第 51 章　ソフトウェア開発に関わるリスク管理

なぜ「リスク管理」が必要か

我々の日常の生活には、多くの「リスク」がある。例えば、思いがけずに病気になるかもしれない。急に失業して、収入がなくなるかもしれない。車を運転していて、事故を起こすかもしれない。これらのリスクについては、日本では国が保険制度を用意し、法律で該当する国民の加入が義務づけられている。

しかし国が保険制度を用意しているリスクは、ごく限られたものである。家の火災については損害保険会社が火災保険を用意し、突然の死亡に対しては生命保険会社が生命保険を用意していて、我々は火災や死亡に対応するために必要に応じてそれらの保険に加入する。これらは、国が用意した保険ではない。

また全てのリスクに、既に保険が用意されている訳でもない。例えば情報システムの開発プロジェクトは、よく予算超過や納期遅延を引き起こす。これらは、潜在的に存在しているリスクの一部が不幸にも顕在化したものである。このようなソフトウェア開発プロジェクトのリスクには、今のところ対応する保険は用意されていない。

このようなリスクに対応するために、「リスク管理」がある。「リスク管理」を適用することによって、発生するリスクを消滅させる、あるいは発生しても影響を軽減することができる。

「日本人は、リスク管理が下手である」といわれる。ここではソフトウェア開発プロジェクトのリスクに限定して、それらのリスクへの対応方法を考える。

リスク管理に関わる ISO の 2 つの規格

ISO は、リスク管理について以下の 2 つの規格を持っている。

- ISO／IEC 16085：2006（JIS X 0162：2008）「システム及びソフトウェア技術－ライフサイクルプロセス－リスク管理」[JIS08d]
- ISO 31000:2009（JIS Q 31000:2010）「リスクマネジメント－原則及び指針」[JIS10c]

ISO／IEC 16085：2006（JIS X 0162：2008）はソフトウェアのライフ・プロセスに関わる規格（ISO／IEC 12207：2008（JIS X 0160-2012））と整合性を持ち、ISO／IEC 12207（および「共通フレーム 2013」[1]）に基づいてソフトウェアを開発しようとする時に、リスク管理にこの規格を適用する目的で作られた[JIS08d]。

一方の ISO 31000：2009（JIS Q 31000：2010）は IEC が規格の検討や制定に関わりを持っていないことからも明らかなように、ソフトウェア開発に限定したものではない。もっと一般の、組織を経営し、運営する活動全般にリスク管理を適用する時に使用する目的で作られた[JIS10c]。

このことからすれば、この原稿は ISO／IEC 16085：2006（JIS X 0162：2008）を取り上げるべきかもしれない。しかしこの原稿では、ISO 31000：2009（JIS Q 31000：2010）を取り上げてリスク管理について議論したい。

理由は、2 つある。前述したようにこの規格は「リスク管理を特別の活動としてではなく、組織の経営や運営での通常の活動として位置づけし、日常の業務として実施する」というスタンスを取っている。1 つ目の理由は、このスタンスに賛成したことである。これは、PMBOK によるプロジェクト管理で、品質マネジメントをプロジェクトに限定した活動として位置づけ

[1] ISO/IEC 12207 と「共通フレーム 2013」については、第 12 章で議論した。

るのではなく、母体の品質向上活動と連動する形でプロジェクトの品質マネジメントを位置づけた考え方と共通するものである[2]。つまり、母体の日常のリスク管理の一環として、プロジェクトのリスク管理も捉えたいと考える。ソフトウェアの開発プロジェクトが立ち上がったから、普段行っていないリスク管理をそのプロジェクトでは実施する、ということではうまく行くはずがないからである。

2 つ目は、この規格では PDCA サイクルを二重に回して、リスク管理のプロセスの改善を実現しようとしていることである。このスタンスに、たいへんに好感を持つことができる。

