Research Focus

日本総研
The Japan Research Institute, Limited
https://www.jri.co.jp

2024 年 10 月 23 日
No.2024-039

「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」の概要と求められる対応

調査部　主任研究員　谷口 栄治

《要　点》

◆ 世界的にサイバーリスクが増大するなか、金融セクターでもサイバーセキュリティ対策が重要な課題に。こうしたなか、本年 10 月、金融庁は、本邦金融セクター全体のサイバーセキュリティを強化するため、「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」（以下、ガイドライン）を策定。

◆ ガイドラインの特徴として、①サイバーセキュリティに関する対応事項をガイドラインとして明示した点、②金融機関の規模や特性等に応じて対応事項を決める「リスクベース・アプローチ」が採用された点、③銀行や証券会社等に加え、資金移動業者や暗号資産交換業者等、幅広い機関を対象としている点、を指摘可能。

◆ ガイドラインでは、具体的な対応事項として、①サイバーセキュリティ管理態勢の構築（基本方針や計画の策定、組織やプロセスの整備）、②サイバーセキュリティリスクの特定（システムの脆弱性管理等）、③サイバー攻撃の防御・④サイバー攻撃の検知（認証・アクセス管理、データ管理）、⑤サイバーインシデント対応及び復旧（コンティンジェンシープランの策定）、⑥サードパーティリスクの管理、を提示。

◆ ガイドラインを踏まえ、より高いレベルでのサイバーセキュリティ対策が求められるなか、本邦金融機関としては、下記の取り組みが重要に。

①　経営層のコミットメントのもとでの主体的なサイバーセキュリティ対策
経営層のコミットメントのもと、各々の業務環境やビジネスモデル、顧客層等を勘案し、金融機関自身の判断でサイバーセキュリティ対策を講じることが重要。

②　サイバーセキュリティ人材の育成、セキュリティリテラシーの向上
サイバーセキュリティを所管するリスク部門やシステム部門に加え、事業部門も含めた幅広い部門でサイバー人材の配置が必要に。地域内、業界内で連携し、セキュリティ人材の育成やセキュリティリテラシー向上を図ることが重要。

③　サードパーティリスクへの対応力強化
金融機関のビジネスモデルやサプライチェーンが複雑化、多様化するなか、サイバーセキュリティの観点からも、サードパーティリスクの管理が重要に。サードパーティと問題意識を共有し、リスク管理態勢を整備する必要あり。

本件に関するご照会は、調査部　主任研究員　谷口栄治　宛にお願いいたします。

Tel：080-4377-3420
Mail：taniguchi.eiji@jri.co.jp

「経済・政策情報メールマガジン」、「X（旧 Twitter）」、「YouTube」でも情報を発信しています。

１．はじめに

経済・社会のデジタル化が急速に進むなか、あらゆる経済主体において、サイバーセキュリティ対策の重要性が高まっている。なかでも、金融セクターは、その社会的、経済的なインフラとしての性質から、サイバー攻撃の対象となりやすく、金融機関やその関連企業を標的とするサイバーインシデントも増加している。こうしたなか、本年 10 月、金融庁は、本邦金融セクター全体のサイバーセキュリティを強化するため、「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」（以下、ガイドライン）を策定し、各業態向けの監督指針や事務ガイドライン等を改訂した。そこで本稿では、金融セクターにおいて、サイバーセキュリティ対策が求められる背景、本ガイドラインの概要やポイントを整理したうえで、わが国の金融機関に求められる対応等について考察する。

２．金融セクターにおいてサイバーセキュリティ対策が求められる背景

企業や政府、個人といった様々な経済主体の活動がデジタル化するなか、グローバルベースでサイバーセキュリティの重要性が高まっている。なかでも、社会的に重要なインフラ機能を提供する業種・業界では、円滑な経済活動や社会秩序の維持等の観点から、より高いレベルでのサイバーセキュリティ対策が求められる。わが国では、サイバー対策の司令塔である内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）[1]が重要インフラを指定している。そこでは、交通インフラ（航空、空港、鉄道、物流）、エネルギーインフラ（電力、ガス、石油、化学）、生活インフラ（情報通信、医療、水道）、政府・行政サービスに加え、金融分野[2]も選定されている。金融セクターは、顧客の個人情報や保有金融資産、口座の入出金履歴など、機微な情報・データを大量に保有しているほか、資金管理や資金決済といった重要な金融取引の実務を担っていることもあり、サイバー攻撃の標的とされやすい業界である。実際、情報処理推進機構（IPA）が取りまとめた「情報セキュリティ 10 大脅威 2024」[3]によれば、重大なサイバーリスクとして、「ランサムウェアによる被害[4]」、「標的型攻撃による機密情報の窃取」、「インターネット上のサービスへの不正ログイン」など、金融機関自身の対応が求められる項目に加え、「クレジットカード情報の不正利用」、「スマホ決済の不正利用」、「フィッシングによる個人情報等の詐取」など、金融サービスに関連するリスクも挙げられている（図表１）。

