金融庁による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
―経営課題としての意識や連携・共助の強化がカギ―

江夏　あかね

▌要　約▐

1. 金融庁は 2024 年 10 月 4 日、「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）を公表した。ガイドラインは、監督指針等とは別のものとして、さらに詳細な内容が盛り込まれた形での策定となった。
2. ガイドラインの適用対象となっている金融機関等は、銀行、証券を始めとして 21 の業種にわたっており、業界横断的と言える。サイバーセキュリティ管理態勢については、「基本的な対応事項」と「対応が望ましい事項」と 2 段階に分けて説明されているほか、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が求められるとの留意点が示された。さらに、昨今注目が集まっているサードパーティに関するリスク管理についても独立した項目が挙げられた。
3. ガイドラインは、公表と同時に適用されたこともあり、対象金融機関等は 2 段階の対応事項や自身が取り巻く状況も踏まえて、サイバーセキュリティ管理態勢を改めて見直し、強化する必要がある。金融業界全体でサイバーセキュリティリスクを軽減し、業務の健全性及び適切性を確保していくための論点としては、（1）企業価値に影響を及ぼし得る経営課題としての意識の醸成、（2）連携と共助の強化、（3）投資家との対話も通じた態勢見直し・強化、が挙げられる。
4. 特に、1 点目について、サイバーセキュリティは情報技術（IT）課題ではなく、企業価値に影響を及ぼし得る経営課題であることを改めて意識し、経営陣のリーダーシップの下、管理態勢の強化にコミットしていくことが重要と言える。

野村資本市場研究所　関連論文等

・門倉朋美・江夏あかね「金融資本市場における当局・金融機関によるサイバーリスクへの対処」『野村サステナビリティクォータリー』第 5 巻第 3 号（2024 年夏号）。
・江夏あかね「サイバーセキュリティと企業価値―投資家による評価と効果的な情報開示―」『野村サステナビリティクォータリー』第 5 巻第 2 号（2024 年春号）。

Ⅰ 金融機関等の業務の健全性及び適切性確保に向けたガイドライン

金融庁は2024年10月4日、「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）を公表した[1]。金融機関等[2]は、各業法[3]において業務の健全性及び適切性を確保することが求められており、金融庁は「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」の発出や、各監督指針・事務ガイドライン（監督指針等）の規定に基づく検査・モニタリング等の実施を通じて、金融セクター全体のサイバーセキュリティ強化を促進してきた（図表1参照）。そして、今般、これまでの検査・モニタリング結果及び金融セクター内外の状況の変化を踏まえて、監督指針等とは別のものとして、さらに詳細な内容を盛り込む形でのガイドラインの策定となった。

図表1　日本の主なサイバーセキュリティ関連の政策動向

年月	概要
2014年11月	サイバーセキュリティ基本法、成立
2015年1月	内閣に「サイバーセキュリティ戦略本部」、内閣官房に「内閣サイバーセキュリティセンター（NISC）」設置
2015年7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（Ver. 1.0）」を公表（2018年10月にVer. 2.0、2022年2月にVer. 3.0を公表）
2015年12月	経済産業省と独立行政法人情報処理推進機構（IPA）、「サイバーセキュリティ経営ガイドライン（Ver. 1.0）」を公表（2017年11月にVer. 2.0、2023年3月にVer. 3.0を公表）
2016年10月	金融庁、金融業界横断的なサイバーセキュリティ演習（Delta Wall）の初回を実施（2024年10月に9回目を実施）
2019年1月	「企業内容等の開示に関する内閣府令」改正（有価証券報告書における「事業等のリスク」に関する情報の充実を求める）
2019年3月	金融庁、「記述情報の開示に関する原則」、「記述情報の開示の好事例集」を公表（同事例集の最新版は2024年3月公表）
2019年6月	総務省、「サイバーセキュリティ対策情報開示の手引き」を公表
2023年1月	「企業内容等の開示に関する内閣府令」等改正（有価証券報告書等において、「サステナビリティに関する考え方及び取組」の記載欄を新設。金融庁、サステナビリティ情報にサイバーセキュリティ等に関する事項が含まれ得るとの考えを提示）
2023年4月	日本銀行と金融庁、2022年度分の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（CSSA）の集計結果を公表（2023年度分は、2024年4月に公表）
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に関するガイドライン」を公表

