

なぜ連携による対応なのか

2006年5月に新会社法が施行され、資本金5億円以上、または負債200億円以上の企業に内部統制の構築が義務づけられた。また、その翌月(2006年6月)に成立した「金融商品取引法」(日本版SOX法)では、上場企業は財務報告の適正性を確保するための体制作りと、その評価報告書、および報告書への監査証明の添付が定められた。

この2つの法律を見ると、上場企業や大企業だけが内部統制の対象になるようだが、連結子会社や関連会社はもちろん、場合によっては業務委託会社も含まれる可能性がある。ということは、System iを利用する規模の企業は大半が、内部統制への備えが必要になる、ということである。

そこで本稿では、ベンダーから提供されているパッケージやツールを連携させることによる内部統制対応を提案したい。

なぜパッケージやツールの「連携による対応」なのかといえば、1つは、パッケージやツール自体が内部統制に対応する高度な機能を備えているからであり、もう1つは、実際の業務を想定すると、個々のパッケージやツールがカバーする範囲は業務全体の一部でしかなく、連携によって全体的なカバレッジが確保できるからである。

つまり、業務の部分的な統制には個別のパッケージ／ツールで対応し、それでカバーしきれない部分は、他のパッケ

ツール／パッケージ連携による効率的で緻密な内部統制への対応〈試案〉

新会社法と日本版SOX法が求める内部統制への対応が急務となってきた。その方策として、ツールやパッケージを活用することは、手動対応による煩雑さを回避する点や対応の正確性・迅速性を得る上で効果的だ。しかし、個別のツール／パッケージがカバーし得る範囲は、業務全体の一部でしかない。そこで本稿では、ツール／パッケージの連携による内部統制対応を検討してみた。本稿は、統合会計パッケージ「SuperStream/400」を持つネスコ、統合型データ抽出・加工・出力・共有ツール「OSS/NOA」を開発・販売するユニチカ情報システム、セキュリティツール「Bitis JS」とHAツール「Bitis HA」を販売するピーティスの3社による討議を参考に、記事をまとめた。文責は編集部。

協力

今井 洋 氏
株式会社ネスコ
SuperStream 事業部
企画グループ グループリーダー

佐藤 啓介 氏
ユニチカ情報システム株式会社
システムプロダクト営業部 部長

野口 義夫 氏
株式会社ピーティス
プロデュース担当 主任

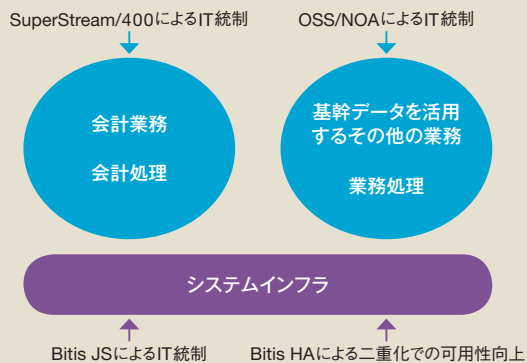
ージ／ツールで補おうというわけである。

日本版SOX法の実施基準案によれば、IT統制は、次の2つの局面に大きく分けられている。1つは、個々の業務が正当かつ正確で、網羅性と業務継続性を確保していることを保障するための「IT業務処理統制」、もう1つが、業務処理統制が有効に機能するのを確保するための「IT全般統制」である。

本稿では、IT全般統制のカテゴリー(統制区分)を、「システムドキュメント」「セキュリティ」「ログ取得」の3つに分け、各ツールがこれらの何に対応しているかを見る。また、IT業務処理統制については、「正確性」「網羅性」「正当性」「維持継続性」「可用性」という5つの管理目標から各ツールのカバレッジを見ることにする。

一般的な業務シーンで考える

ここで、ごく一般的な業務シーンを描いてみよう。売上の計上から会計処理を経て、その処理データを基幹システムか



図表1 ツール/パッケージ連携によるIT統制の全体図

ら取り出して売上分析を行う、というシーンである。一連の流れは次のようになる。

- ①PCから販売管理システムへアクセスし、売上を入力する。
- ②販売管理システム上で入力データが仕訳され、自動で会計システムへ引き継がれる。
- ③会計システム上で会計処理が行われる。
- ④会計システムの標準レポート機能を使って会計データを出力する。

