

情報技術関連のリスクと統制：知っておくべきポイント

最近、企業の情報開示ならびに内部統制の問題が議論のテーマに上り、企業改革法（SOA：サーベンス・オクスレー法）第302条ならびに第404条への準拠が、特に重要な問題として扱われている観がある。こうした背景の中で、企業の情報技術（IT）に対する統制の問題はどのように関係してくるであろうか。なぜITは重要なのか。なぜ企業の取締役や経営者はITに対する考慮が必要なのか。本号のBulletinでは、IT関連のリスクおよび統制に係るこれら幾つかの疑問に対して回答を試みることにする。

ITの観点から何が求められているか？

企業の財務報告に係る内部統制を評価する際には、情報技術がもたらす影響を慎重に検討する必要がある。それは検討すべきIT固有のリスクがあるからである。このIT固有のリスクは情報処理ならびに関連データの信頼性、完全性、可用性に多大な影響を与えるため、そうしたリスクを軽減するための統制が極めて重要になる。

ITに対する統制とは何か？

情報技術関連のリスクならびに統制は、トップダウンにより評価が必要とされる。ITに対する統制には全般統制とアプリケーション統制の二つがある。

全般統制とは、通常、IT環境における複数のアプリケーションに影響を与えるもので、特定の事象が情報処理またはデータの完全性に影響を与えるのを防ぐことを目的としている。コンピュータの稼働、物理的・論理的セキュリティ、プログラムの変更、システム開発、事業継続性などは、全般統制が適用されるプロセスの例である。これらの全般統制は、企業が財務報告上の目的を果たす上で影響を与えるもので、それが事業プロセスの多くと密接に関係しているため、対象が「極めて広範囲にわたる」ことになる。

アプリケーション統制とは、個別の事業プロセスに係る具体的な強い統制である。このタイプの統制には、アプリケーションやデータの個々の責任者が各事業分野で設計、実施する各種の方針や手続きが含まれる。

またこの統制には、アプリケーション内で実施されるいわゆる「プログラム機能」も含まれる。このプログラム機能は、入力されたデータが間違っていないかを自動検証、数値がエラーにより間違っているかを自動検証、必須入力項目の検証、想定されないデータが入力された場合の発見、例外事項に伴うフォローアップなど、具体的な統制活動を実践するものである。

ITに対する統制はなぜ重要なのか？

情報技術は企業の財務報告プロセスにおいて重要な役割を果たしている。アプリケーション・システムの中では数多くの経済的事象が捉えられており、処理された情報がアプリケーションによって統合、報告され、財務諸表を作成するための基礎が形成される。例えば、長距離電話会社の売上報告プロセスは、まず個人顧客ならびに法人顧客による電話の発信数を把握することから始まる。長距離電話会社は、電話利用システムから得られるデータならびに請求システムに登録されている契約条件に基づいて、通話に対する請求を行う。次いで個々の請求書が取りまとめられ、売上高が総勘定元帳に記録される。各事業部門の総勘定元帳が統合システムを通じて他の事業部門の売上結果と統合され、それが財務諸表の総売上高として報告されることになる。このようにアプリケーションは財務報告にとって重要な幾つもの定期的な作業ならびに計算を行っているのである。このアプリケーション内にあるデータとアプリケーションが実行する計算とは、公正かつ信頼性の高い財務諸表を作成するために、完全性のあるものでなければならない。

ITに対する統制を無視することはできない。ほとんど例外なくすべての企業が、情報を記録し、統合し、報告する処理のためにITを活用している。企業がコンピュータを所有していないか或いはその稼働の規模が小さく極めて単純である場合以外は、財務報告に係る内部統制を評価するに当たり、情報技術に対する統制を常に検討の対象としなければならない。人的統制でさえも、情報技術を活用せざるを得ないものが少なくない。例えば、コンピュータが作り出した報告書を他のデータと比較したり、総勘定元帳と補助帳簿の数字を一致させたり、業績評価に数的指標を活用することによって

