企業におけるID管理の全体像

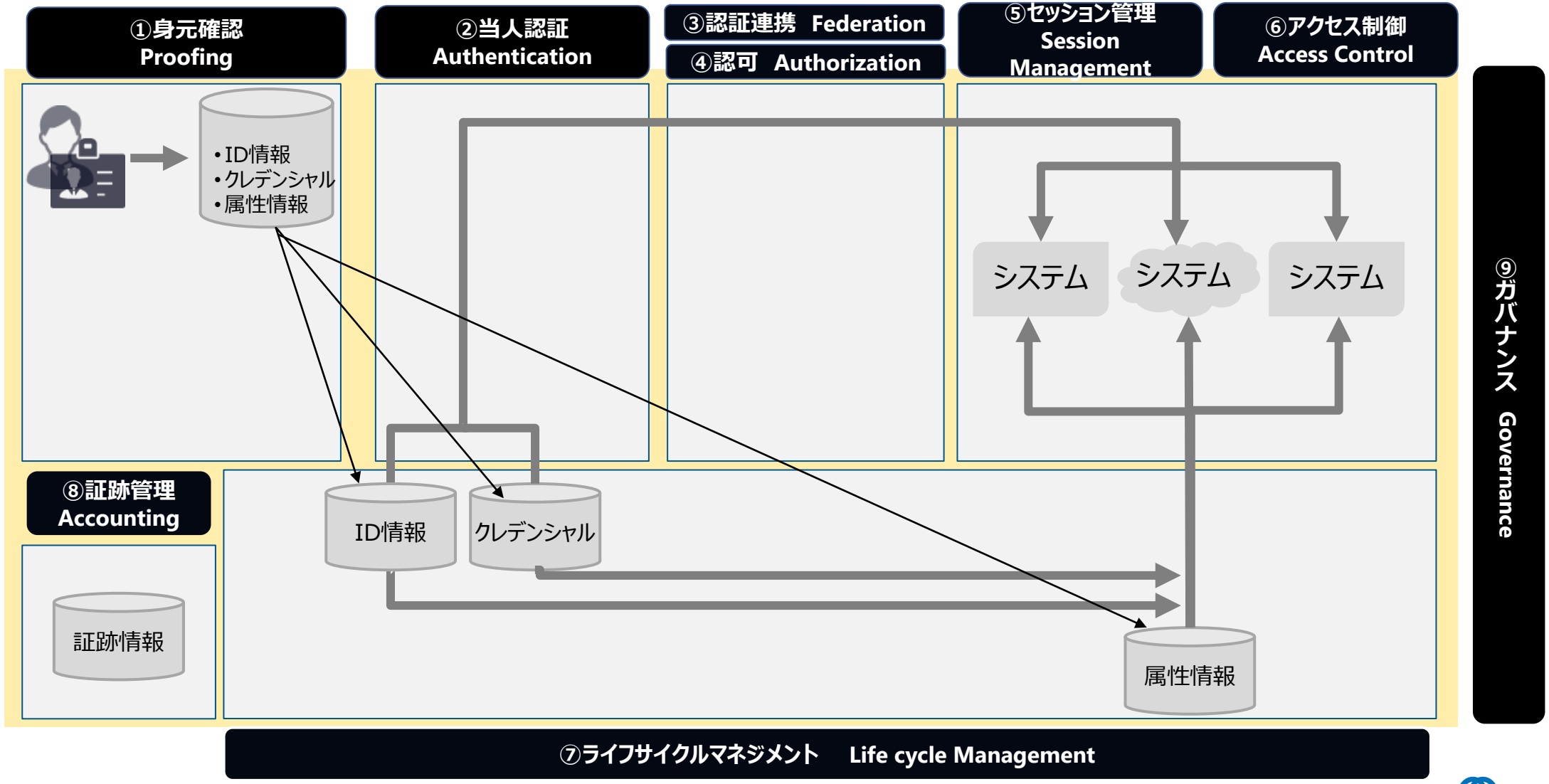
2023/12/14 株式会社NTTデータグループ

ID管理とは？

ID管理(Identity Management)は非常に幅広い技術、業務、ルールを含む。業務をスムースに進め、かつ個人情報保護、J-SOXなどの法令順守のほか、プライバシーマーク、ISMS認証など様々な資格が要求する制御を実現する必要あり

