リスクマネジメントと RMO
～RMO の役割と活用例～

I はじめに

昨今、震災や水害などの自然災害だけでなく、事件・事故・システム障害など不測の事態に対応するため、各企業はリスクマネジメントが強く求められている状況にある。一言でリスクマネジメントといっても、事業継続マネジメントシステム(ISO 22301)、情報セキュリティマネジメントシステム（ISO/IEC 27001）や PMBOK といったように、リスクマネジメントに関連するフレームワークは数多く存在している。一方、ITIL®においてもライフサイクルの様々な段階、プロセスでリスクマネジメントが必要とされているが、具体的な活動は十分に記載されているとはいえない。そこで、2013 年 4 月にリスクマネジメント研究分科会を設立し、リスクマネジメントを効率的に実施するために必要な、具体的な管理手法や手順を研究することとした。

研究成果は第 10 回、第 11 回の *it*SMF Japan コンファレンスを通じて発表してきたが、この度、活動期間を終えるにあたり、研究成果の集大成を本ホワイトペーパーとして発行することにより、効果的／効率的なリスクマネジメントを実践するためのヒントを紹介する。

II リスクとは何か？

リスクは、業務内容や立場により様々であり、災害・事故・政治・経済・社会・経営・情報・プロジェクトなど多岐にわたる。リスクの特徴は以下の通りである。

・目的／目標に対する不確実性であり、目的／目標が変われば、不確実性もまた変わる。
・リスクとは、まだ顕在化していない事象である。（顕在化したらインシデントとなる）
・リスクとは、目的を阻害する外部要因／内部要因であり、問題・既知エラーとは異なる。

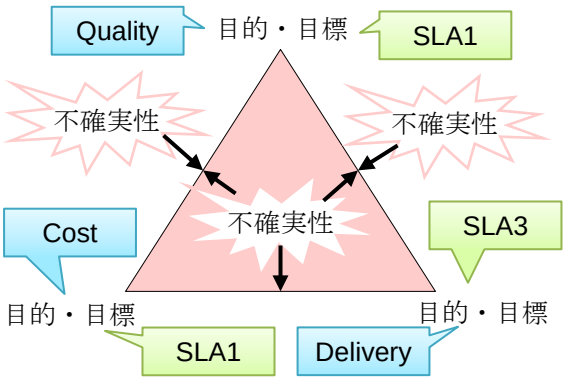

図 1 目的・目標により変わる不確実性

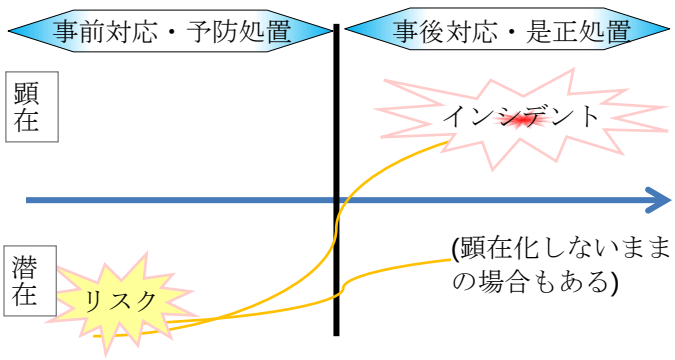

図 2 リスクとインシデント

多くの方は、顕在化すると目的・目標に対して悪影響を与える事象をリスクとして認知しているであろう。これは脅威のリスクとして分類されるが、リスクには中立や好機のリスクも存在する。中立のリスクとは顕在化しても目的・目標に対して影響を及ぼさない事象、好機のリスクとは顕在化により目標・目的に対して好影響を与える事象のことである。

本研究では 3 種のリスクが存在することを理解しつつも、多くの方が認知している脅威のリスクにフォーカスしている。あらかじめご承知おきいただきたい。

III リスクマネジメントとは何か？

リスクマネジメントに関するフレームワークは数多く存在するが、共通して言えることは、リスクマネジメントとは、目的・目標に対する不確実性を洗い出し（リスクの洗い出し）、その起こり易さと影響をコントロールする（リスクのコントロール）プロセスである、ということである。

