オペレーショナル・リスク等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・リスク等管理態勢の整備・確立状況

【検証ポイント】

・　本チェックリストにおいて、「オペレーショナル・リスク等」とは、①～④をいい、「オペレーショナル・リスク等管理」とは、①～④をそれぞれ適切に管理することをいう。

①　役職員等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保険会社が損失を被るリスク（以下「事務リスク」という。）。

②　コンピュータシステムのダウン又は誤作動等、システムの不備等に伴い保険会社が損失を被るリスク、さらにコンピュータが不正に使用されることにより保険会社が損失を被るリスク（以下「システムリスク」という。）。

③　保険会社の財務内容の悪化等による新契約の減少に伴う保険料収入の減少、大量ないし大口解約に伴う解約返戻金支出の増加、巨大災害での資金流出により資金繰りが悪化し、資金の確保に通常よりも著しく低い価格での取引を余儀なくされることにより損失を被るリスク（以下「資金繰りリスク」という。）及び市場の混乱等により市場において取引ができなかったり、通常よりも著しく不利な価格での取引を余儀なくされることにより損失を被るリスク（以下「市場流動性リスク」という。）。なお、資金繰りリスクと市場流動性リスクをあわせて、以下「流動性リスク」という。

④　その他保険会社が「オペレーショナル・リスク」と定義したリスク（以下「その他オペレーショナル・リスク」という。）。

・　保険会社におけるオペレーショナル・リスク等管理態勢の整備・確立は、保険会社の業務の健全かつ適切な運営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・リスク等管理態勢を検証するに当たっては、保険会社の業務の規模・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・リスク等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、保険会社においては、事務リスク、システムリスク、流動性リスクの計量化については、まだ確立されたものはないため、本チェックリストで記載していないが、検査官は、保険会社がリスク管理の更なる高度化に向けた不断の取組みを行っているかについて検証することとする。

・　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（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）及び性格（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。）に十分留意する必要がある。また、本チェックリストによる検証の結果、システムリスク管理態勢に問題が見られ、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、検査官は、「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

基づき行うものとする。さらに、検査官は、保険会社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行うこととする。

・　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。

　また、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。

・　本チェックリストにおいては、流動性リスク管理部門を資金繰りに関する内部基準等の遵守状況等のモニターを行う部門と、資金繰り管理部門を資金繰りの管理・運営を行っている部門とそれぞれ位置付けた上で、流動性リスク管理態勢にかかる検証項目を記載している。検査官は、保険会社によって流動性リスク管理部門と資金繰り管理部門の果たすべき役割と負うべき責任の範囲が異なることに留意し、流動性リスク管理が全体として適切に機能しているかを検証する必要がある。

・　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、オペレーショナル・リスク等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】

（ⅰ）取締役は、オペレーショナル・リスク等の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・リスク等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・リスク等の所在、種類・特性及びオペレーショナル・リスク等の特定・評価・モニタリング・コントロール等の手法並びに管理の重要性を十分に理解し、この理解に基づき当該保険会社のオペレーショナル・リスク等の管理の状況を的確に認識し、適正なオペレーショナル・リスク等の管理態勢の整備・確立に向けて、方針及び具体的な方策を検討しているか。

（ⅱ）取締役は、システム障害等（システム障害やサイバーセキュリティ事案[1]をいう。以下同じ。）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、システムリスク管理（システム障害等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。）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。

②【戦略目標】

（ⅰ）取締役会は、情報技術革新を踏まえ、保険会社全体の経営方針に沿った戦略目標の中に、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

（ⅱ）取締役は、流動性に支障をきたせば、場合によっては経営破綻に直結するおそれがあることを理解し、取締役会において、戦略目標を定めるに当たり、流動性リスクを考慮しているか。

③【オペレーショナル・リスク等管理方針の整備・周知】

（ⅰ）取締役会は、オペレーショナル・リスク等の管理のために以下に掲げる方針（以下総称して「オペレーショナル・リスク等管理方針」という。）を定め、組織全体に周知させているか。

- 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。）

---

[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。

・　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。）

・　流動性リスク管理に関する方針（以下「流動性リスク管理方針」という。）

（ⅱ）事務リスク管理方針には、例えば、以下の項目が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、モニタリング及びコントロールに関する方針

（ⅲ）システムリスク管理方針には、例えば、以下の項目が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]

（ⅳ）流動性リスク管理方針には、例えば、以下の項目が明確に記載される等、適切なものとなっているか。

・　流動性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

・　流動性リスク管理に関する部門（以下「流動性リスク管理部門」という。）及び資金繰り運営に関する部門（以下「資金繰り管理部門」という。）の設置、権限の付与等の組織体制に関する方針

・　流動性リスクの限度枠の設定に関する方針

・　流動性リスク管理部門と資金繰り管理部門の役割・責任の分担に関する方針

・　流動性リスクの特定、評価、モニタリング及びコントロールに関する方針

・　流動性危機管理に関する方針

④【方針策定のプロセスの見直し】

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・リスク等の管理状況に関する報告・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] ・「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。

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

⑴　事務リスク管理態勢の整備

①【内部規程の整備・周知】

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。[3]

（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事務リスク管理部門の管理者を配置し、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。[4]

（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拠点等における事務リスク管理態勢の整備】

取締役会等は、事務リスク管理部門の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拠点等に対し、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するなど、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。例えば、事務リスク管理部門の管理者に各業務部門及び営業拠点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。

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、事務リスク管理部門の管理者に、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、

---

[3] 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、当該保険会社の規模・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、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。

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。

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事務リスク管理部門の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、内部監査部門又は内部監査部門長に、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。[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。

- 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。

⑵　システムリスク管理態勢の整備

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】

（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。[7]

---

[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。

[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。

[7] 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一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

（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システムリスク管理部門の管理者を配置し、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。[8]

