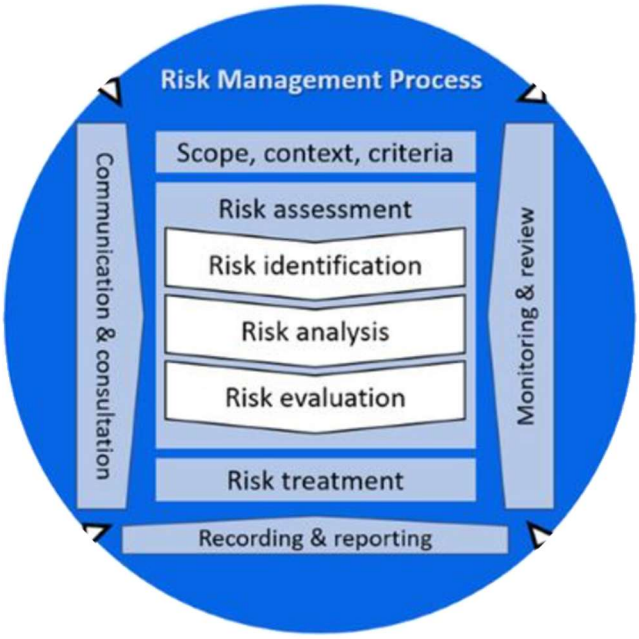
ISO31000

箇条 6 プロセス

6.1 一般

リスクマネジメントプロセスには，方針，手順及び方策を，コミュニケーション及び協議，状況の確定，並びにリスクのアセスメント，対応，モニタリング，レビュー，記録作成及び報告の活動に体系的に適用することが含まれる。このプロセスは図を参照ください。



リスクマネジメントプロセスは，マネジメント及び意思決定における不可欠な部分であることが望ましい。また，組織の体制，業務活動及びプロセスに組み込まれていることが望ましい。リスクマネジメントプロセスは，戦略，業務活動，プログラム又はプロジェクトの段階で適用することができる。

組織の目的を達成することに合わせ，かつ，適用される外部及び内部の状況に適応するために，組織の中で，リスクマネジメントプロセスが，多数適用されている場合がある。

リスクマネジメントプロセス全体にわたって，人間の行動及び文化がもつ動的で可変的な性質を考慮することが望ましい。

リスクマネジメントプロセスは，しばしば逐次的なものとして表されるが，実務では反復的である。

6.2 コミュニケーション及び協議

コミュニケーション及び協議の意義は，関連するステークホルダが，リスク，意思決定の根拠，及び特定の活動が必要な理由が理解できるように支援することである。コミュニケーションは，リスクに対する意識及び理解の促進を目指す。一方，協議は，意思決定を裏付けるためのフィードバック及び情報の入手を含む。コミュニケーションと協議とを密接に組み合わせることによって，情報の機密性及び完全性，並びに個人のプライバシー権を考慮しながら，事実に基づく，時宜を得た，適切で正確かつ理解可能な情報交換が促進される。

適切な外部及び内部のステークホルダとのコミュニケーション及び協議は，リスクマネジメントプロセスの各段階及び全体で実施することが望ましい。 コミュニケーション及び協議の狙いは，次のとおりである。

– リスクマネジメントプロセスの各段階に関して，異なった領域の専門知識を集める。

– リスク基準を定め，リスクを評価する場合には，異なった見解について適切に考慮することを確実にする。

– リスク監視及び意思決定を促進するために十分な情報を提供する。

– リスクの影響を受ける者たちの間に一体感及び当事者意識を構築する。

6.3 適用範囲，状況及び基準

6.3.1 一般

適用範囲，状況及び基準を確定する意義は，リスクマネジメントプロセスを組織に合わせ，効果的なリスクアセスメント及び適切なリスク対応を可能にすることである。適用範囲，状況及び基準は，プロセスの適用範囲を定め，外部及び内部の状況を理解することを含む。

