「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（2024 年 6 月 28 日）

２０２４年７月１６日

弁護士　小坂　光矢

＜目次＞

令和 6 年（2024 年）6 月 28 日、金融庁は、「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（案）」を公表しました。金融セクター内外の状況変化等を踏まえて、金融機関等（※1）のサイバーセキュリティ管理態勢に関して、各監督指針や事務ガイドライン（以下「監督指針等」といいます。）とは別に詳細な対応策を示したものです。金融機関等においては、あわせて公表された監督指針等の改正案（※2）が成立した後は、監督指針等における「システムリスク管理態勢」の主な着眼点の 1 つである「サイバーセキュリティ管理」（例えば、主要行等向けの総合的な監督指針（令和 6 年 7 月）の III-3-7-1-2 の（5））との関係で、本ガイドラインを踏まえた必要な態勢の整備が求められます。

ガイドライン案では、金融機関等がサイバーセキュリティ管理態勢を整備する際の着眼点として以下の 7 つが挙げられています。

1. ガバナンス
2. 特定
3. 防御
4. 検知
5. 対応
6. 復旧
7. サードパーティリスク管理

その上で、各着眼点について、①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である「基本的な対応事項」と、②実践することが望ましい先進的な取組みである「対応が望ましい事項」が示されています。なお、「対応が望ましい事項」のみならず、「基本的な対応事項」についても、すべての金融機関等において一律の対応が求められているものではなく、各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、リスクに見合った低減措置を講ずるいわゆる「リスクベース・アプローチ」が求められます。
本稿では、着眼点毎に、ガイドライン案で示された対応事項について概観します。

（※1）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のほか、金融商品取引所をいいます。
（※2）監督指針等の改正に関する新旧対照表（別紙 1～16）（https://www.fsa.go.jp/news/r5/sonota/20240628-2/20240628.html）

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態勢の構築との関係では、主として経営陣や取締役会による積極的な取組みが求められるものとして、「基本方針、規程類の策定等」、「規程類等及び業務プロセスの整備」、「経営資源の確保、人材の育成」、「リスク管理部門による牽制」、「内部監査」の５項目について対応事項が示されています。主な対応事項は、下表のとおりです。

項目	基本的な対応事項	対応が望ましい事項
(1) 基本方針、規程類の策定等	✓ サイバーセキュリティ管理の基本方針を策定する ✓ サイバーセキュリティ管理態勢を整備し、少なくとも１年に１回レビューを行う ✓ サイバーセキュリティ担当部署及び各関係者の役割と責任及び権限を明確化する　等	✓ サイバーセキュリティに関する十分な知識を利用（外部専門家の利用を含む）できるようにしておく　等
(2) 規程類等及び業務プロセスの整備	✓ サイバーセキュリティに係る規程及び業務プロセスを整備し、少なくとも１年に１回見直しを行う ✓ サードパーティのリスクも含め、サイバーセキュリティリスクにかかる組織横断的な報告・連絡・協議ルートや指揮命令系統を整備する　等	―
(3) 経営資源の確保、人材の育成	✓ 適切な資源配分（サイバーセキュリティ担当部署等への専門性を有する人材の配置。必要な予算の配分等）や整合的な人材の育成・確保のための計画策定を行う　等	―
(4) リスク管理部門による牽制	✓ サイバーセキュリティ管理態勢の有効性について、業務部門から独立した立場で監視・牽制を行う　等	✓ サイバーセキュリティに係る適切な知識及び専門性等を有する職員を配置する

(5) 内部監査	✓ 独立した立場から、内部監査計画を策定し、サイバーセキュリティ（整備状況・運用状況、対応・復旧、法規制の遵守状況、サードパーティリスク管理を含む）をテーマとする内部監査を実施する　等	✓ サイバーセキュリティに係る適切な知識及び専門性等を有する職員を配置する

2. サイバーセキュリティリスクの特定

サイバーセキュリティリスクの特定は、「情報資産管理」、「リスク管理プロセス」、「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」及び「演習・訓練」の 5 項目から構成されています。

(1) 情報資産管理

情報資産管理との関係では、①情報資産をライフサイクル（取得・使用・保管・廃棄）に応じて管理する手続等を策定し、必要に応じて見直すこと、及び②情報資産は、その重要度（機密性、完全性、可用性）に応じて保護の優先度を分類し、管理することの 2 点が「基本的な対応事項」に挙げられています。また、他にも主要な対応事項として以下が挙げられています。

