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

2007－EIP－35（4）
2007／3／17

DBMS における業務処理統制機能の要件と課題に関する考察

間形 文彦，濱田 貴広，岡崎 聖人，塩野入 理，金井 敦
日本電信電話株式会社　NTT 情報流通プラットフォーム研究所

あらまし　金融商品取引法の成立によって，財務報告の虚偽表示のリスクに係る IT システムには，内部統制の評価と監査に耐え得るリスクコントロール機能の実装が望まれるようになる．本稿では，監査実務における財務諸表の虚偽表示リスクの原因と対策を踏まえて，従来の基幹情報システムの形態を分散・独立型情報システムと統合型情報システムに分けて比較し，IT 統制上の特徴を整理する．さらに業務処理統制における統合型情報システムの優位性を前提として，DBMS が実現すべき業務処理統制機能の要件と課題を示す．
キーワード　内部統制，DBMS，リスクコントロール，業務処理統制，全般統制

A Study of Requirement and Problem for Application Controls Function in DBMS

Fumihiko Magata, Takahiro Hamada, Masato Okazaki, Osamu Shionoiri, Atsushi Kanai
NTT Information Sharing Platform Laboratories, NTT Corporation

Abstract　In the IT system related to the risk of material misstatements in the financial statements, Implementing the risk control function for the evaluation and audit of internal control can be endured comes to be hoped by the establishment of Financial Instruments and Exchange Law. In this text, the form of the information system is divided into decentralization/independent type and integrated type. The features of two type system of IT control are arranged from the viewpoint of the internal control audit. In addition, the requirement and problem for the application controls that should be implemented on DBMS are shown on the assumption of the domination of the integrated system in the application controls.
Keywords　Internal Control, Data Base Management System, Risk Control, Application Control, General Control

1. はじめに

2006 年 6 月 7 日，第 164 回国会において証券取引法等の一部を改正する法律が成立した．同法の施行により証券取引法は金融商品取引法に改正される．金融商品取引法はその 24 条の 4 の 4 において，有価証券報告書の提出義務のある会社に対し，さらに内部統制報告書の提出を義務付けるものである．[1]米国 SOX 法がその 404 条において経営者に内部統制報告を求めていることから，金融商品取引法 24 条の 4 の 4 は米国 SOX 法 404 条と対比され，一般に，日本版 SOX 法と呼ばれている．

日本版 SOX 法の定める内部統制報告書とは，「当該会社の属する企業集団及び当該会社に係る財務計算に関する書類その他の情報の適正性を確保するために必要なものとして内閣府令で定める体制について，内閣府令で定めるところにより評価した報告書」をいう．つまり，日本版 SOX 法は内部統制報告書の具体的な内容を内閣府令に委任する．

一方，企業会計審議会は，「財務報告に係る内部統制の評価及び監査の基準」（以下，「内部統制の監査基準」という．）ならびに「財務報告に係る内部統制の評価及び監査に関する実施の基準」（以下，「実施基準」という．）を公表している[1]．内部統制の監査基準は「財務報告に係る内部統制の有

[1] 米国 SOX 法: Sarbanes-Oxley Act of 2002. 正式名称は，「An Act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes」（証券諸法に準拠し，かつその他の目的のために行われる企業のディスクロージャーの正確性と信頼性の向上により，投資家を保護するための法）．

効性に関する経営者による評価及び公認会計士等による監査の基準についての考え方」を示し，実施基準は「各企業等の創意工夫を尊重するとの基本的な考え方を維持しつつ，財務報告に係る内部統制の構築・評価・監査について，できるだけ具体的な指針を示す」ものとなっている．

したがって，わが国の財務報告に係る内部統制監査制度は，金融商品取引法を法的根拠とし，報告すべき内容を内閣府令で定め，内部統制の考え方の枠組みと実施の指針をそれぞれ内部統制の監査基準と実施基準が与えることによって形成されることになる．現時点で未公布のその内閣府令の条文を参照することはできないが，その内容は内部統制の監査基準の枠組みから大きく外れるものにはならないと考えられており，既にわが国の財務報告に係る内部統制の監査制度は実質的な整備をほぼ終えているといえよう．

本稿では，ほぼその全容が明らかとなったわが国の財務報告に係る内部統制の監査制度について財務諸表監査と比較し，財務諸表の監査を行っている公認会計士等（以下，「監査人」という．）の視点から，企業の基幹情報システムの中核となるDBMS が具備すべき内部統制機能の要件と課題を示す．

