protiviti®

Face the Future with Confidence

SAPアプリケーションにおける権限設計

SAPの導入、アップグレード、および権限再設計プロジェクトにおけるSAPアクセスモニタリングソリューションの活用

Internal Audit, Risk, Business & Technology Consulting

はじめに

SAP権限設計プロセスが適切に行われないことによる影響は、不正アクセス、不正の可能性の増大、エンドユーザに対する非効率なアクセス管理、監査関連の問題など多岐に渡ります。潜在的な権限に関する問題を積極的に特定し、対処していない企業は、SAPの導入から1～2年以内に、高額かつ困難な再設計プロジェクトが必要となるケースが少なくありません。これは、合併や買収などの理由でシステム統合を実施した企業、または全般的なSAP権限の戦略を策定しないまま、システム統合を実施した企業などに多く見受けられます。粗悪な権限設計により、権限設定上の問題を緩和するために幾つものプロジェクトが実施されるだけでなく、アクセス権付与の遅延により生産性が低下するといった落とし穴が待ち受けています。

"SAPの権限に関する要件をSAPの導入、アップグレード、または再導入プロジェクトの初期段階で定義することで、効率性および権限リスクの緩和を稼働前に担保することができます。"

SAPでアプリケーション権限を構築する場合、主に二つのアプローチがあります。第一のアプローチは、本稿で詳しく紹介する「トップダウン」または「プロアクティブ」アプローチです。このアプローチでは、設計フェーズの段階で権限要件を定義します。第二のアプローチは、「ボトムアップ」または「リアクティブ」アプローチであり、利用可能なトランザクションおよびジョブ機能に基づいてSAPロールを策定し、システム構築後、権限要件および制約を検討する方法です。

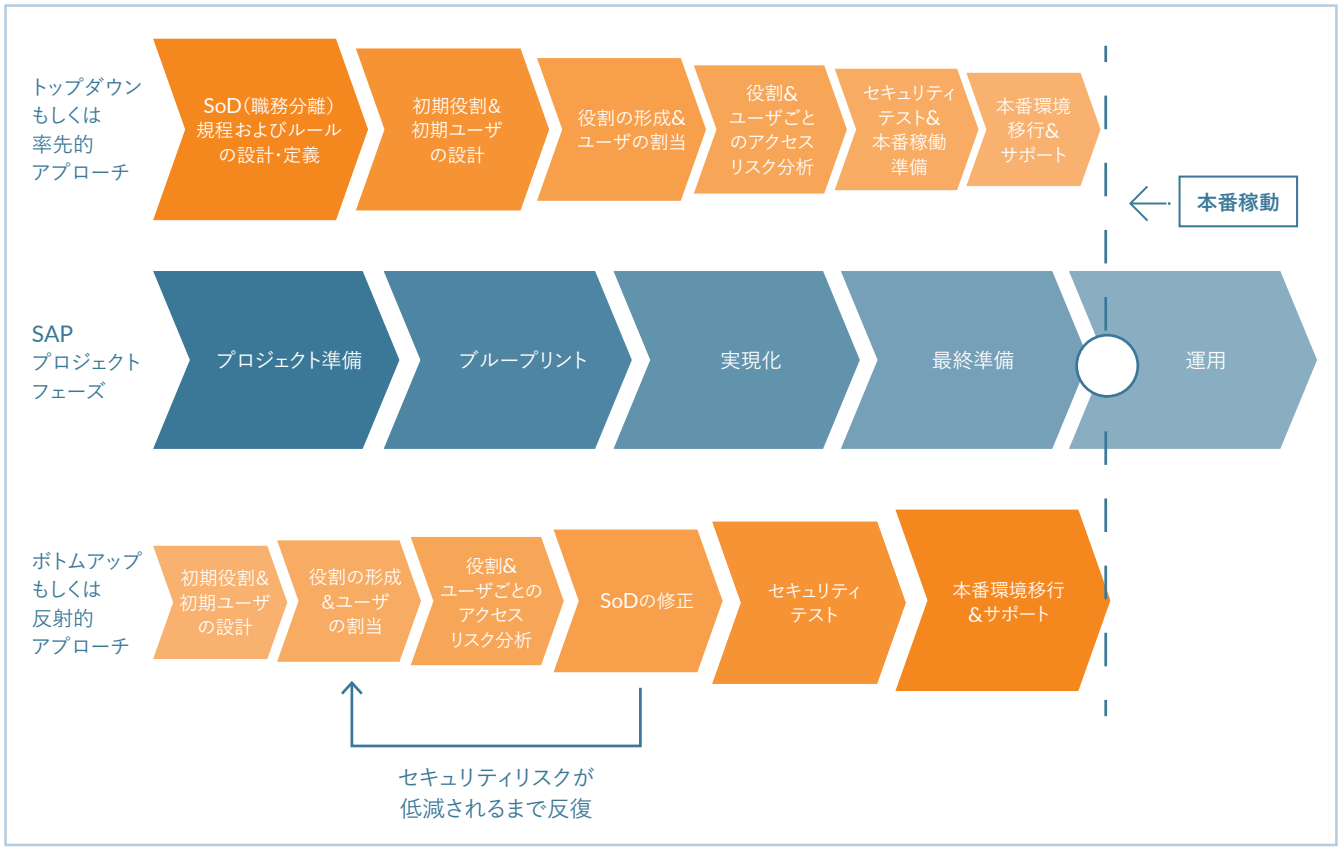
第二のアプローチであるボトムアップアプローチを採用する企業は、SAP導入の初期段階では権限リスクやコンプライアンス要件に対処せず、ロール構築およびユーザへのアクセス権付与後、または稼働後に、権限リスクおよびコンプライアンス要件を評価します。このアプローチは、主にSAPを初期導入する企業で多く採用されます。短期的には時間の効率性が高いように見受けられますが、過度のアクセスおよび多大な職務分掌に関するコンフリクトが原因で、権限設計の見直しはもとより、多くの場合においては再設計が必要となり、最終的に膨大な時間が必要となる方法です。

