パネルディスカッション
ー企業のID管理担当者の10年ー

自己紹介：山田　達司

- NTTデータ技術開発本部 シニアスペシャリスト

  エバンジェリスト（ID管理、xR)

- (兼業）デジタル庁

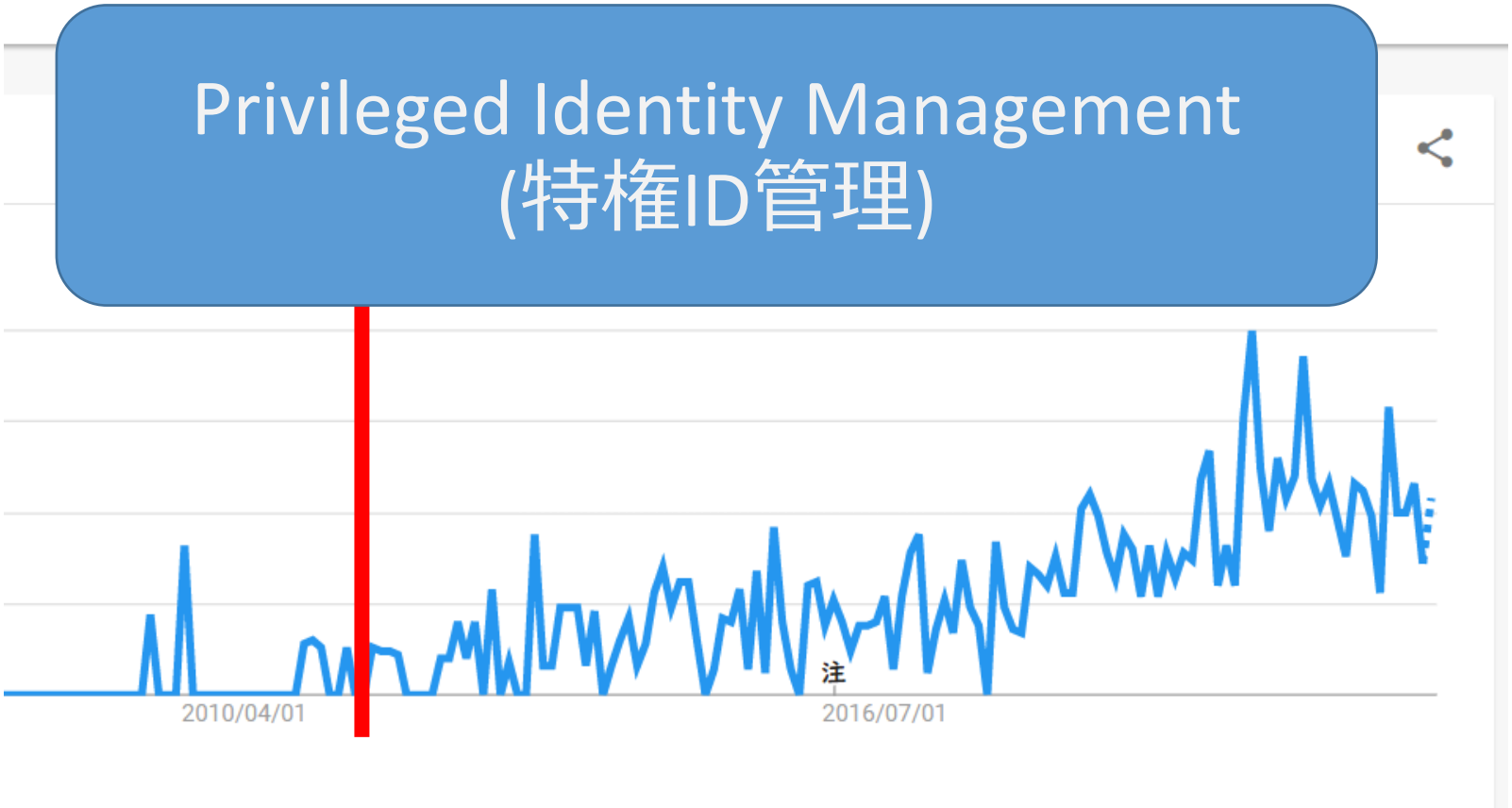
  プロダクトマネージャ（法人ID)

- 専門はセキュリティと先進ITデバイスによる働き方改革
- セキュリティ（統合ID管理/Identity Management）
  - NTTデータおよびデータGのID管理/認証基盤を構築/運用
  - 上記をVANADIS Identity Manager/SSOとして企画・発売。
  - 元Kantara Initiative Japan WG 代表
- 先進ITデバイス
  - 電子手帳ブームの際にPalm OS機用の日本語OS等を開発。
  - 書籍執筆、開発者支援サイト運営。ネット用語「神降臨」元祖
  - VRによるオンライン仮想コミュニケーションシステムを構築
- 働き方改革
  - NTTデータにおけるフリーオフィス、ペーパーレスなどの試行
  - 総務省「テレワークセキュリティガイドライン第4版、 5版」策定委員等 テレワーク普及に尽力
  - 経団連と連携し、「研究開発における技適の規制緩和」を実現

