「SOX 法に伴う IT の活用と IT サービス企業への影響」

渡辺弘美@JETRO/IPA NY

1. はじめに

2005 年 7 月、金融庁の企業会計審議会は、日本版 SOX 法（企業改革法。通称：Sarbanes-Oxley Act）の原案である「財務報告に係る内部統制の評価及び監査の基準」の草案を公開した。SOX 法は、エンロン社など一連の企業スキャンダルを受け 2002 年 7 月に米国で制定されたものである。日本版 SOX 法では、経営陣による IT に関する理解が未熟であったという米国の経験を踏まえ、内部統制の基本的要素として「IT の利用（内部統制の他の基本的要素が、有効かつ効率的に機能するために、業務に組み込まれている一連の IT を活用すること）」が法律上明文化されそうである。ここでは同法の導入を巡る米国の経験を紹介する。

2. SOX 法がもたらす企業への負担

米国では、同法により、企業財務コンプライアンスが高まり、企業のステーク・ホルダーにとっては高いメリットをもたらす環境が整備されたが、一方で、同法遵守が企業にとって大きな負担であることが明らかになっている。

大手弁護士事務所 Foley & Lardner が、2005 年 1 月に 147 の株式公開企業を対象に行ったアンケート調査結果によれば、82%の回答企業が、コーポレートガバナンスや公開企業の情報開示に関する企業改革は「厳しすぎる」とした。また、「厳しすぎる」と回答する企業の割合は、2003 年の 55%、2004 年の 67%と、年々増加していることも明らかになっている。

「厳しすぎる」という認識が高まった背景には、SOX 法の設立当初から企業にとって SOX 法コンプライアンスはかなりのコスト負担となるとされていたが、同法の施行後、実際のコストは企業の最高財務責任者（CFO）たちの予測を上回るものとなっているという状況がある。

全米企業の CFO など財務担当幹部で構成される Financial Executive International（FEI）が 2005 年 3 月に発表した調査結果（株式公開企業で平均年商 50 億ドルの 217 社が対象）によれば、SOX 法を遵守するために最初の 1 年間に要したコストの平均は約 436 万ドルで、これは 2004 年 1 月時点の予測（約 194 万ドル）に比べると、実際のコストはその 2 倍以上となったことが判明した。

SOX 法遵守に伴う初年度のコスト予測と実績（ドル）

	04 年 1 月時点の予測	04 年 7 月時点の予測	05 年 3 月時点のコスト実績	04 年 7 月予測と 05 年 3 月実績の比
社内コスト	613,250	1,283,385	1,337,935	4%↑
社外コスト	732,100	1,037,100	1,716,987	65%↑
監査料金	590,100	823,200	1,301,050	58%↑
合計	1,935,450	3,143,685	4,355,972	39%↑

こうした状況に対して、FEI 調査に回答した企業の多くは SOX 法の趣旨は評価しているものの、94%は「コストが利点を上回っている」と回答しており、コスト増が大きな負担となっていることが示された。

特に、予想を上回るコスト増加の最も大きな原因として、SOX 法に通じた人材を確保するための人件費がある。先の大手法律事務所 Foley & Lardner LLP が行った調査結果（2005 年 6 月発表）によれば、SOX 法により社外監査官の役割や責務が強化されたことで、経験豊富な会計監査ディレクター・レベルの監査官コストが 2001 会計年度から 2004 会計年度の間に 40%以上増加した（S&P 500 企業で 43%、S&P の中規模時価企業で 45%、S&P の小規模時価企業で 46%）。さらに、各社競って優秀な人材を確保・維持しようとするため、人材の獲得合戦となり、価格高騰の傾向が強まっている。

このほか、今日の企業経営にとって不可欠となった IT 予算についても、財務処理系のプロセス見直し、文書管理、セキュリティ対策などが必要となるため増加傾向にある。例えば、調査会社 Forrester Research が 2004 年 5 月に発表した調査結果によれば、調査対象となった 878 社の IT 担当幹部の 77%が、「SOX 法遵守のために IT 予算は増大する」と回答している。

3. SOX 法と企業の IT

SOX 法は直接的には企業の財務報告に関わる内部コントロールを対象としたもので、財務部門に 100%影響するものだが、SOX 法対応のための IT 予算が増加されることに示されるように、全社的にシステム導入・維持・運用など行なう IT 部門への影響も大きい（因みに、内部コントロール（Internal Control または内部統制）とは、後述するトレッドウェイ委員会組織委員会（COSO）が 1992～94 年に公表した報告書「Internal Control - Integrated Framework」の中で示したフレームワークの中で、「（業務の有効性・効率性、財務諸表の信頼性、関連法規の遵守

に）分類される目標を達成するために、合理的な保障を提供することを意図した、取締役会、経営者及びその他職員によって遂行される１つのプロセスである。」と定義されている）。

調査会社のロバート・フランシス・グループ（Robert Francis Group）社が 2003 年に実施した調査結果によると、SOX 法の影響を受ける部門として、95.7%が「IT 部門」を挙げた（当然のことながら、100%の企業が「財務部門」と回答）。

SOX 法の影響に対処するにあたり、企業の IT 部門は解決しなければならない課題に直面している。以下では、①IT 投資決定に対する CFO の強まるコントロール、②アウトソーシング管理、③セキュリティ対策について説明する。

(1)　IT 投資決定に対する CFO の強まるコントロール

SOX 法 404 条（経営陣による内部統制の評価）の影響を受け、同法遵守の主たる責任を負うこととなった CFO（最高財務責任者）は、IT 投資判断への影響力を強めており、これに危機感を感じる CIO（最高情報責任者）が少なくない。

米国では、SOX 法成立以前に、数年前の IT バブルにおける過剰投資のツケで、CIO の権限は低下する傾向にあった。IT バブル崩壊以前は、CEO に直接報告義務のあった CIO のポジションであったが、現在は、CIO は IT 投資判断をまず CFO に仰がなければならない状況に陥っていた。SOX 法が施行に移されるに至り、企業財務コンプライアンスの強化を掲げる CFO は、さらに IT 投資判断を慎重に行なう傾向を強めており、IT 部門の活動を制限することにつながっている。

CFO の慎重姿勢を強める背景として、CFO をはじめとする財務部門が SOX 法における IT の重要性を理解していないということが指摘されている。先述のロバート・フランシス・グループによる報告では、「『財務部門が SOX 法に関連するテクノロジーの問題を理解しているか』という点について、企業の回答は分かれた」としており、企業内部において、財務部門が SOX 法対策における IT 部門の役割についてよくわかっていないことが示された。

こうした状況下で、「企業の IT 幹部はまず、SOX 法の遵守やそのための必要条件について率先して学ぶとともに、ビジネス上の課題について把握することが必要であり、そうすることで SOX 法遵守のための適切な IT ソリューションを構築するアドバイザーとして活躍すべきである」と、ロバート・フランシス・グループは提案している。

