protiviti®
Independent Risk Consulting

ERPの機能を活用した内部統制への対応

米国の多くの企業において、サーベンス・オックスレー法（以下、SOX）対応の 1 年目と継続的な対応が非常に大きな負担となってしまったことは周知の通りです。SOX1 年目における内部統制の文書化と整備状況評価、運用状況評価に要した人件費をはじめとする一連のコストは、予算を大きくオーバーしてしまいました。1 年目の対応においては、多くの企業においてより工数のかかる人手によって実施される発見的なコントロールがより広い範囲において認識され、運用されることとなりました。これに対して、経営者や監査委員会は、SOX 対応プロジェクトのリーダーに対して、SOX において要請されている内部統制への対応をより迅速に進めるよう要求し、それと同時に関連するコストの削減を求めています。

幸いなことに、多くの企業では既に何らかの ERP を導入しており、これを有効活用することによって、SOX 対応を効率的に行うことが期待されています。例えば、コントロールを自動的にモニタリングできるように ERP を適切に設定すれば、企業はマニュアルコントロールへの依存度を軽減させ、人件費等のコスト削減することができます。この結果、企業は SOX 対応をプロジェクトによる管理ではなく、継続的に対応が可能なプロセスにおける管理に移行させることができます。これが経営者や監査委員会の要求に応えるためのキーポイントです。

SOX 対応の実施は、ERP の機能を最大限に活用するための唯一の機会と言うわけではありません。しかしながら、成長過程にある多くの企業は数多くの業務プロセスをサポートするために ERP を選択しています。従って、もし子会社の業務プロセスや利用するシステムが ERP に連携され、財務報告や情報開示の元となる情報が ERP に蓄積されるのであれば、ERP は内部統制への対応をプロジェクトによる管理からプロセスにおける管理へとシフトさせる基盤となります。

ERP は SOX 対応のためのプロジェクトを、継続的に実施可能なプロセスにおける管理に移行させるために必要な多くの機能を有しています。しかし残念なことに、これらの多くの機能は利用されていないか、もしくは十分に活用されていません。

これに対する理由は様々です。例えばソフトウェアベンダーや ERP 導入に携わるコンサルティング会社、そして導入企業はできるだけ早くシステムを稼動させることを優先することを求められます。この結果、ERP におけるパラメータ設定やコントロールの不備を未然に防ぐためのセキュリティ対策に十分な時間をかけることができないのです。

また、多くの企業は SOX 対応の 1 年目にシステムコントロールの導入を回避するようなアプローチを選択しています。効果的なテスティングを定量化するスキルや方針が欠落しているため、企業はシステムコントロールの効率性をよく理解せずに、より工数のかかるマニュアルコントロールに依存してしまうのです。特に情報システム部門が主体的な管理を行っていないような外部に委託しているシステムや業務部門で管理されているシステムでは、システムから出力される情報の妥当性を事後的に確認していることを証明するために、マニュアルコントロールを新たに設けるか、もしくは強化するような対応をとっていました。

システムコントロールの積極的な活用

もし SOX 対応を通じて統制環境を改善して企業価値を高めたいと考えているのであれば、まずは考え方そのものを変えていく必要があります。過剰にマニュアルコントロールを設けるのではなく、システムコントロールに可能な限り依拠するというアプローチにシフトしなければなりません。マニュアルコントロールをどんなに慎重に運用しても、適切に設定された ERP によるシステムコントロールの信頼性に勝ることはありません。

ある研究結果によれば、システムコントロールの運用状況評価はマニュアルコントロールの運用状況評価に比べて 75% も

の時間を削減できることが示されています。ERP におけるシステムコントロールの運用状況評価は、場合によってパラメータの設定画面を確認し、そのスクリーンショットを証跡として入手するという単純な手法で済む場合があります。この際に、唯一気をつけなければいけないことは、そのパラメータ設定が正しいことを確認することです。システムコントロールに依拠することによって、コントロールの信頼性を最大化し、しかもその証跡取得と保存のコストを最小化することができるのです。このように、システムコントロールはマニュアルコントロールに比べてはるかに効率的であるだけでなく、より信頼性の高い結果を提供することが可能なのです。

