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.	関連箇所 （項番等）	コメントの概要 （項番、脚注番号等は原案の文書におけるものを指す）	金融庁の考え方 （項番、脚注番号等は今般公表の文書におけるものを指す）
（１）監督指針等関係			
1		現行案は、サイバーセキュリティリスクについて、オペレーショナルリスクの中のシステムリスクの一要素として記載されていますが、システムリスクのみならず事務リスクについても同様にサイバーセキュリティリスクが懸念されるかと存じます。事業を行う上では、サイバーセキュリティリスクは広い対象範囲に跨ることから、構造としてシステムリスク、事務リスクと並列に位置づけることが、ガイドラインに記載されている内容にも合致するかと考えます。	貴重なご意見として承ります。監督指針等においては、便宜上、システムリスク管理の中に位置づけておりますが、サイバーセキュリティに関するリスクはオペリスクなど他のリスク領域にも関係しうるものと考えられます。
2		監督指針とガイドラインの関係について確認したい。 監督指針の文中では、ガイドライン「を踏まえ」（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）①）や、ガイドライン「も参照すること」（同監督指針Ⅱ－３－４－２－２（２））などの表現で言及されている。 今回制定されるガイドラインは、直接的に監督指針の一部となるものではなく、各金融機関等や監督当局がサイバーセキュリティ対策を考える際に参考にする文書という理解でよいか。	本ガイドラインの考え方については、ガイドライン 1.1 節に記載のとおりです。
3		「④情報セキュリティ管理」と「⑤サイバーセキュリティ管理」の役割上の違いについて、基本的にはどのように考えればよいか。	両者は相互に関連するものもあると考えられます。
（２）「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」関係			
4	全般	当社は、英国を本国とする金融商品取引業者であり、サイバーセキュリティ対策については、基本的に英国及び米国基準で対応しているが、本ガイドラインの策定を踏まえ、英米基準と日本基準のギャップの確認及び必要に応じた日本特有の対応を検討する観点から、本ガイドラインを本国と共有する必要が生じ	英語版の作成を検討します。

		るので、ガイドラインが制定された際には、必ず英語版も準備して頂きたい。	
5	全般	昨今、企業に対するセキュリティ侵害が巧妙化・深刻化している状況があり、サイバーセキュリティ対策の重要性は増しているため、作成されたガイドラインの内容に関して疑義はありません。当ガイドラインで示されている対策が実施できているかの自己チェックを容易にする目的で、文章形式のガイドラインをチェックリスト形式になおした表を同時に公開していただくことは可能でしょうか？	ガイドラインのいずれの項目をどのように実施すべきかは、各金融機関においてリスクベースで検討すべき事柄であるため、当庁からチェックリスト形式で示すことは馴染まないと考えます。
6	全般	サイバーセキュリティに関するガイドラインは、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いる。この点、外国銀行支店については、監督指針において、「支店の業務等に応じて、必要に応じて、本監督指針の他の部分を適宜参照し、これに準じるものと」されている。したがって、今回の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、必ずしもその全文が外国銀行支店に適用されるものではなく、「支店の業務等に応じて、必要に応じて」関係する箇所が準用されるものと理解しているが、かかる理解で良いか確認させていただきたい。	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、記載しております。支店の業務等に応じて、リスクベースで検討することが必要と考えらえます。
7	全般	環境的脅威（災害時等）のサイバーセキュリティ対策に関する記述は見当たらなかったが、全て有事の内容に含まれているということでしょうか？	ガイドラインにおいて、災害時等に特化した記載はしておりませんが、災害時等のサイバーセキュリティ対策を検討することを排除するものではありません（例：コンティンジェンシープランにおいて災害時等のサイバーセキュリティに関する対応を想定いただくなど）。
8	全般	「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」については、今般制定された「重要経済安保情報保護法」を受けて、政府が指定する「重要経済安保情報」を対象としたセキュリティ・クリアランス制度への対応を盛り込むべきである。 金融分野においても、重要経済安保情報の開示を受ける適合事業者となる可能	貴重なご意見として承ります。重要経済安保情報保護法の制度運用の開始に向けて、適切に対応してまいります。

		性はあり、適合事業者において重要経済安保情報を取り扱う者（従業者）に対しては、政府が適性評価を実施する必要がある。 なお、適合事業者におけるシステムの管理者（業務委託先を含む）は、管理するシステムの最高権限を保持している可能性が高く、事実上、システム上で保管されている重要経済安保情報を含むすべてのデータへのアクセスが可能であるものと考えられるため、重要経済安保情報を取り扱う者（従業者）として、政府が適性評価を実施する必要がある。	
9	全般	ゼロトラストについて 本ガイドラインでは、いわゆる「ゼロトラスト」の考え方が明示はされておりませんが、「2.3 サイバー攻撃の防御」や「2.4 サイバー攻撃の検知」における基本的な対応事項として、「ゼロトラスト」を前提としたセキュリティ対策が求められるという理解でよろしいでしょうか。	一般論として、ゼロトラストは、防御、検知に限らず推奨されています。ガイドラインでは、例えば、2.2.2.2 リスクの特定・評価において、「リスク評価に当たっては、境界防御型セキュリティが突破されるリスクや内部不正などの脅威も考慮し、内部ネットワークセグメントに設置したシステムへのリスクも対象とすること」を掲げています。
10	全般	「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」については、内部不正の人的側面に焦点をあてた対策を盛り込むべきである。 特に、システムの管理者（業務委託先を含む）は、管理するシステムの最高権限を保持している可能性が高く、サイバーセキュリティを社会的手段によって無効化出来てしまうため、システムの管理者（業務委託先を含む）に対する適合性評価（反社チェックや AML/CFT に類する人的側面のチェック、外国政府関係者（工作員・スパイ）でないことのチェック）を実施すべきである。 ※大規模なサイバー攻撃は非友好国の国家レベルで実施される可能性が高い。国家レベルのサイバー攻撃においては、システム的手段のみによってサイバー攻撃が行われるとは限らず、大手金融機関の内部に入り込んだ外国政府関係者（工作員・スパイ）によって、内部から社会的手段を組み合わせたサイバー攻	貴重なご意見として承ります。ご指摘の点は、ガイドラインの 2.2.2.2.③の内容に対応するものと考えられます。

		撃（およびその手引き）が行われる可能性を想定すべきである。	
11	全般	「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。 【理由等】 対象者を明確にしたい。	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。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。
12	全般	「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。 【理由等】 対象者を明確にしたい。	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。
13	全般	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場合がある旨の記載があった。 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。	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。

		【理由等】 行政処分の対象となるか否かを明確にしたい。	
14	全般	各事業者の自助努力によるサイバーセキュリティ対策の推進に加えて、貴庁におかれましても、事業者が適切なサイバーセキュリティ対策をより講じやすくなるようなガイドラインの策定にとどまらない環境の整備（例えば、「マネロン・テロ資金供与対策ガイドライン」と同様にＦＡＱ集の策定、他事業者の取組事例を紹介した事例集の策定及びサイバーセキュリティ対策に関する定期的な情報共有会のさらなる実施・充実化等）を検討していただきたく存じます。	貴重なご意見として承ります。状況に応じて、今後、業界団体等とも連携してまいります。
15	全般	本ガイドラインの施行に当たっては、事業者の導入スケジュール等も踏まえた十分な準備期間を確保していただけるようご配慮いただきたく存じます。	ガイドライン 1.1 節に記載のとおり、当庁のモニタリングに当たっては、本ガイドラインへの対応については、金融機関等において、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留意することとしています。
16	全般	監督指針等とは別に、更に詳細な本ガイドラインが策定されることは、金融業界にとって望ましいものと考えます。特に「サードパーティリスク管理に関する着眼点」については、これまでは金融機関内部の意思決定により管理の方針を定めても、契約開始時およびその後の定期的なデューデリジェンス実施の際に、機密情報であること等を理由に必要な情報の提供が得られないという問題や、セキュリティ要件にかかる契約条項に合意してくれないといった問題に直面することがありました。社内の方針のみならず、規制当局が定めたガイドラインに基づきサードパーティーに依頼することができれば、サードパーティリスク管理に必要な情報の取得や望ましい契約条項への合意の取得がより円滑に進むことが期待されます。	賛同のご意見として承ります。
17	全般	今次新たに導入されるガイドラインの英訳版を貴庁にて作成されるご予定は	英語版の作成を検討します。

		あるのか。海外拠点との連携が必要な場合があり、また最新のＩＴ用語は元来の英語表記のままの方が理解しやすいことも多いので、東京での運営を堅確に進めるためには、ガイドラインの英訳の存在が必須と考えている。従来、金融機関のシステム面のリスクやセキュリティに関しては、貴庁の「監督指針」においても、（財）金融情報システムセンターの「安全対策基準」を参照するよう慫慂されており、同基準は英語版も提供されているところ、今回の「ガイドライン」が日本語版だけでは十分とは言えない。是非、英語版を公表していただきたい。	
18	全般	・各節ごとに実施すべきことや用意すべき管理資料などが点在することから、対応内容を一覧化したチェックリストのようなものを提供し、対応事項を一元的に把握・理解できるようした方が分かりやすいと考えます。 ・「少なくとも年一回」や「定期的」等、実施頻度に関する事項は指標を記載して明確化した方が分かりやすいと考えます。	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。いずれの項目をどのように実施すべきかは、各金融機関においてリスクベースで検討すべき事柄であるため、当庁からチェックリスト形式で示すことは馴染まないと考えます。 また、ガイドライン 1.1 節に記載しておりますように、金融機関等においては、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、モニタリングに当たって留意することとしています。
19	全般	また、ガイドライン中で「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、金融機関等が、自らを取り巻く事業環境、経営戦略及びリスクの許容度等を踏まえた上で、サイバーセキュリティリスクを特定、評価し、リスクに見合った低減措置を講ずること」について言及がある。これ	本ガイドラインの考え方については、ガイドライン 1.1 節に記載のとおりであり、建設的な対話を図ってまいります。

		を踏まえ、サイバーセキュリティの確保は、各金融機関の経営判断のもとで取りうる手段や水準の検討や対策等が行われ、監督当局と各金融機関の間では、金融機関ごとに異なる経営判断を十分に踏まえたうえで、建設的な対話が図られるという理解でよいか。	
20	全般	今回提示されたガイドライン案については、適用時期の言及がない。他の監督指針の改正時と同様、公表と同時の適用を想定しているのか、経過措置等が設けられるかなどを伺いたい。また、公表と同時に適用され、経過措置等がない場合には、以下のような考え方で受け止めればよいか確認したい。 本ガイドラインは、これまでの監督・検査・モニタリング等で当局から投げかけてきた問題意識等を改めて取りまとめたものであり、(a)本ガイドラインの策定によって、今後のサイバーセキュリティに関する監督等のあり方が、これまでの監督等と非連続的なものとなるものではないこと、(b)当局による新たな取組み（検査・監督の強化）を意図した性質のものでもなく、これまでも行ってきた金融機関との対話を継続していくこと　を意図しているものと理解すればよいか。 本ガイドラインの最終化・公表と同時に適用となる場合、上記のように、(a)従来の監督から当局の姿勢を非連続的に変える意図はないこと、(b)そのため「対応期限」や経過措置を設ける性質のものではない　と理解すればよいか。	公表と同時に適用しますので、経過措置はございません。また、対応期限を求めるという性質のものではございません。本ガイドラインは、これまでの検査・モニタリングの結果及び金融セクター内外の状況の変化を踏まえてまとめたものです。今後も検査・モニタリングその他行政活動において、金融機関等と対話を継続していきます。
21	全般	本ガイドラインの内容を見ると、策定にあたって、NISC・経産省・FISC等の国内の公的機関や国外の公的機関等の基準・指針・フレームワークなども参考にされているものと窺えるが、以下の点についてお聞きしたい。 （１）他の公的機関等が策定する基準・指針などでは努力事項とされている取組み（義務ではない取組み）も、「基本的な対応事項」に含まれるなど、温度感に差があるようにも感じるが、こうした記述のニュアンスの差は意図的なものか伺いたい。本ガイドラインはリスクベース・アプローチを前提にしているこ	（（１）について）本ガイドラインの策定にあたっては、ご指摘のように、国内外の基準等も参考にしておりますが、「基本的な対応事項」及び「対応が望ましい事項」の分類については、当庁としての視点を反映しています。また、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

		とから、「基本的な対応事項」に挙げられた内容も、金融機関の規模・特性等を踏まえたうえで、一律に対応を求める性質のものではないと認識しているが、この点との関連もあわせて認識確認したい。 （２）上記のような他の基準等と本ガイドラインの関係（優劣の有無など）はどのように考えたらよいか、あわせて伺いたい。 （３）本ガイドラインを策定する上で参考にした基準等が更新された場合、本ガイドラインは都度見直しを行うのか伺いたい。例えば、「脚注４」で参考として挙げられるもののうち、「CRI Profile」は改定頻度が高いことが特長とされているが、その都度見直しを検討するのか。本ガイドラインがリスクベースを前提としており、「基本的な対応事項」も一律対応を求めるものではないのであれば、長期的に見直しを検討する可能性は否定されないとしても、短いサイクルで見直しを行うことは想定していないという理解でよいか。	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、記載しております。 （（２）について）「他の基準等」について、目的や趣旨に応じて参照することが考えられます。 （（３）について）本ガイドライン内で参照されている文献が更新されたり、変更されたりした場合、ガイドラインの修正が必要か否かは、参照文献の更新や変更の内容に応じて検討することとなると考えられます。
22	全般	金融庁では、各金融機関等（主に地域金融機関）を対象に「サイバーセキュリティセルフアセスメント」(CSSA) の取組みを行っているが、本ガイドラインとCSSA の関係性について伺いたい。 CSSA の各設問は毎年見直しが行われているが、本ガイドラインで記載のある項目もあれば、そうでない項目もある。金融機関内での態勢整備等の状況確認をCSSA の設問に沿って行っている場合、本ガイドラインの項目と二重の対応になるようにも見受けられるが、今後、ガイドラインと CSSA の両者の施策をどのように進めていくか伺いたい。 また、ガイドラインの前提が「リスクベース」であり「一律の対応を求めるものではなく」とあるところ、CSSA についても、満点を目指すことが目的ではなく、自組織の状況を相対的に見える化することや、それを踏まえサイバーセキュリティ対策に対して、どのように経営資源を配分するか自組織にとっての優先順位を考えていくきっかけにすることが重要と考えているが、その理解でよ	ご指摘のような点にも留意しつつ、CSSA については、2025事務年度以降に向け、本ガイドラインと整合させる形で自己点検票の見直しを行う予定です。ご指摘のように、自組織における対応の優先順位を考えるにあたって、CSSA を活用いただくことも考えられます。

		いか。	
23	全般	本ガイドラインで「基本的な対応事項」が挙げられているが、これらの事項に対応するために必要な人材について、監督当局では、各金融機関がどの程度充足できると見込んでいるか。特に、地方の金融機関や小規模金融機関においては、高度なサイバー人材の採用・確保が極めて難しい状況にあり、今回のガイドラインに対応するために、今よりも苛烈な人材の奪い合いが生じることも懸念している。 他方、本ガイドラインでは、各金融機関の規模・特性等にも言及されており、そのうえで、各項目についてもリスクベースで考えることとされている。確保できる要員が不足する場合、その限られたリソースの中で、どの対策を重点的・優先的に実施していくかなどもリスクベースであり、不足に対してどのように凌ぐか（対策の優先順位付けや、リスク受容を含む）も含め経営層の判断のもとで対応していくことが求められていると理解すればよいか。	各金融機関のリソースの状況は様々であることから、充足の見込みについて一概にお答えすることは困難です。金融機関等においては、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必要があります。また、ガイドライン 2.1.3 に記載のとおり、計画的に人材を育成すること、外部人材の活用も含めて人材を確保していくことも重要です。
24	全般	本業態では、サイバーセキュリティに関する手順書の参考例を作成し、会員金融機関に公開している。内容は、平時の対応、インシデント発生時の対応があり、ガイドライン案で求められている項目についてもすべてではないが含まれている。ガイドライン案で求められている規程や要領の作成については、手順書というレベルで作成（現在の手順書参考例に不足しているものを追加）する形で対応することは可能か。	本ガイドラインに関連して、当庁として参考例等の形態を指定するものではありませんが、ご指摘のような対応を含め、業界団体等における参考資料の作成は、ガイドライン 1.3 節の趣旨に照らして、有益なものと考えられます。
25	全般	金融庁ではサイバーセキュリティセルフアセスメントの取り組みもあるが、本ガイドラインの「基本的な対応事項」と比べ求める水準感に差があり、本ガイドラインの「基本的な対応事項」が求める水準が相対的に高いように見受けられる。求める水準感がダブルスタンダード化しているようにも見え、整合性を確保してほしい。	本ガイドラインの「基本的な対応事項」にはリスクベースアプローチが適用され、金融機関等において、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と考えます。 サイバーセキュリティセルフアセスメント（CSSA)は、各金融機関において自己評価に活用されることを想定したもの

			です。
26	全般	「基本的な対応事項」の中には、CRI Profileなどのグローバルな評価フレームワークでは大規模な金融機関に求める内容も含まれており、「基本的な対応事項」の求める水準がグローバルスタンダードに比べても高いように見受けられる。中小金融機関を含め、対応については、時限を定めて一律の対応を求めるものではなく、各金融機関がリスクベースアプローチで対応するという理解でよいか。	本ガイドラインの「基本的な対応事項」及び「対応が期待される事項」のいずれについても、各金融機関においてリスクベースアプローチで対応するべきものと考えます。
27	全般	本ガイドラインにおける「経営陣」とは役員・執行役員を指し、「経営トップ」とは頭取・社長・理事長等を指すという理解で相違ないか。サイバーセキュリティ管理態勢について経営陣の主体的な関与が求められる点は各節でも繰り返し述べられている重要事項であるため、本ガイドラインにおける定義を明確に示してはいかがか。	本ガイドラインにおいては、「経営陣」は、会社法上の役員（業法により読み替える場合を含む）が該当し、「経営陣等」には執行役員及びそれに準ずる然るべき責任者が含まれます。「経営トップ」については、ご理解のとおりです。
28	全般	「貸金業者向けの総合的な監督指針」2-2-4 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。 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。 【理由等】 対象者を明確にしたい。	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。 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。