(2)　アウトソーシング管理

SOX 法は、企業における財務管理の内部コントロールを徹底し、さらにその統制状況を外部の第三者が監査することを規定したものである。しかし、米国の多くの企業が財務管理に関連する多くの業務をアウトソーシングしているために、アウトソーシング企業の管理も SOX 法における内部コントロールに含まれるとの解釈が広がり、アウトソーシングを積極的に利用する傾向のある IT 部門はその対応も求められている。

公開企業会計監督委員会（Public Company Accounting Oversight Board: PCAOB）が 2004 年 3 月 9 日に発表した「監査基準 No.2：財務ステートメントの監査に伴って行われる財務報告に関する内部コントロール監査（Auditing Standard No. 2, An Auditing of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements）」の中で、「サービス機関（service organization＝アウトソーシング企業）のサービスを自社の情報システムの一部として利用している（一定の範囲で）場合、それらは財務報告に関する企業内部コントロールに求められる要素の一部である」とし、企業マネジメントおよび会計監査官は、アウトソーシング先の企業によって提供されるサービスについても、企業内部コントロールの一部として対処する必要があるとの見解を示した。さらに PCAOB は、「アウトソーシング企業を利用したからといって、財務報告に際して求められる効率的内部コントロール責任が軽減されることはない」との注釈をしている。この PCAOB とは、SOX 法により、投資家の利益を保護するとともに国民の利益のために有益で公正かつ独立性のある会計監査報告が作成されるよう、上場企業の会計監査官を監督することを目的として設立された非営利民間組織である。

企業マネジメントおよび会計監査官が、アウトソーシング企業の財務管理に関する内部コントロールを把握するための具体的方法としては、①自社の財務管理に関係しているアウトソーシング企業の管理状況、およびアウトソーシング企業のサービスを受けている社内業務などついて熟知する、②企業マネジメントの評価や会計監査官による監査が有効に機能していることを示す証拠を入手することとされている。このうち、②については、以下の 3 つの選択肢があるとされている。

a. ユーザ機関（サービスを利用している企業）で実施している検査をアウトソーシング企業から提供されるサービスに対しても適用する。

b. アウトソーシング企業内で独自に検査を実施する。

c. アウトソーシング企業で利用している検査およびその検査方式についての有効性を評価した報告をアウトソーシング企業から入手する。

なお、c.の「アウトソーシング企業で実施している検査の評価報告」として最も認知されている報告形式の一つに、米国監査基準書第 70 号（Statement on Auditing Standards 70、略称「SAS70」）がある。SAS70 は、米国公認会計士協会（American Institute of Certified Public Accountants: AICPA）によって開発された監査標準で、サービス機関は SAS70 を利用することで、一様の報告形式にのっとり自社のコントロール活動や手順を顧客企業および顧客企業の会計監査官へ開示することができる。

(3) セキュリティ対策

SOX 法の文面では、企業の IT に関する具体的な規定はないものの、関係者の間では SOX 法遵守のためにはセキュリティが重要であるとの認識が広まっている。例えば、セキュリティ技術ベンダの業界団体であるサイバーセキュリティ業界連盟（Cyber Security Industry Alliance: CSIA）は、「SOX 法および公開企業会計監督委員会（PCAOB）による監査標準の内容を解釈すると、SOX 法 404 条の遵守には情報セキュリティが必要であることは明白である」との見解を示している。

SOX 法の関連条項に対するセキュリティ対策の必要性について、情報セキュリティ専門家の Keith Pasley は業界誌 Developer.com の中で、以下の図表のようにまとめている。

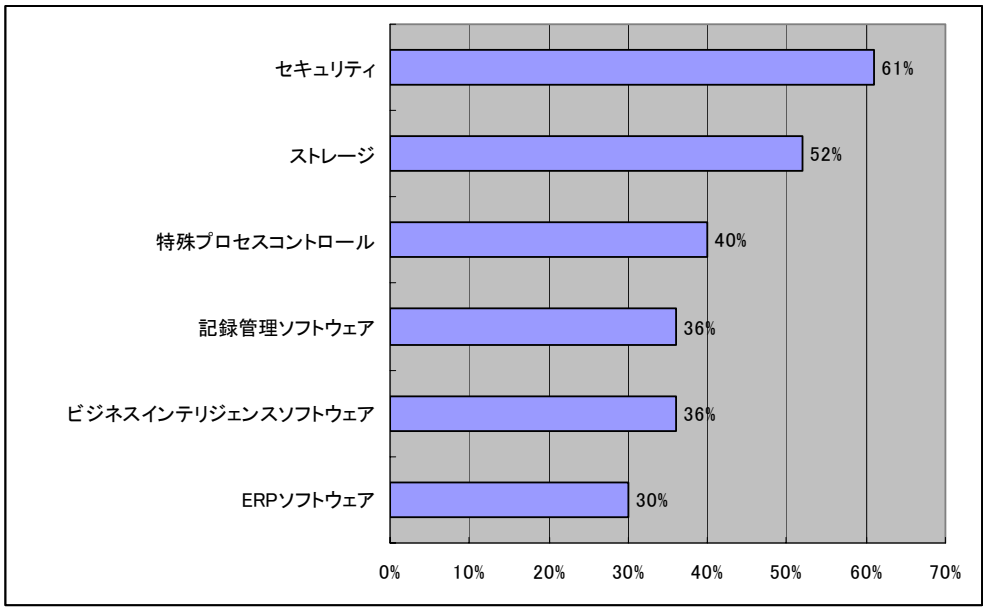
SOX 法関連条項遵守にあたってのセキュリティ上の問題点

Statute	Summary	Threat	Possible Requirement
Section 302—Corporate Responsibility for Financial Reports	Requires executives to certify the accuracy of corporate financial reports.	Unauthorized modification of data; data fraud	Authenticate data using strong data integrity controls—secure hash of data, row level encryption, provide detailed user level logging of access and data change events
Section 404—Management Assessment of Internal Controls	Requires executives and auditors to confirm the effectiveness of internal controls for financial reporting.	Unauthorized access to data, data deletion	Robust access controls, interoperable with enterprise authentication, access and auditing

Section 409—Real Time Issuers Disclose	Requires any material changes in financial state of issuer be communicated quickly and with supporting data to the public.	Non-Availability of data, data recoverability issues, backup, and restore	Data mirroring, Application resilience against DoS, unauthorized application shutdown, data properly recorded and reported

セキュリティ対策が必要であるとする法解釈が広まるにつれ、企業の IT 部門は SOX 法遵守のためにセキュリティ・ソリューションの導入を考えていることが、調査会社 Forrester Research が 2004 年 5 月に発表した調査結果で明らかになった。同調査では、SOX 法遵守のため、向こう 12 ヶ月間に予算増を予定している技術分野として、「セキュリティ」と回答した企業が 61%と最も多かった（61%）。

向こう 1 年間に予算増を予定している技術分野（複数回答）



また、CSIA は 2005 年 8 月に、「IT セキュリティと SOX 法の遵守：教訓を語り合うラウンドテーブル（IT Security and Sarbanes-Oxley Compliance: A Roundtable Dialogue of Lessons Learned）」を開催し、企業経営者、会計監査企業、法律顧問、IT セキュリティ担当幹部などが、「SOX 法遵守の初年度に得られた教訓」として、以下の 5 点を挙げている。