（注）　2024年10月末時点。
（出所）各種資料、より野村資本市場研究所作成

1　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4日。
2　ガイドラインの適用対象となる金融機関等は、図表2を参照。
3　銀行法第12条の2第2項、金融商品取引法第35条の3、保険業法第100条の2の1第1項等（前掲注1参照）。

Ⅱ ガイドラインの概要

ガイドラインは、3 節（基本的考え方、サイバーセキュリティ管理態勢、金融庁と関係機関の連携強化）で構成されている（図表 2 参照）。

図表 2　ガイドラインの概要

項目	概要	
1. 基本的考え方		
サイバーセキュリティに係る基本的考え方	金融機関等は、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。監督指針等とは別に、さらに詳細な本ガイドラインを策定	
金融機関等に求められる取組み	金融機関等には、関係法令、監督指針等及び本ガイドライン等の趣旨を踏まえ、実質的かつ効果的な対応を行うことが求められている。組織全体としての対応を実現するためのガバナンスの確立、そのためには経営陣のリーダーシップが不可欠	
業界団体や中央機関等の役割	業界団体や中央機関等が必要に応じて当局と連携しながら、金融機関等による対応の向上に中心的・指導的な役割を果たすことが望ましい	
本ガイドラインの適用対象等	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、主要行等、中小・地域金融機関、保険会社、少額短期保険業者、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	
2. サイバーセキュリティ管理態勢		
	基本的な対応事項	対応が望ましい事項
サイバーセキュリティ管理態勢の構築	・ 基本方針の策定、経営報告の実施（年 1 回以上）	・ サイバーセキュリティにかかるパフォーマンス指標（KPI）・リスク指標（KRI）の経営報告の実施（年 2 回以上）
サイバーセキュリティリスクの特定	・ 内部ネットワーク配下のシステムもリスク評価対象に追加 ・ 脆弱性対応は「適用」することを前提に検討 ・ 内部環境のセキュリティ上の根幹となる機器への脆弱性診断の実施	・ ソフトウェア部品表（SBOM）の整備 ・ インターネット接続のない仮想プライベートネットワーク（VPN）や内部システムへの脆弱性診断 ・ 脅威ベースペネトレーションテスト（TLPT）の実施
サイバー攻撃の防御	・ 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」の実践 ・ ランサムウェア攻撃リスクを考慮したバックアップ・隔離保護等の実施	・ セキュリティ技術・アーキテクチャーに係る設計標準の策定 ・ DLP（Data Loss Prevention）等を導入したデータ漏えい監視
サイバー攻撃の検知	・ 未承認のハード／ソフトウェアや、不正なアクセス等の検知	・ 常時監視、SIEM（Security Information and Event Management）による監視（各種ログの集約・相関分析）
サードパーティリスク管理	・ サードパーティの特定・把握 ・ リスク評価に応じた対応、取引開始時のデューデリジェンスの実施 ・ 契約、SLA（Service Level Agreement）への言及（監査権、診断・外部評価の実施等）	・ 重要なフォースパーティ（サードパーティの再委託先等）の定期的なモニタリング、代替手段のテスト ・ 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法）における「リスク管理措置」を講じること
3. 金融庁と関係機関の連携強化		
情報共有・情報分析の強化	金融庁は、内閣サイバーセキュリティセンター（NISC）、日本銀行、金融 ISAC（Information Sharing and Analysis Center）、金融情報システムセンター（FISC）及び各 CEPTOAR（重要インフラ事業者等の情報共有・分析機能等を担う組織）との連携を維持・強化	
捜査当局等との連携	金融庁は、金融犯罪における手口の変化を注視し、注意喚起や啓発による金融犯罪の未然防止と被害拡大防止のための活動を警察及び業界団体等と連携して行う	
国際連携の深化	金融庁は、国際的な議論に参画し、海外当局と連携する	
官民連携	金融庁は、共助機関及び金融機関等と連携して金融セクター全体の取組みを推進するとともに、モニタリング等を通じ、個々の金融機関等及び業界の底上げを進める	