29	全般	「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。 【理由等】 本ガイドラインをより深く理解したい。	今後、検討してまいります。
30	全般	最初に、このサイバーセキュリティに関するガイドラインを通して、金融分野におけるサイバーセキュリティ対策が、社会・業界環境や時代の流れに則しながら、より強固にしなやかに進化していくことを期待します。 ＜システムへのリモートアクセスに関して＞ 昨今、様々な企業にて、オペレーショナル・レジリエンス確保に向けた具体的な取り組み検討が行われており、早期復旧、影響範囲軽減の具体策として、システムへのリモートアクセスの導入検討が進んでいる。しかし、システムへのアクセスに対しては、高いセキュリティレベルが求められること、具体策を含むガイドラインが整備されていないことから、各社ともに最終判断に苦慮されているケースが多い。「クラウドサービス利用時の対策」と同様に「システムへのリモートアクセス利用時の対策」のような事項を設け、リモートアクセスによりシステム運用・インシデント対応を実施する際の対応事項の整理・追記をご検討いただきたい。	貴重なご意見として承ります。リモートアクセスに関する項目を別に設けることは致しませんが、リモートアクセスについて言及している項目（2.3.4.1 節、2.3.4.4 節）もご参照ください。
31	全般	サイバーセキュリティインシデントを引き起こす要因のひとつに、いわゆる「内部脅威」がある。不満や悪意を持った従業員が転職先などに情報漏洩する等が代表的であるが、これらは脅威としてれっきとして存在するものの、自社の従業員に疑いの目を向けて監視することの難しさも相俟って、対応方法に苦慮している金融機関が多いのではないか。ガイドラインとしては、内部脅威への対策方法の記述をより充実させ、各社とも対策を講じやすくすることで金融業界におけるサイバーセキュリティ向上に寄与するのではないか。	貴重なご意見として承ります。ご指摘の点は、ガイドラインの 2.2.2.2.③の内容に対応するものと考えられます

		愚案であるが具体的には以下の観点が特に大切と考える。 ・外部脅威は、文字通り「外部」のためいつ何時発生するかを予測することは不可能であるが、内部脅威は一定の対策は可能である。具体的には脅威となる可能性がある従業員は、犯罪学の観点から事前に特定可能である。例えば、自分では能力があると考えているものの、長らく昇進や昇給がなく会社に極度な不満を抱き、上司からの激しいハラスメントをうけている従業員がいたとする。そして、当人が会社の重要な営業秘密を知り得る立場にいたとしたら、国外の競合他社にとって、このような社員は転職先の会社での地位とボーナスを約束・懐柔し、情報を漏洩させることはたやすい。このような兆候は、会社貸与のメールやチャットでの同僚や社外取引先との会話をモニタリングすることで見つけられることが多い。重点監視従業員を特定し、UEBA や DLP で異常行動が検知された際に早期介入することで事案の未然防止ないし最小限の被害に留めることができる。ガイドラインとしては、従業員のコミュニケーションモニタリング実施の非調整、ハイリスク従業員の特定と重点監視の有効性への言及が考えられる。	
32	1.1.	「基本的な対応事項」及び「対応が望ましい事項」につき、いずれも一律の対応を求めるものではないとされておりますが、当該金融機関において対応するリスクの発生が現実的に想定されるにもかかわらず、特段の理由なく「基本的な対応事項」が採られていない場合、業務改善命令等の対象となる可能性があるということでよろしいでしょうか。	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。
33	1.1.	「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。 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	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

		極小と結論付け、低減措置は不要と判断する予定である。 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。 【理由等】 対象者を明確にしたい。	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。 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。 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。
34	1.1.	「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。 【理由等】 行政による検証の範囲を明確にしたい。	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。
35	1.1.	「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。 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。 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。 【理由等】	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。

		行政処分の対象となるか否かを明確にしたい。	
36	1.1.	ガイドライン案で示されたそれぞれの事項について、一律の対応を求めるものではないとしても、リスクベースアプローチでの対応が求められるとすれば、従前対応してきた事項が十分だったとは言えない本業態のような中小金融機関ほど対応する項目が多くなり、「基本的な対応事項」だけをみても、経営体力対比で考えると不可能または実現には相当の時間を要する課題が積み上がることが予想される。そこで、経営体力の効率的活用のため、「基本的な対応事項」の中でも目安としてまず達成すべき・最優先となる項目を明確に提示していただきたい。	対応の優先順位については、個々の組織により異なると考えられ、一概にお示しすることは困難です。ガイドライン1.1節に記載のとおり、当庁としては、金融機関等において、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留意することとしています。
37	1.1.	ガイドライン案では、サイバーセキュリティ対応に係る当局の方針として、マネーローンダリングのように全金融機関一律の対応期限を設けた管理はしないという認識だが、「金融機関等において、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付けた上……取り組むべきである」とある以上、個別金融機関において適切な期限管理の下、策定した計画に基づく対応を行っているかどうかを当局から監督されるという認識で相違ないか。	ご認識のとおりです。金融機関等の規模・特性は様々であり、リスクベース・アプローチで検査・モニタリングを実施します。
38	1.1.	「対応が望ましい事項」の中には、どの金融機関にとってもかなり難度の高い取り組みも含まれている認識でいるが、その理解であっているか。金融庁として、監督・検査の中で今後どのように取り扱うことを想定しているのか。	「対応が望ましい事項」の中には、ガイドラインに記載のとおり、先進的な取組みも含まれます。当庁としては、金融機関等において、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付けた上、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留意することとしています。
39	1.1.	ガイドラインの記載から、各金融機関の規模・特性等によって、取り組める内容や取り組むべき内容は異なると監督当局も認識されているものと思われる。ガイドライン上は、冒頭の位置づけの中で「リスクに見合った低減措置を講ずることに留意」する旨を明記しており、「基本的な対応事項」を含めた各取組事項について、当局から一律の対応を求める意図はないとの認識でよいか（ガイ	ご認識のとおりです。

		ドライン中「1.1.サイバーセキュリティに係る基本的考え方」にも本論点の記載があるが、念のため確認するもの)。	
40	1.1. 1.4.	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（案）１．４．によれば、本ガイドライン案は、主要行等、中小・地域金融機関のほか、前払式支払手段発行者、資金移動業者、暗号資産交換業者等の幅広い事業者を対象とすることとされている。しかし、大規模な主要行や、高度の技術的対策が求められる暗号資産交換業者等と異なり、前払式支払手段発行者や資金移動業者の事業規模や事業形態は様々であるから、本来は、各事業者向けのガイドラインごとに対応事項を区別して明記することが適切であり、全事業者を対象とする統一的なガイドラインを策定することは困難であると考える。本ガイドライン案は、１．１．において「『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い」旨記載しているものの、具体的な要求事項が不明確であり、事業者にとって予測可能性を欠く点で問題がある。各事業者は、ガイドライン案１．１．記載のとおり、リスクベース・アプローチを採用し、現実的に可能な対策を講じていればガイドラインには違反しないという理解でよいか。	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。 また、同1.1節に記載しておりますように、金融機関等においては、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、モニタリングに当たって留意することとしています。
41	1.1.1.	サイバーハイジーンが求められる中で、金融庁として導入を求めるもしくは望ましい基準となるセキュリティシステムの具体例（EDRなど）はありますか。	システムのセキュリティ対策に関する着眼点は、2.3.4節において示しているところです。
42	1.2.	中小金融機関に対して過度な負担とならないよう、リソースの限られた金融機関向けの具体的なサポートやガイドラインの適用範囲を明確化した方が望ましいと考えます。	貴重なご意見として承ります。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、記載しております。また、同1.1節に記載しておりますように、金融機関等においては、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。
43	1.2.	日本の金融機関等のサイバーセキュリティ対策向上に資する、大いに評価されるべき取り組みであり、感謝申し上げる。 経済産業省の産業サイバーセキュリティ研究会（2024 年 4 月 5 日第 8 回）においても、以下のようにあるため本件と平仄を取った対応を進めていただきたい。 今後は、諸外国で議論が進んでいる、「サイバー対策」のレーティング等も参考にしつつ、各企業等の業種・規模などのサプライチェーンの実態を踏まえた満たすべき各企業の対策のメルクマールや、業界間の互換性を確保しながらその対策状況を可視化する仕組みを検討していく。 「併せて、関係省庁とも連携し政府機関・企業による活用を促す枠組みと紐付けることで、その実効性を強化していく。」とされており、本件と平仄を取った対応を進めてもらいたい。	貴重なご意見として承ります。本ガイドラインを含め、金融分野におけるサイバーセキュリティに関する施策を進めるうえで、関係省庁ともよく連携してまいります。
44	1.2.	日本の金融機関等のサイバーセキュリティ対策向上に資する、大いに評価されるべき取り組みであり、感謝申し上げる。 金融機関等がこれらを取り込むにあたり、現在参考としている FISC の安全対策基準に取り込み、その中で統制していく事も各企業の効率性の観点から有用と考えるが、どのように取り込まれるのか、もしくは取り込まれずに別々に管理するのか、本紙にも連携を維持、強化するとしていただいている FISC とご連携のうえ今後の方針も是非ともご開示いただきたい。	FISC 安全対策基準について、本ガイドライン 3.1 節に記載のとおり、FISC をはじめ関係機関とよく連携してまいります。
45	1.2.1.	脚注４で参考として挙げられている米国 NIST「Cybersecurity Framework」や、米国 CRI「The Profile」等の海外のガイドラインについて、今後、監督当局や公的機関等から日本語訳が提供されるかを伺いたい。	現時点で、当庁において日本語訳を作成する予定はございません。

46	1.2.1. 1.2.2.	「経営陣の主体的な関与の下、リソースを適切に配分することが求められる」「経営陣をはじめとして、組織全体で態勢構築と運営を行う必要がある」といった記述があり、後段の「1.2.2.経営陣の関与・理解」につながるものと思料する。これに関連して、以下３点お伺いしたい。 （１）本ガイドライン「1.1.サイバーセキュリティに係る基本的考え方」における「リスクベース・アプローチ」に係る記述の中で、「金融機関等が、自らを取り巻く事業環境、経営戦略及びリスクの許容度等を踏まえた上で、サイバーセキュリティリスクを特定、評価し、リスクに見合った低減措置を講ずること」と触れられており、この点が経営陣の主体的な関与にあたって基本的な部分ではないかと考えるが、その理解でよいか。 （２）本ガイドラインのように、態勢整備事項や対策事項を列挙すると、経営層は「インシデントが起こらないように、漏れなく実施するように」と指示したくなる。他方で、投入できるリソースは有限であり、そもそも、どれだけ対策を講じても、ゼロデイ攻撃を含めリスクをゼロにはできない。経営層は、(a)相応のリソース投入の必要性があることとともに、(b)経営上一定の残存リスクを受容せざるを得ないものであること　-の両方を理解する必要があるのではないかと考える（特に後者については、リスク評価により残存リスクを認識して、「受け入れる」という判断をすることは、リソースに限りがある金融機関ほど重要になると考える）。そのうえで、対策を講じるために投じるリソースと、許容する残存リスクのバランスを考え、経営判断することが経営層の役割と考えるが、その理解でよいか。 （３）「1.2.2.経営陣の関与・理解」では、主に経営陣の責任等の記述はあるが、具体的にどのように「リーダーシップ」「主体性」などを発揮していくことが期待されているかの言及は少ないように感じた。組織の規模・特性に応じて	（（１）について）「基本的な部分」が示す内容は必ずしも明らかではありませんが、ご指摘の点は、重要な点の一つと考えられます。 （（２）について）経営陣は、対策を講じるために投じるリソースと、許容する残存リスクのバランスを考えて経営判断する必要がありますが、リスク受容がリスク管理プロセスの完了を意味するものではなく、残存リスクのモニタリング、状況に応じた追加措置など、残存リスクを受容するという判断以降も残存リスクの管理を適切に行う必要があります（ガイドライン 2.2.2.3 参照）。 （（３）について）経営陣等に関する事項は、特に、ガイドラインの 2.1 節において具体的に記載しているところです。

		異なるものとは承知しているが、上記（１）（２）の観点も含め、こうした点について、監督当局のお考えを伺いたい。	
47	1.3.	「1.3.業界団体や中央機関等の役割」の中では、業態内での業界団体・中央機関等による支援や、金融 ISAC を通じた金融機関同士の共助などについて触れられている。 いずれも、単一の金融機関では限りがあるリソースを克服するために、協調できる部分について助け合い、業態全体で底上げが図られることが望ましいというものだと思われる。他方で、こうした共助等の取組では、情報を提供する側の取組姿勢によって、活動の活発さが変わり得る面があり、積極的に自組織の情報を出していこうとするインセンティブが働くか否かが重要と考える（皆が受け手側のみに留まってしまうと、共助が促進されないが、発信する行為が自組織にとって直接的なインセンティブがない場合、発信が不足し共助が成り立たない可能性がある）。 各組織内・業態内でも検討するべき事項ではあるが、監督当局においても、金融機関が自組織外に対して積極的に発信する姿勢を前向きに評価する（例えば、共助機関等において、対外的な発信（最新動向の情報提供や自組織の取組みの共有など）を行うことを金融機関が組織内で推進・評価している場合、監督当局もそれを後押しするなど）ような考え方を期待したい。	金融機関に対して、共助の取組みへの積極的な参画を促していきます。
48	2.1.	「2.1.サイバーセキュリティ管理態勢の構築」の項目等で、「取締役会等」と「経営陣」の両方の表現があるが、各々の使い分けについて伺いたい（監督指針上では「経営陣」の定義はされていないと認識しているが、本ガイドラインではどのように考えているか伺いたい）。 「取締役会等」は意思決定機関等としての会議体を、「経営陣」については役員・執行役員などの各人を想定しているのか。また、「取締役会等」について、経営層による会議体であれば、「取締役会」にこだわるものではないと考えるが、その理解でよいか（取り扱う内容などによって、例えば、一部の担当役員と担当部門長等を中心に構成する委員会や、取締役会よりも小規模な役員会、	本ガイドラインにおいて、「取締役会等」は、取締役会以外に、役員で構成される理事会などの意思決定機関としての会議体を想定しています。「経営陣」は、会社法上の役員（業法により読み替える場合を含む）が該当します。これに対し、「経営陣等」には執行役員及びそれに準ずる然るべき責任者が含まれます。

		非常勤役員を含めない常勤役員会なども考えられるのではないか)。	
49	2.1.1.	取締役会等・経営陣が、サイバーセキュリティに関する事項に「主体的」に関与する・取り組むことについて、想定される姿があれば伺いたい。 多くの金融機関では、本部の各担当部門等が態勢整備・対策等について検討し、取締役会等・経営陣が意思決定をする形式が一般的であり、取締役会等・経営陣の責任の下で実施されるという意味で、これもひとつの主体的関与のかたちという理解でよいか。	各担当部門が取締役会等に上程した内容を経営陣が受動的かつ形式的に追認するような場合は、経営陣による主体的関与とは一概に言い難いと考えられます。ガイドライン 2.1 節などに記載の事項の実施を通じて、経営陣が主体的にサイバーセキュリティの管理態勢を整備することが重要と考えられます。
50	2.1.1.①	経営陣のコミットメントの続きとして「従業員への方針浸透、遂行指示、定期的なトレース」を明記した方が望ましいと考えます。	ご指摘の点は、ガイドライン 2.1.1.⑥の内容に対応すると考えられます。
51	2.1.1.①	本項目でいう「サイバーセキュリティ管理の基本方針」については、本ガイドライン記載の趣旨に沿っていれば形式にとらわれるものではないとの理解でよいか(「方針」等の名称は問わない、内部向けとするか対外公表するかを問わない、他の規程類の一部に盛り込まれていれば独立したものである必要はない、等)。 また、情報セキュリティやシステムリスク全般について何等かの定めを行っており、そこにサイバーセキュリティの要素が含まれている場合には、サイバーセキュリティのみに特化したものを別に設けることまで求めているものではないとの理解でよいか。	個々の金融機関におけるサイバーセキュリティ管理の基本方針の具体的な内容やそれに関連する状況に即して検討する必要があります。他の規程類の一部である場合、重要なリスクとして適切に取り扱われているかなどを確認する必要があると考えられます。
52	2.1.1.①	「取締役会等は、・・・サイバーセキュリティ管理の基本方針を策定」との記載については、改廃権限が取締役会等にあると理解すればよいか。	ご理解のとおりです。
53	2.1.1.②	また書き部分の「少なくとも１年に１回レビューを行うなどにより、十分な検証、議論を行うこと」について、考え方を伺いたい。 ここでいうレビューの方法に関しては、必ずしも全体の見直しを指すものではなく、「例えば、直近１年のイベント・外部環境変化などを踏まえて担当部門内で見直し要否の検討を行う（その結果、重要性を考慮して、現時点で即時の更新は不要、という結論もあり得る)」というものでも差し支えないと理解して	ここに記載のレビューとは、取締役会等が、サイバー攻撃が高度化・巧妙化していることを踏まえ、組織の経営目標にとってのサイバーセキュリティの確保の重要性を認識し、関係主体等からの要求事項や、法規制等の内外環境を踏まえ、必要なサイバーセキュリティ管理態勢を確保しているか、少なくとも１年に１回、十分な検証、議論を行うことを意味

		よいか。	しています。そのレビューの結果、管理態勢の変更を行わないとする結論もありうるものと考えられます。 なお、レビューは、担当部門内といった現場担当者に止まらず、取締役会等によって行われるべきと考えます。
54	2.1.1.②	サイバーセキュリティ対策の年間予定を組む際には、「今年は演習を通じて課題を洗い出す」「去年の取組みを受けて、今年は対応手順の見直しに注力する」「監査対応の導入に向けて項目整理に力を入れる」「リスク評価を重点的に行う」など、その年の重点テーマを設けることが一般的であり、限られたリソースで毎年態勢全体の見直しを行うことは困難であるものと考えられる。 本項目に関しては、その時点で認識されている自組織の課題等（前回レビュー時や、通年の業務の中で、あるいは演習等を通じて把握された課題など）を踏まえたサイバーセキュリティ管理態勢の十分性や、直近１年の外部環境の変化を経営層（本項目では取締役会等）が認識・考慮しているか（放置していないか）という観点の記載という理解でよいか。	取組計画（含む複数年計画）の策定にあたっては、金融機関等が、自らを取り巻く事業環境、経営戦略及びリスクの許容度等を踏まえた上で、サイバーセキュリティリスクを特定、評価し、リスクに見合った低減措置を講ずることが重要となります。 また、金融機関等は、自らが直面するリスク、重要性・緊急性に応じて優先順位をつけた上で、リソース制約を踏まえ、計画的に、その低減措置に取り組むことが必要と考えられます。 そうした中、経営陣は、サイバーセキュリティ管理の基本方針に基づいて、取組計画（含む複数年計画）の実効性及び十分性を確保する責務を負っているものと考えられます。
55	2.1.1.② 2.1.1.③	②と③はいずれもサイバーセキュリティ管理態勢の整備、十分な検証・議論を求める事項だが、②は合議体、③は人物と役割を果たす責任主体の違いにフォーカスして項目が分けられているという理解で相違ないか。	ご認識のとおりです。
56	2.1.1.③	「情報共有機関等を通じた早期警戒のための情報収集・共有・分析体制」とはどのようなものか。 預金取扱金融機関に関しては、銀行等セプター情報を受け取る仕組みがあるが、こうした情報等を受領した後の対応（必要に応じてベンダー等との連携や対応要否等の相談など）を意図しているという理解でよいか。	ご指摘のような点も含まれると考えられます。なお、情報を受領するだけではなく、場合によっては情報を提供・共有する場合もあると考えられます。

