内部統制ITソリューションフレームワーク
― 内部統制の目的の実現を支援するITソリューションとは何か ―

既にほかの記事で述べられているように、内部統制の目的は(1)財務報告の信頼性、(2)関連法令への準拠、(3)業務活動の有効性と効率性、(4)資産の保全です。(1)(2)だけに一時的に集中すると、内部・外部の監査をパスするためだけの文書化作業にとらわれてしまい、内部統制が本来の目的とする業務活動の有効性・効率性やアカウンタビリティーの向上に目がいかなくなる恐れがあります。さらに内部統制は、企業の存続に従って永久に維持向上していく活動でもあります。

一方、IT(情報技術)は企業活動におけるその影響度から、内部統制の対象としてコントロールすべき業務であると同時に、内部統制の要素(統制環境、リスク評価、統制活動、情報と伝達、モニタリングなど)において飛躍的に有効性と効率性をもたらす技術です。本稿ではその面に注目し、ITが内部統制を支援し、その目的を達するためにどのようにかかわるかを述べます。

Article 2

IT Solution Framework for Internal Control
– What are IT Solutions to Support the Realization of Objectives of Internal Control –

As has already been discussed in other articles, the objectives of the internal control are (1) Reliability of financial reporting, (2) Compliance with applicable laws and regulations, (3) Effectiveness and efficiency of operations, and (4) Safeguarding of assets. When an enterprise concentrates only on (1) and (2), it tends to be preoccupied with documentation work only to pass internal and external audits attention may not be paid to the improvement of the effectiveness/efficiency and accountability of business activities that are the primary objectives of internal control. Internal control should be maintained and improved continually as long as the enterprise keeps operating.

Information technology (IT) related activities are to be controlled as a target of internal control because of its impact on enterprise activities. IT also brings about dramatic effectiveness and efficiency in the internal control elements (control environment, risk assessment, control activities, information and transmission, monitoring, etc.). This article focuses on this aspect and discusses how IT supports internal control and how it is involved in achieving the objectives of internal control.

日本アイ・ビー・エム株式会社
e-セキュリティー・オフィサー
IBMディスティングイッシュト・エンジニア、
IBMアカデミー会員

石垣 良信 Yoshinobu Ishigaki

[プロフィール]
1971年日本IBMにSE(システムエンジニア)として入社。データセンター業務・流通部門のSEとしてシステム設計に従事。その後米国大学院留学にてコンピューターサイエンスで修士課程を終了後、SE技術部門にてシステム管理・人工知能・オープンシステムなどのソリューションサポートに従事。日本アイ・ビー・エム・システムズ・エンジニアリング株式会社の役員、アジア・パシフィック・システム管理事業部長などを経て2003年より現職。専門はITセキュリティー／プライバシー技術、トレーサビリティー技術など。

❶ 内部統制におけるITの位置付け

内部統制の面から見た企業活動におけるITに関連する活動は**図1**に示すように三つに分けられます。

一つは、業務活動の一部として自動的に「② ITにより実施される業務」で「IT業務処理統制」の対象となる部分です。IT化が進むに連れて、企業全体の業務活動に占めるこの部分の割合が年々大きくなってきています。ITによって自動実施される業務は、手作業に比較して生産性・効率性を飛躍的に向上できますが、反面ブラックボックス化により、内在するエラーや悪意のある行為が気付かれることなく大量の誤ったトランザクションを生み出してしまう危険性を持っています。

二つ目は、外部からは見えにくいものの、IT業務処理の実現共通機能部分として通常IT部門だけで実施される「④ IT特有の基盤活動」で「IT全般統制」の対象となる部分です。ITはその複雑性のために共通コンポーネント化が進んだ分野であり、ハードウェア、ソフトウェア、ネットワークおよび開発管理技術に関して標準化が行われています。そのため逆に、IT関連業務の共通部分はIT技術者しか理解・評価できない側面を持っています。

最後に、内部統制の有効性・効率性・維持継続性を向上するための「③ 内部統制を支援するIT機能」です。内部統制は、場合によってはほぼすべての企業活動を対象にしますので、内部統制実施の生産性・効率性は大きく企業活動そのものの有効性・効率性に影響します。現に法制化で先行する米国では内部統制の実施による作業負荷とコストの大きな増加が問題になりつつあります。IT業務処理統制やIT全般統制については既にさまざまなフレームワークが議論され、公表されています。しかしながら、世界的に内部統制の法制化が比較的最近に実施されている事情から、③の部分は参照できるフレームワークや議論が少ないのが現状です。本稿ではそれに対する答えとして、後述する一つのフレームワークを提案しています。

三つのいずれのIT活動分野も固定的ではなく、境界線はIT化が進むに連れて変化していきます。手作業やデスクワークで行われている企業活動はさらにIT化されるでしょう。個々のアプリケーションシステムで実施されていたIT業務統制はコンポーネント化・共通化されて、IT特有の基盤活動として位置付けられることも考えられます。内部統制を支援するIT機能が進化すれば、個々の業務プロセスやITにより実施される業務では、意識しなくても自動的に内部統制が実行される可能性もあります。

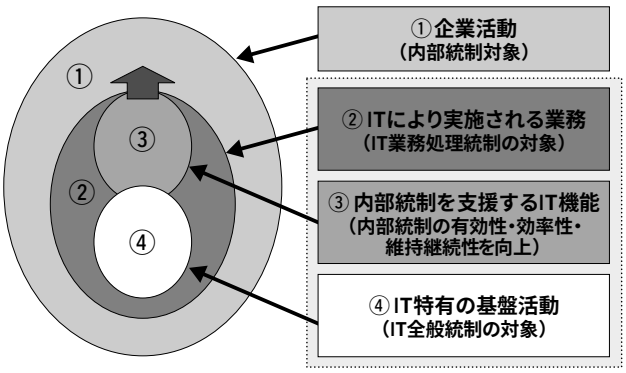

図1.　内部統制におけるITの役割

❷ IT業務処理統制におけるITソリューション

手作業やデスクワークで行われている業務をITで実現することは、それ自体が標準化・共通化・自動化により業務の統制機能を実現することにつながります。従ってIT化すればするほど手作業で内部統制の整備や運用、モニタリングなどの作業負荷を軽減してくれます。

