ID管理/認証システム導入の理想と現実

2016/11/30

伊藤忠テクノソリューションズ株式会社
MVP for Enterprise Mobility

富士榮　尚寛 / Naohiro Fujie(@phr_eidentity)

自己紹介

- Blog
  - IdM実験室：http://idmlab.eidentity.jp
- Modules（codeplex）
  - Generic REST MA for FIM/MIM : https://restmafim.codeplex.com/
- 記事 / 書籍
  - 記事：@IT/企業のID管理／シングルサインオンの新しい選択肢「IDaaS」の活用 他
  - 監訳：クラウド時代の認証基盤 Azure Active Directory 完全解説
  - 共著：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
- その他
  - JNSA アイデンティティ管理WG
  - OpenID Foundation Japan 教育・翻訳WG、エンタープライズ・アイデンティティWG
  - Microsoft MVP for Enterprise Mobility（Jan 2010 -）

アジェンダ

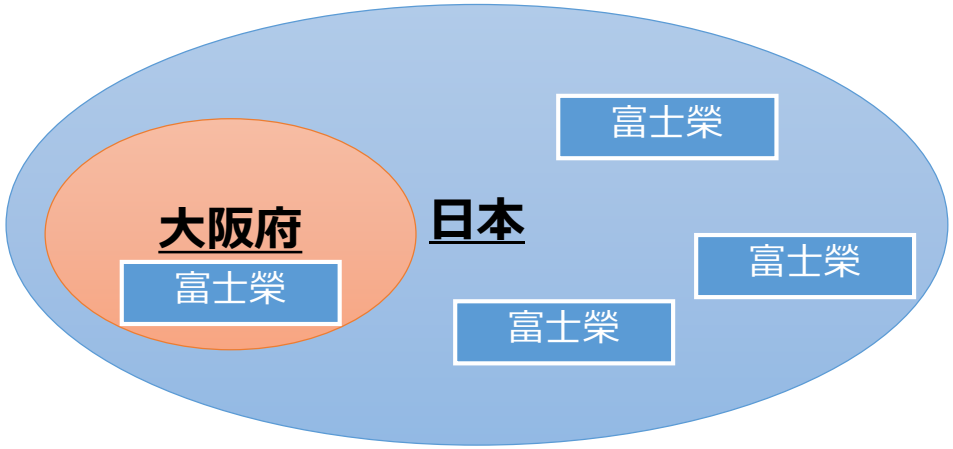
1. 企業におけるIDの利用用途と管理の目的
   - そもそもIDとは？管理とは？
   - 企業におけるIDの利用用途と管理の目的
2. ID管理のシステム化とは？
   - ID管理・制御をシステム化する必要性
   - ID基盤を構成する要素と役割分担
   - 関連キーワード解説
3. ID管理／認証システム導入の理想と現実
   - 理想的なID基盤、ID基盤の現実
   - システム化の限界と発見的統制の重要性
4. 技術面からの現実的アプローチ
   - 具体的なシナリオとデモ
5. まとめ

