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

財務報告に係る内部統制の設計と導入
における IT の役割について（第 2 版）

2006 年 9 月

IT Governance Institute
IT Governance Institute (ITGI™) (*www.itgi.org*) は、企業の情報技術に指針を与え、統制を実施するための国際的な基準や知識を推進する目的で1998年に設立された。ITに関する効果的なガバナンスは、ITによる経営目標のサポート、ITに対する企業の投資を最適化し、また、ITに関連したリスクと機会の適切な管理を確実にする。ITGI はITガバナンスに責任を持つ企業の経営者や取締役をサポートするため、ITに関するリソース、独自の研究およびケーススタディを提供している。

This Work is translated into Japanese from the English language version of IT Control Objectives for Sarbanes-Oxley 2nd Edition by ITGI Japan with the permission of the IT Governance Institute. ITGI Japan assumes sole responsibility for the accuracy and faithfulness of the translation.

本稿は、IT Control Objectives for Sarbanes-Oxley 2nd EditionをITGIより許可を受けてITGI JAPANが英語から日本語に翻訳をした。ITGI JAPANが翻訳の正確性及び信頼性について責任を負っている。

開示

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E- mail: *research@itgi..org*
Web site: *www.itgi.org*

ISBN 1-933284-76-5
IT Control Objectives for Sarbanes Oxley: The Role of IT in the Design and Implementation of Internal Ccontro lOver Financial Reporting, 2nd Edition
Printed in the United States of America

本冊子はIT Governance Instituteが2006 年に出版した*"IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Ccontro lOver Financial Reporting, 2nd Edition"*の翻訳版である。

免責条項

The IT Governance Institute, ISACA® and other contributors make no claim that use of this document will assure a successful outcome. This publication should not be considered inclusive of IT controls, procedures and tests, or exclusive of other IT controls, procedures and tests that may be reasonably present in an effective internal control system over financial reporting. In determining the propriety of any specific control, procedure or test, US Securities and Exchange Commission (SEC) registrants should apply appropriate judgment to the specific control circumstances presented by the particular systems or information technology environment.

IT Governance Institute、ISACA® (Information Systems Audit and Control Association)および他の寄稿者は、本稿の使用により同法の遵守が保証されるという主張は行っていない。本稿は、財務報告に係る有効な内部統制システムに合理的に存在するIT統制、手続きおよびテストをすべて含むものでも、他のIT統制、手続きおよびテストを除外しているわけでもない。特定の統制、手続きまたはテストの妥当性を判断する際、SEC登録企業は特定のシステムまたはIT環境がもたらす特定の統制状況を十分に考慮して、適切な判断を下すべきである。

Readers should note that this document has not received endorsement from the SEC, which is responsible for regulating public companies, or the US Public Company Accounting Oversight Board (PCAOB), which is responsible for regulating the public accounting profession. The issues that are dealt with in this publication will continue to evolve. Accordingly, companies should seek counsel and appropriate advice from their risk advisors and/or auditors. The contributors make no representation or warranties and provide no assurances that an organization's use of this document will result in disclosure controls, procedures, internal controls and procedures for financial reporting that:

• Are compliant with the internal control reporting requirements of the Sarbanes-Oxley Act (the Act)

• Make the organization's plans sufficient to address and correct any shortcomings that would prohibit the organization from making the required certification or reporting under the Act

本稿が、上場企業を規制する責任を持つSEC（米国証券取引委員会）、職業会計士業務を規制する責任を持つPCAOB（米国上場企業会計監視審議会）から承認を受けていないことに読者は注意されたい。本稿で扱った問題は今後さらに改訂される予定である。従って、企業はリスクアドバイザーまたは監査人から適切な助言を求めるべきである。本稿の寄稿者は、企業が本稿を用いた場合、

- 企業改革法の求める内部統制の報告要件に沿っている、
- 同法に基づいて企業が必要な認証と報告を行うことができなくなるような欠陥に取り組み、この欠陥を修正する上で、十分な財務報告に係る開示統制とその手続き、および内部統制とその手続きにつながる

と述べているのでも、またこれを保証するものでもない。

Internal controls, no matter how well designed and operated, can provide only reasonable assurance of achieving an entity's control objectives. The likelihood of achievement is affected by limitations inherent to internal control. These include the realities that human judgment in decision making can be faulty and that breakdowns in internal control can occur because of human failures such as simple errors or mistakes. Additionally, controls, whether manual or

automated, can be circumvented by the collusion of two or more people or inappropriate management override of internal controls.

内部統制は、どのように適切に設計され、運用されているにせよ、企業の統制目的の達成に向けて合理的な保証を提供するに過ぎない。達成の見込みは内部統制特有の限界により影響を受ける。これらは、意思決定における人間の判断は誤る可能性があり、内部統制の瓦解は単純な誤りなどの人為的ミスで起こり得るという現実を反映している。さらに、マニュアル（手作業）または自動化されているかにかかわらず、統制は二名以上の共謀や経営者による内部統制の無視等によって巧みに逃れることが可能である。

IT Control Objectives for Sarbanes-Oxley 2nd Editionの日本語版によせて

日本ITガバナンス協会からの翻訳第一弾として日本のITガバナンスを高めるための海外の知見を紹介する日本語化プロジェクト、COBIT for SOX 第2版の翻訳を、お約束どおり年内にUPすることができました。翻訳を担当、寄付をいただいた新日本監査法人様、レビューを担当していただいたISACAのメンバーの方々に感謝したします。

これからJ-SOXに取り組まれる皆様方に少しでも参考にしていただければ幸甚でございます。

日本ITガバナンス協会会長　松尾　明

☆☆☆

ISACA東京支部では、これまで、COBITに関する様々な研究活動を続けてまいりました。この1年ほどの間にITGIからはCOBIT4が発表され、さらに洗練されたものになってきました。また、eラーニングのコースが開発されたり、ユーザカンファレンスが世界各地で開催されるなど、COBITは、ISACAの活動の柱とするIT アシュアランス、情報セキュリティ、そしてIT ガバナンスの分野での存在価値をますます高めています。

一方日本でも、日本語版SOXに対する関心が高まってきており、"IT Control Objectives for Sarbanes-Oxley"の日本語訳を公表してから、COBITファミリーは日本でも事実上のスタンダードとして認知されるようになって来ました。そして、第2版が公表されると、各方面からタイムリーな日本語化が求められ、ここに、皆様のお手元に届けることができるようになりました。もちろんこの冊子は、米国のSOX法を対象として書かれたものではありますが、日本版SOX法に対応しようとする企業にとっても大いに参考になるものです。

この冊子の日本語化にあたっては、当支部の調査研究委員会、とりわけ、新日本監査法人の土田様には、第1版に引き続き多大な貢献を頂きました。ISACA東京支部を代表して、そしてこの冊子を利用する専門家の皆様を代表して感謝の意を表します。

ISACA東京支部2006-2007会長　高須　昌也

翻訳者まえがき

私はアメリカの企業改革法が成立した 2002 年の秋から、同法 404 条の要求にもとづいて「財務報告に係る内部統制の評価」を行う日本企業に対し、アドバイスをしてきた。

IT Control Objectives for Sarbanes－Oxley－the importance of IT in the design, implementation, and sustainability of Internal control over disclosure and financial reporting に最初に出合ったのはそんな最中の 2004 年である。 そして、2006 年 9 月には、その2版が出版された。

この報告書は、企業改革法 404 条にもとづいた評価、あるいは金融商品取引法 24－4－4 条の要求にもとづいた評価の準備作業を実施している多くの日本企業の関係者の参考書となっている。

この度、初版に引き続き、2版（2006 年 9 月公表）の翻訳にも携われたのは、望外の喜びである。

本翻訳が 2008 年 4 月 1 日以降に開始する事業年度から制度化される「財務報告に係る内部統制の評価及び監査」に関係される日本企業の皆様方のお役に立てれば、幸いである。

なお本翻訳に携った当法人のメンバーは次の通りである。

２　　版	初　　版
土田義憲	土田義憲
新津陽子	伊藤益光
竹内みゆき	加藤寛之
	新津陽子

この誌面をお借りして、御礼を述べるしだいである。

新日本監査法人
代表社員　土田義憲

新日本監査法人
ERNST & YOUNG

謝辞

IT Governance Instituteは本稿の作成にあたり、ご協力を頂いた以下の方々に厚く御礼を申し上げたい。

本稿の主な寄稿者の方々
Christopher Fox, ACA
Paul Zonneveld, CISA, CA

寄稿者の方々
Gordon Bloom, CISA, RSM McGladrey Inc., USA
Michael Cangemi, CISA, CPA, Cangemi Company LLC, USA
Nancy Cohen, CPA, AICPA, USA
Roger Debreceny, Ph.D., FCPA, University of Hawaii, USA
Robert Frelinger, CISA, Sun Microsystems Inc., USA
Kenneth S. Gabriel, CPA, KPMG LLP, USA
Michael Garber, CIA, CPA, Motorola Inc., USA
John Gimpert, CPA, Deloitte & Touche LLP, USA
John Hainaut, Jefferson Wells, USA
Hussain Hasan, CISM, CISSP, RSM McGladrey Inc., USA
Edward Hill, CIA, CPA, Protiviti, USA
Tara Janos, BP Amoco, USA
Peter Koltun, Jefferson Wells, USA
Phillip Lageschulte, CPA, KPMG LLP, USA
Elsa K. Lee, CISA, CSQA, CISM,CSQA, AdvanSoft International Inc., USA
Anthony Noble, CISA, CCP, Viacom Inc., USA
Heroit Prentice, MIIA, FIIA, QiCA, The Institute of Internal Auditors, USA
Debbie Sanneman, Motorola, USA
Sheryl Skolnik, CISA, CISM, CPA, BDO Seidman LLP, USA
Tracy Stewart, CISA, CISSP, CCP, CIA, Allstate Insurance Company, USA
Doug Underwood, CPA, McGladrey & Pullen, USA
Mickey Vaja, CISA, CCNA, CISSP, Grant Thornton LLP, USA
Kenneth Vander Wal, CISA, CPA, CSP, Ernst & Young LLP, USA
Timothy Van Ryzin, CISA, CISM, Harley-Davidson, USA
Jeffrey Ward, CISA, CPA, CITP, Stone Carlie & Company LLC, USA
Margaret Yocher, United Technologies-Carrier, USA
Paul Zonneveld, CISA, CA, Deloitte & Touche LLP, Canada

The ITGI Board of Trusteesの方々
Everett C. Johnson, CPA, Deloitte & Touche LLP（退職）, USA, International President
Georges Ataya, CISA, CISM, CISSP, Solvay Business School, Belgium, Vice President
Abdul Hamid Bin Abdullah, CISA, CPA, Auditor General’s Office, Singapore, Vice President
William C. Boni, CISM, Motorola, USA, Vice President
Lucio Augusto Molina Focazzio, CISA, Colombia, Vice President
Avinash Kadam, CISA, CISM, CBCP, CISSP, Miel e-Security Pvt. Ltd., India, Vice President
Jean-Louis Leignel, MAGE Conseil, France, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Frank Yam, CISA, CIA, CCP, CFE, CFSA, FFA, FHKCS, FHKIoD, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Robert S. Roussey, CPA, University of Southern California, USA, Past International President
Ronald Saull, CSP, The Great-West Life and IGM Financial, Canada, Trustee

The IT Governance Committeeの方々
William C. Boni, CISM, Motorola, USA, Chair
Max Blecher, Virtual Alliance, South Africa
Sushil Chatterji, Singapore
Tony Hayes, FCPA, Queensland Government, Australia
Anil Jogani, CISA, FCA, Tally Solutions Limited, UK
John W. Lainhart IV, CISA, CISM, IBM, USA
Romulo Lomparte, CISA, Banco de Credito BCP, Peru
Michael Schirmbrand, CISA, CISM, CPA, KPMG LLP, Austria
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada

The COBIT Steering Committee の方々
Roger Stephen Debreceny, Ph.D., FCPA, University of Hawaii, USA, Chair
Gary S. Baker, CA, Deloitte & Touche, Canada
Rafael Eduardo Fabius, CISA, Republica AFAP, S.A., Uruguay
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Jimmy Heschl, CISA, CISM, KPMG, Austria
Debbie A. Lew, CISA, Ernst & Young LLP, USA
Maxwell J. Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Dirk E. Steuperaert, CISA, PricewaterhouseCoopers LLC, Belgium
Robert Ernest Stroud, CA Inc., USA

The ITGI Advisory Panelの方々
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Chair
Roland Bader, F. Hoffmann-La Roche AG, Switzerland
Linda Betz, IBM Corporation, USA
Jean-Pierre Corniou, Renault, France
Rob Clyde, CISM, Symantec, USA
Richard Granger, NHS Connecting for Health, UK
Howard Schmidt, CISM, R&H Security Consulting LLC, USA
Alex Siow Yuen Khong, StarHub Ltd., Singapore
Amit Yoran, Yoran Associates, USA

ITGI加盟企業およびスポンサー
ISACA支部
American Institute for Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association of Corporate Governance
Information Security Forum
The Information Systems Security Association
Institut de la Gouvernance des Systèmes d’Information
Institute of Management Accountants
ISACA
ITGI Japan
Solvay Business School
University of Antwerp Management School
Aldion Consulting Pte. Ltd.
CA
Hewlett-Packard
IBM

LogLogic Inc.
Phoenix Business and Systems Process Inc.
Symantec Corporation
Wolcott Systems Group
World Pass IT Solutions

日本語版　翻訳者

土田義憲（新日本監査法人）
伊藤益光（新日本監査法人）
加藤寛之（新日本監査法人）
新津陽子（新日本監査法人）
竹内みゆき（新日本監査法人）

日本語版　レビュー担当者

木村章展（あらた監査法人）
松原 榮一（ガートナージャパン）
島田 裕次（東京ガス株式会社）
高浦 孝次（株式会社日立コンサルティング）
船城謙二郎（新日本監査法人）
柳沼 克志（株式会社　ITプレナーズ　ジャパン・アジアパシフィック）
畠中一浩（株式会社コーポレイト ディレクション）

目次

経営者向け要約

2004 年 4 月に、IT Governance Institute は企業による内部統制システムの評価・拡充をサポートするため、*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*を出版した。以降、同冊子は IT 統制を評価するツールとして、世界中の企業で企業改革法の遵守をサポートするために用いられてきた。

企業改革法の遵守とITガバナンス

リスクのない環境などあるわけがなく、また、企業改革法（以下「同法」）を遵守することでこうした環境が生まれるわけでもない。しかし、同法の遵守を目的として内部統制システムを向上するために大半の企業が取るプロセスは、永続的なメリットを生む可能性が大きい。計画とライフサイクルの統制（コントロール）目標に係る優れたITガバナンスにより、正確でタイムリーな財務報告につながるはずである。

企業改革法の要件を満たすために必要な作業は、単に法律を遵守するためだけのプロセスと見なすべきではない。むしろ、説明責任と業務要件に対処できるように設計された強力なガバナンスのモデルを確立する機会として捉えるべきである。ITにおける強力な内部統制プログラムを構築することにより、以下のことが可能になる。

- より効率的で効果的な業務を通じて競争力を得ること。
- リスク管理能力の向上とイニシアチブの優先順位付けの強化。
- 全体的なITガバナンスの向上。
- 経営者間でのITの理解の向上。
- セキュリティ、可用性、処理のインテグリティの統合されたアプローチにより業務の最適化を図ること。
- より高品質のタイムリーな情報を用いて、最適な業務上の決定を可能にすること。
- プライバシーなどの他の法的な要件の遵守に役立つこと。
- プロジェクトを業務要件に沿ったものとすること。
- 知的資産の損失とセキュリティ侵害の可能性を防ぐこと。

第2版で新たに追加された内容

同冊子の刊行以来、企業は財務報告と IT 統制に関して多くの教訓を学んできた。特に重要な点は、最もリスクの高い領域に十分で適切な注意を確実に払うため、企業改革法の遵守プログラムにおいて、トップダウンでリスクベースのアプローチをとることである。

その結果、ITGI は企業改革法の IT コンプライアンスに関して、学んだ教訓を共有すると同時に、財務報告に係る内部統制のより重要な領域における新たな IT の指針を提供するため、同冊子の改訂を行ってきた。同冊子の第 2 版は 60 日間公開され、ここで受けたコメントに対応して、本最終版に反映された。

同冊子の刊行以来、私たちは多くの教訓を学んできたが、2004 年 4 月に提供された基本的な指針は現在でも適切な内容である。同冊子の改訂の目的は、企業が学んだ教訓を共有し、リスクベースのアプローチを用いた企業改革法の遵守の効率性と有効性を向上させることについて新たな指針を提供することにある。改訂版の要旨は以下のとおりである。

- 対象の決定とリスク評価により大きな焦点を当てる－ トップダウンでリスクベースのアプローチを適用する際の指針が追加されている。特に、同法の IT リスク評価の実施の指針が加筆されている。
- 統制の優先順位付け － 企業が「関連する統制」を定義する際の指針が加筆された。この指針を用いて、参考資料 C:「IT 全般統制」では特定の統制が最も関連する統制として把握されている。
- 変化に関する人的要素の管理 － 同法を遵守する際に考慮する必要のある人的要素を強調するため、文化的・人的な管理に関する問題の洞察が加筆された。
- 業務処理統制（アプリケーション統制）に関する追加的な指針 － さまざまな種類の業務処理統制を把握し、これに対応するとともに、業務処理統制を用いる上での企業の実例を提供する上で企業を支援するための指針が新たに追加されている。
- スプレッドシートのアプローチ－ 統制のベストプラクティスを含む、企業のスプレッドシートへの対応をサポートするための指針が新たに加えられた。
- 遵守のためのロードマップの簡略化－ プロセスを簡略化するため、遵守に至るまでの状況を表すロードマップに変更が加えられた。
- COBIT® 4.0 のプロセスとの相互参照。
- 学んだ教訓 － 世界中の企業による同法遵守の経験を共有するため、プラス面の理解、または共通の落とし穴を避ける上で考慮すべきステップを含む、学んだ教訓に関する要旨が追加された。
- SAS70 報告書を用いる上での課題とアプローチ。
- 重要なアプリケーションの職務の分離に関する拡充された指針。

比較的小規模な企業が考慮すべき点

トレッドウェイ委員会支援組織委員会（COSO）は2006年7月、*Guidance for Smaller Public Companies Reporting on Internal Control Over Financial Reporting:*「比較的小規模な企業における財務報告に係る内部統制に関する報告書のための指針」を公表した。このCOSOの文書では、比較的小規模な企業が企業改革法などの規制を遵守する上で直面する課題を明らかにするとともに、こうした課題に対応する上での指針を提供している。

比較的小規模な企業がSOX法のもとで期待されるIT統制のすべての点に対応することは困難かもしれない。したがって、同じ方法をすべてに適用するという戦略をとらず、その代わりにリスクベースのアプローチを取り、その状況で必要かつ関連性のあるIT統制のみを実施することが重要になる。例えば、比較的小規模な企業は、大規模でカスタマイズされたエンタープライズ・リソース・プランニング（ERP/統合業務）システムではなく、比較的簡易な商用ソフトウェアの財務アプリケーションを用いることが多い。この場合、一般的にアプリケーションによる財務諸表の誤りのリスクは、より大規模で、より複雑なシステムの財務諸表の誤りのリスクよりも小さい。したがって、比較的小規模な企業に必要な統制の特徴と範囲は、大企業のそれよりも少ない。常に例外は存在するものの、比較的小規模な企業はリスクを慎重に評価し、必要な統制のみを実施する必要がある。こうしたサポートを提供するため、本稿ではリスク評価に関する指針が加筆されている。

PCAOBとCOBITとの整合性

PCAOB監査基準第2号とCOBIT（Control Objectives for Information and related Technology: COBIT®）に沿った、全部で12のIT統制目標が企業改革法遵守プログラムのために定義された。**図表1**は、本稿で述べた12のIT統制目標と、PCAOBによるIT全般統制、そしてCOBIT®4.0のプロセスを関連付けたものである。

図表 1 — PCAOB と COBIT との対応付け

	COBIT	PCAOBのIT全般統制			
COBIT の統制目標	COBIT4.0 のプロセスとの対応付け	プログラム開発	プログラム変更	コンピュータ・オペレーション	プログラムとデータへのアクセス
1. アプリケーションソフトウェアの調達と保守	AI 2	●	●	●	●
2. 技術インフラの調達と保守	AI 3	●	●	●	
3. 運用の促進	AI 4	●	●	●	●
4. ソリューションおよびその変更の導入と認定	AI 7	●	●	●	●
5. 変更管理	AI 6		●		●
6. サービス・レベルの定義と管理	DS1	●	●	●	●
7. サードパーティのサービスの管理	DS2	●	●	●	●
8. システムセキュリティの保証	DS5			●	●
9. 構成管理	DS9			●	●
10. 問題とインシデント管理	DS8 DS10			●	
11. データ管理	DS11			●	●
12. 物理的環境とオペレーション管理	DS12 DS13			●	●

本冊子の使用法

本稿の情報は、企業改革法の遵守に関連する IT 組織を組織し、維持しようとする企業に有効な指針とツールを提供している。**しかし、企業は各自の状況に合った適切な IT 統制目標を慎重に検討する必要がある。企業は本稿で述べた統制目標のうち必ずしもすべてのものを対象としなくてもよい。また、同様に、本書で述べていないものを含めてもよい。**いずれの場合にせよ、本稿で提示した統制目標、統制の例、統制のテストの例の内容を、それぞれの企業の特有な状況を反映するように変更することが必要だと考えられる。

信頼できる財務報告の基礎

IT統制に関する指針の必要性

今日の環境では、財務報告プロセスはITシステムにより運用されている。ERPまたはその他のシステムは、会計取引の開始、承認、記録、処理、報告に深く組み込まれている。したがって、ITシステムは財務報告プロセス全体に密接に関連しており、企業改革法の遵守にあたっては、他の重要なプロセスと共にITシステムを評価する必要がある。

企業改革法と内部統制の一般的な重要性について述べた文献は多くある。しかし、この領域においてITが果たす重要な役割について述べたものはほとんどない。例えば、同法は組織に適切な内部統制のフレームワークを選択し、実施するよう求めている。COSOの内部統制の統合的フレームワークは、同法を遵守する企業が最も広く用いるフレームワークとなった。しかし、COSOは、企業のIT統制の設計と導入をサポートするためには、多くの指針を提供しているわけではない。

その結果、企業は全体的な財務報告の遵守プログラムの主要部分であるITに係る統制の評価のための指針を必要としている。本稿は関連するSEC、PCAOB、COSO、COBITの内容を用いてこの点をサポートすることを意図している。COSOとCOBITに関する詳細は、参考資料Bを参照されたい。

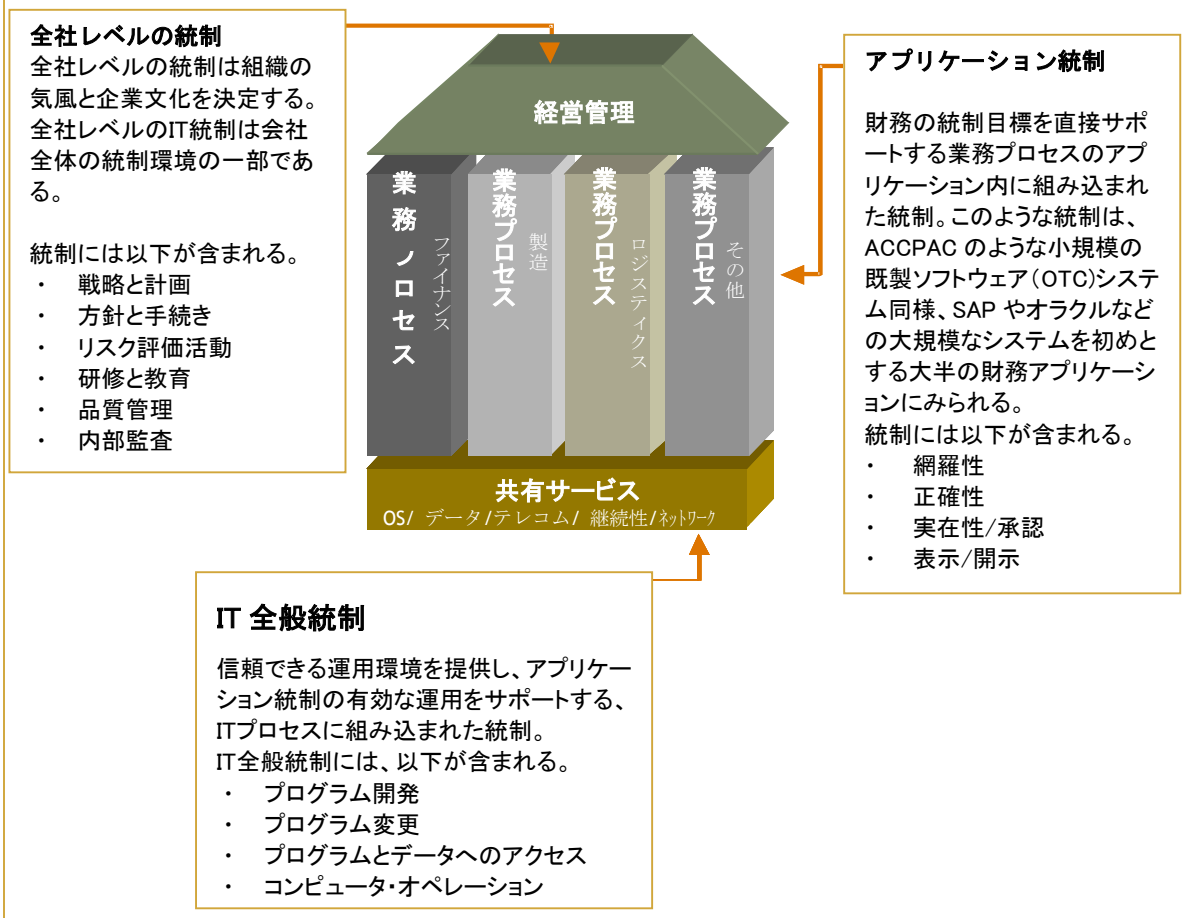
IT統制の把握

典型的な企業内で IT 統制がどこに存在するかを理解する上で、少なくとも 3 つの構成要素、つまり経営管理、業務プロセス、IT サービスを考慮する必要がある。**図表 2** は、組織に共通する構成要素を示したものである。

ITシステムは、ますます業務プロセスを自動化するようになってきている。その際、ITシステムではしばしば、マニュアル統制（人手による統制）から自動化された統制、またはIT依存型の統制に置き換えている。その結果、業務プロセスの変更と新システムの機能と足並みを揃えるため、企業改革法の遵守プログラムではシステムに基づいた統制を検討する必要がある。

経営管理	業務プロセス	IT サービス
経営幹部は、戦略を確立し、業務活動に組み込む。企業全体または全社レベルでは、経営目標を設定し、方針を確立して、企業の資源の配分と管理に関する決定を行う。ITの観点からは、企業の方針と企業全体の他の指針が企業で設定され、伝達される。	業務プロセスは、企業の関連当事者に対して価値を創造し、実現する仕組みである。入力、処理、出力が業務プロセスの機能である。業務プロセスはますます自動化され、複雑で極めて効率的な IT システムに統合されつつある。	IT サービスは、業務の基礎を成し、業務プロセスまたは事業拠点ごとに分離されるのではなく、全組織を通じて提供される。IT サービスは一般に、ネットワーク管理、データベース管理、オペレーティングシステム管理、ストレージ管理、施設管理、セキュリティ管理を含み、多くは中央の IT 部門が管理を行う。

図表 2 – 組織共通の構成要素



IT統制 - 特有な課題

企業改革法は、財務報告に係る内部統制の有効性を確立し、評価し、監視する責任が経営者にあることを明確にしている。大半の企業にとって、この目的を達成する上でのITの役割は極めて重要である。統合されたERPシステムであれ、あるいは本質的に異なる業務および財務管理アプリケーションソフトウェアの寄せ集めであれ、ITは財務報告に係る有効な内部統制システムの根幹である。

しかし、この状況により特有の課題が生じている。というのは、ITシステムが生成する情報の品質とインテグリティに責任を負うITの専門家の多くが、内部統制の複雑さに十分に精通していないことである。これは、ITがリスクを管理していないことを意味するのではなく、企業の経営者や監査人が求めている方法ではリスクが形式化、あるいは構造化されていない可能性があることを意味している。

企業は、ITモニタリング統制、IT全般統制および業務処理統制が存在し、企業改革法の遵守目標をサポートしているかどうかを判断するため、企業改革法のチームにIT専門家を参加させる必要がある。ITの重要な責任分野は以下を含む。

- 組織の内部統制のプログラムと財務諸表作成プロセスの理解。
- 内部統制および財務諸表作成プロセスをサポートするIT環境（ITサービスとプロセス）と財務諸表との関連付け。
- これらのITシステムに関連するリスクの把握。

- 把握されたリスクを低減するための統制の設計と導入、および継続的な有効性に関する統制のモニタリング。
- ITおよびシステムベースの統制の文書化とテスト。
- 内部統制または財務諸表作成プロセスの変更に対応して、IT統制が必要に応じて更新され、変更されていることの保証。
- 長期にわたる有効な運用を目的としたIT統制のモニタリング。
- 企業改革法を遵守のためのプロジェクト・マネジメント・オフィス（PMO）へのIT専門家の参加。

企業改革法に影響を与えるSECの規則が複雑であることは間違いなく、導入には時間とともに多くの費用がかかっている。IT統制の評価作業を進めるにあたり、考慮に入れなければならない二つの重要な事項がある。

- わざわざ一からやり直す必要はない。実質的には、ほとんどの公開企業には何らかのIT統制がある。統制が非公式で、文書化が十分でなく、統制機能に関する十分な証拠に欠けていているかもしれないが、一般的に、セキュリティと変更の管理の分野においてIT統制は存在している。
- 多くの企業は、既存のIT統制プロセスを企業改革法の条項を遵守するように作り上げることが可能である。多くの場合、企業に欠けているものは統制の文書化の一貫性と品質ならびに証拠である。しかし一般的なプロセスはしばしば機能しており、多少の修正を必要としているに過ぎない。

企業の発展にともなってIT統制のプロセスを十分にレビューし、文書化することは、時間のかかる作業である。業務プロセスのリスクと環境により、アプリケーションとITプロセスの評価範囲が決まる。適切な知識と指導がなければ、企業は作業量が多すぎたり、少なすぎたりするリスクを冒すことになろう。責任者がIT統制の設計や評価の経験者でない場合、または最も重要なリスク領域を把握し、焦点を合わせる上で必要なスキルや管理構造を持っていない場合、このリスクは増幅する。

金融サービスなどの一部の業界は、公開市場の環境の厳格な規制と遵守の要件に精通しているが、ほとんどの業界はそうではない。企業改革法の要求を満たすため、大半の企業は企業文化の変革過程にある。特にIT統制の設計、文書化、統制の証拠の維持および評価において、ITシステムとプロセスの強化が必要になっている。

IT統制に関するPCAOBの指針

PCAOB監査基準第2号は、ITと財務報告に係る内部統制の関係を述べており、IT統制の把握と内部統制の設計上・運用上の有効性とテストの重要性を強調している。特に同基準は、以下のように述べている。

> *…財務諸表におけるすべての重要な勘定科目と開示に関連するアサーションに関する統制を含めて、統制をテストする必要がある。一般的にこのような統制は以下を含む。*
> 特に、
> - *IT全般統制を含む、他の統制が依拠する統制*

続いてPCAOB監査基準第2号は、経営者の評価をサポートするための適切なアサーション（適切な財務情報を作成するための要件）や目的を決定する際に、監査人が従うべきプロセスについて説明している。

> *関連するアサーションを把握するために、監査人はそれぞれの重要な勘定科目における潜在的な虚偽記載の出所を判断しなければならない。監査人は特定のアサーションが重要な勘定科目の残高や開示に関連しているか否かを判断する際、監査人は特に以下を評価するべきである。*

- *企業がアサーションを裏付ける情報を処理し、統制する際に用いる情報技術を含む、システムの性質と複雑さ。*

また、PCAOB監査基準第2号は期末の財務諸表作成プロセスで用いられる情報技術についても述べている。

> *監査人は、期末の財務諸表作成プロセスの理解と評価の一部として、特に以下を評価しなければならない。*
> - *各期末の財務諸表作成のプロセスにおける情報技術の関与の度合い。*

ITシステムの統制

ITシステムに広く依拠することにより、大小にかかわらず、こうしたITシステムで統制が必要とされている。IT統制には一般的に、IT環境、コンピュータ・オペレーション、プログラムとデータへのアクセス、プログラム開発とプログラム変更に係る統制が含まれる。これらの統制は、財務上重要とされているシステムに適用される。

IT統制環境

PCAOB監査基準第2号では、統制環境はより重要なものとされている。同基準は、以下のように述べている。

> *…統制環境は財務報告の信頼性に大きな影響を与えるため、統制の有効性に関する監査人の予備的な評価は、必要と考えられる運用の有効性テストの性質、タイミング、範囲にしばしば影響を与える。統制環境に欠陥がある場合、監査人は欠陥が存在しない場合に実施する運用の有効性テストの性質、タイミング、範囲を変更しなければならない。*

また、PCAOBは、有効ではない統制環境は、少なくとも重大な不備として、そして財務報告に係る内部統制に重要な欠陥が存在することを強く示すものと見なされるべきであるとしている。これらのコメントは、ITの統制環境を含む全般的な統制環境に当てはまる。

ITの統制環境には、ITガバナンスのプロセス、モニタリングおよび報告が含まれる。ITガバナンスのプロセスには、情報システムの戦略計画、ITのリスク管理プロセス、遵守および規制に対する管理、ITの方針、手続き、および基準が含まれる。モニタリングと報告は、ITを業務要件に準拠させるために必要である。

ITガバナンスの構造は、ITが事業に価値をもたらし、ITリスクが低減されるように設計する必要がある。ITガバナンスは、適切な職務分離をサポートし、企業の目的の達成を促進するITの組織構造を含む。

