リスクシナリオに基づくシステムリスク評価手法の提案

"Risk Quantification and Application for Risk Management
- scenario-based system risk analysis for life insurance companies -"

ＩＴ研究会第５グループ

＜担当委員＞

三好　　肇　（アクサ生命）

佐川　健一　（朝日生命）

＜メンバー＞

戸田　　徹　（ソニー生命）

岩上　祐二　（三井生命）

青波　久恵　（アクサ生命）

定廣　和典　（ＧＥエジソン生命）

佐藤　浩一　（マニュライフ生命）

増田　明久　（明治生命）

松本　典子　（アイエヌジー生命）

劉　　新江　（アメリカンファミリー生命）

若本　正雄　（太陽生命）

渡部　　亘　（ＪＡ共済連）

＜目次＞

はじめに

今や情報システムは企業の根幹を支えるライフラインとして重要な位置付けを占めている。業務の効率化、情報の共有化、利便性の高いサービス提供を可能にする優れた情報システムは、それ自体が企業の重要な競争力である。一方、情報システムの重要性が高まるにつれて、情報システムが停止・誤作動した場合のビジネスへのインパクトも急速に増大している。特に公共的な役割を担う金融・保険業においては、情報システムの停止・誤作動とそれに起因する業務活動の混乱が社会に対して大きな影響をもたらす危険性を秘めており、システムリスクの適切な管理は、企業にとって重要な経営課題であるだけでなく、企業の範疇を超えた社会的な要請でもある。

適切なリスク管理を行うには、相応の経営資源を投入する必要があるが、保険業界は、長引く不況による保有契約の伸び悩み、資産運用環境の悪化による逆ざや問題といった重い経営課題を抱えており、年々巨大化するシステム投資に対して、各社とも及び腰になっているのが実状である。急速に増大するシステムリスクと厳しいコスト競争の中で、最小限の投資で最大のリスク低減効果をあげることが至上命題となっている。

最小限の投資で最大の効果を得るためには、「どのシステムに、どの程度のリスクが存在するのか？」「リスク対策投資は何を優先すべきか？」を知る必要がある。また、投資効果をチェックするためには、リスク対策によってどれだけ効果があがったのか、それはコストに見合っていたのかを事後的に検証するプロセスも必要になる。しかし、従来行われてきた定性的な観点でのリスク評価では、この種の疑問に対して明快な答えを出せない。こうした疑問に答えるためには、様々な業務プロセスのどこにどれだけのリスクがあるのかを洗い出し、そのリスクがどれほどの損失可能性を秘めているのかを定量的に評価する必要がある。

本稿では、この問題の解決策として、リスクシナリオに基づくリスク評価手法を提案し、実務における具体的な適用と、その活用方法について事例を挙げながら解説する。

I. 保険会社を取巻く環境の変化

ＩＴの浸透と金融自由化の進展を背景に、ここ数年、保険会社を取り巻く環境は大きく変化している。本章では、保険会社のビジネススタイルの変化と情報システムを取り巻く環境について概説し、環境変化に伴うシステムリスク管理の標準化動向をみていく。

１．ビジネススタイルの変化

（１）インターネット取引の拡大

インターネットの普及に伴い、保険業界においても、一部商品のダイレクト販売や既契約者向けのインターネットサービス等、インターネットを活用した顧客へのサービス提供は拡大する傾向にある。インターネット取引は、スピーディで利便性の高いサービスを顧客に提供できるが、一方では、不正アクセスによるＷｅｂサイトの改ざん、第三者によるなりすまし・盗聴、ウィルス、メール誤配信による情報漏洩といった新たなリスクが増大している。

（２）業務のペーパーレス化・キャッシュレス化

情報通信技術（ＩＴ）を活用した業務プロセスの構築によって、業務のペーパーレス化・キャッシュレス化が進められた。紙や現金という物理的な制約から解放されたことで、業務効率は飛躍的に高まったが、その反面、データ化されたことで情報の持ち出し等が容易になり、情報漏洩等のリスクが増大している。

（３）携帯端末の普及

生命保険業界においては、携帯端末（ＰＣ）を利用した訪問販売が一般的になった。このため、盗難等によりＰＣのハードディスクに記録された顧客情報等の機密情報が社外に流出するリスクが高まっている。

（４）取扱商品・販売チャネルの多様化

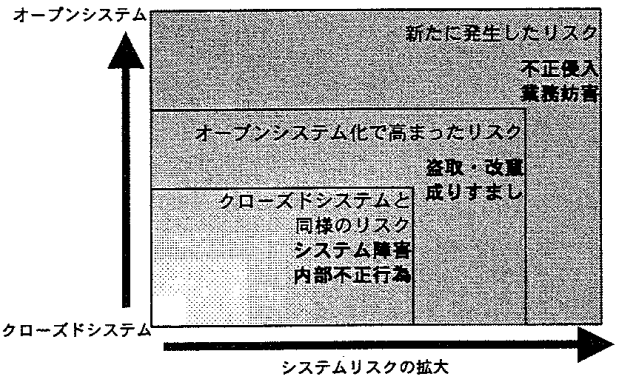
金融自由化を背景に、投資信託や確定拠出型年金（日本版４０１ｋ）といった保険以外の商品販売や他業種とのクロスセリングが行われるようになった。これにより、自社外のシステム・事務との連携が強まっており、顧客情報漏洩や他社のシステム障害等、外部に起因するトラブルの発生リスクが高まっている。

2．　情報システムを取巻く環境の変化

（1）オープンシステム化

従来、保険会社のシステムは、ユーザーを限定したクローズドシステムが主流であったが、インターネットの普及に伴い、ユーザーを限定しないオープンなプラットフォームが導入されてきた。このため、なりすましや盗聴によるリスクが増大し、不正アクセスによる業務妨害等の新たなリスクに対応する必要が出てきた。

また、２４時間３６５日のサービス供給を売り物にしたインターネットサービスは、従来のサービスよりも高いレベルの可用性が求められる。



図Ｉ－１．オープンプラットフォームとリスクの拡大

（2）アウトソーシング化

コスト削減とサービスレベルの向上という、相反する問題を解決する手段としてアウトソーシングが注目されている。情報システムの運用・開発においてもアウトソーシングが進んでいるが、アウトソーシングによるリスクとして、システムがブラックボックス化して自社で制御できなくなるリスクや委託先の倒産といった事態も考慮する必要がある。情報セキュリティの対象である情報システム資産が直接的な管理下にないために、業務委託後のモニタリングを念頭においたリスク管理体制を構築する必要がある。

（3）経営統合の活発化

システム統合を伴う銀行や保険会社等の経営統合が、合併や持株会社化によって進んでおり、これに伴って大小さまざまなシステム障害が発生している。特に今年に入って発生した大手都市銀行での大規模なシステム障害は、社会問題にまで発展したため、事態を重くみた金融庁は、システム統合の準備不足に起因するオペレーションミス、システムのダウン・誤作動によって顧客および統合金融機関が損失を被るリスクをシステム統合リスクとして定義し、検査強化の方針を打ち出した。

（4）システムリスク管理への関心の高まり

システムリスクの複雑化・多様化を背景に、ＩＴガバナンスへの関心が高まっており、その一環としてシステムリスク管理の重要性が今まで以上に注目されるようになった。監督官庁による金融検査も、従来の現物検査からシステムリスク管理の有効性を検証するプロセス検査へと変化してきた。また、その有効性を対外的に証明する手段として情報セキュリティ