また、ボトムアップアプローチは、多数の職務分掌に関するコンフリクトを解決しなくてはならない場合や、財務的な規制および監査要件に準拠するためにSAPロールを変更しなくてはならない場合には、特に非効率なアプローチです。加えて、この方法は、既存の職務分掌に関するコンフリクトを解決するために、更に新たなロールが作成されることで相当数の不要なSAPロールが構築されるリスクがあります。しかも、こうしてSAPロールを作成することは根本原因の解決には至らない場合が多いのです。

SAPの導入、アップグレード、または再導入プロジェクトの初期段階でSAPの権限要件を定義することで、稼働前に効率性および権限リスクの緩和を担保します。

また、SAP Access Controlまたは類似のソリューションといったアクセス・マネジメント・テクノロジーを活用することで、システムの構築、展開、および稼働の各段階において、権限設計要件および職務分掌の制約が適切に管理されていることをモニタリングすることが重要です。

• • • SAPアプリケーションセキュリティ形成のためのアプローチ



トップダウンアプローチによるSAP権限設計

1. 職務分掌規程およびルールセット設計の定義

トップダウンアプローチを用いてSAPアプリケーション権限を実装するための第一の手順は、ビジネスプロセスオーナ（BPO）、SAP機能リーダー、およびコンプライアンス組織と連携し、SAPプロジェクトのスコープであるビジネスプロセスおよびアプリケーションを特定し、異なるSAPのモジュール（例：財務会計、管理会計、在庫/購買管理）およびSAPアプリケーション（例：サプライチェーン管理、人事管理）が各ビジネスプロセスでどのように活用されるかを定義することです。一連のミーティングおよび検証ワークショップを通じて、リスク、リスク評価、コンプライアンスおよび監査要件に関する職務分掌ポリシーを含む、職務分掌管理フレームワークを策定します。

