



## SAPソリューション要約

### SAP Solutions for Governance, Risk, and Compliance

## SAP® GRC ACCESS CONTROL

### アクセス権限のリスクの特定、排除、回避

SAP® GRC Access Controlは、アクセス権限の統制を監視、テスト、および実装するためのアプリケーションです。このアプリケーションは、サーベンス・オクスリー法(SOX法)や他のコンプライアンス対応を支援するために設計されており、企業はシステムのアクセス権限のリスクを迅速に特定して排除し、職務分掌違反が生じないように、予防的な統制をビジネスプロセスに組み込むことができます。その結果、コンプライアンス対応にかかわる時間、リスク、およびコストが飛躍的に削減されます。

企業は、なぜコンプライアンス要件を満たすことに苦勞しているのでしょうか。多くの企業では、多種多様なマニュアル作業による統制活動と、細分化されたシステムを用いてコンプライアンスに対処していますが、このことがガバナンス強化、リスク管理、コンプライアンス(GRC)に関連するコストと複雑さを増大させています。こうしたシステムの細分化は、アクセス権限の統制管理に重大な影響を及ぼします。アクセス権限の統制管理は、有効なコンプライアンス体制を構築する上で最も重要なIT統制のうちの1つです。企業は米国のサーベンス・オクスリー法(SOX法)などの世界中のさまざまな法規制に従って、強力かつ有効なアクセス権限の統制を確立する必要があります。ビジネスプロセスとそれを支えるシステムは、何千ものアクセス権限に関するルールを構築する上で、密接に関係します。それらのルールの分析と比較、潜在リスクの検知、そして統制の実装に関する意思決定をする際に、IT部門と業務部門が必要とする情報を共有するプロセスを自動化するソフトウェアがなければ、アクセス権限の統制を有効に管理することはできません。

### 多くのお客様に認められたSAP® Solutions for GRC

SAP® solutions for governance, risk, and complianceは、全業種共通のさまざまな法規制や業種別の法規制に対処するための全体的なアプローチを提供します。このソリューションには、アクセス統制、プロセス統制、環境コンプライアンス、および貿易コンプライアンスに対処するアプリケーションが含まれています。SAP Solutions for GRCの重要なアプリケーションの1つであるSAP GRC Access Controlを使用すれば、全社レベルのアクセス権限のリスクを検知、是正、軽減、および回避するプロセスがエンドツーエンドで自動化されます。この自動化は、正確な職務分掌、コスト削減、リスク軽減、および業績の向上につながります。

企業は総合的なGRC活動の一環としてSAP GRC Access Controlを導入することで、コンプライアンスリスクやオペレーショナルリスクに低コストで対処できます。競合他社が場当たりのコンプライアンス対応から抜け出せないでいる間に、SAP GRC Access Controlを使用している企業は、迅速なコンプライアンス対応によって、競争力を高めることができます。

## アクセス権限の統制コンプライアンス

世界中で500社を超える企業が、アクセス権限の統制プロセスを管理するためにSAP GRC Access Controlを選択しています。SAP GRC Access Controlには、アクセスリスクの分析と是正、ロール管理、スーパーユーザ管理、およびコンプライアンス要件を考慮したユーザプロビジョニングを実現する、エンドツーエンドのアクセス権限管理機能が含まれます。また、SAP GRC Access Controlは、英語、フランス語、ドイツ語、日本語、ポルトガル語、およびスペイン語を含む、多言語をサポートしています。

## アクセスリスクの分析と是正措置

SAP GRC Access Controlは、リアルタイムコンプライアンスを実現し、セキュリティと統制の違反を未然に防ぎます。このソフトウェアを約1週間で実装した後、最新の権限設定の分析、潜在リスクの探知、および全社レベルのアクセス権限の効果的な統制が可能になります。

## 最新権限データの分析

SAP GRC Access Controlでリスクを評価するには、一旦、別のアプリケーションに権限データをダウンロードすることなく、常にERP等のビジネスアプリケーションに含まれる最新のデータを使用するため、職務分掌上のコンフリクトを即座に特定し、根本原因を突き止め、迅速に問題を解決できます。

## 潜在リスクの検知

SAP GRC Access Controlは、監査が実施されるまで発見されることのないかもしれない潜在的なリスクの検知に役立ちます。たとえば、IT部門はこのアプリケーションを使用して、何千ステップものカスタムプログラムを即時に分析し、リスクが顕在化する前に潜在的なユーザアクセスに関する問題を検知して処置できます。

