社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2008－DD－64 (16)
2008－EIP－39 (16)
2008／2／1

PCAOB監査基準第5号により必要となるデータベース統制の要件と適用技術

松永 豊† 大場 みち子‡

†東京エレクトロン デバイス株式会社 コーポレート企画室 〒163-1034 東京都新宿区西新宿 3-7-1

‡株式会社日立製作所 ソフトウェア事業部 新分野事業推進室
〒244-8555 横浜市戸塚区戸塚町 5030 番地

E-mail: † matsunaga.y@teldevice.co.jp, ‡ michiko.oba.cq@hitachi.com

あらまし 米国で企業改革法(SOX 法)により設立された監視機関 PCAOB (公開会社会計監視委員会)が2007年5月、監査基準第5号を発表し、SOX法の監査基準が事実上変更された。PCAOBの監査基準は、内部統制の弱点を早期発見し、財務報告の誤りを未然防止することを目的としている。従来標準とされていた監査基準第2号から更新された新基準である第5号は、監査の効率化を目指し、監査の対象を必要最小限に絞りかつ問題点をもれなく発見できるように、設計されている。本研究では、新基準による変更を分析し、新基準に適合するためにITシステム面で重要なデータベースの統制における技術的要件を検討している。この検討結果を報告する。

キーワード 内部統制, セキュリティ, 監査, 標準規格, 企業改革法, アクセス制御, データベース

Database Controls Required by PCAOB Audit Standard No.5

Yutaka MATSUNAGA† Michiko OBA‡

† Corporate Planning Dept., Tokyo Electron Device Ltd. 3-7-1 Nishi-Shinjuku, Shinjuku-ku, Tokyo, 163-1034 Japan

‡ Hitachi Ltd. Software Division, Emerging Business Development
5030 Totsuka-cho, Totsuka-ku, Yokohama-shi, Kanagawa 244-8555, Japan
E-mail: † matsunaga.y@teldevice.co.jp, ‡ michiko.oba.cq@hitachi.com

Abstract In May 2007, The Public Company Accounting Oversight Board (PCAOB), the monitoring organization established by the Sarbanes-Oxley Act (SOX), announced the Auditing Standard No.5, which replaces the auditing guideline for SOX. The auditing standard is intended to discover the possible deficiencies in internal control of the applicable companies, and to prevent the material misstatements in the financial report in advance. The new standard, No.5, has changed the substantial portion of preceding standard, The Auditing Standard No.2, to improve the efficiency of the audit, by minimizing the object of the audit and by maximizing the ability to find the important problems in internal control. This study analyzes the changes made in the new standard, and examines technical requirements of database controls that are necessary to meet the changes. This paper will describes the result of the study.

Keyword Internal Control, Security, Audit, Standard, Sarbanes-Oxley, Access Control, Database

1. はじめに

1.1. SOXの内部統制要件準拠における問題

米国で2002年に制定されたSOX法は既に4年にわたって運用されてきているが、その実績をもとに見直しの時期に入っている。特に404条で規定される財務報告に係る内部統制については負担が重いといわれており、改善が求められている。SOX法では、監査業務を監督するための専門の機関である公開会社会計監視委員会(PCAOB)を設置しているが、PCAOBが監査の現場を観察する中で、

2つの発見があったと報告している[1]。

まず、財務報告に関わる内部統制の監査は大きなメリットを生んでおり、企業統治や統制の向上や、財務報告の品質向上が挙げられること。2番目に、これらのメリットを得るために多大な費用がかかっていること。費用は想定よりも大きく、場合によっては、関連する作業が効率よく財務報告の内部統制を監査するために必要だと思われる内容を超えていた。このことは、コストを現実的な範囲に押さえるために監査の有効性に問題が出る可能性があることを示している。

米国商務省が米国企業を対象に実施したアンケート調査[2]でも、PCAOBによる発見を裏付ける結果が出ている。

この調査では半数以上の企業が、SOX法404条への対応費用が企業利益の3%以上におよんだとし、90%が、対応費用はその成果によるメリットに見合わないと答えている。また58%の企業が、SOX404条への準拠は、重大な不正行為の発見あるいは予防につながらないとしている。

