JNSA

クラウド

NPO 日本ネットワークセキュリティ協会

標準化部会

デジタルアイデンティティ WG

特権 ID 管理ガイドライン　実践編

２０２４年5月３１日発行

留意事項

このレポートの利用に際しては、以下の条件を遵守してください。

このレポートに含まれる一切の内容に関する著作権は、レポート作成者に帰属し、日本の著作権法や国際条約などで保護されています。

著作権法上、認められた場合を除き、著作権者の許可なく、このレポートの全部又は一部を、複製、転載、販売、その他の二次利用行為を行うことを禁じます。

これに違反する行為を行った場合には、関係法令に基づき、民事、刑事を問わず法的責任を負うことがあります。

レポート作成者は、このレポートの内容の正確性、安全性、有用性等について、一切の保証を与えるものではありません。また、このレポートに含まれる情報及び内容の利用によって、直接・間接的に生じた損害について一切の責任を負わないものとします。

このレポートの使用に当たっては、以上にご同意いただいた上、ご自身の責任のもとご活用いただきますようお願いいたします。

目次

ご挨拶

本書は 2016 年度に発行した、「エンタープライズにおける特権 ID 管理解説書（第 1 版）」について、これまでに多くのご意見やご指摘をいただいたものを反映すべく再度内容について再検討を行い、新たな形で発行するものである。

今回の解説書は 2 部構成として、1 部は「解説編」2 部は「実践編」とした。「解説編」では、特権 ID 管理の重要性や特権 ID の捉え方、インシデント事例などを紹介した。「実践編」では特権 ID 管理システムの導入の手引きとして利用していただける内容を解説した。

これから、特権 ID 管理を導入検討する人には、プロジェクトの推進の準備として、また、現在特権 ID 管理システムを導入中の人にとっては、現在のプロジェクトをよりよくするためのチェック、ヒント集として、活用していただけると考えている。

また、この分野について詳細に書かれた書籍がほとんど出版されておらず、その意味でも本書の内容は多くの企業に役立つ内容となっている。

なお、本書は「日本ネットワークセキュリティ協会（JNSA）」の「デジタルアイデンティティ管理ワーキンググループ」のサブグループにて検討した内容となっている。本書があらゆる企業において、特権 ID 管理の適切な導入・運用に貢献できれば幸いである。

標準化部会　デジタルアイデンティティ管理　ワーキンググループ　リーダ　宮川 晃一

※「解説編」はこちらから。
https://www.jnsa.org/result/digitalidentity/2022/index.html

第1章 特権 ID の実装とは

1.1. 特権 ID 管理に求められる内容

「解説編」で述べたとおり、特権 ID は高い権限を有することから奪取された場合の影響が大きく、その取り扱いは厳格に行う必要がある。特権 ID の厳格な管理において重要なポイントとなるのは、「アクセス管理の強化」、「本人確認の強化」、「トレーサビリティの確保」の 3 つである。これを図示すると以下のようになる。

図 1-1 特権 ID 管理に求められる内容

1.2. 特権 ID 管理における運用課題

前節で挙げた 3 つのポイントから特権 ID 管理を捉えると、運用上の課題を以下のように整理できる。

表 1-1 特権 ID 管理における運用課題

管理策ポイント		管理策の例	運用上の課題
アクセス管理の強化	✓ アカウントの管理 ✓ アクセス権限の最小化 ✓ アクセス元制限	・ 一意の ID 付与、最小権限の見直し ・ 一時的な払い出し ID の管理 ・ 管理用端末の準備、セグメントの分離	運用負荷の増大に伴う管理の形骸化 例） ・ 特権 ID の共有や必要以上の権限付与 ・ 退職者、異動者の ID 残存 ・ 一時利用 ID の払い出し期間の長期化
本人確認の強化	✓ パスワード管理 ✓ 多要素認証	・ パスワードの定期変更 ・ パスワード忘却時のリセット対応 ・ 多要素認証用のデバイス配布、設定と運用管理	パスワード強度の弱体化 例） ・ 簡易なパスワード/初期状態 ・ 複数システムでの使いまわし ・ 長期間にわたる同一パスワードの利用
トレーサビリティの確保	✓ 操作ログの記録、保存 ✓ 操作ログの監査	・ 運用作業者の申請履歴管理 ・ 申請内容と操作ログ定期監査 ・ 操作ログの保存容量の確保 ・ 操作ログの真正性の担保	トレーサビリティの信頼性低下 例） ・ 自己申請に頼った作業記録、承認行為の形骸化

			・ 保存ログ、作業申請内容の書き換え・改ざんが可能 ログの効果的な活用ができていない 例） ・ 定期監査が行われず、インシデント発覚が遅延 ・ インシデント調査において事実確認に時間がかかる

これらの課題を解消するための実装方式としては、特権 ID 管理システムを利用するパターン、利用しないパターンの 2 つに大別できる。次節以降でそれぞれのパターンについて詳しく見ていく。

1.3. 特権 ID 管理システムを利用する方式

本節では特権 ID 管理システムを利用するパターンについて述べる。

特権 ID 管理システムは、特権 ID の利用を制御し、記録・監視するためのツールである。様々な製品が存在しており、それぞれ有する機能は異なるが、代表的な機能を前節の 3 つの管理策と関連付けると下表のようになる。（「1.5 特権 ID 管理を行うための主要機能と標準技術」に機能をより詳細に列挙しているため、あわせて参照されたい。）

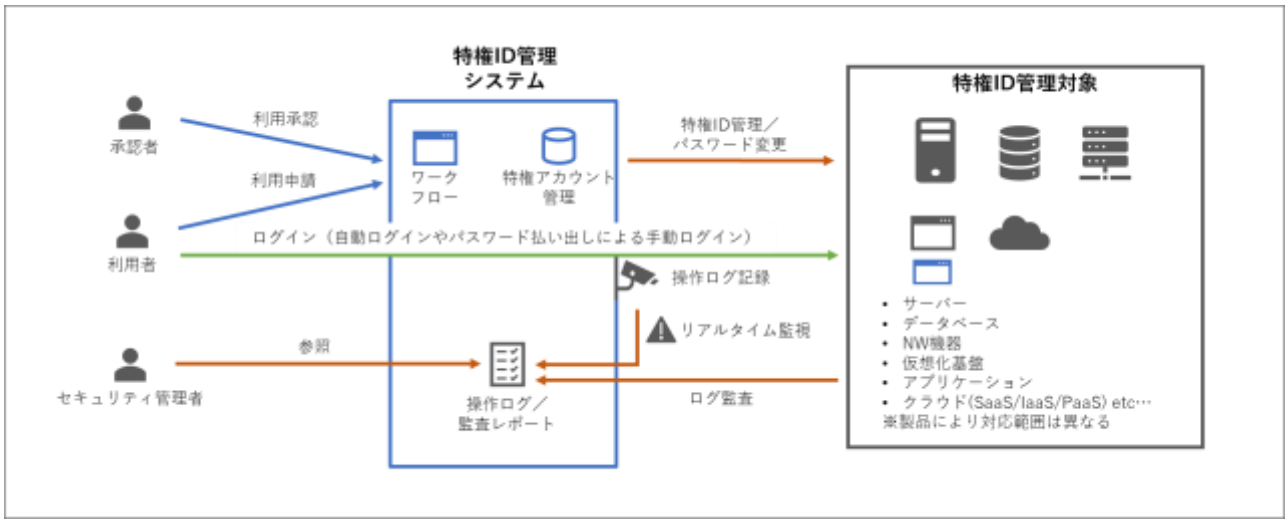
なお、全ての機能を特権 ID 管理システム単体で有するとは限らず、外部システムとの組み合わせで実現することも多い。

表 1-2 特権 ID 管理システムの代表的な機能

管理策ポイント	機能	機能詳細
アクセス管理の強化	特権 ID 管理機能	特権 ID を一元的に管理し、各ユーザーがアクセスできる対象を制御する機能
	ワークフロー機能	事前に定義した申請・承認プロセスを経て特権アクセスを許可するためのワークフロー機能
本人確認の強化	自動ログイン機能（ログイン代行機能）	特権 ID のログインを代行することで、パスワードをユーザーが直接知ることなくログインできるようにする機能
	パスワード変更機能	特権 ID のパスワードを定期的な頻度や特権アクセスの都度、自動変更する機能
	パスワード払い出し機能	特権 ID の利用時に、一時的にパスワードをユーザーに払い出す（参照させる）機能
トレーサビリティの確保	操作ログ記録機能	特権 ID 利用時の操作を動画やテキストログに記録する機能
	ログ監査機能	管理対象システムからアクセスログを収集してワークフロー申請と突き合わせを行うことで不正アクセスを検出するなどの機能
	リアルタイム監視機能	特権アクセスのセッションをリアルタイムで監視し、必要に応じてセッションの切断や操作を一時停止する機能

特権 ID 管理システムの利用イメージは以下のとおりとなる。

図 1-2 特権 ID 管理システムの利用イメージ例



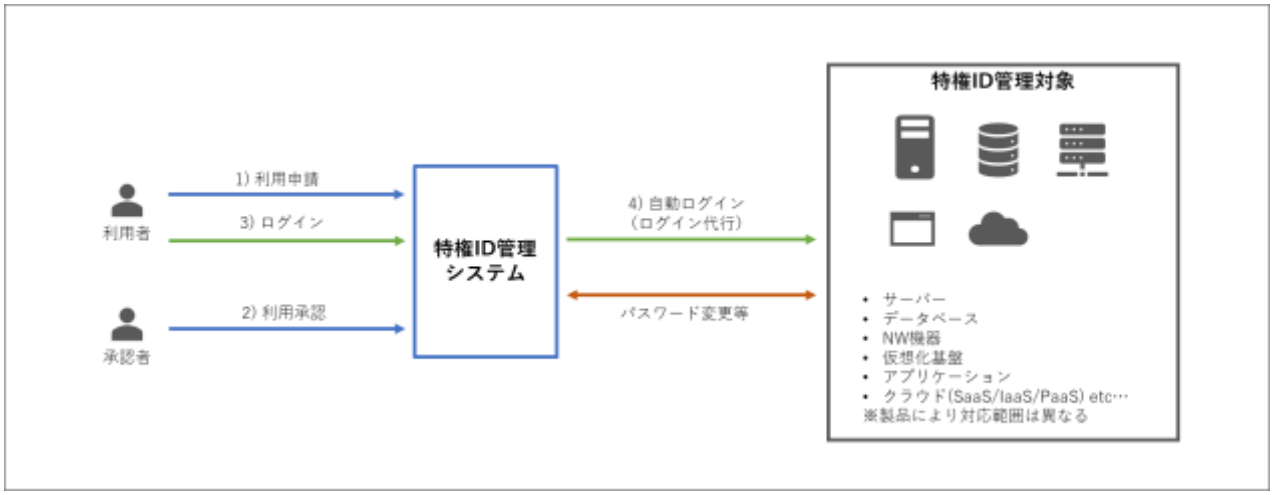
1.3.1. 特権 ID 管理システムの方式と違い

特権 ID 管理システムには、大きく分けてゲートウェイ方式とエージェント方式の 2 種類が存在する。

1) ゲートウェイ方式

ゲートウェイ方式は、特権 ID 作業を実施するクライアント端末等と特権 ID 管理対象となるサーバー等との間に特権 ID 管理システムを配置する方式である。特権 ID 管理システムが中継点となってユーザー認証やアクセス制御を行うとともに、ゲートウェイを介して行われる操作の記録や作業セッションの管理を行うことができる。

図 1-3 ゲートウェイ方式



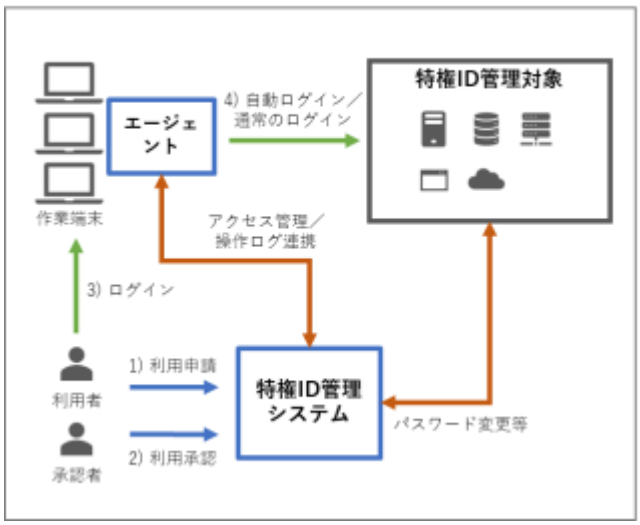
2) エージェント方式

エージェント方式は、特権 ID 管理システムに付属するソフトウェアエージェント（以下、エージェント）を特権 ID 管理対象サーバーや作業用クライアント端末にインストールする方式である。エージェントが導入先のサーバーやクライアント端末上に常駐し、特権 ID 管理システムと連携しながら特権 ID アクセス時の認証やアクセス制御、操作の監視などの役割を担う。

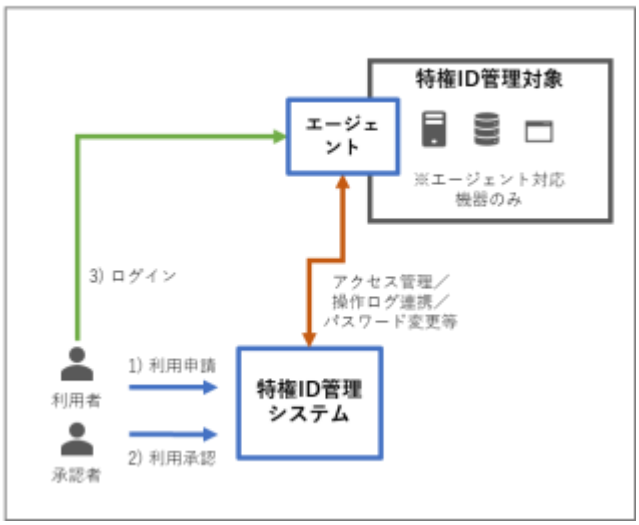
エージェント方式はエージェントの導入先によって 3 つの方式に分けられる。実環境においては複数方式を組み合わせて利用されることもある。