さらにシステムコントロールは、外部監査人がコントロールの運用状況評価に費やす時間をも削減することができます。通常、外部監査人は、被監査企業のテスト手法と同様の手法を用いて運用状況評価を行います。この結果、システムコントロールであれば、企業と外部監査人の双方が効率的な運用状況評価の手法に基づいて、作業時間を大幅に削減することができるのです。

しかしながら、これは言うのは簡単ですが行うのは容易ではありません。システムは時がたつにつれますます複雑化しており、システムの機能、業務プロセス、リスクとコントロールを十分に理解することは困難となっています。また多くの企業において、システム導入に携わった担当者がリスクとコントロールをよく理解していることもまずありません。業務側の担当者がシステムを良く理解し、コントロールがどのタイミングで必要となるのか十分に認識していることも稀です。一般的にシステムが一度実装されたら後戻りすることは許されません。開発期間と予算が限られている中で、リスクとコントロールを特定しシステムを全体的に最適化することはほとんど不可能となっているのです。

職務分掌もまた、多くの企業で問題になっています。SOX 対応の 1 年目では、企業は影響度の高いリスク領域を可能な限り網羅するという目標の達成に注力をしていました。2 年目では、多くの企業がより多くのコントロールをシステム化し、運用状況評価におけるテスト手法を最適化しようとしてきました。コントロールが安定的に運用される 3 年目では外部監査人は評価の対象範囲を広げ、既存コントロールはあえてテストせずに職務分掌のコントロールに焦点を絞っています。実際のところ、職務分掌の不備を重大な欠陥と見なすという外部監査人による指摘は増加しています。

職務分掌に関しては、実は多くの企業に誤解があります。企業は ERP において各担当者の役割をベースとして権限設定を実施しているため、各役割の中、そして役割をまたいだ職務分掌への抵触は必ずしも明示的にはなりません。そして、このような職務分掌への抵触を解決するためには、セキュリティに関するERPの機能や制限について詳細な知識が必要となるのです。

また、セキュリティに関しては、いかに継続的にユーザを維持管理していくかについても課題となっています。通常このようなユーザのアクセス権の追加、変更、削除をサポートするプロセスは非効率的な人手による管理が行われています。

職務分掌の課題を解決するツール

企業が職務分掌の課題を解決するためのひとつの方法は、より詳細なレベルにおけるアクセス権の付与の状況を分析することができるツールを効果的に使用することです。これらのツールは職務分掌への抵触を発見し、適切に権限が付与されているか、あるいは修正が必要かを評価することができます。このようなツールはまた、新規ユーザのアクセス権の付与に関わるワークフローについても管理が可能であり、自動的に職務分掌への抵触を分析し、システム管理者にメールで通知するような機能を有しています。この結果、職務分掌の問題に対する承認を文書によって管理することができます。

初めて職務分掌の現状分析を行うときは、想像以上に多くの職務分掌への抵触が発見されるため、その結果に非常に驚かされると思います。しかしながら、このような発見事項はいい意味での不備であると説明できます。なぜなら、それらの発見事項はシステムの職務権限の設定が企業の状況や戦略に合わせて適切に設定されていないことを示してくれるからです。このような不適切なアクセス権限の付与状況を改善すれば、企業は良好なセキュリティの基盤を作ることができます。

セキュリティの基盤を作ることは決して容易なことではありませんが、その努力を継続し、その基盤を絶えず管理していくことが必要です。例えばこのような管理のためには以下のような手法があります：

- ユーザの登録申請のプロセスに職務分掌のチェック機能を組み込む
- 職務分掌の抵触をモニタリングするために定期的なチェックを実施する
- 例外的な事項を許容するための追加承認に関するプロセスを設ける
- 課題の発生を警告するためのワークフローを持つツールを導入する