特定の事業活動を監視したりといった作業である。

ITに関連した主たるリスクにはどのようなものがあるか？

財務報告のプロセスにおいてITは重要な役割を果たすため、プログラム（またはアプリケーション）とデータの完全性は、内部統制環境における重要な要素であると言える。アプリケーションの完全性といった場合、情報の有効性、効率性、機密性、完全性、規制への準拠、信頼性の問題など、情報の処理と報告に対する何らかの表明が発生する。これらの表明は情報技術のリスクを評価する上で基盤となるものである。例えば、情報の有効性についての表明は、ある情報が事業プロセスに関係しており、適切なタイミングで、正しく、一貫して、有益な形で提供されているかどうかを示すものである。また情報の機密性についての表明は、企業の秘密情報が承認のないまま開示されることのないよう保護されているかどうかを強調したものである。これらの表明はIT関連のリスクを評価する上で基盤となる。

ITに係るリスクとは、これら基本的な表明の内容を達成する上で、その妨げとなる「問題の可能性」を描き出した事象を指す。またリスクは企業のITに対する統制や人的統制を評価する上で、その背景となるものである。例えば、最初のデータ入力が正確で完全なものとなるよう、ITの観点からどのような統制が行われているか。処理情報やその他会計上の情報が蓄積され維持されているIT環境に対して、どのような統制がなされているか。IT環境に付随する固有のリスクを軽減するために、どのような管理が行われているか、などの問題である。具体的な例を挙げると、コンピュータのセキュリティに不備がある場合、「技術的な抜け道」が生じ、それによってデータが変えられてしまうといったリスクが存在する。このような場合、適切な統制を行うことで、データに変更が加えられるのは経営陣が定めた基準に合致する場合のみとすることが可能となる。

統制する主体は誰か？

企業のIT関連の組織は、ITの運営部隊と、ITに影響を与えるプロセスの全体的な管理を担う部門とから構成される。IT関連の組織は通常、最高情報責任者（CIO）が統括する部門から構成され、全般統制の有効性に影響を与える組織となる。CIOは通常、企業改革法第404条へ

の準拠を担当する委員会のメンバーであり、IT部門内で内部統制の重要性を伝達し、財務報告に係る内部統制に対するIT部門の役割を理解しそれを文書化する。さらにITの各種プロセスがアプリケーションとデータの完全性にどのような影響を与えるかに基づき、IT関連のリスクがどの部分で内部統制に関係してくるかを判断する。またCIOは、こうしたリスクを軽減する統制を文書化し、統制上の障害を適時に検出する監視メカニズムを開発する役割も担っている。

アプリケーションならびにデータの保有者となるのは、事業プロセスの責任者と接点を持つ事業グループに帰属し、そこでアプリケーションが処理する事業情報や会計情報に関する責任を有している。彼らはビジネスの観点から各種事業プロセスのニーズに合致するアプリケーションを決定、設計し、当該アプリケーションが期待通りに機能するよう、モニタリングを行う。また当該アプリケーションが主要な事業プロセスに与える影響を判定し、その評価を定期的に更新する役割も担う。さらに、CIOと協調し、情報処理とデータの完全性や可用性に影響を与えるリスクを軽減させるために、組織全体を対象とした有効性の高い統制を確立するという役割も担っている。その場合、特にデータ変更の管理プロセス、職務の分離（データアクセスのセキュリティ向上を目的とする）、事業継続プランなどが対象となる。またアプリケーションならびにデータの保有者は、統制上の問題を検知するモニタリングの手続きを策定、実践し、アプリケーションならびにデータの管理と事業プロセスの管理を有効に統合させることも任務となる。

組織レベルでの統制が重要である

IT関連のリスクならびに統制は、財務報告に係るリスクの総合的評価や、そのリスク軽減を図る統制と統合して検討する必要がある。このIT関連の統制には、組織レベルの統制とプロセスレベルの統制の二つの種類がある。これら二つの統制はITに関するリスクを許容できるレベルにまで軽減させるべく設計されるものである。