さらにこの規格には、関連する 2 つの ISO の規格がある。それは、以下のものである。

- IEC／ＩSO 31010：2009（JIS Q 31010：2012）「リスクマネジメントーリスクアセスメント技法」
- ISO Guide 73：2009（JIS Q 0073：2010）「リスクマネジメントー用語」

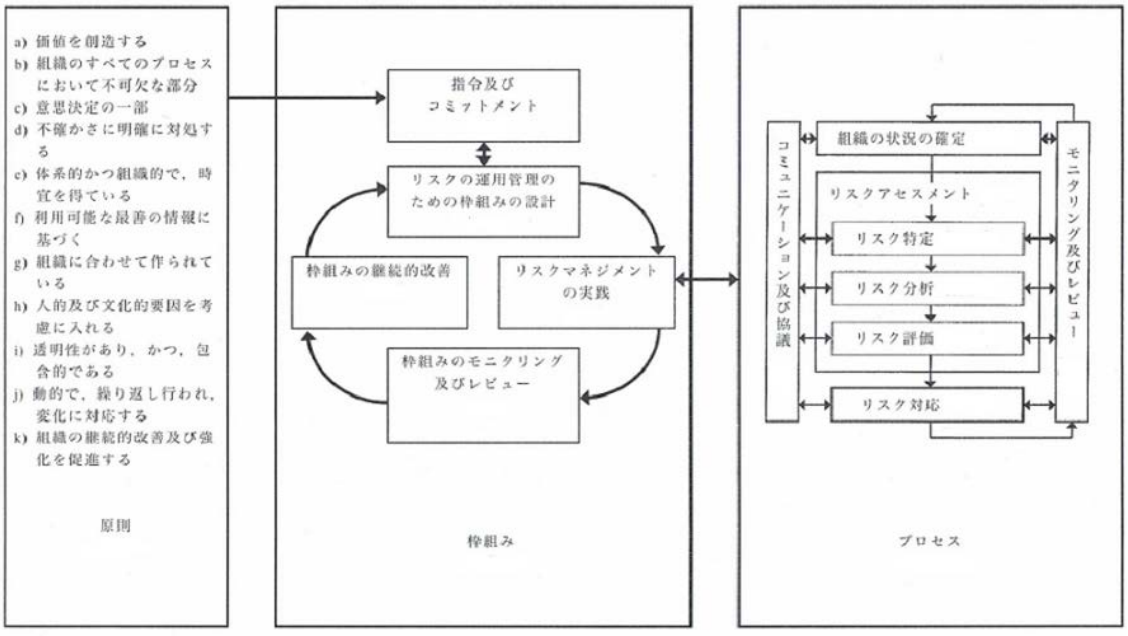
このことは、ISO がこれらの規格を通してリスク管理にたいへん力を入れていることを示している。

「原則」

この規格の考え方と方法を表現したものを、図表 51-1 に示す。

図表 51-1 から明らかなように、この規格は大きく 3 つの部分から構成されている。「原則」と「枠組み」、および「プロセス」である。

「原則」とは、この規格を適用しようとしている組織がどのようなスタンスや考え方でリスク管理を行うべきかを示したものである。図表 51-1 では、左側の枠の中に記載されている。この「原則」では、次の前置きに続いて、以下の 11 項目が明記されている。[JIS10c]



