損失を避けるための、情報に基づくリスク判断が可能**
2. **組織が特定のリスクを受け入れるかどうかのプロセスにステークホルダーを参加させる**
3. **危険な結果をもたらす極端なリスクを防止する**
4. **新しい機会、恩恵をもたらす仕組みと能力を社内に構築する**

ISO 31000（ERM）の重要な活動の一つは、ステークホルダ（利害関係者）とのリスクに対するコミュニケーション活動です。組織内部の人たち全てに組織の戦略と戦略目標に向けての意識を共有し、また組織の外部の人たちにはコミュニケーションを通じて、この戦略やその結果受け入れるリスクについて理解を得るようにしなければなりません。

組織は、リスクマネジメントの機能の対象にステークホルダー（利害関係者）を含めることによって顧客の信頼を獲得することが可能になります。しかし「ステークホルダーを含める」というのは、単に一般の人たちが何に興味を持っているか、何について話しているかを調査することでも、組織が作ったメッセージを送ることだけではありません。

「含める」というのは実際に意見をやり取り（コミュニケーション）することです。

社会的責任（CSR）に重点を置いたリスクマネジメントを実施する場合、様々なステークホルダーたちがリスクをどのように見ているかを理解することが重要なポイントとなります。

リスクマネジメントとは（ISO31000）

定義

コミュニケーション、協議及び組織の状況の確定の活動、並びにリスクの特定、分析、評価、対応、モニタリング及びレビューの活動に対する、マネジメント方針、手順及び実務の体系的な適用

構成要素

（1）コミュニケーション及び協議
（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）

考え方

「組織のマネジメントの不可欠な部分」、「組織の文化及び実務の中に組み込む」、「組織の事業プロセスに合わせて作る」とし、日常の業務の一環として実施すべきもの

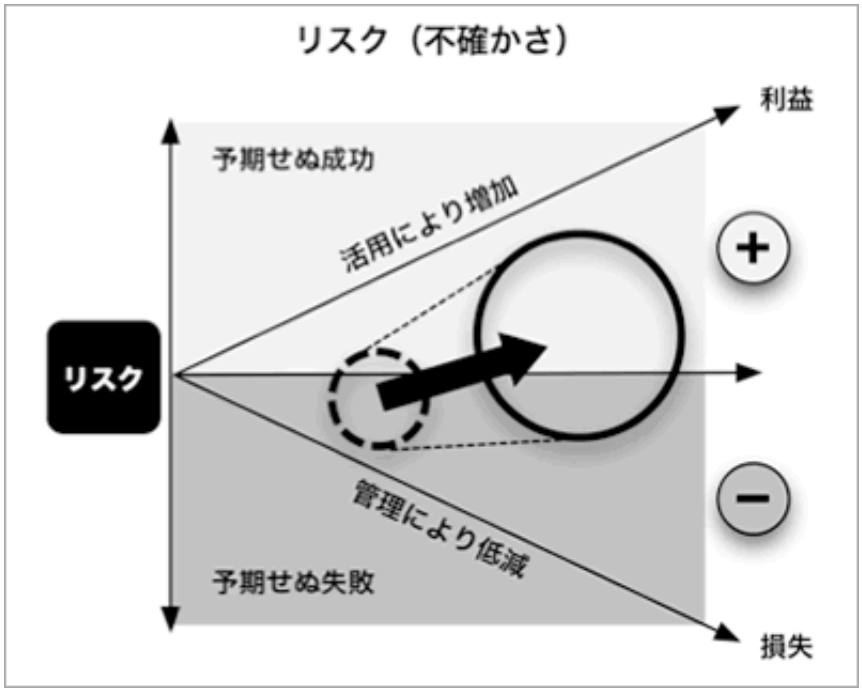
2　ISO31000の役割

今の社会で、問題となるリスクとは何でしょうか。そして、どうとらえれば良いのでしょうか。

今日のように技術や社会環境等の状況変化が大きく、さらにその変化スピードが早い時代においては、組織は目的達成の成否や時期を不確かにする内部及び外部の要素及び影響力に常に直面しています。

この「**不確かさが組織の目的に与える影響**」を「**リスク**」といいます。そして、その影響は、損失（マイナス）だけではなく、利益（プラス）に貢献することの両側面を持っています。

同時に、組織の全ての活動には、結果の良い悪いに関わらず、思い通りにならないリスク要因が多く含まれていることを認識しなければなりません。このようにリスクとは「組織の収益や損失に影響を与える不確実性」と考えることもできます。



今日社会環境は、クラウドやモバイルの普及を後押しするICT（情報通信技術）の驚異的な発展によってIoT（Internet of Things）といわれる革新的なモデルとして進化し、さらにグローバル化によるビジネス環境の広がりはスピードを早め、ダイナミックに変化しています。

