GUIDE TO THE SARBANES-OXLEY ACT: MANAGING APPLICATION RISKS AND CONTROLS

FREQUENTLY ASKED QUESTIONS

［サーベンス・オクスレー法］

米国企業改革法 アプリケーションリスクと コントロールの管理 質問集

米国プロティビティ質問集より

protiviti®
Independent Risk Consulting

Business Risk | Technology Risk | Internal Audit

Introduction

企業改革法（「SOX法」または「サーベンス･オクスレー法」）の施行に伴い、プロティビティは、当法律の条項（特に404条）に準拠するため、多彩な角度からよくある質問（frequently asked questions）をまとめ、複数の冊子を発行しています。「Guide to the Sarbanes-Oxley Act：Internal Control Requirements（米国企業改革法：内部統制の報告要件）第3版」「Guide to the Sarbanes-Oxley Act：IT Risks and Controls（米国企業改革法：ITリスクと統制）」を例とし、その他の発行物は米国プロティビティのホームページ（www.protiviti.com）からダウンロードが可能です。これらは内部統制の報告要件を満たすための手引き書です。

「Guide to the Sarbanes-Oxley Act：Managing Application Risks and Controls（米国企業改革法：アプリケーションリスクとコントロールの管理）」は、企業改革法コンプライアンス対応のための重要な手引きです。アプリケーションシステムに関連するリスクを効率よく特定する具体的な方法が記載されており、これまでの発行物をより具体化した内容となっております。本書に記載されている質問は、前述の報告要件に取り組んでいる弊社のクライアントやその他の企業とのディスカッションの中で取り上げられたものです。それぞれの回答と見解は、財務報告に係る内部統制の文書化・評価・改善、ならびに経営者の承認プロセスの改善について、数多くのクライアントを支援してきたプロティビティの豊富な経験に基づいています。また、本書はEnterprise Resource Planning（ERP）システムに関しての参考情報や例が記載されております。ここで記載されているコンセプトはERPシステムだけではなく、自社開発、クライアント／サーバという2層構造のシステム、マルチベンダシステム、業界特有のパッケージソフト､ウェブベースのツールなど全てのタイプのアプリケーションに対応しています。本書に記載されている内容の例としては、有効な職務分掌、効率的なアプリケーションのセキュリティ設定、及びマニュアル手続きの自動化によるアプリケーションコントロールへの変更などがあります。

米国では多くの会社が、企業改革法へのコンプライアンス対応2年目の終了を向かえ、経営者と監査委員会は、コンプライアンス対応のコストが低減することを期待しています。コストを低減するためには、毎年度同じシンプルな手法で企業改革法プロジェクトを実施するか、費用対効果が高いコンプライアンスのためのプロセスを業務に反映することが必要と考えられます。私たちはアプリケーションレベルにおける企業改革法コンプライアンスの有効性と効率性を改善することが多くの企業にとって重要だと考えております。また、アプリケーションの最適化と機能性の追及は、業務プロセス、コストの効率化を推進し、企業の統制環境強化、法令遵守に係るコスト低減につながると信じています。結果として、投資利益率（Return on investment：ROI）を上昇させることになります。

プロティビティのApplication Control & Effectiveness（ACE）ソリューションは､アプリケーションコントロールを積極的に導入することにより、継続的で、コスト効率のよい、付加価値の高いプロセスの構築を推進するために全力を注いでいます。ACEソリューションは、アプリケーションシステム、ITリスク、内部監査、内部統制、業務プロセスなど企業改革法コンプライアンス対応に関して多くの経験と実績を持っております。我々は、強固な内部統制環境の構築や費用対効果の高い業務プロセスの構築など、企業改革法対応へのコンサルティングで得た経験を十分に活用して、アプリケーションコントロール最適化のご支援をさせて頂いております。

本書は、企業改革法の報告要件を遵守するためのアプローチについて妥当性を法的視点から分析したものではありません。各社それぞれの状況に応じた特定の質問については、弁護士や適切なリスク・アドバイザーに助言を求める必要があります。また、各社のアプローチは、基準の変更、テクノロジーの進歩、アプリケーション機能によって影響を受けます。

本書の翻訳では、有識者、実務経験者が最善の注意を払っておりますが、表現が適切でない可能性もあります。お気付きの点がございましたら、原文（英文）<www.protiviti.com>をご参照いただけますようお願い致します。また、本書は、USにおけるサーベンス・オクスレー法に関するFAQです。

株式会社プロティビティ ジャパン
2006年10月

目次

Contents

Section1: 展望

企業改革法コンプライアンスにおける当初の二年間は、様々な理由により多くの企業がマニュアルコントロールに依拠する結果になっています。一年目における最大の理由としては、早い時期において実際にどのように対応すればよいかという手引きがなかったことと、対応時期の遵守のため「まずはやりとげなければ」というプレッシャーがあったためです。二年目においても一年目と同様で、多くの企業は、コントロールの改善計画を立てる時間がありませんでした。また、法令では、継続的なコンプライアンスのためのプロセスを要求していますが、それとは対照的に年間を通してコンプライアンスのためのプロジェクトは、数人の優秀な担当者の力に頼っているのが現実です。

必要なコントロールレベルを維持し継続するには、コントロールの整備・運用・文書化、マニュアルコントロールなどへの継続的な改善努力が重要です。ERPシステムの機能やそこに組込まれているコントロールを最大限利用することで、コンプライアンスのための「プロジェクト」から、コンプライアンスのための「プロセス」に移行し、ROIを上昇させることが可能となります。また、「法令遵守の負担」を「付加価値」に転換することができます。さらに、システムコントロールの導入による運用状況の評価は、マニュアルコントロールにおける膨大なテスティングの工数を削減する好機となります。このような改善を達成することで、リスクを大幅に低減することができ、統制環境を最適な状態へシフトすることが可能となります。下図は、統制環境の改善過程を表しています。

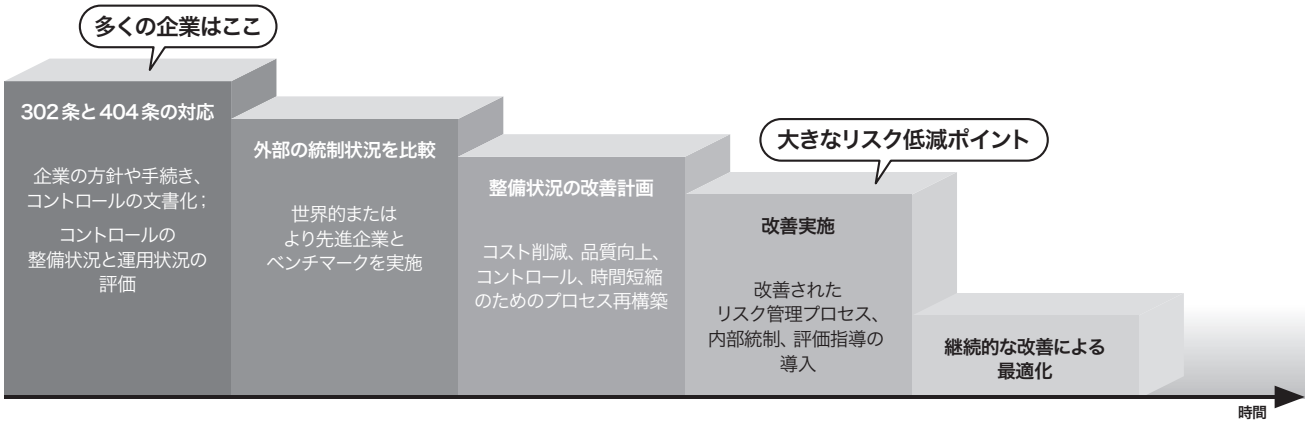
多くの企業は、今後一年から一年半を費やして、リスクマネジメントの仕組みを改善しながらコンプライアンスに係るコスト削減に対応していくことになると我々は考えています。内部統制の質と継続性を改善し、コンプライアンスのためのプロセスに付加価値を加え、費用対効果が高い「プロジェクトからプロセスへ」の移行には時間が必要となります。多くの企業が直面しているようなコンプライアンスのための高コスト環境よりも、より良い環境へのシフトが必要となります。財務報告に係るリスクを低減しながら、品質、時間、費用対効果を改善し「プロジェクトからプロセスへ」の移行を達成している企業は、市場においても強い競争力を確保しています。また、企業の強みとして、投資家の信用を勝ち取り、より多くの投資を得ています。しかしながら、この移行への対応が遅れている企業は、コンプライアンスのための高いコストを払い続け、財務報告に係るリスクが高まり、投資家の信用が得られないことにより投資が減少することになるでしょう。

Section2: 企業改革法を考慮したアプリケーションリスクとコントロールの考慮点

1. 企業改革法404条は企業の重要な業務アプリケーションへの信頼性についてどのように説明していますか?

企業改革法404条では、ERPシステムなどのアプリケーションを特定した説明は行っていませんが、SEC（Securities and Exchange Commision: 米国証券取引委員会）とPCAOB（Public Company Accounting Oversight Board: 公開会社会計監視委員会）は、企業改革法404条に係る基準や発行物において、このトピックを取り扱っています。

SECが2005年5月16日に発行した財務報告に係る内部統制に対する経営者の報告に関するスタッフ報告書によると、会計年度中において、新規アプリケーションまたは情報システムの導入により404条に記載されている経営者の義務が免除・延期されることはありません。企業は、新規導入された情報システムを利用して、信頼できる財務諸表を作成することを要求されていることについてもSECは強調しています。これに従うと、情報システムの統合または導入



プロジェクトへの取組において、404条対応のゴールは、現行の経営陣の責任によるものとなります。特に、SECは、「システム変更において、経営陣は内部統制の計画、設計、準備的な評価をシステムの導入またはアップグレードに先立って実行することができる」。さらに、「必ずしもすべてのテスティングが期末に実施されている必要はない。結果として、財務報告に係る内部統制の評価範囲から、新規IT システムとアップグレードが経営陣によって除外されることはないと考えるべきだ」と述べています。

2005年5月16日にPCAOBから発行されたQ&Aでは、自動化されたアプリケーションコントロールに対して要求される監査人が実施すべきテスティングのレベルと範囲が明確にされ、アプリケーションコントロールにおけるベンチマークコンセプトの増強が行われています。特に質問45で、PCAOBは以下のことを言及しています：

＊ 自動化されているアプリケーションコントロールは、通常人為的ミスが発生する対象ではなく、これらのコントロールは監査人が「ベンチマーク」または「ベースライン」を利用した評価も可能です。もしプログラム変更、プログラムへのアクセス、コンピュータ運用に対する全般統制が有効であり、継続したテスティングが実施されている場合で、前回実施されたテスティング以降、自動化されたアプリケーションコントロールに変更がない場合、監査人は自動化されたアプリケーションコントロールが有効であると判断できます。…コントロールが変更されていないことを証明するために監査人が入手すべき証拠の種類と範囲は、その企業のプログラム変更についてのコントロールの強さによって変わります。

最後に、PCAOBは、ベンチマーク戦略の適正を判断するために以下のように記載しています。

監査人は、ベンチマーク戦略を適用するかどうかの判断をするために、以下の事項を評価しなければなりません：

- アプリケーションコントロールがアプリケーション内の特定されたプログラムに適合しているかどうか。
- アプリケーションが安定しているか。（例：期間内にほとんど変更が行われていない。）
- すべてのプログラムの本番環境への移行完了が報告されており、それに依拠できるかどうか。（この情報はプログラムが変更されていないことを証明する証拠書類として使用できる。）

ベンチマーク計画を再策定するか否か判断する場合、監査人は以下の事項を評価します：

- アプリケーションコントロール、ソフトウェアの取得と維持、アクセスコントロール、コンピュータ運用を含むIT統制環境の有効性。
- コントロールを含むプログラムの変更による影響についての監査人の理解。
- 関連するその他のテスティングの性質とタイミング。
- ベンチマークしたアプリケーションコントロールに関連するエラーの結果。

まとめとして、SECやPCAOBが発行するレポートや説明において強調されている重要な点は、以下の通りです：

- システムコントロール（例：アプリケーションにおいて設定可能なコントロール）は、マニュアルコントロールに比べて信頼性が高い。
- アプリケーションで設定可能なコントロールはベースラインを策定することができ、また一度運用状況が有効的だと確認された場合、テスティングの焦点は、変更管理の手続きやセキュリティ管理を含めた全般統制と、ベースラインが策定された後に新たに導入されたコントロールとなります。
- アプリケーションで設定可能なコントロールについてベースラインが策定されると、同じコントロールのテスティングを毎年度実施する必要はありません。
- 重要な年次における有効性の評価は、変更管理の手続きやセキュリティ管理を含めた全般統制が有効に運用されている状況において、アプリケーションで設定可能なコントロールのテスティングによって効率的に実施できます。
- 重要な年次における有効性の評価は、マニュアルコントロールをアプリケーションコントロールに置き換える数に比例して、効率的に実施できます。
- 設計段階において、コントロールのデザインに関する積極的なテスティングや監査を実施するほうが、導入後の実施に比べて効果的かつ効率的となります。

SECやPCAOBのレポートや監査基準から明らかなように、システムコントロールは財務報告に係る有効な内部統制の中核的役割を担います。PCAOB監査基準第2号に記載されているように、財務報告に係る内部統制の評価においてシステムコントロールを有効活用することは重要です。

2. 企業はERP／アプリケーション導入に関して何を開示しなければならないのですか？

ERP導入に関連して10-K, 10-Qで開示しなければはらない情報量が多くなっています。多くの企業は、ERP導入が内部統制において重要な変更であり、またそれは企業改革法、SECの規則･規定によって定義されているもので、一般的にプロセスの再構築とそれに関連する統制環境の変化がERP導入時に発生すると認識しています。

多くの場合、ERP導入における本番移行の際、四半期ごとの企業の開示内容には、(a) 企業改革法404条に関する前回の報告 (b) 統制環境への影響を確認するための取り組みがERPの設計・導入に適切に考慮されているかといった点が含まれます。その目的のひとつは、財務報告に係る内部統制システムの維持・強化です。企業改革法は、企業がシステム導入を行う際に整備状況の有効性と運用状況の有効性を判断することを要求していません。しかし、経営者は、期末において整備状況の有効性と運用状況の有効性を判断することを求められています。それに加えて、企業は、内部統制に係る重要な改善を開示しなければなりません。詳しくは「Guide to the Sarbanes-Oxley Act：Internal Control Requirements（米国企業改革法：内部統制の報告要件）第3版」に記載されている質問項目170を参照してください。

財務諸表に重大な影響を及ぼす新規アプリケーションの導入に際して、以下のステップを考慮することを強くお勧めします。

1. 質問項目7に関連し、企業は本番稼動に向けてのベースラインを構築すべきであり、また企業改革法の要綱をシステム機能の要件定義とそれに関連するテスト内容に反映させるべきです。

2. 重要なアプリケーションを導入する企業は、コントロールの整備状況評価と、必要に応じて企業改革法を遵守するための文書（例：フローチャート、業務概要記述書、リスクコントロールマトリックスなど）の整備を実施する必要があります。

3. プロセスオーナーとシステムの利用者は、新規アプリケーションのコントロールを理解しなければなりません。特にERPシステム導入においてユーザートレーニングは、統制環境の有効性を保証するために重要な要素です。

4. 最後に、ERPやその他の重要なアプリケーションの導入に関して、計画の段階から外部監査人に参加してもらい、整備と開示についてガイダンスをしてもらうことは大切です。弁護士からのアドバイスは、適切な情報開示に必要です。

これらのステップの積極的な実施は、効率的かつ有効的な企業改革法遵守に役立ち、期末においてリスク低下のための予想外なコスト負担を防ぎます。

以下は、ERPの導入をSECに報告する際の開示例です：

＊ 当社は、成長計画に合わせてERPシステム導入を2006年までに完了させる予定です。ERPシステムの導入は、重要な業務プロセスの変更と組織的なトレーニングの実施を伴います。当社は、段階的導入のアプローチを採用し、これらの変更に対するリスクを低減し、移行期間において適切な内部統制の監視と維持のステップが実施されていると考えています。これらのステップには、内部統制に係るリスクを低減するための人員の配備、追加の検証実施、データのインテグリティのテストを含んでいます。当社は2002年に開始された米国企業改革法404条の報告・認証・宣誓の要件の一部として、財務報告に係る内部統制の有効性に関して、総合的なレビューを実施する必要があります。2004年12月31日の期末時点において、当社の内部統制の運用状況は、重大な欠陥は確認されませんでした。ERPシステム導入に関連して、2005年内に業務プロセスの重要な変更があると想定しており、それらの一部は財務報告に係る内部統制及びコントロールと手続きの開示に影響すると考えています。

3. 404条対応で必要となる代表的なアプリケーションコントロールにはどのようなものがあるのでしょうか？

COSOは、アプリケーションコントロールを「アプリケーションソフトウェアにプログラムされた手続きと関連するマニュアル手続きであり、情報プロセスにおけるデータの網羅性と正確性を保証するために整備されたもの」と定義しています。404条対応の観点からアプリケーションコントロールは､6つの主要なエリアに分類されています。

1. **自動化されたコントロール**―自動化されたコントロールとは、アプリケーションに組み込まれた機能によるコントロールです。これらのコントロールは、開発者またはプログラマーによるプログラム変更・保守を基に実行されるアプリケーションの機能で、コーディングされたコントロールです。貸借が一致しない記帳と転記を認めない機能をアプリケーションに組み込んでいる場合などが例として挙げられます。企業が社内開発のアプリケーションを使用している場合、多くのシステムコントロールはIT担当者による保守を必要とします。また、アプリケーションを使用している企業の場合、多くのシステムコントロールは、企業の方針、規則、戦略などに沿って設定され、運用されています。アプリケーションコントロールは、アプリケーションの機能としてその機能を「スイッチ」