---

[1] わが国では、2014 年 11 月に、「サイバーセキュリティ基本法」が成立。同法に基づき、2015 年 1 月、内閣に「サイバーセキュリティ戦略本部」が、内閣官房に「内閣サイバーセキュリティセンター（NISC）」が設置された。NISC の主な所掌事務は、①サイバーセキュリティ戦略本部の事務局機能、②行政各部の情報システムに対する不正な活動の監視・分析やサイバーセキュリティの確保に関する必要な助言、情報提供、その他の援助、監査等、③サイバーセキュリティ対策に関する総合調整、がある。

[2] 具体的には、金融、クレジットを選定。金融のなかに、銀行、証券、生命保険、損害保険、資金決済、が含まれている。

[3] 社会的に影響が大きかった過去の情報セキュリティ関連の事案から、IPA が脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約 200 名のメンバーからなる「10 大脅威選考会」が脅威候補に対して審議・投票を行い、決定したもの。「個人」、「組織」のセグメントに分類し、それぞれのリスクを選定。

[4] 企業や公的機関、組織のパソコン（PC）やサイトに不正アクセスしたり、コンピューターウイルスを感染させることで、PC 等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭や暗号資産）を要求する不正プログラム。身代金を意味する「Ransom」と「Software」を組み合わせた造語。

（図表１）「情報セキュリティ 10 大脅威 2024」で採り上げられたサイバーリスク

＜個人向け脅威＞	＜組織向け脅威＞
インターネット上のサービスからの個人情報の窃取	ランサムウェアによる被害
インターネット上のサービスへの不正ログイン	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	内部不正による情報漏えい等の被害
スマホ決済の不正利用	標的型攻撃による機密情報の窃取
偽警告によるインターネット詐欺	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
ネット上の誹謗・中傷・デマ	不注意による情報漏えい等の被害
フィッシングによる個人情報等の詐取	脆弱性対策情報の公開に伴う悪用増加
不正アプリによるスマートフォン利用者への被害	ビジネスメール詐欺による金銭被害
メールや SMS 等を使った脅迫・詐欺の手口による金銭要求	テレワーク等のニューノーマルな働き方を狙った攻撃
ワンクリック請求等の不当請求による金銭被害	犯罪のビジネス化（アンダーグラウンドサービス）

（資料）情報処理推進機構（IPA）「情報セキュリティ 10 大脅威 2024」をもとに日本総研作成

（注）色がついている項目は、金融サービスに関連すると想定されるリスク（日本総研によるもの）。

また、このような金融セクターにおけるサイバーリスクについては、国際通貨基金（IMF）や各国の金融当局から、金融システムや金融市場の安定を維持するうえで重大なリスクになると指摘されている[5]、。わが国のガイドラインでも、「サイバー攻撃の脅威は、金融サービス利用者の利益を害し、金融システムの安定に影響を及ぼしかねないもの」と警戒感を強めており、金融機関の「業務の健全性及び適切性の観点から、サイバーセキュリティの確保が重要である」と示されている。

このように、デジタル化が進展するなか、円滑な経済活動や社会秩序の維持、金融システムや金融市場の健全性・安全性の確保といった観点から、重要な社会インフラとなっている金融機関において、サイバーセキュリティ対策を強化することが責務となっている。

３．「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」の概要

（１）これまでの施策の経緯

サイバーリスクの高まりが意識されるなか、わが国では、金融機関のサイバーセキュリティを強化するため、様々な取り組みが進められてきた。具体的には、2015 年に金融庁から「金融分野におけるサイバーセキュリティ強化に向けた取組方針」が公表され、その後も、2018 年９

[5] IMF が 2024 年４月に公表した「Global Financial Stability Report（GFSR）」では、サイバーリスクの高まりが、金融システムや金融市場の安定に重大なリスクになるとしたうえで、金融機能の低下や経済活動の停滞といった悪影響をもたらしかねないと警鐘を鳴らしている。具体的には、①サイバーインシデントの対象となった金融機関の信用力が低下し、預金（預かり資産）の流出や調達コストの上昇につながる、②重要な金融機能（決済等）が停止し、経済活動が停滞する、③市場機能がマヒ（インターバンク市場の停止等）し、流動性危機につながる、といったリスクが指摘されている。

月、2022年２月の２度にわたってアップデートされた[6]。直近版では、①モニタリング・演習の高度化、②新たなリスクへの備え、③サイバーセキュリティ確保に向けた組織全体での取り組み、④関係機関との連携強化、⑤経済安全保障上の対応、といった項目が示されている。なかでも、①モニタリング・演習の高度化については、2016年以降、毎年業界横断的なサイバーセキュリティ演習（Delta Wall）が実施されている[7]。また、金融機関のサイバーセキュリティ管理態勢をチェックするため、金融機関に対してサイバーセキュリティセルフアセスメント（Cyber Security Self-Assessment、CSSA）の実施を求めるとともに、その結果を金融庁と日本銀行が集計、公表している。さらに、金融機関のサイバーセキュリティ管理態勢の監督について、金融庁は、監督指針や事務ガイドラインのなかで、検査やモニタリングを行うにあたって留意すべき点を定めるとともに、その結果に関して、各金融機関と対話を重ねてきた。