こういった問題点を解決し、SOX準拠を現実的かつより有効なものにするために、監査基準の変更が行われた。この結果ITシステムにおいては、財務報告に係わるデータのアクセスに関する統制が、より厳格かつ効率よく実施されることが求められるようになった。

1.2. 日本企業の内部統制に与える影響

この動向は米国におけるものであり、日本企業に対しては直接的な影響を持つものではない。但し、米国で上場している企業においては直接適用されることと、日本における内部統制の取り組みの中で同様の傾向が見られることから、日本企業にも重大な影響を及ぼすことが予想される。

1.3. 研究の目的

そこで本研究においては、この米国における監査の新基準によってITシステム、特にデータアクセス制御に求められるようになった要件を検討している。本稿では新基準がSOX準拠の実務に与える影響を分析し、その為に必要となるITシステムの要件を説明したうえで、焦点になると思われるデータベース操作の統制に関する考察を行う。

2. PCAOB監査基準第5号

2.1. 新基準策定の経緯

当初SOX法404条に基づく内部統制の監査については、PCAOBが監査基準を策定し、ガイドラインとされていた。これは監査基準第2号「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」と呼ばれ、公開されている[3]。

PCAOBはSOX法404条への対応における問題点が顕在化したことを受け、2006年5月に4項目からなる内部統制要件の改善計画を発表した[4]。この中の1項目として監査基準第2号の修正を提案しており、その他には、PCAOBの検査を通じて監査人の作業効率化を図る、比較的規模の小さい企業を担当する監査人向けのガイドラインを策定する、小規模企業向けの委員会「PCAOB Forums on Auditing in the Small Business Environment」を継続する、の3点が発表された。

この時点での監査基準の修正内容としては、

- 重要な不備、重大な欠陥といった用語の定義の明確化
- 「重大な欠陥を強く示唆するもの」という表現の見直し
- 他の監査人による成果の活用に関する指針
- 重大さや対象範囲を決定する基準の明確化
- 内部統制監査の財務諸表監査との統合の強調
- 前年の監査結果を活用することの奨励

が挙げられている。

その後2006年12月に修正案「財務諸表監査と統合される財務報告に係る内部統制の監査」に対して意見招請を行い、寄せられた意見を反映した上で2007年5月24日に監査基準第5号として採択した[5]。

2.2. 監査基準第5号における主な変更点

監査基準第5号は、修正の目的として4項目を掲げて設計された。この4項目に沿った変更がなされている。

1) 内部統制監査の最も重要な事項への集中
監査を、財務報告の重要な虚偽表示の防止または検知を妨げるリスクが最も高い分野に集中させる。このために、そうした虚偽表示の原因となる内部統制における重大な欠陥を、手遅れになる前に発見するベスト・プラクティスを取り入れる。例えば、監査の計画においてトップダウンのアプローチを取る。
同時に、リスクが次に高い分野、例えば財務諸表の作成プロセスや経営者による不正行為防止措置などに対する重要性と、リスクが低い分野に対する選択肢を提供する。

2) 目標の達成に必要ない手順の省略
監査の負担を軽減するために、経営者によ

る内部統制監査の評価廃止や、複数の拠点がある場合にリスク分析による監査対象からの除外を規定する。

3) 企業の規模や複雑さに応じた監査プロセス
小規模あるいは組織構造が複雑でない企業や組織における適用方法を記述する。

4) 文書の単純化
条文を整理してボリュームを削減し、読みやすさを考慮した記述を行う。結果として、監査基準第2号では160ページあった本文が、監査基準第5号では59ページとなっている。

2.3. 用語の定義

監査基準第5号では、分かりやすさを追求する取り組みの一環として、用語定義に関する見直しが行われた。例えば、重大な欠陥(material weakness)は、監査基準第5号における修正目的の1番目に挙げられている「最も重要な事項への集中」の中核をなす概念であり、慎重な再定義が行われている。修正後の定義では重大な欠陥とは、財務報告に係る内部統制における不備、あるいは複数の不備の組み合わせで、企業の年次または期中財務諸表の重要な虚偽表示が防止あるいは適時発見できない合理的な可能性をもつもの、とされている。

