銀行監督行政の効率化に関する提言

－銀行のリスク管理における内部監査の活用について－[1]

2012 年 2 月

一橋大学　国際・公共政策大学院

公共経済プログラム　修士 2 年

加藤　高史

[1]本稿は一橋大学公共政策大学院・公共経済プログラムにおけるコンサルティング・プロジェクトの最終報告書として、受入機関に提出したものです。本稿の内容はすべて筆者の個人的見解であり、受入機関の見解を示すものではありません。

要約

近年の国家公務員の総定員数は、減少傾向で推移している。そのような金融庁の定員は設立以来増加傾向で推移しているものの今後を考えると効率的な監督行政を行う必要がある。本稿では、銀行監督行政の効率化について、銀行のオペレーショナル・リスク管理における内部監査の活用について、参考文献を整理したうえでその有効性について提言している。

謝辞

本研究は、一橋大学大学院で設立された公共政策プログラムの一環で行われたものである。日本ITガバナンス協会会長松尾明様をクライアントとし、約半年間を経て得られた研究成果がまとめられている。報告に先立ち、クライアントとして本プログラムに協力してくださった松尾様に、あらためて感謝の意を表したいと思う。この研究を完成させるにあたり、多くの方々から有益なコメントを頂戴した。ゼミの指導教官である渡辺智之教授（一橋大学）からは、構成から執筆の段階まで何度も助言をいただいた公共政策プログラムの責任者である山重慎二助教授（一橋大学）には、執筆段階において有益なコメントをいただいた。公共政策プログラムの学生など、多くの方々から有益なコメントを頂戴した。ここにあらためて感謝したい。

目次

１．はじめに

政府は、経済財政改革の基本方針 2009 に基づき、行政需要の変化に対応したメリハリのある定員配置を実現する観点から、府省内はもとより府省の枠を越えた大胆な定員の再配置を行うとともに、行政のスリム化を推進するため、平成 22 年度から平成 26 年度までの５年間に平成 21 年度末定員の 10%以上を合理化することを目標としており、近年国家公務員の総定員数は減少傾向で推移している。

このように国家公務員の定員削減が進んでいる状況下であってみ、銀行監督当局である金融庁の定員は、1998 年の発足以降一貫して増加傾向にある（発足当初の定員数は 402 人で 23 年度末における定員数は 1537 人）[2]。このように定員が増加している背景として、金融庁の設置が平成 12 年であり、設置されてからの年数が浅いことから、そもそも業務を行うにあたっての絶対的な職員数が不足していることが考えられる。しかし、今後行政改革が進むなかで、従来のように職員の増員を行うことが難しくなっていくことも予想される。そこで限られた人員で業務を行うためには、現在よりも効率的な監督行政を行うことも必要になってくると考えられる。

金融庁は金融行政当局のあり方について以下の通り述べており、銀行監督を実施するにあたってはまず銀行自身の管理態勢の強化を掲げている。

金融機関経営のあり方は、まずもって「民」の自己責任により決定されるのが基本であることを忘れてはならない。当局の関与は、金融庁の任務である、金融機能の安定、利用者の保護、金融の円滑の観点から必要な範囲においてのみ正当性を有する（金融庁設置法第３条）。例えば銀行であれば、「銀行の業務の健全かつ適切な運営を確保するため」のみに検査・監督が必要となる（銀行法第１条）。そして、それとても出発点はあくまでも、金融機関自身の内部管理と外部監査そして市場規律による監視なのである。「官」の関与は限定的であるべきである。[3]

そこで、本稿では銀行監督行政の効率化を実行するために、銀行のリスク管理のなかでも国民生活に多大な影響を与えるおそれのあるシステムリスクを含めたオペレーショナル・リスク管理態勢について、関連する制度の概要について述べ、実際の銀行の管理態勢の事例を参照しながら、オペレーショナル・リスク管理における内部監査の活用について提言する。

本稿の構成は以下のとおりである。次節で銀行における内部監査の活用について、内部監査の定義も含め述べる。第 3 節では、銀行がリスク管理を行うにあたって、当局が設定しているルールであるバーゼルⅡや金融検査マニュアルといった規制の概要ついて述べる。第 4 節では、バーゼルⅡや金融検査マニュアルといった当局規制の

[2] 金融庁「金融庁の 1 年」（平成 22 事務年度）
[3] 金融庁「評定制度研究会報告書」（2005）

基の考えとなっている COSO－ERM の概要について述べる。第 5 節では、オペレーショナル・リスクの定義や規制で要求されているオペレーショナル・リスク管理態勢、銀行におけるオペレーショナル・リスク管理態勢の事例について述べる。第 6 節はシステムリスク管理について記述する。第 7 節はまとめに充てられる。

２．銀行における内部監査の活用について

本節では、内部監査の定義や業務内容について整理したうえで、銀行の内部監査について、バーゼル銀行監督委員会から公表されているガイドラインについて述べる。

2.1　内部監査の意義

日本内部監査協会より公表されている内部監査基準実践要綱によると、内部監査は次のように定義される。

内部監査とは、組織体の運営に関し価値を付加し、または改善するために行われる、独立にして客観的なコンサルティング業務およびアシュアランス業務をいう。

これらの業務では、リスク・マネジメント、コントロールおよび組織体のガバナンス・プロセスの有効性について検討・評価し、この結果としての意見を述べ、その改善のための助言・勧告を行うことによって、支援することが重要視される。

コンサルティング業務とは、対象部門と合意した内容に応じて、企業価値の増加、組織のガバナンスの改善、リスク・マネジメント等の行為について経営責任を負うことなく行うもので、以下のように分類される（Practice Advisories For Internal Audit）。

① 正式なコンサルティング業務

計画と内容について書面で合意されることを前提とした業務

② 非正式なコンサルティング業務

期間限定のプロジェクト、その場限りの打ちあわせ、日常的な情報交換、定期的な情報交換会の運営支援等

③ 特別なコンサルティング業務

合併と買収やシステム改修のためのチームへの参加

④ 緊急的なコンサルティング業務

災害その他の突発的事象の発生後に、復旧または業務維持管理のために組織されたチーム、または特別な要求や異例な達成期限への対応を一時的に支援するために組織されたチームへの支援

アシュアランス業務とは、主題に責任を負う者が、一定の規準によって当該主題を評価又は測定した結果を表明する情報について、又は当該主題それ自体について、それらに対する想定利用者の信頼の程度を高めるために、業務実施者が自ら入手した証

拠に基づき規準に照らして判断した結果を結論として報告する業務と定義される。アシュアランス業務を行うためには、(1)業務実施者（アシュアランス業務を実施する者)、主題に責任を負う者及び想定利用者（業務実施者が作成した保証報告書を利用する者）の三当事者の存在、(2)適切な主題、(3)適合する規準、(4)十分かつ適切な証拠、(5)合理的保証、業務又は限定的保証業務について適切な書式の報告書といったそれぞれの要件を満たしている必要がある(財務諸表等に係る保証業務の記念的枠組みに関する意見書)。

アシュアランス業務を円滑に実施するためにコンサルティング業務を行うことや、また、コンサルティング業務の結果、アシュアランス業務の実施が求められることもあり、両者は相互に補完的な関係にあるといえ、内部監査人による報告書においては両者の区分が明確にされていなければならない。

2.2 内部監査の独立性と客観性

内部監査が効果的にその目的を達成するためには、検討・評価の結果としての助言・勧告が、公正不偏かつ客観的なものでなければならない。また内部監査活動そのものについても、他からの制約を受けることなく自由に、かつ、公正不偏な態度で客観的に遂行し得る環境になければならない。このため内部監査機能は、その対象となる諸活動についていかなる是正権限や責任も負うことなく、組織的に独立し、また、精神的にも客観的である必要がある。客観性とは、内部監査人が業務の結果について十分な確信を持ち、かつ重大な質的妥協を行わないで業務を遂行する精神的態度をいう。独立性は、客観性を妨げる誘引とならないような組織上の位置づけを確立することにより実現される（内部監査基準実践要綱)。

内部監査機能を独立した部門として組織化することは、内部監査人が内部監査の遂行にあたって不可欠な公正不偏な判断を堅持し、自律的な内部監査活動を行うために必要な条件であるといえる。このように独立的かつ客観的な立場から業務を実施することを求められていることから、内部監査人は、以前に自身が責任を負った業務について、特別のやむを得ない事情がある場合を除き、保証業務を行ってはならない。内部監査人が、以前に責任を負っていた業務についてコンサルティング業務を実施することはできるが、この場合であっても、客観性が保持されないと認められるときは、事前に依頼部門に対してその旨を明らかにする必要がある。

2.3 内部監査人の責任と権限

内部監査を効果的に実施していくためには、その目的や活動範囲等とともに、内部監査人の責任および権限についての基本的事項、その他本基準で求められている事項が、最高

経営者および取締役会、またはそれらのいずれかによって承認された組織体の基本規程として明らかにされなければならない。内部監査規程は、実効ある監査活動遂行のためには必要不可欠のものである。この規程は、組織体における内部監査の目的および実施の内容を明らかにするとともに、これによって監査活動を規律し、あわせて組織体内の人々から内部監査に関する理解と協力が得られるように作成される必要がある（内部監査基準実践要綱）。

このため内部監査規程には、内部監査の目的、対象と範囲、責任と権限、実施の手続・方法、報告、事後処理等に関する各項目が網羅されている必要がある。また内部監査を実施するにあたって、実施に関する記録、従業員および物的資源へのアクセスを認め、関連する業務や諸記録のすべてを検討し得るよう規定されていることが必要となる。

2.4 内部監査人の能力および正当な注意

内部監査人はその責任を果たすために、熟達した専門的能力と専門職としての正当な注意をもって遂行する必要があり、内部監査部門全体としても、その職責を果たすために十分な知識、技能および能力を有していなければならない。内部監査人が個々の職責を果たすに必要な知識、技能および能力とは、以下のようなものがあげられる（内部監査基準実践要綱）。

（1）内部監査の実施に際し、内部監査の基準を実務に適用する熟達した専門的能力。
（2） 会社法等の法令、会計、財務、税務、経済、計量的分析手法、情報技術等の基本についての正しい理解。
（3） リスク・マネジメント、コントロールおよびガバナンス・プロセスについての理解。
（4） 財務諸表に関連する監査に関しては、会計原則や会計手続についての知識。
（5） 適用される法令についての知識。

このように、内部監査を実施するにあたっては、内部監査部門や内部監査人個人に対しても職責を果たすために必要な能力や専門知識が要求されており、内部監査部門長は要求されている水準を満たしていない場合には、直ちに適切な措置を講じる必要がある。

2.5 内部監査の対象範囲

内部監査の対象範囲には、原則として組織体内のすべての業務活動が網羅されており、かつ、リスク・マネジメント、コントロール、ガバナンス・プロセスといった事項が含まれているコンサルティング業務または保証業務である必要がある。

内部監査部門は、重大な潜在的リスクの識別と検討・評価により、またリスク・マネジメントおよびコントロール・システムの改善に貢献することで、組織体の維持・発展に寄与しなければならない（内部監査基準実践要綱）。

次に、内部監査部門は、組織体のコントロール手段の妥当性、有効性および効率性の検討・評価と、組織体内の各人に課せられた責任を遂行するための業務諸活動の合法性と合理性の検討・評価とにより、組織体が効果的なコントロール手段を維持するように貢献しなければならない。

また、内部監査部門は、組織体が倫理観と価値観の高揚、効果的な組織的業績管理とアカウンタビリティの確保、リスクとコントロールに関する情報の組織体内の部署に対する伝達、経営者、取締役会、監査役会、外部監査人および内部監査人の間における活動の効果的な調整と情報の伝達などの目的を達成するために、ガバナンス・プロセスの改善に向けた検討・評価を行い、適切な是正措置を提言しなければならない。

