２１－Ｈ００２

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（リスクマネジメントチェック・評価システム）の構築－

平成 22 年 3 月

財団法人日本情報処理開発協会

本報告書は、競輪の補助金を受けて作成したものです。
http://ringring-keirin.jp

はじめに

本報告書は、財団法人日本情報処理開発協会（JIPDEC）が財団法人 JKA の補助金を受けて実施した平成 21 年度情報化推進に関する補助事業「情報化推進のための基盤整備に関する調査」事業の一環である「IT 環境下における組織運営の評価に関する調査研究」の成果物として作成されたものです。

あらゆる組織をとりまく経営環境はこれまでの常識を超えるスピードで変化し、組織の ICT 依存度は著しく高まるとともに、グローバリゼーションに伴うサプライチェーンの相互依存関係の高まり・人口減少による市場の縮小（購買力の減少）・地球規模における環境問題等により社会環境には従来の判断能力を根本的に揺り動かすような変化が生じてきました。

JIPDEC は、これまでこうした環境変化が組織にもたらすリスクのインパクトの大きさに鑑みて、リスク対応のための理論的・実践的なシステム開発にチャレンジしてきました。その成果として世に問うのが、今回開発したリスクマネジメントチェック・評価システム「JRMS2010（Japan Risk Management verification System2010）」です。

JRMS2010 は、JIPDEC 内にリスク評価指針検討委員会を設置し、ISO/IEC において検討を重ね 2009 年末に発表されたリスクマネジメントの枠組みである ISO/IEC 31000 リスクマネジメント規格の精神を取り入れ、「経営」をベースに、昨今の企業不祥事にも対応するために「内部統制」を加味し、さらに現代社会においてリスクマネジメントが不可欠といえる組織を視野に入れ、「情報システム」、「情報セキュリティ」、「個人情報保護」、「事業継続」、「環境」、「医療」のリスク領域に関する質問項目と、回答・分析ツールで構成されています。これらの領域を取り入れた理由は、JRMS2010 の考え方、種々の領域において活用可能であること、また組織における部門間・担当者間における認識の共有を可能にする仕組みを内包していること、さらに組織が常に変化する環境下にあるため、絶えず現状を多面的に見直し、組織としてのリスク対応を高度化・成熟化させる必要があることなどにあります。

委員会では、リスクマネジメントの実践を支援するツールとして JRMS2010 が広く受け入れられるよう、企業および関係各位に協力を求め、2008 年と 2009 年に実証実験を行いました。実証実験の目的は、JRMS2010 の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の使いやすさ、さらに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にありました。ご協力をいただいた企業ならびに実証実験に関係してくださった方々からは JRMS2010 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とともに、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ご意見・ご指摘をいただきました。ご協力に対し厚くお礼を申し上げます。

現在の組織をめぐる経営環境において、さまざまなリスクに対応できる枠組みを視野に入れて構成されている JRMS2010 は、現代社会の要請に応えうる成果であると確信しております。

本報告書のとりまとめに際し、リスク評価指針検討委員会委員各位のご協力に感謝の意を表します。

2010 年 3 月

財団法人日本情報処理開発協会

2009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　所長／弁護士
	指田　朝久	東京海上日動リスクコンサルティング（株） 経営企画室 企画グループ 主席研究員
	新保　史生	慶應義塾大学 総合政策学部 准教授
	野口　和彦	（株）三菱総合研究所 研究理事
	野村　眞弓	ヘルスケアリサーチ（株）　代表取締役社長
	原田　要之助	（株）情報通信総合研究所 マーケッ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 工学部 特任教授
	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
	盛岡　通	関西大学 環境都市工学部 環境マネジメント研究室 大阪大学 名誉教授
	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
	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
	西田　聖道	（財）日本情報処理開発協会 プライバシーマーク推進センター 主任研究員
	成田　康正	（財）日本情報処理開発協会 情報マネジメント推進センター 主任部員

目　　次

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、現代社会において一段とスピードを速めてきており、組織をめぐる経営環境の著しい変化への対応は難しさを増してきている。とりわけ、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再確認する必要がある。

たとえば、2007 年夏にはアメリカにおいて住宅バブルの予兆が存在していたにもかかわらず、日本のバブル崩壊後の対応の教訓が十分活かされないまま、サブプライム関連で住宅ローン会社が破綻する事態が発生した。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損失から、傘下のファンドを凍結するといった問題も生じ、2008 年夏にアメリカの住宅公社の経営が悪化し、信用不安が増幅した。同年 9 月にはリーマン・ブラザース（Lehman Brothers）が破綻したことで、さらに金融不安が加速化し、金融危機が全世界に連鎖的に波及し、金融を重視してきたヨーロッパ諸国に甚大な影響を及ぼし、実体経済に対するマイナスのインパクトは現在も存在している。こうした側面は、リスクに関する組織や人々の判断の結果に由来することである。

この点は、各関係者間が事態の推移をどう見つめているかといったリスク認識に関係する。日本におけるバブルの際も、アメリカにおけるバブルの際も、人々の行動の論理は同じである。金融商品の購入を勧められ、そうした商品の購入により儲けることができるといった判断から売買に関与するかもしれない。また、みずからはそうした金融商品のリスクがわからないとして購入しないという選択をすることもありうる。その場合、さまざまな意見や考え方が判断に影響すると思われる。

さらに、社会環境の変化として、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。

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。

しかし、個々の人々が、経営環境の変化を認識し、そうした兆候に気づいていたとしても実体経済に影響を及ぼすような金融危機の連鎖からの脱却はグローバリゼーションの動きのなかではそれほど単純なことではなかった。流れを伴った動きを修正させるには特定の人の変化の兆候の認識力だけでは組織内で影響力をもった人々の意思決定を変化させる力とはなりにくいからである。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

ている時代状況のなかでは、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なかで、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

現在、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リスクの影響が重視されてきているが、その対応に関する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なかで、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としても、海外の取引先企業が同じ視点に立った経営を行っていなければ、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（販売子会社グループを含む）はそれぞれ A 社（本社）の海外子会社として海外の拠点における経営については現地に委ねている、と仮定する。その場合、B 社で A 社の部品を製造し、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リゼーションのなかで基準を改正しなければならないことになれば、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かなうことになる。

いずれにしても、現在の経営環境における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である。その意味では、グローバリゼーションのなかで各国が ISO の種々の規格を導入し、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よう。

---

[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１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.

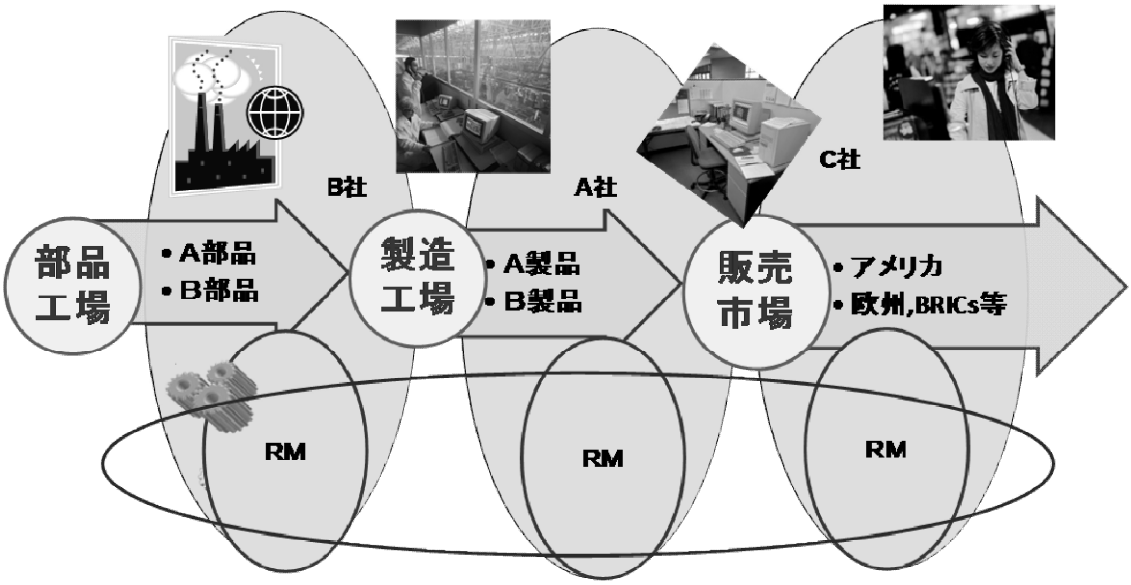


図 1-1-1. サプライチェーンの一例

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く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をもとに実践するプロセスが重要となる。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。そのため

[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、社訓をあてる場合もある。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。

には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]。それゆえ、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、こうした背景には、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視点が感じられる。1 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 1 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、潜在するリスクの影響の度合いは大きくなる。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インパクトも大きく、かつ市民や消費者が要求するレベルも変化してくることと無関係ではない。

問題状況の再発防止に対する考え方でもすでにトラブルが発生している。機械・器具類の耐用年数に関してもメーカサイドにおいても、対策を施す対象の選定や実施の必要性を検討対象に置いたり、金融商品等の投資対象などについての見方や判断にも従来と異なる視点が求められるようになってきた。かつては、問題が生じた後でも事後対応をしっかりと行えば容認されていた場合もあった。また、事故や災害を経験しない限り対応が取れず、失敗に学ぶので精一杯であり、

---

[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.

新たな問題には対応できないといった見方も存在していた。トラブルが再発防止のためによい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１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、ネガティブな影響をコントロールするものと理解されてきた。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ところに原因がある[7]。しかし、その後、「リスクマネジメント－用語規格－」の見直しが 2009 年 11 月に行われ、ISO ガイド 73:2009[8]が公表され、リスクの概念は変化した。

新たな「ガイド 73：2009」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定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１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ているのである。

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

7　こうした側面に関するリスクマネジメント用語の規格として定められたものが、国際標準化機構（International Organization for Standardization：以下、「ISO」という。）と国際電気標準会議（International Electrotechnical Commission；以下、「IEC」という。）により制定された ISO/IEC Guide73（2002 年）（以下、「ガイド 73：2002」という。）である。

8　2002 年以降、2005 年には ISO 内に設置されたワーキンググループにおいて、リスクマネジメントの標準化検討が開始され、2009 年末にリスクマネジメントの指針規格である ISO 31000 が発行された。また、ISO 31000 の検討と並行して、リスクマネジメント用語（ガイド 73：2002）の改正も検討され、ISO ガイド 73：2009（以下、「ガイド 73：2009」という。）として、ISO 31000 と同じ時期に発行された。

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。

1.2.3　ISO 31000 の考え方

（1）ISO 31000 の概要

ISO 31000 により、リスクマネジメントは各分野の好ましくない影響の管理手法というレベルから、組織目標を達成する手法として進化した。

ISO 31000 では、リスクマネジメントを「価値を創造し、保護するもの」ととらえている。

リスクマネジメントを好ましくない影響を管理するプロセスにとどまらず、組織のあらゆるプロセスにおいて不可欠で、意思決定を支援するものとしている。このことは、これまでのリスクマネジメントの考え方と基本的に差異はない。安全分野でのリスクマネジメントも事故や災害を減少し、企業価値や社会価値を増大させてきたからである。しかし、従来の一般的な認識では、リスクマネジメントは好ましくない影響を小さくするという視点で考えられていた。一方、価値の増大というと、利益を大きくしたり新製品を生み出したりというように好ましい影響を増大させるという視点で語られることが多かった。

ISO 31000 では、好ましい影響の増大も、好ましくない影響の減少も、ともに組織の価値を生み出しているということを明確に言及している。このことは、リスクマネジメントを考えるうえで大変重要なことであり、リスクの好ましい影響と好ましくない影響の双方をリスクマネジメントの対象とするという概念を支えている。つまり、好ましい影響と好ましくない影響とのバランスを考えるということは、両者を互いに相反するものととらえるのではなく、価値創造の最大化ととらえることができる、ということを示している。

この最新のリスクマネジメントの考え方は、リスクを組織の目標達成に影響を与える要因ととらえ、組織の目標達成を支援するものとしてISO 31000に集約されている。この規格は、経営の最適化を目指すマネジメント規格ともいえる。

ISO 31000の導入により、以下のことが可能になる。

・目的達成の可能性を増加させ、事前管理を促す。
・組織全体でリスクを特定し、組織全体としての対応の必要性を認識することができる。
・関連する法律および規制の要求事項ならびに国際的な規範を遵守し、義務的および自主的報告の内容を改善する。
・統治を改善し、ステークホルダの信頼と信用を改善する。
・意思決定と計画のための信頼できる基盤を確定し、管理策を改善する。
・リスク対応のために資源を効果的に割り当てて使用し、業務の有効性と効率を改善する。
・健康や安全のパフォーマンスとともに環境保護を高める。
・損失の予防と事態管理を改善し、損失を最小化する。　等

ISO 31000のリスクマネジメントの考え方について、これまでのリスクマネジメントの考え方との差異を整理すると以下のようになる。

①リスクの影響を好ましくない影響に限定していない

リスクを「諸目的に対する不確かさの影響」と定義し、その影響には好ましい影響も好ましくない影響も含まれる、としている。このことは、主として好ましくない影響を取り扱う安全分野においても、設備や活動自体を事故の管理対象としてだけみるのではなく、何がしかのプラスの影響を来たして存在しているものであることを同時に考えることが、組織マネジメントを最適化するためには重要であることを示している。

②リスクを目標達成に影響を与える要素ととらえる

目指す組織目的達成に影響を与える影響は何か、という視点でリスクを検討することの重要性を示している。

③リスク分析に先立って、リスクに影響を与える環境を調査することを求めている

リスクが状況に応じて変わり得ることを示している。このことを認識すれば、リスク分析は常に最新の環境条件を反映したものが必要であることがわかる。

ISO 31000の構造とリスクマネジメントプロセス[9]を、図1-2-1、1-2-2に示す。

9　参照：野口和彦『リスクマネジメント　目標達成を支援するマネジメント技術』日本規格協会, 2009,P.45.

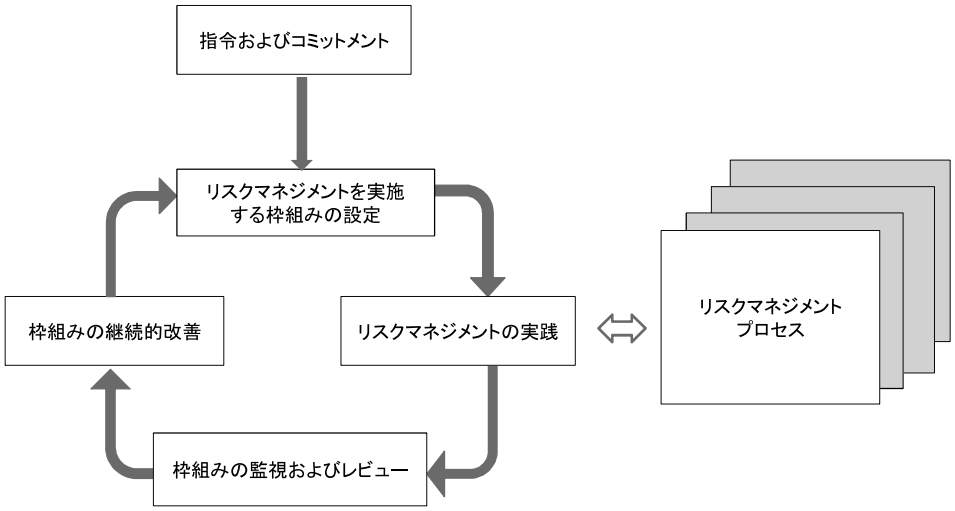


図 1-2-1. ISO 31000 の構造図

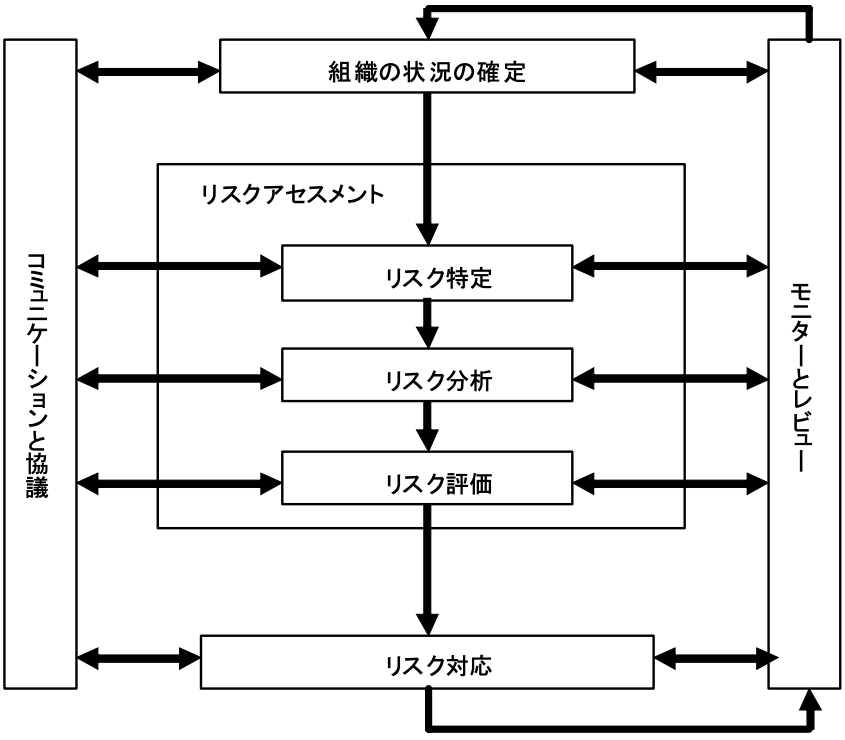


図 1-2-2. ISO 31000 のリスクマネジメントプロセス

(2) リスク概念の変遷

①これまでのリスクの考え方

リスクに対する概念は、リスクマネジメントの適用が拡大するにつれて変化してきている。一般的には、リスクとは何らかの危険な影響、好ましくない影響が潜在することと理解されてきた。

これまでのリスクの定義例を以下に示す。

（a）米国原子力委員会：リスク＝発生確率×被害の大きさ

（b）MIT（Massachusetts Institute of Technology）：リスク＝潜在危険性／安全防護対策

（c）ハインリッヒの産業災害防止論：リスク＝潜在危険性が事故となる確率×事故に遭遇する可能性×事故による被害の大きさ

②ガイド 73：2009 のリスクの定義

これまでリスクマネジメントは、多くの場合、前述のとおり好ましくない影響をコントロールすることだと理解されてきたことが多かった。しかし、ガイド 73 によってリスクの概念は変化した。

ISO/IEC では、多分野で使用されているリスクマネジメントの共通の理解を促進するために、リスクマネジメントの用語の標準化を行い、2002 年にガイド 73:2002 としてとりまとめられた。さらに、ISO 31000 を策定するに際し、用語規格であるガイド 73:2002 の見直しが行われ、2009 年にガイド 73:2009 として改訂された

ISO ガイド 73:2009 では、リスクは「目的に対する不確かさの影響」と定義された。そして、注記として「影響とは、期待されていることから、よい方向及び／又は悪い方向に逸脱すること」と記されている。そして、目的は「たとえば財務・安全衛生・環境に関する到達目的など、さまざまな側面をもち、戦略・組織全体・プロジェクト・製品・プロセスなどさまざまなレベルで設定され得る」とされている。

ガイド 73:2009 においてリスクを「諸目的に対する不確かさの影響」と定義したのは、リスクを定めた目的に対して好ましい方向か否かにかかわらず、影響をもたらす可能性があるものと定めたということである。これは、ある目的を達成するためには、好ましくない影響が存在するとわかっていても、好ましくない影響をもつリスクをとることも必要であることを示している。

この考えの基本は、影響をもたらすリスク源はその方向性までを規定しているわけではないことを示している。爆発の被害をもたらすエネルギー源も、その影響を適切にコントロールすれば適切な動力源となる。重要なことは、そのエネルギー源のもつ影響をより好ましい方向に導くことである。

この好ましい、好ましくないという概念には 2 つの捉え方がある。これまでの一般的なリスクマネジメントにおいては理解が難しいこともあるかもしれない。1 つは、文字どおり社会的に好ましい、好ましくないと考えられている価値観によって判断される双方の影響である。もう 1 つは、期待値からの乖離の方向が好ましい方向か、好ましくない方向かによって定まる場合である。利益がでてもその数値がきたしているものよりも少なければ、好ましくない結果となる。

また、好ましい影響と好ましくない影響は、同じ種類の影響の増減である場合もあれば異なる種別の影響である場合も考えられる。

リスクマネジメントを実際の組織の意思決定において活用しようとする場合、リスクのもつ好ましい影響と好ましくない影響との双方を考慮して判断を行うという概念は非常に重要である。

（3）リスクマネジメント導入のための組織の環境整備

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、リスクの把握とされてきた。しかし、現在ではリスクの把握を的確にするためにも、組織における内外環境の把握などといった事前の組織環境の整備が重視されている。

ISO 31000 では、内外の環境の事例として次のものをあげている。

①外部環境の例

・各国間・国内等を問わず、社会および文化・法律・規制・財務・技術・経済等の環境
・組織の諸目標に影響を与える主要な要因および傾向　他
・外部ステークホルダとの関係、ならびに外部ステークホルダの認識および価値観

②内部環境の例

・企業統治・組織体制・役割・義務
・もろもろの方針および目標、ならびにそれらを達成するために策定された諸戦略
・資源（例：資本、時間、人々、プロセス、システム、技術）
・情報システム、情報の流れ、意思決定プロセス（公式および非公式のいずれも）
・内部ステークホルダとの関係、内部ステークホルダの認識および価値観、ならびに組織の文化
・組織が採択したもろもろの規格、指針、モデル　他

（4）構築すべきリスクマネジメント環境

リスクマネジメントは現場の努力だけで達成されるものではなく、経営者の積極的な関与が欠かせない。本項では、リスク把握の前提となる組織ミッションの明確化、経営方針の明示、リスクマネジメントに必要な資源の確保などといった経営者の実施すべき事項を整理する。

経営者がまず実施すべきことは、組織所掌および公約の明確化である。

リスクマネジメントを導入し、有効な活動を継続するためには、リスクマネジメントの前提となり、組織の存在基盤でもある組織の所掌や活動公約を明らかにして、全組織で共有することが必要である。

ISO 31000 では、リスクマネジメントの実施に際して、次の活動を行うことを推奨している。

・リスクマネジメント方針を明確化し、承認する。
・組織の文化とリスクマネジメント方針を整合させる。
・組織の業績指標と整合のとれたリスクマネジメント指標を設定する。
・リスクマネジメントの方針を組織の目標および戦略と整合させる。
・法律および規制の遵守を徹底する。
・責任および責務を組織内の適切な階層に割り当てる。
・必要な資源がリスクマネジメントに配分されるよう徹底する。
・あらゆるステークホルダにリスクマネジメントの便益を伝達する。
・リスクを取り扱うための枠組みが常に適切な状態であり続けるよう徹底する。

そして、リスクマネジメントが組織目的を達成するための手段であるとすれば、組織目的を定めた組織ミッションを明確にして、そのミッションを達成するためのリスクマネジメント方針、その達成度を図るリスクマネジメント指標を明らかにすることは重要なことである。リスクマネジメント方針は他の組織目的と遊離して存在するわけではなく、他の目標と連動してマネジメントを実施していくものである。なお、社会規範としての法規に抵触する方針を定めることが許されないのはいうまでもない。

また、リスクマネジメントを実施するうえで必要な資源を用意することは、その実効性を確保するうえでも大切なことである。そして、組織全体でリスクマネジメントを実行するためには、内外のステークホルダにリスクマネジメントの必要性や有効性を説明し、納得をしてもらうことが重要である。

経営者は、リスクマネジメント方針を確立する必要があるが、リスクマネジメント方針にはリスクマネジメントに関する組織の諸目標および公約を明確に記述することが望ましく、通常、次の事項について言及することが期待される。

- リスクを取り扱うことに関するその組織における論理的根拠
- 組織の諸目標および方針とリスクマネジメント方針とのつながり
- リスクを取り扱うための義務と責任
- 相反する利害への対処の仕方
- リスクを取り扱う義務および責任をもつ人々を支援するために必要な資源を利用可能にすることへの公約
- リスクマネジメントの能力の測定および報告の仕方
- リスクマネジメントの方針および枠組みを、定期的、ならびに事象または周辺環境の変化に応じて見直し、改善することへの公約

こうして作成したリスクマネジメント方針は、適切に伝達することが望ましい。

リスクマネジメントを実施するうえではその責任の所在を明らかにすることが重要である。当然のことながら、リスクマネジメントに関する責任はさまざまである。リスクマネジメントの仕組み自体を計画どおりに運営する責任から、1つひとつのリスク分析のレベル確保等に至るまで、リスクマネジメントの各プロセスにおいて、各人が自分の責任を果たすことが求められる。そして、組織はこの責任体系を明確に定め、各人に周知させる必要がある。

また、経営者には説明を行うことも含むリスクに関する責任、すなわちアカウンタビリティがある。なお、ここでいうアカウンタビリティは説明責任と訳されることが多いが、アカウンタビリティという概念は、ただ説明を行えばよい、というわけではない。実施すべきことに対してしっかりと責任のある行動を行ったうえで、ステークホルダに説明する責任をもつ、ということである。

また、組織はリスクマネジメントの実行において、それぞれのプロセスが十分な能力のもとに実施されていることを検証し、担保していくことを求めている。

このことを実現するために、次の事項が重要である。

- 諸リスクを取り扱う義務および権限をもつリスク担当者を明確にすること
- リスクを取り扱うための枠組みの構築、実施、維持管理に責任をもつ人を明確にすること

・リスクマネジメントプロセスに関して、組織のあらゆる階層で、人々の前述以外の責任を明確にすること
・能力を測定し、ならびに外部および／または内部に報告し、段階的に拡大していくプロセスを構築すること
・認定の適切なレベルを明確にすること

(5) リスクマネジメントプロセス

①リスク特定

リスク特定の過程では、組織の諸目標の達成を実現、促進、妨害、低下、加速、または遅延するかもしれない多くの事象に基づいて、多様なリスクを把握することが必要となる。その際、小さなトラブルの可能性を考えて大きな利益をもたらす事業を見送り、赤字を出してしまうといった、チャンス（機会）を追求しないことに伴う諸リスクを把握することも重要である。ISO 31000 では、ある機会を追求しないことで発生するリスクに関して注意が記されている。何もしないことは何もリスクを生まないように考えがちであるが、何もしないことがその実施によって獲得できるはずだった利益を獲得できないというリスクを生んだり、事故対応を行うことで得られるはずであった組織の信頼を得る機会を失ったりするリスクが発生することに注意が必要である。

ISO 31000 では、自分の管轄下にあるリスクも管轄下にないリスクも特定することを求めている。なぜならば、リスクの把握に際してはその対応も同時に考えることが多いため、自分の管轄で対応できるリスクに限定する傾向があり、自分の部署で完結できないリスク対応に関しては、特定の段階から排除する傾向にあるからである。

②リスク分析

リスク分析では、影響とその起こりやすさの双方を検討することになる。

リスク分析は、あくまでもリスク対応に関する意思決定を支援するためのものである。リスク分析の内容や結果は対応の判断に有効である必要があり、判断にはどのような情報が必要か、また重要かということを理解し、判断に耐えうる分析にする必要がある。

③リスク評価

ISO 31000 では、対応の判断はリスク基準との比較によって定めることを推奨している。意思決定においては、法規や社会的要求等を満足することが求められる。そして、リスク分析の精度等が判断のために不十分だと考えられる場合は、分析をやり直すこともあるとしている。

さらに、リスクマネジメントにおいては既存の対応以外の新たな対応を行わないという判断をすることがある。

④リスク対応

リスクへの対応は対策を実施したということで十分なわけではなく、実施した対応が判断の意思決定として望んだ状況を創出していることが重要である。このためには、実施した対策の結果、変化したリスクが意思決定に際して目指した状況になっているか否かを確認し、十分でない場合はさらなる対策の追加、変更を検討する必要がある。そして、対策の選択肢

を検討する際には、その影響や受け取られ方をステークホルダごとに細やかに検討しておくことが望ましい。

さらに、好ましい影響と好ましくない影響をともにリスクの結果として考慮すると、影響の数学的期待値を最大にすることが、リスクマネジメントとして最適の判断であると理解しがちであるが、ISO31000 では法規を遵守することや社会責任等は、費用便益に先立って考慮されるべきものであるとしている。

1.3 リスクマネジメントと JRMS

JRMS（Japan Risk Management verification System）[10]は、財団法人日本情報処理開発協会（以下、「JIPDEC」という。）に設置された委員会[11]が開発した、組織のリスクマネジメントの現状や脆弱性を把握するためのチェック・評価システムである。

JRMS[12]は、組織や関係者の行動にかかわるリスクに対して判断の手がかりを提供し、関係者にとってよりよい方策を導くための思考および実践の場を創るために有用である。

1.3.1 JRMS の考え方

JRMS とは、現代の経営環境における組織のリスクに対する実態を把握するため、組織として設定している成熟度の目標レベルをベースに、関連する質問項目への回答結果を通し、各責任領域の構成員により組織の現実をとらえ、検討し、改善の余地を探ることにより、組織としてのリスク対応のレベルアップを可能にするシステムである。

その背景となるのは、組織をめぐる大きな課題が業務展開に係るリスクに対していかに対応するかという点である。組織にとって重要なのは、業種に固有なリスクのみならず、あらゆる組織に係る共通のリスクの存在を理解し、対応することである。たとえば、人、もの、金、情報等に係るリスクは組織のすべての領域に関係している。それだけに、労働関連、開発・製造・販売・知財等関連、金融投融資関連、情報関連に係るリスクを考慮する必要がある。

その場合、注力すべきは組織を構成する「人」のリスクに対する感性である。たとえば、「もの」作りに長けた人々にはその領域における技術はあるが、その技術の適用段階における巧拙が即リスクに関係するといった認識はなかなかもてるものではない。しかも、単に製造工程を任された

---

10 今後の世界展開に鑑みて、Jipdec の J が Japan であることから JRMS2010 を公刊するにあたり表示の仕方を改めることにした。

11 2008～2009 年度に設置された委員会は「リスク評価指針検討委員会」である。なお、JRMS の解説書が 2003 年に公刊された際の委員会は「JIPDEC リスクマネジメント委員会」であった。今回の委員会は、旧委員会メンバーをベースに、本文に掲載されている各領域の専門家を委員に迎えた構成となっている。

12 JRMS という表示は、本著の JRMS2010 および 2003 年に公刊されたリスクマネジメントの基本的システムを総称している。したがって、JRMS2010 は、新たに構成された質問項目、成熟度モデル・評価レベル、回答・分析ツール全体を意味する。

人が原材料の性質を熟知しているとは限らない。かつて実験棟において臨界を引き起こした企業にあっては、いかなる条件のもとで臨界が生じるかについての十分な教育もなく作業員に業務をゆだねていたという実態もあった。

その意味では、JRMS はリスクマネジメントの視点から、その種の問題ができるだけ起こらないようにする仕組みを有している。特に、JRMS では次の 3 つの特長を有している。

1）あらゆる組織を視野に入れ、リスクマネジメントシステムをベースにしている

2）経営環境の変化に即応するため、成熟度モデルを考慮している

3）回答者間・回答部門間の質問への回答結果のギャップを評価し合う仕組みを有している

以下、JRMS の 3 つの特長について簡潔に紹介する。

第 1 に、JRMS があらゆる組織を視野に入れた構成となっているのは、この JRMS の考え方のベースがリスクマネジメント規格によっていることにある。JRMS2003 では、JIS Q 2001「リスクマネジメントシステム構築のための指針」（日本規格協会,2001）の考え方に依拠していた。その根拠は、JIS Q 2001 では、特定の組織に限定することなく、すべての組織に適用できるように、マネジメントシステム（PDCA）を回し、よりよいリスク対応を実践させることが可能になる仕組みを用意していたことによっている。

第 2 に､組織は常に経営環境の変化に直面している｡リスクマネジメントを展開するにあたり、成熟度モデルを取り入れることにより、組織内のみならず、取引相手間におけるリスク対応の質の向上を視野に入れることが可能になる。自組織におけるリスクマネジメントの向上は、取引相手に対する信頼に結実するため、JRMS では成熟度モデル[13]の考え方を用いて、常に組織としてのリスク対応の実態をチェックしながら改善を指向する仕組みを有しているのである。

第 3 の特長は、回答者間・回答部門間の質問への回答結果のギャップを評価しあう仕組みであるが、これは、組織のリスクマネジメントの認識を共有するために欠かすことのできない特徴である。これにより、回答部門間・回答者間の評価に関する問題解決に寄与することが可能になるのである。組織はさまざまな経歴・経験等を有している人で構成されている。同じようなキャリアを積んでいると思われる人でも問題状況に対する判断にギャップ(差異)が生じることもある。このギャップの原因を究明し、解決の方向性（改善）を見いだすのが「ギャップ分析」である。

このギャップの存在については、2 つの視点が重要となる。1 つは、組織における回答者それぞれの役割認識や責任の所在等からあってしかるべきギャップもありうる点である。特定の専門領域に係る業務と現場に係る業務課題とでは、認識や理解の点で差異が生じることがやむを得ない場合があるからである。

もう 1 つは、組織の構成員は共通の認識のもとで業務展開をすべきことから、ギャップそのも

---

13 JRMS2003 においては COBIT-Ⅲおよびその基礎となった 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た。当時の組織のリスクマネジメントの実践状況に鑑みて､JRMS として 0 から 3 までの 4 段階の評価レベルを用いた。ちなみに 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 段階であったが、特に JRMS2010 においては、上記のモデルを参考にしつつも、委員会における審議を通して、リスクマネジメントの現状を的確に把握できるように努力し、後述のように、6 段階で構成した。

のが解決すべき課題である、という点である。一般的には考えられないようなことが現実に発生することがある。たとえば、企業不祥事としてニュースになった食品偽装事件の場合、経営者と現場との間で認識にギャップが存在していた。そうしたギャップを認識できなかったことには、自分がそうされたらどう感じるかといった視点もなく、儲けのためか、もったいないという考えによるものか、理由はさまざまであろうが、商業倫理上、やってはならないことが起こった（コンプライアンス違反）といえる。まさに偽装工作は関係者のモラルハザード、ひいては組織倫理の問題である。

原因が単純であればともかく、組織の規模によってかなり複雑な事情がある場合には、JRMSの質問への回答により問題を解明することが容易となる。このため、質問項目への回答者として現場の担当者のみならず、中間管理者層（JRMS では、たとえばリスクマネジメント担当者層）、さらには経営者層も想定している。仮にここで経営者層に属する X、Y、Z の 3 名を選出し、質問への回答を求めたとする。たとえば、その結果の評価がそれぞれ同じであれば、経営者層においてはリスクに対する認識の共有ができていると一応判断できる。ただし、この場合も目標レベルとの関係からレベルの認識が低い状態で同じなのか、高い状態で同じなのかは、それぞれの組織によることになる。低いレベルで同じであれば、実態としてそれでよいのかが問われるかもしれない。組織として設定していた目標レベルに比べ、それぞれの評価が低ければ、目標との間でギャップが存在することになる。したがって、組織として望ましいと判断できるレベルにするためにはどうすればよいのか、改善の努力が求められることになる。

1.3.2　JRMS2003 から JRMS2010 へ

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、リスクにかか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 2 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 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 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、1 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[14]）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時、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。

特に組織におけるさまざまな業務に係るリスクについて、組織の方針がどうなっているのか、明確に決められているのか、もし方針等が明示されていれば業務に関係するリスクについて同様の判断や行動が求められるものと思われる。そうした現状をよりよく理解するために構成されたのが JRMS である。JIPDEC が JRMS の新たなバージョンを世に問うため「リスク評価指針検討委員会」を立ち上げたのも、社会における組織人のリスクに関する行動において、さらによい方向を見いだすための方法論を導き出すためであり、委員会の成果として誕生したのが JRMS2010 である。

これまでも簡潔に触れたが、社会や組織が高度化し、複雑化すればするほど、潜在するリスクは大きくなる。社会が便利になり事業活動が活発化すれば、われわれが享受している状況や利益が喪失した時のインパクトは非常に大きくなるため、消費者や市民にとって耐えがたい反動となりやすい。

過去の失敗経験や悪影響を被った体験に基づいた再発防止という考え方ではすまないほど、現代社会の変化はスピードアップしている。過去の事例に基づき、対策の選定や実施の必要性をコストとベネフィットの点から比較し、コストがかかりすぎれば、対策を講じないのが経済合理的であるといった判断が妥当とされた時代もあった。また、何らかの問題状況が発生し、その後の再発防止にとってよい経験になったといえるレベルにあれば、組織としての存続が可能になることもあった。

しかし、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。事後的な対応では組織が存続しがたい事態が発生しているからである。そこで、問題状況が発生する前に、つまり、そうした状況が潜在している段階においてリスクに対応する必要性が発生してきたのである。このような要請に応じるため、企業運営におけるマネジメント技術の改革が不可欠となり、その手段の 1 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、その実践的なツールとして JRMS2010 が登場したのである。

14　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）は前記にかかわるリスクの重要性を認識する智恵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

1.4　JRMS2010 の特徴

JRMS2010 では、組織における基本として「経営」をベースにおいている。経営において重要な点は、組織としての経営理念[15]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。そのため、経営理念達成に係る要因であるリスクについて種々の角度から検討することになる。そこで、組織はまず経営環境（外部・内部の状況）を踏まえ、経営方針を明確にし、それに基づきリスクマネジメント方針を構築し、リスク対応のための行動指針を明確にすることが求められる。それゆえ、リスクマネジメント計画を立て、それに従いリスクアセスメント（リスクの特定・分析・評価）を行い、リスク対策を選定し、実行に移す。その後で、その成果を評価し、状況に応じて是正・改善の措置をとる。そのため、リスクマネジメントの実践にあたり、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。しかも、こうしたプロセスにおいては関係部署との間でのモニタリングとレビュー、さらにコミュニケーションやコンサルテーションが重要となる。

とりわけ、組織の経営には特定の部署の最適化ではなく、組織の全体最適を志向する視点からリスクマネジメントの仕組みを構築し、各業務におけるリスクアセスメントを重視し、リスク対応を継続的に行うという基本的な考え方の導入が不可欠となるのである。

1.4.1　JRMS2010 の 3 つの特徴

JRMS2010 では、JRMS で指摘した特徴 3 点をさらに進化させている。

第 1 に、JRMS2010 では ISO（国際標準化機構）のリスクマネジメント規格である ISO 31000 の考え方に基づいている。この ISO 31000 はあらゆる組織を対象にしたフレームワークであり、他のマネジメント規格をカバーするアンブレラ規格[16]である。リスクマネジメントにおいて出発点は組織の置かれた状況の把握である。そこにおいて関係者はリスクを特定することから始まるプロセスに従い、リスク対応を目指すことになる。この点については、本章「1.2.3　ISO31000 の考え方」で論じている。

JRMS2010 において、特に注視したいのはリスクマネジメントを実践するにあたっての関係者

15　組織としての「経営理念」は、JRMS2010 においては、営利組織・非営利組織を問わず、組織として達成すべき最上位概念として位置づけられている。現実に経営を行う際の基本的な考え方は幅が広く、欧米ではミッションといった用語が用いられている。概して、組織の設立目的、存在目的を指し、会社によっては「社是」・「社訓」を意味している。しかし、経営目標との関連もあり、組織の構成員にとってのレーゾンデートル（存在意義）として明文化されたものといえる。経営理念の達成のため組織方針を明確化し、そのために各種の経営資源が投入されることになる。

16　リスク関連の規格には品質規格（ISO 9000 シリーズ）、環境規格（ISO 14000 シリーズ）等があるが、他の規格にとりリスクマネジメントについて基本的な枠組みを示しているという意味でアンブレラ規格として表現されている。
　野口和彦『リスクマネジメント　目標達成を支援するマネジメント技術』（JSQC 選書）日本規格協会,2009

のリスクに関するセンス[17]の度合いを図る仕組みを導入している点である。センスが乏しければそれを養う必要がある。そのためにはそれなりのプログラムや仕組みがなくてはならない。そのためにJRMS2010により有効となる指針を見いだすことが可能になるといえる。

第2に、経営環境が恒常的に変化する現状に鑑みて、リスク環境の変化への対応を重視し、レベルアップを図る必要性から、成熟度モデルを視野に入れている。とりわけ、JRMS2010においては、それぞれの組織がリスクマネジメントの実践を重視せざるをえない現状に鑑みて、成熟度の評価レベルを6段階に設定した。したがって、リスクマネジメントを展開する組織として、どの評価レベルを目標レベルとして設定すべきかを決めることも重要な課題となる。

第3に、業務の実践にあたる業務部門・担当者間におけるギャップの存在を認識するためにギャップ分析を導入している。JRMS2010を活用する組織の部門関係者が、リスク領域別の質問項目への回答結果を通して、組織の実態と回答者の評価度合いを比較考量することができる仕組みを有している。したがって、JRMS2010を用いることにより、設定した目標レベルと回答時点での評価結果との差異から改善すべき問題点が浮き彫りになり、現状からの改善が可能になるといえる。

JRMS2010の活用にあたっては、これらの特徴の重要性を十分に理解することが肝要である。そこで、「評価の仕方」および「ギャップ分析」のそれぞれの特徴について解説する。

1.4.2　JRMS2010における評価の仕方

組織においてリスクマネジメントの現状を客観的に把握するためには、何らかの評価の仕方が必要である。この点、JRMS2003においては注13で示した成熟度モデルを参考にした。JRMS2010でも同様に成熟度モデルの考え方を採用している。以下、この点に関して論じておくことにする。

（1）JRMS2010の成熟度モデルの考え方

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、わが国において、リスクマネジメントの考え方が浸透してきたことを踏まえ、リスクマネジメントの各領域について評価レベルを表1-4-1のようにレベル0～レベル5までの6段階に定義した。

また、評価レベル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、評価レベル4とレベル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

17　リスクに関するセンス、すなわち、リスクセンスのことである。リスクセンス（risk sense）とは組織や個人の行動においてリスクの重要性を認識する知恵や感性を指す。類似語としてリスクマインド（risk mind）があるが、これ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指している（参考：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）

に図示すると、図 1-4-1 のようになる。つまり、組織経営といった組織全体を対象とするときは、レベル 4 とレベル 5 については、リスクコミュニケーション等を重視して評価し、個別リスクの対応においては、PDCA による改善を重視している。

表 1-4-1. JRMS2010 の成熟度の評価

成熟度の評価レベル		定　義	摘要例
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。
1	個人ごとによる対応	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。
2	部門ごとによる対応	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。
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、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)。
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。
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。	・外部のリスクマネジメント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る。

+対象領域

1　組織経営

1.1　経営

1.2　内部統制

2　個別リスク対応編

2.1　情報システム

2.2　情報セキュリティ

2.3　個人情報保護

2.4　事業継続

2.5　環境

2.6　医療

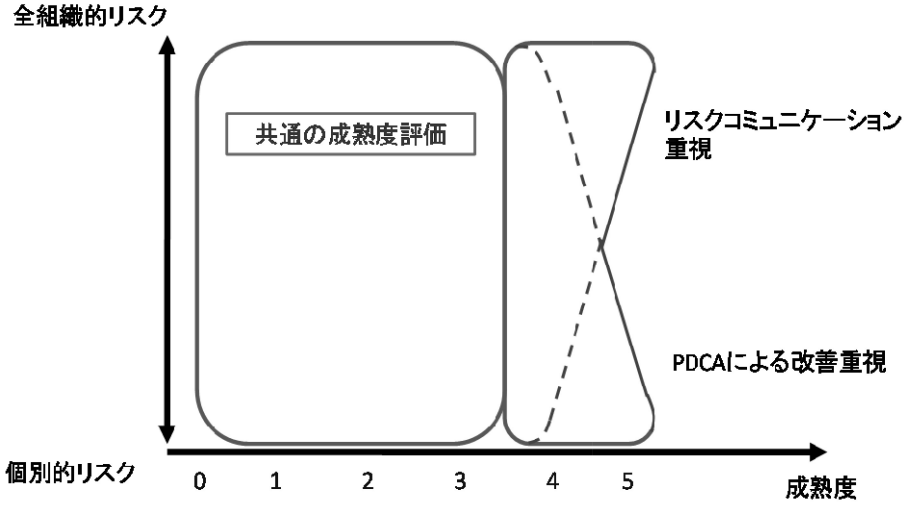


図 1-4-1. リスクマネジメントの対象領域と成熟度の定義

（2）成熟度モデルの具体例

前述の JRMS2010 の成熟度モデルについて、その理解を助けるために、パンデミックと個人情報保護についての具体例を次に提示する。

①パンデミック

評価レベル		摘要例
0	未認識・未対応	・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	個人ごとによる対応	・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	部門ごとによる対応	・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を呼びかけている。
3	全組織による対応	・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	・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	・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。

