13－H003

JIPDECリスクマネジメントシステム(JRMS)のあり方に関する研究(JRAM2002)

平成14年3月

財団法人 日本情報処理開発協会

KEIRIN 00

この資料は競輪の補助金を受けて作成したものです。

序

日本情報処理開発協会（JIPDEC）におけるリスク分析委員会がＪＲＡＭ（『コンピュータセキュリティに関するリスク分析－ＪＲＡＭによるアプローチ』）を発表して10年が経過した。この間、わが国の情報環境は目覚しい変化を遂げた。ＪＲＡＭは、後述するように「ＪＲＡＭ質問票」に対する回答結果に基づいた「脆弱性分析」と「業務日報・障害報告等」の分析シートに基づいたリスクの実態分析から構成されたリスク分析のための方法論であった。開発当時、展開された枠組みにおいてもネットワークを考慮した方がよい状況にあったが、システム環境の中心は分散型というよりまだ集中型であったことから、ネットワークシステムを分析の主眼に置くものではなかった。

その後の経営情報環境の変化は大きく、ＪＲＡＭで構想していた分析の枠組みをはるかに超えた。重視されるべきは、コンピュータそのものよりも通信ネットワークの発展であった。[1]そのため、リスクの発生源は複雑化し、新たな視点からのリスクマネジメントの枠組み構築が不可欠となったのである。

こうした状況認識のもとで、JIPDECでは、1999年にJIPDECリスクマネジメント委員会（以下、ＪＲＭＳ委員会）を構成し、検討を開始した。同委員会では、リスクマネジメントの視点から広範囲にわたる情報リスクへの対応について論議を進めた。とりわけJIPDECが2000年ならびに2002年に発表した『わが国における情報セキュリティの実態－「情報セキュリティに関する調査」集計分析－』もリスクマネジメントの視点から現実的な対応を考慮し、調査項目を編成した。そこでの質問項目の構成・内容は同委員会での「JIPDECリスクマネジメントシステム（以下、ＪＲＭＳ）」構築のための作業に則ったものであった。本報告書は、情報システム全体を経営の視点から捉えたＪＲＭＳ構築作業の成果の一部として公表するものである。

なお、本調査研究報告書取りまとめ等にご協力いただいたリスクマネジメント委員会委員をはじめとする各位に心から謝意を表します。

平成14年3月

財団法人日本情報処理開発協会

---

[1] 集中型とはコンピュータセンターに大型のメインフレームを設置し、回線で各ユーザが利用する端末機を接続する型である。

集中分散型とはコンピュータセンターにメインフレームを持ち、また各場所にもアプリケーションを担当するサーバーを持ちその先にユーザの端末機が接続する型である。ユーザはアプリケーションによりメインフレームやサーバーを使用する。

分散型とは各場所にサーバー機と呼ばれる機器を設置し、サーバー機とユーザの端末機が接続されている型である。この場合サーバー機同士もネットワークで接続されている型も含む。

この他、コンピューター台で完結するスタンドアロン型もある。最近ではモバイルコンピュータ単独で業務を行うのもこの型に入る。しかし実際はこれらの複合形態のものが多く、メインフレームやサーバーからデータやプログラムをダウンロードしてモバイル端末に移し、実際のプログラムとデータの利用はメインフレームやサーバーとは切り離してスタンドアロンで実施することも一般に行われている。

平成13年度リスクマネジメント委員会

（敬称略／五十音順）

委員長	森宮　康	明治大学　商学部教授
委　員	池内　正英	安全工学（株）　代表取締役社長
	笠間　誠一	（株）日立製作所　金融システム事業部金融ソリューションシステム本部　第一部
	指田　朝久	東京海上リスクコンサルティング（株）危機管理・情報グループ主席研究員
	花香　俊明	ハナカリサーチセンター　代表
	原田　要之助	（株）情報通信総合研究所　情報流通プラットフォーム研究グループグループリーダー／エグゼクティブリサーチャー
	松原　榮一	ガートナージャパン（株）ジャパンリサーチセンター　マネージングディレクター

目　　次

第Ⅲ部　回答シート例

第Ⅳ部　ＪＲＭＳ質問項目

参考資料

第Ⅰ部

経営環境とリスクマネジメントシステム

1．経営環境とリスク

バブル経済崩壊後、組織をめぐる経営環境の変化はその激しさを増してきている。変化のパターンは量的・質的に大きく変化しただけでなく、そのスピードが加速化してきた。保護行政下にあった金融の世界では、公的資金の導入後も不確定要因により回復の道が不透明であっただけでなく、金融への信頼が揺らぎ、株安の影響がさらに拡大し、2002年に入っても、さらなる公的資金の導入が取りざたされている。しかも狂牛病関連では、肉骨粉の混入の実態解明が十分進まない中、肉表示の偽装工作事件が判明し、当該業界における企業倫理の問題が浮き彫りになってきた。

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。追い討ちを駆けたのが2001年9月のアメリカ貿易センタービルへのテロ攻撃であった。これにより、世界経済に影響が生じ、さらにエンロンの経営破綻により監査法人の信頼性にも陰りが出てきた。

むしろ今日問題なのは、情報が瞬時に世界をめぐり、影響が特定部署にとどまらないという現状を関係者がどのように認識しているかである。とりわけ、組織運営の基底にはコンピュータがネットワークで結合された環境があり、いやがうえにも情報価値を認識・判断し、情報に関わるプロテクションを組織のひとり一人が考えねばならない現状がある。

こうした経営環境の変化の中で、リスクという視点から分析を行う時、情報の世界はこれまでになく脆弱性への対応というガードが重視されざるを得ない。情報システムに関わる脆弱性の認識を誤ると、組織の屋台骨を根底から揺さぶられ、組織の安定性、ひいては存続を不可能にさせることになる。したがって、組織の経営をリスクマネジメントシステムという点から捉え、リスクの影響を明らかにすることが急務となってきたのである。こうした状況から（財）日本規格協会（ＪＳＡ）より2001年に公表されたのが、次に言及する「リスクマネジメントシステム構築のための指針－JIS Q 2001－」である。

1.1 JIS Q 2001の概要

JIS Q 2001のリスクマネジメントシステムについてはすでに紹介があるが[2)]、1995年1月7日に発生した阪神・淡路大震災を契機として、通商産業省工業技術院の委託事業として設置されたリスクマネジメントシステム規格委員会での検討結果である。この委員会の前身として危機管理委員会が設置され、当該委員会では国際標準化機構（ＩＳＯ）に対して日本発の国際規格提案を行うことが目的の一つにもなっていた。同委員会は再編成され、名称をリスクマネジメントシステム規格委員会（以下、ＲＭＳ委員会）として再編成された。ＲＭＳ委員会は2000年3月にリスクマネジメントシステムのＪＩＳ規格の開発活動を完了し、「リスクマネジメントシステムの構築に関する指針」のＪＩＳ原案のドラフトを完成させ、2001年に『リスクマネジメントシステム構築のための指針－JIS Q 2001－』（日本工業標準調査会審議によるJIS Q 2001として平成13年3月20日制定）がＪＳＡから公表されたの

---

2) 森宮康・井ノ口和好「リスクマネジメントシステムの標準化について」『予防時報』202号、日本損害保険協会、PP.26～33.

であった。

JIPDEC リスクマネジメントシステム委員会（ＪＲＭＳ委員会）では、「JIS Q 2001」は情報関連のリスクを焦点にあてているわけではないが、情報システムに関わるリスクに対応する理論的な枠組みとして JIS Q 2001 が利用可能という認識に立ち、「ＪＲＭＳ」を構成することにした。そこで、以下に JIS Q 2001 の枠組みを簡潔に示し、第Ⅱ部においてＪＲＭＳの構造について論じることにしたい。

1.1.1 JIS Q 2001 の特徴

リスクマネジメントシステムでは、問題解決の手法である意思決定論的なプロセスに従い、組織のリスクに関する脆弱性を発見し、対応手段の妥当性を検証する監査をも視野に入れている。

JIS Q 2001 は、大企業、中小規模の企業、病院、研究機関、自治体等々のあらゆる組織を対象としている。しかも、組織を襲うのは日常業務に関わるリスクだけではないことから、緊急事態と称される危機をも想定されていた。ターゲットは組織を襲うあらゆるリスクにおいていることから、対策への切り方がかなり包括的であり、その反面、リスクとは何か、緊急事態とは具体的に何を指すのか等々の側面に関しては、経営環境をめぐる可変性を考慮して、リスクをかなり弾力的に捉えている。これは、実際の運営の場において組織の構成員がリスクをどう考えるかについて、あまり厳密であれば、用語の共通理解だけも困難になるためである。しかしながら、実際の場においてリスクとは何か、緊急事態とは何を指すのか、リスク対策におけるリスク保有とは何かといった用語の理解について関係者の間である程度理解できていることが不可欠である。

1.2 JIS Q 2001 の構成

JIS Q 2001 のリスクマネジメントシステムでは、これまでの ISO9000 シリーズ、14000 シリーズ等々における規格で展開されてきたようにＰＤＣＡ（Plan、Do、Check、Act）というマネジメントサイクルに従っている。これによりリスクマネジメントにおける意思決定のプロセスがフィードバックするように構成されている。

ところで、リスクマネジメントを実際の場で行うためには、その行動指針と基本目的が明確であることが重要である。この点が確定していなければシステムとしての実効性が確保できないからである。リスクの作用が組織にいかなる影響を及ぼすのか、その点からリスク対応の行動指針を明確にし、往々にして抽象的になりがちなリスク対応の基本目的をできるだけ具体的に設定することが不可欠である。これがリスクマネジメント方針として明示され、それに従いリスクマネジメントの計画が策定されることになる。そうした目的達成のため、計画を策定し、対応組織においてリスクマネジメントを実施し、そのパフォーマンスを評価し、環境変化に応じた是正・改善を行う必要がある。これらの点を要約すれば以下のとおりである。

1.2.1 リスクマネジメント方針

組織としてリスクマネジメントを展開する場合、行動方針・基本目的を明示することが肝要である。JIS Q 2001 では、最高経営者がリスクマネジメント方針を定め、構成員・関係者に文書で明確に表明し、行動指針を定め、それに基づきリスクマネジメントシステムの運用により組織としての到達点等を基本目的として設定することが望ましいとしている。

1.2.2 リスクマネジメントに関する計画（Plan）

リスクマネジメントに関する計画策定は、マネジメントサイクルの最初のプロセスである。そこではリスク分析、リスク評価、リスクマネジメントの目標設定、リスク対策の選択、それにリスクマネジメントプログラムの策定から構成されている。最初のステップであるリスク分析では、特に組織にマイナスの作用（損失）をもたらすリスクを発見することが出発点となる。とりわけ、日常の業務活動におけるリスクを発見し、特に組織に重大な結果をもたらすリスクを特定化することが望ましい。リスク環境は絶えず変化しているため、リスクを発見するための取組みは継続的に行う必要がある。なお、組織にとり問題状況は平常時だけではないことから、緊急事態も当然考慮される。

（1）リスク分析

リスクマネジメントシステムにおける基本的なプロセスは、以下のとおりである。

a）リスク発見

b）リスク特定

c）リスク算定

以下、これらのステップにおける重要事項について概説しておくことにする。

a）リスク発見

まず出発点はリスクの発見であるが、JIS Q 2001 では「組織に損害を及ぼす可能性のあるリスクを発見することが望ましい」としているが、望ましいこととして「リスクをもれなく明らかにする」と書かれている。だが、学術的な場においても困難なように、こうした表現から実際の経営の場において組織の構成員すべてが同じ理解度をもって発見することができるのかが問われることになる。そこで、JIS Q 2001 では定義を設け、リスクを「事態の確からしさとその結果の組み合わせ、又は事態の発生確率とその結果の組み合わせ」とし、備考の一つに「ある状況では、リスクは予想とのかい離のことである」という記載がある。こうした理解は、あらかじめ予想（予定）していることが実際の結果と食い違うことに視点をあてたものであり、ＪＲＡＭでの解釈に近似している。

b）リスクの特定

リスクに関する情報を分析し、「組織に重大な結果をもたらすと懸念されるリスク及び／又は結果の重大性の判断が困難なリスクを特定することが望ましい」としている。なお、その上で、脆弱性および危険性の検討を示唆している。またそのための方法としては、ブレーンストーミング、インタビュー、アンケート調査、専門家への相談などにも触れている。

c）リスク算定

特定化したリスクについては、リスク評価の手がかりとして、発生確率・影響の大きさを

定量的・定性的に把握することが望ましいとしている。

（2）リスク評価

特定化したリスクについて、必要に応じ、その重要性の度合いを評価する条件ともいうべきリスク基準を作成し、またリスク対応の優先項目を決めることになる。

（3）リスクマネジメントの目標設定

目標の設定にあたっては、守るべき対象の明確化・法的要求事項（コンプライアンス）などの実行可能な達成目標を組織内外の関係者が容易に理解できるよう明示しておくことが不可欠である。特定の者だけがわかっているのでは、システム全体として十分に機能できるとは考えられないからである。

（4）リスク対策の選択

組織を襲うリスクに対処するための対策は、時間軸に基づいて「事前対策」と「事後対策」から構成されている。特に事後対策としては、組織への影響を考え、被害の最小化・被害の拡大防止を想定した「緊急時対策」と「復旧対策」があげられる。なお、ＪＩＳ原案では方法としてのリスク対策には「リスク回避」、「リスク移転」、「リスク低減」、「リスク保有」があげられているが、ＪＲＭＳでは、具体的な方法が示されている。

（5）リスクマネジメントプログラムの策定

リスクマネジメントの目標達成のためにプログラムを策定するわけであるが、その際、望ましいとする設定項目は次のとおりである。リスク対策の具体的な内容、関連部署におけるリスク対策の日程、利用する経営資源、責任の範囲・所在である。

なお、リスクマネジメントプログラムには、上記の事前対策、緊急時対策、復旧対策が含まれる。

さらに、プログラムの策定にあたり考慮すべき事項として次のことが挙げられている。上記の具体的な内容であっても継続的に実施できなければ意味がないことから継続的に実施できる内容、適切な手順、参画すべき責任のある関係者、定期的なレビューに必要な仕組み、経営資源・責任・時期・とるべき対策の優先項目の適切さ、リスクマネジメント方針・一般的計画活動への対応の適切さ、監視・レビューの手順等である。これらは、組織の経営計画に組み込まれるのが望ましい。

1.2.3　リスクマネジメントの実施（Do）

リスクマネジメントプログラムの実施・緊急時の追加事項・復旧時の追加事項・運用管理が取り上げられている。

（1）リスクマネジメントプログラムの実施

プログラムの実施にあたっては、組織の関連諸部門・部署において策定されたプログラムにしたがって具体的な施策を実施し、その実施状況を責任者に定期的に報告することが望ましい。とりわけ、関連諸部門・部署の関係者間での相互理解を深めておくことが重要と思われる。

（2）緊急時に特徴的な追加事項

緊急時の対応にはそれなりの実行組織、手順なり準備が必要であるため、追加事項が加味されている。対応手順の策定では、いつ緊急時対応を発動するのか、どのような事態をもっ

て終了とするのか、組織の内外の機関との協力・連絡関係をどうするのかといった側面が考慮されるべきである。また、実行組織を整備するにあたっての必要事項、すなわち実行組織の責任者はどういう者が望ましいか、情報機能の管理の仕方、分析・評価機能として何をするのか、対応機能の中身は何か、広報機能のあり方といった内容が含まれている。

（3）復旧に特徴的な追加事項

復旧に対しても必要な追加事項として、外部機関との協力関係の構築、限られた経営資源の有効活用の手順整備が示されている。

（4）運用管理

これまでのプログラムの実施にあたっては、事前対策の実施手順、緊急時対策の手順、復旧対策の手順、報告様式などの付属資料の文書化など、適切に管理することが望ましいとされている。

1.2.4 リスクマネジメントパフォーマンス評価・リスクマネジメントシステムの有効性評価（Check）

（1）リスクマネジメントパフォーマンス評価

組織としては、リスクマネジメントプログラムの実施により設定された目標達成に鑑みてそのパフォーマンス（測定可能な結果）がどうなのか、評価を行う必要がある。そのためには手順を確定し、リスクマネジメントの実施状況を監視・測定し、その有効性を評価することが求められる。

リスクマネジメントのパフォーマンス評価に際しては客観性・再現性・検証可能性・実行可能性が重視される。指標と考えられるのは、プログラムやリスク対策実施の進捗度、組織における内部基準、関連する法規制ならびに規格、リスクコミュニケーションの実行度等である。

パフォーマンスの評価は、平常時のみならず緊急時対策ならびに復旧対策についても適宜行うことが重要といえる。

（2）リスクマネジメントシステムの有効性の評価

リスクマネジメントシステムの有効性については、リスクマネジメントの基本目的・リスクマネジメントの目標達成に関する有効性を評価するための手順を確立・維持することが望まれる。

システムの有効性を高めるためには、リスクマネジメント計画、リスク対策、リスクマネジメントシステムの体制・仕組みを見直し、是正・改善がどの程度必要なのか、必要であればどの領域なのかといったことを確定することも重要となる。また、有効性の検証が必要となれば、関係部署の協力を得て、評価を行うことも考えられる。

1.2.5 リスクマネジメントシステムに関する是正・改善（Check）

（1）是正・改善の継続的実施

組織をめぐるリスク環境は絶えず変化している。これまで実施してきた対策等のパフォーマンスがリスクマネジメントの目標に照らしてどうなのか、常にチェックする必要がある。それゆえ、リスクマネジメントの実施状況の監視、パフォーマンスの評価、システムの有効

性評価に基づいて、必要に応じてリスクマネジメントシステムを継続的に是正・改善することが求められる。とりわけ是正・改善の実施時期としては、

a）継続的是正・改善

b）リスクマネジメントシステム監査時

c）緊急事態経験後

d）リスクに関する情報の監視結果に基づく要請時

といった４つが考えられている。

（2）実施の確認

是正・改善が実際に行われたのか、実施状況の点検・確認について言及されている。ただ、JIS Q 2001 では点検・確認を「望ましい」としているが、現実問題としてこの作業は不可欠といえる。

1.2.6 組織の最高経営者によるレビュー（Act）

最高経営者は、リスクマネジメントシステムを維持し、適切性・有効性を改善するため、リスクマネジメント方針以下、JIS Q 2001 に示された事項について、自ら定めた間隔で当該システムをレビューすることが望ましいとしている。

1.3 JIS Q 2001 におけるシステム維持のための仕組み

情報に関わるリスクの場合、特にリスクマネジメントシステムを実際の場において実施し維持していくための仕組みが不可欠である。そのための仕組みについては、以下の項目からなっている。その概要について示すことにする。

1.3.1 能力・教育・訓練

システムを運用する要員について、その役割ごとに必要な能力が必要である。また、対策実施のため、必要な能力を身に付けさせ、維持させるため、リスクマネジメントに関わる知識等について教育・訓練を実施することが望まれるとしている。

1.3.2 シミュレーション

リスク対応の実施手順の有効性を検証する目的をもってシミュレーションを行うことが必要である。たとえば、それぞれの関係者に役割を与え，活用できる経営資源を設定して，特定のリスクが顕在化していく過程、緊急時になる過程、緊急時を脱して復旧時となる過程などを想定して実施するのがよいといえる。

1.3.3 リスクコミュニケーション

この目的として、リスクの発見・特定のための情報収集、誤解なり理解不足に基づくリスク顕在化の防止等があげられている。また、リスクコミュニケーション実施のための手順の確立・維持について言及されているほか、リスクへの対応に関して組織としていかに対処しているかを明らかにするために広報活動計画を策定すること、さらに関係機関・関

係者にリスク情報を開示することが指摘されている。

1.3.4 リスクマネジメントシステム文書の作成

組織としていかにリスクに対応しているかを関係者に紙面または電子形式で周知徹底させるとして、その場合、リスクマネジメントシステムの構成および機能、さらに重要な文書類がどこで入手・利用可能かが把握できるようにしておくこととしている。

1.3.5 文書管理

ここでは、他の規格と同様に、種々の文書を作成・改訂し、管理する手順を確立・維持することが重要である。

1.3.6 発見したリスクの監視

組織に作用するリスクの変化を継続的に監視するため、変化を与える要因を特定し、情報を収集することが指摘されている。

1.3.7 リスクマネジメント関係記録の維持管理

記録を維持し管理するのは、リスクマネジメントに関連する様々な活動を追跡可能にするためであり、この点はリスクマネジメントにおいて非常に重要である。

1.3.8 リスクマネジメントシステム監査

リスクマネジメントシステム監査のプログラム・手順を確立し、維持することが望まれている。

1.3.9 組織の最高経営者によるレビュー

最高経営者は、リスクマネジメントシステムを維持し、適切性・有効性を改善するため、リスクマネジメント方針以下、JIS Q 2001 に示された事項について、自ら定めた間隔で当該システムをレビューすることが望ましいとしている。

ところで、JIS Q 2001 では「リスクマネジメントシステム構築のための指針」というタイトルからも理解できるように、組織の経営にとり各項目を実践することが「望ましい」という表現で書かれている。実際にリスクマネジメントを実行するのはそれぞれの組織であるため、組織の判断に委ねるというスタンスに基づくものである。

第Ⅱ部

ＪＲＭＳの構造

1．ＪＲＭＳとＪＲＡＭの関係

リスク分析の方法論は1992年にJIPDECにより『コンピュータセキュリティに関するリスク分析－ＪＲＡＭによるアプローチー（以下、ＪＲＡＭ)』として公刊された[3)]。ＪＲＡＭは次ページの図２－１－１のように、リスクの把握のためＪＲＡＭ質問票による「脆弱性分析」と組織の日常業務に関わるリスク把握のためそれぞれの部署において記載された「業務日報・障害報告」を基に実態を分析する二面的な構造を有していた。後者の業務日報・障害報告に基づく分析手法は過去の損失実態に関わるデータをもとに分析するという分析手法としては極めて基本的なものであり、現在でも十分利用に耐える考え方である。

だが、問題は過去の経験を重視するとしても、情報システム環境の変化の中ではどうしても後手に回る可能性が強い。とりわけ、高度情報化の流れで従来以上に企業の中に情報システムや情報そのものがあふれ、機器も安価で代替が可能となり、さらには機器に触れる者も一部の訓練されたシステムオペレータだけではなくなり、ごく一般の従業員が端末機器を操作することとなった。昨今のように、不正アクセスであるとかコンピュータウイルスとなると、対応策については（たしかに、この点も万全とはいいがたいが）先を読みながら進む必要がある。そうした視点を重視する意味から、組織のリスクマネジメントシステムという枠組みを前提にしたアプローチが重要となってきた。

これらの環境変化に対して、リスク対策を網羅的に実施するアプローチもあるが、リスク分析に基づいた経営判断により特定のリスクに対応する対策を実施していくアプローチも考えられる。リスクを生み出す環境要因の今日的な変化の中でＪＲＡＭの枠組みと共に質問項目の拡充が必要となってきた。

今回、ＪＲＭＳ構築のため、組織全体にとり神経系・血液系となる「システム」と「情報」に関するリスクとその対応に焦点をあて、リスクマネジメントシステムの考え方にたち展開することにした。そのため、前述の『リスクマネジメントシステム構築のための指針－ JIS Q 2001』を拠り所にＪＲＡＭの方法論の脆弱性分析を採用し、質問項目への回答から組織の情報システムに関するリスクを把握し、リスク対策を含め、組織の脆弱性を分析することに重点を置いた。

[3)] リスクを処理するにあたりリスク分析が出発点である。ただ、リスクへのアプローチに際して従来のＪＲＡＭの場合は、情報システムの芽生えの時期であり、情報システムおよび情報機器そのものが高価な宝物であり、なにをおいても守らなくてはならないとの考え方が強い時代の産物であった。そのため万全の対策をとることが社会的な要請であった。そのためＪＲＡＭもその対策編ではまず対策ありきのチェックリストの形を取らざるを得なかった。しかもＪＲＡＭでは、リスクとその対処方法についてはそれぞれの組織によるとして、脆弱性に対するセキュリティの度合いを把握することに関心が集中していた。

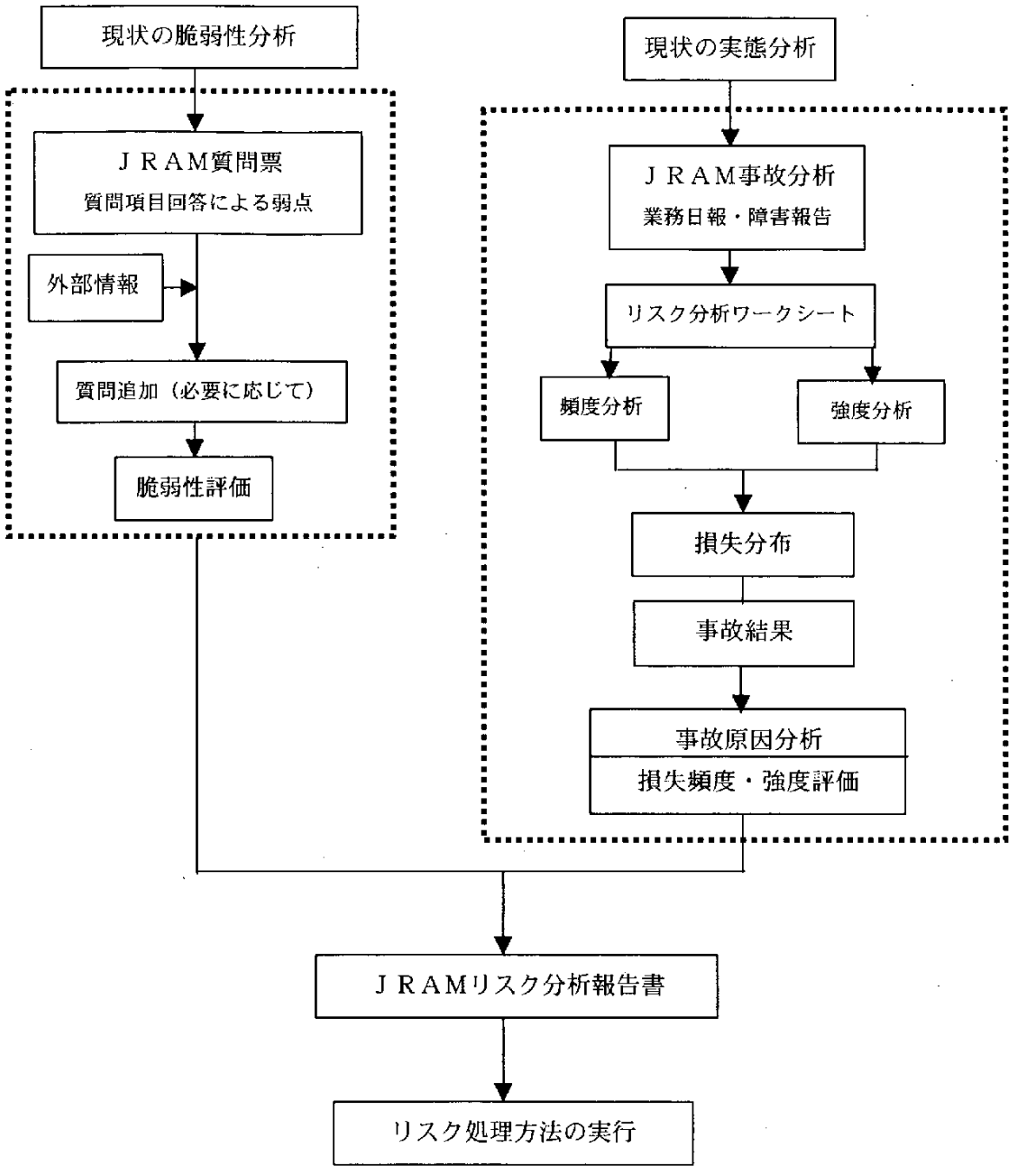


図２－１－１．ＪＲＡＭの構造（参考）

出典：『コンピュータセキュリティに関するリスク分析－ＪＲＡＭによる分析』（日本情報処理開発協会）1992 年

1.1　ＪＲＭＳの構造

ＪＲＭＳは、組織の全体像に関わるリスクマネジメントシステムを基底にすえながら、情報システムにおけるリスクの組織に対する影響を分析するとともに、リスク対策の実施状況から組織としての脆弱性を明らかにするように構成されている。

ＪＲＭＳにおいてはリスクを把握するため後掲の質問票を用いる。既述のようにＪＲＡＭが焦点をあてていた情報環境と異なり、現在では情報ネットワーク環境が前提となっており、この点を考慮し、内部・外部からのアクセスを含む内容となっている。そうした情報環境に鑑み、枠組みを広げ、組織全体の中での情報システム環境の位置づけを明確にする必要性が出てきている。したがって現代の情報システム [5] を利用する組織においてどのようなリスクが考えられるのか、その特徴は何なのか、対策は十分なのか明確に把握しておくことが不可欠である。

ところで、ＪＲＭＳについては基本的に質問票を用いて組織の脆弱性を明らかにする枠組みとなっていることから、別称として「ＪＲＡＭ２００２」として位置づけていくことにしたい。

1.1.1　ＪＲＭＳの目的

ＪＲＭＳは、情報システムの脆弱性を把握し、リスク対策の妥当性を探るところに目的がある。ＪＲＭＳ質問票は、組織のどこにリスクを生み出す源泉があるのかをチェックし、組織に内在する弱点を明らかにする。そのためには、組織の構成員が、経営環境が可変的であり、それによりリスク発生・組織への影響・対策の必要性を共有するところに意味がある。とりわけ、経営者層は、リスクマネジメントの導入・実施を利益のあがらない領域とみなす傾向がある。経営者の認識の低さといった点については、『平成13年度　情報セキュリティに関する調査』の結果からもうなずける。しかし、リスク対応の不備が組織を壊滅に導く現状からリスクに対する感性を磨くことが必要と思われる。

---

[5]　情報システムの構成要素としては次のようなものがある。
○　ユーザ
○　ユーザが使用するクライアント機器（端末機、ＡＴＭ、カードリーダーなど）
○　回線および回線接続装置、サーバー機、ホスト機、システムオペレーター
○　情報システム各種機器の設置場所の環境（空調装置、建物そのものなど）
○　プログラム開発者
○　アウトソーサー（プログラム開発、データ作成、システム運用など）
○　インタネット接続業者
これらの情報システムを利用する組織においてどのようなリスクが考えられるのか、その特徴は何なのか、明確に把握しておくことが肝心である。

2．情報リスクの特性

ＪＲＭＳにおけるリスク対応を考えるに際して、なによりも重要なことは情報システムに関わる情報リスクの特徴を認識することである。そこで、リスクの分析ならびにリスク対策に関する情報リスクの特性を示しておく。

2.1　情報リスクの特徴

情報および情報システムは目に見えないという特徴がある。特に情報はその他の媒体を通して初めて有形の把握が可能である。情報システムはコンピュータの発達とともに論じられるが、昔はコンピュータという機器そのものが相対的に高価であったため、そのハードウェアそのものの有形なものを対象としてその安全対策を論じることが多かった。しかし、機器が安価になり企業経営や家庭の多くの部門で日常的に使われる現状ではデータやサービス内容という無形のものの価値を守ることがより重要となってきている。

その無形な価値の塊である「情報」そのものに着目すると次のような特徴がある。

a）情報そのものの価値が再作成ロードという時間単価や要員の人件費と一致しない。つまり知的財産権が大きい。

b）コピーが容易であり、コピーされるという盗難に気づきにくい。

c）改ざんや消去が簡単にできる。

d）効率化がコンピュータの最大の効果であるため、一度業務停止を行うと、または誤った処理を行うと、その影響を受ける者が何万の単位にも発生し被害対象者数が飛躍的に増大する。また、事件発生に要する時間が短時間である。

e）インターネットなどを通じ国際化しており、事件・事故が国際的に展開する。

f）国際的な対応が求められるが、一方で法律が整備されておらず、複数国家間にまたがる場合などは、どの国の法律の適用を受けるかにも注意が必要である。

g）データの作成、プログラムの作成、ユーザの利用、システムの運用など人的要素が大きい。

2.2　情報システムにおける情報リスクの位置づけ

ＪＲＭＳにおいて、情報リスクを分析するにあたり、情報システムそのものにも焦点をあてている。その場合、当然のことながらシステムに関わる個々の火災や機械故障なども分析対象としている。今や、企業経営にとり情報システムが不可欠な存在であり、情報システムは企業そのものと不可分であり、企業の一部という認識をベースにおいて展開している。企業そのもののリスクは業種や企業の生い立ちにより様々な変化があるが、企業の神経系や血液系に相当する情報リスク特有の、つまり情報システムのプログラムおよびデータなどに固有の特徴は共通して取り上げることができる。

企業の経営者からこのＪＲＭＳをみると、情報システムが企業に寄与する大きさを認識することにより、その寄与を阻害するリスクとその対応策をその他のリスクと平行して検討することは有意義である。ここでは情報担当役員（ＣＩＯ：Chief Information Officer）から情報システム担当部門および情報システム担当者までを対象にすることを考えている。

2.3 情報システムリスクの要素

情報システムのリスクを評価するには各情報システムの要素を以下のように分解してそれぞれの脆弱性を分析することが有効である。分析の仕方については、「４．ＪＲＡＭ質問票の使い方」ならびに「第Ⅳ部　ＪＲＭＳ質問項目」を参照されたい。

ａ）入力情報リスク

これは入力する情報そのものの誤り、入力ができない、適正な者以外の利用入力による作業のミスなどがある。

ｂ）情報処理プロセスリスク（アプリケーションリスク）

ここには情報機器の故障、自然災害、火災などによる業務停止、プログラムミス、運用トラブル、設計そのもののミスなどがある。リカバリの不備、業務継続計画の不備など、事件・事故が発生した後の対応の失敗もここに含む。

ｃ）出力情報リスク

ここには価値ある情報の取扱いに関するリスクが含まれる。情報漏洩、不正使用などがあげられる。

ｄ）組織外情報リスク

アウトソーシング先の事件事故、ネットワークのトラブル、接続企業のトラブル、ハッカー、コンピュータウイルスなどがある。

2.4 情報システムリスクの評価

一般にリスクを評価する場合の評価項目はいくつかあるが、人的リスク、利益リスク、物的リスク、信用リスク、賠償リスクの５つで評価をすると次のような特徴がある。

ａ）人的リスク

業種によるが、一般的には情報システムそれ自身では大きくないとされる。

しかし、交通分野、医療分野など人的要素に影響が大きい分野では大きくなるが、その程度は他の機械の故障や誤作動の持つリスクとオーダー的には同じと考えられる。

ｂ）利益リスク

情報そのものが大きな知的財産権を持つこと、また大量処理による効率化がコンピュータ導入の目的でもあることからその効率阻害を引き起こしたときの利益損害は大きいといえる。ただし、情報システムはその歴史上事故がつきものであることから、バックアップやリカバリの考えが浸透しているため、その普及度合いを勘案する必要がある。一方、情報はコピーされてしまうと価値を損なってしまう特色などがあり、これらの評価は難しいことも抑えておく必要がある。

ｃ）物的リスク

コンピュータの発展期にはきわめて高価な機器を導入することが必要であり、物的リスクが最大であった。したがって初期の情報システムリスクでは高価なコンピュータ機器をどのように保護するかに焦点があった。一方、現在では社員ひとり一人にパソコンが割り当てられる企業も珍しくなくなり、相対的には物的リスクは小さくなってきている。さらには企業自身の機器の調達を自社保有からリースに変更していることも一般的になっており、その場合、企業からみると機

器の損失は小さくなっている。

d）信用リスク

機械の故障や運用の過ちあるいは不祥事などで情報システムサービスの中断、誤処理、あるいは顧客データを含むデータの漏洩、改ざんなどが発生した場合、その影響で長期的に企業が消費者やユーザから信用を失い顧客を失うリスクをいう。事故や事件の内容および各企業や業種の情報システムへの依存度合いにより評価は異なるが、これから大きくなっていくことが予想される。

e）賠償リスク

事故・誤作動、不祥事などで顧客に迷惑をかけた場合の損害賠償リスクである。情報システムの特徴として、ユーザやオペレータなどの人間の感覚ではちょっとしたミスが情報システムの特徴である大量の影響者を発生させてしまう可能性がある。これらの損害に関する評価も難しいが、今後も大量処理・高速化の方向へ情報システムは進化すること、個人情報保護規制の強化など情報の価値に重きをおいた社会法制度が整備されることをみると、今後これらの損害賠償のリスクも増大することが予想される。

3．ＪＲＭＳ質問票の構成

ＪＲＭＳでは、経営とリスクに関する「経営」、ＪＲＭＳにおけるリスクマネジメント計画に関する「計画・組織・維持」、ＪＲＭＳのリスク分析・情報セキュリティポリシーにおけるリスク分析・情報システムのリスク分析からなる「分析」、ＪＲＭＳにおけるリスク対策である「対策」という４つの大項目から構成されている。

3.1　質問項目の階層構造

ＪＲＭＳ質問票は階層構造をもって構成されている。質問項目はキーワードと識別コードにより示されている。これによりリスク対応のためのターゲットをわかりやすくさせている。