しかし、既に述べたように、ITで実施される業務処理には、ITシステムに内在する可能性のあるエラーにより多量の誤ったトランザクションや情報を生み出してしまう危険性を否定できません。特に財務報告につながるアプリケーションシステムにおいては一つのエラーが財務報告書における不正確な数字や判断となって現れる可能性があります。エラーは怠慢や不注意といった無意識の行為により生じるもの（プログラムのバグなど）と、故意に行う行為で生じるものがあり（プログラムやファイルデータの改ざんなどで通常犯罪や規則違反、義務違反行為）、どちらにも対処できるような統制（コントロール）をITシステムに組み込まなければなりません。

財務報告にかかわるIT業務処理統制とは「個々のアプリケーションシステムにおいて、承認された取引がすべて正確に処理され、記録されることを確保するコンピュータープログラムに組み込まれた統制」をいいます。具体的にはデータと処理の正確性（間違えていない）、網羅性（対象となるデータがすべて網羅されている）、正当性（実在する取引に基づき、正当な人により報告・処理されている）、維持継続性（継続して何期にもわたって過不足や不整合なく処理が可能である）ことを確保することです。**表1**に具体的な統制（コントロール）の目標を例示しました。

《IT業務処理統制を支援するITソリューション》

この分野のITソリューションには以下のようなもの

表1. IT業務処理統制のコントロール目標

コントロール目標	内容	IT業務処理統制の具体例
正確性	入力すべき情報が、すべて正しく適時に入力され、その組織体において定められた手続きに準拠して、記録・処理が行われること。	・誤入力防止のための入力画面機能 ・検証リストによる入力データの正確性チェック ・エラーリストの出力とその対応 ・異常／例外データリストの出力とその対応…
網羅性	入力すべき情報が、漏れなく、また重複なく入力・処理され、意図する目的の通りに出力情報が利用できること。	・入力原票の連番管理 ・入力件数の合計照合 ・トランザクションデータの連番管理…
正当性	権限者により承認された真実の経済事象を反映した情報のみが、情報システムに入力され、また承認された担当者のみがファイルやプログラムにアクセスできること。	・権限者による承認とその記録保存 ・ワークフロー上の承認ルート／承認権限の設定 ・マスターおよびトランザクションデータへのアクセス権限の管理…
維持継続性	マスターファイルは常に適時に正しい情報に継続して更新され、関連するマスターファイル間の情報の整合性が保たれていること。また情報の入力・処理・出力の過程において情報の整合性が保たれていること。	・関連するマスター情報間の整合性確認 ・更新結果の整合性の自動照合 ・更新時のエラー表示と対応 ・データベースの統合による情報ソースの一元化…

が考えられます。

- **IT業務処理統制対象アプリケーション登録／評価システム**
  - ― IT業務処理統制対象基準の作成
  - ― IT業務処理統制対象アプリケーションの登録・情報検索・評価プロセスをサポートするシステム
  - ― IT業務処理統制レポートシステム（評価用）
- **アプリケーションシステムの開発・変更・導入管理ツール群**
  - ― アプリケーションプログラムの入力・処理・出力・使用マスターファイル、コントロール方法などが容易に登録／検索／評価できるツール群
  - ― 実際のアプリケーションプログラムの開発・変更作業への連携
- **アプリケーションプログラム開発・調達のガイド・基準書など**
  - ― IT業務統制を導入するためのガイダンスや企業ポリシーを記した基準書など
  - ― 設計ガイド、プログラミングガイドやテンプレートなど
  - ― アプリケーションシステム調達の基準書
- **企業ポリシー、ガイド、マスターファイルの登録／導入／更新ガイド**
  - ― 企業のポリシー、ガイド、マスターファイル類へのポータル
  - ― 企業活動の基準となるマスターファイルの登録・データ入力／更新手順のガイド
  - ― データオーナー部門の登録・更新
- **ユーザーガイド、オペレーションマニュアル、運用・回復・再始動手順書などの整備**
  - ― 各種ガイド、マニュアル、手順書の登録／更新システム
  - ― 文書ポータル機能
- **IT業務処理統制教育**
  - ― e-ラーニング、コンテンツの開発
  - ― 社内教育・訓練サポートシステム

❸ 内部統制の実現ステップ

内部統制を支援するIT機能を説明する前に、内部統制が行われる仕組みを説明しておく必要があります。もちろん内部統制のやり方は企業によってさまざまな形態を採り得ますので、本稿で説明する仕組みは一つの方法にすぎません。

COSO（Committee of Sponsoring Organizations of Treadway Commission：トレッドウェイ委員会組織委員会）[1]や金融庁の基準書[4]による内部統制フレームワークの要素に従って内部統制を実現するステップを以下に説明します（**図2**参照）。

≪ステップ1≫内部統制インフラの開発と保守

企業に内部統制を導入・維持するために体制や環境を整えるステップです。内部統制フレームワークの要素群における「統制環境」や「情報と伝達」に対応します。

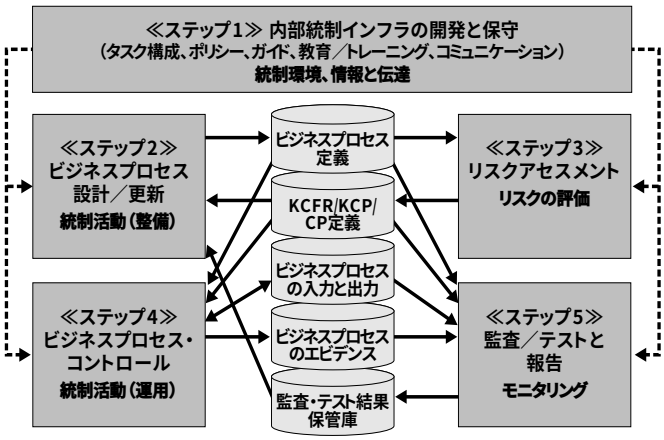

図2.　内部統制実現のステップ

≪ステップ2≫ビジネスプロセス設計／更新

ビジネスプロセス定義の設計と更新を行うステップです。内部統制フレームワークの要素群における「統制活動」の整備に対応します。通常、プロセスオーナーによって行われます。次に続くリスクアセスメントのステップで出力されるリスクの識別と、それを未然に防ぐためのコントロール活動を含むように設計されます。またこのステップの出力の一部は、監査用の文書としてそのコントロールが妥当性を持ったものかどうかが評価されることになります。

