1.『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

要約

- 近年ますます深刻化するサイバーリスクに対処するため、金融庁が『主要行等向けの総合的な監督指針』等の一部改正（案）および『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）を公表（*1）した。
- 『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）ではサイバーセキュリティに関する「ガバナンス」、「特定」、「防御」などの６項目についてそれぞれ「基本的な対応事項」および「対応が望ましい事項」を明確化して記載している。

今回の公表内容について

金融庁は 2024 年６月 28 日に、主要行や金融商品取引業者など向けの監督指針（全 10 種類）と資金移動業者・暗号資産交換業者など向けの事務ガイドライン（全６種類）の改正案および「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）（以降、新ガイドライン）をとりまとめ、公表しました。

監督指針・事務ガイドラインの改正では、新ガイドラインを踏まえたセキュリティ対策が行われることを前提として、参照先としての新ガイドラインの追加、記載の一部削除・簡略化などの見直しが図られています。下表は『主要行等向けの総合的な監督指針』の新旧対照表（案）です。「現行」において詳しく書かれていた箇所の一部は削除され、「新ガイドラインを踏まえ」という簡潔な記載になっています。なお、その他の監督指針、事務ガイドラインの改正も同様の内容となっています。

改正案	現行
Ⅲ－３－７－１－２　主な着眼点 （５）　サイバーセキュリティ管理 ①　取締役会等は、サイバーセキュリティの重要性を認識し、「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」を踏まえ、必要な態勢を整備しているか。 （現行②～⑥の削除）	Ⅲ－３－７－１－２　主な着眼点 （５）　サイバーセキュリティ管理 ①　サイバーセキュリティについて、取締役会等は、サイバー攻撃が高度化・巧妙化していることを踏まえ、サイバーセキュリティの重要性を認識し必要な態勢を整備しているか。 ②～⑥　サイバーセキュリティ管理態勢の整備、サイバー攻撃対策、サイバー攻撃の被害拡大防止対策、システムの脆弱性管理、セキュリティ水準の定期的な評価の実施に関する記述
②　現行⑦を踏襲	⑦　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のセキュリティ対策に関する記述
③　現行⑧を踏襲	⑧　インターネットバンキング等の不正利用防止のための適切な手続きに関する記述
（現行⑨、⑩の削除）	⑨、⑩　サイバー攻撃を想定したコンティンジェンシープラン策定、サイバーセキュリティ人材育成などに関する記述
Ⅲ－３－７－２　ATMシステムのセキュリティ対策 Ⅲ－３－７－２－２　主な着眼点 （２）　セキュリティの確保 （略）また、個別の対策を場当たり的に講じるのではなく、セキュリティ全体の向上を目指しているか。セキュリティの確保に当たっては、「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」も参照すること。（略）	Ⅲ－３－７－２　ATMシステムのセキュリティ対策 Ⅲ－３－７－２－２　主な着眼点 （２）　セキュリティの確保 （略）また、個別の対策を場当たり的に講じるのではなく、セキュリティ全体の向上を目指しているか。（略）

