

コメントの概要及びコメントに対する金融庁の考え方

(システムリスクの総点検の結果を踏まえた監督指針及び検査マニュアルの改正)

No.	項目	コメントの概要	金融庁の考え方
1	<p>「主要行等向けの総合的な監督指針」 Ⅲ-3-7-1-2 (1)</p> <p>「中小・地域金融機関向けの総合的な監督指針」 Ⅲ-3-4-1-2 (1)</p> <p>「金融検査マニュアル」 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 (別紙2) I-1 ①</p>	<p>システムリスクの総点検に基づき、経営者がシステムリスクを把握管理する必要性について賛同するが、総点検の対象となるシステムがシステム部門が関与するいわゆるホストシステムに限定されていることが懸念される。</p> <p>近年の取扱商品拡大に伴い、担当者がPC上でエクセルやアクセスを駆使して簡易なシステムを作成し、新商品取扱いに対応するケースが増えていると認識しているが、この様なケースではシステム部門の目が届かず、結果的にシステムリスクが放置される危険性が高い。</p> <p>当然、銀行が本業とする決済業務や貸出し業務と比べて優先度は下がるものの、この様な簡易なシステムが銀行には多数存在し、システムリスクを抱えながら運用されていることを経営者に認識いただくよう注意喚起することも必要と考える。</p>	<p>金融庁としては、EUC（エンドユーザーコンピューティング）等ユーザー部門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、金融機関の規模・特性に応じて、適切なシステムリスク管理態勢を整備することが必要であると考えています。</p> <p>このため、金融検査マニュアルにおいても、EUC等にシステム管理者を設置することや、システムリスク管理部門がEUC等のリスクを認識・評価することなどを明記しているところです。</p>
2	<p>「主要行等向けの総合的な監督指針」 Ⅲ-3-7-1-2 (1) ③</p> <p>「中小・地域金融機関向けの総合的な監督指針」 Ⅲ-3-4-1-2 (1) ③</p> <p>「金融検査マニュアル」 オペレーショナル・リスク管理態勢の確認検査用</p>	<p>本項には、「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、システムに精通していることが望ましい。」とある。</p> <p>システムに精通していない者がシステムを統括管理することは、著しく困難であると考えますが、取締役会が、システムに精通していない者をシステム統括役員にして、実際の統括管理を部下に頼ることにより、システム統括役員が名目だけのものになってしまうおそれがある。</p>	<p>システム統括役員は、経営陣として、システムに関する十分な知識・経験を有し、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、迅速かつ的確な指示を出せることが必要であり、特に、主要行等においては、顧客に及ぼす影響等を考慮すると、その点が極めて重要であると考えています。</p> <p>したがって、いただいたご意見を踏まえ、「主要行等向けの総合的な監督指針」について、次のとおり修正いたします。 「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</p>

No.	項目	コメントの概要	金融庁の考え方
	チェックリスト（別紙2） I-1 ①（ii）	したがって、小規模な金融機関はともかく、主要行等においては、上記文言を「また、システム統括役員は、システムに精通している者を選任しているか。」とするべきと考える。	で、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を、システムを統括管理する役員として定めているか。
3	「主要行等向けの総合的な監督指針」 III-3-7-1-2（1）③ 「中小・地域金融機関向けの総合的な監督指針」 III-3-4-1-2（1）③ 「金融検査マニュアル」 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（別紙2） I-1 ①（ii） 「主要行等向けの総合的な監督指針」 III-3-7-1-2（3）① 「中小・地域金融機関向けの総合的な監督指針」 III-3-4-1-2（3）① 「金融検査マニュアル」 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（別紙2） II-2（1）（iii）	本項にて、「システム統括役員は、システムに精通していることが望ましい。」とあるが、その必要はない。 理由は、(1)テクノロジーに詳しいことと、自行システムのあるべき姿を企画・監督する能力は別物で、取締役は後者に長けていればよい、(2)大手でなくても銀行システムは巨大かつ複雑であるため、その全貌を正確に理解している人材はいないからである。特に、システム統括役員が「システムに精通している」と判定する基準は存在しないと考える。 また、システム構築後相当年数が経過し、老朽化した機器や陳腐化したプログラムに依存した業務がある場合は、老朽化した機器が突然動かなくなり、代替機の入手が困難になるほか、古いプログラムにはブラックボックス化した部分が多く、障害発生時に原因の特定が困難になる。更新されないシステムは日々停止するリスクが高まっていくので、定期的なリスクを再評価するサイクルを銀行に義務付け、健全度を評価するべきと考える。	経営陣の一員であるシステム統括役員が、システムに精通していない場合には、システム障害の未然防止に向けた有効な対策が取れないおそれがあるほか、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、迅速かつ確かな指示を出せないおそれもあることから、実効性のあるリスク管理態勢を整備・確立するためには、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と考えています。 以上の点を踏まえ、趣旨をより明確化する観点から、「中小・地域金融機関向けの総合的な監督指針」について、次のとおり修正いたします（「金融検査マニュアル」についても、同趣旨の修正）。 「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。」 また、システム構築後、相当期間が経過している場合には、仮に当該システムが長期間安定的に稼働していても、機器の老朽化やプログラムの陳腐化等により、システムが停止する等のリスクが高まっていると考えています。 したがって、今回の改正案においても、外部環境の変化を踏まえ、定期的に又は適時にリスクを認識・評価することや、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

