



ERPにおけるシステムコントロールの導入と管理

米国の多くの企業は、サーベンス・オクスレー法(以下、SOX法)の404条への遵守を通じて多くのことを学びました。SOX法対応の経験を積むことにより、コントロールの文書化やテスト方法に関して企業はより効率的で効果的な方法を採用するようになってきています。特に大企業はSAPやOracleなどのERPシステムに巨額投資しており、この複雑なシステム機能の中に、既存のマニュアルコントロールを自動化できる可能性を模索しています。

既存のマニュアルコントロールを自動化するには大変な労力が必要ですが、それを実現しようとした企業はマニュアルコントロールよりもシステムコントロールの方が本質的に、より堅実に信頼できるコントロールであると認識しています。なぜなら、システムコントロールは休むことを知りません。更に、SOX法対応に必要な統制を日々の業務プロセスの中に組み込む事で、時間、工数、そしてSOX法対応に必要なコストを削減することができます。

SOX法競争

SOX法は新しい時代の到来を告げ、企業にはしっかりした内部統制の構造が構築されている事を証明するよう、高い水準が求められています。SOX法対応を仮に競争に例えた場合、初期段階で企業が行った対応を基に、いくつかのトレンドが見えてきました。

初年度は指針がころころと変わり、SOX法のニュアンスの多くが理解されませんでした。企業や外部監査人は多くの場合において、必要以上にほとんどのコントロールをキーコントロールと定義しました。これらのコントロールを管理、整備、そしてテストするのにどれだけのコストが掛かるのか過小評価していたのです。SOX法対応においては、重要な不備が最低1件見つかれば、重大な欠陥が特定されるのは珍しくありませんでした。この文書化の負担の下、疲れ果てた企業は這い蹲りながら、どうにかゴールにたどり着いたのです。

翌年はSOX法の要件やガイダンスが企業や監査法人に理解

されるようになり、SOX法対応にも改善が見られました。これにより、多くの企業はアプローチやスコープを改善することが可能になりました。SOX法対応のための人事配置を行い、更にテストングに対処するため内部監査部を増員するケースも見られました。キーではないコントロールや余分なコントロールは、より強固なキーコントロールに置き換えられました。企業がシステムコントロールの導入を考え始めた頃、世間一般ではまだマニュアルコントロールへの強い信頼がありました。ほとんどの企業はSOX法プロジェクトを立ち上げ、既存のコントロールの文書化とテストングを行う事に焦点を当てていました。企業は疲れ果てていましたが、なんとかゴールまで歩いてたどり着く事ができました。

SOX法対応3年目になり、企業は今まで以上にSOX法対応における効率と効果を期待するようになりました。監査委員会や上層部経営者はより早く、低コストで結果を得たいと思っていましたし、外部監査人にも彼らなりの期待するレベルがあり、それは発展し続けました。外部監査人は過去の不備が改善され、不正の発生可能性に対してなお一層焦点を当ててほしいと考えていました。また更に包括的な職務分掌のテストが実施され、マニュアルの発見的コントロールに替わって予防的コントロールが整備され、コントロールのモニタリングが実施される事を期待していました。

システムコントロール、特に企業のERPシステムに組み込まれたシステムコントロールは、上記のような期待に応える事のできる対応策だという認識が広まりました。ERPに組み込まれたシステムコントロールを理解し活用する事が、今後のSOX法知識の新たな領域として浮上してきたのです。ERPにおけるシステムコントロールによって、今まで整備・管理・テストなどに利用していた成果物は、品質、コスト、効率性、コンプライアンスの観点でより改善された評価をできるようになります。更にコントロールについての課題は根本的な原因を特定でき、すぐに対処することも可能になるでしょう。SOX法が企業におけるコンプライアンスとリスク管理の一部の要素にしか過ぎないという位置づけになってくれば、企業は全速力でゴールできるようになり、競争に参加していた事すら忘れてしまうでしょう。

大いなる救済

ERP アプリケーションのセキュリティ周りに関して、監査人に重大な欠陥と評価されたある企業で、システムコントロールを導入する事によって付加価値を与えることに成功した事例があります。重大な欠陥との評価は些細な事では済まされません。なぜなら、欠陥となったコントロールは公に公表されてしまうからです。このような事実の公表は、企業イメージの低下というリスクだけではなく、企業の株価や株主の企業に対する認識にまで連鎖反応してしまいます。

システムコントロールへの移行を経験した事がある外部チームに支えられ、この企業は SAP R/3 アプリケーションのセキュリティ部分を再設計し、更に継続的にセキュリティの完全性を管理しモニタリングする事ができるようツールの導入も行いました。再設計プロジェクトが終わる頃には、セキュリティ基盤が構築されました。この時点で全てのセキュリティは職務分掌の観点から適切に設定されている状態、言い換えれば適切な軽減コントロールが特定されている状態になったのです。強固なセキュリティ基盤が構築されたことによって、企業の内部監査チームや外部監査人は仕事がやりやすくなりました。職務分掌、アクセス制限やセキュリティ基盤への変更を検知した場合、レポートが直ちに出力されるからです。

監査人にとって、このような状況はこれまでの仕事のやり方を大きく変更する事を余儀なくされる状態となりました。今までのようにサンプリングや取引データの詳細確認のために膨大な時間を費やしていたのに代わり、今では企業に継続的にセキュリティをモニタリングするプロセスが存在するかどうかを確認するために時間を割いているのです。その影響により、監査人は「企業はツールを使用してセキュリティやセキュリティ基盤の変更をモニタリングしており、強固なセキュリティ体制が整っている。ツールの基となっている業務ルールは正しいため、適切なアプリケーションコントロールが設定されていると確信している」と言っています。

