（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
Ⅰ　基本的考え方	Ⅰ　基本的考え方
２．証券監視委の役割及び金融商品取引業者等のあるべき姿	２．証券監視委の役割及び金融商品取引業者等のあるべき姿
［金融商品取引業者等のあるべき姿］	［金融商品取引業者等のあるべき姿］
⑷　リスク管理態勢 金融商品取引業者等は、その営む業務に内在する種々のリスクを正確に把握し、これが実現することにより生じ得る損失を適切に管理することが、投資者保護ひいては金融システムの安定に欠かせないことを認識し、自己資本規制比率の適正水準での維持（第一種金融商品取引業者に限る。）や必要なリスク管理態勢を整備すべきである。 ［具体的対応例］ （略） ・システムリスクは、円滑な業務遂行を実現するとの観点から、システムの安全かつ安定的な稼動は重要であるとの認識のもと、導入に際しての方針、メンテナンス、障害や災害時の対応など、適切なリスク管理を行うための態勢を整備する。 （略）	⑷　リスク管理態勢 金融商品取引業者等は、その営む業務に内在する種々のリスクを正確に把握し、これが実現することにより生じ得る損失を適切に管理することが、投資者保護ひいては金融システムの安定に欠かせないことを認識し、自己資本規制比率の適正水準での維持（第一種金融商品取引業者に限る。）や必要なリスク管理態勢を整備すべきである。 ［具体的対応例］ （略） ・システムリスクは、円滑な業務遂行を実現するとの観点から、システムの安全かつ安定的な稼動は重要であるとの認識のもと、導入に際しての方針、メンテナンス、システム障害等の発生時や災害時の対応など、適切なリスク管理を行うための態勢を整備する。 （略）
Ⅱ－１－２　態勢編・第一種金融商品取引業者	Ⅱ－１－２　態勢編・第一種金融商品取引業者
５．システムリスク管理態勢	５．システムリスク管理態勢
⑴　システムリスクに対する認識等 （略）	⑴　システムリスクに対する認識等 ①　（略）

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
（新設）	②　取締役会等は、システム障害やサイバーセキュリティに関する事案（⑵、⑸及び⑹並びに８．⑸において「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１）　「サイバーセキュリティに関する事案」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。以下同じ。
⑵　適切なシステムリスク管理態勢の確立 ①　（略） （新設）	⑵　適切なシステムリスク管理態勢の確立 ①　（略） ②　システムリスク管理部門の責任者は、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。
②　取締役会等は、システムリスク管理の方針を適切かつ明確に定めているか。システムリスク管理の方針には、情報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）及び外部委託管理に関する方針が含まれているか。また、管理方針に基づき、具体的な対応部署及びその役割と責任を定め、適切な要員を割当てるとともに、定期的又は随時に、管理状況等の報告を受ける体	③　取締役会等は、システムリスク管理の方針を適切かつ明確に定めているか。システムリスク管理の方針には、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（サイバーセキュリティに関するものを含む。））及び外部委託管理に関する方針が含まれているか。また、管理方針に基づき、具体的な対応部署及びその役割と責任を定め、適切な要員を割当てるとともに、定期的又

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
制を構築しているか。	は随時に、管理状況等の報告を受ける体制を構築しているか。
③・④　（略）	④・⑤　（略）
⑤　取締役会等は、会社を取り巻く環境の変化に応じ、リスクの再評価とこれに対応するための適切な組織（役割と責任及び人員）、管理規程等を適宜見直すことにより、実効性が維持される体制を構築していること。	⑥　取締役会等は、会社を取り巻く環境の変化に応じ、リスクの再評価とこれに対応するための適切な組織（役割と責任及び人員）、管理規程等を適宜見直すことにより、実効性が維持される体制を構築しているか。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。
（新設）	⑦　取締役会等は、システム障害等の発生時において、自らの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か。
⑶　安全対策の整備	⑶　安全対策の整備
①　情報セキュリティ管理態勢の整備	①　情報セキュリティ管理態勢の整備
イ　取締役会等は、コンピュータシステムにより管理される情報資産の漏えいや不正使用等を防止し、金融商品取引業者や顧客が損失を被るリスクを低減するため、情報セキュリティ管理部署及びその役割と責任を定めるなど、情報セキュリティ管理態勢を整備しているか。また、情報セキュリティ管理の対象となる情報資産について、種類や所在を具体的に記載した規程が制定され、情報資産が明確化されているか。	イ　取締役会等は、情報の機密性、完全性、可用性を維持しつつ、コンピュータシステムにより管理される情報資産の漏えいや不正使用等を防止し、金融商品取引業者や顧客が損失を被るリスクを低減するため、情報セキュリティ管理部署及びその役割と責任を定めるなど、情報セキュリティ管理態勢を整備しているか。また、情報セキュリティ管理の対象となる情報資産について、種類や所在を具体的に記載した規程が制定され、情報資産が明確化されているか。
ロ　情報セキュリティ管理部署の責任者は、情報セキュリティに係る全社的な管理体制を明確にするとともに、情報資産の主管部署・担当者に対して適切な牽制機能が働くよう、リスクに配慮した適切な体制を維持しているか。	ロ　情報セキュリティ管理部署の責任者は、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。また、情報セキュリティに係る全社的な管理体制を明確にするとともに、情報資産の主管部署・担当者に対して適切な牽

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
	制機能が働くよう、リスクに配慮した適切な体制を維持しているか。
ハ　（略）	ハ　（略）
（新設）	ニ　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。
（新設）	ホ　業務、システム、外部委託先を対象範囲として、顧客の重要情報等を網羅的に洗い出し、把握、管理しているか。また、洗い出した顧客の重要情報等について、重要度やリスクに応じた情報管理ルールを定め、実施しているか。
（新設）	ヘ　顧客の重要情報等について、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。 a.　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 b.　アクセス記録の保存、検証 c.　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
（新設）	ト　機密情報（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。チにおいて同じ。）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、実施しているか。
（新設）	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、より厳格なルールを定め、実施しているか。