でオン・オフすることにより、不適切な処理からデータを保護できます。設定されているコントロールとは、入力制限、使用制限、リミットチェック、妥当性チェック、エディットチェック、画面レイアウト、権限グループ、バリアントチェック、例外レポート、セキュリティ設定などが考えられます。アプリケーションコントロールは、予防的コントロールにも発見的コントロールにもなりうるコントロールです。アプリケーションコントロールの例としては、発注内容と請求書のチェック、資産区分における耐用年数の範囲チェック、マニュアルで記帳をする際の必須項目チェックなどがあります。重要な業務プロセスや取引サイクルにおいて自動化されたコントロールは、重要なリスクに対して適切に認識され、依拠されることが必要となります。統制環境の維持可能性と費用対効果を向上させること及び重要なコントロールのテスティング実施の効率性を向上させるために、自動化されたコントロールの最適化を継続的に実施していく必要があります。具体的なコントロールについては、セクション3をご参照ください。

2. **自動化が可能なマニュアルコントロール**—アプリケーションがどのような形で統合されていても、通常、企業は、データのインテグリティと財務諸表の信頼性を保証するためにアプリケーション外で運用する重要なマニュアルコントロールを採用しています。勘定科目の照合や承認をマニュアルコントロールの例として挙げることができます。コントロールの有効性と効率性を向上させるために、マニュアルコントロールをシステムコントロールに「切り替える」ためのあらゆる可能性を考慮する必要があります。

3. **インターフェース／インテグレーションコントロール**—SOX法対応のアプローチとして、特にアプリケーション間のインターフェースがマニュアルの場合（例：アップロードまたは転記を行うためにアプリケーションからデータをダウンロードする）、インターフェースは、財務報告に係るリスク要素として考慮しなければなりません。インターフェースされたデータのインテグリティを保証するコントロールを特定し、有効性を確保する必要があります。企業は、コントロールを文書化しファイルがどのようにインターフェースされているか、インターフェース前にユーザーがどのように業務取引に対する承認を実施しているか、インターフェースされたデータの網羅性、正確性を保証する照合手続またはツールについて、それぞれ評価する必要があります。例えば、基幹システムとインターフェースする給与アプリケーションを利用している場合、二つのシステム間で行われる重要なデータ「転送」に係る固有リスクに対応するコントロールを特定し、有効性を確保する必要があります。インターフェースに関するコントロールを評価することは、各アプリケーション独自のコントロールを評価することと同程度の重要性があります。具体的なコントロールについては、質問34をご参照ください。

4. **レポートコントロール**—アプリケーションが作成したレポートが企業の財務状況を正しく反映していることを保証するために、レポート作成のためのコントロールが組み込まれていることが必要となります。コンプライアンスチームは、財務報告に係るリスクについて、関連するアプリケーションの内外を含めてリスク評価を実施する必要があります。レポート作成に関するコントロールの整備状況と作成されたレポートの編集におけるプロセス、すなわちアプリケーションからデータを抽出し編集するプロセスも考慮する必要があります。一般的な例としては、基幹システム（例：ERP）から財務関連データをダウンロードし、SECに報告するためのEDGARフォーマットなど、財務諸表を開示するためのスプレッドシートを作成する場合を指します。財務諸表を最終的に作成する前にデータをダウンロードするにあたり、データが不適切に修正されてしまうリスクに対するコントロールを特定し、有効性を確保する必要があります。上記のようなコントロールが適切に組み込まれていない場合、財務報告に係るリスクが十分に低減されている状態であるとは言えません。

5. **職務分掌（SoD）に関連するアプリケーションセキュリティ**—セキュリティ管理が行われているとしても職務分掌の分野においては、個人またはグループがアプリケーションへ不適切または過度なアクセスをし、職務に関する不正を引き起こしてしまう（例：委託業者を選定する担当者と委託業者へ支払いを実施する担当者が同一など）恐れや、取扱いに注意を払うべき取引を不適切に、もしくは不必要に実行してしまう（例:委託業者の支払データまたはアプリケーションの設定に対する不適切な修正）恐れがあります。アプリケーションのセキュリティは、重要な業務サイクルごとに、明確な役割や定義を基にした適切なアクセス状況を確保する必要があります。すなわち、職務に不正が発生しないように、役割ごとに定義されたアクセス権を設定する必要があります。アクセス権は、個人の役割に応じて付与しなければなりません。役割の重複などの不正を招くようなアクセス権の付与が行われないように注意しなければなりません。具体的なコントロールについては、セクション4をご参照ください。

6. **変更管理、セキュリティ管理、コンピュータ運用などのアプリケーションコントロールに影響を与えるIT全般統制**—正確ではない、かつ／または未承認のシステム変更や、アプリケーションに関連するデータベース・ネットワークへのアクセスなどの全般的なIT環境の保守は、アプリケーションにより生成されるデータのインテグリティに大きな影響を

与えるものであり、これらに係るコントロールは非常に重要です。具体的なコントロールについての詳細は、セクション4をご参照ください。

4. SOX法対応及び財務報告のためにシステムコントロールが重要視されるのはなぜでしょうか?

一般的にシステムコントロールは、マニュアルコントロールのように人為的なミスの影響を受けにくいため、より信頼できるコントロールと言われています。システムコントロールが適切に整備・運用維持されている限り、マニュアルコントロールをテスティングする場合と比べて、システムコントロールのテスティングは費用対効果が高いと考えられています。適度にシステムコントロールとマニュアルコントロールが存在する状況において、それらのコントロールの評価を実施する場合、以下の2つのポイントを考慮してください。第一に、データのインテグリティの確保は、正確な財務諸表の作成において欠くことのできない要素であるということです。第二に、データのインテグリティを保証するためには、アプリケーションシステムに組み込まれているコントロールや適切に設定されたアクセス制限に係るコントロールを確保することが重要であるということです。例えば、会計システムに対するマニュアルによる記帳の際に、貸借の一致をチェックする機能が存在しない／利用していないことは、財務諸表の信頼性に対して影響を与えることになります。

多くの企業は、SAP、Oracle、PeopleSoft、JD Edwards、LawsonなどのERPシステムを導入しています。これらのERPシステムは、企業内の業務の統合・標準化、企業の業務にあわせた機能設定など多くのメリットをもたらします。ERPシステムの統合性という性質により多くのトランザクションは、何らかの形で財務諸表へ影響を与えます。現場レベルから、財務部担当者や役員レベルにいたるまで、ERPシステムへアクセス可能な従業員すべてが財務諸表の信頼性について何らかの影響を与えることになります。記帳と当該仕訳の承認を一人の担当者が実行できる場合、職務分掌の問題として故意または故意でない会計記録の不正または誤謬が発生し、それは不適切な財務諸表の作成につながります。

5. 404条遵守のためにキーとなる業務プロセスで重要なアプリケーションはどのように判断するのでしょうか?

財務諸表における重要な要素とそれに関連するプロセスの確定後、コンプライアンスにおいて重要なステップは、重要と判断されたプロセスに関連するアプリケーションの特定です。これらのアプリケーションは、財務諸表の要素に影響を与えることが多いと考えられます。重要な業務プロセスを分析する際に、コンプライアンスチームは、重要なインプット、プロセスにおける活動とプロセスのアウトプットを文書化する必要があります。この文書化において、プロセス上不可欠なアプリケーションシステムの記述とマッピングを含める必要があります。詳しくはセクション7をご参照ください。

取引の発生から財務諸表が作成されるまでのフローチャート内に含まれる重要な業務プロセスに関連するアプリケーションが（アプリケーションに対する全てのアクセスポイントと人手によるデータ受け渡し、アプリケーション間のインターフェースを含めて）認識され、重要度を付される必要があります。言い換えると、コンプライアンスチームは、(a) プロセスの目的を達成するために不可欠で、(b) 財務報告に対するアサーションの達成を阻害するリスクが高いプロセスに関連するアプリケーションを選択します。選択されたアプリケーションは、文書化と評価プロセスの対象とします。

アプリケーションの特定は以下の事項を考慮する必要があります：

- **処理される取引のボリューム**（件数が多ければ多いほど、アプリケーションは重要になります。）
- **取引金額**（金額が大きければ大きいほど、アプリケーションは重要になります。）
- **計算の複雑さ**—ここで言う複雑さとは、ユーザーが計算の妥当性を判断する際の複雑さです。（複雑であればあるほど、アプリケーションは重要になります。）
- **データと取引の機密性**（機密性が高ければ高いほど、アプリケーションは重要になります。）

下図は、ビジネスプロセスとアプリケーションの関連性を表しています。

ビジネスプロセス	アプリケーション				
	ERP	連結	HR	サプライチェーン	その他
総勘定元帳管理	●	●	●	●	
購買	●			●	
給与	●		●		
売掛	●			●	
在庫管理	●			●	
その他	●				●

多くの企業は、総勘定元帳作成のためERPシステム（例：SAP、Oracle）を導入しています。また、連結財務諸表作成のためのシステム（例：Hyperion）も導入しています。404条遵守の活動に着手し、多くの企業は、ERPでのユーザーアクセス権について、職務上で必要のない権限とデータへのアクセス権をユーザーに対して付与していたことに気づきました。それらの企業は、その対応としてアクセス権の構成を修正し、適切なアプリケーションへのアクセス権を導入しました。しかし、ユーザーはアクセス制限を迂回し、連結システムを通して関連システムにアクセスすることが可能でした。従いまして、ERPのセキュリティに加えて、連結システムがセキュリティ評価範囲の重要な要素であるという認識がなければ、企業の評価は十分なものにはなりません。対象アプリケーションの特定、優先順位付けにおいて、エクセルシート、エクセルのマクロ、ユーザーデータベースプログラム（例：Microsoft Access）、ウェブベースのプログラム、計算機を含む、使用されている全てのアプリケーションを洗い出す必要があります。

まとめとして、重要なプロセスに関連し、財務諸表の重要な要素となる全てのアプリケーションを特定することはとても重要です。コンプライアンスチームが、法令遵守、404条の文書化と統制評価の観点からどのアプリケーションがキーとなるかの確認をすることになります。

6. アプリケーションコントロールの評価は業務プロセスの評価に含めますか、それとも別に評価するのでしょうか？

アプリケーションコントロールは、業務プロセスおいて重要な部分を占めています。可能であれば、業務プロセスの文書化のタイミングで、アプリケーションコントロールの文書化と評価及びマニュアルコントロールの文書化と評価を実施することが望まれます。コンプライアンスチームは、業務プロセスにおけるリスクとキーコントロールを考慮する必要があり、どのコントロールがアプリケーションにより自動化されているコントロール（例えば、発注・請求書・仕分転記の自動照合など）なのか、あるいはどのコントロールが業務を効率的に実施するため、システムから出力された情報（例外事項に関するレポートなど）に依拠するコントロールなのかを識別する必要があります。マニュアルコントロールとアプリケーションコントロールは、何もないところで運用されるわけではありません。両者は、多くの場合、相互に依存している関係にあります。よって、このようなコントロールの依存の度合いを認識し、業務プロセス全体としての総体的な評価を同時に達成することが重要です。PCAOBもこのポイントについて、監査基準第2号の別添において事例を紹介して説明しています。

業務プロセスにおいて、マニュアルコントロールとアプリケーションコントロールを同時に考慮することによって、コンプライアンスチームが運用状況のテスティングを継続的かつ効率的に実施することができます。また、マニュアルコントロールとアプリケーションコントロールの最適な構成を決定できる可能性が非常に高くなります。さらに、コンプライアンスチームは、自動化できる可能性のあるマニュアルコントロールを識別することができるようになります。

404条を遵守するためのキーとなるアプリケーションとマニュアルコントロールが特定されたら、コンプライアンスチームは、アプリケーションに内在するコントロールを完全に理解し文書化するためのステップを考慮する必要があります。これらのステップを策定するにあたり、スキルとリソースは重要な要素となります。（例：重要なアプリケーションシステムの仕様・運用方法とシステムに搭載されたコントロールの性能を理解するためのスペシャリストの必要性）

7. 重要なアプリケーションはどのように決定すればよいのでしょうか？

重要なアプリケーションの特定をする際に考慮する必要のある項目は以下の通りです:

- **重要なアプリケーションの範囲の特定**—網羅性、正確性、適時性、及び関連する取引の処理と報告の適切性を保証するための手段として依拠できるような主要なアプリケーションコントロール、プログラムとして組み込まれた機能とレポートの範囲を特定します。ここで特定されたコントロール、システムの機能、そしてレポートの分量によって重要なアプリケーションの範囲が特定されます。

- **設定可能なコントロールと関連する全般的なアプリケーションプロセスの文書化**—コントロールやシステムの機能、そしてレポートに関するパラメーター設定と業務ルールを文書化します。そして、設定や業務ルールがアプリケーション（例：ERP）において構築（文書化）されていることを確認して、該当するマネジメントから承認を受けます。

- **セキュリティ管理と変更管理における業務手順とコントロールの構築及びその確認**—特定のアプリケーションに対するアクセス制限の管理プロセスが文書化されていると同時に、設定が適切であることを確認します。これに加えて、アプリケーションにおいて中心となるようなロジックに関連する変更管理のプロセスについても、文書化されていると同時に適切であることを確認します。

- **設定可能なコントロールと全般的なアプリケーションプロセスの運用状況の確認**—（設定可能なコントロールと全般的なアプリケーションプロセスに関して）特定された範囲のアプリケーションが意図された通りに運用され、かつ文書化された通りで

あることを確認します。これらは以下のポイントを検証することにより確認できます。

- 単体テスト、結合テスト、システムテスト、ユーザー受入テスト、移行判定確認などのアプリケーションの導入時に作成した文書に関するレビュー。
- 自動的なもしくは手作業によるコントロールやシステム機能のテストの再実施。システム上の既存設定に関するエビデンスや変更管理手順が正しいことを確認するためのシステムテストツールを利用することも出来ます。テスト手法とシステムテストツールに関しては、質問項目の8と10をご参照ください。

- **ベースラインの維持と変更管理**—ベースラインを定義している文書の管理を実施します。次に、全般統制（例：変更管理とセキュリティ管理）における継続性の確保とその確認を実施します。さらに、アプリケーションコントロールまたはIT全般統制における変更は、必ず文書化とテスティングを実施します。

重要なアプリケーションが複数ある場合（例：複数のERPがあるなど）、または、対象となるシステムで、複数のインスタンスやインストールが実施されている場合、企業内の変更管理と全てのアプリケーションに対するセキュリティ管理プロセスを標準化することにより、統制環境を改善することができます。さらに重要なアプリケーションの評価において、作業の大幅な効率化を達成することができます。

8. マニュアルコントロールのみに依存することによって、アプリケーションコントロールを考慮せず評価しないことは可能でしょうか？

理論的には可能ですが、お勧めしません。マニュアルコントロールは、継続的に運用することが難しい上に、人為的なミスにより容易にコントロールが有効でなくなってしまう場合があるからです。さらに、マニュアルコントロールを主要なコントロール、もしくは唯一のコントロールとして保守、テスティングするためには莫大な費用がかかると同時に非効率であり、マネジメントによる効果的なITへの投資を否定することにもつながります。

監査委員会と上級経営者は、コンプライアンス担当者に対して、財務報告に係るコントロールの有効性を高めると同時に運用及び評価するための費用を削減することを指示します。SOX法を遵守するための重要なステップとして多くの企業は、当初2年間において経験した、その場限りの対応（Compliance Project）から、継続的に実施可能なシステムコントロールへの依拠の度合いを増し、より費用対効果を高め付加価値が得られるようなプロセス（Compliance Process）へ移行する過渡期にあります。

このようなコンセプトは決して目新しいものではありません。このようなリエンジニアリングの動きにおいては、まず1990年代にSAP、Oracle、PeopleSoft、JD Edwardsやその他の総合的なERPシステムに注目が集まりました。但し、これらのアプリケーションは様々な業務や財務に関連する取引をシステム化したにもかかわらず、多くの企業において、内部統制のシステム化は先延ばしにされてきました。その理由の一つとして、内部統制は、企業の業務プロセスの再構築の「妨げ」となる見解があったためです。実際、多くの企業では、「パッケージ」であるERPシステムを使用しているため、必要とされているシステムコントロールが既に搭載され、活用されています。しかしながら、このようなコントロールの観点は、ERP導入チームにとって優先的に意図されたり、システム機能の強みとして認識されたりすることはありませんでした。

現在、SOX法やその他のガバナンスに関する要件は、適時に信頼性のある財務諸表を開示し、四半期ごとに内部統制に対する開示を求めており、これは企業にとってかつてないほどのプレッシャーとなっています。このような要件を達成するための内部統制は、毎年度、適切に実施され、同時に運用状況について確認される必要があります。多くの企業は、必要以上にマニュアルコントロールに依存しており、いわゆる昔ながらの「細分化した業務単位での確認」によるテスティングを実施しています。しかし、システムコントロールとマニュアルコントロールの構成を最適化した上で評価を実施しない限り、毎年多くの企業は、膨大な費用をかけテスティングを実施し続けなければなりません。