図表 51-1　リスク管理の原則、枠組みとプロセスの関係（[JIS10c]より）

[2] PMBOK については、第 50 章で記した。

「リスク・マネジメントを効果的なものにするために，組織は，次の原則をすべての階層で順守することが望ましい。」

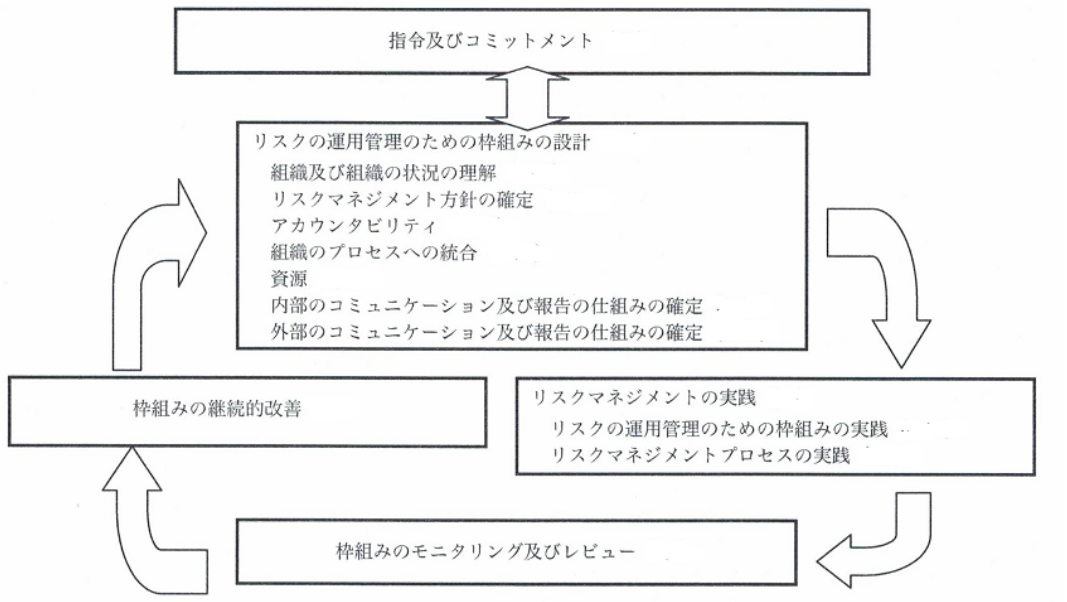
- リスク・マネジメントは，価値を創造し，保護する。
- リスク・マネジメントは，組織のすべてのプロセスにおいて不可欠な部分である。
- リスク・マネジメントは，意思決定の一部である。
- リスク・マネジメントは，不確かさに明確に対処する。
- リスク・マネジメントは，体系的かつ組織的で，時宜を得たものである。
- リスク・マネジメントは，最も利用可能な情報に基づくものである。
- リスク・マネジメントは，組織に合わせて作られる。
- リスク・マネジメントは，人的及び文化的要素を考慮に入れる。
- リスク・マネジメントは，透明性があり，かつ，包含的である。
- リスク・マネジメントは，動的で，繰り返し行われ，変化に対応する。
- リスク・マネジメントは，組織の継続的改善を促進する。

この「原則」を受けて、次の「枠組み」がある。

「枠組み」

リスク・マネジメントを独立した独自のマネジメント・システムとするのではなく、既に組織に組み込まれて稼働し、効果を上げているマネジメント・システムに付加されるのが良い。枠組みには、次の 5 つの要素がある[JIS10c]。

- 指令およびコミットメント
- リスクの運用管理のための枠組みの設計
- リスク・マネジメントの実践
- 枠組みのモニタリングおよびレビュー
- 枠組みの継続的改善



図表 51-2　リスク管理の運用のための枠組みの構成要素間の関係（[JIS10c]より）

指令およびコミットメントは、次に述べる PDCA サイクル全体へのトップ・マネジメントの関わり方を示している。後の 4 つの要素は、PDCA サイクルのそれぞれのフェーズに該当する。

図表 51-2 に、リスク管理の運用のための枠組みの構成要素間の関係を示す。

指令およびコミットメント

リスク管理を組織に定着させ、効果的に実施するために、トップ・マネジメントの強力、かつ持続的な働きかけが必要である。

既に述べた「原則」を受けて、トップ・マネジメントは次の事項などを実施するのが望ましい[JIS10c]。

- リスク・マネジメント方針を定め，是認する。
- 組織の文化とリスク・マネジメント方針とが整合することを確実にする。
- 組織のパフォーマンス指標と整合するリスク・マネジメントのパフォーマンス指標を決定する。
- リスク・マネジメントの目的を，組織の目的及び戦略と整合させる。
- 法律及び規制を順守することを確実にする。
- アカウンタビリティ及び責任を，組織内の適切な階層に割り当てる。
- 必要な資源がリスク・マネジメントに配分されることを確実にする。
- すべてのステークホルダーにリスク・マネジメントの便益を伝達する。
- リスクの運用管理のための枠組みが常に適切な状態であり続けることを確実にする。