一方、④とは別に、OAツールを搭載したユーザーPCへ取り出して加工・分析を行うシーンを想定する。

- ⑤会計システムから会計データをユーザーPCへ抽出する。
- ⑥ユーザーPC上でOAツールを使い、自由に加工・分析し、その結果をプリントアウトして手元資料にする。

では、この①～⑥で、ITによる統制がどのように必要になるか見てみよう。

①では、PCの安全性とユーザーの適格性が問われる。そして、販売管理システムへのアクセスと売上入力に正当であるかの証跡が求められる。

続いて②は、仕訳と会計システムへの引き渡しであるが、ここは「自動引き継ぎ」

なので、システム設定によって自動的に統制がかけられている。

しかし、この仕訳と会計システムへのエントリーを手作業で行う場合は、独自に「より詳細内容」としての統制が必要となる。いわゆる内部統制の3点セットだが、手作業をベースとすると、膨大な量のドキュメントを揃える必要があることを指摘しておきたい。

そして、自動・手動のいずれにおいても、アクセスルールの設定と分析および監視機能が必要となる。さらに、その証跡としてのログ(取得)が不可欠である。

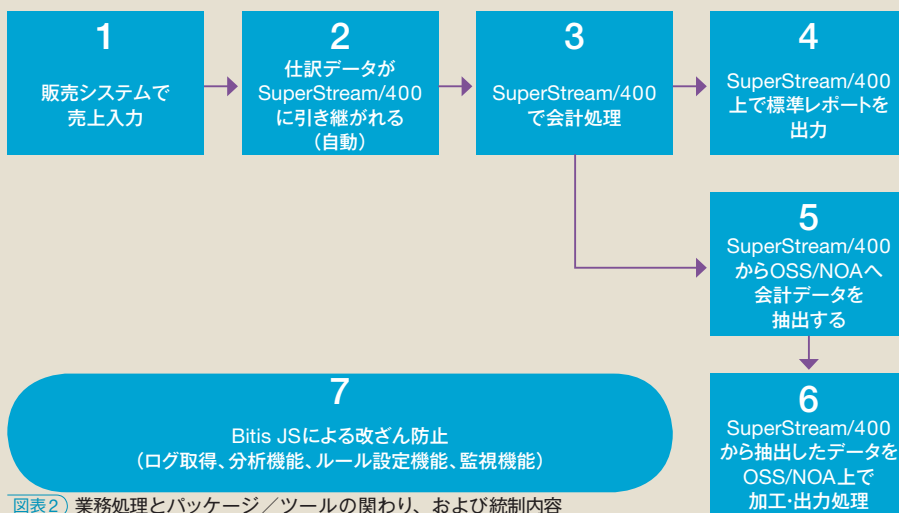
Bitis JSによるIT統制

ここで、①と②と⑤の統制に、Bitis JSが対応することを見ておきたい。このツールは図表3でまとめたように多数のIT統制機能を持つが、中でもDBの更新ログを取得して全ての変更履歴を記録し、改ざんの有無を確認できる点が重要である。また、業務フローが定義されていてもDBが直接改ざんされる恐れがあるが、Bitis JSは自動的にアクセスルールを作成することにより、例外的なDBアクセスをアクセスエラーとしてモニタする機能があるので、確認が可能だ。

SuperStream/400によるIT統制

③と④は会計システム上でのアクションである。会計システムに求められるIT全般統制への対応は、「セキュリティ」「バックアップ」「運用監視インフラへの適合」の3つである。また、IT業務処理統制では「入力支援」「制度改変」「業務プロセスの可視化」への対応が求められる。ここでは、IT統制の範囲で内部統制への対応を実現しているSuperStream/400の機能を見ておこう。

