コメントの概要及びコメントに対する証券監視委の考え方

（別紙１）

番号	関係箇所		コメントの概要	コメントに対する考え方
Ⅱ－１－２　態勢編・第一種金融商品取引業者				
1	５．システムリスク管理態勢	(2)-②	②の文中に、「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。」とあるが、システムリスク管理方針とは別個に情報セキュリティポリシー及び外部委託管理方針を定めることは可能か確認したい。	システムリスク管理の方針と、情報セキュリティポリシーや外部委託管理方針との関係性が明確にされていれば、情報セキュリティポリシーや外部委託管理方針を別個に定めることを妨げるものではありません。
2	５．システムリスク管理態勢	(3)－①-イ	「種類や所在を具体的に記載した規程が制定され」とありますが、制定されているものの名称が「規程」であるかどうかにかかわらず、管理すべき情報資産の種類とその所在が実質的に明示的に定められていればよいと理解しておりますが、それでよろしいでしょうか。	そのようなご理解で結構です。
3	５．システムリスク管理態勢	(3)－①-イ	「種類や所在を具体的に記載した規程」と明示されているが、これは情報資産の種類や所在を具体的に記載した規程を作成していなければならないということを意味しているのか。それとも規定（ルール）や運営上で当該事項について盛り込まれた台帳等を作成していることで、当該項目は対応していると判断してよいか。	「種類や所在を具体的に記載した規程」は、情報資産として認識し、棚卸の対象とすべき情報の種類や所在の大枠が記載されていることを想定しています。 したがって、情報資産の棚卸の結果、「規程」が全く想定していなかった新たな「情報資産」が認識されたような場合には、規程の改正等を行う必要があると考えられます。 また、情報資産の棚卸の結果について、例えば「棚卸結果報告書」や「情報資産台帳」等を用いて、「規程」とは別個に管理することを妨げるものではありません。
4	５．システムリスク管理態勢	(3)－①-イ	イの文中に「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。」とあるが、「種類や所在を具体的に記載した規程」とは情報資産の棚卸の結果を規程に含めるということを意味するのか確認したい。また、情報資産の明確化という観点からは棚卸の結果を規程とは別途管理することは可能なのか確認したい。	
5	５．システムリスク管	(3)－①-ニ	情報セキュリティに係る研修について、全職員のみならず外部委託先等の業務従事者に対して行うことが求められていますす	研修は必ずしも自社で直接実施する必要はありませんが、内容については、一般的な情報セキュリティに係る研修だけでな

	理態勢		が、これは委託元の金融商品取引業者が直接外部委託先への研修を行うことを求めるものではないと理解しておりますが、それでよろしいでしょうか。外部委託先が情報セキュリティに係る十分な研修を行っていることを確認できていればよいでしょうか。	く、自社の情報セキュリティに係る社内規程・規則や管理手続き等の周知徹底を図ることが必要であると考えられます。
6	５．システムリスク管理態勢	(3)－①－ニ	外部委託先等の業務従事者に対する考え方についてお聞きしたい。「全役職員及び外部委託先等の業務従業者」となっているが、外部委託業者等の業務従事者に対しても弊社従業員と同列の扱いとしなければならないのか。「外部委託先等の業務従事者」を全役職員と同列に扱った場合、その範囲やそれらの特定、実際の研修実行者等、運用上の課題が多いかと思われる。「外部委託先等の業務従事者」に関しては、外部委託先による情報セキュリティに関する研修についてのアンケートや直接ヒアリング等を行うことで当該項目は対応していると判断してよいか。	外部委託先の業務従事者に対する扱いについては、情報セキュリティ管理の対象となる情報資産を業務上取り扱う業務従事者に関しては、自社従業員であるか否かを問わず、業務上必要な社内規程・規則や管理手続等を、自社の責任において周知徹底する必要があると考えられますが、その周知徹底すべき範囲やその実施方法は、自社従業員の場合と異なるケースが多く、必ずしも自社従業員と同列の扱いとすることまでを求めている訳ではありません。例えば、研修の実施に当たって、契約等に基づき予め内容を定め、外部委託先に研修の実施を依頼し、事後に報告を受けるなどの方法を採用することを否定するものではありません。 外部委託先による研修内容をアンケートやヒアリングで確認する場合は、外部委託先の業務従事者の担当業務や対象となる情報資産に係る情報セキュリティリスクに応じた適切な内容が対象者全員に研修されていることを、確認する必要があると考えられます。
7	５．システムリスク管理態勢	(3)－①－ホ	ホの文中に「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。」とあるが、当該点検について最低限推奨される期間（週次、月次等）はあるか確認したい。	不正アクセスや情報漏えいの有無等に係る点検の頻度は、点検の対象となる情報資産を有するシステム等の重要性や当該システム等がさらされているリスクによって異なるものと考えられることから、一律に例示することは困難であり、「当該点検について最低限推奨される期間（週次、月次等）」は、個別に判断されるべきものと考えられます。

