

IT環境下における組織運営の評価に関する 調査研究報告書

—JRMS2010年バージョンをめざして—

平成21年3月



財団法人 日本情報処理開発協会



この事業は、競輪の補助金を受けて実施したものです。

<http://ringring-keirin.jp>



はじめに

(財)日本情報処理開発協会(JIPDEC)は、IT環境の著しい変化が組織に与えるリスクの大きさに鑑みて、これまでさまざまな試みを展開してきました。その一つは1992年に発表したJRAM(『コンピュータセキュリティに関するリスク分析-JRAMによるアプローチ』JIPDEC)です。JRAMの特徴は「JRAM質問票」に対する回答結果に基づいた「脆弱性分析」と「業務日報・障害報告等」の分析シートに基づいたリスクの実態分析から構成されたリスク分析のための方法論でした。

JRMS開発当時、すでにネットワーク重視の動きがみられていましたが、システム環境の中心がまだ集中型であったことから、リスク対応のための基本的な枠組みとしてリスク分析に焦点が当てられていました。

JRAM発表後、10年の経過の中でわが国のネットワーク環境が目覚ましい進展を遂げ、一段とリスク環境の変化が複雑多様化してきました。そこで、新たな視点からのリスクマネジメントの枠組みを構築する必要性に鑑み、1999年にJIPDECリスクマネジメント委員会(以下、「JRMS委員会」という。)を構成し、システム環境に関する脆弱性分析に重点を置いたツール開発の検討を開始しました。

当時、ISOにおけるリスクマネジメントに関するガイドラインの検討が行われ、2001年には『JIS Q 2001 リスクマネジメントシステム構築のための指針』(日本工業標準調査会審議, 2001年3月20日制定)(日本規格協会)が公表されました。JRMS委員会では、そこでの審議経過を重視し、議論を踏まえながら新たな視点から広範囲にわたる情報リスクへの対応について論議を進めてきました。特に、2002年に発表した『わが国の情報セキュリティの実態-「情報セキュリティに関する調査」集計分析-』(JIPDEC)でも、JIS Q 2001における基本的なリスクマネジメントの視点を取り入れた質問項目を取り入れて調査を実施しました。

さらに同委員会では、これまでの検討方針に従い、「JIPDEC リスクマネジメントシステム」を構築するため、一連の作業を展開し、2003年3月に情報システム全体を経営の視点から捉えたJRMS構築作業の成果の一部として『情報化社会におけるリスクとJRMS-リスク対策検討委員会調査研究報告書-』を公表し、その成果が2004年1月に『JIPDEC リスクマネジメントシステム(JRMS)解説書』(以下、「JRMS2003」という。)として公刊されたのです。

今回の報告書はJRMS2003における方法論をベースに、その後のリスク環境の変化を踏まえ、現在ISOにおいて審議されているリスクマネジメント規格(ISO31000)を考慮してマネジメントの視点を強化し、リスク評価指針検討委員会において議論・検討を展開した成果であります。組織をめぐる経営環境はグローバル化の中でITへの依存度を一段と高めており、今後のさまざまなリスクにも対応できる枠組みを視野に入れたものであるといえます。

本報告書の公表に際し、検討委員会委員各位のご協力に感謝の意を表する次第です。

2009年3月

財団法人日本情報処理開発協会

2008 年度リスク評価指針検討委員会

(敬称略／五十音順)

委員長	森宮 康	明治大学 商学部 教授
委員	稲垣 隆一	稲垣隆一法律事務所 弁護士
委員	後藤 牧人	コミールグループ CEO & Chairman
委員	指田 朝久	東京海上日動リスクコンサルティング(株) BCM 事業部長 BCM コンサルティング第三グループリーダー
委員	佐藤 厚夫	(社)情報サービス産業協会 プライバシーマーク審査会 審査業務部長
委員	新保 史生	筑波大学大学院 図書館情報メディア研究科 准教授
委員	野口 和彦	(株)三菱総合研究所 研究理事
委員	原田要之助	(株)情報通信総合研究所 マーケティングソリューション研究グループ主席研究員
		大阪大学大学院 工学研究科 特任教授
委員	松原 榮一	ガートナージャパン(株) リサーチバイスプレジデント
委員	盛岡 通	大阪大学 環境・エネルギー工学専攻 環境マネジメント学領域 教授
委員	吉田健一郎	(財)医療情報システム開発センター プライバシーマーク付与認定審査室
委員	渡辺 研司	長岡技術科学大学 大学院技術経営研究科 准教授

目 次

1. 経営環境の変化とリスクマネジメント	1
1.1 リスクマネジメントの重要性	2
1.1.1 リスクマネジメントの捉え方	3
1.2 リスクマネジメントの今後の展開	4
1.2.1 リスクマネジメントが必要とされてきた背景	4
1.2.2 各分野のネガティブな影響管理から組織の不確実性最適化の手法へ	5
1.2.3 最新のリスクマネジメント ISO31000 の紹介	6
2. JRMS2010 の概要	8
2.1 リスクマネジメントと JRMS	8
2.2 JRMS の特徴	9
2.2.1 JRMS の基本的特徴	9
2.2.2 JRMS2010 における三つのポイント	10
2.2.3 JRMS2010 の特徴	11
2.2.4 JRMS2010 の構造－リスクマネジメント意思決定の流れ－	14
2.2.5 JRMS2010 における回答者と質問票の構成	16
3. JRMS2010 の構成	26
3.1 質問構成について	26
3.1.1 三つのバージョンについて	27
3.1.2 JRMS2010 の構成	30
3.2 成熟度モデルについて	34
3.2.1 JRMS2010 の成熟度モデル	34
3.3 JRMS の使い方	36
3.4 JRMS の高度な使い方	36
3.5 JRMS のサポート機能について	38
3.6 JRMS ツール	39
3.6.1 ツールの特徴	39
3.6.2 提供機能	41
3.7 JRMS2010－Quick Start 編の構成	43
4. JRMS の有効性検証	57
4.1 JRMS 分析チャートの読み方	57
4.1.1 ギャップの判定の考え方	57
4.1.2 チャートの分析例	58
4.1.3 JRMS の評価結果の活用	70

4.2	実証実験分析評価例.....	71
4.2.1	A 社の実証実験概要	71
4.2.2	A 社リスク評価レポート	71
4.2.3	実証実験に対する意見・認識.....	117
4.3	JRMS2003 年度版質問編による分析例.....	119
5.	参考資料	128
5.1	JRMS2003 について.....	128
5.1.1	JRMS2003 の特徴.....	128
5.1.2	JRMS2003 における三つのポイント.....	130
5.1.3	JRMS2003 の質問構成	131
5.2	成熟度モデルについて	132
5.2.1	CobiT4.1 の成熟度モデル	132
5.2.2	CMMi の成熟度モデル.....	133
5.2.3	NIST の成熟度モデル	134
5.3	JRMS2010 xml 形式の表示例	134

1. 経営環境の変化とリスクマネジメント

組織をめぐる経営環境の変化は、ICT 社会において一段とスピードを速めてきている。かつてバブル経済の崩壊後、金融・財政に係るリスク対応の不備から「失われた 10 年」といった表現がマスコミを飛び交った。これは組織をめぐる経営環境の著しい変化への対応の難しさを示している。また、環境変化のパターンの量的・質的な変化の大きさ、そのスピードの加速化を重視し、先を読むことの重要性を教訓として残したとみることもできる。

たとえば、保護行政下にあった金融の世界では、公的資金の導入後も不確定要因により回復の道が不透明であっただけでなく、金融への信頼が揺らぎ、株安の影響がさらに拡大し、2002 年以降もその影響は残り、さらなる公的資金の導入が行われた。

さらに、当時金融・財政に係るリスクの他に、人々の食生活に関するリスクも取り沙汰された。狂牛病関連では肉骨粉の混入の実態解明が十分に進まない中、肉表示の偽装工作が判明し、当該業界における関係者のモラルハザード、ひいては組織倫理の問題がクローズアップされた。

グローバル化した現在の経営環境では一国の市場だけが取引対象ではない。サプライチェーンを考慮に入れるとき、国外市場における問題状況が直ちに国内市場に影響を及ぼすため、チェーン全体を視野に入れた経営を考えなければならない状況にあることが確認された。

かつてアメリカにおいてコーポレートガバナンスの面から着目を集めたエネルギー業界の雄、エンロン（Enron Corp.）が経営破綻した結果、取締役会の構成・責任の所在、監査法人の信頼性等に疑問が提起され、企業改革法といわれる Sarbanes-Oxley Act（SOX 法）が 2002 年に制定された。日本では 2006 年に証券取引法が一部改正・改題され、金融商品取引法が誕生したのであった。

今日問題なのは、金融商品の取引すら瞬時に世界をめぐり、その影響が連鎖反応的に拡大し、信用の収縮を引き起こし、世界的に需要がシュリンクし、それが実体経済を揺るがす事態に至っていることである。背景としては、2007 年夏にアメリカにおいてサブプライム関連で住宅ローン会社が破綻し、さらにフランスの大手銀行 BNP パリバ（BNP Paribas）がサブプライムを証券化した商品への投資の損失から傘下のファンドを凍結するなどの問題の発生をあげることができる。2008 年の夏にはアメリカの住宅公社の経営が悪化し、信用不安が拡大した。その後、同年 9 月のリーマン・ブラザーズ（Lehman Brothers）の破綻により、金融不安が一気に加速化し、金融危機が驚くほどの速さで全世界に連鎖的に波及したが、とりわけ、金融を重視したヨーロッパ諸国への影響には大なるものがある。

2008 年夏頃までは、先進国の経済の低迷はブリックス（BRICs）により対応可能といったデカップリング論が謳われていたが、消費者の需要縮減の影響が製造拠点となっていた国々に作用し、需要収縮の連動の実態からリカップリング論が登場するに至っている。

特に、それぞれの国にはそれなりの事情がある。日本の場合、金融（特に株式）・不動産バブルのマイナスの影響を 10 年がかりで回復基調に導くことができたのは、ひとえにアメリカや中国を含む海外への輸出にあった。しかし今回の金融危機では、世界同時不況の影響のもと、輸出関連産業へのインパクトは海外市場における需要の減退、各国の保護貿易的動き、為替の動向（特に円高）等により、過去と異なった状況がうかがえる。

ここで考慮すべき点は、何事にも兆候があるということである。たとえば、アメリカにおける住宅バブル崩壊のリスクについては、2007年の段階ですでに取り上げられていた。それにもかかわらず、金融機関や製造業等のトップマネジメントの多くはその兆候を軽視したのか、他人事視したのか、経営にとってのリスクという視点から状況を判断することがなかったと思われる。

概して、経営環境の変化を認識できていれば、そうした兆候に気づくことができたかもしれない。しかし、今回の金融危機の連鎖から容易に理解できるように、ことはそれほど単純ではない。特定の人には変化の兆候を認識できていたとしても、組織内の他の人々がリスクに関する認識力を持っていなければ、到底意思決定に反映させることはできない。とりわけ ICT 社会において意思決定のスピードが求められ、しかもそのスピードが加速化している中で、環境変化への対応を的確に行うには組織の構成員にリスクに対するセンスなりマインドが共有できていなければ無理である。

しかも、こうした経営環境の変化の中で、リスクという視点を単に個人・部門単位のみで培うだけでは十分とはいえない。一部門だけがよくても、全体の組織のためにプラスにならないければ組織の屋台骨が根底から揺さぶられ、組織の存続が危うくなることがありうるのである。

1.1 リスクマネジメントの重要性

このところリスクならびにリスクマネジメントの文字が飛び交わない日がないほど重視されてきているが、その考え方にはそれぞれ国の経営環境、業界特有のビジネスモデル、関係者のバックグラウンドなどから、重点の置き方により種々のアプローチがあるため、これがリスクマネジメントであると指摘することはなかなか困難である。

しかしながら、取引市場がグローバル化する中で、たとえば、サプライチェーンを考慮する時、国内企業がリスクを重視した経営を行っている場合、海外の取引先企業がそれと同様の視点に立った経営を行っていないければ、リスクが顕在化した場合、対処に窮することになる。

たとえば、「図 1-1-1. サプライチェーンの一例」¹ は、B 社（海外部品工場）および C 社（販売会社グループを含む）をそれぞれ A 社（本社）の海外子会社とし、海外の拠点における経営は現地に委ねていると仮定する。その場合、A 社が B 社で部品を製造し、その部品をもとに A 社で組み立て、完成品を C 社に送り、C 社はそれぞれの販売拠点で消費者に製品を売ることを想定している。

仮に、A 社ではリスクマネジメントを実施しているが、B 社、C 社では現地の責任者に経営を任せ、本社基準のリスクマネジメントを実施していないとなれば、部品製造に起因するリスクを考慮する必要がある。自国と製造拠点における法的責任に差異があれば、法的責任の緩い国での製造ではそれなりの対応ですむことから、自国に比べてコスト節約的な展開が可能かもしれない。しかし、販売後の責任に目を向けるならば、C 社のそれぞれの立地の場における基準に応じて対

1 本図は、システム監査学会における研究活動の一環として設置されている研究プロジェクトの一つである「リスクマネジメント研究プロジェクト」の成果をベースにしている。参照：黒澤兵夫「リスクマネジメント研究プロジェクト成果報告 システム監査と事業継続マネジメントシステム（BCMS）の考察について」『システム監査』Vol.22, No.1(Sep 2008), PP.124～130.

応するとしても、法的責任が厳しい国での製造物責任への対応コストが重くのしかかることも現代では常識となっているはずである。さらに法的責任が緩い国でもグローバル化の中で基準を厳しく改正していかなければならないとなれば、あらかじめ厳しい基準で対応しておくことが消費者の信頼、従業員の安全、企業としての社会的責任に適うことになる。

いずれにしても、現在の経営環境において、リスクマネジメントの展開にあたっては、グローバルな観点からすべての関係会社を本社基準で展開するのがリスクマネジメント戦略として妥当だといえる。その意味では、ISO が種々の規格を設け、国による規格格差をなくす方向で活動していることを理解し、規格の適用を重視する段階にあるといえる。

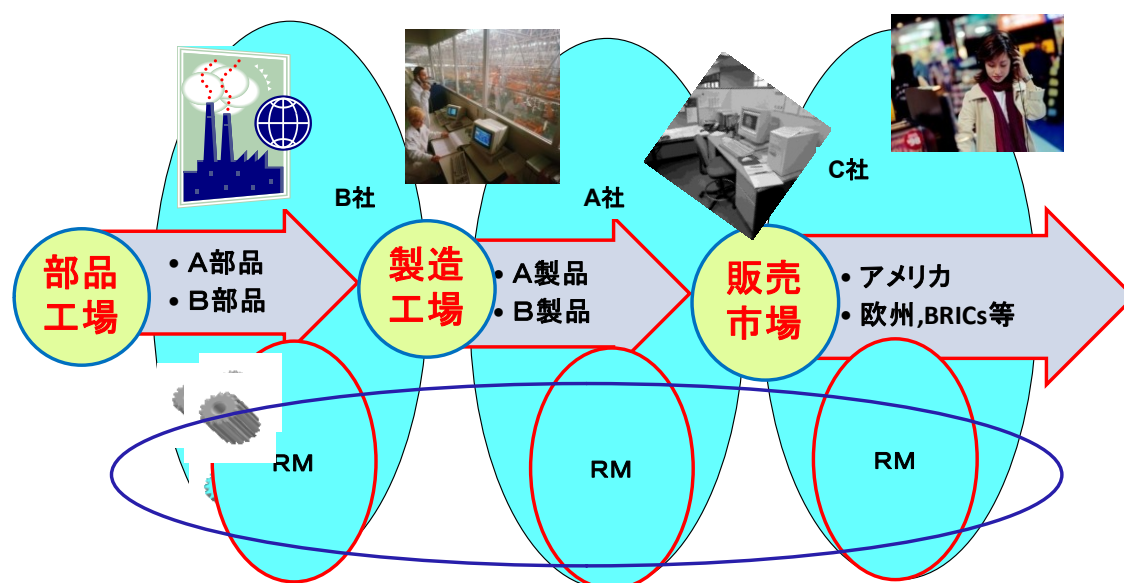


図 1-1-1 サプライチェーンの一例

1.1.1 リスクマネジメントの捉え方

組織において重要な点は、組織としてのミッション²を達成するために経営方針を立て、さまざまな経営資源を投入することである。しかし、ミッション達成を阻害するさまざまな要因が存在し、しかもその要因は単独ではなく、時として複合して阻害要因となることが問題となる。それこそがリスクである。

そのため、組織は経営方針に基づきリスクマネジメント方針を持ち、リスク対応のための行動指針を明確にし、そこでの基本目的を果たすためにリスクマネジメント計画を立て、それに従ってリスクを分析・評価してリスク対策を選定し、実行に移してその成果を評価し、状況に応じて

2 ここでは、組織について、営利企業・非営利企業を問わず、また、企業における部門組織を視野に入れる場合も含んでいる。特に、組織には組織としての存在目的があり、ミッションの実現のため、本文で指摘するように各種の経営資源を投入している。とりわけ、企業においては、ミッションといった表現を使わず、経営理念、社是、社訓を充てる場合もある。ここでは組織として達成すべき最上位概念として位置づけている。

是正・改善の措置をとることが求められる。こうしたプロセスにおいては、リスクマネジメントをシステムとする体制を構築・維持する枠組みが不可欠であることを組織において考慮すべきである。

リスクマネジメントをこうした視点から捉えていくと、いくつかのキーワードが浮かび上がってくる。たとえば、上記の視点に立ったリスク対応活動を行うには、リスクマネジメントの方針を立て、計画を立案し、リスク対策を実行に移し、評価・改善する場合には当然のことながら種々の部門組織の機能（ファンクション）を考慮しなければならない。したがって、リスク対応のための組織の管理・調整活動が必要になる³。

また、企業の価値の維持・増大といった目標と関連づける場合、内外のさまざまなリスクを適切に管理することが重要視されることになる⁴。それとの関連から、リスクを全社的視点から合理的で最適な方法で管理するといった、リスクとリターンとの関連から企業価値に言及する展開がみられるようになった⁵。

ところで、上記の視点の背後には、リスクならびにリスクマネジメントに関する見方にかなり従来と異なる面が感じられる。一つはリスクを損失発生と結びつけた概念、すなわち純粋リスク（pure risk）に関連づける見方とは異なり、たとえばリスクとリターンという表現があり、そこにはリスクの取り方により利益なり収益の増加が可能であるという視点が組み込まれている。もう一つは、リスクマネジメントを単に特定の部署に限定することなく、経営全体を巻き込んで展開する視点である。

たとえば、経済産業省経済産業政策局産業資金課『先進企業から学ぶ事業リスクマネジメント 実践テキスト—企業価値の向上を目指して—』では、リスクマネジメントを「収益の源泉としてリスクを捉え、リスクのマイナスの影響を抑えつつリターンの最大化を追求する活動」と捉えている⁶。

したがって、組織経営のために組織の全体最適を志向し、リスクアセスメントを行い、リスク対応を実践するため、リスクマネジメントの仕組みを作り、それを継続的に維持するという考え方の導入が必要となるのである。

1.2 リスクマネジメントの今後の展開

1.2.1 リスクマネジメントが必要とされてきた背景

社会や企業が高度化すると、潜在するリスクは大きくなる。それは、社会が便利になり企業活動が高度化すれば、あたり前となっている状況や既得利益が失われた際の影響も大きく、かつ市

3 この点については、日本規格協会編『JIS Q 2001 リスクマネジメントシステム構築のための指針』（2003年）に示されているリスクマネジメントの捉え方（定義）を参照されたい（P.15）

4 経済産業省「リスク新時代の内部統制 リスクマネジメントと一体となって機能する内部統制の指針」リスク管理・内部統制に関する研究会（2003年6月）における見方を想起されたい。

5 経済産業省経済産業政策局産業資金課『先進企業から学ぶ事業リスクマネジメント 実践テキスト—企業価値の向上を目指して—』経済産業調査会,2005年,(P.18)を参照されたい。

6 上掲書,P.16.

民や消費者の要求レベルも高くなるからである。

再発防止の考え方ではすでにトラブルが発生している。そのため、対策を施す対象の選定や実施の必要性、投資対象などを疑問に思ったりためらったりする必要はなかった。しかし、この手法には大きな問題点がある。それは、事故や災害を経験しない限り対応が取れず、新たな問題には対応できないということである。さらに、トラブルが再発防止のためにより経験になったといえるレベルに収まっていればこの手法も有効だが、最近では一度の失敗や災害で致命的な影響を受ける場合もある。

そこで、トラブルが発生する前、つまり、まだトラブルが「リスク」として潜在している段階で、トラブルへの対応を考える必要が出てきた。このように新たな要求に対応するため、組織運営におけるマネジメント技術の改革が必要となり、その手段の一つとしてリスクマネジメントという管理技術が導入されてきたのである。

1.2.2 各分野のネガティブな影響管理から組織の不確実性最適化の手法へ

(1) リスク概念の変化

これまで、リスクマネジメントは多くの場合上述のとおりネガティブな影響をコントロールすることだと理解されてきた。それは、リスクの対象概念が失敗や事故、災害のような主に危険やネガティブな結果をもたらすものに対して適用されてきたからである。しかし、「リスクマネジメントー用語ー規格において使用するための指針」（2002年に「ガイド73」としてISO/IECより発行）によってリスクの概念は変化した。

この規格は、これまで各々の分野で使用されていたリスクマネジメントの用語を標準化したもので、さまざまな分野のリスクマネジメント用語を包括した定義づけを行った。また、リスクは顕在化した影響として、ネガティブな影響とポジティブな影響を共に含み、また期待値から乖離しているものとして定義づけられた。このことにより、リスクマネジメントはネガティブな影響の管理手法から不確実性を取り扱うマネジメントとして有効性が拡大したのである。

しかし、リスクの概念が広くなるとこれまでリスクマネジメントとして整理されていたいくつかの概念の変更も必要となる。その一つが「リスク低減」というリスク対応の概念である。リスクがネガティブな影響のみを持つものとして認識されている場合、リスクは低減されるべきものであったが、リスクの概念に好ましい影響も含むのであれば、リスクは必ずしも低減すればよいとはいえない。そこで、現在ではリスクの低減に変わり、「最適化」という概念が重要となってきたのである。

しかしリスクの最適化という概念は、理解を誤ると大きな混乱をもたらす可能性がある。ここでいうリスクの最適化とは、単なる期待値の最大化ではない。リスクの最適化を期待値の最適化として理解すると、ネガティブな影響が大きくてもそれを上回るポジティブな影響がある場合には、そのリスクは無批判に受け入れられてしまう。しかし、社会や組織において、たとえポジティブな効果が期待できても、ある一定以上のネガティブな影響が発生する可能性がある場合には、そのリスクを受け入れないことがあるのは当然である。

したがって、リスクの最適化にあたっては、評価の第1ステップとして、受け入れられないネガティブな影響の発生確率を顕在化のおそれがある発生確率以下にまで下げることが重要で

ある。そしてその後、評価の第 2 ステップとしてポジティブな影響とネガティブな影響の組み合わせの最適化を行うのである。

(2) 組織マネジメントの最適化手法へ

これまでのリスクマネジメントは、安全や保険など各分野でそれぞれの管理手法として発達してきた。そのためリスクマネジメントは各分野の特徴に合わせて発展し、そこで使用される用語の定義もそれぞれ異なっていた。そのような状況でも、リスクマネジメントが各々の適用分野で限定的に使用されている間は特に問題はなかった。

しかし、リスクマネジメントの重要性が広く認識されるにつれ、多様な分野でリスクマネジメントが採用されるようになった。さらに組織経営自体にも適用されるようになると、その手法の標準化が求められるようになったのである。

このような要望に応えるため、ISO（国際標準化機構）はリスクマネジメント規格の整備を始めた。それが汎用的リスクマネジメント規格 ISO31000 である。また同時に ISO/IEC ガイド 73（リスクマネジメント用語規格）の改定も始めた。

ISO31000 は組織のマネジメント要求に応えるため、リスクの概念として ISO/IEC ガイド 73 の考え方を採用している。そのため、リスクマネジメントの対象は「ネガティブな影響を持つ可能性の管理」という考え方から、「組織目標達成を阻害する事項への管理」へと拡大している。つまり、リスクマネジメントにおける意思決定が経営における意思決定へさらに近づこうとしているのである。この考え方によれば、同じ事象でも組織によってリスクとして捉えるか否か、また、リスクの重要性の評価も異なってくる。これは、組織によって重要な意思決定の内容が異なることを考えれば当然のことである。

1.2.3 最新のリスクマネジメント ISO31000 の紹介

(1) ISO31000 規格策定の経緯

ISO31000 は 2005 年に日本とオーストラリアが汎用的リスクマネジメント規格作成の必要性を TMB（技術監理評議会）に提案し、9 割を超す国の賛成を得て開発が承認されたものである。

本規格を作成するために TMB の下にワーキンググループが設置された。ワーキンググループの議長はオーストラリアから、そして事務局は日本が担当することになった。

ワーキンググループは最終案が策定されるまで、2005 年 9 月の東京での第 1 回会議から 2008 年 11 月のシンガポールでの第 6 回会議まで、合計 6 回開催された。

規格名は、最終会議（第 6 回）において“General Guidelines for Principles and Implementation of Risk Management”と決定された。

(2) ISO31000 の概要

本規格はリスクマネジメントプロセスに関する原則と実地的な指針を提供し、あらゆる組織およびあらゆるタイプのリスクに適用できるものとして設定されており、既存のリスクマネジメント規格を排除するものではなく、包含するものである。

また本規格は、リスクマネジメントプロセスの概念を明確にすることやリスクを管理し対処

するために、組織に实际的な指針や組織と利害関係者間の意思疎通と協議のためのツールを提供することを目的としている。

また、組織の統制力を高め、社会や組織に対する不必要な負荷を最小限にすることや利害関係者の信頼と信用を達成し、高めることも目的としている。

(3) リスクの概念の変化による組織目標共有の重要性

先に記したように、これまでリスクの概念はネガティブな影響を持つ可能性という考え方が支配的であったが、本規格では、組織が目指す組織目標を明確にして、その目標の達成を阻害する事項をリスクとして捉える考え方を採用している。この考え方でリスクを考えると、同じ事象であってもリスクか否か、またリスクの重要性の評価が異なってくる。

したがって、リスクマネジメントを実施する場合、いきなりリスクを把握する活動から開始するのではなく、リスクマネジメントの前提となる組織目標を全社員で共有する必要がある。そのためには、組織ミッションを明確にして、経営者が組織目標（または経営目標）や経営方針を明確にすることが重要である。

(4) リスク分析時に必要な組織環境の把握

これまでリスクマネジメントにおいてまず実施すべきことはリスクの把握だとされてきたが、リスクの把握を的確に実施するためにも、事前の活動が重視されてきている。その中で、特に重要視されているのが組織の内外環境の把握である。以下にその事例を示す。

①外部環境の把握例

- ・文化、政治、法律、規制、経済および環境（海外、国内、地域）
- ・外部のステークホルダーの認知度と評価
- ・組織の目的に影響を与える主な要因および動向

②内部環境の把握例

- ・認知度、価値観および文化
- ・方針とプロセス
- ・内部ユニットのステークホルダー
- ・制度（例：ガバナンス、職務、責務 等）
- ・リソースや知識の観点からみた可能性（例：資本金、人材、能力、プロセス、システム、技術力 等）
- ・達成しようとしている目的およびその戦略

(5) リスクマネジメントカルチャーの構築

リスクマネジメントの活動を行うためには、その考え方を担当者が理解するだけではなく、組織として実施するための組織文化の基盤を構築することが重要である。そのためには、まず価値観を共有化するためのコミュニケーション力の向上が必要である。これまでもコミュニケーションの重要性は述べられていたが、それは分析したリスクをステークホルダーで共有する大切さを論じたものであった。しかし、ISO31000 ではコミュニケーションの目的としてリスク分析をする以前に、関係者で必要な知識や価値観を共有することの重要性が記されている。

2. JRMS2010 の概要

2.1 リスクマネジメントと JRMS

JIPDEC は情報環境下におけるリスク分析の手法として 1992 年に JRAM (JIPDEC リスク分析方法論) を公表した。この JRAM は、組織の「業務日報・障害報告等」の報告書類に記載された内容から、原因・対応・組織への影響を明確にする「実態分析」と、リスクに関わる質問項目への回答により組織の実態を把握する「脆弱性分析」の二つの方法論を用いた手法であった。

その後のネットワーク環境の著しい発展に伴うリスク環境の変化に対応させるため、「脆弱性分析」方法論をベースに 2003 年にリスクマネジメントツールとして JRMS2003 (JIPDEC Risk Management System) を開発した。

JRMS2003 は、特にリスクに対する質問票への回答結果に基づく組織の脆弱性を分析する実践的なツールとして有効性が確認されたものである。(JRMS2003 については、後述の「5.1.1 JRMS2003 の特徴」を参照のこと。)

JRMS2003 開発当時、一般にみられたのは組織にとってのマイナス情報は外(たとえば、組織としては外部に、組織内であれば他の部署)に出さないという傾向にあった。しかし、問題の内容によってはタイミングを含め情報の開示が必要な場合もある。ちなみに、アメリカで SOX 法が制定された後、わが国でも 2004 年に「公益通報者保護法」(俗称、内部告発者保護法)が成立し、状況に変化が生じたといえる。

なお、リスクマネジメントにとって重要な点は、リスクの作用は組織全体に及ぶこともあれば、一つの部署で影響が収まる場合もありうる。しかし、問題の軽重の判断については、組織の関係者としてそれなりのリスク認識(リスクマインド、リスクセンス⁷⁾)を有していることが必要である。それには行動に関する「先」の「先」を読むことが前提となる。その対象となるのが、リスクを生み出す組織におけるさまざまな脆弱性の存在である。

たとえば、組織の経営を揺るがす事態を起こした企業を想起するとき、現場での関係者の言動にリスクセンスのなさを思わずにはいられない。某メーカの現場では、基本的に存在していたマニュアルどおりにすべきことを、近代的な装置・衛生設備のもとで工場内の製造パイプライン配管設備の清掃の回数を減らしても現状では影響はない、といった判断が季節の変化による設備内部の異変という「先」を考慮しなかったために大事故が発生したことがあった。

したがって、組織の関係者にある程度のリスク判断に関する共通の理解なり認識を有してほしいという側面がある。そのため、組織の関係者に対しリスクに係る質問票を提供し、それに回答することにより、質問項目に対する回答の差異(バラツキ)の原因分析を通して共通認識を得ることが可能になるといえる。現実には、組織の構成員はこれまでのキャリア(個人の資質、高等教育に関しては文系と理工系による思考パターンの若干の差異、入社以降の部署における経験・体

7 ここではリスクマインド(risk mind)はリスクの発生からその影響について推論し判断するという考える力を、リスクセンス(risk sense)は前記に関わるリスクの重要性を認識する智慧なり感性を指している(森宮康「医療リスクマネジメント—わが国における医療事故対応の方向性を求めて—」『日本保険医学会誌』(第 102 巻 1 号) 2004 年 3 月 17 日

験の違い、所属部署における責任の度合い等）の違いのみならず、質問に対する取組み姿勢等により異なった理解が生じることがある。そうした部門間の回答に対するのギャップを重要なデータとしてリスクマネジメント行動に活かすことが可能となるのである。

2.2 JRMS の特徴

リスクマネジメントの展開において、経営者層を含め、組織の構成員がそれぞれ求められている職能に係るリスクの意味づけならびに対応状況について同じ認識レベルにあることが望ましいが、現実には差異（バラツキ）が存在するといえる。その理由なり根拠については、既述のようにこれまでの職務上の役割・責任等の違いも関係している。こうした差異の原因を究明し、組織構成員のリスクマネジメントに関する認識の共有を確保することに資するのが JRMS の重要なポイントである。

さらに、組織の構成員を取り巻く環境は常に同じとはいえず、今日のように変化が著しい中では、変化それ自体がリスク発生の要因となるため、過去のやり方が今後とも通用するとは限らない。したがって、リスクマネジメントを実践する際には、自らの組織のリスクマネジメントを展開するベンチマークの設定が不可欠となる。そのため、「3.2 成熟度モデルについて」で後述する JRMS2010 の成熟度モデルにおける評価レベルを設定し、スタートとしてのベンチマークを決めておくことが大事である。いわば、JRMS を活用することで組織のリスクマネジメントの現状を把握しうるとともに、構成員のリスクマネジメントに関する認識レベルが把握できるようになる。したがって、JRMS は今後の方向性を見定めることが可能となる実践的なツールである、という特徴を有している。

2.2.1 JRMS の基本的特徴

JRMS の基本的特徴として次の 7 点を指摘することができる。すなわち、

第 1 の特徴は、質問項目が、組織全体と関係部署に係る部門の課題に対応すべく構成されている点である。同一の質問への回答結果を通して部門の異なる回答者のリスクと課題認識の実情を把握することが可能になるわけである。

第 2 の特徴は、質問項目が階層構造化されている点である。質問項目は五つの階層から構成され、キーワードにより質問項目のタイトルが表示されている。

第 3 の特徴は、質問項目に対する回答結果の部門間比較がしやすいようにレーダーチャートにより示され、しかも回答部門の色分けにより視覚的に見やすい方式が採用されている。この点は、次の特徴に関係する。

第 4 の特徴は、回答部門は組織における業務内容との関係、活動領域の範囲等により、部門としての特性を示すことになる。たとえば、メーカーであれば、経営者層と製造部門では業務内容・責任の素材・関係するステークホルダーの違い等により、同じ質問への回答であっても回答結果に差異（difference and/or gap）が生じると思われる。特に、リスクに関する認識の違いは、経営決定に関しても重要である。

第5の特徴は、回答者の回答結果に関するものである。回答者はそれぞれのバックグラウンド（いかなる専攻分野の出身か、これまでいかなる部署での経験を有しているか、部署における責任範囲・重さ等々）により、同じ質問項目であっても回答結果に示される評価レベルが異なることがありうる。したがって、経営者層内であれ、リスクマネジメント部門内であれ、回答者間における回答結果に差異が生じうる。むしろ、回答者間において回答結果に差異が出てくるのは当然であり、重要な点は、その差異の原因が何かを把握することである。差異が発生する原因には、質問内容の理解、回答結果に示される評価の違いなど、さまざまである。

第6の特徴は、成熟度認識である⁸。JRMS2010においては、リスク評価指針検討委員会により、脚注8に示した成熟度モデルを参考にしつつも、JRMSに相応しいモデルを検討し、「3.2 成熟度モデルについて」で示す6段階からなる成熟度モデルを採用することにした。

質問への回答結果は、部門間のレーダーチャートにより視覚的に表示され、また回答者間の回答結果については集計シートに表示される。これにより部門間ならびに回答者間の比較が容易に可能となる。その際、重要な点は、組織としての評価レベルをベンチマークとして組織全体に明示しておくことである。

第7の特徴は、部門間、回答者間におけるリスクマネジメントに関する認識の共有であり、最も重要な点である。回答結果に差異が生じるのは、種々の事情により当然かもしれない。しかし、評価レベルに差異がある場合、その原因が現状ではやむを得ないのか、質問についての理解度が低いためのなのか、さまざまな問題が考えられる。それゆえ組織のベンチマークとの関係からその差異を分析し、リスクマネジメントの認識を共有するため、この作業をJRMSではギャップ分析と呼び、重視している。ギャップ分析については「4 JRMSの有効性検証」で分析例をあげて説明する。

特に、JRMS2010において評価レベルを0から5までの6段階とした根拠は、JRMS2003公表後、組織経営においては、社会的な不祥事の発生、組織の社会的責任、コーポレートガバナンスに関する認識等から、組織のリスクマネジメントに関する実践もそれなりに成熟しつつあるとの判断があり、本報告書発表前の実証実験においてもその点が確認されたことにもよっている。

2.2.2 JRMS2010における三つのポイント

JRMSが重視するのは、次の三つのポイントである。

第一のポイントは、組織のトップマネジメントが経営に関するリスクの作用を時間軸⁹で考えるため、自ら「リスクマインド、リスクセンス」を涵養することである。経営者層として、近年発生してきた問題状況の多くがリスク対応に関わる経営者層の判断の誤りによるところがかなり

8 JRMS2003ではCOBIT-Ⅲ、その基礎となったCMM（Capability Maturity Model）ならびにNIST（National Institute Standard Technology）の成熟度レベルを参考にしながら、JRMSとして0から3までの4段階の評価レベルを用いた。COBIT-Ⅲでは6段階でCMMの成熟度モデル（カーネギーメロン大学のソフトウェアエンジニアリングインスティテュートが提唱したモデル）およびNISTでは評価レベルが5段階であった。

9 リスク対応のプロセスを問題発生前、問題発生段階、問題発生後の対応という時間軸で考え、さらにリスクマネジメントの仕組みを維持し、常に改善を行うというPDCAのサイクルを動かすことを想定している。

多いことを認識する必要がある。この点は、経営者層が直接的に問題の発生状況に関係した場合を想起されたい。とりわけ、経営者として求められるのはステークホルダーに対する説明責任である。問題の発生が予測できるような場合、経営者層としては率先して組織の構成員を含め、リスクマネジメントの導入・実施に関する必要コストを投入すべきであり、この点に関わるのがJRMSである。

現実に社会的責任が問われるような問題が発生すれば、結局は事後的に対処しなければならず、終局的にかかった費用は特別損失として計上しなければならないわけである。それゆえ不測の事態への事前的な対応の不備が組織を壊滅に導くという認識から、日頃からリスクマインドなりリスクセンスを磨くことが経営者層としては必要と思われる。そのため、JRMSの質問項目に対する回答結果の評価レベルの差異（バラツキ）の原因分析を行い、経営者層間において生じ得るギャップ発生の理由を確認し、リスクマネジメントの実践に関する認識を共有することが求められている。

第二のポイントは、現場の担当者がリスク認識の不足により組織のゴーイングコンサーンを脅かす事態を起こす場合があるため、組織の構成員にもリスクマインド、リスクセンスについての認識を共有させる仕組みづくりが必要であり、JRMSがそれに関わることになる。組織の実体維持を考慮するとき、経営に関わるそれぞれの部門の関係者による「リスク認識の共有」は不可欠である。そのため、JRMS 質問項目への回答結果を通して回答者間の認識状況を把握し、「リスクに関する認識の共有」が可能になるのである。トップの判断の誤りのみならず、現場のミスジャッジにしろ組織の存続を危うくするのは、「先」の「先」が読めなくなった場合によることが多い。それゆえ、組織を守るには組織の構成員一人ひとりが同じようにリスク認識を有していることが不可欠である。

第三のポイントは、組織を取り巻く経営環境は絶えず変化していることを常に意識し、そのために絶えず組織内のリスクマネジメントのシステムの実態をチェックし、見直すことが求められる。そのためには「継続的な組織体制」を仕組みとして有しておくことが重要である。

経営環境は恒常的に変化していることを、単なる言葉としてではなく、質問項目への回答結果を通して見直し、改善を行った後もさらに適切な時期に繰り返しシステムを見直すことが問題状況の早期発見に役立つといえる。事後的に問題発生後仕方なく行う場合とのコスト・ベネフィットの比較考量からしても、そうした組織体制の構築は不可欠と思われる。さらに、システムとしての改善・見直しは、他の部署のことは自分のところには関係ないとする「他人事症候群」に陥らないために、特に重視すべきである。

したがって、現代のグローバル化した経営環境において、どのようなリスクの発生が考えられるのか、その特徴は何なのか、組織に対する影響（インパクト）はどうか、対策は十分なのかをあらかじめ事前的に明確に把握しておくことが重要である。

2.2.3 JRMS2010 の特徴

JRMS2010 は、現在の組織をめぐる環境変化に呼応するため、重要な特徴を有している。その基本的な方法論は、JRMS2003（「5.1 JRMS2003 について」を参照）の考え方をベースに置いている。

JRMS2010 は、組織におけるリスクマネジメントをこれまで以上に活用できるように構成している。組織、ここでは企業を対象とすれば、多くの企業はそれぞれの事業活動の展開の中で、さまざまなリスクに対応してきた。たとえば、企業の製品が顧客に与える欠陥製品問題に関しては製品企画・サービス関係の責任部門が対応し、また製造段階での廃水・排気ガスなど、環境に悪影響を与える場合には製造部門・法務部門が対応してきた。また、国や地方自治体などからのさまざまな規制に対しては法務部門・コンプライアンス部門が対応し、コンピュータが管理する個人情報については総務部門・システム部門が対応してきた。

しかしながら、企業のこれらへの対応がばらばらであると、一旦、企業の製品に係る健康被害や個人情報の漏えいやトラブルが起きた場合、企業内の情報が適切に経営者層に伝わらず、マスコミ対応でちぐはぐな対応をして、かえって事態を悪くするケースも多数見られている。

このような中、先進企業ではさまざまな分野でリスクマネジメントを見直し、企業内部で包括的に取り扱うようになってきている。「図 2-2-1. X 社のリスクマネジメント委員会」は、仮設的な会社である X 社がリスクマネジメント執行役員である CRO（リスク担当 Chief Risk Officer）を委員長として、企業内部のさまざまなリスクを一元的に管理し、経営者層にタイムリーにインプットし、指示を受けて対応するためのリスクマネジメント体制として構築されたリスクマネジメント委員会の構成を示したものである。

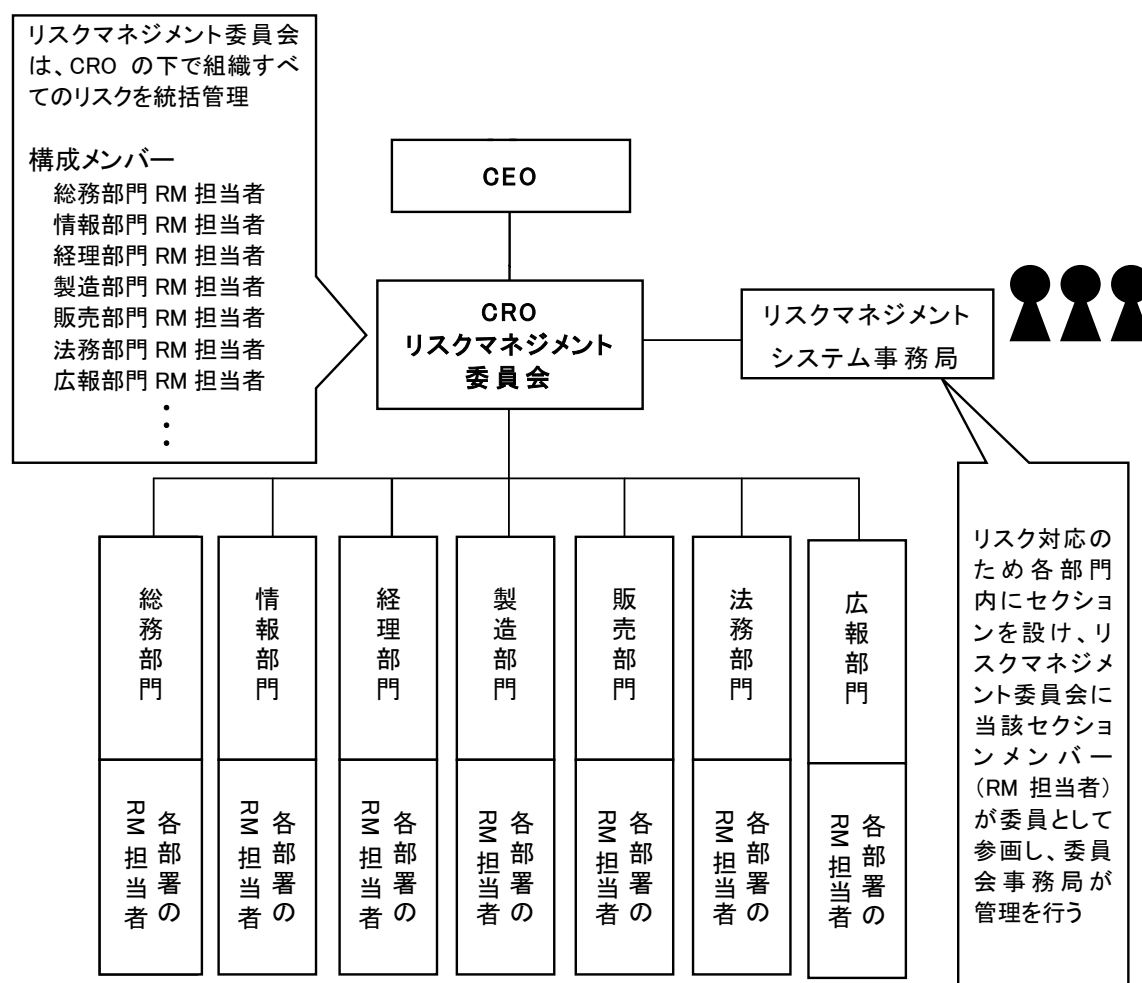


図 2-2-1. X 社のリスクマネジメント委員会

たとえば、自然災害・事故・事件、製品製造・販売・サービストラブル、コンプライアンス、情報セキュリティ、環境、個人情報等、企業内部のリスク情報を各部署のリスクマネジメント担当者（RM 担当者）から構成されるリスクマネジメント委員会に集約し、リスクマネジメント方針を役員会ならびに取締役会に報告することを想定している。したがって、リスクマネジメント委員会では、全体最適の観点からリスクを分析し、リスク対策を検討し、各部門においてリスクマネジメントをブレークダウンして展開する仕組みが構築されている。

なお、各部門内から選出されたメンバーからなるリスクマネジメント委員会に事務局を設置し、組織のリスクマネジメントをシステムとして PDCA（Plan-Do-Check-Act）を動かす重要な機能を持たせている。

JRMS2010 は、こうした側面を考慮に入れながら、リスクマネジメント委員会において組織のリスクマネジメントの実践的な方向性について検討し、個人情報、環境¹⁰、医療、J-SOX など、さまざまな分野におけるリスクマネジメント方法として統合的なリスクマネジメントに利用できる方法論とツールを検討し、社会に公表することが望ましいと考え、図 2-2-2 に示すように構造化したのである。

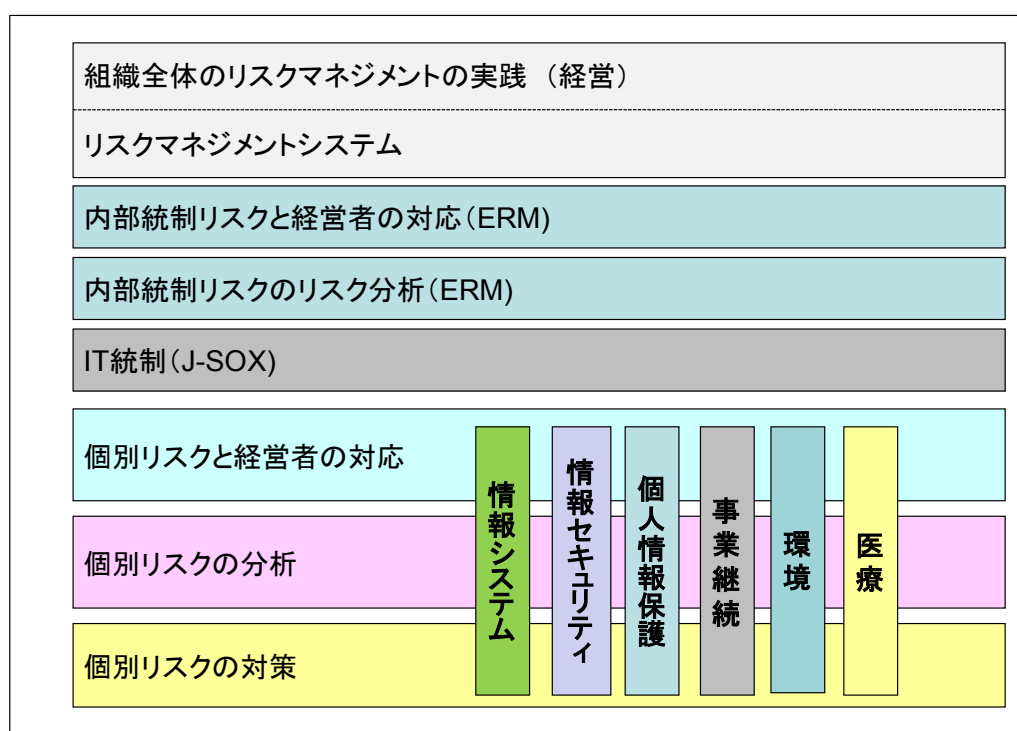


図 2-2-2. 組織のリスクマネジメントのための統合化ツール構想と JRMS2010

10 「5.1 JRMS2003 について」で紹介している JRMS2003 は、全社的なレベルと情報システムの二つに分けてリスク管理を分析するツールであるが、情報システム以外については、全社レベルのⅠ章とⅡ章を利用するに留まっていた。しかし、その後 2004 年度に作成された「個人情報保護編」はツールとして提供されなかったこともあり、あまり普及しなかった。一方、大阪大学工学部環境工学科では、環境リスクを企業組織の観点から検討するための演習型の講義を 2005 年から始め、JRMS2003 を利用した組織リスクの学習を始めた。この中で、環境リスクに対応するツールとして、JRMS2003 が発展できることがわかった。

ここでは、特定の分野に特化してリスクマネジメントを行うこともありうるが、組織の存続を追求するために組織全体のリスクマネジメントを見ながら、全体の予算の範囲内においてできるだけ効果的なリスク戦略を立て、実行できるように構成するのが重要と考えている。したがって、JRMS2010は“組織全体のリスクマネジメント”および“組織のリスクマネジメントシステム”をチェックするため、組織に共通する質問項目から構成されている。

特に、医療分野を取り入れたのは、JIS Q 2001におけるリスクマネジメントシステムがあらゆる組織を対象にしていること¹¹、また、医療機関経営の特殊性を考慮に入れたとしても、経営という視点は同じであると考えられなくはない、との見解が背景にある。また、医療領域に係るパンデミックリスクの問題は組織にとっても無視できない領域であり、そうした認識のもとで医療領域をJRMSに取り込んだわけである。

さらに、JRMS2010では組織の内部統制の構築と2008年度の会計年度から義務づけられるIT統制の評価に利用できるシステムを考慮し、開発している。

JRMS2010は上記に述べるような視点で構成されているが、JRMS2010における“組織全体のリスクマネジメント”では、ISO31000のリスクマネジメントをベースにして組織全体のリスクマネジメントを分析できるように構成されている。また、組織がリスクマネジメントを効率よく実施するために、リスクマネジメントシステムを導入することになる。JRMS2010の“組織のリスクマネジメントシステム”では、このプログラムの実施状況について経年的に分析することができるような仕組みも検討対象とされている。

2.2.4 JRMS2010の構造ーリスクマネジメント意思決定の流れー

JRMS2010の構造において重要な点は、ツール自体を大幅に改善したこと、さらに現状のリスクマネジメントの対象領域を考慮し、質問項目について改編を行ったことである。たとえば、JRMS2010では全体を二つに編成し、「第1部 組織経営とJRMS（経営編）」において組織全体を対象とし、経営に関する質問項目に焦点を当て、第1章「組織全体のリスクマネジメントの実践」、第2章「内部統制リスクと経営者の対応（ERM）」、第3章「内部統制リスクのリスク分析」、第4章「IT統制（J-SOX）」からなる4章構成とした。

「第2部 JRMSと個別リスク対応（各論編）」は、特定の領域に焦点を当て、関係機関により利用可能な質問構成とした。たとえば、後掲の「図2-2-5 JRMS2010第1部・第2部の位置づけ」に基づき、第1章「情報システム（企画・開発）とリスク対応」、第2章「情報セキュリティとリスク対応」、第3章「個人情報保護とリスク対応」、第4章「事業継続のためのリスク対応」、第5章「環境とリスク対応」、第6章「医療とリスク対応」という構成を考えている。

（JRMS2010の質問構成については、後述の「2.2.5 JRMS2010における回答者と質問票の構成」を参照のこと）

JRMS2010は、「図2-2-3 JRMSの構造」に示されているように、組織のミッションの実現のため、経営目標を設定することから出発する。

11 この点は、2009年秋に公表されるISO31000における展開においても基本的に同様である。

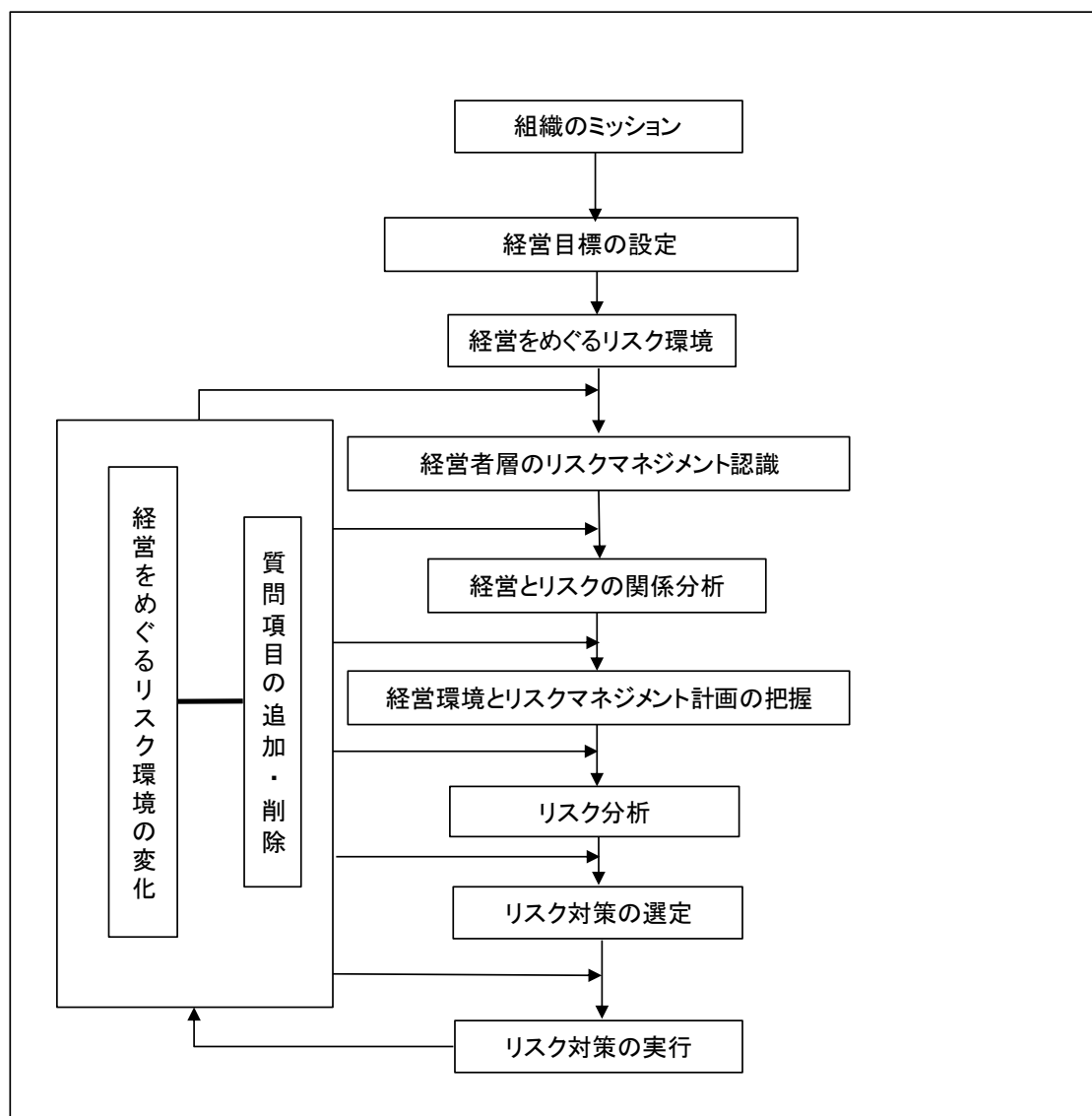


図 2-2-3. JRMS の構造

とりわけ、組織をめぐる経営環境の変化が著しい昨今、経営者層はリスク環境の変化を視野に入れる必要がある。経営者層のリスクマネジメント認識によるため、JRMS の質問構成もこの点に重点が置かれている。その上でリスクマネジメント計画を策定し、リスクを分析し、その結果を踏まえ、リスク対策を選定し、実行に移すという PDCA のマネジメントサイクルを動かすことになる。