管理システム（Information Security Management System（ISMS））認証が注目されており、アウトソーシング先の選定基準として利用されている他、一部金融機関で認証取得する動きも出ている。

3．リスク管理の標準化動向

システムリスク管理への関心の高まりを背景にリスク管理の標準化手法が、さまざまな団体から提唱されるようになってきた。それに伴い、一般的なシステムリスク管理の手法（リスク管理サイクル）が確立されてきた。ここでは昨今注目されているＢＳ７７９９と代表的なリスク分析手法について紹介する。

（1）システムリスクとは

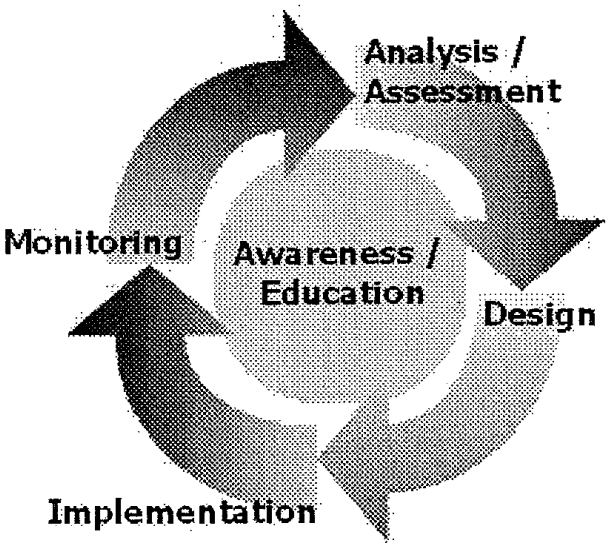
a．システムリスクの定義

システムリスクは様々な定義があるが、本稿では金融庁の「保険会社に係わる検査マニュアル」の定義を採用する。

「システムリスクとは、コンピュータシステムのダウン又は誤作動等、システムの不備等に伴い保険会社が損失を被るリスク、さらにコンピュータが不正に使用されることにより保険会社が損失を被るリスクである」

b．システムリスク管理の基本コンセプト

システムリスク管理は、大きく分けて「分析／評価」、「計画」、「実施」、「監視」の４つのフェーズからなり、「分析」から「監視」までの到達を１サイクルとして捉え、サイクルを繰り返すことで、よりレベルの高いリスク管理を行うことが可能となる。



図Ｉ－２．リスクマネジメントサイクルのイメージ

c．ＢＳ７７９９

ＢＳ７７９９はＢＳＩ（British Standard Institute）によって作成されたものであり、パート１およびパート２の２つのパートから構成されている。パート１は、ＩＴセキュリティ管理実施基準で、情報処理システムのセキュリティを確保するために必要なセキュリティ管理対策を規定している。パート２は、パート１に基づく評価・認定スキームを実現するために１９９８年に作成・発表されており、組織の情報セキュリティ管

理・運用体制全体を意味するＩＳＭＳの内容、策定手順、管理方法を解説するものである。２０００年にＩＳＯ標準となったのは、パート１の部分である。

（２）リスク分析手法

ａ．リスク分析手法とそのアプローチ

システムリスク分析は、大きく「定量分析」と「定性分析」の２つに分類される。

定量分析は、リスクの大きさを金額などの具体的な数値で計る手法である。数値化することにより、対策費用の妥当性や経営判断の補足資料として有効である。

定性分析は、機密性、可用性、完全性といったリスクの性質に着目し、数段階のリスクレベルを設定して大まかなランク付けを行う方法が一般的である。

ｂ．代表的なリスク分析手法

イ．「情報セキュリティポリシーに関するガイドライン」

内閣安全保障・危機管理室情報セキュリティ対策推進室が発表したもので、機密性・完全性・可用性の３つの側面から情報資産の重要性を調査する。各情報資産別に脅威の発生頻度と発生時の被害の大きさを測る事を目的とした定性分析手法である。

ロ．ＪＲＡＭ（JIPDEC Risk Analysis Method）

日本情報処理開発協会（JIPDEC）が１９９２年に発表ＪＲＡＭ質問表を使用する。脆弱性を分析し、実際に発生した損失額と合わせてリスク分析を行う定量分析と定性分析を併せた手法である。

ハ．ＣＲＡＭＭ（CCTA Risk Analysis Management Methodology）

英国大蔵省（CCTA）と英国規格協会（BSI）が１９８８年に発表したもので、ＣＲＡＭＭ質問表を元に定量分析と定性分析を併せて分析する。その後、提供された対策事項から必要な対策を選択する手法である。

ニ．ＡＬＥ（Annual Loss Exposure）

米国立標準・技術院が1977年に発表したもので、発生頻度と損失額をあらかじめ算出する定量分析手法である。$ＡＬＥ＝１０^{(f+i)／3}$の式に基づく。

それぞれＡＬＥ＝年間予想損失額、ｆ＝損失評価額のレベル、ｉ＝発生頻度のレベルを表す。

ホ．その他

上記手法の他に、以下のような手法も広く利用されている。

① ＧＭＩＴＳ（Guidelines for the Management of IT Security）
② マリオン法
③ メリッサ法
④ モンテカルロシミュレーション

II. 各社のシステム管理の取組み状況

第Ⅰ章では、保険会社を取り巻く環境の変化によるシステムリスクの複雑化・多様化について述べた。本章では、情報処理振興事業協会（ＩＰＡ）の実施した平成１３年度の「情報セキュリティに関する調査」※を基に、各社のシステム管理の取組みに関しての傾向を分析する。また、本研究グループ各社で独自に行ったアンケート結果を基に生保各社のリスク管理状況をみていく。

１．　システムリスク管理の現状

（１）システムダウンの発生状況

過去一年間で、運用上影響のあるシステムダウンが発生したかという問いに対しては過半数（５４．１％）の企業で発生しているという結果が出ている。システムダウンの原因としては、「ハードウェア障害」（２２０件）や「ネットワーク障害」（１６１件）、「ソフトウェア障害」（１２８件）が多く挙げられたが、「オペレーションミス」、「ウィルス」、「通信事業者に起因する障害」等も原因となっており、障害の原因は多岐にわたっている。

表Ⅱ－１．過去１年間に発生した運用上影響のあるシステムダウンの件数

内訳	件数	割合(%)
全体的にダウン	65	9.1
部分的にダウン	323	45.0
しない	327	45.5
無回答	3	0.4

（２）システムリスクの顕在化による影響

約７割の企業が、システム関連のリスクは倒産に結びつく可能性があると考えている。

表Ⅱ－２．システム関連のリスクが倒産に結びつくと思うか？

倒産との関連性	件数	割合(%)
思う	86	12.0
重大な影響は受けると思う	402	56.0
重大な影響は受けない	99	13.8
わからない	102	14.2
無回答	29	4.0

※「情報セキュリティに関する調査」－わが国の情報セキュリティの現状および意識を把握すること等を目的として、財団法人日本情報処理開発協会(JIPDEC)が、平成13年10月29日から12月26日にかけて4，000の事業体の情報システム部門を対象に実施した調査である。回収数は718件で、回答事業体の平均従業員数は2，198人である。調査項目は情報セキュリティ管理一般について(9項目)や情報リスクマネジメント関連について(9項目)など89項目の質問から構成される。

（3）リスク分析の実施状況

多くの企業が、システム関連のリスクは倒産に結びつく可能性があると考えているにも関わらず、約8割に当たる571社がリスク分析を行っていない。リスク分析を実施しない理由としては、分析手法や分析による効果がわからないことが挙げられている。