出典：『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）（*1）を基に大和総研作成

（*1）『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

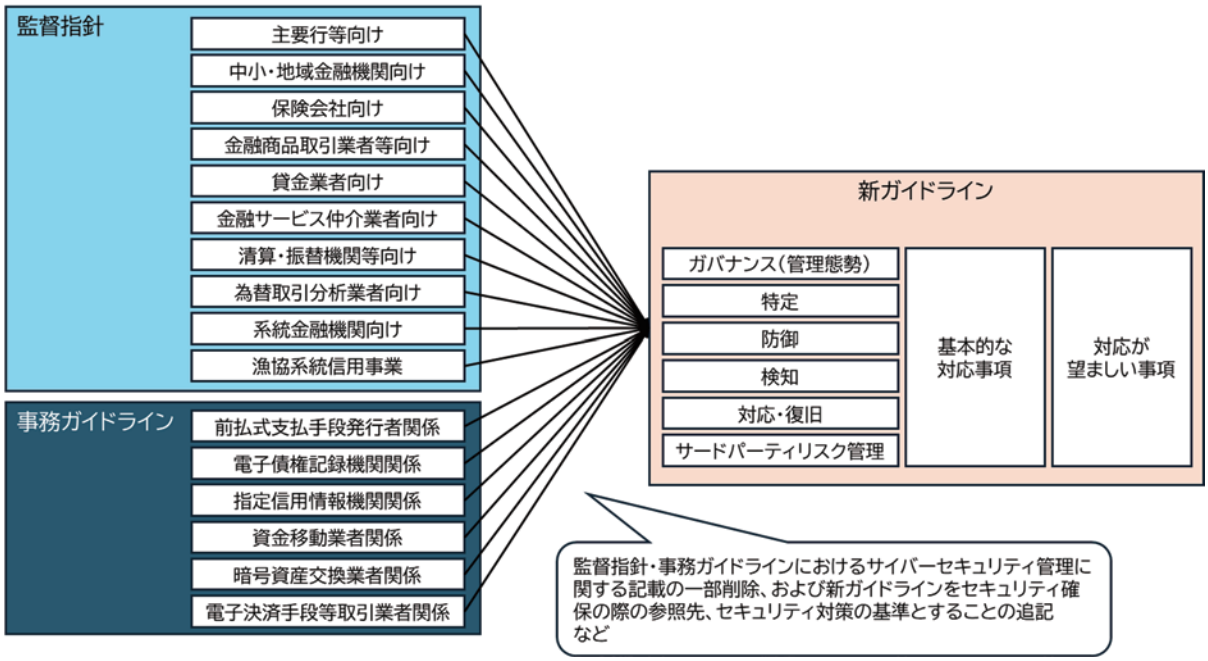
新ガイドラインの概要

昨今のサイバー攻撃の脅威は金融サービスの利用者および金融システムの安定に多大な悪影響を及ぼしかねず、金融庁はその任務である「金融機能の安定と預金者の保護」のために、金融セクター全体のサイバーセキュリティの強化が不可欠であると考えています。金融庁はこれまでも金融業界と協力し、監督指針や事務ガイドラインを通じて金融セクター全体のサイバーセキュリティの強化を促進してきましたが、このたび、これまでの検査・モニタリングの結果および金融セクター内外の状況の変化を踏まえ、監督指針などとは別に、さらに詳細なガイドラインとして新ガイドラインを策定しました。新ガイドラインは、下表のとおりの３節で構成されています。これまでは業種別の監督指針や事務ガイドラインにおいて業種ごとの特性に応じて策定されていた項目などを、新ガイドラインにおいて業種横断の共通項目として一本化しています。

節	概要
1．基本的考え方	金融機関などに求められるサイバーセキュリティに関する基本的な考え方や、自主的かつ積極的なサイバーセキュリティへの取り組み、経営陣の主体的な関与の重要性を記載。またサイバーセキュリティ強化のための業界団体や中央機関などの果たすべき役割についても言及。
2．サイバーセキュリティ管理態勢	サイバーセキュリティの観点から見たガバナンス、特定、防御、検知、対応・復旧、サードパーティリスク管理の 6 項目に関する着眼点について規定し、各項目について「基本的な対応事項」および「対応が望ましい事項」を明確化して記載。
3．金融庁と関係機関の連携強化	脆弱性情報の把握・共有、分析能力の強化のため、金融庁と各種機関との連携に対する基本的な考え方について記載。

出典：『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）（*1）を基に大和総研作成

図：監督指針及び事務ガイドラインと新ガイドラインの位置付け



出典：『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）（*1）を基に大和総研作成

新ガイドラインのポイント

新ガイドラインでは「基本的な対応事項」を“金融機関等が一般的に実施する必要のある基礎的な事項”、「対応が望ましい事項」を“実践することが望ましいと考えられる取組み”と定義しており、いずれも一律の対応を求めるものではなく、自組織を取り巻く事業環境、経営戦略およびリスクの許容度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を求めています。以降、新ガイドラインにおける主なポイントを記載します。