コンピュータ・オペレーション

コンピュータ・オペレーションは、ITインフラの定義、調達、導入、構成、統合および保守管理に係る統制を含む。オペレーションに関する日常的な統制は、サービス・レベルの管理、サードパーティサービス業者の管理、システムの可用性、顧客管理、構成およびシステム管理、問題とインシデント管理、オペレーション管理スケジュールの作成、施設管理など、毎日の情報サービスの提供に関係するものである。

オペレーションのためのシステムソフトウェアの構成要素は、システムを稼動してアプリケーションを機能させるオペレーティング・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、コミュニケーションソフトウェア、セキュリティソフトウェア及びユーティリティなどの効果的な調達、導入、構成と保守管理を含んでいる。また、システムソフトウェアはインシデントの追跡機能、システムログ取得機能およびモニタリング機能なども提供している。システムソフトウェアでは、ユーティリティの使用に関する報告が可能である。このため、何者かがこうした強力なデータ変更機能にアクセスした場合、最低でもアクセスが記録され、レビューのために報告が行われる。

プログラムとデータへのアクセス

プログラムとデータへのアクセスコントロールは、企業のネットワークへの内部および外部からの接続が増加するにつれて、ますます重要となっている。企業内のユーザは、地球の裏側もしくは廊下の向こう側にいる可能性があり、また、企業のシステムにアクセスしている、またはアクセスしようとしている社外ユーザが何千人もいる可能性がある。有効なアクセスセキュリティコントロールにより、不適切なアクセスとシステムの不正使用に対して、合理的なレベルの保証を提供することが可能となる。アクセスセキュリティコントロールが適切に設計されれば、非倫理的なハッカーまたは悪意のあるソフトウェア、もしくはその他の侵入の試みを阻止することができる。

安全なパスワードやインターネットのファイアウォール、データの暗号化、暗号キーなどの適切なアクセスコントロール活動は、不正アクセスを防ぐ効果的な方法と言える。ユーザアカウントや関連するアクセス特権の統制は、アプリケーションやアプリケーション機能へのアクセスを業務上必要な承認されたユーザにのみ制限し、適切な職務分離を促す。アクセスを制限または許可しているユーザプロファイルは、頻繁かつ適時にレビューする必要がある。前任者や不満のある従業員は、システムに対する脅威となり得る。従って、退職した従業員のパスワードやユーザIDは直ちに無効にしなければならない。企業は、システムの不正使用と変更を防ぐことにより、そのデータとプログラムのインテグリティを保護することができる。

プログラム開発とプログラム変更

アプリケーションソフトウェアの開発と保守管理は、2つの主要な構成要素から成る。一つは新しいアプリケーションの調達と導入であり、もう一つは既存のアプリケーションの保守である。

新しいアプリケーションの調達および導入プロセスは、失敗に終わる可能性の高い分野である。アプリケーションが業務の要件と期待を全く満たしていなかったり、あるいは時間内または予算内に導入されずに導入が完全な失敗とみなされたケースが多く見られる。

調達と導入のリスクを低減するために、システム開発と品質保証の手法を採用している企業もある。標準的なソフトウェアツールとITアーキテクチャの構成要素は、しばしばこの手法をサポートしている。この手法は、自動化された解決法の把握、システム設計と導入、文書化の要件、テスト、承認、プロジェクト管理と監視の要件、プロジェクトのリスク評価のための構造を提供している。

アプリケーションの保守管理は、日常的な変更管理と新しくリリースされたソフトウェアの導入に対応している。システムの変更に対する適切な統制は、すべての変更が適切に行われるよう存在していなければならない。また、新しくリリースされたシステムに必要なテスト範囲を決定する必要もある。例えば、新しくリリースされた主要なソフトウェアの導入には、システムの拡張、広範なテスト、ユーザの再研修、および手続きの変更に関する評価が必要な可能性がある。統制は、変更申請に必要な承認、変更の審査、他のITの構成要素と導入プロトコルの変更に関する承認、文書化、テスト、および評価を伴うことがある。変更管理プロセスにおいても、インシデント管理、問題管理、可用性管理およびインフラ変更統制を含む、他のITプロセスとも統合する必要がある。

企業改革法遵守のための変化に関する人的要素の管理

以前には存在していなかった企業改革法遵守のための統制の導入は、大半の企業にとって、重要な課題となっている。多くの場合、社内の財務部門は、長年財務監査に関与していたことから、統制と関連する文書化の必要性について熟知していた。しかし、IT 部門はこうした問題に慣れておらず、このため、長期的に有効に運用される統制を導入することは困難な作業だった。

IT 部門は、統制を効果的に導入し、維持するため、最初に、企業改革法の遵守には現在の実務慣行を変える必要があることを理解する必要がある。同様に、IT 部門は、変化は単なる過程ではなく、成功するために考慮しなければならない重要な文化的・個人的な潜在的要素があることを認識する必要がある。したがって、企業は企業文化の嗜好と従業員の能力を反映した変化のための戦略を持つ必要がある。変化はただ発生するのではなく、管理しなければならないものである。

変化に対するコミットメント

変化を管理するための最初のステップはコミットメント得ることである。このコミットメントを得るために、企業は変化したい内容と、変化が行われた後のビジョンを定義する必要がある。将来の状況に対するビジョンを構築することにより、コミットメントが可能となる。また、企業は変化がどのように社内に影響を与える可能性があるかを理解する必要がある。例えば、変化はトップダウンまたはボトムアップのアプローチを通じて適切に達成されるか、などの質問を検討することが挙げられる。こうした課題を理解することが、コミットメントを得るために重要である。

現在の状況に対する評価

成功につながる変化の管理は、現在の状況を正直に評価することから始まる。現在の状況は、企業が変化に対してどれだけ準備ができているかを意味する。現在の状況を評価する上で、以下の要素を検討されたい。

- 企業文化－　変化が成功につながるかどうかは、企業文化に影響される。つまり、企業が柔軟で企業家精神に富むスタイルに慣れている場合、変化はすでにその企業文化の一部であり、それを前提として捉えるだろう。企業文化がストイックで厳格な場合、変化はより難しいだろう。
- 変化の程度－　変化がより重要であればあるほど、成功の見込みは少なくなる。企業は達成しようとする変化の程度を評価し、現実的な目標を設定する必要がある。
- 従業員に与える影響－　すべての変化に対して、プラスに捉える者とマイナスに捉える者がおり、人々が変化によりどのような影響を受けるかを理解することが重要である。変化をプラスとして捉える者はしばしば変化の推進者（チェンジエージェント）となり、変化をマイナスと捉える者はしばしば変化の障害となる。このため、変化の推進役となる者を早期に把握し、プロセスにおいて彼らを関与させることが、重要な成功要因となる。同様に、障害の比率が高い場合は、企業はどのように変化を組織に導入することができるかを再考する必要がある。
- 基盤の強さ－　組織の変化への適応能力はしばしばスキルと経験に比例する。変化のために大幅な再研修あるいはスキルセットの改善を必要とする場合、成功のためには研修への投資が必要となる。

障害の克服

企業は、現状を評価する過程の一部として、変化に関連する障害を把握する。次に企業は、これらを克服するための戦略を実施する必要がある。例えば、企業が企業改革法の遵守を進めていく場合、統制の設計と実施が必要となり、これを「日常の仕事を片付ける」ための妨げとみなす者もいるかもしれない。だが、これらの統制が適切に設計され、伝達されていれば、これらの統制を業務プロセスの効率性と有効性を促進するために実施することができ、結果として業績の改善がもたらされる。

こうした障害を克服する際、このプロセスをすでに実施している企業から学ぶべき重要な教訓がある。それは以下のとおりである。

1. コミュニケーションー　効果的なコミュニケーションは、定期的な最新情報の報告を超える存在である。組織は本来、変化に抵抗するものであり、従業員は変化の目的とそのプラス面を理解する必要がある。これに関するいくつかの提案を以下に挙げる。
   - 痛みを伴う点を理解する。個人または組織全体にマイナスの影響を与える内容を把握し、変化がどのようにその痛みを軽減するかを明確に伝えることを確実にする。企業改革法には多くの痛みを伴う点があり、そのうち最も重要なのは、企業改革法の要件を満たせないことである。それが人々にどのような影響を及ぼすかを理解すれば、遵守に伴う変化を喜んで受け入れるようになるだろう。
   - コミュニケーションのための最良のメディアを決定する。ニュースレター、電子メール、ワークショップ、昼食会などはすべて、コミュニケーションを図るための良い例であり、ほとんどの場合、メッセージを行き渡らせるためには二つ以上の種類が必要となる。企業改革法のプロジェクトは長期に及び、内容も複雑である。このため、定期的なコミュニケーションを図ることが重要である。
   - フィードバックするー　コミュニケーションが重要であるのと同様、フィードバックの収集と分析も重要である。フィードバックにより、組織は報告に耳を傾けているという態度を示しながら、柔軟性と順応性を示すことが可能となる。変化が成功しない最も大きな理由の一つは、組織が耳を傾けないためである。企業改革法の要件を満たす方法は多くあるが、フィードバックが求められ、それが実施された際に生じる興奮を目にすれば、企業は驚きを隠せないだろう。
2. 研修ー　企業が発展を望むなら、企業はそこに到達するために必要なスキルを従業員に与えることが重要である。研修の要件は影響を受ける従業員ごとに把握する必要があり、この研修を実施するために計画の立案が必要となる。企業改革法の要件は複雑であり、適切な作業量に関するさまざまな意見が、プロジェクトの成功に研修と教育が不可欠であることを示している。例えば、本稿で述べた他の領域と同様に、IT 全般統制が業務処理統制とどのように関連しているかを理解する上で、研修は特に重要である。
3. 動機付けー　動機（インセンティブ）が与えられた場合、変化は最も成功する。動機は変化を起こすための生産性の高い、目的指向のアプローチを提供し、その結果、しばしば企業と従業員にとって相乗効果をもたらす。例えば、企業改革法遵守の目標を全従業員の業績評価プロセスに組み込み、各個人の役割と責任に関連するよう、こうした目標をできるだけ具体的に定義することを検討する。

基本原則の制定

COSOの定義

これまで、企業による統制に関するアサーションは、ほとんどが自主的なものであり、多様な内部統制のフレームワークに基づいていた。SECは、一貫性と品質を向上させるため、パブリックコメントの入手を目的としたフレームワークの広範な普及を含む公正な手続きに従って企業またはグループが確立した、認められた内部統制のフレームワークを用いることを義務付けた。特に、SECはCOSO[1]について言及している。

COSO（トレッドウェイ委員会支援組織委員会）は、企業倫理、有効な内部統制とコーポレートガバナンスを通じて財務報告の質の改善を図る自主的な民間組織である。COSOはしばしばトレッドウェイ委員会と呼ばれ、もともと、National Commission on Fraudulent Financial Reporting（不正な財務報告に関する国家委員会）を後援するために1985年に組織された。同組織は米国公認会計士協会(AICPA)、米国会計学会(AAA)、国際財務担当役員協会(FEI)、内部監査人協会(IIA)、管理会計士協会(IMA)で構成されている。以下の章では、COSOに対するさらに深い洞察とともにITに与える影響について述べている。

COSOのITへの適用

長年、ITは、戦略上・管理上の情報システムの運用において重要な役割を果たしてきた。今日では、これらのシステムは、顧客や業者、他の重要な利害関係者のニーズを満たす上で、組織の能力から切り離すことができない。財務上、業務上の管理システムはITに広く依拠しているため、特に重要な情報システムにとって、統制は長い間必要なものとみなされてきた。この点を強調するため、PCAOB監査基準第2号で規定された指針は以下のように述べている。

> *COSOレポートとして知られるこのレポートは、経営者の評価を目的とした適切で利用可能なフレームワークを提供している。こうした理由から、この基準における実績と報告の方向性はCOSOフレームワークに基づいている。他の適切なフレームワークは他の国々でも発表されており、今後も発展する可能性が大きい。こうした他の適切なフレームワークは、財務報告に係る内部統制監査で用いられる可能性がある。異なるフレームワークは、COSOと全く同じ要素を含んでいない可能性があるが、一般に、COSOのすべてのテーマを含む内容であるべきである。*

企業改革法の遵守作業にとって、ITの統制がどのようにCOSOのフレームワークをサポートしているかを示すことは重要である。企業はCOSOが有効な内部統制に必要不可欠とする5つのすべての構成要素においてITの統制能力を持つ必要がある。これらは以下のとおりである。

- 統制環境
- リスク評価
- 統制活動
- 情報と伝達
- モニタリング

[1] Committee of Sponsoring Organizations of the Treadway Commission Committee,（トレッドウェイ委員会支援組織委員会）*www.coso.org*

5つの各要素は、次のセクションで簡潔に説明する。次にこれらの各要素と関連する上位のIT統制について考慮する。企業改革法の遵守を考慮するため、より詳細なITのコントロール目標を巻末の参考資料に示してある。

統制環境

統制環境は、有効な内部統制の基礎を成すとともに、「経営者の気風」を確立し、企業統治の構造の頂点を表す。統制環境の構成要素として取り上げられる事項は、組織全体に当てはまる。この統制環境は、主に全社レベル（エンティティレベルまたは会社レベル）のものである。

しかし、ITは、しばしば、業務との整合性、役割と責任、方針と手続き、ならびに技術的能力を新たに強調する必要があるかもしれないという特徴がある。統制環境とITに関して考慮すべき点は、以下のとおりである。

- ITは、しばしば誤って業務の別組織とみなされて、したがって、別の統制環境と考えられている。
- ITは、技術的な要素だけではなく、これらの技術的要素がどのように企業の内部統制システム全体に組み入れられているかという点に関しても、複雑である。
- ITは、新たなリスクやリスクの増大をもたらしうるが、リスクを上手に低減するために、新たなまたは強化された統制活動が必要となる。
- ITには専門的なスキルが必要だが、このスキルは不足している。
- ITは、外部サービス業者（サードパーティ）への依存が必要となる可能性があるが、この場合、重要なプロセスまたはITの構成要素は外注されている。
- 特に業務処理統制については、IT統制の責任者が不明瞭になる可能性がある。

リスク評価

リスク評価では、あらかじめ設定した目的を達成するために、経営者による関連リスクの把握と分析を行う。このリスク評価は統制活動を決定する根拠となる。内部統制のリスクは、企業の他の領域におけるよりも、IT部門において、より広範囲に及ぶ可能性が大きい。リスク評価は全社レベル（組織全体）で、またはアクティビティレベル（特定のプロセスまたは事業単位）で行われる。

全社レベルでは、以下の活動が予想される。

- 企業全体の企業改革法運営委員会の中にIT統制小委員会を設置する。
  その責任には以下が挙げられる。
  - IT内部統制の戦略計画の開発の監視、有効でタイムリーな実施と導入、全体的な企業改革法遵守計画との統合。
  - ITリスクの評価。例えばIT管理やデータセキュリティ、プログラム変更と開発の評価。

アクティビティレベルでは、以下の活動が予想される。

- システム開発手法を通じて構築された正式なリスク評価。
- インフラストラクチャの運用と変更プロセスに組み込まれたリスク評価。
- プログラム変更プロセスに組み込まれたリスク評価。

統制活動

統制活動は、業務目標が達成され、リスク低減戦略が実行されるための方針、手続きおよび慣行である。統制活動は把握されたリスクを低減するため、個々の統制目的に特に取り組むために開発される。

公開企業は、信頼できる情報システムと有効なITの統制活動がなければ、正確な財務報告書を作成することができないだろう。COSOは、この関係を認識しており、情報システムの統制活動を大きく2つに分類している。その一つは全般統制であり、もう一つは業務処理統制（アプリケーション統制）である。

全般統制は、企業のアプリケーションシステムが作成した財務情報が信頼できるよう設計されており、以下が含まれる。

- データセンターのオペレーション統制 － ジョブのセットアップ、スケジューリング、オペレーターの行動、データのバックアップとリカバリーの手続きなどの統制。
- システムソフトウェア統制 － システムソフトウェア、データベース管理、通信ソフトウェア、セキュリティソフトウェア、ユーティリティの効果的な調達、導入、保守管理に関する統制。
- アクセスセキュリティ統制 － システム、オペレーティングシステム、データベースおよびアプリケーションのすべての段階において、システムの不適切で不正な使用を防ぐための統制。
- アプリケーションシステムの開発と保守に関する統制 － システム設計と導入（各フェーズの概要を示す）、文書化の要件、変更管理、プロジェクトの開発または保守を管理するための承認とチェックポイントを含む、開発手法に関する統制。

業務処理統制は未承認の取引を防止または発見するため、ソフトウェアプログラム内に組み込まれている。業務処理統制は適切に設定され、また他の統制と併用された場合、取引処理の網羅性、正確性、承認、実在性をサポートする。業務処理統制に関する追加的な指針は参考資料Dに示した。

業務処理統制の機能をサポートするためには全般統制が必要である。そして、正確な情報処理とその結果生じた組織の管理、統治、報告に用いられる情報のインテグリティをサポートするためには、この双方が必要である。自動化された業務処理統制がますますマニュアル統制に取って代わってきているため、全般統制はより重要になってきている。

情報と伝達

COSOは、事業を運営し、企業の統制目的を達成するために、情報はすべてのレベルで必要だとしている。しかし、IT部門にとって関連情報を把握、管理、伝達することは、増え続ける一方の課題である。統制目的を達成するためにどの情報が必要かを決定し、従業員が責務を果たすことのできる形式と時間の中でこうした情報を伝達することにより、COSOのフレームワークの残りの4つの構成要素がサポートされる。

IT部門は、財務報告情報の大半を処理している。しかし、通常、その範囲ははるかに広い。IT部門は、電子メールシステムや管理職の意思決定サポートシステムといった、重大な事象を把握し伝達するメカニズムの導入もサポートしている。

また、COSOは、情報の質には情報が次のような状況であるかどうかを確認することも含まれるとしている。

- 適切 － それは正しい情報か？
- 適時 － 必要な時に利用でき、適切な期間に報告されるか？
- 最新 － それは最新情報か？
- 正確 － データは正しいか？
- アクセス可能 － 必要に応じて承認された者がアクセスすることができるか？

全社レベルでは、以下の活動が予想される。

- 企業方針の策定と伝達。
- 報告義務の決定と伝達。これには締切、照合、月次・四半期・年次の管理報告書形式と内容が含まれる。
- 財務情報の連結と伝達。

アクティビティレベルでは、以下の活動が予想される。

- 企業方針の目的を達成するための基準の作成と伝達。
- 経営目標の達成をサポートする情報の把握とタイムリーな伝達。
- セキュリティ違反の把握とタイムリーな報告。

モニタリング

モニタリングは、継続的なあるいは一定時点での評価のプロセスを通じた経営者による内部統制の監督を対象とするもので、IT管理にとってますます重要になってきている。モニタリングには、日常的なモニタリングと独立的評価という二つの種類がある。

ITのパフォーマンスと有効性は、統制が有効に運用されているかどうかを示すパフォーマンス指標を用いて継続的にモニターされるようになっている。以下の例を考慮する。

- 問題の把握と管理　－　測定指標を確立し、測定指標に対する実際の傾向を分析することが、処理上の問題点の根本的な原因を理解するための根拠となる。これらの根本原因を修正することによって、システムの正確性と処理の完全性、システムの可用性が向上する。
- セキュリティのモニタリング　－　有効なITセキュリティのインフラを構築することにより、不正アクセスのリスクを低減できる。セキュリティの向上により不正取引の処理や不正確な報告書の作成リスクを低減することができ、アプリケーションとITインフラの構成要素をうまく融合させた場合、関連システムの非可用性を確実に低減できる。

全社レベルでは、以下の活動が期待される。

- コンピュータ・オペレーションの集中化された継続的な監視活動
- セキュリティの集中監視活動
- ITの内部監査レビュー（監査はアクティビティレベルで行われるが、監査結果は全社レベルで監査委員会に報告される。）。

アクティビティレベルでは、以下が期待される。

- 問題の把握と管理
- コンピュータ・オペレーションまたはセキュリティの拠点におけるモニタリング
- 拠点のIT要員の監督

IT コンプライアンスのためのロードマップ

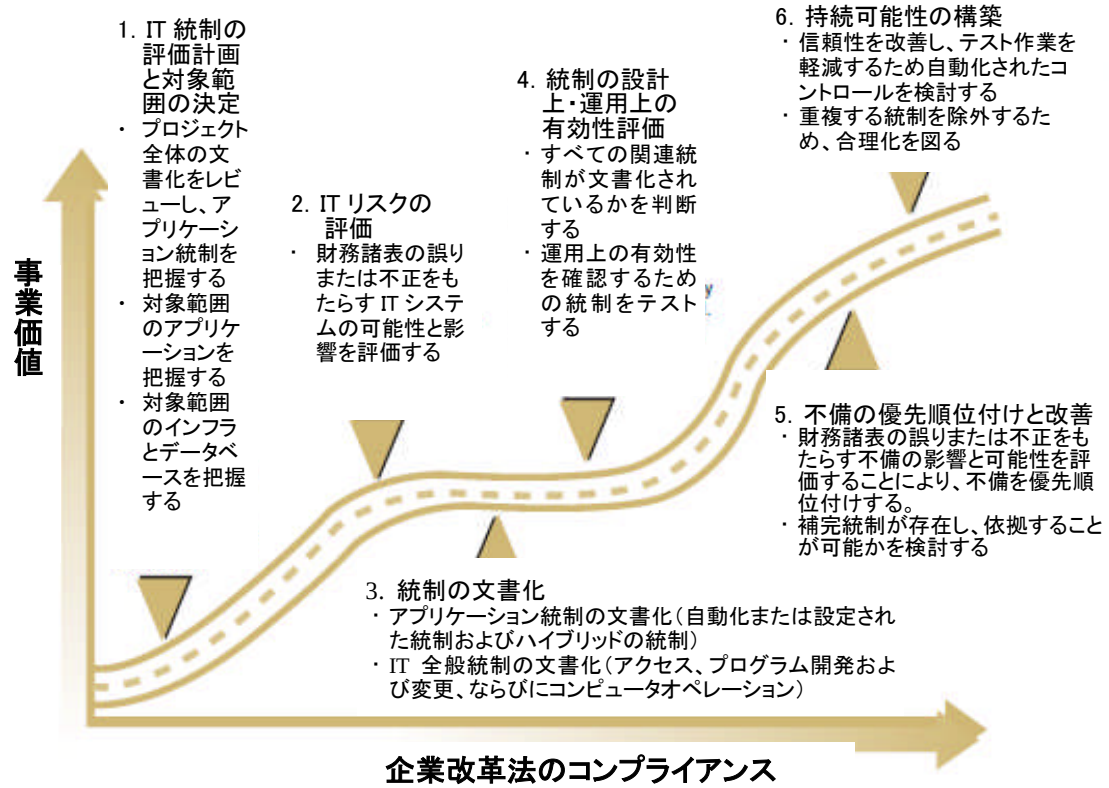
この章では、IT部門の特定の目的と責任に合わせた企業改革法の遵守のためのロードマップについて述べる。このロードマップは企業改革法の遵守にとって最も重要な活動に関する作業に焦点を当てるとともに、これらの導入プロセスの管理を容易にするために、初版の図表をさらに単純化したものである。

事業の特質に基づいて企業改革法をどのように組織に当てはめるかを理解することは、内部統制プログラムを開発する上で手助けとなる。ここでは多くの要因が作用しており、大企業は小企業とは違った難局に直面すると考えられる。また、強力な内部統制のフレームワークが既に機能している場合、活動に大きな影響を及ぼす。

企業改革法の遵守

図表3に示した「ITコンプライアンスのためのロードマップ」は、企業改革法の要件を満たす上で、IT専門家に方向性を示すものである。ロードマップの最初の2ステップ、IT統制の評価計画と対象範囲の決定、及びITリスクの評価は、並行して実施しなければならない。

図表 3　IT コンプライアンスのためのロードマップ



1. IT統制の評価計画と対象範囲の決定

すべての重要なプロジェクトと同様に、遵守プログラムにおけるITの対象範囲を適切に決定し、作成するためには、注意が必要である。財務/業務チームと協同作業し、彼らの発見事項を用いながら、どのITアプリケーションと関連するサブシステムがプロジェクトに含まれるべきか、そしてどのアプリケーションとサブシステムが除外できるかという対象範囲の決定を、理解するプロセスである。システムを含めるか除外するかは企業の全体的な財務リスクの評価プロセスに基づくものであり、これは財務/業務上の遵守チームが主体となって実施する。換言すれば、財務報告に係る業務および関連統制をサポートするサブシステムだけが対象範囲に含まれれなければならない。これとは反対に、計画立案は、人員に課題を割り当てられ、進捗状況をモニターされる活動スケジュールを作成するプロセスである。

説明責任と責任の割当て

IT統制の遵守プログラムにおける最初の重要なステップは、IT統制小委員会を組織することである。IT統制小委員会は企業改革法の運営委員会の一部であり、運営委員会に対して報告を行う。IT統制小委員会は、IT統制の企業改革法への遵守プロセスを監督し、企業改革法プロジェクト全体への伝達と統合を取り持ち、ITプロセスにおける独立監査人との間を取り持つ。小企業においては、既存スタッフを時間ベースで再配置することが可能である。しかし、大企業では、仕事熱心なフルタイムの人員が必要かもしれない。IT統制小委員会は、プロジェクトに責任を持ち、プロジェクトを終了させるための適切な権限と説明責任を与えられている人員をIT統制のリーダーに任命する必要がある。

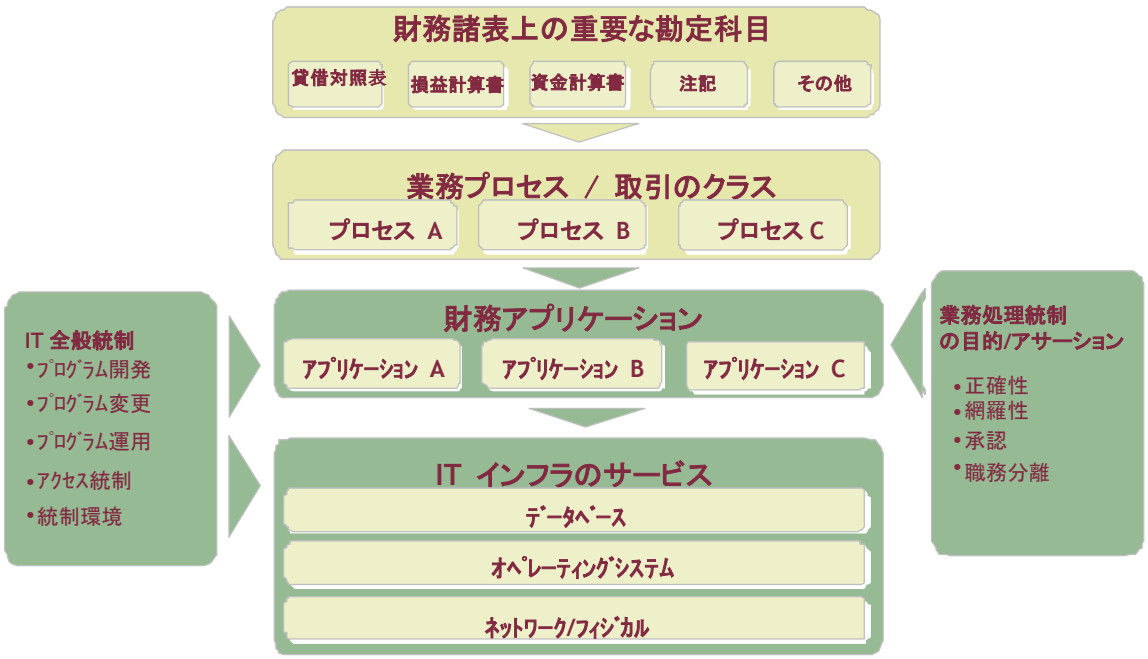
関連アプリケーションと関連サブシステムの棚卸

財務部/業務チームと共同作業を実施し、**図表4**のように、関連する業務処理統制をサポートするアプリケーションを把握することによって、対象範囲に含まれたアプリケーション（企業改革法のアプリケーション及び関連するサブシステム）のリストを作成しなければならない。一般に、オンライン上の承認、複雑な計算または価値評価をサポートするアプリケーション、もしくは棚卸資産、固定資産または借入残高などの重要な勘定科目の残高の誠実性を維持するアプリケーションは、この段階で把握しなければならない。参考資料Dの「業務処理統制（アプリケーション統制）」は、財務/業務チームと協同作業する際に、業務処理統制の定義と社内における所在場所に関する指針を述べたものである。

アプリケーションを管理し運用する IT プロセスと同様に、IT 統制プロジェクトチームは、アプリケーションを棚卸することによって、考慮する必要のあるすべてのアプリケーションを把握し、データベース、サーバ、オペレーティングシステム、およびネットワークを含む、アプリケーションをサポートするすべてのサブシステムを把握することができる（関連アプリケーションとサブシステムのリストの実例は、参考資料 E「アプリケーションとテクノロジ層のリストのサンプル」を参照のこと）。

プロジェクトにおけるこうしたステップの実施によって、IT 部門は財務報告プロセスがどのように機能しているかを理解し、プロセスのサポートにおいて IT が極めて重要な箇所を把握できるようになるだろう。

図表 4—IT 統制プロジェクトの対象範囲の決定 ― トップダウン型のアプローチ



アプリケーションと関連するサブシステムの棚卸は、予備計画案の策定の際に用いられなければならない。統制と必要なテストの特徴と範囲を決定するため、以下のフェーズにおけるリスクを評価する必要がある。

財務報告に関連するプロセスの文書化のレビューと業務処理統制の把握

企業には多くの業務プロセスと統制があるが、企業改革法の遵守は財務報告をサポートする業務プロセスと統制に限定される。したがって、IT 統制チームにとっては業務処理統制を的確に把握することが重要である。これを実施するためには二つの共通するアプローチがある。企業は業務処理統制を把握する上で、IT 統制チームに財務/業務チームをサポートさせる、または、まずすべての統制を財務/業務チームに把握させ、次に IT 統制チームがこれらの統制をレビューし、このうちのどれが IT に依拠しているかを把握する、のいずれかを実施することが可能である。企業がどの統制が IT に依拠しているかを適切に把握する限り、どのアプローチを用いるかは重要ではない。その際、企業は財務報告の目的をサポートする業務処理統制の対象範囲を限定しながら、IT 統制のプロジェクトを適切に立案することが可能となる。

予備計画案の策定と承認

対象範囲に含まれるアプリケーションとサブシステムのリストを用いて、**図表 3** のロードマップで説明した 6 つのフェーズを用いてプロジェクト活動の予備計画案を作成する。計画案は、後に修正し、精緻化するが、現時点ではプロジェクトの規模とアプローチの全体像を得ることが重要である。計画を策定する際、参考資料 F のプロジェクト見積りツールを用いて、各フェーズに必要な作業時間を見積もることができる。

プランを作成した後、対象範囲に含まれるアプリケーションとプロジェクトの範囲の適切さについて財務/業務チームと話し合うことが大切である。これが完成した時点で、プロジェクト進行の承認を得る。プロジェクトの重要性とプロジェクトが組織のさまざまなメンバーに及ぼす影響から、正式な承認を得ることは、極めて重要である。正式な承認を得ることにより、プロジェクトのスポンサーが確定し、プロジェクトに参加する必要のあるすべての関連当事者とスタッフから賛同を得られる。

業務処理統制の責任判断

IT 統制プロジェクトの混乱を招いている共通の領域の一つに、「誰が業務処理統制の責任者か」という問題がある。この責任が不明確なことが、作業の大幅な重複、不必要な重複する関連統制のテスト、そして財務チームと IT チームの双方が、もう一方のチームがその問題に対応していると思っているため関連統制がテストされていない事態につながっている。業務プロセス責任者は業務プロセスに特有な業務処理統制の責任を持つとよい。IT 部門の責任は、全般的な業務処理統制（アクセス制限、変更統制、バックアップの復旧など）が機能しており、信頼できるかを確認しながら、これらの統制を把握しテストする上で、業務プロセス責任者をサポートすることにある。

複数拠点の問題についての考慮事項

IT 統制プロジェクトの対象範囲を決定する上で検討しなければならない要素の一つに、業務が分散した企業、または地理的に分散した業務を持った企業がある。これらの企業は、各地理的な拠点における IT オペレーションが単一の統制環境内で、あるいは複数の統制環境内で運用されているかどうかを判断する必要がある。単一の統制環境では、通常一つのリーダーシップの構造であるが、複数の統制環境では、複数のリーダーシップ構造がある。一般的に、複数の統制環境は、重要な場合、別々に取り扱う必要があり、このためプロジェクトはより大きくなり、作業数も増加する。

対象範囲からアプリケーションを除くことができるかをの考慮

あるアプリケーションが対象範囲に含まれているという事実は、アプリケーションが企業改革法の遵守に必要な、関連アプリケーションまたは複合型の統制をサポートしていることを示している。多くの場合、アプリケーションとその関連するサブシステムが評価されなければならない。しかし、このアプリケーションが非常に限られた数（例えば、業務処理統制が一つだけ）しかサポートしていない場合、この業務処理統制を除外して（つまりそのアプリケーション自体）、全体の作業量を減らすために関連するマニュアル統制を把握する、または既存のマニュアル統制への依拠を高めることのいずれかを検討することが可能になる。これは稀ではあるが、きわめて少数の統制をサポートするアプリケーションを多く有している企業にとって、考慮すべき事項といえる。この状況では、不適切な依拠（システムが作成した報告書に依拠するなど）が起きないよう、注意しなければならない。これは企業全体の企業改革法運営委員会が注目すべき問題である。これは IT に依拠する問題ではない。

外部サービス業者（サードパーティ）（外部委託）への依拠の把握

ある企業では、外部委託したサービスを実施するため外部サービス業者を用いている。これらのサービスは依然として、企業全体の業務と責任の一部であり、このため、IT の内部統制プログラム全体で考慮する必要がある。

PCAOB 監査基準第 2 号は、特にサービスを実施する業者の監査人の報告書について、次のように明確に述べている。

サービス業者の利用によって、財務報告に係る有効な内部統制を維持する経営者の責任が軽減されることにはならない。むしろ、経営者は財務報告に係る内部統制を評価する際、企業における関連統制同様、サービス企業における統制を評価すべきである。