②個人情報保護

評価レベル		摘要例
0	未認識・未対応	・個人情報保護法について知らない。 ・個人情報の識別を行っていない。
1	個人ごとによる対応	・個人情報についての規則を決めた部門もなく、名刺を読み取ったファイルに個人的にパスワードロックをかけている人がいる。
2	部門ごとによる対応	・コールセンタでは、独自に個人情報保護についての規則を決めて、個人情報を保護している。
3	全組織による対応	・全社的な個人情報保護についての規則があり、全組織に配布されている。 ・全社的な個人情報保護について、担当する組織が作られている。
4	全組織による管理された対応	・個人情報保護について、規定どおりに実施されているかを定期的に監査し、経営者に報告している。
5	全組織による最適化された対応	・全社的な個人情報保護を担当する組織は、他の組織で発生した個人情報漏えいについて情報を収集し、自組織の対策に不足している点がないかを見直している。

（3）N/A（Not Applicable）と D/K（Don't Know）の取扱いについて

JRMS2010 の質問票では、回答として評価レベル 0～5 の選択肢に加え、N/A（Not Applicable）と D/K（Don't Know）という選択肢を追加している。大規模な組織では、リスクマネジメントに関する役割を複数の組織や個人に割り当てるため、各個人は自組織のリスクマネジメントについてすべての詳細を把握しているわけではない。したがって、各個人の担当領域以外のリスクについては、その詳細を知らないという回答として D/K が必要となる。たとえば電子商取引を行っていない組織にとっては、電子商取引に関する質問はその前提条件を満たさないので意味がない。こういった場合は N/A を選択することで、その質問を対象外として取り扱うことができる。

JRMS2010 では、質問の解説や用語説明により回答者が質問の意図を理解しやすくしているが、回答者がリスクマネジメントについての基本的な概念や、自組織のリスクマネジメントの概要については理解していることを前提としている。たとえば、情報システムの運用部門から情報セキュリティ部門に異動してきたばかりの要員の教育目的でこの質問票を利用することは想定していない。したがって、質問票である個人の回答に D/K が非常に多いときは、その個人の役割と D/K が多い領域を見て、回答者として適切かを確認する必要がある。

JRMS2010 の質問票は、どのような組織でも使用できるように、網羅的な項目で構成されている。したがって、前述の電子商取引の例のように、自組織では行っていない項目に関する質問がある可能性があり、この場合は N/A と回答する。ただし、注意する必要があるのは、実際には自組織で行っていても、その事実を知らずに N/A と回答する場合があることで、ある質問項目について N/A とレベル 0～5 の回答が混じったときは、自組織の状況を確認する必要がある。

1.4.3　ギャップ分析

JRMS2010 の質問への回答は、回答者によって評価結果にギャップが生じることがある。このギャップを分析することによって、組織のリスクマネジメントの現実について貴重な情報を把握することができる。ここでは、ギャップの種類と JRMS ツールにより描かれるギャップの読み方について簡潔に示しておく。

（1）　ギャップの種類

前述のように JRMS2010 の質問票は、関係各個人が回答する。回答部門内の回答者により出された回答結果が同じ場合もあれば、異なる場合もある。部門としての成熟度を出した場合（たとえば、図 1-4-2 のように評価レベル 3 を組織の目標レベルと設定している場合)、すべての項目について同じレベルということはなく、目標レベル以下のケース（図 1-4-2）もあれば、それ以上の場合（図 1-4-3）もあるといったように、項目間のギャップや組織として目標とする成熟度に対してのギャップが存在する。

つまり、部門間と回答部門内という側面からみると、ギャップという言葉には 2 つの意味がある。1 つは組織の従業員の自組織の現状に対する評価のギャップで、もう 1 つは組織として目標とする成熟度のレベルと現実とのギャップである。各従業員の評価のギャップは、実務レベルになると担当領域以外のリスクの詳細については知らないので、リスクマネジメントを複数の部門で分担している大きな組織では自然と発生する現象である。ただし、同一部門内での役職による違いや、同僚との回答が大きく食い違う場合は、リスクマネジメントのプロセスに問題があることを示唆しており、その分析が必要となる。一方、目標レベルとのギャップは、組織のリスクマネジメントの成熟度を継続的に向上するための評価指標として活用できる。

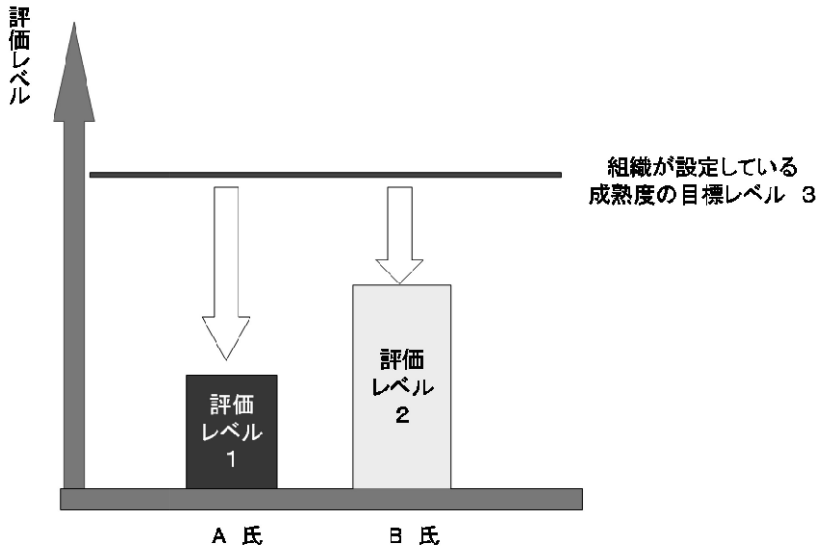


図 1-4-2. 評価モデルにおけるギャップ

ところで、図 1-4-2 のように、同一部門内の同一職種に従事している回答者間にギャップが存在している場合、そのギャップがいかなる原因によるものなのかを分析する必要がある（ギャップの原因分析）。概して、ギャップの発生は、回答部門における回答者の経歴・リスクへの関心の度合い、事実認識の度合い等が質問項目の理解に影響し、回答結果に反映されることがある。

たとえば、部門内において、3 名（A 氏、B 氏、C 氏）の回答者が同一の質問項目を回答した場合を考えてみる（図 1-4-3）。しかも、C 氏のみが組織目標としたレベルより高い評価レベル 4 と回答した場合、他の回答者（A 氏、B 氏）との評価のギャップの大きさには特に着目すべきである。これは部門内のみならずリスクマネジメント部門（以下、「RM 部門」という。）にも重要な意味を投げかける場合があるからである。時として、ギャップの開きが大きい場合、回答者間におけるリスク認識の差異がリスクマネジメントの実践に大きく関係するかもしれないのである。こうした側面は部門間のギャップについても同様に考え、分析することが必要である。

しかしながら、ギャップの発生を否定的にとらえるべきではない。JRMS でギャップ分析を導入しているのは、ギャップの原因を重要なリスクマネジメント情報と考え、ギャップが組織における役割・職能等により当然存在するものと理解できる場合もあるが、リスクに関する関心の度合いやリスクマネジメントに関する認識の低さによるものであれば、これを克服し、認識を共有することにより、リスクマネジメントの強化を達成することが可能になるからである。いわば、ギャップ分析の活用により、リスクに対する組織内の認識が共有でき、ひいては人財の活性化が可能になるといえよう。この点がギャップ分析に着目する理由である。それゆえにギャップ分析を通して組織としてのリスクマネジメントの実態を把握することが不可欠となるのである。

したがって、そうした状況に対応するため、組織の RM 部門内にギャップ分析担当者および改善を行う教育担当者の位置づけを明確にしておくことが必要となる。組織内の担当者については後述する。

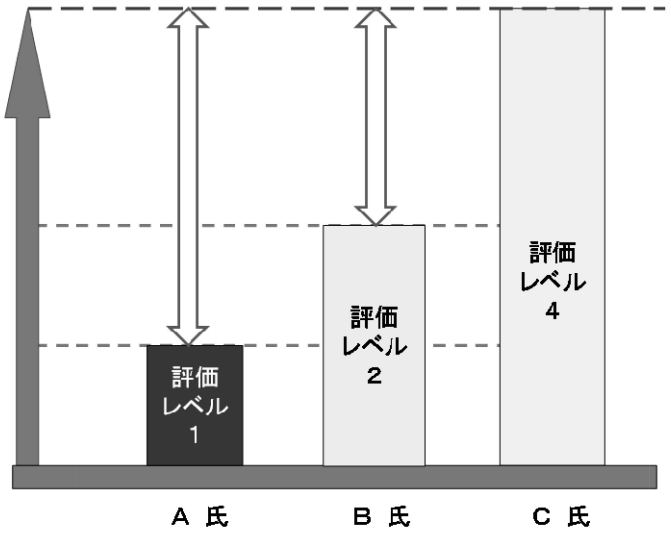


図 1-4-3. 評価モデルにおけるギャップ

（2）ギャップの読み方

質問項目への回答をJRMSツールに入力すると、回答結果に基づいた評価結果がレーダーチャート（後掲）に描かれる。そして、レーダーチャートで評価結果を比較すると、回答がすべて同じということはなく、何らかのギャップが存在するのが一般的である。本節はレーダーチャート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。

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、RM部門、ユーザ部門　等）および回答者別にレーダーチャートで表示される。

このチャートを見ると、回答部門・回答者により、成熟度の判定が異なり、ギャップが発生することが考えられる。この回答部門・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うえで重要な情報となる。また、組織として設定した目標レベル（組織が目指している評価レベル）と回答部門・回答者間のギャップにも留意する必要がある。

しかし、同じようなギャップが見受けられる場合でも、その発生原因は必ずしも同じではない。その原因を、図1-4-4の『JRMSの質問票に対する回答作成のモデル』を使って考える。回答者は、客観的な事実を認識し、JRMSの質問と成熟度の定義を参照してレベルを評価する。この場合に、事実の認識は回答者の関心度に影響される点に注意が必要である。このモデルを用いると、ギャップの発生原因は次のように分析できる。

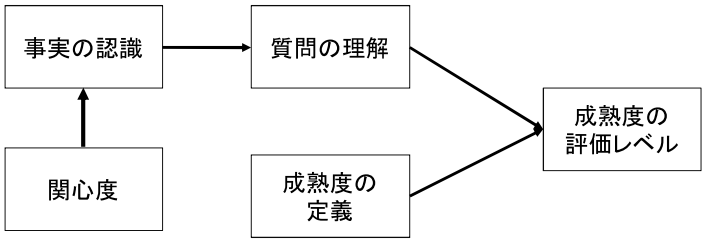


図 1-4-4. JRMSの質問票に対する回答作成のモデル

同一の質問に対して異なる成熟度の判定をした場合は、次の4通りの原因が考えられる。

i　回答者間で事実の認識に違いがある。
ii　回答者間で関心度に違いがある。
iii　回答者間で質問の理解に違いがある。
iv　回答者間で成熟度の定義の理解に違いがある。

JRMS2010では、回答者のリスクマネジメントに対する理解に違いがあっても、質問の解説、用語説明等により、iiiとivの原因による食い違いが少なくなるように配慮している。したがって、同一の質問に対して異なる成熟度と判定する原因の大半は、iとiiになると考えられる。これに対しては、回答者各自が成熟度評価を行った後に、回答者間で、事実の認識について話し合うことにより、iとiiの原因による違いは解消できるので、部門間での成熟度に差があることも含めて、組織としての成熟度を判定できるはずである。

JRMS2010 では、部門の立場により回答の視点が異なる場合を考慮し、部門にあわせて表現を変えている質問文がある。このため、たとえば、あるリスク領域について、経営者層とユーザ部門が異なる質問に答えている場合は、上記 i～iv の原因に加えて、『v 部門の異なる回答者への質問の内容が整合していない』ことにより、成熟度の判定が異なることが考えられる。これに対しては、JRMS2010 の実利用からのフィードバック結果から、質問の論理的な整合性を図ることにより、改善をすすめることも考えられる。

②評価上の留意点

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留意点は以下のとおりである。

i 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。

ii 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。

iii 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、その部門で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。

1.5 組織における JRMS2010 の実施体制

これまでも指摘してきたが、組織がどのような目的のために JRMS2010 を導入するのか、そのために組織内に責任ある体制を構築するのか、この点に関し、3 点示しておくことにする。現在の組織は常にリスク対応を視野に入れて組織経営を行っている。そこで、JRMS2010 の実施にあたっては、少なくとも次の点から活用を図ることが望ましい：その 3 点とは、

①組織のリスクマネジメントの有効性の検証

現在の経営環境に鑑みて、リスクマネジメントの現状に対して JRMS2010 が有効か否かの検証を客観的に行う。

②リスクマネジメントに関する組織の脆弱な部分の発見

組織のリスクマネジメントの脆弱な点について、JRMS2010 の質問項目への回答結果と目標として設定したレベルとのギャップから脆弱性を把握する。

③リスクマネジメントに関する組織構成員の認識の共有

組織活動におけるリスクマネジメントにおいて重要なのは、組織構成員の認識の共有、ひいては一体感である。そのための拠り所を JRMS2010 の実践を通して把握することができる。

リスクマネジメントの実施体制については、上記のような意図のため、JRMS2003 では情報システムを中心に示した。JRMS 2010 では、経営をベースにおいているため、関連する部門・領域は多岐にわたる。しかしながら、現実に組織は業態・規模・事業展開の範囲等々により多様である。ここでは、実施体制について参考として示すにとどめておく。

1.5.1　JRMS2010 の実施体制の例示

組織をとりまく経営環境が厳しくなってきた今日、事業の継続性に対して経営者が責任をもってリスク対応を行うことが必要である。しかも対応状況についてステークホルダに説明できることも強く要請されている。

全社的なリスクマネジメントの実践という観点から、JRMS2010 では経営者層、RM 部門、ユーザ部門と大きく 3 つの部門に分けて回答するように構成されている。その際、それぞれの部門において、とりまとめる責任者および全体の回答結果の集計を担う責任者の指名が組織として求められる。組織の経営規模によるが、全社的なリスクマネジメントについての責任は最終的には経営者層、特に社長（CEO）が担うことになる。とりわけ、中小企業などでは社長が多くの部門にかかわるため、重要な役割を演じることになるが、企業の規模が拡大するとともに、経営者層も業務執行が分担される（図 1-5-1 参照）。

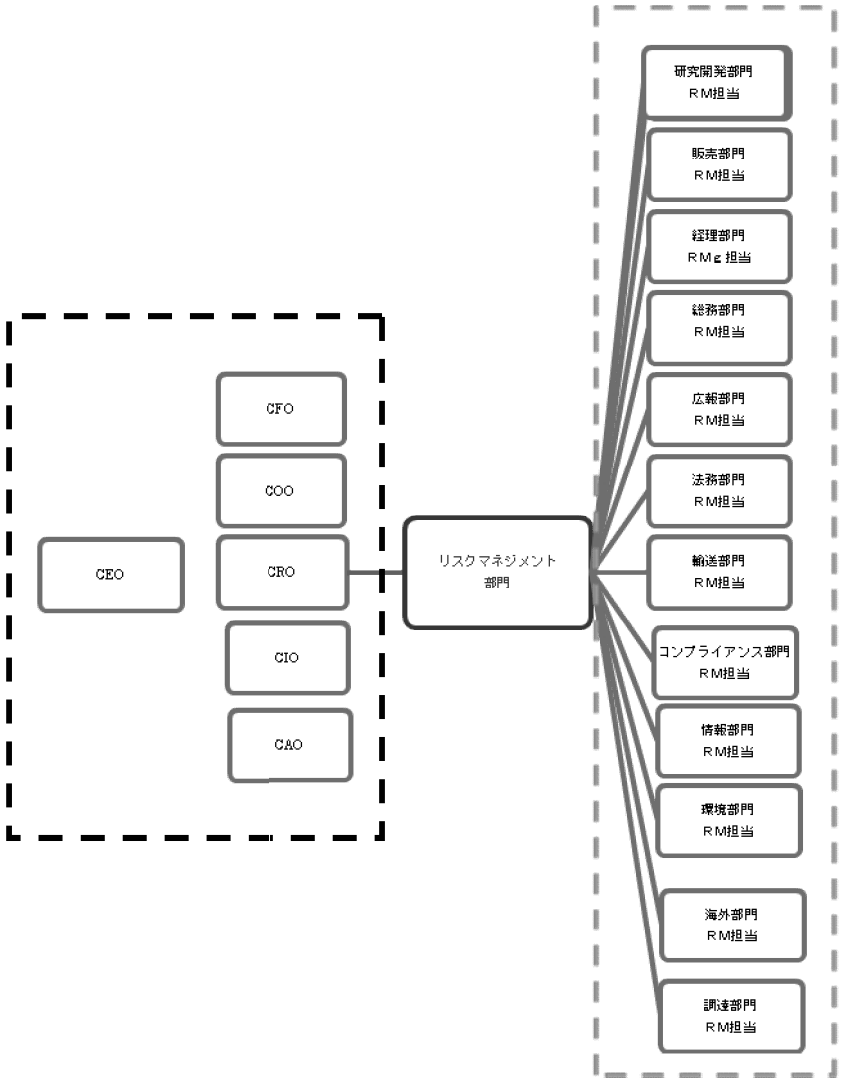


図 1-5-1. 組織の構成図（例示案）

現在は、従来と異なり業務ごとの縦割りによる役割分担では組織としての全体最適は達成しがたいため、各ユーザ部門を含め、企業をとりまくリスクにあわせ、リスク対応にも専門性が要求されている。JRMS2010 においてもリスクマネジメント担当執行役員（CRO）をリスクマネジメント組織のトップとして位置づけている。その CRO の下で、全社的リスクマネジメント組織が構成される。JRMS2010 では、組織におけるリスクマネジメント組織（後述の事務局）を中核として実施されることになる。

専任の CRO を設置しない組織であっても、全社的なリスクを統括する役割を担う執行役員を経営者層から任命することが必要であり、中小企業であれば CRO は社長が兼務することになるといえる。

JRMS2010 ではさらに個人情報保護、事業継続、環境、医療にも着目したことから、関連部門におけるリスク領域の責任を担う担当者（各ユーザ部門の長）が中心となり、回答者を選定し、回答結果の集計を担うことになる。それだけに、それぞれの部門のリスクマネジメントの責任者が誰であるかが明確になっている必要がある。

こうした視点から企業のリスクマネジメントに係る責任体制を示したのが、表 1-5-1 である。

表 1-5-1. JRMS2010 における回答部門とリスクマネジメントの責任体制

部　門	組　織
経営者層	最高経営責任者（CEO） 最高業務執行責任者（COO） リスクマネジメント担当執行役員（CRO） 情報システム執行役員（CIO） 経理担当執行役員（CAO）等執行役員
リスクマネジメント（RM）部門	リスクマネジメント担当者
ユーザ部門	各ユーザ部門リスクマネジメント責任者 情報システム等適用業務別責任者

現在の組織ではリスクマネジメント体制がかなり構築されていると考えられるが、現実的・実践的なリスクマネジメント体制が構築されていない場合はそれぞれの部門長がリスク分析およびリスク対策の責任者として考える必要があるため、部門長にその認識を確認しておく必要がある。

仮に、現段階において全社的リスクマネジメント組織がない場合では、事業継続を困難とさせる万一の事件・事故が発生した場合、どの組織が対応を図るのか十分に検討し、リスク対応に関係する業務を統轄する部門を RM 部門と決めるところから始め、早急に組織内責任体制を構築する必要がある。

1.5.2　JRMS2010 担当事務局の選定

JRMS2010 では、組織全体のリスクを考慮し、リスク対応の実態を目標レベルと比較考量し、その評価結果をもとに組織としてのリスクマネジメントの最適化を図ることから、質問項目はか

なり多岐にわたっている。そのため、JRMS2010 の実施にあたり集計結果をとりまとめ、分析し、経営者に現状を提示するための「事務局」を選定しておくことが必要である。

組織全体のリスクマネジメントを考える場合、各部門のリスクマネジメント担当者から構成される委員会組織をもつことを含め、その推進母体として RM 部門を設置することを想定している。当該部門において、組織に影響を及ぼすリスクに対応することが求められ、全組織的な判断を行い、特定のリスクについては具体的な対策を立案・展開するため、専門性を有している CRO を長とするリスクマネジメント部門に責任と権限を委ねることが望ましいと考えている。

また、部門間の調整等のため、たとえば社長室などの部門が必要に応じてリスク対策状況の定期的な監視や部門間調整、アドバイス部門としての支援に回るのがよいと思われる。

事務局は、経営者層、RM 部門、ユーザ部門にそれぞれ質問票を配付し、各部門の回答者の回答を得、さらに部門間のギャップ分析を踏まえた論議・意見等を集約し、これら 3 つの部門の見解をさらに相互に比較・分析・検討することにより、組織全体のリスク対応の実態を把握することが可能になるのである。また、必要に応じて部門内の回答者間でリスクマネジメントの認識の共有が図れるよう、教育・訓練を行う仕組みの構築の必要性を判断することも、事務局の業務の 1 つといえよう。

図 1-5-2 は、JRMS2010 が ICT 社会の現状に鑑みて、情報関係の質問項目を多く用意しているとともに、他部門でも業務上情報システム・情報セキュリティ関連組織との連携を不可欠にしていることから、CIO の下にある情報システムリスクマネジメント組織との関連性を示した体制図である。

なお、非営利組織、たとえば医療機関の場合、上記と責任体制が異なる場合が一般的といえる。病院においては、CEO を院長として、そのもとでリスクマネジメント組織が構成されている。JRMS2010 の実施にあたっては、回答結果の集計・評価レベル分析・ギャップ分析の結果によっては、改善のための教育体制までを含めた組織構成を整備しておくことが望まれる。

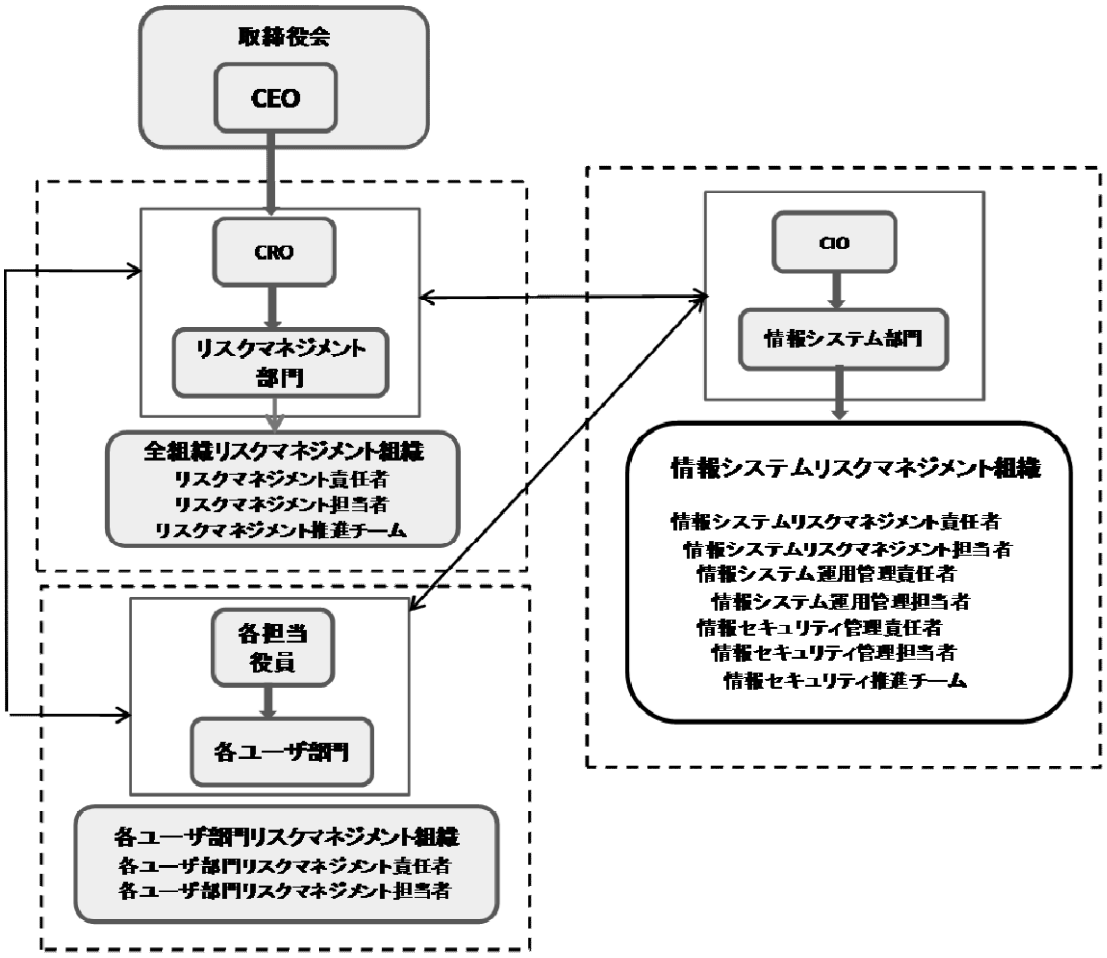


図 1-5-2. リスクマネジメント体制図

ここで JRMS2010 実施にあたっての全体的な流れを簡潔に示しておく。

①リスクマネジメントの実施対象領域について、経営者層を交えて組織内で決定する。(対象領域については、2 章「2.1.2　JRMS の対象領域」を参照)

②経営理念の実行をたしかなものとするため、JRMS2010 の実施を組織として決める。すなわち、中心となる「事務局」を経営者層の承認のもとに組織化する。

③部門内において回答者を選出する。たとえば大規模組織の場合、部門内にいくつかの○○部とその中に□□課があれば、それぞれについてリスクマネジメントの実態を把握するのか、○○部として対象とするのか（マンアワーの考慮)、事務局を交えて決定する。

④回答者決定後、リスクマネジメントの実態を把握するため、使用する質問項目を選択する。

⑤回答者は事務局より指定された質問項目について、JRMS ツールを利用して回答する。

⑥リスクマネジメント部門の分析者は、JRMS ツールを利用して、回答者の回答結果の集計、およびレーダーチャートを作成する。

⑦分析者は、⑥で作成したレーダーチャートおよび回答結果をもとに、組織の脆弱性と設定した目標レベルとのギャップの所在を分析・評価する。

⑧分析者は組織のリスクマネジメントの実態を経営者層に報告する。
⑨経営者層は、提出された分析・評価結果をもとに是正・改善の方策をリスクマネジメント部門と共に構築し、最高経営者のリスクマネジメントレビューを受ける。
⑩必要に応じ、組織としてのリスクマネジメントを改善する。
⑪これまでのプロセスを必要に応じて（定期的・非定期的に）繰り返し、リスクマネジメント体制の維持に努める。

これまで示した内容は、参考としての流れである。実際には、JRMS2010 の使い方は組織のニーズによることになる。

２．JRMS の質問構成

2.1　JRMS2010 の質問構成の特徴

JRMS2010 の質問構成にはいくつかの特徴がある。現代社会において組織にとって重視すべきリスクマネジメントの実践的な適用を考慮し、全体を 2 部構成としている。【1.組織経営編】は、組織における要となる「経営」をベースにおいている。さらに近年、種々の組織において発生した不祥事への対応を考慮し、「内部統制」を加味している。

【2.個別リスク対応編】では、情報社会に鑑みて「情報システム」、「情報セキュリティ」を取り上げ、さらに現在の組織運営にとって不可欠とされる領域に踏み込み、「個人情報保護」、「事業継続」、「環境」、「医療」にメスを入れることにした。

またそれぞれの質問に関しては、その位置づけが理解しやすいように 5 段階に階層構造化している。特に、回答する質問は第 4 および第 5 階層に設定されている。

JRMS2010 の重要な点は、組織をとりまくリスクを洗い出し、対応を検討するための質問項目にあるといえる。

2.1.1　質問項目の構成と階層構造化

JRMS2010 の質問票のタイトルは階層構造化され、質問構成は 5 つの階層からなっている。階層構造化とは、質問に係る表示の仕方を表わしたものであり、第 1 階層の章（対象領域）に始まり、第 2 階層は節（評価項目）の位置づけになっている。具体的な質問項目（評価項目）は第 3 階層で明示されている。実際に回答する質問は第 4 階層および第 5 階層である。たとえば、【1.1 経営】は「リスクマネジメントフレームワークの構築」から「リスクマネジメントシステムの維持」までの 5 つのタイトル軸（節に相当）で構成されている。

ここで第 1 階層の対象領域である「経営」の一部分を参考のために図 2-1-1 に示すと、第 2 階層は「リスクマネジメントフレームワークの構築」、「リスクマネジメントの基盤」、「リスクアセスメント」からなる。「リスクマネジメントフレームワークの構築」については、第 3 階層で「組織の経営理念と経営目標の明示」という評価項目として示している。

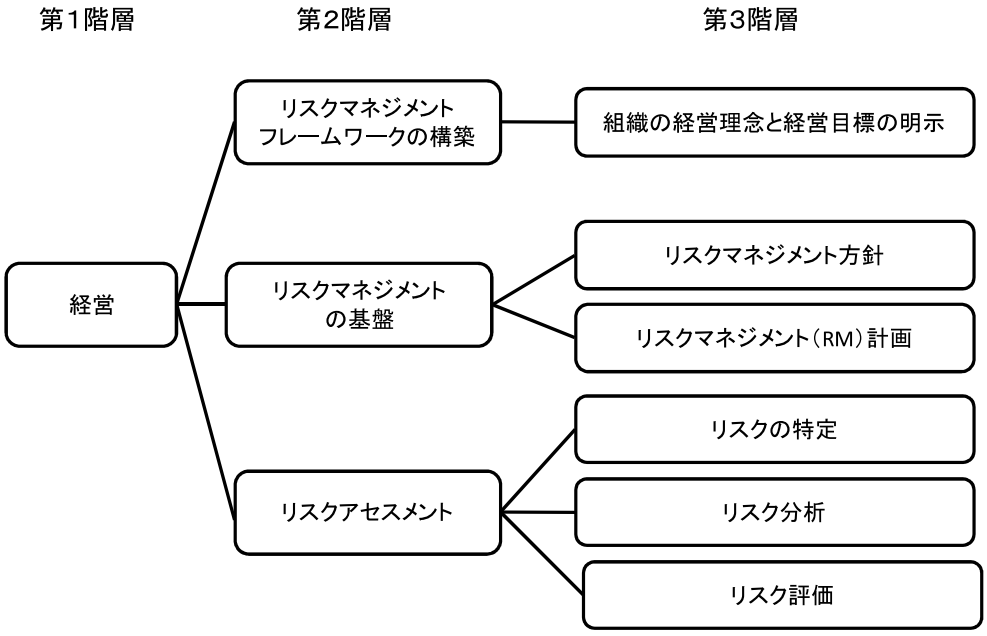


図 2-1-1. JRMS2010 の質問票のタイトル構成

（【1.組織経営編　1.1　経営】の第 1 階層から第 3 階層の例示）

第 3 階層および第 4 階層の質問に対する回答結果は視覚に訴える意図からレーダーチャート（表示の実態は後掲）で表示されるが、その際、第 4 階層の評価項目（キーワード）が評価軸となる。したがって、上位階層の評価項目であるタイトルがレーダーチャートの評価軸のタイトルになる。ちなみに、既述のように【1.組織経営編】は 5 つの評価軸により「経営」の組織の現状を示すわけである。この点については「図 2-1-1. 質問票のタイトル構成」、さらには本文 4 章「4. JRMS 分析例」における図から読み取っていただきたい。

さて、第 3 階層に位置づけられる「組織の経営理念の経営目標の明示」は 3 つの第 4 階層の質問項目からなっている。

質問項目について重視すべき点は、回答は第 4 階層および第 5 階層の質問に対して行うが、第 4 階層の質問への回答は本文 1 章「1.4.2　JRMS2010 における評価の仕方」に示す「成熟度の評価レベル（以下、「評価レベル」という。）」に従って行われることである。この評価レベルは回答者それぞれの判定基準となり、第 4 階層の回答結果をもとに上位階層別の評価結果が JRMS2010 ツールにより自動的にレーダーチャートで表示されるのである。

なお、JRMS2010 では「経営」、「情報システム」、「個人情報保護」および「環境」については第 5 階層の質問項目が設定されている。この第 5 階層は第 4 階層を評価するための評価項目の役割とされており、Yes か No で回答する。この点の詳細は、本文 3 章「3. JRMS ツール」で理解を深めてもらいたい。また、同じ専管部門においても回答者のキャリア等の違い等により知らないこともあるので「D/K」を用意し、さらには回答者にとっては適応外ということもあるため、「N/A」で評価するという工夫もされている。第 5 階層の質問を有する場合、これらの質問をまず評価し、この状況を踏まえて第 4 階層を評価レベル 0～5 で評価し、その結果が集計される。

以上のように構成された質問項目への回答を入力し、その結果を分析・評価するため、自動的にレーダーチャートに表示するソフトウェアが JRMS2010 には装備されている。

それぞれ第 3 階層を構成する第 4 階層・第 5 階層には質問項目が示され、回答者はそれらの質問に対し回答することになる。JRMS2010 において重要なのは、それぞれの回答者がみずからの質問への理解や認識に基づいて回答した回答結果である。

たとえば、業務実態に鑑みた自らの判断について、同じ業務部門の回答者 A、B、C の 3 名のうち、A である自分が低い評価（たとえば評価レベル 1）[18]を出したとする。しかし他の 2 人が組織としてある程度評価できるレベル（たとえば評価レベル 3）の回答であった場合を考えてみる。この場合、当該業務部門の評価は後述のレーダーチャートでは平均値で示されるが、回答者の間で、なぜ回答の評価に差異が生じたかを分析すると、A の回答の低さの原因が、組織としての方針を理解していなかったという A 自身の責任によるのか、それとも組織として当該業務部門全員にしっかりとしたコミュニケーションを行っていなかったためなのか、たまたまその折に業務の都合で外出していたのか等、いろいろなケースが考えられる。

しかし、この場合、A としては評価の違いが自分 1 人であったということから、みずから改善の努力を行い、部門の成熟度を高めることが可能になる。JRMS にはこうした仕組みが特徴の 1 つとして組み込まれているのである。JRMS では、質問に関する理解不足などで誤解が起きないように、質問についての解説文が表示され[19]、回答者間において質問についての認識の共有化ができるだけ図れるように工夫されている。

2.1.2　JRMS の対象領域

JRMS の価値は質問項目そのものにある。組織をとりまく経営環境は常に変化しており、そうした変化への対応を生かしうるのは質問項目であり、絶えず現実を直視しながら改訂することが求められる。2 編構成となっている JRMS2010 における質問と対象領域、質問数の関係は表 2-1-1 のとおりである。

18　ちなみに、評価レベルの構成は「0」から「5」である。

19　後述の「3 章　JRMS ツール」で解説されている。回答画面に解説文が表示されている。

表 2-1-1. JRMS2010 の質問構成

編	対象領域		質問数
1.組織経営	1	経営	36
	2	内部統制	27
2.個別リスク対応編	1	情報システム	124
	2	情報セキュリティ	60
	3	個人情報保護	74
	4	事業継続	58
	5	環境	156
	6	医療	41

【1.組織経営編】は JRMS2010 の質問構成におけるベースとなる「経営」と「内部統制」で構成されている。ここでは、組織の実態を把握するため、経営の根幹に係る内容をチェックし、さらに、昨今の企業不祥事により法的にも求められている内部統制関連の項目および金融商品取引法にかかる J-SOX 関連項目を加味した構成となっている。

【2.個別リスク対応編】は種々の業種ならびに業態において JRMS2010 の考え方を実践することにより、リスクマネジメントを展開できるように、「情報システム」、「情報セキュリティ」、「個人情報保護」、「事業継続」、「環境」、「医療」という 6 つの領域から構成されている。【2.個別リスク対応編】は、【1.組織経営編】における「経営」関連リスクを共有するものとして理解し、各領域における個別リスクへの対応の連携を重視したものとなっている。

ところで、ICT 社会において個人情報を含む情報関連のリスク領域の存在には違和感がないかもしれない。また、「環境」関連は、エコ重視の現在、業種を問わずリスクマネジメントの視点からのアプローチの重要性は理解できると思われる。

しかしながら「医療」については医療機関を対象にした領域と思われるが、医療分野は関連する業種が広い公的サービス産業の 1 つである。たとえば、情報システムの活用が進んでいることから、情報セキュリティ、個人情報保護が重要な課題となる。また、医療廃棄物関連では環境と密接な関係がある。その上、一般の組織と同じく、パンデミックのインパクトが組織を直撃すれば、場合によっては組織の存続すら危ぶまれる以上、「事業継続」とのかかわりも不可欠となってくる。

さらに【2.個別リスク対応編】の「情報システム」、「情報セキュリティ」に関しては重視すべき項目を配置した。「個人情報保護」ではプライバシーマーク対応を意図し、医療においては厚生労働省におけるガイドライン等を勘案した項目となっている。

2.2 【1. 組織経営編】

JRMS2010 の【1.組織経営編】は、2 つの領域から構成されている。第 1 点目として、基本的な視点として組織の経営にベースにおくことにした。組織の特定部門・部署にかかわるリスクに注目し、その好ましくない結果を低減させる対策を実施してもその対策が他の部門・部署のリス

クが組織全体に影響を及ぼし、ひいては組織の存続に赤信号を灯すことになるかもしれない。それゆえ、組織としてまず組織全般の実態がどうなのかを全社経営の視点で見つめなおすことから始めるように工夫されている。

第 2 点目として、社会的な要請を受け、コーポレートガバナンスおよび法令遵守を重視するため、統制環境に着目して内部統制の視点からリスクを見ることにした。この点は、会社法および金融商品取引法を考慮して質問項目を設定している。

2.2.1 【1.1 経営】

組織全体を視野に入れた JRMS2010 の「経営」の領域では、経営に関するリスクマネジメントの評価項目に基づいてリスクマネジメントを展開することになる。

「経営」の評価項目と質問項目数は次のとおりである。

評価項目(第 2 階層)	評価項目(第 3 階層)	第 4 階層 項目数	第 5 階層 項目数
(1)リスクマネジメントフレームワークの構築	①組織の経営理念と経営目標の明示	3	0
(2)リスクマネジメントの基盤	①リスクマネジメント方針	6	0
	②リスクマネジメント(RM)計画		
(3)リスクアセスメント	①リスクの特定	8	1
	②リスク分析		
	③リスク評価		
(4)組織のリスク対策	①リスク対策の選定	6	0
	②リスク対策の実行		
(5)リスクマネジメントシステムの維持	①リスクマネジメントシステムの実行	12	0
	②リスクマネジメントシステムのチェック		
	③リスクマネジメントシステムの改善		
	④リスクマネジメントレビューの実施		
計		35	1

各質問項目の要点を以下に説明する。

(1) リスクマネジメントフレームワークの構築

この質問項目は、経営全体のリスクマネジメントを実施する際にその前提となる経営理念の理解や社内風土の構築の状況について分析・評価するものである。

経営においては経営理念、経営目的・目標、施策が連携していて、そのことが全従業員に理解されていることが必要である。

リスクを検討することはその目的や目標の達成に影響を与える可能性を検討することである。したがって、リスクを特定して対応を行うためにも、その前提となる経営理念や経営目的の、組織における共有状況を確認しておくことは重要である。経営目的は組織の状況においてすべてを同時に達成することが難しい場合もあり、その際、目的の優先順位を定めておくことが、無理な

活動により組織にとって好ましくない状況の発生を防ぐために有効である。

（2）リスクマネジメントの基盤

この質問項目は、リスクマネジメントを実施する際に主として経営者層が準備すべきことを尋ねている。

リスクマネジメント方針に経営理念を反映しておくことは、経営目的の達成に影響を与える要因をリスクとして認定し、運営管理を行う仕組みの基本である。

また、リスクマネジメント方針は設定しているだけでは十分ではなく、その理解が組織内で徹底されていることが重要である。組織内においてリスクマネジメントを実施することの必要性を従業員に徹底させることも必要である。

この質問により、リスクマネジメント基盤の状況とその構築を行っている経営者層と事業部等の認識の差異を評価することにより、リスクマネジメントにおける組織体制の十分性を評価することができる。

（3）リスクアセスメント

この質問項目は、リスクマネジメントにおける意思決定を支援する情報を検討する重要なプロセスである。このステップにはリスク特定、分析、評価が含まれるが、この業務を形式的にではなく、有効な活動とするためには、その活動の重要性を認識し、活動の有効性を確保しているかを常に確認する必要がある。そして、リスク評価においては現場にまかせることなく、経営者層が関与することが重要である。

この質問によりリスクアセスメント自体のレベルを評価するとともに、リスクアセスメントに関して経営者層が関心を持ち、リスクアセスメントの有効性を確保しているかを検証することができる。

（4）組織のリスク対策

リスク対応は、認定したリスクに対して形式的に低減対策を決定することではない。リスクの重要性にあわせて、保有やリスクの起こりやすさ等を変化させる等の対策の中から適切な対策方針を選定し、決定することが重要である。そのためには、候補となる対策をきちんと理解しておくことが望ましい。

リスク対策の選定には、費用対効果や技術的実現性の検討が必要である。

そして、対策を実施することにより、リスクが対策によって目的を達成された状況になっているかを検証することが重要であり、その効果が十分でない場合には、追加の対策を行うなどの施策が必要となる。

リスクマネジメントは、概してリスクアセスメントには注力するが、対策の段階で形骸化する場合が見受けられるので、注意が必要である。

この質問項目に対する評価を分析することにより、その組織におけるリスクマネジメントの有効性を検証することができる。

(5) リスクマネジメントシステムの維持

この質問項目は、組織においてリスクマネジメントをマネジメントシステムとして実施する際の体制等に関する事項をまとめたものである。

リスクマネジメントはタスクフォースとしてある時期に実施すればよいものではなく、継続的に実施することが肝要である。そのためには、リスクマネジメントをマネジメントシステムとして実施することが求められる。

リスクマネジメントシステムでは、まずその責任の所在を明らかにすることが必要である。

そして、マネジメントシステムは、その活動の成果や有効性を検証することが必要であり、そのためには、適切な評価を実施することが重要となる。また、その評価に基づいてマネジメントシステム改善の仕組みを確立しておくことが求められる。

2.2.2 【1.2 内部統制】

内部統制とは、Internal control の訳であり、組織を適切にコントロールおよびマネジメントするために、企業内・組織内に用意する自律的な仕組みを指す。経営者にとって統制という言葉には強い締付感があるが、野球のピッチャーのコントロールを思い浮かべてもわかるように、本来のコントロールは狙ったところにもっていくというニュアンスがある。大きなミスや事件を犯すことがなく、有効かつ効率的に収益をあげて経営していくための経営の仕組みと考えるとわかりやすい。

日本の企業経営への内部統制の導入は、会社法と金融商品取引法の 2 つによるところが大きい。2005 年に成立し、2006 年 5 月に施行された会社法の中には内部統制という言葉はないが、第 348 条、362 条、416 条において「業務の適性を確保するために必要な体制の整備」が求められており、具体的な内容は「会社法施行規則－2006 年 2 月 7 日法務省令第 12 号の第 98 条・第 100 条・第 112 条」において定められている。

また、2006 年には金融商品取引法が成立し、上場企業等対象となる会社に対し 2009 年 3 月期の決算から内部統制報告書の提出が義務づけられた。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が 2007 年 2 月に金融庁企業会計審議会から「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の設定について（意見書)」として公表された。意見書は財務報告を主な対象としているが、内部統制は財務報告のみならず経営の効率性、コンプライアンス、資産の保全などの企業経営にかかわるすべての目的を対象としている。

そのため、JRMS2010 ではこの評価項目を参考としたうえで、経営すべてを対象として内部統制を実施する際の項目を検討し、7 項目に整理した。

企業会計審議会の公表した要素との違いは、JRMS ではリスクの把握を重要視しているため、リスクの評価と対応の前にリスク分析の構築の項目を独立して設定した点にある。なお、企業会計審議会の提供する評価要素そのものは参考にしている。