（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拠点等におけるシステムリスク管理態勢の整備】

取締役会等は、システムリスク管理部門の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拠点等に対し、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するなど、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。例えば、システムリスク管理部門の管理者に各業務部門及び営業拠点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。

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、システムリスク管理部門の管理者に、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。

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システムリスク管理部門の管理者から直接報告を行わせる態勢を整備しているか。[9]

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、内部監査部門又は内部監査部門長に、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。[10]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。

合や、部門や部署で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、当該保険会社の規模・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。

[8] 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。

[9] 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。

[10] 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。

・　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。

⑶　流動性リスク管理態勢の整備

①【内部規程の整備・周知】

取締役会等は、流動性リスク管理方針に則り、流動性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「流動性リスク管理規程」という。）を流動性リスク管理部門の管理者に策定させ、組織内に周知させているか。取締役会等は、流動性リスク管理規程についてリーガル・チェック等を経て、流動性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【限度枠の設定及び見直し】

取締役会等は、適切な流動性リスク管理を行うため、資産運用の内容等により、必要に応じ、市場のない若しくは非常に流動性の低い資産の運用上の限度額等の限度枠の設定及び見直しを行っているか。また、一定の流動性資産の残高を確保するといった限度枠の設定及び見直しを行っているか。

③【流動性リスク管理部門及び資金繰り管理部門の態勢整備】

（ⅰ）取締役会等は、流動性リスク管理方針及び流動性リスク管理規程に則り、流動性リスク管理部門及び資金繰り管理部門を設置し、適切な役割を担わせる態勢を整備しているか。[11]

（ⅱ）取締役会は、流動性リスク管理部門及び資金繰り管理部門に、当該部門を統括するのに必要な知識と経験を有する流動性リスク管理部門の管理者及び資金繰り管理部門の管理者を配置し、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、流動性リスク管理部門及び資金繰り管理部門に、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。[12]

---

[11] 流動性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、他の業務と兼担する部署が流動性リスク管理を担当する場合や、部門や部署でなく責任者が流動性リスク管理を担当する場合等）には、当該保険会社の規模･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。

[12] 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・

（ⅳ）取締役会等は、流動性リスク管理部門について、資金繰り管理部門、資産運用部門、保険引受部門等からの独立性を確保することなどにより、牽制機能が発揮される態勢を整備しているか。

④【資金繰り管理部門、資産運用部門、保険引受部門等における流動性リスク管理態勢の整備】

取締役会等は、流動性リスク管理部門の管理者又は流動性リスク管理部門を通じ、管理すべき流動性リスクの関係する部門（例えば、資金繰り管理部門、資産運用部門、保険引受部門等）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するなど、流動性リスク管理の実効性を確保する態勢を整備しているか。例えば、流動性リスク管理部門の管理者に、資金繰り管理部門、資産運用部門、保険引受部門等が遵守すべき内部規程・業務細則等を特定させ、具体的な施策を行うよう指示しているか。

⑤【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、流動性リスク管理部門の管理者及び資金繰り管理部門の管理者に、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。

⑥【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流動性リスク管理部門の管理者から直接報告を行わせる態勢を整備しているか。[13]

⑦【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、内部監査部門又は内部監査部門長に、流動性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。[14]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。

- 流動性リスク管理態勢の整備状況
- 流動性リスク管理方針、流動性リスク管理規程等の遵守状況
- 流動性リスク管理システム[15]の適切性
- 業務の規模・特性及びリスク・プロファイルに見合った流動性リスク管理プ

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。

[13] 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。

[14] 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。

[15] 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。以下同じ。

ロセスの適切性

- 流動性リスク分析・評価方法、仮定等の妥当性
- 流動性危機管理の有効性
- 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

⑧【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、流動性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【オペレーショナル・リスク等管理の分析・評価】

取締役会等は、監査役監査、内部監査及び外部監査[16]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・リスク等管理の状況に関する情報に基づき、オペレーショナル・リスク等管理の状況を的確に分析し、オペレーショナル・リスク等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万全を期しているか。

②【分析・評価のプロセスの見直し】

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・リスク等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】

---

[16] ここに言う外部監査は、会計監査人による財務諸表監査に限定するものではないが、現状では、制度上義務付けられている財務諸表監査及び同監査手続の一環として実施される内部管理態勢の有効性等の検証以外の外部監査を義務付けるものではないことに留意する必要がある。
ただし、保険会社が、内部管理態勢の有効性等を確保するため、財務諸表監査と別に外部監査を受けている場合は、財務諸表監査の結果と併せて、内部管理態勢の有効性等を総合的に検証することとなる。

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・リスク等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・リスク等管理態勢の整備・確立状況

【検証ポイント】

・　本章においては、

①　事務リスク管理部門の管理者及び事務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

②　システムリスク管理部門の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

③　流動性リスク管理部門の管理者及び資金繰り管理部門の管理者並びに流動性リスク管理部門及び資金繰り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

について記載している。

・　なお、流動性リスクについては、保険会社の業務の規模・特性及びリスク・プロファイル等によって、流動性リスク管理部門と資金繰り管理部門の果たすべき役割と負うべき責任の範囲が異なることに留意し、流動性リスク管理が全体として適切に機能しているかを検証する必要がある。

・　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．事務リスク管理態勢

⑴　事務リスク管理部門の管理者の役割・責任

①【事務リスク管理規程の整備・周知】

事務リスク管理部門の管理者は、事務リスクの所在、種類・特性及び管理手法を十分に理解し、事務リスク管理方針に沿って、リスクの特定、評価及びモニタリングの方法を決定し、これに基づいたリスクのコントロール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、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
・　取締役会等に報告する態勢に関する取決め

③【事務リスク管理部門の管理者による組織体制の整備】

（ⅰ）事務リスク管理部門の管理者は、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）事務リスク管理部門の管理者は、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）事務リスク管理部門の管理者は、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、取締役会等に対し速やかに報告する態勢を整備しているか。