表Ⅱ－3．リスク分析をしない理由

リスク分析をしない理由	件数	割合(%)
重要性を感じていない	76	13.3
手法がわからない	273	47.8
予算がない	51	26.4
発生被害額が算出できない	137	24
リスク分析の意味がわからない	54	9.5
効果がわからない	178	31.2
効果があるとは思えない	35	6.1
無回答	27	4.7

以上の調査結果から、各社ともシステムリスク管理の重要性は認識しているものの、ノウハウがなく、効果が明確に見えないために、リスク管理の起点となるリスク分析が十分に行われていないことが分かる。

2．　生保各社におけるシステムリスク分析の取り組み

次に当研究グループに参加している各社に対して実施したアンケートを基に生保各社のリスク分析の取り組み状況をみていく。

（1）リスク分析の現状

各社においてリスク分析は行われているが、多くの会社では、定性分析が中心となっており、システムリスクを定量的に把握できていない。

表Ⅱ－4．どのようなリスク分析を行っているか

システムリスク分析の形式	割合(%)
定性的分析のみ	66.7
一部定量的分析を行なっているが、定性的分析が中心	22.2
一部定性的分析を行なっているが、定量的管分析が中	0.0
定量的分析のみ	0.0
無回答	11.1
計	100.0

表Ⅱ－5．システムリスクの定量分析実施状況について

システムリスクの定量分析実施	割合(%)
実現できている	11.1
一部実現できているが、まだ不十分	11.1
実現できていない	77.8
計	100.0

（2）定量分析の必要性

現状ではリスクの定量分析はほとんど実施されていないが、将来展望を含め、多くの会社がその必要性を感じている。リスク対策投資に関する判断材料、投資効果を客観的に評価する基準としてリスク定量分析の潜在ニーズは高いことがわかる。

表Ⅱ－6．情報セキュリティに関する調査

システムリスクの定量分析の必要性	割合（%）
必要	55.6
現在はあまり必要でないが、今後は必要になる	44.4
今後も必要ではない	0.0
無回答	0.0
計	100.0

III. システムリスク管理が抱える課題

第Ⅰ章で述べたように、システムリスクの多様化・複雑化を背景にリスク管理の必要性を多くの企業が認識し、理論的に確立されたリスク分析手法も提唱されている。しかし、第Ⅱ章でみてきたように、実際にはノウハウがなく効果も見えないリスク分析に対して企業は苦慮しており、自社のシステムリスクを十分に把握できていない。生命保険業界でもリスク分析は行われているものの、定性分析が中心であり、リスクを定量的に把握できていない。

本章では、システムリスクの把握が不十分なこと、リスクを定量的に把握できていないことによって生じる問題について考察し、解決の方向性を提示する。

1．システムリスクの把握が不十分なことによって生じる問題

企業が自社のシステムリスクを把握できないことによって生じる最大の問題は、経営に重大な影響を与えるリスクを制御できなくなることである。業務のシステム依存が高まっている今日、あらゆるビジネスプロセスにシステムリスクが潜在しており、いつ顕在化しても不思議ではない。特に、保険会社のように公共性の高い業種においては、リスクの顕在化によって社会的に大きな影響を及ぼす危険性を秘めているため、システムリスクの適切な管理は、企業の範疇を超えた社会的な要請といえる。

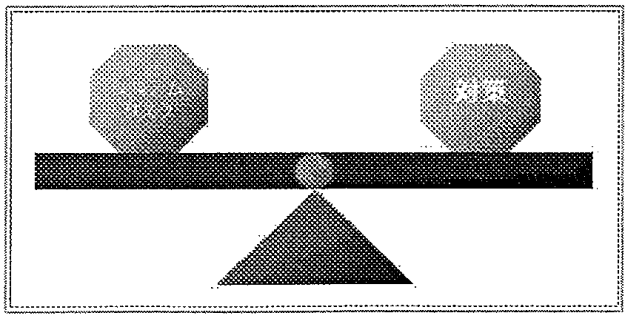
2．定量的なリスク把握ができないことによって生じる問題

（1）効果的なリスク対策が策定できない

第1の問題は、定性分析のみでは効果的なリスク対策の策定が難しいという点である。定性分析ではリスクを大まかに捉え、全体を把握することは可能である。しかしながら、大まかにリスクを捉えるだけでは、「何をどこまでやるか」といったリスク量とその対応策との間に齟齬が生じるため、効果的なリスク対策の策定ができなくなる。緻密で効果的なリスク対策を策定するためには、定量的なリスク把握が欠かせない。

（2）リスク対策への投資判断が困難

第2の問題は、定量的な裏付がないことにより、予測されるリスクに対処する必要性についての、説得力に欠ける点である。経営者は利益を拡大するＩＴ投資には積極的であるが、収益改善に直接貢献せず、投資効果がはっきりしない情報セキュリティ対策には、消極的になりがちである。この点、どの



図Ⅲ－1．システムリスクと対策費のバランス

程度の対策を取れば良いかの定量的な裏付があれば、経営判断を下す際に有効である。

3．解決策の考察

（1）実践的なリスク分析手法の必要性

第Ⅱ章でみてきたように、システムリスクの重要性を認識しながらも、「実際問題として、どのように手をつければ良いのか分からない」という声が多い。世間では様々なリスク分析手法が提唱されているが、実務に導入するとなると、「リスク分析のプロセスが分かりづらい」、「妥当な分析（評価）結果が得られない」、「分析に際して膨大な作業負荷がかかる」といった問題に直面してしまう。つまり、実務での使用に耐え得るようなリスク分析手法が存在しないことが根本的な問題であり、これらの問題を解決する実践的なリスク分析手法が求められている。

（2）定量的なリスク分析手法の必要性

また、上記2（2）で問題点としてあげたように、効果的なリスク対策を策定し、リスク対策の投資判断を可能とするためには、リスクを定量的に分析・評価する手法が必要になる。

以上の考察の結果、システムリスク管理における問題の解決策として以下の条件を満たすリスク分析（評価）法が有効であると考える。次章以降では、今までの考察を踏まえて、実務で使える実践的なリスク分析（評価）手法を提案する。

＜リスク分析（評価）手法の条件＞

a．リスク評価に至る分析のプロセスが分かり易いこと
b．妥当な分析結果（評価）が得られること
c．リスク分析に多大な作業負荷を要しないこと
d．定量的なリスク評価ができること

なお、一般的に「リスク分析手法」と「リスク評価手法」は、類似した意味で使われることが多いが、本稿では、リスク分析を経てリスク評価を行う手法という意味で、以後は「リスク評価手法」という呼称に統一する。

IV. リスク評価手法の提案

本章では、第Ⅲ章までの考察を踏まえた上で、私たちが提案する実践的なリスク評価手法について説明する。

1．リスク評価のプロセス

私たちが提案するリスク評価手法は、業務におけるリスク発生のシナリオを想定し、リスク発生によるインパクト（損失・影響）と発生可能性からシナリオごとのリスクを評価する。具体的には、以下の評価プロセスにそってリスク評価を行う。