つまり、内部監査部門は、組織体のリスク・マネジメント・システムの有効性を評価する必要があり、さらに組織体のガバナンス、業務の実施および情報システムに関連する潜在的リスクを財務および業務上の情報の信頼性、業務の有効性と効率性、資産の保全、法律、規則および契約の遵守といった視点から検討・評価しなければならない。さらに、内部監査人は、診断業務を通じてリスク情報を得た場合には、それを組織体の重大な潜在的リスクを識別し、検討・評価するプロセスに反映させなければならない。

2.6　銀行の内部監査について

銀行の内部監査については、バーゼル銀行監督委員会より銀行組織における内部監査人の重要な業務、および銀行監督当局と銀行の内部・外部監査人との協力関係の必要性に焦点を当てた「銀行組織の内部監査、および監督当局と内部・外部監査人との関係」が公表されている。金融庁による同ガイドラインの仮訳では、銀行の内部監査の機能や目的について以下のように述べられている。

銀行の取締役会は、適切かつ有効な内部管理システム、銀行業務の様々なリスクを評価する計測システム、リスクを銀行の自己資本水準に関連付けるシステム、および法律、規制、当局の監督方針、自行の内部方針の遵守状況を適切にモニターするための手法を上級管理職が構築・維持していることを確保する最終的な責任を負っている（銀行組織の内部監査、および監督当局と内部・外部監査人との関係）。このことから、取締役会は、銀行の内部管理体制の構築のための最終責任者として重責を担っていることがわかる。

銀行の内部監査機能は、行の内部管理システムや自己資本評価の内部プロセスに対する継続的なモニタリングの一環であり、内部監査は既に確立している銀行の方針や手続きの適切性および遵守状況についての独立した評価を提供する（銀行組織の内部監査、および監督当局と内部・外部監査人との関係）ものであり、取締役会が上記のような責務を効率的かつ有効に成し遂げることを支援することが可能である。

銀行の内部監査部門は、被監査業務から独立していなければならないことに加えて、

日常的な内部管理プロセスからも独立していなければならない。これは、内部監査部門は銀行内で適切な地位が与えられ、客観性と公平性のもとに職務を遂行する、ということを意味している（銀行組織の内部監査、および監督当局と内部・外部監査人との関係）。

銀行の内部監査において客観性と公平性の要請は、特に重要であり、内部監査部門は必然的に、銀行のコーポレート・ガバナンスの枠組みに応じて経営最高責任者（CEO）、取締役会、監査委員会のいずれかの直接指揮下で職務を遂行することとなる。内部監査部門が助言行為やコンサルティングに関わる可能性が必ずしも排除されるわけではないが、内部監査規程において条件や制限について明記されている必要がある。

3. 銀行のリスク管理について

銀行が金融仲介機能を発揮していくうえで、リスク・テイクは不可欠な要素であり銀行経営にはさまざまなリスクが想定される。典型的に銀行は、預金者をはじめとする債権者や株主などの資金供給者から託された資金を、資金需要者たる企業等への融資や企業等の発行した有価証券等への運用に振り向けることによって、資金余剰主体と資金不足主体を結び付けている。ここで銀行は、融資先企業の業績悪化による貸出債権の劣化（信用リスク）や、市場の動向による保有有価証券の価格下落（市場リスク）などの損失発生リスクに直面している。さらに、オフ・バランス取引での負担発生のリスク、コンピュータ・システムの障害や事務トラブルなどによるオペレーショナル・リスクにも直面しており、これらを含めたリスク管理が銀行経営には求められている。また、銀行が適切なリスク管理を行い経営の健全性を確保するために当局は、バーゼルⅡや金融検査マニュアルなどの規制を設けている。

3.1　バーゼルⅡについて

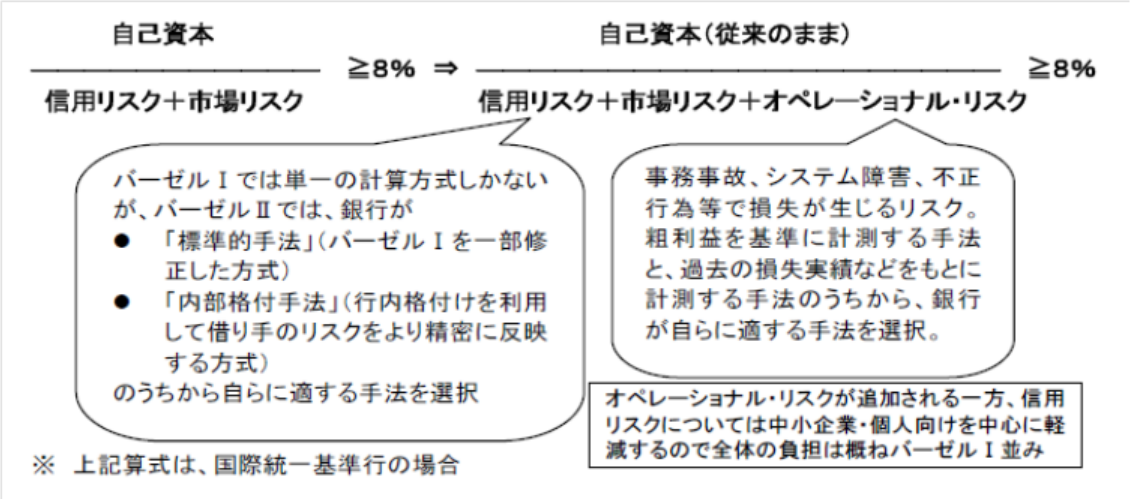
銀行の経営の健全性を確保するために当局が設定している規制の代表的なものに新しい自己資本比率規制（バーゼルⅡ）が存在する。バーゼルⅡとは、1998 年に導入された自己資本比率規制（バーゼルⅠ）からの見直しを経て日本では 2007 年より実施されている規制であり、現在 100 を超える国々の銀行監督において実施されている健全性基準の標準的枠組みとなっている。

自己資本比率とは、銀行が抱えるリスク量に対して保有する自己資本が大きいか小さいかを示す比率である。リスクとは不確実性のことであり、各時点での通常の予想を超えた事態の発生により予想外の損失を生じさせる要因である。つまり自己資本比率とは、予想外の損失発生に備えをどの程度持っているかについての指標でもある（佐藤 2007）。

バーゼルⅡにおける自己資本比率は下図のように計算される。自己資本比率とは、分母である信用リスク、市場リスク、オペレーショナル・リスクといった銀行業務のリスク要素に対して、分子である株式発行によって調達された資本金・資本準備金、

内部留保などの自己資本が一定以上備えられていることがあることを示している。バーゼルⅡではその目安として 8%以上の自己資本比率確保を銀行に求めている。

図表１．バーゼルⅡの計算式



（出典：金融庁公表資料バーゼルⅡについて）

3.2　金融検査マニュアルについて

金融検査マニュアルとは、1999 年 7 月に金融監督庁（現金融庁）が公表したもので、当局が銀行等の金融機関に対して、検査を実施する際の指針を取りまとめた手引書のことをいう。2007 年 2 月には、バーゼルⅡ適用をふまえた改訂版の金融検査マニュアルが公表されている。改訂版の金融検査マニュアルは、自己責任の原則に基づく金融機関経営を補強するものという考え方を基本に、従来の当局指導型から自己管理型への転換、資産査定中心からリスク管理重視の検査への転換を掲げられている。

金融検査マニュアルにおける確認事項として、法令等遵守態勢、リスク管理態勢の 2 つについて規定されている。

法令遵守態勢は、経営陣が金融機関の社会的責任と公共的使命を柱とした企業倫理を構築し、法令等が遵守される態勢を整備しているか、リスク管理態勢については自己責任原則のもと、経営陣・監査役や会計監査任等の役割と責任を明確化するとともに、経営陣等が各種リスク管理の重要性を認識し、リスク管理のための方針を策定し、態勢の整備等を行っているかについて重点を置いている。

各種リスク管理については、信用リスク、市場リスク、流動性リスク、オペレーショナル・リスクがあり、このうちオペレーショナル・リスク管理態勢の整備・確立を検査するにあたって以下のような項目が挙げられている。

3.3 オペレーショナル・リスク管理態勢チェックリスト

金融検査マニュアルではオペレーショナル・リスク管理態勢の確認検査用チェックリスト（オペレーショナル・リスクチェックリスト）を定めており、リスク管理態勢構築のために次のような項目が設定されている[4]。

Ⅰ．経営陣によるオペレーショナル・リスクの総合的な管理態勢の整備・確立状況

１．方針の策定

①【取締役の役割・責任】

②【オペレーショナル・リスク管理方針の整備・周知】

③【方針策定プロセスの見直し】

２．内部規程・組織体制の整備

①【内部規程の整備・周知】

②【オペレーショナル・リスクの総合的な管理部門の態勢整備】

③【各業務部門及び営業店等におけるオペレーショナル・リスクの総合的な管理態勢の整備

④ 【取締役会等への報告・承認態勢の整備】

⑤ 【監査役への報告態勢の整備】

⑥ 【内部監査実施要領及び内部監査計画の策定】

⑦ 【内部規程･組織体制の整備プロセスの見直し】

３．評価・改善活動

(1) 分析・評価

①【オペレーショナル・リスクの総合的な管理の分析・評価】

②【分析・評価プロセスの見直し】

(2) 改善活動

①【改善の実施】

②【改善活動の進捗状況】

③【改善プロセスの見直し】

上記の項目から、検査の視点は、PDCA サイクルが正しく回っているかを確認することにあるといえる。すなわち、オペレーショナル・リスク管理方針において経営陣のオペレーショナル・リスク管理に関する Plan を定め、規程や組織体制の整備を Do、Check および Action として分析・評価ならびに改善活動を行うと捉えている。

システムリスク管理における内部監査部門の役割については以下の項目があげら

[4] 信用リスク、市場リスクなど他のリスクについても同様のチェックリストが制定されている。

れている。

２．内部規程・組織体制の整備

⑥【内部監査実施要領及び内部監査計画の策定】

取締役会等は、内部監査部門に、システムリスク管理について監査すべき事項を適切に特定させ、内部監査の実施対象となる項目及び実施手順を定めた要領（以下「内部監査実施要領」という。）並びに内部監査計画を策定させた上で承認しているか。例えば、以下の項目については、内部監査実施要領又は内部監査計画に明確に記載し、適切な監査を実施する態勢を整備しているか。

- システムリスク管理態勢の整備状況
- システムリスク管理方針、システムリスク管理規程等の遵守状況
- 業務の規模・特性及びリスク・プロファイルに見合ったシステムリスク管理プロセスの適切性
- 内部監査及び前回検査における指摘事項に関する改善状況

上記によれば、内部監査部署は経営陣の積極的な関与を背景に、システムリスク管理部門が行うシステムリスク管理の適切性や重要性を監査しなければならないことがわかる。金融検査マニュアルにおけるオペレーショナル・リスク管理態勢にて求めていることは、適切な仕組みづくりに経営陣等が強く関与することである。そのような態勢構築のために、まず経営層で PDCA サイクルが回る仕組みをつくり、それを文書化することが必要である。具体的には、Plan としてオペレーショナル・リスク管理指針を策定する。次に、Do としてオペレーショナル・リスク管理指針に記載されている事項を実践するためにオペレーショナル・リスク管理部署の設置、必要な人材の提供、内部規定の作成を指示するなどがある。最後に Check と Action として、実践した内容についてオペレーショナル・リスク管理部署等から報告を受け、評価を行い、改善するための方策を打ち出す態勢を整備する。

4. COSO-ERM（全社的リスクマネジメント）について

バーゼルⅡや金融検査マニュアルでリスク管理態勢の構築のために経営陣の積極的関与が求められており、銀行はそれを踏まえたリスク管理態勢を構築しているが、その背景には COSO - ERM の考えがある。COSO とは、米国のトレッドウェイ委員会組織委員会（Committee of Spon-soring Organizations of Treadway Commission）の略称であり、COSO の発行したレポートで提示された内部統制のフレームワークそのものを表すことも多い。バーゼル銀行委員会は、「銀行組織における内部統制（内部管理体制）のフレームワーク」において、COSO による全社的リスク管理（ERM）のフレームワークで示されたガイダンスに従って構築された、内部統制システムに関する定義と