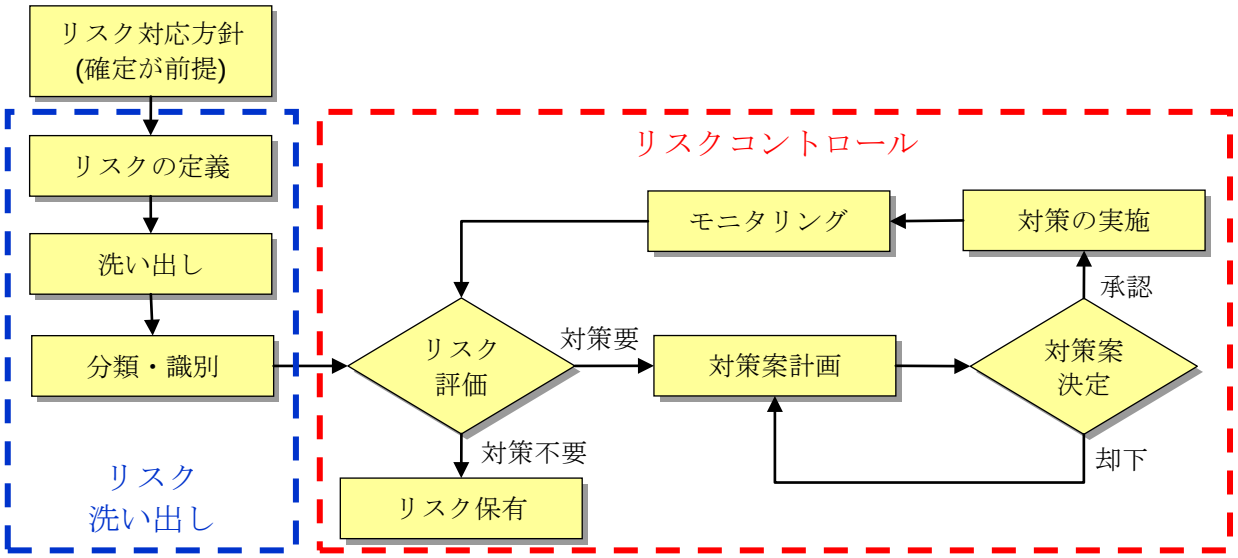

図 3　リスクマネジメントプロセス

1　リスクを洗い出す活動

リスクを洗い出す活動には、「リスクの定義」「洗い出し」「分類・識別」の工程が該当する。本項では、各工程のタスクと考慮点について説明していく。

1)　リスクの定義

ここでは、目的・目標を明確化することにより、何に対する不確実性をリスクとするかを定義する。

リスクは立場や職務によって捉え方が様々であるため、リスクを定義することにより洗い出されたリスクの妥当性を高めることができ、評価も容易となる。

2)　洗い出し

ここでは、定義した目的・目標に対するリスクを洗い出す。洗い出すにあたっては、対応する要員がリスクの定義を十分に理解しておけるよう、必要に応じて教育等も実施する。また、専門知識が求められる場合には、組織内外を問わず、有識者からの支援も得つつ実施していく。

3)　分類・識別

ここでは、洗い出されたリスクに対し、顕在化した場合にどのような影響があるかを明確化する。

2　リスクをコントロールする活動

リスクをコントロールする活動には、「リスク評価」「対策案計画」「対策案決定」「対策の実施」「モニタリング」の工程が該当し、各工程はPDCAサイクルと関連付けることができる。ここで注目すべきは「Plan」ではなく「Check」より工程が開始されることである。

本項では、各工程のタスクと考慮点について説明していく。

表 1　PDCAサイクルとの関連付け

プロセス	リスク評価		対策案計画 対策案決定	対策の実施 モニタリング
PDCA サイクル	Check	Action	Plan	Do

1)　リスク評価

(1)　リスク対応の方針および優先度付け

ここでは、企業の経営方針やビジネス上の重要事項を踏まえた上で、それぞれのリスクへの対応方針を決定する。その際、リスクが顕在化した際の影響 等を考慮する。

(2)　リスク対応の選択肢選定

ここでは、企業の経営方針やビジネス上の重要事項を踏まえた上で、それぞれのリスク対応の選択肢を選定する。旧 ISMS 規格(ISO/IEC 27001:2005)では 4 種の選択肢だったが、ISO 31000：2009 では 7 種の選択肢が存在する。