2 章において内部統制報告書に記載すべき統制の対象であるリスク及びその原因を明らかにし，3 章において IT によるリスクコントロール手法を述べる．さらに 4 章では IT 統制の観点から基幹情報システムの形態を比較し，DBMS に統制機能を実装する効果に言及する．5 章では DBMS が実現すべき業務処理統制機能の要件と課題を抽出して，6 章で本稿をまとめることとする．

2. 財務報告に係るリスクと原因

2.1　財務諸表監査と内部統制監査

従来から有価証券報告書の提出義務のある会社は，監査人による財務諸表の監査を受けていた．日本版 SOX 法は，有価証券報告書の提出義務のある会社に対して，財務諸表監査に加え，さらに内部統制監査を義務付ける制度であることは前述したとおりである．財務諸表監査も内部統制監査もその制度の趣旨は同じ，投資家保護である．有価証券報告書も内部統制報告書も，投資家にとって投資判断の基礎となる情報であり，監査人は監査報告書に自己の意見を表明することにより，投資家の投資判断を支えることになる．

財務諸表監査の目的は,「経営者の作成した財務諸表が，一般に公正妥当と認められる企業会計の基準に準拠して，企業の財政状態，経営成績及びキャッシュフローの状況をすべての重要な点において適正に表示しているかどうかについて，監査人が自ら入手した監査証拠に基づいて判断した結果を意見として表明すること」にある[2].

一方，内部統制監査の目的は,「経営者の作成した内部統制報告書が，一般に公正妥当と認められる内部統制の評価の基準に準拠して，内部統制の有効性の評価結果をすべての重要な点において適正に表示しているかどうかについて，監査人自らが入手した監査証拠に基づいて判断した結果を意見として表明すること」にある[1]．ここにいう内部統制とは「財務報告に係る内部統制」を指す．「内部統制の有効性」とは,「財務報告に係る内部統制が適切な内部統制の枠組みに準拠して整備及び運用されており，当該内部統制に重要な欠陥がないことをいう」．さらに「財務報告」とは,「財務諸表及び財務諸表の信頼性に重要な影響を及ぼす開示事項等に係る外部報告」であるとされる[1].

財務諸表監査と内部統制監査は，どちらも公正妥当な基準に基づいて，監査人が自ら入手した監査証拠に基づき意見表明するという点で共通する．これは監査一般に共通する特徴であって，両者の違いは監査の対象にある．前者が財務諸表を対象とするのに対し，後者は財務報告に係る内部統制の有効性の評価結果としての内部統制報告書である．内部統制報告書は，財務報告の信頼性が達成されているとの合理的な保証を得るために，業務に組み込まれ，組織内のすべての者によって遂行されるプロセスの有効性を評価したものである．つまり，前者は組織が生成した財務諸表を対象とするのに対し，後者は財務諸表を生成するプロセスを評価した組織の報告書を対象とする．

したがって，日本版 SOX 法は生成結果に対する監査（財務諸表監査）だけでなく，さらにその生成過程の評価結果に対する監査(内部統制監査)も加えて投資家保護を図ろうとするものである．

2.2　リスク･アプローチ

財務諸表監査と内部統制監査にはもう一つ重要な共通点がある．リスク・アプローチの採用である．リスクが高い事項について重点的に監査の人員や時間を充てることにより，監査を効果的かつ効率的なものとすることができる監査の実施の方法をリスク・アプローチという[3]．財務諸表監査も内部統制監査も，重要な虚偽の表示が生じる可能性をリスクと捉えている．財務諸表の表示が適正である旨の監査人の意見は，財務諸表には，全体として重要な虚偽の表示がないということについて，合理的な保証を得たとの監査人の判断を含む[2]．他方，内部統制報告書が適正である旨の監査人の意見は，内部統制報告書には，重要な虚偽の表示がないということについて，合理的な保証を得たとの監査人の判断を含む[1]．監査人は，職業的専門家としての懐疑心をもって，重要な虚偽

の表示がもたらされる可能性に関して評価を行い，その結果を監査計画に反映し，これに基づき監査を実施しなければならない[2].