監査基準第2号における定義から変更された内容で重要なのは、防止できない場合の発見について、適時(timely)という言葉が加わっている。つまり、記録によりあとから発見できるだけでは充分でなく、虚偽表示が発生する前に発見できなければいけない、ということである。

3. 監査基準第5号のITシステムへの影響

監査基準第5号による内部統制監査への影響としては、主に二つの側面が考えられる。1点目としては、監査対象の集中や不要な手順の省略などによって、負担が軽減される。2点目としては、重点的な監査が強調されたことによって、リスクの評価と正確性の保証や不正行為防止を確実に実施することが重要になった。この2点に対応するためには、ITシステムに対しては次のような要件が必要となる。

- システムを評価し、財務報告にとって重要な情報の所在とリスクの度合いを明らかにする。
- 重要な情報の変更に関するポリシーを策定する。
- 重要な情報の変更を監視して記録する。
- ポリシーに違反する性質の変更を防止あるいは発見する。
- 内部統制に関する状況を測定し報告する。

この際、財務報告に関する内部統制の定義を鑑み(図1)、記録に関しては必要な変更情報が漏れなく正確に記録されること、変更に関しては承認された正しい方法やユーザによってなされていること、不正に関しては防止できなければ適時に、すなわち手遅れにならないタイミングで発見できることが重要となる。

こうしたITシステム統制は、財務報告にとって重要な情報を中心として実装される必要がある。従って現実のシステムでそのような情報を保持していると考えられるデータベースに対する統制が焦点となる。米国の調査会社の調査によると、あらゆる形態の重要な情報のうち70%に関して、その機密性と完全性はデータベースのセキュリティに依存している[6]。本研究では、そのようなデータベースの統制に関する具体的な要件と適用可能な技術について検討した。

> 財務報告や公開用財務諸表の作成について合理的な保証を提供するプロセスであり、以下の項目に関するポリシーと手続きを含む：
> 1) 資産の取引および処分に係わる正確かつ公正な記録の維持
> 2) 取引の記録と取引が正しく承認されたものであることの保証
> 3) 不正な資産の取引に関する防止または適時発見

図1 監査基準第5号A5条 財務報告に関する内部統制の定義 (抄訳)

4. データベースに対する要件と技術

4.1. データベースの統制とコンプライアンスのライフサイクル

前章で検討したITシステムに対する要件をもとに、データベースに求められる統制の要件は次のようになる。

- 評価 - 重要な情報の所在とリスクの明確化
- ポリシーの作成 - 重要な情報の正確性を保証するために必要なルール
- 監視と記録 - データベース内の重要な情報に対する変更の監視と記録
- 違反の発見と防止 - データベースへの操作の中でポリシーに違反する操作
- 測定と報告 - 前4項目全てにおける状況の把握

データベースのセキュリティ研究者として知られるAmichai Shulmanは、こうしたデータベース

に対するコンプライアンス要件は、一連の流れとしてライフサイクルで管理すべきとしている[7]。（図 2） 次に各要件に対する詳細な説明と、適用可能な技術を解説する。

4.2. 評価

新基準では、リスクの評価をベースとして重要度を判断するため、データベースに対しても評価作業が重要となる。情報の正確性に関するリスクという観点では、1) 重要な情報の所在、2) 重要な情報を変更する要素、3) 不正なアクセスの防止、の 3 点を評価する必要がある。

4.2.1. 重要な情報の所在

重要な情報がどこに存在するか、に関する知識は、データベースの統制を実施し、ひいては実効性のある監査を行ううえで、必須になる。 これには重要なデータを保持するサーバ、データベース、テーブルを特定する必要がある。

