コメントの概要及びコメントに対する金融庁の考え方

No.	該当箇所	コメントの概要	金融庁の考え方
1	全般	セキュリティ対策とユーザーの利便性は反比例するため企業任せでは進まない。行政による一律で強い指導に期待する。	行政による強い指導については、貴重なご意見として承ります。 しかしながら、セキュリティ対策については、個々の金融機関が行う業務に応じて異なるため、一律に指導を行うことはなじまないと考えます。個々の金融機関の業務やリスクに応じて、顧客の利便性も踏まえた対策が実施されるよう促してまいります。
2	「金融商品取引業者等向けの総合的な監督指針」 Ⅲ-2-8(1) 柱書	システムリスク管理態勢の検証は、「Ⅲ－２－８（１）主な着眼点」の柱書にあるとおり「金融商品取引業者の業容に応じて」なされるものであり、改正案で記載されている項目全てを満たすことが求められているわけではないことを、改めて確認したい。 例えばWEBにて顧客としての固有情報の管理ができるような、いわゆるネットバンキングやネット証券のアカウントがある場合における管理と、WEBを単なる情報提供のツールとして利用している場合とでは、一律な対応が求められるべきではないものと考える。	情報セキュリティ管理及びサイバーセキュリティ管理でお示ししているそれぞれの着眼点については、取り扱う業務のリスクに見合った態勢整備や対策を講じる必要があると考えます。 なお、それぞれの着眼点で「例えば」と記載されているような具体的な対策例については、例示に限定されるものではなく、例示以外の方法も含め検討し、適切な対策を講じる必要があります。

No.	該当箇所	コメントの概要	金融庁の考え方
3	事務ガイドライン（第三分冊：５　前払式支払手段発行者関係） Ⅱ-3-1-1 (1)②	サイバー攻撃はインターネット環境が益々広がる昨今、様々な手段にて実行され、インターネット上では常態化していると考えられるため、サイバーセキュリティ事案を以下のように定義できないか。 「サイバーセキュリティ事案とは、・・・(改正案と同じため中略)・・・、いわゆる「サイバー攻撃」により、サイバーセキュリティが著しく脅かされる事案をいう。」	サイバーセキュリティ事案の定義は、政府の「サイバーセキュリティ戦略」を参考としています。 サイバーセキュリティ事案については、業界への影響拡大を防止するためにも初動が重要であることから、 著しく影響を及ぼすような重大事態に至らない場合であっても、業務に影響がある場合や攻撃予告等、侵害の影響がでていない場合も報告が必要と考えます。 したがって、サイバーセキュリティ事案の本指針における定義については、原案どおりとします。 なお、検査マニュアルにおいても同様の意見をいただきましたが、同様の回答となります。
4	事務ガイドライン（第三分冊：５　前払式支払手段発行者関係） Ⅱ-3-1-1 (1)②	「サイバー空間」や「サイバーセキュリティ」について、その範囲が明確でないため、想定の内容を、ガイドライン内に例示できないか。	サイバーセキュリティ事案の定義は、政府の「サイバーセキュリティ戦略」を参考としています。 また、「サイバー空間」や「サイバーセキュリティ」は、情報通信技術の進歩に伴って変化が生じることが考えられます。 したがって、具体的な例示については差し控えます。
5	「主要行等向けの総合的な監督指針」 Ⅲ-3-7-1-2 (2)③	今回の改正案では「体制」が「態勢」に変更されているが、管理体制と管理態勢は両方必要であるため、「管理体制・管理態勢」に表現を変更いただきたい。金融庁の行政処分の基準に、組織性の有無という項目があるように監督指針に「体制」が必要と考える。	ご指摘の改正（体制→態勢）を行っているのは、主要行等向けの総合的な監督指針のみですが、これは他の指針では既に態勢となっていることから平仄をとるために修正したものとなります。 なお、組織体制の整備は、管理態勢が機能するための一つの施策であると考えられ、態勢整備の一環であると考えます。 したがって、原案どおりとします。

