講演論文

内部統制と IT 整備
Internal Control and IT system improvement

末武　透（Suetake, Toru）

日本未来研究センター
TS178051@yahoo.co.jp

Abstract：Spread rumor on threat to continuity of the company if that company do not improve their IT system for adapt New Japanese Company Law so called Japanese SOX Law. This IT system improvement means mainly enforcing their documentation and record management function. Though, author believes as improvement of IT system is highly recommendable for maintain the quality of business process, it is not mandatory to improve IT system for adapt new Japanese Company Law. Even more, activity for try to computerization and improving system management process itself has so many business risks. Author also believes as company could not eliminate risks completely if still some human activities involved. In this paper, author try to explain basic mechanism of internal control, and how SD modeling could analyzes driver of improving IT system management regarding internal control aspects.

キーワード：業務フロー、IT システム統制、チェック・アンド・バランス

要旨：内部統制について、さらには「日本版 SOX 法」として知られる「新会社法」及び「金融商品取引法」について、「日本版 SOX 法に対応できるような、文書管理システムの整備を中心とした IT 整備をしなければ企業は取り潰しに合うので、早急に IT 整備をしなければならない」といった、変な誤解と思われるものがまかり通っているように感じている。文書管理システムの機能充実を中心とする IT 整備は、内部統制が目的とする、「企業の業務品質確保」の上で、必要条件ではあるが十分条件ではなく、そもそも IT 整備のプロセスそのものがリスクに満ちた行為ですらある。さらには、人間が絡む部分がある限り、どのように電算化を整備しようと、完全無欠なシステムなど完成できなく、いわゆる不祥事や業務ミスは発生するものである。本稿では、内部統制の意味について再考察を行い、IT 整備のプロセスに含まれるリスクについて、内部統制との関係から考察を試みた。

1. はじめに

内部統制について、さらには「日本版 SOX 法」（金融庁 2006, [1]）として知られる「新会社法」及び「金融商品取引法」について、変な誤解と思われるものがまかり通っているように感じている。それは、内部統制に合わせた IT 整備をしなければ企業は取り潰しに合うので、早急に IT 整備をしなければならなく、法の執行が 2007 年 5 月 1 日から始まるので、それに間に合わせなければならないというものである。しかし、IT 業界は、この日本版 SOX 法対応のためにとても忙しく、なかなか「日本版 SOX 法」対応のためのシステム整備を引き受けてくれないという。

肝心の IT 業界から、「日本版 SOX 法」対応のために提供されている IT 整備の内容は、確かに内部統制の整備という項目もあるが、「文書管理」システムの整備で終始しているように感じられる。IT 業界に属するコンサルティング会社や関係者の全てが、羊頭狗肉ではないであろうから、IT コンサルティングだけではなく、内部統制に係わる経営コンサルティングも提供されているのであろうが、コンサルティング・サービスのメニューの内容や期間から考えて、とても「内部統制」をきちんと整備するような十分なコンサルティング・サービスが提供され、企業側も確実に内部統制のシステムの整備ができるとは思えない。それに、公示されている法令には、内部統制の基本的要素」に「IT の利用」を挙げてはいるが、「IT の整備」それも「文書管理」のシステム改善など義務付けてはいない（注 1）。何故、このような馬鹿な誤解が生じるのであろうか？筆者には全く理解を超えた狂乱である。

また、文書管理に関する電算化を整備すれば、コンプライアンスとして知られる法律遵守が行われ、さらには、経営者や企業の善意性が確保された上で、企業戦略が効果的かつ効率的に実施できるのであろうか。筆者は、人間が絡む部分がある限り、どのように電算化を整備しようと、いわゆる不祥事やミスは発生するものと考えている。また、電算システムは業務の本質になりえない。そんなこと（電算システムが全てをコントロールすること）をしたら、企業は危機対応もできなく、環境変化にも適合できない。電算化が全てであるかのごとき錯覚がなぜ生まれるのか、筆者には全く理解できない。

本稿では、内部統制の意味について再考察を行い、そもそもの情報システムそのものが、きわめてリスクを多く含んだプロセスであることを示そうと試みたものである。

本稿は、昨年度の発表に続き、内部統制と企業経営の関係について、SD モデルを使って考察を試みたものでもある。内部統制は、企業経営上必須の自律機能であるが、これまでは、必要ではあるがネガティブなもの、つまり、企業成長に直接貢献するのではなく、疎外要因のチェックだけを行っているものと見られ、それゆえに軽視されてきた。また、独立性ゆえに、企業戦略に積極的に組み込まれてこなかった。内部統制は、確かにネガティブで、作業簡略化や作業効率化などの、企業成長にポジティブに機能するものではないが、機能不全を招きかねないしくみの弱点をチェックし、発見する経験や知識、技術の蓄積には無視できないものがあり、近年では、内部統制を企業の内部戦略に組み込み、内部統制による機能チェックを前提に企業内部戦略を進めていくことが主流になりつつある。

文献 2 の論文での著者の主張は、内部統制のメカニズムを、CSR などの、いわゆる企業内部戦略に組み込むことで企業戦略が効果を発揮するが、独立では相乗効果を発揮できなく、内部統制は、単なるチェックやモニタリングの機能しか果たさない。しかし、企業戦略に組み込まれた場合は、戦略そのものに自律機能が加わり、戦略効果を上げることができることを、SD 企業モデルを使って説明したものである。併せて、内部統制の意味や効果についてもモデルで示したと考えている（末武 2006, [2]）。

IT を活用した内部統制機能の強化に関しては、ERP(Enterprise Resources Planning)パッケージ・ソフトなどにあるワークフロー・デザイン機能やワークフロー・コントロール・ソフトなどを活用することが行われている。SAP 社の ERP などでは、自動的に、担当者にすでに与えられた権限と業務プロセスの関係から、業務フローに変更が生じた際に、内部統制の上で問題が発生しそうな箇所を指摘する機能までも持っている。ただ、これらの ERP やワークフロー関係のソフトを使った内部統制機能の検証やデザインと、ST/SD (Systems Thinking/ System Dynamics)を使った内部統制の機能検証とはソフトの性格から違ったものになると考えている。すなわち、ST/SD を使った内部統制の検証は、ドライバーの有効性などのもっと戦略レベルのものになると考えている。本稿では、そのことを最初に検討し、次いで、ST/SD を使い、小規模の IT 整備と内部統制との関係について、その有効な管理方法をめぐる考え方の違いを例に取り上げ、モデル化を行い、シミュレーションによりその強化と費用との関係を考察している。

2. 内部統制をめぐる社会的動き

すでに前稿でも述べたが、エンロン事件など一連の、米国における不詳事件をきっかけに、内部統制機能の強化を企業に義務付ける動きが高まり、サーベイ・オックスレー法(SOX 法)成立など米国では内部統制に関し、かなり厳しい要件を課すようになった。

日本企業は、住友商事事件や大和銀行事件などで暴露されたように、本質的に極めて弱い内部統制機能しか持たず、このことが米国市場での資金調達などで不利な条件として働いてきた。また、内部統制機能に関し、国際化した会計事務所などでは、日本の監査法人が行った会計監査のレベルは国際的なレベルからは一段低く、従って、日本企業の財務報告書は信頼性が一段低いものとして米国などで取り扱われた。世界的には、日本企業は内部統制機能が弱いと見られていた（注 2）（高 2003, [3]）。

米国の SOX 法などの内部統制強化の動きは日本にも取り入れられ、また、国際競争力強化の観点から、日本企業の内部統制機能の弱さを改善しようとする政府の取り組みがなされて、今回の会社法改正になった。企業がグローバル化していく中で、このことはグローバル企業からの要請でもあった。

この内部統制の強化は、企業側から見た場合、企業戦略に生かしていくという肯定的な考えや姿勢の企業はまだ少なく、文書管理の強化だけが要求され、業務が煩雑になったと否定的に捉える企業が多い。特に情報処理の担当者にとっては、「内部統制は単に干渉（インターベンション）を増やしているだけである。」というように取られやすい。

3. 企業経営におけるコントロール・メカニズム

企業をビジネス・プロセスと捉えた場合、ある目的を達するプロセスとそれをコントロールする人間の行為と見なせる。目的やその達成度は、経営指標（KPI: Key Performance Indicator）で計測可能で、その KPI を見ながらビジネス・プロセスを制御していくことになる。

