普通論文

J-SOX法IT全般統制支援ツール ClearSoXit

猪狩 綿光・大菅 与志一
尾澤 進・和田 敏之

要　旨

本稿では、日本版SOX法のIT全般統制でクリアすべき課題とClearSoXit(クリアソキット)による解決方法について説明します。財務報告に影響を与えるアプリケーションシステムに対する作業統制や証跡確保が簡単に行える機能、システム運用業務やSOX法の監査対応を効率的に実施できる機能を紹介します。
また、SOX法の監査対応は、1年で完了するものではなく、監査で指摘されたポイントの改善が必要です。ClearSoXitは、技術面にSOAをベースとした拡張性・柔軟性あるソフトウェアアーキテクチャを採用することで、システムの運用、保守における業務全般の効率化を実現しています。

キーワード
●日本版SOX法・リスク管理　●IT全般統制・監査支援　●ワークフローツール　●SOA・システム間連携

1. はじめに

日本版SOX法の監査基準と実施基準[*1]が2007年2月15日に金融庁から意見書として公表され、2009年(平成21年)3月期の本決算から上場企業およびその連結子会社を対象に適用となるなか、内部統制をどう整備していくかが企業の急務となっています。

本稿では、SOX法に関係するアプリケーションシステムの運用や保守にワークフローを適用し、IT全般統制を支援するClearSoXitを紹介します。本ツールの適用により、監査の効率を向上させ、コストを抑制することができます。

2. IT全般統制の目的と特性

日本版SOX法は、証券市場に上場している企業情報が適正に開示されることを目的としており、対象企業は、内部統制による財務報告の適正性確保が必要となります。このために、財務報告が不正に行われないように、財務関連の業務やシステムに潜むリスクを管理し、財務に係る情報が正しくコントロールされていることを「内部統制報告書」や「内部統制監査報告書」により示す必要があります。

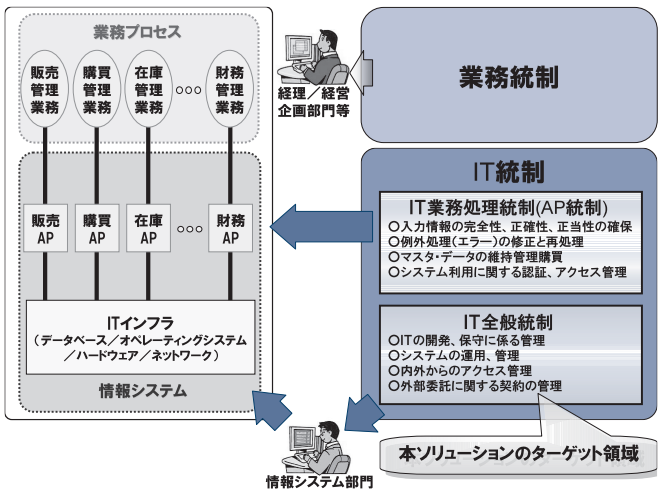

図1　日本版SOX法の対象領域

日本版SOX法の対象領域を**図1**[*2]に示します。

IT統制は、「IT業務処理統制」と、「IT全般統制」に分けられ、それぞれ以下のような特性があります。

1) IT業務処理統制(アプリケーション統制)

・業務プロセスに組み込まれたITに係る内部統制
・業務に即したチェック処理や統制を行うため、各社、各

*1 「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)」として公表されている。
*2 経済産業省、システム管理基準 追補版（財務報告に係るIT 統制ガイダンス）の図をもとに再構成。