SOX 法遵守の初年度における５つの教訓

① **SOX 対応に企業は猛スピードのキャッチアップが必要とされた。** 相次ぐ企業スキャンダルで企業リーダーへ注目が集まったことや、SOX 法の早期制定に至った議会の政治的状況から、IT ガイダンスが十分であるか否かにかかわらず、SOX 法遵守の初年度はあらゆる企業がその対応のために急ピッチで準備を強いられた。
② **IT セキュリティは CEO の優先事項となっていなかった。** 404 条の遵守には IT が重要であるという事実が、上級マネジメントによって十分理解されていないため、彼らは IT を優先的に考えていない。その理由として、議会が IT 問題に沈黙している点が挙げられる（通常、CEO は議会の言うことを聞き、議会の決定に促されて行動する）。さらに、「内部コントロール」のコンセプトと IT が果たす役割の関係も、企業リーダーたちによって十分に理解されていない。
③ **企業マネジメントと法務顧問は会計監査官に従う傾向が強かった。** SOX 法 404 条は、マネジメントと会計監査官の責任をそれぞれ別個にすることを意図している。しかし実際には、404 条の解釈や導入に関して、マネジメントや法務顧問は監査官に従う傾向が強かった。
④ **COSO フレームワークは十分なガイダンスではなかった。** 404 条では、「企業の内部コントロールは、専門家グループが正当な手続きに基づいて確立した、適切かつ一般に認識されたコントロール・フレームワークに基づいて行われなくてはならない」と述べ、具体的に、トレッドウェイ委員会を支持する組織委員会（Committee of Sponsoring Organization（COSO） of the Treadway Commission）による COSO フレームワーク（詳細は後述を参照）に言及している。しかし、COSO フレームワークだけではガイダンスとして不十分で、中には「COSO は広範すぎる」という指摘もある。
⑤ **従来のコントロール・プロセスや手順が SOX 法遵守に向けた作業に影響を及ぼした。** すでに組織全般にわたる内部コントロールを導入していた企業は、404 条の遵守期限を守る上で、時間的に余裕があったが、確実な内部コントロールを確立していない企業は、より複雑な遵守プロセスに直面することになった。

(4)　SOX 法遵守に向けた企業の取り組み

これまで述べてきたように、SOX 法遵守は企業に大きな負担をもたらし、それゆえ「株式の非公開化」を検討する企業も出てきているが、遵守の取り組みが企業の改善や強化につながった例も少なくない。ここでは、SOX 法遵守の取り組みを広範なエンタープライズ・リスク対応の取り組みとしてとらえたマスターカー

ド（Master Card International）社と、SOX 法遵守の取り組みが新たなセキュリティ技術の導入につながった携帯電話会社ネクステル（Nextel）社（2005 年 8 月にスプリント（Sprint）社と合併し、スプリント・ネクステル（Sprint Nextel Corporation）社となった）について紹介する。

① マスターカード社

マスターカード社が SOX 法遵守の取り組みを開始したところ、コンサルタント会社のデロイト＆トウシュ（Deloitte & Touche）社、外部会計監査会社であるプライスウォーターハウス・クーパース（PricewaterhouseCoopers）社によるスタッフ作業時間は延べ 4 万 5000 時間となり、そのコストは相当なものとなった。しかし、同社は、SOX 法遵守の取り組みを企業改善のチャンスと前向きにとらえた。SOX 法遵守の取り組みの一環として、社内データベースを開発し、ドキュメンテーションの収集および記録、1000 以上の主要な財務コントロールの情報の検査を行ったところ、固定資産報告の財務処理に関して、自動化システムが導入されているにもかかわらず、手動で処理されていることが判明するなど、財務コントロールのドキュメンテーションに一貫性がないことや、自動化が適切に行われていないコントロールなどを発見することができたという。

この結果に基づき、可能な部分は自動化を進め、財務報告における人的ミスを削減することが可能になった。「SOX 法は財務報告に関連するリスクにしか焦点を当てていないが、企業はそれ以外にもさまざまなリスクを抱えている。こうしたことから、SOX 法遵守の取り組みを、広範なエンタープライズ・リスク対応の取り組みとして利用した」と、マスターカード社の最高財務責任者（CFO）であるクリス・マックウィルトン（Chris McWilton）氏は述べている。

② ネクステル社

ネクステル社のマネジャーたちは、SOX 法遵守の取り組みの過程で、従業員による重要なデータやプログラムへのアクセスの管理について、より注意を払う必要があることを発見した。同社では、アクセス・コントロールのポリシーが文書化されていたものの、それらは忠実に守られておらず、ずさんな状況であった。こうしたことから同社では、Thor Technologies 社の Xellerate Identity Manager システムを導入し、同社の 9 万人のユーザ・アイデンティティー管理を自動化し、アクセス権限の管理を強化した。同社のある幹部は、「管理業務として始まった SOX 法遵守の取り組みが、競争力の向上へと発展した」と考えている。

アクセス・コントロールを自動化することは、情報セキュリティの強化にもつながる。アクセス・コントロールと情報セキュリティは、SOX 法のほか、「医療保険の携行性と責任に関する法律（Health Insurance Portability and Accountability Act: HIPAA）」の遵守においても重要な要素となっている。アクセス・コントロールと情報セキュリティの重要性が高まるなか、従来、個別に行われてきたそれぞれの活動は、現在、双方をうまく組み合わせて行う重要なビジネス・プロセスへと変わりつつある。

