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

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

【検証ポイント】

- オペレーショナル・リスクとは、金融機関の業務の過程、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を被るリスク（自己資本比率の算定に含まれる分）及び金融機関自らが「オペレーショナル・リスク」と定義したリスク（自己資本比率の算定に含まれない分）をいう。
- オペレーショナル・リスクの総合的な管理とは、金融機関全体として総合的に、オペレーショナル・リスクを特定、評価、モニタリング、コントロール及び削減することをいう。
- 金融機関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・確立は、金融機関の業務の健全性及び適切性の観点から極めて重要であり、経営陣には、これらの態勢の整備・確立を自ら率先して行う役割と責任がある。
- 検査官は、オペレーショナル・リスクの総合的な管理態勢を検証するに当たっては、金融機関の業務の規模・特性及びリスク・プロファイルに加え、金融機関が採用しているオペレーショナル・リスク定量（計量）化手法（基礎的手法、粗利益配分手法も含む。）の複雑さや高度化の水準に見合った適切なオペレーショナル・リスクの総合的な管理態勢が整備されているかを検証することが重要である。

  なお、金融機関が採用すべきオペレーショナル・リスク定量（計量）化手法の種類や水準は、金融機関の戦略目標、業務の多様性及び直面するオペレーショナル・リスクの複雑さによって決められるべきものであり、複雑又は高度なオペレーショナル・リスク定量（計量）化手法が、全ての金融機関にとって適切な方法であるとは限らないことに留意する。
- 検査官は、①方針の策定、②内部規程・組織体制の整備、③評価・改善態勢の整備がそれぞれ適切に経営陣によってなされているかといった観点から、オペレーショナル・リスクの総合的な管理態勢が有効に機能しているか否か、経営陣の役割と責任が適切に果たされているかをⅠ．のチェック項目を活用して具体的に確認する。
- Ⅱ．以降のチェック項目の検証において問題点の発生が認められた場合、当該問題点がⅠ．のいずれの要素の欠如又は不十分に起因して発生したものであるかを漏れなく検証し、双方向の議論を通じて確認する。
- 検査官が認識した弱点・問題点を経営陣が認識していない場合には、特に、態勢が有効に機能していない可能性も含めて検証し、双方向の議論を通じて確認する。
- 検査官は、前回検査における指摘事項のうち、軽微でない事項の改善状況について検証し、実効性ある改善策が策定され実行されているか否か確認する。

１．方針の策定

①【取締役の役割・責任】

取締役は、オペレーショナル・リスクの総合的な管理を軽視することが戦略目標の達成に重大な影響を与えることを十分に認識し、オペレーショナル・リスクの総合的な管理を重視しているか。特に担当取締役は、オペレーショナル・リスクの所在、オペレーショナル・リスクの種類・特性及びオペレーショナル・リスクの特定・評価・モニタリング・コントロール等の手法並びにオペレーショナル・リスクの総合的な管理の重要性を十分に理解し、この理解に基づき当該金融機関のオペレーショナル・リスクの総合的な管理の状況を的確に認識し、適正なオペレーショナル・リスクの総合的な管理態勢の整備・確立に向けて、方針及び具体的な方策を検討しているか。

②【オペレーショナル・リスク管理方針の整備・周知】

取締役会は、オペレーショナル・リスク管理に関する方針（以下「オペレーショナル・リスク管理方針」という。）を定め、組織全体に周知させているか。例えば、以下の項目について明確に記載される等、適切なものとなっているか。

- オペレーショナル・リスクの総合的な管理に関する担当取締役及び取締役会等の役割・責任
- 当該金融機関におけるオペレーショナル・リスクの定義
- オペレーショナル・リスクの総合的な管理に関する部門（以下「オペレーショナル・リスクの総合的な管理部門」という。）の設置、権限の付与等の組織体制に関する方針
- オペレーショナル・リスクの特定、評価、モニタリング、コントロール及び削減に関する方針

③【方針策定プロセスの見直し】

取締役会は、定期的に又は必要に応じて随時、オペレーショナル・リスクの総合的な管理の状況に関する報告・調査結果等を踏まえ、方針策定のプロセスの有効性を検証し、適時に見直しているか。

２．内部規程・組織体制の整備

①【内部規程の整備・周知】

取締役会等は、オペレーショナル・リスク管理方針に則り、オペレーショナル・リスクの総合的な管理に関する取決めを明確に定めた内部規程（以下「オペレーショナル・リスク管理規程」という。）をオペレーショナル・リスクの総合的な管理部門の管理者（以下本チェックリストにおいて単に「管理者」という。）に策定させ、組織内に周知させているか。取締役会等は、オペレーショナル・リスク管理規程についてリーガル・チェック等を経て、オペレーショナル・リスク管理方針に合

致することを確認した上で承認しているか。

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】

（ⅰ）取締役会等は、オペレーショナル・リスク管理方針及びオペレーショナル・リスク管理規程に則り、オペレーショナル・リスクの総合的な管理部門を設置し、適切な役割を担わせる態勢を整備しているか。[1]

（ⅱ）取締役会は、オペレーショナル・リスクの総合的な管理部門に、当該部門を統括するのに必要な知識と経験を有する管理者を配置し、当該管理者に対し管理業務の遂行に必要な権限を与えて管理させているか。

（ⅲ）取締役会等は、オペレーショナル・リスクの総合的な管理部門に、その業務の遂行に必要な知識と経験を有する人員を適切な規模で配置し、当該人員に対し業務の遂行に必要な権限を与えているか[2]。

（ⅳ）取締役会等は、オペレーショナル・リスクの総合的な管理部門から各業務部門に対する牽制機能が発揮される態勢を整備しているか。

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】

（ⅰ）取締役会等は、各業務部門及び営業店等に対し、遵守すべき内部規程・業務細則等を周知させ、遵守させる態勢を整備しているか。例えば、管理者に各業務部門及び営業店等が遵守すべき内部規程・業務細則等を特定させ、効果的な研修を定期的に行わせる等の具体的な施策を行うよう指示しているか。

（ⅱ）取締役会等は、管理者又はオペレーショナル・リスクの総合的な管理部門を通じ、各業務部門及び営業店等において、オペレーショナル・リスクの総合的な管理の実効性を確保する態勢を整備しているか。例えば、各業務部門及び営業店等にオペレーショナル・リスクの総合的な管理の担当者を配置し、管理者と連携させる等の工夫をしているか。

④【取締役会等への報告・承認態勢の整備】

取締役会等は、報告事項及び承認事項を適切に設定した上で、管理者に、定期的に又は必要に応じて随時、取締役会等に対し状況を報告させ、又は承認を求めさせる態勢を整備しているか。特に、経営に重大な影響を与える、又は顧客の利益が著しく阻害される事案については、取締役会等に対し速やかに報告させる態勢を整備しているか。

---

[1] オペレーショナル・リスクの総合的な管理部門を独立した態様で設置しない場合（例えば、他のリスク管理部門と統合した一つのリスク管理部門を構成する場合のほか、他の業務と兼担する部署がオペレーショナル・リスクの総合的な管理を担当する場合や、部門や部署ではなく責任者がオペレーショナル・リスクの総合的な管理を担当する場合等）には、当該金融機関の規模・特性及びリスク・プロファイルに応じ、その態勢のあり方が十分に合理的で、かつ、機能的な側面から見て部門を設置する場合と同様の機能を備えているかを検証する。

[2] 人員の配置及び権限の付与についての権限が取締役会等以外の部署・役職にある場合には、その部署・役職の性質に照らし、牽制機能が働く等合理的なものとなっているか否かを検証する。

⑤【監査役への報告態勢の整備】

取締役会は、監査役へ直接報告されるべき事項を特定した場合には、報告事項を適切に設定した上で管理者から直接報告を行わせる態勢を整備しているか。[3]

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、オペレーショナル・リスクの総合的な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。[4]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。

- オペレーショナル・リスクの総合的な管理態勢の整備状況
- オペレーショナル・リスク管理方針、オペレーショナル・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オペレーショナル・リスクの総合的な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

⑦【内部規程･組織体制の整備プロセスの見直し】

取締役会等は、定期的に又は必要に応じて随時、オペレーショナル・リスクの総合的な管理の状況に関する報告・調査結果等を踏まえ、内部規程・組織体制の整備プロセスの有効性を検証し、適時に見直しているか。

３．評価・改善活動

⑴ 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】

取締役会等は、監査役監査、内部監査及び外部監査の結果、各種調査結果並びに各部門からの報告等全てのオペレーショナル・リスクの総合的な管理の状況に関する情報に基づき、オペレーショナル・リスクの総合的な管理の状況を的確に分析し、オペレーショナル・リスクの総合的な管理の実効性の評価を行った上で、態勢上の弱点、問題点等改善すべき点の有無及びその内容を適切に検討するとともに、その原因を適切に検証しているか。また、必要な場合には、利害関係者以外の者によって構成された調査委員会等を設置する等、その原因究明については万全を期しているか。

②【分析・評価プロセスの見直し】

取締役会等は、定期的に又は必要に応じて随時、オペレーショナル・リスクの総合的な管理の状況に関する報告・調査結果等を踏まえ、分析・評価プロセスの有効

[3] このことは、監査役が自ら報告を求めることを妨げるものではなく、監査役の権限及び活動を何ら制限するものではないことに留意する。

[4] 内部監査計画についてはその基本的事項について承認すれば足りる。

性を検証し、適時に見直しているか。

(2) 改善活動

①【改善の実施】

取締役会等は、上記３．(1)の分析・評価及び検証の結果に基づき、必要に応じて改善計画を策定しこれを実施する等の方法により、適時適切に当該問題点及び態勢上の弱点の改善を実施する態勢を整備しているか。

②【改善活動の進捗状況】

取締役会等は、改善の実施について、その進捗状況を定期的に又は必要に応じて随時、検証し、適時適切にフォローアップを図る態勢を整備しているか。

③【改善プロセスの見直し】

取締役会等は、定期的に又は必要に応じて随時、オペレーショナル・リスクの総合的な管理の状況に関する報告・調査結果等を踏まえ、改善プロセスの有効性を検証し、適時に見直しているか。

Ⅱ．管理者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

【検証ポイント】

- **本章においては、管理者及びオペレーショナル・リスクの総合的な管理部門が果たすべき役割と負うべき責任について検査官が検証するためのチェック項目を記載している。**
- **Ⅱ．の各チェック項目の検証において問題点の発生が認められた場合、当該問題点がⅠ．のいずれの要素の欠如又は不十分に起因して発生したものであるかをⅠ．のチェックリストにおいて漏れなく検証し、双方向の議論を通じて確認する。**
- **検査官が発見した問題点を経営陣が認識していない場合には、特に上記Ⅰ．の各態勢及びその過程が適切に機能していない可能性も含め、厳格に検証し、双方向の議論を通じて確認する。**
- **検査官は、前回検査における指摘事項のうち、軽微でない事項の改善状況について検証し、実効性ある改善策が策定され実行されているか否か確認する。**

１．管理者の役割・責任

①【オペレーショナル・リスク管理規程の整備・周知】

管理者は、オペレーショナル・リスクの所在、オペレーショナル・リスクの種類・特性及びオペレーショナル・リスクの総合的な管理手法を十分に理解し、オペレーショナル・リスク管理方針に沿って、オペレーショナル・リスクの特定、評価及びモニタリングの方法を決定し、これに基づいたオペレーショナル・リスクのコントロール及び削減に関する取決めを明確に定めたオペレーショナル・リスク管理規程を策定しているか。オペレーショナル・リスク管理規程は、取締役会等の承認を受けた上で、組織内に周知されているか。

②【オペレーショナル・リスク管理規程の内容】

オペレーショナル・リスク管理規程の内容は、業務の規模・特性及びリスク・プロファイルに応じ、オペレーショナル・リスクの管理に必要な取決めを網羅し、適切に規定されているか。例えば、以下の項目について明確に記載される等、適切なものとなっているか。

- オペレーショナル・リスクの総合的な管理部門の役割・責任及び組織に関する取決め
- オペレーショナル・リスクの総合的な管理部門において、事務リスク管理部門及びシステムリスク管理部門等（以下「各オペレーショナル・リスク管理部門」という。）を総合的に管理する態勢に関する取決め
- オペレーショナル・リスク管理の管理対象とするリスクの特定に関する取決め
- オペレーショナル・リスクの定性的なリスク管理手法に関する取決め
- オペレーショナル・リスクの定量化の対象範囲及びその手法に関する取決め

・　オペレーショナル・リスクの総合的な管理部門に対する損失事象の報告態勢に関する取決め
・　オペレーショナル・リスクのモニタリング方法に関する取決め
・　取締役会等に報告する態勢に関する取決め
・　粗利益配分手法を採用している場合、「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（平成 18 年金融庁告示第 19 号)」（以下「告示」という。）別表第一の業務区分に粗利益を配分する際の手順及び当該手順を見直す基準に関する取決め

③【管理者による組織体制の整備】

（ⅰ）管理者は、オペレーショナル・リスク管理方針及びオペレーショナル・リスク管理規程に基づき、適切なオペレーショナル・リスクの総合的な管理を行うため、オペレーショナル・リスクの総合的な管理部門の態勢を整備し、牽制機能を発揮させるための施策を実施しているか。

（ⅱ）管理者は、統合的リスク管理に影響を与える態勢上の弱点・問題点等を把握した場合、統合的リスク管理部門へ速やかに報告する態勢を整備しているか。

（ⅲ）管理者は、統合的リスク管理方針等に定める新規商品等に関し、統合的リスク管理部門の要請を受けた場合、事前に内在するオペレーショナル・リスクを特定し、統合的リスク管理部門に報告する態勢を整備しているか。[5]