No.	該当箇所	コメントの概要	金融庁の考え方
6	「主要行等向けの総合的な監督指針」 Ⅲ-3-7-1-2 (4)	現行の監督指針（４）安全対策の「①安全対策の基本方針が策定されているか。」、「②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。」が削除され、（４）情報セキュリティ管理②に「情報の・・・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。」が追加されている。 現行の監督指針にある、安全管理者と管理体制、及びデータ管理者とデータ管理態勢は、システム障害に対する管理者、管理態勢であるため、削除は不要ではないか。 また、現行の監督指針（４）安全対策①、②は、以下のように変更していただきたい。 ①安全対策の基本方針が策定、公表されているか。 ②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。管理体制を公表しているか。	各管理者と管理体制については、現行の監督指針に記載していた安全管理者やデータ管理者にとどまらないため、改正案では、関係する記載箇所を集約し、金融検査マニュアルと平仄をとる形で「情報セキュリティ管理」として再編したものです。システムリスクに係る各管理者の役割や体制整備は、金融検査マニュアルのオペレーショナル・リスク管理態勢の確認検査用チェックリスト（別紙２）において検証項目として記載されているところです。 安全対策の基本方針や安全管理体制の公表については、個々の金融機関の経営判断によるものと考えられ、監督指針において規定することは馴染まないものと考えます。 したがって、原案どおりとします。 なお、検査マニュアルについても関連の意見をいただきましたが、同様の回答となります。

No.	該当箇所	コメントの概要	金融庁の考え方
7	「主要行等向けの総合的な監督指針」 Ⅲ-3-7-1-2 (4)③	現行の着眼点の記載は、金融機関が預金者に対して、保護を行っているかという観点と考えるが、改正案の「③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。」では、対策の対象が金融機関のシステムなのか、利用者の端末なのか分からないため、利用者保護の観点から現行の着眼点の記載のままでよいのではないか。	不正使用等の対策は、「銀行以外の者が占有管理する端末機器」に留まらないため限定的な記載を改めたものとなります。 したがって、原案どおりとします。
8	「金融検査ﾏﾆｭｱﾙ」 顧客保護等管理態勢の確認検査用ﾁｪｯｸﾘｽﾄ Ⅱ-3 (2)③	「顧客の重要情報へのアクセスについて、管理者と担当者の分離等」とは具体的にはどのようなことを指すのか。 このような場合、よく複数名での作業の義務化を対応策とする場合が多いが、管理者と担当者との関係は担当者の作業を管理者が検証するというイメージが通常であり、相互牽制となれば担当者とは職務が異なる管理者が検証しなければならないと思われるが、そのような理解でもよいか。	顧客情報統括管理責任者は、顧客の重要情報が不正に取得・利用されることのないよう適切な措置を講じる必要があると考えます。 具体的には、顧客の重要情報にアクセスする必要がある場合、管理者を含め各担当者の職務と役割を明確にするとともに、権限の分散を図り、相互牽制が働く体制を構築する必要があると考えます。

No.	該当箇所	コメントの概要	金融庁の考え方
9	「金融検査ﾏﾆｭｱﾙ」 顧客保護等管理態勢の 確認検査用ﾁｪｯｸﾘｽﾄ Ⅱ-3 (2)③および ｵﾍﾟﾚｰｼｮﾅﾙ･ﾘｽｸ管理 態勢の確認検査用 ﾁｪｯｸﾘｽﾄ（別紙２） Ⅲ-1 (2)	顧客保護等管理態勢の確認検査用チェックリストにおいて、「顧客の重要情報」についての着眼点が追加されている。 併せて、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においても、「顧客の重要情報」の洗い出しについて着眼点が追加されているが、これら「顧客の重要情報」は同一のものという理解で良いか。 また、「顧客の重要情報」とは具体的にどのようなものなのか。	ご認識のとおり、「顧客保護管理態勢の確認検査用チェックリスト」の顧客情報管理態勢における「顧客の重要情報」と「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」の情報セキュリティ管理における「顧客の重要情報」は同じ内容のものです。 なお、金融機関が責任を負うべき顧客の重要情報については、例えば、個人情報、認証情報、電子的価値情報等が考えられますが、個々の金融機関が業務やリスクに応じて適切に定義を行う必要があると考えます。一般的には、各社のセキュリティポリシーにおいて規定されているものと考えます。 （参考）公益財団法人金融情報システムセンター（FISC）の「金融機関等におけるセキュリティポリシー策定のための手引書」
10	「貸金業者向けの総合 的な監督指針」 Ⅱ-2-4 (1)④二	「重要情報」に関する概念、考え方など具体的にはどういったものを想定しているかご教示願いたい。 監督指針では、事業者の規模・特性を考慮した管理を求めているものの、新たな「重要情報」という表現の内容に関する各社判断・考え方を整理するにあたっては、具体的な例示などを参考としたいため。	金融機関が責任を負うべき顧客の重要情報については、個々の金融機関が業務やリスクに応じて適切に定義を行う必要があると考えます。 一般的には、各社のセキュリティポリシーにおいて規定されているものと考えます。 （参考）公益財団法人金融情報システムセンター（FISC）の「金融機関等におけるセキュリティポリシー策定のための手引書」