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
二　（略）	リ　（略）
ホ　情報資産のリスク状況等を踏まえ、建物への侵入防止設備等の物理的方法やシステムへの利用者パスワードの設定等による論理的方法により、適切なアクセス管理等が実施され、管理状況が点検されているか。また、重要な情報資産を有するシステム等へのアクセス状況が記録され、不正アクセスや情報漏えいの有無等が点検されているか。さらに、顧客や業務への影響が大きいシステムについては、アクセス状況の監視を通じ、サイバー攻撃（注１）等による影響が点検されているか。	ヌ　情報資産のリスク状況等を踏まえ、建物への侵入防止設備等の物理的方法やシステムへの利用者パスワードの設定等による論理的方法により、適切なアクセス管理等が実施され、管理状況が点検されているか。また、重要な情報資産を有するシステム等へのアクセス状況が記録され、不正アクセスや情報漏えいの有無等が点検されているか。さらに、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、情報セキュリティ管理態勢を継続的に見直しているか。
ヘ・ト　（略）	ル・ヲ　（略）
（注１）　「サイバー攻撃」とは、情報通信ネットワーク上で、特定の情報システムや、ネットワークそのものなどに対して意図的に行われる電子的な攻撃を指す。攻撃の種類には、不正侵入、データ改ざん・破壊、不正コマンド実行、ウイルス攻撃、サービス不能（DoS: Denial of Service）攻撃等の犯罪行為が含まれている。以下同じ。	（削る）
（新設）	②　サイバーセキュリティ管理態勢の整備 イ　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。また、例えば、以下のようなサイバーセキュリティ管理態勢を整備しているか。 a.　サイバー攻撃に対する監視体制 b.　サイバー攻撃を受けた際の報告及び広報体制 c.　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

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
	d.　情報共有機関等を通じた情報収集・共有体制　等 ロ　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。 a.　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） b.　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） c.　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） ハ　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の措置を講じているか。 例えば、 a.　攻撃元の IP アドレスの特定と遮断 b.　DDoS 攻撃に対して自動的にアクセスを分散させる機能 c.　システムの全部又は一部の一時的停止　等 ニ　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。 ホ　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。 ヘ　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、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。また、業務に応じた不正防止策を講じているか。 ト　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

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
	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。 チ　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。
②・③　（略）	③・④　（略）
⑸　障害発生時の対応 ①　障害等の発生に備え、公益又は投資者保護の観点から速やかな復旧が図られるよう、復旧手順及び方策について標準化を図っているか。また、障害等の発生を想定した業務の継続や復旧作業の訓練を行うなど、実効性のあるものとなっているか。	⑸　システム障害等の発生時の対応 ①　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、公益又は投資者保護の観点から速やかな復旧が図られるよう、復旧手順及び方策について標準化を図るとともに、外部委託先を含めた報告態勢及び指揮・命令系統が明確になっているか。また、システム障害等の発生を想定した業務の継続や復旧作業の訓練を行うなど、実効性のあるものとなっているか。
（新設）	②　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か。
②　システム障害等発生時に適切かつ速やかな対応が行えるよう、システムに精通した要員を育成し、かつ、必要な際の連絡手段を確保しているか。	③　システム障害等の発生時に適切かつ速やかな対応が行えるよう、システムに精通した要員を育成し、かつ、必要な際の連絡手段を確保しているか。
③　システム障害等発生時に、顧客に無用な混乱を生じさせないため、情報の開示範囲や基準に加え、必要な手順及び手段等を定めて	④　システム障害等の発生時に、顧客に無用な混乱を生じさせないため、情報の開示範囲や基準に加え、必要な手順及び手段等を定めて

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
いるか。	いるか。
④　（略）	⑤　（略）
⑤　システム障害の内容を記録し、定期的に又は必要に応じて随時に、システム納入ベンダー等の専門家を交え、障害の根本的な原因の究明及び対策について検討し、抜本的な改善を図ることにより再発防止に努めているか。なお、障害の全体的な発生状況・原因等についての分析を通じた再発防止策の実施を含む。	⑥　システム障害等の内容を記録し、定期的に又は必要に応じて随時に、システム納入ベンダー等の専門家を交え、システム障害等の根本的な原因の究明及び対策について検討し、抜本的な改善を図ることにより再発防止に努めているか。なお、システム障害等の全体的な発生状況・原因等についての分析を通じた再発防止策の実施を含む。
⑥　障害発生時や復旧時及び原因解明時等において、速やかに当局に報告する体制を整備しているか。	⑦　システム障害等の発生時や復旧時及び原因解明時等において、速やかに当局に報告する体制を整備しているか。
⑹　コンティンジェンシープラン	⑹　コンティンジェンシープラン
（新設）	①　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。
（新設）	②　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。
①　障害の発生を想定し、復旧の必要性及び緊急性を考慮して全ての業務に優先度を定めるとともに、障害の程度や原因等に応じた目標復旧時間や復旧手順及び方策を明示しているか。また、サイバー攻撃等については、的確に状況を把握し、攻撃による被害の拡大を防	③　システム障害等の発生を想定し、復旧の必要性及び緊急性を考慮して全ての業務に優先度を定めるとともに、システム障害等の程度や原因等に応じた目標復旧時間や復旧手順及び方策を明示しているか。また、サイバー攻撃等については、的確に状況を把握し、攻撃

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
止するための体制を構築した上で、当局への報告や関係機関との連携を含めた対応手順や方策を具体化しているか。	による被害の拡大を防止するための体制を構築した上で、当局への報告や関係機関との連携を含めた対応手順や方策を具体化しているか。
②　（略）	④　（略）
③　障害発生を想定した定期的な訓練等によりコンティンジェンシープランの実効性に係る検証を行っているか。	⑤　システム障害等の発生を想定した定期的な訓練等を全社レベルで、かつ、外部委託先等と合同で実施し、コンティンジェンシープランの実効性に係る検証を行っているか。
④　会社を取り巻く環境の変化や組織の変更、要員の異動等をコンティンジェンシープランに反映させるよう、適宜、必要な見直しを図っているか。	⑥　会社を取り巻く環境の変化や組織の変更、要員の異動等をコンティンジェンシープランに反映させるとともに他の金融商品取引業者など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、適宜、必要な見直しを図っているか。
（新設）	⑦　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。
⑤・⑥　（略）	⑧・⑨　（略）
⑺　外部委託管理（注２） （略） ①・②　（略） ③　委託先との契約 業務委託を行うことによるリスクを認識し、契約において機密保持、再委託条項、監査権限、サービスレベル及び紛争解決方法等を明確に定めているか。 ④　委託業務の管理	⑺　外部委託管理 （略） ①・②　（略） ③　委託先との契約 業務委託を行うことによるリスクを認識し、契約において、委託先との役割・責任分担、機密保持、再委託条項、監査権限、サービスレベル及び紛争解決方法等を明確に定めているか。また、委託先が遵守すべきルールやセキュリティ要件を委託先へ提示し、契約書等に明記しているか。 ④　委託業務の管理

