内部統制で大切なのは、社員全員が参加し、内部統制上の役割を果たし、かつ常にモニタリングして見直しを図ることです

内部統制で大切なのは、トップマネジメントのリーダーシップの下に，企業の構成員全員が日々の業務において、着実かつ継続的にその役割に応じた管理責任を果たし、有効に機能しているかを定期的にモニタリングして、問題があれば常に見直すことです。

日本アイ・ビー・エム株式会社（以下、日本IBM）はIBMコーポレーション（以下、米国IBM）の連結子会社であることから、サーベインズ・オックスリー法と略称される、いわゆる企業改革法（以下、SOX法）に2004年から対応。約半年間の取り組みで、従来からあったビジネスプロセスに関する手続きなどの文書を再構築し、日本の企業としてはいち早く内部統制の仕組みを強化しました。

日本IBMにおける業務審査（Business Controls）の責任者である舘林 泰雄と、スタッフとして実際にプロセスの文書化の再構築を支援した長瀬 格が、具体的な取り組みについて語ります。

Interview ❷

Participation by All Employees, together with Constant Review, Is Essential for Internal Controls.

The key things with internal controls are that all the members of the enterprise carry out management responsibility steadily and continuously according to their roles through daily activities under the leadership of top management, and that functioning is monitored periodically to see how effective it is and that, proper corrective action is always taken if a problem is found.

As IBM Japan, Ltd. is a consolidated subsidiary of IBM Corporation, it has been conforming to the so-called Company Reform law, abbreviated as the Sarbanes-Oxley Act (hereinafter, SOX) since 2004. It reconstructed documents such as the procedures of existing business processes and so forth with about half a year's efforts. It was among the first to strengthen the internal control mechanism as an enterprise in Japan.

Yasuo Tatebayashi who is responsible for Business Controls in IBM Japan and Itaru Nagase who actually supported the reconstruction of the documentation of processes as a staff member explained specifically what efforts were made.

日本アイ・ビー・エム株式会社
管理 業務審査 部長
舘林 泰雄

Yasuo Tatebayashi
Manager of Business Controls
IBM Japan, Ltd.

IBMの内部監査と業務審査

わたしたちが所属する日本アイ・ビー・エム（以下、日本IBM）の「業務審査」は、日本の企業にはなじみのない部門かもしれません。

英語ではBusiness Controlsと表記します。各国のIBMにおいて内部統制の仕組みが適切に整備され、かつ有効に機能していることを検証し、問題がある場合は改善策が講じられていることを監視する役割を担っています。

日本の企業において、業務内容の比較的似ている部門を強いて挙げるとすれば、内部監査部門になるかもしれません。しかし、両部門の業務内容には決定的な違いがあります。そのため、かつてはIBMにおいても「内部監査・業務審査」という一つの組織でしたが、SOX法成立後の2003年5月に、監査部門の独立性をより高めるために分離しました。

内部監査部門の役割が、内部統制が整備され機能していることの確認であり、事後発見的な「監査」が主であるのに対し、業務審査部門は、日ごろから主要なプロセスの内部統制を整備し、各部門がいつ監査を受けても内部統制上の問題を指摘されないように、事前予防的な助言・提言を主としています。