2.3　リスク原因

虚偽表示のリスクの原因について，財務諸表の監査基準[2]，実施基準は共に明解であり，「不正及び誤謬により財務諸表に重要な虚偽の表示がもたらされる可能性」[2]，「不正又は誤謬により，虚偽記載が発生するリスク」[1]と明記される．すなわち，虚偽表示をもたらす原因は，不正と誤謬であるとする．さらに日本公認会計士協会監査基準委員会報告書第 10 号[4]は，「財務諸表の重要な虚偽の表示の原因となる不正及び誤謬に関する実務上の指針を提供」し，不正と誤謬を次のように定義している．誤謬とは「財務諸表の虚偽の表示の原因となる意図的でない誤り」であり，不正とは「財務諸表の虚偽の原因となる，経営者，従業員又は第三者による意図的な行為」であり，不正には「不正な財務報告（いわゆる粉飾）と資産の流用がある」とされる．

3. 財務報告に係るリスクコントロール

3.1　IT の利用と IT の統制

IT を利用した情報システムは，財務諸表の虚偽表示のリスクをコントロールするために利用することができる．実施基準によれば，「IT には，情報処理の有効性，効率性等を高める効果があり，これを内部統制に利用することにより，より有効かつ効率的な内部統制の構築を可能とすることができる」からである．さらに，実施基準は，「財務報告の信頼性を確保するために整備するもの」として「IT の統制」を位置づける．IT の統制とは，「IT を取り入れた情報システムに関する統制」である．すなわち，財務報告の虚偽表示のリスクコントロールに利用される IT は，それ自体が統制の対象となるべきことを意味している．

IT の統制を有効なものとするために経営者が設定する目標を，IT の統制目標と呼ぶ．実施基準によれば，IT の統制目標は次のとおりである．

a. 有効性及び効率性 : 情報が業務に対して効果的，効率的に提供されていること
b. 準拠性 : 情報が関連する法令や会計基準，社内規則等に合致して処理されていること
c. 信頼性 : 情報が組織の意思・意図に沿って承認され，漏れなく正確に記録・処理されること（正当性，完全性，正確性）
d. 可用性 : 情報が必要とされるときに利用可能であること
e. 機密性 : 情報が正当な権限を有する者以外に利用されないように保護されていること

3.2　業務処理統制と全般統制

IT の統制は，業務処理統制と全般統制に分けられる．実施基準を次に引用する．

IT に係る業務処理統制とは，業務を管理するシステムにおいて，承認された業務がすべて正確に処理，記録されることを確保するために業務プロセスに組み込まれた IT に係る内部統制である．

IT に係る全般統制とは，業務処理統制が有効に機能する環境を保証するための統制活動を意味しており，通常，複数の業務処理統制に関係する方針と手続をいう．

実施基準では，業務処理統制，全般統制と IT の統制目標との関係は必ずしも明らかにされていない．しかし，実施基準によれば，「財務報告の信頼性を確保するための IT の統制は，会計上の取引記録の正当性，完全性及び正確性を確保するために実施される．正当性とは，取引が組織の意思・意図にそって承認され，行われることをいい，完全性とは，記録した取引に漏れ，重複がないことをいい，正確性とは，発生した取引が財務や科目分類などの主要なデータ項目に正しく記録されること」とされ，また，「全般統制が有効に機能しない場合には，適切な内部統制（業務処理統制）を組み込んだとしても，その有効性が保証されなくなる可能性がある」という．このことから，次のように考えることができる．

業務処理統制は，その定義から，承認された（正当性）業務がすべて（完全性）正確に（正確性）処理，記録されることを確保するもの，すなわち財務報告の信頼性を確保するための IT の統制である．したがって，業務処理統制は，財務報告の信頼性の確保に直接的に関与し，全般統制は業務処理統制との関係を通じて，財務報告の信頼性の確保に間接的に関与するものである．

3.3　リスクコントロール

財務報告の信頼性に影響を与えるのは虚偽表示のリスクである．虚偽表示のリスクに対して IT を利用することができ，そのための直接的な IT の統制目標は，正当性，完全性及び正確性である．これらの統制目標を達成するための統制方法には何が考えられるであろうか．

統制方法はリスクを低減するための解でなければならない．そのリスク原因が不正と誤謬であるとすれば，リスク低減のための解は，不正と誤謬に対して効力をもつ必要がある．

不正と誤謬のどちらも人的要因として捉えるとすれば，人の行為に影響を与えるには他者による牽制が業務処理統制として有効であると考えることができる．これについて実施基準は，次の例を与えている．例えば，取引の承認，取引の記録，資産の管理に関する職責をそれぞれ別の者に担当させることにより，それぞれの担当者間で適切に相互牽制を働かせること．以下，「取引の承認」を(2)承認，「取引の記録」を(3)監視，「職責をそれぞれ別の者に担当させること」を(1)分離とし，次のように考えることとする．

