

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p><b>【本編】</b></p> <p>Ⅲ. 監督上の評価項目と諸手続（清算機関）</p> <p>Ⅲ－３ 業務の適切性</p> <p>Ⅲ－３－４ システムリスク管理</p> <p>（１）意義</p> <p>システムリスクとは、一般に、コンピュータシステムのダウン又は誤作動等の、システムの不備等に伴い、清算機関等が損失を被るリスクや、コンピュータが不正に使用されることにより清算機関等が損失を被るリスクをいう。</p> <p>清算機関のシステムは、清算等のために不可欠な市場の基盤そのものであり、仮にシステム障害が発生した場合には、清算機関及びシステムに接続する参加者等に損害が生じ、ひいては、金融システム全体に影響を及ぼすこととなりかねない。</p> <p>このため、清算機関における堅牢なシステムリスク管理態勢の構築が重要である。</p> <p><u>（新設）</u></p> <p>（２）主な着眼点</p> <p>① システムリスクに対する認識等</p> <p>ア. （略）</p> <p><u>（新設）</u></p> <p>イ. システムリスクに関する情報が、適切に経営陣に報告される体制となっているか。</p>	<p><b>【本編】</b></p> <p>Ⅲ. 監督上の評価項目と諸手続（清算機関）</p> <p>Ⅲ－３ 業務の適切性</p> <p>Ⅲ－３－４ システムリスク管理</p> <p>（１）意義</p> <p>システムリスクとは、一般に、コンピュータシステムのダウン又は誤作動等の、システムの不備等に伴い、清算機関等が損失を被るリスクや、コンピュータが不正に使用されることにより清算機関等が損失を被るリスクをいう。</p> <p>清算機関のシステムは、清算等のために不可欠な市場の基盤そのものであり、仮にシステム障害やサイバーセキュリティ事案が発生した場合には、清算機関及びシステムに接続する参加者等に損害が生じ、ひいては、金融システム全体に影響を及ぼすこととなりかねない。</p> <p>このため、清算機関における堅牢なシステムリスク管理態勢の構築が重要である。</p> <p><u>（注）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。</u></p> <p>（２）主な着眼点</p> <p>① システムリスクに対する認識等</p> <p>ア. （略）</p> <p><u>イ. 取締役会は、システム障害やサイバーセキュリティ事案（以下「システム障害等」という。）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。</u></p> <p><u>ウ. システムリスクに関する情報が、適切に経営陣に報告される体制となっているか。</u></p>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>② （略）  <u>（新設）</u></p> <p><u>（新設）</u></p>	<p>② （略）</p> <p>③ システムリスク評価  <u>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。</u>  <u>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。</u></p> <p>④ 情報セキュリティ管理  <u>ア. 情報資産を適切に管理するために方針の策定、組織体制の整備、社内規則等の策定、内部管理態勢の整備を図っているか。また、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のPDCAサイクルによる継続的な改善を図っているか。</u>  <u>イ. 情報の機密性、完全性、可用性を維持するために、情報セキュリティに係る管理者を定め、その役割・責任を明確にした上で、管理しているか。また、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。</u>  <u>ウ. コンピュータシステムの不正使用防止対策、不正アクセス防止対策、コンピュータウィルス等の不正プログラムの侵入防止対策等を実施しているか。</u>  <u>エ. 清算機関が責任を負うべき参加者の重要情報を網羅的に洗い出し、把握、管理しているか。</u>  <u>参加者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。</u>  <u>・ 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</u>  <u>・ 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 等</u>  <u>オ. 洗い出した参加者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。</u>  <u>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。</u>  <u>・ 情報の暗号化、マスキングのルール</u>  <u>・ 情報を利用する際の利用ルール</u>  <u>・ 記録媒体等の取扱いルール 等</u></p>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>(新設)</p>	<p>カ. <u>参加者の重要情報について、以下のような不正アクセス、不正情報取得、情報漏えい等を牽制、防止する仕組みを導入しているか。</u></p> <ul style="list-style-type: none"> <li>・<u>職員の権限に応じて必要な範囲に限定されたアクセス権限の付与</u></li> <li>・<u>アクセス記録の保存、検証</u></li> <li>・<u>開発担当者と運用担当者の分離、管理者と担当者の分離等の相互牽制体制 等</u></li> </ul> <p>キ. <u>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。</u></p> <p>なお、「機密情報」とは、暗証番号、パスワード等、参加者に損失が発生する可能性のある情報をいう。</p> <p>ク. <u>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。</u></p> <p>ケ. <u>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。</u></p> <p>コ. <u>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。</u></p> <p>⑤ <u>サイバーセキュリティ管理</u></p> <p>ア. <u>サイバーセキュリティについて、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。</u></p> <p>イ. <u>サイバーセキュリティについて、組織体制の整備、社内規則等の策定のほか、以下のようなサイバーセキュリティ管理態勢の整備を図っているか。</u></p> <ul style="list-style-type: none"> <li>・<u>サイバー攻撃に対する監視体制</u></li> <li>・<u>サイバー攻撃を受けた際の報告及び広報体制</u></li> <li>・<u>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</u></li> <li>・<u>情報共有機関等を通じた情報収集・共有体制 等</u></li> </ul> <p>ウ. <u>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</u></p>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
	<p><u>いるか。</u></p> <ul style="list-style-type: none"> <li>・ <u>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）</u></li> <li>・ <u>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）</u></li> <li>・ <u>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）</u></li> </ul> <p>エ. <u>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。</u></p> <ul style="list-style-type: none"> <li>・ <u>攻撃元の IP アドレスの特定と遮断</u></li> <li>・ <u>DDoS 攻撃に対して自動的にアクセスを分散させる機能</u></li> <li>・ <u>システムの全部又は一部の一時的停止 等</u></li> </ul> <p>オ. <u>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。</u></p> <p>カ. <u>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。</u></p> <p>キ. <u>インターネット等の通信手段を利用して業務を行う場合には、例えば、以下のような業務のリスクに見合った適切な認証方式を導入しているか。</u></p> <ul style="list-style-type: none"> <li>・ <u>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</u></li> <li>・ <u>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 等</u></li> </ul> <p>ク. <u>インターネット等の通信手段を利用して業務を行う場合には、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。