9. コントロールを自動化する便益は何でしょうか？

コントロールの自動化は企業にとって大きな便益があります。その具体例は以下の通りです：

- マニュアルコントロールを実施、または管理するための工数を減少させることができます。
- 工数のかかるマニュアルコントロールのテスティングを、より効率的なシステム設定の確認テストに置き換えることによって、年次評価の際に要するコストを減少させることができます。
- システムによって処理の一貫性やコンプライアンスを確保することにより、人為的なミスや不正を削減することができます。
- 問題を適宜に発見し、あるいはこのような問題の発生を予防することに重点を置くことにより、コントロールの品質を向上し、作業の手戻りを削減することができます。

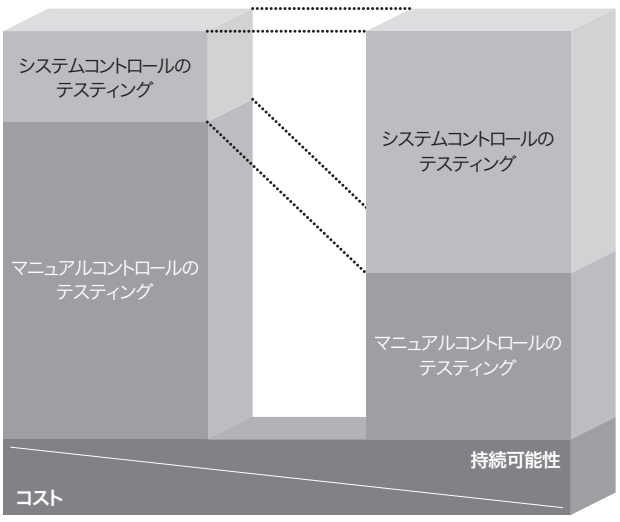
- 外部監査においても同じ論理によってテスティング工数を削減し、そして外部監査人が、より安全なシステムコントロールを対象とする内部監査への信頼性を高めることで、監査報酬を（企業にとって）より積極的に管理することができます。

既存の内部統制に満足しているコンプライアンスチームは、コントロールの自動化に大きな抵抗があるかもしれません。しかしながら、外部監査人からのシステムコントロールへの依拠を多くするようにというプレッシャーと、企業自身の長期的な経費削減を無視することはできません。そして、業務のシステム化の機会については、企業にとっての継続的な付加価値と経費削減をもたらすこととして考慮すべきと言えます。付加価値が高い業務分野におけるシステム化の失敗は、非効率なマニュアルコントロールへの依存度を高める結果となり、内部統制の構築・運用にかかる経費が増大することになります。

10. マニュアルコントロールをシステムコントロールに変更する際、何を基準に変更すればよいでしょうか？

コントロールの構成及びこれに関連するテスティングをよりシステムコントロールへ依拠した状態へ変更するためには、ある程度の期間が必要となります。このためには、社内における様々な業務リソースの供出や、一定のシステムへの投資が必要となります。この場合、企業は財務報告に係る内部統制の運用状況評価に関する経営者による評価結果を裏付けるような証跡を精査することから始めなければなりません。この調査は、システムコントロールへの依拠の度合いを再構成することを目的としています。

まず、企業における既存のキーコントロールを複数の観点から改めて見直してみます。その際には、コントロールを自動化することによる付加価値を最大化するために、以下の観点が重要となります：



- 改善活動が、共通するプロセスに対して乗数的な効果を発揮するような統合的なソリューション（例：ERP）を適用する。
- 運用及びテスティングにかかるコストが高額なマニュアルコントロールをシステムコントロールに変更する。
- コントロールが有効に機能しなかった場合に、財務報告やパフォーマンスに対して最も大きな影響を与えると考えられるリスクの分野において利用する。
- 職務分掌や監査法人が懸念を抱いていると思われる事項などの、外部監査において特に留意が必要と思われる部分に注力する。
- 既存の業務のうちで、エラーや障害が発生しやすいと思われる業務に目を向ける。
- 繰り返し発生する業務、あまり判断や人の手による介入が必要ないような業務の手順に対して適用する。

マニュアルコントロールまたは十分とは言えない様なシステムコントロールに対して上記の観点を当てはめることにより、経営者はコントロールをシステム化または最適化する際の優先順位をつけやすくなります。

システムコントロールに依存する場合の前提条件としては、高いレベルでのセキュリティコントロールを含む適切なプログラム及び設定の変更管理に関するコントロールが必要です。もしいずれかに関する全般統制が脆弱な場合、経営者または担当者によるシステムコントロールへの移行についても脆弱なものとなってしまいます。それに加えて、コンプライアンスチームとしては、この様なシステムコントロールが期末まで有効であることを証明することができなくなってしまいます。

市場に豊富に存在するソフトウェアパッケージは、コントロールの自動化を進める第一歩になります。（詳細についてはセクション10をご参照ください）しかし、自動化という選択肢が、全ての場合において有効であるわけではないことに留意する必要があります。つまり、将来的に達成されるコスト削減の度合い、内部統制の品質と有効性の向上といった効果と、これを達成するために必要な変更に要する総体的なコストを評価する必要があります。

11. 企業はEUC（エンドユーザーコンピューティング）への依存度をどのようにして下げることができるでしょうか？

多くの企業においては、既存のアプリケーションにおけるレポート

関連の機能を向上させる余地があると思われます。企業の担当者は、既存のアプリケーションではなく別のソフトウェアから出力したレポートやデータに依拠している場合があります。このような場合は、財務報告に関連するソフトウェアを利用しているユーザーが、アプリケーションが有しているレポート機能を最大限に使用していないということを示していることになります。つまり、スプレッドシートへの依拠は、このような問題に対する格好の例となっています。

例えば、多くの企業がアプリケーションからデータを抽出し、これをスプレッドシートにダウンロードして、スプレッドシート上でソートやフィルタリングなどの編集を行っています。このような作業は、アプリケーションに搭載されている同様の機能に対する理解がされていないために実施される場合があります。これは、アプリケーションの導入時における、不十分なユーザー要件分析を理由とするものです。なお、その他の理由としては、エンドユーザーに対してアプリケーションが有する機能について明確な説明がされなかったという、トレーニングに関する問題である場合もあります。もし、企業全体でこのようなことが一般的に見受けられるのであれば、経営陣は、これを潜在的なリスクとして考慮する必要があります。また、内部統制に関するコンプライアンスに関与している従業員は、企業で利用されているアプリケーションの機能を適切に理解する必要があります。そのためには、コントロールの意味、及び関連するコンプライアンスを実施するためのコスト、コントロールを実施しない場合のリスクについて理解する必要があります。さらに、アプリケーションから出力されるレポートを利用することの重要性について適切に認識する必要があります。

Section3:
アプリケーションコントロールの考慮点

12. システム化可能なコントロールとは何でしょうか?

アプリケーションに特有のコントロールにおいて考慮すべき事項は、アプリケーションでプログラムされたコントロールに密接に関連しています。これらは「プログラムされたコントロール」と呼ばれており、業務プロセスレベルのリスクを低減するコントロールとして信頼することができます。質問項目4において、「システムコントロール」として記載されています。システム化可能なコントロールとは、自動化が可能なプロセスコントロールの集合として考えることができます。

システム化可能なコントロールの例として、許容される制限値や制限幅、データのインテグリティチェック、入力必須項目の指定、そしてワークフローでの承認などをあげることができ、これらはアプリケーションの機能の一部として導入されています。このようなコントロールは、データが網羅的、かつ正確にまた適時に処理され、そして、財務報告に係るアプリケーションによって出力されるレポートについて、経営者が提示した基準に沿ったものとなることを促進します。これらのコントロールにおいては、重要な業務プロセスを処理するために以下のような点を考慮する必要があります:

- **自動計算**
- **データ照合及び編集チェックの実施**
- **他システムとのインターフェース**
- **経営者が網羅性と正確性について依拠できる重要な財務情報のソート、サマリー、レポート処理**
- **取引とデータへのアクセス管理**

上述したアプリケーションレベルのコントロールは、適切に設計される必要があり、経営者が意図した通りに、そして意図したときに機能する必要があります。コントロールが経営者の意図した通りに、そして意図したときに実施されないことがないように、プログラムに組み込まれたコントロールが変更されておらず、かつプログラムに組み込まれたコントロールに関連するアプリケーションも変更されていないことが前提となります。質問項目7に記載されていますように、企業はシステム化可能なコントロールの「ベースライン」を設定しておく必要があります。これは、システム化可能なコントロールを意図された通りに有効に機能するように設定した上で、変更管理及びセキュリティ管理のプロセスを含む重要なIT全般統制が有効であることを確認しておくことで設定することができます。このようにしてベースラインを設定しておけば、今後においてシステム化可能なコントロールに変更が生じた際にも、これを再設定していくことができます。

アプリケーションレベルのコントロールについて説明する際によく使用する用語としては、「固有のコントロール」という表現があります。この用語については解釈が必要ですが、よく用いられる例としては、アプリケーションに「ハードコーディング」された、データのインテグリティに関するコントロールがあります。例えば、ERPシステムにおける売上処理のデータフローでは、受注から製造、出荷、在庫、収益の認識と記録、債権管理、入金と「順を追って」取引データが引き継がれていきます。実際、企業は、データの受け渡しが正確かつ適時に実施されるようにプログラムに組み込まれている固有のコントロールに依拠することになります。プログラムに組み込まれた固有のコントロールとシステム化可能なコントロールを識別する場合、システム化可能なコントロールとしては、不正確な金額または承認されない金額を許容してしまうリスクを低減する目的から、販売された製品に係る受注データにおいて承認可能な金額の幅を要件に応じて設定することができるというコントロールを例としてあげることができます。他のシステム化可能なコントロールの例とし

て、請求書の金額についてあらかじめ設定された一定の許容金額以下の場合にのみ支払いの処理を許可すると言うコントロールがあります。従いまして、システム化可能なコントロールとは、意図された通りに選択して設定できるようなコントロールを意味しており、固有のコントロールでは、このような設定を実施することはできません。固有のコントロールに対する修正を実施するには、アプリケーションの基礎となっているようなロジックそのものを修正することが必要となります。もしこのような修正を実施するのであれば、企業の変更管理やその他の関連する統制プロセスに従う必要があります。

アプリケーションコントロールのテスティングについては、セクション8とセクション10に記載しています。

13. 文書化とテスティングのためのキーとなるアプリケーションコントロールはどのように特定されるのでしょうか?

全ての主要な取引サイクルにおいては、以下の観点に留意してアプリケーションコントロールを認識し、優先順位付けを行い、文書化を実施することが非常に重要です：

- 全般的な業務プロセスにおいて重要と認識されるサブプロセスと、これに関連するアプリケーション
- 対象として認識された各サブプロセスに関連する処理（主要なインプット、処理機能、主要なアウトプット、及びこれらに関連するアプリケーション）
- 各サブプロセスにおけるリスクとコントロール

質問項目6に記載されているように、アプリケーションに関連するリスクとコントロールは、マニュアルで実施されているその他の業務プロセスのリスクとコントロールと合わせて判断する必要があります。両者を一度に考慮することは、マニュアルコントロールとアプリケーションコントロールの関係についての正確な理解を得る上で重要なことです。このことにより、文書化の費用対効果の向上、対象となるサブプロセスの総合的な優先順位付け、業務プロセスのリスクとコントロールの評価が可能となります。

セクション2で記載したように、アプリケーションに関連するリスクとコントロールは、重要なプロセスで使用されているアプリケーションと関連があるため、以下の事項を認識しておくことが非常に重要です：

- アプリケーションにおける処理機能と重要なアクセス権限（例: 支払処理の実行、など）
- 職務遂行のためにアプリケーションを利用しているユーザー
- 業務プロセスにおいて、職務分掌と望ましいセキュリティ環境を維持するためのセキュリティ管理プロセス
- アプリケーション及び関連するデータの変更管理プロセスにおいて、業務プロセスで必要なマスターデータを作成、維持、そしてコントロールするための方法
- 業務プロセスに関連する、プログラムに組み込まれた固有のコントロールとシステム化可能なコントロール（例：取引データの統合、総勘定元帳と補助元帳の統合、入力値の許容制限、必須項目の設定、ワークフローによる承認、そして警告やエラーメッセージの出力、など）

業務プロセスに含まれているリスクとコントロールを適切に理解するためには、まず第一歩として、主要な業務プロセスに関連しているアプリケーションの機能を十分に理解することが必要です。このセクションでは、特に、主要な業務サイクルに係るERPシステムの機能について記載します。以下に記載している各業務サイクルの基本的な業務プロセスは、異なるERPシステムにおいて大差はありませんが、それぞれのアプリケーションにおいては微妙な差異があり、業務プロセスにおけるリスクとコントロールを効果的に評価するには、業務プロセスとアプリケーションそのものに関する詳細な知識が要求されます。このセクションで扱っている主要な業務サイクルについては、多少のレベル感の相違はあるとしても、多くのアプリケーションに適用することができます。多くのERPシステムの特徴として、システム統合と機能設計における脆弱なシステムコントロールは、広範囲な影響を与えてしまうことになります。従いまして、アプリケーションにおけるシステム化可能なコントロールが適切に設計、導入、維持、そして保護されているという保証が重要になります。

これまでの記載に加えて、以下に例示している質問項目は、重要なコントロールにおける考慮事項となっています。以下の質問項目では、重要な業務サイクルである販売から入金まで（質問項目14）、調達から支払まで（質問項目15）、決算／財務報告（質問項目16）に関連する内容が記載しています。また、SAP、Oracle、PeopleSoft、そしてJD EdwardsといったERPシステムにおいてシステム化可能なコントロールの例を記載しています。以下の記載はあくまでも例であって、各アプリケーションおいて考えられる全てのシステム化可能なコントロールを記載しているわけではありません。ここでの目的は、主要な業務プロセスのシステム化可能なコントロールの例示、そしていくつかのアプリケーションにおける関連する処理機能の例示です。

14. 販売から入金までのサイクルで重要なアプリケーションコントロールは何でしょうか?

ERPシステムにおける、販売から入金まで(OTC)の取引サイクルは、企業が得意先に提供している販売、納品、商品やサービスの提供に伴う請求といった関連する全ての取引を網羅します。ERPシステムがこの取引サイクルで提供する機能は、以下の通りです:

- **得意先マスターデータの管理**
- **引き合い、見積、価格決定、契約に関する管理**
- **受注処理と与信管理**
- **商品/サービスの提供、出荷処理**
- **返品処理**
- **請求処理と支払処理**
- **補助元帳と総勘定元帳への転記**

これらの取引サイクルには、考慮すべきシステム化可能なコントロールや処理機能が存在しています。例えば、得意先マスターデータの管理、重複登録のチェック、価格決定における許容値の制限、請求処理における許容値の制限、請求処理の重複登録チェック、督促処理、与信限度額の設定、クレジットメモの制限金額の決定、出荷に伴う売上計上における許容額の制限、総勘定元帳への記帳処理、取引勘定への影響と照合、そして、収益の認識と勘定科目の決定などの例があげられます。

以下では、このようなコントロールの中から2つのコントロールについて詳しく説明します:

- **得意先マスターデータの管理**—SAPでは、得意先マスターデータが重複して登録されてしまうことを予防、若しくは適時に発見できるように3つのコントロールを提供しています。1つ目は、重複している得意先マスターデータの検索機能です。SAPには、重複して登録されている得意先マスターデータを得意先の名称と得意先の住所で検索できる、「あらかじめ備わった」機能が実装されています。しかし、このコントロールは、得意先マスターデータの重複を検索することができるだけで、入力時における予防的な機能ではありません。2つ目は、システム化可能なコントロールで、あらかじめ定義された検索条件に基づいて、得意先マスターデータが重複して登録されてしまう可能性がある場合に、警告もしくはエラーメッセージを出力します。このコントロールは、SAPに「あらかじめ備わった」機能ではなく、検索条件を「事後的に設定する」ことで有効に利用可能となる機能です。最後のコントロールは、発見的コントロールで、SAPに「あらかじめ備わった」レポートの機能です。SAPの標準レポートである「RFDKVZ00」は、システムに登録されている全ての得意先マスターデータを一覧で表示することによって、重複がないかどうかのレビューを実施し易くしています。

- **請求処理と支払処理と記帳処理**—有効性、網羅性、正確性、もしくは適時性に問題があるような勘定科目の変更に伴うリスクについては、以下に示すようなOracleの統制環境におけるセキュリティの管理やコントロールの管理を実施することで解決することができるかもしれません:
  - キーフレックスフィールドにおける「クロスチェックセグメント」—この設定は、記帳処理において利用できる勘定科目を、特定の勘定科目の組み合わせのみに制限する。
  - フレックスフィールドのセグメント値や組織設定についてのユーザーアクセスの権限範囲に関するルールの設定を行う。

セキュリティコントロールの他に、以下のようなプロセスに関連するコントロールの構築が可能となります:

- **セットオブブックスにおける「仕訳承認要求」**—この設定は、あらかじめ設定された権限の範囲内で記帳を承認する。

- **プロファイルオプション「仕訳:承認者の検索方法」**—この設定は、仕訳について適切な責任者へ承認を促すためのバッチ処理を定義する。

- **「反復仕訳」**—この設定は、日常的に繰返し発生する仕訳を定義する。

- **「逆仕訳の条件」**—この設定は、逆仕訳が自動的に作成・転記されるように、仕訳期間、仕訳日付などを含む逆仕訳の際の方法を定義する。

- **「自動転記条件の設定」**—この設定は、あらかじめ決定された条件に基づいて、仕訳の選択及び転記を実施する。

- **「消去設定」**—この設定は、連結決算における消去仕訳を定義する。

15. 調達から支払までのサイクルで重要なアプリケーションコントロールは何でしょうか?

