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

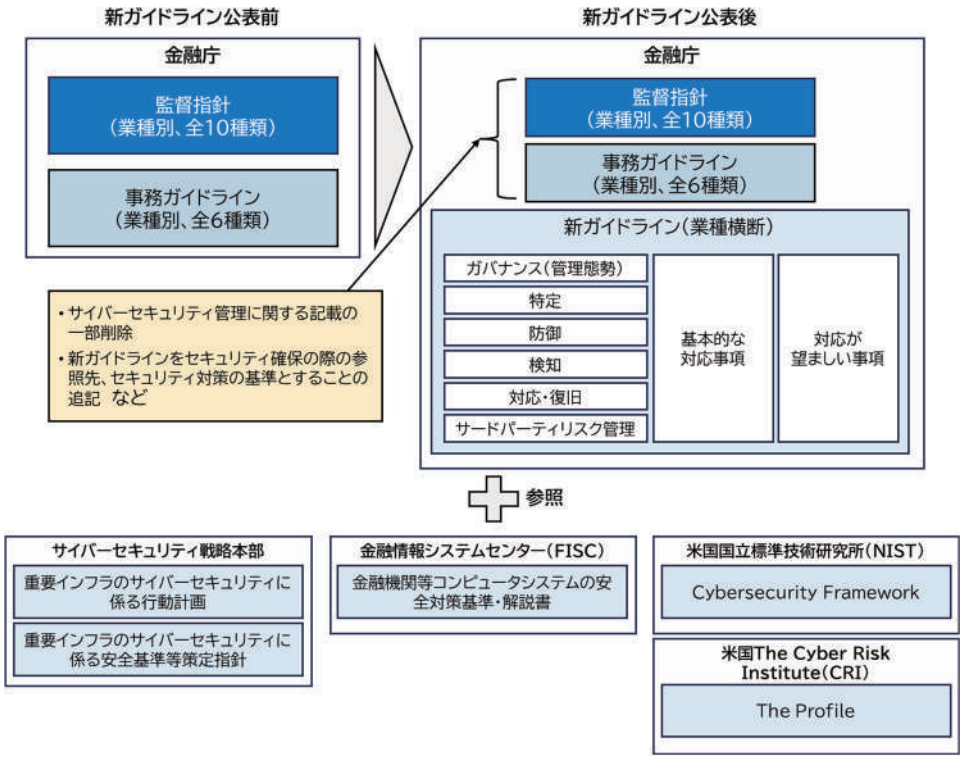
要約

- 金融庁は 2024 年 10 月 4 日に主要行など向けの監督指針などの一部改正および「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」を公表し、同日より適用すると発表した。
- 金融機関などは本ガイドラインを用いて自己評価を行い、自組織のセキュリティレベルの確認およびリスクベース・アプローチに基づいたさらなるセキュリティ向上への取り組みが求められている。

新ガイドラインの位置づけ

金融庁はこれまで金融業界と協力し、主要行など向けの監督指針など（以降、監督指針など）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、監督指針などの一部改正と共に、さらに詳細なガイドラインとして「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」（以降、新ガイドライン）を策定しました。

これまでは業種別の監督指針など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。その内容は米国国立標準技術研究所（NIST）の「Cybersecurity Framework（CSF）」や米国の非営利団体 Cyber Risk Institute（CRI）の「The Profile」などと同様の形式となっており、サイバーセキュリティ観点の「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 つの項目において、「基本的な対応事項」と「対応が望ましい事項」を定めています。



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）に対するパブリックコメントの結果等について』(*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）に対するパブリックコメントの結果等について

新ガイドラインの構成

新ガイドラインは３節で構成されており、第１節では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考え方、取り組み、経営陣の主体的な関与の重要性などについて記載されています。第２節では「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」の各６項目における対応について、第3節では金融庁と各種機関との連携について記載されています。以下の表において第２節での「基本的な対応事項」、「対応が望ましい事項」の項目数と前者の主なポイントをまとめました。

