別紙 3

中小・地域金融機関向けの総合的な監督指針（本編）　新旧対照表

現　　行	改　正　後
Ⅱ－３－４ システムリスク	Ⅱ－３－４ システムリスク
Ⅱ－３－４－１ システムリスク	Ⅱ－３－４－１ システムリスク
Ⅱ－３－４－１－１ 意義	Ⅱ－３－４－１－１ 意義
（略）	（略）
Ⅱ－３－４－１－２ 主な着眼点	Ⅱ－３－４－１－２ 主な着眼点
（１）システムリスクに対する認識等	（１）システムリスクに対する認識等
システムリスクについて経営者をはじめ、役職員がその重要性を十分認識し、定期的なレビューを行うとともに、全行的なリスク管理の基本方針が策定されているか。	①　システムリスクについて代表取締役をはじめ、役職員がその重要性を十分認識し、定期的なレビューを行うとともに、全行的なリスク管理の基本方針が策定されているか。
（新設）	②　代表取締役は、システム障害の未然防止と発生時の迅速な復旧対応について、経営上の重大な課題と認識し、態勢を整備しているか。
（新設）	③　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役員を定めているか。なお、システム統括役員は、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。
（新設）	④　代表取締役及び取締役（委員会設置会社にあっては執行役）は、システム障害発生等の危機時において、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

現　　行	改　正　後
	か。
（２）システムリスク管理態勢 　取締役会は、コンピュータシステムのネットワーク化の進展等により、リスクが顕在化した場合、その影響が連鎖し、広域化・深刻化する傾向にあるなど、経営に重大な影響を与える可能性があるということを十分踏まえ、リスク管理態勢を整備しているか。 　システムリスク管理の基本方針が定められているか。システムリスク管理の基本方針には、セキュリティポリシー（組織の情報資産を適切に保護するための基本方針）及び外部委託先に関する方針が含まれているか。システムリスク管理体制の整備に当たっては、その内容について客観的な水準が判定できるものを根拠としているか。 　また、システムリスク管理体制は、システム障害等の把握・分析、リスク管理の実施結果や技術進展等に応じて、不断に見直しを実施しているか。	（２）システムリスク管理態勢 　①　取締役会は、コンピュータシステムのネットワーク化の進展等により、リスクが顕在化した場合、その影響が連鎖し、広域化・深刻化する傾向にあるなど、経営に重大な影響を与える可能性があるということを十分踏まえ、リスク管理態勢を整備しているか。 　②　システムリスク管理の基本方針が定められているか。システムリスク管理の基本方針には、セキュリティポリシー（組織の情報資産を適切に保護するための基本方針）及び外部委託先に関する方針が含まれているか。 　③　システムリスク管理体制の整備に当たっては、その内容について客観的な水準が判定できるものを根拠としているか。 　また、システムリスク管理体制は、システム障害等の把握・分析、リスク管理の実施結果や技術進展等に応じて、不断に見直しを実施しているか。
（新設）	（３）システムリスク評価 　①　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。 　また、洗い出したリスクに対し、十分な対応策を講じているか。

現　　行	改　正　後
	②　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・管理し、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。 ③　商品開発の担当部門は、新商品の導入時又は商品内容の変更時に、システムリスク管理部門と連携するとともに、システムリスク管理部門は、システム開発の有無にかかわらず、関連するシステムの評価を実施しているか。
（３）安全対策 （略）	（４）安全対策 （略）
（新設）	（５）システム企画・開発・運用管理 ①　経営戦略の一環としてシステム戦略方針を明確にした上で、中長期の開発計画を策定しているか。 また、中長期の開発計画は、取締役会の承認を受けているか。 ②　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。 ③　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。 ④　開発プロジェクトごとに責任者を定め、開発計画に基づき進捗管理されているか。 ⑤　システム開発に当たっては、テスト計画を作成し、ユーザー部門も参加するなど、適切かつ十分にテストを行っているか。