## 職務分掌の実施

より効率的に職務分掌上のルールを定義するために、このアプリケーションはSAP、Oracle、PeopleSoft、およびJD Edwards等のアプリケーションを対象とした職務分掌(SoD)ルールに関する最も包括的なデータベースを提供します。また、このアプリケーションでは、IT部門以外の担当者が一般的なビジネス言語を使用して、自社独自の職務分掌ルールを簡単に作成できます。

## 全社リスク管理

SAP GRC Access Controlでは非SAP製品も対象とするため、業務ごとに異なるアプリケーション用に別のアクセス統制ソフトウェアを導入する必要がありません。このアプリケーションはSoDリスクを可視化し、「対象とするビジネスプロセスの範囲の広さ(会計、販売、購買、人事、等)」、および「異種アプリケーション(非SAP、自社開発システム)との統合」という特徴を生かして、アクセス権限のリスクを検知、排除、および回避します。「購買～支払」や「受注～入金」のようなコアプロセスに対応した、サンプルルールが含まれているのはSAP GRC Access

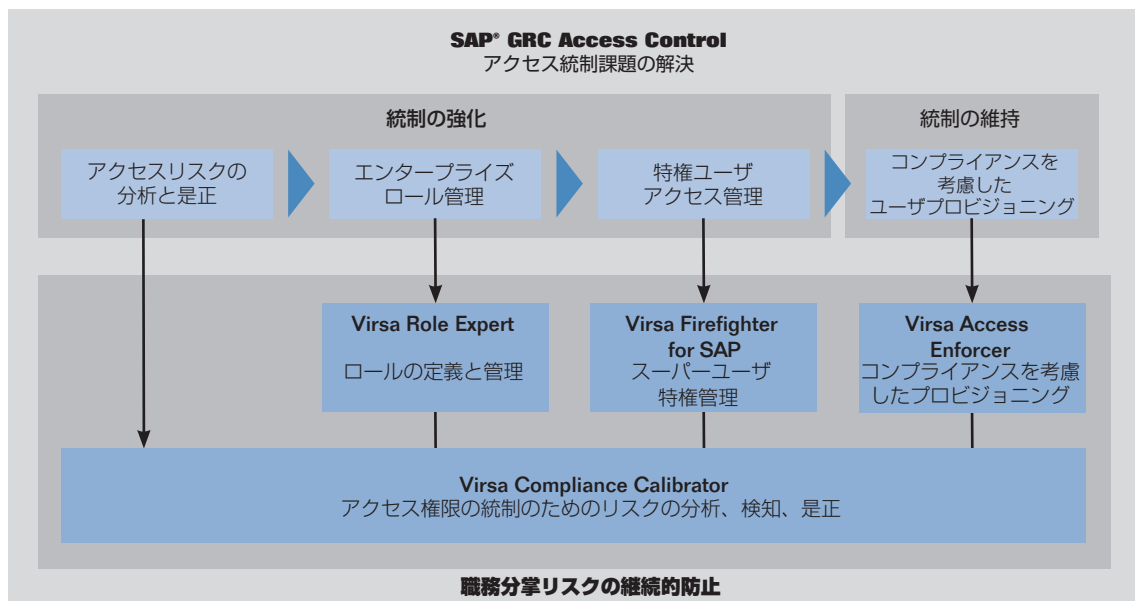


図1: SAP GRC Access Controlによるエンドツーエンドコンプライアンスの実現

## クロスアプリケーション機能

SAP® GRC Access Controlはこれらのビジネスアプリケーションに対応しています。

| SAP GRC ACCESS CONTROL   |  |  |   |   |
|--|--|--|---|---|
| SAP  | Oracle   | PeopleSoft   | JD Edwards  | Hyperion  |
| <ul style="list-style-type: none"> <li>■ 人事管理</li> <li>■ 購買～支払</li> <li>■ 受注～入金</li> <li>■ 会計                             <ul style="list-style-type: none"> <li>- 総勘定元帳</li> <li>- プロジェクトシステム</li> <li>- 固定資産</li> </ul> </li> <li>■ ベーシス、セキュリティ、システム管理</li> <li>■ 在庫 / 購買管理</li> <li>■ Advanced Planning and Optimization</li> <li>■ Supplier Relationship Management</li> <li>■ Customer Relationship Management</li> </ul> | <ul style="list-style-type: none"> <li>■ 人事管理</li> <li>■ 購買～支払</li> <li>■ 受注～入金</li> <li>■ 財務                             <ul style="list-style-type: none"> <li>- 一般会計</li> <li>- プロジェクトシステム</li> <li>- 固定資産</li> </ul> </li> <li>■ システム管理</li> </ul> | <ul style="list-style-type: none"> <li>■ 人事管理</li> <li>■ 購買～支払</li> <li>■ 受注～入金</li> <li>■ 財務                             <ul style="list-style-type: none"> <li>- 一般会計</li> <li>- 固定資産</li> </ul> </li> <li>■ システム管理</li> </ul> | <ul style="list-style-type: none"> <li>■ 人事管理 / 給与計算</li> <li>■ 購買～支払</li> <li>■ 受注～入金</li> <li>■ 財務                             <ul style="list-style-type: none"> <li>- 一般会計</li> </ul> </li> <li>■ 連結</li> </ul> | <ul style="list-style-type: none"> <li>■ カスタムルール</li> </ul> |