つまりIBMでは、内部監査と業務審査の両部門を併置して、お互いにチェック＆バランスを取ることで健全な経営を心掛けているということです。

業務審査部門の役割を知っていただくために、日本IBM内における業務審査部門と内部監査部門の組織上の位置付けをご紹介しましょう（**図1**）。

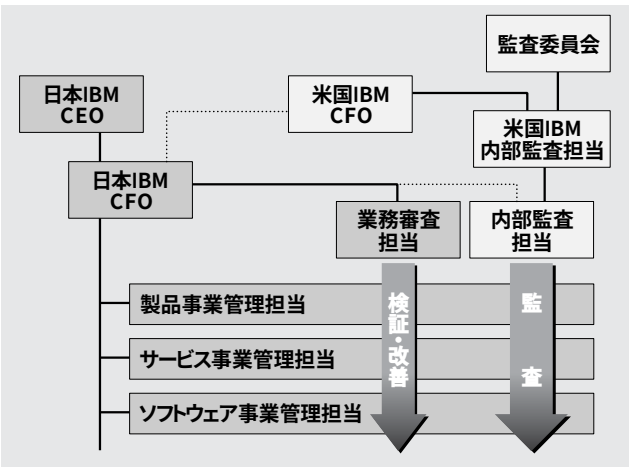

図1. 日本IBMにおける管理組織

内部監査は、組織的には日本IBMのCFO（最高財務責任者）の下に置かれていますが、業務上の指示は、日本IBMの親会社である米国IBMの内部監査部門から直接受けています。監査対象を選んだり、あるいは監査手法を決めるのは日本IBMではなく、米国IBMの内部監査部門ということです。また、米国IBMの内部監査部門は、財務会計の専門家1名を含む最低3人以上の社外取締役（2005年Annual Reportでは4名）で構成される米国IBMの内部監査委員会から、監査実施に関する指示を受けて報告することを義務付けられています。つまり、業務上の指揮命令の流れから見ると、日本IBMの内部監査部門は、日本IBMから完全に独立しているだけでなく、米国IBMの経営者からも独立性を保つようになっています。

内部監査部門にとって何よりも大切なのは、被監査部門から独立性を保ち、客観的に内部統制を評価することですから、その意味ではなかなか工夫された仕組みになっているといえるでしょう。

業務審査部門の役割

わたしたち業務審査部門の役割は「内部統制が適切に整備され、かつ有効に機能していることの検証および改善」と定められており、具体的な業務は次の通りです（**図2**参照）。

- SOX法404条で要求されている内部統制機能の整

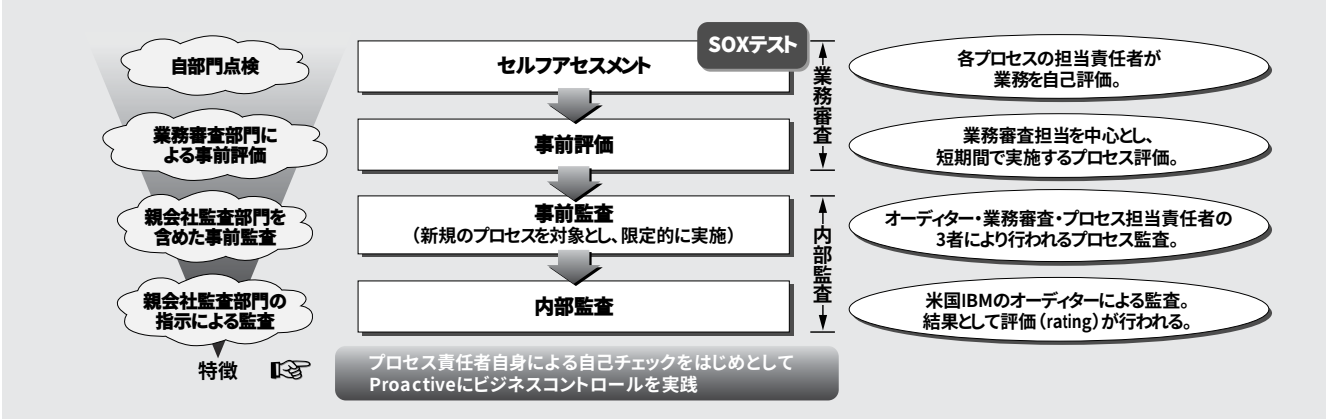

図2.　IBMのビジネスコントロール／監査体系

備と有効性に関する検証（SOXテスト）の実施管理。
- セルフアセスメント（自己評価）による部門別管理状況の評価・問題指摘。
- SOXテスト、セルフアセスメント、外部監査、内部監査などで発見・指摘された問題の解決支援。
- リスク受容申請の評価・承認。
- BCG（Business Conduct Guidelines：IBM企業倫理行動基準）への年次署名の実施管理。
- 新しいプロセスについて、内部統制の観点からの助言提供。

なお、IBMの業務審査部門は、米国で2002年7月から段階的に施行されたSOX法に対応するために設立されたわけではありません。上記の業務のほとんどは、COSO（Committee of Sponsoring Organizations of Treadway Commission：トレッドウェイ委員会組織委員会）が提示した五つの内部統制フレームワークに忠実に対応した形で、それ以前から取り組んできたものです。

