NEWSLETTER

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　概要と留意点

金融 & 危機管理 & 個人情報保護・データ保護規制ニューズレター　2024 年 12 月 6 日号

執筆者:
河合 優子
y.kawai@nishimura.com
北條 孝佳
ta.hojo@nishimura.com
水井 大
d.mizui@nishimura.com

1. ガイドラインの概要と対応方針

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「本 GL」といいます。）に係るパブリックコメントの結果を公表し（以下「パブコメ回答」といいます。）、同日から適用を開始しました[1]。

（1）　対象事業者

本 GL は、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、金融商品取引所を対象としており（本 GL 1.4。総称して「金融機関等」と定義されています。）、広範な範囲の金融関連事業者が適用を受けます[2]。

（2）　「基本的な対応事項」と「対応が望ましい事項」

本 GL は、従来の監督指針・事務ガイドラインとは別に、サイバーセキュリティに関して、データガバナンス等への言及も含む更に詳細な事項を定めるものです。対応事項は「基本的な対応事項」と「対応が望ましい事項」に分けられています。
このうち「基本的な対応事項」は、いわゆるサイバーハイジーンと呼ばれる事項（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）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を指します。「対応が望ましい事項」は、①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、②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

1　金融庁「「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」（2024 年 10 月 4 日公表、同年 10 月 11 日更新）20 番。

2　金融庁及び日本銀行によるサイバーセキュリティセルフアセスメント（「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 23 日））は、地域金融機関（地域銀行 99 先、信用金庫 254 先、信用組合 145 先）、保険会社（71 先）、証券会社（272 先）を対象に実施していました。本 GL の適用対象は、こうした金融機関に限られません。

等、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を指します（本 GL 1.1）。

「基本的な対応事項」と「対応が望ましい事項」のいずれについても一律の対応が求められるものではなく、それぞれの金融機関等が、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、つまり「リスクベース・アプローチ」を採用することが求められます。金融庁としても引き続き金融機関等の規模・特性に応じたリスクベース・アプローチでの検査とモニタリングを実施するとしています（本 GL 1.1）。さらに、金融庁において「チェックリスト形式で示すことは馴染まない」（パブコメ回答 5 番、18 番）とされ、いずれの項目をどの程度又はどのように実施すべきかは、各金融機関等において自ら検討し、講ずる対策の内容を見極める必要があるものと考えられます。

（3） 対応時期・対応方針

本 GL に記載されている各対応事項については、「対応期限を求めるという性質のものではございません。」と回答されています（パブコメ回答 20 番）。各金融機関等は、パブコメ回答で繰り返し述べられているとおり、「自らが直面するリスクを評価し、重要性・緊急性に応じて優先順位をつけた上、リソース制約を踏まえ、低減措置に取り組む」（パブコメ回答 15 番、18 番、23 番、25 番、28 番、33 番、36 番、37 番、38 番、40 番、42 番、54 番）必要があります[3]。仮に対応事項が講じられていない場合には、「一般論として、行政上の対応は、個別・具体的な状況に応じて検討すべきものと考えます。」とされています（パブコメ回答 11 番、12 番、13 番、32 番、33 番、35 番）。
変化し続けるサイバーセキュリティの脅威に対応する上では、組織的・技術的な対応態勢を継続的に見直す必要があるため、本 GL は、複数の「基本的な対応事項」において、必要に応じた見直しや年 1 回以上の定期的な見直しを求めています（本 GL 2.1.2、2.2.2.1 等）。各金融機関等は、リスクの評価や社内態勢、またサードパーティの範囲（後述）等について、定期的な見直しを行う仕組みを確立する必要があるといえます。
また、経営陣の主体的な関与・リーダーシップの下、リソースを適切に配分すると共に、サイバーセキュリティ担当部署や IT 担当部署に限らず、組織全体での態勢構築と運営を行うことを求めている（本 GL 1.2.1、1.2.2）ことにも留意が必要です。