（ⅳ）管理者は、業務の規模・特性及びリスク・プロファイルに見合った信頼度の高いオペレーショナル・リスク管理システム[6]を整備しているか。

（ⅴ）管理者は、オペレーショナル・リスクの総合的な管理を実効的に行う能力を向上させるための研修・教育態勢を整備し、専門性を持った人材の育成を行っているか。

（ⅵ）管理者は、定期的に又は必要に応じて随時、取締役会等が設定した報告事項を報告する態勢を整備しているか。特に、経営に重大な影響を与える事案については、取締役会等に対し速やかに報告する態勢を整備しているか。

④【オペレーショナル・リスク管理規程及び組織体制の見直し】

管理者は、継続的にオペレーショナル・リスクの総合的な管理部門の職務の執行状況に関するモニタリングを実施しているか。また、定期的に又は必要に応じて随時、オペレーショナル・リスクの総合的な管理態勢の実効性を検証し、必要に応じてオペレーショナル・リスク管理規程及び組織体制の見直しを行い、又は取締役会等に対し改善のための提言を行っているか。

---

[5] 経営管理（ガバナンス）態勢－基本的要素－の確認検査用チェックリストⅠ．３．④を参照。

[6] システムには、中央集中型の汎用機システムや分散系システムのほか、EUC（エンド・ユーザー・コンピューティング）によるものも含まれることに留意する。

２．オペレーショナル・リスクの総合的な管理部門の役割・責任

⑴　オペレーショナル・リスクの特定・評価

①【オペレーショナル・リスクの特定】

（ⅰ）オペレーショナル・リスクの総合的な管理部門は、オペレーショナル・リスクを特定するために、必要に応じて各業務部門及び営業店等が把握したデータ等を取得しているか。

（ⅱ）オペレーショナル・リスクの総合的な管理部門は、オペレーショナル・リスクがあらゆる部署で顕在化する可能性があるという特性を理解した上で、オペレーショナル・リスク管理方針及びオペレーショナル・リスク管理規程に基づき、当該金融機関の業務運営上で悪影響を与える内外の要因を幅広く特定しているか。

（ⅲ）オペレーショナル・リスクの総合的な管理部門は、新規商品等の取扱い、新システムの導入、海外拠点・子会社での業務開始を行う場合には、オペレーショナル・リスクを特定しているか。

②【オペレーショナル・リスクの評価】

（ⅰ）オペレーショナル・リスクの総合的な管理部門は、スコアリング（ＣＳＡ等）、財務・経営指標等により、オペレーショナル・リスクを適切に評価しているか。

（ⅱ）オペレーショナル・リスクの総合的な管理部門は、オペレーショナル・リスクの評価を行う過程で、オペレーショナル・リスク損失事象の発生原因を分析し、当該金融機関のオペレーショナル・リスクを網羅的に把握しているか。

③【オペレーショナル・リスクの定量（計量）化】

オペレーショナル・リスクの総合的な管理部門は、当該金融機関の業務の規模・特性及びリスク・プロファイルに見合った、適切なオペレーショナル・リスクの定量（計量）化を行っているか。

（ⅰ）オペレーショナル・リスクの総合的な管理部門は、定量化手法として財務諸表の指標（粗利益、経費等）等に一定の掛目を掛けてオペレーショナル・リスク量を算出する場合、使用する指標の種類や掛目の水準を合理的に設定しているか。

また、スコアリング手法等により、オペレーショナル・リスクの総合的な管理水準の向上、内外環境の変化、影響の大きい内部損失の発生等に応じて、指標や掛目を適切に見直しているか。

（ⅱ）オペレーショナル・リスクの総合的な管理部門は、オペレーショナル・リスク計量手法を用いている場合は、本チェックリストⅢ．２の各項目に留意しているか。

⑵　モニタリング

①【オペレーショナル・リスクのモニタリング】

オペレーショナル・リスクの総合的な管理部門は、オペレーショナル・リスク管理方針及びオペレーショナル・リスク管理規程に基づき、当該金融機関の内部環境

（リスク・プロファイル等）や外部環境の状況に照らし、オペレーショナル・リスクの状況を適切な頻度でモニタリングしているか。

②【取締役会等への報告】

オペレーショナル・リスクの総合的な管理部門は、オペレーショナル・リスク管理方針及びオペレーショナル・リスク管理規程に基づき、オペレーショナル・リスクの総合的な管理の状況に関して、取締役会等が適切に評価及び判断できる情報を、定期的に又は必要に応じて随時、報告しているか。

③【各オペレーショナル・リスク管理部門への還元】

オペレーショナル・リスクの総合的な管理部門は、必要に応じて、オペレーショナル・リスクの状況について、関連する各オペレーショナル・リスク管理部門に評価・分析、検討した結果等を還元しているか。

⑶　コントロール及び削減

①【オペレーショナル・リスクのコントロール】

オペレーショナル・リスクの総合的な管理部門は、評価された重要なオペレーショナル・リスクに係るコントロール方法について、取締役会等が意思決定できる情報を報告しているか。

②【オペレーショナル・リスクの削減】

オペレーショナル・リスクの総合的な管理部門は、オペレーショナル・リスクを削減する方策（保険契約等を含む）を実施する場合、新たなリスクの発生に注意を払っているか。

⑷　【検証・見直し】

オペレーショナル・リスクの総合的な管理部門は、業務環境の変化、リスク・プロファイルの変化及びオペレーショナル・リスクの評価方法の限界及び弱点を把握し、業務の規模・特性及びリスク・プロファイルに見合った適切なオペレーショナル・リスク管理方法であるかを定期的に検証し、見直しているか。

Ⅲ．個別の問題点

【検証ポイント】

- **本章においては、オペレーショナル・リスクの総合的な管理の実態に即した個別具体的な問題点について検査官が検証するためのチェック項目を記載している。**
- **Ⅲ．の各チェック項目の検証において問題点の発生が認められた場合、当該問題点がⅠ．又はⅡ．のいずれの要素の欠如又は不十分に起因して発生したものであるかをⅠ．又はⅡ．のチェックリストにおいて漏れなく検証し、双方向の議論を通じて確認する。**
- **検査官が発見した問題点を経営陣が認識していない場合には、特に上記Ⅰ．の各態勢及びその過程が適切に機能していない可能性も含め、厳格に検証し、双方向の議論を通じて確認する。**
- **検査官は、前回検査における指摘事項のうち、軽微でない事項の改善状況について検証し、実効性ある改善策が策定され実行されているか否か確認する。**

１．オペレーショナル・リスク相当額の算出の適正性

⑴ 【基礎的手法及び粗利益配分手法を採用している場合の検証項目】

外部委託の費用に該当しないものを役務取引等費用から除くか否かを決定し、役務取引等費用から除くことになった場合には、外部委託の費用に当たらないものを明確にしている基準（外部委託の費用に当たるものを限定的に定めている場合を含む）を策定しているか。

⑵ 【粗利益配分手法を採用している場合の検証項目】

① 全ての業務から発生する粗利益について、相互に重複することなく告示別表第一の業務区分に粗利益を配分する手順に基づき算出されているか。

② 告示別表第一のある業務区分に係る業務区分配分値（業務区分に応じ、別表第一に掲げる掛目を乗じて得た額）が負の値である場合に、当該業務区分配分値を他の業務区分に係る業務区分配分値のうち正の値であるものと相殺するか否かを決定し、相殺することになった場合には、客観的に判別できるようにしているか。

③ 信用リスク・アセットの額及びマーケット・リスク相当額を算出する際に用いる基準に告示別表第一と類似の区分がある場合は、両者の区分は整合的になっているか。また、両者の区分が整合的になっていない場合には、その理由を明文化しているか。

④ 告示別表第一の各業務区分に含まれている業務に付随する業務に当たるか否かを判別する客観的な基準及び複数の業務区分に含まれている業務に付随する業務がある場合には、当該付随する業務の粗利益を配分する基準を策定しているか。

⑤ ある業務の粗利益を特定の業務区分に配分することができない場合、当該業務の名称及び配分できない理由を明確にしているか。

⑥　告示別表第一の複数の業務区分に粗利益を配分する基準は、財務会計又は管理会計に基づき策定されているか。

２．オペレーショナル・リスク計量手法を用いている場合の検証項目

⑴　【オペレーショナル･リスク計量態勢の確立】

（ⅰ）オペレーショナル・リスク計量態勢に概念上の問題がなく、かつ、遺漏のない形で運営されているか。

（ⅱ）オペレーショナル・リスク管理方針のもとで、オペレーショナル・リスク計量手法（モデル）の位置づけを明確に定め、例えば、以下の項目について把握した上で運営しているか。また、連結対象子会社に対しても問題がないか確認しているか。

イ．当該金融機関の戦略目標や業務の規模・特性及びリスク・プロファイル

ロ．イ．を踏まえたオペレーショナル・リスク計量手法の基本設計思想

ハ．ロ．に基づいたオペレーショナル・リスクの特定及び計量（範囲、手法、前提条件等）

ニ．ハ．から生じるオペレーショナル・リスク計量手法の特性（限界及び弱点）及び当該手法の妥当性

ホ．ニ．を検証するための検証方法の内容

（ⅲ）資本配賦運営[7]を行っている場合、オペレーショナル・リスク計量手法で算出された結果を踏まえ、資本配賦運営の方針を策定しているか。計量対象外のオペレーショナル・リスクがある場合には、計量対象外としたことについて合理的な理由があるか。また、当該対象外のリスクを十分に考慮してリスク資本を配賦しているか。

⑵　取締役及び監査役の適切な関与

①【オペレーショナル・リスク計量手法への理解】

（ⅰ）取締役は、オペレーショナル・リスク計量手法及びリスク限度枠又はリスク資本枠（資本配賦運営を行っている場合）の決定が、経営や財務内容に重大な影響を及ぼすことを理解しているか。

（ⅱ）担当取締役は、当該金融機関の業務について必要とされるオペレーショナル・リスク計量手法を理解し、その特性（限界及び弱点）を把握しているか。

（ⅲ）取締役及び監査役は、研修を受けるなどして、オペレーショナル・リスク計量手法について理解を深めているか。

②【オペレーショナル・リスクの総合的な管理への取組】

取締役は、オペレーショナル・リスク計量手法によるオペレーショナル・リスクの総合的な管理に積極的に関与しているか。

---

[7] 自己資本管理態勢の確認検査用チェックリスト参照。

⑶　オペレーショナル・リスクの計量

①【統一的な尺度によるオペレーショナル・リスク量の計量】

オペレーショナル・リスク量を、各種オペレーショナル・リスクに共通した統一的な尺度で定量的に把握しているか。統一的な尺度は、全ての必要なオペレーショナル・リスク要素を把握・計量していることが望ましいが、仮に、統一的な尺度で十分な把握・計量を行っていないオペレーショナル・リスクが存在している場合には、補完的な情報を用いることにより、経営上の意思決定に際して、必要な全ての要素を勘案していることを確保しているか。

オペレーショナル・リスク量の計量は、例えば、統計的手法を用いた VaR 法等の、合理的、かつ、客観的で精緻な方式を採用して行っているか。

②【計量手法の適切性】

計量手法として個々のオペレーショナル・リスク損失事象を統計的に処理することで一定の信頼水準における最大損失額をオペレーショナル・リスク量として算出する場合、以下の項目に留意しているか。

- 内部損失事象を適切に用いているか。また、例えば、外部情報や業務プロセス等の評価結果から策定したシナリオについても損失事象として考慮しているか。
- 信頼水準及び保有期間の設定は適切なものとなっているか。
- 低頻度高額損失事象を適切に捕捉した合理的な計量手法となっているか。

③【計量手法等の検証態勢及び管理態勢】

オペレーショナル・リスク計量手法の開発から独立し、かつ十分な能力を有する者より、開発時点及びその後定期的に、オペレーショナル・リスク計量手法、前提条件等の妥当性について検証されているか。仮に、オペレーショナル・リスク計量手法、前提条件等に不備が認められた場合には、適切に修正を行っているか。

また、オペレーショナル・リスク計量手法、前提条件等について、合理的な理由によらずに改変することができないような体制、内部規程等を整備し、その定められた内部規程等に従って適切にオペレーショナル・リスク計量手法等の管理を行っているか。

⑷　【オペレーショナル・リスク計量手法に関する記録】

オペレーショナル・リスク計量手法、前提条件等を選択する際の検討過程及び決定根拠について、事後の検証や計量の精緻化・高度化のために必要な記録等を保存し、継承できる態勢を整備しているか。

⑸ 監査

①【監査プログラムの整備】

オペレーショナル・リスク計量手法の監査を網羅的にカバーする監査プログラムが整備されているか。

②【内部監査の監査範囲】

以下の項目について、内部監査を行っているか。

- オペレーショナル・リスク計量手法と、戦略目標、業務の規模・特性及びリスク・プロファイルとの整合性
- オペレーショナル・リスク計量手法の特性（限界及び弱点）を考慮した運営の適切性
- オペレーショナル・リスク計量手法に関する記録は適切に文書化され、遅滞なく更新されていること
- オペレーショナル・リスクの総合的な管理プロセスにおける変更内容の計量手法への適切な反映
- オペレーショナル・リスク計量手法によって捉えられる計量対象範囲の妥当性
- 経営陣向けの情報システムに遺漏がないこと

③【監査結果の活用】

オペレーショナル・リスクの総合的な管理部門は、監査の結果を踏まえて、オペレーショナル・リスク計量手法を適切に見直しているか。

⑹ 外部業者が開発したオペレーショナル・リスク計量モデル[8]

