特権ID管理ツール「SecureCube Access Check」徹底解説セミナー

特権ID管理の重要性と導入ポイント

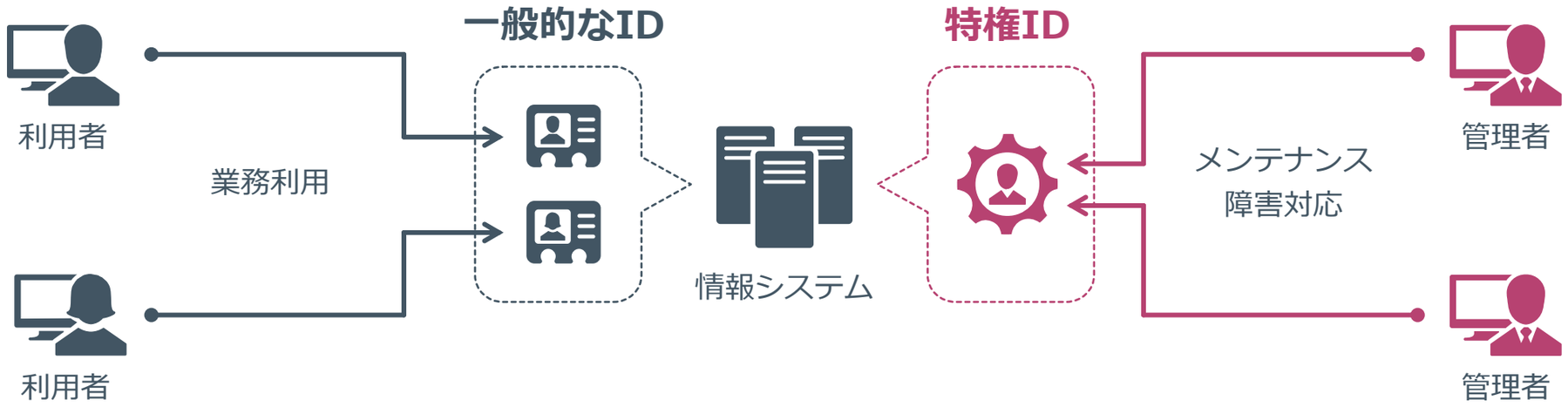
NRIセキュアテクノロジーズ株式会社
セキュリティソリューション事業本部
統制ソリューション事業部

目　次

目　次

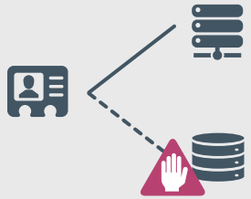
特権IDとは

システムの維持・管理のために用意された、極めて強い操作権限を持つ特別なID

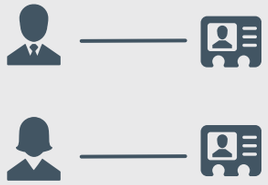


一般的なIDの特徴

限定的な権限



個人ごとに1ID



特権IDの特徴

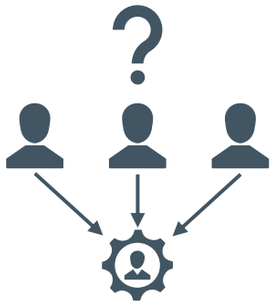
絶対的な権限

1IDを共有

特権IDの不適切な管理に潜むリスク

特権IDの絶対的な権限を持ち、共有して利用されることが多いという特徴から、次のようなリスクに備える必要がある

代表的なリスク

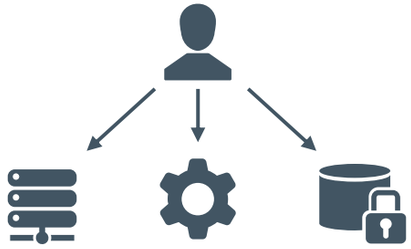


特権IDの利用者を特定するのが困難

- 複数ユーザーの共有利用により、**誰がそのIDを使い不正操作したか判別できない**
- 共有であること、作業者の特定が困難なことにより、**不正操作を行う心理的ハードルも下がる**