(1)分離

財務諸表の虚偽表示をもたらすリスク行為を実施する者が，１人でそのリスク行為を完遂できないように業務範囲及び業務権限を分割すること．業務は，業務プロセスの他，期間を単位として分割される．期間を加えるのは会計期間が重要であるだけでなく，同一業務の担当替え（ジョブローテーション）を考慮に入れたためである．

(2)承認

財務諸表の虚偽表示をもたらすリスク行為の一部または全部を実施する者の行為に対して，他者が承認を与えること．その承認がなければリスク行為は次の業務プロセスに移行できないこと等の理由により，リスク行為は完遂できない．

(3)監視

財務諸表の虚偽表示をもたらすリスク行為をその行為者の特定が可能な状態で記録し，記録を保管し，その行為者とは別の者が記録を確認すること．記録に変更を加える場合には，変更の行為者の特定が可能な状態で変更履歴を残し，その行為者とは別の者が履歴を確認すること．

さらに，組織において上記の３手法を実現するための前提となる組織内部の諸規程を整備することを，(4)規程とする．

以下，具体例を挙げて上記の統制手法について説明する．

先ず，虚偽表示のリスク行為の一般的な例として，「仕入先マスタに架空の仕入先を登録すること」を挙げてみる．これに対するリスク原因は不正である．例えば，会社の資産である現金を着服するという意図を実現するため，購買担当者が自らの管理する銀行口座を指定した架空の仕入先マスタを作成し，架空請求を行うといった資産の流用を意図する場合などである．

このリスク行為に対応する統制行為は上記の分類に従って，次のように考えることができる．

(1)分離

仕入先マスタの業務プロセスを登録依頼とマスタ登録に分け，それぞれ登録依頼者と登録担当者に業務権限を分けて委任し，同一人物が兼務できないこと．

(2)承認

仕入先マスタの登録担当者の登録行為は，上長が承認することによってはじめて完遂し，承認前に当該マスタは他の業務プロセスで使用できないこと．

(3)監視

仕入先マスタの登録依頼は，登録依頼書を持って行い，マスタの登録履歴と共に記録に残し，登録依頼者，登録担当者とは別の者が記録を確認すること．

(4)規程

上記(1)から(3)に関する組織内の諸規程を整備すること．

以上の統制手法によって，資産の流用の意図を持った者のリスク行為は常に他者の協力なしには実行できず，またその行為は常に他者の眼にさらされることになる．つまり，他者による牽制とは，露見せずに悪事をはたらくのが困難なことが明らかなとき，人は悪事を働かないという考えに基礎を置くものである．

一方，意図的でない誤りである誤謬に対する他者の牽制は，意図的な不正に対する他者の牽制の働きと必ずしも同一ではない．意図は牽制できても意図しない誤りは本人による注意を促す契機となるに過ぎないからである．しかし，他者の眼にさらされることを自覚することによって自ら注意を促すことの他に，「分離」では後の業務プロセスを担当する他者，「承認」では上長によって誤りが発見され，修正されることが期待できる．つまり，誤謬に対しては自律的な注意を促し，あわせて他者による誤りの発見と修正という他律的なチェック機能が働くのである．

なお，監査実務において，統制方法を検討する上で，最も権威ある具体例といえるものに，日本公認会計士協会監査委員会研究報告第 16 号の中の「統制行為の例示」[5]がある．表１の列「統制分類」は，統制行為の例示のうち，購買過程を例に，(1)から(4)の統制手法の分類を試みたものである．また，列「統制目標」では，業務処理統制に関わりが深い正当性，完全性，正確性の統制目標の分類も行った．表１の例を見れば，「分離」，「承認」，「監視」，「規定」のいずれの統制手法も正当性，完全性，正確性の各統制目標を達成するために利用可能であることが分かるであろう．

表1: 統制行為の例示[購買サイクル]