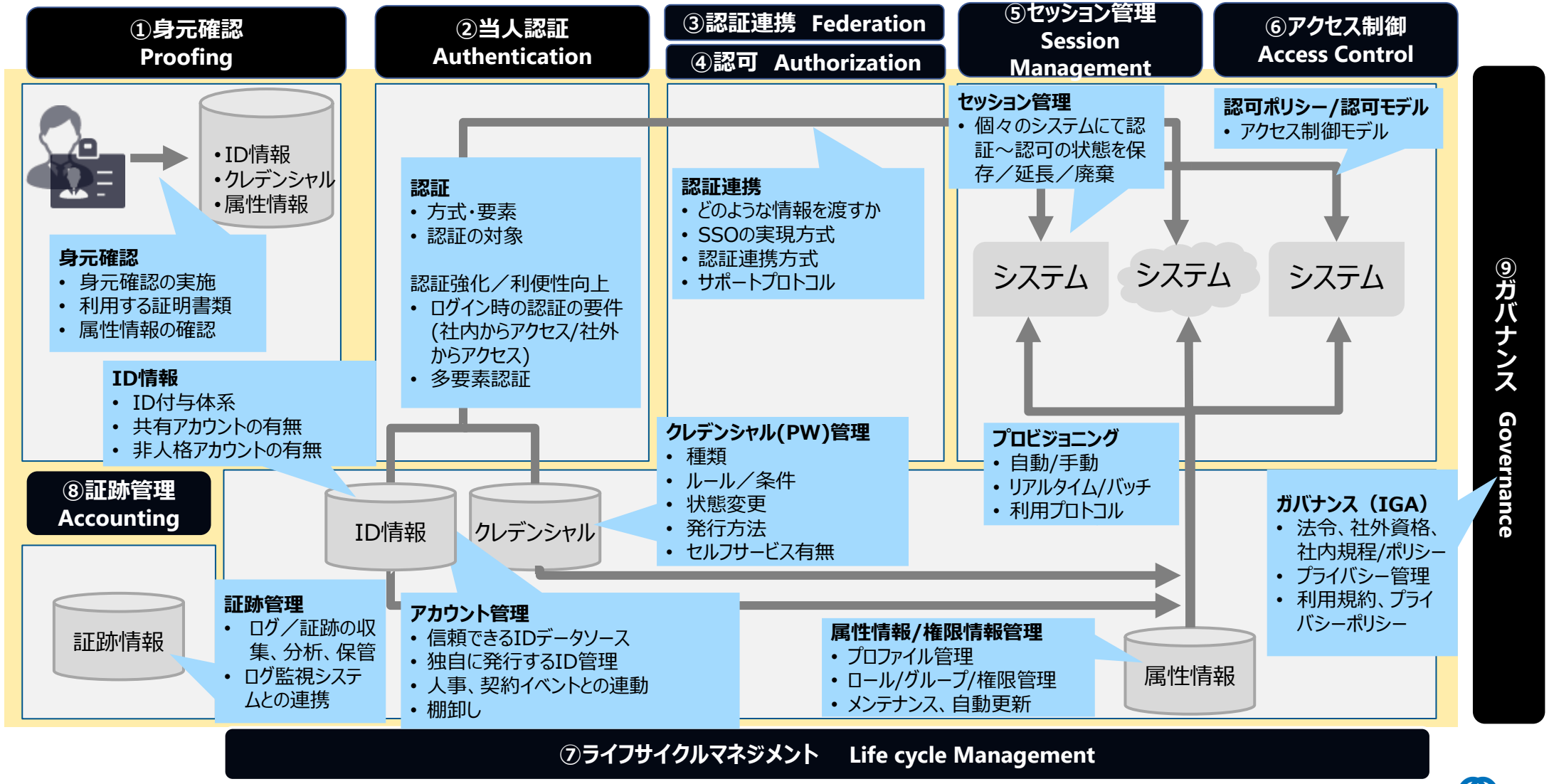
ID管理の全体像

NTTデータによる独自のフレームワーク



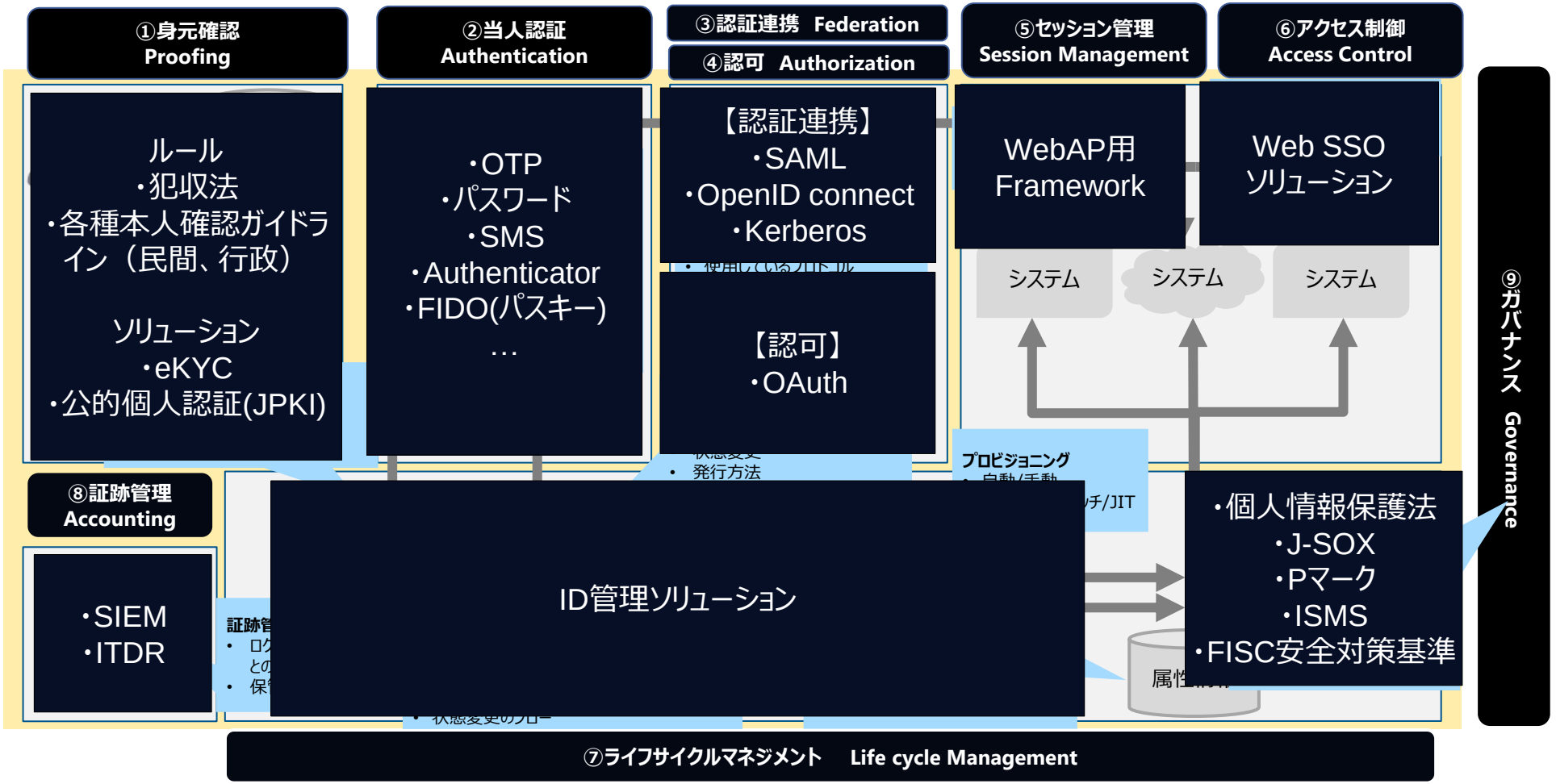
ID管理の全体像

検討すべき多くの課題



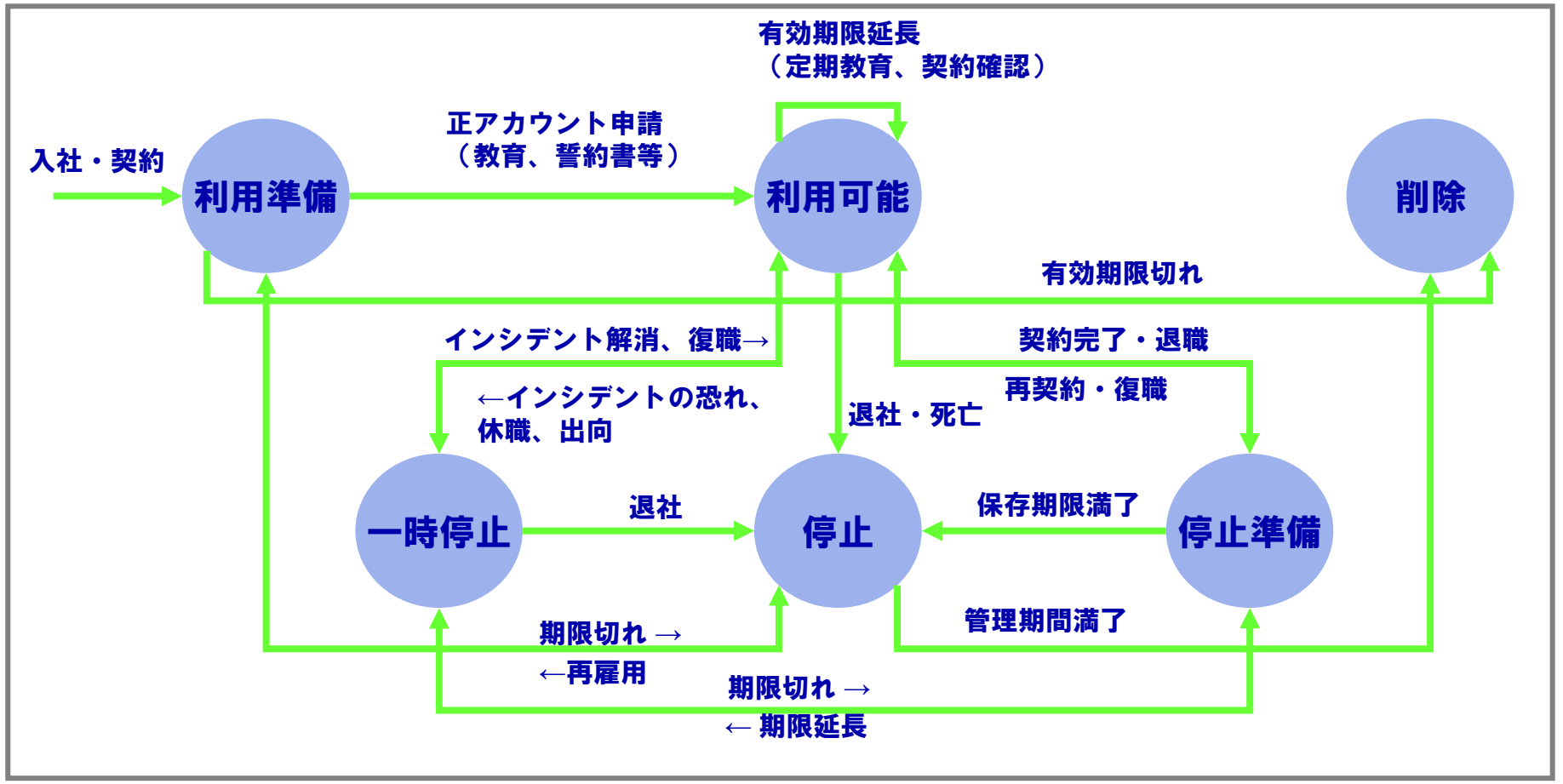
ID管理の全体像

ソリューション導入により解決できる部分、ルール策定（適切なものを参照）、適切な運用など多様な対応が求められる



例１）IDのライフサイクル（ライフサイクル）

利用者の状態変化（社員：入社、退社、休職、復職、出向、出向復帰、契約社員：契約開始、契約中断、契約復帰、契約満了など）をタイムリーに把握し、ID管理の状態（利用者、各種属性）に早急に反映する必要がある。



