はじめに

金融機関が利用する情報システムで昨今、大規模な障害が相次いでいる。原因は様々だが、金融庁は、金融機関で発生したシステム障害を「障害発生等報告書」として提出を受ける都度、金融機関に対し、障害の発生理由やその復旧状況を確認するとともに、当該障害の真の原因や事後改善策の報告を受けている。

こうしたシステム障害に関する報告を踏まえ、金融庁では2019年以降、近年のITやデジタライゼーションの進展に伴う特徴的な事案などを中心に、分析結果や事例を「金融機関のシステム障害に関する分析レポート」として公表しはじめた。金融機関ではフィンテック企業をはじめ新たに金融サービスに進出してきた事業者との連携を強化する一方、システムコスト削減を念頭に、システムそのものの合理化施策を進展させている。

折しもこの間、多数のATMがシステム障害により利用不可となるなど全国的に大きく報道されるような大規模障害も確認されており、多数の顧客に影響を及ぼす事案も発生した。さらに、システム障害発生時に、バックアップ機器への切替えができない、もしくはバックアップ機器自体にも同時に障害が生じるなどして実質的に機能しない例が確認されてもいる。したがって、単に機器の多重化がなされていれば良し、といった従来のような外形的な評価や判断が容認されない状況にも至った。さらに、こうしたケースでは、初動態勢そのものの瑕疵も併せて露呈することがある。

システム障害のモニタリングに相応の人員を割いたとしても、障害時に実務を担うのは、システム部門のみではない。顧客対応を担う営業部門や、店頭での顧客誘導などを中心に、複数の部門が速やかに緊急時行動を実践する必要があるためだ。つまり、障害時における復旧

方針や具体的な対応手順を規程類やマニュアルとして整備するとともに、対応組織ごとに役割分担を明確に定義していない実態が顕在化したことで、金融庁は同レポートの中で、「復旧に想定以上の時間を要する事案が複数見られた」と断じてもいる。

金融庁では、過去に確認された障害事例を通じ、現状を過信することなく、「経営陣の積極的な関与の下、障害発生時を想定した顧客目線での対応態勢を整備することが課題」としており、昨今は、ボトムアップでの対応ではなく、経営陣自らが指揮を執り、緊急時を想定した対応態勢の整備を構築するよう促している。むろん、障害を発生させないことが大前提であり、重要な機器の多重化は当然として、あらかじめ障害発生パターンを可視化したうえで、実効性の確保や、具体的な復旧手順を子細に定義のうえ、訓練等によるシステムリスク管理態勢を高度化するよう要請している。さらに、こうした活動を継続するうえでPDCAサイクルの実務への実装が欠かせない、としている。

このように、単に障害を未然に防ぐといった目的のみならず、障害発生時の業務の早期復旧を通じ、顧客に与える影響の軽減を実現することが重視されるなか、金融機関として実効性のあるシステムリスク管理態勢の整備に組織的に取り組むことが問われている。この一環として位置づけられているのがシステム監査なのだ。

いわゆるシステム監査人によるシステム監査では、「開発工程」「テスト工程」「運用工程」といったプロセス単位でのモニタリングのほか、「システムリスク」「外部委託先」「コンティンジェンシープラン」などを対象にターゲットモニタリングを実施することが一般的とされる。ターゲットモニタリングのうち、「システムリスク」はさらに「情報セキュリティ」「サイバーセキュリティ」「システム障害管理」といった要素に分解することができる。

一口に金融機関のシステム監査といっても、金融機関では本来、内外の組織による複数の切り口での実務対応をこなし、相互に監査結果を補完し合うことで合理的な評価を導出することが期待されている。だが実際のところ、これまで一般に金融機関が理解してきた「システム監査」とは、次のようなものではないだろうか。

「専門性と客観性を備えたシステム監査人が、一定の基準に基づいて情報システムを総合的に点検・評価・検証をして、監査報告の利用者に情報システムのガバナンス、マネジメント、コントロールの適切性等に対する保証を与える、又は改善のための助言を行う監査の一類型」

これは、経済産業省が2018年に公表した「システム監査基準」における「システム監査の意義」とされるものから抜粋したものだ。さらに、同基準では、システム監査の目的を次のように定義する。

