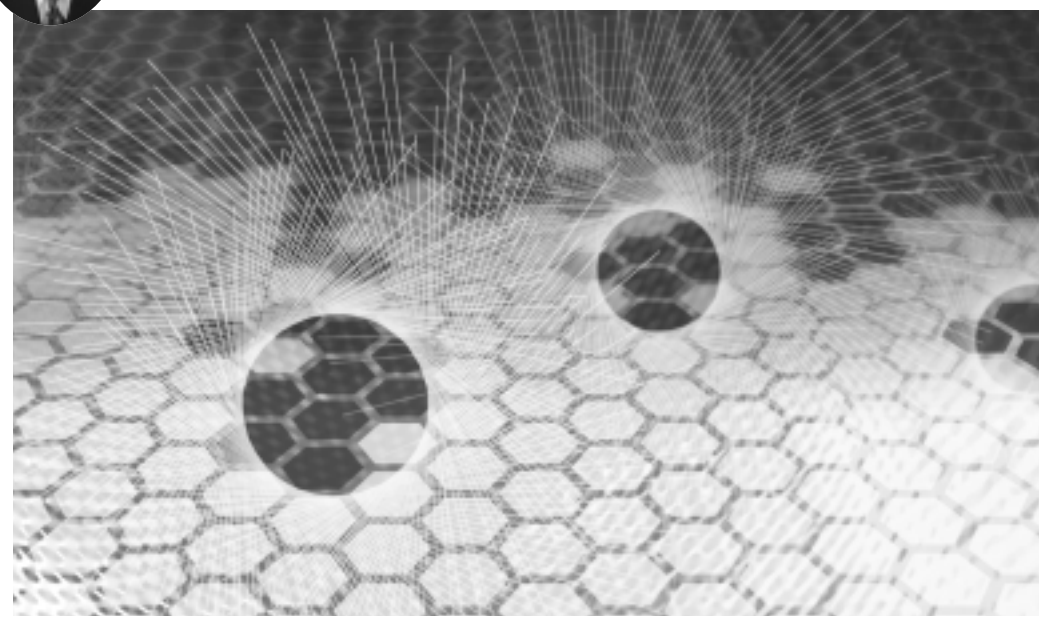
金融機関におけるオペレーショナルリスクの効果的削減

奥井謙一



社会的責任の高まりや事業環境の変化に伴う規制の強化により、金融機関におけるオペレーショナルリスク管理の重要性が増している。規制への対応ということもあり、金融機関の対策はリスク量の計測、所要自己資本の節約という方向に流れがちだが、事業の継続を阻むオペレーショナルリスクは可能な限り削減すべきである。したがって、リスク管理の枠組みを構築したうえ、適切な対策を講じる必要がある。

ミスや不正から災害に至るまで、多岐にわたるオペレーショナルリスクを効果的に削減するためには、優先順位やリスク特性を考慮して、注力すべき対策を絞り込むことが肝要である。バーゼル銀行監督委員会の公表資料から傾向をつかむと、内部管理を中心とした業務プロセスの改善がリスク対策として重要になってくる。鍵となるプロセス改善に際しては、業務プロセスに潜むミスや不正といったリスクに対する適切なチェック・牽制機能の存在を確認する必要がある。そのためには、業務プロセスを可視化することが第一歩となろう。

当レポートに掲載されているあらゆる内容の無断転載・複製を禁じます。すべての内容は日本の著作権法及び国際条約により保護されています。
Copyright © 2004 Nomura Research Institute, Ltd. All rights reserved. No reproduction or republication without written permission.

Ⅰ　オペレーショナルリスク管理が急がれる背景

1　内部統制、リスク管理の必要性

市民社会の成熟、経済活動の国際化、雇用の流動化、情報化社会の進展などにより、企業にはこれまで想定していなかった新たなリスクに対処していく必要が生じている。

たとえば、社会的責任の高まりに伴って、企業の責任を果たせないことに対する社会的制裁という形でのリスクが増大している。相次ぐ不祥事の例に見られるように、罰金や訴訟などの直接的な制裁だけでなく、顧客離れ、株価下落、格付け引き下げなどさまざまな制裁を受ける。

