

SOX法対応を新たな競争優位に つなげるために

－ IT部門におけるSOX法対応の成功要因－

シスコシステムズ株式会社

インターネット・ビジネス・ソリューションズ・グループ (IBSG)

パートナー 鈴木 寿里

2007年4月



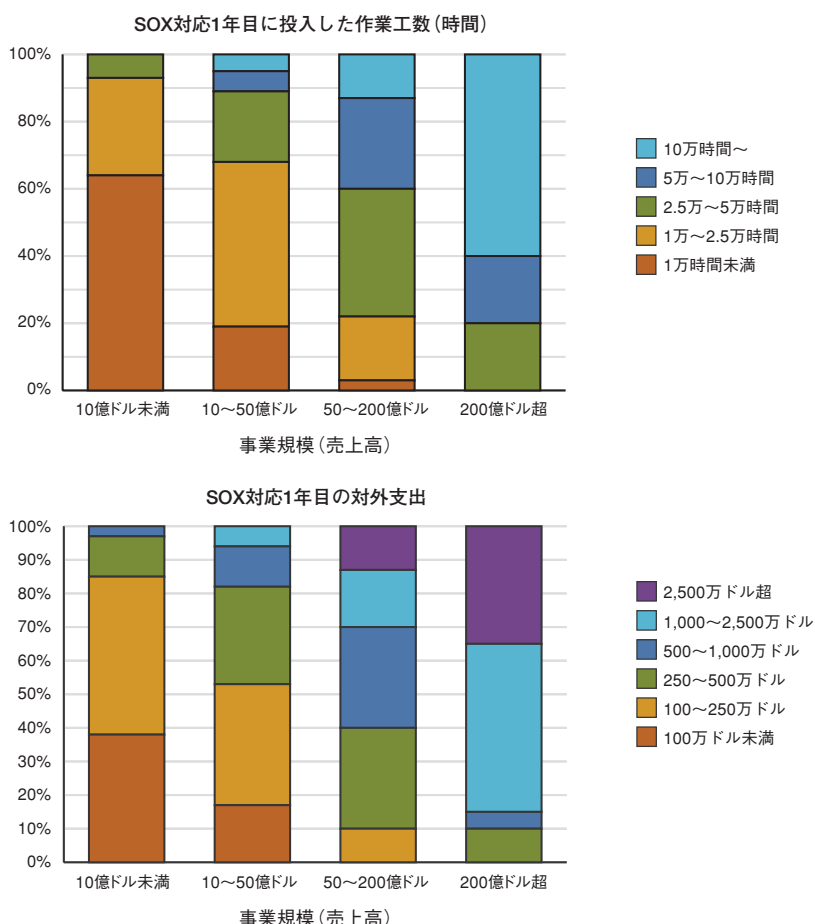
はじめに

2006年11月に金融庁より「財務報告に係る内部統制の評価及び監査に関する実施基準（公開草案）」が発表され、2007年3月には経済産業省より「システム管理基準追補版（財務報告に係るIT統制ガイダンス）」が公開された。これらの文書により、いわゆる「日本版SOX法（以下SOX法）」の要求事項も明らかになってきた。SOX法は2008年4月1日以降に開始する会計年度から適用されるため、各企業は短い期間での対応を迫られている。

このホワイトペーパーでは、SOX法対応のために行う業務変革やIT投資を単に法律準拠のためだけに終わらせることなく、企業競争力強化の基盤とするための成功要因について、日本よりも4年先行してSOX法が施行された米国の経験を踏まえてまとめてみたい。

SOX法対応に要するコスト

世界有数の監査法人のひとつであるアーンスト&ヤングは、2005年に米国の255社を対象にSOX法対応に費やされたコストを調査した。この調査から、SOX法施行初年度にSOX法対応に費やされたコストは企業規模が大きくなるにつれて増加していることがわかる。特に売上高が200億ドル以上の企業においては、60%以上が10万時間以上の工数と、2,500万ドル以上の費用をSOX法対応に費やしている。