No.	該当箇所	コメントの概要	金融庁の考え方
11	「貸金業者向けの総合的な監督指針」 Ⅱ-2-4 (1)④ニ	「業務、システム、外部委託先を対象範囲とし」とあるが、本件はあくまでシステム管理に関連する重要情報の範囲であるという理解でよいか。 業務で取り扱う重要情報や外部委託先で取り扱う重要情報でシステムが関連しない情報の管理態勢は、監督指針の「Ⅱ-2-2 顧客等に関する情報管理態勢」「Ⅱ-2-3 外部委託」に記載済みであるため念のため確認するもの。	重要情報を適切に管理する上では、重要情報を網羅的に洗い出し、把握することが必要と考えます。 そのため、重要情報の洗い出しに際しては、システムの観点からの洗い出しにとどまらず、業務や外部委託先といった観点からも漏れのないように、網羅的に洗い出し、把握する必要があります。 （参考）公益財団法人金融情報システムセンター(FISC)の「金融機関等におけるセキュリティポリシー策定のための手引書」にも記載されているとおり、情報セキュリティ管理の対象である「情報資産」は、「情報」と「情報システム」から成り、「情報」には、コンピュータシステムや記録媒体等に保存されているデータのみならず、紙に印刷されたものやコンピュータシステムに入力される前のメモ等も含まれます。
12	「金融商品取引業者等向けの総合的な監督指針」 Ⅲ-2-8 (1)④ニ	「重要情報の洗い出し」に関して、アプリケーションサービスプロバイダ[※以降、ASP]（国内／海外）との契約にて取引システムを提供している場合は、ASP 側にて機密情報（ID・パスワード）をデータベースに保管されている事以外（システム領域やバックアップ領域、等）の洗い出しが困難である為、ASP システム内に対象情報が存在し、重要度および影響度の整理を行うことでリスク管理（セキュリティ）としての要件を満たすという理解でよいか。	金融機関が責任を負うべき顧客の重要情報については、ASP サービス等の外部委託先を利用する場合においても漏れのないように、網羅的に洗い出し、把握する必要があると考えます。 ご認識のとおり、ASP システム内に存在する顧客の重要情報について、重要度および影響度の整理を行うことはもとより、適切な管理が行われていることを定期的に確認する必要があると考えます。