57	2.1.1.③	「SOC 等のサイバー攻撃に対する監視体制」については、「外部のリソースの活用を含む」と明記されているが、態勢整備に関してすべてを内製化することは難しい面もある。他２項目も含め、本項目の態勢整備に関して、外部リソースを活用すること自体は否定されないとの認識でよいか。	外部リソースを活用すること自体は否定されませんが、外部のリソースに依存することのリスクの評価及び管理、外部リソースの活用を前提とした体制整備に取り組む必要があることにも留意が必要です。ガイドライン 2.6 節もご参照ください。
58	2.1.1.③	「SOC 等のサイバー攻撃に対する監視体制」についてはどのような水準を想定しているか伺いたい。	リスクベースで検討すべきであり、水準を一概にお示しすることは困難です。
59	2.1.1.④	「サイバーセキュリティに係る戦略」は、サイバーセキュリティ管理基本方針や取組計画からは独立した文書として作成することを意図しているようにみえるが、基本方針や取組計画と内容的にはほとんど重複するので、独立して作成する必要はないのではないか。それぞれの定義を明確にしていただきたい。	サイバーセキュリティに係る戦略、取組計画は、サイバーセキュリティ管理の基本方針を具現化するためのものという位置づけです。
60	2.1.1.⑥	通常、地域金融機関の経営陣は、金融業務・サービスや、営業エリアの地域経済・取引先等の状況、自組織の経営などに対する知見・経験などを有していると考えられるが、サイバーセキュリティの専門家ではない。その中で、あえて経営陣を主語にして「基本的な対応事項」を挙げていることから、専門家ではない立場であっても、経営陣だからこそ有する権限をもって、担当部門や外部ベンダーを活用していくことが、リーダーシップとして期待されているのだろうと推察する。 他方で、サイバーセキュリティのみが経営課題ではない中、経営陣自身も有限な時間で他の分野も含めた数多あるインプット事項にどのように対処するか考える必要があり、過度に期待するのも適当ではないと考える。 こうした中、「自らリーダーシップを発揮」や「サイバーセキュリティ確保に向けた組織風土を醸成」とは、具体的にどのようなことを指すか。また、翻って、経営陣に期待されている知見や資質についても監督当局の考えを伺いたい。	経営陣に求められるリーダーシップについては、ガイドライン 1.2.2 節をご参照ください。組織風土の醸成とは、経営陣が、サイバーセキュリティ担当部署等の特定の部署あるいは特定の職員に対応を任せるのではなく、組織全体（部門、職員のレベルなどを問わず）として、サイバーセキュリティ管理態勢を構築・運用することが含まれます。経営陣に期待される知見・資質について、経営陣自身がサイバーセキュリティの専門家である必要はありませんが、ガイドライン 2.1.1.a や 2.1.3 に記載の事項もご参照ください。
61	2.1.1.⑥	「自組織の重要業務」とは、本ガイドライン「2.2.1.2.対応が望ましい事項 c.」の脚注 23 の「重要な業務」（主要行等向けの総合的な監督指針 3-３-６-１に規	原案における「重要な業務」や「重要業務」という表現を見直し、脚注 12 において、本ガイドラインにおける意味を明

		定するもの（その中断が金融システムの安定や利用者の日常生活に著しい悪影響を生じさせるおそれのある金融サービス））を想定すればよいか。	確化しました。なお、本項目において、「重要な業務」のみに限定して対策を推進することを意味するわけではありません。
62	2.1.1.⑦	「サイバーセキュリティ管理に関する担当部署」をどの部門に設置するかについて、監督当局の考えを伺いたい。規模・特性等によって異なり得るとの考えでよいか。	ご理解のとおりです。
63	2.1.1.⑦	金融機関において、CISO を明確に定義し配置することを想定しているのか。また、CIO が実質的に CISO の役割を果たしているケースや、CISO/CIO に相当する役割を部門長（役員でないケースもある）が担うことなどもあるが、金融機関ごとに対応は異なり得るという理解でよいか。 近年、CXO（Chief XXX Officer）といった役割が様々な分野で呼称されるようになっているが、小規模な金融機関の限られた役職員のなかで役割を分担していくことには限界がある。重要なのは CISO 相当の役割（権限・責任等）について組織内で明らかにすることであって、名称や他の役割との兼務可否、あるいは当該役割を担うのが役員であるかどうかなどは、組織の規模・特性に応じて異なり得ると考えて差し支えないか。	ご理解のとおりです。
64	2.1.1.⑦	CISO 等の「任命」という表現について意図はあるか。人員配置や担当割り等とは異なり、「任命」に相当する何らかの手続きが必要になるのか（組織内部での辞令等、または外部向けの登記等の手続きや公表など）。	「任命」に特別な手続きを想定している訳ではありません。
65	2.1.1.⑦	金融商品取引業者等向けの総合的な監督指針では、「III－２－８　システムリスク管理態勢」のうち、「④情報セキュリティ管理」における着眼点として、「ロ.情報の機密性、完全性、可用性を維持するために、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。」という点を挙げているが、これらは情報の定義・分類よりも技術的な安全管理措置に着眼していると思われるところ、「⑤サイバー	兼任させることも含まれると考えられます。いずれにしても、ガイドライン 2.1.1.⑦および 2.1.1.e に記載のように、サイバーセキュリティ担当部署及び各関係者の役割と責任及び権限を明確化することや、サイバーセキュリティに関する十分な知識・経験を有する者を配置することに留意が必要です。

		セキュリティ管理」および新「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」 2.1.1.⑦の「サイバーセキュリティ担当部署および各関係者」や「サイバーセキュリティを統括管理する責任者（CISO 等）」とは別の管理者を設置することを期待するものか。また、その場合、両職責を同一人物に兼任させることは定めの趣旨に反するか。	
66	2.1.1.⑧	担当部署に報告を求めるだけでなく、経営陣にてその報告内容を理解し適切な判断の元で指示および支援を行うことまで踏み込んでも良いかと考えます。	ご指摘の点は、ガイドライン 2.1.1.⑥の内容に対応すると考えられます。
67	2.1.1.a	ガバナンスの確保についての記述とともに、「３線防衛態勢」についての言及がある。 組織の規模・特性等によってガバナンスの確保の在り方や、「３線防衛態勢」の考え方の自組織への当てはめ（例えば、小規模金融機関の場合の、独立した部署間での牽制確保の難しさを踏まえた対応など）も異なると考えるが、その理解でよいか。	ご理解のとおりです。
68	2.1.1.a	記載内容的にディフェンスにフォーカスした「３線防御態勢（３ラインディフェンス）」ではなく、リスク管理にフォーカスした「３ラインモデル」の方が良いと思われる。	一般的な表現として、案文を維持させていただきます。
69	2.1.1.b	「統合的リスク管理の一部」「リスク選好度（リスクアペタイト）」「リスク耐性度（リスクトレランス）」といった記載について、ここでは計量化でなく、定性的なリスク管理を念頭においた意図で記載しているという理解でよいか。	定性的な手法によるものも含まれますが、それに限定されません。
70	2.1.1.c	取組の意義を表明する目的であれば、広く一般に対しての外部への公表は不要という考え方もあると存じます。仮に対外公表することをガイドラインとして記載するのであれば、本文にある通り情報を与えることにより攻撃者の攻撃を助長する可能性を回避するため、記載と合わせ、金融機関の公表基準の提示ないし公表内容を例示する方が望ましいと考えます。	貴重なご意見として承ります。金融機関において、対外公表について一律的な対応を求めるものではありません なお、次の公表資料も参考になると考えられます。 ・サイバーセキュリティ戦略本部「重要インフラのサイバーセキュリティに係る安全基準等策定指針」 ・経済産業省・IPA「サイバーセキュリティ経営ガイドライ

			ン Ver 3.0」 ・NISC「サイバーセキュリティ関係法令 Q&A ハンドブック Ver2.0」」
71	2.1.1.c	経営陣は、可能な範囲で、自組織のサイバーセキュリティに関する取組みの意義を内外の関係者に表明するために、攻撃者の攻撃を助長する可能性を考慮の上、その内容を対外公表すること、とありますが、一般的に対外公表は HP で良いでしょうか。	具体的な公表方法を指定するものではありませんが、ご指摘のように、金融機関が自らのウェブサイトに掲載するなどの公表内容が広く周知されるような方法が望ましいと考えられます。
72	2.1.1.c	「対外公表」の内容として例示されているものについて、一部抽象的なものもあるが、どのような内容（切り口や内容の詳細さなど）を公表すべきか、具体的な想定はあるか伺いたい（特に、「維持するサービス範囲・水準」「サイバーセキュリティに関する責任者の知見」「資源の確保」などについて考え方を示していただきたい）。	【対応が望ましい事項】として、金融機関において、可能な範囲で、対外公表する内容について、検討することを想定しており、対外公表する内容（切り口や内容の詳細さなど）について、一律の対応を求めるものではありません。 なお、次の公表資料も参考になると考えられます。 ・サイバーセキュリティ戦略本部「重要インフラのサイバーセキュリティに係る安全基準等策定指針」 ・経済産業省・IPA「サイバーセキュリティ経営ガイドライン Ver 3.0」 ・NISC「サイバーセキュリティ関係法令 Q&A ハンドブック Ver2.0」
73	2.1.1.c	対外公表に関しては、「攻撃者の攻撃を助長する可能性を考慮の上」という留意事項も付されている。 （１）一般向けの対外公表ではなく、業界内関係者に閉じた範囲での共有とすることで、内容を深めることの意義もあるのではないか（広く一般に対する「対外公表」に拘泥するものではないのではないか）。 （２）公表にあたって、特に先進的な金融機関は、自組織に対する攻撃を助長する可能性だけでなく、水準が相対的に劣後する他の金融機関への攻撃を助長する可能性も考慮したほうがよいのではないか。	業界内関係者に閉じた範囲での共有によって内容が深まれば意義のあることだと考えられますが、加えて、対外公表することで、ステークホルダーや社会に対する金融機関としての姿勢を示し、信頼性を高める効果が期待できます。 また、2.1.1 の対応が望ましい事項 c の「攻撃者の攻撃を助長する可能性」の考慮には、自組織及び他組織への攻撃が含まれます。 次の資料もご参照ください。

			・サイバーセキュリティ戦略本部「重要インフラのサイバーセキュリティに係る安全基準等策定指針」 ・経済産業省・IPA「サイバーセキュリティ経営ガイドライン Ver 3.0」 ・NISC「サイバーセキュリティ関係法令 Q&A ハンドブック Ver2.0」
74	2.1.1.c	公表内容の事例のうち「サイバーセキュリティに関する責任者の知見」の記載例をお教え願いたい。 対外向けにサイバーセキュリティ経営宣言をホームページ等で常時公表する場合、責任者の変更の都度、「サイバーセキュリティに関する責任者の知見」内容を変更するものではなく、責任者の属人的な内容ではなく、役割に応じた記載をするものと考えている。	例えば、「サイバーセキュリティに関する責任者の知見」については、役職に求められるサイバーセキュリティに関する十分な知識・経験を示していただくことが考えられます。
75	2.1.1.d	2.1.1d のみ年 2 回としている理由が不明瞭でした。あわせて、具体的な報告内容例の提示があれば分かりやすいと考えます。	本項目において、「少なくとも 1 年に 2 回」と記載しているのは、KPI や KRI はより頻度の高い報告が望ましいためです。どのような報告内容が経営判断に資するかの判断は、金融機関によって様々であり、報告内容について一律のものを促そうという趣旨ではないため、本ガイドラインで具体例の提示は行いませんが、経営判断に資する内容とすることが考えられます。
76	2.1.1.d	「経営陣は、少なくとも１年に２回、以下の報告を担当部署等に求めること」とあるが、頻度に関して、他の項目では「１年に１回」としている箇所が多く見受けられる。頻度の考え方についてご教示いただきたい。	本項目において、「少なくとも 1 年に 2 回」と記載しているのは、KPI や KRI はより頻度の高い報告が望ましいためです。
77	2.1.1.d	「少なくとも 1 年に 2 回」と具体的な回数の記載があるが、これは実質的な遵守すべき事項と考えるべきか。	本項目は、「対応が望ましい事項」として記載しております。
78	2.1.1.e	前半文章「自組織における～立場の者を配置し」は、基本的な対応事項⑦の最後の文章「サイバーセキュリティを統括管理する～任命すること。」と同義と	2.1.1.e は、2.1.1.⑦に比べ、「CISO 等として、サイバーセキュリティに関する十分な知識・経験を有し、かつ、経営陣

		思われる。表記を片方に寄せた方が良い。「業務部門にサイバーセキュリティに関する十分な知識・経験を有した責任者を配置すること」は、望ましいのはその通りであるが、サイバー人材が枯渇する昨今においては現実離れした記載と思われる。せめて「担当者」レベルか。	に日常的に直接レポートできる立場の者を配置し、平時及び有事に、経営トップと直接コミュニケーションする関係を構築すること」としており、より望ましい事項を記載しています。後段については先進的な取組みなどの「対応が望ましい事項」として記載しております。
79	2.1.1.e	「サイバーセキュリティを統括管理する責任者（CISO 等)」の記述が複数存在する中、本項では「サイバーセキュリティ関連業務を統括管理する責任者（CISO)」とある。書き分けを要しないのであれば、統一いただきたい。	ご指摘を踏まえ、修正いたします。
80	2.1.1.e	「業務部門にも、サイバーセキュリティに関する十分な知識・経験を有し、CISOと業務部門との連携を円滑にする役割を持つ責任者を配置すること。」について、責任者だけ配置しても十分な実効性が期待できず、BISOオフィスのような実務を担うチームが必要であり、「責任者およびその活動を支えるチームや担当者を配置すること」といった趣旨の内容とすべきではないでしょうか。	ご指摘の点は、本項目の「CISO がその役割を果たすに足るサポート、権限及び資源を提供すること。」に含まれると考えられます。
81	2.1.2.①	サイバーセキュリティに係る規程等の見直しについては、状況に応じて行うものと考えています 特段状況の変化がない場合においても、年１回という頻度での見直しは必須ということでしょうか ※他にもガイドライン全般に渡り、同様の表現あり	規程及び業務プロセスを見直した（レビューした）結果、それらの変更が必要ないという結論に至ることもあると考えられます。その場合でも、見直しの中で行った検証の十分性や結論の合理性を疎明できるようにしておくことが望ましいと考えられます。
82	2.1.2.①	「セキュリティ・バイ・デザイン」については、システム企画・開発全般に関する概念であり、一般のセキュリティ・システムリスク等も含む理解であるため、サイバーセキュリティに係る規程等の内容として挙げることに違和感がある。 また、「物理的セキュリティ」「サードパーティリスク管理」など、サイバーセキュリティに限らないシステムリスク全般・委託先管理全般に含まれる事項も見受けられる。 これらに関して、組織内の規程等のいずれかで確保すれば足りるという理解で	本ガイドラインは、内部規程の体系について特定の形を指定するものではありません。例えば、サイバーセキュリティに関する規程等において、他の関連規程を参照することも考えられます。

		よいか。例えば、サイバーセキュリティに係る規程類ではなく、他の規程体系の中で触れることでも差し支えないか（その場合、「経営陣は」や「少なくとも１年に１回」といった記載に、他の業務分野の規程類も引っ張られてしまう懸念はあるものの、サイバーセキュリティの規程類だけがいたずらに複雑化しないよう、内部規程の体系面について伺いたい）。	
83	2.1.2.①	規程等に含めるべきとして例示している「例えば以下の事項」について、もう少し内容を細分化できると、これから対応を進める金融機関にとって、より対策が充実するのではないかと思料するので、踏み込んだ観点や考え方を伺いたい。 例えば、「インシデント対応及び復旧」には、関係当局への報告や対外公表なども要素として含まれるのではないか。	詳細について、本ガイドラインの関連する項目も参照のうえ、規程等において規定することが考えられます。インシデント対応及び復旧に関し、当局への報告や対外公表については、2.5.2.3 節もご覧ください。
84	2.1.2.①	本項目で挙げられる例示に関しては、並列に羅列されているが、実施に対してのハードルなどが異なると考える。例えば、 （１）ペネトレーションテストのような負荷の高い対策は、必要性の程度や費用対効果が考慮されるべきである。 （２）技術的対策（物理的セキュリティ、ネットワークセキュリティ等）については、導入後は恒常的・自動的な対策となり、担当が手を動かす性質のものではないため、マニュアル等の規程類に馴染まない面がある。 こうした観点も含め、(a)上記（１）（２）について具体的にどのような事項を規程等に盛り込むことを想定しているか。また、(b)どのような程度感で規程類に盛り込むか否かなども、リスクベースや自組織の既存の規程類との平仄等が考慮されるものと考えてよいか。	（(a)について）詳細について、本ガイドラインの関連する項目（例えば、ペネトレーションテストについては 2.2.4 節、技術的対策については 2.3.4 節）も参照のうえ、規程等において規定することが考えられます。 （(b)について）ご指摘の平仄の点に加え、例えば、既存の規程類との差異を分析し、自組織において足りない点で、反映が必要なものなども考慮することなども考えられます。
85	2.1.2.①	規程等に含めることを求める「セキュリティ・バイ・デザイン」とは、具体的には 2.3.4.3.に述べられている事項という理解で相違ないか。	主要なものとしては、ご認識のとおりです。
86	2.1.2.①	「サードパーティ」（という用語）は p.1 に記載がある。脚注の記述位置を変	ご指摘の脚注は、「サードパーティ」という用語の初出時に

		更してはどうか。	付すように修正いたします（ガイドライン 1 頁は「サードパーティリスク管理」という表現になっています）。
87	2.1.3.①	サイバーセキュリティ担当部署等に専門性を有する人材の配置とあるが、マネロンと同様のレベル感（専門部署または専任者を配置する）を想定しているのか？金融機関ごと組織態勢要員の状況は異なると思いますが、ある程度の指針があった方が、専任態勢を取っていない金融機関にとっては態勢の見直しがし易いと思われます。	貴重なご意見として承ります。金融機関等の規模・特性は様々であることから、サイバーセキュリティにかかる専門部署や専任者を配置することについて、一律の対応を求めるものではありません。参考文献として、「サイバーセキュリティ体制構築・人材確保の手引き」第 2 版に関連スキルの記載があります。
88	2.1.3.①	「経営陣は、サイバーセキュリティの重要性を踏まえた上で、サイバーセキュリティ担当部署等に、専門性を有する人材を配置し、また、必要な予算を配分するなどにより、適切な資源配分を行うこと」とある。 （１）「専門性を有する人材」の定義はあるか。自組織内で当該人材を配置することが困難である場合、外部専門家の出向を受け入れる、常駐の業務委託を活用する、といったもののほか、自組織への直接の配置ではなく外部ベンダー等の活用をもって専門性を確保する対応でも問題ないか。 （２）「必要な予算を配分するなど」の「など」について具体的に想定する内容があれば伺いたい。	（(1)について）ご指摘のような対応が排除されるものではありませんが、本ガイドライン 2.1.3.②に記載の事項との整合性について留意する必要があると考えられます。 （(2)について）適切な資源配分の例としては、2.1.3①に挙げたもののほか、組織体制の整備、物品またはサービスの購入、導入等も挙げられます。
89	2.1.3.②	内部人材の育成については重要な課題であるが、人事異動の在り方を含めた育成手法は様々であると考えている。例えば、特定の業務に中長期的に配置することで専門性が高まるケースのほか、ローテーションにより幅広い視点を持った人材の育成ができるケース・複数の人材が育つケースなどもある。 本項目では、「資質・意欲のある職員に対し、人材育成を阻害するような人事異動を避け、人材育成の観点から中長期的かつ計画的に人事配置を行い」とあるが、各組織の特性・人員余力や対象職員の人材特性などによって、実現の仕方は異なり得るという理解でよいか。	ご理解のとおりです。
90	2.1.3.④	様々な規模の金融機関がある中で、「フォレンジック調査」や「脆弱性診断やペ	ご理解のとおりですが、リスク受容については、代替措置、