ＪＲＭＳ質問票の大項目は内容によって細分化されており、各内容は識別コードにより理解できるように構成されている。識別コードにおける大項目としての３つの数字、たとえば、経営環境については第１層から第３層目、すなわち〔１－１－１〕のように示されている。タイトルに関しては識別コードを打っていないが質問から理解できるように構成し、質問の位置をわかりやすくさせている。

たとえば、【Ｉ．経営とリスクの関係】の［Ｉ－１．経営環境とリスクマネジメント］の中項目（識別コード第２層目）では、《１．経営者の関心》、《２．経営レベルによるリスクの範囲》、《３．リスクマネジメントポリシー》、《４．組織》、《５．役割・責任》、《６．課題の明確化》、《７．行動指針》、《８．成果》といった８項目から構成されている。ＪＲＭＳ質問票は「第Ⅳ部」に収録されているが、参考のため以下に質問項目の全体構成を示す。

Ｉ.経営とリスクの関係
Ｉ－１．経営環境とリスクマネジメント
Ⅱ．ＪＲＭＳにおけるリスクマネジメント計画
Ⅱ－１．ＪＲＭＳの計画
Ⅱ－２．ＪＲＭＳの実行組織
Ⅱ－３．ＪＲＭＳの維持
Ⅲ．ＪＲＭＳのリスク分析
Ⅲ－１　ＪＲＭＳのリスク分析
Ⅲ－２　情報セキュリティポリシーのリスク分析
Ⅲ－３　情報システムのリスク分析
　Ⅲ－３－（１）情報システムのリスク分析
　Ⅲ－３－（２）情報システム総合企画
　Ⅲ－３－（３）システム開発
　Ⅲ－３－（４）システム運用
　Ⅲ－３－（５）不正アクセス・コンピュータウイルス関連
　Ⅲ－３－（６）災害
　Ⅲ－３－（７）障害
　Ⅲ－３－（８）アウトソーシング

Ⅳ．ＪＲＭＳにおけるリスク対策

Ⅳ－１．リスク対策における情報セキュリティ

Ⅳ－２．情報システムのリスク対策

Ⅳ－２－（１）情報システム総合企画

Ⅳ－２－（２）システム開発

Ⅳ－２－（３）システム運用

Ⅳ－３．不正アクセス

Ⅳ－４．コンピュータウイルス関連

Ⅳ－４－（１）コンピュータ犯罪

Ⅳ－４－（２）コンピュータウイルス

Ⅳ－４－（３）E－Commerce

Ⅳ－４－（４）電子メール

Ⅳ－５．災害対策

Ⅳ－６．障害対策

Ⅳ－７．アウトソーシング関連リスク対策

Ⅳ－８．その他関連項目

Ⅳ－９．バックアップ

Ⅳ－10．緊急時対策

Ⅳ－11．リスクファイナンス

なお、識別コードについては「４．ＪＲＭＳ質問票の使い方」で解説する。

4．ＪＲＭＳ質問票の使い方

ＪＲＭＳにおける質問票を用いて脆弱性を分析するにあたり、いくつかの準備作業が必要である。ＪＲＭＳ質問票では、リスクに対する経営上のそれぞれの役割（職能）におけるアカウンタビリティ（説明責任）の視点を考慮し、「経営者」の観点、情報システムリスクの把握および対策の実施の担い手である「情報システム部門」および情報システムの「ユーザ部門」の３つの観点から分析が行えるように構成されている。

しかし、分析対象となるのが情報リスクであることからそれぞれの回答者の回答方法について共通認識が必要である。それぞれの組織における関係については次に示すことにする。

4.1　ＪＲＭＳ質問票に回答するための事務局選定と進め方

ＪＲＭＳでは情報システムリスクを企業全体のリスクの一部と考え、企業全体のリスクを捉えたうえで情報システムに関するリスクを分析することを想定している。したがって、ＪＲＭＳにおける質問項目はかなり多岐にわたっている。そのため、ＪＲＭＳの実施にあたり「事務局」の選定の仕方を理解しておくことが必要である。このＪＲＭＳ質問票を使うにあたっては、情報リスクの性格から事務局を「情報システム部門」におくことを想定して解説する。

分析に際しては、質問票を経営者、情報システム部門、ユーザ部門にそれぞれ配付し、各回答者の回答を得、さらに回答者の論議による意見集約を実施する。各経営者、情報システム部門、ユーザ部門のそれぞれが単独で集約してもリスクの把握が可能であるが、これらの３つの集約された見解をさらに相互に比較・集約することにより企業全体の情報システムリスクを把握することができる。

4.1.1　経営者・情報システム部門・ユーザ部門

全社的なリスク対応という観点から誰がアカウンタビリティを担うかがまず問われるべきである。その場合、全社的なリスクへの責任は経営者が担うことになるため、リスクマネジメント担当の役員、たとえば、チーフリスクオフィサー（アメリカにおけるリスクマネジメント担当執行役員ＣＲＯ：Chief Risk Officer）を任命することが重要となる。そのＣＲＯの下で、リスクマネジメントを推進する組織が構成される。とりわけ組織において明確にしておくべきはリスク担当者の役割と権限である。この点が明確でないと、リスクが感知されても対策に結びつかないことにもなりかねない。

ＪＲＭＳでは、情報システムリスクをターゲットにすることからそれについてのアカウンタビリティは情報システム部門が担うべきであり、情報システムリスクマネジメント組織の編成が想定できる。ＪＲＭＳでは、情報システムに関わるリスクへの対応に焦点をあてており、また今日の組織におけるシステム環境に鑑みて情報システムリスクマネジメント組織が構成されていることが前提となる。そこでは、情報システムに関わる役割上、情報システムリスクマネジメント担当者、情報セキュリティ管理者ならびに情報システム運用管理責任者等が任命され、そこにおけるリスク対策を推進させる組織と関係者の役割権限が明確になっている必要がある。

また、情報システムを利用するユーザ部門においても適用業務別オーナーならびにユーザ部門のリスク担当責任者が明確になっていることが重要である。こうした視点から示したのが、表２

－４－１である。

表２－４－１．ＪＲＭＳ質問票への回答関係者

領域	回答担当
経営者層	リスクマネジメント担当役員
情報システム（ＩＳ）部門	情報システムリスクマネジメント担当者 情報セキュリティ管理者 情報システム運用管理責任者
ユーザ部門	適用業務別オーナー ユーザ部門リスク担当責任者

回答シートにおける経営者、ＩＳ部門、ユーザ部門は、上記の右側の職位の者が関係することになる。

4.1.2　経営者と情報システム部門

（1）企業全体のリスクの把握についての質問への回答

情報システム部門では、今回のＪＲＭＳの全体をとりまとめる事務局を務めることを想定している。今回のＪＲＭＳの構成は企業全体のリスクを把握したうえで、情報システムリスクを評価する構成としている。そのため情報システム部門の回答としている項目も企業全体のリスクマネジメントに関する質問が多く含まれている。

企業全体としてのリスクマネジメントについては、一般的には、JIS Q 2001 の考え方あるいはＣＲＯの導入を実施している場合、取締役および執行役員の中で企業全体のリスクマネジメントを担当する役員が指名される。その役員を委員長にしてリスクマネジメント委員会が結成され、企業全体のリスクはそこに集約される。企業全体のリスクマネジメントの現状を踏まえて回答する場合はそのリスクマネジメント委員会の事務局である社長室や経営企画部門にリスクに関する情報が集約されている。

したがって、企業全体のリスクを把握する【Ⅰ．経営とリスクの関係】、【Ⅱ．ＪＲＭＳにおけるリスクマネジメント計画】については、情報システム部門では必ずしも企業全体のリスクマネジメント状況を把握していないこともあり得る。その場合は、リスクマネジメント部門に確認し回答する。ここでは企業全体のリスクマネジメントの状況を踏まえたうえで、情報システムリスクの把握が成り立つとの考えを持っている。情報システム部門も全体の事務局を務めるために社長室や経営企画部門へのヒアリングを是非実施してほしい。

（2）情報システム固有の質問への回答

情報システム固有のやや技術的な内容に関する質問について、現在の情報システム部門も企画、開発、運用など業務が分担されている場合が多い。そのため、ＪＲＭＳの事務局を担当する部門がそのすべてを通常の業務の中では把握できていない場合は、当該部門にヒアリングに出向き、回答を得ることでよい。一般的な進め方同様に意見集約を実施するにあたり、事務局も同席して十分な内容を把握することが大切である。

（3）補足

（1）にも述べたように、企業全体でリスクマネジメントを実施し、リスクマネジメント委員会の事務局機能が強力な場合は、このＪＲＭＳについてもリスクマネジメント委員会の事務局である社長室や経営企画部、総務部などが事務局を実施してもよい。その場合は情報システム部門の質問項目を事務局が責任をもって情報システム部門にヒアリングを実施したり、協力を得ながら回答することになる。

4.2 質問項目に対する回答の仕方

ＪＲＭＳ質問票の右側の回答欄への回答の仕方には２つある。１つは「Ｙｅｓ／Ｎｏ」により回答する方法、もう１つは質問項目の内容に関してウエイトづけをして回答する方法がある。

参考までに回答の方法を示す。

①5階層目で、1つでも「No」がある……＞4階層目は「No」
②5階層目の組織の最重要項目が「No」である……＞4階層目は「No」
③5階層目の過半数が「Yes」である……＞4階層目は「Yes」
④5階層目の必須項目が「Yes」で、残りの項目過半数が「Yes」である……＞4階層目は「Yes」
⑤5階層目の結果を参考として……＞4階層目を責任者が判定

上記の判定基準を参考に、各組織の判断に任せる

前者の場合の回答結果については下記の点を留意してほしい。

○基本的に、【Ⅲ．ＪＲＭＳのリスク分析】の場合には、各項目別に「Ｙｅｓ／Ｎｏ」で表記する。

○４階層目に対し５階層目が１つの場合、レベル判定を「Ｙｅｓ／Ｎｏ」とするか、レベル表示とするかは選択可能とする。

後者については、以下に示した４つのレベルを勘案し、回答に際して３～０までの値を下記の判定基準に従い回答欄に記入する。レベルの設定／判断に関しては、次のようにされたい。すなわち、

○５階層目の結果を反映して、４階層目の評価は責任者の判断に任せる。

○【Ⅳ．ＪＲＭＳにおけるリスク対策】はレベル表記とする。

○複数回答者からの回答は平均値をとることにする。

○レーダーチャート（後述）を描く場合には、４階層目ないし３階層目での表記だけとし、４階層目と３階層はＹｅｓ／Ｎｏではなく、レベルで表現する。

○各階層項目の判定結果をその上位項目に反映し、レーダーチャート化していく。

なお、判定基準としてのレベルについては、次の４つのレベルを考慮されたい。

レベル３	組織内で標準を継続的に見直す仕組みができている
レベル２	組織内で標準があり、それに従って実施されている
レベル１	組織内で実施されているが、標準が定められていない
レベル０	組織内で全く意識されておらず、何もしていない

4.2.1　回答者の回答の仕方

（1）経営者

理論的・実務的にトップは最高経営者一人であるが、経営者層としているのは、少なくとも経営責任を有する職位の者が客観的に情報リスクに対する組織の脆弱性を分析するという認識で対応することから、回答者として3名以上が望ましい。

（2）情報システム部門（回答シートにおけるＩＳ部門）

情報システム関係のリスクへの対応に責任ある職位の者、少なくとも5～6名程度が回答シートの該当質問項目に回答するのが望ましい。

（3）ユーザ部門

情報システム以外の業務に従事するとしても、現在の業務環境から情報システムと切り離された仕事は考えにくい。そこで、情報システムと業務に関係するリスク環境に対する認識を共有し深める目的から、部署にもよるが6～10名程度の関係者が回答するのが望ましい。

役職における階層とともに、階層構造になっている質問項目への回答により齟齬が生じる場合がある。いくつかのパターンが考えられるが、たとえば、経営者では脆弱性が低く、情報システム部門では脆弱性が高いといったケースがあったとする。その場合、どこに原因があるのかを究明することにより、リスクの組織に対する作用の意味、リスクについての感覚の違いなどが把握でき、リスク対応の実態を把握することが可能になる。この点については、本報告書に示されている例示を参考にしながら、ビジネスゲーム感覚により回答し、その結果から組織の脆弱性を分析されたい。

4.2.2　識別コードの意味

質問項目に記載されている識別コードには次のような意味がこめられている。たとえば、大項目を意味する1階層目はローマ数字の【Ⅰ．経営とリスクの関係】という見出しのタイトルを表している。

2階層目は［Ⅱ－1．ＪＲＭＳの計画］のタイトル、3階層目では［Ⅲ－3－（1）情報システムのリスク分析］〔3-3-1〕の課題タイトル、4階層目「ＱＩＴ戦略に係わるリスクを分析していますか？」〔3-3-1-1〕、さらに5階層目「Q情報システムに係わるリスクを分析していますか？」〔3-3-1-1-1〕といった質問レベルをそれぞれ表している。

質問項目への回答については、職位により回答シートに示されているそれぞれの層について記入用の空欄で表示している。それぞれの職位に属する関係者、特に5階層目の質問は情報システム部門担当者が関係するが、当該質問項目について脆弱性分析を行い、4階層目の脆弱性を把握するのである。

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
経営とリスク	経営とリスク	1．経営とリスクの関係				
経営環境とリスクマネジメント	経営環境とリスクマネジメント	1－1．経営環境とリスクマネジメント				
1．経営者の関心	経営者の関心	1- 1- 1- 1	Q 経営者は情報システムに関するリスクについて認識していますか？			
2．経営レベルによるリスクの範囲	経営レベルによるリスクの範囲	1- 1- 1- 2	Q 経営レベルのリスクにリスクマネジメントの範囲を広げて対応していますか？			
3．リスクマネジメントポリシー	リスクマネジメントポリシー	1- 1- 1- 3	Q リスクマネジメントに関する全社的なポリシー（方針）を有していますか？			
		1- 1- 1- 3- 1	Q リスクマネジメントポリシーは、最高経営者のもと会社的に構成されていますか？			
		1- 1- 1- 3- 2	Q 貴社では経営理念に基づくリスクマネジメントポリシーを定めていますか？			
		1- 1- 1- 3- 3	Q リスクマネジメントポリシーでは、経営を脅かす事態に対する明確な対策を有していますか？			
		1- 1- 1- 3- 4	Q 緊急事態発生時の役員、スタッフ、担当者の役割はリスクマネジメントポリシーに定められていますか？			
		1- 1- 1- 3- 5	Q リスクマネジメントポリシーではコンプライアンスを重視していますか？			
		1- 1- 1- 3- 6	Q リスクマネジメントポリシーで内部監査の実施を明記していますか？			
		1- 1- 1- 3- 7	Q リスクマネジメントポリシーで外部監査の実施を明記していますか？			
		1- 1- 1- 4	Q リスクマネジメントポリシーに基づき、実施基準が機能部門別に構成されていますか？			
		1- 1- 1- 4- 1	Q 有効に機能するようフィードバックループ構成になっていますか？			
		1- 1- 1- 4- 2	Q 経営にとってのマイナス情報を吸い上げる機能を明確にしていますか？			
		1- 1- 1- 4- 3	Q スタッフに対し業務の機能分野ごとに教育訓練を行うことが計画化されていますか？			
		1- 1- 1- 4- 4	Q 「JIS Q 2001 リスクマネジメントシステム構築のための指針」を知っていますか？			
4．組織	組織	1- 1- 1- 5	Q 組織として守るべき対象を明確にしていますか？			
5．役割・責任	役割・責任	1- 1- 1- 6	Q 守るべき対象との関連において、リスクマネジメントに関する役割・責任・権限が文書化されていますか？			
6．課題の明確化	課題の明確化	1- 1- 1- 7	Q 組織におけるリスクマネジメントの具体的なリスク対応上の課題を明確に定めていますか？			
		1- 1- 1- 7- 1	Q 行動指針は、経営資源の保全を含んでいますか？			
		1- 1- 1- 7- 2	Q リスクに対する社会的責任をも含んでいますか？			
		1- 1- 1- 7- 3	Q 行動指針では基本的な目的を明確に設定していますか？			
		1- 1- 1- 7- 4	Q 機能部門におけるリスク対応は明確にされていますか？			
7．行動指針	行動指針	1- 1- 1- 8	Q リスクマネジメントの行動指針は明確にされていますか？			
		1- 1- 1- 8- 1	Q リスクマネジメントの評価を明確に行うシステムとなっていますか？			
		1- 1- 1- 8- 2	Q リスクマネジメントのテストを行うように定められていますか？			
		1- 1- 1- 8- 3	Q リスクマネジメントの監査を行うように定められていますか？			
		1- 1- 1- 8- 4	Q 環境変化に応じリスクマネジメントの行動計画の是正改善を含んでいますか？			
8．成果	成果	1- 1- 1- 9	Q リスクマネジメントシステムの達成の成果を明示していますか？			

図２－４－１．質問票サンプル

4.3 回答のプロセス

ＪＲＡＭではリスク対策との関係からすべての質問項目についてウエイトづけがなされるようになっていたが、ＪＲＭＳではキーワードに示される質問項目によって、「Ｙｅｓ／Ｎｏ」、もしくはレベルによるウエイトづけを行って回答するという方式を採用している。回答の仕方は、それぞれの回答担当者が出した結果を集計シートに記入し、その結果を判定することになる。

上記のプロセスをフローチャートで描けば、図２－４－２のとおりである。

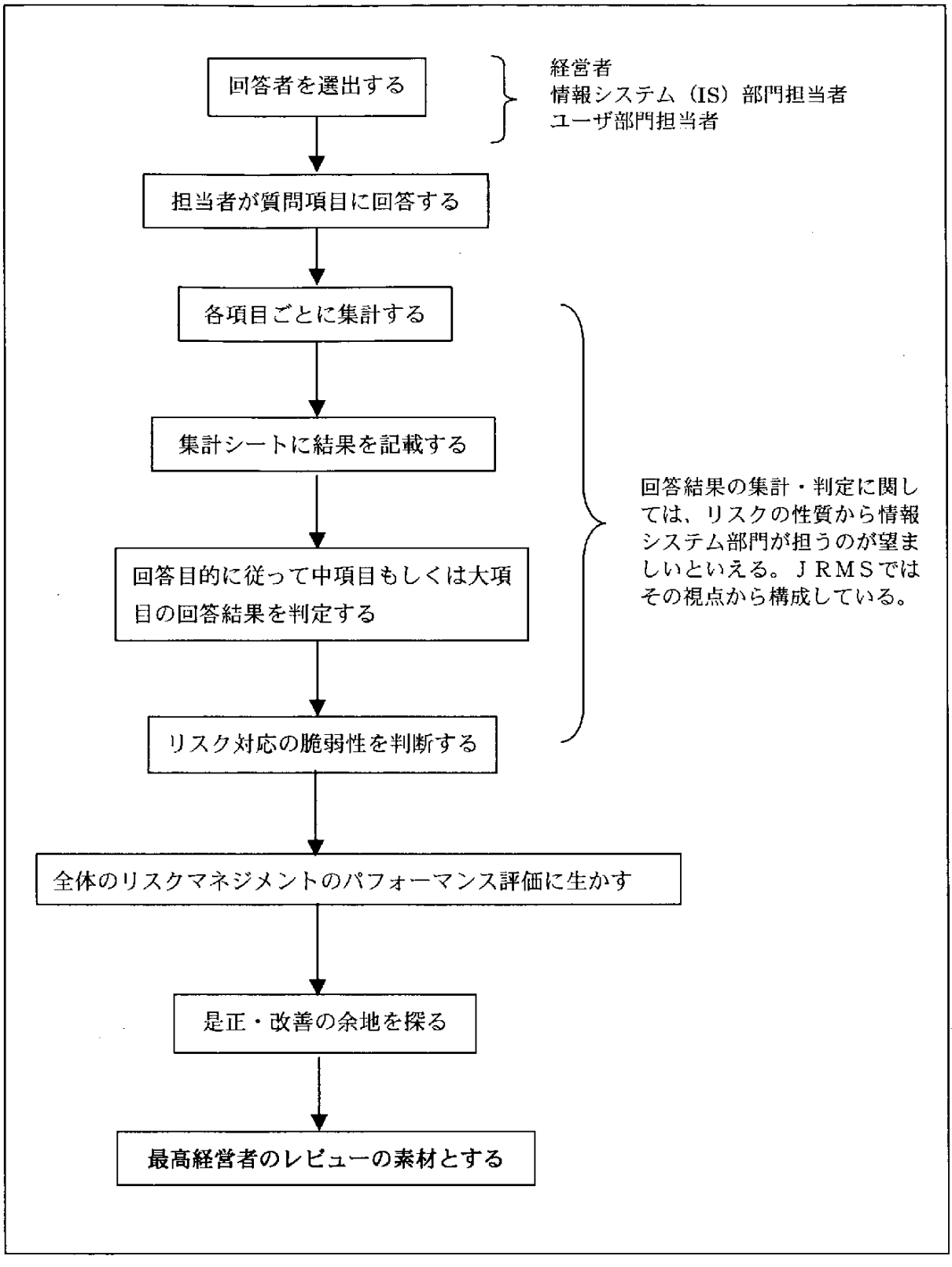


図２－４－２．ＪＲＭＳ回答プロセス

4.4 回答時の留意点

4.4.1 回答者別の留意点

回答の対象が複数である場合、分析目的により対象を１つに絞り込むことが重要である。また、回答しにくい領域では、特にこだわることなく感じたままを回答するのはＪＲＡＭと同じである。以下、回答者別に留意点を示しておきたい。

（１）経営者のケース

ＪＲＭＳ質問票では、その内容により経営者、情報システム部門、ユーザ部門に回答者を分けている。これは、質問の内容について組織の職位に応じたアカウンタビリティ（説明責任）を有しているかに鑑みて、ＪＲＭＳ質問票のそれぞれの回答欄に回答すべき関係者を割り当てている。

経営者は、その立場からステークホルダーにより企業経営を任されており、最終的な責任を持ち、組織としての目的を成し遂げることである。したがって、リスクマネジメントはその大きな柱の１つとなっている。

たとえば、ある会社で3,000万円の資産が紛失した場合、経営者は部下が悪かったとか、部下の管理が不十分だった、で済ませられるだろうか。当然、経営者として適切な内部統制の仕組みを作っていなかったことに対しての責任が問われる。しかし、これと同等な金額の被害がコンピュータウイルスの感染で実際に起きている。2001年９月に発生したNimdaウイルスの感染により、1,000 台位のパソコンが被害を受け、ハードディスクのフォーマットを余儀なくされた会社は１社ではない。この場合、パソコンの再設定費用、パソコンが使えないことによるユーザ業務の阻害等を換算すれば、6,000 万円以上の被害である。この例のように、情報システムに関わるリスクはすでに情報システム部門だけに任せておけばよいレベルを超えて、経営者が直接関与すべき規模に達している。

しかし、経営者がリスク対策の専門家になる必要はない。経営者が行わなければならないのは、組織として適切にリスクを管理する仕組みを作ることである。これには、リスクマネジメントを行う部門に適切なアカウンタビリティを割り当て、定期的に報告させるという、経営として通常行っているPlan-Do-Check-Actのサイクルをリスクマネジメントについても適用すべきである。情報システムのリスクというと、コンピュータウイルスの例のように、非常に技術的な側面に目が行きがちであるが、より重要なのはリスクに対して組織が適切に対応できるように管理することである。このために、経営者は情報システム部門に対して、技術の言葉だけではなく、リスクをビジネスの言葉で説明するように求めるべきである。また、ユーザ部門に対しても、情報システムのリスクマネジメントは情報システム部門だけに任せておくべきものではなく、ユーザ部門にも責任があることをはっきり示し、その役割実施を求めるべきである。

すべての企業がE-Businessに移行しつつある現在、これまでの企業内に閉じていたシステムがインターネットにより外部と接続され、ビジネスが大きく変わるメリットがある反面、インターネットに接続することによるリスクの日常化とその増大もある。経営者はこれに対応して、情報システムのリスクマネジメントをこれまでのような万が一の保険としてではなく、インターネットに接続することに対する税金として捉え、適切な対応を取るべきである。

ＪＲＭＳ質問票における経営者の回答項目は、自社の情報システムのリスクに対するチェックリストとして使うことも可能である。

（2）情報システム部門

【Ⅱ．ＪＲＭＳにおけるリスクマネジメント計画】はJIS Q 2001によるところが多い。したがって、できれば回答者はJIS Q 2001を理解していることが望ましいが、その内容を知らなくても基本的な経営に関する要求事項であるので常識的な回答を行うことでよい。

この【Ⅱ】は企業全体のリスクマネジメントを問うものであるので、情報システム部門だけの視点では答えにくいものもある。その場合は企業全体のリスクマネジメントを実施している部門にヒアリングを行い回答する。他のところでも記述したが、情報システムリスクは単独に企業の中に存在するのではなく、企業全体の大きなリスクマネジメントの中の、企業として優先的に対処を必要とするいくつかのリスクのうちの１つとして認識されるべきである。そのため、情報システム部門としても企業全体のリスクおよびその管理の仕組みについては十分認識しておくことが望ましい。当然、ユーザ部門も同様である。この質問をきっかけに単に部門の中だけのリスクに限定せず、情報システムのリスクの企業規模への広がりを把握することが必要である。

（3）ユーザ部門

現代の情報システム環境においては組織全体がシステムに依存している。したがって、ユーザ部門に固有の情報システム関係のリスクについて分析する必要性がある。そのため、ＪＲＭＳ質問票においてもユーザ部門が回答すべき項目を示している。しかし、回答対象となっている項目数は少ない。そのことでユーザ部門のリスクに対する業務上の位置を軽視しているわけではない。

むしろ、業務内容に鑑みて、必要と思われるキーワードに関係する項目を回答対象とすべきである。重要な留意点は、ユーザとして情報システムを業務上利用しているとしても、利用に関して種々のリスクが付随しているはずであり、思わぬところにリスクが潜んでいるものである。それだけにＪＲＭＳの質問項目に接し、回答を行い、リスクに対する意識なり感性を磨き、リスクに対する認識を共有するように利用してほしい。

ユーザ部門として指摘しておいた回答担当者は適用業務別オーナーとユーザ部門リスク担当責任者であったが、そうした役割担当者の名称については、ＪＲＭＳを利用する組織において指名すればよい。回答者数として６～10名程度をあげておいたが、常に同じ者が回答するのではなく、組織におけるリスク認識の共有のため、ローテーションなどを考慮し、多くのユーザ部門の者がＪＲＭＳ質問票への回答にチャレンジするのが望ましいといえる。

4.4.2　大項目別の留意点

（1）【Ⅰ．経営とリスクの関係】の留意点

a）目的

この質問項目は、経営責任を担う経営者が経営と情報システムに関わる脆弱性を把握し、リスク対応を行う手がかりを与えることを目的としている。経営者として、既述のようにリスク対策の専門家である必要はないが、情報リスクに関する感性をもってリスク対応の仕組みを組織化すべく構成されている。

b）回答の留意点

回答の仕方については、Ｙｅｓ／Ｎｏ方式もしくは３～０のレベルによる方式のいずれも利用可能である。回答シートに該当する質問項目に対する識別コード表を以下に示しておく。

質問項目の識別コードは、次の階層構成になっている。

【Ⅰ．経営とリスク】の関係　［Ⅰ－１．経営環境とリスクマネジメント］の例

１階層	２階層	３階層	４階層	５階層
１－	１－	１－	2	
１－	１－	１－	3	
１－	１－	１－	３－	1
１－	１－	１－	３－	2
１－	１－	１－	３－	⋮
１－	１－	１－	３－	
１－	１－	１－	３－	7

なお、回答に際して、留意してほしい点は、５階層目がある場合とない場合があることである。

（2）【Ⅱ．ＪＲＭＳにおけるリスクマネジメント計画】の留意点

この項目は企業全体のリスクマネジメントおよびその中での情報システムリスクマネジメント推進のための基礎項目を問う設問としているため､多くはＹｅｓ／Ｎｏで回答することができる。当初は多くの項目がＮｏと回答されることが予想される。それは現在の日本の多くの企業や自治体ではこのようなリスクマネジメント態勢の仕組みが構築されていないからである。リスクマネジメントシステムは継続的な改善運動であるため、この項目はまず最低限の項目を網羅的に実施することが望ましい。

そして、情報システム環境の変化に鑑みて、質問項目を増やし個々のレベルアップを図ることが望ましい。特に情報システムリスクでは個々の対応策の技術的側面に目が行きがちである。企業全体でリスクマネジメント態勢を作り上げ、その中で情報システムリスクが位置づけられることがこの設問に取り組むことで期待できる。

（3）【Ⅲ．ＪＲＭＳのリスク分析】の留意点

ａ）目的

リスク対策を考える場合、そのリスク対策にどこまでのリソースを投資するかはそのリスクが組織に対して与える影響の程度により決定すべきである。この影響度の大きさについて、組織内の共通の理解が得られていないと、白黒の議論になり、全く対策を行わないか、不必要な事項まで含んだ過大なリスク対策を実施することになる。リスク分析のプロセスを実施することにより、組織内の関係者で徹底的に議論を行い、共通の理解を得ることができれば、被害が顕在化した場合のリスクの大きさについて統一した数字が得られるので、これとバランスがとれる投資額を決めることができる。

ｂ）回答の留意点

従来、情報システムのリスク分析というと地震を代表とする外部の突発的な要因により組織の情報システムがどの程度の被害を受けるか、という範囲で考えていたが、ＪＲＭＳでは情報システムの開発や運用といった、通常の情報システムのプロセスにおけるリスクも含んでいるのが特徴である。たとえば、銀行等の社会的に重要なシステムでは、地震等の災害によるシステム停止よりも、ソフトウェアのバグや運用でのミスといった、情報システムのプロセスに内在する原因で停止する率が高い。これに対応して、ＪＲＭＳでは、通常の情報システムのプロセスについて

も主にセキュリティの観点からリスク分析の対象にしている。しかし、これらの領域におけるリスク分析、特に［３－（２）情報システム総合企画］のリスク分析は、被害とその原因の因果関係を定量的に結びつけるのは困難である。したがって、回答の作成にあたっては、厳密な定量的リスク分析だけではなく、その項目でリスクについて考慮したか否かといった定性的なリスク分析も含めて回答を作成すべきである。

（４）【Ⅳ．ＪＲＭＳにおけるリスク対策】の留意点

ａ）目的

この質問項目は、組織におけるリスク対策上の脆弱性を把握し、把握した脆弱性を補強するための指針を明確にすることを目的としている。

したがって、単に脆弱性を捉えるのみでなく、その対策のさらなる強化の必要性を捉えて、強化の方向性を明確にすることが大切である。

ここでの分析はレーダーチャートを用いて行うことを基本としており、レーダーチャートで示されたパターンを視覚によって見ることができる。

その結果、組織はそれぞれキーワードごとの脆弱性を把握し、有効な対策を進めることができる。

以上は、各質問項目の回答にあたって、留意しなければならない基本的事項である。

ｂ）事前準備

この質問項目は、多くの組織における情報システム全般を網羅するように設定されている。

したがって、個別の組織が実際に質問項目を用いる場合は、事前に対象質問項目の評価（自組織におけるあるべき状態）をして、脆弱性把握の対象範囲を明確にしておく必要がある。

各質問項目ごとの事前評価は、「4.2　質問項目に対する回答の仕方」に示されている判定基準に基づいて４レベルの方式で評価を行う。

（例）［Ⅳ―２．情報システムのリスク対策］　［Ⅳ－２－（３）システム運用］の例

識別コード	質問項目	事前評価
４－２－３－１	Ｑシステムの運用は…？	3
４－２－３－１－１	Ｑシステムの運用計画は…？	2

（注）：質問項目が自組織体に該当しない場合は「０」とする。

：事前評価は、回答シートの回答欄を用いる。

識別コード〔4-2-3-1〕は、自組織として**十分実施する必要がある**ことが妥当であると事前評価した質問項目。

識別コード〔4-2-3-1-1〕は、自組織として**ほぼ十分であればよい**と事前評価で判断した質問項目。

それぞれの質問項目を上記の要領で事前評価しておくと、自組織のリスクマネジメント上のあるべき姿と実態の格差をレーダーチャートで捉えることができる。

ｃ）回答の留意点

１）全般

回答はすべて４レベルの方式（「4.2　質問項目に対する回答の仕方」）に基づいて行う。

各質問項目ごとに該当する判定基準を用いて回答欄に＜3・2・1・0＞を記入していくが、あまり深く考えないで記入することがポイントである。

2）質問項目の識別コード構成と記入上の留意点

質問項目の識別コードは、次の階層構成になっている。

［Ⅳ－1．リスク対策における情報セキュリティ］の例

質問項目	1階層	2階層	3階層	4階層	5階層
X	4－	1－	1－	1	
Y	4－	1－	1－	2	
	4－	1－	1－	2－	1
	4－	1－	1－	2－	2
	4－	1－	1－	2－	⋮
	4－	1－	1－	2－	⋮
	4－	1－	1－	2－	6

・Xの場合

①直接4階層目に判定基準を適用し、評価した結果を回答欄に記入する。

②**集計欄には単純平均値**を記入する。

・Yの場合

①5階層目の質問項目を判定基準に基づいて評価する。

②5階層目の全質問項目の評価結果を参考にして4階層目の質問項目を「4.2　質問項目に対する回答の仕方」に示されている包括判定基準に基づいて包括的に評価し、結果を該当の回答欄に記入する。

③集計欄への記入はXの場合と同様に単純平均値を記入し、各キーワード単位の全体評価とする。

これらの作業を行った後、全体評価結果を用いてレーダーチャートを作成し、評価する。

表2－4－2．包括判定基準例

	0	1	2	3
個々の項目の判定	標準が何もなく、実施していない	実施しているが標準がない	実施しており標準がある	実施しており、標準があり、継続的に見直している
	定めていない	一部しか定めていない	概ね定めている	定めている
	何もしていない	一部しか実施していない	概ね実施している	十分実施している
	まったく含まれていない	一部しか含まれていない	概ね含まれている	すべて含まれている
	満たしていない	一部しか満たしていない	概ね満たしている	条件を十分満たしている
	1回も実施していない（0%）	たまにしか実施していない（20%程度）	ほぼ実施している（70%程度）	全回実施している（90～100%）
4階層目の総評	評価できない	一部しか評価できない	概ね評価できる	十分評価できる

4.5 レーダーチャートの作り方

4.5.1 レーダーチャートを作成する質問項目の階層

ＪＲＭＳでは階層構造を持った質問項目を示している。この階層は全体で５つの階層を持っており、その４階層目が一番基礎となるレーダーチャートの作成単位となる。

このレーダーチャートの作成にあたっては、[Ｉ－１．経営環境とリスクマネジメント]を事例としてとりあげ、以下の作業を行うことを想定している。ここではレーダーチャートの作り方を説明する。

[Ｉ－１．経営環境とリスクマネジメント]は《１．経営者の関心〔1-1-1-1〕》、《２．経営レベルによるリスクの範囲〔1-1-1-2〕》、《３．リスクマネジメントポリシー〔1-1-1-3〕、〔1-1-1-4〕》、《４．組織〔1-1-1-5〕》、《５．役割・責任〔1-1-1-6〕》、《６．課題の明確化〔1-1-1-7〕》、《７．行動指針〔1-1-1-8〕》、《８．成果〔1-1-1-9〕》の８つのキーワードで構成されている。したがって、[Ｉ－１]のレーダーチャートは８項目で構成されることになる。

4.5.2 各項目の評価

各項目の評価は質問の内容によりＹｅｓ（Y）／Ｎｏ（N）で評価するものや、レベル３から０までの４つのレベルで評価するものがある。これらは質問により使用時にどちらを選択してもかまわない。たとえば、《１．経営者の関心》について関心が高いかにつきＹｅｓ／Ｎｏで回答しても、４レベル方式で回答してもよい。これらレベルの尺度を合わせるためにＹｅｓには３点、Ｎｏには０点の評価を行うこととする。質問項目の内容から該当しない場合が出てくるかもしれないが、この点については、回答対象外として扱うことになる。

さて、実際の評価は、回答者が５人の場合、経営者あるいは情報システム部門などそれぞれの該当項目につき各自が評価を行う。そして、一次的には、これらの回答の平均を取り、レーダーチャートを作成し議論するとよい。その議論を基に意見集約を行い、最終的なレーダーチャートを作成する。