6.3.2 適用範囲の決定

組織は，リスクマネジメント活動の適用範囲を定めることが望ましい。

リスクマネジメントプロセスは，様々なレベル（例えば，戦略，業務活動，プログラム，プロジェクト又はその他の活動）で適用されるため，検討の対象となる適用範囲，検討の対象となる関連目的，並びにそれらと組織の目的との整合を明確にすることが重要である。

取組み方を計画する際の検討事項は，次を含む。

– 目的，及び下す必要のある決定

– プロセスにおいてとられる対策によって期待される結末

– 時間，場所，個々の包含及び除外

– 適切なリスクアセスメントの手段及び手法

– 必要とされる資源，責任，及び残すべき記録

– 他のプロジェクト，プロセス及び活動との関係

6.3.3 外部及び内部の状況

外部及び内部の状況とは，組織が自らの目的を定め，その目的を達成しようとする状態を取り巻く環境である。

リスクマネジメントプロセスの状況は，組織が業務活動を行う外部及び内部の環境の理解から確定されることが望ましい。また，リスクマネジメントプロセスが適用される活動の個々の環境を反映することが望ましい。

状況の理解は，次に示す理由で重要である。

– リスクマネジメントは，組織の目的及び活動に沿って実施される。

– 組織要因がリスク源になることがある。

– リスクマネジメントプロセスの意義及び範囲が，組織全体の目的と相互に関係していることがある。

– 組織は，5.4.1 に挙げた要因を考慮することによって，リスクマネジメントプロセスの外部及び内部の状況を確立することが望ましい。

6.3.4 リスク基準の決定

組織は，目的に照らして，取ってもよいリスク又は取ってはならないリスクの大きさ及び種類を規定することが望ましい。組織はまた，リスクの重大性を評価し，意思決定プロセスを支援するための基準を決定することが望ましい。リスク基準は，リスクマネジメントの枠組みと整合させ，検討対象になっている活動に特有の意義及び範囲にリスク基準を合わせることが望ましい。リスク基準は，組織の価値観，目的及び資源を反映し，リスクマネジメント方針及び声明と一致していることが望ましい。基準は，組織の義務及びステークホルダの見解を考慮に入れて規定することが望ましい。

リスク基準は，リスクアセスメントプロセスの開始時に確定することが望ましいが，リスク基準は動的であるため，継続的にレビューを行い，必要に応じて修正することが望ましい。

リスク基準を設定するに当たっては，次の事項を考慮することが望ましい。

– 結末及び目的（有形及び無形の両方）に影響を与える不確かさの特質及び種類

– 結果（好ましい結果及び好ましくない結果の両方）及び起こりやすさをどのように定め，また，測定するか。

– 時間に関連する要素

– 測定法の一貫性

– リスクレベルをどのように決定するか。

– 複数のリスクの組合せ及び順序をどのように考慮に入れるか。

– 組織の能力

6.4 リスクアセスメント

6.4.1 一般

リスクアセスメントとは，リスク特定，リスク分析及びリスク評価を網羅するプロセス全体を指す。

リスクアセスメントは，ステークホルダの知識及び見解を生かし，体系的，反復的，協力的に行われることが望ましい。必要に応じて，追加的な調査で補完し，利用可能な最善の情報を使用することが望ましい。

6.4.2 リスク特定

リスク特定の意義は，組織の目的の達成を助ける又は妨害する可能性のあるリスクを発見し，認識し，記述することである。リスクの特定に当たっては，現況に即した，適切で最新の情報が重要である。

組織は，一つ以上の目的に影響するかもしれない不確かさを特定するために，様々な手法を使用することができる。次の要素，及びこれらの要素間の関係を考慮することが望ましい。

– 有形及び無形のリスク源

– 原因及び事象

– 脅威及び機会

– ぜい（脆）弱性及び能力

– 外部及び内部の状況の変化

– 新たに発生するリスクの指標

– 資産及び組織の資源の性質及び価値

– 結果及び結果が目的に与える影響

– 知識の限界及び情報の信頼性

– 時間に関連する要素

– 関与する人の先入観，前提及び信条

組織は，リスク源が組織の管理下にあるか否かを問わず，リスクを特定することが望ましい。様々な有形又は無形の結果をもたらす可能性のある 2 種類以上の結末が存在するかもしれないことを考慮することが望ましい。