主にポリシー（非技術）面から
理想と現実についてお話します。

技術面から見たアプローチと、
サンプルシナリオをデモを交え
てお話しします。

1. 企業におけるIDの利用用途と管理の目的

そもそもIDとは？



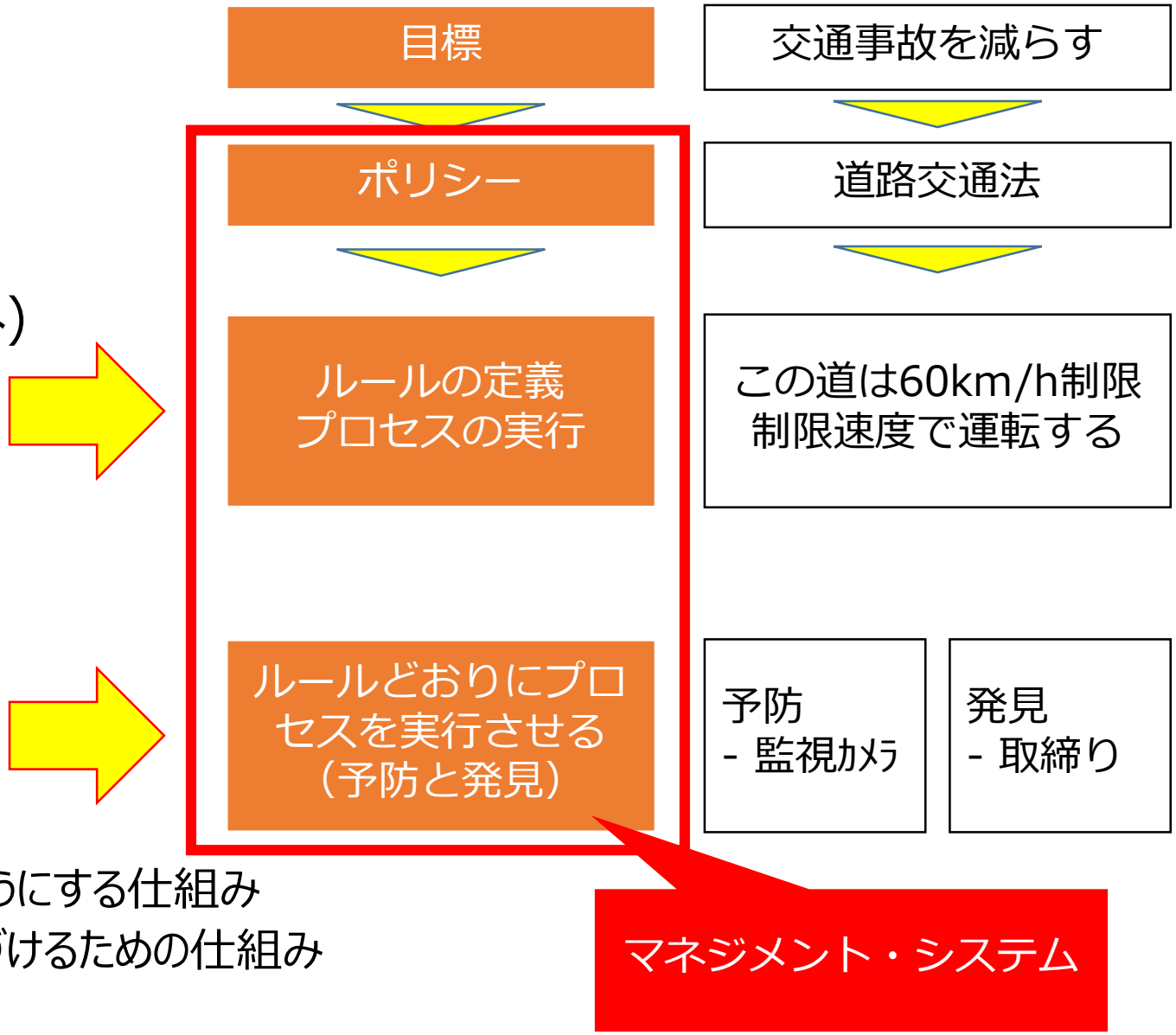
- IDは何の略？
  - **Id**entifier：識別子
    - 特定の集合の中で一意に識別するための属性情報（一つとは限らない）
    - 日本の中に「富士榮」は複数いるので苗字は識別子にならないが、大阪府の中なら苗字で識別できる
  - **Id**entity：アイデンティティ
    - 実体（人など）を構成する属性の集合（ISO/IEC 24760-1より）
    - 識別子もアイデンティティを構成する要素の一つ

「ID管理」で言うIDはこちら

要素	解説	例
属性	後天的に取得された主体に関わる情報（後から変化する）	名前、電話番号、社員番号、メールアドレス、認証状態、位置情報
好み	主体の嗜好に関わる情報	甘いものが好き
形質	主体の先天的な特有の性質（後から変化しにくい）	生年月日、性別？
関係性	他の主体との関係に関わる情報（一部属性と重複）	XX大学卒業、YY部所属

管理とは？

- 2つの管理
  - **Management**（マネージメント）
    - Do Right Things
    - 何が正しい状態なのかを定義する
    - ルール化、手順化
  - **Control**（コントロール）
    - Do Things Right
    - 正しい状態へ持っていく
    - 制御、統制
    - 予防的：抑止力、違反できないようにする仕組み
    - 発見的：証拠、違反したことを気づけるための仕組み