まず、IT全般統制では、System iの標準機能も利用して、次の4つに対応し



図表2 業務処理とパッケージ/ツールの関わり、および統制内容

統制範囲	統制区分	統制項目	統制対応機能
IT全般統制	セキュリティ	<ul style="list-style-type: none"> ●分析機能 ●監視機能 ●アクセスルール設定機能 	<ul style="list-style-type: none"> ●オブジェクト使用状況を自動的に収集し、ユーザー別にオブジェクト使用状況の分析が可能 ●オブジェクトの使用状況を基にアクセスルールを作成して調整しBitis JSへの設定が可能 ●セキュリティツール自身へのセキュリティを仕掛け、高権限ユーザーの内部不正を防止 ●ODBCでのネットワーク接続等のアクセス制限やログ取得が可能 ●不正ジョブを保留し、不正操作の防止が可能 ●アクセスエラー等の発生時にメッセージでの管理者への通知やメッセージ監視ツールとの連携が可能 ●各種エラーリストやログを帳票印刷可能 ●Bitis JSのセキュリティ状態を確認できる統合モニタ機能
	ログ取得		<ul style="list-style-type: none"> ●サインオンエラーのログ取得 ●アクセスルール外のアクセスエラーログ取得 ●使用時間ルール外のアクセスエラーログ取得 ●複数ジャーナルのログを蓄積し任意の項目や日時の範囲、ジャーナル項目を組み合わせて検索が可能 ●データベースのフィールドレベル更新ログ取得 ●特定ユーザー監視(特定のユーザーのコマンドログを取得し検索可能) ●各種エラーリストのログ帳票印刷

図表3 システムインフラを統制するBitis JSの対応機能

ている。

- ユーザーID管理
- バージョン履歴管理
- バックアップ
- DB管理

また、IT業務処理統制では、次の3つに対応している。

•入力支援機能

IT業務処理統制の管理目標である「正確性」「網羅性」「正当性」「維持継続性」の観点から、図表4にまとめた多数の機能を実装している。

•制度改変への対応コンプライアンス対応

定期的なバージョンアップとは別に、制度改正の都度、対応版パッチを提供し、運用管理の「正確性」「網羅性」「正当性」「維持継続性」に対応する。

•業務プロセスの可視化への対応

SuperStream/400の仕様情報を専用ドキュメントで提供し、会計プロセスの可視化に対応する。また、ログイン、プログラム使用、データ操作履歴（伝票操作履歴など）などのログ情報とその閲覧機能を提供している。さらに他社ツールの文書化支援ソリューション「QPR J-SOX」と組み合わせることにより、内部統制用の文書化、評価、実施後の運用と文書メンテナンスなどを網羅するソリューションを提供している。

OSS/NOAによるIT統制

⑤と⑥は、業務の生産性を上げる手段として最近増えているパターンである。基幹データからExcelなどへデータを展開するツールも数多く出回っている。しかし、Excelなどへのデータ抽出と加工、出力は、内部統制上、重大な問題を抱えている。それは、それらのツールがログ機能を備えていないため、「いつ、誰が、どのファイル／業務DBから、どのデータ

を抽出し、どのように加工して、どう処理したか」という証跡がまったく残らないからだ。

そこで、こうした業務プロセスを統制するためには、業務DBのデータ抽出からデータの加工、帳票出力までをカバーし、セキュリティとトレーサビリティ機能を併せ持つツールが不可欠となる。そして、それに対応するのがOSS/NOAである。

OSS/NOAの機能の中から、⑤⑥の業務シーンを統制する機能を見てみよう。

•ホストDBの利用設定

ユーザーごとに、DB、項目、抽出データの利用を制限できる。

•ユーザー資源の一元管理

ユーザーの資源はサーバー側で一元

統制範囲	統制区分	統制項目	統制対応機能
IT全般統制	システムドキュメント	-	<ul style="list-style-type: none"> •マニュアル5種(システム設定・システム操作・出力帳票一覧・データベース定義・インストールマニュアル) •システム改変ドキュメント(リリースノート) •ソースコードの公開(パートナー限定・要契約) ※ログインや暗号化ロジック部分を除く •アドオン・カスタマイズ時における開発規約ドキュメントの提供(パートナー限定) •SuperStream/400内部統制ドキュメント
	セキュリティ	<ul style="list-style-type: none"> •ユーザー管理 •パスワード管理(アプリケーション、データベース) •権限設定 •アクセス管理 	<ul style="list-style-type: none"> •ユーザーIDの一元管理 •最小桁数設定 •誤入力許容回数設定 •有効日数設定 •有効期限切警告 •共通鍵によるパスワード暗号化 •データベースユーザーのアクセスパスワードの変更可能 •ユーザーIDに対する管理者/ユーザーの区分設定 •ユーザーIDごとのメニュー設定 •使用可能なマスタ項目の制限 •処理可能権限の設定(前年仕訳・外部伝票更新・承認済伝票修正など) •端末単位のアクセス制御(マシン登録/プログラム利用許可の2段階) •アプリケーションへのログインモニタリング •プログラムの使用状況モニタリング
	ログ取得	-	<ul style="list-style-type: none"> •システムへのログイン履歴 •プログラムの使用履歴管理 •伝票操作履歴 •アプリケーションの処理実行ログ取得