業務区分	統制No.	統制行為	統制分類	統制目標
全般	1	発注，検収，仕入，支払手続に関する諸規程が作成されている.	規程	正当性
	2	発注担当者，検収担当者，物品受払担当者，支払帳票の作成者，小切手・支払手形・振込依頼書などの準備作成者，支払承認者及び会計帳簿の記録者は，それぞれ独立して業務を行っている.	分離	正当性
	3	各業務担当の手続は，適切な権限者の承認を得ている.	承認	正当性
	6	権限を与えられた者以外は，購買に関するマスターファイル，データファイル，プログラム及び関連記録にアクセスできない.	分離	正当性
	7	仕入先のマスターファイル又はリストの変更・更新手続が確立されている.	規程	正当性
	8	購買部門で作成された商品仕入実績及び原材料仕入実績のデータは，商品部及び製造本部での業績分析の際に査閲され，また月次の経営企画会議において，モニターされる.	監視	正当性 正確性 完全性
発注	1	仕入先の選定及び取引条件の承認に関する権限及び手続が確立している.	規程	正当性
	5	注文書は，発注前に適切な権限者によって適切に承認を受けている.	承認	正当性
	6	注文書は，連番によって管理されており，書き損じ又は未使用の注文書が不正に使用されることのないよう保管されている.	監視	完全性
	7	承認済み注文控に基づいて，注文台帳が作成されており，発注，入荷・未入荷の状況が定期的にモニターされている.	監視	正当性 正確性 完全性
検収	2	すべての検収品及びサービスについて，検収後直ちに検収報告書が作成されている. 検収報告書には，検収した物品又はサービスの内容，数量，検収日等が記載されており，適切な権限者によって承認を受けている.	承認	正当性 正確性
	6	検収報告書は，連番により管理されている.	監視	完全性
仕入計上	3	請求書は，発注担当者以外の者が仕入先から直接入手している.	分離	正当性
	6	仕入，買掛金等の計上は，適切な権限者によって承認を受けている.	承認	正当性
	7	検収済品目で仕入計上されているもののうち，未請求のものがないかどうか定期的に査閲し，未請求品がある場合は原因を調査し，発注担当者，仕入先へ連絡するなど適切な処置がなされている.	監視	完全性
支払	1	支払担当者は，買掛金補助簿から作成される支払伝票(支払日，支払先，金額，支払手段の明細)と関連する個々の支払証憑を照合している.	監視	正当性 正確性
	2	支払伝票は，適切な権限者により適切に承認を受けている.	承認	正当性
	6	支払担当者以外の者により，支払伝票は直ちに記帳されている.	分離	正当性
債務管理	1	経理担当者は，買掛金補助簿の残高と総勘定元帳の残高を定期的に照合している. 差異調整は適切な権限者により承認されている.	承認	正当性 正確性
	3	買掛金残高は，定期的に予算対比，前年対比等により増減分析がなされ，増減理由は適時に調査されている.	監視	正当性 正確性

(注)表の業務区分，統制No.，統制行為は，統制行為の例示[5]からの一部抜粋.

4. 基幹情報システムとDBMS

4.1 基幹情報システムの形態

企業が用いるITを利用した基幹情報システムの構成は，業務アプリケーションとデータベース(DBMSを含む)を中心とする構成要素間の関係で捉えた場合，大きく次の2つに分類することができる．ここで例とする企業像は，販売，購買，在庫，生産，会計の5つの基幹業務に情報システムを利用する製造業とする．

(1)分散・独立型情報システム

分散・独立型情報システムとは，各業務に特化した業務アプリケーションとデータベースとを具備した独立性の高いシステムを単位として構成するものである(図1)．業務アプリケーションとデータベースの結合は強く，一体不可分のものとして構成されている．データベース内のデータは各業務アプリケーションがネットワークを介して交換する．各システムは物理的にも分散して配置され，運用主体も独立していることが多い．組織単位で開発・運用されたシステムに多く見られる形態である．

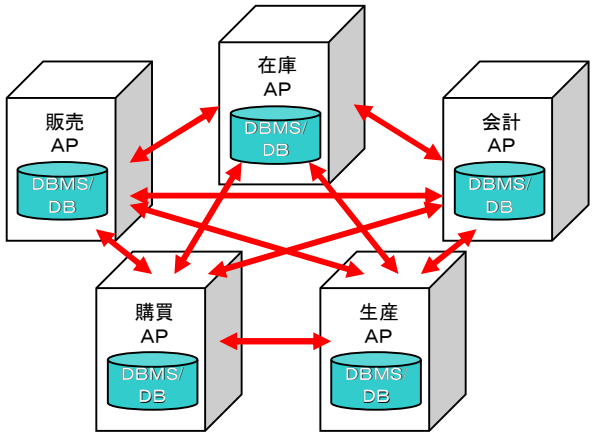

図1: 分散・独立型情報システム

(2)統合型情報システム

統合型情報システムとは，各業務に独立した業務アプリケーションのそれぞれが，共通のデータベースを中心に連携する構成である(図2)．各業務アプリケーションは同一のデータを共有することができる．組織横断的に導入されるメインフレームやERPパッケージに多く見られる形態である．