項目	基本的な対応事項	対応が望ましい事項
①情報システム及び外部システムサービス	✓ 情報システムと外部システムサービスを適切に管理するための台帳等を整備し、最新の状態を網羅的に把握できるようにする　等	―
②ハードウェア・ソフトウェア等	✓ ハードウェア及びソフトウェア等を適切に管理するための手続・台帳等を整備し、最新の状態を網羅的に把握できるようにする　等	✓ 管理対象外となっている個人所有端末等の情報資産や未承認のクラウドサービスの利用（シャドーIT 等）を特定し、管理対象とするか使用を中止するなど、適切に対応する　等
③情報（データ）	✓ 顧客情報や機密情報等を適切に管理するための台帳等を整備し、最新の状態を網羅的に把握できるようにする　等	―
④データフロー図・ネットワーク図	✓ データフロー図・ネットワーク図を作成し、最新の状態を把握できるようにする　等	―

(2) リスク管理プロセス

リスク管理プロセスは、「脅威情報及び脆弱性情報の収集・分析」「リスクの特定・評価」「リスク対応」「継続的な改善活動」の 4 項目から構成されています。主要な対応事項は下表のとおりです。

項目	基本的な対応事項	対応が望ましい事項
①脅威情報及び脆弱性情報の収集・分析	✓ 公的機関や情報共有機関等から、サイバー攻撃の脅威情報及び脆弱性情報を収集する ✓ 収集した情報を整理・分析し、サイバーセキュリティリスクの影響を評価する　等	✓ 過去に発生したことがないサイバー攻撃の脅威（ゼロデイなど）等を脅威分析の対象に含める　等
②リスクの特定・評価	✓ サイバーセキュリティリスクを少なくとも 1 年に 1 回評価する ✓ 境界防御型セキュリティが突破されるリスクや内部不正などの脅威も考慮する　等	✓ 重要な業務を特定し、重要な業務を継続するために必要な組織内の人員、設備、システム、サードパーティの相互依存度を考慮する　等

項目	基本的な対応事項	対応が望ましい事項
③リスク対応	✓ リスク評価の結果に基づき優先順位付けを行い、リスク対応計画（リスク回避、リスク軽減、リスク受容、リスク移転）を策定する　等	―
④継続的な改善活動	✓ リスク評価プロセスやリスク管理態勢の整備状況及び運用状況の有効性を少なくとも１年に１回は評価し、継続的な改善活動を実施する　等	✓ パフォーマンス指標（KPI）及びリスク指標（KRI）を測定・評価し、経営陣に報告する仕組みを整備する等

(3) ハードウェア・ソフトウェア等の脆弱性管理

ハードウェア・ソフトウェア等の脆弱性管理との関係では、管理に関する手続等を策定し、必要に応じて見直すことなどが求められています。その他の主要な対応事項は下表のとおりです。

基本的な対応事項	対応が望ましい事項
✓ 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等の対応期限を設定するとともに対応実績を管理する ✓ 深刻度の高い脆弱性について、重要なサードパーティが保有するシステム（共同利用型のシステムを含む）の脆弱性対応の管理を行う　等	✓ 深刻度の高い脆弱性について、クラウド事業者を含むサードパーティ（左記のサードパーティを除く）が保有するシステムの脆弱性対応の管理を行う　等

(4) 脆弱性診断及びペネトレーションテスト

定期的な脆弱性診断及びペネトレーションテストの実施が求められています。その他の主要な対応事項は下表のとおりです。

基本的な対応事項	対応が望ましい事項
✓ 関連する手続等を策定し、必要に応じて見直す等	✓ インターネットに直接接続していない VPN 網、内部環境も脆弱性診断とペネトレーションテストの対象とする ✓ 定期的に脅威ベースのペネトレーションテスト（TLPT）を実施する　等

(5) 演習・訓練

サイバーインシデント対応計画とコンティンジェンシープランの実効性を確認し、継続的に改善するために定期的に演習・訓練を実施することが求められています。その他の主要な対応事項は下表のとおりです。

基本的な対応事項	対応が望ましい事項
✓ 経営陣、サイバーセキュリティを統括管理する責任者（CISO 等）及び業務部門の責任者が自らサイバー演習・訓練等に関与し、その結果を把握する ✓ 演習・訓練のシナリオに、顧客に深刻な影響を与え、かつ現実に起こりうるシナリオを含める等	✓ 自組織への影響が大規模かつ長期間継続するインシデントや、取引所、清算・振替機関等への接続障害等が生じるインシデントなど、金融システム全体に深刻な 影響が波及するシナリオを用いた演習・訓練を実施する　等