現　　行	改　正　後
	⑥　人材育成については、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。
（４）システム監査 ①　システム部門から独立した内部監査部門が、定期的にシステム監査を行っているか。 ②　システム監査に精通した要員を確保しているか。 ③　監査対象は、システムリスクに関する業務全体をカバーしているか。 ④　システム監査の結果は、適切に経営者に報告されているか。	（６）システム監査 ①　システム部門から独立した内部監査部門が、定期的にシステム監査を行っているか。 ②　システム関係に精通した要員による内部監査や、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。 ③　監査対象は、システムリスクに関する業務全体をカバーしているか。 ④　システム監査の結果は、適切に取締役会に報告されているか。
（５）外部委託管理 （新設） （新設） システムに係る外部委託業務について、リスク管理が適切に行われているか。 特に外部委託先（システム子会社を含む。）が複数の場合、管理業務が複雑化することから、より高度なリスク管理が求められることを十分認識した体制となっているか。	（７）外部委託管理 ①　外部委託先（システム子会社を含む。）の選定に当たり、選定基準に基づき評価、検討のうえ、選定しているか。 ②　外部委託契約において、外部委託先との役割分担・責任、監査権限、再委託手続き、提供されるサービス水準等を定めているか。 ③　システムに係る外部委託業務について、リスク管理が適切に行われているか。 特に外部委託先が複数の場合、管理業務が複雑化することから、より高度なリスク管理が求められることを十分認識した体制となっているか。

現　　行	改　正　後
システム関連事務を外部委託する場合についても、システムに係る外部委託に準じて、適切なリスク管理を行っているか。	システム関連事務を外部委託する場合についても、システムに係る外部委託に準じて、適切なリスク管理を行っているか。
（新設）	④　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しているか。 また、外部委託先任せにならないように、例えば委託元として要員を配置するなどの必要な措置を講じているか。特に共同センターの内部管理、開発・運用管理の状況について、報告を受けているか。 さらに、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運用状況を、委託元が監視、追跡できる態勢となっているか。
（新設）	⑤　共同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。
（注）統合ＡＴＭスイッチングサービスなどの外部のサービスを利用する場合についてもこれに準じる。	（注）統合ＡＴＭスイッチングサービスなどの外部のサービスを利用する場合についてもこれに準じる。
（６）データ管理態勢	（８）データ管理態勢
（略）	（略）
（７）コンティンジェンシープラン	（９）コンティンジェンシープラン
①　コンティンジェンシープランが策定され、緊急時体制が構築されているか。	①　コンティンジェンシープランが策定され、緊急時体制が構築されているか。
②　コンティンジェンシープランの策定に当たっては、その内容につ	②　コンティンジェンシープランの策定に当たっては、その内容につ

現　　行	改　正　後
いて客観的な水準が判断しうるものを根拠としているか。	いて客観的な水準が判断できるもの（例えば「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））を根拠としているか。
（新設）	③　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。
（新設）	④　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。
（新設）	⑤　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、共同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。
（新設）	⑥　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。
（８）障害発生時の対応 ①　顧客に対し無用の混乱を生じさせないよう、適切な措置を講じているか。	（10）障害発生時の対応 ①　システム障害が発生した場合に、顧客に対し無用の混乱を生じさせないよう、適切な措置を講じているか。 　また、システム障害の発生に備え、最悪のシナリオを想定した上

現　　行	改　正　後
	で、必要な対応を行う態勢となっているか。
（新設）	②　システム障害の発生に備え、外部委託先を含めた報告態勢、指揮・命令系統が明確になっているか。
（新設）	③　経営に重大な影響を及ぼすシステム障害が発生した場合に、速やかに代表取締役をはじめとする取締役に報告するとともに、報告に当たっては、最悪のシナリオの下で生じうる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。 　また、必要に応じて、対策本部を立ち上げ、代表取締役等自らが適切な指示・命令を行い、速やかに問題の解決を図る態勢となっているか。
（新設）	④　システム障害の発生に備え、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。
②　障害が発生した場合、障害の内容・発生原因、復旧見込等について公表するとともに、顧客からの問い合わせに的確に対応するため、必要に応じ、コールセンターの開設等を迅速に行っているか。	⑤　システム障害が発生した場合、障害の内容・発生原因、復旧見込等について公表するとともに、顧客からの問い合わせに的確に対応するため、必要に応じ、コールセンターの開設等を迅速に行っているか。 　また、システム障害の発生に備え、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、障害の発生原因の究明、復旧までの影響調査、改善措置、再発防止策等を的確に講じているか。	⑥　システム障害の発生原因の究明、復旧までの影響調査、改善措置、再発防止策等を的確に講じているか。

現　　行	改　正　後
（新設）	また、システム障害の原因等の定期的な傾向分析を行い、それに応じた対応策をとっているか。 ⑦　システム障害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。
（注）着眼点の詳細については、必要に応じ金融検査マニュアルを参照。 （参考）システムリスクについての参考資料として、例えば「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」（金融情報システムセンター）などがある。	（注）着眼点の詳細については、必要に応じ金融検査マニュアルを参照。 （参考）システムリスクについての参考資料として、例えば「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）などがある。