情報化社会の進展は、社会や企業に利便性をもたらす一方、情報の盗難やコンピュータウイルスといった新たな犯罪を引き起こしており、企業はコンピュータ犯罪という新たなリスクに対処しなければならない。

また、雇用の流動化、雇用形態の多様化、賃金格差の拡大、企業再編の進行などによって、企業と従業員との関係が変化しており、従来、暗黙の了解として存在していた信頼関係の希薄化が進んでいる。

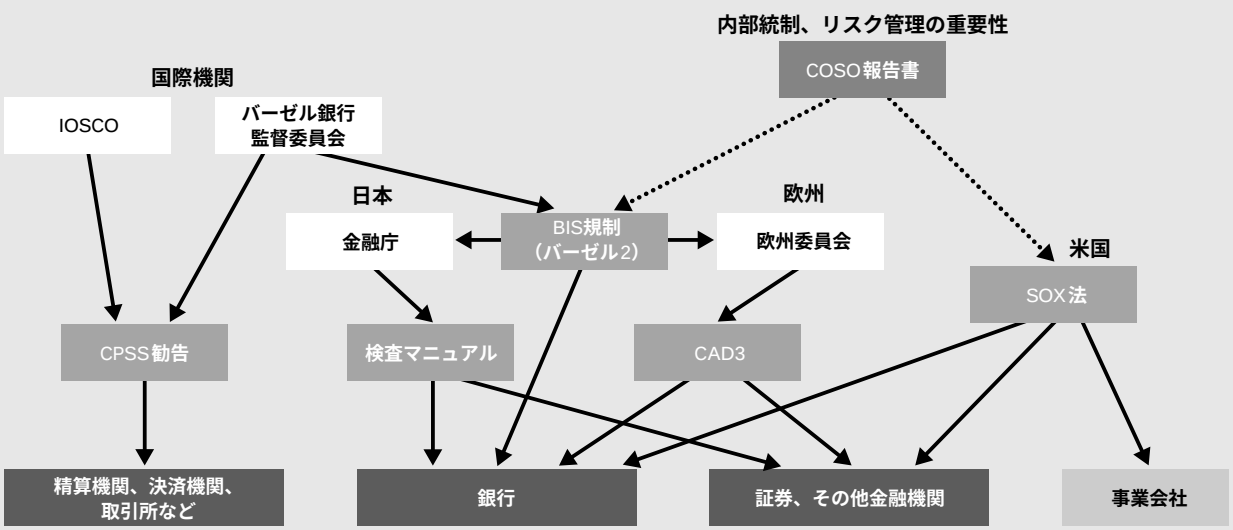
こうしたなか、企業は、環境の変化に伴う新たなリスクに対処し、安全性・健全性を保ちながら継続的に発展していくため、自ら内部統制やリスク管理の強化を図る必要が高まってきている。

2　規制や指針の要求の高まり

企業の内部統制やリスク管理に関する指針として、米国の会計士や監査法人により組織されたトレッドウェイ委員会組織委員会（COSO）の「内部統制の統合的枠組み」（COSO報告書）や「統合リスク管理の枠組み」（COSO ERM）があり、各種規制や指針に影響を与えている（図１）。

不正会計による破綻で有名なエンロン事件に端を発する米国のサーベンス・オクスリー法（いわゆる企業改革法）もその１つである。わが国においても、経済産業省主催の研究会から「リスク新時代の内部統制」という

図1　オペレーショナルリスクをめぐる主な規制・指針の関連



注）BIS：国際決済銀行、CAD：新BIS規制EU域内規制案、COSO：トレッドウェイ委員会組織委員会、CPSS：BIS支払・決済システム委員会、IOSCO：証券監督者国際機構、SOX法：サーベンス・オクスリー法

当レポートに掲載されているあらゆる内容の無断転載・複製を禁じます。すべての内容は日本の著作権法及び国際条約により保護されています。
Copyright © 2004 Nomura Research Institute, Ltd. All rights reserved. No reproduction or republication without written permission.

