日立グループが考える内部統制成熟モデルとリスクマネジメント基盤

Basic Model for Risk Management Based on Internal Controls

伊藤 泰樹 Yasuki Ito
青山 ゆき Yuki Aoyama
小宮 文男 Fumio Komiya
谷岡 克昭 Katsuaki Tanioka

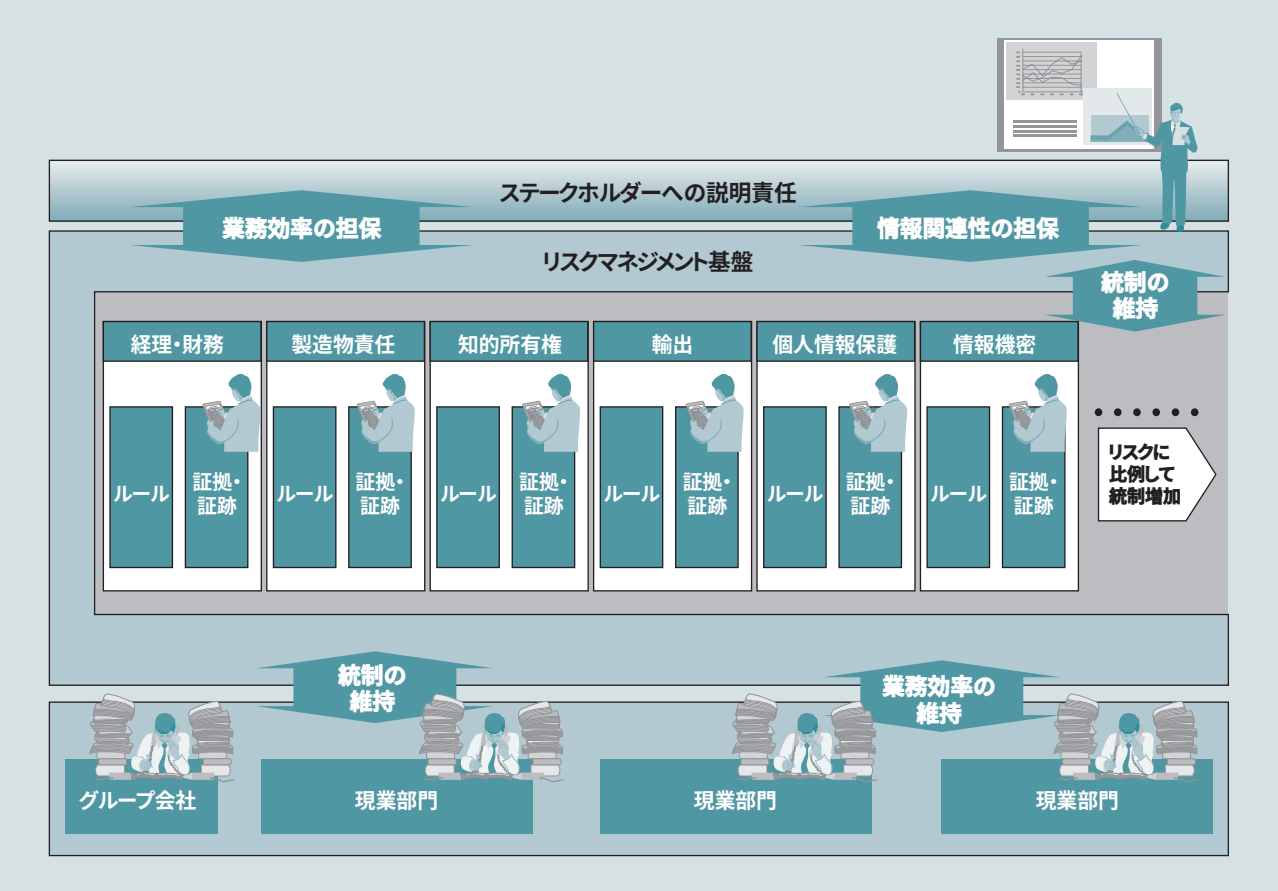

図1　業務を実行する際のリスクマネジメント基盤
業務リスクの中心となるコンプライアンスの維持は，それぞれを支えるルールと証拠・証跡（エビデンス）の確保と，それらの維持する活動を支援する。