2. 金融機関等の対応事項（サードパーティリスクの管理を中心に）

（1） 全体像

本 GL の対応事項は多岐にわたります。「2.サイバーセキュリティ管理態勢」に記載されている対応事項の大枠は、次の 6 つです。

---

[3] 例えば「確保できる要員が不足する場合、その限られたリソースの中で、どの対策を重点的・優先的に実施していくかなどもリスクベースであり、不足に対してどのように凌ぐか（対策の優先順位付けや、リスク受容を含む）も含め経営層の判断のもとで対応していくことが求められていると理解すればよいか。」との質問に対して「各金融機関のリソースの状況は様々であることから、充足の見込みについて一概にお答えすることは困難です。金融機関等においては、自らが直面するリスクを評価し、重要性・緊急性に応じて優先順位をつけた上、リソース制約を踏まえ、その低減措置に取り組む必要があります。」と回答されています（パブコメ回答 23 番）。

・　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リスクの特定
・　サイバー攻撃の防御
・　サイバー攻撃の検知
・　サイバーインシデント対応及び復旧
・　サードパーティリスク管理

（2）　サードパーティリスクの管理

本 GL は、金融機関等のサードパーティへの依存度の増大や、金融機関等のサプライチェーンの拡大・複雑化、サプライチェーン由来のサイバーインシデントにより金融機関等が多大な影響を受ける事例が発生していること等を踏まえ、サードパーティリスクの管理についても具体的に記載しています（本 GL 2.6）。サードパーティの範囲は広範なため、金融機関等との間で取引関係のある事業者に幅広く影響がありうることに留意が必要です。
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いい、例えばシステム子会社やベンダー等の外部委託先[4]のほか、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 連携先等が含まれます（本 GL 2.1.3 の脚注 18）。金融機関等は、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を整備することが求められており、本GLでは、サードパーティとの取引開始にあたってのデューディリジェンスの実施項目や、サードパーティ等との契約等において明記すべき項目についても言及がみられます（本 GL 2.6）。
外部委託先はあくまでサードパーティの一例に過ぎませんので、外部委託先に限らず数多くのサードパーティを対象として管理する必要がありえます[5]。

また、本 GL 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を、特に「重要なサードパーティ」と定義しており（本 GL 2.2.3 の脚注 26）、対応すべき事項が上乗せされる点にも留意が必要です。重要なサードパーティに関する固有の記述は本 GL の各所に見られますが、整理すると以下のとおりです。

【基本的な対応事項】
・　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）も脆弱性対応の範囲に含めること（本 GL 2.2.3.⑥）
・　重要なサードパーティも含めたセキュリティ・バイ・デザインの実践（本 GL 2.3.4.3①）及び自組織にシステムを提供する重要なサードパーティにおいてセキュリティ・バイ・デザインを実施できる体制となっているかの確認（同②）
・　重要なサードパーティに対するデューデリジェンスの実施にあたっては、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も含めて評価を行うこと（本 GL 2.6

[4]　外部委託先には、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）のベンダー等が該当します。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まれます（本 GL 2.1.3 の脚注 18）。

[5]　ただし、対象とするサードパーティについても、リスクベースで検討することとされています（本 GL 2.6、2.2.1.2 の脚注 24、2.3.2 の脚注 32 等）。

⑦）

【対応が望ましい事項】

- 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（サードパーティの再委託先など）、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の、定期的なモニタリング（本 GL 2.6.c）
- 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、適切な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すること（本 GL 2.6.d）

重要なサードパーティか否かは、業務内容等で一律に定まるものではないため、例えばクラウド事業者であるから直ちに重要なサードパーティに該当するわけではなく[6]、各金融機関等がリスクベースで検討する必要があります。また、自組織の業務内容等の変化に応じて、サードパーティや重要なサードパーティの範囲についても、継続的に見直す必要があると考えられます。

以　上

[6] 重要なサードパーティに「クラウド事業者が含まれるかどうかは、ケースバイケースと考えられます。」と回答されています（パブコメ回答 147 番）。

当事務所では、クライアントの皆様のビジネスニーズに即応すべく、弁護士等が各分野で時宜にかなったトピックを解説したニューズレターを執筆し、随時発行しております。N&A ニューズレター購読をご希望の方は N&A ニューズレター　配信申込・変更フォームよりお手続きをお願いいたします。
また、バックナンバーはこちらに掲載しておりますので、あわせてご覧ください。

本ニューズレターはリーガルアドバイスを目的とするものではなく、個別の案件については当該案件の個別の状況に応じ、日本法または現地法弁護士の適切なアドバイスを求めていただく必要があります。また、本稿に記載の見解は執筆担当者の個人的見解であり、当事務所または当事務所のクライアントの見解ではありません。

西村あさひ 広報課 newsletter@nishimura.com