		ネトレーションテスト」等も含め、こうした専門的な業務を行う人材を網羅的に確保していくことは困難と思料する。 他方、本ガイドラインの前提がリスクベース・アプローチで、規模・特性にかかわらず一律に対応を求めるものではないほか、本項目でも「例えば」と例示しているものでもある。サイバーセキュリティの分野には、ここで挙げたような様々な業務があることを経営層が認識し、そうした業務・態勢の確保のために、外部リソース（ベンダー等）の活用も含め、一定の経営資源の投入が必要であることを示唆していると理解すればよいか（そのうえで、リスクを念頭にどの程度の人材を確保するか/できるか、確保できない場合には、その結果のリスクを受容するのかといった判断が経営層の役割になると理解すればよいか）。	リスク低減措置（残余リスクのモニタリングを含む）の検討も重要だと考えられます。
91	2.1.3.④	本項目の「フォレンジック調査」については特に注釈がないが、「2.3.2.a.」の脚注 32 の内容と同義との理解でよいか。	ご理解のとおりです。ご意見を踏まえ、初出時に脚注を移動しました。
92	2.1.4.①	「業務部門等から独立した立場から監視、牽制を行う」とありますが、会社によっては業務部門である IT 企画部門の中にリスク管理部門を設置しているケースがありうることから、そのようなケースが許容されるのであれば、明記していただけないでしょうか。	ご指摘のようなケースにおいては、リスク管理部門による監視・牽制について、業務部門からの独立性が担保されるような措置を講じる必要があると考えられます。
93	2.1.4.①	「業務部門等から独立した立場から監視・牽制」について、「独立した立場」を満たす基準は具体的にどのようなものか。例えば、業務部門とリスク管理部門は部門長や担当役員を別にしなければならない、といった必要があるのか。 また、本記載は３線防御を念頭に置いたものと思うが、中小金融機関はリソースが限られており、例えば、システム部門内において、「サイバーセキュリティ管理に関する担当部署」としての役割と、サイバー分野における２線的役割（サイバーリスク管理）を担っているケースもある。 ここで重要なのは、組織全体として、けん制機能を含めたサイバーセキュリティの態勢確保であって、その在り方は、規模・特性によって異なり得ると理解すればよいか。	金融機関等の規模・特性は様々であることから、一律の組織体制を求めるものではありません。

94	2.1.4.②	リスク管理部門から CRO・取締役会等への報告頻度はどの程度が適切か。 担当部署からの経営陣への報告は「2.1.1.基本的な対応事項 8」で言及されており、「少なくとも 1 年に 1 回」と記載されているが、同等の頻度が想定されるか。	ご理解のとおりです。
95	2.1.4.②	【基本的な対応事項】に記載の「リスク管理部門」は、会社によっては「IT 企画部」が所管しているため、2 の報告先（リスク管理担当役員）は CIO となるケースがあります。必ずしも所管する担当役員が CRO でないケースがあるため「CRO」を削除いただけないでしょうか。	ご指摘を踏まえ、「CRO 等」と修正いたします。
96	2.1.4.a	リスク管理部門に配置することが望ましい「サイバーセキュリティに係る適切な知識及び専門性等を有する職員」については、「2.1.4.①」で挙げられている「サイバーセキュリティ管理態勢が有効に機能しているかについて、業務部門等から独立した立場から監視・牽制を行う」役割を担える知識・専門性等を期待していると理解したが、認識に相違ないか伺いたい。 求められるのは監視・牽制のために必要な範囲のサイバーセキュリティに係る知識・専門性等（脅威動向や法令規制動向の把握や、自組織内部の手続きの適切さの判断に資する知見等）であって、サイバーセキュリティ対策の部門と同等の専門知識（サイバーセキュリティに特化・深堀りした知見）が望まれているというわけではないという理解でよいか。	本項目はサイバーセキュリティに関してより実効的な監視・牽制（2 線機能）を確保するうえで、リスク管理部門（2 線）にサイバーセキュリティに関する知識及び専門性等を有する職員を配置することが先進事例のひとつとして認められたことを踏まえたものです。リスク管理部門の職員のサイバーセキュリティに係る適切な知識及び専門性等は、サイバーセキュリティ担当部署における知識及び専門性等と必ずしも同じであるとは限らないと考えます。
97	2.1.5.	内部監査において、外部専門家を利用する場合システム監査と脆弱性診断等を行う業者は同一業者でも問題ないか。	個別・具体的な状況に応じて検討すべきですが、一般論として、監査と脆弱性診断が不適切に影響を与え合わないように、両者の独立性を確保する必要があると考えられます。
98	2.1.5.①	内部監査は、サイバーセキュリティに限らず業務全般に対して行われるものであり、例えば、その時々の重要テーマなども踏まえて、項目や特に深掘りする監査テーマなどが検討される。 本項目の目的は、サイバーセキュリティの担当部門における対策以外にも、「内部監査」を通じて組織全体でサイバーセキュリティを確保することにあると推	ご認識のとおりです。

		察する。その事業年度に、何をテーマとするかも含め、本項目で挙げられた事項を、内部監査の項目・テーマに一律に当てはめるものではないとの認識でよいか。	
99	2.1.5.a	対応が望ましい事項として専門性を有する要員の配置の代替手段として、専門性を有する団体からの外部監査を受けることを選択肢の一つとして加えてもよいと考えます。	貴重なご意見として承ります。「基本的な対応事項」において、必要に応じて外部専門家を利用することについて記載しております。内部監査に加えて、外部監査を受けることを排除するものではありません。
100	2.2.	「2.2. サイバーセキュリティリスクの特定」においては、サイバーセキュリティに係る人的な（従業者および業務委託先に対する）リスクの特定も盛り込むべきである。 特に、一部の外国においては、法律によって企業や国民に諜報活動への協力が義務付けられているため、当該の外国法の影響下にある従業者および業務委託先については、「サイバーセキュリティリスク」がある。そのため、当該の外国法の影響下にある従業者および業務委託先を把握・特定し、リスクとして管理する必要がある。（これは、当該の外国法に対応する対処策であって、人種差別や国籍差別ではない。）	貴重なご意見として承ります。ご指摘の点は、ガイドラインの 2.2.2.2.③の内容に対応するものと考えられます。
101	2.2.1.	フリーソフトウェアの使用状況を把握していないと脆弱性のある Log4j や MySQL などを知らずに使用しつづけてサイバー攻撃の対象となる危険性があるため、フリーソフトウェアに関しても使用状況の管理対象として明記してもよいと考えます。	貴重なご意見として承ります。フリーソフトウェアに含まれる Log4j などのオープンソースソフトウェアについては、2.2.1.2.e をご参照ください。
102	2.2.1.	最新の状態を網羅的に把握できるようにするためにも、台帳等には「パッチ(修正プログラム)適用状況」を含める方が望ましいと考えます。	貴重なご意見として承ります。脆弱性管理上、パッチの適用状況の把握は必要ですが、資産管理台帳にパッチ適用の状況を含めるかどうかは、金融機関において判断すべき事項と考えます。
103	2.2.1.	侵入経路を正しく把握していない、できないことで適切な設定をせずにサイバ	ご指摘の点は、ガイドライン 2.2.1.4.①の内容に対応する

		一攻撃を受ける事例が多いことから、インバウンド、アウトバウンド通信は可視化したうえでどこにリスクがあるのか把握し、適切な対応を促すことを基本的な対応事項として加えてもよいと考えます。	と考えられます。
104	2.2.1.	脚注 18 で「情報資産とは、①情報システム及び外部システムサービス（外部委託先、クラウドサービス）、②その構成要素であるハードウェア・ソフトウェア等及び保管される情報（データ）並びに③ネットワークを指す」とある。 外部委託先、クラウドサービスは、所有権という観点では、金融機関の情報資産に含まれないと思料するが、その理解でよいか。例えば、「外部委託先が受託業務遂行上保有している自組織の情報」や「クラウド内の自組織のデータ」を意図しているのか。	外部委託先が受託業務遂行上保有している自組織の情報やクラウド内の自組織のデータも、金融機関が管理すべき情報資産に含まれます。
105	2.2.1.1.	2.2.1（情報資産管理）or 2.2.2（リスク管理プロセス）に、ASM 関連の要件を追記してはどうか。例えば、unknown 資産（シャドーIT）にもケアし、domain take over されてフィッシングに悪用されないように、企業側は備えるべきではないかと考える。 2023 年 5 月に経済産業省から ASM 導入ガイダンスが提示されており、ASM ツールによるインターネット公開システムの情報収集・分析、リスクスコア化は、自社/自社外に関わりなく資産把握できることは有用と思料。	貴重なご意見として承ります。ASM ツールの導入は有用と考えられます。
106	2.2.1.1.①	「～管理するための台帳等を整備し、メンテナンス手順を定めるなど、最新の状態を網羅的に把握できるようにすること」とありますが、「メンテナンス手順を定め」だけでなく「たな卸しを含むメンテナンス手順を定め」とし対応内容を具体化してはいかがでしょうか。 〇理由 最新の状態を把握するために「定期的なたな卸し」は必須となりますが、実態として取得／廃棄時の更新は行われているものの、実際の資産との突き合わせができていないケースが散見されるため、記載内容を具体化すべきと考えます。	貴重なご意見として承ります。最新の状態を網羅的に把握する手段として、定期的な棚卸その他手段が含まれ得ます。No.107 もご参照ください。

107	2.2.1.1.①	「台帳等を整備し、メンテンナンス手順を定める」とあるが、「メンテナンス手順」とは、具体的に何（どのような作業）を指しているか。システム導入時や更改時等、システム構成に変更があった都度、台帳を最新化すれば足りると認識しているが、それ以外で考慮すべき点があれば、お示しいただきたい。	「メンテナンス手順」とは、情報システム及び外部システムサービスを適切に管理するための台帳等を維持・更新する手順です。例示されている点のほか、企業の規模・特性に応じてリスクベースでご判断いただくことになりますが、例えば、台帳の更新漏れのリスクを低減するために定期的な内容確認（棚卸）があります。また、例えば、メンテナンスを複数部署で実施し、統括部門が一括管理する場合には、そうした点を踏まえた手順を定める必要があると考えております。
108	2.2.1.1.①	台帳管理に係る「最新の状態」とはどの程度を指すのか。台帳管理の重要性は認識しているものの、リアルタイムでの更新は承認プロセス等を勘案すると実務的に負荷がかかるほか、外部システムサービスについて、委託元側が常に最新の状態を把握することは相当の困難を伴うことが想定される。 例えば、金融機関内のシステムは、システム更改後●●以内に更新する、外部システムサービスは●●の頻度で更新するといったように、システムやネットワーク、内製/外製などに応じて運用することも許容されるのか。 これらについても、リスクベースで、規模・特性等を踏まえ各々の金融機関で考える事項という理解でよいか。	リスクベースで判断するべきものと考えられます。どのような前提かにもよるため、ケースバイケースであり、例えば、深刻な脆弱性が明らかとなった場合に対応できるのかという観点からも考慮する必要があると考えられます。
109	2.2.1.1.①	「網羅的に把握できる」とは、対象システムが一覧化されており、俯瞰的に確認できることを指すという理解でよいか。	ご理解のとおり、情報システム及び外部システムサービスが一覧化され俯瞰的に確認できることを指します。
110	2.2.1.1.①	「下記 2.2.1.2 節」と下記という記述がございますが、「下記」と「節」の利用としてはあまりふさわしくないので、2.2.1.2.　ハードウェア・ソフトウェア等及び 2.2.1.3. 情報（データ）のような記述の方がよいかと思います。	ご意見を踏まえ、修正いたします。
111	2.2.1.1.① 2.2.1.2.① 2.2.1.3.①	例えば、協同組織金融業態のように、個別金融機関が業態センタや共同システムを利用している場合、個別金融機関が当該業態センタ等の情報資産を直接把握することは現実的でなく、管理に必要な情報の報告を受ける対応などが考え	リスクベースで判断するべきものと考えられます。

	2.2.1.4.①	られる（協同組織金融業態でない場合でも、共同利用型サービスなどにおいて同様と考えられる）。 この場合、「情報システム及び外部システムサービスを適切に管理するための台帳等」「ハードウェア及びソフトウェア等を適切に管理するための手続・台帳等」「顧客情報や機密情報等を適切に管理するための台帳等」の整備等あるいは「データフロー図・ネットワーク図」作成等にあたって、サービス提供元が個別金融機関へ提供すべき情報はどこまでの範囲になるか、何らかの水準や目線があるか（個々の金融機関ごとに要求水準が異なる場合、提供情報範囲の特定に苦労すると考えられるため）。	
112	2.2.1.1.① 2.2.1.2.① 2.2.1.3.① 2.2.1.4.①	台帳等の整備管理等に関して、外部システムサービスは情報公開に消極的なケースも多く、限界があるように感じられる面もあるが、このような場合の代替策があれば伺いたい。どうしても把握できない場合は、当該サービスをどのような業務に利用しているかも含め、利用適否のリスク判断をすることになるか。 また、(特にクラウドサービスなど) 金融機関のサードパーティであって、サービス利用金融金融機関に対しての情報提供に消極的な事業者に、行政から働きかけることも検討いただきたい(本ガイドライン案 2.6.の冒頭記述でも触れられているが、特に外部委託先でないサードパーティについて、民間側での対応の難しさがある)。	前段について、把握できない場合は、ご指摘のように、外部システムサービスをどのような業務に利用しているかの確認を含め、利用適否の判断を行うことになると考えられます。 後段について、貴重なご意見として承ります。2.6 節冒頭に記載のとおりです。
113	2.2.1.2.①	「最新の状態を網羅的に把握できるようにすること。台帳等には、以下の項目を含めること。」とありますが、以下のようなハードウェア情報も含むようにしてはいかがでしょうか。 ・ハードウェアの場合、製品名や型番情報 〇理由 保有している製品の脆弱性など問題については、ソフトウェアバージョンだけでなく製品名などから検知することも考えられるため	貴重なご意見として承ります。

114	2.2.1.2.①	「管理を外部委託している自組織の資産を含む」とは何を意図した記載か。「2.2.1.2.対応が望ましい事項b.」で「サードパーティの資産」について触れられているため、別の論点と思われるが、「2.2.1.2.対応が望ましい事項b.」との違い等について伺いたい。	本項の「管理を外部委託している自組織の資産」は、例えば、保守管理を外部委託している自組織の資産を指します。一方、2.2.1.2.対応が望ましい事項 b.の「サードパーティの資産」は、所有権がサードパーティにある資産が該当します。
115	2.2.1.2.①	本項目では、サードパーティが保有するハードウェアおよびソフトウェアの管理までは求められていないとの理解でよいか。	ご理解のとおりです。
116	2.2.1.2.①	「2.2.1.2.基本的な対応事項①」における台帳管理等の範囲は情報システム（自組織の資産）であり、外部システムサービス（外部委託先、クラウドサービス）の資産は含まないという理解でよいか。	本項目は、ハードウェア・ソフトウェア等に係る項目であり、情報システム及び外部システムサービスについては、2.2.1.1節をご参照ください。
117	2.2.1.2.a	脚注 21 の「特定用途機器」にはどこまでの機器が含まれるのか判断に迷う懸念があるため、本機器を管理対象とする趣旨を伺いたい（可能であれば、範囲の考え方も伺いたい）。 例えば、固定電話は通信回線（電話回線）に接続されていて、発受信履歴などを確認できるが、これを含めることに違和感がある。このほか、電卓に内蔵電磁的記録媒体が備わっているものや、通信回線に繋がっているスピーカーなども、定義のみを字面通り読むと含まれてしまうかもしれないが、これらも違和感がある。 また、脚注 21 で挙げられている「ネットワークカメラシステム」「入退管理システム」「施設管理システム」などに関しては、自組織の事務所が入居する建物の設備として備わっている場合もあり、これを自組織が管理対象とすることも、建物管理者との契約上の取り決めによって難しい場合があると考える。	リスクベースで検討すべきであり、範囲等を一概にお示しすることは困難です。
118	2.2.1.2.b	サービス提供型のサードパーティの場合、開示可能な情報が制限されるケースが多い状況です。例えば、2.2.1.2.b.について、パブリッククラウドの資産を管理することは難しいと考えますので、開示制限されることはやむを得ないように記述を加えて頂きたいと考えます。	個別の状況に即して考えるべき事項であり、原案（2.2.1.2.b）では「必要に応じて」としていますので、原案のままとさせていただきます。なお、一般論として、ご指摘のような開示が制限される場合においては、サービス提

			供事業者による管理状況の適切性について、契約書や第三者保証による報告書、同事業者から提供される報告書等により確認し、こうした代替措置によって、リスクを許容できるかどうかについて検討することが必要と考えられます。
119	2.2.1.2.b	サードパーティの資産を管理対象とすることは難易度が高いと思われ、このため「対応が望ましい事項」にされていると思料するが、本項目記載の「必要に応じて」とは具体的にどのような状況を想定しているか、想定があれば伺いたい。	脅威動向や重要な業務に関連する資産との関連等を踏まえ、判断することを想定しております。
120	2.2.1.2.b	サードパーティの資産を管理する、という概念について、リスクベースであることは当然として、どのような管理を想定しているか説明があってほしい。基本的には契約に基づく関係であり、資産を管理する権限があるケースは非常に限定的と考えられる。	2.2.1.2.①に記載の内容による方法が考えられるほか、例えば、リスクの高いと判断した資産について、具体的な製品情報等を把握することが考えられます。また、第三者保証による報告書（SOC2 など）や契約書等を活用することが考えられます（2.2.3.⑥参照）。
121	2.2.1.2.b	「必要に応じて、サードパーティの資産についても管理対象とする」とあるが、望ましいと考えられる管理基準や管理対象とする資産の範囲について、想定があれば例示いただきたい。 また、設定する管理基準によっては、各種法令（個人情報保護法や不正競争防止法、著作権法等）に抵触する可能性があるため、サードパーティとの契約締結時に十分に内容確認が必要であることを注記してはいかがか。	前段の点については、脅威動向や重要な業務に関連する資産との関連等を踏まえ、判断することを想定しております。 後段の点については、貴重なご意見として承ります。ご指摘のように、各種法令との関係も考慮することが必要と考えられます。
122	2.2.1.2.d	本項目で求める事項は、 ・自機関の管理対象外となっている個人所有端末等の情報資産（個人所有のPC、スマートフォン、USB メモリ等）から自機関のネットワークにアクセスできないように制御すること、 ・自機関の管理対象端末から未承認のクラウドサービスの利用を制御することの２点だと解釈した。 この認識が合っている場合、管理対象とするか使用中止を求めるのではなく、	貴重なご意見として承ります。管理対象とすることには、アクセス・利用の制御を求めることも含まれると考えます。