ERPシステムにおける、調達から支払まで(PTP)の取引サイクルは、企業の仕入先や供給元から提供を受けている商品やサービルに関する見積、発注、納品とこれに対する支払といった関連する全ての取引を網羅します。ERPシステムがこの取引サイクルで提供する機能は、以下の通りです:

- **仕入先マスターデータ及び品目マスターデータの管理**
- **購買見積と発注処理**
- **商品やサービスの受取と検収処理**
- **請求入力処理とその確認、及び照合処理**
- **支払処理とクレジットノート処理**
- **補助元帳と総勘定元帳への転記**

OTCと同様に、このプロセスにおいてもシステム化可能なコントロールや処理機能があります。具体的な例示については、以下の通りです：

- **購買発注、商品／サービスの受取と請求書の照合**—ERPシステムは、購買取引における照合を自動化することが可能です。多くのシステムでは、購買取引において2方向、3方向または4方向の照合処理が実現でき、多くの場合、購買の種類によって使い分けています。例えば、直接購入の場合に比べて、間接購入の場合には処理がより複雑となります。従いまして、企業において発生する調達処理における処理パターン、及びそれぞれのパターンで必要となるチェックの程度について深く理解しておくことが重要となります。Oracleの場合には、「照合承認レベル」に関する購買オプションを用いて、請求書に対する支払の際に必要な確認作業について設定が可能となっています。なお、Oracleにおけるオプションの種類は、以下の通りです：

  - **2方向**—発注書と請求書
  - **3方向**—発注書、納品書と請求書
  - **4方向**—発注書、納品書、検収書と請求書

多くのERPシステムにおいて、照合処理は、請求書に対する支払の前にのみ確認処理として実施されます。ソフトウェアを用いることで、仕入価格の相違について、購買見積額と発注書の金額との差額、もしくは発注書の金額と受取書の金額との差額があらかじめ設定された許容金額を超えていないかどうか識別できるように設定することが可能です。

- **商品やサービスの受取と検収の処理**—このプロセスにおける簿外債務に関する固有のリスクが適切に管理されていることを確認することは非常に重要です。多くのERPシステムにおいては、まずは裏づけのない勘定科目として棚卸表に記録し、その後に請求書を受領した際に仕入先元帳へ記帳することによってこのリスクを低減しています。例えば、SAPにおいては、棚卸品を受け取った際に、後で棚卸品の受入れを業者からの請求書と照合できるように、借方：物品受領勘定（GR）、貸方：請求書受領勘定（IR）という形式で記帳します。このような記帳処理は、取引の種類に応じて多くのERPシステムでシステム化することが可能です。例えば、Oracleにおいては、記帳が正確か、または網羅的かを確認する方法が複数ありますので、以下に記載しておきます：

  - 追加費用項目を購買オプションとして定義し、「期末」時の検証項目を定義する。
  - 追加棚卸項目を購買オプションとして定義し、「受入」時の検証項目を定義する。
  - 総勘定元帳へのインターフェースプログラムが稼働した際に、自動的に記帳のバッチデータが作成されるように会計システムオプションとして定義する。

Oracleにおいて、これらのシステム設定が適切に定義されれば、購買に関連する勘定元帳への記帳に係るリスクを低減することができます。

- **請求入力の処理**—不正確な債務を記帳してしまうリスクを低減することも同様に重要だと考えられます。JD Edwordsは、資材の供給者からの請求書番号がすでにシステムに登録されている場合、請求書登録に伴う買掛金の記帳処理について警告を表示し、もしくは処理が完了するのを防ぐようにシステム上で設定が可能です。この設定は、JD Edwordsにおいて請求書の入力を実施する際に、仕入先と請求書の照合を実施するように設定することで可能となります。PeopleSoftにおいては、重要な帳票（例：受取証、伝票、チェック依頼書、調整依頼書、小切手）に対して自動的に整理番号を通番で付与します。この結果として当該整理番号が、仕入先からの請求に対する二重支払の実施というリスクを低減するための予防的なコントロールとして機能することになります。

---

16. 決算／財務報告サイクルで重要なアプリケーションコントロールは何でしょうか？

決算プロセスをERPシステムで自動化することにより、総勘定元帳への記帳、勘定残高の照合、決算に関連するレポートの作成、連結決算、そして財務諸表作成といったサブプロセスにおける固有のリスクを回避・低減できるようになります。なお、その際にERPシステムに関連して考慮する必要のある項目は、以下の通りです：

- 組織体系、勘定科目体系、レポート体系、及び決算締め処理に関する設定内容

- 補助元帳への会計転記の頻度、補助元帳と総勘定元帳の照合の頻度（ERPシステムによって総勘定元帳への会計転記のタイミングは異なっており、月次バッチやリアルタイムで実施されている場合があります）

- 「伝票登録と会計転記」を用いた承認機能の設定、会計転記の際の入力許容金額の設定、そして貸借一致を確認するための設定といった、会計転記におけるシステム設定の定義

例えば、SAPの場合には、以下のようなコントロールが利用可能です:

- 「仮伝票の登録と会計伝票の転記」を利用した、伝票の登録ユーザーとその承認ユーザー（会計転記）の分離
- 会計転記が可能な期間の設定
- 補助元帳もしくは総勘定元帳へ記帳される前に、あらかじめ設定された許容金額を超える記帳が実行されないための、消し込み処理実施時の差額の許容金額の設定

SAPでは、あらゆる会計仕訳の貸借が一致していることが必要となるように設計されています。

PeopleSofにおいては、補助元帳への会計転記を自動的にまとめて、これを総勘定元帳の勘定へ転記するように設定をすることができます。この機能は、サブシステムごとに自動仕訳作成（JG）を有効にすることにより利用することが可能となります。JGを利用することで、標準的に繰返し発生するような会計仕訳についても自動転記することが可能です。また、JGを利用した会計転記において制限したい勘定科目を定義することによって、このような勘定科目を利用したマニュアルでの会計転記が入力できないようになります。なお、総勘定元帳ユーザープリファレンスにおける「JGによる仕訳変更」機能によってこのコントロールの変更が可能なため、この機能に関連する権限については、業務上の正当な理由が存在する場合のみ付与されることになります。

ERPシステムの導入は、設定さえ正しく実施しておけば、補助元帳と総勘定元帳への会計転記作業を統合することができ、その結果として勘定残高の照合にかかる時間を大幅に削減することができます。多くのERPシステムは、このような照合のプロセスをサポートするような標準的なレポートを用意しています。PropleSoftにおいても、こうした標準レポートを利用することで、補助元帳と総勘定元帳を照合することが可能です。例えば、以下のようなレポートを出力することができます：

- **買掛金仕訳サマリーレポート**
- **勘定科目別／仕入先別買掛金残高レポート**
- **仕入先別／勘定科目別買掛金残高レポート**
- **勘定科目別買掛金取引レポート**
- **仕入先別買掛金取引レポート**

これらのレポートは、レビューの際に利用されますが、この様なレポートをもってしてもERPシステムの利用が、貸借対照表や損益計算書といった重要な報告書のレビューやその他の重要な判断／マニュアル作業（例：評価損の計上の検討、引当金の積み立ての検討）の省略につながることはありません。つまり、決算処理における重要なプロセスについては、関連する規程や手続きが適切に文書化されていなければなりません。

Section4:
アクセスに関するセキュリティ上の考慮点

17. アクセス保護に関する主要なリスクは何でしょうか?

アクセス保護に関する主要なリスクには、未承認の取引の発生やアプリケーションデータの信頼性を低下させる結果をもたらす様な、不必要なアクセス、未承認のアクセス、職務分掌に反するようなアクセス、または必要以上の権限によるアクセスといったリスクが含まれます。これまでの事例を参考にすると、以下のような理由により、セキュリティの設定において、職務分掌（SoD）に関する問題を引き起こすような設定や重要な取引に対する必要以上のアクセス権限の設定が実施されてしまっています：

- アプリケーションにおけるセキュリティの設定は、企業において適切に職務が分離され、かつ職務権限上においてそれぞれの従業員が責任を負う業務のみが実施可能となることを意図しています。しかし、重要なアプリケーションの導入時においては、セキュリティをコントロールではなく、あくまでもシステム上の一つの機能としてのみ認識しているケースが多く見受けられます。つまり、システムの機能に関する問題や本番稼動までの時間的制約のため、多くの企業は、このような問題を優先的に解決するために取引データやシステムの機能へのアクセス権限を増加させてしまうのです。こうした課題解決型のアプローチでは、アプリケーションのセキュリティに関する本来の目的の達成が、以下に記載するようなシステム導入後における問題の発生により阻害されてしまいます。
- システムの本番稼働前において、導入直後のメンテナンスの実施を目的として、開発担当者に対して、「スーパーユーザー」権限が付与されることがあります。これは、担当者が新規に導入されたアプリケーションに問題が発生した場合に、解決策を即座に見つける必要があるからです。確かにこのような担当者の役割は必要と考えられますが、一方でこうした設定は有効なセキュリティを損なうことになり、かつ将来的には重

要なコントロールの不備につながる可能性があります。

- アプリケーションの導入時において、適切に重要性を考慮したアクセスコントロールが設定されていない場合があります。例えば、システム導入の責任者は、効率的な業務プロセスを確立するために、ユーザーまたはクライントからのみの情報に依拠してセキュリティの設定や従業員の役割を定義することがあります。このような場合、設定されたアクセス権限が必要以上もしくは不十分になる可能性があります。

- 変更管理及びセキュリティ管理のプロセスにおいて、当初に意図されたセキュリティの設計レベルがその後の期間において適切に維持されることが十分に担保されない場合は、期間ごとに評価・改善が必要となります。有効なセキュリティ管理プロセスが確立されていない限り、アプリケーションレベルにおける特定のセキュリティコントロールが長期にわたって効果的に維持されることはありません。

18. ユーザーのアクセス権限及び特別なアクセス権限に関するコンプライアンスを評価するために考慮すべきことは何でしょうか?

ユーザーのアクセス権限に対するコンプライアンスまたは監査に関するレビューにおいては、複数の観点に留意する必要があります。留意事項については、以下の通りです:

- アプリケーション及びデータのオーナーによる承認行為、及びアクセスポイントにおけるアクセスの妥当性に関するモニタリングの監査証跡が存在すること

- システム管理者が業務取引をレビューする際のアクセス権限が適切に考慮されていること

- 前回のレビュー以降、アクセス権限の変更がなされていたとしても、重要な職務分掌についてのルールには違反していないことに関する監査証跡が存在すること

- アクセス権限の付与に関する企業の方針が遵守されていること

- 前回のレビュー以降、特定の重要な業務取引へのアクセスが適切であったことに関する監査証跡が存在すること

レビューの際は、以下に掲げる重要な事項を考慮して、レビューを実施します:

- ユーザーアクセス権限の管理プロセス(例:システムに対するユーザーアクセス権限の追加、変更、削除)

- 業務プロセスにおける業務側及びIT側の役割

- セキュリティ管理の内容(例:セキュリティ管理のプロセスは、ユーザーアクセス権限の管理及び監視に関するプロセスとどのように異なるのか?)

- ユーザーの特別なアクセス権限に対する予防的なコントロールと継続的なコントロール、及び補完的なコントロールの内容

- ERPシステムのセキュリティの仕組み、SAPプロファイルジェネレータの様なセキュリティの仕組みを補完するようなツールの内容

このようなレビューの結果として、設定の変更が必要だと認識された場合は、これらの変更を適切に実施するための標準的なプロセスが必要です。もし、アクセス保護のセキュリティ管理プロセスにおいて発見事項が検出された場合、原因分析を実施して、適時に問題解決を図る必要があります。

多くのソフトウェアベンダーは、セキュリティルールの導入、テスト、維持を自動化するソリューションを開発しています。この様なツールについてはセクション10で記載しています。

19. 適切なユーザーアクセス制限と職務分掌を確立するにあたりどのようなプロセスが必要でしょうか?

ユーザーアクセス制限と職務分掌を確立するためには、少なくとも以下の4つの手順を考慮する必要があります:

1. **定義**—ユーザーアクセス権限は、各担当者の職務記述において果たすべき役割として記載された内容を遂行することができる業務上の職責という観点から適切に定義する必要があります。各担当の役割において職務分掌への抵触が存在する場合には、このような役割をシステム上に過大な権限として登録してしまう前にこうした抵触を解消するか、もしくは、補完的コントロールによってリスクを低減する必要があります。それぞれの役割がシステム上に登録された後は、ERPシステムの権限が過大になる可能性が高いことを念頭においた上で、職務分掌を適用し続ける必要があります。ERPシステムが職務分掌についてどのようなロジックを持っているかについては、質問項目26を参照してください。

2. **テスト**—ユーザーアクセス権限については、単体テスト(例:システムで特定の機能が実施可能かどうか)で「機能的な観点」からテストを実施し、ユーザー受入テスト(例:ユーザーがシステムにログインし、アクセス権限の要件定義通り

にアクセスが可能かどうか、またはアクセスが拒否されるかの確認を実施する）は、「ユーザーの観点」から、コントロールテスト（例：要件定義通りにアクセス制限と職務分掌が設定されているか）は、「コントロールの観点」からテストを実施します。

3. **導入**—ユーザーのアクセス権限は、テストの段階で承認された要件定義通りに設定します。アクセス権限の設定はシステム開発のライフサイクルを通じて、関連するシステム環境ごと（例：開発環境、テスト環境、品質管理環境と本番環境）に実施します。

4. **監視**—システム環境においてアクセス権限の設定が完了した後には、権限が設定通りに稼働しているかについて監視を実施する必要があります。なお、適切なアクセス権限と職務分掌を維持するための活動については、以降の質問項目にて記載してあります。

20. 定期的なレビュー、保護が必要な取引またはデータへのアクセスの管理においてどのようなプロセスが必要でしょうか？

アプリケーションのオーナー及びデータのオーナーの責任として、それぞれの責任範囲における重要な取引やデータへのアクセス権限について定期的にレビューを実施する必要があります。レビューは、業務上必要性のあるユーザーに限りアクセスが承認されており、このようなユーザーが適切に重要な取引やデータの閲覧または実行が可能であることを確認するために実施します。レビューの頻度は、取引とデータの重要性と機密性により影響を受けますが、最低でも四半期に一度は実施する必要があります。

通常、このような監視業務は、特定の処理機能や一連の処理機能へのアクセスを有している現状のユーザー一覧をレビューすることで実施されます。例えば、購買マネジャーは、購買請求書を作成する処理と発注書を作成する処理に対する権限を有しているユーザーの一覧をレビューします。このレビューにおいて購買マネジャーは、以下の点を考慮する必要があります：

- 部署異動、昇進、退社などの人事異動により、これらの処理機能へのアクセス権限が不要となったユーザーがいないかどうか。
- 物品の受入倉庫の担当者、買掛金管理部署の担当者といった職務分掌に抵触するようなユーザーがいないかどうか。
- 不注意にまたは不適切に誤ったアクセス権限が付与されているユーザーがいないかどうか。

レビュー中に例外事項を発見した場合には、当該事項を調査の上で即座に修正する必要があります。また、そもそも例外事項が発生しないようにセキュリティ管理手順の変更が必要かどうかも検討する必要があります。さらに、レビューの結果、及び例外事項をどのように修正したかに関する証跡は、その後のコンプライアンス活動のために必ず保管してください。

当該レビュー、及びその承認プロセスについては、セクション10で検討しているツールなどを用いて自動化することができます。

21. ユーザーアクセスと職務分掌における管理を実施する際の業務側とIT側の役割は何でしょうか？

これまでは、アクセス権限に対する管理責任は、業務側ではなくIT側にあると考えられてきました。しかし、現在は、IT側が重要な役割を担うのはもちろんですが、不適切な職務分掌への抵触や機密情報へのアクセスを防止するためのアクセス権限に関する管理活動（例：ユーザーアクセステーブルへの権限の追加、変更、停止、及びそれらの承認）の責任は業務側にあるとされる傾向にあります。一方でIT側の担当者は、設定が複雑なERPシステムにおいて、企業の業務要件に基づいた最適なユーザーアクセスの設定及び構築を実施する際に、重要な専門性を発揮することになります。

IT部門は、所属する従業員が適切な職務分掌に則ったアクセス権限と重要な機能へのアクセス権限が適切に制限されていることを担保する必要があります。但し、このようなIT部門の従業員は、業務要件としてのアクセス権限の適切性を判断する責任を担うべきではありません。職務分掌及び重要な機能へのアクセス制限に関する固有のルールは、セキュリティ管理者がアクセス承認依頼に関するルールへの準拠性を効果的に確認できるように定義し、かつ厳格に管理する必要があります。これは、セキュリティ管理者が、特定のアクセス承認依頼自体の妥当性について判断しなければならないことを回避するのが目的です。具体的な手順については、以下の通りです：(1) あらかじめ定義されたルールに則っていない承認依頼に対処する、(2) 特定の例外事項に対して、適切な承認を得る、(3) あらかじめ定義されたルールに則っていない手順によるアクセス承認依頼を修正する。なお、コンプライアンス違反があった場合の経営陣に対する通知手順についてもあらかじめ設定しておく必要があります。

22. 企業はコストと時間の効率性を考慮したセキュリティ管理をどのように向上させていけばよいのでしょうか？

いくつかの企業では、「80／20モデル」を適用しており、あらかじめ定義され、承認されたユーザーアクセスの役割をこれに組み込んでいます。当該モデルによれば、ユーザー管理活動のうちの80%は

標準モデルが適用でき、マニュアルでの追加的な調査を最小限に抑えられます。例えば、固定資産管理マネジャーは、固定資産管理部門として新規採用した従業員に対して、標準モデルの範囲内でのアクセス権限付与を依頼することになります。セキュリティ管理者は、マニュアルまたはツールにより標準的な固定資産管理担当者としての権限を、特別な承認を得ることなく自動的にこの担当者に割り当てます。この権限は、固定資産管理担当者に対する職務上で必要とされている機能であり、あらかじめ決定しておいた役割と一致しています。しかしながら、買掛金管理担当者としての役割に基づくアクセス権限が依頼された場合には、追加的な承認が必要となります。

もし、標準的ではない依頼が、予想を超えて寄せられた場合には、システム導入時においてセキュリティの構成が適切に設定されなかったか、あるいはそれぞれの業務におけるユーザー要件が適切に定義されていなかった可能性があります。さらに、ユーザーがそれぞれの職務において必要となる権限の種類、あるいはシステムにおいてそれぞれの業務がどのように行われるのか、なぜ特定の制限が必要とされているのかについて明確でなかった可能性があります。

従いまして、標準的でない依頼は、職務分掌や重要なアクセスに関する脆弱性をもたらすような依頼として認識することができます。但し、時には通常の業務に加えて特別な業務を実施することが必要な担当者に対して、適切な権限を割り当てるための正当な依頼である場合もあります。この場合、良好な統制環境を維持するために、リスクを低減するような発見的コントロールの存在が重要となります。

シングルサインオン、複数のアプリケーションやインフラストラクチャーに共通したセキュリティ管理、自動化されたセキュリティ管理ツールといった追加的なセキュリティ管理のためのアプローチは、企業がこのようなセキュリティ管理プロセスを適切に維持していくことに貢献するでしょう。なお、自動化されたツールについては、セクション10を参照してください。

23. アクセス権限の承認に関するルールを策定する際の最善の方法は何でしょうか?

