第2回データベース・セキュリティ・コンソーシアム セミナー

ORACLE®

内部統制時代のデータベース・セキュリティ

日本オラクル株式会社
システム製品統括本部　北野晴人
2006年11月7日

以下の事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。以下の事項は、マテリアルやコード、機能を提供することをコミットメント（確約）するものではないため、購買決定を行う際の判断材料になさらないで下さい。オラクル製品に関して記載されている機能の開発、リリースおよび時期については、弊社の裁量により決定されます。

財務諸表・IT業務処理統制・IT全般統制

IT業務処理統制
- 網羅性
- 正確性
- 妥当性
- 承認
- 職務の分離

IT全般統制
- プログラム開発
- プログラム変更
- コンピュータ運用
- プログラムとデータへのアクセス管理
- 統制環境

データベース・セキュリティに求められるもの

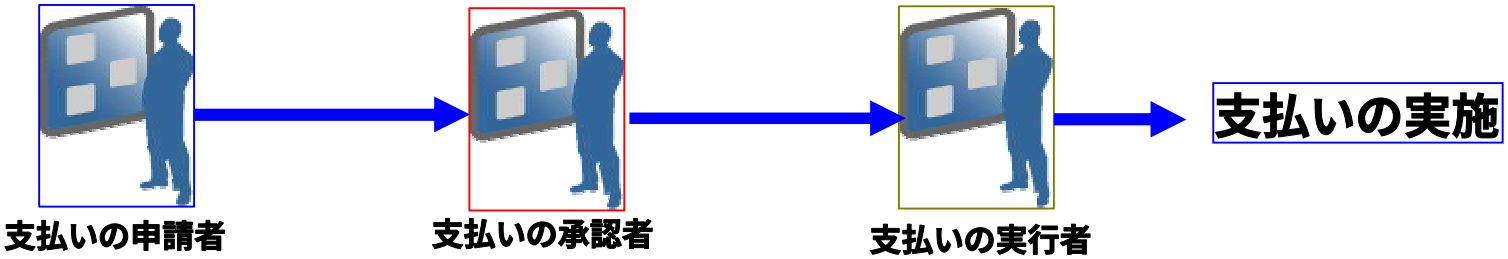
- IT全般統制の中で「情報の正しさ」を保証することで業務処理統制上の統制活動の正当性を担保しなければならない。
  - 業務アプリケーションにおける統制活動が有効に機能することをインフラ側で保証する必要がある。
  - 全てのセキュリティ対策はこの点に貢献している。

- 「情報が正しい」という証明ができなければならない。
  - 情報にかかわる変更履歴の保持と保全が必要となる。
  - データベースの管理操作についても履歴が必要になる。
  - 権限の付与プロセスについても統制と履歴の保持が必要になる。

ORACLE

①情報の正しさを保証する　-職務分掌-

- 一般的な職務分掌（予防的統制）
  - 職務を分離し相互監視、ダブルチェックの仕組みをつくる。
    （例：支払いの実行者と承認者を分離する）



- データベースにおける職務分掌
  - データベース管理者と開発者・一般ユーザ
  - 利用できる権限・操作と職務の一致

職務分掌＝データベース内での最小権限

①情報の正しさを保証する　-職務分掌-

- 最小権限を実現できる設計と実装が必要。
  - スキーマ構造の検討
  - オブジェクトに対するアクセス権限（DML)の最小化
  - ビュー、その他を利用したアクセスコントロール
  - 管理操作（DDL文など）の最小化
- データベース管理者（DBA)に対する抑止策を実装する。
  - 仮想的に分割して管理者を分離するデータベース
  - 管理者権限を制限できるデータベースの利用（事実上のデュアルロック機能が必要）

※デュアルロック：「政府機関の情報セキュリティ対策のための統一基準」にある強化遵守事項の一つ

職務分掌の観点からはDBAが課題

DBAが本来すべき作業

- **運用**
  - バックアップ、リカバリ
  - インスタンス管理
    起動、停止、
  - Table Space、
    データファイルの拡大
- **チューニング作業**
  - SGAメモリのサイズ変更、
  - Redoログバッファのサイズ調整