8	５．システムリスク管理態勢	(7)	（注２）として、「「外部委託管理」には、契約の形態や種類を問わず、金融商品取引業者が他の者にシステムリスクを認識すべきシステムに係る企画・開発・運用等の全部又は一部を行わせることを内容とする契約の一切を含む（明示的な契約が締結されていない場合も含む。）」とあるが、当該外部委託管理にはパッケージ開発されたソフトウエアの買い取りも含まれるのか確認したい。	一般的には、「外部委託管理」に「パッケージ開発されたソフトウェアの買取り」は含まれず、当該行為は、既に製品化されたソフトウェアの購入及び導入・運用行為として、５．⑶の「安全対策の整備」の項目により検証することとなります。ただし、当該ソフトウェアの運用・保守業務を開発元のソフトウェア会社等に委託する場合は、「外部委託管理」の対象となると考えられます。
9	５．システムリスク管理態勢	(7)	従来、「外部委託先管理」とあった文言を「外部委託管理」へと変更した趣旨は何か。	「金融商品取引業者等向けの総合的な監督指針　Ⅲ－二－八　システムリスク管理態勢」の項目名と統一するためです。
10	５．システムリスク管理態勢	(7)	（注２）により、「外部委託管理」の意義が明記されており、本文の末尾が「・・・契約の一切を含む」となっているところからすると、これは「外部委託」の定義であるように読める。「外部委託管理」の定義とするならば、文末を「・・・契約の一切に対する管理を含む」とするか、または文頭において「『外部委託管理』の対象には」としたほうが趣旨が伝わりやすいと考える。	ご意見を踏まえ、記載を修正いたします。
11	５．システムリスク管理態勢	(7)	外部委託については、当該箇所のほか、Ⅱ-1-1態勢編・共通項目　３．内部管理態勢　(10)外部委託業務の管理にも規程があるが、当該箇所のような外部委託管理の対象となる業務の考え方に関する注記はない。この箇所がより広い範囲における外部委託業務の管理を求めるものであることからすれば、「外部委託業務」の趣旨を明確にするために、この箇所においても当該注記と同様の手当てがなされるべきと考える。	当該箇所は、システムの分野において、昨今、ＡＳＰ（アプリケーション・サービス・プロバイダー）業者を利用する金融商品取引業者が増加するなど、外部委託に関し、その契約形態、種類が多様化してきていることを踏まえ、特にその範囲を明確にする必要があったことから、注書きを追加したものであり、他の箇所については特に注記の必要はないと考えます。
12	５．システムリスク管理態勢	(7)	「システムリスクを認識すべき」であるほどの重要なシステムにかかる業務を外部に委託する際は、明示的な契約を締結するのが通常であると思われたが、「明示的な契約が締結されて	具体的な契約形態を想定しているものではありませんが、外部委託に関し、昨今、その契約形態、種類が多様化してきていることに鑑み、そのような場合が生じる可能性を考慮して記載