商品やサービスを販売して利益を得るだけでなく，金融商品取引法や個人情報保護法などコンプライアンス（法令順守）の維持はもとより，さまざまなステークホルダー（利害関係者）への説明責任を果たすことが企業にとっていっそう重要となってきている。

特に内部統制を成熟させていくことは，業務を通して発生するリスクを回避するために業務を標準化（規則化）し，維持するだけでなく，新たに発生したリスクを業務へ反映できるようにするリスクマネジメントの実現と同じ意味を持つ。こうした内部統制の成熟とリスクマネジメントを実現するために，ITを活用し，情報のガバナンスを徹底していくことにより，企業価値の向上に結び付けることができると日立グループは考えている。

1. はじめに

金融商品取引法や会社法などは，企業に対して，財務報告の正確性を維持し，またそれ以外の法令も順守したうえで，企業活動における効率性や効果を確保することを求めている。

まず，財務報告やそれ以外の法令順守には，その企業活動の周辺に存在する法令を整理し，その法令を順守することができるように，企業内の業務規則や業務手順を整備する。それらを従業員に徹底し，徹底できているかどうかを評価するとともに，不備があれば改善する。これらのプロセスを維持することで内部統制が確立できたということができる。

しかし，それぞれの法令に対して，それぞれの規則・手順

を確立し，展開・監査するということは，同じような内容の確認をしたり，確認・監査する作業を増加させたりすることとなり，企業活動の効率を阻害する要因となる。

これらの法令にかかわるリスクは，企業活動の説明責任を求めることから，企業活動の説明に足る証拠・証跡（エビデンス）を確保し，それらを業務の中で一元的に取得，保管していく仕組みが必要である。この証拠・証跡を確実に取得・維持し，企業活動を最適に運営する仕組みや情報システムがさまざまなリスクに対する耐性を備えた組織であり，企業であると言える。

ここでは，日立グループが考える内部統制の成熟とリスクマネジメント基盤について述べる（**図1**参照）。

2．内部統制の成熟とリスクマネジメント基盤

2.1 内部統制の成熟と，それを支える基盤の要件

金融商品取引法の求める財務報告にかかわる内部統制を構築するために，経理・財務の業務を中心に取り組むと，次のような状況が生じる。まず，構築した統制を説明することができない。そこで，説明できるように，作業の依頼・受託の承認，処理の承認などの証拠・証跡を取得するような業務を追加する。しかし，付け焼き刃の過剰な統制では，統制したとおりに仕事ができない。リスクをコントロールしようとして統制を構築したはずが，新たなリスクを生み出す結果となるのである。

具体的な例では，業務の中で発生した売上などのデータはエラーチェック，承認，マスター照合を経た処理ののち，証拠・証跡を突き合わせたうえで監査，保管される。さらに，営業部門の受注データは，出荷部門へ渡され，販売データとして処理されるのである。ここでは，単に営業数値だけでなく，取引先が「輸出管理の観点」などさまざまなリスクに対して妥当か否かチェックすることが必要になり，作業部門ではチェックの負担と内部統制の維持のジレンマに陥る。

内部統制の成熟には，業務を通して発生するリスクを回避できるようにするために業務を標準化（規則化）し，それを維持するだけでなく，新たに発生したリスクを業務へ反映できるようにすることである。つまり，全体を通したリスクマネジメントの実現と同じ意味を持つのである。

リスクを排除するために，業務プロセス間でのデータのやり取りによる「突き合わせ」，「取引の正当性」の承認，それ以外に間接的な情報の監査などの業務がなされている。これらを通常業務の延長で運用し，新たに発生した問題や課題を統制・維持していくことを実現するのがリスクマネジメントの基盤である。