このような状況においては、企業はその内部統制の信頼性について結論に達する上で、サービス業者の活動を見直す必要がある。会計監査人（外部監査人）の監査報告書には、サービス業者の統制活動に関する文書化が必要とされる。したがって、これらの統制の裏付けとなる証拠が十分で、適切であることを判断するため、サービス業者の IT プロセスに関する評価が必要となる。

従来、外部サービス業者（サードパーティ）の内部統制に係る監査意見は SAS70 報告書として知られ、外部サービス業者（サードパーティ）のために実施されてきた。しかし、これらの監査報告書が統制のテスト、テストの結果、統制の運用の有効性に関するサービス業者の監査人の意見を含んでいない場合、それらは企業改革法の遵守目的上、十分とはみなされない。このような場合、企業は会計監査人と相談し、特定の要件の理解を図ろうとするかもしれない。企業は SAS70 報告書がカバーする時期を特に注意する必要がある。また、SAS70 報告書における統制が、テスト結果と監査意見全体同様、企業の用いる環境、プラットフォーム、アプリケーションをカバーしているかどうか、特に注意する必要がある。参考資料 L「SAS70 調査 報告書を用いる際の課題」では、SASA70 報告書の十分性の評価に関するより詳細な議論を取り上げている。

2. IT リスクの評価

この段階では、企業は対象範囲のアプリケーションをサポートする IT プロセス及びレイヤ（層）に内在するリスクを評価する必要がある。企業改革法遵守プロジェクトの導入の最初の数年間を通じて学んだ最も重要な教訓の一つは、プロジェクトはリスクベースでなければならないということである。すべての IT システムまたはプロセスが、財務諸表にとって高リスクというわけではない。したがって、すべての IT システムまたはプロセスが、同じ程度含まれる、または評価される必要があるというわけではない。リスク評価を実施する上で、残存リスク（統制の影響を考慮した後で残るリスク）よりも、むしろ「固有リスク」を考慮する必要がある。リスク評価プロセスをサポートするために、参考資料 F「プロジェクト見積りツール」では多くのツールを提供している。

アプリケーションおよび関連するサブシステムの固有リスクの評価

データベース、オペレーティングシステム、ネットワークおよび物理的環境など、アプリケーションと関連するサブシステムの固有リスクの評価は、こうしたリスク管理に必要な統制の性質と範囲を決定する上で必要である。さらに、これらの統制の運用上の有効性のテストの適切な立案と実施のため、アプリケーションと関連するサブシステムの固有のリスクを理解することも必要になる。

固有リスクの評価を実施する際には、多くのリスク要因を考慮する必要がある。しかし、最終的な評価は、判断に基づく。共通のリスク要因を考慮する目的は、公正で正当なリスク評価を実施できるよう、関連する情報を企業に提供することにある。リスク評価を実施する際、リスク事象の発生可能性と影響の両方を考慮する必要がある。例えば、アクセス統制が存在しない場合には、何者かが主要な財務アプリケーションにアクセスし、システムに虚偽の取引を入力できるリスクがある。統制がない場合であっても、こうした事件の発生の可能性が全くないわけではなく、虚偽の取引の入力が及ぼす影響は大きい。その結果、こうしたリスクは重大だと考えられ、リスクを低減するため統制が必要となる。この目的はリスクを完全に除去することではなく、リスクを妥当な水準まで低減する点にあると注目することが重要である。

以下の要因はリスク評価を実施する際に通常用いられているものだが、企業は特別な状況において他の事項も追加する必要があるかどうかを判断しなければならない（追加的な指針は参考資料 G「固有リスクの評価と統制の優先順位付け表」を参照のこと）。
· IT の特性（複雑か単純か）
· 担当者の特性（経験豊富か経験不足か）
· プロセスの特性（中央に集中しているか、分散しているか）
· 過去の経験
· 財務報告に対する重要性

一度リスク評価が実施されると、その結果は、必要な統制とテストの特徴と範囲を判断する上で役に立つことができる。参考資料 C、「IT 全般統制」はアプリケーションと関連するサブシステム（まとめて「テクノロジ層」と呼ばれる）に関して、考慮すべき、望ましい IT 統制の指針を提供している。参考資料 G で示したマトリクスでも示したように、リスク評価により、単にそのテクノロジ層に関する事象の確率または影響が作業を保証するのに十分ではないという理由によって、リスク評価は、特定の IT 統制プロセスを除外することができる。結果に関係なく、下した決定とその論理的根拠の文書は、経営者または外部監査人との話し合いのために保存する必要がある。

プロジェクト計画の対象範囲の精緻化と更新

リスク評価実施後、IT 統制チームは、プロジェクトの対象範囲を精緻化し、どのアプリケーションと関連するサブシステムを対象範囲から除外できるかについて最新情報を伝えることができる立場にいるはずである。リスク評価プロセスと関連する結論は、特にシステムが対象範囲から除外される箇所を明確に文書化する必要がある。同様に、計画案は対象範囲の変更箇所および作業範囲がリスクベースのアプローチを反映するように更新する必要がある。

3. 統制の文書化

統制の文書化は、経営者に対し、信頼できる財務諸表に関するリスクがどのように対処されているかを説明する。経営者はこれによって、リスクの残されたレベルを受容できるかに関し、情報に基づいた決定を行うことができる。例えば、財務アプリケーションが複雑な計算に大きく依拠している場合、未承認の変更は財務諸表の重要な誤りにつながるリスクを内包する。このため、重要な誤りの発生を防ぐ、または重要な誤りを発見する統制を把握し、文書化することが極めて重要である。

全社レベル IT 統制の把握

全社レベル統制は、組織の運営スタイルが反映する。これには組織の気風を決定する方針、手続きおよび他のハイレベルな慣行が含まれる。全社レベルの統制は、COSO モデルの基礎となる構成要素であり、財務報告をサポートする IT 運用を考慮に入れる必要がある。全社レベル IT 統制の把握は、企業が実施する全社レベルの評価全体に組み込まれなければならない。十分に定義され、伝達された方針と手続きなどの堅固な全社レベル IT 統制の存在は、より信頼できる IT 運用環境が背後にあることをしばしば示している。同様に、脆弱な全社レベル IT 統制を擁する組織は、変更管理やアクセスコントロールなどの統制活動を一貫して実施することが困難である可能性が大きい。その結果、全社レベル統制の相対的な長所または短所がテスト活動の性質、範囲、タイミングに影響を及ぼすことになる。

業務処理統制の把握

財務諸表の作成をサポートする業務処理統制の把握は、このプロセスで極めて重要なステップである。すべての業務処理統制が把握された後、業務処理統制がサポートする IT 全般統制の把握も可能となる。ほとんどの場合、業務処理統制は、業務プロセスの文書化に含まれている。理想的には、IT 専門家が統制の専門家と共にプロセスを文書化し、プロセスの関連統制を共に把握するのが望ましい。しかし、多くの場合、プロセスの文書化は既に行われており、このため、誰かがこの文書をレビューし、業務処理統制を把握しなければならない。参考資料 D「業務処理統制（アプリケーション統制）」では、業務処理統制の把握に関する追加的な指針を述べている。

自動化された統制の把握は、取るに足らないことのようにみえるかもしれないが、多くの場合、そうではない。企業は、一般的に 2 種類の業務処理統制を用いており、これらは文書化される必要がある。

- 自動化された統制 － 本質的にコンピュータと 2 進法により実施され、設計通りに機能し、断続的なエラーの影響を受けにくい。例えば、受注数を検証する入力の際のエディット・チェック、およびあらかじめ設定された上限までの受注しか許可しない自動化購入システムにおける構成による統制などがある。
- IT 依存マニュアル統制（複合型） － 本質的には IT システムに依存するマニュアル統制である。

エラー発見のタイミングと、統制の費用対効果が注目されるようになるにしたがって、IT 業務処理統制がより重要になってきている。例えば、数年前であれば手作業による調整が誤りや不正を発見するのに数週間を要しても、それを待つことができたかもしれない。しかし、今日ではこのような遅れはますます容認できなくなっている。したがって、自動化されたプロセスがサポートしないマニュアル統制は、もはや許容できない可能性がある。業務処理統制の実施例を含む、追加的な指針を参考資料 D「業務処理統制（アプリケーション統制）」で示した。

特に、複合型の統制は、PCAOB が 2004 年 11 月の指針でも強調したにもかかわらず、多くの企業で十分に文書化されていない。

> *業務処理統制も、IT に依存するマニュアル統制の可能性がある（例外事項報告書が IT で作成される場合、その例外事項報告書の在庫管理責任者によるレビューなど）。IT 全般統制の不備は、直接財務諸表の虚偽記載をもたらすわけではないが、関連する有効でない業務処理統制は、虚偽記載につながる可能性がある。したがって、IT 全般統制の不備の重要性は、業務処理統制に及ぼす影響と関連して評価される必要がある。すなわち、関連する業務処理統制が有効であるかどうかが問われることになる。*

IT 全般統制の把握

業務処理統制と IT 全般統制との関係は、業務処理統制の信頼性をサポートするために IT 全般統制が必要とされている、というものである。例えば、データベースのセキュリティの確保は、信頼できる財務諸表の作成の要件であると考えられている。データベースレベルでのセキュリティがなければ、企業は、財務データへの未承認の変更のリスクにさらされることになる。

IT 全般統制の課題は、財務諸表にほとんど直接的な影響を及ぼさないことである。しかし、PCAOB は、IT 全般統制をすべての内部統制について「大きな」影響を及ぼしているものとして記述している。すなわち、関連する IT 全般統制（例えば、プログラムとデータへのアクセスを制限する統制）が失敗すると、財務アプリケーションを含む、これに依存するすべてのシステムに大きな影響力を及ぼす。そ

の結果、承認されたユーザのみが財務アプリケーションへのアクセスを許されていることを確実にできなければ、企業は、承認されたユーザのみが取引を開始し、承認していると結論付けることができない。

どの統制が関連統制かを把握する

財務上のリスクは、発生可能性と影響の大きさにおいて財務上のリスクはすべて等しいわけではない。同様に、財務上の統制も、把握されたリスクを低減する際の有効性において同じではない。さらに、経営者は、リスクに関連するすべての統制活動の評価を求められているわけではない。このため、企業は統制の文書化を関連統制に限る努力をする必要がある。

大半の企業が尋ねる質問は、「関連統制とは何か」である。残念なことに、用語が普遍的に用いられているにもかかわらず、関連統制に関して、正式な定義は存在しない。理解しにくいかもしれないが、関連統制は、企業が統制目標を達成するために依拠することを選択した統制であり、統制責任者に対し、財務上の統制目標が達成されたことについて最大限の保証を与える統制である。

統制が関連統制であるかどうかを判断する際、企業は、以下を検討する必要がある。

- 関連統制は、一般的に重要なリスクを低減し、関連する統制の目標を達成するため、経営者にとって必要不可欠な方針、手続き、慣行、組織構造を含む。
- 関連統制は、しばしば二つ以上の統制目標をサポートする。例えば、アクセス統制は金融取引の存在、財務上の勘定科目の評価、職務分離などをサポートする。多くの場合、関連統制の組み合わせは、特定の目標または連続した目標を達成する効果的な方法である。単独の統制に信頼を置き過ぎるのは遵守プログラムに失敗をもたらす可能性がある。
- 重要なリスクに直接対応する（目標を直接達成する）統制は、多くの場合関連統制である。例えば、不正アクセスのリスクは、大半の企業にとって重要なリスクである。したがって、不正アクセスを防止または発見するセキュリティ統制は関連統制である。
- 予防的統制は、発見的統制よりも、一般的に、より効果的である。例えば、不正の発生の防止は、不正が実際に起きた後に単にそれを発見するよりもはるかに好ましい。したがって、不正の予防的統制はしばしば関連統制と考えられる。
- 自動化された統制は、マニュアル統制よりも信頼できる。例えば、ユーザによる定期的なパスワード変更を強制する自動化された統制は、強制力のない一般的な方針よりも信頼できる。また、手作業によるプロセスは、人為的なエラーを免れない。

参考資料 C「IT 全般統制」に、企業改革法の遵守を目的とする IT 部門が作成すべきガイドとして、IT 全般統制のリストを示した。このリストでは、「もっとも関連する」統制とされる重要な統制は、信頼される堅固な IT 全般統制の環境を設計する上で、最も一般的に用いられている統制であることを示している。

IT ベースの不正防止統制の検討

企業改革法に基づく不正防止統制の重要性は、決して軽視することができない。不正はそもそも企業改革法を導入した主な理由であり、この問題に十分かつ適切な注意を払う必要がある。

多くの不正防止統制が IT システムに依拠しているため、IT は不正の防止と発見において重要な役割を果たしている。企業の企業改革法の遵守プログラムを目的として、以下の IT ベースの不正防止統制の実例を含めることを検討する必要がある。

- アプリケーションにより実施される職務分離 － 大半のシステムには、アプリケーション内でユーザに割り当てられる特権の内容を定義する能力がある。その結果、システムが取引処理の適切な承認を行い、ユーザが自身の取引を開始し、承認することを防止している。

- アクセス統制 － 大半のシステムには、給与データなど機密情報にアクセスできる特権を与えられたユーザが存在する。こうした特権を与えられたユーザは、架空の従業員を追加し、不正を行うことが可能である。こうしたアクセスを数人の従業員に限定し、財務報告担当者にこうしたアクセス権がないことを確実にすることは、財務報告に係る内部統制を確立する上で重要である。

統制の文書化
企業改革法の下では、企業は、財務報告に係る統制の文書化、ならびに統制の設計と運用の有効性の評価が求められる。文書化は、企業の方針マニュアル、IT 方針と手続き、説明文、フローチャート、意思決定表、手続きに関する詳細な記述、または完成した質問書など、さまざまな形式をとる可能性がある。企業改革法ではどのような特定の文書化の書式も義務付けられておらず、文書化の範囲は、企業の規模と複雑さにより異なる可能性がある。

大半の企業については、IT 統制の文書化は以下を含まなければならない。
- 全社レベル
  - 経営者の対応と意見を裏付ける証拠を含む、全社レベル統制の評価
- アクティビティレベル
  - プロセスと関連するサブプロセスの記述（説明文形式の可能性があるが、フローチャートとして例示するほうがより効果的かもしれない）
  - リスクが及ぼす影響と発生可能性の分析を含む、プロセスまたはサブプロセスに関連するリスクの記述。プロセスまたはサブプロセスの規模及び複雑さ、ならびに企業の財務報告プロセスに及ぼす影響を検討する必要がある。
  - プロセスまたはサブプロセスのリスクを容認できるレベルにまで低減することを目的とした、統制目標の内容および COSO フレームワークとの連携の記述。
  - プロセスまたはサブプロセスに関連する統制目標を達成するために設計され、実施された統制活動の記述。これには、統制の種類（予防的または発見的）および実施される頻度を含む。
  - 統制活動の存在と運用上の有効性を確認する（テストする）ために取ったアプローチの記述
  - テストの結果、統制の有効性に関して達した結論

4. 統制の設計上・運用上の有効性評価

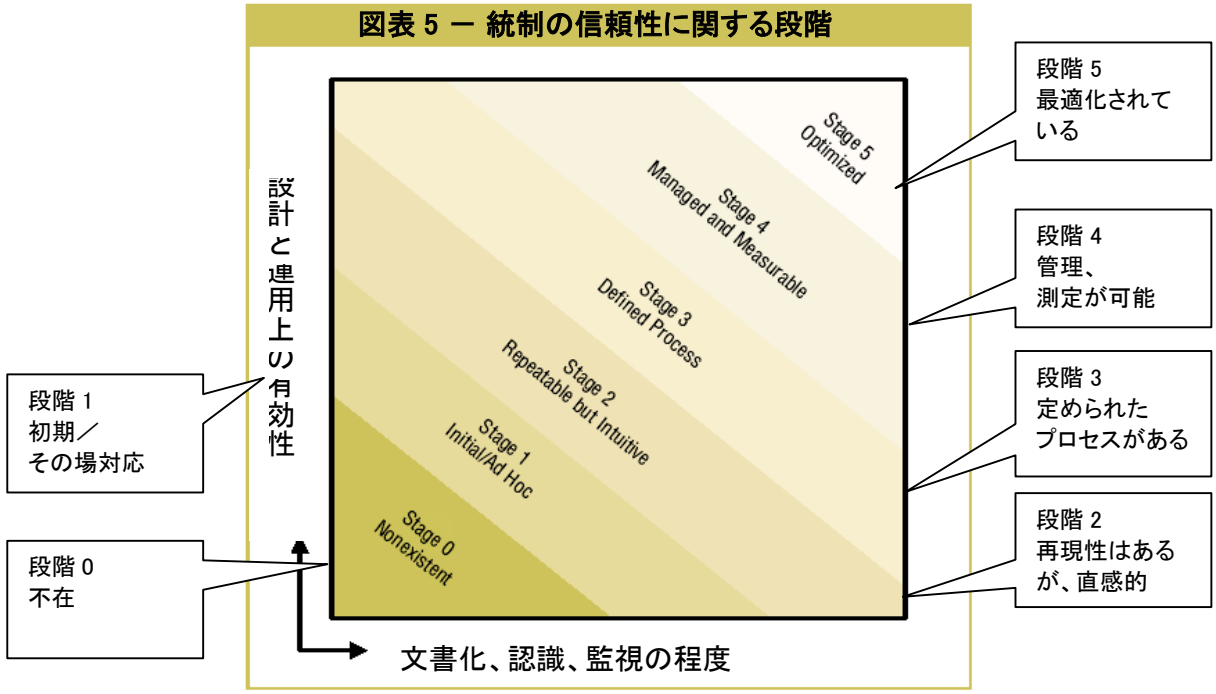
統制の設計上の評価
統制の設計は、IT 部門が一歩下がって、IT リスクを容認できるレベルにまで低減する統制プログラムの能力を評価することを引き起こす。具体的には、経営者は統制の設計について結論を下す際に、予防的統制、発見的統制、自動化された統制およびマニュアル統制を含む統制の属性に関する適切性の評価を経営者に強いる。例えば、変更管理のリスクが把握されており、これが不正なプログラムの本番環境への移行をもたらす場合、適切に設計された統制により、この発生を防ぐことができる。この例では、事件発生後に不正なプログラムを本番環境で発見する発見的統制は適切ではない可能性がある。

全体の IT 統制環境における統制の設計は、決して軽視することができない。PCAOB 監査基準第 2 号は IT 統制の重要性を指摘しており、全体の内部統制環境をサポートするために IT 統制が必要であるという事実を強調している。特に、企業全体の内部統制のシステムの有効性は、他の統制（統制環境または IT 全般統制など）の有効性に依拠していると述べている。このため、統制の設計評価は、IT 統制環境を評価する上で不可欠のステップと言える。

このプロセスをサポートするため、**図表 5** の IT 統制の設計と有効性のモデルを検討されたい。組織がどのように基準を満たしているかによって、統制プログラムの設計と有効性を高めるためには、少なからざる時間を費やすことが必要になるかもしれない。

図表 5 は、組織に存在する統制の信頼性の段階を示したものである。内部統制を確立するという目的から、段階が高ければ高いほど、より信頼できる統制環境になり、段階が下がれば下がるほど、信頼性が小さくなることに注意することが重要である。企業改革法では統制を文書化し、テストする要件以外に特定の段階が求められているわけでないが、組織は現在どの段階（成熟度）に位置し、それが遵守にとってのどの程度のリスクを示しているかを慎重に検討する必要がある。

図表 5 ― 統制の信頼性に関する段階



図表 6 は、統制の信頼性に関する各段階および関連する影響の特徴を理解する手がかりとなる。IT 部門は、企業改革法の遵守に必要な属性や特徴に関する定義や指針が、他にはほとんどないことを知っておく必要がある。文書化に際して特定の書式は認められておらず、または必要でなく、文書化の範囲は、企業の規模や複雑さにより異なる可能性があるという見解を SEC が示しているにすぎない。

前述のように、統制の設計の適切性に関する経営者のアサーションの根拠を提供するため、経営者は統制の設計の評価を文書化する必要がある。経営者の統制の設計の評価の文書化は、外部監査人が設計をレビューし、ウォークスルーを実施し、統制の有効性をテストするのに十分であるよう詳細に記述する必要がある。会計監査人は、統制の設計のテストを再実施するため、十分な記述に基づいて経営者による統制の設計の評価を理解しなければならない。通常、設計の評価プロセスとの調整を行わずに方針やマニュアルを提示するだけでは十分ではない。

図表 6－ 統制の品質

	段階 0 存在しない	段階 1 初期段階/ その場対応	段階2 再現性はあるが、 直感的	段階3 定められたプロセスがある	段階4 管理、測定されている	段階5 最適化されている
特徴	このレベルでは、認識可能な統制プロセスが完全に欠如している、あるいは関連する手続きが全く存在していない。組織は、対応すべき問題があることすらも認識していない。したがって、問題に関するどのような情報の伝達も行われていない。	統制および関連する手続きが重要で、対応する必要があることを組織は認識している証拠がある。しかし、統制と関連する方針、および手続きは実施されておらず、文書化されていない。 事象および開示のプロセスが存在していない。従業員は統制活動の責任に気付いていない。 統制活動の運用上の有効性は定期的に評価されていない。統制の不備は把握されていない。	統制、関連する方針および手続きが実施されているが、常に完全に文書化されているわけではない。 事象と開示のプロセスが実施されているが、文書化されていない。 従業員は統制活動の責任に気付いていない可能性がある。 統制活動の運用上の有効性は、定期的に適切に評価されておらず、プロセスは文書化されていない。 統制の不備が把握されている可能性があるが、適時に改善されていない。	統制、関連する方針、手続きが実施されており、適切に文書化されている。 事象と開示のプロセスが実施されており、適切に文書化されている。 従業員は統制活動の責任に気付いている。 統制活動の運用上の有効性は定期的(例えば、四半期ごと)に評価される。しかし、そのプロセスは十分に文書化されていない。 統制の不備は適時把握され、改善策がとられる。	統制、関連する方針および手続きが実施されており、適切に文書化されている。従業員は統制活動の責任に気付いている。 事象および開示のプロセスが実施されており、適切に文書化され、モニターされている。しかし、関連する主要なプロセスや組織上の変更を反映するために、常に再評価されているわけではない。 統制活動の運用上の有効性は定期的に(例えば、毎週)評価され、そのプロセスは適切に文書化されている。 プロセス、統制目的、および活動を文書化するため、限定された、主に戦略的な情報技術が利用されている。	段階5は段階4のすべてを満たした状態をいう。 企業全体で統制およびリスク管理プログラムが存在するため、統制と手続きは、十分に文書化され、主要なプロセスまたは組織上の変更を反映するために継続的に再評価されている。 統制の設計と有効性を評価するために自己評価プロセスが用いられる。 プロセス、統制目的、アクティビティを文書化し、ギャップを把握し、統制の有効性を評価するために、情報技術が最大限に利用されている。
影響	この組織は、最低水準ですらも遵守が全くできていない。	経営者のアサーションを裏付けるため、不十分な統制、方針、手続き、および文書化が存在している。統制の文書化、テスト、改善の作業は非常に重要である。	統制、方針、および手続きが実施されているが、経営者の認証（宣誓）とアサーション（適切な財務情報を作成するための要件）を裏付けるためには、文書化は不十分である。 統制の文書化、テスト、改善の作業は重要である。	経営者の認証とアサーションを裏付けるため、十分な文書化が存在する。 組織の状況により、統制の文書化、テストおよび改善の作業が重要となる可能性がある。	経営者の認証とアサーションを裏付けるため、十分な文書化が存在する。 組織の状況により、統制の文書化、テストおよび改善の作業はそれほど重要ではないかもしれない。	段階4の影響が残っている。 高品質で、タイムリーな情報により、改善された意思決定が可能となる。 社内のリソースが効果的、効率的に用いられている。 情報がタイムリーで信頼できる。

統制の運用上の有効性評価

統制の設計が必要に応じて評価されたならば、その設計と有効性がテストされる必要がある。この段階では、統制活動の設計及び運用上の有効性をテストするため、その統制の実施責任者である個人と内部統制プログラムのプロジェクトマネジメントチームが、初期および継続的なテストを実施しなければならない。

サンプルサイズの選択を検討するには、多くの要因（例えば、他の統制のテストや予想エラー率など）があるが、**図表 7** は、統制の運用上の有効性の評価をテストするために企業および監査人が用いる、共通（最低）サンプルの選択手法を示したものである。IT 全般統制については、選択されたサンプルサイズは、統制の運用頻度と一致する。

図表7　サンプルサイズ選択の指針[2,3]

統制の性質	実施頻度	最低サンプルサイズ
マニュアル	1 日に何度も	25
マニュアル	毎日	25
マニュアル	毎週	5
マニュアル	毎月	2
マニュアル	四半期ごと	2
マニュアル	年次	1
自動化	プログラム化された統制活動ごとに、一つのアプリケーションをテストする（IT 全般統制は有効であると仮定）	
IT 全般統制	マニュアル及び自動化された IT 全般統制については、上述の指針に従う	

経営者は、統制の運用上の有効性のテスト、および経営者が評価した関連する統制が設計通りに運用されているかについての結論を文書化する必要がある。統制の設計の評価の文書化と同様に、経営者は、経営者が行った運用上の有効性のテストを会計監査人が再実施できるよう、十分に詳細に統制の運用上の有効性の評価を文書化する必要がある。

統制設計の評価で文書化された情報に加えて、統制の運用上の有効性の文書化では、以下を盛り込む必要がある。

- 実施されるテストステップの特性、タイミング、範囲
- テストの結果
- テスト実施者およびテスト実施日
- サンプルサイズおよび母集団
- 参考資料/証拠資料の場所
- 運用上の有効性に関する結論
- 把握された例外事項および関連する改善計画または補完統制

[2] 詳しい指針は SAS39 Audit Sampling に記述されている。
[3] 統制が効率的に運用されていることを想定している。

必要な証拠の性質の検討

監査基準第 2 号は、統制の設計および運営の有効性のテストで入手可能な、証拠の異なる形態について記述している。原則的に、登録企業は、適切な従業員に対する質問、関連文書化の調査、企業の統制の運用に関する観察、統制の適用の再実施の組み合わせを入手することが期待されている。証拠の形態には、以下のものがある。

a. 質問 － 質問は、社内で知識のある者の情報を探す手続きである。大半の組織では、専ら質問のみが用いられ、しばしば他の手続きがこれを補足する。
b. 文書の調査 － 質問だけでは統制の設計または運用の有効性を裏付ける十分な証拠を提供することができないため、追加のテストを実施しなければならない。統制の運用の有効性に関する十分な証拠を入手するために、組織は報告書または統制の実施の際に用いられた他の文書の検査などの他の手続きを行うことで質問を裏付ける必要がある。
c. 観察 － 統制について文書による証拠や実施の証拠がなく、証拠が今後も存在すると思われない場合、組織は、企業の活動を観察することにより、適切な従業員に関する質問を裏付けなければならない。
d. 再実施 － 統制の設計または運用の有効性に関し、証拠の質が十分ではない可能性がある場合、組織は統制を再実施し、独自に例外事項報告書を出力し、例外事項を調査することを選択することがある。例えば、例外事項報告書の署名だけでは、全ての例外事項が調査されたことを証明するのに十分ではない可能性がある。その場合、企業は、その統制の再実施を選択し、独自に例外実行報告書を出力し、例外事項を調査することを選択できる。

統制のテストタイミングの検討

企業は、統制の基準目標を達成するために必要な統制が有効に運用されているかどうかを判断する上で適切な経営者報告書における特定の期日付けで、統制テストを一定期間実施しなければならない。組織のテスト実施期間は、テストを行う統制の性質と特定の統制が運用される頻度、そして適用される特定の方針により異なる。継続的に運用される統制もあれば（例えば、ユーザアクセス申請の承認など）、特定の時期にしか運用されない統制（例えば、ユーザアクセスリストの定期的なレビューなど）もある。一般的に、企業は、統制が運用されている時期にテストを実施しなければならない。

ロールフォワードのテスト

多くの企業において、IT 統制のテストは、中間期（期末以前）に実施される。組織が統制を中間期にテストする際、残りの期間についての統制の運用に関してどのような追加的な証拠を入手するかを決定しなければならない。こうした決定を下す際に、組織は以下の点を考慮する必要がある。

- 「期日」前にテストされた特定の統制とこれらのテスト結果
- これらの統制の運用の有効性に関して入手した証拠の程度
- 期末までの期間
- 中間期後に財務報告に関する内部統制における重要な変更が起きた可能性

5. 不備の優先順位付けと改善

PCAOB の指針を考慮

2004 年 11 月に、PCAOB は、業務処理統制の不備がない場合の IT 全般統制の不備は、単なる統制の不備として分類されうると示唆する指針を公表した。しかし、PCAOB は、IT 全般統制の不備が、不備以上のもの、そしておそらく「重要な欠陥」につながる可能性のある 3 つの条件についても、引き続き述べている。その 3 つの条件は、以下のとおりである。

- アプリケーションレベルにおける不備 － IT 全般統制の不備の重要性は、業務処理統制に及ぼす影響に関連して評価される。すなわち、関連する業務処理統制が有効でないかどうかを評価する必要がある。アプリケーションの不備が IT 全般統制によってもたらされている場合、両者は同じように対応される。例えば、アプリケーションに基づいた税額計算が大幅に間違っており、税率表の変更に係る統制がお粗末だったためにそれが引き起こされている場合、その業務処理統制（計算）および全般統制（変更管理）は、重要な欠陥として分類されうる。
- 統制環境の不備 － IT 全般統制の不備が業務処理統制に及ぼす影響に関連して評価されると、その統制の不備は、他の統制の不備と合わせて評価される必要がある。例えば、経営者が修正しないことに決めた IT 全般統制の不備が統制環境に関連する場合、これらが統制環境に影響を及ぼす他の不備とまとまった場合、統制環境に重大な不備または重要な欠陥が存在するという結論につながりうる。
- 合理的な期間内での不備の未改善 － PCAOB による監査基準第 2 号の指示に基づいて、監査人は、善管注意義務を負って職務を遂行する者であれば、IT 全般統制の不備それ自体が重大な不備だという結論付を判断するだろう。このように、経営者と監査委員会には伝えられているものの、ある合理的な期間を超えて修正されていない IT 全般統制の不備は、重要な欠陥の大きな目安となる。

IT 全般統制の不備の把握と評価

すべての不備は、IT の不備も含め、財務/業務チームがレビューし、全体的な内部統制の評価の一部として評価する必要がある。IT 統制の不備は、単独で評価してはならない。同様に、財務諸表の統制目標を直接支援する業務処理統制も、財務/業務チームがレビューし、評価する必要がある。

参考資料 H「統制の文書化とテストテンプレートのサンプル」に示した IT 全般統制の不備の評価に対する一般的な指針は、統制の不備に関する予備的な評価をサポートするために、不備の評価に関する決定手順の例を示したものである。しかし、これは単に予備的な分析にすぎず、全体的な財務/業務チームは、追加レビューを実施し、結論を下す必要がある。
一般に、企業が対応しなければならない不備には 2 つの種類がある。

1. 設計の不備 － これらは、関連するリスクを十分に低減しない、欠落した統制、不適切な統制、付属書類の欠如、その他の統制の設計上の不具合に関する問題である。
2. 運用上の有効性の不備 － これらは、年間を通じて統制が設計された通りに一貫して実施されないといった、統制の運用上の一貫性に関する問題である。

統制の不備が合わせた影響の考慮

ある場合、個別の統制の不備は重要でないと考えられるかもしれないが、他の同様の不備とまとまった場合、その効果はより大きくなる可能性がある。例えば、財務アプリケーションへのユーザアクセスリストの定期的なレビューを実施しない企業は、統制の設計上の不備を有すると通常考えられる。特に他の補完統制が存在する場合、統制の不備はそれ自体では重要でない可能性がある。しかし、この組織が同じアプリケーションのユーザアクセス申請も承認しなかった場合、この二つの不備のまとまった影響は重大な不備または重要な欠陥につながる可能性がある。換言すれば、ユーザアクセス申請およびユーザアクセスレビューに関する統制の不備の影響を合わせた場合、財務アプリケーション内のユーザアクセスの正当性、ひいてはシステム内の処理の正当性にも疑問が生じる可能性がある。

統制の不備の改善

大半のプロジェクトの改善の局面では、どこに多大な作業と費用をつぎ込むかが絡んでくる。導入にはあまり費用と時間がかからないが、運用にはより多くの費用がかかる改善を短期間で実施するという選択をとるかもしれない。例えば、システム内のユーザを追加、変更、削除するというマニュアルのプロセスは時間がかかり、進捗度が遅い。しかし、企業が迅速な解決を求めている場合、マニュアルによる承認と入力のアプローチは、最も即効性のある解決であることが多い。しかし、より長期の解決法は、適切な承認のないユーザアクセスを制限するプロセスの自動化が含まれる可能性がある。このアプローチは、短期的には費用が間違いなくかさむが、長期的には信頼性が高く、費用対効果が高まることが多い。

6. 持続可能性の構築

この時点で、IT 統括責任者は IT 内部統制プログラムの有効性を評価する立場にいなければならない。有効な内部統制、統制の評価と経営者の業務遂行能力は、IT 部門の組織と企業文化の一部となる必要があり、それは長期的に持続可能でなければならない。統制は、事象でなく、継続的なサポートと評価を常に新しい状態で維持する必要のあるプロセスである。最終的な目標は、IT 統制プロジェクトを、プロセスに変換することである。この目的を達成するために、以下のアクティビティを考慮する必要がある。

- 企業改革法プロジェクトの導入後のレビューを実施し、正しく行われているもの、改善が必要な領域を把握する。
- 最新の SEC および PCAOB による解釈の変更が将来のアプローチに影響を与えるかを見極めるため、彼らのスピーチおよび指針をレビューする。
- このアプローチを改善するための提案および機会がないか、他の個別資料にあたる。
- このプロセスに対する改善の可能性を話し合うために、同業他社とミーティングを行う。
- プロセスの自動化およびプログラム変更統制のソフトウェアの導入といった、企業改革法の問題点に対処する長期的な解決法を検討する。
- 深く根付いたプロセスとするため、次年度に向けた予備計画およびスケジュールを作成する。
- 企業改革法のプロセスを、より広範な IT ガバナンスのイニシアチブに組み入れる。