企業におけるIDの利用用途と管理の目的

- IDの利用用途
  - 業務に必要なITシステムや情報を利用させること
- ID管理の目的
  - **正しい利用者に**業務に必要なITシステムや情報を**正しく**利用させること
- ITシステムを利用させるために必要なプロセス
  - 「正しい利用者に」
    - **識別**（Identification）：利用者を他者と区別する
    - **認証**（Authentication）：利用者の正当性を検証する
  - 「正しく利用させる」
    - **認可**（Authorization）：利用者応じた権限を与える

これらのプロセスを管理・制御することが必要

2. ID管理のシステム化とは？

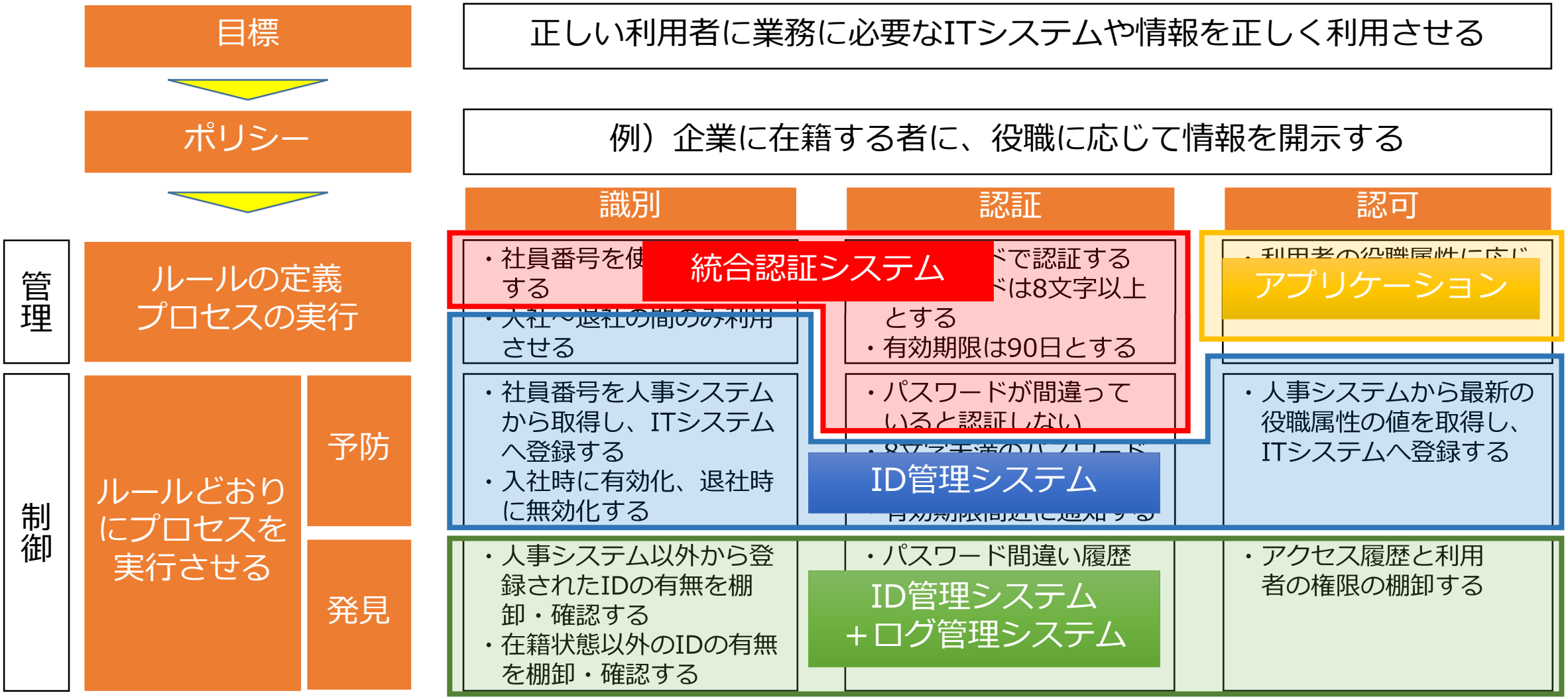
ID管理・制御をシステム化する必要性

		識別	認証	認可
目標	正しい利用者に業務に必要なITシステムや情報を正しく利用させる			
ポリシー	例）企業に在籍する者に、役職に応じて情報を開示する			
管理	ルールの定義 プロセスの実行	・社員番号を使って識別する ・入社～退社の間のみ利用させる	・パスワードで認証する ・パスワードは8文字以上とする ・有効期限は90日とする	・利用者の役職属性に応じて情報を開示する
制御	ルールどおりにプロセスを実行させる 予防	・社員番号を人事システムから取得し、ITシステムへ登録する ・入社時に有効化、退社時に無効化する	・パスワードが間違っていると認証しない ・8文字未満のパスワードを登録させない ・有効期限間近に通知する	・人事システムから最新の役職属性の値を取得し、ITシステムへ登録する
制御	ルールどおりにプロセスを実行させる 発見	・人事システム以外から登録されたIDの有無を棚卸・確認する ・在籍状態以外のIDの有無を棚卸・確認する	・パスワード間違い履歴を確認する ・パスワード期限切れのユーザ一覧の棚卸をする	・アクセス履歴と利用者の権限の棚卸する