企業のID管理におけるこの10年

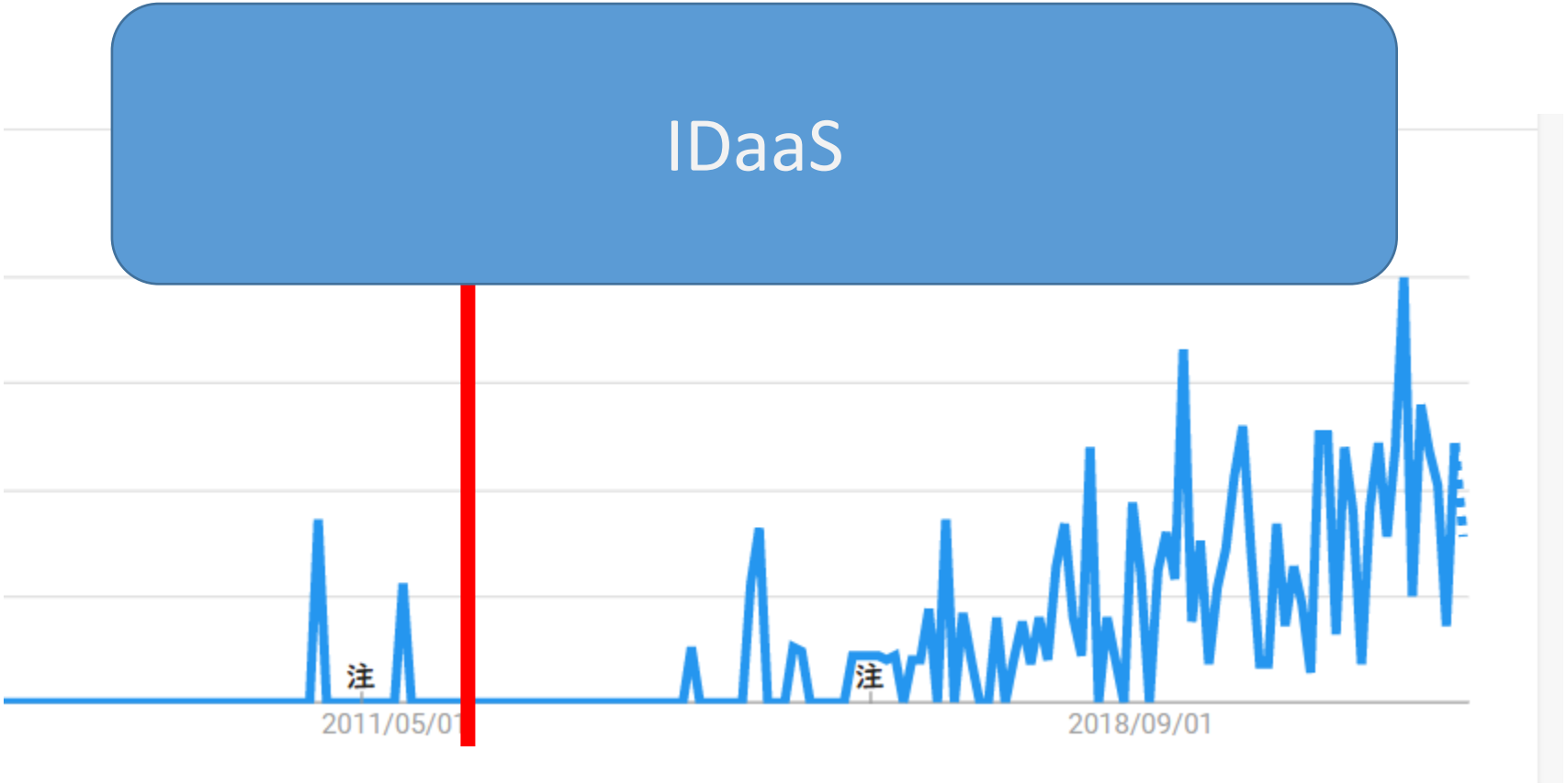
10年前ってどんな時期？

Google Trendによる検索数の推移



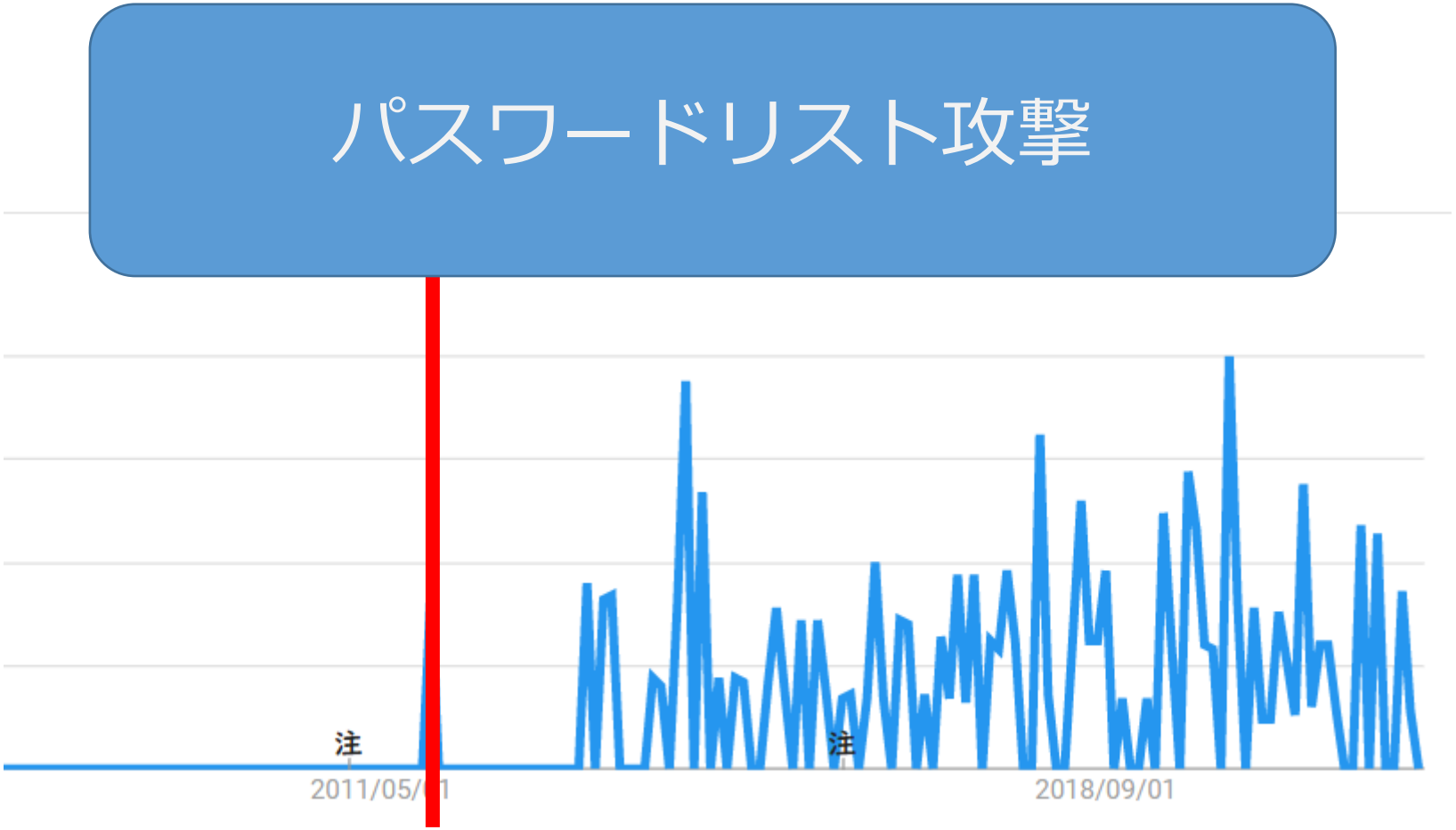
10年前ってどんな時期？

Google Trendによる検索数の推移



10年前ってどんな時期？

Google Trendによる検索数の推移

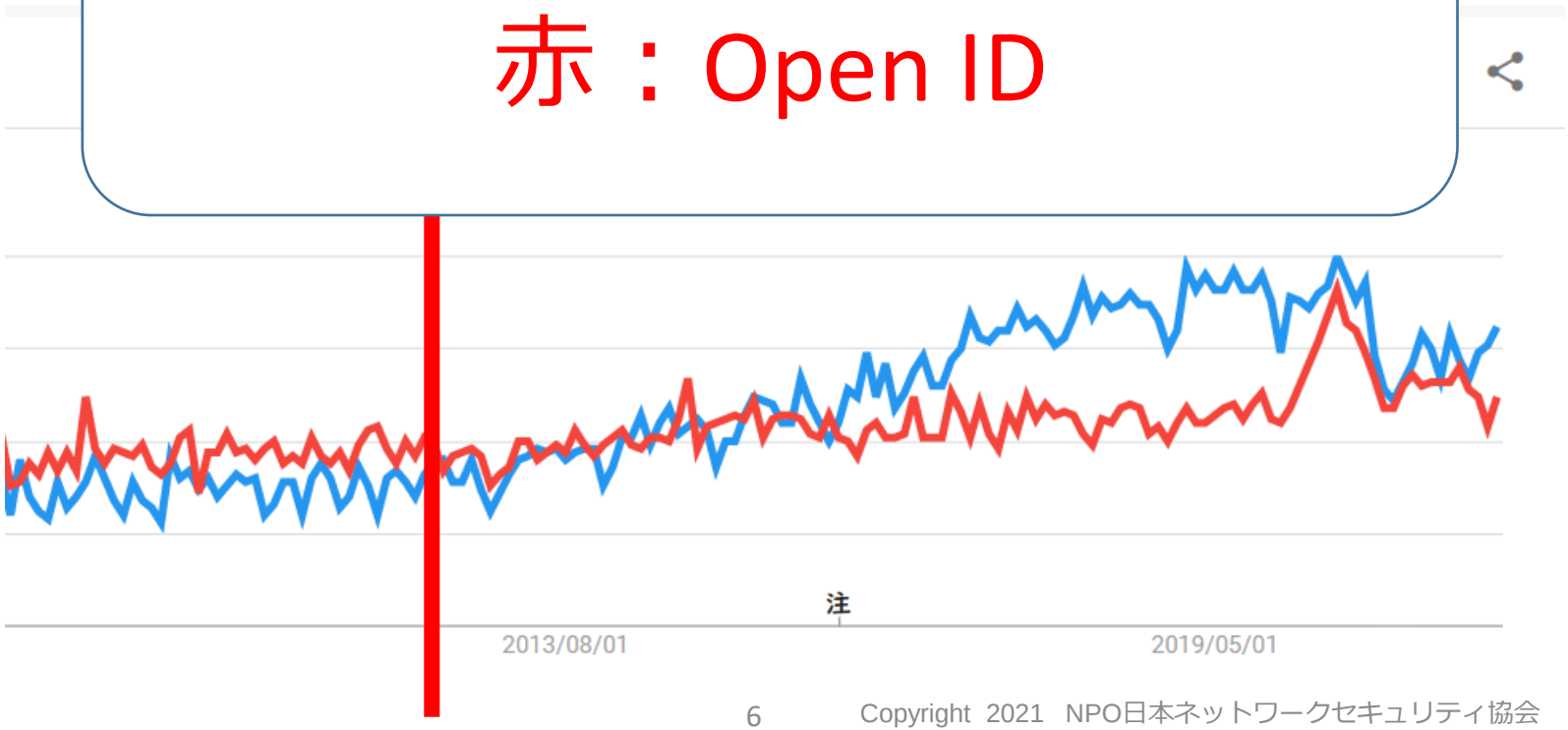


10年前ってどんな時期？

Google Trendによる検索数の推移

青：SAML

赤：Open ID