▲米国におけるSOX法対応の工数および対外支出と事業規模の関係

出典：Emerging Trends in Internal Controls — Fourth Survey and Industry Insights, Ernst & Young, 2005

では、なぜこれだけの莫大な労力と資金を投じる必要があったのだろうか。

SOX法では、財務報告において意図的な改ざんや事故による誤りの起こるリスクを洗い出し、それに対する統制を確立し、その統制が有効に機能していることを検証することが求められる。このため、企業規模が拡大し、組織やプロセスが複雑になり、統制の数が増えるにつれて作業工数は増えていく。またIT分野においては、財務会計に関係するシステムの種類や数、それらのシステムが稼働しているデータセンターの数が増えるにつれ、作業工数も増加する。

こうした要因に加え、初年度においては、企業、監査法人とも非常に保守的な姿勢でSOX法対応を実施したことも上げられる。SOX法施行のきっかけとなったエンロンやワールドコム等の粉飾決算問題において、当該企業だけでなく、エンロンの会計監査を担当していたアーサーアンダーセンもが解体されたことに大きな衝撃を受け、企業、監査法人とも慎重になったのである。さらに、SOX法対応に助言を与える外部コンサルタントの存在がこれに拍車をかけた。企業の内部統制報告書を監査する監査法人には独立性が要求され、監査対象企業の内部統制の構築自体に助言を与えることは許されない。このため、多くの企業は自社の監査を担当する監査法人とは別の監査法人に対してコンサルタントとしての助言を求めた。助言を与えるコンサルタントは、自分たちの助言に基づいて構築された内部統制が外部監査人によって「不適切」と判定されることのないよう、より高いレベルでの内部統制の確立を顧客企業に提言したことが担当者らの話から推察される。

SOX法では、財務報告に関わる「内部統制」を確立・維持し、毎年外部監査を受けることが求められる。

そのためには、財務報告に関わるすべての業務プロセスに内在する不正やミスリスクを洗い出し、それに対する「統制」を構築する必要がある。

多くの企業では、財務報告に関わる業務プロセスにはアプリケーションシステムが用いられているので、業務に対する統制の確立にはシステム統制の確立が前提となる。

業務に用いられるアプリケーションシステムの信頼性を高めるためには、そのシステムが稼働しているIT基盤の信頼性を高める必要がある。



▲財務報告に関する内部統制とIT統制の関係

内部統制およびIT統制構築における成功要因

米国のSOX法施行から4年遅れて同法が導入される日本企業においては、先行した米国企業の経験から何を学ぶことができるだろうか。

以下では、筆者自身が米国に本部を置く多国籍企業の日本法人のCIOとしてSOX法対応に取り組んだ経験、シスコおよび他の米国上場企業のSOX法対応担当者から得た情報等を総合し、IT分野におけるSOX法対応を効果的に進め、それに伴う変革を企業の競争力強化につなげるための成功要因を(1)組織、(2)プロセスとツール、(3)戦略とアプローチという3つの観点からまとめてみたい。

(1) 組織

■ 内部統制に対して継続的に責任を持つ部署を明確にする

ある期限までに情報システムの信頼性を確保しなければならないという共通点から、SOX法が2000年問題と比較されることがある。しかし、大きく異なる点は、SOX法対応は「一度乗り切れば終わるものではない」という点である。日本においては、SOX法の対象企業は会計報告とともに内部統制報告書を作成し、外部監査を受けるという作業を2008年度以降、毎年継続して行わなければならない。

米国企業では、SOX法対応1年目に多くのコストと労力をかけた経験から、2年目以降はより長期的な観点で内部統制を捉え、効果的にSOX法対応を進めようと努めている企業が多く、内部監査部門がその中心的役割を担っている。内部監査部門は法令の要求事項を正確に理解し、自社の内部統制の現状を評価し、不十分な点に対しては関連部門に働きかけ確実に改善策を実施していくという役割を果たす。