アクセス権限の承認についてベストプラクティスとされているのは、複雑なシステム環境において、あるまとまった単位でアクセス権限を付与するようなロールベースのアクセス制御（RBAC）モデルです。これは、厳密に個々のユーザーのアクセス権限を決定するのではなく、その時々の状況や職責の変更に応じて、アクセス権限のまとまりを単位として調整を実施した上で、こうしたアクセス権限のまとまりやアクセスレベルを個別の役割に割り当て、次に個別の役割を職務上の要件や職務領域を基礎として個別のユーザーに割り当てます。

アクセス権限の導入時においては、個別の役割に対して必要のない権限が付与されてしまわないように注意が必要です。個別のユーザーが複数の役割を持つことはよくあることですが、これに対応して個別のユーザーに対して付与されている全ての権限を対象として評価し、その中で適切な職務分掌が維持されていることを確認する必要があります。

残念ながら、ERPシステムのように多くのアプリケーションを含むシステムの複雑性は、適切で強固な職務分掌を導入するためのIT部門のスキルレベルを超えてしまう場合があります。今日のERPシステムは、RBACモデルの考え方を取り入れていますが、具体的な設定方法はそれぞれで異なります。但し、数は少ないですが、役割を割り当てる前から職務分掌に抵触しているようなモデルを提供している場合もあります。

このような理由から多くのベンダーが役割の分析、定義、そしてテストを自動的にあるいは統合的に支援し、かつ役割を適切に割り当てるためのツールを開発しています。このようなツールについては、セクション10においてより詳細に記載しています。

24. 特別なユーザー権限に対してどのようなコントロールが必要でしょうか?

スーパーユーザーは、「パワーユーザー」、「特権ユーザー」などとも呼ばれます。これらのタイプのユーザー権限は、重要な処理機能に対する幅広い権限を有しているか、またはアプリケーションにおける全ての管理者権限を有しています。従来、このようなユーザーに対するコントロールは、数名の「信頼できる」従業員にのみ付与する、という点に焦点が当てられていました。しかしながら、現在の企業を取り巻く法令などを考慮すると、企業や外部監査人がこのような弱いコントロールに信頼を置くことは難しいと考えられます。

通常、システム管理者には、アプリケーションにおける重要な機能に対するアクセス権限が付与されています。（例：テーブルの編集、セキュリティ管理、バッチ処理の実行、など）質問項目21に記載されていますように、ITに関与するマネジメントがこのような重要な処理機能に対するアクセスが適切に制限されていることを確認できることが重要となっています。例えば、ITに関連する部門が10人から構成されている場合、単に「緊急時に備えて」誰かが必要になるかもしれないという理由から、簡単に10人のメンバー全員にシステムへの全アクセス権限を付与するべきではありません。十分な注意を払った上で、部門内においてそれぞれのメンバーの職責や役割を定義して、そしてこの定義に従ってアプリケーションへのアクセスが許可される必要があります。さらに、以上のような大きな権限を割り当てる際には、追加的な補完的コントロールを認識する必要があります。なお、補完的コントロールとしては、実施された処理のログを記録すること、あるいは特定の処理機能を実施する際にはこれを監視した上

で、マニュアルでの承認を必要とすることなどが考えられます。

このようなユーザーが、意図したシステムコントロールをすり抜けてしまうことを制限するための共通的なアプローチの一つとして、「ライブラリ」を利用したプロセスがあります。このプロセスを利用した場合、必要に応じて「チェックイン」と「チェックアウト」の機能を利用し、これらの機能に関連する権限をユーザーの標準的な権限として含めてしまわないようにします。特に、「チェックアウト」の機能を利用する際の承認とその監視は、ライブラリの管理プロセスを確実なものにするためにとても重要です。その他の手法としては、独立した別のグループにスーパーユーザーの活動を監視させる手法があります。なお、いずれにしてもこういった手法をマニュアルによって管理することは困難であると考えられるため、企業は、セクション10で記載されているようなソフトウェアを導入することが多くなっています。

25. セキュリティの変更は変更管理のプロセスに則って実施するべきでしょうか?

統制環境及び企業によって定義された運用手順によって異なりますが、ユーザーへのアクセス権限付与（ユーザーへのセキュリティ上の役割の割り当て）については、通常、変更管理ではなくセキュリティ管理の手順に従うことになります。しかしながら、セキュリティ上の役割を変更する際には、変更管理プロセスにおける様々な活動を適用することが望ましいと考えられます。役割を変更する際には、変更が与える影響についてのレビューやマネジメントからの承認、本番環境へ適用する前におけるテストの実施が必要となります。なお、全般統制における変更管理の一般的なコントロールの詳細については、セクション5をご参照ください。

26. 職務分掌と重要な取引やデータに対するアクセス保護に関するコンプライアンスについて、ERPシステムにおけるセキュリティの構成をどのように評価すればよいでしょうか?

システムにおけるセキュリティの不備について評価する際、まずコンプライアンスチームは、評価を実施する際のアクセス権限に関する潜在的な問題と、組織構造に固有な問題を認識しておく必要があります。例えば、倉庫に数人の従業員しか居ない場合には、物品の受入業務と棚卸業務を一人の従業員によって実施せざるを得ませんが、十分な人員を抱える企業においては、こうした業務は別々の従業員によって実施されることになります。通常、商品の仕入から代金の支払までといった業務サイクルにおいては、一人の従業員がベンダーのデータ登録とベンダーへの支払データ作成の両方へのアクセス権限を持つべきではない、といった観点を考慮する必要があります。さらに、複数の業務サイクルにまたがるような全体的な観点についても考慮する必要があります。例えば、一人の従業員が売上データと仕入データの両方にアクセス権を持たないようにしなければなりません。こうした業務サイクルをまたがるような全体的な観点からの分析を実施する際には、企業全体としての方針や手順について考慮する必要があります。なお、このようなアクセス制限の考え方については、ある企業は従業員に対して多くのデータをより自由に閲覧可能としている一方で、その他の企業では閲覧可能なデータをより絞り込むようなアプローチがとられています。

潜在的な問題を特定するにあたり、企業は「重要なアクセス権限」に関する判断基準を決定する必要があります。ERPシステムでは通常、数多くの種類のアクセス権限設定が可能となっています。そこで、企業における固有の要件や方針を踏まえてERPシステムの機能を確認し、優先順位をつけることによって、コンプライアンスに関するプロセスをより合理化することが可能です。

次のステップとして、問題を引き起こすような重要なアクセス権限の組み合わせについて考慮しなければなりません。もしこのような組み合わせを職務上の役割を評価する際に考慮できるのであれば、こうした評価活動は、ユーザーのアクセス権限ルールと関連させることで、結果として職責に関するルールを決定することにつながります。このようなアクセス権限の組み合わせの評価における作業項目は、どのようなERPシステムが導入されているかによって大きく異なってきます。例えば、SAPにおいては、固有の権限パラメーターを含むトランザクション（システム上の機能）が紐付いたロールやプロファイルに対してユーザーIDが関連付けられています。権限パラメーターは、ユーザーがそれぞれのトランザクションにおいて何が出来るか(例:読取、更新、登録など)を定義しています。従いまして、ロールやトランザクションレベルでの分析は比較的容易ですが、このような権限パラメーターの内容を理解しないことには、各ユーザーが実行可能な行為を完全に理解することは不可能です。

SSA Baanの場合、ユーザーには、複数の権限から構成されるパーミッションが付与されます。最も重要な権限は「セッション」と呼ばれます。各セッションは、更新と表示、印刷として定義され、テーブル承認は、ユーザーが実行するものを決定するために評価されます。例えば、「購入注文の整備」は、セッションコードがtdsls4101m000です。ある一人のユーザーについて、このセッションコードのテーブル承認が、「読取」とされていれば、そのユーザーは、そのセッションコードで購入注文を更新することはできないということを意味します。

このようにERPシステムの場合、コンプライアンスチームは、ユーザーがどの機能を使用する必要があるのかについてレビューを行います。次に、そのレビュー結果に基づいて、どこに職務分掌の問題が発生しているかを把握して、それぞれのERPシステムに沿った適切な権限設定を見つける必要があります。このアプローチにおいては、各

ERPシステムのアプリケーション機能に関する深い知識が必要とされており、特に対象となるERPシステムにおける重要な権限機能には、どのようなものがあるのかを理解しておく必要があります。

27. ERPシステムのセキュリティは評価あるいは構築の段階で、どのようにコントロールを考慮すればよいでしょうか?

原則的に、全てのコントロールプロセスは、資産の保全と業務における資産の交換や加工といった資産の利用という異なる目的において、これらをどのようにバランスして、またチェックするのかといった観点で実施します。特に資産の加工の業務サイクルにおいて内部統制の目的を達成するために、コントロールが有効かどうかを決定する際には、適切な職務分掌が達成されているかどうかを十分に考慮する必要があります。職務分掌の基本的な考え方として、従業員は、それぞれの職務において犯罪、問題の隠匿、不正などを行えない状況でなければなりません。職務分掌において一般的に分ける必要があるとされる職務は、以下の通りです:

- **資産の保管**
- **資産に関連する取引の承認**
- **取引の記録または報告**
- **取引の執行**

企業の責任として、職務分掌によるコントロールは、全ての従業員に対して、また全ての取引に対して有効でなければなりません。複数の人間による資産の交換または加工に関する職務分掌の有効性を評価するための主要な手段には、取引発生時における有効なコントロールの実施と取引の始まりと終わりからの双方向からのチェックが行われているかということです。例えば、ここで言う取引発生時におけるコントロールには、複数の承認、例外／サマリーレポート、そして上長者によるレビューと承認などが含まれます。バッチ処理やアプリケーションプロセスツールにおけるアクセスコントロールなど、関連するプロセスとイベントが違うタイミングで起きていることにより、しばしば職務分掌が不備であっても統制された環境に見えてしまうことがあります。誰もその職務を担当していない場合は、コントロールの不備となりうる可能性があります。

通常、職務を相反する形に分離することができるかどうかは、企業の大きさによると考えられています。小さな業務プロセスや小規模の経理部門では、本来あるべき職務分掌を実現することが出来ないため、その他の適切な統制に依拠する必要があります。例えば、少数の会計担当者が記録と取引の執行をしている場合です。しかしこの場合、管理者は、取引レポートを受け取り、バッチ処理の結果をレビューし、システムへのアクセス権を管理し、監視の強化に努めなければなりません。このような活動結果の証拠に依拠するその他の統制は、適切な統制環境の維持を可能とします。また、これらは、慎重な状況の変化への対応が必要です。

28. 管理者はユーザーのアクセス管理、職務分掌の再定義とユーザーアクセス権限の再構築のどちらを行うべきかをどのように判断すればよいでしょうか?

多くの企業は、ERPシステムにおけるユーザーのアクセス権限の再構築を実施することで、現状のユーザー権限を単純に修正しようとするよりも、大きな投資利益を得られると考えています。このような再構築は、まずはオプションとして現在の手続きを把握するところから開始し、そして、コンプライアンス上の目的の達成という観点から現在のERPシステムのセキュリティの状態を評価します。もし、再構築が大掛かりなものになってしまうのだとすれば、初期導入の場合と同様に、一度白紙の状態に戻した上で、再度セキュリティの設計を実施した方が良いかもしれません。こうすることによって、維持可能性が低く、時がたつにつれ安全上の要件も満たせなくなってしまうような現在のセキュリティ構成を修正しようとするよりも、運用にかかる維持費、そして時間や工数を削減することができます。

29. 職務分掌と重要なデータへのアクセスをどのように文書化するのが効率的でしょうか?

職務分掌と重要なデータへのアクセスに関する文書化は、可能であれば業務側のRCMに組み込むのではなく、個別のRCMとして実施することをお勧めします。このアプローチによって、整備状況評価とそのテスティングの際には、職務分掌と重要なデータへのアクセスに関するそれぞれの作業を明確に実施することができます。

文書化においては、職務分掌と重要なデータへのアクセスについて、それぞれのプロセスが起こった順番に沿って連続していることが望ましいと考えます。例えば、収益サイクル（受注から入金まで）における得意先マスターデータの組み合せは、以下の観点から分析されます:

1. **引き合いと見積もり**
2. **価格決定と契約管理**
3. **販売注文処理**
4. **出荷 — 配送 — 返品**
5. **回収管理 — 売掛金 — 請求書 — 債権管理 — 入金管理**

もし、これらの文書がRCMに対応する業務プロセスと同じ体系で作成されているのであれば、特定のアクセスコントロールにおける不備を改善するようなコントロールを理解することを容易に理解することができます。文書化の概念に関する検討については、セクション7をご参照ください。

30. 自動化されたツールの利用は職務分掌と重要なデータへのアクセスのためのコントロールを常に監視する有効なものとなるでしょうか?

職務分掌と重要なデータへのアクセスに関する評価を実施するために、多くの企業がシステムツールを利用するようになってきています。このようなツールを利用することによって、ユーザーの権限に関する評価をより明確に、正確に、そして再現性を伴って実施することができ、時間の節約にもつながります。このようなツールはいろいろなパッケージとして販売され、それぞれが特有の長所や短所をもっています。もし、ツールがユーザー権限の付与プロセスや権限そのものを管理するような、「企業全体に対するソリューション」として導入されるのであれば、このようなツールは、SOX法404条コンプライアンスにおけるキーコントロールともなりえます。従いまして、このような企業全体に関連するツールに対応するルールや業務の流れについては、その妥当性と正確性を確認するために独立してテストを実施する必要があります。自動化されたツールに関する詳細はセクション10をご参照ください。

Section5:
IT全般統制に関連するアプリケーションコントロールについて

弊社発行の「Guide to the Sarbanes-Oxley Act：IT Risks and Controls（米国企業改革法：ITリスクと統制）」は、弊社HPであるwww.protiviti.comに掲載されている企業改革法404条ガイド（Section 404 guide）の最新版と共にご覧ください。本書は、前述の発行物の内容を補完する内容を記載しました。企業改革法404条コンプライアンスに関る部分については、より詳細に記載しております。

31. 404条コンプライアンスチームはアプリケーション変更管理を検討する際、何を考慮する必要があるでしょうか?