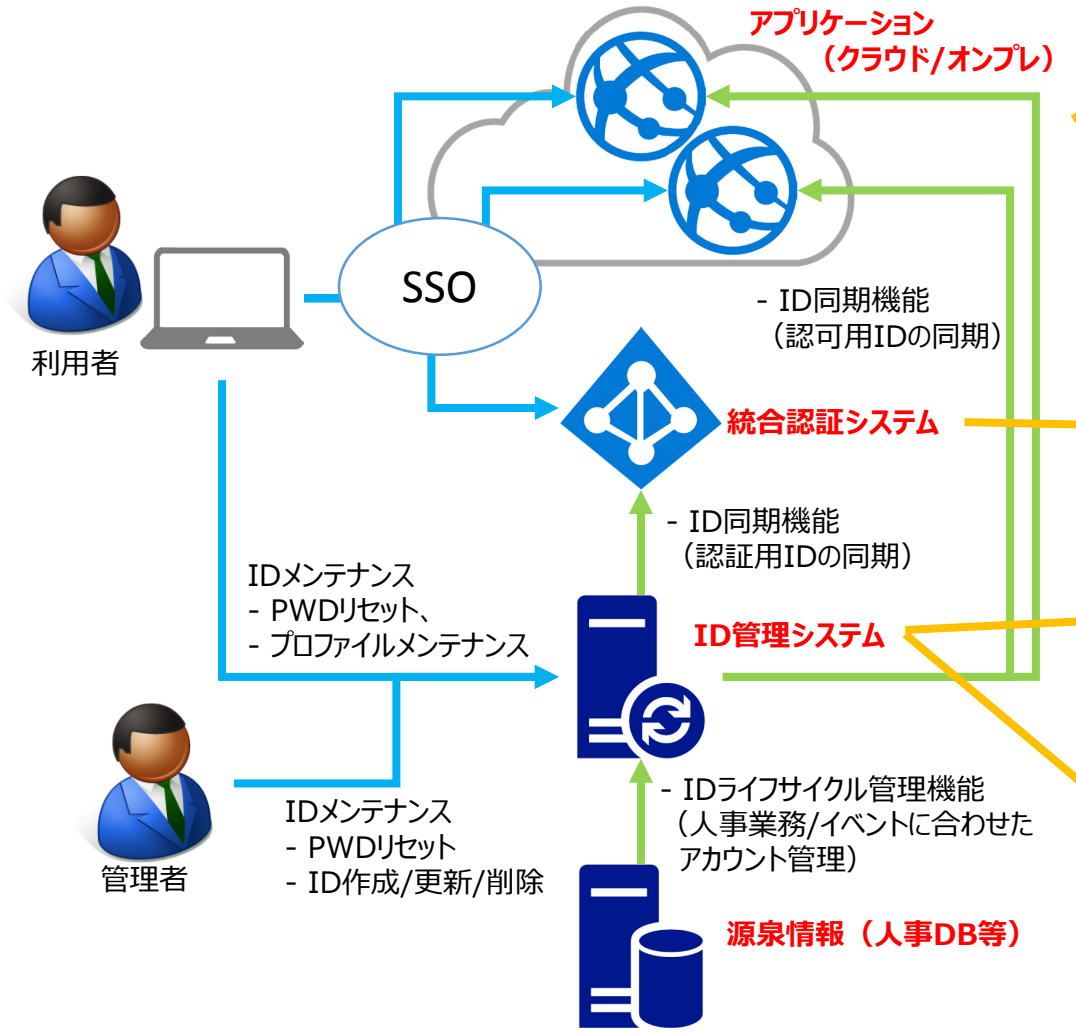
手動での管理・制御は不確実かつ煩雑

システム化（ID基盤の整備）が必要

ID基盤を構成する要素と役割分担



クラウド利用等による機能分離の必要性