DBAができてしまう作業

- **データの盗み見、不正持出し**
  - 全従業員の給料、個人情報
  - 決算発表前の会計データ
  - 全顧客データ
- **不正なコマンド発行**
  - 全ビジネスデータの削除、
  - 不当なデータのUpdate
  - アプリケーションへの
    不要なユーザーの作成

職務分掌の観点からはDBAが課題

DBAが本来やるべき作業

- 運用
  - バックアップ、リカバリ
  - インスタンス管理
    起動、停止、
  -
- チュー
  SGAメモリのサイズ変更

DBAができてしまう作業

不正持出し

- 全従業員の給料、個人情報
- 決算発表前の会計データ
- 会員客データ

の削除、

データベース利用者

明確な職務分掌が必要

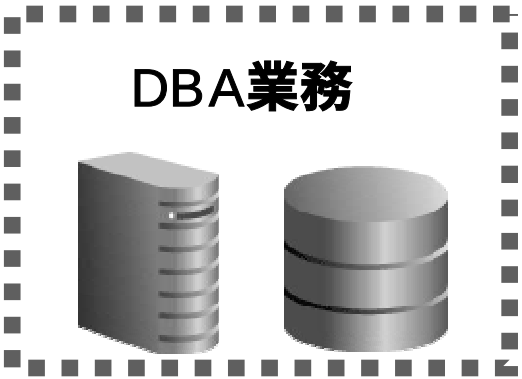
データベース管理者

- ✓ 内部統制上、「データベース利用者」と「データベース管理者」は明確に区分されるべき
- ✓ 相互に監視できる仕組みを確立することが重要

内部統制の強化のための職務分掌イメージ

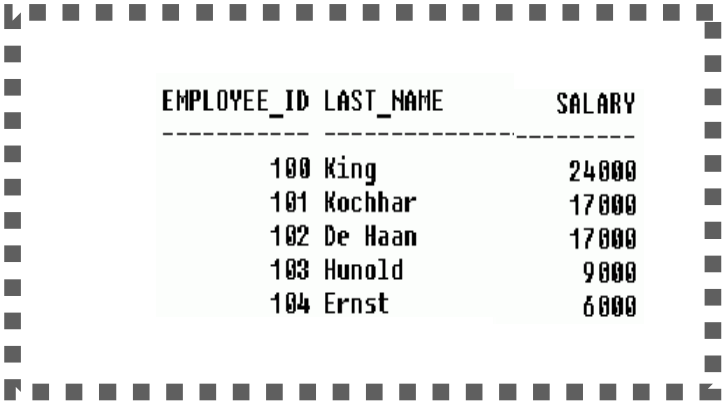
可：セキュリティポリシーの決定、適用
不可：ビジネスデータの操作、DBA業務

セキュリティ管理責任者　Aさん



情報システム部
データベース管理者
Bさん

可：DBA業務
不可：ビジネスデータの操作



EMPLOYEE_ID	LAST_NAME	SALARY
100	King	24000
101	Kochhar	17000
102	De Haan	17000
103	Hunold	9000
104	Ernst	6000

人事部給与担当　Cさん

可：給与データの管理

ご参考：Oracle Database Vault でできること
データベース管理者の権限を制限 ～権限の分割～

～ 今までの Oracle Database ～
データベース管理者に管理権限が一極集中

- データベース管理
- ユーザー・アカウント管理
- セキュリティ・ポリシー管理
- アプリケーション・データの管理

データベースの起動停止から、全スキーマ・
オブジェクトの操作やセキュリティの設定まで、
あらゆるシステム権限の実行が可能
➔➔➔
データベース管理者自身による、不正なデータの操作や情報漏えいのリスク！

