

「主要行等向けの総合的な監督指針」等の一部改正（案）及び「金融分野におけるサイバーセキュリティに関するガイドライン」（案）の公表について」へのコメントの概要及びコメントに対する金融庁の考え方

（別紙1）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	当協会から提出した意見・質問	金融庁の考え方
1	「金融分野におけるサイバーセキュリティに関するガイドライン」	<p>「金融分野におけるサイバーセキュリティに関するガイドライン」の遵守をすべての貸金業者を対象にした場合、業者の大半を占める小規模貸金業者にとっては、情報の流出を防ぐ取り組みなどのセキュリティ対応が、その事業規模に比して過大な負担となってしまうことが考えられるため、対象となる貸金業者の規模等を限定してほしい。</p> <p>（理由等） 対象者を明確にしたい。</p>	<p>11 同じ事業規模であっても、サイバーセキュリティに関するリスクプロファイルが異なることがあると考えられ、ガイドラインの適用関係を、事業規模によって限定することは困難であり、リスクベースでの対応が必要と考えられます。</p> <p>ガイドライン 1.1 節の（注）において、金融機関等の規模・特性は様々であることから、「基本的な対応事項」及び「対応が望ましい事項」のいずれについても、一律の対応を求めるものではなく、リスクベース・アプローチを採ることについて、記載しているところです。</p>
2	「貸金業者向けの総合的な監督指針」II-2-4	<p>「貸金業者向けの総合的な監督指針」II-2-4 システムリスク管理態勢の柱書には、「貸金業務をコンピュータシステムを用いて大量に処理する貸金業者において（省略）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。」と規定されている。</p> <p>当社は、自社において自動契約受付機又は現金自動設備を設置しておらず、また、受払等業務委託先との利用提携もしていないため、いわゆる「貸金業務をコンピュータシステムを用いて大量に処理する貸金業者」に該当しないが、「金融分野におけるサイバーセキュリティに関するガイドライン」の遵守は求められるのか。</p> <p>（理由等） 対象者を明確にしたい。</p>	<p>28 ガイドライン 1.1 節の（注）において、金融機関等の規模・特性は様々であることから、「基本的な対応事項」及び「対応が望ましい事項」のいずれについても、一律の対応を求めるものではなく、リスクベース・アプローチを採ることについて、記載しているところです。</p> <p>ご指摘の監督指針における「貸金業務をコンピュータシステムを用いて大量に処理する貸金業者」に該当しない場合でも、ガイドライン記載項目が必ずしも全て該当しないとは限らないと考えられます。金融機関等は、ガイドライン 1.1 節に記載しておりますように、自らが直面するリスクを評価し、重要性・緊急性に応じて優先順位をつけた上、リソース制約を踏まえ、その低減措置に取り組むべきであることに、金融庁として留意することとしています。</p>