統制の合理化

統制の合理化（または除外）は、統制を維持する段階で起こるべきもう一つのイニシアチブである。文書化されたものの、時が経つにつれて、次第に有用でなくなる統制が出てくることは間違いないだろう。企業は、統制を定期的に見直し、統制のリストから除外できる統制を把握する必要がある。その際に、統制を除外することによる影響および、なぜその統制が除外されたのかについての論拠を説明するた

めに文書を作成する必要がある。

統制の自動化

ほとんどの場合、自動化が可能なマニュアル統制が相当数存在する。参考資料 D「業務処理統制〔アプリケーション統制〕」に示した自動化された統制の例は、マニュアル統制をどの時点で自動化された統制に転換するかを把握する上で、重要な出発点を示している。企業は、参考資料 D の例とマニュアル統制をレビューし、どれが自動化された統制に変換可能かを判断することが可能である。多くの場合、企業が入手可能なアプリケーションおよび望まれる統制の性質により、より詳しい情報が必要になるだろう。SAP およびオラクルといったアプリケーションについては、より詳しいベンチマークを提供する組織もある。

アプリケーションのベンチマーキングの実施

アプリケーションのベンチマーキングに関する概念は、PCAOB が 2004 年 11 月の指針で導入したもので、参考資料 D にその全貌が詳述されている。この考えでは、テストを通じてアプリケーションがひとたび信頼できるとみなされれば、毎年これをテストする必要はない。その結果、遵守のプロセスをより効率的で有効にすることで、作業の削減が実現できる。

参考資料 A ー 企業改革法入門

企業改革法は、企業の責任を強化するという米国議会の強固な意志を示したものである。同法は、企業のスキャンダルや企業統治における失敗によってダメージを受けた米国の公開市場における投資家の信頼を取り戻すために制定された。同法および関連規制は、説明責任、開示、報告に関する規則を改訂したが、同法は多くの箇所で、以下のように明確な前提を述べている。すなわち、良い企業統治と倫理的な商慣習はもはや自明のものではないということである。

背景

企業改革法は、2002 年 7 月に米国議会で可決され、同月 30 日に大統領によって法制化された。中でも同法の 404 条は、SEC に登録する公開企業およびその監査人に、財務報告に係る内部統制の設計および有効性について、年次評価および報告を行うことを要求している。

企業改革法と内部統制全般の重要性については、一般に多くの記述がある。しかし、この領域で IT が果たす重要な役割についてはほとんど触れられていない。財務報告の信頼性は、よく統制された IT 環境に大きく依拠することに、多くの人が同意するだろう。このため、財務報告の観点から IT 統制の対応を考慮する組織は情報を必要としている。本稿は、主に SEC 登録企業が評価活動の一環として IT 統制を考慮する際の支援を目的としているが、他の国や地域の法律に準拠して設立された企業およびアメリカと同様の CEO または CFO による認証（宣誓）を導入した国や地域の企業を支援するために用いることも可能である。

本稿の作成にあたり、多くの IT 統制が検討された。しかし、検討対象を財務報告に係る内部統制に直接関連する統制に限定するために多大な努力が払われた。したがって、本稿は、統制の業務上および効率性の問題をサポートする統制を意図的に排除している。しかし、いずれは統制の業務上および効率性の問題に対応し、開発中の統制構造およびプロセスに組み入れることは避けられないだろう（そして望ましい）。これらの領域についてのより詳しい指針は、ITGI 発行の *Board Briefing on IT Governance 第 2 版*[4]および *IT Governance Implementation Guide*[5]を参照されたい。

企業改革法ー企業の説明責任の強化ー

企業改革法は、ビジネスと規制環境を根本的に変えてしまった。同法は、内部のチェック・アンド・バランスを強化する手法を通じて企業統治を高め、最終的に企業の説明責任の強化を目指すものだ。しかし、重要な点は、同法404条は経営幹部や業務プロセス・オーナに単に適切な内部統制の構造を確立し、維持することだけを求めているのではなく、毎年その有効性を評価することも求めていることである。この区別は重要である。

ITは、内部統制で決定的な役割を果たしている。システム、データ、およびインフラの構成要素は財務報告プロセスにとって極めて重要である。PCAOBの監査基準第2号は内部統制におけるITの重要性を次のように述べている。

[4] IT Governance Institute, *Board Briefing on IT Governance, 2nd Edition*, USA, 2003
[5] IT Governance Institute, *IT Governance Implementation Guide*, USA, 2003（2006 年後半に第 2 版が出版の予定）

情報システムにおける企業のITの使用に関する性質と特徴は、企業の財務報告に係る内部統制に影響を及ぼす。

特に経営幹部の地位にあるIT専門家は、企業改革法の要件を満たすために、内部統制の理論と実践に精通している必要がある。最高情報責任者（CIO）および信頼度の高いITシステムの運用責任者は、以下の課題に取り組まなければならない。

- 内部統制に関する知識を高める。
- 組織全体の企業改革法に対する遵守計画の理解。
- 特にIT統制に対応するための遵守計画の策定。
- この計画を企業改革法の遵守計画全体と統合する。

従って本稿の目的は、経営幹部、IT担当責任者、IT統制の専門家、アシュアランス専門家を含む、ITシステムの信頼できるオペレーション責任者に、以下に関する指針を提供することである。

- IT統制環境の現状を評価する。
- 企業改革法404条の要件を満たすために必要な統制を設計する。
- 将来に向けて、統制のテストおよび維持のためのアプローチを開発する。
- 例外事項を把握し、把握した例外事項に対しては補完統制を追加し、関連する改善計画を立案する。

財務報告に係る内部統制の監査

2004 年 3 月、PCAOB は、「財務諸表監査に関連して実施される財務報告に係る内部統制の監査」と題する監査基準第 2 号を承認した。本基準は、SEC の承認を受け、2004 年 6 月に発効した。この監査基準は、財務報告に係る内部統制の監査を実施する上での要件を確立し、監査人に求められる範囲とアプローチについての重要な方向性を与えている。

PCAOB による監査基準第 2 号は、取引がどのように開始、承認、記録、処理、報告されているかを含む取引の流れを監査人が理解するための要件を盛り込んでいる。多くの場合、これらの取引には業務情報の記録および処理をサポートする財務アプリケーションが関与している。これらのアプリケーションの信頼性は、それ自体がデータベース、ネットワークおよびオペレーティングシステムといった他のシステムに依拠している。これらはまとまった形で財務報告プロセスに関わる IT システムを定めており、その結果、財務報告に係る内部統制の設計および評価の際に検討が必要となる。

PCAOB の監査基準第 2 号は、情報技術（IT）は財務報告に係る内部統制に「広範な」影響を及ぼすと述べている。つまり、同監査基準は、全体的な統制環境に対する IT 統制の重要性を認識し、財務報告プロセスにおいてどのように IT が用いられているか、およびリスク管理のために統制がどのように設計され、実施されているかを理解することを企業に求めている。特に、同監査基準は、企業改革法に関して考慮する必要のある 4 つの IT 統制、すなわちプログラム開発、プログラム変更、コンピュータ・オペレーション、プログラムおよびデータへのアクセスを強調している。

企業改革法が経営者に求めている事項

企業改革法に関する議論の多くが 302 条と 404 条に係わるものである。その要点を**図表 8** に簡潔に示した。

図表 8－企業改革法の要件の要約

	302 条	404 条
対象	主たる経営幹部および財務責任者を含めた経営者（認証を行う経営幹部）	経営者、経営幹部、および財務責任者（「経営者」は PCAOB によって定義されていない）
内容	1. 認証を行う経営幹部は財務報告に係る内部統制を確立し、維持する責任がある。 2. 認証を行う経営幹部は、一般に認められた会計原則に従った対外的な目的のための財務報告の信頼性と財務諸表の作成に関して合理的な保証を提供するため、財務報告に係る内部統制を設計している、または彼らの監督の下、財務報告に係わる内部統制を設計させている*。 3. 直近の四半期に発生し、企業の財務報告に係わる内部統制に重要な影響を与えた、または重要な影響を与え得る財務報告に係る内部統制の変更は開示されている。 4. 財務報告に係る内部統制における変更の理由が重要な欠陥の修正である場合、経営者は変更の理由と状況が、その変更に関する開示に誤解を与えないために必要な重要な情報かどうかを判断する責任がある。	1. 企業の財務報告に係る適切な内部統制を確立・維持する責任が経営者にあることの表明 2. 企業の財務報告に係る内部統制の有効性に関して必要な評価を行う際に、経営者が用いたフレームワークを把握していることの表明 3. 財務報告に係る内部統制が有効であるかどうかに関する明確な表明を含む、企業の直近の会計年度末付での財務報告に係る内部統制の有効性の評価 4. 年次報告書に含まれる財務諸表を監査した登録会計事務所（監査法人）が、企業の財務報告に係る内部統制に関する経営者による評価に対して監査報告書を発行していることの表明 5. 財務報告に係る内部統制に関する経営者報告書と監査人へのリプレゼンテーション・レター（経営者確認書）の両方に含まれた、企業の財務報告に係る内部統制の有効性について経営者による書面での結論。企業の財務報告に係る内部統制の有効性に関する結論はさまざまな形式で述べることが可能である。しかし、経営者は企業の財務報告に係る内部統制が有効であるかどうかに関して、率直な結論を述べることが要求される。 6. 一つ以上の重要な欠陥が存在する場合、経営者は財務報告に係る内部統制が有効であると結論を下すことができなくなる。さらに、経営者は直近の会計年度末付で存在するすべての重要な欠陥を開示する必要がある。
時期	2002 年 7 月に既に実施されている	2004 年 11 月 15 日またはそれ以降に終了する会計年度末**
頻度	四半期毎および年次の評価	経営者と会計監査人による年次の評価

404 条の最新の要件については、SEC のウェブサイトを参照のこと。

*外国民間発行企業については年に一度である。

**外国適用企業の一部は 2007 年 7 月 15 日に適用開始、非早期適用企業(7,500 万ドル未満の企業)は 2007 年 12 月 15 日まで延期できる。さらに、非早期適用企業は、2008 年 12 月 15 日までに企業改革法 404 条（B）の求める内部統制に関する監査人の証明報告を提出しなければならない。

開示に関する統制と手続き

開示に関する統制と手続きは、企業がすべての重要な情報をSECに提出する報告書で開示することを確実にするために設計されたプロセスをいう。また、これらの統制は、SECの規則と様式に定められた期間内に開示が承認され、これが完全かつ正確であり、記録され、処理され、要約され、報告されることを求めている。統制に対する重要な変更と同様に、統制の不備は、監査委員会と監査人に適時に伝達されなければならない。企業の主要な経営幹部と財務責任者は四半期ベースでこれらの統制が存在していることを証明しなければならない。

302条の経営者に対する要件

302 条

302条は主たる経営幹部および財務責任者を含めた経営幹部（認証を行う経営幹部）に対し、4半期、年度毎に財務報告に係る内部統制に関して以下のような認証を行うことを求めている。

- 認証を行う経営幹部は財務報告に係る内部統制を確立し、維持する責任があることの表明。
- 認証を行う経営幹部は、一般に認められた会計原則に沿って対外的な目的のための財務報告の信頼性と財務諸表の作成に関して合理的な保証を提供するために、財務報告に係る内部統制を設計し、またはこの者の監督の下で、財務報告に係わる内部統制を設計させたことの表明。
- 直近の四半期（年次報告書の場合は第4四半期）に生じ、企業の財務報告に係わる内部統制に重要な影響を与えた、または重要な影響を与え得る財務報告に係る内部統制の変更を報告書で開示していることの表明。

財務報告に係る内部統制における変更の理由が重要な欠陥の修正である場合、経営者は、その変更の理由と状況がその変更に関する開示に誤解を生じさせないために必要な重要な情報であるかどうかを判断する責任があり、また監査人はこれを評価する必要がある。

404条の経営者に対する要件

企業改革法404条は、経営者が財務報告に係る内部統制の評価について年次報告書で開示することを求めている。
同法は以下のように述べている。*財務報告に係る内部統制に関する経営者の報告書は、以下を含むことが要求されている。*

- *企業の財務報告に係る適切な内部統制を確立し、維持する責任が経営者にあることの表明。*
- *企業の財務報告に係る内部統制の有効性に関して必要な評価を行う際に、経営者が用いたフレームワークを把握していることの表明。*
- *財務報告に係る内部統制が有効であるかどうかに関する明確な表明を含む、企業の直近の会計年度末での財務報告に係る内部統制の有効性の評価。*
- *年次報告書に含まれる財務諸表を監査した登録会計事務所（監査法人）が、企業の財務報告に係る内部統制に関する経営者による評価に対して監査報告書を発行していることの表明。*

経営者は財務報告に係る内部統制に関する報告書と監査人へのリプレゼンテーション・レターの双方において、企業の財務報告に係る内部統制の有効性に関して書面による結論を提出しなければならない。企業の財務報告に係る内部統制の有効性に関する結論は、さまざまな様式で述べることが可能である。しかし、経営者は、企業の財務報告に係る内部統制が有効であるかどうかに関して、率直な結論を述べる必要がある。

一つ以上の重要な欠陥が存在する場合、経営者は財務報告に係る内部統制が有効であると結論を下すことができなくなる。さらに、経営者は直近の会計年度末で存在するすべての重要な欠陥を開示する必要がある。

会計年度中に一つ以上の重要な欠陥が存在する場合でも、経営者は直近の会計年度末付で、財務報告に係る内部統制が有効であると明言できる場合がある。このような表明を行う場合、経営者は「年度末」の前に重要な欠陥を除去するために財務報告に係る内部統制を変更していなければならない。さらに、会計年度末付で財務報告に係る内部統制の設計と運用が有効であるかどうかを判断するために、適切な期間にわたってその有効性を十分にテストしなければならない。

財務報告に係る内部統制

財務報告に係る内部統制はSECによって以下のに通り定義されている。

一般に認められた会計原則に従い、対外的な目的のための財務諸表の信頼性と財務報告の作成に関して合理的な保証を提供するため、登録企業の主要な経営幹部と財務責任者、または同様の職務を遂行する担当者により、またはその監督のもとで設計され、取締役、経営者およびその他の担当者によって実施されるプロセス。その方針と手続きは以下を含む。

1. *登録企業の資産の取引と処分を合理的な詳細さで正確かつ公正に反映する記録を維持するための方針と手続き。*
2. *一般に認められた会計原則に従った財務諸表の作成を可能にするために取引が必要に応じて記録されること、そして登録企業の収入と支出が経営者や取締役の承認に基づいていることに関して合理的な保証を提供する方針と手続き。*
3. *財務諸表に重大な影響を与えうる登録企業の資産が、未承認で取得、使用および処分されることを防止、または適時に発見することに関して合理的な保証を提供する方針と手続き。*

「登録企業」が「企業」として表現されていることを除き、PCAOBは同様の定義を用いている。

企業改革法における監査人の焦点

404条は、企業の会計監査人が財務報告に係る内部統制に関する経営者の評価を証明することを要求している。企業は、適切な統制（IT統制を含む）が機能していることを確保しなければならないだけでなく、統制の設計と運用の有効性に関する証拠およびテスト手続きの結果に関する文書を会計監査人に提供しなければならない。

企業改革法において、監査人の証明のための基準設定はPCAOBの責任となっている。404条の証明は特定の期日付で行われるが、PCAOB監査基準第2号は、財務報告の統制は証明の日付以前にある程度の期間にわたって機能していなければならず、また証明の日付以降も運用される見込みがあると言及している。

> *統制の運用上の有効性に対する監査人のテストは、統制が運用されている時点で行うべきである。統制が特定の期日以降に運用されていないとしても、「特定の期日」における統制は、その特定の期日での企業の財務報告に係る内部統制に関連する統制を含む。*

証明日以前に統制が運用されていなければならない期間を決定するために、経営者は会計監査人と話し合いを持つことが勧められる。

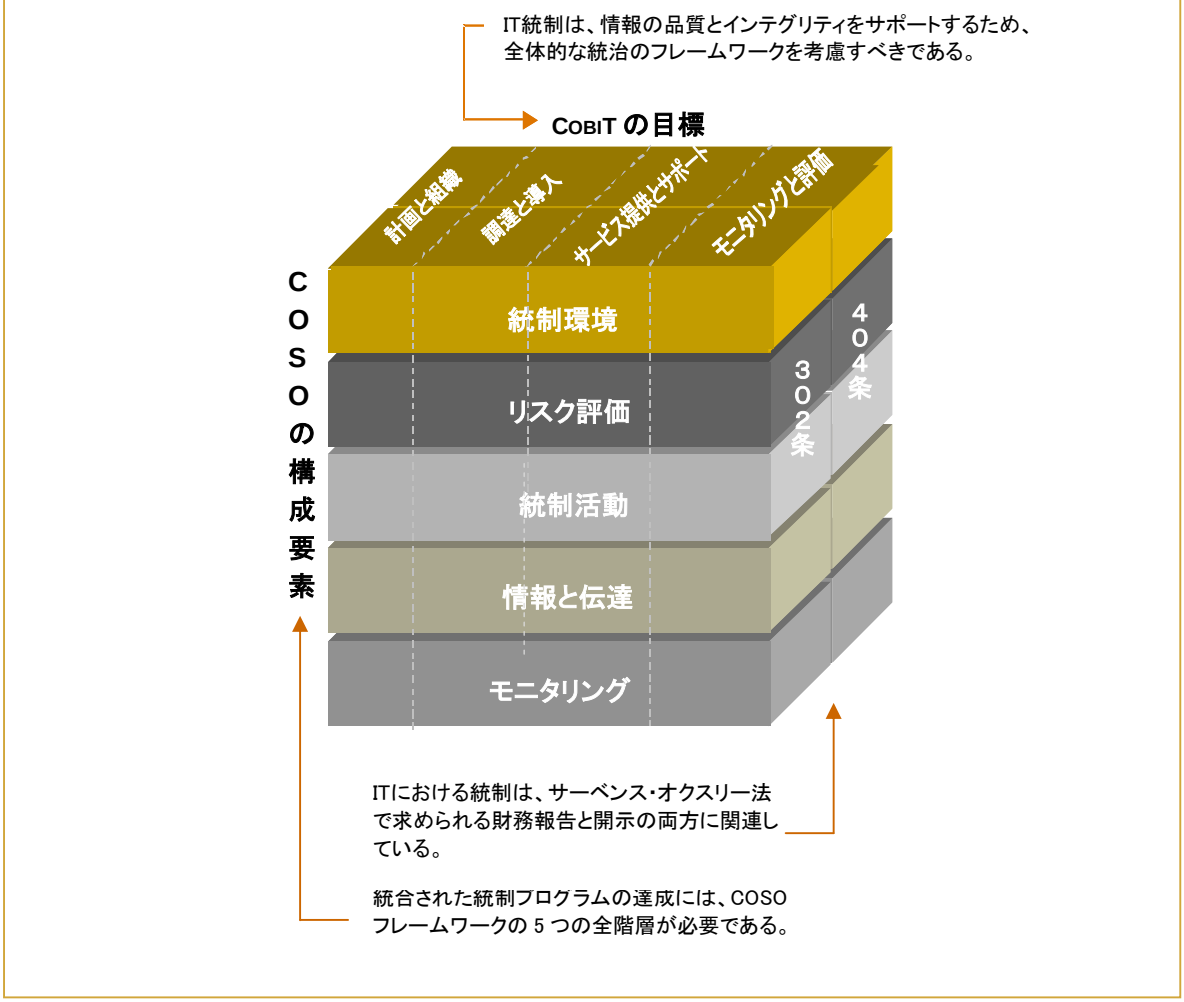
PCAOB監査基準第2号は、302条に関する会計監査人の責任について、特に次のように述べている。

> *財務報告に係る内部統制について経営者の四半期毎の認証に関する監査人の責任は、経営者による財務報告に係る内部統制の年次の評価に関する監査人の責任とは異なる。認証が的確で、かつ同法302条の要件を遵守するために、監査人の判断において、財務報告に係る内部統制の変更に関する開示に重大な修正が行われるべきだと気付いたかどうかを決定する根拠を示すために、監査人は四半期毎に限定された手続きを実施しなければならない。*
>
> *この責任を果たすために、監査人は四半期ベースで以下の手続きを実施する必要がある。*
> - *前回の通年監査の後、または中間財務諸表の事前レビューの後に生じた可能性がある、年次・中間財務諸表の作成に関連する財務報告に係る内部統制の設計と運用の重大な変更について経営者に質問する。*
> - *財務報告に係る有効な内部統制に関連している場合は、中間財務諸表のレビュー（AU sec.722、中間財務情報を参照）において監査人が把握した虚偽記載の可能性を評価する。*
> - *財務報告に係る内部統制における変更が、企業の財務報告に係る内部統制に重大な影響を及ぼしたか、または重大な影響を及ぼす見込みがあるかどうかを、観察と質問により判断する。*

参考資料 B ― COSO と COBIT

前頁でも述べたように、COSO は内部統制を 5 つの構成要素に分類している。**図表 9** は、財務報告と開示の目標を満たすために、これらの要素のすべてが機能し、統合される必要があることを示している。COBIT も同様に IT のための詳細な指針を提供している。統制環境の把握に始まり、内部統制のモニタリングで終点に達する COSO の 5 つの構成要素は、立方体の水平の層で表現することができる。一方、計画と組織からモニタリングと評価に至るまでの COBIT の目標の領域は個別、およびまとまっても適用が可能である。

図表 9. COSO と COBIT の統制の構成要素の相互参照図



図表10は、COBIT のITプロセスについて述べるとともに、このITプロセスを適切なCOSOの構成要素と関連付けたものである。多くのCOBIT のITプロセスが、1つ以上のCOSOの構成要素と関連していることは明らかである。IT全般統制が業務処理統制に依拠する基盤を形成しているという性質からも、このことが予想される。また、こうした多様な相関関係は、IT統制が全ての基盤であり、信頼できる内部統制にとって極めて重要な理由をさらに明確にしている。

COBIT は、IT のリスクと統制のガバナンスを管理する包括的なフレームワーク（枠組み）であり、4 つの領域、34 の IT プロセスならびに 215 の統制目標から構成される。COBIT には IT ガバナンスのすべ

ての観点に取り組む統制が含まれているが、本稿の作成には財務報告に係る重大な統制のみが用いられている。COBIT は自由に利用できるフレームワークであり、用いられるすべてのフレームワークはアクセスが容易で一般的に受け入れることが可能でなければならないという企業改革法の要件の精神に沿ったものである。COBIT は関連する統制とともに全社レベルおよびアクティビティレベルの目標を提供しており、COSO の補完として広く組織に用いられている。

これまでは財務報告に必要な要件に焦点を当ててきたが、本稿で述べた統制目標と考慮すべき事項は、企業改革法の遵守を考えている組織に必要とされる内容を上回っている可能性がある。企業改革法の遵守のために提唱されている内部統制のフレームワーク（COSO）は、SEC が推奨するように、IT 統制の項目を含んでいるが、こうした統制目標および関連する統制活動の要件を定めたものではない。こうした決定は依然として各組織の自由裁量となっている。したがって、企業は内部統制プログラムのサポートに必要な IT 統制の内容と範囲を個別に評価する必要がある。

本稿は、すべての事例に当てはまる手法を提案するものではない。本稿は替わりに、企業に特定の状況に合った統制目標のマトリクス表の作成を推奨している。例えば、システム開発が低リスクだと考えられる場合、企業は提案された統制目標のいくつか、あるいは全部の修正または削除を選択する可能性がある。また、企業は会計監査人と相談し、監査上極めて重要な全ての統制目標に確実に取り組む必要がある。

本稿の重要な役割は、COSO、そして最終的には企業改革法の遵守に沿った、特定の統制目標に関する指針を IT 専門家に提供することにある。したがって、参考資料 C ではこうした情報を取り上げている。これまでも述べたように、IT 部門は、統制目標、統制の実例および統制のテストのうち、企業の内部統制評価プログラムにはどれが必要かを判断する上で、業務の内容と範囲を考慮する必要がある。

以下の図表を用いた指針を作成する上で、各統制目標は企業改革法の財務報告の要件との関連性と重要性を明確にすることが求められた。この過程で、ある COBIT の統制目標は消却され、または財務報告目的の適用性に関して単一の目標に統合された。さらに、各 IT の統制目標は、企業の企業改革法の遵守プログラム全体との整合を取るために COSO の構成要素に合わされた。これについては、**図表 10** を参照されたい。

図表 10 ― COBIT の領域と COSO の構成要素

			COSOの構成要素				
全社レベル	アクティビティレベル	COBIT の IT 領域	統制環境	リスク評価	統制活動	情報と伝達	モニタリング
計画と組織（IT 環境）							
●		IT戦略計画の策定		●		●	●
		情報アーキテクチャの定義					
		技術指針の決定					
●		ITプロセスと組織及びその関わりの決定	●			●	●
		IT投資の管理					
●		マネジメントの意図と指針の周知	●			●	
●		IT人材の管理	●			●	
●		品質管理	●		●	●	●
●		ITリスクの評価と管理		●			
		プロジェクト管理					
調達と導入（プログラムの開発と変更）							
		コンピュータ化対応策の明確化					
	●	アプリケーションソフトウェアの調達と保守			●		
	●	技術インフラの調達と保守			●		
	●	運用の促進			●	●	
		IT資源の調達					
	●	変更管理		●	●		●
	●	ソリューションおよびその変更の導入と認定			●		
サービス提供とサポート （コンピュータ･オペレーションおよびプログラムとデータへのアクセス）							
	●	サービス・レベルの定義と管理	●		●	●	●
	●	サードパーティのサービスの管理	●	●	●		●
		性能とキャパシティの管理					
		継続的なサービスの保証					
	●	システムセキュリティの保証			●	●	●
		コストの捕捉と配賦					
●		利用者の教育と研修	●			●	
	●	サービスデスクとインシデントの管理			●	●	●
	●	構成管理			●	●	
	●	問題管理			●	●	●
	●	データ管理			●	●	
		物理的環境の管理					
	●	オペレーション管理			●	●	
モニタリングと評価 （IT環境）							
●		IT成果のモニタリングと評価			●	●	●
●		内部統制のモニタリングと評価	●				●
●		規制遵守の確実化			●	●	●
●		ITガバナンスの提供	●				●

参考資料 C ― IT 全般統制

企業改革法は、組織が適切な内部統制のフレームワークを選択し、導入することを求めている。COSOの「*内部統制－統合的フレームワーク*」は、企業改革法を遵守する企業に最も広く用いられるフレームワークとなった。COSOは、全体的な統制環境に対するITの重要性に言及する一方で、企業がその環境に合わせた特定のIT統制を設計し導入するために必要な、詳しい指針は与えていない。

本稿を作成する際、IT統制の目標、具体的な統制例および統制のテストはCOBIT を用いた（参考資料Bを参照）。また、ISO17799、*The Code of Practice for Information Security Management*も考慮した。サービスの管理に関しては、ITインフラストラクチャ・ライブラリ（ITIL®）も考慮した。これらの統制のフレームワークはすべて業務上および財務上の目的に対応しているが、本稿では財務報告の統制に重大な指針**のみ**を選択し、用いている。

全社レベルのIT統制

一般的に、IT 全般統制は、全社レベルおよびアクティビティレベルの目標を含んでいる。本稿ではその両方を扱っているが、全社レベル統制の目的は、企業の企業文化および運用のスタイルを理解することにあるため、全社レベル統制の目標は「考慮すべき点」として示されている。さらに、全社レベル統制は、特定のアクティビティを伴う可能性が低い。したがって、全社レベル統制の各領域について統制とテストを定義しようとすることは本稿の範囲を超える。このため、本稿では、全社レベル統制の設計と有効性の全体的な評価のための考慮事項について述べている。

これらを用いる際、企業は「はい」または「いいえ」といった単純な回答をしないように留意する必要がある。考慮事項として挙げた質問は、統制がどのように実施されているかの事例を挙げている。これを参考に、文書を閲覧したり、追加の質問をして、統制の運用の確証を得ることができるだろう。

図表 11 から **14** は、企業の IT 統制に係る全社レベル統制の評価について考慮すべき事項を示したものである。大半の企業が内部統制プログラムに対して COSO の統制フレームワークを用いていることから、図表は COSO と同じ順序で構成されており、全社レベル統制の目的が達成されているかどうかを判断する上で考慮すべき点を扱っている。

統制環境

統制環境は、有効な内部統制の基盤を作り、「上級役員の気風」を確立し、企業ガバナンスの構造の頂点を表す。統制環境の構成要素で提起された問題は、IT 部門全体に当てはまる。

図表11-統制環境について考慮すべき事項		
考慮すべき事項	**COBIT4.0の参照項目**	**回答/証拠**
IT戦略の策定		
1. 経営者は経営目標に沿ったIT戦略計画を作成しているか? 計画の策定手法は IT戦略計画により影響を受ける内部・外部利害関係者からの要望を反映する仕組みを含んでいるか?	PO1.4	
2. IT部門は社内の業務プロセス・オーナおよび関連当事者と、IT計画について話し合っているか？	PO1.2 PO6.5	
3. IT統括責任者は、定期的に最高経営責任者と最高財務責任者に自らの業務、課題、リスクを伝えているか? また、この情報は取締役会と共有されているか?	PO1.2 PO6.5	
4. IT部門は設定した目標を達成するため、戦略計画の進捗状況をモニターし、これに従って行動しているか?	PO1.3 ME1.2	
ITプロセス、組織および関係		
5. ITマネージャーには、責務を遂行する上で適切な知識と経験があるか?	PO7.2 PO7.4	
6. 関連システムとデータの一覧が作成され、オーナが把握されているか?	PO4.9	
7. IT部門の役割と責任が、定義・文書化され、理解されているか?	PO4.6	
8. ITスタッフは、内部統制に関する自分達の責任を理解し、受け入れているか?	PO4.6 PO6.1 ME2.2	
9. データのインテグリティの責任と義務は、適切なデータ/業務責任者に伝えられ、こうした義務が果たされたか?	PO4.9 PO6.5	
10. IT統括責任者は、一個人が重要なプロセスを崩壊させることを合理的に防ぐ役割と責任の分割（職務の分離）を設けているか?	PO4.11	
IT人的資源の管理		
11. IT部門は、企業の倫理、業務慣行、および人事評価を含む誠実性を育てるという企業精神を採用・促進しているか?	PO6.1 PO7.7	
利用者の教育と研修		
12. IT統括責任者は全スタッフの倫理的行動、システム・セキュリティの実践、守秘基準、誠実性基準、およびセキュリティ上の義務を含む教育と継続的な研修プログラムを提供しているか?	PO7.4 DS7.1	

情報と伝達

COSOは、事業を運営し、企業の統制目標を達成するためには、組織の全レベルで情報が必要になると述べている。しかし、重要な情報の把握、管理そして伝達は、IT部門にとってますます困難な課題となっている。統制目標を達成するため、どの情報が必要かを決定しなければならない。従業員の責務の遂行が可能な形式と時間内でこの情報を伝達することにより、COSOのフレームワークにある他の4つの構成要素がサポートされる。

図表12—情報と伝達について考慮すべき事項		
考慮すべき事項	**COBIT4.0の参照項目**	**回答/証拠**
マネジメントの意図と指示の周知		
13. IT統括責任者は、変化しつつあるビジネスの状況を反映するため、定期的に方針、手続き、基準を見直しているか?	PO6.3	
14. IT統括責任者には、方針、手続き、基準の遵守を評価するプロセスと手続きがあるか?	ME2	
15. IT統括責任者は企業改革法（SOX法）に関連する自己の役割と義務を理解しているか?	ME3.1 ME3.2	

リスク評価

リスク評価は、予め設定された目標を達成する目的で、重大なリスクの管理責任者による把握・分析を伴い、この把握・分析により統制活動の基盤が形成される。内部統制のリスクは、企業内の他の部署よりも、IT事業部でより大きい可能性が高い。リスク評価は全社レベルで（組織全体で）、またはアクティビティレベルで（特定のプロセスまたは事業単位で）行うことが可能である。

図表13—リスク評価について考慮すべき事項		
考慮すべき事項	**COBIT4.0の参照項目**	**回答/証拠**
ITリスクの評価と管理		
16. IT部門には、財務報告の目的達成を満たすために、情報リスクを定期的に評価する際に用いる、全社レベル、アクティビティレベルのリスク評価のフレームワークがあるか? またそのリスク評価はITが脅威にさらされる確率と見込みを考慮しているか?	PO9.1	
17. IT部門のリスク評価のフレームワークは、経営陣のブレーンストーミング、戦略的な計画、過去の監査、その他の評価等を含む、異なる領域からのインプットを用いて、質的・量的基準に従ってリスクの影響を測定しているか?	PO9.2 PO9.3 PO9.4 ME4.5	
18. リスクを許容できる場合、適切な保険、債務引受契約および自家保険などの関連するリスクの相殺および残余リスクに関する正式な文書化と受容の承認が行われているか?リスクが許容できない場合、経営者はリスク対応を行うための行動計画を準備しているか？	PO9.5 PO9.6	