≪ステップ3≫リスクアセスメント

業務プロセスの設計と内在するリスク、そこに導入された内部統制のためのコントロールが妥当なものかを評価します。必要であればビジネスプロセスを変更したり、新たなコントロールを導入するように改善策を出力します。内部統制フレームワークの要素群における「リスクの評価」に対応します。プロセスオーナーが自ら行い、内部・外部の監査エキスパートによってその妥当性評価が行われます。また対応や修正が未完のリスクやコントロールの重要欠陥が発見されれば、内部・外部の監査人によって報告されることになります。

≪ステップ4≫ ビジネスプロセス・コントロール

設計されたビジネスプロセス定義に従って実際の業務を実施統制する活動です。内部統制の中核になる活動で、内部統制フレームワークの要素群における「統制活動」の運用に対応します。業務（ビジネス）プロセスの実施とその統制活動は一体となって行われます。またその実施よってエビデンスとなるビジネスプロセス・インスタンス（例えば業務報告／記録）、入出力データ、参照マスターファイルやガイド、決定項目と内容、後続ビジネスプロセスなどが記録されます。

≪ステップ5≫監査・テストと報告

ビジネスプロセスの実施が設計されたように行われているかを検証し（テスト）、コントロール活動が正しく行われ、有効であるかどうかを評価する（内部・外部の監査）ステップです。内部統制フレームワークの要素群における「モニタリング」に対応します。通常テスター、内部監査チームや外部監査チームによって行われます。テストや監査の結果は集計・評価され、重要な欠陥については緊急の修正活動や外部への報告を行い、軽微なものや受容できる範囲のものは報告と同時に、新たなビジネスプロセス定義やコントロールの追加・変更につなげることになります。

❹ 内部統制を支援するIT機能における ITソリューション

より具体的なITソリューション群を説明するために**図3**に、典型的な内部統制フレームワークによる財務報告システムを示しました。これは財務報告における内部統制の有効性と効率性、維持継続性を向上するために十分なIT化を行った最終形と考えてください。

以下にそれぞれのITプロセス群におけるITソリューションを説明します。

≪ITプロセス群1≫内部統制インフラの開発と保守

前節の≪ステップ1≫に相当する業務を支援するITプロセス群です。この分野のITソリューションには以下のようなものが考えられます。

- **内部統制タスクチーム管理**
  - ― ビジネスオーナーとプロセスオーナーの構成
  - ― リスク管理チーム
  - ― 監査／テストチーム
  - ― 関連会社サポートチーム

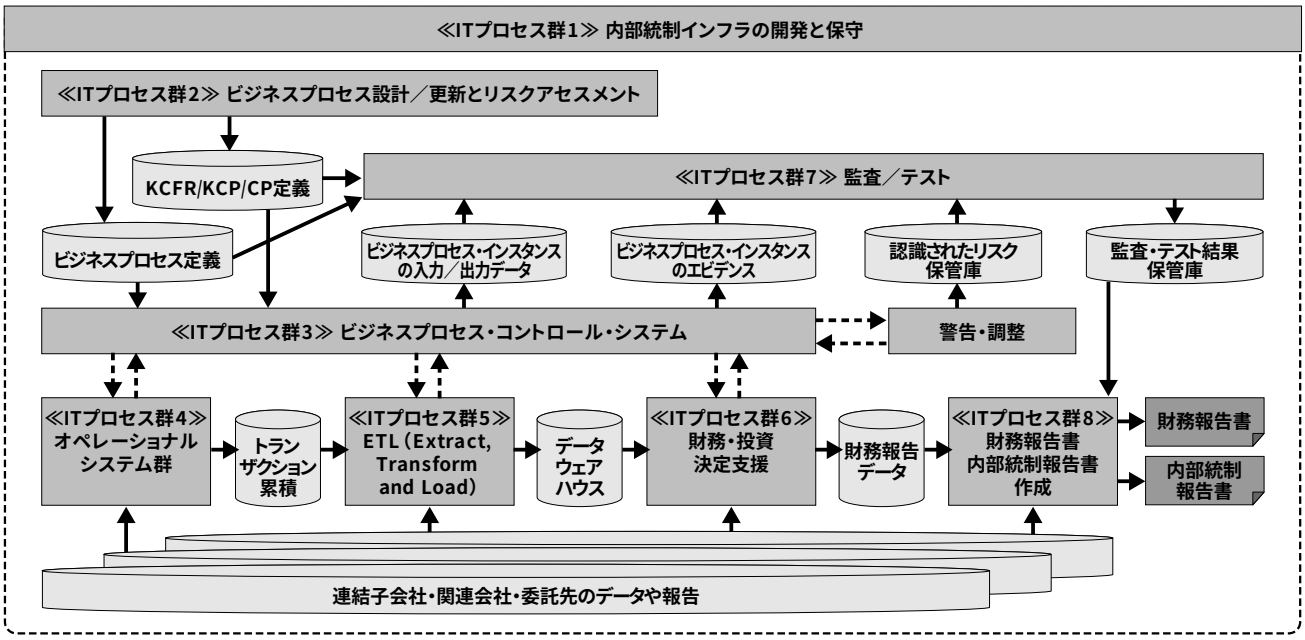

図3.　内部統制フレームワークによる財務報告システム例

- **スコアカード管理**
  - ― ビジネスオペレーション内部統制報告の健全性指標群
  - ― 財務リスクとオペレーショナルリスクの双方をカバー
- **企業ポリシーとガイドの開発・保守**
  - ― 関連法規、標準の整理ツール
  - ― ITシステムで参照／実行可能なビジネスオペレーションのポリシーとガイド
  - ― ITシステムで参照／実行可能な監査・テストのポリシーとガイド
- **社内コミュニケーション**
  - ― Webページ、ディスカッションデータベース、メーリングリスト
  - ― セキュリティー／プライバシー保護機能
- **社内教育**
  - ― e-ラーニングツールとテキストの提供