～ Oracle Database Vault ～
複数の管理者に管理権限を分割、分担

データベース管理
データベースの起動/停止 など
※実データへのアクセス不可！

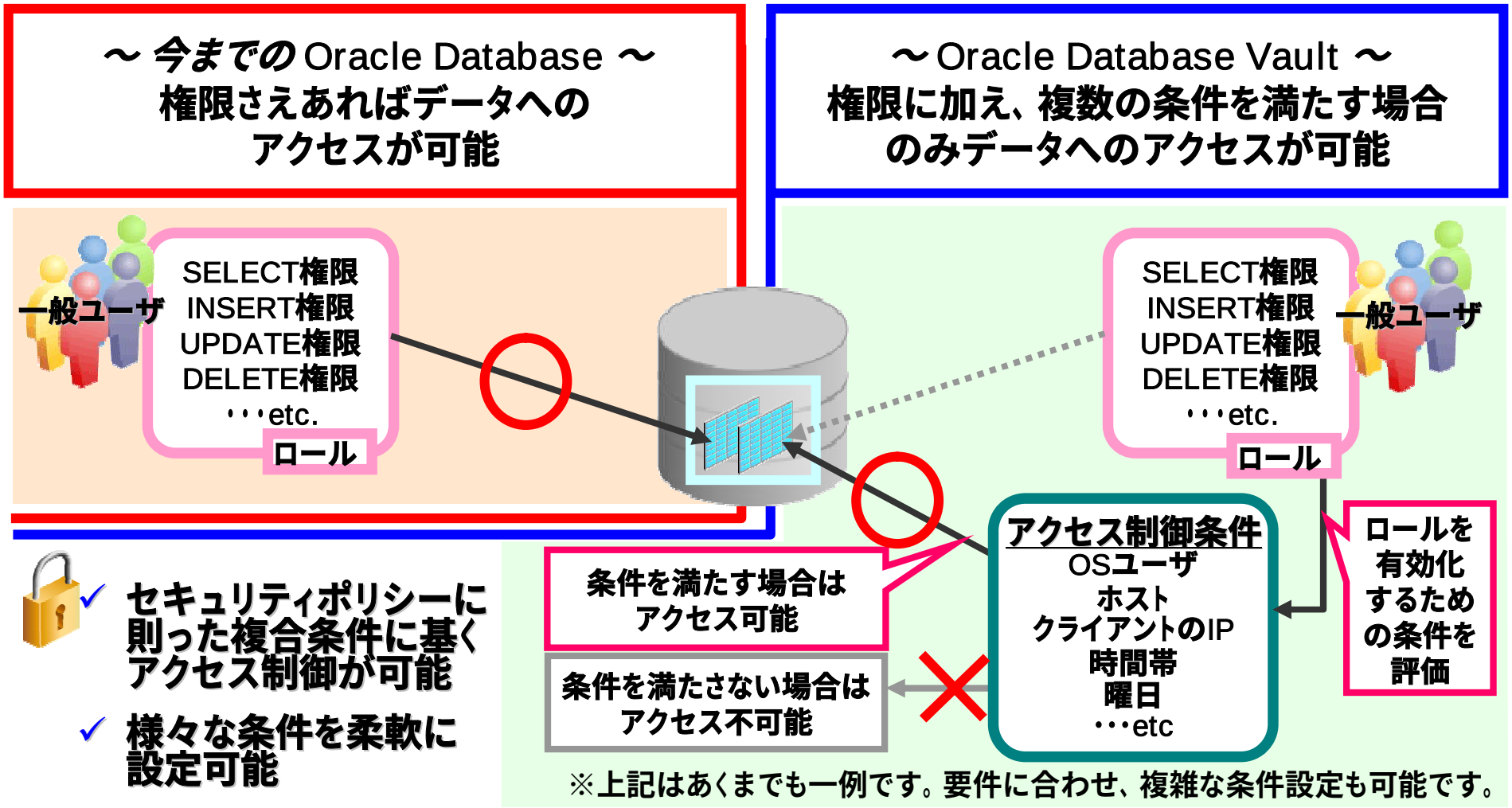
ユーザー・アカウント管理
ユーザの作成・変更、プロファイル
の作成・変更、接続の許可
※実データへのアクセス不可！