基本要素を採用した。バーゼルⅡでは、このレポートを、最低基準を満たすための必須要件と見なしている。本節では、ERM の定義、目的及び構成要素について述べる。

4.1　ERM の定義

ERM（Enterprise Risk Management）は、事業体の取締役会、経営者、その他の組織内のすべての者によって遂行され、事業体の戦略策定に適用され、事業体全体にわたって適用され、事業目的の達成に関する合理的な保証を与えるために事業体に影響を及ぼす発生可能な事象を識別し、事業体のリスク選好に応じてリスクの管理が実施できるように設計された、1 つのプロセスであると定義されている（八田 2006）。

ERM の根本的な前提は、すべての事業体は、利害関係者に対して何らかの価値を提供するために存在するということである。どんな事業体であっても不確実性に直面するのであって、経営者にとっての課題は、利害関係者のために価値を高める努力をする際に、事業体がどの程度の不確実性を受け入れる用意があるかについて決定することである。不確実性は、事業体の価値を喪失させたり、付加したりする可能性を持つのでリスクでもあり、事業機会でもある。ERM によって経営者は、不確実性とそれに付随するリスクや事業機会に有効に対応でき、それによって事業体の価値を創造する事業体の能力を向上させることができる。

4.2　ERM の目的と構成要素

経営者は、戦略目的を設定し、戦略を選択し、企業全体にわたって浸透させるような戦略を選択し、企業全体に浸透させるような目的と適切に組み合わせる。ERM のフレームワークは、事業体の目的を達成するように作られている。目的は戦略（事業体のミッションと連動しそれを支えるハイレベルな目標）、業務（事業体の資源の有効かつ効率的な利用）、報告（報告の信頼性）、コンプライアンス（適用される法規の遵守）の 4 つのカテゴリーに分類され、これらのカテゴリー分けによって、各々の目的カテゴリーからどのようなことが期待できるかを見極めることができる。

ERM は、8 つの相互に関連する構成要素からなる。これらの要素は経営者が企業を運営する方法から導き出されたものであり、経営プロセスと整合性が取れたものである。これらの構成要素は以下の通りである（八田 2006）。

（1）　内部環境：内部環境は、組織の気風を組み込み、リスクを事業体の人々がどのように捉えて対処するかということについての基礎を構築する。その中には、リスク・マネジメントの考え方、リスク選好、誠実性、倫理観、ならびにその中で構成員が業務活動を行っている環境などが含まれている。

（2）　目的の設定：経営者が目的の達成に潜在的な影響を及ぼす事象を識別する以前に、目的は存在していなければならない。ERM は、経営者が目的を設定するプ

ロセスをきちんと持つこと、およびその選ばれた目的が事業体のミッションを支援し、ミッションの方向性と合致して事業体のリスク選好とも整合性が取れていることを保証するものである。

(3) 事象の識別：事業体の目的達成に影響する、事業体内部と外部の事象は、リスクなのか事業機会なのかを識別されなければならない。事業機会は、経営者の戦略や目的の設定プロセスにフィードバックされることになる。

(4) リスクの評価：リスクをどのように管理するかを判断する基礎として、発生可能性と影響度を考慮しながらリスクが分析される。リスクは、そのリスクが本来持つ固有ベースと残余ベースで評価される。

(5) リスクへの対応：経営者は、リスクの回避、受容、低減および共有などのリスク対応策を選択し、事業体のリスク許容度およびリスク選好とリスクの方向性が合致するように、一連の行動を選択する。

(6) 統制活動：リスク対応策が有効に実行されることを保証する手助けとして方針や手続が設定され実施される。

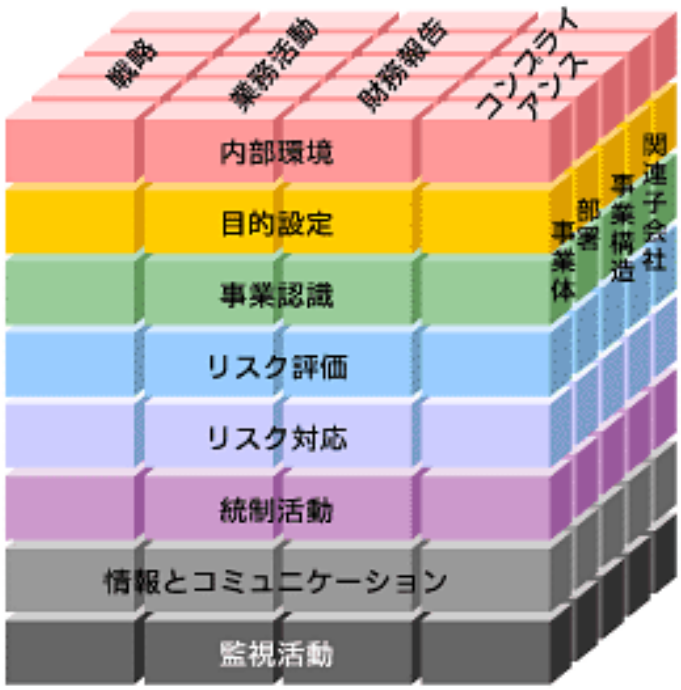
(7) 情報と伝達：関連する情報が認識、補足され、人々が自分達の実行責任を全うできるようなやり方や時間枠で伝達される。

(8) モニタリング：ERM の全体はモニターされ、適宜補正されている。モニタリングは、継続的な経営活動、独立した評価、あるいはその両方で遂行される。

事業体が達成しようと努力する目的と、その達成のために必要とされる ERM の構成要素との間には直接的な関係がある。その関係は下図のように表されている。4 つの目的カテゴリー、すなわち戦略、業務、報告、コンプライアンスは縦の列に示され、8 つの構成要素は横の列に、また事業体およびその部門は、第 3 次元に示されている。この表現は、ある事業体の ERM の全容についても、1 つの目的カテゴリー、1 つの構成要素、1 つの事業体の組織単位、あるいはそれらの任意の部分集合について焦点を当てることができる。

ERM が有効なものであるかは、8 つの構成要素が存在し適切に機能しているかどうかを評価した結果からの判断で決定される。したがって、構成要素は有効な ERM の規準となる。ERM が目的の 4 つの分類のそれぞれにおいて有効である場合には、取締役会や経営者は自らが事業体の戦略や業務目的の達成度を理解していること、また事業体の報告に信頼性があり、適用される法規が遵守されていることについて合理的な保証を持つ。なお、各々の構成要素が適切に機能していれば、中小企業であっても有効な ERM を実施することは可能であり、8 つの構成要素は、すべての事業体で同様に機能するとは限らない。下図は COSO キューブと呼ばれており、ERM における目的と構成要素の関係を示すものとして広く利用されている。

図表 2. COSO キューブ



（出典：http://www.atmarkit.co.jp/aig/04biz/cosoerm.html）

5. オペレーショナル・リスクについて

1998 年に実施された自己資本比率規制（バーゼルⅠ）は、信用リスクや市場リスクの管理重点を置いており、オペレーショナル・リスクは信用リスク、市場リスク以外のその他リスクとして扱われていた。しかし、1995 年に発生したベアリングス銀行の行員の不正取引による倒産や同年に発覚した大和銀行ニューヨーク支店の職員による巨額損失事件の発生は、これまでの信用リスク、市場リスクを管理するのみでは十分ではないことを知らしめ、その他リスクの管理の重要性にも関心が集まった。バーゼル銀行監督委員会はバーゼルⅠの見直しとオペレーショナル・リスクが自己資本規制の枠組みの中で別途取り扱うだけの重要性があるリスクであることを発表した。

5.1 オペレーショナル・リスクの定義

わが国では、バーゼルⅡは銀行法第十四条の二の規定に基づき、銀行がその保有する資産等に照らし自己資本の充実の状況が適当であるかどうかを判断するための基準という告示において定められており、同告示ではオペレーショナル・リスクは次のように

定義されている。

オペレーショナル・リスクとは、銀行の業務の過程、役職員の活動若しくはシステムが不適切であること又は外生的な事象により損失が発生するしうる危険をいう（銀行法第十四条の二の規定に基づき、銀行がその保有する資産等に照らし自己資本の充実の状況が適当であるかどうかを判断するための基準第 307 条第 2 項第 3 号）。

また、同告示では管理すべきオペレーショナル・リスクの範囲を明確化するため具体的損失事象を以下のとおり規定している。

図表 3. オペレーショナル・リスクの分類

損失事象の種類	オペレーショナル・リスク損失
内部の不正	詐欺若しくは財産の横領又は規制、法令若しくは内規の回避を意図したような行為による損失であって、銀行又はその子会社等の役職員最低 1 人は関与するもの（差別行為を除く）
外部からの不正	第三者による、詐欺、財産の横領又は脱法を意図したような行為による損失
労使慣行及び職場の安全	雇用、健康若しくは安全に関する法令若しくは協定に違反した行為、個人損傷に対する支払、労働災害又は差別行為による損失
顧客、商品及び取引慣行	特定の顧客に対する過失による職務上の義務違反（受託者責任、適合性等）又は商品の性質若しくは設計から生じる損失
有形資産に対する損傷	自然災害その他の事象による有形資産の損傷による損失
事業活動の中断及びシステム障害	事業活動の中断又はシステム障害による損失
注文等の執行、送達及びプロセスの管理	取引相手や仕入先との関係から生じる損失又は取引処理若しくはプロセス管理の失敗による損失

（出典：自己資本比率告示を参照に作成）

バーゼルⅡは、各銀行が選択するオペレーショナル・リスク計測手法について、「基礎的手法（BIA）」、「粗利益配分手法（TSA）」、「先進的計測手法（AMA）」を定めている。このうち計量方法について、BIA 及び TSA についてはトップダウン・アプローチ、AMA については主としてボトムアップ・アプローチを採用している。トップダウン・アプローチとは、銀行の利益や費用、資産額など、銀行全体を表現する指標の一定割合がオペレーショナル・リスクであるとみなして計量するアプローチである。このアプローチにおいては、計算が容易である一方で、業務の改善と計量結果との因果関係が把握

しづらいというデメリットがある。他方ボトムアップス・アプローチは、リスク事象の観測と外部損失データなどを活用したシナリオ分析によって、オペレーショナル・リスクを積み上げて計量する方法である。このアプローチでは、損失事象毎に詳細な分析を実施する必要があり、知識と作業面での負荷が大きいものの、積み上げの特性から、各リスク事象への削減対策やその効果測定が可能になるという非常に大きなメリットがある。

BIA は最も簡便な手法であり、銀行粗利益の 15%をオペレーショナル・リスク相当額として所要自己資本額を求めるものである。TSA は、粗利益を業務区分に配分した上で当該業務区分に応じ、掛け目を乗じて得た額をすべての業務区分について合計したものをオペレーショナル・リスク相当額とする。また、粗利益を業務区分に当てはめるための基準を作成し、経営陣の承認を受けることと内部監査部門による定期的な検証を求めている（告示別表第 1 の注)。AMA では、オペレーショナル・リスク相当額の計測についての具体的手法を特定していない。先進的計測手法を用いて算出するオペレーショナル・リスク相当額は、銀行の内部管理において用いられるオペレーショナル・リスクの計測手法に基づき片側 99.9 パーセントの信頼区間で、期間を 1 年間として予想される最大のオペレーショナル・リスク損失の額に相当する額とする（告示第 311 条）とされている。つまり、AMA は、自由度が高い半面、手法の選択やプロセスの根拠、そして計測と評価結果の妥当性についての検証が重要となり、その信頼性など多岐にわたる項目を監督当局に対して証明しなければならない。

5.2　オペレーショナル・リスク管理諸原則について

オペレーショナル・リスク管理に関する指針としてバーゼル銀行監監督委員会より「Principals for the Sound Management of Operational Risk 」（オペレーショナル・リスク管理諸原則）が 2011 年 6 月に公表されている。本文書は、全ての銀行が遵守すべき共通の指針として 2003 年 2 月に公表された「オペレーショナル・リスクの管理と監督に関するサウンド・プラクティス」を、その後のオペレーショナル・リスク管理の進展や金融危機の教訓等を踏まえて改訂したものである（山本・足立 2011)。