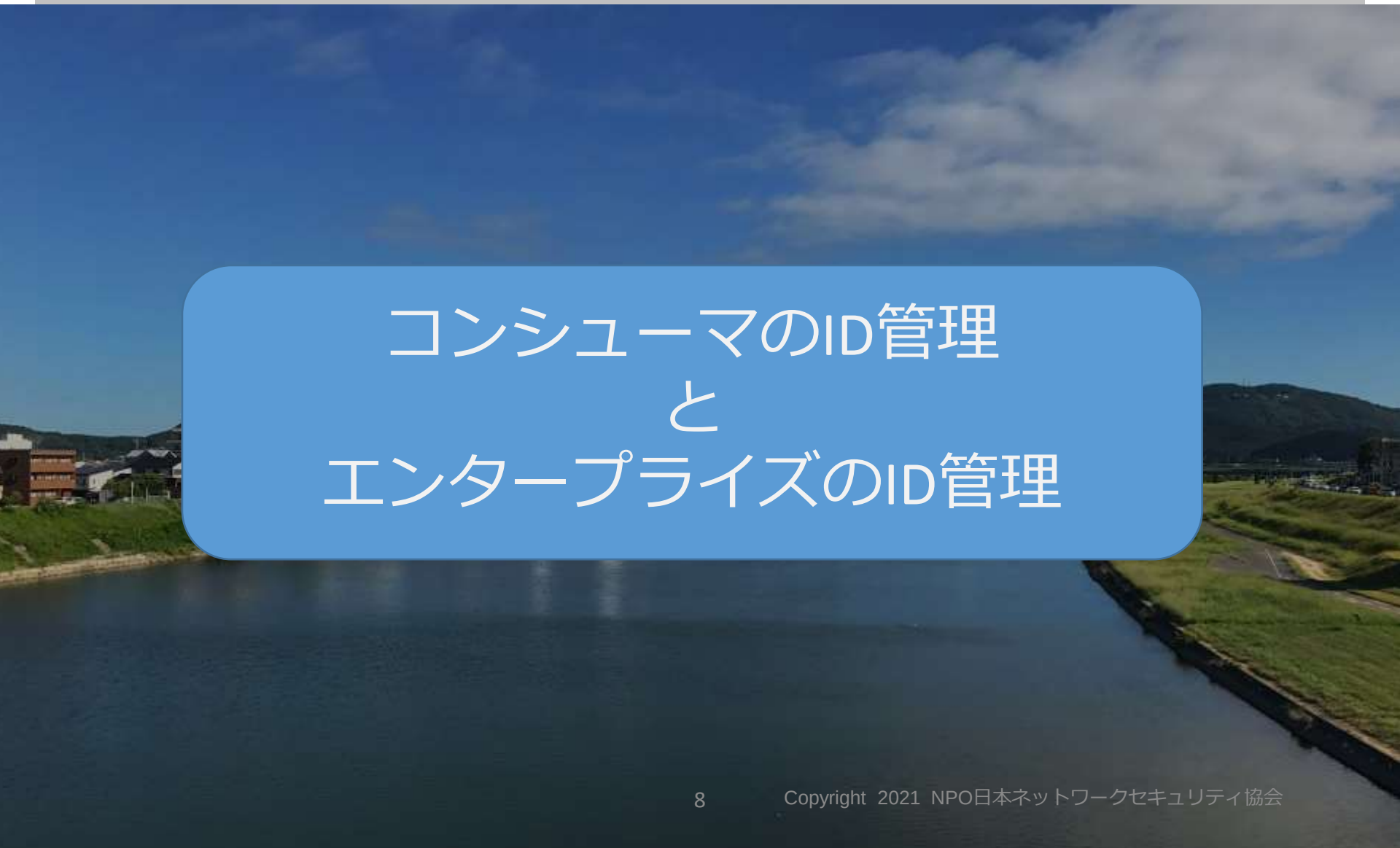


10年前ってどんな時？

- 影も形もない
  - マイナンバー/マイナンバーカード
  - FIDO
  - “Identity is the new Perimeter “（当然ゼロトラスト）

（ググると私の記事が出てきます）

横たわる広くて深い河



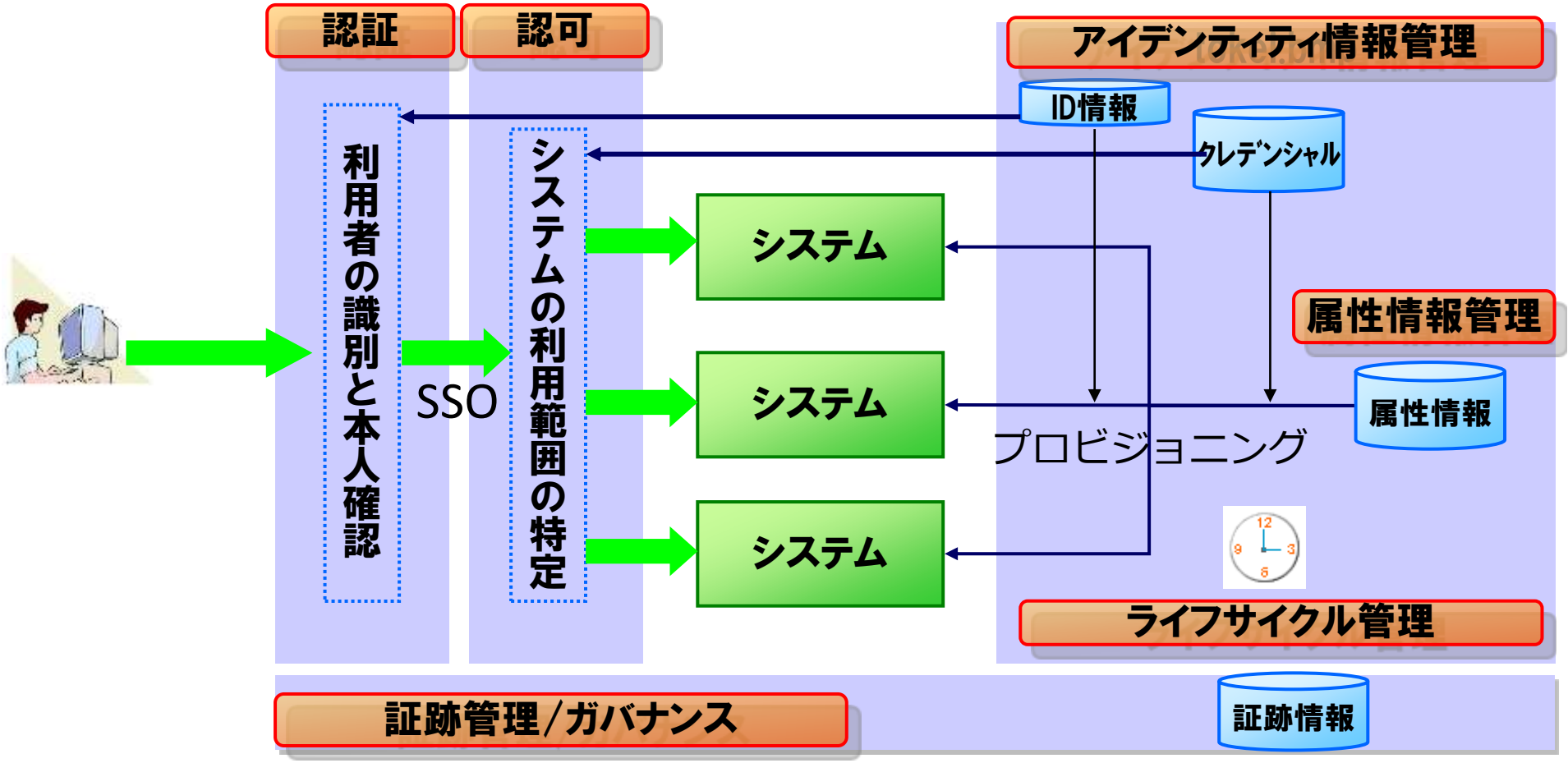
コンシューマとエンタープライズ

- コンシューマ
  - とにかくユーザを獲得。メールアドレスが命
  - Open ID：Yahoo, Line,などがアイデンティティエコノミー
  - 生体認証、 Password is dead