</u></p> <ul style="list-style-type: none"> <li>・ <u>参加者のパソコンのウィルス感染状況を清算機関側で検知し、警告を発するソフトの導入</u></li> <li>・ <u>電子証明書を IC カード等、当該業務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</u></li> <li>・ <u>不正なログイン・異常な入力等を検知し、速やかに参加者に連絡する体制の整備 等</u></li> </ul>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>③ システム企画・開発・運用管理 ア. ～カ. (略)</p> <p>④ システム監査 ア. システム部門から独立した内部監査部門において、<u>システムに精通した監査要員による定期的なシステム監査が行われているか。</u> <u>(新設)</u></p> <p>イ. <u>監査の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。</u></p> <p>⑤ 安全対策 ア. <u>安全対策の基本方針が策定されているか。</u> イ. <u>定められた方針、基準及び手順に従って安全対策を適正に管理する安全管理者を設置しているか。安全管理者は、システム、データ、ネットワークの管理体制を統括しているか。</u></p> <p>⑥ 外部委託管理 ア. (略) イ. <u>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、提供されるサービス水準等を定めているか。</u></p> <p>ウ. 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。 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。</p> <p>エ. <u>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。</u></p>	<p><u>ケ. 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。</u></p> <p><u>コ. 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。</u></p> <p>⑥ システム企画・開発・運用管理 ア. ～カ. (略)</p> <p>⑦ システム監査 ア. システム部門から独立した内部監査部門において、定期的なシステム監査が行われているか。 イ. <u>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。</u> ウ. <u>監査の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。</u> <u>(削除)</u></p> <p>⑧ 外部委託管理 ア. (略) イ. <u>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、提供されるサービス水準等を定めているか。また、外部委託先の社員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。</u></p> <p>ウ. <u>システムに係る外部委託業務（二段階以上の委託を含む）について、リスク管理が適切に行われているか。</u> 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。</p> <p>エ. <u>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しているか。</u> また、外部委託先における投資者や参加者のデータの運用状況を</p>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>⑦ データ管理態勢</p> <p>ア. データについて機密性等の確保のため、データ管理者を置いているか。</p> <p>イ. データ保護、データ不正使用防止、不正プログラム防止策等について適切かつ十分な管理態勢を整備しているか。</p> <p>⑧ コンティンジェンシープラン</p> <p>ア. (略)</p> <p>イ. コンティンジェンシープランは、自社の業務の実態やシステム環境等に応じて常時見直され、実効性が維持される態勢となっているか。</p> <p>(新設)</p> <p>(新設)</p> <p>(新設)</p> <p>(新設)</p> <p>⑨ システム更改等のリスク</p> <p>ア. ～オ. (略)</p> <p>⑩ 障害発生時の対応等</p> <p>ア. 投資者や参加者等に無用の混乱を生じさせないための適切な措置を講じるとともに、速やかに復旧や代替手段の稼働に向けた作業を実施することとなっているか。</p>	<p><u>委託元が監視、追跡できる態勢となっているか。</u></p> <p>(削除)</p> <p>⑨ コンティンジェンシープラン</p> <p>ア. (略)</p> <p>イ. <u>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。</u></p> <p>ウ. <u>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なく、清算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。</u></p> <p><u>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。</u></p> <p>エ. <u>コンティンジェンシープランは、他の金融機関及び清算・振替機関等におけるシステム障害等の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。</u></p> <p>オ. <u>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、定期的を実施しているか。</u></p> <p>カ. <u>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に、速やかに業務を継続できる態勢を整備しているか。</u></p> <p>⑩ システム更改等のリスク</p> <p>ア. ～オ. (略)</p> <p>⑪ 障害発生時の対応等</p> <p>ア. <u>システム障害等が発生した場合に、投資者や参加者等に無用の混乱を生じさせないための適切な措置を講じるとともに、速やかに復旧や代替手段の稼働に向けた作業を実施することとなっているか。</u></p> <p><u>また、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</u></p>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>(新設)</p> <p>(新設)</p> <p>イ. 発生した障害について、原因を分析し、それに応じた再発防止策を講じることとしているか。</p> <p>ウ. 障害発生時に速やかに当局に対する報告を行うこととなっているか。</p> <p>(3) (略)</p> <p>(4) システム障害に対する対応</p> <p>① システム障害の発生を認識次第、直ちに、その事実の当局宛て報告を求めるとともに、「障害発生等報告書」(別紙様式1-1)にて当局宛て報告を求めるものとする。</p> <p>また、復旧時、原因説明時には改めてその旨報告を求めることとする(ただし、復旧原因の解明がされていない場合でも1か月以内に現状について報告を求める)。</p> <p>(注) 報告すべきシステム障害</p> <p>その原因の如何を問わず、清算機関又は清算機関から業務の委託を受けた者等が現に使用しているシステム・機器(ハードウェア、ソフトウェア共)に発生した障害であって、取引、決済、入出金、資金繰り、財務状況把握、その他参加者等の利便等に影響があるもの又はそ</p>	<p>で、必要な対応を行う態勢となっているか。</p> <p>イ. システム障害等の発生に備え、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。</p> <p>ウ. 経営に重大な影響を及ぼすシステム障害等が発生した場合に、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、投資者や参加者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。</p> <p>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。</p> <p>エ. 発生したシステム障害等について、原因を分析し、それに応じた再発防止策を講じることとしているか。</p> <p>また、システム障害等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。</p> <p>オ. システム障害等の発生時に速やかに当局に対する報告を行うこととなっているか。</p> <p>(3) (略)</p> <p>(4) システム障害等に対する対応</p> <p>① システム障害等の発生を認識次第、直ちに、その事実の当局宛て報告を求めるとともに、「障害発生等報告書」(別紙様式1-1)にて当局宛て報告を求めるものとする。</p> <p>また、復旧時、原因説明時には改めてその旨報告を求めることとする(ただし、復旧原因の解明がされていない場合でも1か月以内に現状について報告を求める)。</p> <p>(注) 報告すべきシステム障害等</p> <p>その原因の如何を問わず、清算機関又は清算機関から業務の委託を受けた者等が現に使用しているシステム・機器(ハードウェア、ソフトウェア共)に発生した障害であって、取引、決済、入出金、資金繰り、財務状況把握、その他参加者等の利便等に影響があるもの又はそ</p>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>のおそれがあるもの。</p> <p>ただし、一部のシステム・機器にこれらの影響が生じても他のシステム・機器が速やかに代替することで実質的にはこれらの影響が生じない場合を除く。</p> <p>なお、障害が発生していない場合であっても、サイバー攻撃の予告がなされ、又はサイバー攻撃が検知される等により、<u>上記のような障害が発生する可能性が高いと認められる時は、報告を要するものとする。</u></p> <p>② （略）</p>	<p>のおそれがあるもの。</p> <p>ただし、一部のシステム・機器にこれらの影響が生じても他のシステム・機器が速やかに代替することで実質的にはこれらの影響が生じない場合を除く。</p> <p>なお、障害が発生していない場合であっても、サイバー攻撃の予告がなされ、又はサイバー攻撃が検知される等により、<u>参加者や業務に影響を及ぼす、又は及ぼす可能性が高いと認められる時は、報告を要するものとする。</u></p> <p>② （略）</p>