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
イ　委託先における事故、不正等の防止及び機密保持等の対策の実施状況を会社として把握し、必要な措置を講じているか。	イ　委託先（委託先から委託（二以上の段階にわたる委託を含む。）を受けた者を含む。ロにおいて同じ。）における事故、不正等の防止及び機密保持等の対策の実施状況を会社として把握し、必要な措置を講じているか。
（新設）	ロ　外部委託した業務について、委託先におい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、委託先における顧客データ等の運用状況を監視、追跡できる態勢となっているか。
ロ・ハ　（略）	ハ・ニ　（略）
8．大規模かつ複雑な業務をグループ一体として行う証券会社グループのリスク管理態勢等	8．大規模かつ複雑な業務をグループ一体として行う証券会社グループのリスク管理態勢等
⑸　システムリスク管理態勢	⑸　システムリスク管理態勢
①　方針の策定	①　方針の策定
○　システムリスク管理方針の整備・周知	○　システムリスク管理方針の整備・周知
イ　経営管理会社は、グループ全体の経営方針に則った戦略目標を踏まえ、システムリスクの所在、規模、種類、特性を反映した、グループ全体のシステムリスク管理方針を定め、海外拠点を含むグループ全体に周知しているか。また、システムリスク管理方針には、情報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）及び外部委託管理に関する方針が含まれているか。	イ　経営管理会社は、グループ全体の経営方針に則った戦略目標を踏まえ、システムリスクの所在、規模、種類、特性を反映した、グループ全体のシステムリスク管理方針を定め、海外拠点を含むグループ全体に周知しているか。また、システムリスク管理方針には、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（サイバーセキュリティに関するものを含む。））及び外部委託管理に関する方針が含まれているか。
ロ　（略）	ロ　（略）

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
②　内部規程・組織態勢の整備 イ・ロ　（略） ハ　システムリスクの把握 a.　経営管理会社は、システムリスク管理方針及びシステムリスク管理規程に基づき、グループ各社における業務の内容を検討し、コントロール・セルフ・アセスメント等のリスク評価手法等を用いることにより、国内外拠点あるいは各部門のシステムリスクを適切に評価する態勢を整備しているか b.　経営管理会社は、システムリスクの評価を行う過程で、システム障害や情報セキュリティ事故等の発生原因を分析し、システムリスクを網羅的及び体系的に把握する態勢を整備しているか。 c.　（略） d.　経営管理会社は、グループ各社からのシステムリスクの状況に係る報告に、リスク管理の実効性を保つために必要な情報が含まれていることを確かめているか。例えば、以下の情報が含まれ、適切な判断及び対応が実施される態勢がとられているか。 （略） －システム障害への対応・改善状況等に関する情報 （略） e.　（略） ③　有効性の評価・改善 イ　システムリスク管理の分析・評価	②　内部規程・組織態勢の整備 イ・ロ　（略） ハ　システムリスクの把握 a.　経営管理会社は、システムリスク管理方針及びシステムリスク管理規程に基づき、グループ各社における業務の内容を検討し、コントロール・セルフ・アセスメント等のリスク評価手法等を用いることにより、国内外拠点あるいは各部門のシステムリスクを適切に評価する態勢を整備しているか。 b.　経営管理会社は、システムリスクの評価を行う過程で、システム障害等や情報セキュリティ事故等の発生原因を分析し、システムリスクを網羅的及び体系的に把握する態勢を整備しているか。 c.　（略） d.　経営管理会社は、グループ各社からのシステムリスクの状況に係る報告に、リスク管理の実効性を保つために必要な情報が含まれていることを確かめているか。例えば、以下の情報が含まれ、適切な判断及び対応が実施される態勢がとられているか。 （略） －システム障害等への対応・改善状況等に関する情報 （略） e.　（略） ③　有効性の評価・改善 イ　システムリスク管理の分析・評価

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
a.・b.　（略）	a.・b.　（略）
c.　経営管理会社は、グループ各社が、重要な個別リスク（※）の管理状況について、適切に分析・評価し、態勢上の問題点、弱点等改善すべき点の有無及びその内容を検討するとともに、その原因を検証しているかについて、定期的かつ必要に応じて随時検証を行っているか。	c.　経営管理会社は、グループ各社が、重要な個別リスク（※）の管理状況について、適切に分析・評価し、態勢上の問題点、弱点等改善すべき点の有無及びその内容を検討するとともに、その原因を検証しているかについて、定期的かつ必要に応じて随時検証を行っているか。
（※）「重要な個別リスク」とは、過去に発生したグループ全体に重大な影響を及ぼすシステム障害や情報セキュリティ事故等を通じて顕在化したリスク、及び監査等を通じてグループ全体のシステムリスク管理上重大なリスクが顕在化する可能性を指摘されたリスクを指す。	（※）「重要な個別リスク」とは、過去に発生したグループ全体に重大な影響を及ぼすシステム障害等や情報セキュリティ事故等を通じて顕在化したリスク、及び監査等を通じてグループ全体のシステムリスク管理上重大なリスクが顕在化する可能性を指摘されたリスクを指す。
ロ　（略）	ロ　（略）
Ⅱ－１－３　態勢編・第二種金融商品取引業者	Ⅱ－１－３　態勢編・第二種金融商品取引業者
４．システムリスク管理態勢	４．システムリスク管理態勢
⑴　システムリスクに対する認識等 （略） （新設）	⑴　システムリスクに対する認識等 ①　（略） ②　取締役会等は、システム障害やサイバーセキュリティに関する事案（⑵、⑸及び⑹において「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。
⑵　適切なシステムリスク管理態勢の確立	⑵　適切なシステムリスク管理態勢の確立

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
①　（略）	①　（略）
（新設）	②　システムリスク管理部門の責任者は、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。
②　取締役会等は、システムリスク管理の方針を適切かつ明確に定めているか。システムリスク管理の方針には、情報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）及び外部委託管理に関する方針が含まれているか。また、管理方針に基づき、具体的な対応部署及びその役割と責任を定め、適切な要員を割当てるとともに、定期的又は随時に、管理状況等の報告を受ける体制を構築しているか。	③　取締役会等は、システムリスク管理の方針を適切かつ明確に定めているか。システムリスク管理の方針には、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（サイバーセキュリティに関するものを含む。））及び外部委託管理に関する方針が含まれているか。また、管理方針に基づき、具体的な対応部署及びその役割と責任を定め、適切な要員を割当てるとともに、定期的又は随時に、管理状況等の報告を受ける体制を構築しているか。
③・④　（略）	④・⑤　（略）
⑤　取締役会等は、会社を取り巻く環境の変化に応じ、リスクの再評価とこれに対応するための適切な組織（役割と責任及び人員）、管理規程等を適宜見直すことにより、実効性が維持される体制を構築しているか。	⑥　取締役会等は、会社を取り巻く環境の変化に応じ、リスクの再評価とこれに対応するための適切な組織（役割と責任及び人員）、管理規程等を適宜見直すことにより、実効性が維持される体制を構築しているか。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。
（新設）	⑦　取締役会等は、システム障害等の発生時において、自らの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か。
⑶　安全対策の整備	⑶　安全対策の整備