（２）ガイドラインの主な特徴

このようにわが国では、金融庁を中心に金融機関のサイバーセキュリティ強化が進められてきたが、本年10月、金融機関に対してサイバーセキュリティに関するより詳細な対応要件や対応事項を示すため、「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」が公表された[8]。本ガイドラインの主な特徴は、以下の３点である。

１点目は、サイバーセキュリティに関して金融機関が対応すべき事項が、従来の監督指針から切り離す形で示された点である。近年、世界各地で国家的な関与が疑われるようなサイバーインシデントが発生するなど、サイバー攻撃の手口が組織化、洗練化、巧妙化している。また、金融業界では、ブロックチェーンやクラウドを基盤とする金融商品・サービス、API連携を活用したBaaS（Banking as a Service）、生成AI（人工知能）といった技術進歩を受けて、金融機能やチャネルが多様化・複雑化し、サイバーインシデントに巻き込まれるリスクが年々高まっている。こうした状況下、従来監督指針に記載されていたサイバーセキュリティ関連の対応事項を、ガイドラインに拡充しつつ、明示することで、金融機関に求められるサイバーセキュリティ関連の対応やその重要性が強調されることになった。

２点目は、金融機関に求める対応として、「基本的な対応事項」と、「対応が望ましい事項」に分類された点である。「基本的な対応事項」は、すべての金融機関において対応が必須となる項目であり、いわゆる「サイバーハイジーン（IT資産の適切な管理、セキュリティパッチ適用などの基本的な行動を組織全体に浸透させる取り組み）」が該当する。一方、「対応が望ましい事項」は、金融機関の業態や規模、特性等を踏まえ、対応が求められる項目である。具体的には、大手金融機関や主要な清算・振替機関など、金融システムや金融インフラの安定の観点で重要な役割を果たしている金融機関が対応すべき項目と言えるだろう。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、

---

[6] 2018年の改訂は、2020年（当初）の東京オリンピック・パラリンピック等を念頭においたもの。2022年の改訂は、巧妙化したランサムウェア攻撃など、サイバー攻撃が多発化していることを受けたもの。

[7] この演習は、サイバーインシデント発生時における初動対応や原因の分析、システムトラブル時の顧客対応や封じ込め策、復旧対応、当局等との連携状況等を検証するとともに、結果や要諦を業界全体にフィードバックするというものである。開始当初は、銀行、信用金庫・信用組合、証券会社、保険会社といった伝統的な金融機関を対象としていたが、回を重ねる毎に、貸金業者、資金移動業者、外国為替証拠金取引業者（FX業者）、暗号資産交換業者、監査法人、等へと対象が拡大している。

[8] 本ガイドラインについては、同案が同年６月に公表され、同月28日～7月29日にかけて、パブリックコメントが募集された。

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うえで、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（いわゆる「リスクベース・アプローチ」を採ること）が求められる。

３点目は、本ガイドラインが、広範な金融機関を対象としている点である。具体的に、ガイドラインの対象は、銀行・信用金庫（主要行等、中小・地域金融機関）、保険会社（少額短期保険業者含む）、金融商品取引業者等、信用格付業者、貸金業者、前払式支払手段発行者、電子債権記録機関、指定信用情報機関、資金移動業者、清算・振替機関等、金融サービス仲介業者、為替取引分析業者、暗号資産交換業者、銀行代理業、電子決済手段等取引業者、電子決済等取扱業者、電子決済等代行業者、農漁協系統金融機関、金融商品取引所が対象となっている。伝統的な金融機関にとどまらず、足元にかけてプレゼンスが拡大している新興の金融機関（FinTech 事業者等）も対象とすることで、金融業界全体としてサイバーセキュリティに取り組む姿勢が示されている。

（３）ガイドラインで示された「サイバーセキュリティ管理態勢」に関する取り組み

ガイドラインでは、金融機関に求められる取り組みとして、主に「サイバーセキュリティ管理態勢」の整備が示されている[9]。本稿では、サイバーセキュリティ管理態勢について、ガイドラインで示された主な取り組みを項目ごとに整理する。

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管理の基本方針の策定、検証
- 基本方針に基づいた管理態勢の整備、戦略・取組計画の策定及び進捗確認
- 基本方針に基づいた規定、業務プロセスの整備、必要に応じた見直し
- 経営資源の確保、人材の育成、最適な人員配置
- リスク管理部門による牽制（業務部門等から独立した監視・牽制）
- 内部監査（必要に応じて外部専門家からの知見を活用）