セキュリティ・ポリシー管理
セキュリティポリシーに基くアクセス
制御の設定、管理
※実データへのアクセス不可！

アプリケーション・データの管理
アプリケーションに紐付く実データ
の管理、アクセス権限の付与

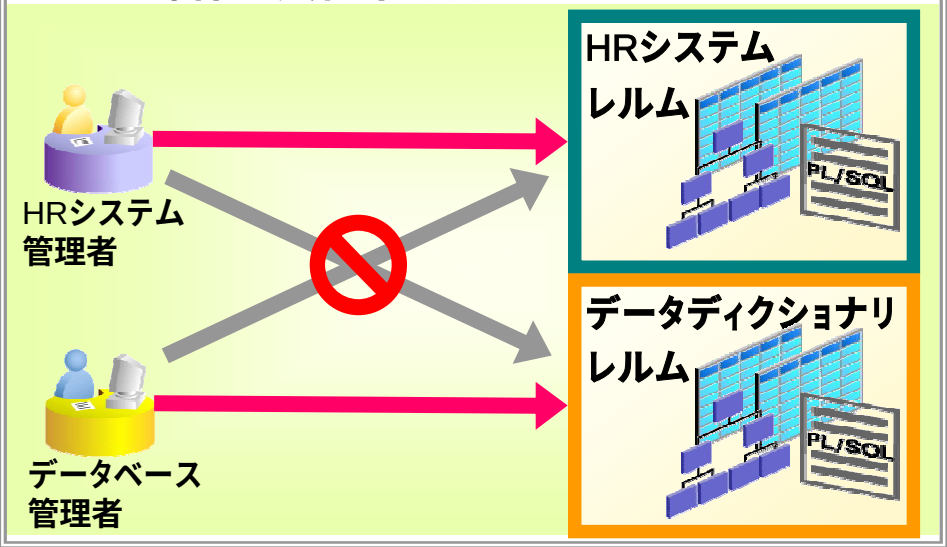
- ✓ 管理権限の一極集中によるリスクを回避し、各役割に応じた権限のみを持つ 複数の管理者によって、データベースを安全に管理
- ✓ 日本版SOX法などの法規制に備えた、内部統制の基盤作りが可能

ご参考：Oracle Database Vault でできること
様々な条件に基く強靭かつ柔軟なアクセス制御

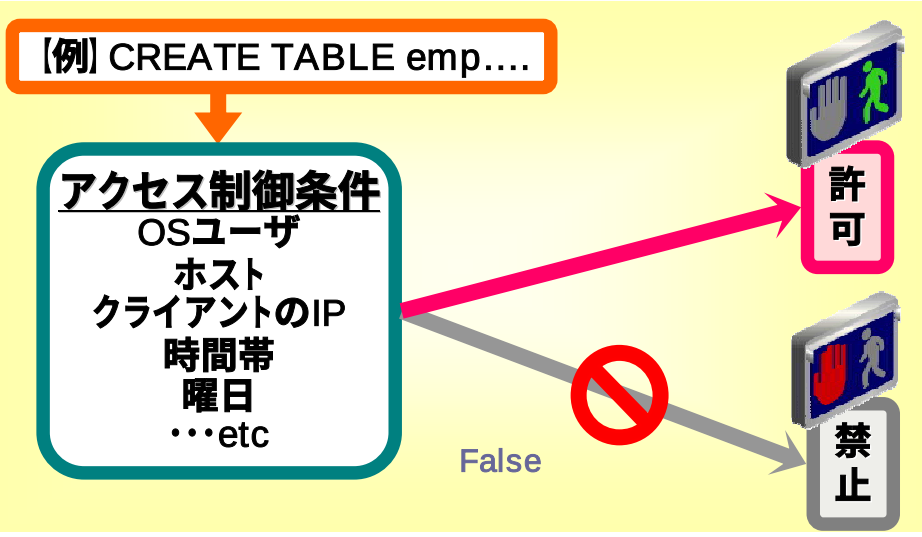


ご参考：Oracle Database Vault でできること Realm や Command Rule によるデータの保護

- Realm (レルム)
  - スキーマあるいは一部オブジェクトのセットを保護・管理するための論理的な単位。
  - レルム所有者はDBAの権限と役割を持ち、システム権限の行使やオブジェクト権限の付与等を行うことが可能。ただしその権限はレルム内に閉じるため、他レルムに対する操作は実行不可能。