≪ITプロセス群2≫ ビジネスプロセス設計／更新とリスクアセスメント

前節の≪ステップ2≫と≪ステップ3≫に相当する業務を支援するITプロセス群です。以下のようなITソリューションが考えられます。

- **ビジネスプロセス設計／更新**
  - ― ビジネスプロセス・フロー作成ツール
  - ― ビジネスプロセス入力／出力構成（HIPO：Hierarchy plus Input Process Output構成）作成・操作
  - ― ビジネスプロセス定義の作成と一貫性確認
  - ― ビジネスプロセス定義データベースと各種検索機能
  - ― ビジネスプロセス・コントロールとの自動連携機能
  - ― ビジネスプロセス変更管理ツール（版管理）
  - ― リスクアセスメント、KCFR/KCP/CPの設定との連携
- **（財務）リスク識別**
  - ― リスクによるCBM（Component Business Modeling）解析
  - ― 財務報告リスク解析ツール
  - ― ビジネスプロセス・リスク解析ツール
- **ITシステムリスク識別**
  - ―「戦略的情報セキュリティーフレームワーク開発メソドロジー」
  - ― セキュリティー／プライバシー・リスク解析ツール
  - ― BRCS（Business Resiliency and Continuity Systems）リスク解析ツール
  - ― プログラム開発／変更／導入リスク解析ツール
- **KCFR/KCP/CP登録・変更管理**
  - ― ビジネスプロセス定義内の自動KCFR/KCP/

CP登録／識別
- KFCR/KCP/CP変更管理ツール
- コントロール追加／変更／削除ツール

・ 主要パフォーマンス指標の見積もり
- ビジネスプロセス・パフォーマンス・シミュレーター
- コントロールプロセス・パフォーマンス・シミュレーター

≪ITプロセス群3≫ビジネスプロセス・コントロール・システム

前節の≪ステップ4≫に相当する業務を支援するITプロセス群です。以下のようなITソリューションが考えられます。

・ビジネスプロセス・スケジューリング、フローコントロール
- ビジネスプロセス・スケジューラー
  - 定期的インターバル・頻度・経過時間・トリガーによるスケジューリング
- ビジネスプロセス・フロー・コントローラー
  - トランザクション種別による自動フローコントロール：トランザクションタイプ・契約額・顧客タイプなど
  - 誤りや再試行を防ぐための自動フローコントロール
  - リスクを回避するための自動フローコントロール
- ワークプレースソリューション群
- ビジネスプロセス・ガイド検索システム

・エビデンスデータの記録・保管
- e-文書法ソリューション
- 文書保管庫在庫管理システム
- ビジネスプロセス入出力記録保管システム
- ビジネスプロセス・トレーサビリティー・システム
- XBRLに基づくLedgerデータの保管
- SBC（Server Based Computing）

・プロセスインスタンス実施者アサイン
- SOD（Separation of Duties）表管理システム
- コンテキストによるダイナミックな実施者アサインシステム
  - トランザクション種別による自動アサイン：トランザクションタイプ・契約額・顧客タイプなど
  - 利害関係などのバランスによるトランザクションのトレーサビリティーデータ（履歴）による自動アサイン
  - 関連するデータの構成による自動アサイン

・データアクセス管理
- 企業ポリシーに基づくデータアクセス管理
- ビジネスプロセスの進行に基づいてダイナミックに行われるデータアクセス管理

またこのITプロセス群には、業務プロセスの進行を常時監視し、リスクを発見して警告したり、場合によっては自動的に調整するIT機能が考えられます。以下のようなITソリューションです。

・リスク発見と警告
- 財務リスク、コンプライアンスリスク、または不十分なデータの発見
- チェックリストやガイドに基づくチェックや警告
- IT実行可能な企業ポリシーステートメント群による半自動発見
- 管理者による割り込みと記録による警告処理
- リアルタイムの発見と警告
  - 特定のプロセスインスタンスに関する情報だけによる自動リスク発見
  - 利害関係などのバランスによるトランザクションのトレーサビリティーデータ（履歴）による自動発見
  - 関連するデータの構成による自動発見

・調整
- 企業ガイドによる調整
- IT実行可能な回復プロシージャーによる半自動調整
- 状況把握による自動調整

≪ITプロセス群7≫監査／テスト

前節の≪ステップ5≫に相当する業務を支援するITプロセス群です。以下のようなITソリューションが考えられます。

・内部監査、テストの管理
- アトランダムまたは異常なトランザクションのスクリーニング

— 第三者としての内部監査、テスターのアサインシステム
— 日・週・四半期・年のテスト項目ごとの自動アサイン
— 内部監査、テストの実施プロジェクト管理ツール

- **エビデンスデータの収集**
  — e-文書管理システム、文書管理システム
  — ビジネスプロセス・エビデンス検索・自動収集システム
  — 社内外データ探索システム
- **内部監査実施**
  — CAAT（Computer Assisted Audit Techniques）
  — ETL（Extract, Transform and Load）ツール
  — さまざまなシングルビューが可能なツール群
- **テスト実施**
  — トランザクションへの関係者へのコンタクトリスト作成
  — テスト実施ガイドシステム
- **監査／テスト結果報告**
  — 監査／テスト結果登録・統合・集計システム
  — e-文書管理システム、文書管理システム