リスクマネジメントを重視する多国籍企業では、内部監査部門が非常に強い権限を持ち、外部監査以上に高い水準の統制を世界のグループ会社に要求しているケースも少なくない。その結果、外部監査からの想定外の指摘事項を防ぐなどして、外部監査の実施の効率化にも寄与している。企業によっては内部監査部門の中にIT統制に精通した担当者を配置したり、IT部門の中にコンプライアンスに責任を持つ担当者を置き、IT分野におけるSOX法の要求事項に効率良く対応するために求められる知識や経験を蓄積している。

■ 内部人員と外部人員の配置を最適化する

ある外資系企業では、各国拠点を含むグローバルな方針としてSOX法対応業務の多くを外部コンサルタントに委託した。日常業務に重要な責務を持つ主要社員を長期間にわたってSOX法対応に割り当てるのは経営にとってマイナスと判断したためであった。この結果、SOX法対応初年度においては、日本法人だけで5億円以上の支出があったという。

その企業で現在行われているのは、外部コンサルタントがSOX法対応で得た知識を社員に移転する作業である。前述のようにSOX法対応は毎年継続して行わなければならない。また、一度構築した内部統制も、業務や組織が変わるたびに変更し、有効性の評価を行わなければならない。これらすべてを外部コンサルタントに頼り続けるのは得策ではないと判断を改めたのである。

プロジェクトの計画や管理、文書フォーマットの標準作成、プロジェクトチームに対する教育や助言などでは外部専門家のサポートは有効だが、現状のプロセスや統制に関する調査、

統制の改善設計、その有効性の評価などには、実際の業務に精通している社員の知識は欠かせない。

また、一方で、作成した文書の部分修正や統制の有効性評価の作業の一部など、比較的単純な作業も発生するので、こうした分野においては単価の安い外部リソースの活用も検討すべきだろう。必要な知識とスキルを持った社内外の人材を適切に配置することが、コストを抑えつつ効果的にSOX法対応を進める上での重要なポイントである。

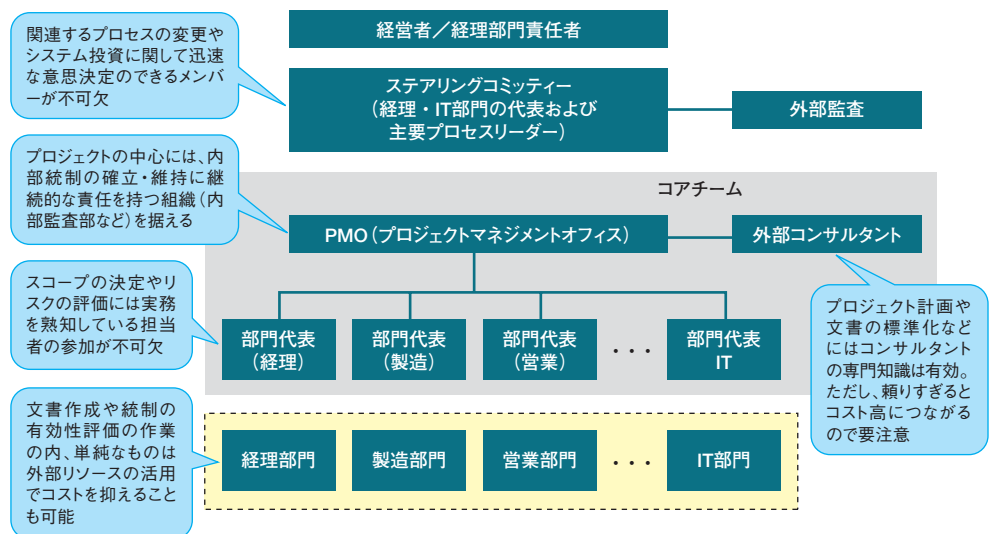
■ 主要なプロセスの責任者を意思決定機関のメンバーとする

「SOX法対応は経理部門と情報システム部門の仕事」と誤解されることがあるが、実際にはそうではない。

例えば、売上計上のプロセスであれば、多くの企業では営業部門が関わるであろうし、受注業務の管轄が物流部門であるケースもある。事務用品などの購買プロセスであれば、会社の中で関わらない部門はごく少ないはずだ。