なお、JRMS2010 は JRMS2003 に比べ質問項目を重点化・選別して項目数を少なくするとともに、回答時間を短縮できるよう JRMS ツールの利便性を高めている。また、第 5 階層についても、現在回答の仕方を工夫するように鋭意検討している。

また、回答者間のリスクに関する認識をもとに調整するための集計結果を表示しやすくし、回答結果についての個々の差異（バラツキ）の原因を究明しやすくしている。

ここで大事なことは、回答結果の差異（バラツキ）の原因を究明し、レーダーチャートで示される平均化された値とのギャップの原因がどこにあるのか、いかなる理由により発生したのか、

回答者間で意見交換を行い、リスクマネジメントの実態を認識し、ベンチマークアップを含め、望ましい方向に持っていくには何をどうすればよいのかを検討することである。回答者間で得られた共通の認識により、リスクマネジメントの実体について組織として妥当な方法を見出し、改善に結びつけるところに JRMS の構造特性がある。図 2-2-4 は JRMS の回答プロセスを示したものである。

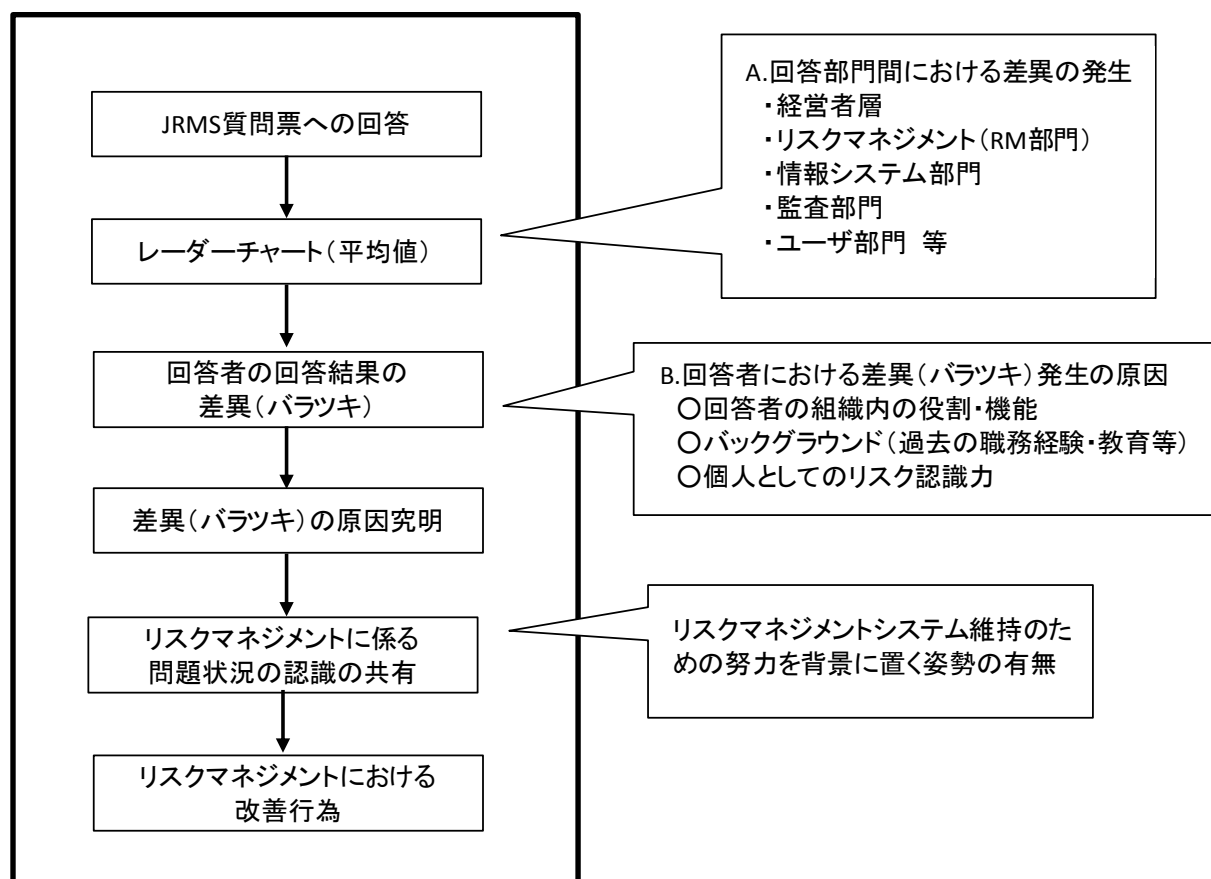


図 2-2-4. JRMS の回答プロセス

2.2.5 JRMS2010 における回答者と質問票の構成

JRMS には既述のように組織の脆弱性を把握するためにいくつかの特徴がある。その特徴は、組織のリスクマネジメントの実践に関して回答者の属する部門間と共に回答者間の認識の共有が組織のミッション達成にきわめて重要であることから、システムツールに回答者の区分を設定できるよう構成されていることである。この点については、回答者の組織における職能なり、責任の所在に関して組織図を質問項目との関連から示しておく。

また、質問は既述のとおり 2 部編成とし、かつ質問項目の理解を深めるために、項目にキーワードを設けて階層化している。ここではこれらの点について簡潔に示しておくこととする。

2.2.5.1 回答者

JRMS2003、JRMS2010 共に回答者の区分として基本的に経営者層、リスクマネジメント部門、ユーザ部門の三つを置くことに変わりはない。経営者層は CEO（Chief Executive Officer 最高経営責任者）、COO（Chief Operating Officer 最高業務執行責任者）、CFO（Chief Financial Officer 財務執行役員）、CRO（Chief Risk Officer リスクマネジメント執行役員）、CIO（Chief Information Officer 情報システム執行役員）等、ユーザ部門の役員を想定している。

リスクマネジメント部門は、組織の中核である社長室、経営企画部、総務部など全社的なリスクマネジメントを司る部門を想定している。個別リスクの管理においては、全社に指示を出すスタッフ部門もここに該当すると考えてよい。ユーザ部門は営業、購買、経理、人事、製造、サービスなど組織の最前線を担う部門である。

一般に経営者層は経営全般のリスクを把握する責務があり、リスクマネジメント部門（担当責任者）は経営に関わるリスクの分析・対応に責務があるとされている。

現在の組織は相互依存関係がこれまで以上に密になっており、一つの部署の問題（制約条件）が他の部署に大きな影響を与え、結果として経営そのものにも影響が及ぶようになっている。

このような現在の経営環境下において、たとえば情報システムのリスクマネジメント責任者は、自部門のみでなくユーザ部門などのあらゆる部門との接点のもとでリスクに対応することが非常に重要となってきた。ある一つのリスクが組織全体のすべてに作用する現在の環境下では、それぞれのリスクの統括部門が自部門だけのリスクに目を配るだけでは十分とはいえなくなってきた。そのため、リスクマネジメントに関する部門は経営全般に関わるリスクについても理解し、リスクマネジメント部門と協同してリスク対応を図ることが大切である。

実際にリスクマネジメントを実施しようとする場合には関係者の共通認識が不可欠であり、とりわけ経営者層の関わりが重要である。

JRMS の質問項目では、経営者層の部門を設けることで経営者層が関与（回答）することにより、経営者層のリスクに対する関わりが強くなる。これによって全社的なリスクマネジメントの有効性が確保されることになる。

2.2.5.2 質問票の構成

JRMS2010 では質問項目の構成を大きく変更した。「2.2.1 JRMS の基本的特徴」でも触れたように、全体を 2 部構成としている。「第 1 部 組織経営と JRMS（経営編）」は経営全般に関わるリスクマネジメントに関するものとし、さらに全体を 4 章構成としている。第 1 章「組織全体のリスクマネジメントの実践」、第 2 章「内部統制リスクと経営者の対応（ERM）」、第 3 章「内部統制リスクのリスク分析」、第 4 章「日本版内部統制（JSOX）の中の IT 統制」とした。

第 1 章は全社的なリスクマネジメントを実践するための項目で、JIS Q 2001 および今回新たに制定される ISO31000 を先取りした質問項目を設定した。

第 2 章以降については、現在経営に求められている内部統制の観点から経営を見つめるための項目建てとした。

第 2 章「内部統制と経営者の対応（ERM）」は、金融庁企業会計審議会が 2007 年 2 月 15 日に示した「財務報告に係る全社的な内部統制に関する評価項目の例」を参考にしている。ただし、金融庁の示した指針が主に財務報告の適切性に関するものに絞られていることに対し、内部統制

の考えそのものは経営の効率性、コンプライアンス、資産の保全など、経営全般の観点も含まれるため、幅広く応用できるように質問項目を工夫した。

第3章「内部統制リスクのリスク分析」は、第2章の内部統制のチェック項目が表面に顕在化した事象に関して評価する項目建てであるが、第3章は、それらの項目が現れる前の内面的な脆弱性を浮彫りにする評価項目を設定している。たとえば事務ミスが多いという場合であってもそれが要員の能力なのか、事務処理数なのか、IT活用度の問題なのか、ビジネスプロセスの変化速度の問題なのかについて掘下げができる質問項目を取り入れている¹²。

第4章「IT統制」は、金融庁の示した内部統制の実施の中でも特にITの活用に言及されていることを考慮し、それを実現するためのIT統制の項目を取り入れている。

第2部は、第1章が経営全般のリスクを扱うものに対し、個別のリスクを取り上げており、社会的また経営的に関心度合いの高いリスクの各論編としている。JRMS2003では前半が経営全般、後半がITリスクとしたが、その後半にあたる部分である。

第1部と第2部（概要）の位置づけは図2-2-5のとおりである。

第1部	組織経営とJRMS(経営編)
第1章	組織全体のリスクマネジメントの実践（経営）
第2章	内部統制リスクと経営者の対応（ERM）
第3章	内部統制リスクのリスク分析（ERM）
第4章	IT統制
第2部	JRMSと個別リスク対応(各論編)
第1章	情報システム(企画・開発)
第2章	情報セキュリティ
第3章	個人情報保護
第4章	事業継続
第5章	環境
第6章	医療

図 2-2-5. JRMS2010 第1部・第2部の位置づけ

第2部「JRMSと個別リスク対応（各論編）」では主要なリスクとして情報システム、個人情報保護、環境、事業継続の各分野を取り扱う。さらに、重要な社会基盤である医療経営に関する経営も含めた全般的な対応について第2部で取り扱うこととする。

このように、JRMS2010は第1部と第2部に大きく分かれているが、経営全般の取組みに加えて各論の個々のリスクをも合わせて総合的な評価ができるようにシステム設計を行っている。

¹² 第3章「内部統制リスクのリスク分析」の評価項目作成にあたっては、甲良好夫堀裕監修・伊藤勝教著「インターナルコントロール 内部統制システム構築の手引き」を参照させていただいた。

2.2.5.3 質問票の階層構造

JRMS 質問項目は質問票にまとめられているが、質問項目は単純に羅列されているのではなく、一定の規則に従い、全部で 5 階層の階層構造で構成されている。

以下、質問票の階層構造について解説する。

(1) 質問票の大項目（第 1 階層・第 2 階層）について

質問票は四つの大項目で構成されており、それぞれが第 1 階層項目を構成している。

第 1 階層項目は各章番号にあたる。内容例は表 2-2-1 のとおりである。

表 2-2-1. JRMS2010 の第 1 階層項目

	第 1 階層	
経営全般に関するリスクマネジメント	I	組織全体のリスクマネジメントの実践
内部統制に関するリスクマネジメント	II	内部統制リスクと経営者の対応 (ERM)
	III	内部統制リスクのリスク分析
	IV	IT統制

質問項目は第 1 階層と第 2 階層によってカテゴリ化されており、第 2 階層項目を構成する内容は表 2-2-2 のとおりである。

表 2-2-2. JRMS2010 第 2 階層項目 (Advanced 編)

階層	タイトル
1	組織全体のリスクマネジメントの実践
1-1	経営環境の変化とリスクに対する組織文化の醸成
1-2	リスクマネジメントシステムの基盤
1-3	リスクアセスメント
1-4	組織のリスク対策
1-5	リスクマネジメントシステムの維持
1-6	リスクマネジメントシステムの継続改善
1-7	文書化に関する要求事項
2	内部統制リスクと経営者の対応 (ERM)
2-1	統制環境
2-2	リスクの評価と対応
2-3	統制活動
2-4	情報と伝達
2-5	モニタリング
2-6	ITへの対応

階層	タイトル
3	内部統制リスクのリスク分析
3-1	リスク分析の構築
3-2	経営の観点によるリスクの分析
3-3	リスクを発生させる根本原因の分析
4	IT 統制
4-1	IT 全社的統制

第 1 階層、第 2 階層、第 3 階層の各階層の主要な内容はキーワードとして示されており、さらに 4 階層、5 階層の質問項目を含め、識別コードが付けられている。

(2) 第 3 階層について

第 3 階層は、第 2 階層を構成するキーワードに係る質問項目のタイトルを明示し、その質問項目を通して組織の実態が把握できるように階層化されている。特に第 3 階層は、第 4 階層の回答対象となる質問の評価項目のタイトルを示しており、レーダーチャートにおける重要な評価軸を表すことになる。しかも、組織なり回答部門における質問項目の重要性に鑑みて、JRMS ツールでは重みづけ（ウエイト）による修正が可能となっている（図 3-1-1 を参照）。したがって、重みづけの修正により、第 3 階層の意味づけが大きな影響を組織のリスクマネジメントに与える場合がある。

(3) 第 4 階層と第 5 階層について

第 3 階層の質問項目に対する回答結果が評価軸を通して明らかにされるため、第 4 階層・第 5 階層には具体的な質問項目を設定している。これらの質問項目は識別コードによって明らかにされており、それぞれの質問に対してなされる回答の結果が集計され、分析が行われることになる。

階層構造化された質問項目の一例は表 2-2-3 のとおりである。

表 2-2-3. JRMS2010 の階層別項目例（第 1 章 Advanced 編）

階層	キーワード	キーワード	識別コード	質問項目
第 1 階層	経営とリスク	経営とリスク	1	組織全体のリスクマネジメントの実践
第 2 階層	リスクアセスメント	リスクアセスメント	1-3	リスクアセスメント
第 3 階層	リスク評価	リスク評価	1-3-(3)	リスク評価
第 4 階層	評価方法	経営者の関心	1-3-(3)-1	Q 評価対象に関するリスクの評価方法は明確ですか？
第 5 階層		制度の明確化	1-3-(3)-1-①	Q 評価に必要な分析の精度を明らかにしていますか？
		技術的・作業量の妥当性	1-3-(3)-1-②	Q その精度は技術的・作業量的に妥当ですか？

(4) JRMS の効果的運用について

①JRMS 実行組織とリスクマネジメント体制

JRMS の効果的な運用を図るためには、組織化を図ることによる責任と権限の明確化が必要である。そのためには、JRMS の実行組織とリスクマネジメント体制を確立する必要がある。第 1 部では回答者の部門は経営者層、リスクマネジメント部門、ユーザ部門の三つであるが、IT 統制を評価する場合、および第 2 部のように個別のリスクマネジメントを合わせて検討する場合については、情報システムリスクマネジメント組織や各個別のリスクマネジメントの統括部門が存在する。その場合の考え方をあらかじめ説明する。

経営者層を除くと具体的なリスクへの対応にあたっては、IT 統制を例にとると、表 2-2-4 のような三つの実行組織に整理することができる。

表 2-2-4. JRMS2010 の実行組織（IT 統制を想定した場合）

組織名	実行担当
全社的リスクマネジメント組織	リスクマネジメント責任者 リスクマネジメント担当者 リスクマネジメント推進チーム (リスクマネジメント委員会、連絡会など)
	内部監査部門(内部統制の実施の場合)
情報システムリスクマネジメント組織	情報システムリスクマネジメント責任者 情報システムリスクマネジメント担当者 情報システム運用管理責任者 情報システム運用管理担当者 情報セキュリティ管理責任者 情報セキュリティ管理担当者 情報セキュリティ推進チーム
ユーザ部門リスクマネジメント組織	ユーザ部門リスクマネジメント責任者 ユーザ部門リスクマネジメント担当者 情報システム適用業務別オーナー

さらに、これらの実行組織を踏まえたリスクマネジメント体制の一例を示すと図 2-2-6 のようになる。

なお、表 2-2-4 は執行役員体制を考慮したものであるが、特に同種の体制を採用していない、または同様の実行組織が存在しない場合には、しかるべき適任者を任命し、リスクマネジメント体制を整えて JRMS の運用を図ることが望ましい。

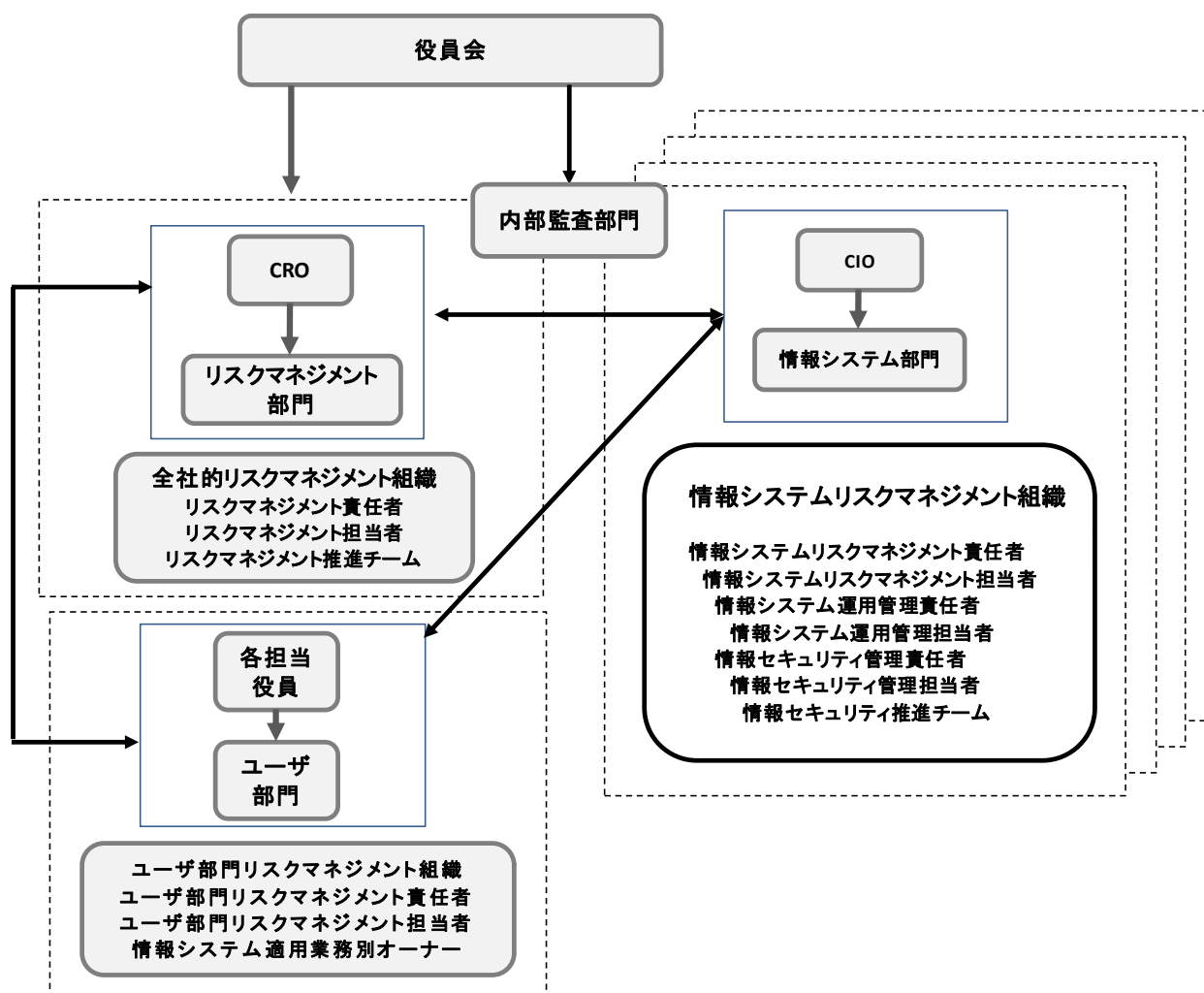


図 2-2-6. IT 統制を想定したリスクマネジメント体制

②JRMS の運用

図 2-2-6 に示したリスクマネジメント体制の一例に基づく JRMS の運用は、次のように行うことが理想的であり望ましい。（なお、各責任者、担当者、組織、部門などは専任、兼務を問わない）

(a) 全社リスクマネジメント組織

全社リスクマネジメント組織は、役員会の指示を受けてリスクマネジメント担当役員（CRO）が運営する。

ただし、CRO が社内で明確に任命されていない場合は、役員のうち適任者を役員会で任命してその任にあたらせる必要がある。

一般に CRO を補佐するために社長室、経営企画部、総務部などの部からリスクマネジメント部門を指名し、責任者（部長）、担当者（課長など）を任命する。また別途事業体を横断する形でリスクマネジメントチーム（リスクマネジメント委員会など）を設置することも望ましい。（役員レベルの横断組織を委員会、部門長や担当者レベルの横断組織をチーム、などと区別することもあるが、ここでいうチームは横断組織のことを指す。）

なお、内部統制の観点から全社的なリスクマネジメント組織の回答者に内部監査部門の内部監査人を加えることが望ましい。内部監査部門は CEO（社長）直属の部隊であり、CRO およびリスクマネジメント部門からも独立した存在である。

(b) 情報システムリスクマネジメント組織

情報システムリスクマネジメント組織は、情報システム担当役員（CIO）、または役員会で任命した適任者（以下、「CIO 等」という）の指示に従い、情報システムリスクマネジメント責任者が運営する。

この場合、CIO 等は情報システムリスクマネジメント担当者を兼務することができる。通常は情報システム部門が情報システムリスクマネジメント組織を担う。情報システムリスクマネジメント組織にはシステム運用管理、情報セキュリティなどの各組織が所属する。

IT 統制を評価する場合は、経営者層、リスクマネジメント部門、ユーザ部門に加えてこの情報システムリスクマネジメント部門も状況把握を行う単位となる。

なお、図 2-2-6 の右側の点線の枠は、CIO を中心とした情報システム部門と同様に、他の部門も関連するリスクマネジメント機能を展開する組織が想定されている。

(c) ユーザ組織

ユーザ組織はユーザ部門のリスクマネジメント組織を構築する。その中で情報システムリスクも取り扱うが、一般に情報システムリスクは情報システム部門（含む CIO 等）の指示に従い、情報システム業務別オーナーがリスク対応を実施する。（JRMS2003 ではこの点に焦点を当てていた。）

(d) JRMS 運用の役割と責任

先に示した質問の大項目（第 1 階層）のうち、第 1 章については CRO が、第 2 章の個別リスク（医療リスクを除く）については、各リスク統括の役員が（たとえば情報リスクであれば CIO 等）が質問票のそれぞれを適切に運用する役割と責任を持つ。

そして、JRMS 全体の総括的实施責任者は、社長の任命により各個別のリスク担当役員（情報リスクであれば CIO 等）が担当するのが JRMS の効果的運用上、望ましい。

(e) 第 1 章の回答にあたっての個別リスクの担当部門

各組織の実態により二通りの考え方ができる。一つは各リスクの統括者はリスクマネジメント部門の一員としてリスクマネジメント部門で回答する。もう一つは、各部門のリスクの責任者は全社的なリスクマネジメントに関してはユーザ部門として回答する。これらはどちらが正しいというものではなく、各組織の全社的なリスクマネジメントの推進体制にあたって、全社の各部門がどのような関わりを持っているかによる。場合によっては、各リスクの統括部署であってもリスクマネジメント責任者はリスクマネジメント部門で、その他の一般社員はユーザ部門として回答してもよい。

2.2.5.4 JRMS の今後の計画

これまでリスク評価指針検討委員会は、およそ月 1 回のペースで委員会活動を実施し、課題となった点についてはメール作業を行い、検討の結果を今回の報告書に集約することになった。重要な点は、JRMS の質問票の完成度ならびに JRMS ツールの操作性を高めることにあった。

特に、同委員会としては JRMS2010 年バージョンの有効性の検証を重視し、JRMS2010 の公

表前に実証実験を行い、その結果を踏まえ、JRMS2010 が社会の期待に応えることができるようにツール化するのが使命であると考えている。

なお、JRMS2010 に関する 2008 年度および今後のスケジュールについて、参考としてその「工程表」を図 2-2-7 に示す。

今後の計画としては、2009 年度には第 2 部の質問票の完成、さらに第 1 部の英語バージョンの作成を考慮に入れ、海外展開を視野に入れている。また、JIPDEC 内にサイトを設け、JRMS2010 に関するニーズへの対応、JRMS2010 の解説書作成、広報活動、研修会等の諸活動も予定に入れている。

平成20年度													
	4月	5月	6月	7月	8月	9月	10月	11月	12月	H22/1月	2月	3月	4月
委員会													
1. 質問項目作成													
(共有ベース)													
第1部													
第2部 (個別リスク)													
翻訳													
2. システム開発													
システム仕様 (設計～構築)													
実証実験													
改修													
サイト構築													
3. 報告書とりまとめ													
報告書作成													
4. 普及・広報活動													
解説書作成													
広報													
講演会													
研修													

図 2-2-7-1. 工程表 (2008 年度)

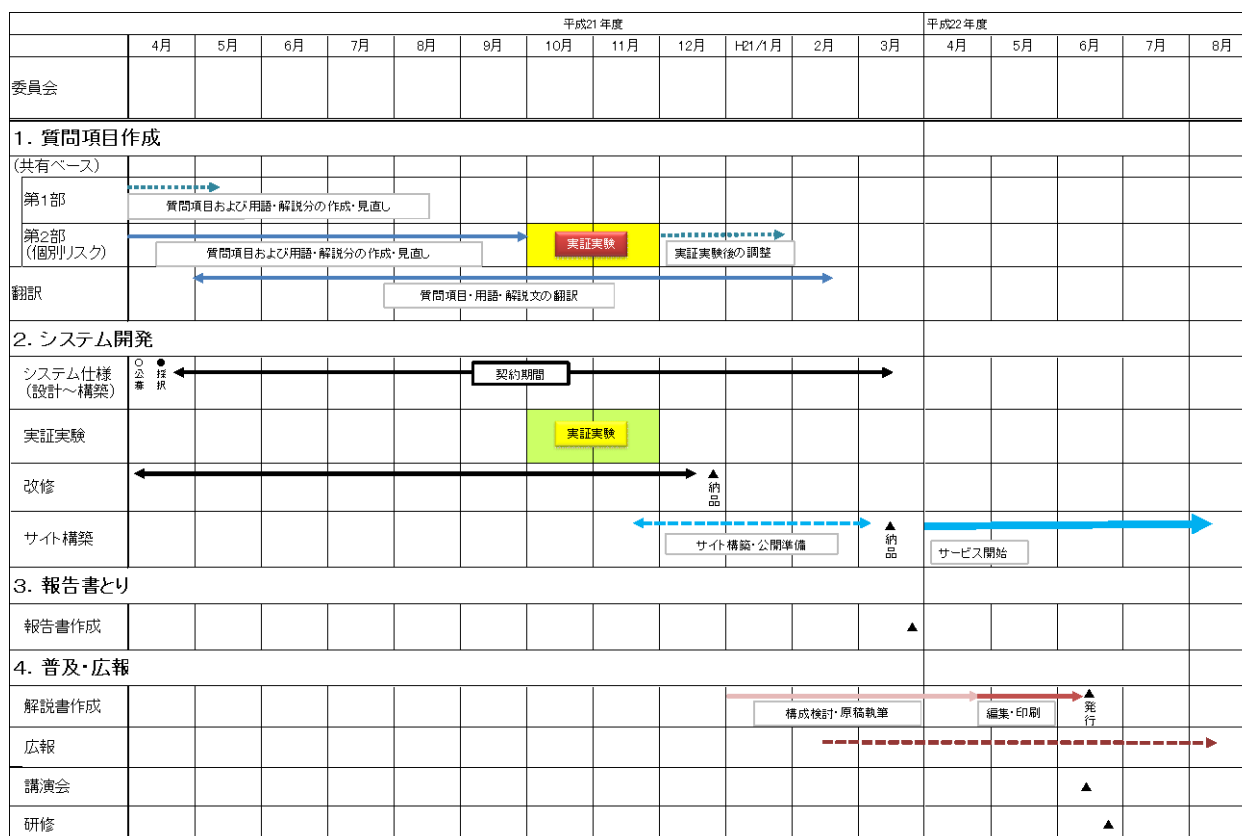


図 2-2-7-2. 工程計画表 (2009～10 年度)

3. JRMS2010 の構成

3.1 質問構成について

JRMS の目的は、組織全体としてのリスク対応の実態（現状）を JRMS 質問票の回答結果であるレーダーチャートを通して認識し、レーダーチャート上に表示された各部門（経営者層、リスクマネジメント部門、ユーザ部門）のリスク対応に関する認識のギャップを確認し、なぜ、そのようなギャップが生じたかについて関係各部門が話し合うことにより、組織として今後のリスク対応の方向性を共有化することにある。

JRMS は質問項目が中心であるが、質問項目は組織におけるリスクマネジメントのあるべき姿と実態とのギャップを確認し、組織としての効果的なリスクマネジメントを構築するために必要な情報を得るためのものとしてまとめられている。

JRMS は JRAM（「コンピュータセキュリティに関するリスク分析－JRAM によるアプローチ」）の方法論に基づき、さらに「JIS Q 2001 リスクマネジメントシステム構築のための指針」に沿って情報システムにおけるリスクを対象として展開した。今回の改訂で情報システムのみならず経営全般を対象とし、その中でも大きな関心分野である内部統制、環境、事業継続、情報システム、個人情報保護の分野に適用し、また個別業務においては医療経営に関するリスクへの適応を試みることにした。このため JRMS の質問項目は大きく二つの部分から成り立っている。

第 1 部「組織経営と JRMS（経営編）」は経営全般としてのリスクマネジメントを取り上げ、全体を 4 章で構成している。

第 1 章は「組織全体のリスクマネジメントの実践」とし、全社的なリスクマネジメントを行うための評価項目を整理している。JIS Q 2001 および ISO31000 と整合性を保ちながら JRMS のノウハウを活かした階層構造を構築している。

第 2 章から第 4 章は経営のリスクマネジメントを行う一つの手法である内部統制の考え方を取り入れた章立てとしている。第 2 章は「内部統制リスクと経営者の対応(ERM)」とし、金融庁が 2007 年 2 月 15 日に公表した「財務報告に係る全社的な内部統制に関する評価項目の例」を参考とした。

第 3 章は「内部統制リスクのリスク分析」とし、組織が対応すべき顕在化したリスクとそれを生み出す隠れた遠因分析を実施するための評価項目とした¹³。

第 4 章は J-SOX で求められる「IT 統制」に関する項目建てとした。この IT 統制は、金融庁の実施基準をベースとしているが、IT 全社統制、IT 全般統制、IT 業務処理統制については、2007 年 3 月 30 日公表の経済産業省の「システム管理基準（追補版）」を参考にして編成した。ただし、質問内容については実施基準や追補版を参照しなくても回答できるように工夫している。

第 2 部「JRMS と個別リスク対応（各論編）」は組織経営上関心が比較的高いと想定される個別リスクへの対応である。JRMS2003 の第 3 章および第 4 章で展開した情報リスクの個別分析にあたる部分である。第 2 部では情報リスクの他に、個人情報保護、環境、事業継続の各リスクを

13 前掲脚注 12 に指摘。

テーマとするほか、他業種への適用が可能という観点で、医療経営についても検討する。

3.1.1 三つのバージョンについて

組織のリスクマネジメントやマネジメントシステムの導入のレベルにはいろいろな段階がある。統合的なリスクマネジメントシステムを構築している組織から、リスクマネジメントを取り扱う専門的なセクションを持たない組織までさまざまである。

また、組織においてリスクマネジメントを担当する人材には、リスクマネジメントについての深い知識がある担当者から初心者まで存在する。彼らの中には一つの分野には詳しいが、全社的な立場でのリスクマネジメントは初めてという場合もある。たとえば、現場で情報セキュリティのリスクマネジメントを実践した担当者が、全社の組織のリスクマネジメントを担当することになるようなことも多い。この場合、自己の経験を基にして、組織全体のリスクマネジメントを分析することになり、その場合は一部分には専門的なレベルを要求し、その他の部分には初心者的なレベルを要求する場合もある。加えて組織の経営者が手始めに、簡単に自社のレベルを評価したいというニーズもある。

JRMS2010 では経営リスクに関する第 1 部においても質問数が数百にのぼる。経営全般において網羅的にこれらの項目を定期的（1 年に 1 度など）に実施することは欧米においては一般化されている。日本においてもこれらの定期的に自己点検し自己評価する方法は、ISO のマネジメントシステムの導入により少しはなじみが出てきているが、まだ発展途上である。また、これらの評価方式がたとえ十分効果があることがわかっていても、取り入れにくさがあると発展の制約となりうることから、JRMS2010 では提供する質問項目について、その組織の発展状況や実施の目的において選択できる Advanced 編、Baseline 編、Quick Start 編の三つのバージョンを設定することとした。

Advanced 編	第 4 階層および第 5 階層のすべての質問を提供するバージョン
Baseline 編	第 4 階層の質問を提供するバージョン
Quick Start 編	第 4 階層の質問のうち重要な質問を選抜して提供するバージョン

JRMS の質問構成および Advanced 編、Baseline 編、Quick Start 編の三つのバージョンについてはいずれも本委員会で作成・設定したものであり、経済産業省の各基準や規定そのものに基づいたものではないことに留意願いたい¹⁴。

14 情報セキュリティマネジメントシステムの情報資産の評価などではベースラインアプローチと詳細リスク分析を組み合わせるとよいとされている。このベースラインアプローチは詳細リスク分析とは異なり、リスクそのものを評価するのではなく、ある“ベースライン”として何らかの基準やガイドラインなどの管理策を“ベースライン”の対象とし、その管理策を網羅的に参照し適宜補強することで一定の情報セキュリティ水準を確保する方法である。一方 JRMS の Baseline 編は JRMS 全体の質問構成のうち、設問の重要度、優先度、難易度、詳細度などから質問をピックアップした状況で 3 段階に分けたものの中でベースとなるものという意味で Baseline という用語を用いているので混同しないように留意願いたい。なお JRMS の質問項目（三つの編のどれでも）をベースラインアプローチの“ベースライン”として用いることは問題ない。

JRMS の質問項目には五つの階層がある。このうち第 1 階層～第 3 階層は質問のカテゴリを適宜分類しており、レーダーチャートを作成する際の得点集計の軸となる。第 4 階層は評価項目そのものであり、成熟度モデルにより得点評価を行う階層であり、基礎項目となる。この第 4 階層を評価するにあたり補足の評価項目を設定する場合があります、それが第 5 階層の質問項目である。

第 5 階層のある質問項目については第 5 階層を Yes/No で回答する。場合によっては知らない D/K、適応外 N/A で評価する。階層構造を持つこれらの質問をまず評価し、この状況を踏まえて第 4 階層の 0～5 の得点をつける。

以下に質問の階層例（表 2-2-3）を再掲する。（「2.2.5.3 質問票の階層構造」を参照のこと）。

表 2-2-3. JRMS2010 の階層別項目例（第 1 章 Advanced 編）

階層	キーワード	キーワード	識別コード	質問項目
第1階層	経営とリスク	経営とリスク	1 組織全体のリスクマネジメントの実践	
第2階層	リスクアセスメント	リスクアセスメント	1-3 リスクアセスメント	
第3階層	リスク評価	リスク評価	1-3-(3)	リスク評価
第4階層	評価方法	経営者の関心	1-3-(3)-1	Q評価対象に関するリスクの評価方法は明確ですか？
第5階層		制度の明確化	1-3-(3)-1-①	Q評価に必要な分析の精度を明らかにしていますか？
		技術的・作業量の妥当性	1-3-(3)-1-②	Qその精度は技術的・作業量的に妥当ですか？

参考までに、JRMS ツールで第 4 階層の回答結果から集計した評価点を基に第 1～第 3 階層のレーダーチャートを作成するにあたり、評価点に重みづけをして集計した状態を図 3-1-1 に示す。（なお、これらの重みづけ値は集計の際に変更が可能である）

このとき、Advanced 編においては、すべての第 5 階層が対象となり、この回答結果を参考にしながら評価者は最終的に 0～5 の評点をつける。第 5 階層に No が多いにもかかわらず第 4 階層が高得点になったりすることを防ぐために、Yes の数を参考に第 4 階層を評価する。なお D/K は No (=0) と同じ扱い、N/A は計算対象外と設定している。

この方式ではすべての項目の評価を行う必要があるため、慣れていない場合などは評価ロードが多いために普及しない可能性があるかと判断し、Baseline 編として第 5 階層を表示および評価を行わないバージョンとして提供することとした。Baseline 編を選択した場合は第 4 階層を直接評価することができ、評価ロードを削減できる。ただし当然のことながら第 5 階層のきめ細やかな判断を踏まえての評価ではないことに留意する必要がある。

さらに、経営者層を踏まえて概括的に現状を捉えたいなどのニーズに対応することも本ツールの普及には必要であり、また組織のニーズもあることから、第 4 階層の中から特に重要な項目を抜き出して評価することができる Quick Start 編を設定した。これらは質問数を絞り込み、重点として押さえるべきとしたものであるため、概括的に組織の実態を把握することには適しているが、詳細を把握していることではないことに留意する必要がある。

設問選択		回答入力		集計操作		評価処理		設問設定		システム設定		ログアウト							
回答年月: 2008年度第3四半期		部門: 経営層		期間・部門選択		重み初期化		重み集計											
集計表示／重み設定										2階層		3階層		4階層					
										点数	配点	点数	配点	点数	配点				
第4章_J-SOX(IT全社統制)										3.8	100								
4-1: IT全社統制										3.8	100	3.8	100						
4-1-(1): IT全社統制												3.3	50	3.3	100				
4-1-(1)-1: 経営者の関心														3.6	20				
4-1-(1)-2: ITに関する戦略、計画、予算等の策定および体制の?														3.6	20				
4-1-(1)-3: ITにかかる教育、研修方針														3.4	20				
4-1-(1)-4: ITに関連するリスク評価方針														2.6	20				
4-1-(1)-5: IT全統制およびIT業務処理統制に関する方針およ														3.4	20				
4-1-(2): IT全統制												4.2	50	4.2	100				
4-1-(2)-1: データの信頼性のリスク														3.6	20				
4-1-(2)-2: コードやデータの改変														4.2	20				
4-1-(2)-3: テスト方針と手続														4.2	20				
4-1-(2)-6: 情報セキュリティフレームワーク														4.6	20				
4-1-(2)-8: 情報セキュリティインシデントの管理														4.6	20				
										重みづけ値									

図 3-1-1. JRMS ツールによる重みづけ集計例

JRMS ツールは各組織の取組状況に応じて適宜これらの三つの編を使い分けることも有効である。「組織全体のリスクマネジメント」および「組織のリスクマネジメントシステム」を分析する場合、組織のリスクマネジメントの取組み段階に応じて、三つのレベルを用いることができる。まず、簡単に組織のリスクマネジメントに取り組めるように **Quick Start** 編を用いる。次に、組織のリスクマネジメントに慣れ、リスクマネジメントが実施されている組織となれば **Quick Start** 編では不十分になるので、組織のリスクマネジメントとして必要と考えられるレベルとして **Baseline** 編を用いる。さらにリスクマネジメントに長けてきたら詳細に組織のリスクマネジメントを分析できるように、**Advanced** 編を用いる。また、毎回 **Advanced** 編ではロードが大きいと判断する場合は、「3年に1回は **Advanced** 編で網羅的にチェックする。**Quick Start** 編で対応ができているところを **Baseline** 編で詳細確認を行う。」などの対応も可能である。

これらの分析に一貫性を持たせるため、三つのレベルには包含関係があるように構成されている。すなわち、リスク分析の質問項目は **Advanced** 編 $\supset$ **Baseline** 編 $\supset$ **Quick Start** 編としている。なお、**Quick Start** 編で分析できるのはリスクマネジメントにおける必須の項目に絞り込まれているため、これだけでリスク分析が十分と考えるのは早急である。JRMS2010 では、**Quick Start** 編から取り組み、組織のリスクマネジメントが成熟するに従い **Baseline** 編に移り、最終的には **Advanced** 編に評価を進めていくように質問項目が構成されていることに留意願いたい。

JRMS を初心者が利用する場合には、最初に Advanced 編からではなく、Quick Start 編からスタートして早めに全体像を掴んでほしい。Quick Start 編でもそれなりの組織のリスクについて分析が可能である。Quick Start 編で利用の仕方を学んでから Baseline 編を利用すると理解が容易になると考えている。なお、質問項目数の違いを表 3-1-1 に示す。

表 3-1-1. 三つのレベルによる質問項目数の違い

タイトル	Quick Start 編	Baseline 編	Advanced 編
1.組織全体のリスクマネジメントの実践(Ver.7)	36	63	137
2.内部統制リスクと経営者の対応(Ver.5)	12	35	70
3.内部統制リスクのリスク分析(Ver.5)	37	81	180
4.IT 統制(Ver.5)	20	54	81
計	105	233	468

注) 質問項目は随時見直しを行っているため、報告書とりまとめ時点での質問数を記載する。

3.1.2 JRMS2010 の構成

3.1.2.1 第 1 章「組織全体のリスクマネジメントの実践」

JIS Q 2001 および ISO31000 の評価項目と整合性をとり、組織全体、つまり会社全体で取り組むべきすべてのリスクを対象とした、リスクマネジメントを実施する上で必要な基礎項目をまとめている。継続的改善の考えを取り入れ、計画のみならず実践性、定着化をも考慮している。

主な項目は以下のとおりである。(Advanced 編)

- 1.1 経営環境の変化とリスクに対する組織文化の醸成
 - 1.1.1 組織のミッションと経営方針の明示
 - 1.1.2 コミュニケーションに関する事項
 - 1.1.3 当該組織と外部環境に関する的確な把握
- 1.2 リスクマネジメントシステムの基盤
 - 1.2.1 方針
 - 1.2.2 計画
 - 1.2.3 リスクマネジメント方針の明確化
 - 1.2.4 リスクマネジメントの実効性
 - 1.2.5 リスクマネジメントシステムの実効性
- 1.3 リスクアセスメント
 - 1.3.1 リスクの特定
 - 1.3.2 リスク分析
 - 1.3.3 リスク評価

- 1.4 組織のリスク対策
 - 1.4.1 リスク対策のメニュー
 - 1.4.2 リスク対策の選定
 - 1.4.3 リスク対策の実行
 - 1.4.4 リスク対策の効果
- 1.5 リスクマネジメントシステムの維持
 - 1.5.1 実行
 - 1.5.2 チェック
 - 1.5.3 改善
 - 1.5.4 マネジメントレビューの実施
- 1.6 リスクマネジメントシステムの継続改善
 - 1.6.1 リスクマネジメント記録管理
 - 1.6.2 リスクマネジメントに関する教育・訓練
 - 1.6.3 リスクマネジメントシステムのチェック
 - 1.6.4 リスクマネジメントシステムの改善
- 1.7 文書化に関する要求事項
 - 1.7.1 一般
 - 1.7.2 文書管理
 - 1.7.3 記録の管理

3.1.2.2 第2章「内部統制リスクと経営者の対応（総論）」

全社的な経営に関するリスクマネジメントを実施する場合の一つの方法論に内部統制の考え方がある。内部統制とは、コンプライアンスを遵守しながら組織を効率的に運用することを目的として、定められたコントロールへの遵守適合を自己点検監査することにより達成しようというものである。金融庁の示した主に有価証券報告書の適切性の確保、平たく言えば粉飾決算の防止のための評価項目を元に経営全体の評価にも応用できるように質問内容を工夫したものである。

主な項目は以下のとおりである。（Advanced 編）

- 2.1 統制環境
 - 2.1.1 経営
 - 2.1.2 経営組織
 - 2.1.3 経営実務
- 2.2 リスクの評価と対応
 - 2.2.1 リスク評価のしくみ
- 2.3 統制活動
 - 2.3.1 統制活動全般
- 2.4 情報と伝達
 - 2.4.1 情報共有と伝達に係る活動

2.5 モニタリング

2.5.1 モニタリング活動

2.6 IT への対応

2.6.1 IT による統制活動

3.1.2.3 第3章「内部統制リスクのリスク分析」

第3章は内部統制で対象とするリスクについて、まずリスク評価をする体制が適切かどうかを評価し、次に標準的な組織が直面する可能性のある、顕在化するリスクを網羅的に1回は認知し評価すること、および顕在化する事象を生み出すリスクの遠因となる組織の脆弱性について評価することを目的としている。いわゆるリスクの気づきに関する項目である。そのため2項、3項においてはリスクのチェックリストとしても用いることができる。

主な項目は以下のとおりである。(Advanced 編)

3.1 リスク分析の構築

3.1.1 リスク分析の仕組み

3.1.2 リスク分析の体制

3.1.3 リスク分析の実施

3.2 経営の観点によるリスク分析

3.2.1 リスク分析（戦略リスク）

3.2.2 リスク分析（財務リスク）

3.2.3 リスク分析（ハザードリスク）

3.2.4 リスク分析（オペレーショナルリスク）

3.3 リスクを発生させる根本原因の分析

3.3.1 プロセス

3.3.2 スタッフ

3.3.3 機械設備

3.3.4 資産管理

3.3.5 複雑性

3.3.6 処理ボリューム

3.3.7 技術

3.3.8 コンプライアンス

3.3.9 ストラテジ

3.1.2.4 第4章「IT 統制」

第4章は財務報告に係る IT 統制の対象とするリスクについて、三つの主要な分野に分けて評価している。まず、組織としての IT 統制に関するリスクを管理しているか、そのための方針や体制が構築されているかを評価する。次に、IT 全般統制として、IT 基盤についての四つの分野のリスクを管理できているかを評価する。最後に、業務処理に係る IT の部分についてのリスクの管理ができているかについて評価する。

この評価項目は、J-SOX の整備・評価でチェックする項目でもあるので、J-SOX の IT 統制に

係る整備評価、運用評価のチェックリストとして、大まかな弱点を見つける目的で利用することもできる。なお、JRMS2010 では複数年度にまたがる評価ができるので、IT 統制について経年的な変化を毎年記録することで、改善の度合いの進捗についてチェックすることができる。

主な項目は以下のとおりである。(Advanced 編)

4-1 IT 全社的統制

4.1.1 IT 全社的統制

4.1.2 IT 全般統制

4.1.3 IT 業務処理統制

3.2 成熟度モデルについて

3.2.1 JRMS2010 の成熟度モデル

JRMS2010 では、利用者が自組織のリスクマネジメントの現状を評価するために成熟度モデルの考え方を取り入れている。この場合の成熟度モデルとは、リスクマネジメントの各領域の管理プラクティスについて、どの程度のレベルに達しているかを評価するためのモデルである。JRMS2010 では、CobiT4.1 の成熟度モデルを参考に、リスクマネジメントの各領域について成熟度レベルを表 3-2-1 のように定めている。JRMS2003 では、わが国におけるリスクマネジメントの浸透度を考慮して、CobiT で定義している成熟度レベル 4 とレベル 5 についてはあえて外した定義とした。その後、わが国にもリスクマネジメントの考え方が浸透してきたことを受け、CobiT4.1 と同様にレベル 0～レベル 5 までの 6 段階定義とした。

また、成熟度 0～3 についてはリスクマネジメントの各領域で成熟度を判定する項目は同じであるが、成熟度 4 と成熟度 5 については、リスクコミュニケーションの項目を重視すべき領域と、リスクマネジメントプロセスの継続的な改善を重視すべき領域がある。これを概念的に図示すると、図 3-2-1 のようになる。

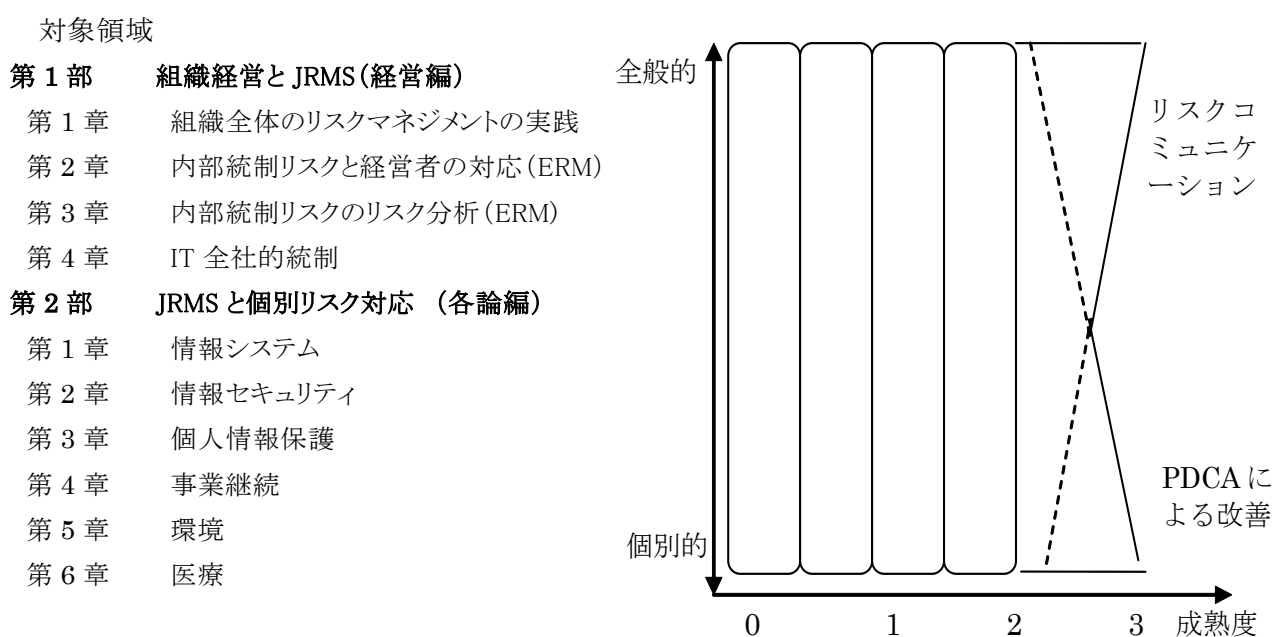


図 3-2-1. リスクマネジメントの対象領域と成熟度の定義

表 3-2-1. JRMS2010 の成熟度モデル（案）

評価レベル		定 義	摘 要 例	具体例 (パンデミックのリスクを対象に各レベルを例示)
0	未認識・未対応	対象のリスクに対して、インシデントの発生まで何の対応もしていない。	- 対象のリスクに対する認識もリスクを管理する認識もなく、対応方法について知識を持っている要員もいない。 - インシデントの発生により、最大限の被害を受ける。	- パンデミックに対しての認識がない。 - 事前の準備をしていない。
1	個人ごとの対応	対象のリスクに対して個人的な対応を実施している。	- 対象のリスクに対する認識や対応方法は、個人に依存している。 - 発生した個別のインシデントに対し、各個人が個人的な対応を行う。 - インシデントの発生による被害は、誰が対応したかにより、大きく異なる。	部門としての対応も決まっておらず、個人的にマスク等を備蓄している人がいる。
2	部門ごとの対応	対象のリスクに対する対応は部門ごとに統一されているが、全組織で統一した対応は行われていない。	- 同一のリスクに対して、支店等の部門ごとに対応が定められ、文書化もされている。 - 発生した個別のインシデントへの対応は、その部門では統一されているが、部門が異なると、違った対応がある。 - インシデントの発生による被害は、どの部門が対応したかにより、大きく異なる。	外部との接触が多い営業部門では、客先を除く外部でのマスク着用や、帰社時の手洗いとうがい呼びかけている。
3	全組織による対応	対象のリスクに対する対応が全組織で標準化され、組織的な承認を得ている。	- 同一のリスクに対して、全組織としての対応が定められ、の文書化が行われており、手続き等も定められている。 - 実施された対応にバラツキ・ブレがあっても、その把握はできていない。 - インシデントの発生による被害は、対応が外部から見える（外部に対し客観的な説明ができる）。	- パンデミック発生時の対応マニュアルが作られ、全組織に配布されている。 - 総務部が音頭をとり、パンデミック対応の関連部長会が作られている。
4	全組織による管理された対応	全組織での標準化された対応に加え、対象のリスクへの対応が基準どおり実施されているかを管理している。または、外部へのリスクコミュニケーションを行っている。	- 対応のバラツキやブレが、基準からの逸脱として把握されている。 - 一般公衆も含め、外部への情報開示が行われている。 - リスクマネジメントシステム改善のための仕組みがある。	パンデミック対応マニュアルの重要項目について、実施率が関連部長会で定期的に報告されている。
5	全組織による最適化された対応	管理された全組織での対応に加え、リスクへの対応を組織として継続的に改善している。または、リスクへの外部からのフィードバックを取り入れている。	- 外部のリスク管理について組織的な情報収集を行い、その情報をリスクマネジメントシステム改善の PDCA サイクルに活用している。 - 全社的な CSR 活動との連携が図られている。 - 外部への情報開示に対するフィードバックを取り入れる仕組みができています。	- 他組織でのパンデミック対応の情報収集に基づいて、産業医の意見も参考に定期的にマニュアルを見直している。 - 外部委託企業に対しても、対応の状況を確認している。