No.	項目	コメントの概要	金融庁の考え方
			<p>持・改善のための投資を計画的に行うことなどを求めているところです。</p>
4	<p>「主要行等向けの総合的な監督指針」 Ⅲ-3-7-1-2 (3) ② 「中小・地域金融機関向けの総合的な監督指針」 Ⅲ-3-4-1-2 (3) ② 「金融検査マニュアル」 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（別紙2） Ⅱ-2 (1) (iv)</p>	<p>「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」とあるが、必ずしもソースコード上の『制限値』といったものに限定されるものではなく、業務におけるシステムの処理能力の評価という観点からの管理を行っていくということが趣旨であると考えられ、処理能力の評価方法などは各行の業務・顧客特性などに応じたものを行うことでよいか。</p>	<p>「システムの制限値」については、ソースコード上の「制限値」に限定されるものではなく、例えば、ユーザー側で設定した「制限値」なども含め、現にシステム障害を発生させるおそれのある「制限値」を意味しています。</p> <p>いずれにせよ、金融機関においては、システム障害が顧客や経営に重大な影響を及ぼすこと等を十分に認識し、金融機関の業務・システムの特성에応じて、どのような制限値があるのかを事前に把握し、管理することが重要であると考えています。</p>
5	<p>「金融検査マニュアル」 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（別紙2） Ⅲ-4 (1) ①</p>	<p>「レピュテーション等の観点」は、当該業務に関し責任を全うできるであろう合理的に考えられる企業規模・専門家の有無・管理態勢の整備状況、最近の行政処分や敗訴判決の有無、その内容と深刻度、反社会的勢力との関係の有無といった客観的な内容に書き換えて頂きたい。</p>	<p>外部委託先の選定に当たっては、各金融機関において、「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ること」が必要です。</p> <p>いただいたご意見を踏まえ、次のとおり「レピュテーション等の観点」に関する脚注を追加いたします。</p> <p>「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。」</p>
6	<p>「主要行等向けの総合的な監督指針」 Ⅲ-3-7-1-2 (7) ② 「中小・地域金融機関向けの総合的な監督</p>	<p>外部委託管理に記載されている「提供されるサービス水準」の水準は、どのように解釈すれば良いか。サービスの内容と理解してよいのか。</p>	<p>「提供されるサービス水準」とは、一般的にSLA (Service Level Agreement) と呼ばれ、外部委託業務の達成レベルを計測するためのベンチマークです。</p> <p>この中には、外部委託先が提供するサービスの内容だけでなく、サービスの品質等に対する金融機関側の要求水準等も</p>