- エンタープライズ
  - 年度ごとの棚卸、組織変更、ID新規作成処理が地獄
  - パスワードがなくなるなんて考えられない。
  - SSOやれって言われたんだけど、高い…

- そもそも体系化された知識が徹底的に不足

- ID管理＝Open ID、 SAML,、 LDAP、 PKI等ごくわずかな標準。それ以外はすべて独自の設計、実装が必要



（閑話休題）IDとは何か？

- IDentifier:識別子
  - 「社員番号をIDとして入力」
- IDentity：アイデンティティ
  - 「半年利用がないとIDが無効化されます」
- Identity Document：身分証明書
  - 「IDを見せてください」

かけられた橋

10年で進んだ相互理解

- IDライフサイクル管理（E→C）
  - 身元確認の重要性

- 認証/SSO（C ⇔ E）
  - SAML/Open IDによるFederation/SSO/クラウド利用
  - 操作の重要性に合わせた多要素認証

理解が進んだ理由

環境の変化
- クラウド
- モバイル
- IDに対する攻撃の激化
- テレワーク：ゼロトラスト

様々な取り組みによる知識の体系化と蓄積
- 当WG作成各種ドキュメント
- 「デジタルアイデンティティー」 (Nat崎村)
- NIST SP-800-63-3他

（「統合ID管理入門」をググッてみてください…）

いまだに残る大きな違い

- 認可：
  - C：認可とはアプリの契約の有無に基づく利用可否。
    今の注目は属性ベースの認可(ABAC)
  - E：認可とはアプリの利用可否＋業務ごとの詳細な制御
    偽ロール管理から本物への移行が必要。
    委任、引継ぎも必要

根本原因はモチベーション？

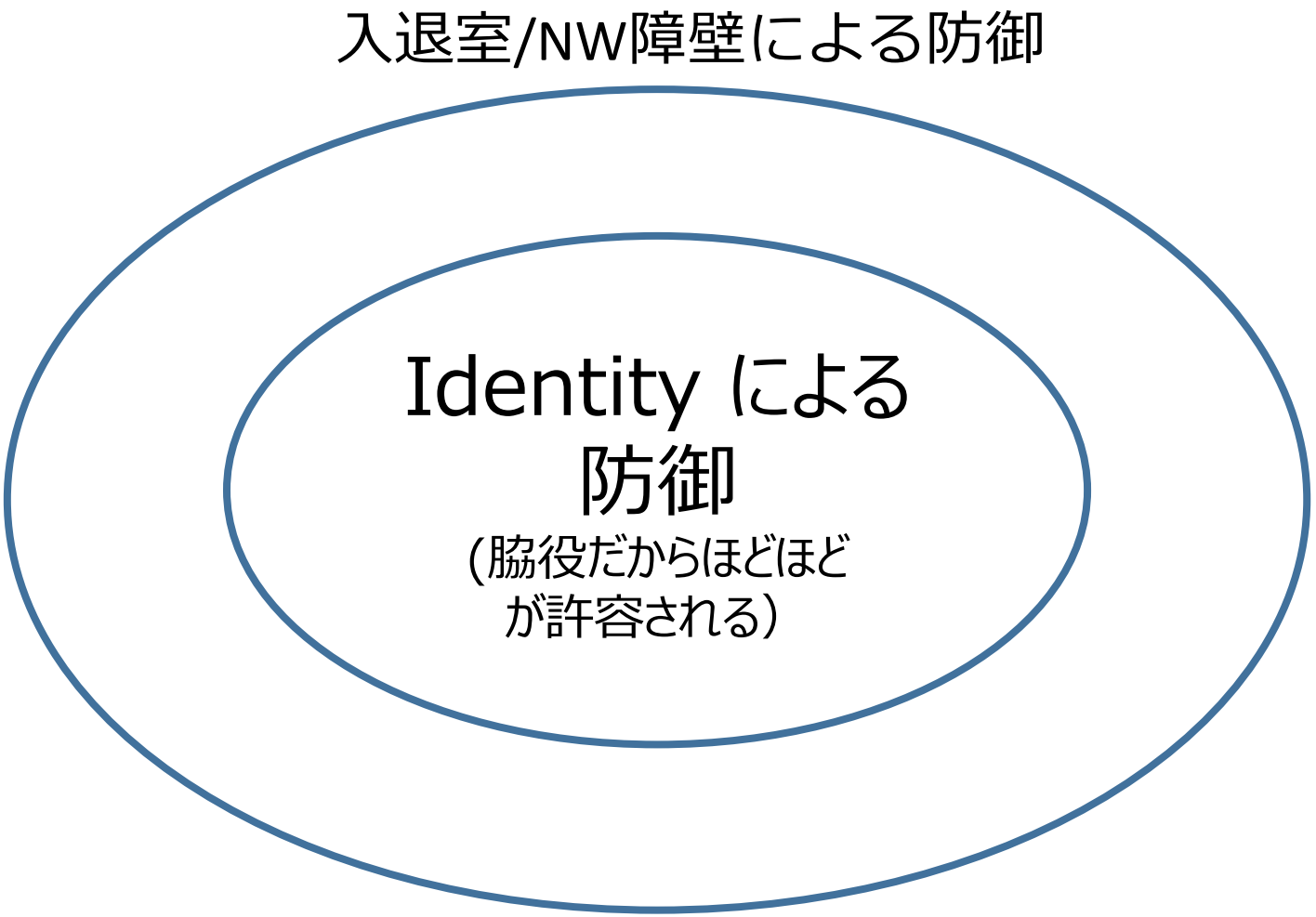
- コンシューマ
  - ユーザビリティ向上によるユーザ獲得
  - セキュリティ
  - プライバシー保護（違反によりたたかれたくない）
  - ビジネス継続

- エンタープライズ：
  - セキュリティ
  - コンプライアンス

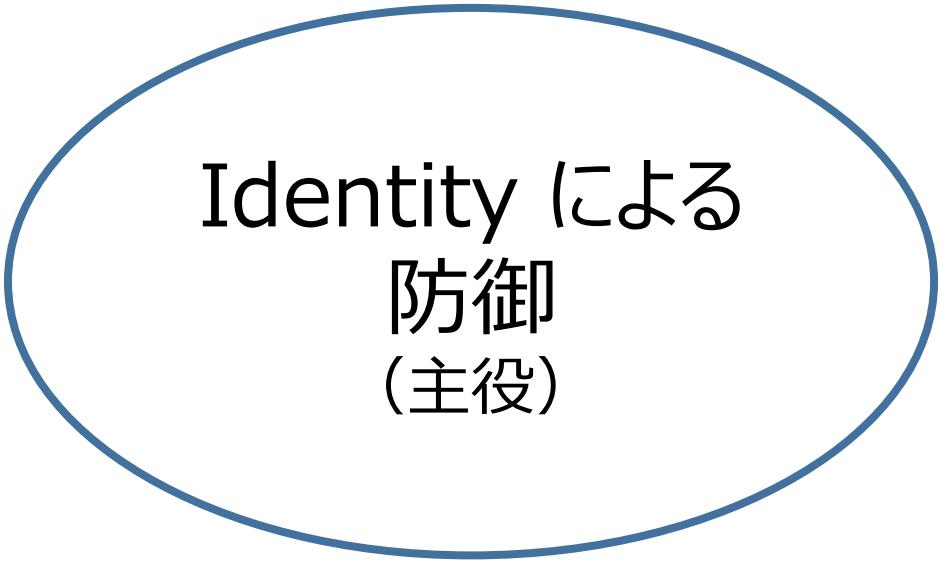
    .