組織レベルの統制は、情報処理とデータの完全性を確保し、それを維持、モニタリングする支援環境を提供するものである。ITに関連する組織レベルでの統制には、通常、情報技術の運営やアプリケーションの管理に対する権限や責任の付与など、統制環境の構築が含まれる。

また一貫した方針や手続き、すべての事業拠点や事業部門に適用される行動規範や不正防止策などの組織全体での取り組みなども含まれる。また経営陣やプロセスの責任者、アプリケーションやデータの責任者がリスクを認識し評価するために活用するプロセスも含まれる。さらに、シェアード・サービス環境など中央一元管理による情報処理や統制に対する組織構成面での考慮のほか、例外報告（例えばセキュリティの不備）のモニタリングなど、統制の実施状況を監視するプロセスも含まれる。また経営陣はアプリケーションとデータの完全性に直接的な影響を与える特定のプロセスに対して有効な管理が実施されるよう、監視プロセスを策定することが求められる。

経営陣は、組織内の複数の拠点や部門を対象に、組織レベルでの統制を評価することが必要となることもある。経営陣の構成や統制の範囲は、組織の範囲を定義する上で主たる基準となることが多い。内部統制の観点から組織構成を検討する場合、企業内のIT関連組織は他とは分かれた別の組織となっている場合が多い。これはIT関連組織が独自の目標や目的を設定し、特定の部門によって管理されているという理由からである。大規模な組織では、複数のIT関連部門が検証の対象となる場合がある。

プロセス・レベルの統制も検討する必要がある

いわゆるプロセス・レベルの統制には広く分けて3つの分野が存在する。まず情報技術に対する全般統制では、アプリケーションとデータの完全性に直接的な影響を与えうるITのプロセスが対象となる。このプロセスをその相対的重要性の順番で例示すると、アプリケーションの維持ならびに変更の管理、セキュリティの管理、コンピュータの稼働ならびに障害の管理、データ・マネジメント、災害復旧、資産管理などが挙げられる。

次にアプリケーションに関連するプロセス、ならびにデータ責任者に関連するプロセスであるが、これはアプリケーションやデータの完全性に直接的に関係する事業部門またはプロセス責任者の活動についてである。その例を相対的重要性の順序で提示すると以下の通りである。

- ・アプリケーションの維持と変更の管理
- ・アプリケーション・レベルのセキュリティの定義ならびに管理

- ・相互に分離されるべき役割の定義と管理
- ・セキュリティ関連の役割の全体的なレビューならびに承認。（アクセス権限を含む）
- ・重要な情報処理ならびにデータの処理・閲覧の権限を有すべき担当者の定期的なレビュー。
- ・最新の事業影響分析および事業継続プランの策定と維持。（企業改革法規則の影響を考慮に入れて）

上記活動のそれぞれについて、IT関連組織内で実行されるべき役割があるが、事業プロセスの責任者は、業務上の機能や統制を支えるアプリケーションがそれぞれの要件に従って適切に設計、維持、管理されていることを確かめるプロセスを策定する必要がある。こうしたプロセスはIT関連組織だけでは有効に実行することはできない。

アプリケーション固有の統制は、統制として、或いは事業プロセスに伴う統制を支援する目的で、個別のアプリケーションの中にプログラムされるものである。この分野の統制では、企業改革法第404条への準拠に当たって重要と判断される各事業プロセスを対象に、実施されている重要なプログラム統制を特定し、評価することが重要である。プロセスの責任者は人的統制を評価する際に、アプリケーションによるプログラム統制について理解することが求められる。もし自動化された統制と人的統制が統合された形で評価されるのであれば、統制面でのギャップが生じるか、或いは文書化されていない統制に不当に依存するという結果になる。プログラム統制は、財務報告関連のアプリケーションによる処理に関して、完全かつ正確で、迅速で、一貫した処理と報告を可能とするものである。こうしたプログラム統制に関しては、業務プロセスのフローの幾つかの重要な局面において考慮が必要となる。例えば、アプリケーションが計算を行う、データや編集のパリテーション・チェックを行う、他のシステムと情報のやりとりをする、情報処理やデータへのアクセスを制限する、経営陣がその完全で正確なものとして依拠する重要な財務情報を選出し、統合し、報告する、といった局面である。