これらリスクマネジメントを補助するIT基盤の要件を次に挙げる（**図2**参照）。

（1）日常の業務

（a）日常での入力チェックだけでなく，周辺業務との矛盾を示すことが可能な入力時の予防的な検査

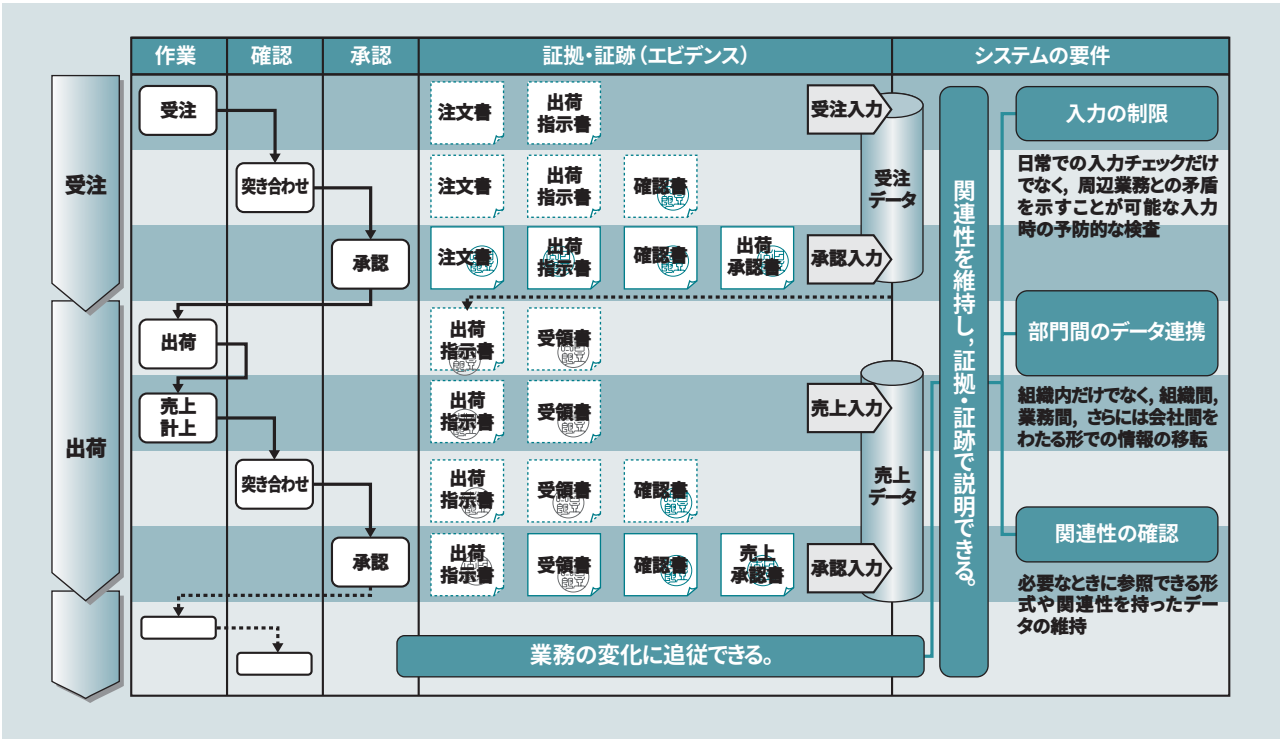

図2　業務のリスクを回避するための証拠・証跡の維持と，それを支えるシステムの要件
作業の進行に合わせて処理するだけでなく，それらの業務を説明するために必要な証拠・証跡が取得される。それらを突き合わせたり，管理者によって確認されたりすることで業務の正当性を維持する。そのために，入力を制御・制限し，部門間で扱われるデータを標準化していくこと，さらには，業務の改善，リスク対策などにより，変化に追従できるようにする必要がある。

（b）組織内だけでなく，組織間，業務間，さらには会社間をわたる形での情報の移転の自動運用
（c）業務で発生した情報の「誰が，いつ，何を」を記録する形での網羅的な保管
（d）規則や規定の変化，不備に追従できる業務の変化への即応

（2）業務の正当性の説明
（a）進行，逆進行のテストに耐える関連性の維持
（b）保管中の改ざんや誤廃棄などが発生しないような情報の維持や「誰が，いつ，何を」の記録採取による正当性の維持
（c）必要なときに参照できる形式や関連性を持ったデータの発見，データの所在の明白性など，保管期間内の的確な参照
（d）関係したシステムで発生したデータの矛盾を提示するなど，システム間のデータの整合性監査
（e）権限分離やシステム間・業務間の関連性の説明
（f）監査結果の不備や課題のフィードバック

2.2 リスクマネジメント基盤を支えるITアーキテクチャ

これらの要件を満たしていくためのITアーキテクチャを**図3**に示す。主に，次の三つの階層で考えていくことができる。（1）業務処理の中で必要な統制処理を促すBusiness Process Management層，（2）それらの統制に基づく処理を履行するProcedure層，および（3）処理した結果や過程を保管するRecord Keeping層である。