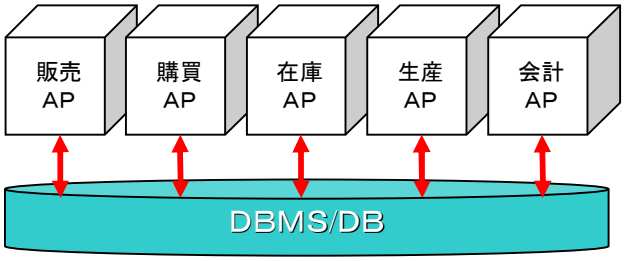

図 2: 統合型情報システム

4.2 分散･独立型情報システムと統合型情報システムの比較

内部統制監査を前提に,分散･独立型情報システムと統合型情報システムの比較を行う．ここで評価の主体となる基準を監査人とする．すなわち，内部統制監査における情報システムの IT 統制について監査を行うにあたり，監査人にとって，監査上の留意点が少ないシステム構成はどちらかを評価するのである．ここで留意点とは，監査人が統制上のリスクを考慮すべき点という意味である.

先ず，両システム構成に差異のある一般的な特徴を整理すると，(1)データの分散と集中，(2)システム運用管理の分散と集中の 2 点が挙げられる．この 2 点から監査人が留意すべき IT 統制目標は何かを検討する．

(1)データの分散と集中

分散・独立型情報システムでは業務毎に独立したデータが分散して存在するのに対し，統合型情報システムでは特定の業務に依拠することのない単一のデータが存在する．一般に前者では，分散するデータの漏れ，重複をなくし，正確に記録することは，後者に比べ困難である．

したがって，監査において，後者と比べ前者についてより留意すべき点としては，完全性，正確性を挙げることができる．

(2)システム運用管理の分散と集中

分散・独立型情報システムでは業務別の組織毎に独立したシステム運用管理が行われることが多いのに対し，統合型情報システムでは情報システム部門などの特定の組織に一括してシステム運用管理が委任されることが多い．前者では，後者に比べて管理運用体制が整備されない場合があり，法令や会計基準，社内規則等への準拠，組織の意図にそった承認手続，アクセス権の管理，障害対策が不十分であることが考えられる．一方，後者は特定の業務に特化した運用管理ができないことから，前者よりも効果的，効率的なサービスの提供が困難な場合がある．また，後者はデータベースの運用の停止が，すべての業務の運用の停止に直結するため，前者よりもシステム全体の稼働率に影響を与えることが考えられる．

したがって，監査において，後者と比べ前者についてより留意すべき点としては，準拠性，正当性，機密性を挙げることができ，前者と比べ後者についてより留意すべき点としては，有効性及び効率性を挙げることができる.

可用性については，前者後者にそれぞれ一長一短があり一概に一般化することは難しいが，前者の運用管理体制の整備に係る懸念が後者のデータベースの稼働率に係る懸念を上回るとすれば，後者と比べ前者についてより留意すべき点に，可用性も加えることができよう.

以上，分散・独立型情報システムと統合型情報システムについて監査人が留意すべき IT 統制目標を表 2 に整理した．表 2 は，統制目標毎に両者を比較して，より留意すべきシステム形態を示したものである．統合型情報システムの方が分散・独立型情報システムよりも留意点の少ないことが分かる．すなわち，分散・独立型情報システムの方が統合型情報システムよりも統制リスクが大きいと考えられる.

表2: 情報システムの形態別IT統制目標の留意点

統制目標		より留意すべきシステム形態
a.有効性及び効率性		統合型
b.準拠性		分散･独立型
c.信頼性	正当性	分散･独立型
	完全性	分散･独立型
	正確性	分散･独立型
d.可用性		分散･独立型
e.機密性		分散･独立型

4.3 DBMS による業務処理統制機能の実装

財務報告の信頼性の確保に直接的に関与する業務処理統制機能の実装について，統合型情報システムを前提に検討を行う．統合型情報システムの方が分散・独立型情報システムよりも業務処理統制に係る正当性，完全性，正確性におけるリスクが小さく，より実効が期待できると考えるからである.