清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>IV. 監督上の評価項目と諸手続（資金清算機関）</p> <p>IV-3 業務の適切性</p> <p>IV-3-4 システムリスク管理</p> <p>(1) 意義</p> <p>システムリスクとは、一般に、コンピュータシステムのダウン又は誤作動等の、システムの不備等に伴い、資金清算機関等が損失を被るリスクや、コンピュータが不正に使用されることにより資金清算機関等が損失を被るリスクをいう。</p> <p>資金清算機関のシステムは、資金清算等のために不可欠な市場の基盤そのものであり、仮にシステム障害が発生した場合には、資金清算機関及びシステムに接続する参加者等に損害が生じ、ひいては、金融システム全体に影響を及ぼすこととなりかねない。</p> <p>このため、資金清算機関における堅牢なシステムリスク管理態勢の構築が重要である。</p> <p><u>(新設)</u></p> <p>(2) 主な着眼点</p> <p>① システムリスクに対する認識等</p> <p>ア. (略)</p> <p><u>(新設)</u></p> <p>イ. システムリスクに関する情報が、適切に経営陣に報告される体制となっているか。</p>	<p>IV. 監督上の評価項目と諸手続（資金清算機関）</p> <p>IV-3 業務の適切性</p> <p>IV-3-4 システムリスク管理</p> <p>(1) 意義</p> <p>システムリスクとは、一般に、コンピュータシステムのダウン又は誤作動等の、システムの不備等に伴い、資金清算機関等が損失を被るリスクや、コンピュータが不正に使用されることにより資金清算機関等が損失を被るリスクをいう。</p> <p>資金清算機関のシステムは、資金清算等のために不可欠な市場の基盤そのものであり、仮にシステム障害やサイバーセキュリティ事案が発生した場合には、資金清算機関及びシステムに接続する参加者等に損害が生じ、ひいては、金融システム全体に影響を及ぼすこととなりかねない。</p> <p>このため、資金清算機関における堅牢なシステムリスク管理態勢の構築が重要である。</p> <p><u>(注) 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。</u></p> <p>(2) 主な着眼点</p> <p>① システムリスクに対する認識等</p> <p>ア. (略)</p> <p>イ. <u>取締役会又は理事会等は、システム障害やサイバーセキュリティ事案（以下「システム障害等」という。）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。</u></p> <p>ウ. システムリスクに関する情報が、適切に経営陣に報告される体制となっているか。</p>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>② （略）  <u>（新設）</u></p> <p><u>（新設）</u></p>	<p>② （略）</p> <p>③ <u>システムリスク評価</u>  <u>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。</u>  <u>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。</u></p> <p>④ <u>情報セキュリティ管理</u>  <u>ア. 情報資産を適切に管理するために方針の策定、組織体制の整備、規則等の策定、内部管理態勢の整備を図っているか。また、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のPDCAサイクルによる継続的な改善を図っているか。</u>  <u>イ. 情報の機密性、完全性、可用性を維持するために、情報セキュリティに係る管理者を定め、その役割・責任を明確にした上で、管理しているか。また、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。</u>  <u>ウ. コンピュータシステムの不正使用防止対策、不正アクセス防止対策、コンピュータウィルス等の不正プログラムの侵入防止対策等を実施しているか。</u>  <u>エ. 資金清算機関が責任を負うべき参加者の重要情報を網羅的に洗い出し、把握、管理しているか。</u>  <u>参加者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。</u>  <u>・ 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</u>  <u>・ 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 等</u>  <u>オ. 洗い出した参加者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。</u>  <u>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。</u>  <u>・ 情報の暗号化、マスキングのルール</u>  <u>・ 情報を利用する際の利用ルール</u>  <u>・ 記録媒体等の取扱いルール 等</u></p>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>(新設)</p>	<p>カ. <u>参加者の重要情報について、以下のような不正アクセス、不正情報取得、情報漏えい等を牽制、防止する仕組みを導入しているか。</u></p> <ul style="list-style-type: none"> <li>・<u>職員の権限に応じて必要な範囲に限定されたアクセス権限の付与</u></li> <li>・<u>アクセス記録の保存、検証</u></li> <li>・<u>開発担当者と運用担当者の分離、管理者と担当者の分離等の相互牽制体制 等</u></li> </ul> <p>キ. <u>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。</u></p> <p>なお、「機密情報」とは、暗証番号、パスワード等、参加者に損失が発生する可能性のある情報をいう。</p> <p>ク. <u>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。</u></p> <p>ケ. <u>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。</u></p> <p>コ. <u>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。</u></p> <p>⑤ <u>サイバーセキュリティ管理</u></p> <p>ア. <u>サイバーセキュリティについて、取締役会又は理事会等は、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。</u></p> <p>イ. <u>サイバーセキュリティについて、組織体制の整備、規則等の策定のほか、以下のようなサイバーセキュリティ管理態勢の整備を図っているか。</u></p> <ul style="list-style-type: none"> <li>・<u>サイバー攻撃に対する監視体制</u></li> <li>・<u>サイバー攻撃を受けた際の報告及び広報体制</u></li> <li>・<u>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</u></li> <li>・<u>情報共有機関等を通じた情報収集・共有体制 等</u></li> </ul> <p>ウ. <u>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</u></p>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