COSOによれば、「内部統制は、次に掲げる目的達成に関して合理的な保証を提供することを意図した事業体の取締役会、経営者およびその他の構成員によって遂行されるプロセスである」と定義されています。

・業務の有効性および効率性

事業活動の目的の達成のため、業務の有効性および効率性を高めること。

・財務報告の信頼性

財務諸表および財務諸表に重要な影響を及ぼす可能性のある情報の信頼性を確保すること。

・事業活動にかかわる法令などの順守

事業活動にかかわる法令その他の規範の順守。

そして、「内部統制は、次の五つの構成要素からなる」として、以下の五つの内部統制フレームワークを提示しました。

・統制環境

組織の気風を決定し、組織内のすべての者の統制に対する意識に影響を与えるとともに、ほかの基本的要素の基礎となるもの。

・リスクの評価

目的の達成に関連するすべてのリスクを識別・分析することにより、そのリスクをいかに管理すべきかを決定するための基礎を提供すること。

・統制活動

経営者の命令および指示が適切に実行されているとの保証を与えるのに役立つ方針および手続き。

・情報と伝達

事業体の人々が自己の責任を果たし得るために必要な情報が、適切に識別、捕捉そして伝達されることを確保すること。

・モニタリング（監視活動）

内部統制プロセスの質を継続的に監視および評価するプロセス。

（出典：トレッドウェイ委員会組織委員会『内部統制の統合的枠組み 理論編』白桃書房P 33,53,81,97,113）

以前からCOSOのフレームワークに対応していたので、結果的に、SOX法に対しても十分に対応できたということです（**図3**参照）。

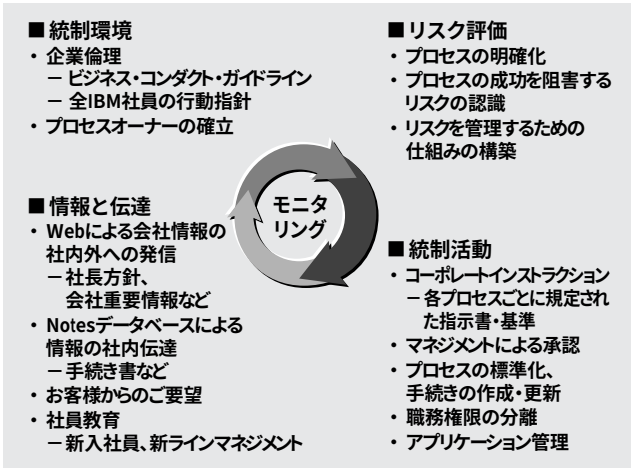

図3.　IBMの内部統制のフレームワーク

「統制環境」への取り組み

それでは、COSOの五つのフレームワークに沿って、日本IBMの内部統制への取り組みを見ていきましょう。

内部統制は、トップマネジメントのリーダーシップの下に、全社員が各人の役割に応じた管理責任を、日々の業務において着実かつ継続して果たしていくことが重要です。

健全な内部統制を構築・維持することは、トップマネジメントの責任であることを自ら十分に認識し、日ごろから健全な内部統制を重視する組織風土を醸成して、全社員に参加と協力を要請する必要があります。

そこで連結グループ会社を含む日本IBMの全社員は、トップマネジメントからの要請を受けて、BCGを年に1度読んで、その内容を理解した上で違反行為を行わないことを誓約しています。

また2005年度からは、営業活動における事例を用い、間違った行為が財務諸表にどのような影響を与えるかという教育も、全社員に実施しています。

さらに、リスクをプロセスごとに管理するという観点から、経理・購買・財務・人事などの主要プロセスごとの全世界の責任者（グローバル・プロセス・オーナー）を定め、各国のオーナーに指示する仕組みを整えています。これにより、IBMのいずれかのプロセスで何らかの問題が発生した場合は、すぐさま世界中のIBMに対して再発防止のアクションを取らせることができます。しかもプロセスごとにオーナーを定めることで、複数の権限を一人に集中させないことにもなり、オーナー間でのチェック&バランスが働きます。

「リスク評価」への取り組み

先ほども申しましたように、IBMはリスクをプロセスで管理するという考え方を採っています。各プロセスのオーナーを定め、プロセス全体を文書化して、プロセス上で発生すると考えられるリスクを明確化し、どのようにしてリスクを避けるのかという管理の仕組みを整えているのです。