4. SOX 法遵守のフレームワーク

(1) SOX 法対応 IT コントロールのフレームワーク

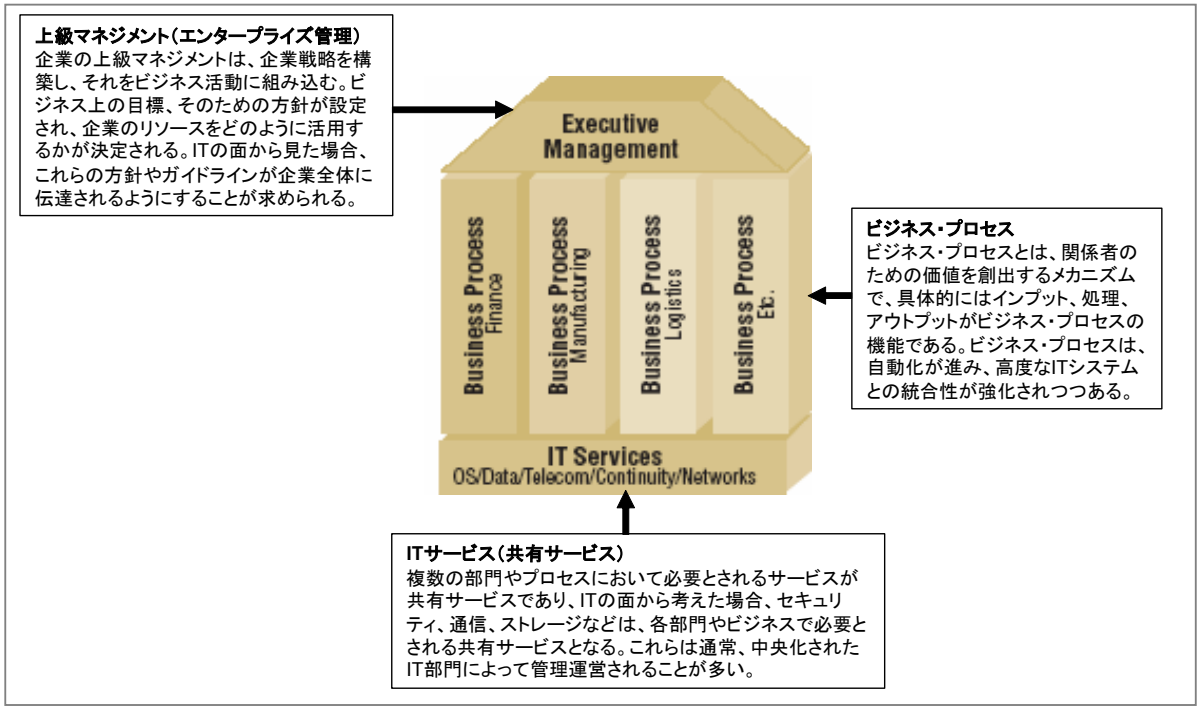
企業独自の取り組みをサポートする形で、企業が SOX 法に準拠するために必要となる IT 管理のためのフレームワーク作成が進んでいる。IT ガバナンスを推進する民間団体、IT ガバナンス研究所（IT Governance Institute: ITGI）は、2004 年 4 月、「SOX 法のための IT コントロール・オブジェクティブ（IT Control Objectives for Sarbanes-Oxley）」と題する報告書を発表した。以下、同報告書に基づき、①SOX 法遵守に IT コントロールのフレームワークを必要とする背景、②IT コントロールの課題、③COBIT と COSO フレームワーク、④遵守のためのロードマップについてまとめる。

① SOX 法遵守に IT コントロールのフレームワークを必要とする背景

同報告は、現在、企業の財務報告を取り巻くプロセスは、ERP やその他の IT システムによって機能しており、こうしたシステムは、財務取引の着手、認証、記録、処理、報告に深く関与しているため、企業が SOX 法に遵守するためには、その他の重要なプロセスとともに、IT システムも改めて評価する必要性があるとしている。

こうした背景から、SOX 法に対応した財務文書の監査標準として、PCAOB 監査標準 No.2「An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements」などでは、IT コントロールのフレームワークの必要性が強調されてきたが、SOX 法に基づく IT コントロール・フレームワークは存在してこなかった。そこで、ITGI はこれまでに開発した一般的な（SOX 法に特化しない）IT コントロール・フレームワークである COBIT（Control Objectives for Information and related Technology）をベースとしたフレームワークを提示すべく、同報告書を作成するに至った。

企業の 3 つの要素



② IT コントロールの課題

SOX 法では、企業のマネジメントに対し、財務報告に関する内部コントロールの有効性を評価、監視、報告することを義務付けており、この目標を達成するために IT 部門が果たす役割は非常に重要である。ERP システムを利用しているにしろ、運営および財務管理のさまざまなソフトウェア・アプリケーションを利用しているにしろ、IT は有効な内部コントロールを確立する基礎となる。

有効な内部コントロールを確立するためには、企業の SOX 法遵守チームに IT 部門の代表者を入れ、IT コントロールを確実に行うことが必要である。SOX 法遵守における IT 部門の責務として、ITGI の報告では以下の点が求められると指摘している。

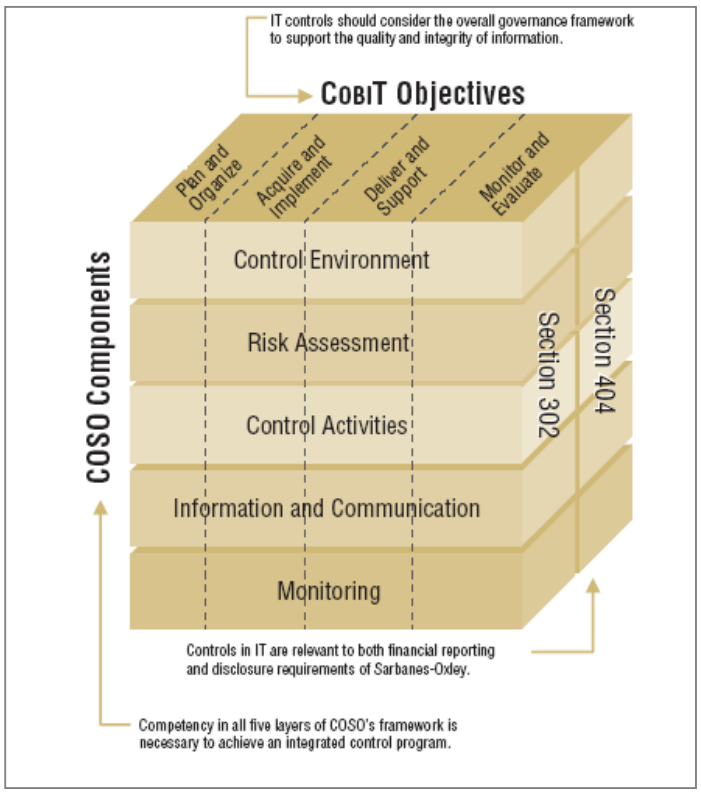
- 企業の内部コントロール・プログラムおよび、財務報告プロセスに関する理解。
- 内部コントロールおよび財務報告プロセスを支える IT システムのマッピング。
- IT システムに関連するリスクの発見。

- 発見したリスクを軽減し、有効性を継続的に監視するためのコントロールの設計および導入。
- IT コントロールのドキュメント化および検査。
- 内部コントロールや財務報告のプロセスが変更された場合、必要に応じて IT コントロールが改良、修正されるようにすること。
- 効果的な運営を目的とした IT コントロールの継続的な監視。
- SOX 法対応プロジェクトのマネジメント・オフィスに IT の担当者が参加すること。

③　COBIT と COSO フレームワーク

また、ITGI の報告書『IT Control Objectives for Sarbanes-Oxley』では、情報セキュリティおよび IT コントロールのプラクティスのガイダンスとして ITGI が開発した COBIT を基に、証券取引委員会（SEC）が推奨する COSO フレームワークに合致させる形で、IT コントロールのフレームワークを示している。ITGI は、同報告書の作成に当たり、SEC が COSO を推奨していることから、COSO のフレームワークを支持することは重要であると考えた。

COBIT と COSO の内部コントロール・コンポーネント



＜COBIT＞

COBIT (Control Objectives for Information and related Technology) は、Information System Audit and Control Association （ISACA）によって、1996 年に発表された情報システムのコントロールに関する基準として公表された。2000 年にその第 3 版が ITGI から発表され、IT ガバナンスの成熟度モデル（5 段階）が組み込まれた。COBIT は現在、情報及び IT、またそれに関するリスクをコントロールするためのプラクティスとして、世界中で導入されている。