キーワード	キーワード	識別コード	質問項目	回答欄 A	B	C	D	E	集計	全体評価
経営とリスク	経営とリスク	Ⅰ．経営とリスクの関係								
経営環境とリスクマネジメント	経営環境とリスクマネジメント	Ⅰ－１．経営環境とリスクマネジメント								
1．経営者の関心	経営者の関心	1-1-1-1	Q 経営者はコンピュータ関連のリスクについて関心は高いですか？							
2．経営レベルによるリスクの範囲	経営レベルによるリスクの範囲	1-1-1-2	Q 経営レベルのリスクにリスクマネジメントの範囲を広げて考えていますか？							
3．リスクマネジメントポリシー	リスクマネジメントポリシー	1-1-1-3	Q リスクマネジメントに関する全社的なポリシー(方針)を有していますか？							
		1-1-1-3-1	Q リスクマネジメントポリシーは、最高経営者のもと全社的に構成されていますか？							
		1-1-1-3-2	Q 貴社では経営理念に基づくリスクマネジメントポリシーを定めていますか？							
		1-1-1-3-3	Q リスクマネジメントポリシーでは、経営を脅かす事態に対する明確な対策を有していますか？							
		1-1-1-3-4	Q 緊急事態発生時の役員、スタッフ、担当者の役割はリスクマネジメントポリシーに定められていますか？							
		1-1-1-3-5	Q リスクマネジメントポリシーではコンプライアンスを重視していますか？							
		1-1-1-3-6	Q リスクマネジメントポリシーで内部監査の実施を明記していますか？							
		1-1-1-3-7	Q リスクマネジメントポリシーで外部監査の実施を明記していますか？							
		1-1-1-4	Q リスクマネジメントポリシーに基づき、実施基準が機能部門別に構成されていますか？							
		1-1-1-4-1	Q 有効に機能するようフィードバックループ構成になっていますか？							
		1-1-1-4-2	Q 経営にとってのマイナス情報を吸い上げる機能を明確にしていますか？							
		1-1-1-4-3	Q スタッフに対し業務の機能分野ごとに教育訓練を行うことが計画化されていますか？							
		1-1-1-4-4	Q リスクマネジメントシステム構築の指針(JIS)を知っていますか？							
4．組織	組織	1-1-1-5	Q 組織として守るべき対象を明確にしていますか？							
5．役割・責任	役割・責任	1-1-1-6	Q 守るべき対象との関連において、リスクマネジメントに関する役割・責任・権限が文書化されていますか？							
6．課題の明確化	課題の明確化	1-1-1-7	Q 組織におけるリスクマネジメントの具体的なリスク対応上の課題を明確に定めていますか？							
		1-1-1-7-1	Q 行動指針は、経営資源の保全を含んでいますか？							
		1-1-1-7-2	Q リスクに対する社会的責任をも含んでいますか？							
		1-1-1-7-3	Q 行動指針では基本的な目的を明確に設定していますか？							
		1-1-1-7-4	Q 機能部門におけるリスク対応は明確にされていますか？							
7．行動指針	行動指針	1-1-1-8	Q リスクマネジメントの行動指針は明確にされていますか？							
		1-1-1-8-1	Q リスクマネジメントの評価を明確に行うシステムとなっていますか？							
		1-1-1-8-2	Q リスクマネジメントのテストを行うように定められていますか？							
		1-1-1-8-3	Q リスクマネジメントの監査を行うように定められていますか？							
		1-1-1-8-4	Q 環境変化に応じリスクマネジメントの行動計画の修正を含んでいますか？							
8．成果	成果	1-1-1-9	Q リスクマネジメントシステムの達成の成果を明示していますか？							

Y= 3
N= 0

レベル3：組織内で標準を、継続的に見直す仕組みができている。
レベル2：組織内で標準があり、それに従って実施されている。
レベル1：組織内で実施されているが、標準が定められていない。
レベル0：組織内で全く実施されておらず、何もしていない。

図２－４－３．回答シート

4.5.3　実際のレーダーチャートの作成方法

この［Ｉ－１］にはいくつかの構造の異なる項目があるので、その場合の平均値算出の仕方について「図２－４－４．回答シート例１」を用いて説明する。

キーワード	キーワード	識別コード	質問項目	回答欄 A	B	C	D	E	集計	全体評価
経営とリスク	経営とリスク	Ｉ．経営とリスクの関係								
経営環境とリスクマネジメント	経営環境とリスクマネジメント	Ｉ－１．経営環境とリスクマネジメント								
1．経営者の関心	経営者の関心	1-1- 1- 1	Q 経営者はコンピュータ関連のリスクについて関心は高いですか？	3	3	2	1	1	2	2
2．経営レベルによるリスクの範囲	経営レベルによるリスクの範囲	1-1- 1- 2	Q 経営レベルのリスクにリスクマネジメントの範囲を広げて考えていますか？	3	3	2	2	2	2.4	2.4
3．リスクマネジメントポリシー	リスクマネジメントポリシー	1-1- 1- 3	Q リスクマネジメントに関する全社的なポリシー(方針)を有していますか？	2	3	2	2	2	2.2	2.3
		1-1- 1- 3- 1	Q リスクマネジメントポリシーは、最高経営者のもと全社的に構成されていますか？	Y	Y	Y	Y	Y		
		1-1- 1- 3- 2	Q 貴社では経営理念に基づくリスクマネジメントポリシーを定めていますか？	Y	Y	Y	Y	Y		
		1-1- 1- 3- 3	Q リスクマネジメントポリシーでは、経営を脅かす事態に対する明確な対策を有していますか？	Y	Y	Y	Y	N		
		1-1- 1- 3- 4	Q 緊急事態発生時の役員、スタッフ、担当者の役割はリスクマネジメントポリシーに定められていますか？	Y	Y	Y	Y	Y		
		1-1- 1- 3- 5	Q リスクマネジメントポリシーではコンプライアンスを重視していますか？	N	Y	N	N	N		
		1-1- 1- 3- 6	Q リスクマネジメントポリシーで内部監査の実施を明記していますか？	Y	Y	Y	Y	Y		
		1-1- 1- 3- 7	Q リスクマネジメントポリシーで外部監査の実施を明記していますか？	N	N	N	N	N		
		1-1- 1- 4	Q リスクマネジメントポリシーに基づき、実施基準が機能部門別に構成されていますか？	Y	Y	N	Y	Y	2.4	
		1-1- 1- 4- 1	Q 有効に機能するようフィードバックループ構成になっていますか？	Y	Y	N	Y	Y		
		1-1- 1- 4- 2	Q 経営にとってのマイナス情報を吸い上げる機能を明確にしていますか？	N	N	N	Y	N		
		1-1- 1- 4- 3	Q スタッフに対し業務の機能分野ごとに教育訓練を行うことが計画化されていますか？	Y	Y	Y	Y	Y		
		1-1- 1- 4- 4	Q リスクマネジメントシステム構築の指針(JIS)を知っていますか？	Y	N	N	N	N		
4．組織	組織	1-1- 1- 5	Q 組織として守るべき対象を明確にしていますか？	N	N	Y	Y	Y	1.8	1.8
5．役割・責任	役割・責任	1-1- 1- 6	Q 守るべき対象との関連において、リスクマネジメントに関する役割・責任・権限が文書化されていますか？	Y	N	Y	N	N	1.2	1.2
6．課題の明確化	課題の明確化	1-1- 1- 7	Q 組織におけるリスクマネジメントの具体的なリスク対応上の課題を明確に定めていますか？	2	3	1	3	2	2.2	2.2
		1-1- 1- 7- 1	Q 行動指針は、経営資源の保全を含んでいますか？	Y	Y	N	Y	Y		
		1-1- 1- 7- 2	Q リスクに対する社会的責任をも含んでいますか？	N	N	N	N	Y		
		1-1- 1- 7- 3	Q 行動指針では基本的な目的を明確に設定していますか？	N	N	Y	Y	N		
		1-1- 1- 7- 4	Q 機能部門におけるリスク対応は明確にされていますか？	Y	Y	Y	Y	Y		
7．行動指針	行動指針	1-1- 1- 8	Q リスクマネジメントの行動指針は明確にされていますか？	N	Y	Y	N	N	1.2	1.2
		1-1- 1- 8- 1	Q リスクマネジメントの評価を明確に行うシステムとなっていますか？	N	Y	Y	N	N		
		1-1- 1- 8- 2	Q リスクマネジメントのテストを行うように定められていますか？	N	N	Y	Y	Y		
		1-1- 1- 8- 3	Q リスクマネジメントの監査を行うように定められていますか？	N	N	N	N	N		
		1-1- 1- 8- 4	Q 環境変化に応じリスクマネジメントの行動計画の修正を含んでいますか？	Y	Y	Y	Y	N		
8．成果	成果	1-1- 1- 9	Q リスクマネジメントシステムの達成の成果を明示していますか？	Y	Y	Y	Y	N	2.4	2.4

Y= 3
N= 0

レベル3：組織内で標準を、組織的に見直す仕組みができている。
レベル2：組織内で標準があり、それに従って実施されている。
レベル1：組織内で実施されているが、標準が定められていない。
レベル0：組織内で全く意識されておらず、何もしていない。

図２－４－４．回答シート例１

（１）１項目１問の場合

《１．経営者の関心〔1-1-1-1〕》などでは１項目が１つの質問で構成されている。関心の程度について５人の回答者が上記に従い、各自４つのレベルで評価をしたとすると、回答シートの右欄の「集計」・「全体評価」に５人の平均点が表示される。たとえば各々の評価が＜３，３，２，１，１＞であった場合、この評価は＜２点＞となる。

次に《８．成果〔1-1-1-9〕》をＹｅｓ／Ｎｏで評価したとする。この場合５人が＜Y，Y，Y，Y，N＞と回答したとすると、Ｙ＝３点、Ｎ＝０点であるので、回答シートの右欄の「集計」・「全体評価」に示す値は＜2.4点＞となる。

（２）１項目に１問で５階層目がある場合

【７．行動指針〔1-1-1-8〕】の場合、４階層目〔1-1-1-8〕までの質問は１つだが、それに５つ目の階層〔1-1-1-8-1〕から〔1-1-1-8-4〕がある。この場合は５階層目の評価をまず実施し、その内容を各自が判断して４階層目の評価を行う。たとえばすべてＹｅｓ／Ｎｏで評価するとして、５人の回答者のうち、Ｂ氏は〔1-1-1-8-1〕から〔1-1-1-8-4〕について、５層目を＜Y，N，N，Y＞と評価した。この総合的な内容を判断して４階層目〔1－1－1－8〕を＜Y＞と評価した。

このように、５人の回答者が各々評価を行い、４階層目を評価する。たとえば、その評価が＜N、Y、Y、N、N＞であれば、集計・全体評価は＜1.2 点＞となる。この５階層目の集約の仕方は質問ごとに定めておく。５階層目から４階層目を評価する場合、どのように評価するかであるが、一般には各項目を暗黙的に重み付けを行って総合評価を実施する。もう１つは、監査などでの考え方であるが、どれか１つでもＮｏがあれば全体もＮｏとする考え方である。この間を取って、設問のうちいくつかを必須項目として考えるものもある。この場合、設問のうちいくつかの必須項目についてすべてにＹｅｓがついて初めてその他の項目を合わせて総合評価する。

（３）１項目に複数の質問がある場合

《3.リスクマネジメントポリシー》の項目の場合、中の４階層目に２つの括りの質問、〔1-1-1-3 Qリスクマネジメントポリシーに関する全社的なポリシーを有していますか？〕と〔1-1-1-4 Qリスクマネジメントポリシーに基づき、実施基準が機能部門別に構成されていますか？〕が存在する。今までと同様に各々作業すると〔1-1-1-3〕が＜2.2 点＞、〔1-1-1-4〕が＜2.4 点＞となり、この《3》全体の評価はこの２つの平均をとり＜2.3 点＞となる。また、質問項目により質問間に重み（ウエイト）をつけて加重平均を行ってもよい。（加重平均の方法については、（５）で後述する）

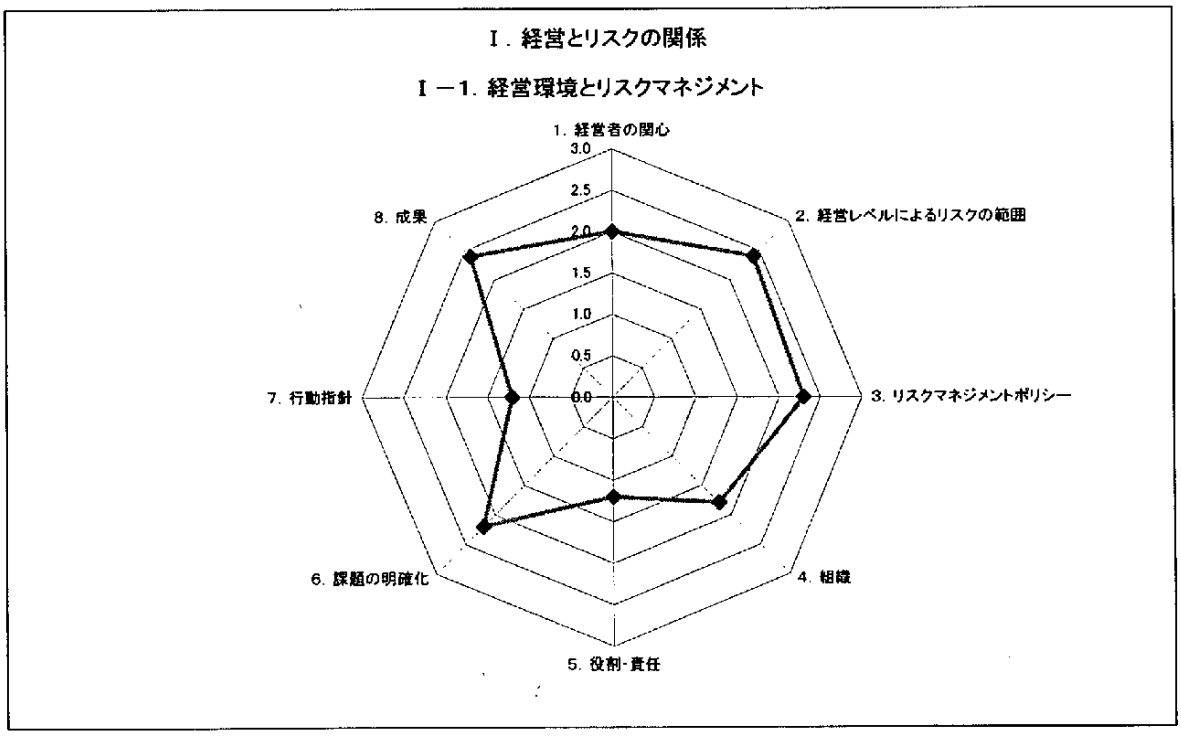


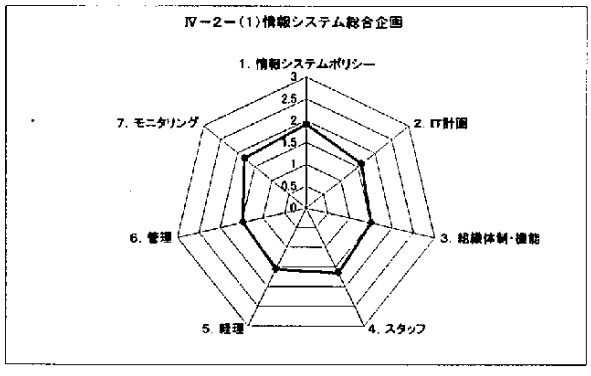
図２－４－５．４階層目のレーダーチャート例

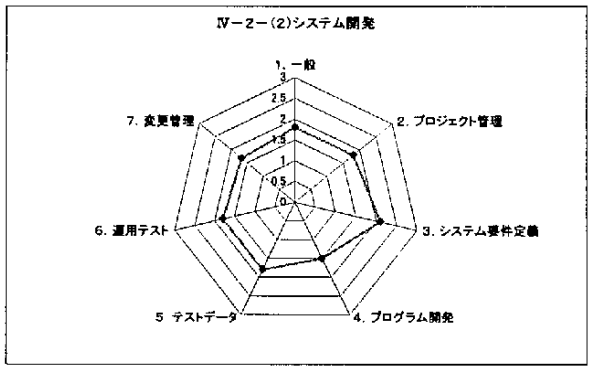
（４）上位階層のレーダーチャート

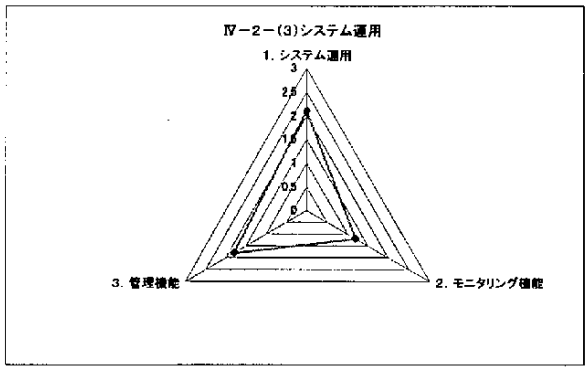
今まで４階層目のレーダーチャートの作成について解説した。このＪＲＭＳはさらに上位階層にレーダーチャートを集約していくことができる。たとえば、３階層目のレーダーチャートの例としては〔Ⅳ－２．情報システムのリスク対策〕では４階層目で作成したレーダーチャートをさ

らに３階層目の［（１）情報システム総合企画］、［（２）システム開発］、［（３）システム運用］の３つの評価項目によるレーダーチャートを作成することができる。この場合それぞれの評価点は中の４階層目の評価点の単純平均である。もちろん加重平均を用いてもよい。たとえば、［（３）システム運用］では《１．システム運用》、《２．モニタリング機能》、《３．管理機能」の３つの平均値で評価される。

そして２階層目、１階層目とそれぞれ区分ごとに評価が集約されていく。







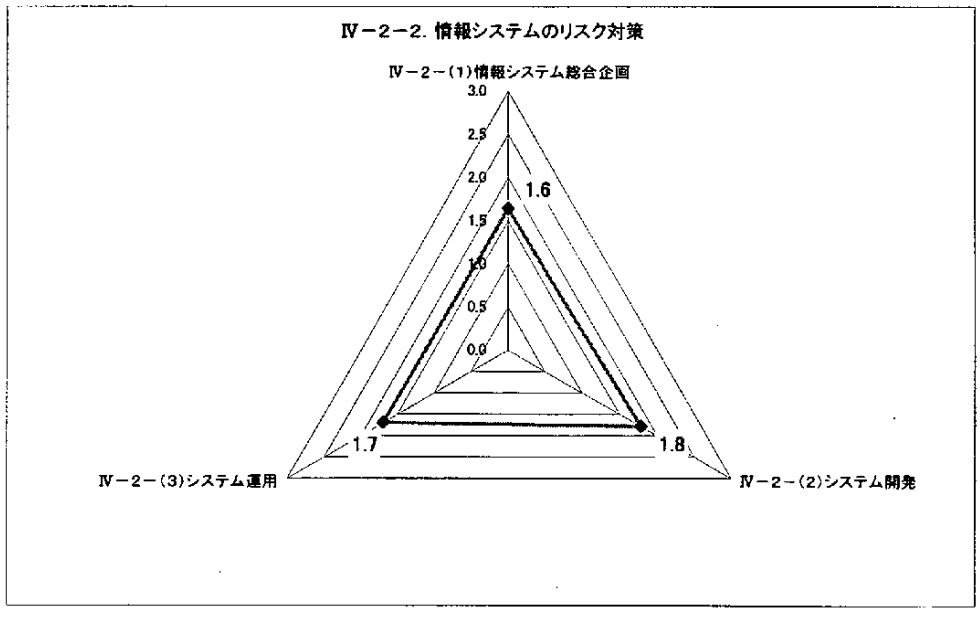


図２－４－６．３階層目のレーダーチャート例［Ⅳ－２－２］

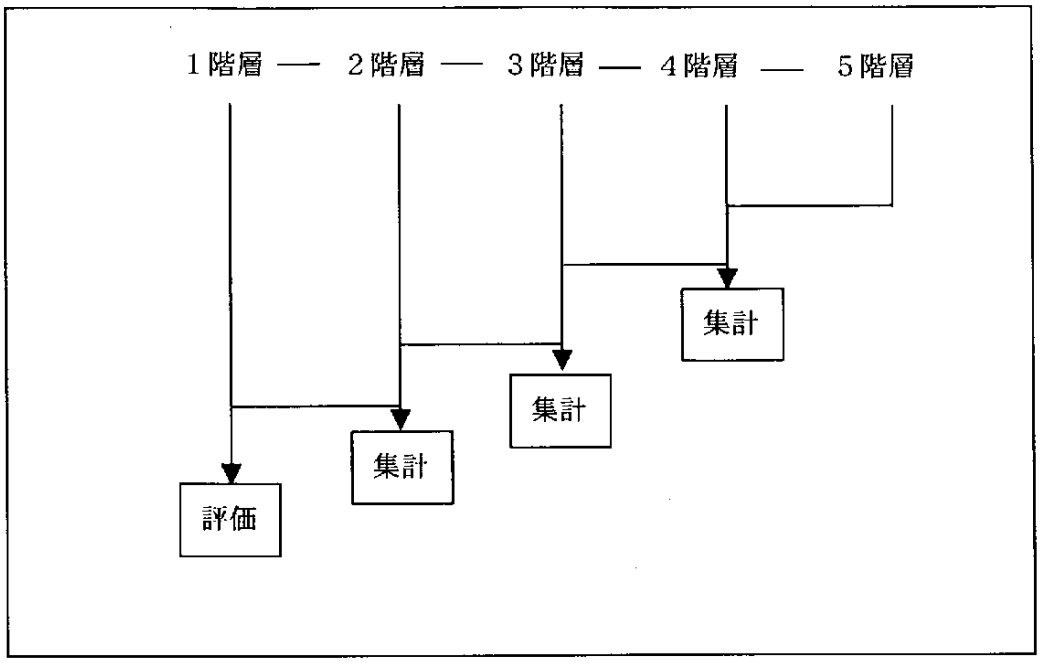


図２－４－７．集計の流れ

補足

ここまでの分析例では［Ⅰ．経営とリスクの関係］を用いてＹｅｓ／Ｎｏの回答と４レベルの回答を組み合わせた回答例を便宜的に作成し解説している。委員会の意図としては、「Ⅰ－１．経営者とリスクマネジメント」評価項目は「図２－４－７．回答シート例２」にあるようにすべてがＹｅｓ／Ｎｏで回答することを意図している。

キーワード	キーワード	識別コード	質問項目	回答欄					集計	全体評価
				A	B	C	D	E		
経営とリスク	経営とリスク	Ⅰ．経営とリスクの関係								
経営環境とリスクマネジメント	経営環境とリスクマネジメント	Ⅰ－1．経営環境とリスクマネジメント								
1．経営者の関心	経営者の関心	1-1-1-1	Q 経営者はコンピュータ関連のリスクについて関心は高いですか？	Y	Y	Y	N	N	1.8	1.8
2．経営レベルによるリスクの範囲	経営レベルによるリスクの範囲	1-1-1-2	Q 経営レベルのリスクにリスクマネジメントの範囲を広げて考えていますか？	Y	Y	Y	Y	N	2.4	2.4
3．リスクマネジメントポリシー	リスクマネジメントポリシー	1-1-1-3	Q リスクマネジメントに関する全社的なポリシー(方針)を有していますか？	Y	Y	Y	N	N	1.8	2.1
		1-1-1-3-1	Q リスクマネジメントポリシーは、最高経営者のもと全社的に構成されていますか？	Y	Y	Y	Y	Y		
		1-1-1-3-2	Q 貴社では経営理念に基づくリスクマネジメントポリシーを定めていますか？	Y	Y	Y	Y	Y		
		1-1-1-3-3	Q リスクマネジメントポリシーでは、経営を脅かす事態に対する明確な対策を有していますか？	Y	Y	N	Y	N		
		1-1-1-3-4	Q 緊急事態発生時の役員、スタッフ、担当者の役割はリスクマネジメントポリシーに定められていますか？	Y	Y	Y	Y	Y		
		1-1-1-3-5	Q リスクマネジメントポリシーではコンプライアンスを重視していますか？	N	Y	Y	Y	N		
		1-1-1-3-6	Q リスクマネジメントポリシーで内部監査の実施を明記していますか？	Y	Y	Y	Y	Y		
		1-1-1-3-7	Q リスクマネジメントポリシーで外部監査の実施を明記していますか？	N	Y	N	N	N		
		1-1-1-4	Q リスクマネジメントポリシーに基づき、実施基準が機能部門別に構成されていますか？	Y	Y	N	Y	Y	2.4	
		1-1-1-4-1	Q 有効に機能するようフィードバックループ構成になっていますか？	Y	Y	Y	Y	Y		
		1-1-1-4-2	Q 経営にとってのマイナス情報を吸い上げる機能を明確にしていますか？	Y	N	N	N	Y		
		1-1-1-4-3	Q スタッフに対し業務の機能分野ごとに教育訓練を行うことが計画化されていますか？	Y	Y	Y	Y	Y		
		1-1-1-4-4	Q リスクマネジメントシステム構築の指針(JIS)を知っていますか？	Y	N	N	Y	Y		
4．組織	組織	1-1-1-5	Q 組織として守るべき対象を明確にしていますか？	N	N	Y	Y	Y	1.8	1.8
5．役割・責任	役割・責任	1-1-1-6	Q 守るべき対象との関連において、リスクマネジメントに関する役割・責任・権限が文書化されていますか？	Y	N	Y	N	N	1.2	1.2
6．課題の明確化	課題の明確化	1-1-1-7	Q 組織におけるリスクマネジメントの具体的なリスク対応上の課題を明確に定めていますか？	N	Y	N	Y	Y	1.8	1.8
		1-1-1-7-1	Q 行動指針は、経営資源の保全を含んでいますか？	Y	Y	N	Y	Y		
		1-1-1-7-2	Q リスクに対する社会的責任をも含んでいますか？	N	N	N	N	Y		
		1-1-1-7-3	Q 行動指針では基本的な目的を明確に設定していますか？	N	N	Y	Y	N		
		1-1-1-7-4	Q 機能部門におけるリスク対応は明確にされていますか？	Y	Y	Y	Y	Y		
7．行動指針	行動指針	1-1-1-8	Q リスクマネジメントの行動指針は明確にされていますか？	N	Y	Y	N	N	1.2	1.2
		1-1-1-8-1	Q リスクマネジメントの評価を明確に行うシステムとなっていますか？	N	Y	Y	Y	Y		
		1-1-1-8-2	Q リスクマネジメントのテストを行うように定められていますか？	Y	Y	Y	Y	N		
		1-1-1-8-3	Q リスクマネジメントの監査を行うように定められていますか？	N	Y	Y	N	N		
		1-1-1-8-4	Q 環境変化に応じリスクマネジメントの行動計画の修正を含んでいますか？	Y	Y	Y	Y	Y		
8．成果	成果	1-1-1-9	Q リスクマネジメントシステムの達成の成果を明示していますか？	Y	Y	Y	Y	N	2.4	2.4

Y= 3
N= 0

レベル3：組織内で標準を、継続的に見直す仕組みができている。
レベル2：組織内で標準があり、それに従って実施されている。
レベル1：組織内で実施されているが、標準が定められていない。
レベル0：組織内で全く意識されておらず、何もしていない。

図２－４－８．回答シート例２

（5）加重平均での集計方法

加重平均を行う場合は各々の評価項目について全体を100%として項目ごとにパーセントを割り振るのが一般的にわかりやすい。その例を「表２－４－３．集計シート　ウエイトづけ回答例」に示す。この場合は【Ⅱ．ＪＲＭＳにおけるリスクマネジメント計画】の例であるが、[Ⅱ－１．ＪＲＭＳの計画]は８つのキーワードから構成されている。この例では《１．経営理念と計画》、《２．管理体制の組織化》を10%、《３．適用業務責任権限》には５%、《４．適用業務とリスクマネジメント》に20%などと割り振る。

【Ⅱ】全体を評価する場合は、[Ⅱ－１．ＪＲＭＳの計画]に40%、[Ⅱ－２．ＪＲＭＳの実行組織]に20%、[Ⅱ－３．ＪＲＭＳの維持]に40%とウエイトをつけて、それぞれの評価にこのウエイトをかけて評価する。この場合は<1.8×40%＋1.6×20%＋1.9×40%＝1.8>となる。

このようにしてレーダーチャートが各キーワードごとに完成する。

表２－４－３．集計シート　ウエイトづけ回答例

(集計シート)	1階層評価	2階層評価	ウエイト	3階層集計	ウエイト	4階層集計	ウエイト	5階層集計
Ⅱ. JRMSにおけるリスクマネジメント計画	1.8							
Ⅱ－1. JRMSの計画		1.8	40%					
1. 経営理念と計画				2.2	10%			
2. 管理体制の組織化				1.2	10%			
3. 適用業務責任・権限				2.4	5%			
4. 適用業務とリスクマネジメント				1.2	20%			
5. 管理目標				1.8	5%			
6. 目標脅威				2.3	20%			
7. 分析および対策				2.4	10%			
8. 緊急時対応				2.0	10%			
Ⅱ－2. JRMSの実行組織		1.6	20%					
1. 全社的リスクマネジメント組織				1.8	50%			
2. 情報システムリスクマネジメント組織				1.2	30%			
3. ユーザの組織				1.7	20%			
Ⅱ－3. JRMSの維持		1.9	40%					
1. 是正改善				1.2	10%			
2. 監査				1.8	10%			
3. 監視				2.3	10%			
4. 文書化				2.4	10%			
5. リスクコミュニケーション				2.0	10%			
6. 教育の承認				2.4	10%			
7. 教育内容				2.2	20%			
8. レビュー				1.2	20%			

4.6　レーダーチャートの読み方

一部の企業ではすでに情報システムのリスクは経営のリスクになっており、このような企業の割合は今後さらに上昇して行く。したがって、経営者は情報システムのリスクについて、自らの責任として立ち向かう必要がある。経営者が自社の情報システムに関するリスクを評価するには、

作成された全体のレーダーチャートから概要を把握し、次に評価が低い項目についてドリルダウンを行う。つまり、１階層目のレーダーチャートで評価が低い項目について、２階層目のレーダーチャートを見て、評価が低い項目が何かを識別し、それについての詳しい説明を情報システム部門に行わせる。情報システム部門は、必要ならばさらにドリルダウンを行い、最終的には５階層目のどの質問項目が評価を下げているのかを経営者にわかる言葉で説明すべきである。

では、レーダーチャートで自社の評価はどのくらいのレベルに達していればよいのか。もちろんすべての項目について最高のレベルを取る必要はない。各企業で必要となるセキュリティのレベルは、その企業の特性により大きく依存している。特に、インターネットを使ったE-Businessにその会社が積極的に取り組み、業務が情報システムに依存する割合が高まるにつれ、必要なセキュリティのレベルも上昇していく。たとえば、インターネットでの証券取引を行っている会社で必要とされるリスク対策のレベルと、Ｗｅｂで自社の製品カタログを提供しているのみの製造会社では必要な対策のレベルは大きく異なる。しかし、これを的確に判断するためには、自社のユーザー業務に基づいたリスク分析を実施して、必要なレベルを判断すべきである。（「2.4 情報システムリスクの評価」参照）

このように、各企業が必要とするセキュリティのレベルは異なるので、他社のセキュリティレベルがどこにあるかは参考にはなるが、それだけで自社に必要なレベルを決めることはできない。そこで必要となるのは、自社のレベルがどのように改善されたかを継続的に見ていくことである。たとえば、レーダーチャート上に毎年の評価を継続的に入れていくことで、自社の弱点がどの程度の速さで改善されているかをわかりやすく見ることができる。特に、弱点とされた項目については、下位のレーダーチャートでもこれを行うことが必要である。

今後ＪＲＭＳが普及していくとともに、各企業でＪＲＭＳ質問票を使った実績が蓄積されてくれば、現在、JIPDEC で行っている、「情報セキュリティに関する調査」のようなアンケート調査（「情報システム・リスクマネジメントシステム調査」（仮称））を実施し、日本企業の情報システムリスクに対する意識向上を図ることも可能となる。また、リスク対策のベストプラクティスは、ユーザ企業間の情報交換を活発にする仕組みが必要とされる分野であり、米国での CERT Coordination Center や Forum of Incident Response and Security Teams の動向は大変参考になる。

4.7 COBIT成熟度モデルとリスクマネジメント

COBIT－Ⅲでは、情報システムの業務を 34 のプロセスに分け、各プロセスについてその成熟度を定義している。情報システムに関するリスク評価を行う場合、特定のペリルについて、関連するプロセスの成熟度により、リスクが発生する確率は大きく異なってくる。したがって、情報システムに関するリスク評価を実施する際には、関連するプロセスの成熟度の評価を行い、成熟度が低い場合には、ハザードとして、損害が発生しやすい状況があるとすべきである。

COBIT－Ⅲのフレームワークでは、34 のＩＴプロセスを定義し、各プロセスでの成熟度を定義している。成熟度はレベル０からレベル５までの６段階があり、それぞれのレベルは次の基準で判定される。

レベル０	未認識	組織として、当該プロセスの標準が必要なことすら認識されておらず、標準のプロセスも全くない。
レベル１	初　期	組織として、当該プロセスの標準が必要なことは認識されているが、標準は確立されておらず、個人や場合によりその場限りの対応が行われている。プロセス全体についての組織的な対応はない。
レベル２	反復可能	ある作業を行う人たちが、同じ手続きを使うようになっている。しかし、標準手続きが公式的に教育・周知されてはおらず、個人任せになっている。各個人の知識に頼るところが多く、エラーも発生する。
レベル３	定　義	手続きの標準化、文書化、教育・周知が行われている。しかし、標準のプロセスに従うかは、個人任せなので逸脱が見られる。各手続きは、あまり洗練されてはおらず、既存のやり方を公式化したものである。
レベル４	管　理	標準の手続きに従っているかをモニターし測定することが可能で、標準プロセスが有効でないときには是正措置を取ることができる。プロセスには絶えず改良が加えられ、グッド・プラクティスが提供される。自動化ツールが部分的に利用されている。
レベル５	最適化	継続的な改良と他組織の成熟度モデルを使って、プロセスはベスト・プラクティスのレベルまで改良されている。ＩＴは自動化されたワークフローに組み込まれ、品質や効率の改良のツールや企業の対応速度向上に役立っている。

情報システムの各プロセスに内在するリスクは、各プロセスの成熟度が高ければ顕在化するおそれが低いが、成熟度が低いとプロジェクト開発の失敗や重大なシステム障害の形で顕在化する。

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

ＪＲＭＳについてもCOBITのように、成熟度モデルを導入し、各プロセスのリスク対応の度合いに応じて低い部分に焦点をあて、是正・改善を求めるべく質問項目の回答結果をリスク対応に反映させることが望ましい。

5．ＪＲＭＳ維持のための仕組み

5.1　ＪＲＭＳにおける留意事項

ＪＲＭＳの実際的な利用にあたっては、前述のJIS Q 2001におけるリスクマネジメントシステム維持の考え方が不可欠である。とりわけ、対象が情報リスクであるためその特徴を十分理解しなければならない。それゆえ、ＪＲＭＳに関わる要員の能力維持、状況変化の確認のためのシミュレーションなどが重要になる。

しかし、脆弱性を分析するとしても、情報システム環境の変化の早さからすべての項目を質問票に列挙することは不可能である。それゆえ、組織内外との接点をもち、リスク情報の入手・交換等のためのリスクコミュニケーションを密にするほか、リスクマネジメント関連の文書管理を行い、リスクマネジメントシステム監査等を含め、常に質問項目の見直しに腐心することが肝要である。

以上のような点からＪＲＭＳを組織内で展開するためには、実行組織が必要となる。

5.2　実行組織

ＪＲＭＳにおいてはリスクマネジメントシステムを実行させるための体制を想定している。体制それ自体は組織が行う業務内容によって差異があるが、一般的に情報リスク対応としては以下のような実行組織を持つことが望ましい。その根拠は、従来のように単独の組織、たとえば情報セキュリティ部門だけに委ねられるシステム環境ではないことにある。特に経営者層の役割が重要であることは言うまでもない。

表２－５－１．ＪＲＭＳの実行組織

組織名	実行担当
全社的リスクマネジメント組織	リスクマネジメント担当役員 　リスクマネジメント推進組織 　リスク担当者の役割権限
情報システムリスクマネジメント組織	情報システムリスクマネジメント担当者 情報セキュリティ管理者 　情報システムリスク対策組織 　情報セキュリティ対策推進組織 情報システム運用管理責任者 　リスクマネジメント担当者の役割権限
ユーザ組織	適用業務別オーナー ユーザ部門リスク担当責任者

そうした意味を含め、JIS Q 2001 を参考にしてＪＲＭＳ維持のための仕組みについて簡潔に論じておく。

5.3 維持のための仕組み

ＪＲＭＳをシステム環境の中で動かすためには、以下のような維持のための仕組みが必要である。

5.3.1 能力および教育・訓練

ＪＲＭＳにおけるリスクマネジメントシステムをＰＤＣＡプロセスに従って動かすにはシステムを運用する要員が必要である。情報環境の変化の著しさからリスクマネジメントを実施する要員には、役割に応じ常に新しい情報システム環境への適応力を有していることが求められる。そのため組織としては、要員の能力確保とともに、常に要員のため適切な教育・訓練を行うことが必要である。

5.3.2 リスクコミュニケーション

組織においてリスクコミュニケーションが重要なのはリスク情報の誤解なり理解不足が致命的となるおそれがあるからである。リスクに関する情報が組織内において一方通行では効果的なリスク対応ができない。これまでも幾度となく指摘されたように、組織内と組織外との間に存在するリスク関連情報の格差が問題であり、適切な情報の開示の仕方はリスクマネジメントにおいて重要である。情報リスクへの対応に関して組織としていかに対処しているかを明らかにするために広報活動を計画することも必要である。