図 1-4 エージェント 3 方式

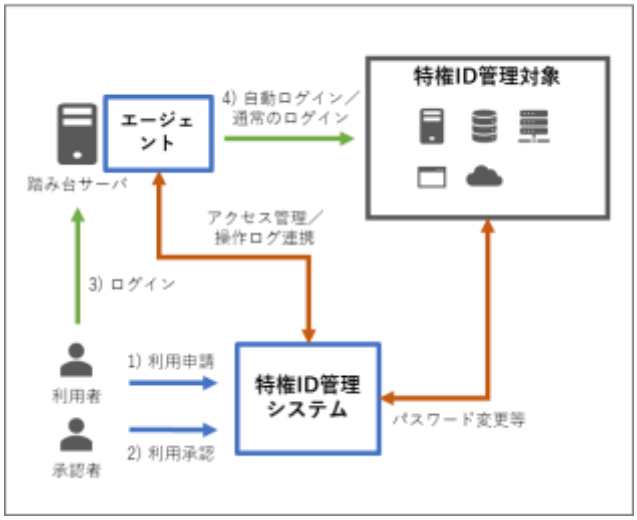
クライアント・エージェント方式



サーバ・エージェント方式



踏み台方式



※踏み台方式は前項のゲートウェイ方式と類似した特徴を持つが、ゲートウェイ方式が特権 ID 管理システムの用意する Web コンソール等にログインしてから管理対象にアクセスするのに対し、踏み台方式は踏み台サーバーの OS にログインしてから管理対象にアクセスする点が異なっている。

3 方式を比較したものが下表である。

表 1-3 エージェント 3 方式の比較

比較項目	クライアント・エージェント方式	サーバー・エージェント方式	踏み台方式
構成変更の範囲・影響	作業端末に対するエージェント導入が必要	管理対象サーバーへのエージェント導入が必要 エージェント導入に伴う管理対象に対する影響確認や検証が必要	踏み台サーバーの用意が必要 踏み台サーバーへのエージェント導入が必要
操作ログ取得・アクセス制御の細かさ	作業端末上での詳細な操作ログを取得可能だが、アクセス制御はサーバー・エージェント方式に劣る	詳細な操作ログを取得可能 コンソール等からの直接アクセスについても管理可能	踏み台サーバー上での詳細な操作ログを取得可能だが、アクセス制御はサーバー・エージェント方式に劣る
拡張性	作業端末追加の都度、エージェント導入が必要	管理対象追加の都度、エージェント導入が必要	踏み台サーバーを追加する場合はエージェント導入が必要
その他留意点	－	エージェントが非対応の管理対象では利用できない	－

3) ゲートウェイ方式とエージェント方式の比較

ゲートウェイ方式とエージェント方式を比較すると以下のような違いがある。両方式の特性を理解した上で、導入先の環境に適した方式を選ぶことが肝要である。

表 1-4 ゲートウェイ方式とエージェント方式の比較

比較項目	ゲートウェイ方式	エージェント方式
構成変更の範囲・影響	ゲートウェイの追加が必要 ゲートウェイを経由せずに管理対象にアクセスする経路をふさぐなどの対処が必要	作業端末や管理対象に対するエージェントの導入が必要 エージェント導入に伴う管理対象に対する影響確認や検証が必要
操作ログ取得・アクセス制御の細かさ	ゲートウェイを経由する通信のみが制御対象となる	エージェントによる詳細な操作ログを取得可能 コンソール等からの直接アクセスについても管理可能 ※上記いずれもエージェントを導入したシステムに限る
拡張性	ゲートウェイの設定のみで対応可能	エージェント導入が必要
その他留意点	－	管理対象の種類や OS 等によってはエージェントが非対応の場合がある

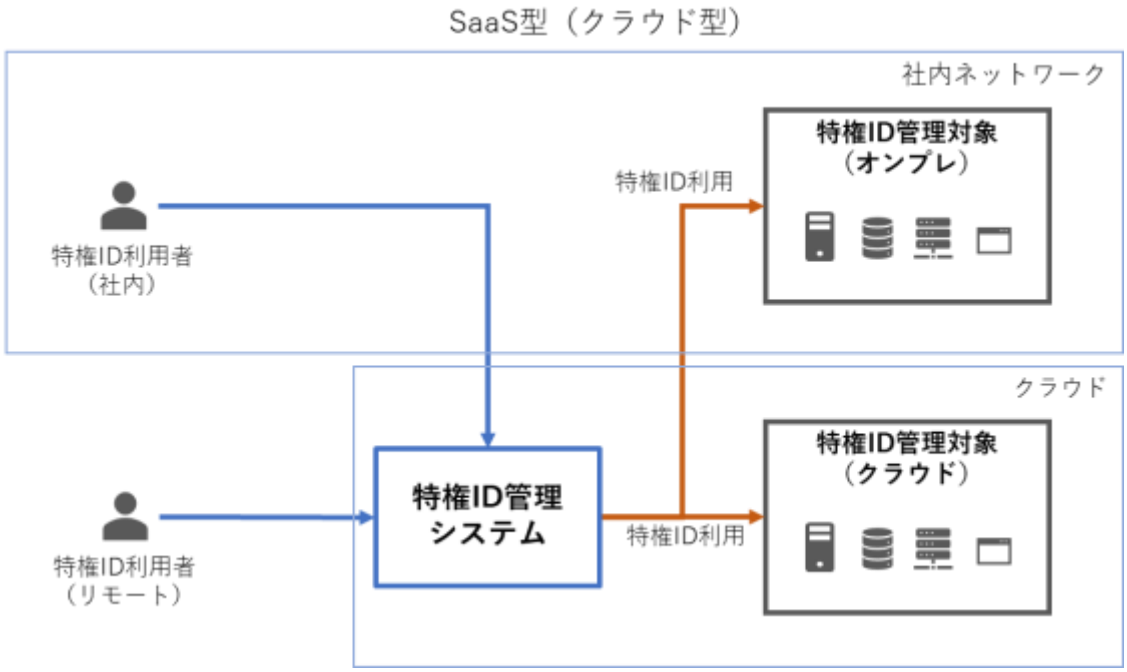
1.3.2. 利用形態による違い

特権 ID 管理システムの利用形態としては、オンプレミス型と SaaS 型（クラウド型）の 2 パターンが挙げられる。

前者は社内や利用するデータセンター等の自社ネットワーク環境内に特権 ID 管理システムを構成して利用する形態、後者は SaaS 型で提供される特権 ID 管理システムを利用する形態である。

近年は SaaS 型への移行がトレンドとなりつつあるが、インターネット経由での特権 ID 利用が認められないなど、セキュリティ要件によって前者を採用することも少なくない。

図 1-5 オンプレ型と SaaS 型（クラウド型）



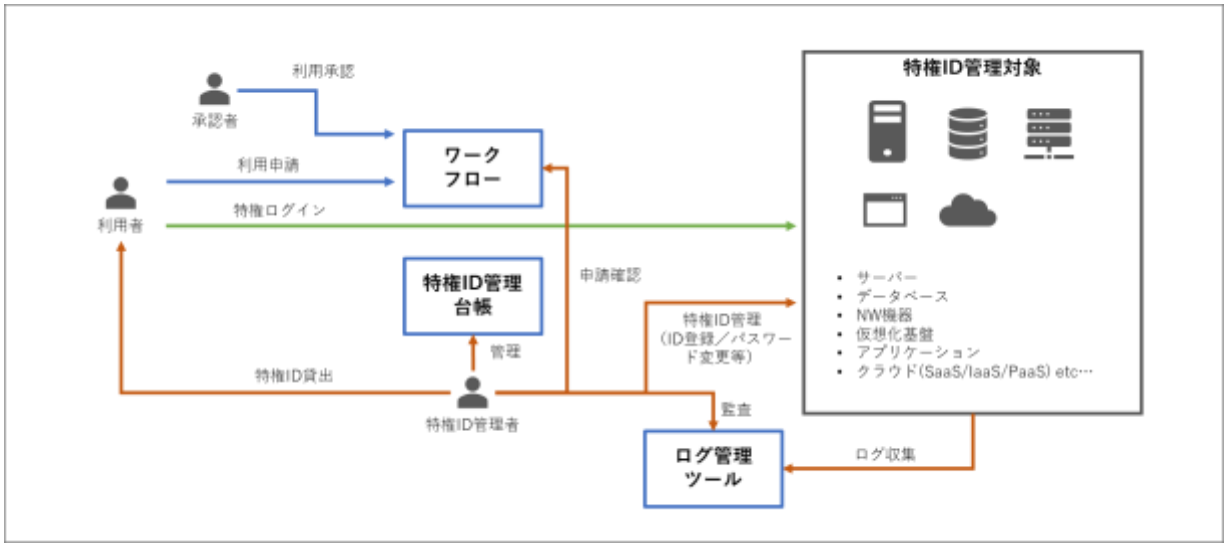
※本図の構成はあくまでも一例であり、製品によって異なる場合がある。

1.4. 特権 ID 管理システムを利用しない方式

本節では特権 ID 管理システムを利用しない方式について述べる。

特権 ID 管理システムを利用しない場合には、当然のことながら特権 ID 管理システムに備わっている機能を人手による運用でカバーする必要が生じる。具体的には「1.2 特権 ID 管理における運用課題」で「管理策の例」として挙げた各種事項を運用で実現する必要がある。

図 1-6 特権 ID 管理システムを利用しない方式の例



人手による運用では時間と労力を要する上、作業ミスのリスクも増加する。また自動ログイン機能やリアルタイム監視機能など、特権 ID 管理システムなしに実現が難しい要素もあり、これらを必要とする場合は特権 ID 管理システムが不可欠となる。

以下は特権 ID 管理システム利用の有無を比較したものである。

表 1-5 特権 ID 管理システム利用有無の比較

比較項目	特権 ID 管理システムを利用する	特権 ID 管理システムを利用しない
費用	特権 ID 管理システムのライセンス費用や構築/維持費用が発生する	システムの費用は発生しないが、手動運用に伴う工数としてのコストが発生する
運用負荷	特権 ID の管理を自動的かつ一元的に管理できるため、運用負荷は低い	特権 ID の管理、パスワード変更、貸出管理、ログ確認など多くの作業を手動で行う必要があり、運用負荷が高い
リスク	特権 ID/パスワードの管理をシステムで行うため、漏洩や不正利用のリスクは低い 特権 ID 管理システムやゲートウェイ等に障害が発生した際にアクセスできないリスクがある	特権 ID/パスワードを台帳等で管理することによる漏洩や不正利用のリスクが高い パスワード変更忘れなど作業ミスによる不正アクセスのリスクが高い 管理対象システム数が多くなった場合に特権 ID 管理の運用レベルを統一することが難しくなり、十分に管理されないシステムが残るなど不正アクセスに繋がるリスクが高まりやすい

特権 ID 管理システムの導入・利用には費用が発生する一方、運用負荷やリスクを大きく減らすことができることから、可能な限り特権 ID 管理システムを利用することが望ましい。

以降の章では特権 ID 管理システムを利用する場合に絞り、導入検討フェーズから導入後の運用フェーズまで順を追って説明する。

1.5. 特権 ID 管理を行うための主要機能と標準技術

本節では特権 ID 管理システムの機能を列挙する。製品によって有する機能は異なるため、あくまでも一例としてご理解いただきたい。

表 1-6 特権 ID 管理システムの主要機能

管理策ポイント	機能	機能詳細
アクセス管理の強化	特権 ID 管理機能	特権 ID を一元的に管理し、各ユーザーがアクセスできる対象を制御する機能 • 特権 ID を手動入力で登録する機能 • 特権 ID を CSV ファイル等から一括登録する機能 • 特権 ID を管理対象システムから自動収集して登録する機能 • 様々な管理対象（OS、データベース、ネットワーク機器、仮想化基盤、ストレージ機器、クラウド、アプリケーション等）への対応 • 作業ユーザー、時間帯、対象システム等を絞ってアクセス許可する機能 • 一般ユーザーID によるログイン後の特権昇格に対応する機能 • 特権 ID 利用のタイミングで ID を作成し、利用期間が終了すると ID を削除する機能（ワンタイム ID 方式、Just-in-Time プロビジョニング）

	ワークフロー機能	事前に定義した申請・承認プロセスを経て特権アクセスを許可するためのワークフロー機能 • ワークフロー機能の保有、もしくは外部のワークフローシステムとの連携機能 • 多段階承認など柔軟な承認フローへの対応 • 自己承認（申請者が自身で承認する）の制限 • 代理承認機能 • 緊急時の承認スキップ（事後承認）や通知機能
	棚卸機能	特権 ID/利用ユーザーの一覧や権限設定を出力する機能 • 特権 ID の一覧を出力する機能 • 特権 ID の追加/変更/削除履歴を出力する機能 • 特権 ID を利用可能なユーザーの一覧を出力する機能 • 特権 ID を利用可能なユーザーの追加/変更/削除履歴を出力する機能
本人確認の強化	利用ユーザー管理	特権 ID 管理システムの利用ユーザーを適切に管理する機能 • 多要素認証への対応 • 連続したログイン失敗時のアカウントロック機能

		• Active Directory や LDAP 等とのユーザー管理やログイン認証の連携機能 • グループ等により利用可能な権限を制御する機能
	自動ログイン機能（ログイン代行機能）	特権 ID のログインを代行することで、パスワードをユーザーが直接知ることなくログインできるようにする機能
	パスワード変更機能	特権 ID のパスワードを定期的な頻度や特権アクセスの都度、自動変更する機能
	パスワード払い出し機能	特権 ID の利用時に、一時的にパスワードをユーザーに払い出す（参照させる）機能
	パスワード以外のクレデンシャル管理機能	パスワード以外のクレデンシャルを管理する機能 • パスワード以外のクレデンシャル（SSH キー、API キーなど）を管理する機能 • アプリケーション等からのクレデンシャル呼び出し機能
トレーサビリティの確保	操作ログ記録機能	特権 ID の利用や操作内容を記録する機能 • 特権 ID 管理システムへのログインや特権 ID の利用履歴を記録する機能 • 特権 ID を利用した操作をテキストや動画で記録する機能 • ログ/証跡データにアクセスできるユーザーを制限する機能