	<p>いるか。</p> <ul style="list-style-type: none"> <li>・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）</li> <li>・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）</li> <li>・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）</li> </ul> <p>エ. 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。</p> <ul style="list-style-type: none"> <li>・攻撃元の IP アドレスの特定と遮断</li> <li>・DDoS 攻撃に対して自動的にアクセスを分散させる機能</li> <li>・システムの全部又は一部の一時的停止 等</li> </ul> <p>オ. 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。</p> <p>カ. 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。</p> <p>キ. インターネット等の通信手段を利用して業務を行う場合には、例えば、以下のような業務のリスクに見合った適切な認証方式を導入しているか。</p> <ul style="list-style-type: none"> <li>・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</li> <li>・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 等</li> </ul> <p>ク. インターネット等の通信手段を利用して業務を行う場合には、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。</p> <ul style="list-style-type: none"> <li>・参加者のシステムのウィルス感染状況を資金清算機関側で検知し、警告を発するソフトの導入</li> <li>・電子証明書を IC カード等、当該業務に利用しているシステムとは別の媒体・機器へ格納する方式の採用</li> <li>・不正なログイン・異常な入力等を検知し、速やかに参加者に連絡する体制の整備 等</li> </ul>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>③ システム企画・開発・運用管理 ア. ～カ. (略)</p> <p>④ システム監査 ア. システム部門から独立した内部監査部門において、<u>システムに精通した監査要員による定期的なシステム監査が行われているか。</u> <u>(新設)</u></p> <p>イ. <u>監査の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。</u></p> <p>⑤ 安全対策 ア. <u>安全対策の基本方針が策定されているか。</u> イ. <u>定められた方針、基準及び手順に従って安全対策を適正に管理する安全管理者を設置しているか。安全管理者は、システム、データ、ネットワークの管理体制を統括しているか。</u></p> <p>⑥ 外部委託管理 ア. (略) イ. <u>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、提供されるサービス水準等を定めているか。</u></p> <p>ウ. <u>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。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。</u></p> <p>エ. <u>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。</u></p>	<p>ケ. <u>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。</u></p> <p>コ. <u>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。</u></p> <p>⑥ システム企画・開発・運用管理 ア. ～カ. (略)</p> <p>⑦ システム監査 ア. システム部門から独立した内部監査部門において、<u>定期的なシステム監査が行われているか。</u> イ. <u>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。</u> ウ. <u>監査の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。</u> <u>(削除)</u></p> <p>⑧ 外部委託管理 ア. (略) イ. <u>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、提供されるサービス水準等を定めているか。また、外部委託先の役職員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。</u> ウ. <u>システムに係る外部委託業務（二段階以上の委託を含む）について、リスク管理が適切に行われているか。（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。</u> エ. <u>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しているか。</u> また、外部委託先における参加者のデータの運用状況を委託元が</p>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>⑦ データ管理態勢</p> <p>ア. データについて機密性等の確保のため、データ管理者を置いているか。</p> <p>イ. データ保護、データ不正使用防止、不正プログラム防止策等について適切かつ十分な管理態勢を整備しているか。</p> <p>⑧ コンティンジェンシープラン</p> <p>ア. (略)</p> <p>イ. コンティンジェンシープランは、自社の業務の実態やシステム環境等に応じて常時見直され、実効性が維持される態勢となっているか。</p> <p>(新設)</p> <p>(新設)</p> <p>(新設)</p> <p>(新設)</p> <p>⑨ システム更改等のリスク</p> <p>ア. ～オ. (略)</p> <p>⑩ 障害発生時の対応等</p> <p>ア. 参加者等に無用の混乱を生じさせないための適切な措置を講じるとともに、速やかに復旧や代替手段の稼働に向けた作業を実施することとなっているか。</p>	<p><u>監視、追跡できる態勢となっているか。</u></p> <p><u>(削除)</u></p> <p>⑨ コンティンジェンシープラン</p> <p>ア. (略)</p> <p>イ. <u>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。</u></p> <p>ウ. <u>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なく、資金清算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。</u></p> <p><u>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。</u></p> <p>エ. <u>コンティンジェンシープランは、他の金融機関及び清算・振替機関等におけるシステム障害等の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。</u></p> <p>オ. <u>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、定期的を実施しているか。</u></p> <p>カ. <u>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に、速やかに業務を継続できる態勢を整備しているか。</u></p> <p>⑩ システム更改等のリスク</p> <p>ア. ～オ. (略)</p> <p>⑪ 障害発生時の対応等</p> <p>ア. <u>システム障害等が発生した場合に、参加者等に無用の混乱を生じさせないための適切な措置を講じるとともに、速やかに復旧や代替手段の稼働に向けた作業を実施することとなっているか。</u></p> <p><u>また、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</u></p>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>(新設)</p> <p>(新設)</p> <p>イ. 発生した障害について、原因を分析し、それに応じた再発防止策を講じることとしているか。</p> <p>ウ. 障害発生時に速やかに当局に対する報告を行うこととなっているか。</p> <p>(3) (略)</p> <p>(4) システム障害に対する対応</p> <p>① システム障害の発生を認識次第、直ちに、その事実の当局宛て報告を求めるとともに、「障害発生等報告書」(別紙様式2-1)にて当局宛て報告を求めるものとする。</p> <p>また、復旧時、原因説明時には改めてその旨報告を求めるとする(ただし、復旧原因の説明がされていない場合でも1か月以内に現状について報告を求める)。</p> <p>(注) 報告すべきシステム障害</p> <p>その原因の如何を問わず、資金清算機関又は資金清算機関から業務の委託を受けた者等が現に使用しているシステム・機器(ハードウェア、ソフトウェア共)に発生した障害であって、取引、決済、入出金、資金繰り、財務状況把握、その他参加者等の利便等に影響があるもの</p>	<p><u>で、必要な対応を行う態勢となっているか。</u></p> <p>イ. <u>システム障害等の発生に備え、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。</u></p> <p>ウ. <u>経営に重大な影響を及ぼすシステム障害等が発生した場合に、速やかに代表取締役や理事長をはじめとする役員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、参加者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。</u></p> <p><u>また、必要に応じて、対策本部を立ち上げ、代表取締役や理事長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。</u></p> <p>エ. 発生したシステム障害等について、原因を分析し、それに応じた再発防止策を講じることとしているか。