デジタル監査の最新動向のポイント
～ドイツからの知見～

Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft（ドイツ）
Associate Partner
後藤　英夫

2022年３月１日付けでドイツ・デュッセルドルフに現地日系企業の経営課題対応支援コンサルタントとして赴任し、現在対応中の立場から、７つの事例とその内部監査的な観点からのポイントをご紹介する。

１．プロセスマイニング

標準SAP（ERP（統合基幹業務）システム＝企業内の各部門で独自に管理されている経営資源を一元化するために開発されたシステムのひとつ）のグローバル導入が完了したメーカーA社では、当該システムインフラを活用した経営価値創出が課題であった。デジタルツールと標準システムインフラの相性はよい。理由は、標準システムインフラ上で構築するデジタルツールは、世界のどの拠点でも利用可能になるからだ。つまりデジタルツール導入コストを、全拠点で「割り勘」することができる。

A社の内部監査部門では、現在プロセスマイニングという取引ログのタイムスタンプを使った取引手順の異常とリードタイム異常の両方のデジタル的点検手法を実践している。ポイントは２つである。まず第１にこの点検は従来の監査の基本手法であるサンプリングではなく全件点検になっているということ（図１）。次にこの点検はリモート点検として東京から全世界を対象に行われているということ。なお、筆者チームによるコンサルティングもドイツ⇒東京で、基本的にリモートで行われている。プロセスマイニングはドイツ発のデジタルツールによる方法であることから、先行事例とノウハウの多くはドイツに存在する。したがってリモートでドイツ⇒東京の技術移転が行われているのである。現時間断面、このツール活用においてドイツの先進企業は日本企業の７～８年先を行っている。

図１　プロセスマイニングのインパクト

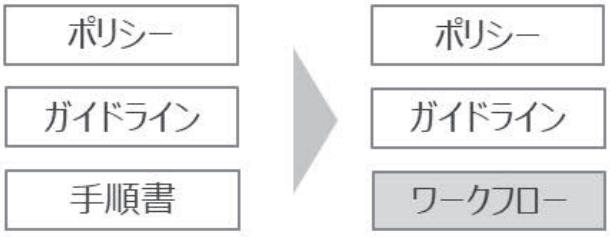
２．ワークフロー

ドイツにあるメーカーB社に昨年秋に赴任した欧州社長は驚愕していた。この会社ではほとんどの決済案件が事実上社長承認にのみ依存して回っていたのだ。マネジャーによる内部統制が事実上全く存在していなかった。全責任が社長に負わされる状況はきわめて不健全であると考えた同社長は、スピードを伴った改善を筆者チームに依頼してきた。販社現地法人であるこの会社の規模は欧州統括会社のみだと100人以下だ。こういった小さな拠点における内部統制の構築と運用の難易度は一般に日本本社より高い。一方使える予算は本社より桁違いに小さい。したがってこの会社の「惨状」は日系企業の海外現法としてはある意味普通だ。業務プロセス管理の水準は日本本社のそれに20年は遅れている。外部監査も内部監査もこれまで明示的にそういった実態を指摘してこなかったこともその原因の一端だといえるかもしれない。

この状況を改善するために筆者チームはワークフローツールの導入を推奨し現在実装対応中である。ワークフローツールとは、RPA：Robotic Process Automationがデータベース機能と関与する人々とのインターフェース（入力、承認など）を備え進化してきたものである。このツールはSAP等基幹システムの機能と会社のあるべき業務プロセスのギャップを埋めるために使うことができる。内部監査的には、ポリ

シー・ガイドライン・手順書の３層からなる規程体系を現場に実装整備するための最新ツールだととらえるとよいだろう。従来の手順書はワークフローツール上でデジタル的に実装される（図２）。このツールの導入により、現場管理者による管理も内部監査によるリモート監査もデジタル的に実行することができるようになる。内部統制的には整備と運用が一体化するという点も見逃せないだろう。

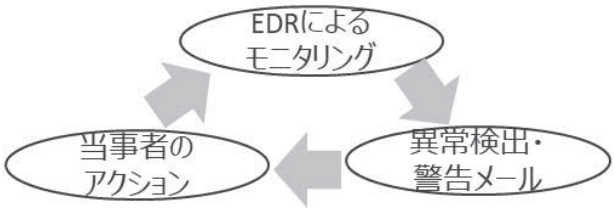
図２　ワークフローの位置づけ



３．サイバーセキュリティ

メーカーC社ではサイバーアタックによる情報漏洩が発覚した。実に２年以上にわたり機密情報を盗まれ続けていたのだ。この会社にはファイアウォール（アナログの世界の守衛所・門番機能に相当）もEDR：Endpoint Detection and Response（アナログの世界の監視カメラに相当）も導入済みであった。そして、EDRは異常状態についての警告メールを発信もしていた。にもかかわらず、情報漏洩の発覚が遅れた原因は、警告メールを当事者として受け取り、危機を認識したうえで必要なアクションをとる人間が割り付いていなかったからだ。サイバーセキュリティのためには、必要なモニタリングシステム導入に加えて、そのシステムが検知・発信する警告メールを受け取り、対応する当事者（意識）の割り付けが必須だということだ（図３）。メーカーC社の場合、乗っ取られたユーザーIDは当事者（意識）の割り付けがなされていないテンポラリーユーザーだった。サイバーセキュリティの内部監査においては、必要なシステムの充足に加えて、システムが発する警告メールへの当事者（意識）割り付け充足の点検が求められている。