リスクの運用管理のための枠組みの設計

図表 51-2 には、ここで行うべき事項として次の 7 項目が挙げられている[JIS10c]。

- 組織及び組織の状況の理解
- リスク・マネジメント方針の確定
- アカウンタビリティ
- 組織のプロセスへの統合
- 資源
- 内部のコミュニケーション及び報告の仕組みの確定
- 外部のコミュニケーション及び報告の仕組みの確定

最初の時は、これらを全て行わなければならない。しかし 2 回目以降は、前回の結果を受けて修正／変更するべきところだけに対応すれば良い。

なおこのフェーズは、PDCA サイクルの P（計画）のフェーズに当たる。

リスク・マネジメントの実践

次の「プロセス」で述べる「リスク・マネジメントのプロセス」を、全ての組織で実施する。後述するようにこのプロセスも PDCA サイクルを回す形になっており、こちらの PDCA サイクルの「リスク対応」の部分は全ての部門で日常業務の一部として実施されることになる。

このフェーズは、PDCA サイクルの D（実行）のフェーズに当たる。

枠組みのモニタリングおよびレビュー

このモニタリングは適宜行う必要があるが、レビューは特別の問題がなければ年に一度程度、時期を決めて実施するので良い。ここでは計画段階で考えたことが適切に実施されているかをチェックすることが目的である。

このフェーズは、PDCA サイクルの C（チェック）のフェーズに当たる。

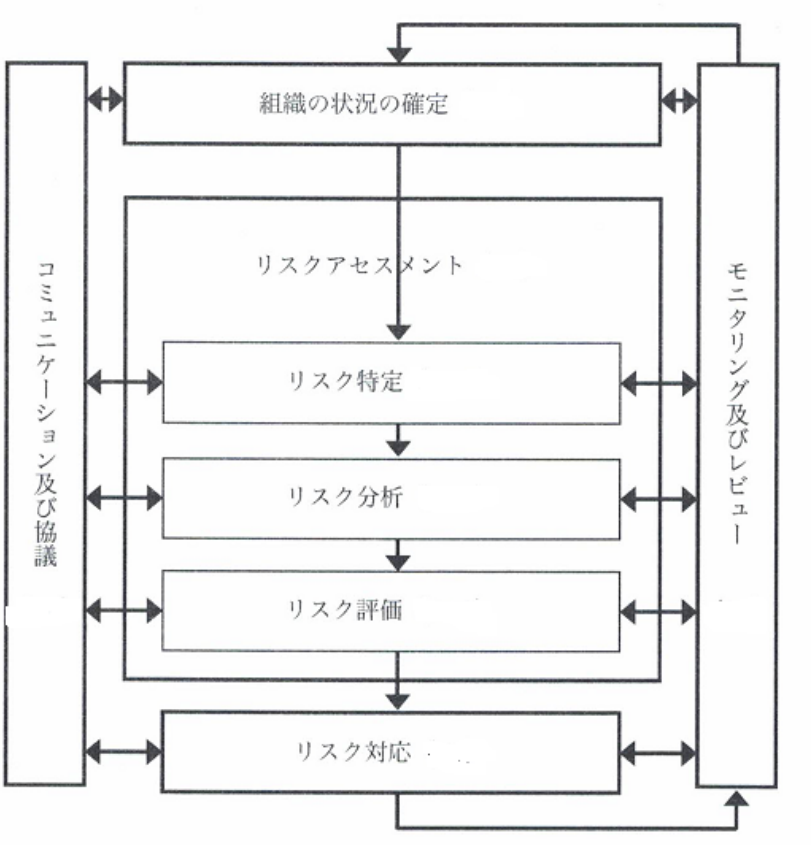
枠組みの継続的改善

モニタリングとレビューの結果何かうまくないことが見つかれば、そのうまくないことがなぜ、どのようにして起きたのかを明確にし、同じ状況が起きても再びそのうまくないことが発生しないように手順を変える。これによって、この「枠組み」のプロセスが継続的に改善されることになる。