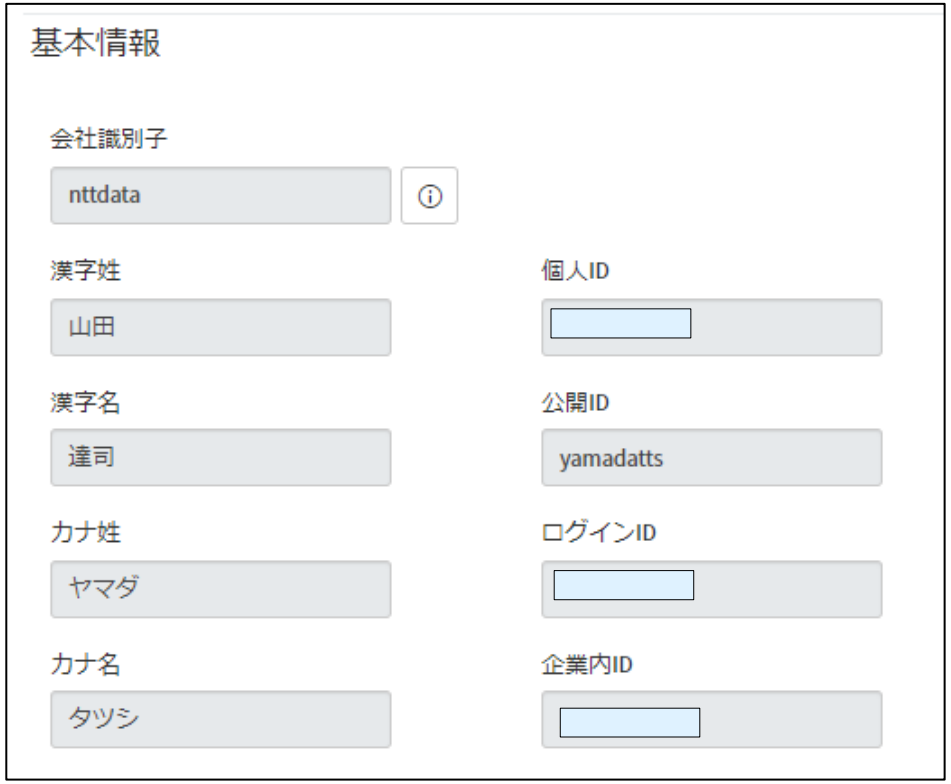
例２）複数のIdentifier

当社ではひとつのIdentityは３つのIdentifierを保有

・個人ID：システムのログなどで利用される。7桁英数字。利用者は意識しない
　　変更不可(IAMが発行）。社内公開可

・公開ID：主にコミュニケーションにおける人の識別に利用される
（姓名をもとにIAMが発行）
　　変更可（姓名変更時など）。社内公開可

・ログインID　：ログイン時に利用。7桁の英数字
（社員：初期値は社員番号、それ以外はIDシステムが発行）。
　　変更可。社内公開不可



例３）複数のアイデンティティの使い分け

複数のアイデンティティを持つことがあり、それを使い分ける利用者が存在するため、アイデンティティの切り替えとそれに基づくアクセス制御を実装する必要あり。

例）
NTTデータ社員
ー＞NTTデータのグループ企業であるNTTデータABC社に出向
ー＞NTTデータABC社から、NTTデータのプロジェクトXYZに参画

この社員は３つのアイデンティティをもち、それぞれ異なる属性および権限を制御する必要がある。

・NTTデータ社員（出向中）
・NTTデータABC社員（出向受け入れ）
・NTTデータの協力会社社員（プロジェクトXYZ参画）

例４）ID発行基準

IDの発行は下記の３条件を満たすものが対象。ID発行範囲の拡大を可能とするため、RPはIDを保有することのみで利用を許してはならなず、なんらかのアクセス制御を実施する必要がある

条件）

・当社との間に契約（雇用契約、派遣契約、業務委託契約等業務の実施に関するもの）があること
・セキュリティに関する十分な知識を有すること（社内で教育及びテストを実施）
・問題を発生した際に責任を取る社員が明確になっており、当人がそれに合意していること

例外）

・インターン学生
・保険営業＊
・自動販売機（オフィスグリコ等を含む）メンテナンス、補充要員＊

＊　当社では入退館もID管理システムに統合されているため、アテンドなしでの入館が必要な利用者はID取得が必要

例５）アクセス制御

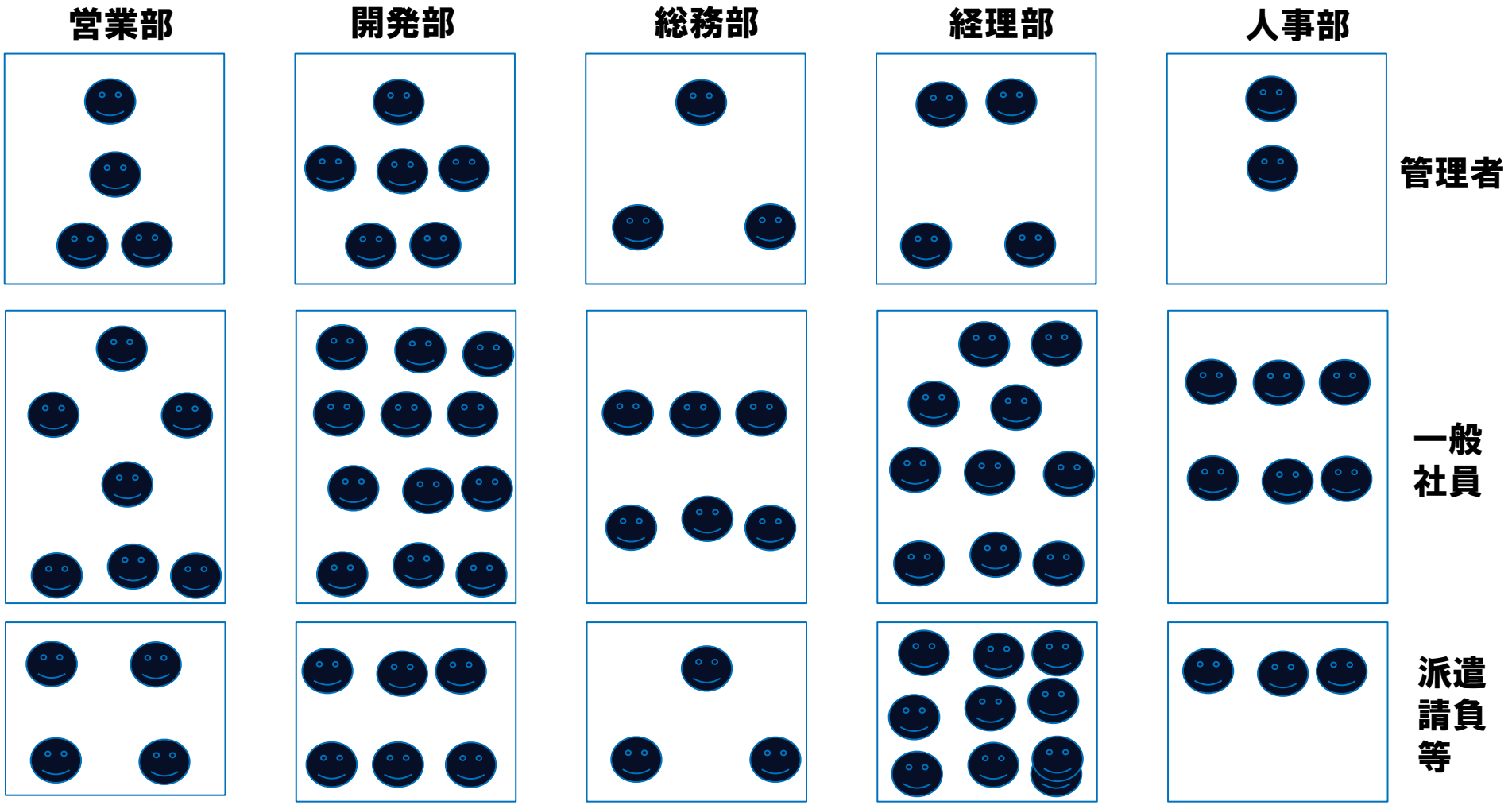
利用者の各種属性（役職、所属、業務、参画プロジェクトなど）を適切に把握し、「最小限の原則」にのっとり、サービス利用におけるアクセス制御を実施する必要がある。