• • • SoD管理フレームワークの重要構成要素

	定義	例
スコープ内 SAPアプリケーション	リスクに関連する情報が入力・処理されるシステム、モジュールもしくはアプリケーション	SAP売掛金(AR)モジュール、サプライヤー関係管理(SRM)アプリケーション 等
ビジネスリスク	SoDのルールとセキュリティを推進する全体的なリスクの定義	不正:内外部の人間によって犯される、資産価値および風評に悪影響を与える意図的な行為、隠ぺいされた行為、もしくは不正な利益
リスク ディスクリプション	SAPのシステムにおいて、アクセスが許可された際にユーザが可能な行為の定義	不正もしくは未承認の小切手を処理する。
SoD機密 アクセスルール	適切なモニタリング無しにユーザに提供された場合にリスクを引き起こすまたは増加させるジョブ機能	調達から支払までのトランザクションの作成または変更、およびマスタデータの更新
ジョブファンクション	特定のユーザに割り当てられたタスク	仕入先マスタ勘定の作成、支払転記等
SoDルール	競合するジョブ機能に関連するSAPトランザクション、およびそれぞれの権限オブジェクト	仕入先変更(共通)(例: XK02)と自動支払プログラムパラメータ(例: F110)

フレームワーク定義プロセスの一環として、以下の例で説明するように、職務分掌ポリシーはリスクレベル（例：重大、高、中、低）に分類する必要があります。これにより、ロール構築や権限改修フェーズにおいて、マネジメントがフォーカスする領域の優先順位付けを行うのに寄与します。

- **重大リスク：**
  - 業務または企業価値への重大な影響をもたらすリスク
  - 低減することができない、改善が求められるリスク

- **高リスク：**
  - 直接的な財務虚偽リスクまたは損益に重大な影響をもたらすリスク
  - 企業イメージに影響するリスク
  - 標準的なベストプラクティスからの逸脱または法規制違反のリスク
  - マスタデータガバナンスまたはトランザクションデータの不整合が生じるリスク
  - 紛失や盗難の原因となるリスク
  - 効果的なマネジメントレベルレポートによって低減される可能性がある、または改善が必要となるリスク

- **中リスク**
  - 財務諸表における再分類
  - 損益への中程度の影響（例：収益の一部、重要性、潜在的損失）
  - 業務プロセスの中断（財務諸表への影響はなし）
  - 社内ポリシー違反
  - マネジメントレベルレポートによって低減することができる

- **低リスク**
  - リスク低減コストがビジネスに対するリスクのコストを上回る

上記の定義は、組織および業界特有の基準に基づいており、企業により異なります。職務分掌ポリシーおよびリスクが特定された後、SAP標準およびカスタムトランザクションを評価し、特定のリスクに関するデータの作成、更新、転記、または削除に関するトランザクションを識別します。最終的に、これらのSAPトランザクションはジョブ機能（例：総勘定元帳勘定の作成、支払の転記）とグループ化され、ロールまたはユーザレベルにおける職務分掌に関するコンフリクトの分析に用いられる、自動SAP権限モニタリングソリューション（SAP Access Controlや類似のソリューション等）において、ルールセット[1]として設定される必要があります。

職務分掌ポリシーやリスク定義に加え、機密性の高いSAPトランザクションを定義し、グループ化し、区別する必要があります。これにより、仕入先価格一覧、顧客一覧、部品表（BOM）、機密性の高いSAPテーブル、財務データ、および人事情報などの機密情報へのアクセス権の追加、変更、または表示が可能であるSAPロールおよびユーザのモニタリングや報告が可能となります。

SAP S/4HANAシステムユーザ

SAP S/4HANAの導入により、職務分掌に関するルールセットは、200を超える新規トランザクション、従来のトランザクションおよびチェックの統合/交換（例：簡略化された財務会計および物流、ビジネスパートナ）を含む新たな権限階層の導入による変更を再評価し、反映する必要があります。

1 ほとんどのSAPアクセス・マネジメント・ソリューションには、標準/定義済みの職務分掌ルールが含まれていますが、これらのルールは会社のリスクプロファイルを反映するように、リスクレベル（重大、高、中、低）と合わせて調整される必要があります。さらに、権限パラメータ（権限オブジェクト）が権限設計を反映するように調整されていない場合、これらの標準的なルールセットによって偽陽性が報告されてしまうことがあるため注意が必要です。