節	項	基本的な対応事項数	対応が望ましい事項数	「基本的な対応事項」の主なポイント
2.1. サイバーセキュリティ管理態勢の構築		-	-	・サイバーセキュリティ基本方針の策定、管理態勢の整備、戦略・取組計画の策定、規程および業務プロセスの整備 ・各関係者の役割と責任、権限の明確化、サイバーセキュリティ統括責任者（CISOなど）の任命 ・計画的な人材計画・育成・配置、予算などの適切な配分 ・サイバーセキュリティリスク状況などの報告会の開催 ・サードパーティも含めた組織横断的な報告・連絡・協議ルートや指揮命令系統の整備 ・リスク管理部門・内部監査による監視、牽制、監査、報告の実施
	2.1.1. 基本方針、規程類の策定等	9	5	
	2.1.2. 規程等及び業務プロセスの整備	2	-	
	2.1.3. 経営資源の確保、人材の育成	4	-	
	2.1.4. リスク管理部門による牽制	2	1	
	2.1.5. 内部監査	2	1	
	小計	19	7	
2.2. サイバーセキュリティリスクの特定		-	-	・情報資産の管理手続の策定、優先度に応じた分類 ・クラウドサービスなども含めた情報システム・ハード/ソフトウェア・データなどの台帳、データフロー・ネットワーク図の整備 ・内外から得られる脅威・脆弱性情報の収集・分析と共に自組織への影響評価の実施 ・評価結果に基づいたリスク対応の優先順位付け・対応計画策定 ・脆弱性が発見された際の管理・対応方法の策定 ・脆弱性診断・ペネトレーションテスト、サイバー演習・訓練の実施および検知された脆弱性・課題などへの対応
	2.2.1. 情報資産管理	6	5	
	2.2.2. リスク管理プロセス	12	7	
	2.2.3. ハードウェア・ソフトウェア等の脆弱性管理	6	1	
	2.2.4. 脆弱性診断及びペネトレーションテスト	1	4	
	2.2.5. 演習・訓練	5	4	
	小計	30	21	
2.3. サイバー攻撃の防御		1	-	・不正侵入防止のための多層防御の実施 ・認証およびアクセス権付与の方針・規程の策定 ・機器・ユーザIDおよび認証情報の適切な管理 ・ユーザ処理のログへの記録・ユーザ操作内容との照合 ・システムや扱う情報の重要度に応じた認証要件の決定 ・重要度に応じたデータ管理方針の策定 ・ランサムウェア攻撃などを想定したバックアップ規程の整備 ・セキュリティ・バイ・デザインの実践 ・利用するクラウドサービスの理解、責任範囲の明確化、設定内容の確認
	2.3.1. 認証・アクセス管理	8	-	
	2.3.2. 教育・研修	5	2	
	2.3.3. データ保護	5	2	
	2.3.4. システムのセキュリティ対策	19	8	
	小計	38	12	
2.4. サイバー攻撃の検知		2	-	・アノマリ（異常値）、IoC（侵害の痕跡）などのサイバー攻撃の端緒の検知のための監視・分析・報告に係る手続きの策定（監視の対象には責任分界に応じてクラウドサービスも含める） ・サイバー攻撃の脅威に応じた必要な監視・分析などの実施
	2.4.1. 監視	7	3	
	小計	9	3	
2.5. サイバーインシデント対応及び復旧		-	-	・サイバー攻撃の種別ごとのインシデント対応計画および復旧計画までを含んだコンティンジェンシープランの策定 ・インシデント検知などから収集した情報を基にした対応要否の判断、対応の優先順位付け、サイバーセキュリティ統括責任者（CISOなど）、経営陣への報告 ・インシデントの攻撃手口や原因、経路、影響などの分析 ・インシデント検知・受付から復旧までの一連の対応の記録 ・インシデント発生時の必要に応じた顧客への影響の伝達、法令などに基づいた規制当局への速やかな報告、公表の実施、金融ISACなどの情報共有機関への攻撃技術情報の共有 ・被害拡大防止のための封じ込め、原因の除去、復旧
	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	1	1	
	2.5.2. インシデントへの対応及び復旧	19	1	
	小計	20	2	
2.6. サードパーティリスク管理		10	5	・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に係る戦略、取組計画の策定、組織体制の整備、組織内規程の策定 ・サードパーティが提供する商品・サービスの役割・重要度・取り扱い情報の種類、組織内システムへの接続状況などを踏まえたリスク評価と対応 ・サードパーティ管理のための台帳の整備、維持 ・サードパーティを含めた必要な態勢の整備 ・サードパーティとの取引開始前のデューデリジェンスの実施 ・サードパーティとの適切な契約、SLAの締結および契約履行状況の継続的なモニタリング ・サードパーティとの取引終了時の管理プロセスの整備
合計		126	50	－