5.3.3 リスクマネジメントシステム文書の作成と文書管理

文書の作成が必要なのは組織としていかに情報リスクに対応しているかを関係者に紙面または電子形式で周知徹底させることにある。その場合、リスクマネジメントシステムの構成および機能、さらに重要な文書類がどこで入手・利用可能かを把握できるように作成しておくことが大切である。

また、情報リスク対応に関して作成された文書を適切に管理する手順を確立・維持しておくことが重要である。これにより、情報リスク対応のデータが蓄積され、組織の共有財産となる。

5.3.4 発見したリスクの監視

このことが意味をもつのは、組織に作用するリスクを生み出す情報環境の変化である。そうした変化を生み出す要因を明らかにし、関連するリスク情報を入手することは非常に大切である。

5.3.5 リスクマネジメント関係記録の維持・管理

情報リスク対応の記録を維持・管理するのは全体のリスクマネジメントに関連する様々な活動を追跡可能にするためには非常に重要である。

5.3.6 リスクマネジメントシステム監査

リスクマネジメントにおいて監査の視点は不可欠である。リスクマネジメントシステム監査が必要なのは、組織が適切に構築・実施・維持されているかどうかを「客観的な視点」から判断し、リスクマネジメントの実効性を高めることにある。この点は、情報システムのリスクに関わるＪＲＭＳにおいても重要である。

5.3.7　最高経営者のコミットメント

ＪＲＭＳの維持において重要なのは最高経営者のコミットメントである。とりわけリスクを処理する仕組みとしてのリスクマネジメントシステムにとり、組織の最高経営者（ＣＥＯ）もしくは同ＣＥＯにより任命されたリスクマネジメントシステム担当役員（ＣＲＯ相当）、また情報担当役員（ＣＩＯ：Chief Information Officer）によるレビューが意味をもつ。そうした経営責任を担う担当役員によりリスクマネジメントシステムを維持し、適切性および有効性を改善するためにすべての活動にわたり全体との関連性を見ながら包括的にレビューするのである。これにより、情報関連のリスクについて組織全体に緊張感がみなぎり、リスクを適切に処理するという視点が徹底されることになる。とりわけ、組織の最高経営者がこうした認識を有していることがリスクマネジメントの成否を握るといって過言ではない。

リスクマネジメントシステムの利用は、組織がさらされている情報リスク環境によるが、こうしたシステム維持の構造を前提に取り組むことが必要であるといえる。その意味で、ＪＲＭＳにおいて組織の実体維持が考慮されることになる。

6．今後の課題　むすびにかえて

ＪＲＭＳ質問票の意義は、現在の情報システム環境を前提に組織のリスク対応の実態を分析するツールとしてまとめたことにある。ＪＲＡＭでは、情報セキュリティの視点からリスク分析のための方法を提示したのであったが、組織における情報システム関係のリスクは情報セキュリティの領域だけを考慮すればよいとはいいがたい。情報システムが関係するすべての対象を総合的に分析する必要があるからである。

そのため、ＪＲＭＳではかなり多くの質問項目を用意している。特に、組織の脆弱性を視覚的に把握するためレーダーチャートを用いる方法を採用している。ＪＲＭＳの質問項目に対する回答を集計し、その結果に基づき、全体評価を行い、レーダーチャートを描き、リスク対応における問題状況、すなわち脆弱性を明らかにし、対応への視点を与える仕組みとなっている。質問票それ自体も必ずしも万全とはいえないかもしれないが、質問項目の理解によっては関係者に少なからずリスク対応上の示唆を与えるものと確信している。

しかしながら、質問項目の見直しならびに質問構成における階層構造、最高経営者のレビューに役立たせるための評価への持っていき方等の点でまだ熟慮すべき点がある。ＪＲＭＳ委員会としては、そうした課題を見据えながら、より完成度の高いツールとしてＪＲＭＳを創り上げていきたいと考えている。

第III部

回答シート例

1．回答シート例

ＪＲＭＳ質問票に関わる回答シートを参考として示しておく。

I.1　ＪＲＭＳ質問票

ＪＲＭＳ質問票における回答者が回答すべきと思われる質問項目については白抜きにし、回答しなくてもよいと思われる項目については黒で消しておいた。しかし、組織の実態に応じて回答すべき項目については考慮されたい。

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
経営とリスク	経営とリスク	1．経営とリスクの関係				
経営環境とリスクマネジメント	経営環境とリスクマネジメント	I－1．経営環境とリスクマネジメント				
1．経営者の関心	経営者の関心	1-1- 1- 1	Q 経営者は情報システムに関するリスクについて認識していますか？			
2．経営レベルによるリスクの範囲	経営レベルによるリスクの範囲	1-1- 1- 2	Q 経営レベルのリスクにリスクマネジメントの範囲を広げて対応していますか？			
3．リスクマネジメントポリシー	リスクマネジメントポリシー	1-1- 1- 3	Q リスクマネジメントに関する全社的なポリシー（方針）を有していますか？			
		1-1- 1- 3- 1	Q リスクマネジメントポリシーは、最高経営者のもと全社的に構成されていますか？			
		1-1- 1- 3- 2	Q 貴社では経営理念に基づくリスクマネジメントポリシーを定めていますか？			
		1-1- 1- 3- 3	Q リスクマネジメントポリシーでは、経営を脅かす事態に対する明確な対策を有していますか？			
		1-1- 1- 3- 4	Q 緊急事態発生時の役員、スタッフ、担当者の役割はリスクマネジメントポリシーに定められていますか？			
		1-1- 1- 3- 5	Q リスクマネジメントポリシーではコンプライアンスを重視していますか？			
		1-1- 1- 3- 6	Q リスクマネジメントポリシーで内部監査の実施を明記していますか？			
		1-1- 1- 3- 7	Q リスクマネジメントポリシーで外部監査の実施を明記していますか？			
		1-1- 1- 4	Q リスクマネジメントポリシーに基づき、実施基準が機能部門別に構成されていますか？			
		1-1- 1- 4- 1	Q 有効に機能するようフィードバックループ構成になっていますか？			
		1-1- 1- 4- 2	Q 経営にとってのマイナス情報を吸い上げる機能を明確にしていますか？			
		1-1- 1- 4- 3	Q スタッフに対し業務の機能分野ごとに教育訓練を行うことが計画化されていますか？			
		1-1- 1- 4- 4	Q 「JIS Q 2001 リスクマネジメントシステム構築のための指針」を知っていますか？			
4．組織	組織	1-1- 1- 5	Q 組織として守るべき対象を明確にしていますか？			
5．役割・責任	役割・責任	1-1- 1- 6	Q 守るべき対象との関連において、リスクマネジメントに関する役割・責任・権限が文書化されていますか？			
6．課題の明確化	課題の明確化	1-1- 1- 7	Q 組織におけるリスクマネジメントの具体的なリスク対応上の課題を明確に定めていますか？			
		1-1- 1- 7- 1	Q 行動指針は、経営資源の保全を含んでいますか？			
		1-1- 1- 7- 2	Q リスクに対する社会的責任をも含んでいますか？			
		1-1- 1- 7- 3	Q 行動指針では基本的な目的を明確に設定していますか？			
		1-1- 1- 7- 4	Q 機能部門におけるリスク対応は明確にされていますか？			
7．行動指針	行動指針	1-1- 1- 8	Q リスクマネジメントの行動指針は明確にされていますか？			
		1-1- 1- 8- 1	Q リスクマネジメントの評価を明確に行うシステムとなっていますか？			
		1-1- 1- 8- 2	Q リスクマネジメントのテストを行うように定められていますか？			
		1-1- 1- 8- 3	Q リスクマネジメントの監査を行うように定められていますか？			
		1-1- 1- 8- 4	Q 環境変化に応じリスクマネジメントの行動計画の修正を含んでいますか？			
8．成果	成果	1-1- 1- 9	Q リスクマネジメントシステムの達成の成果を明示していますか？			

I.2　回答シート例

回答シートにおける右欄に「A，B，C，D，E」という記号があるが、５人の回答者を想定して示している。ここでは例として【I】のみを示したが、実際の作業においては、各項目別にこのようなシートを作成することになる。

キーワード	キーワード	識別コード	質問項目	回答欄					集計	全体評価
				A	B	C	D	E		
経営とリスク	経営とリスク	1．経営とリスクの関係								
経営環境とリスクマネジメント	経営環境とリスクマネジメント	I－1．経営環境とリスクマネジメント								
1．経営者の関心	経営者の関心	1-1- 1- 1	Q 経営者はコンピュータ関連のリスクについて関心は高いですか？							
2．経営レベルによるリスクの範囲	経営レベルによるリスクの範囲	1-1- 1- 2	Q 経営レベルのリスクにリスクマネジメントの範囲を広げて考えていますか？							
3．リスクマネジメントポリシー	リスクマネジメントポリシー	1-1- 1- 3	Q リスクマネジメントに関する全社的なポリシー（方針）を有していますか？							
		1-1- 1- 3- 1	Q リスクマネジメントポリシーは、最高経営者のもと全社的に構成されていますか？							
		1-1- 1- 3- 2	Q 貴社では経営理念に基づくリスクマネジメントポリシーを定めていますか？							
		1-1- 1- 3- 3	Q リスクマネジメントポリシーでは、経営を脅かす事態に対する明確な対策を有していますか？							
		1-1- 1- 3- 4	Q 緊急事態発生時の役員、スタッフ、担当者の役割はリスクマネジメントポリシーに定められていますか？							
		1-1- 1- 3- 5	Q リスクマネジメントポリシーではコンプライアンスを重視していますか？							
		1-1- 1- 3- 6	Q リスクマネジメントポリシーで内部監査の実施を明記していますか？							
		1-1- 1- 3- 7	Q リスクマネジメントポリシーで外部監査の実施を明記していますか？							
		1-1- 1- 4	Q リスクマネジメントポリシーに基づき、実施基準が機能部門別に構成されていますか？							
		1-1- 1- 4- 1	Q 有効に機能するようフィードバックループ構成になっていますか？							
		1-1- 1- 4- 2	Q 経営にとってのマイナス情報を吸い上げる機能を明確にしていますか？							
		1-1- 1- 4- 3	Q スタッフに対し業務の機能分野ごとに教育訓練を行うことが計画化されていますか？							
		1-1- 1- 4- 4	Q リスクマネジメントシステム構築の指針（JIS）を知っていますか？							
4．組織	組織	1-1- 1- 5	Q 組織として守るべき対象を明確にしていますか？							
5．役割・責任	役割・責任	1-1- 1- 6	Q 守るべき対象との関連において、リスクマネジメントに関する役割・責任・権限が文書化されていますか？							
6．課題の明確化	課題の明確化	1-1- 1- 7	Q 組織におけるリスクマネジメントの具体的なリスク対応上の課題を明確に定めていますか？							
		1-1- 1- 7- 1	Q 行動指針は、経営資源の保全を含んでいますか？							
		1-1- 1- 7- 2	Q リスクに対する社会的責任をも含んでいますか？							
		1-1- 1- 7- 3	Q 行動指針では基本的な目的を明確に設定していますか？							
		1-1- 1- 7- 4	Q 機能部門におけるリスク対応は明確にされていますか？							
7．行動指針	行動指針	1-1- 1- 8	Q リスクマネジメントの行動指針は明確にされていますか？							
		1-1- 1- 8- 1	Q リスクマネジメントの評価を明確に行うシステムとなっていますか？							
		1-1- 1- 8- 2	Q リスクマネジメントのテストを行うように定められていますか？							
		1-1- 1- 8- 3	Q リスクマネジメントの監査を行うように定められていますか？							
		1-1- 1- 8- 4	Q 環境変化に応じリスクマネジメントの行動計画の修正を含んでいますか？							
8．成果	成果	1-1- 1- 9	Q リスクマネジメントシステムの達成の成果を明示していますか？							

Y= 3
N= 0

レベル3：組織内で標準を、継続的に見直す仕組みができている。
レベル2：組織内で標準があり、それに従って実施されている。
レベル1：組織内で実施されているが、標準が定められていない。
レベル0：組織内で全く認識されておらず、何もしていない。

2．ＪＲＭＳ集計シート例

ＪＲＭＳ質問票には入っていないが、回答シート例の右欄に「集計」・「全体評価」欄を設けている。これを用いてレーダーチャートを作成するため、キーワードに基づき、１階層から５階層まで記入できる集計シートを作業用に用意しておいた。集計・評価に際し利用されたい。

なお、質問項目によっては４層目を重視する（例：[Ⅲ－３－（１）情報システムのリスク分析]）ものもある。しかしながら、基本的には４層目のキーワードについて５層目を回答してから集計することになることを留意されたい。

(集計シート)	1階層評価	2階層評価	ウエイト	3階層集計	ウエイト	4階層集計	ウエイト	5階層集計
Ⅰ．経営とリスクの関係								
Ⅰ－1．経営環境とリスクマネジメント								
1．経営者の関心								
2．経営レベルによるリスクの範囲								
3．リスクマネジメントポリシー								
4．組織								
5．役割・責任								
6．課題の明確化								
7．行動指針								
8．成果								

(集計シート)	1階層評価	2階層評価	ウエイト	3階層集計	ウエイト	4階層集計	ウエイト	5階層集計
Ⅱ．JRMSにおけるリスクマネジメント計画								
Ⅱ－1．JRMSの計画								
1．経営理念と計画								
2．管理体制の組織化								
3．適用業務責任・権限								
4．適用業務とリスクマネジメント								
5．管理目標								
6．目標脅威								
7．分析および対策								
8．緊急時対応								
Ⅱ－2．JRMSの実行組織								
1．全社的リスクマネジメント組織								
2．情報システムリスクマネジメント組織								
3．ユーザの組織								
Ⅱ－3．JRMSの維持								
1．是正改善								
2．監査								
3．監視								
4．文書化								
5．リスクコミュニケーション								
6．教育の承認								
7．教育内容								
8．レビュー								

(集計シート)	1階層評価	2階層評価	ウエイト	3階層集計	ウエイト	4階層集計	ウエイト	5階層集計
Ⅲ. JRMSのリスク分析								
3－1. JRMSのリスク分析								
1. リスク分析の仕組み								
2. リスク分析の体制								
3. リスク分析基準								
4. リスク分析(自然災害)								
5. リスク分析(情報)								
6. リスク分析(物理)								
7. リスク分析(経営)								
8. 特筆すべきリスクの認知								
Ⅲ－2. 情報セキュリティポリシーのリスク分析								
1. 情報セキュリティの経営からの視点								
2. 情報セキュリティポリシーの対象								
3. 特筆する情報リスク								
4. 時間分析								
5. 情報リスク洗い出し実施基準								
Ⅲ－3. 情報システムのリスク分析								
Ⅲ－3－(1)情報システムのリスク分析								
1. IT戦略のリスク分析								
2. 業務影響								
3. 利益阻害								
4. 情報資産リスク								
5. 情報リスクと自組織の倒産								
6. 情報リスクと経営存続								
7. システム不全								
Ⅲ－3－(2)情報システム総合企画								
1. システム企画のリスク分析								
2. データ所有者								
3. IT資産管理目録								
4. ライセンス管理								
5. 構成管理								
Ⅲ－3－(3)システム開発								
1. プロジェクトリスク								
2. ライフサイクル								
3. 開発管理								
4. 変更管理								
5. 運用テスト								
Ⅲ－3－(4)システム運用								
1. システム運用								
2. 運用管理								

(集計シート)	1階層評価	2階層評価	ウエイト	3階層集計	ウエイト	4階層集計	ウエイト	5階層集計
Ⅲ－3－(5)不正アクセス・コンピュータウイルス関連								
1. 不正アクセスのリスク								
2. コンピュータ犯罪のリスク								
3. ウイルスのリスク								
4. E-Commerce のリスク								
5. 電子メールのリスク								
Ⅲ－3－(6)災害								
1. 自然災害その他の災害と影響								
2. 包括的リスクの可能性								
3. 物的資産喪失の可能性								
4. 人的リスクの可能性								
5. ネットワーク障害リスクの可能性								
6. 委託先リスクの可能性								
Ⅲ－3－(7)障害								
1. ハードウェア障害								
2. ソフトウェア障害								
3. 運用ミス障害								
Ⅲ－3－(8)アウトソーシング								
1. アウトソーサの決定								
2. 役割分担								
3. 守秘義務								
4. 実施								
5. 変更管理								

(集計シート)	1階層評価	2階層評価	ウエイト	3階層集計	ウエイト	4階層集計	ウエイト	5階層集計
Ⅳ. JRMSにおけるリスク対策								
Ⅳ－1. リスク対策における情報セキュリティ								
1. 情報セキュリティポリシー								
2. 情報セキュリティポリシーに基づく実施基準								
3. 情報資産インベントリとサービススタッフ								
4. 情報セキュリティ個別対策								
5. ID、パスワード、アクセス権付与								
6. 自社ホームページ承認								
7. 緊急対策								

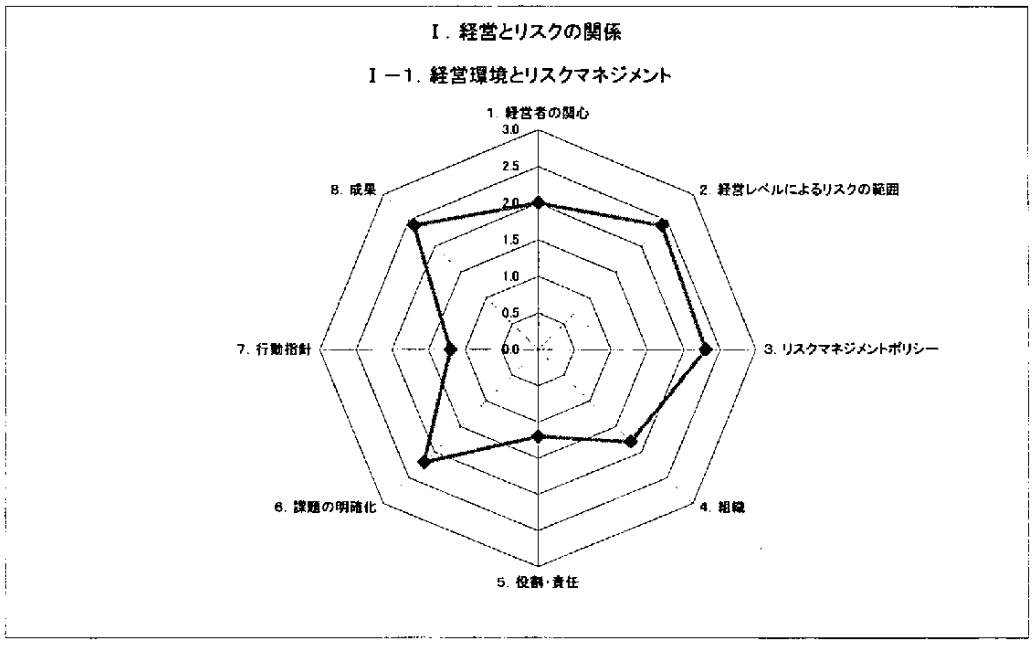
(集計シート)	1階層評価	2階層評価	ウエイト	3階層集計	ウエイト	4階層集計	ウエイト	5階層集計
Ⅳ－2. 情報システムのリスク対策								
Ⅳ－2－(1)情報システム総合企画								
1. 情報システムポリシー								
2. IT計画								
3. 組織体制・機能								
4. スタッフ								
5. 経理								
6. 管理(文書化を含む)								
7. モニタリング								
Ⅳ－2－(2)システム開発								
1. 一般								
2. プロジェクト管理								
3. システム要件定義								
4. プログラム開発								
5. テストデータ								
6. 運用テスト								
7. 変更管理								
Ⅳ－2－(3)システム運用								
1. システム運用								
2. モニタリング機能								
3. 管理機能								
Ⅳ－3. 不正アクセス								
1. アクセス権管理								
2. 論理的アクセス対策								
3. 物理的アクセス対策								
4. 個人認証								
5. ネットワーク中のデータ保護								
6. 不正検出								
7. 緊急時対応								
Ⅳ－4. コンピュータウイルス関連								
Ⅳ－4－(1)コンピュータ犯罪								
1. パスワード								
2. データ保護対策								
3. 盗聴対策								
Ⅳ－4－(2)コンピュータウイルス								
1. ウイルス手続き								
2. ウイルス検出・駆除								
3. 教育・訓練								
4. ウイルス感染対策								
5. 事後対策								

(集計シート)	1階層評価	2階層評価	ウエイト	3階層集計	ウエイト	4階層集計	ウエイト	5階層集計
Ⅳ－4－(3) E-Commerce								
1. プライバシー保護								
2. 不良客情報管理								
3. データ保護対策								
4. ネットワーク機器対応								
5. インターネット接続管理								
6. 電子的証拠								
Ⅳ－4－(4) 電子メール								
1. 管理								
2. メールサーバ管理								
3. ネットワーク機器管理								
4. インターネット接続機器管理								
5. デジタル署名								
6. 悪質メール対策								
7. 転送エラー対策								
Ⅳ－5. 災害対策								
1. 管理								
2. 防火対策								
3. 耐震対策								
4. 水害対策								
Ⅳ－6. 障害対策								
1. 管理								
2. 手続き								
3. 情報システム								
4. ユーティリティ								
Ⅳ－7. アウトソーシング関連リスク対策								
1. 目的								
2. 役割分担								
3. プロジェクト管理								
4. アウトソーサ管理								
5. 契約								
6. 知的財産権								
7. セキュリティ上の留意点								
Ⅳ－8. その他関連項目								
1. テロおよび人命損失								
2. サービス提供								
3. ユーザ間トラブル								
4. 苦情処理対応								
5. リスク対策手順整備								
6. 危機管理計画徹底								
7. 危機管理計画時間軸								
8. 移動体データ保護								

(集計シート)	1階層評価	2階層評価	ウエイト	3階層集計	ウエイト	4階層集計	ウエイト	5階層集計
Ⅳ－9. バックアップ								
1. 二重化対策								
2. ファイルのバックアップ								
3. DBファイルバックアップ								
4. ネットワーク対策								
5. 予備サイト								
Ⅳ－10. 緊急時対策								
1. 事前対応								
2. 緊急時対応手続き								
3. 復旧計画								
Ⅳ－11. リスクファイナンス								
1. リスクファイナンスの役割								
2. リスクファイナンスの対象領域								
3. ファイナンスのリスク区分								
4. 財務的対応								
5. 外部コンサルタント活用								
6. リスク対応のための組み合わせ								

3．レーダーチャート例

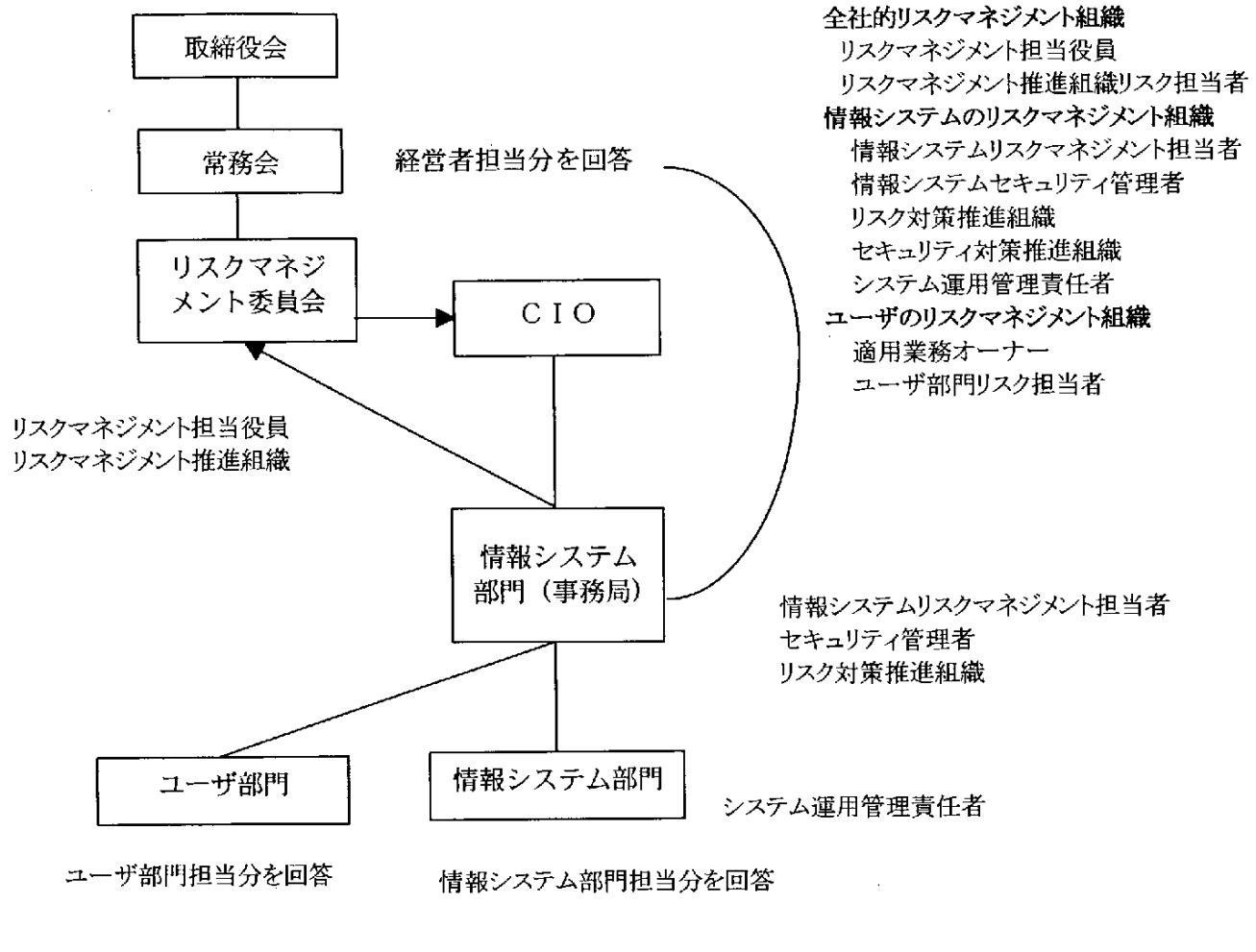
第Ⅱ部の「4.5　レーダーチャートの作り方」に従い、参考として［Ⅰ－1．経営環境とリスクマネジメント］の全体評価のレーダーチャートを例示しておく。重要なことは、リスクへの対応を組織がいかに実行し、リスク対策に生かしているのか、リスク対策は万全か、といった側面をレーダーチャートでの結果をいかに読むかにある。この点は、第Ⅱ部の「4.7　COBIT成熟度モデルとリスクマネジメント」において示しておいたので、熟慮されたい。



4．リスクマネジメント体制例

リスクマネジメントシステムに係わる関係者・関係組織について参考として示しておく。

－某大手企業の体制－



注1）各質問項目の内容に関しては、職務権限と責任を持つ部門が回答を行う。

注2）JRMSの質問票回答とりまとめは、情報システム部門（事務局）が行う。

第Ⅳ部

ＪＲＭＳ質問項目

大項目		識別コード	質問項目数
Ⅰ	**経営とリスクの関係**		**9**
Ⅰ－1	経営環境とリスクマネジメント	1－1－1－　1 ～　9	9
Ⅱ	**JRMSにおけるリスクマネジメント計画**		**48**
Ⅱ－1	JRMSの計画	2－1－1－　1 ～　19	19
Ⅱ－2	JRMSの実行組織	2－2－1－　1 ～　11	11
Ⅱ－3	JRMSの維持	2－3－1－　1 ～　18	18
Ⅲ	**JRMSのリスク分析**		**113**
Ⅲ－1	JRMSのリスク分析	3－1－1－　1 ～　36	36
Ⅲ－2	情報セキュリティポリシーのリスク分析	3－2－1－　1 ～　11	11
Ⅲ－3	情報システムのリスク分析		66
	(1)情報システムのリスク分析	3－3－1－　1 ～　7	7
	(2)情報システム総合企画	3－3－2－　1 ～　5	5
	(3)システム開発	3－3－3－　1 ～　8	8
	(4)システム運用	3－3－4－　1 ～　5	5
	(5)不正アクセス・コンピュータウイルス関連	3－3－5－　1 ～　17	17
	(6)災害	3－3－6－　1 ～　6	6
	(7)障害	3－3－7－　1 ～　8	8
	(8)アウトソーシング	3－3－8－　1 ～　10	10
Ⅳ	**JRMSにおけるリスク対策**		**266**
Ⅳ－1	リスク対策における情報セキュリティ	4－1－1－　1 ～　35	35
Ⅳ－2	情報システムのリスク対策		62
	(1)情報システム総合企画	4－2－1－　1 ～　34	34
	(2)システム開発	4－2－2－　1 ～　23	23
	(3)システム運用	4－2－3－　1 ～　5	5
Ⅳ－3	不正アクセス	4－3－1－　1 ～　16	16
Ⅳ－4	コンピュータウイルス関連		43
	(1)コンピュータ犯罪	4－4－1－　1 ～　11	11
	(2)コンピュータウイルス	4－4－2－　1 ～　9	9
	(3)E－Commerce	4－4－3－　1 ～　11	11
	(4)電子メール	4－4－4－　1 ～　12	12
Ⅳ－5	災害対策	4－5－1－　1 ～　28	28
Ⅳ－6	障害対策	4－6－1－　1 ～　17	17
Ⅳ－7	アウトソーシング関連リスク対策	4－7－1－　1 ～　41	41
Ⅳ－8	その他関連項目	4－8－1－　1 ～　12	12
Ⅳ－9	バックアップ	4－9－1－　1 ～　8	8
Ⅳ－10	緊急時対策	4－10－1－　1 ～　5	5
Ⅳ－11	リスクファイナンス	4－11－1－　1 ～　15	15
計			436

注)質問No. 質問項目数ともに階層化されている場合の下位レベルの質問はカウントしていない

キーワード一覧

カテゴリ		キーワード一覧							
Ⅰ 経営とリスクの関係	Ⅰ－1. 経営環境とリスクマネジメント	1. 経営者の関心	2. 経営レベルによるリスクの範囲	3. リスクマネジメントポリシー	4. 組織	5. 役割・責任	6. 課題の明確化	7. 行動指針	8. 成果
		経営者の関心	経営レベルによるリスクの範囲	リスクマネジメントポリシー	組織	役割・責任	課題の明確化	行動指針	成果
Ⅱ JRMSにおけるリスクマネジメント計画	Ⅱ－1. JRMSの計画	1. 経営理念と計画	2. 管理体制の組織化	3. 適用業務責任・権限	4. 適用業務とリスクマネジメント	5. 管理目標	6. 目標脅威	7. 分析および対策	8. 緊急時対応
		経営理念	管理体制	適用業務責任・権限	基幹適用業務	管理目標	目標脅威	分析方法	緊急時対応
		目的	周知		設計時の前提			対策	
		保護対象	対策実施		目標と現状のギャップ				
			日常管理						
	Ⅱ－2. JRMSの実行組織	1. 全社的リスクマネジメント組織	2. 情報システムRM組織	3. ユーザの組織					
		RM担当役員の任命	情報システムリスク管理者	適用業務別オーナー					
		RM推進組織	情報システム情報セキュリティ管理者	ユーザ部門リスク担当者責任者					
		リスク担当者の役割権限	情報システムリスク対策組織						
			情報セキュリティ対策推進組織						
			情報システム運用管理責任者						
			リスク管理者の役割権限						
	Ⅱ－3. JRMSの維持	1. 是正改善	2. 監査	3. 監視	4. 文書化	5. リスクコミュニケーション	6. 教育の承認	7. 教育内容	8. レビュー
		是正改善	監査	統制、監視	基準の文書化	リスクコミュニケーション	経営者の教育承認	教育内容	RMS成果レビュー
		ボトルネックの発見、解決	監査基準	リスクマネジメント遵守度	RM文書管理	リスク情報開示	教育	ユーザ教育計画	
					記録の保持・活用				

カテゴリ			キーワード一覧							
Ⅲ JRMSのリスク分析	Ⅲ－1. JRMSのリスク分析		1. リスク分析の仕組み	2. リスク分析の体制	3. リスク分析基準	4. リスク分析(自然災害)	5. リスク分析(情報)	6. リスク分析(物理)	7. リスク分析(経営)	8. 特筆すべきリスクの認知
			JRMSのリスク分析の実施	変化を含めた社内体制	洗い出し実施基準	経営影響分析(自然災害)	ネットワーク	経営影響分析(障害)	経営影響分析(故意)	存続脅威分析
			未実施の場合の問題状況の認識	対応優先順位	発見方法		不正侵入		共謀犯罪	
			関連情報提供システム	フィードバック	測定実施基準		不正アクセス		スタッフ	
			保護対象リスク分析	分析の予算・スタッフ			ウイルス		共謀情報漏れ	
							テンペスト		経営影響分析(その他)	
							スパムメール			
	Ⅲ－2. 情報セキュリティポリシーのリスク分析		1. 情報セキュリティの経営からの視点	2. 情報セキュリティポリシーの対象	3. 特筆する情報リスク	4. 時間分析	5. 情報リスク洗い出し実施基準			
			経営の視点からの分析	情報セキュリティポリシーの対象	基幹システム情報漏洩(情報)	機能停止	情報リスク洗い出し実施基準			
					組織(情報)	SLA				
					ホームページ(情報)					
					爆弾テロ					
					システミックリスク					
					基幹システムダウン					
	Ⅲ－3. 情報システムのリスク分析	3－3－(1)情報システムのリスク分析	1. IT戦略のリスク分析	2. 業務影響	3. 利益阻害	4. 情報資産リスク	5. 情報リスクと自組織の倒産	6. 情報リスクと経営存続	7. システム不全	
			IT戦略のリスク分析	業務影響	利益阻害	情報資産リスク	情報リスクと自組織の倒産	情報リスクと経営存続	システム不全	
		3－3－(2)情報システム総合企画	1. システム企画のリスク分析	2. データ所有者	3. IT資産管理目録	4. ライセンス管理	5. 構成管理			
			システム企画のリスク分析	データ所有者	IT資産管理目録	ライセンス管理	構成管理			
			外注							
			コンプライアンス							
			担当部門別リスク							
			スタッフに関するリスク							
		3－3－(3)システム開発	1. プロジェクトリスク	2. ライフサイクル	3. 開発管理	4. 変更管理	5. 運用テスト			
			プロジェクトリスク	ライフサイクル	スタッフのリスク	ライフサイクル	テスト仕様書のリスク分析			
					コンプライアンス		運用テスト結果のリスク分析			
					情報セキュリティ要件					
					開発環境リスク					
					システムソフトウェア変更リスク					

カテゴリ			キーワード一覧							
Ⅲ JRMSのリスク分析	Ⅲ－3. 情報システムのリスク分析	3－3－(4)システム運用	1. システム運用	2. 運用管理						
			システム運用計画	運用管理のリスク分析						
			システム運用	運用管理ツールのリスク分析						
			システム運用資源							
		3－3－(5)不正アクセス・コンピュータウイルス関連	1. 不正アクセスのリスク	2. コンピュータ犯罪のリスク	3. ウイルスのリスク	4. E-Commerceのリスク	5. 電子メールのリスク			
			モバイル機器盗難	コンピュータ犯罪のリスク	ウイルス被害・復旧コスト	E-Commerce	電子メール			
			インターネット経由内部犯罪		感染の影響					
			ネッティングリスク		ベンダー緊急時対応の遅れ					
			不正アクセス痕跡		アンチウイルス更新遅れ					
			妨害		定期検診以上の要延					
			基幹システム不正		感染源の判明					
			DOS(情報)							
		3－3－(6)災害	1. 自然災害その他の災害と影響	2. 包括的リスクの可能性	3. 物的資産喪失の可能性	4. 人的リスクの可能性	5. ネットワーク障害リスクの可能性	6. 委託先リスクの可能性		
			情報システムへの影響	災害別リスク分析	物的資産喪失の可能性	人的リスクの可能性	ネットワーク障害リスクの可能性	委託先リスクの可能性		
		3－3－(7)障害	1. ハードウェア障害	2. ソフトウェア障害	3. 運用ミス障害					
			停電障害	ソフトウェア障害	運用ミス障害					
			ネットワーク障害							
			ハードウェア障害							
			回線障害							
		3－3－(8)アウトソーシング	1. アウトソーサの決定	2. 役割分担	3. 守秘義務	4. 実施	5. 変更管理			
			アウトソーサの選定手続き	契約内容	守秘義務	内容の確認	変更管理			
			アウトソーサの評価基準	責任分担	再委託の際の守秘義務	障害時対応				
				作業内容						