		アクセス・利用の制御対応を求めることを、より明確に表現してはいかがか。	
123	2.2.1.2.e	「ソフトウェア部品表 （SBOM、Software Bill of Materials）を整備すること」については、金融機関の有するシステムや機器の幅広さと多さ、管理上で依存関係も考慮することなどを念頭に置くと、非常に難しい作業に思われる。例えば、全てのソフトウェア部品表ではなく、優先的にサイバーセキュリティリスクの高いシステムや重要システム等を対象として取組みを開始すること、取り組んだ結果、全体の管理が困難である場合、重要性も考慮して自組織が管理継続できる範囲で取り組んでいく対応でも差し支えないという理解でよいか。	貴重なご意見として承ります。SBOM による管理のほか、先進事例としては、構成要素分析を併せて活用することも挙げられます。リスク受容に係る判断や残存リスクの管理は各金融機関において行う必要があります（2.2.2.3 節参照）。
124	2.2.1.3.①	本項目で台帳等整備の対象とされる「情報」の対象としては、自組織の情報システムに保管している情報のほか、外部システムサービスに保管している情報も含むという理解でよいか。	ご理解のとおりです。
125	2.2.1.4.①	2.2.1.4 において、データフロー図・ネットワーク図の作成を求めているが、ソースコードや設定値等から最新の情報が確認できるのであれば、必ずしも図を作成することは必要とされないと考えられ、また、最新の状態も確認することも可能であると考えられる。また、設計と実装が食い違う可能性もなくなることから、データフロー図やネットワーク図の作成を必須とするのではなく、最新のデータフローやネットワークを把握できる仕組み、のような表現に変更することはできないか。	貴重なご意見として承ります。ご指摘のような方法も本項目に含まれると考えられます。
126	2.2.1.4.①	データフロー図・ネットワーク図について、当局で想定している具体的なレベル感はあるか。もし可能であれば、図のサンプル等をお示しいただけると、金融機関・ベンダー間での意思疎通が図りやすいのでご検討いただきたい。 あるいは、本項目に関してもリスクベースでの判断が前提であって、範囲・粒度等も含め、システム・業務の重要度や各金融機関の規模・特性によって異なり得るものか。	データフロー及びネットワークの適切な管理のため、最新の状況を把握できるようにするために用いるデータフロー図、ネットワーク図、メンテナンス手順などは、金融機関によって様々であり、一律のものを想定しているものではありません。

127	2.2.1.4.①	データフロー図・ネットワーク図に含める内容の範囲について、業態によっては、多段階の接続構造（例：業態センター経由、業態のオープン基盤経由など）になっているケースや、サードパーティの情報を十分に取得できないケース（特に、クラウドサービスなど）が想定される。 また、含める内容が多いほど、図の内容が重厚になり、定期的な更新が難しくなる懸念もある。 本項目に関して、内容の範囲・深度などを含め、金融機関の規模・特性に応じ、リスクベースでの取組みになるとの理解でよいか。	データフロー図、ネットワーク図、メンテナンス手順手段などは、金融機関によって様々であると考えられますが、いずれにしても、データフロー及びネットワークの最新の状況を把握し、管理するうえで適切なものである必要があります。
128	2.2.2.	評価結果をリスク管理部門など適切な部門に報告することまで明示した方がよいと考えます。	ガイドライン 2.1.1.⑧において、経営陣は、少なくとも１年に１回、リスク評価の報告を担当部署等に求めることが記載されています。これは、経営陣に対する報告に限らず、関連部署にも報告すべきと考えられます。また、報告を年１回に限定する趣旨ではなく、より頻度の高い報告が行われることを妨げるものではありません。また、重要なリスクが認められた場合には迅速な報告が行われるべきと考えられます。
129	2.2.2.	「2.2.2.リスク管理プロセス」全体に関して、一義的なリスク管理主体は自組織であると理解しているが、具体的な対応を行う際には外部ベンダーに依頼することなども想定される。 例えば、「2.2.2.1.脅威情報及び脆弱性情報の収集・分析」のうち、「基本的な対応事項 2」については、具体的な対応としては、情報資産の管理・運用等を委託しているベンダー等に脅威情報を提供して対処依頼をすることが考えられ、自組織自身のみですべての対応を行うものではないと想定される。 このように、（本項目以外でも同様であるが、）外部ベンダー等の役割・活用を念頭に置いて、自組織のサイバーセキュリティを確保するということで問題ないと考えているが、認識相違ないか。	外部委託先や外部ベンダーに対する統制、管理の責任が金融機関にあることを前提として、必要に応じ、こうした外部リソースを活用し、自組織のサイバーセキュリティを補完、強化することが考えられます。

130	2.2.2.1.③	「情報の収集元及び収集・分析の方法を少なくとも１年に１回は見直し、必要に応じて改善を図ること」とあるが、以下２点について伺いたい。 （１）収集元（収集元として想定すべき範囲）としては何が想定されるか（当方では、銀行等 CEPTOAR 情報や、業界システム組織、外部ベンダーなどを想定している）。 （２）収集元は継続的に利用しているものであって、頻繁に変わることは通常ないのだが、「少なくとも１年に１回は見直し」とは何を意図しているか。現状の収集元として、「どこがあるか」「どう活用できているか」を年１回は自組織として確認するよう求めるという意図か（結果、収集元や収集情報の活用方法が変わらないことは問題ないか）。	（(1)について）当庁として指定するものではありませんが、例示いただいたもののほか、金融 ISAC や JPCERT/CC 等も挙げられます。 （(2)について）ご指摘の確認事項も含まれると考えられます。例えば、自組織として対応が必要な脅威情報及び脆弱性情報であるにも関わらず、見落とされていた場合は、収集元及び収集・分析の方法の見直しが必要と考えられます。
131	2.2.2.1.a	脅威情報や脆弱性情報等の収集先として、次の組織をどのように捉えているか伺いたい。また、このほかに有益な組織があれば伺いたい。 ・FISC（特に会員として参加する場合） ・IPA（公表情報の活用等を想定） ・JPCERT/CC（特にポータルサイト「CISTA」を利用する場合） ・サイバーセキュリティ協議会	No.130 への回答をご参照ください。
132	2.2.2.1.b	「脅威分析を行う際に、過去に発生したことがないサイバー攻撃の脅威（ゼロデイなど）や、深刻だが現実に起こりうるサイバー攻撃の脅威を対象に含めること。」とありますが、「過去に発生したことがないサイバー攻撃の脅威（ゼロデイなど）」という表現は適切でしょうか？ 〇理由 まず、ゼロデイ攻撃の定義とも異なると思われます。 また、「過去に発生したことがない」というのが世間一般なのか当該組織なのかがはっきりしませんし、世間一般で発生したことがない攻撃を脅威分析するというのも非現実的に思われます。	ご指摘を踏まえ、「過去に発生したことがない場合でも、深刻だが現実に起こりうるサイバー攻撃の脅威を対象に含めること」と修正いたします。 「過去に発生したがない」という点については、自組織では起こっていないが同業他社/他分野で起こったサイバーインシデントや、サイバー攻撃を起因としないものを含め過去に起こったインシデントを参考にすることが考えられます。
133	2.2.2.1.b	「過去に発生したことがないサイバー攻撃の脅威（ゼロデイなど）」とあるが、過去に発生していないサイバー攻撃について、どのように脅威分析をするべき	No.132 への回答をご参照ください。

		か、想定している脅威の把握方法を含めご教示いただきたい。 あるいは、本項目は、ゼロデイによる具体的な脅威の内容を想定するのではなく、例えば、（どのようなゼロデイ攻撃かは置いておいて）ゼロデイ攻撃によって、自組織が利用するセキュリティ製品がセキュリティ機能を発揮しない（すり抜けられてしまう/脆弱性を悪用されてしまう）といった場合を想定する（そういう机上での頭の体操をする）ことを趣旨としているのか。	
134	2.2.2.2.①	「サイバーセキュリティリスクの特定・評価を行う体系的な手法や枠組みを構築すること」とは具体的にどのようなことか。何らかのフレームワークを参照して、特定・評価すればよい、ということか。フレームワークを参照して評価する、というルールを制定すればよいか、それとも、そのフレームワーク自体を規程化する必要があるかも含め、ご教示いただきたい。 また、本項目は、表現が抽象的だと感じるが、どのような状態が「体系的」「構築」ということになるのかご教示いただきたい（複雑なことを要求されているように感じる）。参考になる資料等があればあわせてご教示いただきたい。	ご指摘を踏まえ、「サイバーセキュリティリスクの特定・評価に係る手順を定めること。」と修正いたしました。2.1.2.①に規定するサイバーセキュリティのリスク評価に係る規程及び業務プロセスに準じた手順を定めるという趣旨です。
135	2.2.2.2.③	情報セキュリティではなく「サイバーセキュリティ」に関するガイドラインという名称であるにも関わらず、サイバー範疇ではない内部不正への言及（2.2.2.2.③）がある点に違和感がある。	サイバーセキュリティを確保する上で、内部不正の脅威を考慮することも重要であると考えられます。例えば、経済産業省・独立行政法人情報処理推進機構による「サイバーセキュリティ経営ガイドライン Ver3.0」の「指示４　サイバーセキュリティリスクの把握とリスク対応に関する計画の策定」においても、「事業に用いるデジタル環境、サービス及び情報を特定させ、それらに対するサイバー攻撃（過失や内部不正を含む）の脅威や影響度から、自組織や自ら提供する製品・サービスにおけるサイバーセキュリティリスクを識別させる。」と記載されております。
136	2.2.2.2.③	リスク評価について、「境界防御型セキュリティが突破されるリスクや内部不正などの脅威も考慮し、内部ネットワークセグメントに設置したシステムへのリスクも対象とすること」とされている。	ご記載いただいた防御の観点に加え、境界防御型セキュリティが突破された場合や内部不正が発生することを想定したインシデント対応の観点でのリスク評価も重要と考えま

		この点、具体的リスク評価の手法として、ネットワークの境界防御対策の頑健性（回線の安全性の度合い、ネットワーク機器の脆弱性管理の適切性、通信制御の適切性、不正侵入の検知・防御機能の十分性等）や内部不正防止対策の十分性（システムへのアクセス制御やユーザーの認証情報管理の十分性・適切性等）について、ゲートウェイ毎に現行の取組みを評価し、足らざる部分（残存リスク）を明確にすることを考えているが、そうした対応で問題はないか。また、このほか留意する点があれば伺いたい。	す。
137	2.2.2.2.b	「深刻だが現実に起こりうる多様なシナリオ」について解釈が難しいため、想定されている事例があれば例示いただきたい。	No.132 への回答をご参照ください。
138	2.2.2.3.①	「2.2.2.3.リスク対応」の「基本的な対応事項 1」で、リスク対応の方針として「回避」「軽減」「受容」「移転」があげられている。ここで挙げられる通り、残存リスクについてどのように扱うか（受容も含む）を経営の責任のもとで判断することが、リスク対応にあたっては重要であると理解している。 事務システムリスクに関して「ゼロリスク」にすることは極めて困難であるが、経営層からするとリスクを無くすよう指示したくなる面もある。 本ガイドラインを運用していく際に、リスクをゼロにすることは困難であるという前提や、それを踏まえて(a)自組織の投入可能なリソースの範囲で低減を図ること、(b)残存リスクについて許容範囲を確認して受容することが、経営としての役割であることについて、認識を深めることが重要と感じた。検査・監督・モニタリング等にあたっても、こうした観点を持ち、建設的な対話が図られることを期待したい。	賛同のご意見として承ります。
139	2.2.2.3.②	「2.2.2.3. リスク対応」における例外事項について、一律、「承認を得ること」とされている。 承認については、例えば事後的な確認でもよいのか。	少なくとも１年に１回実施するサイバーセキュリティリスクの評価（ガイドライン 2.2.2.2.②を参照）を前提とすると、当該リスク評価をもとにリスク対応計画が策定されると考えられるため、リスク対応計画の適切性を確保する観点から、事後的な確認ではなく、事前に承認を得ることが適当と考えられます。

140	2.2.2.3.②	通常、サイバーセキュリティ対応において、様々なリスクをゼロにすることは困難であると想定されるが、ここで言う「例外的な取扱い」や「リスク受容」となるレベル感を認識したく、具体的な例をご教示いただきたい。	リスクベースで検討すべきであり、水準を一概にお示しすることは困難です。
141	2.2.2.4.b	KPI や KRI として設定すべき内容や、具体的な目標及び達成指標については、「2.1.1.対応が望ましい事項 d.」の脚注 15・16 の内容が想定されているか。このほかに想定されている事項があれば伺いたい。 また、改善活動が実効性のあるものになるよう、いたずらに KPI や KRI を多数設定するのではなく、自組織にとって相対的に弱い部分（演習やサイバーセキュリティセルフアセスメントなどで認識することが考えられる）についてピンポイントで設定することも有効と思うが、その対応でも差し支えないか。	一点目のご質問については、2.1.1.d 脚注の指標のほか、目標の達成状況を確認できるものが考えられます。 二点目のご質問については、サイバーセキュリティ管理態勢の一部分に対して設定した指標が、全体を表しているかのような誤解を招かないように留意すべきと考えられます。
142	2.2.3.③	″例外的にパッチ適用等の対応を実施しない場合には、実施しないことと実施しないことのリスクについて経営陣等から承認を得ること” となっている。ハードウェア・ソフトウェアでは利用されているミドルウェアを含めると多くのぜい弱性管理対象がある。これらに日々発見されるぜい弱性及びパッチについて、適用の可否判断（含む例外）について、都度、経営陣等から承認を得ることを必要とする際には、運用管理が非効率化され、リスクの増加につながりかねない。たとえば、②におけるぜい弱性対応の要否が必要とされたうえで、特定のパッチ適用をできない場合、ワークアラウンド適用が必要になる。しかし、前者の判断に都度、経営陣が関わっていては、後者のワークアラウンド適用の準備及び適用に遅れが生じる。ぜい弱性自体はなくなっていないため、手つかずのリスク自体が残存することになりかねない。 事前のパッチ適用の基準に従って、「パッチ適用等の対応」ではなく②と整合を取る形で「ぜい弱性管理の対応」とすべきではないか。 また、「等」と書いてあるが、日々の運用に経営陣の判断を必用とするようにもみえる。この場合、「1.2.1 サイバーセキュリティ管理態勢」において懸念されていた 「形式的に準拠することのみを重視したリスク管理態勢」につながり	状況に応じて、CISO といった然るべき責任者による承認を含意するために「経営陣等」と記載しています。

		かねない。適切な権限委譲を前提にするような項目を設けていただきたい。	
143	2.2.3.③	「パッチ適用等」の「等」は何を想定しているか伺いたい（パッチが適用できない場合の回避策か）。	ご指摘のように、何らかの理由でパッチが適用できない場合の回避策を指します。
144	2.2.3.③	セキュリティパッチの適用については、深刻な脆弱性が判明した場合、システムへの影響を確認し対応したうえで、パッチの適用率等のデータを経営陣に報告し、その適否に関し判断を仰ぐことを考えている。 パッチ適用に関しては、速やかに行うことも重要であるが、適用した結果、他のトラブルが生じる懸念もあるため、判断に幅が出ると考えている。経営によるリスク判断という観点から、上記のような対応も、本ガイドラインの趣旨に沿っていると考えているが、その理解でよいか。	脆弱性の重要度にもよるため、ケースバイケースと考えられます。例えば、深刻かつ機密性・可用性・完全性に重大な影響のある脆弱性であるにもかかわらず、他のトラブルがあることをもって代替的な低減措置なしにパッチ適用を否とするか是とするかは慎重な検討が必要と考えられます。
145	2.2.3.③ 2.2.4.①	「リスクの高い構成」とは本項目で記載のある「業務系ネットワークとインターネット系ネットワークを分離していない」環境分離の論点のほか、どのようなものを含むか伺いたい。	金融機関等のシステム構成によるため、限定列挙は困難ですが、例示列挙しているものです。
146	2.2.3.④ 2.2.3.⑤ 2.2.3.⑥	「深刻度の高い脆弱性」という表現について、具体的な判定基準は定義されないのでしょうか （例えば、CVSS などの数値で判定するなど）。 それとも金融機関が独自に基準を定義するものなのでしょうか。	「深刻度の高い脆弱性」の基準を一概に示すことは困難ですが、一例として、ご指摘のように、金融機関等において、CVSS などの数値で判定することが考えられます。
147	2.2.3.⑥	重要なサードパーティーとしてクラウド事業者が含まれるのかどうか、明示的に記載した方が分かりやすいと考えます。	貴重なご意見として承ります。重要なサードパーティは、脚注に記載のとおり、「自組織として業務運営上重要と認識しているサードパーティ」を指し、クラウド事業者が含まれるかどうかは、ケースバイケースと考えられます。
148	2.2.3.⑥ 2.2.3.a	クラウド事業者に対する直接的な脆弱性対応の管理は現実的に不可能。責任共有モデルの概念と反しているように感じられる。(「管理」という言葉の定義が不明瞭なため、より踏み込んだ具体的補足、例えば『第三者保証による報告書等の活用した脆弱性対応状況の把握を含む』といったような補記があることが	「なお」以降で同趣旨の内容を記載しております。

		望ましい。） →2.2.3 ハードウェア・ソフトウェア等の脆弱性管理⑥におけるサードパーティの管理にも同様のことが言える。	
149	2.2.3.⑥ 2.2.3.a	サードパーティが保有するシステムとは、システム子会社やシステムベンダー、クラウドサービス事業者が自機関に提供するシステムやクラウドサービスのことではなく、サードパーティが自社で保有・使用するシステムのことで相違ないか。その場合、自機関に提供するシステムやクラウドサービスであっても「脆弱性対応状況につき非開示」とするサードパーティもあるため、自社保有システムに関してはよりその傾向が強くなり、本事項の達成が困難と推察する。 また、各種法令（不正競争防止法や著作権法等）やサードパーティと締結している契約に抵触しないよう、十分に内容確認が必要であることを注記してはいかがか。	ご指摘の項目における「サードパーティが保有するシステム」とは、システム子会社やベンダー等の外部委託先、クラウド等のサービス提供事業者等が保有するが、金融機関の業務のために金融機関に提供するシステムを想定しています。
150	2.2.3.⑥ 2.2.3.a	本事項で指す「脆弱性対応の管理」とは、サードパーティにヒアリングを行い、会社として脆弱性対応に係る回答を得るという対応で充足するか。その場合、第三者保証による報告書の活用等と同様に例示してはいかがか。 全サードパーティについて、個別の保有システムを洗い出し、それぞれの脆弱性対応結果を整理するのは非現実的であり、本事項は達成困難と考えられるため。	本項目は、全サードパーティではなく、重要なサードパーティについて規定したものです。第三者保証による報告書の活用については、本項目に記載のとおりです。
151	2.2.4.	留意事項に見合う業者の選定やテスト水準の担保を金融機関が個別にやっていくことは難しいと思料するので、例えば、認定された業者から選定することができるような仕組みの検討をお願いしたい。	ガイドライン 2.2.4.b もご参照ください。また、既存の認定制度を参考情報の一つとすることも考えられます。共助機関などで参考になる情報を収集することも役に立つ可能性があります。
152	2.2.4. 2.2.5. 2.2.2.3.	以下の項目について、定期的な実施について記載がありますが、「定期的」とは頻度の目安はどのくらいを指すのでしょうか。 2.2.4.脆弱性診断及びペネトレーションテスト	頻度を示すことが可能かつ有用と思われるものについては記載していますが、ご指摘の項目を含め、それ以外のものについては、それぞれの項目について、個別・具体的な状況を

