






## アクセス ガバナンス ソリューション

### クラウドサービスによる持続可能な管理体制構築の実現

#### サービス概要

日本企業に対する監査経験を基盤に、デロイト トーマツ グループが提携するクラウドソリューションを活用し、クライアントの個別ニーズに合わせたソリューションをご提案します。デロイト トーマツは、アプリケーションシステムのセキュリティ診断からアクセス管理を強化するソリューション導入まで、一貫したサービスを提供します。

#### アクセスガバナンス強化のためのクライアントにおける一般的な作業の例示

 Quick Check 事前診断	 Remediation 課題解決と改善	 Implementation ソリューション導入
<ul style="list-style-type: none"><li>診断ツールの選定</li><li>対象アプリ、業務範囲の検討</li><li>ツール設定とルール設計</li><li>データ抽出プログラムのテスト</li><li>診断データの自動分析</li><li>分析結果の報告</li></ul>	<ul style="list-style-type: none"><li>改善方針の検討と決定</li><li>ID削除、ロール等の再割当、再設計の実施</li><li>管理方針、判断基準の策定</li><li>運用プロセスの再設計</li><li>ツールによる再チェック</li></ul>	<ul style="list-style-type: none"><li>ソリューション検証・デモ</li><li>費用対効果の検証</li><li>POC実施</li><li>初期設定・ルール設計</li><li>テスト実施</li><li>トラブルシューティング</li></ul>

## 日本企業における課題

個人情報や機密情報の漏洩の事件・事故が近年著しく増えており、企業の情報セキュリティ対策は喫緊の課題です。しかしながら、情報セキュリティ対策に最も有効的な手段の一つであるアクセス制御について、米国企業改革法(SOX)の施行にあわせ、欧米企業では先進的にさまざまな対策が施されていますが、日本企業においては、まだ十分な対策が実施できているとは言えない状況です。

## 企業におけるアクセス制限に係る共通的な課題



### 過剰なアクセス権の付与

- システム稼働における初期流動対応のための高権限が削除されず、そのまま利用されている
- 権限付与依頼時に権限の妥当性を判断する基準が無く、依頼ベースで権限を付与している