    .
  - ユーザビリティによる業務効率向上、人材獲得

ゼロトラストとは？



ゼロトラストとは？



ゼロトラストとゼロトラストでないもの

ゼロトラストな考え方

けして信頼せず、必ず検証する

ゼロトラストではない考え方

・イントラネットは安全、インターネットは危険

・オフィス内は安全、オフィス外は危険

・会社配布端末は安全、私物は危険

・社員は信頼できる。社員以外は信頼できない

・自組織メンバーは信頼できる
他組織メンバーは信頼できない

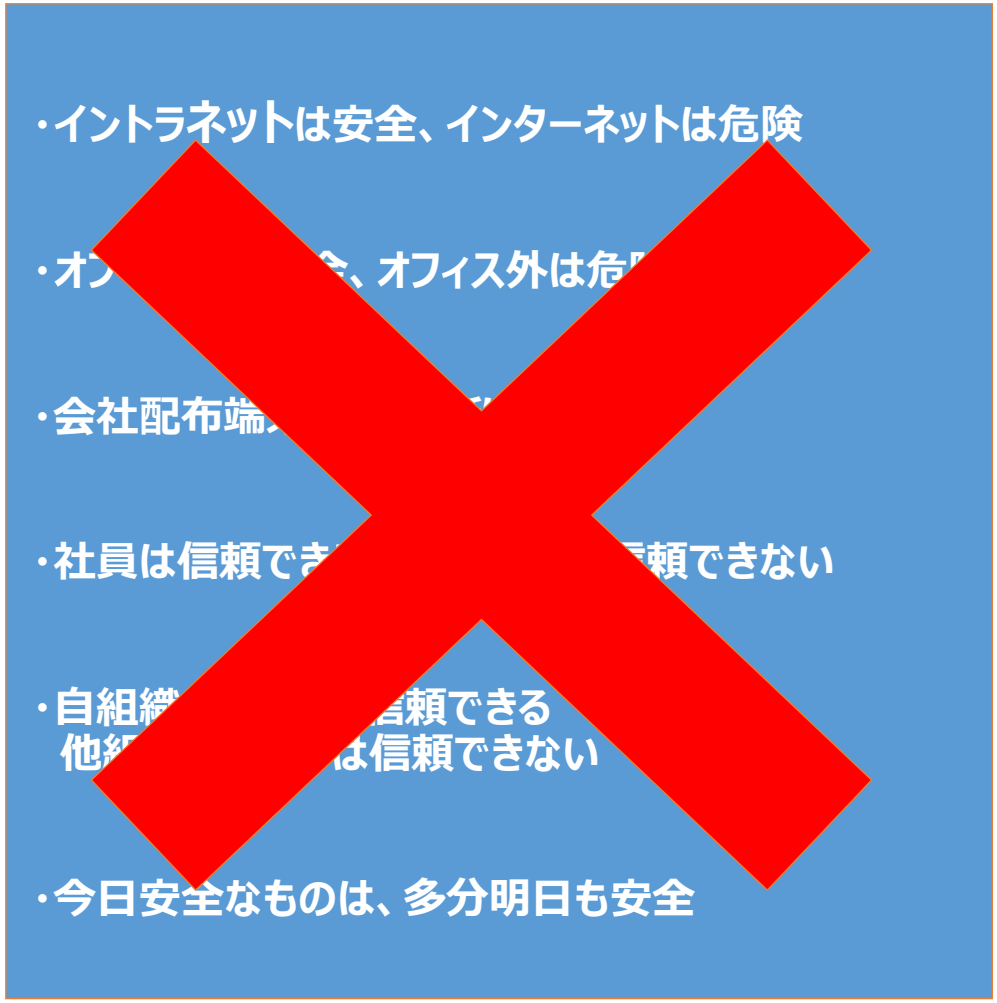
・今日安全なものは、多分明日も安全

ゼロトラストとゼロトラストでないもの

ゼロトラストな考え方

けして信頼せず、必ず検証する

ゼロトラストではない考え方



最小権限とは

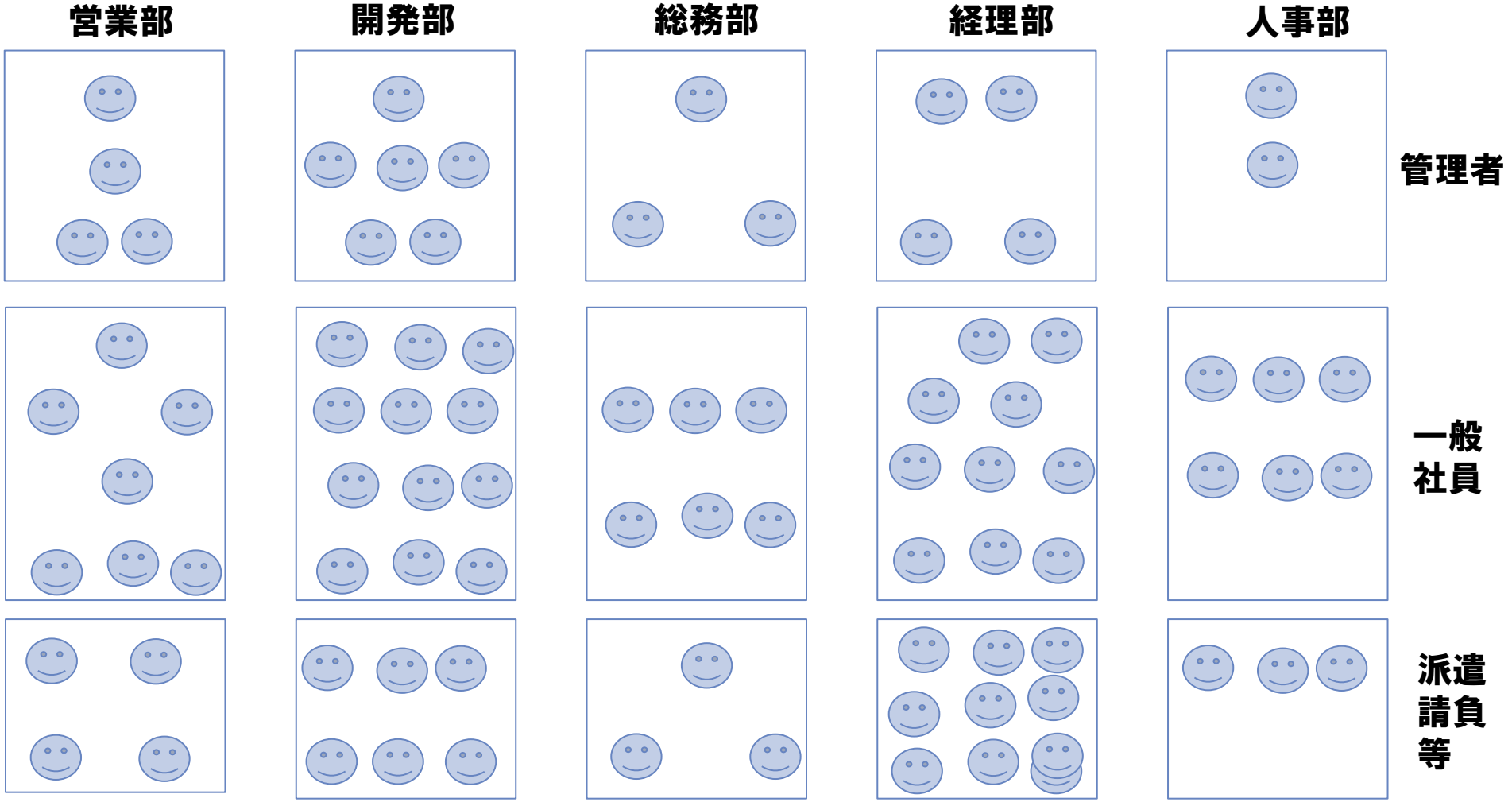
最小権限の原則とは、情報セキュリティや計算機科学などの分野において、コンピューティング環境の特定の抽象化レイヤー内で全てのモジュール（主題によっては、プロセス、ユーザー、プログラム）がその正当な目的に必要とされる情報と計算資源のみにアクセスできるように制限する設計原則である[1][2]。