仮に、ある業務プロセスの評価の結果、現状での統制が不十分であることがわかった場合、それをどのような方法で改善するかについて意思決定をする必要がある。システム化が適切な場合もあれば、プロセスや役割を変更することが妥当な場合もある。その判断および意思決定には、業務プロセスに対する知識も必要であるし、組織や役割の変更、IT投資などに対する権限も必要である。

ところが、ひとつの業務プロセスを担当している部門が複数部門にわたることが少なくない。そこで、シスコでは部門の責任者とは別に主要な業務プロセスに責任を持つ「ビジネスプロセスリーダー」を定め、彼らの会議体であるビジネス・プロセス・オペレーションズ・カウンシル (BPOC) において業務プロセスに関わる協議や意思決定を行っている。日本では「業務プロセス単位の責任者」が不在の企業が少なくないが、SOX法に対応する内部統制の整備を効率良く進めるためには、少なくとも財務報告に関係する業務プロセスについては必要な意思決定を迅速に行うことのできる責任者を定め、SOX法対応プロジェクトの主要メンバーとすることが望ましい。



▲ SOX法対応プロジェクト組織の例

(2) プロセスとツール

■ 監査法人との協議を早期に開始する

「SOX法に対応するためにどのレベルで内部統制を構築すればよいのかわからない」とい声をよく聞かすが、すべての企業に共通する答えは存在しない。筆者自身の経験においても、監査対象の業務やシステムの範囲、テストを実施する対象となる統制などは監査人との協議の中で決まった。ある統制が「キーコントロール（重要な統制）」であるかどうかといった判断においては、監査人によって見解の異なる場合も少なからずあった。

したがって、早期に監査人との打ち合わせを開始し、監査の範囲、時期、方法などを十分話し合い、適切な内部統制構築計画を作ることが望ましい。前述の「内部統制に対して責任を持つ部署」が継続的に外部監査機関と意見交換を持つことにより、外部監査の要求事項に変化があった際などにもタイムリーに対応することが可能になる。

■ 適切なIT統制ガイドラインを活用する

IT統制をどのように構築し、それが適切であるかをどう評価するのか等について、監査人やコンサルタントを含めた関係者間でのコミュニケーションを効果的に進めるためには、共通の言語となる「枠組み」を持つことが有効である。2007年1月に経済産業省から出された「システム管理基準」は日本国内におけるIT統制構築のガイドラインのひとつとして使用されることになるであろう。

ただし、金融証券取引法や「内部統制の評価及び監査に関する実施基準」は、「システム管理基準」を使用することを求めている訳ではなく、これを採用するかどうかは各企業の判断に委ねられている。米国では、ITIL (Information Technology Infrastructure Library) およびCOBIT (Control Objectives of Information Technology) 等がIT統制のガイドラインとして用いられている。特にITガバナンス協会が作成しているCOBITは、2002年にSOX法対応に目的を絞った「COBIT for SOX」が発表されて以来、多くの企業に採用されている。2006年には「COBIT for SOX第2版」が公開され、その日本語版は日本ITガバナンス協会のウェブサイト (<http://www.itgi.jp/>) から無償でダウンロード可能になっている。