- Command Rule (コマンド・ルール)
  - 各SQLコマンドの実行をアクセス制御条件に基いて制限するためのもの。
  - 紐付くアクセス制御条件を満たす場合にのみ、その SQLコマンドを発行する許可が与えられる。
    ※注：各コマンドの実行権限は別途必要。

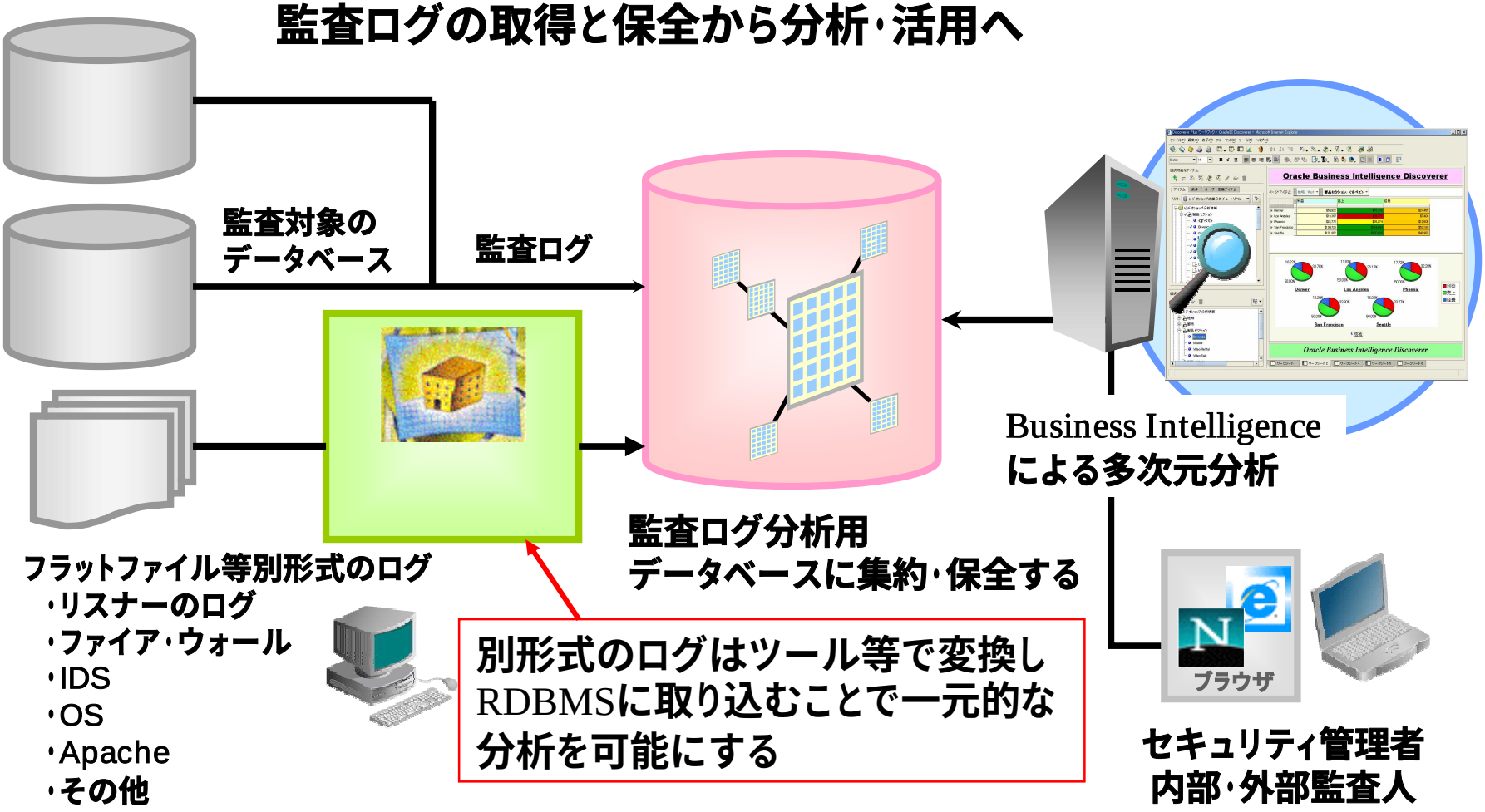


②情報が正しいと証明する

- 各種監査ログの取得と保全が必要。
  - ログを取っておくだけではなく活用するフェーズへ
  - 定期的な傾向分析による不正の早期発見
- ユーザのID・権限・ロールの付与プロセスやポリシーを管理する必要がある。
  - 「権限を与えて良い」と誰が承認するのか？
  - 承認のポリシーとプロセスは可視化されているか？
  - IDの生成・変更・削除とそれにともなう承認プロセスは履歴を保持しているか？