「情報システムにまつわるリスクに適切に対処しているかどうかを、独立かつ専門的な立場のシステム監査人が点検・評価・検証することを通じて、組織体の経営活動と業務活動の効果的かつ効率的な遂行、さらにはそれらの変革を支援し、組織体の目標達成に寄与すること、又は利害関係者に対する説明責任を果たすことを目的とする」

ここで注目すべきは、同基準はシステム監査を、「システム監査人」が実施し、監査報告の利用者に一定の「保証」を与えることを目的に実施される監査を指すうえでの「監査の一類型」と定義していることである。つまり、監査には、外部監査、内部監査と異なる目的で実施される複数の類型が存在するものの、いわゆる「金融機関のシステム

監査」という語感から金融機関は、システム監査を高度人材が専門的に担う「システム監査人による監査行為」を指すものとして一意に特定してしまっている可能性が否定できないということだ。

金融機関では、外部監査、監査役、内部監査といったように、複数の組織が同一のテーマで実務をこなしており、相互での情報連携は欠かせないものの、本来は監査の目的も着目すべき視点も異なる。にもかかわらず、ことシステム監査に至っては、監査役や内部監査が実施するはずのシステム監査は、専門家のシステム監査人が実施するシステム監査の見解や結果を追認するような行為にとどまっているように見えてならないのだ。

この背景には、IT人材そのものやサイバーセキュリティをはじめ高度化する技術要件に精通した人材の内部監査部門としての確保、配置に困難を抱える事情が垣間見える。

本来、内部監査部門が果たすべきシステム監査の要諦の１つに、専門性の高いシステム監査人による監査を念頭に、金融機関のシステムが金融当局や業界団体が定義する要件に沿って企画、開発され、安定した運用がなされているかの評価がある。つまり、内部監査部門は、過度にITの専門性を高めることばかりを期待されているのではなく、専門性の高いIT人材を抱えるシステム部門やITベンダー、メーカーに対する牽制機能の発現に重心を置くことも求められているのだ。

金融機関のシステムは、金融当局が示すレギュレーションに沿って定義された業務要件を踏まえ、システム部門がこれを企画し、開発される形態を採っている。そこで内部監査部門では、金融当局が発出する政省令やガイドライン、業界団体からの通達、申し合わせ事項などを精査のうえ、金融機関に課せられる要件を整理し、当該要件に沿った評価作業を行うことが有効な一手となるだろう。つまり、内部監査

部門におけるシステム監査では、当局が検査を通じて確認しようとする視点を踏襲すればよいのだ。

本書では、実際に金融機関の監査役（監事）として監査機能を担う立場にある筆者が、自身が被監査部門に問いかけているポイントを念頭に、金融当局が発信する種々の情報を網羅的に整理し、金融機関で内部監査機能を担う方々の参考に資することを祈念して執筆したものである。

本書発行の時期には、新たに内部監査部門に配置され、監査のイロハから学ぼうとされる金融機関の行職員諸氏も数多おられることだろう。そのため本書では、必ずしも情報システムそのものや監査業務に精通しない方にも参考に資していただけるよう、必要以上の深度で情報システムや監査プロセス、監査規則の技術的な解説に偏らぬよう配慮した。

本書が、こうした方々の、今後の効果的な監査業務の１つの拠り所として位置づけられたら望外である。

末筆ながら、本書発行に際しては、経済法令研究会の松倉由香氏に構想段階から章構成に至るまで子細な指導とご協力を拝受した。この場をお借りして心から御礼申し上げたい。

2024年３月吉日

大野博堂

第1章 金融機関の内部監査とシステム監査

第2章 金融機関のITガバナンスとITマネジメント

第5章 テーマ別システム監査の論点

第1章

金融機関の内部監査とシステム監査

第１節

金融機関の内部監査高度化への期待

いま、金融機関のシステム障害は、利用者のみならず社会、経済全体に大きな影響を及ぼし、自組織にとって信用を大きく毀損する要因になることは自明。健全なシステムを持続するためには内部監査の実効性を最大限に高めることが期待されている。まずは、その核心について金融庁発出の２つの資料から整理する。