3.3 JRMS の使い方

組織はリスク分析を行うことで、どの領域のリスクマネジメントが改善されたかについて理解が得やすくなるが、JRMS は特にレーダーチャートにより改善度合いが可視化されることから、比較や目標との乖離についても把握しやすくなる。また、相対的にリスク項目を比較することができるので、対応の進んでいる分野と遅れている分野についても簡単に把握できる。経営者層はレーダーチャートを見ることでリスク対応の実態を容易に判断できることから、経営ツールとしても利用が可能である。

経年的にリスクマネジメントを捉えていくためには、次のような課題がある。JRMS2010 のリスクマネジメントでは成熟度によるリスク対応の評価をベースとしている。そのため、どうしても主観的な評価となる危険性がある。すなわち、評価者によって評価結果が異なる可能性と、同一の評価者であっても翌年に同一の判断ができるという保証がないからである。これには 3.2 章で述べる成熟度をいかに普遍的なものとするかという測度の問題と、これを利用してリスク項目を評価する評価者の問題がある。前者については 3.2 章で論じているのでここでは割愛するが、成熟度による評価を正確なものとするためには、評価者の成熟度による評価や質問項目による違いを事前トレーニングなどで矯正していく必要がある。後者については質問の内容を評価しやすく、ぶれがないような質問内容とする工夫が必要である。

組織内部での利用においては、経年的にリスクマネジメントを評価する場合、評価者が同一でない場合についても、比較評価ができることが求められる。これについては上記で述べたように、成熟度による評価が評価者によって恣意的に変わらない仕組みが必要である。これには質問項目で評価する前に評価結果を合わせるように、標準パターンを用いて評価が一致するようにすることで対応できると考える。

外部のコンサルタントが利用する場合は、評価者が JRMS2010 に精通していると考えられること、同一者が評価を実施することが多いと想定されることから、利用上における問題は少ないと考えられる。

3.4 JRMS の高度な使い方

JRMS2010 では次のような利用も可能である。

- (1) 質問項目をカスタマイズして利用する（たとえば、自社にそぐわない質問項目を削除し、自社に必須の項目を追加することができる）
- (2) 質問項目間の重要度を重みづけでカスタマイズすることができる。

分析では組織によって質問項目の持つ重要度が変わる。また、リスク項目では発生頻度の違いを考慮したいときもある。このような場合には、質問項目について重みを変化させることができる。

- (3) 質問に対する回答について第 4 階層では 0-5 の成熟度と N/A（Not Applicable；質問内容について回答できない）や D/K（Don't Know；質問内容が判断できない）での回答を設定することができる。なお、質問によっては、回答を必須項目と設定しうる項目もある。

第5層は0-5の6段階評価で回答するのではなく、Y/N (Yes/No)、N/A、D/Kで回答することになる。(図3-4-1参照)

- (4) 同一の質問項目を誰に回答させるかをカスタマイズすることができる。これにより、複数の部門に対して同一の質問をすることができる。
- (5) 回答部門に合わせて質問項目の内容(聞き方)を変更することができる。たとえば、「Q 経営者はリスクマネジメントの教育を実施していますか?」という質問について、リスクマネジメント部門に対しては、「リスクマネジメントとしての教育メニューを検討していますか?」、担当部門には、「リスクマネジメントの教育が実施されていますか?」というようにカスタマイズすることができる。すなわち、回答者に対して回答しやすいように同じ趣旨の質問を変更することができる。部門による同一の質問項目を聞くことで、その項目が実施されているかについてのギャップ分析が可能となる。

JRMS2010では、これらの機能を利用することで組織のリスクマネジメントを高度にカスタマイズすることができる。

個別KW	コード番号			質問項目(案)	解説文 オンマウスでツールチップ表示される説明	用語説明 マウスクリックで別ウィンドウ表示される説明文	備考 (コメント記入欄) 注)この欄は検討用のものです。最終的には削除します	部門別設問指定								
	(第1~3階層)	(第4階層)	(第5階層)					経営者層			RM部門			ユーザー部門		
								SECTIONA			SECTIONB			SECTIONC		
								回答	D/K	N/A	回答	D/K	N/A	回答	D/K	N/A
	1			組織全体のリスクマネジメントの実践												
	1-1			経営環境の変化とリスクに対する組織文化の醸成												
	1-1-(1)			組織のミッションと経営方針の明示												
組織のミッション	1-1-(1)	1		Q 組織としてのミッションを明らかにしていますか? (経)		ミッション: 設立目的、存在目的、組織化目的のこと		0-5	*	*						
				Q 組織としてのミッションは明らかですか? (RM、ユ)							0-5	*	*	0-5	*	*
経営目標の明確化	1-1-(1)	2		Q 組織のミッションを達成するための経営目標を明らかにしていますか? (経)		経営目標: ミッションを果たすために設定する経営としての具体的な成果目標		0-5	*	*						
				Q 組織のミッションを達成するための経営目標は明らかですか? (RM、ユ)							0-5	*	*	0-5	*	*
経営の優先順位の明確化	1-1-(1)	3		Q 経営の優先順位は、明らかになっていますか?		経営の優先順位: 経営においてどのようなことを達成することが、より重要であると考えているかということ 例: コンプライアンス(法令等の遵守)、顧客の安全、社員の健康、適正な利益の獲得等の何から確実に確保していくかということ		0-5	*	*	0-5	*	*	0-5	*	*
	1-1-(2)			方針												
マネジメント方針の確立	1-1-(2)	1		Q 自分の組織に相応しい経営方針を確立していますか?		経営方針: 経営目標を達成するための優先順位、投資等の考え方		0-5	*	*	0-5	*	*			
経営理念との連動	1-1-(2)	2		Q 経営方針は経営理念と連動していますか?		経営理念: 経営を行う際の基本的な考え方や価値観のこと。社是、社訓等がこれにあたる。		0-5	*	*	0-5	*	*	0-5	*	*
理解状況の確認	1-1-(2)	3		Q 経営方針の全社員への理解状況を確認していますか?	重要な施策に関しては、通達をするだけでなくその理解状況を把握することが、経営意思を徹底するためには大切です			0-5	*	*	0-5	*	*			
	1-1-(3)			計画												
リスクマネジメント計画	1-1-(3)	1		Q マネジメント方針に基づき計画を策定していますか? (経)		マネジメント方針・リスクマネジメント等を実施する際に、全員に徹底すべきことや重要な事項を定めたもの		0-5	*	*						
	1-1-(3)			Q マネジメント方針に基づき計画が策定されていますか? (RM、ユ)							0-5	*	*	0-5	*	*
負荷の把握	1-1-(3)	2		Q 計画達成に必要な負荷を把握していますか?		計画達成に必要な負荷: 計画しているリスクマネジメントを実施する際に必要となる人員、時間、経費等をいう。		0-5	*	*	0-5	*	*			
コンプライアンスの徹底	1-1-(3)	3		Q コンプライアンスの徹底を計画に入れていますか? (経)				0-5	*	*						
	1-1-(3)			Q コンプライアンスの徹底を計画に入られていますか? (RM、ユ)							0-5	*	*	0-5	*	*

図 3-4-1. JRMS2010 の質問シートの例

3.5 JRMS のサポート機能について

JRMS2010 では次のような機能がサポートされており、高度な分析が可能となっている。

(1) 質問項目の作成形式

質問項目は図 3-4-1 に示すように Excel 形式で作成し、これを xml 形式のプログラム入力ファイルに変換する。メインプログラムでは、この xml 形式のファイルを入力データとして読み込む。質問項目は組織におけるリスクマネジメントが進展するにつれて見直すことが必要である。しかし、xml 形式のファイルではファイルの修正が専門家以外には対応できないため、JRMS2010 ではこれを解決するために Excel 形式で質問文を修正、加除できるように作成している。

(2) 質問項目についてのグラフ化と統計数値

質問項目の分析結果は、回答データをファイルとして保存することやレーダーチャートを描いて分析できるようにしている。特に、レーダーチャートについてはカット&ペースト機能により、図 3-5-1 に示すように簡単にパワーポイントなどのファイルに貼り付けることができる。

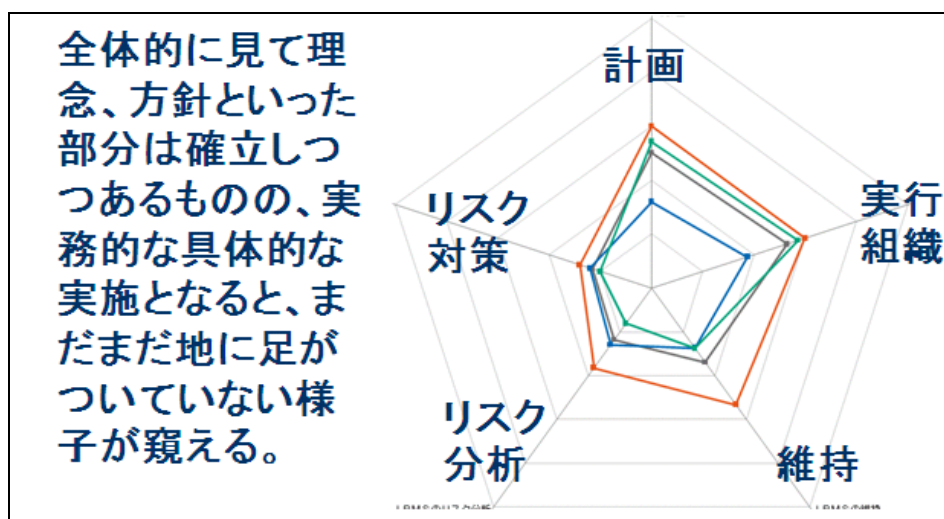


図 3-5-1. JRMS2010 の分析の例

さらに、質問項目の同一ジャンルにおける平均値や標準偏差が得られ、経年比較などを行いやすい。

(3) 分析データのエクスポート機能

分析データは Excel 形式で外部ファイルにエクスポートすることができる。これによって JRMS2010 のデータを用いてさまざまな分析が可能となる。

(4) 質問項目および回答データのファイル形式

質問項目および回答データは xml 形式のファイルとなっている。xml はデータの表現形式と

しては汎用性の高いものであり、今後、他のプログラムと質問項目および分析のコントロールデータを共有することも可能である。

3.6 JRMS ツール

JRMS ツールは JRMS で行う作業を直感的に、わかりやすく、効率的に行うことも可能としたツールである。

3.6.1 ツールの特徴

JRMS ツールには、組織におけるリスクマネジメントの実践をさらに進展させることができるように、以下の特徴を備えている。

(1) 回答組織に合わせた組織構成の登録

回答する組織の部門や、部門に所属する回答者を自由に登録することが可能である。この機能の実現により、本ツールで評価する組織が、より現実の組織に近い形で評価可能となる。

(2) 回答者のレベルに合わせた質問表現の設定

部門により質問の解釈や用語の理解が異なることが予想されることから、部門ごとに質問の表現を変更できる質問設定機能を提供している。

また、質問設定機能にはどの部門がどの質問に回答する必要があるか、あるいは回答対象から外すことも設定（N/A 設定）することもでき、回答者は全質問の中で関係する質問のみ回答をすればよい。

(3) 視覚や操作性に配慮した回答入力機能

回答者は大量の質問に回答しなければならないため、回答を短時間に入力するための画面構成、色使いに配慮した回答入力機能（図 3-6-1 参照）を提供している。

(4) 質問の理解を助けるヘルプ機能

回答者により JRMS で提供する質問の意図、概要、専門用語を理解するのは困難が予想される。このため、回答者がいつでも見たい時に質問の解説や用語説明の情報を表示するヘルプ機能（図 3-6-1 参照）を提供している。

(5) 直観的でわかりやすい評価結果の提示

評価結果をわかりやすく、かつさまざまな角度（経年、部門間、部門内回答者等）からの比較ができるような結果出力を可能としている。

評価結果はレーダーチャート（図 3-6-2 参照）で出力することを基本とし、質問に対する全回答データを一覧表示した集計表（図 3-6-3 参照）を表示することで、より詳細な分析も可能としている。

設問選択 一時保存 回答の登録 ガイダンス表示 ログアウト

IT統制 10 / 10

第4章_J-SOX(IT全社の統制)

4-1: IT全社の統制

4-1-(1): IT全社の統制

4-1-(2): IT全般統制

全体で何問の質問があるのか、また現在どの階層の質問項目を回答しているのか、一目でわかる

Q 経営者は、ITに対して、組織として計画を作成していますか？

0 1 2 3 4 5 D/K N/A

Q ITに関する戦略、計画、予算等の作成体制が整備されていますか？

0 1 2 3 4 5 D/K N/A

ITの戦略や計画、予算を策定するための組織が整備されていることが必要

Q ITに係る教育、研修に関する方針はありますか？

0 1 2 3 4 5 D/K N/A

Q 全社的なITに関連するリスク評価の方針はありますか？

0 1 2 3 4 5 D/K N/A

Q IT全般統制およびIT業務処理統制に関する方針および手続を制定していますか？

0 1 2 3 4 5 D/K N/A

質問の意味や用語解説を表示

次へ

図 3-6-1. 回答入力画面表示例（第4章 Quick Start 編より）

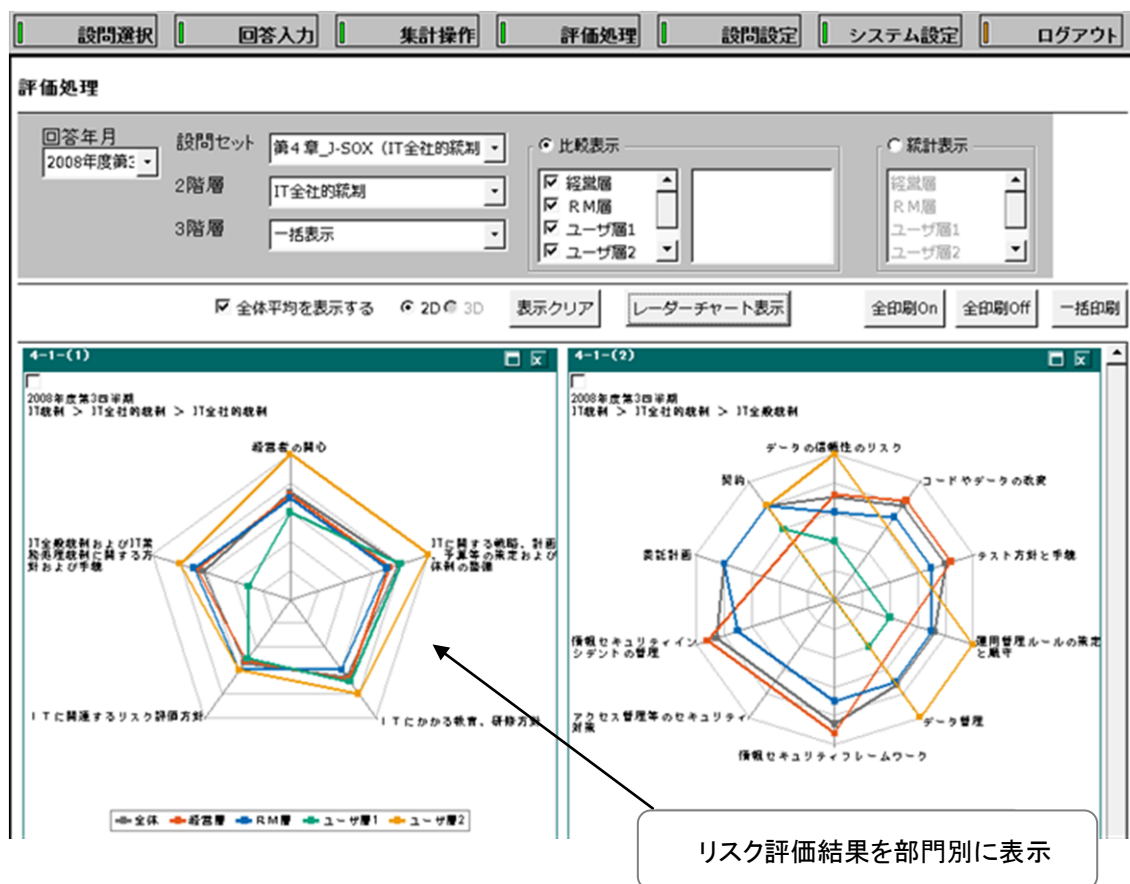


図 3-6-2. リスク評価結果の表示（レーダーチャート）

設問選択

回答入力

集計操作

評価処理

設問設定

システム設定

ログアウト

集計表

回答年月

2008年度第3

設問セット

第1章_経営リスク

第4章_「SOX」(IT全社統制)

集計部門・利用者選択

経営層

R M層

ユーザ層1

ユーザ層2

経営層1

経営層2

経営層3

経営層4

集計表表示

集計表印刷

5階層表示

CSV出力

設問設定			全体評価			回答詳細				
識別コード	タイトル	設問	第1層	第2層	第3層	部門	01	02	03	04
4	IT統制		4.0							
4-1	IT全社統制			4.0						
4-1- (1)	IT全社統制				3.5					
4-1- (1) -1	経営者の関心	Q 経営者は、ITに対して、組織として計画を作成して				3.7	4	3	4	
▶ 4-1- (1) -2	ITに関する戦略、計画、予	Q ITに関する戦略、計画、予算等の作成体制が整備さ				3.3	4	2	4	
4-1- (1) -3	ITにかかる教育、研修方	Q ITに係る教育、研修に関する方針はありますか？				3.3	4	2	4	
4-1- (1) -4	ITに関連するリスク評価	Q 全社的なITに関連するリスク評価の方針はありますか				3.7	4	3	4	
4-1- (1) -5	IT全般統制およびIT業務処	Q IT全般統制およびIT業務処理統制に関する方針お				3.7	4	3	4	
4-1- (2)	IT全般統制			4.4						
4-1- (2) -1	データの信頼性のリスク	Q IT基盤が適切でない場合には、財務報告のアプリ				3.7	3	4	4	
4-1- (2) -2	コードやデータの改変	Q プログラムや重要なデータが無断で変更されるリス				4.7	5	4	5	
4-1- (2) -3	テスト方針と手続	Q テストが正しく行われないと、テストが適切に実施				4.3	4	4	5	
4-1- (2) -6	情報セキュリティフレーム	Q 情報セキュリティ基本方針に基づいて組織の情報セ				4.7	5	4	5	

図 3-6-3. リスク評価結果の表示(集計表)

3.6.2 提供機能

JRMS2010 は、回答入力、集計表示／重み設定、評価設定、質問設定、ユーザ管理の五つの機能を提供している。

(1) 回答入力

ツールに組み込まれている質問を表示し、利用者に回答を入力させる。また、未回答の質問がないかをチェックし、回答途中でも回答を保存する機能（一時保存機能）を実装している。

500 問程度の質問を回答することになるため、できるだけ回答者が操作しやすいよう、以下の点に注意して入力画面を構成している。

- ①質問の章立てをわかりやすく表現し、回答者自身がどこまで回答を入力したかを把握しやすくしている。
- ②できるだけマウス操作のみで回答操作を行えるように配慮し、入力に抵抗感を与えないようにしている。

JRMS は画面左側に質問構成をツリー状に表示して現在の質問位置を明示し、右側の回答入力フォームでは入力を基本的にラジオボタンのみとし、マウス操作のみで次々と回答入力が行えるようにしている（図 3-6-1 参照）。

(2) 集計表示／重み設定

回答入力画面により入力・登録されたデータを、個別項目別、総合評価値、階層別に集計し、表示する。

同時に、それぞれの質問集計に対して重みを設定できるような画面とし、この重みを考慮して集計計算を行う（図 3-6-4）。

	2階層		3階層		4階層	
	点数	配点	点数	配点	点数	配点
第4章_J-SOX(IT全社的統制)	3.8	100				
4-1: IT全社的統制	3.8	100	3.8	100		
4-1-(1): IT全社的統制			3.3	50	3.3	100
4-1-(1)-1: 経営者の関心					3.6	20
4-1-(1)-2: ITに関する戦略、計画、予算等の策定および体制の?					3.6	20
4-1-(1)-3: ITにかかる教育、研修方針					3.4	20
4-1-(1)-4: ITに関連するリスク評価方針					2.6	20
4-1-(1)-5: IT全般統制およびIT業務処理統制に関する方針およ					3.4	20
4-1-(2): IT全般統制			4.2	50	4.2	100
4-1-(2)-1: データの信頼性のリスク					3.6	20
4-1-(2)-2: コードやデータの改変					4.2	20
4-1-(2)-3: テスト方針と手続					4.2	20
4-1-(2)-6: 情報セキュリティフレームワーク					4.6	20
4-1-(2)-8: 情報セキュリティインシデントの管理					4.6	20

図 3-6-4. 集計表示画面

質問は階層構造となっているため、個々の質問ごと、あるいはその上位階層ごとに入力された素点の集計値が表示される。また、その横には重み値が入力できるボックスを設けている。

重みは、規定値として同一階層の質問に対し均等に配分されているが、その配分比を変更することができ、質問ごとに重みを設定することを可能とした。

(3) 評価処理

回答結果を用いて各種グラフなどの評価情報を表示する。グラフは図 3-6-5 のようなレーダーチャートにより表示される。

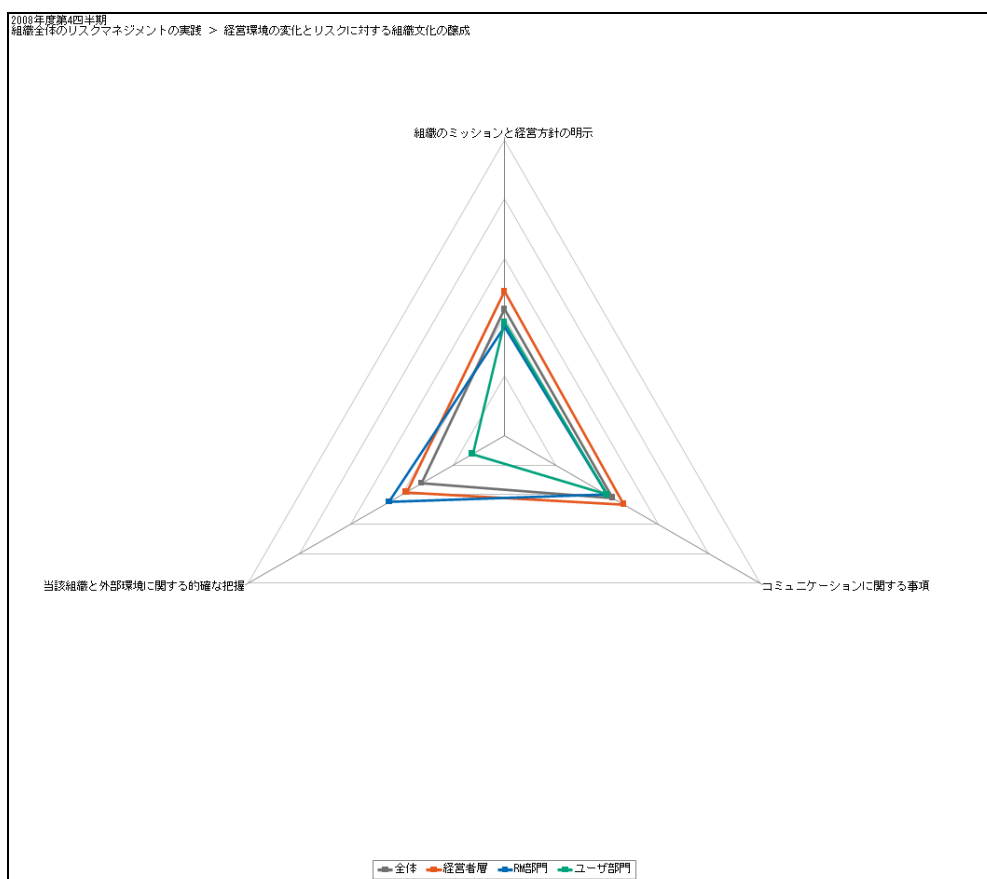


図 3-6-5. レーダーチャート画面例

(4) 質問設定

質問の属性および文言の変更等を行うための機能も備えている。事前に登録する回答者の立場や所属部門により、同じ質問でも表現を変えた方がよい場合を考慮し、質問の文言を個別に変更することもできる。

(5) ユーザ管理

回答者、部門の登録、修正、削除機能を提供する。

3.7 JRMS2010－Quick Start 編の構成

JRMS2010・Quick Start 編は、JRMS2010 の構造を通してその有効性を速やかに理解できるように、最も基本的と思われる質問を約 100 項目抽出し、構成したものである。

Quick Start 編の質問項目への回答結果は、組織のリスクマネジメントの全体像を把握するにはかなり限定的かもしれないが、組織のリスクマネジメントの実態をある程度容易に描き出すことが可能となる。それにより、組織における問題点の所在、リスク分析の意義、リスク対策の必要性等、PDCA を回すことの意味、組織としてリスクマネジメント認識の共有の重要性を手軽に感得することができると思われる。また、JRMS ツールに慣れることにより、さらに段階的に

Baseline 編、Advanced 編へと進むことも可能となる。

以下に、第 1 部「組織経営と JRMS（経営編）」の第 1 章から第 4 章（Quick Start 編）の質問項目を掲載する。

なお、質問項目については随時見直しを行っているため、以下に記載する質問内容は報告書とりまとめ時点のものである。

第 1 章「組織全体のリスクマネジメントの実践」（Ver.7／質問数：36）

KW	コード番号	質問項目(案)	解説文	用語説明
	1	組織全体のリスクマネジメントの実践		
	1-1	経営環境の変化とリスクに対する組織文化の醸成		
	1-1-(1)	組織のミッションと経営方針の明示		
組織のミッション	1-1-(1)-1	Q 組織としての <u>ミッション</u> を明らかにしていますか？(経)		ミッション：設立目的、存在目的、組織化目的のこと
		Q 組織としての <u>ミッション</u> は明らかですか？(RM、ユ)		
経営目標の明確化	1-1-(1)-2	Q 組織のミッションを達成するための <u>経営目標</u> を明らかにしていますか？(経)		経営目標：ミッションを果たすために設定する経営としての具体的な成果目標
		Q 組織のミッションを達成するための <u>経営目標</u> は明らかですか？(RM、ユ)		
経営の優先順位の明確化	1-1-(1)-3	Q <u>経営の優先順位</u> は、明らかになっていますか？		経営の優先順位：経営においてどのようなことを達成することが、より重要であると考えているかということ 例：コンプライアンス（法令等の遵守）、顧客の安全、社員の健康、適正な利益の獲得等の何から確実に確保していくかということ
	1-1-(2)	方針		
マネジメント方針の確立	1-1-(2)-1	Q 自分の組織に相応しい <u>経営方針</u> を確立していますか？(経、RM)		経営方針：経営目標を達成するための優先順位、投資等の考え方
経営理念との連動	1-1-(2)-2	Q 経営方針は <u>経営理念</u> と連動していますか？		経営理念：経営を行う際の基本的な考え方や価値観のこと。社是、社訓等がこれにあたる

KW	コード番号	質問項目(案)	解説文	用語説明
理解状況の確認	1-1-(2)-3	Q 経営方針の全社員への理解状況を確認していますか？(経、RM)	重要な施策に関しては、通達をするだけではなくその理解状況を把握することが、経営意思を徹底するためには大切です。	
	1-1-(3)	計画		
リスクマネジメント計画	1-1-(3)-1	Q マネジメント方針に基づき計画を策定していますか？(経) Q マネジメント方針に基づき計画が策定されていますか？(RM、ユ)		マネジメント方針：リスクマネジメント等を実施する際に、全員に徹底すべきことや重要な事項を定めたもの
負荷の把握	1-1-(3)-2	Q 計画達成に必要な負荷を把握していますか？(経、RM)		計画達成に必要な負荷:計画しているリスクマネジメントを実施する際に必要となる人員、時間、経費等をいう
コンプライアンスの徹底	1-1-(3)-3	Q コンプライアンスの徹底を計画に入れていますか？(経) Q コンプライアンスの徹底が計画に入れられていますか？(RM、ユ)	コンプライアンスは単に法令を順守するだけではありません。社内規則・規定の他、社会的な倫理をも含みます。	
	1-2	リスクマネジメントプロセス		
リスクの特定	1-2-(1)	リスクの特定		
リスクの特定	1-2-(1)-1	Q 組織に影響を与える事象に関するリスク特定の重要性を認識していますか？(経、RM)	組織に重要な影響を及ぼす問題をリスクとして特定できていないことは、事前の対策を講じえないことになります。	
リスクの源泉	1-2-(1)-2	Q リスクをもたらすハザードを把握できていますか？(経、RM)		ハザード:潜在的なリスクの要因
リスク変化の認識	1-2-(1)-3	Q リスクが組織や社会の状況変化と共に変化することを認識していますか？(経、RM)	社会環境の変化によって、それまでリスクとは考えられていなかったものもリスクとして考える必要が出てきたり、企業状況等によってリスクの重大さが変化する場合があります	
	1-2-(2)	リスク分析		
重要性の認識	1-2-(2)-1	Q リスク分析の重要性を認識していますか？		

KW	コード番号	質問項目(案)	解説文	用語説明
実施の組織化	1-2-(2)-2	Q リスク分析を組織的に実施していますか？		
有効性・妥当性の確認	1-2-(2)-3	Q 分析対象となる <u>分析手法の有効性・妥当性</u> を確認していますか？(RM、ユ)		分析手法の有効性・妥当性:そのリスク分析手法によって分析された結果が、評価する際に十分な内容や精度があるかということ。すべてのリスクに対して、高い精度の分析や綿密なデータが必要であるわけではないことに注意すること
リスク評価	1-2-(3)	リスク評価		
評価方法	1-2-(3)-1	Q 評価対象に関するリスクの評価方法は明確ですか？(経)		
リスク対応の判断	1-2-(3)-2	Q リスク対応の判断について判断基準はありますか？(経、RM)		
経営の関与	1-2-(3)-3	Q リスク評価に経営者は関与していますか？(経、RM)		
	1-2-(4)	リスク対策の選定		
リスクマネジメント方針下での検討	1-2-(4)-1	Q リスク対策について、組織として定めたリスクマネジメント方針の下で検討・選定が行われていますか？		
リスク対策の優先順位	1-2-(4)-2	Q 対応優先順位の高いリスクに対して対策を検討していますか？		
選定基準	1-2-(4)-3	Q リスク対策について選定基準がありますか？		
	1-2-(5)	リスク対策の実行		
リスク対策の最適化	1-2-(5)-1	Q 最適なリスク対策を実施していますか？	リスク対策を実施する前に、適切な対応を実施するために複数の対策を検討し、その中から最適な対策を選ぶことが重要です。	
対策における責任者	1-2-(5)-2	Q リスク対策の責任者は定まっていますか？		
費用対効果の検討	1-2-(5)-3	Q リスク対策の費用対効果の検討を行っていますか？		

KW	コード番号	質問項目(案)	解説文	用語説明
	1-3	リスクマネジメントシステムの維持		
	1-3-(1)	実行		
体制構築	1-3-(1)-1	Q <u>マネジメントシステム</u> の体制が構築されていますか？		マネジメントシステム：マネジメントを実施する際の仕組み
実行組織	1-3-(1)-2	Q マネジメントの実施体制の実施能力や責任体制は十分ですか？		
マニュアル類の作成状況	1-3-(1)-3	Q マニュアル、計画書が作成されていますか？		
	1-3-(2)	チェック		
チェック体制	1-3-(2)-1	Q マネジメントシステムのチェック体制は整備されていますか？		
パフォーマンス評価	1-3-(2)-2	Q マネジメントシステムの <u>パフォーマンス評価</u> を実施していますか？		パフォーマンス評価：目標とした活動の成果が得られたかを評価すること
有効性評価	1-3-(2)-3	Q マネジメントシステムの <u>有効性評価</u> を実施していますか？		有効性評価：投下した資源と得られた成果を比較して、実施した活動の妥当性を評価すること
	1-3-(3)	改善		
改善の仕組み	1-3-(3)-1	Q マネジメントシステムの改善の仕組みを持っていますか？		
マネジメントシステムの改善	1-3-(3)-2	Q 定期的にマネジメントシステムの改善を行っていますか？		
改善効果の確認	1-3-(3)-3	Q 経営者は、マネジメントシステムの改善効果を確認していますか？(経)		
	1-3-(4)	マネジメントレビューの実施		
レビューの実施	1-3-(4)-1	Q 経営者がマネジメントシステムに関する <u>レビュー</u> を行っていますか？(経、RM)		レビュー：その実施した事項に関して、実効性や有効性を検討すること
継続改善	1-3-(4)-2	Q レビューされた結果は継続的な改善に活かされていますか？		
組織開示	1-3-(4)-3	Q レビューの実施が組織内に開示されていますか？		

第2章「内部統制リスクと経営者の対応（総論）」（Ver.5／質問数：12）

KW	コード番号	質問項目(案)	解説文	用語説明
	2	内部統制リスクと経営者の対応（総論）		
	2-1	統制環境		
	2-1-(1)	経営		
経営者の基本方針	2-1-(1)-1	Q 経営者の内部統制に係る基本方針は明確に示されていますか？（経）	組織が経営会議で了承された経営を実現するための方針です。この方針はステークホルダーに対する説明責任を果たします。	
		Q 経営者の内部統制に係る基本方針を知っていますか？（R、ユ）		
	2-1-(2)	経営組織		
取締役会および監査役または監査委員会	2-1-(2)-1	Q 取締役会および監査役または監査委員会は、内部統制に関し経営者を適切に監督・監視する責任を理解し、実行していますか？（経、RM）	取締役会および監査役または監査委員会は、企業のガバナンス方法によって異なることに注意して下さい。必要なのは、経営者を監督する仕組みがあることです。	
	2-1-(3)	経営実務		
役割分担	2-1-(3)-1	Q 経営者は、企業内の個々の職能（生産、販売、情報、会計等）および活動単位に対して、適切な役割分担を定めていますか？		
	2-2	リスクの評価と対応		
	2-2-(1)	リスク評価の仕組み		
リスク評価	2-2-(1)-1	Q リスク評価は内部統制を重視した経営にとって有効となっていますか？（経、RM）		
リスクの識別	2-2-(1)-2	Q 企業経営に影響を及ぼす社内外のリスク要因の影響が適切に考慮されていますか？（経、RM）	リスクが発生した場合の組織経営に与える損害などの大きさをリスクごとに経営として把握することです。	
	2-3	統制活動		
	2-3-(1)	統制活動全般		
リスク対処方針と手続き	2-3-(1)-1	Q 内部統制を重視した経営を行うことを妨げるリスクに対処するための方針と手続きを定めていますか？	どのようなリスクに対処するのか、またどの程度経営資源を投入するのか、新たなリスクへ対応することを決定するための稟議などの手続きなどを定めることです。	
統制活動	2-3-(1)-2	Q 統制活動は業務全体にわたって誠実に実施されていますか？		

KW	コード番号	質問項目(案)	解説文	用語説明
	2-4	情報と伝達		
	2-4-(1)	情報共有と伝達に係る活動		
方針や指示の伝達	2-4-(1)-1	Q 経営者は、内部統制を重視した経営に関する経営者の方針や指示を、組織内のすべての者に適切に伝達できるような体制にしていますか？(経)		
		Q 経営者は、従業員に対し、内部統制を重視した経営に関する経営者の方針や指示を伝えていますか？(RM、ユ)		
情報伝達の体制	2-4-(1)-2	Q 会計および財務に関する情報が、適切に利用可能となるような体制が整備されていますか？(経、RM)	売上げや利益などの会計・財務に関する情報が経営分析や商品ごと、支店・支社など組織ごとの分析などに適宜利用できるようにすることです。	
会社機関の情報共有	2-4-(1)-3	Q 経営者、取締役会、監査役または監査委員会およびその他の関係者の間で、情報が適切に伝達・共有されていますか？(経、RM)		
	2-5	モニタリング		
	2-5-(1)	モニタリング活動		
モニタリングによる統制	2-5-(1)-1	Q 組織の内外から伝達された内部統制に関する重要な情報は適切に検討され、必要な是正措置が取られていますか？		
	2-6	ITへの対応		
	2-6-(1)	ITによる統制活動		
IT戦略と計画	2-6-(1)-1	Q 経営者は、ITに関する適切な戦略、計画等を定めていますか？		

第3章「内部統制リスクの分析」(Ver.5／質問数：37)

KW	コード番号	質問項目(案)	解説文	用語説明
	3	内部統制リスクの分析		
	3-1	リスク分析の構築		
	3-1-(1)	リスク分析の仕組み		
リスク分析の実施	3-1-(1)-1	Q リスク分析(発見・算定・評価)の実施について、リスクマネジメント計画上明確にしていますか？		
	3-1-(2)	リスク分析の体制		
社内体制	3-1-(2)-1	Q 内外の経営環境の変化を含めたリスク環境の動きを捉える社内体制を有していますか？		

KW	コード番号	質問項目(案)	解説文	用語説明
優先順位	3-1-(2)-2	Q リスク評価を行い、リスク対応の優先順位を確定していますか？		
	3-1-(3)	リスク分析の実施		
リスクの洗い出し	3-1-(3)-1	Q 定期的にリスクを洗い出していますか？	組織を取り巻く環境は常に変化しています。変化はリスク発生の源泉といえます。したがって、1 回リスクの洗い出しを行ったから、それでよしでは不十分ですので、定期的に分析を行うことが求められています。	
リスク頻度の算定	3-1-(3)-2	Q リスク頻度を算定していますか？		
影響度の算定	3-1-(3)-3	Q リスク影響度を算定していますか？		
リスク評価	3-1-(3)-4	Q リスク評価を実施していますか？	頻度と影響度を総合的に判断し、どの程度の対応を行うリスクであるかを評価します。対応するリスクの優先順位をつけることも含まれます。	
	3-2	経営の観点によるリスクの分析		
	3-2-(1)	リスク分析(戦略リスク)		
ビジネス戦略リスク	3-2-(1)-1	Q ビジネス戦略リスクが経営に与える影響を考えていますか？		
市場マーケティング	3-2-(1)-2	Q 市場マーケティングが経営に与える影響を考えていますか？		
人事制度	3-2-(1)-3	Q 人事制度のリスクが経営に与える影響を考えていますか？	成果主義、定年延長、裁量労働性、処遇などさまざまな制度の変更、あるいは変更しないことによる経営に与えるリスクを考えます。	
政治リスク	3-2-(1)-4	Q 政治のリスクが経営に与える影響を考えていますか？	法律の制定改廃や国際情勢、地政学的リスクなどが該当します。	
経済リスク	3-2-(1)-5	Q 経済のリスクが経営に与える影響を考えていますか？	サブプライムローンによる不況、為替の上下変動などのリスクがあります。	
社会リスク	3-2-(1)-6	Q 社会のリスクが経営に与える影響を考えていますか？	少子高齢化、人心の安定度など、社会環境による経営への影響の事です。	

KW	コード番号	質問項目(案)	解説文	用語説明
メディアリスク	3-2-(1)-7	Q メディアのリスクが経営に与える影響を考えていますか？	マスコミの記事(好意的、敵対的)、誤報などによる影響です。	
資本リスク	3-2-(1)-8	Q 資本・負債のリスクが経営に与える影響を考えていますか？	資本の適切性、負債額、無借金経営の良否、資本の有効活用、適正な会社事業規模と資本金、負債額のバランスなどの観点です。	
	3-2-(2)	リスク分析(財務リスク)		
資産運用	3-2-(2)-1	Q 資産運用のリスクが経営に与える影響を考えていますか？		
流動性リスク	3-2-(2)-2	Q 流動性のリスクが経営に与える影響を考えていますか？		
	3-2-(3)	リスク分析(ハザードリスク)		
自然災害	3-2-(3)-1	Q 自然災害のリスクが経営に与える影響を考えていますか？		
事故・故障	3-2-(3)-2	Q 事故・故障のリスクが経営に与える影響を考えていますか？		
情報システムのリスク	3-2-(3)-3	Q 情報システムのリスクが経営に与える影響を考えていますか？		
	3-2-(4)	リスク分析(オペレーショナルリスク)		
製品・サービスのリスク	3-2-(4)-1	Q 製品・サービスのリスクが経営に与える影響を考えていますか？	不良品、製品事故、苦情対応、リコールなどの影響を指します。	
情報管理のリスク	3-2-(4)-2	Q 情報管理のリスクが経営に与える影響を考えていますか？		
法務・倫理のリスク	3-2-(4)-3	Q 法務・倫理のリスクが経営に与える影響を考えていますか？		
環境リスク	3-2-(4)-4	Q 環境のリスクが経営に与える影響を考えていますか？	組織のおかれている経営環境のことではなく、土壌汚染、環境汚染、地球温暖化、有害物質排除などの環境問題を指します。	
労務・人事リスク	3-2-(4)-5	Q 労務・人事のリスクが経営に与える影響を考えていますか？		
経営者のリスク	3-2-(4)-6	Q 経営者のリスクが経営に与える影響を考えていますか？	経営者の不適切な行動・言動、乱脈経営、優秀な経営者の死亡などのリスクをいいます。	

KW	コード番号	質問項目(案)	解説文	用語説明
	3-3	リスクを発生させる根本原因の分析		
	3-3-(1)	プロセス	製品・サービスを提供する過程に内在するリスクをいいます。	
過去の不正分析	3-3-(1)-1	Q 過去の不正の分析が行われていないことによる経営に与える影響を考えていますか？		
	3-3-(2)	スタッフ		
倫理・価値観	3-3-(2)-1	Q 倫理・価値観による経営に与える影響を考えていますか？	組織倫理に基づく組織経営を行う価値観の醸成が重要です。組織不祥事の発生はまさに組織倫理違反によるといえますので、この点の影響を認識しているかが問われます。	
	3-3-(3)	機械設備		
機械への依存度	3-3-(3)-1	Q 業績達成において機械などの依存度の高低による経営に与える影響を考えていますか？	製品やサービスの供給にあたって機械への依存度が高い場合は設備投資や機械の刷新をしているか否かが経営に大きな影響を与えます。	
	3-3-(4)	資産管理		
資産保全・使用	3-3-(4)-1	Q 資産の保全がされていないことや、資産誤使用の防止がされていないことによる経営に与える影響を考えていますか？	特許など無形資産などをよく考える必要があります。	
	3-3-(5)	複雑性		
業務フローの複雑度	3-3-(5)-1	Q 業務フローの複雑度による経営に与える影響を考えていますか？	業務フローが複雑な場合、効率化を阻害したり、ミスが多発する原因になることがあります。	
	3-3-(6)	処理ボリューム		
業務処理量	3-3-(6)-1	Q 業務処理量の変化・増加に対する柔軟性の有無による経営に与える影響を考えていますか？	業務処理量が大きく変動することが通常である場合、処理量が多い場合には対応不能やミスが生じること、また極端に少ない場合は余剰人員が発生しモラルの低下や採算割れが発生することなどを考えます。	

KW	コード番号	質問項目(案)	解説文	用語説明
	3-3-(7)	技術		
システム依存度	3-3-(7)-1	Q システム依存度の高低による経営に与える影響を考慮していますか？	製品やサービスを提供する場合、システム依存度が高い場合は、システムの更新の有無が経営に与えるリスクや情報システムの停止や誤作動につながるリスクを考慮します。一方依存度が低い場合はシステムを導入しコストダウンの余地を検討する必要があります。	
	3-3-(8)	コンプライアンス		
コンプライアンス醸成	3-3-(8)-1	Q コンプライアンスを醸成する気風が欠けることによる経営に与える影響を考慮していますか？	コンプライアンスは単に法令を遵守するだけではなくありません。社内規則・規定の他、社会的な倫理をも含みます。	
倫理規範整備	3-3-(8)-2	Q 倫理規範などの整備状況による経営に与える影響を考慮していますか？		
	3-3-(9)	ストラテジ		
経営情報	3-3-(9)-1	Q 経営情報の十分性、正確性、早さを欠くことによる経営に与える影響を考慮していますか？		
コスト要因	3-3-(9)-2	Q 主要コスト要因の把握の度合いが不十分なことによる経営に与える影響を考慮していますか？		

第4章「IT統制」(Ver.5／質問数：20)

KW	コード番号	質問項目(案)	解説文	用語説明
	4	IT統制		
	4-1	IT全社的統制		
	4-1-(1)	IT全社的統制		
経営者の関心	4-1-(1)-1	Q 経営者は組織としてITに対する計画を作成していますか？(経)	ITへの対応が組織として計画的に実施されていないことにより、財務報告の信頼性が阻害されます。	IT：財務報告に利用するコンピュータ、ソフトウェア、リードなどの入力装置、プリンタなどの出力装置をさす IT計画：IT設備調達、導入、運用体制、監視体制、機器の廃棄が含まれる
		Q 組織としてITの計画を知っていますか？(RM、IS、ユ)		

KW	コード番号	質問項目(案)	解説文	用語説明
IT に関する戦略、計画、予算等の策定および体制の整備	4-1-(1)-2	Q IT に関する戦略、計画、予算等の作成体制が整備されていますか？(経) Q IT に関する戦略、計画、予算が策定されていることを知っていますか？(RM、IS、ユ)	IT の戦略や計画、予算を策定するための組織が整備されている必要があります。	
ITにかかる教育、研修方針	4-1-(1)-3	Q IT に係る教育、研修に関する <u>方針</u> はありますか？(経、RM、IS) Q IT に係る教育、研修は方針に基づいて実施されていますか？(ユ)	IT については日進月歩で進化するので、教育は必須です。	方針:IT の利用方法、内部統制のしくみ、情報セキュリティ対策などが含まれる
ITに関連するリスク評価方針	4-1-(1)-4	Q 全社的な <u>ITに関連するリスク</u> 評価の方針はありますか？(経、RM) Q 全社的な IT に関連する <u>リスク評価</u> について知っていますか？(IS、ユ)	IT のリスクの評価が重要です。	IT のリスク:IT 機器への破壊行為、ソフトウェア改ざん、不正アクセス、データベースの改ざんなどがある IT のリスク評価:IT のリスクに対する対策の程度をいう
IT 全般統制および IT 業務処理統制に関する方針および手続	4-1-(1)-5	Q <u>IT 全般統制</u> および <u>IT 業務処理統制</u> に関する方針および手続を制定していますか？(経、RM) Q IT 全般統制および IT 業務処理統制に関する方針および手続を知っていますか？(IS、ユ)	IT のリスクを低減するために IT 全般統制や IT 業務処理統制が必要となります。	IT 全般統制:組織が用いる IT に共通するネットワーク、システム、開発方法、運用方法、アクセス管理、外部委託などが含まれる IT 業務処理統制:財務データや売上などの情報システムに対する統制のことをさす。たとえば、二重入力の禁止やデータの後日書き換え禁止などがある
	4-1-(2)	IT 全般統制		
データの信頼性のリスク	4-1-(2)-1	Q <u>IT 基盤</u> が適切でない場合には、財務報告のアプリケーションシステムに正しいデータが提供されないリスクがあることを知っていますか？(経、RM、ユ) Q <u>IT 基盤が適切</u> でない場合には、財務報告のアプリケーションシステムに正しいデータを提供できないリスクがあることを知っていますか？(IS)	IT 基盤が適切でないときには、システムに不正に侵入されて、データが改ざんされるリスクがあります。不要な利用者に利用されないようにする必要があります。	IT 基盤:IT のハードウェアやソフトウェアなど共通に用いるものをいう IT 基盤の適切さ:IT 基盤でデータが改ざん可能であれば、IT による処理がすべて信用されなくなるため、重要である

KW	コード番号	質問項目(案)	解説文	用語説明
コードやデータの改変	4-1-(2)-2	Q プログラムや重要なデータが <u>無断で変更</u> されるリスクを知っていますか？(経、RM、IS)	プログラムや重要なデータについて、改変されないように、管理することが必要です。	プログラムの無断変更: 財務データに不正が存在することに繋がるため、統制が重要である
テスト方針と手続き	4-1-(2)-3	Q <u>テスト</u> が正しく行われないと、アプリケーションシステムや IT 基盤が設計で意図したどおりに機能せず、その結果、財務情報が信頼できなくなるリスクがあることを知っていますか？(経、RM、ユ)	テストを正しく行うことで、誤動作や改ざんなどのリスクを回避できます。	テスト: 入力データと出力データが意図したとおりになっているか、などの確認を行う
		Q テストが正しく行うために <u>テスト方針</u> が作成され、テストを実施する手続きがありますか？(IS)	テストを正しく実施するためには、方針と手続きを決めておく必要があります。	テスト方針: テストするための方針のこと。テスト項目は多岐にわたり、項目数も多いことから、絞り込むための方針が重要である
テスト作業の権限の分離	4-1-(2)-4	Q テスト作業において <u>権限分離</u> が正しく行われていないと、不正のリスクが高くなることを知っていますか？(RM、IS)	テストを実施する際に、権限の分離を確認することで、不正に対するけん制機能となります。	権限分離: たとえば、承認と実施を一人で行えば、不正のチェックができなくなるため、分離することをいう
運用管理ルールの策定と順守	4-1-(2)-5	Q 財務報告に係る IT の <u>運用管理</u> ルールに不備がある場合、結果として財務報告の信頼性に重大な影響を及ぼすことを知っていますか？(RM、IS、ユ)	IT の運用では人手が介在します。そのため、不正などの余地があるので、運用管理ルールが重要になります。	運用管理: 情報処理の手順に従って、権限者が実施することが必須である。これを担保しないと不正が可能になる
データ管理	4-1-(2)-6	Q 財務報告に係る <u>データの入力</u> 、登録、処理、集計、報告等のデータ管理に不備があると、財務情報の信頼性が損なわれることを知っていますか？(RM、IS、ユ)	データが改ざんされないように管理することがきわめて重要です。	データの入力: たとえば、売上のようなデータを改ざんすると二重売上や仮称売上に繋がる
情報セキュリティフレームワーク	4-1-(2)-7	Q 情報セキュリティ基本方針に基づいて組織の情報セキュリティの <u>フレームワーク</u> を構築していますか？(経)	情報セキュリティ基本方針に基づいて組織の情報セキュリティのフレームワークが構築され、財務情報の信頼性(改ざん)や機密性を確保することが重要です。	フレームワーク: 情報セキュリティは部門によって実施する内容が違うため、大枠を決めて、細部は現場に任せるような形態をとることがある。これをフレームワークという
		Q 組織の情報セキュリティのフレームワークに基づいて、財務情報の信頼性(改ざん)、機密性を担保していますか？(RM、IS)		

KW	コード番号	質問項目(案)	解説文	用語説明
アクセス管理等のセキュリティ対策	4-1-(2)-8	Q 業務上およびセキュリティの要求事項に基づいて職務権限に対応した <u>アクセス範囲やアクセス権限のレベル</u> を定めていますか？(IS)	業務上およびセキュリティの要求事項に基づいて職務権限に対応したアクセス範囲やアクセス権限のレベルを定め、財務情報を保護することが重要です。	アクセス範囲やアクセス権限のレベルの設定：権限分離を実現するため、きわめて重要である。これが担保されないと、財務情報への改ざんを防げない
情報セキュリティインシデントの管理	4-1-(2)-9	Q <u>事故</u> の報告、記録および対応ルールと手順はありますか？(経、RM、IS)	インシデントについては、経営者に直ちに報告されるような仕組みが必要です。	情報セキュリティ事故：再発防止や事故からの回復のため、関係者に素早く連絡することが求められている
委託計画	4-1-(2)-10	Q (財務報告に直接係る)情報システムの開発・運用等を外部委託するとき、その委託計画は承認されていますか？(経、RM、ユ)	委託契約では、委託先での不正や改ざんが起きないようにコントロールされていることが求められます。	
契約	4-1-(2)-11	Q <u>契約書</u> には、委託業務に関する主要なリスクに対する統制方法を明記していますか？(RM、ユ)	契約によるリスクの低減は重要なポイントです。契約書に記載することで、リスクを転嫁することができます。	
	4-1-(3)	IT 業務処理統制		
データ入力	4-1-(3)-1	Q データの入力は、入力管理ルールに基づいて漏れなく、重複なく、正確に行っていますか？(IS、ユ)		
データ交換の対策	4-1-(3)-2	Q データを交換するときには、不正防止および機密保護の対策を講じていますか？(RM、IS、ユ)	データ交換に際して、不正が行われないような対策が必要です。	
出力情報の作成手順および取扱い	4-1-(3)-3	Q 出力情報の作成手順、取扱い等は、誤り防止、不正防止および機密保護の対策を講じていますか？(RM、IS、ユ)	出力では処理結果が得られますが、ここで不正がなされないような対策が必要です。	
改ざんを防止する機能や仕組み	4-1-(3)-4	Q 利用者が <u>スプレッドシート</u> の数式や <u>マクロ</u> 等を変更できないようにしていますか？(RM、ユ)	スプレッドシートでは計算式がセルに埋め込まれていたり、高度なマクロが使われたりしているため、不正やエラーの可能性が高いため、十分な対策が必要です。	スプレッドシート、マクロ：スプレッドシートへの入力、処理、出力などを外部から制御することができる

