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

金融庁が公表したサイバーガイドライン案では、管理基準の引き上げと、広範な管理の双方が求められている。経営の立場からは、事業経営に直結するサイバーリスクの可視化を図り、各部門の管理業務と連動させることで、全社的な管理態勢を実現していくことが期待される。

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）」（以下、ガイドライン案）を公表した。サイバーセキュリティに関する事項は2015年に監督指針等[1]に追加され、以降は金融分野全体の強化が促進されてきた。昨今の状況変化のもと、本ガイドライン案は、監督指針等から参照される形で、詳細かつ広範な事項について定められたものとなっている。この重厚なガイドライン案の主な留意点と注目点について触れたい。

従来の常識を超える対応基準の引き上げ

昨今の国内外のサイバー攻撃事案に見られるように、日々サイバーセキュリティリスクは増大し、過去の対応基準では必ずしも十分とはいえない状況になっている。

例えば、サイバーセキュリティ対策はインターネットに接続するシステムのみが対象、といった考えはもはや通用しない。ガイドライン案では、基本的な対応事項として「内部ネットワークセグメントに設置したシステムのリスクも評価対象」と言及され[2]、「脆弱性診断及びペネトレーションテストは、インターネットに直接接続していないVPN網、内部環境も対象とすること」が望ましいとされている[3]。また、定型的なテストをしていれば十分というわけでもない。「脅威ベースのペネトレーションテスト（TLPT）」などの実践的なテストが望ましいとされ、実施上の観点への言及もある。主要なサービスを担うシステムでは、インターネット接続の有無によらず、診断やテストを行うことが一般的となっていくだろう。

サイバーセキュリティ対策は開発後や導入後のシステムに対して実施するもの、といった発想も変えていく必要がある。ガイドライン案では、セキュリティ対策をシステムの企画や設計等の初期段階から考慮する「セキュリティ・バイ・デザイン」が基本的な対応事項に追加され、開発プロセスへのサイバー対策の組み込みが求められている[4]。

他にも、ランサムウェア対策や脆弱性パッチ対応強化[5]への言及、経済安全保障推進法に準拠した対応[6]が望ましいとされるなど、注目すべき事項を多く含んでいる。

サードパーティリスク管理は既存の枠組みの見直しから

また、関連企業や取引先・委託先企業などを介したサプライチェーン攻撃が発生している状況を受け、サード

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（案）」の主なポイント（抜粋）

主なポイント	主な対応事項（抜粋）	
	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）	• KPI・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	• 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への言及（監査権、診断・外部評価の実施等）	• 重要な4th party等の定期的なモニタリング、代替手段のテスト • 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

（出所）「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）」（金融庁 2024年6月28日）を基に野村総合研究所作成

NOTE

1) 各監督指針及び事務ガイドラインのこと。
2) ガイドライン案では、個々の対応事項は【基本的な対応事項】または【対応が望ましい事項】のいずれかに分類されている。
【基本的な対応事項】は、「サイバーハイジーンと呼ばれる事項、その他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」を指す。
【対応が望ましい事項】は、「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り組みや、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り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」を指す。
3) リスクの高い構成である場合は、内部環境のセキュリティ上の根幹となる機器（Active Directoryサーバやファイルサーバ等）への脆弱性診断が、【基本的な対応事項】として言及されている。
4) 関連する概念として、システム開発の早い段階でセキュリティテストを行う「Shift Left」がある。Shift Leftについては、『金融ITフォーカス特別号 金融機関のリスク・レジリエンスの潮流　第2章 金融機関におけるシステム開発の実態とこれからの開発スタイル』（野村総合研究所 2023年9月）参照。
5) 【基本的な対応事項】として、「例外的にパッチ適用等の対応を実施しない場合は、実施しないことのリスクについて経営陣から承認を得ること」とあり、深刻な脆弱性に限って適用するといった考えから、今後は「適用することを前提に検討」することへの転換が期待される。
6) 経済安全保障推進法の概要については、『金融ITフォーカス特別号 金融機関のリスク・レジリエンスの潮流 第1章 経済安全保障推進法：金融分野における「第2の柱」対応概説』（野村総合研究所 2023年9月）参照。

パーティリスク管理に関する内容が新設された。ここでは、サードパーティリスクに対する全般的な管理プロセスの整備が求められているが、サードパーティリスク管理に特化した新たな枠組みを検討する前に、まずは既存の管理枠組みに基づく整備を進める必要がある。新たな枠組みの安易な導入は、既存枠組みとの多重管理を誘発しかねない。

サードパーティには、次に示すような、様々な対象が含まれている。

- 外部委託先、業務提携先、API連携先
- サービス提供事業者（クラウド、ASP等）
- ハードウェアメーカー、ソフトウェアベンダー、等

例えば、外部委託先については、既に金融機関の中に専門的な管理部門があり、監督指針等に基づく伝統的な管理枠組みを有している。まずは、こうした枠組みをベースにガイドライン案の対応事項を組込むことで、サイバー観点を含めた効率的な管理を図ることが考えられる。

また、サービス提供事業者についても、既にクラウド管理やASP管理などの枠組みを有しているところもある。仮にない場合でも、自社システムを対象としたシステムリスク管理に組み込むことによってガイドライン案に基づくアップデートをすることも可能であろう。

経営が最大リスクを「可視化」できる工夫を

問題は、経営として「注視すべきリスクは何か？」を見定めることにある。ガイドライン案では、経営へのサイバーセキュリティリスクに関する報告（年次以上）が求められているが、個別各論から全社的なリスクを的確に把握することは難しい。また、個別の管理において、サイバー分野の専門知見の特殊性から、許容水準が分からないまま「リスト」ベースの管理に拘泥し、コンプライアンス疲れを助長してしまうおそれもあるだろう。

経営がサイバーセキュリティリスクを理解するためのヒントは、事業経営に直結する「最大リスクの可視化」にあるのではないだろうか。例えば、内外の事例にみられるような、経営自身が「危ない」と感じるサイバーシナリオを自社に置きかえて書き下す。これらの最大リスク（KPI、KRI等）を評価することで、実感を伴ってリスクを認識できるようにする。更に、こうしたサイバーシナリオを基礎として各部門での管理水準や体系を整備し、関連する情報がエスカレーションされるようにする。このような態勢の整備を通じて、経営として全社的な管理を実現していくことが求められるのではないか。

金融機関の伝統的なリスク管理は、「経営」「管理」「個別対応」の3つの階層が有機的に連携する形で整備されてきた。サイバーセキュリティ管理では、その専門性から「個別対応」のウェイトが高く、「管理」態勢をどのように整備し「経営」につなげていけるかがポイントになるだろう。

現状では、金融機関の経営から現場まで精通し、かつサイバーセキュリティの専門性とともに態勢整備が行える人材は、決して多くはない。サイバー対応態勢の高度化に向けた人材の育成と確保は、避けては通れない課題となっている。

Writer's Profile

上杉 信孝 Nobutaka Uesugi
金融デジタルビジネス推進部
エキスパートリサーチャー
専門は金融分野のリスク管理
focus@nri.co.jp