自動化されたプロセスを監査するのに有する時間は、マニュアルコントロールをテストする方法で同じ結果を導き出そうとする場合に比べて 60 ~ 75% も時間を短縮する事ができます。例えばあるコントロールを確認するためにマニュアルコントロールのサンプルを 60 件抽出する必要があった場合、自動化されたシステムであればサンプル数は 1 件で済みます。企業は 59 件のサンプルに対するテストに掛かる時間と監査コ

ストを節約することができます。これらの節約は内部監査に掛かるコストにも適応されます。

更に、ERP ソフトウェアが関連している業務プロセスに対し、新しいシステムコントロールを適応する事も可能となります。例えば、SAP などのシステムを利用した業務プロセスにおいて定義できる数々の許容範囲、項目の妥当性チェック、ワークフロー、パラメータ設定はコントロールとして認識できる見込みがあります。

例えば、仕入先のデータファイルを 1 件 1 件見ながら重複が存在するか確認するより、システムに組み込まれた重複した仕入先を登録する事ができないような仕組みを利用することができます。このコントロールをテストするには、既に存在する仕入先を登録しエラーメッセージが表示される事を確認すればよいのです。つまり、データをテストするのではなく実際のロジックをテストする事になるのです。

システムコントロールを優先させる

システムコントロールを導入するためには、まず企業のキーコントロールとリスク領域を特定するところから始まります。例えば、企業はどの領域においてなら、コントロールが機能しなかったとしてもそのリスクを負うことができるか決める必要があります。また、どのマニュアルコントロールにおいてエラーが発生する傾向にあるか、運用にコストがかかるコントロールはどれか、反復的であり判断や解釈を必要としないマニュアルコントロールにはどの様なものがあるのかについても判別します。

既存の ERP システム内のコントロールを精査すると、初期導入時に設定されなかったコントロールが多々発見されます。多くの場合、これらのコントロールはユーザや既存の業務プロセスに影響を与えることなく設定する事ができます。また、アセスメントを実施する事によって、誰も把握していなかったコントロールが既に設定されている事を発見するケースもあります。

自動評価ツールなどを使用し、企業は SAP や Oracle などのシステムにて、認識されていない自動化が可能なコントロールを特定する事ができます。我々の経験では、SAP R/3 のコアモジュールでは約 500 の発見的および予防的なコントロールが存在しています。コントロールを自動化させる際に覚えておく必要があるのは、関係者間の協力なくしてはこれを達成することはありえないということです。コントロールを評価し、変

更できる余地がどこにあるのか理解し、それを設定し文書化するには様々なスキルが必要とされ、これら全てのスキルをたった一人の従業員に見出そうとしても困難です。システムコントロールを導入するには企業の情報システム、業務プロセス、更にSOX法コントロールや文書化に関する知識が必要となります。該当する知識に精通した関係者がクロス・ファンクショナルなチームとして集まり、この困難な挑戦に対して共に同じゴールに向かって行かなくてはなりません。更に困難なのは、大手ソフトウェアベンダーよりERP導入時に提供された文書は多くの場合、設定可能ではあるけれども、設定しなかったコントロール(パラメータ設定)については記載していないところです。

システムコントロールの実現と管理

コントロールを自動化するために大量のコントロールを確認する作業は、大抵一度限りの努力です。一度その壁を越えてしまえば、その後は改善されたコントロール設定が時間と共に劣化していかないよう、継続的に運営と管理していけば良いのです。

システムコントロールを継続的に管理するための重要なポイントは、強固な変更管理プロセスを設定する事にあります。システムコントロールに信頼を置くためには、システムコントロー

ルを導入する前にシステム変更に伴うインパクトを理解する必要があります。更に、システムコントロールが故意に変更される(解除される)リスクを防止するために強固な変更管理プロセスが必要になります。

もう一つの重要なポイントとして、新規コントロールやコントロールの変更を認識することです。めまぐるしく変わる昨今のビジネス環境により、多くの企業は商品を開発し、合併や組織変更、システムのアップグレードやその他現状にマイナス影響を与えるようなイベントに対応するために継続的にプロジェクトを立ち上げています。コアとなる業務プロセスやシステムに対し影響を与えるプロジェクトにおいては、既に設定されたコントロール構造を考慮し、どの様な影響を与える可能性があるのかを分析してプロジェクトを遂行する必要があります。自動化するコントロールを特定したらすぐに対応できるよう、適切な時間と人員を割当てておく事が大切です。

効率的で効果的なSOX法対応のために努力を続けている多くの企業にとって、ERPのシステムコントロールを導入する事は重要なテコ入れを行うポイントとして考慮されるべきです。自動化されたERPのコントロール群は、企業に対して定量的な事業価値を実現させる重要なプロセスとシステムのリエンジニアリングの可能性を示しているのです。

株式会社プロティビティ ジャパン

東京オフィス：〒100-0004 東京都千代田区大手町1-1-3 大手センタービル Tel.03-5219-6600[代表] Fax.03-3218-5533

大阪オフィス：〒541-0056 大阪府大阪市中央区久太郎町4-1-3 大阪センタービル 13F Tel.06-6282-0710[代表] Fax.06-6282-0711

お問い合わせメールアドレス：pj-mktg@protiviti.jp

ホームページ：http://www.protiviti.jp/

Protiviti, Protivitiロゴは、Protiviti Inc.の米国ならびにその他の国における商標または登録商標です。その他の記載されている会社名・製品名は各社の登録商標です。