リスクの評価においては、発生する可能性のある重要なリスクのすべてを検討対象とする必要があります。そのため、各プロセスのリスクを識別するには、業務の最初から完結までを網羅して文書化する必要があります。例えば、営業のプロセスでは、新規のお客様の登録に始まり、見積書の提示、売掛金の回収までを文書化します。文書化とは、簡単に言えば「与信以上に注文を取ってはいけない」というように、社員の誰が見ても分かるような形でプロセスの重要なルールを定義し、社員が守れるようにすることです。

注意しなくてはならないのは、プロセスの文書化は、守るべきルールを明確化したにすぎず、それだけで内部統制が行われたことにはならないことです。何よりも、文書化されたプロセスに沿って、日常業務を行うことが大切です。同時に、会社として新しいビジネスを始めたり、あるいは社会環境が大きく変化したときには、文書化したプロセスに合わない事象が生じることもあります。その意味では、プロセスの継続的な改善が必要不可欠であり、内部統制の改善に終わりはありません。

「統制活動」への取り組み

プロセス上のリスクは、実際に発生しないように、日々のオペレーションに組み込んで、管理項目として関係者に伝えなくてはなりません。具体的には、プロセスごとの手続きや指示書という形になります。

日本アイ・ビー・エム株式会社
管理 業務審査
アドバイザリー・ビジネスコントロール・アナリスト
長瀬 格

Itaru Nagase
Advisory Business Control Analyst
Business Controls
IBM Japan, Ltd.

統制活動において、IBMが重視しているのは、SOD（Separation of Duties：職務権限の分離）です。購買プロセスを例に取れば、「物・サービスの購入を承認する人」「売り手を探して価格を決めて発注する人」「納入を確認する人」「売り手に対価を支払う人」という少なくとも4人の職務権限が分かれている必要があります。職務権限の分離により「実際に受け取っていないものにお金を払ってしまった」とか「必要以上に高い物を買ってしまう」という行為を防ぎ、健全な購買プロセスを実施することができます。

また、プロセス管理にはITシステムが用いられますから、アプリケーションシステム自体に内部統制上の不具合や抜けがないかをチェックする必要があります。内部監査部門に所属しているITスペシャリストが、リスクの高いアプリケーションについてシステム監査を行い、稼働する前にしかるべき内部統制が組み込まれているかどうかをチェックする仕組みになっています。

「情報と伝達」への取り組み

ここまでご説明してきた「統制環境」「リスク評価」「統制活動」や「モニタリング」などの内部統制にかかわるさまざまな情報について、組織の上層～下層、横方向、下層～上層へ、効果的かつ正確に伝達することが必要です。また、お客様や協力会社様など外部の方々との間の情報伝達も同様に大切です。ここでもITシステムが活躍します。

先ほどもご説明したように、BCGの開示をはじめとする会社情報の外部発信にはインターネットを用い、社長方針や会社重要情報、部門情報／会計処理手続きなどの社内伝達にはイントラネットを利用しています。また、手続き書やコントロール情報などのプロセス情報の伝達には、社内のNotes®データベースを利用して徹底を図っています。

さらに、社員および臨時雇用者から、会社の方針・施策・運営に関する疑問を吸い上げる「スピーク・アップ・プログラム」や、お客様からのご要望やご意見、苦情などが関係部門に効果的に伝達する仕組みも整えています。

正確な伝達のためには、教育も重要です。新入社員はもちろん、新しくラインマネジメントに昇進した社員に対しても情報伝達にかかわる社員教育を実施しています。また、重要プロセスの変更を行った場合には、関連者への周知徹底のための教育も欠かせません。

「モニタリング」への取り組み

「統制環境」「リスク評価」「統制活動」「情報と伝達」が有効に機能し（**図3**参照）、内部統制の目的である業務の有効性および効率性、財務報告の信頼性、法令などを順守できているかどうかを常にチェックしなければなりません。これが「モニタリング」です。

冒頭で説明したように、内部監査部門のレビューにより、何らかの問題があればそれを指摘するとともに、業務審査部門は問題が発生しないように事前予防的なレビューを行っています。