6.4.3 リスク分析

リスク分析の意義は，必要に応じてリスクのレベルを含め，リスクの性質及び特徴を理解することである。リスク分析には，不確かさ，リスク源，結果，起こりやすさ，事象，シナリオ，管理策及び管理策の有効性の詳細な検討が含まれる。一つの事象が複数の原因及び結果をもち，複数の目的に影響を与えることがある。 リスク分析は，分析の意義，情報の入手可能性及び信頼性，並びに利用可能な資源に応じて，様々な詳細さ及び複雑さの度合いで行うことができる。分析手法は，周辺状況及び意図する用途に応じて，定性的，定量的，又はそれらを組み合わせたものにすることができる。 リスク分析では，例えば，次の要素を検討することが望ましい。

– 事象の起こりやすさ及び結果

– 結果の性質及び大きさ

– 複雑さ及び結合性

– 時間に関係する要素及び変動性

– 既存の管理策の有効性

– 機微性及び機密レベル

リスク分析は，意見の相違，先入観，リスクの認知及び判断によって影響されることがある。その他の影響としては，使用する情報の質，加えられた前提及び除

外された前提，手法の限界，並びに実行方法が挙げられる。これらの影響を検討し，文書化し，意思決定者に伝達することが望ましい。

非常に不確かな事象は，定量化が困難なことがある。重大な結果をもたらす事象を分析する場合，これは課題になる。このような場合は，一般的に手法の組合せを用いることによって洞察が深まる。

リスク分析は，リスク評価へのインプット，リスク対応の必要性及び方法，並びに最適なリスク対応の戦略及び方法の決定へのインプットを提供する。結果は，選択を行う場合に決定を下すための洞察力を提供する。また，選択肢は，様々な種類及びレベルのリスクを伴う。

6.4.4 リスク評価

リスク評価の意義は，決定を裏付けることである。リスク評価は，どこに追加の行為をとるかを決定するために，リスク分析の結果と確立されたリスク基準との比較を含む。これによって，次の事項の決定がもたらされる。

– 更なる活動は行わない。

– リスク対応の選択肢を検討する。

– リスクをより深く理解するために，更なる分析に着手する。

– 既存の管理策を維持する。

– 目的を再考する。

意思決定では，より広い範囲の状況，並びに外部及び内部のステークホルダにとっての実際の結果及び認知された結果を考慮することが望ましい。

組織の適切なレベルで，リスク評価の結果を記録し，伝達し，更に検証することが望ましい。

6.5 リスク対応

6.5.1 一般　リスク対応の意義は，リスクに対処するための選択肢を選定し，実施することである。

リスク対応には，次の事項の反復的プロセスが含まれる。

– リスク対応の選択肢の策定及び選定

– リスク対応の計画及び実施

– その対応の有効性の評価

– 残留リスクが許容可能かどうかの判断

– 許容できない場合は，更なる対応の実施

6.5.2 リスク対応の選択肢の選定

最適なリスク対応の選択肢の選定には，目的の達成に関して得られる便益と，実施の費用，労力又は不利益との均衡をとることが含まれる。

リスク対応の選択肢は，必ずしも相互に排他的なものではなく，また，全ての周辺状況に適切であるとは限らない。リスク対応の選択肢には，次の事項の一つ以

上が含まれてもよい。

– リスクを生じさせる活動を開始又は継続しないと決定することによってリスクを回避する。

– ある機会を追求するために，リスクを取る又は増加させる。

– リスク源を除去する。

– 起こりやすさを変える。

– 結果を変える。

– （例えば，契約，保険購入によって）リスクを共有する。

– 情報に基づいた意思決定によって，リスクを保有する。

リスク対応の根拠は，単なる経済的な考慮事項より幅広いため，組織の義務，任意のコミットメント及びステークホルダの見解の全てを考慮に入れることが望ましい。リスク対応の選択肢の選定は，組織の目的，リスク基準及び利用可能な資源に基づいて行われることが望ましい。