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
①　情報セキュリティ管理態勢の整備	①　情報セキュリティ管理態勢の整備
イ　取締役会等は、コンピュータシステムにより管理される情報資産の漏えいや不正使用等を防止し、金融商品取引業者や顧客が損失を被るリスクを低減するため、情報セキュリティ管理部署及びその役割と責任を定めるなど、情報セキュリティ管理態勢を整備しているか。また、情報セキュリティ管理の対象となる情報資産について、種類や所在を具体的に記載した規程が制定され、情報資産が明確化されているか。	イ　取締役会等は、情報の機密性、完全性、可用性を維持しつつ、コンピュータシステムにより管理される情報資産の漏えいや不正使用等を防止し、金融商品取引業者や顧客が損失を被るリスクを低減するため、情報セキュリティ管理部署及びその役割と責任を定めるなど、情報セキュリティ管理態勢を整備しているか。また、情報セキュリティ管理の対象となる情報資産について、種類や所在を具体的に記載した規程が制定され、情報資産が明確化されているか。
ロ　情報セキュリティ管理部署の責任者は、情報セキュリティに係る全社的な管理体制を明確にするとともに、情報資産の主管部署・担当者に対して適切な牽制機能が働くよう、リスクに配慮した適切な体制を維持しているか。	ロ　情報セキュリティ管理部署の責任者は、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。また、情報セキュリティに係る全社的な管理体制を明確にするとともに、情報資産の主管部署・担当者に対して適切な牽制機能が働くよう、リスクに配慮した適切な体制を維持しているか。
ハ　（略）	ハ　（略）
（新設）	ニ　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。
（新設）	ホ　業務、システム、外部委託先を対象範囲として、顧客の重要情報等を網羅的に洗い出し、把握、管理しているか。また、洗い出した顧客の重要情報等について、重要度やリスクに応じた情報管理ルールを定め、実施しているか。
（新設）	ヘ　顧客の重要情報等について、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。

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
	a.　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
	b.　アクセス記録の保存、検証
	c.　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
（新設）	ト　機密情報（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。チにおいて同じ。）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、実施しているか。
（新設）	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、より厳格なルールを定め、実施しているか。
ニ　（略）	リ　（略）
ホ　情報資産のリスク状況等を踏まえ、建物への侵入防止設備等の物理的方法やシステムへの利用者パスワードの設定等による論理的方法により、適切なアクセス管理等が実施され、管理状況が点検されているか。また、重要な情報資産を有するシステム等へのアクセス状況が記録され、不正アクセスや情報漏えいの有無等が点検されているか。さらに、顧客や業務への影響が大きいシステムについては、アクセス状況の監視を通じ、サイバー攻撃等による影響が点検されているか。	ヌ　情報資産のリスク状況等を踏まえ、建物への侵入防止設備等の物理的方法やシステムへの利用者パスワードの設定等による論理的方法により、適切なアクセス管理等が実施され、管理状況が点検されているか。また、重要な情報資産を有するシステム等へのアクセス状況が記録され、不正アクセスや情報漏えいの有無等が点検されているか。さらに、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、情報セキュリティ管理態勢を継続的に見直しているか。
ヘ・ト　（略）	ル・ヲ　（略）
（新設）	②　サイバーセキュリティ管理態勢の整備
	イ　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

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
	備しているか。また、例えば、以下のようなサイバーセキュリティ管理態勢を整備しているか。 a.　サイバー攻撃に対する監視体制 b.　サイバー攻撃を受けた際の報告及び広報体制 c.　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 d.　情報共有機関等を通じた情報収集・共有体制　等 ロ　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。 a.　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） b.　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） c.　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） ハ　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の措置を講じているか。 例えば、 a.　攻撃元の IP アドレスの特定と遮断 b.　DDoS 攻撃に対して自動的にアクセスを分散させる機能 c.　システムの全部又は一部の一時的停止　等 ニ　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。 ホ　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

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
	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。 ヘ　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、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。また、業務に応じた不正防止策を講じているか。 ト　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。 チ　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。
②・③　（略）	③・④　（略）
⑸　障害発生時の対応 ①　障害等の発生に備え、公益又は投資者保護の観点から速やかな復旧が図られるよう、復旧手順及び方策について標準化を図っているか。また、障害等の発生を想定した業務の継続や復旧作業の訓練を行うなど、実効性のあるものとなっているか。	⑸　システム障害等の発生時の対応 ①　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、公益又は投資者保護の観点から速やかな復旧が図られるよう、復旧手順及び方策について標準化を図るとともに、外部委託先を含めた報告態勢及び指揮・命令系統が明確になっているか。また、システム障害等の発生を想定した業務の継続や復旧作業の訓練を行うなど、実効性のあるものとなっているか。
（新設）	②　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

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
	題の解決を図る態勢となっているか。
②　システム障害等発生時に適切かつ速やかな対応が行えるよう、システムに精通した要員を育成し、かつ、必要な際の連絡手段を確保しているか。	③　システム障害等の発生時に適切かつ速やかな対応が行えるよう、システムに精通した要員を育成し、かつ、必要な際の連絡手段を確保しているか。
③　システム障害等発生時に、顧客に無用な混乱を生じさせないため、情報の開示範囲や基準に加え、必要な手順及び手段等を定めているか。	④　システム障害等の発生時に、顧客に無用な混乱を生じさせないため、情報の開示範囲や基準に加え、必要な手順及び手段等を定めているか。
④　（略）	⑤　（略）
⑤　システム障害の内容を記録し、定期的に又は必要に応じて随時に、システム納入ベンダー等の専門家を交え、障害の根本的な原因の究明及び対策について検討し、抜本的な改善を図ることにより再発防止に努めているか。なお、障害の全体的な発生状況・原因等についての分析を通じた再発防止策の実施を含む。	⑥　システム障害等の内容を記録し、定期的に又は必要に応じて随時に、システム納入ベンダー等の専門家を交え、システム障害等の根本的な原因の究明及び対策について検討し、抜本的な改善を図ることにより再発防止に努めているか。なお、システム障害等の全体的な発生状況・原因等についての分析を通じた再発防止策の実施を含む。
⑥　障害発生時や復旧時及び原因解明時等において、速やかに当局に報告する体制が整備されているか。	⑦　システム障害等の発生時や復旧時及び原因解明時等において、速やかに当局に報告する体制が整備されているか。
⑹　コンティンジェンシープラン	⑹　コンティンジェンシープラン
（新設）	①　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。
（新設）	②　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