取締役会などが、サイバーセキュリティリスクを組織全体のリスク管理の一部として捉えたうえで、サイバーセキュリティ管理の基本方針を策定することが求められている。これまで金融機関では、サイバーセキュリティ対策に関するマニュアル等を整備・実装してきたが、今後はより高い目線で、経営陣がコミットする形で、基本方針として取りまとめることが必要とされた。その基本方針では、①セキュリティ対策の目的や方向性、②関係主体等（顧客、地域社会、株主、当局等）からの要求事項への対応および法規制等への対応、③経営陣によるコミットメント、を記載することとされ、これに基づいて、サイバーセキュリティに関する個別の戦略や取組計画の策定や、規定や業務プロセスの整備等を行うとともに、必要に応じてそれらを見

9 「サイバーセキュリティ管理態勢」以外では、「金融庁と関係機関の連携強化」が採り上げられている。具体的には、①金融庁と NISC、日本銀行、金融 ISAC、金融情報システムセンター（FISC）、CEPTOAR 等との情報共有・連携、②捜査当局等との連携、③国際連携の深化（海外当局との連携）、④官民連携、が挙げられている。

直すことが定められた。

また、ガイドラインでは、経営陣が、年に一回、①自組織を取り巻くサイバーセキュリティリスクの状況（自組織におけるサイバーインシデント発生状況、国内外・業界におけるサイバーインシデント発生状況、重大な脆弱性情報等）、②サイバーセキュリティに関するリスク評価（第三者評価を含む）の結果、③取組計画の進捗状況、について、リスク管理部門から報告を受けることが必要とされたほか、大手金融機関等には、「対応が望ましい項目」として、少なくとも年に２回、サイバーセキュリティにかかるパフォーマンス指標（KPI）及びリスク指標（KRI）に関する報告を受けることが求められた。

さらには、サイバーセキュリティ強化に向けた経営資源の確保については、とりわけ、人材確保や人材育成に焦点があてられた。本ガイドラインでは、「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などに、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」とされたほか、「サイバーセキュリティ管理の基本方針と整合的な人材の育成・確保のための計画（人材育成計画、採用計画及び教育研修・訓練計画など）を策定すること」、「サイバーセキュリティ確保に向けた組織風土醸成のためにも、経営陣が積極的に研修・訓練等に参加すること」、「サイバーセキュリティ人材の育成については、外部人材の活用も含め、計画的に確保していくこと」等が示された。

② サイバーセキュリティリスクの特定

- 情報資産（情報システム・外部システムサービス、ハードウェア・ソフトウェア、データ等）の管理
- リスク管理プロセス（脅威情報・脆弱性情報の収集・分析、リスクの特定・評価、リスク対応等）
- ハードウェア・ソフトウェア等の脆弱性管理
- 脆弱性診断及びペネトレーションテストの定期的な実施
- サイバーインシデントに対する定期的な演習・訓練の実施

サイバーリスクを特定、把握するために必要となる事項が示されている。具体的には、自社の情報資産（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）、③ネットワーク）の整備やメンテナンスが求められたほか、自社のみならず、他金融機関や他業態におけるサイバーインシデントの情報を収集、分析することが必要とされた。また、テスト（脆弱性診断、ペネトレーションテスト）や演習・訓練を定期的に実施することで、自社のシステムや対応計画等のリスクや脆弱性を特定、把握することが重要とされた。

③サイバー攻撃の防御 ・ ④サイバー攻撃の検知

- 認証・アクセス管理（アクセス権、アカウントの適切な管理、認証要件の設定 等）
- サイバーセキュリティに関する教育・研修の実施
- データ管理方針の策定、データ保護、バックアップの確保

システムのセキュリティ対策（ハードウェア・ソフトウェア管理、ログ管理、セキュリティ・バイ・デザイン、インフラストラクチャ（ネットワーク等）の技術的対策、クラウドサービス利用時の対策）
- サイバー攻撃検知に向けた継続的な監視

サイバー攻撃を防御したり、それを事前に検知するための対応事項が示されている。具体的には、自社システムへの不正侵入や不正利用、外部への情報漏えい等を防止、抑止するため、アクセス権限やアカウント（ID）管理を適切かつ厳格に行うほか、システムの重要度等に応じて、認証要件を設定することが求められた。

またデータ管理についても、その重要度に応じて、暗号化や認証、アクセス制御等の保護策を講じることが要されたほか、システムのセキュリティ対策として、ハードウェア・ソフトウェア管理の管理、適切なログの管理、インフラ（ネットワーク）やクラウドサービスに係るセキュリティ対策等を講じることが必要とされた。なかでも、「セキュリティ・バイ・デザイン」の確保は、新たな取り組みとして挙げられる。セキュリティ・バイ・デザインとは、新たなシステムやデジタルサービスを展開するにあたって、その企画・設計段階から、セキュリティ要件を組み込む考え方である。金融機関にとって、デジタル技術を活用したサービスの開発が不可欠となるなか、サイバーセキュリティを考慮することが基本的な行動として位置づけられることとなった。