モニタリング

継続的、かつある一時点の評価プロセスを用いた経営者による内部統制の監視を含むモニタリングは、ITマネジメントにおいてますます重要になっている。

図表14—モニタリングについて考慮すべき事項		
考慮すべき事項	**COBIT4.0の参照項目**	**回答/証拠**
品質管理		
19. すべての重要なITプロセス・統制・アクティビティに対して文書が作成され、保管されているか?	PO8.2	
20. 重要なIT機能に対し品質管理計画（例えば、システム開発やシステム導入）が存在するか? またその計画は、全般的およびプロジェクト特有の品質保証活動の双方に取り組むための一貫した手法を提供しているか?	PO8.1 PO8.6	
成果のモニタリングと評価		
21. IT統括責任者はIT部門の日々の活動を効果的に管理する適切な管理基準を確立しているか?	ME1.2 ME1.4	
22. IT統括責任者はITサービスの提供をモニターし、不足を把握しているか？ IT部門は改善のための活動計画に取り組んでいるか？	ME1.2 ME1.4	
内部統制のモニタリングと評価		
23. IT統括責任者は方針、手続き、IT全体のシステムとプロセスを含む、ITのオペレーションについて、独立した第三者のレビューを受けているか? 独立した第三者のレビューは、方針および手続きの遵守状況を評価しているか?	ME1.6 ME2.1 ME2.5	
24. 組織には、IT全般統制と業務処理統制を含むITに係る業務と統制の見直しに責任を持つIT内部監査機能があるか? 残された活動をフォローアップするプロセスがあるか? 外部サービス業者（サードパーティ）による内部統制のモニターを可能にする仕組みはあるか?	ME2.5 ME2.6 ME2.7	

アクティビティレベルのIT統制

規制当局、投資家、利害関係者に対する経営者の報告を可能にする情報の提供は、完全で正確な情報の収集と、それを適時に報告するサイクルの一部である。予想されるように、このサイクルはアプリケーション、データベース、データ処理の効率および有効性を高めるために用いられる他のツールなどの情報システムに大きく依存している。

この参考資料の以下の部分は、財務報告の目的をサポートするために特に設計された IT 統制に関する指針を提供することに焦点を当てている。前述の通り、これらの統制は網羅的なリストとなることを意図したものではなく、また、会計監査人が考慮する可能性のある内容を完全に表したものでもない。しかし、これらはどの IT 統制が企業の環境にとって必要かを企業自身が決定する上での出発点となる。以下の表には含まれていないかもしれないが、企業が考慮した上で関連のある IT 統制に対しても考慮する必要がある。

図表 15 から 27 では、特定の統制の例を星のマーク（✶）で強調し、これがもっとも関連する統制であることを示している。財務諸表のアサーションに適用されるもっとも関連する統制は、総勘定元帳への金額の記録および仕訳記入の記録（基準、基準外、連結）を含む、財務報告または他の求められる開示における重要な虚偽記載を予防、発見、修正する活動を含むと定義される。もっとも関連する統制はマニュアルの場合も、自動化されている場合もあり、性質上は予防的または発見的である。この定義は、企業改革法を遵守する上で一般に求められる統制を把握するため、**図表 15** から **27** までの統制に適用されている。**図表 15** から **27** までのタイトルには、COBIT の統制目標が括弧内で示してある。

前述の通り、この指針は例を示したものである。本稿でもっとも関連する統制として強調されない可能性のある統制も含め、遵守プログラムに盛り込む必要のある統制を決定する際には、いつものように専門的な判断が必要とされる。

図表 15ー アプリケーションソフトウェアの調達と保守(AI2)		
統制に関する指針		
統制目標ー財務報告の要件を効果的にサポートするアプリケーションおよびシステムソフトウェアが調達・開発されている合理的な保証を提供する。		
根拠理由ーソフトウェアの調達または保守のプロセスには、経営目標の達成をサポートするシステムの設計、調達/構築および導入が含まれる。このプロセスは既存のシステムの主要な変更を含む。ここでは財務情報の開始、記録、処理および報告ならびに開示をサポートするために統制が設計され、実施される。この領域に不備がある場合、財務報告と開示に重大な影響を与える可能性がある。例えば、アプリケーション・インタフェースに関する十分な統制がない場合、その財務情報は完全でない、または正確ではない可能性がある。		
統制の例	**統制のテストの例**	**COBIT4.0 の参照項目**
組織は、セキュリティ、および処理のインテグリティといった組織の要件を含むシステム開発ライフサイクル方法論(SDLC)を有する。 ☆	組織の SDLC 方法論のコピーを入手する。これをレビューし、セキュリティおよび処理のインテグリティといった要件の記載があるかを確かめる。これらの要件が開発または調達ライフサイクルを通じて、常に考慮されていることを判断する適切なステップが存在しているかを考慮する（セキュリティおよび処理のインテグリティを要件の段階で考慮する必要がある。）。	PO8.3 AI2.3 AI2.4
組織の SDLC 方法論に関する方針および手続きは、新システムの開発と調達、既存システムの大幅な変更を考慮している。	組織の SDLC 方法論をレビューし、新システムの開発と調達、既存システムの大幅な変更の両方を考慮しているかを確かめる。	PO6.3 AI2 AI6.2
SDLC 方法論は、情報システムが、完全で、正確で、承認された、そして正当な取引の処理をサポートする業務処理統制を含むよう設計されなければならないという要件を含んでいる。 ☆	SDLC 方法論をレビューし、業務処理統制についての記載があるかを確かめる。業務処理統制について、開発または調達ライフサイクルを通じて常に考慮されるように適切なステップが存在するかを考慮する（業務処理統制が概念設計また詳細設計の両段階において組み込まれていなければならない）。	AI1 AI2.3 AC
組織には、全般的な戦略の方向性に沿った調達・計画プロセスがある。	SDLC 方法論をレビューし、組織の全体的な戦略の方向性が考慮されているかを判断する。例えば、IT 運営委員会は提案されたプロジェクトが戦略的な事業要件に沿っており、承認済みの技術を活用するように、プロジェクトをレビューし、承認しなくてはならない。	PO4.3 AI3.1
信頼できる環境を維持するため、IT 統括責任者は、アプリケーションの設計、パッケージソフトウェアの選択、テストの実施においてユーザを適切に関与させている。 ☆	SDLC 方法論をレビューし、ユーザが適切にアプリケーションの設計、パッケージソフトの選択、テストに適切に関与しているかどうかを確かめる。	AI1 AI2.1 AI2.2 AI7.2
統制が有効に運用されていることを検証するため、導入後レビューを実施している。	新システムと報告された重要な変更事項に対して、導入後レビューを行っているかを確かめる。	AI7.12
組織は調達・開発・計画プロセスに沿ってシステムソフトウェアを調達・開発している。 ☆	新しい財務システムの導入をもたらしたプロジェクトのサンプルを選ぶ。これらのプロジェクトの文書や成果物をレビューし、企業の調達・開発・計画プロセスに従って完成したかを確かめる。	AI2

図表 16－技術インフラストラクチャの調達と保守（AI3）		
統制に関する指針		
統制目標－財務報告のアプリケーションをサポートする適切なプラットフォームを提供するため技術インフラストラクチャを調達しているという合理的な保証を、統制により提供する。		
根拠理由－技術インフラストラクチャの調達と保守のプロセスには、アプリケーションとコミュニケーションをサポートするシステムの設計、調達/構築および導入が含まれる。サーバ、ネットワーク、データベースを含むインフラの構成要素は、安全で信頼できる情報処理にとって極めて重要である。適切なインフラストラクチャがない場合、財務報告のアプリケーションがアプリケーション間でデータを移行できないリスクや、財務報告のアプリケーションが作動しないリスク、そして重要なインフラストラクチャの欠陥が適時に検出されないリスクが増大する。		
統制の例	**統制のテストの例**	**COBIT4.0 の参照項目**
文書化された手続きが存在し、参照され、ネットワークデバイスとソフトウェアを含むインフラストラクチャシステムが、財務アプリケーションの要件に基づいて調達される。	技術インフラストラクチャ導入のサンプルを選出する。これらのプロジェクトに関連する文書や成果物をレビューし、調達プロセスの間、インフラストラクチャの要件が適時に検討されていたかどうかを確認する。	AI3

図表 17－運用の促進（PO6、PO8、AI6、DS13）		
統制に関する指針		
統制目標－必要な調達と保守プロセスを定義する方針または手続きが策定、維持されており、これらがアプリケーションの適切な使用と、実施している技術的な解決策をサポートするために必要な文書化を定義しているという合理的な保証を提供する。		
根拠理由－方針と手続きには SDLC 方法論、アプリケーションの調達・開発、保守プロセスならびに必要な文書化が含まれる。組織によっては、方針と手続きに、サービス・レベル・アグリーメント、業務上の慣行、研修資料も含まれる。方針と手続きは、業務プロセス活動を一貫した客観的な方法で実施するという企業の意欲をサポートする。		
統制の例	**統制のテストの例**	**COBIT4.0 の参照項目**
組織にはプログラム開発、プログラム変更、プログラムとデータへのアクセス、コンピュータ・オペレーションに関する方針と手続きがあり、これらは経営者が定期的にレビューし、更新し、承認している。 ☆	組織には、業務の変化に合わせて定期的に見直しされ、更新される方針と手続きがあることを確認する。方針と手続きが変更された際には、経営者がその変更を承認しているかを確かめる。 プロジェクトのサンプルを抽出し、ユーザ参照文書、サポートマニュアル、システム文書および操作マニュアルが作成されているかを判断する。これらのマニュアルの草案が、ユーザ受入テスト（UAT）に組み込まれているかを検討する。提案された統制に変更があった場合、その文書も更新されているかを確かめる。	PO6.1 PO6.3 PO8.1 PO8.2 PO8.3 AI6.1 DS13.1
組織は、承認され文書化された方針と手続きに従ってシステムを開発、保守、運用している。 ☆	方針と手続きの文書を入手し、組織がその IT 環境を、組織に沿って管理しているかを判断する。	PO6.1 PO6.3 PO8.1 PO8.2 PO8.3 AI6.1 DS13.1

図表 18－ソリューションおよびその変更の導入と認定(AI7)		
統制に関する指針		
統制目標－本番環境に移行する前にシステムが適切にテストされ、検証されている、そして関連統制が意図した通りに運用され、財務報告の要件をサポートしているという合理的な保証を提供する。		
根拠理由－導入テストと検証は、新システムの本番環境への移行に関連している。新システムの導入前に、システムが設計通りに稼動しているかを判断するため、適切なテストと検証を行う必要がある。適切なテストが実施されない場合、システムは意図した通りに機能せず、無効な情報を提供する可能性がある。その結果、信頼できない財務情報と報告書が生じることになる。		
統制の例	**統制テストの例**	**COBIT4.0 の参照項目**
アプリケーションと技術インフラのすべての重要な変更は、テスト戦略を策定し、これに従っている。この中では、導入されたシステムが意図した通りに稼動するように、単体テスト、システムテスト、統合テスト、およびユーザ受入テスト（UAT）を行っている。 ☆	システム開発プロジェクトと重要なシステム更新のサンプルを選ぶ（技術更新を含む）。正式なテスト戦略を策定し、これに従っているかを判断する。この戦略が潜在的な開発および導入リスクについて検討しており、これらのリスクに取り組む上で必要なすべての要素 について言及しているかを検討する。（例えば完全で正確な報告書を作成する上で、システム・インタフェースの完全性と正確性が不可欠である場合、これらのインタフェースをテスト戦略に含める。）（注: 本番環境への最終的な移行に関する統制は、**図表 19** の変更管理で述べる。）	AI7.2 AI7.4 AI7.6 AI7.7
テスト計画と確立されたテスト基準に従って、負荷テストとストレステストを実施する。	財務報告にとって重要なシステム開発プロジェクトとシステム更新のサンプルを選ぶ。キャパシティとパフォーマンスが潜在的な懸念事項と考えられる場合、負荷テストとストレステストの手法をレビューする。負荷テストとストレステストで構造化した手法がとられたか、そしてその手法が、処理される取引の種類、そして同時に稼動している他のサービスのパフォーマンスに与える影響など、予想される量を適切にモデル化しているかを検討する。	AI7.2
データの転送が完全・正確・正当であることを確かめるために、他のシステムとのインタフェースをテストする。 ☆	財務報告にとって重要なシステム開発プロジェクトとシステム更新のサンプルを選ぶ。データ転送が完全であることを確認するため、記録の合計が正確で正当であるなど、他のシステムとのインタフェースをテストしているかを確認する。テスト範囲が十分であるか、そしてデータ転送が不完全な場合はテスト範囲に「修復」も含まれているかを検討する。	AI7.5
データ移行が完全・正確・正当であることを確認するため、データの移行元と移行先でテストを行う。 ☆	財務報告にとって重要なシステム開発プロジェクトとシステム更新のサンプルを入手する。データ移行戦略が文書化されているかを確認する。また、その文書にはデータ移行前に旧システムのデータを整理する、または不要なデータを消去するための戦略が含まれているか判断する。移行テスト計画をレビューする。	AI7.5

図表 19－ 変更管理（AI6、AI7）		
統制に関する指針		
統制目標－財務報告上重要なシステム変更は、本番環境に移行する前に承認され、適切にテストが実施されている合理的な保証を提供する。		
根拠理由－変更管理は、業務の財務報告の目標達成をサポートするため、組織がどのようにシステムの機能を変更するかに取り組むものである。この領域に不備がある場合、財務報告に重大な影響を与える可能性がある。例えば、財務データを勘定に振り分けるプログラムを変更する際は、適切な分類と報告のインテグリティが維持されるように、変更前の適切な承認とテストが必要になる。		
統制の例	**統制のテストの例**	**COBIT4.0 の参照項目**
システムソフトの変更を含む、プログラム変更、システム変更および保守のリクエストは、標準化、ログ、承認、文書化され、正式な変更管理手続きに従っている。	文書化された変更管理プロセスが存在し、現行のプロセスを反映するように内容が維持されているかを確かめる。 プログラム変更、システムの保守、インフラの変更を含む、本番環境のすべての変更について、変更管理手続きが存在するかを検討する。 変更申請を統制し、モニターするための手続きを評価する。 変更申請は適切に開始され、承認され、追跡されているかを検討する。 プログラム変更は、職務分離が行われた、統制された環境で実施されているかを確認する。 アプリケーションまたはシステムに行われた変更のサンプルを選び、本番環境移行前に、これらが適切にテストされ、承認されたかを確かめる。オペレーション、セキュリティ、IT インフラの管理、IT の管理が承認手続きに含まれているかどうかを確かめる。 権限を与えられた/承認された変更のみが本番に移行していることを判断するために、設計された手続きを評価する。 変更のサンプルを選び、変更申請ログおよび関連資料を追跡する。 これらの手続きがシステムソフトの修正に適時に対応していることを確認する。サンプルを選び、文書化された手続きに従っているかを確認する。	AI6.1 AI6.2 AI6.4 AI6.5 AI7.3 AI7.8 AI7.9 AI7.10 AI7.11

図表 19－ 変更管理（AI6、AI7）（続き）		
統制に関する指針		
統制の例	**統制のテストの例**	**COBIT4.0 の参照項目**
緊急の変更申請は文書化された正式な変更管理手続きに従っている。	緊急な変更を管理・監督するプロセスが存在するかを確かめる。 緊急に実施されたすべての活動に対して監査証跡が存在するかを判断し、独立した者がレビューしているかを検証する。 手続で、緊急変更の根拠となる書類を必要とすることを確かめる。 緊急な変更に対し、「切り戻し処理」手続きが確立していることを確かめる。 緊急変更の実施後に、すべての変更がテストされ、標準的な変更手続きに従っていることを保証する手続きを評価する。「緊急な変更」の記載のある変更のサンプルをレビューし、必要な承認がなされているか、またある一定期間の経過後、必要だったアクセスが解除されているかを確かめる。その変更のサンプルは適切に文書化されていることを確かめる。	AI6.3 AI7.10
プログラムの本番への移行は権限を与えられた者のみに制限する統制を実施している。	プログラムの本番移行前に、必要な承認を、評価する。システム責任者、開発スタッフ、コンピュータ・オペレーションの承認を検討する。 プログラムの本番への移行の責任があるスタッフとプログラム開発スタッフとの間に、適切な職務の分離があることを確認する。この根拠となる証拠を入手し、テストする。	AI7.8
IT 統括責任者は、システムに保存されるデータとプログラムのセキュリティを危険にさらさないシステムソフトウェアを導入している。	変更がシステムソフトウェアに及ぼす潜在的な影響について、リスク評価を実施していることを確かめる。システムソフトウェアの変更が本番環境に導入される前に、開発環境でのシステムソフトウェアの変更をテストする手続きをレビューする。「切り戻し処理」手続きが存在することを確かめる。	AI6.2 AI7.4 AI7.9

図表 20－サービス・レベルの定義と管理(DS1)		
統制に関する指針		
統制目標－財務報告のシステムの要件を満たすとともに、サービスの質を測る成果水準に関する共通の理解をもたらすような方法でサービス・レベルが定義され、管理されているという合理的な保証を提供する。		
根拠理由－サービス・レベルの定義と管理のプロセスは、組織がユーザの機能上・運用上の期待にいかに応えるか、そして最終的にはビジネスの目標をいかに達成するかに取り組むものである。サービスが要求通りに実施されているかを判断するため、役割と責任が定義され、説明責任と測定モデルが用いられる。この領域に不備がある場合、企業の財務報告と開示に重大な影響を及ぼす可能性がある。例えば、システムの管理が十分に行われていない、またはシステムの機能が要求水準に達していない場合、財務情報は意図した通りに処理されていない可能性がある。		
統制の例	**統制のテストの例**	**COBIT4.0 の参照項目**
財務報告システムの要件をサポートするためにサービス・レベルを定義し、管理している。	サービス・レベル・アグリーメント（SLA）からサンプルを選び、サービス内容に関する明確な定義とユーザの期待事項をレビューする。 組織のサービス・レベルの管理に責任を持つメンバーと話し合い、サービスレベルが適切に管理されているかを判断するための証拠をテストする。 サービス・レベルがサービス・レベル・アグリーメントに従って適切に管理されている証拠を入手し、テストする。 財務報告システムは、ユーザの期待サービス・レベル・アグリーメントに従ってサポートされ、実施されているかをユーザと話し合う。	DS1.2 DS1.3 DS1.5 DS1.6
社内外でのサービス・レベル・アグリーメント（SLA）を管理する目的で、関連する成果指標を確立するためのフレームワークを定義している。	サービス・レベルに関する成果報告書を入手し、主要な成果指標が含まれていることを確認する。 成果をレビューし、問題を把握し、サービス・レベルのマネージャーがこれらの問題にどう対応しているかを評価する。	DS1.1 DS1.3

図表 21－サードパーティのサービスの管理（DS2）

統制に関する指針

統制目標－サードパーティのサービスが安全で、正確で、利用可用であり、処理のインテグリティをサポートしており、外注契約により適切に定義されているという合理的な保証を提供する。

根拠理由－サードパーティのサービスの管理は、財務アプリケーションと関連システムのサポートを目的とした、業務委託された外部委託業者の使用を含む。この領域で不備があった場合、企業の財務報告と開示に重大な影響を与える可能性がある。例えば、外部委託業者による処理の正確性に関して統制が不十分な場合、不正確な財務上の結果をもたらす危険がある。

統制の例	統制のテストの例	COBIT4.0 の参照項目
責任者がサードパーティのサービス・レベルの基準達成度を定期的にモニターし、報告する。	サードパーティのサービスの管理責任者が適切かを確認する。	DS2.2
組織の業者管理方針に沿って外部委託業者を選定する。	組織の業者管理方針を入手し、基準に準拠しているかについてサードパーティのサービス管理責任者と話し合う。 外部委託業者の選定が組織の業者管理方針に沿って行われている証拠を入手し、テストする。	PO1.4 PO6.3 DS2
外部委託業者の選定前に、IT 統括責任者が候補業者に必要なサービスの提供能力についての評価と財務上の存続性に関するレビューを行い、適格性を判断する。	外部委託業者選定にあたっての基準と事例を入手する。 これらの基準に、外部委託業者の財務上の安定性、管理下にあるシステムに関する技術と知識、および安全性、処理のインテグリティに係る統制に関する考慮が含まれているかを評価する。	DS2.3
両当事者の外部サービス契約書に、情報システムとネットワークにおけるリスク、セキュリティ統制と手続きを明記する。	サードパーティのサービス契約のサンプルを選び、企業の方針と手続きに従って、安全性および処理のインテグリティをサポートする統制が記載されているかを検討する。	DS2.3
サードパーティのサービスに関し、作業開始前に正式な契約が定義され、承認されなければならないという要件を含む手続きが存在し、これに従っている。この手続きには、内部統制の要件の定義と組織の方針および手続きを外部委託業者が受諾することが含まれる。	契約書のサンプルをレビューし、以下を検討する。 • 実施するサービスが明示されているか。 • 財務報告システムに関する統制の責任が適切に明示されているか。 • 外部委託業者が、セキュリティに関する方針と手続きなど、組織の方針と手続きに準拠することを承諾しているか。 • 作業開始前に、適切な当事者が契約をレビューし、署名しているか。 • 契約で述べられた財務報告システムとサブシステムに関する統制が、組織で求められているものと一致しているか。 ギャップが発見された場合これをレビューし、財務報告に及ぼす影響を判断するため、さらに分析する。	DS2.3
外部委託業者（サードパーティ）とのサービス・レベルの契約および関連契約について、安全性と処理のインテグリティを定期的にレビューする（例えば米国の SAS70 報告書、カナダの 5970、およ	外部委託業者（サードパーティ）がセキュリティおよび処理のインテグリティに関して、監査報告書などの独立したレビューを実施しているかを質問する。 直近のレビューのサンプルを入手し、財務報告に影響を与える統制の不備の有無を判断する。	ME2.6

図表 21－サードパーティのサービスの管理（DS2）		
統制に関する指針		
び ISA402 条）。		

図表 22－ システムセキュリティの保証（DS5）		
統制に関する指針		
統制目標－データの不正使用、開示、変更、破損または損失を防ぐために、財務報告システムおよびサブシステムの安全が適切に確保されている合理的な保証を提供する。		
根拠理由－不正アクセスを防止する物理的・論理的な統制を含むシステムセキュリティを管理する。これらの統制には一般に、承認、認証、否認防止、データの分類、およびセキュリティのモニタリングといったものがある。この領域の不備は財務報告に重大な影響を与えるおそれがある。例えば、取引承認の統制が不十分な場合、不正確な財務報告につながる可能性がある。		
統制の例	**統制のテストの例**	**COBIT4.0 の参照項目**
情報セキュリティ方針が存在し、適切なレベルの経営責任者がこれを承認している。	組織のセキュリティ方針のコピーを入手し、以下の点を考慮して有効性を評価する。 • 組織にとってのセキュリティの重要性に触れた全体的な記述があるか? • 特定の方針の目的が明確に記載されているか? • 従業員と受託業者のセキュリティに関する義務について言及されているか? • セキュリティに関する経営者の決意を示すために、適切なレベルの経営幹部が方針を承認しているか？ • すべての経営者と従業員に方針を伝達するプロセスがあるか？	PO6.3 PO6.5 DS5.2
セキュリティ方針の目的をサポートする、セキュリティ基準の枠組みが構築されている。	セキュリティ基準のコピーを入手し、基準の枠組みがセキュリティ方針の目的を効果的に満たしているかを判断する。セキュリティ基準が頻繁に述べる以下の項目を適切にカバーしているかを考慮する。 • セキュリティに関する組織構造 • 役割と責任 • 物理面・環境面のセキュリティ • オペレーティングシステムのセキュリティ • ネットワークのセキュリティ • アプリケーションのセキュリティ • データベースのセキュリティ これらの基準を伝達し、維持するためのプロセスが確立されているかを判断する。	PO8.2 DS5.2
IT 戦略計画全体に沿った IT セキュリティ計画が存在する。	財務報告システムおよびサブシステムのセキュリティ計画または戦略のコピーを入手し、企業全体の計画と関連してその妥当性を評価する。	DS5.2
IT 環境における変化ならびに特定システムのセキュリティ要件を反映するよう、IT セキュリティ計画を更新する。	セキュリティ計画が、財務報告システムおよびサブシステムに特有なセキュリティ要件を反映していることを確かめる。	DS5.2

図表 22－ システムセキュリティの保証（DS5）（続き）		
統制に関する指針		
統制の例	**統制のテストの例**	**COBIT4.0 の参照項目**
取引の実在性をサポートするため、そのシステムの全ユーザ（社内および社外）の認証手続きが存在し、これに従っている。 ☆	財務報告用システムおよびサブシステムのユーザの権限を検証するために用いる認証の仕組みを評価し、一定時間経過後に、ユーザがセッション・タイム・アウトされることを検証する。ユーザ・プロファイル（管理用プロファイルを含む）が共有されていないことを検証する。	DS5.3 AC
認証およびアクセス機能の有効性を維持するための手続きが存在し、これに従っている（例えば、定期的なパスワードの変更）。 ☆	セキュリティの実施状況をレビューし、認証統制（パスワード、ID、2 要素認証など）が適切に用いられ、共通の機密保持に関する要求事項（ID とパスワードは共有しない、英数字を組み合わせたパスワードを使用するなど）に従っていることを確かめる。	DS5.3 DS5.4
ユーザアカウントの申請、設定、発行、一時停止、削除への適時の対応に関する手続きが存在し、これに従っている（社外で開始される取引を承認するための手続きを含む）。 ☆	財務報告システムとサブシステムのユーザ登録、変更および削除が適時に行われるための手続きが存在し、これに従っていることを確かめる。 新規ユーザのサンプルを抽出し、責任者がアクセス権を承認したかどうか、そして与えられたアクセス権が、承認されたアクセス権と合致しているか検討する。 退職者のサンプルを抽出し、退職後にアクセス権が即座に削除されていることを確かめる。 アクセス権の与えられたユーザおよび現行のユーザのサンプルを抽出し、職務機能に基づいて、そのユーザのアクセス権の適切性をレビューする。	DS5.4
アクセス権を定期的にレビューし確認するための統制プロセスが存在し、これに従っている。 ☆	財務報告システムとサブシステムのアクセスコントロールを責任者が定期的に見直しているかを質問する。 例外事項が適切に再検討されているか、対処されているかを検討する。	DS5.4
必要に応じて双方の当事者はいずれも取引を否定できないような統制が存在し、取引の発送または受領の否認防止、発送と受領の証拠を提供するための統制が実施されている。	取引の開始と承認に関して、組織がどのように説明責任を確立しているかを確かめる。 ユーザが権限のない取引の入力を試みる現場に立ち会い、どのように説明責任に関する統制が行われるかのテストを行う。 取引のサンプルを抽出し、説明責任または取引開始の証拠を確かめる。	DS11.6 AC AC

図表 22－ システムセキュリティの保証（DS5）（続き）		
統制に関する指針		
統制の例	**統制のテストの例**	**COBIT4.0 の参照項目**
ファイアウォール、侵入の検知、脆弱性の評価を含む適切な統制が存在し、公共のネットワークを通じた不正アクセスを防ぐためにこれらが用いられている。	ファイアウォールや侵入検知システムを含む周辺セキュリティの統制が十分で適切であることを確かめる。 過去一年間に、経営者が倫理的なハッキングやソーシャルエンジニアリングなどの統制に関して独立した第三者による評価を実施したかを質問する。 この評価に関する報告書のコピーを入手し、把握された欠陥の対応に関する適切性を含む結果をレビューする。 ウイルス防止システムが、財務報告システムとサブシステムのインテグリティとセキュリティを保護するために用いられているかを検討する。 適切な場合、あるシステムから別のシステムに送られる財務情報の機密性を確保するため、暗号技術が用いられているかを検討する。	DS5.10
IT セキュリティ管理部門は、オペレーティングシステム、アプリケーションおよびデータベースレベルにおけるセキュリティ行為のモニタリングと記録を行い、把握したセキュリティ違反を経営幹部に報告する。	アプリケーションとデータベースレベルにおけるセキュリティの脆弱性と関連する警戒すべき事象をモニターするため、セキュリティ部門が存在しているかを質問する。 過去一年間に起きたこのような事象の性質と範囲を評価し、財務報告システムとサブシステムの不正アクセスや操作にどのような統制をもって対応したかについて責任者と話し合う。 財務報告システムとサブシステムへの不正アクセスの試みが記録され、適時に調査が実施されていることを検証する。	DS5.5
システムとデータへのアクセス権の申請と承認について、適切な職務分離に関する統制が存在し、これに従っている。	システムとデータへのアクセス権の申請および承認プロセスをレビューし、同じ人物がこれらの行為を行っていないことを確かめる。	DS5.3 DS5.4
施設へのアクセスは、権限のある者に制限され、適切な本人確認と認証を必要とする。	施設のセキュリティ、鍵、およびカードリーダー・アクセスに関する方針と手続きを入手し、これらの手続きが適切な本人確認と認証をしているかを検証する。 企業の施設の出入りを観察し、アクセスが適切にコントロールされていることを確かめる。 ユーザのサンプルを抽出し、職務に基づいた適切なアクセス権が与えられているかを検討する。	DS12.2 DS12.3

図表 23－構成管理（DS9）		
統制に関する指針		
統制目標－セキュリティおよび処理に関連するすべての IT 構成要素が十分に保護されており、これが不正な変更をすべて防止するとともに、現在の構成の検証と記録をサポートするという合理的な保証を提供する。		
根拠理由－構成管理は、セキュリティおよび処理のインテグリティに関する統制がシステムに設定され、ライフサイクルを通じて保守される手続きを含んでいる。構成の管理が不十分な場合、セキュリティの問題につながり、システムとデータへの不正アクセスを許し、財務報告に影響を及ぼす危険性がある。新たな潜在的リスクは、システム変更を行う際の構成の管理が十分でない、または不正なシステムの構成要素を導入することにより、データのインテグリティが損なわれることである。		
統制の例	**統制のテストの例**	**COBIT4.0 の参照項目**
企業の IT 資産を使用する従業員に、許可されたソフトウェア以外の使用を禁止する。	無許可のソフトウェアの使用を発見し、防止するための手続きが実施されているかを検討する。また、企業の方針を入手し、ソフトウェアの使用に関して明確な記述があるかをレビューする。 アプリケーションとコンピュータのサンプルをレビューし、それらが組織の方針と適合しているか検討する。	DS9.2
不正アクセスを防止するため、ファイアウォール、ルータ、スウィッチ、ネットワーク・オペレーティングシステム、サーバ、その他関連装置を含むシステムのインフラが適切に設定されている。	組織の方針として、現在の構成およびセキュリティ構成の設定を文書化することが要求されているかを確かめる。 サーバ、ファイアウォール、ルータなどのサンプルをレビューし、組織の方針に従ってそれらが設定されているかを検討する。	DS5.3 DS5.4 DS5.10
データの表示、追加、変更または削除といった個人の明確な必要性に基づき、アクセスを提供するためにアプリケーションソフトとデータ格納システムが適切に設定されている。 ☆	構成の記録について責任者のレビューの頻度と適時性を評価する。 責任者が構成管理手続きに関する文書化を行なっているかを評価する。 構成の変更、追加または削除についてサンプルをレビューし、明確な必要性に基づき適切に承認されているかを検討する。	DS5.4
IT 統括責任者は組織全体でコンピュータウイルスから情報システムと技術を守るための手続きを確立している。	コンピュータウイルスの検出を行なう、組織の手続きをレビューする。 ネットワークとパーソナルコンピュータにウイルス対策ソフトウェアをインストールして使用していることを確かめる。	DS5.9
ソフトウェアとネットワークインフラが適切に設定されることを確認するため、定期的にテストと評価を実施する。	ソフトウェアとネットワークインフラストラクチャをレビューし、組織の文書化された手続きに従って、適切に設定、維持されていることを立証する。	AI3.2 AI3.3

図表 24 – 問題とインシデントの管理（DS8、DS10）		
統制に関する指針		
統制目標ー問題または障害が適切に対応され、記録され、解決され、または適切な解決に向けて調査が行われている合理的な保証を提供する。		
根拠理由ー問題とインシデント（障害）の管理プロセスは、組織が通常のオペレーションの枠を超えた事象をいかに把握し、文書化し、これに対応するかに取り組むものだ。この領域に不備がある場合、財務報告に重大な影響を及ぼす可能性がある。		
統制の例	**統制のテストの例**	**COBIT4.0 の参照項目**
IT 統括責任者は、データのインテグリティおよびアクセスコントロールの障害が適時に記録され、分析され、解決され、管理者に報告されるような障害および問題管理システムを定義・導入している。 ★	障害管理システムが存在するか、そしてそれがどのように用いられているかを判断する。システムがどのように用いられるべきかについての管理者による文書化をレビューする。 障害報告書のサンプルをレビューし、問題が適時に対応（記録、分析または解決）されたかを検討する。	DS8
問題管理システムは適切な監査証跡機能を提供しており、これにより障害から根本の原因を辿ることが可能となる。	組織の手続きが監査証跡機能、つまり問題または障害の追跡を含んでいるかを確かめる。 適切な監査証跡が存在し、用いられているかを検討するため、問題管理システムに記録された問題のサンプルをレビューする。	DS10.2
適時の対応と未承認の行為に関する調査をサポートするため、セキュリティインシデントの対応プロセスが存在する。	未承認の行為が適時に対応され、適切な処置をサポートするためのプロセスが存在することを確認する。	DS5.6 DS8.3 DS10.1 DS10.3

図表 25－ データ管理（DS11）		
統制に関する指針		
統制目標－記録・処理・報告されたデータが、更新および保存プロセスを通じ、完全で、正確で正当であり続ける合理的な保証を提供する。		
根拠理由－データ管理は情報の完全性、正確性、承認、実在性を含む、情報のインテグリティをサポートするために用いられる統制と手続きを含む。統制は、財務情報の開始、記録、処理、報告をサポートするために設計される。この領域に不備がある場合、財務報告に重大な影響を及ぼす。例えば、取引の開始に関する適切な承認の統制がない場合、これにより生じる財務情報は信頼できない可能性がある。		
統制の例	**統制のテストの例**	**COBIT4.0 の参照項目**
データおよび報告用出力の配布、保存に関する方針と手続きが存在する。	データおよび報告用出力の配布、保存に関する方針と手続きをレビューする。この方針と手続きが、データを保護し、正確な財務報告書（電子版の報告書を含む）を適切な従業員に適時に配布するために適切であるかどうかを検討する。 データ保護と財務報告書（電子版の報告書を含む）の適切な従業員への適時な配布に関する統制が効果的に運用されている証拠を入手し、テストする。	DS11.1 DS11.2 DS11.6
管理者は保管中または転送中の機密情報を不正なアクセスまたは修正から論理的、物理的に保護している。	セキュリティのテスト結果をレビューする。保管中または転送中の機密情報を不正なアクセスまたは修正から論理的、物理的に保護するための適切な統制があるかどうかを確かめる。	DS11.6
書類、データ、プログラム、報告書、メッセージ（送受信）、ならびに暗号化と認証に用いられたデータ（暗号キー、電子証明書）の保存期間と保存条件が定義されている。	データの配布と保存手続きを入手する。 その手続きが、書類、データ、プログラム、報告書、メッセージ（送受信）、ならびに暗号化と認証に用いられたデータ（暗号キー、電子証明書）の保存期間と保存条件を定義していることを確認する。 これらの保存期間が企業改革法に沿っていることを確かめる。 以前アーカイブに格納したデータ類の保存期間が企業改革法に準拠していることを確認する。アーカイブに格納したデータ類のサンプルを選び、同法の要件に従ってアーカイブに格納されている証拠をテストする。	DS11.2
管理者はデータとプログラムの定期的なバックアップのための戦略を実行している。 ★	組織に IT およびユーザ要件に基づいてデータとプログラムをバックアップするための手続きがあるかを判断する。データファイルとプログラムのサンプルを選び、必要に応じてこれらのバックアップがとられているかを確かめる。	DS11.5