2. 初期ロールおよびユーザ設定

職務分掌ポリシーおよびSAP Access Controlにルールセットを定義した後は、SAPロールの初期設計を行います。この手順は、将来のビジネスプロセスを見直し、SAPシステムの稼働後に実施される個別タスクおよびSAPトランザクションの予備分析を実行することから始まります。この時点で、SAPアプリケーション権限チームがトランザクションをSAPロールにグループ化しますが、トランザクション機能に関連するロール設計に利用可能な文書が限られているため、事前に定義されたロールテンプレート無しでは困難な場合があります。

更新されたSAPロールに含める一連のSAPトランザクションを定義するもう一つの方法は、SAPのトランザクション履歴を確認することです。新規SAP導入の場合ではトランザクション履歴は利用できないため、この方法は、SAPのアップグレードおよび権限再設計プロジェクトのみに適用されます。この方法では、トランザクション履歴を分析し、新たに設計されるSAPロールに含まれるべき月次、四半期、年次の一連のトランザクションを定義します。

初期のトランザクショングルーピングの次は、BPOとのワークショップを実施し、ビジネスプロセスおよびSAPトランザクショングループの整合性が保たれていることを検証します。この段階で、ロールの技術的な名称およびトランザクションコードを含む「ロールテンプレート」が文書化されます。ロールテンプレートは、会社コード、原価センタ、伝票タイプなどの権限制限に関する重要な情報が含まれている場合があります。（注：これらのパラメータは、SAPプロジェクトの経過と共に変化する可能性があります。導入中は、“To-be”のビジネスプロセスが適宜調整されます。）

• • • SAPのロールテンプレート例

ロール名	トランザクションコード*	トランザクションコード詳細
請求ロール Z:US_SD_BLLNG	FBL5	得意先明細照会
	VF01	請求伝票登録
	VF02	請求伝票変更
	VF04	一括請求更新
	VF11	請求伝票取消
	VF31	請求伝票からの出力
	Z038	請求期日に関する出荷伝票
SD 得意先マスタビュー Z:US_SD_CUSTMST_SLSVIEW	VD01	得意先登録(SD)
	VD02	得意先変更(受注)
	VD03	得意先照会(SD)
	VD04	得意先コード変更(販売)
ブロック中請求伝票ロール Z:US_SD_BLCKD_BLLNG	VF02	請求伝票変更
	V.23	請求ブロック中販売伝票

*一部のトランザクションコードはSAP S/4HANAでは利用不可となっています。

ロールおよびユーザ設計フェーズにおける次の重要な手順は、各ユーザテンプレートのロールオーナーを定義することです。ロールオーナーは通常、機能的な導入またはビジネスチームの一員であり、SAPトランザクションおよびロールにより更新されるデータの管理および報告の責任者です。例えば、コントローラは財務関連のロールを担うことになります。ロールオーナーとしての責任には、ロールに含まれるSAPトランザクションのレビューと承認、およびロールの継続的なメンテナンス（例：トランザクションの追加、削除、コンフリクトが発生した場合のコントロールの承認）が含まれます。

• • • SAP権限の検討事項

「ジョブベース」または「タスクベース」ロール

SAP権限の設計時に第一に行う重要な意思決定は、「ジョブベース」または「タスクベース」のどちらを使用するかどうかです。ジョブベースロールは、ユーザが担当するタスクをすべて包含する1つのロール（例：債務管理マネージャ）を、各ユーザに割り当てられることを意味します。このアプローチでは、ロールの数は限られていますが、ユーザが必要でないトランザクションコードへのアクセスも可能となります。このように、多数のトランザクションコードにアクセスが可能であることにより、ロール内に職務分掌に関するコンフリクトが生じる可能性があります。一方、タスクベースは、ジョブタスク毎のロール（例：購買申請のリリース）を、各ユーザへ複数割り当てることを意味します。このアプローチでは、複数のロールを利用することになりますが、ユーザの各タスクへのアクセスを制限することができます。ジョブベースまたはタスクベースのどちらのアプローチを使用するかは、全体的な職位の一貫性、およびSAPアクセス要請と従業員の採用・異動・退職プロセスの統合に関する人事部門の成熟度により決定されます。