		• ログ/証跡データを改ざん防止した形で保管する機能 • 特権 ID 管理システム自体の管理者アカウントの操作内容を記録する機能
	ログ監査機能	管理対象システムからアクセスログを収集してワークフロー申請と突き合わせを行うことで不正アクセスを検出するなどの機能 • 管理対象システムからアクセスログを収集する機能 • アクセスログとワークフロー申請等を突き合わせることで許可されていない特権 ID の利用を検出する機能 • 保管されたログ/証跡データをキーワード等で検索する機能
	リアルタイム監視機能	特権アクセスのセッションをリアルタイムで監視し、必要に応じてセッションの切断や操作を一時停止する機能 • 許可されていない特権 ID の利用を検知する機能 • 不正なコマンド実行やアクションを検知、制限する機能 • 特権 ID を利用した操作を管理者がリアルタイムでモニタリングできる機能 • 不正検知時の管理者へのメール通知や作業セッションを自動的に一時停止/切断する機能

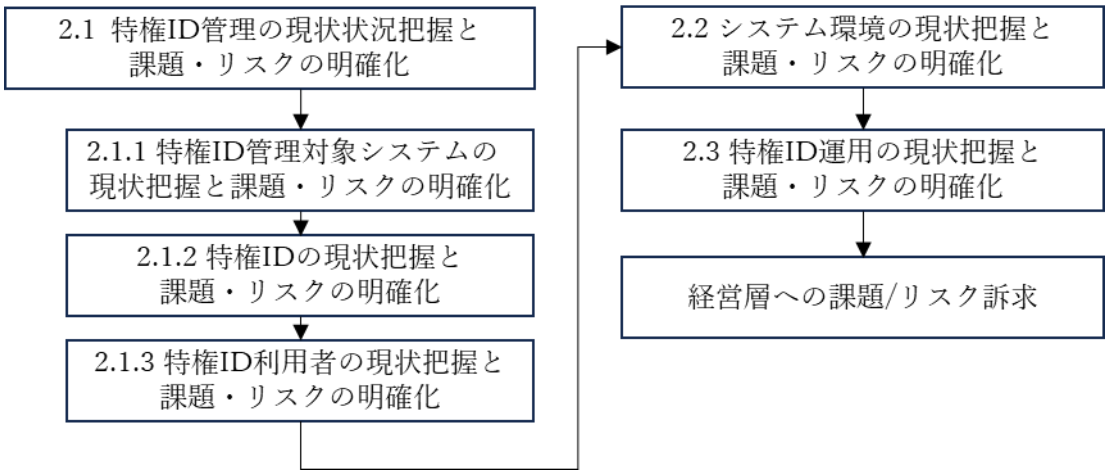
その他	耐障害性・性能	特権 ID 管理システムの耐障害性や性能 • 特権 ID 管理システムの冗長化や障害復旧機能 • 同時接続数が増加した際の動作性能 • ログ/証跡データの保存可能期間 • スケールアウトやスケールアップの容易性
	その他の機能	• ファイルの持ち込み/持ち出しを検知、制限する機能 • 管理対象システムへの接続に利用できる各種ツール（リモートデスクトップや Tera Term 等）への対応 • UI やキーボードの多言語対応 • エージェントのアンインストールを防止する機能

第2章 特権 ID 管理の現状把握と課題・リスクの訴求

特権 ID 管理システムの導入を検討していく上で、特権 ID 管理、システム環境、運用に関して現状を把握し明らかにすることで経営層へ特権 ID 管理の実態と課題・リスクを訴求することが可能となる。また現状の把握、課題とリスクは企画フェーズにおけるインプットにもすることができる。

本章では、特権 ID システム導入検討においてその必要性を経営層に訴求する上で必要となる現状把握と課題・リスク洗い出しのポイントに関しての内容の概要を示す。

図 2-1 特権 ID の課題整理フロー



2.1. 特権 ID 管理状況の現状把握と課題・リスクの明確化

経営層に特権 ID 管理システムの必要性を特権 ID 管理の観点で訴求していくために、主に特権 ID を利用してアクセスする重要データを所持するサーバーやシステム環境で重要な役割を持つ機器に対して、適切な利用者が適切な特権 ID を適切に利用しているか現状を把握し課題とリスクを明確にすることが重要である。そのうえで特権 ID 管理システムを導入した際にセキュリティ面としてどのような点に留意しなければいけないのかを明確にし、企画フェーズで特権 ID 管理対象システム、管理対象の特権 ID、特権 ID 利用者を検討していく必要がある。

2.1.1. 特権 ID 管理対象システムの現状把握と課題・リスクの明確化

サーバー、ミドルウェア、NW 機器、本番環境、検証環境があげられ仮想環境やクラウド環境に対象システムがある場合、仮想環境やクラウド環境の管理コンソールがどこまで把握できているか、適切に管理されているか現状を把握し課題とリスクを明確にする。

表 2-1 管理対象システムの洗い出し（例）

システム	環境	OS 種別	重要データ/システム	特権 ID	特権 ID の利用者	利用環境
サーバーA	本番	Windows	○			
サーバーB	本番	Linux	○			
サーバーC	検証	Linux	○			
サーバーD	検証	Linux	−			
NW 機器 A	本番	ネットワーク OS	○			
…	…	…	…			
クラウドコンソール	本番	管理コンソール	○			
クラウドサーバーA	本番	Windows	○			
クラウドサーバーB	本番	Linux	○			
…	…	…	…			

2.1.2. 特権 ID の現状把握と課題・リスクの明確化

特権アクセスが必要なデータにアクセス可能な ID やシステム設定が変更可能な ID や、本番環境、検証環境にかかわらず特権でアクセスする重要データを保持するシステムの特権 ID、また適切に管理されているか現状を把握し課題とリスクを明確にする。

表 2-2 特権 ID 管理対象システムの特権 ID の洗い出し（例）

システム	環境	OS 種別	重要データ/システム	特権 ID	特権 ID の利用者	利用環境
サーバーA	本番	Windows	○	Administrator		
サーバーB	本番	Linux	○	管理者 ID A		
サーバーC	検証	Linux	○	管理者 ID B		
サーバーD	検証	Linux	−	sa		
NW 機器 A	本番	ネットワーク OS	○	root		
…	…	…	…	管理者 ID C		
クラウドコンソール	本番	管理コンソール	○	root		
クラウドサーバーA	本番	Windows	○	root		
クラウドサーバーB	本番	Linux	○	root		
…	…	…	…	…		

2.1.3. 特権 ID 利用者の現状把握と課題・リスクの明確化

管理者権限を持つことの多いシステムオーナー、システム運用者、データ管理者、開発者、場合によってはエンドユーザーも含め適切な方法で、適切なシステム、データにアクセスしているか現状を把握し課題・リスクを明確にする。

表 2-3 特権 ID 対象システムと特権 ID 管理対象の洗い出し（例）

システム	環境	OS 種別	重要データ/システム	特権 ID	特権 ID の利用者	利用環境
サーバーA	本番	Windows	○	Administrator	サーバー管理者 1	
サーバーB	本番	Linux	○	管理者 ID A	サーバー管理者 2	
サーバーC	検証	Linux	○	管理者 ID B	サーバー管理者 3	
サーバーD	検証	Linux	−	sa	サーバー管理者 1	
NW 機器 A	本番	ネットワーク OS	○	root	サーバー管理者 2	
…	…	…	…	管理者 ID C	DB 管理者	
クラウドコンソール	本番	管理コンソール	○	root	サーバー管理者 4	
クラウドサーバーA	本番	Windows	○	root	サーバー管理者 1	
クラウドサーバーB	本番	Linux	○	root	サーバー管理者 1	
…	…	…	…	…	サーバー管理者 2	

2.2. システム環境の現状把握と課題・リスクの明確化

経営層に特権 ID 管理システムの必要性を現状のシステム環境の観点で訴求していくために、現在特権 ID 管理対象システムがどのような環境に存在し、特権 ID の利用者がどのような環境から特権 ID 管理対象システムに安全な経路でアクセスし、安全に利用できているか現状を把握し課題とリスクを明確にすることが重要である。

具体的には社内ネットワークからのオンプレ環境の対象システムへアクセス、社内からクラウド環境にある対象システムへのアクセス、社外からインターネット経由でクラウド環境にある対象システムへ直接アクセスするなどの自社で利用するアクセス経路、環境の課題・リスクを明確にすることである。

そのうえで特権 ID 管理システムを導入した際にシステム環境としてどのような点に留意しなければいけないのかを明確にし、企画フェーズで対象とするシステムや対象とするアクセス経路を検討していく必要がある。

表 2-4 特権 ID 利用者と利用環境の洗い出し（例）

システム	環境	OS 種別	重要データ/システム	特権 ID	特権 ID の利用者	利用環境
サーバーA	本番	Windows	○	Administrator	サーバー管理者 1	社内/リモート
サーバーB	本番	Linux	○	管理者 ID A	サーバー管理者 2	社内/リモート
サーバーC	検証	Linux	○	管理者 ID B	サーバー管理者 3	社内/リモート
サーバーD	検証	Linux	−	sa	サーバー管理者 1	社内/リモート
NW 機器 A	本番	ネットワーク OS	○	root	サーバー管理者 2	社内/リモート
…	…	…	…	管理者 ID C	DB 管理者	社内/リモート
クラウドコンソール	本番	管理コンソール	○	root	サーバー管理者 4	社内
クラウドサーバーA	本番	Windows	○	root	サーバー管理者 1	社内
クラウドサーバーB	本番	Linux	○	root	サーバー管理者 1	社内
…	…	…	…	…	サーバー管理者 2	社内

2.3. 特権 ID 管理運用の現状把握と課題・リスクの明確化

すでに特権 ID 管理の運用を行っていることも多いと想定されるが、経営層に特権 ID 管理システムの必要性を特権 ID 管理運用の観点で訴求していくために、特権 ID の利用申請、承認、棚卸などプロセスや特権 ID の改廃、特権 ID 利用者の改廃プロセス、特権 ID を利用する作業の種類などの現状を把握するとともに、特権 ID 管理に係る運用にどのくらいの工数がかかっている現状を把握し課題とリスクを明確にすることが重要である。

そのうえで特権 ID の利用者の利用形態や本番環境、検証環境など対象システムの環境をどの範囲まで特権管理システムで管理するべきか、変更管理、構成管理、ログ管理・分析、監視、棚卸、監査などとの連携をどこまで行うのか、特権 ID の管理、利用に関するプロセスを特権 ID 管理システム全体としてどの範囲まで導入するか企画フェーズ、運用設計フェーズで検討する。

第3章 特権 ID 管理システム導入全体の流れ

3.1. 特権 ID 管理導入の流れ

特権 ID 管理システムを導入する際は以下のような流れで導入を行う。

各フェーズの作業概要を以下に示す。

表 3-1 各フェーズの作業概要

フェーズ	作業概要
システム企画	特権 ID の現状を調査・分析し、課題を明確にした上で、システム化の企画、導入ロードマップ、実行体制の策定を行う。
要件定義	特権 ID システムに対する機能要件・非機能要件を洗い出し、システム化の範囲を確定する。パッケージやサービスを利用するケースにおいては、上記要件との適合性を確認し、システムで実現する範囲を決定する。
システム設計	要件定義で洗い出された要件をもとに、外部仕様（ユーザー I/F、外部 I/F、業務ロジック、リポジトリ）を設計する。
システム実装・テスト	設計にもとづき、モジュールの導入、各種機能の設定、ユーザーと特権 ID の管理対象システムの登録、外部連携機能の設定を実施する。システム開発の V 字モデルに従ったテストを実施し、要件や設計書で定めた内容がシステムに反映されているか確認する。

システム運用	特権 ID 管理システムを運用するための運用体制の構築、ならびに教育・トレーニングを実施する。定期的に運用状況の課題を洗い出し、システム改善計画を立案する。

3.2. 前提条件、留意事項

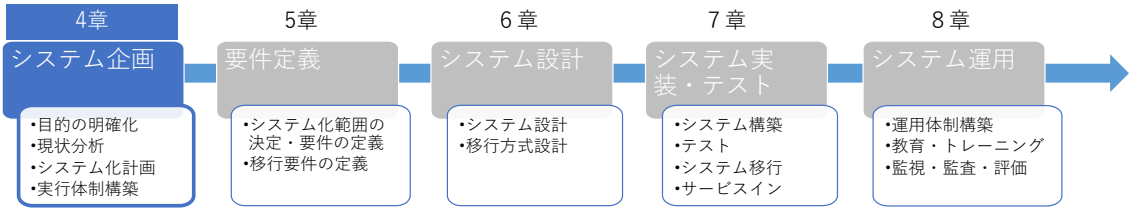
特権 ID 管理システムを導入する際には以下のような前提条件、留意事項を考慮する必要がある。

表 3-2 前提条件や留意事項の整理

前提条件、留意事項	考慮が必要な理由	対策例
既存業務フローや手順が確認可能であること	現状分析を行うため、既存業務フローや手順が記載されたドキュメントが存在している、もしくはそれらを説明ができるメンバーが存在する必要がある。	システム導入時には業務フローや手順をドキュメントとして残すように、システム構築ベンダーに依頼する。
システム化範囲が肥大化しないようにすること	特権 ID はあらゆるシステムに存在するため、一度にすべてを対応することは困難である。	個人情報を扱うシステムなど重要システムを優先的し、一部システムから導入を実施する。
標準化を意識した業務フロー設計を行うこと	システム個別の業務フロー乱立してしまうと、システム運用の負荷増大やガバナンスの低下に繋がる。	既存業務フローの踏襲を優先すると、業務フロー乱立に繋がりやすいため、あるべき姿をベースに検討を行う。
企業の特性にあったプロセス設計を行うこと	各システムの運用体制や役割分担は企業ごとに特色が出やすいため、安易に類似	安易に類似企業のプロセスを採用するのではなく、セキュリティリスクや課題を

	企業のプロセスを採用すると逆に導入難易度が高くなる可能性がある。	明確にした上で最適なプロセスを採用する。
運用開始後も定期的に運用プロセスを見直すこと	導入時に決定したプロセスを盲目的に守り続けているだけでは、運用が形骸化する可能性がある。	システム環境の変化やセキュリティリスクの変化に合わせて運用の見直しを行う。
企業トップからのガバナンスを利かせること	ステークホルダーが多岐に渡るケースが多いため、組織間の利害関係で衝突が発生する可能性がある。	特権 ID 管理はセキュリティリスクを低減するための重要な基盤であることをトップメッセージによりステークホルダーに認識してもらう。