No.	該当箇所	コメントの概要	金融庁の考え方
13	事務ガイドライン（第三分冊：５　前払式支払手段発行者関係） Ⅱ-3-1-1 (4)④	「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」とは、具体的にどのようなデータを指すのか。	重要情報の洗い出しでは、業務プログラム等で呼び出されるデータベース内の情報のみを対象にするだけではなく、例えば、OSが取得しているシステムログやメモリ領域等の一次的に保管されるデータ等も含め、洗い出す必要があると考えます。
14	事務ガイドライン（第三分冊：５　前払式支払手段発行者関係） Ⅱ-3-1-1 (4)④、⑤、⑥および (5)③、④、⑦、⑧	「例えば」「以下のような」との記述があるが、こちらは規模・特性に応じた適切な対策を講じればよいという理解でよいか。 また、ガイドラインは一つの例示という認識でよいか。	情報セキュリティ管理及びサイバーセキュリティ管理でお示ししているそれぞれの着眼点については、取り扱う業務のリスクに見合った態勢整備や対策を講じる必要があると考えます。 なお、それぞれの着眼点で「例えば」と記載されているような具体的な対策例については、例示に限定されるものではなく、例示以外の方法も含め検討し、適切な対策を講じる必要があります。
15	「金融商品取引業者等向けの総合的な監督指針」 Ⅲ-2-8 (1)④へ	「アクセス記録についての検証」とあるが、アクセスコントロール表で定義されたアカウント権限を無視したアクセス（アクセス権限エラー）の記録を分析することで不正アクセス防止行動を満たすという理解でよいか。	検証に際しては、アクセス権限エラーの分析のみに留まらず、正常アクセスであっても通常とは異なる挙動（アクセス時間帯や短期間における大量アクセス等）を検出することも有効と考えられます。
16	「中小・地域金融機関向けの総合的な監督指針」 Ⅱ-3-4-1-2 (4)⑩	「（外部委託先におけるセキュリティ教育を含む）」とあるが、その対象範囲は「外部委託している業務に直接的に関与している役職員」との理解で良いか。	ご認識のとおりです。

No.	該当箇所	コメントの概要	金融庁の考え方
17	「金融商品取引業者等向けの総合的な監督指針」 Ⅲ-2-8 (1)④ヌ	外部委託先の役職員に対するセキュリティ教育の実施については、必ずしも金融商品取引業者が直接的に行うものに限られず、国内外を問わず各委託先において情報セキュリティに係る研修等を実施することも含まれるとの理解でよいか。	ご認識のとおり、着眼点としてセキュリティ教育を実施する対象範囲を示しているものであり、セキュリティ教育の実施者までを限定するものではありません。 外部委託の形態や階層によっては、委託先においてセキュリティ教育が適切に実施されていることを委託元として確認するという方法も考えられます。 なお、他の監督指針・検査マニュアル等についても同様の意見をいただきましたが、同様の回答となります。
18	「金融商品取引業者等向けの総合的な監督指針」 Ⅲ-2-8 (1)⑤ロ	サイバーセキュリティ管理態勢の整備に関する項目として、「サイバー攻撃に対する監視体制」、「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」が挙げられているが、投資運用業者や投資助言・代理業者の対策としては過剰と考える。 柱書を「・・・ほか、例えば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。」などの文言修正が望ましいと考える。	サイバーセキュリティ事案については、業界への影響拡大を防止するためにも初動が重要であることから、監視体制や緊急時対応及び早期警戒のための体制の整備が重要と認識しています。 なお、業態によっては、これらを単独で設けることが困難である場合も考えられますので、その場合は、外部委託や共同で整備する等の工夫も考えられます。 したがって、原案どおりとします。

No.	該当箇所	コメントの概要	金融庁の考え方
19	事務ガイドライン（第三分冊：５　前払式支払手段発行者関係） Ⅱ-3-1-1 (5)②	「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」について、関係会社でそのような組織が備わっている若しくは自社において独立した組織でなくても機能が備わっておれば足りるという理解でよいか。	ご認識のとおりです。 「組織内 CSIRT 等の緊急時対応及び早期警戒のための体制」の整備は、態勢整備の一例であり、物理的な組織体制や組織名称に係らず同等以上の機能が備わった態勢を整備していただくことが必要と考えます。 なお、関係会社で機能を有している場合は、自社で機能を備えている場合と同様の機能の提供が受けられる必要があると考えます。
20	「貸金業者向けの総合的な監督指針」 Ⅱ-2-4 (1)⑤ロ	「情報共有機関等」とは、具体的にどのような機関を想定しているのか。	例えば、金融セプター（※）や業界団体、IPA、JPCERT のほか、金融 ISAC、日本シーサート協議会などが考えられます。 なお、他の監督指針等についても同様の意見をいただきましたが、同様の回答となります。 ※重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。(「重要インフラの情報セキュリティ対策に係る第３次行動計画」（平成 26 年５月 19 日情報セキュリティ政策会議))