単一または集合ロール

もう一つの決定事項は、グループ化された複数のロールが別のロール内で保持される集合ロールを使用するかどうかです。ジョブベースロールは、複数のタスクベースロール（集合ロール）により構成されることが一般的です。集合ロールの主な利点は、各ユーザに1つのロールが割り当てられることにより、ユーザプロビジョニングプロセスが簡易化されることです。一方で、集合ロールに追加タスクやバックアップとしての責任が含まれることで、ユーザが必要以上にアクセス可能である点が、主な欠点にあげられます。

カスタムまたは既製のSAPロール

SAPシステムには、既製のロールが事前に提供されており、権限設計を調節する代わりに、これらのロールを導入することができます。しかし、SAP権限を維持するための長期的な戦略として既製のロールが使用されることは推奨されません。これらは、幅広いジョブタスクを一つのロールとして設計しているため、過度なアクセスを許可することなくロールを割り当てることが極めて難しくなります。さらに、ビジネスアクセスの要件およびコントロールの制限を満たさない可能性があります。

人事・ポジションベース設計または機能設計

SAP権限設計時のもう一つの検討事項は、人事プロセス（例：採用、退職）との統合レベル、および職務記述や職位との全体的な一貫性です。理想的なシナリオではSAPロールが職務を反映することが求められますが、人事部門および職位の成熟度が低い場合、または一貫性に乏しい場合は、機能に基づいた独立した権限設計が最適となります。ポジションベースの設計を適用するためには、職務記述が明確に定義され、社内で一貫している必要があります。また、統合されたプロビジョニングを可能にするには、雇用開始から退職に至るまでのプロセスが、成熟段階にある必要があります。

SAP S/4HANAシステムユーザ

従来のSAP GUIのほか、ユーザインターフェースとしてSAP Fioriを使用する場合、ユーザはバックエンドトランザクションコードにアクセスする必要が無くなり、代わりにFioriアプリケーションを使用して、S/4HANAシステム内の様々な機能にアクセスします。S/4HANAの役割は、エンドユーザによるFiori UI上の特定のアプリケーションへのアクセスを許可するために必要な追加の承認、およびマッピングを含むように設計される必要があります。SAP S/4HANAの場合、HANAデータベース内で作業を行う個人（例：アドミニストレータ、データモデリング担当者、開発者、サポートスタッフ）、およびデータベースから直接データを読み取るエンドユーザは、HANAデータベースへのアクセスが必要です。ユーザがSAP HANA内の重要なデータに直接アクセスする必要がある場合は、データベースにアクセスするユーザのタイプに基づいてデータを保護し、アクセスを制限するために、特権のロール設計が必要になります。