（ⅳ）事務リスク管理部門の管理者は、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（事務リスク管理部門の管理者含む。）が職場を離れる方策をとっているか。事務リスク管理部門の管理者は、その状況を管理し、当該方策を確実に実施しているか。

（ⅴ）事務リスク管理部門の管理者は、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には、他の方策により事故防止等の実効性を確保しているか。事務リスク管理部門の管理者は、その状況を管理し、当該方策を確実に実施しているか。

（ⅵ）事務リスク管理部門の管理者は、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。
・　職員に比べて人事情報が少ない等の派遣職員等の特性を踏まえ人事・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。

（ⅶ）事務リスク管理部門の管理者は、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、新規商品等管理方針等に基づき、事前に内在する事務リスクを特定し、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。[17]

④【事務リスク管理規程及び組織体制の見直し】

事務リスク管理部門の管理者は、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、

[17] 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。

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。

⑵ 事務リスク管理部門の役割・責任[18]

①【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、営業拠点等の事務だけでなく、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
- 保険募集（禁止行為等）に関する手続
- 現金・現物・重要書類（保険料領収証）・便宜扱い等の異例扱いの手続
- 通信販売等の非対面募集に関する手続

（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・相談・苦情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拠点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拠点長が、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、営業拠点等及び保険募集人による自主点検等の実施基準、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、営業拠点等及び保険募集人において実施した自主点検結果の報告を受けているか。また、実効性のある自主点検となっているか検証を行っているか。

（ⅷ）事務統括部門は、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、事務リスクを特定しているか。リスクの特定に当たっては、例えば、商品開発等に関し、既存の各種規程等との整合性について検討を行

[18] 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。

っているか。これらの検討に当たっては、営業推進部門から不当な影響を受けることなく行っているか。[19]

（ix）事務統括部門は、事務規程の整備又は見直し及び改善、自主点検等の実施基準、実施要領の策定等にあたっては、保険募集管理部門及び他のリスク管理部門等との連携を適切に行っているか。

②【事務指導部門の役割・責任】

（ⅰ）事務指導部門は、各業務部門、営業拠点等及び保険募集人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等を活用して、内部監査部門及び保険募集管理部門等と連携して各業務部門、営業拠点等及び保険募集人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、営業拠点等及び保険募集人からの問い合わせ等に迅速かつ正確に対応しているか。

[19] 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。

２．システムリスク管理態勢

⑴　システムリスク管理部門の管理者の役割・責任

①【システムリスク管理規程の整備・周知】

システムリスク管理部門の管理者は、システムリスクの所在、種類・特性及び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、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、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
- 取締役会等に報告する態勢に関する取決め

③【システムリスク管理部門の管理者による組織体制の整備】

（ⅰ）システムリスク管理部門の管理者は、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）システムリスク管理部門の管理者は、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）システムリスク管理部門の管理者は、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、取締役会等に対し速やかに報告する態勢を整備しているか。

（ⅳ）システムリスク管理部門の管理者は、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）システムリスク管理部門の管理者は、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）システムリスク管理部門の管理者は、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）システムリスク管理部門の管理者は、ネットワーク稼働状況の管理、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。

（viii）システムリスク管理部門の管理者は、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、新規商品等管理方針等に基づき、事前に内在するシステムリスクを特定し、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。[20]

④【システムリスク管理規程及び組織体制の見直し】

システムリスク管理部門の管理者は、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。

⑵　システムリスク管理部門の役割・責任

①【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、業務系、情報系、資産運用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日当たりの処理可能な契約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、

[20] 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。

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。

（ⅶ）システムリスク管理部門は、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、システムリスクを特定しているか。[21]

②【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、当該保険会社の内部環境（リスク・プロファイル等）や外部環境の状況に照らし、当該保険会社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【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。

④【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。

[21] 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。

３．流動性リスク管理態勢

⑴　流動性リスク管理部門の管理者及び資金繰り管理部門の管理者の役割・責任

①【流動性リスク管理規程の整備】

流動性リスク管理部門の管理者は、流動性リスクの所在、種類・特性及び管理手法を十分に理解し、流動性リスク管理方針に沿って、リスクの特定、評価及びモニタリングの方法を決定し、これに基づいたリスクのコントロールに関する取決めを明確に定めた、統合的リスク管理態勢と整合的な流動性リスク管理規程を策定しているか。流動性リスク管理規程は、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【流動性リスク管理規程の内容】

流動性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、流動性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。

- 流動性リスク管理部門及び資金繰り管理部門の役割・責任及び組織に関する取決め
- 流動性リスクに影響を与える要因の特定及び要因発生時の報告基準に関する取決め
- 流動性リスクの分析・評価方法に関する取決め
- 流動性リスクのモニタリング方法に関する取決め
- 流動性リスクの限度枠の設定に関する取決め
- 資産と負債の総合的な管理に関する取決め
- 統合的リスク管理部門との連携に関する取決め
- 資金繰りの逼迫度区分（例えば、平常時、懸念時、危機時、巨大災害時等）及び判定基準に関する取決め
- 資金繰りの各逼迫度区分における管理手法、報告方法、決裁方法及び対応策に関する取決め
- 流動性危機発生時の保険会社全体での対応策に関する取決め
- 取締役会等に報告する態勢に関する取決め

③【流動性危機時の対応策（コンティンジェンシー・プラン）の策定】

流動性リスク管理部門の管理者は、流動性リスク管理方針、流動性リスク管理規程に則り、流動性危機時の対応策（コンティンジェンシー・プラン）を策定しているか。当該対応策に、流動性危機の定義、流動性危機時の連絡・報告体制（直接代表取締役に報告される体制等）、対処方法（調達手段の確保）、決裁権限・命令系統等が明確に定められているか。流動性危機時の対応策（コンティンジェンシー・プラン）は、取締役会等の承認を受けた上で、周知されているか。