また、日本IBMは米国IBMの連結子会社であることから、SOX法に基づいて四半期ごとにSOXテストを実施することが求められています。

こうした客観的なレビューに加え、プロセスオーナーが、自身でセルフアセスメントを行うことになっています。担当しているプロセスについて自分で点検を実施し、健全な状態の場合は「Satisfactory」、問題はあるものの当面の応急的な対策が取られている場合は「Marginal」、問題があって対策が取られていない場合は「Unsatisfactory」という3段階の自己診断を行

います。評価が「Marginal」「Unsatisfactory」のときには、そのオーナーはグローバル・プロセス・オーナーに対して、内部統制上の問題点、根本的な原因、恒久的な対策、問題解決予定日を説明することが求められます。

「ITの活用」への対応

2005年12月に公表された内部統制部会の報告書では、COSOの五つのフレームワークに加えて「ITへの対応」（前年7月の公開草案では「ITの利用」）が追加されました。今日のビジネスにおけるITの役割を考えると、やはりITを抜きに内部統制を実施するのは困難でしょう。

そこでITシステムに関連する内部統制の監視という観点から、IBMでは大きく「インフラ」と「アプリケーション」に分けて管理しています。

IT部門が管理するインフラ、すなわちサーバーやネットワークについては、IT部門自身が内部統制の管理状況をセルフアセスメントします。このセルフアセスメントは、IBM全体で機器やソフトウェアの種類別に設けられた共通のセキュリティー基準に従っています。悪意ある攻撃はもちろんのこと、「間違い」や「見落とし」に対してもシステムが保護されているかを確認します。特に、アクセス権限などのように重要な点検項目に関しては、SOX法に対応する形で四半期ごとに確認しています。

セルフアセスメント以外に、内外の監査人による監査も実施しています。SOX法対応で実施した点検項目については、毎年、外部監査人による実地監査が行われます。

アプリケーションシステムについては、SOXアプリケーション（IBMの財務諸表に影響を与えるアプリケーションシステム）については財務諸表関連の項目を、それ以外のアプリケーションシステムについては開発・運用・保守にかかわる項目について、アプリケーションから独立した第三者によって四半期ごとに点検されています。

なお、IBMではASCA（Application System Control & Auditability）と呼ばれる独自の監査制度を設けています。アプリケーションの中でプロセス上のリスクの高いものについては、この監査に合格しなければ使えないという制度であり、内部監査部門のIT専門家によって、アプリケーション導入時・変更時に監査を行います。また、導入あるいは変更後期間が経過しているものに対しては抜き打ち監査もあり、合格しなければ運用はできないようになっています。

使用アプリケーションに対する責任は、IT部門ではなく、ビジネスプロセス・オーナーが負います。なぜなら、そのプロセスで当該アプリケーションを使う／使わないの判断はプロセスオーナーに委ねられているからです。また、複数のアプリケーションを使用するプロセスも多く、これらのアプリケーション利用者間の職務権限の分離についてはIT部門が判断するのが難しいからです。

IBMのBCGについて

以上、IBMの内部統制の仕組みについて、その大枠をCOSOのフレームワークに沿って紹介してきましたが、「統制環境」で簡単にご紹介したBCGについて、もう少し説明することにしましょう。

表1にBCGの各項目を示します。BCGは全世界のIBMで共通であり、細かい内容を規定しているわけではなく、文字通り社員の行動指針を示しています。

もちろん社会環境の変化や法制度の変更に合わせて、内容の見直しを常に図っています。例えばSOX法の施行に合わせて「会計・財務報告に関する法律」という項目が加わりました。

BCGは、当社のWebサイトでも公開していますので（http://www-06.ibm.com/jp/ibm/bcg/）、具体的な内容についてご覧いただくこともできます。

プロセスオーナーの役割

もう一つ、IBMの内部統制への取り組みで大切なのがプロセスオーナーという考え方です。

図4に示したように、例えば経理であれば、日本IBMだけではなく、各国IBMの経理プロセスのすべ

表1.　BCGの項目一覧

■あなたとIBMでのあなたの仕事
- コミュニケーション・チャネル
- ひとりひとりの行動
- 職場環境
- 社員のプライバシー
- IBM資産の保護
- IBM社内情報システム
- 不注意による情報漏洩
- 直接に情報を求められた場合と報道関係者、アナリスト等との接触
- 専有情報の使用
- IBMの知的所有権
- IBMを退職する場合
- 法律上の救済手段
- 情報の記録と報告