（1）リスクシナリオの洗い出し

情報システムを利用した様々な業務で発生しうるリスクシナリオを洗い出す。

（2）リスクの定量分析

全てのリスクシナリオに対してリスクが顕在化した場合のビジネスインパクトを分析し、損失額が算出可能か否かを判断する。損失額が算出可能であれば定量評価を行う。

（3）リスク定量評価

a．過去の障害発生実績等を基にビジネスインパクトとリスクの発生頻度を算出する。

b．aを基に各シナリオのリスク量（期待損失額）を算出する。
年間期待損失額　＝　ビジネスインパクト　×　発生頻度

（4）リスク定性評価

a．リスク定性評価は全てのリスクシナリオについて行う。リスク定性評価では、リスクの性質に着目し、「可用性」、「機密性」、「完全性」のいずれかにリスク区分して定性的な観点でのリスクレベルを評価する。

b．リスク軽減策の実施状況を評価し、最終的な残余リスクを判定する。

2．評価プロセスの解説

以下では、上記1で挙げた各評価プロセスについて詳細解説する。

（1）リスクシナリオの洗い出し

リスク評価を行う前に、どのようなリスクが存在しているかを知るために、リスク管理部門の取りまとめの下、まずリスクシナリオの洗出しを行う。担当業務によって生じやすいリスクへの認識の偏りを最小限にするために、リスクの洗い出しは情報システム部門とシステムユーザー部門と共同で行う必要がある。

また、洗い出したシナリオは「リスク調査シート」に記入する。下記の表Ⅳ－１は、リスクの起因という側面から洗出しを行う「リスク調査シート」の例である。

表Ⅳ－１．リスク調査シート

起因			事象	リスク評価				対策費
大分類	中分類	小分類		ビジネスインパクト	発生確率	定量	定性	
内部に起因	アプリケーション	プログラミング						
	運用 ハードウェア	ハード障害						
	ネットワーク	ネットワーク障害						
	その他	運用ミス						
	その他	入力データ不良等						
外部に起因	災害 テロ 外部からのデータのバグ							

（２）リスクの定量分析

全てのリスクシナリオに対してリスクシナリオが顕在化した場合のビジネスインパクトを分析し、損失額が算出可能か否かを判断する。ここで、リスク顕在化による損失額が算出可能であれば、次の評価プロセスとして定量評価を行うが、風評リスクのように損失が金額換算に適さないものは定量評価を行わない。

例えば、顧客に送付する案内状の内容が間違っていたというシナリオの損害額には次のような項目が含まれる。

- 顧客からのクレーム処理費用（電話対応等の人件費・通信費）
- システムのバグ対応費用
- 追加案内の郵便費用　等

（３）リスク定量評価

シナリオ間のリスク比較ができるよう各シナリオについて年間期待損失額（１年間に被るであろう損失額）を算出する。

年間期待損失額〔単位：円／年〕　＝　**ビジネスインパクト　×　発生頻度**

ビジネスインパクト　＝　リスク発生に伴う損失を金額換算したもの〔単位：円／回〕

発生頻度　＝　年間発生頻度　〔単位：回／年〕

ａ．リスクシナリオの規模設定

リスクシナリオを描く上でインパクトを左右する重要な決め事の１つは、障害の発生量である。例えば、ある障害によるエラーが１００件発生した場合と１０，０００件発生した場合ではインパクトは大きく違ってくる。とは言え、同じ障害について発生量を色々設定していたのでは、非効率である上パターンも無限にあるので不可能である。

そこで、当研究においては発生量の規模について統一の基準を次のとおり設けることにした。

バッチ系　　：　年間処理件数の０．５％

オンライン系　　：　システムダウン１日（１日のサービス時間を９時間とする）

b．ビジネスインパクトの算出

イ．発生実績のあるリスクシナリオ

システム障害発生時は、通常障害報告書を作成しており、大まかな影響度の記録は残している。そこで、既に発生記録のある事象については、記録を基に事後処理に要した費用に加え要員・時間から割出した人件費、機会損失額（逸失利益）等を参考にして、リスクシナリオの発生時のビジネスインパクトを算定する。

作成日　年　月　日

システム障害報告書

システム区分			
処理区分(業務名)			
発生・復旧(修復)日時	発生		復旧(修復)
障害内容			
影響(インパクト)	量(件数・時間)	範囲	損失
発見の経緯	発見者		
初期対応(復旧・修復)	コスト		
再発防止策	コスト		

図Ⅳ－１．システム障害報告書

ロ．発生実績のないリスクシナリオ

過去に発生実績のないリスクについては、情報システム部門およびユーザー部門へのインタビュー・アンケート等を実施することで想定されるビジネスインパクトを算出する。特にリスク発生によって直接影響を受けるユーザーは影響度（損失）についての情報を豊富に持っているため協力が欠かせない。

作成日　年　月　日

システム障害による影響調査票

システム区分		
処理区分(業務名)		
ユーザー部門名		(部・課・支社・営業所)
設定障害内容		
設定障害の程度	量(件数・時間)	範囲
想定される影響(インパクト)		
ユーザー対応による想定コスト		

図Ⅳ－２．システム障害による影響調査票

ハ．ビジネスインパクトの算出基準

リスクシナリオから損失額を算定する場合、何を損失額に含めるかは算定者の主観に左右されやすく金額に大きな差を招きやすい。そこで、損失額の算定に際しては、大まかな基準となるビジネスインパクト分類表を使うことで算定者の主観の入る余地を最低限に抑える必要がある。（図Ⅳ－３参照）

分類	リスク発生に伴う損失例	損失費用	算出方法(推定)
直接損失	社内事後処理対応(システム誤処理発生時)	人件費換算相当分	職種別時間単価を基に対応時間で概算
	社内代替処理対応(システムダウン時)		
	障害修復(社内)		
	事後処理・代替処理に伴う外部委託	外部発注費用	外部発注費用全額
	システム障害に対する損害賠償等対応	損害賠償・裁判費用	損害額については請求額ではなく支払確定額
	障害修復(社内)	人件費換算相当分	職種別時間単価を基に対応時間で概算
	障害修復(委託、機材・部品購入等)	機材等購入・修復委託費用	外部発注・購入費用全額
逸失利益	システムダウン等による営業活動の停滞	人件費換算相当分	直近数ヶ月の平均給与を基に算出

図Ⅳ－３．ビジネスインパクト分類表

c．リスク発生頻度の算出

イ．過去３年間に発生実績のあるリスク

過去３年間に発生実績のあるリスクの場合、発生頻度はリスクシナリオで設定した障害規模（基準損失）が年間何回発生したかを示す値となる。

＜バッチ系＞

設定障害規模（エラー量）　＝　年間アウトプット件数の０．５％

発生頻度　＝　年間エラー発生件数　÷　年間アウトプット件数の０．５％

＜オンライン・基盤系＞

設定障害規模（システム停止時間）　＝　９時間（１日のサービス提供時間）

発生頻度　＝　年間停止時間　÷　９時間（１日のサービス提供時間）

〔算定例〕

●障害事例：１，２００件のエラーが過去３年間に４回発生した場合

（年間処理件数：１００万件）

エラーの年平均発生回数は、４／３＝１．３３［回／年］

①１年間のエラー発生件数：　１，２００　×　４　÷　３

＝　１，６００［件／年］

②リスクシナリオで基準とするエラー：　１００万件　×　０．５％

＝　５，０００［件／回］

③：　①　÷　②　＝　１，６００　÷　５，０００　＝　０．３２

基準エラー量に対する年間発生頻度は、０．３２［回／年］

ロ．過去３年間に発生実績のないリスク

過去３年間に発生実績のないリスクについては、要因別に以下の３手法で年間発生頻度を算定する。

①手法１－アプリケーションのバグ等の場合

システム規模による推計（工数比例）

→　エラー発生実績のあるシステム工数から工数比例で算定する。

②手法２－事故・災害等外的要因が根本原因の場合

外的要因自体（地震、落雷、火災等）の発生頻度

→　システムダウン、ネットワーク障害等の原因が事故・災害にある場合は、事故・災害自体の発生頻度を適用する。

③手法３－その他（手法１、２に非該当）

類似事象推察法による推計

→　同程度のシステムサービスを提供している他のシステム障害実績を適用する。

（4）リスク定性評価

明確な数値（コスト換算）によってリスクを評価する定量評価が大切であることはもちろんであるが、実際には、風評リスクのように損失額が算定できないケースや、定量評価の結果が同じでも、性質によって重要度が全く異なるリスクも存在する。こうしたリスクに対して定量評価だけで対応すれば不合理な結果を招いてしまう。したがって定性的なリスク評価を併用することが必要となる。