この自動化されたプログラム統制は、以下の二つの根本的な原則の上に立脚している。

- ・その統制が適切に設計され、経営陣の意図する設計通りに機能している。

・プログラム統制もプログラム統制に絡むアプリケーションも変更されない場合、その結果として、経営陣が意図するような形で、或いは意図するタイミングで統制が実施されなくなる。

外部委託している場合の注意点は何か？

ITの機能または何らかの重要な処理プロセスのすべてまたは一部が外部委託される場合でも、経営陣には、企業の会計システム・コントロールにとって重要性の高い処理を行う場合の統制を評価する責任があることには変わりはない。処理プロセスが社内で行われるか社外で行われるかにかかわらず、ITその他の統制に関する問題は存在するのである。経営陣は、財務報告に係る会社の内部統制にとって重要性の高いプロセス活動やアプリケーションについて、その統制状況を評価する必要がある。この評価は(1)会社が実行するプロセスやアプリケーション、(2)会社が社外のサービス・プロバイダーに外部委託するプロセスやアプリケーションを対象としていなければならない。

外部委託するアプリケーションについては、経営陣はサービス・プロバイダーの外部監査人から提出される報告書を当該サービス・プロバイダーから入手することができる。このサービス・プロバイダーの外部監査人による報告書は、会社の外部監査人にとって許容できる一定の基準を満たしていなければならない。またサービス契約の条件については、それが何を管理し、何を管理しないのかについて企業が期待する内容を定めるものであることから、内容を十分に理解することが重要である。経営陣はアプリケーションならびにデータの責任者の役割を外部委託することはできない。これはアプリケーション固有の統制やその統制の事業プロセスの中での活用方法について、個々の担当者が責任を有するからである。

IT関連の統制に不備が生じた場合どうするか？

組織レベルの統制環境が脆弱である場合、プロセス・レベルでの強力な統制を策定し維持することを規定した全体的な方針やガイドラインが存在しないか、或いは欠如しているケースが多い。そのような場合、強力な統制が必要であることを強調したメッセージが明確に伝達されていないのが通常である。IT関連組織の目標と目的（さらに経営陣が定めた基調）については、

組織レベルでの統制が脆弱である場合、IT関連の全般統制が一貫して強力に進められる可能性は大きく損なわれる。これは強力な統制が会社の様々なプロセスの中に存在し得ないことを意味するものではないが、上級経営陣がそのような統制の必要性を明確に伝達していなかったり、統制環境に対する一貫した監視が実施されていないことを意味するものである。組織レベルでのリーダーシップの欠如は、場当たりの一貫性のない統制環境を助長するものであり、そうした統制環境の中では、経営陣ならびにプロセス責任者はIT関連の適切な統制が必要であることを十分に強調できない可能性がある。

もし統制環境が脆弱で、その結果としてIT関連の全般統制が不十分であったり、或いはアプリケーションならびにデータの責任者の統制に弱点がある場合には、経営陣は、事業プロセス・レベルにおいて、職務の分離や情報処理の正確性・完全性に関して、代替的統制や弱点を補う統制がないか、評価し理解する必要があるであろう。もしアプリケーション・レベルでの統制が脆弱である場合には、経営陣はそれを補う発見的ならびに監視的な統制方法を探し出さなければならない。この発見的・監視的統制方法は非常に詳細部分で、適用範囲も広範なものである必要があるであろう。またその統制が効果的に運用されるためには、コンピュータ処理に依存したものであってはならず、文書化され、評価、検証され、テストが実施されなければならない。