No.	該当箇所	コメントの概要	金融庁の考え方
21	事務ガイドライン（第三分冊：５　前払式支払手段発行者関係） Ⅱ-3-1-1 (5)③	「サイバー攻撃に備え、入口・内部・出口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。」とあるが、多層防御は侵入から情報漏えい・破壊までの活動に限定されるため、以下の内容としてはどうか。 「サイバー攻撃に備え、入口・内部・出口において、サイバーセキュリティ対策を適切に講じているか。」	多層防御は、情報通信技術を利用した対策だけでなく、物理的な対策や人的な対策を含めた防御戦略を指すものと考えています。 不正侵入等の早期検知や情報漏えいや破壊等の被害の拡大を防止するためには、入口、内部、出口の各段階において、それぞれ適切な対策を講じ、それらを組み合わせた多層防御を講じることが有効であると考えます。 したがって、原案どおりとします。
22	「中小・地域金融機関向けの総合的な監督指針」 Ⅱ-3-4-1-2 (5)④	「DDoS 攻撃に対して自動的にアクセスを分散させる機能」は、具体的にどのような機能を想定しているのか。	特定の方法を求めるものではありませんが、例えば、ミラーサイト等を活用して経路分散を行う方法等が考えられます。 なお、他の監督指針・検査マニュアル等についても同様の意見をいただきましたが、同様の回答となります。
23	「金融検査ﾏﾆｭｱﾙ」 ｵﾍﾟﾚｰｼｮﾅﾙ･ﾘｽｸ管理態勢の確認検査用 ﾁｪｯｸﾘｽﾄ（別紙２） Ⅲ-2 (1)（ⅱ）	「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」の３つが挙げられているが、これらは例示であり、これら全ての措置を講じなければならないわけではないという理解でよいか。	ご認識のとおり、具体的な対策例については、例示ですが、例示以外の適切な方法も含め、提供する業務に応じてサイバー攻撃を受けた場合の被害の拡大を防止するための適切な対策を講じる必要があります。 なお、他の監督指針等についても同様の意見をいただきましたが、同様の回答となります。
24	「金融商品取引業者等向けの総合的な監督指針」 Ⅲ-2-8 (1)⑤へ	脆弱性診断サービスを導入する際の推奨レベルや要件等がある場合は教えていただきたい。	ネットワークへの侵入検査や脆弱性診断等を活用する場合には、個々の金融機関が取り扱う業務やリスクに応じて適切に診断項目を定める必要があると考えます。 また、情報通信技術の進展にあわせて、適切な間隔で診断を継続する必要があると考えます。

No.	該当箇所	コメントの概要	金融庁の考え方
25	「金融商品取引業者等向けの総合的な監督指針」 Ⅲ-2-8（1）5ト、チおよび 「保険会社向けの総合的な監督指針」 Ⅱ-3-14-2-2 (5)⑦、⑧	「ト.」に列記された認証方式を導入促進することは、金融業界全体のセキュリティ水準を向上に有用と考える。そのため、ト.の（注）は金商業者等がそれらの認証方式を導入するまでの間の経過的な措置として設けられたもの、という理解でよいか。 インターネットバンキング不正送金事犯の抑止、根絶に向けては、金融業界全体のセキュリティレベルの底上げを図ることが重要であり、過去の犯罪手口も参考に効果的な対策を講じていく必要があると考えられる。 こうしたなか、金商業者等向けの監督指針改正案では、「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」として、３つの対策例が記載されており、その上で、「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」を例に、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、とされている（保険会社向けの監督指針改正案について同じ）。 一方で、顧客が証券会社に開設した証券取引口座から、顧客本人名義の出金先預金口座に対して、本人が意図せず不正に出金され、当該本人名義の預金口座からさらに第三者の預金口座へ不正送金された事例があると聞いている。そのような事例の拡大を防止するためには、まずもって本項の「ト.」に列記された認証方式の導入促進を図ることが有用であると考えるもの。	経過措置として設けたものではありません。 なお、ご指摘のとおり、金融業界全体のセキュリティ水準を向上させることは重要と考えています。 たとえ顧客本人名義の口座あての送金であっても、本人が意図しない不正送金を防止することは顧客保護上重要な課題であることから、金融機関が業務のリスクに見合った適切な認証方式を採用していくよう促してまいります。