「内部統制」に関するリスクマネジメントの評価項目と質問項目数は次のとおりである。

評価項目(第 2 階層)	評価項目(第 3 階層)	第 4 階層 項目数	第 5 階層 項目数
(1)統制環境	①経営	3	0
	②経営組織		
	③経営実務		
(2)リスク分析の構築	①リスク分析の仕組み	7	0
	②リスク分析の体制		
	③リスク分析の実施		
(3)リスクの評価と対応	①リスク評価の仕組み	3	0
	②リスク状況の把握		
	③リスク対応		
(4)統制活動	①統制活動全般	3	0
	②職務分掌		
	③統制業務		
(5)情報と伝達	①情報共有と伝達に係る活動	4	0
	②重要情報の共有		
	③伝達経路		
(6)モニタリング	①モニタリングの調整活動	3	0
	②是正活動		
	③モニタリング情報の共有		
(7)IT への対応	①IT による統制活動	4	0
	②IT 全社的統制		
	③IT リスク		
計		27	0

各質問項目の要点を以下に説明する。

(1) 統制環境

統制環境は組織の気風を決定し、組織内のすべての者の統制に対する意識に影響を与えるとともに、他の基本的要素の基礎となす最も重要な要素である。経営者層の意識が本物であるか、予算などの経営資源を十分に投入しているか、人材育成を図っているかなどの経営にかかわる重要な項目を評価する。

ここでは統制環境を経営そのもの、経営組織、経営実務の 3 つに整理している。いずれも経営者自身が取り組むべき重要課題であり、内部統制の基本方針の設定や効率的な経営、法令遵守、不正発見の仕組みなどの整備や、コーポレートガバナンスである取締役による監視や監督責任、監査人との連携、組織内の各部門の役割分担、人材の確保と配置などの経営にかかわる重要項目を質問として掲げている。また、一般に組織は財務諸表等で評価されることから、財務報告の適切性に関する質問も含めている。

(2) リスク分析の構築

組織の目標達成に影響を与えるリスクを発見・特定し、識別することが大切である。リスクの発見ができなければ、その後の対応を検討する余地もない。そのため、リスク分析を実施するた

めの体制を作り上げることが必要である。担当者の個人のスキルによらない組織立ったリスクを発見し、適切に評価する仕組みを構築し実践することが求められる。

ここではリスク分析の仕組み、リスク分析の体制、リスクの算出の 3 つに整理している。リスク分析をリスクマネジメント計画上明確にすることからはじめて、問題意識の認識、情報提供、対象の明確化などの仕組みづくり、予算やスタッフの充実、優先順位づけ、内外の環境の変化の動きをとらえる体制の整備、リスクの日常的な洗い出し、リスク評価基準の整備などの質問を整理している。

（3）リスク評価と対応

リスクを評価し、当該リスクへの適切な対応を行う一連のプロセスがここでの課題である。分析されたリスクの発生頻度と影響度を算定し、それらを総合評価して優先順位をつけ、リスクの大きさに応じた、いわば身の丈にあった適切な対応・対策を講じる段階である。

リスク評価は評価基準に照らして評価するだけではなく、コンプライアンスや効率性などの観点を含めて経営戦略の作成に役立つものである必要がある。また、リスクは常に変化するものであることから、変化が発生する頻度やリスクを再評価する仕組み、不備がある場合の対応など、実践的な運用体制の構築についても質問に組み込んでいる。

（4）統制活動

統制活動は、経営者の命令および指示が適切に実行されることを確保するために定める方針および手続きであり、日々の実践そのものである。統制活動は定められたリスク対策を適切に行うことであり、具体的には個々のリスクに対するハード・ソフト対策、組織編成、マニュアルの作成、教育・指導の実践などがある。

統制活動は日常の業務そのものであるが、業務によっては収益に直結しない後向きの仕事ととらえられかねないため、実践にあたっての内部統制の重要性の認識、経営資源の確保、具体的には内部統制要員の確保、内部統制を実施するための時間の確保、内部統制の教育の実施などを確認している。また、相互牽制や業務プロセス管理者の説明責任、業務手順の明確化、統制活動そのものの実施の確認、そして統制活動の不備を把握する仕組みづくりとその改善など、実務レベルの確認点を質問に組み込んでおり、内部統制を業務の中に組み込んでいく必要性が認識できる質問となっている。

（5）情報と伝達

必要な情報が識別、把握および処理され、組織内外および関係者相互に正しく伝えられることが重要である。風通しのよい組織であり、よい情報および悪い情報とも必要な情報が必要な者に、必要な時に行き渡ることが求められる。

企業経営においては、経営者の戦略や意思決定が速やかに従業員など関係者に共有され、それに基づいた活動が行われることが望ましい。そのため経営者の方針や指針の伝達ができる体制の構築や、売上げや利益などの財務情報の利用、会社情報について経営者、取締役会、監査役・監査委員会など重要機関において共有されていること、内部通報などの伝達経路の整備、そして組

織外部から内部統制に関する情報を入手する体制などの構築について質問している。経営にあたっては情報の欠落が誤った判断を下すおそれがあるため、よい情報および悪い情報それぞれが適切にかつ遅滞なく、必要とされる関係者で共有されることが必要である。

（6）モニタリング

モニタリングは、内部統制の有効性を組織的に評価するプロセスであり、点検や監査およびそれらの結果に基づく是正である。一般的に日本の組織ではモニタリングの取組みが不足していると指摘されていることもあり、重要な評価項目である。

モニタリングは独立性が重要であり、その独立的評価の範囲と頻度をリスクや内部統制の重要度に応じて調整することを経営者は求めている。留意点は、モニタリングが重要であるからといってむやみに経営資源を投じることを求めていないことであり、業務への影響を最小限にし、リスクの大きなところを重点的に行うなど、モニタリングそのものも効率的に実施することが必要である。一方では経営環境が厳しいなどの理由をもって内部統制項目を省略してはならない点もあり、まさに経営者の資質が問われるものである。情報と伝達と同様に内部統制に係る重大な欠陥などの情報は経営者、取締役会、監査役・監査委員会等、重要な機関に遅滞なく伝達される必要がある。

（7）IT への対応

IT への対応とは、組織目標を達成するためにあらかじめ適切な方針および手続きを定め、それを踏まえて業務の実施において、組織内外の IT に対し適切に対応することである。IT への対応はアメリカで検討された内部統制「COSO」の中では明示されてない日本独自のものである。IT を適切に活用することで組織の活動をより強いものにすべきという意図がある。

IT による統制活動では、組織経営においていかに IT を活用するかについて経営者の戦略、計画を求めている。また IT を活用することによって利便性が得られるとともに、新たにリスクが生じることを認識することも重要視している。IT に対する全社的統制では、IT に関する組織的な計画や IT 関連教育、IT に関するリスク評価およびそのリスクに関する全社的な情報共有を行う仕組みについて質問している。

2.3 【2. 個別リスク対応編】

【2.個別リスク対応編】は、「情報システム」、「情報セキュリティ」、「個人情報保護」、「事業継続」、「環境」、「医療」という 6 つのリスク領域から構成されている。これらは、現代の経営環境下において、組織の経営に係るリスクの面から対応することが求められる不可欠な領域である。それゆえ、【1.組織経営編】の「経営」、「内部統制」についての質問と連動させてリスク対応に取り組むのが望ましいといえる。

なお、医療については専門性の点から他の組織およびリスク領域と責任体制において異なるという理解もあるが、組織の安全確保における医療面の影響（健康管理や安全衛生などの日常業務、

パンデミックのような事態）に鑑みて、医療機関における経営の視点からのリスクへの対応は重要であり、また、他の組織においてもその取組みが、自組織に及ぼす影響を認識する必要があると思われる。

2.3.1 【2.1 情報システム】

情報システムは、ビジネスプロセスを実現するために用いられる。そのため、ビジネスでのリスクについては、ビジネスプロセスを変えない限り情報システムのリスクとして残る。そのため、情報システムの導入にあたっては、ビジネスプロセスでのリスクを持ち込まないように、ビジネスプロセスの見直しが必要である。一方、情報システムの導入により新しく発生するリスクもある。情報システムの導入に伴って、たとえば、個人情報を一元化して管理することから、情報漏えいが起きるとその規模が莫大なものとなる。これは、データベースを導入して、顧客管理を自動化するために導入した情報システムが持つ新しいリスクである。

したがって、組織のリスクマネジメントを考えていく際、情報システムを導入することでどのようなリスクがあるのか、ビジネスプロセスのまま持ち込まれるリスクとあわせて分析することで、情報システムにかかわるリスクを低減することができる。

また、多くの組織において、情報システムの導入による自動化や効率化は避けて通れない段階となっており、この中で、IT ガバナンスの視点が重要になっている。すなわち、情報システムが企業の経営に与える価値の最適化、コスト管理、戦略、資源割当などを総合的に行うことが求められており、この視点からリスクを総合的に分析できるようにツールを編成した。

なお、JRMS2003 では、情報システムと情報セキュリティが分けられていなかったが、JRMS2010 では、この 2 つのリスクが必ずしも重ならない部分があることなどから、それぞれを個別のリスク領域としてとらえている。

情報システムに関するリスクマネジメントの評価項目と質問項目数は、次のとおりである。

評価項目(第 2 階層)	評価項目(第 3 階層)	第 4 階層 項目数	第 5 階層 項目数
(1)状況特定	①情報システムの外部環境	14	0
	②情報システムの内部状況		
	③IT ガバナンス		
	④情報システムを運用する組織・能力		
(2)情報システムのリスク特定	①経営目標との関係	13	2
	②適用業務の責任・権限に関するリスク認識		
	③経営目標への阻害要因		
	④システムの阻害要因		
(3)情報システムのリスク分析	①リスク分析技法とリスク情報の収集	17	3
	②プロジェクトリスク分析		
	③開発に関するリスク分析		
	④導入に関するリスク分析		
	⑤アウトソーサのリスク分析		
	⑥運用に関するリスク分析		
(4)情報システムが受けるリスク評価	①災害の影響の評価	13	1
	②事故の影響の評価		
	③人的災害の影響の評価		
	④障害の影響		
(5)情報システムが受けるリスク対策	①IT ガバナンス対策	26	15
	②情報システム組織のリスク対策		
	③開発に関するリスク対策		
	④運用テストにおけるリスク対策		
	⑤本番環境のリスク対策		
	⑥システム運用におけるリスク対策		
	⑦アウトソーサのリスク対策		
	⑧総合リスク対策の実施		
(6)モニタリングとレビュー	①リスクマネジメントの評価指標	9	0
	②評価指標の測定		
	③評価指標の報告		
(7)リスクコミュニケーションと協議	①ステークホルダの識別	11	0
	②ステークホルダへのコミュニケーション		
	③ステークホルダからのフィードバック		
計		103	21

各質問項目の要点を以下に説明する。

(1) 状況特定

ここでは、情報システムのリスクマネジメントを実施する際にその前提となる経営環境、情報システムへの投資などの IT ガバナンスや組織の内部環境、情報システムの運用状況などについて評価する。

リスクは組織の環境の変化により変化する可能性がある。そのため、組織内外の環境、経営をめぐる状況を把握することが重要である。

（2）情報システムのリスク特定

情報システムのリスクマネジメントが有効に実施されるためには、情報システムのリスクが経営のリスクとどのようにつながっているかを理解すること、すなわち経営目標との関係および情報システムのダウンやサービス低下が経営に与える影響や関係を明確にする必要がある。そして、具体的に経営目標への阻害要因が何か、また、情報システムの廃棄による情報漏えいや環境への影響、盗難による個人情報などの漏えい、物理的侵入、物理的攻撃などによる情報システムの運用停止などの組織のリスクを特定して評価する必要がある。

（3）情報システムのリスク分析

ここでは、特定された情報システムのリスクがどのような原因によるものかを分析する。分析にあたり、どのような分析を行うのか、どのようなリスク情報を集めるかを明らかにする。次にリスクを 5 つの観点から分析していく。テーマとしては、プロジェクトリスク分析、開発に関するリスク分析、導入に関するリスク分析、アウトソーサのリスク分析、運用に関するリスク分析である。これらのリスクは、フェーズによって与える影響が異なることから分けて分析する。

ここでの質問は、それぞれのリスクについて経営的観点、実務の運用的観点から分析されるように構成されている。

（4）情報システムが受けるリスク評価

リスク評価では、リスク特定、リスク分析で明確になったリスクに対して、リスクが情報システムにどのような影響を与えるかを評価することになる。ここでは、特に情報システム停止の原因となる災害、事故、人的災害について、どのような影響があるかを評価する。さらに、情報システムへの障害についてもさまざまな原因が経験的にわかっているはずであり、これをベースに該当する項目が何かを理解しておくことが望ましい。

このようにして、事故や障害の情報システムへの影響がどの程度かについて評価を行う。

リスクマネジメントは、概して一般化して検討される傾向があるため、ともすれば障害などの問題を見逃すことがある。質問項目に対する評価により、組織におけるリスクマネジメントの有効性や網羅性を検証することができる。

（5）情報システムが受けるリスク対策

この質問項目には、情報システムのライフサイクル（情報システムの企画、開発、調達、導入、試験、移行、運用、廃棄の段階）におけるリスク対策が網羅されている。

リスクマネジメントは継続的に実施することが求められる。

リスク対応はリスク分析の結果に基づいて形式的に低減対策を採用することではない。リスクの重要性、実際に対応できるかの実現性にあわせて、保有からリスクの起こりやすさを変化させ、適切な対策方針を選定し、決定することが望ましい。

なお、情報システムへのリスク対策には、IT ガバナンス対策、情報システム組織のリスク対策、開発に関するリスク対策、運用テストにおけるリスク対策、本番環境のリスク対策、システム運

用におけるリスク対策、アウトソーサのリスク対策、総合リスク対策の実施があげられている。なお、重要なことはこれらのリスク対策がすべて要求されるのではなく、リスク評価を受けて自社に関係するリスクの高いものから対策を採ることである。

（6）モニタリングとレビュー

従来のリスクマネジメントは、前提とした状況の変化はあるのか、また、リスク対策後の残余リスクが予想したものとなっているのかについてレビューするモデルであった。今回、ISO31000では、さらにこのモデルをモニタリングとレビューに発展させている。モニタリングでは、リスクマネジメントの各プロセスについてモニタリングすることになっており、問題があった場合にはフィードバックを受けてリスクマネジメントシステムを適切に改善させること、さらには残余リスクをモニタリングすることで、リスクが増えてきた場合には、状況特定を行ってリスクマネジメントプロセスをやり直すことになる。なお、このプロセスを実行するためには、情報やデータに関する評価指標、新たなリスクの評価指標が重要となる。

（7）リスクコミュニケーションと協議

情報システムに関するリスクマネジメントシステムが活用されるには、そのシステムに関する情報が利害関係者の中で共有されていなければならない。

このためには、情報システムに関する企画、開発、運用の各段階でリスク情報が関係者からいつでも参照できるようになっている必要がある。

特に、情報システムに固有な情報である脆弱性の情報やインシデント情報が特に内部の利害関係者に共有されている必要がある。また、情報システムは顧客に直接サービスを提供したり、顧客の個人情報を管理したりする場合がある。このような場合には、顧客に対してリスク情報やその対策の方針（個人情報ポリシーや情報セキュリティポリシー）を公開することが望ましい。

2.3.2 【2.2 情報セキュリティ】

情報セキュリティは、情報の機密性、完全性および可用性を維持することとして一般的に定義されている。これに従えば、IT サービス継続は、主に可用性の維持に関係するものとして位置づけることができる。実際には、情報セキュリティと IT サービス継続とは、どちらかが他方を包含する関係というよりも相互に関係するものとして位置づけられる。そのため、経済産業省が定めている「情報セキュリティ管理基準」や JIS Q 27001 等の情報セキュリティに関する基準・規格等においても、事業継続計画（BCP）を関連要件の 1 つとしている。

2.3.2.1 情報セキュリティ、情報システム、事業継続の関係

情報セキュリティリスクと情報システムリスク、および事業継続リスクは関係が深いので、情報セキュリティリスクを中心に次のように整理した。

①情報システムは事業に必要な業務プロセスを広い範囲でサポートしているため、IT サービスの継続は事業継続の重要な要素である。そして、経済産業省の IT サービス継続ガイドラインでは、次のように両者の関係を整理している。

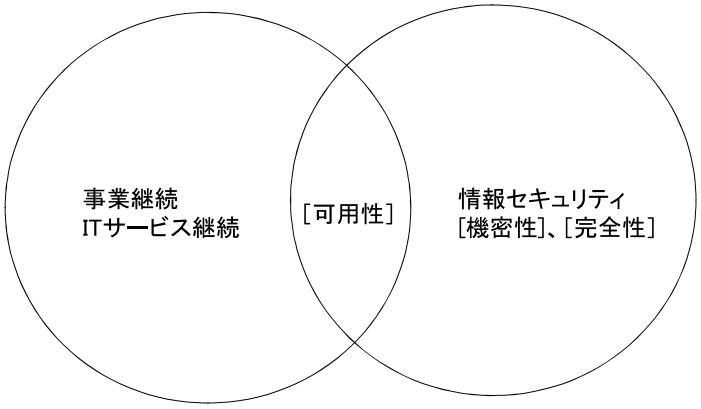


図 2-3-1. IT サービスと事業継続の関連要因
（参考　経済産業省　IT サービス継続ガイドライン）

②情報システムのリスクマネジメントではシステム開発や運用といった情報システムにかかわる業務そのものに内在するリスクの原因を対象とするのに対し、情報セキュリティのリスクマネジメントではコンピュータウイルスといった業務そのもの以外からのリスク原因を対象とする。したがって、情報システムのリスクの原因は、ヒューマンエラーや故障のように起こそうとして起こされたものではないのに対し、情報セキュリティの場合は外部から意図的にリスクを起こそうとするものになる。

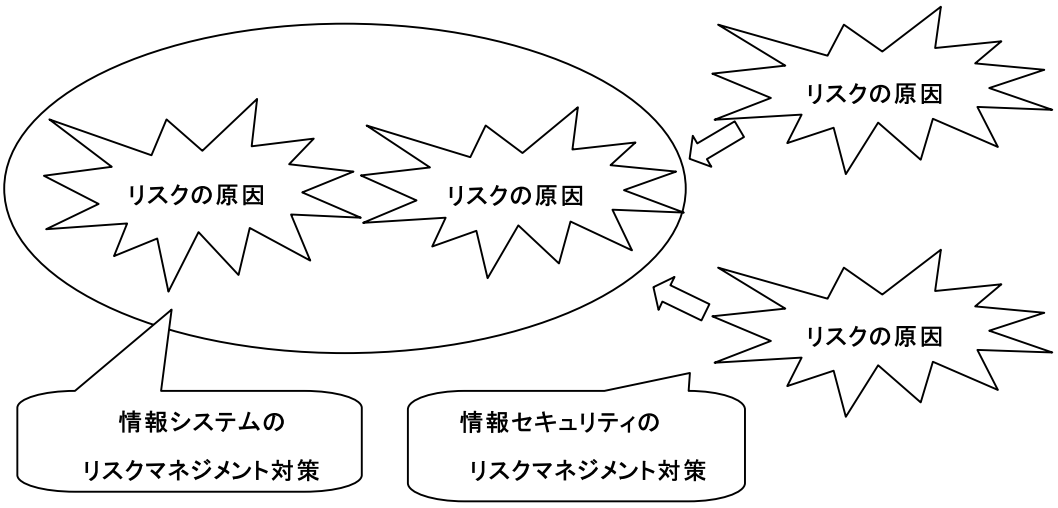


図 2-3-2. 情報システムに係る業務とリスクの原因

2.3.2.2　情報セキュリティリスクマネジメントにおけるトップダウンアプローチの必要性

これまでの日本企業の情報セキュリティに対する姿勢は、マスコミに取り上げられた大規模な個人情報漏えい事件といった個別のインシデントに対し、経営者が情報システム部門に対策を命ずるといった個別対策の積上げで行われてきた傾向があった。しかし、情報システムが企業活動のあらゆる領域に浸透し、さらに企業間のトランザクションにおいても使われるようになると、情報セキュリティインシデントによる IT サービスの停止や情報漏えいは企業活動の停止を意味するようになった。このような環境においては、発生したインシデントを起点とする後追いの対策では企業の社会的な責任を全うすることができなくなった。つまり、情報セキュリティリスクは経営的なリスクとなり、対策も全体的なトップダウンアプローチが必要になった。

情報セキュリティに関するリスクマネジメントの評価項目と質問項目数は次のとおりである。なお、「(1) 状況特定」～「(4) リスク評価」の詳細な項目は【1. 組織経営編　1.1 経営】の組織全体のリスクマネジメントにかかわる項目に委ね、ここでは情報セキュリティとしての第 2 階層の質問項目に絞っている。

評価項目(第 2 階層)	評価項目(第 3 階層)	第 4 階層 項目数	第 5 階層 項目数
(1)状況特定	①外部環境変化の把握	5	0
	②内部状況の把握		
	③情報セキュリティポリシー		
	④情報セキュリティ実施基準		
(2)リスク特定	①経営目標とリスクの関係	3	0
	②管理対象とするリスク		
	③包括的なリスクの把握		
(3)リスク分析	①リスク分析の手法	4	0
	②リスク分析の体制		
	③リスク分析結果の文書化		
(4)リスク評価	①リスク評価の手法	3	0
	②リスク評価の体制		
	③リスク評価結果の文書化		
(5)リスク対策	①包括的リスク対策	38	0
	②コンピュータ犯罪		
	③不正アクセス・不正利用		
	④コンピュータウイルス		
	⑤電子商取引		
	⑥電子メール		
	⑦災害		
(6)モニタリングとレビュー	①リスクマネジメントの総合的な評価指標	3	0
	②評価指標の測定		
	③情報セキュリティ監査		
(7)コミュニケーションと協議	①ステークホルダの識別	4	0
	②ステークホルダへのコミュニケーション		
	③ステークホルダからのフィードバック		
計		60	0

各質問項目の要点を以下に説明する。

（1）状況特定

状況特定の範囲としては大きく外部環境、内部の状況、組織の全体目標との関連がある。外部環境としては、たとえばパンデミックといった新しいリスクの原因が発生するので、まず組織としてそのリスク原因が出現しそうなことを認識する必要がある。外部環境でこの点を質問している。また、外部環境の範囲は二次的な影響も含めると広範囲になりすぎるので、一次的な影響に限定している。たとえば、不正アクセスの動機が金銭的なものになり脅威が増しているが、これは不正アクセスの脅威が増しているというレベルにとどめ､その原因についてはたどっていない。

リスクの原因がどのような悪影響を及ぼすかはその組織の準備状況により大きく異なる。内部の状況では、情報セキュリティにかかわる体制と対策についての網羅的な把握ができているかを評価している。

情報セキュリティに関する組織の全体目標は情報セキュリティポリシーとして管理されるべきであり、これについて評価している。

（2）リスク特定

リスクマネジメントの対象となるリスク原因は、見える化しないと適切なリスクマネジメントはできない。ここでは、組織としてマネジメントの対象とするリスク原因を明確にし、かつ外部環境の変化に追従できるように定期的に見直しているかを評価している。

（3）リスク分析

リスクが発生した場合に、業務に対しどのような阻害状況が発生するかを明らかにする評価項目である。これを確実に実施するためには、リスク分析の手法、分析の体制、文書化が重要であり、これについて評価している。

（4）リスク評価

業務に対して発生した阻害状況が、経営に対してどのような影響を与えるかを明らかにし、経営的な影響度を評価する項目である。このための業務影響度分析（BIA）を実施するには、リスク評価の手法、評価の体制、文書化が重要であり、これについて評価している。

（5）リスク対策

リスク対策では、最初に保有・軽減・移転・回避の 4 つの対応のどれを取るかを選択する。情報セキュリティについては、一般的に低減対策が取られるので、質問項目は低減対策について作成している。この分類軸には、IT に関するプロセス軸（企画・開発・運用・監視）と、特定のリスク原因による分類軸、対策の性質軸（技術、要員、仕組み）、対策により守られる資産軸がある。JRMS2010 では、この分類軸は、リスク原因軸－対策の性質軸－プロセス軸と構成しており、JRMS2003 の質問項目を再編成している。つまり、不正アクセスというリスク原因に対し、アクセス管理ソフトという対策とその運用、という構成になっている。

（6）モニタリングとレビュー

情報セキュリティの場合は、インシデントが起きないことが前提であり、たとえば、ウイルス感染の発生件数といった指標を取ることは、対策のレベルが低い場合は有効かもしれないが、ある程度の対策が実施された場合は、感染が非常に少なくなるのでモニタリングとしての難しさがある。これに対してはハインリッヒの法則を適用して、軽微なインシデントに基づいた評価指標をモニタリングすべきであり、組織として総合的な指標を定め、経営者に定期的に報告しているかを評価している。

（7）コミュニケーションと協議

コミュニケーションと協議の対象になるステークホルダは、情報セキュリティの場合、社内は経営者、外部は法律等の規制機関と消費者を含む取引先が対象となる。問題になるのは一般公衆や報道機関で、開示する情報が広すぎて情報セキュリティの低下にならないように注意する必要がある。そして、ステークホルダの識別、開示範囲、規制の状況と対応について評価している。

2.3.3 【2.3 個人情報保護】

組織では、個人を特定する個人特定情報は権利義務の主体を把握するため、また本人の属性を示す個人属性情報は、事業企画や市場動向を把握するためにいずれも不可欠な情報である。しかも、個人情報の収集から廃棄までの過程は、個人情報保護法、行政機関個人情報保護法、個人情報保護条例、独立行政法人個人情報保護法などのいわゆるハードローにとどまらず、各組織の事業戦略、コーポレートガバナンスや市場、顧客保護戦略との関係を反映した、ソフトローなど多様な規範への重層的なコンプライアンスが求められている。個人情報保護はコーポレートガバナンス、事業戦略、顧客保護、情報セキュリティとコンプライアンス経営の接点としての重要性を帯びており、これらの観点からの積極面・消極面双方のリスクマネジメントが必要となる。

そこで､ここでは個人情報に関するリスクを積極面､消極面双方からとらえることはもちろん、経営から現場までの各セクションが取り扱うすべての個人情報に関するリスクを､すべての業務、収集から廃棄までのライフサイクル全体、コンプライアンスすべきさまざまな規範（特に個人情報保護法と JIS Q 15001：2006）との関係で把握し、これに対する取組みを評価できるように配慮している。

個人情報保護に関するリスクマネジメントの評価項目と質問項目数は、次のとおりである。

評価項目（第 2 階層）	評価項目（第 3 階層）	第 4 階層 項目数	第 5 階層 項目数
(1)個人情報と経営	①個人情報の価値の把握	12	0
	②個人情報の経営への位置づけ		
	③個人情報の事業への位置づけ		
	④個人情報の利用と保護に関する組織の体制		
(2)個人情報にかかわる状況の特定	①外部状況の特定	6	0
	②内部状況の特定		
(3)リスク特定	①個人情報リスクに関するリスクマネジメントの概要	6	0
	②リスク特定の実践		
(4)リスク分析	①リスク分析体制	19	4
	②リスク分析の実施		
	③取得・利用目的		
	④第三者提供		
	⑤安全管理		
	⑥委託先のリスク分析		
	⑦本人関与・周知に係るリスク分析		
(5)リスク評価	①リスク評価のマネジメント	6	0
	②リスク評価の実施		
(6)リスク対策	①リスク対策	15	0
	②コンプライアンスの確保		
	③利用目的に関するリスク対策		
	④個人情報の安全対策に関するリスク対策		
	⑤本人への対応に関するリスク対策		
(7)モニタリングとレビュー	①モニタリングとレビューの実施	3	0
(8)コミュニケーションと協議	①ステークホルダの識別	3	0
計		70	4

各質問項目の要点を以下に説明する。

(1) 個人情報と経営

ここでは、組織が経営にとっての個人情報の価値を把握し、経営・業務に的確に位置づけ、適切に利用できる体制を整えているかを分析・評価する。

リスクとは、その目的や目標の達成に影響を与える可能性であるから、個人情報が経営にもたらすリスクを把握するには、個人情報の積極的・消極的価値が経営理念や目的の達成にどのように関係づけられているかを確認できなくてはならない。

本人を特定する個人特定情報は、権利・義務の主体・帰属点を示す情報として組織の活動を支え、本人の属性、活動履歴を示す個人属性情報は、組織の経営、業務の遂行に資するなど、積極的価値を有している反面、個人情報の収集から廃棄までのプロセスが個人情報保護法その他の規範によって規制される結果、組織は個人情報の取扱いに伴う負担を余儀なくされる。組織が個人情報を取り扱うにあたっては、このような個人情報の積極的・消極的価値を、組織の価値体系に適切に位置づけ、これを経営・業務の遂行に適切に位置づけることが求められる。

「①個人情報の価値の把握」は、こうした個人情報の積極的・消極的価値の把握と組織の価値

体系への位置づけが明確かを評価している。

「②個人情報の経営への位置づけ」、「③事業への位置づけ」は、個人情報の積極的・消極的価値を組織の経営理念、経営方針、経営目的、経営戦略に的確に位置づけて、組織の活動に役立てられる体制にあるか、個人情報の利用と保護の価値、事業への価値をリスクの視点から把握しているかを評価している。

（2）個人情報にかかわる状況の特定

ここでは、個人情報にかかわる組織外部、内部の状況の変化、規制違反の可能性を特定し把握できる体制が整っているかを評価する。

リスクは環境の変化により変化する可能性があるため、組織内外の環境の変化を知ることは、リスクを適切に把握するために重要なことである。そのためには、内外の環境を特定する仕組みの有無、有効性とそれを適用した外部状況の変化、内外部状況の特定がなされているかを評価する必要がある。

「①外部状況の特定」では、まず、外部状況の変化を把握する仕組みが構築され、有効に機能しているか、その仕組みが個人情報を利用したビジネスモデル、個人情報の利用技術、法令等の公的規制、取引先からの要請、権利行使、消費者保護の動向などの変化の把握に適用されているかを評価している。「②内部状況の特定」では、取扱者、権限と責任、業務、個人情報のライフサイクル、例外的利用方法の要件と手続きの特定の状況を評価している。

（3）リスク特定

ここでは、リスク特定の仕組みと実践について評価する。

対処すべきリスクに的確に対処するには、堅固なリスクマネジメント方針、緻密な計画を背景とするリスクマネジメントプロセスが必要である。「①個人情報リスクに関するリスクマネジメントの概要」の質問はその点を評価する。「②リスク特定の実践」では、この仕組みによる個人情報リスクの把握の実務が行われるための要素を評価している。

（4）リスク分析

ここでは、特定した個人情報リスクを分析する体制と方法を評価した後、その方法を用いて、個人情報の取得・利用目的、第三者提供、安全管理、外部委託、本人関与・周知など、個人情報の取扱いに係る積極的・消極的リスクの高いプロセスにおけるリスクを把握しているか否かを評価する。

質問は、すべての個人情報１つひとつについて、すべての取扱プロセス（業務フロー）を網羅し、個人情報のライフサイクル全般に及んでリスクを把握するものとなっており、プライバシーマークやISMSの構築、維持、認証取得、更新作業、審査実務に資することが意図されている。

（5）リスク評価

ここでは、リスクの経営上の意味を明らかにするための体制、具体的には、体制整備、評価基準、評価方法の有無と合理性・有効性を評価した後、それによるリスク評価の実施、その結果の

利用とリスク評価方法の点検、改善を評価する。

「①リスク評価のマネジメント」では、経営にとってのリスクの意味を明らかにする合理的で有効な仕組みを組織が備えているかを評価する。「②リスク評価の実施」の質問は、その仕組みの運用を評価するものである。

(6) リスク対策

ここでは、組織が適切なリスク対策を講じているかを評価する。

個人情報リスク対策の特性は、対策の対象である個人情報の収集から廃棄までのライフサイクルを持つことである。そのため、「①リスク対策」の質問は、リスク対策が個人情報のライフサイクル全般に及んでいるかを問うことから始まる。そして、組織、リソース、ルールがあるか、それらが個人情報の有効利用と安全対策に及んでいるか、不断に改善されているかを評価する。「②コンプライアンスの確保」は、個人情報の取扱いが個人情報保護法によって規制されることから、個々のリスク対策の評価の前にコンプライアンス経営体制のマネジメントサイクルの存在と運用を評価するものであり、これに続く「③利用目的」、「④安全対策」、「⑤本人対応」に関する質問は、個人情報保護法の構造に沿ったリスク対策の有無を評価するものである。

(7) モニタリングとレビュー

ここでは、個人情報リスクに関するモニタリングとレビューが適切に行われているかを評価する。

「①モニタリングとレビューの実施」は、適切に設定されたリスクマネジメントの評価の仕組みが運用され、その結果を活かすことに経営者層が責任をもって関与しているかを評価するものである。

(8) コミュニケーションと協議

ここでは、組織が組織の個人情報リスクについて、その影響を受けるステークホルダとのリスクコミュニケーションを適切に行い、個人情報リスクの分析、評価を通じて得られた成果をステークホルダとの取引、関係構築に活かす適切な仕組みを持ち、運用を行っているかを評価する。

「①ステークホルダの識別」は、組織の個人情報リスクに関するステークホルダをすべて把握し、これに対する影響、組織の責任を漏らさず把握しているかを評価するものである。

2.3.4 【2.4 事業継続】

日本における事業継続については、各省庁で事業継続に関するガイドラインが発行される等、その認知度は高くなりつつある。それは、製造業において地震等による事業の中断により全国の製造ラインがストップした等の事例が多く発生しているからである。最近では、パンデミックによる事業中断も懸念され、パンデミックに対するガイドラインも発行されている。また、海外に目を向ければ、各国の規格、ガイドラインなどがあり、ISO 22301 として規格化が進められてい

る状況である。世界的にみても事業継続に対する関心は高いといえる。

JRMS2010 では、組織の事業継続性を脅かすリスクに対するリスクマネジメントの観点から質問項目を整理した。

事業継続に関するリスクマネジメントの評価項目と質問項目数は、次のとおりである。

評価項目(第 2 階層)	評価項目(第 3 階層)	第 4 階層 項目数	第 5 階層 項目数
(1)状況特定	①事業系像の目的	18	0
	②主要な製品および／またはサービスの特定		
	③事業継続管理の方針		
	④経営資源の提供		
	⑤BCMS 従事者への教育および訓練		
(2)リスクアセスメント	①リスク特定:事業継続を脅かす要因の把握	12	0
	②リスク分析:業務中断による影響度の分析		
	③リスク分析:事業中断からの復旧目標		
	④リスク評価		
(3)リスク対策	①事業継続戦略の決定	12	0
	②緊急時対応計画		
	③事業継続計画(BCP)の策定		
	④事業継続計画(BCP)の管理		
(4)モニタリングとレビュー	①BCM の演習	7	0
	②マネジメントレビュー		
(5)コミュニケーションと協議	①事業継続管理方針の周知	9	0
	②事業継続に対する認識度向上		
	③継続的なステークホルダとの協議		
計		58	0

各質問項目の要点を以下に説明する。

(1) 状況特定

ここでは、事業継続上のリスクマネジメントを実施する際にその前提と組織の内外に関する環境の把握状況について評価する。

内部環境として、事業継続の必要性、組織が負う社会的責任や従業員に対する教育状況などがあげられる。外部環境として、ステークホルダの要求事項、地域特性(起こりうる自然災害等)や法規制等があげられ、場合によっては、地域住民との関係も重要となることがある。

事業継続に対するリスクは、組織をとりまく環境によって変化する可能性が大きく、そのためには組織内外の環境について、その状況を適切に把握することが重要となる。

(2) リスクアセスメント

ここでは、ISO31000 のリスク特定、リスク分析、リスク評価に沿った形で、組織の事業に対する理解度、また、事業中断による影響度の把握について評価する。

事業継続のリスクマネジメントを有効に実施していくために、組織の事業でどのような活動が行われ、どの経営資源(要員、資産、情報等)に支えられているかを把握することが重要である。

そして、それらの活動が中断したとき、組織にどの程度の影響があるかを明確にする必要がある。さらに、事業の中断時間がどの程度であれば受容できるかをステークホルダの要求事項等を戦略的に踏まえて評価し、どのくらいで復旧すればよいかを決めることが重要である。

（3）リスク対策

ここでは、前段のリスクアセスメントで分析した結果をもとに、どの程度対策ができているかを把握する。

事業の重要性、実際に対応できるのかの実現性にあわせて、組織の方針に従って適切な対策を決定することが望ましい。代替サイトの用意やバックアップの人員の配備等、重要な活動のどこに資源を投入するか、また、どの活動を優先的に継続していかなければならないか等を決めておく必要がある。

また、事業継続計画の整備も重要なポイントとなる。緊急時の連絡体制の整備状況、事業の復旧手順の用意や、緊急時におけるステークホルダとの連絡方法等、重要となる部分について質問している。

（4）モニタリングとレビュー

ここでは、組織における事業継続性を維持するための運用状況の把握について評価する。

組織における事業継続の能力の維持は重要なポイントとなり、事業継続計画の演習が大きな要因となる。事業継続計画の演習を定期的に実施し、どのようなシナリオを想定するかが重要である。また、組織が要求されている事項を踏まえた事業継続計画であるかを評価し、さらなる改善を行っていく必要がある。

内部監査による定期的な確認や、経営者の観点でみたマネジメントレビューも重要なポイントとなる。状況特定で明確になった組織内外の環境がどのように変化しているかを把握することが大事となる。

（5）コミュニケーションと協議

ここでは、主に組織内のコミュニケーションと外部とのコミュニケーションの 2 つの側面について評価する。

組織が事業継続性を維持していくためには、事業継続の必要性を従業員に対してどのように浸透させるかが重要である。事業継続は日常的に必要とされるものではなく、緊急時に必要となるため、日頃からの意識づけは重要となる。

また、社会的責任の面からみて、ステークホルダに対してどのようなコミュニケーションを取っているか、その対応も重要となる。場合によっては、事業継続に対する取組みにステークホルダにも参加してもらう必要がある。

2.3.5　【2.5　環境】

組織はさまざまな経営状況下にあり、環境はリスクの源泉の１つでもある。最近では、社会的関心も高まり、種々の業態において、各組織とも環境への対応を重視し、環境行動が試みられている。ISO14000 シリーズの環境マネジメント規格も活用されている。しかし、リスクマネジメントの視点からみると、きわめて複雑・多様な環境リスクへの認識・対応は十分であるとは言い難い。たとえば、組織の事業エリアで生じた廃棄物について考慮するとき、その廃棄物が有害物質や波及的な環境負荷を含むものであれば、「誰により、どこで、どのように処理（資源化）されるのか」という、それぞれの局面ごとにリスクが内在している。そのため、リスマネジメントの枠組みにおいて、環境リスクの状況把握から始まるプロセスに沿った展開が不可欠となる。

環境に関するリスクマネジメントの評価項目と質問項目数は、次のとおりである。

評価項目（第２階層）	評価項目（第３階層）	第４階層 項目数	第５階層 項目数
(1)環境リスクの状況把握	①環境活動の目標設定	15	3
	②環境リスクに影響を与える動向の認識		
	③環境戦略の策定		
	④環境管理の実践		
(2)環境リスクの特定	①人や生態系への環境リスクの特定	24	0
	②バリューチェーンを通じた環境リスクの特定		
	③技術使用・選択による環境リスクマネジメント		
	④環境市場・金融の環境リスク要因		
	⑤企業の社会的環境責任		
	⑥国際連携における環境リスク対応		
	⑦地球環境制約への対応		
	⑧環境クライシスの特定		
(3)環境リスクの分析	①人や生態系への環境リスクの分析	24	0
	②バリューチェーンでの環境リスク分析		
	③技術開発・適用の環境リスク分析		
	④環境市場・金融のリスク分析		
	⑤社会的環境責任に伴うリスク分析		
	⑥国際連携におけるリスク分析		
	⑦地球環境制約のリスク分析		
	⑧環境クライシスのリスク分析		
(4)環境リスクの評価	①人や生態系への環境リスクの評価	26	4
	②バリューチェーンでの環境リスク評価		
	③技術開発・適用に付随する環境リスクの評価		
	④環境市場・金融のリスク評価		
	⑤社会的環境責任にかかわるリスク評価		
	⑥国際連携に関連するリスク評価		
	⑦地球環境制約と組織の関係性の評価		
	⑧環境クライシスのリスク評価		

評価項目（第 2 階層）	評価項目（第 3 階層）	第 4 階層 項目数	第 5 階層 項目数
(5)環境リスクの対策	①環境リスクマネジメントシステムの構築	28	0
	②人や生態系への環境リスク対策		
	③バリューチェーンでの環境リスク対策		
	④技術に伴う環境リスクマネジメント		
	⑤環境市場での競争力の確保		
	⑥組織の社会的環境責任への対応		
	⑦国際連携による環境リスクマネジメント		
	⑧地球環境制約への適応		
	⑨危機管理		
(6)環境リスクのモニタリングとレビュー	①環境リスクの監視	21	0
	②環境リスクマネジメントプロセスの確認		
	③環境リスクマネジメント結果のレビュー		
	④プロセスのモニタリングとレビュー結果の活用		
(7)環境リスクのミュニケーションと協議	①環境コミュニケーションの展開	10	1
	②共考による決定		
	③コミュニケーションの実施		
	④コンサルテーションの実施		
計		148	8

各質問項目の要点を以下に説明する。

「環境リスク」とは、何らかの（環境に対する）行動が、ある状況下での状態（自然環境や社会など）に変化を与えた結果の事象（環境対応のための費用の増加や企業イメージの低下、法律改定への機会等）として定義される。図 2-3-3 は組織と環境とステークホルダの関係を示した模式図であり、組織が対面する環境リスクを 2 種類に区分している[20]。

第 1 の環境リスクは、「環境の応答が不確実な状況下で、組織の生産や廃棄などの行動の結果、環境が変化して、その結果、組織にもたらされる影響（すぐに因果関係がわからないことがある）」につながることを言う。この場合、組織行動が環境に影響を与える作用側に注目している。つまり、組織活動（図 2-3-3 の①）に伴って発生する環境負荷により、人間・生物・生態系・社会に対して影響を与え（図 2-3-3 の②）、その結果が、組織活動に対して社会からの評価や要請（企業行動に対する追求やメディアなどによる批判など）や規制（企業の負荷排出行動の制限、環境保

20 松井孝典、織田朝美、松村憲一、加藤悟、原田要之助、盛岡通「組織のサステイナビリティマネジメントを指向した環境リスクマネジメントシステムの開発」、日本リスク研究学会第 21 回研究発表会講演論文集、PP. 475-480、 2008 年；松井孝典、齊藤修、松村憲一、加藤悟、盛岡通「高度技術産業における組織リスクマネジメント機能発現のための知識モデリング」、人工知能学会第 22 回全国大会予稿集、3D3-01、 2008 年；松井孝典、織田朝美、松村憲一、加藤悟、原田要之助、盛岡通「組織活動に連関する環境リスクを対象としたマネジメントタスクインベントリの開発」、 日本リスク研究学会第 22 回年次大会、講演論文集、Vol.22、Nov. PP. 28-29、2009 年

全の監視、行動に対する罰則）などの形で跳ね返ってくるリスクである（図 2-3-3 の③）。

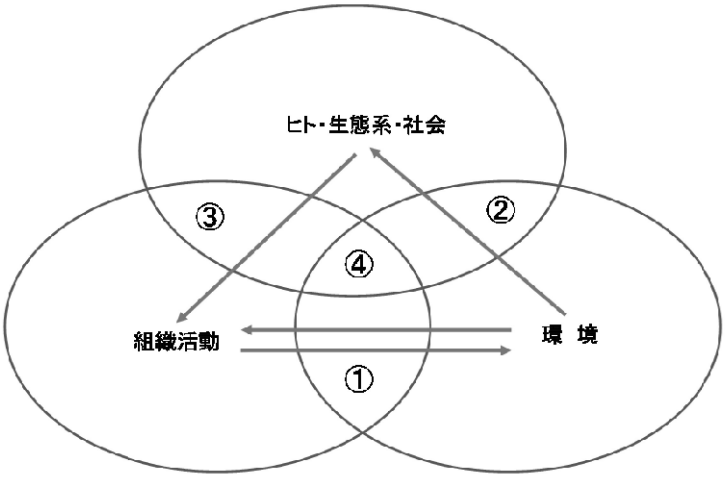


図 2-3-3. 組織の環境リスクの類型

（出典：松井他、「組織のサスティナビリティマネジメントを指向した環境リスクマネジメントシステムの開発」、日本リスク研究学会、2008 を一部修正）

第 2 の環境リスクは、組織自身に直接のかかわりがないにもかかわらず、環境が変化したことによって、その効果で組織に対して直接的な影響を与える（図 2-3-3 の④）リスクであり、組織が予見していない場合にはとりわけその事業活動、存続に大きな影響を与える。たとえば、代替エネルギー開発に乗り遅れ、あるいは、生態系・生物多様性の保全のために事業の大幅変更を強いられるなど、企業の活動や戦略が大きく変わってしまう場合を含む。

組織の立場からは、第 1、第 2 の両方の環境リスクを見据えて対応する必要がある。以下では、この両方を包含した観点から、各リスクマネジメントプロセスについて述べる。