コントロール、すなわち、情報をベースに意思決定を行う作業（肯定、否定、抑制など）は、直接ビジネス・プロセスに組み込まれているものもあるが、内部統制は、通常、大部分は直接的にビジネス・プロセスに組み込まれることはない。従って、経営コントロール・プロセスでは、業務プロセスそのものと、それを包括的にモニタリングする内部統制という 2 重のコントロール機能で制御されたものとなる。イメージ的に、業務プロセスは単体での直線的な流れと捉えられやすく、またなるべく直線的な流れにすることが業務効率性の観点からは最上であるが、通常は内部統制が加わるので、中断箇所もあれば 2 重、3 重の重層的な支配構造にもなってくる。いわば、何段ものブレーキが付いた機械のようなものと考えられる。このことは、業務プロセスは、単体でかつブレーキがない場合、勝手に暴走するものと基本的に捉えられていることを意味している。

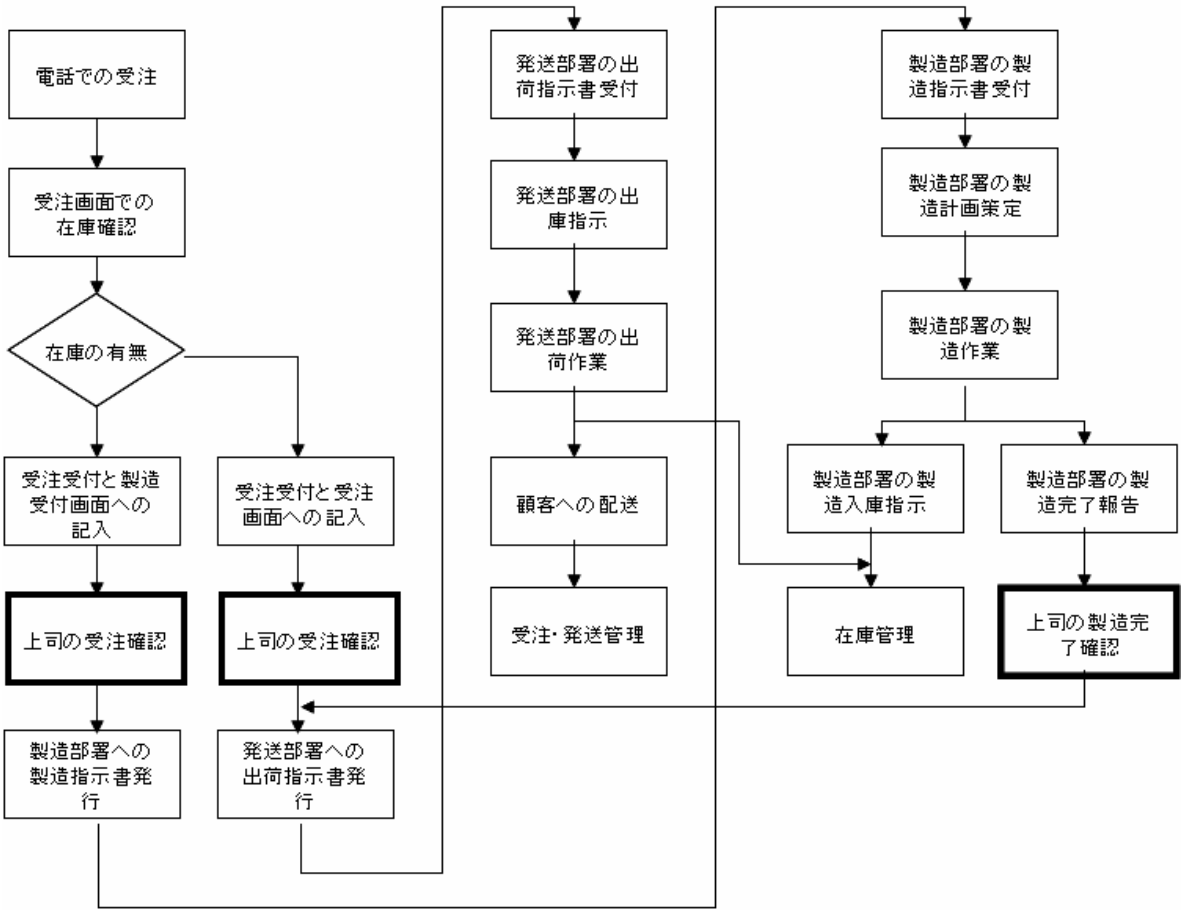

図1　ワーク・フロー設計例（フロー・チャート方式）

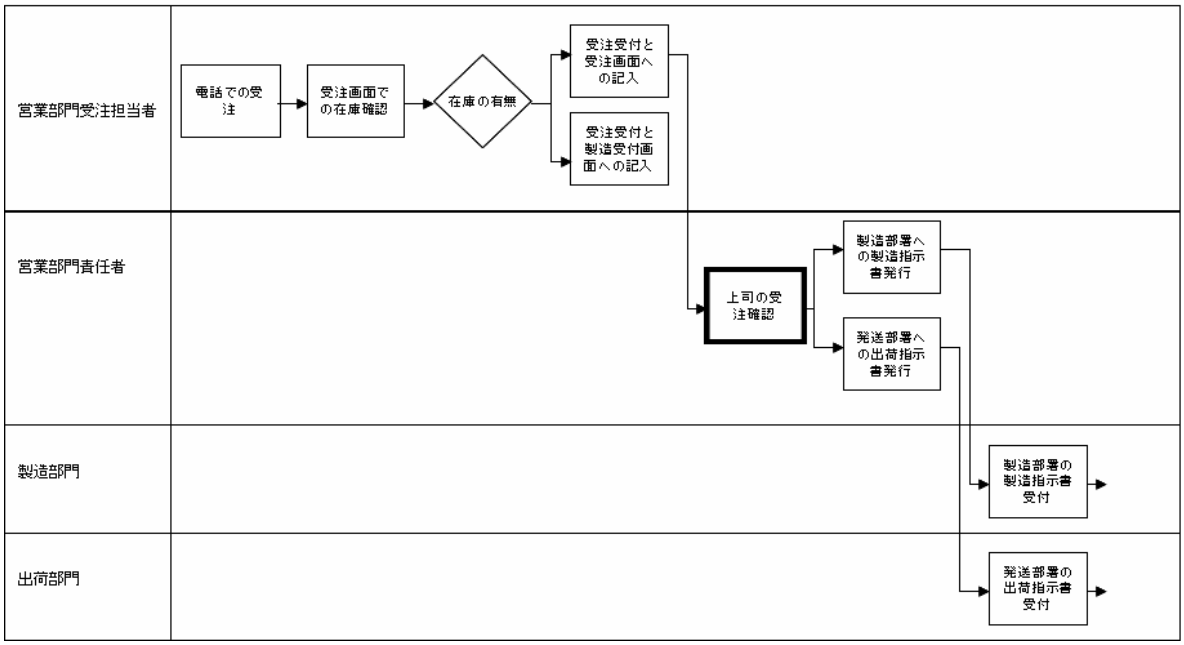

図2　ワーク・フロー設計例（部門別担当者別業務フロー）

直接的に業務フローに組み込まれるものは、チェック機能とバランス機能である。図 1、図 2 は、典型的な受注業務フローの例を示したもので、ここでは簡単に、パートタイマーである受注担当が顧客からの電話で注文を受け、電算機を使って在庫確認を行い、受注を受け付ける（注3)。　在庫があれば出荷指示画面に出荷情報を記入する。在庫がなければ製造指示画面に製造情報を記入する。それを正社員である上司が画面もしくは出力帳票

で確認し、上司の確認の画面入力により出荷あるいは製造を許可するというものである。この業務に対し、内部統制のデザインを行う場合、「上司が確認しているか」の「確認行為」が入っていることがキーになり、この「確認行為」が欠如している、あるいは確認情報が記録管理されていないと多分問題になる。これがチェック・アンド・バランスと呼ばれる内部統制の原則のうちのチェック機能である。すなわち、重要なアクティビティ（業務活動）に関し、チェックにより、「行為とその結果」が確認されていることが重要である。

バランス機能は、図2で、受注担当と出荷担当を同一人物（あるいは同一部署）にしないで、権限や業務を分けることで、受注情報（例えば受注量）と出荷情報（例えば出荷量）を対比でき、差異があれば何か問題があるが、差異がない、すなわち受注通りに出荷されていれば、このことに関しては問題がないことがチェックできる。