あるクライアントにおいては、新規で SAP を導入した際に外部監査人からシステムのセキュリティと職務分掌に関する課題

を年末までに解決するようにと指摘されたことがあります。このケースでは、独自の評価ツールにより既存のセキュリティ構造を検査し、典型的と思われる職務分掌への抵触を 4,000 個も発見しました。但し、分析の結果それらのおよそ半分は、本来は不必要な特権ユーザに関する権限が付与されてしまっていたことを原因としており、セキュリティに関するデザインを修正することによって改善することができました。

残りに関しては、業務側の責任者とともにあるべき職責をひとつひとつ付与していくことにより対応しました。それは例えば不必要なアクセス権を取り除くことであったり、継続的に抵触を引き起こすような役職を分離することであったり、抵触する職務を取り除くために同じ職責を再配分することであったり、役職を統合し業務コントロールの埋め合わせるというようなコントロールを設定することにより対応しました。

この事例においては初期段階で、モニタリングと管理維持のためのツールを導入しました。セキュリティに関わる各申請プロセスでは、新たな職務分掌への抵触を生まないかどうかをツールが自動的に検知するようになっています。そのクライアントでは前述のツールを用いて発見事項と追加承認の文書管理を一元的に行い、半期に一度の頻度で職務分掌に関する妥当性を検証し、四半期に一度の頻度でユーザに付与された権限の妥当性についてレビューを行っています。

以上のように、一旦セキュリティに関する設定と関連するアクセス権に関する設定が適切に実施され維持されたら、当該 ERP においては各種のレビューと承認プロセスにおける処理やレポートの証跡をたどることが可能となり、ERP の利点を最大限に生かすこと可能になります。

データ保管管理機能とプロセス管理機能の比較

多くのケースにおいて、承認やレビューはシステムの外側において手作業で行われています。これは、既存の業務プロセスとシステムで実施可能な機能のギャップを埋めることができないことを理由としています。数多くのマニュアルによるプロセスを持つ企業や、非常に多くの業務プロセスを持つような大企業では、そのような業務プロセスを ERP が想定する業務プロセスにあわせようとすると業務側は拒否反応を示します。このような企業では、ERP を業務プロセスのためのツールとしてではなく、単にデータの保管管理ツールとして利用することになってしまいます。

ERP がすべての業務プロセスを集約することは不可能ですが、それでも多くの業務プロセスを一元的に管理することは可能です。グローバルに共通するルールが構築されていたとしても、ERP は粒度の高い例外事項を許容可能なように設定することができます。例えば、あるシステムでは原則として仕入先からの購買処理に関して、3 つの帳票の突合（3-way matching）に関するグローバルルールを設定している場合でも、特定の仕入先については例外として設定を行うことが可能です。多くの企業は ERP のコントロールの機能に気付かずに、或いはコントロールの設定に必要な時間と予算が与えられていないために、コントロールの柔軟性を効果的に利用していません。

何か問題が発生したときに生成される監査ログ、発見事項報告書やアラートシステムは、問題のソースとして非常に有用です。さらに、ERP やツールはそれ自体で文書を作成する機能を豊富にもっており、コンプライアンスに関わる文書作成の作業を大幅に軽減することを可能にします。

ERP に関連するコントロールを効果的に活用するためのキーポイントは、広範囲にわたってさまざまなリスクをリアルタイムにモニタリングすることが可能な洗練されたアプローチを持つことです。より多くのプロセスがシステムに組み込まれれば、企業はより信頼性のある財務報告を作成することができます。企業にはリスクが発現してしまう前にこれを特定し、問題解決するために、リアルタイムのモニタリングを実施することができます。

システムコントロールのもうひとつの利点は、SOX 対応を超えたリスクマネジメントが可能になるということです。ERP に組み込まれた重要な業務プロセスは、個人情報保護、業務処理の異常検知等に関する様々なリスクを軽減することができるのです。

これはエンタープライズリスクマネジメント（ERM）に続く長い道です。ERM を一言で言えば、それはリアルタイムで管理できるリスクマネジメントです。ERP のプラットフォームを最大限に活用し、コントロールをリアルタイムでモニタリングしていくことこそ ERM へと続く道であると言えます。

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/