業務での独自のノウハウに依存

2) IT全般統制

・業務処理統制が有効に機能する環境を保障するための統制活動

・業務システム運用を標準化すれば、全業務に適用可能

本稿で紹介するClearSoXitは、後者のIT全般統制を支援するワークフローをベースとしたソリューションです。

3. IT全般統制の課題

IT全般統制の監査は、人間系による統制や管理でも対応は可能ですが、準拠性や正確性、正当性の保障に大変な労力を必要とします。たとえば、文書や承認記録を残していても、どれが該当する文書なのか、また承認は権限を持つ管理者によって適切に行われているのかなど、業務フロー通りに統制されていることを証明するのは困難です。また統制を確実にするためには、作業マニュアルを作成し、担当者や承認者にルールを徹底させる必要があり、多大な工数やコストがかかることになります。これらを踏まえ、IT全般統制では統制を取りながらコストをいかに抑えるかが企業の課題となります。IT全般統制における具体的な要件と課題を**表**に示します。

課題のうち、(1)〜(3)はワークフローツールの導入で解決が可能ですが、(4)〜(7)は監査対応として特殊な機能が必要です。ClearSoXitは、これらの課題に対する解決策を提供します。

表　IT全般統制における要点と課題

項番	要件	課題
(1)	すべての業務が運用マニュアル通りに処理されていること	証明困難
(2)	プロセス変更時の徹底、教育	教育コスト大
(3)	証跡の確保、保存	不足する場合は監査不適合
(4)	部門毎にプロセスが違う場合の統制	監査対応コストが掛かる
(5)	監査時の証跡のスムースな検索	監査対応コスト増加
(6)	プロセスのモニタリング	内部監査の実施困難
(7)	関連システム上にある証跡も確保	監査対応コスト増加

4. ワークフローツールでの解決

ClearSoXitは、Webベースのワークフローツールであり、Webブラウザから簡単に利用することができます。ClearSoXitを業務アプリケーション（以下AP）変更管理業務に適用した例を**図2**に示します。ClearSoXitは、障害発生から一連のAP改訂作業をあらかじめ登録されているワークフローに従って制御し、各部署にまたがる作業も的確に記録を残しながら進めることができます。

図3にAP変更管理のリリース作業におけるClearSoXitによる統制例を示します。リリース作業には、不完全な変更が本番環境にリリースされるというリスクが存在します。これに対して、リリース判定という統制ポイントを設け、システム改訂内容に即した変更がAPに行なわれたかどうかを確認する

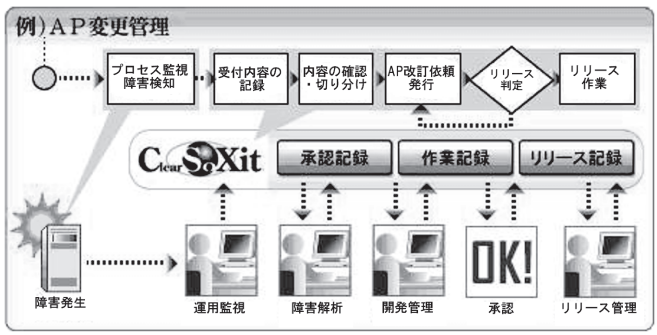

図2　業務への適用例（AP変更管理）

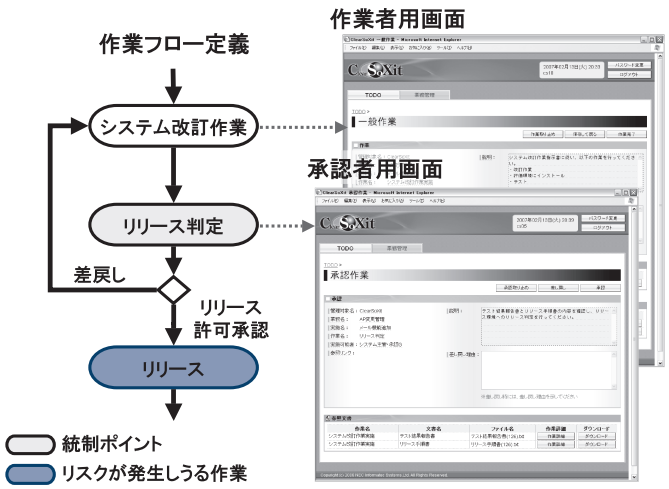

図3　ClearSoXitによる統制例（リリース作業）

ことで、不完全な変更が本番環境に適用されるのを防ぎます。

ClearSoXitは、ワークフローによって作業の流れを制御するため、以下の機能を実現しています。

1) 実行制御と権限チェック（課題(1)への対応）

ClearSoXitは、あらかじめ登録された業務フローに従って、確実に業務の実行を制御します。作業者のTODOリストに作業や承認を割り当て、作業が終わると電子メールで次の作業者へ作業通知することで、作業手順の漏れや連絡ミスによる作業遅延などを防止します。

