Deloitte.
デロイト トーマツ

サイバーセキュリティ/内部統制の要となる特権アクセス管理支援サービス

特権アクセス管理の重要性の高まり

企業を標的としたサイバー攻撃は年々増加傾向にあり、被害が多発しています。調査会社フォレスター・リサーチの調査レポートでは、セキュリティ被害の80%は特権の認証情報が関連している*1ことを報告しており、被害を未然に防止する為には、特権の濫用や悪用を許さない厳密な管理及び監視の仕組みが必要不可欠となっています。また、このような社会状況を背景に、監査においても厳密な特権アクセス管理の有効性を高いレベルで求める傾向にあり、多くの企業で見直しが行われています。

多くの日本企業で見られる特権アクセス管理に関わる課題

多くの企業が抱える課題として、主に「認証情報管理」、「アクセス制御」、「モニタリング」の3つが挙げられます。

認証情報管理	■ パスワード変更等管理が手動である為、認証情報の漏えいや抜け漏れ等の作業ミスのリスクを払拭できない ■ クラウド、DevOps、RPA、IoT等のIT資産の増加に伴い、サイバー攻撃の標的となる範囲が拡大しているが、統合的に且つ適時性を持って管理する手立てがない
アクセス制御	■ 外部委託者等特権利用者が多様化する傾向の中、機密情報の漏えいや改ざんのリスクを払拭できず、また内部統制の有効性に関する説明責任を果たすことができない ■ リモートワークの必要性に伴い、社外ネットワークからの特権アクセスが急増しているが、不正アクセス対策が十分に検討、整備されていない
モニタリング	■ 特権利用のモニタリングを実施していない若しくは手動で行っている為、適時的に検知できない、若しくは不正利用を抑止できない ■ 必要なログを取得していない若しくは一部取得に留めている為、監査人からモニタリングの網羅性について監査指摘を受けるリスクがある

*1: The forrester Wave : Privileged identity Management, Q4 2018 November 14, 2018 2018 Forrester research, Inc.