■ Eラーニングを活用する

SOX法は内部統制を確立し、それが有効に機能していることを評価することを求めている。その内部統制が有効に機能するためには、業務プロセスを改善したり社内規定などの文書を整備することもさることながら、社員一人ひとりの理解と自覚が不可欠である。しかし、企業が大きくなればなるほど全社員のスケジュールを調整し、教室形式の研修を行うためには多大な労力を必要とする。また、企業規模が拡大すれば新たに入社したり社内でも異動する社員も増えてくるので、教育も継続的に行う必要がある。その点Eラーニングは、必要なシステムと各社員がアクセスできる環境を構築してしまえば、場所や時間にとらわれることなく教育を実施できる上、同じ講習を繰り返し行っても追加コストはほとんど掛からない。また、受講後に理解度を評価する試験もオンラインで実施可能で、社員一人ひとりの受講状況や理解度もほぼリアルタイムで把握し、部署別、地域別などで集計することも可能だ。シスコをはじめ、Eラーニングを積極的に行っている米国企業では、管理職がEラーニングプログラムの冒頭でその研修の重要性をビデオメッセージで伝えることにより、社員の受講意識を高め

ている。

(3) 戦略とアプローチ

■ 前向きな「リスクマネジメント」として取り組む

日本企業のCIOやIT部門のSOX法担当者から、「トップからはコストをかけずに、必要最低限のことをやってくれと言われている」という話を聞くことが少なくない。これでは、SOX法対応チームのメンバーの士気もなかなか上がらないだろう。たしかにSOX法対応は法令により課せられた義務であるが、その目的は投資家保護である。企業が公表する財務情報に意図的な改ざんやミスによる誤りが入り込むことのないよう、必要な内部統制を確立するのは企業のリスク管理の観点からも重要だ。

会社として取り組む以上、「法律ができたから仕方なくやる」のではなく「企業の社会的責任を高いレベルで果たすために積極的に行う」という姿勢をとった方が、関係者のモチベーションも上がり、経営者に対する社員や投資家の評価も高まるはずだ。

米国でもSOX法対応に要する負担の大きさに対する不満の声もあるが、「業務上の無駄が明らかになり改善できた」「作られた文書が従業員教育に役立った」など、ポジティブな側面を評価する経営者も少なくない。

■ 業務プロセスやシステムの標準化、集約化を図る

米国企業においてSOX対応のコストが膨れ上がった要因のひとつとして、数多くのグループ企業やビジネスユニットを持つ巨大企業で業務やシステムが分散し、標準化されていなかったケースがある。

グループ各社の会計システムや業務プロセスが独立していると、内部統制の構築も個別に実施する必要があり、企業の数に比例して内部統制の構築と維持にかかる費用が増加する。同様に、会計システムが稼働するデータセンターが複数存在し、運用が標準化されていない場合、データセンターごとにIT全般統制を構築する必要がある。逆に、規模が多く、組織が複雑な企業であっても財務会計に関わる業務を標準化し、業務が行われる場所を集約し、使われるシステムも同様に標準化、集約化することにより、SOX法対応に要するコストを低下させることができる。

		SOX法対応コスト	
		低	高
財務報告に関係する業務	標準化の度合い	高	低
	業務を行う場所	少	多
財務報告に関係する情報システム	システムの標準化の度合い	高	低
	システム(インスタンス)の数	少	多
	運用手順の標準化度合い	高	低
	データセンターの数	少	多

▲業務およびシステムのデザインとSOX法対応コストの関係

グローバルに活動する企業の中でも、シスコはトップダウンで業務の標準化に取り組んでおり、単独のシステムで全世界の主要なビジネスの会計処理を集中処理している典型的な例である。

また、「標準化」は会社や部門レベルだけでなく、各社員レベルでも重要な意味を持つ。「COBIT for SOX 第2版」や経済産業省の「システム管理基準」では、エンドユーザーコンピューティングもIT統制の重要な要素として取り上げており、ExcelのマクロやAccessなどのツールを使ってエンドユーザーが自ら作成したプログラムであっても、財務会計処理に関わるものはIT統制の対象と捉えている。したがって、IT部門としては個々の社員レベルにおいても財務会計処理に関わる業務に使われるITツールの標準化を進め、統制を確立する必要がある。

■ SOX法対応を契機に中長期的IT戦略を再構築する

SOX法対応にどれだけの労力やコストがかかるかは、IT統制を含む内部統制の仕組みや、業務やシステムの標準化が現状どれだけでできているかによって大きく左右される。集約化、標準化ができていない企業においては、対症的なアプローチで一度の監査は乗り切れたとしても、2年、3年と続けていくのは負担が大きく、長期的には競争力の低下につながりかねない。