先に挙げたアンケートの結果によれば、ほとんどの保険会社において何らかの方法で定性的な評価を実施しているが、当研究では、金融庁検査マニュアルの項目にもある「機密性」、「完全性」、「可用性」の３つの観点による評価手法を提案する。

ａ．リスクシナリオの性質にもとづく定性分析と一次評価

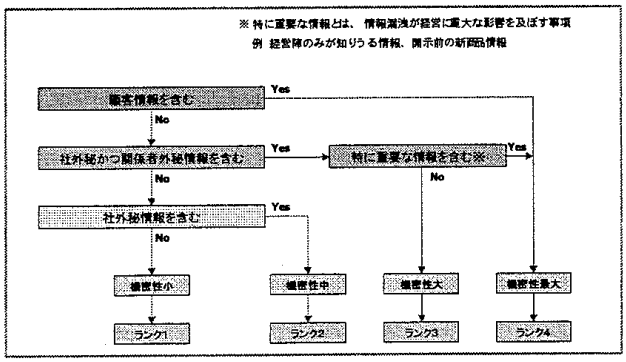
全てのリスクシナリオについて、「機密性」、「完全性」、「可用性」のなかから、そのリスクシナリオに最も関連するリスクを選択し、定性分析を行う。定性分析の結果は、危険度に応じて４段階評価とする。

危険度（ランク）：「小（ランク１）」、「中（２）」、「大（３）」、「最大（４）」

なお、この定性評価は、リスクシナリオの持つ絶対的な性質に依存するため、各企業がそのリスクに対して軽減策を施しているかどうかについては考慮されない。よって、この結果は一次評価とし、軽減策を加味したうえで最終的な定性評価を行う。評価手順は以下のｂ～ｄに示すとおりである。なお、「機密性」、「完全性」、「可用性」のランクを設定するための重要項目は各企業によって異なるため、各社の置かれている状況等にあわせて決定する。

ｂ．「機密性」の観点にもとづく定性評価

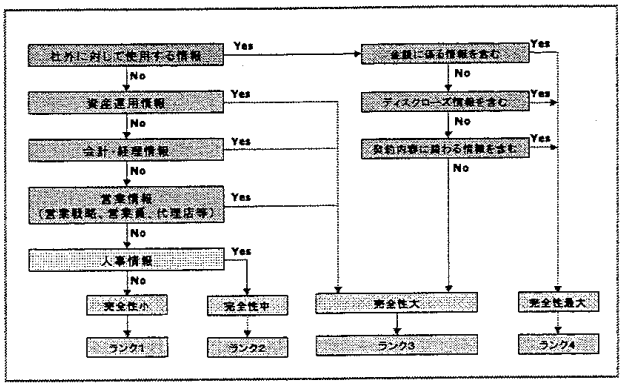
機密性の観点から見て一番重要と思われる内容は、「顧客情報を含むデータ」である。次に「社外秘かつ関係者外秘情報（重要プロジェクト等）を含むデータ」である。ただし、この中でも特に重要な情報はランク４となる場合がある。（これは評価担当者の判断に委ねられる。）次に社外秘情報となる。これ以外のものはランク１とする。



図Ⅳ－４．「機密性」の観点に基づく定性評価分類手順

c．「完全性」の観点にもとづく定性評価

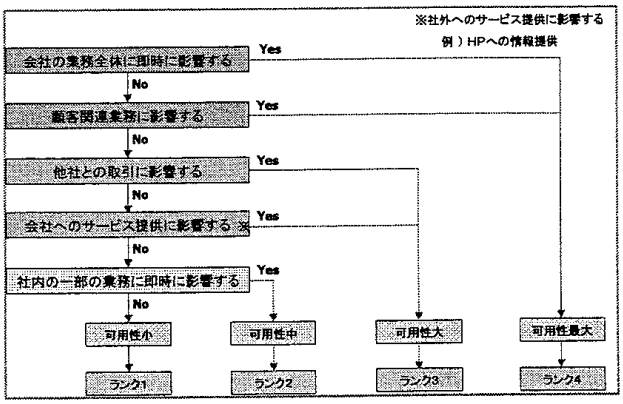
完全性の観点から見て一番重要と思われる内容は、「社外に対して使用する情報」である。ただし、その中でも「金額に係るもの、ディスクローズ情報、契約内容に関わるもの」は特に重要である。次に「資産運用、会計・経理、営業情報等」であり、最後に「人事情報」とする。これ以外のものはランク１とする。



図Ⅳ－５．「完全性」の観点に基づく定性評価分類手順

d．「可用性」の観点にもとづく定性評価

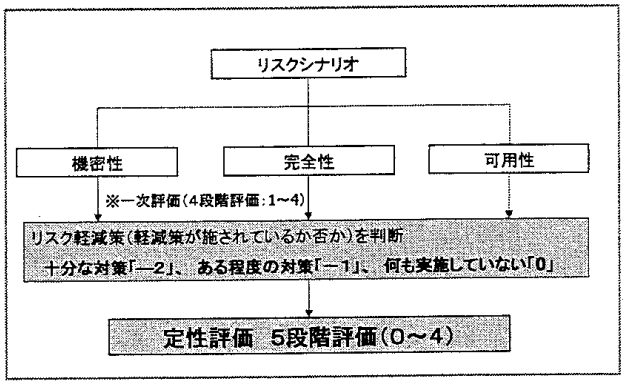
可用性の観点から見て一番重要と思われる内容は、「会社の業務全体に即時に影響するもの」、「顧客関連業務に影響するもの」である。次に「他社との取引に影響するもの、社会へのサービス提供に影響するもの」である。最後に「社内の一部の業務に即時に影響するもの」である。これ以外のものはランク１とする。



図Ⅳ－６．「可用性」の観点に基づく定性評価分類手順

e．リスクの最終的な定性評価

一次評価の結果にリスク軽減策の実施状況を勘案した残余リスクを判定する。「充分な対策を施している」場合には、一次評価の結果を２ランクを引き下げる。「ある程度の対策を施している」場合には、同様に１ランクを引き下げる。「何も実施していない」場合には、一次評価の結果の通りとする。最終的に、全てのリスクシナリオに対して５段階による定性評価を実施する。