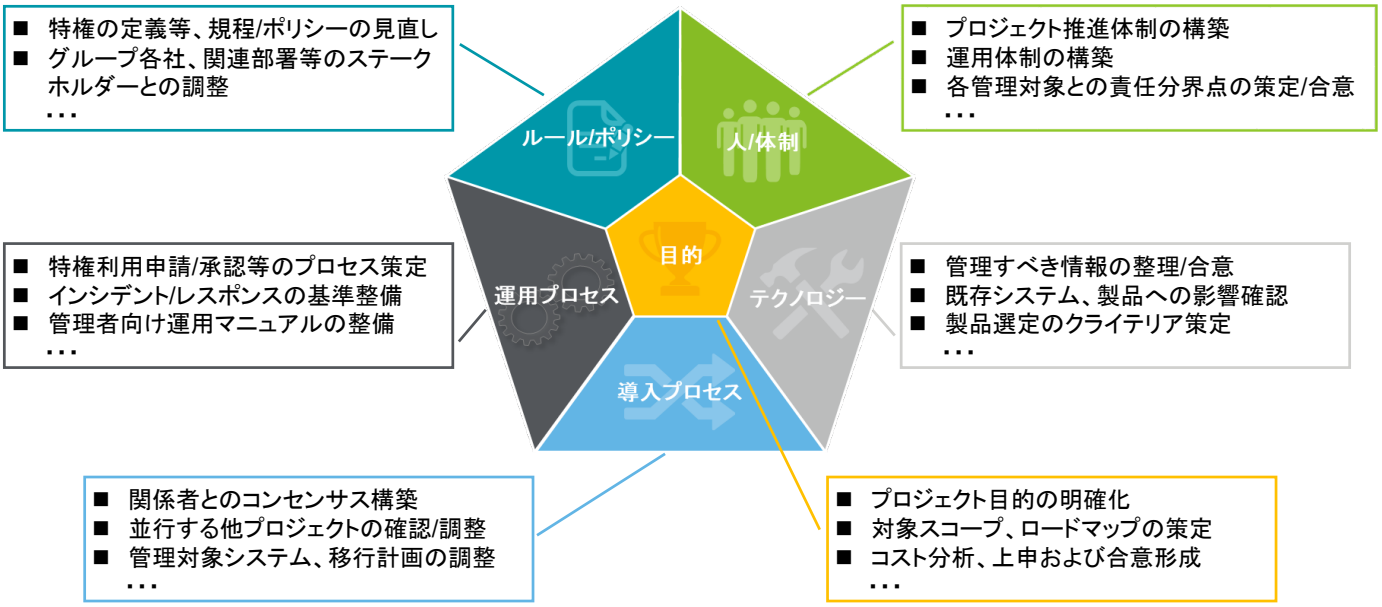
課題解決に向けて検討すべきこと

厳密な特権アクセス管理を実現するには、主に「網羅性」、「正確性」、「適時性」を満たすことが求められます。先に挙げた「認証情報管理」、「アクセス制御」、「モニタリング」の3つに対しては、具体的に以下のようなソリューションを検討する必要があります。

認証情報管理	■ 特権の認証情報（パスワード、認証キー等）を利用都度若しくは定期的に自動変更する ■ 認証情報（パスワード、認証キー等）を特権利用者に秘匿のまま、利用できる環境を提供する ■ あらゆるIT資産に存在する認証情報を種類を関わらず一元的且つ安全に管理する
アクセス制御	■ 特権の利用都度、申請及び承認を必須とし、また当該プロセスを自動化する ■ 特権利用のプラットフォームを一元化し、バイパス等の承認のない不正な利用を防御する ■ 一元化したプラットフォームに多要素認証（MFA）等を施し、認証を強化する
モニタリング	■ 重要システムの利用ログを網羅的に集約し、一元的に管理する ■ 特権を使用したセッションをリアルタイムで自動的にモニタリングする ■ 特権利用に関する不正または不審なセッションを自動的に検知/切断する

特権アクセス管理プロジェクトを成功させるポイント

特権アクセス管理の整備は、全社的且つ特殊な領域のプロジェクトである為、製品のみにフォーカスを当ててしまい目的やその他の検討事項を疎かにした場合、期待した効果が得られないといった結果となる事が少なくありません。サイバーセキュリティや監査の専門的な知見/経験を活用し、以下のような観点を漏れなく明らかにする事が成功のポイントとなります。



サービスの概要

様々な業界/企業に対して、監査やサイバーセキュリティサービスを提供してきた経験を基に、デロイトの方法論を活用し、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供します。例えば、フレームワークを用いた現在の成熟度診断から目指す姿に到達するまでのロードマップ策定、テクノロジー選定/導入や運用段階におけるあるべき業務プロセス、組織のあり方まで、一貫したサービスをご提案することが可能です。

Planning /Grand Design
構想策定支援

- 目的、全体ビジョンの策定支援
- As-IsとTo-Beのギャップ分析
- 期間・コストを考慮したロードマップ作成
- 必要となる予算およびコストの分析
- 上申等の社内でのプロジェクト推進の支援

System Design
設計支援

- 要件定義書作成
- 業務プロセス、運用フロー、運用態勢の設計
- 基本/詳細設計、テスト仕様書作成支援
- 単体・結合・総合テスト実施支援
  およびユーザ受入テストのサポート

PMO and Change Management
プロジェクト管理 / 運用変更支援

- プロジェクト体制策定
- テンプレート、ツール活用のプロジェクト管理
- 各フェーズ、マイルストーンのレビュー支援
- 業務プロセス、ガイドライン類等の整備支援
- 運用・サポートチームへのナレッジ展開支援

デロイトの方法論

デロイトの方法論は、成功事例をベースにしたグローバル水準のアプローチ、各種フレームワーク/テンプレート、ツールから成り立ちます。本方法論を活用することで、実現すべき要件の絞込み、採用すべきテクノロジーの決定、投資効果等を効率的且つ効果的に導き出す事が可能となります。