オペレーショナル・リスク管理諸原則では、(1) オペレーショナル・リスク管理の基本原則（2）ガバナンスの強化（3）リスク管理の環境（4）ディスクロージャーの役割の各分野について、健全なオペレーショナル・リスク管理の実施のための 11 の原則が掲げられており、具体的な内容は次のとおりである。

原則 1 および 2 ではオペレーショナル･リスク管理の基本原則について述べられている。

原則 1 は、取締役会は、強靭なリスク管理文化を育成するため、自ら指導的な役割を果たすべきであると述べている。取締役会と上級管理職は、強靭なリスク管理によって

導かれる企業文化を育成すべきである。取締役会と上級管理職が育成する企業文化はまた、適切な基準とインセンティブを支持および提示することによって、職業意識と責任感に基づく行動を促すものとなるべきである。この観点から、強靭なオペレーショナル・リスク管理の文化が組織全体に存することを確保する責任は、取締役会にあると規定している。原則 2 では、銀行は、「枠組」を構築、実施および維持し、銀行の総合的なリスク管理プロセスに完全に組み入れるべきである。個別銀行が選択するオペレーショナル・リスク管理の「枠組」は、それぞれの銀行の性質、規模、複雑性、リスク・プロファイルを含む様々な要因に依存するとしている（健全なオペレーショナル・リスク管理のための諸原則仮訳）。

原則 1 および 2 からは、オペレーショナル・リスクは信用リスクや市場リスク以上にリスク管理に関与する部署・職員が多岐にわたり、さらにその発生形態も多様であるため、日頃からの組織横断的な取り組みが必要であり、オペレーショナル・リスク管理の枠組が効果を発揮するためには、経営トップが自ら指導的な役割を果たすことによるリスク管理文化の熟成が重要とされていることがわかる。

原則 3、4 および 5 ではガバナンスの強化について述べられており、原則 3 および 4 では取締役会、原則 5 では上級管理職がガバナンスの強化のために行う事項について述べている。

原則 3 は、取締役会は、「枠組」を設定・承認し、定期的に検証すべきであるとしている。取締役会は上級管理職を監督し、方針、プロセスおよびシステムが全ての意思決定レベルにおいて有効に実施されていることを確保すべきである。取締役会は、オペレーショナル・リスクに係るリスク選好度ないしリスク許容度を定めた趣意書（statement）を承認し、検証すべきである。本趣意書には、当該銀行として、どのような性質、タイプおよび水準のオペレーショナル・リスクを引き受ける用意があるかが明記されているべきであると規定している。また、原則 5 では、上級管理職は、明快、実効的かつ頑健なガバナンス構造を構築し、取締役会の承認を受けるべきである。同構造には、明確に定義され、透明性と一貫性を備えた責任系統が設けられているべきである。上級管理職は、自行の主要な商品、業務、プロセスおよびシステムに伴うオペレーショナル・リスクを管理するための方針、プロセスおよびシステムを組織全体にわたって一貫性をもって実施し、維持することについて責任を有する。上級管理職は、定められたリスク選好度ないしリスク許容度との整合性に配意しつつ本責任を果たすべきであるとしている（健全なオペレーショナル・リスク管理のための諸原則仮訳）。

オペレーショナル・リスク管理の基本としてのガバナンスは 2003 年のサウンド・プラクティスでも指摘されているが、オペレーショナル・リスク管理諸原則では、ガバナンスの強化を改めて強調していることがわかる。また、ガバナンスの強化として、経営陣によるリスク選好度ないし許容度の設定や 3 つの防衛線（業務ライン各部署での管理、ミドル部署での独立した全社的なオペリスク管理機能、第三者機能による独

立した検証）の導入についても述べられている。経営陣によるリスク選好度ないし許容度の設定と 3 つの防衛線の導入は、オペレーショナル・リスク管理を全社的・継続的に実施するために必要な構造といえる（山本・足立 2011)。

オペレーショナル・リスク管理には、銀行内で多数の部署や職員が関わっているためその目線を統一し、一貫した漏れのない運用を確保することが必要である。仮に全社的管理機能と検証機能がなければ、各部署および職員が独自の視点でオペレーショナル・リスクを管理することとなるため、十分な対策が取られないまま、重大な損失が発生するおそれがあり、リスク管理の観点から望ましいものではないことがわかる。

原則 6～10 ではリスク管理環境について扱われており、近年の銀行関連業務を巡る環境変化に対応したオペレーショナル・リスク管理について述べられている。このうちリスク管理環境の中でも原則 6 及び 7 ではリスクの特定と評価、原則 8 ではモニタリングと報告、原則 9 では統制と削減、原則 10 では業務の復旧と継続についてそれぞれ述べられている。

原則 6 は、上級管理職は、リスクとインセンティブが十分に理解されるように、全ての主要な商品、業務、プロセスおよびシステムに付随するオペレーショナル・リスクが特定および評価されることを確保すべきであるとしている。また原則 7 では上級管理職は、全ての新しい商品、業務、プロセスおよびシステムが所定の承認プロセスを経て導入されること、また、同プロセスにおいてオペレーショナル・リスクも十分に評価されることを確保すべきであると定めている（健全なオペレーショナル・リスク管理のための諸原則仮訳)。

原則 6 および 7 では、リスクとインセンティブが十分に理解されるように、全ての主要な商品、業務、プロセスおよびシステムに付随するオペレーショナル・リスクを特定し評価することを銀行の上級管理職に求めていることがわかる。リスクの特定や評価は、通常内部的な損失データの収集と分析によって行われているが、内部的な損失データのみでは事例が限定的であり、その他の有効な手法として内部監査での指摘事項からオペレーショナル・リスクの目星をつける方法などが例示されている。

原則 8 は、上級管理職は、オペレーショナル・リスク・プロファイルと大規模な損失エクスポージャーを定期的にモニターするプロセスを実施すべきとしている。またオペレーショナル・リスクの能動的管理を支えるものとして、取締役会、上級管理職および業務ラインの各レベルに適切な報告メカニズムの設置を求めている（健全なオペレーショナル・リスク管理のための諸原則仮訳)。

このことから原則 8 では、自行におけるオペレーショナル・リスクを能動的に管理するために、オペレーショナル・リスクの分析結果などを定期的に経営陣、管理職および業務ラインに適切に報告することの重要性とこれを実現するための制度の構築求めているといえる。

原則 9 では、銀行に方針とプロセスとシステム、適切な内部統制、適切なリスク削減

および（または）リスク移転戦略から成る、強靭な統制環境の整備を求めている（健全なオペレーショナル・リスク管理のための諸原則仮訳）。原則 9 からは、適切な統制環境の整備によって、リスクを削減ないし、移転することの重要性を指摘している。また、移転の例として、専門的な能力を有しているものへのアウトソーシングがあげられている。

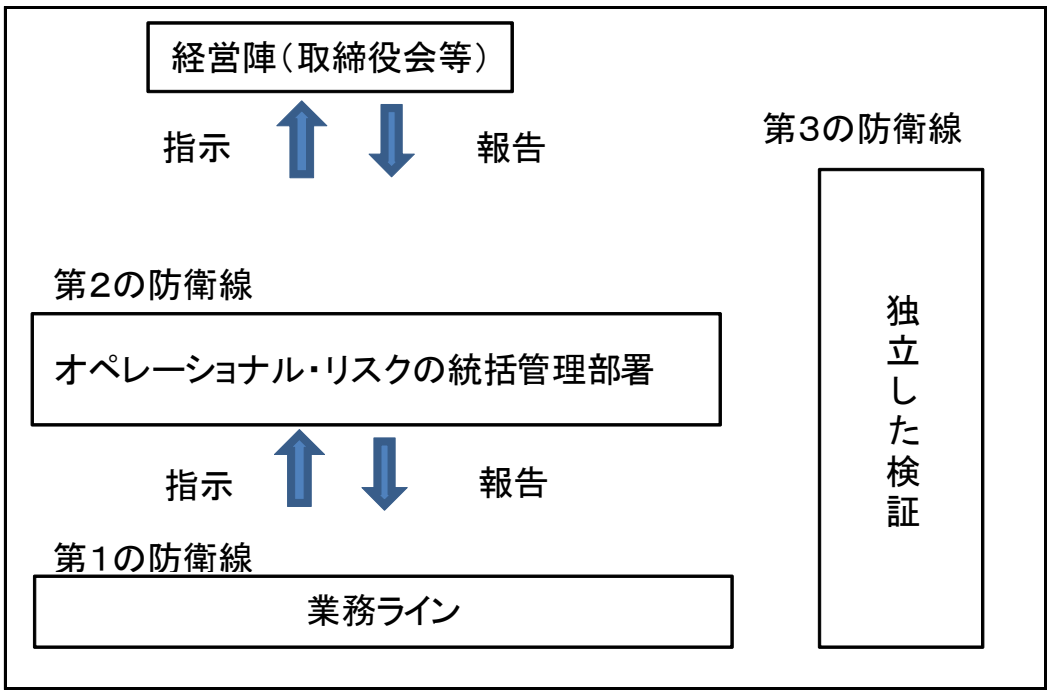
原則 10 では、銀行に対して業務の復旧と継続に関する計画を策定し、業務に甚だしい混乱が生じた場合にも事務を継続し、損失の拡大を防ぐ能力の確保を求めている（健全なオペレーショナル・リスク管理のための諸原則仮訳）。原則 10 では、業務の復旧と計画の継続に関する計画の策定により、緊急時であっても社会的なインフラである金融・決済サービスを円滑に提供することが銀行に期待されているといえる。

原則 11 はディスクロージャーの役割について述べている。銀行のパブリック・ディスクロージャーは、当該銀行がオペレーショナル・リスク管理に如何に取り組んでいるかを利害関係者が評価できるような方法で行われるべきである（健全なオペレーショナル・リスク管理のための諸原則仮訳）。 適切なディスクロージャーは、投資家や市場参加者が銀行のオペレーショナル・リスク管理を正確に評価することを可能にするとともに、市場規律の発揮によってオペレーショナル・リスク管理の向上に資するといえる。

オペレーショナル・リスク管理諸原則は、内部監査という観点からは、各業務の手続きが遵守されているか否かにとどまらず、銀行全体を見渡してオペレーショナル・リスク管理の枠組みとそれに関連するガバナンス・プロセスが総合的に適切かつ十分であるかを評価するよう求めている。また、内部監査がオペレーショナル・リスク管理に係る統制、プロセスおよびシステムについて独立した検証と評価を行うことを第 3 の防衛線と位置付け、強固なオペレーショナル・リスク管理の重要な要件としている。このことからも銀行のオペレーショナル・リスク管理において、内部監査の役割の重要性をみてとることができる。

図表 4 はそれぞれの防衛線を図式化したものである。図表 4 から全社的に統一した目線でリスク管理を行うためには、業務ラインで設置されている第 1 の防衛線と第 2 の防衛線に加え、独立した立場からの検証である第 3 の防衛線の存在が重要であることが見てとれる。

図表 4. 銀行のオペレーショナル・リスク管理のための 3 つの防衛線の関係図



（出典：山本・足立（2011）を参照に筆者作成）

5.3　銀行のオペレーショナル・リスク管理の事例

本節では、銀行のオペレーショナル・リスク管理態勢の事例について、検討する。具体的なオペレーショナル・リスク管理態勢は以下のとおりである（瀧本・稲葉 2011）。

5.3.1　オペレーショナル・リスク管理態勢の整備

オペレーショナル・リスクを組織横断的に議論する体制の構築に係る取組みとして、オペレーショナル・リスク管理委員会の設置を行い、さらにその下位組織としてオペレーショナル・リスク管理部会を併設し、個別事象の掘り下げやオペレーショナル・リスク管理委員会への報告事項の選定について議論を行うことを可能にしている。

