

SAP システムにおけるセキュリティの改善：  
SAP GRC 活用のための3つのステップ

protiviti®

すべての企業において全社的リスクマネジメント戦略を成功させるためには、その戦略の一翼を担うアプリケーションにおける強固なセキュリティ環境が不可欠である。リスクを重視した強固なセキュリティ環境では、セキュリティリスクを軽減する際、全社レベル或いはプロセスレベルのコントロールは最後の手段であって、アプリケーションシステムに内蔵されているセキュリティ管理機

能を最大限活用することが鍵となっている。近年、多くの企業は複雑なセキュリティ環境を改善、管理するために **Governance, Risk, Compliance** ソフトウェア（以下、GRC ソフトウェア）を利用し始めている。ここでは、**SAP GRC Access Control** を使用した場合を例に取り、GRC ソフトウェアの活用方法について説明する。

改善アプローチ	経験に基づくキーポイント
<p><b>ステップ1：</b></p> <p><b>SAPシステムのセキュリティリスクの把握</b></p> <ul style="list-style-type: none"> <li>• SAPシステムに内在するセキュリティリスクを把握する。</li> </ul> <p><b>ステップ2：計画の策定及び実行</b></p> <p>下記を通じて改善計画を策定する。</p> <ul style="list-style-type: none"> <li>• 起こりうるリスクの大きさを測定する。</li> <li>• プロジェクトの目的及び改善要件を決定する。</li> <li>• 改善の優先順位を決定し、実行する。</li> </ul> <p><b>ステップ3：</b></p> <p><b>権限の割当て及び継続的なモニタリングの実施</b></p> <ul style="list-style-type: none"> <li>• SAP 環境を新たなリスクから守るような手続を導入する。</li> </ul>	<p><b>プロジェクト管理</b></p> <ul style="list-style-type: none"> <li>• セキュリティ改善プロジェクトをシステム導入プロジェクトと同様に扱う。</li> <li>• 利害関係者の賛同と外部監査人のアドバイスを早い段階で得る。</li> <li>• 早い段階から改善効果を得るために、改善アクティビティに優先順位を付ける。</li> </ul> <p><b>ソフトウェア設定</b></p> <ul style="list-style-type: none"> <li>• 標準ルールセットを改良し自社の業務内容に合致したものを<b>Compliance Calibrator</b> に設定する。</li> <li>• 特権ユーザ管理に<b>Firefighter</b> を使用する。</li> <li>• GRCソフトウェアをインストールする前にSAPシステムにパッチを当てる。</li> </ul>

## コンセプトの明確化：SAPシステムにおけるセキュリティ範囲

SAPシステムには、プロファイル、ロール、トランザクションコード、権限オブジェクト、項目及びインフォタイプ複数のセキュリティないし特権の階層がある。コンプライアンスの観点から、各階層についてリスク分析が行われ、リスクは典型的に、職務分掌（SoD）、重要なトランザクションへのアクセス制限及びユーザプロビジョニングに分類される。SoDリスクは、ユーザが「仕入

先の登録」と「請求書の処理」などといった対立する2つのトランザクションが実行可能である場合に発生する。アクセス制限リスクとは、仕入先の振込先銀行情報の登録・保守など重要なトランザクションへの権限を過剰な数のユーザが有している場合に発生する。

## 複雑性の解消：改善への3つのステップ

セキュリティリスクの改善には幾通りかのアプローチがあるが、プロティビティの経験では、以下

に紹介するアプローチが、伝統的な改善ステップとSAP GRC Access Controlを効率的に統合し、その結果、早期に多大な効果を得ることができると考えている。

## ステップ1 –SAPシステムのセキュリティリスクの把握

まず、SAPシステムのセキュリティ環境をよく理解し、セキュリティリスクを把握することが重要である。セキュリティリスクの把握のために、SAPシステムでクエリを実行したり、データの抽出と纏めのために市販のツールを使用する場合もよく見かける。しかし、SAPシステムは複数階層のセキュリティ構造であるため、このようなマニュアル手法では実際には存在しないリスクを誤って検出する結果になることも多い。これに対して、SAP GRC Access ControlのCompliance Calibratorは、データを自動化して抽出し、セキュリティの全ての階層を精査するよう設定されているため、誤った検出結果を最小限に抑えることが可能となる。