図表 25－ データ管理（DS11）（続き）		
統制に関する指針		
統制の例	**統制のテストの例**	**COBIT4.0 の参照項目**
情報の保存が定期的にテストされている。 	メッセージ、書類、プログラムなどの保存と保管が過去 1 年の間にテストされたことがあるかを質問する。 テストの結果を入手し、レビューする。 不備が発見されたかどうか、そしてこれらが再調査されたかどうかを立証する。組織のアクセスセキュリティ方針を入手し、機密性の高いバックアップデータを取扱う基準と指針を守っているかを責任者と話し合う。	DS11.5
データ構造の変更は、適時に権限が与えられ、設計仕様書に沿って行われ、実施されている。	データ構造変更のサンプルを入手し、それらが設計仕様書に沿っているかどうか、必要な時間内に導入されたかを確かめる。	AI6

図表 26 – オペレーション管理（DS13）		
統制に関する指針		
統制目標–承認されたプログラムが計画通り実行され、予定された処理の逸脱が把握され、調査される合理的な保証を提供する。この中にはジョブ・スケジューリング、処理、エラーのモニタリングに関する統制が含まれる。		
根拠理由 – 運用管理は、企業が財務情報を開始、記録、処理、報告するためのサポートを行う上で、信頼できるアプリケーションシステムをいかに保守管理するかに取り組むものである。この領域に不備がある場合、企業の財務報告に大きな影響を及ぼす可能性がある。例えば、アプリケーションシステムが中断した場合、組織は取引の記録ができなくなり、これによって、取引記録のインテグリティが損なわれる可能性がある。		
統制の例	**統制のテストの例**	**COBIT4.0 の参照項目**
経営者は、ジョブ・スケジューリング、モニタリング、ならびにセキュリティ、処理のインテグリティに関する事象への対応を含む IT オペレーションの標準的な手続きを確立、文書化し、これに従っている。	経営者が IT オペレーションの手続きを文書化しているかどうか、そして遵守のためにオペレーションを定期的にレビューしているかを確認する。 事象のサンプルをレビューし、対応の手続きが有効に行われているかを確認する。手続きを用いる場合、全てのジョブが実施されたことをモニターするために実施されているジョブ・スケジューリング・プロセスとその手続きをレビューする。	DS13.1 DS13.2
システムイベントデータは、システムとデータ処理のレビュー、調査、再構築を可能にするため、時系列の情報とログを提供するよう適切に保存される。	十分な時系列の情報がログに記録され、保存されているか、必要な場合に再構築に利用できるかどうかを確かめる。再構築が十分可能かを判断するため、ログ項目のサンプルを入手する。	DS13.3
システムイベントデータは、システムとデータ処理の完全性と適時性に関して合理的な保証を提供するために設計されている。	システムとデータ処理の完全性と適時性を判断するため、管理者が用いる情報の種類を質問する。 処理の完全性と適時性を確認するため、システム処理イベントデータのサンプルをレビューする。	DS11.1 DS13.3

図表 27 – エンドユーザ・コンピューティング	
統制に関する指針	
エンドユーザ・コンピューティングに関する以下の統制の例は、**図表 15 から 26** の統制指針から抜粋したものであり、代表的なエンドユーザ・コンピューティング環境の特徴に対応するために提示したものである。適切な COBIT プロセスがエンドユーザ・コンピューティングに適用される。	
統制の例	**統制のテストの例**
セキュリティおよび処理のインテグリティに関するエンドユーザ・コンピューティングの方針と手続きが存在し、これに従っている。 ☆	エンドユーザ・コンピューティングに関する方針と手続きを入手し、これらがセキュリティおよび処理のインテグリティに関する統制に対応していることを確かめる。 ユーザのサンプルを選び、エンドユーザ・コンピューティングの方針を認識しているか、これに従っているかを質問する。
スプレッドシートおよびユーザが開発した他のプログラムを含む、エンドユーザ・コンピューティングが文書化されており、正確なソート、要約、正確な報告能力を含む処理のインテグリティが定期的にレビューされている。 ☆	企業中で用いられているエンドユーザのプログラムに関する経営者の知識について質問する。 処理のインテグリティについてエンドユーザのプログラムをレビューする頻度と、その際に取った手法について質問する。そして、サンプルをレビューし、プログラム・レビューの有効性を確かめる。 ユーザが開発したシステムをレビューし、管理者の意図に従って、ソート、要約、報告する能力をテストする。
ユーザが開発したシステムとデータは、定期的にバックアップをとり、安全な領域に保存する。 ☆	エンドユーザ・システムのバックアップをとる方法と保存場所を質問する。
スプレッドシートや他のエンドユーザ・プログラムなどの、ユーザが開発したシステムは、不正使用から保護されている。 ☆	ユーザが開発したシステムへの不正アクセスを防ぐために用いるセキュリティをレビューする。 ユーザが開発したシステムへの不正アクセスをユーザが試みるところを観察することを検討する。 管理者がどのように不正アクセスを発見できるか、こうした不正アクセスの影響を評価するためにどのようなフォローアップの手続きがとられているかを質問する。 ユーザが開発したシステムのサンプルを選び、誰にアクセス権があるか、そのアクセスが適切であるかを確かめる。
ユーザが開発したシステムへの入力、処理、出力は、完全性と正確性について独自に検証されている。 ☆	管理者がどのように、ユーザが開発したシステムから処理、報告された情報の正確性と完全性を検証しているかを質問する。 後続処理または最終報告書を目的として提出される前に、ユーザ開発によるシステムからの出力を誰がレビューし、承認しているかを質問する。 ユーザ開発システムで用いたロジックを再実行、またはレビューすることを検討し、完全で正確な処理能力に関する結論を出す。

参考資料 D ― 業務処理統制（アプリケーション統制）

業務処理統制の重要性

複雑で、IT に依存する財務報告環境においては、評価作業を実施する際、多くの企業が業務処理統制に依然として十分な注意を払っていない。PCAOB はこの領域の重要性を強調しており、これらの統制を適切に検討していない企業は、企業改革法を遵守できないリスクにさらされる可能性がある。

企業は、財務報告システムについて何ら問題を経験したことがない、または過去のある時点でのテストの信頼度が十分に高いという理由により、自社の財務報告システムは信頼できると思い込んでいることが極めて多い。その他の場合には、企業は「ブラックボックス」的なアプローチを取り、マニュアル統制を全面的に信頼し、そのシステム内に存在するリスクを考慮できなくなっている。どちらの場合にも問題なのは、過度な信頼をシステムに寄せている、すなわち、企業はシステムがどのように財務報告目的をサポートしているかを理解せずに、システムに依存しているという点である。これは、内部統制における重要な欠陥につながる深刻な見落としと言える。

これに対応して、多くの企業が、システムがどのように財務報告プロセスをサポートしているかを理解するために、関連するアプリケーションを検討し始めている。その中で、「ベースライニング」またはベンチマーキングと呼ばれるプロセスを通じて、アプリケーションによる処理のインテグリティを文書化している。

業務処理統制の実ケース

業務プロセスレベルでは、統制は、財務目的を達成するための特定の業務活動に用いられる。ほとんどの業務プロセスはコンピュータ化され、IT アプリケーションシステムに統合されており、その結果、このレベルでの統制の多くもまたコンピュータ化されている。これらの統制は、自動化された業務処理統制として知られている。

自動化された業務処理統制は、それらがサポートする業務プロセスにのみ用いられる。これらは、不正取引を予防または発見し、取引の網羅性、正確性、承認、正当性を含む財務報告目的をサポートするため、アプリケーション内で設計された統制である。統制の把握および文書化を始める前に、用いるべき統制の種類を慎重に考慮する必要がある。

どの統制を文書化する必要があるかを決定する際、各統制の特徴を理解することが大切である。一般に、統制には 3 つの種類がある。

- マニュアル統制 ― アプリケーションまたは他の IT システムによる支援なしに実施される。例えば、上司の監督、小切手上の署名といった書面による承認、注文書と商品受領書の照合といった手作業などである。マニュアル統制は人為的エラーのリスクを伴いやすく、したがって、信頼性が低いとみなされることが多い。
- 自動化された統制 ― コンピュータが実施するもので、性質上、二進法であり、常に設計された通りに機能し、断続的エラーの影響を受けにくい。例えば、受注数を検証する入力エディット・チェック、またはあらかじめ設定された上限までの注文しか許可しない自動購入システムの構成による統制などである。その他の例を以下に挙げる。
  - 照合による統制活動 ― 手作業または自動的に読み込んだ金額を合計金額と照合することにより、データ入力エラーを検出するコントロール。例として、企業はオンラインによる受注

入力システムが処理し受け渡した取引合計数を、請求システムが受け取った取引数と照合することが挙げられる。
  - チェックディジット － データを検証するための計算。例えば、ある企業は業者からの不正確な発注を発見し、修正するため、チェックディジットを部品番号に含めている。統一商品コードには製品と業者を検証するためのチェックディジットが含まれている。
  - あらかじめ定義されたデータリスト － 許容できるデータをあらかじめ定義して作成したリストをユーザに提供する統制。例えば、ある企業のイントラネット・サイトは購入可能な製品のドロップダウンリストを載せている。
  - データの妥当性テスト － 読み込まれたデータを現在または過去の妥当性のパターンと比較するテスト。例えば、住宅改築の小売店が業者に極めて大量の木材を発注した場合、レビューの対象となる。
  - ロジックテスト － 上限または金額/英数字のテストの使用を含むテスト。例えば、クレジットカード番号にはあらかじめ決められた形式がある。
  - 計算 － アプリケーション内で設定され、自動化された処理ルーチンにより実行される数字操作。
- IT 依存マニュアル統制（複合型） － 基本的にマニュアルおよび自動化された統制の組み合わせである。システムが作成する報告書は経営者のレビューのためのデータを提供するため、複合型の統制に見ることができる。例えば、売掛金の評価は、受取勘定の責任者がその妥当性について月次の滞留売掛金報告書をレビューする統制を含む可能性がある。この場合、報告書が売上債権のシステムから作成され（自動化されたプロセス）、妥当性についてレビューされる（マニュアルプロセス）。その結果、自動化されたプロセス（報告書の作成）とマニュアルのプロセス（責任者によるレビュー）の双方が売掛金の評価を裏付ける必要がある。

業務処理統制の投資対効果

マニュアル統制および自動化された統制には、長所と短所がある。複雑でない小規模な企業では、マニュアル統制を文書化し、その証拠を集めることが容易な場合もある。しかし、複雑な大企業では、マニュアル統制の文書化は極めて費用がかさむ作業となる。大規模で複雑な企業にとっては、オペレーションの頻度に基づいてテストが必要なマニュアル統制に比べれば、テストの必要が一度しかない、自動化された統制の文書化とテストに関わる作業の方が、長期的には好ましいのである。マニュアル統制のサンプルサイズは実施頻度によって異なる一方、自動化された統制のサンプルサイズは変化しない。これは、企業にとっては結局、非常に大きな節約につながる。例えば企業改革法の遵守プログラムを目的として、500 の統制を把握する必要があり、マニュアルまたは自動化された統制のどちらを文書化すべきかを検討中の企業を考えてみよう。**図表 28** は、その分析をサポートするために作成されたものである。

図表 28—マニュアル統制および自動化された統制のアプローチの比較

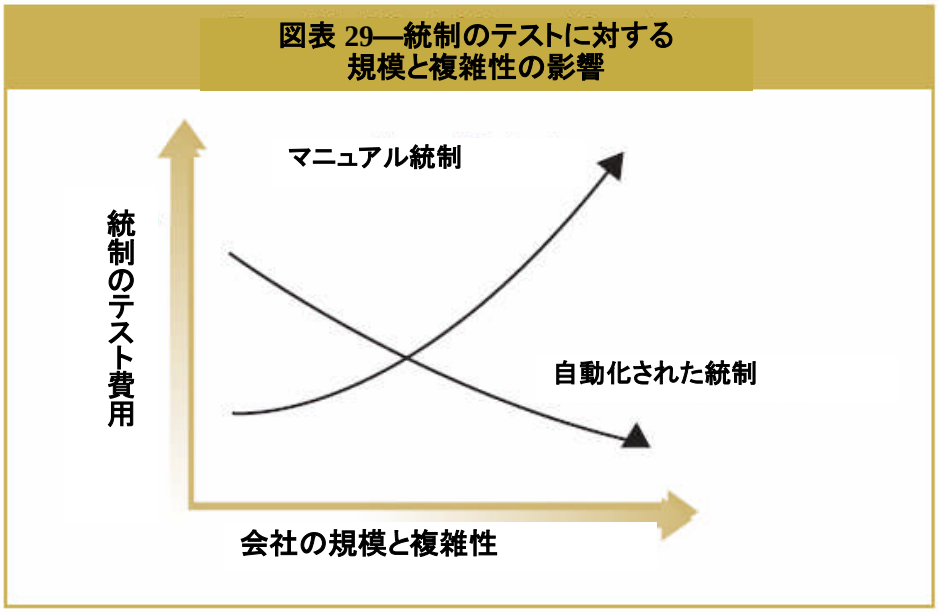
マニュアル統制のアプローチ		**自動化された統制のアプローチ**	
総統制数	500	総統制数	500
統制ごとの文書化所要時間	1 時間	統制ごとの文書化所要時間	3 時間
文書化総所要時間	500 時間	文書化総所要時間	1,500 時間
統制ごとの平均サンプルサイズ	10	統制ごとの平均サンプルサイズ	1
テストされるサンプル項目総数	5,000	テストされるサンプル項目総数	500
サンプルごとのテスト所要時間	30 分	サンプルごとのテスト所要時間	30 分
テスト総所要時間	2,500 時間	テスト総所要時間	250 時間
総所要時間	**3,000 時間**	**総所要時間**	**1,750 時間**

この例では、いくつか留意する点がある。第一に、マニュアル統制の文書化に当初必要とされる作業時間は、自動化された統制に比べて少ない。これは主に、IT システムの複雑性とそのアプリケーションがどのように稼動しているかを理解する必要性による。第二に、マニュアル統制のテストに要する作業時間は、自動化された統制のテストに要する時間よりも多い。これは、自動化された統制が設計された通りに稼動するものであり、IT 統制（プログラム開発、プログラム変更、プログラムおよびデータへのアクセス、コンピュータ・オペレーション）が信頼できるものであれば、テストは一度ですむという事実による。

しかし、「同じ統制の利用」が 5 年に及ぶ場合、その影響はより大きくなる。この例では、初年度の節約時間は 1,250 時間であるが、2 年後以降、企業が統制の再テストのみを必要とする場合、年間の節約時間は 2,250 時間に増加する。したがって、5 年間では、企業が自動化された統制を文書化し、テストすることを選択していれば、10,250 時間を節約できることになる。**図表 29** は、企業の規模と複雑性が作業時間にどのように影響を与えるか、したがって、マニュアル統制対自動化された統制の文書化およびテストの費用を示したものである。

自動化された統制が一般的に、より信頼度が高いと考えるならば、このアプローチの利点は大きな説得力を持つ。

図表 29—統制のテストに対する規模と複雑性の影響



アプリケーションのベンチマークの設定

アプリケーションのベンチマークの設定は、統制の設計上・運用上の有効性を確認するため、財務諸表をサポートする財務アプリケーション内に組み込まれた関連する統制の文書化およびテストを伴う。これらの統制を把握し、テストを実施すれば、これらはベンチマーク化するのに適したものとなる。基本的に、以下で説明する特定の条件を満たしている限り、テスト頻度の削減が可能になる。

アプリケーションのベンチマークを設定する（アプリケーションがどのように稼動するのかを理解し、その処理に係る関連統制を文書化するなど）ために必要な追加費用がある一方で、その利点も極めて説得力がある。**図表 28** にも述べたように、テスト作業の削減だけをとっても、確実な投資対効果が生

じる。しかし、以下のような他の利点もある。

- 次章でさらに説明するように、特定の状況が存在する限り、業務処理統制は人為的な誤りに影響されず、通常設計通りに運用されるため毎年テストを受けなくてもよく、テストをさらに削減することができる。
- 業務処理統制は概して予防的統制であり、マニュアル統制よりも確実なため、信頼性が増す。業務処理統制は、財務統制目的のみならず、多くが不正防止目的をサポートするため、二重目的の統制として機能することが多い。

アプリケーションのベンチマーキングは、2004 年 11 月に PCAOB が公表した指針で、特に以下のような特定の条件が満たされた場合、好ましいプラクティスであると述べられている。

- 業務処理統制をサポートするアプリケーションの関連部分が把握されている（例えば、自動的な勘定科目の経年変化をサポートする売掛金モジュールまたは完全で正確な在庫管理表の作成をサポートする在庫管理モジュール）。
- 関連するアプリケーションが適切に設計されている。
- 関連するアプリケーションが当該年度に変更されていない。
- 直近の業務処理統制のテストにより、運用上の有効性を確認している。
- サポートを行う関連する IT 全般統制、特にアプリケーションをサポートするアクセスコントロールおよび変更統制は、適切に設計され、有効に運用されている。

自動化された業務処理統制の例

自動化された統制のアプローチを採用する企業を支援するために、自動化された統制の例を**図表 31-38** に示した。ほとんどの場合、これらの統制は、内蔵の業務処理統制機能を用いることで可能となる。こうした機能は通常、SAP、ピープルソフト、オラクル、JD エドワーズ、その他の統合 ERP 環境でみられる。この機能がない環境では、こうした統制目的を満たすためのマニュアル統制および自動化された統制の手続きを組み合わせることが必要となる。

図表 31-38 の統制目的は完全なリストというわけではないが、業務処理統制によって通常可能となる統制の例である。企業は特定の業界と運用環境に基づいて新たにどのような統制目標が必要になるかを考慮する必要がある。

図表 31-38 は網羅性、正確性、評価および承認の統制を含む、財務諸表のアサーション（適切な財務情報を作成するための要件）に寄与するアプリケーションと業務プロセスに及ぶ統制について述べたものである。これらの財務諸表のアサーションの定義といくつかの例を**図表 30** にまとめた。

図表 30 – 財務諸表のアサーションの定義と例		
財務諸表のアサーション	**定義**	**例**
実在性	実在性または発生に関するアサーションは、ある一定の時期に企業の資産または負債が存在するかどうか、そして記録されている取引がその期間に実際に発生しているかどうかを言う。	経営者は、貸借対照表上の製品の棚卸資産が売却可能であることを主張している。同様に、経営者は損益計算書上の売上が現金または他の対価による財またはサービスとの交換を表していることを主張している。
網羅性	網羅性に関するアサーションは、財務諸表で提示されるすべての取引と勘定科目が含まれているかどうかを言う。	経営者はすべての財とサービスの購入は記録され、財務諸表上に含まれていると主張している。同様に、経営者は貸借対照表上の支払手形は企業のこうした債務のすべてを含んでいることを主張している。
評価	評価または分配に関するアサーションは、資産、負債、資本、収益および費用が適切な金額で財務諸表に含まれているかどうかを言う。	経営者は、固定資産は取得原価で記録されており、この取得原価は適切な会計期間にわたって体系的に分配されていると主張している。同様に、経営者は、貸借対照表に含まれる売掛金は正味実現可能価額で表示されていることを主張している。アサーションは適切に分類され、表示されている。

図表 31 – 決算における業務処理統制の目標	
統制目標の例	**財務諸表のアサーション**
決算プロセスにおける取引の記入は完全かつ正確である。	網羅性 実在性
自動化された減価償却の時期、期間、方法は適切かつ正確である。	評価 実在性
転記のエラー/貸借不均衡な仕訳の把握に用いるため、差異分析報告が作成されている。	網羅性 実在性 評価
補助元帳システムから出力された標準的で経常的な期末の仕訳記入は、自動化され、適切な承認を受け、正確に記入されている。	網羅性 実在性 評価
システムはすべての経常および非経常の仕訳入力に関する報告書を生成する。	網羅性 実在性
すべての標準外の仕訳入力は追跡されており、適切である。	網羅性 実在性
勘定科目コードおよび取引金額は正確かつ完全であり、例外事項が報告されている。	網羅性 実在性
総勘定元帳残高は、補助元帳残高と照合されている。	網羅性 実在性
記録された金額は予測金額と自動的に比較されている。	網羅性 実在性
貸借が不均衡な記入は禁じられている。	網羅性 実在性
標準的な企業間取引を含む全社連結は、第三者のソフトウェア製品を用いて自動化/実施されている。	網羅性 実在性 評価
システムの機能は、転記と承認の機能を分離している。	実在性
総勘定元帳記録へのアクセスは適切で、承認されている。	網羅性 実在性 評価
取引は決算締めのスケジュール期間外には記録することができない。	網羅性 実在性 評価
毎年承認を受けている経常的な発生取引は適切な期間内に正確に記帳されている。	網羅性 実在性 評価
資産の消却を承認するためのシステム統制が機能している。	実在性
相互に関連する貸借対照表と損益計算書の勘定科目は、自動照合を受けている。	網羅性 実在性
すべての記入の根拠は容易に把握可能である。	実在性
データに例外事項がある場合、拒否または許可された取引は、例外事項報告書上で把握される。	網羅性 実在性
勘定科目のマッピングは更新されている。	実在性

図表 32 – 総勘定元帳における業務処理統制の目標	
統制目標の例	**財務諸表のアサーション**
総勘定元帳の仕訳へのアクセスは適切で、承認されている。	網羅性 実在性 評価
総勘定元帳の残高は補助元帳の残高と照合され、こうした照合は管理職にある者が正確性をレビューし、承認している。	網羅性 実在性
相互に関連する貸借対照表と損益計算書の勘定科目は、正確性を確認するために自動照合を受けている。	網羅性 実在性
正確性について経営者のレビューを受けるために、システムはすべての経常および非経常の仕訳入力に関する報告書を生成する。	網羅性 実在性
システムの機能は、転記と承認の機能を分離している。	実在性
すべての標準外の仕訳入力は追跡されており、適切である。	網羅性 実在性
勘定科目コードおよび取引金額は正確かつ完全であり、例外事項が報告されている。	網羅性 実在性
記録された金額は、入力の正確性を確認するため、予測金額と自動的に比較されている。	網羅性 実在性
貸借が不均衡な記入は禁じられている。	網羅性 実在性
標準的な企業間取引を含む全社連結は、自動化/実施されている。	網羅性 実在性 評価
転記のエラー/貸借不均衡な仕訳の把握に用いるため、差異分析報告が作成されている。	網羅性 実在性 評価
資産の消却を適切に承認するためのシステム統制が機能している。	実在性
当該月に総勘定元帳に転記された例外的な金額の仕訳入力はシステムが警告を与え、その後、月末以降にコントローラーまたは CFO が正確性をレビューし、承認する。	網羅性 実在性 評価
決算プロセスの一部として完了したすべての仕訳入力に関する報告書は、記録された仕訳の完全性および適切性の確認のため、経営者がレビューする。	網羅性 実在性
総勘定元帳マスターファイルの変更報告書がシステムにより作成され、必要に応じ、その変更の入力を行っていない者がこれをレビューする。	網羅性 実在性
実績対実績、実績対予算および収益報告書が、総勘定元帳の最終の締め以前に毎月総勘定元帳システムにより作成される。これらの報告書はコントローラーおよび CFO に配布され、レビューされる。異常な金額または差異は調査され、必要な場合、組み替えられる。	網羅性 実在性 評価
標準的な勘定科目一覧表は経営者によって承認され、全社で活用されている。総勘定元帳への追加または削除は、権限のある経理部担当者によってのみ行われるよう制限されている。	網羅性 実在性
適時のフォローアップおよび未決項目の解消をモニターするため、長期経過項目（例えば、90 日以上未払いとなっている調整項目）の報告書がシステムにより生成される。	網羅性 実在性

図表 32 – 総勘定元帳における業務処理統制の目標（続き）	
統制目標の例	**財務諸表のアサーション**
決算プロセスにおける取引の記入は完全かつ正確である。	網羅性 実在性
自動化された減価償却の時期、期間、方法は適切かつ正確である。	評価 実在性
補助元帳システムから出力された標準的、経常的な期末の仕訳入力は、自動化され、適切な承認を受け、正確に記入されている。	網羅性 実在性 評価
取引は決算締めのスケジュール期間外は記録することができない。	網羅性 実在性 評価
毎年承認を受けている経常的な発生取引は適切な期間内に正確に記帳されている。	網羅性 実在性 評価
すべての入力の根拠は容易に把握可能である。	実在性
データに例外事項がある場合、拒否または許可された取引は、例外事項報告書上で把握される。	網羅性 実在性
勘定科目のマッピングは更新されている。	実在性

図表 33 – 販売における業務処理統制の目標	
統制目標の例	**財務諸表のアサーション**
承認された顧客の信用限度額以内でのみ注文を処理する。	評価
販売価格と販売条件に関し、経営者が受注を承認する。	実在性
受注と受注の取消が正確に入力される。	評価
受注入力データは出荷および請求書の発送に至るまで、完全に、正確に転送される。	評価 網羅性
顧客からの受注はすべて入力され、処理される。	網羅性
正当な注文のみが入力され、処理される。	実在性
承認された条件と価格を用いて請求書が作成される。	評価
請求書は正確に計算され、記録される。	評価
貸方票と売掛金の修正伝票は正確に計算され、記録される。	評価
出荷された全商品の請求書が作成される。	網羅性
企業の方針に従って、すべての返品された商品と売掛金の修正に対して貸方票が発行される。	実在性
請求書は正当な出荷と関連している。	実在性
すべての貸方票は返品またはその他の正当な修正に関連している。	網羅性
すべての発行された請求書が記録される。	網羅性
発行されたすべての貸方票が記録される。	実在性
請求書は適切な時期に記録される。	評価
発行された貸方票は適切な時期に記録される。	評価
金額を受領した時期に入金が記録される。	評価
処理の正確性を目的として入金データが入力される。	評価
すべての入金データが処理のために入力される。	実在性
入金データは正当であり、処理のため一度限り入力されている。	網羅性
現金割引は正確に計算され、記録される。	評価
売掛金のタイムリーな徴収がモニターされる。	評価

図表 33 – 販売における業務処理統制の目標（続き）	
統制目標の例	**財務諸表のアサーション**
顧客マスターファイルが維持管理されている。	網羅性 実在性
顧客マスターファイルには正当な変更のみが行われる。	網羅性 実在性
顧客マスターファイルのすべての正当な変更が入力され、処理されている。	網羅性 実在性
顧客マスターファイルの変更は正確である。	評価
顧客マスターファイルの変更は適時に処理されている。	網羅性 実在性
顧客マスターファイルのデータは最新の状態を維持している。	網羅性 実在性

図表 34 – 購買における業務処理統制の目標	
統制目標の例	**財務諸表のアサーション**
承認された購入依頼書についてのみ発注が行われる。	実在性
注文書は正確に記入されている。	評価
発行されたすべての注文書が、入力され、処理されている。	網羅性
買掛金に転記された金額は受領した商品またはサービスを表している。	実在性
買掛金の金額は正確に計算され、記録される。	評価
受領した商品またはサービスの全金額が入力され、買掛金として処理される。	網羅性
受領した商品またはサービスの金額は適切な期間に記録される。	評価
正当な理由に基づく場合にのみ、買掛金が修正される。	網羅性 実在性
貸方票と他の修正伝票は正確に計算され、記録される。	評価
すべての正当な貸方票と買掛金に関連する他の修正が入力され、処理される。	網羅性 実在性
貸方票と他の修正伝票は適切な時期に記録される。	評価
受領した商品とサービスにのみ、支払が行われる。	実在性
適切な仕入先に対して支払が行われる。	実在性
支払は正確に計算され、記録される。	評価
すべての支払が記録される。	網羅性

図表 34 – 購買における業務処理統制の目標（続き）	
統制目標の例	**財務諸表のアサーション**
支払が行われる期間に支払が記録される。	評価
仕入先マスターファイルには正当な変更のみが行われる。	網羅性 実在性
仕入先マスターファイルのすべての正当な変更が入力され、処理される。	網羅性 実在性
仕入先マスターファイルの変更は正確である。	評価
仕入先マスターファイルの変更は適時に処理される。	網羅性 実在性
仕入先マスターファイル・データは最新の状態を維持する。	網羅性 実在性

図表 35 – 棚卸資産に関する業務処理統制の目標	
統制目標の例	**財務諸表のアサーション**
棚卸資産の価格または数量に関する修正は、直ちに、適切な時期に記録される。	実在性 網羅性 評価
棚卸資産の価格または数量に関する修正は正確に記録される。	評価
正当な注文書がある場合に限り、原材料が受理される。	実在性
受領された原材料は正確に記録される。	評価
すべての受領された原材料は記録されている。	網羅性
原材料の受領は速やかに、適切な時期に記録される。	評価
欠陥のある原材料は仕入先に速やかに返品される。	実在性
原材料から製造への振替は、すべて正確に、適切な期間に記録される。	評価 網羅性
製造に関連するすべての直接・間接経費は、正確に、適切な期間に記録される。	評価
完成した製品の製品在庫への振替はすべて、適切な期間に完全に正確に記録される。	評価 網羅性
顧客が返品した製品は、適切な期間に完全に、正確に記録される。	評価 網羅性
製造過程から受領した製品は、適切な期間に完全に、正確に記録される。	網羅性 評価
すべての出荷が記録される。	実在性
出荷は正確に記録される。	評価

図表 35 – 棚卸資産に関する業務処理統制の目標（続き）	
統制目標の例	**財務諸表のアサーション**
出荷は速やかに、適切な期間に記録される。	評価
商品が承認された注文を受けて出荷される時にのみ、棚卸資産が減少する。	網羅性 実在性
出荷された棚卸資産の原価は、棚卸資産から売上原価に振り替えられる。	実在性 評価
出荷された棚卸資産の原価は正確に記録される。	評価
売上原価に転記された金額は、出荷された棚卸資産の金額を表している。	網羅性 実在性
出荷された棚卸資産の原価は、速やかに、適切な期間に、棚卸資産から売上原価に振り替えられる。	評価
在庫管理マスターファイルには正当な変更のみが行われる。	実在性 網羅性
在庫管理マスターファイルへのすべての正当な変更が、入力され、処理される。	実在性 網羅性
在庫管理マスターファイルへの変更は正確である。	評価
在庫管理マスターファイルへの変更は速やかに処理される。	実在性 網羅性
在庫管理マスターファイルのデータは最新の状態を維持している。	網羅性 実在性

図表 36 – 固定資産管理における業務処理統制の目標	
統制目標の例	**財務諸表のアサーション**
固定資産の取得は正確に記録される。	評価
固定資産の取得は適切な期間に記録される。	評価
すべての固定資産の取得が記録される。	網羅性
減価償却費は正確に計算され、記録される。	評価
すべての減価償却費が適切な期間に記録される。	実在性 評価 網羅性
すべての固定資産の除却が記録される。	実在性
固定資産の除却は正確に計算され、記録される。	評価
固定資産の除却は適切な期間に記録される。	評価
固定資産の保守管理の記録は正確に維持されている。	網羅性

図表 36 – 固定資産管理における業務処理統制の目標（続き）	
統制目標の例	**財務諸表のアサーション**
固定資産の保守管理の記録は適時に更新される。	網羅性
固定資産台帳またはマスターファイルには正当な変更のみが行われる。	網羅性 実在性
固定資産台帳またはマスターファイルへのすべての正当な変更が入力され、処理される。	網羅性 実在性
固定資産台帳またはマスターファイルへの変更は正確である。	評価
固定資産台帳またはマスターファイルへの変更は速やかに処理される。	網羅性 実在性
固定資産台帳またはマスターファイルのデータは最新の状態を維持する。	網羅性 実在性

図表 37 – 人事部における業務処理統制の目標	
統制目標の例	**財務諸表のアサーション**
給与マスターファイルへの追加は有効な従業員に限られる。	実在性
すべての新入社員が給与マスターファイルに追加される。	網羅性
退職した従業員が給与マスターファイルから削除される。	実在性
従業員は法定の、組合が定めた要件に沿って退職する。	網羅性
給与マスターファイルからの削除は有効な退職に限られる。	網羅性
すべての実働時間が入力される。	網羅性
実働時間が正確に入力され、処理される。	評価
給与は適切な期間に記録される。	評価
給与（報酬と源泉徴収分を含む）は正確に計算され、記録される。	評価
適切な従業員に給与が支払われる。	実在性
給与マスターファイルには正当な変更のみが行われる。	実在性 網羅性
給与マスターファイルへのすべての正当な変更が、入力され、処理される。	実在性 網羅性
給与マスターファイルの変更は正確である。	評価
給与マスターファイルの変更は適時に処理される。	実在性 網羅性
給与マスターファイルのデータは最新の状態を維持する。	実在性 網羅性

図表 37 – 人事部における業務処理統制の目標	
統制目標の例	**財務諸表のアサーション**
給与の源泉徴収票には正当な変更のみが行われる。	実在性 網羅性
給与の源泉徴収票の正当な変更がすべて入力され、処理される。	実在性 網羅性
給与の源泉徴収票の変更は正確である。	評価
給与の源泉徴収票の変更は速やかに処理される。	実在性 網羅性
給与の源泉徴収票のデータは最新状態を維持する。	実在性 網羅性