④【流動性リスク管理部門の管理者及び資金繰り管理部門の管理者による組織体制の整備】

（ⅰ）流動性リスク管理部門の管理者は、流動性リスク管理方針及び流動性リスク管理規程に基づき、適切な流動性リスク管理を行うため、流動性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）流動性リスク管理部門の管理者は、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）流動性リスク管理部門の管理者は、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、新規商品等管理方針等に基づき、事前に内在する流動性リスクを特定し、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。[22]

（ⅳ）流動性リスク管理部門の管理者及び資金繰り管理部門の管理者は、リスク・プロファイルに見合った適切な流動性リスク管理を行う観点から、例えば大口取引動向など、取得すべき情報を特定し、当該情報を保有する部門から、定期的に又は必要に応じて随時、報告を受ける態勢を整備しているか。

（ⅴ）流動性リスク管理部門の管理者及び資金繰り管理部門の管理者は、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流動性リスク管理システムを整備しているか。

（ⅵ）流動性リスク管理部門の管理者及び資金繰り管理部門の管理者は、流動性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。

（ⅶ）流動性リスク管理部門の管理者及び資金繰り管理部門の管理者は、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。

⑤【流動性リスク管理規程及び組織体制の見直し】

流動性リスク管理部門の管理者は、継続的に流動性リスク管理部門及び資金繰り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、流動性リスク管理態勢の実効性を検証し、必要に応じて流動性リスク管理規程等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。

⑵　流動性リスク管理部門の役割・責任

①【流動性リスクの特定・評価】

（ⅰ）流動性リスクに影響を与える要因の特定

イ．流動性リスク管理部門は、流動性リスクに影響を与える内生的要因及び外生的要因を特定しているか。また、信用リスク、市場リスク、オペレーショナル・リ

[22] 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。

スク等が流動性リスクに影響を与えることを理解し、例えば、大口の資金移動、決算状況の悪化、市場の大幅な下落、事務処理システムの障害等について流動性リスクに影響を与える要因として特定しているか。

ロ．流動性リスク管理部門は、新規商品等の取扱い、新規の商品の購入、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、事前に流動性リスクの所在及びその影響を把握しているか。[23]

（ⅱ）流動性リスクの統合的な管理

流動性リスク管理部門は、通貨毎に流動性リスクを管理するだけではなく、それぞれの流動性リスクを統合して管理しているか。また、当該保険会社の流動性リスクに影響を与える重要なグループ会社の資金繰りの状況も把握しているか。

（ⅲ）出再保険の管理

流動性リスク管理部門は、資金繰りリスクの管理に当たっては、出再先の保険会社の財務状況によっては、出再保険金を受領できなくなる恐れがあることを十分考慮しているか。

（ⅳ）流動性リスクの評価

イ．流動性リスク管理部門は、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流動性リスクの分析・評価を行っているか。例えば、以下の状況を把握して分析を行うことにより流動性リスクの状況を評価しているか。

- 国内外にて取扱う各国通貨の特性
- 金融商品毎の市場流動性の状況（市場規模・取引量等）
- 全体及び通貨毎の資金繰り状況
- 保険料収入及び保険金等支出の実績と計画
- 保有資産の通貨・商品・期間別の構成及び残高
- 流動性資産の残高
- 市場性資金調達状況及び調達可能性
- 契約上の受信枠及び与信枠の残高　　等

ロ．流動性リスク管理部門は、資産・負債の総合的な管理及び自己資本等の状況を踏まえた上で、内生的要因及び外生的要因の両面について考慮した複数のシナリオを用いて流動性リスクの分析・評価を行っているか。

（ⅴ）現状の資金繰りの逼迫度区分の判定

流動性リスク管理部門は、資金繰り管理部門と連携し、当該保険会社のリスク・プロファイル等の内部環境、経済や市場等の外部環境等の情報を収集・分析し、当該保険会社が現状においてどの資金繰りの逼迫度区分に該当するかを適切に判定しているか。

②【モニタリング】

[23] 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。

（ⅰ）流動性リスクのモニタリング

流動性リスク管理部門は、流動性リスク管理方針及び流動性リスク管理規程に基づき、資金繰り管理部門からの報告、当該保険会社のリスク・プロファイル等の内部環境、経済や市場等の外部環境等の情報を収集・分析し、それらの動向について継続的にモニタリングしているか。また、モニタリングしている情報は流動性リスク管理のために有効なものとなっているか。

（ⅱ）限度枠の遵守状況等のモニタリング

流動性リスク管理部門は、限度枠を設定している場合には、適切にその遵守状況及び使用状況をモニタリングしているか。

（ⅲ）資金繰りの逼迫度区分の判定基準の適切性等のモニタリング

流動性リスク管理部門は、資金繰りの逼迫度区分の判定基準となる各種指標等の状況及び判定基準の適切性についてモニタリングしているか。

（ⅳ）取締役会等への報告

流動性リスク管理部門は、流動性リスク管理方針及び流動性リスク管理規程に基づき、流動性リスク管理の状況及び流動性リスクの状況に関して、取締役会等が適切に評価・判断できる情報を、定期的に又は必要に応じて随時、直接、報告しているか。例えば、以下の項目について報告しているか。

- 流動性リスクに大きな影響を与える要因
- 経済や市場等の外部環境の状況
- 資金繰りの逼迫度の状況
- 流動性リスクの水準及びその傾向
- 限度枠の遵守状況及び使用状況