背景

アプリケーション変更管理プロセスは、財務報告に係る内部統制上、重要性が高いプロセスです。アプリケーション変更のインテグリティは、取引処理の正確性、インテグリティ、網羅性、正確でタイムリーな取引の累計と報告に直接影響を及ぼします。

企業が社内のアプリケーションシステムを変更すると、システムやデータのインテグリティが失われてしまうリスクが発生します。このリスクの発生は、正確性、網羅性の問題、または不適切な処理による財務報告への影響の発生可能性を大きくします。財務報告に関連するリスクを低減するために、企業においては、アプリケーション変更管理プロセスを適切に整備し、かつ有効に運用することが必要です。セクション2に記載されているように、適切な変更管理手順は、有効な変更管理とベースラインに基づくテスト戦略の一環として重要な要素です。

変更管理手順は、着手、監視、テスト、承認、承認後の本番環境への移行など、変更サイクルの全ての項目が網羅されていなければなりません。このプロセスは、従業員による不適切、あるいは未承認のプログラム変更または関連するデータの変更を防止するため、適切に保護する必要があります。この変更管理手順は、包括的に構築される必要があり、システムインターフェース、データとエラーのチェックルーチン、アプリケーションセキュリティの変更、経営管理レポートなどの、全ての変更による影響を考慮する必要があります。

財務報告のアサーションへの影響

a) アプリケーションの変更は、取引処理、会計情報の集計と分類及び開示、に関してアプリケーションの網羅性、正確性、インテグリティに直接影響する。

b) 職務の追加、変更、または保護が必要なデータへのアクセス権の追加や変更に伴うアプリケーションの変更は、職務分掌に影響を与える場合がある。

c) 変更管理活動により、従業員による未承認の情報資産へのアクセスが可能となってしまう場合がある。

強いコントロールによる影響

a) アプリケーション機能とコントロールは、ユーザーによって整合性を持って運用される必要がある。質問項目7に記載されているように、変更管理は、処理の網羅性、正確性、インテグリティといったコントロールのアサーションに直接影響を及ぼし、ベースラインによるテスティングの実施を可能とする。

〈注意〉これらのコントロールは、アプリケーション機能が仕様通りに構築されていることを保証する。従って、信頼できる財務報告を行うために、必要なコントロールが各アプリケーションの設計に仕様として組み込まれているかどうかについても評価する必要がある。

b) 変更管理手順は、データのインテグリティに対し妥協をしないことを保証する。

弱いコントロールによる影響

a) プログラムの変更が意図通りにプログラムされたコントロールに対し不利な影響を及ぼさないという保証はない。よって、補完的なコントロールを、評価し、文書化する必要がある。補完的なコントロールは、一般的には発見的、かつマニュアルのコントロールであり、詳細なレベルで実施されなければならない。さらに、アプリケーションにおける変更が不適切であったために生じたエラーを発見するために必要となるコントロールの種類を理解するために、重要なプログラム（例：種類と頻度）への変更については詳しい調査が必要である。

b) アプリケーション変更管理プロセスにおいて、アプリケーションや本番データへのアクセスが適切に制限されないのであれば、データやプログラムへの不注意または意図的な変更を検出するための補完的なコントロールを考慮し、文書化する必要がある。

c) 単に、変更管理プロセスや期中に変更されたコントロールをテストするのではなく、全ての重要なアプリケーションコントロール（例：設定可能なコントロールとセキュリティ）を、SOX法404条コンプライアンスのため毎年テストする必要がある。

---

32. データ管理と障害回復のどの要素をアプリケーションに関連させ評価すればよいでしょうか？

PCAOBの監査基準第2版、別紙C5（リリースNo.2004-001）に説明されている通り、業務継続に関連する事項は、SOX法404条の要件として直接の対象にはなっていません。PCAOBは、非常に限定されたコンプライアンスの意味合いでこの事項を取り扱っています。監査委員会は、業務継続に関連するリスク管理のビジネス的なメリットについては判断をしていません。これに対して弊社は、業務とシステムの運用継続への適切な考慮は、経営上の理由や企業の名誉のために必要だと考えています。詳しくは、弊社が発行している「Guide to Business Continuity Management（業務継続管理へのガイド）」（www.protiviti.comに掲載）にて、重要な事項についてのガイダンスをご覧ください。カトリーナとリタ（ハリケーン）の爪痕が見せたように、財務報告に影響を及ぼすような危機に直面する場合があります。また、大惨事によって、企業が公的な報告期日に間に合わなくなるリスクに直面する「ニアミス」が発生する場合もあります。

以上の議論とは対照的に、データ管理は、包括的なコンプライアンス計画の一環として必要であり、特に企業がSECの委員会ルールと規定に則り、正確かつタイムリーに財務やその他の報告書を作成するために必要です。ここで記載している対象は、データバックアップ、データの復旧、データのリストアに関連する「データ管理」についてです。現在利用できるデータは、企業にとって適切なアプリケーションの使用をする上で不可欠なものです。企業は、取引またはデータのインテグリティと網羅性を喪失しないように、データのリストアまたは処理の再起動をする機能が必要です。

データ管理について考慮する際には、アプリケーションの重要性を考慮しなければなりません。つまり、データバックアップは、正しいタイミングと頻度で実施しなければなりません。データが効率的に保管され、必要に応じてアプリケーションをリストアできることを保証するために、オフサイトでのデータ保管と定期的なリストアテストの準備は重要なことです。重要な四半期または期末など、企業の文書保管規定に則り、バックアップの「スナップショット」を保管することをお勧めします。

---

33. ネットワーク、運用システム、データベースに対するアプリケーションコントロールの有効性についてどのような要素を考慮すればよいでしょうか？

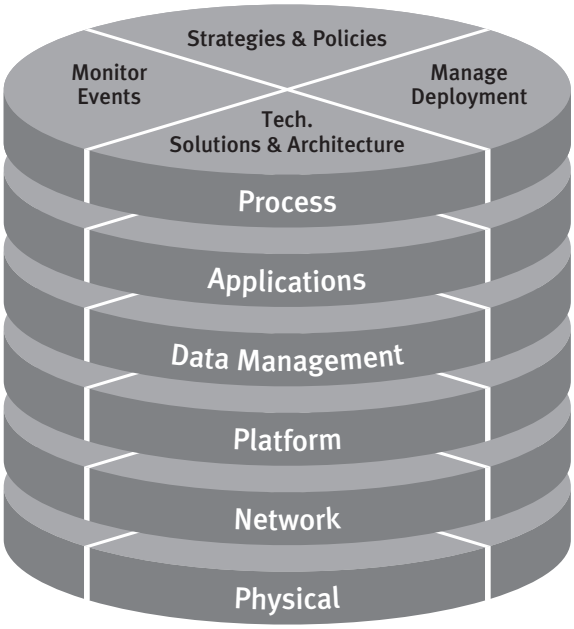
情報処理におけるリスクは、テクノロジー階層体系にあると考えられています。これまで本書で述べてきたように、アプリケーション機能におけるコントロールの有効性は、関連する業務プロセスのコントロールの有効性に寄与しています。同様に、データベース全般に渡るコントロールの有効性は、アプリケーション機能におけるコントロールの有効性に寄与しており、これより下位の階層においても同様となっています。以下は、全般統制におけるコンプライアンスのプロセスにおいて特に注意を払ってレビューすべきインフラストラクチャーの階層の代表例です。なお、このリストは網羅的な記載を意図していません。

データベース（Oracle, SQL Server, DB2など）

- データベースにおいて第一に考慮すべきセキュリティ事項は、セキュリティの目的とアプリケーションコントロールが、その基礎となるデータベース階層の機能によって台無しにされてしまわないことである。例えば、アプリケーションへのログイン手続きを踏まないデータベーステーブルへの直接接続は、十分に制限されるべきである。

- ベンダーは、カスタムテーブルの追加を除き、ERPシステムに対するデータベース体系の変更を禁止している。テーブルにアクセスし、データを作成する場合は、適切な制限をし、変更管理プロセスをもって管理すべきである。

- 自動的にデータを更新または変換（集約、再計算、削除など）



するストアドプロシージャとバッチジョブは、十分にテストされた厳格な変更管理プロセスによって管理されるべきである。

- アプリケーションに対するスーパーユーザーと同様に、データベース管理者（DBA）は、データベースへの多くのアクセス権限が付与されるため、管理者の数を制限する必要があり、可能であれば未承認のデータ変更を監視するべきである。時に、企業は、ITの専門家／DBAによる「データ修正」を必要とするが、修正を加える前に、適切な業務上の承認を変更管理として得る必要がある。

- 特定の静的テーブルや設定オプションは、リスクの影響度によって特別なロギングや監査証跡を保持する必要がある。データベースロギングの適用範囲は、不適切な動作により処理速度やディスク領域を消費してしまわないように、十分考慮しなければならない。

プラットフォームとネットワーク（Windows、XP, UNIXなど）

- オペレーティングシステム（OS）やデータベースサーバには、コントロールすべきリスクが内在している。今日、OSのバージョンアップは、常に変化しているセキュリティの脆弱性に対応していくために欠かせないものである。しかし、OSのアップデートに関しては、データベースまたはアプリケーションが適切に稼働するために互換性を保証する必要があり、アップグレード版を個別に評価をし、インストール前にテストをする。

- アプリケーションが稼働するサーバは適切なアンチウィルスの仕組みを備えている必要がある。

- ネットワークディレクトリ（ファイルシェア）にアプリケーションがアウトプットまたはファイル転送をする場合、データ保管の観点からデータが必要とするセキュリティは、アプリケーションレベル、ディレクトリレベル両方のレベルで必要である。実際には、キーとなるディレクトリの特定と、そのディレクトリ内の重要なファイルへアクセス権を持っているユーザーの定期的なレビューが必要である。

- ID管理ソフトであるマイクロソフトのAvtive Directoryなどを導入することで、企業は従業員が覚えておかなければならないパスワードの数を少なくしている傾向にある。しかしながら、シングルサインオンは、パスワードを書いたメモがキーボードの上に貼り付けられるリスクを低減するが、ネットワークとアプリケーション階層の二重の認証による複数の防衛バリアを排除することになる。よって、このような環境においては、セクション4で記載されている事項をネットワークレベルのコントロールとして導入し、パスワードの要求とその他のユーザーに関連する管理コントロールを実施することが重要である。

物理的セキュリティ

- データセンターへのアクセスまたはサーバが物理的に設置されているロケーションへのアクセスは、十分に制限され、不正アクセスと機器への妨害を回避している必要がある。

- アプリケーションがインストールされている機器は、必要に応じたアップグレード、運用に必要なディスクスペース拡張、データ破壊を防ぐため最適の環境を保つべきである。

---

34. インターフェースにおけるリスクとは何か？また、それらはどのように管理されるべきでしょうか？

インターフェースに関するリスクは、システム間、もしくはシステム内におけるインターフェースが適切に特定、定義、設計、文書化、監視されていない場合に発現します。このようなインターフェースに関するリスクは、データの受け渡しの際に不整合が生じてしまい、その結果として想定できないようなエラーがデータに発生してしまうような事態を引き起こします。インターフェースを有効に設計することによって、こうしたエラーを関連する業務プロセスの早い段階で予防・発見したり、エラーの修正が可能となったりします。また、このような結果として適切なユーザーコントロールの設計が可能となります。インターフェースを適切に構築し、文書化することで、コストを節約した維持管理や何かがあった場合の復元可能性が実現できます。

以上のようなインターフェースに関するリスクは、データに対する未承認の変更を防ぐこと、正確かつ網羅的、適時にデータの送受信

コントロールの目的	リスク	コントロール
アプリケーションコントロールによって、送受信するデータを適切に準備し、処理する。	アプリケーションコントロールが不十分なため、ERPシステム及びレガシーシステムのユーザーが適切かつ適時に必要なデータにアクセスできない。	・アプリケーションはデータを受信して、適切なフォーマットに変換し、変換を確認した後にセッションを開始し、生じたエラーをログとして記録する。 ・エラーが解消された後に再送し、解決内容を記録して、承認する。 ・解消されないエラーについて、インターフェースオーナーに報告する。
システム間のファイル転送で発生した障害を適時に解決するためのインターフェースセッションの再実施と復旧する。	再実施と復旧に関する手順が不適切に設定されることによって、データ処理に必要以上の遅延が生じた結果、多大なコストと従業員の時間を要してしまう。	・インターフェースセッションには、接続状態に問題が生じた場合に、自動的に再実施を行う機能を実装する。 ・ファイル転送時にチェックポイントを設定するようなアプリケーションを利用する。(このようなシステムにおいては、データが受信先と送信元の間で適切に転送されることを確認できるように設定可能) ・転送作業が完了する前に停止または失敗した場合、直前のチェックポイントから処理を継続する。
エラーを適切に解消するため、または適切なエスカレーションを実施するためにアプリケーション間で送受信されたデータのログを記録し、監視する。	データをマニュアルで入力することで人為的ミスが発生しやすくなる。(適切なログの記録と監視が実施されていない場合は、エラーが見過ごされる可能性は高くなる)	・照合作業を含む定期的な編集チェックを実施することで、インターフェース用のファイルが作成される前に不適切なデータを発見する。

を実施すること、そして、エラーを解決する手順を適切かつ適時に実施することによって管理することができます。その他のインターフェースに関するリスクを管理する方法としては、データを受取る側のシステムにおいて、複数回にわたり処理を可能とする方法もあります。上の表は、コントロールの目的と、それに関連するリスクとコントロールを例示したものです。

上表に加えて、インターフェースの設計においては、送信元のデータと受信先のシステム、またはテーブル構造が適切にマッピングされる必要があります。同時に、対象となるアプリケーションシステムで必要とされているレベルでのデータの評価を実施する必要があります。

Section6: 新規アプリケーションの導入に関するコントロールについて

新規のアプリケーション導入または既存システムのアップグレードなどの大きなシステム変更の際には、通常は大きなリスクが存在します。このような場合には、新規またはアップグレードされたシステムだけではなく、既存のシステムに存在するコントロールについても考慮する必要があります。しかしながらこのような場合には、固有のリスクについても考慮しなければなりません。

35. アプリケーションの新規導入に対する主要なリスクは何か？また、それらはどのように管理されるべきでしょうか？

アプリケーションの導入時における主要なリスクは、アプリケーションの複雑性、企業規模、アプリケーションの利用目的、導入の範囲などにより影響を受けます。

重要なアプリケーションの導入に際しては、適切なリスクマネジメントの方法論を用いて、導入時の幅広いリスクを認識し、優先順位を付け、進捗管理していくことが必要となります。なお、このような方法論には、以下のステップが組み込まれるべきです：

1. 導入時におけるリスク管理を実施するために、関連するリスクを評価できるような役割と責任を持つメンバーで構成されるリスク管理チームを編成する。

2. 個別の状況に応じてカスタマイズされた、IRU (Inplementation Risk Universe)を利用して、関連するリスクを特定する。(IRUについては、後述する例を参照のこと)

3. 企業にとっての発生可能性と重要度をもとに、導入時に考慮すべきリスクについて優先順位を決定する。

4. リスク管理のためのアクションプランと優先順位の高いリスクを低減できるコントロールを検討し、それらを全般的な導入計画に組み込む。

5. あらかじめ定義されたリスクが存在する範囲に対する定期的な監視を実施するために、優先順位の高いリスクに関する評価指標を定義する。

6. 404条コンプライアンスチームリーダー及びリスク管理チームメンバーに対して、リスク管理の役割を割り当てる。例えば、特定のリスクとコントロールを認識するためのトレーニングを実施する。

7. リスク管理のためのアクションプランを実施する。

8. プロジェクト管理の一環としてリスクの評価指標を監視し、上記で定義したリスク管理のアクションプランによって優先順位の高いリスクを効率的に認識できていることを日常的にチェックする。

企業における、導入時に考慮すべきリスクは、プロジェクト管理リスク、プロセス／テクノロジーリスク、そして情報リスクとして分類できます。

- **プロジェクト管理リスク**は、通常は以下のようなプロジェクトの構成要素に関連します:

  - プロジェクトの範囲
  - 必要なスキルセットを含む配員
  - 外部の専門家の信頼性
  - システム導入時と本番移行後の役割と責任
  - プロジェクトのスケジュールと進捗
  - プロジェクトにおける課題の特定と対応
  - プロジェクト実施中、またはプロジェクト後のチームメンバーの引き継ぎ
  - システム導入におけるコミュニケーションの実施と期待レベルの管理

- **プロセス／テクノロジーリスク**は、設計、構成、アーキテクチャ、実装、セキュリティ、変更管理、保守とデータのインテグリティといった項目に分類することができます。これらのリスクは、通常は以下のようなシステム導入における項目に関連します：

  - 要件定義
  - プロセス設計
  - 機能設計
  - プロダクトのカスタマイズ
  - プログラム変更とバージョン管理
  - システムとパラメーター設定管理
  - 一時的データとマスターデータ管理
  - 取引データ管理
  - インターフェース
  - セキュリティ構造
  - 機能テスト
  - データ移行
  - エンドユーザーによる受け入れ
  - 責務の変更
  - トレーニングと役割
  - システムの本番稼働
  - 拡張性と信頼性
  - アクセス管理
  - ユーザーサポート
  - 運用保守（バックアップ、バッチ処理など）

- **情報リスク**—新規に導入されるシステムは、意思決定や報告に利用するための情報を提供し、結果としてプロセスのリエンジニアリングにつながることがあります。さらに、システム導入それ自体についても、これを維持管理していくための様々な関連文書が必要となります。情報リスクは、適切に識別され、優先順位付けされ、そして管理される必要があり、これらは以下のような項目に関連します：

  - システムのパフォーマンスに関する評価指標
  - システムに関連する各種文書
  - エンドユーザーのための処理手順書
  - ベースラインに関する文書（キーとなる機能に関する適切な運用の証跡）
  - SOX404法条及び302条を遵守するための関連文書
  - 運用、管理、財務に関する報告書
  - システムから提供されるクエリやその他の情報

---

36. システム導入時のデータ移行に対する主要なリスクは何か？また、それらはどのように管理されるべきでしょうか？

以下に記載されているハイレベルの手順は、データ移行のプロセスに関連するリスクを特定し、評価し、そして管理するための適切な手順と考えられています。古いことわざにあるように、アプリケーションがどんなに適切に稼働しいたとしても、「投入したのがごみなのであれば、結果として出てくるものもごみ」となります。従いまして、導入プロセスにおけるデータ移行の部分は、関連する重要なリスクが受容可能なレベルにまで低減されていることを、適切な注意を払って確認しておかなければなりません。

システム導入前に利用していたアプリケーション（データの移行元）における一時的なデータと過去のデータを、新規のアプリケーション（データの移行先）へ移行する際の計画と実施手順においては、適切なコントロールが考慮されている必要があります。データは、

十分な注意を払って抽出、分析、転送し、データの正確性と網羅性を損なわないように新しいシステムへ適用する必要があります。このプロセスにおいては、データの喪失、破損、または不正な操作が行われた場合に、これを認識するための手順と評価項目が必要となります。担当者は、このような評価項目におけるコントロールが継続的かつ正確に実施されていることを監視できなければなりません。これらを実施するための手順と必要とされる技術は、対象となるデータの大きさ、複雑性、移行するデータの転送能力などの各種の要素に影響を受けます。