No.	該当箇所	コメントの概要	金融庁の考え方
26	「金融商品取引業者等向けの総合的な監督指針」 Ⅲ-2-8（1）5ト、チおよび 「保険会社向けの総合的な監督指針」 Ⅱ-3-14-2-2（5）⑦、⑧	ト．およびその（注）は、金商業者等のサイバーセキュリティ管理に関する監督上の考え方を示したものであり、かかる措置を講じることで「取引のリスクに見合った対応がなされている」としても、金商業者等は、不正アクセスによる顧客口座からの不正出金に遭った当該顧客に対する補償については、真摯な対応が求められるという理解でよいか。 現状、金商業者等については、不正アクセスによる不正な有価証券売買取引や証券取引口座からの不正出金への対応を定める法令や法令解釈はなく、業界団体による具体的な申し合わせはない（保険会社についても同様）と認識している。 そのため、金商業者等が「ト．」またはその注記に記載された措置を講じていた場合に、「取引のリスクに見合った対応がなされている」とされ、加えて、金商業者等向けの監督指針改正案では、不正取引に係る損失補償の言及がないことを以て、顧客への補償は不要とされてしまうことを懸念する。 仮に、本人名義の預金口座への出金であっても、それが不正取引の場合は、出金元金融機関を含む関係金融機関間（金商業者等と振込先金融機関）で、補償の負担主体や負担割合等の顧客対応に関する協議が真摯に行われるべきと考える。	金商業者等の顧客が不正アクセスによる被害を受けた場合には、金商業者等は適切な顧客説明が求められるものと考えます。 なお、ご指摘いただいた点については、貴重なご意見として、参考にさせていただきます。

No.	該当箇所	コメントの概要	金融庁の考え方
27	「金融商品取引業者等向けの総合的な監督指針」 Ⅲ-2-8 (1)⑤チ	監督指針の改正案における不正防止策について、不正防止策によってその導入にあたり相応の時間・期間を必要とし、改正後の監督指針が適用される日時点における導入が難しい場合も考えられることから、その適用について経過措置期間を設けていただきたい。	金融取引における不正防止対策は喫緊の課題であるため、経過措置は設けません。 なお、改正の施行時点においては、未だ対策が講じられていない場合であっても、例えば、業務やリスクに見合った適切な対策に向けた対応計画を策定し、計画を推進しているかどうか等の取組み状況も含めて検証することで金融機関の対応を促してまいります。
28	事務ガイドライン（第三分冊：５　前払式支払手段発行者関係） Ⅱ-3-1-1 (5)⑧	「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」とあるが、前払式支払手段発行者の場合は、無記名式の利用者も多数いるため、連絡を取るのが現実的ではない。 以下のとおりご変更頂きたい。 「不正なログイン・異常な取引等を検知し、連絡可能な利用者に対して速やかに利用者に連絡する体制の整備」	匿名を前提としたサービスが存在することは承知していますが、他方、サービスの利用開始時に連絡先（メールアドレス等）を登録するケースもあることから、そういった場合は、連絡を行うことが可能と考えます。 貴見を踏まえ、次のとおり修正します。 「不正なログイン・異常な取引等を検知し、連絡可能な利用者に対して速やかに連絡する体制の整備」
29	「金融検査ﾏﾆｭｱﾙ」 ｵﾍﾟﾚｰｼｮﾅﾙ･ﾘｽｸ管理態勢の確認検査用ﾁｪｯｸﾘｽﾄ（別紙２） Ⅲ-1(5)（ⅱ）	「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」は、利用者側がやることであるため、ここまで金融機関に求めるのは酷ではないか。	インターネットバンキングに関わる犯罪が急増している現状を踏まえ、金融機関は、利用者利便を確保しつつ、利用者保護の徹底を図る観点から、インターネットバンキングに係るセキュリティ対策を十分に講じる必要があります。また、併せて、顧客に対する情報提供、啓発及び知識の普及を図ることも重要と考えます。 ご指摘いただいた対策についても、全国銀行協会が加盟行間で申し合わせた事項に基づき「インターネット・バンキングにおいて留意すべき事項について」（平成 26 年７月改訂）において例示され、金融機関における取組みが進められているところです。