（ⅴ）資金繰り管理部門、資産運用部門等への還元

流動性リスク管理部門は、資金繰り管理部門、資産運用部門等に対し、流動性リスクの状況について分析・評価し、検討した結果等を還元しているか。

③【コントロール】

（ⅰ）限度枠を超過した場合の対応

流動性リスク管理部門は、限度枠を設定している場合で、その限度枠を超過した場合には、速やかに、対応策を策定できる情報を取締役会等に報告しているか。

（ⅱ）資金繰りの逼迫度が変更される場合の対応

流動性リスク管理部門は、現状の資金繰りの逼迫度区分が変更される場合又はそのおそれがある場合、速やかに、資金繰りの逼迫度の状況及び今後の見通しなど対応策を策定できる情報を取締役会等に報告しているか。

（ⅲ）流動性危機時の調達手段の確保

流動性リスク管理部門は、国内外において即時売却可能な資産（国債等）の保有残高や調達可能時点・金額を常時把握するとともに、資金繰り管理部門に市中金融機関から調達が行えるよう借入枠を設定させるなど、危機時を想定した調達

手段を確保させているか。

④【検証・見直し】

（ⅰ）流動性リスクに影響を与える要因の特定の妥当性の検証及び要因発生時の報告基準の見直し

流動性リスク管理部門は、流動性リスクに影響を与える内生的及び外生的要因の特定の妥当性について、定期的に又は必要に応じて随時、検証し、見直しているか。

また、要因発生時の報告基準について、その基準が当該保険会社のリスク・プロファイル等の内部環境、経済や市場等の外部環境等に応じて適切であるかを定期的に又は必要に応じて随時、検証し、見直しているか。

（ⅱ）流動性リスクの分析・評価方法の見直し

流動性リスク管理部門は、流動性リスクの分析・評価方法が業務の規模・特性、リスク・プロファイル及び外部環境に見合ったものかを、定期的に又は必要に応じて随時、検証し、見直しているか。特に分析・評価における仮定は継続的に有効なものとなっているか。

（ⅲ）限度枠の設定方法及び水準の見直し

流動性リスク管理部門は、複数のストレス・シナリオ等による影響度評価及び流動性リスクに影響を与える内生的及び外生的要因について分析・評価を行うことで、必要に応じ設定した限度枠の設定方法及び水準が、業務の規模・特性、リスク・プロファイル、財務状況及び資金調達能力に見合ったものかを、定期的に又は必要に応じて随時、検証しているか。見直しの必要性が認められる場合には、速やかに、取締役会等が適切に評価及び判断できる情報を報告しているか。

（ⅳ）資金繰りの逼迫度区分、判定基準等の見直し

流動性リスク管理部門は、以下の観点から複数のストレス・シナリオ等による影響度評価及び対応策の実効性についての確認等を行うことにより、資金繰りの逼迫度区分、判定基準、管理手法、報告方法、決裁方法等が適切であるかを、定期的に又は必要に応じて随時、検証し、見直しているか。

- 具体的な資金繰り逼迫状況と資金繰り逼迫への対応策を念頭に置いた適切な逼迫度区分（例えば、平常時、懸念時、危機時等）となっているか。
- 適時適切な対応策が取れるよう、資金繰りの逼迫度区分の判定基準が可能な限り具体的で認識しやすい基準となっているか。例えば、流動性資産（有効性のある調達手段を含む。）、信用格付業者の格付、保険会社の株価、社債のスプレッドなどの複数の判定基準を設け、資金繰りの逼迫度の状況を適時適切に認識できるものとなっているか。
- 資産・負債両面にわたり幅広い対応策を考慮した、資金繰りの逼迫度に応じた実効性ある管理手法、報告方法、決裁方法等となっているか。

（ⅴ）流動性危機時の対応策（コンティンジェンシー・プラン）の見直し

流動性リスク管理部門は、資金繰り管理部門や営業推進部門等に想定訓練等を行わせることにより、流動性危機時の対応策（コンティンジェンシー・プラン）の実効性を定期的に確認しているか。情勢の変化等により当該対応策の見直しの必要性が認められる場合には、遅滞なく、取締役会等（重要な見直しの場合は、取締役会）の承認を受けて、当該対応策を見直しているか。

⑶　資金繰り管理部門の役割・責任

①【適切な資金繰り運営・管理】

資金繰り管理部門は、流動性リスク管理方針、流動性リスク管理規程等に基づき、当該保険会社のリスク・プロファイル等の内部環境、経済や市場等の外部環境等の情報を収集・分析し、適切な資金繰り運営を行っているか。なお、この運営に当たっては、資産・負債の両面から流動性についての評価を行うとともに、保険金等に対する支払準備が可能となる時点と金額などの流動性の確保状況を把握しているか。

②【資金繰り表の作成】

資金繰り管理部門は、通貨毎の日次の資金繰り表並びに週次、月次及び四半期ベースの資金繰り見通しを作成しているか。

③【資金繰りへの影響の把握】

資金繰り管理部門は、必要に応じて以下の管理等を行うことにより、資金繰りへの影響を早期に把握しているか。

- 保険料と保険金等の集中管理
- 市場性資金の調達管理
- 保有資産の通貨別・商品別・期間別の構成の管理
- 新規契約及び解約見込みの計画と実績の管理
- 契約上の受信枠及び与信枠の残高管理
- キャッシュの管理（ＡＴＭ等を含む。）
- 各国通貨毎の資金繰りの管理
- 各国通貨間の融通も考慮した資金繰りの管理　　等

④【運用予定額の把握】

資金繰り管理部門は、各部門からの報告等を踏まえ、運用予定額（有価証券・貸付等の予定額）、調達可能額（インターバンク市場やオープン市場における調達可能額等）を把握しているか。運用予定額、調達可能額を的確に把握するため、保険引受部門等から必要な報告・情報を適時に受けているか。なお、運用予定額、調達可能額を把握するに当たっては、以下の項目について考慮しているか。