</p> <p><u>また、システム障害等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。</u></p> <p>オ. <u>システム障害等の発生時に速やかに当局に対する報告を行うこととなっているか。</u></p> <p>(3) (略)</p> <p>(4) システム障害等に対する対応</p> <p>① システム障害等の発生を認識次第、直ちに、その事実の当局宛て報告を求めるとともに、「障害発生等報告書」(別紙様式2-1)にて当局宛て報告を求めるものとする。</p> <p>また、復旧時、原因説明時には改めてその旨報告を求めるとする(ただし、復旧原因の説明がされていない場合でも1か月以内に現状について報告を求める)。</p> <p>(注) 報告すべきシステム障害等</p> <p>その原因の如何を問わず、資金清算機関又は資金清算機関から業務の委託を受けた者等が現に使用しているシステム・機器(ハードウェア、ソフトウェア共)に発生した障害であって、取引、決済、入出金、資金繰り、財務状況把握、その他参加者等の利便等に影響があるもの</p>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>又はそのおそれがあるもの。</p> <p>ただし、一部のシステム・機器にこれらの影響が生じても他のシステム・機器が速やかに代替することで実質的にはこれらの影響が生じない場合を除く。</p> <p>なお、障害が発生していない場合であっても、サイバー攻撃の予告がなされ、又はサイバー攻撃が検知される等により、<u>上記のような障害が発生する可能性が高いと認められる時は、報告を要するものとする。</u></p> <p>② （略）</p>	<p>又はそのおそれがあるもの。</p> <p>ただし、一部のシステム・機器にこれらの影響が生じても他のシステム・機器が速やかに代替することで実質的にはこれらの影響が生じない場合を除く。</p> <p>なお、障害が発生していない場合であっても、サイバー攻撃の予告がなされ、又はサイバー攻撃が検知される等により、<u>参加者や業務に影響を及ぼす、又は及ぼす可能性が高いと認められる時は、報告を要するものとする。</u></p> <p>② （略）</p>



清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>V. 監督上の評価項目と諸手続（振替機関）</p> <p>V-3 業務の適切性</p> <p>V-3-4 システムリスク管理</p> <p>(1) 意義</p> <p>システムリスクとは、一般に、コンピュータシステムのダウン又は誤作動等の、システムの不備等に伴い、振替機関等が損失を被るリスクや、コンピュータが不正に使用されることにより振替機関等が損失を被るリスクをいう。</p> <p>振替機関のシステムは、振替等のために不可欠な市場の基盤そのものであり、仮にシステム障害が発生した場合には、振替機関及びシステムに接続する口座管理機関等に損害が生じ、ひいては、金融システム全体に影響を及ぼすこととなりかねない。</p> <p>このため、振替機関における堅牢なシステムリスク管理態勢の構築が重要である。</p> <p><u>（新設）</u></p> <p>(2) 主な着眼点</p> <p>① システムリスクに対する認識等</p> <p>ア. (略)</p> <p><u>（新設）</u></p> <p>イ. システムリスクに関する情報が、適切に経営陣に報告される体制となっているか。</p> <p>② (略)</p>	<p>V. 監督上の評価項目と諸手続（振替機関）</p> <p>V-3 業務の適切性</p> <p>V-3-4 システムリスク管理</p> <p>(1) 意義</p> <p>システムリスクとは、一般に、コンピュータシステムのダウン又は誤作動等の、システムの不備等に伴い、振替機関等が損失を被るリスクや、コンピュータが不正に使用されることにより振替機関等が損失を被るリスクをいう。</p> <p>振替機関のシステムは、振替等のために不可欠な市場の基盤そのものであり、仮にシステム障害やサイバーセキュリティ事案が発生した場合には、振替機関及びシステムに接続する口座管理機関等に損害が生じ、ひいては、金融システム全体に影響を及ぼすこととなりかねない。</p> <p>このため、振替機関における堅牢なシステムリスク管理態勢の構築が重要である。</p> <p><u>（注）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。</u></p> <p>(2) 主な着眼点</p> <p>① システムリスクに対する認識等</p> <p>ア. (略)</p> <p>イ. <u>取締役会は、システム障害やサイバーセキュリティ事案（以下「システム障害等」という。）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。</u></p> <p>ウ. システムリスクに関する情報が、適切に経営陣に報告される体制となっているか。</p> <p>② (略)</p>



清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>(新設)</p>	<p><u>不正情報取得、情報漏えい等を牽制、防止する仕組みを導入しているか。</u></p> <ul style="list-style-type: none"> <li>・職員<span style="font-size: small;">の権限に応じて必要な範囲に限定されたアクセス権限の付与</span></li> <li>・アクセス記録<span style="font-size: small;">の保存、検証</span></li> <li>・開発担当者<span style="font-size: small;">と運用担当者の分離、管理者と担当者の分離等の相互牽制体制</span> 等</li> </ul> <p>キ. <u>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。</u></p> <p>なお、「機密情報」とは、暗証番号、パスワード等、口座管理機関に損失が発生する可能性のある情報をいう。</p> <p>ク. <u>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。</u></p> <p>ケ. <u>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。</u></p> <p>コ. <u>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。</u></p> <p>⑤ <u>サイバーセキュリティ管理</u></p> <p>ア. <u>サイバーセキュリティについて、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。</u></p> <p>イ. <u>サイバーセキュリティについて、組織体制の整備、社内規程の策定のほか、以下のようなサイバーセキュリティ管理態勢の整備を図っているか。</u></p> <ul style="list-style-type: none"> <li>・サイバー攻撃<span style="font-size: small;">に対する監視体制</span></li> <li>・サイバー攻撃<span style="font-size: small;">を受けた際の報告及び広報体制</span></li> <li>・組織内 CSIRT (Computer Security Incident Response Team) <span style="font-size: small;">等の緊急時対応及び早期警戒のための体制</span></li> <li>・情報共有機関等<span style="font-size: small;">を通じた情報収集・共有体制</span> 等</li> </ul> <p>ウ. <u>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</u></p>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
	<p>いるか。</p> <ul style="list-style-type: none"> <li>・ <u>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）</u></li> <li>・ <u>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）</u></li> <li>・ <u>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）</u></li> </ul> <p>エ. <u>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。</u></p> <ul style="list-style-type: none"> <li>・ <u>攻撃元の IP アドレスの特定と遮断</u></li> <li>・ <u>DDoS 攻撃に対して自動的にアクセスを分散させる機能</u></li> <li>・ <u>システムの全部又は一部の一時的停止 等</u></li> </ul> <p>オ. <u>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。</u></p> <p>カ. <u>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。</u></p> <p>キ. <u>インターネット等の通信手段を利用して業務を行う場合には、例えば、以下のような業務のリスクに見合った適切な認証方式を導入しているか。</u></p> <ul style="list-style-type: none"> <li>・ <u>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</u></li> <li>・ <u>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 等</u></li> </ul> <p>ク. <u>インターネット等の通信手段を利用して業務を行う場合には、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。