（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」2024 年 10 月 4 日、上杉信孝「サイバーセキュリティガイドラインへの対応：リスク管理高度化への留意点」『金融 IT フォーカス』野村総合研究所、2024 年 10 月、より野村資本市場研究所作成

主な特徴としては、（1）業界横断的な適用対象、（2）2 段階の対応事項と「リスクベース・アプローチ」、（3）サードパーティ[4]リスク管理、が挙げられる。

１．業界横断的な適用対象

ガイドラインの適用対象となっている金融機関等は、21 の業種にわたっている。この中では、銀行、証券、保険といった伝統的な業種のみならず、情報化社会の進化も背景に存在感が増している暗号資産交換業者等も含まれている。

２．2 段階の対応事項と「リスクベース・アプローチ」

ガイドラインの第 2 節（サイバーセキュリティ管理態勢）においては、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に関する着眼点について規定している。そして、それぞれの点について、「基本的な対応事項」と「対応が望ましい事項」と 2 段階に分けて説明されている（図表 3 参照）。

なお、ガイドラインにおいては、両段階いずれについても、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が求められるとの留意点が示されている。リスクベース・アプローチは、「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」と説明されている。

図表 3　2 段階の対応事項

段階	内容
基本的な対応事項	いわゆるサイバーハイジーン(注)と呼ばれる事項その他の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	金融機関等の規模・特性等を踏まえると、インシデント発生時に、地域社会・経済等に大きな影響を及ぼしうる先において実践することが望ましいと考えられる取組みや、他国の当局又は金融機関等との対話等によって把握した先進的な取組み等の大手金融機関及び主要な清算・振替機関等が参照すべき優良事例

（注）　情報技術（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組み。

（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」2024 年 10 月 4 日、より野村資本市場研究所作成

[4] サードパーティとは、自組織がサービスを提供するために、業務上の関係や契約等を有する他の組織を言う（例：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、資金移動業者等の業務提携先、API〔Application Programming Interface〕連携先）。外部委託先とは、業務を委託している組織を言う（金融機関等が金融サービスを提供するために外部委託するシステム〔共同センター等を含む〕のベンダーなど。形式上、外部委託契約が結ばれていなくともその実態において外部委託と同視しうる場合や当該外部委託された業務等が海外で行われる場合も含む）（前掲注 1 参照）。

３．サードパーティリスク管理

金融業界においては近年、システム子会社やベンダー等の外部委託先を始めとしたサードパーティへの依存度が増大していることもあり、サードパーティリスク管理の重要性が増している。例えば、米国では 2023 年にクラウド情報技術（IT）サービスプロバイダに対するランサムウェア攻撃が発生し、約 60 の信用組合のサービスが一斉に停止したといった事案が発生した[5]。日本でも、（1）印刷業務や情報処理を企業等から請け負うイセトーが 2024 年 5 月にランサムウェアを利用したサイバー攻撃を受け、同社に業務委託していた多くの企業で顧客の個人情報等が漏えいし、その被害が保険会社、信託銀行、地方銀行、信用金庫にまで及んだ、（2）髙野総合会計事務所へのランサム攻撃を通じて保険会社や地方銀行において個人情報の漏えいが明るみになった、といった事案が起きている[6]。その一方で、日本銀行と金融庁が 2024 年 4 月に公表した「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）」においては、重要なサードパーティリスクについて統括部署にて一元的に管理している先は全体の 6 割弱にとどまったほか、リスクを管理していない先も 1 割強見られたといった状況が示された[7]。

このような背景も踏まえ、本ガイドラインでは、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管理態勢の整備等が対応事項として記された（図表 4 参照）。