図2: 企業全体のプロセスをサポートするソリューション

Control だけです。SAP パートナエコシステムを背景に、Oracle、PeopleSoft、JD Edwards、および Hyperion を含む、さまざまなベンダの企業アプリケーションへのコネクタが多数提供されています。

SAP GRC Access Control では、Virsa Compliance Calibrator アプリケーションを利用して、アクセスリスクの分析と是正措置が提供されます。

### エンタープライズロール管理

SAP GRC Access Control は、標準化および集中管理されたロール設計、テスト、モニタリングを継続させることによって、アクセス管理問題の根本原因に対処します。そのため、このソフトウェアはマニュアル作業によるエラーの排除に役立ち、アクセス管理のベストプラクティスの適用がより簡単になります。IT 部門と業務部門のオーナーは、ロール定義の記録、リスク自動評価の実行、変更の追跡、および保守の実施を簡単に行うことができることから、職務分掌に関する情報の共有が強化され、IT コストが削減されます。

### 監査対象ロールの定義

SAP GRC Access Control では、IT 部門ではなく業務部門のオーナーがロール管理者となります。ロール管理者は、各ロールを構成するアクションと権限の定義、承認ワークフローのトリガ、ロールステータスの記録、および変更履歴の保存を行うことができ、作業履歴を追跡する際にスプレッドシートを使用する必要がなくなります。SAP をすでにご利用され、マニュアル作業で登録された大量のロールセットをお持ちのお客様は、ロールの一括インポート機能で迅速にアップロードすることができます。SAP GRC Access Control は、業務部門のオーナーによるロールの再設計を支援します。業務部門のオーナーは、特定のトランザクションが使用されているすべてのロールを照会するか、あるいは SAP アプ

リケーションにおけるロール情報とロール定義とを比較することができます。SAP GRC Access Control のリスク分析と是正措置機能によって、ロールの本番機での利用以前の定義段階で SoD リスクが事前に認識され警告が発信されます。

### ロールの自動登録

ロールの定義後、業務部門のオーナーは簡単な操作でそれらのロールを登録できます。このアプリケーションではプロファイル生成機能が活用されているため、このプロセス中にデータをマージする必要がなくなります。業務部門のオーナーは、SAP GRC Access Control で SAP アプリケーション内の権限設定とロール定義を比較して、ロールの完全性を確保することができます。また SAP GRC Access Control では、レポートと分析の履歴を記録して、監査人の要件に対応します。

SAP GRC Access Control では、Virsa Role Expert アプリケーションを利用して、エンタープライズロール管理機能が提供されます。

### 特権ユーザアクセス管理

どのようにすれば、企業はコンプライアンス違反を犯さずに、緊急時のシステムへの特権的なアクセスをユーザに許可できるでしょうか。

### 迅速かつセキュアなスーパーユーザログオンの実現

緊急時に SAP GRC Access Control では、ユーザが監査可能な制御環境下でスーパーユーザのような特権をもって、自らのロール外の作業を実行できます。それには一時的な ID を割り当て、ユーザに特権を与えながらも制御されたアクセスを許可することができます。このソフトウェアは簡単に設定することが可能で、管理も容易です。また、このソフトウェアは他の SAP ソフトウェアと同じような操作で利用可能です。