3. ロール構築およびユーザ割当

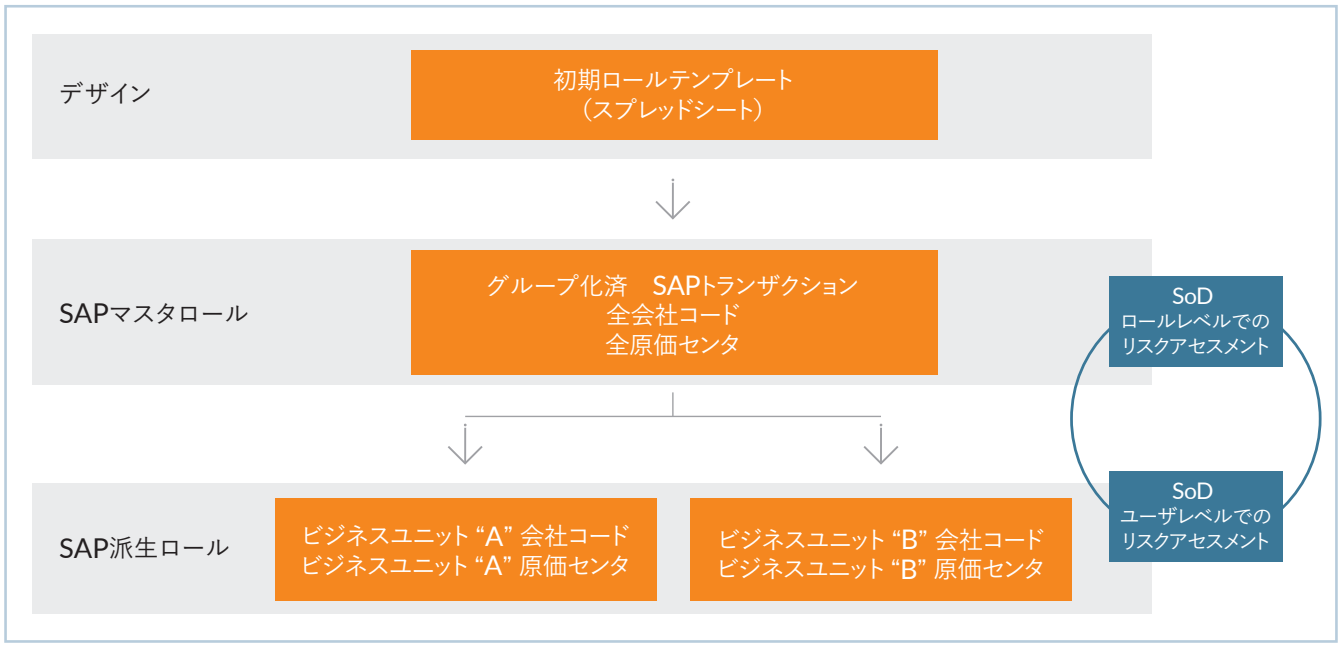
ロールテンプレートが設計され、承認されると、ロールがSAPに構築され、その後エンドユーザに割り当てられます。技術的な設計フェーズは、グループ化されたトランザクションを含む「マスタロール」または「テンプレートロール」の構築から始まります。マスタロールの構築には、システムインテグレータおよびBPOとの緊密な連携が必要です。これにより、ロール設計の一部として使用されるすべての標準およびカスタムSAPトランザクションやオブジェクトが機能面から理解され（例：マスタデータ作成、財務諸表の更新）、ロールテンプレートに適切に組み込まれます。SAPロール設計における第二の手順は、権限制限（例：会社コード、原価センタによる制限）が適用される「派生」ロールまたは「子」ロールを作成することです。

SAPプロジェクトの早い段階で職務分掌に関するコンフリクトが存在しないロールを設計することで、ユーザに与えられた権限に関する透明性が高まるのみならず、細分性が高まり、アクセスがより効果的に制限されることが期待できます。さらに、新たなSAP機能の導入や、組織の再編成に付随するユーザの責任に関する変更への対応がより柔軟になるため、継続的な権限メンテナンスの効率化も可能となります。

エンドユーザの割当は、各ユーザに適用される必要がある制限が異なるため（例：シェアードサービス部門の場合、ユーザにより、アクセスする必要がある会社コードや原価センタが異なる）、SAPアプリケーション権限を設計するうえで重要な手順です。

これらの手順では、SAP Access Controlや他のSAP権限モニタリングソリューションを活用し、ロールをエンドユーザに割当てる前に、ロールに職務分掌に関するコンフリクトが存在しないことを確認することが重要です。マスタロールに固有のコンフリクトが存在する場合、すべての派生ロールおよび当該ロールを割り当てられたユーザにもコンフリクトが発生します。

• • • SAPのロールの作成およびユーザ割り当てプロセス



4. ロールおよびユーザアクセスのリスク分析

この段階では、SAP Access Controlまたは別のSAP権限モニタリングソリューションを活用して、定期的なロールおよびユーザ分析を実施し、新たに設計されたSAPロールが職務分掌ポリシーに準拠しているか判断する必要があります。これは、SAP権限設計に影響を与える変更をシミュレーションし、モニタリングを実施し、コンフリクトが発生する恐れがある場合は、適時BPOにフィードバックすることによって行われます。

リスク分析は、定期的に実施される必要がありますが、プロセス改善においてSAPシステム設計が更新される際のユニットテストおよび統合テスト後には、特に必要です。また、SAPプロジェクトの過程で新たなSAPトランザクションがビジネスプロセスへ追加される場合、または新たなカスタムトランザクションが開発される場合、SAP Access Controlで定義されたSAPルールセットが変更される可能性があることに注意が必要です。