特権IDを利用した作業内容を改ざん可能

- 特権IDは高権限であることから、システムのログにもアクセスでき、不正操作した後、**操作の証跡を消すことも容易**
- 問題が発生しても、影響調査が困難になる恐れがある



実際の作業に不必要な権限での操作が可能

- 利便性の高さから特権IDを多用することで、**本来の権限以上の操作が行えてしまう**
- **操作ミスによる影響範囲が広く**なる
- 内部不正による情報漏えいの経路に利用される脅威が増す

特権IDを悪用された場合の影響

- サイバー攻撃や内部不正では、高権限を持つ特権IDが狙われる
- 特権IDを悪用されると信用の失墜や顧客離れ等の大きな被害につながる

データの盗難
・情報漏えい

データの改ざん
・破壊・消去

システムダウン
・サービス停止

さらなる攻撃
の踏み台化

ビジネス活動への悪影響
＝企業・組織へのダメージ

損害賠償・
対策費用発生

信用の失墜

顧客離れ
従業員離れ

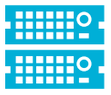
特権IDを取り巻く環境の変化｜特権IDの多様化

昨今のクラウド利用やシステム間連携の拡大により、「特権ID」として管理するべき範囲が広がり、その数は膨大になっている

従来の特権ID

WindowsやLinux等のサーバに存在する高権限ID
例）　Administrator, root

重要情報を含むデータベースへアクセス可能なID
例）　Oracle sys, SQL Server sa



ネットワーク機器等の設定・運用を行うためのID

DX時代における特権ID

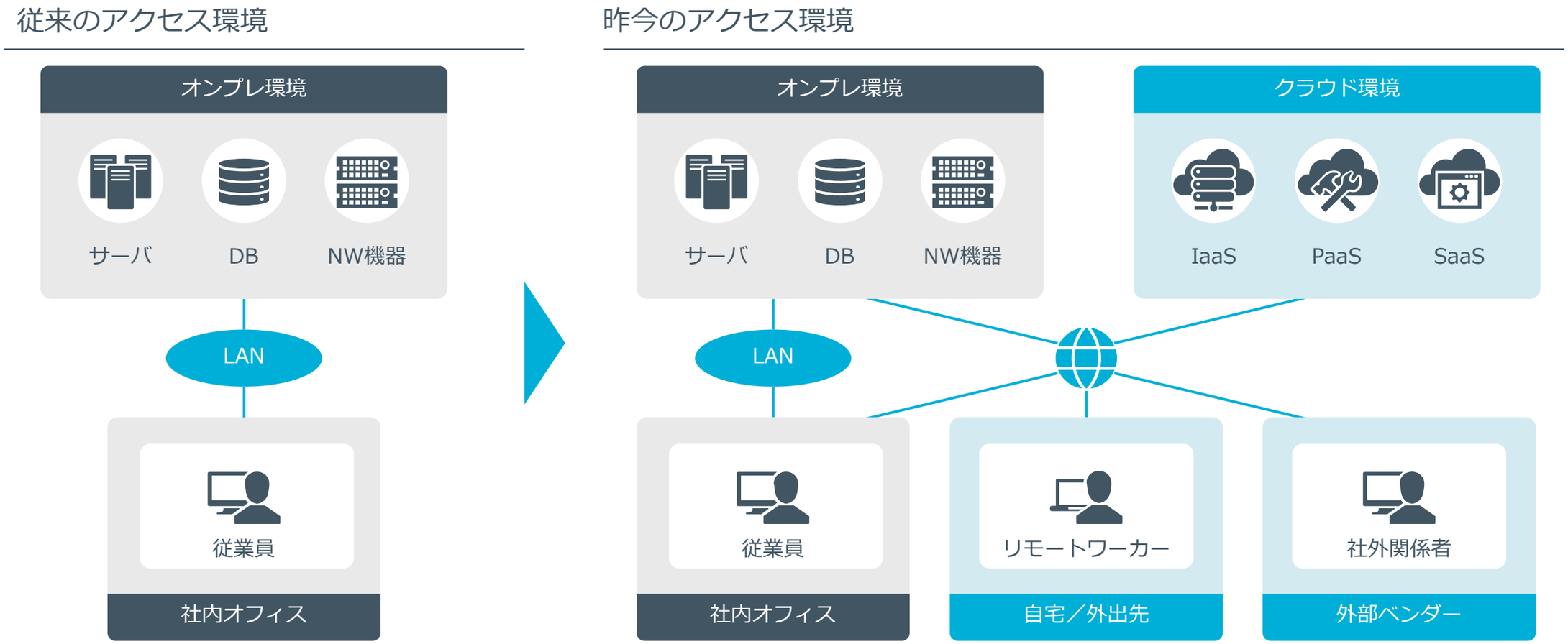
クラウド利用の機会が増え、IaaS、SaaSの管理が可能なアカウントや、その他業務上必要となるサービスの管理アカウントも 特権 として管理するべき