3. サイバー攻撃の防御

サイバー攻撃の防御との関係では、不正侵入を防止するための境界ネットワーク対策、内部ネットワークでのシステム不正利用を防止するための対策、外部への情報漏洩対策といった多段階のサイバーセキュリティ対策を組み合わせた多層防御を講じることが基本的な対応事項とされています。また、これに加えて、「認証・アクセス管理」、「教育・研修」、「データ保護」及び「システムのセキュリティ対策」の４つの項目について対応事項が示されています。主要な対応事項は、以下のとおりです。

(1) 認証・アクセス管理

「基本的な対応事項」として、認証及びアクセス権の付与に係る方針及び規程等を策定し、定期的に見直すことが求められています。その他の主要な対応事項は下表のとおりです。

基本的な対応事項	対応が望ましい事項
✓ ID を認証し、システムへのアクセスを許可する前にユーザのアクセス権限の適切性を検証する。また、アクセスしたユーザを特定できる措置を講じ、処理内容をログに記録し、ユーザの操作内容と対応させる ✓ システムや情報の重要度に応じて、認証要件（多要素認証、リスクベース認証等、認証時におけるリスク低減策等）を決定する。特に、重要なシステムへのリモートアクセスには、多要素認証を使用する　等	―

(2) 教育・研修

「基本的な対応事項」として、経営陣を含むすべての役職員に対して、役割と責任に応じたサイバーセキュリティの意識向上に係る教育・研修を定期的に実施することが求められています。その他の主要な対応事項は下表のとおりです。

基本的な対応事項	対応が望ましい事項
✓ サードパーティ在籍の担当者が、業務を適切に行う上で必要となるサイバーセキュリティの教育・研修を受講（必要に応じて、金融機関に関するインシデント対応及び復旧計画における役割及び運用手順に係る内容を含む）していることを確保する　等	✓ フォレンジック調査や脆弱性診断等を内部の役職員で実施する場合、該当する役職員のスキルと知識を維持・向上させる　等

(3) データ保護

「基本的な対応事項」として、情報の重要度と、使用される技術環境における固有のリスクに応じて、データの管理方針を策定することが求められています。その他の主要な対応事項は下表のとおりです。

基本的な対応事項	対応が望ましい事項
✓ システム及び情報の重要度に応じたバックアップ要件、バックアップデータの隔離と保護、整合性の検証、復旧テストの実施等を含む、バックアップに関する規程等を整備し実装する ✓ 特に、ランサムウェア攻撃のリスクを考慮して、バックアップの期間や頻度を検討する　等	✓ DLP（Data Loss Prevention）等を導入し、役職員や外部関係者によるデータ漏えい（機密データの窃取や破壊を含む）を監視し、保護する等

(4) システムのセキュリティ対策

システムのセキュリティ対策は、「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」及び「クラウドサービス利用時の対策」の 5 項目から構成されています。主要な対応事項は下表のとおりです。

項目	基本的な対応事項	対応が望ましい事項
①ハードウェア・ソフトウェア管理	✓ システムの保守におけるサイバーセキュリティを確保するための手続を定める ✓ サポートの終了に伴うハードウェア・ソフトウェアの廃止・更改を計画的かつ安全に実施する　等	✓ サプライチェーンのリスク評価の中で、ハードウェアに関するサイバーセキュリティリスク（不正なファームウェア導入のリスク等）を評価対象とする　等

項目	基本的な対応事項	対応が望ましい事項
②ログ管理	✓ ログの取得・監視・保存のための手続を策定し、定期的にレビューする ✓ 情報システムのイベントログや運用担当者の作業ログの適切性を定期的又は必要に応じて都度確認する　等	―
③セキュリティ・バイ・デザイン	✓ 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」を実践する　等	✓ セキュリティ・バイ・デザインにかかる管理プロセスを、整備し、運用する。
④インフラストラクチャ（ネットワーク等）の技術的対策	✓ ネットワーク機器の設定（ファイアウォールルール、ポート、プロトコルなど）を定期的及びシステム環境の更新時に点検し、必要に応じて更新する。 ✓ 専用線や暗号技術の活用等を通じてネットワークのセキュリティを確保する　等	✓ DDoS/DoS 攻撃対策等によって、組織の通信及びネットワークサービスの耐性度を強化する　等
⑤クラウドサービス利用時の対策	✓ 利用するクラウドサービスの仕様を確認し、理解を深める ✓ 責任共有モデル（※3）を理解し、クラウド事業者との責任範囲等を明確にする ✓ 情報公開等の設定にミスがないか確認する ✓ 多岐にわたる関係主体等を把握し、情報共有体制・インシデント対応体制を構築する　等	―