以下の手順は、従来までのバッチによる抽出、変換、読み込み処理によるアプローチのモデルです。しかし、ここで推奨しているコントロールの考え方は、様々な形の移行においても適用が可能です。

1. **データの元となるシステムからの正しいデータの抽出**—データ移行においては、データの種類、共通のデータ、そしてデータの総数の確認を含む注意深いデータの分析が必要となります。移行しようとしている現在の数値や残高のデータは、後の比較を実施できるように、保持しておく必要があります。このようなデータの中で、特定のデータの種類については、データ移行が適切に実施されているかどうかを定期的に確認するための評価項目として識別しておく必要があります。これらの評価項目は、「レコードID」として固有のデータ要素であったり、重要な財務要素である「売上」であったりします。また、データ移行の次の手順に進む前に、移行ツール、データツールや、使い慣れたクエリを利用してデータを抽出し、移行対象となっている全てのデータや要素が正しく抽出されているかを事前に保持したデータと比較し確認します。

   もし必要があれば、データの抽出を実施する前に、現在のシステムに存在しているデータについて、データの重複がないか、古いデータがないか、そしてその他のエラーを生じさせるようなデータがないか確認を実施しておくことが必要です。

2. **データの移行先に整合したフォーマットへのデータ変換**—アップグレードの場合を除き、フォーマットや移行元と移行先のシステムにおける項目の一致に関する定義については、移行元におけるどの項目が、移行先のどの項目にならなければならないのかについて確認しておく必要があります。このデータマッピングの正確性と網羅性については、特に重要な作業であり、データが単に移行されることの保証だけではなく、各要素が正しい場所に移行されるかどうかを確認することが非常に重要です。このためには、マッピングに対する業務側のユーザーレビューと承認が、正確なデータ移行とデータ移行結果をユーザーが受入れるための重要な要素となっています。

3. **移行先のシステムにおけるデータのアップロード**—データ移行ロジックやデータ移行において起こりうる課題を解決するためには、移行プログラムとその手順の試行を何度も実施してみる必要があります。様々なデータを読み込む際の順番は、データの相互依存性とデータの関連（例：発注書のデータを移行する前には、仕入先マスタのデータの移行が必要）を考慮して、注意深く計画し、実行する必要があります。アップロードが完了した後には、移行先のシステムにおける評価項目について、移行元のシステムの関連する項目と比較して、想定する全てのデータが正しく移行されていることを確認する必要があります。この結果として、対象となったデータの一部については、原則的な移行プロセスにおいて上手くいかない場合があります。このようなデータについては、別途マニュアルの「データ修正」手順によって、その他のデータと同じレベルでのデータの網羅性と正確性を保証する必要があります。

4. **データ移行後のユーザー／管理者による受入**—データ移行におけるITを基礎としたコントロールは、移行されるデータの網羅性（例：全ての項目とデータについて整合が取れているか?）に関連しています。また、特定の数値について、その内容が正確に保持されていることを確認するため、システム的に比較を実施している場合があります。しかしながら、正確性についての確認は、ユーザーまたは管理者によって実施されることが必要となる場合があります。このような場合、ユーザーまたは管理者は、データの比較に関するレポートを用いたデータの内容に問題がないかのレビュー、そして、移行先の新規システムから出力されたレポートを用いたデータの互換性に関する問題や明らかなエラーやデータの欠落がないかどうかのレビューを実施することが必要となります。この作業を大雑把に一見するだけにとどめないためには、ユーザー受入時には正式な承認を得て、その証跡を残しておくことが推奨されます。

5. **データ移行に関連する文書の保持**—財務関連のデータは、企業の公正かつ正確な財務状況を表すものであるため、データ移行は内部監査、外部監査、そしてSOX法コンプライアンスのための重点的なポイントになります。従いまして、データ移行が正確かつ網羅的に実施されたことを証明するための処理結果は、今後においてもレビューが実施できるように保持しておくことが必須となります。データ移行に関連する文書とは、移行前の状態に関する情報、比較用の移行後の状態に関するレポート、データマッピング、ユーザー受け入れに関する承認とその確認書、テスト及び実施した確認を証明する文書、移行プログラムに関する変更管理に関する情報などが例としてあげられます。

なお、その他のアプリケーションにおけるデータ移行や関連するインターフェースへの影響についても十分に考慮する必要があります。例えば、相互依存の関係にある環境での変更の際は、新規システムにおけるデータ特性を十分に考慮しておく必要があります。

37. 新規アプリケーションの機能テストにおける重要なリスクは何か？また、それらはどのように管理されるべきでしょうか？

新規アプリケーション導入時において、アプリケーションコントロール（必要性についてはセクション8をご参照ください）のテストを実施する際に最も気を付けなければいけないのは、対象となるアプリケーションの機能が意図した通りの結果を生じさせる設定となっていること、もしくは、意図せざる結果が生じたときにはこれを事前に予防し、あるいは適時に発見できるような設定がなされていることを確認することです。よって、企業は、処理が意図された通りであった場合（積極的保証）、及び処理が意図された通りではなかった場合（消極的保証）の両方を適切にテストできるような手法を用いる必要があります。これらのテストのタイプについては、以下の通りです:

- **積極的保証**のテスティングでは、コントロールまたは機能という観点から、アプリケーションが意図通りに処理されることを確認します。例えば、外国通貨による取引において、取引で使用された外貨額が正しく国内通貨またはその他の所定の通貨による金額に変換され、適切な勘定科目を用いて記帳されていることを確認します。その他の例としては、発注書の金額が200,000円以上ならば適切な承認が必要な場合において、金額が200,000円以上で適切な承認がなされた発注書については、登録が完了することを確認します。

- **消極的保証**のテスティングでは、コントロールまたは機能という観点から、アプリケーションが意図された通りではない場合には処理がエラーとなることを確認します。例えば、転記処理において、貸借が一致していない場合には、処理が中断され、エラーメッセージが表示されることを確認します。その他の例としては、発注書の金額が200,000円以上ならば適切な承認が必要な場合において、金額が200,000円以上で適切な承認がない発注書については、登録が完了しないことを確認します。

Section7: 文書化

文書化は、財務報告に係る内部統制の評価において重要な意味を持ちます。このセクションにおける質問項目に対する内容は、組織レベルとプロセスレベルを含む様々なレベルでの文書化のガイドラインを示しています。ITに関連するリスクとコントロールの文書化は、SOX法404条コンプライアンスチームによって設定された全体的な基準とアプローチに準拠する必要があります。なお、文書化は同時に外部監査プロセスにおいて必要とされる要件も満たしている必要があります。

38. 404条コンプライアンスチームは業務プロセスにおけるITコントロールについてどの様に文書化すれば良いでしょうか？

アプリケーションオーナーやデータオーナーによって管理されている業務プロセスの文書化においては、フローチャートとリスクコントロールマトリックス（RCM）の形式で文書化することが最も適切だと考えられています。セクション2に記載されている通り、業務プロセスにおけるアプリケーションレベルのコントロールは、各業務プロセスのリスクとコントロールを統合した形で文書化されることが最善です。実際のところ、このように各業務プロセスにアプリケーションコントロールを反映することは、ITの内部統制に対する依拠の度合いを理解する最も良い方法となっています。つまり、アプリケーションコントロールについて、ITの専門家が必要に応じてレビューとテスティングを実施するためには、業務プロセスにおけるどのコントロールがアプリケーションを利用したコントロールなのかを明示しておくことが必要となっているのです。その他の文書としては、キーとなるアプリケーションに関連するシステム構成図、データフロー、業務プロセス・アプリケーション関連表、そしてキーとなるアプリケーションのコントロールにおける考慮事項をまとめた表といったものが追加で必要となります。なお、キーとなるアプリケーションコントロールにおける考慮事項には、システムにおける計算の複雑性、キーとなるデータの妥当性や正確性のチェック、重要または複雑なインターフェースなどが含まれます。このような文書化を実施するためには、適切なスキルセットが必要となります。

39. IT部門、アプリケーション・データオーナーが用意すべきコントロールと重要なアプリケーション機能の証拠書類はどれくらい必要でしょうか？

この質問については、二つの種類の文書を考慮する必要があります。第一に、アプリケーションプログラム及び関連するコントロールが有効に機能していることを立証できるような文書、第二に、アプリケーションプログラム及び関連するコントロールが有効に機能することを継続的に担保するためのシステム上の要件が記載されている文書です。

第一の文書では、主要なアプリケーションの機能がどのようなプロ

セスで、どのように運用されるかについて明らかにする必要があります。質問項目38で記載されているように、主要なアプリケーションの機能には、重要なアプリケーションコントロールを含みます。これには多くの文書が含まれることになりますが、例えば、フローチャートや業務概要記述書、プログラム処理のステップを記載したフローチャート、データの関連とデータベースの設計などの技術的な要件を記載した文書などが挙げられます。

第二のシステム上の要件が記載されている文書には、対象となるシステムについてはまだ十分な理解が得られていないようなプログラマーが、対象プログラムの機能や重要なインターフェース要件、データ処理要件、セキュリティ要件などについて理解できる程度の詳細さが必要です。このような文書には、対象となるアプリケーションの保守を実施するにあたって必要とされる基本的な情報についても記載される必要があります。

基礎となるソースコードやデータベースのシステム上の要件定義書のみでは、ほとんどの環境において十分な文書とはなり得ません。また、アプリケーションに関する文書が不十分である場合、当該アプリケーションの変更が適切に行われないというリスクが高くなります。そして、もしこのようなリスクが存在する場合には、変更管理において不備が発生する可能性を考慮しておかなければなりません。

40. PCAOBの監査基準第2号には取引の「開始、記録、処理、報告」が記載されていますが、取引フローの文書化はどのように行うのがよいでしょうか?

取引のフローを文書化するために最も良い方法は、アプリケーションとデータフローを図示した文書を作成することだと考えられています。これらの図は、企業が利用している様々なアプリケーションについて、取引の始まりから財務諸表の作成及びその開示にいたるまでを重要なデータフローとして明示することができます。このような図については、まずは概要のレベルから記載して、徐々に重要な取引とアプリケーションを詳細に記載していくことになります。詳細な記載においては、取引におけるインプット、処理内容、アウトプットを記載することが重要です。なぜなら、PCAOBは、外部監査人に対してウォークスルーを実施することで、企業の「重要な業務プロセス」について確認することを要求しているからです。

Section8
テスティング

業務プロセスのコントロールと同様に、ITに関連するコントロールについても、整備された通りに運用されていることを確認するテスティングを実施する必要があります。テスティングについての詳細は「Guide to the Sarbanes - Oxley Act：Internal Control Requirements（米国企業改革法：内部統制の報告要件）第3版」に記載されています。以下では、その中から関連する内容を記載していますが、必要に応じて、アプリケーションコントロールのテスティングに関連する事項を追記しています。

41. ITコントロールはどのようにテスティングするのでしょうか?

ITに関連するコントロールについては、業務プロセスにおけるコントロールと同様な方法でテスティングを実施します。テスティングにおいては、適切な質問、観察、検査、再実施といったテスト手法を使用します。全ての場合に、テスティングに関する十分な文書を作成する必要があります。このようなテスト手法を組み合わせることによって、運用状況の有効性に関する結論を適切に得ることができるようになります。

ITに関連する組織レベルのコントロールについては、通常、再実施のテスト手法で評価を実施することができないため、質問、観察、または検査のテスト手法を用いて実施することになります。IT全般統制に関連するコントロールやアプリケーションコントロールまたはデータオーナーによるコントロールについては、再実施を含む4つ全ての種類のテスト手法を用いてテスティングを実施します。これらのプロセスにおいて、プロセスレベルのコントロールは、各プロセスが適切に完了したことを示す証跡が得られるように整備することが必要となります。（例：書類への署名やその他のサインなど）

42. 誰がシステムコントロールのテスティングを実施するのでしょうか?

システムコントロールのテスティングは、関連する業務プロセスのオーナーが内部監査人の立会いのもとで実施します。これらのコントロールは、入力された内容がどのように承認されるか、または特定の業務データがどのように処理されるかを制御しています。なお、ほとんどの場合、内部監査のITチームは、システムコントロールが機能するためのトリガーとなる事象を適切にテストパターンとするための業務プロセスの知識がありません。しかしながら、システムコントロールをテスティングする担当者は、テスト対象となっている業務プロセス、関連するシステムコントロール、そのコントロールの目的、またコントロールが機能した場合にシステムがどのような処理を実施するかについて理解しておくことが必要です。従いまして、企業は、有効かつ正確なテスティングを実施するために、アプリケーションコントロールの専門家を関与させることを考慮する必要があります。質問項目43では、アプリケーションにおいて設定されたコ

ントロールを効率的にテスティングするための自動化されたテストツールについて記載しています。

43. アプリケーションコントロールはどのようにテスティングするのでしょうか?

質問項目3においては、業務において利用されているアプリケーション及び取引における処理に関連する6種類の異なるタイプのアプリケーションコントロールについて記載しています。このようなアプリケーションコントロールについて、関連するアプリケーション及び業務プロセスにおけるテスティングを効率よく実施するためには、異なるテスト手法やテスト手続きを織り交ぜて実施することが必要となります。以下においては、「アプリケーションコントロール」として通常定義されている最も一般的な二つのコントロールタイプである、アプリケーションの処理ロジックに関するシステムコントロールとセキュリティコントロールについて説明します。これらのアプリケーションコントロールをテスティングする際の主な手法としては、自動化されたツール（詳細はセクション10を参照のこと）を用いる方法とマニュアルによる確認方法があります。

- **マニュアルによるテスティング**—「最も簡単な」アプローチとされています。しかしながらこの方法は、コントロールが有効に機能していることを確認するための十分な証跡を入手するために様々なテストパターンを考慮しなければなりません。また、テスティングにおいては、多くのコントロールが対象となるため、多大な時間を要し、実施するのが困難な方法となる場合があります。さらに、質問項目37で記載しているように、積極的保証と消極的保証の両側面からテスティングを実施する必要があります。このように、関連するテストケースを網羅的に作成し、これに従って適切にテスティングを実施して、業務担当者から情報を入手し、そしてテスト結果を適切に解釈するためには、十分なスキルセットと関連する深い知識が必要となります。また、この方法は、テスティングの実施者が本番環境に対して不適切な影響を及ぼさないように、本番環境と同期の取られた環境においてテスティングを実施することが多くなっています。最後に、マニュアルによるテスティングは、一般的に人によって実施される場合と同様に、人為的なミスが発生するリスクが高いと言えるでしょう。但し、これらの欠点により、マニュアルによるテスティングにおける長所が失われてしまうわけではありません。事実、多くの企業がマニュアルによるテスティングを実施し、成功しています。しかしながら、多くの企業は、アプリケーションのデータやテーブルを利用したテスティング、ツールを用いたテスティングの方法を積極的に採用することで、テスティングに要する負担を大幅に削減し、テスティングの有効性を改善することが出来ると考えています。これらの方法に関しての詳細は、以下に記載しています。
- **アプリケーションのデータやテーブルを利用したテスティング**—アプリケーションによっては、特定のコントロールが適切な方法で設定されていることが確認できる証跡として、一定のデータテーブルを抽出できる機能が実装されています。場合によって監査人は、このようなデータテーブルからサンプルを抽出して、対象となるアプリケーションのデータテーブルが適切に設定され、有効に運用されていることを確認するための「スコープテスト」を実施することがあります。
- **ツールを用いたテスティング**—多くの場合、ツールを用いたテスティングを実施することで、企業のテスティングへの負担を少なくし、その効率性を向上することができます。このようなツールは、アプリケーションのパラメーター設定情報を抽出することが可能であり、そしてあらかじめ定義され、想定された結果に基づいて自動的にデータを分析します。ツールによるテスティングの実施は、取引レベルの業務ルールが定義されることによって、特定のコントロールの運用状況の証跡となります。最後に、ルールに基づいた「継続的な監視」を実施するためのツールを用いることで、あらかじめ定義されたパラメーターの設定変更、そして企業にとってリスクが高いと想定されるような特定の取引を監視することができます。これらのツールは、従来のマニュアルによるテスティングのアプローチよりも広い範囲を対象としています。

このようなテスティングのためのツールは、「特効薬」ではありません。アプリケーションの開発・導入時また稼動初期には、パラメーター設定の詳細要件、知識に基づくスキル、経験、さらにテスティングの目的について熟知している必要があります。しかしながら、適切な専門的スキルを有する担当者によって正しく設定され、利用されるのであれば、このようなテスティングのためのツールは、評価プロセスを著しく効率化し、付加価値を与えることになります。これらのツールについての詳細は、質問項目10に記載しています。

Section9: アプリケーションコントロールの不備の発見と報告

内部統制における不備が発見された場合、不備の重要度により改善が必要です。内部統制における不備への対応については、「Guide to the Sarbanes - Oxley Act：Internal Control Requirements（米国企業改革法：内部統制の報告要件）第3版」に記載しています。以下では、その中から関連する内容を記載していますが、必要に応じて、アプリケーションコントロールのテスティングに関連する事項を追記しています。

44. アプリケーションコントロールの不備、ギャップに対し管理者はどのように対応すべきでしょうか?