IT では、図1のようなフロー・チャートを使った業務フロー図により、チェック機能が存在し、そのチェック機能が業務フローをコントロールする上で有効であることを確認することが古典的なやり方である。アクティビティ（業務活動）とそのアクティビティに対する入出力をどの時点で「確認」することが、業務の流れを効率的に保ち、なおかつ入出力を有効にチェックできるか、を考えながらチェック機能や業務フローを設計する。内部監査などでは、設計されたその「チェック」行為の有効性を確認していく。無駄な箇所にある、あるいは有効ではないチェック機能は削除し、有効な時点での有効な「チェック」機能を付加して、業務フローのコントロール性を維持させる。この図の場合、「受注受付と発送指示画面入力」後、「上司の受注確認」を行っているが、「受注受付」後に「上司の受注確認」を行い、「発送指示画面入力」あるいは「製造指示画面入力」を行うやりかたに変更する方が、チェック機能がより有効ではないか？といったことが議論となる。

一方、バランス機能については、内部統制専門家などは図2のような、担当者や担当部門別に業務が流れる図を描き、確認することが古典的なやり方である。この図で、受注担当者が出荷担当を兼任していない、従ってバランスが保たれているといったチェックを行う。もし、兼任していれば、不正、例えば架空受注と架空出荷、それによる商品横流しがあった場合、チェックがしにくくなる。

それぞれいろんな手法があり、図2では、この変形版とも言うべき産能大式のフローが、企業が証券取引所に上場する場合などで義務付けられているビジネス・プロセスを記載する文書に添付する図として標準的に使われている。この産能大式では、情報の流れと物の流れを分けるなど、もっと分かりやすい表記になっている。

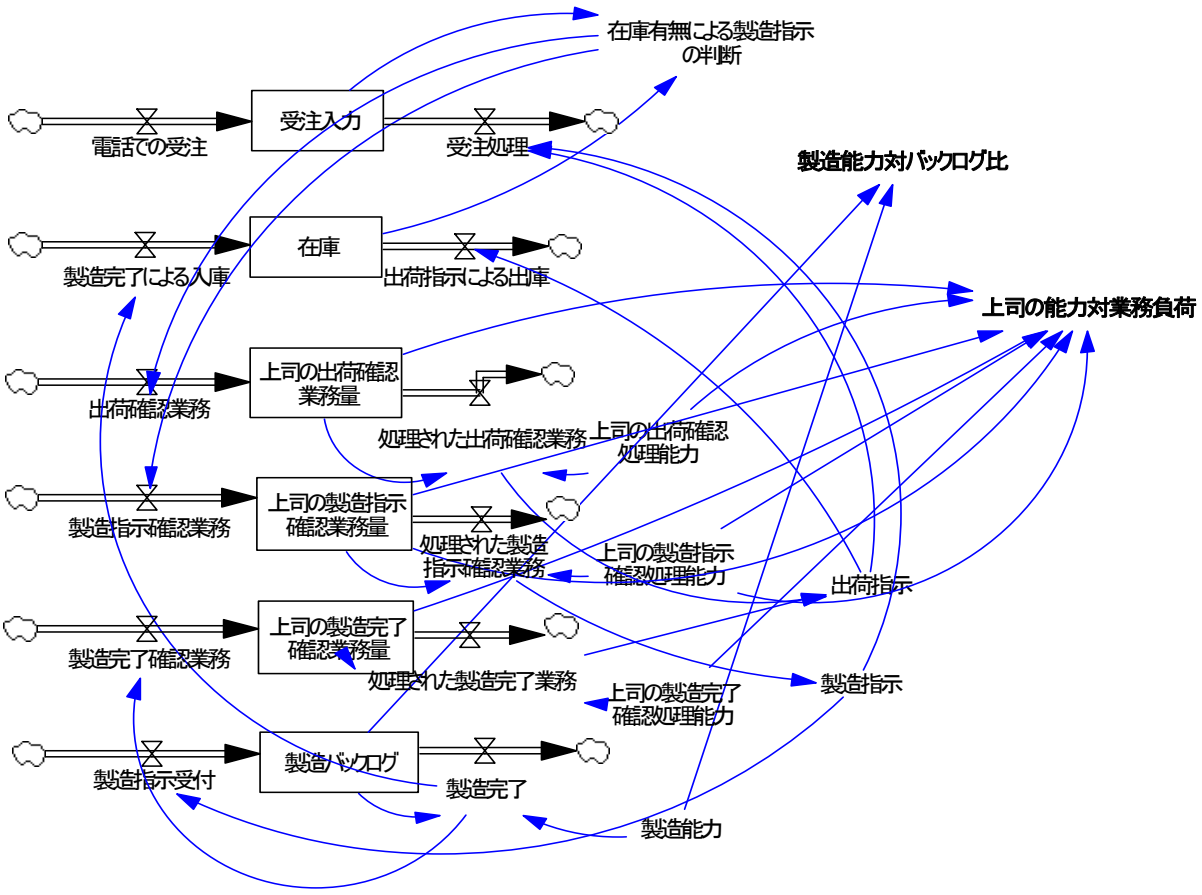

図3　SD モデルによる受注業務例

内部統制では、他にもいろいろ基本原則があるが、大雑把に言えば、チェック・アンド・バランスの原則など

の企業のビジネス・プロセスをコントロールする原則的な機能が組み込まれ、それが機能しているか、それを確認できているかという視点でビジネス・フローを見ている。この内部統制の業務レビューが、ビジネス・プロセス自体をチェックする 2 重目の機能である。それはさておき、ここで内部統制が問題にしているのは、業務のやり方の妥当性であり、それをアクティビティに注目しながら、プロセスに沿って流れを考えチェックしている。ただ、この業務フロー・ベースでアクティビティを見ても、上位の経営あるいは戦略レベルの機能との関係、例えば業績評価指標などから得られる評価結果との関係はあまり明確ではない。社会的責任と企業価値との関係が業務フローから明確化されるわけではない。上位のアクティビティとして、例えば、業績評価指標に関する情報を収集し、分析し、評価しているかどうかをといった事項を、それを実施しているアクティビティや業務フローが存在するかどうかで判断しているだけである。存在し、機能しているらしいと判断されれば、それで内部統制のレビューは終わりである（注 4)。従って、時には木を見て森を見ずになってしまう。

図 1、図 2 と同じようなフローを SD でも記載できるが、それは全く意義がないと筆者は考えている。ジョブ・フローを設計する、あるいは内部統制機能の一部をチェックするソフトが存在し、機能としてはそちらの方がはるかに優れている。ERP にすらこのような機能がある。同じことを SD でモデル化しても、SD には内部統制機能を自動チェックするような機能は現在存在しない。

図 3 は同じ業務を非常に簡単な SD モデルで表現したものである（注 5)。　通常の内部統制のチェックでは、この SD モデルのように、上司のチェック機能を、「出荷指示確認」、「製造指示確認」、「製造完了確認」に分け、それぞれの処理能力を設定し、業務負荷をシミュレーションして、それでチェック機能が果たされていることを確認するといったマニアックなことまでは行なってはいない。図 1、図 2 のようなフローを使い、チェック機能が業務フローの中に組み込まれていることの確認だけで十分としている。

ただ、このチェックのやり方には問題がある。確かにアクティビティはチェックしているが、経営方針や制度、経営戦略などのドライバー（動因）の有効性は、先の図 1、図 2 では確認できない。確認できるのは、そのようなドライバーを受け止め、機能するアクティビティが存在するかだけである。内部統制を実施することの意味は、企業活動を健全たらしめる点（そして、業務品質を保証すること）であることには疑問の余地はないが、何が健全かということに関する定義に関してしては実は確固たる根拠を持たない。ここは内部統制の意味、あるいは限界として議論が分かれる点であるが、極言すれば、現在の内部統制で目指しているのは、対象企業を、標準的な機能モデルが仮想している企業にすり合わせることである。対象企業を標準的なある機能モデルに当てはめ、欠落している、あるいは弱い部分を洗い出し、改善し、仮想されている標準的な機能モデルの企業に変身したら完璧な企業になったと考える。この、仮想されている標準的な企業の機能モデルは、過去の不祥事の経験や優良とされている企業が持っている、そして多くの会社に共通化できそうな統制機能を経験的に体系化しただけで、企業の存在目的や経営の基本戦略などから合理的に導き出されたものではない。仮想されている標準的な機能モデルの企業は確かに内部統制に関しては完璧なのかも知れないが、企業は存在理由や達成目的を持っていて、組織や業務プロセスは効率的かつ効果的にその達成を実現できるように設計されてきたはずである。仮想されている標準的な機能モデルは、当然ながら汎用性ゆえに、後者の観点が欠落し、場合によればリダンダンシーを内包している。さらには、当然ながらこの機能モデルは保守的な体系でもある。従って、経営戦略などドライバーに関する有効性や健全性の事前チェックや、統制が機能し、かつ最大限に効果を発揮せしめるためには対象企業そのものがそもそもどうあるべきであり、そこから考えて内部統制はどうあるべきであるかといった提案をしたくてもできない。「標準的には、あるいは一般的には、このような機能があってしかるべきであり、当社には欠落している。欠落していると機能問題が発生するリスクが高い。従って、機能を整備すべきである」としか提言できない。このやり方では、統制は抑制的な部分では強化されるが、増幅的な部分は皆無である。(注 6)。