注) 文末に回答対象部門(経営者層、RM 部門、IS 部門、ユーザ部門)の略称を示す。特に記載がない質問項目は、全部門を対象とする。

4. JRMS の有効性検証

組織のリスクマネジメント実践に関して JRMS の有効性を確認するため、数社に協力を求め、2008 年秋から冬にかけて実証実験を行った。実証実験の課題は、質問項目が現在の経営環境の変化に対応できているか、リスクマネジメントのツールとして（JRMS2003 に比較して）使いやすさ、レーダーチャートの表示、質問項目への回答のしやすさを含め、その有効性を確認することができるかどうかにあった。

協力をいただいた企業からは JRMS について、リスクマネジメントのツールとして総じて利便性・機能性・有効性に関し高い評価をいただくことができた。しかし、その反面、質問項目およびツールのわかりやすさ等に関して貴重な意見・指摘をいただいた¹⁵。

リスク評価指針検討委員会としては、いただいた貴重な指摘なり意見を JRMS2010 に取り込み、機能性を一段と高めていく予定である。

4.1 JRMS 分析チャートの読み方

本節は、JRMS による分析結果をチャートとして表記したものから、その組織の課題をどのように見るかという事例を示したものである。

4.1.1 ギャップの判定の考え方

JRMS による評価結果は、評価対象の回答部門別（経営者層、リスクマネジメント部門（以下、「RM 部門」という。）、ユーザ部門 等）に、レーダーチャートで表現される。

このチャートを用いて評価する場合は、組織として設定されているベンチマークと回答部門・回答者間のギャップに留意する必要がある。回答部門・回答者間のギャップは組織におけるリスクマネジメントの浸透状況を把握する上で重要な情報となる。

しかし、同じようなギャップが見受けられる場合でも、その発生理由は同じではない。たとえば、回答者のリスクマネジメントに対する理解が不足している場合にもギャップは発生する。この場合、評価結果のギャップを正しい状況評価と認識して分析を行うと、間違った評価を行うこととなる。

このような状況では以下の四つのケースが考えられる。

- ①リスクマネジメントに関する理解が不足しているために評価の正確性が不足している場合
- ②業務状況の理解が不足しているために評価の正確性が不足している場合
- ③JRMS の質問内容の理解が不足しているために評価の正確性が不足している場合

15 たとえば、設問の意味理解に関する課題、成熟度モデルにおける評価レベルの境界（この点は、本報告書にて改善させたものを提示）、また、ツールの編集機能・画面表示機能の改善等について、非常に好意的で積極的な意見が出された。それらに対しては、JRMS2010 公表時には可能な限り改善させる予定である。

④評価への意欲がないために評価の正確性が不足している場合

また、リスクマネジメントは正しく理解されていて客観的に同じような状況にあっても、結果としてギャップが見受けられる場合もある。

JRMS を用いて組織のリスクマネジメントの状況进行评估する際には、以下の事項に留意をして評価されたい。

(1) 実際に回答部門間によって評価レベルが異なっている場合の評価

- ①最低の評価がその組織が目指している評価レベルを満たしている場合は、全体としては特に問題とする必要はない。特に高いレベルとなっている回答部門の評価を参考として、全組織の改善を図ることで、組織のリスクマネジメントレベルは改善される。
- ②リスクマネジメントの導入中で理解や運用状況に差がある状況での評価の場合にも、ギャップは発生する。このことは当然の結果であり、この評価結果を参考として導入計画の進捗を検証し、教育内容等に関する検討材料とすればよい。
- ③その組織が維持したいと考えている評価レベルを下回る評価レベルが存在する場合は、その部門の不足している事項に関して、改善方法を検討する必要がある。

(2) 実際の状況は同じであるが、評価が異なる場合の状況認識

- ①上位者の評価の方が高い場合：経営者は指示を出しているためできていると考えているが、その指示が徹底していないため下位にはその意思が伝わっていない状況等が考えられる。
- ②上位者の評価の方が低い場合：経営者は十分と思われる指示を出していないため実行レベルは低いと考えているが、部下が理解して実施している状況等が考えられる。
- ③リスクマネジメントに対する理解が深く、そのレベルを達成できたとする理想が高いため、実際より低く評価するものがある状況等が考えられる。
- ④項目の中で達成できている部分と達成できていない部分があり、そのどちらに着目するかで評価が異なる状況等が考えられる。

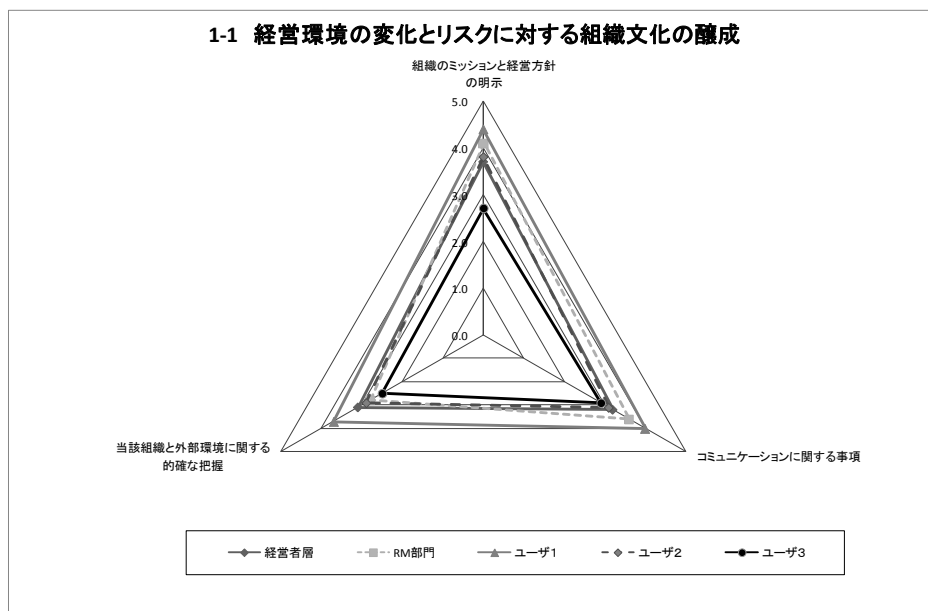
4.1.2 チャートの分析例

本節は、第 1 部「組織経営と JRMS（経営編）」の「第 1 章 組織全体のリスクマネジメントの実践（Advanced 編）」から抜粋した回答事例を参考にして、レーダーチャートのギャップ評価の事例を示すものである。4.1.1 で記したように、ギャップの発生原因はさまざまであるため、本分析事例は評価事例の一つとして参照していただきたい。

なお、分析に際し、対象組織はすべての階層においてレベル 3 以上を目標とする組織であるという前提とする。また、今回の分析は部門間のギャップに着目をして行うため、部門内の個々人の評価の差異（バラツキ）には言及しない。（注：JRMS には、部門内の各回答者の評価の差異（バラツキ）も検討する機能がある）

4.1.2.1 第1章「組織全体のリスクマネジメントの実践 第2階層（Advanced 編）」の評価事例

【チャート1 経営環境の変化とリスクに対する組織文化の醸成】

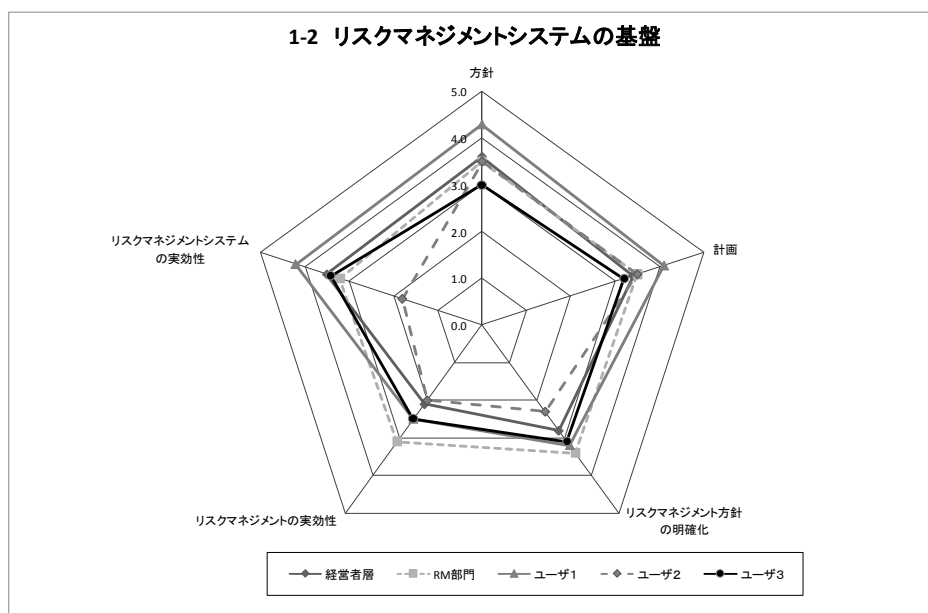


まず、チャート分析において注目すべきことは、各部門の評価レベルが目標としている評価レベルに達しているか否かである。その視点で見ると、ユーザ3の評価レベルが3項目とも3以下(2.7, 2.9, 2.5)であるのは、リスクマネジメントを推進する上で大きな課題である。

次に着目すべきことは、回答部門における弱点事項に関する分析である。ユーザ2のように、コミュニケーション、環境把握に関する事項が低いのは、意識が自分の業務のみに向いていて、他の部署、課員、外部状況の環境変化に関心が低い可能性があり、リスクを考える際も自分の経験のみによって考える傾向が強くなる可能性が高い。また、ユーザ3のように組織ミッションに関する事項が低いのは、自分の業務と組織全体の目的との関係の理解が十分でない可能性がある。

そして、部門間のギャップについての検討が重要である。まずユーザ1の評価が全般的に高いことは他のユーザと比較しても特徴的なことである。このユーザが特に優秀な状況にあるか否かは、その職場に対しヒアリングを行って確認すべき事項である。また、RM部門がユーザ2、3と比較して高い評価となっていることは当然ともいえるが、事務局が全社の理解を得られない状況で引っ張っていく環境となっていないかを確認する必要がある。

【チャート2 リスクマネジメントシステムの基盤】

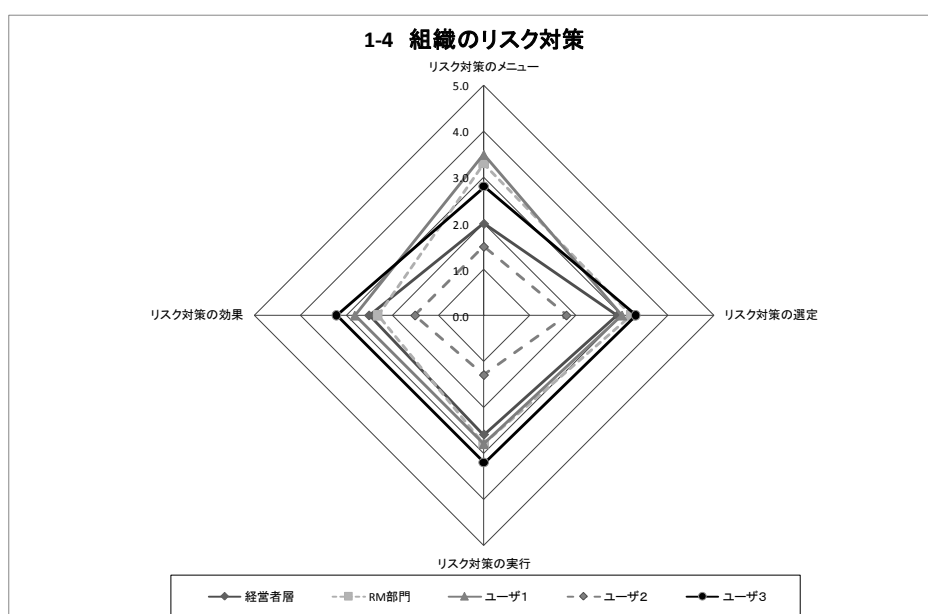


このチャートで特徴的なことは、リスクマネジメントの実効性の評価が相対的に低いことである。このことはリスクマネジメントが形式的に行われる可能性があることを示している。この事項について、RM 部門以外の部門がすべてレベル 3 以下なのは今後の重要な改善課題である。

また、リスクマネジメントシステムの実効性の評価に関しては、ユーザ 2 の評価がかなり低い。このことは、この部門においてリスクマネジメントの「やらされ感」がかなり高い可能性がある。

また、ユーザ 3 の計画に関する評価が低いのは、リスクマネジメントに関する活動の仕事における位置づけが理解されておらず、方針の明確化に関する理解が低いのも、漠然とリスクマネジメントに関する業務を行っている可能性を示している。

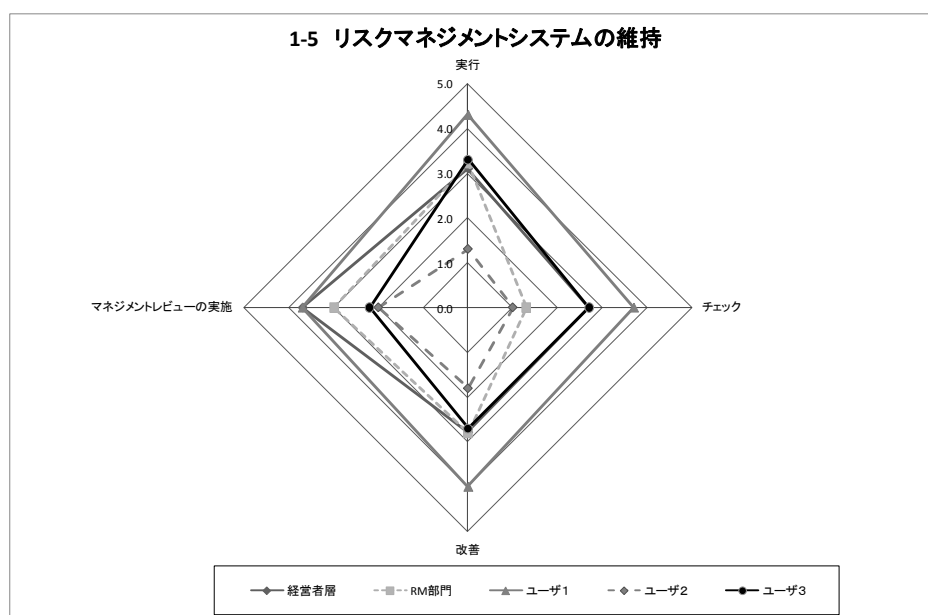
【チャート3 組織のリスク対策】



本チャートで見る限り、リスク対策全般に関してユーザ 3 を除いて十分なレベルではない。特にユーザ 2 の評価は、全項目に渡りかなり低く問題である。逆にユーザ 3 の評価は相対的に高いが、これは、特定の分野（ユーザ 3 の担当分野）について高いレベルを持っているか、または逆に対策の十分性ということに関して理解が十分でないために評価が高くなっている、という二つの可能性が考えられる。

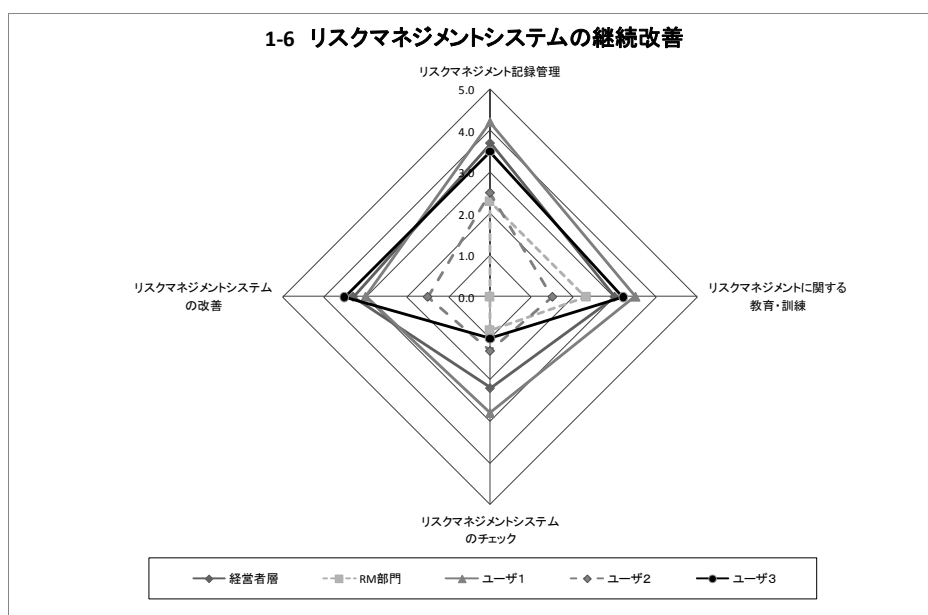
特に経営者層において対策効果の評価レベルが他の質問に比べて低いということは、リスクマネジメントがリスク評価から対策までの一貫した活動であることが理解されておらず、問題を洗い出すことに重点を置きすぎている可能性がある。

【チャート 4 リスクマネジメントシステムの維持】



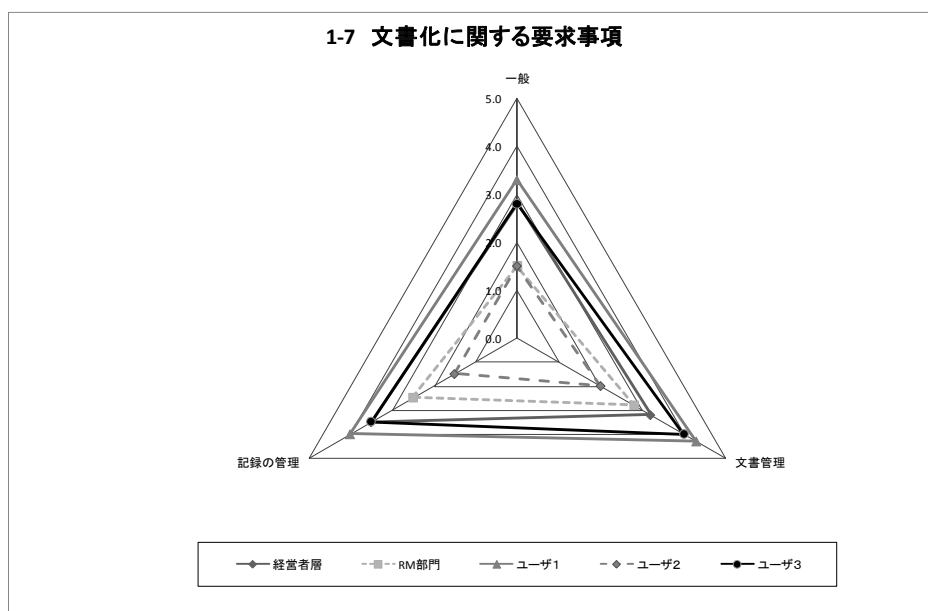
経営者層に比べ他部門の評価がユーザ 1 を除いて相対的に低いのは、マネジメントシステムの運営の実態の理解が不足している可能性があり、そのことはリスクマネジメントシステムの実効性が現場では実感されていないということをも意味する。特に、実行、レビューに比べてチェックの評価が低いのは、体制としては定められているが、その実際の活動に関しては十分ではない可能性を示している。

【チャート5 リスクマネジメントシステムの継続改善】



この評価で特徴的な点は、リスクマネジメントシステムのチェックが非常に低いということである。特に **RM** 部門が一番低いことは、この組織においてはシステムのチェックがなされていないことを示している。そのことはユーザ部門のシステム改善の評価の低さにも示されている。教育に関するユーザ間の差（ユーザ1と2の差）の原因もよく検討する必要がある。

【チャート6 文書化に関する要求事項】



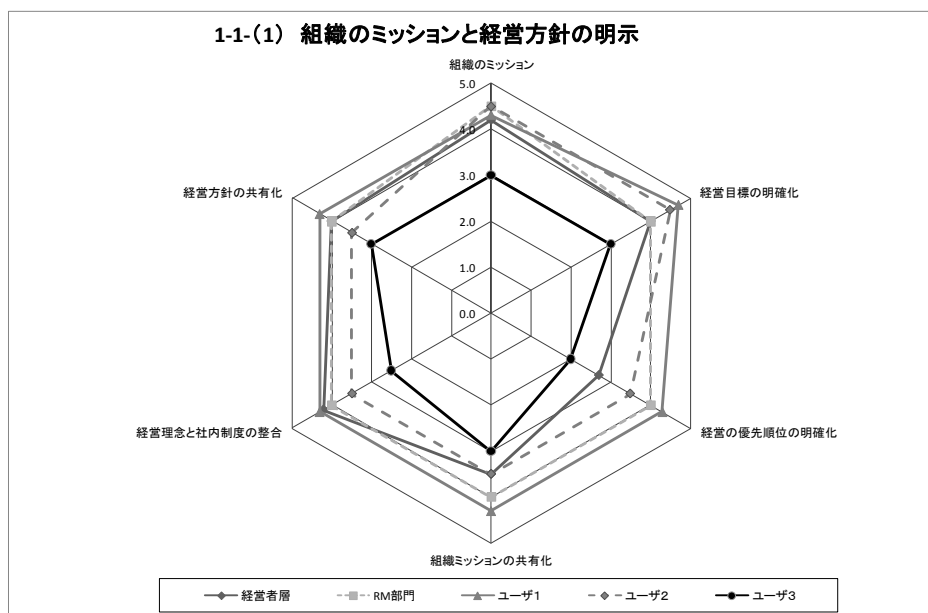
文書化に関しては、**RM** 部門が十分なレベルになっていないことが大きな問題である。

ユーザ1と2の評価の差が大きいこと自体が組織としては大きな問題である。また、ユーザ2や**RM** 部門の評価が低いにも関わらず、経営者層の評価が高いのは、経営者が現場の実態を把握していないか、経営者が評価の高いユーザ1の状況のみで全社の状況を把握しているつもりにな

っている可能性もある。

4.1.2.2 第1章「組織全体のリスクマネジメントの実践 第3階層（Advanced 編）」の評価事例

【チャート7 組織のミッションと経営方針の明示】

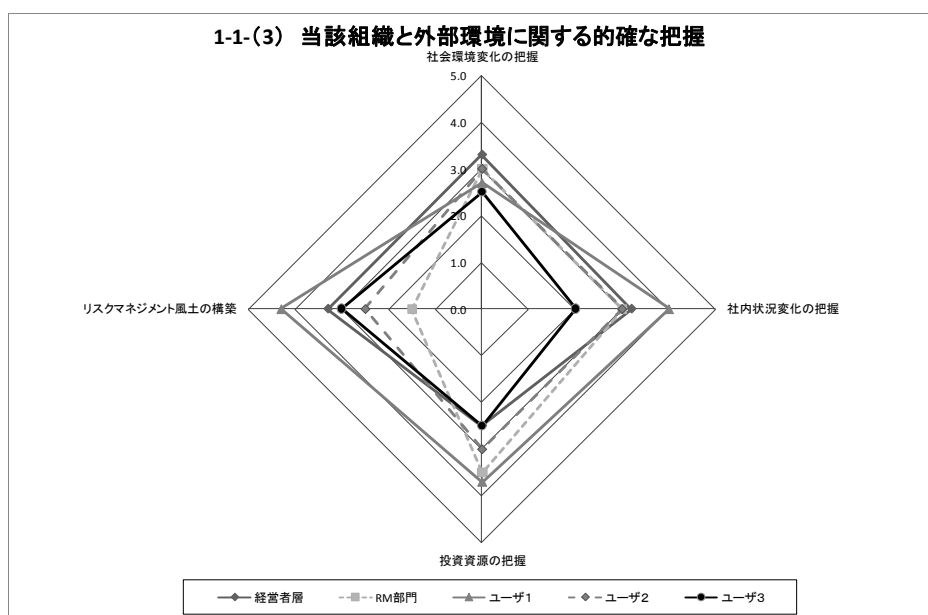


ここで評価されている項目はリスクマネジメントの大前提となる事項である。したがって、この評価対象事項において、各部門の意識、理解度が揃っていることがリスクマネジメントの遂行には大変重要である。

その点で見ると、経営の優先順位に関して各部門の評価が揃っていないことは、組織の意思統一の問題、リスクマネジメントの目標という観点でもよく議論する必要がある。特に、経営者層に比べて **RM** 部門やユーザ部門の評価が高いことも、経営の優先順位ということに関する理解が共有されていないことを示している。

さらには、三つのユーザ間でリスクマネジメントの大前提となる組織ミッションや経営方針の理解に関して大きな差があること自体が、この項目に関する組織自体の問題点を表している。

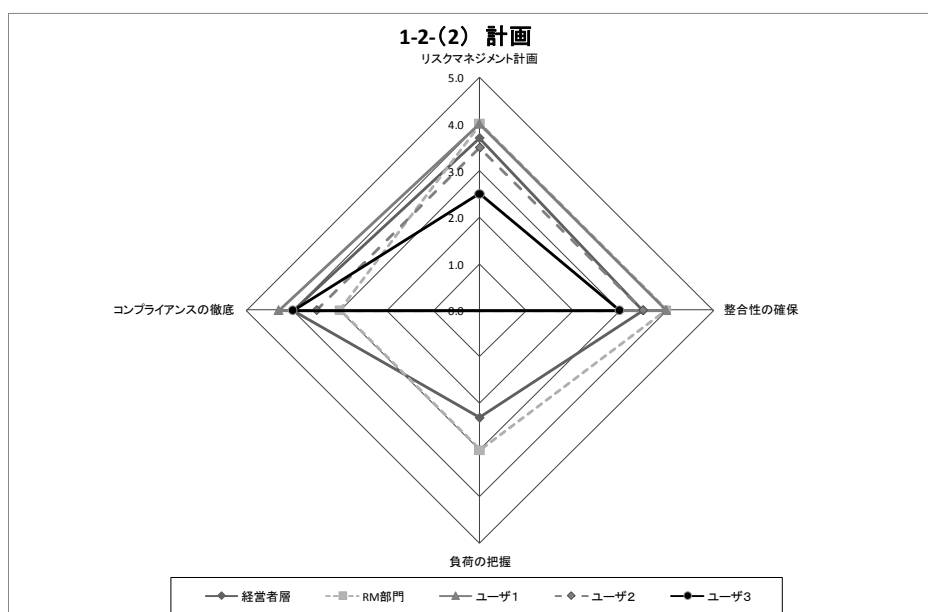
【チャート 8 当該組織と外部環境に関する的確な把握】



社会環境や社内状況の変化および投資資源の把握に関してユーザ 3 の評価が低いことは、この部門が自分の業務以外に関心が薄く、状況の変化に気づきにくいことを示している。

リスクマネジメント風土の構築に関して、RM 部門の評価がレベル 2 未満であることは、この組織のリスクマネジメント環境が十分でないことを端的に示している。また、RM 部門やユーザ部門に比べて経営者層の評価が相対的に高いことにより、実際よりもリスクマネジメント環境が不十分であることに経営者層が気づくことを遅らせる可能性を生む。このことは、投資資源の把握に関して RM 部門の評価が高いことも、その傾向を助長する可能性を示している。

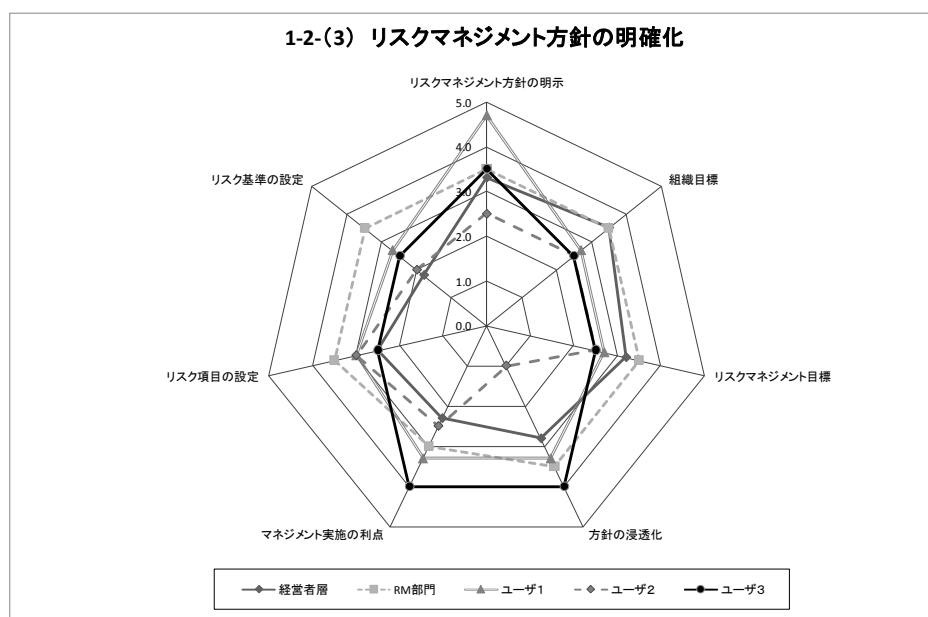
【チャート 9 計画】



リスクマネジメント計画や整合性に関してユーザ3の評価が低いことは、現場がリスクマネジメントの活動に対して組織のマネジメント活動として十分に納得しておらず、個人的ながんばりの中で実施しているような状況を示している。

しかしながら、RM 部門の評価レベルは 4 である。ユーザ部門間のギャップに鑑みて、RM 部門としては、回答部門に対して何らかの対応（指導・助言・勧告）をすべき状況を示している。

【チャート 10 リスクマネジメント方針の明確化】

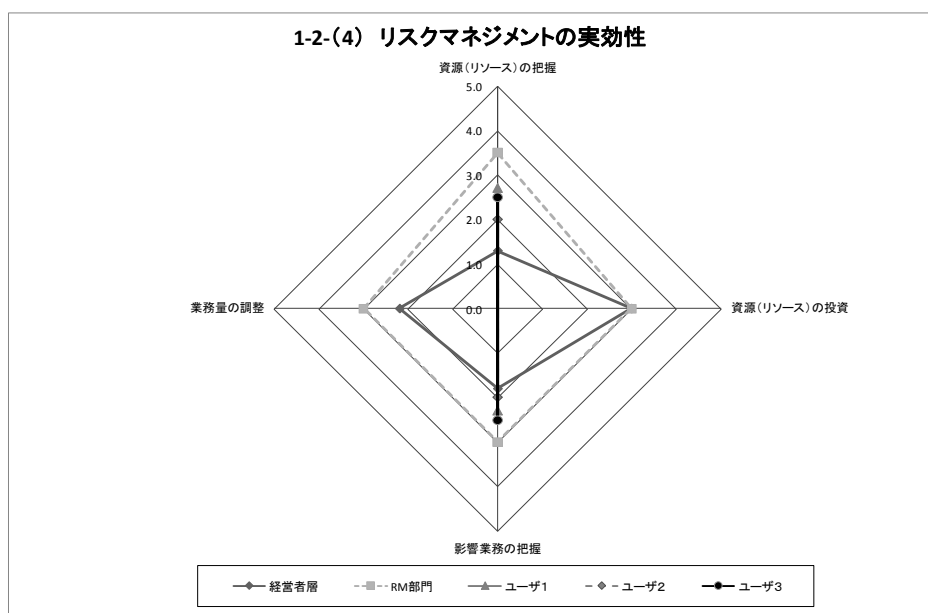


方針の浸透、利点の説明、リスク項目や基準設定について、ユーザ部門の評価が非常に低いのは、チャート 9 と同様にリスクマネジメントが組織的にではなく個人的ながんばりによって行われることを示している。

リスク項目や基準に関して、経営者層の評価も低いにも関わらず、RM 部門の評価が高いのは、リスクマネジメントがまだ RM 担当者から多くの人がやらされているような状況にある可能性を示している。

また、ユーザ部門の評価が 3 グループとも形が歪（いびつ）になっているのは、リスクマネジメントに関する理解や取組みが部署によって異なり、組織全体としての活動となりえていないことを示している。

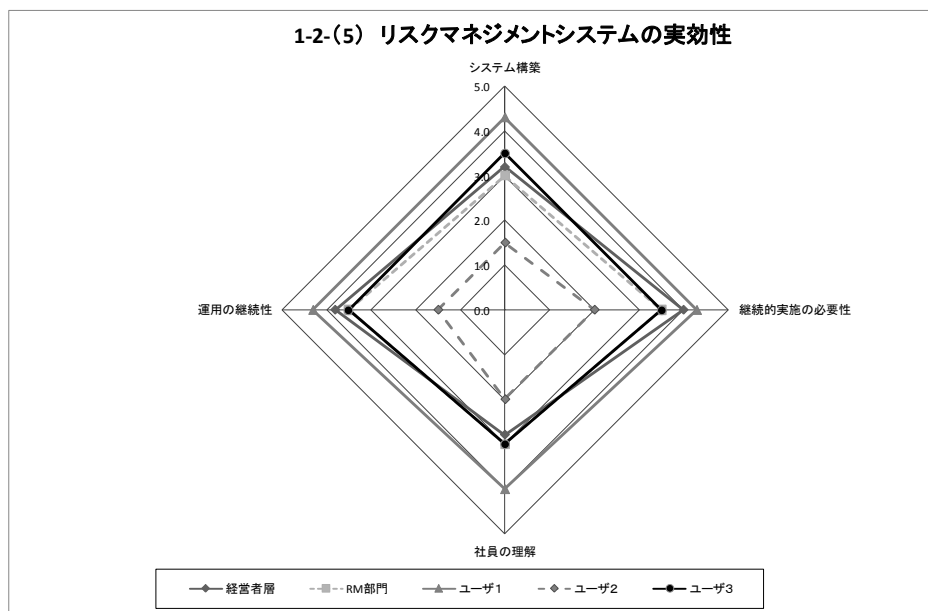
【チャート 11 リスクマネジメントの実効性】



この項目もチャート 10 と同様に RM 部門の評価が他よりも高い。

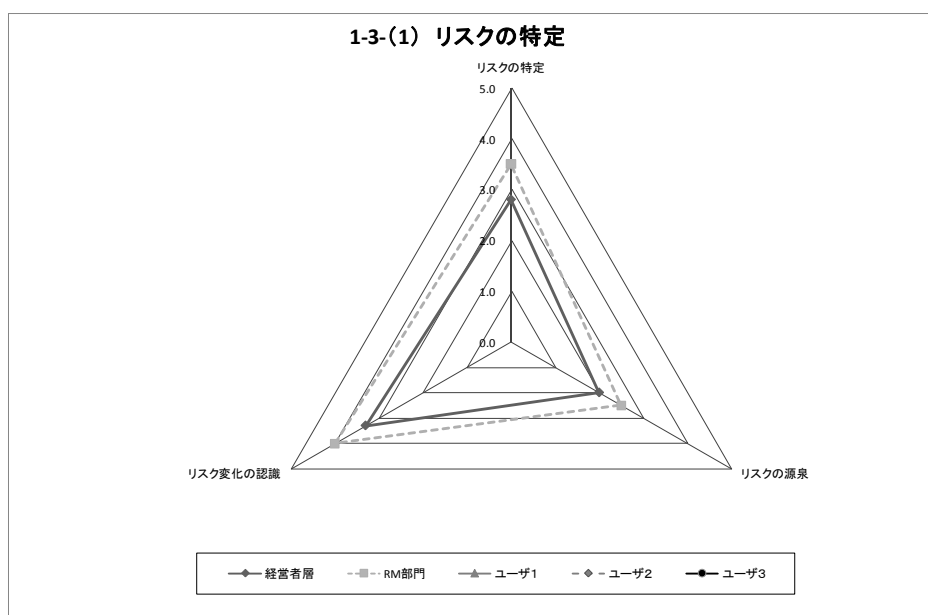
このことは、前項と同様にこの組織のリスクマネジメントが RM 担当者により引っ張られている状況を示している。

【チャート 12 リスクマネジメントシステムの実効性】



この項目もユーザ部門と経営者層、RM 部門の評価の乖離が大きい。特にユーザ 2 と他との差が大変大きいのは、リスクマネジメントが組織的に行われていない、すなわちシステムとしての運用がなされていないことを示している。

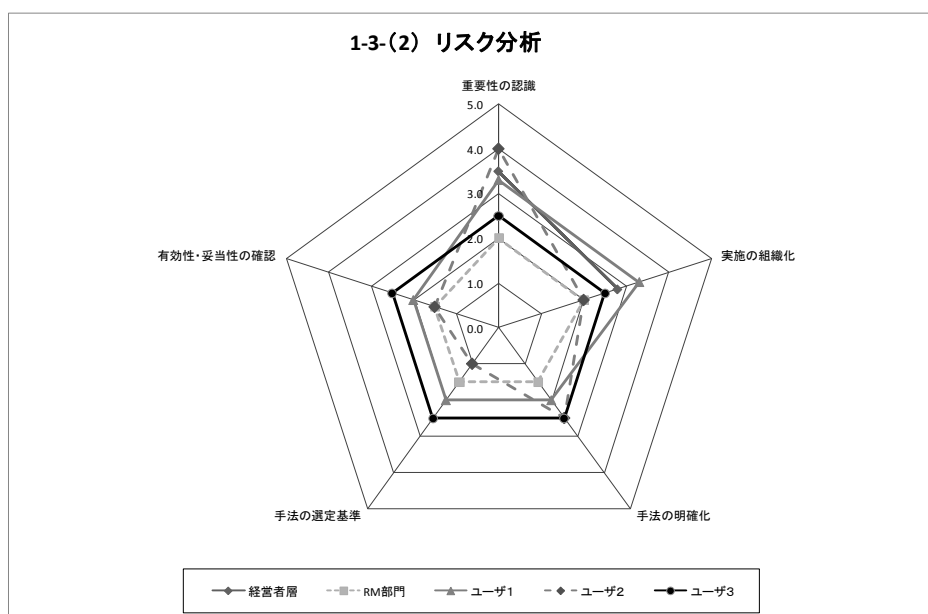
【チャート 13 リスクの特定】



リスクアセスメントにおけるリスクの特定についての評価の特徴は、リスクの源泉（リスク発生の潜在的要因の理解）の評価が他の項目より低いことにある。このことは、一般的にはリスクに関する理解レベルが十分でないことを示している。このような場合、リスクの把握が発生したトラブルの整理になりやすいので注意が必要である。

特に経営者層の理解レベルが低い場合には、発生した事故や不祥事などに対する事後的な対応になりがちで、未然防止がうまくいかない場合が多い。

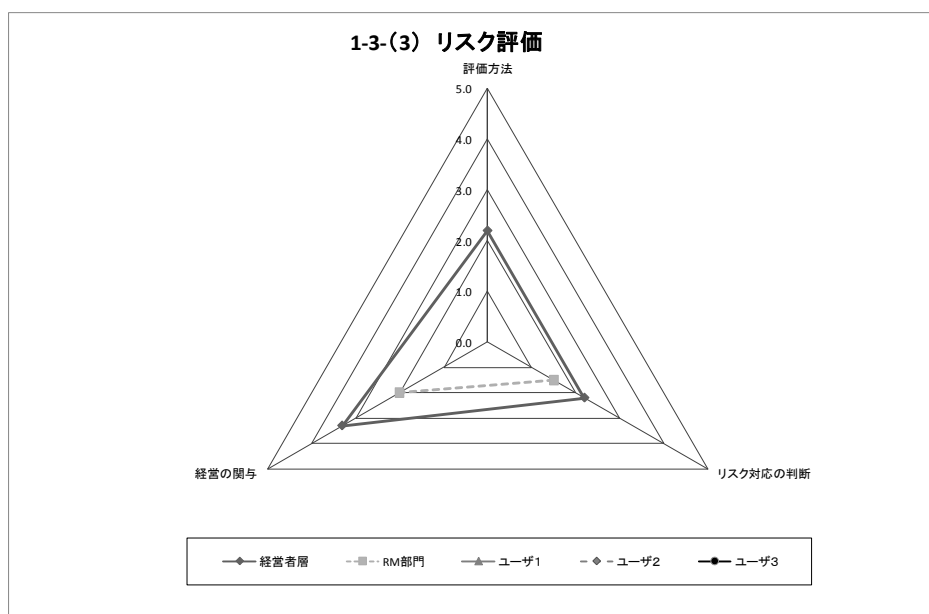
【チャート 14 リスク分析】



リスク分析では、重要性の認識以外、多くの評価項目が低いレベルにとどまっている。このことは、分析活動が個人の経験に基づいて実施されていて、必要な分析手法に関する教育や検討が

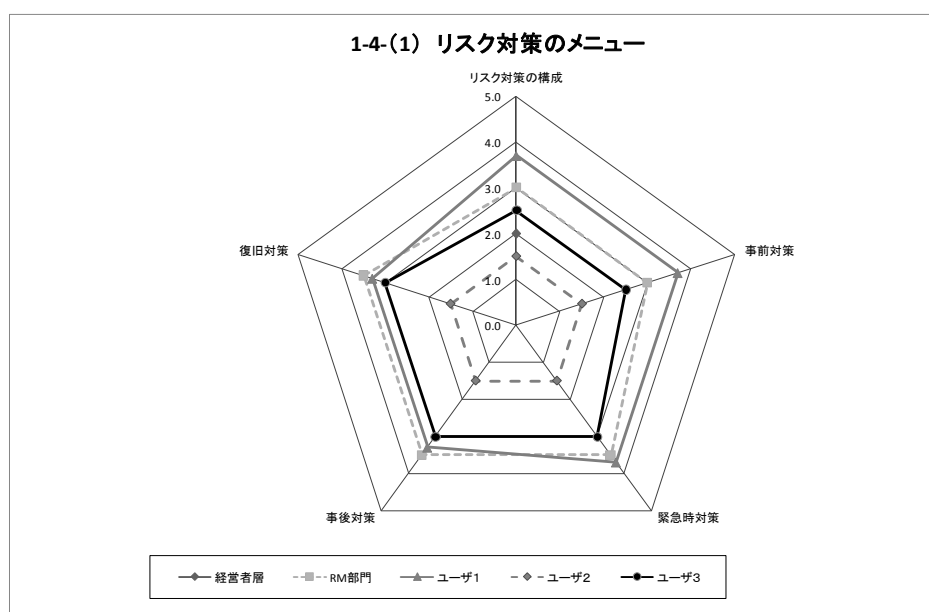
不十分である可能性が高いことを示している。

【チャート 15 リスク評価】



リスク評価で特徴的なことは、RM 部門の評価が低いことである。これは、リスクマネジメント活動において、全組織的な評価基準がない、またはリスク対応検討が全社のレベルでは行われていないなど、部門単位で分析したリスクに対する評価や対応が当該部門で実施されているような場合に見受けられる傾向である。

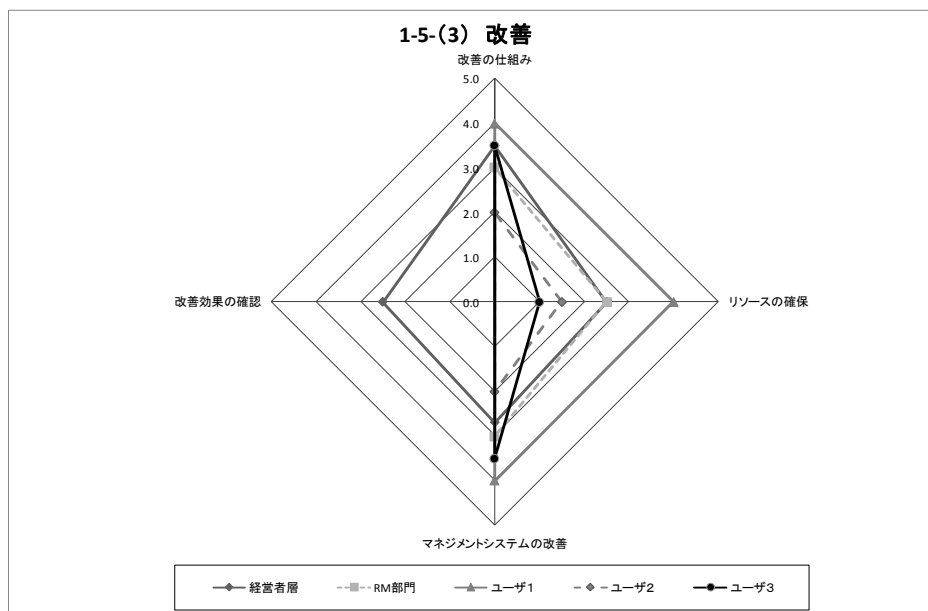
【チャート 16 リスク対策のメニュー】



リスク対策に関して、RM 部門がレベル 3 以上で、他の大半がレベル 3 未満であり、しかも部門ごとのバラツキが大きいという特徴がある。

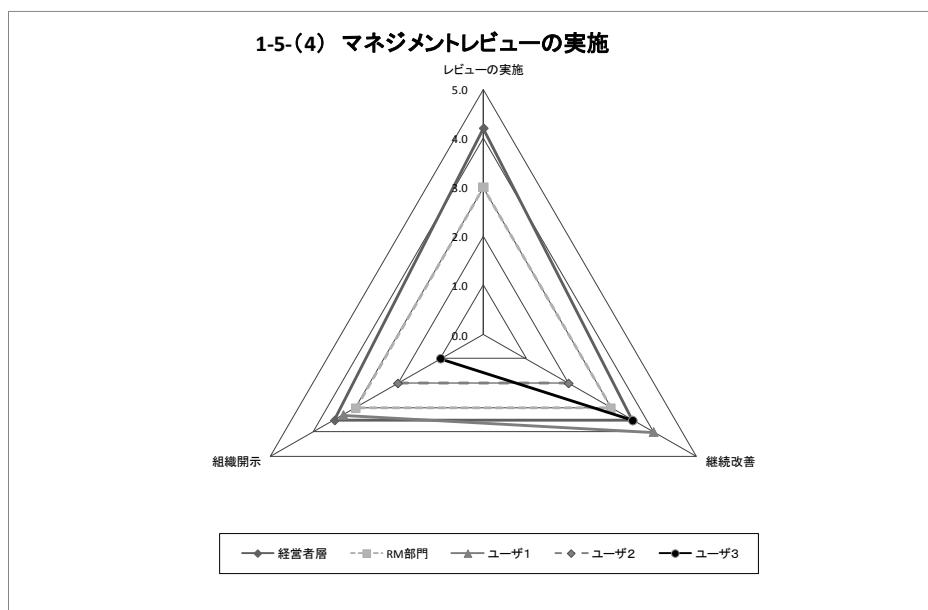
このことは、対策の実施以前にリスク対策そのものの理解というレベルから組織として共有されていない可能性がある。

【チャート 17 改善】



改善におけるリソースの確保について、全体的に評価が大変低いところが問題である。このことは、この組織におけるリスクマネジメントの実施にかなり無理があり、負担感が大きい可能性を示している。また、改善の仕組みに関して、ユーザ2の評価が大変低いことや、相対的にRM部門の評価が高いことも、リスクマネジメントが現場になじんでいない可能性を示唆している。

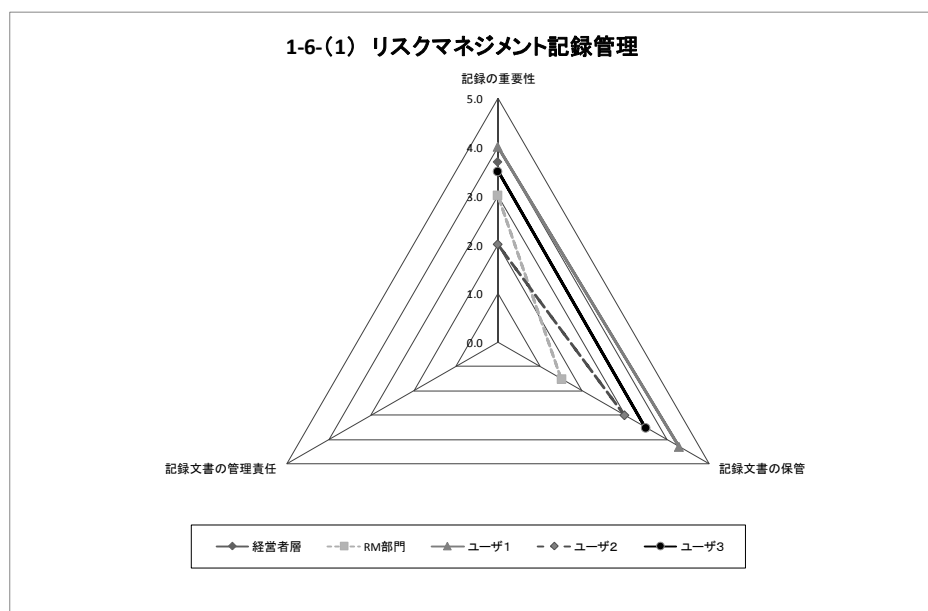
【チャート 18 マネジメントレビューの実施】



マネジメントレビューの実施に関する特徴は、経営者層の評価に比べて現場の評価が低いということである。このパターンは、経営者層が現在の状況において、自組織の状況を過大評価、もしくは楽観視している可能性が大きい。

【チャート 19 リスクマネジメント記録管理】

(注) この評価は全部門とも「記録文書の管理責任」の回答データがないケース



本来、組織的に実施されていれば、評価の差が出ない項目である。この評価からは、記録が組織的には実施されてないことが見受けられる。

4.1.3 JRMS の評価結果の活用

「4.1 JRMS 分析チャートの読み方」では、JRMS の評価チャートを用いた組織分析の例を示した。「4.1.1 ギャップの判定の考え方」で記したとおり、ギャップの発生原因はその組織や評価時期によりさまざまである。

評価において重要なことは、そのチャートが示す多くの可能性を検討してみることである。検討に際しては、一つのチャートからその組織の傾向を決めつけるのではなく、複数のチャートから見えるその組織の状況や活動傾向に留意する必要がある。

さらには、このチャート分析において組織状況を検討し課題の存在が懸念される場合には、その評価対象に対してヒアリングを行う等の活動により、その問題点の可能性に関して検証を行うべきである。

組織の進歩は急速に行われるものではない。大切なことは、定期的に組織状況を検証し、現在の活動レベルを把握し、改善を継続することである。

JRMS には組織間のギャップ分析のほかに、同じ組織の経年変化を比較する機能も有している。

JRMS の多様な機能を活用し、組織の改善を図られたい。

4.2 実証実験分析評価例

本報告書では、協力企業のうち A 社から回答結果および分析に関する報告書への使用許諾をいただき、ここに分析例として紹介させていただくことにした。以下、JIPDEC より依頼した企業への分析回答という形式から、表現は「敬体」とさせていただくこととする。

4.2.1 A 社の実証実験概要

- (1) 事業概要：アプリケーションの設計および開発・ネットワーク構築を業とする企業
- (2) 実証実験期間：2008 年 11 月 5 日～11 月 18 日
- (3) 実験対象項目：第 1 部 第 1 章「組織全体のリスクマネジメントの実践」(Advanced 編 Ver.6)
第 2 章「内部統制リスクと経営者の対応（総論）」(Advanced 編 Ver.5)
第 3 章「内部統制リスクの分析」(Advanced 編 Ver.5)
第 4 章「IT 統制」(Advanced 編 Ver.5)
- (4) 回答対象者：2 部門 計 10 名
 - ①回答部門別内訳 経営者層 4 名
RM 部門 4 名
ユーザ部門 2 名
 - ②役職別内訳（管理者／一般社員数） A 部門 3／2 名
B 部門 1／4 名

4.2.2 A 社リスク評価レポート

ここでは、A 社がレーダーチャートを用いたリスク分析結果をとりまとめた各章の自社分析評価として出された「2. 評価レポート」に対し、参考としてコメントを記載している。

なお、実証実験の段階で、回答対象部門の指定に不備があったため、全部門とも回答対象外となっている項目が含まれていることをご了承いただきたい。

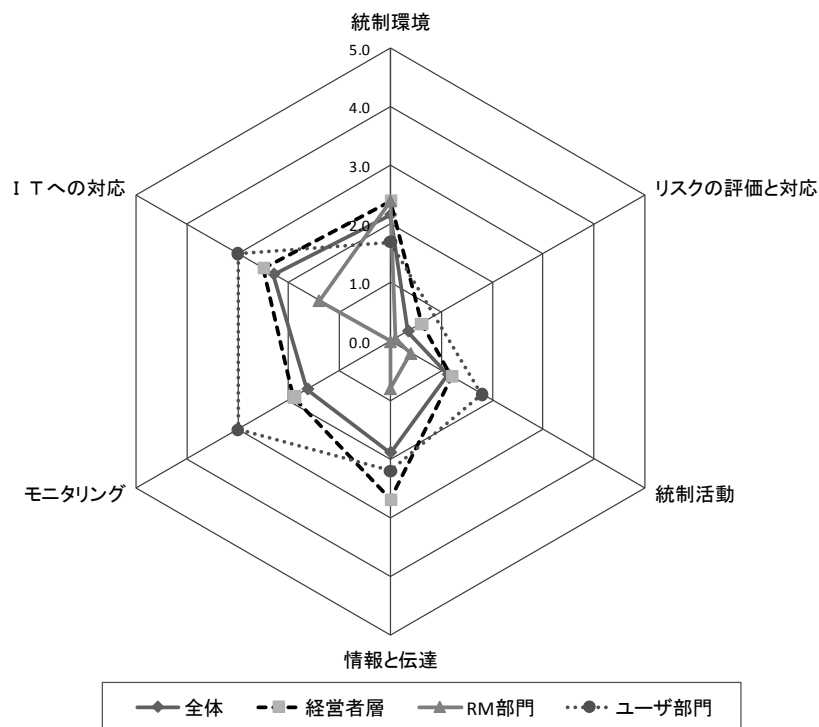
4.2.2.1 第1部「組織経営とJRMS（経営編）」の分析結果（全体）

第1章：組織全体のリスクマネジメントの実践
1. レーダーチャート
1. 組織全体のリスクマネジメントの実践 経営環境の変化とリスクに対する組織文化の醸成 リスクマネジメントシステムの基盤 リスクアセスメント 組織のリスク対策 リスクマネジメントシステムの維持 リスクマネジメントシステムの継続改善 文書化に関する要求事項 0.0 1.0 2.0 3.0 4.0 5.0 ● 全体 ■ 経営者層 ▲ RM部門 ◆ ユーザ部門
2. (A社による) 評価レポート
現時点でリスクマネジメントが啓蒙されてはいるが、仕組みとして整備されておらず、実質的に経営陣からのトップダウンでリスク対応が行われている。 経営陣と管理職ではおおまかに意思の疎通がとられており、認識は近いが、ユーザ部門とは乖離がある。 文化の醸成の低さと他の項目の高さからはリスクマネジメントの仕組みが明示されていないが、経営陣（や管理職）に任せておけば安心と考えていることが想定される。ユーザ部門の意識を高めることが必要。
評価レポートに対するコメント
組織全体のリスクマネジメントの実践においては、重要な課題は「リスクに対する組織文化の醸成」です。この点について経営陣によるトップダウン方式でのリスク対応が確認できなくはありません。しかしながら、組織としてどの程度の評価レベル（ベンチマーク）を基準に考えるかにより、評価は異なるといえます。とりわけ、リスクマネジメントに関して専管部門であるべきRM部門に比べ、「リスクに対する組織文化の醸成」以外ではユーザ部門が相対的に高く評価していることは、ユーザ部門への依存度が高いことに起因していると思われます。リスクに対する意識を高めるべきは、経営者層を含めた組織全体に言えることであり、リスクマネジメントに関する仕組みをどうするかが問われているといえるでしょう。