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
	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。
①　障害の発生を想定し、復旧の必要性及び緊急性を考慮して全ての業務に優先度を定めるとともに、障害の程度や原因等に応じた目標復旧時間や復旧手順及び方策を明示しているか。また、サイバー攻撃等については、的確に状況を把握し、攻撃による被害の拡大を防止するための体制を構築した上で、当局への報告や関係機関との連携を含めた対応手順や方策を具体化しているか。	③　システム障害等の発生を想定し、復旧の必要性及び緊急性を考慮して全ての業務に優先度を定めるとともに、システム障害等の程度や原因等に応じた目標復旧時間や復旧手順及び方策を明示しているか。また、サイバー攻撃等については、的確に状況を把握し、攻撃による被害の拡大を防止するための体制を構築した上で、当局への報告や関係機関との連携を含めた対応手順や方策を具体化しているか。
②　（略）	④　（略）
③　障害発生を想定した定期的な訓練等によりコンティンジェンシープランの実効性に係る検証を行っているか。	⑤　システム障害等の発生を想定した定期的な訓練等を全社レベルで、かつ、外部委託先等と合同で実施し、コンティンジェンシープランの実効性に係る検証を行っているか。
④　会社を取り巻く環境の変化や組織の変更、要員の異動等をコンティンジェンシープランに反映させるよう、適宜、必要な見直しを図っているか。	⑥　会社を取り巻く環境の変化や組織の変更、要員の異動等をコンティンジェンシープランに反映させるとともに他の金融商品取引業者など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、適宜、必要な見直しを図っているか。
（新設）	⑦　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。
⑤・⑥　（略）	⑧・⑨　（略）
⑺　外部委託管理	⑺　外部委託管理
①・②　（略）	①・②　（略）
③　委託先との契約 業務委託を行うことによるリスクを認識し、契約において機密保	③　委託先との契約 業務委託を行うことによるリスクを認識し、契約において、委託

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
持、再委託条項、監査権限、サービスレベル及び紛争解決方法等を明確に定めているか。	先との役割・責任分担、機密保持、再委託条項、監査権限、サービスレベル及び紛争解決方法等を明確に定めているか。また、委託先が遵守すべきルールやセキュリティ要件を委託先へ提示し、契約書等に明記しているか。
④　委託業務の管理 イ　委託先における事故、不正等の防止及び機密保持等の対策の実施状況を会社として把握し、必要な措置を講じているか。	④　委託業務の管理 イ　委託先（委託先から委託（二以上の段階にわたる委託を含む。）を受けた者を含む。ロにおいて同じ。）における事故、不正等の防止及び機密保持等の対策の実施状況を会社として把握し、必要な措置を講じているか。
（新設）	ロ　外部委託した業務について、委託先におい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、委託先における顧客データ等の運用状況を監視、追跡できる態勢となっているか。
ロ・ハ　（略）	ハ・ニ　（略）
Ⅱ－１－４　態勢編・投資助言・代理業者	Ⅱ－１－４　態勢編・投資助言・代理業者
４．システムリスク管理態勢	４．システムリスク管理態勢
⑴　システムリスクに対する認識等 （略） （新設）	⑴　システムリスクに対する認識等 ①　（略） ②　取締役会等は、システム障害やサイバーセキュリティに関する事案（⑵、⑸及び⑹において「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。

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
⑵　適切なシステムリスク管理態勢の確立	⑵　適切なシステムリスク管理態勢の確立
①　（略）	①　（略）
（新設）	②　システムリスク管理部門の責任者は、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。
②　取締役会等は、システムリスク管理の方針を適切かつ明確に定めているか。システムリスク管理の方針には、情報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）及び外部委託管理に関する方針が含まれているか。また、管理方針に基づき、具体的な対応部署及びその役割と責任等を定め、定期的又は随時に、管理状況等の報告を受ける体制を構築しているか。	③　取締役会等は、システムリスク管理の方針を適切かつ明確に定めているか。システムリスク管理の方針には、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（サイバーセキュリティに関するものを含む。））及び外部委託管理に関する方針が含まれているか。また、管理方針に基づき、具体的な対応部署及びその役割と責任等を定め、定期的又は随時に、管理状況等の報告を受ける体制を構築しているか。
③・④　（略）	④・⑤　（略）
⑤　取締役会等は、会社を取り巻く環境の変化に応じ、リスクの再評価とこれに対応するための適切な組織（役割と責任等）、管理規程等を適宜見直すことにより、実効性が維持される体制を構築しているか。	⑥　取締役会等は、会社を取り巻く環境の変化に応じ、リスクの再評価とこれに対応するための適切な組織（役割と責任等）、管理規程等を適宜見直すことにより、実効性が維持される体制を構築しているか。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。
（新設）	⑦　取締役会等は、システム障害等の発生時において、自らの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か。

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
⑶　安全対策の整備	⑶　安全対策の整備
①　情報セキュリティ管理態勢の整備	①　情報セキュリティ管理態勢の整備
イ　取締役会等は、コンピュータシステムにより管理される情報資産の漏えいや不正使用等を防止し、金融商品取引業者や顧客が損失を被るリスクを低減するため、情報セキュリティ管理部署及びその役割と責任を定めるなど、情報セキュリティ管理態勢を整備しているか。また、情報セキュリティ管理の対象となる情報資産について、種類や所在を具体的に記載した規程が制定され、情報資産が明確化されているか。	イ　取締役会等は、情報の機密性、完全性、可用性を維持しつつ、コンピュータシステムにより管理される情報資産の漏えいや不正使用等を防止し、金融商品取引業者や顧客が損失を被るリスクを低減するため、情報セキュリティ管理部署及びその役割と責任を定めるなど、情報セキュリティ管理態勢を整備しているか。また、情報セキュリティ管理の対象となる情報資産について、種類や所在を具体的に記載した規程が制定され、情報資産が明確化されているか。
ロ　情報セキュリティ管理部署の責任者は、情報セキュリティに係る全社的な管理体制を明確にするとともに、情報資産の主管部署・担当者に対して適切な牽制機能が働くよう、リスクに配慮した適切な体制を維持しているか。	ロ　情報セキュリティ管理部署の責任者は、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。また、情報セキュリティに係る全社的な管理体制を明確にするとともに、情報資産の主管部署・担当者に対して適切な牽制機能が働くよう、リスクに配慮した適切な体制を維持しているか。
ハ　（略）	ハ　（略）
（新設）	ニ　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。
（新設）	ホ　業務、システム、外部委託先を対象範囲として、顧客の重要情報等を網羅的に洗い出し、把握、管理しているか。また、洗い出した顧客の重要情報等について、重要度やリスクに応じた情報管理ルールを定め、実施しているか。
（新設）	ヘ　顧客の重要情報等について、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