先ず，業務処理統制機能をどこに実装するかを検討する．統合型情報システムの構成要素が，業務アプリケーションとデータベース（DBMS を含む）であることは前述した．業務アプリケーションとデータベースのどちらに業務処理統制機能を実装するのがより効果的であろうか.

業務アプリケーションに統制機能を実装する場合には，各々の業務アプリケーション毎に統制機能を実装することになる（図 3）.

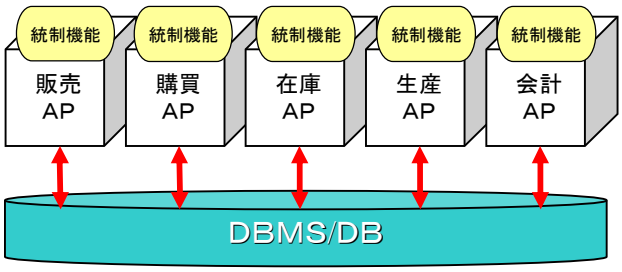

図 3: 業務アプリケーションへの統制機能の実装

一方，データベースに統制機能を実装する場合には，データベースを管理する DBMS に統制機能を実装すればよい（図 4）.

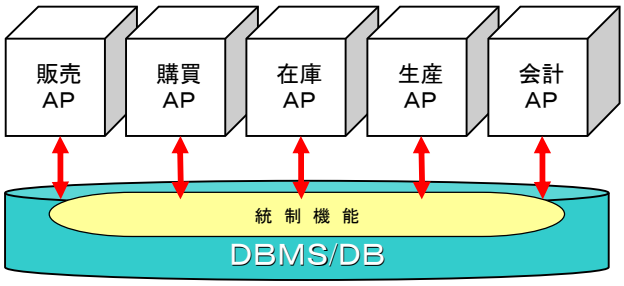

図 4: DBMS への統制機能の実装

DBMS が業務アプリケーションとは独立に中立的な形式でデータを管理するだけでなく，統制機能をも提供することができれば，真に業務横断的で網羅的な統制機能を効率的に実現できる可能性がある.

以下，統合型情報システムにおける DBMS による業務処理統制機能の実装に的を絞り，その要件と課題について検討する.

5. DBMS 業務処理統制の要件と課題

DBMS における業務処理統制機能の要件と課題を明らかにするため，先ず，業務処理統制の 3 つの手法ごとに，データベースの構造とそれに対する動態を明確化する．ここでは，商用データベースや企業の基幹情報システムへの導入事例が多数あることから，関係データベースモデルを前提として検討を行う.

5.1 分離

前述したように,「分離」とは財務諸表の虚偽表示をもたらすリスク行為を実施する者が，1 人でそのリスク行為を完遂できないように業務範囲及び業務権限を分割することであり，このとき業務は，業務プロセスの他，期間を単位として分割されるのであった.

ここでデータベースの対象となる情報は従来の業務において取り扱ってきた情報であるから，構造に関する特段の検討は必要ないであろう. 一方，それに対する操作については検討を要する.「業務範囲及び業務権限」の分割をデータベースの操作に置き換えなくてはならない.

業務範囲とは, データベースのテーブル, 属性, 組，カラムなどを業務単位で一括した範囲であると同時に，操作できる期間も条件に加えた範囲である．業務権限とは，業務範囲内のテーブル，属性，組，カラムなどに対する有効期間を加えたアクセス権限と考えることができる.

従来の DBMS のアクセス権管理の単位はテーブル，属性，組などであり，これらに有効期間まで柔軟に組み合わせる必要のある「業務」という概念を持たない.「分離」を実装するには，業務単位でアクセス権を管理するための新たな権限操作の仕組みが必要である.

要件：業務単位のアクセス管理
課題：テーブル，属性，組，カラム等を柔軟に組み合わせて有効期限と共に一括管理の可能なアクセス権の設定操作

5.2 承認

前述したように,「承認」とは財務諸表の虚偽表示をもたらすリスク行為の一部または全部を実施する者の行為に対して，他者が承認を与えることであり，その承認がなければリスク行為は次の業務プロセスに移行できないこと等の理由により，リスク行為を完遂することはできないのであった.