第2章:内部統制リスクと経営者の対応

1. レーダーチャート

2. 内部統制リスクと経営者の対応(総論)



2. 評価レポート

経営陣の評価の高さに比べ、管理職の評価が極端に低くなっている。
経営陣による判断が管理職に伝わる際、経営陣が伝達したと思っているものに比べ、管理者側が正確に受け取っていないと意識している可能性を考えたい。

評価レポートに対するコメント

内部統制については、第1章と異なり、「リスク評価と対応」を除き、経営者層においてある程度高いレベルの評価がなされています。

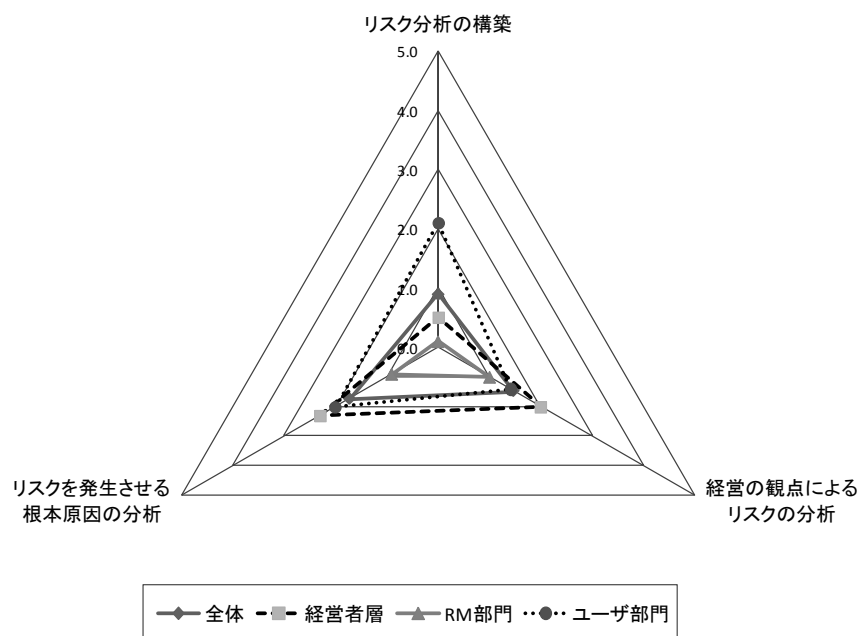
しかしながら、内部統制において「リスク評価と対応」はきわめて重要な課題です。この点に関する経営者層のリスク対応への姿勢を特にRM部門がどのように受け止めているのか、全体的に認識ギャップが大きすぎます。

とりわけ、情報と伝達（コミュニケーション）におけるギャップの問題だけとは言い難いと思います。経営者としても、特に「リスク評価と対応」と「統制活動」について組織として最適なレベルの確認をもとにリスク認識を深め、さらに「IT統制」、「モニタリング」については組織全体に対し、その意義の徹底を図るべきでしょう。

第3章：内部統制リスクの分析

1. レーダーチャート

3. 内部統制リスクの分析



2. 評価レポート

第2章同様、経営陣に比べて管理者の評価が低い。仕組みとして存在しないため、経営陣はそれなりにできていると考えているが、管理者は自身が理解できていないと思っているようだ（経営陣と前提知識が違うため、現状に対する過不足がつかめない）。

ユーザについては、第1章と同じく経営陣に対する一任をもって、内部統制リスクを評価していると思われる。

評価レポートに対するコメント

経営者層と管理者との間で内部統制リスクに対し「前提知識」が異なるため、現状に対するギャップが存在すると考えること自体が問題かもしれません。むしろ、RM部門におけるリスク認識の不足をいかに改善するかが重大な課題といえるでしょう。

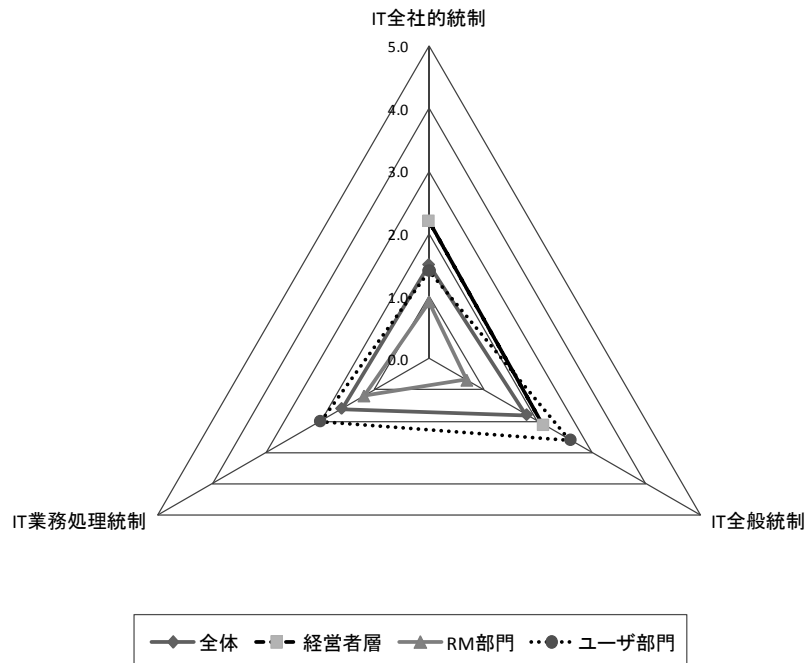
しかも、「リスク分析の構築」に関し、ユーザ部門に比べ評価レベルが低いことを経営者層がどのように理解しているのか、内部統制リスクに関し、大和銀行ケースにみられるように、経営者層が部門の下位層に委ねておいたことへの反省があることを認識すべきです。したがって、ユーザ部門に一任しているという認識自体に検討の余地があるといえます。

なお、「リスク分析の構築」において評価レベルが低いにもかかわらず、「経営の観点によるリスク分析」および「リスクを発生させる根本原因の分析」について経営者層がいずれの部門より高い評価レベルを示しています。このことから内部統制のリスク分析の意味を経営者層がどの程度理解しているのか、問う必要があるかもしれません。

第 4 章: IT 統制

1. レーダーチャート

4-1 IT全社的統制



2. 評価レポート

A 社では ISO9001、14001 などの取得に向けた活動を行っておらず、J-SOX に対しても同様の対応をしていることから、他の章に基づき個人的にやっている（人がいる）と判断しているようだ。

これまでの延長で漫然と認証を取得しないとするのではなく、認証の取得に対するスタンスを決め、それに基づいた行動が必要と思われる。

評価レポートに対するコメント

IT 全社的統制について、それぞれの部門における個人的な対応ですませていることでよいのかどうか、組織としてリスクマネジメントの観点から成熟度モデルにおけるベンチマークの設定を早々に検討する必要があると思われます。

以下に「第 1 部」についての概要評価を参考としてとりまとめ、示す。

4.2.2.2 第 1 章「組織全体のリスクマネジメントの実践」の詳細分析

1. 全体評価

- (1) 全般的に経営者よりユーザ部門の評価が高い傾向があります。（「1-1-(1) 組織のミッションと経営方針の明示」、「1-2-(4) リスクマネジメントの実効性」、「1-3-(2) リスク分析」、「1-4 組織のリスク対策」、「1-5 リスクマネジメントシステムの維持」、「1-6 リスクマネジ

メントシステムの継続改善」、「1-7 文書化に関する要求事項」)

このことは、以下の要因が考えられます。

- ①経営者自身は経営にいろいろ問題があると考えていますが、社員は相対的に経営者を信用しています。「1-3-(3) リスク評価」においてリスク評価における経営者の関与だけが突出して高いことがそのことを示しています。
- ②リスクマネジメントで実施すべきと考えている管理内容またはレベルが、経営者と社員間で異なっています。(他の項目も考えあわせると社員の理解不足の可能性もあります。)
- (2) リスクマネジメントに関する基本的活動はこれから基礎を作っていく状況です。(1-2 から1-7 までの評価レベルが小さい)

また、「1-2-(5) リスクマネジメントシステムの実効性」において、リスクマネジメントシステムの構築や運用の継続性において、ユーザの評価レベルが高くなっていますが、他の評価事項と考え合わせると、A 社においてリスクマネジメントシステムの構築や継続に関する仕組みが存在するとは考えづらいです。リスクマネジメントシステムに関する基本的な教育が必要と考えられます。「1-5-(3) 改善」の図からも同様のことがうかがえます。

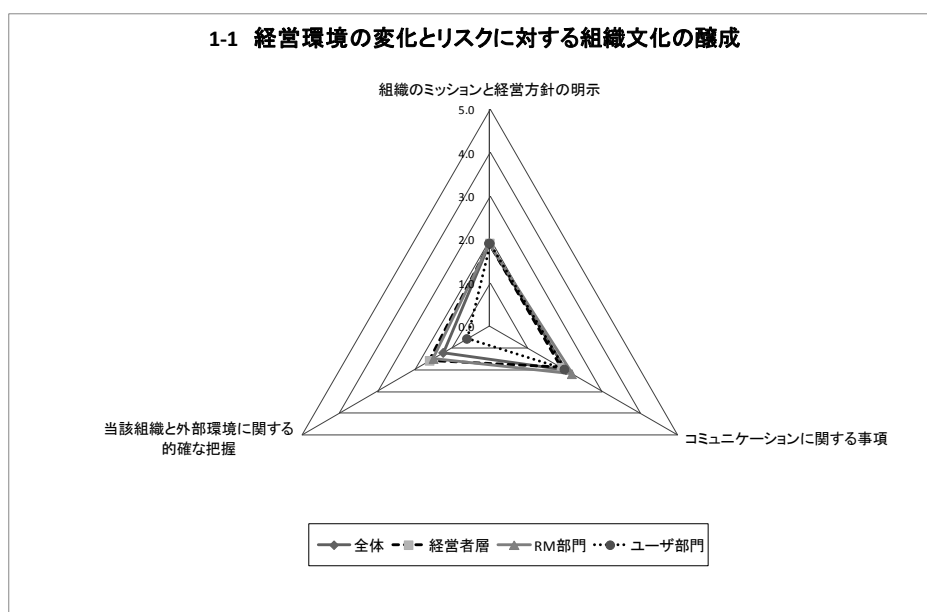
- (3) 階層間で極端に評価の異なる事項があります。

「1-2-(4) リスクマネジメントの実効性」、「1-3-(2) リスク分析」

- (4) 「1-1-(3) 当該組織と外部環境の的確な把握」に関して、経営者や RM 部門はかなりのレベルで実施できていると評価していますが、社員にその実感がないのは、その検討内容が実際の業務において反映されていないか、または説明不足である可能性があります。「1-2-(2) 計画」においても同様の傾向が見られます。
- (5) 「1-3-(2) リスク分析」において、リスク特定の重要性についてユーザ部門の評価が他の事項よりも低く、その事項に関して経営者等よりも低くなっていることも、リスク分析が基本から理解されていないことを示しています。

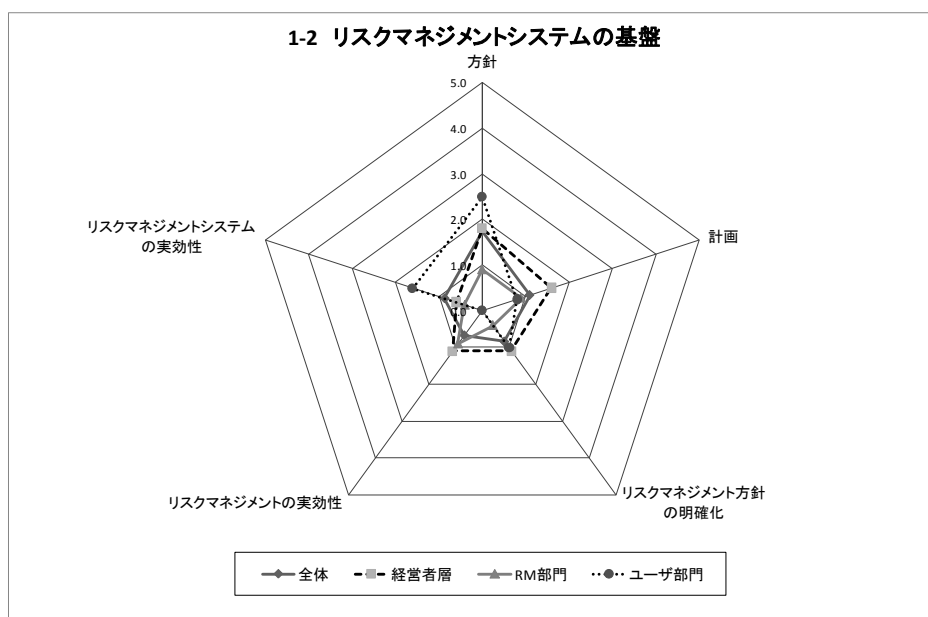
2. 第2階層の分析

【1-1 経営環境の変化とリスクに対する組織文化の醸成】



「1-1 組織全体のリスクマネジメントの実践」に関し「組織のミッションと経営方針の明示」、「コミュニケーションに関する事項」は重要な意味を有しており、この点は経営者層および RM 部門がユーザ部門に比べて若干高い自己評価を行っていることはよいとしても、組織としての評価レベルをどこに置くべきか合意形成が必要でしょう。なお、「当該組織と外部環境に関する的確な把握」についてユーザ部門はかなり低く評価しています。経営環境についての認識をユーザ部門としても考慮すべきであり、経営者層としてはそれなりの周知徹底を図るべきでしょう。

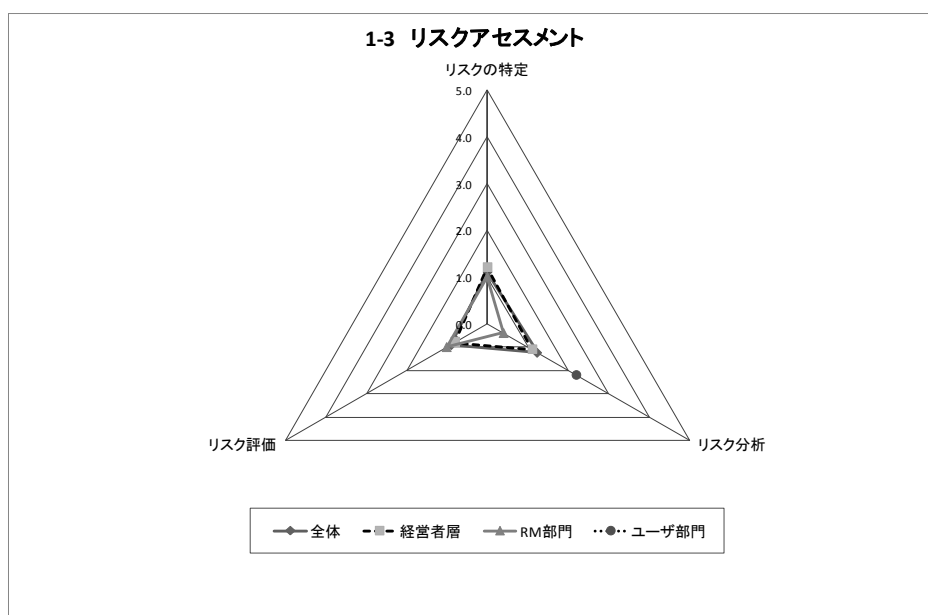
【1-2 リスクマネジメントシステムの基盤】



「1-2 リスクマネジメントシステムの基盤」に関する「方針」、「計画」、「リスクマネジメント方針」、「リスクマネジメントの実効性」、「リスクマネジメントシステムの実効性」に関し評価は相対的に低く、とりわけ「リスクマネジメントシステムの実効性」に関する経営者層および RM 部門の評価の低さについては、その理由を課題として取り上げ、改善の余地があるか検討すべきと思われます。

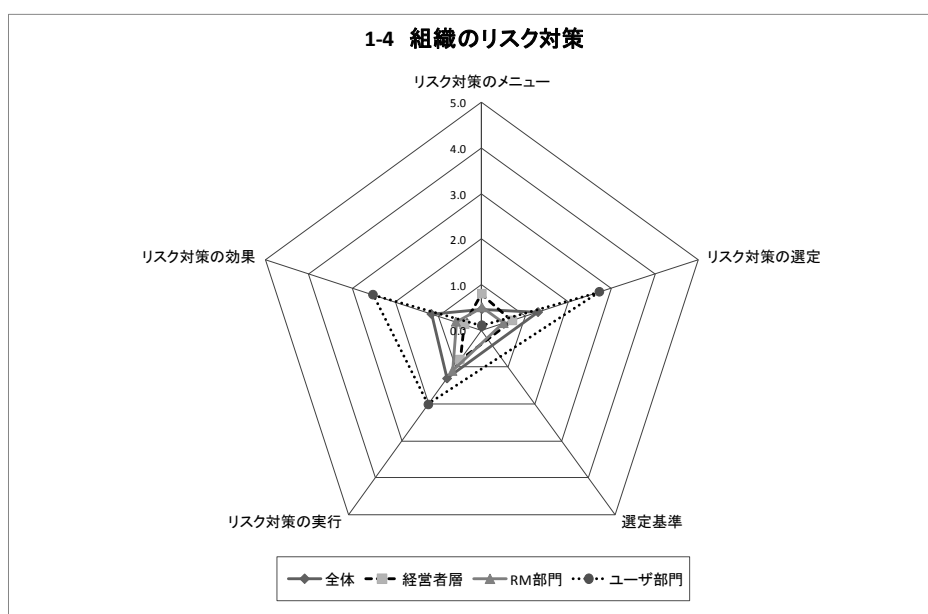
また、ユーザ部門では「リスクマネジメントシステムの実効性」について相対的に若干高い評価が見られますが、「リスクマネジメントの実効性」についての認識については検討を要します。

【1-3 リスクアセスメント】



「1-3 リスクアセスメント」における「リスクの特定」、「リスク評価」について、全体的に評価レベルは低いのですが、ユーザ部門における「リスク分析」の評価が相対的に高く、回答に整合性が見られません。この点に関しては、リスクマネジメントにおけるリスクアセスメントの意味を再考することが必要でしょう。

【1-4 組織のリスク対策】



(「選定基準」は回答対象部門の指定がなかったため、全部門回答なし)

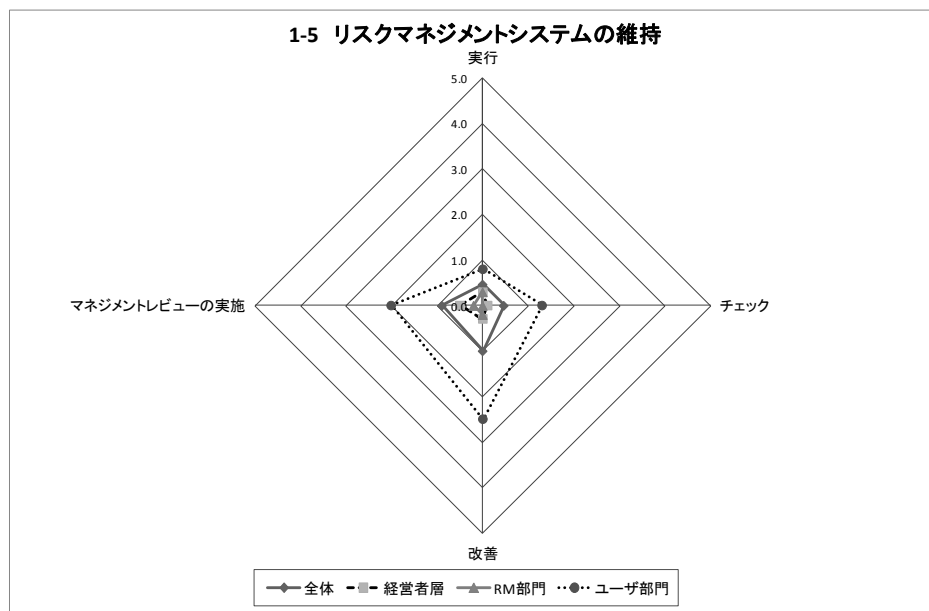
「1-4 組織のリスク対策」に関し「リスク対策のメニュー」については各部門ともに低い評価であったのに対し、「リスク対策の選定」、「リスク対策の実行」、「リスク対策の効果」ではユーザ部門の評価が相対的に高く、経営者層、RM 部門共にユーザ部門に任せきりといった認識が感

じられます。

組織として、こうした実態が望ましいか否か、検討の余地があるといえます。

特に、組織としてゴーイングコンサーンを考える場合、組織としてリスクアセスメントとの連携を考慮すべきといえます。

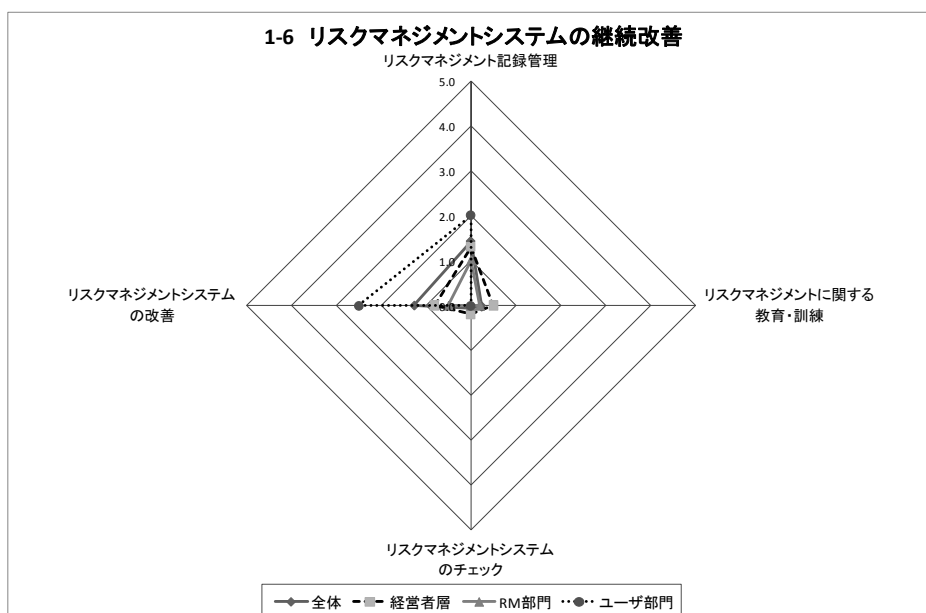
【1-5 リスクマネジメントシステムの維持】



組織として、リスクマネジメントシステムの維持はゴーイングコンサーンの視点から不可欠といえます。「1-5 リスクマネジメントシステムの維持」について、「実行」、「チェック」、「改善」「マネジメントレビューの実施」のいずれにおいても経営者層、RM 部門の評価は低く、ユーザ部門の「改善」が評価レベルは低いながらも突出しており、上記「1-4 組織のリスク対策」と同様に、ユーザ部門に信頼を置いているためか、一任している印象が強いといえます。

組織として PDCA のマネジメントサイクルの徹底を図る仕組み作りが必要でしょう。

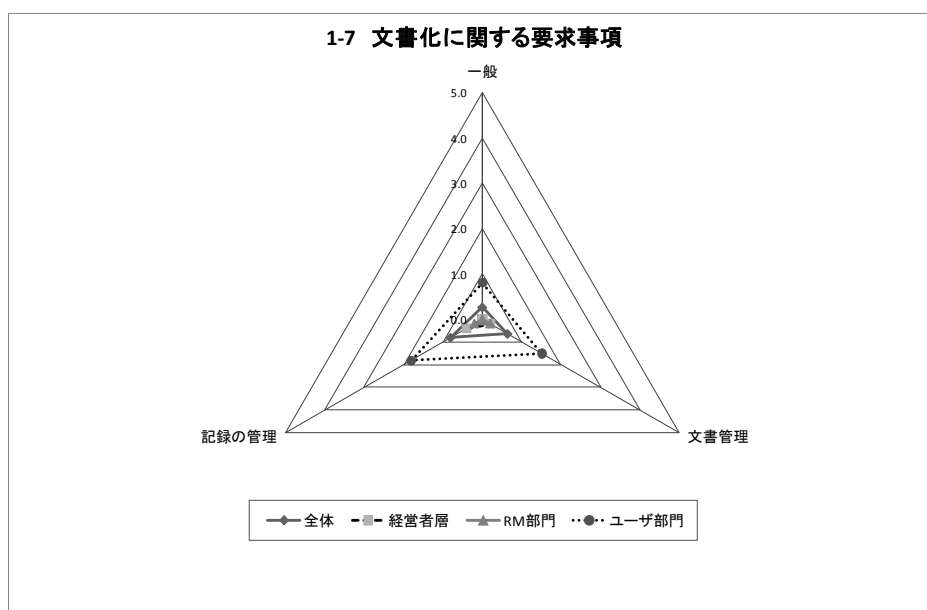
【1-6 リスクマネジメントシステムの継続改善】



リスクマネジメントシステムの継続改善は PDCA サイクルから重要です。特に、「リスクマネジメントに関する教育・訓練」および「リスクマネジメントシステムのチェック」について、経営者層はさほどこの点についてこれまで考慮してこなかった傾向がうかがえます。

また、「リスクマネジメント記録管理」、「リスクマネジメントシステムの改善」についても RM 部門よりユーザ部門に（信頼性ゆえか）依存してきたきらいが見えます。リスクマネジメントにおいては特定の部門に任せ、そこがしっかりやっていたらそれで済む場合だけではありません。全体的な視点から検討・実施することが求められます。

【1-7 文書化に関する要求事項】



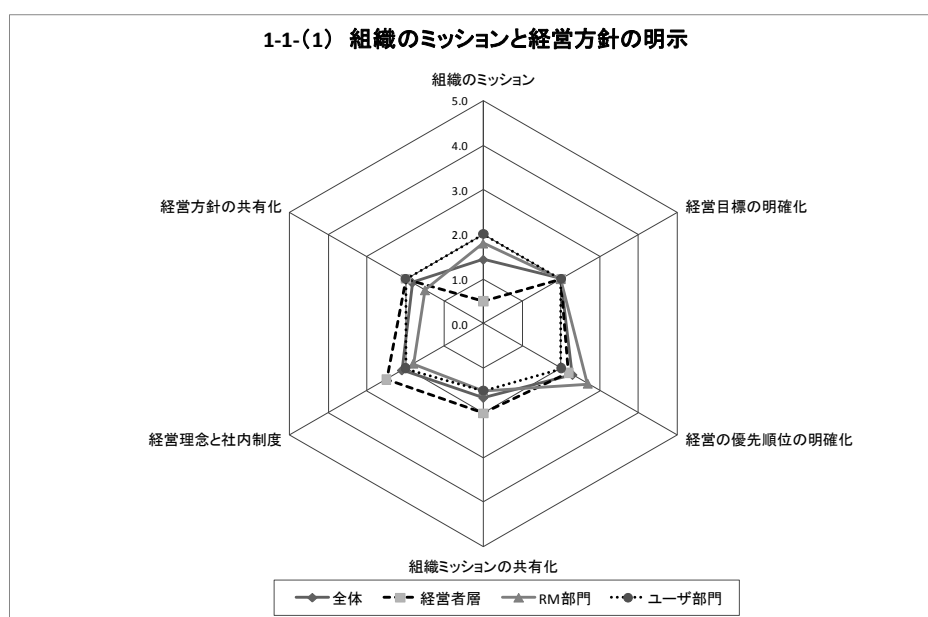
「1-7 文書化に関する要求事項」では、「一般」、「文書管理」、「記録の管理」が重視されています。

RM 部門では D/K の回答が多く、経営者層においても低い評価しか見られません。

概して、ユーザ部門が文書化についても個々の立場に応じ、それなりに要求事項を考慮し対応していることが読み取れます。これまでも触れてきましたが、現在の可変的な経営環境下において、組織全体にとってリスクマネジメントをどのように考えるか、検討の余地があるといえます。

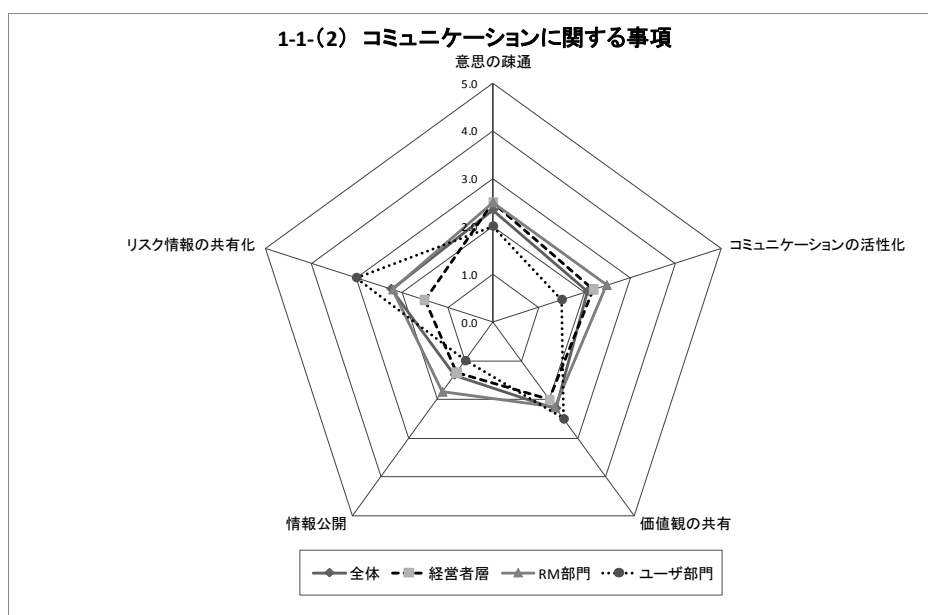
3. 第3階層の分析

【1-1-(1) 組織のミッションと経営方針の明示】



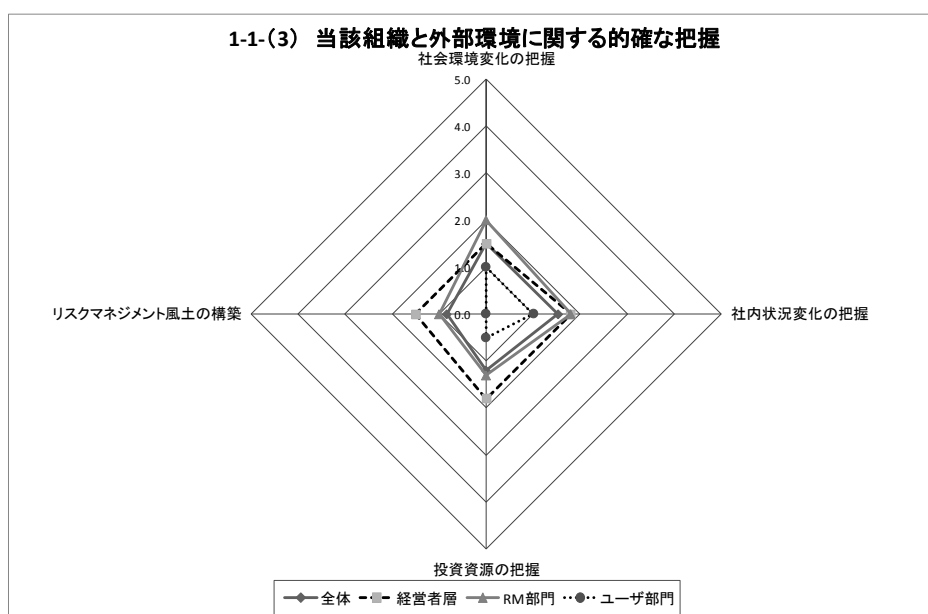
「1-1-(1) 組織のミッションと経営方針の明示」は、組織全体が共有すべき課題です。しかし、経営者層では「組織のミッション」が非常に低い反面、他の項目では他部門より相対的に高い評価を示しており、ミッションの明確化の点で検討の余地があります。「経営の優先順位の明確化」では RM 部門が経営者層と同様、高く評価していますが、他の項目ではユーザ部門より低く、ギャップの存在について全社でよく議論する必要があると思われます。

【1-1-(2) コミュニケーションに関する事項】



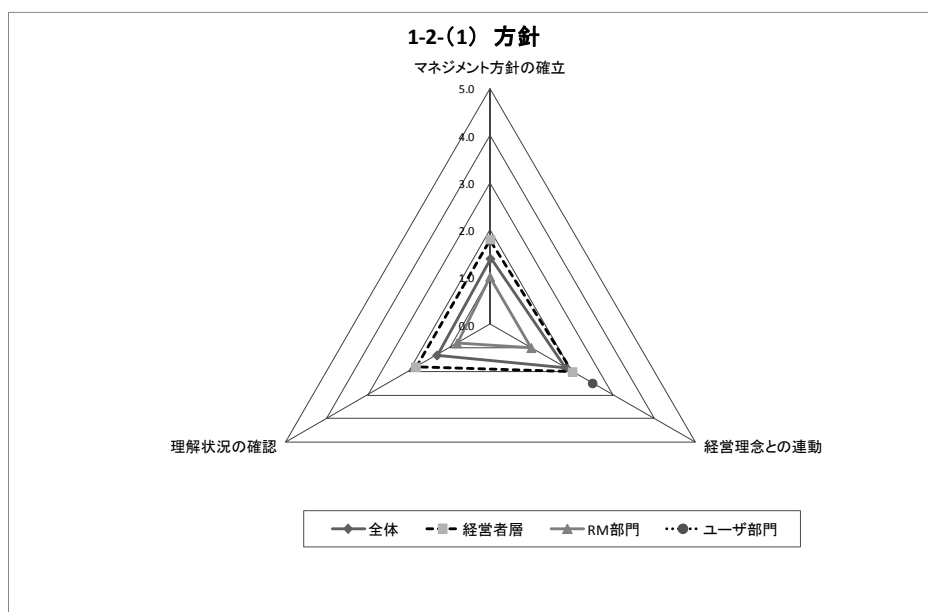
「1-1-(2) コミュニケーションに関する事項」は、特に価値観の共有の点から重要です。「意思の疎通」では経営者層と他部門とのギャップがかなり大きく、また、「コミュニケーションの活性化」ではユーザ部門が低い反面、「リスク情報の共有化」についてはユーザ部門に比べ他部門の評価が低く、組織における部門間でかなりのバラツキが見られます。組織としての意思や情報の共有というリスクマネジメント環境として重要な風土が十分ではない可能性を示しており、この点に関して、組織としての評価レベルについてのベンチマークを考慮するためにも、各回答者間の回答のギャップ分析が必要といえます。

【1-1-(3) 当該組織と外部環境に関する的確な把握】



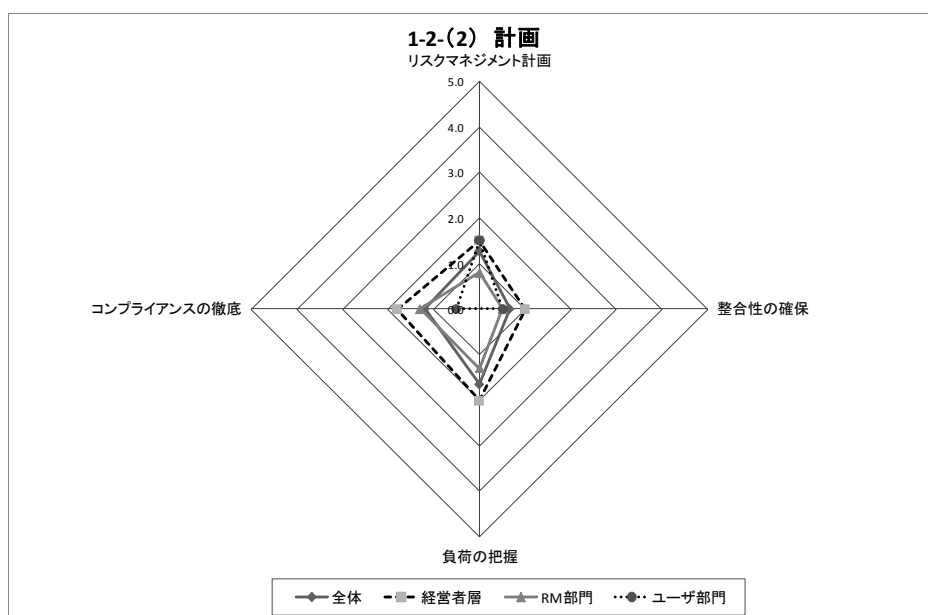
「1-1-(3) リスクマネジメント」において「当該組織と外部環境に関する的確な把握」は不可欠な課題です。「社会環境変化の把握」、「社内状況変化の把握」について RM 部門の評価レベルは相対的に高いとしても部門対応のレベルです。とりわけ、ユーザ部門の低さは部門としての把握に直接関係ないといった印象が見られます。管理部門と現場であるユーザ部門のバラツキが大きいためリスクマネジメントに関する認識の共有のなさを反映していると思われます。

【1-2-(1) 方針】



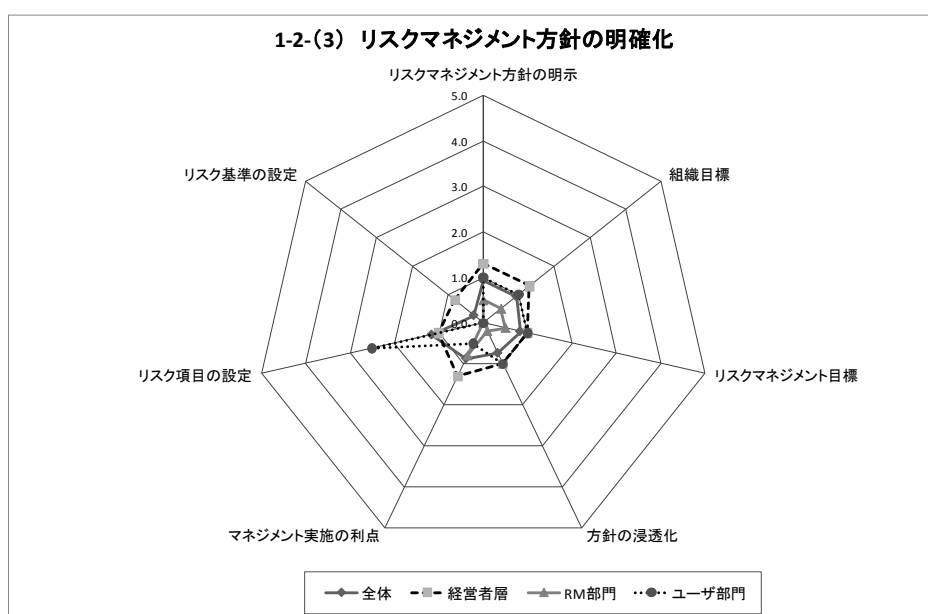
「1-2-(1) 方針」に関して評価レベルは相対的に部門対応レベル 2 であり、「経営理念との連動」に関してユーザ部門の 2.5 が他部門を超えているぐらいであり、組織として経営者層が「リスクマネジメント方針」をどう考え、組織対応を考えるかが課題と思われます。特に、経営者層において「マネジメント方針の確立」では、回答者 4 名中 2 名が評価レベル 3 でありながら残りの 2 名は 0 と 1 であり、ギャップの大きさがどこにあるのか、検討の余地があります。

【1-2-(2) 計画】



「1-2-(2) 計画」については「リスクマネジメント計画」から「整合性の確保」、「負荷の把握」、「コンプライアンスの徹底」まで、経営者層が全体をリードしている様子がうかがえます。しかしながら、全体的に質問に対する回答結果の評価レベルは低く、しかも、回答者間のバラツキも大きいため、そのギャップの原因分析を行い、問題の所在を確認することをお勧めします。

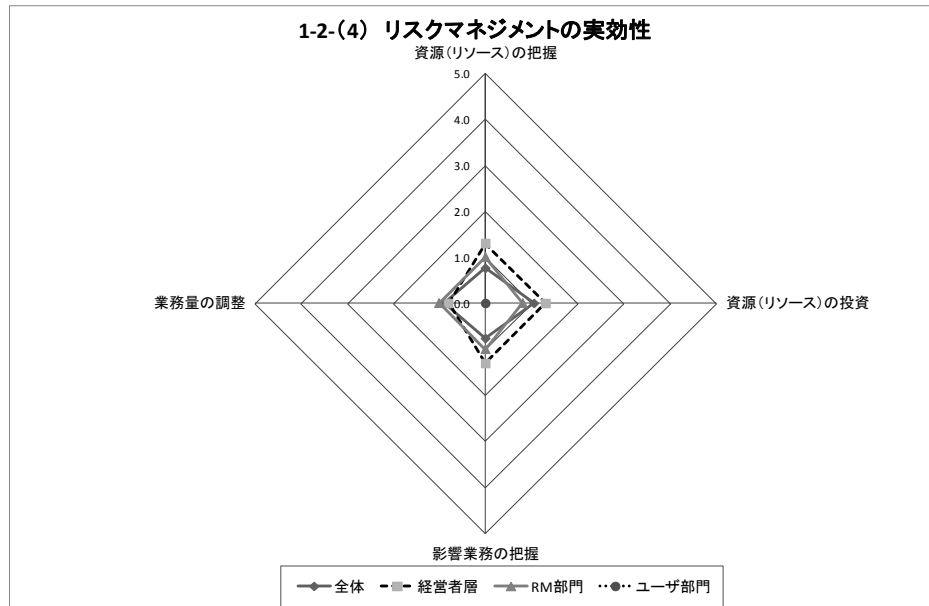
【1-2-(3) リスクマネジメント方針の明確化】



「1-2-(3) リスクマネジメント方針の明確化」における「リスクマネジメント方針の明示」、「組織目標」、「リスクマネジメント目標」、「方針の浸透化」、「マネジメント実施の利点」、「リスク基準の設定」については評価レベルが低いものの、一応、経営者層が部門対応レベルの回答を行っています。しかし、「リスク項目の設定」に関して、ユーザ部門では評価レベル 2.5 と高めと

なっていますが、回答者間では評価は 0 と 5 であり、極端なバラツキが見られます。組織経営とリスクマネジメント方針に関して有機的な結びつきを有するため、ギャップ分析を行う必要性が感じられます。

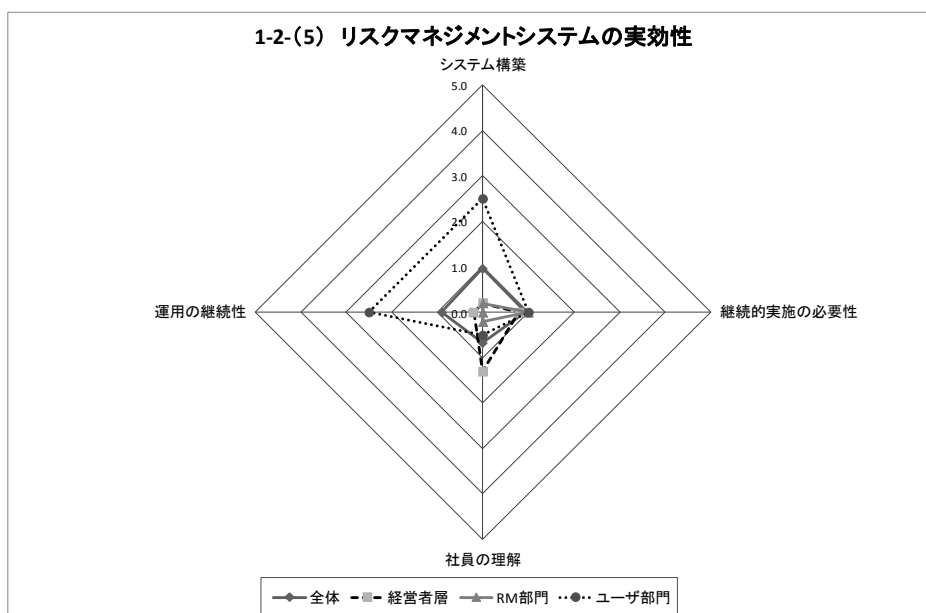
【1-2-(4) リスクマネジメントの実効性】



「1-2-(4) リスクマネジメントの実効性」に関しては、リスクマネジメントの実践上、資源（リソース）の把握が課題となるかもしれません。この点、「資源（リソース）の投資」については、経営者層として評価レベルは低い（1.3）ものの、他の部門より高い回答となっています。しかも、経営者層として、リスクマネジメントへの「資源（リソース）の把握・投資」、「影響業務の把握」については RM 部門よりも評価レベルが高いとはいえ、いずれにしても個人対応レベルという結果となっています。

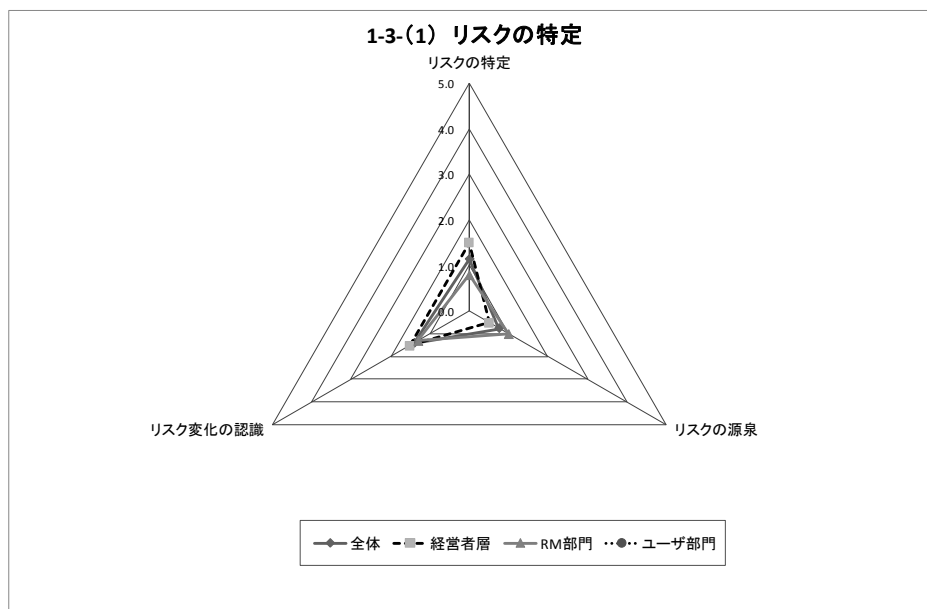
いずれにしても、「資源（リソース）の把握」、「資源の把握」や「影響業務の把握」について経営者層の評価が非常に低いのは、リスクマネジメントの実効性や現場の負担感に大きな影響を及ぼすため、早急に検討する必要があると思います。

【1-2-(5) リスクマネジメントシステムの実効性】



「1-2-(5) リスクマネジメントシステムの実効性」において、経営者層は「社員の理解」を除き、ユーザ部門に比べ、非常に低い評価となっています。たとえば、「システム構築」、「継続的実施の必要性」、「運用の継続性」では、ユーザ部門に全面的に委ねている様子が見られます。同様の傾向は RM 部門でも見られ、この点に関し、リスクマネジメントシステムの意義を組織として検討する必要があると思います。

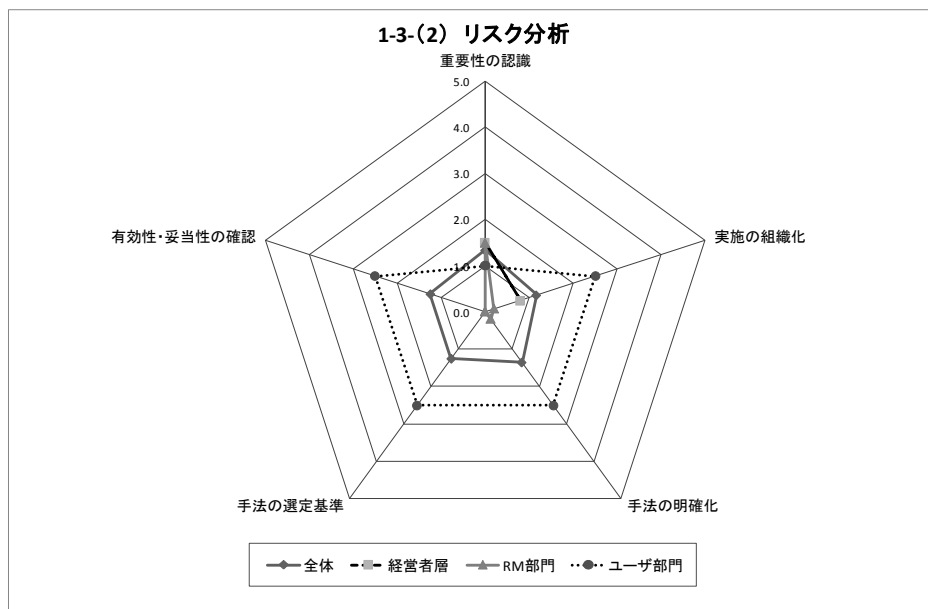
【1-3-(1) リスクの特定】



「1-3-(1) リスクの特定」はリスク対策のカギを握るステップです。この点、評価レベルは低いものの経営者層が「リスクの特定」と「リスク変化の認識」で評価レベルは 1.5 となっています。現在の経営環境に鑑みて、回答結果が示していることは一般的にリスクに関する理解レベル

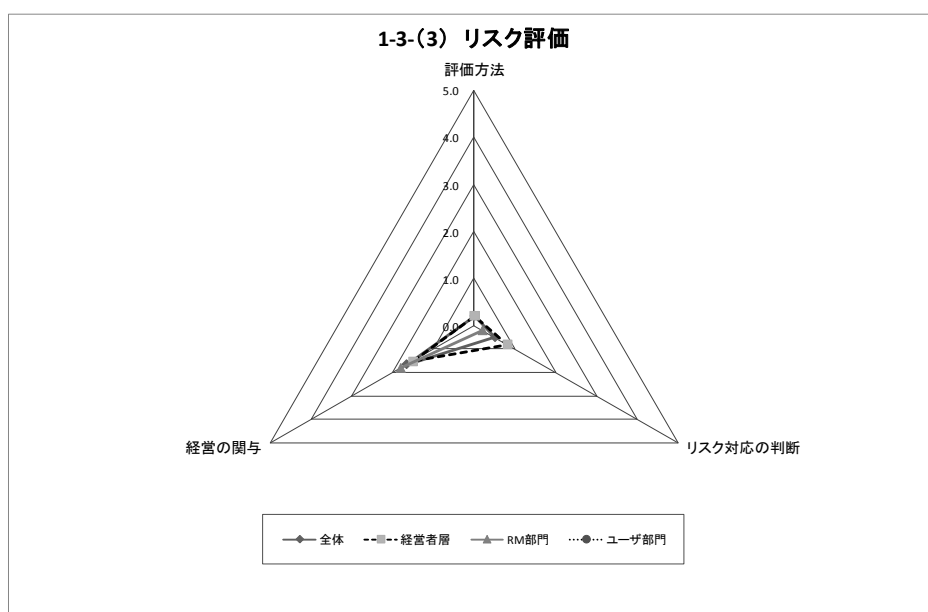
が十分でないことを示しています。組織としてこの点をどう考えるか、検討の必要があると思われます。

【1-3-(2) リスク分析】



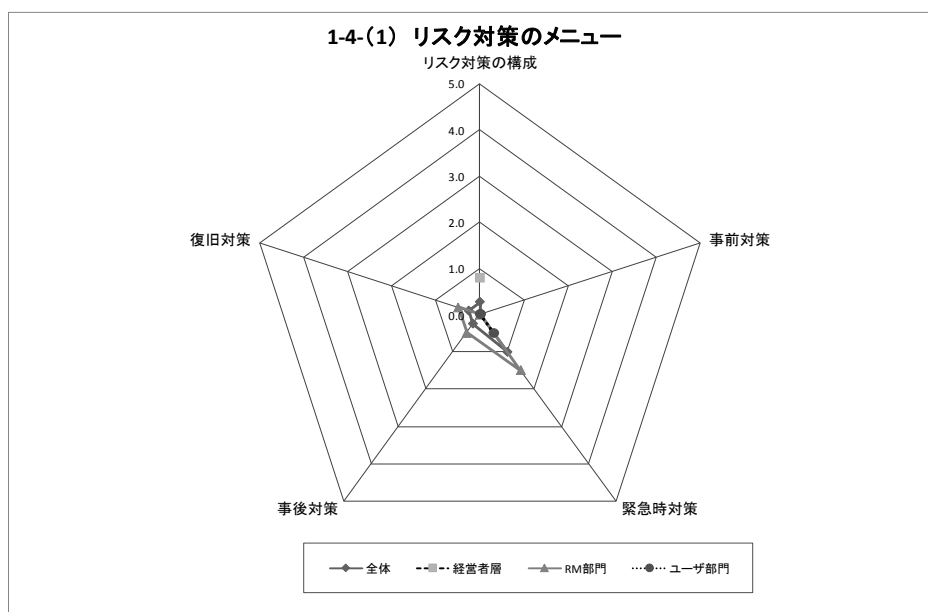
「1-3-(2) リスク分析」では、「重要性の認識」では経営者層・RM 部門の評価レベルは共に 1.5 ですが、問題は回答者間のバラツキが大きい点です。また、「実施の組織化」、「手法の明確化」、「手法の選定基準」、「有効性・妥当性の確認」では RM 部門はいずれもユーザ部門のそれよりきわめて低く、「重要性の認識」以外では 0、1、D/K という回答結果でした。特に、RM 部門の存在意義という点から、組織として再考の余地があると思われます。