AWS、AzureなどのIaaS管理者アカウント
例）　AWS IAMアカウント

Microsoft365、SalesforceなどのSaaS管理者アカウント
例）　Microsoft365 管理者アカウント
Salesforce システム管理者

特権IDを取り巻く環境の変化｜アクセス環境の多様化

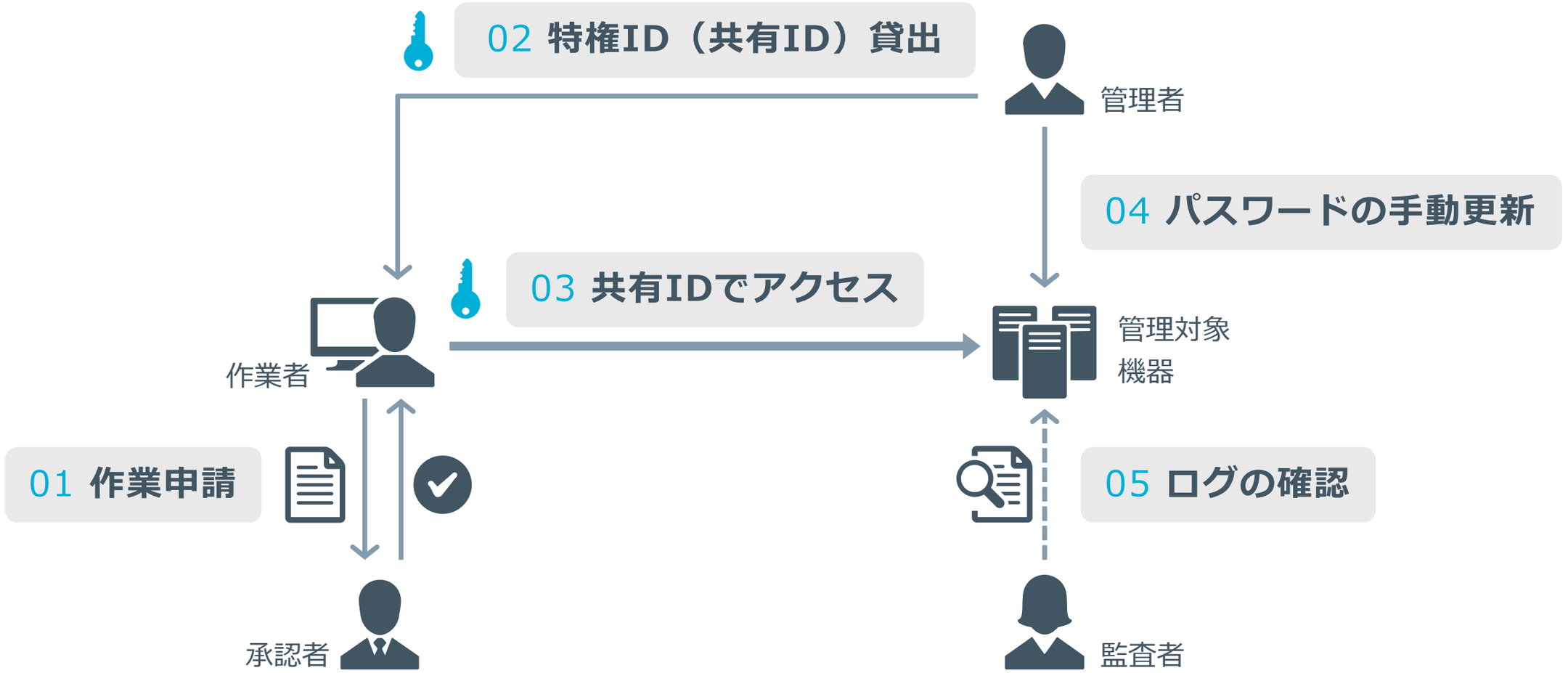
- クラウド活用が進むことで、自宅や外出先、外部ベンダーからのリモートアクセスが増加
- ゼロトラストへと変化する中で、アクセス管理・ID管理の重要性はますます高まる