指針が出されている。

こうした外部からの要請は、金融機関に対して特に顕著である。バーゼル銀行監督委員会のいわゆるBIS（国際決済銀行）規制では、国際的な金融システムの健全性・安全性を維持するため、銀行に対し、内部統制やリスク管理の強化に加え、予想外の損失（リスク）をカバーできるよう自己資本の充実を求めている。

欧州では、BIS規制を銀行だけでなく、証券会社などを含む幅広い金融機関に適用している。わが国においても、金融庁の「検査マニュアル」に見られるように、多岐にわたる業態の金融機関に対し、内部統制やリスク管理の高度化を求めている。

3　オペレーショナルリスクも重要な管理対象

金融機関を取り巻くリスクには、事業機会につながる戦略リスク、信用リスク、市場リスクと、事業の継続を阻害するオペレーショナルリスク、風評リスクとがある。現行BIS規制では、信用リスクと市場リスクが自己資本比率の計算対象となっていたが、オペレーショナルリスクも2004年６月公表の新BIS規制において対象に加えられたため、管理が必須となった。

ところで、オペレーショナルリスクとはどのようなものだろうか。バーゼル銀行監督委員会によれば、「内部プロセス、人、システムが不適切であることもしくは機能しないこと、または外性的事象が生起することから生じる損失にかかわるリスク」と定義される。すなわち、事務ミス、不正、法令違反、システム障害などの内部管理上の問題や、災害、テロリズム、犯罪などの外部要因により損失が発生するリスクのことである。

表１に示すように、近年、金融機関においてオペレーショナルリスクと見なされる事象が数多く発生している。ここに記載した以外

表1　金融機関の損失事象の例

件名	具体的な事象	分類
違反行為による認可取り消し（2004年9月）	富裕層を対象としたプライベートバンキング部門で、融資との抱き合わせ販売、不適切な勧誘（証券取引法違反）、免許外商品の販売（銀行法違反）などの違反行為が発覚。業務改善命令、4拠点の認可取り消し、一部業務停止など、金融庁より厳しい処分を科せられた	法令違反
資金洗浄（2004年6月）	ヤミ金融で得た46億円により割引債を購入し、証券会社で現金化	法令違反
誤発注による損失（2003年7月）	証券会社が、大証のオプション取引で400枚とすべきところを40万枚と誤発注。約3億5000万円の手数料返還に関する調停へ	事務ミス
ネット銀行口座なりすまし（2003年3月）	インターネットカフェに仕組んだハッキングソフトにより口座情報700件を入手。知り得た口座情報により1600万円を不正送金	詐欺
重機によるATMの強奪（2002年頃～）	全国各地で発生しているATM（現金自動預け払い機）の強奪により、1件当たり数千万円の現金が盗難	窃盗
合併におけるシステム統合の失敗（2002年4月）	金融機関の合併時のシステム統合における障害が発生。事態収拾に時間がかかり、口座振替遅延に対する賠償請求を受ける。金融庁からも業務改善命令が出された	システム障害
米国同時多発テロ（2001年9月）	大手金融機関、ニューヨーク証券取引所、ナスダックにおける業務中断による損失（1時間のダウンタイムコストは、証券業界で600万ドル、銀行業界で400万ドルといわれる）	テロリズム
大和銀行ニューヨーク支店（1995年9月）	大和銀行ニューヨーク支店において11年間にわたる米国債不正取引により11億ドルもの損失が発生。組織的隠蔽として米金融監督当局より罰金と業務停止処分が科された	内部不正

当レポートに掲載されているあらゆる内容の無断転載・複製を禁じます。すべての内容は日本の著作権法及び国際条約により保護されています。
Copyright © 2004 Nomura Research Institute, Ltd. All rights reserved. No reproduction or republication without written permission.

にも、トレーダーの不正取引が経営破綻を招いた例（内部不正）や、経済制裁地域への違法送金により１億ドルもの罰金を科せられた例（法令違反）などが発生している。

損失の多寡にかかわらず、経営に大きな影響を及ぼす事例も多くあり、広範にわたる活動となるオペレーショナルリスク管理は、金融機関にとって喫緊に対応すべき重要な経営課題となっている。

II　オペレーショナルリスク管理の導入に向けて

オペレーショナルリスク管理の導入に向けて必要となる最初の取り組みは、その手順の中身を明確にすることである。方針や焦点を定めずに取り組むと、対象範囲が広いこともあり、無駄なコストをかけることになりかねない。