No.	該当箇所	コメントの概要	金融庁の考え方
30	「金融検査ﾏﾆｭｱﾙ」 ｵﾍﾟﾚｰｼｮﾅﾙ･ﾘｽｸ管理 態勢の確認検査用 ﾁｪｯｸﾘｽﾄ（別紙２） Ⅲ-1 (5)（ⅱ）	「利用者のパソコンのウィルス感染状況を金融機関側で検知し、警告を発するソフトの導入」は、金融機関システム側からは、利用者が正しい動作をしているように「見える」からこそ MITB 等による不正送金が可能なわけであり、根本的には不可能な要求ではないか。	同上
31	「貸金業者向けの総合的な監督指針」 Ⅱ-2-4 (1)⑤リ	「業界横断的な演習に参加」とは、具体的にどのような演習を想定しているのか。	個別金融機関単独の訓練ではなく、業界内の演習や銀行、保険、証券、貸金等の垣根を越えた演習を想定しています。 また、既に NISC が毎年実施している演習のように金融分野以外の重要インフラ事業者との演習も考えられます。 なお、他の監督指針等についても同様の意見をいただきましたが、同様の回答となります。
32	「金融商品取引業者等向けの総合的な監督指針」 Ⅲ-2-8 (1)⑥へ	「具体的な計画」とは、【入社３ヶ月間は OJT による直接指導を行い、以降は現行システムの一部専門分野における担当として業務経験を担い、日々および月次のルーティン作業を他要員と共同にて実施する事で他分野における業務知識も習得する】といった計画内容でも十分との理解で良いか。	人材育成の手法は、個々の金融機関によって異なるため、一律にお示しすることは差し控えますが、現行システムの仕組み、開発技術の継承、専門性をもった人材の育成という観点で具体的な計画を策定し、実施していくことが必要と考えます。
33	事務ガイドライン（第三分冊：５　前払式支払手段発行者関係） Ⅱ-3-1-1 (8)②	「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。」の「契約書等」は、マニュアル・仕様書等への記載等でも足りると考えてよいか。	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について、委託元と委託先の間で合意することが必要と考えます。そのため、契約書以外にもサービスレベル合意書（SLA）等、契約書に付随する資料等が考えられます。

No.	該当箇所	コメントの概要	金融庁の考え方
34	「主要行等向けの総合的な監督指針」 Ⅲ-3-7-1-2 (8)⑤	現行の監督指針、Ⅲ－３－７－１－２（７）⑤（改正案ではⅢ－３－７－１－２（８）⑤）に、「共同センター等の重要な外部委託先に対して、内部監査部門又はシステム監査人等による監査を実施しているか。」との記載があり、今回の改正対象ではないが、監督指針改正案の趣旨を鑑みれば、外部委託先について、その取り扱う情報の重要性を考慮した管理が求められるものと考える。 そのため、内部監査部門又はシステム監査人等による監査の実施に加えて、公認会計士又は監査法人によるＩＴ委員会実務指針第７号やＳＯＣ２等の保証報告書の利用も記載してはどうか。	いただいたご意見については、今回の改正箇所ではありませんが、外部委託先については、その取り扱う情報の重要性を考慮した管理が求められると考えられることから、貴重なご意見として今後の参考にさせていただきます。
35	「金融商品取引業者等向けの総合的な監督指針」 Ⅲ-2-8 (3)	「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、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。」の、「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」という基準は定義が曖昧であり、軽微なものでも報告が必要であるかは疑問であるため、「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、顧客や業務継続に影響を及ぼす、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。」と変更して頂きたい。	サイバーセキュリティ事案については、業界への影響拡大を防止するためにも初動が重要であることから、業務継続に影響を及ぼすような重大事態に至らない場合であっても、業務に影響がある場合や攻撃予告等、侵害の影響がでていない場合も報告が必要と考えます。 したがって、原案どおりとします。 なお、他の監督指針等についても同様の意見をいただきましたが、同様の回答となります。

