アンチパターンから学ぶID管理

2011 年 2 月1日

標準化部会 セキュリティにおける
アイデンティティ管理 WG

駒沢　健（NTTコムウェア）

自己紹介

- **1997年NTTコムウェア入社**
  - NTTの通信設備のシステム開発に従事
- **1999年よりセキュリティのSE**
  - 認証（シングルサインオン・生態認証）
  - PKI
  - 端末制御・端末管理
  - ウィルス対策
  - セキュリティグランドデザイン
- **2008年にID管理の案件従事**
  - 難しい・・・

ID管理に関する様々な課題検討

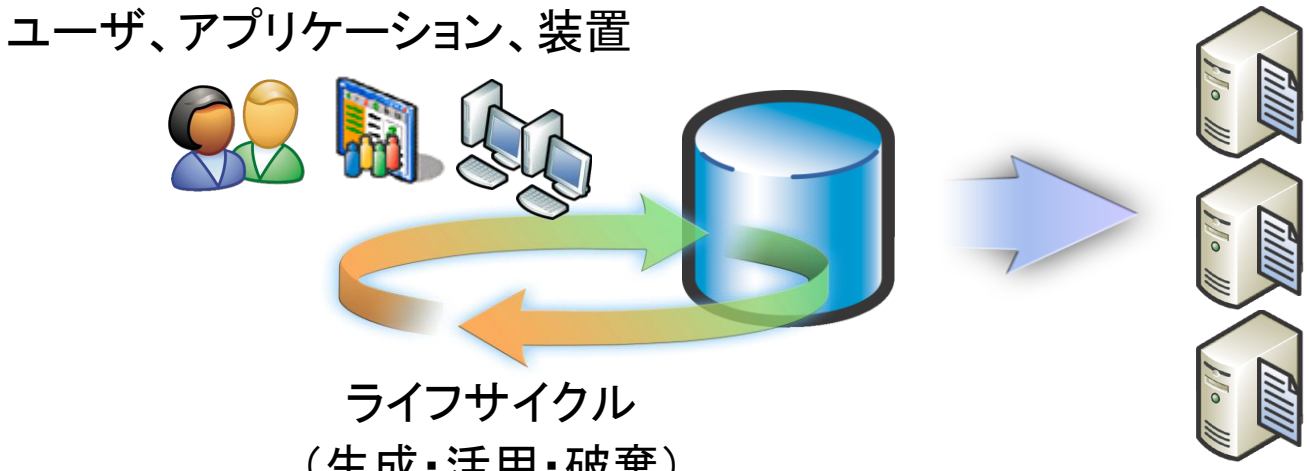
JNSA

標準化部会「セキュリティにおけるアイデンティティ管理 WG」

NRI SECURE TECHNOLOGIES
NEC
TOSHIBA Leading Innovation
東芝ソリューション株式会社
FUJITSU
SIGMAXYZ Xpartner for Your Z
JBS
NTTコムウェア
INTEC
CTC Challenging Tomorrow's Chang
ORACLE
IBM
NET MARKS
Microsoft
MITSUBISHI Changes for the Better