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）に対するパブリックコメントの結果等について』(*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）に対するパブリックコメントの結果等について

新ガイドラインを取り巻く議論について

金融庁では 2024 年 6 月 28 日に「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）を公表し、2024 年 7 月 29 日までの約 1 ヶ月間意見を募集しました。244 件集まったパブリックコメントに加えて、SNS や金融機関関係者の反応は、今回の金融庁の取り組みを肯定的に捉える意見もありましたが、同時に否定的な意見も散見されましたのでその主なものを以下の表にまとめました。

肯定的な意見	否定的な意見
網羅性 サイバーセキュリティに関する対策が網羅的かつ業種横断の共通項目として示されており、金融業界全体の対応力の底上げが期待できる。	**対応内容の曖昧さ** 対応すべき内容として列挙されている例や括弧内で記載されているものなど、どこまでを対応すべきかが不明瞭で、組織間で解釈が異なる可能性がある。
リスクベースのアプローチ 一律的ではなく各組織の実情に合わせた柔軟な対応が可。	**実効性の疑問** 新ガイドラインの遵守によってどれだけの効果が望めるかを疑問視。
国際基準との整合性 NIST の「CSF」、CRI の「The Profile」などの国際基準との整合性があり、グローバルな視点で対応が可能。	**対応のための負担** 中小金融機関などは「基本的な対応事項」に対応するだけでもリソース面での負担が大きく、経営体力対比で考えると実現は不可能または相当の時間を要する。
サードパーティ管理の円滑化 ガイドラインによって金融庁の方針が示されたことでサードパーティリスクの管理が円滑になることが期待される。	**要求が抽象的** セキュリティ・バイ・デザイン、セキュリティ・バイ・デフォルトを取り入れている業者を選定するという項目があるが、何を以て取り入れているとするか基準が曖昧。

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）に対するパブリックコメントの結果等について』(*1)を基に大和総研作成

新ガイドラインは対応項目を網羅的に記載している一方で、その内容は一部曖昧でどこまで対応すべきか分からないといった不安を抱える方もいるようです。サードパーティの管理については金融庁による方針策定を歓迎する一方で、実際の管理の難しさから金融庁によるさらなる働きかけを求める声もありました。

また、対応項目のチェックリスト形式での公開の要望も見受けられましたが、新ガイドラインはリスクベースで検討すべきなのでチェックリスト形式には馴染まないというのが金融庁の回答でした。しかし、実務上、自己評価を行う際に金融庁の項目に基づいて自社でリストを作成している組織が大半だと推測されます。情報公開の在り方についても、効率性の観点から改善の余地があると考えられます。

最後に

今回の新ガイドラインの公表ではこれまでの業態ごとの監督指針などの規程からサイバーセキュリティに関する対応項目を取り出し、金融業界で共通のガイドラインを制定しており、近年ますます深刻化するサイバーリスクへの対応策として大変有用な取り組みとなっています。今後、新ガイドラインは金融機関のセキュリティ対策を考える上では重要な資料になりますが、その項目数は合計で176個と点検項目としては少なくない数になります。まずは新ガイドラインに記載のある通り、リスクベース・アプローチの下、対応項目の一つ一つを自社なりに解釈し、現状を把握する必要があります。その際、自社だけでの対応が難しい場合は専門家の力を借りることも選択肢とするとよいでしょう。新ガイドラインの対応を各社が着実に行うことで金融業界全体のサイバーセキュリティが強化されることを期待しています。

（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）に対するパブリックコメントの結果等について