認証/ID管理に関連する機能

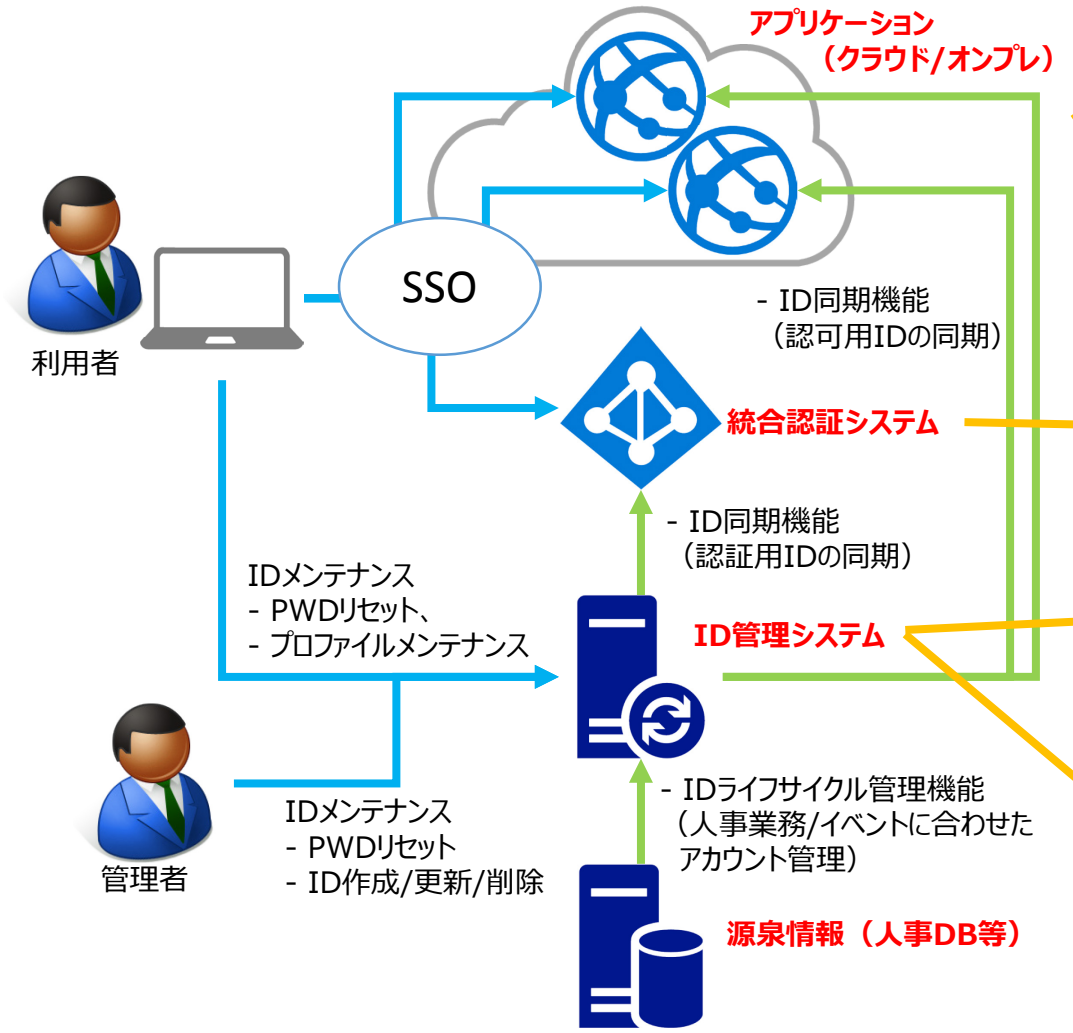
認可機能＝アプリケーション
- ログオン後、ユーザの権限（メニューを出す・出さない等）制御を行う