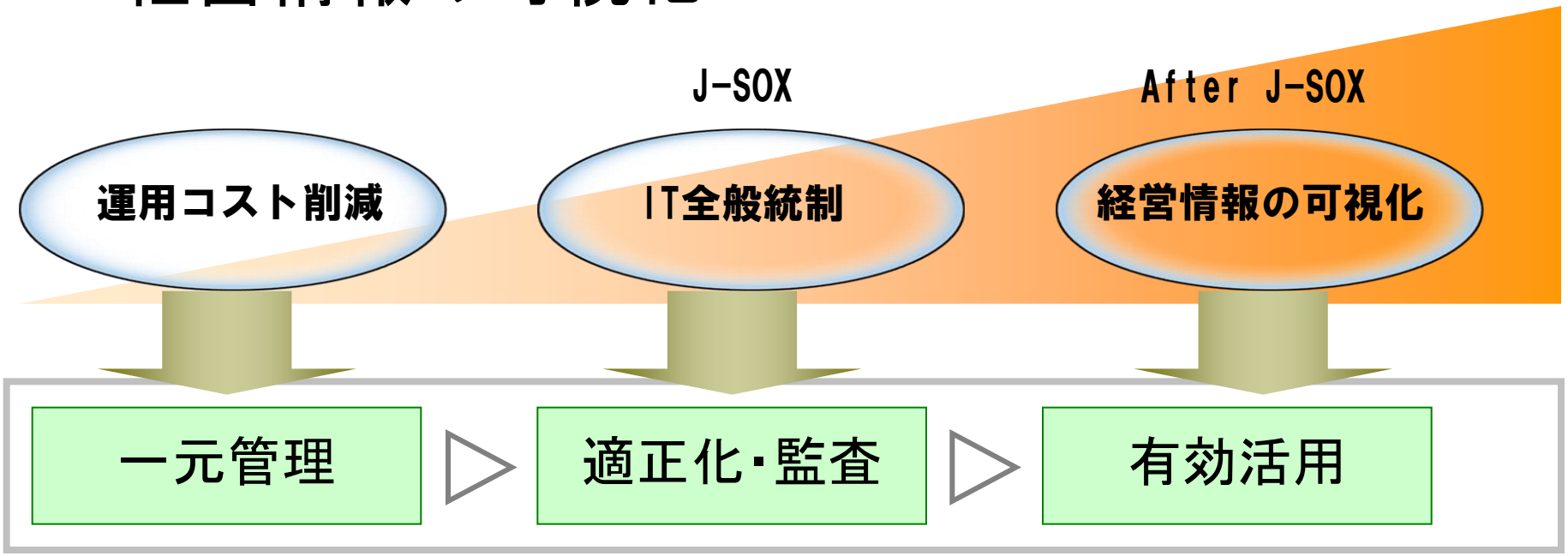
ID管理とは

ID管理は、組織または企業全体にわたり、すべてのユーザ、アプリケーション、または装置のデジタルIDのライフサイクルを管理する機能



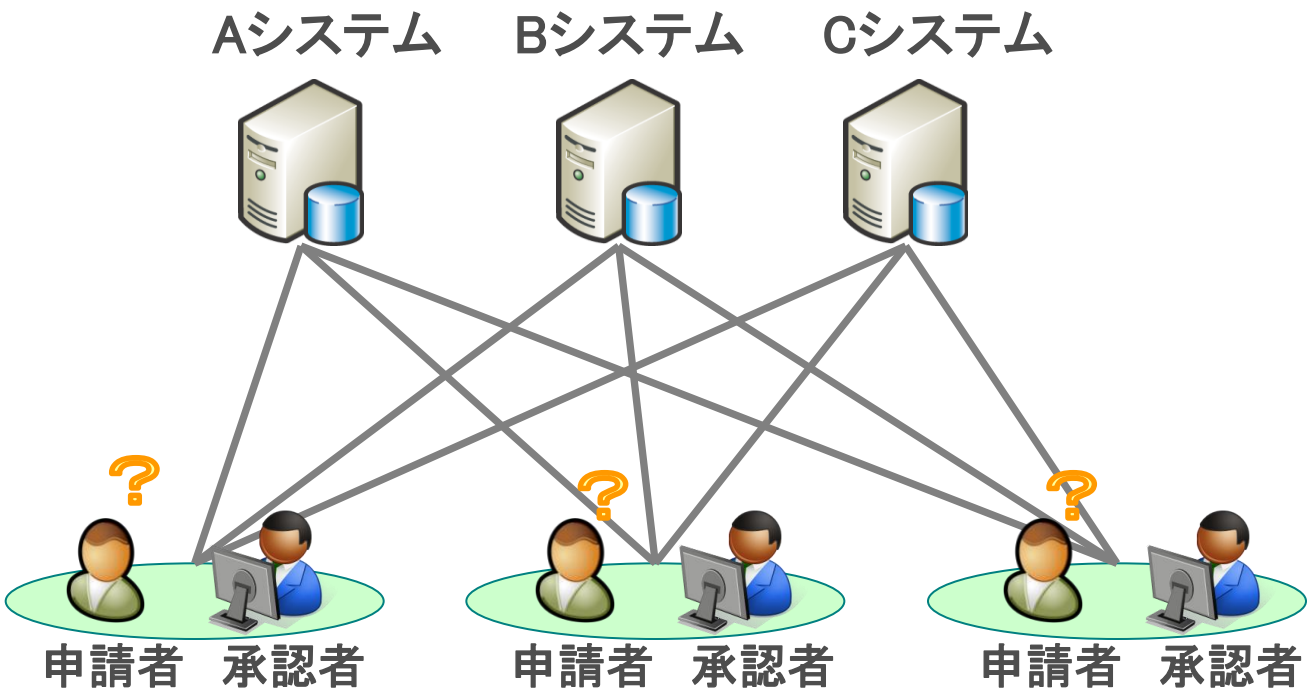