	2.3.1. 2.3.2. 2.3.4.2.	2.2.5. 演習・訓練 2.2.2.3. リスク対応 2.3.1. 認証・アクセス管理 2.3.2. 教育・研修 2.3.4.2. ログ管理	踏まえて検討すべきものと考えられます。
153	2.2.4.①	対象機器として「Active Directory サーバ」が明記されていることは、昨今のサイバー攻撃の教訓から、より注意喚起することができるので、セキュリティ対策を進めて欲しい側からすると具体的で大変ありがたいです。 しかしながら攻撃の実態を見ると簡単な話ではなく、Active Directory の脆弱性は、システム自体の脆弱性よりユーザー等が作り出す設定構成の問題に起因することがほとんどです。 Active Directory についての本当の意味での脆弱性対策は、OS 等のシステム脆弱性に加えて、Active Directory アプリケーション設定および関連するデータの不備による脆弱性までカバーする必要があるため、そこまではっきりと明示することで、より具体的な注意喚起ができると考えます。またそれらの不備は気づかずに発生・存続する(内部犯行者による変更や、すでに潜伏済みの外部攻撃者による変更)ため、いわゆる単発の「診断」では不十分であり、継続的かつリアルタイムの監視が必要です。 26 ページに「継続的な監視を実施」という文言がありますが、それは攻撃行動に対するものだけではなく、上述の AD 設定やデータの不備にも適用すべきと強く考えますし、それをガイドラインのどこかに追加することを強く要望します。AD 不備が招く悲惨なサイバーセキュリティ事故はできるところから対策して、なんとしても防ぐべきです。	貴重なご意見として承ります。ご指摘の箇所の記載において、脆弱性診断の対象には、Active Directory サーバの設定や関連するデータの不備に関する脆弱性も含まれると考えられます。
154	2.2.4.①	脆弱性診断については、対象と必要な診断サービスについて記載があるものの、ペネトレーションテストについては「定期的な実施」と「重要性のあるものについては迅速に経営陣等に報告すること。」以外の言及がありません。脆弱性診断と同程度の留意事項の記載は不要でしょうか。	No.159 への回答をご参照ください。

		○理由 規模が小さい金融機関の場合、ペネトレーションテストの経験がほとんどないケースが想定されるため。また、どの程度のレベルのペネトレーションテストが必要なのか判断できず適切なサービス選択ができないように思われるため	
155	2.2.4.①	脆弱性診断やペネトレーションテストを実施するタイミングについての言及は必要ないでしょうか。例えば脆弱性診断は年１回、ペネトレーションテストは○年に１回または大規模なネットワーク更改を行ったタイミングなど。 ○理由 適切なタイミングで必要なテストが実施されない可能性が考えられるため。また、過度に診断やテストを繰り返しても、費用に対して有用な結果が得られれないことが想定されるため。	貴重なご意見として承ります。脆弱性診断については対象、ペネトレーションテストについては対象及び内容、いずれについても脅威の状況、システム更改の有無などによって必要な頻度は変わると考えられるため、一律に頻度をお示しすることは困難だと考えられますが、いずれについても状況を踏まえて適切なタイミングで実施すべきと考えます。また、一度だけでよいものではないため、適切な形で定期的に実施する必要があると考えます。
156	2.2.4.①	「定期的に」の具体的な期間について、適切なリスク許容度を判断したうえで、１年に１回より少ない頻度（例えば、２～３年に１回等）で実施する場合でも問題ないか。	No.155 への回答をご参照ください。
157	2.2.4.①	実施タイミングについて、「定期」だけではなく、システム更改時等に設計漏れ、設定漏れ等がないかを確認するために実施するタイミングで行う考え方もある。このように、定期のタイミングとは異なる時点で実施する場合、追加で定期分の実施は不要と考えるが、その理解でよいか。	リスクベースで検討すべきと考えられます。システム更改時等における実施を妨げるものではありません。
158	2.2.4.①	基本的な対応事項として留意する点として箇条書きされている箇所の１つに、プラットフォーム診断およびWebアプリケーション診断について記載されている。いずれも脆弱性診断に属するものと考えられるが、そのことを本文または脚注により明確にしてもらいたい。	ご指摘を踏まえ、修正いたします。
159	2.2.4.①	柱書には　脆弱性診断及びペネトレーションテストを定期的に実施することとある。他方、留意する点として箇条書きされている箇所では、最後の一文以	本項目の 5 つ目の箇条書きも脆弱性診断及びペネトレーションテストの両方に当てはまります。診断またはテスト対

		外はすべて脆弱性診断に関する記載である。 脆弱性診断とペネトレーションテストを別扱いしているが、留意する点として箇条書きされている箇所に対してペネトレーションテストへの言及を行うか、あるいは　基本的な対応事項からペネトレーションテストを除外するかのいずれかにしてもらいたい。これでは基本的な対応事項としてペネトレーションテストまで踏み込んで実施すべきか否かが判断に迷う。(いずれか、あるいは両方実施するかはリスクベースアプローチで、と云われればそれまでですが)	象のシステム等のリスクの大きさや重要度等を考慮した上で、脆弱性診断とペネトレーションテストのいずれかまたは両方を行うべきかをリスクベースで検討すべきと考えられます。
160	2.2.4.①	「リスクの高い構成」の例として、「業務系ネットワークとインターネット系ネットワークを分離していない場合」が示されているが、ネットワークが論理分離されている場合もリスクが高いとして想定しているのかを確認したい。なお、「リスクの高い構成」という言葉に定量性がないので、参考となるような指針があれば示していただきたい。	指標をお示しすることは困難であり、リスク評価は金融機関において行うべきものと考えられます。
161	2.2.4.a	「インターネットに直接接続していない VPN 網、内部環境も対象とすること」が【対応が望ましい事項】になっていますが、対象システムが直接インターネットに接続していなくてもコンテンツがインターネット経由で提供されるケースもあります。直接接続の有無に関わらず、提供するコンテンツのエンドユーザがインターネットを介する場合は、【基本的な対応事項】とするのも一つの案と考えます。	貴重なご意見として承ります。ご指摘のような場合についても、リスクベースで脆弱性診断等を実施することが重要と考えられます。
162	2.2.4.b	・TLPT は規模の小さな金融機関では過度の負担になるとも考えられ、システムの規模、特性を踏まえて実施有無を検討するような記載を加えてもよいと考えます。 ・【対応が望ましい事項】としても、本番環境を利用してかつ予告なく実施することは、業務運営を行いながらでは現実的に難しいのではないかと考えます。	貴重なご意見として承ります。 一点目について、TLPT は、「対応が望ましい事項」として記載しており、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、記載しております。 二点目について、適切なリスク管理策を講じた上で、本番環境においてブルーチームに予告することなく TLPT が行われ

			た例もあります。TLPT 実施上のリスク管理については、金融情報システムセンター「金融機関等における TLPT 実施にあたっての手引書」などが参考になると考えられます。
163	2.2.4.b	「テストは、本番環境を利用し、防御側の担当者（ブルーチーム）に予告することなく、実施すること。」 上記について、対応能力を評価するための理想的な TLPT では担当者に連絡なしで実施することが望まれますが、担当者以外への周知や調整など、いわゆるホワイトチーム側で考慮すべき事項についても記述してはいかがでしょうか。 〇理由 金融機関のような重要インフラにおいては、テストの影響でユーザーや業務へ及ぼす重大さの意味が他の業界と異なる部分があるため。	貴重なご意見として承ります。ガイドラインの本項目に参考として記載している以下の文献を参考にしていただくことが考えられます。 ・金融庁「諸外国の「脅威ベースのペネトレーションテスト（TLPT）」に関する報告書」（平成 30 年 5 月） ・金融情報システムセンター「金融機関等における TLPT 実施にあたっての手引書」（令和元年 9 月） ・金融庁「金融機関のシステム障害に関する分析レポート」（令和 6 年 6 月）別紙 1「コラム：金融機関における脅威ベースのペネトレーションテスト（TLPT）の好事例及び課題」
164	2.2.4.b	本項目で触れている TLPT について、ブルーチームの対応能力を図る有効性を確保したいという意図はわかるものの、「本番環境を利用し、防御側の担当者（ブルーチーム）に予告することなく」との記載については、事前説明なく実施した場合、混乱が生じる可能性がある。 字面通りに、本番環境・無予告で実施した場合、本物のインシデントが生じたと認識してブルーチームが動いてしまい、結果、TLPT で予定していない、経営への報告、緊急会議や対顧客サービス・業務の縮退判断、対顧客周知などが行われてしまう可能性もある。事前準備において、一定のホワイトチームとの情報共有は必須と考える。 この点、冒頭、「テストは」とされていることから、テスト実施は無予告だが、その前のコーディネーション段階ではブルーチームに対しても事前レクが行われることを否定するものではないと理解すればよいか。	ブルーチームへの事前予告により疑似攻撃が発生することを把握していると、その検知・対応能力が適正に評価されていないおそれがあるため、本項目を設けています。ご指摘の可能性については、ホワイトチームにおいて、適切にコントロールすることが考えられます。
165	2.2.4.c	「自組織のシステム環境を熟知する内部人材によるペネトレーションテスト（レッドチーム（ＴＬＰＴにおける攻撃側の担当者）によるテストを含む）を	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

		実施すること」とあるが、当該人材リソースは世の中的に供給が少なく、また高報酬でないと雇用できないことから本要件の実現は難しいと考えます。	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。
166	2.2.4.c	対応が望ましい事項であることは承知しているが、組織内のメンバーでペネトレを実施することは相当ハードルが高いように感じます。例えば、セキュリティベンダへ内部情報を多分に共有し、ホワイトボックスに近い形でペネトレを実施してもらう形でもよいのではないでしょうか。 〇理由 テストの目的が、内部犯行やより高度な攻撃への対策のためであれば、ホワイトボックスに近い形のベンダによるテストでもよいと考えられるため。	テストの目的等を踏まえ、検討いただくべき事項と考えられます。
167	2.2.5.	「2.2 サイバーセキュリティリスクの特定」の「2.2.5 演習・訓練」が、2.5「サイバーインシデント対応及び復旧」と重複しているように読める。2.2.5 の内容は「特定」分野に限った演習・訓練とも読めないので、2.5 にあわせたらどうか。	2.5「サイバーインシデント対応及び復旧」では、サイバー攻撃を想定したインシデント対応計画及びコンティンジェンシープラン（復旧計画まで含む）の策定について記載しております。これに対し、2.2.5「演習・訓練」は、演習・訓練を通じ、サイバーインシデント対応計画及びコンティンジェンシープランの課題を特定する観点から、「2.2 サイバーセキュリティリスクの特定」の項目としております。
168	2.2.5.①	演習や訓練については「定期的」に実施することとの抽象的な表記がある。 ガイドラインとして、「少なくとも 1 年 1 回」といった具体性な表記とするべきではないか。	当庁によるこれまでのモニタリングを踏まえ、具体的な最低頻度を示したほうがよいと考えている項目については記載し、それ以外は「定期的」としています（他の箇所も同様です）。いずれにしても、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、記載しております。
169	2.2.5.②	"CISO"や"業務部門の責任者"という固定的な記述は避けるべきではないか。ま	本項は、責任者が関与する演習・訓練を前提とした記載をし

		た演習や訓練の目的/スコープにもよるため、「経営陣や業務部門を含む適切な参加者」というような柔軟性をもった表現のほうが望ましいのではないか。 「責任者が自らサイバー演習・訓練等に関与し、その結果を把握」と書かれているが、「関与し」という表現は何を指しているのか。（要件の期待値が参加なのか、指示なのか。結果の把握に繋がる何らかの関与なのか。表現を改めるか、具体例を例示していただきたい。）	ております。責任者の関与方法については、実施する演習・訓練ごとに実態に即して判断されるべきものと考えられますが、いずれにしても責任者自らが演習・訓練に関与したうえで、結果を把握し、態勢の改善につなげることが重要であると考えられます。
170	2.2.5.c	「しかるべき承認」とは何か。2.2.2.3「経営陣等の承認」のように表記を合わせた方が良いのではないか。	ご指摘を踏まえ、修正いたします。
171	2.2.5.d	金融庁の取組みであるDelta Wallについては、「業界横断的」である点や、「最新の脅威動向等」をシナリオ策定上考慮していると思うが、このほかに「演習主催者による評価」を受けることができるという特徴もある。このほか存在する外部の演習・訓練についても各々特徴があると認識している。 参加可能な演習・訓練には、参加費用・日程・参加枠などの制約もあるため、毎回思うように実施できるものではないが、実施検討の考慮要素として「演習主催者による評価」の有無もあってよいと思うが、いかがか。	貴重なご意見として承ります。「演習主催者による評価」を考慮要素に含めることを妨げるものではありません。
172	2.2.5.d	複数の演習・訓練に参加することは、金銭負担のみならず、人員や振返り検討の時間も含め負担が大きい。各演習・訓練の特性を踏まえて、自組織が当年度に参加・実施する演習・訓練を検討する（特性の異なる演習・訓練を複数年かけてサイクルするように実施していく、その過程で例えば「前回演習の振り返りの年」と位置付けてあえて参加しない対応も含む）ことも現実的な対応と思うが、そのような対応も差し支えないか。	「『前回演習の振り返りの年』と位置付けてあえて参加しない対応」については、実質的に演習参加の先延ばしとならないように、慎重な判断が必要と考えます。
173	2.2.5.d	「組み合わせて実施」とは、各システムに対して複数の訓練・演習等を複合的に実施することではなく、自機関として必要な訓練・演習等を複合的かつ戦略的に実施することを意図しているか。 その場合、「自機関に必要な訓練・演習等を組み合わせて実施すること」と表現	自機関として必要な訓練・演習等だけでなく、各システムに対して複数の訓練・演習等を複合的に実施することも含みます。

		してはいかがか。	
174	2.3.	「2.3.サイバー攻撃の防御」の小項目として、「2.3.1.認証・アクセス管理」～「2.3.4.システムのセキュリティ対策」が設けられている。 これらの記載については技術的なものが多く、中小規模の金融機関では自組織での内製化よりも、外部ベンダー等に運用・管理を含め委託等する方が多いのではないかと思料する。 このような場合には、当該外部ベンダー等の対応状況などについて、サイバー以外の事項（広義のシステムリスク対応等）も含めた定期報告等を受ける中で、必要な情報提供を求めていくことで差し支えないか。	No.129 への回答をご参照ください。
175	2.3.	監督指針の「④情報セキュリティ管理」の「ハ. 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。 」は、「⑤サイバーセキュリティ管理」および新「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」2.3 の「サイバー攻撃の防御」とは別の対策等を実施設置することを期待するものか。また、その場合、両職責（管理者・担当部署）を同一人物に兼任させることは定めの趣旨に反するか。	必ずしも別の対策や管理者・担当部署でなければならないというものではありません。管理者・担当部署について、ガイドライン 2.1.1.⑦および 2.1.1.e に記載のように、サイバーセキュリティ担当部署及び各関係者の役割と責任及び権限を明確化することや、サイバーセキュリティに関する十分な知識・経験を有する者を配置することに留意が必要です。
176	2.3.1.①	特権 ID 管理を含む、認証・アクセス権等について触れているが、これらの対応について、必ずしもシステム的な管理やツール導入を求めるものではないとの理解でよいか。	システム的な管理やツール導入が必要か否かは、個々の状況によると考えます。
177	2.3.1.①	本ガイドラインでは「定期的に見直すこと」等の表現が多用されている（他の項目も含む）が、確認した結果として、見直す必要がないケースもあり得て、それ自体は問題ないと理解しているが、認識相違ないか。	見直し結果の妥当性は、個別・具体的な状況を踏まえて確認すべき事項ですが、見直した結果、修正の必要がないと認められる場合もあると考えられます。
178	2.3.1.①	観点の２つ目に「アカウントの～を実施し、無権限者によるアカウントの不正使用を防止すること」とあるが、適正な付与改廃の管理と、不正利用の防止の話は書き分けてはいかがでしょうか。 前者（管理）は、標準手続きを定める話。後者（不正利用防止）は、標準外への措置なので、対策のレベル感が異な	ご指摘を踏まえ、認証及びアクセス権の付与に係る方針及び規程等を策定し、定期的に見直す際に踏まえる観点として、アカウントのライフサイクルの管理及びアカウントの定期的な棚卸し等の管理並びに無権限者によるアカウント

		る。 例えば、NISC 統一基準 7.1.1 主体認証機能でも、(2)識別コード及び主体認証情報の管理にて、下記２つを書き分けている。 (a) は管理するための措置 (b) は不正行為の防止のための措置	の不正使用の防止を掲げる形に修正いたします。
179	2.3.1.⑤	「認証要件（多要素認証、リスクベース認証等、認証時におけるリスク低減策等）を決定すること」とあるが、リスクベース認証は「対応が望ましい事項」として書き分けてはいかがでしょうか。 本人性を確認するための認証方式（MFA 含む）に比べて、リスクベースの方式（RAdAC）は実装面や運用面の難易度の違いだけでなく、同方式の適用判断は MFA ほど単純ではないと思われる。	貴重なご意見として承ります。リスクベース認証は、例示として記載しております。
180	2.3.1.⑥	「2.3.1. 認証・アクセス管理」では、メールの送信ドメイン認証として SPF、DKIM、DMARC の記載があるが、リスクや運用コスト等を踏まえると、各金融機関における導入の必要性は区々と思料される。具体的なソリューションは明記せず「メールの送信ドメイン認証」といった記載にすることも考えられたと思うが、これら 3 つの認証を並列で記載した意図を伺いたい。 これらについては、いずれかを実施することを想定しているのか、あるいは、いずれも実施することを期待しているのかもあわせて伺いたい（仮に、３つ全てを実施する想定の場合、現時点では導入が難しいケースもあり、リスク考慮の上で導入しない判断もあり得ると考えている）。	フィッシングによるものとみられる不正送金の被害が増加していることを踏まえ、送信ドメイン認証を計画的に導入していただくことが重要と考えられます。DMARC は、SPF・DKIM のいずれか又は両方の認証結果を利用し総合的に送信ドメイン認証を行う技術であるため、受信者に表示される差出人アドレスの詐称に対応可能であり、なりすましメールにおける送信元の把握が可能であること等からフィッシングメール対策の一つとして有効です。 「国民を詐欺から守るための総合対策」(令和 6 年 6 月 18 日犯罪対策閣僚会議) においても、対策として DMARC 等の計画的導入が掲げられています。
181	2.3.1.⑥ 2.3.1.⑦	「基本的な対応事項⑥」の「送信ドメイン認証（SPF/DKIM/DMARC)」や、同⑦の「機密性、完全性及び真正性を確保」といった記載については、求める水準によって対策導入費用が大幅に変わると理解している。 これらも一律に適用されるものではなく、各金融機関の規模・特性等に応じて	フィッシングによるものとみられる不正送金の被害が増加していることを踏まえ、送信ドメイン認証を計画的に導入していただくことが重要と考えられます。