## ステップ2 –計画の策定及び実行

ステップ1でセキュリティリスクが把握されたら、発見されたリスクに対する改善計画を策定する必要がある。主な作業として以下がある。

**リスクの測定：**潜在的なセキュリティリスクがどの程度存在するのかという観点から、リスクを評価し定量化する必要がある。誤って検出されたデータを取り除き、残りのリスクについて原因を特定する必要がある。Compliance Calibratorを活用した場合に、誤って検出されるデータを取り除くには、Compliance Calibrator内の重要トランザクションやSoDルールセットに関する標準設定を改良する。改良の結果、改善対象となるリスクあるいは焦点を当てるべきリスクについて、Compliance Calibratorから有用なサマリーレポート及び詳細レ

ポートが出力される。

**改善要件の決定：**どの改善プロジェクトにおいても、プロジェクトのゴールを設定し、マネジメント上どのリスク及びどの改善方法が受容できるのかを決定することが重要である。ときに外部監査人から完全に改善しなければならぬものは何かという有用なガイダンスが得られることもある。セキュリティリスクの改善に際し、費用対効果の観点からプロジェクトの選択肢が考慮され、プロジェクトスポンサーがプロジェクトをどのように進めるべきかについて意思決定できるようにすることが重要である。

**改善の優先順位付け及び実施：**リスクが定量化され改善要件が決定されたら、改善活動の費用対効果を勘案しながらリスクの重要性に応じて、優先順位付けされた改善計画を立案する。例えば、ユーザ権限から「SAP\_ALL」を外すことによって、工数をかけずにSoDリスクを飛躍的に減らすことができる。改善すべき領域が優先順位付けされたら、以下の作業を行う。

- **不要なアクセス権限の整理** – この作業は、基本的に、不要なアクセス権限を外す作業である。ユーザは、現在の職務に関する権限だけではなく、過去のプロジェクトに関する権限を持ち続けているケースがある。例えば、システム導入時に会計モジュールを担当していたシステムアドミニストレータは、稼働後はシステム管理機能についてだけ権限を保有すべきである。
- **重要な処理機能に対するアクセス権限の評価及び制限** – ビジネスオーナーは、銀行情報などの重要な機能やデータに対して誰がアクセス権限を持つべきかを決定しなければならない。仮に、分析の結果、20人が権限を持っており、そのうち本当にその権限が必要なのは5

人である場合には、残りの15人から権限を外す必要がある。SoDに焦点を当てる前にこのような分析を行うことによって、SoDコンフリクトの数を事前に減らすことができる。もし、特定のユーザが重要なアクセス権限を持つ必要があると決定された場合（このようなユーザは「特権ユーザ」あるいは「パワーユーザ」と呼ばれている）には、重要なアクセス権限の付与と削除を手作業で管理するプロセスを採用しなければならないが、重要なアクセス権限を管理するためにSAP GRC Access ControlのFirefighterを使用することも選択肢の1つとなる。

- **職務分掌の評価及び制限** – このフェーズでは、ユーザからアクセス権限を削除したり、ユーザの権限及び職務の再設計を行うことを検討する。権限および職務の再設計を行う必要があると決定された場合、SAP GRC Access ControlのRole Expertは権限のモデリング及び分析ツールとして有用である。
- **補完的コントロールの適用** – 上記の改善を行ったとしても、セキュリティリスクを完全にはなくすることはできず、セキュリティリスクは一部残る。SAPシステムは、500以上の自動化されたコントロールを有しており、残りのセキュリティリスクを軽減することが可能である。これまでは、このようなコントロールをリスク・コントロール・マトリクス (RCM) やCompliance Calibratorに登録したりしてきた。SAP社の最新GRCソフトウェアであるSAP GRC Process Controlでは、軽減コントロールの管理が改善できるように設計されており、コンプライアンスの文書やテスト結果などを集中管理できる。

### ステップ3 – 権限の割当て及び継続的なモニタリングの実施

一旦、セキュリティリスクの改善がなされたら、権限設定及び継続的なモニタリングのプロセス及び手続が実行可能となる。定期的なセキュリティのレビューは、Compliance Calibratorによって容易に行うことができる。また、重要なアクセス権限の使用とその承認はレビューされなければならないが、そのレビューをFirefighterとそのログによって行うことができる。付与、変更、削除などのユーザ権限設定はその環境に従って確立され、あるいは、拡張されなければならない。