また、オペレーショナル・リスクを総合的に管理する部署としては、営業部門だけでなく、オペレーショナル・リスクを構成するすべてのリスク種類からも独立したオペレーショナル・リスク統括部署を設置している。ここでは、現場からの報告に基づくリスク主管部署での各種分類作業（業務分類・工程分類等）の検証、リスクシナリオの検証、リスク主管部署が実施したリスク削減等の効果検証（モニタリング）、オペレーショナル・リスク分析レポートの設計（CSA と KRI を融合した分析結果をもとに BPR に軸足を置いたリスク削減等の規格・提言を付保したものの設計）などを

主要な業務として、統括としての実効性を高める点に注力している。

オペレーショナル・リスク統括部署の活動で最も重要なものはオペレーショナル・リスク管理委員会及び部会の運営とオペレーショナル・リスクの評価・分析である。オペレーショナル・リスクの評価・分析の総括として実施しているオペレーショナル・リスク分析レポートでは、発生しているリスク事象の分析だけでなく、数年後・数十年後に必ず発生する重大リスク事象（優先的にリスク対策を処方すべきシナリオ事象）の想定を、各リスク主管部署が日々実施している活動とは別の視点で実施し、それぞれに応じたリスク削減策提言とともに公開している。

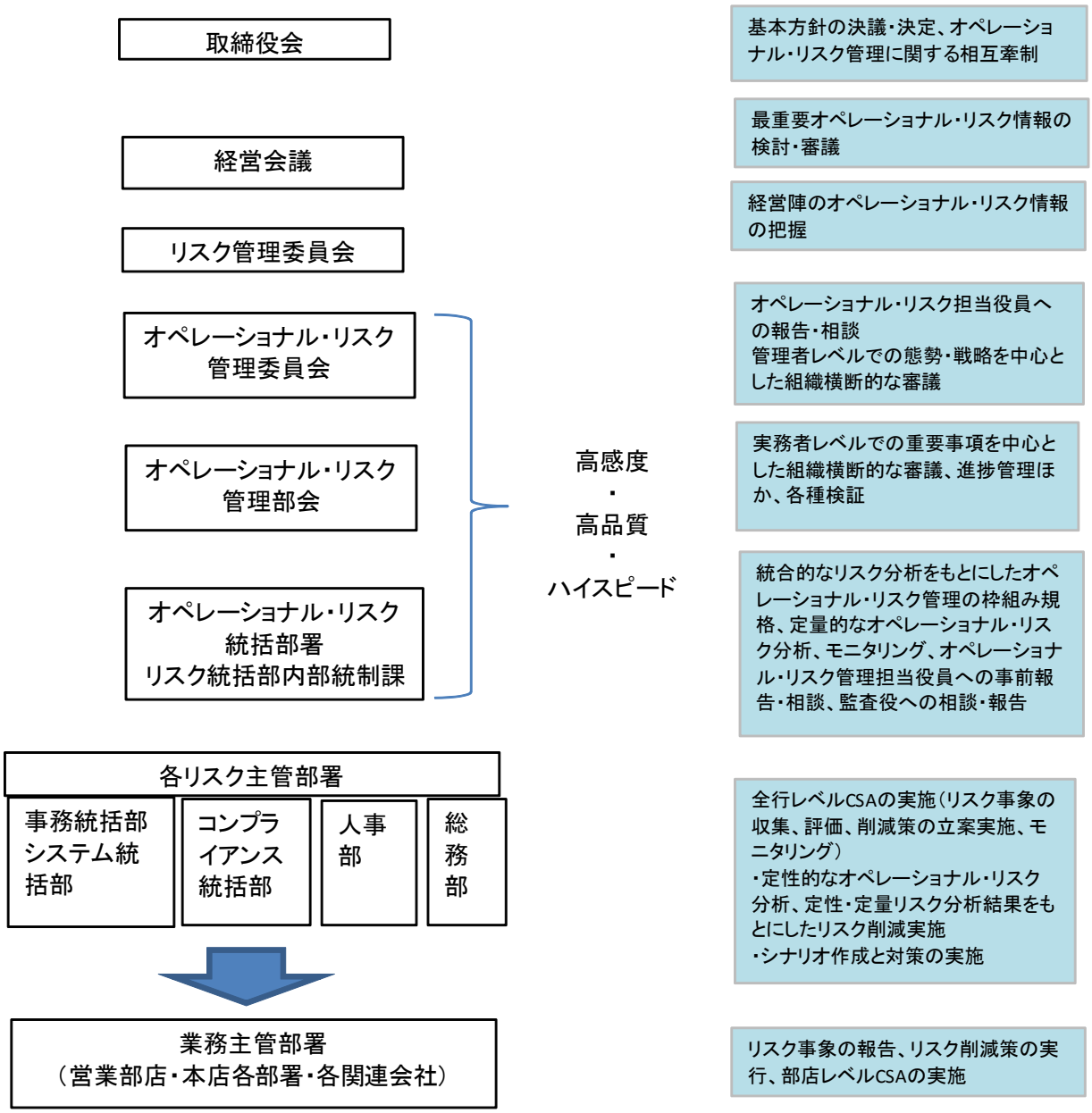
オペレーショナル・リスク分析レポートは、業務環境変化を自行データだけでなく、他行の内部損失データや大学の研究室から入手する係争中案件とも照らし合わせたうえで、近い将来発生するリスク事象の予測を実施し、その影響度を適正に見積もったうえで重大リスク事象を特定・評価している点に特徴がある。遠い将来よりも近い将来発生すると考えられるリスク事象を重要であると認識し、予測する内容に重点を置いてある理由については、銀行の中期経営計画が 3 年や 5 年単位で作成されている状況では、数年・数十年以内に相当な確立で発生するリスク事象の想定に優先的にパワーをかけて精緻に把握したほうが行内のコンセンサスも得やすく、リスク削減活動のスピード化が図りやすいとされるためである。

また、リスク事象が改善すべき脆弱なプロセスとともにみえるようにすること、これに対してリスク削減提言という付加価値をつけて公開することで、各リスク主管部署がリスク削減活動と直結させやすいオペレーショナル・リスク分析レポートを設計している点にも特徴があるといえる。具体的には、重大と認識したリスク事象については、その発生原因を、プロセスに対する視点、コントロールの視点をはじめとする 5 つの視点から分析し、それぞれの分析結果をもとにしてリスク削減強度（発生ゼロ、発生抑制等）に応じた 3 段階のリスク削減策を設計し、費用対コストを加味したリスク許容量の観点から 1 つのリスク削減策を選定して提言する仕組みを構築している。このリスク削減提言は、BPR を軸としたものに限定し、注意喚起文書の発信や勉強会の開催等による啓蒙のようなリスク削減の継続性が担保されないその場しのぎのリスク削減を提言するものではなく、さらに提言事項に対する各リスク主管部署での対応方針を吟味し、その進捗管理を行っている点からも、オペレーショナル・リスク統括部署のスキルや存在価値が問われる最も重要な業務として位置づけられている。

オペレーショナル・リスク管理委員会運営やオペレーショナル・リスク分析レポート作成に必要なリスク感応度を維持・向上させるためには、各種リスク報告書の検証・管理を皮切りにしてオペレーショナル・リスク統括部署が担当している業務のすべてを完全に実施することが必要不可欠である。これは、オペレーショナル・リスク統括部署が担当している業務知識の何れかが欠けた場合には、オペレーショナル・リスク管理委員会の運営およびオペレーショナル・リスク分析レポートの作成が不可能

となることから、オペレーショナル・リスク統括部署の担当者が自ら率先して分析や管理業務にあたることを義務付けている。

図表 4. オペレーショナル・リスク管理体制



（出典：瀧本・稲葉（2011））

5.3.2 オペレーショナル・リスク管理の仕組整備

また従来から実施されてきたオペレーショナル・リスク管理の仕組整備として、オペレーショナル・リスクを特定・評価・把握・削減・管理するための仕組強化の取組みとしてオペレーショナル・リスクデータの一元管理、重要度を決定する基準、シナリオ作成、リスク削減実施効果のモニタリング管理（効果検証）、オペレーショナル・リスク削減活動管理があげられる。

オペレーショナル・リスクデータの一元管理のための手段として、自行設計によるオペレーショナル・リスク報告書管理システムを導入している。システムを構築するにあたっては、既存の事務ミス記録書、苦情トラブル記録簿、システム障害記録簿の項目の見直しを行い、追加項目については、リスク特定、リスク評価、リスク把握、モニタリングまでの PDCA を可能な限り担わせること、長期化するオペレーショナル・リスク事象の管理や監督当局等の検証対応を容易にすることを最低限の要件として設計している。システム構築にあたって、リスク評価を行う基礎となる仕分け分類の中身を構成する仕分け項目の設定に最も注力しており、仕分け→集計→分析結果からみた仕分け項目の有効性評価→仕分け項目の修正→集計→分析結果からみた仕分けの有効性評価を繰り返すことで、仕分け分類の組合せによるメリットを十分に引き出すことができ、結果として当初 5000 個以上あった業務分類の項目は 243 項目に、1000 個以上あった工程分類の項目は 25 項目、無限大であった事象項目を 70 項目に整理し、各項目も事例も掲載して詳細に定義することで、集計時の有効性を向上させるだけでなく、仕分け時間の短縮と仕分けのブレ防止を同時に実現できる仕組みとなっている。

重要度を決定する基準として、一般的に重要なリスク事象に、発生件数の多いリスク事象、発行時の損失金額の大きいリスク事象、自行では発生していないものの、他行で実際に起きたリスク事象、新たに発生し始めたリスク事象などがある。これらを参考にして、重要なリスク事象を判定するための統一基準とリスク削減の優先順位づけに使用する複数の個別目線の基準を設計し活用することで、顧客保護の目線とリスク量の目線を重視したリスク評価を実現している。

シナリオについては、数年先に生起するものから 1000 年以上先に生起する可能性があるものまで網羅的に想定することとしているが、リスク削減活動からみた重要なシナリオという観点から、各種研究機関から入手する地震や津波の発生規模・発生確率や店舗倒壊率から銀行が被るリスク量を想定している有形資産リスクについては、主要リスクとして精緻に研究している。それ以外では、数年先、数十年先に必ず生起するシナリオを重要なシナリオと位置づけている。

リスク削減実施効果のモニタリングとして、オペレーショナル・リスク統括部署では、リスク主管部署が実施したリスク削減策の実施効果を数値で評価する方策を採用している。この方法により、従来はリスク削減策実施の有無のみで評価していた管理から、実効性を管理する方法への転換を図っている。