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
	か。 a.　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 b.　アクセス記録の保存、検証 c.　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
（新設）	ト　機密情報（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。チにおいて同じ。）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、実施しているか。
（新設）	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、より厳格なルールを定め、実施しているか。
ニ　（略）	リ　（略）
ホ　情報資産のリスク状況等を踏まえ、建物への侵入防止設備等の物理的方法やシステムへの利用者パスワードの設定等による論理的方法により、適切なアクセス管理等が実施され、管理状況が点検されているか。また、重要な情報資産を有するシステム等へのアクセス状況が記録され、不正アクセスや情報漏えいの有無等が点検されているか。さらに、顧客や業務への影響が大きいシステムについては、アクセス状況の監視を通じ、サイバー攻撃等による影響が点検されているか。	ヌ　情報資産のリスク状況等を踏まえ、建物への侵入防止設備等の物理的方法やシステムへの利用者パスワードの設定等による論理的方法により、適切なアクセス管理等が実施され、管理状況が点検されているか。また、重要な情報資産を有するシステム等へのアクセス状況が記録され、不正アクセスや情報漏えいの有無等が点検されているか。さらに、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、情報セキュリティ管理態勢を継続的に見直しているか。
ヘ・ト　（略）	ル・ヲ　（略）
（新設）	②　サイバーセキュリティ管理態勢の整備 イ　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

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
	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。また、例えば、以下のようなサイバーセキュリティ管理態勢を整備しているか。 a.　サイバー攻撃に対する監視体制 b.　サイバー攻撃を受けた際の報告及び広報体制 c.　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 d.　情報共有機関等を通じた情報収集・共有体制　等 ロ　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。 a.　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） b.　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） c.　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） ハ　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の措置を講じているか。 例えば、 a.　攻撃元の IP アドレスの特定と遮断 b.　DDoS 攻撃に対して自動的にアクセスを分散させる機能 c.　システムの全部又は一部の一時的停止　等 ニ　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。

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
	ホ　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。 ヘ　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、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。また、業務に応じた不正防止策を講じているか。 ト　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。 チ　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。
②・③　（略）	③・④　（略）
⑸　障害発生時の対応 ①　障害等の発生に備え、公益又は投資者保護の観点から速やかな復旧が図られるよう、復旧手順及び方策について標準化を図っているか。また、障害等の発生を想定した業務の継続や復旧作業の訓練を行うなど、実効性のあるものとなっているか。	⑸　システム障害等の発生時の対応 ①　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、公益又は投資者保護の観点から速やかな復旧が図られるよう、復旧手順及び方策について標準化を図るとともに、外部委託先を含めた報告態勢及び指揮・命令系統が明確になっているか。また、システム障害等の発生を想定した業務の継続や復旧作業の訓練を行うなど、実効性のあるものとなっているか。
（新設）	②　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

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
	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。
②　システム障害等発生時に適切かつ速やかな対応が行えるよう、システムに精通した要員を育成し、かつ、必要な際の連絡手段を確保しているか。	③　システム障害等の発生時に適切かつ速やかな対応が行えるよう、システムに精通した要員を育成し、かつ、必要な際の連絡手段を確保しているか。
③　システム障害等発生時に、顧客に無用な混乱を生じさせないため、情報の開示範囲や基準に加え、必要な手順及び手段等を定めているか。	④　システム障害等の発生時に、顧客に無用な混乱を生じさせないため、情報の開示範囲や基準に加え、必要な手順及び手段等を定めているか。
④　（略）	⑤　（略）
⑤　システム障害の内容を記録し、定期的に又は必要に応じて随時に、システム納入ベンダー等の専門家を交え、障害の根本的な原因の究明及び対策について検討し、抜本的な改善を図ることにより再発防止に努めているか。なお、障害の全体的な発生状況・原因等についての分析を通じた再発防止策の実施を含む。	⑥　システム障害等の内容を記録し、定期的に又は必要に応じて随時に、システム納入ベンダー等の専門家を交え、システム障害等の根本的な原因の究明及び対策について検討し、抜本的な改善を図ることにより再発防止に努めているか。なお、システム障害等の全体的な発生状況・原因等についての分析を通じた再発防止策の実施を含む。
⑥　障害発生時や復旧時及び原因解明時等において、速やかに当局に報告する体制が整備されているか。	⑦　システム障害等の発生時や復旧時及び原因解明時等において、速やかに当局に報告する体制が整備されているか。
⑹　コンティンジェンシープラン	⑹　コンティンジェンシープラン
（新設）	①　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。
（新設）	②　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

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
	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。
①　障害の発生を想定し、復旧の必要性及び緊急性を考慮して全ての業務に優先度を定めるとともに、障害の程度や原因等に応じた目標復旧時間や復旧手順及び方策を明示しているか。また、サイバー攻撃等については、的確に状況を把握し、攻撃による被害の拡大を防止するための体制を構築した上で、当局への報告や関係機関との連携を含めた対応手順や方策を具体化しているか。	③　システム障害等の発生を想定し、復旧の必要性及び緊急性を考慮して全ての業務に優先度を定めるとともに、システム障害等の程度や原因等に応じた目標復旧時間や復旧手順及び方策を明示しているか。また、サイバー攻撃等については、的確に状況を把握し、攻撃による被害の拡大を防止するための体制を構築した上で、当局への報告や関係機関との連携を含めた対応手順や方策を具体化しているか。
②　（略）	④　（略）
③　障害発生を想定した定期的な訓練等によりコンティンジェンシープランの実効性に係る検証を行っているか。	⑤　システム障害等の発生を想定した定期的な訓練等を全社レベルで、かつ、外部委託先等と合同で実施し、コンティンジェンシープランの実効性に係る検証を行っているか。
④　会社を取り巻く環境の変化や組織の変更、要員の異動等をコンティンジェンシープランに反映させるよう、適宜、必要な見直しを図っているか。	⑥　会社を取り巻く環境の変化や組織の変更、要員の異動等をコンティンジェンシープランに反映させるとともに他の金融商品取引業者など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、適宜、必要な見直しを図っているか。
（新設）	⑦　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。
⑤・⑥　（略）	⑧・⑨　（略）
⑺　外部委託管理	⑺　外部委託管理
①・②　（略）	①・②　（略）
③　委託先との契約	③　委託先との契約