組織レベルでIT環境が脆弱であるか、或いはプロセス・レベルで全般統制またはアプリケーションの統制が脆弱である場合、重要な不備または重大な欠陥が存在する可能性がある。例えば、情報処理の量が膨大で複雑な環境においては、発見的・監視的統制に依存することは、有効でも現実的でもない可能性がある。こうした環境は、少なくとも重要な不備をもたらすものであり、内部統制における重大な欠陥さえももたらす可能性がある。重大な欠陥があると判定される場合、財務報告に係る内部統制が有効でないという表明が導かれることになる。また監査人から不適正意見が出される可能性もある。これは誰も望まない事態である。

欠陥にはどのように対処すべきか？

経営陣は、発見された弱点の性質や重大さに応じて、以下の二つの方法でIT関連の統制の欠陥に対応するこ

とになる。まず第一に、整備状況または運用状況が有効でない処理また統制に関して、経営陣がギャップ分析を実施し、そのギャップを埋めるためのアクションプランを策定する。IT関連の統制の場合、ギャップの分析ならびにその改善には相当な期間を要する可能性がある。対応の過程においては、以下の二点について検討する必要がある。

- ・内部統制は、共通的なものであっても個別のものであっても、予防的なものかあるいは発見を目的としたものである。内部統制はリスクの源泉に対して設置されるものであるか（予防的）或いはプロセス内でリスクの源泉よりもさらに下流のプロセスに設置されるか（発見目的）によって区別される。
- ・内部統制は、アプリケーションによるもの（つまりプログラム統制）か、或いは人的なものかどちらかである。情報処理の量やリスク発生の可能性や複雑性が増した場合、アプリケーション・レベルの統制の方が、人的統制よりも信頼性が高い場合が多い。アプリケーションは有効に設計、運営、維持、確保される限り、人的な処理よりもエラーを起こしにくい。但し、アプリケーション・レベルでの統制は設計と構築により多くの時間がかかる場合がある。

上記二点の意味するところは、企業はIT関連その他のリスクの統制に対してより積極的なアプローチをとる方向に、統制の設計をシフトさせる必要があるという点である。こうした積極的な統制へのシフトにおいては、発見的統制の特徴である「見つかった場合に修正する」という受身のアプローチや、非効率で煩わしい過度の人的統制よりも、アプリケーション・レベルの予防的統制により重点を置くことが求められる。しかしながら、全体的な設計の中で、これらの統制を効果的に織り交ぜる必要が生じることも多い。

IT関連の欠陥に対応するもう一つのアプローチは、IT関連の統制の弱点がもたらすリスクを発見し、それを補うための適切な人的統制を文書化または設計することである。これは少なくとも短期的には適切な手段と考えられる。統制上の不備についてのリスク分析、ならびにリスク軽減のための統制についての分析は、短期的には企業にとって時間稼ぎとなる可能性があるが、情報処理の量と複雑さを考慮すると、このような代替的な統制が不可能な場合もある。

外部監査人のアプローチはどのようなものか？

外部監査人は、内部統制報告書における経営者の表明の根拠を評価するに当たり、IT関連のリスクならびに統制を強く意識すると言って間違いない。全般統制が不十分である場合、それが重要な情報処理や勘定に影響を与える可能性がある。また全般統制の中に何らかのギャップが存在する場合には、外部監査人は、内部統制が有効であるとの総合意見に到達するために、そのギャップへの対応が必要であると指摘する可能性がある。我々は外部監査人がその監査顧客に対して、統制環境について証明をおこなうまでに、会社はユーザーの情報アクセスに対するセキュリティなど、アプリケーション上のセキュリティに関して統制を強化しなければならないと指摘した例を知っている。こうした背景から、企業改革法第404条への準拠に取り組むチームは、統制に関する何らかのギャップが存在するかどうかを判定するプロセスにおいて、可能な限り早く、全般統制などのIT統制環境について評価を行うべきである。