○ 変化には、生活やビジネス環境の利便性を高め、ビジネスを活性化するプラスのリスクと同時に、利用依存度を高めることによりさらに大きなマイナスのリスクが潜

在しています。

○ 組織は、変化に敏感に対応し両側面のリスクを管理できなければ、これからの環境変化の中で健全な組織として発展することは困難と考えられます。それは、B to B、B to C等のビジネス形態においても同様です。

○ イノベーションや組織変革にも大きなリスクが伴うことは言うまでもありません。

○ 組織は、プラスのリスク（思いがけない成功）を効果的に役立てるために、マイナスのリスク（存在する脅威やぜい弱性、不確実性）を最小限にコントロールし、バランスよく管理できるシステム（仕組み）を持つこと事が必要です。

○ 以前からさまざまなテーマで、リスクをコントロールするために、品質、環境、情報セキュリティ、事業継続等、組織の事業活動に潜在するリスクに取り組むための仕組み（フレームワーク）が開発され、組織に導入されてきましたが、そのシステムも変化に合わせて改定が進められています。

このISO31000のリスクマネジメントの原則と指針は、さまざまなテーマのリスクマネジメント活動の原則的な指針となり、リスクマネジメントが負への対応だけではなく、組織の目的達成のために活力を与えるものとして期待されています。

3　ISO31000（リスクマネジメントの原則と指針）の特徴

ISO31000の原則と指針は、組織のマネジメント活動にどのような影響を与えるのでしょうか。

○ ISO31000は、品質マネジメントや環境マネジメントなどのその他のマネジメントに関する国際標準規格と同様に、すべての組織、すべてのリスクに適用できるように設計され、近年の各ISO規格の改定において、リスクを管理する上での原則的な指針として参照されています。

○ 必要に応じて、いつでも、組織全体に適用することも、特定の部門、プロジェクト及び活動にも適用でき、従来の情報セキュリティ対策、防火対策、交通安全などの個々のリスクマネジメントの取組みに加えて、企業戦略そのものの検討、研究開発や大規模システムの開発などのプロジェクトリスクマネジメントなどにも適用することができます。

○ マネジメントの基本であるプロセスアプローチ、PDCAによる継続的改善の考え方を採用していますが、マネジメントシステムとしての認証規格ではなく、指針、ガイドライン規格として開発されています。

○ 対象として日常のリスクマネジメントが想定され、緊急事態対応や危機管理そのものを対象としていません。

○ 予防活動を実施しても発生を防ぎきれない事件や事故（インシデント）が発生した場合の被害軽減策などを検討し、日常時に事前準備を実施したり訓練を実施することがこのリスクマネジメント原則および指針の役割です。

○ 実際の緊急事態対応そのものを円滑に実施するためのマネジメントや事業を継続するための対応などは、対象外とし、情報セキュリティマネジメント（ISO27001）や社会セキュリティ事業継続マネジメント（ISO22301）などの規格に委ねています。

4　ISO31000（ERM）の考え方

なぜ、この時代にエンタープライスリスクマネジメントが必要とされているのでしょうか。

ISO31000はERM（エンタープライズ・リスク・マネジメント）として開発されています。

エンタープライズがついている理由は、このリスクマネジメントが、より戦略的な視点で、組織間の相互依存と毎日の業務への関わりを考え、リスク・マネジメントが組織を守るだけでなく価値を創出することを目的としているためです。

ISO31000のERMは戦略的な事業の進め方であり、事業のすべての面でのリスクを特定し、それらのリスクの総合的な影響を、相互に関連するリスク対応ノウハウとして管理することにより企業が事業目標を達成することを支援します。