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
業務委託を行うことによるリスクを認識し、契約において機密保持、再委託条項、監査権限、サービスレベル及び紛争解決方法等を明確に定めているか。	業務委託を行うことによるリスクを認識し、契約において、委託先との役割・責任分担、機密保持、再委託条項、監査権限、サービスレベル及び紛争解決方法等を明確に定めているか。また、委託先が遵守すべきルールやセキュリティ要件を委託先へ提示し、契約書等に明記しているか。
④　委託業務の管理 イ　委託先における事故、不正等の防止及び機密保持等の対策の実施状況を会社として把握し、必要な措置を講じているか。	④　委託業務の管理 イ　委託先（委託先から委託（二以上の段階にわたる委託を含む。）を受けた者を含む。ロにおいて同じ。）における事故、不正等の防止及び機密保持等の対策の実施状況を会社として把握し、必要な措置を講じているか。
（新設）	ロ　外部委託した業務について、委託先におい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、委託先における顧客データ等の運用状況を監視、追跡できる態勢となっているか。
ロ・ハ　（略）	ハ・ニ　（略）
Ⅱ－１－５　態勢編・投資運用業者	Ⅱ－１－５　態勢編・投資運用業者
４．システムリスク管理態勢	４．システムリスク管理態勢
⑴　システムリスクに対する認識等 （略） （新設）	⑴　システムリスクに対する認識等 ①　（略） ②　取締役会等は、システム障害やサイバーセキュリティに関する事案（⑵、⑸及び⑹において「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。

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
⑵　適切なシステムリスク管理態勢の確立	⑵　適切なシステムリスク管理態勢の確立
①　（略）	①　（略）
（新設）	②　システムリスク管理部門の責任者は、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。
②　取締役会等は、システムリスク管理の方針を適切かつ明確に定めているか。システムリスク管理の方針には、情報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）及び外部委託管理に関する方針が含まれているか。また、管理方針に基づき、具体的な対応部署及びその役割と責任を定め、適切な要員を割当てるとともに、定期的又は随時に、管理状況等の報告を受ける体制を構築しているか。	③　取締役会等は、システムリスク管理の方針を適切かつ明確に定めているか。システムリスク管理の方針には、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（サイバーセキュリティに関するものを含む。））及び外部委託管理に関する方針が含まれているか。また、管理方針に基づき、具体的な対応部署及びその役割と責任を定め、適切な要員を割当てるとともに、定期的又は随時に、管理状況等の報告を受ける体制を構築しているか。
③・④　（略）	④・⑤　（略）
⑤　取締役会等は、会社を取り巻く環境の変化に応じ、リスクの再評価とこれに対応するための適切な組織（役割と責任及び人員）、管理規程等を適宜見直すことにより、実効性が維持される体制を構築しているか。	⑥　取締役会等は、会社を取り巻く環境の変化に応じ、リスクの再評価とこれに対応するための適切な組織（役割と責任及び人員）、管理規程等を適宜見直すことにより、実効性が維持される体制を構築しているか。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。
（新設）	⑦　取締役会等は、システム障害等の発生時において、自らの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か。

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
⑶　安全対策の整備	⑶　安全対策の整備
①　情報セキュリティ管理態勢の整備	①　情報セキュリティ管理態勢の整備
イ　取締役会等は、コンピュータシステムにより管理される情報資産の漏えいや不正使用等を防止し、金融商品取引業者や顧客が損失を被るリスクを低減するため、情報セキュリティ管理部署及びその役割と責任を定めるなど、情報セキュリティ管理態勢を整備しているか。また、情報セキュリティ管理の対象となる情報資産について、種類や所在を具体的に記載した規程が制定され、情報資産が明確化されているか。	イ　取締役会等は、情報の機密性、完全性、可用性を維持しつつ、コンピュータシステムにより管理される情報資産の漏えいや不正使用等を防止し、金融商品取引業者や顧客が損失を被るリスクを低減するため、情報セキュリティ管理部署及びその役割と責任を定めるなど、情報セキュリティ管理態勢を整備しているか。また、情報セキュリティ管理の対象となる情報資産について、種類や所在を具体的に記載した規程が制定され、情報資産が明確化されているか。
ロ　情報セキュリティ管理部署の責任者は、情報セキュリティに係る全社的な管理体制を明確にするとともに、情報資産の主管部署・担当者に対して適切な牽制機能が働くよう、リスクに配慮した適切な体制を維持しているか。	ロ　情報セキュリティ管理部署の責任者は、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。また、情報セキュリティに係る全社的な管理体制を明確にするとともに、情報資産の主管部署・担当者に対して適切な牽制機能が働くよう、リスクに配慮した適切な体制を維持しているか。
ハ　（略）	ハ　（略）
（新設）	ニ　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。
（新設）	ホ　業務、システム、外部委託先を対象範囲として、顧客の重要情報等を網羅的に洗い出し、把握、管理しているか。また、洗い出した顧客の重要情報等について、重要度やリスクに応じた情報管理ルールを定め、実施しているか。
（新設）	ヘ　顧客の重要情報等について、以下のような不正アクセス、不正

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
	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。
	a.　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
	b.　アクセス記録の保存、検証
	c.　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
（新設）	ト　機密情報（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。チにおいて同じ。）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、実施しているか。
（新設）	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、より厳格なルールを定め、実施しているか。
ニ　（略）	リ　（略）
ホ　情報資産のリスク状況等を踏まえ、建物への侵入防止設備等の物理的方法やシステムへの利用者パスワードの設定等による論理的方法により、適切なアクセス管理等が実施され、管理状況が点検されているか。また、重要な情報資産を有するシステム等へのアクセス状況が記録され、不正アクセスや情報漏えいの有無等が点検されているか。さらに、顧客や業務への影響が大きいシステムについては、アクセス状況の監視を通じ、サイバー攻撃等による影響が点検されているか。	ヌ　情報資産のリスク状況等を踏まえ、建物への侵入防止設備等の物理的方法やシステムへの利用者パスワードの設定等による論理的方法により、適切なアクセス管理等が実施され、管理状況が点検されているか。また、重要な情報資産を有するシステム等へのアクセス状況が記録され、不正アクセスや情報漏えいの有無等が点検されているか。さらに、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、情報セキュリティ管理態勢を継続的に見直しているか。
ヘ・ト　（略）	ル・ヲ　（略）
（新設）	②　サイバーセキュリティ管理態勢の整備