- 保険料収入及び保険金等支出の実績と計画
- 流動性資産
- オフ・バランス取引
- コミットメント・ライン

・　当座貸越契約
・　実態に応じた運用期間の把握（例えば、形式的には短期の運用となっているが、実態は長期の運用となっているものなど）
・　資金繰りの逼迫度（例えば、平常時、懸念時、危機時等）

⑤【流動性危機管理】

資金繰り管理部門は、流動性危機時において、有価証券の処分など資金調達のための資産の流動化が円滑に行えるよう、常時、取引環境を踏まえて適切に対応しているか。

⑥【流動性リスクのコントロール】

（ⅰ）資金繰り管理部門は、流動性リスク管理方針、流動性リスク管理規程等に基づき、流動性リスクをコントロールしているか。

（ⅱ）資金繰り管理部門は、限度枠を設定している場合には、その限度枠を遵守する運営を行っているか。

⑦【流動性危機時の調達手段の確保】

資金繰り管理部門は、国内外において即時売却可能な資産（国債など）の保有残高や調達可能時点・金額を常時把握するとともに、市中金融機関から調達が行えるよう借入枠を設定するなど、危機時を想定した調達手段を確保しているか。

⑧【流動性リスク管理部門への報告】

資金繰り管理部門は、当該保険会社のリスク・プロファイル等の内部環境、経済や市場等の外部環境等の情報を収集及び分析した結果並びに資金繰りの状況及び予測について、流動性リスク管理部門に対し、定期的に又は逼迫度の状況に応じて随時、報告しているか。

⑨【取締役会等への報告】

資金繰り管理部門は、資金繰りの状況及び予測について、代表取締役及び担当取締役に対し、定期的に又は逼迫度の状況に応じて随時、報告しているか。また、取締役会等に対しても定期的に又は必要に応じて随時、報告しているか。さらに、取締役会等は、報告を受けた内容が流動性リスク管理方針を遵守したものであることを検証しているか。

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・リスク等の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。**
- **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．事務リスク管理態勢

⑴　各業務部門及び営業拠点等における事務処理態勢

①【各業務部門の管理者及び営業拠点長の役割】

（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拠点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。

（ⅶ）保険募集管理部門と連携し、保険募集人が禁止行為を行わないよう適切に指導・監督しているか。

②【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）現金事故及び代理店事故（消費・流用）は、発生後直ちに各業務部門の管理者又は営業拠点長へ連絡し、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）特に、保険契約申込書、第一回保険料充当金領収証の取扱いについて、事務規程に従い厳正なチェックを行っているか。

（ⅴ）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、営業拠点長又は役席等の承認を受けた後に処理しているか。

（ⅵ）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拠点長の指示に基づき処理をしているか。

③【自主点検の適切性】

（ⅰ）各業務部門、営業拠点等、保険募集人における事故、不正等の未然防止、顧客への被害拡大を防ぐため、保険募集管理部門及び他のリスク管理部門等と連携のうえ、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、実効性のある自主点検を実施しているか。

（ⅱ）自主点検の結果等について、自主点検の実施者から、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）自主点検の結果を事務の改善に活用しているか。

２．システムリスク管理態勢

⑴　情報セキュリティ管理

①【セキュリティ管理者等の役割・責任】

（ⅰ）セキュリティ管理者の役割・責任

イ．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。

ロ．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。

ハ．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
- コンピュータ稼働環境の整備
- 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

ニ．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。

ホ．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。

（ⅱ）システム管理者の役割・責任

イ．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。

ロ．システム管理者は、各業務部門、営業拠点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。

ハ．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。

（ⅲ）データ管理者の役割・責任

イ．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。

ロ．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。

（ⅳ）ネットワーク管理者の役割・責任

イ．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。

ロ．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。

②【情報資産の保護】

（ⅰ）保険会社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。

③【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。

（ⅳ）募集代理店が使用するシステムについては、廃業後にアクセスを行うことができないよう適正にアクセス権限の廃止を行っているか。

④【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

⑤【インターネットを利用した取引の管理】

（ⅰ）インターネット等の通信手段を利用した非対面の取引を行う場合には、例えば、以下のような取引のリスクに見合った適切な認証方式を導入しているか。[24]

・　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

[24] 不正アクセスによる顧客口座からの不正出金を防止するための措置を講じている場合（例えば、保険金振り込み金融機関口座（出金先口座）の指定・変更手続きにおいて、顧客口座と名義が異なる出金先口座への指定・変更を認めないこととし、更に転送不要郵便により顧客の住所地に口座指定・変更手続きのための書面を送付するなどにより、顧客口座と名義が異なる出金先口座への振込みを防止する措置を講じている場合）は、取引のリスクに見合った対応がなされているものと考えられる。

証　等

（ⅱ）インターネット等の通信手段を利用した非対面の取引を行う場合には、例えば、以下のような業務に応じた不正防止策を講じているか。

・　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保険会社側で検知し、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）顧客からの相談・苦情（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）モラルリスク回避、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）利用者自身が使用状態を確認できる機能を設け、利用者を不正使用から守っているか。

⑵　サイバーセキュリティ管理

①【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。

②【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。

③【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。

⑶　システム企画・開発・運用管理等

①【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。

②【システム企画・開発態勢】

（ⅰ）企画・開発態勢

イ．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。

ロ．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。

ハ．中長期の開発計画を策定しているか。

ニ．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。また、システム開発・運用管理に当たっては、十分な予算や人的資源を配分しているか。

ホ．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。

ヘ．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。

ト．本番システムの変更案件も承認のうえ実施しているか。

チ．保険商品の開発、改定時におけるプログラムミスの発生を防止するために、ユーザー部門及びシステム部門の連携が十分に図られる態勢となっているか。特に、保険料・配当金等の重要な事項に関する計算結果についてのシステムの機能の検証に、ユーザー部門が主体的に関与する態勢となっているか。