### スーパーユーザ活動の追跡

このアプリケーションは、特権ユーザIDを使用してスーパーユーザが実行するすべての作業を追跡、監視、および記録します。Webベースのレポートでは、業務部門のオーナーと監査人に対して、SAPソフトウェア環境全体における利用状況についての詳細レポートが提供されます。作業ログでは、項目値レベルまで作業内容が記録され、簡単にフィルタ、ソート、およびダウンロードできます。

SAP GRC Access Control では、Virsa FireFighter for SAP アプリケーションを利用して、特権ユーザアクセス管理に対応します。

### コンプライアンスを考慮したユーザプロビジョニング

システムへのアクセスを許可および解除する際に、企業はそれが SoD 上、どのような影響を及ぼすかについて見落としがちです。SAP GRC Access Control を使用すると、ユーザID管理プロセス全体を通してコンプライアンスを考慮したユーザプロビジョニングが可能であり、SoD 違反を防止できます。企業はプロビジョニングの自動化、SoD リスクのテスト、承認の効率化、および IT 部門の作業削減を実現できます。

### 自動プロビジョニングワークフロー

SAP GRC Access Control は、複雑な承認プロセスでも自動化します。直感的でわかりやすい Web ベースのインタフェース上で、ユーザは自身の業務内容に従って、ロールを選択し、アクセス申請を行うことができます。ロールコンテンツは SAP GRC Access Control のエンタープライズロール管理機能で定義されます。SAP GRC Access Control のワークフローエンジンでは、申請者の役職と申請された権限タイプが考慮され、承認パスが自動的に決定されます。このアプリケーションでは、本来の承認者が対応できないか、あるいは回答しない場合に、代替の承認者に申請データを回すことで、アクセス承認の遅延を回避します。

### コンプライアンスを考慮したユーザプロビジョニングの提供

SAP GRC Access Control はクロスシステム対応となっており、2つの方法でコンプライアンスを考慮したユーザプロビジョニングを実現します。まず、プロビジョニング前に、多様なビジネスプロセスにおけるアクセスリスクのシミュレートと検知を行います。次に、SAP や Oracle などの選ばれた複数の企業アプリケーションにプロビジョニングを行います。プロビジョニングは、SAP またはそのパートナーのソフトウェアに組み込まれたリアルタイムエージェントで、マニュアル実行または自動的に実行されます。

### リアルタイムで SoD 問題を特定

このアプリケーションでは、本稼動システムで SoD のリアルタイムシミュレーション、および SAP (または SAP 以外の) ソフトウェア環境全体のテストによって、SoD リスクを防止します。日常のビジネスプロセスにアクセス権限統制を盛り込むことで、アクセス違反の発生を回避できます。

### 承認の効率化

SAP GRC Access Control はアクセス申請のプロセスを効率化します。LDAP ディレクトリ、または人事管理データベースからユーザID情報が申請データに自動的に組み込まれるため、ユーザによる入力が必要がなくなります。承認者は、申請データへのリンクが記載された電子メールを受信しますので、このアプリケーション上で申請を簡単に閲覧および承認できます。その後、このアプリケーションでは、ユーザアカウントの自動更新前に SoD リスクがチェックされます。

### IT 部門の負担軽減

業務部門のオーナーは、IT 部門が使用している IT の専門用語を学ばなくても、SAP GRC Access Control でユーザアクセスを定義できます。業務部門のオーナーは、申請者に対してロールをマニュアル作業で割り当てるか、あるいは類似したロールを持つ他のユーザにならってアクセスを許可できます。このアプリケーションでは、セルフサービスのパスワードリセット機能が提供されています。ユーザは IT 部門の支援を受けずに、この機能でポータルにログオンし、自らのパスワードをリセットできます。この機能により、ヘルプデスクへの問合せ件数を最大 50% 削減できます。

SAP GRC Access Control では、Virsa Access Enforcer アプリケーションを利用して、コンプライアンスを考慮したユーザプロビジョニングに対応します。

### アクセスと権限のリスク統制

SAP GRC Access Control は、ユーザアクセスと権限のリスクを管理および回避するための最も包括的なアプリケーションです。詳細につきましては、<http://www.sap.com/japan/solutions/grc/> にアクセスしてください。