①【オペレーショナル・リスク計量態勢の適切性】

（ⅰ）金融機関の担当者は、計量手法に関する知識を十分持ち、オペレーショナル・リスク計量のモデル化の過程について理解しているか。

（ⅱ）金融機関のオペレーショナル・リスクの総合的な管理部門及び内部監査部門は、計量手法の理論的及び実証的な妥当性検証を行っているか。

②【オペレーショナル・リスク計量モデルの適正性】

（ⅰ）計量モデルに関してブラックボックスの部分はないか。仮に、ブラックボックスの部分がある場合には、計量モデルの妥当性について検証しているか。

（ⅱ）外部データ、自行データ、シナリオデータの整合性、正確性は確保されているか。

（ⅲ）金融機関の業務の規模・特性及びリスク・プロファイルに見合った計量モデルが選択されているか。

---

[8] オペレーショナル・リスクの計量を外部委託している場合は、当該検証項目を準用して検証を行う。

③【オペレーショナル・リスク計量モデルの開発業者の管理】

（ⅰ）継続的なモデル運用ができ、モデルの精緻化・高度化に向けた取組が可能なモデルの開発業者と委託契約をし、定期的に、開発業者の評価を行っているか。

（ⅱ）オペレーショナル・リスク計量のユーザーに対するサポート体制（研修、コンサルティング及び保守）が十分な開発業者を選定しているか。

（ⅲ）モデルの開発業者における計量モデルの妥当性の検証状況について、定期的に又は必要に応じて随時、報告を受けられる態勢となっているか。

３．外部委託業務のオペレーショナル・リスク管理[9]

①【外部委託先の選定】

オペレーショナル・リスクの総合的な管理部門は、外部委託管理責任者と連携[10]し、外部委託の実施前に当該外部委託業務に内在するオペレーショナル・リスクを特定し、サービスの質や存続の確実性等のリスク管理上の問題点を認識した上で、外部委託業務を的確、公正かつ効率的に遂行することができる能力を有する者に委託するための措置を講じているか。外部委託先の選定に当たり、例えば、オペレーショナル・リスク管理の観点から、以下のような点に留意しているか。

- 金融機関の合理性の観点からみて十分なレベルのサービスの提供を行い得るか。
- 委託契約に沿ったサービス提供や損害負担が確保できる財務・経営内容か。
- 金融機関のレピュテーション等の観点[11]から問題ないか。

②【委託契約の内容】

オペレーショナル・リスクの総合的な管理部門は、外部委託管理責任者と連携し、委託契約において、提供されるサービス水準、外部委託先との責任分担（例えば、委託契約に沿ってサービスが提供されない場合における外部委託先の責務、又は委託に関連して発生するおそれのある損害の負担の関係）について定めていることを確認するための措置を講じているか。

③【外部委託先のモニタリング】

オペレーショナル・リスクの総合的な管理部門は、外部委託管理責任者と連携し、外部委託した業務について、定期的にモニタリングを行うための措置を講じているか。

④【問題点の是正】

オペレーショナル・リスクの総合的な管理部門は、問題点等を発見した場合には、

---

9 外部委託の形態や委託される業務内容は多様であり、当該検証項目においては、外部委託された業務の内容及びその当該金融機関における重要度等を踏まえた検証が必要である。

10 オペレーショナル・リスクの総合的な管理部門の管理者と外部委託管理責任者との兼務を妨げるものではないことに留意する。

11 例えば、外部委託先と反社会的勢力との関係の有無などを含む。

外部委託管理責任者と連携して速やかに是正する措置を講じているか。

４．事務リスク管理態勢

事務リスク管理態勢については、別紙１を参照。

５．システムリスク管理態勢

システムリスク管理態勢については、別紙２を参照。

６．その他オペレーショナル・リスク管理態勢

当該金融機関がオペレーショナル・リスクと定義したリスクのうち、事務リスク及びシステムリスクを除いたリスク管理態勢（以下「その他オペレーショナル・リスク管理態勢」という。）については、別紙３を参照。

（別紙１）

Ⅰ．　経営陣による事務リスク管理態勢の整備・確立状況

【検証ポイント】

- **事務リスクとは、役職員が正確な事務を怠る、あるいは事故・不正等を起こすことにより金融機関が損失を被るリスクをいう。**
- **金融機関における事務リスク管理態勢の整備・確立は、金融機関の業務の健全性及び適切性の観点から極めて重要であり、経営陣には、これらの態勢の整備・確立を自ら率先して行う役割と責任がある。**
- **検査官は、①方針の策定、②内部規程・組織体制の整備、③評価・改善態勢の整備がそれぞれ適切に経営陣によってなされているかといった観点から、事務リスク管理態勢が有効に機能しているか否か、経営陣の役割と責任が適切に果たされているかをⅠ．のチェック項目を活用して具体的に確認する。**
- **Ⅱ．以降のチェック項目の検証において問題点の発生が認められた場合、当該問題点がⅠ．のいずれの要素の欠如又は不十分に起因して発生したものであるかを漏れなく検証し、双方向の議論を通じて確認する。**
- **検査官が認識した弱点・問題点を経営陣が認識していない場合には、特に、態勢が有効に機能していない可能性も含めて検証し、双方向の議論を通じて確認する。**
- **検査官は、前回検査における指摘事項のうち、軽微でない事項の改善状況について検証し、実効性ある改善策が策定され実行されているか否か確認する。**

１．方針の策定

①【取締役の役割・責任】

取締役は、事務リスク管理を軽視することが戦略目標の達成に重大な影響を与えることを十分に認識し、事務リスク管理を重視しているか。特に担当取締役は、事務リスクの所在、事務リスクの種類・特性及び事務リスクの特定・評価・モニタリング・コントロール等の手法並びに事務リスク管理の重要性を十分に理解し、この理解に基づき当該金融機関の事務リスク管理の状況を的確に認識し、適正な事務リスク管理態勢の整備・確立に向けた方針及び具体的な方策を検討しているか。

②【事務リスク管理方針の整備・周知】

取締役会は、事務リスク管理に関する方針（以下「事務リスク管理方針」という。）を定め、組織全体に周知させているか。例えば、以下の項目について明確に記載される等、適切なものとなっているか。

- 事務リスク管理に関する担当取締役及び取締役会等の役割・責任
- 事務リスク管理に関する部門（以下「事務リスク管理部門」という。）の設

置、権限の付与等の組織体制に関する方針

・　事務リスクの特定、評価、モニタリング、コントロール及び削減に関する方針

③【方針策定プロセスの見直し】

取締役会は、定期的に又は必要に応じて随時、事務リスク管理の状況に関する報告・調査結果等を踏まえ、方針策定のプロセスの有効性を検証し、適時に見直しているか。

２．内部規程・組織体制の整備

①【内部規程の整備】

取締役会等は、事務リスク管理方針に則り、事務リスク管理に関する取決めを明確に定めた内部規程（以下「事務リスク管理規程」という。）を事務リスク管理部門の管理者（以下本チェックリストにおいて単に「管理者」という。）に策定させ、組織内に周知させているか。取締役会等は、事務リスク管理規程についてリーガル・チェック等を経て、事務リスク管理方針に合致することを確認した上で承認しているか。

②【事務リスク管理部門の態勢整備】

（ⅰ）取締役会等は、事務リスク管理方針及び事務リスク管理規程に則り、事務リスク管理部門を設置し、適切な役割を担わせる態勢を整備しているか。[1]

（ⅱ）取締役会は、事務リスク管理部門に、当該部門を統括するのに必要な知識と経験を有する管理者を配置し、当該管理者に対し管理業務の遂行に必要な権限を与えて管理させているか。

（ⅲ）取締役会等は、事務リスク管理部門に、その業務の遂行に必要な知識と経験を有する人員を適切な規模で配置し、当該人員に対し業務の遂行に必要な権限を与えているか[2]。

（ⅳ）取締役会等は、事務リスク管理部門から各業務部門に対する牽制機能が発揮される態勢を整備しているか。

③【各業務部門及び営業店等における事務リスク管理態勢の整備】

（ⅰ）取締役会等は、各業務部門及び営業店等に対し、遵守すべき内部規程・業務細則等を周知させ、遵守させる態勢を整備しているか。例えば、管理者に各業務部門及び営業店等が遵守すべき内部規程・業務細則等を特定させ、効果的な研修を定期的

---

[1] 事務リスク管理部門を独立した態様で設置しない場合（例えば、他のリスク管理部門と統合した一つのリスク管理部門を構成する場合のほか、他の業務と兼担する部署が事務リスク管理を担当する場合や、部門や部署ではなく責任者が事務リスク管理を担当する場合等）には、当該金融機関の規模・特性及びリスク・プロファイルに応じ、その態勢のあり方が十分に合理的で、かつ、機能的な側面から見て部門を設置する場合と同様の機能を備えているかを検証する。

[2] 人員の配置及び権限の付与についての権限が取締役会等以外の部署・役職にある場合には、その部署・役職の性質に照らし、牽制機能が働く等合理的なものとなっているか否かを検証する。

に行わせる等の具体的な施策を行うよう指示しているか。

（ⅱ）取締役会等は、管理者又は事務リスク管理部門を通じ、各業務部門及び営業店等において、事務リスク管理の実効性を確保する態勢を整備しているか。

④【取締役会等への報告・承認態勢の整備】

取締役会等は、報告事項及び承認事項を適切に設定した上で、管理者に、定期的に又は必要に応じて随時、取締役会等及びオペレーショナル・リスクの総合的な管理部門に対し状況を報告させ、又は承認を求めさせる態勢を整備しているか。特に、経営に重大な影響を与える、又は顧客の利益が著しく阻害される事案については、取締役会等及びオペレーショナル・リスクの総合的な管理部門に対し速やかに報告させる態勢を整備しているか。

⑤【監査役への報告態勢の整備】

取締役会は、監査役へ直接報告されるべき事項を特定した場合には、報告事項を適切に設定した上で管理者から直接報告を行わせる態勢を整備しているか。[3]

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、事務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。[4]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。

- 事務リスク管理態勢の整備状況
- 事務リスク管理方針、事務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事務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

⑦【内部規程･組織体制の整備プロセスの見直し】

取締役会等は、定期的に又は必要に応じて随時、事務リスク管理の状況に関する報告・調査結果等を踏まえ、内部規程・組織体制の整備プロセスの有効性を検証し、適時に見直しているか。

３．評価・改善活動

⑴ 分析・評価

①【事務リスク管理の分析・評価】

取締役会等は、監査役監査、内部監査及び外部監査の結果、各種調査結果並びに各部門からの報告等全ての事務リスク管理の状況に関する情報に基づき、事務リス

[3] このことは、監査役が自ら報告を求めることを妨げるものではなく、監査役の権限及び活動を何ら制限するものではないことに留意する。

[4] 内部監査計画についてはその基本的事項について承認すれば足りる。

ク管理の状況を的確に分析し、事務リスク管理の実効性の評価を行った上で、態勢上の弱点、問題点等改善すべき点の有無及びその内容を適切に検討するとともに、その原因を適切に検証しているか。また、必要な場合には、利害関係者以外の者によって構成された調査委員会等を設置する等、その原因究明については万全を期しているか。

②【分析・評価プロセスの見直し】

取締役会等は、定期的に又は必要に応じて随時、事務リスク管理の状況に関する報告・調査結果等を踏まえ、分析・評価プロセスの有効性を検証し、適時に見直しているか。

⑵　改善活動

①【改善の実施】

取締役会等は、上記３．⑴の分析・評価及び検証の結果に基づき、必要に応じて改善計画を策定しこれを実施する等の方法により、適時適切に当該問題点及び態勢上の弱点の改善を実施する態勢を整備しているか。

②【改善活動の進捗状況】

取締役会等は、改善の実施について、その進捗状況を定期的に又は必要に応じて随時、検証し、適時適切にフォローアップを図る態勢を整備しているか。

③【改善プロセスの見直し】

取締役会等は、定期的に又は必要に応じて随時、事務リスク管理の状況に関する報告・調査結果等を踏まえ、改善プロセスの有効性を検証し、適時に見直しているか。

Ⅱ．管理者による事務リスク管理態勢の整備・確立状況

【検証ポイント】

- **本章においては、管理者及び事務リスク部門が果たすべき役割と負うべき責任について検査官が検証するためのチェック項目を記載している。**
- **Ⅱ．の各チェック項目の検証において問題点の発生が認められた場合、当該問題点がⅠ．のいずれの要素の欠如又は不十分に起因して発生したものであるかをⅠ．のチェックリストにおいて漏れなく検証し、双方向の議論を通じて確認する。**
- **検査官が発見した問題点を経営陣が認識していない場合には、特に上記Ⅰ．の各態勢及びその過程が適切に機能していない可能性も含め、厳格に検証し、双方向の議論を通じて確認する。**
- **検査官は、前回検査における指摘事項のうち、軽微でない事項の改善状況について検証し、実効性ある改善策が策定され実行されているか否か確認する。**

１．管理者の役割・責任

①【事務リスク管理規程の整備・周知】

管理者は、事務リスクの所在、事務リスクの種類・特性及び事務リスク管理手法を十分に理解し、事務リスク管理方針に沿って、事務リスクの特定、評価及びモニタリングの方法を決定し、これに基づいた事務リスクのコントロール及び削減に関する取決めを明確に定めた事務リスク管理規程を策定しているか。事務リスク管理規程は、オペレーショナル・リスクの総合的な管理部門が確認し、取締役会等の承認を受けた上で、組織内に周知されているか。

②【事務リスク管理規程の内容】

事務リスク管理規程の内容は、業務の規模・特性及びリスク・プロファイルに応じ、事務リスクの管理に必要な取決めを網羅し、適切に規定されているか。例えば、以下の項目について明確に記載される等、適切なものとなっているか。

- 事務リスク管理部門の役割・責任及び組織に関する取決め
- 事務リスク管理の管理対象とするリスクの特定に関する取決め
- 事務リスク評価方法に関する取決め
- 事務リスクのモニタリング方法に関する取決め
- 取締役会等及びオペレーショナル・リスクの総合的な管理部門に報告する態勢に関する取決め