⑤ サイバーインシデント対応及び復旧

- 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
- インシデントへの対応及び復旧（初動対応、分析、顧客対応、組織内外の連携、広報、封じ込め、根絶、復旧）

サイバーインシデントが発生した際の対応計画やコンティンジェンシープランの策定や、そこに含まれるべき内容等が示されている。対応計画については、サイバー攻撃の種別ごとに、対応の優先順位や目標復旧時間、目標復旧水準を定めることが求められた。また、①初動対応（インシデントの検知等）、②インシデント発生時の情報公表や情報伝達、注意喚起（顧客対応、内外連携、広報）、③被害拡大の防止（封じ込め）、④原因の特定、根絶、⑤システムの復旧、といった段階に応じた具体的な対応が必要と示されている。

⑥ サードパーティリスクの管理

- サードパーティを含む業務プロセス全体を対象としたサイバーセキュリティ態勢の整備
- サードパーティリスク管理の方針の策定、組織体制や規定の整備
- サードパーティのデューデリジェンス
- 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の明確化

サードパーティリスクとは、システム会社やシステムベンダー、クラウド等のサービス提供

事業者、業務提携先、API 連携先といった外部組織（サードパーティ）から生じるサイバーリスクを指す。足元で金融機関がサードパーティの提供するシステムやインフラを活用したり、外部機関と API 等を通じてシステム連携したりする事例が増加するなか、このサードパーティリスクの適切な管理が重要となっている。こうしたなか、ガイドラインでは、金融機関に求められるサードパーティリスク管理に関して、リスク管理方針の策定や組織体制、社内規定の整備、取引開始時のデューデリジェンスや提供される商品・サービスのモニタリング等を通じたリスクの評価、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の明確化等の対応事項が示された。

４．ガイドラインを踏まえ金融機関に求められる対応

サイバーリスクの高まりが意識されるなか、金融セクターにおいても主要金融機関を中心に対策が進められてきたが、今般、金融庁から、本稿で概説したガイドラインが策定されるなど、金融システムの安定性や金融市場の機能維持の観点から、より高いレベルでのサイバーセキュリティ対策が求められることとなった。このような当局の姿勢を踏まえ、サイバーセキュリティの強化に向けて、金融機関（主として地域金融機関）に求められる対応の要諦を３点指摘したい。