導入に向けて必要となる手順は、（１）目的の再確認、（２）組織・体制の樹立、（３）分類体系の整備、（４）管理ルールの制定――である。図２に示すように、この４つの手順に体系立てて考えると整理しやすい。

1　目的の再確認

まず実施すべきことは、目的の再確認である。達成すべき目的は、

①当局からの規制に対応すること

②市場からの要請に応えること

③自社の競争力を強化すること

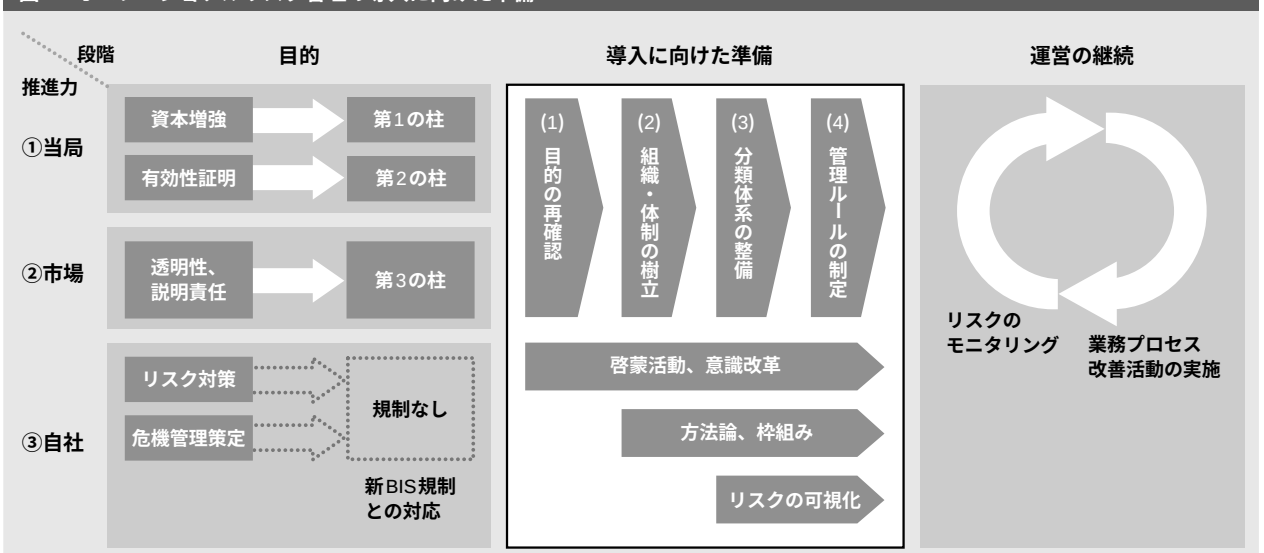
という３つのドライバー（推進力）によって規定される。

①は新BIS規制の適用に対応するものであり、自己資本不足により活動の縮小を迫られることや、自己資本の積み増しによる資本効率の低下を回避することが目的となる。

②は株主への説明責任を果たすことや、企業としての透明性を確保することをゴールにするためのドライバーである。リスク管理についての不明瞭な説明は、格付け機関による格下げにつながり、ひいては資金調達コストの上昇を招く、といったリスクを回避することが目的となる。

③は自社の経営の安定性・継続性を保ち、かつ競争力の強化を目指すためのドライバー

図２　オペレーショナルリスク管理の導入に向けた準備



当レポートに掲載されているあらゆる内容の無断転載・複製を禁じます。すべての内容は日本の著作権法及び国際条約により保護されています。
Copyright © 2004 Nomura Research Institute, Ltd. All rights reserved. No reproduction or republication without written permission.

である。対策や危機管理計画の策定により、リスク自体を削減することが目的となる。

金融機関のオペレーショナルリスク管理への取り組みは、ややもすると、規制当局や格付け機関といった外圧への対応にとどまる嫌いがある。確かに、リスク量を計量し、当局や株主への説明に活用することは、最低限必要なことである。しかし、改善活動につながらなければ、資本を無駄に毀損させることがあり、そればかりか、重大な事故が発生した場合に適切な対策がとれないことも予想される。

そのための備えとして、BCP（事業継続計画）などの危機管理計画を策定すること、業務プロセス改善、アウトソーシングあるいは保険によるリスク対策を講じなければならない。これらは、金融機関経営の安定性・健全性を確保するためのリスク管理の本質的な目的である。