ドライバーの有効性のチェックは、SD など経営シミュレーションを使わないと分析できない。先の業務では、ドライバーの例として、費用削減のために権限を持った正社員の数を減らし、パートタイマーで必要な労働力を補うといった企業の方針、あるいは、製造能力を一定とし、外注をあまり使わないようにするといった製造方針がドライバーとして関係してくる。SD モデルを使えば、正社員に要求される能力と実際の業務量に関して問題がないかどうかがチェックできる。このことから、製造能力や上司の業務処理能力との関係で、受注プロセスに課題があるかどうかを判断できる。例えば、製造能力対バックログ比が 5 以上で、顧客から注文を受けても 5 営業日以内に納入できない、あるいは、上司の能力対処理量が 3 以上で、3 営業日以内で受注処理の確認ができないことが、過去の受注データなどを使ってシミュレーションにより示されれば、製造能力や上司の業務処理能力、あるいは承認権限を持った人員数に課題があることが示される。従って、厳密な人員削減方針は、営業成績に不利に働いているので、営業部門では内部統制を保ちながら、もっと権限のある正社員数を増やすことや、品質管理能力を十分確保しながら、外注などを柔軟に使い、製造能力を需要変化に対応させるといったことを提言できる。

このように、SD モデルを使った定量的な内部統制の機能チェックは、アクティビティを追いかけながらチェックするという業務レベルではなく、ドライバーなど、もっと経営レベルの話になるべきであると筆者は考えて

いる。ドライバーが変われば、アクティビティや業務プロセスなどいくらでも変わる。いや、変わらざるを得ない。どう変えるかなど細かい議論は、ジョブ・フロー設計ソフトなどに任せておけばいい話であり、もっと戦略などドライバーに目を向けるべきであると考えている。

このように考えていくと、SD で定量的に解明することが有効な内部統制の項目がかなり明確化され、その項目もかなり多いことが分かる。繰り返しになるが、制度や方針、経営戦略などのドライバーの有効性の解析には、経営シミュレーションによる検証が有効で、既存の内部統制のレビューで実施されているような、「業務プロセス上に製造能力の妥当性をチェックする機能があり、過去には製造能力に関し大きな問題がなかった」といったチェック方式だけでは十分ではない。また、経営シミュレーションを活用した内部統制のレビューによりどのようなアクセルが必要であるかも見えてくると考えている。

4. IT 整備と内部統制

先の議論を念頭に、IT 整備と内部統制について考察する。IT 整備において、一般的に以下の 3 つの分野で内部統制機能が検討される。すなわち、①IT が代替したアクティビティ及び業務プロセスに関する内部統制上のリスク、②IT セキュリティも含めた電算システム運用管理プロセスに対する内部統制上のリスク、③IT 整備（開発）プロセスにおけるセキュリティや業務リスクである。なお、②は、さらにユーザー側の責任に属するリスクとシステム運用管理者側に属するリスクに分けられる。

IT 整備は、③で実施されるものと、②の中で、すでに開発されたシステムを運用管理し、不具合や変更依頼に対応するためにシステムを小規模に改善するといった行為を示している。ただ、③のシステム開発に関する内部統制のチェックに関しては、実際の所、システム開発の現場は戦場であり、時間的制約や実施の困難さなどから、事後的にチェックし、次のシステム開発の際に活用しているだけで、進行中のシステム開発にはあまり活用されていないという印象を持っている。ただ、筆者は IT の専門家ではないので、誤解があればご容赦願いたい。

IT 整備や運用管理の内部統制状況に関し、基本的にはシステム監査という確立した手法があり、このシステム監査の実施により IT 整備上の内部統制状況がチェックされている。健全な電算システムというものが、「設計された通りに機能し、正確かつ迅速に与えられたデータを処理し、中断しないこと」と限定的に捉えるのであるならば、現在すでに確立されているシステム監査でも十分にその任務を果たせると考えている。いろんな事情があることは承知していての乱暴な極言だが、現在の IT システムは完成度や信頼度という点ではまだまだ品質的に劣り、先の、「設計された通りに機能し、正確かつ迅速に与えられたデータを処理し、中断しない」システムを構築することすら完璧に達成できないものである。IT システムは隠されたリスクを多分に含んだ欠陥商品のようなものである。IT 整備とは、この隠されたリスクを多分に含んだ欠陥商品を使うことである。

先にも述べたように、現在のシステム監査での IT 内部統制のチェックでは、企業の成長や戦略実現を考慮しながら、何を戦略的に整備すべきか、整備しないとどのような戦略的なリスクが起き得るかといった議論はされない。この議論については、過去に、「戦略情報システム」というブームがあり、その時には関係者の間でかなり真剣に議論されたことがあるようだが、その後、戦略情報システムのブームが終わり、あまり議論されなくなったように感じている。また、情報優位性がグローバル化や標準化の流れの中であまり価値を持たなくなったのかも知れない。確かに、情報は、知っていても活用できなければ意味がない。

それはさておき、①では、IT が実施している業務処理に、内部統制上の問題がないかを見る。特に、電算化されたために人間のチェックが弱くなっていないか、情報システムがストップした場合の処理に内部統制上のリスクが存在しないか、例外的な事態になった際の処理に内部統制上のリスクが存在しないかがチェックされる。通常、業務を電算化する際には、電算化した場合の効果（費用削減などの定量効果と業務品質向上などの定性効果）と共に、電算化することによるリスクも十分考慮され、対応策も設計されているはずなのだが、それでも多くの企業では、リスクが実際に発生して初めて存在に気付くことが多い。さらには、リスク抑制のためのしくみや制度などが、時間と共に形骸化し、機能しなくなっていくといった時間変化の要素や、いくら完璧そうに見えても、完全なシステムの開発は絶対に不可能ということを忘れがちで電算システムをつい妄信してしまうということもある。バグもあれば、機能が弱いという欠陥もある。業務環境の変化や運用環境、利用環境などによる機能劣化もある。従って、定期的に既存システムを監査することは重要なことである。

SD でこの分野の内部統制を上位レベルでチェックすることに何か貢献できるとすれば、対象業務を電算化した戦略的な理由を、モデルを使ってシミュレーションし、その理由が変わっていないかどうかを確かめることが考えられる。

②、③でも基本的には①と同じで、セキュリティも含めた電算システム管理プロセスやシステム開発プロセスに内部統制上のリスクが存在しないか、例外的な事態になった際の処理に内部統制上のリスクが存在しないか、そして担当者の資質（経験、知識、必要な経験や知識の確保や維持管理、持続性など）がチェックされる。

②IT が行っているアクティビティ及び業務プロセスに関する内部統制上のリスクとして代表的なものは、情報システム化により、処理プロセスがブラック・ボックス化され、経験をベースとする人間の判断とブラック・ボ

ックスの中に組み込まれた判断の間に齟齬をきたすもので、ちぐはぐな人間の判断によるアクションが問題を引き起こすというものである。特に、例外処理に対する人間の柔軟性など暗黙知の部分が情報システム化できなく、例外が発生した場合、事故が発生しやすい。業務プロセスは、環境変化などで少しずつ変化するものであり、情報システム化されることによって業務プロセスが固定された場合、環境変化への対応がスムーズに行かなくなることもある。しかし、多くの内部統制専門家は、業務を出来る限り標準化し、標準化の方法として電算化を行う、その結果、業務レベルでの人間の判断の介入が極小化され、業務プロセスが固定化されるので、業務プロセスが目的としている、「効率的に均一の品質の成果」を生み出すことができると信じている。従って、最初に厳密な業務設計を実施し、決められた手続きを厳格に守らせることで目的としている業務品質が保たれると考えられがちであり、特にIT セキュリティに関しては、多くの内部統制専門家もそのような固定化の方向で管理プロセスを標準化させようとしている。

このいずれも、IT による業務プロセス上の内部統制欠如に関するリスク箇所の発見を、SD のよるモデル化によって行うことは、できないことではないが、非効率的である。先にも示したように、IT セキュリティ業務プロセスも含めた電算システム運用管理プロセス及びIT 整備プロセスをSD でモデル化することにはあまり意味がない。それらは通常のシステム監査やシステム統制手続きに任せればいいことである。しかし、業務方針や制度などのドライバーの有効性と費用対効果の評価など、経営方針や内部戦略に関する事項では SD によるモデル化とシミュレーションは有効である。