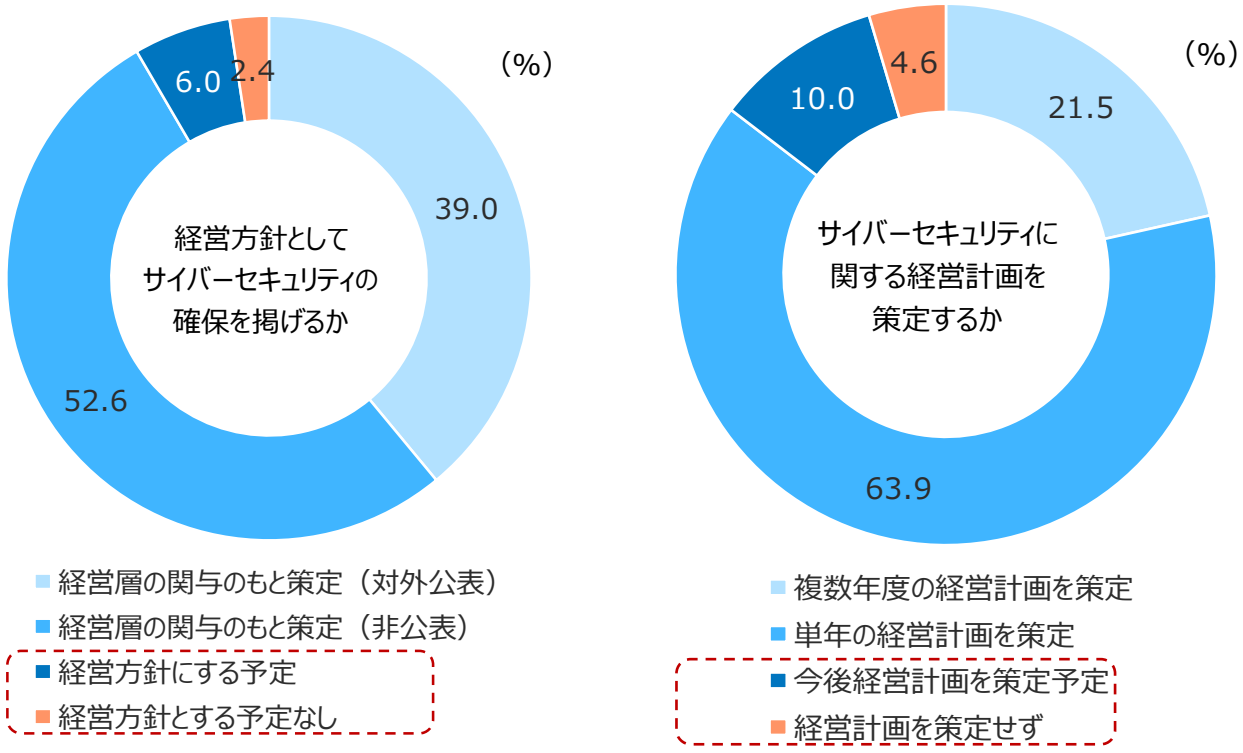
（１）経営層のコミットメントのもとでの主体的なサイバーセキュリティ対策

ガイドラインを受けて、金融機関には、サイバーセキュリティに係る経営方針や経営戦略の策定、それを踏まえた組織体制の整備や業務プロセスの再構築、実効性のある不正対策の検討・推進、経営資源の確保、システム基盤やデータ等の適切な管理、コンティンジェンシープランの策定、サードパーティリスクの管理など、多岐にわたる対応が求められる。これらにあたって重要となるのが、経営層によるコミットメントである。金融機関に限った話ではないが、サイバーセキュリティ対策は、往々にして「守り」の施策と位置付けられ、経営層の関心が高まらず、必要な態勢整備や投資が後回しになったり、施策の検討が関係部署任せになったりするケースが存在する。例えば、地域金融機関を対象とした日本銀行のアンケート調査[10]では、サイバーセキュリティの確保を経営方針として掲げていない先が８％、サイバー関連の経営計画を策定していない先が 15%程度存在するとの結果が示されている（図表２）。過去と比較すれば、状況は改善しているものの、地域金融機関を含めたすべての金融機関が、経営層のコミットメントのもとで、サイバーセキュリティ対策の強化を経営戦略上の重要なイシューとして位置づけ、態勢整備を主体的に進めていくことが不可欠である。

この点、今回のガイドラインでは、金融機関自身が、自らの事業戦略やリスク許容度等を踏まえたうえで、サイバーリスクを特定、評価し、リスクに見合った措置を講じるという「リスクベース・アプローチ」が採用されている。つまり、ガイドラインの内容を画一的にチェックリストのような形で確認するのではなく、金融機関自身が業務環境やビジネスモデル、顧客層等を考慮し、最適な資源配分のもと、自らの経営判断でサイバーセキュリティ対策を講じることが重要になる。

10 日本銀行「地域金融機関におけるサイバーセキュリティアセスメントの集計結果（2023 年度）」。地域金融機関 498 先（地域銀行 99、信用金庫 254、信用組合 145）を対象としている。

（図表２）地域金融機関におけるサイバーセキュリティ戦略への経営層の関与状況



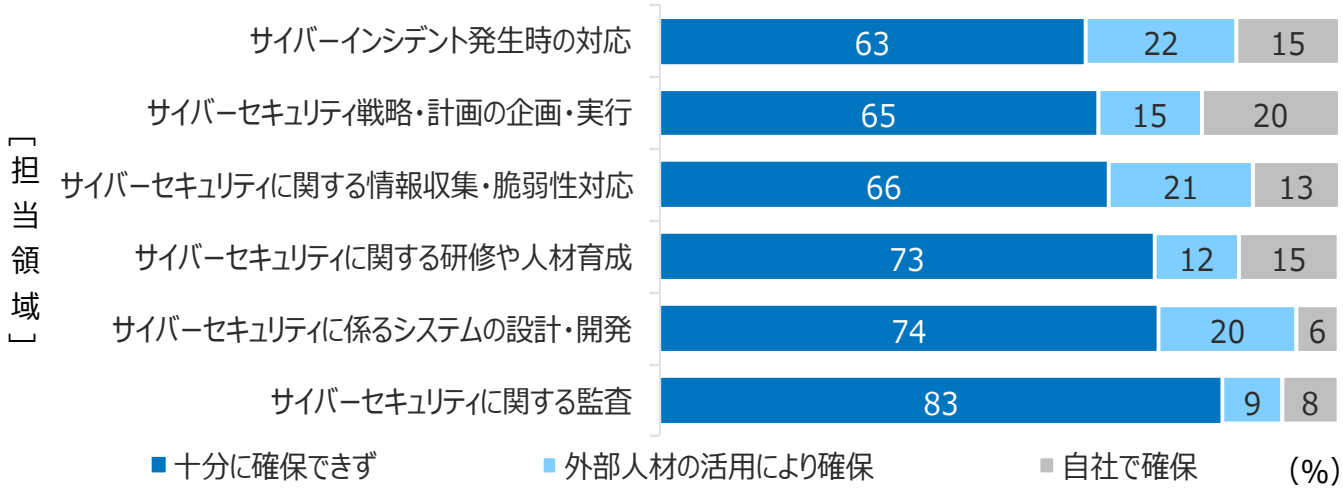
（資料）日本銀行「地域金融機関におけるサイバーセキュリティセルフアセスメントの集計結果（2023 年度）」をもとに日本総研作成