■IBMのビジネスを行うにあたって
- 購買取引先との関係
- 互恵取引を避けること
- 市場における競争
- 競争会社について虚偽または誤解を招く表現を避けること
- 競争会社の受注と競合する販売活動
- 他の企業との取引関係
- 競争会社との業務上の接触
- 他社に関する情報の収集と利用
- 機密情報または使用制限付情報の受領
- ソフトウェアの取得
- 商標の使用
- 賄賂，贈物および接待
- ビジネス上の接待
- 贈物の授受
- 紹介料
- 官公庁の職員との関係
- 公務員によるキャンペーン訪問、講演と謝礼
- 法の遵守
- 競争
- 輸出・輸入
- ボイコットの禁止
- 環境
- 官公庁の調達
- 会計・財務報告に関する法律

■私的活動とIBM社員としての立場
- 利益の衝突
- 競争会社への協力
- IBMとの競争
- IBMとの取引
- 勤務時間とIBM資産の私的使用
- 個人の財務上の利益
- 上場会社／非公開企業の株式
- 内部情報利用とインサイダー取引
- 公共活動
- 政治活動への参加
- 意見の表明
- 近親者が同業他社で働いている場合

てをグローバル・プロセス・オーナーが統括する仕組みになっています。図は簡略化され日本IBMと中国IBMのみが表示されていますが、全世界のIBMに対する責任者を設けているということです。

グローバル・プロセス・オーナーの下には、リージョンと呼ばれる幾つかの国を束ねた地域（日本はアジア／パシフィックに所属）のオーナーがいて、さらにその下に各国のオーナーがいるという階層構造になっています。ですから、各国の各プロセスのオーナーは、グローバル・プロセス・オーナーあるいはリージョンのオーナーからの指示に基づいて、それぞれの責任を果たすことになります。

また、縦軸のハードウェア販売・ソフトウェア販売・サービスといった各ビジネスエリアにもオーナーを定めて、こちらもビジネスエリアごとのグローバル・プロセス・オーナーからの指示に従うことになっています。各ビジネスエリアのオーナーは、例えば、信用審査プロセスや価格設定承認プロセスなどのように、それぞれのエリアに特有なプロセスについて責任を持ちます。

このグローバル・プロセス・オーナーのマトリックス構造により、IBMのすべての主要なプロセスをカバーしています。

内部統制の限界を知り、常に見直しを図る

今日の企業経営にとって内部統制は不可欠です。しかしながら内部統制の整備さえ行えば、この領域の問題をすべて解決できるというわけではありません。例えば次のような行為が行われたときには、内部統制が有効に機能しない場合があるからです。

- 担当者の判断の誤りや不注意。あるいは複数の担当者が共謀したとき。
- 想定していなかった組織内外の環境の変化や非定型的な取引など、内部統制で文書化してない状況が生じたとき。
- 内部統制の整備と運用に、費用対効果の側面から十分なコストを掛けられないとき。
- 経営者が不当な目的のために内部統制を無視したとき。