2　組織・体制の樹立

次は明確な役割を持った組織・体制の構築である。全社的に継続して取り組む環境を築くためには、内部監査部門、リスク管理部門などの専任部署の設置だけでなく、現場から経営上層部まで管理に携わる役割を持った担当者（兼任可能）を配置する必要がある。組織・体制が整うことで、現場での啓蒙活動や意識改革が行われ、リスク情報の収集が可能となる。

しかし、オペレーショナルリスク管理においてはミスや不正などが管理対象の中心であるため、隠蔽心理が邪魔をして、リスクの把握に必要となる情報が表に出てこない可能性がある。そのため、損失事象ないしニアミスを発生させた個人を非難・懲罰するのではなく、事象を公表し共有することが、同様なミスの再発を防止して企業全体のリスク削減に寄与することになる、という意識、企業文化を教育により醸成する必要がある。

3　分類体系の整備

３番目は収集された情報からリスクを抽出し、分類することである。これは、リスクの所在・偏在を明らかにし、組織内相互での共通認識を持つために必要な作業である。バーゼル銀行監督委員会には後述の表２に示すような７つの分類があるが、これをベースにして個々の金融機関に合致したレベルの分類体系、つまりリスクのカテゴリーを定めることが有効である。

抽出・分類したリスク要因は蓄積・管理する必要があるが、その枠組みをどう選択するかは議論の分かれるところである。しかし、昨今の内外金融機関の動向を見ると、①自社の損失事象の実績を一元管理する「損失事象データベース」、②定性評価により潜在リスクを洗い出す「RCSA（リスク管理自己評価）」、③損失事象の発生を予見する「KRI（主要リスク指標）」――の３つに収斂してきているように思える。

4　管理ルールの制定

最後は管理のルールを定め、リスク削減に向けた業務プロセスの改善をどのように実施していくかについて明確にすることである。改善対象をどのように決定し、どのレベルまで管理するか、その指針となるルールの策定が業務プロセスの改善に向けて必要となる。

これまで金融機関は、発見されたリスクに

当レポートに掲載されているあらゆる内容の無断転載・複製を禁じます。すべての内容は日本の著作権法及び国際条約により保護されています。
Copyright © 2004 Nomura Research Institute, Ltd. All rights reserved. No reproduction or republication without written permission.

対し、費用対効果を十分考慮せず、ひたすら削減する努力を重ねてきたように見える。果たして、それがオペレーショナルリスク管理に求められる正しい姿なのだろうか。徹底してリスクをゼロに近づけるという従来のルールに変えて、たとえば平均して一定基準以内にリスクをコントロールするという管理ルールも考えて然るべきではなかろうか。

オペレーショナルリスク管理の最終的な目的は、優先順位、コントロールの可能性、費用対効果を考慮したうえで、バランスのとれた削減活動を行うことにある。そのためには、管理対象となるリスク要因の見極めと、リスク管理全体におけるバランスの調整が重要なのである。

III　オペレーショナルリスク対策の実際

1　優先順位付けとコントロールの可能性

オペレーショナルリスクは、内外の不正から法令違反や事務ミスに至るまで非常に管理対象が広い。実際にオペレーショナルリスクを削減しようとするなら、何らかの基準で優先順位を付けて、具体的な対策範囲を絞り込む必要性がある。

効果的な絞り込みのためには、実際の損失事象データを参考に、損失規模の大きな分野を優先するという考え方がわかりやすい。参考までに、バーゼル銀行監督委員会が公表した、63銀行における2001年分の損失事象データを用いて分析を試みる（表２）。同データはサンプル数が限られているうえ、精度にもばらつきがあると思われるが、発生頻度や損失額の大きさに関して、損失事象ごとの一般的な傾向を見てとることはできよう。

表２の損失額合計を見ると、オペレーショナルリスクの７分類のうち、事務・アウトソーシングにかかわる「取引実行、デリバリー、プロセスの管理」によるものが最大で全体の30％を占め、次いで「物的資産の損傷」が29％、「外部の不正行為」が16％となっている。上位３つで損失額全体の75％を占める構造になっており、まずはこれら３つのリスクに注目すべきことを示唆している。

