Report 4

金融分野におけるサイバーセキュリティ対応

金融セクターでは、その社会的・経済的なインフラとしての重要性から、サイバーセキュリティ対応が喫緊の課題となっている。わが国では、金融庁が2024年10月に「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」を発表しており、金融機関には、その内容を踏まえ、主体的な対応が必要となる。

谷口 栄治　調査部金融リサーチセンター 主任研究員

サイバーセキュリティ対策の重要性

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、2024年10月、金融庁は、わが国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）を策定した。

「ガイドライン」を踏まえた対応のポイント

ガイドラインでは、さまざまな業態の金融機関を対象に、サイバーセキュリティに関して対応すべき事項が示されている。具体的には、①サイバーセキュリティ管理態勢の構築、②サイバーセキュリティリスクの特定、③サイバー攻撃の防御、④サイバー攻撃の検知、⑤サイバーインシデント対応及び復旧、⑥サードパーティリスクの管理である（**図表**）。これを受けて、金融機関に求められる対応のポイントとして、以下の5点を指摘したい。

(1) 経営陣のコミットメント

サイバーセキュリティ対策は、「守り」の施策と位置づけられ、経営陣の関心が薄くなったり、対応が後回しにされたりするケースもあるが、そのような意識では甚大なサイバーインシデントを防げない。サイバーセキュリティ対策を経営戦略上の重要なイシューと位置づけ、経営資源の配分、管理態勢の整備、組織としてのマインド醸成に継続的に取り組む必要がある。

(2) 主体的な対応・不断の見直し

ガイドラインの特徴の1つが、「リスクベース・アプローチ」である。これは、金融機関の業態や規模、顧客層、提供するサービス等に応じて、対応項目が異なるという考え方である。そのため、ガイドラインを「遵守すべきルール」と位置づけ、チェックリストを作って、画一的・機械的に埋めるような対応は適切でなく、金融機関自身が、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不可欠である。現状の管理態勢がいつまでも万全とは限らず、不断の検証・フィードバックによる継続的なアップデートが必要となる。

(3) セキュリティ人材の育成、セキュリティ・リテラシーの醸成

サイバーセキュリティ人材の育成・確保が急務であり、ガイドラインでは、「セキュリティ・バイ・デザイン」の確保が基本的な対応として示されている。これは、新たなシステムやサービスの開発にあたっては、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。サイバーセキュリティの所管部署（システム、リスク管理）に加え、事業部門や監査部門におけるセキュリティ人材の配置や、組織全体でのセキュ

図表「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

	概要
サイバーセキュリティ管理態勢	・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、業務プロセスの整備、戦略・取組計画、規定の策定 ・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、内部監査による牽制（業務部門等から独立した監視・牽制）
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） ・脆弱性診断及びペネトレーションテスト、演習・訓練の定期的な実施
サイバー攻撃の防御・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） ・データ管理方針の策定、データ保護、システムのセキュリティ対策 ・サイバー攻撃検知に向けた継続的な監視
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、顧客対応、組織内外の連携、広報、復旧等）
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、遵守すべきサイバーセキュリティ要件の明確化

出所：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」を基に日本総研作成

リティ・リテラシーの醸成が必要となる。金融機関としては、外部研修・セミナーの参加等にとどまらず、人材育成計画の策定、人事制度改定など、包括的な対応が求められる。

(4) サードパーティリスクへの対応力強化

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。金融機関において、外部機関と連携した金融サービスや取引チャネルの開発、内部管理システムにおけるクラウドサービスの活用が進むなか、提携機関（サードパーティ）を含めたサプライチェーン全体のサイバーセキュリティ管理態勢の強化が不可欠となる。サードパーティリスクを統括的に管理する態勢の構築、サードパーティとの問題意識やリスク情報の共有、サードパーティも参加した訓練やテストの実施、インシデント発生時の対応要領の策定が求められる。

(5) 情報・ノウハウの共有を通じた「集合知」の形成

サイバーセキュリティは重要な経営戦略事項ではあるが、その巧拙を競うものではなく、セクター全体の対応力を高めるものと認識する必要がある。金融機関単独ですべての課題に対応をすることは困難であり、業界横断的、官民連携での対応が求められる。金融機関、業界団体、当局（金融庁、日本銀行）、金融ISAC、金融情報システムセンターといった機関と連携し、サイバーセキュリティに関する「集合知」を形成していくことが重要となる。

おわりに

サイバーセキュリティ対策の重要性が年々増すなか、金融システムや金融市場の安定の観点から、金融機関のサイバーセキュリティ対策は重要な課題となる。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、金融セクター全体で対応することが不可欠である。

Profile

谷口 栄治

（たにぐち・えいじ）

2007年三井住友銀行入行。2010年7月から2012年6月、経済産業省経済産業政策局調査課。2012年7月から、三井住友銀行経営企画部金融調査室。2020年4月より、日本総研調査部金融リサーチセンター。