2019年６月、金融庁は「金融機関の内部監査の高度化に向けた現状と課題」と題した文書（以下、「現状と課題」という）を公表した。公表の前提として金融庁は、「当局のモニタリングにおいても、本文書の個々の論点を形式的に適用したり、チェックリストとして用いたりすることはしない」としている。ただし、「現状と課題」記載の観点が業界団体から金融機関に対して示されたことに加え、「現状と課題」に基づくモニタリングが当局により実施されてきたのが実態だ。

そのうえで2023年10月には、「現状と課題」公表後における金融機関向けの内部監査の高度化に向けたモニタリングにより得られた示唆が、「『金融機関の内部監査の高度化』に向けたプログレスレポート（中間報告）」（以下、「中間報告」という）として金融庁から公表された。

「中間報告」は、大手銀行グループにおける内部監査の取組状況及び課題認識を整理したものとされてはいるものの、「現状と課題」を補完する位置づけとして、地域金融機関の内部監査の高度化にも資する情報である。

そこで本節では、2019年公表の内部監査における「現状と課題」及

び2023年公表の「中間報告」記載の要件を解説することで、金融庁が金融機関の内部監査高度化に向けて期待するポイントを探っていく。

1「金融機関の内部監査の高度化に向けた現状と課題」の要諦

⑴　公表当時の金融庁の問題意識の理解

「現状と課題」公表当時（2019年）、金融庁は当時の現状について、世界的な低金利環境が継続しており、金融を取り巻く環境そのものが激変しつつあると認識を示したうえで、フィンテックの進展のなかで金融機関業務が複雑化・高度化するところ、次の課題があるとした。

▶持続可能なビジネスモデルを構築することにより、業務の適切性や財務の健全性を確保し、金融システムの安定に寄与していくためには、ガバナンスが有効に機能していることが重要

▶内部監査部門が、リスクベースかつフォワードルッキングな観点から、組織活動の有効性等についての客観的・独立的な保証（アシュアランス）、助言（アドバイス）、見識を提供することにより、組織体の価値を高め、保全するという内部監査の使命を適切に果たすことが必要

こうした課題感は、内部監査部門が実務をこなすうえで最低限理解すべきものであり、内部監査規程の冒頭で述べるべき基礎的概念ともなる。

なお、「内部監査の使命」について、内部監査人協会（The Institute of Internal Auditors：IIA）は、次のように求めている。

著者

大野 博堂　Ohno Hakudo

株式会社NTTデータ経営研究所
金融政策コンサルティングユニット
ユニット長／パートナー

1993年早稲田大学卒業後、NTTデータ通信（現NTTデータ）入社。金融派生商品のプライシングシステムの企画などに従事。大蔵省大臣官房調査企画課、総合政策課にてマクロ経済分析を担当した後、2006年からNTTデータ経営研究所。中央省庁、自治体、金融機関向けの調査・分析・コンサルティング活動に従事。著書に『金融機関のためのサイバーセキュリティとBCPの実務』『AIが変える2025年の銀行業務』他多数。金融業界団体主催の各種セミナー等にて講演多数。飯能信用金庫非常勤監事、総務省地方公共団体財務・経営アドバイザー、東工大キャリアアップMOT「サイバーセキュリティ経営戦略コース」講師。

金融システム監査の要点

2024年５月15日　　初版第１刷発行

著　　者　大　野　博　堂
発 行 者　志　茂　満　仁
発 行 所　㈱経済法令研究会

〒162-8421　東京都新宿区市谷本村町３-21
電話　代表 03(3267)4811　制作 03(3267)4823
https://www.khk.co.jp/

営業所／東京03(3267)4812　大阪06(6261)2911　名古屋052(332)3511　福岡092(411)0805

カバー・表紙デザイン／土屋みづほ　本文デザイン・DTP／㈱アド・ティーエフ
制作／松倉由香　印刷／あづま堂印刷㈱　製本／㈱ブックアート

ISBN978-4-7668-3510-6

☆　**本書の内容等に関する追加情報および訂正等について**　☆
本書の内容等につき発行後に追加情報のお知らせおよび誤記の訂正等の必要が生じた場合には、当社ホームページに掲載いたします。
（ホームページ　書籍・DVD・定期刊行誌　メニュー下部の　追補・正誤表　）