表2　オペレーショナルリスクにかかわる損失事象データ（2001年）

	発生頻度（件）	損失額（千ユーロ） 合計	構成比	1件当たり平均	発生原因の所在
内部不正（内部の不正行為）	1,291	442,600	8%	343	内部
外部不正（外部の不正行為）	16,224	939,300	16%	58	外部
雇用問題（労務慣行および職場の安全）	2,951	321,800	6%	109	内部
法令違反（顧客、商品とビジネス慣行）	2,626	634,900	11%	242	内部
物的損傷（物的資産の損傷）	315	1,694,900	29%	5,381	外部
事業中断（事業活動の中断、およびシステム障害）	377	40,700	1%	108	外部、内部
事務・OTS（取引実行、デリバリー、プロセスの管理）	13,070	1,724,700	30%	132	内部
合計	36,854	5,798,900	100%	157	

注１）銀行63行の損失額1万ユーロ以上の損失事象を集計
　２）OTS：アウトソーシング
出所）バーゼル銀行監督委員会の資料（"The 2002 Loss Data Collection Exercise for Operational Risk"）より作成

当レポートに掲載されているあらゆる内容の無断転載・複製を禁じます。すべての内容は日本の著作権法及び国際条約により保護されています。
Copyright © 2004 Nomura Research Institute, Ltd. All rights reserved. No reproduction or republication without written permission.

一方、損失事象の発生原因が企業の内部にあるか外部にあるかという視点で見ると、詐欺や窃盗などによる「外部の不正行為」、災害などによる「物的資産の損傷」、通信・システム障害による「事業中断」以外はすべて企業の内部要因によるものと考えることができる。

損失事象への対策として、

①保険によるカバー（リスク移転）

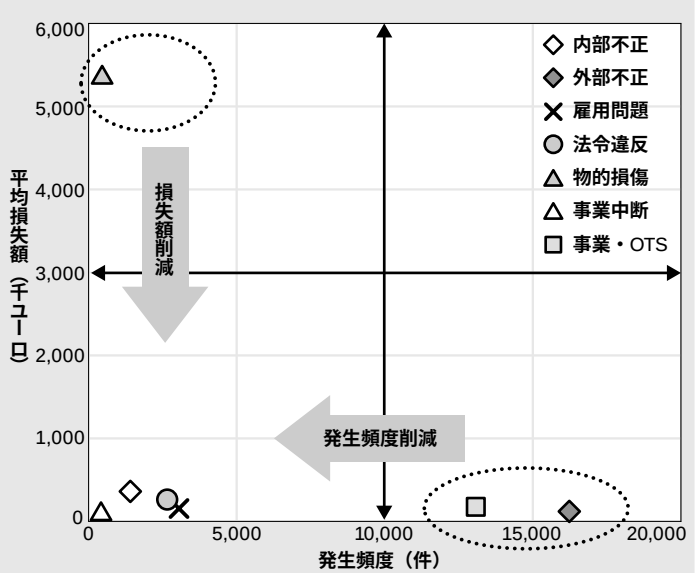
②内部管理を中心とした対策による削減

③あえてリスクを放置（リスク受容）

の３通りを考えた場合、外部に主な原因のある損失事象に対しては①、内部に主な原因のある損失事象に対しては②、いずれの場合に関しても、対策費用と効果とのバランスがとれないと判断されるケースでは③ということも対策の１つと考えられる。

損失金額上位３事象に注目すると、「外部の不正行為」と「物的資産の損傷」については主として保険による対応、「取引実行、デリバリー、プロセスの管理」に関しては主として内部管理による削減という対策が想定される。

図３　損失事象別オペレーショナルリスクの特性（損失額1万ユーロ以上）



出所）バーゼル銀行監督委員会の資料（"The 2002 Loss Data Collection Exercise for Operational Risk"）より作成

2　リスク特性を反映した対策の有効性

ここで、想定した対策の有効性・現実性を確認するために、各事象のリスク特性を見てみよう。図３は、前掲のバーゼル銀行監督委員会のデータを発生頻度と１件当たりの損失額とでマッピングしたもので、各損失事象のリスク特性を表している（一般に「リスクマップ」と呼ばれる）。前述の上位３つのうち、「物的資産の損傷」は低頻度高損失、「取引実行、デリバリー、プロセスの管理」と「外部の不正行為」は高頻度低損失となっている。

