システムリスク管理態勢の確認検査用チェックリスト

① 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である。
② 検査官は、「リスク管理態勢の確認検査用チェックリスト（共通編）」及び本チェックリストにより、システムリスクの管理態勢の確認検査を行うものとする。しかしながら、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基準書」及び「同解説書」（財団法人金融情報システムセンター編）に基づき、またコンティンジェンシープランの具体的検証に当たっては、「金融機関等におけるコンティンジェンシープラン要領」及び「金融機関等におけるコンティンジェンシープラン策定のための手引書」（財団法人金融情報システムセンター編）に基づき行うものとする。
③ また、本チェックリストは、邦銀の海外拠点（海外支店、現地法人及び駐在員事務所等。ただし、本チェックリストの対象として検査を行うかどうかは現地法制を踏まえ実態に応じて判断する。）及び外国銀行の在日支店も含め、全ての預金等受入金融機関を対象としている。なお、協同組織金融機関のチェックに当たっては、チェックリスト中「取締役会」とあるのは「理事会」に、「取締役会等」とあるのは、「理事会等」に、「代表取締役」とあるのは「代表理事」に、「取締役」とあるのは「理事」に、「監査役、監査役会」とあるのは「監事」に読み替える（協同組織金融機関にあっては、会計監査人の選任を義務付けられる場合が限定されているので、その点に留意する必要がある。）。

【本チェックリストにより検査を行うに際しての留意事項】
本検査マニュアルはあくまでも検査官が金融機関を検査する際に用いる手引書として位置付けられるものであり、各金融機関においては、自己責任原則の下、このマニュアル等を踏まえ創意・工夫を十分に生かし、それぞれの規模・特性に応じたより詳細なマニュアルを自主的に作成し、金融機関の業務の健全性と適切性の確保に努めることが期待される。
マニュアルの各チェック項目は、検査官が金融機関のリスク管理態勢を評価する際の基準であり、これらの水準の達成を金融機関に直ちに法的に義務付けるものではない。
マニュアルの適用にあたっては、金融機関の規模や特性を十分踏まえ、機械的・画一的な運用に陥らないよう配慮する必要がある。チェック項目に記述されている字義通りの対応が金融機関においてなされていない場合であっても、金融機関の業務の健全性及び適切性確保の観点からみて、金融機関の行っている対応が合理的なものであり、さらにチェック項目に記述されているものと同様の効果がある、あるいは金融機関の規模や特性に応じた十分なものである、と認められるのであれば、不適切とするものではない。
したがって、検査官は、立入検査の際に金融機関と十分な意見交換を行う必要がある。
また、特に、システムリスクの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検査官は十分留意することとする。
・ システムの重要度とは、当該システムの顧客取引また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、コンピューター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を表し、それぞれに適した管理手法がある。

（注）チェック項目についての説明
① チェック項目の語尾が「しているか」または「なっているか」とあるのは、特にことわりのない限り、全ての金融機関に対してミニマム・スタンダードとして求められる項目である。
したがって、検査官は各チェック項目を確認の上、その実効性を十分検証する必要がある項目である。
② チェック項目の語尾が「望ましい」とあるのは、特にことわりのない限り、全ての金融機関に対してベスト・プラクティスとして望まれる項目である。
したがって、検査官は各チェック項目の確認をすれば足りる項目である。
③ なお、両者を組み合わせて、国際統一基準により自己資本比率を算定している金融機関（以下「国際統一基準適用金融機関」という。）にあっては①、国内基準により自己資本比率を算定している金融機関（以下「国内基準適用金融機関」という。）にあっては②としている項目がある。

（注）取締役会及び取締役会等の説明
① 「取締役会」の役割とされている項目については、取締役会自身においてその実質的内容を決定することが求められるがその原案の検討を常務会等で行うことを妨げるものではない。
② 「取締役会等」には、取締役会のほか、常務会、経営会議等を含む。なお、「取締役会等」の役割とされている項目についても、取締役会自身において行われることが望ましいが、常務会等に委任している場合には、取締役会による明確な委任があること、常務会等の議事録の整備等により事後的検証を可能としていることに加え、取締役会に結果を報告する、又は、常務会等に監査役等の参加を認める等により、十分な内部牽制が確保されるような体制となっているかを確認する必要がある。