（1）環境リスクの状況把握

ここでは、組織経営の中に環境リスクマネジメントを明確に位置づけて目標設定と戦略・行動計画の策定ができているかを問う。リスクマネジメントの際に何を環境リスクとして認識しているかを評価する。

前提となる経営環境、環境リスクの目標設定、環境リスクに影響を与える動向の認識、環境戦略の策定、環境管理の実践について、組織の状況を把握することがマネジメントサイクルの出発点である。

（2）環境リスクの特定

ここでは、先に示した 2 種類の環境リスクに応じて、(I) 環境負荷が発生するシナリオとそれを生じる組織の行動、および (II) 組織行動に影響を与えうる環境的制約をとらえているさまを、

次の 7 つのドメインごとに評価している。

①人や生態系への環境リスクの特定（I）

②バリューチェーンを通じた環境リスクの特定（I）

③技術使用・選択による環境リスクマネジメント（I）

④市場・金融の環境リスク要因（I）

⑤組織の社会的環境責任のリスクの特定（II）

⑥国際連携上の環境リスク対応（II）

⑦地球環境制約への対応（II）

（3）環境リスクの分析

ここでは、特定された環境リスクに対する（I）環境負荷の量反応関係やその環境負荷を生じる組織行動の分析、および（II）環境的制約に対する組織行動を分析していく。分析にあたっては、どのような対象の環境リスクに着目するのか、どのようなリスク情報を集めるかを明らかにする。

それぞれのリスク分析について、経営的観点、組織運用の実務的観点から評価する。

①人や生態系への環境リスクの分析（I）

②バリューチェーンでの環境リスクの分析（I）

③技術開発・適用の環境リスクの分析（I）

④環境市場・金融のリスク分析（I）

⑤社会的環境責任に伴うリスク分析（II）

⑥国際連携におけるリスク分析（II）

⑦地球環境制約のリスク分析（II）

に加えて、重大な危機として認識することで意味が深まる

⑧環境クライシスのリスク分析（II）

を実行する。

（4）環境リスクの評価

リスク評価では、リスク特定、リスク分析で明確になった結果を社会・経済的視点から吟味、解釈し、対応すべきリスクの特定や総合評価、優先順位づけなどを行う評価業務を定義している。特に、リスクが与える影響について、（I）環境負荷の量反応関係やその環境負荷を生じる組織行動を評価し、および（II）環境的制約に対して応答する組織行動の評価に分けている。

①人や生態系への環境リスクの評価（I）

②バリューチェーンでの環境のリスク評価（I）

③技術開発・適用に付随する環境リスクの評価（I）

④市場・金融のリスク評価（I）

⑤社会的環境責任にかかわるリスク評価（II）

⑥国際連携に関連するリスク評価（II）

⑦地球環境制約と組織の対応の評価（II）

⑧環境クライシスのリスク評価（II）

リスクマネジメントは、概してリスクを一般化して検討するため、ともすればその具体的な様相を見逃すことがある。それを避けるために、個別の質問項目による評価により、組織をとりまく多様性を浮き彫りにして、組織の行うリスクマネジメントの有効性を検証する。

（5）環境リスクの対策

リスク対策のプロセスでは、状況把握、リスクの特定、分析、評価に至る一連の評価結果に基づいて､対策を講じるための環境リスクマネジメントシステムの運用や組織行為を定義している。

①環境リスクマネジメントシステムの構築（I)、(II)
②人や生態系への環境リスク対策（I)
③バリューチェーンでの環境リスク対策（I)
④技術に伴う環境リスクマネジメント（I)
⑤環境により相互に影響を受ける市場での競争力の確保（I)、(II)
⑥組織の社会的環境責任への対応（II)
⑦国際連携による環境リスクマネジメント（II)
⑧地球環境制約への適応（II)
⑨環境クライシスのリスクマネジメント（危機管理）(II)

環境リスク対策とは、リスク分析の結果に基づいて形式的に低減対策を採用することを意味しない。総体として環境リスクを管理するためのリスクマネジメントシステムを構築することが重要である。構築したリスクマネジメントシステムを基礎にして、各分野のリスクの重要性を比較し、実際に対応できるかの対策実現性にあわせて、保有リスクからリスクの顕在化の起こりやすさを変化させる等の対策の中から、効果的で適切な対策方針を選定し、決定する。

（6）環境リスクのモニタリングとレビュー

このプロセスはマネジメントシステム全体を通じて実行するものであり、リスクマネジメントプロセスの検証と結果の妥当性に関する監視とレビュー、結果の活用についてのタスクを定義している。ここでは、環境リスクの監視、環境リスクマネジメントプロセスの確認、環境リスクマネジメント結果のレビュー、プロセスのモニタリングとレビュー結果の活用の観点から組織行動を評価する。

ISO31000 では、モニタリングはリスクマネジメントのすべての段階についても実施することになっており、フィードバックを受けてリスクマネジメントシステムを適切に改善させ、さらに残余リスクをモニタリングし、リスクが増大してきた場合にはリスクマネジメントプロセスをやり直すことが必要となる。

（7）環境リスクのコミュニケーションと協議

このプロセスは、環境リスクマネジメントの全体を通じて実行する行為であり、環境コミュニケーションができているか、その際に関係者と共考して専門事項の相談を実行しているかを評価する。特に、ISO31000 の考え方を取り入れている JRMS2010 は、既存のモデルと比べると、リ

スク特定、リスク分析、リスク評価の各プロセスについてもコミュニケーションの対象として扱っている点が大きく違っている。ここでは、環境コミュニケーションの展開、共考による決定、コミュニケーションの実施、コンサルテーションの実施について具体的に問いかけている。

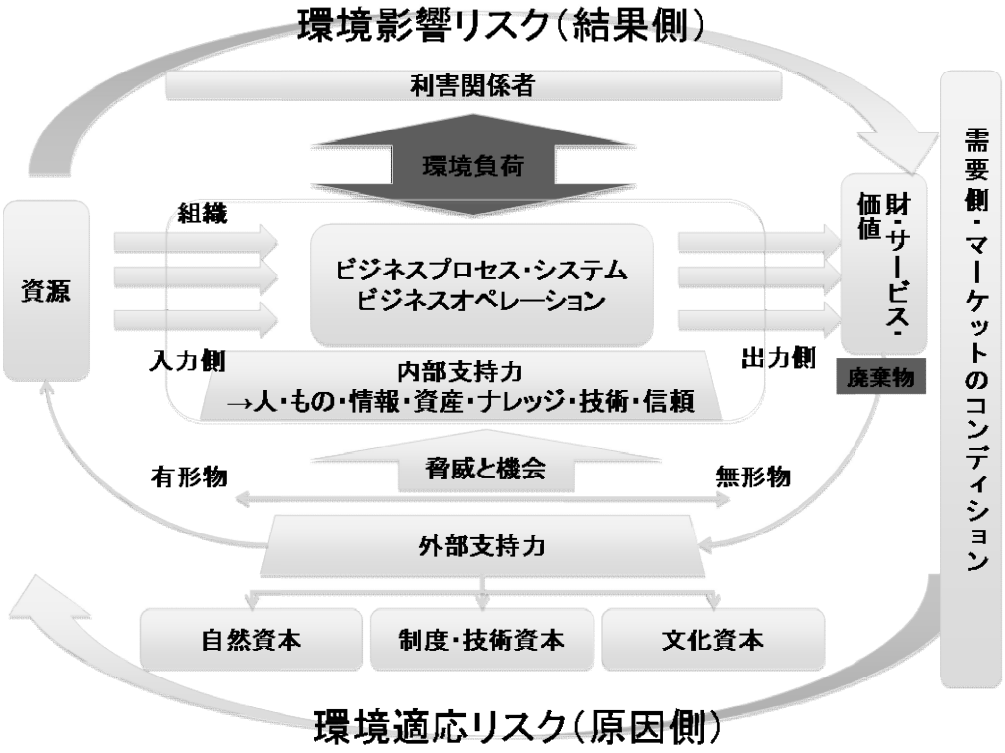


図 2-3-4. 環境リスクマネジメントの対象世界モデル（プロセスアプローチ）

（出典：松井他、「組織のサステイナビリティマネジメントを導く環境リスクマネジメントシステムの開発」、日本リスク研究学会、2008 を一部修正）

◆環境リスクのドメインについて

リスクマネジメントプロセスを適用する対象となる環境リスクのドメインは、図 2-3-4 で示した相互的なプロセスアプローチによる対象世界モデルを基にしている。

このモデルでは、環境リスクのドメインとしては大気系・土壌・水系などの環境媒体や廃棄物、原材料、地域環境といった空間的・物的ドメインのみに限定せず、それらの環境負荷が発生する源となる調達・設計・開発・輸送・販売・運用・廃棄・再生という組織活動のバリューチェーンとプロダクトのライフサイクルを含んでいる。

バリューチェーンを通じた社会・市場との対話もリスクマネジメントのドメインとして選定することを勧める。これは図 2-3-4 に示したように、産業組織などの主体がプロダクトやサイト周辺環境の物理的な環境マネジメントだけではなく、コンプライアンスや社会的環境責任に適応しうるか否かの観点から、環境リスクに関するコミュニケーションもリスクマネジメントの対象に含まれているからである。

特に重要なことは、今後の組織にとって低炭素社会の構築や気候変動への適応、生態系サービ

スの持続利用や生物多様性保全といった地球規模の環境制約に対する適応方略が、きわめて大きな組織リスクあるいは機会の要因になっていることである。低炭素社会への移行について、日本版グリーンニューディールや排出量取引、温暖化ビジネス等の状況をリスクの文脈で語る機会が増えており、生態系対応を観察すると、低炭素化社会の移行の歴史から類推して、機会と脅威を先取りする動きもある。こうしたリスク群に対して、新規技術の開発や発展途上国への環境技術の移転・支援を構想し、環境的に公平かつ公正な社会整備も視野に入れてグローバル化する世界の下での組織行動をデザインすることが必要であり、その際には、国際連携や市場や社会との対話を通じた環境リスクマネジメントが求められる。

［参考文献］

[1] 松井孝典、織田朝美、松村憲一、加藤悟、原田要之助、盛岡通　組織のサステイナビリティマネジメントを指向した環境リスクマネジメントシステムの開発、日本リスク研究学会第 21 回研究発表会講演論文集、475-480、2008 年

[2] 松井孝典、松村憲一、織田朝美、加藤悟、原田要之助、盛岡通　組織のサステイナビリティマネジメントを導く環境リスクマネジメントシステムの開発、日本リスク研究学会第 21 回年次大会講演論文集、Vol.21、Nov.29-30、2008 年

[3] 松井孝典、齊藤修、松村憲一、加藤悟、盛岡通 高度技術産業における組織リスクマネジメント機能発現のための知識モデリング、人工知能学会第 22 回全国大会予稿集、3D3-01、2008 年

[4] 松井孝典、織田朝美、松村憲一、加藤悟、原田要之助、盛岡通　組織活動に連関する環境リスクを対象としたマネジメントタスクインベントリの開発、日本リスク研究学会第 22 回年次大会、講演論文集、Vol。22、 Nov。28-29、2009 年

[5] 松井孝典、熊澤輝一、加藤悟、織田朝美、原田要之助、盛岡通：オントロジー技術を用いた組織における環境リスクマネジメントシステム構築のための知識モデル開発, 電子情報通信学会，技術研究報告 vol. 109, no.386, AI2009-26, pp. 43-48 2010.1

[6] Takanori MATSUI, Asami ORITA, Satoru KATO, Ken’ichi MATSUMURA, Yonosuke HARADA, Tohru MORIOKA: Diagnostic Management Process for Corporate Environmental Risk toward Sustainable Society: a with ISO 31000 harmonious scheme, Asian Conference on Risk Assessment and Management 2009, R139, (2009.5)

2.3.6 【2.6 医療】

医療の分野では、医療事故の防止や患者の安全確保という目的でのリスクマネジメントが広く医療関係者に認知されている。2002 年 4 月に厚生労働省医療安全対策検討会議が、「医療に内在するリスクを管理し、患者の安全を確保する」ことに重点を置き、「『リスクマネジメント』を『医療安全管理』と同義として用いる」と概念整理を行っている[21]。その後の 2006 年の医療法改正に

[21] 厚生労働省医療安全対策検討会議「医療安全推進総合対策」報告書　2002 年 4 月 17 日

おいて、各医療機関は医療の安全確保が義務づけられ、関連する法令やガイドライン等の整備が進んでいる[22]。

2000 年に「患者の安全」を緊急課題として取り上げた報告書[23]を公表した米国医療の質委員会は、その最終報告書[24]で、「設計がよくないシステムのもとでは、そこで働く人が懸命に仕事をする、しないにかかわりなく、失敗をまねく。より安全で質の高い医療を望むのであれば、医療システムを医療サービスの運営と臨床プロセスをサポートする情報技術の活用を含めて再設計する必要がある」としている[25]。

わが国の医療法の第 1 条の目的においても、「医療を受ける者の利益の保護及び良質かつ適切な医療を効率的に提供する体制の確保」が掲げられている。

ここでは、専門性の高い公共サービスを継続して提供することを目的とした、医療機関の組織運営（=経営）のリスクマネジメントにかかわる項目を整理した。医療経営については経済産業省サービス産業人材育成事業　医療経営人材育成テキスト[26]を参考資料としている。医療安全管理については法令やガイドライン、管理者講習のテキスト[27]等があるので、ここでは医療機関としての経営の全体最適を指向するリスクマネジメントとして、リスクを包括的に把握することを重視した。

現代の経営環境下の組織の経営にかかわる部分は、【1.組織経営編】の「経営」、「内部統制」、【2.個別リスク対応編】の「情報システム」、「情報セキュリティ」、「個人情報保護」、「事業継続」、「環境」として取り上げているので、各編を併用していただきたい。

質問項目は医療機関の社会的使命の達成に影響を及ぼすリスクを認識し、それをマネジメントする体制を整え、実践できているかを確認し、次の改善へとつなげるシステムとして 7 つの評価項目で構成されている。近年の医療機関の経営においては欠くことのできない業務の外部委託と情報システム、情報セキュリティについては別の領域の質問項目を参照されたい。【2.個別リスク対応編】では、JRMS2010 の概念の根拠となった ISO31000 のリスクマネジメントを検討する枠組みに沿って、リスクを網羅的かつ包括的にとらえているかを重視した質問項目を配置している。

医療に関するリスクマネジメントの評価項目と質問項目数は、次のとおりである。

22　2007 年 3 月の医療法施行令の改正政令等では、医療安全管理、院内感染対策、医薬品安全管理、医療機器安全管理の体制整備が義務付けられた。また、病院等のインフラとなった情報システムについても、厚生労働省は「医療情報システムの安全管理に関するガイドライン」をまとめており、2010 年 2 月には第 4.1 版が公表されている。

23　Institute of Medicine: To err is human: building a safer health system, National Academy Press, 2000.

24　Institute of Medicine: Crossing the quality chasm,　National Academy Press, 2001

25　同上　邦訳 p.5

26　黒川清、尾形裕也監修、KPMG ヘルスケアジャパン編集「医療経営の基本と実務」経済産業省サービス産業人材育成事業　医療経営人材育成テキスト、日経メディカル開発、2006 年

27　四病院団体協議会医療安全管理者養成委員会編「医療安全管理者必携　医療安全管理テキスト」日本規格協会、2005

評価項目（第 2 階層）	評価項目（第 3 階層）	第 4 階層 項目数	第 5 階層 項目数
(1)医療機関経営のリスクに影響を与える状況の把握	①リスク分析の前提となる経営目標	7	0
	②医療機関経営の外部環境		
	③組織内部の状況		
	④業務管理		
	⑤医療リスクマネジメント		
(2)リスクの特定	①患者にかかわるリスク	6	0
	②組織にかかわるリスク		
	③スタッフにかかわるリスク		
	④地域住民にかかわるリスク		
(3)リスク分析	①組織的要因の影響分析	11	0
	②人的要因の影響分析		
	③物的要因の影響分析		
	④情報管理と情報システムの影響分析		
(4)医療経営のリスク評価	①医療サービスのリスクの評価基準	3	0
	②経営管理にかかわるリスクの評価基準		
	③リスクマネジメントの重要度の評価		
(5)リスク対策	①人的要因にかかわるリスク対策	4	0
	②組織要因にかかわるリスク対策		
	③情報システムのリスク対策		
	④医療機関の緊急時対応		
(6)モニタリングとレビュー	①日常運用の点検	4	0
	②内部評価と外部評価		
	③是正措置の点検・評価		
	④経営者の役割		
(7)コミュニケーションと協議	①患者および家族とのリスクコミュニケーション	6	0
	②医療機関内部のリスクコミュニケーション		
	③取引先とのリスクコミュニケーション		
	④関係官庁とのリスクコミュニケーション		
	⑤地域社会やメディアとのリスクコミュニケーション		
計		41	0

各質問項目の要点を以下に説明する。

(1) 医療機関経営のリスクに影響を与える状況の把握

はじめに、どのような状況の変化が医療機関の経営に影響を与え、それを認識してリスクマネジメントの対象ととらえるか、リスクマネジメントを実施する体制が整っているかを確認する。

リスクマネジメントを行うためには、医療機関の使命（ミッション）や理念が具体的に経営目的や経営目標に示され、組織としての共通認識となっていることが必要である。

医療は専門性の高い公共サービスであることから、社会状況の変化は経営に影響を与える重要な要素となる。経済や社会の状況は制度・政策に反映される。医療技術や情報技術の進歩にどう向き合うか、地域の高齢化や患者の価値観の変化、近隣の競争環境などの変化や自組織の活動が

与える環境への負荷などを網羅的に把握しておく必要がある。

組織の統治、経営方針や経営戦略、組織の能力、各業務の管理・運営、内部統制や業務の見直しなど、内部の状況を把握することは経営の重要課題である。また、重要なインフラである情報システムも常に把握しておくべき対象である。医療経営にとっては医療行為だけでなく、雇用や購買、治験や研究などに伴うさまざまな契約関係の把握も重要である。

リスクマネジメント活動そのものもリスクに影響する項目として評価対象となる。

（2）リスクの特定

ここでは、リスク要因を特定しているかを確認する。リスクの源、影響を受ける領域、発生する一連の状況、その原因と起こりうる結果を把握しておくことが重要となる。ここでは、医療機関にとって欠くことのできない医療における安全の確保、安心と納得に着目し、その主要なステークホルダである「①患者」、「②組織」、「③スタッフ」、「④地域住民」にかかわるリスク要因として、質問項目を整理した。

人対人のサービスである医療にとって、コミュニケーションギャップや医療のもつ本来的な不確実な特性は、安全の確保、安心と納得にどのような影響を与えるのか。医療機関の日常で起きうる医療上あるいは療養環境で起きる事故、あるいは感染症の流行や災害などは、リスクマネジメントの対象として広く認識されている。医療機関経営にとっては、制度・政策、技術の変化、組織の運営、業務管理、スタッフの勤務環境、業務の外部委託、情報管理などが、患者、組織、スタッフ、地域住民に与える影響を包括的に把握することが重要となる。

（3）リスク分析

医療機関において、「①組織」、「②人」、「③物」、「④情報」にかかわる各要因が経営目標の達成を阻害する影響を定性的・定量的に分析・把握しているかを確認する。

各要因と経営目的との不整合、経営体制や資産および業務の管理状況、スタッフの能力や行動、医療機器・設備や施設の管理、組織内での情報の伝達や管理、委託業務の管理、情報システムの障害や不正侵入などについて、問題意識をもっているか、組織的な情報の提供と分析が行われているか、そのための資源は確保されているか、などを評価する。

（4）医療経営のリスク評価

ここでは、医療機関経営のリスクについて、「①医療サービス」と「②経営管理」にかかわるリスクに大別し、それぞれのリスク評価に用いる基準と、リスクマネジメントの重要度を評価しているかを確認する。

医療サービスでは、医療事故の患者への影響度、医療事故と過誤、医療水準、医師としての品位、患者の苦情・クレームを取り上げている。経営管理では、経営目標、経営指標の評価、医療技術の評価、外部委託、情報セキュリティについて評価する。

いずれの項目も、基準や評価指標に何を採用し、組織のなかでそれが認識されているかが重要となる。

（5）リスク対策

評価したリスクに対してどのような対応が取られているかを確認する。対応を要するリスクを、「①人的要因」、「②組織要因」、「③情報システム」、「④緊急時対応」が必要なものに大別した。

それぞれについて、対策は原因を反映しているか、対策の効果は確認されているか、その効果は継続（持続）しているか、その対策を取ることで他の業務に影響を及ぼしていないか、その対策に投入した費用や資源と効果は評価されているか、について評価する。

（6）モニタリングとレビュー

ここではリスクマネジメントに対する点検と評価が行われているかを確認する。点検および確認のレベル、点検から改善のサイクルに着目し、「①日常運用の点検」、「②内部評価と外部評価」、「③是正措置の点検・評価」、「④経営者の役割」について取り上げている。

リスクマネジメント活動を日常の運用でモニタリングすることは、リスクマネジメントの見直しにつながる。内部での業務監査や会計監査、医療機能評価や情報システム監査などの第三者評価はさらなる見直しの機会となる。

重要なのは、リスクマネジメントが経営者層のレビューを受けているかである。モニタリングとレビューのいずれの段階においても経営者層が関与しているかを確認する。

（7）コミュニケーションと協議

医療サービスにかかわるステークホルダとのリスクコミュニケーションについて確認する。コミュニケーションの対象は、「①患者および家族」、「②医療機関内部」、「③取引先」、「④関係官庁」、「⑤地域社会やメディア」に区分している。

患者とその家族、関係官庁、地域社会やメディアは、外部の重要なコミュニケーション先である。取引先とは、医薬品・医療機器・医用材料などのベンダ、業務委託先、金融機関等を指している。医療機器等のベンダや情報システムの業務委託先とは、リスク情報の共有やリスク対応への協力など、日常的なコミュニケーション関係を築く必要がある。組織内部のリスクコミュニケーションが重要であることは、言うまでもない。

JRMS2010 を医療機関で利用するメリットは、医療安全だけでなく、組織全体のリスクマネジメントを包括的にとらえられることにある。医療安全管理に重点をおく医療機関のリスクマネジメントでは、リスクマネジメント部門は担当業務のリスクの発見と分析には精通している。それが組織全体の改善にどのようにつながるかを意識することで、リスク連鎖の可能性を軽減し、持続的な改善につながることが期待される。

［参考文献］

[1] 厚生労働省医療安全対策検討会議「医療安全推進総合対策」報告書　2002 年 4 月 17 日

[2] 厚生労働省「医療情報システムの安全管理に関するガイドライン」第 4.1 版　2010 年 2 月

[3] Kohn, L.T., Corrigan, J.M., and Donaldson, M.S. Committee on Quality of Healthcare,

Institute of Medicine: To err is human: building a safer health system, National Academy Press, 2000〔米国医療の質委員会／医学研究所著　医学ジャーナリスト協会訳「人は誰でも間違える - より安全な医療システムを目指して」日本評論社，2000〕

[4] Institute of Medicine: Crossing the quality chasm, National Academy Press, 2001.〔米国医療の質委員会／医学研究所著　医学ジャーナリスト協会訳「医療の質　谷間を越えて 21 世紀へ」日本評論社，2002 〕

[5] 黒川清、尾形裕也監修、KPMG ヘルスケアジャパン編集「医療経営の基本と実務　上下」経済産業省サービス産業人材育成事業　医療経営人材育成テキスト、日経メディカル開発、2006

[6] 四病院団体協議会医療安全管理者養成委員会編「医療安全管理者必携　医療安全管理テキスト」日本規格協会、2005

[7] 全日本病院協会「病院のあり方に関する報告書 2007 年版」

[8] 梁井皎，大坂顯通編「実践医療リスクマネジメント」じほう、2003

[9] 黒田雅美，稲垣隆一「医療機関の内部統制とリスクマネジメント」清文社、2006

３．ＪＲＭＳツール

JRMS2010 は、対象リスク領域に関する質問項目に対し、回答部門から選出された回答者が組織の実態を把握するために回答し、その回答結果をもとに組織のリスクマネジメントの目標レベルと比較考量し、分析するシステムである。

JRMS2010 で提供されている質問数は、対象リスク領域によっては 100 問以上ある。このため、組織がリスクマネジメントを実践するにあたり、JRMS2010 の効率的、効果的な導入を図るために開発されたのが、JRMS ツール（回答および分析ソフトウェア）である。ここでは、JRMS ツールを利用するうえで必要となる基礎知識、およびツールの利用について説明する。

3.1　JRMS ツールの基礎知識

JRMS ツールの利用にあたっては、現在の経営環境の下で組織としてのリスクマネジメントの現状を把握する必要性を認識していることが重要である。現状認識のためには、組織に関係するリスク領域に係る質問項目に対する回答を通して把握するのが最も効果的な方法であるといえる。その際求められるのは、JRMS2010 に装備されている JRMS ツールの機能を十分理解することである。

そこで、JRMS ツールを利用するうえで必要となる基礎知識を説明する。

3.1.1　JRMS ツールの概要

（1）JRMS ツール

JRMS ツールは組織に JRMS2010 を効率よく、効果的に導入するためのソフトウェアである。

（2）利用メリット、導入効果

JRMS ツールを使って JRMS2010 を組織に導入することにより、組織のリスクマネジメントの現状、課題を把握することができる。もしも関係部門・回答者間で認識ギャップがあれば、その原因を究明することにより、現状認識の共有が可能になり、必要に応じて改善の方向を見いだすことができる。

（3）想定利用者

①組織のリスクマネジメントの現状を認識する必要がある人
②組織のリスクマネジメントの実践から改善すべき課題を把握したい人
③組織のリスクマネジメントを分析するコンサルタント
④JRMS2010 を利用して、リスクマネジメントを学びたい人

（4）特徴

①回答する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、組織の現状を評価することが可能となる。

②回答者にとって理解しやすい質問表現、解説表示

組織の部門ごとに質問の理解度が異なることが予想されるため、質問の意図がわかりやすいように解説や用語の説明文を加えている。また、部門により回答に対する視点に差異があると思われる質問は、回答部門に合わせて表現を変えている。

③回答する組織に合わせた評価基準の変更

組織により、リスクの評価項目の重要度が異なることがある。このため、どの評価項目を重要視するかの「重み」を設定することができる。この機能により、より組織の現状に合わせた評価を行うことができる。

④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。このため、回答を短時間に入力できるようなインタフェースを提供している。

⑤質問の理解を助けるヘルプ機能

回答者によってはJRMS2010で提供する質問内容の意図、解説、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それらの情報を表示する「ヘルプ機能」を提供する。

⑥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）から比較ができるように、評価結果をレーダーチャートで表示する。また、質問に対する回答を一覧表示した集計表も表示し、より詳細な分析を可能とした。

（5）利用イメージ

JRMSツールを組織に導入した際の利用イメージを図3-1-1に示すので、下記の説明を通して理解してもらいたい。

JRMSツールは、J-inputとJ-analyzeで構成されている。

J-input は、複数の部門および複数の回答者からリスクマネジメントの現状（回答評価結果、以下、「回答データ」という。）を抽出するためのソフトウェアであり、J-analyze は、回答データを分析するためのソフトウェアである。

まず、回答者は、J-inputが提示するリスクマネジメントに関する質問に対して回答し（①）、回答データをファイルに保存する（②）。

次に、リスクマネジメント担当者は、J-analyze を使い、レーダーチャートなどを出力し、回答データを分析する（③）。

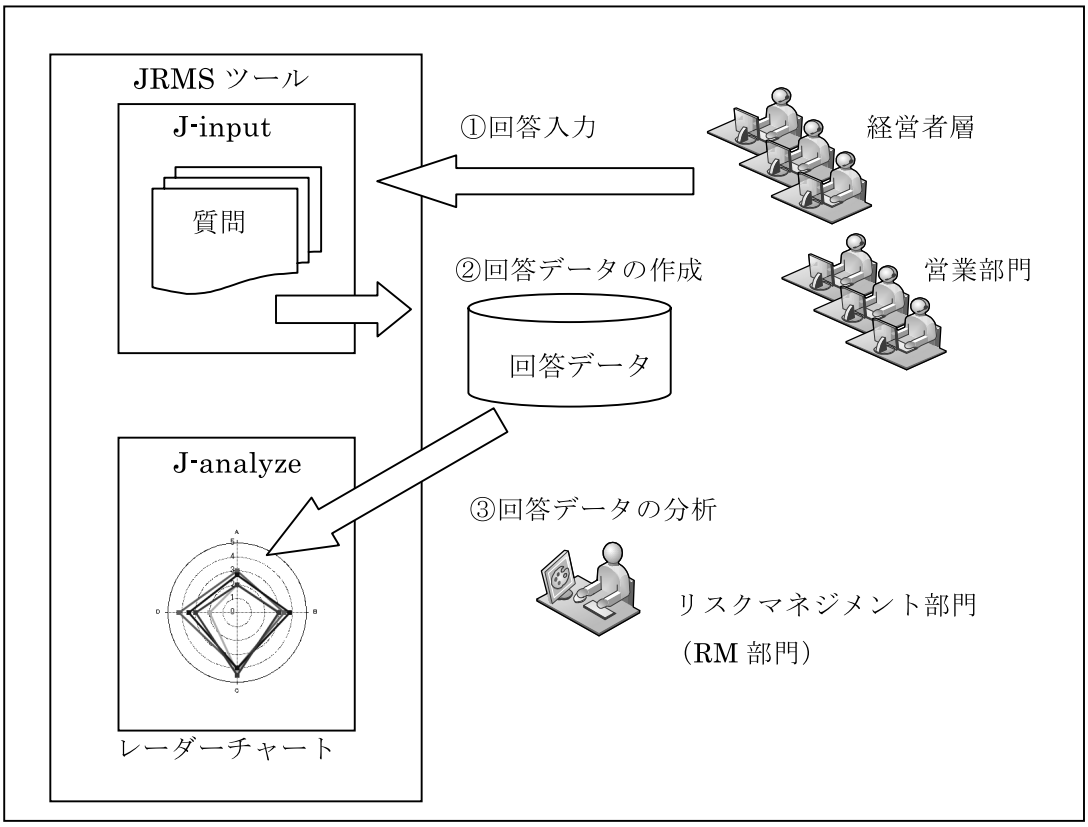


図 3-1-1. JRMS ツール利用イメージ

(6)　提供機能

①J-input

・認証

　ユーザ ID、パスワードによりユーザの認証を行う。

・質問セット選択

　回答する質問セット（詳細は本章「3.1.3　質問セット」の項を参照のこと）を選択し、質問セットに含まれる質問を表示する。

・回答入力

　質問に対する回答を入力する。質問への回答は成熟度の評価レベルを指定する。

・回答データの作成

　質問への回答結果をファイル（回答データ）に保存する。この際、未回答の質問がある場合はファイルへの保存はできない。ただし、回答の入力を中断して同じ状態から再開できるよう一時保存の機能を提供する。

②J-analyze

・認証

　ユーザ ID、パスワードによりユーザの認証を行う。

・重み設定

重みを設定することにより、組織で重視する評価項目（または質問）を指定することができる。

・出力

回答データの分析結果を集計表、レーダーチャートで出力できる。

集計表は、回答データの回答年月、部門、回答者を指定し、回答データを表形式で表示する。

レーダーチャートは、回答データを部門ごとに集計し、レーダーチャートの形式で表示する。

・システム設定

ユーザ、部門、回答年月の登録・修正・削除および接続先（質問セットや回答データのファイルパス名）について設定する。

3.1.2　ユーザ管理

ツール利用者はユーザごとにそれぞれユーザ ID、パスワード、ユーザ名、部門および権限が付与されている。

ここでいう「部門」とはユーザの所属する部門を指し、「権限」は、それぞれのユーザが利用できる機能の範囲を規定するものであり、回答者、分析者、システム管理者に区別される。

「回答者」は J-input で提供する機能（回答処理）のみが利用でき、「分析者」および「システム管理者」は、J-analyze で提供する機能（集計・分析処理）が利用できる。

なお、「分析者」はユーザの登録・修正・削除を行うことができるが、回答データなどが保存されている場所（接続先）の設定については、「システム管理者」のみに権限が与えられている。

表 3-1-1 は、JRMS ツールにあらかじめ登録されているユーザの一覧である。

表 3-1-1. 登録済ユーザー覧

ユーザ ID	パスワード	ユーザ名	部門	権限
useraN	useraN	経営者層 N	経営者層	回答者
userbN	userbN	RM 部門 N	RM 部門	回答者
usercN	usercN	IS 部門 N	IS 部門	回答者
userdN	userdN	ユーザ 1 部門 N	ユーザ 1 部門	回答者
usereN	usereN	ユーザ 2 部門 N	ユーザ 2 部門	回答者
userfN	userfN	ユーザ 3 部門 N	ユーザ 3 部門	回答者
usergN	usergN	ユーザ 4 部門 N	ユーザ 4 部門	回答者
analyze	analyze	分析者	分析・システム管理	分析者
root	root	システム管理者	分析・システム管理	システム管理者

※N は 1～5 の数字を表す。

たとえば、useraN は usera1～usera5 の 5 ユーザが登録されていることを示している。

3.1.3　質問セット

質問セットとは、組織のリスクマネジメントの状況を抽出するための質問の集合を指す。

JRMS ツールにはリスク領域別に質問セットが設定されており、ツール利用者は、回答対象となるリスク領域の質問セットを選択して回答を入力する。

（1）　種類

質問セットの種類は 8 つのリスク領域からなる。

表 3-1-2. 質問セット一覧

編	リスク領域	質問数
1	1.1 経営	36
	1.2 内部統制	27
2	2.1 情報システム	124
	2.2 情報セキュリティ	60
	2.3 個人情報保護	74
	2.4 事業継続	58
	2.5 環境	156
	2.6 医療	41

（2）構造

質問セットは組織のリスクマネジメントの状況を評価するための評価項目、ならびにその評価項目に対して組織がどのような状況にあるのかを抽出するための質問からなる。以下は質問セットの構造の例である。なお、101-2、101-3、101-1-2、101-1-3、101-1-1-2、101-1-1-3 の下階層は省略している。

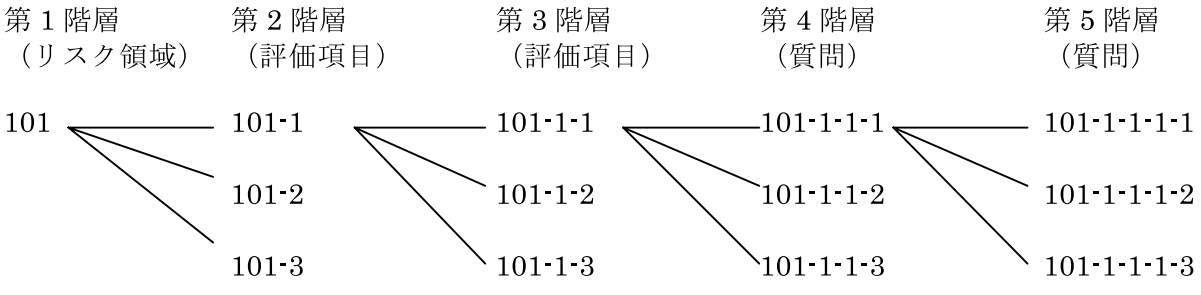


図 3-1-2. 質問セットの階層構造例

・第 1 階層は、リスク領域を表す。

・第 2 階層は、第 1 階層のリスク領域に対する評価項目である。特に、質問セットはこの第 2 階層にリスクマネジメントのプロセスが設定されている。

・第 3 階層は、第 2 階層をさらに詳細化した評価項目である。
・第 4 階層は、第 3 階層の評価項目に対して組織がどのような状況にあるのかを抽出するための質問で構成され、成熟度の評価レベルで回答する。
・第 5 階層は、第 4 階層の質問をさらに詳細化した質問で構成されており、Yes/No で回答する。第 5 階層の質問に対する回答の Yes の数を参考に、第 4 階層の評価レベルを回答者みずから決定する。たとえば、第 5 階層に 5 つ質問があり、そのうちの 3 つに Yes と回答した場合は、第 4 階層の評価レベルは 2 と回答する（リスク領域によっては、第 5 階層がないものもある）。

なお、質問セットの第 2、3、4 階層は、レーダーチャートの軸として利用される。

(3) 部門と質問セットの関係

すべての部門に対して質問セットが用意されているわけではなく、表 3-1-3 に示すように、部門により、用意されている質問セットが異なる。

表 3-1-3. 質問セットと部門

編	リスク領域	経営者層	RM 部門	IS 部門	ユーザ 1 部門	ユーザ 2 部門	ユーザ 3 部門	ユーザ 4 部門
1	1.1 経営	○	○	－	○	○	○	○
	1.2 内部統制	○	○	－	○	○	○	○
2	2.1 情報システム	○	○	○	○	○	○	○
	2.2 情報セキュリティ	○	○	○	○	○	○	○
	2.3 個人情報保護	○	○	－	○	○	○	○
	2.4 事業継続	○	○	－	○	○	○	○
	2.5 環境	○	○	○	○	○	○	○
	2.6 医療	○	○	－	－	－	－	－

3.1.4 質問への回答

第 4 階層の質問への回答は、成熟度の評価レベル（0～5）、D/K（わからない）、または N/A（対象外）で回答する。一方、第 5 階層の質問への回答は Yes/No または D/K、N/A で回答する。

(1) 成熟度の評価レベル

成熟度の評価レベルは、質問に対して組織がどの程度達成しているかを定量的に表したものである。

表 3-1-4. 成熟度の評価レベル

評価レベル		定義
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。
1	個人ごとによる対応	対象のリスクに対して個人的な対応を実施している。
2	部門ごとによる対応	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。
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。
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。
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。

(2) D/K、N/A

質問に対して「わからない」、「対象外」の場合はそれぞれ D/K、N/A で回答する。

大規模な組織では、リスクマネジメントに関する役割を複数の組織や個人にわりあてるため、各個人は自組織のリスクマネジメントについてすべての詳細を把握しているわけではない。したがって、各個人の担当領域以外のリスクについてはその詳細を知らない、という回答として D/K が必要となる。

質問の解説や用語説明により質問の意図を理解しやすくしているが、リスクマネジメントについての基本的な概念や、自組織のリスクマネジメントの概要については回答者が理解していることを前提としている。したがって、D/K が非常に多いときは、その個人の役割と D/K が多い領域を見て、回答者として適切かを確認する必要がある。

一方、質問は、どのような組織でも使用できるように網羅的な項目で構成されている。したがって、たとえば電子商取引を行っていない組織にとっては、電子商取引に関する質問はその前提条件を満たさないので意味がない。こういった場合は N/A を選択することで、その質問を対象外として取り扱うことができる。

ただし、実際には自組織で行っていても、その事実を知らずに N/A と回答する場合があるので、ある質問項目について N/A と評価レベル 0～5 の回答が混在したときは、自組織の状況を確認する必要がある。

(3) Yes、No

第 5 階層への質問に対して、あてはまるかどうかを Yes、No で回答する。

第 5 階層の質問は、第 4 階層の質問への回答に際して、参考となるチェック項目で構成されている。このため、第 5 階層の質問への回答の Yes の個数を参考にして、回答者がみずから第 4 階層の質問について評価する。

3.1.5　回答データ集計方法

回答データを部門ごとに集計し、レーダーチャートを作成する方法を以下で説明する。

ここでは図 3-1-3 の質問セットで、101-2 のレーダーチャートを作成する場合を例に説明する。

第 1 階層はリスク領域の名称、第 2、3 階層は評価項目、第 4 階層は質問を表す。101-1、101-3 の第 3、4 階層以下は省略している。括弧内は重みを表す。

ある評価項目の評価レベルは、その評価項目の直下の評価項目（または質問）の評価レベルをもとに計算する。重みはこの直下の評価項目（または質問）の評価レベルをどの程度の比率で評価項目の評価レベルの計算に反映させるかを示すものである。

たとえば、101-2-1 の評価レベルは、101-2-1-1、101-2-1-2、101-2-1-3 の評価レベルに重み 30：30：40 を勘案して計算される。

なお、重みの初期値は、均等に重みが設定されている。

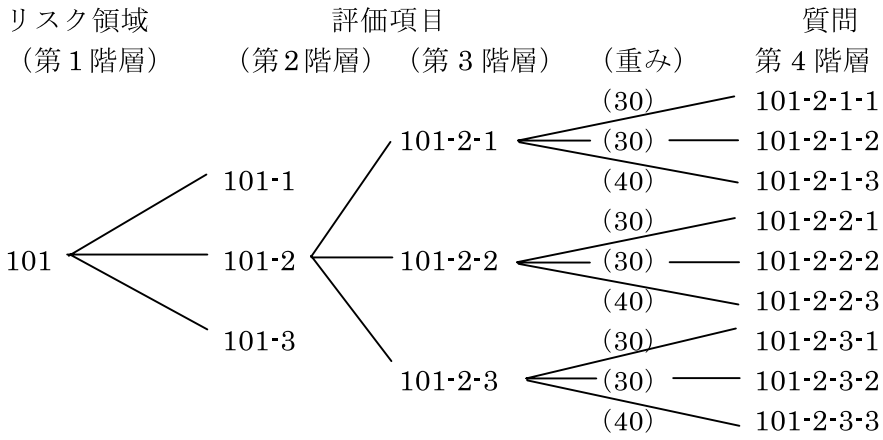


図 3-1-3. 質問セットの例

第 4 階層の 101-2-1-1～101-2-3-3 の質問に対して回答者が以下の評価レベルを回答した場合の集計方法を説明する。

表 3-1-5. 回答データ例

第 4 階層	経営者層			RM 部門		
	X1	X2	X3	Y1	Y2	Y3
101-2-1-1	4	4	3	2	3	3
101-2-1-2	3	3	4	2	4	2
101-2-1-3	5	4	3	5	2	3
101-2-2-1	3	3	N/A	4	4	2
101-2-2-2	4	5	5	3	5	2
101-2-2-3	3	5	4	D/K	3	4
101-2-3-1	4	5	3	4	3	4
101-2-3-2	3	3	3	2	3	4
101-2-3-3	3	2	3	2	3	2

（1）回答データの重み集計

回答データ（表 3-1-5）を使い、回答者ごとに第 3 階層評価項目の評価レベルを、重みを勘案したうえで計算する。

(101-2-1) = (101-2-1-1) × 0.3 + (101-2-1-2) × 0.3 + (101-2-1-3) × 0.4
(101-2-2) = (101-2-2-1) × 0.3 + (101-2-2-2) × 0.3 + (101-2-2-3) × 0.4
(101-2-3) = (101-2-3-1) × 0.3 + (101-2-3-2) × 0.3 + (101-2-3-3) × 0.4

たとえば、経営者層に属する回答者 X1 の 101-2-1 は、以下のように算出される（表 3-1-6）。

(101-2-1)= 4 × 0.30 + 3 × 0.30 + 5 × 0.40 = 4.1

表 3-1-6. 集計データ 1

第 3 階層	経営者層			RM 部門		
	X1	X2	X3	Y1	Y2	Y3
101-2-1	4.1	3.7	3.3	3.2	2.9	2.7
101-2-2	3.3	4.4	4.4	2.1	3.9	2.8
101-2-3	3.3	3.2	3.0	2.6	3.0	3.2

もしも評価レベル 0～5 以外の N/A または D/K と回答した場合、N/A は集計に含めず、D/K は評価レベル 0 として計算する。

101-2-2-1 を N/A で回答している経営者層 X3 の 101-2-2 は、N/A を無視して計算する。この際 101-2-2-1 は重みも無視され、101-2-2-2、101-2-2-3 の 30:40 だけで計算される。

(101-2-2) = 5 × {30 ÷ (30 + 40)} + 4 × {40 ÷ (30 + 40)} = 4.429… ≒ 4.4

101-2-2-3 を D/K で回答している RM 部門 Y1 の 101-2-2 は、D/K を評価レベル 0 として計算する。

(101-2-2) = 4 × 0.30 + 3 × 0.30 + 0 × 0.40 = 2.1

（2） 部門集計

（1）で計算した各回答者の第 3 階層評価項目の値を平均し、部門の 101-2-1、101-2-2、101-2-3 を計算する（表 3-1-7）。

表 3-1-7. 集計データ 2

第 3 階層	経営者層	RM 部門
101-2-1	3.7	2.9
101-2-2	4.0	2.9
101-2-3	3.2	2.9

（3）レーダーチャート作成

（2）の集計をもとに 101-2 のレーダーチャートを作成する。

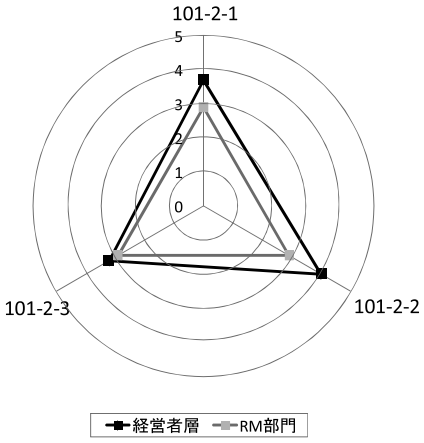


図 3-1-4. レーダーチャート例

3.1.6　レーダーチャート表示上の注意点

JRMS2010 では回答する部門ごとに用意している質問の数が異なる。このため、ある部門では存在する質問が、別の部門では存在しない場合がある。このような場合、レーダーチャートの表示が通常と異なるので注意が必要である。また、質問に対して部門の全回答者が N/A（対象外）で回答した場合も同様である。