ITGI の報告書によれば、COBIT のコントロールには一般的に、IT コントロールのための環境、コンピュータ・オペレーション、プログラムやデータへのアクセス、プログラム開発およびプログラムの変更がある。これらのコントロールは、メインフレームからクライアント・サーバまであらゆるシステムに適用される。各コントロールをまとめると、以下のようになる。

IT システムのコントロールの内容

IT コントロール環境（IT control environment）
IT コントロール環境とは、IT ガバナンスのプロセス、監視、報告の状況を指している。IT ガバナンスは、IT がビジネスに価値をもたらすこと、およびリスクを軽減するよう構築されなくてはいけない。PCAOB は、コントロール環境の重要性を認めており、「非効率的なコントロール環境は、重大な欠陥とみなされるべきであり、財務報告の内部コントロールに重要な弱点があることを示唆すると考えるべきである」と述べている。
コンピュータ・オペレーションのコントロール（Computer operations）
IT インフラの定義、購入、導入、設定、統合に関するコントロール、および日々の運営（情報サービスの伝達）のコントロール。また、オペレーション・システム・ソフトウェア（オペレーティング・システム・ソフトウェア、データベース管理システム、ミドルウェア・ソフトウェア、通信ソフトウェア、セキュリティ・ソフトウェアなど）の効果的な購入、導入、設定、管理のコントロールも含まれる。
プログラムやデータへのアクセスのコントロール（Access to programs an data）
ネットワーク化が進むなか、プログラムやデータへのアクセス・コントロールは重要性を増しつつある。効果的なアクセス・セキュリティ・コントロールを実施することで、不適切なアクセスやシステムの不正使用を防止する確証が強化される。
プログラム開発およびプログラムの変更のコントロール（Program development and program change）
プログラム（アプリケーション・ソフトウェア）の開発および変更のコントロールの対象には、新アプリケーションの購入および導入と、既存のアプリケーションの管理がある。新アプリケーションの購入および導入はトラブルを伴うことが多く、このリスクを軽減するために、システム開発や品質保証に関する手順を確立する企業もある。一方、既存のアプリケーションの管理は、管理方法の変化や改良版の導入に対応するもので、システムの変化が正しく導入されるよう、適切なコントロールを実施することが必要である。

＜COSO フレームワーク＞

一方、SEC が推奨する COSO (Committee of Sponsoring Organizations of the Treadway Commission)のフレームワークは、企業の内部コントロールのためのフレームワークとして知られる。SOX 法は具体的な遵守のためのフレームワークを含んでいないため、SEC は、特に COSO の提言をフレームワークとして使うようにとの特定の指示を出している。

COSO は、ビジネス倫理、効果的な内部コントロール、企業ガバナンスを通じて財務報告の質を向上させることを目的とし、1985 年に、「不正財務報告に関する全米委員会（National Commission on Fraudulent Financial Reporting）イニシアチブを支援する組織（Committee of Sponsoring Organizations of the Treadway Commission）」として発足したものである。これは、不正な財務報告につながる要素について分析し、それらを基に勧告をまとめたイニシアチブであり、同委員会の委員長の名称から、通称「トレッドウェイ委員会（Treadway Commission）」と呼ばれる。

COSO は、効果的な内部コントロールの重要な要素として以下の 5 つを挙げている。各要素を簡潔にまとめ、IT との関連性について示すと以下のようになる。

COSO による効果的な内部コントロールの要素

コントロール環境（Control environment）
＜内容＞ コントロール環境は、効果的な内部コントロールの土台を成すものであり、企業トップの姿勢を確立し、企業ガバナンス構造の頂点を示すものである。コントロール環境で提起された問題は企業全体に適用される。 **＜IT との関連性＞** 企業全体のコントロール環境と IT の問題について注意すべき点としては、「IT 部門は、ビジネス部門とは切り離して考えられることが多く、それゆえコントロール環境も別個に考えられてしまうことが多い」、「IT は、技術的に複雑な要素であるだけでなく、これらの複雑な要素をどのように企業全体の内部コントロールシステムに統合するかという点においても複雑な問題であることを理解する必要がある」などが挙げられる。
リスク評価（Risk assessment）
＜内容＞ リスク評価とは、マネジメントが、定められた事業目標を達成する上での関連リスクを認識および分析することである。リスク評価は、企業レベル（組織全体）および、活動レベル（特定のプロセスや事業部門ごと）で行われる。 **＜IT との関連性＞** 企業レベルのリスク評価においては、企業の SOX 法遵守運営委員会の下に IT 計画小委員会を設置し、IT 内部コントロール戦略計画の開発や効果的かつタイムリーな実施、企業全体の SOX 法遵守計画との調整の監督を責務とすることが求められる。

コントロール活動（Control activities）
＜内容＞ コントロール活動とは、事業目標の達成を目指すとともに、リスク軽減戦略を遂行すべく、導入される方針や手順、プラクティスのことである。 **＜IT との関連性＞** 信頼性の高い情報システムや有効な IT コントロール活動なくして、企業が正確な財務報告を作成することは難しいだろう。COSO もこの点を認識した上で、情報システムのコントロール活動として、「一般コントロール（general controls、企業のアプリケーションシステムから信頼性の高い財務情報を作成することを確実にするためのコントロール）」、「アプリケーション・コントロール（ソフトウェア・プログラムに組み込まれ、不正な取引を防止または発見するためのコントロール）」について言及している。
情報および通信（Information and communication）
＜内容および IT との関連性＞ COSO は、「人々が自分の責務を遂行できるよう、適切な情報が適切な形式と時間に認識、管理、伝達されなくてはいけない」と述べている。適切な情報を認識、管理、伝達することは IT 部門にとって大きな課題となりつつある。コントロールの目標を達成するために適切な情報を判断し、その情報を伝達することは、COSO フレームワークのその他の 4 つの要素をサポートすることにもなる。
監視（Monitoring）
＜内容＞ マネジメントが内部コントロールを監視することは、IT 管理の重要な任務となりつつある。監視には、継続的な監視と、個別の監視（内部監査、外部監査、規制面の検査など個別の評価）の 2 種類がある。 **＜IT との関連性＞**コントロールの有効性を測る測定基準などを用いて、IT のパフォーマンスや効果が監視されるケースが増えている。また、個別の監視によって IT 部門が監視されることも多い。

＜COBIT と COSO の要素比較＞

ITGI は、COBIT に基づく IT コントロールと、COSO のフレームワークの要素を一覧にして比較している。この中で、COSO と COBIT の要素がかなりの分野で重なっていることがうかがえ、COBIT を同法遵守の IT コントロールにも適用可能であることを示している。