（注）地域金融機関 498 先（地域銀行 99、信用金庫 254、信用組合 145）を対象。

（２）サイバーセキュリティ人材の育成、セキュリティリテラシーの向上

より高いレベルでのサイバーセキュリティ対策を進めるためには、これらを担うサイバーセキュリティ人材の確保・育成が急務となる。日本銀行のアンケート調査によれば、６割超の地域金融機関が、サイバーインシデント発生時の対応や、サイバーセキュリティ戦略等の企画・立案を行う人材を十分確保できていないと回答するなど、同人材の不足が指摘される（図表３）。

（図表３）地域金融機関におけるサイバーセキュリティ人材の確保状況

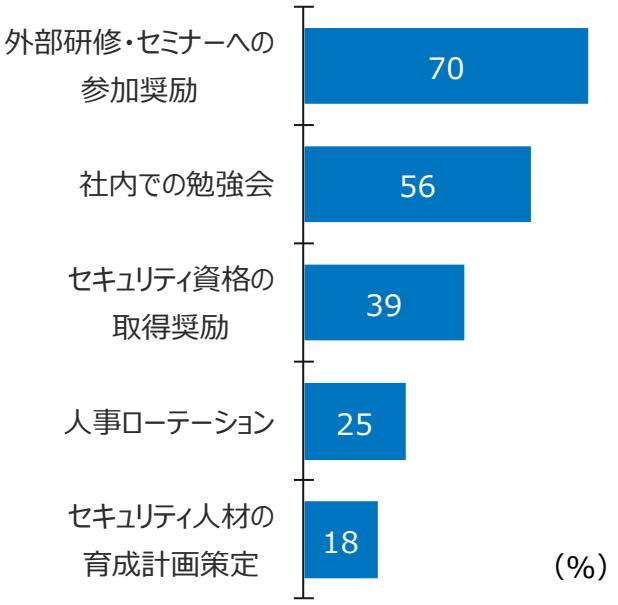


（資料）日本銀行「地域金融機関におけるサイバーセキュリティセルフアセスメントの集計結果（2023 年度）」をもとに日本総研作成

また、従来のサイバーセキュリティ対策は、既存のシステムやサービスに具備していくものとの考え方が主流であったが、ガイドラインでは、新たなシステムやデジタル関連のサービスを企画・開発・設計する段階から、サイバーセキュリティ対策を組み込むという「セキュリティ・バイ・デザイン」が「基本的な対応」として求められている。つまり、サイバーセキュリティを所管するシステム部門やリスク部門に加え、事業部門においても、セキュリティリテラシーを有する人材を育成・配置することが求められる。

現在、サイバーセキュリティ人材の育成に関する金融機関の取り組みとしては、外部研修・セミナー等への参加、社内での勉強会の実施など、比較的対応しやすい施策が中心となっている一方、人事ローテーションやセキュリティ人材の育成計画の策定など、中長期的な取り組みは十分に着手できていないのが実情である（図表４）。前述の通り、サイバーセキュリティ対策の経営上の重要性が高まり、幅広い部門でそのノウハウが求められるなか、今後は、サイバーセキュリティ人材の確保・育成に向けて、外部機関とも連携しながら、精力的な取り組みが求められる。例えば、人材不足が懸念される地域金融機関においては、地方公共団体や地域の学術機関（大学等）、経済団体など、地域内での産・学・官・金の連携のもと、サイバーセキュリティに関する研究や人材育成カリキュラムの策定等を進めるといった取り組みが考えられる。また、自らの取り組みのなかで得られたサイバーセキュリティ等に関するノウハウや知見を、顧客、なかでも自社でのリソースが限られる中堅・中小企業や医療法人向けのソリューションに、うまく取り込んでいくことも有用になる。同時に、業界内においても、他の金融機関や、金融 ISAC （Information Sharing and Analysis Center）、金融情報システムセンター（FISC：The Center for Financial Industry Information Systems） といった関連機関とも連携し、サイバーセキュリティ対策に関する情報や知見、実務面でのノウハウ等の共有を進めていくことが重要となる。