### アクセス権の監視する仕組みの未整備

- システム上の権限状況の全体像や権限の問題を把握する手段および仕組みが存在しない
- アクセス管理において権限を見直す判断基準が存在しない

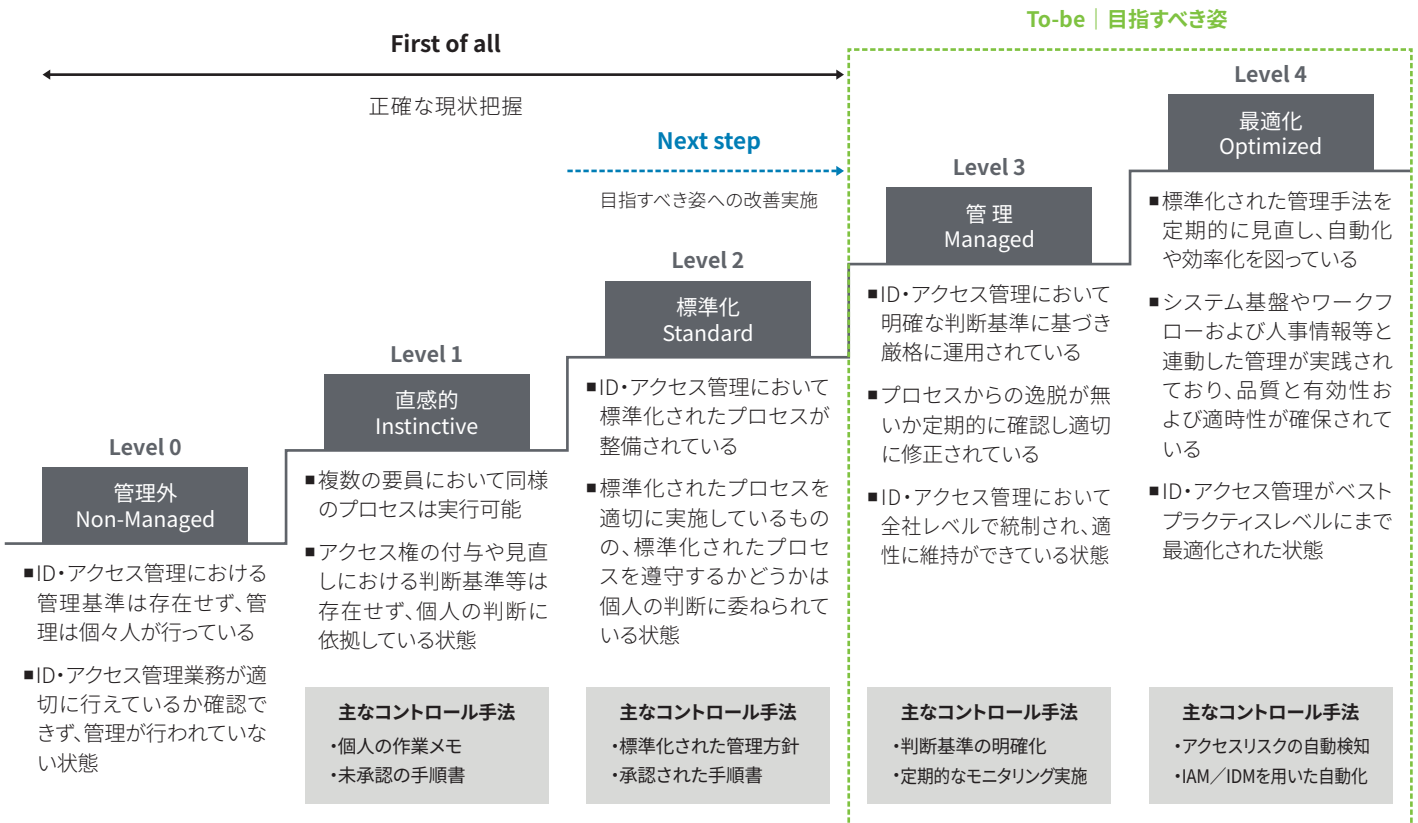


### 権限設定のブラックボックス化

- システム導入時にベンダ主導で権限設定を実施していたため、誰がどの機能にアクセス可能か把握していない
- 権限設計、仕組みについて引継ぎを実施していないため、権限高度化および複雑化に対応出来ない


## 目指すべき姿を見据えた現状把握の重要性

アクセス制御に係る共通の課題を抱えている企業の多くは、成熟度モデルに照らし合わせると標準化までに留まっており、管理の為の適切な体制が整っていません。アクセス制御における十分な管理体制の構築を図るべく、成熟度Level3以上のアクセスガバナンスの状態を目指しつつ、まずは自社に対する現状の理解から課題を整理し、成熟度レベルに応じたコントロールの導入を進めていく必要があります。



## 課題解決へのアプローチ

自社システムのアクセス状況を把握するため、デロイト ネットワークが開発したアクセス ガバナンスのツールを活用してアクセス権の付与状況をアクセスした事実に基づいて短期間で調査を実施し、課題や改善策のアドバイスを提供します。そして、課題解決としての管理方針の標準化や共通化、SoD（職務分掌）判断基準の策定などの管理面の強化から権限の再設計、SoD対応を踏まえ、課題解決に向けて業務プロセスの再検討に関する助言をします。また、成熟度モデルLevel3以上に必要となるIT基盤については、海外のクラウドベンダーが提供するソリューションを活用します。

Level 3以上の成熟度に必要な事項	課題	ソリューション
アクセス権限の追加や変更は、明確な判断基準に基づいて承認され、厳格に運用されている	特にSoDについては、明確な判断基準（ルール）が定義されていない	<p>ツールを活用した効率的なアクセス管理への移行</p> <ul style="list-style-type: none"> <li>✓ 判断基準はシステムへ登録され、自動的にチェック</li> <li>✓ モニタリングレポートの結果をクイックに出力</li> <li>✓ システムのワークフローによる連動</li> <li>✓ 作業ログの表示</li> </ul> <p>▼</p> <p> デロイトでは専用ツールを活用したサービスメニューを用意しています</p>
権限付与状況は定期的にモニタリングされ、職務分掌（以下SoDという）のコンフリクトは適切に修正されている	手作業のモニタリングは膨大な時間がかかる	
申請ワークフローはシステム化され、人為的な誤りや不正によるID利用がされない仕組みである	申請は紙ベースでありシステムとの連動性が無い	
特権IDは管理され、誰でも使用できる状態ではない。特権IDが使用された場合は、作業ログがレビューされている	作業ログを確認する仕組みが無い	