特に，意識が必要になってきているのは，証拠性を持った情報を保管していくためのRecord Keepingと呼ばれる層である。この層で保管されている情報が企業活動の説明責任を維持するための基盤となっているばかりでなく，部門間でデータを連動させるなどの業務全体の最適化を促す仕組みとして機能するのである。

3．内部統制の成熟を図るシステムの要件

ここまで述べてきた要件をシステムとして実現していくためには次の要件が必須となる。

日常の業務の中で処理・実行される行為については，「規則・規定」の徹底とそれらの日常的なモニタリングの仕組みを構築することによって内部統制が確立されていく。これらを確立するための鍵となるコントロールの方法に「照合/調整・承認/決裁・職務の分離」などがある。このコントロールが企業の業務で有効に運用されることが内部統制を維持する仕組みである。これらの維持ができ，さらに維持していることが体系的・網羅的に説明できる状態が内部統制の成熟している状況である。内部統制を成熟させるためには，次のようなステップで検討していくことが求められる（**図4**参照）。

金融商品取引法などの監査への対応で，それぞれの業務はレベル3である「規定はあるが，改善のプロセスに向けた反映の流れが確立していない状態」には達することができる。それ以上のレベルに到達するためには，全体のバランスを見た

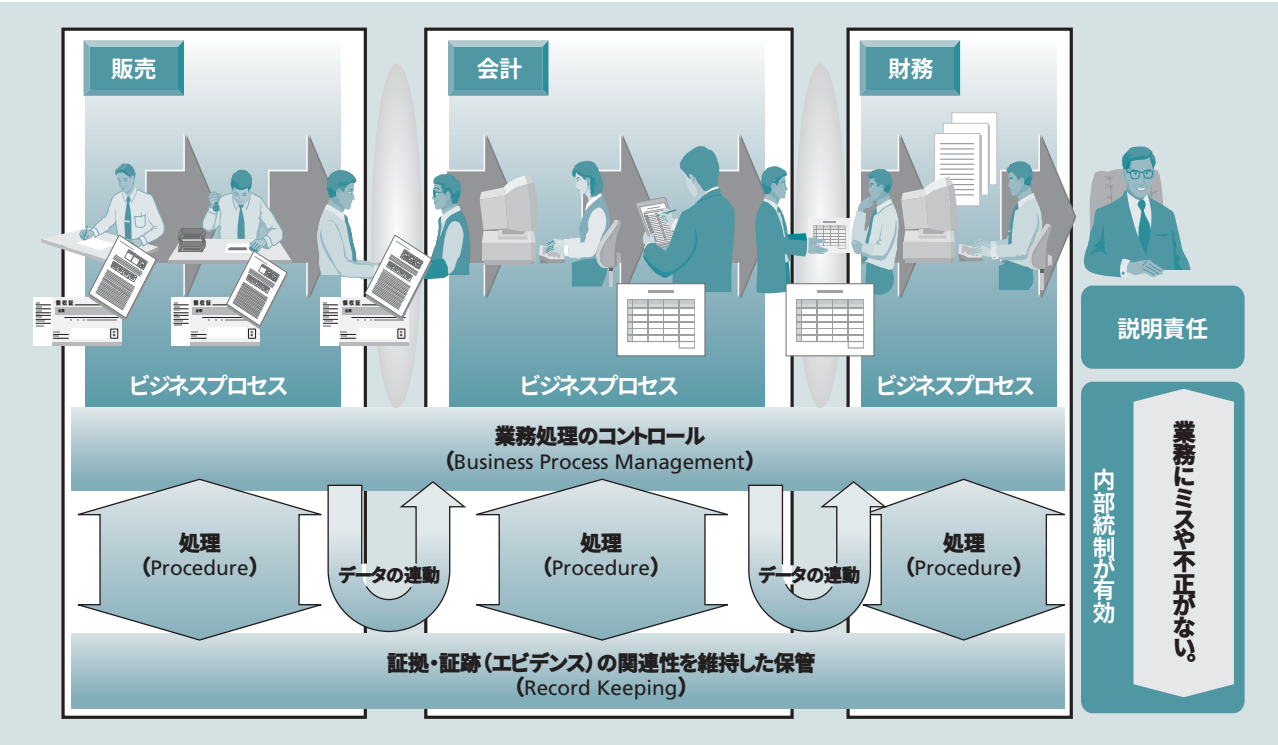

図3　リスクマネジメント基盤のITアーキテクチャ
コントロールされた業務処理に基づき，処理されたものが証拠・証跡として説明責任を果たす構造を維持する。

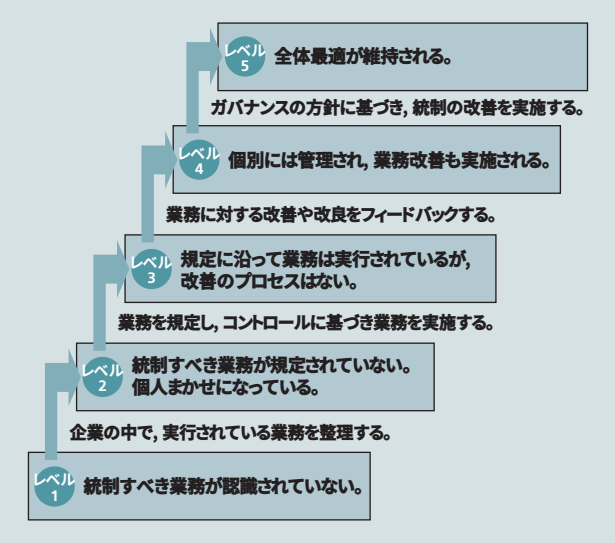

図4　内部統制を成熟させるためのステップ
内部統制全体を最適化した環境で維持するためには，規則・規定化するだけでなく，ガバナンスに基づいた改善の維持が必要である。

最適化を意識して対応していく必要が出てくる。それを実現していくためには，全体のリスク度合いから見た緊急度や重要度から，業務やITシステムを選択していくことが必要になる。このときに優先づけの根拠となるのが，ガバナンスである。このガバナンスの意識づけによって，経営方針とITの運営方針を一体化させ，ITサービスとしての充実と統制の充実の両面をねらうことが可能となる。

4．日立グループの対応