認証機能＝統合認証システム
- ID/PWDなどで利用者の正当性検証を行う

ID同期機能＝ID管理システム
- ID管理システムから認証システムやアプリケーションへ、認証や認可に使うID情報を同期する

IDライフサイクル管理機能＝ID管理システム
- ID情報を源泉（人事等）から取り込み、ID情報の精度・鮮度を維持する

クラウド利用等による機能分離の必要性



認証/ID管理に関連する機能

認可機能＝アプリケーション

- ログオン後、ユーザの権限（メニューを出す・出さない等）制御を行う

認証

- ID

認証/シングルサインオン

ID連携/フェデレーション

ID同期機能＝ID管理システム

- ID

プロビジョニング

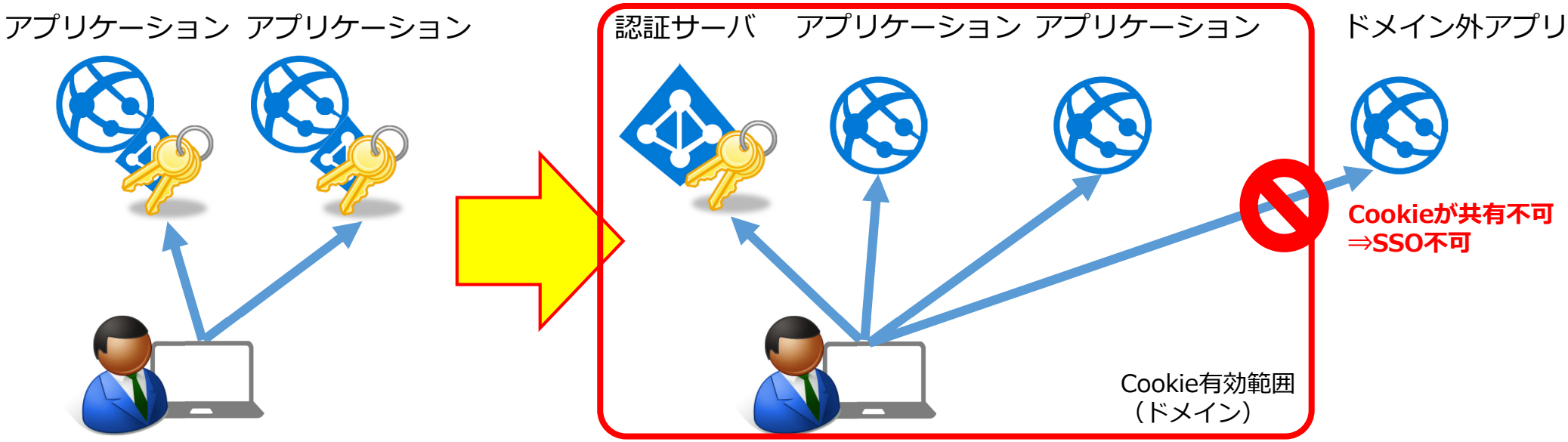
IDライフサイクル管理機能＝ID管理システム