図３　サイバーセキュリティ管理サイクル例



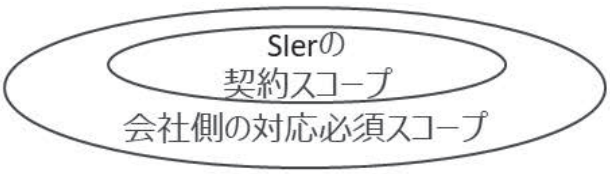
４．ITプロジェクト

メーカーの金融子会社D社の内部監査部門のグローバル責任者は、欧州統括会社社長から異動された方だった。内部監査部門の経験がなかった彼は、内部監査の仕事を経営管理者の視点でゼロベースで見直す能力をもっていた。その結果、彼が気づいた内部監査業務スコープの抜け漏れのひとつが、ITプロジェクトだった。内部監査部門は通常のルーティン業務は監査対象にしていたが、プロジェクトものは対象外だった。ITプロジェクトのいくつかは数百万USドル以上の規模だったが、監査対象の外におかれていた。この内部監査責任者は加えて驚くべきことに気づいた。彼が点検した一定規模以上のITプロジェクトのほとんどすべてが予算超過・納期遅延の失敗プロジェクトだったということだ。「この状況をなんとかしたい」それが筆者チームへの彼からの相談事項だった。これも日本からドイツの筆者へのリモートでの相談。アフターコロナの時代、クライアントと経営課題対応コンサルタントの関係性はときに時空を超えて維持されるようになった。

SIer：System Integratorとの成果物契約（請負契約）を用いることが一般的であるITプロジェクトの場合、プロジェクトの予算超過・納期遅延の原因の多くは実はきわめて単純である。会社のプロジェクトリーダーが、プロジェクト予算の稟議をあげるときに、会社側の対応コストがごっそり抜け漏れてしまうのである（図４）。プロジェクトリーダーはSIerに払うコストの予算を確保するつもりが、いつの間にかその予算はプロジェクト全体予算としてのレッテルを貼られてしまう。結果として、予算化から漏れた会社側の対応工数不足を、追加予算投入で外部調達せざるを得なくなり、プロジェクトは必然的に予算超過・納期遅延に陥る。これを内部監査的に未然に防止するためには、プロジェクト稟議書への事前の内部監査が必要だ。抜け漏れている会社側タスクと工数を指摘することになる。ただ短期的問題は、内部監査部門にその監査スキ

ルがあるとは限らないということだろう。したがって、もしITプロジェクト監査を有意義・実効的に行おうとする場合、内部監査の年度予算で外部専門家の支援分の確保が必要になる。巨大プロジェクトの予算超過・納期遅延の予防で得られる企業経営上のメリットは小さくないはずだ。過少予算で意図せずしかし必然的に「ババを引かされてしまう」プロジェクトリーダーの、エリートとしてのキャリアを守ってあげるという意味でも、この面での内部監査業務の拡張は喜ばれるはずだ。

図４　ITプロジェクトの構造



５．滞留債権

自動車部品メーカーE社では、毎年数百万ユーロ規模の滞留債権のライトオフ（貸し倒れ償却）が発生していた。滞留債権の回収は経理部の仕事ということになっていたが、経理部の担当者には滞留債権の原因特定に必要な情報も、原因特定や対応のための工数と権限も与えられていなかった。

この会社が長年このような滞留債権発生を結果的に放置してきた背景には、同社の欧州での業績の好調があった。高性能の部品供給者としてドイツおよび欧州の自動車メーカーからの引き合いが途切れることはなかったのである。したがって、目先の受注への対応が優先され、滞留債権問題への対応は先延ばしされてきた。会計監査・内部監査でも滞留債権が問題視されることはなかった。理由はこの会社の滞留債権ライトオフは、実は引当金を積んだうえでのPlanned write offだったからだ。筆者チームは、現在この問題解消のための支援プロジェクトに関与している。対応のための武器は、プロセスマイニングとワークフローツールだ。販売業務プロセスの現状を網羅的に可視化し、滞留債権発生の根本原因を具体的に特定し、対応策を立案し、それをワークフローツール上に実装する。