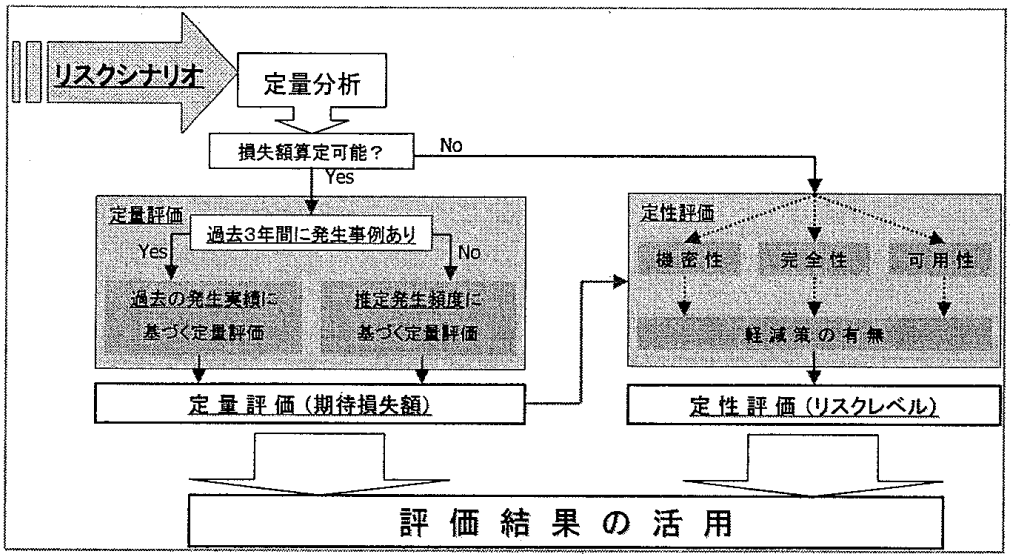
図Ⅳ－７．リスクの定性評価決定手順

「最小（０）」、「小（１）」、「中（２）」、「大（３）」、「最大（４）」

なお、「充分な対策」とは、システムダウンに備えたサーバーの２重化のように、その対策によってリスクが著しく減少する仕組みが確立されているケースを指す。一方、「ある程度の対策」とは、人的作業によるサンプルチェックのようにリスク発生確率は、ある程度減少するものの、リスク低下保証には至らないケースを指す。ここは評価担当者の判断に委ねられる部分があるため、関係者間でコンセンサスを得た基準を作っておくことが望ましい。

3．リスク評価手法のポイント

最後に、私たちが提案するリスク評価手法の全体像を図Ⅳ－８に示すとともに、前章末で示した「リスク評価手法に求められる条件」にそって当評価手法のポイントを整理する。



図Ⅳ－８．リスク評価手法の全体像

（１）リスク評価に至る分析のプロセスが分かり易い

当評価手法は、ユーザーと情報システム部門が主体となって業務で発生しうる様々なリスクシナリオを洗い出して評価するボトムアップ型の手法である。ユーザーが主体的に参加してリスク発生源とビジネスインパクトを分析していくため、リスク評価のプロセスがユーザーにとっても分かり易い。

（２）妥当な分析結果（評価）が得られる

定量化に適さないリスクを無理に定量評価することは、余分な労力がかかるだけでなく、不合理な評価結果を招く危険がある。当評価手法は、定量的なリスク分析と定性的なリスク分析を組み合わせることで互いのメリットを活かした合理的な評価結果を導くことができる。

また、評価者の主観によって評価結果が左右される問題に対しては、ビジネスインパクトの算出基準を定めることで評価者の主観が入る余地を最低限に抑えている。

（３）リスク分析に多大な作業負荷を要しない

特に定量分析の実施に際しては、基礎データの調査・蓄積といった膨大な作業が必要になるが、当評価手法は、業務のリスクを直感的に分かっているユーザーが主体となってリスクシナリオを作成するため、重要なリスクシナリオから始めて、徐々に精緻なものにしていくといった柔軟な制御がしやすい。このため、手法導入に際しての障壁が低く、適切な作業負荷で着実に実行できる範囲でリスク分析を行うことができる。

（4）定量的なリスク評価ができる

当評価手法では、これまで説明してきたようにリスクを定量的に評価することが可能である。また、リスクシナリオにおける障害の規模（発生量）の統一基準を設けることで各シナリオのリスク量比較が可能である。

Ⅴ．リスク評価手法の活用

第Ⅳ章では、私たちの提案するリスク評価手法の内容と留意点について説明した。本章では、具体例を使って実務におけるリスク評価を解説した上で、リスク評価結果の活用方法を紹介する。

１．リスク評価の適用例

この節で、発生実績のあるリスクシナリオと発生実績にないリスクシナリオ例を使って具体的な評価手順・方法を説明する。

（１）リスクシナリオ例１　～証券誤表示～

ａ．シナリオ条件

・リスク事象　：　新規発行の保険証券に誤表示の項目がある。
・リスク起因　：　アプリケーションのバグによるもの。
・リスクによる被害　：　アプリケーションの修復工数
お客様のクレーム処理等の事務対応
紙、郵送関連費用
会社の信用への影響

ｂ．評価の手順

このシナリオでは、定量分析における損失額の算出が可能なので、定量分析と定性分析の両方でリスク評価を行う。なお、過去三年間に発生実績があるため、発生実績に基づき定量評価を行うことができる。（図Ⅳ－８「リスク評価手法の全体像」参照）

ｃ．評価の前提条件

実際の業務でリスクを評価する際の条件は各社が異なるものになるが、ここで評価の条件を下記のように仮定する。

・年間の証券発行件数　：　５０万件
・過去３年間の発生実績　：　３回発生し、合計１０００件
・リスク軽減策は施されているが、十分ではない
・１件あたりの対応費用※　：　１６００円

※対応費用－実際のリスク発生時に、発生件数比例の費用と発生回数比例の費用が存在するが、ここでは計算の便宜上、発生回数比例の費用を簡略化し、件数比例費用の中に入れることにする。