≪ITプロセス群4≫オペレーショナルシステム群

販売・生産・調達・経理・人事・資産管理など日常の業務システムで財務報告につながるITシステムすべてを含みます。この部分は既に述べた「2. IT業務処理統制におけるITソリューション」の主要な対象業務ですが、例示した典型的な内部統制フレームワークによる財務報告システムにおいて、内部統制の追加のITソリューションがありますので再度説明しています。

IT業務やそのほかの業務のアウトソーシングが一般的になりつつある現在は、委託先とのデータのやり取りや業務プロセスの同期化に伴うインターフェースの正確性・網羅性・正当性・維持継続性を十分に確保する必要があります。

≪ITプロセス群5≫ETL（Extract, Transform and Load）

オペレーショナルシステム群で生成された財務報告に関係するトランザクションを財務報告の各期に合わせて抜き出し（Extract）、必要であれば変換し（Transform）、データウェアハウス・データベースに入力（Load）するITプロセス群です。

連結会社が多数ある場合は、会計費目の正規化に従ってトランザクションのスクリーニングやクレンジングが必要である場合が多くあります。また会計基準が変更になると、一部のトランザクションの会計費目を短時間で変換する必要も出てくるでしょう。

このITプロセス群では内部統制の要件を満たすために、柔軟で素早い変更に耐えられるシステムであるだけでなく、入出力データと処理において正確性・網羅性・正当性・維持継続性を十分に確保し、監査やテストが容易なように変更やコントロールを可視化しておく必要があります。

≪ITプロセス群6≫財務・投資 決定支援

財務報告のデータウェアハウス・データベースを使用してさまざまなシミュレーションを繰り返し、会議や稟議（りんぎ）を経て配当や新たな投資を決定します。

このITプロセス群は会議や個人の意思決定を支援するために、非定型な業務活動に対応できる十分な柔軟性を持つと同時に、データエラーや誤った判断が財務報告の正確性に大きく影響しますので、処理や判断の追跡が容易にできるようにしておく必要があります。

≪ITプロセス群8≫財務報告書、内部統制報告書作成

株主総会や役員会などを経て最終的な財務報告書を作成します。さらに、自社や連結会社および委託先の内部統制の有効性を評価し内部統制報告書を作成します。また内部統制を評価し、必要であれば緊急の対策実施を開始することもあります（委託先の内部統制の有効性の評価については57ページ「外部委託業務の内部統制」をご一読ください）。

≪ITプロセス群4、5、6、8のITソリューション≫

「2. IT業務処理統制におけるITソリューション」で既に述べたITソリューションに加えて、以下のようなITソリューションが考えられます。

- **財務報告のためのデータ抽出／正規化、データウェアハウス整備**

— 連結会社のデータ収集
— Ledgerデータの抽出・正規化
— データウェアハウス機能

- **外部との財務関連データの交換・報告**
  — XBRLに基づく財務データの交換・蓄積
  — 文書セキュリティーシステム
- **財務・投資・株式に関する意思決定支援**
  — ワークフローと意思決定支援システム
  — 財務／投資シミュレーター
  — 会議記録システム
- **エグゼクティブダッシュボード**
  — 内部統制情報を含むMIS
  （Management Information Systems）
- **内部統制報告書の作成**
  — 内部統制報告書データ／報告書登録・統合・集計システム
  — 内部統制スコアカード作成システム

❺ 内部統制におけるエビデンスログ機能

内部統制が正しく運用され有効であることを評価するために、業務プロセスの実施エビデンス（監査証跡など）をログ機能で記録し解析できるようにしておく必要があります。テストや内部監査ではこれらエビデンスを使用して業務プロセスの正確性・網羅性・正当性・維持継続性が保たれていることを確認することになります。

エビデンスには**図4**に示すように、3種類（3層）のものがあり、それぞれ業務プロセスの実施に関連してお互いが関連付けられます。

《第1層》業務プロセスの実施記録

手作業やデスクワークであるか、IT業務処理であるかは問わず、業務プロセスの実施プロセスインスタンスが記録されます。記録単位は通常業務プロセス実施の条件（実施者・実施日付・業務内容など）が同じ作業ロット単位で行われます。開始／終了時間、処理トランザクション番号群、実施者、次の業務プロセス番号などが記録されます。作業報告や作業記録などに相当します。

《第2層》トランザクションの正式記録

ITアプリケーションの実行により出力記録されるトランザクションデータです。最終的なデータ記録はLedgerデータを形成し、財務報告の基になります。正確性・網羅性・正当性・維持継続性が最も必要とされるデータ記録です。

《第3層》トランザクション処理の実施痕跡

ITアプリケーションの実施に伴うITシステムのユーザー識別、セッション開始／終了時間、セキュリティーバイオレーション事象、使用入出力ファイル、Eメールなどが記録されます。場合によっては膨大な容量が必要になります。

一つの統合されたログファイルに上記のすべてのエビデンスを記録することも考えられますが、検索性が悪いこと、さらに情報セキュリティーを考えると別々に保管する方が望ましいといえます。手作業やデスクワーク、ITにおける自動処理にかかわらず、一つのトランザクションについて3層のエビデンスがそろって初めてトランザクションの正確性・網羅性・正当性・維持継続性の証明ができることになります。以下に3層のエビデンス構造の利点を挙げます。