第4章 特権 ID 管理システム企画フェーズ



4.1. 企画フェーズの目的

このフェーズでは、特権 ID 管理システムの必要性を確認するために、特権 ID 管理の現状を調査・分析することで課題やその優先順位を明らかにする。その後、特権 ID 管理システム導入に向けたシステム計画およびプロジェクト体制を策定する。

4.2. 特権 ID 管理の目的の明確化

特権 ID 管理システムを導入する前に、まず特権 ID 管理の目的を明らかにする。特権 ID 管理システムの検討をしているということは、特権 ID 管理（あるいは特権アクセス管理）に関する何らかの課題が生じているはずである。その課題を洗い出し、分類・整理し、優先順位付けすることで、目的を明確化していく必要がある。

■必要なインプット情報

インプット情報	利用方法/内容
特権 ID 管理の課題	現状抱えている課題

特権 ID 管理に関する一般的な（よくある）課題は以下のとおり。

- 誰が、いつ、どの特権 ID（特権アクセス）を使用しているか不明
- 誰が、どの権限（全権、高権限）を持っているか不明
- 誰が、特権 ID のパスワードを知っているか不明
- インシデントが発生したが、特権 ID の利用履歴はそもそも取得しているのか？
- システムセキュリティ監査で特権 ID の利用（管理）について指摘を受けた
- 全社的なセキュリティ認定を取得したいが、特権 ID の管理はできているのか
- 取引先（最重要顧客）からセキュリティ対策要請（特に特権 ID）がきた

課題を洗い出した後、それらを分類・整理し、優先順位付けしていく必要がある。整理の指標は企業毎に定義していく必要があるが、指標の例として「重要度」や「緊急度」がある。

表 4-1　課題の整理

課題	重要度（高、中、低）	緊急度（高、中、低）
取引先からセキュリティ対策の一環として特権 ID 管理を要請されている	高 弊社の最重要顧客の 1 社のため	高 202x/3/31 までに対応が必要
内部のシステムセキュリティ監査で特権 ID 管理の不備を指摘された	中 任意のセキュリティ監査のため、重要性は高くない	中 現時点でインシデントは発生していないため、緊急性は高くない
XXX	低	低
…	…	…

上記の例では重要度/緊急度は 3 段階（高、中、低）としているが、これは企業毎に定義していく必要がある。また、優先順位についても定義する必要がある。

表 4-2　優先順位の整理

表　優先順位優先順位	説明
1	重要度「高」かつ緊急度「高」のもの
2	重要度「高」あるいは緊急度「高」のもの
3	重要度「中」あるいは緊急度「中」のもの
…	…

上記の例では優先順位は重要度と緊急度の組み合わせをベースにしているが、これは企業毎に定義していく必要がある。

優先順位を定義した後、今回の検討目的の範囲を決定する。例えば、優先順位の 1～2 を範囲とする場合、その優先順位に含まれる課題に対応することが、今回の特権 ID 管理の目的となる。

表 4-3　検討目的の範囲

課題	重要度 （高、中、低）	緊急度 （高、中、低）	優先順位	今回の範囲
取引先からセキュリティ対策の一環として特権 ID 管理を要請されている	高 取引先は弊社の最重要顧客の 1 社であるため	高 202x/3/31 までに対応が必要	1	◎
内部のシステムセキュリティ監査で特権 ID 管理の不備を指摘された	中 任意のセキュリティ監査のため、重要性は高くない	中 現時点でインシデントは発生していないため、緊急性は高くない	3	－
XXX	低	低	…	…
…	…	…	…	…

上記の例では、優先順位 1～2 に該当する課題は 1 つだけであるため、今回の特権 ID 管理の目的は「サプライチェーンのセキュリティ対策強化要請に伴う特権 ID 管理の見直し」となる。課題が複数ある場合は、共通部分を抜き出して目的とするか、複数の課題を包括する目的とすることが望ましい。

■成果物

成果物	内容
特権 ID 管理の目的	特権 ID 管理の課題、重要度、緊急度、優先順位をまとめたもの

4.3. 現状分析

特権 ID 管理の目的が明らかになったため、次に特権 ID 管理の現状を分析する。

■必要なインプット情報

インプット情報	利用方法/内容
特権 ID 管理の検討	第 2 章「特権 ID 管理の現状把握と課題・リスクの訴求」で検討した次の事項 ・特権 ID 管理対象システムの洗い出し ・特権 ID 管理対象の特権 ID の洗い出し ・特権 ID 対象システムと特権 ID 管理対象 ・特権 ID 利用者と利用環境の洗い出し ・特権 ID 管理プロセスの洗い出し

現状分析のステップは以下のとおり。

1. 対象範囲（スコープ）の定義

2. 現状の調査

3. ギャップの抽出

4. 目的との整合性確認

まず、現状分析の対象範囲（スコープ）を定義する。対象範囲（スコープ）の一般的な（よくある）検討内容は以下のとおり。

- 対象とするサービス、システム（オンプレのみか、クラウドも含むか）
- 対象とする OS、データベース、ミドルウェア、Web サーバー

- 対象とする環境（本番環境、開発環境、検証環境など）
- 対象とする ID、権限（全権管理者のみとするか、高権限も含めるか）
- 人が使う ID のみか、システムが使う ID も対象とするか（バッチ処理用の ID なども対象とするか）

対象範囲は、特権 ID 管理の目的を達成するために十分な内容になっていることを確認する必要がある。もし対象範囲が目的達成にふさわしくないものになっている場合、再度目的を見直すか、あるいは対象範囲を再検討することが必要となる。

次に、現状を調査する。先ほど定義した対象範囲（スコープ）に対し、現状どうなっているかを調査する。調査方法は以下のとおり。

- システムの文書（設計書、パラメータシート）を確認する
- システムにログインし、実機のパラメータを確認する

文書が最新化されており、かつ文書の記載に抜け漏れがないことを保障できるのであれば、文書による現状調査が最も効率が良い。しかし実際は文書が適切にメンテナンスされていないこともあるため、大枠の調査は文書を使用し、細部の調査はシステムで確認することになる。

現状調査の調査内容は多岐にわたる。次に例を示す。

- 利用者、利用場所、利用デバイス、利用目的
- 利用時の申請/承認、ワークフローシステム利用有無
  - 代理申請の可否、複数承認の有無、多段承認の有無、代理承認の有無
  - 申請時間の延長可否、など
- 特権 ID のパスワード受け渡し方法
  - 特権 ID 返却時のパスワード変更有無、変更時のパスワードポリシー

- MFA 利用の有無

- 特権 ID 利用の点検/監査
  - 点検内容、監査内容、問題発見時の対処内容/対処フロー
  - ID 棚卸の有無
  - どの部署が点検/監査しているか

次にギャップを抽出する。先ほど調査した現状に対し、本当だったらこうしたい（あるべき姿）と比較していく。あるべき姿については、企業のセキュリティポリシーや関連文書をベースとしても良いし、企業の中期計画や経営理念等をベースとしても良い。あるいは、自社が所属する業界に関するセキュリティガイドラインがある場合は、そういったものもあるべき姿として現状との比較に使用することができる。

現状調査の例を示す。

＜調査対象システム　〇〇〇システム＞

表 4-4　現状調査　調査項目

現状調査　調査項目	調査結果	ギャップ （あるべき姿との差異）
利用者	各システムの管理責任者、副責任者の他、業務委託先のメンバーも利用している。業務委託先利用者の名前、人数は把握できていない。	利用者は自社メンバーのみに限定すべきである。やむを得ない理由で自社メンバー以外に貸し出す場合、申請書に基づき個人を特定し、返却後にパスワード変更することが望ましい。
パスワード受け渡し	特権 ID のパスワードを変更していないため、一度教えたパスワードをそのまま利用していることがわかった。 ※最初のパスワード受け渡しは申請者にメールでそのまま（暗号化せずに）送っている。	パスワードを知っていれば申請無しで特権 ID を利用できてしまうため、この運用を変更したい。 可能であれば、申請者にパスワードを開示しないで特権 ID を使えるようにしたい。
…	…	…

最後に目的との整合性を確認する。ギャップの内容を確認し、このギャップを解消すれば目的が達成されるかどうかを確認する。例えば目的が達成されるものを「〇」、部分的に達成されるものを「△」、あまり達成されないものを「×」として印付けする。

表 4-5　目的との整合性

現状調査　調査項目	調査結果	ギャップ	目的との整合性
利用者	（略）	（略）	○
パスワード受け渡し	（略）	（略）	△
…	…	…	…

■成果物

成果物	内容
現状調査報告	特権 ID 管理の現状をまとめた調査報告書

4.4. 特権 ID 管理システム計画作成

特権 ID 管理に必要なものが把握できたため、システム計画を作成する。

■必要なインプット情報

インプット情報	利用方法/内容
現状調査報告	4.3 現状分析で作成した現状調査報告書

これは自社のシステム開発計画として利用するためのものである。また、自社でシステム開発を実施しない場合、システム計画ではなく RFP（提案依頼書：Request for Proposal）を作成しても良い。

システム計画の目次案は次のとおりである。システム計画に必要な項目は各組織により異なるため、必要に応じて項目は追加/削除していただきたい。

表 4-6　システム計画書目次案

目次	記載内容
概要	背景 課題 目的（目標） 成果物　など
スコープ	範囲（システム、拠点、環境など） 要求事項（機能要件、非機能要件など） 制約 前提条件　など ※法令や各種ガイドラインによる制約/前提条件がある場合は必ず明記すること

目次	記載内容
スケジュール	タスク/WBS マイルストーン 依存関係 期間 リソース　など ※事前に PoC を実施する場合、それらも加味したスケジュールを立案すること ※契約等で時間がかかる場合、スケジュール間に適切な間隔を開けておくことも重要
予算	予算 予算に含まれるもの（ライセンス、役務、構築費用、保守費用など） ※予算執行に期限がある場合、明記すること
その他	品質管理（管理基準、管理方法など） リスク（分析方法、管理基準、発生時の対応方針など） 調達（方針、契約形態、調達プロセスなど） コミュニケーション（会議体の設定、コミュニケーション方法、対象者など） 人的リソース（プロジェクト運営に必要なリソース計画、外部ベンダー選定基準、要員育成方針など） ※その他必要に応じて

■成果物

成果物	内容
特権 ID 管理システム計画	特権 ID 管理プロジェクトのシステム計画書

4.5. プロジェクト体制

システム計画に基づきプロジェクトを推進するためのプロジェクト体制を構築する必要がある。

■必要なインプット情報

インプット情報	利用方法/内容
社内外の関係者情報（会社名、組織名、名前、連絡先など）	プロジェクト体制（連絡先、体制図）を作成するために使用

- 社内

社内のプロジェクト関係者は多岐にわたる。次は一例である。

- プロジェクト主管部門
- システム企画部門
- システム構築部門
- システム保守部門
- 特権 ID 管理システムの対象となるシステムの主幹部門
- 経営層
- システム監査部門
- セキュリティ部門

- 品質管理部門

プロジェクトのフェーズによって関係部門が変わる場合は、それがわかるようにプロジェクト体制を記載しておくと良い。

- 社外

社内と同様、社外のプロジェクト関係者も多岐にわたる。次は一例である。

- 導入するシステムの開発ベンダー
- 提供会社（ディストリビュータ）
- システム構築ベンダー
- システム運用/保守ベンダー
- HW/SW メーカー（システムをオンプレミスで構築する場合）
- データセンター（サーバーをデータセンターに置く場合）

- その他

次の事項についても検討しておくことが望ましい。

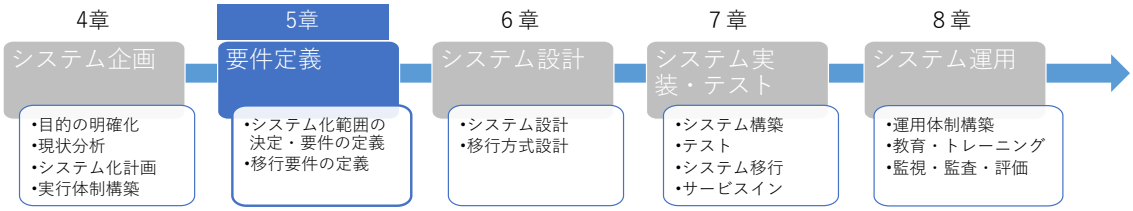
- プロジェクト期間中の連絡方法/連絡先
- 定例等の会議体の設定（オンライン会議含む）

※プロジェクト計画に記載してある場合は省略可能

■成果物

成果物	内容
プロジェクト体制	特権 ID 管理プロジェクトのプロジェクト体制（体制図、連絡先など）

第5章 特権 ID 管理システム要件定義フェーズ



5.1. 要件定義フェーズの目的

本フェーズでは、特権 ID 管理システムに求められる役割および求められる機能を明確化することを目的とする。特権 ID 管理システムとしてあるべき姿を定義し、必要となる機能を整理することで、どのような仕組みで対応するのか、どのようなソリューション・サービスが適切なのかを検討するために要件として定義する。

5.2. 要件定義フェーズの前提条件

要件定義フェーズを実施するにあたっては以下の内容の確認・整理が必要であり、企画フェーズのアウトプットを踏まえる必要がある。

- 監査要件
  - IT システム監査の目的・スコープについて明確化し、監査対象項目、管理手法の定義を行う
  - 監査対象のデータは何かを明確にするため、取扱情報や漏洩・改ざんによる影響の大きい要素の定義を行い特権管理で取り扱う使用アカウントの役割定義や権限制限を明確化する。
- セキュリティ要件
  - 特権 ID を悪用されることへのリスクの整理

- 対象システム毎の特権 ID の管理状況の確認

・ 運用要件

- 管理対象システムにおける既存運用要件の整理し、特権管理システムへの移行を見据えた運用要件を整理する。
- 運用要件においては、既存システムに対する改修の可否、運用における影響などを整理する。