②情報が正しいと証明する

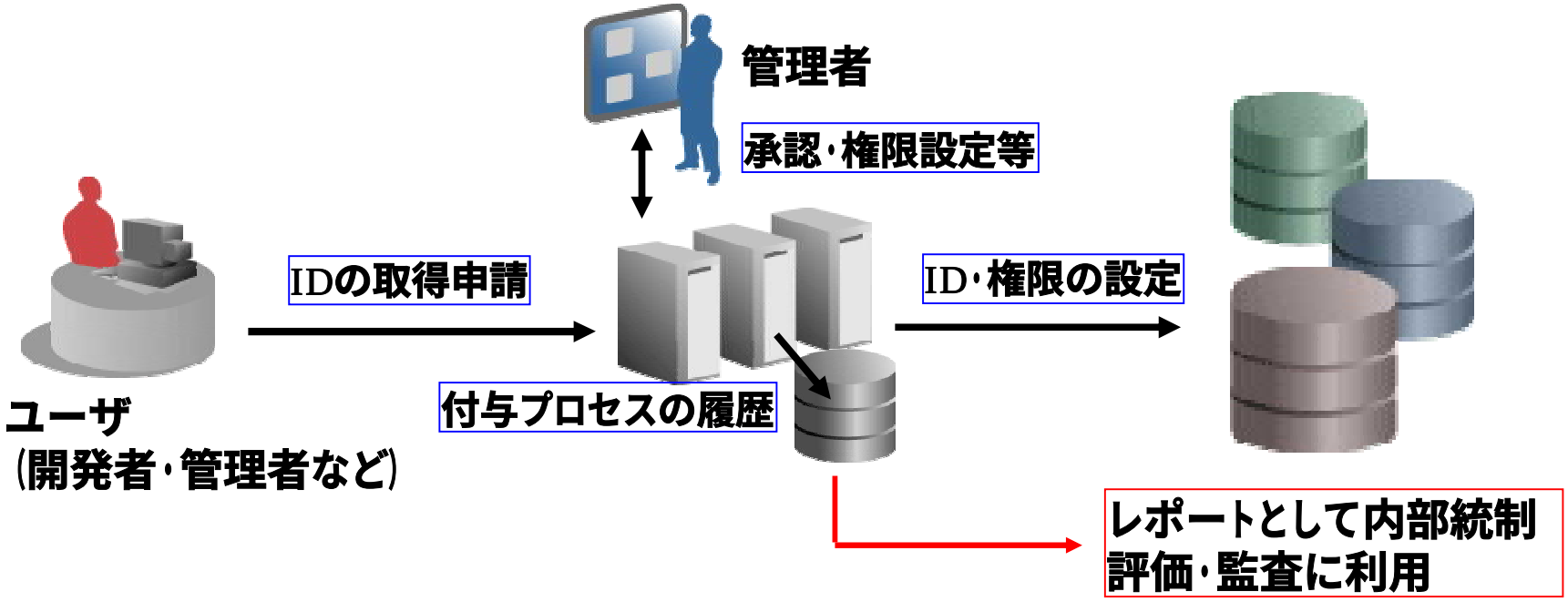
監査ログの取得と保全から分析･活用へ



監査ログ → 取り込み → 蓄積 → 分析 → 追跡･証拠保全

②情報が正しいと証明する

- ID管理基盤（アイデンティティ・マネジメント）によるユーザ・権限・ロールの一元管理と履歴の取得
  - OS・アプリケーションなど様々なIDを一元的に管理する必要があるためデータベースもここに取り込む。



ご参考：Oracle Identity Managerを使ったID管理