また、作業者と承認者が別の人であり、正しく職務の分離が実現されていることを容易に確認できます。

2) ツールでフローを変更（課題(2)への対応）

ClearSoXitに登録されているワークフローを変更し、適用することで直ちにプロセスを変更することが可能となり、対人的な教育のコストを削減できます。

3) 証跡の確保・保存（課題(3)への対応）

ClearSoXitは、作業実施に当たり、実施時点の作業実施者の所属や役職を記録し、監査時に提示することができます。

また、作業指示や作業結果を入れた電子ファイルを、作業に紐付けたスナップショットとして管理することで、監査時に作業実施時の入出力として提示することができます。

これらの機能を利用し、証跡は確実に保存され、監査対応作業の効率化を図ることができます。

5. 監査対応機能による解決

ClearSoXitは単なるワークフローツールではなく、IT全般統制の監査対応を効率化できるよう以下の機能を備えています。

1) 母集団の特定（次の2)と併せて課題(4)への対応）

AP変更管理では、インプットとなる改定要件に対応してリリースされるすべてのプログラム、ジョブなどが監査の母集団となります。ClearSoXitでは、本番環境にリリースされるすべてのプロダクトの変更を母集団[3]として捉え記録します。

2) 監査対象数の削減（課題(4)への対応）

部署ごとに作業手順が異なる場合でも、標準のワークフローをベースとして各作業フローをカスタマイズすることで監査対象数を削減できます。**図4** に示すように、異なるシステムであっても、リスクが発生しうる作業を標準システムのフローにマッピングすることで、1つの母集団に集約化することができます。これにより、監査対象となる統制ポイントも集約化されます。

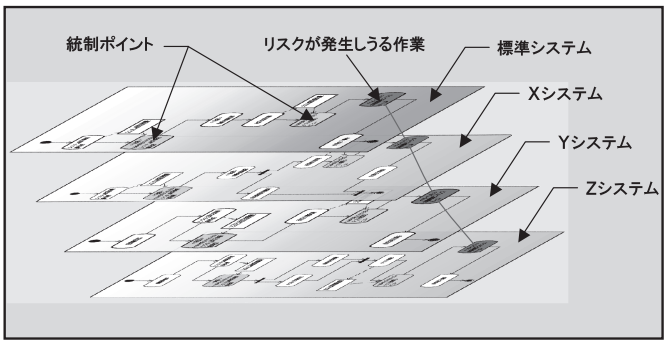

図4　標準システムの手順と各システムの手順のマッピング

日本版SOX法では、リスクが発生しうる作業ごとに25件のサンプルで監査が行われます。図4の例のように、もしシステムX、Y、Zを別々に監査するとなると、監査対象となる作業は2 [箇所/システム] × 3 [システム] =6箇所存在し、それぞれ25件の監査を行うため、合計で150件の記録を確認することになります。しかしClearSoXitを利用すると、監査対象となる作業を2箇所に集約できるため2箇所×25件＝50件の変更記録を確認するだけですむようになります。つまり監査に掛かるコストを1/3に圧縮できるわけです。

3) 監査対象の自動抽出（課題(5)への対応）

ClearSoXitは、母集団からランダムに指定した件数（通常25件）の変更記録を選択する機能があります。この機能を利用して、ランダムに25件ずつ選び出し、監査セットとして登録することで、証跡の確認(再確認)をスムーズに行うことができます。