5.3. 特権 ID システムの要件定義

特権 ID システムの適用範囲、実装対象の要件について検討し定義する。

本プロセスの目的は特権 ID 管理業務を明確にし、システム化に必要な要件を定義することである。

本プロセスの前提となるインプット情報は企画フェーズの成果物であり、以下のとおりである。

■必要なインプット情報

インプット情報	利用方法/内容
現状調査報告	特権 ID 管理システムに求められる要件定義するための情報として、特権 ID 管理の対象となるシステム・サービス、各種リソースの特権 ID が現状どのように管理・運用されており、どのような課題があるのを把握する必要がある。
特権 ID 管理システム計画	要件定義時の基本方針として、特権 ID 管理システムのどういう目的でどのような目標を目指し、どこまでの範囲を適用対象とするのかといった企画・計画の内容を認識する必要がある。

プロジェクト体制	プロジェクト体制

■留意事項

留意事項	留意内容
利用者の ID	役割に応じて管理対象の特権アカウントが異なる
共有 ID と個人 ID	ID の利用方法について個人利用する特権 ID を用意するのか、共有利用する特権 ID を用意するのかの検討が必要。 特にクラウドサービスにおいては、ID の共有利用が禁止されているケースや ID を新たに作成することで、ライセンスが発生することも考えられるため、個別に検討が必要となるケースもある。
利用中の特権 ID の停止可否	現在利用中の ID を特権 ID 管理システムの貸出対象とするかもしくは新たに貸出用の ID を準備するのかの検討が必要となる。利用中の ID を特権 ID 管理システムの貸出対象とする場合、申請外の利用を防止するための対応（パスワードリセットなど）について検討が必要となる。 アプリやバッチなどの組み込みとして利用されている場合は、パスワード変更が難しい可能性があり、アプリ側の変更なども考慮する必要がなる。
例外要件の想定	運用において融通性を持たせるために、通常運用では対応しきれない緊急運用が求められる事態での例外要件も想定し、対応案を検討しておく。

■具体的な検討項目

以下に具体的な検討項目を記載します。

① システム化範囲の整理

システム化の範囲を明確化するために特権 ID 管理の対象となるシステム、および対象となる業務を整理し定義する。

その際、例えば、会計に関わるシステムを対象とする、通常運用で利用するアカウントは除外するなど、システムやサービスの観点とそのシステムおよび業務のなかで利用されるアカウントの両方の観点が必要となる。

アカウントの種類によって、想定される利用方法や特権 ID の管理方法も異なるため、定めた範囲に合わせて、各 ID がどのような業務・用途で利用されているのかを整理し、どのような管理が必要なのかを明確にする。

- 管理対象システム・サービス
  - 対象システム
    - 対象システムの区分（会計システムなど、システムの区分）
    - 対象サービス（アカウント種別）
      - OS、DB、アプリケーション、SaaS など
- 対象業務・アカウント種別（利用者・用途）
  - システム維持・運用担当者が利用するアカウント
  - システム開発・更改にて利用するアカウント
  - システム組み込み用アカウント

② 制限事項の整理

特権 ID 管理システムの導入にあたって、対象となるシステム、アカウントに関して、以下のようなシステム的な制限事項を整理する。

・エージェントの導入可否

・特権 ID のパスワード変更可否

・直接アクセスの可否

・ログ収集の可否、ログ収集場所

③ 特権 ID の管理要件の定義

対象システム上の特権 ID を正しく維持するための対応に関する要件を定義する。

例えば、ターゲットシステムへの特権 ID の作成・更新・削除のタイミングの整理や方法の定義、また、ID の棚卸方法やレポート出力の要否について明確にする。

④ 特権 ID の利用フローに関する要件定義

特権 ID の利用に関して、どのようなフローで利用者に ID 利用させるのかの要件を定義する。利用者は一般的にはワークフローによる申請・承認を経て ID の利用権限を取得する。そのため、管理対象の特権 ID ごとに以下のような事項を明確にする。

- 利用者・申請者・承認者は誰か
- 申請・承認の実行や依頼の通知方法（一般的にはメールでの通知）
- 申請・承認時の入力項目（一般的な入力項目に加え、作業手順書エビデンスなどの添付が必要かなども確認する）

・ 申請可能な利用期間、申請の頻度

・ 申請無しでの利用を許可するか

・ 緊急時など承認なしの利用（事後承認など）を許可するか

⑤ 特権 ID の利用方法に関する要件定義

特権 ID の利用フローと合わせて特権 ID を利用させるためにどのようにアクセス制御を行うのか、また特権 ID を利用者にどのように払い出していくのかの要件を定義する。

特権 ID の払い出しについては、想定される利用シーン、対象 ID のパスワード変更可否などによって変わる。

※「表 1-2 特権 ID 管理システムの代表的な機能」参照のこと

以下に主な方式について例示する。

表 5-1 特権 ID 払い出しの主な方式

	方式	内容
1	パスワード貸出方式（ワンタイムパスワード方式）	利用のタイミングで利用者に特権 ID のパスワードを通知することで、特権 ID の利用を制限する。 利用の前後でパスワードを変更することで、申請時間外の利用を防止する。
2	自動ログイン方式	ユーザーにはパスワードを通知せずに、特権 ID 管理システムの仕組みでアプリケーションに自動的にログインさせることで特権 ID の利用を制限する。

		ユーザーにはパスワードを隠ぺいして利用させるため、申請時間外での利用、直接アクセスなどの利用を防止する。
3	ワンタイム ID 方式（Just-in-Time プロビジョニング）	特権 ID の利用のタイミングで、ID を作成（もしくは有効化）し、利用期間が終了すると ID を削除（もしくは無効化）して、特権 ID の利用を制限する。利用申請時間外は特権 ID 自体が利用できない状況となるため、申請時間外、直接のアクセスを防止する。 特権 ID を実際に利用する際には、パスワード貸出もしくは自動ログインのどちらかで利用する。

⑥ 特権 ID の利用状況の確認に関する要件定義

特権 ID が申請・承認に基づき正しく利用されていることを確認するためにどのような証跡を取得するのかの要件を定義する。

また、取得するログの種類・量に応じてログ保存用のリポジトリ設計も必要になるため、証跡確保の目的に合わせて、どのようなログをどの程度の期間保持するのかを明確にする。

※「表 1-2 特権 ID 管理システムの代表的な機能」参照

以下に主なログについて例示する。

表 5-2 ログの主な種類

	方式	内容
1	ターゲットシステムのアクセスログ	ターゲットシステムに出力されるアクセスログを収集し、申請のあった時間のみにログインが行われていることを確認する。

2	特権 ID 管理システムの利用ログ	特権 ID 管理システムを利用してターゲットシステムにログインした履歴を特権 ID 管理システム上のログから確認する。
3	動画ログ	特権 ID の利用に関して、操作内容を確認するためのログ。 踏み台方式やゲートウェイ方式の場合など、特権 ID を利用するために必ず特定のサーバーを経由する場合に、該当サーバー上で動画のログを取得し、実際の操作内容を視覚的に確認する。
4	操作ログ	特権 ID の利用に関して、操作内容を確認するためのログ。 動画ログと異なり、実行したコマンドや、プロセスなどを取得し、機械的に実行内容を確認可能。 取得した操作ログの内容をもとに検索性の向上や特定操作に対して通知するなどの対応が可能。

⑦ 運用に関する要件定義

特権 ID 管理システムの運用に関する要件を定義する。

運用については、システムの利用に関する要件と、システム管理業務における要件の観点で検討する。

（システム管理業務に関する要件）

・特権 ID システムにログインするためのユーザーID の管理について

ユーザーID の管理方針や方法、認証方法などの要件を定義する。

企業の従業員の場合、全てのユーザーがこのシステムを利用するわけではないため、どのような従業員がどのようなタイミングでこのシステムを利用できるようになるのかを整理し、システムを利用するためのユーザー情報の登録・更新・削除のライフサイクルについて整理する。

また、ユーザー情報のメンテナンス方法や認証についてどのような方式での対応が可能なのかを整理しておく。例えば、社内の ID 管理システムから必要な情報を連携して特権 ID管理システムの利用者を管理する、ActiveDirectory など認証基盤と連携するなど、組織内の ID 管理および認証基盤となるシステムとの連携についてどのような要件が必要になるのかを明確にする。

・管理対象のターゲット追加時の運用手順の整理

ターゲットの登録者、登録のためのフロー、ネットワーク設定などの事前作業、前提条件などを整理し、明確にする。

どのようなサーバー、サービスが特権 ID 管理システムの対象となるのかを明確にし、新システムが追加された際に、特権 ID 管理システムの運用者に連携すべき事項を定義する。

・監査対応のための要件に関する定義

特権 ID 管理システムを利用した特権 ID の管理が適切に実施されているかの監査に対応するためにどのような情報の提示が必要なのかを確認し、レポート出力など必要な機能を明確にする。

例えば、申請・承認にもとづいた作業が行われていることを証明するために、申請・承認の履歴と実際のシステムの利用実績の突合せなどが求められる。このような情報を提示するために、必要となる、ログの種類、出力項目、保管期間なども決めておく必要がある。

（システムの利用に関する要件）

・夜間の緊急利用など、承認者不在時での特権 ID に関する要件定義

承認者が不在の際にどのようなフローで特権 ID を利用するのかを整理する。一般的には、事後承認機能などが求められるケースが多い。

・システム停止時の特権 ID 利用に関する要件定義

特権 ID 管理システムが停止している際に、どのようなフローで特権 ID を利用するのかを明確にする。システム停止のため、未申請での利用や、システムを介さない直接のアクセスが必要になり、特権 ID の利用方法、不正利用をチェックするための仕組みの検討が必要になる。

⑧ 非機能要件

・ 非機能要件については、以下のような内容を検討する。

※ただし、各サービスの実装方式や運用の要件によっても変わるため、実装方式や採用するサービス側で定義されている方針に従って検討することを推奨する。

- ✧ 障害時対応
- ✧ パフォーマンス・レスポンス
- ✧ セキュリティ（特権 ID 管理システム自体のセキュリティ）
- ✧ システム監視
- ✧ バックアップ・リカバリ
- ✧ 構成（冗長化、災対、スケールアウト）

■成果物

成果物	内容
特権 ID 管理システムの要件定義書	上記要件にて検討された結果としての要件の集合。主に以下の内容を含む ・特権 ID 管理システム利用フロー

	・管理対象 ID に関する要件 ・取得対象の証跡に関する要件 ・サービス機能要件一覧 ・運用要件

5.4. 実装方式の検討

本フェーズでは、特権 ID 管理システムの各要件をもとに、実装機能、実現方式について検討する。

実現方式の各パターンについては、1 章を参照。

今後のソリューション選定に向けて、自社の要件と実現方式の Fit&Gap を整理し、適合する実現方式について検討する。なお、製品・ソリューション選定に向けて実装方式が明確になる場合は、成果物として提示する。

■必要なインプット情報

インプット情報	利用方法/内容
特権 ID 管理システムの要件定義書	特権 ID 管理システムの要件一覧と特権 ID 管理システムの実現方式もしくは個別のソリューションとの適合性を判断するために利用する。

■留意事項

留意事項	留意内容
全ての要件を満たすソリューションは存在しない	必要な要件に優先順位をつけて検討する。 単一のソリューションでは対応できない場合に運用等で回避するのか、複数の製品を組み合わせて実現するのか、等の検討が必要となる。

■具体的な内容

対象システムや特権 ID における制限事項および要件一覧に応じた実装方式を検討する。

例えば、対象サーバーや作業端末へのモジュールの導入可否、必要なログの取得方法、想定される貸出方式などにより、対応可能な実装方式を決定する。

複数の方式にて対応可能なケースもあるため、実際のソリューション選定までは、自社の運用でどのような方式が対応しているのかを確認するにとどめておく。

■成果物

成果物	内容
特権 ID 管理の実現方式	想定される、もしくは推奨される特権 ID 管理の実装方式について記述する。記載内容については可能な限り システム構成図なども含める

5.5. 移行の要件定義

本プロセスの目的は、ID 管理システム導入に伴い必要となる移行に関する要件を具体化することである。

本プロセスの成果物が移行の設計フェーズのインプットとなる。

本プロセスのインプットとしては、企画フェーズでの成果物である。

■必要なインプット情報

インプット情報	利用方法/内容
現状調査報告	移行に求められる要件を定義するために、特権 ID 管理システムの対象となる一覧や対象となる特権 ID、現行の運用などを把握するために利用する

特権 ID 管理システム計画	移行の要件定義のベースとなる特権 ID 管理システムの全体像を把握するために利用する。 移行のロードマップを決定するために、最終的にどこまでをシステム化し、どのように展開していくのかを決定する。

■留意事項

留意事項	留意内容
管理対象システムの利用者との	特権 ID 管理システム移行後は本システムでの申請が必須となるため、利用者との調整が必須となる。 申請外の利用を禁止するだけでなく
リスクの想定	管理対象の特権 ID が意図せず、アプリケーションやバッチなどの組み込み利用していた場合パスワード変更などに伴って、障害となるケースが考えられる。 要件定義フェーズから移行の影響を考慮し、初期の対応について想定しておく。

■具体的な内容

① 必要となる移行作業の洗い出し

特権 ID 管理システム導入に伴い必要となる移行作業として、どのような作業項目があるかを洗い出す。

ターゲットシステム側での情報収集や設定変更作業に加え、特権 ID 管理システムの初期登録に必要なデータの収集方法、利用者への新システムでの運用手順の周知や教育、マニュアル作成などの運用業務など、必要なる移行作業を明確にする。

ただし、具体的な作業については、実装方式や採用するソリューションに影響されるため、本フェーズでは今後の関係各所との調整のために作業が必要な範囲の整理にとどめておく。

② 移行作業の要件定義

① で洗い出した移行作業項目に関する要件を定義する。

たとえば、初期登録に必要なデータがどこに存在しているか、ターゲットシステム側での作業に必要な手順は何か、ターゲットシステム側のシステム的な制約や本番運用中であるがゆえの制約など、移行作業に関する要件を明確にする。