アプリケーションコントロールの不備に対応するには、2種類の方法があります。第一のアプローチであり、かつ最も分かりやすいのは、プロセスまたはコントロールの整備状況または運用状況が有効ではない部分についてのギャップ分析を実施し、発見されたギャップを解決するための改善計画を策定することです。第二のアプローチは短期的な対策として適切であると考えられており、不備及び関連する補完的コントロールに対する徹底的なリスク分析を実施し、財務報告のアサーションに関連するリスクの範囲やリスクが十分に低減できるかどうかについて判断します。なお、この手順は短期間で実施することが重要です。なぜならば、こうしたギャップ分析とギャップ分析結果への対応は、時間を要し、このような対応においてはITコントロールにおける不備を修正しなければならないことが多いためです。多くの場合、業務プロセスレベルにおけるエラーまたは不作為が生じた場合に、これを識別し修正するための発見的なマニュアルコントロールを多数追加しなければならない結果ともなります。取引量が多いまたはとても複雑な取引の場合は、非常に困難かつコスト負担の大きい結果を招くことになります。

45. 外部監査人は監査過程においてアプリケーションコントロールをどのように考慮するのでしょうか?

この質問は、各外部監査法人がそれぞれのクライアントに説明するべき事項です。なぜなら、外部監査人が、経営者の内部統制に関する宣誓を評価する場合には、ITに関連するリスクとコントロールを念頭においていることが前提と思われるからです。2004年の終盤に、Big4を含む9つの監査法人が、「A Framework for Evaluating Control Exceptions and Deficiencies（コントロールにおける例外事項と不備の評価のためのフレームワーク)」を発表しました。このフレームワークは、IT全般統制とアプリケーションコントロールが財務報告の信頼性に対して、どのような影響を及ぼしているかについての監査法人の見解が記載されています。通常監査法人は、「IT全般統制は、直接的に虚偽報告にはつながらない」としています。一方で、アプリケーションコントロールは、重要な影響を及ぼす可能性があると考え、「アプリケーションコントロールの不備は虚偽報告につながる」としています。IT全般統制の欠陥は､これがアプリケーションコントロールへ影響を及ぼすことによって、間接的に重要な取引と勘定科目に影響を及ぼす可能性があります。従いまして、IT全般統制の欠陥は、広範囲において影響を及ぼす可能性があり、経営者による財務報告に係る内部統制評価と外部監査人のその評価に対する監査を困難にするため、改善する必要があります。

例えば、時として外部監査法人は、彼らのクライアントに対して、セキュリティ管理やユーザーアクセスといった観点から、セキュリティについてより強く、より広範囲にわたるコントロールを導入することを求めてきます。このような結果から、SOX法404条コンプライアンスチームは、IT全般統制とアプリケーションコントロールを含めたITコントロール環境において、出来るだけ早く、関連するプロセスにおいて対応しなければならないギャップがあるのかどうかを評価する必要があります。このような評価が適切に実施できない場合、企業における外部監査が実施できないといった結果を招いてしまう可能性があります。

Section10:
ERPのコンプライアンスソフトウェアと自動テスティングツール

46. SOX法対応においてどのようなソフトウェアを使用するのがよいでしょうか?

ベンダーは、5つのカテゴリに分けることができます。

- **ERPコンプライアンスアプリケーションと文書の格納**—ソフトウェアとしては、Oracle E-business SuiteのInternal Control Manager（ICM)、People SoftのInternal Control Enforcer（ICE)､そしてSAPのManagement of Internal Controls（MIC）などがあります。
- **ERPコンプライアンスとテスティングソリューション**—製品提供を行っている企業として挙げられるのは、Applimation、Approva、Consul、CSI、D2C、LogicalApps、PCI、QSmart、Qsoftware、Virsaなどです。
- **リスク管理と内部監査ソフトウェア**—PaisleyのRisk Navigator、AutoAudit、ProtivitiのGovernance Portalなど。
- **文書管理**—Documentum、Stellentなど。
- **業務プロセスの自動化**—Certus、HandySoft、OpenPagesなど。

多くのERPシステムは、統合的なコンプライアンスツールを開発しています。さらに、多くのソフトウェアベンダーが、新しい製品を市場に提供しています。ソフトウェアの評価する際に、企業は、機能要件と共に固有のビジネス要件を考慮する必要があります。例えば、企業が複数のERPシステムを利用している場合、複数のプラット

フォームに対応しているソフトウェアを選定する必要があります。どのようなソフトウェアを購入する場合においても、固有のハードウェア要件も考慮しなければなりません。また、経営者は、最終的な判断において、既存のインフラも考慮する必要があります。例えば、全面的なERPシステムの利用は、コンプライアンスソリューションとして活用できる可能性があります。同様に、ある特定ベンダーの文書管理ソリューションを使用した場合、ガバナンスが向上する可能性があります。

本書に記載されている通り、自動評価ツールは、「特効薬」ではない、と理解することは極めて重要です。如何なるソフトウェアパッケージにおいても、個々の環境において効果的な結果を保証するためには、プランニングとセットアップにかなりの労力を費やすことになります。これらのツールの購入を検討する場合、企業は以下の事を考慮しなければなりません。

- 十分な時間と労力をかけ、評価ツールより出力された初期結果を検証する必要があります。多くの企業は、評価ツールより出力された初期結果に圧倒されます。プロセスやコントロールの継続的な改善のために、例外処理の根本的な原因や評価結果を分析しなければならないことを、初期の段階で理解しておくことが大切です。

- 統制環境を継続的に向上させるために、現行のプロセスとツールを統合させる必要があります。問題の根本的な原因が特定されず、解決されないままになっており、プロセスの向上や予防策がなされていない場合、年次の評価では、毎年同じような結果となります。

- ツールを導入、設定、活用する担当者は、ツールの知識のみならず、評価対象のアプリケーション、対象業務プロセス、及び関連するリスクとコントロールに関しても理解していることが重要です。

---

47. SOX法コンプライアンスをサポートするツールの評価をするにあたり、どのような質問をすればよいでしょうか?

ツールの評価を実施するに当たって、テスティング、監査、文書保管、プロジェクト管理、その他の関連事項などについて考慮しなければならない質問事項は、いくつか存在しますが、ここでは特に重要だと思われる質問事項を記載しています:

現在利用しているツールは、コンプライアンスに関する情報を適切に保管していますか?

ツールの情報は、企業が必要な情報にアクセスが柔軟に対応できるよう構造化されている必要があります。この情報構造によって、財務報告における様々な観点から見た、コントロールの運用状況の有効性を理解することができます。例えば、ツールは、複雑な関連性の中で、リスクとそれに対応するコントロールを強く関連付ける必要があります。一つのコントロールが複数の財務報告に係るアサーションに対応する場合などがそれに当たります。また、ある特定の業務分野におけるコントロールが、他の業務分野において認識されているリスクと対応することもあります。言い換えれば、コントロールポイントは、業務プロセスにおけるリスクの発生地点に存在していると同時に、その発生地点の上流または下流にも存在していることがあります。ツールは、こうしたリスクとコントロールを適切に結びつける必要があります。

さらに、こうしたツールのベースとなる情報構造は、様々な組織レベルや業務プロセスレベルでの文書化が可能となる必要があります。ある業務活動は、二つの階層のみに関連することになるかもしれませんし、ある業務活動は第三階層、または第四階層といったより詳細なレベルに関連することになるかもしれません。こうした業務活動に対応するために、情報保持の体系は複数階層を持つような体系で整理されることが必要となります。

ツールは、業務担当者のコンプライアンス活動に対する関与を促進していますか?

状況に応じて、エンドユーザーもコンプライアンス活動に参加する必要があります。その際には、例えば以下の四つの観点を考慮する必要があります:

1. ツールは、重要なコンプライアンス活動（例:テスティング、文書化、評価、改善）に関連する作業をサポートする必要があります。

2. ツールには、302条の宣誓、四半期報告に関するレビュー、または404条に関する組織レベルのレビューなど、様々なコンプライアンス活動に関連する継続的な自己評価をサポートする仕組みが組み込まれている必要があります。また、その他の活動としては、倫理規則への抵触といったSOX法に関連しないような項目についての評価活動が含まれ、これらについてもツールでサポートされる必要があります。

3. 自己評価を実施する場合、自己評価に関連する作業において、割り当てられた評価の役割が各担当に対して連絡される機能がシステムに組み込まれている必要があります。このような連絡は、タスクの完了、改善活動の実施、または例外事項の発生に伴って行われます。

4. ツールには、エンドユーザーによる操作を簡略化するため

のナビゲーションによるサポートが必要です。

ツールは、変更管理を支援していますか？

情報を保持することによって、企業の統制環境に関する履歴が保持されます。従いまして、変更履歴を保持し、変更管理を実施することが非常に重要な要素となっています。そこでツールでは、文書のバージョン管理のサポートや、リスクとコントロールに関する情報が変更された場合の監査証跡の提供、そして、ある時点において保管された評価結果の情報をユーザーへ提供する必要があります。また、ユーザーの担当業務の範囲において、必要な役割のみが実施できるように利用を制限するための、適切に階層化されたセキュリティ構造を実現している必要があります。

ツールには、十分なレポート作成の機能がありますか？

レポート作成の機能では、財務報告に関わる全般的なアサーションの達成をサポートするための情報が提示される必要があります。レポート作成の機能は、すべての集大成となっています。ツールで利用可能な全ての重要な情報を抽出する際の一時的なデータ整理機能だけでなく、ドリルダウン機能が付加されたサマリーレポートやグラフィカルなレポートが必要とされています。さらに、エンドユーザーが特定のデータを引き出せるような柔軟な条件設定や検索機能が必要とされています。最終的には、業務担当者が誤ってデータのインテグリティを損なってしまうのを防ぐようなセキュリティ機能が必要になります。

ツールは、コンプライアンス活動を意図した通りに管理するために役立っていますか？

コンプライアンスのためのツールを選定する際には、業務プロセスを集中して管理しているのか、または分散して管理しているのかについて考慮しなければなりません。もし、分散して管理されているのであれば、業務の流れとセキュリティといった要素が非常に重要な意味合いを持ちます。逆に、集中して管理されているのであれば、これらの要素の重要性は低くなります。

また、ツールを選定する際には、コンプライアンス活動をどのように改善するのかを正しく理解する必要があります。例えば、どれだけのデータが「一度限り」の設定で利用可能となるのか、それとも、翌年のコンプライアンス活動の際、再設定する必要があるのかということです。その他の例としては、特定された例外事項が、複数回に渡るレビューにおいて存在しているものなのか、それとも初めて特定されたものなのかを区別するための分析が可能かどうかということです。

推奨するツールは、すぐに利用できますか？ 一般的に、ツールのどのような部分について設定が必要となり、または設定が可能となっていますか？

何よりもまず、ツールは、ユーザーによって簡単に設定可能であり、さらに、大掛かりなカスタマイズが不要であることが重要です。一般的に、設定の柔軟性が要求される範囲は、以下の通りです：

- サポートされている階層のレベル（例：必要な組織階層やプロセス階層は、企業によって異なる。）
- ドロップダウンを利用した選択機能（例：値リスト）
- 自己評価における質問項目の内容
- コンプライアンス活動において、必要とされる業務の流れ
- あらかじめ設定されたシナリオ、ユーザーが定義する項目

従って、設定の柔軟性が高いツールが求められます。多くのカスタマイズが必要となるツールは、高価で保守が困難となりますが、レポート機能のカスタマイズは、ツールによってサポートしておくことが必要となります。

監査人は、ツールやその分析結果を信頼することができますか？

コンプライアンスツールにおいては、これを取り巻く様々な関係者についても考慮しなければなりません。SOX法コンプライアンスに関連するソフトウェアを選定する場合は、外部監査人からの要求事項を考慮する必要があります。もし、外部監査人が推奨している特定のツールや、既に彼らがテスティングの際に依拠できると「認定した」特定のツールが存在するのであれば、これはツールの導入後におけるコンプライアンス活動の全体的なコスト削減に役立つかもしれません。もし、導入したツールがERPシステムにおいてユーザーアクセスを管理するために必要不可欠なものになっているのであれば、それ自体がキーコントロールして識別され、SOX法コンプライアンスのためにテスティングが必要となってくることに注意を払う必要があります。

---

48. 404条コンプライアンスチームは、ERPシステムのSOX法に対応するコントロール（文書化とテスティングが必要）とSOX法コンプライアンスのためのソリューションとの関連付けをどのように行えばよいでしょうか？

両者は異なる概念ですが、時に混乱を招くことがあります。アプリケーションコントロールにおける考慮事項（セクション3に記載）とSOX法コンプライアンスのために設計されたアプリケーションの機

能における考慮事項には明らかな相違があります。これらの混乱は、今日、多くの主要なアプリケーションベンダーが、SOX法コンプライアンスのためのソリューションを提供しているからです。

SOX法コンプライアンスのためのソリューションとツールは、SOX法に対応するコントロールとして機能するわけではありません。しかしながら、アプリケーションや業務プロセスに存在するキーコントロールの特定、文書化、そして評価の実施を可能とします。これらは、コンプライアンスのための作業において重要なポイントとなります。コンプライアンスのためのソリューションは、業務の流れや業務処理の実施や完了に関する結果報告が適切になされるようにその実施を促進します。コントロールを時間とともに最適化していくために企業は、コンプライアンスチームが保持している文書において記載されたコントロールを、実際に業務プロセスにおいてコントロールとして認識されているポイントと関連付けていきます。このような作業は、ERPシステムにおける自動文書保存機能やその他の様々なERPシステム以外のアプリケーションを用いることによって実現可能です。

プロティビティ ジャパンについて

米国において、企業エグゼクティブの人材派遣の先駆者であり、全米で100万人の登録者を有する最大手のRobert Half International Inc.（RHI：NYSE上場）が、新たなビジネス戦略の柱として、2002年6月に解散した米Arthur Andersen LLP. のリスクコンサルティング部門を、メソドロジ、データ等を含め1億ドルで買い取り、ビジネス並びにITに関するリスクコンサルティングと内部監査を専門とする会社をProtiviti Inc.として2002年に設立しました。プロティビティ ジャパンは、アンダーセンのメンバーファームであった監査法人のリスクコンサルティングの人材を中心に、グローバルファームであるProtivitiのアジア・パシフィックの拠点として2003年2月に設立されました。現在は、世界各国で54ヶ所の事務所と2,300名のコンサルタントが稼動しております。特に、最近ニーズの高まっている内部統制コンサルティングにおいては、国外で数百社、国内においてもSEC登録企業の中で、12社のお客様への米国企業改革法（US-SOX）対応支援コンサルティングをご提供させて頂いており、金融庁の内部統制法制（通称：J-SOX）対応支援コンサルティングに関しても、多くの実績を積み重ねてきております。世界レベルのナレッジで皆様を効率的かつ効果的にご支援させて頂くことを目標としております。

■ ビジネスリスク（Business Risk）

- 全社的リスクマネジメント（ERM）サービス
- 財務リスクマネジメントサービス
- 内部統制法制対応支援サービス
  - ・内部統制ガイダンス・研修プログラム
  - ・内部統制文書化支援
- 米国企業改革法（Sarbanes-Oxley Act）対応支援
- 金融機関向けサービス
- 環境リスクマネジメントサービス

■ テクノロジリスク（Technology Risk）

- セキュリティ＆プライバシーリスク関連サービス
- 内部統制法制IT対応支援サービス
  - ・IT全般統制
  - ・ITアプリケーション統制
- アプリケーションコントロール評価支援サービス
- プロジェクトリスク管理サービス
- テスト支援サービス
- コンティンジェンシープラン・業務継続計画関連サービス

■ 内部監査（Internal Audit）

- 内部監査アウトソーシング・コソーシングサービス
- 内部監査高度化支援サービス
- 情報システム内部監査サービス
- コントロール・セルフ・アセスメント（CSA）プログラム導入支援
- 内部監査品質評価サービス

■ リスクテクノロジ・ソリューション（Risk Technology Solution）

- Pro-i（Protiviti Internet Service）
  - ・iTraining（eラーニングサービス）
  - ・iAssessor（自己診断支援サービス）
- プロティビティ ジャパン標準RCM（リスクコントロールマトリックステンプレート）
- SarbOx Portal™（内部統制構築・評価支援ツール）
- The Self-Assessor™（CSA支援・セルフアセスメントツール）
- AutoAudit®（内部監査支援ツール）

■ アプリケーションコントロール評価支援サービス（ACE）

プロティビティ ジャパンのACEサービスは、全体的な観点から企業のセキュリティとプライバシーに取り組みます。我々は基幹業務プロセス、規制、そしてお客様の事業戦略を支えるテクノロジーをまず理解します。その次に、我々の専門知識と、様々な手法やツールを用いた構造的アプローチを通じて、持続可能な対策を実施します。我々のアプローチでは、以下の項目を実施します。

- **導入プロジェクトのリスク管理 ― アプリケーション開発ライフサイクルにおけるリスク管理**
- **システムコントロールの最適化 ― 最適なマニュアルコントロールからシステムコントロールへの移行**
- **セキュリティと職務分掌の強化 ― セキュリティ管理プロセス、SoDフレームワークの構築**
- **モニタリングツールの導入 ― 内部統制とコンプライアンスの監視ツールの導入**
- **コンプライアンス評価支援 ― 文書化とテスティングにおける専門知識とツール利用による効率化**

プロティビティ ジャパンのACEサービスは、技術面とビジネス面のプロセスに関する専門知識をもとに、ERPベンダーとのリレーションを保ち、お客様のERPシステムがより内部統制に役立つようお手伝いします。

MEMO

株式会社プロティビティジャパン
〒100-0004 東京都千代田区大手町1-1-3 大手センタービル
T. 03・5219・6600［代表］ F. 03・3218・5533

PJ.D.06113T

protiviti.jp