表 2　リスク対応選択肢

旧 ISMS 規格	ISO 31000 のリスク対応の選択肢
リスク低減	起こりやすさを変える(change the likelihood)
	結果を変える(change the consequence)
リスク受容	リスク保有(retain)
リスク移転	リスク共有(share)
リスク回避	リスク回避(avoid)
	リスク源の除去(remove)
-	リスクを取る(take)ことによる機会追求

(3)　リスク対策案の作成指示

ここでは、関連する組織に対し、選定したリスク対応の選択肢に基づいたリスク対策案の作成を指示する。

(4)　リスク対策実施後の再評価

ここでは、リスク対策を実施したことにより変化したリスクの再評価を実施する。再評価結果は経営層へ報告し、再評価結果の合意形成を図る。したがって、本タスクは 2 サイクル目以降のタスクとなる。

2)　対策案計画

(1)　リスク対応計画の作成

ここでは、選定された選択肢に基づき、具体的なリスク対策計画案を作成する。

3)　対策案決定

(1)　リスク対応計画のレビュー

ここでは、作成したリスク対応計画についてのレビューを実施する。その際、リスクが顕在化した場合のコストと対応コストを比較し、費用対効果が得られる計画であることを確認する。レビューでの承認を持って対応計画の決定となる。

(2)　関係者調整

ここでは、決定したリスク対応計画にて対策が複数組織に関連する場合、組織間での調整を実施する。また、稟議が必要な場合、稟議の起案も実施する。

4)　対策の実施

(1)　対策実施の指示

ここでは、決定したリスク対応計画について、関係組織も含めて実施する旨を指示する。

5)　モニタリング

(1)　対策実施状況の点検

ここでは、リスク対応の進捗状況について点検を実施し、計画通りに対応されていることを確認する。

(2)　対策の有効性測定

ここでは、実施した対策が当初の見込み通りに機能しているか等、対策の有効性を測定する。

(3)　モニタリング結果の報告

ここでは、リスク対応の進捗状況および有効性測定結果を経営層へ報告するとともに、計画を作成した組織へフィードバックする。

以上の通り、リスクマネジメントの活動には多くの工程が存在するが、適切かつ確実に実施していくためには様々な課題も存在する。次章では、各工程での課題と解決策について説明していく。

IV リスクマネジメントの課題と解決策

1. リスクマネジメントの課題

リスクの種類が業務内容や立場により様々であることは、II 章で記載した通りである。そのため、実際の職場の当事者間のみで意識を合わせるだけでは、リスクの洗い出しやリスクマネジメントの活動が偏る傾向があり、適切な導入は難航すると思われる。

分科会では、多種・多様なリスクに対するマネジメントを適切に行うために、どのような課題が存在するのかを検討した。当分科会メンバーが、経営層から現場担当者までの職種が網羅されており、また業種も多岐にわたっていたため、それぞれの視点で課題を精査することによって、53 件の課題を得ることができた。その結果、以下に示す通り、洗い出し・コントロールのどちらの活動においても「人材」「組織」に対する課題が多く、これらの解決なくしてリスクマネジメントを推進することは不可能であると判断した。

表 3 リスクマネジメントに対する課題

分類	説明	課題数	
		洗い出し	コントロール
人材	スキルセットや理解度、モチベーションに依存する課題	11	9
組織	活動範囲および権限、視点の違いに依存する課題	10	10
費用	活動に必要となる費用負担に依存する課題	1	6
時間	活動に必要となる工数に依存する課題	3	3

1) 人材に関する課題

(1) リスクやリスクマネジメントに対するスキル（知識・経験）がない
(2) リスクに対する理解度は低い（ない）
(3) ビジネス全体に対しての観点（意識）が低い
(4) 上司は指示するだけ、部下だけが忙しく、モチベーションが下がる
(5) 身近なリスクには対応できるが、ビジネス全体でのリスクがわからない

人材に関する課題の多くは、リスクマネジメントに対するスキル（知識・経験）や、理解の不足が原因となるものである。リスクを洗い出すための考え方や手法でつまずくため、リスクマネジメントの導入部である、リスク洗い出しの段階で必要な項目を見落としやたり、影響範囲、優先度を過小（過大）評価してしまうことである。