> 最小権限の原則とは、情報セキュリティや計算機科学などの分野において、コンピューティング環境の特定の抽象化レイヤー内で全てのモジュール（主題によっては、プロセス、ユーザー、プログラム）がその正当な目的に必要とされる情報と計算資源のみにアクセスできるように制限する設計原則である[1][2]。

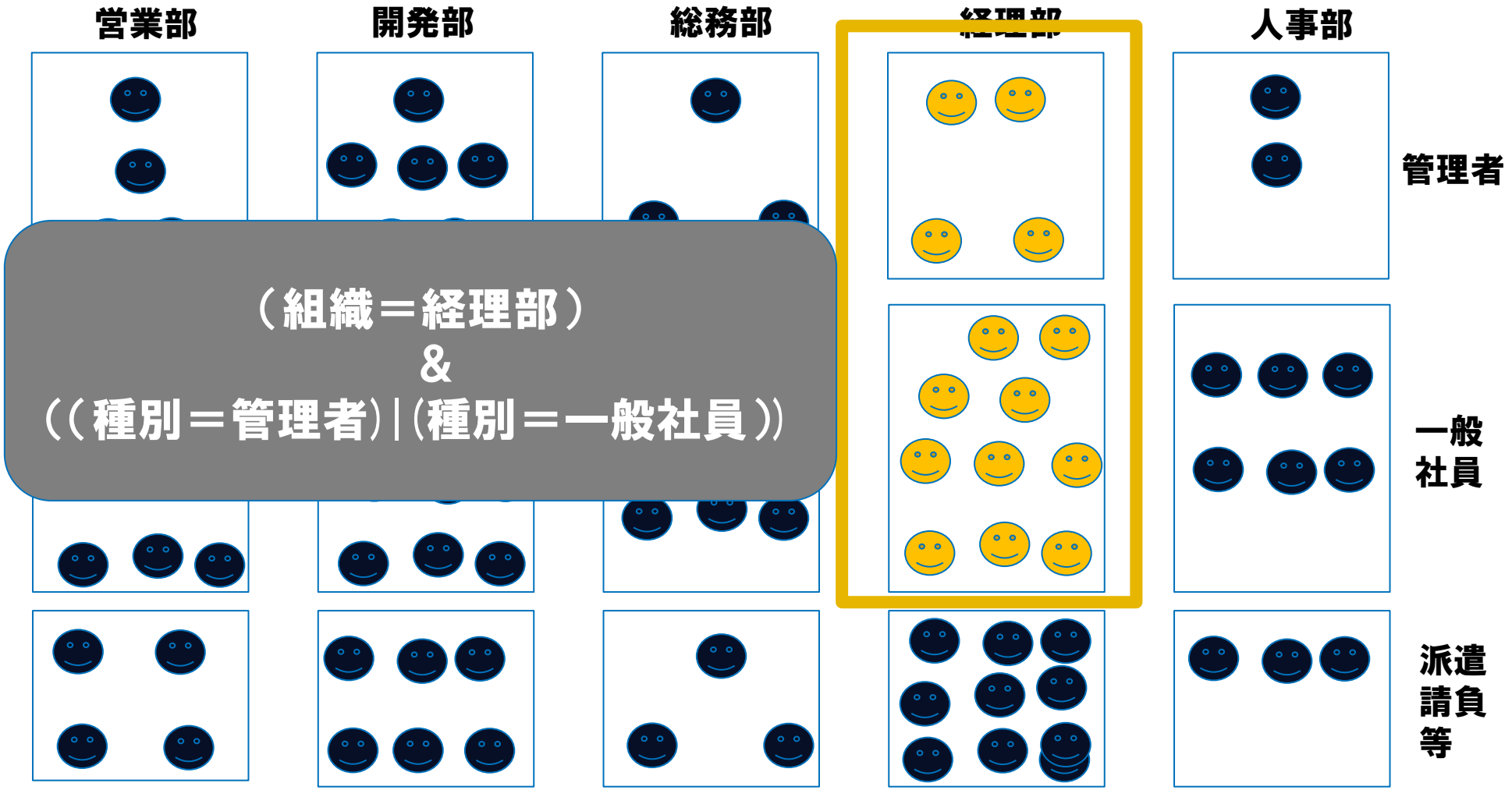
Wikipediaより
https://ja.wikipedia.org/wiki/%E6%9C%80%E5%B0%8F%E6%A8%A9%E9%99%90%E3%81%AE%E5%8E%9F%E5%89%87