SAP GRC Access ControlのAccess Enforcerは、このプロセスを自動化し、セキュリティリスクが改善されてクリーンな状態を保持することを可能にする。手続に対する一切の変更は、文書化され、正式なものとして適切なマネジメントに承認される必要がある。さらに、権限設定及びモニタリングの各ステップについてオーナーが明確にされる必要がある。

### ケーススタディ：グローバルな製薬会社

グローバルな製薬会社は、ジェネリック医薬品を取り扱うヨーロッパの大手製薬会社を買収した。その会社の内部監査チームはProtivitiと緊密に連携し、買収した会社のSAPシステムのセキュリティリスクの評価を行った。同時に、その会社はSAP GRC Access ControlとSAP GRC Process Controlを導入した。

**改善の評価とアプローチ**：初回の評価では、3つのSAPインスタンス、計6カ国において、200,000件以上のSoDリスクが検出された。その会社の経理部門、監査部門及びIT部門はProtivitiをパートナーとして、検出されたリスクの状況を判断し、改善計画を策定するためのプロジェクトを組成した。

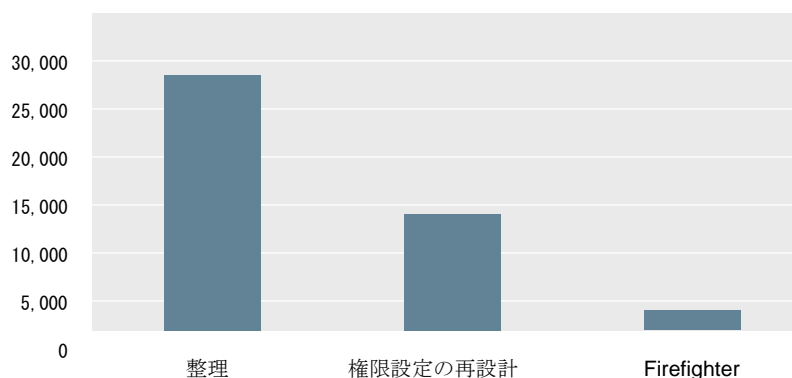
チームは、SAPシステムのセキュリティ環境を把握した結果、50,000件のリスクが高レベルのリスク、40,000件のリスクが中レベルのリスクと分類した。残りのリスクは、その会社のビジネス環境、業界ベンチマーク、外部監査人の意見を考慮した上で低レベルのリスクと定義した。

**改善結果と教訓**：6ヶ月のプロジェクト期間を経て、高レベルと判断されたリスクは、60%（約30,000件）が整理作業によって、30%（約15,000件）が

権限設定の再設計によって、そして10%（約5,000件）がFirefighterの導入によって削除された。中レベルのリスクも同様の方針で削除され、低レベルのリスクは業務プロセスにおけるマニュアルコントロールによって軽減された。

下図は、高レベルのリスクがどのように改善されたかを示している。

### 重要性の高いリスクの削減



このプロジェクトにより、以下の教訓を得た。

- セキュリティの改善プロジェクトも通常のシステム導入プロジェクトと同様に、スポンサーとしての経営者層からの支援、変更管理（単体テスト、ユーザ受入れテストの実施含む）、定期的な進捗会議の実施と研修の実施が必要である。
- 利害関係者の早い段階での巻き込み（外部監査人の意見を含む）が必要である。
- 早期に効果を出すために、改善活動の優先順位を決める必要がある。
- 企業のビジネス環境に合わせて、Compliance Calibratorの標準ルールセットを適切にカスタマイズすることが必要である。
- システム管理機能だけでなく、重要な業務処

理機能に対するアクセス権限についても、Firefighter を活用することが必要である。例えば、決算財務報告プロセスにおける決算処理や銀行マスタの更新処理などにFirefighterの活用を検討する。

- GRCソフトウェアを導入する前に、最新版のソフトウェアパッチが当てられていること、ハードウェア・ソフトウェアがGRCソフトウェアのサイジング要件を満たしていることの確認が必要である。

### サマリー

セキュリティの改善プロジェクトは大規模で複雑な取り組みになる場合がある。キーサクセスファクターの1つは、ここで述べた3つの改善ステップな

ど、すでに効果が実証された手法を用いることである。

SAP GRC Access ControlなどのGRCソフトウェアを正しく活用すれば、改善効果を最大化し、改

善プロジェクトの時間と費用を短縮、削減することができる。

---

#### 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](mailto: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。