リスクのコントロールにおいては、対応方法の誤りや、対応不足のみでなく、現場担当者とマネジメント部門の目的の共有や説明、対応結果の評価をすることも必要である。

2)組織に関する課題

(1) 役割・権限・責任等が不明確となっている
(2) 基準が不明確なため、リスクと認識されない
(3) エスカレーションルール不在、隠蔽・隠匿するカルチャがある
(4) 立場や職務によって、リスクは異なる
(5) リスクの共有ができていない

組織に関する課題は、リスクマネジメント体制におけるプロセス（手順）の規定化や、承認や確認の権限が不明確なことから、コントロール活動を適切に運用することができないことなどが挙げられる。

業務や役職毎に課題が異なることを理解し、各部署間、各担当者間でリスクを相互に認識し、それを共有できる組織文化を醸成することも必要である。

3)費用に関する課題

(1) リスクマネジメントの費用（予算）がない
(2) 投資効果が見えない（見えにくい）
(3) 業務には関係ない費用がかかる
(4) 実際に使用されないものに費用をかけられない

費用に関する課題は、具体的なリスク管理の費用（予算）の不足や、リスクマネジメントの必要性や対応費用の妥当性が説明できないなどの人材に関する課題から発生するものが挙げられる。
セキュリティ対策と同様に、事象として発生していないものに対して、本業以外の費用負担をしたくないという意識がマネジメント部門や実務担当者の双方にみられる。
導入段階でのマネジメント部門、実務担当者双方への理解と、リスクアセスメントによる明確な費用対効果の提示が必要である。

4)時間に関する課題

(1) 業務が忙しくリスクマネジメントをする時間がない
(2) リスクアセスメントに対して十分な時間を確保していない
(3) 改善するプロセス（PDCA）を維持する時間がない
(4) 社会情勢・業界動向・新技術など、常に新しいリスクが生まれている

リスクマネジメントの専任者を用意できる環境でない限り、リスクマネジメントに割ける時間が限られる。その限られた時間でリスクマネジメントを推進する場合、顕在化したリスクへの対応が優先され、サービスの継続的な改善に割ける時間の不足による、サービスの低下、予防への未対応が考えられる。
特に、昨今の急速な情報社会の拡充や国際化を考慮すると、予防のためのリスクアセスメントやPDCAによる継続的なサービス向上のために時間を確保することが必要である。

2 課題に対する解決策

いろいろな課題があるが、分科会としてはRMOを設置することを解決策として提言する。
・まずは、リスクマネージャを専任者として設置する
・その配下にリスクマネジメントを推進する組織RMO（Risk Management Office）を設置する
・RMO、リスクマネージャを中心に各部門がリスクマネジメントを実施する
IV章1項の課題に対するアプローチについて以下に述べる。

1)人材に関する課題へのアプローチ

リスクマネジメントでは、ビジネスリスク、品質リスク、セキュリティリスク他いろいろなリスクへの知識が必要になる。また、リスクが発生し対策をとる際、深い知識が必要となる場合もあり、必要により外部の専門知識を有する者を活用することができる必要がある。そういったことが可能となる人材の育成や、リスクマネジメントの体制を整備することからはじめる。
また、リスクに対する意識を向上させるためにも、全社的な教育・訓練を定期的に実施して、業務にはリスクが伴うものであることを理解させる必要がある。

2)組織に関する課題へのアプローチ

リスクに対する知識が得られたら、人的な体制だけでなくリスクに対するプロセスを規定し、マネジメントする態勢を整備することである。経営層と現場の意識を埋めるためにも、洗い出されたリスクを情報共有し、解決した成果を実感できる態勢にすることでリスクへの意識向上が望まれる。その中心的な役割となるのがリスクマネージャであり、リスクマネージャのもと、推進する組織がRMOと考える。このような体制が機能し、継続的な改善プロセスが運用できれば、リスクマネジメントの成熟度が高まる。

3)費用に関する課題へのアプローチ

人的対策や組織的な対策を実施するためには費用がかかることを経営層が認識し、リスクが発生してからの対策費用と予防に向けたリスクマネジメントにかける費用のどちらが低くなるかを理解して、年間単位で必要な費用を予算計上する。それぞれの部署から予算計上された時、どれを優先すべきかの判断が必要となる。声が大きい組織に予算が集中してしまって、本来優先すべき組織に予算がわりあてら