事業継続性を無視してはならない

財務報告において前提となるのは、公開企業がその財務報告の期限を遵守することが可能であり、信頼できる最新情報に基づく会計上の見積りを含む公正な表示と開示に必要なすべての重要情報を入手できるという点である。これらの要件から、企業には幾つかの義務が発生する。それは、開示に関するものを含む法規制に加えて広範囲にわたる事業リスクを評価することによって、事業影響分析を適切な形で経営陣の同意と承認のもとに文書化する必要があるといった義務である。企業が総合的かつ最新の事業継続プランならびに災害復旧プランを通じて、予測できない事態に対応する用意ができていない場合には、企業が証券取引委員会（SEC）に対して適時で完全かつ正確な報告書を提出できるかどうかに影響が生じる可能性がある。事業影響分析の妥当性と、その事業影響分析の結果から生じる事業継続プランの策定や維持に総合的な責任を有するのはプロセスの責任者であるが、災害復旧プランを開発し事業継続プランを実現させるのは、通常はIT関連組織の責任である。企業が事業継続や災害復旧に有効に対応できるかどうかは、ゴーイング・コンサーンとしての継続性の前提など、会社の全体的な事業リスクの管理に関する重要な側面である。

規則対応にとどまらない

本稿においては、企業が財務報告の信頼性に係る内部統制の目的を達成するに当たり、IT関連のリスクならびに統制がどのように関係するかに焦点を当ててきた。情報技術は、企業が意思決定のために必要な情報を作成するために機能し、実質的にあらゆる活動に影響を与えるものである。有効に機能しているIT関連組織は、直接または間接的に何らかの形で企業の事業活動に影響を与えており、その例外を想像することは困難である。ITは財務報告の目的に影響を与えるのと同様に、業務の有効性や効率性、法令順守目的の達成にも影響を与えるものである。さらにITに対する組織の依存の度合いは、事業モデルが進化するにつれて継続的に高まっていく。アプリケーションならびにデータの信頼性、完全性、可用性が企業の経営者や取締役にとって極めて重要であるのはこのためである。

プロティビティは以前発行した「企業改革法(SOA)質問集：内部統制報告要件 (Internal Control Reporting Requirements) - 第404条」に続き、「企業改革法(SOA)質問集：情報技術のリスクならびに統制」(英文)を発行いたしました。情報技術関連のリスクならびに統制に関してさらに質問がございましたら、同質問集をご参照ください。詳しい内容は当社ホームページ www.protiviti.com をご覧頂くか、(03)5219-6600までご連絡ください。

取締役会への質問

- CIO (最高情報責任者) は情報技術に関する内部統制環境の現状について、監査委員会に報告を行うべきか？
- 内部監査人および外部監査人は、IT関連の統制について、どんな考えを持っているか？もし監査人が会社のIT関連の統制について数多くの改善提案を出してきた場合には、会社側はどのように判断すべきか？
- IT機能の一部を外部委託する場合、外部委託された会計システムや統制に影響を与えるプロセスに関して、経営陣は、その統制を評価するという責任をどのように果たしたか？
- 会社の内部監査の機能は、ITに対してどの程度焦点を当てているか？もし内部監査のリソースや監査プランがITに関して十分でない場合、それは会社に対してさらなるリスクをもたらすことになるか？
- 会社は競合他社に比べて、どの程度ITに投資しているか？もし会社の投資額が業界平均を大幅に下回っているのであれば、それはリスクが低いということか、それとも潜在的なリスクであるか？

経営陣への質問

- CIOは、企業改革法第302条および404条に準拠する目的で、IT関連の統制環境を強化するために、実施すべきことを認識しているか？
- CIOは企業改革法準拠のために追加的な投資が必要であることを理由の一部として、さらなる投資を行うことを要請しているか？そのような場合、どうしてその要請が妥当であると考えられるのか？
- ハッカーによる不正アクセスやその他IT関係の事件の公表は、企業改革法第302条の宣誓または第404条の報告の中で検討または開示されるべき内部統制の欠陥として解釈されるという点に関し、会社はどの程度関心を払う必要があるか？
- 会社がIT関連組織の業務に関して外部委託の量を増やすか、或いはそのすべてを外部委託する場合、IT関連における企業改革法第404条準拠の要件をどのように満たすか？
- 会社が複数の新しいシステム関連プロジェクトを進める場合、それは企業改革法への準拠にどのような影響を与えるか？