No.	項目	コメントの概要	金融庁の考え方
	指針」 Ⅲ-3-4-1-2 (7) ② 「金融検査マニュアル」 ホレシヨナル・リスク管理 態勢の確認検査用 チェックリスト (別紙2) Ⅲ-4 (1) ②		含んでいます。
7	「主要行等向けの 総合的な監督指針」 Ⅲ-3-7-1-2 (7) ④ 「中小・地域金融機関 向けの総合的な監督 指針」 Ⅲ-3-4-1-2 (7) ④ 「金融検査マニュアル」 ホレシヨナル・リスク管理 態勢の確認検査用 チェックリスト (別紙2) Ⅲ-4 (1) ③	<p>「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、追跡できる態勢を整備しているか。」とあるが、この場合の「監視、追跡できる態勢」とは、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)の「運90」の2.(1)(委託先の管理状況の把握)および(2)(委託先の業務の点検または監査の実施)で具体的事例として挙げている態勢を整備することが考えられる。こうした理解でよいか。</p> <p>この理解でないとすれば、各金融機関がその規模や特性、外部委託の形態に応じた管理態勢の整備を効果的に行うため、具体的な態勢整備の事例を提示いただきたい。</p>	<p>「監視、追跡できる態勢」とは、ご指摘の「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」に記載されている具体的事例のほか、外部委託先における</p> <ul style="list-style-type: none"> ・顧客データの所在の特定状況 ・顧客データの使用状況 ・顧客データの不正使用の監視態勢 ・情報漏えい等が発生した場合の追跡態勢 <p>等を、委託元である金融機関が検証できる態勢のことを想定しています。</p> <p>なお、検証の方法としては、定期的に報告を受けるほか、直接モニタリングする方法などが考えられます。</p>
8	「金融検査マニュアル」 ホレシヨナル・リスク管理 態勢の確認検査用 チェックリスト (別紙2) Ⅲ-4 (1) ③	<p>外部委託先のモニタリングについて、「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要員を配置する」こととあるが、委託先管理の手法等に関するひとつの例として示されたものとの理解で差し支えないか。</p> <p>また、監督指針と平仄を合わせ、「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」としてはどうか。</p>	<p>ご意見のとおり、委託元として要員を配置することは、外部委託先任せにならないようにするための必要な措置の一例として記載しています。</p> <p>いただいたご意見を踏まえ、次のとおり修正いたします。「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。」</p>

No.	項目	コメントの概要	金融庁の考え方
9	<p>「主要行等向けの総合的な監督指針」 Ⅲ-3-7-1-2 (7) ④</p> <p>「中小・地域金融機関向けの総合的な監督指針」 Ⅲ-3-4-1-2 (7) ④</p> <p>「金融検査マニュアル」 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（別紙2） Ⅲ-4 (1) ③</p>	<p>多数の金融機関からの委託を受ける受託者としては、委託を行う各金融機関がそれぞれモニタリングを行う人員を配置されたりすると、その人数が一定数を上回る場合、または一定レベルの専門知識等において不適切な人員が受託者に派遣された場合等、正常な業務の遂行に重大な支障をきたすおそれも生ずる。</p> <p>また、具体的なモニタリング方策について大規模な受託業者が対応可能な合理的モニタリング内容について、主要なIT業者や学識経験者等を交えて議論のうえ、具体的な方策を示して頂きたい。なお、その際にはいわゆるパブリッククラウド等、国外のデータセンター等を利用している場合に、実際に物理的に現地に行かなくても良い監査方法を一定の条件下で承認いただく等、国際的な現実も考慮頂きたい。</p>	<p>外部委託については、委託元が委託先任せにならないように、委託業務が適切に行われることを定期的にモニタリングすることが重要ですが、外部委託の形態や委託される業務内容は多様であり、「要員を配置」することを一律に求めるものではありません。</p> <p>例えば、共同センターについては、加盟金融機関の代表である金融機関が、外部委託先に対して、システム上の適切に対応がなされていることを確認し、加盟金融機関に報告する方法等が考えられます。</p> <p>なお、国外のデータセンター等を利用している場合には、データの所在の特定やデータのトレーサビリティの確保等を実地で確認するなど、実効性のあるモニタリングが必要であると考えています。</p>
10	<p>「主要行等向けの総合的な監督指針」 Ⅲ-3-7-1-2 (7) ⑤</p> <p>「中小・地域金融機関向けの総合的な監督指針」 Ⅲ-3-4-1-2 (7) ⑤</p> <p>「金融検査マニュアル」 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（別紙2） Ⅲ-4 (1) ④</p>	<p>「重要な外部委託先」の具体的な基準を示して頂きたい。</p> <p>また、数多くの金融機関から外部委託を受ける可能性のある受託機関については、それぞれの委託金融機関から内部監査やシステム監査を受け入れると通常の業務の実施が著しく阻害される可能性のある事を配慮し、各受託者が中立の第三者によるIT監査を受け、委託金融機関はこれらの監査結果を確認することで、各金融機関独自の監査に代用する等の代替策も認めて頂きたい。</p>	<p>「重要な外部委託先」については、委託業務の内容や、取り扱っている情報の質、置かれている外部環境等、様々な要素を総合的に勘案して判断することが必要であり、その基準を一律にお示しするのは困難であると考えています。</p> <p>また、外部委託先に対する監査については、金融機関の内部監査部門による監査のほか、第三者であるシステム監査人による監査も考えられますが、いずれにせよ、委託元による主導的なシステム監査が実施される必要があると考えています。</p>