		検討されるべきとの理解でよいか念のため確認したい。	
182	2.3.2.	各種教育・研修の実施頻度は、各社の事情等次第と理解しているが、2.1.2.の「基本的な対応事項」において、規程・業務プロセスに関し「少なくとも1年に1回見直し」すべしとあることから、教育・研修の実施頻度も同様に解釈をしてよいか。	教育・研修の実施頻度と、2.1.2.に掲げている規程及び業務プロセスの見直しの頻度は同じである必要はないと考えられます。規程及び業務プロセスの見直しの際に、教育・研修の実施頻度も含めて見直すことが考えられます。
183	2.3.2.① 2.3.2.④ 2.3.2.⑤	「経営陣を含む役職員」、「IT又はセキュリティを所管する部門の職員」、「全ての役職員」に対しての教育や研修を「定期的」に実施することの記載あり。ガイドラインとして、2.1.1 、2.1.2 の様に「少なくとも1年1回」などの具体性な表記とするべきではないか。 「IT又はセキュリティを所管する部門の職員に対して」とありますが、この職員とは当該ガイドラインの対象となる金融機関の「役職員」との理解で良いでしょうか。	前段の頻度の点について、当庁によるこれまでのモニタリングを踏まえ、具体的な最低頻度を示したほうがよいと考えている項目については記載し、それ以外は「定期的」としています（他の箇所も同様です）。いずれにしても、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、記載しております。 後段について、ご理解のとおりです。ご指摘を踏まえ、修正いたします。
184	2.3.3. 2.3.4.2.①	バックアップデータの「保存期間」および「頻度」について、具体的な基準等は示されないのでしょうか。それとも金融機関が独自に定義するべきなのでしょうか。 同様に、ログについても「保存期間」および「保存方法」等の具体的な基準等は示されないのでしょうか。それとも金融機関が独自に定義するべきなのでしょうか。	ご指摘の点について、リスクに応じて、金融機関等において定義すべきものと考えられます。 参考として、バックアップに関して、公益財団法人金融情報システムセンター「金融機関等コンピュータシステムの安全対策基準・解説書（第12版）」の実39の参考1において、バックアップの取得サイクルを検討する際の目安についての説明があります。

			また、ログに関して、特定非営利活動法人日本セキュリティ監査協会「サイバーセキュリティ対策マネジメントガイドライン Ver2.0」において、ログの保存期間は１年以上とすることが望ましいとされているほか、ログの把握、確認、管理等に関する説明があります。
185	2.3.3.①	データの管理方針として、暗号化方式の危殆化時の対応を含むのは行き過ぎではないか（FISC 安対基準にもそこまでの記述はない認識）。システムライフが１０年近くに及ぶ金融機関では、実際の対応は次期システム開発時に盛り込むこととなり、現行システム稼働中は対応ができない。記載するとしても対応が望ましい事項に分類すべき。	システムのライフサイクルが長期に及ぶことを踏まえると、暗号化方式が危殆化した後にシステム対応を始めると、重要なデータを保護できなくなるおそれがあるため、危殆化時の対応について予め時間的な余裕をもって準備を進めることが重要であると考えられます。このため、原案のとおりとさせていただきます。
186	2.3.4.	オンプレミス環境における物理的なネットワーク機器管理に関する記述と同様に、クラウド環境上にリソースとして作成される仮想ネットワーク機器の設定情報についても管理する旨の記述もあった方が望ましいと考えます。	貴重なご意見として承ります。参考として、例えば、公益財団法人金融情報システムセンター「金融機関等コンピュータシステムの安全対策基準・解説書」の実 21 の参考 1 において、仮想ネットワークの境界等への不正侵入検知についての説明がありますのでご参照ください。
187	2.3.4.1.②	作業要員・ツール・交換部品といった個別・具体的な内容を、細やかに明文化することは困難であるため、可能であれば定めておく内容の好事例など、参考となる情報を提供いただきたい。	公益財団法人金融情報システムセンター「金融機関等コンピュータシステムの安全対策基準・解説書」の実 51、54 などが参考になると考えられます。
188	2.3.4.1.③	本項目の記述のうち「補完的な措置を講じる」以外に、リスク受容という選択もあってよいのではないか。	ただちにリスク受容するのではなく、まず補完的な措置を検討することが必要と考えられます。その上で、リスク受容については、ガイドライン 2.2.2.3 節（リスク対応）に記載の対応に則ることが考えられます。
189	2.3.4.1.④	「マルウェアシグニチャ（パターンファイル）及び動作プロファイル（ふるまい定義）の自動更新」とありますが、まず「マルウェア対策ソフトの導入」といった項目が必要と思われます。	ご指摘を踏まえ、修正いたします。

		○理由 シグネチャや動作プロファイルの更新は、マルウェア対策ソフトの利用が前提であるはずで、まずそちらを明記すべきであるため。	
190	2.3.4.1.④	対象：「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)」 箇所：2.3.4.1.基本的な対応事項④ コメント： 本項目では、マルウェア対策として考えられるものが挙げられているが、ネットワーク構成等によって、挿入できる対策に制約・限界がある（例えば、閉域環境についてインターネット接続を前提としたパターンファイルの自動取得・自動更新は不可能)。 ここでは「システムをマルウェアの感染から保護すること」が一義的な事項であるため、(過信は禁物とは言え、）境界防御を前提とした環境分離も一つの対策となり得ると考えるが、その理解でよいか。	仮に境界防御を前提とした環境分離を行う場合であっても、境界防御型セキュリティが突破されるリスク（ガイドライン 2.2.2.2③参照）などに留意する必要があります。
191	2.3.4.1.a	「システムで利用するサードパーティのライブラリやミドルウェア、ハードウェアについては、セキュリティ・バイ・デザインやセキュリティ・バイ・デフォルト等の安全な開発手法を製品開発に取り入れている事業者から提供されており、不正侵入の経路となるバックドア等が含まれていない安全なプロダクトを選定すること」とあるが、表立ってバックドアが設置されるケースなどはありえず、要件として意味がないと考えます。	ご意見を踏まえ、修正いたします。
192	2.3.4.1.a	概念は理解できるが、特に a.に関してはセキュリティ・バイ・デザイン自体が抽象的かつ広範に及ぶものであり、明示的な基準や指針がないと準拠は難しく、形骸化する恐れがないか。	貴重なご意見として承ります。デジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」を参考にしていただくことが考えられます。
193	2.3.4.1.a	事業者がセキュリティ・バイ・デザイン等をとりいれているかどうかについて、どのようにすれば確認できるのか、何か具体的方法で想定しているものはあるのか。	例えば、調達段階において、システムのセキュリティ要件に基づく仕様を策定した上で、当該仕様を満たす能力を有した事業者を選定することが考えられます。

			本項目において参考として記載しているデジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」もご参照ください。
194	2.3.4.1.a 2.3.4.3.②	2.3.4.1.a.において「セキュリティ・バイ・デザインやセキュリティ・バイ・デフォルト等の安全な開発手法を製品開発に取り入れている事業者～選定すること」とあるが、何が出来ていればセキュリティ・バイ・デザインやセキュリティ・バイ・デフォルトを取り入れていると判断できるのか基準が必要と思われる。抽象度が高いままでは、どのサードパーティも「取り入れていない」と回答するはずもなく、当該項目の記載が形骸化することが懸念される。 2.3.4.3.②「外部委託先等において、セキュリティ・バイ・デザインを実施できる体制となっているか」についても上記と同様。	貴重なご意見として承ります。デジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」を参考にしていただくことが考えられます。
195	2.3.4.1.c	「ハードウェア（機器、ファームウェア、ＵＥＦＩ又はＢＩＯＳ等）の真正性を確保し、また、不正な書き換えを防止するための対策（改竄検知など）を導入すること」とあるが、正規のメーカーから導入することは可能ながら、工場出荷前や設置・実装時の悪性コード混入等の不正行為については検知が非常に困難と考えます。	本項目は、製造者による正規のものと納入、設置等された製品のファームウェアが同等であることを意味しています。ハードウェアの真正性の確保のため、不正を検知する製品・ツールを利用することが考えられます。
196	2.3.4.2.①	本項目で例示されるもののうち「ログに記録する内容」については、サイバーセキュリティの観点で最低限記録すべき項目と理解すればよいか。	ログに記録する内容は、ログ取得の目的を定めたうえで、目的に対して必要な内容を検討することが考えられます。
197	2.3.4.2.①	本項目で例示されるもののうち「ログへのアクセス制御」「ログの改ざん防止」については、システムごとの具体的な技術的対策を規定するのではなく、これらの対策を講じることについて規定するという理解でよいか。	「ログへのアクセス制御」や「ログの改ざん防止」を確保するための手続きについて規定することが考えられます。
198	2.3.4.2.①	ガイドライン「2.3.4.2.ログ管理」が、「ログの取得・監視・保存」について定めているところ、ログデータが日々大量に発生すると人間の目による監視が困難になる場合がある。 　いわゆるSIEM（Security Information and Event Management）ツール等を	ご指摘のような手法も含まれると考えられます（2.4.1.cもご参照ください）。

		用いて、リスクに応じて情報を自動的に抽出させる手法も認められるか。	
199	2.3.4.3.	「2.3.4.システムのセキュリティ対策」の中で、「セキュリティ・バイ・デザイン」については「2.3.4.3.」で着眼点等の記載があるが、「セキュリティ・バイ・デフォルト」については、「2.3.4.1.対応が望ましい事項a.」の脚注34以外に言及がない。 導入時の注意事項等について着眼点等があれば伺いたい。	デジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」の説明（以下）を参考にしていただくことが考えられます。 （以下、抜粋） 「システムの初期設定値としてセキュリティが担保された状態を実現し、システム運用者や利用者による設定ミスを極力少なくすることが求められる（セキュリティ・バイ・デフォルトの実施）。」
200	2.3.4.3.①	「金融商品・サービスの企画・設計段階から、セキュリティ要件を組み込む「セキュリティ・バイ・デザイン」を実践すること。サービス全体の流れの中で、外部委託先等も含めてリスクを検証し対策を講ずること」とあるが、SaaSなどの場合、外部委託先が設計部分を非開示とする場合がありセキュリティ要件がどの程度組み込まれているか確認できないケースがあることから、本要件は自社資産に限定するか推奨事項にすべきと考えます。	外部委託先が受託業務遂行上保有している自組織の情報やクラウド内の自組織のデータも、金融機関が管理すべき情報資産に含まれます。 本項目において参考として記載しているデジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」もご参照ください。
201	2.3.4.3.① 2.3.4.3.②	セキュリティ・バイ・デザイン自体が抽象的かつ広範に及ぶものであり、明示的な基準や指針がないと準拠は難しく、形骸化する恐れがないか	貴重なご意見として承ります。デジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」を参考にしていただくことが考えられます。
202	2.3.4.3.②	「外部委託先等において、セキュリティ・バイ・デザインを実施できる体制となっているかを確認すること」とあるが、「セキュリティ・バイ・デザインを実施できる体制」とは何を確認することで充足できるのでしょうか。外部委託先等が容易に提示できないようなものを求めるのであれば、本要件は推奨事項にすべきと考えます。	例えば、システムのセキュリティ要件に基づく仕様を策定した上で、当該仕様を満たす能力を有した委託先を選定することが考えられます。 本項目において参考として記載しているデジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」もご参照ください。

203	2.3.4.3.②	外部委託先等がセキュリティ・バイ・デザインを実施する体制になっているかどうかについて、どのようにすれば確認できるのか、何か具体的方法で想定しているものはあるのか。	例えば、システムのセキュリティ要件に基づく仕様を策定した上で、当該仕様を満たす能力を有した委託先を選定することが考えられます。 本項目において参考として記載しているデジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」もご参照ください。
204	2.3.4.3.②	各金融機関それぞれが委託先等のセキュリティ・バイ・デザインの体制を確認する場合、双方（委託先・金融機関ともに）の確認負荷が社会的コストになりうるため、公的なセキュリティ・バイ・デザインの実施体制の認定制度等の導入を検討いただきたい。斯かる認定制度があれば、金融機関は、委託先の認定状況を確認するだけでよく、また、委託先側も複数の金融機関から類似の個別照会を受けることなく、社会的コストを削減できるものと考える。	貴重なご意見として承ります。
205	2.3.4.3.②	ここでいう「外部委託先等」とは、自機関にシステムやクラウドサービスを提供するシステム子会社やシステムベンダー、クラウドサービス事業者を指しているか。その場合、「サードパーティ等において、自機関に提供するシステムやクラウドサービスを開発するに際してセキュリティ・バイ・デザインを実施できる体制になっているかを確認すること。」と表現してはいかがか。 仮に p9 注釈 17 の通り、「外部委託先等」が業務を委託している組織を指す場合は、業務の委託先でセキュリティ・バイ・デザインを実施するか否かは委託元の金融機関に影響を与えず、対応を求められる理由が不明瞭なため、理由を明示いただきたい。	ガイドラインの本項目において、趣旨明確化のため、「外部委託先等」を「重要なサードパーティ」と修正いたします。「重要なサードパーティ」の定義は、脚注 26 をご参照ください。
206	2.3.4.4.①	基本的な対応事項として定義されている「外部ネットワークと内部ネットワークの物理的（論理的）な分離」が、クラウド利用の促進を阻害している要因のひとつとなっています。ゼロトラスト等の新しい考え方も出てきており、ネットワーク分離以外のシステム構成も検討する時期に来ているのではないでしょうか。	貴重なご意見として承ります。本項目の「物理的な分離・論理的な分離」は、不正侵入防止策の一例にすぎません。ゼロトラストについては、No.9 に対する回答もご参照ください。

207	2.3.4.4.④	本項では「無線 LAN ネットワークへのアクセス」について触れているが、自組織において無線 LAN 環境を整備している場合に対象となるとの理解でよいか。	ご理解のとおりです。
208	2.3.4.4.⑤	【基本的な対応事項】⑤に「ログの取得」とありますが、「利用者認証や通信内容等を含むログ」とし記載内容を具体化してはいかがでしょうか。 〇理由 有事の調査において必要なログが保存されておらず、原因や被害範囲の特定に支障を来たすケースが散見されます（例：通信内容は出力内容が大量で保存していない等）。このため、記載内容を具体化すべきと考えます。	ご指摘を踏まえ、修正いたします。
209	2.3.4.5.	「2.3 サイバー攻撃の防御」における「2.3.4.5 クラウドサービス利用時の対策」だが、2.3 サイバー攻撃の防御の範囲に限定されない用に思える。例えば①についてや ②についてはガバナンスの話であり、5 はインシデント対応である。 基本的に「クラウドサービス」の利用は（委託にも該当しうる）第三者管理すなわちサードパーティのサービスの利用であり、である。それについて適切なサイバーセキュリティ態勢は必用であるものの、特定のサイバー攻撃対応の段階（防御）に限定されず、包括的な対応が必要になるはずである。 したがって、より「2.x」の粒度で取り扱うべきと考えられる。 イセトー事例なども考慮すれば、例えば、「2.6 サードパーティリスク管理」に包有しても良いのではないだろうか	貴重なご意見として承ります。クラウドサービス提供事業者は、本ガイドラインにおける「サードパーティ」に該当するため、2.6「サードパーティリスク管理」の項目を参照いただくべきものと考えます。
210	2.3.4.5.	本項目のうち、多くの部分については、自組織だけで対処できず、クラウドサービス事業者の協力が必要となる。ついては、以下３点についてご配慮いただきたい。 （１）国内のクラウドサービス事業者については、行政当局からも、こうした事項について協力が得られるよう働きかけていただきたい。(NISC の行動計画においてクラウドサービス事業者が一定程度責務を負っていることも踏まえて働きかけていただきたい。) （２）国外のクラウドサービス事業者については、協力を得ることができず、	貴重なご意見として承ります。クラウドサービス事業者を含め、金融機関等にサービス等を提供するサードパーティについての当庁の考え方（サイバーセキュリティ関連）は 2.6 節冒頭に記載のとおりです。また、リスク許容度に応じたリスク受容を排除するものではありませんが、クラウドサービスを利用する前にはリスク評価が、リスクを受容する場合にはリスク管理プロセスが必要であると考えられます。

		また国内法や行政当局からの働きかけも通じないことがあるため、サービスを利用する業務・システム等のリスクに応じた運用を許容いただきたい（リスク度合いによっては、①～⑥を完全に満たせない場合も許容されることとしていただきたい）。 （３）クラウドサービスの利用自体が、ここ数年で生じてきた論点であり、ここに記載される「基本的な対応事項」が実行可能かどうか、今後の状況によって不透明な部分があるため、監督上、柔軟な運用をお願いしたい。	
211	2.3.4.5.	クラウド事業者は、サードパーティとして、「2.6.サードパーティリスク管理」に記載の対応が求められると思われるが、明確化の観点からその旨を記載したほうがいいのではないか。	貴重なご意見として承ります。ご指摘のとおり、クラウドサービス提供事業者は、本ガイドラインにおける「サードパーティ」に該当します。脚注 18 をご参照ください。サードパーティリスク管理については、2.6 節を参照いただくべきものと考えます。
212	2.3.4.5.①	ここで確認することとされている「クラウドサービスの仕様」について、最低限確認することが望ましい項目等を例示いただきたい。	ガイドライン 2.3.4.5②～⑥に関連する事項が仕様においてどのように定められているかを確認することが考えられますが、これらに限られません。
213	2.3.4.5.⑤	「多岐にわたる関係主体等」については、具体的にどのようなものを想定しているか。	例えば、クラウド事業者、組織内のクラウドサービス利用者、API 連携先などが考えられます。
214	2.4.①	本項目で記載されるもののうち、IoC 情報の平時の活用については、どのように実務に落とし込むか悩んでいる（監督当局として、検知のために活用してほしいという意図は理解している）。 IoC 情報を受領した後の後続事務について、具体的な手順等、有効な手続きに係る手引・参考資料等があればご教示いただきたい。	ガイドラインにおいて具体的な手順等を取り扱うものではありませんが、ガイドライン 2.4.1「監視」に掲げている監視活動を効率的・効果的にするために IoC 情報の活用手順を定めることを想定しています。独立行政法人情報処理推進機構「脅威インテリジェンス導入・運用ガイドライン」なども参考になると考えられます。
215	2.4.①	該当項目に記載されている「なお、クラウドサービスの監視には、クラウド事業者がシステムの監視状況を同事業者から提供されるレポート等により確認することを含む」について確認させてください。	レポートの提出を求めることが困難な場合においては、代替措置、リスク低減措置（残余リスクのモニタリングを含む）の検討も重要だと考えられます。