それにはまずデータベースが稼動するサーバを特定して各データベースの種類や役割を把握する必要がある。通常これは既存の資料の参照や関係者のヒアリングによってリストを作成する形で行うが、ネットワーク上の通信を監視してデータベース・サーバを自動発見するツールも存在する。あるいは、業務プロセスから、財務情報を取り扱うアプリケーションを特定し、それらのアプリケーションが接続するサーバ、データベースとテーブルを見つけることもできる。 次に、重要な情報を保持するデータベースを抽出するが、これも既にデータベースが管理され、保持するデータの情報も存在する場合には、洗い出しの作業を行えば良い。既存の情報が完全でないと思われる場合は、関係者のヒアリングを行うか、評価ツールを使うことになる。 評価ツールの機能としては例えば、特定のアプリケーション(財務アプリケーション等)がクエリを発行しているデータベースやその中のテーブルを発見し、その中でも変更のクエリに絞り込む、といったことができる。

4.2.2. 情報変更の評価

特定した重要なデータをアクセスし変更する要素を把握する。誰が、どのデータに対して、どのような時に、どこから、どのような操作を行うのか、正常な操作のリストを作成する。具体的には、重要と判断されたデータが存在するテーブルに対してアクセスおよび変更するアプリケーション、ユーザを特定する。

ユーザに関しては、役割ベースでアクセスポリシーが策定されている環境では、その情報から該当するデータへのアクセス権限から抽出すること

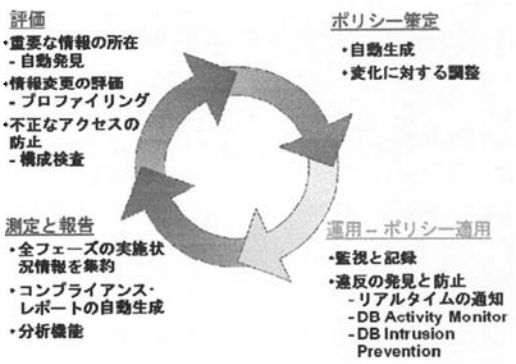

図 2 データベース・コンプライアンスのライフサイクル (Shulman の図を筆者が変更)

ができる。 アプリケーションに関しては、全てのアプリケーションに対して設計情報が明確であれば、そこから該当するデータベースとその中のテーブルについてのアクセスを洗い出せば良い。

そうした情報が存在しない場合は、日常のアクセス統計から判断することができる。データベース監査ツールの中には、アクセスの統計を取りプロファイリングと呼ばれる手法で、アクセス元のユーザ名、IP アドレス、アプリケーション、アクセス時間帯などを報告できるものが存在する[8]。

4.2.3. 不正なアクセスの防止

データベース内データの変更の統制に関しては、主に変更権限を持つユーザによる変更が焦点となる。 但し、権限を持たないユーザによる不正なアクセスおよび変更の可能性も除外するわけにはいかない。

表 1 データベース構成検査の検査項目分野例

項目	説明
データベースの一般情報	主にユーザ登録、特権関係のレポート
既知の攻撃情報	侵入を許すような既知の脆弱性
変更管理	設定ファイル、レジストリなどの変更を監視
OS の完全性	SQL Server に関する Windows の権限、ファイル設定など
制限されたシステム・プロシージャ	危険とされるプロシージャの利用制限設定
認証	安易なパスワード、ディフォルトのアカウントなど
アクセス制御	所有権の設定など

不正なアクセスによる変更のリスクを評価するには、サーバやデータベースに対する不正利用と、

不適切な権限設定に起因する想定外のユーザによる操作を考慮する必要がある。不正利用の防止には、ソフトウェア・コンポーネント全てに対する修正ソフトウェア(パッチ)の確実な適用と設定ミスの排除が必要になる。また権限設定については、全ユーザに対して役割を明らかにし、役割ベースのアクセス権設定を実装し維持する。これらの統制の評価は、それぞれの項目を含むデータベースの構成検査()を行うことで達成できるが、評価の時点で検査を行うことの他に、運用の段階で継続的に検査を行う仕組みを実装できているかどうかも重要になる。