たとえば、図 3-1-5 のレーダーチャートの場合、RM 部門は、すべての軸に対して評価レベルが存在するので 6 角形が作図されているが、経営者層は 3 角形となっている。これは、経営者層に対する 101-2-1、101-2-3、101-2-5 に関する質問が存在しないか、経営者層の回答者すべてが N/A で回答していることを示している。

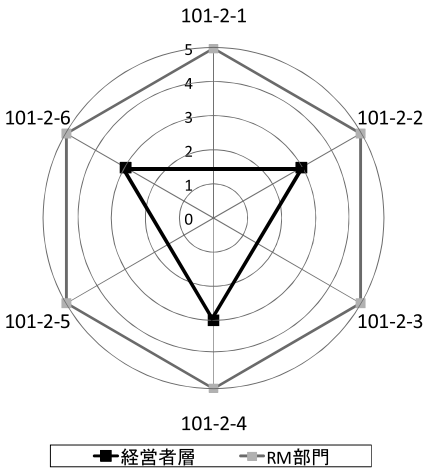


図 3-1-5. 注意が必要なレーダーチャート

3.2　JRMS ツールの利用

JRMS2010 に依拠してリスクマネジメントを実践するにあたり、重要なのは JRMS ツールをうまく利用することである。JRMS ツールは操作性・機能性等を高めているが、質問内容の理解は当然としても、ツールの使い方により組織のリスク対応の回答データの入手が期待どおりに行われない場合もある。そのため、以下に記載されている「利用手順」、「回答データの作成」、「回答データの分析」について熟知しておくことが不可欠である。

3.2.1　利用手順

JRMS ツールを組織で利用する場合の手順を以下に示す。

（1）導入準備

JRMS を導入するにあたり、以下の決定すべき事項や、協力してもらう従業員への周知事項を検討する。決定、周知事項は関係者に連絡する。

①質問セット（経営、内部統制など）の決定

リスクマネジメントの実践にあたり、対象とするリスク領域を決定し、質問セットを選択する。

②目標レベルの設定

組織の目標とする成熟度の評価レベル（目標レベル）を決定する。

回答データを分析する際に、この目標レベルと組織の現状である回答データとのギャップを検証することにより、組織の課題や問題を発見することができる。

③回答する部門、回答者の決定

回答する部門、回答者を決定する。さらに、回答者のユーザ ID、パスワードを決定し、回答者に通知する。パスワードの初期設定は変更して利用する。

④回答者への周知

回答者に評価レベル、リスクマネジメント用語、J-input の操作方法や手順を周知させる。特に評価レベルの理解が個人により大きく異なると正しい結果が得られないので、注意が必要である。

（2）事前準備

JRMS ツールのインストールや各種設定を行う。

①J-input をインストールする。

②J-analyze を分析者の PC にインストールする。

③J-analyze を使い、回答の入力や分析に使用する回答年月（以下、「現在の回答年月」という。）を設定する。本操作は、複数ある回答年月のうち、どの回答年月を利用するかを指定するものである。

回答年月は、回答データがいつ作成されたかを示すものであり、J-analyze では、同一の回答年月の回答データで部門間、部門内比較を行い、回答データを分析する。

④JRMS ツールから今回使用する質問セットを認識できるように、質問セットファイルを所定の位置にコピーする。

（3）回答データの作成

部門（経営者層、IS 部門など）に所属する回答者は、J-input を使い、組織のリスクマネジメントの現状を J-input が提示する質問に回答する。

次に、この回答を回答データとしてファイルに保存する。

（4）回答データの分析

分析者は、J-analyze を使い、個別の回答データを集計し、分析・評価するために必要となるレーダーチャートや集計表を出力する。

3.2.2　回答データの作成

回答者が J-input を使い、回答データを作成する場合の操作方法を説明する。

（1）マクロ設定の変更

J-input は Microsoft® Excel（以下、「Excel」という。）のマクロを利用して作成されている。このため、J-input を動作させるには、Excel のマクロが動作するようにマクロ設定を変更する。

なお、J-input 利用後は、変更前のマクロ設定に戻すこと。

（2）J-input の起動

回答者 PC から、J-input のプログラムファイル（J-input.xls）を起動する。

起動する前に、現在開いている Excel ファイルはすべて閉じる。

（3）ログイン

「3.2.1（1）導入準備」で通知したユーザ ID、パスワードでログインする。

図 3-2-1. J-input ログインウインドウ

(4) 質問セットの選択

左上のドロップダウンメニューから、回答する質問セットを選択する。

図 3-2-2. 回答する質問セットの選択

(5) 質問への回答

質問への回答は以下の手順で行う。

①質問への回答

質問に対し、成熟度の評価レベル（0～5）、または N/A（対象外）、D/K（わからない）で回答する。

評価レベルは、質問に対してどの程度の達成度なのかを定量的に表したものである。

②次の質問への回答

次の質問がある場合は、[次へ]をクリックし、すべての質問に回答する。

③回答データの作成

すべての質問への回答が終了したら[登録]をクリックする。

図 3-2-3. J-input メインウインドウ

［回答にあたってのヒント］

成熟度の評価レベルを確認したい	ウインドウ上部にある[回答の選択肢]をクリックする。
用語説明を見たい	質問で使われている専門用語の説明がある場合は、［用語］が表示されるので、ここをクリックする。
質問文、解説の文字が切れていて見えない、大きい文字で見たい	対象となる質問をダブルクリックすると、別ウインドウに質問、解説が表示される。
回答作業を一時中断したい	回答を一時中断する場合は、[一時保存]をクリックする。次回 J-input を起動すると、中断したところから回答入力を再開することができる。
質問番号を表示したい	[質問番号]をオンにする。質問番号は、質問をユニークに識別するための番号である。

[第 5 階層]

質問セットに第 5 層階層が存在する場合は、第 3 階層タイトルの前に「＊」が表示される。

第 5 階層の質問は Yes/No で回答し、この回答結果をもとに第 4 階層の回答を行う。

たとえば、第 5 階層の 5 つの質問に対し、3 つに Yes と回答した場合は第 4 階層の評価レベルは「2」、1 つに Yes と回答した場合は第 4 階層の評価レベルは「1」というように判断する。

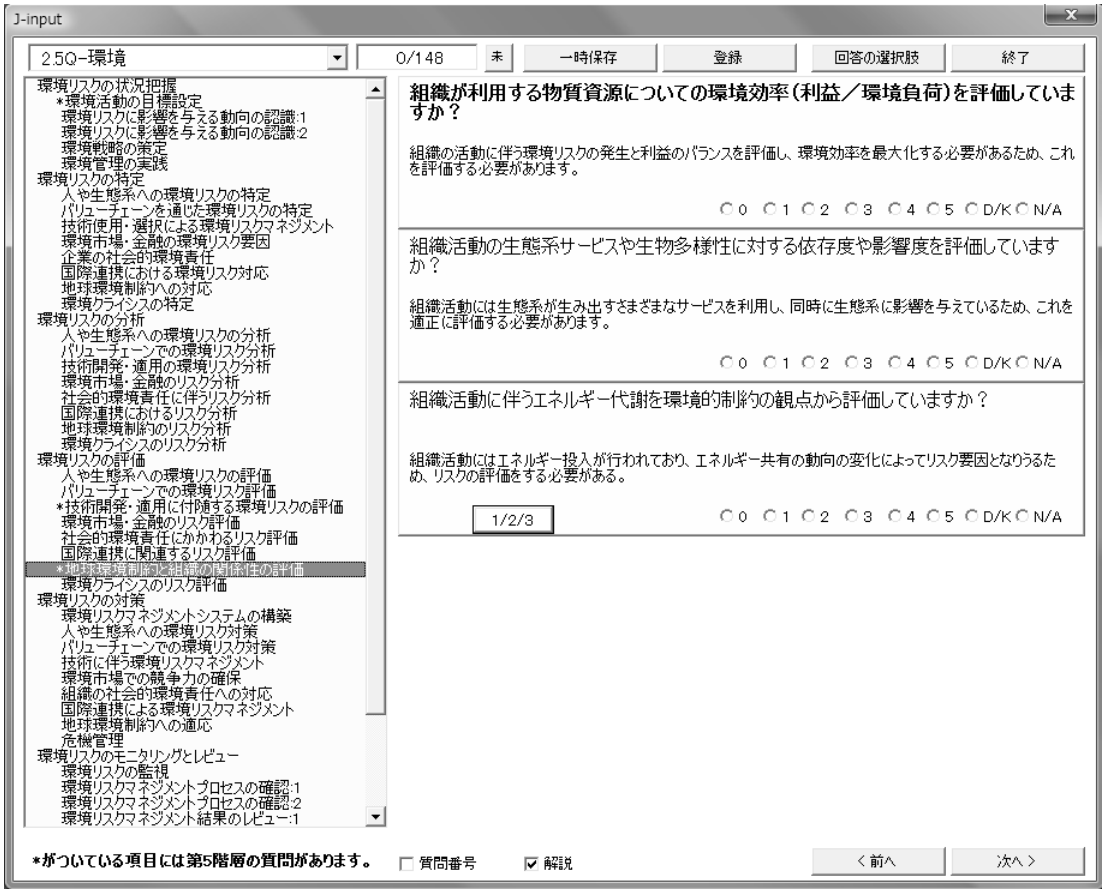


図 3-2-4. 第 5 階層がある場合の J-input メインウインドウ

第 5 階層の質問がある場合は、図 3-2-4 のように質問文の下にボタンが表示される。このボタンをクリックすると第 5 階層の質問が表示される。このボタンに表示される 3 つの数字は、第 5 階層の質問数やその回答に関する情報であり、それぞれ順番に Yes の数/回答した数／全質問数を表す。

（6） J-input の終了

[終了]をクリックする。

（7） 後処理

Excel のマクロの設定を J-input 使用前の設定に戻す。

3.2.3 回答データの分析

分析者が J-analyze を使い、レーダーチャートを作成する場合の操作方法を説明する。

①J-analyze の実行

分析者の PC にインストールした J-analyze を起動する。起動方法は、 [スタート] - [すべてのプログラム] - [JRMS2010]-[J-analyze]をクリックする。

②ログイン

分析者権限をもつユーザとしてログインすると、J-analyze メインウインドウが表示される。

本ツールでは、ユーザ ID：analyze、パスワード：analyze があらかじめ設定されている。

実際に組織に JRMS ツールを導入する場合は、この analyze ユーザのパスワードを変更して利用する。

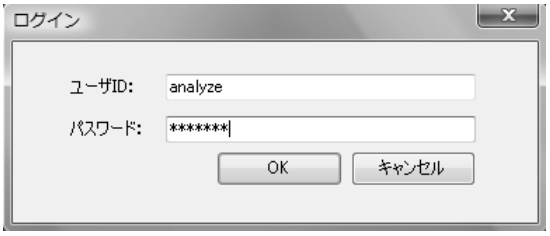


図 3-2-5. J-analyze ログインウインドウ

③集計表の出力

メニューの[出力]-[集計表]をクリックする。

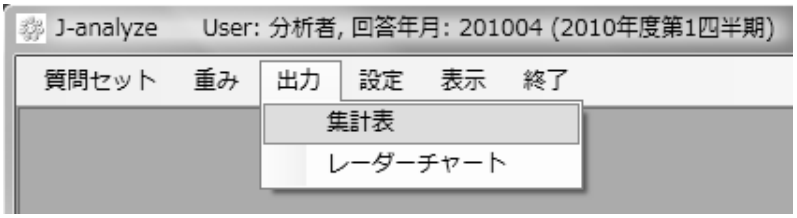


図 3-2-6. 出力メニュー

集計表を表示する際の条件である質問セット、部門、ユーザを指定する。

次に、[プレビュー]をクリックし、集計表を表示する。

質問番号	評価項目	質問	全体評価			回答詳細	
			第1層	第2層	第3層	01	02
101	経営		4.0			5.0	3.0
101-1	リスクマネジメントフレームワークの構築			4.0		5.0	3.0
101-1-1	組織の経営理念と経営目標の明示				4.0	5.0	3.0
101-1-1-1	経営理念	経営理念は組織で共有化されていますか？				5	3
101-1-1-3	経営方針と経営目標の連動	経営目標は経営方針を反映していますか？				5	3
101-1-1-5	経営目標の優先度	経営目標の優先順位は明らかですか？				5	3
101-2	リスクマネジメントの基盤			4.0		5.0	3.0
101-2-1	リスクマネジメント方針				4.0	5.0	3.0
101-2-1-1	経営理念との連動	リスクマネジメント方針は経営方針を反映していますか？				5	3
101-2-1-2	マネジメント方針の確立	リスクマネジメント方針は達成すべき経営目標にふさわしい内容になっていますか？				5	3
101-2-1-3	理解状況の確認	リスクマネジメント方針は、全社員が知っていますか？				5	3
101-2-2	リスクマネジメント				4.0	5.0	3.0
101-2-2-1	リスクマネジメント計画	RM計画は、リスクマネジメント方針に基づいて策定されていますか？				5	3
101-2-2-4	資源の把握	RM計画達成に必要な資源について検討されていますか？				5	3
101-2-2-5	コンプライアンス計画	コンプライアンスに関する対応がリスクマネジメントに入っていますか？				5	3
101-3	リスクアセスメント			4.0		5.0	3.0
101-3-1	リスクの特定				4.0	5.0	3.0

図 3-2-7. 集計表出力ウインドウ

④レーダーチャートの出力

メニューの[出力]-[レーダーチャート]をクリックする。

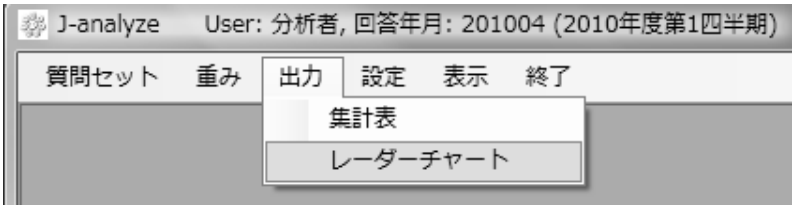


図 3-2-8. 出力メニュー

レーダーチャートを表示する質問セットの階層、部門、ユーザ（省略可能）を指定して[プレビュー]をクリックする。

図 3-2-9. レーダーチャートウインドウ

⑤終了

メニューの[終了]をクリックし、J-analyze を終了する。

４．JRMS 分析例

本章では JRMS2010 を使って、組織におけるリスクマネジメントの実態を把握するため、JRMS ツールの回答結果であるレーダーチャートの分析方法を具体的な例をあげて説明する。

4.1　分析・評価結果の見方

JRMS2010 は、組織にとり、よりよいリスクマネジメントを実践するためのシステムである。組織が JRMS ツールを本文 3 章「3.2　JRMS ツールの利用」に従い、質問に回答し、その回答結果により評価することこそがこの JRMS2010 活用の根幹にあると言える。

4.1.1　組織の構成

組織はさまざまな構成要素からなっている。JRMS2010 では、経営者層、リスクマネジメント（RM）部門、ユーザ部門（業務内容に応じて表記の仕方は、ユーザ 1、ユーザ 2 部門等に区分）の部門構成を想定している。特にリスクマネジメントの実態を分析するためには、組織として回答結果を集計・分析・評価を行う部門（ここでは RM 部門）を確定しておくことが必要である。なお、JRMS2010 を利用する組織においては、業種・規模・活動範囲等によりリスクマネジメントの分析範囲を規定し、内部的に分けながら JRMS ツールを使用する場合も出てくると思われる。

4.1.2　分析の視点

組織が展開しているリスクマネジメントの実態がいかなる成熟度にあるかを認識することは、現在の組織運営においてきわめて重要な意味を有している。とりわけグローバルに事業展開をしている組織では、国内組織と国外組織の成熟度の差異は、企業にとって死活問題を生み出す原因となる場合もある。そのため、リスクマネジメントの成熟度をどの評価レベルに設定するか、いわば目標レベルをまず決め、従業員にこの点を周知徹底させておくことが必要不可欠である。従業員間における認識がバラバラであれば、統一のとれたリスク対応はおぼつかなくなる。また、回答者のこれまでの経歴、リスクに対する関心度、事実認識、質問項目の理解度によりギャップが生じることがある。分析者はレーダーチャートを通して、ギャップの発生を当然と考えるのか、または組織を脅かす原因となるのかを見極めることが肝心である。

リスクマネジメントの実践には、従業員がリスクマネジメントに関し、共通の認識を有していることが望ましいと言える。この点は、経営者層と現場のユーザ部門とで同一の目標レベルを定める場合にあてはまると言える。

なお、本章の分析例は、ある程度リスクマネジメントを理解していることを前提として示した

ものである。

（1）組織としての目標レベル

組織として、少なくとも出発点として成熟度における「評価レベル 3」を設定しておくことがよいと思われる。

しかし、特定部門の役割の違いにより異なる目標レベルを設定する可能性がある。その場合には、当然のことながら、それなりの理由について関係者にその認識をもってもらうことが重要である。

（2）目標レベル設定の意味

経営者層、RM 部門、ユーザ部門等における JRMS2010 質問への回答者の回答結果には重要な情報が少なくとも 2 つ含まれている。1 つはそれぞれの部門間の回答ギャップであり、もう 1 つは同部門の回答者間の回答ギャップの存在である。

これらのギャップこそ、組織のリスクマネジメントの実態を反映する情報となる。重要なのは、少なくとも同じ部門に属する回答者の間では、同じ質問に対してギャップの少ない回答結果が得られることが望ましいと言える。

4.1.3　評価レベルの結果

レーダーチャートの評価は目標レベルを基準として行われることになる。仮に、経営者層の回答結果が目標レベルに設定したレベル 3 を大きく下回るようであれば、組織としてどうであろうか。これは組織としての脆弱性を表していると言えよう。この場合、評価結果と目標レベルとのギャップについて原因を究明し、経営者は問題の所在を解明し、改善を行うことが求められるべきである。こうしたギャップも、単に質問の読み違いといった単純なものであれば改善も容易であるが、みずからの思い込みの違いや認識の差であれば、それなりの対応が求められる。こうした側面は、他の部門である RM 部門、ユーザ部門でも同様と言える。

なお、部門内におけるギャップのほかに、他部門との比較において明らかにされるギャップについては、全部門共通の目標レベルに基づく場合であれば、上記同様にその原因を探り出し、たとえば部内教育で解決できれば改善を促すよう、手配を行う必要があるだろう。

しかし、特定の部門について異なる目標レベルを有している場合には、目標レベルを上回る場合はともかくも、下回る場合にはギャップの読み方に注意が必要である。したがって、ギャップの原因究明とともに、組織のあり様にもメスを入れる必要も出てくるかもしれない。こうした側面は、情報システムが異なる組織との合併の場合等に生ずる可能性がある。

いずれにしても JRMS2010 では、リスクマネジメントを展開する各リスク領域の質問に回答し、評価することになっている。そのため、リスク領域ごとにリスクアセスメントにおけるリスクの特定、分析、評価、対策についての回答結果から描き出されたレーダーチャート、および回答結果を通して組織における課題や弱点を分析するのである。

4.2　分析・評価例

ここでは JRMS2010 を用いて組織のリスクマネジメントの実態をいかに把握し、改善の方途を見いだすための分析例を示す。

ここで取り上げるのは、経営、情報システム、個人情報保護、医療の各領域である。それぞれについて参考とすべく、特定の質問項目の回答結果により描かれたレーダーチャートをもとに、組織における部門間・回答者間のギャップを含め、分析の視点等を例示している。

4.2.1　経営

本節では、「経営」に関する回答結果のレーダーチャートを参考として、「経営」分野の分析事例を示す。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 1 つとして参照していただきたい。

4.2.1.1　経営に関するリスクマネジメントの状況分析の前提と視点

（1）対象組織の前提

①組織の構造は、経営者層、リスクマネジメントを推進する RM 部門、ユーザ部門（業務の内容に応じてユーザ 1、2 部門等により区分する）の 3 部門に分けて評価を行ったものとする。

②分析に際し、対象組織はすべての部門において評価レベル 3 以上を目標としている、という前提とする。

（2）分析の視点

①組織のリスクマネジメントレベルの評価においては、各部門はこの組織の目標であるレベル 3 を基準として評価を行う。

②各部門の評価のギャップを分析することにより、組織におけるマネジメントシステムとしての課題を明らかにする。

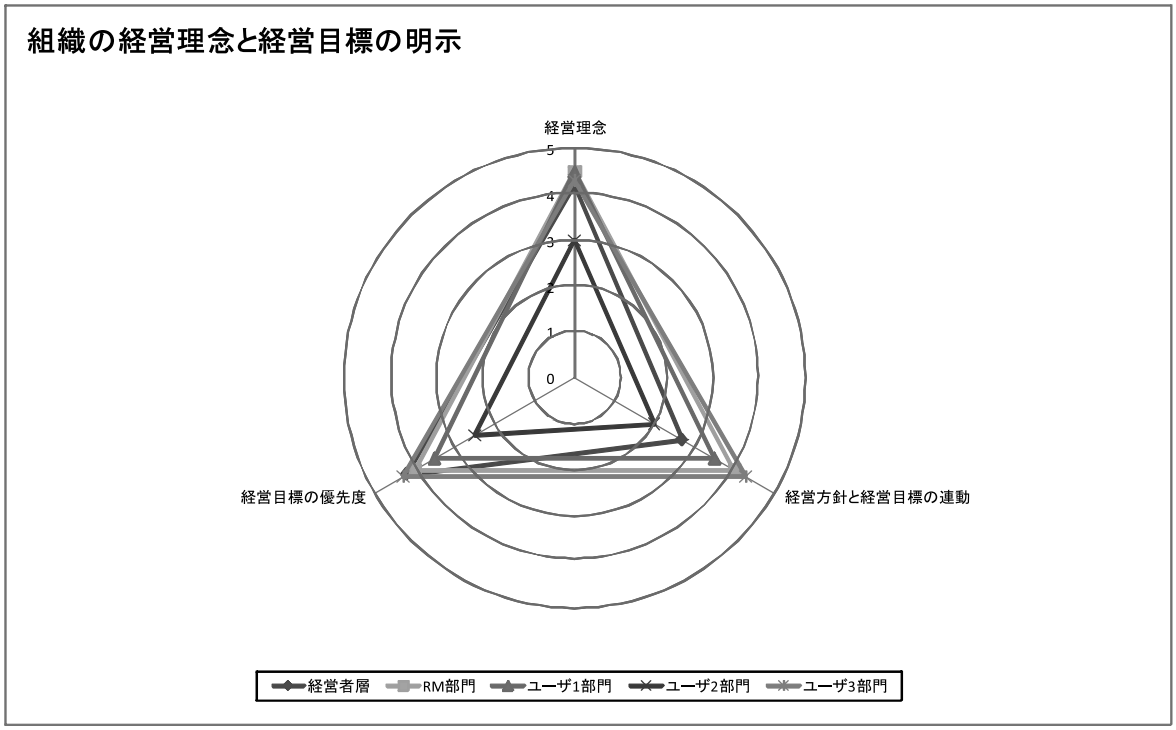
③評価レベルの分布状況から、各部門のリスクマネジメントの実施上の弱点を明らかにする。

4.2.1.2　ギャップ分析による課題の解明

ギャップ分析の重要性は、組織のリスクマネジメントにとり課題の所在を知ることができる点にある。

○チャート事例 1：組織の経営理念と経営目標の明示

	経営者層	RM 部門	ユーザ 1 部門	ユーザ 2 部門	ユーザ 3 部門
経営理念	4.2	4.5	4.5	3.0	4.3
経営方針と経営目標の連動	2.7	4.0	3.5	2.0	4.3
経営目標の優先度	4.2	4.0	3.5	2.5	4.3



ここで評価されている対象はリスクマネジメントの大前提となる項目[28]である。したがって、この評価対象項目において、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。

その点でみると、「経営方針と経営目標の連動」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が、「経営方針と経営目標の連動」に関する理解が共有されていないことを示している。

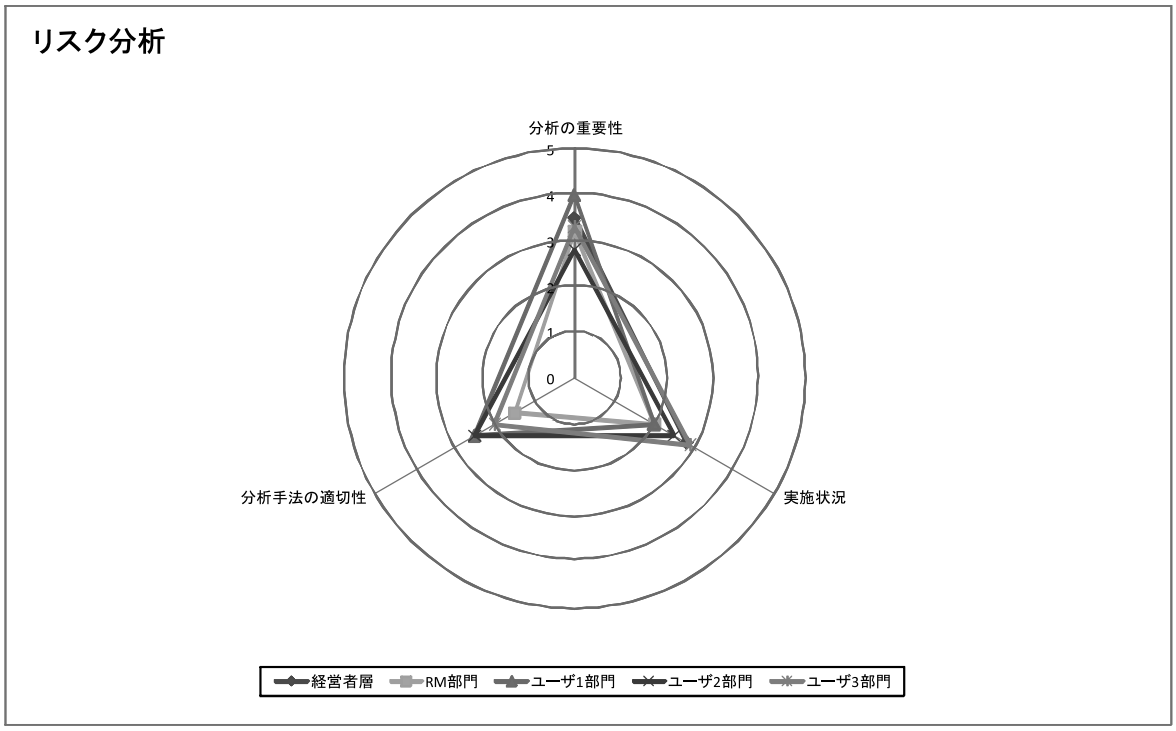
さらには、3 つのユーザ部門間でリスクマネジメントの大前提となる経営理念や経営方針ならびに経営目標の理解に関して大きな差があること自体が、この項目に関する組織自体の問題点を表している。

4.2.1.3　組織のレベル

○チャート事例 2：リスク分析

	経営者層	RM 部門	ユーザ 1 部門	ユーザ 2 部門	ユーザ 3 部門
分析の重要性	3.3	3.2	4.0	2.8	3.5
実施状況	2.9	2.0	2.0	2.5	2.8
分析手法の適切性	-	1.5	2.5	2.5	2.0

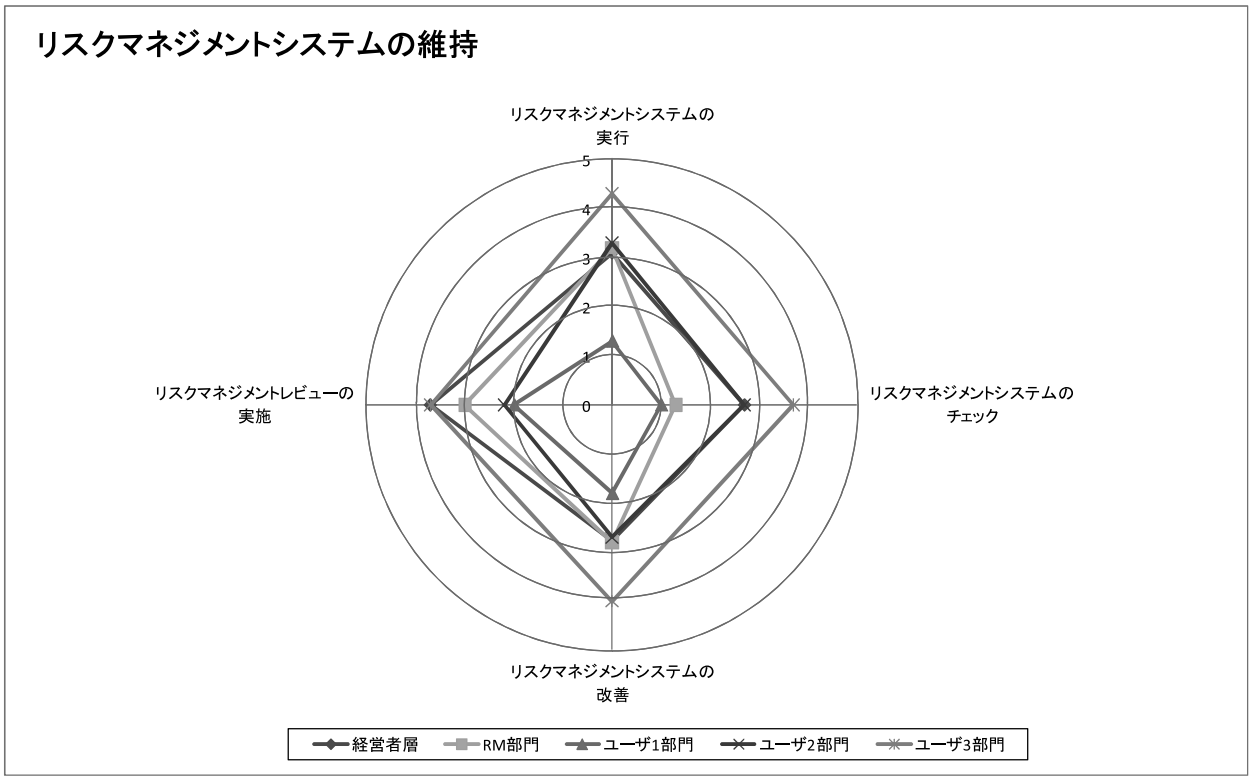
[28]　第 3 階層、第 2 階層のタイトル（軸名）を指している。



このチャート事例では、「分析の重要性」以外の評価が低いレベルにとどまっている。分析活動が、組織的に計画され、必要な教育が実施されていれば、「分析の重要性」と「実施状況」や「分析手法の適切性」に関してこのようにギャップが生じることはないはずである。したがって、このようなことは、分析活動がその必要性だけを説明され、その後は各人が個人の経験に基づいて実施している状況であり、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。

○チャート事例 3：リスクマネジメントシステムの維持

	経営者層	RM 部門	ユーザ 1 部門	ユーザ 2 部門	ユーザ 3 部門
リスクマネジメントシステムの実行	3.1	3.2	1.3	3.3	4.3
リスクマネジメントシステムのチェック	2.7	1.3	1.0	2.7	3.7
リスクマネジメントシステムの改善	2.8	2.8	1.8	2.7	4.0
リスクマネジメントレビューの実施	3.7	3.0	2.0	2.2	3.7



この事例では、ユーザ 3 部門の相対的な高さに比べ、ユーザ 1 部門の低さが気になるところである。経営者層に比べて相対的に他の部門の評価が低いのは、リスクマネジメントシステム維持の実効性が現場には実感されていないということであり、マネジメントシステムの運営の実態が乏しい可能性がある。

特に、「リスクマネジメントシステムの実行」、「リスクマネジメントレビューの実施」に比べて「リスクマネジメントシステムのチェック」の評価がユーザ 3 部門を除いて低いのは、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に反映されていない可能性を示している。

なお、ユーザ 3 部門の評価は相対的に高いが、これは、ユーザ 3 部門担当の特定分野だけが対策が高いレベルをもっているのか、逆に対策の十分性ということに関して、ユーザ 3 部門の理解が十分でないため評価が高くなっている、という 2 つの可能性が考えられる。

4.2.2　情報システム

ケーススタディは、図 4-1-1 に示す A 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、経営者層、RM 部門、IS 部門、現場部門（ユーザ部門）におけるリスクへの対応が描かれている。

・A 企業は、スポーツセンタを経営しており、会員の健康情報や体力情報などを管理する情報システムを導入している。しかし、リスクマネジメントが十分ではなく、一部会員の個人情報を漏えいしてしまった。現場や RM 部門では、スポーツインストラクタの個人情報の取扱いでヒヤリ・ハットが起きていたが、企業としての RM 体制ができておらず、現場や情報システムでの対応を実施してこなかった。このため、経営者は、事件後、現場の状況を考慮することもなく対症療法的に厳しい制限を付けることにした。 この結果、現場では過剰な対策がとられ、表面的な対応で取り繕った。また、厳しいセキュリティを無理やり情報システムに導入したため、トラブルが多発して、情報システムのセキュリティシステムがダウンして、会員管理ができなくなるという第 2 の事件を起こしてしまった。
・経営者は、現場の対応や情報システムの運用の現実を見て、本格的にリスクマネジメントシステムを導入することにした。

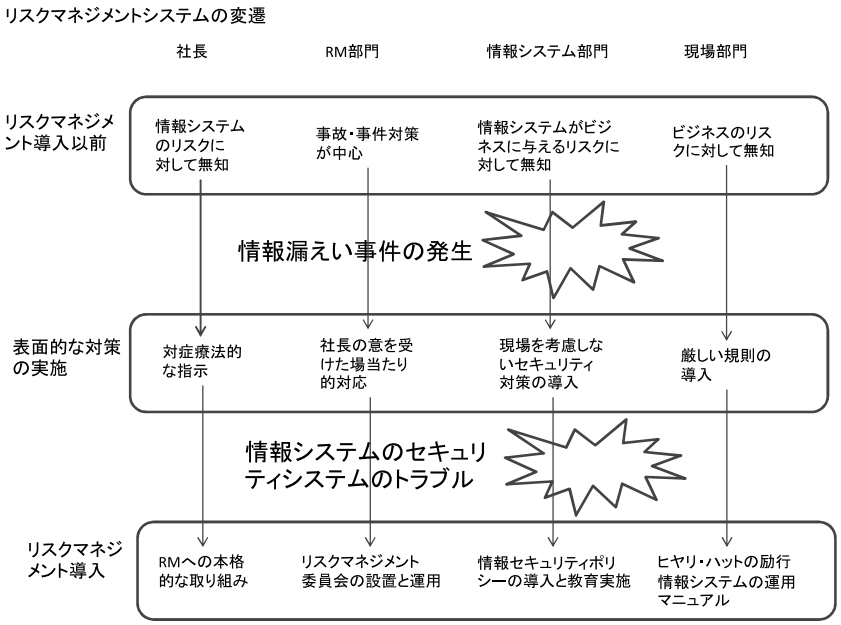
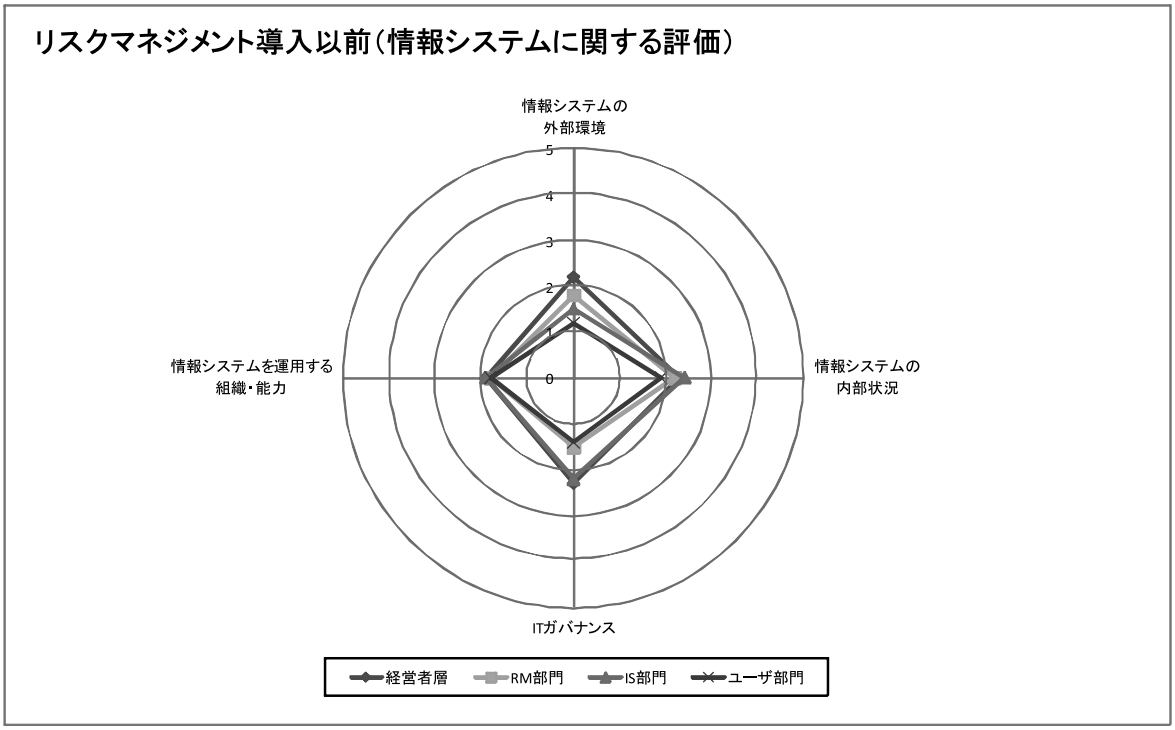


図 4-1-1. A 企業のリスクマネジメントを導入するまでの段階

ここでは、4 人から 6 人程度のグループに分かれ、企業の社長、RM 部長、現場マネジャー、IS 部門長に分かれて情報システムに関して評価する事例について述べる。

○チャート事例 1：リスクマネジメント導入以前（情報システムに関する評価）

	経営者層	RM 部門	IS 部門	ユーザ部門
情報システムの外部環境	2.2	1.8	1.5	1.2
情報システムの内部状況	2.3	2.2	2.4	1.9
IT ガバナンス	2.3	1.5	2.2	1.4
情報システムを運用する組織・能力	1.9	1.8	1.9	1.8

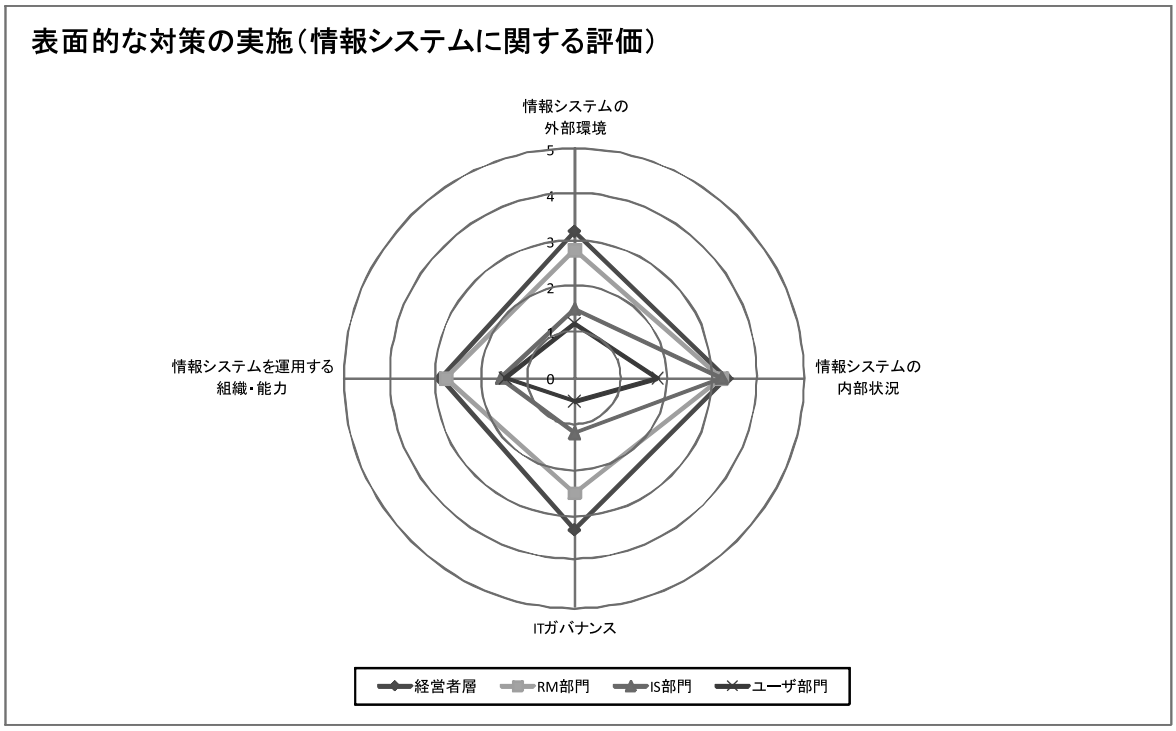


この段階では、経営者層が楽観的すぎる点が見てとれる。特に、「IT ガバナンス」と「情報システムの外部環境」に関しては、経営者層の甘い評価が見てとれる。

一方、RM 部門では「IT ガバナンス」は低く見ているものの、「情報システムの外部状況」に関して甘い見方をしていることがわかる。また、全社的に「情報システムの内部状況」について、あまり差が見られない。さらに、「情報システムを運用する組織・能力」を 1.8 と評価しており、情報システムに関して、組織として十分と錯覚している様子がうかがえる。この分析からは、情報システムの外部環境を十分に理解しておらず、IT に対するガバナンスも不十分ななか、情報システムの問題について、軽視していることがわかる。

○チャート事例 2：表面的な対策の実施（情報システムに関する評価）

	経営者層	RM 部門	IS 部門	ユーザ部門
情報システムの外部環境	3.2	2.8	1.5	1.2
情報システムの内部状況	3.3	3.2	3.2	1.8
IT ガバナンス	3.3	2.5	1.2	0.5
情報システムを運用する組織・能力	2.9	2.8	1.6	1.5



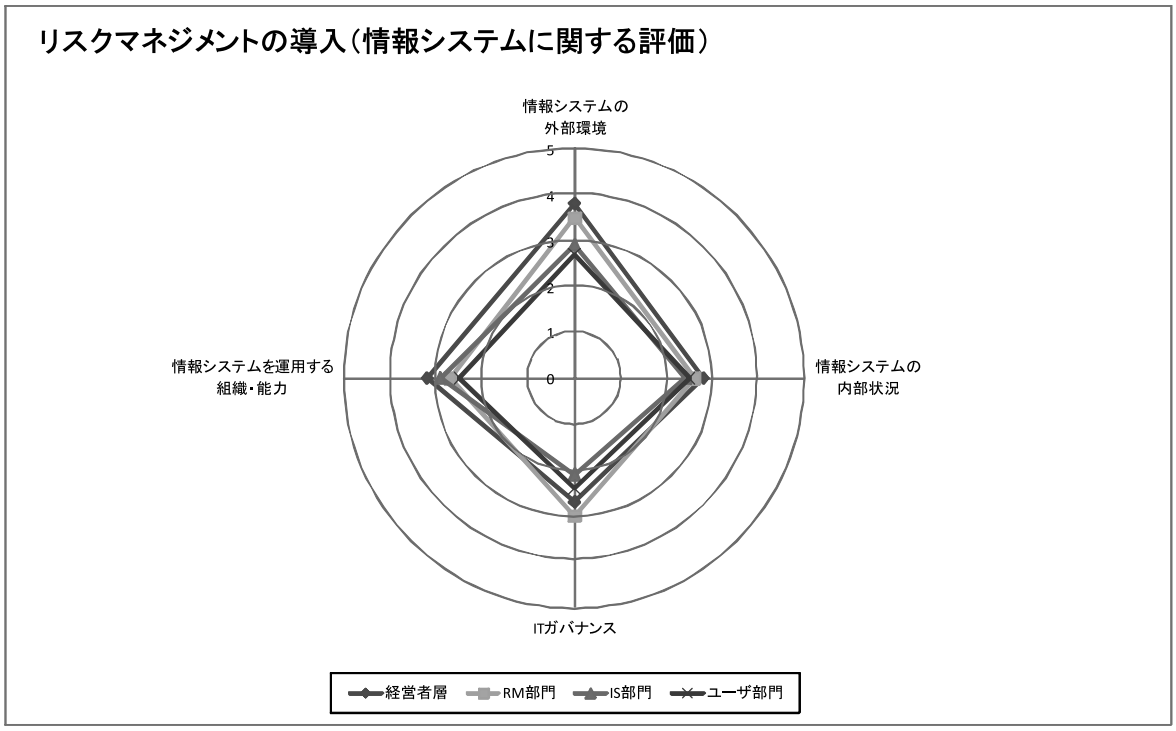
この段階では、経営者層が情報漏えいを経験して、慌てて全社に対策をとらせたことがわかる。特に経営者層と RM 部門は、「情報システムの外部環境」、「情報システムの内部状況」、「情報システムを運用する組織・能力」の点でほぼ一致している。すなわち、全社的なマネジメントを実施して問題解決したと楽観視しており、現場の本当のリスクを理解できていない。