図表 4　サードパーティリスク管理に関する対応事項の概要

段階	内容
基本的な対応事項	1. サイバーセキュリティに係る戦略、取組計画を策定する際にはサプライチェーン全体を考慮。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管理態勢を整備 2. サードパーティのリスク管理のライフサイクル全体を通じ、サードパーティに起因するサイバーセキュリティリスクを管理するために必要な態勢を整備し、サードパーティリスク管理の方針を策定 3. サードパーティリスクを管理するための組織体制の整備、組織内規程の策定を実施 4. サードパーティのリスク評価を行い、そのリスクに応じた対応を実施 5. サードパーティを管理するための台帳等を整備、維持 6. 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において、サードパーティを含めた態勢を整備 7. サードパーティとの取引開始に当たっては、事前に定めた基準に基づき、デューデリジェンスを実施 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、サードパーティ等の契約や SLA（Service Level Agreement）等において、例えば、サードパーティとの役割分担・責任分界等の項目を明記 9. サードパーティ及びその製品・サービスによってもたらされるサイバーセキュリティリスク並びに契約の履行状況等について、リスクの重大性に応じて、継続的にモニタリング 10. サードパーティとの取引終了時の管理プロセスを整備

[5] International Monetary Fund, “Rising Cyber Threats Pose Serious Concerns for Financial Stability,” April 9, 2024.

[6] 「迫り来るサイバー攻撃の脅威 急迫のサイバー攻撃リスクに立ち向かう金融業界」『週刊金融財政事情』第 75 巻第 35 号、金融財政事情研究会、2024 年 9 月 3 日。

[7] 日本銀行金融機構局・金融庁総合政策局「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。

図表 4　サードパーティリスク管理に関する対応事項の概要（続き）

段階	内容
対応が望ましい事項	a. サードパーティリスク管理に係る統括部署に適切な知識等を有する人員の配置 b. サードパーティリスク管理において、重要な業務のサードパーティへの依存関係、サードパーティの集中リスク、地政学リスクの影響、フォースパーティ（サードパーティの再委託先等）の影響を考慮 c. 重要なサードパーティがそのサードパーティを管理する能力及びそのサプライチェーンリスク、集中リスク等について、定期的にモニタリング d. 重要なサードパーティの事業撤退や業務停止、契約関係の終了に備えて、適切コンティンジェンシープランと出口戦略を事前に策定し、定期的に代替手段のテスト等を実施 e. 経済安全保障推進法に基づき、特定社会基盤事業者が、特定重要設備の導入やその重要維持管理等の委託を行おうとする場合に提出する届出において記載することとされているリスク管理措置を講ずる

（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」2024 年 10 月 4 日、より野村資本市場研究所作成

Ⅲ 今後の論点

ガイドラインは、公表と同時に適用された[8]こともあり、対象金融機関等は 2 段階の対応事項や自身を取り巻く状況も踏まえて、サイバーセキュリティ管理態勢を改めて見直し、強化する必要がある。金融業界全体でサイバーセキュリティリスクを軽減し、業務の健全性及び適切性を確保していくための論点としては、（1）企業価値に影響を及ぼし得る経営課題としての意識の醸成、（2）連携と共助の強化、（3）投資家との対話も通じた態勢見直し・強化、が挙げられる。

1 点目として、ガイドラインにおいても経営陣の関与・理解に関する項目があったように、サイバーセキュリティは IT 課題ではなく、企業価値に影響を及ぼし得る経営課題であることを改めて意識し、経営陣のリーダーシップの下、管理態勢の強化にコミットしていくことが重要である。サイバー攻撃は、企業にとって、事故対応や賠償等を通じた財務面への影響のみならず、風評被害等を通じて非財務面にも影響を及ぼし得る[9]。その意味で、サイバーセキュリティリスクへの対応は、企業価値を維持・保全する上で不可欠なものであることは言うまでもない[10]。

2 点目として、業界全体のサイバーセキュリティリスクの軽減に向けて、連携と共助の強化がますます大切になると想定される[11]。ガイドラインについては、メガバンク関係者からは大手企業であれば既に取り組んでいる水準に近いといった声があった一方、地方銀行からは取り組むべき項目が多く、限られた経営資源の中で優先順位を付けることが難し