COBIT の IT プロセスと COSO の要素の関係

企業レベル	活動レベル	COBIT のエリア	COSO の要素				
			コントロール管理	リスク評価	コントロール活動	情報および通信	監視
Plan and Organize （IT のコントロール環境）							
●		IT strategic planning	●	●		●	●
●		Information architecture			●	●	
		Determine technological direction					
●		IT organization and relationship	●			●	
		Manage the IT investment					
●		Communication of management aims and direction	●			●	●
●		Management of human resources	●			●	
●		Compliance with external requirements				●	●
●		Assessment of risks		●			
		Manage projects					
●		Management of quality	●		●	●	●
Acquire and Implement（プログラム開発およびプログラムの変更）							
		Identify automated solutions					
	●	Acquire or develop application software			●		
	●	Acquire technology infrastructure			●		
	●	Develop and maintain policies and procedures			●	●	
	●	Install and test application software and technology infrastructure			●		
	●	Manage changes			●		●
Deliver and Support（コンピュータ・オペレーション、プログラムやデータへのアクセス）							
	●	Define and manage service levels	●		●		●
	●	Manage third-party services	●	●	●		●
●		Manage performance and capacity			●		●
		Ensure continuous service					
	●	Ensure systems security			●	●	●
		Identify and allocate costs					
●		Educate and train users	●			●	
		Assist and advise customers					
	●	Manage the configuration			●	●	
	●	Manage problems and incidents			●	●	●
	●	Manage data			●	●	
●		Manage facilities		●			

	●	Mange operation			●	●	
Monitor and Evaluate （IT のコントロール環境）							
●		Monitoring				●	●
●		Adequacy of internal controls					●
●		Independent assurance	●				●
●		Internal audit					●

④　遵守のためのロードマップ

最後に、ITGI が、SOX 法遵守のためのロードマップとして紹介しているプロセスについて取り上げる。企業の IT 担当者が SOX 法遵守のために取り組むロードマップの流れは以下の通りである。

遵守のためのロードマップ

ステップ	内容
1. 計画と領域の決定（Plan and Scope）	最初の重要なステップは、財務報告のプロセスについて理解し、そのプロセスを支える上で IT が重要となっている部分を認識することである。そうすることで、SOX 法遵守プロジェクトの対象となるべきシステムやサブシステムを把握することができる。
2. リスク評価の実施（Performa risk assessment）	正確な財務情報を提供するために重要な IT のロケーションやシステム、アプリケーションを決定したら、リスク評価を実施する。リスク評価は、ドキュメント化のレベルや検査の範囲を確定する上でのリスクを判定するのに役立つ。リスク評価には、リスクの「影響」と「（それが発生する）可能性」の 2 種類がある。
3. 重要なアカウント／コントロールの発見（Identify significant accounts/controls）	COSO は、情報システムのコントロール活動として、アプリケーション・コントロールと、一般コントロールを指摘している。アプリケーション・コントロール（ビジネス・プロセスに適用され、不正な取引を防止、発見する）に関しては、企業はまず、財務報告や開示プロセスに重大な影響を及ぼす重要なアカウントを発見することが必要である。 その後、重要なアカウントに関連するアプリケーション・コントロールを特定し、文書化する。一般コントロール（全ての情報システムに適用され、確実で継続的な運営をサポートする）に関しては、コントロールが情報の品質や正確性を支えているか、認識されたリスクを緩和するよう設計されているかについて評価する。

4. コントロール設計のドキュメント化（Document control design）	ドキュメント化は SOX 法遵守プロセスのユニークな側面である。多くの企業がコントロールを実践しているものの、それらの設計や運営を十分に示すドキュメンテーションを有している企業はほとんどない。IT コントロールの設計を定義する理論やコンセプトを理解することは、IT 部門の重要な能力となっていくであろう。
5. コントロール設計の評価（Evaluate control design）	次に、ここで一度立ち止まり、IT リスクを許容範囲まで削減するために開発されたコントロール・プログラムを評価する。
6. 運営上の有効性の評価（Evaluate operational effectiveness）	コントロール設計の評価が終了したら、導入および運営上の継続的な有効性を確認する検査を行う必要がある。コントロール活動の運営上の有効性について検査する。検査は、その他のコントロールから依存されているコントロール（具体的には、アプリケーション・コントロールが依存している一般コントロールなど）に対して、より広範により頻繁に行う必要がある。
7. 欠陥の発見および修復（Identify and remediate deficiencies）	内部コントロールにおける欠陥の重要度を判断する。欠陥の重要度には、「重要ではない欠陥（inconsequential shortcoming）」、「重大な欠陥（significant deficiency）」、「重大な欠陥（material weakness）」などがあり、その判断はさまざまな要素を検討して行う。
8. プロセスおよび結果のドキュメント化（Document process and results）	評価段階において実施された検査の結果は、記録すべきである。これらは後に、企業マネジメントの評価や会計監査官の認証の根拠となる。
9. 持続可能性の確立（Build sustainability）	ロードマップの最後は、持続可能な内部コントロールを確実にすることである。

(2)　SOX 法遵守のための補足ガイダンス

SOX 法 404 条に基づき規則を策定する SEC は、2005 年 4 月に、内部コントロール報告の実践に関するラウンドテーブル会議を開催するとともに関係機関からのフィードバックを募った。そして本会議に基づくガイダンスを 5 月に発表した。

ラウンドテーブル会議で寄せられたフィードバックによれば、企業は、「内部コントロール義務の実践により、内部コントロールの改善を実現でき、社内全体

で内部コントロールに対する意識が強化された」との認識を示したという。その一方で、「不要なコスト増や負担増を削減するために、明確化が必要な部分も指摘された」とし、これらの部分に対応することを目的にいくつかの解説がなされた。ここではその中から、IT に関係する以下の 2 点について取り上げる。

① 適度な確証、リスクベース・アプローチ、検査と評価の領域

ガイダンスによれば、企業からのフィードバックで、財務報告の信頼性について、適度な確証を達成するために必要なコントロールの特定や検査のレベルを決定するための判断やプロセスに、多くの疑問が示されたという。

企業のマネジメントは、財務報告に関する内部コントロールが財務報告の信頼性に関して「適度な確証（reasonable assurance）」を示すのに有効であるかどうかを評価することを義務付けられている。しかし、「適度な確証」とは、高度な確証を意味するが、絶対的な確証を意味するわけではない。SEC は、ガイダンスの中で「404 条の範囲において「適度」は、一つの定義や方法論を示すものではなく、さまざまな処理や結論、方法論を網羅する」と説明している。

また、SEC は、「フィードバックによれば、過剰なコントロールやプロセスが認識、ドキュメント化、検査される理由の一つとして、多くの場合、トップダウン方式やリスクベースのアプローチが効果的に利用されていないことが考えられる」と述べている。現在利用されている評価方法には、メカニズム的、チェックリスト方式が多いが、ガイドラインでは「これは 404 条の本来の目的ではない」としている。評価は、「企業の特定のリスクに焦点を当てるもの」ととらえるべきである。その理想的なアプローチは、最大のリスクにリソースを注ぎ、あらゆる重要なアカウントおよび関連のコントロールに対して、リスクに関係なく等しく着目してしまうことを避けることである。