No.	項目	コメントの概要	金融庁の考え方
11	「金融検査マニュアル」 その他	<p>膨大な時間と税金を投入して検査を細かく行っても、主要行のひとつで発生したシステム障害は防止できない。無駄なところに時間と税金をより多くかける方向の改正は、行うべきではない。</p> <p>もっとポイントを絞り、金融機関側の検査対応負担も減らす方向で検討すべきである。</p>	<p>金融庁としては、主要行のひとつで発生したシステム障害への対応で得た教訓を他の金融機関においても活かし、重大なシステム障害を未然に防止するとともに、迅速かつ確な復旧対応ができるようにするために、今回の改正を行うこととしています。</p> <p>今回の改正を踏まえ、重大なシステム障害が起こらないよう、適切な検査・監督に取り組んでまいります。</p>

(検査・監督上の配慮について明確化した監督指針及び検査マニュアルの改正)

No.	項目	コメントの概要	金融庁の考え方
1	<p>「主要行等向けの総合的な監督指針」 I-2-2 (4)、 VIII-2-2</p> <p>「中小・地域金融機関向けの総合的な監督指針」 I-2-2 (4)、 IV-2-2</p> <p>「保険会社向けの総合的な監督指針」 I-1-2 (4)</p>	<p>今回の改正案では、小規模な営業店について、その対応能力を踏まえ、業務の円滑な遂行に支障が生じないよう監督上の配慮を行うこととしている。銀行法等では、小規模な営業所（銀行代理業者）については、(1) 人的構成等に照らして、銀行代理業を的確、公正かつ効率的に遂行するために必要な能力を有すること、(2) 他に業務を営むことによりその銀行代理業を適正かつ確実に営むことにつき支障を及ぼすおそれがあると認められない者であること、等を求めているところ。監督上の配慮をしなければならない者が業務を営むことは、預金者・利用者保護の観点から問題があるのではないか。</p>	<p>御指摘の銀行代理業者の許可の基準については、小規模な営業店において銀行代理業を営む場合においても適合することが求められています。</p> <p>今般の改正は、当該基準に適合しない者のために行うものではなく、当該基準に適合している銀行代理業者の小規模な営業店について、検査・監督上、その対応能力等を踏まえ、業務の円滑な遂行に支障が生じないよう配慮することを明確化したものです。</p>
2	<p>「金融商品取引業者等向けの総合的な監督指針」 I-1-2 (4)</p> <p>「金融検査マニュアル」</p>	<p>今回の改正案では、小規模な営業店について、その対応能力を踏まえ、業務の円滑な遂行に支障が生じないよう検査・監督上の配慮を行うことについて明確化されたが、実際に、今回の改正の考え方を踏まえた検査・監督が行われることを期待する。</p>	<p>金融庁では、従来から金融機関の規模・特性に応じた検査・監督を行ってきており、「小規模な営業店」については、その対応能力等を踏まえ、業務の円滑な遂行に支障が生じないよう配慮してきたところです。</p> <p>今後とも、検査・監督を行うに当たり、引き続き、業務の円滑な遂行に支障が生じないよう配慮していく考えです。</p>
3	<p>【本マニュアルにより検査を行うに際しての留意事項】(2)</p> <p>「保険検査マニュアル」</p> <p>【本マニュアルにより検査を行うに際しての留意事項】(2)</p>	<p>金融検査マニュアルに、検査官は指針およびマニュアルで定められた範囲について厳格に検査することとし、個人的興味からの技術的な質問をすることで、検査対応時間を無駄に延ばすことのないよう十分に留意する旨を追記すべき。</p>	<p>金融検査に関する基本指針には、「オンサイトの検証は、金融機関に大きな負担等をもたらすおそれがある。(略) 立入検査は、(略) 現場において確認すべき必要性が高い事項に焦点を絞り、行う必要がある」と記載されており、金融庁では、検査モニター等により、本指針の適切な運用を確保することとしています。</p> <p>こうした取組を通じて、引き続き、適切な検査の実施に努めてまいります。</p>