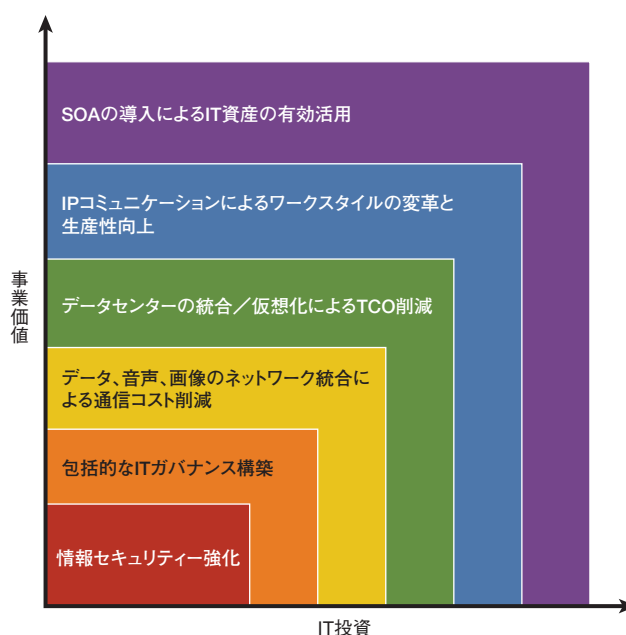
効果的なSOX法対応のためには、全社的な業務の見直しなど、大きな投資を必要とする場合もあるが、問題はその投資を会社の競争力強化に活かすことができるかどうかだ。それだけに、SOX法対応はCIOまたはIT部門の責任者にとっては、中長期的なIT戦略を策定し、経営陣のサポートを得る絶好の機会でもあるとも言える。優先順位は各社の状況に応じて異なるが、2007年現在において企業のIT戦略を策定する際には、以下の要素を考慮に入れるべきであろう。

● 情報セキュリティの強化

情報セキュリティは会計情報の正確性を保証するだけでなく、顧客情報漏えいなどのリスクから企業を守る上でも重要である。企業規模が拡大し、情報技術の利用方法も多様化するとともに、従来の機器単位のセキュリティ対応ではリスクを十分にコントロールすることが困難になってきている。大規模かつ複雑化した企業ネットワーク全体を不正侵入や改ざん、情報漏えいなどの危険から保護するためには、これらをひとつのシステムとして包括的に防御するアプローチが効果的である。

● データセンターの集約化および仮想化

会計データを取り扱うサーバーが設置されているデータセンターが多数存在する企業では、そのデータセンターごとに物理的セキュリティを含むIT全般統制を確立する必要があり、コンプライアンスに要するコストも増加する。また、データセンター数の増大は、情報の改ざんや漏えいのリスクをも増加させる。したがって、事業継続リスクや、通信コストとのバランスを考慮しつつ、データセンターはなるべく集約することが望ましい。また、最近では演算装置や記憶装置を仮想化する技術が進歩し、データセンター内のIT資産をより効果的に活用できるようになってきている。こうした技術も考慮し、中長期



▲ SOX法対応を起点とした中長期的IT戦略

的な成長戦略とそれに伴う演算処理およびデータ蓄積の需要増を見込み、適切なデータセンターの配置とネットワークアーキテクチャーを設計すべきだろう。

● データ、音声、映像のネットワークの統合

音声や映像の通信網のIP化によるデータネットワークとの統合は、単に通信コストを低下させるだけでなく、これまでの技術では困難だった新しい情報活用を可能にする。在席情報や電話会議、ビデオ会議、ウェブ上での情報共有などを効果的に連携することで、企業内コミュニケーションの生産性を飛躍的に高めることのできる可能性がある。SOX法対応の重要性を社員に周知徹底する上でEラーニングが有効であることはすでに述べたが、Eラーニングを実施する際にもこうした新しいコミュニケーションツールは有効である。