ここでデータベースの対象となる情報は従来の業務において取り扱ってきた取引情報とは限らないことに注意が必要である．取引情報に加えて，その情報に対する他者による承認の有無というメタレベルの情報が必要になる.

これをデータベースの構造に置き換えるとすれば，例えば，取引情報を対象とする承認という名の属性となろう.

そして取引情報は承認属性を持たなくては，他の業務プロセスでは利用できない．これをデータベースの操作に置き換えるとすれば，当該データの参照，承認属性の付与後に操作されるべき他の範囲（テーブル，属性，組，カラム等）へのアクセスに制限が加わることを意味する.

従来の DBMS のアクセス権の管理は他の範囲（テーブル，属性，組，カラム等）の値を参照してアクセスの可否を決定するものではない. また，範囲（テーブル，属性，組，カラム等）の間に順序関係はなく，ある範囲への入力を終えなければ他の範囲への入力ができないといった制限はない.

「承認」を実装するには，取引情報の承認を表すとメタ属性と，他の範囲（テーブル，属性，組，カラム等）内の値を参照してアクセスの可否を決定する操作の仕組みが必要である.

要件：承認前データのアクセス権の制限と業務手順に従ったアクセス管理
課題：特定のデータに対する承認を示すメタ属性の構造，メタ属性の有無による参照制約及び特定データを参照した後に行う他のデータへのアクセス管理の設定操作

5.3 監視

前述したように,「監視」とは財務諸表の虚偽表示をもたらすリスク行為をその行為者の特定が可能な状態で記録し，記録を保管し，その行為者とは別の者が記録を確認することであり，記録に変更を加える場合には，変更の行為者の特定が可能な状態で変更履歴を残し，その行為者とは別の者が履歴を確認することであった.

ここでデータベースの対象となる情報は従来の業務において取り扱ってきた情報であるから，構造に関する特段の検討は必要ないであろう.また，記録，保管については，データベースの対象となる情報の操作としてではなく, DBMS に対する使用者の要求と結果の記録を指している．これは従来の DBMS の多くが既に実装済みのログ機能である.

強いて課題を挙げるとすれば，行為者を確実に特定することであろう．エンドユーザが業務アプリケーションを通して DBMS にアクセスする場合，DBMS はどのエンドユーザにも同じユーザ ID を付与することがある．DBMS にとっての直接のユーザは業務アプリケーションに過ぎないからである．しかし，これは DBMS がユーザ管理機能を提供できないといった機能上の問題ではない．システムの全体設計においては，アクセス権の管理を業務アプリケーションと DBMS のどちらで実行するかについて性能条件等をも加味して選択を行う．その選択の結果，DBMS ではなく業務アプリケーションにおいてユーザ管理を行うことが多いとすれば，この課題は DBMS のユーザ管理に係る性能等の問題に帰することができると考える.

要件：行為者単位のアクセス管理とログ記録
課題：ユーザ管理の容易性及び性能等の向上またはアプリケーション等が介在するときのユーザの特定

6. まとめと今後の課題

本稿では，ほぼその全容が明らかとなったわが国の財務報告に係る内部統制の監査制度の重要な担い手の一者である監査人の視点から，企業の基幹情報システムの中核となる DBMS が具備すべき業務処理統制機能の要件と課題を検討した．従来の基幹情報システムの形態を分散・独立型情報システムと統合型情報システムに分けて比較し，IT 統制上の特徴を整理した．さらに業務処理統制における統合型情報システムの優位性を前提として, DBMS が実現すべき業務処理統制機能の要件と課題を示した.

本稿における検討はデータベース設計でいえば概念設計の初期段階に過ぎない．今後は本検討を踏まえ，内部統制の観点から考え得る機能要件の検討を進める予定である.

文 献

[1] 企業会計審議会, "財務報告に係る内部統制の評価及び監査の基準並びに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の設定について(意見書)", 2007 年 2 月 15 日. http://www.fsa.go.jp/singi/singi_kigyou/tosin/20070215.pdf

[2] 企業会計審議会, "監査基準", 2005年10月28日.

[3] 企業会計審議会, "監査基準の改訂について", 2002 年 1 月 25 日.

[4] 日本公認会計士協会, "監査基準委員会報告書第 10 号 不正及び誤謬", 2004 年 3 月 17 日.

[5] 日本公認会計士協会, "監査委員会研究報告第 16 号 統制リスクの評価手法〔付録 5〕統制行為の例示", 2003 年 11 月 4 日.