（図表４）サイバーセキュリティ人材育成の取り組み



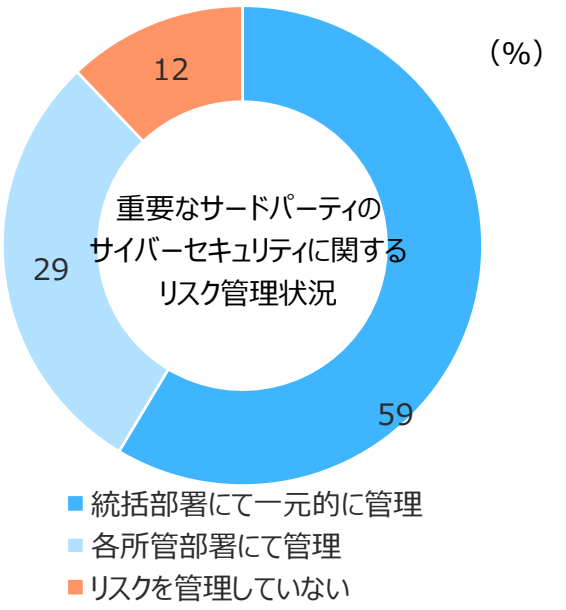
（資料）日銀「地域金融機関におけるサイバーセキュリティセルフアセスメントの集計結果（2023 年度）」をもとに日本総研作成

（３）サードパーティリスクへの対応力強化

外部機関と連携した金融チャネルやサービスの提供、内部管理システムにおけるクラウドサービスの活用など、金融機関のビジネスやサプライチェーンが複雑化、多様化するなか、サイバーセキュリティの観点から、サードパーティリスクの管理が重要となる。この点、ガイドラインでは、サードパーティリスク管理に関して、サードパーティを含んだ包括的なサイバーセキュリティ管理態勢の整備、サードパーティリスクを一元的に管理する統括部所の設置、サードパーティリスクの適切な評価・デューデリジェンス等を「基本的な対応」として実施すべき

旨が示されている。もっとも、これについては、重要なサードパーティ[11]に関連するサイバーリスクの管理状況をみると、統括部署において一元的に管理しているとの回答は金融機関の６割弱にとどまっており、同リスクを管理していないとの回答も１割強みられるなど、対応は道半ばといえる（図表５）。とりわけ、地域金融機関では、基盤システムの共同利用や、クラウドサービスの活用等を進めているだけに、サードパーティリスクを統括的に管理する態勢を構築するとともに、サードパーティと問題意識を共有し、リスクに関する定期的な情報連携やアセスメントの実施、インシデント発生時の対応要領の策定等を進めていくことが肝要となる。

（図表５）サードパーティ関連のサイバーリスクの管理状況



（資料）日銀「地域金融機関におけるサイバーセキュリティセルフアセスメントの集計結果（2023 年度）」をもとに日本総研作成
（注）「重要なサードパーティ、また、それらが提供するサービス等のサイバーセキュリティに関するリスク管理状況」に関する調査結果。

同時に、ガイドラインでは、金融機関にサービスを提供するサードパーティに対しても、「金融機関等によるサイバーセキュリティリスクの適切な管理のために、必要な支援（当該サードパーティに関するサイバーセキュリティリスクを含め、金融機関が必要な情報を利用できるようにすることなど）を行うべき」と明記されている。これらは、クラウドサービスやシステムインフラを提供するシステムベンダー等が主に該当するとみられるが、金融機関のなかにも、API 連携を通じて金融機能を提供する事業者も存在する。こうした金融事業者については、ガイドラインに基づいて、自らのサイバーセキュリティ対策を講じるとともに、サプライチェーンの一角として、サービスを提供する金融機関のリスク管理態勢の整備に貢献していくことが求められる。

５．おわりに

経済・社会活動のデジタル化や地政学リスクの高まり等に伴い、サイバーセキュリティ対策の重要性は年々増大している。とりわけ、金融機関は、日常生活や企業活動を営むうえで不可欠なインフラ機能を提供しているほか、大量の顧客情報やデータを扱うという業界の特性もあり、金融システムや金融市場の安定の観点からも、サイバーセキュリティ対策は重要な課題となる。今般策定された「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」は、そうした問題意識を反映したものであり、本邦金融機関としては、経営層のコミットメントのもと、人材育成やシステム整備、サードパーティリスク管理など、これまでよりも高いレベルでのサイバーセキュリティ対策やそのための態勢整備を進めていくとともに、金融セクター全体

[11] 本アンケート調査では、「重要なサードパーティ」は、「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」と定義している。

で機運を高めていくことが不可欠になるだろう。

＜参考文献・資料＞

- 金融庁「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」（2024 年 10 月）
- 金融庁 「金融分野におけるサイバーセキュリティ強化に向けた取組方針」
  （初版：2015 年 7 月、第２版：2018 年 10 月、第３版：2022 年２月）
- 日本銀行・金融庁
  「地域金融機関におけるサイバーセキュリティセルフアセスメントの集計結果（2023 年度）」
  （2024 年４月）
- 独立行政法人 情報処理推進機構（IPA）
  「情報セキュリティ 10 大脅威 2024［個人編］［組織編］」
- 谷口 栄治［2024］「サイバーリスクの高まりがもたらす金融システムへの影響と対策の方向性」 日本総研 Viewpoint No,2024-010 （2024 年 5 月 23 日）