【1-3-(3) リスク評価】



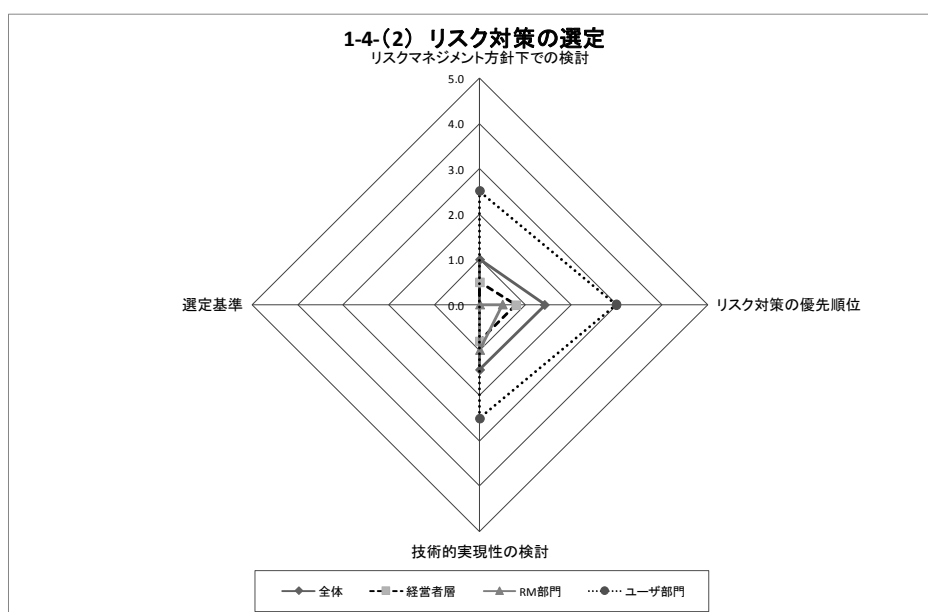
「1-3-(3) リスク評価」で重要な点は「経営の関与」です。この点について相対的に高い評価が認められますが、それでも部門対応レベルに達していない状況にあります。ただ、問題は回答者間に評価レベルについてかなりのバラツキが確認できることです。たとえば、「経営の関与」について経営者層で0から3、RM部門・ユーザ部門でD/Kから4となっています。さらに「評価方法」、「リスク対応の判断」の低さは組織として問題とすべきレベルにあると思われます。

【1-4-(1) リスク対策のメニュー】



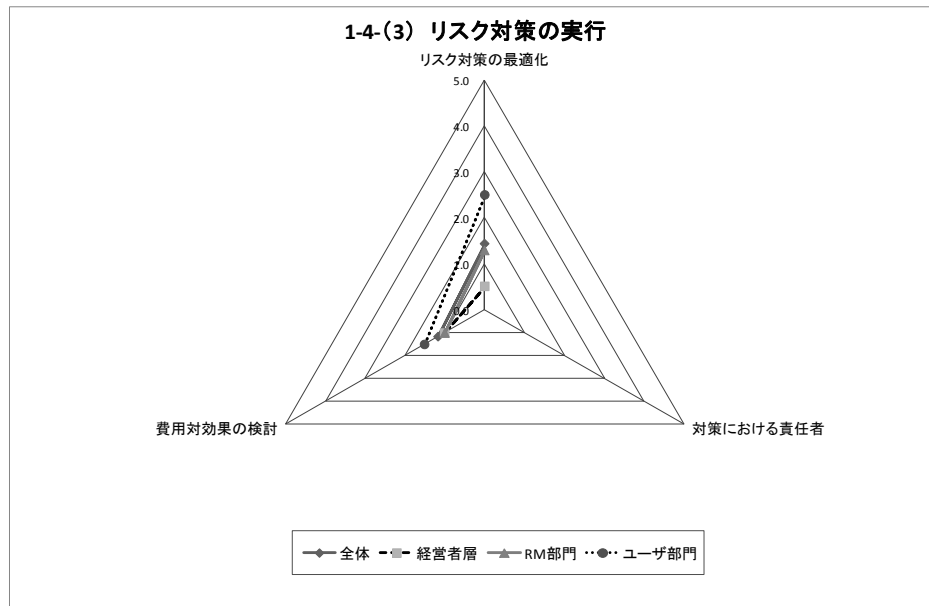
「1-4-(1) リスク対策のメニュー」では、全体的に評価が低く、また、関連質問間における回答結果にバラツキが大きく、組織として検討すべきであるといえます。

【1-4-(2) リスク対策の選定】



「1-4-(2) リスク対策の選定」では、ユーザ部門の回答結果に比べ、経営者層、RM 部門での評価レベルが低く、この原因が何に由来しているのか分析が必要といえます。しかしながら、ユーザ部門の回答にも極端なバラツキ（0 から 5）が見られ、回答者間のギャップ分析が不可欠といえます。

【1-4-(3) リスク対策の実行】

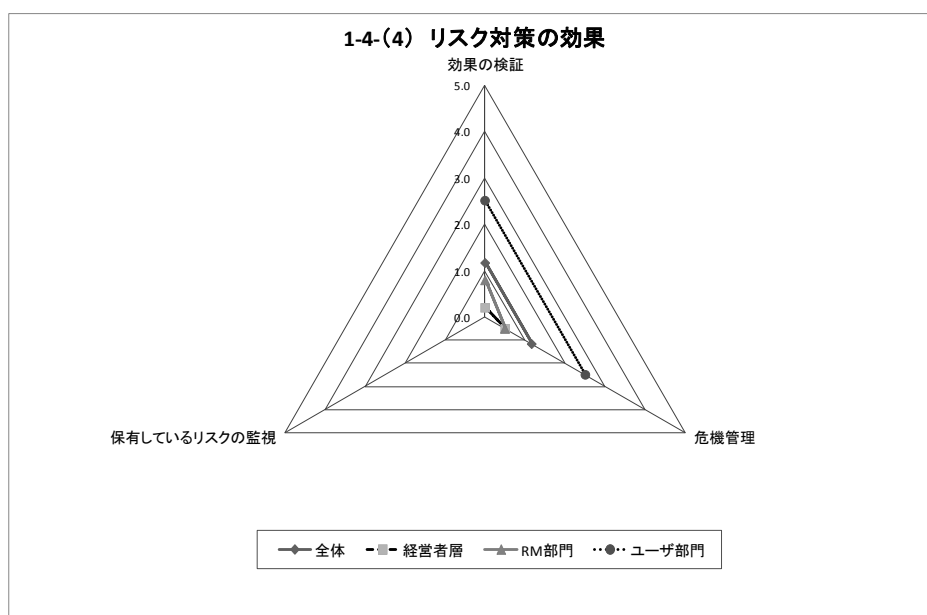


（「対策における責任者」は回答対象部門の指定がなかったため、全部門回答なし）

「1-4-(3) リスク対策の実行」では「リスク対策の最適化」、「費用対効果の検討」において、「1-4-(2) リスク対策の選定」と同様に、ユーザ部門の回答結果に比べ経営者層、RM 部門での評価レベルが低く、特に RM 部門において「リスク対策の最適化」について回答者間でのバラツキが大きいです。

この点、質問において「最適」とはいかなることを指しているのか、理解状況が回答結果に反映されたのではないかと思います。

【1-4-(4) リスク対策の効果】

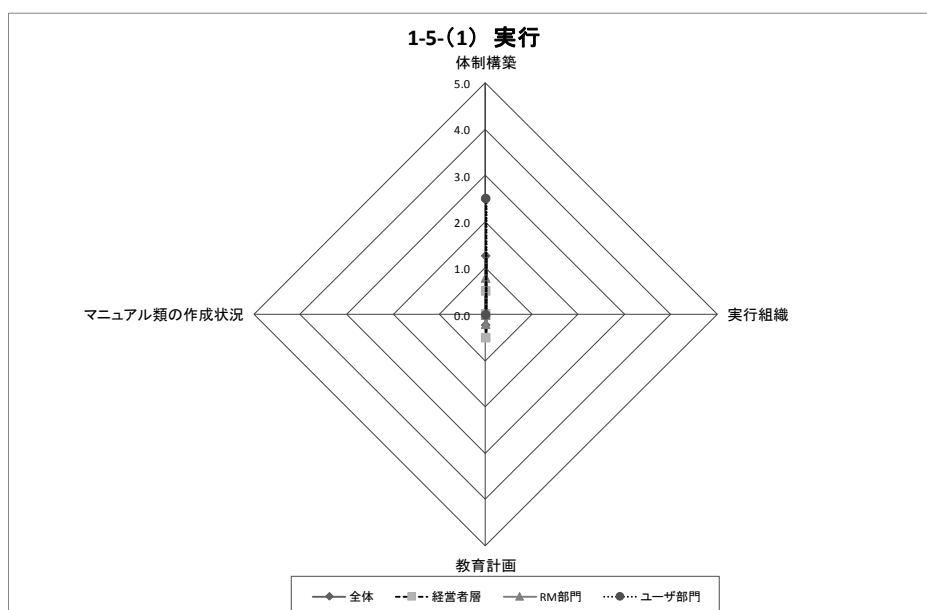


（「保有しているリスクの監視」は回答対象部門の指定がなかったため、全部門回答なし）

「1-4-(4) リスク対策の効果」では、「効果の検証」、「危機管理」において、「1-4-(2) リスク対策の選定」および「1-4-(3) リスク対策の実行」と同様に、ユーザ部門の回答結果に比べ、経営者層、RM 部門での評価レベルが低いのが気になります。特に RM 部門では、「効果の検証」について、各自の回答結果が D/K から 2 と評価のバラツキが比較的大きかったといえます。

また「危機管理」について、ユーザ部門に比較して RM 部門の 4 名中 3 名が D/K と回答した状況から見ると、質問項目における「保有しているリスクの監視」と危機管理の関連が掴み切れなかった、したがって質問項目の表現の理解状況が回答結果に反映されたきらいがあるかもしれません。しかし、組織における RM 部門として、どうなのかは検討の余地があります。

【1-5-(1) 実行】

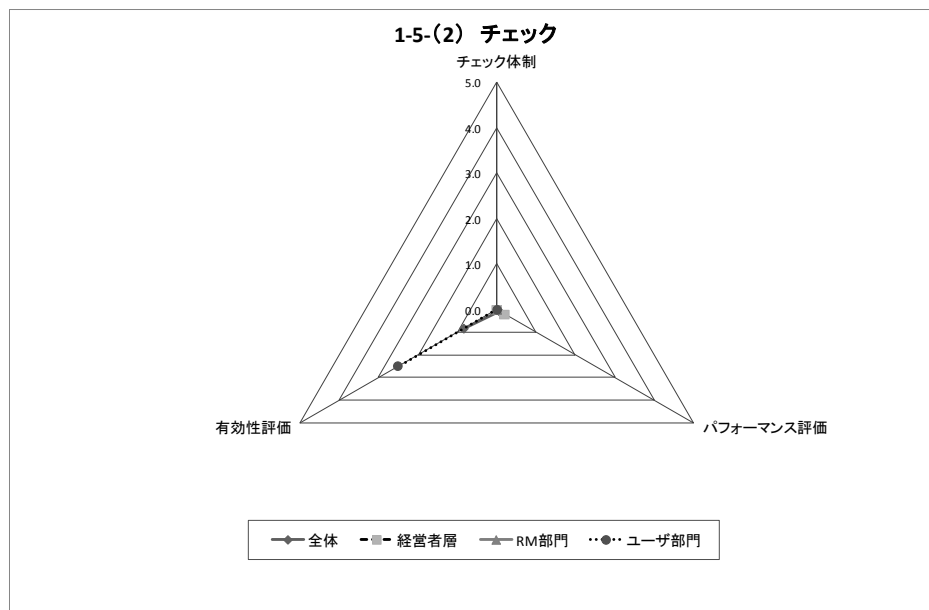


（「実行組織」は回答対象部門の指定がなかったため、全部門回答なし）

「1-5-(1) 実行」において、「体制構築」についてユーザ部門の評価が 2.5 となっていますが、回答結果は 0 と 5 であり、ギャップの存在は極端といえます。また、他部門でも回答結果にバラツキが見られます。

欠かせない項目といえる「教育計画」、「マニュアル類の作成状況」を含め、経営者層、RM 部門、ユーザ部門がそれぞれリスクマネジメントのあり方について検討することが望ましいといえます。

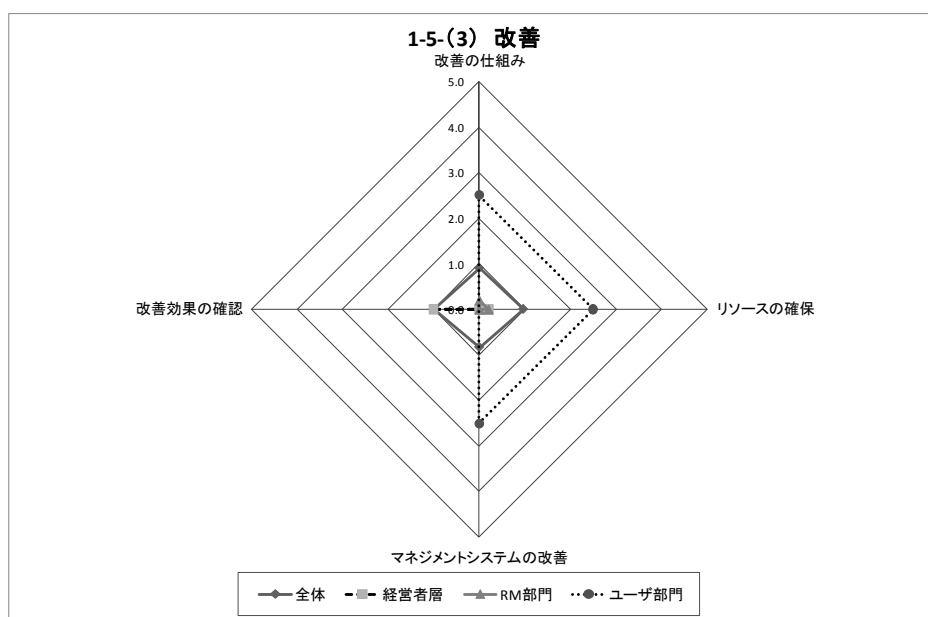
【1-5-(2) チェック】



（「チェック体制」は回答対象部門の指定がなかったため、全部門回答なし）

「1-5-(2) チェック」は、現状を振り返り、是正・改善に結びつける重要な意味を有しています。ここでは「パフォーマンス評価」と「有効性評価」が回答対象となっていました。特に「パフォーマンス評価」についてはほとんど見るべき回答がありませんでした。「有効性評価」については、ユーザ部門の評価レベル 2.5 が確認できますが、「1-5-(1) 実行」での評価と同様に回答結果は 0 と 5 であり、バラツキが大きすぎます。上記同様、経営者層、RM 部門、ユーザ部門それぞれ、リスクマネジメントのあり方について検討の機会を持っていただきたいと思います。

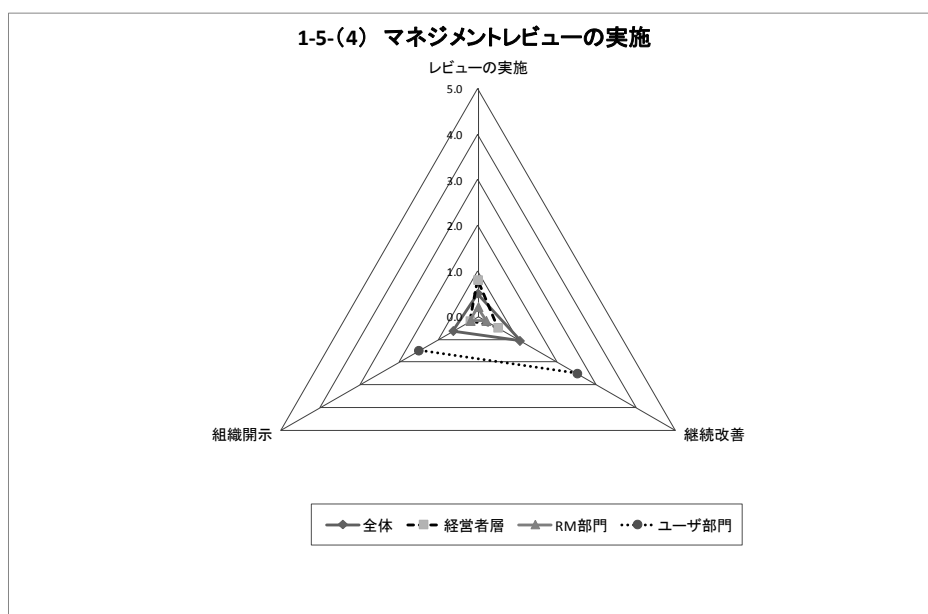
【1-5-(3) 改善】



「1-5-(3) 改善」における「改善の仕組み」は、経営環境の激しい中での重要な課題となります。その評価レベルは経営者層の第4階層は0、RM部門では0.2という結果でした。ユーザ部門では2.5でしたが、回答者間では0と5とバラツキが著しいです。また、「リソースの確保」、「マネジメントシステムの改善」についても同様といえます。

なお、経営者層のみに回答を求めた「改善効果の確認」で第4階層の評価レベルは2.5でしたが、回答者間のバラツキは0と5であり、ギャップの原因についての検討が必要だと思われます。

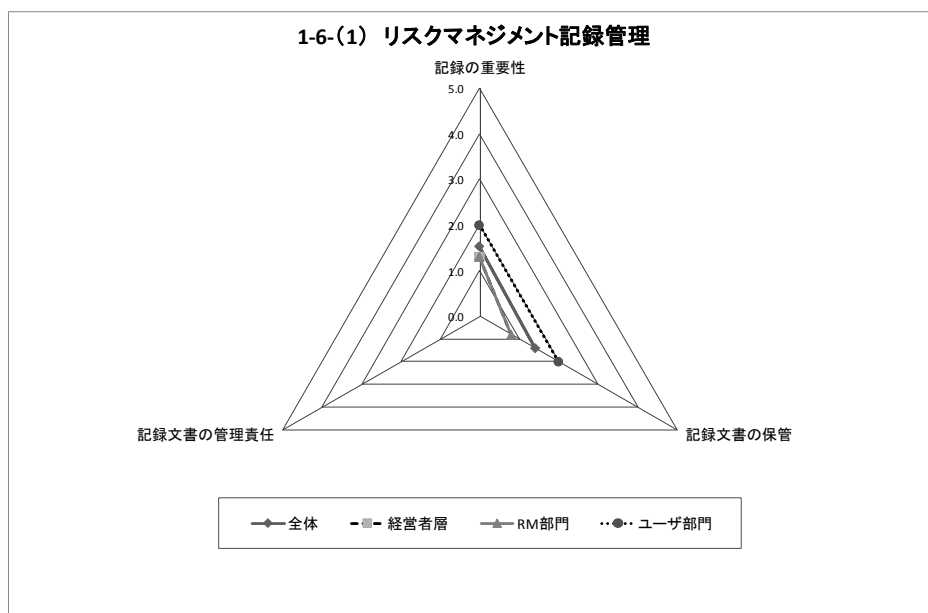
【1-5-(4) マネジメントレビューの実施】



「1-5-(4) マネジメントレビューの実施」における「レビューの実施」、「継続改善」、「組織開示」について第4階層の評価レベルは経営者層、RM部門で低く、かつバラツキが特に経営者層では大きく、ギャップ分析の必要性が感じられます。

ユーザ部門では、評価レベル2という結果でした。ユーザ部門には「継続改善」、「組織開示」の質問が回答対象となっており、それぞれの評価レベルは2.5、1.5でしたが、バラツキが著しく、ギャップ分析による認識の共有が必要といえます。

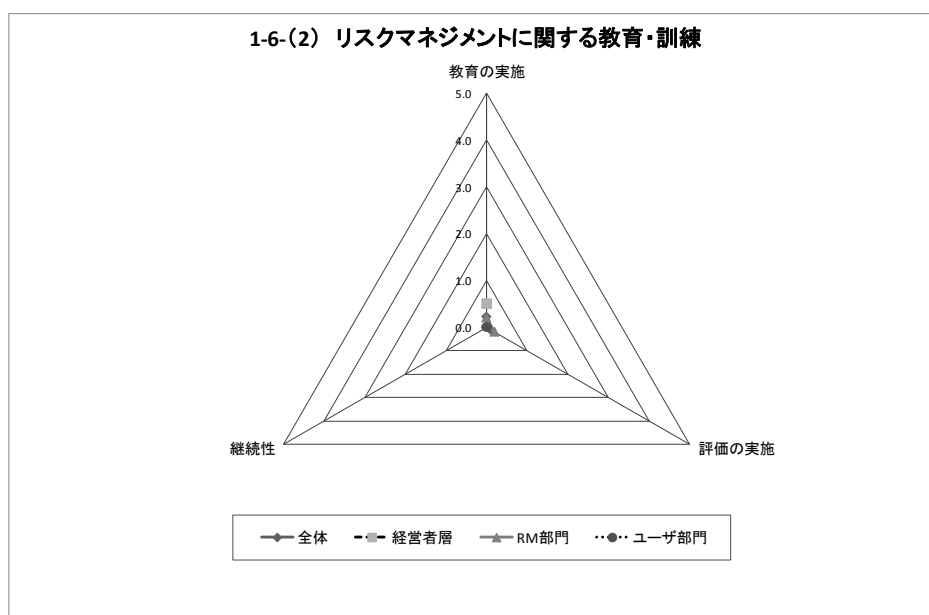
【1-6-(1) リスクマネジメント記録管理】



（「記録文書の管理責任」は回答対象部門の指定がなかったため、全部門回答なし）

「1-6-(1) リスクマネジメント記録管理」については、「記録の重要性」、「記録文書の保管」について経営者層は前者のみが回答対象となっていました。第4階層の評価レベルは経営者層、RM部門で1.3と低く、かつバラツキが大きく、また、ユーザ部門では両方の回答結果が評価レベル2（部門対応レベル）であり、部門間および回答者間におけるギャップについて検討が必要だと思われます。

【1-6-(2) リスクマネジメントに関する教育・訓練】

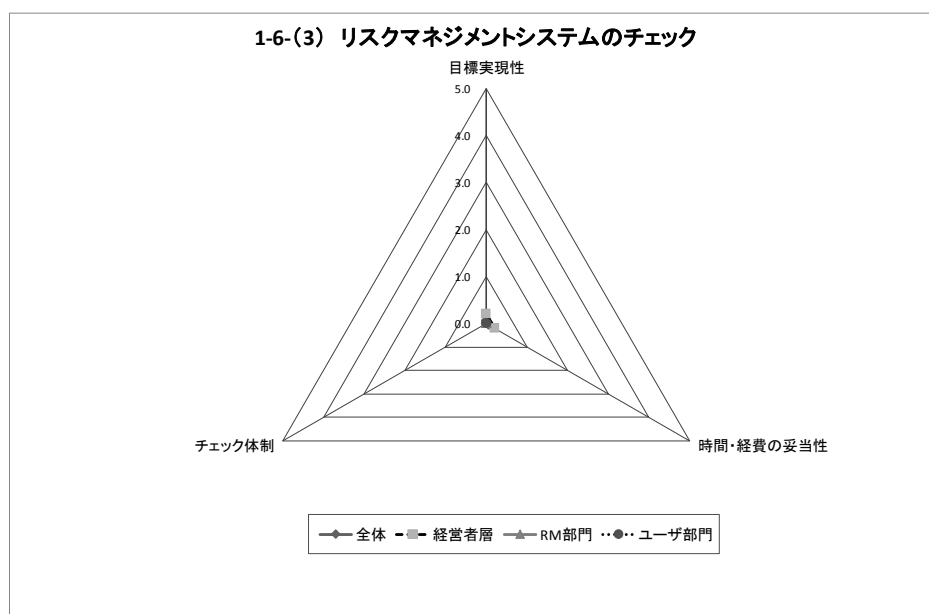


（「継続性」は回答対象部門の指定がなかったため、全部門回答なし）

「1-6-(2) リスクマネジメントに関する教育・訓練」について、経営者層は「教育の実施」のみが回答対象となっていますが、第4階層の評価レベルは0.5、RM部門は0.2とさらに低く、ユーザ部門では、当該質問と「評価の実施」に対して未対応の回答でした。

この点に関して、特に経営者層、さらにRM部門においては組織としてリスクマネジメントの意義をどう考えているか、検討の余地があるでしょう。

【1-6-(3) リスクマネジメントシステムのチェック】

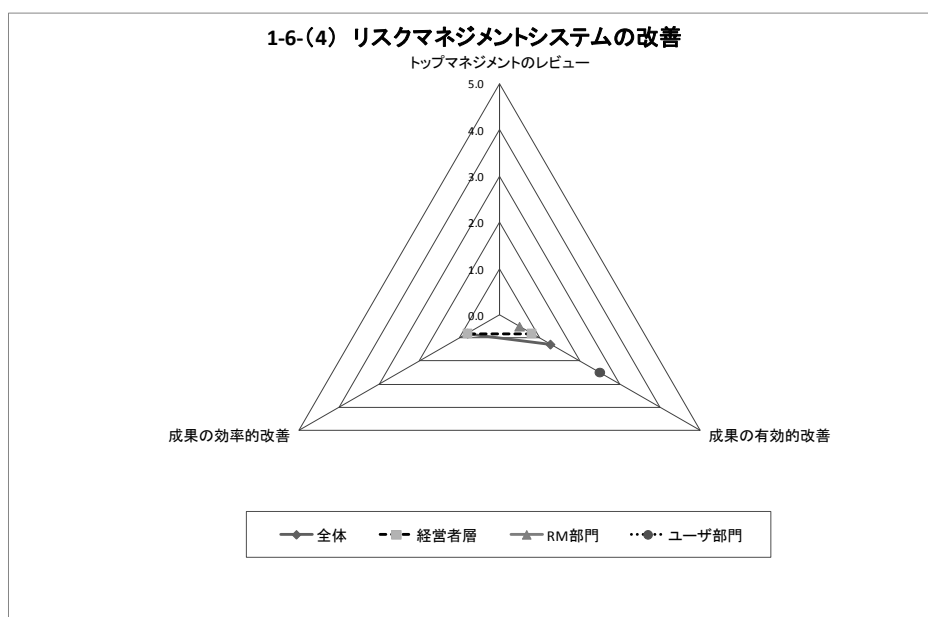


（「チェック体制」は回答対象部門の指定がなかったため、全部門回答なし）

「1-6-(3) リスクマネジメントシステムのチェック」に関する「目標実現性」、「時間・経費の妥当性」については、経営者層の第4階層の評価レベルは0.2、RM部門・ユーザ部門では未対応0の回答結果でした。

リスクマネジメントシステムのチェックに関しては、特に経営者層、RM部門においては組織としてリスクマネジメントの意義をどう考えるか、上記同様に検討の余地があるといえます。

【1-6-(4) リスクマネジメントシステムの改善】

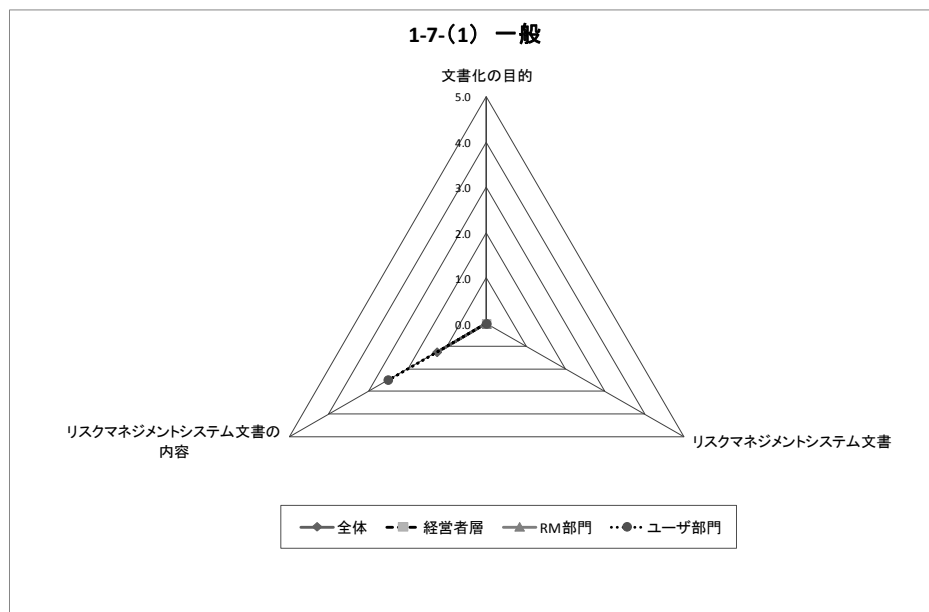


(「トップマネジメントのレビュー」は回答対象部門の指定がなかったため、全部門回答なし)

「1-6-(4) リスクマネジメントシステムの改善」に関する「成果の有効的改善」、「成果の効率的改善」については、経営者層は第4階層の評価レベルは0.8と低く、「成果の有効的改善」の質問項目にのみ回答しているRM部門は0.5、これに対しユーザ部門は2.5となっています。しかし、回答者間のバラツキは大きく、検討の余地があります。

特に経営者層、RM部門においては組織としてリスクマネジメントの意義をどう考えるか、これまでの指摘同様に検討の余地があるといえます。

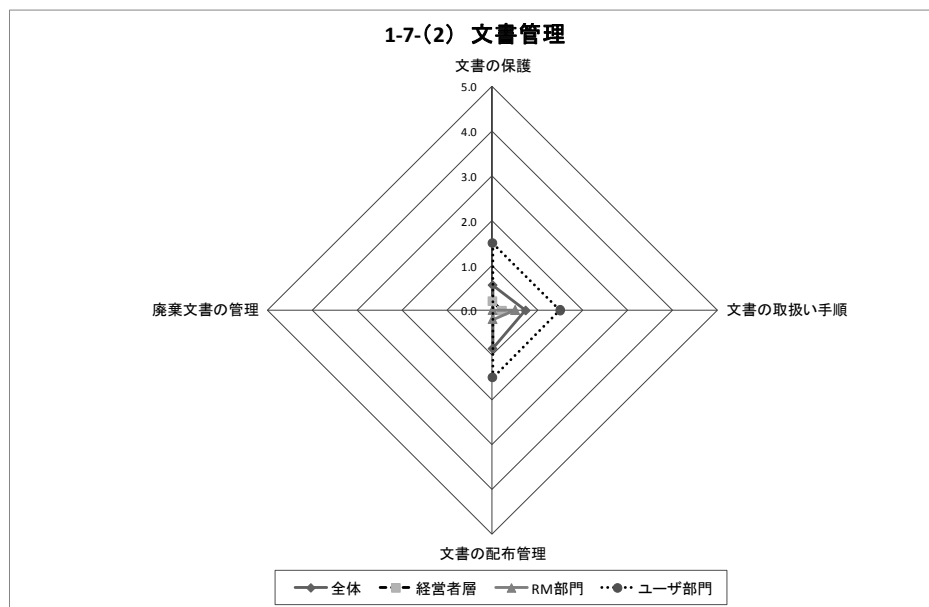
【1-7-(1) 一般】



「1-7-(1) 一般」においては、全部門共に「文書化の目的」、「リスクマネジメントシステム文書」、「リスクマネジメントシステム文書の内容」について 0 または D/K と回答しており、最後の「リスクマネジメントシステム文書の内容」に対してユーザ部門のみ評価レベル 2.5 と回答しています。しかも、回答者間のバラツキは 0 から 5 と大きく、検討の余地があります。

これまでと同様、組織としてリスクマネジメントの意義について検討の余地があるといえます。

【1-7-(2) 文書管理】

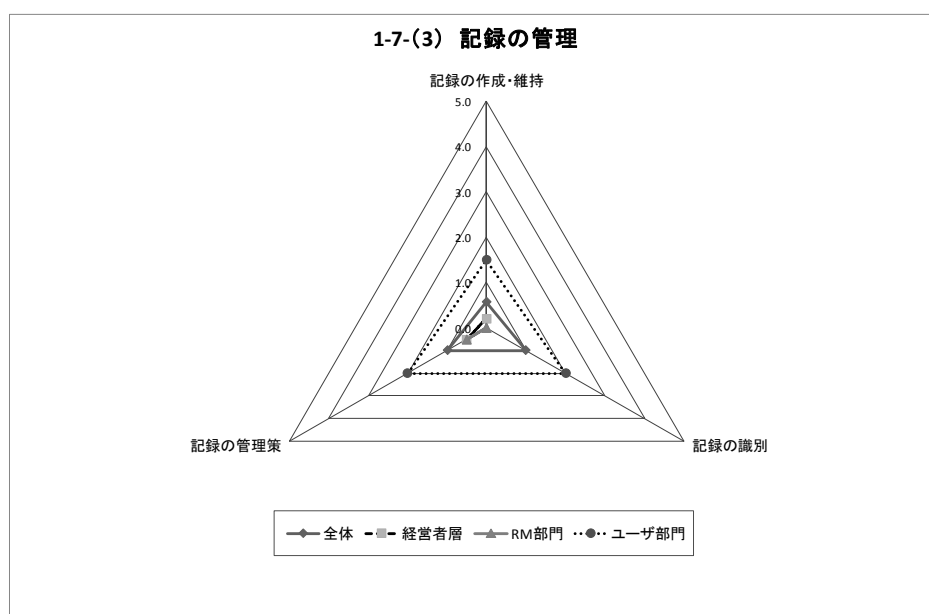


(「廃棄文書の管理」は回答対象部門の指定がなかったため、全部門回答なし；「文書の配布管理」は経営者層のみ回答対象外)

「1-7-(2) 文書管理」における「文書の保護」では経営者層（第4階層の評価レベル0.2）、RM部門は応えていない（0かD/K）という結果でした。ユーザ部門のみ1.5の評価でした。「文書の取扱い手順」「文書の配布管理」に関しても同様の傾向が見られます。

特に、リスクマネジメントシステムとの関係から文書管理について全体的に検討の余地があるといえます。

【1-7-(3) 記録の管理】



（「記録の識別」は経営者層のみ回答対象外）

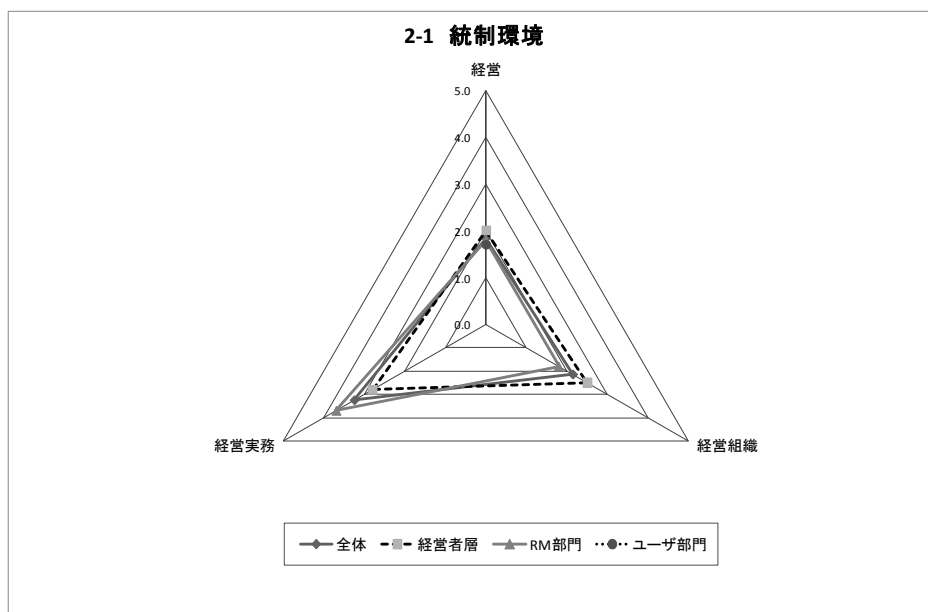
「1-7-(3) 記録の管理」における「記録の作成・維持」、「記録の管理策」では経営者層でも低い回答でしたが、「記録の作成・維持」、「記録の識別」、「記録の管理策」についてのRM部門の回答は第4階層の評価レベルでそれぞれ0、0、0.5、ユーザ部門ではそれぞれ1.5、2、2でした。したがって、部門間のギャップは大きいといえます。この点は、ユーザ部門に任せっきりといった印象があります。

特に記録の管理はPDCAを実質的に回すために重要なので、リスクマネジメントシステムとの関係から検討の余地があるといえます。

4.1.2.3 第2章「内部統制リスクと経営者の対応」(Ver.5)の詳細分析

1. 第2階層の分析

【2-1 統制環境】

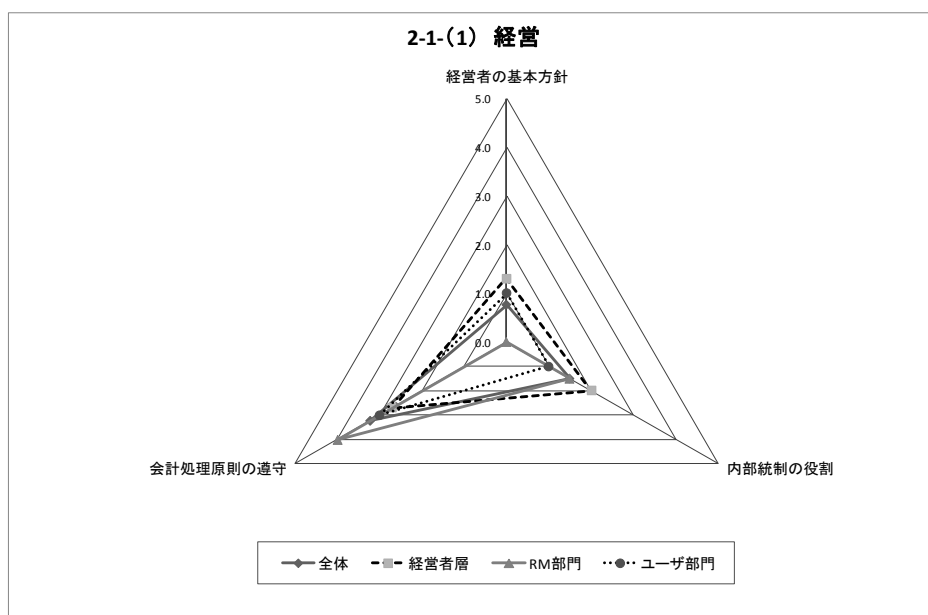


「2-1 統制環境」は経営者の基本方針や取締役会の基本的機関、役割分担、人材配置などを評価します。経営環境については、標準的な評価が行われ、しかも経営者層、RM 部門、ユーザ部門の評価がほぼ同じであり、総合点では階層間の認識のギャップは感じられません。

(2-2～2-6 は第3階層が1つずつしかないため、レーダーチャート掲載なし)

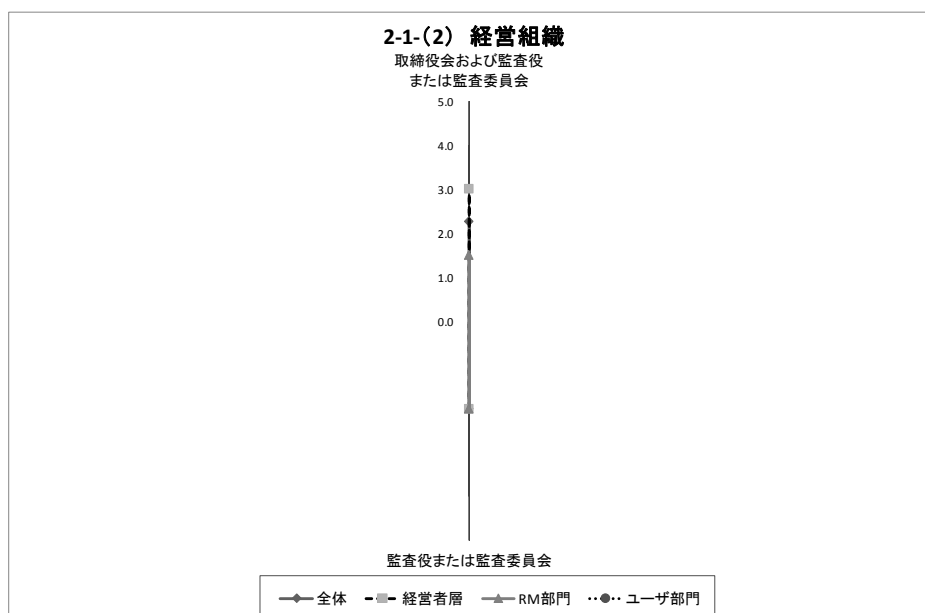
2. 第3階層の分析

【2-1(1) 経営】



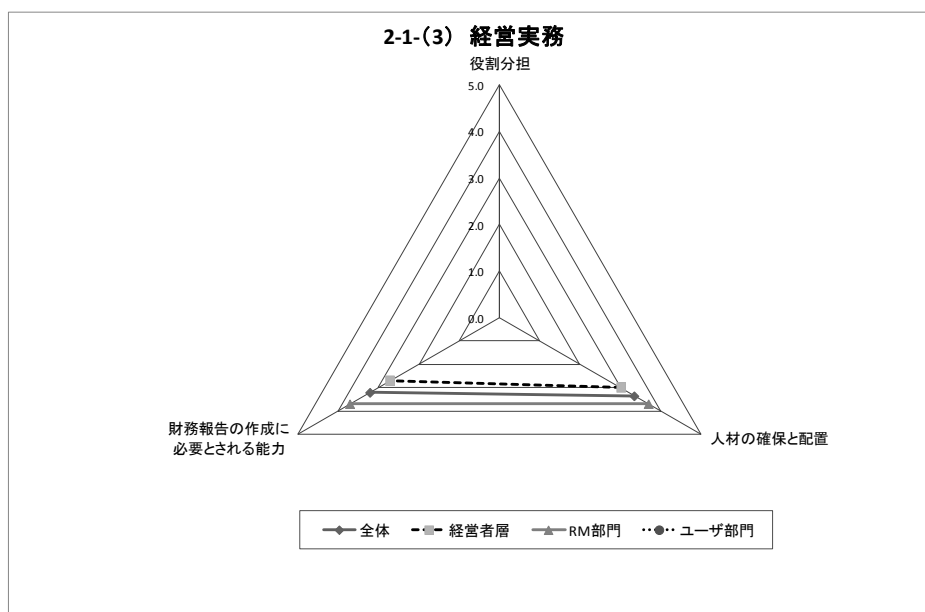
「経営者の基本方針」についての評価では経営者層が高い自己評価を行っていますが、RM 部門、ユーザ部門は「経営者の基本方針」および「内部統制の役割」について比較的 low に評価しています。「会計処理原則の遵守」については各階層とも揃って高めの評価を行っています。このことから、基本方針について、経営者層は今以上に周知するとよいでしょう。

【2-1-(2) 経営組織】



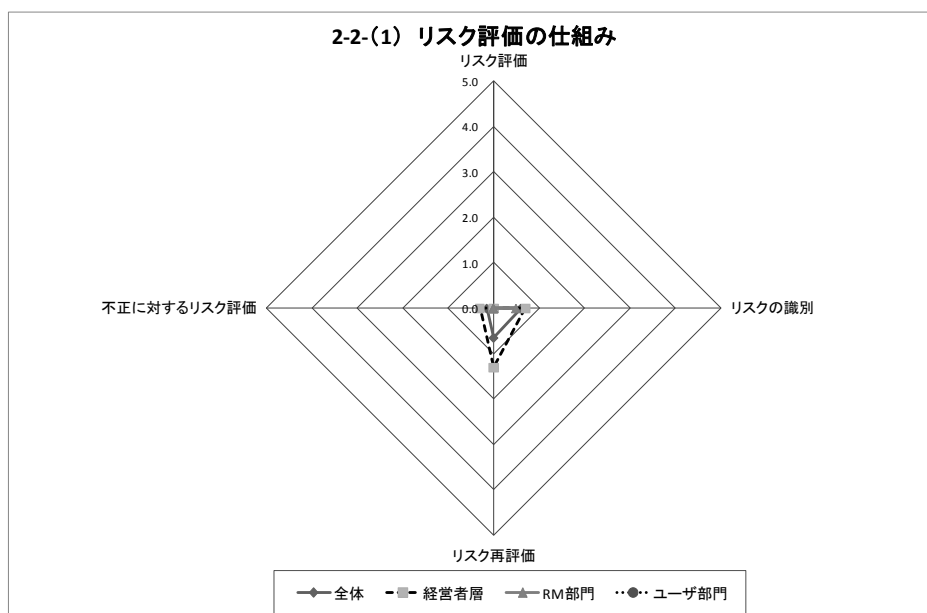
「2-1-(2) 経営組織」については取締役や監査役会の責任の理解などについては各階層による評価の差は少ないといえます。

【2-1-(3) 経営実務】



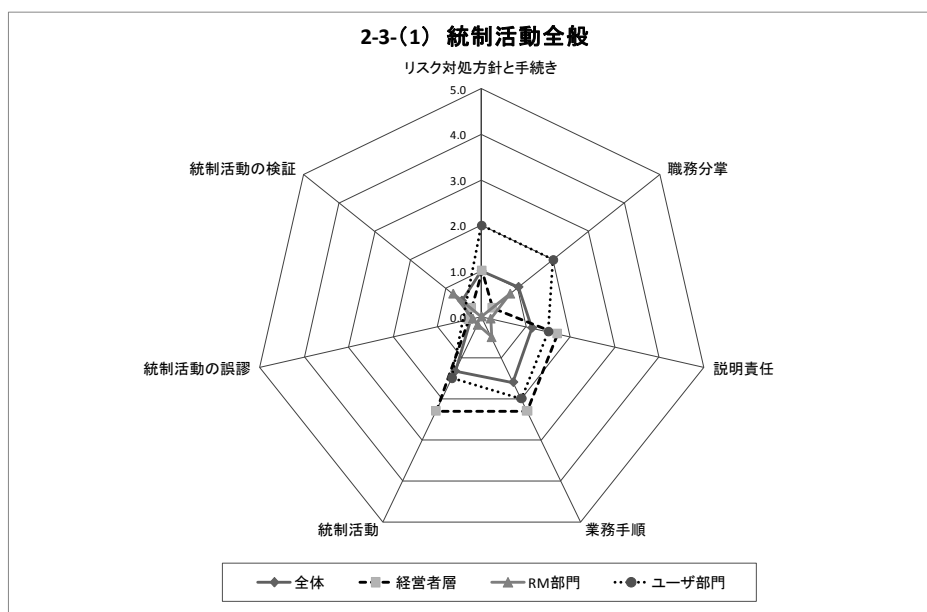
「2-1-(3) 経営実務」において、「人材の確保と配置」および「財務報告の作成に必要とされる能力」の適切性についてはほぼ中程の評価となっており、階層間の差があまりない評価となっています。

【2-2-(1) リスク評価の仕組み】



「2-2-(1) リスク評価の仕組み」については「リスク評価」、「リスクの識別」、「リスクの再評価」、「不正に対するリスク評価」について、いずれも低い評価となっており、組織としてリスク評価能力の改善が必要と判断されます。

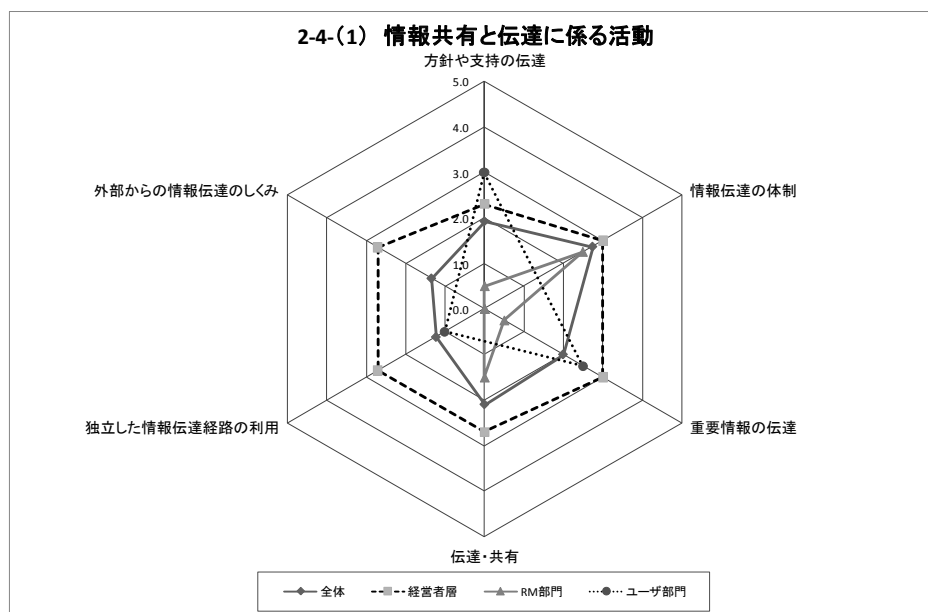
【2-3-(1) 統制活動全般】



「2-3-(1) 統制活動全般」については経営者層、RM 部門、ユーザ部門の評価が大きく分かれています。経営者の「職務分掌」の評価が低いのに対し、ユーザ部門では担当者の相互牽制がされていると認識しています。一方、「説明責任」、「統制活動」そのものの評価については経営者の評価が高いのに対し、RM 部門、ユーザ部門の評価は低く、経営者層が思っているよりも現場では批判的に感じています。なお、「検証」についてはすべての部門で対応が全くされていないとの評価がされており、改善が必要です。

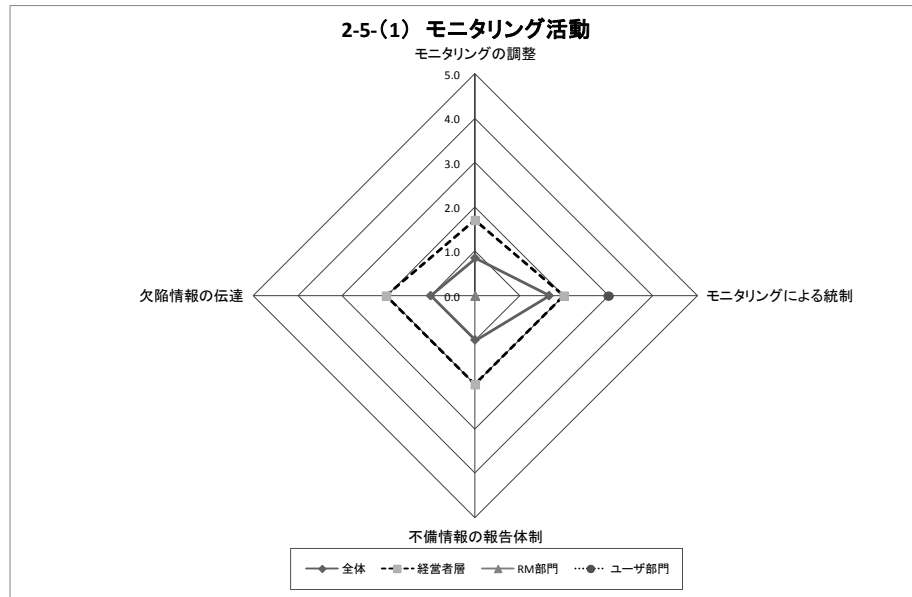
また、RM 部門は評価基準軸が高いせいか、自己評価を低く見えています。リスクマネジメントの必要性を認識したことが自己点検を厳しくしていると見られます。

【2-4-(1) 情報共有と伝達に係る活動】



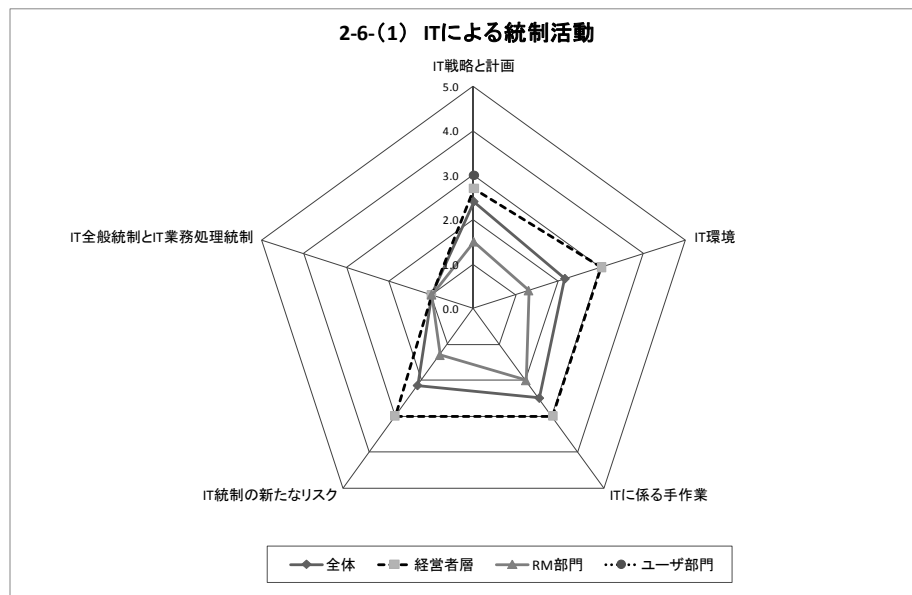
「2-4-(1) 情報共有と伝達に係る活動」については、経営者層がすべての項目において高い評価を行っていますが、ユーザ部門および RM 部門の自己評価は低く、明確なギャップが現れています。経営者が思っているほど方針や指示がされていないということを認識し、従来以上にコミュニケーションを密にすることが望まれます。

【2-5-(1) モニタリング活動】



「2-5-(1) モニタリング活動」については、経営者層がすべての項目において高い自己評価を行っていますが、RM 部門からは全く評価されていません。ユーザ部門では内部統制に関する内外の情報提供については経営者層よりも高い評価がされていますが、「モニタリングの調整」、「不備情報の報告体制」や「欠陥情報の伝達」など、取締役会など会社機関への報告については経営者層よりも低い評価となっています。社内で悪い情報が必ずしもすべて経営者層に報告されていない可能性もありますので、経営者層は伝達情報が上層部へ適切に報告されるような仕組みについて検討されることが望まれます。