4.3. データベースの評価における課題

上記3点の評価をデータベースに対して実施する際は以下のような点に留意して計画する。

- 知識とスキル - これらの評価を確実に行うためには、データベース、システム、ネットワーク、セキュリティといった幅広い分野の技術的スキルが必要となる。 例えばデータベースの構成検査を行う際に、データベース管理者が単独で実施することでは充分な評価は達成できない。
- 対象範囲 - 評価の目的に必要となる要素に対して漏れがないよう、範囲を周到に計画する。 財務情報が存在しうる場所、ネットワークやサーバ、ソフトウェアなどの構成、各構成要素が内在する脆弱性などのリスク、対象となるシステムとそれらにアクセスするアプリケーションの操作権限を持つユーザの利用動向などが含まれる。
- 実施の現実性 - 評価は、稼働中のシステムと業務実施中の関係者に対して実施される。業務の遂行とシステムの運用を阻害しない形の評価手段を選択する必要がある。 例えば、データベース・サーバ上への評価用ツールのインストールや、全ユーザ対象のヒアリング調査などは実現が難しい場合がある。
- 正確性 - 評価の結果は、正確でないと意味がない。 不適切なサンプリングによる調査や、開発用システムのみを対象とした評価作業では、正しい評価が得られず、監査の目的に適合しない場合がある。
- 評価結果の有効性 - 評価はそれ自体が目的ではない。 現状を把握した上で、ポリシー策定への反映、監査レポートでの利用、ライフサイクルの最終フェーズとなる測定と報告で必要となる継続的な情報収集に活用できることが前提となる。

4.4. ポリシーの策定

重要な情報の変更に関するポリシーとしては、所在が特定されたデータに対して、誰が、どのデータに対して、いつ、どこで、どのような操作を行って良いかのルールを決定する。 この内容は、情報変更の評価結果を利用して決定することができる。また、プロファイリングの機能を持つ監査ツールがあれば、プロファイリング結果から自動的にポリシーを生成することもできる。

4.5. 監視と記録

監視基準第5号では、3章で触れたように、重要な情報の変更はもれなく正確に必要な情報が記録されている必要がある。 このためには、対象となるデータへのアクセスを全て監視し、ログとして記録する必要がある。このためにはデータベース監査ツールが各種提供されており、利用することができる。但し監査ログの取得については、かつて筆者らも指摘したように[9]、いくつかの問題点(表2)が存在しており、留意する必要がある。

表 3 データベース監査における主要な問題点

ユーザ名の特定・記録
監査機能の迂回
ログデータの管理
権限の分離
サーバへの負荷
DBMS 互換性

4.6. 違反の発見と防止

監査基準では重要な虚偽表示を防止するか適時に発見することを強調しており、ポリシーに反するデータ操作への対策は必須となる。このためには、重要なデータに対するアクセスを全て監視し、ポリシーに合致するかどうかを判断することが必要になる。さらに特定のアクセスがポリシーに違反していることが判明した場合には、これを遮断することによって防止するか、リアルタイムに通知する機能の実装が要求される。

これらを実現する技術としては、データベース操作監視(Database Activity Monitor)およびデータベース侵入防御(Database Intrusion Prevention)といった技術が提供され始めている[10]。

4.7. 測定と報告

全ての統制項目を実証するためには各項目について、明確なレポートを作成できるようにする必要がある。評価で明らかになったリスク項目に基づいて、関連する変更記録や違反の検知および防止履歴などの情報を集約し一覧性のある形でレポ

ートすることによって、正規の、あるいは疑わしい操作の状況を提示できる。必要な情報を簡単に集計しレポートの形式に仕上げられる仕組みを示すことによって、監査のプロセスを単純化し、確実にすることができる。 このためには、全ての統制の仕組みから必要な情報を収集し、分析、加工する工程を自動化する技術を利用する。

5. 実装上の検討事項

監査基準第5号の変更に対処するためのデータベース統制要件を実装する際には、これまで説明した機能的な要求事項を満たすことの他に、システム構成上留意すべき点が存在する。