カテゴリ		キーワード一覧							
Ⅳ JRMSにおけるリスク対策	Ⅳ－1．リスク対策における情報セキュリティ	1．情報セキュリティポリシー	2．情報セキュリティポリシーに基づく実施基準	3．情報資産インベントリとサービススタッフ	4．情報セキュリティ個別対策	5．ID、パスワード、アクセス権付与	6．自社ホームページ承認	7．緊急対策	
		情報セキュリティポリシー	情報セキュリティポリシーに基づく実施基準	情報資産目録	複数人によるリスク分析	ID、パスワード、アクセス権付与	自社ホームページ承認	平時からのバックアップセンタ	
			実施基準での禁止事項	情報セキュリティ管理・担当者	ID、パスワード、アクセス管理			緊急連絡、対処	
			実施基準による自己点検、監査	スタッフ	情報オーナーの責任			個別緊急対策	
				外部のコンサルタント	手順と装置の仕様レベル				
					操作と業務処理手順				
					実施基準の定期的見直し				
					出張、移動中の実施基準				
					物理的破壊対策				
					中継地回避の実施基準				
					中継地懸念とログ分析				
					ファイアウォールレイアウト				
					コンピュータ利用手続き				
					データ、媒体利用				
					機密度ランク				
					アクセスログ権限				
					機密情報ログ				
					ログ確認				
					プログラムソースライブラリ管理				
					基幹システムの国際利用				
					個人情報保護				
					企業内教育				
					携帯端末				

カテゴリ			キーワード一覧							
Ⅳ JRMSにおけるリスク対策	Ⅳ－2. 情報システムのリスク対策	4－2－(1)情報システム総合企画	1. 情報システムポリシー	2. IT計画	3. 組織体制・機能	4. スタッフ	5. 経理	6. 管理(文書化を含む)	7. モニタリング	
			ポリシーの文書化	IT戦略とITインフラ計画	指揮命令系統	スキル	投資収益方針	全社データ管理	規制監視	
			ポリシーの徹底	ITインフラ計画	機能	人事計画	投資決定方法	全社データ標準化	是正措置	
			経営戦略との整合	導入計画	決裁権限	プロジェクト管理スキル	予定利益	全社データ所有者		
			標準ステップ		リスク別担当部門	品質管理教育訓練	IT資産管理目録	構成管理		
			外部統制				関連費用識別	リスク管理文書化		
								管理工程分割		
								品質管理文書化		
								工程ごとの品質基準		
								ファイル管理		
								ライセンス管理		
								プロジェクト管理標準		
								方法論		
								IT戦略		
		4－2－(2)システム開発	1. 一般	2. プロジェクト管理	3. システム要件定義	4. プログラム開発	5. テストデータ	6. 運用テスト	7. 変更管理	
			決裁実施基準	システム開発方法論	セキュリティ基準の遵守	開発環境	テストデータ	テスト仕様書の内容	管理責任者	
			開発に応じた決裁	進捗管理手続き	システム構成要素の入手可能性	コンプライアンス		運用テストの結果	バージョンアップ手続き	
			システム調達のライフサイクルにおけるセキュリティ						区分によるバージョンアップ	
			調達						変更管理	
			不正防止・機密保護基準						識別のための体系	
			破棄基準						高機密プログラム保管	
			品質管理						作業とレビューの分離	
			要員						アクセスの職務分離	
			職務定義						テストの機密保持規定	
			職務分離						配布先でのバージョン管理	
			情報セキュリティ保持の役割・責任							
			機密保持合意							

カテゴリ			キーワード一覧							
Ⅳ JRMSにおけるリスク対策	Ⅳ－2. 情報システムのリスク対策	4－2－(3)システム運用	1. システム運用	2. モニタリング機能	3. 管理機能					
			システム運用計画	記録・状況把握	運用管理					
			システム運用	モニタリング						
	Ⅳ－3. 不正アクセス		1. アクセス権管理	2. 論理的アクセス対策	3. 物理的アクセス対策	4. 個人認証	5. ネットワーク中のデータ保護	6. 不正検出	7. 緊急時対応	
			アクセス管理の実施基準	重要なデータ保護対策	携帯端末によるアクセス	個人認証	ネットワークの不正アクセス対策	アクセスログ確認	緊急対処方法	
			アクセス権付与	暗号鍵管理			自社ネットワークの不正アクセス対策		IPAへの届出	
			教育、訓練				外注先ネットワークの不正アクセス対策		JPCERT/CCへの相談	
			特別アクセス管理						外部機関への相談	
			職務分離							
	Ⅳ－4. コンピュータウイルス関連	Ⅳ－4－(1)コンピュータ犯罪	1. パスワード	2. データ保護対策	3. 盗聴対策					
			サーバ、基幹システムのパスワード変更	データ伝送の情報セキュリティ対策	盗聴対策					
			個人使用システム	データ保護対策	録音機器持込管理					
				暗号鍵	携帯電話持込					
					PDA					
					無線LAN					
					電磁波漏れ					
		4－4－(2)コンピュータウイルス	1. ウイルス手続き	2. ウイルス検出・駆除	3. 教育・訓練	4. ウイルス感染対策	5. 事後対策			
			ウイルス実施基準	ウイルス検出・駆除	スタッフの教育・訓練	ウイルス感染対策	事後対策			
						感染の緊急時対策	IPAへの届出			
						感染ウイルスの転送防止				
						伝染防止対策				
		4－4－(3)E-Commerce	1. プライバシー保護	2. 不良客情報管理	3. データ保護対策	4. ネットワーク機器対応	5. インターネット接続管理	6. 電子的証拠		
			プライバシー保護	不払い、不良客情報管理	電子商取引時のデータ保護対策	ネットワーク機器、サーバの信頼性	インターネット接続の規制	デジタル署名		
				不良客情報入手	インターネットからの攻撃	ネットワーク機器、サーバの性能	インターネット接続機器管理	時刻証明		
		4－4－(4)電子メール	1. 管理	2. メールサーバ管理	3. ネットワーク機器管理	4. インターネット接続機器管理	5. デジタル署名	6. 悪質メール対策	7. 転送エラー対策	
			電子メールの実施基準	メールサーバのデータ保護対策	ネットワーク機器、サーバの信頼性	インターネット接続機器管理	デジタル署名	添付ファイル	転送エラー	
			プライバシー保護	メールサーバへの攻撃	ネットワーク機器、サーバの性能			スクリプト		
								不正メール対策		

カテゴリ		キーワード一覧							
Ⅳ JRMSにおけるリスク対策	Ⅳ－5. 災害対策	1. 管理	2. 防火対策	3. 耐震対策	4. 水害対策				
		経営者の決定	防火壁	コンピュータ室の耐震対策	コンピュータ室の浸水対策				
		緊急事態対応計画	自動消火装置	データ保管場所の耐震対策	基幹システムの漏水対策				
		災害復旧レベル	区画放出対応消火システム	コンピュータ設置場所の耐震対策	電源設備の水害対策				
		是正措置	消火器	電源設備の耐震対策					
		避難対策	消火栓						
			遮断装置						
			2方向非常口						
	Ⅳ－6. 障害対策	1. 管理	2. 手続き	3. 情報システム	4. ユーティリティ				
		SLA	ソフトウェア更新手続き	障害対策機能	施設障害対策				
		ポリシーとの整合性	緊急時対応手続き	ディスク障害対策	電源設備				
		管理責任者の承認	携帯端末紛失連絡体制		空調設備				
		トランザクション量	代替バックアップ対策						
		緊急事態対応計画	ソフトウェア更新手続き						
		復旧手順	変更後障害						
		是正措置	SLAトランザクション量						
			更新確認						
			ソフトウェア更新						
			切り替えテスト						
	Ⅳ－7. アウトソーシング関連リスク対策	1. 目的	2. 役割分担	3. プロジェクト管理	4. アウトソーサ管理	5. 契約	6. 知的財産権	7. セキュリティ上の留意点	
		外注	役割分担	プロジェクト管理手法	選定評価基準	委託契約ルール	秘密保持	委託先情報セキュリティ	
		コスト削減	作業内容	共通開発方法論	SLA	賠償上限	再委託	受託者のシステムのセキュリティ対策	
				外注委託のレビュー	運用障害時対応	海外委託	知的財産権	不正防止、機密保持、破棄	
				会議体	ソフトウェア障害時対応	開発納期延期	知的財産権侵害	機密区分	
					品質管理	ソフトウェア瑕疵担保		形態に応じた保全対策	
						契約監査			
						変更手続き			

カテゴリ		キーワード一覧							
Ⅳ JRMSにおけるリスク対策	Ⅳ－8. その他関連項目	1. テロおよび人命損失	2. サービス提供	3. ユーザ間トラブル	4. 苦情処理対応	5. リスク対策手順整備	6. 危機管理計画徹底	7. 危機管理計画時間軸	8. 移動体データ保護
		テロ	会員規約	ユーザ間トラブル	苦情処理対応	その他リスク対策手順整備	危機管理計画の内外関係者への徹底	危機管理計画の時間軸別対応	移動体内蔵データ保護
		人命損失	規約違反	SLA					
			通信の秘密保護教育						
	Ⅳ－9. バックアップ	1. 二重化対策	2. ファイルのバックアップ	3. DBファイルのバックアップ	4. ネットワーク対策	5. 予備サイト			
		二重化対策	プログラムバックアップ	DBファイルバックアップ	回線・ネットワーク対策	予備サイト設置			
		電源設備	OSファイルバックアップ						
		空調設備	データファイルバックアップ						
	Ⅳ－10. 緊急時対策	1. 事前対応	2. 緊急時対応手続き	3. 復旧計画					
		事前対応	緊急時対応手続きの明確化	復旧計画					
		緊急時対応の訓練	定期的評価、是正改善						
	Ⅳ－11. リスクファイナンス	1. リスクファイナンスの役割	2. リスクファイナンスの対象領域	3. ファイナンスのリスク区分	4. 財務的対応	5. 外部コンサルタント活用	6. リスク対応のための組み合わせ		
		リスク分析	対象領域	ファイナンスのリスク区分	財務的判断基準	外部コンサルタント活用	リスク対応のための各種方法組み合わせ		
		マニュアル		管理不能リスクの明確化	財務的対応		リスクファイナンス成果評価基準		
		責任者決定			あらかじめの算定				
		責任者の役割・権限			リスクファイナンス見直し				
					実施関連部署間の協議				

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
経営とリスク	経営とリスク	Ⅰ．経営とリスクの関係				
経営環境とリスクマネジメント	経営環境とリスクマネジメント	Ⅰ－1．経営環境とリスクマネジメント				
1．経営者の関心	経営者の関心	1- 1- 1- 1	Q 経営者は情報システムに関するリスクについて認識していますか？			[redacted]
2．経営レベルによるリスクの範囲	経営レベルによるリスクの範囲	1- 1- 1- 2	Q 経営レベルのリスクにリスクマネジメントの範囲を広げて対応していますか？			
3．リスクマネジメントポリシー	リスクマネジメントポリシー	1- 1- 1- 3	Q リスクマネジメントに関する全社的なポリシー(方針)を有していますか？			
		1- 1- 1- 3- 1	Q リスクマネジメントポリシーは、最高経営者のもと全社的に構成されていますか？			[redacted]
		1- 1- 1- 3- 2	Q 貴社では経営理念に基づくリスクマネジメントポリシーを定めていますか？			
		1- 1- 1- 3- 3	Q リスクマネジメントポリシーでは、経営を脅かす事態に対する明確な対策を有していますか？			
		1- 1- 1- 3- 4	Q 緊急事態発生時の役員、スタッフ、担当者の役割はリスクマネジメントポリシーに定められていますか？			
		1- 1- 1- 3- 5	Q リスクマネジメントポリシーではコンプライアンスを重視していますか？			
		1- 1- 1- 3- 6	Q リスクマネジメントポリシーで内部監査の実施を明記していますか？			
		1- 1- 1- 3- 7	Q リスクマネジメントポリシーで外部監査の実施を明記していますか？			
		1- 1- 1- 4	Q リスクマネジメントポリシーに基づき、実施基準が機能部門別に構成されていますか？			
		1- 1- 1- 4- 1	Q 有効に機能するようフィードバックループ構成になっていますか？			
		1- 1- 1- 4- 2	Q 経営にとってのマイナス情報を吸い上げる機能を明確にしていますか？			
		1- 1- 1- 4- 3	Q スタッフに対し業務の機能分野ごとに教育訓練を行うことが計画化されていますか？			
		1- 1- 1- 4- 4	Q 「JIS Q 2001 リスクマネジメントシステム構築のための指針」を知っていますか？			
4．組織	組織	1- 1- 1- 5	Q 組織として守るべき対象を明確にしていますか？			
5．役割・責任	役割・責任	1- 1- 1- 6	Q 守るべき対象との関連において、リスクマネジメントに関する役割・責任・権限が文書化されていますか？			
6．課題の明確化	課題の明確化	1- 1- 1- 7	Q 組織におけるリスクマネジメントの具体的なリスク対応上の課題を明確に定めていますか？			
		1- 1- 1- 7- 1	Q 行動指針は、経営資源の保全を含んでいますか？			
		1- 1- 1- 7- 2	Q リスクに対する社会的責任をも含んでいますか？			
		1- 1- 1- 7- 3	Q 行動指針では基本的な目的を明確に設定していますか？			
		1- 1- 1- 7- 4	Q 機能部門におけるリスク対応は明確にされていますか？			
7．行動指針	行動指針	1- 1- 1- 8	Q リスクマネジメントの行動指針は明確にされていますか？			
		1- 1- 1- 8- 1	Q リスクマネジメントの評価を明確に行うシステムとなっていますか？	[redacted]		
		1- 1- 1- 8- 2	Q リスクマネジメントのテストを行うように定められていますか？			
		1- 1- 1- 8- 3	Q リスクマネジメントの監査を行うように定められていますか？			
		1- 1- 1- 8- 4	Q 環境変化に応じリスクマネジメントの行動計画の是正改善を含んでいますか？			
8．成果	成果	1- 1- 1- 9	Q リスクマネジメントシステムの達成の成果を明示していますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスクマネジメント計画	リスクマネジメント計画	Ⅱ. JRMSにおけるリスクマネジメント計画				
JRMS計画	JRMS計画	Ⅱ－1. JRMSの計画				
1. 経営理念と計画	経営理念	2-1- 1- 1	Q リスクマネジメント計画は経営理念を明確に反映していますか？			
	目的	2-1- 1- 2	Q 計画ではリスクマネジメントにおける基本的な目的はわかりやすく示されていますか？			
	保護対象	2-1- 1- 3	Q リスクマネジメント計画では護るべき対象を明確にしていますか？			
2. 管理体制の組織化	管理体制	2-1- 1- 4	Q リスクマネジメント計画においてリスク管理の体制が定義されていますか？			
	周知	2-1- 1- 5	Q リスクマネジメントの具体的な目標を関係者に周知させていますか？			
	対策実施	2-1- 1- 6	Q リスク対策の実施にあたって、責任権限は明確ですか？			
	日常管理	2-1- 1- 7	Q リスクマネジメントの日常管理方式は全社およびシステム担当者に明らかにされていますか？			
3. 適用業務責任・権限	適用業務責任・権限	2-1- 1- 8	Q システムの適用業務に関する責任と権限それぞれの機能部門・分野について明確になっていますか？			
		2-1- 1- 8- 1	Q 企画業務に関する責任と権限それぞれの機能部門・分野について明確になっていますか？			
		2-1- 1- 8- 2	Q 開発業務に関する責任と権限それぞれの機能部門・分野について明確になっていますか？			
		2-1- 1- 8- 3	Q 運用業務に関する責任と権限それぞれの機能部門・分野について明確になっていますか？			
		2-1- 1- 8- 4	Q 保守業務に関する責任と権限それぞれの機能部門・分野について明確になっていますか？			
		2-1- 1- 8- 5	Q 予算業務に関する責任と権限それぞれの機能部門・分野について明確になっていますか？			
		2-1- 1- 8- 6	Q その他の機能分野(　　)に関する責任と権限それぞれの機能部門・分野について明確になっていますか？ (該当する機能分野を(　)内に記入して利用)			
4. 適用業務とリスクマネジメント	基幹適用業務	2-1- 1- 9	Q 基幹システム適用業務はリスクマネジメントを前提に構築されていますか？			
	設計時の前提	2-1- 1- 10	Q 適用業務の設計時、情報セキュリティを前提の1つとしていますか？			
	目標と現状のギャップ	2-1- 1- 11	Q 目標と現状のレベルの差を明確にしていますか？			
5. 管理目標	管理目標	2-1- 1- 12	Q リスクマネジメントの管理目標を具体的に明示していますか？			
		2-1- 1- 12- 1	Q 物理的資産の管理目標を具体的に明示していますか？			
		2-1- 1- 12- 2	Q 情報資産の管理目標を具体的に明示していますか？			
		2-1- 1- 12- 3	Q 業務収益の管理目標を具体的に明示していますか？			
		2-1- 1- 12- 4	Q 社会的信用の管理目標を具体的に明示していますか？			
		2-1- 1- 12- 5	Q 社会的責任の管理目標を具体的に明示していますか？			
		2-1- 1- 12- 6	Q 人的資産の管理目標を具体的に明示していますか？			
		2-1- 1- 12- 7	Q 法的準拠の管理目標を具体的に明示していますか？			
6. 目標脅威	目標脅威	2-1- 1- 13	Q 具体的な目標を脅かすリスクやハザードについて情報の視点から分析を行っていますか？			
		2-1- 1- 13- 1	Q 物理的資産を脅かすリスクやハザードについて情報の視点から分析を行っていますか？			
		2-1- 1- 13- 2	Q 情報資産を脅かすリスクやハザードについて情報の視点から分析を行っていますか？			
		2-1- 1- 13- 3	Q 業務収益を脅かすリスクやハザードについて情報の視点から分析を行っていますか？			
		2-1- 1- 13- 4	Q 社会的信用を脅かすリスクやハザードについて情報の視点から分析を行っていますか？			
		2-1- 1- 13- 5	Q 社会的責任を脅かすリスクやハザードについて情報の視点から分析を行っていますか？			
		2-1- 1- 13- 6	Q 人的資産を脅かすリスクやハザードについて情報の視点から分析を行っていますか？			
		2-1- 1- 13- 7	Q サイバーテロを脅かすリスクやハザードについて情報の視点から分析を行っていますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスクマネジメント計画	リスクマネジメント計画	Ⅱ. JRMSにおけるリスクマネジメント計画				
JRMS計画	JRMS計画	Ⅱ－1. JRMSの計画				
7. 分析および対策	分析方法	2-1-1-14	Q リスク分析の方法は明確ですか？			
		2-1-1-14-1	Q 費用対効果分析の方法は明確ですか？			
		2-1-1-14-2	Q 意思決定分析の方法は明確ですか？			
		2-1-1-14-3	Q チェックリストの方法は明確ですか？			
		2-1-1-14-4	Q フローチャート分析の方法は明確ですか？			
		2-1-1-14-5	Q ソフトウェアリスク管理手法の方法は明確ですか？			
	対策	2-1-1-15	Q リスク分析の結果をリスク対策に反映させていますか？			
		2-1-1-16	Q リスク対策の方法は明確ですか？			
		2-1-1-17	Q リスク対策のための実施基準を有していますか？			
		2-2-1-18	Q リスク対策の採用につき経営者が最終承認していますか？			
8. 緊急時対応	緊急時対応	2-1-1-19	Q リスクマネジメントの緊急時対応は事前に備えられていますか？			
		2-1-1-19-1	Q 機密漏洩に対する緊急時対応は事前に備えられていますか？			
		2-1-1-19-2	Q 不正アクセスに対する緊急時対応は事前に備えられていますか？			
		2-1-1-19-3	Q マクロウイルスに対する緊急時対応は事前に備えられていますか？			
		2-1-1-19-4	Q 自然災害に対する緊急時対応は事前に備えられていますか？			
		2-1-1-19-5	Q 各種法令侵害に対する緊急時対応は事前に備えられていますか？			
		2-1-1-19-6	Q バックアップに対する緊急時対応は事前に備えられていますか？			
		2-1-1-19-7	Q その他ファシリティの移動が必要な事態に対する緊急時対応は事前に備えられていますか？			
実行組織	実行組織	Ⅱ-2. JRMSの実行組織				
1. 全社的リスクマネジメント組織	RM担当役員の任命	2-2-1-1	Q リスクマネジメントのための担当役員は最高経営者により任命されていますか？			
	RM推進組織	2-2-1-2	Q リスクマネジメントシステム推進のための組織が定められていますか？			
	リスク担当者の役割権限	2-2-1-3	Q リスク対策担当者の役割権限が明確に定められていますか？			
2. 情報システムリスクマネジメント組織	情報システムリスク管理者	2-2-1-4	Q 情報システムのリスク管理者を任命していますか？			
	情報システム情報セキュリティ管理者	2-2-1-5	Q 情報システムの情報セキュリティの管理者を任命していますか？			
	情報システムリスク対策組織	2-2-1-6	Q 情報システムのリスク対策組織は定められていますか？			
	情報セキュリティ対策推進組織	2-2-1-7	Q 情報システムの情報セキュリティ対策推進組織は定められていますか？			
	情報システム運用管理責任者	2-2-1-8	Q 情報システムの運用管理責任者を定めていますか？			
	リスク管理者の役割権限	2-2-1-9	Q 情報システムのリスク管理者の役割権限が明確に定められていますか？			
3. ユーザの組織	適用業務別オーナー	2-2-1-10	Q 情報システムの適用業務に関するユーザ側のオーナーは明示されていますか？			
	ユーザ部門リスク担当者責任者	2-2-1-11	Q ユーザ部門の適用業務に対するリスク担当責任者を定めていますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスクマネジメント計画	リスクマネジメント計画	Ⅱ. JRMSにおけるリスクマネジメント計画				
維持	維持	Ⅱ-3. JRMSの維持				
1. 是正改善	是正改善	2- 3- 1- 1	Q リスクマネジメントシステムに関して監視ならびに是正・改善の重要性を認識していますか？			
		2- 3- 1- 1- 1	Q リスクマネジメントシステムの実施に関するパフォーマンス評価基準をもっていますか？			
		2- 3- 1- 1- 2	Q リスクマネジメントの実施に関する監視を行っていますか？			
		2- 3- 1- 1- 3	Q リスクマネジメントの実施に関するパフォーマンス評価を行っていますか？			
		2- 3- 1- 1- 4	Q リスク対応のため、是正改善行動を採択する基準を有していますか？			
		2- 3- 1- 1- 5	Q 是正改善のためのフィードバックループをもっていますか？			
		2- 3- 1- 1- 6	Q フィードバックループはリスクマネジメントシステムのどの段階(リスク発見・確認・測定・リスク対策の策定・実施等)にも対応していますか？			
		2- 3- 1- 1- 7	Q 是正・改善措置を継続的に行っていますか？			
		2- 3- 1- 1- 8	Q 是正改善の状況を点検していますか？			
		2- 3- 1- 1- 9	Q 是正改善の実施後の有効性に関する検証を関係部門・部署に求めていますか？			
	ボトルネックの発見、解決	2- 3- 1- 2	Q リスクマネジメントの実施にとり、ボトルネックがあれば、それを排除する対応を取っていますか？			
2. 監査	監査	2- 3- 1- 3	Q リスク対応におけるシステム監査の重要性を認識していますか？			
		2- 3- 1- 3- 1	Q リスクマネジメントシステムの監査を実施していますか？			
		2- 3- 1- 3- 2	Q 内部監査による監査を実施していますか？			
		2- 3- 1- 3- 3	Q 外部監査による監査を実施していますか？			
		2- 3- 1- 3- 4	Q システム監査人を選任していますか？			
		2- 3- 1- 3- 5	Q システム監査を重視していない場合、そのことによるリスクを評価していますか？			
		2- 3- 1- 3- 6	Q リスクマネジメント責任者とシステム監査人の位置付けは明確ですか？			
		2- 3- 1- 3- 7	Q リスクマネジメント責任者とシステム監査人が同一人物でないことが公示されていますか？			
		2- 3- 1- 3- 8	Q 情報システム監査を実施していますか？			
		2- 3- 1- 3- 9	Q 内部監査による監査を実施していますか？			
		2- 3- 1- 3- 10	Q 外部監査による監査を実施していますか？			
		2- 3- 1- 3- 11	Q リスクマネジメントに関する記録を保存していますか？			
	監査基準	2- 3- 1- 4	Q システムに関する全業務(企画、開発、保守、運用)における監査基準は、リスクマネジメントの視点から明確で確実に守られていますか？			
3. 監視	統制、監視	2- 3- 1- 5	Q リスクマネジメントに関するトランザクション等の統制、監視は行われていますか？			
	リスクマネジメント遵守度	2- 3- 1- 6	Q リスクマネジメントシステム実施の遵守度を定期的にモニターしていますか？			
4. 文書化	基準の文書化	2- 3- 1- 7	Q リスクマネジメントに用いる実施基準は文書化されていますか？			
	RM文書管理	2- 3- 1- 8	Q リスクマネジメントシステム実施に関する文書管理を行っていますか？			
	記録の保持・活用	2- 3- 1- 9	Q リスク情報・リスクマネジメントに関する記録を保持・活用していますか？			
5. リスクコミュニケーション	リスクコミュニケーション	2- 3- 1- 10	Q リスクコミュニケーションに努力していますか？			
		2- 3- 1- 11	Q リスクコミュニケーションにおける課題は明確ですか？			
	リスク情報開示	2- 3- 1- 12	Q リスク情報の開示に関する実施基準を策定していますか？			
6. 教育の承認	経営者の教育承認	2- 3- 1- 13	Q 経営者は教育訓練計画を承認していますか？			
		2- 3- 1- 13- 1	Q スタッフについて教育訓練を行うことを計画していますか？	[redacted]		
		2- 3- 1- 13- 2	Q スタッフは定期的に訓練を実施していますか？			
		2- 3- 1- 13- 3	Q 情報システム部門は定期的に訓練を実施していますか？			
		2- 3- 1- 13- 4	Q ユーザ部門は定期的に訓練を実施していますか？			
	教育	2- 3- 1- 14	Q 組織維持のためリスクマネジメントに関する教育の位置付けは明確ですか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスクマネジメント計画	リスクマネジメント計画	Ⅱ. JRMSにおけるリスクマネジメント計画				
維持	維持	Ⅱ-3. JRMSの維持				
7. 教育内容	教育内容	2- 3- 1- 15	Q 教育訓練計画の内容について情報システムリスクを網羅していますか？			
		2- 3- 1- 15- 1	Q 教育訓練計画の内容について緊急事態対応を含んでいますか？	[redacted]		
		2- 3- 1- 15- 2	Q 教育訓練計画の内容についてシステムの誤作動対応を含んでいますか？			
		2- 3- 1- 15- 3	Q 教育訓練計画の内容についてシステムの停止対応を含んでいますか？			
		2- 3- 1- 15- 4	Q 教育訓練計画の内容についてシステムへの侵入対応を含んでいますか？			
		2- 3- 1- 16	Q ユーザ部門に対して情報システムの利用に関する実施基準について、企業で教育を実施していますか？			
	ユーザ教育計画	2- 3- 1- 17	Q ユーザ部門の教育訓練計画について情報システムリスクを網羅していますか？			
		2- 3- 1- 17- 1	Q ユーザ部門の教育訓練計画について緊急事態対応を含んでいますか？	[redacted]		
		2- 3- 1- 17- 2	Q ユーザ部門の教育訓練計画について実施基準を含んでいますか？			
		2- 3- 1- 17- 3	Q ユーザ部門の教育訓練計画について情報システム利用の実施基準を含んでいますか？			
8. レビュー	RMS成果レビュー	2- 3- 1- 18	Q 最高経営者によるリスクマネジメントシステムの成果のレビューを行っていますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク分析	リスク分析	Ⅲ. JRMSのリスク分析				
JRMSのリスク分析	JRMSのリスク分析	Ⅲ－1. JRMSのリスク分析				
1. リスク分析の仕組み	JRMSのリスク分析の実施	3- 1- 1- 1	Q リスク分析(発見・算定・評価)をリスクマネジメント計画において明確にしていますか？			
	未実施の場合の問題状況の認識	3- 1- 1- 2	Q リスク分析を実施していない場合の問題を認識していますか？			
	関連情報提供システム	3- 1- 1- 3	Q リスク関連情報をリスク分析担当者に提供する仕組みが構築されていますか？			
	保護対象リスク分析	3- 1- 1- 4	Q 明確にされた守るべき対象についてリスクを分析していますか？			
2. リスク分析の体制	変化を含めた社内体制	3- 1- 1- 5	Q 内外の経営環境の変化を含めたリスク環境の動きを捉える社内体制を有していますか？			
	対応優先順位	3- 1- 1- 6	Q リスクを洗い出して対応の優先順位を確定していますか？			
	フィードバック	3- 1- 1- 7	Q リスク発見・評価の見直しのフィードバックループをもっていますか？			
	分析の予算・スタッフ	3- 1- 1- 8	Q 予算・スタッフをリスク分析のため適切に導入していますか？			
3. リスク分析基準	洗い出し実施基準	3- 1- 1- 9	Q リスクをもれなく洗い出す実施基準を有していますか？			
	発見方法	3- 1- 1- 10	Q リスクの発見方法を持っていますか？			
		3- 1- 1- 11	Q 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？			
		3- 1- 1- 12	Q 定期的にリスクを洗い出していますか？			
		3- 1- 1- 13	Q 特定機能部門からの要請によりリスクの洗い出しを行っていますか？			
	測定実施基準	3- 1- 1- 14	Q リスク頻度を測定する実施基準を用意していますか？			
		3- 1- 1- 15	Q リスク強度を測定する実施基準を用意していますか？			
4. リスク分析(自然災害)	経営影響分析(自然災害)	3- 1- 1- 16	Q 災害の経営に与える影響をリスクの視点から分析していますか？			
		3- 1- 1- 16-1	Q 地震の経営に与える影響をリスクの視点から分析していますか？			[redacted]
		3- 1- 1- 16-2	Q 水害・津波の経営に与える影響をリスクの視点から分析していますか？			
		3- 1- 1- 16-3	Q 落雷の経営に与える影響をリスクの視点から分析していますか？			
		3- 1- 1- 16-4	Q 噴火の経営に与える影響をリスクの視点から分析していますか？			
		3- 1- 1- 16-5	Q 風害の経営に与える影響をリスクの視点から分析していますか？			
		3- 1- 1- 16-6	Q 雪害の経営に与える影響をリスクの視点から分析していますか？			
		3- 1- 1- 16-7	Q 雷害の経営に与える影響をリスクの視点から分析していますか？			
		3- 1- 1- 16-8	Q 浸水の経営に与える影響度を分析していますか？			
5. リスク分析(情報)	ネットワーク	3- 1- 1- 17	Q ネットワークの経営に与える影響をリスクの視点から分析していますか？			
	不正侵入	3- 1- 1- 18	Q 基幹システムへの不正侵入の経営に与える影響をリスクの視点から分析していますか？			[redacted]
	不正アクセス	3- 1- 1- 19	Q 不正アクセスの経営に与える影響をリスクの視点から分析していますか？			
	ウイルス	3- 1- 1- 20	Q コンピュータウイルスの経営に与える影響をリスクの視点から分析していますか？			
	テンペスト	3- 1- 1- 21	Q テンペスト(電波漏れ)の経営に与える影響をリスクの視点から分析していますか？			
	スパムメール	3- 1- 1- 22	Q スパムメールの経営に与える影響をリスクの視点から分析していますか？			
6. リスク分析(物理)	経営影響分析(障害)	3- 1- 1- 23	Q 障害の経営に与える影響をリスクの視点から分析していますか？			
		3- 1- 1- 23-1	Q 火災の経営に与える影響をリスクの視点から分析していますか？			[redacted]
		3- 1- 1- 23-2	Q 停電の経営に与える影響をリスクの視点から分析していますか？			
		3- 1- 1- 23-3	Q 物理的な侵入の経営に与える影響をリスクの視点から分析していますか？			
		3- 1- 1- 23-4	Q 爆発事故の経営に与える影響をリスクの視点から分析していますか？			
		3- 1- 1- 23-5	Q 漏水の経営に与える影響をリスクの視点から分析していますか？			
		3- 1- 1- 23-6	Q 動物の害の経営に与える影響をリスクの視点から分析していますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク分析	リスク分析	Ⅲ. JRMSのリスク分析				
JRMSのリスク分析	JRMSのリスク分析	Ⅲ－1. JRMSのリスク分析				
7. リスク分析(経営)	経営影響分析(故意)	3- 1- 1- 24	Q 複合リスクの経営に与える影響をリスクの視点から分析していますか？			
		3- 1- 1- 25	Q 盗難の経営に与える影響をリスクの視点から分析していますか？			
		3- 1- 1- 26	Q 盗聴の経営に与える影響をリスクの視点から分析していますか？			
		3- 1- 1- 27	Q 脅迫の経営に与える影響をリスクの視点から分析していますか？			
		3- 1- 1- 28	Q コンプライアンスに反する行為の経営に与える影響をリスクの視点から分析していますか？			
		3- 1- 1- 29	Q 上記の質問に対してリスク分析を実施していない場合の問題点を明確にしていますか？			
	共謀犯罪	3- 1- 1- 30	Q 経営者やスタッフ同士の共謀による(たとえば本社入金を他支店端末を用いて振替入金し、現金窃取)犯罪に関するリスクを分析していますか？			
	スタッフ	3- 1- 1- 31	Q 経営資産の管理において経営者やスタッフの不正・犯罪に関わるリスクを分析していますか？			
	共謀情報漏れ	3- 1- 1- 32	Q 経営者やスタッフ共謀により退職時に不正に重要データを持ち出しあるいは転送して新会社を設立する例がありますが、これらの経営に与える影響をリスクの視点から分析していますか？			
	経営影響分析(その他)	3- 1- 1- 33	Q 物理的な攻撃(爆弾)の経営に与える影響をリスクの視点から分析していますか？			
		3- 1- 1- 34	Q 戦争・動乱・テロ・暴動の経営に与える影響をリスクの視点から分析していますか？			
		3- 1- 1- 35	Q 人命損失の経営に与える影響を分析していますか？			
8. 特筆すべきリスクの認知	存続脅威分析	3- 1- 1- 36	Q 経営の存続にとり、信用が揺らぐ事態を分析していますか？			
		3- 1- 1- 36-1	Q 製品欠陥により、自社の信頼を揺るがす事態を分析していますか？			
		3- 1- 1- 36-2	Q 人事問題(スタッフ、経営者)が自社の信頼を揺るがすことになる事態を分析していますか？			
		3- 1- 1- 36-3	Q 内部不正の内部告発が自社の信頼を揺るがす事態を分析していますか？			
		3- 1- 1- 36-4	Q 業績不振が自社の信頼を揺るがす事態を分析していますか？			
		3- 1- 1- 36-5	Q 事後関係維持が自社の信頼を揺るがす事態を分析していますか？			
		3- 1- 1- 36-6	Q 不適切な広報対応が自社の信頼を揺るがす事態を分析していますか？			
		3- 1- 1- 36-7	Q ホームページ改ざんの及ぼす影響が自社の信頼を揺るがす事態を分析していますか？			
		3- 1- 1- 36-8	Q 情報システムを原因とする自社が提供するサービス・製品の重大な瑕疵PL事故が、自社の信頼を揺るがす事態を分析していますか？			
		3- 1- 1- 36-9	Q 原因を問わず情報システムが影響を受けての自社が提供するサービス・製品提供の著しい中断が、自社の信頼を揺るがす事態を分析していますか？(システムが1時間止まった場合の組織への損失))			
		3- 1- 1- 36-10	Q 会社ぐるみの違法行為(コンプライアンス違反)が及ぼす影響により、自社の信頼が揺らぐ事態を分析していますか？			
		3- 1- 1- 36-11	Q 情報システム犯罪行為を防げなかった場合、自社の信頼を揺るがす事態を分析していますか？			
		3- 1- 1- 36-12	Q 経営者の犯罪行為が自社の信頼を揺るがす事態を分析していますか？			
		3- 1- 1- 36-13	Q スタッフの犯罪行為(特に情報システム犯罪)が自社の信頼を揺るがす事態を分析していますか？			
		3- 1- 1- 36-14	Q ペーパーレス化の徹底の下ではシステム停止、遮断のリスクを分析していますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク分析	リスク分析	Ⅲ. JRMSのリスク分析				
情報セキュリティポリシー	情報セキュリティポリシー	Ⅲ-2. 情報セキュリティポリシーのリスク分析				
1. 情報セキュリティの経営からの視点	経営の視点からの分析	3- 2- 1- 1	Q 情報セキュリティポリシーを経営の視点から分析の対象としていますか？			■
2. 情報セキュリティポリシーの対象	情報セキュリティポリシーの対象	3- 2- 1- 2	Q 情報セキュリティポリシーでリスク分析の対象を定めていますか？			■
		3- 2- 1- 2- 1	Q ユーザ間トラブルリスクは情報セキュリティポリシーのリスク分析の対象となっていますか？			■
		3- 2- 1- 2- 2	Q 苦情処理対応トラブルリスクは情報セキュリティポリシーのリスク分析の対象となっていますか？			■
		3- 2- 1- 2- 3	Q バックアップリスクは情報セキュリティポリシーのリスク分析の対象となっていますか？	■		■
		3- 2- 1- 2- 4	Q 情報システム総合企画の内容が情報セキュリティポリシーのリスク分析の対象となっていますか？			■
		3- 2- 1- 2- 5	Q システム開発の内容が情報セキュリティポリシーのリスク分析の対象となっていますか？			■
		3- 2- 1- 2- 6	Q システム運用の内容が情報セキュリティポリシーのリスク分析の対象となっていますか？	■		■
		3- 2- 1- 2- 7	Q 災害が情報セキュリティポリシーのリスク分析の対象となっていますか？	■		■
		3- 2- 1- 2- 8	Q 障害が情報セキュリティポリシーのリスク分析の対象となっていますか？	■		■
		3- 2- 1- 2- 9	Q 不正アクセスが情報セキュリティポリシーのリスク分析の対象となっていますか？	■		■
		3- 2- 1- 2- 10	Q コンピュータウイルスが情報セキュリティポリシーのリスク分析の対象となっていますか？	■		■
		3- 2- 1- 2- 11	Q アウトソーシングに関わるリスクが情報セキュリティポリシーのリスク分析の対象となっていますか？			
		3- 2- 1- 2- 12	Q 緊急時対応の内容が情報セキュリティポリシーのリスク分析の対象となっていますか？			
		3- 2- 1- 2- 13	Q 情報セキュリティ推進組織の内容が情報セキュリティポリシーのリスク分析の対象となっていますか？			
		3- 2- 1- 2- 14	Q 点検の内容が情報セキュリティポリシーのリスク分析の対象となっていますか？	■		■
		3- 2- 1- 2- 15	Q 監査内容が情報セキュリティポリシーのリスク分析の対象となっていますか？			
3. 特筆する情報リスク	基幹システム情報漏洩(情報)	3- 2- 1- 3	Q 基幹情報システムから機密情報が窃取されるリスクを分析していますか？	■		■
	組織(情報)	3- 2- 1- 4	Q 組織の情報セキュリティ対策の脆弱性により、信用が大きく傷つくリスクを分析していますか？			
	ホームページ(情報)	3- 2- 1- 5	Q ホームページに関わる誹謗中傷リスク(被害リスク)を分析していますか？			■
	爆弾テロ	3- 2- 1- 6	Q 爆弾テロのリスクを想定していますか？			■
	システミックリスク	3- 2- 1- 7	Q 貴社にとり、システミックリスクの影響を分析していますか？	■		■
	基幹システムダウン	3- 2- 1- 8	Q 貴社の基幹システムに関して不正手段による影響のリスクを分析していますか？	■		■
4. 時間分析	機能停止	3- 2- 1- 9	Q システムの機能停止が許される時間をリスクの点から分析していますか？	■		■
	SLA	3- 2- 1- 10	Q SLAで示された各アプリケーションシステム障害回復までの時間が経営に与える影響を分析していますか？			
5. 情報リスク洗い出し実施基準	情報リスク洗い出し実施基準	3- 2- 1- 11	Q 情報システムのリスクをもれなく洗い出す実施基準を有していますか？ 例)媒体・システム・セキュリティソフトの保全機能の側面から、また、個別情報保全の行動基準、両者統合による現状評価等。	■		■
		3- 2- 1- 11- 1	Q 媒体が機能しているかを洗い出す実施基準を有していますか？	■		■
		3- 2- 1- 11- 2	Q 情報システムが機能しているかを洗い出す実施基準を有していますか？	■		■
		3- 2- 1- 11- 3	Q 情報セキュリティソフト(ファイアウォール等)が機能しているかを洗い出す実施基準を有していますか？	■		■
		3- 2- 1- 11- 4	Q 個別情報資源のリスクを洗い出す実施基準を有していますか？	■		■
		3- 2- 1- 11- 5	Q 上記以外に係わるリスクを洗い出す実施基準を有していますか？	■		■