図表 38– 税務における業務処理統制の目標	
統制目標の例	**財務諸表のアサーション**
適時の税務申告のために、自動化された作業フローが用いられる。	網羅性
税金の支払は正しく計算され、総勘定元帳に記録される。	網羅性 評価 実在性
税額のエクスポージャーと評価引当金は正しく計算され、記録される。	網羅性 評価 実在性
税金費用は正しい期間に記録される。	網羅性 評価 実在性
永久差異と一時差異は把握され、正確に記録される。	網羅性 評価 実在性
未払税額の計算には、正しい帳簿上の利益が用いられる。	網羅性 実在性
税金資産、負債および費用は網羅的に正しく計算され、報告される。	網羅性 実在性
減価償却は適切な基準を用いて計算され、正しい税額および税効果の計算につながる。	網羅性 実在性
売上税および使用税は適切、正確、適時に計算される。	網羅性 実在性
付加価値税は正しく計上され、適切に申告される。	網羅性 実在性
移転価格の方針は更新され、システム内で正確に表示される。	網羅性 実在性
すべての税金支払は総勘定元帳に正確に反映される。	評価
固定資産税の申告は適時かつ正確である。	網羅性 実在性 評価

参考資料 E － アプリケーションとテクノロジ層の一覧表の例

図表 39 － アプリケーションとテクノロジ層のリストのサンプル

アプリケーション名	関連する業務プロセス	アプリケーションの詳細			データベース		オペレーティングシステム		ハードウェア･プラットフォーム		物理的ロケーション	
		パッケージ/自社開発	カスタマイズされている	責任者	バージョン	責任者	バージョン	責任者	バージョン	責任者	施設名	責任者
SAP	財務	パッケージ	はい	ケリー M	オラクル 9i V9.2.0	クレイグ T	ソラリス 3.2/ノベル	ライアン S	HP 9000	ダグ W	カルガリー	ダーシー M
ピープルソフト	人事給与	パッケージ	はい	トム M	オラクル 9i V9.2.0	クレイグ T	HP-UX V11.11/ノベル	アデル M	HP 9000	ダグ W	ヒューストン	ロンダ M
ACCPAC	子会社会計	パッケージ	いいえ	エスター C	オラクル 9i V9.2.0	クレイグ T	HP-UX V11.11/ノベル	アデル M	HP 9000	ダグ W	デンバー	ロバート P
TIMS	勤務時間記録	パッケージ	はい	ダリル J	DB2 400	アラン S	OS400/ノベル	リード C	AS400	ロブ K	カルガリー	ダーシーM
VIBS	請求書発行	カスタム	はい	ポール Z	DB2 400	アラン S	OS400/ノベル	ライアン R	AS400	バーブ V	カルガリー	ダーシーM
SunGard	投資	外部委託	いいえ	ケリー M	SAS70 を参照	クレイグ T	SAS70 を参照	ライアン S	SAS70 を参照	ダグ W	SAS70 を参照	ダグ W

参考資料 F — プロジェクト見積りツール

図表 40 – プロジェクト見積りツール

プロジェクトフェーズ	企業の規模によるプロジェクトフェーズごとの見積り作業時間（単なる見積りであり、各企業特有の状況によりこれを超過または下回る可能性がある）					
	小規模（単一拠点、アプリケーションが 5 未満）		中規模（拠点が 5 未満、アプリケーションが 5-10）		大規模（拠点が 5-10、アプリケーションが 10-15）	
作業見積り（日数）	最低見積り	最高見積り	最低見積り	最高見積り	最低見積り	最高見積り
1. 計画と対象範囲の決定	2	5	5	10	10	20
2. リスク評価	2	5	2	5	5	15
3. 統制の把握と文書化	5	10	10	20	20	50
4. 統制の設計上・運用上の有効性評価	5	10	10	20	20	30
5. 不備の優先順位付けと改善	注 1	注 1	注 1	注 1	注 1	注 1
6. 持続可能性の構築	注 2	注 2	注 2	注 2	注 2	注 2

注 1—改善作業日数は不備の深刻度による。企業は改善にとどまらず、新しいシステム開発または変更管理プロセスの導入といった運用上の効率の問題に取り組む選択をする可能性がある。
注 2—持続のための作業には、自動化および合理化の機会の評価が含まれるが、企業ごとに異なる、導入に要する時間は含まれない。

図表 41 – 文書化およびテストの作業見積り（日数）

文書化およびテストの作業見積り（日数）		
各 IT 環境	最低見積り	最高見積り
小型のパッケージアプリケーション	1	2
大型のパッケージアプリケーション	2	5
小型のカスタマイズされたアプリケーション	1	2
大型のカスタマイズされたアプリケーション	5	10
職務分離の評価—小型のアプリケーション	2	10
職務分離の評価—大型のアプリケーション	5	30

図表 42 – 文書化およびテストの作業見積り（日数）

文書化およびテストの作業見積り（日数）		
各 IT 環境	最低見積り	最高見積り
表計算ソフト（低い複雑度）	0.25	1
表計算ソフト（高い複雑度）	0.5	2
データベース	2	5
オペレーティングシステム	0.5	2
ネットワーク	0.5	5
物理的施設	0.5	1

最初の評価が実施されれば、これらの統制を維持するための作業見積りは時間とともに減少する可能性がある。**図表 41 と 42** の見積りは、初期計画における見積りであり、変化する可能性がある。例えば、非常に分散化した、多数のアプリケーションを有する企業は、実際にはより多くの作業を要するかもしれない。同様に、単純なプロセスとわずかなアプリケーションを有する極めて小規模な企業では、これほど多くの作業を必要としない可能性がある。

参考資料 G ー 固有リスクの評価と統制の優先順位付け表

リスク評価に関して考慮すべき事項

対象となる範囲のアプリケーションと関連するサブシステムのリスク評価を実施することにより、企業は高リスク領域での作業に優先順位をつけ、低リスク領域の作業を減らすことができる。リスクの評価は判断を伴う決定であることに注意する必要がある。しかし、考慮すべき共通のリスク要因がある。
図表 43 から 45 の図表は、固有リスクの評価を支援するためのものである。

図表 43—固有リスクに関して考慮すべき事項

リスク要因の例	高リスクのポイント	低リスクのポイント
テクノロジーの性質	複雑、特有、カスタマイズされている、社内で開発されている	単純、広く利用されている、カスタマイズされていない、市販ですぐに使える
担当者の特性	経験がない、研修不足、限られた人材、高い離職率	経験豊か、研修を受け専門知識がある、十分な人材、低い離職率
プロセスの特徴	分散型、複数拠点、その場対応	集中型、正式化されている、一貫している
過去の事例	処理エラー、システムの停止、データ破損を含む、問題の履歴	過去に問題がない
財務報告書に対する重要性	直接的—財務報告書への数字の初期入力および記録に用いられる	間接的—分析目的で用いられるが、財務報告書への数字の初期入力または記録は行わない。

情報技術のリスク評価

対象となる範囲の各アプリケーションについて評価を実施する必要がある。多くの、またはすべてのアプリケーションで、サブシステム（データベース、オペレーティングシステム、ネットワーク、物理的環境）が同じという場合もある。この場合、サブシステムの評価は一度でよい。

図表 44—テクノロジ層に対する固有リスクの評価

	テクノロジ層				
固有のリスク要因	**アプリケーション**	**データベース**	**オペレーティングシステム**	**ネットワーク**	**物理的環境**
テクノロジーの性質	高/中/低	高/中/低	高/中/低	高/中/低	高/中/低
担当者の特性	高/中/低	高/中/低	高/中/低	高/中/低	高/中/低
プロセスの特徴	高/中/低	高/中/低	高/中/低	高/中/低	高/中/低
過去の事例	高/中/低	高/中/低	高/中/低	高/中/低	高/中/低
財務報告書に対する重要性	高/中/低	高/中/低	高/中/低	高/中/低	高/中/低
全体的な結論（判断）	**高/中/低**	**高/中/低**	**高/中/低**	**高/中/低**	**高/中/低**

リスク評価を実施し、リスクのランク付けを行う際に、リスクのランク付けに関して考慮すべき事項または論理的根拠を文書化することが大切である。図表 44 は出発点として用いることができるが、リスク評価をサポートするためには、さらに分析を進める必要がある。

統制を考慮すべき箇所についての推奨事項

この表は、各テクノロジ層について考慮すべき IT 統制に関する指針を示したものである。一般的に、この表は、財務統制をより直接的にサポートする財務アプリケーションは財務報告にとってより大きなリスクであり、したがって、深い考慮が必要であるという見解を反映している。同様に、IT 全般統制の環境をサポートするものの、財務諸表からはかけ離れている物理的セキュリティの統制は、リスクが低く、それほどの考慮を必要としない。いつものように、すべてに当てはまるアプローチというものはなく、各企業は特定のニーズと状況に基づいて、この表をカスタマイズする必要がある。

図表 45ー統制の優先順位表

PCAOB の表題	企業改革法のための IT 統制	テクノロジ層				
		アプリケーション	データベース	オペレーティングシステム	ネットワーク	物理的環境
プログラム変更およびプログラム開発	アプリケーションソフトウェアの調達と開発	**推奨**	**推奨**	任意	任意	任意
	技術インフラの調達	任意	任意	任意	任意	任意
	方針と手続きの開発と維持	**推奨**	**推奨**	**推奨**	**推奨**	**推奨**
	アプリケーションソフトウェアと技術インフラの導入とテスト	**推奨**	**推奨**	任意	任意	任意
	変更管理	**推奨**	**推奨**	**推奨**	任意	任意
プログラム、データベースへのアクセス、およびコンピュータ運用	サービス・レベルの定義と管理	任意	任意	任意	任意	任意
	サードパーティのサービスの管理	**推奨**	**推奨**	**推奨**	任意	任意
	システムセキュリティの保証	**推奨**	**推奨**	**推奨**	**推奨**	任意
	構成管理	**推奨**	**推奨**	**推奨**	任意	任意
	問題とインシデントの管理	**推奨**	**推奨**	**推奨**	**推奨**	任意
	データ管理	**推奨**	**推奨**	任意	任意	任意
	オペレーション管理	**推奨**	**推奨**	任意	任意	任意

推奨 ー 上述の通り、IT 統制はテクノロジ層ごとに考慮する必要がある。各領域における作業範囲は固有のリスク評価による。
任意 ー IT 統制はリスクが把握された箇所で考慮しなければならない。

参考資料 H － 統制の文書化とテストのテンプレートのサンプル

文書化のテンプレートのサンプル

このマトリクスは、企業改革法遵守プログラムの一貫として文書化し、維持すべき統制の属性の種類に関する指針を提供するものである。
いつものように、すべてに当てはまるアプローチというものはなく、各企業は特定のニーズと状況に基づいてこの表をカスタマイズしなければならない。

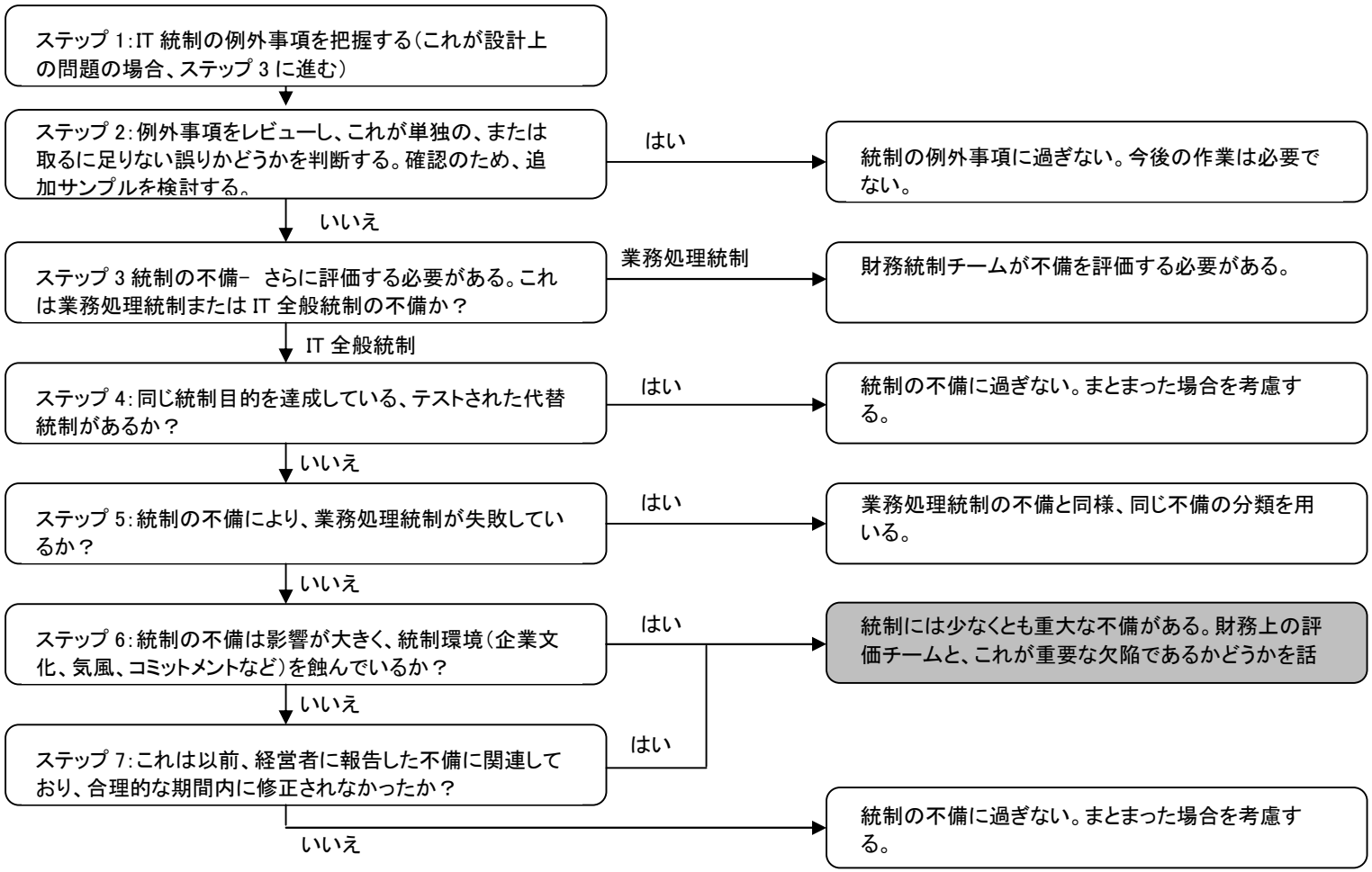
図表 46 － IT 全般統制のマトリクス

IT 全般統制のマトリクス				
統制の目標 #:				
結論： 統制は、この目的達成のために十分な有効性をもって運用されている。				
統制活動	**統制の頻度**	**サンプルサイズ**	**統制のテスト**	**テスト結果**

参考資料 I ー 不備の評価決定手順の例

図表 47 の評価決定の手順は、統制の設計または運用の有効性評価の際に用いることができる。企業は統制の不備が重大な不備、または重要な欠陥かどうかを結論付ける前に、財務上の評価チームと、そして最終的には経営幹部と話し合う必要がある。この例は正式な発表に基づくものではないが、多くの企業が取る共通のアプローチを反映したものである。

図表 47 ー 不備の評価手順の例



参考資料 J ― スプレッドシートのサンプルアプローチ

多くの企業は財務報告プロセスにおけるツールとしてスプレッドシートに依存している。不幸なことに、スプレッドシートには、ユーザアクセス統制と変更管理統制を含む、多くのアプリケーションが備えている固有の統制が欠けている。その結果、重大なリスクが財務報告プロセスにもたらされている。

すべてのスプレッドシートが同じ重要性とリスクを持つわけではないとして、どのスプレッドシートを評価すべきかを決定するために、同じ対象範囲とトップダウンのアプローチが用いられる必要がある。この目的は、財務諸表作成プロセスにとって最も重要なスプレッドシートを把握し、統制が機能しているか、そして統制が合理的な方法でテストされているかどうかを判断することにある。そのために、**図表 27** の指針を用いて、以下の 3 段階のアプローチが開発された。いつものように、各企業の個々のニーズに合わせるため、専門家による判断を検討し、このアプローチをカスタマイズすることが必要となる。3 段階のアプローチの詳細は以下の通りである。

1. スプレッドシートの棚卸 ― 出発点として業務プロセスの文書を用いて、財務諸表作成プロセスに関与するすべてのスプレッドシートを棚卸し、スプレッドシート名、スプレッドシートに関連する業務プロセス名、スプレッドシートが影響を及ぼす財務諸表上の勘定科目、スプレッドシートの作業内容、およびスプレッドシートが処理する取引額を文書化する。

2. リスク評価 ― 棚卸した各スプレッドシートについて、財務諸表の誤りに及ぼす影響とその発生可能性を評価する。
   ―影響― スプレッドシートの影響を評価するときには、組織はスプレッドシートが如何に使われているかと同じようにそのスプレッドシートによって処理される取引額を考慮すべきである
   ―発生可能性― スプレッドシートから引き起こされるエラーの発生可能性を評価するときには、企業は、スプレッドシートの複雑性、ユーザー数、スプレッドシートに加えられる変更の頻度を考慮するべきである。

   影響と発生可能性の評価指針として考慮すべき点を**図表 48 と図表 49** に示した。

   影響度と発生可能性の評価を使う上で、影響と発生可能性の評価を掛けることによりに、複合したリスクスコアを計算する(図表 50 を参照)。たとえば、影響度2（中程度）と発生可能性度3（高い）を持つスプレッドシートは、6（2*3）の複合リスク度を持つ。複合リスク度を持つ全てのスプレッドシートは、スプレッドシートの関連した重要性を確かめるためにまとめて、優先順位付けをし、レビューするべきである。

   リスク評価が終了した時点で、スプレッドシートに対応するためのアクションプランを策定する。以下のアクションプランを指針として示した。

- リスク評価 1-3 - スプレッドシートの固有リスクは低い。行動を取る必要はない。
- リスク評価 4-6 - スプレッドシートの固有リスクは中程度である。以下の 3a-3c で説明するスプレッドシートの統制を実施し、評価する。
- リスク評価 7-9 - スプレッドシートの固有リスクは高い。以下の 3a-3g で説明するスプレッドシートの統制を実施し、評価する。

図表 48－ 影響の評価			
影響度について考慮すべき点	**低い**	**中程度**	**高い**
スプレッドシートが処理する合計額	＜重要性の 20%	重要性の 20～50%	＞重要性の 50%
スプレッドシート出力の目的	分析的なレビュー	財務報告の開示	総勘定元帳への転記
影響の全体評価	（1－低い、2－中程度、3－高い）		

図表 49－ 発生可能性の評価			
発生可能性について考慮すべき点	**低い**	**中程度**	**高い**
スプレッドシートの複雑さ	低い （ロギング/データ追跡に使用）	中程度 （単純な計算/比較的重要でない仕訳入力）	高い （複雑なモデル、ピボットテーブル、他のデータソースへのリンク）
スプレッドシートのユーザの数	1 ユーザ	＜5 ユーザ	＞5 ユーザ
スプレッドシートの変更頻度	稀	時折	頻繁
発生可能性の全体評価	（1－低い、2－中程度、3－高い）		

図表 50－複合リスク評価			
影響の評価 (1-3)	3（低）	6（中）	9（高）
	2（低）	4（中）	6（中）
	1（低）	2（低）	3（低）
	発生可能性の評価(1-3)		

3. スプレッドシートの統制を実施または評価する － 上述の複合リスク評価に基づいて、スプレッドシートの統制の指針を以下に示した。組織の状況とスプレッドシートの使用状況により、他の統制を考慮する必要があるかもしれない。
   a) アクセスコントロール － ネットワークサーバ上にスプレッドシートを格納し、適切なアクセス制限を割り当てることによってスプレッドシートへのアクセスを制限する。
   b) 変更統制 － スプレッドシートの変更に関するプロセスを確立する。これはスプレッドシート内のタブの変更の文書化を含む。
   c) 文書化 － 経営目的とスプレッドシートの特定の機能を理解するため、適切なレベルのスプレッドシートの文書化を維持し、内容の更新を確実にする。
   d) テスト － 業務プロセスに直接関与していない者にスプレッドシートを見直させることによって、スプレッドシートの正式なテストを行う。その者にスプレッドシートの処理と関連する出力が意図した通りに機能していることを確認させる。
   e) 入力統制 － データが完全にかつ正確に入力されていることを確認するため、入力データをソースドキュメントと照合する。

f) データのセキュリティとインテグリティ - 数式やマスターデータなど、データ処理にとって重要な機密事項を有するセルを「ロック」、または保護することによって、スプレッドシートへの不正なまたは不注意な変更を防ぐ。
g) ロジックの点検 - 重要なスプレッドシートのユーザまたは開発者以外の者に、スプレッドシートのロジックを点検させる。このレビューは正式に文書化されなければならない。

参考資料 K ー 学んだ教訓

企業改革法導入の初年度および導入 2 年目に企業は多くの教訓を学んだ。**図表 51** から **56** はすべてを完全に網羅するものではないが、**図表 3** の IT コンプライアンスのためのロードマップで示した 6 つのステップを詳細に説明したものである。

図表 51 - 学んだ教訓 ー 評価計画と対象範囲の決定

学んだ教訓	今後の対応
a) 不適切な組織と報告の構造が構築され、IT が組織の企業改革法運営委員会全体と完全に統合されなかった。これにより、全体のコミュニケーションの効果が上がらなかった。	企業は、企業改革法運営委員会全体と統合され、これに報告を行う IT 統制小委員会を設立する必要がある。IT 統制小委員会は、IT による企業改革法の遵守を監督し、企業改革法のプロジェクト全体とのコミュニケーションと統合を取り持ち、企業改革法の IT プロセスにおける会計監査人との間を取り持つ必要がある。
b) IT 統制の責任が明確に定義されていなかった。混乱を招いた一般的な領域には、重要なアプリケーションのビジネスオーナと、業務処理統制と重要なスプレッドシートの責任者を把握することが含まれていたのにである。これにより、効果的な IT 統制が企業改革法の要件を確実に満たすことが困難となった。	IT 統制の責任は明確に定義する必要がある。重要なアプリケーションのビジネスオーナを明確に定義しなければならない。関連する業務処理統制、重要なスプレッドシートおよび他のエンドユーザ・コンピューティングツールの責任に関し、正式に合意する必要がある。
c) 多くの場合、企業改革法プログラム導入プロセスの初期の対象範囲はよく理解されていなかった。さらに、財務報告プロセスに関連のないいくつかのアプリケーションが、対象範囲から除外されていなかった。そして、対象範囲に含まれているはずのアプリケーションのいくつかが、会計監査人が問題を提起するまで含まれていなかった。これにより、企業改革法 404 条の要件を満たす上で、IT 統制の対象範囲が多すぎたり、少なすぎたりする事態となった。 IT 統制の立案と対象範囲の決定に、トップダウンの手法はしばしば取られなかった。経営者と監査人の双方は他の COSO の統制のリスクに与える影響を考慮せずに、しばしば統制活動のテストを開始した。関連統制の欠陥が発見されないリスクを他の統制が低減している可能性があるにもかかわらず、潜在的に減らせる可能性のある相当数の作業を統制活動レベルで実施した。トップダウンのアプローチがない場合、IT 統制の対象範囲が多すぎたり、少なすぎたりする事態は起こりうる。	過去 2 年間の企業改革法 404 条への遵守から学んだ経験と教訓同様、PCAOB による追加的な指針が、IT 統制の有効性の文書化とテストの対象範囲の決定プロセスをより良く理解することにつながった。企業は本冊子の対象範囲の決定の項（ロードマップ）を参照し、そこで得た経験を活用し、IT 統制の有効性の文書化とテストに関する、より合理化された、費用対効果のある対象範囲の決定プロセスを採用する必要がある。 企業は IT 統制のテストに関して対象範囲が多すぎたり少なすぎたりする事態を避けるため、そして、より合理化され、費用対効果のある対象範囲の決定プロセスを達成するため、本冊子の立案および対象範囲決定の項で述べたトップダウン・アプローチを採用すべきである。

図表 51 - 学んだ教訓 ー 評価計画と対象範囲の決定（続き）	
学んだ教訓	**今後の対応**
d) 導入計画にはコミュニケーション計画は含まれていなかった。正式なコミュニケーション計画がない場合、新たな統制が常に効果的に導入されにくい。コミュニケーション計画は、関連当事者に進捗状況と責任について最新情報を伝えておくために必要である。	新しい統制の導入計画の実施の一部として、コミュニケーション計画が含まれていなければならない。例えば、新しい方針を策定する際、これを従業員と契約社員に伝える計画がなければならない。
e) 会計監査人による作業実施時期が導入計画に含まれていなかった。このため、会計監査人による作業が望ましい時期を過ぎて行われた。ある場合には、重大な不備がプロセスの後期まで把握されず、年度末の後まで修正することができなかった。	作業実施時期に関する合意を含む、会計監査人との計画の策定は年度内に早期に完了しなければならない。この期限に関し、IT 統制の全責任者とコミュニケーションを取る必要がある。これにより、重大な不備があった場合に修正のための時間が与えられ、会計監査人が年度末のテストを実施することが可能となる。
f) 標準化された、または中央で実施される統制を導入する機会が失われた可能性があり、テスト戦略に関する、標準化された、または中央で実施される統制とプロセスが与える潜在的な影響が考慮されていなかった。これが有効でない内部統制をテストする結果につながった。	組織は統制の設計と運用の有効性の達成に寄与するため、標準化され、中央で実施される統制のプラットフォームを導入すべきである。さらに、組織は標準化され、中央で実施される内部統制の構造と矛盾しないテスト戦略をカスタマイズする必要がある。こうしたアプローチにより、より効率的で有効な統制のテストプロセスが実現できるだろう。
g) 企業改革法の財務/業務チームと IT チームとの間でしばしばコミュニケーション不足がみられた。双方のチームはしばしば、同じ統制目標に対応する関連統制を把握していた。さらに、マニュアル統制でなく自動化された統制に依拠する機会が失われ、もう一方のチームにおける統制の適切性に関する仮定が時折正しくなかった。これが実施作業の重複につながった。	企業改革法の財務/業務チームと IT チームは効果的なコミュニケーションを確実にするため、協力して作業を実施しなければならない。可能な場合、所定の業務プロセスの全体的な統制の有効性について結論付けるため、マニュアルと自動化された統制の双方の評価を統合する必要がある。さらに、適切な場合、マニュアル統制でなく自動化された統制により確実に依拠するため、この二つのチームは協力して作業を行わなければならない。
h) スプレッドシートとワープロのソフトウェア以外に、評価作業プロセスの自動化がほとんど行われていなかった。進捗状況の把握、または単独の解決策で対処できる統制の不備の根本的原因を把握することがしばしば困難だった。	生産性を高め、より効果的に進捗状況を把握し、統制の不備の根本的原因を把握するため、組織は評価作業プロセスの自動化を検討すべきである。
i) 統制の設計、リスク評価および文書化など、統制の実施に必要な一連のスキルはしばしば不足している。年度の最終四半期には、会計監査の専門家は企業の外部監査の責任を果たすことに主眼を置くため、これらの専門家を探し、作業を依頼することはますます難しくなった。しばしば、必要な外部の専門家は当初に予想したよりもより高価だった。このため、把握されたすべての不備を改善し、企業改革法 404 条の要件を満たすことができないリスクが高まった。	組織は適切な一連のスキルを持つ社内の人材を確保するため、年度の早い時期に計画を早めに策定する必要がある。これには、採用、外注または必要な一連のスキルを獲得するための社内の人材の研修が含まれる。

図表 51 - 学んだ教訓 ー 評価計画と対象範囲の決定（続き）	
学んだ教訓	**今後の対応**
j) 多くの場合、内部監査部が 404 条プロジェクトの導入作業において重要なサポートを提供した。しかし、これは、内部監査計画が達成されず、財務報告以外のリスク領域がレビューされていないことを意味する。また、統制を設計する監査人は、導入した統制をレビューし、テストしてはならないという独立性の問題もあった。これは将来、内部監査活動に影響を与える可能性がある。	組織の監査委員会および企業改革法運営委員会は、年度の早い時期に内部監査および企業改革法 404 条の評価作業のための人材の配分を連携して承認する必要がある。さらに、内部監査部門は統制の改善を提案し、改善すべき統制の決定、承認および導入に業務プロセスのオーナが最終決定権を持つべきである。内部監査部門は統制の有効性をテストする際、内部監査部門として独立性を維持することが可能である。可能な場合、企業改革法 404 条の遵守が年次のプロジェクトとしてではなく、継続的な業務プロセスの一部として導入されなければならない。
k) 通常の監査計画の一環として統制自己評価プログラムをテストするため、内部監査部を用いる可能性は検討されなかった。統制活動のテストを軽減するため、統制自己評価プログラムが及ぼす潜在的な影響は検討されなかった。	統制活動のテストを軽減するため、組織は統制自己評価プログラムの利用を検討すべきである。
l) アプリケーションが対象範囲に含まれるという事実は、アプリケーションが企業改革法の遵守に必要な、関連する業務処理統制をサポートしていることを示している。アプリケーションが非常に限られた数の関連業務処理統制をサポートしている場合でも、多くの場合、アプリケーションと関連するサブシステムが評価されなければならない。これにより、対象範囲から除外されていた可能性のあるアプリケーションの統制の文書化とテストにつながる。	アプリケーションが単独の統制をサポートしている場合、その業務処理統制（したがって、そのアプリケーション自体）を除外すること、そして関連するマニュアル統制を把握すること、または全体の作業数を軽減するため、既存のマニュアル統制への依拠を高めることのいずれかを検討することができる。これは稀ではあるが、ほとんど統制をサポートしていないアプリケーションを多く有する企業にとって、検討する価値がある。こうした状況で、軽率な特定の依拠（例えば、システムが作成する報告書への依拠など）が起きないことを確実にするため、留意が必要である。

図表 52 - 学んだ教訓 - リスク評価	
学んだ教訓	**今後の対応**
a) IT 全般統制に関連するリスクはしばしば検討されなかった。テストのレベルは、低リスク領域にとって必要なレベルよりも高いレベルにしばしば設定されていた。これとは反対に、テストのレベルに関して高リスクの影響は考慮されていなかった。 IT 全般統制に関しては、リスク評価はしばしば実施されなかった。財務報告に関する IT 環境のリスク評価を実施できなかったため、これが 404 プロジェクトの対象範囲が多すぎる、または少なすぎることにつながった。	組織は本稿の IT コンプライアンスのためのロードマップのステップ 2、IT リスクの評価で述べたプロセスを検討し、組織特有のニーズに合うよう、IT リスク評価のプロセスをカスタマイズする必要がある。

図表 53 － 学んだ教訓 － 統制の把握と文書化	
学んだ教訓	**今後の対応**
a） 多くの場合、必要な文書化の特徴と範囲に関し、会計監査人は相談を受けていなかった。これは、あるプロセスが必要以上に文書化され、文書化が急速に陳腐化するリスクが高まったことを意味していた。同様に、プロセスの文書化が必要最低限を満たしておらず、新たにやり直しをしなければならない可能性があった。	組織は対象範囲、適用されたアプローチ、文書化の性質と範囲、予想される成果物が要件を確実に満たすよう、年度の早い時期に会計監査人と緊密に共同作業を実施する必要がある。企業と会計監査人は SEC と PCAOB の新しい要件と指針に対応するため、年度中に継続的に意志伝達を図る必要がある。
b） 統制のフレームワークに関する全体的なアプローチが取られなかった。マニュアル統制、自動化された業務処理統制、IT 全般統制、統制のモニタリング（統制の定期的なモニタリングとしての内部監査を含む）、および統制環境の影響が、リスク評価プロセスにおいて全体として考慮されることがなかった。これらを考慮することによって、不必要なテストのリスクを低減させた可能性がある。	組織は組織における統制環境全体の影響を評価するため、財務および IT 監査人と共同作業を実施することによって、統制のフレームワークの全体的なアプローチを採用する必要がある。これにはマニュアル統制、自動化された業務処理統制のレビュー、統制のモニタリング、および統制のテストの最適なアプローチの決定が含まれる。

図表 54 － 学んだ教訓 － 統制の設計上・運用上の有効性評価	
学んだ教訓	**今後の対応**
a） 関連する統制の把握をサポートするはずのプロセスの文書化自体が目標となってしまっている。これが、関連統制のすべてが把握されない事態につながっている。	プロセスの文書化は最終目的ではない。それでも文書化は、企業および取引レベルにおける重要な勘定科目をサポートする業務プロセスを記録するための妥当な手段である。この作業の一環として、企業は虚偽記載につながりうるリスクと、これらのリスクに対応するための統制を把握する必要がある。重要な勘定科目、関連するアサーション、および重要なプロセスを把握した後、企業はテストを実施する関連統制を把握するため、本稿の IT コンプライアンスのためのロードマップのステップ 3 で述べたステップを検討する必要がある。
b） ある場合には、把握されたすべての統制が関連統制だと考えられた。これが不必要なテストにつながった。	組織は関連統制を文書化しテストする際の適切な作業量を確認するため、関連統制を他の統制から明確に区別しなければならない。前述したように、組織はテストすべき関連統制を把握するため、本稿の IT コンプライアンスのためのロードマップのステップ 3 で述べた行動も検討するべきである。
c） パラメータ主導の IT 全般統制の文書化と、プロセス主導の IT 全般統制の文書化が検討されていなかった。このことが内部統制の構造の不適切な文書化につながった。	内部統制の文書化と評価作業の際には、プロセス主導の IT 全般統制同様、パラメータ主導の IT 全般統制にも取り組む必要がある。