③ 移行スケジュールの要件定義

特権 ID 管理業務をシステムに移行するための移行作業のスケジュールに関する要件を定義する。

移行作業項目の作業の順序に関する制約を整理し、段階的な移行を実施するのか、現状の運用と並行した実施が可能なのかを明確にする。

④ 想定されるリスクと対処の方針の整理

移行作業でどのようなリスクが想定されるのかを洗い出し、問題が発生したときの対処方針について定義する。

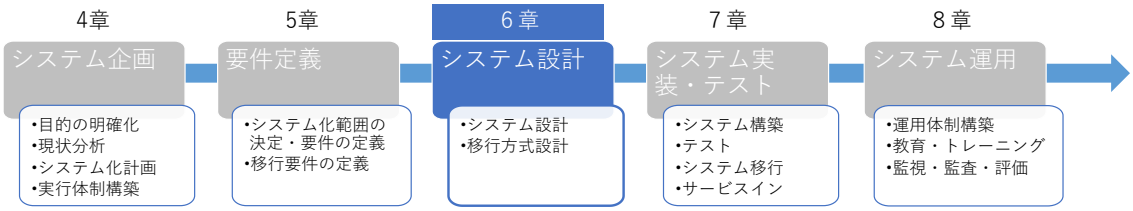
例えば、移行作業が予定通りに進まずに、一部のターゲットシステムの特権 IDのみが管理されている状態において、特権 IDの利用フローが従来のものと新システムで混在するケースなどが想定される。

また、特権 ID管理システム側から誤って特権 ID を削除やパスワードを書き換えてしまうことで、現在、運用や作業、システムの組み込みなどで利用中の特権 ID が使えなくなるケースなど、様々なリスクについて想定しておくことが重要である。

■成果物

成果物	内容
要件定義書（移行要件）	特権 ID 管理システムの移行要件を整理した要件集合で、主に以下の内容を含む ・移行作業要件 ・リスク・対処一覧

第6章 特権 ID 管理システム設計フェーズ



本フェーズでは、『特権 ID 管理システムの要件定義』にて定義された内容をもとに、特権 ID 管理システムの外部設計を行う

6.1. 設計フェーズの目的

特権 ID 管理システムの外部設計として、実装方式をベースに特権 ID 管理の業務フローを確定し、システムに必要な機能や処理内容について定義を行う。

6.2. 特権 ID 管理システムの設計

特権 ID システムの適用範囲、実装対象の要件について検討し定義する。

本プロセスの目的は特権 ID 管理システムの利用フローや業務を明確にし、システム化に必要な機能を定義することである。

本プロセスの前提となるインプット情報は要件定義フェーズの成果物であり、以下のとおりである。

■必要なインプット情報

インプット情報	利用方法/内容
要件定義書	要件定義フェーズで定義された特権 ID 管理システムの要件を満たすようにシステム機能の外部設計を行うために、実装する機能や方式を明確にするために利用する。

■留意事項

留意事項	留意内容
要件に従った設計	要件定義フェーズで定義された特権 ID 管理システムの要件を満たすように設計を行う。
業務フローの合意と承認	新たにシステムを構築する場合、システムの利用者が多岐にわたり、各業務フローが大きく変わることが予想されるため、後々変更が発生しないように必ず合意や承認をとってから設計を進めることが重要である。
体制の確認	特権 ID 管理システムの利用者は社内の複数の部署での利用や、外部ベンダーも含めた様々な人員が対象となるため各体制の役割を改めて意識してことが重要である。

■具体的な検討内容

具体的な設計内容は以下のとおりである。

1. 実装方式の確定

   要件にしたがい特権 ID 管理の実装方式について確定する。

2. 実装方式に合わせた特権 ID の利用フローの定義

   実装方式に合わせて特権 ID を利用するために、どのような手順、システムへのアクセスが発生するのかを整理する

3　ワークフローの設計

特権 ID の利用に際し、必要な申請・承認フローを定める。また利用時だけでなく、必要に応じて報告業務に関するフローについても設計を行う。

4　ログ管理の設計

特権 ID 管理システムで取得するログについてログ収集機能、ログ保管・管理について設計する。

5　特権 ID 管理システムのセキュリティ設計

特権 ID 管理システムへの不正アクセスを防止するために、ID 管理や認証、特権 ID 管理システム自体の管理者権限の管理方法について設計する。

■成果物

成果物	内容
基本設計書	基本設計のなかで要件から導き出された実装すべき、機能の一覧を定義し、各機能をどのような方式やソリューションで実装するのかを設計する。 システムが持つ機能をどのように実装するのかを機能一覧やシステム構成図の形式で成果物として作成する。

6.3. 移行計画の詳細化

移行の要件定義において定義されて以降要件に従って、移行設計を行う。

移行設計の目的は移行要件に基づいて移行の対象、手順、体制、リスク対策を明確にすることである。

移行の際には、ID の棚卸を行い、不要な ID の洗い出しや利用状況の精査を行うことが重要である。

■必要なインプット

インプット情報	利用方法/内容
要件定義書（移行要件）	要件定義フェーズ定義された移行要件に応じて移行設計を行う。

■留意事項

留意事項	留意内容
リスク管理	特権 ID 管理システムは様々なシステムの ID 情報に影響し、移行作業はリスクを伴う作業であるため、失敗するリスクや影響度を考慮し、問題発生時に切り戻せるように準備しておくことが重要である。

■具体的な検討内容

具体的な移行に関する検討内容は以下のとおりである。ここでの移行とは特権 ID の管理・運用を現行の方法から新たに構築するシステムに変更するための移行である。

1. 移行対象、手順、体制の明確化

特権 ID 管理システムに運用を移行する対象のシステム、移行のための手順・手続き、また、その手順、体制の明確化を行う。

2. 移行に必要なデータや移行のための機能の整理

特権 ID 管理システムへの登録が必要なデータ（利用者の情報や管理先となる IT リソースの情報）の整理や収集方法の確認を行う。

その他、データの収集やクレンジング、モジュールの配布などシステム化にあたって追加で必要な機能があれば、移行用の機能として設計する。

3. 移行の影響範囲とリスクへの対策に関する検討

設計した特権 ID 管理の実装方式をもとに、移行要件で確認してリスクがどう変化するのかを改めて検討し、システム化に伴う、リスクの整理および、対策についての検討を実施する。

4. 移行スケジュールの設計

移行のリハーサル、関係各所への説明や管理対象システムへの事前作業の依頼、必要な手順書やマニュアル作成などを含めた全体の移行スケジュールを設計する。

■成果物

成果物	内容
移行計画書	移行要件に基づいて、移行の対象、手順、体制、リスク対策、移行スケジュールについて設計を行う。
移行テスト計画書	移行のために必要な手順、機能に関しての試験要領、試験の観点、達成条件などを記述する
移行データ一覧	特権 ID 管理システムに登録するためのデータの一覧、該当データの取得方法、データを整理するための方針について記載する

6.4. 詳細設計

特権 ID 管理システムを構成する特権 ID 管理製品やソリューションの実装に向けた仕様の詳細を決定するための設計となる。

設計にあたっては、要件定義および基本設計にて定義した実装機能に合わせて製品のパラメータを決定する作業となる。ソリューションなどを利用しない場合や外部プログラムの開発などが必要な場合は、プログラム開発に必要な設計も含まれる。

■必要なインプット情報

インプット情報	利用方法/内容
要件定義書 基本設計	要件定義フェーズおよび基本設計フェーズで定義された特権 ID 管理システムの要件および実装機能を満たすようにシステム機能の詳細パラメータを決定するために利用する。

■留意事項

留意事項	留意内容
パッケージ製品、サービスによる制限	特権 ID 管理システムの仕様やシステムの実装方式によって、連携方式等が制限される可能性がある。 なお、製品やサービスによっては、外部プログラムとの連携用の API やデータの取り込み機能など、カスタマイズ用の機能が存在する場合もある。

■具体的な検討内容

① 製品設計

実装する製品・サービスの仕様に合わせたパラメータを設計する。

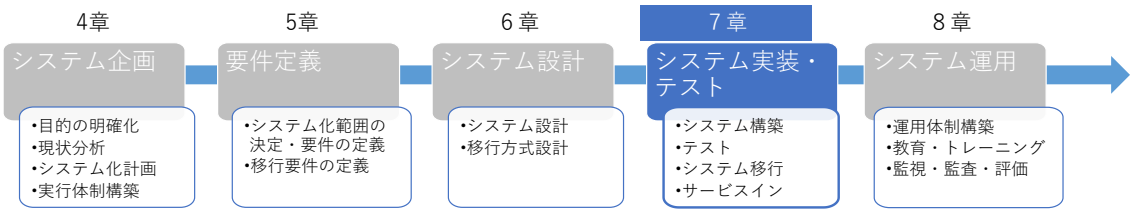
② プログラム開発設計（必要に応じて）

製品が対応していない、特権 ID の管理先が存在する場合や、運用業務におけるログの退避機能などが用意されていない場合など製品機能で充足できない機能要件がある場合はスクリプトや外部プログラムの開発内容について設計する。

■成果物

成果物	内容
詳細設計書	実装対象の製品のパラメータについて記述する。一般的には、利用するミドルウェアやプログラムの構成を含めた設計書として記載する。 ただし、クラウドサービスを利用する場合は設計書ではなく、サービス固有のパラメータシートの作成にとどまるケースもある。

第7章 特権 ID 管理システム実装・テストフェーズ



7.1. システムの実装・テスト

本プロセスの目的は特権 ID 管理システムを実際に構築すると共に、構築した各機能が正しく動作しているかテストを行って担保することである。

本プロセスの前提となるインプット情報はシステム設計フェーズの成果物であり、以下のとおりである。

■必要なインプット情報

インプット情報	利用方法/内容
基本設計書	6.2 特権 ID 管理システムの設計の成果物。システムが持つ機能をどのように実装するのかを機能一覧やシステム構成図の形式で成果物として作成する。
詳細設計書	6.4 詳細設計の成果物。実装すべき製品機能のパラメータの一覧。

■留意事項

留意事項	留意内容
なし	

■具体的な作業内容

①システムの実装

前章で作成した設計書に基づき特権 ID システムを実装する。実装作業の一例としては以下のようなものがある。

・モジュールの導入

・設計書に基づく各種機能設定

・ユーザー/特権 ID 管理の対象システムの登録

・外部連携機能の設定

・タイムサーバーとの時刻同期設定

＜SaaS 型（クラウド型）の場合の追加作業＞

・SaaS 基盤のアカウント払い出し

・管理用コンソールへの認証制御

・SaaS 基盤と管理対象システム間のネットワーク回線設定

なお、開発元よりセキュリティ設定が考慮されたテンプレート等がある場合は、人為的なミスや品質のばらつきを防止のために参考とすることが望ましい。

②テスト項目の策定

テスト項目の策定においては以下のような事項に配慮することが望ましい。以下は特権 ID 管理システムのテスト項目の策定において実施が望ましい観点の一例である。

表 7-1 テスト観点の例

カテゴリ	テスト観点
緊急時の対応を想定する	・特権 ID システムのサービス停止を想定し、緊急時は管理対象のシステムに直接ログインが可能であること ・夜間、休日など承認権限者の不在時に用いる緊急承認（承認の割愛や代理申請の許可）が可能であること。また当該緊急承認履歴について後から検証が可能であること
悪意/ヒューマンエラーによる操作を想定する	・ID を持たないユーザーからのログオンを受け付けないこと ・管理対象システムに対する、特権 ID 管理システムを経由しないログオンを受け付けないこと ・閲覧権限のないユーザーが制限されている情報にアクセスできないこと ・変更権限のないユーザーがシステムの書き換えを実行できないこと ・保存された操作ログについて変更操作を受け付けないこと ・リアルタイム監視機能で禁止操作を設定した場合、当該操作を行った際にセッションの切断や操作の一時停止が行われること ・運用作業の申請履歴と実際の作業内容に乖離があった場合の検出～報告までの運用手順が実施できること
その他、特権 ID 管理システム特有のテスト	・パスワードの自動変更機能を設定した場合、管理対象システムのパスワードが正常に更新されること ・一時的に払い出した特権アカウントについて、設定した有効期間が過ぎたあとに無効化されること

SaaS 型（クラウド型）を利用する場合のテスト	・SaaS 基盤と管理対象システム間の通信が正常に行われていること ・SaaS 基盤とのネットワーク回線に障害が起きた場合の検出が可能であると共に、代替通信経路/手段への切替が可能であること

③テスト環境の準備

テスト環境の準備にあたっては、以下のような事項を留意することが望ましい。

・原則としてテスト環境は本番環境と切り離す

・システムテスト等で既存の ID 管理システム等と連携させる場合、既存アクセス権の上書きなどが起きないよう配慮する

・単体テスト、結合テストで用いるテストデータには実際の職員情報を含む本番データや機密情報を含むデータを用いない。特段の事由により利用する場合は、データの一部をマスキング処理するなどして匿名化加工を実施の上、終了後は確実に消去する

・システムテスト、運用テストなど本番データを用いるテストについては、データの管理部門から使用許可を得るとともに可能な限り社内の要員がテストを実行する。外部ベンダーがテストを行う場合には閲覧可能になる本番データに配慮する

④テストの実施

システム開発 V 字モデル等を参考に工程に応じたテストを実施し、要件や設計書で定めた内容が適切に反映されていることを確認する。テスト工程には以下のような区分がある。

表 7-2　テスト工程ごとの項目例

テスト工程	テスト項目の例
単体テスト	・通信とセッションの確立 ・各サービスの起動、停止、動作確認

	（アカウント/装置管理機能、パスワード管理、操作ログや画面録画の取得と監査、レポーティング機能 など）
結合テスト	・管理端末/操作端末からのログイン ・ワークフローなど画面遷移や申請を伴う機能の動作確認 ・違反操作を行った場合のルールアクション
システムテスト	・統合ログ管理製品へのアラート発報 ・ログのバックアップとリストア ・他システムと連携したユーザー情報の登録、更新
運用テスト／ユーザー受入テスト	・実際の運用を想定したワークフローの実施 ・ユーザーの一部を対象にした先行運用

■成果物

成果物	内容
テスト計画書兼成績書	各工程のテスト項目ならびに実施結果をまとめた資料

7.2. 移行・サービスイン

本プロセスの目的はテストが完了した特権 ID 管理システムを移行させサービスを開始することである。本プロセスの前提となるインプット情報はシステム設計フェーズの成果物であり、以下のとおりである。

■必要なインプット情報

インプット情報	利用方法/内容
移行計画書	5.5 移行の要件定義の成果物

■留意事項

留意事項	留意内容
移行作業の実施日時や環境整備について	移行に際して関連システムに影響が出る場合においては、業務の可用性を確保するために実施日時や環境整備に考慮が必要となる。

■具体的な作業内容

移行においては、システム設計フェーズで作成した移行計画書を実際に実行に移す。計画の変更などがあれば適宜修正を行って作業ミスなどが無いように万全に準備を行う。移行計画書内には以下のような内容を含むことが望ましい。