項　目	リスク管理態勢のチェック項目	リスク管理態勢のチェック項目に係る説明	備　考
Ⅰ．リスク管理に対する認識等 1．取締役の認識及び取締役会等の役割	(1) 金融機関全体の経営方針に沿った戦略目標の明確化	(1) 取締役会は、戦略目標を定めているか。戦略目標には、情報技術革新を踏まえ、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含んでいるか。 システム戦略方針には、①システム開発の優先順位（制度的対応を優先すること・・例：2000年問題、ＥＵの統合、連結決算に対するシステム改革等）、②情報化推進計画、③システムに対する投資計画等を定めているか。	
	(2) リスク管理の方針の確立	(2) 取締役会は、リスク管理の基本方針を定めているか。リスク管理の基本方針には、セキュリティーポリシー（組織の情報資産を適切に保護するための基本方針）を含んでいるか。 セキュリティーポリシーには、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を定めているか。	
Ⅱ．適切なリスク管理態勢の確立 1．リスクの認識と評価	管理すべきリスクの所在、種類の特定	①　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。 ②　システム部門以外において独自にシステムを構築する場合においても該当システムのリスクを認識・評価しているか。 ③　ネットワークの拡充（インターネット、電子メール）及びＰＣ（パソコン）の普及等によりリスクが多様化・増加していることを認識・評価しているか。	

項　目	リスク管理態勢のチェック項目	リスク管理態勢のチェック項目に係る説明	備　考
2．職責の分離	相互牽制体制の構築	①　国際統一基準適用金融機関にあっては、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。 　また、海外拠点においては、下記②によるものとしてもよい。 ②　国内基準適用金融機関にあっては、上記①により分離分担を行っていることが望ましいが、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。 ③　また、上記①、②に関わらず、ＥＵＣ（エンドユーザーコンピューティング）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。 ④　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。 ⑤　監査結果については、定期的に取締役会等に報告をしているか。	
Ⅲ．監査及び問題点の是正 1．内部監査	(1)　内部監査部門の体制整備	(1)　内部監査部門は、システム関係に精通した要員を確保しているか。	
	(2)　内部監査部門の監査の手法及び内容	(2)①　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。 ②　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対しては、原則として年一回以上の内部監査を行っているか。 ③　営業店等システム部門以外でのコンピュータ機器（端末機・ＡＴＭ等）の使用に関する手続は、システムリスクの観点からのチェックをしているか。 ④　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、システムの稼働内容について裏付けをとっておくことが望ましい。	
	(3)　コンピュータ犯罪・事故	(3)　コンピュータ犯罪（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、カード犯罪等）及びコンピュータ事故（ハードウェア、ソフトウェア、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、十分に留意した体制を整備し、監査及び点検等の事後チェック体制を整備しているか。	
2．外部監査	外部監査の活用	国際基準適用金融機関にあっては、３年に１回以上は、システムリスクについての会計監査人等による外部監査を受けているか。（国内基準適用金融機関にあっても受けていることが望ましい。）	

項　目	リスク管理態勢のチェック項目	リスク管理態勢のチェック項目に係る説明	備　考
Ⅳ．企画・開発体制のあり方 １．企画・開発体制	(1) 企画・開発体制	(1)① 信頼性が高くかつ効率的なシステム導入を図る企画・開発のための規定を整備しているか。 ② 機械化委員会等の横断的な審議機関を設置していることが望ましい。 ③ 中長期の開発計画を策定しているか。 ④ 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。 ⑤ 開発案件の検討・承認ルールが明確になっているか。 ⑥ 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	(2)① 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。 ② 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が進捗状況をチェックしているか。	
	(3) 規定・マニュアルの整備	(3)① 設計、開発、運用に関する規定・マニュアルが存在しているか。 ② 業務実態に即した見直しを実施しているか。 ③ 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ことが望ましい。 ④ 開発に当たっては、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）を残すようなシステムとすることが望ましい。 ⑤ 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	(4)① テストは適切かつ十分に行われているか。 ② 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体制を整備しているか。 ③ テスト計画を作成しているか。 ④ 総合テストには、ユーザー部署も参加していることが望ましい。 ⑤ 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) 人材の養成	(5)① 人材の養成に当たっては、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。 ② デリバティブ業務・電子決済等、専門性の高い業務分野や新技術について、精通した開発要員を養成していることが望ましい。	

項　目	リスク管理態勢のチェック項目	リスク管理態勢のチェック項目に係る説明	備　考
	⑹　委託先管理	⑹①　システムの開発を外部ベンダー等に委託する際には、守秘義務契約を締結しているか。 ②　派遣要員が接することができるデータには、必要に応じて一定の制限を設けているか。 ③　委託業務の実施状況を管理簿等により把握しているか。	
2．新規分野への進出	新規分野への進出	新規分野・新技術について、情報収集・研究等が行われ、経営戦略上の位置付けについて検討していることが望ましい。	
Ⅴ．体制の整備 1．管理体制	⑴　セキュリティ管理体制	⑴①　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ているか。 （注）セキュリティは、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・点検体制等 ロ．ロジカルセキュリティ ・開発・運用の各組織間・組織内の相互牽制体制 ・開発管理体制 ・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 ②　セキュリティ管理者は、システム、データ、ネットワーク管理体制を統括しているか。	
	⑵　システム管理体制	⑵①　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ているか。 ②　システム管理者は、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。 ③　それぞれシステムの資産調査は１年に１度以上行い、適正なスクラップアンドビルドを行っているか。 ④　本部・営業店・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に管理する体制を整備しているか。 ⑤　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体制を整備しているか。 ⑥　システム部門以外で独自にシステムを構築しているシステムについても、システム管理者を定めているか。	