さらに SEC は、「内部コントロールの評価の対象を決定するためにはトップダウン方式、リスクベースのアプローチを利用すべきである」と述べている。トップダウン方式とは、企業と監査官が、財務ステートメントの中の主要アカウントから調査を行い、次に、これらの主要アカウントの中で報告されたデータの基となるビジネス・プロセスや IT システムを特定していく方法である。このプロセスにおいて、財務ステートメントに直接的または間接的に影響するビジネス・プロセスや IT システムは、SOX 法 404 条の適用対象とみなされることになる。なお、このリスクベースのアプローチは、先述の ITGI によるフレームワーク報告書でも、推奨されていた。

② IT の問題

企業からのフィードバックでは、IT の内部コントロールのドキュメンテーションや検査の適切な範囲について、さまざまな見解があることが明らかになった。これは特に、「一般 IT コントロール」（プログラム開発、プログラムの変更、コンピュータ・オペレーションなど、IT 環境全般にかかわるコントロール）に関して、顕著であったという。

SEC は、「ドキュメンテーションや検査の範囲については、マネジメントの判断（judgment）が求められるが、適切なアプリケーション・コントロール（アプリケーション・システムから生成される財務情報の信頼性を確実にすることを目的としたコントロール）および、関連のある一般 IT コントロールのドキュメント化と検査が行われることを期待している」と述べている。また、「404 条においては、財務報告と関連のない一般 IT コントロールの検査は求められていない」としている。さらに、IT を対象とした内部コントロールのフレームワークの利用については、「特定の IT フレームワークを利用することは義務付けられていないものの、一部の企業においては、利用可能なフレームワークが有益となっている」との認識を示している。利用可能なフレームワークには、前述の COBIT などが考えられている。

5. SOX 法にビジネス・チャンスを見出す IT ベンダ

（1） SOX 法は第二の「Y2K」とみなす IT ベンダ

企業が SOX 法遵守の取り組みに試行錯誤するなか、IT ベンダは、企業の財務報告および IT システムに大きな影響を及ぼす SOX 法は、第二の「Y2K」になり得る、と期待している。

上場企業において、使用している情報プラットフォームが一つという企業はほとんどない。実際、ビジネス・プロセス・コンサルティング会社のハケット・グループ（Hackett Group）社では、10 億ドル規模の企業では、48 種類の財務プログラムと 3 種類の ERP システムを利用しているのが平均だという。

このように多数のプラットフォームを管理し、整合性を持たせることは容易なことではない。こうしたことから、ビジネス・ソフトウェアのベンダは、SOX 法遵守を第二の「Y2K」と見なし、それがもたらすブームに大きな期待を寄せている。調査会社、メタ・グループ（Meta Group）社によれば、SOX 法 404 条遵守を目的としたソフトウェアを販売しているベンダは 50 社以上あり、さらに同社が IT

ベンダを対象として実施した調査によれば、回答企業の 92%が、「SOX 法による売上増を期待している」と答えている。

また、AMR リサーチ（AMR Research）社が、企業側を対象に行った調査でも、回答企業の 65%が、「（企業内でそれぞれ独自に利用されている ERP を連携させる）ERP インスタンス・コンソリデーションの導入を強く検討している」と回答している。同社では、SOX 法遵守は、企業が IT システムの改良や変更に投資するのに戦略的な正当性を与えているとし、「これは Y2K の時の状態と類似している」と結論している。

上記のメタ・グループ社の調査によれば、IT ベンダの 92%が SOX 法による売上増を期待しているものの、現実には、57%が、「いまのところ、期待通りにはいっていない」とも回答している。その理由はいくつか考えられるが、SOX 法遵守の初年度を経験した企業の CFO や幹部らは、その作業が非常に煩雑で、「この作業を毎年行うことはできない」と考えていることから、今後、SOX 法遵守の難作業を確実に軽減してくれる有望なソフトウェアやシステムが登場すれば、CFO たちがそれに飛び付くことは間違いないであろう。

SOX 法対応の IT 製品の売上が IT ベンダの期待どおりに伸びていない背景には、いくつかの要因が考えられる。まず、SOX 法遵守の取り組みの第一歩は、社内の経理担当者や内部監査担当者によって行われるのが一般的で、IT 部門は登場しない。また、SOX 法遵守のための予算の大半は、人件費やコンサルタントなどに優先され、ソフトウェア購入はその次になっているのが現状である。さらに、SOX 法遵守に特化したスタートアップ企業から ERP ベンダ、業界大手（IBM やマイクロソフトなど）が、次々と「SOX 法対応製品」「SOX 法対応改良版」を発売しているものの、いずれも「新製品」であり、市場のリーダーがまだ確定しないことなども挙げられるだろう。最後に、SOX 法に遵守するために必要な機能やシステムは、企業によってそれぞれ異なることが挙げられる。先述の AMR リサーチも、「全ての状況に対応できる万能型の IT ソリューションはない。SOX 法遵守を目指す企業は、まず、『404 条遵守』と『リスク緩和』というレンズを通して IT 事業を評価し、IT 投資の優先付けを効果的に行うべきである」と警告している。

(2)　IT ベンダによる SOX 対策ワーキング・グループ

一方、複数の IT ベンダ大手が結集し、グローバルな SOX 法遵守の取り組み活動を行うという動きも見られる。オラクル（Oracle）社、HP 社、サン・マイクロシステムズ（Sun Microsystems）社、日立データシステム（Hitachi Data Systems）社などは 2005 年 3 月、「インターネットの法律およびポリシーに関するフォーラ

ム（Internet Law & Policy Forum: ILPF）」活動の一環として、「電子情報作業部会（Electronic Information Working Group: CMEI）」を発足したと発表した。ILPF は、法律および公共政策のイニシアチブを通じて世界のインターネットの持続的な発展に貢献することを目的として活動する国際非営利団体である（1995 年設立）。

CMEI は、今後、官民の代表者や業界グループと協力しながら、法規の遵守と電子情報管理に関するグローバルなフレームワークの確立に取り組むという。CMEI の会長であるハラルド・コレット（Harld Collet）氏（オラクルの記録管理／コンプライアンスサポート担当製品マネジャー）によれば、CMEI の発足は、SOX 法遵守のために企業が 60 億ドル以上を投資すると見込まれることがきっかけであったという。「企業はすでに、連邦法、州法、国際法で課せられた義務を遵守するために多くのリソースを投じているなか、SOX 法によりさらにリソースの拠出が必要となる。規制の急速な増加に加え、規定の多くが不明瞭なことから、法規遵守は、非常に難しくかつ高コストとなっている」と同氏は述べている。

CMEI の今後の具体的なスケジュールはまだ決まっていないが、法規遵守に伴う技術的な問題やビジネス上の課題について議員らに助言を行うほか、ベンダや規制対象機関、政府関係者政策専門家による議論の場として定期的なフォーラムの開催、企業が効率的なビジネス活動を継続しつつ放棄遵守を促進するようなガイドラインの作成などを検討している。