図表 54 － 学んだ教訓 － 統制の設計上・運用上の有効性評価（続き）	
学んだ教訓	**今後の対応**
d） 場合によっては、マニュアル統制のギャップ、IT 業務処理統制のギャップならびに IT 全般統制のギャップを含む、ギャップのリストが中央で作成されていなかった。これによって、潜在的な代替統制を評価することが困難になり、共通の統制ギャップの解決策を中央で改善できるかを判断することが困難になった。この結果、同じ問題に対して個々のグループに異なった解決法を生み出させることになった。	組織はマニュアル統制のギャップ、IT 業務処理統制のギャップならびに IT 全般統制のギャップを含む、ギャップのリストを中央で作成する必要がある。最も適切な改善策を決定するため、関連する代替統制を把握しなければならない。
e） パラメータ主導の IT 全般統制のウォークスルーが、統制の運用上の有効性評価の際に再実施されることがあった。これが重複する文書化とテストにつながった。	原則として、組織は IT 統制の文書化とテストにおいて重複する作業を行うべきではない。これはとりわけ、パラメータ主導の IT 全般統制のウォークスルーに当てはまる。
f） リスク・コントロール・マトリクス（組織による統制も含むべきである）の中で、外部サービス業者（サードパーティ）の監査報告書は対象範囲とされていなかった。これにより、関連統制が発見されなかった。同様に、外部サービス業者（サードパーティ）の説明文で文書化されているものの、外部サービス業者（サードパーティ）の監査人による説明文に明記されていない統制に依拠できるかどうか、または経営者による追加的なテストが必要かどうかに関して、しばしば混乱があった。	リスク・コントロール・マトリクス（RCM）を作成する際、組織は外部サービス業者（サードパーティ）の監査報告書の統制の記録とテスト結果を含める必要がある。これが、全体的でまとまった統制評価を目的とした、社内での、または外注したすべての関連統制を確実に検討することに寄与する。外部サービス業者（サードパーティ）の監査報告書の統制の説明文に依拠する必要がある。

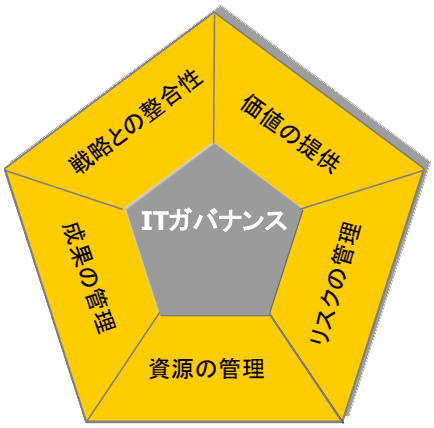
図表 55 － 学んだ教訓 － 不備の優先順位付けと改善	
学んだ教訓	**今後の対応**
a） ある場合には、経営者が主要な統制と不備を把握することを怠り、会計監査人が経営者による評価を評価した。経営者は会計監査人の評価を受け入れ、追加的な作業を実施した。これにより、ある統制の不備が年度の後半に把握されることになった。その結果、経営者は改善策に十分な時間をかけることができなかった。	組織は経営者が把握した関連統制が会計監査人の対象範囲を満たし、期待に応えていることを確実にするため、会計監査人と早期にそして継続的にコミュニケーションを取る必要がある。これにより、経営者が年度末に追加的な作業を行う必要がなくなるだろう。

図表 56 － 学んだ教訓 － 持続可能性の構築	
学んだ教訓	**今後の対応**
a） これまでは、企業改革法のプロセスをどのように改善できるかについて、導入後のレビューや評価が行われることがなかった。企業改革法プロジェクトの導入初年度のプロセスが完了し、導入 2 年目がスタートした。導入後のレビューが実施された際、常に関連当事者の全員が含まれているわけではなかった。これによって、企業改革法遵守のための時間とコスト削減の機会が失われた可能性がある。	企業は企業改革法のプロセスがどのように改善できるかを評価するため、関連当事者全員と導入後のレビューを実施する必要がある。こうして経営者は学んだ教訓を把握し、翌年度により費用対効果の高い計画を導入することが可能となる。
b） 企業改革法の遵守のフレームワークを、他の規制地域での遵守のモニタリング、そして企業の方針の遵守にまで広げることが考慮されていなかった。これが複数の規制当局およびガバナンスの要件を満たす際、作業の重複をもたらした。	組織は企業改革法の遵守のフレームワークを、企業方針の遵守および他の規制当局の要件の遵守を含むことにまで広げることを考慮する必要がある。これが組織の遵守作業全体の最適化に寄与するだろう。

図表 56 － 学んだ教訓 － 持続可能性の構築（続き）

学んだ教訓	今後の対応
c） 企業改革法 404 条の遵守の要件は、IT ガバナンスの部分をコーポレートガバナンスのプロセスに統合するのではなく、しばしば一度限りのプロジェクトとして当局の要件を満たすために始められている。これにより、長期的な遵守の維持ができなくなっている。	組織はコーポレートガバナンス全体の一部として以下の関連する IT ガバナンスの領域の導入を考慮すべきである。 • 戦略との整合性 • 価値の提供 • 資源の管理 • リスクの管理 • 成果の管理 詳細については、以下の**図表 57** および COBIT 4.0 を参照されたい。IT ガバナンスの導入により、組織は**図表 5** で述べた統制の信頼性に関するモデルの中でこれを継続し、長期的な継続性を築くことができるようになるだろう。

図表 57 － IT ガバナンスが焦点を当てる領域



- **戦略との整合性**はビジネスと IT 計画の連携の確保、IT 価値の提案に関する定義、維持、検証、そして IT オペレーションと企業のオペレーションとの連携に焦点を置く。
- **価値の提供**は、IT が戦略に沿った、約束された利点を提供することを確実にし、コストの最適化に集中して取り組み、IT の本質的価値を証明しながら、納入サイクルを通じて価値を提供することを意味する。
- **資源の管理**は、アプリケーション、情報、インフラおよび人材を含む、極めて重要な IT 資源への最適化された投資と、その適切な管理を言う。主要な問題は知識とインフラの最適化に関するものである。
- **リスクの管理**は、上級役員のリスクに対する認識、企業のリスク意欲に関する明確な理解、遵守要件の理解、企業に対する重大なリスクの透明性、リスク管理責任の組織への導入を意味する。
- **成果の管理**は、伝統的な会計を超える計測可能な目標に到達するため、例えば、戦略を実行に移すバランス・スコアカード（BSC） を使用することによって、戦略の導入、プロジェクトの完了、資源の使用、プロセスの実施とサービス提供の追跡とモニタリングを行うことを言う。

参考資料 L ー SAS70 調査報告書を用いる際の課題

多くの企業は、情報システムを含む業務の一部を外部サービス業者（サードパーティ）（サードパーティ）に委託している。アメリカ公認会計士協会は監査基準セクション 324「外部サービス業者（サードパーティ）」（SAS70）パラグラフ 3（AU324.03）で、以下のように述べている。

外部サービス業者（サードパーティ）のサービスが以下のいずれかに影響を与える場合、そのサービスは、サービスを依頼している企業の情報システムの一部とみなされる。
- 企業の財務諸表にとって重要な企業の業務内の取引の内容。
- 企業の取引を開始、記録、処理、報告する、取引の発生から財務諸表への算入に至るまでの自動化および手作業による手続き。
- 情報をサポートする、電子化された、または手作業による関連する会計記録および企業の取引の開始、記録、処理、報告に関わる企業の財務諸表内の特定の勘定科目。
- 企業の情報システムによる、財務諸表にとって重要なその他の事象および状況の捉え方。
- 重要な会計上の見積りおよび開示を含む、企業の財務諸表を作成するために用いられている財務報告プロセス。

外部サービス業者（サードパーティ）のサービスが、サービスを依頼している企業の情報システムの一部である場合、これらのサービスは財務報告に係る内部統制の一部であり、経営者は財務報告に係る内部統制の評価を行う際、PCAOB 監査基準第 2 号に則して当該外部サービス業者（サードパーティ）の活動を考慮する必要がある。監査基準第 2 号は、SAS70 報告書が十分であるとみなされる場合、経営者と企業の監査人が、その評価と意見を裏付けるため、実施されている統制とその統制の運用の有効性についてのテストに関し、外部サービス業者（サードパーティ）の監査人による報告書（SAS70 報告書）に依拠することを認めている。

本参考資料の以下の部分では、SAS70 報告書の十分性を評価する際に存在する、または表面化する可能性のある SAS70 に関連する問題点を取り上げる。

範囲

いくつかの問題点から、SAS70 報告書の範囲が、外部サービス業者（サードパーティ）が統制を有効に運用している証拠を提供する上で十分な結果をもたらしていない可能性がある。これらの問題点には以下の事項が含まれる。
- 記述された統制は財務報告との関連性がない。または委託されたサービスの一部分にしか関連がない。
- 統制の記述は、ユーザ企業にサービスを提供する外部サービス業者（サードパーティ）の拠点を十分に述べていない。
- 外部サービス業者（サードパーティ）は、さらに下請の企業に依存しており、その下請企業は SAS70 報告書の対象から「除外」されているため、下請企業からの SAS70 報告書が入手できない。

上述の場合、経営者と監査人は、以下を考慮する必要がある。
- SAS70 報告書の対象外ではあるが、外部サービス業者（サードパーティ）で実施されている、ユーザ企業の財務諸表のアサーション（適切な財務情報を作成するための要件）に関連する統制について理解する。
- これらの統制が有効に運用されている証拠を、直接的なテストまたは他の方法で入手する。

経営者と監査人は、これらの手続きを実施する際に、経営者評価における外部サービス業者（サードパーティ）が実施する統制の重要性と、ユーザである企業の統制と外部サービス業者（サードパーティ）での統制間の相互作用のレベルにより、実施される手続きが異なることを認識する必要がある。

統制の記述

PCAOB 監査基準第 2 号、パラグラフ B20 は、外部サービス業者（サードパーティ）が提供する統制の記述は、ユーザ企業と監査人が以下を可能にすることを意図していると述べている。

> *ユーザ企業の内部統制に関連する外部サービス業者（サードパーティ）側における統制、および外部サービス業者（サードパーティ）の活動に係るユーザ企業側における統制の理解*

外部サービス業者（サードパーティ）は統制の記述の適正な表示に責任を負い、外部サービス業者（サードパーティ）の監査人はその記述の適正性について見解を述べる。しかしその一方で、ユーザ企業のプロセスと財務諸表のアサーションに特有な側面により、外部サービス業者（サードパーティ）の統制の記述が、ユーザ企業およびその監査人のニーズを満たしていない結果を招く可能性がある。

問題点：統制の記述が、経営者または監査人が以下を行うのに十分な詳細なレベルで提示されていない。
- その統制の影響を受ける可能性のあるユーザ企業の財務諸表のアサーションの種類および虚偽記載の可能性の原因を把握する。
- 重大な虚偽記載のリスクに影響を与える要因を考慮する。
- 内部統制に関する経営者の評価を裏付ける。
- 内部統制についての監査人の意見を裏付ける。

問題点：外部サービス業者（サードパーティ）の経営者が特定した統制の目標が、ユーザ側の経営者が把握した財務諸表のアサーションのリスクのすべてに対応していない。または、そのリスクに対応したかどうかを判断するのに十分な記述をしていない。

問題点：ユーザ企業の経営者または監査人の意見では、外部サービス業者（サードパーティ）の経営者が特定した統制が、ユーザ企業の財務諸表のアサーションに関連する特定の統制の目標を達成するのに十分ではない。

問題点：統制の記述が、関連する全社レベルの IT 統制について十分な情報を提示しておらず、ユーザ企業の経営者または監査人が、アクティビティレベルの IT 統制の有効性の確立、強化または低減において全社レベルの IT 統制の運用の有効性を評価することができない。

これらの問題点は、SAS70 報告書で提示示される統制の記述を、さまざまな情報源から得られる情報により増強することで対応可能な場合が多い。情報源には、ユーザマニュアル、システムの概要、技術マニュアル、ユーザ企業と外部サービス業者（サードパーティ）間の契約書、外部サービス業者（サードパーティ）に関する内部監査人および規制当局による報告書などがある。この情報は、外部サービス業者（サードパーティ）との口頭または文書による質問と回答から直接得られる情報により補足する必要があるかもしれない。

問題点：統制の記述が、外部サービス業者（サードパーティ）の統制の設計段階において意図された、ユーザ企業で実施する必要がある統制の記述を含んでいない。

外部サービス業者（サードパーティ）における統制は通常、プロセスに係る有効な内部統制がユーザ企業による特定の統制の実施を前提とする形で設計されている。統制の記述にこうしたユーザ企業が実施すべき統制が見当たらない場合、ユーザ企業およびその監査人は、統制が把握されているべきかどうかを検討する。この評価を行う際に、ユーザ企業はすでに把握している虚偽記載の可能性の原因と SAS70 報告書にある統制との比較を望むかもしれない。

タイミング

経営者と監査人が外部サービス業者（サードパーティ）の統制について可能な限り最新の評価を得る必要性と、統制の例外事項または統制目的の達成度を評価し、リスクを低減する十分な時間的余裕をもって SAS70 報告書を受理することとの間に、固有のトレードオフが存在する。このトレードオフにより、SAS70 報告書の日付がユーザ企業の貸借対照表日以前となることが多くなる。これにより、対応を要する 2 つの問題が生じる。

第一に、運用の有効性のテストの対象期間と、経営者による評価日との間に、提供されるサービスに係る統制に重要な変更が行われた場合である。

外部サービス業者（サードパーティ）における統制に重要な変更があった場合、経営者と監査人は以下を考慮する必要がある。
- 変更されたユーザ企業の財務諸表のアサーションに関連する統制について理解すること。
- 変更された統制が有効に運用されている証拠を得ること。

外部サービス業者（サードパーティ）からの変更の通知、技術マニュアルの更新、トレーニング資料その他の情報伝達は、ユーザ企業の経営者および監査人が財務諸表のアサーションへの変更の影響を理解する上で十分な場合が多い。しかし、追加的な文書の受領に加え、外部サービス業者（サードパーティ）社員への追加的な質問が必要な場合もある。

変更された統制が有効に運用されている証拠は、入手がより難しい可能性がある。外部サービス業者（サードパーティ）が有効な IT 全般統制を維持している場合、ユーザ企業の経営者と監査人は、ユーザ企業の現場で業務処理統制の変更が機能している証拠を、業務処理統制の直接テストまたはユーザアクセプタンステストへの関与およびテスト結果の調査を通じて得られる可能性がある。

この他、外部サービス業者（サードパーティ）が変更した統制が、ユーザ企業に配備され機能している統制と重複している場合がある。このような場合、ユーザ企業の経営者と監査人はこれらの重複する統制のうち、どちらをテストするかを選択することができる。最後に、経営者または監査人は、統制が外部サービス業者（サードパーティ）の拠点でしかテストできないと判断する場合がある。このような場合には、経営者または監査人は外部サービス業者（サードパーティ）の拠点まで出向くか、外部サービス業者（サードパーティ）の監査人に変更された統制をテストし、合意された手続きまたは監査報告書を発行してもらうよう手配する必要が生じるかもしれない。

経営者および監査人による手続きの性質と範囲は、経営者による評価に対する統制の重要性およびユーザ企業の統制と外部サービス業者（サードパーティ）における統制間の相互作用のレベルにより異なる。

タイミングに関する第二の問題は、統制の運用の有効性テストの対象期間と、経営者のアサーションの日の間に長い経過期間が生じる点である。

このような場合、外部サービス業者（サードパーティ）での統制に変更があった、または統制が有効に運用されなくなったリスクがある。経営者はこうした変更が起きたかどうかを把握するための手続きを実施する必要がある。実施すべき手続きは、PCAOB 監査基準第 2 号、パラグラフ B25 から B27 で論じられている。外部サービス業者（サードパーティ）における統制に変更があった場合、その変更を上述の方法で評価する必要がある。

テストの性質と範囲

外部サービス業者（サードパーティ）の監査人が実施するテストの性質または範囲が、経営者による財務諸表のアサーションに関連する統制の評価を裏付ける上で十分でない場合、経営者および監査人は、追加的な手続きを実施する必要がある。

問題点：報告書は整備されている統制はカバーしているが、統制の運用の有効性のテストは含んでいない。

問題点：外部サービス業者（サードパーティ）が特定する統制の運用の有効性のテストは、ユーザ企業の財務諸表のアサーションに関する統制のリスクについての結論を裏付ける上で十分な証拠を提供していない。

PCAOB 監査基準第 2 号、パラグラフ B21 は、以下のように述べている。

> *統制のテスト、テスト結果、統制の運用の有効性についての外部サービス業者（サードパーティ）の監査人の意見を含まない、外部サービス業者（サードパーティ）の監査人による報告書（すなわち、監査基準セクション 324 パラグラフ.24a に記載されている、整備されている統制についての報告書）は、統制の運用の有効性の証拠を提供するものではない。*

報告書で特定されている統制が、経営者が把握する財務諸表のリスクに対応するための十分なテストを受けていない場合、同様の問題が存在する。SAS70 は以下の例でこれについて述べている。

> *経営者による評価および監査人の意見に関連する統制が有効に運用されているという証拠は、監査基準セクション 324 パラグラフ.12 に記述された手続きを踏むことで得られる。これらの手続きには以下の事項が含まれる。*
>
> *a.* *外部サービス業者（サードパーティ）の活動に係るユーザ企業の統制のテストを実施する（例えば、外部サービス業者（サードパーティ）が処理する選択された項目について、ユーザ企業による統制の独立した再実施をテストする。または、出力された報告書と元の文書とのユーザ企業による照合をテストする）。*
>
> *b.* *外部サービス業者（サードパーティ）において統制のテストを実施する。*

外部サービス業者（サードパーティ）が、統制の説明で記述された統制の運用の有効性のテストのために実施した手続きについての報告書が、合意された手続きに関する報告書である場合、ユーザ企業の経営者および監査人は、整備されている統制についての報告の評価で用いるのと同じ方法で、実施されたテストの十分性を評価する必要がある。

問題点：統制のテストの記述が、テストの性質、タイミング、範囲について詳しく記されていないため、ユーザ企業の経営者または監査人が、財務諸表のアサーションに関する統制のリスクを評価できない。

この場合、経営者と監査人は、テストの内容に関する追加的な情報を得るために、外部サービス業者（サードパーティ）とその監査人との話し合いを設定できるかもしれない。このような質問と回答は、基準および受け取った回答に基づいて文書化する必要がある。

こうした話し合いが持てない場合、この特定のテストは結論を裏付ける上で十分な証拠を提供できないものとして取り扱う必要がある。

問題点：提供されるサービスに関する統制環境、情報と伝達、リスク評価、モニタリングといった関連のある側面について実施されるテストの説明が十分でないため、ユーザ企業の経営者または監査人が、特定の統制の有効性を確立、強化、あるいは低減する際に、これらの統制の運用の有効性を評価することができない。

SAS70 によると、実施されたテストの説明が「提供されるサービスに関する統制環境、情報と伝達、リスク評価、モニタリングといった関連する側面」のテストを含まない場合、ユーザ企業の経営者と監査人は、これらの統制の経営者による評価に対する重要性と、ユーザ企業の統制と外部サービス業者（サードパーティ）の統制との間の相互作用のレベルを考慮する必要がある。経営者と監査人は、その後、規制当局への届出および他の文書の照会ならびに調査を通じて、これらの統制をテストする限定的な手続きを実施することを考慮しなければならない。

問題点：実施された統制の運用の有効性についてのテストの結果を記述する際に、例外事項の説明が十分でなく（例えばサンプルサイズ、発見された例外事項の数、例外事項の性質、原因、是正措置、その他関連する定性的な情報）、ユーザ企業の経営者または監査人が、これらの例外事項が財務諸表のアサーションに関する統制のリスクに与える影響を評価することができない。

この場合、経営者および監査人は、例外事項の内容に関する追加情報を入手するため、外部サービス業者（サードパーティ）との話し合いを設定できるかもしれない。このような質問と回答は、基準に従って文書化し、統制は受け取った回答に基づいて評価する必要がある。

このような話し合いを設定することができない場合、ユーザ企業の経営者と監査人は、この統制が有効に運用されていないとみなし、統制がユーザ企業の財務諸表のアサーションに与える影響について評価する必要がある。

限定付適正意見（限定意見）と除外事項

問題点：外部サービス業者（サードパーティ）の監査人の意見、または報告書の「外部サービス業者（サードパーティ）の監査人が提供する情報」の項で報告された除外事項により、外部サービス業者（サードパーティ）が提供する内部統制が、これらの側面から有効ではないと評価されている。

外部サービス業者（サードパーティ）の監査人の意見が限定意見を含む、または、テスト結果の説明で除外事項が指摘されている場合、経営者はその限定意見または除外事項を統制の不備として把握し、指摘された統制の不備を補う、あるいはその不備に伴うリスクを低減する、ユーザ企業が実施した統制を把握する必要がある。その後、この不備は、不備を評価するためのユーザ企業のメソドロジーに従って評価する必要がある。

問題点：外部サービス業者（サードパーティ）の監査人の意見に含まれている限定意見の記述が十分ではなく、ユーザ企業の経営者またはその監査人が、財務諸表のアサーションに関する統制のリスクへの影響を評価することができない。

この場合、経営者および監査人は、この限定意見の記述に関する追加情報を得るために、外部サービス業者（サードパーティ）およびその監査人との話し合いを設定できる可能性がある。このような質問と回答は、基準に従って文書化し、統制の目標と関連する統制は受け取った回答に基づいて評価する必要がある。

こうした話し合いを持つことができない場合、経営者および監査人はこの統制目標が達成されていないことを考慮し、これがユーザ企業の財務諸表のアサーションに与える影響を評価する必要がある。

外部サービス業者（サードパーティ）の監査人

問題点：外部サービス業者（サードパーティ）の監査人の評判、能力、独立性および外部サービス業者（サードパーティ）の監査人としての専門的見解が十分ではなく、経営者による評価および監査人の意見を裏付けることができない。

PCAOB 監査基準第 2 号、パラグラフ B24 は以下を義務付けている。

> *外部サービス業者（サードパーティ）の監査人の報告書が経営者による評価および監査人の意見を裏付ける上で十分な証拠を提供しているかどうかを判断する際、経営者および監査人は外部サービス業者（サードパーティ）の監査人の評判、能力、独立性に関する照会を行う必要がある。外部サービス業者（サードパーティ）の監査人の専門家としての評判に関する適切な情報源は、監査基準セクション 543、パラグラフ.10a(AU543.10a)、「他の独立監査人が実施する監査」で論じられている。*

外部サービス業者（サードパーティ）の監査人の評判、能力、独立性、および外部サービス業者（サードパーティ）の監査人としての専門的見解が十分ではない場合、経営者および監査人は実施された手続きの性質と範囲が十分ではなかったとみなし、前に述べた手続きを実施する必要がある。

参考資料 M － 重要な会計アプリケーションにおける職務分離

適切な職務分離は、内部統制の目標を達成する上で、企業の統制活動が有効であるかどうかを判断する際に重要な考慮事項である。職務分離の根底にある基本概念は、いかなる従業員またはグループも、通常の職務において、誤りや不正を犯し、同時にそれを隠蔽できる立場にあってはならないということである。一般に、分離する必要のある、両立し得ない主要な職務は以下の通りである。
- 資産に影響を与える、関連する取引の許可または承認
- 資産の管理
- 関連する取引の記録または報告

内部統制の従来のシステムは、これらの職務を異なった個人に割り当てること、または、両立し得ない機能を分離することに依拠してきた。このような職務分離は、一個人が資産へのアクセスを持つことと、この資産の説明責任を維持する責任の両方を持てなくすることを目的としている。IT 環境においては、機能の分離は以前から考慮されており、IT 全般統制の重要な構成要素としてテストされている。例えば、企業は許可された個人のみにプログラムの本番への移行権限を与える統制を導入している。同様に、企業は通常、システムおよびデータへのアクセスの申請と交付に係る職務を分離している。

しかし、適切な機能分離はアプリケーションレベルまたは業務プロセスレベルにおいても重要である。例えば、在庫管理システムにおいては、一般的に、異なる個人が以下の職務に責任を負う。
- 購入の開始または申請
- 注文書の発行および入力
- 商品の受領
- 確実な在庫管理
- 在庫記録の維持または除却もしくは廃棄の許可を含む、原価または数量への調整の許可
- 在庫マスターファイルの変更
- 担当者以外の者による実地棚卸の実施
- 実地棚卸での差異のフォローアップ
- 生産の申請または原料の移動の許可
- 製造過程からの商品の受領、または製造過程への商品の移動
- 商品の発送

多くの企業が直面する課題は、これらの両立し得ない、または相反する職務をアプリケーションレベルで把握することである。旧来の（レガシー）システム環境は、主にマニュアル統制のフレームワークがその環境を取り巻いていたために、職務分離を必要とし、これを推進してきた。また、購買システム、在庫システム、総勘定元帳システムが分離されたため、旧来の（レガシー）システムの断片化も職務分離を推進した。しかし、この従来の職務分離の概念は、完全に自動化された ERP システム環境で精緻化される必要がある。ERP システムはユーザ権限の付与に重点を移しており、これにより、ユーザはビジネス機能の全域にアクセスでき、またはこの代わりに実物資産を取り扱い、その動きを直接コンピューティングシステムおよび会計システムに記録することができる。職務分離の統制の概念は、リスク管理の視点を含み、長所と短所のバランスを取るように発展させる必要がある。

業務プロセスのレベルでの職務分離の矛盾を把握する上で、さまざまなアプローチがある。以下に挙げるのは、企業がその環境に合わせて活用／適用できる可能性のあるツール／テンプレートの 2

例である。**図表 58** にある最初の例は旧来のシステムに、**図表 59** の 2 つ目の例は統合システムに適用しやすい。

図表 58 は販売アプリケーションにおいて実施されている、相反する職務に焦点を当てるためのアプローチを示したものである。他の重要なアプリケーションのために、これと同様の文書を作成する必要がある。このテンプレートはリストにあるアプリケーションの各機能に責任を負う個人名を記入することで完成する。一つの機能が一つのコンピュータ・アプリケーションで実施される場合、個人名の代わりに「コンピュータ」あるいは「IT」と入力すればよい。

図表 58－販売アプリケーション

	許可	資産管理	記録	統制活動
注文書の発行				
売掛およびその条件の承認				
売掛関連のデータファイルへのアクセスの承認				
出荷の許可				
出荷書類の起票				
在庫品の出荷準備				
請求書作成の開始				
請求書作成の正確性の検証				
価格設定関連のデータファイルへのアクセスの承認				
標準価格からの逸脱の承認				
請求書作成の完全性の検証				
販売記録の維持				
売掛金記録の管理				
出荷と請求書の照合				
売掛金記録と総勘定元帳の照合				

重要なアプリケーションすべてについてこの表を記入した後、両立し得ないと思われる職務を一個人が実施している場合がないかをレビューする。一個人が一つを超える種類の職務（許可または承認、管理、または記録/報告）を実施している場合、またはある取引について、一個人がその記録/報告に責任を負いつつ、その取引に係る統制の実施も担当する場合、両立し得ない職務が存在する可能性がある。加えて、誰も職務を実施していない場合、それが統制内の欠陥を示す場合がある。二つ以上職務を一個人が実施する場合、すべてが職務分離の欠如を示すわけではないことに留意しなくてはならない。さらに、企業は同一のカテゴリー内で、職務分離が欠如している可能性があることを考慮する必要がある（例えば、売掛を許可する個人が回収不能勘定の消却も承認するなど）。

ある個人が両立し得ない複数の職務を実施していると把握される場合には、その個人が実施したすべての職務について、職務分離の欠如により、これらの職務の有効性が低減または解消されているかどうかを考慮する必要がある。有効性が低減または解消されている場合、次のステップはアプリケーションに係る統制と、誤りまたは不正行為のリスクに与える影響に対応することである。リスクの増大が把握された場合には、企業はこのようなリスクを予防または発見する他の統制を探し、これらの統制の有効性を評価する必要がある。追加の統制が把握されない場合、職務分離の欠如により、財務報告の誤りのリスクはより大きなものとなる。

職務分離を評価するための第 2 のアプローチは、業務プロセスの機能をリストにしたマトリクスを活用することである。このマトリクスは、企業のどの職務が両立可能で、同一人物が実施しても相反が

起きないかを示す。企業改革法 404 条の遵守の一環として、多くの企業がリスク管理の視点および機能上のアクセスとセキュリティの間のトレードオフを反映する、このような職務分離のマトリクスを作成している。組織内の各業務プロセス、および権限の付与と不正行為または不正取引のリスクを最小限度に抑える必要性との間の適切なトレードオフに合わせて、このようなテンプレートを適正化する必要がある。**図表 59** はこの概念を、購入から支払までのビジネス機能に適用した例である。例示されている通り、「×」は両立し得ない職務についての経営者による定義に基づいた、両立し得ない機能を示している。

図表 59－購買から支払までの職務分離のマトリクス

機能	仕入先の記録の作成および維持	注文書の承認・発行	商品受領書の処理	仕入伝票の処理	現金支払の処理	ブロックされた仕入伝票のブロック解除	仕入先の借方伝票を入力
仕入先の記録の作成と維持		×	×	×			
注文書の承認/発行			×	×			
商品受領書の処理				×			
仕入伝票の処理						×	×
現金支払の処理							×
ブロックされた仕入伝票のブロック解除							
仕入先の借方伝票を入力							

職務分離のテストを自動化するための特定の技法は、ここでは扱っていない。しかし、システムそのものの中ですでに入手可能な報告書について考慮することが出発点となる。なるべく多くのレビューおよびテストのプロセスを自動化するために、監査ソフトウェアについても考慮する必要がある。

参考資料 N ー 図表リスト

翻訳レビュー者のあとがき

今回も前回同様に翻訳のご提供をいただいた新日本監査法人の土田様他の皆様のご協力に感謝いたします。また、翻訳のレビューにも前回担当された ISACA 東京支部調査研究委員会の皆様に感謝いたします。

翻訳のレビューの方針として、今後公表される COBIT4 の翻訳用語との整合性や企業会計審議会の内部統制部会の「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」公開草案の用語にできるかぎりの整合性をとっています。なお、本翻訳は 2006 年 10 月に ITGI の HP に UP された COBIT for SOX version2 のバージョンではなく、その後 UP された COBIT for SOX version2 に従って翻訳されております。

ISACA 東京支部 2006－2007 調査研究担当常務理事 木村章展

参考文献

Committee of Sponsoring Organizations of the Treadway Commission

(COSO), *Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting*, USA, July 2006, *www.coso.org*

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management Framework*, USA, September 2004, *www.coso.org*

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control—Integrated Framework*, USA, 1992, *www.coso.org*

CSE (Canada), SCSSI (France), BSII (Germany), NLNCSA (Netherlands), CESG (UK), NIST (USA) and NSA (USA), *Common Criteria and Methodology for Information Technology Security Evaluation*, 1999

Deloitte & Touche LLP, “Moving Forward–A Guide to Improving Corporate Governance Through Effective Internal Control,” 2003

Deloitte & Touche LLP, “Taking Control, A Guide to Compliance with Section 404 of the Sarbanes-Oxley Act of 2002,” 2003

Dewitt, Ron; “Managing Change is Managing People,” 30 April 2004, *www.cioupdate.com*

Ernst & Young LLP, “The Sarbanes-Oxley Act of 2002, The Current Landscape—Rules, Updates and Business Trends,” 2003

International Organization for Standardization (ISO), *Code of Practice for Information Security Management*, ISO/IEC 17799, Switzerland, 2005

IT Governance Institute, COBIT 4.0, USA, 2005, *www.itgi.org*

IT Governance Institute, *Board Briefing on IT Governance, 2nd Edition*, USA, 2003, *www.itgi.org*

IT Governance Institute, *IT Governance Implementation Guide*, USA, 2003, *www.itgi.org*

KPMG, “The Defining Issues—Implications of Proposed Auditing Standard on Internal Control,” 2003

LaMarsh & Associates Inc., Managed ChangeTM Model, USA

Office of Government Commerce (OGC), Central Computer and Telecommunications Agency (CCTA), IT Infrastructure Library (ITIL), UK, 1989

Public Company Accounting Oversight Board, “Report on the Initial Implementation of Auditing Standard No. 2,” Standard: Release No. 2005-023, USA, 30 November 2005

Public Company Accounting Oversight Board, Staff Questions and Answers on Auditing Internal Control Over Financial Reporting, USA, 16 May, 21 January 2005

Public Company Accounting Oversight Board, Staff Questions and Answers on Auditing Internal Control Over Financial Reporting, USA, 22 November, 6 October 2004

Public Company Accounting Oversight Board, Staff Questions and Answers on Auditing Internal Control Over Financial Reporting, USA, 23 June 2004, revised 27 July 2004

Public Company Accounting Oversight Board, “An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements,” Final Auditing Standard: Release No. 2004-00 1, USA, 9 March 2004

PricewaterhouseCoopers LLP, “The Sarbanes-Oxley Act of 2002, Strategies for Meeting New

Internal Control Reporting Challenges," 2003

PricewaterhouseCoopers LLP, "Understanding the Independent Auditor's Role in Building Trust," 2003

Securities and Exchange Commission, Concept Release Concerning Management's Reports on Internal Control Over Financial Reporting (Release No. 34-54122, File No. 57-11-06), USA, 11 June 2006

Securities and Exchange Commission, SEC Announces Next Steps for Sarbanes-Oxley Implementation, USA, 17 May 2006

Securities and Exchange Commission, Commission Statement on Implementation of Internal Control Reporting Requirements, USA, 16 May 2005

Securities and Exchange Commission, Office of the Chief Accountant, "Division of Corporation Finance: Staff Statement on Management's Report on Internal Control Over Financial Reporting," USA, 16 May 2005

Securities and Exchange Commission, Office of the Chief Accountant, "Division of Corporation Finance: Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports-Frequently Asked Questions," USA, revised October 6, 2004

Securities and Exchange Commission, "Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports," Release Nos. 33-8238; 34-47986; IC-26068; File Nos. S7-40-02; S7-06-03, USA, June 2003, *www.sec.gov/rules/final/33-8238.htm*

図表の帰属：

本稿の図表 2、3、4、30、31、32、33、34はDeloitte & Touche LLPにより提供されたものである。