項　目	リスク管理態勢のチェック項目	リスク管理態勢のチェック項目に係る説明	備　考
	(3) データ管理体制	(3)① 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ているか。 ② データの管理手順及び利用承認手続等を規定・マニュアルとして定め、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。 ③ データ保護、データ不正使用防止、不正プログラム防止策について適切かつ十分な管理体制を整備しているか。	
	(4) ネットワーク管理体制	(4)① 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ているか。 ② ネットワークの管理手順及び利用承認手続等を規定・マニュアルとして定め、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。 ③ 国際統一基準適用金融機関にあっては、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。（国内基準適用金融機関にあっても、考慮していることが望ましい。）	

項　目	リスク管理態勢のチェック項目	リスク管理態勢のチェック項目に係る説明	備　考
2．システム運用体制	(1) 職務分担の明確化	(1)① データ受付、オペレーション、作業結果確認、データプログラム保管の職務分担は明確になっているか。 ② 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	(2)① 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。 ② 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。 ③ オペレーションは、全て記録され、かつ管理者は、チェック項目を定め点検しているか。 ④ 重要なオペレーションは、複数名による実施が可能となることが望ましく、また、可能な限り自動化することが望ましい。 ⑤ オペレーションの処理結果を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。 ⑥ 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) トラブル管理	(3)① トラブル発生時には、記録簿等に記入し、必要に応じ本部に報告が行われる体制を整備しているか。 ② トラブル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。 ③ 経営に重大な影響を与えるような重要なトラブルの場合には、速やかに本部と連携し、問題の解決を図るとともに取締役会に報告しているか。	
	(4) 委託先管理	(4)① システムの運用を外部ベンダー等に委託する際には、守秘義務契約を締結しているか。 ② 派遣要員が接することができるデータには、必要に応じて一定の制限を設けているか。 ③ 委託業務の実施状況を管理簿等により把握しているか。	

項　目	リスク管理態勢のチェック項目	リスク管理態勢のチェック項目に係る説明	備　考
	⑸　顧客等のデータ保護	⑸①　法的に許される及び顧客自身の同意がある場合を除き、原則として顧客データを第三者に開示することを禁止しているか。顧客データの取扱については、管理責任者、管理方法及び取扱方法を定め、適切に管理しているか。 ②　顧客データへの不正なアクセス又は顧客データの紛失、破壊、改ざん、漏洩等の危険に対して、適切な安全措置を講じているか。	
	⑹　不正使用防止	⑹①　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体制を整備しているか。 ②　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。	
	⑺　コンピュータウィルス等	⑺　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・除去する体制を整備しているか。 ・コンピュータウィルスへの感染 ・正規の手続を経てい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	

項　目	リスク管理態勢のチェック項目	リスク管理態勢のチェック項目に係る説明	備　考
Ⅵ. 防犯・防災・バックアップ・不正利用防止	(1) 防犯対策	(1)① 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。 ② 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) 防災対策	(2)① 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。 ② 防災組織、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。 ③ 防火・地震・出水に対する対策を確保しているか。 ④ 重要データ等の避難場所をあらかじめ確保しているか。	
	(3) 不正利用防止策	(3) 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。	
	(4) バックアップ	(4)① 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。 ② 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。 ③ 国際統一基準適用金融機関にあっては、営業店オンラインシステム等、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を保有しているか。（国内基準適用金融機関にあっても、保有することが望ましい。） ④ バックアップ取得の周期を文書化しているか。	
	(5) コンティンジェンシープランの策定	(5)① 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。 ② 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。） ③ コンティンジェンシープランの整備に当たっては、「金融機関等におけるコンティンジェンシープラン要領」及び「金融機関等におけるコンティンジェンシープラン策定のための手引書」（財団法人金融情報システムセンター編）に準拠しているか。 ④ コンティンジェンシープランの整備に当たっては、災害による緊急事態を想定するだけではなく、金融機関の内部に起因するものや金融機関の外部に起因によるものも想定しているか。 ⑤ コンティンジェンシープランの整備に当たっては、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。	