③【管理者による組織体制の整備】

（ⅰ）管理者は、事務リスク管理方針及び事務リスク管理規程に基づき、適切な事務リスク管理を行うため、事務リスク管理部門の態勢を整備し、牽制機能を発揮させるための施策を実施しているか。

（ⅱ）管理者は、事務リスク管理を実効的に行う能力を向上させるための研修・教育態

勢を整備し、専門性を持った人材の育成を行っているか。

（ⅲ）管理者は、定期的に又は必要に応じて随時、取締役会等が設定した報告事項を取締役会等及びオペレーショナル・リスクの総合的な管理部門に報告する態勢を整備しているか。特に、経営に重大な影響を与える事案については、取締役会等及びオペレーショナル・リスクの総合的な管理部門に対し速やかに報告する態勢を整備しているか。

（ⅳ）管理者は、事故防止の観点から、人事担当者等と連携し、連続休暇、研修、内部出向制度等により、最低限年一回一週間連続して、職員（管理者も含む）が職場を離れる方策をとっているか。管理者は、その状況を管理し、当該方策を確実に実施しているか。

（ⅴ）管理者は、事故防止の観点から、人事担当者等と連携し、特定の職員を長期間にわたり同一部署の同一業務に従事させないように、適切な人事ローテーションを確保しているか。やむを得ない理由により長期間にわたり同一部署の同一業務に従事している場合は、他の方策により事故防止等の実効性を確保しているか。管理者は、その状況を管理し、当該方策を確実に実施しているか。

（ⅵ）管理者は、派遣職員等についても、事故防止の観点から、以下の点に留意した人事管理を行っているか。

- 派遣職員等が行うことのできる業務の範囲を明確化しているか。
- 職員に比べ人事情報が少ない等の派遣職員等の特性を踏まえた人事・労務管理（研修の実施を含む。）を行うとともに、日常的な牽制が機能する態勢となっているか。

④【事務リスク管理規程及び組織体制の見直し】

管理者は、継続的に事務リスク管理部門の職務の執行状況に関するモニタリングを実施しているか。また、定期的に又は必要に応じて随時、事務リスク管理態勢の実効性を検証し、必要に応じて事務リスク管理規程及び組織体制の見直しを行い、又は取締役会等に対し改善のための提言を行っているか。

２．事務リスク管理部門の役割・責任[5]

⑴ 【事務統括部門の役割・責任】

（ⅰ）事務統括部門は、事務規程を整備しているか。事務規程の内容は、業務の規模・特性及びリスク・プロファイルに応じ、網羅的でかつ法令等に則って、適切に規定されているか。また、事務規程は、営業店等の事務だけではなく、各業務部門の事務についても規定しているか。

なお、以下の項目については、事務規程に明確に記載し、漏れのない適切な事務

[5] 事務リスク管理部門として以下に記載のある事務統括部門、事務指導部門の管理部門について、組織形態としてこれらの部門が設置されているかを検証するのではなく、これらの部門の役割・責任が機能として果たされているかを検証することに留意する。

規程となっているか。

- 事務規程外の取扱い及び事務規程の解釈に意見の相違があった場合の処理手続
- 現金・現物・重要書類・便宜扱い等の異例扱いの手続

（ⅱ）事務統括部門は、関係する他のリスク管理部門等と連携し、監査結果、不祥事件、業務上の事故、苦情・問い合わせ等で把握した問題点の発生原因分析・再発防止策の検討を講じているか。その結果、事務規程について、必要に応じて見直し、改善しているか。

（ⅲ）事務統括部門は、事務規程を法令等の外部環境が変化した場合等について、必要に応じて見直し、改善しているか。

（ⅳ）事務統括部門は、各業務部門及び営業店等の事務管理態勢を常時チェックする措置を講じているか。

（ⅴ）事務統括部門は、各業務部門の管理者及び営業店長が、不正なことを隠蔽しないような態勢を整備しているか。

（ⅵ）事務統括部門は、各業務部門及び営業店等による自店検査等の実施基準、実施要領について、内部監査部門の意見を踏まえた上で策定しているか。

（ⅶ）事務統括部門は、各業務部門及び営業店等において実施した自店検査結果の報告を受けているか。また、実効性のある自店検査となっているか検証を行っているか。

⑵ 【事務指導部門の役割・責任】

（ⅰ）事務指導部門は、各業務部門及び営業店等において事務処理が適切に行われるよう事務指導及び研修を行っているか。

（ⅱ）事務指導部門は、内部監査部門の監査結果を活用して、各業務部門及び営業店等の事務水準の向上を図っているか。

（ⅲ）事務指導部門は、事務処理に係る各業務部門及び営業店等からの問い合わせ等に迅速かつ正確に対応しているか。

Ⅲ．個別の問題点

【検証ポイント】

- **本章においては、事務リスク管理の実態に即した個別具体的な問題点について検査官が検証するためのチェック項目を記載している。**
- **Ⅲ．の各チェック項目の検証において問題点の発生が認められた場合、当該問題点がⅠ．又はⅡ．のいずれの要素の欠如又は不十分に起因して発生したものであるかをⅠ．又はⅡ．のチェックリストにおいて漏れなく検証し、双方向の議論を通じて確認する。**
- **検査官が発見した問題点を経営陣が認識していない場合には、特に上記Ⅰ．の各態勢及びその過程が適切に機能していない可能性も含め、厳格に検証し、双方向の議論を通じて確認する。**
- **検査官は、前回検査における指摘事項のうち、軽微でない事項の改善状況について検証し、実効性ある改善策が策定され実行されているか否か確認する。**

１．各業務部門及び営業店等における事務処理態勢

⑴ 【各業務部門の管理者及び営業店長の役割】

（ⅰ）事務処理について生じる事務リスクを常に把握しているか。

（ⅱ）適正な事務処理・事務規程の遵守状況、各種リスクが内在する事項についてチェックを行っているか。

（ⅲ）精査・検印担当者自身が業務に追われ、精査・検印が本来の機能を発揮していないことがないように努めているか。

（ⅳ）担当する各業務部門又は営業店等の事務処理上の問題点を把握し、改善しているか。

（ⅴ）特に便宜扱い等の異例扱いについて、厳正に対処しているか。

（ⅵ）事務規程外の取扱いを行う場合については、事務統括部門及び関係業務部門と連携のうえ責任をもって処理をしているか。

⑵ 【厳正な事務管理】

（ⅰ）事務処理を、厳正に行っているか。

（ⅱ）精査・検印は、形式的、表面的であってはならず、実質的で厳正に行っているか。

（ⅲ）現金事故は、発生後直ちに各業務部門の管理者又は営業店長へ連絡し、かつ事務統括部門・内部監査部門等必要な部門に報告しているか。

（ⅳ）便宜扱い等の異例扱いについては、必ず各業務部門の管理者、営業店長又は役席等の承認を受けた後に処理しているか。

（ⅴ）事務規程外の取扱いを行う場合には、事務統括部門及び関係業務部門と連携のうえ、必ず各業務部門の管理者又営業店長の指示に基づき処理をしているか。

⑶ 【自店検査の適切性】

（ⅰ）各業務部門及び営業店等における事故、不正等の未然防止、顧客への被害拡大を防ぐため、実施基準、実施要領に基づき、定期的又は必要に応じて随時、実効性のある自店検査を実施しているか。

（ⅱ）自店検査の結果等について、自店検査の実施者から、定期的又は必要に応じて随時、事務統括部門及び内部監査部門に対して、報告しているか。

（ⅲ）自店検査の結果を事務の改善に活用しているか。

２．市場取引の事務管理態勢

⑴ 【厳正な事務処理】

為替、資金、証券取引等及びこれらの派生商品取引については、例えば以下のとおり各市場取引の内部規程・業務細則等に沿った厳正な取扱いを行っているか。

（ⅰ）市場取引の事務管理部門が、全ての取引を漏れなく把握しているか。（例えばシステム入力の最終確認、チケットの打刻や連続番号による確認等）

（ⅱ）取引内容の入力は遅滞なく行われているか。

（ⅲ）確認・調整段階で検出されたディーリング・チケットの誤りの修正は市場取引の事務管理部門の管理者によって承認されているか。

（ⅳ）処理が将来行われるため未完扱いとされているディーリング・チケットは適切に管理・記録されているか。

（ⅴ）市場取引担当者以外の者がコンファメーションを送受しているか。

（ⅵ）コンファメーションとディーリング・チケットの照合は適切に行われているか。

（ⅶ）ディーリング・チケット、ディーリング･シート、コンファメーション等の保存・保管状況は適切か。

（ⅷ）市場部門及び市場取引の事務管理部門の個々の取引記録等の証拠書類については、内部監査部門のチェックを受けることとし、内部規程・業務細則等に定められている保存年限（最低１年以上）に基づいて保存しているか。

⑵ 【取引内容、残高等の照合】

市場部門と市場取引の事務管理部門における取引データの突合を行うとともに、誤差等がある場合には、速やかにその原因究明を行い、予め定められた方法に基づき補完しているか。

例えば、証券取引においては、市場部門でのディーリング・システムによるポジションと事務管理部門での金融商品取引業者及びカストディ部門等に確認後の勘定系の証券保有残高との照合を定期的（最低限月１回）に行っているか。

３．実地調査用チェックリスト

⑴　本チェックリストは、検査官が事務リスク管理の状況について実地に調査を行う際に活用するため、あくまで例示として掲げたものであり、金融機関の全業務を網羅したものではない。

⑵　調査に当たっては、実際の事務処理状況のチェックは、基本的に金融機関の内部監査部門等が負っていることに留意し、内部監査部門が有効に機能していることが確認出来れば、例示事項の全てについてまで、実地に調査を行う必要はなく、逆に内部監査部門が有効に機能していないようであれば、さらに深くその他の業務分野についてもチェックを行う必要がある。

⑶　新規業務、新商品販売を開始している際には、例示事項に掲げられていなくても実地に調査を行う必要がある。

⑷　本チェックリストについては、単なる軽微な事務ミスを指摘することが目的ではなく、リスク管理態勢の機能の発揮状況を確認することを目的としていることに留意する。

項目	チェック内容
１．内部業務	内部業務の取扱いについて、例えば以下の点に留意しているか。 ⑴　現金・現物の管理 ①　役席者による残高管理 ②　現金事故の連絡 ⑵　異例扱いによる取引 ①　異例扱いに係る取扱基準の内容 ②　異例扱いの発生原因及び記録 ③　営業店長又は役席者の承認と事後検証 ④　異例扱いの補完処理の適切性 ⑤　異例扱いの多発等の現象 ⑶　役席キー等を使用する取引 ①　起算取引などの特殊取引のチェック ②　役席キー等を必要とする重要取引の選別 ⑷　過振りの発生状況 ①　決済懸念のない先等過振先の確定 ②　資金負担の発生する取引に対する事前の承認 ⑸　書損証書・通帳等の取扱い ⑹　手数料徴求・物件費支払い ⑺　証書・通帳・カード等の喪失に係る取扱い（設定コードの設定状況） ⑻　総合振込、資金化前振込の管理

	⑼　店頭預り物件の取扱い及び保管状況 ⑽　CD カードの管理 ⑾　手形取扱、小切手取扱、内国為替取引・送金、外国為替 ⑿　テロ資金供与・マネー・ローンダリング関連 ①　取引時確認、確認記録の作成・保存、取引記録の保存等 ②　金融機関等による疑わしい取引の届出（犯罪収益移転防止法第 9 条） ③　犯罪収益等隠匿及び収受（組織犯罪処罰法第 10 条及び第 11 条） ⒀　未処理案件の整理・管理状況 ⒁　職員の人事管理
２．渉外業務	渉外業務の取扱いについて、例えば以下の点に留意しているか。 ⑴　渉外係の担当割、ローテーション ⑵　顧客からの苦情・問い合せ ⑶　届け金や電話依頼による送金 ⑷　預り証の発行・回収 ⑸　渉外・内部事務部門間の現物の授受 ⑹　現金・通帳・帳票などの長期預り ⑺　集金先の事故防止 ⑻　出先払い
３．預金関係業務	預金関係業務の取扱いについて、例えば以下の点に留意しているか。 ⑴　預金者に対する情報の提供 ①　主要な預金金利の店頭表示 ②　手数料一覧の店舗内備置・縦覧 ③　取り扱う預金商品のうち預金保険の対象となるものの明示 ④　商品内容全般に対する情報提供 ⑤　変動金利預金の基準とされている指標及び一定利率設定方法が定められている場合は、その方法及び金利情報の適切な提供 ⑵　協力預金、歩積両建預金 ①　過度な協力預金、過当な歩積預金及び両建預金の防止 ②　預金増強運動が過剰な勧誘とならないような歯止め措置 ③　期末計数を重視した業務計画への配慮 ⑶　別段預金・借受金・仮払金 ⑷　元本保証のない商品の取扱い ⑸　導入預金等法律に抵触する行為