オペレーショナル・リスク削減活動では、定量的な指標に基づくリスク削減活動と定性的な指標に基づくリスク削減活動を実施している。

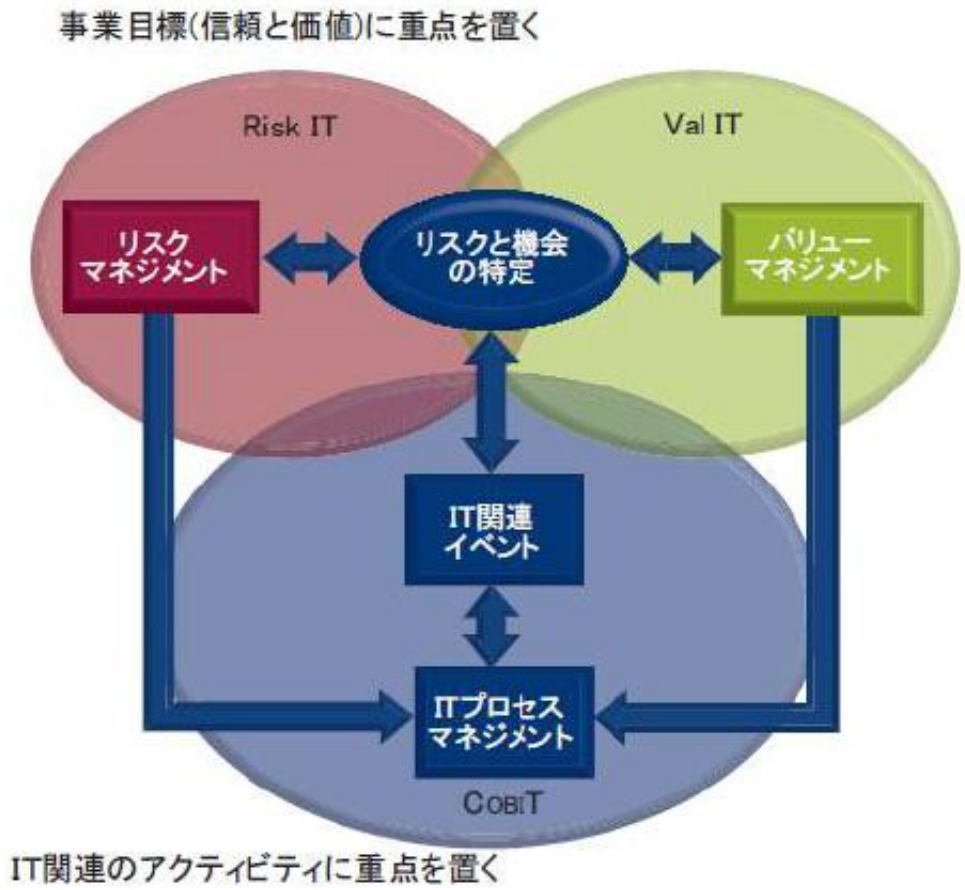
このことから、銀行のオペレーショナル・リスク管理体制では、オペレーショナル・リスク統括部門において、ペレーショナル・リスク管理に係る統制、プロセスおよびシステムについて独立した検証と評価まで行われており、本来内部監査部門に期待される独立した検証と評価が行われておらず、内部監査部門が第 3 の防衛線として必ずしも十分に機能していないのではないかと考えられる。

６．システムリスク管理について

「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金融機関が損失を被るリスク、さらにコンピュータが不正に利用されることにより金融機関が損失を被るリスクをいう（預金等受入金融機関に係る検査マニュアル)。適切な情報技術（IT）は、オペレーショナル・リスク管理のフレームワークの基礎であり、またこれを推進するものである。IT システムは、広範なオペレーショナル・リスク情報に対応するとともに、さまざまな内部システムおよび外部情報と連携しなければならない。

企業が IT に関連するリスクを管理することを支援するために情報システムコントロール協会（ISACA）と IT ガバナンス協会（ITGI）は、世界中の組織に IT ガバナンスのための明確な方針とより良い実務を提供するために IT カバナンスの枠組みと詳細なコントロール目標のガイドを示す Control Objectives for Information and related Technology (COBIT)の初版を 1996 年に発表した。また COBIT を補完する形(図表６)で RISK　IT フレームワークと Val　IT フレームワークが発表されている。

図表 6. COBIT、Val IT、Risk IT の位置づけ



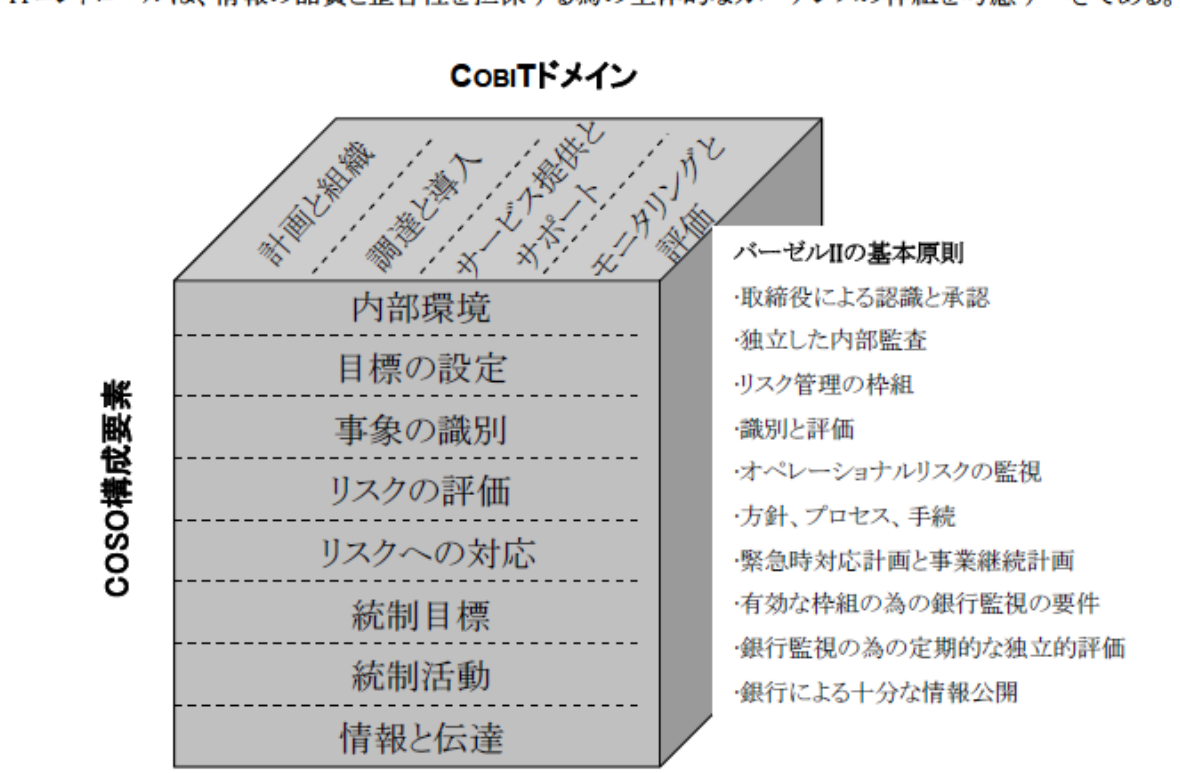
（出典：「RISK IT フレームワーク日本語版」日本 IT ガバナンス協会）

6.1　COBIT と ERM およびバーゼルⅡの対応関係について

COBIT は、金融機関に対して、全社レベルの統制に関する、戦略的な視点を持った、総合的な一連の統制目標を提供している。COBIT は、IT のリスクとコントロールのガバナンスに関するマネジメントのための統合的フレームワークであり、4 つのドメイン（計画と組織、調達と導入、サービス提供とサポート、モニタリングと評価）、34 の IT プロセス、200 を超える統制目標によって構成されている。COBIT は、組織レベルと活動レベルの両方の目的を、関連するコントロールと合わせて提供しており、COSO やその他のガバナンスのフレームワークに対して、IT に関する構成要素を補完するものとして、世界中の組織で広く利用されている。前述のとおり、バーゼルⅡは 10 の基本原則、COSO-ERM は 8 つの構成要素に区分された内部統制がある。バーゼルⅡにおけるオペレーショナル・リスク管理の目的を達成するためには、このすべてが実施され、統合されている必要があることが図表 7 からわかる。図表 7 は、バーゼルⅡの基本原則、および COSO の構成要素および、COBIT のドメインとの関係を示し

ており、COBIT の多くの IT プロセスは、2 つ以上のバーゼルⅡおよび COSO の構成要素と関連している。

図表 7. COSO-ERM と COBIT のクロスリファレンス



（出典：バーゼルⅡのための IT 統制目標）

6.2 オペレーショナル・リスクと IT の対応関係

アプリケーション、インフラストラクチャの各要素、および統制など、IT に関連する部分は、全てオペレーショナル・リスクの一部として定義されている。図表 8 は、オペレーショナル・リスクに関するバーゼルⅡの原則、それに対応する COSO ERM の構成要素、ならびに IT への関連性と要求事項を示している。

図表 7. バーゼルⅡの原則、COSO の構成要素、IT への関連性と要求事項

バーゼルⅡの原則	COSO の構成要素	IT への関連性と要求事項
原則 1： 取締役会は、個別に管理すべきリスクカテゴリーの１つとして、銀行におけるオペレーショナル・リスクの主な状況を認識し、銀行のオペレーショナル・リスク管理フレームワークの承認、および定期的な見直しを行うべきである。このフレームワークでは、銀行全体としてのオペレーショナル・リスクを定義し、その識別、評価、モニタリング、および統制と低減に関する原則を提供すべきである。	内部環境	IT は、全般的なリスク管理プロセスの一部に統合すべきである。
原則 2： 取締役会は、銀行のオペレーショナル・リスク管理のフレームワークを、業務から独立し、必要な教育を受けた適切な要員による、効果的かつ包括的な内部監査の対象とすべきである。内部監査部門は、オペレーショナル・リスク管理に、直接の責任を負うべきではない。	モニタリング	IT を含む金融機関のオペレーショナル・リスク管理のフレームワークは、内部監査計画の対象とすべきである。 IT 内部監査部門には、適切なスキルを備えた要員を配置すべきである。この要員は、バーゼルⅡ、リスク管理の原則、金融機関に対する規制および監督上の要求事項について理解すべきである。 IT 内部監査部門は、金融機関の監督当局によるレビューの対象とすべきである。適切な場合、外部の専門家を利用すべきである。
原則 3： マネジメントは、取締役会に承認されたオペレーショナル・リスク管理のフレームワークの導入に関して、責任を負うべきである。フレームワークは銀行全体を対象として導入されるべきであり、また、全ての階層の従業員が、オペレーショナル・リスク管理におけ	内部環境 情報と伝達	IT 部門の幹部は、経営陣と同等の責任を負う。 銀行で採用されたフレームワークは、IT に関する要求事項を満たすよう、適合させるべきである（最も一般的な GRC（コンプライアンス） フレームワークは、IT について、詳細には解説していない）。金融機関の GRC フレームワークに適合し

る自身の役割について理解すべきである。マネジメントは、銀行の主要な商品、活動、プロセスおよびシステムにおけるオペレーショナル・リスクの管理方針、プロセスおよび手続の策定にも責任を負うべきである。		た、IT 統制のフレームワークを導入することも考えられる。 採用されたフレームワークは、金融機関の監督当局と検査官が対象とする可能性がある範囲を網羅しているべきである。例えば、IT コーポレート・ガバナンス、IT 計画と組織、セキュリティ、システム開発、プログラム変更、運営とサポート、内部統制に関する責任などがある。
原則 4： 銀行は、全ての主要な商品、活動、プロセス、システムにかかわるオペレーショナル・リスクを識別し、評価すべきである。銀行は、新しい商品、活動、プロセス、システムの導入前、または実施前に、オペレーショナル・リスクについて、適切な評価を行うようにすべきである。	目的の設定 事象の識別 リスクの評価	リスク評価は、銀行に大きな影響を及ぼす可能性がある全ての IT 活動、例えば、プログラム変更、インフラストラクチャ変更、またセキュリティモニタリングなどについて行うべきである。 リスク評価は、システム開発とリリース管理のプロセスに統合すべきである。 重大な影響を受ける可能性のある利害関係者は、リスク評価に関与すべきである。 リスク評価の結果は、その他のリスク評価の結果と統合されて、GRC フレームワークに盛り込まれるべきである。
原則 5： 銀行は、オペレーショナル・リスクの状況と、損失につながる可能性がある重大なエクスポージャについて、定期的に監視するプロセスを導入すべきである。オペレーショナル・リスクを積極的に管理するための情報を、経営陣と取締役会に対して定期的に報告すべきである。	事象の識別 リスクの評価 情報と伝達	オペレーショナル・リスクの評価を、年間計画と戦略計画のサイクルに含むべきである。オペレーショナル・リスクは、組織内外で重要な事象が発生した場合には、再評価すべきである。例えば、災害が発生したときに、コンティンジェンシープランを見直すことなどがある。 リスクの評価指標を識別し、監視すべきである。望ましくない兆候が発見された場合、原因調査を実施し、的確な対策をとらるべきである。
原則 6： 銀行は、重大なオペレーショナル・リ	リスクへの対応	オペレーショナル・リスクを低減するために、IT 内部統制のフレームワークを構