目　次

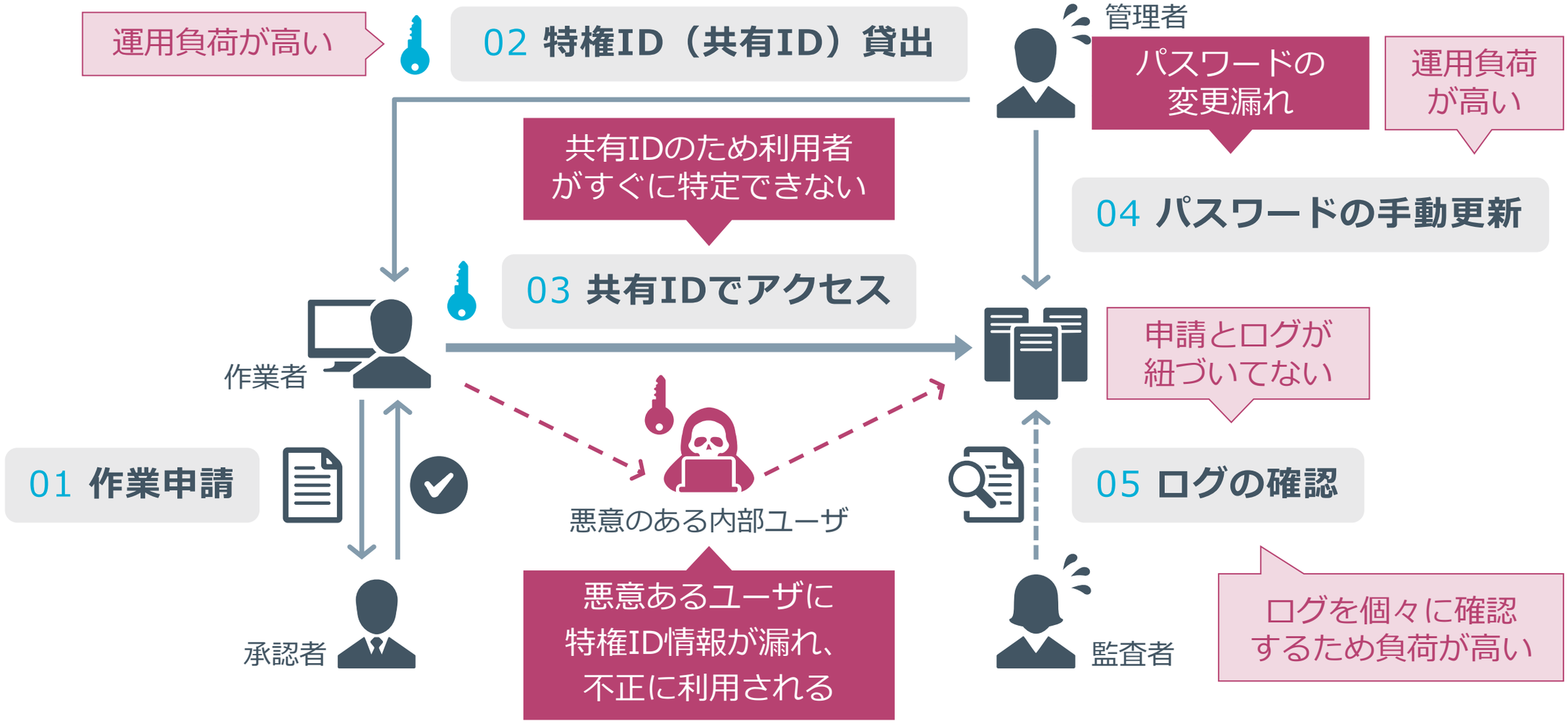
特権IDを手運用で管理するイメージ

利用の都度、特権IDを貸し出す運用をすることで、最低限の管理は可能



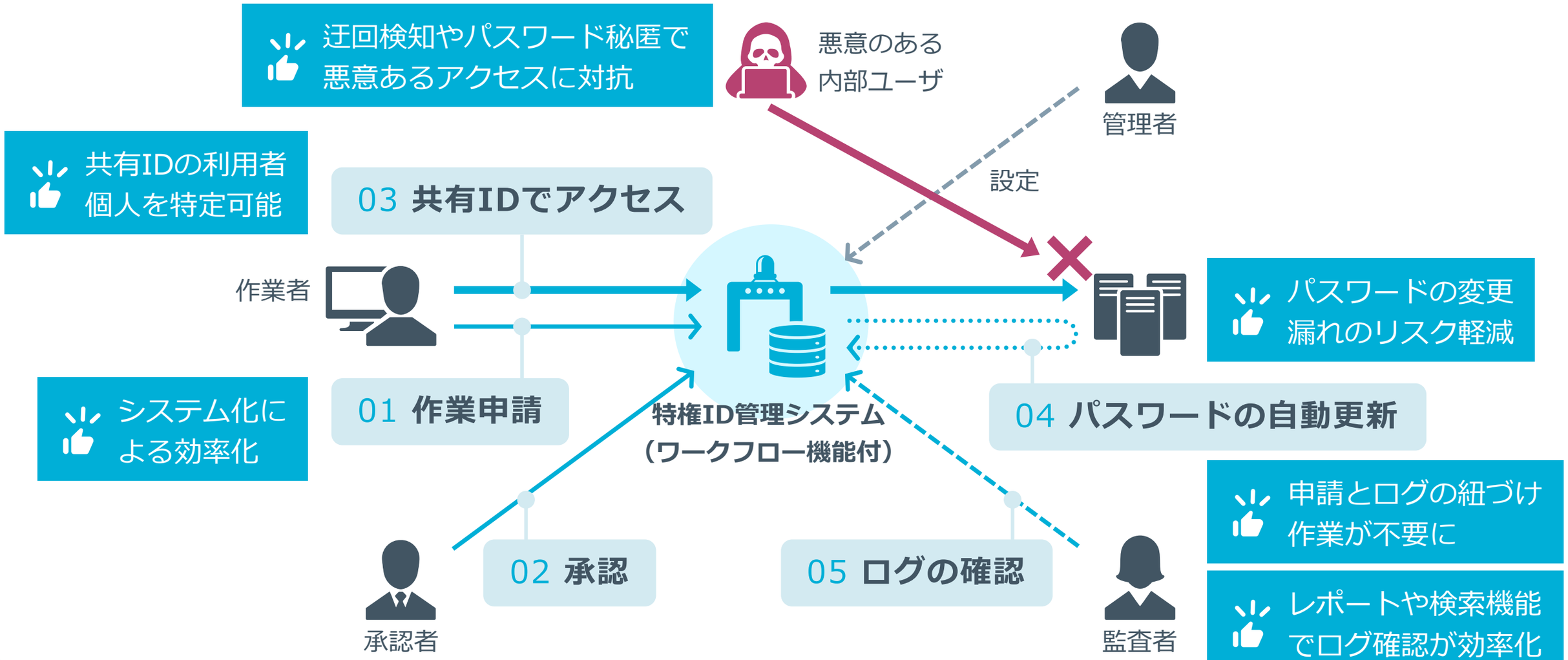
特権IDを手運用で管理する場合のリスクや課題

手運用の場合、様々なセキュリティリスクが残り、運用負荷も高くなる



特権ID管理ソリューションを導入した場合のイメージ

ソリューションを活用することで手運用の場合に発生する課題を解決



特権ID管理ソリューションの導入効果

特権ID管理ソリューション活用により、手運用における課題の解決だけでなく、更なるセキュリティ強化や利便性の向上が可能

特権ID管理ソリューションの活用

手運用における課題の解決

セキュリティ強化

認証強化	二要素認証による認証強化
不正操作検知	キーワードによる検知等、不正操作の早期検知や遮断
