金融商品取引業者等向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
【本編】 Ⅲ－２－８　システムリスク管理態勢 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顧客や金融商品取引業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顧客や金融商品取引業者が損失を被るリスクをいうが、金融商品取引業者の経営再編に伴うシステム統合や新商品・サービスの拡大等に伴い、金融商品取引業者の情報システムは一段と高度化・複雑化し、更にコンピュータのネットワーク化の拡大に伴い、重要情報に対する不正なアクセスや漏えい等のリスクが大きくなっている。 システムが安全かつ安定的に稼動することは、金融商品市場及び金融商品取引業者に対する信頼を確保するための大前提であり、システムリスク管理態勢の充実強化は極めて重要である。 （１）主な着眼点 システムリスク管理態勢の検証については、金融商品取引業者の業容に応じて、例えば以下の点に留意して検証することとする（着眼点の詳細については、必要に応じて証券検査マニュアルを参照。）。 ①　システムリスクに対する認識等 イ．　（略） （新設） （新設） ロ．システムリスクに関する情報が、適切に経営者に報告される体制となっているか。	**【本編】** Ⅲ－２－８　システムリスク管理態勢 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顧客や金融商品取引業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顧客や金融商品取引業者が損失を被るリスクをいうが、金融商品取引業者の経営再編に伴うシステム統合や新商品・サービスの拡大等に伴い、金融商品取引業者の情報システムは一段と高度化・複雑化し、さらにコンピュータのネットワーク化の拡大に伴い、重要情報に対する不正なアクセスや漏えい等のリスクが大きくなっている。 システムが安全かつ安定的に稼動することは、金融商品市場及び金融商品取引業者に対する信頼を確保するための大前提であり、システムリスク管理態勢の充実強化は極めて重要である。 （１）主な着眼点 システムリスク管理態勢の検証については、金融商品取引業者の業容に応じて、例えば以下の点に留意して検証することとする（着眼点の詳細については、必要に応じて金融商品取引業者等検査マニュアルを参照。）。 ①　システムリスクに対する認識等 イ．　（略） ロ．取締役会等は、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。 （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。 ハ．システムリスクに関する情報が、適切に経営者に報告される体制となっているか。

金融商品取引業者等向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
②　（略） （新設）	②　（略） ③　システムリスク評価 　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。 　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。
（新設）	④　情報セキュリティ管理 イ．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、社内規程の策定、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。 ロ．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。 ハ．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。 ニ．金融商品取引業者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 ホ．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

現　　行	改　正　後
	・記録媒体等の取扱いルール　等 ヘ．顧客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。 ・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 ・アクセス記録の保存、検証 ・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 ト．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。 チ．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。 リ．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。 ヌ．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。
（新設）	⑤　サイバーセキュリティ管理 イ．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。 ロ．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。 ・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 ハ．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

現　　行	改　正　後
	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） ニ．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 ホ．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。 ヘ．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。 ト．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。 ・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証　等 （注）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、振込先金融機関口座（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

現　　行	改　正　後
（新設）	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。 チ．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金融商品取引業者側で検知し、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 リ．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。 ヌ．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。 ⑥　システム企画・開発・運用管理 イ．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。 ロ．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。 ハ．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。 ニ．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。 ホ．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。 ヘ．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。

金融商品取引業者等向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
③　システム監査	⑦　システム監査
イ．システム部門から独立した内部監査部門において、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。	イ．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。
（新設）	ロ．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。
ロ．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。	ハ．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。
④　安全対策の整備	（削除）
イ．安全対策の基本方針が策定されているか。	
ロ．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。	
⑤　外部委託管理	⑧　外部委託管理
（新設）	イ．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、検討の上、選定しているか。
（新設）	ロ．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。
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。	ハ．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。
（新設）	ニ．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。 また、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。
⑥　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
イ．　（略）	イ．　（略）
ロ．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。	ロ．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

金融商品取引業者等向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
	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）	ハ．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、金融商品取引業者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）	ニ．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。
（新設）	ホ．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。
（新設）	ヘ．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。
⑦　システム統合リスク イ．～ホ．　（略）	⑩　システム統合リスク イ．～ホ．　（略）
⑧　障害発生時の対応 イ．障害発生時に、顧客に無用の混乱を生じさせないための適切な措置を講じているか。	⑪　障害発生時の対応 イ．システム障害等が発生した場合に、顧客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。 　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。
（新設）	ロ．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。
（新設）	ハ．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、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

現　　行	改　正　後
ロ．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ているか。	か。 ニ．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ているか。 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。
ハ．障害発生時、速やかに当局に報告する体制が整備されているか。	ホ．システム障害等が発生した場合、速やかに当局に報告する体制が整備されているか。
（２）監督手法・対応 ①・②　（略）	（２）監督手法・対応 ①・②　（略）
（３）システム障害時における対応 ①　コンピュータシステムの障害の発生を認識次第、直ちに、その事実の当局あて報告を求めるとともに、「障害発生等報告書」（別紙様式Ⅲ－１）にて当局あて報告を求めるものとする。 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ヵ月以内に現状について報告を行うこと。）。 なお、財務局は金融商品取引業者から報告があった場合は直ちに金融庁担当課室に連絡すること。 （注）報告すべきシステム障害等 その原因の如何を問わず、金融商品取引業者又は金融商品取引業者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、金融商品取引、決済、入出金、資金繰り、財務状況把握、その他顧客利便等に影響があるもの又はそのおそれがあるもの。 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（例えば、立会時間外に受注システムが停止した場合において、速やかに当該システムに相当する代替システムを起動させることによって受注が可能となり、立会時間に間に合った場合。）を除く。 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	（３）障害発生時 ①　システム障害等の発生を認識次第、直ちに、その事実の当局あて報告を求めるとともに、「障害発生等報告書」（別紙様式Ⅲ－１）にて当局あて報告を求めるものとする。 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ヵ月以内に現状について報告を行うこと。）。 なお、財務局は金融商品取引業者から報告があった場合は直ちに金融庁担当課室に連絡すること。 （注）報告すべきシステム障害等 その原因の如何を問わず、金融商品取引業者又は金融商品取引業者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、金融商品取引、決済、入出金、資金繰り、財務状況把握、その他顧客利便等に影響があるもの又はそのおそれがあるもの。 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（例えば、立会時間外に受注システムが停止した場合において、速やかに当該システムに相当する代替システムを起動させることによって受注が可能となり、立会時間に間に合った場合。）を除く。 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

金融商品取引業者等向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
予告がなされ、又はサイバー攻撃が検知される等により、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。 ②　（略）	予告がなされ、又はサイバー攻撃が検知される等により、顧客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。 ②　（略）