日立グループは，さまざまな業務で発生するリスクに備え，それに対処していくために経営的な視点から具体的なIT施策に至るソリューションを準備している。例えば，IT経営を実現していくためのIT戦略，およびITガバナンスの策定を支援していくコンサルティング関連商品や，企業活動の証拠・証跡を確保し，保管運用していく文書管理システムやハードディスク運用関連商品がある。これらを，日立グループ自身の経験などに裏付けられたノウハウや，そのノウハウを具現化した商品として提供している。

5．おわりに

ここでは，日立グループが考える内部統制の成熟とリスクマネジメント基盤について述べた。

日本版SOX法によって，ステークホルダーに内部統制を説明することが，財務報告に誤りや不正が入り込まないというリスクマネジメントの第一歩であるとして広く認識された。しかし，業務の周辺には，財務報告に関連したこと以外にも多数のリスクが潜在している。これらのリスクに耐性を持っていくためには，業務を説明するための証拠・証跡を維持し，その中から不備を見つけ，不備を改善していくことが求められる。その証拠・証跡を蓄積するのみならず業務の効率向上に活用することと，これらを維持して向上していくためにITを活用し，情報のガバナンスを徹底することにより，リスクマネジメントだけでなく，企業価値の向上に結び付けることができるのである。

参考文献

1）**船城，外：図解 これならできるIT統制，ケーススタディでわかる日本版SOX法実践ガイド，日本実業出版社**（2007.4）
2）**社団法人 ビジネス機械・情報システム産業協会 ドキュメントマネージメントシステム部会：内部統制のカギを握る文書管理システム導入のすすめ，東洋経済新報社**（2006.10）

執筆者紹介

伊藤 泰樹
1985年日立製作所入社，株式会社日立コンサルティング所属
現在，企業システムのコンプライアンス維持に関するコンサルティングに従事
情報処理学会会員

小宮 文男
1987年日立製作所入社，株式会社日立コンサルティング所属
現在，企業システムのコンプライアンス維持に関するコンサルティングに従事

青山 ゆき
1993年日立製作所入社，株式会社日立コンサルティング所属
現在，企業システムのコンプライアンス維持に関するコンサルティングに従事
情報処理学会会員

谷岡 克昭
1980年日立製作所入社，情報・通信グループ 経営戦略室 uVALUE事業インキュベーション本部 新事業推進部 所属
現在，企業改革ソリューションの企画・拡販に従事