5.1. 職務分掌

内部統制のためのコントロールについては実施者の職務分掌が必要であるが、データベースの統制については、二つの側面から職務の分掌を確実にする必要がある。

まず、データベース管理者を重要な情報の操作から分離する。財務的に重要な情報に対してデータベース管理者による操作があってはならない。但し、データベース管理者がデータベース内データを操作できないようにすることは、技術的に難しい。 従ってまずポリシー策定の段階で、データベース管理者が財務関連情報に対してアクセスおよび変更してはならないことを明確にし、運用フェーズにおける監視と記録および違反の発見と防止の要件実装において、データベース管理者によるそうした不正な操作を確実に記録し、防止あるいは発見できるようにする。

次に、データベース統制の機能を他の職務、特にデータベースやシステムの管理者から分離する。評価における構成検査から始まって、運用フェーズでの監視と記録および違反の発見と防止、そして測定と報告に至るまで、データベース・コンプライアンスのライフサイクル全域にわたって、システム機能として技術的に実装されるコントロールは、管理者を含むシステム利用者の介在を許すと、破綻する危険がある。 一つの例として、前述のデータベース管理者を重要な情報の操作から分離する機能は、データベース管理者による操作(停止やログの修正など)を許してはならない。

総合的には、財務的情報の利用者による操作、システムやデータベースの管理、アクセス情報や変更情報を利用したデータベース統制実施、の三つの職務は明確に分離される必要がある。(図3)

5.2. 最小権限の原則

4.2.3節で述べたように、不適切な権限の設定が、不正な変更につながる可能性がある。職務分掌で

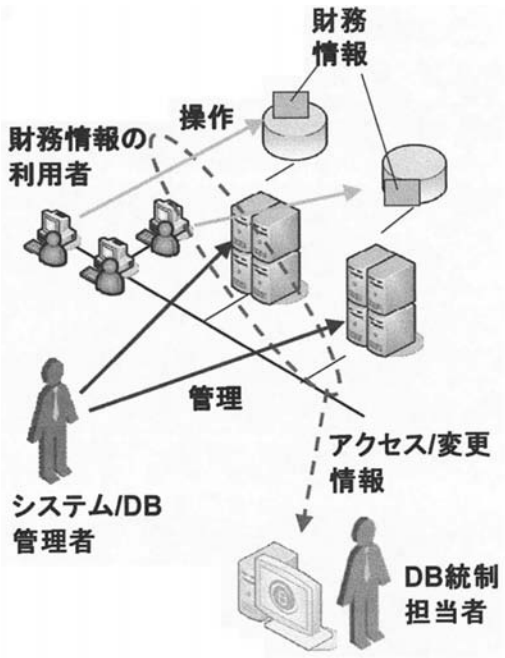

図 3 データベース統制における 3 種類の職務の分掌

登場した3種類の職務、すなわち財務的に重要な情報の操作、データベースやシステムの管理、データベース統制の実施、のいずれにおいても、必要最低限の権限をユーザごとに設定する必要がある。 これを現実的なプロセスで実施するには、役割ベースのアクセス権設定が有効と考えられる。

役割ベースのアクセス制御 (RBAC, Role Based Access Control)については D.F. Ferraiolo らによるモデルをはじめ[11]、詳細な解説が数多く利用可能だが、基本的には RBAC とは、 ユーザの役割に応じた属性に基づいて権限を付与し、ユーザ単位での特権の付与設定を禁止する手法を指す。データベース統制の中では具体的には、データベース構成検査の中で、ユーザに直接特権が付与されているケースを洗い出すことにより、役割ベースのポリシーが遵守されていることの評価を実施する。

5.3. 自動化

データベース統制は、その内容自体多岐にわたっており、それを、財務情報を扱うアプリケーション群、データが保存されるデータベース群、関与するユーザ群など、すべての要素において適用する必要がある。これらの全てにおいて欠陥なく実装し、そのことを監査において証明するためには、各コントロールを自動化し、さらにライフサ

