

SAPのシステムコントロールと セキュリティ評価のための新ツール



企業の統制環境へのインパクトを考慮した場合、SAPはその場しのぎのちょっとした対応で改善ができるような仕組みにはなっていません。更に、SAPは買ったその日からすぐ使用できるように予め最適な設定がされているわけでもありません。SAPにおいて内部統制の観点から最適な設定を実現するためには、企業におけるリスクを十分に考慮した上で、主体的に設定を行う必要があります。つまり、このような考慮が十分にされていない場合、企業は導入完了後、リスクに対するコントロールの設定不備に遭遇する可能性があります。

SAPはパラメータ設定によるシステムコントロールの多くが有効化されていないまま出荷されています。例えば：

- 得意先や仕入先マスタの重複登録の可能性に対して、入力時の警告メッセージ表示は初期設定に含まれていないので、個別に設定をする必要があります。
- 購買から請求プロセスにおいて、仕入先からの仕入金額や仕入数量の許容範囲設定はSAPの初期登録値である会社コード0001に対してのみ設定されています。つまり、この設定は全ての有効な会社コードに対して個別に設定をする必要があります。
- 出荷時に初期登録されている多くのプロファイルは広範囲なアクセスが可能となっているため、ユーザーアクセス権限を最適化するために個別に設定をする必要があります。

その理由は？

多くの場合、SAP導入コンサルタントは導入時の作業スコープとして、内部統制に関連するSAPのパラメータ設定を最適化させる事を明確に依頼されません。更に多くの企業では、SAPの導入時において強固な統制環境を整備し、その環境を維持・管理することを確実にするための能力を持つ専門家が社内にはいません。

サーベンス・オクスレー法（以下、SOX法）対応において多くの企業は、SAP導入におけるパラメータ設定によるシステムコントロールとセキュリティに関して、SAPには、まだまだ改善の余地がある事を学びました。導入時にSAPのコントロールとセキュリティを標準化・自動化する事によって、企業はSOX法対応のための投資に対する効果を向上させる事が可能になりました。また現在市場に出ているSAPツールを使用し、コントロールや関連するテストを自動化する事によって、更に投資に対する効果を向上させる事ができます。

SAPを利用した内部統制環境とは？

SAPを利用した内部統制環境の4つの基本的要素に留意しておくといでしょう。4つの内2つの要素は前述したパラメータ設定によるシステムコントロールとセキュリティであり、“システムの内的な要素”です。その他2つの要素は、“システムを取り巻く外的な要素”であり、マニュアルコントロールと発見的コントロールです。マニュアルのプロセスコントロールの例には直接入力された請求書や減価償却などに対するマニュアルでの承認が含まれます。発見的コントロールの例には、原価センター一覧の確認や重複請求書一覧の確認などが含まれます。

自動化されたSAP評価ツール

今まで多くの場合、SAPにおけるシステム設定の監査はマニュアルで行うプロセスでした。このようなマニュアルでの作業では、システムの複雑性に起因して評価そのものを実施することが困難であり、コントロールの運用状況の有効性や効率性を評価するための判断材料を明らかにすることが困難でした。これに対して過去数年にわたり、“システムの内的な要素”であるシステムコントロールの評価プロセスを自動化し、その有効性や効率性を評価するための判断材料を幅広く提供するためにいくつかのツールが開発されてきました。これらのツールは、SAP監査におけるマニュアルでのアプローチを不要とするほ

どの影響力を有しています。

自動化された SAP 評価ツールは、組み込んだロジックによって SAP のコアとなるデータ（セキュリティ プロファイルやパラメータ設定など）を抽出し分析します。SAP のパラメータが想定通りに設定されているか確認するアプローチは、サンプリングによるアプローチに比べてより効率的、効果的に評価を行う事ができます。自動化された評価ツールを使う事によって、監査人はサンプルに基づいて結果を推定するのではなく、全母集団に基づく分析を実施し、結論を出す事が可能となります。

セキュリティ設定を監査する場合、マニュアルによる監査アプローチには SAP 標準の SUIM プログラムを使用する場合がありますが、その場合以下のような問題点があります。

- SUIM はトランザクションコードと権限オブジェクトのみを個別にテストします。
- 監査担当者は、各トランザクションに対して必要な権限オブジェクトが何であるか知っている必要があります。なぜなら、レポートにおいてはテストが必要なトランザクションコードや職務分掌に関する課題が特定されないからです。
- 提供される重要なトランザクションの組み合わせレポートでは、必ずしも権限オブジェクトによるチェックが行われておらず、誤まった結論を導くレポートが提供される可能性があります。

一方で Protiviti が所有している SAP 評価ツールである Assure Security を使用したアプローチでは、以下のような機能が用意されています。

- 重要なトランザクションや職務分掌をテストするための参照情報や、それぞれのトランザクションの評価に必要な権限オブジェクトに関する情報
- 予め想定している設定との相違に関する自動化された予防的なチェック
- 様々な観点からの職務分掌に関する自動化されたテスト
- ユーザ管理とセキュリティ構造の分析
- ベンチマーク機能

ケーススタディ：GM との連携および学んだ教訓

General Motors Audit Service (GMAS) は SAP 導入に関する内部監査のため、Assure Controls と Assure Security を使用する契約を Protiviti と結びました。このプロジェクトの一番の目的は、今までマニュアルで行ってきたパラメータ設定や職務分掌、重要なトランザクション権限のテストを自動化することでした。