</u></p> <ul style="list-style-type: none"> <li>・ <u>口座管理機関等のパソコンのウィルス感染状況を振替機関側で検知し、警告を発するソフトの導入</u></li> <li>・ <u>電子証明書を IC カード等、当該業務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</u></li> <li>・ <u>不正なログイン・異常な入力等を検知し、速やかに口座管理機関等に連絡する体制の整備 等</u></li> </ul>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>③ システム企画・開発・運用管理 ア. ～カ. (略)</p> <p>④ システム監査 ア. システム部門から独立した内部監査部門において、<u>システムに精通した監査要員による定期的なシステム監査が行われているか。</u> <u>(新設)</u></p> <p>イ. <u>監査の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。</u></p> <p>⑤ 安全対策 ア. <u>安全対策の基本方針が策定されているか。</u> イ. <u>定められた方針、基準及び手順に従って安全対策を適正に管理する安全管理者を設置しているか。安全管理者は、システム、データ、ネットワークの管理体制を統括しているか。</u></p> <p>⑥ 外部委託管理 ア. (略) イ. <u>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、提供されるサービス水準等を定めているか。</u></p> <p>ウ. <u>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。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。</u></p> <p>エ. <u>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。</u></p>	<p><u>ケ. 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。</u></p> <p><u>コ. 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。</u></p> <p>⑥ システム企画・開発・運用管理 ア. ～カ. (略)</p> <p>⑦ システム監査 ア. システム部門から独立した内部監査部門において、<u>定期的なシステム監査が行われているか。</u> イ. <u>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。</u> ウ. <u>監査の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。</u> <u>(削除)</u></p> <p>⑧ 外部委託管理 ア. (略) イ. <u>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、提供されるサービス水準等を定めているか。また、外部委託先の社員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。</u> ウ. <u>システムに係る外部委託業務（二段階以上の委託を含む）について、リスク管理が適切に行われているか。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。</u> エ. <u>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しているか。</u> <u>また、外部委託先における投資者や口座管理機関等のデータの運</u></p>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>⑦ データ管理態勢</p> <p>ア. データについて機密性等の確保のため、データ管理者を置いているか。</p> <p>イ. データ保護、データ不正使用防止、不正プログラム防止策等について適切かつ十分な管理態勢を整備しているか。</p> <p>⑧ コンティンジェンシープラン</p> <p>ア. (略)</p> <p>イ. コンティンジェンシープランは、自社の業務の実態やシステム環境等に応じて常時見直され、実効性が維持される態勢となっているか。</p> <p>(新設)</p> <p>(新設)</p> <p>(新設)</p> <p>(新設)</p> <p>⑨ システム更改等のリスク</p> <p>ア. ～オ. (略)</p> <p>⑩ 障害発生時の対応等</p> <p>ア. 投資者や口座管理機関等に無用の混乱を生じさせないための適切な措置を講じるとともに、速やかに復旧や代替手段の稼働に向けた作業を実施することとなっているか。</p>	<p>用状況を委託元が監視、追跡できる態勢となっているか。</p> <p>(削除)</p> <p>⑨ コンティンジェンシープラン</p> <p>ア. (略)</p> <p>イ. 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。</p> <p>ウ. 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なく、振替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。</p> <p>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。</p> <p>エ. コンティンジェンシープランは、他の金融機関及び清算・振替機関等におけるシステム障害等の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。</p> <p>オ. 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、定期的実施しているか。</p> <p>カ. 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に、速やかに業務を継続できる態勢を整備しているか。</p> <p>⑩ システム更改等のリスク</p> <p>ア. ～オ. (略)</p> <p>⑪ 障害発生時の対応等</p> <p>ア. システム障害等が発生した場合に、投資者や口座管理機関等に無用の混乱を生じさせないための適切な措置を講じるとともに、速やかに復旧や代替手段の稼働に向けた作業を実施することとなっているか。</p>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>(新設)</p> <p>(新設)</p> <p>イ. 発生した障害について、原因を分析し、それに応じた再発防止策を講じることとしているか。</p> <p>ウ. 障害発生時に速やかに当局に対する報告を行うこととなっているか。</p> <p>(3) (略)</p> <p>(4) システム障害に対する対応</p> <p>① システム障害の発生を認識次第、直ちに、その事実の当局宛て報告を求めるとともに、「障害発生等報告書」(別紙様式3-1)にて当局宛て報告を求めるとする。</p> <p>また、復旧時、原因説明時には改めてその旨報告を求めるとする(ただし、復旧原因の説明がされていない場合でも1か月以内に現状について報告を求め)。</p> <p>(注) 報告すべきシステム障害</p> <p>その原因の如何を問わず、振替機関又は振替機関から業務の委託を受けた者等が現に使用しているシステム・機器(ハードウェア、ソフトウェア共)に発生した障害であって、取引、決済、入出金、資金繰</p>	<p>また、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となっているか。</p> <p>イ. システム障害等の発生に備え、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。</p> <p>ウ. 経営に重大な影響を及ぼすシステム障害等が発生した場合に、速やかに代表取締役をはじめとする取締役等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、投資者や口座管理機関等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。</p> <p>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。</p> <p>エ. 発生したシステム障害等について、原因を分析し、それに応じた再発防止策を講じることとしているか。</p> <p>また、システム障害等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。</p> <p>オ. システム障害等の発生時に速やかに当局に対する報告を行うこととなっているか。</p> <p>(3) (略)</p> <p>(4) システム障害等に対する対応</p> <p>① システム障害等の発生を認識次第、直ちに、その事実の当局宛て報告を求めるとともに、「障害発生等報告書」(別紙様式3-1)にて当局宛て報告を求めるとする。</p> <p>また、復旧時、原因説明時には改めてその旨報告を求めるとする(ただし、復旧原因の説明がされていない場合でも1か月以内に現状について報告を求め)。</p> <p>(注) 報告すべきシステム障害等</p> <p>その原因の如何を問わず、振替機関又は振替機関から業務の委託を受けた者等が現に使用しているシステム・機器(ハードウェア、ソフトウェア共)に発生した障害であって、取引、決済、入出金、資金繰</p>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>り、財務状況把握、その他口座管理機関等の利便等に影響があるもの又はそのおそれがあるもの。</p> <p>ただし、一部のシステム・機器にこれらの影響が生じても他のシステム・機器が速やかに代替することで実質的にはこれらの影響が生じない場合を除く。</p> <p>なお、障害が発生していない場合であっても、サイバー攻撃の予告がなされ、又はサイバー攻撃が検知される等により、<u>上記のような障害が発生する可能性が高いと認められる時は、報告を要するものとする。</u></p> <p>② （略）</p>	<p>り、財務状況把握、その他口座管理機関等の利便等に影響があるもの又はそのおそれがあるもの。</p> <p>ただし、一部のシステム・機器にこれらの影響が生じても他のシステム・機器が速やかに代替することで実質的にはこれらの影響が生じない場合を除く。</p> <p>なお、障害が発生していない場合であっても、サイバー攻撃の予告がなされ、又はサイバー攻撃が検知される等により、<u>口座管理機関や業務に影響を及ぼす、又は及ぼす可能性が高いと認められる時は、報告を要するものとする。</u></p> <p>② （略）</p>