すべての利用者は
正当な目的に必要な情報「のみ」に
アクセスできる

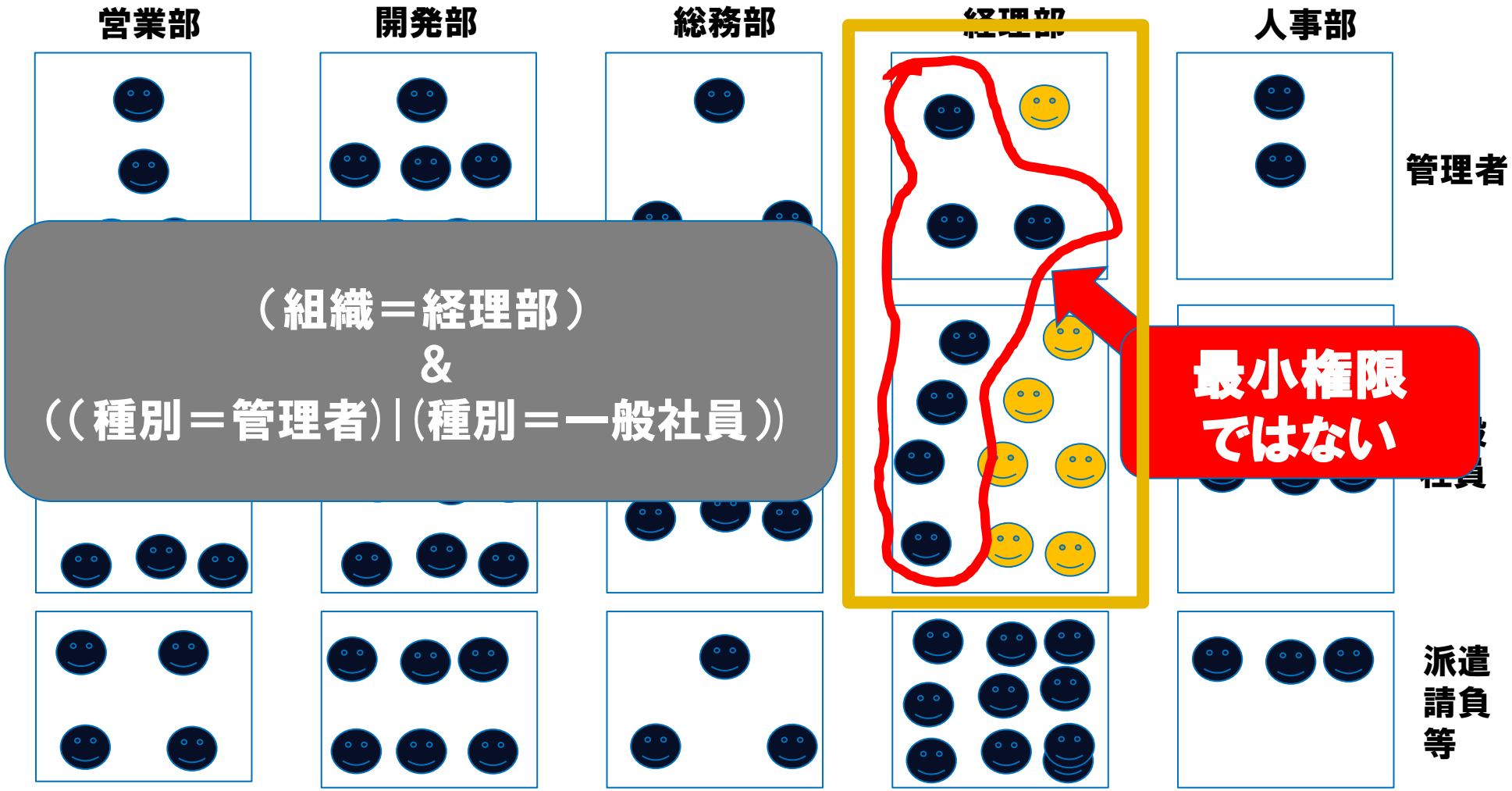
適切なアクセス制御とは？



ちゃんとアクセス制御をしよう

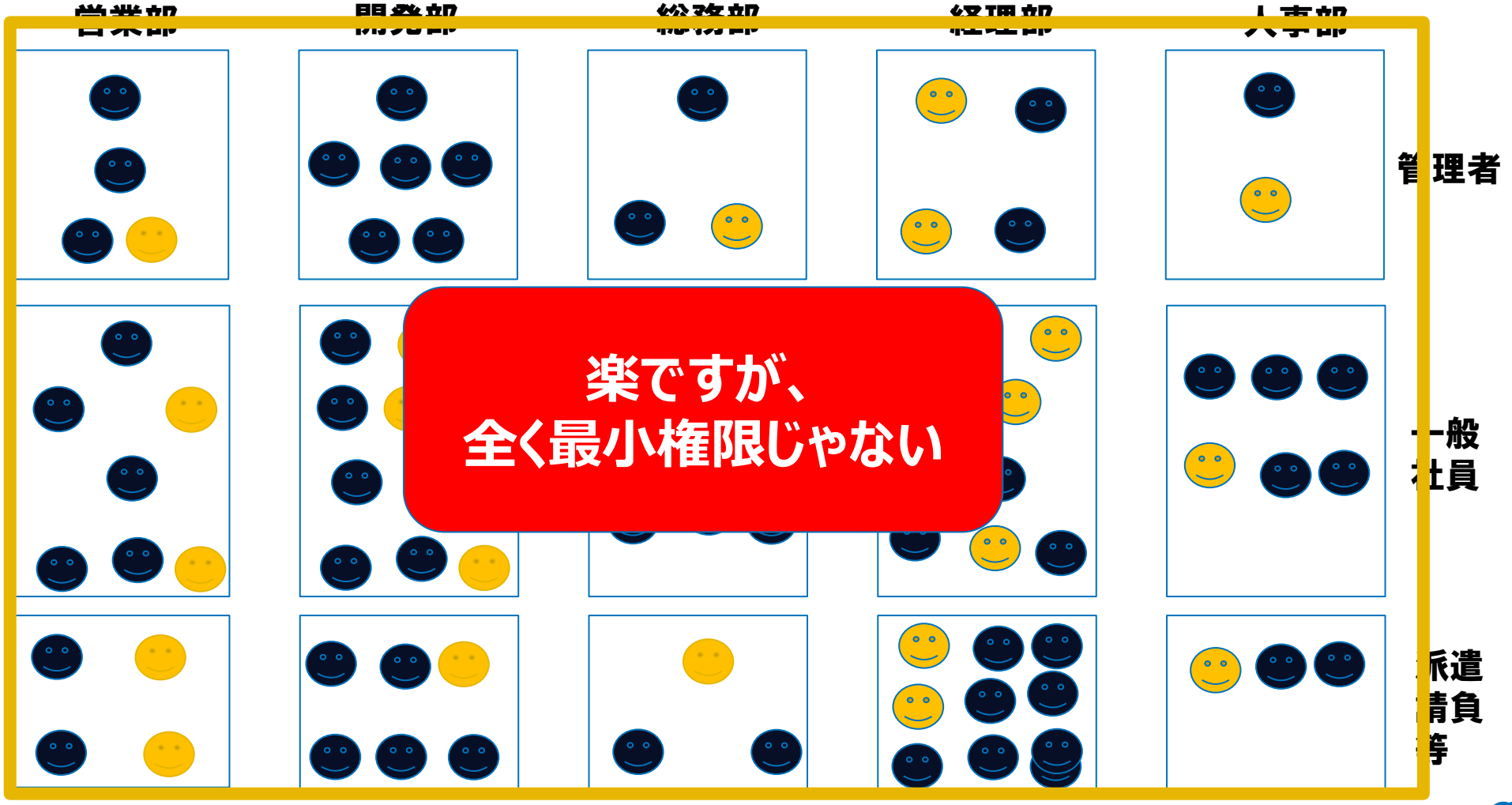


ちゃんとアクセス制御をしよう

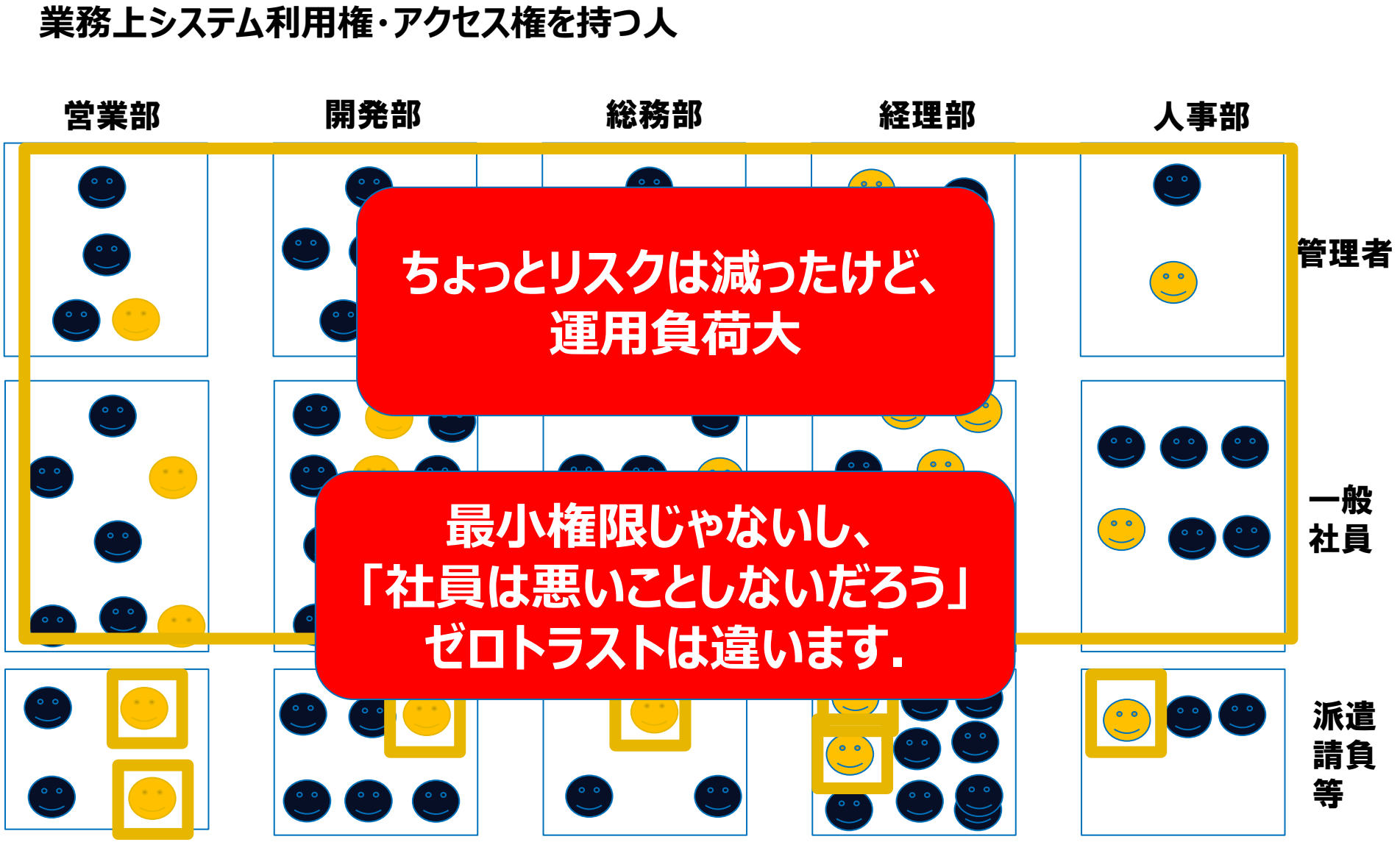


ちゃんとアクセス制御をしよう

業務上システム利用権・アクセス権を持つ人

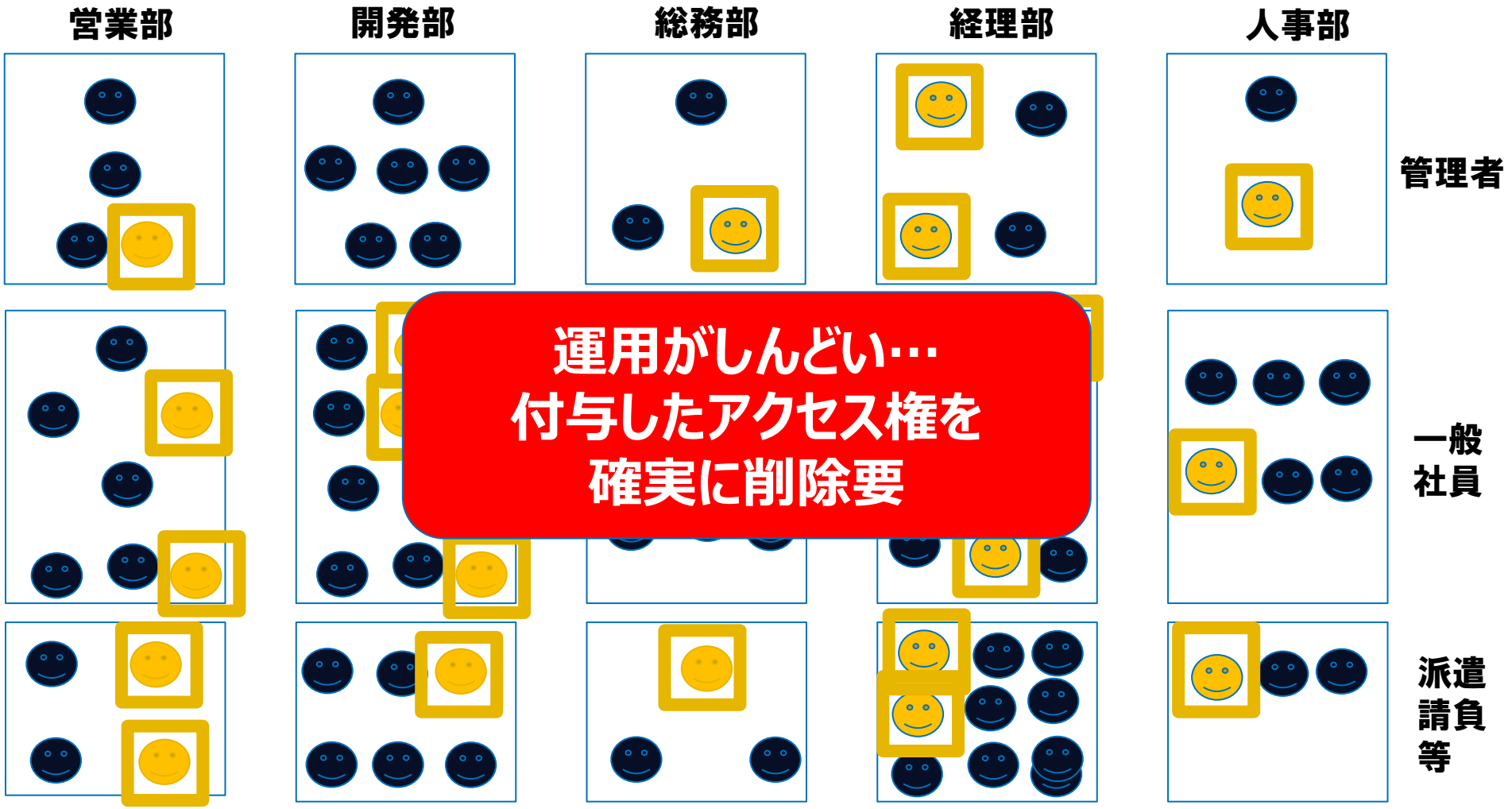


ちゃんとアクセス制御をしよう



ちゃんとアクセス制御をしよう

業務上システム利用権・アクセス権を持つ人



アクセス制御のための仕組み

ID管理システムでは３つのアクセス制御モデルをサポート。アクセス制御のもととなる属性情報を最新とするためのライフサイクルマネジメントを実施

・IBAC(Identity Based Access Control)　：個人単位にアクセス権限を付与し、アクセス制御を実施
　・人事/研修、給与明細、通勤/旅費、BYOD、モバイルアクセス等個人に関するもの