			いない場合」というのは、具体的にどのような契約形態を想定しているか示していただきたい。	しております。
13	５．システムリスク管理態勢	(7)	同項目の③においては「・・・、契約において～明確に定められているか。」とあるが、この記述に則して考えると、今後「明示的な契約が締結されていない場合」は外部委託の管理のあり方として、許容されないということを意図しているという理解でよいか。	当該箇所には、「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。」と記載していますが、あくまで明示的な契約が締結されている場合の確認項目を例示したものであり、明示的な契約が締結されていないことのみをもって、外部委託管理のあり方として許容されないという趣旨ではありません。
14	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	注書き	注1及び注2によれば、新8.「大規模かつ…リスク管理態勢等」の適用対象となりうるのは、いわゆる外資系の場合には「外国持株会社等グループ」の日本拠点の証券会社であり、海外の親会社ないし経営管理会社ではないという理解でよいか。	「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」に記載の項目は、国際的に活動する外国持株会社等グループの日本拠点である証券会社のうち、相当程度の人員、資産規模を有し、日本国内で幅広い業務を展開しているものの検査において、日本拠点に係るリスク管理態勢の検証を行う際の確認項目であり、検査対象先は当該日本拠点ということになります。 ただし、（注２）に記載しているとおり、日本拠点に係るリスク管理方針の策定や管理態勢の整備が、最終的には国外のグループ本部等において行われている場合については、それが日本拠点におけるリスク・プロファイル等に応じた適切なものとなっているか、日本拠点においても適切な態勢が整備され、十分な関与が行われているか、といった観点から、検証を行うこととしています。
15	８．大規模かつ複雑な業務をグループ一体と	注書き	川下連結と川上連結の相違について周知を徹底し、規制・検査の重複を排除する観点から川上連結を適用しない旨を当局が判断した外資系グループの日本拠点については、趣旨を踏まえてリスク・ベースの検査を徹底すべきである。	貴重なご意見として参考にさせていただきます。 なお、（注２）に記載しているとおり、いわゆる外資系証券会社については、「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」に記載の確

	して行う証券会社グループのリスク管理態勢等			認項目は、相当程度の人員、資産規模を有し、日本国内で幅広い業務を展開しているもの、を対象とすることとしています。
16	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	注書き	Ⅱ-1-2-8.に記載されている確認項目は、注1では当面国内系の「特別金融商品取引業者」のみに対象を限るとしつつ、注2では「上記に加え、国際的に活動する外国持株会社等グループの日本拠点である証券会社のうち、相当程度の人員、資産規模を有し、日本国内で幅広い業務を展開しているもの」については、「日本拠点に係るリスク管理態勢の検証」を行う際にも用いるものとしているが、注2では、注1で除外されている外国持株会社等グループに属する特別金融商品取引業者のみを対象として想定しているという理解でよいか。	（注２）の趣旨は、いわゆる外資系証券会社については、Ⅱ－１－２　８．の確認項目の対象は、日本国内で相当程度の人員、資産規模を有し、幅広い業務を展開しているものとするというもので、特別金融商品取引業者のみを対象として想定している訳ではありません。
17	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	注書き	注2によれば、国際的に活動する外国持株会社等グループの日本拠点である証券会社のうち、相当程度の人員、資産規模を有し、日本国内で幅広い業務を展開しているものの検査においては、日本拠点に係るリスク管理態勢の検証を行う際にも、「以下の確認項目を用いるものとする」としているが、ここでいう「以下の確認項目」とは、本来日本に本店がある大規模証券会社グループの検証のための項目であって、外国持株会社等グループの日本拠点である証券会社における態勢検証にあてはめて用いるには無理がある項目が多い。「以下の確認項目を用いる」のを原則とすると、適用できない理由について過大な説明責任が生じ、被検査会社の負担が過大となるおそれがあるため、これを「以下の確認項目を参考とするものとする」などの表現に変更していただきたい。	（注２）において、「機械的、画一的な検証に陥らないよう検査対象業者における実態を把握した上で、十分な意見交換を行うこととする。」と記載しているとおり、実際の検査においては、ご質問の趣旨に十分留意して検証を行うこととしているところであり、原文のとおりとさせていただきます。
18	８．大規模	(1)-	「外国持株会社等グループ」の場合、経営管理会社において	「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