（ⅱ）開発管理

イ．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。

ロ．開発プロジェクトごとに責任者を定めているか。また、プロジェクト計画（目的・概要、スケジュール、システム投資額、体制、報告ルール等）を策定し、関係者に周知しているか。

ハ．システムの重要度及び性格を踏まえ取締役会等が進捗状況をチェックしているか。

ニ．システム部門及びユーザー部門が連携して進捗状況を適切に管理しているか。

（ⅲ）内部規程・業務細則等の整備

イ．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。

ロ．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。

ハ．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。

ニ．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。

（ⅳ）テスト等

イ．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。また、テスト計画には、品質管理基準を設定し、テスト結果を検証しているか。

ロ．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。

ハ．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。特に、保険料・配当金等の重要な事項に関するテストには、ユーザー部門が参加し、テスト結果の確認を行っているか。

ニ．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。

（ⅴ）システム移行の決定

イ．システム移行に係る責任者が明確になっているか。

ロ．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。

ハ．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。

（vi）システム移行後の検証

イ．システムの稼働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。

ロ．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。

ハ．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。

ニ．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。

ホ．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。

（vii）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。

③【システム運用態勢】

（ⅰ）職務分担の明確化

イ．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。

ロ．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。

（ⅱ）システムオペレーション管理

イ．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。

ロ．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。

ハ．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。

ニ．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。

ホ．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。

ヘ．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。

（ⅲ）本番データ管理

イ．システム障害等対応や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。

ロ．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。

ハ．本番データへの不正アクセス又は本番データの紛失、破壊、改ざん、漏洩等の脅威に対して、適切な安全対策を講じているか。

（ⅳ）システム障害等の管理

イ．顧客や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。

ロ．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。

ハ．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。

ニ．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。

ホ．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。また、システム障害等の影響の調査や原因の究明を行い、再発防止策を講じているか。

ヘ．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。

ト．システム障害等の内容の定期的な分析（発生推移、発生原因の分類による傾向分析等）を行い、それに応じた対応策を講じることにより、システム障害等の未然防止を図っているか。

チ．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。

④【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。また、必要に応じてシステム監査とシステム以外の監査を連携して行うことが

できる態勢となっているか。

（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。

（ⅲ）内部監査部門の監査の手法及び内容

イ．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。

ロ．システム部門及び独自にシステムを構築している部門におけるリスクの管理状況を把握した上、リスクの種類・程度に応じて、定期的に内部監査を行っているか。

ハ．営業拠点等システム部門以外でのコンピュータ機器（端末機・ＡＴＭ等）や電子媒体等の使用に関する手続について、システムリスクの観点からのチェックを行っているか。

ニ．内部監査を行うに当たっては、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）の確認等、システム稼働内容について裏付けをとっておくことが望ましい。

⑷ 防犯・防災・バックアップ・不正利用防止

①【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。

②【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。

③【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。

④【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。

（v）バックアップデータを使用してデータ修復を行う際の手順が整備されているか。

⑤【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、保険会社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、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、他の金融機関等におけるシステム障害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、外部委託先等と合同で、定期的に実施しているか。

⑸ 外部委託管理[25]

①【外部委託業務の管理】

（i）外部委託業務の計画・実行

システムに係る外部委託業務（二段階以上の委託を含む。）の計画・実行に当たっては、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、外部委託を行う範囲の決定

[25] 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保険会社における重要度等を踏まえた検証が必要である。

及びリスク管理の具体策の策定を行っているか。

（ⅱ）外部委託先の選定

イ．システムリスク管理部門は、外部委託管理責任者と連携し、外部委託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。

・ 受託実績等による信用度や、委託業務の技術レベル・実施体制等、保険会社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。

・ 保険会社のレピュテーション等の観点[26]から問題ないか。

ロ．外部委託した業務（二段階以上の委託を含む。）及び業者について定期的に評価を行っているか。

なお、外部委託した業務について、業務の内容等に応じ、第三者機関の評価を受けていることが望ましい。

（ⅲ）委託契約の内容

イ．システムリスク管理部門は、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。

ロ．委託先と守秘義務契約を締結しているか。

ハ．外部委託先が再委託を行う場合、外部委託先との委託契約書において再委託先に係る契約上の義務や責任等の条項を整備しているか。

ニ．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。

（ⅳ）外部委託先のモニタリング

イ．外部に委託しているシステム及び業務を適切に管理する管理者を設置し、委託契約に基づいて各種ルールの遵守状況や委託業務の遂行状況の管理、検証を行っているか。

ロ．システムリスク管理部門は、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、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。また、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

[26] 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。

整備しているか。

ハ．委託先社員等に付与するシステムやデータへのアクセス権限は、委託業務を遂行するうえで必要最小限の範囲に限定しているか。

（ｖ）外部委託先への監査

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。

（vi）問題点の是正

システムリスク管理部門は、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。

②【システム関係の業務委託先の検証】

（ｉ）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。

（ii）保険会社等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。

（iii）保険会社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保険会社等と合意しているか。

（iv）企画段階、設計・開発段階、テスト段階において、保険会社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。

（ｖ）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。

（vi）システムの運用状況について、保険会社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。

（vii）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。

（viii）複数の保険会社の業務を受託するセンターの場合、他の保険会社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。

⑸　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。

３．流動性リスク管理態勢

⑴　資産運用部門、保険引受部門等の役割・責任

資産運用部門、保険引受部門等は、流動性リスクに影響を与え、かつ報告基準を満たす要因が発生した場合、内部規程・業務細則等に基づいて、速やかに流動性リスク管理部門及び資金繰り管理部門に報告しているか。