● アウトソーシングの再考

SOX法では、財務報告に関わる限り、たとえ外部に委託された業務であっても内部で行われている業務と同様に統制を構築し、評価することが求められる。このため、委託先の選定は非常に重要である。すでに高いレベルの統制を確立している企業であれば、委託する側が新たに文書を作成したり、評価項目を検討する必要がない可能性もある。逆に、万が一、現在業務委託している企業の内部統制が不十分である場合は、委託先を再検討するか、委託先と協力して適切なレベルの統制を構築し、それを業務委託契約に盛り込み、統制が適切に機能していることを検証する必要がある。

● サービス指向アーキテクチャー (SOA) の採用

今後数年間を考えれば、企業の情報システムの構成要素として、他企業がサービスとし

て提供するソフトウェア (SaaS) と企業内システムを連携させたり、前述のアウトソースパートナーを含む取引先とのシステム間連携を行う必要性は確実に増加すると思われる。そこで注目されているのがサービス指向アーキテクチャーだ。まだ発展途上の技術と言えるが、技術やビジネス環境の変化に柔軟に対応し、同時に既存の情報資産の有効活用を実現する上で有望な技術である。SOX法対応を契機に中長期的なIT戦略を見直すのであれば、こうした新技術の導入も検討してはどうだろうか。

結び

日本版SOX法は、内部統制構築への取組みが遅れていたり、業務やシステムの標準化、集約化が遅れている企業にとっては大きな負担となる可能性が高い。特に目先の法律準拠だけを目的に付け焼刃的な対応をすると、2年目、3年目と継続して多大な労力を消費し続けることになりかねない。

逆に、中長期的な視点でSOX法対応を捉え、この機会に自社の業務の無駄を省き、IT基盤を再構築することができれば、SOX法対応は競争力強化のための価値ある投資になり得る。そうした「攻めのSOX法対応」を行っていかこうとする企業にとって本稿が多少なりとも参考となれば幸いである。

参考文献

- *IT Control objectives for Sarbanes-Oxley - The role of IT in the Design and Implementation of Internal Control over Financial Reporting 2nd Edition*, IT Governance institute, 2006
- 財務報告に係る内部統制の評価及び監査に関する実施基準 (公開草案), 企業会計審議会内部統制部会, 2006
- サーベインズ・オクスリー法 (企業改革法) 遵守のためのIT統制目標 (翻訳版), IT Governance Institute, 2004
- “The Unexpected benefits of Sarbanes-Oxley,” Stephen Wagner and Lee Dittmar, *Harvard Business Review*, April, 2006
- *Management - Integrated Framework - Executive Summary*, Committee of Sponsoring Organizations of the Treadway Commission, 2004
- *Emerging Trends in Internal Controls - Fourth Survey and Industry Insights*, Ernst & Young, 2005
- 日本版SOX法, 日本版SOX法研究会, 2006
- 財務報告に係る内部統制の評価及び監査の基準のあり方について, 企業会計審議会 内部統制部会, 2005
- システム管理基準 追補版 (財務報告に係るIT統制ガイダンス) (案), 経済産業省, 2007

著者: 鈴木 寿里 (すずき かずさと)

シスコシステムズ株式会社 インターネット・ビジネス・ソリューションズ・グループ (IBSG)
パートナー

経歴: プライスウォーターハウス・コンサルタント、ウォルト・ディズニーマー・インターナショナル、ジョンソン・エンド・ジョンソン (メディカルカンパニー) を経て2006年より現職。前職では日本人のCIOとしてIT分野のSOX法対応を統括。

© 2007 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0704R)

この資料の記載内容は2007年5月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先 (シスコ コンタクトセンター)

<http://www.cisco.com/jp/go/contactcenter>

0120-933-122 (通話料無料) 、 03-6670-2992 (携帯電話、PHS)

電話受付時間：平日 10:00～12:00、13:00～17:00