Wikipedia**より**

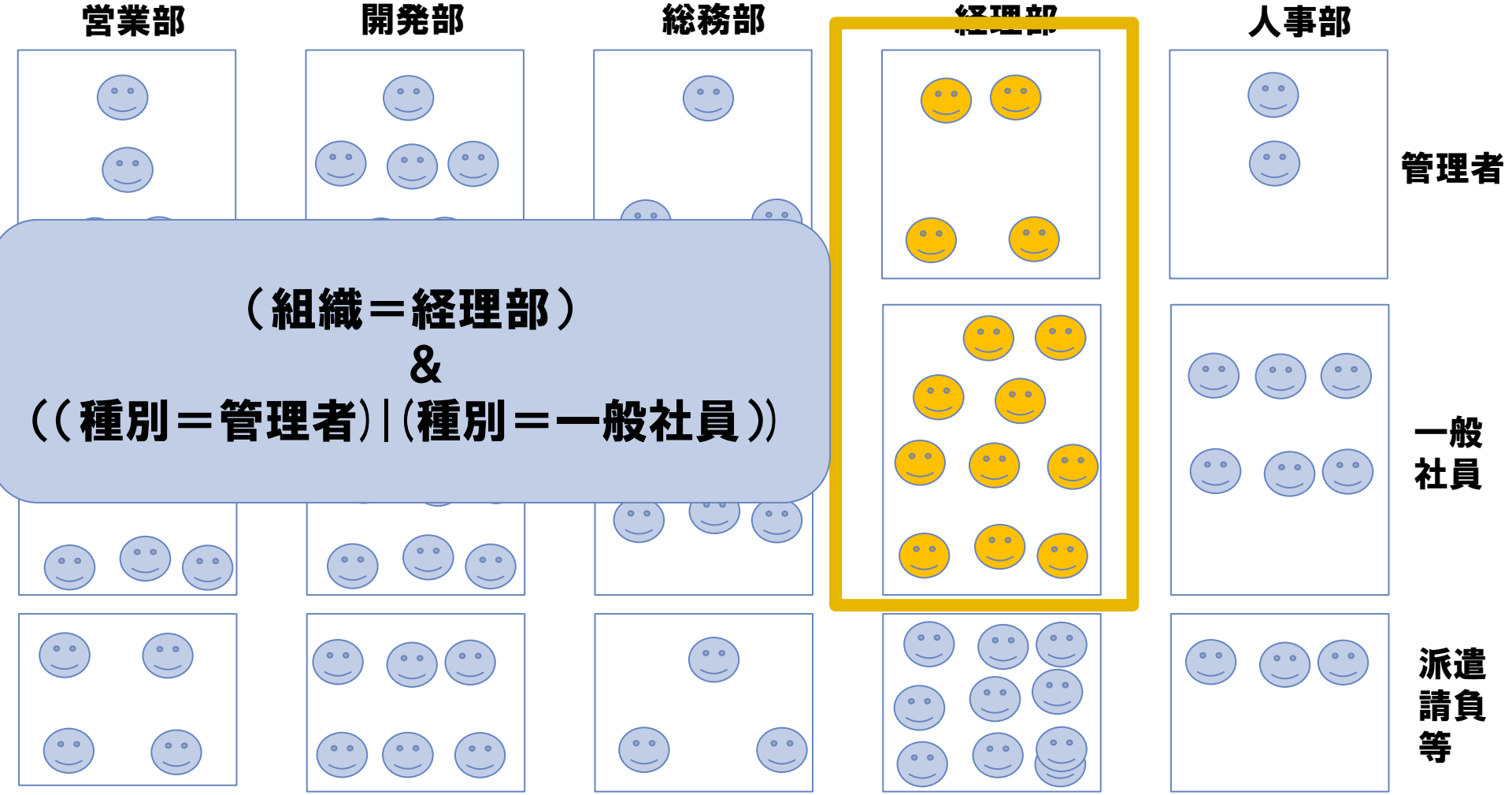
https://ja.wikipedia.org/wiki/%E6%9C%80%E5%B0%8F%E6%A8%A9%E9%99%90%E3%81%AE%E5%8E%9F%E5%89%87