ID管理の導入目的

- 運用コスト削減
- IT全般統制
- 経営情報の可視化



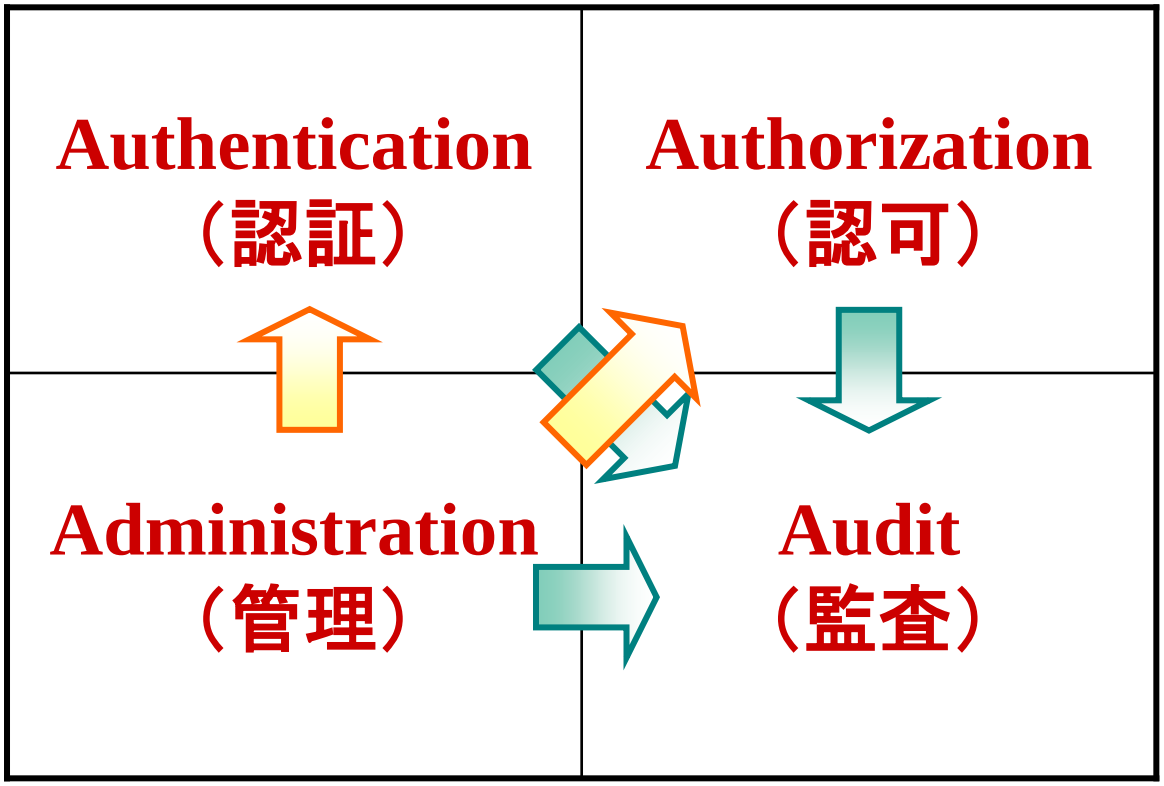
ID管理における問題

- 業務システムが個別にIDを管理
  - 現場の負担増