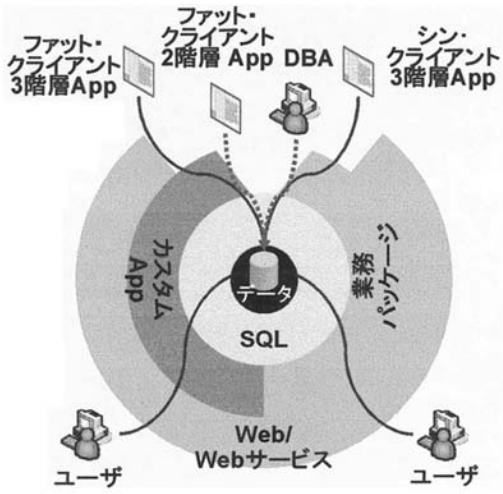

図 4 アプリケーション構造によるデータベースアクセスの経路

イクルのフェーズ間の連携が自動化されるべきである。

5.4. スケーラビリティ

監査基準第5号においては、特に小規模な組織においても効率の良い監査を行うための指針が示されている。一方、大規模な組織においては、多数のシステム要素に分散される可能性がある統制対象を確実に把握しなければならない。その為には、可能な限り統制のための機能が一元化されていることが望ましい。特に、測定と報告においては、レポート作成の機能は関連する情報を集約し、自動的にレポート化される仕組みが、確実かつ効率の良い統制につながる。

5.5. アプリケーション構造

最近の IT システムではアプリケーションの構造が多様化している。データベース統制の観点から見ると、データベースへのアクセスが多様な経路で行われることに留意する。全ての経路において、データベース統制の各コントロールが確実に適用されなければならない。(図 4)

6. まとめ

米国ではSOXの運用が第2段階というべきフェーズに入り、効率性と実効性が求められるようになった。その表れの一つが変更され採択された監査基準第5号である。この新基準によって、より負担の少ない SOX 法準拠が可能になったが、その為には重要な欠陥を阻止するための確かな施策が求められる。IT システムにおけるデータベースは、この施策の中核をなすべき要素であり、その為の要件と技術を検討した。監査要求に応えるには、データベースのコントロールだけでも多くの要件とライフサイクルを考慮する必要がある。本研究では，これらへ充分に対応でき，コストの抑制を両立できる関連技術と留意点を示した。

文献

[1] "AUDITING STANDARD No. 5 –AN AUDIT OF INTERNAL CONTROL OVER FINANCIAL REPORTING THAT IS INTEGRATED WITH AN AUDIT OF FINANCIAL STATEMENTS AND RELATED INDEPENDENCE RULE AND CONFORMING AMENDMENTS", PCAOB Release No. 2007-005A, June 12, 2007

[2] "Cost of SOX 404 Survey", U.S. Chamberof Commerce Center for Capital Markets Competitiveness, November 8, 2007, http://www.uschamber.com/publications/reports/0711soxsurvey.htm

[3] Auditing Standard No. 2: An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements, The Public Company Accounting Oversight Board, March 9, 2004
翻訳版：PCAOB 監査基準第２号 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」，日本公認会計士協会，
http://db.jicpa.or.jp/visitor/search_detail.php?id=1001

[4] "Board Announces Four-Point Plan to Improve Implementation of Internal Control Reporting Requirements", The Public Company Accounting Oversight Board , May 17, 2006

[5] "Board Approves New Audit Standard For Internal Control Over Financial Reporting and, Separately, Recommendations on Inspection Frequency Rule", The Public Company Accounting Oversight Board , May 24, 2007

[6] Phebe Waterfield, "Security Begins at the Database Level", Yankee Group DecisionNote, October 3, 2005

[7] "Imperva Data Security and Compliance Lifecycle", Imperva Whitepaper, September, 2007

[8] 松永豊，大場みち子，“内部統制を実現するためのデータベース・セキュリティ技術-モニタリングからコントロールへ-”，情報処理学会研究報告，2007-DD-062，Vol.2007 No.77, pp.65-70 (2007)

[9] 松永豊，大場みち子，"Web システムにおけるデータベース監査ログの課題と解決法"，情報処理学会研究報告，2006-EIP-034, Vol.2006 No.128, pp.61-68 (2006)

[10] Rich Mogull, et al., "Hype Cycle for Data and Application Security, 2007", June 29, 2007

[11] D.F. Ferraiolo and D.R. Kuhn, "Role Based Access Control" 15th National Computer Security Conference, Oct, 1992