さて、このような、業務標準化による業務プロセスの固定化という経営方針は、IT 整備において果たして有効なのであろうか？特に、①の業務プロセスを標準化し、電算化し業務効率を改善すること、極端化すれば全自動化、無人化すること、②のそれをセキリティも含め業務フローをがちがちに固定化し、固定された運用マニュアル通りに運用管理することは果たして有効なのだろうか？　確かに標準化には意味があり、標準化することで効率性も改善され、管理もしやすくなる。ただ、固定化に関しては疑問を持たざるを得ない。多くの場合、それは実務的ではなく、有効でもない。特に電算システムも管理体制もあまり規模が大きくない場合はそうである。まず、どんなに完璧そうに業務プロセスを電算化しても、完全なシステムなどはなく、必ず欠陥があり、その前兆が通常は何かの形で現れる。また、運用における小さな失敗やリスク顕在化は日常的に存在するもので、それを早期に発見し、そこから学習し、その学習成果をシステム改善、プロセスや制度改善に向ける方が有効である。それには、経営者や管理者が積極的に、IT 整備に対する関与を行い、また IT 担当者や業務担当者も、積極的に小さな改善努力を、決められた安全ルールのもとに実施することが有効であると考えられる。そこで、この有効性を確認する SD モデル化を行い、有効性を確認し、有効性を実現させる上での検討項目を考えた（注 7）。ただし、本稿では、IT 整備においてシステムを修正するに際し、修正作業がかえって欠陥を内在させてしまうリスクやメカニズムについては取り上げていない。

5. SD 定性モデル

使っている SD モデルは非常に単純化されたもので、図 4、5 にその定性モデルを示した。一般に、IT 統制リスクは、リスクが顕在化し、被害が発生して、ビジネス・リスクとして認知され、学習される。IT 統制リスクに関する組織学習があれば、対応に関する知識から、システム改善や担当者教育、あるいはマニュアルの整備、改善といった、IT 統制リスクの発生を予防する措置が即座に取られると共に、被害が発生した場合、その被害を最小限に食い止めるコンティエンジェンシー的な措置が取られる。このことで、IT 統制リスクの発生頻度や発生した場合の被害の程度を軽減できる。これがメインのループで、2 重のバランス・ループになっているので、有効に機能すれば安全なしくみである。

さらに、IT 統制リスクに関し、もし経営者の意識が高く、システム監査を十分実施し、これらのしくみが機能するように強制し、また、従業員であるユーザーや IT システム統制リスク管理担当者が、この経営者の姿勢と徹底により十分理解し、IT 統制リスクに対して関心を払っていれば、ユーザーからの IT システム統制リスクに対する早期発見がなされ、うまく組織学習に取り込まれることで、リスク顕在化に対しより適切かつ早期に対応が図られ、組織学習により蓄積された対応に関する知識や能力を活用し、より効果的な予防的対応及び対処的対応が早期的に図られる。

もし、逆で、従業員であるユーザーや IT システム統制リスク管理担当者の関心が低く、早期発見も、適切な早期処置も取られなかった場合は、リスクが顕在化した場合の被害が大きくなり、企業が持っている財務的な IT 統制リスク対応能力では十分に対応できなく、企業は存続の危機に陥ることになる。また、経営者の IT システム統制に関する関心は、業界で発生している IT に関するビジネス・リスクの発生度と関係するとしている。ただ、経営者の関心は政策変数であるので、設定は自由である。経営者の関心は、システム監査などの実施や従業員の認識向上のための研修などによって実現可能で、ここでは、経営者からの指示によるそのような IT 統制強化の活動が図られるとしている（注 8）。