(3) 注目される IT ソリューション分野

SOX 法 404 条の遵守が Y2K 並みの売上増をもたらすと期待する IT ベンダは、さまざまなソフトウェアやソリューションの開発に取り組んでいる。ここでは、業務システム統合ソリューション、リスクマネージメント・ソリューション、セキュリティ・インフラストラクチャー・マネージメント（SIM）・ソリューションについて取り上げる。

① 業務システム統合ソリューション

SOX 法 404 条では、財務報告と関連のある内部コントロールのドキュメンテーションおよび評価が求められる。これを受けて、企業の統合的管理を図る ERP のベンダは相次いで「SOX 法 404 条対応製品」を販売している。ERP ベンダは当初、「ERP のユーザ企業は、404 条に遵守するには、ERP システム内に装備されている既存のコントロールを利用するだけでよい」と主張していたが、そうすると、ERP システムがもともと有する基本的なコントロールに加え、独自に設定可能なコン

トロールをあわせると、膨大なコントロール・オプションが生じ、その中から 404 条に有効なコントロールを選択するのは難作業となる。

こうしたことから、オラクル（Oracle）社は、「Internal Controls Manager」を発売した。同製品は、SOX 法 404 条に準拠した形で、リスクやコントロール、ビジネス・プロセスの定義、監査プロセスの管理、ビジネス・プロセスおよび財務ステートメントの認証などを行う包括的なツールで、検査の効率性やリスク評価の確実性を高めるとともに、外部監査官による有効性認証コストを低下させることが可能である。このほか、ピープルソフト（PeopleSoft）社（2005 年 6 月にオラクル社に買収）の「Enterprise Internal Controls Enforcer」、SAP 社の「Compliance Management for Sarbanes-Oxley Act」など、SOX 法 404 条対応の ERP 製品は次々と販売されている。

② リスクマネージメント・ソリューション

エンロンやワールドコムなどの事件により、企業の経営者および財務責任者に対する信頼が失墜したことから、SOX 法では、企業の CEO や CFO が企業の財務ステートメントおよび提出を個人的に保証すること、ならびに企業のあらゆるレベルで情報開示のためのコントロールや手順を確立かつ実施することに責任を持つことが義務付けられた（302 条）。さらに、CEO や CFO は会計監査委員会に対して、全ての重要な問題点や重大な欠陥、詐欺行為について開示することが義務付けられている。

このように、SOX 法遵守とリスク管理は密接に結び付いており、SOX 法遵守をリスク管理の面からアプローチするソリューションを提供するベンダもある。エンタープライズ・ガバナンスおよびリスクマネージメント・ソリューション・プロバイダのオープンページ（OpenPages）社は、リスクマネージメント・ソリューションのベンダとして急成長している 1 社である。同社の Sarbanes-Oxley Express（SOE）は、プロセス管理、リスクマネージメント報告、ドキュメント管理、コンプライアンス・レポジトリー（収納庫）の 4 つの要素で構成されている SOX 法コンプライアンス・ソリューションである。SOE は、企業の内部コントロール・フレームワークのデザイン、ドキュメンテーション、レビュー、承認、検査といったプロセスを自動化するとともに、COSO ベースのリスク管理フレームワークにより、遵守に要する時間の短縮および迅速な監査が可能になる。さらに、金融情報の開示のためのサーベイ自動化機能により、各プロセスを実施した担当者がまずプロセスの認証を提出し、各事業部門の幹部たちの認証を受け、最終的に企業マネジメントが最終レビューおよび認証を行う、という流れが確立できる。

③　SIM ソリューション

SOX 法や HIPAA では、企業のネットワークや情報セキュリティの監査を定期的に実施し、記録するよう義務付けている。「情報セキュリティとは企業のネットワークを脅威から守るだけではない。企業のアカウンタビリティの一つでもある」（調査会社、Ptak, Noel & Associates の社長）と指摘されるように、企業マネジメントは、自社のインフラおよび資産を保護するために適切な策を講じていることを確実に証明する必要がある。こうした点に着目してソフトウェアやソリューションを提供するのが、セキュリティ・インフラストラクチャー・マネージメント（SIM）のベンダである。SIM ソフトウェアは、セキュリティ関連機器のイベント・ログ・データを自動収集し、集合データや各イベントの相関関係などを分析し、情報セキュリティを目的としたユーザのデータ管理に役立てることを狙いとしている。

SIM ソリューションを提供しているベンダの一つに、インテリタクティクス（Intellitactics）がある。同社では、SIM 製品として、Network Security Manager（NSM）を販売している。NSM は、脅威の可能性があるイベントを特定し、セキュリティ関連機器に警告を発することや、情報セキュリティに影響を及ぼすイベントが特定の機能または部門に影響を及ぼす可能性などを分析することが可能である。インテリタクティクス社では従来、NSM をアプライアンス型のバンドル・ソリューションとして販売していたが、2005 年 2 月、「報告に関する法規遵守のニーズと、法規遵守の環境を維持するニーズに応えるため」として、脅威管理、インシデント管理、セキュリティ報告などの機能を総合したモジュール型の統合ソリューション「Security Manager」として販売し、同年４月には、Security Manager のモジュールの最初の単独型製品として、ログのモニタリングおよび報告機能を自動化した Security Reporter を販売するなど、顧客のニーズに柔軟に応える体制を整えている。

（参考資料）

http://www.fei.org/download/foley_6_16_2005.pdf
http://www.fei.org/download/404_pr_3_21_2005.pdf
http://www.forrester.com/FirstLook/Vertical/Issue/0,6454,137,00.html
http://www.itcinstitute.com/display.aspx?ID=34
http://www.pcaobus.org/
http://www.pcaob.com/Rules/Docket_008/2004-03-09_Release_2004-001-all.pdf
http://www.sas70.com/about.htm
https://www.csialliance.org/home
http://www.developer.com/security/article.php/3320861
https://www.csialliance.org/resources/pdfs/CSIA_PostSox_Summit_Report.pdf
http://www.informationweek.com/shared/printableArticle.jhtml?articleID=159902183
http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&CONTENTID=9757&TEMPLATE=/ContentManagement/ContentDisplay.cfm
http://www.pcaobus.org/Standards/Standards_and_Related_Rules/Auditing_Standard_No.2.aspx
http://www.isaca.org/
http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981
http://www.coso.org
http://www.sec.gov/info/accountants/stafficreporting.htm
http://www.cfo.com/premium/index.cfm/l_centre/3011495?pi=/article.cfm/3011495
http://www.amrresearch.co.uk/content/printversion.asp?pmillid=16179&print=1
http://www.ilpf.org/
http://searchoracle.techtarget.com/originalContent/0,289142,sid41_gci1065665,00.html
http://www.oracle.com/applications/financials/internal_controls_mgr.html
http://www.openpages.com/solutions/sarbanes-oxley/sarbanes-oxley_express.asp
http://www.networkworld.com/news/2004/0301simmgmt.html
http://www.intellitactics.com/news_item.asp?PageID=58&NewsItem=57
http://www.intellitactics.com/news_item.asp?PageID=58&NewsItem=61

このレポートに対するご質問、ご意見、ご要望がありましたら、
hiroyoshi_watanabe@jetro.go.jpまでお願いします。