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク分析	リスク分析	Ⅲ. JRMSのリスク分析				
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－3. 情報システムのリスク分析				
情報システムのリスク分析	情報システムのリスク分析	3－3－(1) 情報システムのリスク分析				
1. IT戦略のリスク分析	IT戦略のリスク分析	3- 3- 1- 1	Q IT戦略(組織全体の情報システム化戦略)に係わるリスクを分析していますか？			
		3- 3- 1- 1- 1	Q 情報システムに係わるリスクを分析していますか？			
		3- 3- 1- 1- 2	Q 情報システムの経営に関する重要度の測定を行っていますか？			
		3- 3- 1- 1- 3	Q 情報(コンテンツ、データ)の経営に関する重要度の測定を行っていますか？			
2. 業務影響	業務影響	3- 3- 1- 2	Q 情報システムが業務に与える影響を分析していますか？			
3. 利益阻害	利益阻害	3- 3- 1- 3	Q 情報システムが生み出す企業利益を阻害するリスクを分析していますか？			
4. 情報資産リスク	情報資産リスク	3- 3- 1- 4	Q 重要情報資産ごとのリスクを分析していますか？			
		3- 3- 1- 4- 1	Q 情報資産の重要性をランキングしていますか？			
		3- 3- 1- 4- 2	Q 情報資産のオーナーが明確になっていますか？			
		3- 3- 1- 4- 3	Q 情報資産の機密度を分類していますか？			
		3- 3- 1- 4- 4	Q 情報資産の可用性が維持されていますか？			
		3- 3- 1- 4- 5	Q 情報資産の改ざんのリスクを分析していますか？			
5. 情報リスクと自組織の倒産	情報リスクと自組織の倒産	3- 3- 1- 5	Q 情報システム関連のリスクが倒産に結びつくことについてリスクを分析していますか？			
6. 情報リスクと経営存続	情報リスクと経営存続	3- 3- 1- 6	Q 情報システムに関し、経営の存続を左右すると考えられるリスクを明確に定義していますか？			
7. システム不全	システム不全	3- 3- 1- 7	Q 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について分析していますか？			
		3- 3- 1- 7- 1	Q ネットワークの情報システムに与える影響をリスクの視点から分析していますか？			
		3- 3- 1- 7- 2	Q 情報システム(コンピュータシステム)の全面停止が情報システムに与える影響について分析していますか？			
		3- 3- 1- 7- 3	Q 情報システムの一部停止が情報システムに与える影響について分析していますか？			
		3- 3- 1- 7- 4	Q 誤作動が情報システムに与える影響について分析していますか？			
		3- 3- 1- 7- 5	Q 犯罪が情報システムに与える影響について分析していますか？			
		3- 3- 1- 7- 6	Q 対応ミスによるタイミングの遅れが情報システムに与える影響について分析していますか？			
		3- 3- 1- 7- 7	Q システムの質の低下が情報システムに与える影響について分析していますか？			
		3- 3- 1- 7- 8	Q 成果の量的減少が情報システムに与える影響について分析していますか？			
		3- 3- 1- 7- 9	Q 安全性・機密保持の悪化が情報システムに与える影響について分析していますか？			
		3- 3- 1- 7- 10	Q 変化(状況・環境・ニーズ・制度等)への対応性の欠如が情報システムに与える影響について分析していますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク分析	リスク分析	Ⅲ. JRMSのリスク分析				
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－3. 情報システムのリスク分析				
情報システム総合企画	情報システム総合企画	3－3－(2)情報システム総合企画				
1. システム企画のリスク分析	システム企画のリスク分析	3-3- 2- 1	Q システム企画に関するリスクを分析していますか？			
	外注	3-3- 2- 1- 1	Q システム企画におけるアウトソーシングに関するリスクを分析していますか？			
	コンプライアンス	3-3- 2- 1- 2	Q システム企画に関して外部法規制・各種契約等の観点からコンプライアンスのリスクを分析していますか？			
	担当部門別リスク	3-3- 2- 1- 3	Q システム企画に関係する部門の固有のリスクを明確にしていますか？			
	スタッフに関するリスク	3-3- 2- 1- 4	Q システム企画に関してスタッフのスキルの妥当性についてリスクを分析していますか？			
2. データ所有者	データ所有者	3-3- 2- 2	Q データのオーナーが不明確な場合のリスクを分析していますか？			
3. IT資産管理目録	IT資産管理目録	3-3- 2- 3	Q リスク分析のためIT資産のインベントリ(目録)がありますか？			
4. ライセンス管理	ライセンス管理	3-3- 2- 4	Q ライセンス管理が不備なために起こりうるリスクを分析していますか？			
5. 構成管理	構成管理	3-3- 2- 5	Q システムの構成管理に関するリスクを分析していますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザー
リスク分析	リスク分析	Ⅲ. JRMSのリスク分析				
情報システムのリスク分析	情報システムのリスク分析	Ⅲ-3 情報システムのリスク分析				
システム開発	システム開発	3−3−(3)システム開発 （システム開発においてアウトソーシングを利用する場合は、「3−3−(8)アウトソーシング」を適用し、評価に用いること）				
1. プロジェクトリスク	プロジェクトリスク	3- 3- 3- 1	Q システム開発に関してプロジェクトリスクを分析していますか？			
2. ライフサイクル	ライフサイクル	3- 3- 3- 2	Q 開発のライフサイクルの視点から情報システム開発に関するリスクを分析していますか？			
3. 開発管理	スタッフのリスク	3- 3- 3- 3	Q システム開発に関してスタッフのスキルの妥当性についてリスクを分析していますか？			
	コンプライアンス	3- 3- 3- 4	Q 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？			
	情報セキュリティ要件	3- 3- 3- 5	Q システム開発に関して情報セキュリティ要件に関してリスクを分析していますか？			
	開発環境リスク	3- 3- 3- 5- 1	Q 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？			
	システムソフトウェア変更リスク	3- 3- 3- 5- 2	Q システム開発に関してシステムソフトウェア変更のリスクを分析していますか？			
4. 変更管理	ライフサイクル	3- 3- 3- 6	Q システム開発のライフサイクルの視点から情報システムの変更のリスクを分析していますか？			
		3- 3- 3- 6- 1	Q システム開発における情報システムの未承認の変更のリスクを分析していますか？			
5. 運用テスト	テスト仕様書のリスク分析	3- 3- 3- 7	Q テスト仕様書の適格性についてリスクを分析していますか？			
	運用テスト結果のリスク分析	3- 3- 3- 8	Q 運用テスト結果についてリスクを分析していますか？			
		3- 3- 3- 8- 1	Q インストールの妥当性についてリスクを分析していますか？			
		3- 3- 3- 8- 2	Q 操作性についてリスクを分析していますか？			
		3- 3- 3- 8- 3	Q システム導入後の処理能力についてリスクを分析していますか？			
		3- 3- 3- 8- 4	Q システム導入後の処理時間についてリスクを分析していますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク分析	リスク分析	Ⅲ. JRMSのリスク分析				
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－3. 情報システムのリスク分析				
システム運用	システム運用	3－3－(4) システム運用　(システム運用においてアウトソーシングを利用する場合は、「3－3－(8)アウトソーシング」を適用し、評価に用いること)				
1. システム運用	システム運用計画	3- 3- 4- 1	Q システム運用計画策定に関する実施基準は明確に示されていますか？			
		3- 3- 4- 1- 1	Q システム運用計画は適正であるか定期的に確認していますか？			
	システム運用	3- 3- 4- 2	Q 円滑なシステム運用を阻害する要因についてリスクを考慮した対応策を考えていますか？			
		2- 3- 4- 2- 1	Q システム運用に関する実施基準は明確に示されていますか？			
	システム運用資源	3- 3- 4- 3	Q システム資源についての運営方式についてリスクを考慮した方針を設定していますか？			
		3- 3- 4- 3- 1	Q システムで取り扱う共用データについての運営方式についてリスクを考慮した方針を設定していますか？			
		3- 3- 4- 3- 2	Q システム資源についての運営方式についてリスクを考慮した方針を設定していますか？			
		3- 3- 4- 3- 3	Q ファイル管理についてリスクを考慮した方針を設定していますか？			
2. 運用管理	運用管理のリスク分析	3- 3- 4- 4	Q ファイル世代管理についてリスクを考慮した方針を設定していますか？			
		3- 3- 4- 4- 1	Q ライブラリ管理についてリスクを考慮した方針を設定していますか？			
		3- 3- 4- 4- 2	Q ファイル、データの定期的なバックアップは想定されるリスクを考慮して方針を設定していますか？			
		3- 3- 4- 4- 3	Q 適用業務管理、(たとえば入出力データの完全性)についてリスクを考慮した方針を設定していますか？			
	運用管理ツールのリスク分析	3- 3- 4- 5	Q 運用管理ツールについてリスクを分析していますか？			
		3- 3- 4- 5- 1	Q 構成管理ツールについてリスクを分析していますか？			
		3- 3- 4- 5- 2	Q 性能管理ツールについてリスクを分析していますか？			
		3- 3- 4- 5- 3	Q 障害管理ツールについてリスクを分析していますか？			
		3- 3- 4- 5- 4	Q セキュリティ管理ツールについてリスクを分析していますか？			
		3- 3- 4- 5- 5	Q 自動運用ツールについてリスクを分析していますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク分析	リスク分析	Ⅲ. JRMSのリスク分析				
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－3. 情報システムのリスク分析				
不正アクセス・ウイルス関連	不正アクセス・ウイルス関連	3－3－(5)不正アクセス・コンピュータウイルス関連				
1. 不正アクセスのリスク	モバイル機器(パソコン、PDAなど企業外で使う情報機器)盗難	3- 3- 5- 1	Q モバイル機器の盗難により重要情報を搾取されるリスクを分析していますか？			
		3- 3- 5- 1- 1	Q モバイル機器を共謀して社外に情報が流出するリスクを分析していますか？			
		3- 3- 5- 1- 2	Q 置き忘れ等の不注意によるモバイル機器内部の情報流出のリスクを分析していますか？			
	インターネット経由内部犯罪	3- 3- 5- 2	Q 内部者が(社内から)インターネット経由で中継点を変え、再び社内にアクセスすることで情報窃取されるリスクを分析していますか？			
	ネッティングリスク	3- 3- 5- 3	Q ネッティングに関するリスクを分析していますか？			
	不正アクセス痕跡	3- 3- 5- 4	Q WWWのログファイルやファイアウォールで不正アクセスらしき行為の痕跡を発見できますか？			
	妨害	3- 3- 5- 5	Q 悪意によるコンピュータなどへの妨害行為によってサービス中断するリスクを分析していますか？			
	基幹システム不正	3- 3- 5- 6	Q 基幹システムに対する内・外部からの不正アクセス、改ざん、妨害行為(例:メール爆弾)によって情報システムが正常に運用できなくなるなどのリスクを分析していますか？			
	DOS(情報)	3- 3- 5- 7	Q DOSによる妨害行為などでサービスが中断したりサービスレベルが低下することで、自社の経営に与えるリスクを分析していますか？			
2. コンピュータ犯罪のリスク	コンピュータ犯罪のリスク	3- 3- 5- 8	Q コンピュータ犯罪が経営に与える影響(サービスの中断や重要な情報流出、企業の不名誉なうわさのひろがり、など)のリスクを分析していますか？			
		3- 3- 5- 8- 1	Q 内部犯罪の場合、外部の関係者の信頼に与える影響のリスクを分析していますか？			
		3- 3- 5- 8- 2	Q 経営者や授業員が、コンピュータ犯罪を軽微と捉える傾向がありますか？			
3. ウイルスのリスク	ウイルス被害・復旧コスト	3- 3- 5- 9	Q コンピュータウイルス被害からの復旧作業にかかる費用の見積もりをしたことがありますか？			
	感染の影響	3- 3- 5- 10	Q コンピュータウイルス感染の(サービス中断など)のリスクを分析していますか？			
		3- 3- 5- 10- 1	Q コンピュータウイルス感染により取引先に悪影響や不安を与えるリスクを分析していますか？			
		3- 3- 5- 10- 2	Q コンピュータウイルス感染により株価への影響のリスクを分析していますか？			
		3- 3- 5- 10- 3	Q コンピュータウイルス感染により取引先から損害賠償を請求されるリスクを分析していますか？			
	ベンダー緊急時対応の遅れ	3- 3- 5- 11	Q アンチウイルスに関するベンダのウイルスサポート体制をチェックしなかったため、緊急時に対応できないリスクを分析していますか？			
	アンチウイルス更新遅れ	3- 3- 5- 12	Q アンチウイルスのデータファイルが更新されていなかったため、ウイルスに対応できず、被害を受けるリスクを分析していますか？			
	定期検診以上の蔓延	3- 3- 5- 13	Q 定期的なウイルスチェックだけでは間に合わず、ウイルスの蔓延を防ぐことができなかった時のリスクを分析していますか？			
	感染源の判明	3- 3- 5- 14	Q ウイルスの感染原因を追求したり、感染の経路を追跡することができますか？			
4. E-Commerceのリスク	E-Commerce	3- 3- 5- 15	Q E-Commerceサービスの提供やサービスの利用の両面からリスクを分析していますか？			
5. 電子メールのリスク	電子メール	3- 3- 5- 16	Q 電子メールの利用によって社内情報が漏れたり、ウイルスを誤って他社に送る等のリスクを分析していますか？			
		3- 3- 5- 17	Q 電子メールが使えなくなったときの企業活動に与えるリスクを分析していますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク分析	リスク分析	Ⅲ. JRMSのリスク分析				
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－3. 情報システムのリスク分析				
災害別リスク分析	災害別リスク分析	3－3－(6) 災害				
1. 自然災害その他の災害と影響	情報システムへの影響	3- 3- 6- 1	Q 災害の情報システムに与える影響をリスクの視点から分析していますか？			
		3- 3－ 6- 1- 1	Q 火災の情報システムに与える影響をリスクの視点から分析していますか？			
		3- 3－ 6- 1- 2	Q 盗難の情報システムに与える影響をリスクの視点から分析していますか？			
		3- 3- 6- 1- 3	Q 物理的な侵入の情報システムに与える影響をリスクの視点から分析していますか？			
		3- 3－ 6- 1- 4	Q 物理的な攻撃(爆弾)の情報システムに与える影響をリスクの視点から分析していますか？			
		3- 3－ 6- 1- 5	Q 爆発事故の情報システムに与える影響をリスクの視点から分析していますか？			
		3- 3- 6- 1- 6	Q 漏水の情報システムに与える影響をリスクの視点から分析していますか？			
		3- 3－ 6- 1- 7	Q 動物の害の情報システムに与える影響をリスクの視点から分析していますか？			
		3- 3－ 6- 1- 8	Q 盗聴の情報システムに与える影響をリスクの視点から分析していますか？			
		3- 3- 6- 1- 9	Q 脅迫の情報システムに与える影響をリスクの視点から分析していますか？			
		3- 3－ 6- 1- 10	Q 情報システム(ハード、ソフト、メディア)のライフサイクルの全過程をリスクの視点から分析していますか？			
		3- 3－ 6- 1- 11	Q 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の視点から分析していますか？			
		3- 3- 6- 1- 12	Q コンプライアンスに反する行為の情報システムに与える影響をリスクの視点から分析していますか？			
		3- 3－ 6- 1- 13	Q 戦争・動乱・暴動の情報システムに与える影響をリスクの視点から分析していますか？			
		3- 3－ 6- 1- 14	Q 上記の質問に対してリスク分析を実施していない場合の問題点を明確にしていますか？			
2. 包括的リスクの可能性	災害別リスク分析	3- 3- 6- 2	Q 自然災害がもたらす包括的リスクの可能性を災害別に分析していますか？			
		3- 3- 6- 2- 1	Q 地震がもたらす包括的リスクの可能性を分析していますか？			
		3- 3- 6- 2- 2	Q 水害・津波がもたらす包括的リスクの可能性を分析していますか？			
		3- 3- 6- 2- 3	Q 落雷がもたらす包括的リスクの可能性を分析していますか？			
		3- 3- 6- 2- 4	Q 噴火がもたらす包括的リスクの可能性を分析していますか？			
		3- 3- 6- 2- 5	Q 風害がもたらす包括的リスクの可能性を分析していますか？			
		3- 3- 6- 2- 6	Q 雪害がもたらす包括的リスクの可能性を分析していますか？			
		3- 3- 6- 2- 7	Q 雹害がもたらす包括的リスクの可能性を分析していますか？			
		3- 3- 6- 2- 8	Q 火災がもたらす包括的リスクの可能性を分析していますか？			
3. 物的資産喪失の可能性	物的資産喪失の可能性	3- 3- 6- 3	Q 自然災害がもたらす物的資産喪失のリスクの可能性を分析していますか？			
		3- 3- 6- 3- 1	Q ディスク破損がもたらす物的資産損失のリスクの可能性を分析していますか？			
		3- 3- 6- 3- 2	Q テープ破損がもたらす物的資産損失のリスクの可能性を分析していますか？			
		3- 3- 6- 3- 3	Q フロッピィディスク破損がもたらす物的資産損失のリスクの可能性を分析していますか？			
		3- 3- 6- 3- 4	Q メモリーカード破損がもたらす物的資産損失のリスクの可能性を分析していますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク分析	リスク分析	Ⅲ. JRMSのリスク分析				
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－3. 情報システムのリスク分析				
災害別リスク分析	災害別リスク分析	3－3－(6) 災害				
4. 人的リスクの可能性	人的リスクの可能性	3-3-6-4	Q 自然災害に乗じて起こす人的リスクの可能性を分析していますか？	[redacted]		[redacted]
		3-3-6-4-1	Q 固定コンピュータ(デスクトップ、サーバ、大型)の盗難に乗じて起こす人的リスクの可能性を分析していますか？			
		3-3-6-4-2	Q 携帯コンピュータ(モバイル)盗難・置き忘れに乗じて起こす人的リスクの可能性を分析していますか？			
		3-3-6-4-3	Q テープ、フロッピィディスク、カードの盗難・置き忘れに乗じて起こす人的リスクの可能性を分析していますか？			
		3-3-6-4-4	Q オペレーションミスによる消去、誤記入に乗じて起こす人的リスクの可能性を分析していますか？			
		3-3-6-4-5	Q プログラムミスによる消去、誤記入に乗じて起こす人的リスクの可能性を分析していますか？			
		3-3-6-4-6	Q 不正アクセス(内部犯罪)による消去、誤記入に乗じて起こす人的リスクの可能性を分析していますか？			
		3-3-6-4-7	Q 不正アクセス(外部犯罪)による消去、誤記入に乗じて起こす人的リスクの可能性を分析していますか？			
		3-3-6-4-8	Q ウイルスによる消去、誤記入に乗じて起こす人的リスクの可能性を分析していますか？			
		3-3-6-4-9	Q 乱入による記憶媒体の物理的破壊に乗じて起こす人的リスクの可能性を分析していますか？			
		3-3-6-4-10	Q テロ爆破による記憶媒体の物理的破損に乗じて起こす人的リスクの可能性を分析していますか？			
5. ネットワーク障害リスクの可能性	ネットワーク障害リスクの可能性	3-3-6-5	Q 自然災害によってもたらされるネットワーク障害によるリスクの可能性を分析していますか？			
6. 委託先リスクの可能性	委託先リスクの可能性	3-3-6-6	Q 自然災害における委託先での上記リスクの可能性を分析していますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク分析	リスク分析	Ⅲ. JRMSのリスク分析				
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－3. 情報システムのリスク分析				
障害	障害	3－3－(7) 障害				
1. ハードウェア障害	停電障害	3- 3- 7- 1	Q 停電の情報システムに与える影響をリスクの視点から分析していますか？			
	ネットワーク障害	3- 3- 7- 2	Q ネットワーク障害リスクは情報セキュリティポリシーのリスク分析の対象となっていますか？			
		3- 3- 7- 3	Q ネットワーク障害リスクについて、リスク評価:頻度および経営に与える影響度を分析していますか？			
	ハードウェア障害	3- 3- 7- 4	Q ハードウェア障害のリスク分析を行っていますか？			
		3- 3- 7- 4- 1	Q サーバの障害のリスク分析を行っていますか？			
		3- 3- 7- 4- 2	Q 回線障害、LAN障害についてリスク分析を行っていますか？			
		3- 3- 7- 4- 3	Q インターネットプロバイダのサービス機能障害についてリスク分析を行っていますか？			
		3- 3- 7- 4- 4	Q ユーザまたは端末、クライアント機の障害についてリスク分析を行っていますか？			
	回線障害	3- 3- 7- 5	Q 回線障害リスクは情報セキュリティポリシーのリスク分析の対象となっていますか？			
		3- 3- 7- 6	Q 回線障害リスクについて、リスク評価:頻度および経営に与える影響度を分析していますか？			
		3- 3- 7- 6- 1	Q 回線障害による未着による情報紛失によってもたらされるネットワーク障害によるリスクの可能性を分析していますか？			
		3- 3- 7- 6- 2	Q インターネット送信中の未着による情報紛失によってもたらされるネットワーク障害によるリスクの可能性を分析していますか？			
2. ソフトウェア障害	ソフトウェア障害	3- 3- 7- 7	Q ソフトウェア障害のリスク分析を行っていますか？			
		3- 3- 7- 7- 1	Q サーバのO/S、ライセンスプログラムの障害についてリスク分析を行っていますか？			
		3- 3- 7- 7- 2	Q サーバのアプリケーションプログラムの障害についてリスク分析を行っていますか？			
		3- 3- 7- 7- 3	Q ユーザまたは端末、クライアント機の障害についてリスク分析を行っていますか？			
		3- 3- 7- 7- 4	Q その他ソフトウェアの障害についてリスク分析を行っていますか？			
3. 運用ミス障害	運用ミス障害	3- 3- 7- 8	Q 運用ミス障害のリスク分析を行っていますか？			
		3- 3- 7- 8- 1	Q バックアップリスクについて、リスク評価:頻度および経営に与える影響度を分析していますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク分析	リスク分析	Ⅲ. JRMSのリスク分析				
情報システムのリスク分析	情報システムのリスク分析	Ⅲ－3. 情報システムのリスク分析				
アウトソーシング	アウトソーシング	3－3－(8)アウトソーシング				
1. アウトソーサの決定	アウトソーサの選定手続き	3- 3- 8- 1	Q アウトソーサの選定手続きについてリスク分析を行っていますか？	[redacted]		[redacted]
	アウトソーサの評価基準	3- 3- 8- 2	Q アウトソーサの評価基準についてリスク分析を行っていますか？			
2. 役割分担	契約内容	3- 3- 8- 3	Q アウトソーシング契約内容についてリスク分析を行っていますか？			
	責任分担	3- 3- 8- 4	Q 委託者と受託者の責任分担についてリスク分析を行っていますか？			
	作業内容	3- 3- 8- 5	Q 受託者の作業(業務内容、範囲、スケジュール)内容についてリスク分析を行っていますか？			
3. 守秘義務	守秘義務	3- 3- 8- 6	Q 受託者の守秘義務についてリスク分析を行っていますか？			
	再委託の際の守秘義務	3- 3- 8- 7	Q アウトソーシングの再委託を許す場合の、委託者と同様の守秘義務についてリスク分析を行っていますか？			
4. 実施	内容の確認	3- 3- 8- 8	Q アウトソーシング契約で両者で交わす文書や会議の内容についてリスク分析を行っていますか？			
	障害時対応	3- 3- 8- 9	Q 障害時の対応(体制、手続き)についてリスク分析を行っていますか？			
5. 変更管理	変更管理	3- 3- 8- 10	Q アウトソーシング契約での契約内容の変更手続き(作業、契約、システム)についてリスク分析を行っていますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
情報セキュリティ	情報セキュリティ	Ⅳ－1. リスク対策における情報セキュリティ				
1. 情報セキュリティポリシー	情報セキュリティポリシー	4- 1- 1- 1	Q リスクマネジメントポリシーに基づいて情報セキュリティポリシーを定めていますか？			
2. 情報セキュリティポリシーに基づく実施基準	情報セキュリティポリシーに基づく実施基準	4- 1- 1- 2	Q 情報セキュリティポリシーに基づく実施基準を定めていますか？			
		4- 1- 1- 2- 1	Q 実施基準はリスクマネジメントシステム計画と整合性がとられた包括的な実施基準として明確に定められていますか？			
		4- 1- 1- 2- 2	Q 実施基準は、企業の特性を重視して作成していますか？			
		4- 1- 1- 2- 3	Q 実施基準には実践的な項目配列、継続的な日常点検、点検結果の評価リストが含まれていますか？			
		4- 1- 1- 2- 4	Q 緊急事態発生後の復旧計画で経営者、スタッフ、担当者の役割、最低限の復旧サービスレベル等について実施基準で定められていますか？			
		4- 1- 1- 2- 5	Q 実施基準の策定に関してCC(Common Criteria)との国際的な整合性は、考慮していますか？			
		4- 1- 1- 2- 6	Q 実施基準の策定に関してISO17799等との国際的な整合性は、考慮していますか？			
	実施基準での禁止事項	4- 1- 1- 3	Q 実施基準で禁止事項を明確にしていますか？			
		4- 1- 1- 3- 1	Q 市販のソフトをコピーして使う行為を禁止していますか？			
		4- 1- 1- 3- 2	Q 所有者のあるデータ、プログラムを無断で使う行為を禁止していますか？			
		4- 1- 1- 3- 3	Q 悪意によりイントラネットあるいはLAN情報処理環境に侵入し、機密情報を窃取する行為を禁止していますか？			
		4- 1- 1- 3- 4	Q 所有者のあるデータ、プログラムを覗き見る行為を禁止していますか？			
		4- 1- 1- 3- 5	Q 会社のコンピュータを私用に使う行為を禁止していますか？			
		4- 1- 1- 3- 6	Q コンピュータウイルスを伝染させる行為を禁止していますか？			
		4- 1- 1- 3- 7	Q 他社のシステムへ不正侵入する行為を禁止していますか？			
		4- 1- 1- 3- 8	Q WWWを仕事以外(個人目的での発注、アンケート回答等)で利用する行為を禁止していますか？			
		4- 1- 1- 3- 9	Q 意図的に外部端末からインターネットを通じてデータの不正入力を行い、情報撹乱する行為を禁止していますか？			
		4- 1- 1- 3- 10	Q 私用の電子メールを受発信する行為を禁止していますか？			
		4- 1- 1- 3- 11	Q ネットワークにログインしている他のマシンのファイルを見る行為を禁止していますか？			
		4- 1- 1- 3- 12	Q 共有サーバにある仕事に関係していないファイルを見る行為を禁止していますか？			
		4- 1- 1- 3- 13	Q 他人のIDを無断借用する行為を禁止していますか？			
		4- 1- 1- 3- 14	Q メール、ブラウザ等接続されたままの他人のマシンを操作する行為 を禁止していますか？			
		4- 1- 1- 3- 15	Q 時間外に会社のコンピュータでゲームを行う行為を禁止していますか？			
		4- 1- 1- 3- 16	Q 業務上入手した顧客情報を正当な理由なしに第3者に売却する行為を禁止していますか？			
		4- 1- 1- 3- 17	Q 許可なくホームページを書き換えて会社や組織に対する誹謗中傷する行為を禁止していますか？			
		4- 1- 1- 3- 18	Q 電子掲示板を用いて特定の組織、人間を誹謗中傷したり、名誉を傷つける行為を禁止していますか？			
		4- 1- 1- 3- 19	Q 情報システムの動作障害を引き起こす行為を禁止していますか？			
		4- 1- 1- 3- 20	Q 正当な理由なくプログラム、データを改ざんする行為を禁止していますか？			
		4- 1- 1- 3- 21	Q 許可なく情報をシステムを通じて開示する行為を禁止していますか？			
		4- 1- 1- 3- 22	Q スパムメールを発信する行為を禁止していますか？			
		4- 1- 1- 3- 23	Q 社会秩序の安全維持に反する情報の提供を禁止していますか？			
	実施基準による自己点検、監査	4- 1- 1- 4	Q 内部者のコンピュータ利用に関する自己点検システム、監査システムは実施基準によって定められていますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
情報セキュリティ	情報セキュリティ	Ⅳ－1. リスク対策における情報セキュリティ				
3. 情報資産インベントリとサービススタッフ	情報資産目録	4- 1- 1- 5	Q 保護対象の情報資産は漏れなく掘り起こされ、インベントリ(目録)リストに列挙されていますか？			
		4- 1- 1- 5- 1	Q 掘り起こしのための実施基準は定められていますか？			
		4- 1- 1- 5- 2	Q 保護対象インベントリ(目録)から劣化した媒体を排除していますか？			
	情報セキュリティ管理・担当者	4- 1- 1- 5- 3	Q 情報セキュリティ管理者または担当者がいますか？			
	スタッフ	4- 1- 1- 5- 4	Q スタッフに対して強制休暇をとらせる制度がありますか？			
		4- 1- 1- 5- 5	Q スタッフに対してリスクの視点から定期的な業務のローテーションを組んでいますか？			
	外部のコンサルタント	4- 1- 1- 6	Q 外部のコンサルタントやサービスを利用していますか？			
4. 情報セキュリティ個別対策	複数人によるリスク分析	4- 1- 1- 7	Q 情報資産への脅威(リスク)の分析は、関係する組織から視点の異なる複数人の参画を得てなされていますか？			
		4- 1- 1- 7- 1	Q 実施基準の中のリスク対策は情報処理プロセスに沿って論理的なプロセスを踏んで構築されていますか？			
	ID、パスワード、アクセス管理	4- 1- 1- 8	Q IDに関する実施基準がありますか？			
		4- 1- 1- 9	Q パスワード付与に関する実施基準がありますか？			
		4- 1- 1- 10	Q アクセス権限に関する実施基準がありますか？			
	情報オーナーの責任	4- 1- 1- 11	Q 実施基準には、機密性の高い個別情報の生成、管理、破棄に至るまでの情報のオーナーの責任と役割について明確に定められていますか？			
	手順と装置の仕様レベル	4- 1- 1- 12	Q 実施基準では重要資産の取扱い実施基準と重要装置の仕様を含んでいますか？			
	操作と業務処理手順	4- 1- 1- 13	Q 実施基準では、情報システムに関して、操作および業務処理実施基準等を具体的に示していますか？			
	実施基準の定期的見直し	4- 1- 1- 14	Q 実施基準を定期的に見直していますか？			
	出張、移動中の実施基準	4- 1- 1- 15	Q 出張中、移動中の環境についての実施基準がありますか？			
	物理的破壊対策	4- 1- 1- 16	Q 所有者以外の者からシステムの物理的破壊を受けることを防げる対策は*規定*によって義務づけられていますか？			
	中継地回避の実施基準	4- 1- 1- 17	Q 不正侵入や電子メールの不正中継地とされることを避けるための実施基準は定められていますか？			
	中継地懸念とログ分析	4- 1- 1- 18	Q 知らない間にサイバーテロの中継基地とされているのではないかとの疑いをもってEメール受信ログ、ホストごとのシステムアプリケーションログの監視をしていますか？			
	ファイアウォールレイアウト	4- 1- 1- 19	Q ファイアウォールが効果的に機能を果たすために実施基準によってレイアウトが定められていますか？			
	コンピュータ利用手続き	4- 1- 1- 20	Q コンピュータ利用の*手続き*が定められていますか？			
	データ、媒体利用	4- 1- 1- 21	Q データや媒体の使用・保管の管理は実施基準で定められていますか？			
	機密度ランク	4- 1- 1- 22	Q 情報についての機密度のランクを実施基準において設定していますか？			
	アクセスログ権限	4- 1- 1- 23	Q アクセスログについてアクセスの権限、権限外の記録方法について実施基準で定めていますか？			
	機密情報ログ	4- 1- 1- 24	Q 機密度の高い個別情報に関して、生成、アクセス、その他の処理プロセスは、ログに残されていますか？			
	ログ確認	4- 1- 1- 25	Q 情報のオーナーおよびシステム管理者が上記ログを定期的に確認していますか？			
	プログラムソースライブラリ管理	4- 1- 1- 26	Q プログラムソースライブラリの管理・修正・変更の記録についての方法について実施基準で定めていますか？			
	基幹システムの国際利用	4- 1- 1- 27	Q 基幹システムを国際的に利用している場合、国際利用している基幹システムについて、情報システムのセキュリティ対策を講じていますか？			
	個人情報保護	4- 1- 1- 28	Q 個人情報保護に関し、実施基準で定められていますか？			
	企業内教育	4- 1- 1- 29	Q 情報システムの利用に関する実施基準について、企業で教育を実施していますか？			
	携帯端末	4- 1- 1- 30	Q 社内システムへアクセスできるような携帯端末を利用している場合、携帯端末からのユーザ認証、アクセス管理は適切ですか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
情報セキュリティ	情報セキュリティ	Ⅳ－1. リスク対策における情報セキュリティ				
5. ID,パスワード、アクセス権付与	ID,パスワード、アクセス権付与	4- 1- 1- 31	Q コンピュータ利用の申し込み実施基準が定められていますか？			
		4- 1- 1- 31-1	Q ID、パスワード付与の手続きが定められていますか？			
		4- 1- 1- 31-2	Q ID、パスワードの付与についてチェックシステムがありますか？			
		4- 1- 1- 31-3	Q アクセス権付与の手続きが定められていますか？			
		4- 1- 1- 31-4	Q アクセス権の付与についてチェックしていますか？			
		4- 1- 1- 31-5	Q リモートアクセスサービスの手続きが定められていますか？			
		4- 1- 1- 31-6	Q リモートアクセスサービスの利用許可についてチェックしていますか？			
6. 自社ホームページ承認	自社ホームページ承認	4- 1- 1- 32	Q 自社のホームページへの掲載許可についてチェックしていますか？			
		4- 1- 1- 32-1	Q 自社のホームページへの掲載許可について実施基準で定められていますか？			
		4- 1- 1- 32-2	Q コンテンツの知的財産権の審査・登録の制度は実施基準によって整備されていますか？			
		4- 1- 1- 32-3	Q 侵害があった場合の手続きを定めていますか？			
		4- 1- 1- 32-4	Q コンテンツに関して、組織体の営業機密が不用意に漏洩されていないかチェックしていますか？			
		4- 1- 1- 32-5	Q HP記載内容の正確性、表現（差別用語等）等をチェックする部署を適切に定めていますか？			
7. 緊急対策	平時からのバックアップセンタ	4- 1- 1- 33	Q 情報喪失に備えて、平時からのバックアップセンタが準備されていますか？			
	緊急連絡、対処	4- 1- 1- 34	Q ハッカー、ウイルス侵入、不正アクセス等による緊急事態対処のための緊急連絡、対応方法は*手続き*として定められていますか？			
	個別緊急対策	4- 1- 1- 35	Q この緊急時対策は防災・事故緊急対策または別の情報セキュリティ用の対策ですか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策				
情報システム総合企画	情報システム総合企画	4－2-(1) 情報システム総合企画				
1. 情報セキュリティポリシー	ポリシーの文書化	4- 2- 1- 1	Q ITに関する情報セキュリティポリシーが文書化されていますか？			
	ポリシーの徹底	4- 2- 1- 2	Q 情報セキュリティポリシーは、関係者に徹底されていますか？			
	経営戦略との整合	4- 2- 1- 3	Q 経営戦略とIT戦略の整合性、(例:経営戦略での業務改革と、それを実現するシステム)がとられていますか？			
	標準ステップ	4- 2- 1- 4	Q IT戦略を作成するための標準化されたステップが存在しますか？			
	外部規制	4- 2- 1- 5	Q 外部規制に関する情報セキュリティポリシーが文書化されていますか？			
2. IT計画	IT戦略とITインフラ計画	4- 2- 1- 6	Q IT戦略とITインフラストラクチャ計画の整合がとられていますか？			
	ITインフラ計画	4- 2- 1- 7	Q ITインフラストラクチャ計画、(例:新アプリケーションシステムに必要な技術)が文書としてまとめられていますか？			
	導入計画	4- 2- 1- 8	Q 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？			
3. 組織体制・機能	指揮命令系統	4- 2- 1- 9	Q 情報システム組織として、適切な指揮命令系統が作られていますか？			
	機能	4- 2- 1- 10	Q 情報システム組織に、適切な情報セキュリティ機能が置かれていますか？			
		4- 2- 1- 10-1	Q 情報システム組織に、適切なインターナルコントロール機能が置かれていますか？			
		4- 2- 1- 10-2	Q 情報システム組織に、適切な品質管理機能が置かれていますか？			
	決裁権限	4- 2- 1- 11	Q 決済権限を明確に定めていますか？			
	リスク別担当部門	4- 2- 1- 12	Q 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？			
4. スタッフ	スキル	4- 2- 1- 13	Q 将来必要となるスキルが識別され、教育訓練計画に反映されていますか？			
	人事計画	4- 2- 1- 14	Q IT戦略と整合の取れた人事計画が作成されていますか？			
	プロジェクト管理スキル	4- 2- 1- 15	Q スタッフのプロジェクト管理スキルは、十分ですか？			
	品質管理教育訓練	4- 2- 1- 16	Q 品質管理の教育訓練が、適切に行われていますか？			
5. 経理	投資収益方針	4- 2- 1- 17	Q 投資収益に対する方針が文書化されていますか？			
	投資決定方法	4- 2- 1- 18	Q 投資決定に際して、短期的な影響を想定していますか？			
		4- 2- 1- 18-1	Q 投資決定に際して、長期的な影響を想定していますか？			
		4- 2- 1- 18-2	Q 投資決定に際して、他部門への影響を想定していますか？			
		4- 2- 1- 18-3	Q 投資決定に際して、ビジネス上の採算を明確にしていますか？			
		4- 2- 1- 18-4	Q 投資決定に際して、利益実現の方法を明確にしていますか？			
	予定利益	4- 2- 1- 19	Q 予定利益を実現するための経営的な管理が行われていますか？			
	IT資産管理目録	4- 2- 1- 20	Q 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？			
	関連費用識別	4- 2- 1- 21	Q IT関連費用が全て識別される仕組みがありますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策				
情報システム総合企画	情報システム総合企画	4－2-(1) 情報システム総合企画				
6. 管理(文書化を含む)	全社データ管理	4- 2- 1- 22	Q 全社的なデータ管理の機能が確立されていますか？			
	全社データ標準化	4- 2- 1- 23	Q 全社的なデータの標準化が行われていますか？			
	全社データ所有者	4- 2- 1- 24	Q データの所有者が識別されていますか？			
	構成管理	4- 2- 1- 25	Q システムの構成管理は適切ですか？			
	リスク管理文書化	4- 2- 1- 26	Q リスク管理に関する情報セキュリティポリシーが文書化されていますか？			
	管理工程分割	4- 2- 1- 27	Q プロジェクト計画は、成果をチェックできるまでブレークダウンした工程分割がされていますか？			
	品質管理文書化	4- 2- 1- 28	Q 品質管理基準は文書化されていますか？			
	工程ごとの品質基準	4- 2- 1- 28- 1	Q 品質管理基準は分割された工程ごとに定めていますか？			
	ファイル管理	4- 2- 1- 29	Q ファイル管理のルールは適切ですか？			
	ライセンス管理	4- 2- 1- 30	Q ライセンス管理を行っていますか？			
	プロジェクト管理標準	4- 2- 1- 31	Q プロジェクト管理基準が、文書化されていますか？			
	方法論	4- 2- 1- 31- 1	Q 社内で基準となるシステム開発方法論が文書化されていますか？			
	IT戦略	4- 2- 1- 32	Q IT戦略が文書としてまとめられていますか？			
7. モニタリング	規制監視	4- 2- 1- 33	Q 外部規制を遵守しているかを監視する機能が存在しますか？			
	是正措置	4- 2- 1- 34	Q 必要な是正措置の実施状況が管理されていますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策				
システム開発	システム開発	4－2－(2) システム開発				
1. 一般	決裁実施基準	4- 2- 2- 1	Q 開発プロジェクトにおける決裁権限者、決裁文書等の決裁実施基準が定められていますか？			
	開発に応じた決裁	4- 2- 2- 1- 1	Q 決裁実施基準は、プロジェクトの規模に応じて定めていますか？			
	システム調達のライフサイクルにおけるセキュリティ	4- 2- 2- 2	Q システム調達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？			
	調達	4- 2- 2- 2- 1	Q 情報システムの調達において、情報セキュリティ要件を満たすための明確な実施基準を設けていますか？			
	不正防止・機密保護基準	4- 2- 2- 2- 2	Q 情報システムの開発／変更に関して、不正防止や機密保護の観点から明確な実施基準を設けていますか？			
	破棄基準	4- 2- 2- 2- 3	Q 情報システムの破棄に関して、不正防止や機密保護の観点から明確な実施基準を設けていますか？			
	品質管理	4- 2- 2- 3	Q 品質管理に関して標準的な手法を定めていますか？			
	要員	4- 2- 2- 4	Q 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？			
	職務定義	4- 2- 2- 4- 1	Q 各職務に求められる資質や職能を明確に定義していますか？			
	職務分離	4- 2- 2- 4- 2	Q 開発作業における職務分離－開発者・プログラマ・テストスタッフーを実施していますか？			
	情報セキュリティ保持の役割・責任	4- 2- 2- 4- 3	Q 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？			
	機密保持合意	4- 2- 2- 4- 4	Q 開発スタッフとの契約において機密保持に関する条項が盛り込まれていますか？			
2. プロジェクト管理	システム開発方法論	4- 2- 2- 5	Q システム開発プロジェクトにおいて標準的なシステム開発方法論を定めていますか？			
		4- 2- 2- 5- 1	Q プロジェクト開発の各工程について、その作業内容と成果物を定めていますか？			
		4- 2- 2- 5- 2	Q 各工程の開発作業に関して標準的な技法／ツールを定めていますか？			
		4- 2- 2- 5- 3	Q 各工程が完了したかの判定基準を定めていますか？			
	進捗管理手続き	4- 2- 2- 6	Q 進捗管理に関して標準的な手続きを定めていますか？			
3. システム要件定義	セキュリティ基準の遵守	4- 2- 2- 7	Q システム要件定義で、セキュリティに関する実施基準を遵守していますか？			
		4- 2- 2- 7- 1	Q 情報セキュリティポリシー／実施基準等で定められた要件を反映させていますか？			
		4- 2- 2- 7- 2	Q 管理指標に関しては、SLAとして関係者の合意が取れていますか？			
		4- 2- 2- 7- 3	Q 個人認証、暗号化等のシステム要件がシステム機能に反映されていますか？			
	システム構成要素の入手可能性	4- 2- 2- 8	Q 情報システムにあたり、システム構成要素（補修部品、消耗品）の入手可能性に関して検討を行いましたか？			
4. プログラム開発	開発環境	4- 2- 2- 9	Q 開発環境の維持、管理を適切に実施していますか？			
		4- 2- 2- 9- 1	Q システムとデータについて、機密保持のクラス分けがなされていますか？			
		4- 2- 2- 9- 2	Q プログラムライブラリへのアクセス管理は適切に行われていますか？			
		4- 2- 2- 9- 3	Q 機密性の高いプログラムの保管に関して、適切な機密保護の対策を実施していますか？			
		4- 2- 2- 9- 4	Q 設計文書の保管に関して、適切な機密保護の対策を実施していますか？			
		4- 2- 2- 9- 5	Q ウイルス等不正なソフトウェアの混入への対策を実施していますか？			
	コンプライアンス	4- 2- 2- 10	Q システム開発にあたっては、関連する法規、契約等に係わる要求事項を確認していますか？			
		4- 2- 2- 10- 1	Q 知的財産権に係わる法規、契約に係わる要求事項を確認していますか？			
		4- 2- 2- 10- 2	Q 個人情報保護に係わる法規、契約等に係わる要求事項を確認していますか？			
		4- 2- 2- 10- 3	Q 暗号等の使用に関しては輸出入管理等関連する法規等に係わる要求事項を確認していますか？			
		4- 2- 2- 10- 4	Q 国際的な情報システムを構築する場合、各国の規制（例：ECの個人情報保護規定）に遵守するべく必要な措置を講じていますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策				
システム開発	システム開発	4－2－(2) システム開発				
5. テストデータ	テストデータ	4- 2- 2- 11	Q テストデータの作成、保管は適切に実施していますか？			
		4- 2- 2- 11- 1	Q テストデータには、原則として保護すべきデータを含まないようにしていますか？			
		4- 2- 2- 11- 2	Q テストデータとして本番データを使用する場合には、適切な保護対策を実施していますか？			
		4- 2- 2- 11- 3	Q テストデータは、本番データと分離して保管していますか？			
6. 運用テスト	テスト仕様書の内容	4- 2- 2- 12	Q テスト仕様書はテストの目的に照らして適切ですか？			
	運用テストの結果	4- 2- 2- 13	Q 運用テストの結果は十分確認していますか？			
		4- 2- 2- 13- 1	Q インストールの妥当性は十分確認していますか？			
		4- 2- 2- 13- 2	Q システムの性能は十分把握していますか？？			
		4- 2- 2- 13- 3	Q システム運用上の操作性について確認していますか？			
		4- 2- 2- 13- 4	Q システム導入後の異常時のバックアップについて対応は十分ですか？			
7. 変更管理	管理責任者	4- 2- 2- 14	Q 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？			
	バージョンアップ手続き	4- 2- 2- 15	Q 本番プログラムへのバージョンアップの実施基準が明確になっていますか？			
		4- 2- 2- 15- 1	Q 本番プログラムへのバージョンアップについて、全体的な管理方針が明確になっていますか？			
		4- 2- 2- 15- 2	Q 本番プログラムへのバージョンアップについて、非常時の実施基準が明確になっていますか？			
		4- 2- 2- 15- 3	Q バックアップや他所保管の実施基準が明確になっていますか？			
	区分によるバージョンアップ	4- 2- 2- 16	Q システムの機密保持の区分により、特別のバージョンアップ手続きが定められていますか？			
	変更管理	4- 2- 2- 17	Q プログラムライブラリの変更は記録されていますか？			
	識別のための体系	4- 2- 2- 18	Q 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？			
		4- 2- 2- 18- 1	Q プログラムのネーミングルールを確立していますか？			
	高機密プログラム保管	4- 2- 2- 19	Q 機密性の高いプログラムの変更内容は、管理責任者により事前に承認を受けた上で実施されていますか？			
		4- 2- 2- 19- 1	Q 機密性の高いプログラムの変更は、本番前および本番後で独立したレビューにより検証されていますか？			
		4- 2- 2- 19- 2	Q 機密性の高いプログラム変更について、本番前および本番後のレビュー内容を文書化していますか？			
		4- 2- 2- 19- 3	Q 機密性の高いプログラム変更は管理責任者により承認されていますか？			
	作業とレビューの分離	4- 2- 2- 20	Q 機密性の高いプログラムを開発する場合、開発作業とレビューの職務の分離が行われていますか？(たとえば、設計、プログラミング、テスト)			
	アクセスの職務分離	4- 2- 2- 21	Q 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？			
	テストの機密保持規定	4- 2- 2- 22	Q 本番データをテストに使用する場合の、機密保持規定が明確化されていますか？			
	配布先でのバージョン管理	4- 2- 2- 23	Q クライアントPCにソフトウェアを配布している場合、適切なバージョン管理の 手続きが定められていますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
情報システムのリスク対策	情報システムのリスク対策	Ⅳ－2. 情報システムのリスク対策				
システム運用	システム運用	4－2－(3) システム運用				
1. システム運用	システム運用計画	4- 2- 3- 1	Q 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？			
		4- 2- 3- 1- 1	Q システム運用計画は定期的に見直されていますか？			
	システム運用	4- 2- 3- 2	Q システム運用上、システム構成管理は適切か定期的に確認していますか？			
		4- 2- 3- 2- 1	Q 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？			
		4- 2- 3- 2- 2	Q 更新された運用マニュアルに従ってシステム運用が行われていることを確認していますか？			
		4- 2- 3- 2- 3	Q 運用手順は常に適切であるか確認していますか？			
		4- 2- 3- 2- 4	Q システム運用時の各種データは常に適切であるか確認していますか？			
		4- 2- 3- 2- 5	Q システム運用に関するスタッフのスキルの妥当性について定期的に確認していますか？			
2. モニタリング機能	記録・状況把握	4- 2- 3- 3	Q システム運用関連の記録・監視は適切に行われていますか？			
		4- 2- 3- 3- 1	Q システムの資源の記録・監視は適切に行われていますか？			
		4- 2- 3- 3- 2	Q システム運用の結果(実績)に関する報告(正常終了、異常終了など)の体制は適切ですか？			
	モニタリング	4- 2- 3- 4	Q システム運用に関するモニタリングを実施していますか？			
		4- 2- 3- 4- 1	Q アプリケーションシステム自体のモニタリング機能を重視していますか？			
		4- 2- 3- 4- 2	Q システムで扱う共用データのモニタリングを実施していますか？			
		4- 2- 3- 4- 3	Q サーバやクライアント端末のモニタリングを実施していますか？			
		4- 2- 3- 4- 4	Q ネットワーク系のモニタリングを実施していますか？			
3. 管理機能	運用管理	4- 2- 3- 5	Q ファイル世代管理のリスク対策は十分行われているか定期的に確認していますか？			
		4- 2- 3- 5- 1	Q ライブラリ管理のリスク対策は十分行われているか定期的に確認していますか？			
		4- 2- 3- 5- 2	Q ファイル、データの定期的なバックアップは方針に基づいて行われていることを定期的に確認していますか？			
		4- 2- 3- 5- 3	Q 適用業務管理、(たとえば入出力データの完全性)に対するリスク対策は方針に基づいて行われていることを定期的に確認していますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
アクセス管理	アクセス管理	Ⅳ－3. 不正アクセス				
1. アクセス権管理	アクセス管理の実施基準	4- 3- 1- 1	Q アクセス管理について実施基準で定めていますか？			
		4- 3- 1- 1- 1	Q アクセス権を与える方法(IDやパスワード)を実施基準で定めていますか？			
		4- 3- 1- 1- 2	Q 社外からのダイヤルアップやインターネットからのアクセスを実施基準で定めていますか？			
		4- 3- 1- 1- 3	Q サーバ、ファイアウォール、ルータなどへの不正アクセスの防止を実施基準で定めていますか？			
		4- 3- 1- 1- 4	Q 社外との通信での重要なデータを守る方法(VPNの利用、プロバイダの暗号サービス利用など)を実施基準で定めていますか？			
		4- 3- 1- 1- 5	Q 暗号の利用を実施基準で定めていますか？			
		4- 3- 1- 1- 6	Q プロバイダの選定基準を実施基準で定めていますか？			
	アクセス権付与	4- 3- 1- 2	Q ID付与、パスワード、アクセスできる範囲に関し、実施基準を定めていますか？			
		4- 3- 1- 2- 1	Q 入退館システムを通りぬけ、組織に侵入、組織内情報システム－LAN構造、サーバ、レイアウト、指定端末、アプリケーション、データベース等－の情報が詳細に入手されることを防ぐ仕組みがありますか？			
		4- 3- 1- 2- 2	Q ID, パスワードの不正入手があった場合、その不正入手の原因はつきとめられましたか？			
		4- 3- 1- 2- 3	Q ID、パスワードの付与についてチェックやレビューのシステムがありますか？(例:ID, パスワードの付与にあたり、2人で相互牽制する仕組みを導入する等)			
		4- 3- 1- 2- 4	Q アクセス権の付与についてチェックやレビューのシステムがありますか？(例:アクセス権の付与にあたり、2人で相互牽制する仕組みを導入する等)			
		4- 3- 1- 2- 5	Q 情報システム上での、機密度のランクとアクセス制限を実施基準で定めていますか？			
		4- 3- 1- 2- 6	Q 情報システム上での、機密度のランクとアクセス制限を実施していますか？			
	教育、訓練	4- 3- 1- 3	Q ユーザにアクセス管理の実施方法や基準、概念(need to know)について教育・訓練を実施していますか？			
		4- 3- 1- 3- 1	Q 情報システム部門のスタッフに対し、不正アクセス対策についての専門的な教育・訓練を実施していますか？			
	職務分離	4- 3- 1- 4	Q データへのアクセスに対して職務の分離が行われていますか？(例: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なっていますか			
2. 論理的アクセス対策	重要なデータ保護対策	4- 3- 1- 5	Q 機密度の高いシステムとデータについて、特別の取扱いが定められていますか？(アクセス管理の実施、アクセス記録の取得とレビュー、暗号化、テスト)			
		4- 3- 1- 5- 1	Q 通信に暗号を利用していますか？			
		4- 3- 1- 5- 2	Q (改ざん防止のために)デジタル署名を利用していますか？			
		4- 3- 1- 5- 3	Q インターネット利用の場合、閉域サービスやVPNサービスを利用していますか？			
	暗合鍵管理	4- 3- 1- 6	Q 暗号鍵(公開鍵の秘密鍵や共有鍵)を適切に管理していますか？			
3. 物理的アクセス対策	携帯端末によるアクセス	4- 3- 1- 7	Q 携帯端末からのユーザ認証、アクセス管理を適切に実施していますか？			
4. 個人認証	個人認証	4- 3- 1- 8	Q 個人認証を行っていますか？			
		4- 3- 1- 8- 1	Q 入退室にあたり、パスワード、指紋・虹彩・網膜・顔形状などの確認装置等を設置して不正アクセス対策を行っていますか？			
		4- 3- 1- 8- 2	Q 声紋(音声を利用したパスワードを含む)を利用した不正アクセス対策行っていますか？			
		4- 3- 1- 8- 3	Q 筆跡(パッドに書いた文字の特徴を認識する)による不正アクセス対策を行っていますか？			
		4- 3- 1- 8- 4	Q 暗号化、ICカードメディア、等を利用して不正アクセス対策を行っていますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
アクセス管理	アクセス管理	Ⅳ－3. 不正アクセス				
5. ネットワーク中のデータ保護	ネットワークの不正アクセス対策	4- 3- 1- 9	Q ネットワークを介してのアクセスではIS、パスワードを利用していますか？			
		4- 3- 1- 9- 1	Q ネットワークを介したアクセスの場合、ID、パスワードは暗号化して転送していますか？			
		4- 3- 1- 9- 2	Q 重要なシステムなどでは、ID、パスワードを入力するにあたって、より高いセキュリティを実施していますか？（例：ICカードやワンタイムパスワード（ハード）の併用、セッション開始時に特殊なプロトコルを採用等）			
	自社ネットワークの不正アクセス対策	4- 3- 1- 10	Q 自社でネットワーク管理を行っている場合に不正アクセス対策を行っていますか？			
		4- 3- 1- 10- 1	Q ファイアウォールを設けて（フィルタリングの設定を含む）いますか？			
		4- 3- 1- 10- 2	Q WWWやメールサーバはDMZ(バリアセグメント)に設置していますか？			
		4- 3- 1- 10- 3	Q 重要なデータを保存管理するサーバはインターネットから直接アクセスできないようにしていますか？			
		4- 3- 1- 10- 4	Q 重要なデータを管理する情報システムやネットワークシステム（ファイアウォールやアクセスサーバ）にはログを残す機能がありますか？			
		4- 3- 1- 10- 5	Q 当該ログを定期的にチェック（自動で分析するツールを導入）していますか？			
		4- 3- 1- 10- 6	Q 不信なアクセスがあった場合、追跡できる機能を設けていますか？			
	外注先ネットワークの不正アクセス対策	4- 3- 1- 11	Q ネットワーク管理をアウトソーシングしている場合に不正アクセス対策を行っていますか？			
		4- 3- 1- 11- 1	Q アウトソーシング先にアクセス権を十分に説明していますか？			
		4- 3- 1- 11- 2	Q 重要なデータを保存管理するサーバはインターネットから直接アクセスできないようにしていますか？			
		4- 3- 1- 11- 4	Q 不信なアクセスがあったときにはアウトソーシング先と追跡できる機能を設けていますか？			
6. 不正検出	アクセスログ確認	4- 3- 1- 12	Q アクセスログについてアクセスの権限、権限外の記録方法について情報セキュリティ実施基準で定めていますか？			
		4- 3- 1- 12- 1	Q 機密度の高い個別情報に関して、生成、アクセス、その他の処理プロセスは、ログに残されていますか？			
		4- 3- 1- 12- 2	Q 情報のオーナーおよびシステム管理者が上記ログを定期的に確認していますか？			
7. 緊急時対応	緊急対処方法	4- 3- 1- 13	Q ハッカー、ウイルス侵入、不正アクセス等による緊急事態対処のための緊急連絡、対応方法は手続きとして定められていますか？			
	IPAへの届出	4- 3- 1- 14	Q 不正アクセスのの被害にあたりコンピュータ不正アクセス被害届出機関である情報処理振興事業協会（IPA）に被害を届け出ましたか？			
	JPCERT/CCへの相談	4- 3- 1- 15	Q 不正アクセスの被害にあたり、JPCERT／CC（コンピュータ緊急対応センター）に相談していますか？			
	外部機関への相談	4- 3- 1- 16	Q 不正アクセスの被害にあたり、関係機関や警察（サイバーポリス）に相談していますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
ウイルス関連	ウイルス関連	Ⅳ－4. コンピュータウイルス関連				
コンピュータ犯罪	コンピュータ犯罪	4－4－(1) コンピュータ犯罪				
1. パスワード	サーバ、基幹システムのパスワード変更	4- 4- 1- 1	Q 重要なデータを扱うサーバや基幹システムのパスワードを定期的に変更していますか？	[redacted]		[redacted]
	個人使用システム	4- 4- 1- 2	Q 個人が日常使用するシステム(パソコンなど)はパスワードを利用していますか？	[redacted]		
2. データ保護対策	データ伝送の情報セキュリティ対策	4- 4- 1- 3	Q データ伝送の情報セキュリティ対策について実施基準がありますか？	[redacted]		[redacted]
		4- 4- 1- 3- 1	Q 通信に暗号を利用していますか？	[redacted]		[redacted]
		4- 4- 1- 3- 2	Q (改ざん防止のために)デジタル署名を利用していますか？	[redacted]		[redacted]
		4- 4- 1- 3- 3	Q インターネットでデータを伝送する場合、閉域サービスやVPNサービスを利用していますか？	[redacted]		[redacted]
	データ保護対策	4- 4- 1- 4	Q 重要なデータの保護について、データベースに対策を講じていますか？	[redacted]		[redacted]
		4- 4- 1- 4- 1	Q 重要なデータをデータベースに記録する場合、暗号化していますか？	[redacted]		[redacted]
		4- 4- 1- 4- 2	Q 重要なデータをデータベースに記録する場合、(改ざん防止のために)デジタル署名を利用していますか？	[redacted]		[redacted]
	暗合鍵	4- 4- 1- 5	Q 暗号鍵の盗難、搾取、改ざんなどが行われないように管理していますか？	[redacted]		[redacted]
3. 盗聴対策	盗聴対策	4- 4- 1- 6	Q 盗聴対策を行っていますか？	[redacted]		[redacted]
	録音機器持込管理	4- 4- 1- 7	Q コンピュータ室への、個人のパソコンや小型デジタル録音装置(録音・記録ができる機器)の持ち込みの管理を行っていますか？	[redacted]		
	携帯電話持込	4- 4- 1- 8	Q コンピュータ室への個人の利用の携帯電話機器の持込を管理していますか？	[redacted]		
	PDA	4- 4- 1- 9	Q 個人が管理するPDAなどの会社関連の情報について重要なデータとして管理を行うよう指示を徹底していますか？	[redacted]		
	無線LAN	4- 4- 1- 10	Q 無線LANの利用においては盗聴、データ漏洩対策を行っていますか？	[redacted]		[redacted]
	電磁波漏れ	4- 4- 1- 11	Q ディスプレイの電磁波漏れなどの対策を行っていますか？	[redacted]		[redacted]