Deloitte's *Methods*™

Deloitte's *Methods*™ の利点

- 成熟度モデル、現状と理想のギャップ、コストにフォーカスをあてたアプローチによる要件の確定
- 主要PAM*2ベンダーとのアライアンス、フレームワークを基にしたテクノロジー/ソリューションの評価及び選定
- コスト分析テンプレートを活用した投資効果の算出

DeloitteのPAM Frameworkにおいて重要とする領域

1. Policy & Governance	2. PAM Reporting	3. Enterprise PAM Service
4. Privileged Account Lifecycle Management	5. People Skills	6. PAM Policy Alignment & Coverage

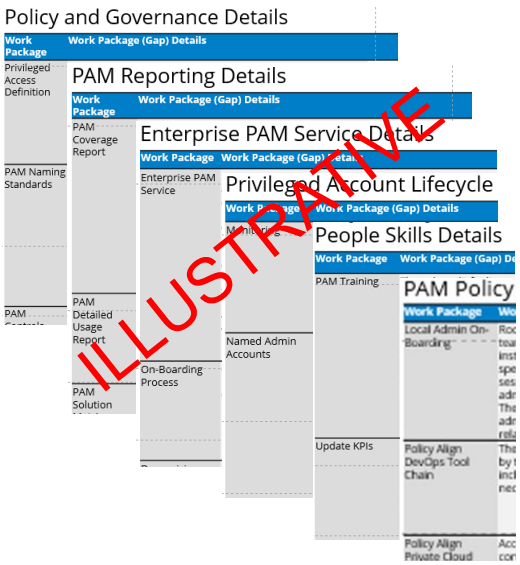
Deloitteの標準的な質問集によって効率的に現状把握を実施

IAM Capability	#	Example Questions	Response
Privileged Access Management	15	How is access for privileged users added and removed?	
	16	What is the process for approving access to privileged user?	
	17	How is privileged user access monitored?	
	18	Is session recording (documenting user's actions or keystrokes) enabled for privileged user access	
	19	Is there multi-factor authentication enabled for use of privileged access	
	20	What is the tool being used for privileged access management	
	21	Is there temporary access to privileged accounts, what is the process to request/grant access to this?	
	22	What is the tool being used for privileged access management	
	23	Are privileged identities stored in safes? If they are, is there a safe naming standard being implemented?	

Example Document Request

IAM Capability	#	Process Flow or Documentation
General	1	List of applications and systems currently managed
	2	List of applications and systems currently integrated with centralized Identity Management tools
User Administration	2	Employee/Contractor Onboarding
	3	Employee/Contractor Termination
	4	User access request and approval (including delegated access requests)
	4	User access revocation
	5	User access review
	6	Any other relevant processes of workflows relevant to User Administration
Privileged Access Management	7	Privileged user access request and approval
	8	Privileged user access removal
	9	Privileged access safe naming conventions (if used)

貴社の規程/ポリシー、業界の標準、DeloitteのPAM Templateから効率的に分析し、To-Be像を導出



*2: Privileged Access Managementの略称

デロイト トーマツ グループの提供価値

デロイト トーマツ グループでは、「専門的な知見」、「グローバル連携」、「中立的な見解」という3つの柱をベースに特権アクセス管理に関するサービスをご提供しています。

専門的な知見

様々な業界/企業に対して、内部統制 / サイバーセキュリティの専門家として サービスを提供してきた実績及び知見

グローバル連携

グローバルの各リージョンで活躍する Deloitteのプロフェッショナルとの連携や 人財/テクノロジーに関する支援

中立的な見解

特定の製品ではなく、クライアント視点 / 最適なソリューションを重視した中立的 な立場からのコンサルティングサービス

デロイト トーマツ サイバー合同会社
Mail iam_advisory@tohmatsu.co.jp
URL www.deloitte.com/jp/dtcy
【国内ネットワーク】東京・名古屋・福岡