	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	①、②	定めた方針や内部規程において、すべての項目が網羅的に記載されていることまでを求めるものではなく、日本拠点を含む各地域レベルでの規程等と併せて必要な項目が網羅されているか否かを検査の主眼とする理解でよいか。	会社グループのリスク管理態勢等」の項目は、外国持株会社等グループの日本拠点に関し、実態を把握した上で実効的なリスク管理態勢が整備されているかどうかを検証する際の確認項目を例示したものであり、すべての項目が規程等に網羅的に記載されていることまでを求めるものではありません。
19	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	(1) ～ (7)	「外国持株会社等グループ」の場合、海外経営管理会社によるグローバル管理態勢の中で、日本拠点である証券会社において実効性ある管理が適切に行われていること、及び、当該リスク管理態勢が本邦において要求されるリスク管理レベルに照らして十分であること、の2点が検証の主眼となるということでよいか。	１点目については、そのようなご理解で結構です。２点目については、証券会社グループのリスク管理態勢は、グループの経営戦略や業務内容等に応じて構築されるものであることから、これらの特性に応じた実効的なリスク管理態勢が整備されているかどうかを検証することとなります。
20	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	(5)－①－ロ	「グループの関連会社や外部委託先等が海外に存在する場合の法制度や商慣習等のリスク」について伺い致します。ここで言及されている点は、例えば、海外の関連会社が海外の法令に従ってシステムを構築しておらず、システムが正しく動作しておらず損失が発生するリスク、また、商慣習の違いにより日本の法令が守られず情報漏えいが発生するリスクといったようなシステムリスクと解釈してよろしいでしょうか。	例えば、海外で開発したシステムを国内で使用する場合に、法制度や商慣習の差異を考慮したカスタマイズ等を行わなかったために、業務が適切に履行できないリスク等を想定しています。
Ⅱ－１－５　態勢編・投資運用業者				
21	４．システ	(2)-②	②の文中に、「システムリスク管理の方針には、情報セキュ	システムリスク管理の方針と、情報セキュリティポリシーや

	ムリスク管理態勢		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。」とあるが、システムリスク管理方針とは別個に情報セキュリティポリシー及び外部委託管理方針を定めることは可能か確認したい。	外部委託管理方針との関係性が明確にされていれば、情報セキュリティポリシーや外部委託管理方針を別個に定めることを妨げるものではありません。
22	４．システムリスク管理態勢	⑶－①－イ	イの文中に「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。」とあるが、「種類や所在を具体的に記載した規程」とは情報資産の棚卸の結果を規程に含めるということを意味するのか確認したい。また、情報資産の明確化という観点からは棚卸の結果を規程とは別途管理することは可能か確認したい。	「種類や所在を具体的に記載した規程」は、情報資産として認識し、棚卸の対象とすべき情報の種類や所在の大枠が記載されていることを想定しています。 したがって、情報資産の棚卸の結果、「規程」が全く想定していなかった新たな「情報資産」が認識されたような場合には、規程の改正等を行う必要があると考えられます。 また、情報資産の棚卸の結果について、例えば「棚卸結果報告書」や「情報資産台帳」等を用いて、「規程」とは別個に管理することを妨げるものではありません。
23	４．システムリスク管理態勢	⑶－①－ホ	ホの文中に「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。」とあるが、当該点検について最低限推奨される期間（週次、月次等）はあるのか確認したい。	不正アクセスや情報漏えいの有無等に係る点検の頻度は、点検の対象となる情報資産を有するシステム等の重要性や当該システム等がさらされているリスクによって異なるものと考えられることから、一律に例示することは困難であり、「当該点検について最低限推奨される期間（週次、月次等）」は、個別に判断されるべきものと考えられます。
Ⅱ－２－２　業務編・第一種金融商品取引業者				
24	５．デリバティブ営業等	⑶－①	「デリバティブ商品等を販売する場合や中途解約及び解約清算する場合には」とありますが、法令諸規則・監督指針においては、リスクなどの説明をする書面の交付は販売時に行うことが求められているのみであり、中途解約時や解約清算の場合には求められていないと認識しております。この点は、「デリバティブ商品等を販売する場合には」に修正していただきたい。	ご意見を踏まえ、Ⅱ－２－２　５．⑶については、趣旨を明確にするために、構成も含め記載を修正いたします。 ご質問の点については、別紙２「新旧対照表」新Ⅱ－２－２５．⑶③をご参照下さい（別紙２「新旧対照表」新Ⅱ－２－２５．⑶①については、改正前マニュアルを変更しないこととしました。）。