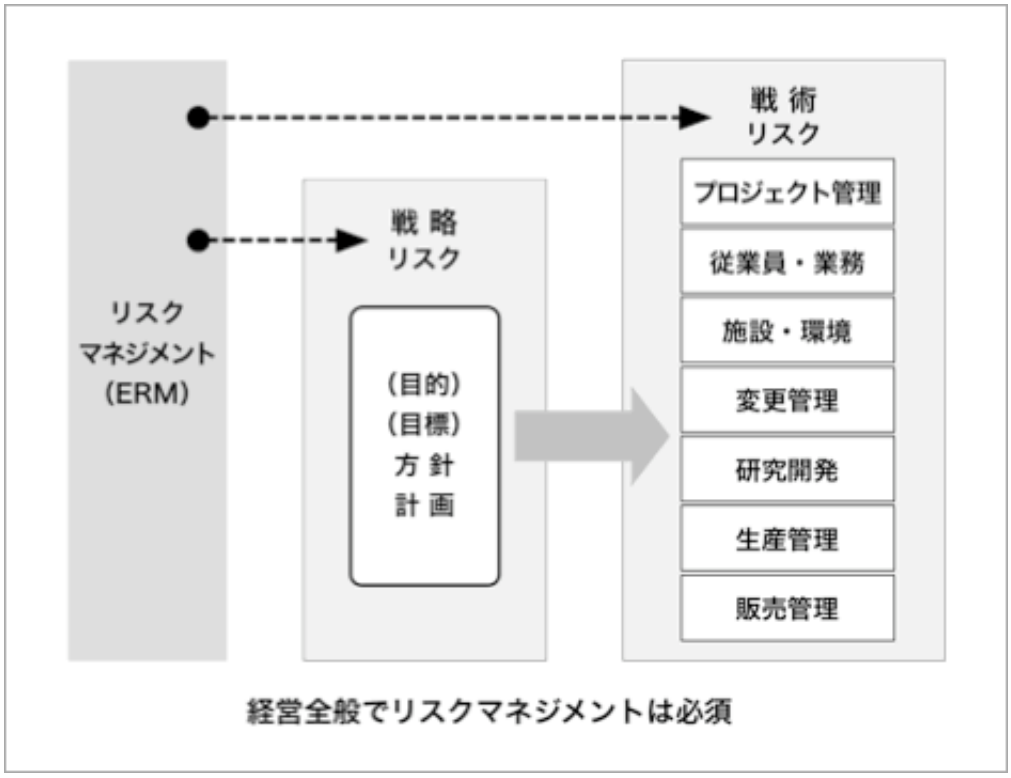
ISO31000（ERM）はそれまでのリスク・マネジメントについてのアプローチと比べて以下の点で大きく進化しています。

- 財務、サプライチェーン、事業運用、企業評価、その他の**あらゆる組織の直面するリスクを対象**としています。
- それらのリスクを独立した個別の要素ではなく、**相互に関連するリスクとして優先順位づけし管理**します。
- リスク対応計画を全ての**重要な利害関係者**（内部、外部環境、システム、環境、ステークホルダー等）**との関係において評価**します。
- ERMを利用すると、企業内の**様々なリスクが相互に関連**しており、他の部門にも**影響を与えうるものであることが理解**されるようになります。個別のリスクは他のリスク、部門に影響することにより、より大きなリスクに拡大することが認知されます。
- ERMにより全ての定性的および定量的なリスクが決められた**プロセスに沿って管理できる**ようになります。
- ERMによりリスクの効果的な管理が**競争力の源泉**になります。

そして、

- ERMにより、組織全体にわたって全ての**重要な意思決定にリスク・マネジメント**

の要素が考慮されるようになります。



多くの企業では、情報セキュリティマネジメント（ISMS）や環境マネジメントシステム（EMS）、品質マネジメントシステム（QMS）等がERMの一部として、すでに取り組まれています。

そして、ERMを導入する前の最初の重要なステップは、企業がすでに取り組んでいるリスクマネジメントが、ERMの枠組みの中のどの段階にあるのか現状を正しく評価することです。それからERMの考え方、実践方法を受け入れるための計画を作ることになります。

ISO31000は、ERM文化を適用していく上で不可欠な内部・外部の脅威、人材、プロセス、コミュニケーションとシステムを適切に評価する仕組みです。

この仕組みによって、実務に携わるリスク管理者やリスク所有者、実務者がリスクマネジメントの全体像を把握するための支援をし、組織の中でリスクマネジメントのレベルを上げることを支援します。

このように、ERMの導入を成功させるためには**組織の全体的な事業目標と連携**していくことが重要なポイントとなります。この連携によりERMプログラムは戦略的リスクマネジメントへとレベルアップしてくことができます。

そして、事故、傷害、自然災害があった時だけに利用するものではなく、組織の使命、目標、目的を明確にして、組織のすべての階層に対して伝え、組織の全員が自らの成果を組織の戦略目標と連動させます。

リスクマネジメントの目標は、技術者や顧客サービス、組織の全ての階層の従業員が**目標達成を妨げる多くの側面の不安定要素を見つけ、管理できるよう支援する**ことにあります。

5　リスクの考え方

組織の目的とリスクとの関係、目的に対する影響をどう考えればよいのでしょうか。

リスクマネジメントの管理対象は「リスク」です。このリスクの定義には変遷があり、現在の「JIS Q 31000：2010リスクマネジメント―原則及び指針」では、リスクを『目的に対する不確かさの影響』と定義しています。

「組織の目的の達成」のために

あらゆる業態及び規模の組織は、
自らの目的達成の成否及び時期を不確かにする内部及び外部の要素及び影響力に直面している。
この不確かさが組織の目的に与える影響を“リスク”という。

リスクは目的との関係で把握すべきものであり、目的に影響のない不確実性はそもそもリスク管理の対象から外れることを意味します。

すなわち、リスクマネジメントを実施する上では、**まずは目的をしっかりと認識すること**が重要なテーマとなります。

また、この定義は、**『不確かさ』と『その影響』いう二つの視点からリスクを検討する**必要があることを示唆し、**プラスであれマイナスであれ、『影響』はすべてリスクと捉えている**ところに、今までとの大きな違いがあります。