清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>VI. 監督上の評価項目と諸手続（取引情報蓄積機関）</p> <p>VI-3 業務の適切性</p> <p>VI-3-4 システムリスク管理</p> <p>(1) 意義</p> <p>システムリスクとは、一般に、コンピュータシステムのダウン又は誤作動等の、システムの不備等に伴い、取引情報蓄積機関や利用者が損失を被るリスクや、コンピュータが不正に使用されることにより取引情報蓄積機関や利用者が損失を被るリスクをいう。</p> <p>取引情報蓄積機関のシステムは、取引情報蓄積業務等のために不可欠な市場の基盤そのものであり、仮にシステム障害が発生した場合には、取引情報蓄積機関及びシステムに接続する利用者等に損害が生じかねない。</p> <p>このため、取引情報蓄積機関における堅牢なシステムリスク管理態勢の構築が重要である。</p> <p><u>(新設)</u></p> <p>(2) 主な着眼点</p> <p>① システムリスクに対する認識等</p> <p>ア. (略)</p> <p><u>(新設)</u></p> <p>イ. システムリスクに関する情報が、適切に経営陣に報告される体制となっているか。</p> <p>② (略)</p>	<p>VI. 監督上の評価項目と諸手続（取引情報蓄積機関）</p> <p>VI-3 業務の適切性</p> <p>VI-3-4 システムリスク管理</p> <p>(1) 意義</p> <p>システムリスクとは、一般に、コンピュータシステムのダウン又は誤作動等の、システムの不備等に伴い、取引情報蓄積機関や利用者が損失を被るリスクや、コンピュータが不正に使用されることにより取引情報蓄積機関や利用者が損失を被るリスクをいう。</p> <p>取引情報蓄積機関のシステムは、取引情報蓄積業務等のために不可欠な市場の基盤そのものであり、仮にシステム障害やサイバーセキュリティ事案が発生した場合には、取引情報蓄積機関及びシステムに接続する利用者等に損害が生じかねない。</p> <p>このため、取引情報蓄積機関における堅牢なシステムリスク管理態勢の構築が重要である。</p> <p><u>(注) 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。</u></p> <p>(2) 主な着眼点</p> <p>① システムリスクに対する認識等</p> <p>ア. (略)</p> <p>イ. <u>取締役会は、システム障害やサイバーセキュリティ事案（以下「システム障害等」という。）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。</u></p> <p>ウ. システムリスクに関する情報が、適切に経営陣に報告される体制となっているか。</p> <p>② (略)</p>



清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>(新設)</p>	<p><u>報取得、情報漏えい等を牽制、防止する仕組みを導入しているか。</u></p> <ul style="list-style-type: none"> <li>・<u>職員の権限に応じて必要な範囲に限定されたアクセス権限の付与</u></li> <li>・<u>アクセス記録の保存、検証</u></li> <li>・<u>開発担当者と運用担当者の分離、管理者と担当者の分離等の相互牽制体制</u> 等</li> </ul> <p>キ. <u>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。</u></p> <p>なお、「機密情報」とは、暗証番号、パスワード等、利用者に損失が発生する可能性のある情報をいう。</p> <p>ク. <u>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。</u></p> <p>ケ. <u>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。</u></p> <p>コ. <u>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。</u></p> <p>⑤ <u>サイバーセキュリティ管理</u></p> <p>ア. <u>サイバーセキュリティについて、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。</u></p> <p>イ. <u>サイバーセキュリティについて、組織体制の整備、社内規則等の策定のほか、以下のようなサイバーセキュリティ管理態勢の整備を図っているか。</u></p> <ul style="list-style-type: none"> <li>・<u>サイバー攻撃に対する監視体制</u></li> <li>・<u>サイバー攻撃を受けた際の報告及び広報体制</u></li> <li>・<u>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</u></li> <li>・<u>情報共有機関等を通じた情報収集・共有体制</u> 等</li> </ul> <p>ウ. <u>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。</u></p>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
	<ul style="list-style-type: none"> <li>・<u>入口対策（例えば、ファイアウォールの設置、抗ウイルスソフトの導入、不正侵入検知システム・不正侵入防止システムの導入等）</u></li> <li>・<u>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）</u></li> <li>・<u>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）</u></li> <li>エ. <u>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。</u> <ul style="list-style-type: none"> <li>・<u>攻撃元のIPアドレスの特定と遮断</u></li> <li>・<u>DDoS 攻撃に対して自動的にアクセスを分散させる機能</u></li> <li>・<u>システムの全部又は一部の一時的停止等</u></li> </ul> </li> <li>オ. <u>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。</u></li> <li>カ. <u>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。</u></li> <li>キ. <u>インターネット等の通信手段を利用して業務を行う場合には、例えば、以下のような業務のリスクに見合った適切な認証方式を導入しているか。</u> <ul style="list-style-type: none"> <li>・<u>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</u></li> <li>・<u>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等</u></li> </ul> </li> <li>ク. <u>インターネット等の通信手段を利用して業務を行う場合には、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。</u> <ul style="list-style-type: none"> <li>・<u>利用者のパソコンのウイルス感染状況を取引情報蓄積機関側で検知し、警告を発するソフトの導入</u></li> <li>・<u>電子証明書をICカード等、当該業務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</u></li> <li>・<u>不正なログイン・異常な入力等を検知し、速やかに利用者に連絡する体制の整備等</u></li> </ul> </li> <li>ケ. <u>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、</u></li> </ul>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>③ システム企画・開発・運用管理 ア. ～カ. (略)</p> <p>④ システム監査 ア. システム部門から独立した内部監査部門において、<u>システムに精通した監査要員による定期的なシステム監査が行われているか。</u> (新設)</p> <p>イ. 