一方、IS 部門とユーザ部門は、事件をきっかけに現実を共有しており、「情報システムの外部環境」、「情報システムを運用する組織・能力」については現実を厳しく見ていることがわかる。しかし、「情報システムの内部状況」については、IS 部門は理解しているものの、他の部門は実態が見えていない。「IT ガバナンス」は大きく差が出ており、IT について経営者層が何をすべきか、RM 部門、IS 部門とユーザ部門が何をすべきかがバラバラな状態となっていて、社内で混乱があることがうかがえる。

この状態で、経営者層が、IS 部門やユーザ部門の現場に命令しても、経営者層が意図したような結果は期待できず、リスクが大きい状態となっている。

○チャート事例 3：リスクマネジメントの導入（情報システムに関する評価）

	経営者層	RM 部門	IS 部門	ユーザ部門
情報システムの外部環境	3.8	3.5	2.9	2.7
情報システムの内部状況	2.8	2.6	2.4	2.5
IT ガバナンス	2.7	3.0	2.1	2.4
情報システムを運用する組織・能力"	3.2	2.7	2.9	2.5



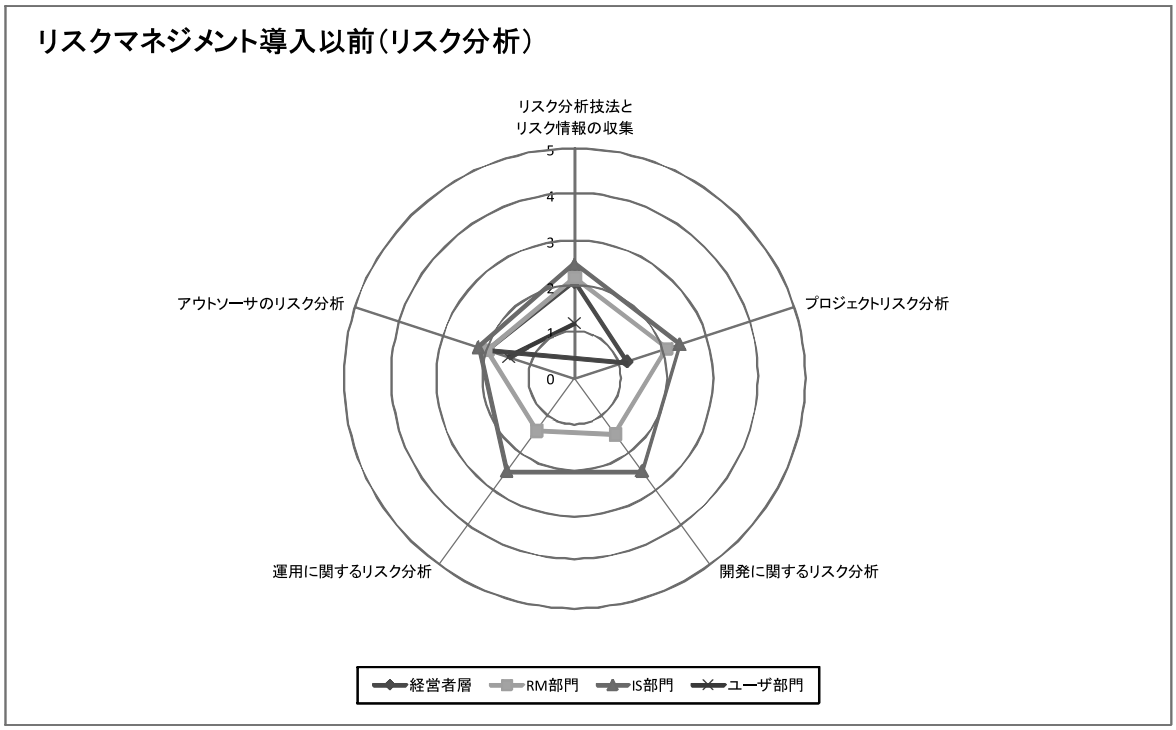
この図では、経営者層、RM 部門、IS 部門、ユーザ部門間での「情報システムの外部環境」、「情報システムの内部状況」、「情報システムを運用する組織・能力」、「IT ガバナンス」のギャップが小さくなり、リスクに対する改善が実施されていることがわかる。これは、前段階では経営者層や RM 部門が現場のリスクを理解できていなかったものの、第 2 の事件を介して、実際の現場を知って対策をとった成果が示されている。また、多くの評価レベルが 3 を超えたり、3 に近いことから、組織としての IT に対するマネジメントが機能するようになったことがわかる。ただ、「IT ガバナンス」については、まだ、IS 部門やユーザ部門の成熟度が経営者層に比べて低いことから、今後も改善していく必要がある。

次に、3 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のかがわかる。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と比較すると、RM 部門とユーザ部門では、リスクに関して改善していることがわかる。しかし、経営者層は、リスクマネジメントの導入段階では、表面的な対策の実施のときより「情報システムの内部状況」、「情報システムを運用する組織・能力」、「IT ガバナンス」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とらわれていると、正しい対応がなされた事実を見逃す可能性があるので注意してもらいたい。これらの考察から、A 社では、リスクマネジメントが導入され、それなりに組織の情報システムのリスクマネジメント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、組織、維持、リスク分析・対策について、企業での対応を示したものである。

○チャート事例 4：リスクマネジメント導入以前（リスク分析）

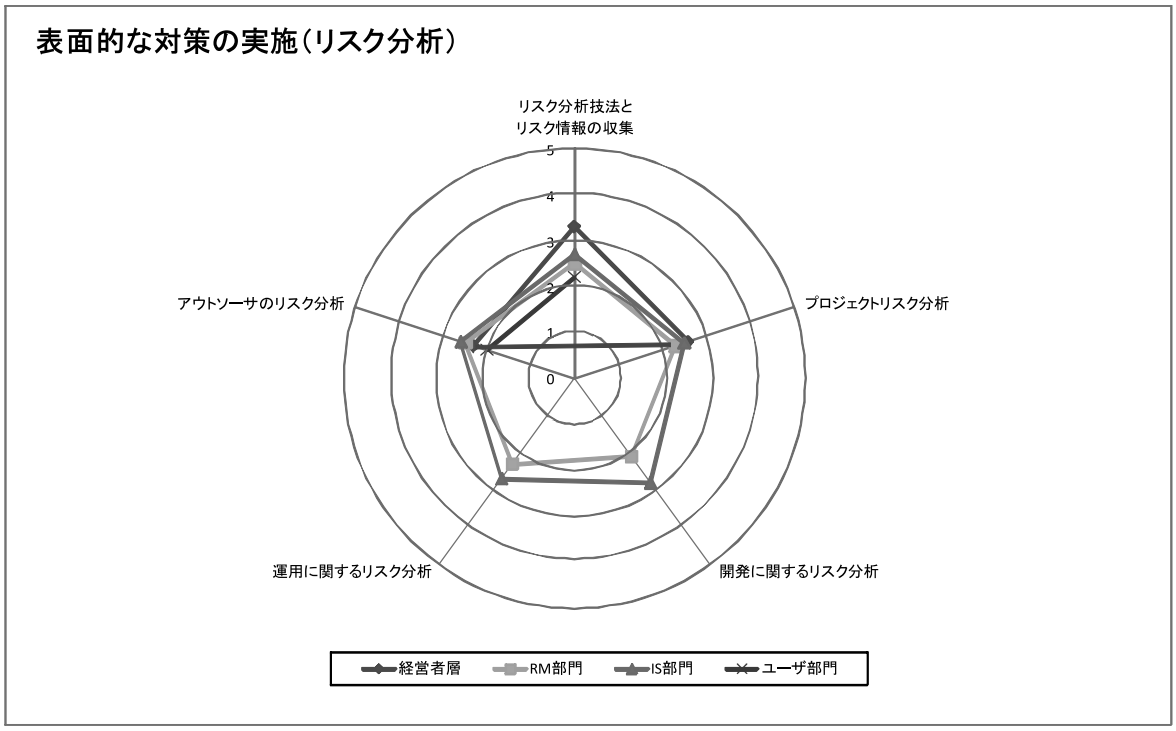
	経営者層	RM 部門	IS 部門	ユーザ部門
リスク分析技法とリスク情報の収集	2.1	2.2	2.5	1.2
プロジェクトリスク分析	1.2	2.1	2.4	-
開発に関するリスク分析	-	1.5	2.5	-
運用に関するリスク分析	-	1.4	2.5	-
アウトソーサのリスク分析	2	2	2.2	1.5



この段階では、経営者層は「プロジェクトリスク分析」、「リスク分析技法とリスク情報の収集」、「アウトソーサのリスク分析」について答えているが、その評価結果は低く、ほとんど関心をもっていないことがわかる。また、RM 部門も、経営者層の関心がないため、「プロジェクトリスク分析」、「開発に関するリスク分析」、「運用に関するリスク分析」、「アウトソーサのリスク分析」が低い。IS 部門は、事件が情報システムに関することであり、全体のなかでは成熟度が相対的に高い。しかし、成熟度が 2.5 程度であり、十分なものとなっていない。このような企業の状態では、組織的なリスクマネジメントがうまくいくはずがない。その結果として、問題が起きて対応できなかったことが見てとれる。

○チャート事例 5：表面的な対策の実施

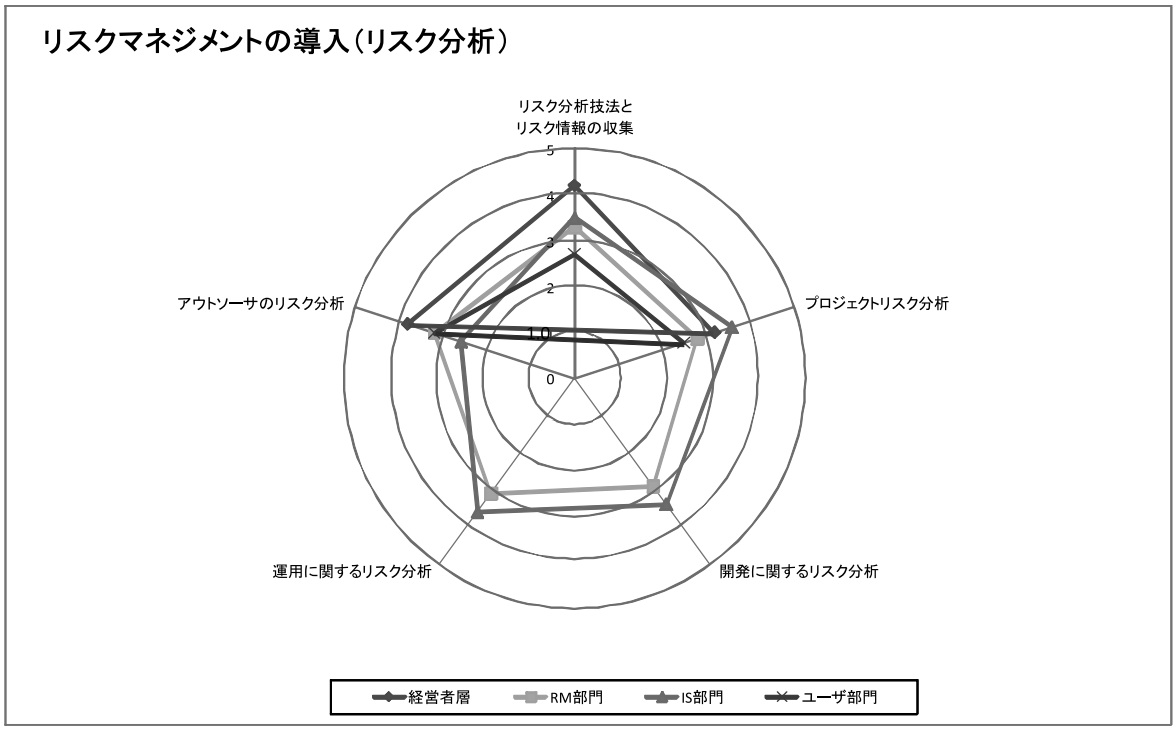
	経営者層	RM 部門	IS 部門	ユーザ部門
リスク分析技法とリスク情報の収集	3.3	2.5	2.7	2.2
プロジェクトリスク分析	2.6	2.3	2.5	-
開発に関するリスク分析	-	2.1	2.8	-
運用に関するリスク分析	-	2.3	2.7	-
アウトソーサのリスク分析	2.3	2.5	2.6	2.0



この段階では、経営者層は、問題が発生したことから、慌てて対症療法に走ったことが「リスク分析技法とリスク情報の収集」と「プロジェクトリスク分析」が突出していることからもわかる。事件が起きて、RM 部門、IS 部門は関係者として「プロジェクトリスク分析」、「リスク分析技法とリスク情報の収集」、「開発に関するリスク分析」、「運用に関するリスク分析」、「アウトソーサのリスク分析」の全体が改善されていることがわかる。一方、ユーザ部門にとっては、本当のリスクがユーザ部門にあることから「プロジェクトリスク分析」、「リスク分析技法とリスク情報の収集」が他の部門と比べて低くなっている。すなわち、このユーザ部門のリスクがぬぐえていないことが見てとれる。これにより、企業としてユーザ部門にリスクが残存していることがわかる。なお、ユーザ部門を除くと、評価レベルは 2.7 から 3.3 となっており、一部、組織的なリスクマネジメントが回り始めていることがわかる。しかし、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おらず、したがって、第 2 の事件が起きる可能性が見てとれる。

○チャート事例 6：リスクマネジメントの導入

	経営者層	RM 部門	IS 部門	ユーザ部門
リスク分析技法とリスク情報の収集	4.2	3.3	3.5	2.7
プロジェクトリスク分析	3.2	2.8	3.6	2.5
開発に関するリスク分析	-	2.9	3.4	-
運用に関するリスク分析	-	3.1	3.6	-
アウトソーサのリスク分析	3.8	3.2	2.6	3.2



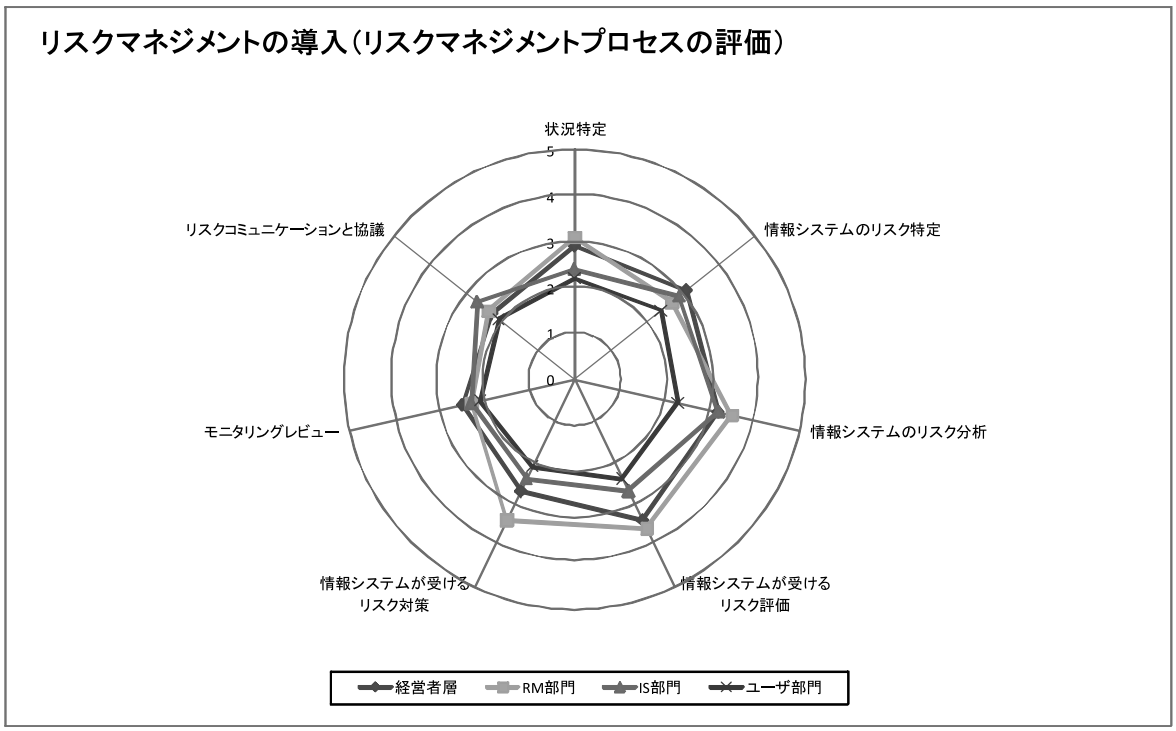
この段階では、経営者層、RM 部門、IS 部門、ユーザ部門間でのギャップが小さくなり、リスクに対する大きな改善が図られているのがわかる。特に「プロジェクトリスク分析」でのギャップが小さくなり、情報システムのプロジェクトの重要性が RM 部門、経営者層やユーザ部門に認知され、組織として機能し始めたことがわかる。「開発に関するリスク分析」や「運用に関するリスク分析」においても評価レベルが 3 を超えており、RM 部門と IS 部門の認識ギャップが小さくなっていることから、リスク対応が組織的になったことがわかる。

次に、組織の情報システムに関する 3 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、リスクマネジメントの導入に向けて、順次改善していることがわかる。

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う。その際、まず、部門ごと、時点ごとに、個別のリスクマネジメントへの対応状況を分析する。次に、時系列に、リスクマネジメントへの対応がどのように変化したかを分析する。また、部門が異なることで、リスクとなるところについてもあわせて分析する。最後に、これらを総合的に分析して、改善案とその優先度を決めて、総合的な対策を提言することができる。

○チャート事例 7：リスクマネジメントの導入（リスクマネジメントプロセスの評価）

	経営者層	RM 部門	IS 部門	ユーザ部門
状況特定	2.9	3.1	2.4	2.2
情報システムのリスク特定	3.1	2.7	2.9	2.4
情報システムのリスク分析	3.2	3.5	3.2	2.3
情報システムが受けるリスク評価	3.4	3.6	2.7	2.4
情報システムが受けるリスク対策	2.7	3.4	2.4	2.1
モニタリングレビュー	2.5	2.3	2.3	2.1
リスクコミュニケーションと協議	2.3	2.4	2.7	2.1



この段階で 7 つのリスクマネジメントプロセスを評価した。「状況特定」では経営者層と RM 部門が高く、IS 部門とユーザ部門が低い。評価レベルも 3 となっておらず、両者が状況を十分に理解していない。「情報システムのリスク特定」では、ユーザ部門が低いが、経営者層、RM 部門、IS 部門はほぼ近い値であり、リスクを特定できていると考えられる。「情報システムのリスク分析」ではユーザ部門が低く、経営者層、RM 部門、IS 部門はほぼ近い値であり、リスク特定とほぼ同じとなっている。「情報システムが受けるリスク評価」では、経営者層と RM 部門が高く、IS 部門とユーザ部門が低い。情報システムに対するリスクをどのように見るかについては経営者層や RM 部門と意見の相違があるように見える。「情報システムが受けるリスク対策」では、RM 部門が高く、経営者層、IS 部門、ユーザ部門がほぼ同様となっている。RM 部門が単独で高い数値を示しているのは、リスク対策がとられればよい、と安易に考えている懸念があるのでチェックすべきであろう。

さて、「モニタリングレビュー」と「リスクコミュニケーションと協議」の 2 つは、経営者層、RM 部門、IS 部門、ユーザ部門のすべての評価が低い。この企業の情報システムの場合、ようやくリスクマネジメントが導入されて回り始めた段階であり、まだモニタリングが機能していない

ことがわかる。今後、マネジメントをきちんと展開していくためにはモニタリングを機能させることが必要であろう。「リスクコミュニケーションと協議」については新しい概念であり、この程度でもやむを得ないであろう。今後、この企業はリスクコミュニケーションを通じてリスク情報を共有すべきであろう。

4.2.3　個人情報保護

本節では、「個人情報保護」に関する回答のレーダーチャートをもとに「個人情報保護」分野の分析の一事例を示す。ギャップの発生原因はさまざまであるため、本分析事例は評価の一事例として参照していただきたい。

4.2.3.1　個人情報保護に関するリスクマネジメントの状況分析の前提と視点

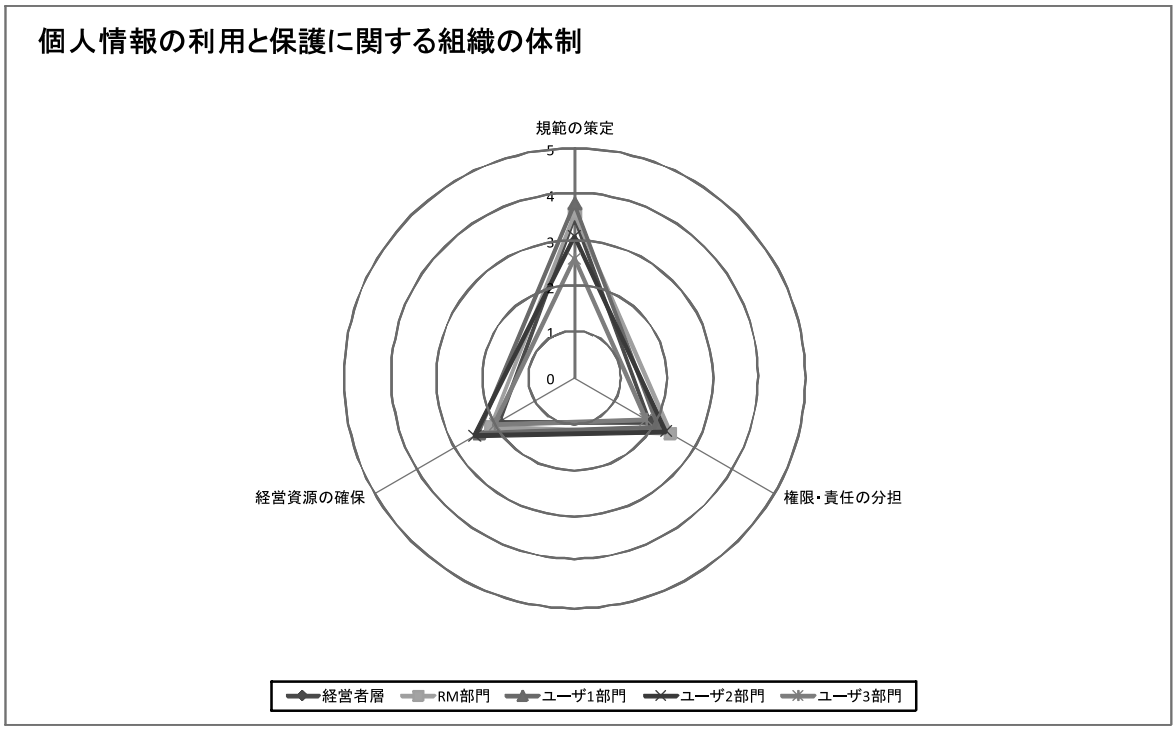
（1）対象組織の前提
①組織の構造は、経営者層、RM 部門、ユーザ部門の 3 部門からなること。
②対象組織の全部門がレベル 3 以上を目標としていること。

（2）分析の視点
①組織のリスクマネジメントレベルの評価にあたっては、各部門はこの組織の目標であるレベル 3 を基準として評価を行う。
②各部門の評価のギャップを分析することによって、組織におけるマネジメントシステムの課題を明らかにする。
③評価レベルの分布状況から、各部門のリスクマネジメントの実施上の弱点を明らかにする。

4.2.3.2　組織のレベル

○チャート事例１：個人情報の利用と保護に関する組織の体制

	経営者層	RM 部門	ユーザ 1 部門	ユーザ 2 部門	ユーザ 3 部門
規範の策定	3.5	3.6	3.8	3.1	2.6
権限・責任の分担	1.9	2.4	2.1	2.3	1.8
経営資源の確保	1.9	2.1	2.4	2.5	2.0

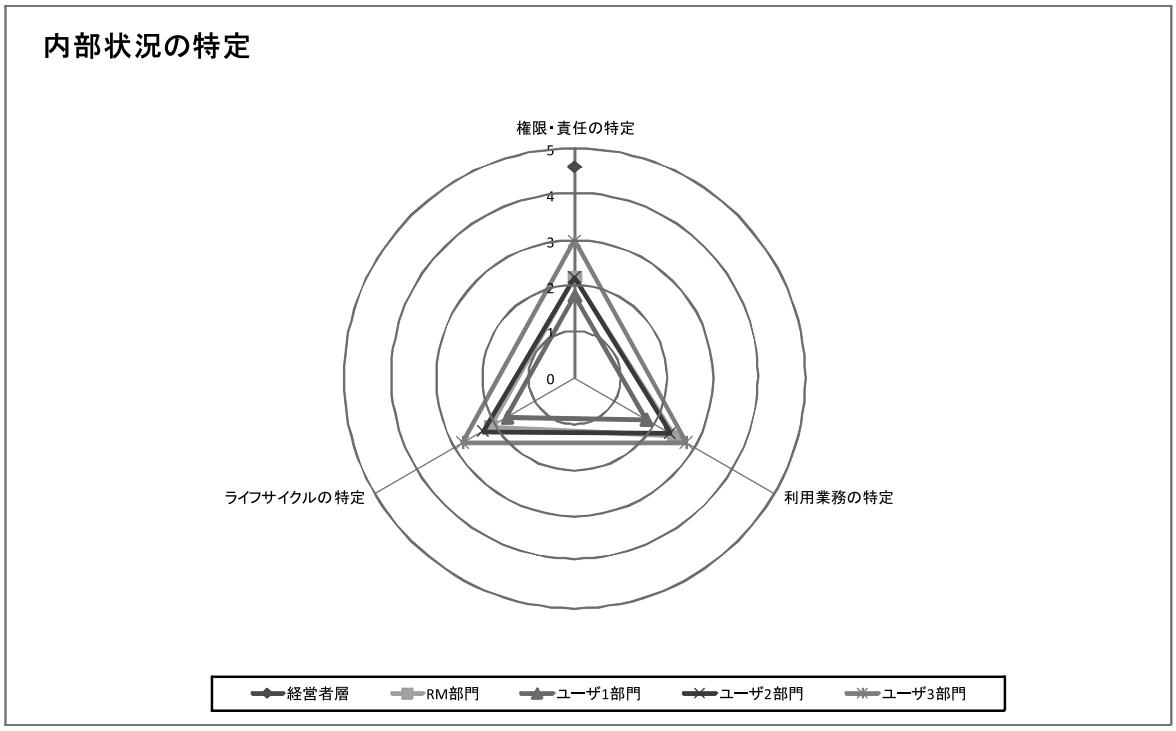


この事例では、「規範の策定」以外の評価項目がレベル 3 未満にとどまっている。このことから、この組織の個人情報の利用と保護に関する組織の体制整備は、「規範の策定」を除き、組織が目的とするレベル 3 に至っていないことが見てとれる。また、このように、あるポイントのレベルだけが高いとき、低いときには、なぜそのような差が生まれるのかを検討することが望まれる。たとえば、この事例でいえば、なぜ「規範の策定」だけがレベル 3 以上なのかの検討が求められる。その結果、ただ単に規範を存在させるだけの取組みに重点が置かれていることが判明する可能性も否定できないであろう。

4.2.3.3　ギャップ分析による課題の解明

○チャート事例 2：内部状況の特定

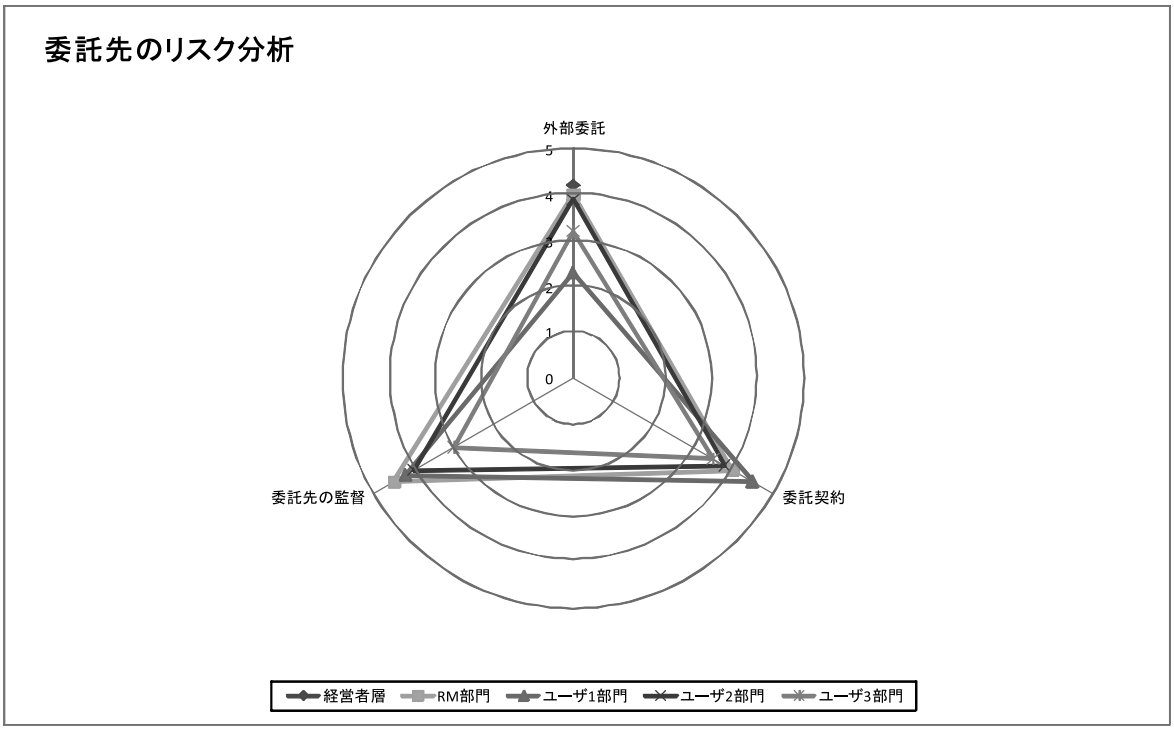
	経営者層	RM 部門	ユーザ 1 部門	ユーザ 2 部門	ユーザ 3 部門
権限・責任の特定	4.6	2.2	1.8	2.2	3.0
利用業務の特定	-	2.5	1.8	2.4	2.8
ライフサイクルの特定	-	2.1	1.7	2.3	2.8



この事例ではレベル 3 とレベル 2 の比較的きれいな三角形が描かれている。しかし、経営者層の回答はレベル 4 であるのに対し、RM 部門とユーザ 1、2 部門の回答はレベル 2 に集中している。このことから、この組織では、経営者層の認識（レベル 4）と RM 部門、ユーザ部門の認識（レベル 2）が異なっていること、RM 部門およびユーザ部門の認識が経営者層に伝達されていない事実、「情報と伝達」が適切に機能していない可能性を認めることができる。

○チャート事例 3：委託先のリスク分析

	経営者層	RM 部門	ユーザ 1 部門	ユーザ 2 部門	ユーザ 3 部門
外部委託	4.2	4.0	2.3	3.9	3.2
委託契約	-	4.0	4.5	3.8	3.5
委託先の監督	-	4.5	4.2	4.0	3.0



リスクマネジメントの遂行には、各部門の意識、理解度が揃っていることが大変重要である。しかし、この事例では、「委託先の監督」については RM 部門、ユーザ 1 部門とも一致してレベル 4 の高い評価をしている反面、ほかについてはレベル 4 から 2 までバラバラである。

各部門の評価が異なることは、部門の成熟度に差があることを示している。評価レベルが異なることは組織のリスクマネジメントに多くの負荷を強いる。たとえば、評価レベルの異なる者に対する教育の方法、内容は、レベルに応じた内容にしなければ、教育効果が期待できない。

4.2.4　医療

本節では、「医療」分野の回答のレーダーチャートを用いた分析例を示す。ギャップ分析については、1 章「1.4.3　ギャップ分析」に解説されているが、同一の質問に対して回答者間で評価レベルが異なる判定がなされる原因としては、①回答者間での事実の認識の違い、②回答者間での関心度の違い、③回答者間での質問の理解の違い、④回答者間での成熟度の定義の理解の違いが考えられる。

項目間、回答者間のギャップが発生する原因を検討することで、それぞれの組織のリスクマネジメント評価に活用していただきたい。

4.2.4.1　医療に関するリスクマネジメントの状況分析の前提と視点

（1）対象組織の前提

①評価対象の医療機関では、経営者層（GM)、リスクマネジメントを推進するリスクマネジメント部門（RM)、ユーザ部門（U-Med：臨床系、U-Adm：管理事務系、U-IT：情報システム系の 3 区分）の 3 部門に分けて評価を行ったものとする。

②分析に際し、対象の医療機関はすべての部門においてレベル 3 以上を目標としているという前提とする。

（2）分析の視点

①組織のリスクマネジメントレベルの評価にあたっては､各部門の評価レベルはこの医療機関の目標であるレベル 3 を基準として評価を行う。

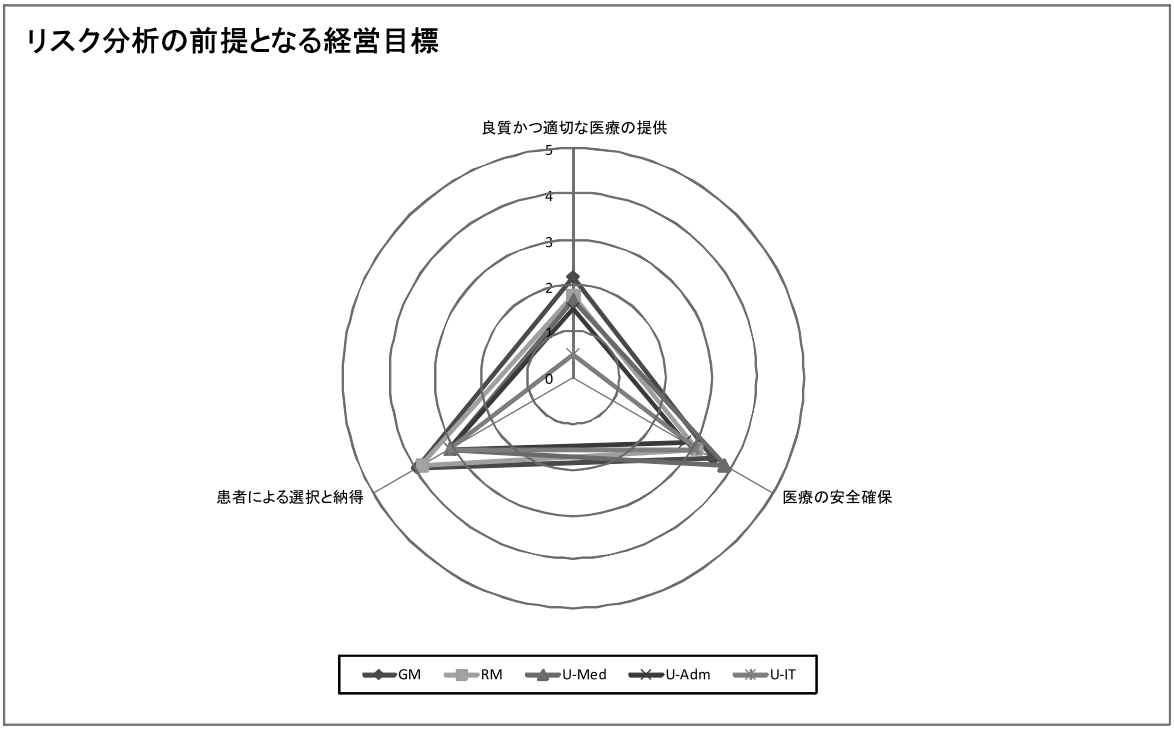
②各部門の評価のギャップを分析することによって､この医療機関におけるリスクマネジメントシステムとしての課題を明らかにする。

③評価レベルの分布状況から、各部門のリスクマネジメントの実施上の弱点を明らかにする。

4.2.4.2　ギャップ分析による課題の解明

○チャート事例 1：リスク分析の前提となる経営目標

	GM	RM	U-Med	U-Adm	U-IT
良質かつ適切な医療の提供	2.2	1.8	1.7	1.5	0.5
医療の安全確保	3.5	3.1	3.8	2.5	3.1
患者による選択と納得	3.9	3.8	3.1	3.1	3.1



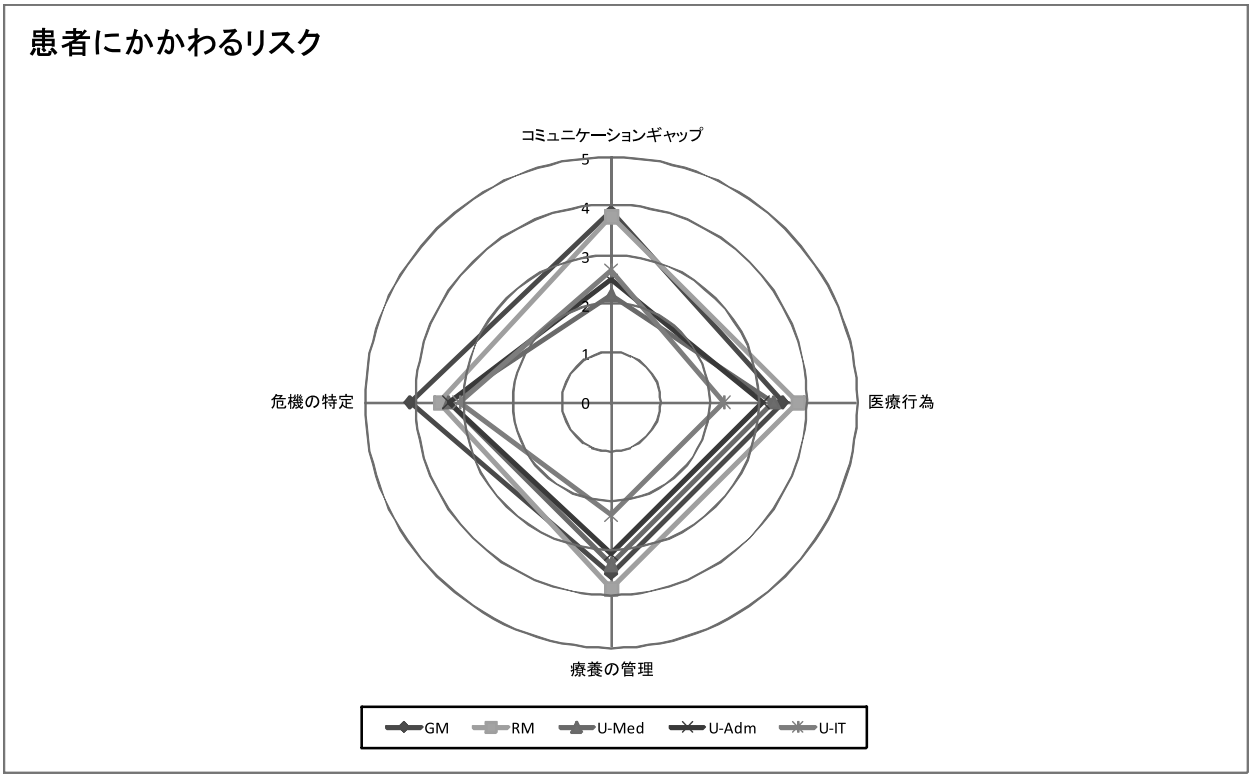
医療経営のリスクマネジメントを行う前提となる項目の認識度の評価である。各回答部門の評価レベルを見ると、「医療の安全確保」が認識されていることがわかる。

チャートの形は、「医療の安全確保」と「患者の選択・納得」に意識が集中している RM 部門と臨床系ユーザ部門に対し、事務系ユーザ部門の意識が低い点から、部門間の関心の違いを示している。また、「良質かつ適切な医療の提供」についての評価レベルが各回答で低いのは、組織としての取組みではなく、個人または部門単位での取組みと認識されている可能性が高い。

この事例は、経営目標間の認識に経営者層、RM 部門、ユーザ部門といった回答部門間、また、ユーザ部門では、臨床系、事務系、情報系といった部署間で差があること、社会の視点が経営目標に取り入れられていないことを示している。このような内向きで部門間の独立性が高い組織を、社会の変化に対応する統合された組織とすることが課題となる。

○チャート事例 2：患者にかかわるリスク

	GM	RM	U-Med	U-Adm	U-IT
コミュニケーションギャップ	3.9	3.8	2.2	2.5	2.7
医療行為	3.5	3.8	3.3	3.1	2.3
療養の管理	3.5	3.8	3.3	3.1	2.3
危機の特定	4.1	3.5	3.3	3.3	3.1



医療機関にとって重要な患者の安全の確保、安心と納得に関するリスクの特定では、医療上または療養環境で起きる事故のように、医療安全管理の分野として認識されている項目への評価レベルは回答部門間でほぼ一致している。

「コミュニケーションギャップ」についてユーザ部門の評価が低いのは、リスクマネジメント

が個人と部門レベルの頑張りで行われることを示している。経営者層とRM部門は、その個人と部門レベルの頑張りが各部門で行われていることで、組織全体の取組みと評価している可能性が高い。

医師の責任において行われる個々の診断や治療のプロセスとその結果、患者とのコミュニケーションについて、リスクマネジメントに取り組む主体が、医療従事者個人またはその所属する部門レベルで問題がないかを検討する必要がある。

JRMS2010はリスクマネジメント活動の評価項目ごとに評価する構成となっているので、リスク領域ごとに、リスクの把握、特定、分析、対策といった各評価項目のチャートを組み合わせることで、課題や弱点を分析することができる。

また、網羅的かつ包括的に評価する第2部と、業務レベルでの実践状況を評価する第3部のチャートを組み合わせることで、具体的な業務とその背景が相互に分析できる。

組織の特性に合わせて、JRMS2010を活用して、横断的な分析を行っていただきたい。

５．JRMS の有効性検証

組織のリスクマネジメント実践に関し、JRMS の有効性を確認するため、2008 年度および 2009 年度にそれぞれ実証実験を行った。

2008 年度の課題は、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の使いやすさ、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。このため、複数の企業にツールを提供し、回答から集計、レーダーチャート表示、分析までの一連の作業を実施していただいた。

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、成熟度の評価レベルの内容、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。

2009 年度の課題は、作成中の質問項目が JRMS 利用者にわかりやすく有用に作成されているか、成熟度の評価レベルでの回答が可能か、ツールの操作性について検証することにあった。そこで、複数業種に属する個人を対象に、各リスク領域別に回答作業を実施していただいた。

協力をいただいた実験参画者からは、特に質問項目の表現の難しさ、成熟度の評価レベルの解釈の難しさ等について貴重な意見・指摘をいただいた。

委員会では、JRMS2010 の有用性を高めるため、実証実験の結果を反映しつつ質問項目の見直しおよびツールの改変を行い、JRMS2010 を完成させた。

６．JRMS 質問票

6.1　質問票の構成

JRMS 質問票は、JRMS2010 の構造を通してその有効性を速やかに理解できるために、最も基本的と思われる質問を抽出し、構成したものである。質問票への回答結果は、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ものと思われる。

質問票は、第 1～3 階層の評価項目と第 4～5 階層の質問内容および回答対象部門で構成されており、「経営者層」、「リスクマネジメント（RM 部門）」「情報システム（IS）部門」、「ユーザ部門」が回答すべき質問に○印をつけている。