統制範囲	管理目標	統制項目	統制対応機能
IT業務処理統制	正確性	<ul style="list-style-type: none"> •入力誤謬防止機能 •エラーチェック •ブルーリスト •エラーリストとフォローアップ •その他 	<ul style="list-style-type: none"> •伝票番号連番管理 •マスタ参照ダイアログによる簡易入力 •税額の自動計算(リアルタイム処理) •自動書式設定 •貸借バランスチェック •書式チェック •マスタデータ存在チェック •入力画面入力チェックリスト •外部取込データ修正機能 •エラー一覧出力帳票 •システムエラーのダイアログ表示 •自動仕訳機能 •テンプレート入力機能
	網羅性	<ul style="list-style-type: none"> •入力原票管理 •重複防止 •入力漏れ防止 •登録件数確認 •データ出力 	<ul style="list-style-type: none"> •外部伝票固有情報の保持 •外部システム伝票のエラー修正 •システム・ユーザー固有定義による伝票番号管理 •伝票連番管理 •データ未入力チェック機能 •登録データの件数カウント •残高→明細情報へのドリルダウン •さまざまな抽出条件指定が可能な帳票および検索・照会画面
	正当性	<ul style="list-style-type: none"> •承認設定・処理・承認記録保持 •アクセス管理 •データ変更管理 	<ul style="list-style-type: none"> •多段階承認 •ワークフロー機能(現場入力システム) •承認・修正・削除ログの取得 •マスタ情報の閲覧・使用に関する制御(ユーザーIDごと) •締め処理による修正・削除の制限
	維持継続性	-	<ul style="list-style-type: none"> •マスタ修正時における他マスタ/トランザクションデータとの整合性チェック •マスタブルーリストの出力 •データ更新時の排他制御

図表4 会計業務/システムを統制するSuperStream/400の対応機能

統制範囲	統制区分	統制項目	統制対応機能
IT全般統制	セキュリティ	<ul style="list-style-type: none"> ユーザー管理 パスワード管理 (アプリケーション、データベース) 権限設定 アクセス管理 出力制限 	管理者対象 ●全体管理者、運用メニューごとの権限付与 利用者対象 (1) DBアクセス制限 ●使用ユーザーごとに、1~3の制限設定 ①データベース ②項目 ③抽出データ (2) 出力行為制限 ●印刷、エクスポート、表示画面からのデータの切り取り・コピーなどの行為をユーザー単位で制限
	ログ取得	-	ユーザーの操作について、「いつ、誰が、どのクライアントPCから、どのような処理を実行したか」さらに、DB抽出処理については「どのDBの、どの項目から、どのような条件で抽出したもののか」まで詳細に記録され、これらを簡単操作で閲覧可能