４．貸出金関係業務	貸出金関係業務の取扱いについて、例えば以下の点に留意しているか。 ⑴　本人確認（借主、保証人、担保提供者等の意思確認） ⑵　担保物件評価・管理 ①　不動産鑑定士又は路線価等により根拠のある客観的な評価・自店評価の妥当性 ②　担保物件又は保証書等についての担保台帳・管理簿等への記載状況 ③　火災保険の付保と更新 ④　担保価額と担保による回収可能性 ⑤　連帯保証人の意思確認（保証確認） ⑶　保険料ローン ⑷　申込案件の進捗管理 ⑸　謝絶案件の対応状況 ⑹　大口先、赤字先等の与信管理 ⑺　延滞管理 ⑻　店長専決権限
５．証券関係業務	証券関係業務の取扱いについて、例えば以下の点に留意しているか。 ⑴　公社債の窓口販売業務 ①　売買に関する虚偽の表示、自己の保有する特定の有価証券の大量推奨販売、信用供与を利用した行為等の禁止行為等に留意した業務運営の確保 ②　金融商品取引法等の法規制や日本証券業協会等の規則に沿った内部規程・業務細則等の整備 ③　職員に対する周知徹底 ⑵　投資信託販売業務 ①　内部管理統括責任者、営業責任者、内部管理責任者等の責任者の設置 ②　「自己責任原則」、「適合性の原則」に基づき、断定的判断の提供による勧誘、取引一任勘定、損失補填、利益追加等の禁止行為等に留意した業務運営の確保 ③　金融商品取引法、投資信託及び投資法人に関する法律等の法規制や日本証券業協会等の規則に沿った内部規程・業務細則等の整備 ④　元本割れするリスクを負っていることの顧客に対する適切かつ十分な説明

	⑤　間貸し方式を採用している金融機関については、投資信託の直接募集・解約等のための他と区別された専用のスペースの設置 ⑥　職員に対する周知徹底
６．保険関係業務	保険関係業務の取扱いについて、例えば以下の点に留意しているか。 ⑴　責任者等を置くなど責任態勢の確立 ⑵　保険業法等に沿った内部規程・業務細則等の整備 ⑶　職員に対する周知徹底 ⑷　適切な業務運営の確保 ①　取引上の優越的地位を不当に利用して保険募集をするなどの弊害を防止するための措置の徹底 ②　保険商品のリスク等について顧客に対する適切かつ十分な説明及び情報提供
７．その他業務	その他業務の取扱いについて、例えば以下の点に留意しているか。 ⑴　デリバティブ商品 ①　販売者の資格、商品知識 ②　元本割れ等のリスクを伴う商品であることの顧客に対する適切かつ十分な説明 ③　時価レポートの送付・保管状況 ⑵　商品ファンド ①　名義貸し、金銭等の貸付・媒介、不当な勧誘等禁止行為等の投資家保護等のための規制に留意した業務運営の確保 ②　元本割れ等のリスクを伴う商品であることの顧客に対する適切かつ十分な説明 ③　職員に対する周知徹底 ⑶　抵当証券 ①　名義貸し、不当な勧誘等禁止行為等の購入者保護のための規制に留意した業務運営の確保 ②　元利金を保証する契約であるか否か等商品内容についての購入者に対する適切かつ十分な説明 ③　職員に対する周知徹底 ⑷　貸付債権信託 ①　顧客の知識や経験等に応じた勧誘 ②　顧客への適切かつ十分な説明 ③　職員に対する周知徹底

	⑸　小口債権販売 ⑹　地方公共団体等に対する債権の流動化 ⑺　一般貸付債権の流動化 ⑻　ローン・パーティシペーション ⑼　外為業務 ⑽　両替業務

（別紙２）

Ⅰ．　経営陣によるシステムリスク管理態勢の整備・確立状況

【検証ポイント】

・　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使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。

・　金融機関におけるシステムリスク管理態勢の整備・確立は、金融機関の業務の健全性及び適切性の観点から極めて重要であり、経営陣には、これらの態勢の整備・確立を自ら率先して行う役割と責任がある。

・　インターネットを利用したサービスの普及等に伴い顧客利便性が飛躍的に向上する一方で、サイバー攻撃の手口が巧妙化し影響も世界的規模で深刻化しており、金融機関においてはサイバーセキュリティを確保することが喫緊の課題となっている。

　経営陣においては、サイバー攻撃による顧客、取引先の被害を防止し、安定したサービスを提供するため、サイバーセキュリティ管理態勢を構築し、状況の変化に対応し継続的に改善していくことが求められている。

・　検査官は、①方針の策定、②内部規程・組織体制の整備、③評価・改善態勢の整備がそれぞれ適切に経営陣によってなされているかといった観点から、システムリスク管理態勢が有効に機能しているか否か、経営陣の役割と責任が適切に果たされているかをⅠ．のチェック項目を活用して具体的に確認する。

・　Ⅱ．以降のチェック項目の検証において問題点の発生が認められた場合、当該問題点がⅠ．のいずれの要素の欠如又は不十分に起因して発生したものであるかを漏れなく検証し、双方向の議論を通じて確認する。

・　検査官は、システムリスク管理態勢に問題点が見られ、さらに深く業務の具体的検証をすることが必要と認められる場合には、「金融機関等コンピュータシステムの安全対策基準・解説書」（公益財団法人金融情報システムセンター編）等に基づき確認する。

・　検査官は、金融機関が保持する保護すべき情報が役職員又は部外者等により、改ざん削除又は外部に漏洩するリスクについても本チェックリストに基づき確認することとする。

・　検査官が認識した弱点・問題点を経営陣が認識していない場合には、特に、態勢が有効に機能していない可能性も含めて検証し、双方向の議論を通じて確認する。

・　検査官は、前回検査における指摘事項のうち、軽微でない事項の改善状況について検証し、実効性ある改善策が策定され実行されているか否か確認することとする。

・　検査官は、システムリスク管理態勢の確認検査を行うに当たっては、個別システムの重要度及び性格に十分留意する。

　　・　システムの重要度とは、当該システムの顧客取引又は経営判断への影響の大きさを表す。

・　システムの性格とは、コンピュータセンターにおける中央集中型の汎用機システム、クライアントサーバーシステム等の分散系システム、ユーザー部門設置の単体システム等のそれぞれの特性を表し、それぞれに適した管理手法がある。

１．方針の策定

①【取締役の役割・責任】

（ⅰ）取締役は、システムリスク管理（システム障害やサイバーセキュリティ事案[1]（以下「システム障害等」という。）の未然防止及び発生時の迅速な復旧対応を含む。以下同じ。）を軽視することが戦略目標の達成に重大な影響を与えることを十分に認識し、システムリスク管理を重視しているか。

（ⅱ）取締役は、システム障害等発生時において、自らの果たすべき責任やとるべき対応について具体的に定めているか。また、自らが指揮を執る訓練を行い、その実効性を確保しているか。

（ⅲ）取締役会等は、サイバー攻撃が高度化・巧妙化していることを踏まえ、サイバーセキュリティの重要性を認識し必要な態勢を整備しているか。

また、取締役会等は、サイバーセキュリティについて、例えば、以下のような態勢を整備しているか。

・　サイバー攻撃に対する監視体制
・　サイバー攻撃を受けた際の報告及び広報体制
・　組織内 CSIRT（Computer Security Incident Response Team）等の緊急時対応及び早期警戒のための体制
・　情報共有機関等を通じた情報収集・共有体制　等

（ⅳ）取締役会は、システムリスクの重要性を十分に認識した上で、システムを統括管理する担当取締役（以下「システム担当取締役」という。）を定めているか。なお、システム担当取締役は、システムに関する十分な知識・経験を有し業務を適切に遂行できる者であることが望ましい。

（ⅴ）システム担当取締役は、システムリスクの所在、システムリスクの種類・特性及びシステムリスクの特定・評価・モニタリング・コントロール等の手法並びにシステムリスク管理の重要性を十分に理解し、この理解に基づき当該金融機関のシステムリスク管理の状況を的確に認識し、適正なシステムリスク管理態勢の整備・確立に向けた方針及び具体的な方策を検討しているか。

②【戦略目標の明確化】

取締役会は、情報技術革新を踏まえ、金融機関全体の経営方針に沿った戦略目標

[1] サイバーセキュリティ事案とは、情報通信ネットワークや情報システム等の悪用により、サイバー空間を経由して行われる不正侵入、情報の窃取、改ざんや破壊、情報システムの作動停止や誤作動、不正プログラムの実行や DDoS 攻撃等の、いわゆる「サイバー攻撃」により、サイバーセキュリティが脅かされる事案をいう。

の中に、経営戦略の一環としてシステムを捉えるシステム戦略方針を盛り込んでいるか。例えば、以下の項目について、システム戦略方針に明確に記載しているか。

- システム開発の優先順位
- 情報化推進計画
- システムに対する投資計画

③【システムリスク管理方針の整備・周知】

取締役会は、システムリスク管理に関する方針（以下「システムリスク管理方針」という。）を定め、組織全体に周知させているか。例えば、以下の項目について明確に記載される等、適切なものとなっているか。

- システムリスク管理に関する担当取締役及び取締役会等の役割・責任
- システムリスク管理に関する部門（以下「システムリスク管理部門」という。）の設置、権限の付与等の組織体制に関する方針
- システムリスクの特定、評価、モニタリング、コントロール及び削減に関する方針
- 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であり、①保護されるべき情報資産、②保護を行うべき理由、③それらについての責任の所在等の記載がなされたもの。)[2]

④【方針策定プロセスの見直し】

取締役会は、定期的に又は必要に応じて随時、システムリスク管理の状況に関する報告・調査結果等を踏まえ、方針策定のプロセスの有効性を検証し、適時に見直しているか。

また、取締役会等は他社における不正・不祥事件も参考に、情報セキュリティ管理態勢を PDCA サイクルにより継続的に改善しているか。

２．内部規程・組織体制の整備

①【内部規程の整備・周知】

取締役会等は、システムリスク管理方針に則り、システムリスク管理に関する取決めを明確に定めた内部規程（以下「システムリスク管理規程」という。）をシステムリスク管理部門の管理者（以下本チェックリストにおいて単に「管理者」という。）に策定させ、組織内に周知させているか。取締役会等は、システムリスク管理規程についてリーガル・チェック等を経て、システムリスク管理方針に合致することを確認した上で承認しているか。

②【システムリスク管理部門の態勢整備】

---

[2] ・「セキュリティポリシー」の対象範囲は、コンピュータシステムや記録媒体等に保存されている情報のみならず紙に印刷された情報等を含む。
・「金融機関等におけるセキュリティポリシー策定のための手引書」（公益財団法人金融情報システムセンター編）を参考。

（ⅰ）取締役会等は、システムリスク管理方針及びシステムリスク管理規程に則り、システムリスク管理部門を設置し、適切な役割を担わせる態勢を整備しているか[3]。

（ⅱ）取締役会は、システムリスク管理部門に、当該部門を統括するのに必要な知識と経験を有する管理者を配置し、当該管理者に対し管理業務の遂行に必要な権限を与えて管理させているか。

（ⅲ）取締役会等は、システムリスク管理部門に、その業務の遂行に必要な知識と経験を有する人員を適切な規模で配置し、当該人員に対し業務の遂行に必要な権限を与えているか[4]。

（ⅳ）取締役会等は、システムリスク管理部門から各業務部門に対する牽制機能が発揮される態勢を整備しているか。

③【各業務部門及び営業店等におけるシステムリスク管理態勢の整備】

（ⅰ）取締役会等は、各業務部門及び営業店等に対し、遵守すべき内部規程・業務細則等を周知させ、遵守させる態勢を整備しているか。例えば、管理者に各業務部門及び営業店等が遵守すべき内部規程・業務細則等を特定させ、効果的な研修を定期的に行わせる等の具体的な施策を行うよう指示しているか。

（ⅱ）取締役会等は、管理者又はシステムリスク管理部門を通じ、各業務部門及び営業店等において、システムリスク管理の実効性を確保する態勢を整備しているか。

④【取締役会等への報告・承認態勢の整備】

取締役会等は、報告事項及び承認事項を適切に設定した上で、管理者に、定期的に又は必要に応じて随時、取締役会等及びオペレーショナル・リスクの総合的な管理部門に対し状況を報告させ、又は承認を求めさせる態勢を整備しているか。特に、経営に重大な影響を与える、又は顧客の利益が著しく阻害される事案については、取締役会等及びオペレーショナル・リスクの総合的な管理部門に対し速やかに報告させる態勢を整備しているか。

⑤【監査役への報告態勢の整備】

取締役会は、監査役へ直接報告されるべき事項を特定した場合には、報告事項を適切に設定した上で管理者から直接報告を行わせる態勢を整備しているか。[5]

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

---

[3] システムリスク管理部門を独立した態様で設置しない場合（例えば、他のリスク管理部門と統合した一つのリスク管理部門を構成する場合のほか、他の業務と兼担する部署がシステムリスク管理を担当する場合や、部門や部署ではなく責任者がシステムリスク管理を担当する場合等）には、当該金融機関の規模・特性及びリスク・プロファイルに応じ、その態勢のあり方が十分に合理的で、かつ、機能的な側面から見て部門を設置する場合と同様の機能を備えているかを検証する。

[4] 人員の配置及び権限の付与についての権限が取締役会等以外の部署・役職にある場合には、その部署・役職の性質に照らし、利益相反等の問題を生じない合理的なものとなっているか否かを検証する。

[5] このことは、監査役が自ら報告を求めることを妨げるものではなく、監査役の権限及び活動を何ら制限するものではないことに留意する。

「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。[6]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

⑦【内部規程･組織体制の整備プロセスの見直し】

取締役会等は、定期的に又は必要に応じて随時、システムリスク管理の状況に関する報告・調査結果等を踏まえ、内部規程・組織体制の整備プロセスの有効性を検証し、適時に見直しているか。

３．評価・改善活動

⑴ 分析・評価

①【システムリスク管理の分析・評価】

取締役会等は、監査役監査、内部監査及び外部監査の結果、各種調査結果並びに各部門からの報告等全てのシステムリスク管理の状況に関する情報に基づき、システムリスク管理の状況を的確に分析し、システムリスク管理の実効性の評価を行った上で、態勢上の弱点、問題点等改善すべき点の有無及びその内容を適切に検討するとともに、その原因を適切に検証しているか。また、必要な場合には、利害関係者以外の者によって構成された調査委員会等を設置する等、その原因究明については万全を期しているか。