  - 運用ルールの不統一

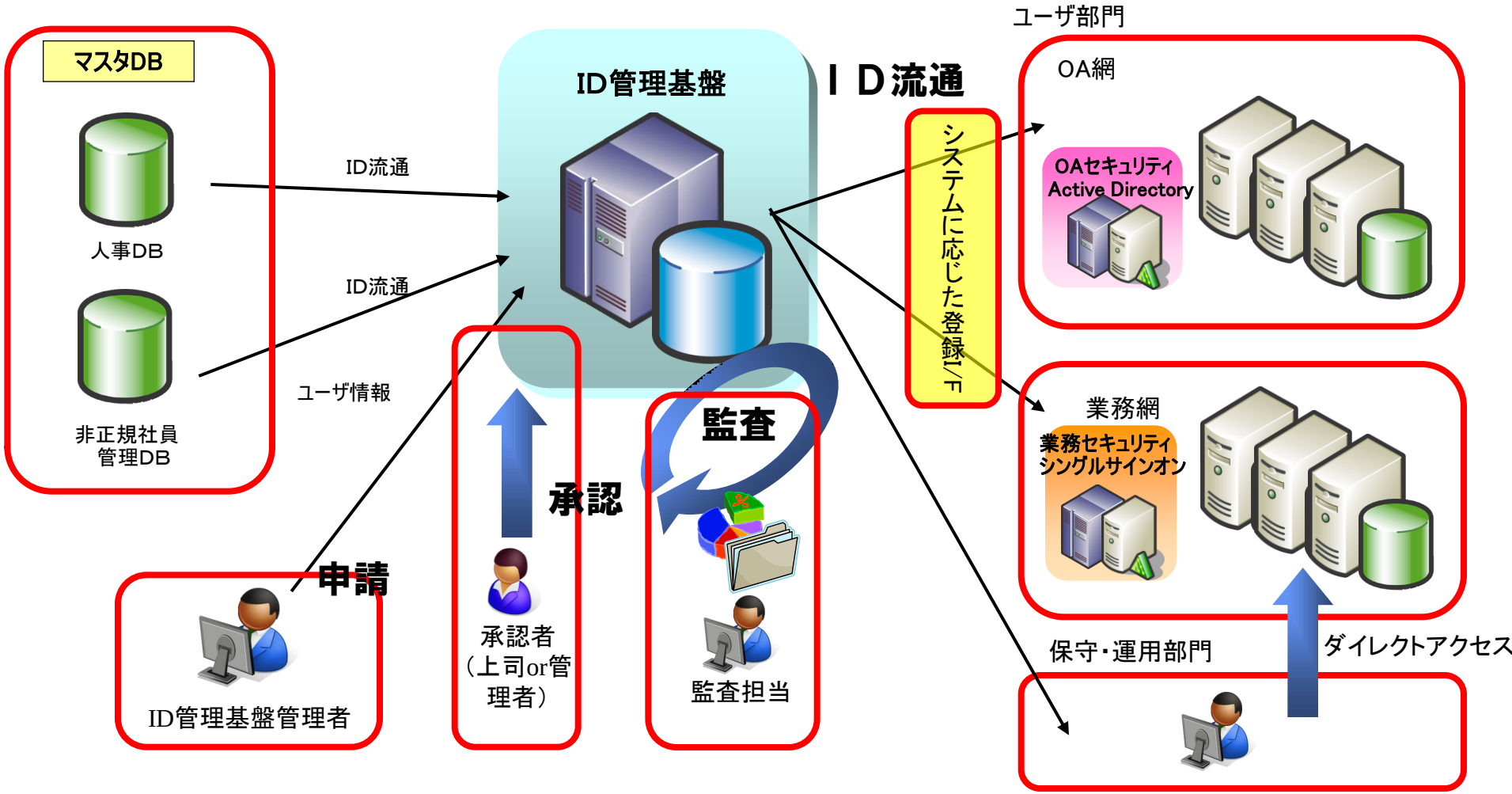


認証とID管理

制御部（認証・認可）のIDを管理する



ID管理の理想形態



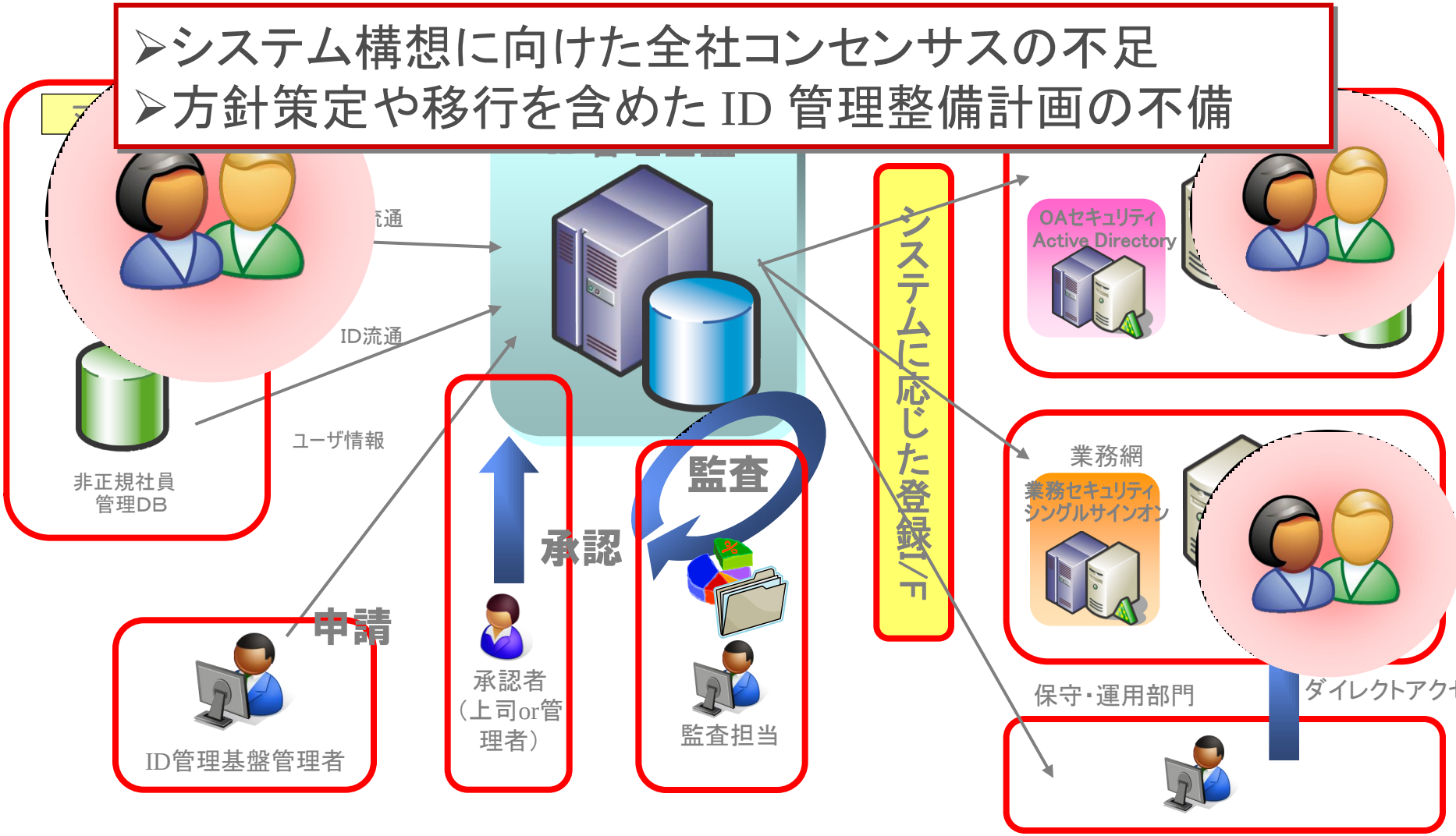
アンチパターン：絵に描いたモチ

絵に描いたモチ

- IT部門がJ-SOX対応としてID管理を企画
- 企画の全体像に関連する組織を巻き込まず検討を実施
- 施策推進の課題が十分に把握できないままプロジェクトは進む
- プロジェクトが進むにつれ関連組織からクレームが膨らむ
- 業務要件からやりなおし・・・