6.2　対象リスク領域別質問票

以下に、【1.組織経営編　1.1　経営】から【2.個別リスク対応編　2.6　医療】の質問項目を掲載する。

6.2.1　【1.組織経営編】

6.2.1.1　【1.1　経営】

（1）第 1～第 3 階層の構成

階層	階層タイトル	質問数
101	経営	36
101-1	リスクマネジメントフレームワークの構築	3
101-1-1	組織の経営理念と経営目標の明示	3
101-2	リスクマネジメントの基盤	6
101-2-1	リスクマネジメント方針	3
101-2-2	リスクマネジメント(RM)計画	3
101-3	リスクアセスメント	9
101-3-1	リスクの特定	2
101-3-2	リスク分析	4
101-3-3	リスク評価	3
101-4	組織のリスク対策	6
101-4-1	リスク対策の選定	3
101-4-2	リスク対策の実行	3
101-5	リスクマネジメントシステムの維持	12
101-5-1	リスクマネジメントシステムの実行	3
101-5-2	リスクマネジメントシステムのチェック	3
101-5-3	リスクマネジメントシステムの改善	3
101-5-4	リスクマネジメントレビューの実施	3

（2）質問票

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
101	経営				
101-1	リスクマネジメントフレームワークの構築				
101-1-1	組織の経営理念と経営目標の明示				
101-1-1-1	経営理念は組織で共有化されていますか？	○	○	○	○
101-1-1-2	経営目標は経営方針を反映していますか？	○	○	○	○
101-1-1-3	経営目標の優先順位は明らかですか？	○	○	○	○
101-2	リスクマネジメントの基盤				
101-2-1	リスクマネジメント方針				
101-2-1-1	リスクマネジメント方針は経営方針を反映していますか？	○	○	○	○
101-2-1-2	リスクマネジメント方針は達成すべき経営目標にふさわしい内容になっていますか？	○	○	○	○
101-2-1-3	リスクマネジメント方針は、全従業員が知っていますか？	○	○	○	○
101-2-2	リスクマネジメント(RM)計画				
101-2-2-1	RM 計画は、リスクマネジメント方針に基づいて策定されていますか？	○	○	○	○
101-2-2-2	RM 計画達成に必要な資源について検討されていますか？	○	○		
101-2-2-3	コンプライアンスに関する対応がリスクマネジメントに入っていますか？	○	○	○	○
101-3	リスクアセスメント				
101-3-1	リスクの特定				
101-3-1-1	組織に影響を与えるリスクの特定の十分性が、リスクマネジメントの有効性に、大きく影響することは社内で認知されていますか？	○	○		
101-3-1-2	リスクが組織や社会の状況変化と共に変化することは、組織内で認識されていますか？	○	○		
101-3-2	リスク分析				
101-3-2-1	リスク分析の重要性は、組織内で認識されていますか？	○	○	○	○
101-3-2-2	リスク分析を実施していますか？	○	○	○	○
101-3-2-3	リスク分析手法は適切ですか？		○	○	○
101-3-2-3-1	分析の対象ごとに分析手法の有効性を確認していますか？		○	○	○
101-3-3	リスク評価				
101-3-3-1	リスク対応を検討する際の判断基準はありますか？	○	○		
101-3-3-2	リスク評価の判断基準は、対象となるリスクにふさわしいですか？	○	○	○	○
101-3-3-3	リスク評価に経営者は関与していますか？	○	○		
101-4	組織のリスク対策				
101-4-1	リスク対策の選定				
101-4-1-1	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？	○	○	○	○
101-4-1-2	対応優先順位の高いリスクに対して、対策は決定され実施されていますか？	○	○	○	○
101-4-1-3	リスク対策について選定基準がありますか？	○	○	○	○

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
101-4-2	リスク対策の実行				
101-4-2-1	リスク対策は複数の候補の中から、最適な対策が実施されていますか？	○	○	○	○
101-4-2-2	リスク対策の責任者は、決まっていますか？	○	○	○	○
101-4-2-3	リスク対策の費用対効果の検討を行っていますか？	○	○	○	○
101-5	リスクマネジメントシステムの維持				
101-5-1	リスクマネジメントシステムの実行				
101-5-1-1	リスクマネジメントシステムを構築していますか？	○	○	○	○
101-5-1-2	リスクマネジメントシステムの実施体制の責任体制は適切ですか？	○	○	○	○
101-5-1-3	リスクマネジメントシステムのマニュアルは作成されていますか？	○	○	○	○
101-5-2	リスクマネジメントシステムのチェック				
101-5-2-1	リスクマネジメントシステムの検証の仕組みはありますか？	○	○	○	○
101-5-2-2	リスクマネジメントシステムのパフォーマンス評価を実施していますか？	○	○	○	○
101-5-2-3	リスクマネジメントシステムの有効性評価を実施していますか？	○	○	○	○
101-5-3	リスクマネジメントシステムの改善				
101-5-3-1	リスクマネジメントシステムの改善の仕組みがありますか？	○	○	○	○
101-5-3-2	定期的にリスクマネジメントシステムの改善を行っていますか？	○	○	○	○
101-5-3-3	経営者は、リスクマネジメントシステムの改善効果を確認していますか？	○	○		
101-5-4	リスクマネジメントレビューの実施				
101-5-4-1	経営者はリスクマネジメントシステムに関するレビューを行っていますか？	○	○		
101-5-4-2	レビューされた結果は継続的な改善に生かされていますか？	○	○	○	○
101-5-4-3	レビューの実施が組織内に開示されていますか？	○	○	○	○

6.2.1.2 【1.2 内部統制】

(1) 第1～第3階層の構成

階層	階層タイトル	質問数
102	内部統制	27
102-1	統制環境	3
102-1-1	経営	1
102-1-2	経営組織	1
102-1-3	経営実務	1
102-2	リスク分析の構築	7
102-2-1	リスク分析の仕組み	1
102-2-2	リスク分析の体制	2
102-2-3	リスク分析の実施	4

階層	階層タイトル	質問数
102-3	リスクの評価と対応	3
102-3-1	リスク評価の仕組み	1
102-3-2	リスク状況の把握	1
102-3-3	リスク対応	1
102-4	統制活動	3
102-4-1	統制活動全般	1
102-4-2	職務分掌	1
102-4-3	統制業務	1
102-5	情報と伝達	4
102-5-1	情報共有と伝達に係る活動	2
102-5-2	重要情報の共有	1
102-5-3	伝達経路	1
102-6	モニタリング	3
102-6-1	モニタリングの調整活動	1
102-6-2	是正活動	1
102-6-3	モニタリング情報の共有	1
102-7	ITへの対応	4
102-7-1	ITによる統制活動	1
102-7-2	IT 全社的統制	2
102-7-3	ITリスク	1

（2）質問票

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
102	内部統制				
102-1	統制環境				
102-1-1	経営				
102-1-1-1	内部統制に係る基本方針は明文化されたものがありますか？	○	○	○	○
102-1-2	経営組織				
102-1-2-1	取締役会は、内部統制に関し、経営者を適切に監視・監督する責任を果たしていますか？	○	○		
102-1-3	経営実務				
102-1-3-1	経営者は、企業内の個々の職能（生産、販売、情報、会計など）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？	○	○		
102-2	リスク分析の構築				
102-2-1	リスク分析の仕組み				
102-2-1-1	リスクアセスメント（特定・分析・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？	○	○	○	○
102-2-2	リスク分析の体制				
102-2-2-1	内外の経営環境の変化を含めたリスク環境の動きをとらえる社内体制を有していますか？	○	○	○	○
102-2-2-2	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？	○	○	○	○
102-2-3	リスク分析の実施				
102-2-3-1	定期的にリスクを洗い出していますか？	○	○	○	○
102-2-3-2	リスク頻度を算定していますか？	○	○	○	○

質問番号	質問項目	回答対象			
		経営 者層	RM 部門	IS 部門	ユーザ 部門
102-2-3-3	リスク影響度を算定していますか？	○	○	○	○
102-2-3-4	リスク評価を実施していますか？	○	○	○	○
102-3	リスクの評価と対応				
102-3-1	リスク評価の仕組み				
102-3-1-1	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？	○	○		
102-3-2	リスク状況の把握				
102-3-2-1	経営に影響を及ぼすリスクの要因を把握していますか？	○	○		
102-3-3	リスク対応				
102-3-3-1	経営に重要な影響を及ぼす可能性のある変化が発生する都度、リスクを再評価する仕組みがありますか？	○	○		
102-4	統制活動				
102-4-1	統制活動全般				
102-4-1-1	内部統制を妨げるリスクに対応する仕組みがありますか？	○	○	○	○
102-4-2	職務分掌				
102-4-2-1	内部統制実現のための職務分掌規程が明文化されたものがありますか？	○	○	○	○
102-4-3	統制業務				
102-4-3-1	統制活動は、業務全体にわたって規則や基準の則って実施されていますか？	○	○	○	○
102-5	情報と伝達				
102-5-1	情報共有と伝達に係る活動				
102-5-1-1	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、企業内のすべての者に適切に伝達できるような体制としていますか？	○			
	経営者は、従業員に、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？		○	○	○
102-5-1-2	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？	○	○		
102-5-2	重要情報の共有				
102-5-2-1	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？	○	○		
102-5-3	伝達経路				
102-5-3-1	内部統制に関する外部からの情報を適切に利用し、経営者、取締役会、監査役または監査委員会に適切に伝達する仕組みとなっていますか？	○	○		
102-6	モニタリング				
102-6-1	モニタリングの調整活動				
102-6-1-1	経営者は、独立的評価の範囲と頻度を、リスクの重要性に応じて適切に調整していますか？	○	○		
102-6-2	是正活動				
102-6-2-1	企業の外部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、必要な是正措置がとられていますか？	○	○		
102-6-3	モニタリング情報の共有				
102-6-3-1	内部統制に係る重要な欠陥等に関する情報は、経営者、取締役会、監査役または監査委員会に適切に伝達されていますか？	○	○		

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
102-7	ITへの対応				
102-7-1	ITによる統制活動				
102-7-1-1	経営者は、ITに関する適切な戦略、計画などを定めていますか？	○	○	○	○
102-7-2	IT 全社的統制				
102-7-2-1	組織として IT の計画がありますか？	○	○	○	○
102-7-2-2	IT に関する戦略、計画、予算などの作成体制がありますか？	○	○	○	○
102-7-3	ITリスク				
102-7-3-1	IT に関するリスク評価の方針がありますか？	○	○	○	○

出典 「財務報告に係る内部統制の評価および監査に関する実施基準」
参考1 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：平成 19 年 2 月 15 日金融庁企業会計審議会

6.2.2 【1.個別リスク対応編】

6.2.2.1 【2.1 情報システム】

（1）第 1～第 3 階層の構成

階層	階層タイトル	質問数
201	情報システム	124
201-1	状況特定	14
201-1-1	情報システムの外部環境	3
201-1-2	情報システムの内部状況	3
201-1-3	IT ガバナンス	5
201-1-4	情報システムを運用する組織・能力	3
201-2	情報システムのリスク特定	15
201-2-1	経営目標との関係	5
201-2-2	適用業務の責任・権限に関するリスク認識	3
201-2-3	経営目標への阻害要因	3
201-2-4	システムの阻害要因	4
201-3	情報システムのリスク分析	20
201-3-1	リスク分析技法とリスク情報の収集	4
201-3-2	プロジェクトリスク分析	3
201-3-3	開発に関するリスク分析	3
201-3-4	導入に関するリスク分析	3
201-3-5	アウトソーサのリスク分析	3
201-3-6	運用に関するリスク分析	4
201-4	情報システムが受けるリスク評価	14
201-4-1	災害の影響の評価	3
201-4-2	事故の影響の評価	3
201-4-3	人的災害の影響の評価	4
201-4-4	障害の影響	4
201-5	情報システムが受けるリスク対策	41
201-5-1	IT ガバナンス対策	3
201-5-2	情報システム組織のリスク対策	5
201-5-3	開発に関するリスク対策	5
201-5-4	運用テストにおけるリスク対策	2
201-5-5	本番環境のリスク対策	4

階層	階層タイトル	質問数
201-5-6	システム運用におけるリスク対策	7
201-5-7	アウトソーサのリスク対策	9
201-5-8	総合リスク対策の実施	6
201-6	モニタリングとレビュー	9
201-6-1	リスク管理の評価指標	3
201-6-2	評価指標の測定	3
201-6-3	評価指標の報告	3
201-7	リスクコミュニケーションと協議	11
201-7-1	ステークホルダの識別	4
201-7-2	ステークホルダへのコミュニケーション	4
201-7-3	ステークホルダからのフィードバック	3

（2）質問票

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
201	情報システム				
201-1	状況特定				
201-1-1	情報システムの外部環境				
201-1-1-1	IT（情報システム、通信システムおよび情報を取り扱うデバイスに関する技術）の変化を把握していますか？	○	○	○	○
201-1-1-2	業務のリスクの変化が情報システムに与える影響があることを理解していますか？	○	○		
	業務のリスクが変化すると、情報システムのリスクにつながることを知っていますか？			○	○
201-1-1-3	IT に関連する法制度について、制定・変更のチェックを行っていますか？	○	○	○	
	IT に関連する法制度の制定・変更があったとき、直ちに対応を講じていますか？				○
201-1-2	情報システムの内部状況				
201-1-2-1	情報システムの企画にかかわる組織の内部状況を把握していますか？	○	○	○	○
201-1-2-2	IT戦略（組織全体の情報システム化戦略）を見直す仕組みはありますか？	○	○		
	IT戦略（組織全体の情報システム化戦略）は見直されていますか？			○	○
201-1-2-3	IT に関し、事業継続の観点から分析していますか？	○	○		
	企業がビジネスに利用している IT が事業継続に影響を与えることを知っていますか？			○	○
201-1-3	IT ガバナンス				
201-1-3-1	IT戦略（組織全体の情報システム化戦略）は組織の目指す戦略と整合していますか？	○	○	○	○
201-1-3-2	IT 戦略やITインフラストラクチャ計画を実施できる予算が準備されていますか？	○	○	○	
201-1-3-3	ITインフラストラクチャ計画に基づいて、導入計画が作成されていますか？	○	○	○	
201-1-3-4	情報システムに、適切な内部統制機能が実現されていますか？	○	○	○	
201-1-3-5	情報システムのオーナーが明確になっていますか（責任の帰属が図られていますか）？	○	○	○	

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
201-1-4	情報システムを運用する組織・能力				
201-1-4-1	リスクの種類に応じて、担当する部門が明確化されていますか？	○	○	○	
201-1-4-2	IT戦略で将来必要となるスキルが識別され、人事計画や教育訓練計画に反映されていますか？	○	○	○	
201-1-4-3	IT資産管理のためのインベントリ（目録）が作られていますか？	○	○	○	
201-2	情報システムのリスク特定				
201-2-1	経営目標との関係				
201-2-1-1	情報システムの資産リスクを分析していますか？		○	○	
201-2-1-2	重要な情報システムにかかわる人的リスクを特定していますか？		○	○	
201-2-1-3	情報システムへの不正操作のリスクを特定していますか？		○	○	
201-2-1-4	システム開発に内在されるリスクを特定していますか？	○	○	○	○
201-2-1-5	会社の業績に大きな影響を与えるシステム障害のリスクを特定していますか？	○	○	○	○
201-2-2	適用業務の責任・権限に関するリスク認識				
201-2-2-1	情報システムにかかわる意思決定や業務に係る責任と権限に関して、リスクがあることに気づいていますか？	○	○	○	
201-2-2-2	企画・開発業務に関する責任と権限に関して、リスクがあることに気づいていますか？		○	○	
201-2-2-3	運用・運用業務に関する責任と権限に関して、リスクがあることに気づいていますか？		○	○	○
201-2-3	経営目標への阻害要因				
201-2-3-1	情報システム（ハード、ソフト、メディア）の破棄についてリスクを特定していますか？		○	○	○
201-2-3-1-1	情報システム内にデータが残っていて、情報漏えいにつながることを知っていますか？		○	○	
201-2-3-2	物理的な攻撃（爆弾）の情報システムに与える影響のリスクを特定していますか？		○	○	
201-2-4	システムの阻害要因				
201-2-4-1	内的、外的理由による機能不全が情報システムに与える影響のリスクを特定していますか？		○	○	○
201-2-4-2	人的な要因が情報システムに与える影響のリスクを特定していますか？		○	○	○
201-2-4-2-1	誤作動が情報システムに与える影響のリスクを特定していますか？		○	○	
201-2-4-3	システムの質の低下が情報システムに与える影響のリスクを特定していますか？		○	○	○
201-3	情報システムのリスク分析				
201-3-1	リスク分析技法とリスク情報の収集				
201-3-1-1	業務のリスクについて、分析する方法論はありますか？		○	○	
201-3-1-1-1	情報システムに関するセキュリティポリシーにリスクに関する記述がありますか？		○	○	
201-3-1-2	情報システムのリスク分析を実施するための教育や訓練が行われていますか？		○	○	
201-3-1-3	情報システムのリスクにつながる情報が収集されていますか？		○	○	○

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
201-3-2	プロジェクトリスク分析				
201-3-2-1	システム開発の対象となる業務について、導入効果やセキュリティ要件が明確になっていますか？		○	○	○
201-3-2-2	システム開発に関して企画段階でプロジェクトリスクを分析していますか？		○	○	○
201-3-2-3	プロジェクトの技術面のリスクを分析していますか？		○	○	○
201-3-3	開発に関するリスク分析				
201-3-3-1	開発ライフサイクルの各工程で、開発のリスクを分析していますか？		○	○	
201-3-3-2	システム開発に関してコンプライアンスの観点からリスクを分析していますか？	○	○	○	
201-3-3-3	システム開発に関して開発環境のリスクを分析していますか？		○	○	
201-3-4	導入に関するリスク分析				
201-3-4-1	システムを導入する場合にリスクを分析していますか？		○	○	
201-3-4-2	システム導入に関してコンプライアンスの観点からリスクを分析していますか？	○	○	○	
201-3-4-3	システム導入に必要な受入検査のリスクを分析していますか？		○	○	
201-3-5	アウトソーサのリスク分析				
201-3-5-1	アウトソーサの選定手続きにおいてリスクを分析していますか？	○	○	○	○
201-3-5-2	アウトソーシングの契約内容についてリスクを分析していますか？	○	○	○	○
201-3-5-3	アウトソーサがコンプライアンスを守らなかった場合のリスクを分析していますか？	○	○	○	○
201-3-6	運用に関するリスク分析				
201-3-6-1	運用テストの結果から、プログラムがシステム要件を満足しているかについて、リスクを分析していますか？		○	○	○
201-3-6-1-1	システム稼働後の処理／応答時間、処理能力のリスクを分析していますか？		○	○	
201-3-6-2	ファイル管理について、重要度に応じて改ざんや不正に対するリスクを分析していますか？		○	○	○
201-3-6-2-1	ライブラリ管理について、リスク（改ざんなど）を考慮していますか？		○	○	
201-4	情報システムが受けるリスク評価				
201-4-1	災害の影響の評価				
201-4-1-1	災害が情報システムに与える影響度を分析していますか？（災害（自然災害・人的災害を含む）が発生した場合、情報システム全体に与える影響度を想定していますか？）	○	○	○	○
201-4-1-2	災害発生時の復旧手順について情報システムに与える影響を分析していますか？	○	○	○	○
201-4-1-3	自然災害が情報システムに与える影響を分析していますか？	○	○	○	
201-4-2	事故の影響の評価				
201-4-2-1	事故が情報システムに与える影響度を分析していますか？	○	○	○	
201-4-2-2	火災・爆発が情報システムに与える影響を分析していますか？		○	○	

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
201-4-2-3	停電が情報システムに与える影響を分析していますか？		○	○	
201-4-3	人的災害の影響の評価				
201-4-3-1	人的災害が情報システムに与える影響のリスクを分析していますか？	○	○	○	
201-4-3-2	自然災害に乗じて起こる人的リスクの可能性を分析していますか？	○	○	○	○
201-4-3-3	伝染病の感染によって情報システムを運用できなくなる可能性を分析していますか？	○	○	○	○
201-4-3-3-1	インフルエンザの流行や感染によって情報システムを運用できなくなる可能性を分析していますか？	○	○	○	○
201-4-4	障害の影響				
201-4-4-1	障害発生時における情報システムに与える影響のリスクを分析していますか？（情報システムの機能に支障をきたす障害が発生した場合の影響度を想定していますか？）	○	○	○	
201-4-4-2	障害発生時の復旧手順が情報システムに与える影響のリスクを分析していますか？	○	○	○	
201-4-4-3	ハードウェア障害（LAN機器、電源装置などを含む）のリスクを分析していますか？		○	○	
201-4-4-4	運用での誤操作による障害のリスクを分析していますか？		○	○	○
201-5	情報システムが受けるリスク対策				
201-5-1	IT ガバナンス対策				
201-5-1-1	IT戦略は経営戦略と整合をとっていますか？	○	○	○	
201-5-1-2	IT は、組織に対して価値を提供していますか？	○	○	○	○
201-5-1-3	IT に係るリスクについては、経営的な観点から把握されて、判断されていますか？	○	○	○	○
201-5-2	情報システム組織のリスク対策				
201-5-2-1	システム開発基準にシステム開発のリスク対策を定めていますか？		○	○	
201-5-2-2	システムのライフサイクルにおけるプロセスごとの処理実施基準が定められていますか？		○	○	
201-5-2-3	開発要員の管理の観点から明確な実施基準を設けていますか？		○	○	
201-5-2-3-1	開発作業における職務分離（開発者・プログラマ・テストスタッフ）を実施していますか？		○	○	
201-5-2-3-2	各職務において情報セキュリティに関する役割や責任を明確にしていますか？		○	○	
201-5-3	開発に関するリスク対策				
201-5-3-1	システム要件定義で、セキュリティに関する実施基準を定めていますか？		○	○	○
201-5-3-2	開発環境の維持、管理を適切に実施していますか？		○	○	
201-5-3-2-1	システムとデータについて、機密保持のクラス分け（本番環境とテストでの区分など）がなされていますか？		○	○	
201-5-3-3	システム開発にあたって、関連する法規、契約などにかかわる要求事項を確認していますか？		○	○	
201-5-3-3-1	個人情報保護にかかわる法規、契約などにかかわる要求事項を確認していますか？		○	○	

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
201-5-4	運用テストにおけるリスク対策				
201-5-4-1	テスト仕様書はテストの目的に照らして適切ですか？		○	○	
201-5-4-2	運用テストの結果は十分確認していますか？		○	○	○
201-5-5	本番環境のリスク対策				
201-5-5-1	プログラムライブラリの管理責任者が明確になっていますか？		○	○	
201-5-5-2	本番プログラムへの変更管理の実施基準が明確になっていますか？		○	○	
201-5-5-3	プログラムの重要度を識別するための体系を確立していますか？		○	○	
201-5-5-4	プログラムの開発／変更を行うプログラマが、本番バージョンのライブラリに対するアクセスが認められないように職務の分離が行われていますか？		○	○	
201-5-6	システム運用におけるリスク対策				
201-5-6-1	運用基準にシステム運用のリスク対策が定められていますか？		○	○	○
201-5-6-2	システムの運用は、システム運用計画どおりに行われていますか？		○	○	○
201-5-6-3	システム運用管理が適切か、管理者が定期的に確認していますか？		○	○	○
201-5-6-3-1	運用マニュアルは、常に最新の状態で維持されていますか？		○	○	○
201-5-6-4	システム運用に関する障害監視を実施していますか？		○	○	
201-5-6-4-1	システム運用に関するオンライン監視を実施していますか？		○	○	
201-5-6-4-2	サーバのオンライン運用監視を実施していますか？		○	○	
201-5-7	アウトソーサのリスク対策				
201-5-7-1	実施基準（開発基準や外部委託基準など）にアウトソーシング関連のリスク対策を定めていますか？	○	○	○	
201-5-7-2	アウトソーシング契約で、委託者と受託者の責任分担は明確になっていますか？	○	○	○	
201-5-7-2-1	アウトソーシングの場合、受託者内の責任範囲は明確になっていますか？		○	○	
201-5-7-2-2	委託業務の実施内容をレビューしていますか？		○	○	
201-5-7-3	社内規程には、委託契約のルールが定められていますか？		○	○	
201-5-7-3-1	ソフトウェア瑕疵担保について定められていますか？		○	○	
201-5-7-3-2	契約でアウトソーサに対する監査を行うことが可能となっていますか？		○	○	
201-5-7-4	アウトソーサに情報セキュリティポリシーがない場合、委託者の情報セキュリティポリシーや実施基準を遵守することに合意していますか？		○	○	
201-5-7-4-1	アウトソーサでは、情報セキュリティのマネジメント体制ができていますか？		○	○	
201-5-8	総合リスク対策の実施				
201-5-8-1	リスクが高いことがわかっていても、事業の実施上必要な場合の情報システムを利用する決定をしていますか？	○	○	○	

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
201-5-8-1-1	想定するリスクが低く、対策をとらない場合には、リスクを受容することを関係者間で了解していますか？		○	○	
201-5-8-1-2	想定するリスクが高く、情報システム化をやめるなど回避する場合には、リスクを回避することを関係者間で了解していますか？		○	○	
201-5-8-1-3	想定するリスクが高く、保険などの回避策の場合には、リスクを移転することを関係者間で了解していますか？		○	○	
201-5-8-2	ネガティブな影響の大きなリスク対策については、RM部門に集約されていますか？	○	○	○	
201-5-8-3	リスク対策の決定は、企業の職務の権限規定に基づいて行われていますか？		○	○	
201-6	モニタリングとレビュー				
201-6-1	リスク管理の評価指標				
201-6-1-1	情報システムに関するリスクについて総合的な評価指標を定めていますか？	○	○	○	○
201-6-1-2	情報システムの扱う情報やデータに関するリスクについて評価指標がありますか？		○	○	○
201-6-1-3	情報システムを利用することで、新たに発生するリスクについて評価指標がありますか？		○	○	○
201-6-2	評価指標の測定				
201-6-2-1	情報システムに関するリスクを測定する機能が存在しますか？	○	○	○	
201-6-2-2	レビューしたリスクは、文書化されていますか？		○	○	
201-6-2-3	システム監査や情報セキュリティ監査を、定期的に受けていますか？		○	○	
201-6-3	評価指標の報告				
201-6-3-1	発見されたリスクを管理する仕組みがありますか？		○	○	
201-6-3-2	決定したリスク対策に対して、定期的にレビューをしていますか？	○	○	○	
201-6-3-3	情報システムのリスクの変化が検知されたときに、対応できますか？	○	○	○	
201-7	リスクコミュニケーションと協議				
201-7-1	ステークホルダの識別				
201-7-1-1	ステークホルダの識別ができていますか？	○	○		
201-7-1-2	情報システムの企画のステークホルダを特定していますか？		○	○	○
201-7-1-3	情報システムの開発のステークホルダを特定していますか？		○	○	○
201-7-1-4	情報システムの運用のステークホルダを特定していますか？		○	○	○
201-7-2	ステークホルダへのコミュニケーション				
201-7-2-1	情報システムの企画のリスクについてステークホルダに説明していますか？	○	○	○	
201-7-2-2	情報システムの開発のリスクについてステークホルダに説明していますか？	○	○	○	
201-7-2-3	情報システムの運用のリスクについてステークホルダに説明していますか？	○	○	○	
201-7-2-4	インシデント情報が共有されていますか？		○	○	○

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
201-7-3	ステークホルダからのフィードバック				
201-7-3-1	情報システムのリスクについてステークホルダにフィードバックしていますか？	○	○	○	○
201-7-3-2	情報システムの投資効果についてオーナーにフィードバックしていますか？	○	○	○	
	情報システムの投資効果についてフィードバックされていますか？				○
201-7-3-3	情報システムのリスクに対する投資効果についてオーナーにフィードバックしていますか？	○	○	○	
	情報システムのリスクに対する投資効果についてフィードバックされていますか？				○

6.2.2.2 【2.2 情報セキュリティ】

（1）第1～第3階層の構成

階層	階層タイトル	質問数
202	情報セキュリティ	60
202-1	状況特定	5
202-1-1	外部環境変化の把握	1
202-1-2	内部状況の把握	1
202-1-3	情報セキュリティポリシー	1
202-1-4	情報セキュリティ実施基準	2
202-2	リスク特定	3
202-2-1	経営目標とリスクの関係	1
202-2-2	管理対象とするリスク	1
202-2-3	包括的なリスクの把握	1
202-3	リスク分析	4
202-3-1	リスク分析の手法	1
202-3-2	リスク分析の体制	2
202-3-3	リスク分析結果の文書化	1
202-4	リスク評価	3
202-4-1	リスク評価の手法	1
202-4-2	リスク評価の体制	1
202-4-3	リスク評価結果の文書化	1
202-5	リスク対策	38
202-5-1	包括的リスク対策	2
202-5-2	コンピュータ犯罪	5
202-5-3	不正アクセス・不正利用	6
202-5-4	コンピュータウイルス	5
202-5-5	電子商取引	5
202-5-6	電子メール	4
202-5-7	災害	11
202-6	モニタリングとレビュー	3
202-6-1	リスク管理の総合的な評価指標	1
202-6-2	評価指標の測定	1
202-6-3	情報セキュリティ監査	1

階層	階層タイトル	質問数
202-7	コミュニケーションと協議	4
202-7-1	ステークホルダの識別	1
202-7-2	ステークホルダへのコミュニケーション	1
202-7-3	ステークホルダからのフィードバック	2

（2）質問票

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
202	情報セキュリティ				
202-1	状況特定				
202-1-1	外部環境変化の把握				
202-1-1-1	情報セキュリティリスクに関する外部環境の変化を把握するために、担当の部署が作られていますか？	○	○	○	○
202-1-2	内部状況の把握				
202-1-2-1	各情報セキュリティリスクに対する体制と対策の現状を把握するために、担当の部署が作られていますか？	○	○	○	○
202-1-3	情報セキュリティポリシー				
202-1-3-1	経営目標を反映した、情報セキュリティポリシーを文書化していますか？	○	○	○	○
202-1-4	情報セキュリティ実施基準				
202-1-4-1	情報セキュリティポリシーを反映した、情報セキュリティ実施基準を文書化していますか？		○	○	○
202-1-4-2	情報セキュリティ実施基準は、組織的な承認を得ていますか？		○	○	○
202-2	リスク特定				
202-2-1	経営目標とリスクの関係				
202-2-1-1	経営に影響を与える情報システムセキュリティインシデントの原因となるリスクの原因について、どの原因を管理対象にするかについて、承認していますか？	○			
	経営に影響を与える情報システムセキュリティインシデントの原因となるリスクの原因について、どの原因を管理対象にするかについて、経営者の承認を得ていますか？		○	○	○
202-2-2	管理対象とするリスク				
202-2-2-1	管理対象にするリスク原因について、文書化されていますか？	○	○	○	○
202-2-3	包括的なリスクの把握				
202-2-3-1	情報セキュリティリスクの原因について、定期的に見直しを行っていますか？	○	○	○	○
202-3	リスク分析				
202-3-1	リスク分析の手法				
202-3-1-1	組織体としてリスク分析の手法を定めていますか？		○	○	
202-3-2	リスク分析の体制				
202-3-2-1	リスク分析の体制は、各リスク原因の担当と全体総括について、役割分担が明確になっていますか？		○	○	
202-3-2-2	リスク分析にかかわる要員は、必要な知識・スキルを持っていますか？		○	○	

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
202-3-3	リスク分析結果の文書化				
202-3-3-1	リスク分析の結果を、文書化していますか？		○		
202-4	リスク評価				
202-4-1	リスク評価の手法				
202-4-1-1	組織体としてリスク評価の手法を定めていますか？		○	○	
202-4-2	リスク評価の体制				
202-4-2-1	リスク評価の体制は、各リスク原因の担当と全体総括について、役割分担が明確になっていますか？		○	○	
202-4-3	リスク評価結果の文書化				
202-4-3-1	リスク評価の結果を、文書化していますか？		○		
202-5	リスク対策				
202-5-1	包括的リスク対策				
202-5-1-1	リスク対策の全般的な方針を策定していますか？	○	○	○	○
202-5-1-2	外部委託先の情報セキュリティを管理していますか？	○	○	○	○
202-5-2	コンピュータ犯罪				
202-5-2-1	コンピュータ犯罪に関する実施基準が整備されていますか？		○	○	
202-5-2-2	内部犯罪の防止対策を行っていますか？		○	○	
202-5-2-3	データ保護対策を行っていますか？		○	○	
202-5-2-4	盗聴（通信回線の盗聴や室内での特殊機器による盗聴）対策を行っていますか？		○	○	
202-5-2-5	コンピュータ犯罪に対する緊急時対策を準備していますか？		○	○	
202-5-3	不正アクセス・不正利用				
202-5-3-1	不正アクセス・不正利用について、実施基準が整備されていますか？		○	○	
202-5-3-2	アクセス管理を行っていますか？		○	○	○
202-5-3-3	物理的アクセス対策を行っていますか？		○	○	○
202-5-3-4	論理的アクセス対策を行っていますか？		○	○	○
202-5-3-5	情報、資産に対する不正アクセスの検出を行っていますか？		○	○	
202-5-3-6	コンピュータ犯罪に対する緊急時対策を準備していますか？		○	○	
202-5-4	コンピュータウイルス				
202-5-4-1	コンピュータウイルスに対する実施基準が整備されていますか？		○	○	
202-5-4-2	コンピュータウイルスに対する予防対策を行っていますか？		○	○	
202-5-4-3	コンピュータウイルスに対する教育・訓練を行っていますか？		○	○	○
202-5-4-4	コンピュータウイルス感染時の対策を準備していますか？		○	○	
202-5-4-5	コンピュータウイルスに対する事後対策を行っていますか？		○	○	
202-5-5	電子商取引				
202-5-5-1	電子商取引に関する実施基準を整備していますか？		○	○	
202-5-5-2	電子商取引にあたって個人情報保護対策を行っていますか？		○	○	
202-5-5-3	電子商取引で利用するデータの保護対策を行っていますか？		○	○	

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
202-5-5-4	インターネット接続管理を行っていますか？		○	○	
202-5-5-5	電子的証拠を確保していますか？		○	○	
202-5-6	電子メール				
202-5-6-1	電子メール利用に関する実施基準が整備されていますか？		○	○	
202-5-6-2	メールサーバの保護対策を行っていますか？		○	○	
202-5-6-3	スパムメール対策を行っていますか？		○	○	
202-5-6-4	送信エラー対策を行っていますか？		○	○	
202-5-7	災害				
202-5-7-1	災害に対する実施基準を整備していますか？		○	○	
202-5-7-2	災害対策を管理していますか？	○	○	○	
202-5-7-3	耐震対策を行っていますか？		○	○	
202-5-7-4	水害対策を行っていますか？		○	○	
202-5-7-5	落雷対策を行っていますか？		○	○	
202-5-7-6	防火対策を行っていますか？		○	○	
202-5-7-7	停電対策を行っていますか？		○	○	
202-5-7-8	ネットワーク障害対策を行っていますか？		○	○	
202-5-7-9	断水対策を行っていますか？		○	○	
202-5-7-10	テロ対策を行っていますか？		○	○	
202-5-7-11	疾病対策を行っていますか？	○	○	○	○
202-6	モニタリングとレビュー				
202-6-1	リスク管理の総合的な評価指標				
202-6-1-1	情報セキュリティリスク管理の総合的な評価指標を定めていますか？	○	○	○	○
202-6-2	評価指標の測定				
202-6-2-1	評価指標について、定期的に測定を行っていますか？	○	○	○	○
202-6-3	情報セキュリティ監査				
202-6-3-1	情報セキュリティ監査を定期的に受けていますか？	○	○	○	○
202-7	コミュニケーションと協議				
202-7-1	ステークホルダの識別				
202-7-1-1	情報セキュリティリスクの管理について、ステークホルダを定義していますか？		○	○	
202-7-2	ステークホルダへのコミュニケーション				
202-7-2-1	ステークホルダごとに、情報セキュリティについて開示する範囲を定めていますか？		○	○	
202-7-3	ステークホルダからのフィードバック				
202-7-3-1	外部の法律等の規制について、包括的に把握していますか？		○	○	
202-7-3-2	取引先との契約が、情報セキュリティリスクの管理に与える影響を、把握していますか？		○	○	

6.2.2.3　【2.3　個人情報保護】

（1）第 1～第 3 階層の構成

階層	階層タイトル	質問数
203	個人情報保護	74
203-1	個人情報と経営	12
203-1-1	個人情報の価値の把握	3
203-1-2	個人情報の経営への位置づけ	3
階層	階層タイトル	質問数
203-1-3	個人情報の事業への位置づけ	3
203-1-4	個人情報の利用と保護に関する組織の体制	3
203-2	個人情報にかかわる状況の特定	6
203-2-1	外部状況の特定	3
203-2-2	内部状況の特定	3
203-3	リスク特定	6
203-3-1	個人情報リスクに関するリスクマネジメントの概要	3
203-3-2	リスク特定の実践	3
203-4	リスク分析	23
203-4-1	リスク分析体制	3
203-4-2	リスク分析の実施	3
203-4-3	取得・利用目的	3
203-4-4	第三者提供	3
203-4-5	安全管理	5
203-4-6	委託先のリスク分析	3
203-4-7	本人関与・周知にかかるリスク分析	3
203-5	リスク評価	6
203-5-1	リスク評価のマネジメント	3
203-5-2	リスク評価の実施	3
203-6	リスク対策	15
203-6-1	リスク対策	3
203-6-2	コンプライアンスの確保	3
203-6-3	利用目的に関するリスク対策	3
203-6-4	個人情報の安全対策に関するリスク対策	3
203-6-5	本人への対応に関するリスク対策	3
203-7	モニタリングとレビュー	3
203-7-1	モニタリングとレビューの実施	3
203-8	コミュニケーションと協議	3
203-8-1	ステークホルダの識別	3

（2）質問票

質問番号	質問項目	回答対象			
		経営者層	RM 部門	IS 部門	ユーザ部門
203	個人情報保護				
203-1	個人情報と経営				
203-1-1	個人情報の価値の把握				
203-1-1-1	個人情報が組織にもたらす積極的価値を把握していますか？	○	○		○
203-1-1-2	個人情報が組織にもたらす消極的価値を把握していますか？	○	○		○
203-1-1-3	個人情報の価値は組織全体の価値の序列の中に位置づけられていますか？	○	○		○

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
203-1-2	個人情報の経営への位置づけ				
203-1-2-1	組織のミッションと個人情報の利用と保護の関係を明確にしていますか？	○	○		○
203-1-2-2	個人情報の利用と保護のための経営方針を明確にしていますか？	○	○		○
203-1-2-3	個人情報の利用と保護に関する経営目的を実現するための経営戦略を明確にしていますか？	○	○		○
203-1-3	個人情報の事業への位置づけ				
203-1-3-1	個人情報の適切な利用を事業の要素として位置づけていますか？	○	○		○
203-1-3-2	個人情報の利用の可能性を事業の可能性と位置づけていますか？		○		○
203-1-3-3	個人情報の保護の可能性を事業の可能性と位置づけていますか？		○		○
203-1-4	個人情報の利用と保護に関する組織の体制				
203-1-4-1	個人情報の利用と保護に関する経営戦略を具体化するための規範がありますか？	○	○		○
203-1-4-2	個人情報の利用と保護に関する必要な権限を与え、責任の分担を行っていますか？	○	○		○
203-1-4-3	個人情報の利用と保護に関する必要な経営資源を準備していますか？	○	○		○
203-2	個人情報にかかわる状況の特定				
203-2-1	外部状況の特定				
203-2-1-1	個人情報に関する外部環境の変化を把握する仕組みを構築していますか？		○		○
203-2-1-2	個人情報の利用に関する法令など、国や自治体などによる公的な規制の変化を把握していますか？	○	○		○
203-2-1-3	個人情報の利用に関する取引先からの要請の変化を把握していますか？	○	○		○
203-2-2	内部状況の特定				
203-2-2-1	個人情報のすべてについて、その取扱者の権限と責任は特定されていますか？	○	○		○
203-2-2-2	すべての個人情報について、利用するすべての業務が特定されていますか？		○		○
203-2-2-3	すべての個人情報について、その収集から廃棄までの流れが特定されていますか？		○		○
203-3	リスク特定				
203-3-1	個人情報リスクに関するリスクマネジメントの概要				
203-3-1-1	個人情報リスクに対するリスクマネジメント方針を定めていますか？	○	○		○
203-3-1-2	個人情報リスクに対するリスクマネジメント計画を定めていますか？	○	○		○
203-3-1-3	個人情報リスクに対するリスクマネジメントプロセスを定めていますか？	○	○		○
203-3-3	リスク特定の実践				
203-3-3-1	リスク特定の対象となる個人情報の取得から廃棄までの流れをすべて把握していますか？		○		○
203-3-3-2	特定すべきリスクを把握する基準を定めていますか？		○		○
203-3-3-3	基準に従って個人情報の取扱いに係るリスクを把握していますか？		○		○

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
203-4	リスク分析				
203-4-1	リスク分析体制				
203-4-1-1	個人情報保護に係るリスク分析（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？	○	○		○
203-4-1-2	リスク分析の方法を定めていますか？		○		○
203-4-1-3	リスク分析を行う体制がありますか？	○	○		○
203-4-2	リスク分析の実施				
203-4-2-1	個人情報に関して、定期的にリスクを洗い出していますか？		○		○
203-4-2-2	個人情報に関して、経営環境の変化から生じるリスクを日常的に洗い出していますか？		○		○
203-4-2-3	個人情報の取扱いに関して、特定機能部門からの要請によってリスクを洗い出していますか？		○		○
203-4-3	取得・利用目的				
203-4-3-1	利用目的の特定に関するリスクを分析していますか？	○	○		○
203-4-3-2	個人情報の取扱いにあたり、目的外利用となるリスクを分析していますか？		○		○
203-4-3-3	個人情報の不正取得に関するリスクを分析していますか？	○	○		○
203-4-4	第三者提供				
203-4-4-1	個人情報を第三者に提供する場合のリスクを分析していますか？	○	○		○
203-4-4-2	個人情報の取扱いの一部または全部を外部に委託する場合、委託のための手続きに関するリスクを分析していますか？		○		○
203-4-4-3	共同利用を行う場合のリスクを分析していますか？		○		○
203-4-5	安全管理				
203-4-5-1	個人情報の正確性確保に関するリスクを分析していますか？		○		○
203-4-5-2	個人情報保護のための組織・体制の整備に関するリスクを分析していますか？	○	○		○
203-4-5-2-1	個人情報の漏えい、滅失またはき損によるリスクを分析していますか？		○		○
203-4-5-3	漏えい等の事故または取扱規程違反に関するリスクを分析していますか？	○	○		○
203-4-5-3-1	社内不正による個人情報の漏えいなどのリスクを分析していますか？		○		○
203-4-6	委託先のリスク分析				
203-4-6-1	個人情報の取扱いを委託する場合のリスクを分析していますか？	○	○		○
203-4-6-2	委託先との契約における締結内容（責任分担、非開示契約など）に関するリスクを分析していますか？		○		○
203-4-6-3	委託先に対する監督に関するリスクを分析していますか？		○		○
203-4-7	本人関与・周知にかかるリスク分析				
203-4-7-1	本人からの開示請求に関するリスクを分析していますか？		○		○

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
203-4-7-1-1	個人情報の利用の停止または第三者への提供の停止を求められた場合の手続きに関するリスクを分析していますか？		○		○
203-4-7-1-2	本人からの利用目的の通知・開示・訂正・利用停止などの要請に関するリスクを分析していますか？		○		○
203-5	リスク評価				
203-5-1	リスク評価のマネジメント				
203-5-1-1	リスク評価を行う体制がありますか？		○		○
203-5-1-2	個人情報の取扱いに関して経営に与えるリスクの評価基準を定めていますか？	○	○		○
203-5-1-3	個人情報の取扱いに関して経営に与えるリスクの評価方法を定めていますか？		○		○
203-5-2	リスク評価の実施				
203-5-2-1	リスク評価基準に基づいて個人情報リスクを評価していますか？		○		○
203-5-2-2	リスク評価方法に基づいて個人情報リスクを評価していますか？		○		○
203-5-2-3	リスク評価の結果を把握していますか？		○		○
203-6	リスク対策				
203-6-1	リスク対策				
203-6-1-1	リスク対策は個人情報のライフサイクル全般に及んでいますか？		○		○
203-6-1-2	個人情報のリスク対策に必要なリソースが整備されていますか？	○	○		○
203-6-1-3	個人情報の取扱ルールを遵守する対策を講じていますか？		○		○
203-6-2	コンプライアンスの確保				
203-6-2-1	収集したすべての個人情報の取扱いについて、コンプライアンスすべき規範をすべて特定していますか？		○		○
203-6-2-2	すべての個人情報の取扱いについて、必要な規範に準拠するにたる統治の仕組みを構築していますか？	○	○		○
203-6-2-3	すべての個人情報の取扱いについて、従うべき規範に準拠していることを検証・評価していますか？		○		○
203-6-3	利用目的に関するリスク対策				
203-6-3-1	すべての個人情報の利用目的を特定していますか？		○		○
203-6-3-2	収集したすべての個人情報を、利用目的達成に必要な範囲内で利用していますか？		○		○
203-6-3-3	組織の個人情報の取扱いの例外的措置は、根拠に基づいて適切に行われていますか？		○		○
203-6-4	個人情報の安全対策に関するリスク対策				
203-6-4-1	組織は、収集したすべての個人情報について、取得・入力のプロセスにおける滅失・漏えい、き損、可用性などに対する安全対策のリスクを把握していますか？		○		○
203-6-4-2	組織は、収集したすべての個人情報について、移送・送信のプロセスにおける滅失・漏えい、き損、可用性などに対する安全対策のリスクを把握していますか？		○		○
203-6-4-3	収集したすべての個人情報について、消去・廃棄のプロセスにおける滅失・漏えい、き損、可用性などに対する安全対策のリスクを把握していますか？		○		○