滞留債権問題に直面していたのは、E社だけではなかった。電子部品メーカーのF社も北米子会社で10年超にわたって数千万USドル規模の滞留債権を累積していた。この「惨状」の原因のひとつは、当該北米子会社は外部監査・内部監査ともに対象外だったからだ。売上的な意味での金額的重要性基準ではこの子会社には重要性はなかった。金額的重要性基準には本来、PL的基準だけでなく、累積滞留債権金額といったBS的基準が設定されるべきということだろう（図５）。なお、興味深い後日談がある。東京本社から滞留債権回収を指示された当該北米子会社は、管理欠如ゆえ証跡を示せない状況下、それでも取引先に「払ってくれ」の交渉を断行した。その結果、７割超の滞留債権が現実に回収されたのである。取引先の方も長期滞留債務の解消が経営課題になっていたのかもしれない。彼らはきちんと管理していたということだ。彼らからすればただ単に「請求書が届いていないから」ということだったということだろう。プロテスタントの国らしいエピソードだ。あきらめる必要はない。

図５　あるべき重要性基準

６．CSRD

自動車部品メーカーG社のCSRD：Corporate Sustainability Reporting Directive 対応は当初日本本社のIR部門が対応しようとした。しかしほどなくしてそのボールは、同社の欧州統括会社にパスされてきた。理由は２つだった。まず日本本社より欧州法人の対応納期の方が早いからということ。次に日本本社および日本国内にはCSRDの対応知見・ノウハウがないということ。その結果本社予算を使った欧州統括会社でのCSRD対応プロジェクトが立ち上がった。

欧州統括会社のプロジェクトリーダーは、CSRD対応も試作品⇒量産化アプローチで行きたいとの意向を筆者チームに示した。自動車部品メーカーらしい発想だ。さらに彼は「自分たちのメンバーはただでさえ工数不足に直面しているので、CSRD対応の予算を本社からもらえたとしても、重点部分に対応スコープを絞り込んだ対応しかできない」との立場を選択した。結果として同社は、世の中で一般的な網羅的なギャップ分析から始まるウォーターフォール的アプローチではなく、早いタイミングで重要機能にフォーカスした仕組みの試作品を作るプロトタイプアプローチでのプロ

ジェクト遂行を選択した（図６）。なお、CSRDが要請する非財務情報開示は外部監査および内部監査の対象である（図７参照）。したがって、当然ながら開示される非財務情報は内部統制管理下で点検後の情報である必要がある。ただ単に情報収集して開示するでは済まない。プロトタイプアプローチをとると、会社側で整備が必要となる機能・業務の総量を早いタイミングで具体的に把握することができる。

図６　CSRD／TISAX対応の現実解

図７　CSRDによる監査対象の変化

７．TISAX

自動車部品メーカーH社のドイツ現地法人では、ドイツ自動車工業会が規定した、顧客である自動車メーカー各社からの必須取引条件としてのTISAX：Trusted Information Security Assessment Exchange認証の取得に失敗していた。TISAXとは、自動車メーカーが部品サプライヤーに要求する情報セキュリティ整備認証である。つまり車の設計情報という機密情報を部品メーカーに開示するのはよいが情報漏洩されては困るので、情報漏洩を予防するために必要な情報セキュリティの整備が完了していることを、第三者機関による認証取得によって立証せよという要請である。もしこの認証を一定の猶予期間中に取得できない場合、部品メーカーは自動車メーカーから取引停止を通達されることになる。自動車部品メーカーの内部監査の視点では、この認証取得およびその前提となる情報セキュリティ整備の状況の点検は、ビジネスリスクの点検として必須とみることができるだろう。この部品メーカーH社がはまってしまったワナは、実は前述のCSRD対応で、別の部品メーカーG社が回避したワナと同様だった。H社は100点を目指すフルスペックでの網羅的なウォーターフォールアプローチを外部コンサルタントに推奨され、採用してしまっていたのだ。社員数わずか50名の会社で、フルスペックの情報セキュリティ規程とそれに準拠した整備と運用を導入・維持するのは最初から無理がある。彼らの仕事は情報セキュリティだけではないからだ。最初から合格ぎりぎりの70点を目指し、その合格状況をいかに低コストで維持するのか？の構想と工夫が、彼らが必要するものだ。筆者チームは、TISAX対応においてもプロトタイプアプローチの採用を推奨した（図６）。

（筆者略歴）
後藤英夫（ごとうひでお）
2022年３月１日付けでEYジャパンよりEYドイツコンサルティングに出向し日系企業の経営課題対応を支援中。グローバルマトリックス経営への移行、全社基幹システム再構築、グローバル内部統制整備、新規事業立ち上げ、M&A、サプライチェーン最適化、サイバーセキュリティ対応など高難度のプロジェクトを30年以上に渡り手掛ける。日本政府のスポーツコンプライアンス強化プロジェクト外部委員（2017年～2020年）。会計教育研修機構講師（2019年～現在）。経営学修士、政策法学修士、経済学修士、理学修士（物理学）。