（*1）『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

- 規定内容の詳細化
  『主要行等向けの総合的な監督指針』を例として、監督指針から削除された項目の一部が新ガイドラインにおいてどのように定められているかを下表にまとめました。新ガイドラインでは各項目についてより具体的な対応内容が記載されていることがわかります。

新ガイドラインでの項目	新ガイドライン「基本的な対応事項」の例（要点）	監督指針での削除箇所の内容
ガバナンス（管理態勢） 人材育成	・定年や退職を踏まえた持続可能な人事政策の実施、資質・意欲のある職員の人材育成を阻害する人事異動の回避。 ・人材育成の観点から中長期的かつ計画的な人的配置の実施、外部からの採用・外部人材の活用だけでなく、内部人材の育成も考慮　など	サイバーセキュリティに係る人材について、育成、拡充するための計画を策定し、実施しているか。
特定 脆弱性管理	・脆弱性管理に係る手続の「脆弱性情報の入手先・入手プロセス、脆弱性の深刻度・影響の大きさおよび影響範囲の評価に関すること」などを含めた策定、必要に応じた見直し ・システムの重要度、リスク又は脆弱性の深刻度に基づいたパッチ適用などの対応期限の設定および対応実績の管理 ・深刻度の高い脆弱性は、グループ会社、海外拠点のシステムについても対応の範囲に含め、サードパーティが保有する重要なシステムについては対応の管理を行う　など	システムの脆弱性について、OS の最新化やセキュリティパッチの適用など必要な対策を適時に講じているか。
対応・復旧 サイバー攻撃の被害拡大防止策	サイバー攻撃による被害拡大を防止するための対応（封じ込め）を行う際の考慮点は以下のとおり。 ・被害拡大防止のため通信遮断やシステム停止などの実施判断者の事前の明確化。また判断に必要な「停止する時間帯や期間、業務影響、業務の代替手段」などの情報整理 ・通信遮断やシステム停止などを行う場合、封じ込めと証拠保全のいずれを優先すべきか、インシデントの状況や自組織の方針に従い判断すること　など	サイバー攻撃を受けた場合に被害の拡大を防止するために、以下のような措置を講じているか。 ・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 等

出典：『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）（*1）を基に大和総研作成

- 管理態勢、規程などの定期的な見直し
  攻撃手法が多様化・巧妙化している現状、最新のサイバー攻撃の傾向などを踏まえ「サイバーセキュリティに係る管理態勢、規程及び業務プロセス、サイバー攻撃の脅威情報・脆弱性情報の収集元及び収集・分析方法、サイバーセキュリティリスク評価のプロセス」などについては、少なくとも１年に１回の見直しを求めています。
- サイバーセキュリティに関する取り組みの対外公表の推奨
  「対応が望ましい事項」として自組織のサイバーセキュリティに関する取り組みの意義を内外の関係者に表明するため、その内容を対外公表することを求めています。なお、この対外公表により、攻撃者の攻撃を助長する可能性があることも注意としてあげています。
- サードパーティリスク管理の詳細化
  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の策定、サードパーティが提供する商品・サービスの自組織での位置付けに応じたリスク評価の実施、サードパーティ管理のための台帳整備、サードパーティも含めたサイバーインシデント対応計画やコンティンジェンシープランの整備など、サプライチェーン全体のセキュリティ向上のためのより細やかな取り組みが求められています。

この他、新ガイドラインには様々な対応内容が詳細に記載されていますので、ご一読をお勧めします。

最後に

金融機関向けのサイバーセキュリティ対策についてはこれまで監督指針や事務ガイドラインはあったものの、具体的な対応内容などは提示されていませんでした。今回の公表により金融機関の業種横断的な指針が示され、自組織の状況に応じた必要な対応の検討が求められます。また、策定した方針や規程については昨今の攻撃手法やサードパーティのサービス利用などによるシステム構成の変化を踏まえ、継続的な見直しも計画に含めることが必要です。

（田川　晋作）

（*1）『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