統制範囲	管理目標	統制項目	統制対応機能
IT業務処理統制	正確性	<ul style="list-style-type: none"> データ処理プロセス保管 ログ取得、調査 	<ul style="list-style-type: none"> ユーザーの行ったデータ抽出・加工・出力の全プロセスを保管・管理しているため、帳票作成のデータ処理ロジックを確実に再現、確認することが可能 ユーザーの操作について、「いつ、誰が、どのクライアントPCから、どのような処理を実行したか」さらに、DB抽出処理については「どのDBの、どの項目から、どのような条件で抽出したもののか」まで詳細に記録され、これらを簡単操作で閲覧可能
	網羅性	●データ出力	さまざまな抽出加工条件、帳票レイアウト作成ができ、意図する目的の通りに出力情報が利用可能
	正当性	<ul style="list-style-type: none"> アクセス管理 出力制限 レポートの適切配布 	管理者対象 ●全体管理者、運用メニューごとの権限付与 利用者対象 (1) DBアクセス制限 ●使用ユーザーごとに、1~3の制限設定 ①データベース ②項目 ③抽出データ (2) 出力行為制限 ●印刷、エクスポート、表示画面からのデータの切り取り・コピーなどの行為をユーザー単位で制限
	維持継続性	<ul style="list-style-type: none"> データ処理プロセスの最新版管理 利用者資源のサーバー一元管理 	<ul style="list-style-type: none"> ユーザーの行ったデータ抽出・加工・出力の全プロセスは、最新情報を管理 利用者の資源は、すべてサーバー側で管理基幹業務システムと同等レベルの機密保持、運用が可能

図表5 基幹データの業務利用とシステムを統制するOSS/NOAの対応機能

統制範囲	統制区分	統制項目	統制対応機能
IT業務処理統制	可用性	<ul style="list-style-type: none"> オブジェクト/データの二重化 プライマリ障害や災害時の業務停止時間短縮 計画停止時の停止時間短縮 プライマリでのバックアップ時の業務停止時間短縮 バックアップ取得 	<ul style="list-style-type: none"> リアルタイムミラーリングによるSystem iのオブジェクト/データの二重化を行うことにより、可用性が向上 高速・確実にプライマリ(本番機)とセカンダリ(バックアップ機)の役割を切り替えられるシナリオ機能 OSのバージョンアップや電気の法定点検等の計画停止時にプライマリを止めずに業務を継続でき、可用性の向上が可能 プライマリでの業務を止められない場合にセカンダリでバックアップを取得するバックアップ支援機能 二重化により、プライマリの障害・災害時に業務停止時間をマネジメントでき、こと業継続計画を綿密な物とすることが可能(マシン1台体制時では、復旧にかかる時間が計画できない)
	正確性	<ul style="list-style-type: none"> データチェック セカンダリでのオブジェクト/データの正確性 	<ul style="list-style-type: none"> データの適用がNGの場合に即座に再送信して同期を取り、セカンダリへの確実なデータ適用を行うCCI(*1)機能 オブジェクト/データも含めて発生順ソートしに正確にセカンダリへ適用するSIP(*2)機能 プライマリとセカンダリのデータをブロック単位で高速でチェックし、差異があれば最小単位で再同期するCheckSync機能 <p>(*1) Core Cycle Information (*2) Sequence Integrity Processing</p>

図表6 システムインフラを統制するBitis HAの対応機能

管理され、基幹システムと同等レベルの機密保持と運用が可能。

- データ処理プロセスの保管
ユーザーが行ったデータ抽出・加工・出力の全プロセスを保管・管理し、帳票作成のデータ処理ロジックを再現・確認できる。
- ユーザーごとに出力行為の制限
印刷、エクスポート、表示画面からのデータの切り取り・コピーなどをユーザーごとに制限できる。
- 操作ログを簡単閲覧
ユーザーのすべてのアクションを記録し、簡単な操作で閲覧できる(オプション)。

基幹データを利用するというごく一般的な業務シーンの中にも、数多くの統制が必要となる。それを確実に行うにはITを利用した統制が有効になるが、業務全体の統制を実現するには、複数のツールの連携が不可欠になるのだ。

Bitis HAによるIT統制

なお、①~⑥の可用性や正確性、事業継続性をさらに高める方法として、HAシステムによるデータ・バックアップがある。これは、Bitis HAがカバーする領域である(図表6)。

Bitis HAの特徴は単に事業継続性のために遠隔地へデータを複製できるだけでなく、全てのオブジェクト・データを「発生した順番に正確」に送ることができる。これは正確性を保障するために有効な機能である。

業務フローが整備されている環境であれば、これらのツールを効果的に導入することによって、業務DBごとにアクセスするユーザーを特定でき、セキュリティの設定も容易となる。また、System i対応のツール/パッケージであれば、それらの運用をSystem i上で一元管理することも大きなアドバンテージとなることを付け加えておきたい。 **①**