・移行対象

・移行日時（開始予定時間、終了予定時間）

・移行作業体制（役割分担、連絡先）

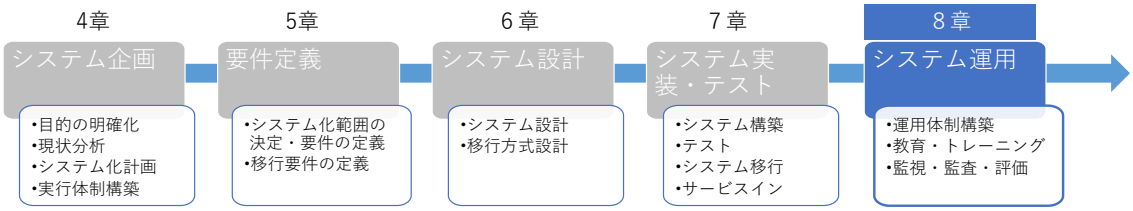
・移行手順

・切り戻し判断箇所と判断基準

■成果物

成果物	内容
移行作業エビデンス	移行作業の操作ログ、画面のハードコピーなど作業証跡

第8章 特権 ID 管理システム運用フェーズ



8.1. 運用設計

事前に定められた手順に則り運用を行うことは、特権 ID を正しく運用するにあたって重要となる。

特権運用の基本プロセスを踏まえたうえで、通常時に加え、非常時の役割と手順についても可能な限り明確化し、特権 ID 管理システムの運用にあたり必要なポリシーを運用設計で規定することが望ましい。

表 8-1 特権 ID 運用に係る基本プロセスは大きく下記の 3 つに大別される。

プロセス	概要	プロセスにおける実施事項
特権 ID 利用プロセス	特権 ID を利用する際の手続き。利用・貸出証跡の取得を行う	● 特権 ID 利用申請・承認 ● 特権 ID 利用
特権 ID 管理システム 運用プロセス	特権 ID 管理システム自体のシステム運用を行う	● 機能追加、ライセンス更新などのシステム運用・保守・トラブルシュート ● 管理対象システム登録 ● 特権 ID 管理システム利用ユーザー登録・削除 ● 特権 ID 利用状況監視

確認・保証プロセス	管理対象 ID、システムの棚卸、および申請に基づく作業実績の確認を行う	● 特権 ID、管理対象システム、および利用ユーザーの棚卸 ● 監査対応 ● 報告

8.1.1. 特権 ID 利用

特権 ID の利用に際して、特権 ID を利用しようとする人は ID の利用申請を行い、申請内容の是非、及び申請者に対し特権 ID を付与することの妥当性を判断できる人員により利用を承認される必要がある。

従って、運用設計では、利用者が利用申請する際の方法と、承認プロセスをあらかじめ定義しておくことが望ましい。

表 8-2 特権 ID の利用申請と承認

プロセス	設計観点	概要
特権 ID 利用申請	利用申請方法	申請時に利用する WF 設計 利用者が申請できる対象システムと対象 ID を設計
特権 ID 利用承認	利用承認方法/承認段階	特権 ID の利用承認における承認者、及び承認段階の設計 申請時の通知手段も含む
緊急申請	緊急申請可否 事後承認取得方法	夜間対応等、承認者不在のユースケースを想定した緊急申請の対応プロセス

8.1.2. 特権 ID 管理システム運用

特権 ID 管理システムは高権限のアカウントを管理するシステムであるため、そのシステム運用についても適切な人員により、適切なプロセスに基づいて実施される必要がある。

表 8-3 特権 ID の利用プロセスと設計観点

プロセス	設計観点	概要
システム運用	バージョン管理 トラブルシュート	特権 ID 管理システムのパッチ適用等、バージョン管理に係る方針 及び、運用時にエラーが発生した場合の問い合わせ先などに係るオペレーション手順の設計
システム利用ユーザー登録	特権 ID 利用を申請可能なユーザー	特権 ID の利用を申請することを許可する利用者を識別し、特権 ID 管理システム上にユーザーとして登録
管理対象システム登録	ターゲットシステム管理アカウント ターゲットシステム個別設定	特権 ID 管理システムでターゲットシステムを管理するにあたり
監視	検知するアクティビティ・コマンドの定義	特権 ID 管理システムで検知し、アラートを上げるべきユーザーのアクティビティや実行コマンドなどを定義する
BCP	特権 ID 管理システムダウン時の対応	特権 ID 管理システムが停止した場合の ID 貸出手順の定義

8.1.3. 確認・保証

特権 ID はシステムやデータへの高いアクセス権を持つため、その使用と管理には厳格な監査が求められる。通常のシステム運用設計と同様に監査計画の策定、基準の設定、データ収集と分析、リスク評価、報告/改善の一連のフローを設計の内、特出すべき点を以下の表に挙げる。

表 8-3 特権 ID の利用確認と保証プロセス

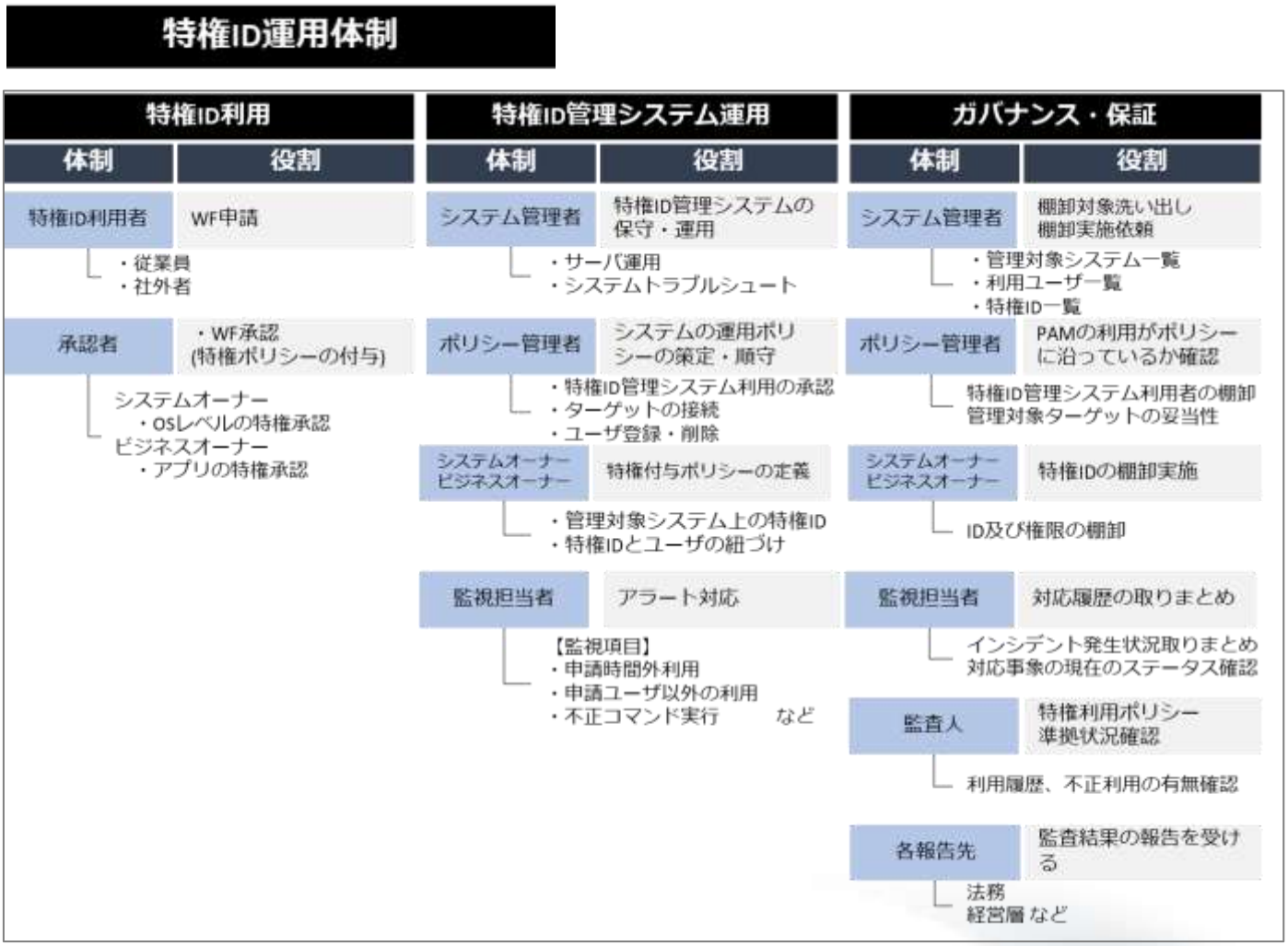
プロセス	設計観点	概要
監査計画の策定	年間計画（頻度と範囲）	対象システム数、利用者数の規模、利用頻度およびリスクレベルを踏まえ策定
監査基準	アクセス制御	最小権限の原則を踏まえたアクセス権の定期的なレビュー
	認証/認可	認証方式の妥当性（多要素認証） セッション管理（時間制限、同時セッション数）の設定有無
	ログ管理	ログの保全方式と保証
監査手法	ツールの利用	自動化ツールの利用
	サンプルチェックまたは全チェック	時間とリソース面を踏まえ設定
対応事項取りまとめ	検知レポート	どのタイミングでどう利用するか
	不正対応履歴	セキュリティ違反が発生した場合の対応プロセスと記録
	エスカレーション	緊急度に応じたコミュニケーションライン

8.2. 特権 ID 管理体制

特権 ID 管理の運用プロセスを担う体制として、プロセスの遂行に必要な役割を明確にし、役割に応じた人員の配置を行う必要がある。

特権 ID 管理の運用プロセスとその遂行に求められる役割を概略化した図が下記の通りである。実際の導入に当たっては、組織の既存体制や業務プロセスに応じて、体制の細分化や兼務が適宜発生する。

図 8-1 特権ＩＤ運用体制図の例



8.2.1. 特権 ID 利用プロセス

特権 ID を人が利用する際のプロセスは、対象の特権 ID の特性により 2 パターン想定される。

① ビルトインの特権 ID 利用

Administrator や root など、ビルトインされている特権 ID を利用するパターン。特権 ID 管理システム上で当該 ID の管理を行っているため、利用者は承認者に対し、一時的なアカウントの貸し出しを申請する。

② 一時的な高権限 ID 利用

ビルトインの特権 ID が、組織のポリシーで無効化されていたり、利用が禁止されている場合に、特定の権限を有する ID を一時的に作成し、貸与するパターン。利用者は作業に必要な権限を有する一時 ID の作成を申請する。

- **特権 ID 利用者**

利用者は特権 ID の各利用パターンにおいて、下記の内容について利用申請を行う。

①ビルトインの特権 ID 利用

利用対象システム、貸出対象 ID、貸出目的、貸出期間

②一時的な高権限 ID 利用

利用対象システム、利用目的、必要な権限、利用期間限

- **承認者**

承認者は、各利用パターンに応じて、下記の観点で申請内容を確認し、承認の可否について判断する

①ビルトインの特権 ID 利用

・特権 ID を貸出して問題ない人物か

・特権 ID が無ければ実施できない作業内容か

・貸出期間は適切か(作業内容に照らし過剰、過小申請ではないか)

②一時的な高権限 ID 利用

・特権 ID を貸出して問題ない人物か

・申請された権限は申告のあった作業内容に照らして妥当か

・貸出期間は適切か

8.2.2. 特権 ID 管理システム運用プロセス

特権 ID 管理を適切に実施するためには、導入した特権 ID 管理システムが適切に運用される必要がある。特権 ID 管理システムの管理者・運用者のアクターと役割は下記の通りである。

- **システム管理者**

  特権 ID 管理システムのシステム運用を行う。ライセンス更新やシステム障害発生時のトラブルシュートに加え、特権 ID 管理システム停止時の ID およびパスワードの手動貸し出し等、BCP 対応を含むシステム運用全般の管理を担う。

- **ポリシー管理者**

  組織の ID 管理ポリシーに照らし、特権 ID 管理システムの運用ポリシーの準拠対応を行う。具体的には、特権 ID の利用申請を行うことを特定のユーザーに認めるかどうかの判断や、当該ユーザーの特権 ID 管理システムへアクセスするためのアカウント登録・削除手続きを行う。

  同様に、管理対象システムについても、ポリシー管理者が管理対象とするかどうかについて判断し、管理対象とするシステムについては、システムオーナーと連携の特権 ID 管理システムと対象システムとの接続手続きを行う。

- **システムオーナー/ビジネスオーナー**

  管理対象システム上の特権の定義を行う。

特権と定義された ID は、対象のシステムが特権 ID 管理システムで管理される際、特に貸出利用時に申請・承認利用の対象として扱われることになる。
また、ビジネスオーナーは、システム上の特権 ID とユーザーとの紐づけを行うことで、ユーザーが ID 貸出申請時に申請対象として選択できる ID の絞り込みを行う。

- **監視担当者**

  監視担当者は、特権 ID の利用に際する挙動の監視を行う。
  特権 ID 管理システムが具備する基本的な監視項目として、特権 ID 利用時の入力コマンド監視、管理対象システム上の認証ログ収集、特権 ID 利用時の操作画面の録画などがある。必要に応じ、ログは SIEM 等と連携し、より詳細な監視体制を構築する。
  監視担当者は、不審なアクティビティや申請外の特権 ID 利用が検出された際、当該アカウントの利用を停止し、ユーザーに利用状況や利用目的のヒアリング、必要に応じて影響範囲等を調査し、組織で規定された報告先へ事象の連絡を行う。

8.2.3. ガバナンス/保証プロセス

特権 ID に係る運用が正しく実施されていることを保証するために、特権 ID 管理に係る確認と保証を行うプロセスを実施する。ID・権限の棚卸作業が中心となるが、異常検知履歴がある場合については、その対応状況及びクロージング等が求められる。

- **システム管理者**

  システム管理者は、棚卸作業に当たり、ID およびアカウント・権限や管理対象システムの一覧を出力する。これらの情報は、それ自体が気密性の高いものであるため、一覧の出力権限は特定の管理者に限定される必要がある。