8 金融庁は、公表と同時に適用し、経過措置はないほか、対応期限を求めるという性質のものではないとの考えを示している（金融庁「コメントの概要及びコメントに対する金融庁の考え方」2024 年 10 月 4 日）。

9 サイバー攻撃による企業に発生し得る主な損害の種類としては、費用損害（事故対応損害）、賠償損害、利益損害、金銭損害、行政損害、無形損害が挙げられる（日本ネットワークセキュリティ協会「インシデント損害額調査レポート　第 2 版」2023 年 2 月 9 日）。

10 詳細は、江夏あかね「サイバーセキュリティと企業価値―投資家による評価と効果的な情報開示―」『野村サステナビリティクォータリー』第 5 巻第 2 号（2024 年春号）、を参照されたい。

11 ガイドラインにおいても、「金融庁は、共助機関及び金融機関等と連携して金融セクター全体の取り組みを推進」といった文言が示されている（前掲注 1 参照）。

いといった意見があったとも報じられている[12]。連携と共助の観点からは、例えば、ガイドラインで共助機関として取り上げられた、一般社団法人金融 ISAC（Information Sharing and Analysis Center）では、日本の金融機関の間でサイバーセキュリティに関する情報の共有・分析、及び安全性の向上のための協働活動を行っている[13]。業界団体関連では、全国銀行協会はサイバー攻撃対策を強化すべく、2024 年 2 月に好事例集を公表したほか、同年 3 月には会員行の経営層向け勉強会を開催した[14]。日本証券業協会では、会員におけるサイバーセキュリティ対策水準の向上支援としてサイバーインシデント情報の共有を始めとした各種取り組みを行っている[15]。

さらに、複数の金融機関等による共助の事例としては、横浜銀行、東日本銀行、京都銀行等が 2023 年 3 月に共同で設立した「CMS-CSIRT」という組織が挙げられる[16]。同組織では、定例会等の交流を通じて参加行のセキュリティ部門間の関係構築やセキュリティ強化に資する情報共有を行うとともに、セキュリティ担当者の能力向上に資する勉強会、セキュリティ対応訓練や演習、共同でのセキュリティ対策実現をめざした調査、検討等も実施するとしている。これらはあくまでも一例だが、連携・共助の強化は、業界全体の取り組みの促進の上でも重要になると考えられる。

3 点目について、金融庁による「投資家と企業の対話ガイドライン」（2021 年 6 月改訂版）[17]においてサイバーセキュリティ対応の必要性に関する言及があるように、近年は投資家が投資先企業のサイバーセキュリティの取り組みについてエンゲージメントを行う事例が見られるようになっている[18]。投資家からの客観的な意見も通じて、自身の管理態勢を見直し、強化を続けていくといったことも意義があると考えられる。

---

12 前掲注 6 参照。

13 金融 ISAC「活動概要」。

14 全国銀行協会「福留会長記者会見（三井住友銀行頭取）」2024 年 7 月 18 日、「全銀協、サイバー対策で好事例集　各行に自律的対策促す」『ニッキン』2024 年 3 月 19 日。

15 日本証券業協会では、会員におけるサイバーセキュリティ対策水準の向上支援として、「政府における経済安全保障に係る戦略的な方向性を踏まえ、必要な対応を行う。会員からのサイバーインシデント情報の共有及び政府からのサイバーセキュリティ対策に関する会員への情報提供及び政府の各種サイバーセキュリティ演習へ会員が参加する際の各種調整を行うほか、会員への研修の充実を図る」としている（日本証券業協会「当面の主要課題」2024 年 7 月 1 日）。

16 コンコルディア・フィナンシャルグループ「サイバーセキュリティの共助を推進する組織『CMS-CSIRT』の設立について―『地銀共同センター・MEJAR システム・ワーキンググループ』の取り組み【第 2 弾】―」2023 年 3 月 29 日。

17 金融庁「投資家と企業の対話ガイドライン」2021 年 6 月 11 日。

18 前掲注 10 参照。