内部統制が、経営者と取締役会への提供を期待されるのは「合理的な保証であって、絶対的な保証ではない」といわれるのはこのためです。

また、先ほども述べましたが、健全な内部統制の構築と維持には、継続的な改善が不可欠です。文書化すればそれで完成ということではなく、COSOフレー

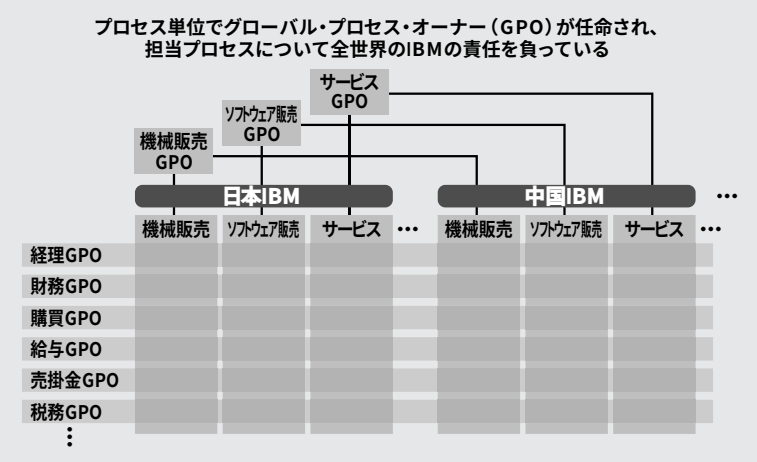

図4.　プロセスオーナーのマトリックス構造

ムワークに示されているように、ビジネス環境の変化や各種法案の施行などに合わせて、次のようなときには見直しを図る必要があります。

- 会社を取り巻く環境の大きな変化
- 新しい法律施行
- 新しいビジネスの発生
- 大きな問題の発生
- 大きな組織変更、経営目標の変更

（出典：トレッドウェイ委員会組織委員会『内部統制の統合的枠組み 理論編』白桃書房　P18, P 21, P71-79）

逆に言えば、内部統制には限界があるからこそ、常に問題が起きていないか監視し続けなければいけないということです。内部監査も、SOXテストやセルフアセスメントもその目的のためにあるわけです。

常時監視することで、何か問題があったときには、すぐさま改善のアクションにつなぐとこができる体制をつくっておくということです。

今後の法制化への対応に向けて

最近では、お客様からの依頼を受けて、日本IBMにおけるSOX法や内部統制への取り組みについてお話しさせていただく機会がよくありますが、先ほども申し上げたように、わたしたちがSOX法の施行以前から内部統制に取り組んでいたことに皆様驚かれます。

図5に示したように、SOX法対応のために新たに取り組んだ項目は、QCM（Quarterly Certification of Management）という四半期ごとの財務諸表の信頼性ならびにその作成プロセスの健全性についてのCEO（最高経営責任者）、CFOによる宣誓プロセスと、四半期ごとの内部統制の有効性についてのサンプルテスト（SOXテスト）だけです。それ以外は、すべて以前から実施していた内容です。

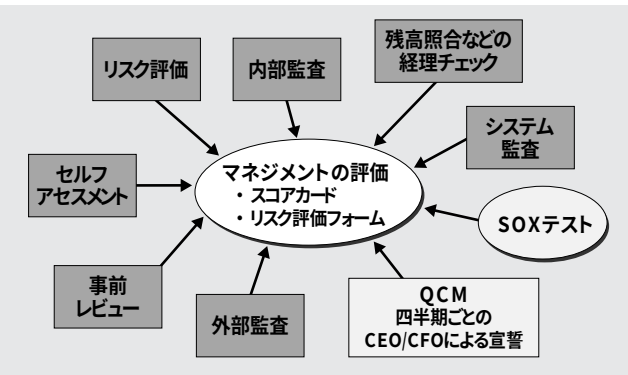

図5.　IBMの内部統制の有効性評価

例えば契約上のリスクの管理に関しては、IBMには世界中で共通の契約書があり、そこから逸脱する契約の場合は法務部門のレビューを受けるというプロセスがありました。こうした仕組みが整っていたため、SOX法対応のための準備作業は、既存のプロセスを文書化すればよく、約6カ月で済みました。

しかし、契約書の標準化などの仕組みが整っていなければ、まずはゼロからつくり上げることから始めなければなりません。かなり大変な作業となることでしょう。つまり、文書化以前のプロセスの標準化に時間がかかるということです。だからといって事業部ごと、国ごとに取り組んでしまうと、さまざまな標準ができてしまい、かえって収拾がつかないことになりかねません。

そう考えると、グローバル・プロセス・オーナーのようなコンセプトを導入した方が、結果的に早いのではないでしょうか。

大切なのは、内部統制は、事業目的遂行上必須となる業務の有効性および効率性、財務報告の信頼性、法令などの順守を達成するために、日常業務プロセスに組み込む管理手法であるということです。従って、企業の事業目的、プロセスや企業を取り巻く環境の違いによって、最適な内部統制は異なったものになります。

当然ながらIBMのアプローチが唯一のものではありませんし、IBMの採った方法を採用すれば問題は生じないと言い切ることもできません。当社の取り組みは一事例として参考にしていただいた上で、外部監査法人の意見をお聞きいただき、自社にとってベストと思われる方法で取り組まれるといいでしょう。