- 一つの業務プロセスの実施から三つの

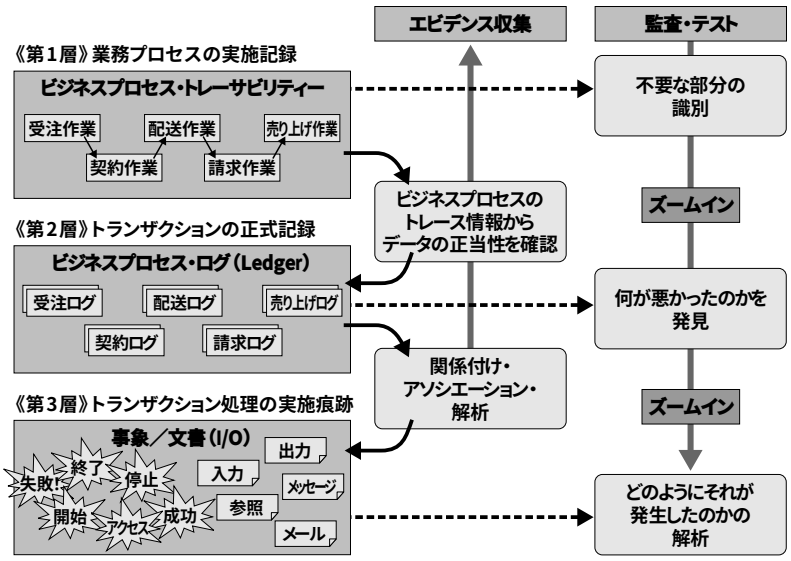

図4.　3層のエビデンス

ログが出力され、別々に管理されるので、データタンパリングに強い。

- 異なる視点からの複数ログであり、使用目的により使い分けが簡単である。また「業務プロセスの実施記録」や「トランザクションの正式記録」をテストし、ほかのログ情報でその妥当性を検証できる。
- 業務プロセスはすべてがIT化されているわけではないので、場合によっては「トランザクションの正式記録」が抜け落ちる事故が発生する場合や、「トランザクション処理実施記録」がない場合もある。「業務プロセスの実施記録」により事故を未然に防いだり、後で検証したりすることができる。
- 「業務プロセスの実施記録」をビジネスプロセス・インスタンスのネットワーク体系として、トレーサビリティーデータ形式で記録すると、個々のトランザクションや財務報告の勘定科目からバックトラックしたり、フォワードスキャンしたりして、検索性をより大きく向上することができる。

また、「業務プロセスの実施記録」を上手に利用すると次節で説明するさまざまな応用が可能になり、内部統制の価値を高めることができます。

❻ ビジネスプロセスの定義とその応用

内部統制を求める各種法律およびそれに伴うガイドやフレームワークは例外なく業務プロセスの記述とリスクの識別、それらに対応するコントロールの設定と記述を求めています（「3. 内部統制の実現ステップ」の《ステップ2、3》に相当します）。

最低限のIT投資で、文書化ツールだけを使用し、文書化と作成された文書による経営者・従業員の教育・訓練、それに従った手作業の業務プロセス実施およびテストや監査も可能です。しかし、従業員数・拠点数・業務プロセス数が多い大企業は大きな作業負荷を背負うことになります。また業務プロセスは経営判断や企業合併、コンプライアンス要件によって常時変更されるのが当たり前となっています。ITの機能を利用して内部統制の有効性・効率性・維持継続性を飛躍的に向上しておく必要があります。さらに内部統制フレームワークには重要な目的として「業務の有効性と効率性」が挙げられており、それをどのように実現するかが問われています。

図5、6に、ビジネスプロセスの定義情報をIT要件に従って設計し、応用システム群で使用可能にすることにより、内部統制システムの価値を飛躍的に向上する可能性を示しています。

具体的な実現の方法については「内部統制のため

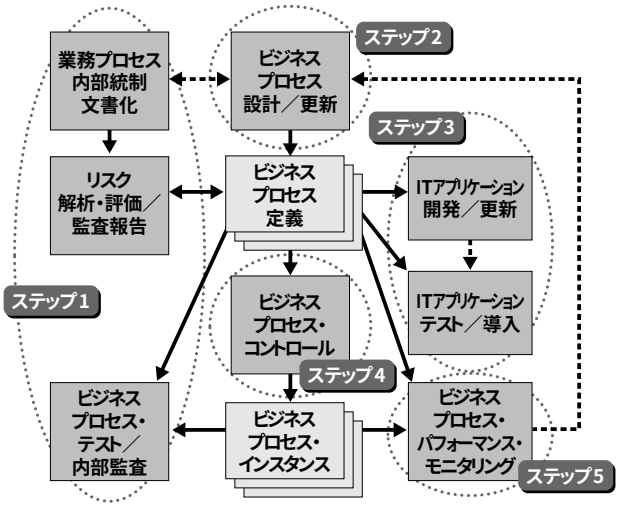

図5. ビジネスプロセス定義の応用

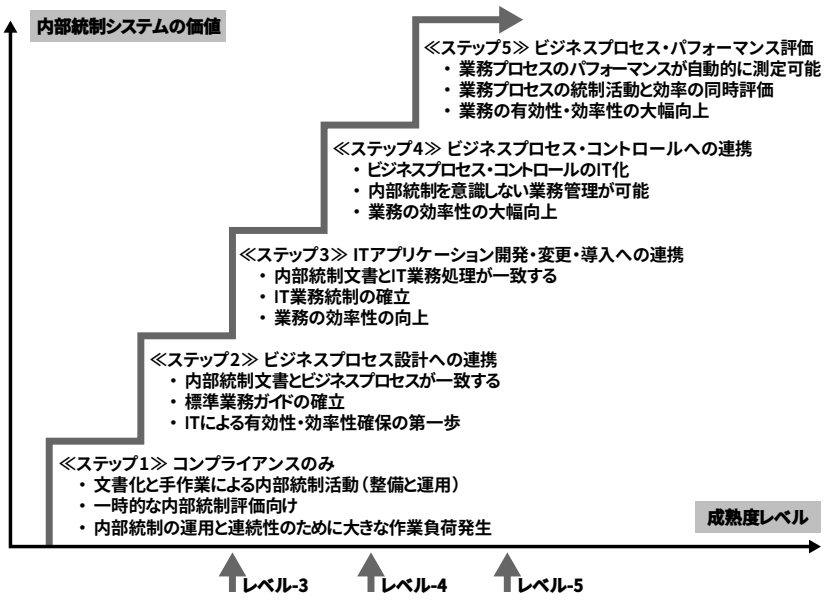

図6. 内部統制システムの価値向上ステップ

のビジネスプロセス・モデリング」（50ページ）を参照してください。以下にそのステップとその有効性・効率性の意味を説明します。

≪ステップ1≫コンプライアンスのみ

企業改革法などの法律の解釈で求められる業務プロセスの最低限の文書化だけを行います。業務プロセスの有効性や効率性に寄与することはあまりありません。作成された文書類は監査を終わると参照されることは少ないです。内部統制の評価のたびに作成作業を繰り返すことも珍しくありません。また実際の業務は作成された文書類とは無関係に実施される危険性もあります。