②【分析・評価プロセスの見直し】

取締役会等は、定期的に又は必要に応じて随時、システムリスク管理の状況に関する報告・調査結果等を踏まえ、分析・評価プロセスの有効性を検証し、適時に見直しているか。

⑵ 改善活動

①【改善の実施】

取締役会等は、上記３．⑴の分析・評価及び検証の結果に基づき、必要に応じて改善計画を策定しこれを実施する等の方法により、適時適切に当該問題点及び態勢上の弱点の改善を実施する態勢を整備しているか。

②【改善活動の進捗状況】

取締役会等は、改善の実施について、その進捗状況を定期的に又は必要に応じて

[6] 内部監査計画についてはその基本的事項について承認すれば足りる。

随時、検証し、適時適切にフォローアップを図る態勢を整備しているか。

③【改善プロセスの見直し】

取締役会等は、定期的に又は必要に応じて随時、システムリスク管理の状況に関する報告・調査結果等を踏まえ、改善プロセスの有効性を検証し、適時に見直しているか。

Ⅱ．管理者によるシステムリスク管理態勢の整備・確立状況

【検証ポイント】

- **本章においては、管理者及びシステムリスク管理部門が果たすべき役割と負うべき責任について検査官が検証するためのチェック項目を記載している。**
- **Ⅱ．の各チェック項目の検証において問題点の発生が認められた場合、当該問題点がⅠ．のいずれの要素の欠如又は不十分に起因して発生したものであるかをⅠ．のチェックリストにおいて漏れなく検証し、双方向の議論を通じて確認する。**
- **検査官が発見した問題点を経営陣が認識していない場合には、特に上記Ⅰ．の各態勢及びその過程が適切に機能していない可能性も含め、厳格に検証し、双方向の議論を通じて確認する。**
- **検査官は、前回検査における指摘事項のうち、軽微でない事項の改善状況について検証し、実効性ある改善策が策定され実行されているか否か確認する。**

１．管理者の役割・責任

①【システムリスク管理規程の整備・周知】

管理者は、システムリスクの所在、システムリスクの種類・特性及びシステムリスク管理手法を十分に理解し、システムリスク管理方針に沿って、システムリスクの特定、評価及びモニタリングの方法を決定し、これに基づいたシステムリスクのコントロール及び削減に関する取決めを明確に定めたシステムリスク管理規程を策定しているか。システムリスク管理規程は、オペレーショナル・リスクの総合的な管理部門が確認し、取締役会等の承認を受けた上で、組織内に周知されているか。

②【システムリスク管理規程の内容】

システムリスク管理規程の内容は、業務の規模・特性及びリスク・プロファイルに応じ、システムリスクの管理に必要な取決めを網羅し、適切に規定されているか。例えば、以下の項目について、明確に記載される等、適切なものとなっているか。

- システムリスク管理部門の役割・責任及び組織に関する取決め
- システムリスク管理の管理対象とするリスクの特定に関する取決め
- システムリスク評価方法に関する取決め
- システムリスクのモニタリング方法に関する取決め
- 取締役会等及びオペレーショナル・リスクの総合的な管理部門に報告する態勢に関する取決め

③【管理者による組織体制の整備】

（ⅰ）管理者は、システムリスク管理方針及びシステムリスク管理規程に基づき、適切なシステムリスク管理を行うため、システムリスク管理部門の態勢を整備し、牽制機能を発揮させるための施策を実施しているか。

（ⅱ）管理者は、システムリスク管理を実効的に行う能力を向上させるための研修・教

育態勢を整備し、専門性を持った人材の育成を行っているか。

（ⅲ）管理者は、定期的に又は必要に応じて随時、取締役会等が設定した報告事項を取締役会等及びオペレーショナル・リスクの総合的な管理部門に対して報告する態勢を整備しているか。特に、経営に重大な影響を与える事案については、取締役会等及びオペレーショナル・リスクの総合的な管理部門に対し速やかに報告する態勢を整備しているか。

（ⅳ）管理者は、定められた方針、基準及び手順に従ってセキュリティが守られているかを適正に管理するセキュリティ管理者を設置し、管理業務の遂行に必要な権限を与えて管理させているか。

（ⅴ）管理者は、システムの安全かつ円滑な運用と不正防止のため、システムの管理手順を定め、適正に管理するシステム管理者を設置し、管理業務の遂行に必要な権限を与えて管理させているか。

また、EUC（エンドユーザーコンピューティング）等ユーザー部門等が独自にシステムの企画、開発、運用を行うシステムについても、システム管理者を設置しているか。なお、システム管理者については、システム単位あるいは業務単位で設置していることが望ましい。

（ⅵ）管理者は、データについて機密性、完全性、可用性の確保を行うためにデータ管理者を設置し、管理業務の遂行に必要な権限を与えて管理させているか。

（ⅶ）管理者は、ネットワーク稼動状況の管理、アクセスコントロール及びモニタリング等を適切に管理するために、ネットワーク管理者を設置し、管理業務の遂行に必要な権限を与えて管理させているか。

④【システムリスク管理規程及び組織体制の見直し】

管理者は、継続的にシステムリスク管理部門の職務の執行状況に関するモニタリングを実施しているか。また、定期的に又は必要に応じて随時、システムリスク管理態勢の実効性を検証し、必要に応じてシステムリスク管理規程及び組織体制の見直しを行い、又は取締役会等に対し改善のための提言を行っているか。

２．システムリスク管理部門の役割・責任

⑴ 【システムリスクの認識・評価】

（ⅰ）システムリスク管理部門は、勘定系・情報系・対外系・証券系・国際系といった業務機能別システムのリスクの評価を含め、システム全般に通じるリスクを認識・評価しているか。

（ⅱ）システムリスク管理部門は、EUC 等ユーザー部門等が独自にシステムを構築する場合においても当該システムのリスクを認識・評価しているか。

（ⅲ）システムリスク管理部門は、顧客チャネルの多様化による大量取引の発生や、ネットワークの拡充によるシステム障害等の影響の複雑化・広範化など、外部環境の

変化によりリスクが多様化していることを踏まえ、定期的に又は適時にリスクを認識・評価しているか。

（ⅳ）システムリスク管理部門は、例えば１口座当たりの未記帳取引明細の保有可能件数などのシステムの制限値を把握するなど、システムの処理能力に関するリスクを認識・評価しているか。

（ⅴ）システムリスク管理部門は、新商品の導入時又は商品内容の変更時に、システム開発の有無にかかわらず、関連するシステムのリスクを認識・評価しているか。

（ⅵ）システムリスク管理部門は、インターネット等を利用した取引においては、非対面性、トラブル対応、第三者の関与等の問題が特に顕在化する可能性があるなど、インターネット等を利用した取引のリスクの所在を理解し、当該リスクを認識・評価しているか。

⑵　【システムリスクのモニタリング】

（ⅰ）システムリスク管理部門は、システムリスク管理方針及びシステムリスク管理規程等に基づき、当該金融機関の内部環境（リスク・プロファイル等）や外部環境の状況に照らし、当該金融機関のシステムリスクの状況を適切な頻度でモニタリングしているか。

（ⅱ）システムリスク管理部門は、システムリスク管理方針及びシステムリスク管理規程等に基づき、システムリスクの状況に関して、取締役会等及びオペレーショナル・リスクの総合的な管理部門が適切に評価及び判断できる情報を、定期的に又は必要に応じて随時、報告しているか。

⑶　【システムリスクのコントロール及び削減】

（ⅰ）システムリスクのコントロール

システムリスク管理部門は、システムの制限値を超えた場合のシステム面・事務面の対応策を検討しているか。また、評価された重要なシステムリスクに係るコントロール方法について、取締役会等が意思決定できる情報を報告しているか。

（ⅱ）システムリスクの削減

システムリスク管理部門は、システムリスクを削減する方策を実施する場合、新たなリスクの発生に注意を払っているか。

⑷　【検証・見直し】

システムリスク管理部門は、業務環境の変化、リスク・プロファイルの変化を把握し、業務の規模・特性及びリスク・プロファイルに見合った適切なシステムリスク管理方法であるかを定期的に検証し、見直しているか。

Ⅲ．個別の問題点

【検証ポイント】

- **本章においては、システムリスク管理の実態に即した個別具体的な問題点について検査官が検証するためのチェック項目を記載している。**
- **Ⅲ．の各チェック項目の検証において問題点の発生が認められた場合、当該問題点がⅠ．又はⅡ．のいずれの要素の欠如又は不十分に起因して発生したものであるかをⅠ．又はⅡ．のチェックリストにおいて漏れなく検証し、双方向の議論を通じて確認する。**
- **検査官が発見した問題点を経営陣が認識していない場合には、特に上記Ⅰ．の各態勢及びその過程が適切に機能していない可能性も含め、厳格に検証し、双方向の議論を通じて確認する。**
- **検査官は、前回検査における指摘事項のうち、軽微でない事項の改善状況について検証し、実効性ある改善策が策定され実行されているか否か確認する。**

１．情報セキュリティ管理

⑴ セキュリティ管理者等の役割・責任

①【セキュリティ管理者の役割・責任】

（ⅰ）セキュリティ管理者は、システムの企画、開発、運用、保守等にわたるすべてのセキュリティの管理を行っているか。

（ⅱ）セキュリティ管理者は、重大な障害・事故・犯罪等に関するセキュリティ上の問題について、システムリスク管理部門に報告しているか。

（ⅲ）セキュリティ管理者は、セキュリティについて、例えば、以下の観点から確保しているか。

イ．フィジカルセキュリティ

- 物理的侵入防止策・防犯設備
- コンピュータ稼動環境の整備
- 機器の保守・点検態勢　等

ロ．ロジカルセキュリティ

- 開発・運用の各組織間・組織内の相互牽制態勢
- 開発管理態勢
- 電子的侵入防止策
- プログラムの管理
- 障害発生時の対応策
- 外部ソフトウェアパッケージ導入時の評価・管理
- オペレーション面の安全管理　等

（ⅳ）セキュリティ管理者は、システム、データ、ネットワーク管理上のセキュリティに関することについて統括しているか。

（ｖ）セキュリティ管理者は、セキュリティ意識の向上を図るため、全役職員に対するセキュリティ教育（外部委託先におけるセキュリティ教育を含む）を行っているか。

②【システム管理者の役割・責任】

（ｉ）システム管理者は、それぞれのシステムの資産調査を定期的に行い、適正なスクラップ・アンド・ビルドを行っているか。

（ⅱ）システム管理者は、各業務部門、営業店等及びコンピュータセンターについて、それぞれの設備・機器も適切かつ十分な管理を行っているか。

（ⅲ）システム管理者は、社外に持ち出すコンピュータに対する適切かつ十分な管理を行っているか。

③【データ管理者の役割・責任】

（ｉ）データ管理者は、データの管理手順及び利用承認手順等を内部規程・業務細則等として定め、関係者に周知徹底させることにより、データの安全で円滑な運用を行っているか。

（ⅱ）データ管理者は、データ保護、データ不正使用防止について適切かつ十分な管理を行っているか。

④【ネットワーク管理者の役割・責任】

（ｉ）ネットワーク管理者は、ネットワークの管理手順及び利用承認手続等を内部規程・業務細則等として定め、関係者に周知徹底させることにより、ネットワークの適切かつ効率的で安全な運用を行っているか。

（ⅱ）ネットワーク管理者は、ネットワークがダウンした際の代替手段を考慮しているか。

⑵　【情報資産の保護】

（ｉ）金融機関が責任を負うべき顧客の重要情報を網羅的に洗い出し、把握、管理しているか。

顧客の重要情報の洗い出しにあたっては、業務、システム、外部委託先を対象範囲とし、例えば、以下のようなデータを洗い出しの対象範囲としているか。

- 通常の業務では使用しないシステム領域に格納されたデータ
- 障害解析のためにシステムから出力された障害解析用データ
- ＡＴＭ（店舗外含む）等に保存されている取引ログ　等

（ⅱ）洗い出した顧客の重要情報について、重要度判定やリスク評価を実施しているか。

また、それぞれの重要度やリスクに応じ、以下のような情報管理ルールを策定しているか。

- 情報の暗号化、マスキングのルール
- 情報を利用する際の利用ルール
- 記録媒体等の取扱いルール　等

（ⅲ）機密情報について、暗号化やマスキング等の管理ルールを定めているか。また、暗号化プログラム、暗号鍵、暗号化プログラムの設計書等の管理に関するルールを定めているか。

なお、「機密情報」とは、暗証番号、パスワード、クレジットカード情報等、顧客に損失が発生する可能性のある情報をいう。

（ⅳ）機密情報の保有・廃棄、アクセス制限、外部持ち出し等について、業務上の必要性を十分に検討し、より厳格な取扱いをしているか。

（ⅴ）情報資産について、管理ルール等に基づいて適切に管理されていることを定期的にモニタリングし、管理態勢を継続的に見直しているか。

⑶ 【不正使用防止】

（ⅰ）不正使用防止のため、業務内容や接続方法に応じ、接続相手先が本人若しくは正当な端末であることを確認する態勢を整備しているか。

（ⅱ）不正アクセス状況を管理するため、システムの操作履歴を監査証跡として取得し、事後の監査を可能とするとともに、定期的にチェックしているか。

（ⅲ）端末機の使用及びデータやファイルのアクセス等の権限については、その重要度に応じた設定・管理方法を明確にしているか。

⑷ 【コンピュータウィルス等】

コンピュータウィルス等の不正なプログラムの侵入を防止する方策を取っているとともに、万が一侵入があった場合速やかに発見・除去する態勢を整備しているか。

- コンピュータウィルスへの感染
- 正規の手続きを経てないプログラムの登録
- 正規プログラムの意図的な改ざん　等

⑸ 【インターネットを利用した取引の管理】

（ⅰ）インターネットバンキングの犯罪手口が高度化・巧妙化し、被害が拡大していることを踏まえ、リスク分析、セキュリティ対策の策定・実施、効果の検証（顧客に対する対策普及状況を含む）、対策の評価・見直しなどを行う態勢を整備しているか。