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
ウイルス関連	ウイルス関連	Ⅳ－4. コンピュータウイルス関連				
コンピュータウイルス	コンピュータウイルス	4－4－(2)コンピュータウイルス				
1. ウイルス手続き	ウイルス実施基準	4- 4- 2- 1	Q コンピュータウイルスに対する実施基準がありますか？			
2. ウイルス検出・駆除	ウイルス検出・駆除	4- 4- 2- 2	Q コンピュータウイルスを防ぐソフトウェアを用意していますか？			
		4- 4- 2- 2- 1	Q コンピュータウイルスの検出・駆除システム(メールサーバでウイルス検出する場合を含む)がありますか？			
3. 教育・訓練	スタッフの教育・訓練	4- 4- 2- 3	Q スタッフに対し、コンピュータウイルス対策に関して教育・訓練を実施していますか？			
4. ウイルス感染対策	ウイルス感染対策	4- 4- 2- 4	Q コンピュータウイルスに感染した場合の緊急連絡体制ができていますか？			
		4- 4- 2- 4- 1	Q 仕事への影響をすぐに判断できるようになっていますか？			
		4- 4- 2- 4- 2	Q すぐに情報を集め、ウイルスの感染防止や復旧など対処できるようになっていますか？			
		4- 4- 2- 4- 3	Q 感染ルートを突き止めることができますか？			
	感染の緊急時対策	4- 4- 2- 5	Q ウイルス対策を実施したにもかかわらず感染した場合に備えた緊急時の対策を有していますか？			
	感染ウイルスの転送防止	4- 4- 2- 6	Q 感染ウイルスを送付しないための対策を講じていますか(ソフトでの対策、個人のパソコン利用のモラル向上など)？			
	伝染防止対策	4- 4- 2- 7	Q ウイルスの伝染を防ぐための対策を策定していますか？			
5. 事後対策	事後対策	4- 4- 2- 8	Q ウイルス感染した場合、事後対策を講じていますか？			
		4- 4- 2- 8- 1	Q ウイルス感染に関する情報を共有していますか？			
		4- 4- 2- 8- 2	Q ウイルス感染の通知を作成し周知していますか？			
		4- 4- 2- 8- 3	Q ウイルス対策を強化(サーバの導入、ウイルス対策担当者をおくなど)していますか？			
		4- 4- 2- 8- 4	Q ウイルスが伝染しないような対策を講じていますか？			
		4- 4- 2- 8- 5	Q ウイルス駆除後のシステムの復旧対策がありますか？			
		4- 4- 2- 8- 6	Q ウイルス駆除後、再発防止対策がありますか？			
		4- 4- 2- 8- 7	Q ウイルス感染、駆除の経験は組織で共有化されていますか？			
	IPAへの届出	4- 4- 2- 9	Q コンピュータウイルス被害届出機関である情報処理振興事業協会(IPA)に被害を届け出ましたか。			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
ウイルス関連	ウイルス関連	Ⅳ－4. コンピュータウイルス関連				
E-Commerce	E-Commerce	4－4－(3)E-Commerce				
1. プライバシー保護	プライバシー保護	4- 4- 3- 1	Q インターネットでの電子商取引において利用者情報の収集についてはプライバシー保護対策を行っていますか？			
2. 不良客情報管理	不払い、不良客情報管理	4- 4- 3- 2	Q インターネットでの電子商取引での不払いなどの不良客に対する情報の管理を行っていますか？			
	不良客情報入手	4- 4- 3- 3	Q 外部からの不良客などの情報を入手していますか？			
3. データ保護対策	電子商取引時のデータ保護対策	4- 4- 3- 4	Q インターネットでの電子商取引が増えるにつれて情報が増えていきます。情報が集積されるにつれてデータの保護対策をより強化していますか？			
	インターネットからの攻撃	4- 4- 3- 5	Q インターネットからの攻撃を想定して対策を行っていますか？			
		4- 4- 3- 5- 1	Q DOS攻撃対策を行っていますか？			
		4- 4- 3- 5- 2	Q 不正侵入のアタックへの対策を行っていますか？			
		4- 4- 3- 5- 3	Q セキュリティホール対策を行っていますか？			
		4- 4- 3- 5- 4	Q ウイルス対策を行っていますか？			
4. ネットワーク機器対応	ネットワーク機器、サーバの信頼性	4- 4- 3- 6	Q 電子商取引に利用するネットワーク機器、サーバなどの信頼性(二重化) は十分ですか？			
	ネットワーク機器、サーバの性能	4- 4- 3- 7	Q 電子商取引に利用するネットワーク機器、サーバなどの性能(能力)は十分ですか？			
5. インターネット接続管理	インターネット接続の規制	4- 4- 3- 8	Q インターネットの利用について規制していますか？			
	インターネット接続機器管理	4- 4- 3- 9	Q インターネットと接続する機器の管理を行っていますか？			
		4- 4- 3- 9- 1	Q ファイアーウォールの管理(性能、情報セキュリティ、ログ)を行っていますか？			
		4- 4- 3- 9- 2	Q DNS(設置されている場合)の管理を行っていますか？			
		4- 4- 3- 9- 3	Q ユーザ情報や購入情報などの転送にあたって、暗号を利用し、その暗号鍵の管理、デジタル署名を管理していますか？			
		4- 4- 3- 9- 4	Q ビジネスに対するリスク(利益保護、賠償額の低減、信用の保護等)の対策を行っていますか？			
		4- 4- 3- 9- 5	Q 利用者への詐欺行為を監視(チェック)していますか？			
6. 電子的証拠	デジタル署名	4- 4- 3- 10	Q 改ざん防止が必要な場合、デジタル署名を利用していますか？			
	時刻証明	4- 4- 3- 11	Q 時刻などの証明が必要な場合、時刻の証明を利用していますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
ウイルス関連	ウイルス関連	Ⅳ－4. コンピュータウイルス関連				
電子メール	電子メール	4－4－(4)電子メール				
1. 管理	電子メールの実施基準	4- 4- 4- 1	Q 社内に電子メールの実施基準(ユーザの利用基準を含む)がありますか？			
	プライバシー保護	4- 4- 4- 2	Q インターネットでの電子メールのプライバシー保護対策を行っていますか？			
2. メールサーバ管理	メールサーバのデータ保護対策	4- 4- 4- 3	Q メールサーバはデータの改ざんから保護されていますか？			
	メールサーバへの攻撃	4- 4- 4- 4	Q スパム攻撃を想定して対策を行っていますか？			
		4- 4- 4- 4- 1	Q DOS攻撃対策を行っていますか？			
		4- 4- 4- 4- 2	Q 不正アクセス対策がとられていますか？			
		4- 4- 4- 4- 3	Q セキュリティホール対策を行っていますか？			
		4- 4- 4- 4- 4	Q ウイルス対策を行っていますか？			
		4- 4- 4- 4- 5	Q 不正を招くおそれのあるメール転送を禁止していますか(例:社外経由で自社メールを転送するなど)？			
3. ネットワーク機器管理	ネットワーク機器、サーバの信頼性	4- 4- 4- 5	Q 電子メールのネットワーク機器、サーバの信頼性は十分にありますか？			
	ネットワーク機器、サーバの性能	4- 4- 4- 6	Q 電子メールのネットワーク機器、サーバなどの性能(能力、記憶容量)は十分にありますか？			
4. インターネット接続機器管理	インターネット接続機器管理	4- 4- 4- 7	Q インターネットと接続する機器の管理を行っていますか？			
		4- 4- 4- 7- 1	Q ファイアーウォールの管理(性能、情報セキュリティ、ログ)を行っていますか？			
		4- 4- 4- 7- 2	Q DNS(設置している場合)の管理を行っていますか？			
		4- 4- 4- 7- 3	Q 暗号の利用と暗号鍵の管理、デジタル署名の管理を行っていますか？			
		4- 4- 4- 7- 4	Q ビジネスに対するリスク(利益保護、賠償額の低減、信用の保護等の)対策を行っていますか？			
		4- 4- 4- 7- 5	Q 利用者への不正行為を監視(チェック)していますか？			
5. デジタル署名	デジタル署名	4- 4- 4- 8	Q 改ざん防止が必要な場合、デジタル署名を利用していますか？			
6. 悪質メール対策	添付ファイル	4- 4- 4- 9	Q 添付ファイルによる悪意のあるプログラムを阻止する対策がありますか？			
	スクリプト	4- 4- 4- 10	Q メールと共に送られてくる不正スクリプトを防止する対策がありますか？			
	不正メール対策	4- 4- 4- 11	Q 送信元のないメールや悪意のあるメールを防止する対策がありますか？			
7. 転送エラー対策	転送エラー	4- 4- 4- 12	Q 電子メールの不用意な転送エラーによる重要な情報の漏洩対策を行っていますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
災害対策	災害対策	Ⅳ－5. 災害対策				
1. 管理	経営者の決定	4- 5- 1- 1	Q 災害リスク対策を採用するか否かにつき経営者が決定していますか？			
		4- 5- 1- 1- 1	Q 火災リスク対策を検討していますか？			
		4- 5- 1- 1- 2	Q 地震リスク対策を検討していますか？			
		4- 5- 1- 1- 3	Q 浸水リスク対策を検討していますか？			
	緊急事態対応計画	4- 5- 1- 2	Q 災害発生時の緊急事態対応計画を作成していますか？			
	災害復旧レベル	4- 5- 1- 3	Q 災害復旧のレベルに関してあらかじめ段階的に決められていますか？			
		4- 5- 1- 3- 1	Q 事業再開のための最低限のレベルを決めていますか？			
		4- 5- 1- 3- 2	Q 災害復旧にあたり、平常時に必要な水準レベルを決めていますか？			
		4- 5- 1- 3- 3	Q 復旧にあたり、災害以前以上の改善レベルを決めていますか？			
	是正措置	4- 5- 1- 4	Q 復旧手順について不具合があった場合、是正処置をとっていますか？			
	避難対策	4- 5- 1- 5	Q 経営者、スタッフの避難対策を実施していますか？			
2. 防火対策	防火壁	4- 5- 1- 6	Q 防火壁を採用していますか？			
		4- 5- 1- 6- 1	Q コンピュータ室に防火壁を採用していますか？			
		4- 5- 1- 6- 2	Q データ保管場所に防火壁を採用していますか？			
		4- 5- 1- 6- 3	Q ネットワーク設備室に防火壁を採用していますか？			
		4- 5- 1- 6- 4	Q コンピュータ設置場所に防火壁を採用していますか？			
	自動消火装置	4- 5- 1- 7	Q 自動消火装置を設置していますか？			
		4- 5- 1- 7- 1	Q コンピュータ室に自動消火装置を設置していますか？			
		4- 5- 1- 7- 2	Q データ保管場所に自動消火装置を設置していますか？			
		4- 5- 1- 7- 3	Q ネットワーク設備室に自動消火装置を設置していますか？			
		4- 5- 1- 7- 4	Q コンピュータ設置場所に自動消火装置を設置していますか？			
	区画放出対応消火システム	4- 5- 1- 8	Q 区画放出対応消火システムを採用していますか？			
		4- 5- 1- 8- 1	Q コンピュータ室に区画放出対応消火システムを採用していますか？			
		4- 5- 1- 8- 2	Q データ保管場所に区画放出対応消火システムを採用していますか？			
		4- 5- 1- 8- 3	Q ネットワーク設備室に区画放出対応消火システムを採用していますか？			
	消火器	4- 5- 1- 9	Q 消火器を設置していますか？			
		4- 5- 1- 9- 1	Q コンピュータ室に消火器を設置していますか？			
		4- 5- 1- 9- 2	Q データ保管場所に消火器を設置していますか？			
		4- 5- 1- 9- 3	Q ネットワーク設備室に消火器を設置していますか？			
		4- 5- 1- 9- 4	Q コンピュータ設置場所に消火器を設置していますか？			
	消火栓	4- 5- 1- 10	Q 消火栓を設置していますか？			
		4- 5- 1- 10-1	Q コンピュータ室に消火栓を設置していますか？			
		4- 5- 1- 10-2	Q データ保管場所に消火栓を設置していますか？			
		4- 5- 1- 10-3	Q ネットワーク設備室に消火栓を設置していますか？			
		4- 5- 1- 10-4	Q コンピュータ設置場所に消火栓を設置していますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
災害対策	災害対策	Ⅳ－5. 災害対策				
2. 防火対策	遮断装置	4- 5- 1- 11	Q 遮断装置を設置していますか？	[redacted]		[redacted]
		4- 5- 1- 11-1	Q コンピュータ室遮断装置を設置していますか？			
		4- 5- 1- 11-2	Q データ保管場所遮断装置を設置していますか？			
		4- 5- 1- 11-3	Q ネットワーク設備室遮断装置を設置していますか？			
		4- 5- 1- 11-4	Q コンピュータ設置場所遮断装置を設置していますか？			
	2方向非常口	4- 5- 1- 12	Q 経営者、スタッフの避難対策として2方向非常口を設置していますか？			
3. 耐震対策	コンピュータ室の耐震対策	4- 5- 1- 13	Q コンピュータ室ではフリーアクセスの耐震補強を実施していますか？			
		4- 5- 1- 14	Q コンピュータ室では耐震対策としてコンピュータ機器の固定をしていますか？			
		4- 5- 1- 15	Q コンピュータ室では耐震対策としてコンピュータ機器の転倒防止をしていますか？			
	データ保管場所の耐震対策	4- 5- 1- 16	Q データ保管場所では耐震対策として機器およびラックの固定をしていますか？			
		4- 5- 1- 17	Q データ保管場所では耐震対策としてテープ等の落下防止策をとっていますか？			
	コンピュータ設置場所の耐震対策	4- 5- 1- 18	Q コンピュータ設置場所では耐震対策として機器の落下防止策をとっていますか？			
	電源設備の耐震対策	4- 5- 1- 19	Q 電源設備の耐震対策として機器の転倒防止、固定をしていますか？			
4. 水害対策	コンピュータ室の浸水対策	4- 5- 1- 20	Q コンピュータ室の浸水対策として浸水の恐れのない場所への設置をしていますか？			
		4- 5- 1- 21	Q コンピュータ室の浸水対策として上げ床の実施をしていますか？			
		4- 5- 1- 22	Q コンピュータ室の浸水対策として防水堤およびピットの設置をしていますか？			
		4- 5- 1- 23	Q コンピュータ室の浸水対策として漏水検知機の設置をしていますか？			
		4- 5- 1- 24	Q コンピュータ室の浸水対策として排水口を設置していますか？			
	基幹システムの漏水対策	4- 5- 1- 25	Q 基幹コンピュータシステムに対する漏水対策として天井配管から水落下の恐れのない場所への設置をしていますか？			
		4- 5- 1- 26	Q 基幹コンピュータシステムに対する漏水対策として窓からの雨水の吹き込みの恐れのない場所へ機器を設置していますか？			
		4- 5- 1- 27	Q 基幹コンピュータシステムに対する漏水対策として防水シートの準備をしていますか？			
	電源設備の水害対策	4- 5- 1- 28	Q 電源設備の水害対策として防水堤の設置をしていますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
障害対策	障害対策	Ⅳ－6. 障害対策				
1. 管理	SLA	4- 6- 1- 1	Q 障害対策に関してSLAを取り決めていますか？			
	ポリシーとの整合性	4- 6- 1- 1- 1	Q SLAで取り決めた内容は、情報セキュリティポリシーの要件を満たしていますか？			
	管理責任者の承認	4- 6- 1- 1- 2	Q SLAで示された内容に関して、アプリケーションの管理責任者の承認を得ていますか？			
	トランザクション量	4- 6- 1- 1- 3	Q SLAでシステムへ入力するトランザクション量が示されていますか？			
	緊急事態対応計画	4- 6- 1- 2	Q 障害発生時の緊急事態対応計画を作成していますか？			
	復旧手順	4- 6- 1- 3	Q 復旧手順についての文書を定めていますか？			
		4- 6- 1- 3- 1	Q 緊急事態発生後の復旧処理に関する経営者およびスタッフの役割が明確になっていますか？			
		4- 6- 1- 3- 2	Q 障害復旧のレベルを定めていますか？			
		4- 6- 1- 3- 3	Q 必要な場合の代替手段を講じていますか？			
	是正措置	4- 6- 1- 4	Q 復旧手順について不具合があった場合、是正処置をとっていますか？			
2. 手続き	ソフトウェア更新手続き	4- 6- 1- 5	Q 障害対策として、ソフトウェアの更新手続きが示されていますか？			
	緊急時対応手続き	4- 6- 1- 6	Q 緊急時対応手続きが明確になっていますか？			
		4- 6- 1- 6- 1	Q 機器障害発生時における縮退・再編成の際の適用業務の優先順位を決めていますか？			
		4- 6- 1- 6- 2	Q すべての障害についての障害管理票の作成要領を定めていますか？			
	携帯端末紛失連絡体制	4- 6- 1- 7	Q 携帯端末を紛失した場合の連絡体制、アクセス禁止等の手続きは明確に示されていますか？			
	代替バックアップ対策	4- 6- 1- 8	Q 復旧計画には代替手段によるバックアップが示されていますか？			
	ソフトウェア更新手続き	4- 6- 1- 9	Q ソフトウェアの更新手続きについて明確になっていますか？			
		4- 6- 1- 9- 1	Q アプリケーションの管理責任者が最終テスト結果を確認していますか？			
		4- 6- 1- 9- 2	Q すべての更新記録を整備していますか？			
		4- 6- 1- 9- 3	Q 更新記録と許可内容を一致させる手順を明確にしていますか？			
	変更後障害	4- 6- 1- 10	Q プログラム変更後に障害が発生した時に、変更前のプログラムに戻す手続きが文書化されていますか？			
	SLAトランザクション量	4- 6- 1- 11	Q SLAで示されたシステムへ入力するトランザクション量は、定期的に測定を行い結果を記録していますか？			
	更新確認	4- 6- 1- 12	Q ソフトウェアの更新について、手続きどおりに実施されているか定期的な確認が行われていますか？			
	ソフトウェア更新	4- 6- 1- 13	Q ソフトウェアの更新手続きについての各項目は、その妥当性について定期的に評価し、不具合の是正処置をとっていますか？			
	切り替えテスト	4- 6- 1- 14	Q バックアップ機器への切り替えテストが実施され、その結果の評価が行われていますか？			
3. 情報システム	障害対策機能	4- 6- 1- 15	Q セキュリティマネジメントポリシーを満たすべく情報システムの障害対策機能を実施していますか？			
		4- 6- 1- 15- 1	Q 運用監視機能を設置していますか？			
		4- 6- 1- 15- 2	Q 障害検出機能を設置していますか？			
		4- 6- 1- 15- 3	Q 縮退運転機能を設置していますか？			
		4- 6- 1- 15- 4	Q 代替運転機能を設置していますか？			
		4- 6- 1- 15- 5	Q 回復機能を設置していますか？			
	ディスク障害対策	4- 6- 1- 16	Q ディスク障害対策として、重要なディスクドライブは冗長な構成が取られていますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
障害対策	障害対策	Ⅳ－6. 障害対策				
4. ユーティリティ	施設障害対策	4- 6- 1- 17	Q 施設の障害対策を講じていますか？	[redacted]		[redacted]
	電源設備	4- 6- 1- 17-1	Q 主要な機器の電源は無停電装置（含む自家発電装置）から供給されていますか？			
		4- 6- 1- 17-2	Q 設置した無停電装置（含む自家発電装置）は定期的にテストが行われていますか？			
		4- 6- 1- 17-3	Q 無停電装置の供給能力は、計画された拡張も含む機器構成に対して十分ですか？			
	空調設備	4- 6- 1- 17-4	Q 空調設備は、室内設備および屋外設備ともに多重化がされていますか？			
		4- 6- 1- 17-5	Q 空調設備の電源は、無停電装置から供給されていますか？			
		4- 6- 1- 17-6	Q 空調設備が水冷の場合、水冷用の予備水を確保していますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
アウトソーシング	アウトソーシング	Ⅳ－7. アウトソーシング関連リスク対策 (ここでのアウトソーシングは、システム開発やデータセンタや分散環境の運用を外部に委託することを指します。アウトソーシング契約には、契約本文と作業内容を定める附属文書等を含みます。)				
1. 目的	外注	4- 7- 1- 1	Q アウトソーシングについて、明確な情報セキュリティポリシーがありますか？			
		4- 7- 1- 2	Q アウトソーシングについて、TCOを認識したマネジメントコントロールが確立されていますか？			
	コスト削減	4- 7- 1- 3	Q 情報システムに関わるコストの削減がアウトソーシングの目的となっていますか？			
		4- 7- 1- 4	Q システム部門のスリム化がアウトソーシングの目的となっていますか？			
		4- 7- 1- 5	Q 関連技術の安価な利用がアウトソーシングの目的となっていますか？			
		4- 7- 1- 6	Q コスト削減に通じる技術の専門化、高度化がアウトソーシングの目的となっていますか？			
2. 役割分担	役割分担	4- 7- 1- 7	Q 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？			
		4- 7- 1- 8	Q アウトソーシング契約で、受託者の作業(業務内容、範囲、スケジュール)は明確になっていますか？			
	作業内容	4- 7- 1- 9	Q 受託者の作業(業務内容、範囲、スケジュール)は明確になっていますか？			
		4- 7- 1- 10	Q 委託者の作業(業務内容、範囲、スケジュール)は明確になっていますか？			
3. プロジェクト管理	プロジェクト管理手法	4- 7- 1- 11	Q アウトソーシングした場合の、プロジェクト管理手法が、明確化されていますか？			
	共通開発方法論	4- 7- 1- 12	Q 開発方法論について、両者で共通のものを用いていますか？			
	外注委託のレビュー	4- 7- 1- 13	Q 委託業務の実施内容をレビューしていますか？			
	会議体	4- 7- 1- 14	Q アウトソーシング契約に、両者で交わす文書や会議について、定められていますか？			
4. アウトソーサー管理	選定評価基準	4- 7- 1- 15	Q アウトソーサの選定手続きと評価基準が、社内で定められていますか？			
	SLA	4- 7- 1- 16	Q アウトソーシング契約に、SLA(サービスレベル合意)を含んでいますか？			
		4- 7- 1- 17	Q SLAが守れなかった場合のペナルティが定められていますか？			
	運用障害時対応	4- 7- 1- 18	Q アウトソーシング契約に、運用障害時の対応(体制、手続き)が定められていますか？			
	ソフトウェア障害時対応	4- 7- 1- 19	Q ソフトウェア障害時の対応(体制、手続き)が定められていますか？			
	品質管理	4- 7- 1- 20	Q 委託作業の品質管理について、体制や手続きが定められていますか？			
5. 契約	委託契約ルール	4- 7- 1- 21	Q 委託契約ルールが定められていますか？			
	賠償上限	4- 7- 1- 22	Q アウトソーシング契約で、賠償責任の上限が定められていますか？			
	海外委託	4- 7- 1- 23	Q 海外の事業者に委託する場合、各国の輸出入管理規制に遵守するべく必要な措置を講じていますか？			
	開発納期延期	4- 7- 1- 24	Q 委託契約で、開発納期が遅延した場合のペナルティが定められていますか？			
	ソフトウェア瑕疵担保	4- 7- 1- 25	Q ソフトウェア瑕疵担保について定められていますか？			
	契約監査	4- 7- 1- 26	Q 委託契約が定められた委託契約ルールに基づいて締結していることを監査していますか？			
	変更手続き	4- 7- 1- 27	Q 契約内容の変更手続き(作業、契約、システム)が定められていますか？			
6. 知的財産権	秘密保持	4- 7- 1- 28	Q アウトソーシング契約に、受託者の守秘義務と秘密保持手段が含まれていますか？			
		4- 7- 1- 29	Q アウトソーシング契約で、再委託を許す場合は、委託者と同様の守秘義務と秘密保持手段が含まれるようになっていますか？			
	再委託	4- 7- 1- 30	Q 再委託を許す場合は、委託者と同様の守秘義務と秘密保持手段が含まれるようになっていますか？			
	知的財産権	4- 7- 1- 31	Q 委託契約で、委託先との間で知的財産権を明確にしていますか？			
	知的財産権侵害	4- 7- 1- 32	Q 第三者の知的財産権の侵害があった時の、責任分担が明確になっていますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
アウトソーシング	アウトソーシング	Ⅳ－7. アウトソーシング関連リスク対策				
7. セキュリティ上の留意点	委託先情報セキュリティ	4- 7- 1- 33	Q 委託契約に、不正防止、機密保護等の対策を盛り込んでいますか？	[redacted]		[redacted]
		4- 7- 1- 34	Q 委託先における不正防止、機密保護等の対策の実施状況を把握し、必要な措置を講じていますか？			
		4- 7- 1- 35	Q 発注者の情報セキュリティポリシーと実施基準を遵守することが、要件に含まれていますか？			
	受託者のシステムのセキュリティ対策	4- 7- 1- 36	Q 受託者のシステムのセキュリティを確保しているか？			
		4- 7- 1- 36-1	Q 受託者にアクセス権について十分に説明していますか？			
		4- 7- 1- 36-2	Q 委託者の重要なデータを保存管理するサーバはインターネットから直接アクセスできないようにしていますか？			
		4- 7- 1- 36-3	Q 委託者の重要なデータを管理する情報システムやネットワークシステムのログを定期的に報告していますか？			
		4- 7- 1- 36-4	Q 受託者から報告されたログやログ分析の結果を定期的にチェックしていますか？			
		4- 7- 1- 36-5	Q 受託者が不倡なアクセスを受けたときに、追跡できる機能を設けていますか？			
	不正防止、機密保持、破棄	4- 7- 1- 37	Q 受託者の情報システムの開発／変更に関して、不正防止や機密保護の観点から明確な基準を設けていますか？			
		4- 7- 1- 38	Q 受託者の情報システムの破棄に関して、不正防止や機密保護の観点から明確な基準を設けていますか？			
	機密区分	4- 7- 1- 39	Q 受託者のシステムとデータについて、機密保持のクラス分けがなされていますか？			
	形態に応じた保全対策	4- 7- 1- 40	Q 委託者の開発のアウトソーシングは、その形態に応じて情報保全の対策を講じていますか？			
		4- 7- 1- 41	Q 委託者開発のアウトソーシング形態に応じた情報保全対策は契約に反映されていますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
その他	その他	Ⅳ－8. その他関連項目				
1. テロおよび人命損失	テロ	4- 8- 1- 1	Q テロリスクの対策を採用するか否かにつき経営者が決定していますか？			
		4- 8- 1- 1- 1	Q テロリスクについてのリスク分析の結果、対応策を講じていますか？	■		
		4- 8- 1- 1- 2	Q 自社への脅迫やトラブル事例を分析の結果、対応策を講じていますか？	■		
		4- 8- 1- 1- 3	Q テロ対策として巡回警備を実施していますか？	■		
		4- 8- 1- 1- 4	Q テロ対策として用紙保管庫に納品物を24時間以上寝かせる対策をとっていますか？	■		■
		4- 8- 1- 1- 5	Q テロ対策としてシステムセンタや帳票センタの納品物に対して金属探知器をかけていますか？	■		■
		4- 8- 1- 1- 6	Q テロ対策としてさまざまなホームページに掲載される誹謗中傷の調査把握分析を実施していますか？	■		■
	人命損失	4- 8- 1- 2	Q 人命損失リスクの対策を採用するか否かにつき経営者および責任者が決定していますか？			
		4- 8- 1- 2- 1	Q 人命損失リスクについて、リスク評価：頻度および経営に与える影響度分析の結果、対策を講じていますか？			
		4- 8- 1- 2- 2	Q 経営者、スタッフの避難対策（避難訓練、2方向非常口設置）は実施されていますか？	■		
2. サービス提供	会員規約	4- 8- 1- 3	Q サービス提供にあたり利用者の会員規約を定めていますか？	■		
	規約違反	4- 8- 1- 4	Q サービス提供の停止となる規約違反事項を明確にし、会員に説明していますか？	■		
	通信の秘密保護教育	4- 8- 1- 5	Q サービス提供の実務に携わっている管理者に対し、「通信の秘密保護（電気通信事業法第4条）について教育を行っていますか？	■		
3. ユーザ間トラブル	ユーザ間トラブル	4- 8- 1- 6	Q ユーザ間トラブルリスクの対策を採用するか否かにつき経営者が決定していますか？			
		4- 8- 1- 6- 1	Q ユーザ間トラブルリスクについての分析の結果、対策を講じていますか？	■		■
		4- 8- 1- 6- 2	Q 会員が提供しているサービスを利用して違法行為を行った場合について事前にシナリオを作成し、サービス提供企業（自社）の法的責任および事後対応について検討していますか？ ［なお、ここにいう規約違反行為に該当するものとしては①誹謗中傷意見の掲載、②著作権違反、③誇大広告（消費者保護を含む）④事業妨害などがありメールサービス、ホームページ提供、ショッピグモール、広告掲載などサービスの内容で関与の度合いに応じて様々な法的責任を有しうる。］	■		■
		4- 8- 1- 6- 3	Q 会員間で提供しているサービスの利用の結果トラブルが発生した場合について事前にシナリオを作成し、サービス提供企業（自社）の法的責任および事後対応について対象を定めていますか？	■		■
	SLA	4- 8- 1- 7	Q SLA（サービスレベル合意）が整備されていますか？	■		
4. 苦情処理対応	苦情処理対応	4- 8- 1- 8	Q 苦情処理対応トラブルリスクの対策を採用するか否かにつき経営者および責任者が決定していますか？			
		4- 8- 1- 8- 1	Q 苦情処理対応におけるトラブルリスクについて分析の結果、対策を講じていますか？	■		
		4- 8- 1- 8- 2	Q サービス提供に対する苦情処理対応マネジメントシステムを導入していますか？			
5. リスク対策手順整備	その他リスク対策手順整備	4- 8- 1- 9	Q その他（テロ等）のリスクについて包括したリスク対策手順を整備していますか？			
		4- 8- 1- 9- 1	Q アプリケーションシステムの運用手順が整備されていますか？			
		4- 8- 1- 9- 2	Q 緊急時対応手続きが整備されていますか？			
		4- 8- 1- 9- 3	Q 復旧手順が整備されていますか？			
6. 危機管理計画徹底	危機管理計画の内外関係者への徹底	4- 8- 1- 10	Q 危機管理計画は、資産の喪失・破壊に関してユーザ、アウトソーサも含め関係者に周知徹底されていますか？			
		4- 8- 1- 10-1	Q 物的資産の喪失・破壊に関してユーザ、アウトソーサを含め関係者に周知徹底されていますか？	■		
		4- 8- 1- 10-2	Q 情報資産の喪失・破壊に関してユーザ、アウトソーサを含め関係者に周知徹底されていますか？	■		
		4- 8- 1- 10-3	Q その他の資産の喪失・破壊に関してユーザ、アウトソーサを含め関係者に周知徹底されていますか？	■		
7. 危機管理計画時間軸	危機管理計画の時間軸別対応	4- 8- 1- 11	Q 危機管理について時間軸別に対策を策定していますか？			
		4- 8- 1- 11-1	Q 緊急事態発生前の対策を策定していますか？	■		
		4- 8- 1- 11-2	Q 緊急事態発生時の対策を策定していますか？	■		
		4- 8- 1- 11-3	Q 緊急事態発生後の対策を策定していますか？	■		