- **ポリシー管理者**

  特権 ID 管理システムに登録されているユーザー情報、及び管理対象システムの棚卸を行う。特権 ID 利用の申請が許可された利用者のみユーザー登録されているかという観点で確認を行う。

- **システムオーナー/ビジネスオーナー**

  管理対象システムの管理者であるシステムオーナー/ビジネスオーナーは、特権アカウント、及び権限の棚卸を行う。IT 管理者であるシステムオーナーは不正に権限操作が行われていないかを確認し、ビジネスオーナーは過剰/過小なアカウント・権限の有無を確認する。

- **監視担当者**

  監視担当者は、対応した検出項目の履歴取りまとめを行う。対応ケースの事象概要、発生日時、ヒアリング対象者、現在の対応状況等について記録する。

- **監査人**

  棚卸実施結果を踏まえ特権 ID 管理のプロセスが正常に運用されていることの確認を内外の監査を通じて行う。

8.3. 教育・トレーニング

特権 ID 管理の目的を達成するには、特権 ID 運用体制に関わる関係者に対し、次の点の教育・トレーニングが不可欠である。

- 特権 ID 管理の目的の理解
- 特権 ID 管理システムの利用法のトレーニング
- 緊急時対応手順

8.3.1. 特権 ID 管理の目的の理解

特権 ID は通常のユーザーアカウントより広範なアクセス権限を持っていることより、使い方を誤ると組織やシステムに甚大な影響を与える可能性がある。そのため特権 ID の利用を厳重に管理し、不正アクセスや悪用、誤操作などのリスクから保護する必要がある。特権 ID 管理システムを導入することにより、特権 ID のアクセスが正確に管理され誰がいつどのシステムにアクセスしたかトレースすることが可能になり、コンプライアンスの確保、セキュリティ侵害やその他のインシデントが発生した場合の調査や原因究明に役立ち、さらには特権 ID の利用者の保護にもつながる。組織の特権 ID 管理にまつわる関係者に対して、特権 ID 管理の目的の理解を促す教育が必要となる。

8.3.2. 特権 ID 管理システムの利用法のトレーニング

特権 ID 管理システムにまつわる関係者の教育内容について、対象者別に教育内容を次に示す。

表 8-3 特権 ID 管理システムの教育内容

対象者	教育内容
特権 ID 利用者 （ベンダー/パートナー）	・特権 ID 管理システムの使い方：WF 申請、承認後のアクセス方法
承認者 （ビジネスオーナー） （システムオーナー）	・特権 ID 管理システムの使い方：WF 承認方法、棚卸実施方法 ・承認時における判断基準/確認事項 ・組織に規定された特権 ID 管理ポリシー（設定されているアクセスポリシーやロールポリシーの理解）
特権 ID 管理システム管理者	・特権 ID 管理システムの製品理解：トラブルシューティング、ライセンス体系 ・特権 ID 管理システムに対する侵害時の対応

特権 ID 管理システムポリシー管理者	・特権 ID 管理システムの機能理解：特権 ID 管理システムの機能と組織のポリシーの差分の把握
監視担当者	・特権 ID 管理システムの使い方：ログ、アラートの確認方法、監査報告事項のとりまとめ方法
監査人	・組織に規定された特権 ID 管理ポリシーの理解

導入する特権 ID 管理システムの製品による特徴・特性を踏まえシステム的な制御とその限界、一方で抑止のための仕組み、利用者のモラルや倫理に関する教育も必要である（やれること≠やって良いことではないこと）。

8.3.3. 緊急時対応手順

ターゲットシステムのセキュリティ侵害やシステム障害時、特権 ID 管理システム自体の障害時など、緊急時の対応手順についての整備と教育が求められる。特権 ID を利用する場面として定期的な運用やあらかじめ計画された作業に加え、緊急対応のための利用が一定の割合で発生することが考えられる。そのため、特権 ID 利用時に承認者がつかまらないなどの状況で承認フローがまわらない場合、どのような代替手順を踏めば目的を達成できるか理解しておく必要がある。また特権 ID 管理システム自体の障害時も同様に、アクセス制御や証跡の記録が不十分になる可能性がある場合の手順と後日それらを補完するための操作・作業についても把握しておく必要がある。

8.4. 監視・監査・レポーティング

8.4.1. 監視

特権 ID 管理の運用においては、申請内容に沿った特権 ID の利用が行われているかを常時監視し、承認された利用から逸脱した場合には、運用者やシステムオーナー等、適切な人員に通知する必要がある。主な監視項目としては下記のようなものが挙げられる。

表 8-4 特権 ID 管理システムの監視

監視機能	概要
操作画面録画	➢ 特権アカウント利用時の操作画面を動画で記録 ➢ 取得した動画へのアクセス権は監査権限を有するユーザーに制限
実行コマンド監視	➢ ユーザー毎に利用可能なコマンドを制御。特定のコマンドが実行された際にアラートを発出
ログ監視	➢ 管理対象システム上のログを収集し、不正なアクセス、アクティビティを検知し、アラートを発出 ➢ 特権 ID 管理システムのログ収集

8.4.2. 監査・レポーティング

特権 ID 管理に係るレポートは、運用者が日次で正常性確認を行うことを目的としたものと、年に一、二回程度、定期的に実施する監査を目的としたものの 2 つに大別される。

正常性確認を目的としたレポートでは、申請内容と利用実績の突合せを行い、申請外の作業が行われていないかの確認を行う。

監査を目的としたレポートでは、特権 ID 管理システムの管理対象となっている ID やシステムの一覧を出力し、不要な ID や権限の有無、及びシステムの適切な管理が行われているかを確認する。

これらの目的に沿うレポートとして下記のものが挙げられる。

表 8-4 特権 ID 管理システムのレポート種別

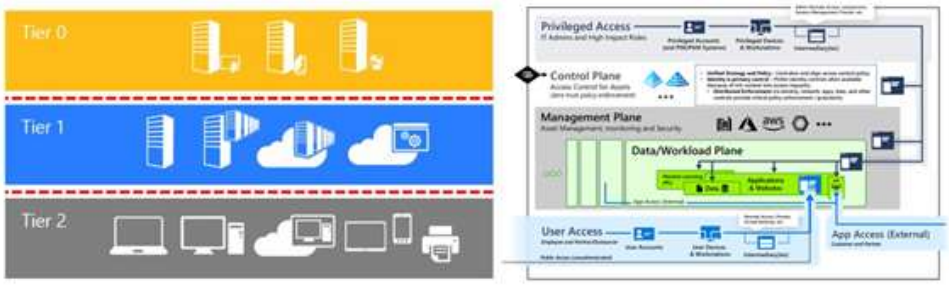
レポート種別	概要
利用実績突合せ(日次)	特権 ID の利用は基本的に ID 貸出であるため、承認を受けた期間に、承認の範囲内の利用を実施していることを確認する。 【確認事項】 ➢ 承認期間外の利用有無 ➢ 承認内容以外の操作履歴の有無
アクセス履歴(日次)	特権 ID 管理システムを経由しない不正アクセスが施行されていないかを確認するため、管理対象システムへのアクセス履歴を確認する。また、特権 ID 管理システムへのアクセス 【確認事項】 ➢ 複数回のログイン失敗履歴の有無
棚卸(定期)	特権 ID 管理システム上の登録情報、管理情報が、実態と乖離していないかを確認する。 【棚卸に用いるレポート例】 ➢ 管理対象システムリスト ➢ 特権 ID(管理対象 ID)リスト ➢ アカウントに紐づく権限一覧 ➢ 特権 ID システム利用ユーザーの一覧 ➢ 管理対象システム上の ID と特権 ID 管理システム上の ID の差分リスト

コラム

～アイデンティティベースの攻撃の紹介～

サイバー攻撃において、初期侵入を成功させた攻撃者は内部侵害を行うために権限昇格やラテラルムーブメントといった戦術をとる。具体的な攻撃手法として脆弱性を狙ったエクスプロイトを行うこともあるが、多くの組織で利用されている Active Directory 環境においては、アイデンティティベースの攻撃を連鎖させることで効果的に目的を達成する。このアイデンティティベースの攻撃の連鎖を Attack Path や Identity Snowball Attacks と呼ぶ。

一般権限でのリモートアクセスを可能とした攻撃者は、ネットワーク全体の掌握のために特権の取得を試みる。特権に代表される重要資産のうち、最も守られるべき資産はセキュリティ保護モデルである管理階層モデル（Administrative Tier Model）において Tier 0 に位置する。現在は、管理階層モデルに代わって、エンタープライズアクセスモデル（Enterprise Access Model）が活用されている。管理階層モデルでの Tier 0 は、エンタープライズアクセスモデルでの Privileged Access および Control and Management Planes 領域に拡張したとみることが出来る。ここでは、シンプルに考えるためにエンタープライズアクセスモデルでの Privileged Access および Control and Management Planes 領域も含めて Tier 0 と見なすことにする。



管理階層モデルとエンタープライズアクセスモデル

Active Directory 環境において、Tier 0 に位置するアセットの一例としては、以下のようなアセットがある。

・Domain Admins
・Enterprise Admins
・Backup Operators
・krbtgt
・Schema Admins
・AdminSDHolder

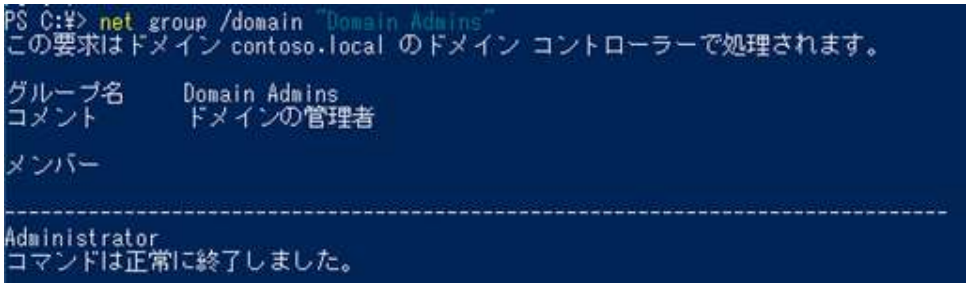
初期侵入の成功によって一般権限である Domain Users の権限を持った攻撃者が、Tier 0 の一つである Domain Admins に昇格するシンプルな Attack Path の例を見ていく。

侵害された想定のアカウントである victimuser1 の情報を確認すると、一般権限のユーザグループである Domain Users グループと Group2 というグループに所属していることが分かる。

net user /domain victimuser1 のコマンド結果 (一部)

この時点で Group2 グループの詳細は不明ではあるものの、Domain Users グループに所属しているということから victimuser1 は高権限を所有していない低権限のアカウントであると判断される。

また、Tier 0 アセットである Domain Admins グループに所属するユーザーの情報を確認すると、Administrator のみが Domain Admins グループに所属していることを示す結果が表示される。



net group /domain "Domain Admins" のコマンド結果 (一部)

ここまでの偵察結果からは、victimuser1 が高権限を有していること示唆する情報は得られていない。続いて、victimuser1 が所属している Group2 グループについて確認していく。

Group2 のプロパティ

Group2 はさらに別のグループである Group1 に所属していることが分かる。同様に Group1 について確認すると、Group1 は Domain Admins に所属していることが判明する。

Group2 のプロパティ

victimuser1 は Domain Admins の直接的なメンバーではないものの、Group1 と Group2 を介して間接的に Domain Admins のメンバーであると考えることができる。

グループメンバーの間接的な関係性

victimuser1 が実際に Domain Admins のメンバーと同等の権限を持っていることを確認するために、ドメインコントローラーにアクセスを行う。低権限の Domain Users のアカウントではドメインコントローラーにログインできないが、間接的な Domain Admins のメンバーである victimuser1 は PsExec を用いてログインできることが分かる。

```
PS C:¥> .¥PsExec64.exe -accepteula ¥¥192.168.0.100 -u contoso¥victimuser1 -p 1qazxcvbnm,./¥ -i cmd

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 10.0.17763.1098]
(c) 2018 Microsoft Corporation. All rights reserved.

C:¥Windows¥system32>hostname && whoami
DC-01
contoso¥victimuser1
```

PsExec を用いたドメインコントローラーへのアクセス

このような間接的な Domain Admins のメンバーを把握するための手法の一つとして、LDAP プロトコルを用いて、Domain Admins のメンバーを再帰的に列挙する方法がある。

```
PS C:¥> Get-AdObject -ldapfilter "(&(objectClass=user)(memberof:1.2.840.113556.1.4.1941:=CN=Domain Admins,CN=Users
,DC=CONTOSO,DC=LOCAL))"

DistinguishedName                          Name          ObjectClass ObjectGUID
-----------------                          ----          ----------- ----------
CN=Administrator,CN=Users,DC=contoso,DC=local Administrator user        28eefad9-b4ab-4626-8556-fa838613d8c1
CN=victimuser1,CN=Users,DC=contoso,DC=local   victimuser1   user        732d11dc-737d-4132-8dcf-ef4f81c2b293
```

Domain Admins メンバーの再帰的列挙

本コラムでは、Active Directory 環境を侵害する攻撃者が、一般権限から特権である Domain Admins に昇格する Attack Path について最もシンプルな例でご紹介をした。実際のエンタープライズ環境では、より複雑なアカウント・権限の関係性が長年の運用によって構成されていることが考えられる。攻撃者は常にアイデンティティベースの攻撃を連鎖させ目的を達成することを狙っている。

以上

あとがき

本書の執筆にあたっては以下のメンバーにご尽力をいただいた。

この場をお借りして謝辞を申し上げる。

【検討・執筆メンバー】

宮川　晃一（WG リーダー）	日本電気株式会社
大竹　章裕	株式会社ラック
斎藤　知明	TIS 株式会社
松井　祐輔	日本電気株式会社
吉本　紀浩	デロイトトーマツサイバー合同会社
石崎　貴嗣	デロイトトーマツサイバー合同会社
金子　敬祐	SCSK 株式会社
内田　健一	NEC ソリューションイノベータ株式会社
番井　孝之	NEC ソリューションイノベータ株式会社
毛利　幹宏	株式会社アシスト
伊藤南美子	株式会社富士通エフサス
河原林　広	株式会社富士通エフサス

（順序不同）

なお、本 WG の活動内容およびメンバーは以下の紹介ページを参照いただきたい。

【デジタルアイデンティティ WG 紹介ページ】

https://www.jnsa.org/active/std_idm.html