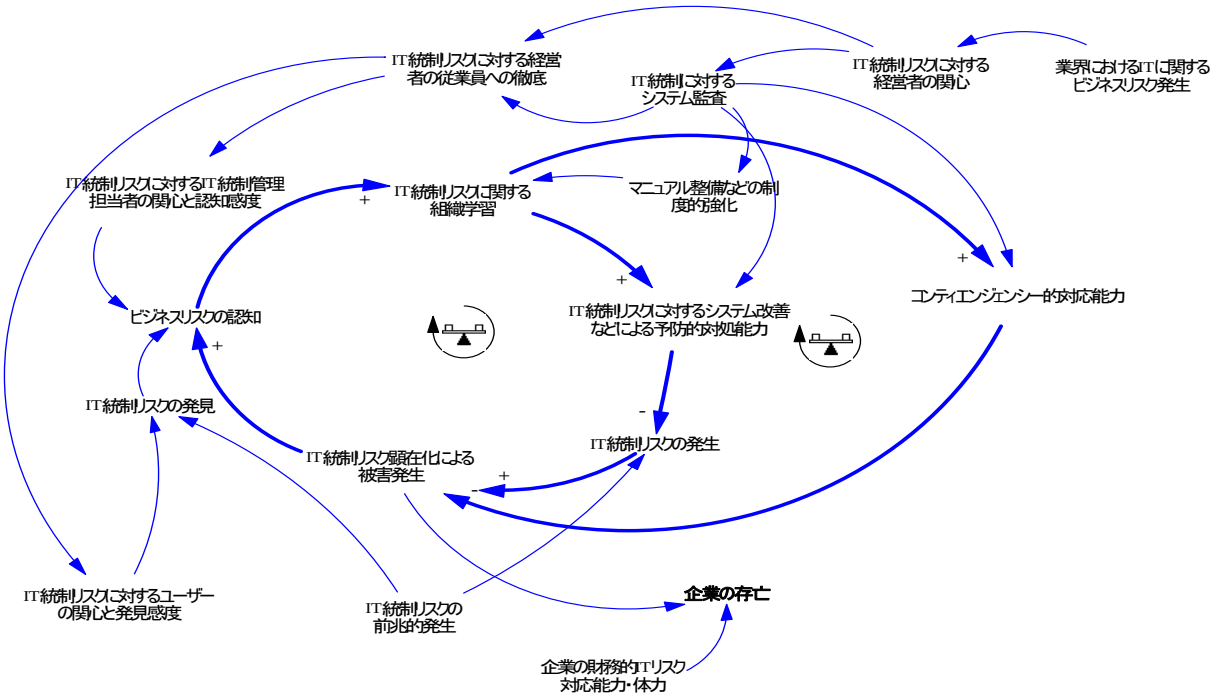

図4　SD 定性モデル

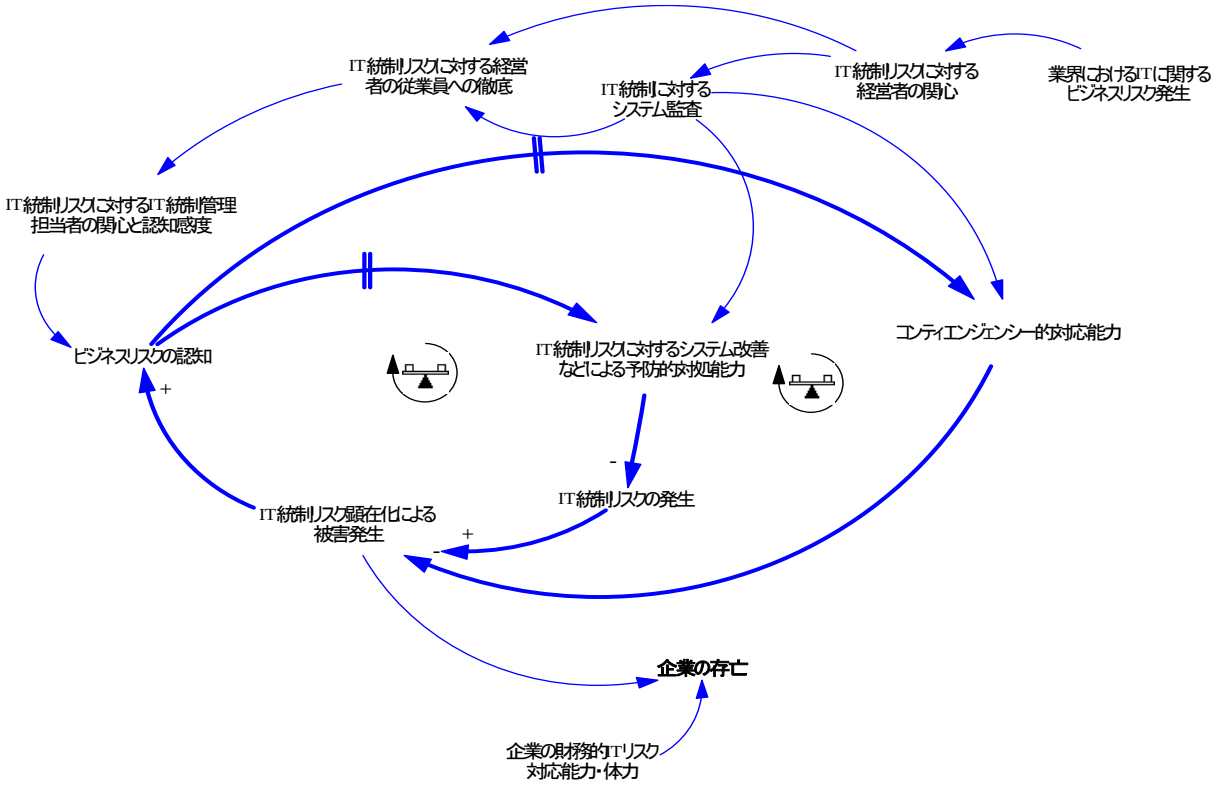

図5　SD 定性モデル

逆に、IT システム統制ががちがちに固められてしまった場合は、ユーザーの関心と発見感度が IT 統制リスク早期発見に繋がらなく、また IT 統制リスクに関する組織学習もないので、IT 統制リスクが顕在化し、被害が発生し、ビジネス・リスクとして認知されて初めて、予防的措置及び対処的措置が時間遅れで行われると考えられる。これは、アウトソーシングなどで IT システム運用・管理業務や電算処理業務を一括して外注している場合などに起きやすい状況である。図 5 にその定性モデルを示した。このような場合、経営者が IT 統制リスクに関心を持ち、その徹底を図ろうとしても、せいぜい IT 統制管理者に対する意識向上や IT 統制に対するシステム統制を実施できる程度で、通常は、IT 統制リスクが顕在化してはじめて、経営者も危機感を持ち、また、システム監査

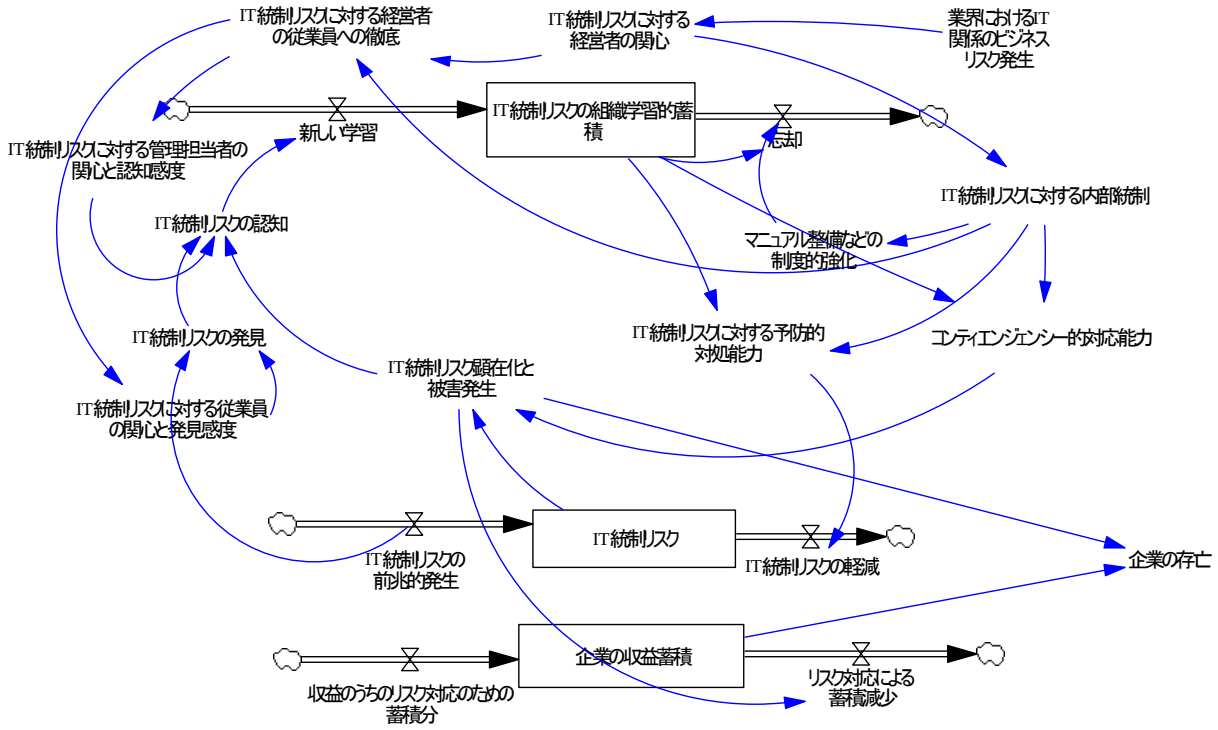

図 6　SD 定量モデル

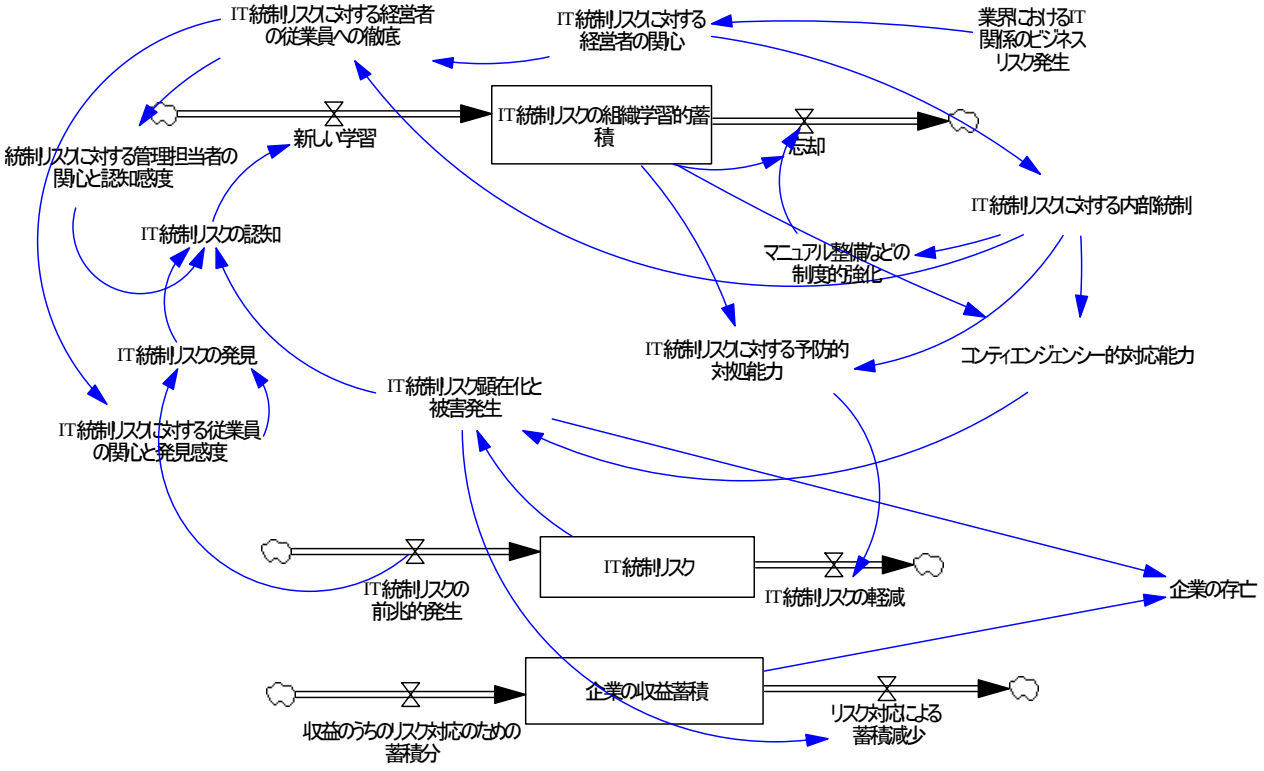

図 7　SD 定量モデル

などでの改善提言を受け入れるので、IT 統制リスクに対して取られる措置（予防及び発生後の被害低減措置）は、時間遅れで対応され、組織学習があり、即時にこまめに対応される場合と違ってくる（図 5）。

図 6 は図 4 の定量モデルで、ここではモデルを単純化するために、企業のリスク対応財務能力を、企業の収益から一定の割合で蓄積されるとしている。また、組織学習も予防的対応とコンティエンジェンシー的対応には分