≪ステップ2≫ビジネスプロセス設計への連携

実際に実施される業務処理において文書化作業のアウトプットが参照できるように業務プロセス設計作業をIT化します。またそのアウトプットは社員の業務教育にも使用できます。

≪ステップ3≫ITアプリケーション開発・変更・導入への連携

業務プロセスの文書化作業のアウトプットがそのまま対応するITアプリケーションの外部仕様書の一部となるようにIT化します。それ自体がITアプリケーション開発作業負荷を軽減するばかりでなく、業務プロセスの文書化における追加・変更・削除において企業全体のITアプリケーション群にどのように影響下するかを知ることができます。

≪ステップ4≫ビジネスプロセス・コントロールへの連携

業務プロセスの文書化のアウトプットがそのまま実際の業務処理のワークフローやスケジューリングの入力パラメーターとなるようにIT化します。内部統制のための文書化作業はそのまま企業の業務処理の設計とまったく同じことになります。

≪ステップ5≫ビジネスプロセス・パフォーマンス評価

ビジネスプロセス・コントロールの実行システムは個別の業務処理の記録を行います。この記録は個々の業務処理のパフォーマンスを記録して、それを集計し解析することにより、企業のビジネスプロセスのボトルネックを識別し、業務プロセスの改善を常時行うことができるようになります。

❼ おわりに

内部統制は一時的なコンプライアンスのための文書化作業ではありません。内部統制の目的（業務の有効性・効率性、財務報告信頼性、関連法令の準拠性、資産の保全）を達成するための永続的な努力です。ITを最大限に利用して内部統制の各要素（統制環境、リスク評価、統制活動、情報と伝達、モニタリング）の有効性・効率性・維持継続性を向上していくのは企業として自然な行為といえます。また同時にITシステムの脆弱（ぜいじゃく）性を評価してそれに対応していかなければなりません。

ここで述べたITソリューションセットは、今考えられる最大限のIT機能の可能性を示しています。もちろんすべてを早急に実現する必要があるわけではありませんし、中には実現が難しい内容も含まれています。すべての内部統制のフレームワークや実現方法がそうであるように、それを支えるITシステムも一つのソリューションセットがすべての企業に適合するとは限りません。所属する企業の経営環境に従って読者が内部統制システムの構築・運用を計画する上で、本稿を参考として取捨選択あるいは不足機能追加のベースセットとして使用していただければ幸いです。

[参考文献]

[1] COSO（The Committee of Sponsoring Organizations of the Treadway Commission）, http:/www.coso.org/

[2] IIA（The Institute of Internal Auditors）, "Applying COSO's Enterprise Risk Management - Integrated Framework", IIA, 2004

[3] PCAOB（Public Company Accounting Oversight Board）, Auditing Standard Number -2 "An Audit of Internal Control over Financial Reporting Performed in Conjunction with An Audit of Financial Statements", PCAOB, 2004

[4] 金融庁企業会計審議会内部統制部会、財務報告に係る内部統制の評価及び監査の基準のありかたについて、金融庁企業会計審議会内部統制部会、2005

[5] ITGI（IT Governance Institute）, "COBIT4.0", ITGI, 2005

[6] ITGI, "IT Control Objectives For Sarbanes -Oxley", ITGI, 2004

[7] ITGI/OGC（The Office of Government Commerce）, "Aligning COBIT, ITIL and ISO 17799 for Business Benefit, ITGI/OGC, 2005

[8] あずさ監査法人経営改革支援本部、なるほど図解内部統制のしくみ、中央経済社、2006

[9] 中央青山監査法人、システム監査と内部統制の実務、税務経理協会、2006

[10] 青山奈々子、会社員のための内部統制入門、第一法規、2005

内部統制のためのビジネスプロセス・モデリング

― ITアプリケーション統制を支えるビジネスプロセス・マネジメント技術 ―

日本アイ・ビー・エム株式会社
東京基礎研究所
IBMディスティングイッシュト・エンジニア
IBMアカデミー会員
榊原 彰 Akira Sakakibara

［プロフィール］
1986年、日本IBM入社。以来、SEとして銀行・新聞社・部品メーカー・自動車メーカーなど、多数のお客様のプロジェクトに参画。
専門はアーキテクチャー設計技術。最近は非機能要求のフォーマルな取り込み、およびアーキテクチャーの単純化に興味を持つ。

内部統制IT（情報技術）ソリューションの根幹を成す技術の一つがビジネスプロセス・モデリングです。業務処理統制においてビジネスプロセスは（1）設計・定義され、（2）監視され、（3）テストされる対象として取り扱われなければなりません。これは、内部統制に関する対応が話題になる以前から、ITソリューションとしてビジネスプロセスの「可視化」「自動化」「モニタリング」といったキーワードで語られてきた取り組みがベースとなります。

ビジネスプロセスの文書化のみがクローズアップされがちなIT業務統制において、これらのキーワードに代表される総合的なビジネスプロセス・マネジメントの考え方を取り入れることこそが、本来論としての内部統制を推進する原動力となります。本稿ではこうしたビジネスプロセスに関する技術の概要を踏まえ、その重要性を簡単にご説明します。