証跡管理	● 動画形式やテキスト形式で操作ログを取得 ● ログの改ざん検知や暗号化

利便性の向上

緊急アクセス	● 緊急時には事後承認でアクセス ● 事後承認でも操作記録は取得
申請・承認	● 定期的な作業は定期利用申請 ● グループメンバによる効率的な承認
IDの可視化	管理対象機器のID情報収集（ID棚卸）と管理状況の可視化

手運用とソリューション利用の比較

法令基準への素早い対応、特権IDやアクセス環境の多様化を考慮すると、ソリューション利用がおすすめ

おすすめ

	手運用	ソリューション利用
コスト	△ ● ソリューション**導入や維持の費用がかからない** ● 手運用のため、**運用工数（コスト）がかかる**	△ ● ソリューション**導入や維持の費用がかかる** ● システム化により、**運用工数（コスト）が削減できる**
セキュリティ	× ● 作業ミス、作業漏れが**発生しやすい** ● 不正行為が**発生しやすい** ● インシデント発生時の対応に**時間がかかる**	◎ ● 作業ミス、作業漏れが**発生しにくい** ● 不正行為の実施**ハードルがあがる** ● インシデント発生時の対応を**迅速に行える**

目　次

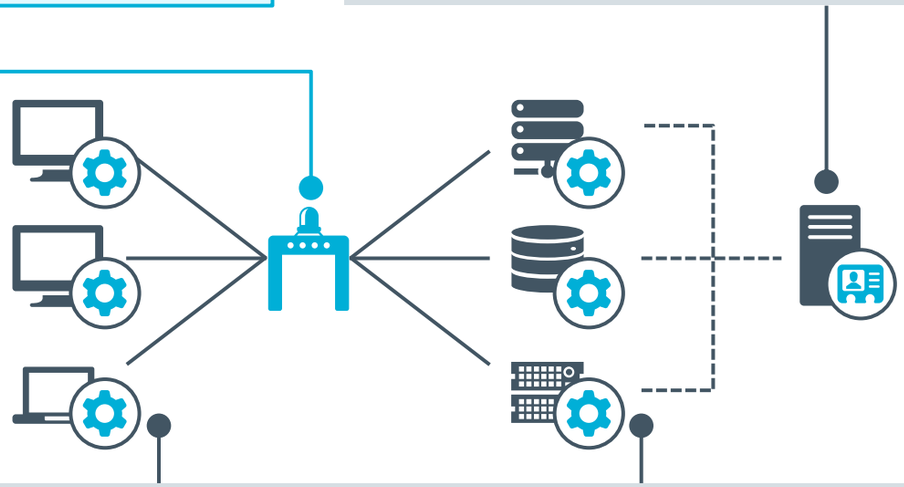
特権ID管理ソリューションの代表的な制御方式

ゲートウェイ方式（完全エージェントレス型）

クライアント端末と管理対象機器の間に関所（ゲートウェイ）を設置して、一元管理する方式。関所上で、個人ID管理、アクセス制御、及びログ管理を統合するため構成がシンプル。**管理対象機器が多い場合や、既存環境への影響を最小限にしたい場合**などに最適。

ID・パスワード貸出方式

管理対象機器の特権ID棚卸とパスワード貸出管理で制御する方式。
アクセス制御用にクライアントエージェントを必要としたり、認証用サーバを別途立てたりする必要がある。**特権IDが少ない場合や、統合ID管理システムが稼動済みの場合**などに最適。