ないような状態にならないように、リスクマネージャはリスクやコストから何を優先するか客観的に判断して経営層が判断する際に適切にフォローすることが必要である。

4)時間に関する課題へのアプローチ

時間がないのではなく時間を作ること、即ちリスクマネジメントを軽視することなく専任者を確保することで、場当たり的に対応するのではなく、継続的にリスク対応を図ることが必要である。現在、リスクがなくても潜在的なリスクがあることを理解し、社会情勢・業界動向・新技術など、常に新しいリスクが生まれることを想定して、プロアクティブな対応を図ることが必要である。

この章では、リスクマネジメントの課題を大きく人材、組織、費用、時間の4つに分け、それらの課題を解決するためのアプローチ手法について述べた。
次章では、これらについてより具体的なケースを挙げ、そのコントロール方法について説明していく。

Ⅴ ケースによる説明

上記「2. 課題に対する解決策」のポイントをケースに照らし合わせ説明する。なお、今回は当分科会でモデルケースを作成し、議論を行った。

アイテル商事の概要（会社概要）
会社名：アイテル商事株式会社
本社所在地：東京都内
事業内容：文房具、日用雑貨品等の卸売業
売上高：100億円
従業員数：380人
IT投資額：5億円
拠点：5ヶ所（都内本社、北関東支社、南関東支社、大阪営業所、仙台営業所）
重要顧客：首都圏内の大手・中堅スーパー

モデルケース

1 人材に関する課題

1) 外部情報の採用

組織では、様々なリスクに対する専門知識を保有しているスタッフが存在しているわけではない。
必要に応じ、外部情報などを適宜に取り込む必要がある。
業務担当は、発生頻度の少ないリスクへの情報収集は、おろそかになってしまいがちである。
RMOは業務担当と違い、リスク対応に有意義な情報を、広く浅く情報収集し、必要に応じて業務担当にアドバイスすることができる。

「図 4 RMOにおける外部情報アドバイス」はリスクコントロールにおける対策案検討のRMO活動をあらわしている。

仙台営業所において電力供給リスクに対し、自家発電機導入と対策が検討されている。本社情報システム部リスク担当および仙台営業所リスク担当において、自家発電機導入における計画が立案された。

RMOはその計画に対し外部情報を活用し適宜有益なアドバイスを行う。かつ、その進行状況を経営層リスク責任者に報告することにより、リスク対処における的確なコントロールを行える。

図 4 RMOにおける外部情報アドバイス

2) 全社的な教育

リスクの様々な管理には、リスク管理特有の考え方やプロセスなどが必要になる。また、組織に適合したリスク管理の場合、組織特有の考え方も盛り込まれ、外的要因の変化や組織の成長具合などにより、適宜改善されることになる。

RMOは、それら特有のプロセスや考え方、また適宜改善変更される考え方を統括管理し、リスク管理実施のメンバーに教育・展開する必要がある。

「図 5 RMOによる教育」は、RMOがリスク管理担当部門の立ち上げ支援を行うことあらわしている。

RMOは、新設された営業所・事業所のリスク担当者に対し、自社のリスク管理プロセスをレクチャーし、実施可能な状態への支援を行うこととなる。

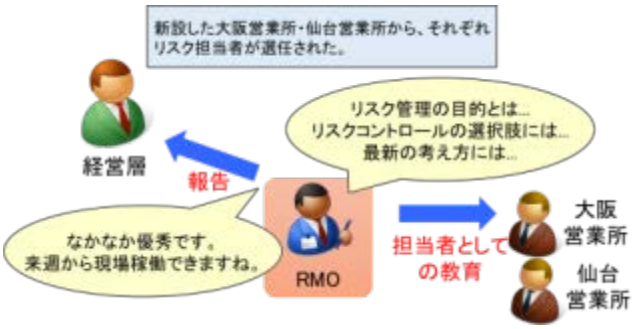

図 5 RMOによる教育

2. 組織に関する課題

1) 組織の意識共有

リスクは目的／目標に対する不確実性であり、目的／目標が変わればリスクの捉え方も変わってくる。役割や責任が細分化されるような組織では、立場・階層によってリスクの捉え方が変わってくる。