SAP環境が「クリーン」かつ「コンフリクトフリー」であることを保証するためには、妥当なSAP権限プロビジョニングプロセスを設計し、実行する必要があります。このプロセスには、ユーザアクセスの許可またはロールの変更を実施する前に、SAP権限チームよるSAP Access Controlを用いたリスクシミュレーションの実施が含まれます。このシミュレーションにより、ロールまたはユーザの変更が職務分掌または過剰なアクセス権限リスクを引き起こしていないかを確認できます。さらに、プロジェクトの本番稼働日が近づくと、継続的モニタリングの手順を確立し、準拠する必要があります。また、定期的に権限の変更を検証するため、BPOおよびロールオーナーによる職務分掌違反レポートのレビューを含む、発見的なSAP権限モニタリングプロセスも確立する必要があります。SAPアップグレードまたは権限再設計プロジェクトの場合、稼働後のタスクに、新規ロールの割当と管理、および時間経過によるレガシーロールの使用停止などの追加の変更管理プロセスが含まれる場合があります。

SAP S/4HANAシステムユーザ

新しい権限階層の導入によるアクセスリスクに対処するために、SAPアクセスコントロールの機能は、S/4HANA環境全体へと拡張する必要があります。ユーザがFioriおよびHANAデータベースへのアクセスが可能な場合、システムアーキテクチャレベル（追加コネクタの設定）およびAccess Controlツールの機能レベル（ワークフローの変更）両方での変更を行う必要があります。

5. 権限テストおよび稼働準備

SAP権限ユニットテスト（UT）およびユーザ受け入れテスト（UAT）は、稼働前にユーザアクセスに関する問題が最小限であることを担保するための重要な手順です。SAP権限テストは、ロール内のすべてのトランザクションを実行し、当該ロールが、プロセスを完了するために必要なトランザクションおよび承認オブジェクト（例：金融取引の照会、更新および転記）を保持していることを確認します。これらの手順は、プロジェクトの機能テスト（SAP導入またはアップグレードプロジェクト）、または本番環境における新規ロールの割当前（権限再構築プロジェクト）に実行される必要があります。権限テストには、正式な職務分掌および機密性の高いアクセスレビューが含まれ、新たに作成された、または更新されたSAPロールに、職務分掌に関するコンフリクトが存在しないこと、および重要な機能（例：仕入先マスタの更新、勘定コード表の更新）が適切に制限されていることを確認する必要があります。

機能テストフェーズの初期段階でSAP権限チームを関与させることで、ロールの修正の手遅れ、または費用の高騰が生じる前に、潜在的な権限の問題を発見することが可能です。また、最終的なUATプロセスでは、本番環境で使用されるSAPロールを用いて、品質保証環境にテストユーザ（正確なSAPロール割当を持つユーザ）を作成することが非常に重要です。これにより、SAPプロジェクトの本番稼働前に、コンフリクトの検証を含む権限変更の適切な識別、および関連する問題の改善が可能になります。

BPO, ロールオーナー、およびSAP権限チームと緊密に連携し、コンフリクトが存在するロール内のトランザクションコードの再グループ化、コンフリクトが存在するユーザへのロールの再割当を実施することで、コンフリクトを改善することが重要です。従業員が限られている場合など、容認された理由により職務分掌に関するコンフリクトが解決できない場合は、補完的なコントロールを特定し、文書化する必要があります。

SAP S/4HANAシステムユーザ

S/4HANAでは、プレゼンテーション（Fiori）およびデータベース（HANA）レベルで導入された権限レベルを考慮し、テストステップを更新する必要があります。アプリケーションレベル（SAP S/4HANA）のテスト手順では、統合 / 簡略 / 削除されたトランザクションを考慮する必要があります。

6. 本番環境への移行およびサポート

テストが完了すると、新たに設計されたSAPロールは、企業の変更管理規程に基づいて本番環境に移行され、ユーザの割当が可能になります。ERPシステムおよび組織のプロセスの導入・変更は複雑であるため、UTおよびUATの効果的な実施にも関わらず、稼働日、安定期、および稼働後に、アクセスに関する問題が発生する可能性は非常に高いです。