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
その他	その他	Ⅳ－8. その他関連項目				
8. 移動体データ保護	移動体内臓データ保護	4- 8- 1- 12	Q （論理的アクセスの視点から、）携帯のパソコンを使っている場合、内蔵しているデータ(会社の重要なデータ)の保護策としてアクセス制御や暗号の利用などを行っていますか？	[redacted]		[redacted]
		4- 8- 1- 12-1	Q 接続方式については、リスクを考慮して適切な方式を選定していますか？	[redacted]		[redacted]
		4- 8- 1- 12-2	Q 直接会社のネットワークに接続していますか？	[redacted]		[redacted]
		4- 8- 1- 12-3	Q 直接ネットワークに接続している場合、呼び返し方式を利用していますか？	[redacted]		[redacted]
		4- 8- 1- 12-4	Q 直接ネットワークに接続している場合、ワンタイムパスワードを利用していますか？	[redacted]		[redacted]

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
バックアップ	バックアップ	Ⅳ－9. バックアップ				
1. 二重化対策	二重化対策	4- 9- 1- 1	Q 情報システムのバックアップ対策を実施していますか？(ここでいうバックアップは二世代保存を含む)			
		4- 9- 1- 1- 1	Q 交換機、チャネルの二重化を行っていますか？			
		4- 9- 1- 1- 2	Q 機器の二重化を行っていますか？			
		4- 9- 1- 1- 3	Q LANの二重化を行っていますか？			
		4- 9- 1- 1- 4	Q WANの二重化を行っていますか？			
	電源設備	4- 9- 1- 1- 5	Q 主要な機器の電源は無停電装置(含む自家発電装置)から供給されていますか？			
		4- 9- 1- 1- 6	Q 設置した無停電装置(含む自家発電装置)は定期的にテストが行われていますか？			
		4- 9- 1- 1- 7	Q 無停電装置の供給能力は、計画された拡張も含む機器構成に対して十分ですか？			
	空調設備	4- 9- 1- 1- 8	Q 空調設備は、室内設備および屋外設備ともに多重化がされていますか？			
		4- 9- 1- 1- 9	Q 空調設備の電源は、無停電装置から供給されていますか？			
2. ファイルのバックアップ	プログラムバックアップ	4- 9- 1- 2	Q プログラムのバックアップを行っていますか？			
		4- 9- 1- 2- 1	Q プログラムファイルバックアップの実施基準は明確ですか(バックアップ頻度、バックアップ取得方法、保管場所)？			
		4- 9- 1- 2- 2	Q プログラムファイルバックアップの遠隔地保管を行っていますか？			
		4- 9- 1- 2- 3	Q プログラムファイルバックアップの同一サイト内保管を行っていますか？			
	OSファイルバックアップ	4- 9- 1- 3	Q OSファイルのバックアップを行っていますか？			
		4- 9- 1- 3- 1	Q OSファイルバックアップの実施基準は明確ですか(バックアップ頻度、バックアップ取得方法、保管場所)？			
		4- 9- 1- 3- 2	Q OSファイルバックアップの遠隔地保管を行っていますか？			
		4- 9- 1- 3- 3	Q OSファイルバックアップの同一サイト内保管を行っていますか？			
	データファイルバックアップ	4- 9- 1- 4	Q データファイルのバックアップを行っていますか？			
		4- 9- 1- 4- 1	Q データファイルバックアップの実施基準は明確ですか(バックアップ頻度、バックアップ取得方法、保管場所)？			
		4- 9- 1- 4- 2	Q データファイルはリアルタイムで遠隔地ミラーデータを作成していますか？			
		4- 9- 1- 4- 3	Q データファイルバックアップの遠隔地保管を行っていますか？			
		4- 9- 1- 4- 4	Q データファイルバックアップの同一サイト内保管を行っていますか？			
		4- 9- 1- 4- 5	Q データの保存期間について実施基準がありますか？(DB／OSファイル)			
		4- 9- 1- 4- 6	Q 機能停止許容時間内に、復旧ができる頻度でバックアップを実施していますか？			
3. DBファイルのバックアップ	DBファイルバックアップ	4- 9- 1- 5	Q DBファイルのバックアップを行っていますか？			
		4- 9- 1- 5- 1	Q DBファイルバックアップの実施基準は明確ですか(バックアップ頻度、バックアップ取得方法、保管場所)？			
		4- 9- 1- 5- 2	Q DBファイルはリアルタイムで遠隔地ミラーDBを作成していますか？			
		4- 9- 1- 5- 3	Q DBファイルバックアップの遠隔地保管を行っていますか？			
		4- 9- 1- 5- 4	Q DBファイルバックアップの同一サイト内保存を行っていますか？			
		4- 9- 1- 5- 5	Q ボリューム単位でバックアップを取得している場合、必要なボリュームはすべて対象となっていますか？			
		4- 9- 1- 5- 6	Q ボリューム単位でバックアップを取得している場合、災害時用に同一モデルのディスクを確保していますか？			
		4- 9- 1- 5- 7	Q DBMSのログは、定期的にバックアップされていますか？			
		4- 9- 1- 5- 8	Q DBMSのログは、データベース本体と別のディスクを使用していますか？			
4. ネットワーク対策	回線・ネットワーク対策	4- 9- 1- 6	Q 回線障害対策を実施していますか？			
		4- 9- 1- 6- 1	Q 代替回線を確保していますか？			
		4- 9- 1- 6- 2	Q 交換機に避雷器を設置していますか？			
		4- 9- 1- 7	Q ネットワーク障害対策を実施していますか？			
		4- 9- 1- 7- 1	Q 代替機を準備していますか？			
		4- 9- 1- 7- 2	Q 手作業による代替手段を準備していますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
バックアップ	バックアップ	Ⅳ－9. バックアップ				
5. 予備サイト	予備サイト設置	4- 9- 1- 8	Q 情報システムの予備サイトを設置していますか？	[redacted]		[redacted]
		4- 9- 1- 8- 1	Q 同一コンピュータ室内にバックアップ用のコンピュータを設置していますか？			
		4- 9- 1- 8- 2	Q 同一建物内の別室にバックアップ用のコンピュータを設置していますか？			
		4- 9- 1- 8- 3	Q 情報喪失に備えて、平時からのバックアップセンタが準備されていますか？			
		4- 9- 1- 8- 4	Q 遠隔地にバックアップセンタを設置していますか？			
		4- 9- 1- 8- 5	Q バックアップサービス業者と契約していますか？			
		4- 9- 1- 8- 6	Q 同種コンピュータのユーザと相互バックアップ契約を締結していますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
緊急時対策	緊急時対策	Ⅳ－10. 緊急時対策				
1. 事前対応	事前対応	4-10- 1- 1	Q リスクマネジメントの緊急時対応は事前に備えられていますか？			
		4-10- 1- 1- 1	Q 機密漏洩に対する緊急時対応は事前に備えられていますか？			
		4-10- 1- 1- 2	Q 不正アクセスに対する緊急時対応は事前に備えられていますか？			
		4-10- 1- 1- 3	Q マクロウイルスに対する緊急時対応は事前に備えられていますか？			
		4-10- 1- 1- 4	Q 自然災害に対する緊急時対応は事前に備えられていますか？			
		4-10- 1- 1- 5	Q アウトソース先の倒産による緊急事態に備えていますか？			
		4-10- 1- 1- 6	Q 各種法令侵害に対する緊急時対応は事前に備えられていますか？			
		4-10- 1- 1- 7	Q バックアップに対する緊急時対応は事前に備えられていますか？			
		4-10- 1- 1- 8	Q その他ファシリティの移動が必要な事態に対する緊急時対応は事前に備えられていますか？			
	緊急時対応の訓練	4-10- 1- 2	Q 緊急事態発生時の対応についてスタッフに対して情報セキュリティの面から定期的に訓練を行っていますか？			
2. 緊急時対応手続き	緊急時対応手続きの明確化	4-10- 1- 3	Q 緊急時対応手続きについて明確になっていますか？			
		4-10- 1- 3- 1	Q 緊急連絡網を整備していますか？			
		4-10- 1- 3- 2	Q 緊急時の対応体制を明確にしていますか？			
		4-10- 1- 3- 3	Q 緊急時の代替対応手順を明確にしていますか？			
		4-10- 1- 3- 4	Q 発生した障害について、解決までの業務をフローチャート化していますか？			
		4-10- 1- 3- 5	Q 緊急事態を想定した教育訓練計画を作成していますか？			
		4-10- 1- 3- 6	Q 緊急時対策本部の組織と物理的な設定基準はあらかじめ定められていますか？			
		4-10- 1- 3- 7	Q 情報資産に関する緊急事態の判定基準は明確ですか？			
		4-10- 1- 3- 8	Q 緊急事態宣言（シナリオ）と通知方法は事前に決められていますか？			
		4-10- 1- 3- 9	Q 情報資産固有の緊急事態対応手順はあらかじめ定められていますか？			
		4-10- 1- 3- 10	Q 不審・異常ログの発見とシステム管理者への通報手順があらかじめ定められていますか？			
		4-10- 1- 3- 11	Q システム遮断、ユーザへの緊急サービス停止などのバックアップ手順があらかじめ定められていますか？			
		4-10- 1- 3- 12	Q 機器障害発生時における縮退・再編成の際の適用業務の優先順位を決めていますか？			
		4-10- 1- 3- 13	Q 障害切り分けのために必要な設備を整備していますか？			
		4-10- 1- 3- 14	Q ネットワークを含むシステム全体の運用監視で、障害発生時に運用スタッフに知らせることのできるアラーム等を整備していますか？			
		4-10- 1- 3- 15	Q すべての障害についての障害管理票の作成要領を定めていますか？			
	定期的評価、是正改善	4-10- 1- 4	Q 緊急時のリスク対応について不具合があった場合、是正処置をとっていますか？			
3. 復旧計画	復旧計画	4-10- 1- 5	Q 復旧計画は、詳細な手続きが定められていますか？			
		4-10- 1- 5- 1	Q 主幹システム、重要ビジネスプロセスごとの、復旧のオーナ、支援のためのシステム管理者、その他の支援スタッフを決めていますか？			
		4-10- 1- 5- 2	Q 代替手段によるバックアップ実施を決定していますか？			
		4-10- 1- 5- 3	Q 計画の維持、テストのためのスケジュールを決定していますか？			

キーワード	キーワード	識別コード	質問項目	回答欄		
				経営者層	IS部門	ユーザ
リスク対策	リスク対策	Ⅳ. JRMSにおけるリスク対策				
リスクファイナンス	リスクファイナンス	Ⅳ－11. リスクファイナンス				
1. リスクファイナンスの役割	リスク分析	4-11- 1- 1	Q リスク分析に基づきリスクファイナンスの必要性を確認していますか？			
	マニュアル	4-11- 1- 2	Q リスクファイナンスについての実施基準はありますか？			
	責任者決定	4-11- 1- 3	Q リスクファイナンスについて最高経営者により責任者が決められていますか？			
	責任者の役割・権限	4-11- 1- 4	Q 全体のリスクマネジメントにおいてリスクファイナンスについて責任者の役割・権限は明確ですか？			
2. リスクファイナンスの対象領域	対象領域	4-11- 1- 5	Q リスクファイナンスの対象領域をリスクの点から分けていますか？			
		4-11- 1- 5- 1	Q リスクファイナンスの対象領域を明確にしていますか？			
		4-11- 1- 5- 2	Q 対象領域を海外、または国内／海外とした場合、リスクファイナンスの責任者の役割を地域別に明確にしていますか？			
3. ファイナンスのリスク区分	ファイナンスのリスク区分	4-11- 1- 6	Q リスクファイナンスに関わるリスク区分を明確にしていますか？			
		4-11- 1- 6- 1	Q 経営リスクを明確にしていますか？			
		4-11- 1- 6- 2	Q 資産リスクを明確にしていますか？			
		4-11- 1- 6- 3	Q 資産運用リスクを明確にしていますか？			
		4-11- 1- 6- 4	Q 信用リスクを明確にしていますか？			
		4-11- 1- 6- 5	Q 為替変動リスクを明確にしていますか？			
		4-11- 1- 6- 6	Q 関連会社リスクを明確にしていますか？			
		4-11- 1- 6- 7	Q オフバランス取引リスクを明確にしていますか？			
		4-11- 1- 6- 8	Q 保険リスクを明確にしていますか？			
		4-11- 1- 6- 9	Q カントリーリスクを明確にしていますか？			
		4-11- 1- 6- 10	Q その他（　　）リスクを明確にしていますか？			
	管理不能リスクの明確化	4-11- 1- 7	Q リスク対策を実施してもコントロールできないリスクを明確にしていますか？			
4. 財務的対応	財務的判断基準	4-11- 1- 8	Q リスクファイナンスのための財務的なリスク分析により定められた判断基準を定めていますか？			
	財務的対応	4-11- 1- 9	Q リスクコントロールで対処できないリスクへの財務的対応を策定していますか？			
	あらかじめの算定	4-11- 1- 10	Q リスクファイナンスの対策をあらかじめ策定していますか？			
		4-11- 1- 10-1	Q コンピュータ総合保険に加入にしていますか？			
		4-11- 1- 10-2	Q 利益保険に加入していますか？			
		4-11- 1- 10-3	Q 賠償責任保険に加入していますか？			
		4-11- 1- 10-4	Q コンピュータ機器の保険に加入していますか？			
		4-11- 1- 10-5	Q 金融デリヴァティヴ・ボンドの利用を考慮していますか？			
		4-11- 1- 10-6	Q 保有しているリスクは定められた範囲内としていますか？			
		4-11- 1- 10-7	Q ARTの利用を考慮していますか？			
	リスクファイナンス見直し	4-11- 1- 11	Q 定期的にリスクファイナンスの見直しを行っていますか？			
	実施関連部署間の協議	4-11- 1- 12	Q リスクファイナンス実施のため、他の部署の責任者と協議していますか？			
5. 外部コンサルタント活用	外部コンサルタント活用	4-11- 1- 13	Q リスクファイナンス実施にあたり、必要に応じ外部の専門家（コンサルタント）を利用していますか？			
6. リスク対応のための組み合わせ	リスク対応のための各種方法組み合わせ	4-11- 1- 14	Q リスク対応のため、リスクファイナンスとリスクコントロールの各種の方法との組合せを実施していますか？			
	リスクファイナンス成果評価基準	4-11- 1- 15	Q リスクファイナンスの成果の評価基準を持っていますか？			

参考資料
情報セキュリティ関連のＵＲＬ

（順不同）

・内閣（ＩＴ政策）　http://www.kantei.go.jp/jp/it/index.html
・経済産業省（ＭＥＴＩ／）　http://www.meti.go.jp
・警視庁（ＮＰＡ）　http://www.npa.go.jp/
・総務省（MHA）　http://www.mha.go.jp/
・日本工業標準調査会（ＪＩＳＣ）　http://www.jisc.org/
・情報処理振興事業協会（ＩＰＡ）　http://www.ipa.go.jp
・(財) 日本情報処理開発協会（ＪＩＰＤＥＣ）　http://www.jipdec.or.jp
・コンピュータ緊急対応センター（ＪＰＣＥＲＴ／ＣＣ）
　http://www.jpcert.or.jp/
・(財) 日本規格協会（ＪＳＡ）　http://www.jsa.or.jp
・(財) 金融情報システムセンター（ＦＩＳＣ）　http://www.fisc.or.jp
・(社) 情報サービス産業協会（ＪＩＳＡ）　http://www.jisa.or.jp
・システム監査学会（ＪＳＳＡ）　http://www.sysaudit.gr.jp
・情報システム・コントロール協会（ＩＳＡＣＡ）
　東京支部　http://www.isaca.gr.jp/homepage_j.htm
　大阪支部　http://www.isaca-osaka.org/
・日本システム監査人協会（ＳＡＡＬ）　http://www.saaj.or.jp

・British Standards Institution（ＢＳＩ）
　http://www.bsi-global.com/group.html
・National Institute of Standards and Technology（ＮＩＳＴ）
　http://www.nist.gov/
・NIST SP 800-12, An Introduction to Computer Society
　http://csrc.nist.gov/publications/nistpubs/800-12 のサイトを参照
・The CERT® Coordination Center （ＣＥＲＴ／ＣＣ）
　http://www.cert.org/
・Computer Operations, Audit, and Security Technology
　http://www.cerias.purdue.edu/coast/coast.html
・Federal Government's Chief Information Officers(CIO) Council.
　http://bsp.cio.gov/
・Forum of Incident Response and Security Teams
　http://www.first.org/
・"The Information Systems Audit and Control Association & Foundation"
　http://www.isaca.org/isacafx.htm
・Internet Security Systems (ISS) Corporate
　http://www.iss.net/

・IT Governance Institute

http://www.ITgovernance.org/index2.htm

・The Risk and Insurance Management Society, Inc. （ＲＩＭＳ）

http://www.rims.org/

・Risk Management Magazine

http://www.rmmag.com/

・The SANS (System Administration, Networking, and Security) Institute

http://www.sans.org/newlook/home.htm

・TruSecure® Corporation （旧ＩＣＳＡ社）

http://www.trusecure.com/

平成14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)９３８７

印刷所　株式会社　美　行　企　画
東京都千代田区神田錦町2丁目5番地
鈴木第2ビル　2Ｆ
ＴＥＬ　03(3219)２９７１