低頻度高損失の事象に対して企業単独でリスク対策を講じることは、コストがかさみ過ぎる。このような損失事象に対しては、互助的なリスク負担ネットワークとしての保険を利用することが有効である。一方、高頻度低損失の事象に対して保険などの手段を用いることは、かえってコストが高くつく。企業内部の業務プロセス改善、もしくは内部統制の強化を通じてリスク削減に努めることが、現実的かつ効果的な解決策となる。

以上を勘案すると、上位３つのうち２つは、想定どおりのリスク対策が妥当と確認できる。「物的資産の損傷」については保険によるカバー、「取引実行、デリバリー、プロセスの管理」については内部管理を中心とした業務プロセスの改善である。残りの「外部の不正行為」については、高頻度低損失というリスク特性を考慮すると、保険によるカバーだけではコスト面で適さないことがわかる。自ら可能な範囲で防犯対策を講じたうえ

当レポートに掲載されているあらゆる内容の無断転載・複製を禁じます。すべての内容は日本の著作権法及び国際条約により保護されています。
Copyright © 2004 Nomura Research Institute, Ltd. All rights reserved. No reproduction or republication without written permission.

で、残りのリスクを保険でカバーする、もしくは受容するといった対策が有効であろう。

3　保険の限界と業務プロセス改善の重要性

ところで、保険によるリスク移転はどの程度有効なのだろうか。表３は、同じバーゼル銀行監督委員会の資料によるもので、金融機関が保険をかけていた場合にどの程度の損失額をカバーできたのかを示している。平均の回収率が54.6％ということからもわかるように、カバーできる金額には限界がある。

これは、「内部の不正行為」における回収率が34.2％と極めて低いことに代表されるように、保険料率の抑制のために設定した免責事項（金融機関自身の責任分の減額など）に該当するケースが多いからと想定される。したがって、保険を利用する場合でも、企業内部の業務プロセス改善、もしくは内部統制の強化が求められよう。

「オペレーショナルリスク削減に向けた対策として何をなすべきか」という命題に立ち返った場合、保険もある程度有効であるものの、金融機関として特に努力が必要で、かつ効果的なリスク対策は、やはり内部管理を中心とした業務プロセスの改善に絞られてくるように思われる。

表3　損失事象別の保険による回収率

	回収率（%）
内部不正	34.2
外部不正	56.3
雇用問題	47.8
法令違反	55.2
物的損傷	65.8
事業中断	50.0
事務・OTS	46.6
平均	54.6

出所）バーゼル銀行監督委員会の資料（"The 2002 Loss Data Collection Exercise for Operational Risk"）より作成

Ⅳ　プロセス改善のポイント

本稿では、重要性が増してきたオペレーショナルリスク管理について、本質的な目的は適切な対策によりリスクを削減すること、最も注力すべき対策は業務プロセスの改善であることを述べてきた。

最後に、プロセス改善のポイントを簡単に整理したい。改善に当たっては、業務プロセスに潜むミスや不正などのリスクに対して、適切なチェック・牽制機能が存在するのかを確認する必要がある。そのためには、まず業務プロセスの可視化、すなわち業務フローを描いてみることが第一歩となろう。経験則だけに頼らず、作成した業務フローを用いてミスや不正の可能性を客観的に分析することが、潜在リスクの把握、ひいてはリスク削減に向けたプロセス改善につながる。

今日、金融機関は収益機会の拡大のため、新しい商品やサービスを取り扱うなど業務を多様化している。新しい業務においては経験の浅いこともあり、プロセスが定着しておらず、潜在リスクへの対策が不十分かもしれない。このような業務については、特に注意して業務プロセスを可視化し、リスク削減に向けた改善を行うべきだろう。

著者

奥井謙一（おくいけんいち）
金融IT研究センター金融IT事業開発室上級研究員
専門は債券分析、金融リスク管理

当レポートに掲載されているあらゆる内容の無断転載・複製を禁じます。すべての内容は日本の著作権法及び国際条約により保護されています。
Copyright © 2004 Nomura Research Institute, Ltd. All rights reserved. No reproduction or republication without written permission.