データ、データ、そして更にデータ

SAP Assure Tools はパラメータ設定およびセキュリティ設定に関して、とてつもない量のデータを出力します。しかし、データそのものだけでは不十分で、SAP の知識や経験を基に結果を正確に解釈する必要があります。このケースでは Assure Security を使用し、総勘定元帳に関連するプロセス、販売から入金までのプロセス、調達から支払までのプロセスの各プロセスにおいて、トランザクションコードおよび権限を分析し、その結果職務分掌のルールに抵触する 8,518 個のトランザクションコードの組み合わせが発見されました。この分析により、数多くの職務分掌リスクの事例が発見されました。Assure Controls では、上記プロセス内において 234 個のパラメータ設定によるシステムコントロールが自動的にテストされ、多くの改善点が特定されました。

分析結果を効果的に提示するためには、結果が分かりやすく理解され、それに対してアクションを起こすことができるよう優先順位をつける必要があります。不明確かつサポート体制が明らかでない状態で結果を説明してしまうと、最も重要で有用な情報でさえも否定的に捉えられ抵抗されてしまいます。また状況やリスクレベルを明確にせず、SAP の経験なしに結果を分析してしまうと、無駄な試みになってしまいます。そのため、SAP の経験や専門知識がない状態にもかかわらず、このような自動化された評価ツールそのものを特効薬として理解してしまうのは危険です。

マニュアルコントロールや評価アプローチからの逸脱

上記のケースのような場合、結果を見せられたシステムオーナーやプロセスオーナーは、提示された職務分掌リスクを改善するための補完的コントロールの設定や、SAP パラメータ設定によるシステムコントロールの最適化に対応するため、マニュアルコントロールで埋め合わせをしようとしていました。

しかしながら最終的には、システムコントロールの考え方に賛同を得る事が大切です。例えば、発見された問題に対して単純に、継続してマニュアルコントロールに頼って対応するよりも、SAP のセキュリティ設定を実際に改善する方が実際に理に適ったものであるとの一致した意見を得ることが重要なのです。

第一に、マニュアルコントロールに比べてシステムコントロールの方がより一層信頼できます。第二に、特に SOX 法への対応という観点からは、マニュアルコントロールに比べてシステムコントロールを監査する場合の方が、コストがかからずしかも難しくありません。更に、マニュアルコントロールをシステムコントロールに置き換えているような企業では人事異動などの影響は少なく、コントロール環境を維持するために特定

の個人に頼る必要がなくなります。

パラメータ設定によるシステムコントロールに関して、システムコントロールに移行する事により、以下のような向上や最適化が期待できるでしょう。

- 監査プロセスにおける効率化と有効化
- 監査および維持・管理にかかるコストの削減
- より強固な統制環境
- データの正確性

GMAS は、SAP のパラメータ設定によるシステムコントロールとセキュリティのテストを自動化し、更なる統制環境の向上という目的を遂げただけではなく、Protiviti の Assure Controls と Assure Security ツールを使用する事によってトレーニングやナレッジ・トランスファーに関連するメリットを得ました。GMAS チームメンバーは以下のように述べています。

「Assure Tools の中に保持されているリスクとコントロールに関する参照資料は、実際のビジネスで使用する言葉で説明されたためトレーニングセミナーのようであった。」

このことから、GMAS チームやプロセスオーナーにとって効率的にナレッジ・トランスファーを行う良い機会となりました。

SAP の自動化ツールのその他の使い方

評価のためだけでなく、その他以下のような場面でも SAP 自動化ツールを活用する事が可能です。

- システム導入プロジェクトの準備としてコントロールのデザインとベースラインの設定をすることで、システム設計やブループリントを前もって最適化する。
- SOX 法対応において依拠しているコントロールと、SAP にて設定可能なパラメータ設定によるシステムコントロールを比較し、マニュアルコントロールをシステムコントロールに置き換える。
- 既存の補完的なマニュアルコントロールを自動化し、セキュリティ管理やコントロール変更を自動的にモニタリングする。
- コントロールに対する責任をプロセスオーナーへと移管させるため、ワークフロー機能を活用し、リスクとモニタリングルール（例外事項の管理を含む）の定義を通じてプロセスオーナーを関与させる。
- 特定の取引データ分析を自動化し、特定のリスク事象を取引ベースでモニタリングすることを可能にする。これにより、コンプライアンスの取り組みに必要な労力を省力化させた上で、非常に強固なモニタリングを実施する。
- 不正に対するコントロールを自動化すると共にそのモニタリングを自動化する。

企業が SOX 法対応のプロジェクトから、継続的に維持可能で費用対効果があるプロセスへ変えていこうとする中、Protiviti の Assure Tools などの自動化ツールを使用する事によって、大きな 1 歩を踏み出す事が可能になります。その結果、「コントロールの自動化」、「モニタリングの活用可能性の向上」、「コンプライアンスプロセスの効率化と有効化」という観点から SAP をより一層、最適化する事ができるでしょう。

株式会社プロティビティ ジャパン

東京オフィス：〒100-0004 東京都千代田区大手町1-1-3 大手センタービル Tel.03-5219-6600[代表] Fax.03-3218-5533

大阪オフィス：〒541-0056 大阪府大阪市中央区久太郎町4-1-3 大阪センタービル 13F Tel.06-6282-0710[代表] Fax.06-6282-0711

お問い合わせメールアドレス：pj-mktg@protiviti.jp

ホームページ：http://www.protiviti.jp/

Protiviti、Protiviti ロゴは、Protiviti Inc. の米国ならびにその他の国における商標または登録商標です。その他の記載されている会社名・製品名は各社の登録商標です。