その際、情報共有機関等を活用して、犯罪の発生状況や犯罪手口に関する情報の提供・収集を行うとともに、有効な対応策等を共有し、自らの顧客や業務の特性に応じた検討を行った上で、今後発生が懸念される犯罪手口への対応も考慮し、必要な態勢の整備に努めているか。

（ⅱ）セキュリティ対策については、犯罪手口に対する個々のセキュリティ対策の強度を検証した上で、顧客属性を勘案し、複数の対策を組み合わせるなど、犯罪手口の

高度化・巧妙化（例えば「中間者攻撃」や「マン・イン・ザ・ブラウザ攻撃」など）に対応した対策を講じているか。

認証方式や不正防止策として、以下のような対策事例がある。

- 可変式パスワードや電子証明書などの、固定式の ID・パスワードのみに頼らない認証方式
- 取引に利用しているパソコンのブラウザとは別の携帯電話等の機器を用いるなど、複数経路による取引認証
- ハードウェアトークン等でトランザクション署名を行うトランザクション認証
- 取引時においてウィルス等の検知・駆除が行えるセキュリティ対策ソフトの利用者への提供
- 利用者のパソコンのウィルス感染状況を金融機関側で検知し、警告を発するソフトの導入
- 電子証明書を IC カード等、取引に利用しているパソコンとは別の媒体・機器へ格納する方式の採用
- 不正なログイン・異常な取引等を検知し、速やかに利用者に連絡する体制の整備　等

（ⅲ）リンク等によって生じうるサービス提供主体についての誤認を防止するための対策を講じているか。

（ⅳ）システムのダウン又は不具合により、適正な処理がなされなかった場合、それを補完する態勢となっているか。また、システムダウン等が発生した場合の責任分担のあり方についても、明確に示しているか。

（ⅴ）顧客からの苦情・相談（不正取引の発生を含む）等を受け付ける態勢を整備しているか。

（ⅵ）マネー・ローンダリング防止等の観点から取引時確認を行っているか。

（ⅶ）顧客情報の漏洩、外部侵入者及び内部の不正利用による顧客データの改ざん、書き換え等を防止する態勢を整備しているか。

（ⅷ）インターネットを利用した取引が非対面であるということに鑑み、顧客との取引履歴等について改ざん・削除等されることなく、必要に応じて一定期間保存されているか。

（ⅸ）顧客に求められるセキュリティ対策事例を顧客に対して十分に周知しているか。顧客自らによる早期の被害認識を可能とするため、顧客が取引内容を適時に確認できる手段を講じているか。また、新たな犯罪の手口が発生するなど必要な場合、速やかにかつ顧客が容易に理解できる形で周知しているか。

不正取引を防止するための対策が利用者に普及しているかを定期的にモニタリングし、普及させるための追加的な施策を講じているか。

（ｘ）不正取引に係る損失の補償については、預貯金者保護法及び全国銀行協会の申合せの趣旨を踏まえ、顧客対応方針を定め、顧客対応態勢を整備しているか。

⑹ 【偽造・盗難キャッシュカード対策】

（ⅰ）偽造･盗難キャッシュカード対策として、ATM システム等のセキュリティレベルを一定の基準に基づき評価しているか。当該評価を踏まえた体制面、技術面の検討を行い、適切な対策を講じているか。

（ⅱ）不正払戻し防止のために、適切な認証技術の採用、情報の漏えいの防止のための情報システムの整備等の措置を講じているか。

（ⅲ）異常な取引に関する基準や把握時の対応等を定め、異常な取引が把握された場合には適切な措置を講じているか。

２．サイバーセキュリティ管理

⑴ 【サイバーセキュリティ対策】

（ⅰ）サイバー攻撃に備え、入口対策、内部対策、出口対策といった多段階のサイバーセキュリティ対策を組み合わせた多層防御を講じているか。

- 入口対策（例えば、ファイアウォールの設置、抗ウィルスソフトの導入、不正侵入検知システム・不正侵入防止システムの導入　等）
- 内部対策（例えば、特権 ID・パスワードの適切な管理、不要な ID の削除、特定コマンドの実行監視　等）
- 出口対策（例えば、通信ログ・イベントログ等の取得と分析、不適切な通信の検知・遮断　等）

（ⅱ）サイバー攻撃を受けた場合に被害の拡大を防止するために、以下のような措置を講じているか。

- 攻撃元の IP アドレスの特定と遮断
- DDoS 攻撃に対して自動的にアクセスを分散させる機能
- システムの全部又は一部の一時的停止　等

（ⅲ）システムの脆弱性について、OS の最新化やセキュリティパッチの適用など必要な対策を適時に講じているか。

（ⅳ）サイバーセキュリティについて、ネットワークへの侵入検査や脆弱性診断等を活用するなど、セキュリティ水準の定期的な評価を実施し、セキュリティ対策の向上を図っているか。

⑵ 【コンティンジェンシープランの策定】

サイバー攻撃を想定したコンティンジェンシープランを策定し、訓練や見直しを実施しているか。また、必要に応じて、業界横断的な演習に参加しているか。

⑶ 【人材育成】

サイバーセキュリティに係る人材について、育成、拡充するための計画を策定し、実施しているか。

３．システム企画・開発・運用管理等

⑴ 【システム開発・運用部門の相互牽制態勢】

個人のミス及び悪意を持った行為を排除するため、システム開発部門と運用部門の分離分担を行っているか。なお、要員数の制約から業務部門を開発部門と運用部門に明確に分離することが困難な場合には、開発担当と運用担当を定期的にローテーションすること等により相互牽制を図っているか。また、EUC 等開発と運用の組織的分離が困難なシステムについては、内部監査部門等により牽制を図っているか。

⑵ システム企画・開発態勢

①【企画・開発態勢】

（ⅰ）信頼性が高くかつ効率的なシステム導入を図る企画・開発のための内部規程・業務細則等を整備しているか。

（ⅱ）システム企画・開発を行うに当たり、例えば、機械化委員会等の横断的な審議機関を設置し検討しているか。

（ⅲ）中長期の開発計画を策定しているか。

（ⅳ）現行システムに内在するリスクを継続的に洗い出し、その維持・改善のための投資を計画的に行っているか。

（ⅴ）システムへの投資効果を検討し、システムの重要度及び性格を踏まえ、必要に応じ（システム部門全体の投資効果については必ず）、取締役会に報告しているか。

（ⅵ）開発案件の企画・開発・移行の承認ルールが明確になっているか。

（ⅶ）本番システムの変更案件も承認のうえ実施しているか。

②【開発管理】

（ⅰ）開発に関わる書類やプログラムの作成方式は、標準化されているか。

（ⅱ）開発プロジェクトごとに責任者を定め、システムの重要度及び性格を踏まえ取締役会等及びオペレーショナル・リスクの総合的な管理部門が進捗状況をチェックしているか。

③【内部規程・業務細則等の整備】

（ⅰ）設計、開発、運用に関する内部規程・業務細則等を策定し、業務実態に即した見直しを実施しているか。

（ⅱ）設計書等は開発に関わる書類作成の標準規約を制定し、それに準拠して作成しているか。

（ⅲ）開発に当たっては、利用目的等に応じて監査証跡（処理内容の履歴を跡付けることができるジャーナル等の記録）を残すようなシステムとなっているか。

（ⅳ）マニュアル及び開発に関わる書類等は、専門知識のある第三者に分かりやすいものとなっているか。

④【テスト等】

（ⅰ）テスト計画を作成し、適切かつ十分にテストを行っているか。

（ⅱ）テストやレビュー不足が原因で、長期間顧客に影響が及ぶような障害や経営判断に利用されるリスク管理用資料等の重大な誤算が発生しないようなテスト実施態勢を整備しているか。

（ⅲ）総合テストは、ユーザー部門も参加するなど適切に実施されているか。

（ⅳ）検収に当たっては、内容を十分理解できる役職員により行われているか。

⑤【システム移行の決定】

（ⅰ）システム移行に係る責任者が明確になっているか。

（ⅱ）システムの移行計画を策定し、システム開発部門、システム運用部門、ユーザー部門等の役割と責任を明確にしているか。

（ⅲ）システムの移行判定基準等を策定し、当該基準等に基づきシステムの移行を決定しているか。

⑥【システム移行後の検証】

（ⅰ）システムの稼動後一定期間をおいて、移行後のレビューが実施されているか。

（ⅱ）移行後のレビューは、ユーザー要件の充足及び費用対効果等が検討、評価されているか。

（ⅲ）移行後のレビュー結果は、当該システムの今後の改善計画に反映されているか。

（ⅳ）移行後のレビュー結果は、システム開発部門及びユーザー部門等の責任者へ報告されているか。

（ⅴ）新しい商品や仕組みの導入後、ユーザー部門に対し、必要に応じてサンプルチェック等を実施させているか。

⑦【人材の育成】

現行システムの仕組み及び開発技術の継承並びに専門性を持った人材の育成のための具体的な計画を策定し、実施しているか。また、人材の育成に当たっては、開発技術の養成だけではなく、開発対象とする業務に精通した人材の養成を行っているか。例えば、デリバティブ業務、電子決済、電子取引等、専門性の高い業務分野や新技術についても、精通した開発要員を養成しているか。

⑶　システム運用態勢

①【職務分担の明確化】

（ⅰ）データ受付、オペレーション、作業結果確認、データやプログラムの保管の職務

分担は明確になっているか。

（ⅱ）システム運用担当者が担当外のデータやプログラムにアクセスすることを禁じているか。

②【システムオペレーション管理】

（ⅰ）所定の作業は、スケジュール表、指示表などに基づいてオペレーションを実施しているか。

（ⅱ）承認を受けた作業スケジュール表、作業指示書に基づいてオペレーションを実施しているか。

（ⅲ）オペレーションは、全て記録され、かつシステム運用部門の管理者は、チェック項目を定め点検しているか。

（ⅳ）重要なオペレーションについては、複数名により実施しているか。また、可能な限り自動化しているか。

（ⅴ）オペレーションの処理結果をシステム運用部門の管理者がチェックするためのレポート出力機能や、作業履歴を取得し、保存する機能を備えているか。

（ⅵ）開発担当者によるオペレーションへのアクセスを原則として禁じているか。障害発生時等でやむを得ず開発担当者がアクセスする場合には、当該オペレーションの管理者による開発担当者の本人確認及びアクセス内容の事後点検を行っているか。

③【本番データ管理】

（ⅰ）システムテスト等において、本番データを使用する場合の当該データの貸与に係る方針、手続きを明確に定めているか。

（ⅱ）本番データの貸与について、方針及び手続きに従った運用を行うなど、本番データの管理を適切に行っているか。

④【システム障害等の管理】

（ⅰ）経営に重大な影響を与えるような重要なシステム障害等が発生した場合には、速やかにシステムリスク管理部門及び関係業務部門と連携し、問題の解決を図るとともに、取締役会等及びオペレーショナル・リスクの総合的な管理部門に速やかに報告が行われる態勢を整備しているか。なお、報告に当たっては、最大リスク等を報告する態勢（例えば、顧客に重大な影響を及ぼす可能性がある場合、報告者の判断で過小報告することなく、最大の可能性を速やかに報告すること）となっているか。

（ⅱ）システム障害等の発生に備え、最悪のシナリオを想定した上で、必要な対応を行う態勢を整備しているか。

（ⅲ）システム障害等の発生に備え、関係業務部門への情報提供方法、内容が明確になっているか。また、顧客に適切に対応する態勢を整備しているか。

（ⅳ）システム障害等の発生に備え、外部委託先を含めた指揮・命令系統が明確になっているか。また、ノウハウ・経験を有する人材をシステム部門内、部門外及び外部委託先等から速やかに招集するために事前登録するなど、応援体制が明確になって

いるか。

（ｖ）システム障害等が発生した場合には、記録簿等に記入し、内部規程・業務細則等に基づき、システムリスク管理部門に報告が行われる態勢を整備しているか。

（vi）システムの運用を外部委託している場合、委託先において発生したシステム障害等について、報告が行われる態勢を整備しているか。

（vii）システム障害等の内容の定期的な分析を行い、それに応じた対応策をとっているか。

（viii）システム障害等の影響を極小化するために、例えば障害箇所を迂回するなどのシステム的な仕組みを整備しているか。

⑷ システム監査

（ｉ）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。

（ii）システム関係に精通した要員による内部監査の実施や、システム監査人等による外部監査の活用を行っているか。

４．防犯・防災・バックアップ・不正利用防止

⑴ 【防犯対策】

（ｉ）犯罪を防止するため、防犯組織を整備し、責任者を明確にしているか。

（ii）コンピュータシステムの安全性を脅かす行為を防止するため、入退室管理・重要鍵管理等、適切かつ十分な管理を行っているか。

⑵ 【コンピュータ犯罪・事故等】

コンピュータ犯罪及びコンピュータ事故（ウィルス等不正プログラムの侵入、CD/ATM の破壊・現金の盗難、カード犯罪、外部者による情報の盗難、内部者による情報の漏洩、ハードウェアのトラブル、ソフトウェアのトラブル、オペレーションミス、通信回線の故障、停電、外部コンピュータの故障等）に対して、十分に留意した態勢を整備し、点検等の事後チェック態勢を整備しているか。