d．リスクの定量評価

第Ⅳ章で説明したように、

・　リスクの定量評価（年間期待損失額）

＝　ビジネスインパクト（A）　×　発生頻度（B）

・　ビジネスインパクト

＝　基準損失額

（誤処理の場合は年間総処理件数の０．５％で計算する）

・発生頻度　　＝　基準損失の補正（基準損失額は年間何回発生したか）

となっているため、ここで、

ビジネスインパクト（A）　＝　（年間の処理件数　×　０．５％）×　１６００円

＝　５０万件　×　０．５％　×　１６００円

＝　２５００件（年間発生基準件数）×　１６００円

＝　４００万円

リスク発生頻度（B）　＝　（過去３年間の実績）／（（年間発生基準値）×３）

＝　１０００件　／（２５００件　×　３）

＝　１３．３％

リスクの定量評価　＝　（A）×（B）

＝　４００万円　×　１３．３％

＝　５３．３万円

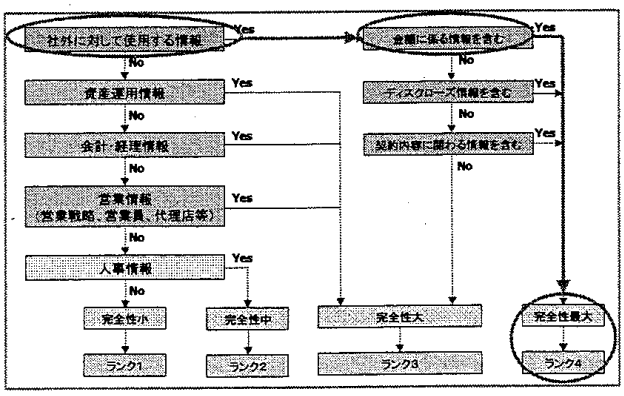
という計算ができる。

e．リスクの定性評価

リスク事象から、このシナリオは「完全性リスク」に分類することができる。

図Ⅴ－１のように定性評価フローを適用すると、「社外に対して使用する情報」と「金額にかかわる情報」の２点から、「完全性リスク最大で、ランク４」との結論が導かれる。

さらに、「リスク軽減策が施されている」という前提条件から、評価が１ランク下がり、最終評価が「ランク３」となる。



図Ⅴ－１．リスクシナリオ例１の定性評価

（2）リスクシナリオ例２　～地震によるシステム停止～

ａ．シナリオ条件

・リスク事象　：　首都圏直下型の大型地震でシステム全面停止。
バックアップセンターを保有しておらず、復旧までの２週間業務が停止した。

・リスク起因　：　地震による電算センター機能停止

・リスクによる被害　：　２ヶ月会社業務が停止することによる人件費の無駄
システム復旧のためのコストが発生
営業活動が２ヶ月停止することによる機会損失の発生

ｂ．評価の手順

このシナリオでも、定量分析における損失額の算出が可能なので、定量分析と定性分析の両方でリスク評価を行う。しかし、過去３年間に発生実績がないため、発生頻度を推定して定量評価を行うことになる。

なお、このシナリオでは地震がリスクの根本原因になっているため、発生頻度推定手法２により、地震の発生頻度をリスクの発生頻度に適用して定量評価を行う。

ｃ．評価の前提条件

・年間の新契約件数は５０万件とし、１日の業務停止により獲得できなかった契約件数は２５００件。１件で会社が得たであろう付加Ｐは１０万円とする。
・固定給従業員数は２千人とし、人月単価１００万円（１人日５万円）とする。
・復旧コストは３０億円とする。
・巨大地震の発生確率は７５年に１回とする。

ｄ．リスクの定量評価

リスクの定量評価（年間期待損失額）
＝　ビジネスインパクト（Ａ）　×　発生頻度（Ｂ）

ビジネスインパクト　＝　基準損失額（システム停止の場合は１日で計算する）

発生頻度　＝　基準損失の補正（基準損失額は年間何回発生したか）

２ヶ月間の損失額　＝　２ヶ月の営業機会損失　＋　人件費損失　＋　復旧コスト
＝　（２５００件×１０万×４０日）
＋（２０００人×５万円×４０日）　＋　（３０億円）
＝　１７０億円

ビジネスインパクト（Ａ）　＝　（２ヶ月間の損失額）　／　４０日
＝　１７０億円　／　４０日
＝　４．２５億円

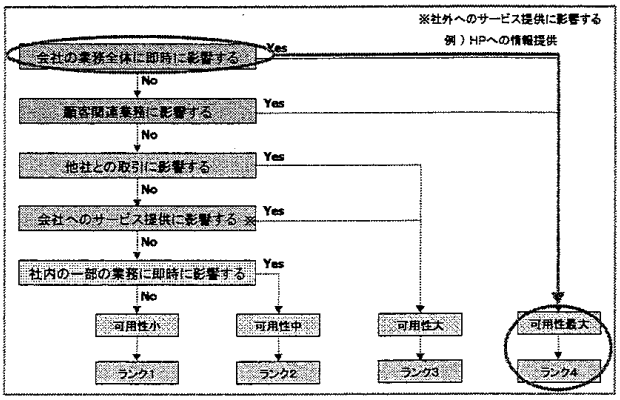
発生頻度（Ｂ）　＝　４０　÷　７５　＝　５３．３％

リスクの定量評価 ＝ （A） × （B）
＝ ４．２５億円 × ５３．３％
＝ ２．２５億円

e．リスクの定性評価

リスク事象から、このシナリオは「可用性リスク」に分類することができる。

図Ｖ－２のように定性評価フローを適用すると、「会社の業務全体に即時に影響する」から、「可用性リスク最大で、ランク４」との結論が導かれる。



図Ｖ－２．リスクシナリオ例２の定性評価

また、「バックアップセンターを保有していない」との条件から、軽減策が施されていないと見なすことができるので、最終評価は「可用性リスク最大で、ランク４」のままである。

２．対策費算定例

ここまで２つのリスクシナリオについて定量評価と定性評価の２つの評価視点から実際のリスク評価手法の適用を確認してきた。ここでは、これら２つのリスクシナリオに対して、リスク軽減を実現ための対策とその費用を例示する。

（１）リスクシナリオ例１　～証券誤表示～

a．方法

現在、「証券誤表示」に対するリスク軽減策として、商品改定等のシステム対応本稼働後１ヶ月間の出力証券詳細チェックを実施しているが、１ランク上のリスク軽減策として以下の対応の実施を想定する。

●日次業務における出力証券のサンプルチェック

b．費用

保険証券の発行量は年次・月次でピークオフがあるものの、サンプルチェックレベルであれば１人が完全に張り付く程の業務量ではないとの認識から以下の人件費を想定する。

●年間費用　：　サンプルチェックに要する人件費
＝　０．５人月／月
＝　５０万円／月
＝　６００万円

（2）リスクシナリオ例２　～地震によるシステム停止～

a.方法

現在、「地震によるシステム停止」に対するリスク軽減策は特に実施していない状況にあり、１ランク上のリスク軽減策として以下の対応の実施を想定する。

●同時に災害に見舞われることのない遠隔地に、最低限の業務継続を可能とするレベルのバックアップシステムを構築する。

b.費用

オフサイトのバックアップシステムを構築する為の一時費用と、そのバックアップシステムを維持・管理する為の経常費用の発生を想定する。

●初期導入費用　　：１０億円（ホストコンピュータ・通信機器・周辺機器等）

●年間運用費用　　：　１億円（保守料・回線費用・センター利用料等）

（4）調査シートへの記入

２つのリスクシナリオに関する対策費の算定結果を、先に行っているリスク評価結果と合わせて調査シートに記入すると表Ｖ－１のような形に整理される。

表Ｖ－１．リスク調査シート

原因				事象(リスクシナリオ)	リスク評価				対策費
大分類	中分類		小分類		ビジネスインパクト	発生確率	定量(金額)	定性(5ランク)	
内部に起因	アプリケーション		プログラムミス バグ	①発行した保険証券に誤表示が発生	400万円	0.133	53万円	3	初期：　－ 年間:600万円
				******	*****	*.*	*,***万円	*	*,***万円
				******	*****	*.*	*,***万円	*	*,***万円
	運用	ハードウェア	ハード障害 運用ミス	******	*****	*.*	*,***万円	*	*,***万円
				******	*****	*.*	*,***万円	*	*,***万円
		Network	ネットワーク障害 運用ミス、Web障害	******	*****	*.*	*,***万円	*	*,***万円
				******	*****	*.*	*,***万円	*	*,***万円
	その他		入力データ不良　等	******	*****	*.*	*,***万円	*	*,***万円
外部に起因	災害 テロ 外部からのﾃﾞｰﾀのﾊﾞｸﾞ等			②地震によるシステム全面停止	42,500万円	0.53	22,525万円	4	初期:10億円 年間:1億円
				******	*****	*.*	*,***万円	*	*,***万円
				******	*****	*.*	*,***万円	*	*,***万円
トータルリスク評価					24,000万円			最小2～最大4	初期:11億5000万円 年間:1億2000万円