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

ちゃんと認可をしようよ。

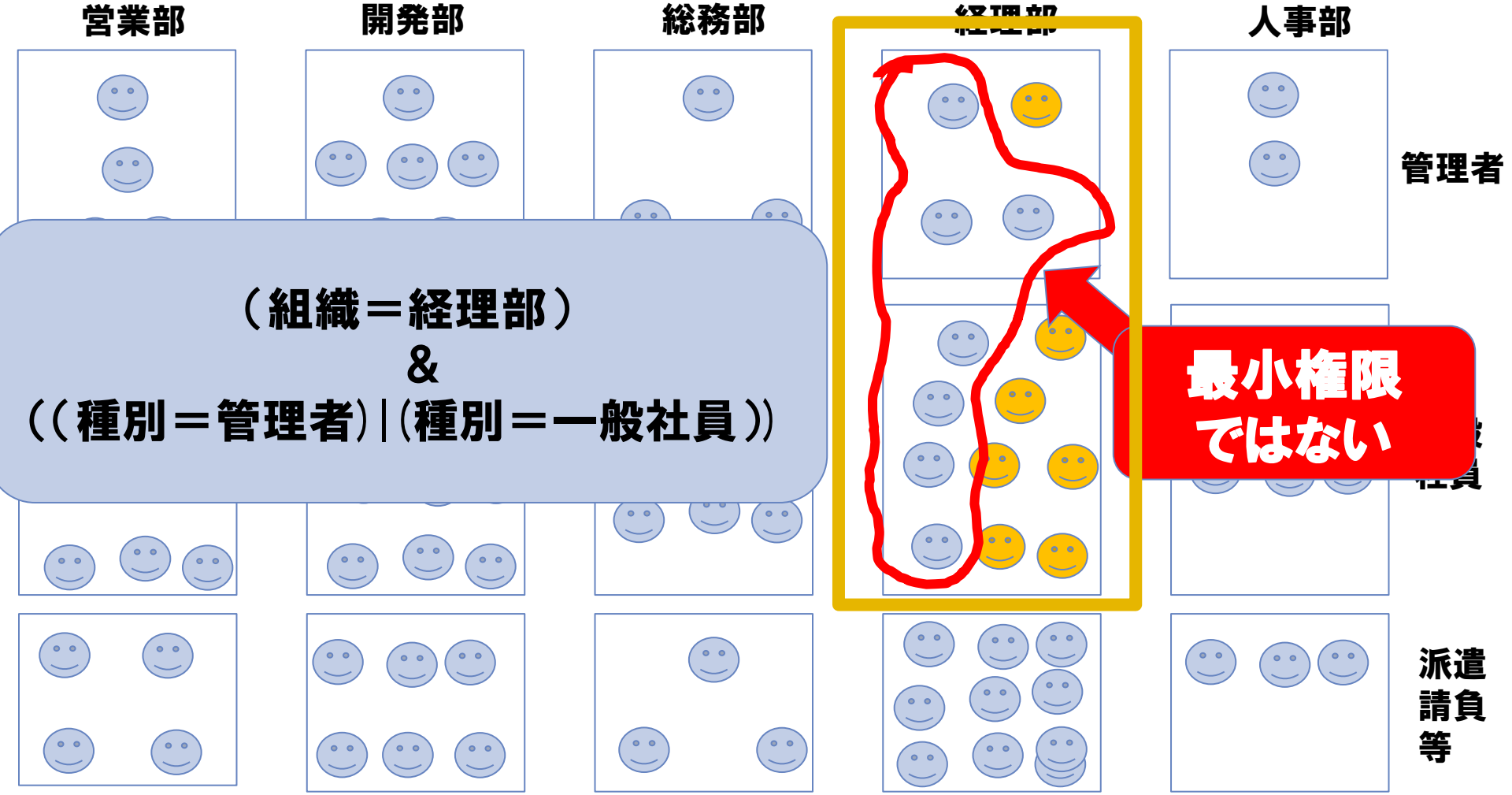


業務上システム利用権・アクセス権を持つ人

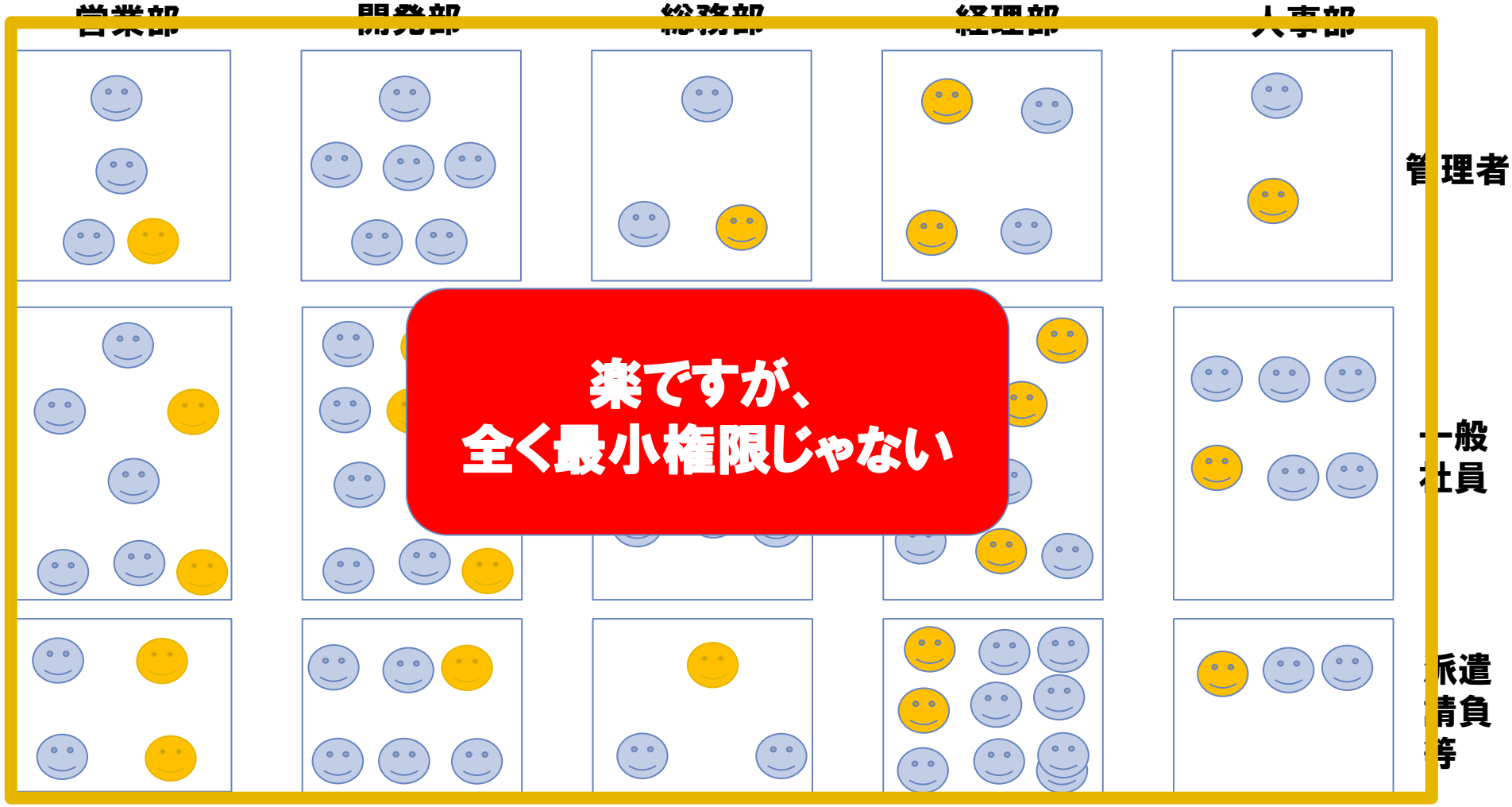


ちゃんと認可をしようよ

業務上システム利用権・アクセス権を持つ人

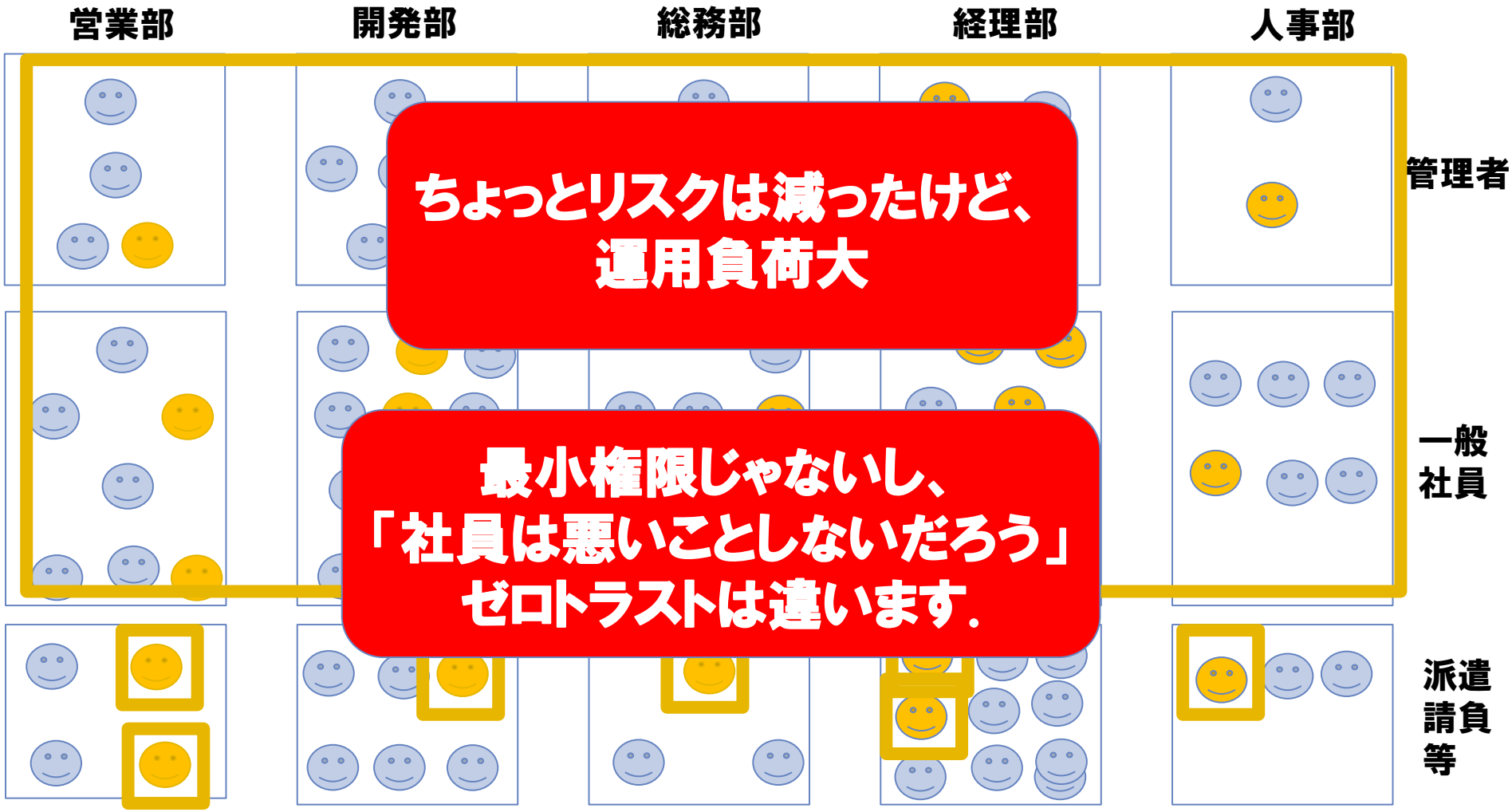


業務上システム利用権・アクセス権を持つ人

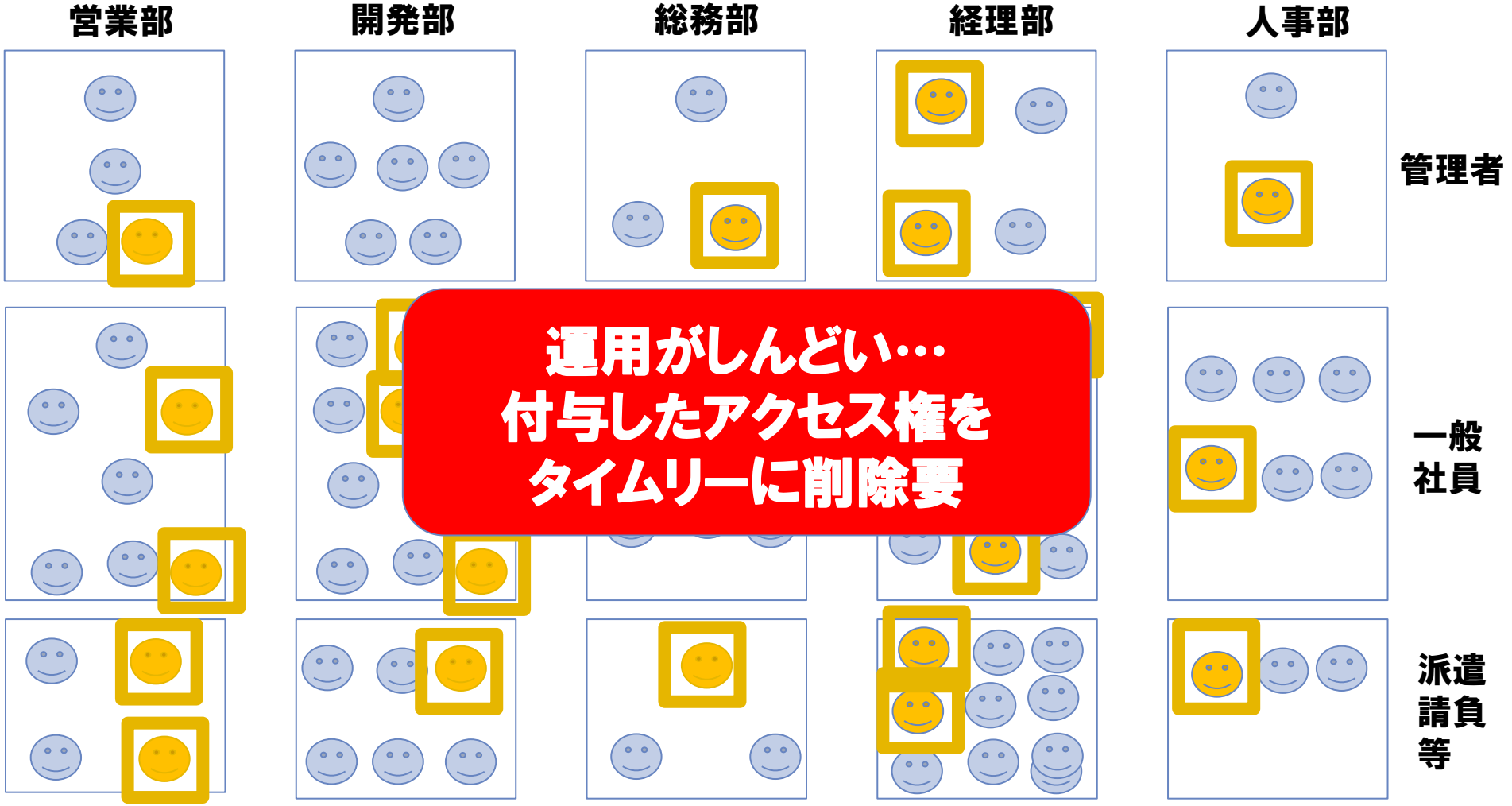


ちゃんと認可をしようよ

業務上システム利用権・アクセス権を持つ人