## クラウドベンダーのアクセス ガバナンス ソリューション

デロイトトーマツ グループが提携している海外クラウドベンダーは、さまざまなシステムに対するアクセス ガバナンスに関するソリューションを提供しています。対象アプリケーションとしては、SAP ERP、HANAをはじめ、オラクルEBSやJDE、SFDC、Workday等にも対応しています。また、Windows・Linux等のOS、オラクルやSQL等のDBのデータに対するアクセス権の管理やアクセスログ分析などの機能に加え、クラウドアプリケーションとの連携やセキュリティ対策のためのアイデンティティ ガバナンス&管理 (IGA) やCASBの機能を備えたIT基盤を提供することが可能です。

## クラウドソリューション機能の一例



### SoD Analysis

SoDコンフリクトが発生しているユーザとロール特定し、レポート表示します。数分の実行時間でレポートは表示され、繰り返しの機能により自動的に出力することも可能です



### Sensitive Access

重要な機能に対して、アクセスが可能なユーザとロールを特定してレポートを表示します



### Compliant Provisioning

ユーザの権限を変更する場合、アクセスリスクに対するインパクトを事前に確認することが可能です



### Emergency Access

特権IDの貸出プロセスを自動化し、ワークフローによる承認と作業ログの確認が可能になります



### Transaction Monitoring

トランザクションのログから、ユーザのアクセス履歴を分析することが可能です。権限の修正を行う際に、実際の使用有無が確認できるため、調査にかかる時間が短縮されます



### Proven Rulebook

SoDの判断基準となるルールブックが用意されています。このルールブックに従い、SoDの分析やプロビジョニングが実施されます

本サービスに関するお問い合わせ：seiki.matsui@tohatsu.co.jp (担当:松井 靖己)

#### 有限責任監査法人トーマツ

リスクアドバイザリー

〒100-0005 東京都千代田区丸の内3-3-1 新東京ビルTel: 03-6213-1112

#### デロイトトーマツ リスクサービス株式会社

〒100-0005 東京都千代田区丸の内3-3-1 新東京ビル Tel: 03-6213-1300

Making another half century of **Impact**

デロイト トーマツ 50周年 次の50年へ



デロイト トーマツグループは日本におけるデロイト トウシュ トーマツ リミテッド(英国の法令に基づく保証有限責任会社)のメンバーファームであるデロイト トーマツ合同会社およびそのグループ法人(有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ 税理士法人、DT弁護士法人およびデロイト トーマツ コーポレート ソリューション合同会社を含む)の総称です。デロイト トーマツ グループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約40都市に約11,000名の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト(www.deloitte.com/jp)をご覧ください。

Deloitte(デロイト)は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリーサービス、リスクアドバイザリー、税務およびこれらに関連するサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界150を超える国・地域のメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスをFortune Global 500®の8割の企業に提供しています。“Making an impact that matters”を自らの使命とするデロイトの約245,000名の専門家については、Facebook、LinkedIn、Twitterもご覧ください。

Deloitte(デロイト)とは、英国の法令に基づく保証有限責任会社であるデロイト トウシュ トーマツ リミテッド(“DTTL”)ならびにそのネットワーク組織を構成するメンバーファームおよびその関係会社のひとつまたは複数指します。DTTLおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。DTTL(または“Deloitte Global”)はクライアントへのサービス提供を行いません。Deloitteのメンバーファームによるグローバルネットワークの詳細は www.deloitte.com/jp/about をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性もあります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的事案をもとに適切な専門家にご相談ください。

Member of  
Deloitte Touche Tohmatsu Limited

© 2018. For information, contact Deloitte Touche Tohmatsu LLC, Deloitte Tohmatsu Risk Services Co., Ltd.  
2018.03\_0234



IS 669126 / ISO 27001