（※3）利用者とクラウド事業者が、責任分界点を定めるだけではなく、運用責任を共有し合っているという考え方をいいます。

4. サイバー攻撃の検知

サイバー攻撃の検知との関係では、以下が基本的な対応事項に挙げられています。

✓ サイバー攻撃の端緒の検知のための監視・分析・報告に係る手続等を策定し、必要に応じて見直す・

✓ 監視の対象にクラウドサービスを含める

✓ サイバー攻撃の脅威に応じて、 必要な監視・分析などの対策を講ずる。対策を外部委託している場合には、委託先で実施している対策の具体的な内容を把握するとともに、対策の講じられていない領域が判明した場合は必要な措置をとる

また、「監視」に関して、以下の対応項目が挙げられています。

基本的な対応事項	対応が望ましい事項
✓ ハードウェア・ソフトウェア、ネットワーク、役職員によるシステムへのアクセス、外部のサービスプロバイダによるシステムへのアクセス（保守作業等）等について、継続的な監視を実施する	✓ おとりアカウントやサーバを用いて、攻撃の初期段階に検知するための仕組みを導入する　等

5. サイバーインシデント対応及び復旧

サイバーインシデント対応及び復旧は、「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」と「インシデントへの対応及び復旧」から構成されています。

(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

サイバー攻撃を想定した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（復旧計画まで含む）を、サイ

バー攻撃の種別ごとに策定することが「基本的な対応事項」として求められています。その他の主要な対応事項は下表のとおりです。

基本的な対応事項	対応が望ましい事項
✓ 対応の優先順位や目標復旧時間、目標復旧水準を定めておく	✓ データセンターやクラウド等を含めたサードパーティが提供するサービス等が長期間利用できないようなインシデントなどの、大規模な被害が生じるサイバーインシデントに対応するためのコンティンジェンシープランも整備する

(2) インシデントへの対応及び復旧

インシデントへの対応及び復旧は「初動対応（検知・受付、トリアージ）」、「分析」、「顧客対応、組織内外の連携、広報」、「封じ込め」、「根絶」及び「復旧」の 6 項目から構成されています。主要な対応事項は下表のとおりです。

項目	基本的な対応事項	対応が望ましい事項
①初動対応（検知・受付、トリアージ）	✓ 各種システムの監視やセキュリティ対応機関など外部組織からの連絡により、インシデントを検知する ✓ 収集した情報を基に、事実関係を確認のうえ、インシデント対応の要否を判断する ✓ 業務影響等に応じた優先順位付けを行い、あらかじめ定めた基準に従って、インシデント対応組織の管理者や経営陣等に報告する	―
②分析	✓ 対応が必要と判断したインシデントについて、攻撃の手口や原因・経路、システムへの影響、現在発生している業務影響及び今後発生しうる業務影響等を分析する ✓ インシデントの検知・受付から復旧までのフェーズに関し、記録（インシデントの内容、その対応において取られた行動内容や調査における収集ログの一覧等）を残しておく　等	―
③顧客対応、組織内外の連携、広報	✓ 顧客保護等の観点から公表が適切な場合は、被害、対応状況、復旧見込み等の判明している事実について、セキュリティ上のリスクを配慮した上で、適切かつ速やかに公表する ✓ 攻撃者の TTP（Tactics（戦術）、Techniques（技術）、Procedures（手順））等、他機関にとっても有効となる攻撃技術情報について、機密情報を除いた上で、必要に応じ、金融 ISAC や JPCERT/CC 等の情報共有機関に共有する　等	―
④封じ込め	✓ 被害拡大を防止するための対応（「封じ込め」。例えば、通信の遮断やシステム停止等）を行う	✓ 影響が生じる可能性のあるサードパーティに適切に通知を行う
⑤根絶	✓ サイバー攻撃により被害が発生した原因を除去する（マルウェアの駆除、パッチの適用等による脆弱性の修正等）	―