4) 作業履歴から証跡提示（課題(5)への対応）

監査対象として選択されたプロダクトの変更記録から、その作業の実施者や承認者、またその作業に紐付けられた確証となる情報や登録されている文書を容易に参照できる機能を備えています。

5) 内部監査の実施（課題(6)への対応）

上記の(1)から(4)の機能を利用して、IT全般統制の内部監査が容易に実施できるようになります。

[3] 母集団=監査ポイントとなるイベントの集合。例: 本番環境へのリリース総数。

6) 関連システム上の証跡確保（課題(7)への対応）

母集団の特定では、ClearSoXitが記録している変更と本番環境の更新が等しいことを証明する必要があります。ClearSoXitは、本番環境に対して意図しない変更が行われていないことを保障するため、APの更新日付やサイズ、バージョン等をリリースの前後で記録します。このデータを付き合わせることで、不正にAPが変更されていないことを証明することができます。

6. さらなる業務改善に向けて

企業は、税務報告の信頼性が高まるようIT全般統制のコントロール方法や作業手順を改善し続ける必要があります。また、IT全般統制は、売上に直接貢献するものではないため、いかに効率よく現場に適用し、コストを抑えるかが統制を継続させる鍵になります。

ClearSoXitは、SOAをベースとした拡張性を備えており、絶え間ない改善活動にも十分対応できる仕組みを提供します。その特徴を以下に紹介します。

1) 業務改善が容易

IT全般統制への対応は、現状のプロセスを見直し、統制を効率良く行えるように業務を改善する機会と捉えることができます。現場の改善活動を取り入れ、ワークフローを柔軟に変えられないと改善のサイクルが止まってしまいます。ClearSoXitは、並列処理、分岐、合流、繰返しなど、業務に沿った柔軟なフロー定義が可能です。たとえば、複数のシステム改善要求依頼を１つのシステム改訂依頼にまとめる処理や１つのシステム改訂依頼から複数のリリース依頼を発行するようなフローも記述できます。さらに、フローを変更する場合、前の仕掛かっている作業はすべての業務が終了するまでは旧フローに従って処理され、新規作業に関しては開始分から新しいフローが適用されます。

2) 外部システム連携が可能（課題(7)への効率的な対応）

ClearSoXitは、運用ツール等と連携するインタフェースを用意しており、人と運用ツールの混在したワークフローを柔軟に組むことができます。各種運用ツールと人の連携により、現場に適合した運用を実現するとともに作業品質の向上と運用コストの削減が可能となります。

7. おわりに－今後の予定－

ClearSoXitは、NEC標準テンプレートに基づいて開発されており、現場への適用を開始しています。また、運用事故によるリスク低減や運用コスト削減のため、システム運用におけるインシデント管理ツールやリリース管理ツール、認証システムと連携可能な部品の提供を予定しています。

さらに、監査対応作業の効率化だけではなく、ITIL準拠のアプリケーション変更管理プロセスを実現し、システム運用や保守に係る業務全体の最適化が行えるようワークフローを中心にサービスの組み込みを行っていく予定です。

参考文献

1) 金融庁から2007年2月15日に公表されている企業会計審議会の意見書「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」
2) 経済産業省から2007年1月19日に公開されている「システム管理基準追補版（財務報告に係るIT統制ガイダンス）（案）」
3) NECプレスリリース、http://www.nec.co.jp/press/ja/0611/2901.html

執筆者プロフィール

猪狩 綿光
NEC情報システムズ
先端技術ソリューション事業部
アプリケーション構築基盤グループ
マネージャー

大菅 与志一
NEC情報システムズ
先端技術ソリューション事業部
アプリケーション構築基盤グループ
マネージャー

尾澤 進
NEC情報システムズ
先端技術ソリューション事業部
品質管理グループ
品質管理マネージャー

和田 敏之
NEC情報システムズ
先端技術ソリューション事業部
アプリケーション構築基盤グループ
グループマネージャー