教訓（絵に描いたモチ）

- システム構想に向けた全社コンセンサスの不足
- 方針策定や移行を含めた ID 管理整備計画の不備



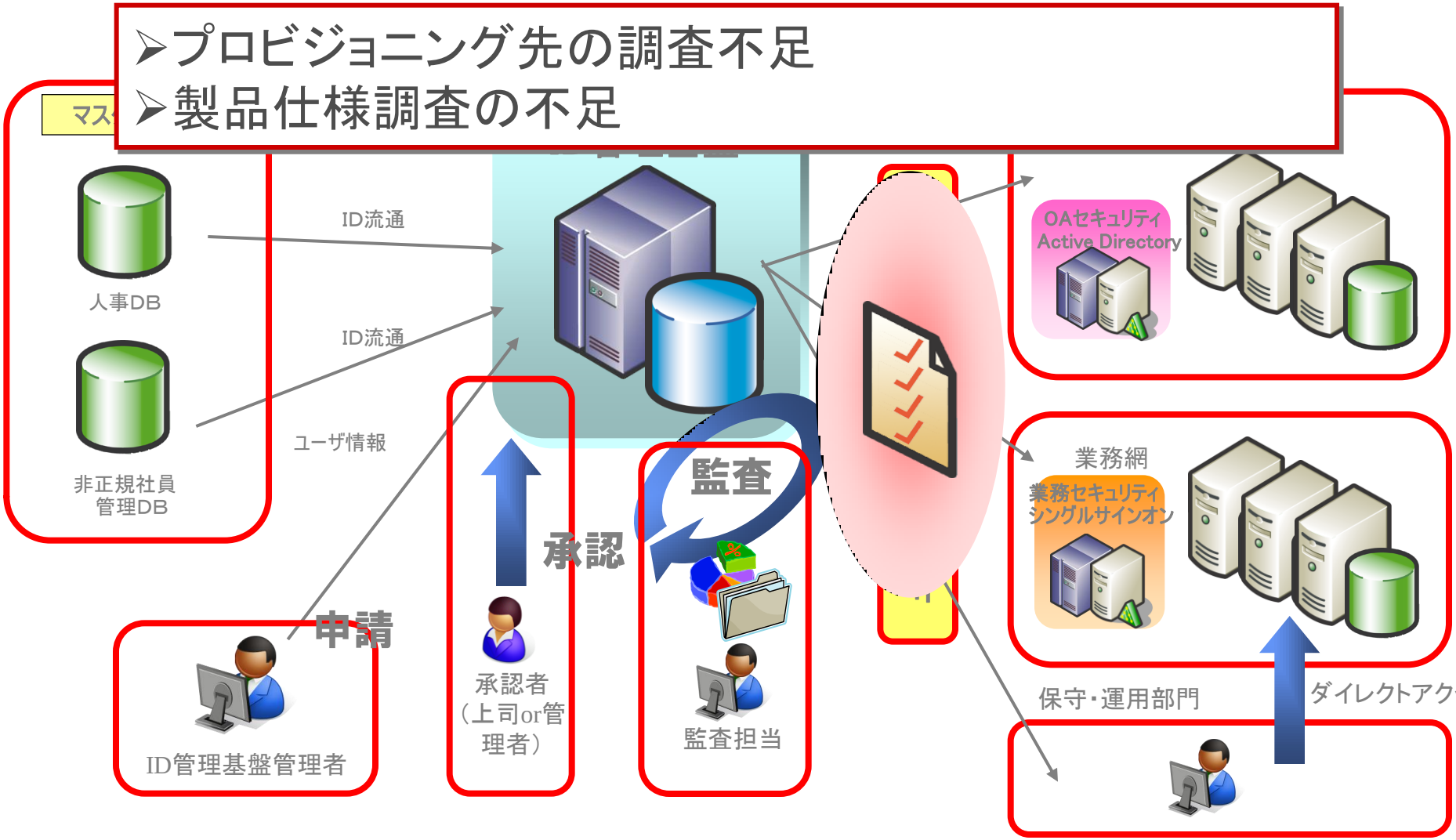
アンチパターン：繋がるだろう症候群

繋がるだろう症候群

- IT部門がJ-SOX監査対応としてID管理を企画
- ID管理製品（パッケージ）を極力活用して導入する方針
- 製品標準の連携コネクタでプロビジョニング先のシステムと連携を判断（製品パンフレット確認）
- テスト段階で標準コネクタが扱えない属性の配信要望が・・・
- 当初計画外の拡張開発が・・・

教訓（繋がるだろう症候群）

- プロビジョニング先の調査不足
- 製品仕様調査の不足



ID管理基盤構築のポイント

- ID 管理プロジェクトは全社プロジェクトとしてスタートすること
- プロビジョニング先の事前調査と製品仕様の確認を徹底すること
- 関連部署との協力体制を構築し、業務フロー分析・整理は必ず行うこと
- 製品を意識し、要件の範囲を広げすぎないようにする
- プロビジョニング先の徹底的な事前調査が必ず行うこと