けないで、一律に扱っているが、分けた方がより正確である。ここでは、モデル単純化のために特に区別はしていない。

図 7 は、図 5 の定量モデルで、組織学習による対応がなく、ユーザーからの早期 IT 統制リスクがなされないことだけが図 6 との違いで、あとは基本的にパラメーターも設定値も同じである。早期発見がなされないことで対応が遅れることを遅延ループで表現している。

6. SD 定量モデルによるシミュレーション

まず、感度分析のために、図 6 のモデルによるシミュレーションで、ユーザーの関心と発見感度を変化させてみた。モデルの構造から、当然といえば当然の結果であるが、ユーザーの関心と発見感度を低く設定すると、図 7 のような遅れを伴うことはないが、シミュレーション結果は、IT 統制リスクの組織学習的蓄積が高まらず、IT 統制リスクに対する予防的措置もコンティエンジェンシー的な措置も効果的にすぐには機能しなく、リスクの顕在化が少し多発する。

感度分析の結果が妥当だったので、ユーザーの IT 統制リスクに対する関心と感度をやや低め、担当者の関心と認知度を中、経営者の関心度をやや高めに設定し、これをベースラインとした。そして、図 7 の定量モデルによるシミュレーション結果と比較した。図 6 と図 7 の違いは、図 7 のモデルでは、組織学習による早期の IT 統制リスク対応が存在することと、ユーザーによる IT 統制リスクの早期発見がやや低めながらもあるかないかだけで、図 7 では、その早期対応がないので、内部統制があり、システム監査などが実施されていれば、リスクがある閾値を超えた場合に、リスクが発見され、やや早期対応（ここでは 6 週間）、なければ、いろいろ専門家に依頼するので 12 週間遅れの対応になるとしている。その他のパラメーターは全く同一である。

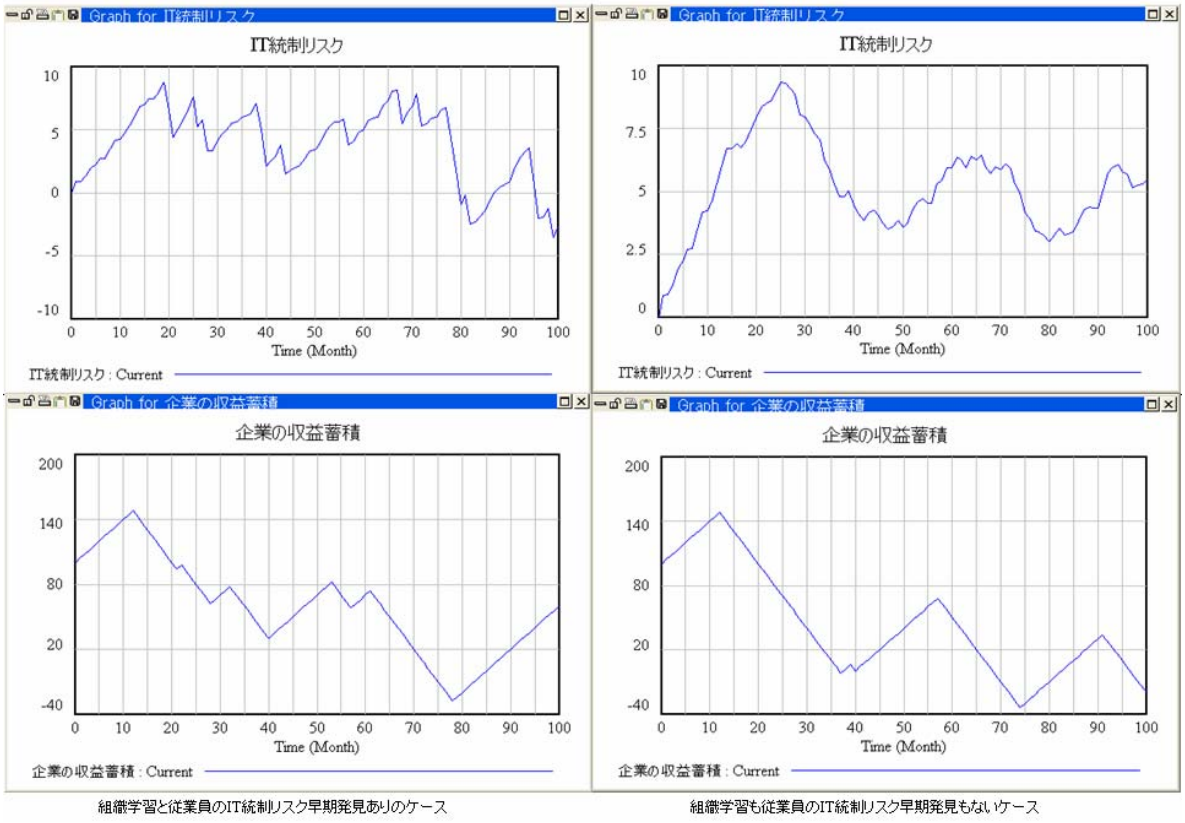

図 8　2 つのモデルによるシミュレーション結果

図 8 に 2 つのモデルのシミュレーション結果を示した。IT 統制リスクの発生は乱数を用いているので、厳密には 2 つのシミュレーション結果による IT 統制リスクは同じではないが、組織学習とユーザーの IT 統制リスク早期発見がある場合の、IT 統制リスク（図 8 左）は平均約 4（やや低め）で抑えられ、ない場合（図 8 右）は平均約 6（やや高め）になる（注 9）。また、リスクが顕在化しても、組織学習とユーザーの IT 統制リスク早期発見がある場合は、一気にリスクが加速化することはない。

企業の収益蓄積では、一度でもゼロを割ったら、赤字補填のケースだが、組織学習とユーザーの IT 統制リスク早期発見がある場合は、IT リスク対応のための収益蓄積の減少はより緩やかである（注 10）。

このことから、経営者が業界などで発生している IT 統制リスクに関心を払い、まだ自社で発生していないリス

クにも注意を喚起し、システム管理者だけではなく、ユーザーにも、IT 統制リスク発生の前兆状態に注意を喚起させ、予防的処置や対応的処置を早めに決めておくことが有効であることが示される。経営者はまた、システム管理者だけではなく、ユーザーの意識も高め、IT 統制リスク発生の前兆状態の発見から、早期に IT システムの改善や運用管理の改善を早期に実施することが有効である。

このように、SD モデルは、IT リスク統制をモデル化するに際しても、業務プロセスそのものではなく、むしろ IT リスク統制に影響を与えるドライバーの分析に有効であり、IT 統制リスクそのものをプロセスとして表現しても、あまり有効ではない。

IT リスク統制に関係して、近年の SD 研究では、リスク現在化のメカニズムがいろいろ追及されている。例えば、IT リスク統制で近年頻繁に発生する情報漏洩に関し、漏洩者の犯罪にいたる心理をモデル化し、どのような対策が有効なのかといった研究が実施されている。先のモデルに、このような視点を取り込んだモデルや解析も、ドライバーの分析として有効と考えられる(Sawicka 2003, [4])。

注釈：

注 1) 2006 年に公示された金融庁、「財務報告に係る内部統制の監査（案）」には、「IT に係る全般統制の不備は、それ自体が財務報告の重要な事項に虚偽記載が発生するリスクに必ずしも直接に繋がるものではないため、業務処理統制が現に有効に機能していることが検証できているのであれば、全般統制の不備をもって直ちに重要な欠陥と評価されるものではないことに留意する。」と注記されている。また、2007 年 1 月に産業経済省から公表された、「システム管理基準追補版－財務報告に関する IT 統制ガイダンス案」を見ても、日本版 SOX 法導入に際して、特に従来のシステム監査基準やシステム管理基準の内容を大きく変えるような内容や項目は発見できない。既存の情報システムが従来のシステム監査を受けて、信頼性や安全性などが保障されているのであれば、日本版 SOX 法導入に合せるために、特に大きな情報システム改善が必要とは考えにくい。しかしながら、従来のシステム監査を受け、信頼性や安全性に問題があると指摘されるような低品質の情報システムであれば、それは情報システム自体の欠陥であり、日本版 SOX 法導入が決まったからどうのこのという話以前の事項である。また、IT 統制の整備は財務報告の信頼性に係るものに関してのみ要求されていることも注意すべきである。