稼働日および安定期に生じるSAPアクセスに関する問題に対処するために、特別に配属されたサポートチームを構成することが重要です。このチームは、アクセスに関する問題を適時解決するだけではなく、アクセスレポートを実行し、権限の変更が職務分掌上、または他のアクセスリスクを引き起こす可能性がないかを確認します。また、影響を受けるユーザがSAPシステムの稼働に関連する変更や、サポートプロトコルを認識できるように、コミュニケーションの計画を立てる必要があります。

SAP導入およびアップグレードプロジェクトにおける一般的な事例として、稼働日および安定期に「パワーユーザ」に対して、一時的に広範なアクセスを可能にすることがあります。これは、SAP Access Controlを用いてトランザクションおよびパワーユーザのアクションログをレビューすることで、稼働日および稼働後にユーザがジョブ機能を実行することが可能であることを確認し、新規システムの安定化を支援することを目的に実施されます。システムの新規導入の安定で、一時的なアクセスを見直し、削除することが重要です。

また、SAPプロビジョニング・ソリューションを活用し、ユーザプロビジョニングプロセスを自動化することが推奨されます。例えば、SAP Access Controlは、ロールの承認および割当を自動化することにより、ペーパーレスのSAP権限プロビジョニングが可能になり、ウェブページ上で数回クリックすることで可能となります。ユーザ割当プロセス中に問題が検出された場合、承認パスは自動的にリダイレクトされるため、適切なロールオーナーは、アクセスが許可される前に職務分掌に関するコンフリクトを解決することが可能です。

おわりに

SAP権限の設計、設定、および導入は、複雑かつ多くのリソースを要する作業です。SAPプロジェクトの初期段階で、SAPアプリケーション権限を構築するアプローチを検討する必要があります。適切な権限要件をシステム構築プロセスに組込みことで、再設計の必要を最小限にすることができます。SAP Access Controlなどの自動権限モニタリングソリューションや、ベストプラクティスを適用することで、権限設計の効率化や高速化、およびコンフリクトのないSAPロールの構築が可能となり、SAP権限の再設計が生じる可能性を大幅に削減できます。

以下のいずれかの基準を満たす企業は、SAP権限環境を見直し、維持するために、SAP権限設計への対処、またはSAP権限モニタリングの最適化を検討する必要があります。

- 組織固有の職務分掌ポリシーが定義されていない、承認されていない、または職務が適切に反映されていない
- 新たなロールの作成およびロールの割当により、改善または緩和を必要とする職務分掌に関するコンフリクトが発生する
- ロール内に、多数の職務分掌に関するコンフリクトが存在する
- SAP環境は、ユーザ数よりも多くのロールで構成されている
- 職務分掌のチェックは、マニュアルで実施されている
- プロビジョニングプロセスや継続的なモニタリングをサポートするSAP Access Controlなどの自動権限モニタリングソリューションが導入されていない
- 職務分掌に関するリスク管理プロセスにおける業務側の関与が欠如している

SAP S/4HANAシステムユーザ

S/4HANAへ移行する場合、新たなデータモデルの導入による変更や、追加の階層が生じていることを認識し、費用対効果に優れた適切な権限アーキテクチャを開発することが求められます。

THE AMERICAS

UNITED STATES
Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Fort Lauderdale
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Winchester
Woodbridge

ARGENTINA*
Buenos Aires

BRAZIL*
Rio de Janeiro
Sao Paulo

CANADA
Kitchener-Waterloo
Toronto

CHILE
Santiago

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE MIDDLE EAST AFRICA

FRANCE
Paris

GERMANY
Frankfurt
Munich

ITALY
Milan
Rome
Turin

NETHERLANDS
Amsterdam

UNITED KINGDOM
London

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

SOUTH AFRICA*
Johannesburg

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

ASIA-PACIFIC

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

INDIA*
Bangalore
Hyderabad
Kolkata
Mumbai
New Delhi

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

*MEMBER FIRM

プロティビティLLC

お問い合わせ先：マーケティング部 pj-mktg@protiviti.jp

〒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
〒541-0056 大阪市中央区久太郎町 4-1-3 大阪センタービル Tel. 06-6282-0710［代表］ Fax. 06-6282-0711 protiviti.jp

protiviti®