3．リスク評価結果に対する対策の妥当性の検討

今回取り上げている２つのリスクシナリオに沿って、対策の妥当性を検討する際の視点を紹介する。

表Ⅴ－２．リスク評価結果と対策費比較

リスクシナリオパターン	リスク対策費用算定額	定量評価の期待損失	定性評価のリスクレベル	対策後のリスクレベル
証券誤表示	年間：６００万円	５３万円	大（3）	中（2）
地震によるシステム停止	初期：　１０億円 年間：　１億円	２億２５２５万円	最大（4）	中（2）

「（1）証券誤表示」のシナリオの場合には、[定量：５３万円・定性：大（３）]のリスク評価に対して、年間６００万円のコストを投入してもリスクレベルは[定性：中（２）]までしか改善されない。したがって費用対効果の面で問題のあるリスク対策と考えられる。

一方、「（２）地震によるシステム停止」のシナリオの場合には、[定量：２億２５２５万円・定性：最大（４）]のリスク評価に対して、初期投資１０億円・年間１億円のコストを投入することとなる。しかし、年間あたりの対比で見た場合には[定量：２億２５２５万円]に対して[１億円]のコスト投入ですむ。また、本来許容すべきでない[定性：最大（４）]のリスクを[定性：中（２）]とすることができ、妥当なリスク軽減策といえる。

以上のように、リスク対策のコストの多寡は、掛かる費用の大小のみに着眼するのではなく、費用対効果や、現状の定性・定量両面のリスク量が会社として許容できる範囲内なのかを総合して判断する必要がある。リスク対策投資については、この様な視点に基づいてリスクに対する対策の妥当性を検討していくことがポイントとなる。

4．リスク評価結果の活用

最後に、リスク評価結果の活用方法を紹介する。リスク評価結果は、大きく２つの視点での活用が考えられる。１つが「リスク管理部門での活用」であり、もう１つが「経営における活用」である。この２つの視点は、言いかえるとリスク個々の状態に着眼する「ミクロな視点（＝リスク管理部門での活用）」と会社全体が抱えるリスクの状態に着眼する「マクロな視点（＝経営における活用）」とも言うことができる。

（1）リスク管理部門での活用

a.リスク評価によるリスク実態の把握

リスク管理において先ず出発点になるのが、抱えているリスク状況がどの様な実態にあるかを把握することである。

これまで多くの会社で行われてきたリスク評価は定性評価を中心とした、大まかなリスク把握となっている。この様な評価方法は、例えば顧客に関わるリスクについては、すべてが最重要なリスクとして認識されるなど、必ずしも実態を正しく表した評価とならず、評価者の主観に左右される恐れもある。

こういった状況を踏まえ、今回提案するリスク評価手法は、より客観的なものとすべく定量評価を主体として、「機密性」、「完全性」、「可用性」といったリスクシナリオの性質

に応じた定性評価を組み合わせたものとしている。

b.リスク管理の達成目標の設定

リスク実態の把握を受けて次に必要となるのが、リスク実態に基づくリスク管理の達成目標の設定である。このリスク管理の達成目標は各社のリスク対策に掛けられる予算や既に実施しているリスク対策の成熟度に応じてまちまちである。リスク実態を把握できれば中長期での達成目標として、どこまでが必要かを判断できる。また、予算の制約がある短期の達成目標としては、どこまでが現実的な水準なのかを判断することもできる。

（2）経営における活用

a.システム投資判断材料の提供

企業経営においてプロジェクトを実施する場合、当然その結果として何らかの利益を得ることが目標とされる。しかし、リスク対策の難しいところは、そのリスク対策を行ったとしても、その効果を明示的に示すことができないという所にある。この事から、今回提案するリスク評価手法においては、期待損失額という定量評価の金額を通じて、いかに金額的な観点を明確にするかという点を意識した。

経営者の立場から見たシステムリスクのインパクトを、期待損失額という定量評価の金額を通じて明確化することにより、会社全体を俯瞰したリスク対策投資の優先順位や費用対効果が明らかになり、最終的な経営資源投入時の有効な判断材料として活用することができる。

b.効果的な内部監査の実施

企業統治という考え方が昨今注目を集めているが、この統治機能を適正に働かせる上で不可欠な位置付けにあるものが内部監査である。しかし、システムリスクについては、その専門性の障壁から、内部監査による正確な実態把握が十分に行われてこなかったものと考えられる。今回提案するリスク評価手法を活用することによって、金額やリスクレベルによって潜在するリスクを視覚化することが可能になるため、効果的な内部監査の実施が期待できる。

おわりに

リスク管理は、「終わりのない旅」に例えられる。リスク管理には決定打となるような対策は存在せず、分析／評価、計画、実施、監視のリスク管理サイクルを継続し、レベルアップする中でリスク低減を図っていくしか道はない。時々刻々と変化する環境の中でリスクという目に見えない敵を封じ込めるのは厄介な仕事だ。「何とかリスクを視覚化できないか」「誰もが分かる物差しでリスクを計量できないか」リスク管理業務に携わった人であれば、一度は、こんなことを考えたことがあるのではないだろうか。業務プロセスに潜在するリスクのインパクトが視覚化でき、金額ベースでリスク量を把握できれば、単にリスク管理レベルが向上するだけでなく、リスク係数を織り込んだ精度の高いシステム投資が可能になり、システム戦略を展開する上で貴重な判断材料になる。

しかし、世間では様々なリスク評価手法が提唱されているものの、実務で使えるものはほんの一部分しかない。それとて現実の業務で使うためには、いくつもの高いハードルを超えなければならず、費用対効果を考えればとても真剣に取り組めるようなものではない。そういった意味で、当研究会のテーマとして、リスク定量評価を中心に据えたリスク評価手法を選んだのは大きな冒険だったと思っている。実際、手に余るテーマであったが、「どうせやるなら、本当に実務で使えるものを考えよう」というコンセプトのもと、知恵を絞って産み出されたのが本稿の提案である。まだ検討が不十分な点は多いが、実践的なリスク評価というテーマに対して、現場の視点でかなり踏み込んだ提案ができたと考えている。

リスクという言葉は否定的な意味で使われることが多いが、その語源は「勇気を持って試みる」。国籍と業種の壁を超えたグローバルな規模での生存競争が激しくなる中で保険会社が生き残っていくためには、ＩＴを活用した果敢な戦略展開が鍵になる。今後も、システムリスク管理の重要性は、ますます高まり、リスクマネジメント能力が企業の命運を左右する重要な競争力になるだろう。本稿での提案が各社のリスク管理を前進させる一助になれば幸いである。

最後に当研究にあたり、ご指導・ご協力頂いた各位にこの場を借りて深くお礼申し上げます。

＜参考文献・資料＞

「国際セキュリティ標準 ISO/IEC17799入門」 オーム社
田渕治樹 著

「経営リスクとセキュリティ・ポリシー」2001 ソフトバンク出版
楠正宏／川西宏昌 ㈱日本総合研究所セキュリティコンサルティング 著

シリーズ・経営情報システム（高原康彦 島田達巳 監修） 1993.3 日科技連出版社
（第１０刊）「情報システムマネジメント」
小暮仁 是澤輝昭 島田達巳 著

金融情報システム No．２４６ ２００１．８
調査レポート「金融機関等のための実践的システムリスク管理手法に関する調査報告」
監査安全部 主任研究員 坂口克巳

金融情報システム No．２４１ ２００１．３
調査レポート 「欧州におけるコンテンジェンシープラン策定状況調査」
監査安全部 主任研究員 坂口克巳

「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

「新しい金融検査の影響と対策」 ＴＫＣ出版
木村剛 著