注 2) 日本企業の財務報告書は信頼性が一段低いと見られたのは、当時の日本の会計制度が簿価主義で、米国では標準的であった時価主義ではなかったので、日本企業の財務報告書が、企業資産を正確に表していると見なされなかったことが一番の原因である。内部統制機能が弱いと考えられたのは、一連の日本企業の米国における不祥事の発生が、(1)経営方針のあいまいさ、(2)経営方針の従業員への不徹底さ、(3)上司と部下の業務実施上にみられる実際の権限行使や業務内容、権限委譲、責任行使のあいまいさ、(4)上司の部下への業務指示のあいまいさ、(5)上司の部下に対する業務チェックのあいまいさ、(6)上司の責任の取り方に対するあいまいさ、(7)事故や不祥事に対する原因追求や内部監査が厳密に実施されなく、また実施されても、その成果が経営改善に反映されていないこと、などから発生したものと理解され、内部統制が不在であるとみなされたからである。特に、事故や不祥事が発生すると、上司は、責任を取って辞任し、その後、厳密な原因追及と業務改善や事故や不祥事に関与した部下への厳密な懲戒、経営システムの改善が見られないという日本的な責任の取り方が米国人には理解されなかった。また、監査人が馴れ合い的な内部監査しか実施していなく、内部監査により常に業務改善がなされていない点も日本企業には内部統制が不在であるとしか理解されなかった。「まあまあ」、「ほどほど」という日本的な感覚は、国際ビジネス社会には通用しない。

注 3) 受注業務の例として挙げたもので、完全に全部の受注業務を記載したものではない。特に、図 2 については、不完全であり、本来であれば、製造プロセスや出荷プロセス、製造後の出荷に際しての受注情報の確認作業などが必要であるが、この図には記載していない。

注 4) ここでは明確化するために業務プロセス上のチェック・アンド・バランスにしか触れていないような記述になっているが、誤解を避けるために少し詳しく述べると、内部監査や内部統制のチェックでは、実務的に必ずしもこのような業務フローをベースに本文中に述べたようなことをチェックしているわけではない。このようなやり方は非効率的であるので、COSO (トレッドウェイ委員会組織委員会) の ERP (Enterprise Risk Management − Integrated Framework) 統制フレームワークなどをベースにした統制モデルを基に、企業の業務プロセスが内部統制の観点から標準的に具備すべきビジネス・リスク管理に係る機能リストを用意し、その機能に対するチェック項目を挙げ、チェック項目に沿って、そのチェック項目が、業務フローの中にアクティビティとして組み込まれていて、実際にその組み込まれたアクティビティが機能していることを、現場での観察やヒアリング、活動記録、サンプリング・テストなどの手法によって確認するというやり方が採用されている。いきなり業務フローで制御性を見ているわけではない。

また、業務フローのチェックにしても、標準的な業務の流れと、標準から外れた業務の場合に分け、その上で業務フロー上のコントロール機能をチェックしている。特に、標準から外れた業務に関しては、リスク顕在化の可能性が高いので、より重点的にチェックされる。

業務フローによるチェックが最終的なチェックになるのだが、このように記載すると下位の業務レベルのアクティビティのチェックだけに終始するように誤解を招きかねない。しかし、下位の業務レベルのアクティビティのチェクだけではなく、上位レベルのアクティビティの検証、例えば、「経営陣の経営に対する姿勢として、経営方針を明確化し、それをさまざまなチャネルや手段を使って従業員に徹底させているか」などのチェックも行っている。さらには、「業務プロセスに関する業績評価指標を明確化し、明確化された業績評価指標で業務プロセスの効率性などを評価し、業務プロセスの効率性を改善する必要があれば修正しているか」などもチェックしている。後者では、業績評価指標を明確化する活動が存在することと、その活動で明確化された指標による評価を企業が実施しているかどうかをチェックしている。しかしながら、企業の業績がどうであるかといった業績評価業務そのものは業務対象外である。このように、あくまでも、業務成果を生み出すメカニズムに対して、その信頼性を業務品質の観点からチェックしているという点に注意してほしい。

注 5) これも SD モデルの例として挙げたものであり、これが SD 的な意味で適正に図 1、図 2 の業務を表しているというわけではない。SD モデルは業務フローのモデルではないし、業務フローを SD で描いても意味がない、むしろ、業績評価指標、あるいは業務負荷などを、シミュレーションを使って見ることで、翻ってドライバー評価のために使うべきであるとしてこのモデル例を挙げたものである。評価したいドライバーが違えば、SD モデルや SD 記載方法も違ってくる。

注 6) この部分は極論を述べているであり、内部統制を標準化する流れになることは効率性や実務性の上から十分理解できるし、筆者にはこの標準化の流れに反対する意図はない。また、内部統制担当者がブレーキをかける役割に徹するのは、機能分担や専門性を高める上で当然であり、ブレーキをかけるために保守的に考え行動する必要があることも理解している。本稿では、内部統制の標準化の流れの一方で、このような問題や議論も存在するのだということを指摘しているだけである。意図に関し誤解を招きかねないのでコメントをしておきたい。

注 7) ここではすでに③でのシステム開発により①が完成し、業務が標準化され、電算化され、②に移管され、②が IT 整備ということで問題になるとして、②での業務改善に与えるドライバーの 1 つを取り上げ、議論している。基本的には IT 整備に係らず、他の業務プロセスの改善についても言えることである。ただ、標準化や IT 整備、それによって達成された業務効率化、管理効率化、あるいは内部統制を否定して、それらを無視して小規模改善を推進せよと主張しているわけではない。

注 8) 優良企業では、自社にまだ IT 統制リスクが発生していない場合でも、他の業界や外国などで IT 統制リスクが発生した場合、そのような情報を適切にキャッチして経営陣に提案し、自社の組織学習に取り込んでいるが、このモデルではそこまでは考えていなく、経営者からの指示によるとしている。また、定量モデルを単純化するために、ここでは IT 統制リスクに対応できる企業の財務能力のフローを一定としている。

一般的には、貸倒引当金で準備されている内部留保資金が、全てのビジネス・リスク対応財務能力と見なせるが、経営者の判断で、資産の一部をさらに当てることも可能である。

注 9) ここでは、10 段階評価を用いた。また、IT 統制リスクは、0 から 1 までの乱数を発生させ、その蓄積が 5 以上（中）になった場合にリスクが顕在化するとしている。ここでも、IT 統制リスクは、10 段階評価で行っている。ここで、IT 統制リスクをストックにより 0 から 10 まで高まる変数としているのは、重大な IT 統制リスクが直ちに顕在化することは一般的になく、小さな IT 統制リスクが前兆的に発生し、それを放置して初めて重大な IT 統制リスクが顕在化するという仮説に基づく。

注 10) ここでは、IT 統制リスクのコントロールには、ユーザーの関心や早期発見と、有効な組織学習が重要であることの説明を中心にするために、財務的な対応能力についてはかなり省略している。ただ、実務的に用いる場合には、財務的な説明は重要であるので、このモデルを参考に企業に適用する際には、財務機能をきちんとモデル化することが望ましい。

参考文献：

[1] 金融庁、企業会計審議会、「第 15 回内部統制部会配布資料」、2006
なお、この配布資料は http://www.fsa.go.jp/singi/singi_kigyou/siryou/naibu/20061120.html から入手できる。日本版 SOX 法は、この資料が対象にしている「金融商品取引法第 24 条の 4 の 4 第 1 項に定める上場会社等における内部統制報告書の提出義務、及び、同 193 条の 2 第 2 項に定める提出する内部統制報告書に対する公認会計士又は監査法人による監査証明の義務」を示していると本稿では定義している。
その IT 統制に関するガイドラインは、
経済産業省、「システム管理基準追補版－財務報告に関する IT 統制ガイダンス案」、2007
http://search.e-gov.go.jp/servlet/Public?CLASSNAME=Pcm1010&BID=595207003&OBJCD=100595&GROUP=から入手可。
古いものは、
経済産業省、「新システム監査基準」、2004、経済産業省
経済産業省、「新システム管理基準」、2004、経済産業省
経済産業省、「情報セキリティ管理基準」Ver.1.0、2004、経済産業省
なお、記載した URL は 2007 年 3 月 1 日時点のものである。
[2] 末武透、「ビジネス・プロセスにおける内部統制の重要性」、システム・ダイナッミクス・ジャーナル、2006
[3] 高巌、「コンプライアンスの知識」、日本経済新聞出版社、2003
[4] Sawicka, A, et al. “A System Dynamics Model of an Insider Attack on an Information System”, Proceeding of ICSD 2003, New York, System Dynamics Society
[5] あずさ監査法人、「内部統制ガイドブック」、東洋経済新報社、2005
[6] 土田義憲、「内部統制の評価モデル」、中央経済社、2006
[7] 土田義憲、「業務プロセスから見た内部統制実践マニュアル」、中央経済社、2005