スクの統制と低減のいずれか、または両方を行うための方針、プロセスおよび手続を策定すべきである。銀行は、リスク制限とコントロール戦略を定期的に見直し、適切な戦略を用いて、リスク選好とリスク・プロファイル全体の観点に基づいて、オペレーショナル・リスクに関する現状認識を修正すべきである。	内部環境 情報と伝達 統制活動	築すべきである。 IT 内部統制のフレームワークを、適切な方針、プロセス、手続によって確立すべきである。 オペレーショナル・リスクは、組織内外で重要な事象が発生した場合には、再評価すべきである。例えば、他の銀行を買収したときに、システム統合がオペレーショナル・リスクに与える影響について検討することなどがある。 IT に関する方針と手続を、最低年に 1 回、見直し、承認すべきである。
原則 7： 銀行は、重大な業務の中断が発生した場合にも事業を継続し、損失を最小化できるよう、コンティンジェンシープランおよび事業継続計画を策定すべきである。	リスクへの対応	IT 部門は、全社事業継続計画と事故対応管理に対応した、IT に関する継続計画と管理手続を策定すべきである。
原則 8： 監督当局は、全ての銀行に対して、リスク管理に関する全体的な取り組みの一部として、主要なオペレーショナル・リスクの識別、評価、モニタリング、および統制/低減を行うための効果的なフレームワークを確立することを求めるべきである。	モニタリング	IT 部門は、金融機関の監督当局の要求事項に対応した、IT リスク管理のフレームワークを導入すべきである。
原則 9： 監督当局は、オペレーショナル・リスクに関する銀行の方針、手続および実務に対する、直接的または間接的な独立的評価を、定期的に実施すべきである。監督当局は、銀行の対応状況を継続的に把握する仕組みを構築すべきである。	モニタリング	IT 部門の幹部は、IT に関する監督上のコンプライアンス要件が、オペレーショナル・リスクおよび監督当局の要求事項に対応するための組織全体の方針と手続に、確実に統合されるようにすべきである。また検査官が発見した不備については、適時に対応が行われるようにすべきである。 IT コンプライアンス担当部門は、監督当局が、IT に関する対応状況を継続的に把

		握できるように、金融機関のコンプライアンス部門に統合すべきである。
原則 10： 銀行は、市場参加者がオペレーショナル・リスク管理に関するアプローチを評価できるように、十分な情報公開を行うべきである。	内部環境 情報と伝達	IT 部門は、主要なオペレーショナル・リスクを構成する全ての関連リスクを識別し、その内容を取締役会と経営陣に伝達すべきである。

（出典：バーゼルⅡのための IT 統制目標）

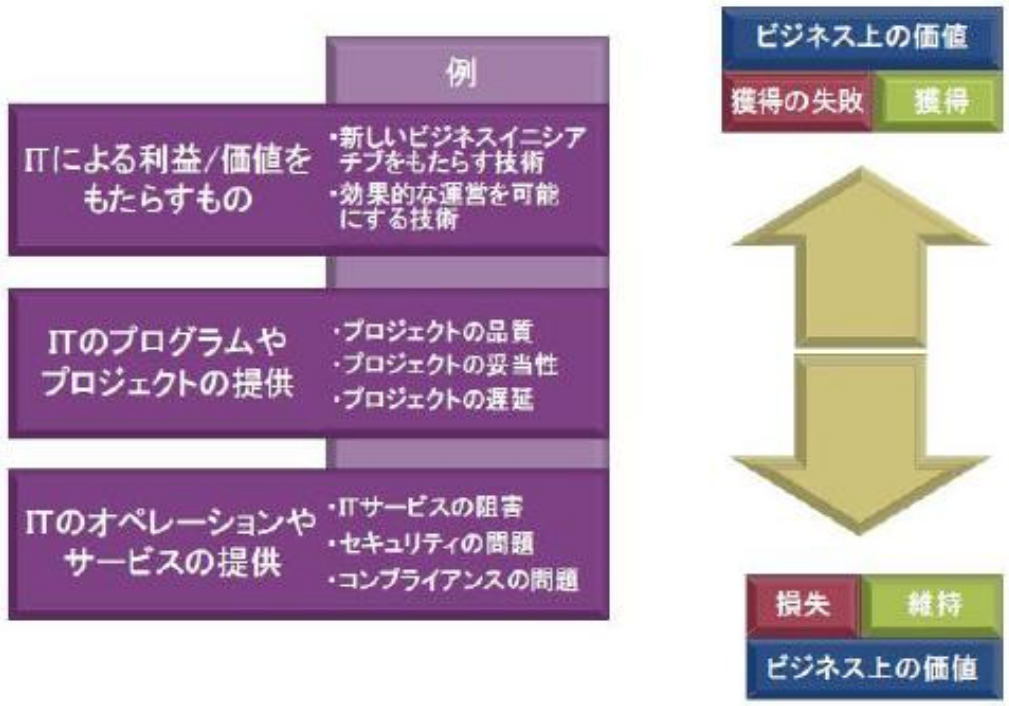
6.3 Risk IT フレームワーク及びその原則

Risk IT フレームワークは、COBIT を補完するもので、COBIT が IT リスクの低減につながる一連のコントロールの提供により、リスク・マネジメントのための手段のための優れた活動方針を規定しているのに対して、Risk IT は企業における IT リスクを特定、コントロールし、そして管理するためのフレームワークを提供することにより、その目的のための優れた活動方針を規定している。Risk IT フレームワークは、企業が IT ガバナンスを導入する際に役立てることができ、また既に IT ガバナンスのフレームワークとして、COBIT を採用している（あるいは採用を検討している）企業では、Risk IT を用いてリスク・マネジメントの機能を高めることができる。（「Risk IT フレームワーク 日本語版」）

COBIT のプロセスでは、企業内における全ての IT に関連する活動を管理する。これらのプロセスは、社内外におけるイベントに対応できなければならない。社内のイベントは、経営上の IT に関わるインシデント、プロジェクトの失敗、戦略の方向転換、企業の合併などを含む。社外のイベントには、市場環境の変化、新規競合の発生、利用可能となる新技術の出現、IT に影響を与える新しい法律・規則の制定などがある。これらのイベントは全てリスクリスクや機械をもたらすため、評価を行い、対応を図る必要がある。このうちリスクに関わる部分や、管理方法などが Risk IT フレームワークの主題である。

IT リスクとは、ビジネスリスクであり、具体的には、企業内における IT の利用や所有、オペレーション、関連、影響、適用に関連するビジネスリスクを示し、下図のように分類される。それはビジネスに影響を及ぼす IT に関連したイベントでもある。そのリスクは、不確定な頻度と大きさで発生し、戦略的な目標へ到達するための大きな障害となる。

図表 9. IT リスクの分類



（出典：「Risk IT フレームワーク日本語版」日本 IT ガバナンス協会）

また、Risk IT は、IT リスクを効果的に管理する複数の基本原則を定義しており、この基本原則の下に成り立っている(「Risk IT フレームワーク　日本語版」)。基本原則は、ERM の原則に基づいており、Risk IT のプロセスモデルは、企業が実践的に原則を適用し、または成果のベンチマークを行うことができるように設計、構造化されている。Risk　IT フレームワークは IT リスクについて記述されたものであり、IT の利用に関連したビジネスリスクといえる。ビジネスとの関連は、フレームワークが構築された原則のもとに成り立っている。すなわち、①常に事業目標と関連付けられる②適用可能であれば、ERM 全体と IT に関連するビジネスリスクの管理との整合性をとる③IT リスク・マネジメントにおけるコストと効果のバランスを保つ④IT リスクの公正でオープンなコミュニケーションを促進する。⑤経営上層部が適切な風土を確立し、同時に受容可能で十分に定義された許容レベルで運用するために個人の責任を定義し守らせる⑥継続的なプロセスと日常的活動の一部とするといった原則を示すことで、図表 10 に示すように効果的な企業ガバナンスと IT リスクの管理が可能となる。

図表 10. Risk IT の原則

（出典：「Risk IT フレームワーク日本語版」日本 IT ガバナンス協会）

Risk IT フレームワークは、これらの原則の下に構築され、さらに包括的なプロセスモデルへと展開されている。リスク・マネジメントのプロセスモデルは主要なアクティビティを複数のプロセスにグループ化しており、これらのプロセスは、３つのドメイン（リスクガバナンス、リスク評価、リスク対応）にグループ化されている。

図表 11. Risk IT フレームワーク

（出典：「Risk IT フレームワーク日本語版」日本 IT ガバナンス協会）

6.4　Val IT フレームワーク及びその原則

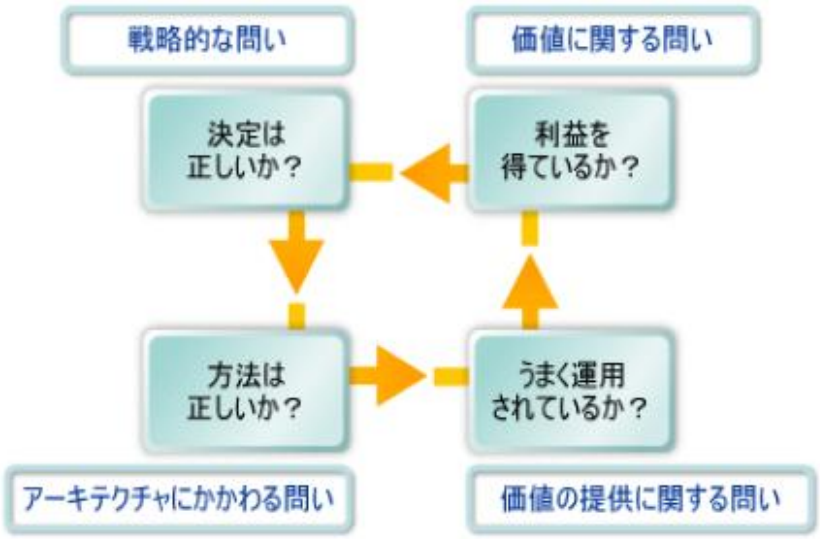
Val IT フレームワークとは、IT 関連の投資に基づいた事業価値の創出を支援する、実践に即して体系化された包括的な枠組みである。COBIT との整合性を維持し、これを補完する目的で策定された Val IT には、取締役会、経営幹部チーム、その他の企業の指導者層が、IT 投資による価値の実現を最適化できるように、実践に即した実証済みのガバナンス原則、プロセス、施策およびこれらを支援するガイドラインが統合されている。（「Val IT フレームワーク日本語版」）

Val IT は COBIT を補完するものであり、COBIT によってサポートされる関係にある。Val IT は企業ガバナンスの観点からアプローチしており、これにより経営陣は、IT ガバナンスに対する 4 つの基本的な問いのうち、「正しいことをおこなっているか」（戦略面での問い）と「効果が得られているか」（価値の面での問い）という 2 点に焦点を合わせることができる。一方 COBIT では IT の観点からアプローチしており、「実

施方法は正しいか」（アーキテクチャ面での問い）と「首尾よく行っているか」（価値の提供に関する問い）という問いへの答えに焦点を合わせることができる。

COBIT は IT を基盤とした高品質なサービスを設計と提供を支援する包括的なフレームワークとして、IT 部門での価値創出プロセスに貢献するための手段について、優れた活動指針を定めているが、Val　IT では、企業が IT 関連の投資から得られる価値を、財務および非財務の両面から、測定、監視、最適化できるように、目的、すなわち成果に関する優れた活動指針を定めている。

図表 12. IT ガバナンスに関する 4 つの問い



（出典：「Val IT フレームワーク日本語版」日本 IT ガバナンス協会）

Val　IT は、一連の指針となる原則と、その原則に準拠した数々のプロセスで構成される。このプロセスは、さらに重要な管理政策をいくつかまとめて定義され、これらの原則、プロセス、施策の間にある関係は次のようになる。すなわち、Val　IT が支援する企業の達成目標は、負担可能なコストと許容可能レベルのリスクで、IT 関連の投資から最適な価値を創出することで、その目標を達成するための指針が、バリューマネジメントプロセスに適用する一連の原則であり、実現する手段として重要な管理政策が用いられ、評価項目として達成目標に対する成果と測定指標が適用される。