RMOは、階層間によるリスクの捉え方や視点を把握し、リスク管理におけるスムーズな意思決定を図れるように説明をする責任がある。

「図 6 組織におけるリスクの捉え方」は、営業所・事業所の新設に伴う階層別で考えるリスクの違いを例としてあらわしている。

各現場担当やマネージャは、各自の業務責任の下リスク管理を実施するが、経営層としては「採算」や「時間」に捉われすぎることにより、本来の経営リスクを招いてしまう場合がある。

RMOは、経営リスクを詳細化する形で、組織にリスク管理を説明する必要がある。

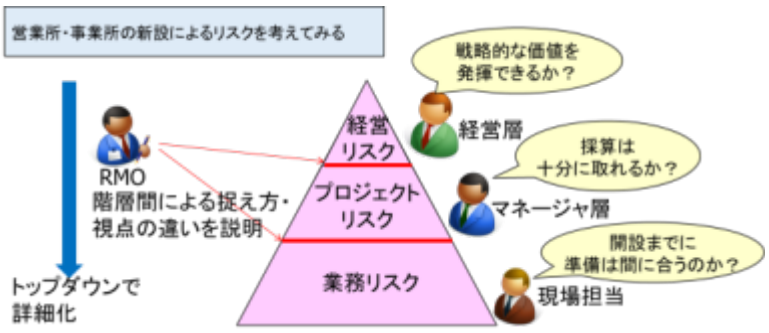

図 6 組織におけるリスクの捉え方

3. 時間に関する課題

1) 費用対効果の評価

現在のリスクを評価し、対策を決定する為の材料を揃え、経営層に進言する役割をRMOが担う。

例として「図 7 経営層と現場を繋ぐRMOの活動」では、各現場で洗い出されたリスクを正確に伝え、回避・低減・転嫁・保有のどれに当てはめるかを経営層に判断してもらい、方針と優先度を決定し、現場にその決定事項の説明と、具体的な計画を作成するように指示を出すまでを行う。

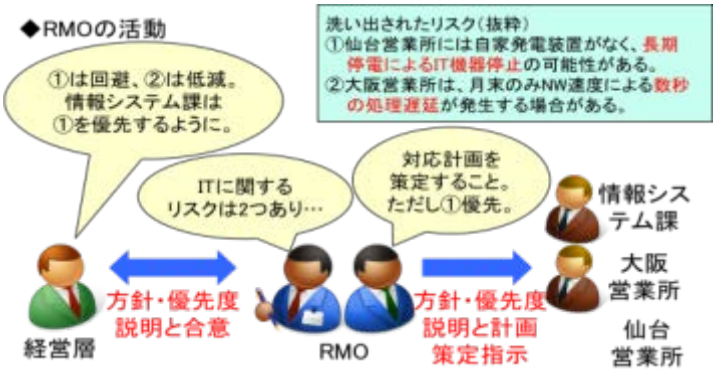

図 7 経営層と現場を繋ぐRMOの活動

しかし、「図 8 組織のパワーバランスが大きい場合」のように、RMOの役割を担う者がおらず、組織間のパワーバランスが大きい場合、大きな組織の施策を優先してしまい、本来処置しなければならないリスクがそのままとなってしまう場合がある。

図 8 のような事にならないためにRMOは、現場とリスクに対する業務（経営）に対する影響を正しく捉え、リスク対策において実施可能な対策とその費用対効果などを鑑みて効果的な施策を決定する。

また、経営層とは、各現場で洗い出されたリスクと施策を正確に伝え、リスクの最終評価から対策方針と優先度を合意する。

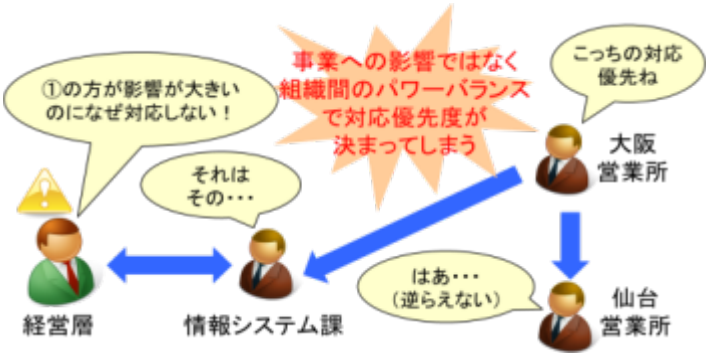

図 8 組織のパワーバランスが大きい場合

このように業務（経営）に対する影響や費用対効果などを可視化して評価することで、経営層が的確な判断を行えるようにし、現場と経営層との間を橋渡しする活動もRMOの役割である。