⑶ 【防災対策】

（ｉ）災害時に備え、被災軽減及び業務の継続のための防災組織を整備し、責任者を明確にしているか。

（ii）防災組織の整備に際しては、業務組織に即した組織とし、役割分担毎に責任者を明確にしているか。

（iii）防火・地震・出水に対する対策を確保しているか。

（ⅳ）重要データ等の避難場所をあらかじめ確保しているか。

⑷ 【バックアップ】

（ⅰ）重要なデータファイル、プログラムの破損、障害等への対応のため、バックアップを取得し、管理方法を明確にしているか。

（ⅱ）バックアップを取得するに当たっては、分散保管、隔地保管等保管場所に留意しているか。

（ⅲ）バックアップ取得の周期を文書化しているか。

（ⅳ）業務への影響が大きい重要なシステムについては、オフサイトバックアップシステム等を事前に準備し、災害、システム障害等が発生した場合等に、速やかに業務を継続できる態勢を整備しているか。

⑸ 【コンティンジェンシープランの策定】

（ⅰ）災害等によりコンピュータシステムが正常に機能しなくなった場合に備えたコンティンジェンシープランを整備しているか。また、取締役の果たすべき役割・責任やとるべき対応について具体的に定めるとともに、取締役が自ら指揮を執る訓練を行い、その実効性を確保しているか。

（ⅱ）コンティンジェンシープランの策定及び重要な見直しを行うに当たっては、取締役会による承認を受けているか。（上記以外の見直しを行うに当たっては、取締役会等の承認を受けているか。）

（ⅲ）コンティンジェンシープランの策定に当たっては、「金融機関等におけるコンティンジェンシープラン（緊急時対応計画）策定のための手引書」（公益財団法人金融情報システムセンター編）を参照しているか。

（ⅳ）コンティンジェンシープランの策定に当たっては、災害による緊急事態を想定するだけではなく、金融機関の内部又は外部に起因するシステム障害等も想定しているか。また、バッチ処理が大幅に遅延した場合など、十分なリスクシナリオを想定しているか。

（ⅴ）コンティンジェンシープランの策定に当たっては、決済システムに及ぼす影響や、顧客に与える被害等を分析しているか。

（ⅵ）コンティンジェンシープランは、他の金融機関におけるシステム障害等事例や中央防災会議等の検討結果を踏まえるなど、想定シナリオの見直しを適宜行っているか。

（ⅶ）コンティンジェンシープランに基づく訓練は、全社レベルで行い、複数の金融機関の業務を受託するセンター等の外部委託先等と合同で、定期的に実施しているか。

５．外部委託管理[7]

[7] 外部委託の形態や委託される業務内容は多様であり、当該検証項目においては、外部委託された業務の

⑴ 外部委託業務の管理

①【外部委託先の選定】

システムリスク管理部門[8]は、外部委託管理責任者と連携し、外部委託（二段階以上の委託を含む。）の実施前に当該外部委託業務に内在するシステムリスクを特定し、サービスの質や存続の確実性等のリスク管理上の問題点を認識した上で、外部委託業務を的確、公正かつ効率的に遂行することができる能力を有する者に委託するための措置を講じているか。外部委託先の選定に当たり、例えば、システムリスク管理の観点から、以下のような点に留意しているか。

- 金融機関の合理性の観点からみて十分なレベルのサービスの提供を行い得るか。
- 委託契約に沿ったサービス提供や損害負担が確保できる財務・経営内容か。
- 金融機関のレピュテーション等の観点[9]から問題ないか。

②【委託契約の内容】

システムリスク管理部門[8]は、外部委託管理責任者と連携し、委託契約において、提供されるサービス水準、外部委託先との役割分担や責任分担（例えば、委託契約に沿ってサービスが提供されない場合における外部委託先の責務、又は委託に関連して発生するおそれのある損害の負担の関係）、監査権限及び再委託手続き等について定めていることを確認するための措置を講じているか。

また、外部委託先が遵守すべきルールやセキュリティ要件を外部委託先へ提示し、契約書等に明記しているか。

③【外部委託先のモニタリング】

システムリスク管理部門[8]は、外部委託管理責任者と連携し、外部委託した業務（二段階以上の委託を含む。）について、委託元として委託業務が適切に行われていることを定期的にモニタリングするために、例えば要員を配置するなどの必要な措置を講じているか。特に複数の金融機関の業務を受託するセンターの内部管理、開発・運用管理の状況について、報告を受ける態勢を整備しているか。

また、システムの共同化等が進展する中、外部委託先における顧客データの管理状況を、委託元が監視、追跡できる態勢を整備しているか。

④【外部委託先への監査】

複数の金融機関の業務を受託するセンター等の重要な外部委託先に対して、内部監査部門又はシステム監査人等による監査を実施しているか。

⑤【問題点の是正】

システムリスク管理部門[8]は、問題点等を発見した場合には、外部委託管理責任者と連携して速やかに是正する措置を講じているか。

内容及び当該金融機関における重要度等を踏まえた検証が必要である。

[8] オペレーショナル・リスクの総合的な管理部門において行うことを妨げるものではない。

[9] 例えば、外部委託先と反社会的勢力との関係の有無などを含む。

⑵ システム関係の業務委託先の検証

① 業務委託を受けたシステム全般について、システムリスクを認識・評価しているか。

② 金融機関から受託したシステム業務について、委託者による監査又は外部監査を定期的に受けているか。また、外部監査を実施した場合は、委託者に対して監査結果を報告しているか。

③ 金融機関等が求めるセキュリティレベルを設定し、その内容についてあらかじめ金融機関等と合意しているか。

④ 企画段階、設計・開発段階、テスト段階において、金融機関等によるユーザーレビューやユーザーテストが実施されているか。

⑤ 開発標準ルールの遵守状況や品質管理状況について、品質管理部署等により客観的に評価する態勢を整備しているか。

⑥ システムの運用状況について、金融機関等に対して報告する事項を定め、定期的に報告しているか。

⑦ システム障害等の発生時の連絡態勢を、あらかじめ定めているか。

⑧ 複数の金融機関の業務を受託するセンターの場合、他の金融機関への影響等を速やかに判断し、対応する態勢を整備しているか。

６．付保預金の円滑な払戻しのための整備状況等

⑴ 預金保険法第 55 条の２第４項及び第 58 条の３第 1 項を遵守するための取組みがなされる態勢を整備しているか[10]。

⑵ 名寄せに係るデータベース及びシステムの整備等を適切に行っているか。

具体的には、以下のような対応を適切に行っているか。

① 名寄せデータが適切に維持、登録される態勢を整備しているか。

② 名寄せデータ（名寄せ用カナ氏名、生年月日等）を正しく登録しているか。また、登録状況を検証しているか。

⑶ 保険事故が発生した場合における支払対象預金等に係る保険金の支払又はその払戻し、その他の保険事故に対処するために必要な措置の円滑な実施の確保を図るために必要なシステムの整備等を適切に行っているか。

⑷ 新商品取扱に係るプログラム修正やシステム更改等を実施した場合におけるシステムの整備等を適切に行っているか。

⑸ 以下の作業について、手順書・マニュアルを整備しているか[11]。

① 保険事故発生から磁気テープ等を預金保険機構に提出するまでの作業（同法第 55 条の２第３項）。

---

10 「預金保険法第 55 条の２第４項及び第 58 条の３第１項関連チェック項目」（監督指針・参考資料編）を参照。

11 「預金保険法第 55 条の２及び第 58 条の３に規定された有事の措置を円滑に行うための手順書・マニュアルに関するチェックポイント」（預金保険機構）を参照。

② 金融機関が預金保険機構から預金等に係る債権に関するデータを受け取った後、当該データを預金等の払戻しを行っているシステムにおいて処理するまでの作業（預金保険法第 58 条の３第１項に規定する措置に関する内閣府令第１条第１項第１号)。

③ 上記②のデータを用いずに支払対象決済用預金の払戻しを行う作業（同項第２号)。

④ 保険事故発生後の預金等の変動に係るデータを預金保険機構に提出する作業（同項第３号)。

⑤ 預金者等に対する債権と支払対象預金等との相殺及び預金等債権の買取り等に係る作業（同項第４号)。

７．システム統合に係るリスク管理態勢

システム統合に係るリスク管理の検証については、「システム統合リスク管理態勢の確認検査用チェックリスト」(平成 14 年 12 月 26 日付検第 567 号)に基づき行うものとする。

（別紙３）

その他オペレーショナル・リスク管理態勢の整備・確立状況

【検証ポイント】

- **その他オペレーショナル・リスクとは、当該金融機関がオペレーショナル・リスクと定義したリスクのうち、事務リスク及びシステムリスクを除いたリスクをいう。**
- **金融機関におけるオペレーショナル・リスクのうち、事務リスク及びシステムリスクを除いたリスク管理態勢の整備・確立についても、金融機関の業務の健全性及び適切性の観点から極めて重要であり、経営陣には、その他オペレーショナル・リスクの管理について態勢の整備・確立を自ら率先して行う役割と責任がある。**
- **検査官は、その他オペレーショナル・リスク管理態勢が有効に機能しているか否か、経営陣の役割と責任が適切に果たされているかを、必要に応じて、「事務リスク管理態勢」、「システムリスク管理態勢」等を参考にして、確認する。**

１．【取締役の役割・認識】

取締役は、金融機関がオペレーショナル・リスクと定義したリスクのうち、事務リスク及びシステムリスクを除いたオペレーショナル・リスク管理について軽視することが戦略目標に重大な影響を与えることを十分に認識し、当該リスク管理を重視しているか。特に担当取締役は、当該リスクの所在、当該リスクの種類・特性及び当該リスクの特定・評価・モニタリング・コントロール等の手法並びに当該リスク管理の重要性を十分に理解し、この理解に基づき金融機関の当該リスク管理の状況を的確に認識し、その他オペレーショナル・リスクに応じた適正な管理態勢を整備しているか。

２．その他オペレーショナル・リスク管理部門のうち、主なリスク管理部門の役割・責任

⑴ 【法務リスクを管理する部門】

法務リスクを管理する部門は、顧客に対する過失による義務違反及び不適切なビジネス・マーケット慣行から生じる損失・損害（監督上の措置並びに和解等により生じる罰金、違約金及び損害賠償金等を含む）など当該金融機関が法務リスクとして定義したものについて、当該金融機関が直面するリスクを認識し、適切に管理を行っているか。例えば、法務リスクを管理する部門は、「法令等遵守態勢の確認検査用チェックリスト」、「顧客保護等管理態勢の確認検査用チェックリスト」に記載している点のうち、当該金融機関の定義に該当するものについて、法務リスクとして認識し、適切な管理を行っているか。

⑵ 【人的リスクを管理する部門】

人的リスクを管理する部門は、当該金融機関が、人事運営上の不公平・不公正（報酬・手当・解雇等の問題）・差別的行為（セクシュアルハラスメント等）から生じる損失・損害など人的リスクとして定義したものについて、当該金融機関が直面するリスクを認識し、適切な管理を行っているか。例えば、人的リスクを管理する部門は、各業務部門及び営業店等の人的リスクの管理能力を向上させるための研修・教育などの方策を実施し、適切な管理を行っているか。

⑶ 【有形資産リスクを管理する部門】

有形資産リスクを管理する部門は、当該金融機関が災害その他の事象から生じる有形資産の毀損・損害など有形資産リスクとして定義したものについて、当該金融機関が直面するリスクを認識し、適切な管理を行っているか。

⑷ 【風評リスクを管理する部門】

風評リスクを管理する部門は、当該金融機関が評判の悪化や風説の流布等により、信用が低下することから生じる損失・損害など風評リスクとして定義したものについて、当該金融機関が直面するリスクを認識し、適切な管理を行っているか。例えば、以下の点のような方策を実施することにより、適切な管理を行っているか。

- 風評リスクを管理する部門は、風評発生時における各業務部門及び営業店等の対応方法を定めているか。
- 風評リスクを管理する部門は、風評が伝達される媒体（例えば、インターネット、憶測記事等）に応じて、定期的に風評のチェックを行っているか。

３.【危機管理態勢の適切性】

（ⅰ）平時の危機管理を担当する担当者又は担当部門は、定期的な点検・訓練を行うなど危機発生時のリスク回避又は軽減の取組みを行っているか。

（ⅱ）危機管理マニュアル等には、危機発生の初期段階における的確な状況把握や客観的な状況判断を行うことの重要性や情報発信の重要性など、初期対応の重要性が盛り込まれているか。

（ⅲ）危機管理マニュアル等には、自らの業務の実態やリスク管理の変化に応じ、不断の見直しが行われているか。

（ⅳ）危機管理マニュアル等には、危機発生時における責任態勢が明確化され、危機発生時の組織内及び関係者（関係当局を含む。）への連絡態勢等が明記されているか。

（ｖ）業務継続計画（BCP）においては、テロや大規模な災害等の事態においても早期に被害の復旧を図り、金融システムの機能の維持にとって必要最低限の業務の継続が可能となっているか。例えば、以下の項目について、明確に規定する等適切な内容となっているか。

- 災害等に備えた顧客データ等の安全対策（紙情報の電子化、電子化されたデータファイルやプログラムのバックアップ等）は講じられているか。
- コンピュータシステムセンター等の安全対策（バックアップセンターの配置、要員・通信回線確保等）は講じられているか。
- これらのバックアップ措置は、地理的集中を避けているか。
- 個人に対する現金払出や送金依頼の受付、インターバンク市場や銀行間決済システムを通じた大口・大量の決済の処理等の金融機能の維持の観点から重要な業務を、暫定的な手段（手作業、バックアップセンターにおける処理等）により再開（リカバリー）するまでの目標時間は具体的に計画されているか。

（vi）危機発生時の情報発信・収集態勢は、危機のレベル・類型に応じて十分なものになっているか。また、日頃からきめ細かな情報発信及び情報収集に努めているか。