項目	基本的な対応事項	対応が望ましい事項
⑥復旧	✓ 復旧完了し業務再開を判断する際には、判断権限者を明確にしておくとともに、判断要素を整理しておく ✓ インシデントからの復旧後、当該インシデントの発生原因や被害の拡大に関する原因等を分析し、対応の評価を行い、当該評価を基に、インシデント対応計画やコンティンジェンシープランを含むサイバーセキュリティ管理態勢の見直しや改善を行う	―

6. サードパーティリスク管理

「基本的な対応事項」として、サードパーティリスク管理との関係では、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とサードパーティリスク管理方針を策定すること、またサードパーティを含む業務プロセス全体を対象とした管理態勢等を整備することが求められています。その他の主要な対応事項は下表のとおりです。

基本的な対応事項	対応が望ましい事項
✓ 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行う ✓ 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する ✓ サードパーティを管理するための台帳等を整備し、維持する ✓ サードパーティとの取引開始に当たって、例えば、以下の事項等について、デューデリジェンスを行う ・ サードパーティとの取引がもたらす潜在的なサイバーセキュリティリスクや脆弱性の評価 ・ 自組織がサードパーティに求めるサイバーセキュリティ（契約等で求める事項）の充足状況 ・ 過去のインシデントの発生状況 特に重要なサードパーティに対しては、サイバーセキュリティ管理態勢、サイバーインシデント対応計画、コンティンジェンシープランについても、評価を行う ✓ 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等を明確化して、サードパーティ等との契約や SLA（サービスレベルアグリーメント）等に明記する ✓ サードパーティの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する ✓ 取引終了時の管理プロセス（データ廃棄や組織内システムへのアクセス遮断措置等）を整備する	✓ 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、フォースパーティの影響を考慮する ✓ 重要なサードパーティがそのサードパーティ（2 以上のサードパーティ（自組織から見たフォースパーティ、フィフスパーティ及び N 番目のパーティ）を含む）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する ✓ 経済安保推進法に基づき、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（特定妨害行為の手段として使用されるおそれを低減させるためのもの）を講じる

サードパーティ等との契約や SLA（サービスレベルアグリーメント）等に明記することが考えられる項目の例としては、以下が挙げられています。

- ✓ サードパーティとの役割分担・責任分界
- ✓ 監査権限
- ✓ 再委託手続
- ✓ 実施すべきセキュリティ対策
- ✓ サードパーティの役職員が遵守すべきルール
- ✓ インシデント発生時の対応及び報告
- ✓ 脆弱性診断等の実施及び報告
- ✓ 深刻な脆弱性が判明した場合の対応及び報告
- ✓ サイバーセキュリティに係る演習・訓練の実施（共同演習・訓練への参加を含む）
- ✓ データの所在・保管・保持・移転・廃棄に関する取決め
- ✓ 契約終了の条件及び契約終了時の取決め
- ✓ 外部評価等の実施（第三者保証報告書の提出、第三者認証の取得を含む）

サードパーティリスク管理については、監督指針等においても、外部委託（二段階以上の委託に関するものを含む）に関する一般的な着眼点及びシステムリスク管理における外部委託管理の着眼点が示されています（例えば、主要行等向けの総合的な監督指針（令和 6 年 7 月）の III-3-3-4）。

7. 実務上の示唆

ガイドライン案が示す 7 つの着眼点のうち、「サードパーティリスク管理」を除いた 6 つの着眼点（「ガバナンス」「特定」「防御」「検知」「対応」「復旧」）は、2024 年 2 月 28 日に米国の国立標準技術研究所（National Institute of Standards and Technology。“NIST”）から公表されたサイバーセキュリティフレームワーク（「CSF」）の ver. 2.0 に沿っているものと推察されます。CSF は、すべての組織においてサイバーセキュリティのリスクをマネジメントし、低減できるようにすることを目指す文書と位置付けられていますので、同様の着眼点を採用している本ガイドライン案は、金融機関等以外の事業者においても大いに参考にする余地があるように思われます。

また、「サードパーティリスク管理」に関しても、委託先との取引を開始するに当たってのデューデリジェンス項目や委託契約等に明記することが考えられる項目の例が示されるなど、委託先に対するランサム攻撃に起因するサイバー攻撃被害が大きな問題となっている昨今の状況を踏まえ、自社の委託先管理を見直す際の参考とすることができるものと考えられます。

関連記事

・特集記事「業務委託先の情報セキュリティを確保するための実務上のポイント」

以 上