JNSAによるガイドライン

JNSA

クラウド環境における アイデンティティ管理ガイドライン

［内部統制に対応した統合ID管理の計画から導入まで］

インターネット メディア 総合研究所 REPORT

impress R&D An impress Group Company

クラウド環境に対応したアイデンティティー管理導入について 日本ネットワークセキュリティ協会の約5年間の活動を集大成したガイドライン

本書の内容

実際にシステムを販売しているベンダー、コンサルタント、SIerによる初の書き下ろし

現場の担当者がすぐ使えるテンプレート付き クラウドを活用する際の要点がわかる!

インプレス社より電子書籍にて販売中

つつ、ID管理システムを導入するユーザ、SIerなどにとって有用となる知識・ノウハウが持ち寄られています。

その結果、本書の解説はアイデンティティ管理とは何か？から始まり、主要な構成要素の定義、内部統制や情報セキュリティといった外部的な要請との関係、ID管理システムの導入効果、ID管理システム導入の各フェーズのタスクについての指針、アイデンティティ管理システムの導入事例、プロジェクトの失敗パターンと処方箋、FAQと広範囲にわたって詳細にまとめられています。

また、近年急速にクラウドサービスの活用が普及の兆しをみせていますが、インターネット上のサービスということもあり、利用においてはセキュリティ面の課題があります。特にID管理に関しては技術・運用の観点で新たな知識が必要となっています。本ガイドラインではクラウドを活用する際の考慮点もまとめていますので、クラウドを検討する際に活用いただけます。

となっています。

項番	カテゴリ	対象となる業務アプリ	管理者	部門	課題	備考	回答数
1	仕様	経費精算システム		営業部	システムへのログイン	Windowsにログオンしているのだから、再度ログオンさせることなく、そのまま利用できるようにしてほしい。	5
2	仕様	全システム	○	企画部	システムへのログイン	派遣社員のユーザーIDの管理が面倒。システム部門で集中的に管理してもらうことはできないか？	1
3	仕様	経費精算システム		営業部	システムへのログイン	ユーザーIDがWindowsログオンのIDと異なるため、どんなIDを使っていたか忘れてしまうことがある。同じものを使用したい。	3
4	仕様	全システム	○	営業部	システムへのログイン	＊	1
5	仕様	経費精算システム		営業部	定期的なパスワードの変更	パスワードに使える文字が、Windowsにログオンする文字と違う。同じパスワードにしたいのに、統一できな	3
6	仕様	経費精算システム		営業部	その他	承認者の選択時に自動的に上司が入力されるようにしてほしい。	12
7	仕様	経費精算システム		営業部	その他	所属が変わったら、自動的に「所属」表示を変更しては	1
8	コスト	ファイルサーバー		企画部	その他	ファイルサーバーに共有を作成する際の手続きが面倒なので、すぐに使い始めることができない。管理者も不在のことが多い。紙ではなく電子メール等で処理できない	2
9	コスト	経費管理システム	○	システム	人事異動に伴うユーザーIDの[illegible]	人事システムからのデータに不備が多く、取込み時の検証に手間がかかっている。Input Readyな形式で受け取ることはできないか？	1
10	コスト	経費管理システム	○	システム	人事異動に伴うユーザーIDの[illegible]	人事データにユーザーIDが入っていないため、独自にユーザーIDを割り振っている。過去に使っていたIDと重複が無いかどうかを確認する作業にとても時間がかかり、ミスが発生することがある。	1

【テンプレート1】ID管理に関する現状の問題点リスト

本書のセールスポイント

- ●内部統制に対応した統合ID管理の計画から導入までを解説
- ●日本ネットワークセキュリティ協会の約5年間の活動を集大成したガイドライン
- ●実際にシステムを販売しているベンダー、コンサルタント、SIerによる初の書き下ろし
- ●現場の担当者がすぐ使える「ID管理に関する現状の問題点リスト」や「現状調査記述書—業務フロー」などのテンプレート付き
- ●クラウドを活用する際の要点がすぐわかる

ご清聴ありがとうございました