リスク対応の選択肢を選定する際に，組織は，ステークホルダの価値観，認知及び関与の可能性，並びにステークホルダとのコミュニケーション及び協議に最適な仕方を考慮することが望ましい。有効性は同じでも，ステークホルダによってリスク対応策の受け入れやすさは異なることがある。

慎重に設計し，実施したとしても，リスク対応は予想した結末を生まないかもし

れないし，意図しない結果をもたらすこともある。様々な形態のリスク対応を有効にし，その有効性が維持されることを保証するためには，モニタリング及びレビューをリスク対応実施の一体部分とする必要がある。

リスク対応が，新たにマネジメントを行うことが必要なリスクをもたらす可能性もある。 利用可能なリスク対応の選択肢がない場合，又はリスク対応の選択肢によってリスクが十分に変化しない場合には，そのリスクを記録し，継続的なレビューの対象とすることが望ましい。

意思決定者及びその他のステークホルダは，リスク対応後の残留リスクの性質及び程度を知ることが望ましい。残留リスクは，文書化し，モニタリングし及びレビューし，並びに必要に応じて追加的対応の対象とすることが望ましい。

6.5.3 リスク対応計画の準備及び実施

リスク対応計画の意義は，関与する人々が取決めを理解し，計画に照らして進捗状況をモニタリングできるように，選定した対応選択肢をどのように実施するかを規定することである。対応計画には，リスク対応を実施する順序を明記することが望ましい。

対応計画は，適切なステークホルダと協議の上で，組織の経営計画及びプロセスに統合されることが望ましい。

対応計画で提供される情報には，次の事項を含めることが望ましい。

– 期待される取得便益を含めた，対応選択肢の選定の理由

– 計画の承認及び実施に関してアカウンタビリティ及び責任をもつ人

– 提案された活動

– 不測の事態への対応を含む，必要とされる資源

– パフォーマンスの尺度

– 制約要因

– 必要な報告及びモニタリング

– 活動が実行され，完了することが予想される時期

6.6

モニタリング及びレビュー

モニタリング及びレビューの意義は，プロセスの設計，実施及び結末の質及び効果を保証し，改善することである。責任を明確に定めた上で，リスクマネジメントプロセス及びその結末の継続的モニタリング及び定期的レビューを，リスクマネジメントプロセスの計画的な部分とすることが望ましい。

モニタリング及びレビューは，プロセスの全ての段階で行うことが望ましい。モニタリング及びレビューは，計画，情報の収集及び分析，結果の記録作成，並びにフィードバックの提供を含む。

モニタリング及びレビューの結果が，組織のパフォーマンスマネジメント，測定及び報告活動全体に組み込まれることが望ましい。

6.7 記録作成及び報告

適切な仕組みを通じて，リスクマネジメントプロセス及びその結末を文書化し，報告することが望ましい。記録作成及び報告の狙いは，次のとおりである。

– 組織全体にリスクマネジメント活動及び結末を伝達する。

– 意思決定のための情報を提供する。

– リスクマネジメント活動を改善する。

– リスクマネジメント活動の責任及びアカウンタビリティをもつ人々を含めたステークホルダとのやり取りを補助する。

文書化した情報の作成，保持及び取扱いに関する意思決定に際しては，情報の用途，情報の機微性，並びに外部及び内部の状況を考慮することが望ましいが，考慮する事項はこれらに限らない。

報告は，組織の統治の不可欠な部分であり，ステークホルダとの会話の質を高め，トップマネジメント及び監督機関が責任を果たすことができるように支援することが望ましい。報告に当たって考慮すべき要素には，次の事項が含まれる。ただし，これらに限らない。

– 様々なステークホルダ，並びにそれらのステークホルダに特有の情報の必要性及び要求事項

– 報告の費用，頻度及び適時性

– 報告の方法

– 情報と組織の目的及び意思決定との関連性