No.	該当箇所	当協会から提出した意見・質問	金融庁の考え方
3	「1.1. サイバーセキュリティに係る基本的考え方（注）」	<p>「1.1. サイバーセキュリティに係る基本的考え方（注）」において、リスクベース・アプローチが求められている。</p> <p>当社の事業環境を整理したところ、パソコンやスマホ等の機器にて外部接続はあるものの個人情報（データベース）や勘定系業務（システム）は、紙又はオフラインのパソコンで処理をしている理由から、サイバー攻撃に係るリスクは極小と結論付け、低減措置は不要と判断する予定である。</p> <p>この判断の妥当性を登録行政庁が行う検査・モニタリングの前に事前に相談したいが可能か。</p> <p>なお、相談ができない場合、当該検査・モニタリングにより妥当ではないと判断された場合であっても、直ちに行政処分をされるものではないとの理解で良いか。</p> <p>（理由等） 対象者を明確にしたい。</p>	<p>33 金融機関等は、ガイドライン 1.1 節に記載しておりますように、自らが直面するリスクを評価し、重要性・緊急性に応じて優先順位をつけた上、リソース制約を踏まえ、その低減措置に取り組むべきであることに、金融庁として留意することとしています。今後、本ガイドラインの運用にあたっては、業界団体・共助機関等と連携して金融セクター全体の取組みを推進してまいります。</p> <p>また、一般論として、行政上の対応は、個別・具体的な状況に応じて検討されるべきものと考えます。</p> <p>なお、ご指摘のような環境であるからといって、ガイドライン記載の対応が全て不要とは言い切れないと考えられます。</p>
4	「金融分野におけるサイバーセキュリティに関するガイドライン」	<p>「金融分野におけるサイバーセキュリティに関するガイドライン」は、都道府県知事登録業者も対象であるか。</p> <p>（理由等） 対象者を明確にしたい。</p>	<p>12 本ガイドラインは、サイバーセキュリティ管理について監督指針等に定めのある金融機関等を対象としており（1.4 節参照）、「貸金業者向けの総合的な監督指針」において、「都道府県における監督行政に当たっても、本監督指針が参考とされることが期待される」とされていることを踏まえ、都道府県知事登録貸金業者の監督に当たっても、本ガイドラインを参考とされることが期待されます。</p>
5	「1.1. サイバーセキュリティに係る基本的考え方」	<p>「1.1. サイバーセキュリティに係る基本的考え方」において「金融庁としては、引き続き、金融機関等の規模・特性に応じ、リスクベース・アプローチで検査・モニタリングを実施し、その中で個別金融機関等のサイバーセキュリティ管理態勢を検証していく。」とあるが、都道府県知事登録業者業者に対しても同様な検証を行うのか。</p> <p>（理由等） 行政による検証の範囲を明確にしたい。</p>	<p>34 一般論として、「貸金業者向けの総合的な監督指針」の「I. 基本的考え方」に記載の考え方に則り、都道府県知事登録貸金業者の監督が行われることが期待されます。</p>

No.	該当箇所	当協会から提出した意見・質問	金融庁の考え方	
6	「1.1. サイバーセキュリティに係る基本的考え方（注）」	<p>「1.1. サイバーセキュリティに係る基本的考え方（注）」において、リスクベース・アプローチが求められている。</p> <p>当社の事業環境を整理したところ、当社の規模ではサイバー攻撃に係るリスクは極小と結論付け、低減措置は不要と判断する予定である。</p> <p>この判断の妥当性を登録行政庁が行う検査・モニタリングの前に事前に相談したいが可能か。なお、相談ができない場合、当該検査・モニタリングにより妥当ではないと判断された場合であっても、直ちに行政処分をされるものではないとの理解で良いか。</p> <p>（理由等） 行政処分の対象となるか否かを明確にしたい。</p>	35	一般論として、行政上の対応は、個別・具体的な状況に応じて検討すべきものと考えます。No.33 の回答もご参照ください。
7	「金融分野におけるサイバーセキュリティに関するガイドライン」	<p>令和3年4月28日付文書「マネー・ローンダリング及びテロ資金供与対策に係る態勢整備の期限設定について」（金監督第953号）において、「マネロン・テロ資金供与対策に関するガイドライン」で対応を求めている事項について、検査やモニタリングを通じて確認していくほか、仮にマネロン・テロ資金供与対策に問題があると認められた場合には、法令に基づく行政対応を含む対応を行う旨の記載があった。</p> <p>今回の「金融分野におけるサイバーセキュリティに関するガイドライン」についても同様に、検査やモニタリングを通じて確認していくほか、問題があると認められた場合には、法令に基づく行政対応を含む対応を行うのか。</p> <p>（理由等） 行政処分の対象となるか否かを明確にしたい。</p>	13	一般論として、行政上の対応は、個別・具体的な状況に応じて検討すべきものと考えます。
8		<p>「金融分野におけるサイバーセキュリティに関するガイドライン」に関する説明会を開催する予定はあるか。</p> <p>（理由等） 本ガイドラインをより深く理解したい。</p>	29	今後、検討してまいります。