【2-6-(1) IT による統制活動】



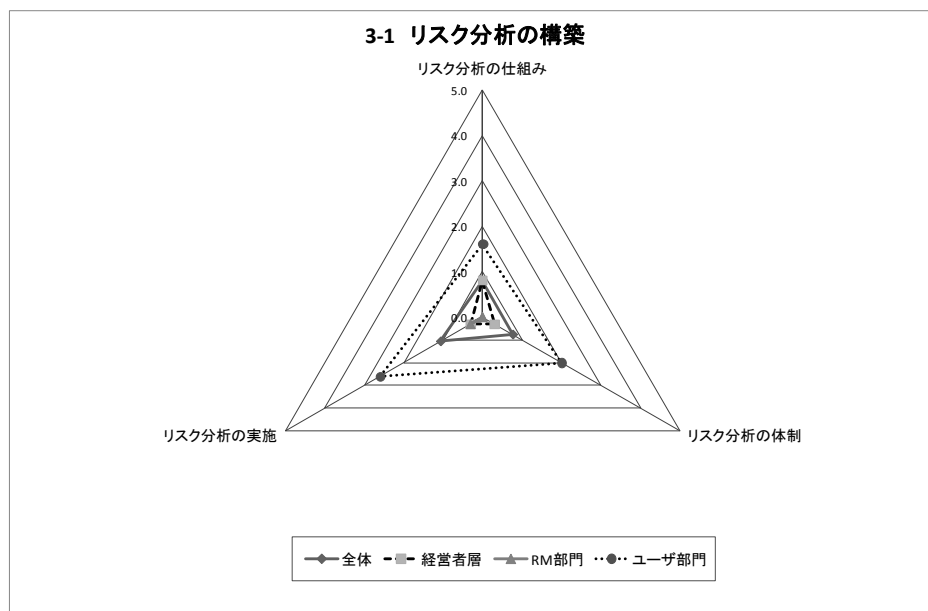
「2-6-(1) IT による統制活動」についても経営者層が高く評価し、ユーザ部門、RM 部門が比

較的低く評価しています。中でも「IT 全般統制と IT 業務処理統制」についてはすべての回答部門で評価が低くなっています。

4.1.2.4 第3章「内部統制リスクのリスク分析」(Ver.5)の詳細分析

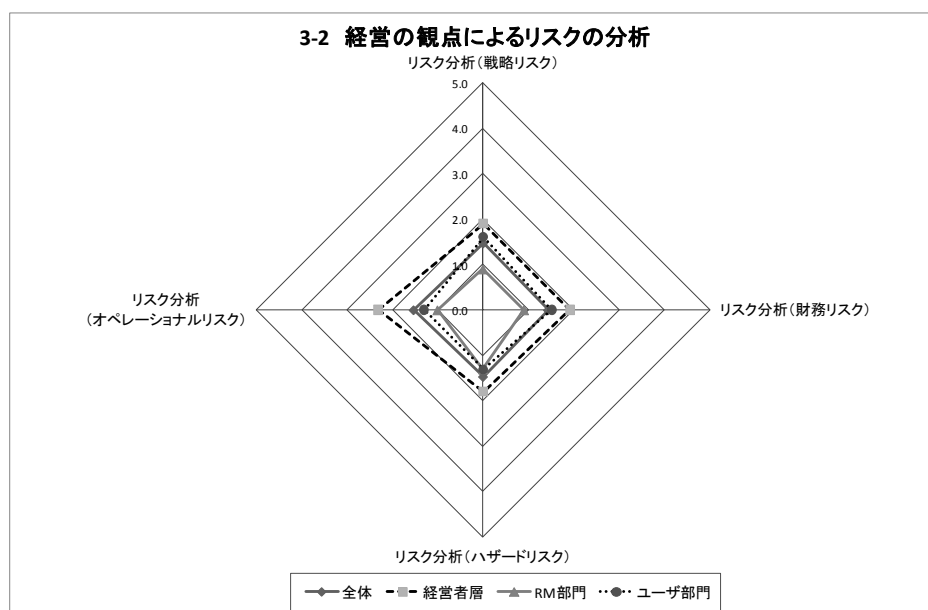
1. 第2階層の分析

【3-1 リスク分析の構築】



内部統制のリスク分析については、全体的に第2章とは反対に経営者層の評価が低く、ユーザ部門の評価が高くなっています。RM部門の評価が低いのはリスクマネジメントの認識が高まるにつれて評価が厳しくなっていることが考えられます。「リスク分析の仕組み」、「リスク分析の体制」に比べ、「リスク分析の実施」という実務部分の評価が高くなっています。

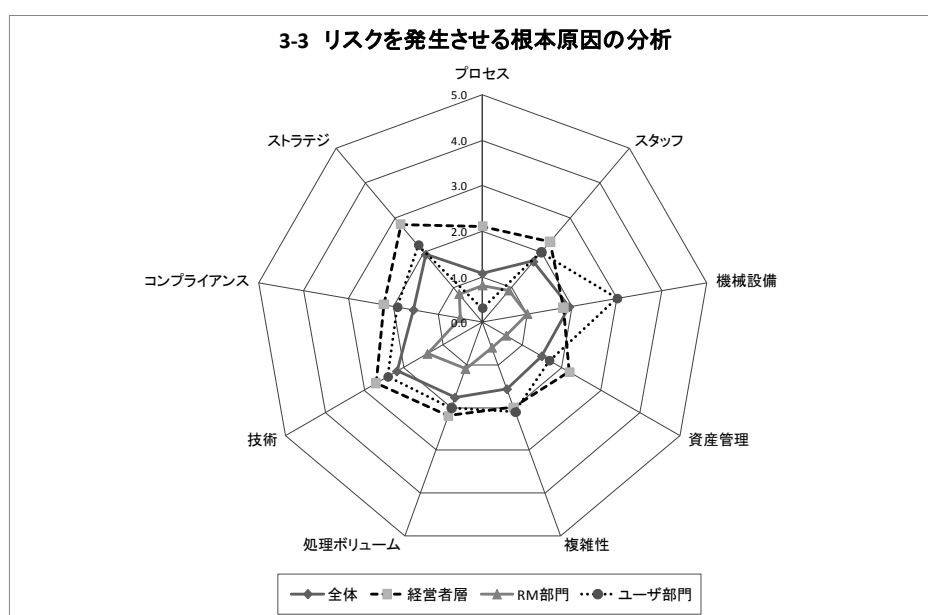
【3-2 経営の観点によるリスクの分析】



「3-2 経営の観点によるリスク分析」において「戦略リスク」、「財務リスク」、「ハザードリスク」、「オペレーショナルリスク」の四つの区分では経営者層が最も高く評価しており、次いでユーザ部門、RM 部門の評価レベルとなっています。経営者層では四つのリスクの中では特に「オペレーショナルリスク」を高く評価しています。ユーザ部門はほぼ同程度であり、RM 部門では「ハザードリスク」が高く評価されています。

これらは経営者層がオペレーショナルリスク、RM 部門がハザードリスクを重点的に認識していることの現れと考えられます。

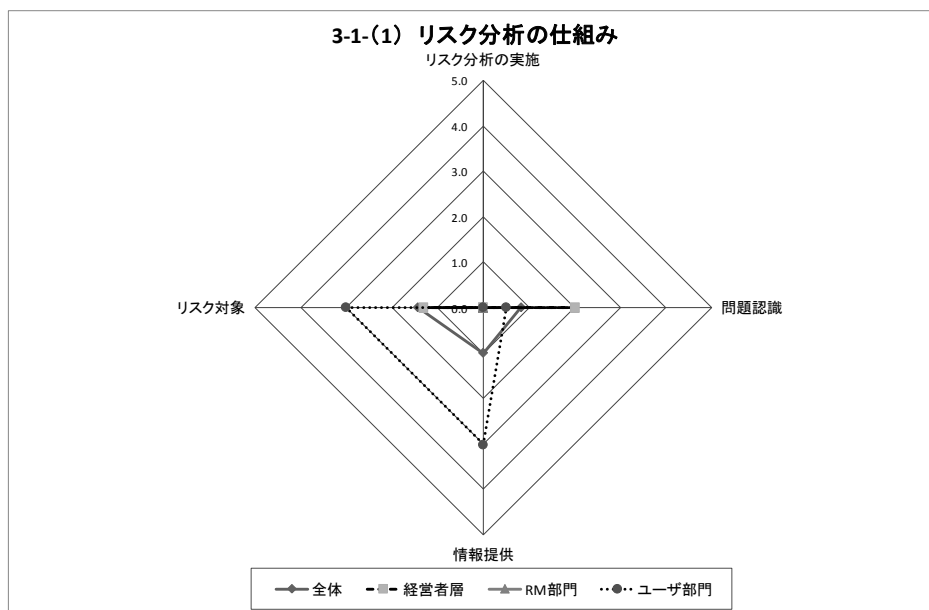
【3-3 リスクを発生させる根本原因の分析】



「3-3 リスクを発生させる根本原因の分析」においては経営者層＞ユーザ部門＞RM 部門の評価順位は他の評価と同様です。経営者層はほぼすべてのリスク要因につき同程度の評価を行っていますが、ユーザ部門ではプロセスの認識が低いです。RM 部門でも「プロセス」および「試算管理」ができていないと評価しています。ミスの記録が行われず、あるいは過去の不正の分析などの評価について認識度合いが少なかった可能性があります。

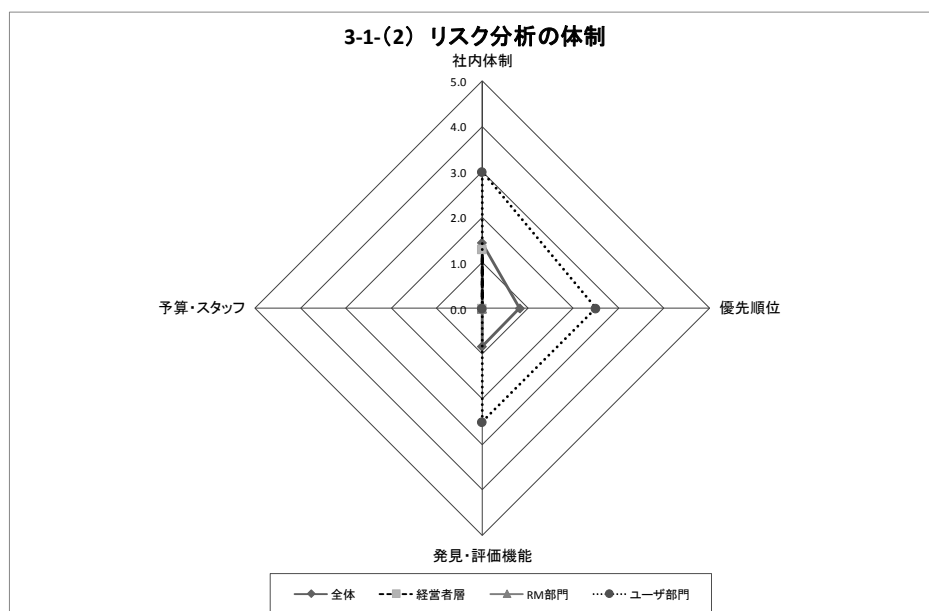
(2) 第3階層の分析

【3-1-(1) リスク分析の仕組み】



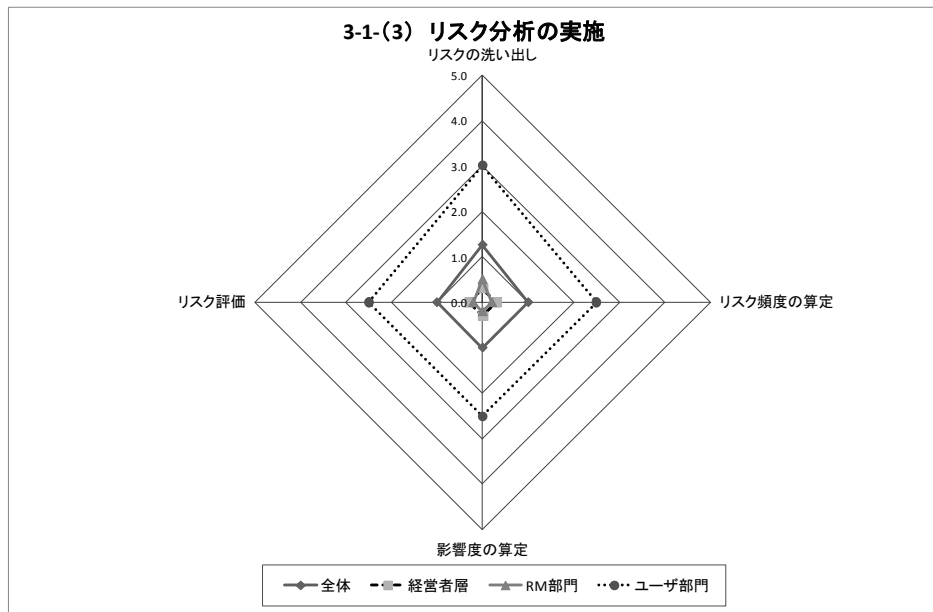
「3-1-(1) リスク分析の仕組み」について「リスク分析」実施」が評価レベル0という厳しい評価となっています。ユーザ部門ではリスク情報の提供や守るべき対象を損なうリスクについて比較的高い評価がされています。

【3-1-(2) リスク分析の体制】



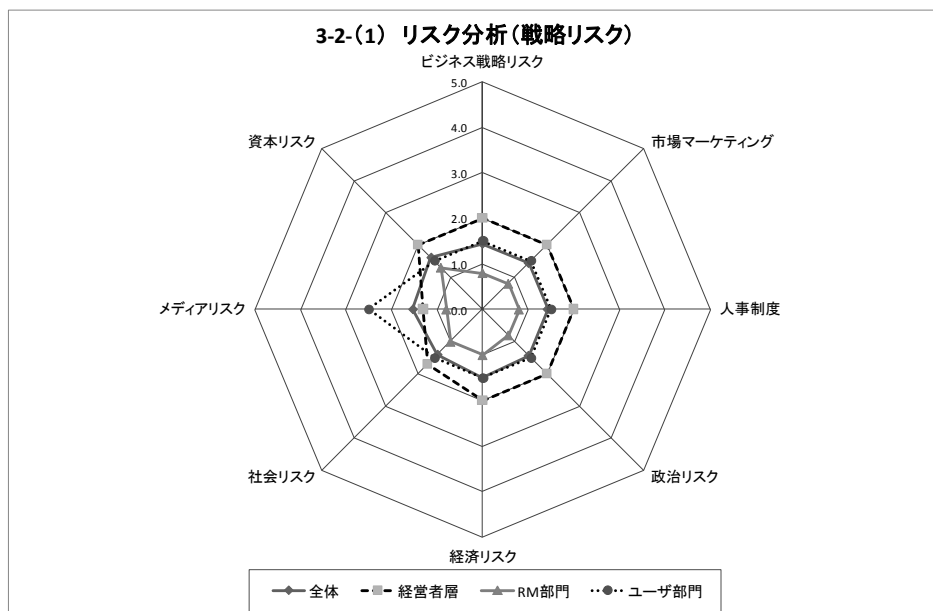
「3-1-(2) リスク分析の体制」については経営者層が低い評価を行っており、RM部門も0評価です。中でも「予算・スタッフ」についてはすべての階層で評価が0となっており、経営資源が投入されてこなかったことがわかります。

【3-1-(3) リスク分析の実施】



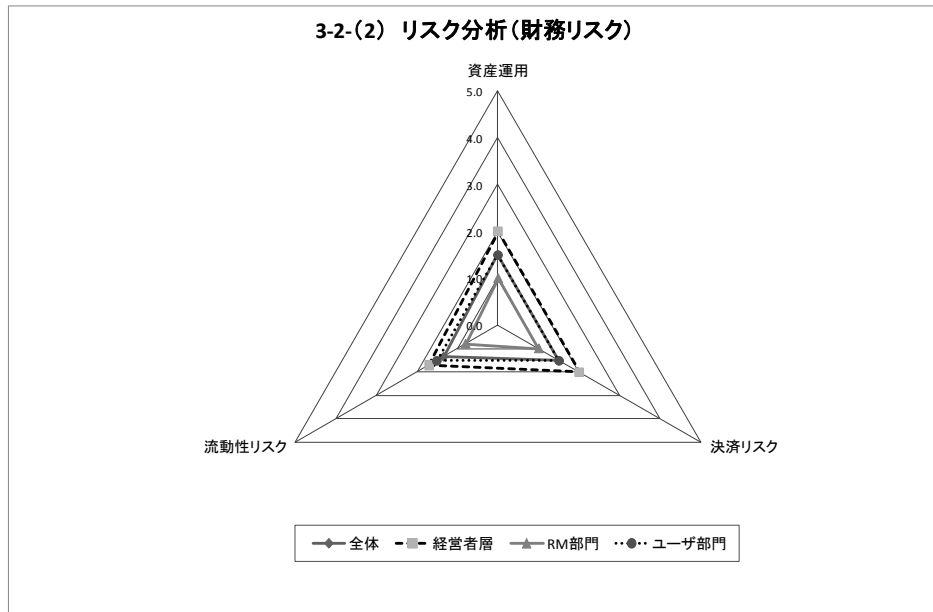
「3-1-(3) リスク分析の実施」についてはユーザ部門が高い評価を行っていますが、経営者層、RM 部門は評価が低いです。「リスクの洗い出し」、「リスク頻度の算定」、「影響度の算定」、「リスク評価」がほぼ同じ評価となっており、これらは一連の作業で同様に実施されていると考えられます。

【3-2-(1) リスク分析（戦略リスク）】



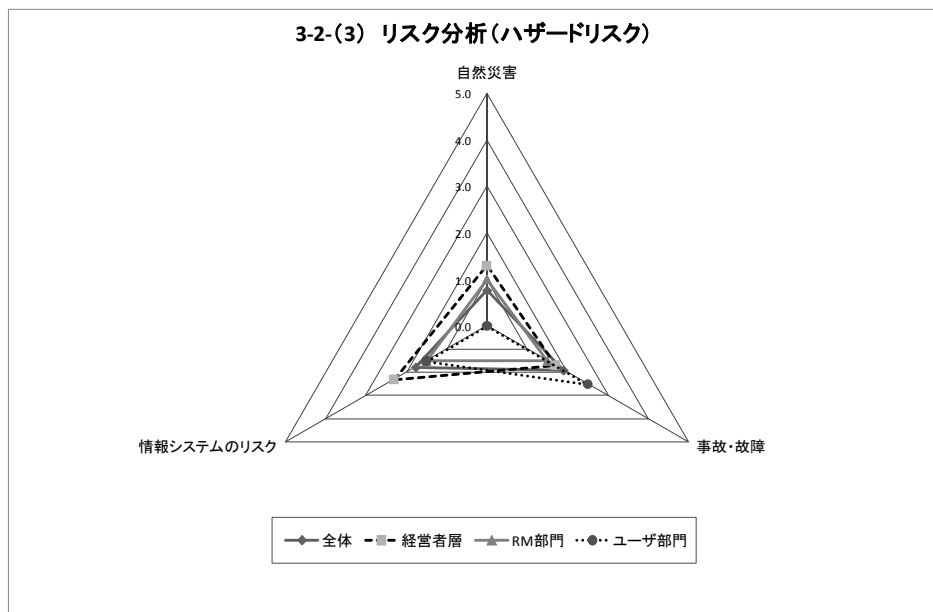
「3-2-(1) リスク分析（戦略リスク）」のうち、「メディアリスク（マスコミ、インターネットなど）」に対してユーザ部門では検討していると評価しているのに対して経営者層は相対的に低めの評価となっています。しかしながら、記者会見では経営者層が矢面となる可能性が強く、その重要性に関するユーザ層の認識が現れていると思われます。

【3-2-(2) リスク分析（財務リスク）】



「3-2-(1) リスク分析（財務リスク）」については、ほぼ全部門とも同程度の評価となっています。

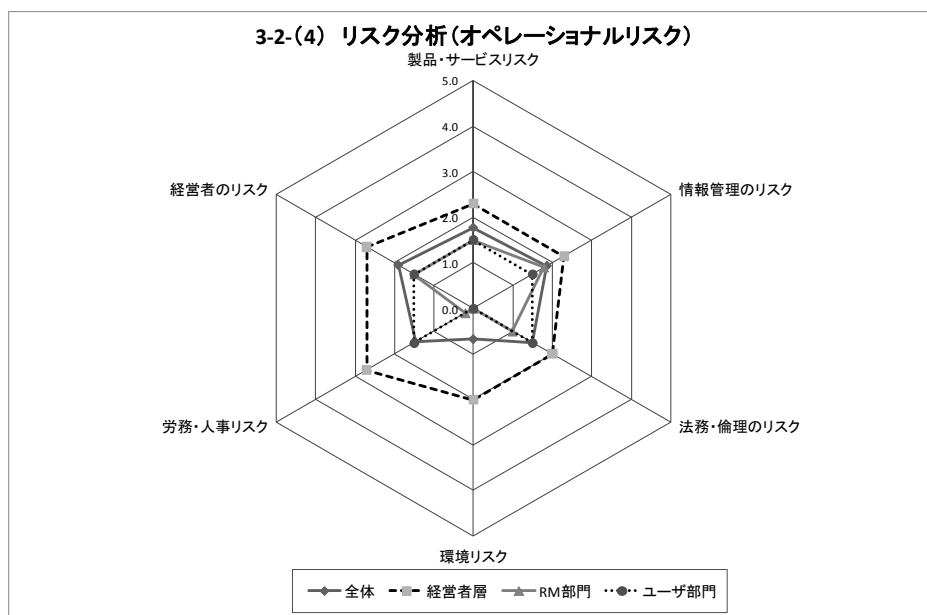
【3-2-(3) リスク分析（ハザードリスク）】



「3-2-(3) リスク分析（ハザードリスク）」については、ユーザ部門が自然災害のリスクについては検討できていないとの評価であり、一方では「事故・故障」のリスクについて高めに評価しています。これは身近にある出来事の方へのリスク認識が高いことの現れと考えられます。

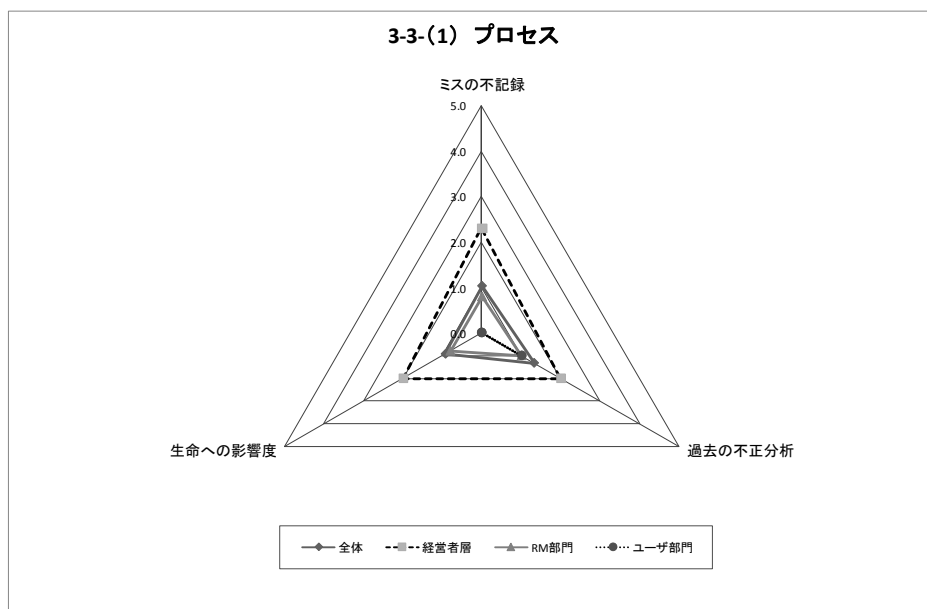
また、「自然災害」は高度な被害想定が必要との認識があると評価が低くなります。

【3-2-(4) リスク分析（オペレーショナルリスク）】



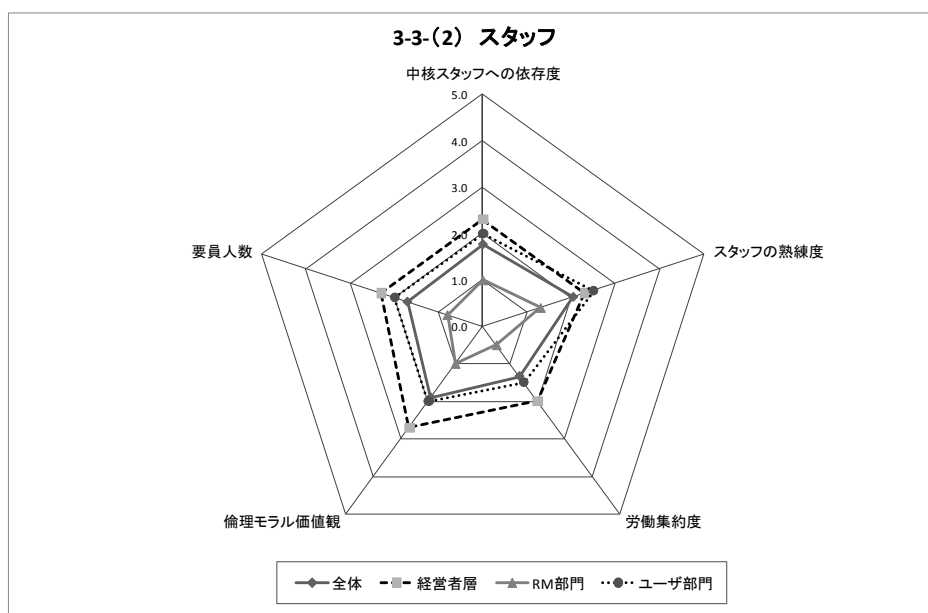
「3-2-(4) リスク分析（オペレーショナルリスク）」については、ユーザ部門は「環境リスク」について検討ができていないという低い評価を示しています。RM 部門は環境リスクに加えて「労務人事」、「経営者のリスク」も評価していません。環境問題については廃棄物、土壌汚染など難しい評価があると認識されています。また業務形態からすぐにはリスクが思いつかないという問題もあるかもしれません。

【3-3-(1) プロセス】



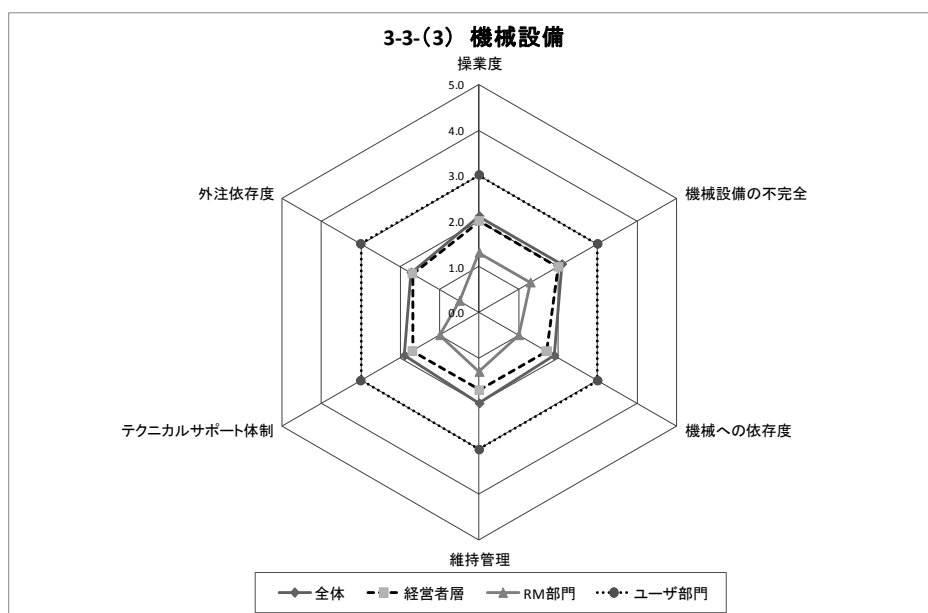
「3-3-(1) プロセス」のリスクについては RM 部門、ユーザ部門では「生命への影響度」について低い評価ですが、これは A 社の普段の業務が生命の危険が少ない業務形態であり、リスクがすぐには認識できない、という可能性もあります。

【3-3-(2) スタッフ】



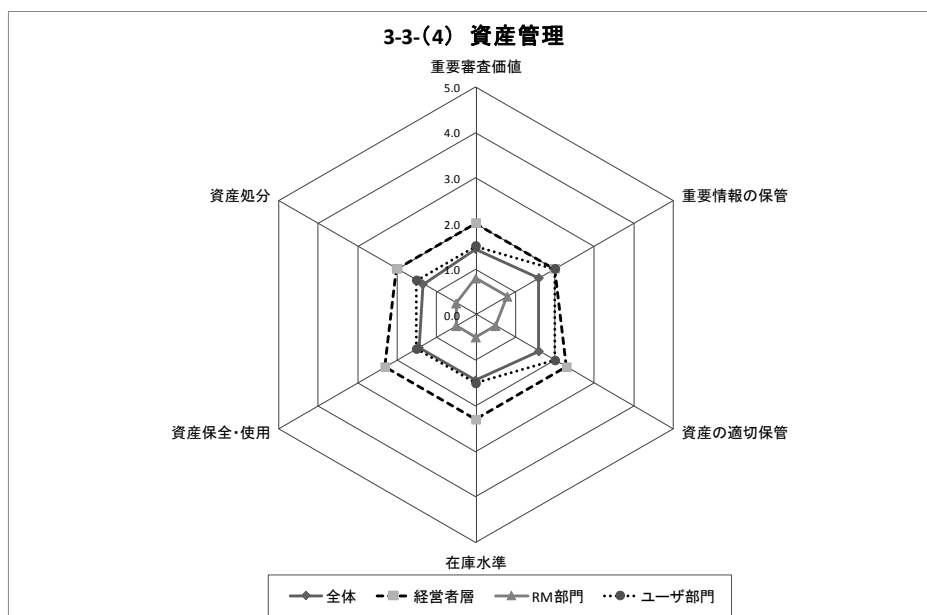
「3-3-(2) スタッフ」のリスクについて、各リスクにおいて大きな検討状況の差はありません。

【3-3-(3) 機械設備】



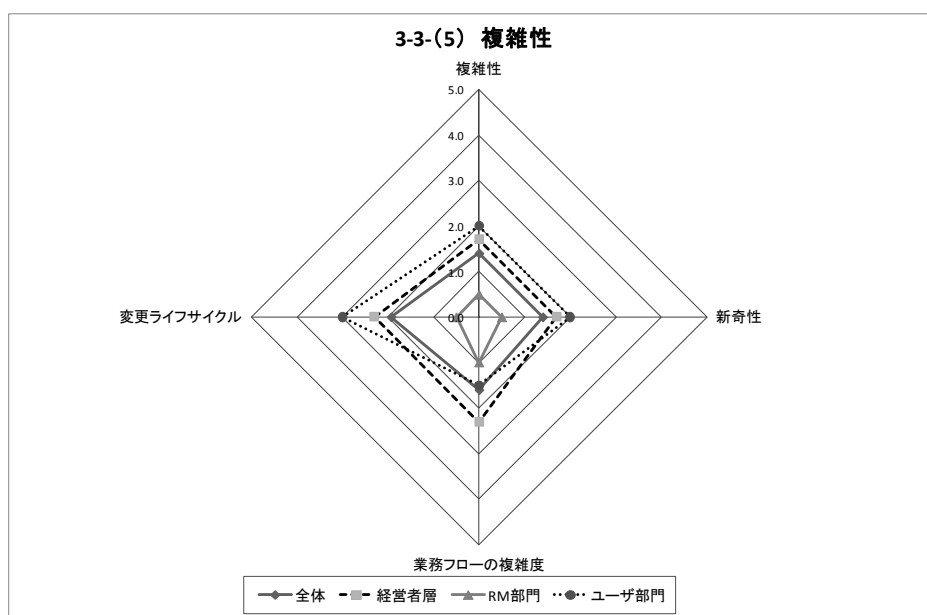
「3-3-(3) 機械設備のリスク」においても同様のリスク検討状況です。RM 部門では「維持管理」、「テクニカルサポート体制」、「外部依存度」など、メンテナンスに関するリスク検討状況が低いと見られています。

【3-3-(4) 資産管理】



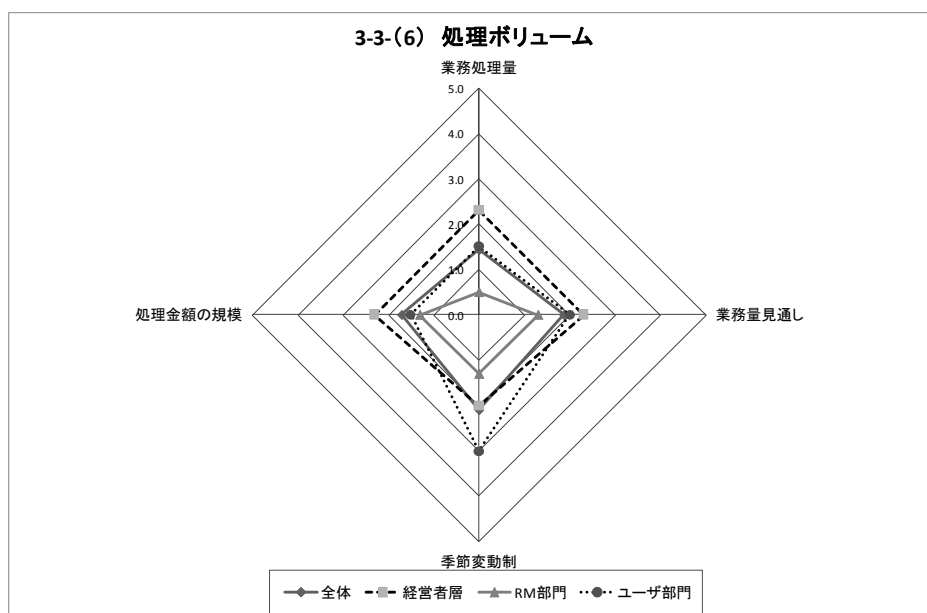
「3-3-(4) 資産管理」のリスクの検討状況において特に大きな差はありませんが、「資産処分」について経営者層が相対的に若干低い評価となっています。

【3-3-(5) 複雑性】



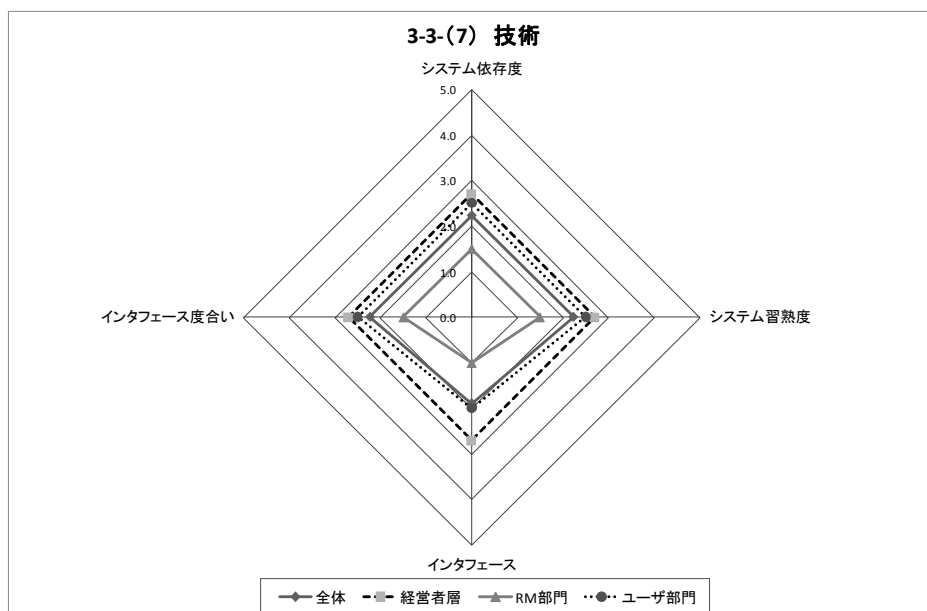
「3-5-(5) 複雑性」についてはほぼ同様な評価ですが、若干「複雑性」、「新規性」の評価について経営者層の検討状況の評価は低く、一方ユーザ部門の評価がやや高めとなっています。現場においては具体的なオペレーションが伴うためとも考えられます。

【3-3-(6) 処理ボリューム】



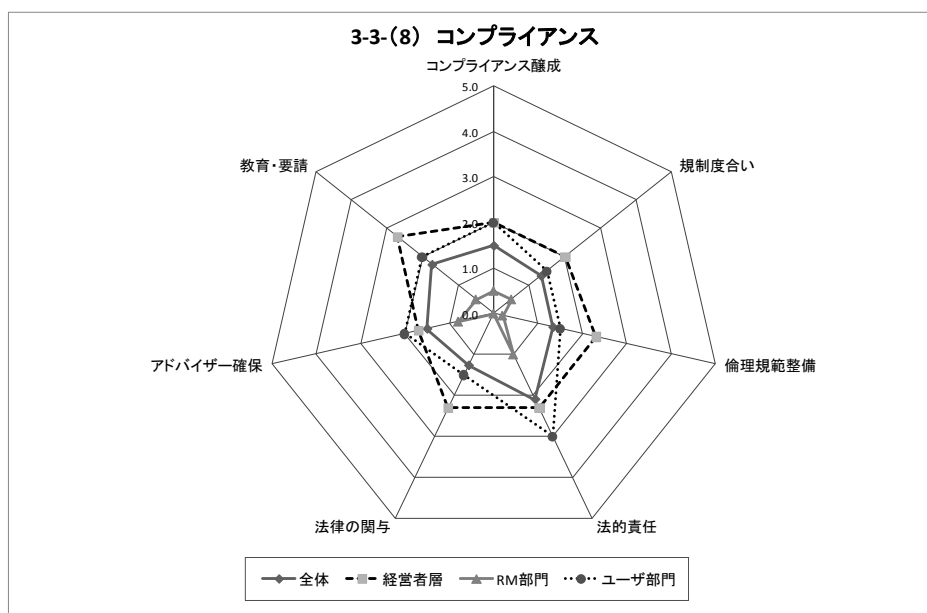
「3-3-(6) 処理ボリューム」に関する評価でもほぼ同程度の評価となっていますが、RM 部門では「処理金額の規模」について検討度合いがやや高いと評価され、一方、「業務処理量」については検討度合いが低くなっています。日常において金額が意識される一方で、繁忙度に繋がりやすい業務処理量そのものは当然という意識かもしれません。

【3-3-(7) 技術】



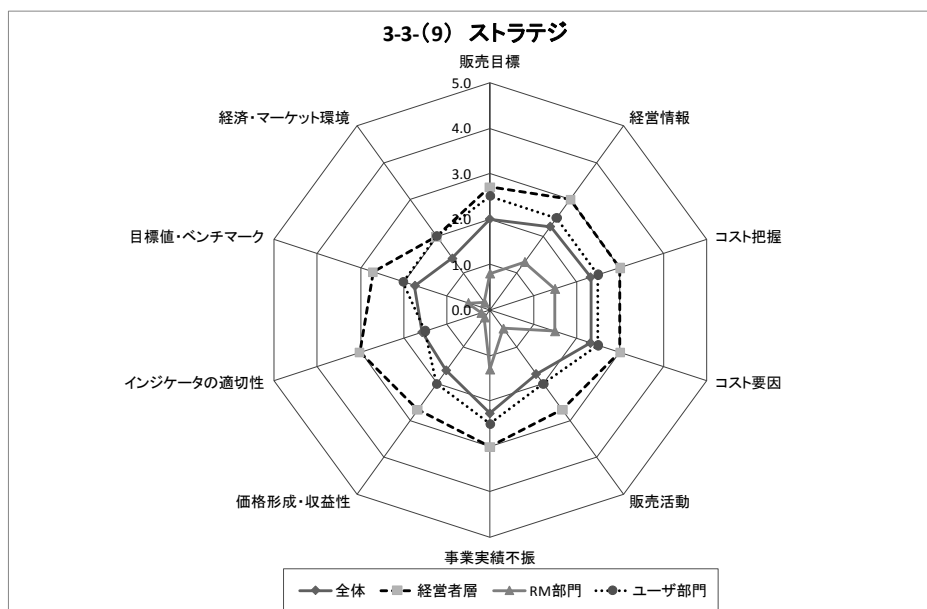
「3-3-(7) 技術」については各項目ともに大きな差は見られませんでした。

【3-3-(8) コンプライアンス】



「3-3-(8) コンプライアンス」についても全体的に他の項目と同様の評価傾向ですが、「アドバイザーの確保」については経営者層がやや低い評価となっており、何らかのサポートが必要であるとの意識の現れの可能性があります。また、RM 部門では法律による販売方法、購入方法、輸出入に関するリスクの検討が弱いと感じられており、法律に対する意識を持つことの必要性を感じていると思われます。

【3-3-(9) ストラテジ】



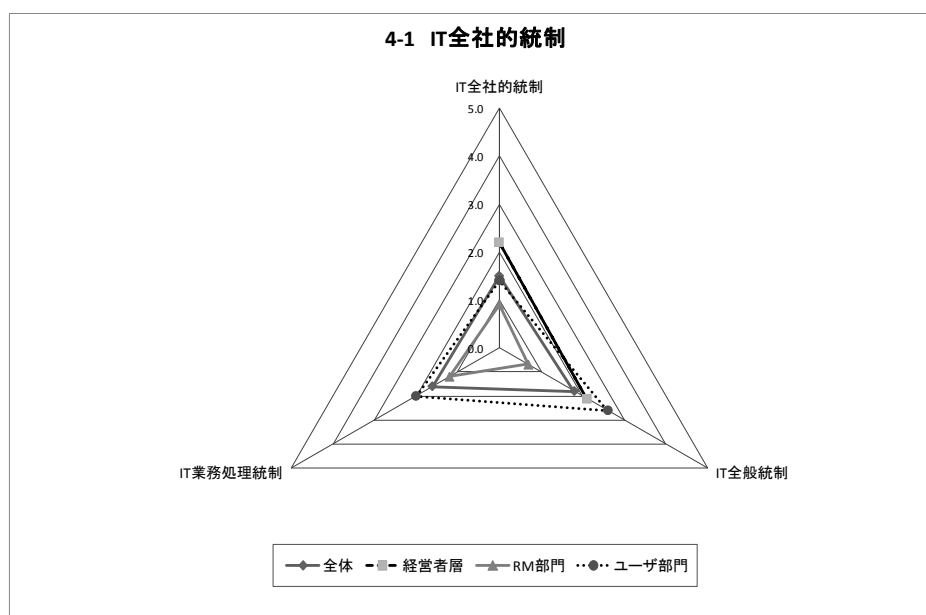
「3-3-(9) ストラテジ」もほぼ同様の評価であり項目ごとの差は少ないです。経営者層において「インジケータ（経営指標）の適切性」については相対的に高めの評価となっています。「経済・マーケット環境」についてはやや低めとなっており、不透明な経済環境での経営について若

干意識している可能性もあります。

一方、ユーザ部門では「インジケータの適切性」についてはやや低い評価となっています。具体的な日常の活動において直接指標に接することが少ない可能性があります。（営業などでは目標数字に敏感であると思えますが）。また RM 部門では想定的に「目標値・ベンチマーク」を相対的に高く評価していますが、「経済・マーケット環境」、「販売活動」については低く評価しています。これは日々の売上管理が厳しいことへの意識の現れの可能性もあります。

4.2.2.5 第4章「IT 全社的統制」(Ver.5) の詳細分析

1. 第2階層の分析



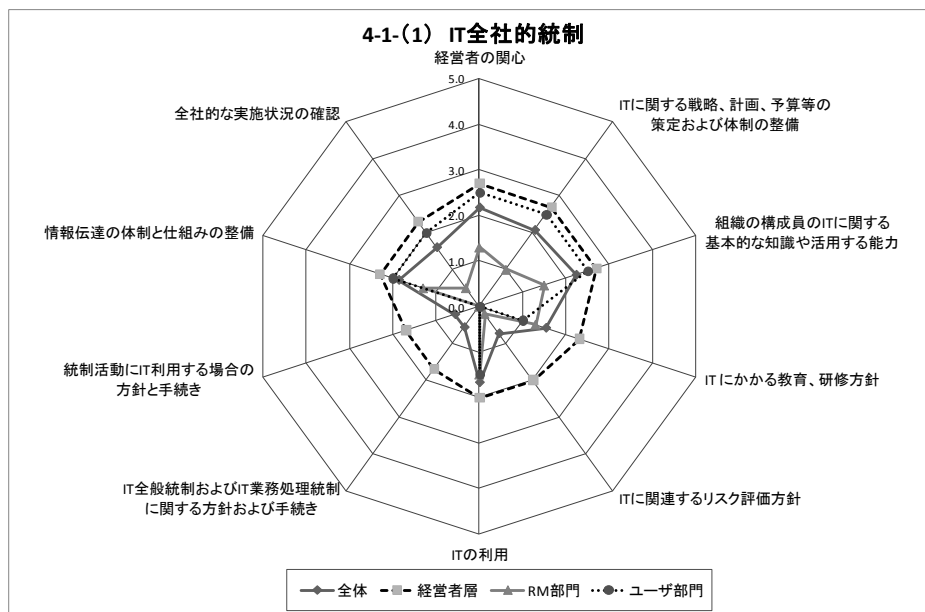
「4-1 IT 統制」について、経営者層はその重要性を理解していると考えられます。特に、全社的な対応は経営者の責務であることから多少実施していると考えているように思えます。しかし、RM 部門、ユーザ部門にとって J-SOX 対応が要請されていない、また、ISMS などの認証取得も計画がないとのことなので、IT 統制などの外部の目に見える形での対策への認識が低いものと考えられます。経営者層がすべての評価項目について RM 部門、ユーザ部門よりも高い（甘い）評価となっているのは、ソフトウェアの品質管理をしながら製品を出してきており、最小限の管理ができていると判断していることと考えられます。しかし、RM 部門やユーザ部門は、シビアに現実を見ていることがわかります。

A 社が J-SOX についての対象となっていないのに対して、「4-1-(3) IT 業務処理統制」では業務システムに要求される内部統制に関する質問が多いため、回答に窮したようにうかがえます。しかし、結果からは経営者も含めて業務システムに対するリスクなど最低限の統制への認識があることがうかがえます。

結論としては、A 社は IT 統制への認識が不足しているようです。これは、企業の実態上やむをえないと考えられますが、一方、IT 分野の企業であることから、今後上場企業が導入するシステムには、IT 統制などの内部統制に係る機能が要請されているので、これを契機に自主的に IT 統制（内部統制の仕組み）について取り組み、今後の製品開発に活かすべきと考えます。

2. 第3階層の分析

【4-1-(1) IT 全社的統制】



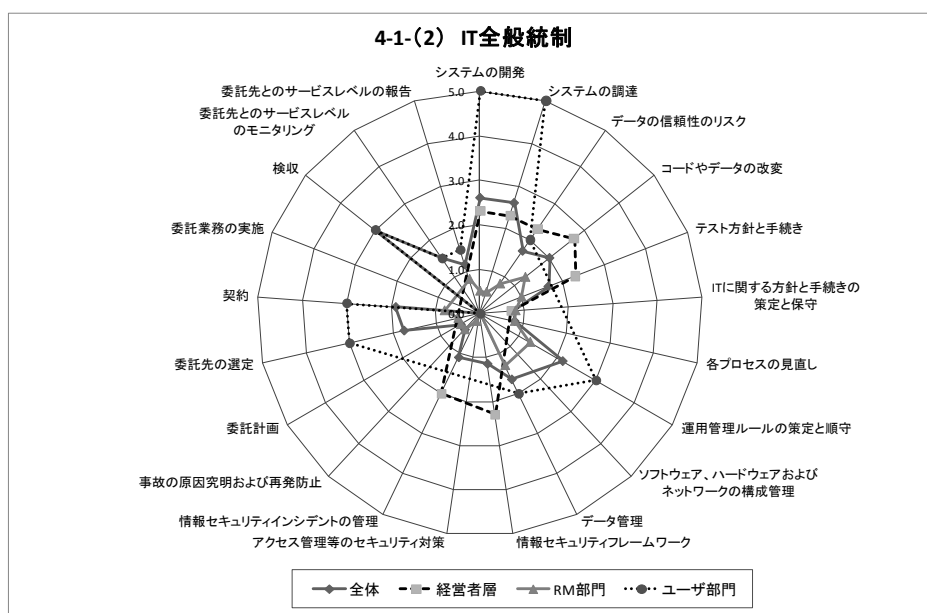
「4-1-(1) IT 全社的統制」を俯瞰したときに見えるのは、全社的な方策について経営者層とユーザ部門、RM 部門に大きな認識のギャップが存在することです。特に、リスク管理の観点からは、「IT の利用」について、経営者層、RM 部門、ユーザ部門ともに評価レベルがほとんど同じとなっており、IT の利用がリスクにつながるという点では、共通認識ができています。これは、IT の無謀な利用に対する節制につながるため、組織のリスク管理の観点からは望ましいと思われる。

一方、「情報伝達の体制と仕組みの整備」に対する回答では、経営者層が 2.3 とコミュニケーションが図られていると考えているにもかかわらず、RM 部門、ユーザ部門ともにコミュニケーションが不十分と考えており、これは A 社全体の傾向と同様となっています。

以上の点からは、特に、IT 統制に係る部分での評価が低い点は、A 社が J-SOX の対応企業となっていないためと考えられますが、今後、IT 統制は上場企業から一般の企業に広がると考えられますので、長期的なテーマとして検討されるとよいでしょう。

まずは、組織として IT のリスクについて経営者や従業員の間で情報共有を諮り、全社的な IT 統制を強める体制、標準類の作成、従業員への教育などが喫緊の課題といえるでしょう。

【4-1-(2) IT 全般統制】

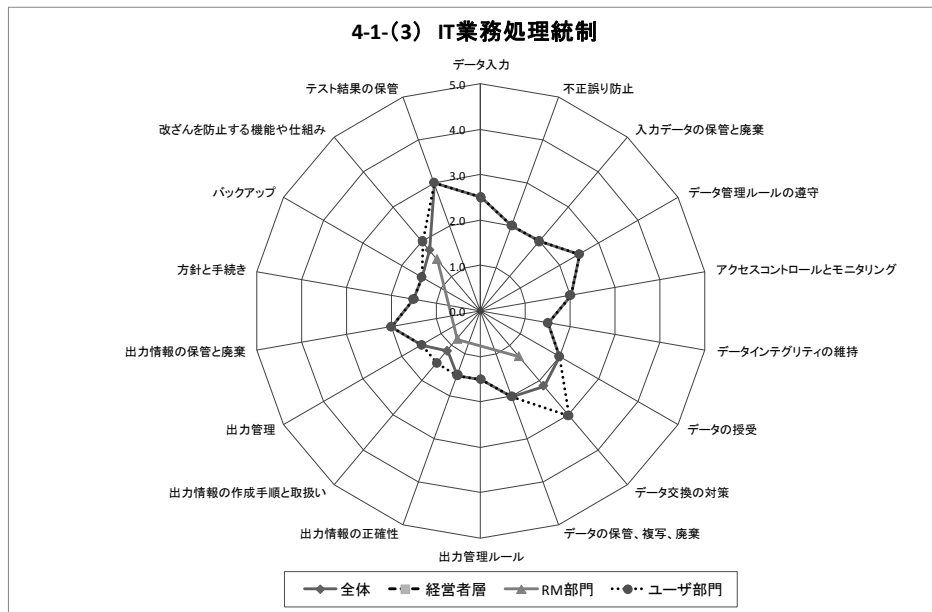


（「ソフトウェア、ハードウェアおよびネットワークの構成管理」、「アクセス管理等のセキュリティ対策」は IS 部門を対象とする質問のため、全部門回答対象外）

「4-1-(2) IT 全般統制」については、経営者層は IT 統制についての認識が高いようで、「システム開発」、「変更管理」、「テスト」、「セキュリティフレームワーク」、「情報セキュリティインシデント管理」については、2 を超えた評価となっています。一方、現場のユーザ部門や RM 部門については、IT 統制や財務報告に関係する情報システムに関する内部統制についての認識は高くありません。これは、A 社が上場会社ではなく、IT 統制についての整備・運用を求められていないため、IT 統制が後回しとなっていて仕方がないといえるでしょう。しかし、「変更管理（コードの改変）」や「データの信頼性のリスク（IT 基盤の構築）」、「テスト方針と手続き」については、財務の情報システムに限定しない設問となっています。これらについて、本来ソフトウェアの作成を業とする企業である以上、しかるべきレベルになってほしいと思います。

IT 統制分野が強くなれば、不正やいい加減さというものがなくなり、結果としては、製品の品質向上にもつながると考えられます。まずはテーマを限定して、たとえば変更管理などから取り組まれてはいかがでしょうか。

【4-1-(3) IT 業務処理統制】



「4-1-(3) IT 業務処理統制」について、ユーザ部門では「アクセスコントロール」、「データ交換の対策」、「データ管理規則の遵守」、「テスト結果の保管」、「出力情報の保管と廃棄」がレベルとして3を越えています。その他の項目ではレベル2から3と低くなっています。また、RM部門が回答している「データ交換」、「出力情報の作成手順と取扱い」、「改ざんを防ぐ仕組み」ではユーザ部門を下回っており、リスクに対する認識の違いが見てとれます。A社がJ-SOXの対象企業ではないことがよく見てとれます。IT全般統制と比べ、IT業務処理統制はJ-SOX対象企業にとって縁遠い存在のため、今回の結果となっていると考えられますが、今回の結果から、改善すべきテーマ、たとえばデータ交換などのリスク認識について、RM部門とユーザ部門で意見が合うように見直してもよいのではないのでしょうか。

3. 分析にあたっての反省事項

今回の質問はJ-SOXに係るITという特殊な設定であるため、IT統制についての基本的な概念がないと答えにくいといえるでしょう。内容が理解できないような質問については、今後見直しが必要だと思います。

同様に、「委託」についてはほとんどが「0」であり、A社では委託を実施していないと考えられます。しかし、一般論で契約についてのみ回答があります。このような場合については、委託をしていない場合には質問をパスできるような工夫（設問の仕方や企業に適用する前に、簡単に企業についてヒアリングを行い、不要な設問を削除して聞くなど）が必要と思われます。

4.2.3 実証実験に対する意見・認識

実証実験に参画された A 社ご担当者の意見を以下に紹介する。

<A 社のコメント>

今回の実証実験に参加し、当社におけるリスクマネジメントの現状をあらためて認識する機会となりました。質問項目への回答を通して現状分析ができたといえます。そこで、実証実験に関し、当社の理解を示し、参考に供することにしたいと思います。

