「主要行等向けの総合的な監督指針」等及び「金融検査マニュアル」等の一部改正（案）に対する意見及び金融庁の考え方
【別紙７「貸金業者向けの総合的な監督指針」について】

平成 27 年 4 月 24 日
日本貸金業協会

No.	該当箇所	当協会の意見	金融庁の考え方
1	Ⅱ－2－4 (1)④ニ	「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」
2	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。

「主要行等向けの総合的な監督指針」等及び「金融検査マニュアル」等の一部改正（案）に対する意見及び金融庁の考え方
【別紙７「貸金業者向けの総合的な監督指針」について】

平成 27 年 4 月 24 日
日本貸金業協会

No.	該当箇所	当協会の意見	金融庁の考え方
3	Ⅱ－2－4（1)④ヌ	セキュリティ教育の対象に「(外部委託先におけるセキュリティ教育を含む。)」とあるが、外部委託先については、外部委託先内でのセキュリティ教育の実施状況を確認するなどの代替策も含まれると考えていいか。	(※他の監督指針改正案において同様の意見があったため、当該意見に対する回答の中で回答されております。当該意見及び当該意見に対する金融庁の考え方（下記）をご参照下さい。)
	【各業界共通項目】 「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	【コメントの概要】 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。	【金融庁の考え方】 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。
4	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))

「主要行等向けの総合的な監督指針」等及び「金融検査マニュアル」等の一部改正（案）に対する意見及び金融庁の考え方
【別紙７「貸金業者向けの総合的な監督指針」について】

平成 27 年 4 月 24 日
日本貸金業協会

No.	該当箇所	当協会の意見	金融庁の考え方
5	Ⅱ－2－4　(1)⑤ニ	「DDoS 攻撃に対して自動的にアクセスを分散させる機能」を設ける措置が求められているが、自社が利用するシステムにどのような機能を備えればよいのか具体的にご教示願いたい。	（※他の監督指針改正案において同様の意見があったため、当該意見に対する回答の中で回答されております。当該意見及び当該意見に対する金融庁の考え方（下記）をご参照下さい。）
	【各業界共通項目】 「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	【コメントの概要】 「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。	【金融庁の考え方】 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。
6	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。

（補足）
・IPA（独立行政法人 情報処理推進機構　https://www.ipa.go.jp/　）
・JPCERT（一般社団法人 JPCERT コーディネーションセンター　https://www.jpcert.or.jp/ ）
・金融 ISAC（一般社団法人 金融 ISAC　http://www.f-isac.jp/ ）
・日本シーサート協議会（日本コンピュータセキュリティインシデント対応チーム協議会　http://www.nca.gr.jp/ ）
・NISC（内閣サイバーセキュリティセンター　http://www.nisc.go.jp/ ）