			同様に、「中途解約及び解約清算」に当たって、必要に応じて説明を受けた旨の確認が求められていますが、法令諸規則・監督指針においては、この点も販売時に求められているものであり、「中途解約及び解約清算」は削除していただきたい。	
25	５．デリバティブ営業等	⑶-①	デリバティブ取引に関して、その商品内容やリスクについて、取引の概要や取引に係る損失の危険に関する事項その他顧客の注意を喚起すべき事項を記載した書面を交付するなどの方法により、十分に説明する場合として、「中途解約及び解約清算する場合」には、その商品内容やリスクについて改めて説明することは不要ではないか。「金融商品取引業者等向けの総合的な監督指針」及び日本証券業協会の「協会員の投資勧誘、顧客管理等に関する規則」でも中途解約及び解約清算する場合の、商品内容やリスクについての説明は求められていない。そもそも、中途解約及び解約清算をした場合、契約が終了しリスクがなくなるので、説明は不要と考えられるため。	
26	５．デリバティブ営業等	⑶-①	中途解約及び解約清算について顧客と取引する場合には、その時点での実際の価格を提示することが一般的であり、最悪シナリオを提示することが必ずしも実態に沿わないと考えられる。監督指針では販売時のみを想定していると認識しており、監督指針と平仄をあわせていただきたい。 明確化のため。	

27	５．デリバティブ営業等	⑶-①	デリバティブ商品等を販売する場合のみでなく、中途解約及び解約清算する場合についても、その商品内容やリスクについて十分な説明を行い、また説明を受けた旨の確認を行うよう規定されているが、法令や自主規制ルールにおいても、中途解約及び解約清算の場合については規制されているものではないことから、削除いただきたい。	
28	５．デリバティブ営業等	⑶-①	「特に顧客自身がリスクを負っている商品の販売、中途解約及び解約清算に当たっては、必要に応じて取引先から説明を受けた旨の確認を行っているか。」とあるが、顧客が商品のリスク特性を理解すべき時点は、商品の販売時であり、「中途解約及び解約清算」の追加改正は不要と考える。	
29	５．デリバティブ営業等	⑶-①	日本証券業協会の協会規則では、市場デリバティブ取引及び金商業府令 116 条 1 項 3 号イ又はロに規定する取引に関してシナリオに基づく想定最大損失額を説明する対象から除外されている。上記取引は当マニュアルに記載のデリバティブ取引の中から除外されるということでよいか。	そのようなご理解で結構です。 なお、ご質問の点については、別紙２「新旧対照表」新Ⅱ－２－２　５．⑶③をご参照下さい（別紙２「新旧対照表」新Ⅱ－２－２　５．⑶①については、改正前マニュアルを変更しないこととしました。）。
30	５．デリバティブ営業等	⑶-①	「見込額」との表記を削除していただきたい。 「見込額」の内容が明確でないことから、監督指針と平仄をあわせていただきたい。	ご意見を踏まえ、記載を修正いたします。

31	５．デリバティブ営業等	⑶-③	日本証券業協会の協会規則では、金商業府令 116 条 1 項 3 号イ又はロに規定する取引に関して確認書の徴求が必要な取引から除外されている。上記取引は当マニュアルに記載の店頭デリバティブ取引の中からは除外されるということでよいか。	そのようなご理解で結構です。