4. 時間に関する課題

1) 費用対効果の測定、報告

経営層に提示した費用対効果を測定して、報告を行うもRMOの役目である。

経営層からリスクに関する権限委譲を受けて、RMOを専任化する事により、報告や分析はRMOが取り仕切り、実際の実行と測定は各マネージャにお願いすることで分業化し、協力体制を引くことが重要となる。

「図 9 各ステークスホルダーの役割」として、経営層はリスクに関する全てを権限委譲し、リスクマネージャは業務（経営）に対する影響のあるリスクに関する全て報告・連絡・相談を行う。

また、現場との間は、連絡・依頼・相談を各マネージャと行い、各マネージャからの報告・回答・相談を受けて、一緒に考えるなど、現場と密に行動する必要がある。リスクマネージャは、経営層と各マネージャ層の橋渡し役となり、業務（経営）に対する影響のあるリスクに対峙する事で、リスクをコントロールしながら、適切な分析を基に費用対効果を算出し、報告する役割である。

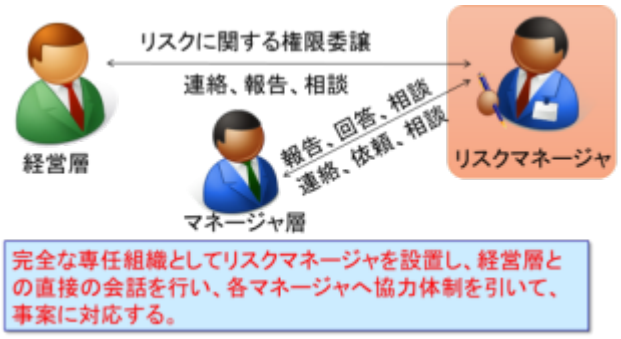

図 9 各ステークスホルダーの役割

VI. まとめ

リスク、もしくはリスクマネジメントに関しては、過去、様々なフレームワークで論じられてきており、ほとんどの組織では、何らかの形でリスクマネジメントを実施していると推測する。これまでの説明により、リスクマネジメントを効果的／効率的に実施していくにあたっては、RMO が有用であることは理解できたであろう。

しかしながら、当分科会では研究しきれなかったリスクマネジメントにおける課題が存在するのも事実である。例えば以下のような課題である。

・リスクマネジメントの実行者を、どのように評価して人事考課に反映するか？
・コントロール中の状況変化を、どのように発見および識別するか？
・プラスあるいは中立のリスクを、どのようにマネジメントするか？

これらに対し、RMO が同様に有効な場合もあるだろうし、まったく異なったアプローチが必要な場合もあるであろう。機会があれば、再び研究していきたいと考えている。

本ホワイトペーパーの発行をもって当分科会での研究は終了となるが、研究成果が読者それぞれの IT サービスマネジメント向上の一助となれば幸いである。

＜著者紹介＞
リスクマネジメント研究分科会

座長	白井　祐司	(株式会社 NTT データ SMS)
副座長	谷　芳文	(株式会社 ビーエスピーソリューションズ)
	阿部　正峰	(富士通 株式会社)
	萱原　渉	(団体会員)
	金田一　啓史	(NTT データ先端技術 株式会社)
	小林　知美	(JB サービス 株式会社)
	角　一己	(アイエックス・ナレッジ 株式会社)
	中谷　英雄	(個人会員)
	松田　浩幸	(株式会社 サンシーシステム)
	三浦　康弘	(個人会員)
	村上　憲也	(IT 経営コンサルタント塾)
	梁島　泰之	(東京海上日動システムズ 株式会社)
	山内　裕史	(個人会員)

事業継続マネジメントシステム(ISO 22301)や、情報セキュリティマネジメントシステム(ISO/IEC 27001)などビジネス側のリスク管理領域に対する ICT 継続としての IT-BCP と、ITIL®v3 プロセス(ITSCM)との連携と活用についての研究を目的として 2013 年 4 月発足。本ホワイトペーパーの発行をもって活動をクローズ。