No.	該当箇所	コメントの概要	金融庁の考え方
36	事務ガイドライン（第三分冊：５　前払式支払手段発行者関係） Ⅱ-3-1-2 (2)①	「サイバーセキュリティ事案」の当局宛報告は、（注）に記載のあるとおり、前払式支払手段の発行若しくは利用の停止等利用者に対して重大な損害が発生するもののみ報告すれば足りるとの認識で相違ないか。 その認識で相違なければ、「サイバーセキュリティ事案」の定義を以下のように変更できないか。 「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著しく脅かされる事案をいう。」 「サイバーセキュリティ事案」の定義変更が適わない場合、報告基準を以下のように変更できないか。 「財務局が別途通知する前払式支払手段発行者のIC型又はサーバ型前払式支払手段についてコンピュータシステムの障害や、サイバーセキュリティ事案の発生により、利用者や業務に著しい影響を及ぼした場合」	サイバーセキュリティ事案の定義は、政府の「サイバーセキュリティ戦略」を参考としています。 サイバーセキュリティ事案については、業界への影響拡大を防止するためにも初動が大切であることから、著しく影響を及ぼすような重大事態に至らない場合であっても、業務に影響がある場合や攻撃予告等、侵害の影響がでていない場合も報告が必要と考えます。 したがって、サイバーセキュリティ事案の本指針における定義については、原案どおりとします。

No.	該当箇所	コメントの概要	金融庁の考え方
37	事務ガイドライン（第三分冊：５　前払式支払手段発行者関係） Ⅱ-3-1-2 (2)①	「サイバーセキュリティ事案」が、（注）に記載のあるとおり、前払式支払手段の発行若しくは利用の停止等利用者に対して重大な損害が発生するもののみ報告すれば足りるとの認識で相違がないという前提の場合、「障害が発生していない場合」の報告基準は、以下のように変更できないか。 「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、利用者や業務に著しい影響を及ぼす、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。」	重大な損害が発生するものに限り報告を求めるものではありません。 サイバーセキュリティ事案については、業界への影響拡大を防止するためにも初動が大切であることから、著しく影響を及ぼすような重大事態に至らない場合であっても、業務に影響がある場合や攻撃予告等、侵害の影響がでていない場合も報告が必要と考えます。 したがって、原案どおりとします。
38	「主要行等向けの総合的な監督指針」 Ⅲ-3-8-2 (3)	該当の改正案では「インターネット上での暗証番号等の個人情報の詐取の危険性・・・等、様々なリスクの説明や、顧客に求められるセキュリティ対策事例の周知を含めた注意喚起等が顧客に対して十分に行われる態勢が整備されているか。」となっており、顧客にセキュリティ対策を求めています。 利用者保護、利用者保護の観点から、預金者に対しての十分な説明を金融機関は行っているかどうかを監督していただきたい。	インターネットバンキングにおける不正送金事案を低減させるためには、金融機関側におけるシステム対策に留まらず、預金者側の意識とセキュリティ対策の向上が不可欠であると考えます。そのため、金融機関は、預金者に対して十分な説明を行う必要があると考えます。 金融機関に対しては、ご指摘の点も踏まえて監督してまいります。

No.	該当箇所	コメントの概要	金融庁の考え方
39	「主要行等向けの総合的な監督指針」 Ⅲ-3-8-2（3）本文および（参考）	全国銀行協会の申し合わせは、預貯金者保護法を踏まえ作成されたものであり、預貯金者保護法及び全国銀行協会の申し合わせの趣旨を同等に扱うのは不公正なため、本文中、「及び全国銀行協会の申し合わせ」を削除すべきではないか。 また（参考）として記載している「預金等の不正な払戻しへの対応について（平成 20 年２月 19 日：全国銀行協会）」及び「法人向けインターネット・バンキングにおける預金等の不正な払戻しに関する補償の考え方（平成 26 年７月 17 日：全国銀行協会）」を削除して、Ⅲ－３－８－３監督手法・対応の（参考）として記載すべきではないか。	個人及び法人顧客への損失補償の対応については、預貯金者保護法及び全国銀行協会の申し合わせの趣旨を踏まえる必要があるため、原案どおりとします。 なお、検査マニュアルについても同様の意見をいただきましたが、同様の回答となります。