　・多くの業務システムおよびビル管理会社が提供する入退館システム等も本モデルを利用。権限の付与/削除が負担に

・RBAC(Role Based Access Control)　　：人に役割を割り当て、役割に基づき、アクセス制御を実施
　・ファイルサーバ、コミュニケーショングループ、業務システムなど時々の役割に基づくもの

・ABAC(Attribute Based Access Control)：Identity内の属性およびDynamicに変化する情報（時刻、アクセス元IPアドレス等）をもとにアクセス制御
　・適切な属性付与により、柔軟なアクセス制御が可能（一つの仕組みでIBAC,RBACも実現可能）
　・ABACでの利用を容易とするための属性をID管理システムが提供（社員、管理職、所属部署等）
　・XXX組織所属限り、管理職限り、社員限り、特定PJ関係者限りなどのアクセス制御が容易に実現可能
　・アクセス時間、アクセス元（自社オフィス、自宅、顧客拠点等）等ガバナンス、セキュリティ強化にも利用可能

EIAM/CIAM/教育機関におけるIAM

技術・フレームワークが同じID管理でも、企業内(EIAM: Enterprise Identity and Access Management)、コンシューマー（CIAM: Consumer Identity and Access Management）、教育機関におけるID管理の重要性、困難さ、目的は大きく異なる。

	主目的	複雑さ	ガバナンス
EIAM(企業)	セキュリティ、コンプライアンス、生産性向上	一般に非常に複雑	一般的に利かせやすいが、M&A先、グローバル企業などは困難も
CIAM(顧客)	ユーザ獲得と保護	比較的シンプル	難しい
大学（学生）	職員/学生の管理、知的財産保護、利便性向上	？	利かせやすい？

ID管理はビジネス課題と直結する

・企業内セキュリティ、コンプライアンス確保	->企業内における適切なID管理
・業務効率の向上	->シングルサインオン、適切なアクセス制御
・テレワーク、モバイルワーク、クラウドサービス利用	->ゼロトラストに対応したID管理
・パートナ企業連携、BPO強化	->パートナー企業、契約社員、委託先企業など社員のID管理、認証連携
・グループ会社のシナジーおよびガバナンス	->グループ企業全体でのID管理
・グローバル化	->各国の規範を守ったうえで、統一ポリシーに従ったグローバルID管理
・サプライチェーン管理	->多大な企業の存在確認、反社チェック等。システム利用者のID管理
・先端技術の活用	->大学、教育機関との認証連携

そのほか中途入社社員の増加と職歴の確認等


NTT DATA