

現場でのグローバルID 管理システムのニーズ と課題

富士榮 尚寛

@phr_eidentity

グローバルID管理に関するニーズ

- **現場で聞く声**
 - 海外拠点とも情報共有を迅速に行いたい
 - グローバルでのポータル・グループウェア展開
 - 出張しても同じPC環境で仕事をしたい
 - NW基盤、認証基盤の統一
 - パブリッククラウドを全世界で使いたい（小規模拠点にわざわざシステムを入れたり管理者を置きたくない）

実現したいことはアプリケーションの共通利用、しかし結局は

グローバルで使える統一されたアイデンティティ管理基盤が必要

・・・しかし実際にシステム化を行おうとすると色々と課題も

ID管理システムを設計する際の検討事項

・ アイデンティティ管理システムの構成要素

構成要素	役割概要
プロビジョニング	他システムへのアイデンティティの伝搬 - 連携先のアカウント保守（作成、編国、削除）
IDプロセスサービス	ライフサイクルに係るプロセスの管理 - 源泉からのデータ取り込み - ワークフロー、セルフサービスなどでの保守
レポジトリ	アイデンティティ情報ストア - 属性 - プロビジョニング先との紐付け

・ システム化を行う際の視点

視点	概要
法令・文化	遵守すべき法令、業界標準、社内ルール、企業文化
組織・人事	採用～退職までのライフサイクル、雇用区分
システム	連携するシステム間での属性のマッピング、I/F

グローバルで設計する際の課題

	プロビジョニング	IDプロセスサービス	レポジトリ
法令・文化	個人属性の移送の可否	利用者の同意	保持できる属性 本名に関する考え方
組織・人事	組織改編のサイクル 引き継ぎバッファ 兼務	採用プロセス（レポジトリへの投入基準） 本人確認プロセス	役職や役割の統一 識別子の付番体系
システム	時差対応（バッチジョブスケジュール）	UIの多言語対応 時差対応（バッチジョブスケジュール）	文字コード（言語依存文字） 属性データの言語（英名、現地語名）

結局は・・・

独自の採用プロセス、源泉データ作成

認証データは各リージョンで複製を保持

アプリケーション側で個別情報のメンテナンス

属性の絞り込みと本人同意の取り付け、社内ルールでの調整

アプリケーションに最低限必要な属性の収集と伝搬