このフェーズは、PDCA サイクルの A（アクション）のフェーズに当たる。

「プロセス」

「プロセス」は既に述べた外側の PDCA サイクルの D（実行）の部分に当たり、図表 51-3 に示すようにこれ自身が小さな 1 つの PDCA サイクルを構成している。このサイクルには、次のフェーズがある[JIS10c]。



図表 51-3　リスクマネジメントプロセス（[JIS10c]より）

- コミュニケーション及び協議

- 組織の状況の確定
- リスクアセスメント
  - リスク特定
  - リスク分析
  - リスク評価
- リスク対応
- モニタリング及びレビュー

ISO の規格は、この「プロセス」そのものが、以下の状態であることが望ましいとしている[JIS10c]。

- 組織の運用管理に不可欠な部分として、組織の文化及び実務の中に組み込まれている。
- 組織の事業プロセスに合わせて作られている。

以下で、このサイクルの各フェーズについて議論する。

コミュニケーション及び協議

ここでの「コミュニケーションと協議」は内外のステークホルダーとの間で、リスク・マネジメントのあらゆる側面で実施される。

ここでは、以下のようなものが取り扱われる[JIS10c]。

- リスクを適切に特定することを確実にすることを援助する。
- リスクを分析するために，異なった領域の専門知識を集めてくる。
- 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。
- 対応計画への是認及び支援を確保する。
- リスクマネジメントプロセス実践中に，適切な変更管理を強化する。

組織の状況の確定

この PDCA サイクルの P（計画）の最初に、「組織の状況の確定」がある。

この組織の状況の確定は、次の事項から構成される [JIS10c] 。

- 外部状況の確定
- 内部状況の確定
- リスクマネジメントプロセスの状況の確定
- リスク基準の決定

最初にこの作業を行う時は、全部が実施の対象になる。しかし 2 回目以降は、前回に確定した内容の見直しから始めるので良い。

リスクアセスメント

次の 3 つの作業を、「リスクアセスメント」と呼ぶ。

- リスク特定
- リスク分析
- リスク評価

これもまだ、P（計画）作業の一部である。

なおこのリスクアセスメントの詳細な実施方法などについて、ISO は別の規格を用意してい

る[JIS12c]。

リスク特定

今リスク管理で対象としている領域にどんなリスクがあるのかをリストアップする作業を、「リスクの特定」と呼ぶ。

ここでは、できるだけ漏れなくリスクをリストアップすることが重要である。従って 2 回目以降にこの作業を行う時には、前回のリスク特定で漏れがなかったかという立場で見直すことが重要である[JIS10c]。

なおリスクの中に「本来なら行うべき作業を行わない」ことで発生するリスクがあれば、それも漏らさないように含める必要がある。

リスク分析

「リスク特定」でリストアップしたリスクを、次の 2 つに区分するために「リスク分析」を行う。

- そのリスクは起こりやすさと起きた時の影響から、充分に監視する必要がある（優先順位が高い）。
- そのリスクはとりあえず監視の対象から外しても良い（優先順位が低い）。

特定されたリスクの数が少なく、その全てを次の「リスク評価」と「リスク対応」の対象にできるのであれば、この「リスク分析」を行う必要はない。特定されたリスク全てを、評価と対応の対象にすれば良い。リスクの数が多くてその全てに対応しきれない時に、対応の対象にするリスクを選ぶことが、ここでの「リスク分析」の目的である。

リスクの分析は普通、「発生確率」と「予想される被害」を掛けて、その数値の大きなものから次のリスク評価の対象にするという方法をとる [3]。しかしこれが唯一無二の方法という訳ではない。何らかの方法でリストアップしたリスクを、前記の 2 つの区分に分けられれば良い。