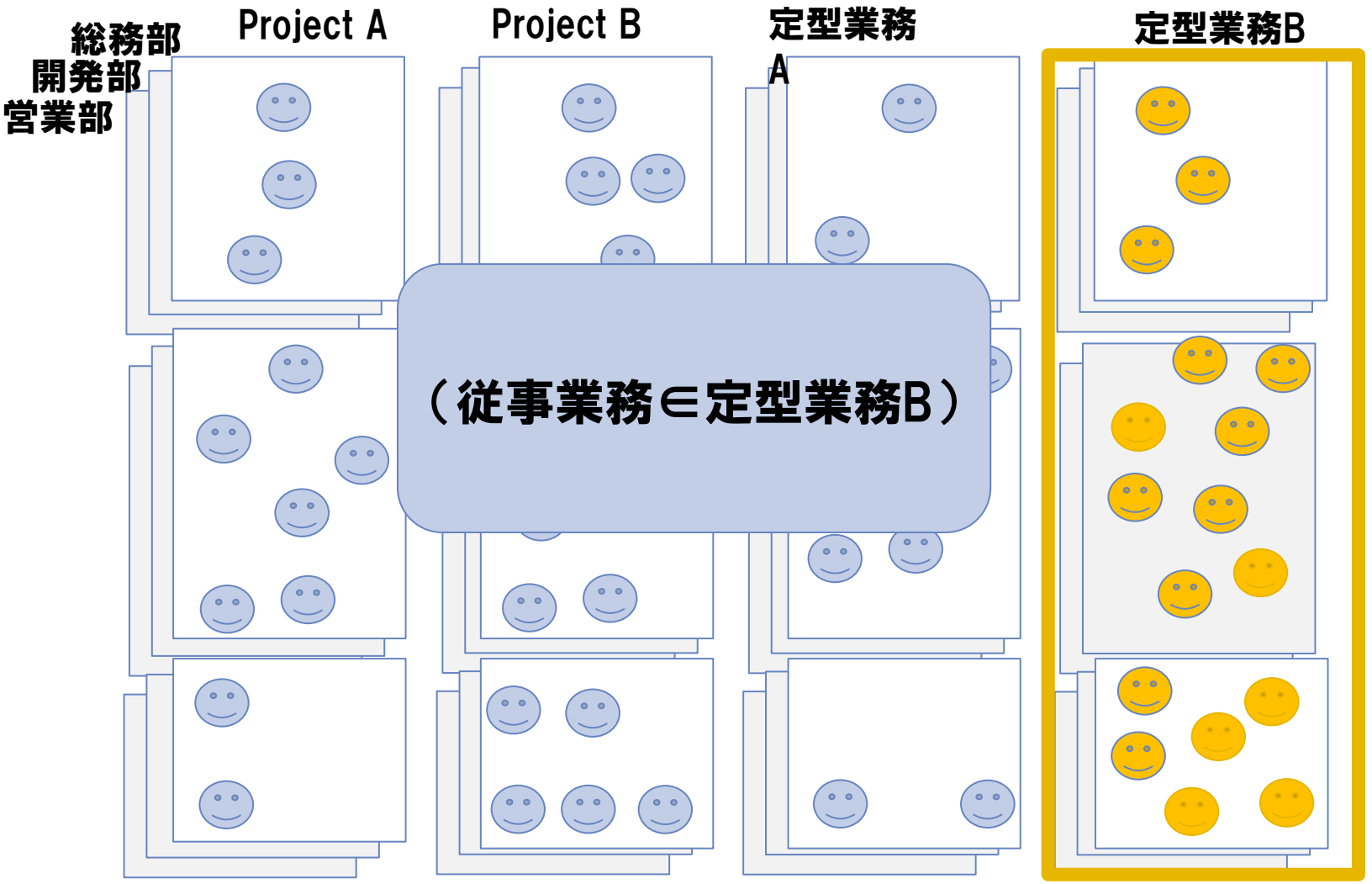


業務上システム利用権・アクセス権を持つ人



ロールベースアクセス制御により運用も利用も楽に

組織、人単位ではなく、ロール（役割）に基づくアクセス制御



最後に：働き方が変われIDMも変わる

NTT DATA

・人の範囲（人、協働者、派遣、アルバイト、委託先、サプライチェーン）
・人の身元確認（対面、オンライン）
・属性（役職、資格、所属、場所、時間等）に基づく認可と不正アクセス検知が統合化していく
・より迅速なオンボーディングのためID作成との権限付与
・＆迅速なID、権限の削除
・セキュリティとIdentity Managementはちゃんと連携できていますか？

・これらは根性や努力ではなく、システムで担保されるべき。