		前段の記載から、クラウドサービスに関する自社での監視の対象に含めるか否かについてはクラウドサービス事業者との責任分界点を踏まえて決定するものと認識しております。クラウド事業者の監視状況に関するレポートの取付についても、責任分界点を踏まえ実施することで良いという認識で問題ないでしょうか。 責任共有モデルによる責任分界点の観点から、クラウド事業者からすべからくレポートの提出を求めることは難しいと考えております。記載の解釈によっては、レポートの取付が必須のようにも見受けられ、念のため確認させていただけますと幸いです。	
216	2.4.1.	この項目に限らずだが、個別の実施事項については、1.2.1 に示されているリスクベースの考え方により金融機関側に一定の判断余地があるという解釈でよいか。	ご理解のとおりです。その上で、リスク受容に係る判断や残存リスクの管理は各金融機関において行う必要があります（2.2.2.3 節参照）。
217	2.4.1.①	「ソフトウェア、ファームウェアの更新時に当該ソフトウェア、ファームウェアの改ざん等が行われていないこと」を監視する方法やサービスの具体例を伺いたい。	例えば、更新時に、デジタル署名やハッシュ値による確認を行う製品・サービス、ファームウェアセキュリティリスクを管理する製品・サービスを使用することが考えられます。
218	2.4.1.① 2.4.1.② 2.4.1.③	2.4.1.①～③において「例えば、以下の監視をすること。」のような言い回しがありますが、【基本的な対応事項】で例えばという例示的な記載をされてしますと対応する必要があるのか無いのかの判断の揺らぎが生じるかと思います。 ②ネットワークについて、例えば、以下の監視をすること。 ・組織内ネットワークへの不正侵入（IPS や IDS の利用等）。 は、 「例えば」であるにもかかわらず、 2.3.4.4. 技術的対策 ①不正侵入を防止するため、外部ネットワーク（オープンネットワーク、リモートアクセス等）と内部ネットワークの接続部分に適切な不正侵入防止策（物理的な分離・論理的な分離等）を講ずること。また、外部ネットワークと内部	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おります。その上で、ご指摘いただいた箇所について、例示的な記載としていることをもって、直ちに、対応する必要がないということを意味するものではなく、同 1.1 節に記載しておりますように、金融機関等においては、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。

		ネットワークとの間のデータ授受に対する不正侵入防止策を講ずること。 と、基本的対応事項となっていますので、場合分けするなど「例えば」以外の文言に変更したほうがよいかと思います。	
219	2.4.1.① 2.4.1.② 2.4.1.③ 2.4.1.④ 2.4.1.⑤	これらの監視項目は、すべてのシステム（サーバ）・端末・役職員に対し、漏れなく、かつシステム的に実施される必要があるか。この項目についても、一律の対応を求められるものではなく、リスクベース・アプローチで取り組むということで理解してよいか。 例えば、重要度・利用ネットワーク環境に応じて、リスクの高い環境下のサーバ・端末についての実施、機器種類別に複数台のサンプリング確認による実施、端末保有者が定期的に目視による監視を行う等でも求められる要件を充足するのか。	リスクベースで検討すべきものと考えられます。後段の対応についてもそれぞれリスクベースで検討すべきと考えられます。
220	2.4.1.②	「組織内ネットワークへの不正侵入（IPS や IDS の利用等）」とありますが、2.3. サイバー攻撃の防御の【基本的な対応事項】にも『内部ネットワークでのシステム不正利用を防止するための対策』とある通り、外部との境界だけではなく、ゼロトラストの観点から内部間であっても不審な挙動を監視する必要があると考えます。 そのため、『IPS や IDS』といった境界対策に加えて、『NDR』といった内部対策についても言及すべきだと考えます。	貴重なご意見として承ります。内部対策については、2.4.1.②の 2 つ目の箇条書き以降で包含されると考えられます。
221	2.4.1.②	「・ネットワークフローやトラフィックの異常値（DDoS 攻撃）。」とありますが、「・DDoS 攻撃等によるネットワークフローやトラフィックの異常値。」などに変更してはいかがでしょうか。 〇理由 １つ上の行に「・組織内ネットワークへの不正侵入（IPS や IDS の利用等）。」とあり、括弧内には対策手段が書かれています。一方、「（DDoS 攻撃）」は対策手段ではないため、括弧内に書く内容が統一されておらず、分かりづらく感じられます。	ご指摘を踏まえ、修正いたします。

222	2.4.1.②	「・不正又は通常と異なるネットワーク接続やデータ転送。」とありますが、（NDR の利用等）などと追記してはいかがでしょうか。 ○理由 他の項目にも（IPS や IDS の利用等）といった例示がなされており、具体的な対策手段を挙げることで金融機関等がより理解しやすくなると思われるため。	貴重なご意見として承ります。基本的な対応事項としては、原案を維持させていただきますが、NDR の利用を妨げるものではありません。
223	2.4.1.④	「外部のサービスプロバイダによるシステムへのアクセス（保守作業）について監視をすること」とあるが、これは、委託ベンダーによる保守作業に伴うアクセスを監視するという意図か。	ご指摘のようなものも含まれますが、委託ベンダー以外の外部プロバイダがアクセスすることを可能としている場合や、保守作業以外のためにアクセスする場合も含まれます。
224	2.4.1.⑤	「しかるべき責任者」とありますが、「2.1.1. 基本方針、規程 類 の策定 等」にて サイバーセキュリティを統括管理する責任者（CISO 等）を任命しているとともに、最終的にサイバーセキュリティを統括管理する責任者（CISO 等）へ報告すべき内容ですので、「しかるべき責任者」ではなく、サイバーセキュリティを統括管理する責任者（CISO 等）でよいかと思います。	例えば、アラートが過検知か否かなどについては、SOC 内で完結する場合もあると考えられるため、必ずしも CISO に限られないと考えられます。このため、原案のままとさせていただきます。
225	2.5.1.①	意見・要望を申し上げたいことは、サイバーセキュリティに関するガイドライン（案）（以下「ガイドライン案」という。）の「2.5.1. インシデント対応計画及びコンティンジェンシープランの策定（ページ 27）」において、「コンティンジェンシープラン（復旧計画まで含む）を、サイバー攻撃の種別ごとに策定すること」と示されていることに関するものです。 当社では、サイバー攻撃のインシデント対応に関して、BCP 基本方針、個別 BCP（サイバー攻撃）、サイバーセキュリティインシデント対応手順書（以下「対応手順書」という。）を定め、必要に応じ更新し運用しています。また、コンティンジェンシープラン（以下「CP」という。）も定めていますが、CP ではサイバー攻撃について特に触れていません。その理由は、当社では、サイバー攻撃は原因事象（地震、風水害、サイバー攻撃等）であり結果事象（システム利用不能、情報漏えい等）ではないこと、CP は基本的に結果事象を対象として策定す	原案を維持させていただきます。 サイバー攻撃か否かによって、復旧計画やインシデント対応は異なってくると考えられます（例えば、復旧、再接続時の再感染のリスクがないかの確認、法執行当局への連絡、顧客情報の漏えい（及びその可能性）を踏まえた顧客対応等）。このため、サイバー攻撃の種別ごとにコンティンジェンシープランを策定することは重要なことであると考えられます。その上で、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、記載しております。同 1.1 節に記載しておりますように、金融機関等においては、自らが直面する

		るものと考えているからです。 以下に、ガイドライン案に記載の「CP をサイバー攻撃の種別ごとに策定すること」に関わる当社の主な意見を申し上げます。十分に整理できていない面もあるとは存じますが、その点は何卒ご容赦ください。 ・サイバー攻撃の種別（ガイドライン案の注釈にある、DDoS 攻撃、Web サイト改ざん、マルウェア・ランサムウェアといった標的型攻撃等、脆弱性の悪用、不正送金を引き起こす攻撃など。）は今後も絶えず進化・変化し続けることが明白であることから、「サイバー攻撃の種別ごとに CP を策定する」という対応については、策定することの難しさや限界もありますが、サイバーインシデント対応の実効性を考えた場合に必須（基本的な対応事項）とすることには疑問を感じます。 ・ガイドライン案のもとになっている、金融商品取引業者等向けの総合的な監督指針（以下「監督指針」という。）では「サイバー攻撃を想定した CP を策定」という記載までででしたが、今回ガイドライン案では「基本的な対応事項」として「CP をサイバー攻撃の種別ごとに策定」という具体的な対応を示されています。サイバー攻撃の種別ごとに適切にインシデント対応を行うことについては異論ありませんが、その対応方法は様々あることから、必須（基本的な対応事項）とされたことには抵抗感が否めません。 ・代表的な事例と考えている、日本取引所を始めとする各取引所の CP が Web 公開されていますが、現状それらの CP には「サイバー攻撃」という文言もなくその種別にも触れられていません。これは、CP の想定ケースが、サイバー攻撃等という「原因事象」を対象とするのではなく、サイバー攻撃等により取引システムに障害が発生した等の「結果事象」を対象として、各対応を定めているからだと推測しますが、実際のところどのように考えられているのでしょうか。 ・今回はサイバーセキュリティに関するガイドラインではありますが、「サイ	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。

		バー攻撃の種別ごとに CP を策定する」ことが必須になるのであれば、例えば、その他の大きなリスクである「地震」（原因事象）についても地震の種別（首都直下地震、南海トラフ巨大地震など。）ごとに CP の策定が必須になるのではないかと思われます。など 以上のことを踏まえ、サイバー攻撃の種別に応じたインシデント対応が必要なことは承知しておりますが、ガイドライン案においては、その対応方法としてサイバー攻撃の種別ごとに CP を策定することを必須（基本的な対応事項）とするのではなく、サイバーインシデント対応が種別ごとの CP にこだわることなく柔軟に対応できるよう、以下２つの案をご検討頂きたく要望いたします。 案１:「基本的な対応事項」における「サイバー攻撃の種別ごとに」という文言を削って頂きたい。 案２：もし案１が叶わなければ、サイバー攻撃の種別ごとに CP を策定することについては「対応が望ましい事項」として頂きたい。	
226	2.5.1.①	インシデント対応計画及びコンティンジェンシープランについて、計画策定後の定期的な見直しを行う方針にすることで、よりよい計画になるものと考えます。	ご意見を踏まえ、修正いたします。
227	2.5.2.1.①	「～インシデントを検知すること」とあるが、検知自体は自然と生じるイベントであり、対応事項と呼べるのか違和感がある。 例えば顧客からの問い合わせや外部組織からの連絡を受けられるような窓口を設置しておくことであれば対応事項かと思われる。	ご指摘の項目は、インシデントへの初動対応として基本的な事項の一つと考えられることから、記載しております。
228	2.5.2.3.①	・「～統括管理する責任者（CISO 等）のサイバーセキュリティの責任者や担当者」となっており、日本語がおかしい（責任者の責任者と読める）。 ・「それぞれの各役割」となっており、日本語がおかしい。それぞれの役割もしくは各役割	ご意見を踏まえ、修正いたします。

229	2.5.2.3.③	「規制当局等」については、金融庁や財務局の規制当局や警察当局等のほか、個人情報漏えいに関しては個人情報保護委員会も含まれるものと想定するが、認識相違ないか。 なお、個人情報保護委員会に関しては、個人情報保護法の定めで、金融庁や財務局に権限委任が行われているため、このような場合には、結果として、金融機関は、インシデントについても個人情報漏えい事案についても、金融庁や財務局が報告窓口になると理解しているが、相違ないか。	前段について、ご理解のとおりです。 後段のインシデント報告については、金融庁の監督指針等（例：主要行等向けの総合的な監督指針Ⅲ－３－７－１－３）をご参照ください。 後段の個人データの漏えいについては、「金融機関における個人情報保護に関する Q&A」（令和 6 年 3 月、個人情報保護委員会事務局・金融庁）の問Ⅴ-３をご参照ください。
230	2.5.2.3.⑤	「攻撃者の TTP（Tactics（戦術）、Techniques（技術）、Procedures（手順））等、他機関にとっても有効となる攻撃技術情報について、機密情報を除いた上で、必要に応じ、金融 ISAC や JPCERT/CC 等の情報共有機関に共有すること」とあるが、「必要に応じ」共有するのであれば、推奨事項として頂きたい。	サイバーセキュリティには、情報共有を通じた共助の取組みも重要と考えられ（1.3 節参照）、これを促進することも目的として、本項目を「基本的な対応事項」としています。
231	2.5.2.4.①	インシデント発生前に準備しておくことと、インシデント発生後に封じ込めフェーズとして実際に行うことが混在しており分かりづらい。①、②と分けて書いた方が良いのではないか。	ご意見を踏まえ、修正いたします。
232	2.5.2.4.a	「適切に通知」とあるが、「適切に」が何を求めるための記載が理解しづらい。不要な表現であれば削除で良いのではないか。 これに限らず、本ガイドライン全般にわたり「適切に」が 32 回も用いられているが、読み手にとっては具体性がなく意味のない記載と感じる。	貴重なご意見として承ります。
233	2.5.2.6.	「復旧」の言葉にデータのリストア、OS やシステムのリカバリ、業務サービスの再開、インシデントの収束が混在しており、①～⑥でそれぞれどれを指しているのか理解しづらい。 特に④は、OS やシステムのリカバリに見えるが、「業務が稼働していること」という記載から既に業務サービスを再開した後にも読み取れて分かりづらい。更にその後ろに⑤として「他システムと再接続する前」（つまり業務サービスの再開の前）の記載があり、時系列的にも分かりづらい。	ご意見を踏まえ、修正いたします。
234	2.6.	本ガイドライン「2.6 サードパーティリスク管理」の「サードパーティ」には	貴見のとおりと考えられます。

		クラウドサービスの提供事業者も含まれますでしょうか。含まれる場合、クラウドサービスの利用に当たっては、「2.3.4.5　クラウドサービス利用時の対策」に加え、上記 2.6 も適用されることになりますか。	
235	2.6.	「サードパーティー」に OSS が含まれていない場合において、OSS を取り扱う場合のリスクベースアプローチはどう考慮すればよいか、ガイドラインに加えて頂くと分かりやすくなると考えます。	貴重なご意見として承ります。なお、OSS（オープンソースソフトウェア）は、サプライチェーンに含まれます。
236	2.6.	金融機関等よりも優越的な立場にあるサードパーティ等が相応に存在する中で、契約書や SLA 等の文言を自社様式から頑なに変更しないケースも容易に想定される。各金融機関が円滑に進められるよう、御庁からも他省庁や他業界に対して強く働きかけをお願いしたい。	貴重なご意見として承ります。官民連携した対応を検討してまいります。
237	2.6.	現在、API 接続先の定期的な点検・モニタリングは監査法人が実施する FISC「API 接続チェックリスト」等に基づく「合意された手続」にて、第三者機関を通じた信頼性の付与と双方の事務効率化を両立している状況。 １．当スキームをサードパーティリスク管理全般にも適用でき、監査法人等によるリスク評価でも確認できるという理解でよいか。 ２．例えば、サードパーティリスク管理に係る点検・モニタリング精度の均質化、作業の効率化を図る観点から、例えば、当スキームをサードパーティを管理する他社と共同で実施する制度（しくみ）もご検討いただきたい。	（一点目について） 個別の状況に即して考えるべき事項であり、一般論として、ご指摘のような手続が、サードパーティリスク管理全般等に必ずしも適用できるとは限らないため、慎重な検討が必要です。 （二点目について） 貴重なご意見として承ります。
238	2.6.①	「サプライチェーン全体を考慮したサイバーセキュリティ戦略」ではなく、「サイバーセキュリティに係る戦略を策定する際にはサプライチェーン全体を考慮することとし」とすべき（2.1.1　①のサイバーセキュリティに係る戦略」と同じものであることを示すため）。	ご指摘を踏まえ、修正いたします。
239	2.6.⑦	「過去のインシデントの発生状況」とあるが、過去にインシデントが起きていないことが良いことのようにも見えるためミスリードかと思われる。実際には	ご意見を踏まえ、修正したします。

		インシデントに気づいていないだけのセキュリティレベルが低いサードパーティもありえる。 むしろ、過去のインシデントの発生状況に加えて、対応状況や改善の取り組みまで確認して初めて評価観点として意味があるのではないか。	
240	2.6.⑧	2.6.⑧の「データの所在・保管・保持・移転・廃棄に関する取決め」の他、データの再利用や修正・管理方法についても、有無を含めて明記する方が良いと考えます。	貴重なご意見として承ります。ご指摘の「データの再利用や修正・管理」は、2.6.⑧の「データの所在・保管・保持・移転・廃棄」に含まれると考えられます。
241	2.6.⑧	「サードパーティが遵守すべきサイバーセキュリティ要件を明確化の上、重要度に応じ、サードパーティ等との契約やSLA（サービスレベルアグリーメント）等において、例えば、以下の項目を明記すること。」とあるが、後続の項目例の内の「実施すべきセキュリティ対策」について、最低限押さえておくべき具体的な例示をいただきたい。 技術的な対策について要求レベルに足りていないサードパーティに対して、充足するように依頼を行っても対応されないこともあり、どこまでプッシュして担保すべきか、悩ましいケースが発生している（恐らく委託先としても同様の点で悩んでいるものと思料）。	貴重なご意見として承ります。金融機関等にサービス等を提供するサードパーティについての当庁の考え方（サイバーセキュリティ関連）は2.6節冒頭に記載のとおりです。
242	2.6.a	サードパーティリスク管理における「適切な知識等を有する人員」の適切な知識等はサイバーセキュリティに限らないと思われるが、どのような人員が望まれるか、業務経験や資格等の具体例を示していただきたい。	どのような人員が望まれるかについては、リスクベースで金融機関において判断するべきものと考えられます。
243	2.6.b	「フォースパーティ」の意味を補記した方が良いと思われる。	ご意見を踏まえ、修正いたします。
244	3.1.	情報共有・情報分析の強化に関して、連携先として挙がっている日本銀行については、金融庁・日本銀行の協同の取組として、2022年から「サイバーセキュリティセルフアセスメント」(CSSA)が実施されている。本ガイドラインが制定された後、金融庁と金融機関双方で、どのようにCSSAを利用・活用し、ガイドラインの各項目への取組を考えていくか、監督当局のお考え等を伺いたい。	CSSAにつきましては、2025事務年度以降に向け、本ガイドラインと整合させる形で自己点検票の見直しを行う予定です。