Val　IT には次のような原則がある。それは、IT 関連の投資について、①投資のポートフォリオ（最適保有率）として管理する。②事業価値を達成する上で必要となるアクティビティがすべて含まれる。③経済的ライフサイクル全体を通じて管理する。また、価値の提供の施策について、(1) 投資にはさまざまな分類があるので、評価と管理の方

法をそれぞれに変えて行う。(2) 主要な測定指標を定義し監視して、どのような変更や逸脱にも迅速に対応できるようにする。(3) 能力の提供と事業面の効果が実現されるように、すべての利害関係者を関与させ、適切な説明責任を割り当てる。(4) 継続的に監視、評価および改善を行う。というものである。

企業が IT 関連の投資から、負担可能なコストと許容可能レベルのリスクで、最適な価値を実現できるようにするという、Val　IT によるバリューマネジメントの達成目標を果たすためには、Val　IT の原則を価値ガバナンス、ポートフォリオ管理、投資管理の 3 つのドメインに適用する必要がある。

価値ガバナンスの目標は、バリューマネジメント手順が企業内に確実に組み込まれ、経済的ライフサイクル全体を通じて、IT 関連の投資から最適な価値を確実に創出できるようにすることにある。ポートフォリオ管理の目標は、Val　IT フレームワークの文脈の中では、IT 関連の投資のポートフォリオを通じて、企業が最適な価値を確実に創出できるようにすることである。また、投資管理の達成目標は、企業の個々の IT 関連の投資が、最適な価値に確実に貢献できるようにすることである。

6.5　システムリスク管理に対する規制

銀行の経営再編に伴うシステム統合や新商品・サービスの拡大等に伴い、銀行の情報システムは一段と高度化・複雑化し、さらにコンピュータのネットワーク化の拡大に伴い、重要情報に対する不正なアクセス、漏えい等のリスクが大きくなっている。仮に銀行でシステム障害が発生した場合は、利用者の社会経済生活、企業等の経済活動、ひいては、我が国経済全体にも極めて大きな影響を及ぼすおそれがあるほか、その影響は単に一銀行の問題にとどまらず、金融システム全体に及びかねないことから、システムが安全かつ安定的に稼働することは決済システム及び銀行に対する信頼性を確保するための大前提であり、システムリスク管理態勢の充実強化は極めて重要であるとされている（主要行等向けの総合的な監督指針）。同監督指針では、システムリスク管理について監督を行うにあたっての着眼点を次のように記述している。

（１）システムリスクに対する認識等

システムリスクについて経営者をはじめ、役職員がその重要性を十分認識し、定期的なレビューを行うとともに、全行的なリスク管理の基本方針が策定されているか。

（２）システムリスク管理態勢

取締役会は、コンピュータシステムのネットワーク化の進展等により、リスクが顕在化した場合、その影響が連鎖し、広域化・深刻化する傾向にあるなど、経営に重大な影響を与える可能性があるということを十分踏まえ、リスク管理態勢を整備しているか。

システムリスク管理の基本方針が定められているか。システムリスク管理の基本方針には、セキュリティポリシー（組織の情報資産を適切に保護するための基本方針）及び外部委託先に関する方針が含まれているか。システムリスク管理体制の整備に当たって

は、その内容について客観的な水準が判定できるものを根拠としているか。また、システムリスク管理体制は、システム障害等の把握・分析、リスク管理の実施結果や技術進展等に応じて、不断に見直しを実施しているか。

（３）安全対策

① 安全対策の基本方針が策定されているか。

② 定められた方針、基準及び手順に従って安全対策を適正に管理する安全管理者を設置しているか。安全管理者は、システム、データ、ネットワークの管理体制を統括しているか。

③ 銀行以外の者が占有管理する端末機等（入出力装置等を含む。）を利用する資金移動取引については、コンピュータシステムの事故防止対策、不正使用防止対策、不正アクセス防止対策、取引者のプライバシー保護対策が施されているか。

（４）システム監査

① システム部門から独立した内部監査部門が、定期的にシステム監査を行っているか。

② システム監査に精通した要員を確保しているか。

③ 監査対象は、システムリスクに関する業務全体をカバーしているか。

④ システム監査の結果は、適切に経営者に報告されているか。

（５）外部委託管理

システムに係る外部委託業務について、リスク管理が適切に行われているか。特に外部委託先（システム子会社を含む。）が複数の場合、管理業務が複雑化することから、より高度なリスク管理が求められることを十分認識した体制となっているか。システム関連事務を外部委託する場合についても、システムに係る外部委託に準じて、適切なリスク管理を行っているか。

（６）データ管理態勢

① データについて機密性等の確保のため、データ管理者を置いているか。

② データ保護、データ不正使用防止、不正プログラム防止策等について適切かつ十分な管理態勢を整備しているか。

（７）コンティンジェンシープラン

① コンティンジェンシープランが策定され、緊急時体制が構築されているか。

② コンティンジェンシープランの策定に当たっては、その内容について客観的な水準が判断しうるものを根拠としているか。

（８）障害発生時の対応

① 顧客に対し無用の混乱を生じさせないよう、適切な措置を講じているか。

② 障害が発生した場合、障害の内容・発生原因、復旧見込等について公表するとともに、顧客からの問い合わせに的確に対応するため、必要に応じ、コールセンターの開設等を迅速に行っているか。また、障害の発生原因の究明、復旧までの影響調査、改善措置、再発防止策等を的確に講じているか。

さらに、システム障害に対する監督手法・対応について以下のように定められている。

（1）障害発生時

① 一般的な対応

イ．コンピュータシステムの障害の発生を認識次第、直ちに、その事実を当局宛てに報告を求めるとともに、「障害等発生報告書」にて当局宛て報告を求めるものとする。また、復旧時、原因解明時には改めてその旨報告を求めることとする。ただし、復旧原因の解明がされていない場合でも、1か月以内に現状についての報告を行うこととする。

ロ．必要に応じて法第 24 条に基づき追加の報告を求め、重大な問題があると認められる場合には、法第 26 条に基づき業務改善命令を発出するものとする。

② 緊急対応

特に、大規模な障害の場合や障害の原因の解明に時間を要している場合等には、直ちに、障害の事実関係等についての一般広報及び店頭等における顧客対応等のコンティンジェンシープランの発動状況をモニタリングするとともに、迅速な原因解明と復旧を要請し、法第 24 条に基づき速やかな報告を求める。

さらに、大規模な障害の復旧の見通しが不確実であり、市場取引、ＡＴM取引・口座振替・給与振込等の決済システムに大きな影響が生じている場合には、早期に法第 26 条に基づく業務改善命令を発出することを検討する等の対応を行う。

7．まとめ

オペレーショナル・リスクは、信用リスクなど銀行業務におけるその他のリスクと異なり、損失の一方で利益が期待できるものではない。しかし、2011 年 3 月に発生したみずほ銀行のシステム障害の事例[5]からもわかるように、問題が発生した場合に国民生活に与える影響は甚大である。そのような事態を引き起こさないためにもシステムリスクをはじめとした日々のオペレーショナル・リスク管理は非常に重要なものであるといえる。バーゼル銀行監督委員会が公表しているオペレーショナル・リスク管理諸原則では、内部監査部門がオペレーショナル・リスク管理に係る統制、プロセスおよびシステムについて独立した検証と評価を行うことを第 3 の防衛線と位置付け、強固なオペレーショナル・リスク管理のための重要な要件としている。しかし、実際の銀行オペレーショナル・リスク管理態勢をみると、オペレーショナル・リスクを総合的に管理する部署としては、営業部門だけでなく、オペレーショナル・リスクを構成するすべてのリスク種類からも独立したオペレーショナル・リスク統括部署を設置し、検証やモニタリングを実施ており、内部監査部門が第 3 の防衛線として必ずしも十分に機能していないのではないかと考えられる。

銀行は決済業務などを通じて国民生活に密接に関わっており、システムに障害が発生

[5] システム障害はなぜ二度起きたか（日経コンピュータ 2011）によると、給与振り込みも含めた振り込みの積み残しが 120 万件発生し、ATM の全面停止などの事態に発展した。

した場合は多大な影響を与えるとともに、他の銀行に影響が波及することもあるためオペレーショナル・リスク管理には万全を期すべきであり、現在の管理態勢に加え、内部監査部門を第 3 の防衛線として積極的に活用し、独立・客観的な立場からオペレーショナル・リスク管理についての検証やモニタリング業務を行わせるべきである。このような銀行の態勢強化は、金融機関の自主的な努力を尊重しつつ、業務の健全かつ適切な運営を確保することを目的とする監督当局の方針とも整合的であるといえる。

また、内部監査部門が強化されることで、銀行に対する検査を実施する際に、内部監査部門から監督当局に現状の問題点を提供することなどのよって、監督当局との意見交換の際により多くの情報の提供が期待できる。[6]このことからも内部監査部門が強化されることは、結果として銀行監督行政の効率化に寄与するといえる。

[6] 主要行等向けの総合的な監督指針では、銀行のリスク管理やコンプライアンスの状況等について、年 1 回ヒアリングを実施すると定めている。その際、銀行の内部監査部門の役割、内部監査の実施状況、今後の課題等についてもヒアリングを行うこととなっている。

（参考文献）

企業会計審議会（2005）「財務情報等に係る保証業務の概念的枠組みに関する意見書」
http://www.fsa.go.jp/news/newsj/16/singi/f-20041129-1/01.pdf
金融庁（2011）「金融庁の 1 年平成 22 事務年度版」
http://www.fsa.go.jp/common/paper/22/zentai/00.pdf
金融庁（2011）「主要行等向けの総合的な監督指針」
金融庁（2012）「預金等受入金融機関に係る検査マニュアル」
金融庁（2000）「銀行組織の内部監査、および監督当局と内部監査の関係（仮訳）」
http://www.fsa.go.jp/inter/bis/bj_20000726.pdf
金融庁（2011）「健全なオペレーショナル・リスク管理のための諸原則（仮訳）」
http://www.fsa.go.jp/inter/bis/20110708-1/01.pdf
金融庁（2008）「バーゼルⅡ（新しい自己資本比率規制）について」
http://www.fsa.go.jp/policy/basel_ii/00.pdf
佐藤隆文（2007）『バーゼルⅡと銀行監督』東洋経済新報社
山本真一・足立光年（2011）『バーゼル銀行監督委員会による「健全なオペレーショナル・リスク管理のための諸原則」の公表について』月刊監査研究
瀧本和彦・稲葉大明（2011）『【実践】オペレーショナル・リスク管理』金融財政事情研究会
田邉政之・作井博・桑原大祐・八ツ井博樹・久永健生・小西（2009）『バーゼルⅡ対応のすべて』金融財政事情研究会
日経コンピュータ（2011）『システム障害はなぜ二度起きたか』日経 BP 社
日本 IT ガバナンス協会（2008）『バーゼルⅡのための IT 統制目標』
http://itgi.jp/download.html
日本 IT ガバナンス協会（2011）『Risk　IT フレームワーク』
http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx
日本 IT ガバナンス協会（2011）『Val　IT フレームワーク 2.0』
http://itgi.jp/download.html
日本内部監査協会（2006）　『内部監査基準実践要綱』
http://www.iiajapan.com/pdf/guide/IIAJ-PAh18.pdf
COSO（2004）, *Enterprise Risk Management - Integrated Framework*
（八田進二訳（2006）『全社的リスク・マネジメント フレームワーク篇』東洋経済新報社）

International Federation of Accountants (2010) *Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncement*

（参考 HP）

金融庁　http://www.fsa.go.jp/

社団法人日本内部監査人協会　http://www.iiajapan.com/

日本 IT ガバナンス協会　http://itgi.jp/

日本銀行　http://www.boj.or.jp/

バーゼル銀行監督委員会　http://www.bis.org/bcbs/index.htm