⑵　市場流動性リスク管理

①【市場流動性の適切な把握】

流動性リスク管理部門は、市場流動性の状況を正確に把握しているか。

また、必要に応じ、市場流動性の状況を代表取締役及び取締役会等へ報告しているか。

②【限度枠の設定及び見直しの実施】

マーケットの状況により、市場において企図した時点価格での取引や企図した量の取引ができないこともあることを踏まえ、流動性リスク管理部門は、市場流動性の状況を勘案し、適切に取締役会等の承認を得た上で（緊急の場合には担当取締役が決定し、事後的に取締役会等に報告し検証を受ける。）、必要に応じ限度枠を設定しているか。

また、運用商品、市場環境の変化等により定期的に（最低限半年に 1 回）及び状況に応じて随時、限度枠を見直しているか。

③【市場流動性リスクを勘案した運用】

資産運用部門は、商品ごとに市場規模・取引量、流動性を勘案した運用を行っているか。また、一度に多量の商品を売買することは、その商品の売買自体によって市場流動性リスクが生じることがあることを認識し、その影響を勘案した上で運用を行っているか。

④【モニタリングの実施】

流動性リスク管理部門は、商品ごとの日々のポジションの状況を把握するとともに、市場規模の変化、信用状況の変化をモニタリングしているか。

⑤【報告の実施】

流動性リスク管理部門は、把握されたポジションの状況等について、規程に基づき正確に担当取締役（必要に応じ代表取締役及び取締役会）に報告しているか。また、商品の売買自体によって流動性リスクが生じる可能性がある場合、限度枠を超過した場合や、懸念時・危機時の場合には、極力、頻繁に代表取締役又は取締役会に報告を行うとともに、適切な対応策をとっているか。

４．その他オペレーショナル・リスク管理態勢

⑴　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

①【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。）など当該保険会社が法務リスクとして定義したものについて、当該保険会社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、当該保険会社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。

②【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、当該保険会社が、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、当該保険会社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拠点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。

③【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、当該保険会社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、当該保険会社が直面するリスクを認識し、適切な管理を行っているか。

④【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、当該保険会社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、当該保険会社が直面するリスクを認識し、適切な管理を行っているか。なお、他の保険会社や取引先等に関する風評が発生した場合の対応方法についても、検討しておくことが望ましい。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拠点等の対応方法を定めているか。特に、風評が保険契約の解約に結びついた場合の対応について、支社等の営業推進部門等の状況把握、顧客対応、対外説明等、初動対応に関する規程を設けているか。
- 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。
- また、金融庁担当課室、提携先、警備会社等へ、速やかに連絡を行う体制になっているか。

⑵ 危機管理態勢の整備・確立状況

①【平時における対応】

（ⅰ）何が危機であるかを認識し、可能な限りその回避に努める（不可避なものは予防策を講じる）よう、平時より、定期的な点検・訓練を行うなど未然防止に向けた取組みに努めているか。

（ⅱ）危機管理マニュアルを策定しているか。また、危機管理マニュアルは、自らの業務の実態やリスク管理の状況等に応じ、不断の見直しが行われているか。なお、危機管理マニュアルの策定に当たっては、客観的な水準が判定されるものを根拠とし

て設計されていることが望ましい。

【参考】想定される危機の事例

イ．自然災害（地震、風水害、異常気象、伝染病等）

ロ．テロ・戦争（国外において遭遇する場合も含む。）

ハ．事故（大規模停電、コンピュータ事故等）

ニ．風評（口コミ、インターネット、電子メール等）

ホ．対企業犯罪（脅迫、反社会的勢力の介入、データ盗難等）

ヘ．営業上のトラブル（相談・苦情対応、データ入力ミス等）

ト．人事上のトラブル（内紛、セクシャルハラスメント等）

チ．労務上のトラブル（内部告発、過労死、人材流出等）

（ⅲ）危機管理マニュアルには、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。

（ⅳ）危機発生時における責任体制が明確化され、危機発生時の組織内及び関係者（関係当局を含む。）への連絡体制等が整備されているか。危機発生時の体制整備は、危機のレベル・類型に応じて、組織全体を統括する対策本部の下、部門別・支社等の営業拠点別に想定していることが望ましい。

（ⅴ）業務継続計画（ＢＣＰ）においては、大規模な災害・疫病やテロ等の事態においても早期に被害の復旧を図り、保険契約者等の保護上、必要最低限の業務の継続が可能となっているか。その際、必要に応じ、当該保険会社の所属する業界団体（㈳生命保険協会、㈳日本損害保険協会、㈳外国損害保険協会）及び他の保険会社と連携し対応する体制が整備されているか。また、業務の実態等に応じ、国際的な広がりを持つ業務中断に対応する計画となっているか。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。

- 災害等に備えたコンピュータシステム、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。
- これらのバックアップ体制は、地理的集中を避けているか。
- 保険契約に基づく保険金等の適切な支払いなど保険契約者等の保護の観点から重要な業務を、暫定的な手段（バックアップデータに基づく手作業等）で対応する準備が整っているか。
- 業務継続計画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。また、業務継続体制が、内部監査、外部監査など独立した主体による検証を受けているか。

（ⅵ）大規模自然災害等の危機発生時において、保険金支払業務を継続・復旧させていくべき機能と明確に位置付けた上で、日頃から、災害発生時に支払業務の継続・復旧が図られるような態勢が整備されているか。また、保険契約者等に対して、保険

金等の支払等について便宜措置（監督指針「Ⅲ－1－6 災害における金融に関する措置」参照）が図られるような態勢が整備されているか。

（vii）日頃からきめ細かな情報発信及び情報の収集に努めているか。また、危機発生時においては、危機のレベル・類型に応じて、情報発信体制・収集体制が十分なものとなっているか。

②【危機発生時における対応】

危機的状況の発生又はその可能性が認められる場合において、危機対応の状況（危機管理体制の整備状況、関係者への連絡状況、情報発信の状況等）が危機のレベル・類型に応じて十分なものになっているか。

③【事態沈静化後における対応】

危機的状況が沈静化した後、発生原因分析及び再発防止に向けた取組みを行っているか。