リスク評価

リスク分析の結果得られた「優先順位の高い」リスクについて、そのリスクが顕在化した時にどう対応するかを決める。

ここでは「リスク評価」の方法として、次の手順が 1 つの参考になる[JIS12c]。

- リスク対応の必要の有無を判断する。
- 対応への優先順位を決める。
- 行動の必要性の有無を明確にする。
- 幾つかある選択肢から選択する。

優先順位が高いリスクについては、全てに対応することが望ましい。しかし、必ずそうしないとならないという訳ではない。対応することが望ましいけれど、対応に著しい困難を伴う／費用がかかるというようなものがあれば､そのリスクに対応することをとりあえずあきらめて、「残存リスク」として別途管理するのが良い。残存リスクは毎回 PDCA サイクルを回す時に見直しの対象にして、リスクが解消していないか、あるいは技術進歩などで対応が行えるように

[3] ここでは、発生確率は無限小になり、予想される損害が無限大になる、というような評価になることがある。この場合には、「無限小の発生確率」と「無限大の損害」の掛け算というナンセンスな作業になりかねないので、そうならないよう注意が必要である。

なっているか、などをチェックするのが良い。

リスク対応

リスクアセスメントの結果対応が必要と判断されたリスクについて、定期的に、必要があれば毎日「そのリスクが発生していないか／発生しそうにないか」をチェックし、発生した、あるいは発生しそうであると判断された時に、「リスク評価」で決めた対応手順を実施する。

これは PDCA サイクルの D（実行）に相当する。

モニタリング及びレビュー

「モニタリングおよびレビュー」では、次の事項に対応する[JIS10c]。

- リスクアセスメントを改善するための更なる情報を入手する。
- 事象（ニアミスを含む。），変化，傾向，成功例及び失敗例を分析し，そこから教訓を学ぶ。
- リスク基準，並びにリスク対応及びリスクの優先順位の見直しを必要とすることがあるリスク自体の変化を含む，外部及び内部の状況の変化を検出する。
- 新たに発生しているリスクを特定する。

これは、PDCA サイクルの C（チェック）と A（アクション）に相当する。

このフェーズの後、2 回目以降の「組織の状況の確定」を実施する。

なおこの PDCA サイクルは、適宜回すのが良い。プロジェクトに適用するのであれば、プロジェクトのフェーズごとに対応するのが良い。

リスクマネジメントプロセスの記録作成

図表 51-3 の図には含まれていないが、このリスク・マネジメントのプロセスについて記録を作成するのが良い[JIS10c]。この記録によって、リスク管理のプロセスを改善することが可能になるからである。

キィワード

リスク管理、PDCA サイクル、リスク特定、リスク分析、リスク評価、残存リスク

規格

ISO 31000：2009、JIS Q 31000：2010、IEC／ISO 31010：2009、JIS Q 31010：2012、ISO Guide 73：2009、JIS Q 0073：2010

参考文献とリンク先

[JIS08d] 日本工業標準調査会審議、「システム及びソフトウェア技術－ライフサイクルプロセス－リスク管理 JIS X 0162：2008（ISO/IEC 16085：2006)」、日本規格協会、平成 20 年.

[JIS10c] 日本工業標準調査会審議、「リスクマネジメント－原則及び指針 JIS Q 31000：2010（ISO 31000：2009)」、日本規格協会、平成 22 年.

[JIS10d] 日本工業標準調査会審議、「リスクマネジメント－用語 JIS Q 0073：2010（ISO Guide 73：2009)」、日本規格協会、平成 22 年.

[JIS12c] 日本工業標準調査会審議、「リスクマネジメント－リスクアセスメント技法 JIS Q

31010：2012（IEC/ISO 31010：2009）」、日本規格協会、平成 24 年.

（2016 年（平成 28 年）11 月 10 日　新規作成）