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
203-6-5	本人への対応に関するリスク対策				
203-6-5-1	すべての個人情報について、本人からの問合せに応え、その要求に応じて開示する仕組みを持っていますか？		○		○
203-6-5-2	すべての個人情報について、本人からの問合せに応え、その要求に応じて内容を訂正する仕組みを持っていますか？		○		○
203-6-5-3	すべての個人情報について、本人からの問合せに応え、その要求に応じて消去または第三者への提供の停止を行う仕組みを持っていますか？		○		○
203-7	モニタリングとレビュー				
203-7-1	モニタリングとレビューの実施				
203-7-1-1	組織として個人情報リスクに対応するためのモニタリングとレビューを評価指標によって実施していますか？		○		○
203-7-1-2	モニタリングとレビューの結果は経営者層に報告されていますか？	○	○		○
203-7-1-3	経営者層はモニタリングとレビューにコミットしていますか？	○	○		○
203-8	コミュニケーションと協議				
203-8-1	ステークホルダの識別				
203-8-1-1	個人情報リスクに関するステークホルダをすべて把握していますか？	○	○		○
203-8-1-2	個人情報リスクに関するステークホルダに与える影響を把握していますか？	○	○		○
203-8-1-3	個人情報リスクに関するステークホルダへの責任を把握していますか？	○	○		○

6.2.2.4　【2.4　事業継続】

(1) 第 1～第 3 階層の構成

階層	階層タイトル	質問数
204	事業継続	58
204-1	状況特定	18
204-1-1	事業継続の目的	4
204-1-2	主要な製品および／またはサービスの特定	5
204-1-3	事業継続管理の方針	3
204-1-4	経営資源の提供	3
204-1-5	BCMS 従事者への教育および訓練	3
204-2	リスクアセスメント	12
204-2-1	リスク特定：事業継続を脅かす要因の把握	3
204-2-2	リスク分析：業務中断による影響度の分析	3
204-2-3	リスク分析：事業中断からの復旧目標	3
204-2-4	リスク評価	3
204-3	リスク対策	12
204-3-1	事業継続戦略の決定	3
204-3-2	緊急時対応計画	3
204-3-3	事業継続計画（BCP）の策定	3
204-3-4	事業継続計画（BCP）の管理	3

階層	階層タイトル	質問数
204-4	モニタリングとレビュー	7
204-4-1	BCM の演習	3
204-4-2	マネジメントレビュー	4
204-5	コミュニケーションと協議	9
204-5-1	事業継続管理方針の周知	3
204-5-2	事業継続に対する認識度向上	3
204-5-3	継続的なステークホルダとの協議	3

（2）質問票

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
204	事業継続				
204-1	状況特定				
204-1-1	事業継続の目的				
204-1-1-1	組織の事業継続の目的を組織全体に明示していますか？	○	○		
	組織の事業継続の目的を組織全体で理解できていますか？				○
204-1-1-2	事業継続の目的を策定するにあたって、経営戦略および経営目標が考慮されていますか？	○			
	事業継続の目的を策定する前提となった経営戦略・経営目標を理解していますか？		○		○
204-1-1-3	組織が果たさなければならない社会的責任および義務を組織全体で理解できていますか？	○	○		○
204-1-1-4	組織において受容可能なリスクのレベルは明確になっていますか？	○	○		
	組織において受容可能なリスクのレベルを理解していますか？				○
204-1-2	主要な製品および／またはサービスの特定				
204-1-2-1	業務を継続していくうえで重要となる製品および／またはサービスを特定していますか？	○	○		
	業務を継続していくうえで重要となる製品および／またはサービスを把握していますか？				○
204-1-2-2	特定された重要な製品および／またはサービスは、ステークホルダの要求事項を反映させていますか？	○	○		○
204-1-2-3	特定された重要な製品および／またはサービスは、法規制の要求事項を反映させていますか？	○	○		○
204-1-2-4	特定された重要な製品および／またはサービスが組織の収入のなかに占める割合を把握していますか？	○	○		○
204-1-2-5	業務を継続していくうえで重要と特定した製品および／またはサービスに対して、コミットメントをしていますか？	○			
	業務を継続していくうえで重要と特定した製品および／またはサービスに対して、経営者のコミットメントは得られていますか？		○		○

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
204-1-3	事業継続管理の方針				
204-1-3-1	事業継続管理(BCM)方針が文書化されていますか？		○		○
204-1-3-2	事業継続管理(BCM)方針について、コミットメントをしていますか？	○			
	事業継続管理(BCM)方針は経営者のコミットメントが得られていますか？		○		○
204-1-3-3	事業継続管理(BCM)方針は定期的に見直していますか？	○	○		○
204-1-4	経営資源の提供				
204-1-4-1	事業継続に必要な要員が明確になっていますか？	○	○		○
204-1-4-2	事業継続に必要な資金が確保されていますか？	○	○		○
204-1-4-3	事業継続を実施していくための責任者が任命されていますか？	○	○		○
204-1-5	BCMS 従事者への教育および訓練				
204-1-5-1	事業継続活動を実施するにあたり、実行要員への教育および訓練が必要に応じて実施されていますか？		○		○
204-1-5-2	要員の力量の達成度を評価するための方法が確立されていますか？		○		○
204-1-5-3	要員の力量の評価結果がフィードバックされていますか？	○			
	要員の力量の評価結果を経営者へフィードバックしていますか？		○		○
204-2	リスクアセスメント				
204-2-1	リスク特定：事業継続を脅かす要因の把握				
204-2-1-1	主要な製品および／またはサービスを支える活動(人員、システム、機器なども含む)を特定していますか？		○		○
204-2-1-2	特定された主要な製品および／またはサービスは、事業継続の目的に合致していますか？		○		○
204-2-1-3	事業継続を脅かす要因の特定に、経営者として参画していますか？	○			
	事業継続を脅かす要因の特定に、経営者が参画していますか？		○		○
204-2-2	リスク分析：業務中断による影響度の分析				
204-2-2-1	主要な製品および／またはサービスを支える活動が停止した場合の影響度を把握していますか？	○	○		○
204-2-2-2	主要な製品および／またはサービスを支える活動が停止した場合の影響度が時間とともにどのように変化するかを想定していますか？	○	○		○
204-2-2-3	業務中断による影響度分析の結果は、経営陣のコミットメントを得ていますか？		○		○
204-2-3	リスク分析：事業中断からの復旧目標				
204-2-3-1	事業継続の目標とする復旧レベルは、決められていますか？	○	○		○
204-2-3-2	事業継続の目標復旧時間は、決められていますか？		○		○
204-2-3-3	業務復旧のために必要となる経営資源(人、機器、資金、情報など)は明確になっていますか？		○		○
204-2-4	リスク評価				
204-2-4-1	目標とする復旧レベルは、ステークホルダの合意を得ていますか？	○	○		○
204-2-4-2	リスク評価は、法規制を踏まえて行われていますか？		○		○

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
204-2-4-3	リスク評価の結果、リスク対応が困難なリスクを受容する場合、経営陣の承認を得ていますか？	○	○		○
204-3	リスク対策				
204-3-1	事業継続戦略の決定				
204-3-1-1	目標復旧時間を実現できるような対策を講じていますか？	○	○		○
204-3-1-2	組織の財務状況に応じた対策を講じていますか？	○	○		○
204-3-1-3	業務を継続していくうえで、ある特定の人に業務を依存しないような戦略を講じていますか？	○	○		○
204-3-2	緊急時対応計画				
204-3-2-1	緊急時対応体制が明確になっていますか？	○	○		○
204-3-2-2	意思決定者が不在の場合の緊急時対応の権限委譲の手順は明確になっていますか？	○	○		○
204-3-2-3	緊急時のメディア対応手順は明確になっていますか？		○		○
204-3-3	事業継続計画（BCP）の策定				
204-3-3-1	事業継続計画を策定していますか？	○	○		○
204-3-3-2	事業継続計画は、経営陣が承認していますか？	○	○		○
204-3-3-3	事業継続計画は、経営戦略で掲げている方針を満たすものとなっていますか？	○	○		○
204-3-4	事業継続計画（BCP）の管理				
204-3-4-1	事業継続計画は、定期的かつ必要に応じて見直されていますか？	○	○		○
204-3-4-2	事業継続計画の内容について、評価をしていますか？	○	○		○
204-3-4-3	事業継続計画を発動後は、既存の計画を見直す仕組みがありますか？	○	○		○
204-4	モニタリングとレビュー				
204-4-1	BCMの演習				
204-4-1-1	事業継続計画の演習は、定期的に実施されていますか？	○	○		○
204-4-1-2	事業継続計画の演習内容は、経営陣の承認を得ていますか？	○	○		○
204-4-1-3	演習の評価がフィードバックされていますか？	○			
	演習の評価を経営陣にフィードバックしていますか？		○		○
204-4-2	マネジメントレビュー				
204-4-2-1	経営陣によるマネジメントレビューを定期的に実施していますか？	○	○		○
204-4-2-2	重大な変更が生じたとき、経営陣によるマネジメントレビューを実施していますか？	○	○		○
204-4-2-3	マネジメントレビューで決まった対応処置について、ステークホルダへ周知する仕組みがありますか？	○	○		○
204-4-2-4	マネジメントレビューで決まった対応処置について、実施責任者、期限、優先順位が明確になっていますか？	○	○		○
204-5	コミュニケーションと協議				
204-5-1	事業継続管理方針の周知				
204-5-1-1	事業継続管理（BCM）方針は組織の要員に周知されていますか？	○	○		○
204-5-1-2	事業継続管理（BCM）方針を説明する責任者が明確されていますか？	○	○		○

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
204-5-1-3	事業継続管理(BCM)方針が要員に理解されていますか？	○	○		
	事業継続管理(BCM)方針を理解していますか？				○
204-5-2	事業継続に対する認識度向上				
204-5-2-1	要員全員に対し、事業継続活動においてどのような貢献ができるかを認識させていますか？	○	○		
	事業継続の活動に対して、自分はどのような貢献ができるかを認識していますか？				○
204-5-2-2	組織が置かれている社会的立場を要員は把握していますか？		○		○
204-5-2-3	事業継続への取組みは、取引先を含めて実施されていますか？		○		○
204-5-3	継続的なステークホルダとの協議				
204-5-3-1	事業継続の取組みに関係するステークホルダの経営陣・マネージャレベルと役割分担について協議していますか？	○	○		
	事業継続の取組みに関係するステークホルダの担当者と役割分担について協議していますか？				○
204-5-3-2	ステークホルダとの役割分担については契約や覚書などで文書化されていますか？		○		○
204-5-3-3	ステークホルダとの取組みの実効性を確認するために演習および訓練などに参加してもらっていますか？		○		○

6.2.2.5 【2.5 環境】

(1) 第1～第3階層の構成

階層	階層タイトル	質問数
205	環境	156
205-1	環境リスクの状況把握	18
205-1-1	環境活動の目標設定	6
205-1-2	環境リスクに影響を与える動向の認識	6
205-1-3	環境戦略の策定	3
205-1-4	環境管理の実践	3
205-2	環境リスクの特定	24
205-2-1	人や生態系への環境リスクの特定	3
205-2-2	バリューチェーンを通じた環境リスクの特定	3
205-2-3	技術使用・選択による環境リスク管理	3
205-2-4	環境市場・金融の環境リスク要因	3
205-2-5	企業の社会的環境責任	3
205-2-6	国際連携における環境リスク対応	3
205-2-7	地球環境制約への対応	3
205-2-8	環境クライシスの特定	3
205-3	環境リスクの分析	24
205-3-1	人や生態系への環境リスクの分析	3
205-3-2	バリューチェーンでの環境リスク分析	3
205-3-3	技術開発・適用の環境リスク分析	3
205-3-4	環境市場・金融のリスク分析	3

階層	階層タイトル	質問数
205-3-5	社会的環境責任に伴うリスク分析	3
205-3-6	国際連携におけるリスク分析	3
205-3-7	地球環境制約のリスク分析	3
205-3-8	環境クライシスのリスク分析	3
205-4	環境リスクの評価	30
205-4-1	人や生態系への環境リスクの評価	4
205-4-2	バリューチェーンでの環境リスク評価	3
205-4-3	技術開発・適用に付随する環境リスクの評価	5
205-4-4	環境市場・金融のリスク評価	3
205-4-5	社会的環境責任にかかわるリスク評価	3
205-4-6	国際連携に関連するリスク評価	3
205-4-7	地球環境制約と組織の関係性の評価	6
205-4-8	環境クライシスのリスク評価	3
205-5	環境リスクの対策	28
205-5-1	環境リスクマネジメントシステムの構築	4
205-5-2	人や生態系への環境リスク対策	3
205-5-3	バリューチェーンでの環境リスク対策	3
205-5-4	技術に伴う環境リスク管理	3
205-5-5	環境市場での競争力の確保	3
205-5-6	組織の社会的環境責任への対応	3
205-5-7	国際連携による環境リスク管理	3
205-5-8	地球環境制約への適応	3
205-5-9	危機管理	3
205-6	環境リスクのモニタリングとレビュー	21
205-6-1	環境リスクの監視	3
205-6-2	環境リスク管理プロセスの確認	6
205-6-3	環境リスク管理結果のレビュー	6
205-6-4	プロセスのモニタリングとレビュー結果の活用	6
205-7	環境リスクのコミュニケーションと協議	11
205-7-1	環境コミュニケーションの展開	4
205-7-2	共考による決定	4
205-7-3	コミュニケーションの実施	3

（2）質問票

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
205	環境				
205-1	環境リスクの状況把握				
205-1-1	環境活動の目標設定				
205-1-1-1	組織の経営に影響を与える可能性のある環境活動について経営管理目標を設定していますか？	○	○	○	○
205-1-1-1-1	エネルギー転換・温室効果ガス削減に関する経営管理目標を設定していますか？	○	○	○	○
205-1-1-1-2	自然資源の保全・持続的活動に関する経営管理目標を設定していますか？	○	○	○	○
205-1-1-1-3	物質資源の循環に関する経営管理目標を設定していますか？	○	○	○	○
205-1-1-2	組織の中長期の経営に影響を与える可能性のある環境リスクを経営管理の目標として設定していますか？	○	○	○	○
205-1-1-3	経営目標と環境目標は整合していますか？	○	○	○	○

質問番号	質問項目	回答対象			
		経営 者層	RM 部門	IS 部門	ユーザ 部門
205-1-2	環境リスクに影響を与える動向の認識				
205-1-2-1	自組織の事業形態に特徴的な環境応答特性を認識していますか？	○	○	○	○
205-1-2-2	組織活動に伴う環境負荷が労働者や周辺住民に影響を及ぼす環境リスクが組織に与える影響を認識していますか？	○	○	○	○
205-1-2-3	製品・サービスの流通先や部品、原材料のサプライヤや使用者を通じて発生する環境リスクが組織に与える影響を認識していますか？	○	○	○	○
205-1-2-4	環境にかかわる技術の開発や適用の動向を認識していますか？	○	○	○	○
205-1-2-5	国際的協調の環境リスク管理や、発展途上国などに対する環境保全の動向を認識していますか？	○	○	○	○
205-1-2-6	地球環境の制約に関する動向を認識していますか？	○	○	○	○
205-1-3	環境戦略の策定				
205-1-3-1	環境リスクに対する行動計画を経営目標に組み込んで明示していますか？	○	○	○	○
205-1-3-2	経営者は環境リスク対応を進めることを株主および社会に対して誓約していますか？	○	○	○	○
205-1-3-3	環境リスクに対応すべき資源を投入する行動計画を明らかにしていますか？	○	○	○	○
205-1-4	環境管理の実践				
205-1-4-1	環境対応と企業価値向上を両立させる手順を明確にしていますか？	○	○	○	○
205-1-4-2	組織が環境と共生する長期ビジョンを明確にしていますか？	○	○	○	○
205-1-4-3	環境保全に関連して法令遵守以上の社会要求に応える姿勢を明確にしていますか？	○	○	○	○
205-2	環境リスクの特定				
205-2-1	人や生態系への環境リスクの特定				
205-2-1-1	組織の活動による環境負荷がもたらす労働安全衛生上の健康リスクを特定していますか？	○	○	○	○
205-2-1-2	組織の活動による環境負荷がもたらす地域周辺住民への健康リスクを特定していますか？	○	○	○	○
205-2-1-3	組織の活動がもたらす環境負荷が生じさせる生態環境リスクとみなされる様相を定義していますか？	○	○	○	○
205-2-2	バリューチェーンを通じた環境リスクの特定				
205-2-2-1	製品・サービスの部品や部材の供給源が発生させる環境負荷が悪影響を与えるリスクを特定していますか？	○	○	○	○
205-2-2-2	サプライヤの行為が原因となって、サプライチェーン関連組織が訴訟を起こされる環境リスクを特定していますか？	○	○	○	○
205-2-2-3	製品・サービスの使用および廃棄時の環境影響が原因となって、組織が訴訟を起こされるリスクを特定していますか？	○	○	○	○
205-2-3	技術使用・選択による環境リスク管理				
205-2-3-1	新規技術の応用と産業化、商品化がもたらす環境リスクを特定していますか？	○	○	○	○

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
205-2-3-2	採用する技術が環境的側面から不適合であるとされるリスクを特定していますか？	○	○	○	○
205-2-3-3	保有する環境技術を応用して新しい製品・サービスを生み出す機会を生かしていますか？	○	○	○	○
205-2-4	環境市場・金融の環境リスク要因				
205-2-4-1	事業モデルの環境上の特性で、組織の市場競争力が変化するリスクを特定していますか？	○	○	○	○
205-2-4-2	事業モデルの拡大に伴う環境的側面の拡大が要因となって、組織の市場競争力が変化するリスクを特定していますか？	○	○	○	○
205-2-4-3	消費者の環境配慮の志向やライフスタイルの変化に伴って、組織の市場競争力が変化するリスクを特定していますか？	○	○	○	○
205-2-5	企業の社会的環境責任				
205-2-5-1	組織の活動に伴う将来世代や他地域への環境影響が原因となって、組織が社会的責任を問われるリスクを特定していますか？	○	○	○	○
205-2-5-2	環境リスク情報の伝達が不適切であることによって説明責任を問われるリスクを特定していますか？	○	○	○	○
205-2-5-3	新規の環境関連法規が組織の活動に影響を与えるリスクを特定していますか？	○	○	○	○
205-2-6	国際連携における環境リスク対応				
205-2-6-1	環境リスク管理に対する国際的要求の変化が、組織の経営に対して与える影響を特定していますか？	○	○	○	○
205-2-6-2	組織の活動が社会・経済・環境的少数者へ環境リスクを与えていることが経営に対して与える影響を特定していますか？	○	○	○	○
205-2-6-3	組織の活動に伴う環境リスクによって国際的不正義（貧困・文化抑圧・民族差別など）を生み出すことにより組織に与えるリスクを特定していますか？	○	○	○	○
205-2-7	地球環境制約への対応				
205-2-7-1	生態系サービスや生物多様性の変化が組織に与えるリスクを特定していますか？	○	○	○	○
205-2-7-2	物質資源の枯渇や資源循環の要求が組織に与えるリスクを特定していますか？	○	○	○	○
205-2-7-3	エネルギー利用形態や温室効果ガスの排出が組織に与えるリスクを特定していますか？	○	○	○	○
205-2-8	環境クライシスの特定				
205-2-8-1	不可抗力の事態が発生した際に生じうる重大な環境リスクを特定していますか？	○	○	○	○
205-2-8-2	不可抗力の事態が発生した際に生じうる環境上の影響で組織存続の危機となるリスクを特定していますか？	○	○	○	○
205-2-8-3	不可抗力の事態が発生した際に生じうる環境上の影響で事業継続の危機となるリスクを特定していますか？	○	○	○	○
205-3	環境リスクの分析				
205-3-1	人や生態系への環境リスクの分析				
205-3-1-1	組織の活動による環境負荷がもたらす事業所内での健康リスクを評価していますか？	○	○	○	○

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
205-3-1-2	組織の活動による環境負荷がもたらす周辺住民への健康リスクを評価していますか？	○	○	○	○
205-3-1-3	周辺環境の生物種、生態系の状態を観察・計測し、もしくは既存の観測値などを含めて分析していますか？	○	○	○	○
205-3-2	バリューチェーンでの環境リスク分析				
205-3-2-1	製品・サービスの部品や部材のサプライヤやディマンダの環境的な不都合が組織に及ぼすサプライチェーンを分析していますか？	○	○	○	○
205-3-2-2	サプライヤの行為が原因となって、サプライチェーン関連組織が訴訟を起こされる環境リスクを分析していますか？	○	○	○	○
205-3-2-3	製品・サービスの使用および廃棄時までのライフサイクルを通じた環境影響が原因となって、組織が訴訟を起こされるリスクを分析していますか？	○	○	○	○
205-3-3	技術開発・適用の環境リスク分析				
205-3-3-1	技術の応用と産業化、商品化がもたらす環境上の影響を分析していますか？	○	○	○	○
205-3-3-2	高度技術の適用に伴う環境リスクを分析していますか？	○	○	○	○
205-3-3-3	自組織の技術の環境浄化・保全への応用可能性を分析していますか？	○	○	○	○
205-3-4	環境市場・金融のリスク分析				
205-3-4-1	環境市場・融資システムとその動向を分析していますか？	○	○	○	○
205-3-4-2	自組織の活動に関連する環境ビジネスの市場規模や雇用規模の動向を分析していますか？	○	○	○	○
205-3-4-3	自組織活動の環境ビジネス市場への適合性を分析していますか？	○	○	○	○
205-3-5	社会的環境責任に伴うリスク分析				
205-3-5-1	新規の環境関連法規が組織の活動に影響を与えるリスクを分析していますか？	○	○	○	○
205-3-5-2	組織の活動に伴う将来世代や他地域への環境影響が原因となって組織の社会的責任を問われるリスクを分析していますか？	○	○	○	○
205-3-5-3	組織の活動の関連分野の環境政策動向を分析していますか？	○	○	○	○
205-3-6	国際連携におけるリスク分析				
205-3-6-1	環境リスク管理に対する国際規格や国際的報告書などを分析していますか？	○	○	○	○
205-3-6-2	組織の活動が社会・経済・環境的少数者へ与える環境影響を分析していますか？	○	○	○	○
205-3-6-3	途上国への環境関連の技術移転の適合性を分析していますか？	○	○	○	○
205-3-7	地球環境制約のリスク分析				
205-3-7-1	組織が利用している物質資源の利用形態を分析していますか？	○	○	○	○
205-3-7-2	生態系サービスや生物多様性の状況が組織の経営に与える影響を分析していますか？	○	○	○	○
205-3-7-3	組織のエネルギー代謝を分析していますか？	○	○	○	○

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
205-3-8	環境クライシスのリスク分析				
205-3-8-1	不可抗力の事態による環境汚染が人の健康や生態系に及ぼす被害規模、確率を分析していますか？	○	○	○	○
205-3-8-2	不可抗力の事態に対する脆弱性を分析していますか？	○	○	○	○
205-3-8-3	不可抗力の事態に対する回復力を分析していますか？	○	○	○	○
205-4	環境リスクの評価				
205-4-1	人や生態系への環境リスクの評価				
205-4-1-1	人の健康や生態系に影響が生じる確率や損害規模の観点から環境リスクを評価していますか？	○	○	○	○
205-4-1-2	環境負荷がもたらす影響を踏まえて社会経済的受容水準の観点からリスクレベルを評価していますか？	○	○	○	○
205-4-1-3	環境負荷の許容レベルを評価していますか？	○	○	○	○
205-4-1-4	環境負荷を発生するプロセスを管理するための代替案の優先順位を評価していますか？	○	○	○	○
205-4-2	バリューチェーンでの環境リスク評価				
205-4-2-1	バリューチェーンに沿った環境リスクの規模と確率を評価していますか？	○	○	○	○
205-4-2-2	バリューチェーン中を流れる環境負荷・環境影響要因の許容レベルを設定していますか？	○	○	○	○
205-4-2-3	プロダクトのライフサイクル全般における環境負荷を評価していますか？	○	○	○	○
205-4-3	技術開発・適用に付随する環境リスクの評価				
205-4-3-1	新規技術が環境に影響をもたらす環境リスクを評価していますか？	○	○	○	○
205-4-3-2	ビジネスオペレーションにおいて使用する技術システムの信頼性を評価していますか？	○	○	○	○
205-4-3-3	組織が用いる技術について、長期的な視点から運用性を評価していますか？	○	○	○	○
205-4-3-3-1	組織が用いる技術について、長期的な視点から経済性を評価していますか？	○	○	○	○
205-4-3-4	新規技術開発や運用に伴う環境的側面の経済的評価を行っていますか？	○	○	○	○
205-4-4	環境市場・金融のリスク評価				
205-4-4-1	組織のプロダクトの環境市場での適合性評価を行っていますか？	○	○	○	○
205-4-4-2	第三者による組織の環境格付けを評価していますか？	○	○	○	○
205-4-4-3	消費者の環境配慮の志向やライフスタイルの傾向と、組織のプロダクトの適合性を評価していますか？	○	○	○	○
205-4-5	社会的環境責任にかかわるリスク評価				
205-4-5-1	新規の環境関連法規が組織の活動に影響を与えるリスクを評価していますか？	○	○	○	○
205-4-5-2	組織の活動に伴う将来世代や他地域への環境影響が原因となって組織の社会的責任を問われるリスクを評価していますか？	○	○	○	○
205-4-5-3	組織の環境リスク管理に関する NGO や環境団体の要求レベルに対する実行可能性を評価していますか？	○	○	○	○
205-4-6	国際連携に関連するリスク評価				
205-4-6-1	環境リスク管理に対する国際的要求報告などを評価していますか？	○	○	○	○

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
205-4-6-2	組織活動が退去・移転など社会・経済・環境的少数者の非自発的行動を誘発していないかを評価していますか？	○	○	○	○
205-4-6-3	途上国などへの環境関連の技術の移転効果や有効性を評価していますか？	○	○	○	○
205-4-7	地球環境制約と組織の関係性の評価				
205-4-7-1	組織が利用する物質資源についての環境効率（利益／環境負荷）を評価していますか？	○	○	○	○
205-4-7-2	組織活動の生態系サービスや生物多様性に対する依存度や影響度を評価していますか？	○	○	○	○
205-4-7-3	組織活動に伴うエネルギー代謝を環境的制約の観点から評価していますか？	○	○	○	○
205-4-7-3-1	組織活動に伴う温室効果ガスの排出量を評価していますか？	○	○	○	○
205-4-7-3-2	組織活動に利用する資源の省エネルギー性能を評価していますか？	○	○	○	○
205-4-7-3-3	組織が生み出す製品・サービスの炭素集約度を評価していますか？	○	○	○	○
205-4-8	環境クライシスのリスク評価				
205-4-8-1	不可抗力の事態によって発現する可能性がある残留環境リスクを評価していますか？	○	○	○	○
205-4-8-2	不可抗力の事態による環境汚染が、人の健康や生態系に及ぼす被害規模、確率を評価していますか？	○	○	○	○
205-4-8-3	想定外の事象が生じた際に、最悪のシナリオが発生する可能性を評価していますか？	○	○	○	○
205-5	環境リスクの対策				
205-5-1	環境リスクマネジメントシステムの構築				
205-5-1-1	企業組織の最高意思決定機関のメンバーに総括的な環境リスク担当者がいますか？	○	○	○	○
205-5-1-2	環境リスクを経営面から統括する部門を設置していますか？	○	○	○	○
205-5-1-3	環境リスク対応に物質資源を投入していますか？	○	○	○	○
205-5-1-4	環境リスクを扱うマネジメントシステムを導入していますか？	○	○	○	○
205-5-2	人や生態系への環境リスク対策				
205-5-2-1	労働衛生、作業場の状況から特定した労働者、検査項目で健康診断を行っていますか？	○	○	○	○
205-5-2-2	労働者のメンタルな側面のヘルスケアは行っていますか？	○	○	○	○
205-5-2-3	周辺環境の環境負荷レベルの調査項目を指定し、モニタリングしていますか？	○	○	○	○
205-5-3	バリューチェーンでの環境リスク対策				
205-5-3-1	自組織が関係するサプライチェーンを通じて環境リスク対策を講じていますか？	○	○	○	○
205-5-3-2	プロダクト・サプライチェーンにおいて、環境情報のトレーサビリティを確保していますか？	○	○	○	○
205-5-3-3	プロダクトのライフサイクルを通じて環境リスク対策を講じていますか？	○	○	○	○

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
205-5-4	技術に伴う環境リスク管理				
205-5-4-1	環境リスクの大きさを考慮したうえで最適な技術選択を行っていますか？	○	○	○	○
205-5-4-2	プロダクト・プロセスでの技術利用に伴うヒューマンエラーの防止策を講じていますか？	○	○	○	○
205-5-4-3	自組織が利用する技術システムについてヒヤリハット・インシデントレポートを活用していますか？	○	○	○	○
205-5-5	環境市場での競争力の確保				
205-5-5-1	環境会計を実行していますか？	○	○	○	○
205-5-5-2	組織の環境格付けに対する対応策を講じていますか？	○	○	○	○
205-5-5-3	消費者の環境配慮の志向やライフスタイルの変化に対応した組織活動を実践していますか？	○	○	○	○
205-5-6	組織の社会的環境責任への対応				
205-5-6-1	組織の活動による環境負荷により環境リスクの悪影響を受けるステークホルダと共同していますか？	○	○	○	○
205-5-6-2	同業者などの環境リスク管理の事例を反映させていますか？	○	○	○	○
205-5-6-3	組織の活動に関係する環境関連法規を遵守していますか？	○	○	○	○
205-5-7	国際連携による環境リスク管理				
205-5-7-1	発展途上国などとの間で衡平な資源配分と利益分配の仕組みを構築していますか？	○	○	○	○
205-5-7-2	将来世代との間で衡平な資源配分と利益分配の仕組みを構築していますか？	○	○	○	○
205-5-7-3	国際的不正義を招かないための環境改善支援活動を行っていますか？	○	○	○	○
205-5-8	地球環境制約への適応				
205-5-8-1	組織が利用している物質資源の持続的な利用可能性や資源代替の方略を講じていますか？	○	○	○	○
205-5-8-2	生物多様性オフセットを実施していますか？	○	○	○	○
205-5-8-3	サプライチェーンを通じて生態系保全に配慮した資材・製品の調達・購入を実施していますか？	○	○	○	○
205-5-9	危機管理				
205-5-9-1	事故・問題が起きた場合のバイオレメディエーションなどの環境回復の手だてを準備していますか？	○	○	○	○
205-5-9-2	残留環境リスクに対して多重防護などの環境リスク低減を行っていますか？	○	○	○	○
205-5-9-3	ステークホルダと連携して非常事態に対応する計画をたてていますか？	○	○	○	○
205-6	環境リスクのモニタリングとレビュー				
205-6-1	環境リスクの監視				
205-6-1-1	環境リスクに伴う情報を収集する仕組みがありますか？	○	○	○	○
205-6-1-2	組織の環境基準を決める場合、規制で定められた方法で算出していますか？	○	○	○	○
205-6-1-3	自組織の環境リスクアセットにかかわる情報を整備していますか？	○	○	○	○
205-6-2	環境リスク管理プロセスの確認				
205-6-2-1	環境リスクの特定プロセスをモニタリングしていますか？	○	○	○	○
205-6-2-2	環境リスクの分析プロセスをモニタリングしていますか？	○	○	○	○

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
205-6-2-3	環境リスクの評価プロセスをモニタリングしていますか？	○	○	○	○
205-6-2-4	環境リスクの対策プロセスをモニタリングしていますか？	○	○	○	○
205-6-2-5	環境リスクのモニタリング・レビュープロセスをモニタリングしていますか？	○	○	○	○
205-6-2-6	環境リスクのコミュニケーション・協議プロセスをモニタリングしていますか？	○	○	○	○
205-6-3	環境リスク管理結果のレビュー				
205-6-3-1	環境リスクの特定結果の妥当性をレビューしていますか？	○	○	○	○
205-6-3-2	環境リスクの分析結果の妥当性をレビューしていますか？	○	○	○	○
205-6-3-3	環境リスクの評価結果の妥当性をレビューしていますか？	○	○	○	○
205-6-3-4	環境リスクの対策結果の妥当性をレビューしていますか？	○	○	○	○
205-6-3-5	環境リスクのモニタリング・レビュー結果の妥当性をレビューしていますか？	○	○	○	○
205-6-3-6	環境リスクのコミュニケーション・協議結果の妥当性をレビューしていますか？	○	○	○	○
205-6-4	プロセスのモニタリングとレビュー結果の活用				
205-6-4-1	環境リスクの特定結果を改善に活用していますか？	○	○	○	○
205-6-4-2	環境リスクの分析結果を改善に活用していますか？	○	○	○	○
205-6-4-3	環境リスクの評価結果を改善に活用していますか？	○	○	○	○
205-6-4-4	環境リスクの対策結果を改善に活用していますか？	○	○	○	○
205-6-4-5	環境リスクのモニタリング・レビュー結果を改善に活用していますか？	○	○	○	○
205-6-4-6	環境リスクのコミュニケーション・協議結果を改善に活用していますか？	○	○	○	○
205-7	環境リスクのコミュニケーションと協議				
205-7-1	環境コミュニケーションの展開				
205-7-1-1	自組織の環境情報の透明性と説明責任を確保していますか？	○	○	○	○
205-7-1-1-1	自組織の環境情報はGRIなどの定める記述フォーマットに準拠していますか？	○	○	○	○
205-7-1-2	環境リスクについて外部評価を活用していますか？	○	○	○	○
205-7-1-3	環境コミュニケーションを通じて環境適合型のライフスタイルを提案していますか？	○	○	○	○
205-7-2	共考による決定				
205-7-2-1	環境リスクの分析プロセスを通じて関係主体と共考していますか？	○	○	○	○
205-7-2-2	環境リスクの評価プロセスを通じて関係主体と共考していますか？	○	○	○	○
205-7-2-3	環境リスクの対策プロセスを通じて関係主体と共考していますか？	○	○	○	○
205-7-2-4	環境リスクのモニタリング・レビュープロセスを通じて関係主体と共考していますか？	○	○	○	○
205-7-3	コミュニケーションの実施				
205-7-3-1	環境リスクの分析プロセスを通じて関係主体とコミュニケーションをとっていますか？	○	○	○	○

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
205-7-3-2	環境リスクの評価プロセスを通じて関係主体とコミュニケーションをとっていますか？	○	○	○	○
205-7-3-3	環境リスクの対策プロセスを通じて関係主体とコミュニケーションをとっていますか？	○	○	○	○

6.2.2.6 【2.6 医療】

（1）第 1～第 3 階層の構成

階層	階層タイトル	質問数
206	医療	41
206-1	医療機関経営のリスクに影響を与える状況の把握	7
206-1-1	リスク分析の前提となる経営目標	3
206-1-2	医療機関経営の外部環境	1
206-1-3	組織内部の状況	2
206-1-4	業務管理	1
206-2	リスクの特定	6
206-2-1	患者にかかわるリスク	3
206-2-2	組織にかかわるリスク	1
206-2-3	スタッフにかかわるリスク	1
206-2-4	地域住民にかかわるリスク	1
206-3	リスク分析	11
206-3-1	組織的要因の影響分析	4
206-3-2	人的要因の影響分析	3
206-3-3	物的要因の影響分析	3
206-3-4	情報管理と情報システムの影響分析	1
206-4	医療経営のリスク評価	3
206-4-1	医療サービスのリスクの評価基準	1
206-4-2	経営管理にかかわるリスクの評価基準	1
206-4-3	リスク管理の重要度の評価	1
206-5	リスク対策	4
206-5-1	人的要因にかかわるリスク対策	1
206-5-2	組織要因にかかわるリスク対策	1
206-5-3	情報システムのリスク対策	1
206-5-4	医療機関の緊急時対応	1
206-6	モニタリングとレビュー	4
206-6-1	日常運用の点検	1
206-6-2	内部評価と外部評価	1
206-6-3	是正措置の点検・評価	1
206-6-4	経営者の役割	1
206-7	コミュニケーションと協議	6
206-7-1	患者および家族とのリスクコミュニケーション	2
206-7-2	医療機関内部のリスクコミュニケーション	1
206-7-3	取引先とのリスクコミュニケーション	1
206-7-4	関係官庁とのリスクコミュニケーション	1
206-7-5	地域社会やメディアとのリスクコミュニケーション	1

（2）質問票

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
206	医療				
206-1	医療機関経営のリスクに影響を与える状況の把握				
206-1-1	リスク分析の前提となる経営目標				
206-1-1-1	良質かつ適切な医療の提供について、経営としての具体的な成果目標（経営目標）として、組織の中でどのように認識されていますか？	○	○		
206-1-1-2	医療の安全確保のあり方は、組織の中でどのように認識されていますか？	○	○		
206-1-1-3	患者による選択と納得のあり方について、組織の中でどのように認識されていますか？	○	○		
206-1-2	医療機関経営の外部環境				
206-1-2-1	医療制度・医療政策の動向が医療経営に影響を与えることについて、組織の中でどのように認識されていますか？	○	○		
206-1-3	組織内部の状況				
206-1-3-1	自院の統治（ガバナンス）が経営目標に影響を与えることについて、組織の中でどのように認識されていますか？	○	○		
206-1-3-2	自院の能力が経営目標に影響を与えることについて、組織の中でどのように認識されていますか？	○	○		
206-1-4	業務管理				
206-1-4-1	診療プロセスの管理が経営目標に影響を与えることについて、組織の中でどのように認識されていますか？	○	○		
206-2	リスクの特定				
206-2-1	患者にかかわるリスク				
206-2-1-1	コミュニケーションギャップが患者の安全・安心に与える影響は、組織の中で認識されていますか？	○	○		
206-2-1-2	患者の安全・安心を脅かす医療行為の影響は、組織の中で認識されていますか？	○	○		
206-2-1-3	患者の安全・安心を脅かす療養の管理の影響は、組織の中で認識されていますか？	○	○		
206-2-2	組織にかかわるリスク				
206-2-2-1	医療に関連する制度や政策の変更が経営に与える影響は、組織の中で認識されていますか？	○	○		
206-2-3	スタッフにかかわるリスク				
206-2-3-1	業務上の安全管理がスタッフに与える影響は、組織の中で認識されていますか？	○	○		
206-2-4	地域住民にかかわるリスク				
206-2-4-1	自院の経営が地域住民の医療機能へのアクセスに与える影響は、組織の中で認識されていますか？	○	○		
206-3	リスク分析				
206-3-1	組織的要因の影響分析				
206-3-1-1	経営目的間の不整合が発生させる影響は、定性的・定量的に把握されていますか？	○	○		
206-3-1-2	経営体制の整備・運用の影響は、定性的・定量的に把握されていますか？	○	○		
206-3-1-3	業務管理体制の整備・運用の影響は、定性的・定量的に把握されていますか？	○	○		

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
206-3-1-4	災害、犯罪などが経営に与える影響は、定性的・定量的に把握されていますか？	○	○		
206-3-2	人的要因の影響分析				
206-3-2-1	コミュニケーションの良し悪しが医療サービスに与える影響は定性的・定量的に把握されていますか？	○	○		
206-3-2-2	医療スタッフの技能が、医療サービスに与える影響は、定性的・定量的に分析されてしていますか？	○	○		
206-3-2-3	行動・行為の良し悪しが医療サービスに与える影響は、定性的・定量的に分析されてしていますか？	○	○		
206-3-3	物的要因の影響分析				
206-3-3-1	医療機器の故障や事故が医療サービスに与える影響は、定性的・定量的に分析されてしていますか？	○	○		
206-3-3-2	ライフラインの事故が医療サービスに与える影響は、定性的・定量的に分析されてしていますか？	○	○		
206-3-3-3	物品の管理不全が医療サービスに与える影響は、定性的・定量的に分析されてしていますか？	○	○		
206-3-4	情報管理と情報システムの影響分析				
206-3-4-1	情報システムの障害が医療サービスに与える影響は、定性的・定量的に分析されていますか？	○	○		
206-4	医療経営のリスク評価				
206-4-1	医療サービスのリスクの評価基準				
206-4-1-1	医療事故における患者への影響度の評価基準は、組織の中で明確になっていますか？	○	○		
206-4-2	経営管理にかかわるリスクの評価基準				
206-4-2-1	経営目標に沿ったリスク評価基準が、組織の中で設定されていますか？	○	○		
206-4-3	リスク管理の重要度の評価				
206-4-3-1	リスク対応の優先度からリスクは評価されていますか？	○	○		
206-5	リスク対策				
206-5-1	人的要因にかかわるリスク対策				
206-5-1-1	リスク対策には、リスクの根拠となる人の行為・行動などにかかわる要因が反映されていますか？	○	○		
206-5-2	組織要因にかかわるリスク対策				
206-5-2-2	組織の目標、戦略、構造、運営にかかわるリスク対策は、実効性を伴っていると思われますか？	○	○		
206-5-3	情報システムのリスク対策				
206-5-3-1	情報システムに関するガイドライン等に沿ったりスク対策は、実効性を伴っていると思われますか？	○	○		
206-5-4	医療機関の緊急時対応				
206-5-4-1	緊急時対応策は、策定されていますか？	○	○		
206-6	モニタリングとレビュー				
206-6-1	日常運用の点検				
206-6-1-1	リスクマネジメント活動について、組織の中に定期的にモニタリングする仕組みがありますか？	○	○		
206-6-2	内部評価と外部評価				
206-6-2-1	内部監査は定期的に行われていますか？	○	○		
206-6-3	是正措置の点検・評価				
206-6-3-1	是正・改善の計画は策定されていますか？	○	○		

質問番号	質問項目	回答対象			
		経営者層	RM部門	IS部門	ユーザ部門
206-6-4	経営者の役割				
206-6-4-1	経営者(層)によるリスマネジメントのレビューは行われていますか？	○	○		
206-7	コミュニケーションと協議				
206-7-1	患者および家族とのリスクコミュニケーション				
206-7-1-1	自院の医療サービスに対する患者や家族の期待や不安は、どのように聞きとられていますか？	○	○		
206-7-1-2	医療に関するリスクは患者および家族に伝えられていますか？	○	○		
206-7-2	医療機関内部のリスクコミュニケーション				
206-7-2-1	医療や経営のリスクに関する情報は組織の中で共有されていますか？	○	○		
206-7-3	取引先とのリスクコミュニケーション				
206-7-3-1	医療リスクに関する重要な情報は、迅速に取引先に伝達・開示されていますか？	○	○		
206-7-4	関係官庁とのリスクコミュニケーション				
206-7-4-1	医療リスクに関する重要な情報は、迅速に関係官庁に報告・開示されていますか？	○	○		
206-7-5	地域社会やメディアとのリスクコミュニケーション				
206-7-5-1	医療リスクに関する重要な情報は、地域やメディアに伝えていますか？	○	○		

参考資料:

・四病院団体協議会医療安全管理者養成委員会編 「医療安全管理者必携 医療安全管理者テキスト」日本規格協会, 2005

・全日本病院協会「病院のあり方に関する報告書」(2007 年版)

・黒川清、尾形裕也監修、KPMG ヘルスケアジャパン編集「医療経営の基本と実務 上下」経済産業省サービス産業人材育成事業 医療経営人材育成テキスト、日経メディカル開発、2006 年

・財団法人日本医療機能評価機構 「医療事故情報収集等事業の開始について」財日医機評第 362 号 平成 16 年 9 月 21 日

平成 22 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　新高速印刷株式会社
東京都港区区新橋５丁目８番地４号
柴田ビル６Ｆ
TEL　03（3437）6365

21-H002