エージェント方式

クライアント・エージェント型

アクセス元のクライアント端末ごとにエージェントをインストールする方式。
クライアントごとで、本人認証（特権ID利用者の特定）とログ取得を行う。**ログを詳細に取得したい場合や、管理対象機器への接続用端末が特定されている場合**などに最適。

サーバ・エージェント型

アクセス先の管理対象機器ごとにエージェントをインストールする方式。
管理対象機器ごとに個人ID管理、操作制御、ログ取得を行う。**物理コンソールでの接続を含めたアクセス制御とログを取得したい場合や、管理対象機器側で詳細な操作制御を行いたい場合**に最適。

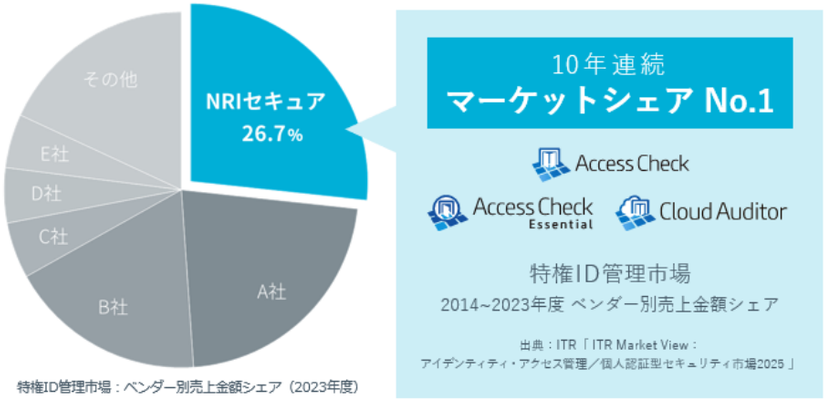
特権ID管理ソリューション選定のポイント

セキュリティへの素早い対応を考慮すると、「導入のしやすさ」も重要なポイントとなるため、「ゲートウェイ方式」がおすすめ

比較項目	システム導入	システム運用	アクセス制御	ログ取得
おすすめ **ゲートウェイ方式**	◎ エージェントレスのため導入が容易	◎ 拡張性に優れ、システム構成がシンプルなため運用が容易	○ ゲートウェイでアクセス制御可能、迂回アクセス対策が必要	○ エージェントレスで取得可能
サーバ・エージェント型	△ 各サーバへの導入影響がないか調査・検証が必須	△ メンテナンスごとに影響の調査・検証が必須	◎ ローカルログインを含めたきめ細かい制御が可能	◎ ローカルログインを含めたログの取得が可能
クライアント・エージェント型	○ 各クライアントへの導入影響がないか調査・検証が必須	△ アクセス制御とログ取得は別製品が必要となり、運用が煩雑	○ エージェント未導入の端末からのアクセス対策が必要	○ エージェント未導入の端末からのアクセスログは取得できない
ID棚卸・貸出方式	△ ID・パスワードの棚卸が必須 パスワード変更できないIDは別対策が必要	○ ID・パスワードの管理（定期棚卸など）が必須、パスワード変更できないIDは別管理	○ パスワード変更できないIDの対策が必要	△ ID貸出・利用のログは取得できるが、操作内容の取得のためには別の仕組みが必要

特権ID管理ソリューション「SecureCube Access Check」の概要

特権ID管理に必要な機能をすべて備えた オールインワンソリューション



特権ID管理市場：ベンダー別売上金額シェア（2023年度）

様々な業種のお客様の課題を解決

idemitsu / ONE COMPATH / KDDI / TOWER RECORDS / IIJ / CTC / TOKYU CARD / JEOL / 東計電算 / ベネッセコーポレーション / SoftBank

一部抜粋・順不同

販売代理店

CTC / TIS INTEC Group / Marubeni IT Solutions / Hewlett Packard Enterprise / IIJ / Computer Science Corporation / GRCS

一部抜粋・順不同

NRI SECURE