(1) 第 1 章「組織全体のリスクマネジメントの実践」

自社評価を行った時点では、

- ・啓蒙されている
- ・仕組みの整備はできていない
- ・トップダウンでリスク対応している
- ・経営⇔RM 部門→ユーザ部門との乖離がある
- ・ユーザ部門の意識向上が必要

と自己評価しましたが、だいたい、社内での評価レベル（ベンチマーク）などというものが希薄で存在しないといっても過言ではなく、その中でユーザ部門への回答はいささか酷であったと感じていました。しかし、結果はよくしたもので、思いのほか「意識はしている」ということが明示化されたように思います。

ただし、継続的な改善の

- ・計画性
- ・実践性
- ・定着化

などには程遠く、ご指摘のとおり、経営者層および RM 部門はユーザに依存し、ユーザは経営者層・RM 部門に依存するという現象が起こっていることも明確化しました。

では、今後どのように改善すべきか....。

このように「改善すべきか」と検討できること事態がこの実証実験をさせていただいた効果があると思えてなりません。

専門家のおっしゃる「組織文化の醸成」には程遠いですが、進めるべき方向は明確になるように感じました。

- ・社員への説明不足
- ・ユーザへの教育が必要

とのご指摘を踏まえ、今後は会議などで定常的にテーマに掲げ、意識の標準化を図る必要性を痛感しています。しかしながら、弊社のような規模では一定レベルの意識を標準化することは困難で、過去に発生したリスクなど、日常的に起こる具体例を挙げながら認識していくステッ

プが必要だろうと思います。

また、「組織」という概念も実証実験時では明確にすることもなかったため、回答にバラツキが生じるのは当然のことですが、まず弊社の場合、「組織」とは何に値するかから話し合う必要性があるという実情も十分に理解することができました。その上で、経営者層／RM 部門／ユーザ部門の考えるべき視点を明確に提示することも重要なステップと考えています。

(2) 第2章「内部統制リスクと経営者の対応」

コンプライアンスを遵守しながら組織を効率的に運用すること、と解説にありますが、私どもは実証実験時にこの認識も希薄でありました。

弊社のような組織体では、「内部統制」という言葉自体接触する機会がなく、今回初めて概要を知るという実態であったように感じてなりません。平易な言葉では「自己点検監査」もしくは「金融に関する部分に特化した内容」との認識が強く、日常的にユーザ部門が意識する観点ではなかったのも事実です。弊社の場合、会計などの監査については特殊な部門（経営層と関係者のみ）に委ね実施されているような認識で、ユーザにとっては「会社依存」思考が強いと日頃感じています。

また、組織としても長年「現場がここまで正確な情報を提供するように」という枠を最小限にすることにより、社内の事務効率を上げているという施策もとっていました。

よって、ユーザが正確な概念としてこの質問を捉えているかははなはだ疑問ではありますが、コンプライアンス遵守ということは、社会人として最低限度守るべき意識としては持ち合わせていましたが、今回のように具体的に質問された場合、戸惑うばかりだったように感じます。経営者層の評価が高いのは当然ですが、RM 部門への伝達という観点で低いのか、意識していないのか見きわめる必要があることがよく理解できました。

情報と伝達。コミュニケーションにおけるギャップの問題だけではないとのご指摘には、弊社は RM 部門とユーザの境目があまりない組織体なのだと再認識した次第です。これらの意義を徹底する必要があるとのご指摘もしかり。

第1章と同様、わかるはず、理解できているはず...はないのだから、具体的な会話の中で「この話が内部統制リスクです」と噛み砕いて説明する責任が経営者層にあるということも再認識できました。

(3) 第3章「内部統制リスクのリスク分析」

第2章に続く「リスクの気づき」の部分にあたるとの解説を拝見し、前述のとおり、ユーザに対して「気づかせる」機会が少ないことに今回認識を深めることができました。

リスクを分析するということは組織の現実を目をつぶることなく、「見える化」を徹底しないと意識も認識も困難です。そういう誘導が経営者層もしくは RM 部門が強く認識していく必要性を痛感しています。

特に、「リスクを生み出す組織の脆弱性についての評価」という点では必要不可欠な活動に感じ、それをしないことには正しい評価はできないことから、今後はこの結果を踏まえて具体的なテーマを一つずつ分析していく必要性を感じています。

(4) 第4章「IT 統制」

弊社の組織体が小さいからか、「全社的統制」という言葉がしっくりきていないのかもしれませんが。内部統制と同様、IT を統制する部門が専門的にリスクヘッジを行うことで組織としての対応がなされているのが現実です。

組織として、成熟度モデルにおけるベンチマークの設定を早々に検討する必要があるとのご指摘については、前述の IT を統括する組織からユーザ部門へ情報共有をすることからスタートできそうだと感じます。

第1～3章に比べ、比較的实施できそうな項目です。

まず、できる所から手をつけていくことが弊社のような組織が取り組むことと感じます。

(5) 全体を通じて

今回の実証実験を終え、詳細な評価を受けたことにより、組織としての取組みの脆弱性が顕現し、会社の運営を考えた軸がいくぶん明確になったように思います。

ただ、まだまだ「経営者層」、「RM 部門」、「ユーザ部門」のすみわけは不明瞭ですが、今後の情報共有、意識共有の中でだんだんと明確になっていくことだと前向きに捉えていく機会となりました。

このシステムで「経年比較」分析ができるところも魅力に感じ、機会があれば弊社のメンバーがリスクマネジメントに対する意識変革が進んだかを評価してみたいと感じた機会になりました。

4.3 JRMS2003 年度版質問編による分析例

大阪大学では、2004～2008 年度に文部科学省科学技術振興調整費振興分野人材養成「環境リスク管理のための人材養成」コースを実施した。このコースでは、環境リスク「組織リスクマネジメント論」を組み入れている。このコースでは、JIS Q 2001 に基づいて、組織のリスクマネジメントを学習している。

組織では、リスクに対応するときにはリスク特定、リスク分析、リスク対応、リスク対応の効果分析の順で進む。この取組みを一時的なものではなく再現できるようにしたものが組織のリスクマネジメントである。すなわち、組織にとってリスクに対する取組みやマネジメントを分析することで、組織のリスクとマネジメントを改善できるのである。

コースでは、組織のリスクマネジメントを定量化する学習にケーススタディを用いて実際に分析を行っており、分析のためのツールとして JRMS2003 を用いている。ケーススタディは、情報漏えいを経験した企業の事例をもとに、「経営とリスクの関係」、「リスクマネジメント計画」に注目して分析している。さらに、JRMS が現場部門、情報システム部門についても分析できることから、演習では、経営者、リスクマネジャー、現場部門、情報システム部門に分かれてリスクの状況を分析し、問題点が何かを分析している。JRMS2003 は表 4-3-1 の構造となっており、経営、リスクマネジメント計画、情報システムのリスク分析と情報システムのリスク対策を含めた組織のリスクマネジメントが分析できる。

表 4-3-1. JRMS2003 の質問構成

I	経営とリスクの関係	I-1	経営環境とリスクマネジメント
II	JRMS におけるリスクマネジメント計画	II-1	JRMS の計画
		II-2	JRMS の実行組織
		II-3	JRMS の維持
		II-4	JRMS のリスク分析
		II-5	JRMS のリスク対策
III	情報システムのリスク分析	III-1	情報セキュリティポリシーのリスク分析
		III-2	情報システムのリスク分析
		III-3	情報システムの個別リスク分析
IV	情報システムにおけるリスク対策	IV-1	リスク対策における情報セキュリティ
		IV-2	情報システムのリスク対策
		IV-3	不正アクセス・コンピュータウイルス関連
		IV-4	災害対策
		IV-5	障害対策
		IV-6	その他関連項目
		IV-7	バックアップ
		IV-8	緊急時対策

ケーススタディは図 4-3-1 に示す B 企業の例を用いている。この例では、企業のリスクマネジメントを導入する以前の段階、現場部門で表面的なリスク対策の実施、リスクマネジメントの導入につながる 3 段階で構成されている。各段階での経営者、RM 部門、現場部門、IS 部門におけるリスクへの対応が描かれている。

B 企業は、ホテル事業とスポーツセンタを経営しており、個人情報の取扱いは厳しいものが要求されるが、リスク管理が十分ではなく、個人情報の漏えい事故を起こしてしまった。現場やリスクマネジメント部門では、日常的にヒヤリハットが起きていて、リスクに気づいていたものの、経営者にリスク対応を行う意図がないことから、この事実を伝えてこなかった。このため、経営者は、現場の状況を考慮することもなく対処療法的に厳しい対応をとることにした。この結果、現場では、過剰な対処策に、表面的な対応をするようになった。このため、現場や情報システム部門ではトラブルが多発して、第 2 の事故を起こしてしまった。ここにいたって、経営者は、現実を見てリスクマネジメントシステムを導入することにした。

図 4-3-1. B 企業のケーススタディ

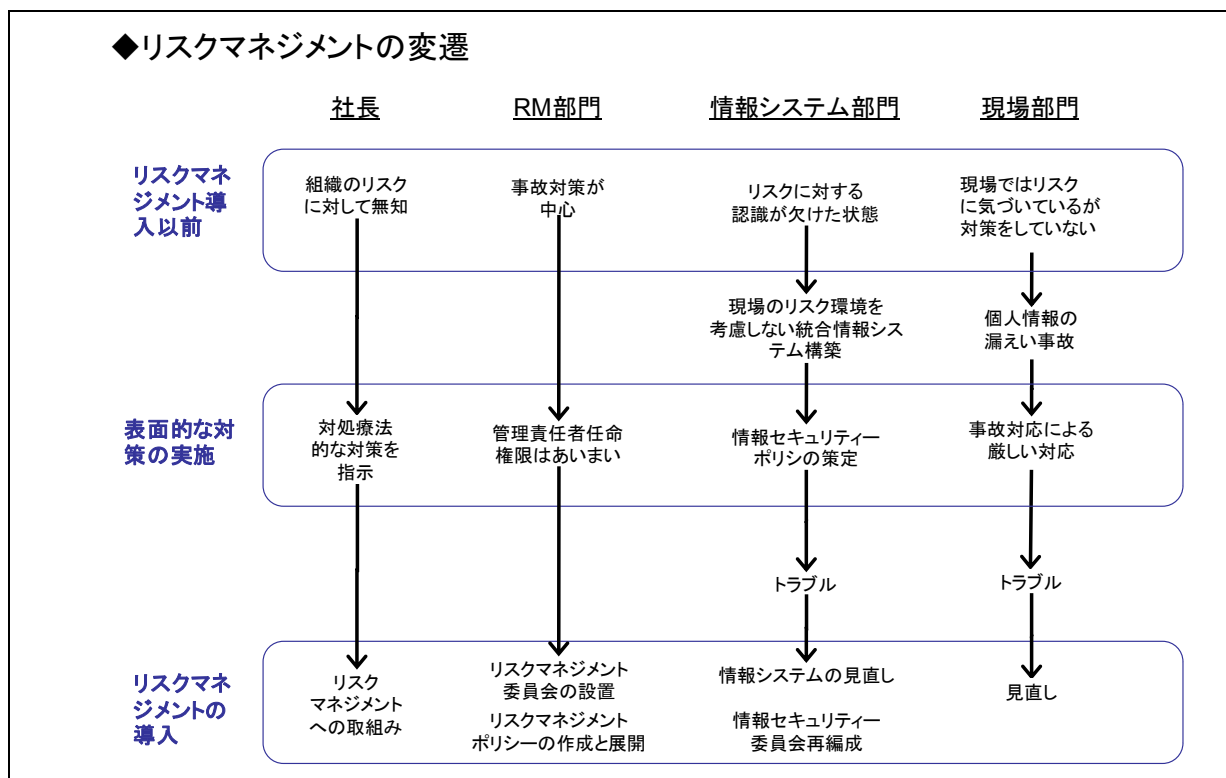


図 4-3-2. B 企業のリスクマネジメントを導入するまでの段階

演習では 4 人から 6 人程度のグループに分かれ、ロールプレイングで演習を行っている。たとえば社長、RM 部長、現場マネジャー、IS 部門長などである。これらの立場でケーススタディに示す各段階でのリスクに対する分析項目に回答していく。

JRMS2003 は Excel をベースとしたツールを提供しているが、質問項目を JRMS2010 ツールにインポートすることができる。2008 年度の演習はプロトタイプの JRMS2010 ツールを用いて JRMS2003 の質問項目を用いて実施した。三つの段階で JRMS2010 を用いて分析した例と、各段階での分析結果を以下に示す。

(1) リスクマネジメント導入以前

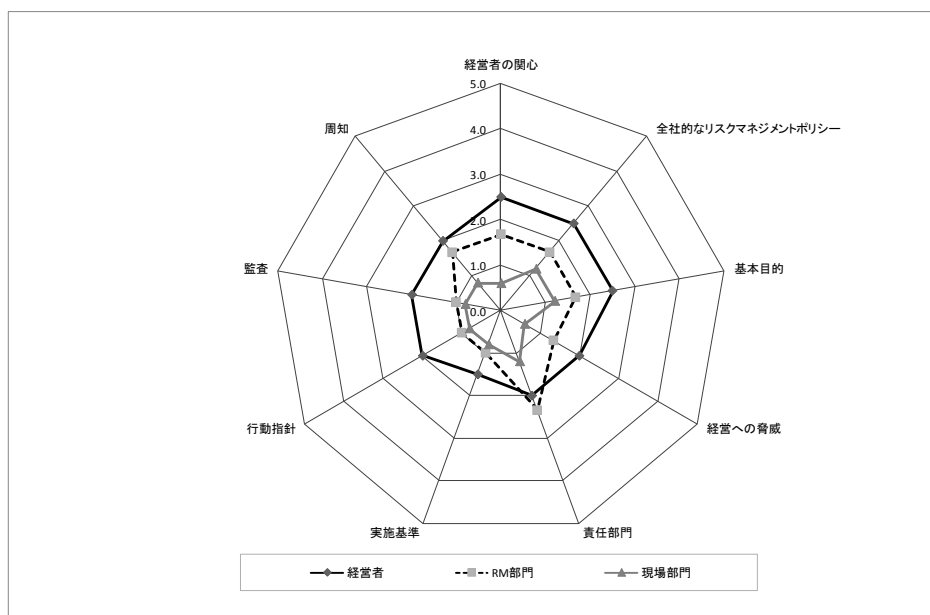


図 4-3-3. リスクマネジメント導入以前

リスクマネジメント導入以前では「経営者の関心」が低く、経営者が楽観的すぎるのが見て取れる。RM 部門では「全社的なリスクマネジメントポリシー」が現場部門より低く、「経営への脅威」では、経営者や現場より評価が低い。

すなわち、B 社のリスクについての問題をわかっているか、経営者に迎合して適切な対応をしていないことがわかる。また、「行動指針」、「監査」でも、経営者および RM 部門と現場にはギャップがあり、経営者が考えているように行動されていないことがわかる。

(2) 表面的な対策の実施

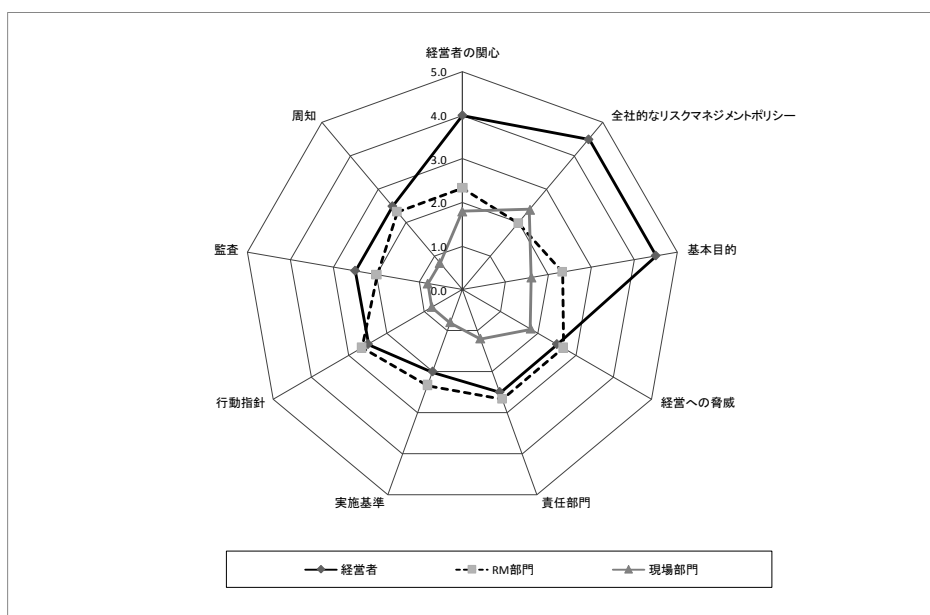


図 4-3-4. 表面的な対策実施後

表面的な対策を実施した段階では、経営者が情報漏えいを経験して慌てて全社に命令する場合を示している。特に、経営者は全社的なマネジメントを実施したと楽観的に考えており、現場の本当のリスクを理解できていない。そのため、「経営者の関心」、「全社的なリスクマネジメント」、「基本目的」では実施できたと考えている。しかし、現場や RM 部門は現実がわかっており、経営者との間で大きいギャップが生まれていることがわかる。

RM 部門も同様に、「実施基準」や「行動指針」については、経営者と RM 部門間でのギャップは小さいが、現場とのギャップは大きい。すなわち、現場に命令すればリスク対策として十分、と安易に考えていることが推測される。

(3) リスクマネジメントの導入

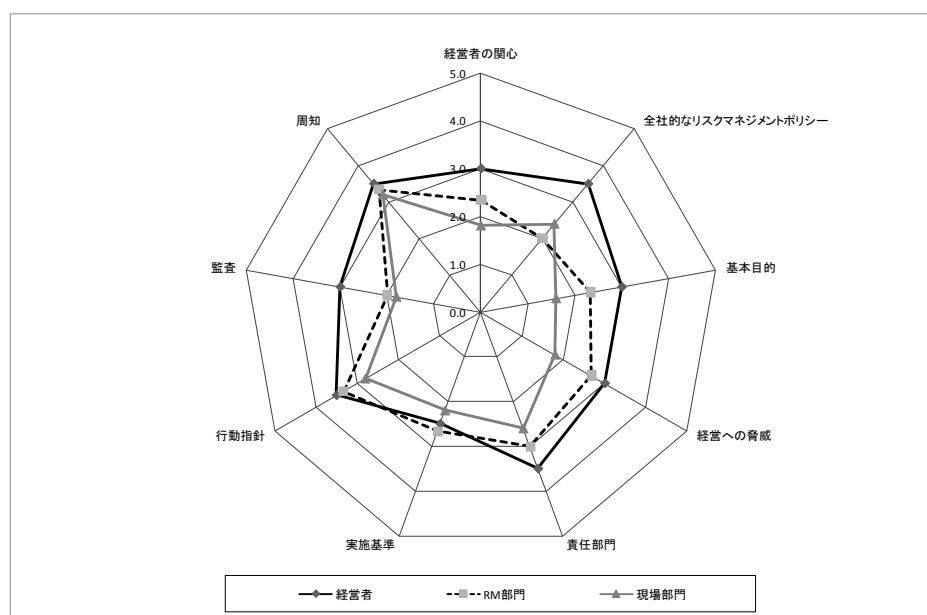


図 4-3-5. リスクマネジメント導入後

リスクマネジメント導入後では、経営者、RM 部門、現場部門でのギャップが小さくなり、リスクに対する改善が実施されているのがわかる。これは経営者が現場のリスクを理解できていることを示す。また、レベル 3 を超えていることから、マネジメントとして機能するようになったことがわかる。

三つのグラフを俯瞰するとマネジメントがどのように変化していくかについてもわかる。リスクマネジメント導入以前、対症療法、リスクマネジメントの導入の段階で比較すると、RM 部門と現場部門では、リスクに関して改善していることがわかる。しかし、経営者はリスクマネジメントの導入段階では対症療法の時よりレベルが下がっている。経営者が本気で対策を実施した結果、「経営者の関心」、「全社的なリスクマネジメント」、「基本目的」の評価が下がっている。これは、以前の段階では十分に問題を把握せずに表面的に答えたためである。レベルが下がったことだけに捉われていると正しい対応がなされた事実を見逃す可能性があるため、注意されたい。これらの考察から、B 社ではリスクマネジメントが導入され、それなりに組織のリ

スク管理が実施されるようになったことがわかる。

以下は、リスクマネジメントに関する「計画」、「実行組織」、「維持」、「リスク分析」、「リスク対策」についての企業での対応について示したものである。

(1) リスクマネジメント導入以前

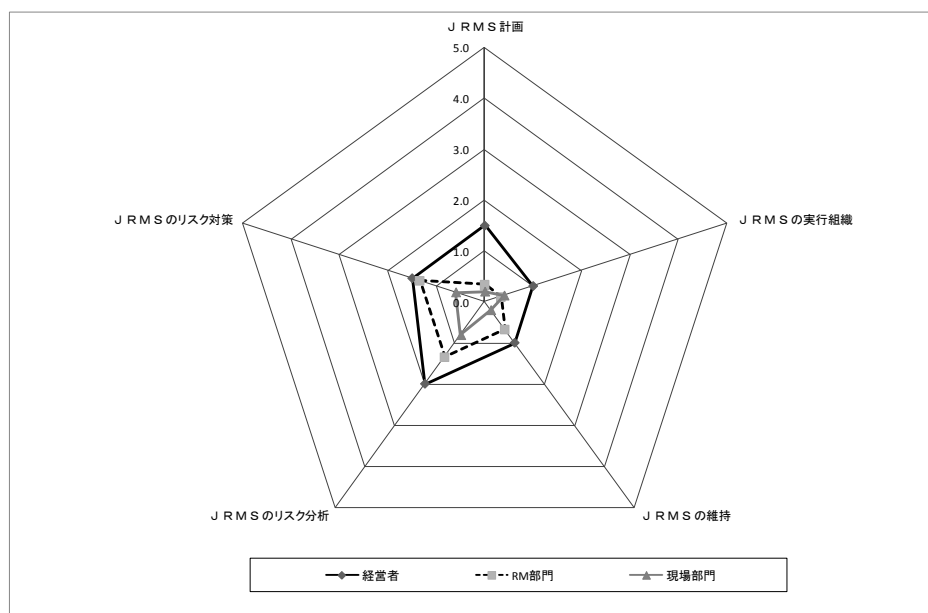


図 4-3-6. リスクマネジメント導入以前

リスクマネジメント導入以前の段階では「JRMS 計画」は経営者がワンマンで「JRMS の実行組織」となるべき RM 部門は、専務が人的ネットワークで解決しており、組織的なものとなっていない実態が示されている。ただし、企業である以上最低限のリスク対策がなされていることから、「JRMS のリスク分析」は他の項目よりも高い。

部門間のギャップは実態としては機能していないことは共有されていて、企業として脆弱であると誰もが感じているものの、無責任体制のままであることがわかる。

(2) 表面的な対策の実施

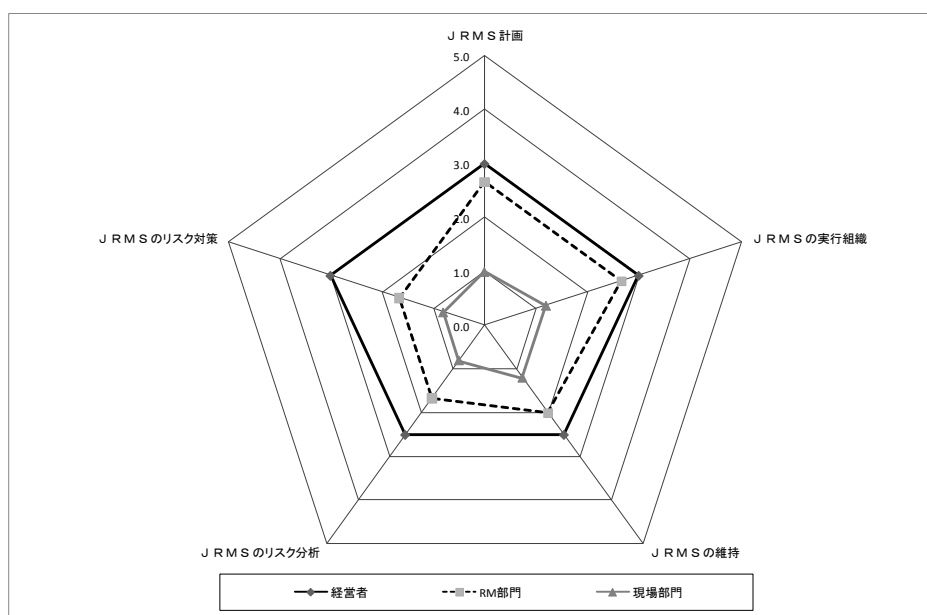


図 4-3-7. 表面的な対策の実施

表面的な対策を実施した段階では、問題が起きたことからトップダウンでとりあえずの指示がなされ、「JRMS の計画」については、経営者は最低限のレベルが実施されていると考えている。また、「JRMS の実行組織」である RM 部門は、組織的に活動を始めたことが見てとれる。しかし、それは経営者と RM 部門のみで、実際の問題が発生した現場部門とのギャップが大きいことがわかる。

「JRMS のリスク分析」や「JRMS のリスク対策」において、経営者はそれなりの対策を実施したと考えているが、RM 部門、現場部門での認識ギャップが大きくなっており、このままでは本当のリスクに対して適切な対応がなされているとは思えない。したがって、第 2 の事故が起きる可能性が見てとれる。

(3) リスクマネジメントの導入

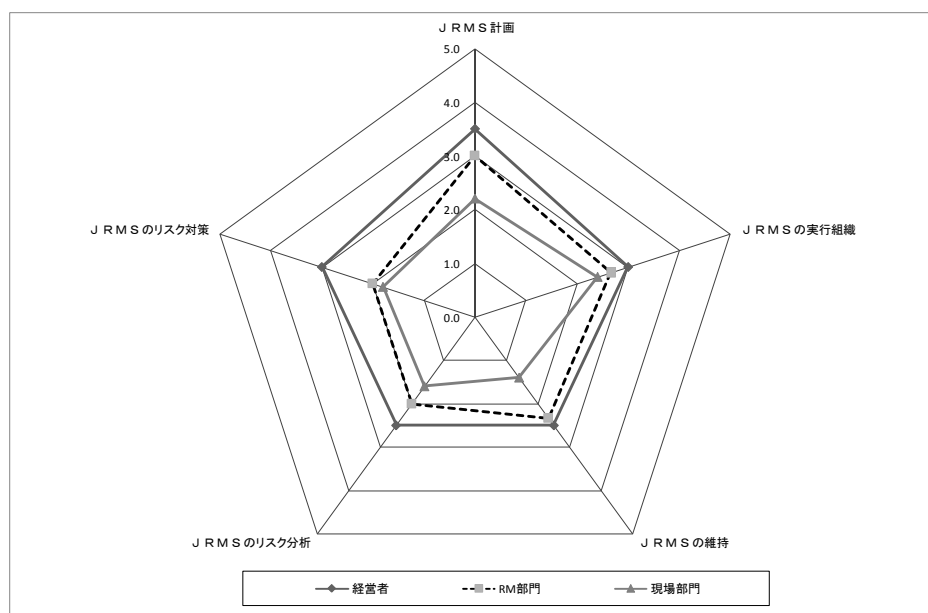


図 4-3-8. リスクマネジメントの導入

リスクマネジメント導入後には経営者、RM 部門、現場部門でのギャップが小さくなり、リスクに対する改善が実施されているのがわかる。特に、「JRMS の実行組織」でのギャップが小さくなり、RM 部門が経営者や現場部門に認知され、組織として機能し始めたことがわかる。「JRMS のリスク分析」や「JRMS のリスク対策」においても認識ギャップが小さくなっていることから、リスク対応が組織的になったことがわかる。

次に、JRMS の組織についての三つのグラフを俯瞰すると、リスクマネジメントの未導入、部分的対症療法の段階、組織化に向けて改善していることがわかる。

大阪大学の演習では、上記のようにケーススタディを分析して部門ごと、段階ごとにリスクに対する組織の変化を分析し、この組織が今後どのような面で改善が必要かについて分析を行っている。

最後に表 4-3-2 のように、関係する部門についての改善案とその優先度を決めて総合的な対策を提言している。

表 4-3-2. B 社に対する是正・改善案

部門名	優先度	主な是正・改善
経営者層	1	自らリスクセンスを磨き、組織をリード。 方針が確実に実施され、またその確認が容易な「仕組み」作りが不可欠。
RM 部門	3	クライシスを未然に防ぐシステムづくり。 リスク、管理の実態の「見える化」。
IS 部門	4	受動的対応から、積極的な情報発信へ。
現場部門	2	RM 部門、IS 部門との十分な情報交流。 システムを担当者によって差異が出ないよう整備し、継続して取組み。

このように JRMS を利用することで組織のリスクマネジメントについて分析することができる。また、大学やリスクマネジャーの養成課程では、このようなケーススタディを行うことでより現実に近い分析を通じてリスクマネジメントについて学習でき、受講者の理解を深めることができる。

2008 年度の大阪大学での組織マネジメントでは、JRMS2003 を JRMS2010 で利用することで、新しいツールの使い方や使い勝手、分析での利用方法などについても合わせて検討した。その中で、以下のような意見が寄せられ、ツールの機能として拡充することになった。

- (1) 入力 of 簡素化、分析の手軽さから、十分に実用性がある。
- (2) 上記で実施した経年分析を行うためのファイル構造にすべきである。

分析ごとにファイル名を変えて分析するのは大変なので、一つの固まりとしてデータを利用できるようにしたい。

- (3) 分析結果のデータのエクスポート機能を設ける。
グラフ分析をより多彩にするため、データを外部で利用する。
- (4) JRMS2010 のツールにデータを取り込むための機能を拡充する。

5. 参考資料

5.1 JRMS2003 について

JRMS2003 登場の背景には、当時 IT の著しい変化に対するわが国の組織対応がいま一つ明確でなく、組織のトップマネジメントから各部門の担当者に至るまで、リスクマネジメントシステムを横串として通し、リスク認識を共有する必要性があった。しかも、わが国のネットワーク環境はさらに進展を遂げ、リスク環境は一段と複雑多様化していった。そこで、新たな視点からリスクマネジメントのためのツールを構築すべく、JIPDEC のさまざまな試みの一つである 1992 年発表の JRAM (『コンピュータセキュリティに関するリスク分析—JRAM によるアプローチ』JIPDEC) の考え方をベースに誕生したのが JRMS2003 といえる。そこで、若干、JRMS2003 に関する動きを参考として示しておくことにしたい。

5.1.1 JRMS2003 の特徴

JRMS2003 は、JIPDEC が情報リスク環境下におけるリスク分析の手法として 1992 年に公表した JRAM (JIPDEC リスク分析方法論) に依拠していることから、JRMS2003 を論じる前に JRAM の一端を参考としてここに紹介する。

JRAM の基本的な特徴は、従来の日本企業ではリスクが顕在化し損失となった時、それを将来に役立てるための媒体 (たとえば、損失発生から対応、その後の組織に対する影響を示す紙媒体) およびそれを集積する部署の存在が明確でない企業が多いという認識から、そうした媒体および部署の存在を明確化させ、そこにおけるリスク対応のためのツールとして開発されたものである。

具体的には図 5-1-1 に示されているように、二つの側面から組織の情報セキュリティの実態を明らかにする分析ツールである。一つは「JRAM 質問票」に対する回答結果から実態を把握する「脆弱性分析」である。もう一つは組織の「業務日報・障害報告等」の報告書類を分析シートとし、そこでの原因・対応・組織への影響を明らかにするリスクに関する「実態分析」である。これらのいずれかの方法に基づきリスクを分析することは可能であるが、JRAM ではリスクマネジメントの実態を明らかに把握するには両者の結果を判断素材として考慮し、リスク分析を行い、リスク対応を展開するのが望ましいとする方法論であった。

JRMS2003 は、JRAM のうち、特に脆弱性分析の手法を高度化させ、組織の実態を掘り下げるという方法論を採用したものである。その理由は、リスク対応の実態に迫るには、特定の組織の関係者に委ねたリスクマネジメントは特定の部門最適といった側面に限定されやすく、組織の構成員が組織のミッション達成を脅かすリスクに対して、全体としていかなる認識を有しているのか、そのためには経営者層から現場におけるリスク認識の共有実態を把握することが組織の全体最適を指向するには不可欠である、と考えたところに主眼がおかれている。

ところで、組織の脆弱性は、たしかにネットワーク社会においては情報システム環境を重視す

る必要があるが、組織の経営を考えると、情報システムを展開する経営のあり方とリスクの関係性を根幹に据えることが必要である。そこで視点を新たに質問項目の構成に関していくつかの側面を包含させることにした。基本的な側面は「経営環境とリスクマネジメント」に関するリスク認識を把握することであった。

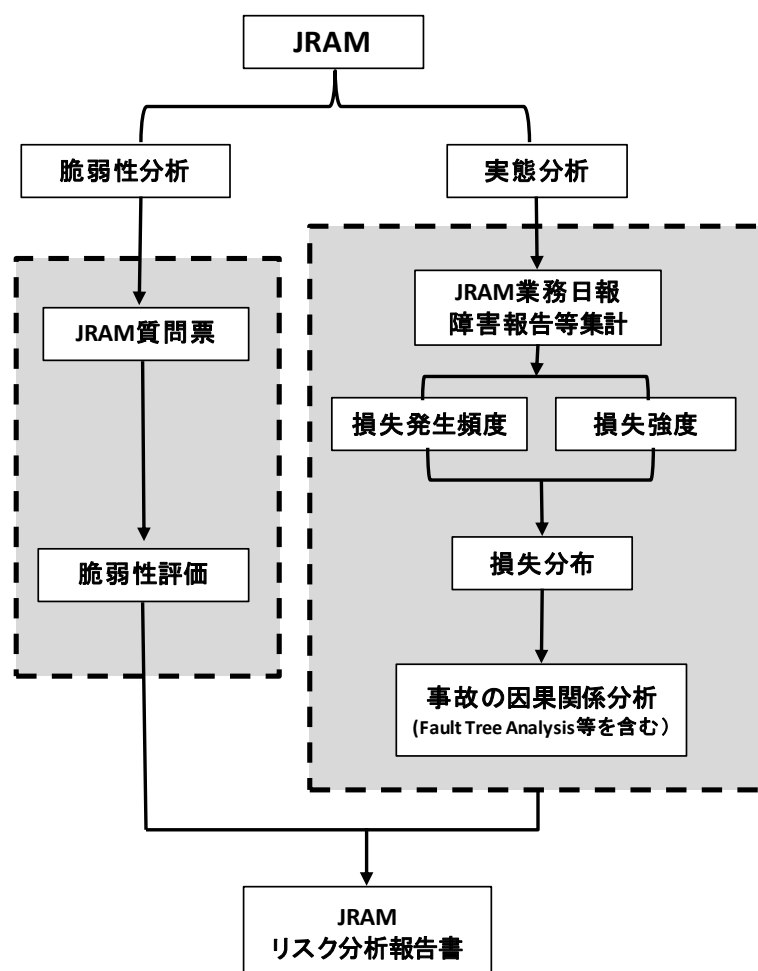


図 5-1-1. JRAM の構造

組織は規模がどうであれ、血液の循環が悪ければ栄養素は体（組織）全体に回らないし、血液を十分に循環させるためにはそうした働きをリードする神経系（適切な情報の流れ）について考慮しなければならないことは、JRMS2003 において指摘したとおりである。血液の流れも、神経系の働きも、それを統括する経営者層が的確に指令・指示を出し、組織の駆動部署がそれらに従い業務展開を行えないようでは、組織全体が目標達成のために動くことは困難である。しかし、そうした視点が具体的でなく観念的であれば、担当者の認識なり判断にギャップが生じ、全体最適が遠のくことになりかねない。JRMS2003 の構造はそうした事態を招来することのないように組織の構成員がリスクマネジメントに関する認識を共有し、経営環境の変化により発生するリスクに注視する仕組みをつくるための素材を提供することを目的としたものである。

したがって、組織を脅かす問題状況に対して局所的な対応の限界を把握し、組織の種々の資

産・活動を守るため、経営者層がまずリスクマネジメントを認識することが組織を守るベースにあるといえる。そのため、JRMS2003 は経営者層の判断に関わる項目を踏まえ、組織の構成員のリスクセンス（マインド）を刺激し、経営者層のコミットメントを前提に構成されている。

可変的な経営環境において、常に問題を発見し、不備があれば見直すことが不可欠であることから、「リスクマネジメントシステムを維持するための仕組み」に着目し、マネジメントシステムに則り PDCA サイクルを前提にしている。いわば『リスクマネジメントシステム構築のための指針 JIS Q 2001』の方法論に基づいた展開となっている。

5.1.2 JRMS2003 における三つのポイント

JRMS2003 が重視したのは次の三つのポイントであった。

第一のポイントは、まず組織としてトップマネジメントによる経営に関する「リスクマインド、リスクセンス」を持ってもらうことにあった。経営者層が組織を脅かす問題状況に関係したことが多く生じていたことに原因がある。簡潔に言えば、リスクに関わる経営者層の判断の誤りによるところに起因していたといえる。

しかし、経営者層の一般的な認識は、利益に直結しない領域へのコストの投入には消極的であるという点である。たとえば、データとして若干古いが、『2001 年度 情報セキュリティに関する調査』（JIPDEC）にそうした結果が示されている。問題が発生すれば終局的に事後的に対処し、予算化されていなくともかかったコストは特別損失として計上しなければならないわけである。

第二のポイントは、組織をゴーイングコンサーンの視点から考察するとき、経営に関わるそれぞれの部門の関係者による「リスク認識の共有」が不可欠である。JRMS2003 では、経営者（役員）層に加えて、リスクマネジメント部門・情報システム部門・ユーザ部門（管理職ならびに現場の担当者）を回答者として考慮しておいた。前述の「図 2-2-6. IT 統制を想定したリスクマネジメント体制」には、内部統制関連部門が入れられているが、それ以外は JRMS2003 での回答者を考慮する際の参考とした部門である。たとえば、CRO を中心に全体を考慮するのか、情報システム関連のリスクに対しては CIO を中心に展開するのかは、それぞれの組織の内部事情による。いずれにしても、「リスクに関する認識の共有」は、経営者層を含め、トップの判断の誤りにしろ、現場のミスジャッジにしろ、組織の存続を危うくするのは予見可能性を組織の構成員が軽視した時にある。それ故、組織を守るには、組織の構成員一人ひとりが同じようにリスク認識を有していることであるといえる。

第三のポイントは、組織を取り巻く経営環境は絶えず変化しているため、絶えずチェックし、見直すという「継続的な組織体制」を仕組みとして有しておくことである。JRMS2003 の質問項目に回答し、評価を終え、仮に組織としての対応すべき方向を見出すことができたとしても、経営環境は恒常的に変化しているわけであり、したがって、見直し・改善後もさらに適切な時期に見直しを行うことができる仕組みとしての組織体制を構築しておくことが不可欠である。

かつて JRMS2003 の有効性を確認するために実証実験を行ったが、過去に何らかの問題状況が発生し、その折にリスクマネジメント体制を作り対応を行った企業でも、担当部署が代わり、また担当者が代わることにより、過去の経験がいつの間にかお蔵入りするといった傾向が見られた。しかも、部門によってはこれまでの体験をベースに慣行化したやり方に固執しているケース

もなくはない。それ故、経営環境の変化の中では後手に回ることがある。

5.1.3 JRMS2003 の質問構成

JRMS2003 の質問項目は、回答者による質問項目の理解度を増すための工夫をいくつも施している。JRMS2003 では主として当該システムにおける理解を高めるためにページが割かれていた。たとえば、JRMS2003 の解説書は、第 1 章「JRMS の構造」、第 2 章「マネジメントシステムと成熟度モデル」、第 3 章「JRMS の質問票の構成」、第 4 章「JRMS の使い方」、第 5 章「JRMS 分析ツールの使い方」、第 6 章「ケーススタディ「X 社のリスクマネジメント」」、第 7 章「他のガイドライン、規格、制度との関係」から構成されていた。

参考のため、ここで JRMS2003 について若干質問構成の基本を示しておくことにする。特に組織の経営の視点について現状を把握するため、大きく分けて組織の経営に関わる部分と情報システムに関わる部分から構成されている。前者については、「経営とリスクの関係」と「JRMS に関するリスクマネジメント計画」の二つの大項目（第 1 階層）からなっている。これらに回答した上で、情報システムについて二つの大項目（第 1 階層）「情報システムのリスク分析」と「情報システムにおけるリスク対策」を設け、前者と合わせて四つの大項目から JRMS2003 は構成されている。

【Ⅰ．経営とリスクの関係】（第 1 階層）では、第 2 階層は「Ⅰ－1．経営環境とリスクマネジメント」に焦点を当て、組織の経営を担う関係者のリスクセンスを確認する。そのため、第 3 階層は「経営者の関心」、「リスクマネジメントポリシー」、「リスクマネジメントポリシーのフレームワーク」、「リスクマネジメントポリシーの監査」、「リスクマネジメントポリシーの周知」を考慮している。第 3 階層では「経営者の関心」、「全社的なリスクマネジメントポリシー」、「基本目的」、「監査」、「周知」というキーワードで示し、直接回答者が回答する質問項目は第 4 階層・第 5 階層で示されている。質問項目数は、第 4 階層で 9 項目、第 5 階層で 21 項目である。質問項目数はそれぞれの層により異なるが、基本的な質問項目数は階層構造により示されている。

【Ⅱ．JRMS に関するリスクマネジメント計画】では、組織としてのリスクマネジメントに関する枠組みを計画の面から把握する。まず、「JRMS におけるリスクマネジメント計画」がどうなっているのかが問われる。ここでは第 2 階層「Ⅱ－1．JRMS の計画」、「Ⅱ－2．JRMS の実行組織」、「Ⅱ－3．JRMS の維持」、「Ⅱ－4．JRMS のリスク分析」、「Ⅱ－5．JRMS のリスク対策」で構成されている。質問項目数は第 4 階層が 79 項目、第 5 階層と合わせての質問項目数は 237 項目である。

【Ⅲ．情報システムのリスク分析】では、第 4 階層が 54 項目、総項目数は 152 項目、【Ⅳ．情報システムにおけるリスク対策】については、第 4 階層が 245 項目、総項目数は 594 項目で構成されている。

したがって、JRMS2003 では、1,000 を超える質問項目により組織の脆弱性を把握するため、かなり包括的・網羅的となっている。これだけの質問に対して回答し、その結果を集計するにはかなりのマンパワーを要するため、分析の便宜性のため、JRMS 回答処理フォーマットに入力することにより「レーダーチャート」が自動的に描けるようになっており、これにより作業への投入時間を格段に節約できると共に、レーダーチャートにより関係者の視覚に容易に訴えることが

でき、部門間の比較が可能となっている。さらに、Excel シートを通して回答者間の回答結果をチェックし、ギャップ分析が行えるようになっている。

5.2 成熟度モデルについて

前述の「3.2 成熟度モデルについて」で説明しているとおり、JRMS は JRMS2003 構築の時点から成熟度モデルの考え方を取り入れている。以下に参考とした成熟度モデルを紹介する。

5.2.1 CobiT4.1 の成熟度モデル

JRMS で参考にしている CobiT4.1 は、情報システムの全業務を 34 のプロセスに分け、各プロセスについてその成熟度を定義している。成熟度はレベル 0 からレベル 5 までの 6 段階があり、それぞれのレベルは表 5-2-1 のように定義されている。

表 5-2-1. CobiT4.1 の成熟度モデル

レベル 0	不 在	識別可能なプロセスが完全に欠落している。企業は、対応すべき問題が存在することすら認識していない。
レベル 1	初期／その場対応	企業は、対応が必要な問題の存在について認識している。ただし、標準化されたプロセスは存在せず、対応は、個人的に、または場合に応じて場当たり的に行われている。総合的な管理方法は体系化されていない。
レベル 2	再現性はあるが直感的	同じ仕事に携わる複数の要員において同等の手続が行われる段階にまで、プロセスが進歩している。標準的な手続に関する正式な研修や周知は行われておらず、実行責任は個人に委ねられている。個人の知識への依存度が高く、そのため、誤りが発生しやすい。
レベル 3	定められたプロセスがある	手続は標準化および文書化されており、研修により周知されている。ただし、このプロセスに従うかどうかの判断は個人に委ねられ、プロセスからの逸脱はほとんど発見されない。手続自体は、既存の実践方法を公式化しただけのものであり、最適化されてはいない。
レベル 4	管理され、測定が可能である	マネジメント層は、手続のコンプライアンス状況をモニタリングおよび測定でき、プロセスが効果的に機能していないと判断された場合に対処できる。プロセスは常に改善され、優れた実践方法(手法)が提供される。自動化やツールの活用は、限定的または断片的に行われている。
レベル 5	最適化	継続的改善、および他社との比較による成熟度モデル化の結果、プロセスが優れた実践方法(手法)のレベルにまで最適化されている。IT は統合され、ワークフローが自動化されている。これにより、品質と有効性を向上させるツールが提供され、企業の迅速な環境適応に貢献している。

出典：CobiT4.1 (ITGI 2008.6)

CobiT では、CMM の成熟度モデルを参照しながら、対象を情報システムの全プロセスに拡大し、成熟度のレベルを定義している。また、CMM のレベル分けがレベル 1～5 となっているのに対し、レベル 0 を定義しているところが大きな違いである。

情報システムに関するリスク評価を行う場合、関連するプロセスの成熟度により、リスクが現実化する確率は大きく異なってくる。したがって、情報システムに関するリスク評価を実施する際には、関連するプロセスの成熟度の評価を行い、成熟度が低い場合には、損害が発生しやすい状況があるとすべきである。つまり、情報システムの各プロセスに内在するリスクは、各プロセスの成熟度が高ければ顕在化するおそれが低い、成熟度が低いとプロジェクト開発の失敗や重大なシステム障害の形で顕在化する。

各プロセスに内在するリスクを評価する時には、そのプロセスの成熟度があるレベルに達していることが前提条件として必要であり、レベル 2 以下のものがあつたらそのプロセスの成熟度向上について検討を行う必要がある。

5.2.2 CMMi の成熟度モデル

CobiT-III で導入された成熟度モデルは、そのベースとして CMM (Capability Maturity Model) の成熟度モデルを使っている。これは、カーネギーメロン大学のソフトウェアエンジニアリングインスティテュートが提唱したモデルで、ソフトウェア開発のプロセスを対象に作られている。CMM は、現在 CMMi に発展しているが、CMMi の成熟度モデルでは、各プロセスの成熟度レベルを表 5-2-2 のように定義している。

表 5-2-2. 開発のための CMMi の成熟度モデル

レベル 1	初期	成熟度レベル 1 では、通常、プロセスは場当たり的で無秩序である。このレベルでは、通常、組織はプロセスを支援するための安定した環境を提供しない。成熟度レベル 1 の組織での成功は、組織に属する人員の力量や英雄的行為に依存しており、実績のあるプロセスの使用に依存するのではない。
レベル 2	管理された	成熟度レベル 2 では、組織のプロジェクトは以下のことを確実にやっている。プロセスは、方針に従って計画され実施され、制御された出力を作成するためにプロジェクトが必要十分な資源を持つ熟練した人員を利用し、直接の利害関係者を関与させ、監視され制御されかつレビューされ、そしてプロセス記述に対する忠実さが評価される。
レベル 3	定義された	成熟度レベル 3 では、プロセスは、特性が十分に明確化され理解され、標準、手順、ツール、および手法の中で記述されている。成熟度レベル 3 の基盤となる「組織の標準プロセスの集合」が確立され、時間の経過とともに改善されている。
レベル 4	定量的に管理された	成熟度レベル 4 では、組織およびプロジェクトは、「品質およびプロセス実績の定量的目標」を確立し、プロセスを管理する基準として使用する。定量的目標は、顧客、最終利用者、組織、およびプロセス実装者のニーズに基づいている。品質およびプロセス実績は、統計的な用語で理解され、プロセスのライフサイクル全般にわたって管理される[SEI 2001]。
レベル 5	最適化している	成熟度レベル 5 では、組織は、プロセスに本来備わっている変動の共通原因に関する定量的な理解に基づいて、プロセスを継続的に改善する。 成熟度レベル 5 は、プロセスおよび技術上の漸進的および革新的な改善策によって、プロセス実績を継続的に改善することに焦点を合わせる。組織の定量的プロセス改善目標は、確立され、継続的に改訂されて事業目標の変化が反映され、そしてプロセス改善を管理する基準として使用されている。

出典：日本語版の開発のための CMMi® 1.2 版

<http://www.sei.cmu.edu/cmmi/translations/japanese/models/index.html>

5.2.3 NIST の成熟度モデル

NIST (National Institute Standard Technology) では、Program Review for Information Security Management Assistance (PRISMA) で利用される成熟度のレベルとして、表 5-2-3 のような定義を行っている。

表 5-2-3. NIST の成熟度レベル

レベル 1	ポリシー	管理目標が、セキュリティポリシーで定められている。
レベル 2	手続き	セキュリティコントロールを実施するための手続きが定められている。
レベル 3	実施	セキュリティの手続きとコントロールが実施されている。
レベル 4	テスト	実施の適切性・有効性を評価するテストが定期的に行われ、レビューされている。
レベル 5	統合	ポリシー、手続き、実施、テストが継続的にレビューされ改善が行われている。

出典：National Institute Standard Technology (NIST)

Program Review for Information Security Management Assistance (PRISMA) は次の URL からダウンロードが可能である。

<http://csrc.nist.gov/publications/nistir/ir7358/NISTIR-7358.pdf>

5.3 JRMS2010 xml 形式の表示例

JRMS2010 では、設問項目については国際的に広く利用されている xml 形式を採用している。これによって、質問部分の設計を外部のプログラムで実施することもできる。さらに、他のチェックリスト形式のデータを簡単に変換することで、JRMS2010 の質問項目として取り扱うこともできる。

さらに、xml 形式は視認性がよいため、ツールを使わなくても質問文の構造やその質問内容をエディタなどで容易に見ることも編集することもできる。また、高度な使い方として、データ構造も xml で定義されているため、質問文の構造すら外部で編集することができる。

以下に「第 4 章 IT 統制 (QuickStart 編)」の例を紹介している。IT 統制では、IT 全社的統制が続く、最初の質問が「経営者の関心」であることが読み取れる。

```

    <?xml version="1.0" encoding="shift-jis" ?>
<!-- 設問セット -->
<qsets>
  <qset>
    <company_code>A</company_code>
    <qset_code>15</qset_code>
    <qset_name> IT 統制</qset_name>
    <qset_remark></qset_remark>
    <!-- 章 -->
    <chapter>
      <chapter_code>5</chapter_code>
      <chapter_name>IT 統制</chapter_name>
      <chapter_remark></chapter_remark>
    <lv2>
      <lv2_code>1</lv2_code>
      <lv2_title>IT 全社統制</lv2_title>
    <lv3>
      <lv3_code> (1) </lv3_code>
      <lv3_title>IT 全社統制</lv3_title>
    <lv4>
      <lv4_code>1</lv4_code>
      <lv4_title>経営者の関心</lv4_title>
      <lv4_element_code></lv4_element_code>
      <lv4_question>
        <qno>1</qno>
        <question>Q 経営者は、IT に対して、組織として計画を作成しています
か？</question>
        <question_remark>IT への対応が組織として計画的に実施されていないこ
とにより、財務報告の信頼性が阻害されます</question_remark>
      <pattern>
        <section_code>SECTIONA</section_code>
        <pattern_dk>true</pattern_dk>
        <pattern_na>true</pattern_na>
        <pattern_data>true</pattern_data>
      </pattern>
    </lv4>
  </qset>
</qsets>

```

(以下、省略)

図 5-3-1. JRMS2010 の xml 形式による質問項目の例

JRMS2010 では、設問項目のみならず回答結果についても xml 形式を採用している。これによって、回答データの管理や視認性が高まり、他のプログラムでこの結果を分析することもできる。ズ 5-3-2 では、回答者、回答期日、時間、回答項目、回答した分類などがヘッダーに示されている。

```

<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<answer><user_code>user2</user_code>
<company_code>A</company_code>
<section_code>SECTIONC</section_code>
<qset_code>11</qset_code>
<chapter_code>1</chapter_code>
<answer_period>200810</answer_period>
<answer_date>2008/10/18 14:57:14</answer_date>
<answer_detail>
  <lv2><lv2_code>1</lv2_code>
    <lv3><lv3_code>(1)</lv3_code>
      <lv4><lv4_code>2</lv4_code><point>0</point></lv4>
      <lv4><lv4_code>3</lv4_code><point>0</point></lv4>
      <lv4><lv4_code>4</lv4_code><point>0</point>
        <lv5><lv5_code>1</lv5_code><point></point></lv5>
        <lv5><lv5_code>2</lv5_code><point></point></lv5>
        <lv5><lv5_code>3</lv5_code><point></point></lv5>
        <lv5><lv5_code>4</lv5_code><point></point></lv5>
        <lv5><lv5_code>5</lv5_code><point></point></lv5>
        <lv5><lv5_code>6</lv5_code><point></point></lv5>
        <lv5><lv5_code>7</lv5_code><point></point></lv5>
      </lv4><lv4_code>5</lv4_code><point>0</point></lv4>
      <lv4><lv4_code>6</lv4_code><point>0</point>
        <lv5><lv5_code>1</lv5_code><point></point></lv5>
      </lv4><lv4_code>7</lv4_code><point>0</point></lv4>
      <lv4><lv4_code>8</lv4_code><point>0</point>
        <lv5><lv5_code>1</lv5_code><point></point></lv5>
        <lv5><lv5_code>2</lv5_code><point></point></lv5>
      </lv4><lv4_code>9</lv4_code><point>0</point></lv4>
    </lv3>
  </lv2>
</answer_detail><answer_completed>true</answer_completed>
</answer>

```

図 5-3-2. JRMS2009 の xml 形式による回答データの例

一 禁 無断転載 一

平成 21 年 3 月発行

発行所 財団法人日本情報処理開発協会
東京都港区芝公園 3 丁目 5 番 8 号
機械振興会館内
TEL 03 (3432) 9381

印刷所 株式会社美行企画
東京都千代田区神田錦町 2 丁目 5 番地
アシスト竹橋ビル
TEL 03 (3219) 2971