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
	イ　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。また、例えば、以下のようなサイバーセキュリティ管理態勢を整備しているか。 a.　サイバー攻撃に対する監視体制 b.　サイバー攻撃を受けた際の報告及び広報体制 c.　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 d.　情報共有機関等を通じた情報収集・共有体制　等 ロ　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。 a.　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） b.　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） c.　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） ハ　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の措置を講じているか。 例えば、 a.　攻撃元の IP アドレスの特定と遮断 b.　DDoS 攻撃に対して自動的にアクセスを分散させる機能 c.　システムの全部又は一部の一時的停止　等 ニ　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

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
	の適用など必要な対策を適時に講じているか。 ホ　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。 ヘ　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、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。また、業務に応じた不正防止策を講じているか。 ト　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。 チ　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。
②・③　（略）	③・④　（略）
⑸　障害発生時の対応 ①　障害等の発生に備え、公益又は投資者保護の観点から速やかな復旧が図られるよう、復旧手順及び方策について標準化を図っているか。また、障害等の発生を想定した業務の継続や復旧作業の訓練を行うなど、実効性のあるものとなっているか。	⑸　システム障害等の発生時の対応 ①　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、公益又は投資者保護の観点から速やかな復旧が図られるよう、復旧手順及び方策について標準化を図るとともに、外部委託先を含めた報告態勢及び指揮・命令系統が明確になっているか。また、システム障害等の発生を想定した業務の継続や復旧作業の訓練を行うなど、実効性のあるものとなっているか。
（新設）	②　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

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
	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。
②　システム障害等発生時に適切かつ速やかな対応が行えるよう、システムに精通した要員を育成し、かつ、必要な際の連絡手段を確保しているか。	③　システム障害等の発生時に適切かつ速やかな対応が行えるよう、システムに精通した要員を育成し、かつ、必要な際の連絡手段を確保しているか。
③　システム障害等発生時に、権利者に無用な混乱を生じさせないため、情報の開示範囲や基準に加え、必要な手順及び手段等を定めているか。	④　システム障害等の発生時に、権利者に無用な混乱を生じさせないため、情報の開示範囲や基準に加え、必要な手順及び手段等を定めているか。
④　（略）	⑤　（略）
⑤　システム障害の内容を記録し、定期的又は必要に応じて随時に、システム納入ベンダー等の専門家を交え、障害の根本的な原因の究明及び対策について検討し、抜本的な改善を図ることにより再発防止に努めているか。なお、障害の全体的な発生状況・原因等についての分析を通じた再発防止策の実施を含む。	⑥　システム障害等の内容を記録し、定期的に又は必要に応じて随時に、システム納入ベンダー等の専門家を交え、システム障害等の根本的な原因の究明及び対策について検討し、抜本的な改善を図ることにより再発防止に努めているか。なお、システム障害等の全体的な発生状況・原因等についての分析を通じた再発防止策の実施を含む。
⑥　障害発生時や復旧時及び原因解明時等において、速やかに当局に報告する体制を整備しているか。	⑦　システム障害等の発生時や復旧時及び原因解明時等において、速やかに当局に報告する体制を整備しているか。
⑹　コンティンジェンシープラン	⑹　コンティンジェンシープラン
（新設）	①　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。
（新設）	②　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

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
	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。
①　障害の発生を想定し、復旧の必要性及び緊急性を考慮して全ての業務に優先度を定めるとともに、障害の程度や原因等に応じた目標復旧時間や復旧手順及び方策を明示しているか。また、サイバー攻撃等については、的確に状況を把握し、攻撃による被害の拡大を防止するための体制を構築した上で、当局への報告や関係機関との連携を含めた対応手順や方策を具体化しているか。	③　システム障害等の発生を想定し、復旧の必要性及び緊急性を考慮して全ての業務に優先度を定めるとともに、システム障害等の程度や原因等に応じた目標復旧時間や復旧手順及び方策を明示しているか。また、サイバー攻撃等については、的確に状況を把握し、攻撃による被害の拡大を防止するための体制を構築した上で、当局への報告や関係機関との連携を含めた対応手順や方策を具体化しているか。
②　（略）	④　（略）
③　障害発生を想定した定期的な訓練等によりコンティンジェンシープランの実効性に係る検証を行っているか。	⑤　システム障害等の発生を想定した定期的な訓練等を全社レベルで、かつ、外部委託先等と合同で実施し、コンティンジェンシープランの実効性に係る検証を行っているか。
④　会社を取り巻く環境の変化や組織の変更、要員の異動等をコンティンジェンシープランに反映させるよう、適宜、必要な見直しを図っているか。	⑥　会社を取り巻く環境の変化や組織の変更、要員の異動等をコンティンジェンシープランに反映させるとともに他の金融商品取引業者など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、適宜、必要な見直しを図っているか。
（新設）	⑦　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。
⑤・⑥　（略）	⑧・⑨　（略）
⑺　外部委託管理	⑺　外部委託管理
①・②　（略）	①・②　（略）

（別紙2）

金融商品取引業者等検査マニュアル　新旧対照表

現　　行	改　正　後
③　委託先との契約 　業務委託を行うことによるリスクを認識し、契約において機密保持、再委託条項、監査権限、サービスレベル及び紛争解決方法等を明確に定めているか。	③　委託先との契約 　業務委託を行うことによるリスクを認識し、契約において、委託先との役割・責任分担、機密保持、再委託条項、監査権限、サービスレベル及び紛争解決方法等を明確に定めているか。また、委託先が遵守すべきルールやセキュリティ要件を委託先へ提示し、契約書等に明記しているか。
④　委託業務の管理 イ　委託先における事故、不正等の防止及び機密保持等の対策の実施状況を会社として把握し、必要な措置を講じているか。	④　委託業務の管理 イ　委託先（委託先から委託（二以上の段階にわたる委託を含む。）を受けた者を含む。ロにおいて同じ。）における事故、不正等の防止及び機密保持等の対策の実施状況を会社として把握し、必要な措置を講じているか。
（新設）	ロ　外部委託した業務について、委託先におい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、委託先における顧客データ等の運用状況を監視、追跡できる態勢となっているか。
ロ・ハ　（略）	ハ・ニ　（略）