監査の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。</p> <p>⑤ 安全対策 ア. <u>安全対策の基本方針が策定されているか。</u> イ. <u>定められた方針、基準及び手順に従って安全対策を適正に管理する安全管理者を設置しているか。安全管理者は、システム、データ、ネットワークの管理体制を統括しているか。</u></p> <p>⑥ 外部委託管理 ア. (略) イ. 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、提供されるサービス水準等を定めているか。</p> <p>ウ. 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。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。</p> <p>エ. 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。</p>	<p><u>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。</u></p> <p>コ. <u>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。</u></p> <p>⑥ システム企画・開発・運用管理 ア. ～カ. (略)</p> <p>⑦ システム監査 ア. システム部門から独立した内部監査部門において、定期的なシステム監査が行われているか。 イ. <u>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。</u> ウ. 監査の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。 (削除)</p> <p>⑧ 外部委託管理 ア. (略) イ. 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、提供されるサービス水準等を定めているか。<u>また、外部委託先の社員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。</u> ウ. システムに係る外部委託業務（二段階以上の委託を含む）について、リスク管理が適切に行われているか。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。 エ. 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しているか。 <u>また、外部委託先における投資者や利用者等の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。</u></p>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>⑦ データ管理態勢  <u>ア. データについて機密性等の確保のため、データ管理者を置いているか。</u>  <u>イ. データ保護、データ不正使用防止、不正プログラム防止策等について適切かつ十分な管理態勢を整備しているか。</u></p> <p>⑧ コンティンジェンシープラン            ア. (略)  <u>イ. コンティンジェンシープランは、自社の業務の実態やシステム環境等に応じて常時見直され、実効性が維持される態勢となっているか。</u></p> <p><u>(新設)</u></p> <p><u>(新設)</u></p> <p><u>(新設)</u></p> <p><u>(新設)</u></p> <p>⑨ システム更改等のリスク            ア. ～オ. (略)</p> <p>⑩ 障害発生時の対応等            ア. 投資者や利用者等に無用の混乱を生じさせないための適切な措置を講じるとともに、速やかに復旧や代替手段の稼働に向けた作業を実施することとなっているか。</p>	<p><u>(削除)</u></p> <p>⑨ コンティンジェンシープラン            ア. (略)  <u>イ. 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。</u>  <u>ウ. 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なく、取引情報蓄積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。</u>  <u>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。</u>  <u>エ. コンティンジェンシープランは、他の金融機関及び清算・振替機関等におけるシステム障害等の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。</u>  <u>オ. 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、定期的実施しているか。</u>  <u>カ. 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に、速やかに業務を継続できる態勢を整備しているか。</u></p> <p>⑩ システム更改等のリスク            ア. ～オ. (略)</p> <p>⑪ 障害発生時の対応等            ア. <u>システム障害等が発生した場合に、投資者や利用者等に無用の混乱を生じさせないための適切な措置を講じるとともに、速やかに復旧や代替手段の稼働に向けた作業を実施することとなっているか。</u>  <u>また、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となっているか。</u></p>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p><u>(新設)</u></p> <p><u>(新設)</u></p> <p>イ. 発生した障害について、原因を分析し、それに応じた再発防止策を講じることとしているか。</p> <p>ウ. 障害発生時に速やかに当局に対する報告を行うこととなっているか。</p> <p>(3) (略)</p> <p>(4) システム障害に対する対応</p> <p>① システム障害の発生を認識次第、直ちに、その事実の当局宛て報告を求めるとともに、「障害発生等報告書」（別紙様式4-1）にて当局宛て報告を求めものとする。</p> <p>また、復旧時、原因解明時には改めてその旨報告を求めることとする（ただし、復旧原因の解明がされていない場合でも1か月以内に現状について報告を求め）。</p> <p>(注) 報告すべきシステム障害</p> <p>その原因の如何を問わず、取引情報蓄積機関又は取引情報蓄積機関から業務の委託を受けた者等が現に使用しているシステム・機器（ハードウェア、ソフトウェア共）に発生した障害であって、取引情報の収集・保存・報告に遅延、停止等が生じているものその他利用者等の利便等に影響があるもの又はそのおそれがあるもの。</p>	<p><u>イ. システム障害等の発生に備え、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。</u></p> <p><u>ウ. 経営に重大な影響を及ぼすシステム障害等が発生した場合に、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、投資者や利用者等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。</u></p> <p><u>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。</u></p> <p><u>エ. 発生したシステム障害等について、原因を分析し、それに応じた再発防止策を講じることとしているか。</u></p> <p><u>また、システム障害等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。</u></p> <p><u>オ. システム障害等の発生時に速やかに当局に対する報告を行うこととなっているか。</u></p> <p>(3) (略)</p> <p>(4) システム障害等に対する対応</p> <p>① システム障害等の発生を認識次第、直ちに、その事実の当局宛て報告を求めるとともに、「障害発生等報告書」（別紙様式4-1）にて当局宛て報告を求めものとする。</p> <p>また、復旧時、原因解明時には改めてその旨報告を求めることとする（ただし、復旧原因の解明がされていない場合でも1か月以内に現状について報告を求め）。</p> <p>(注) 報告すべきシステム障害等</p> <p>その原因の如何を問わず、取引情報蓄積機関又は取引情報蓄積機関から業務の委託を受けた者等が現に使用しているシステム・機器（ハードウェア、ソフトウェア共）に発生した障害であって、取引情報の収集・保存・報告に遅延、停止等が生じているものその他利用者等の利便等に影響があるもの又はそのおそれがあるもの。</p>

清算・振替機関等向けの総合的な監督指針（新旧対照表）

現 行	改 正 後
<p>ただし、一部のシステム・機器にこれらの影響が生じても他のシステム・機器が速やかに代替することで実質的にはこれらの影響が生じない場合を除く。</p> <p>なお、障害が発生していない場合であっても、サイバー攻撃の予告がなされ、又はサイバー攻撃が検知される等により、<u>上記のような障害が発生する可能性が高いと認められる時は、報告を要するものとする。</u></p> <p>② （略）</p>	<p>ただし、一部のシステム・機器にこれらの影響が生じても他のシステム・機器が速やかに代替することで実質的にはこれらの影響が生じない場合を除く。</p> <p>なお、障害が発生していない場合であっても、サイバー攻撃の予告がなされ、又はサイバー攻撃が検知される等により、<u>利用者や業務に影響を及ぼす、又は及ぼす可能性が高いと認められる時は、報告を要するものとする。</u></p> <p>② （略）</p>