1 ビジネスプロセスの可視化

前述の通り、日本版SOX法の導入により財務報告にかかわるビジネスプロセスは文書化を求められるようになります。ビジネスプロセスの文書化とは、すなわちビジネスプロセスを可視化するということです。可視化によってビジネスプロセスの透明性を高めることが必要なのです。ただし、ビジネスプロセスの文書化といっても、その記述方法にはさまざまな方法が考えられます。そのような中、可視化するという観点から非常に有効な手段が、ビジネスプロセスのモデリングです。

特に、内部統制においてビジネスプロセス・モデリングは、As-Isのプロセスを文書化するだけではなく、識別されたリスク項目や必要ログを取得することを前提とした内部統制活動を支えるためのTo-Beプロセスの「設計」を可能とするものです。

ビジネスプロセスのモデリングには、通常なんらかのビジネスプロセス表記が可能なダイアグラム（図）を用います。伝統的な業務フロー図、あるいはDFD（Data Flow Diagram：データフロー図）、IDEF3（Integrated Definition Methods 3）表記やUML（Unified Modeling Language：統一モデリング言語）など、システム設計のパラダイムをビジネスプロセスの表記に持ち込んできたもの、最近ではBPMN（Business Process Modeling Notation）など、ビジネスプロセス・モデリングに特化して考案された表記を用いたプロセスモデリングが行われています。

こうしたモデリングを行う際に重要なことは、表記自体にセマンティクス（意味）が定義されていることです。プロセスを文書化するという側面だけをとらえてみれば、確かに手っ取り早く、「このプロセスはこんな感じ、こっちのプロセスはそんな感じ」という流れを感覚的に記述するだけでよいのかもしれません。しかし、プロセスを「設計する」という観点からはもう少し厳密性が必要になります。

内部統制対応は、決して後ろ向きの仕事ではありません。業務統制をテコにして業務を支えるITソリューション自体をよりアグレッシブなものへと変革させる絶好の機会なのです。きちんとしたビジネスプロセス・モデリング

を通してTo-Beプロセスを設計することは、まさにその第一歩といえるでしょう。

2 ビジネスオペレーション

IBMでは、WBM（WebSphere® Business Modeler）というビジネスオペレーション・モデリング・ツールやWebSphere Business Monitorや Tivoli® Business Systems Managerといったプロセスモニタリング、プロセスマネジメント機能を持つ製品を提供しています。そしてそれらは、UMLのセマンティクスを拡張しビジネスオペレーションのモデリングを可能にする共通の定義を内在しています。ビジネスオペレーションのモデリングと表現したのは、必ずしもビジネスプロセスだけをモデル化するわけではなく、それに付随するさまざまな要素をモデル化することが必要であることからです。具体的には以下のような要素が含まれます。

- **ビジネスプロセス・モデリングの要素**
  - プロセス
  - リソース
  - 情報
  - 組織
  - ビジネスルール
  - オーソライゼーション
- **インターフェースの要素**
  - サービス
  - ユーザーインターフェース
- **シミュレーション（設計内容のシミュレーション）**
- **オブザーベーション（監視と監視対象の設定）**

これらが有機的に結び付くよう機能させることによってビジネス駆動のITライフサイクルを実現できます（**図1**）。具体的には、「可視化（モデリング）→自動化（フロー制御の生成とオブザーベーション設定）→モニタリング→フィードバック」という図式を、ビジネス要求を反映したITを構築し運用するプロセスに重ね合わせることをいいます。

3 内部統制におけるビジネスプロセス・モデリングの重要性

ビジネス駆動のITライフサイクル実現のみならず、各業務統制という点でもビジネスプロセス・モデリングは、重要な活動だといえるでしょう。なぜならば、コントロールポイントの識別や必要な対応の定義はビジネスプロセスを可視化しなければ適正な判断が困難だからです。従ってビジネスプロセス・モデリングは、ガバナンス上、業務設計・IT運用設計・統制対応のすべての活動のスタート地点として位置付けられるものと認識することが重要です（**図2**）。

また、前述した自動化・モニタリングといった技術により、モデルと実際のビジネスプロセスが直結する環境をつくり出すことができます。

このようにビジネスプロセス・モデリングは、単なる可視化の域を超え、ガバナンスに深く根ざした企業IT関連活動の根幹を成す活動です。ビジネスプロセス・モデリングを単なる文書化作業として終わらせずに、ぜひ、ビジネスオペレーション全体をカバーするITソリューション中での重要活動として昇華するよう検討していただきたいと思います。

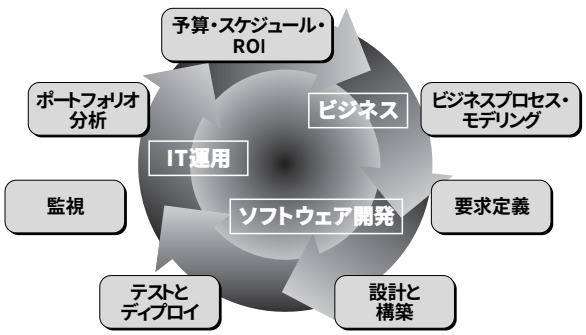

図1. ビジネス駆動のITライフサイクル

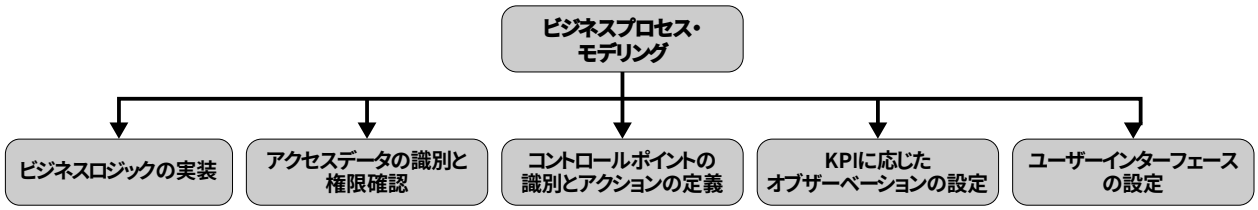

図2. ビジネスプロセス・モデリングから継続する活動