- ID情報を源泉（人事等）から取り込み、ID情報の精度・鮮度を維持する

関連キーワード解説

認証/シングルサインオン）原始的なSSO

- シングルサインオン
  - アプリケーション毎に持っていた認証機能を外部へ出し一元化
  - 認証Cookieを共有することでシングルサインオンを実現



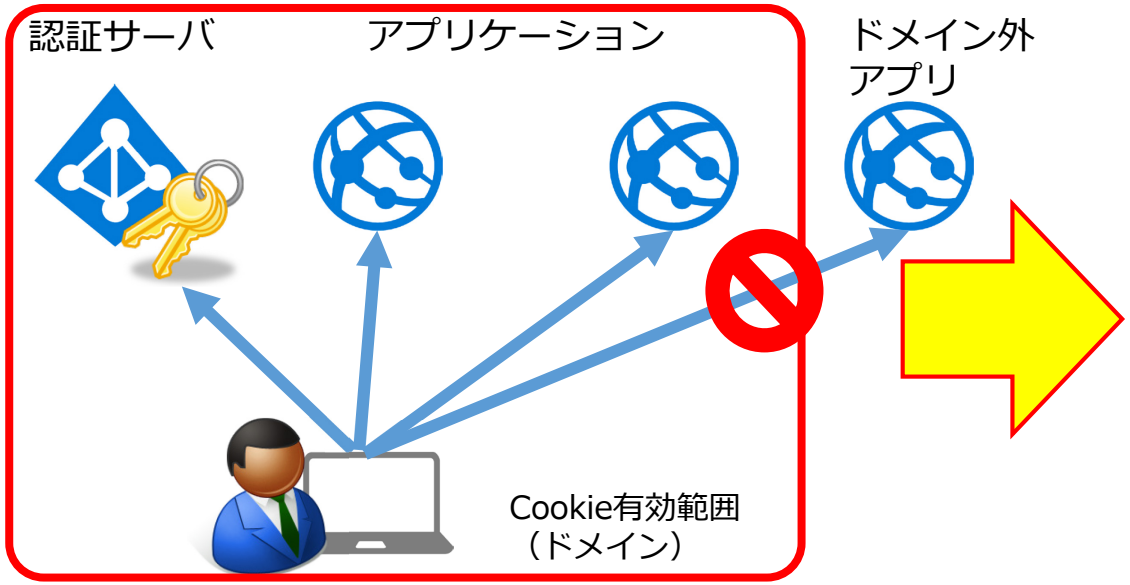
分散管理状態（SSO不可）

認証サーバの外部化、
認証Cookieを共有（SSO可）

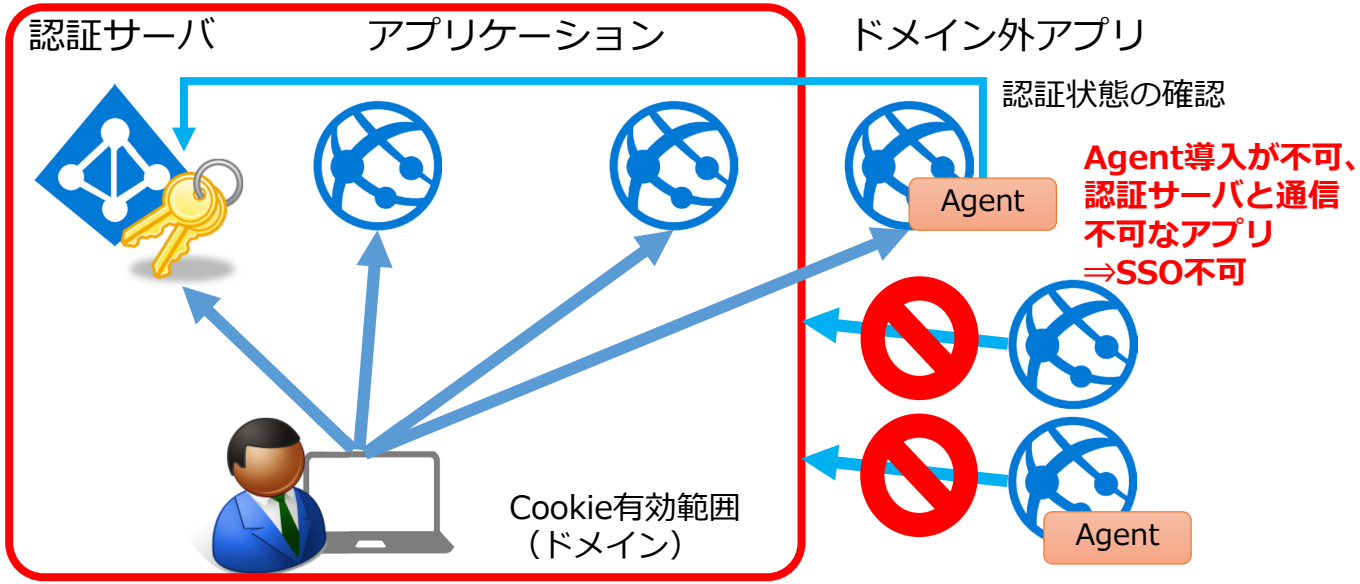
関連キーワード解説

認証/シングルサインオン）WAMの活用

- WAM（Web Access Management）による解決
  - アプリケーション側にAgentを導入し認証状態を確認、Cookieの有効範囲（ドメイン）を超えたSSOを実現



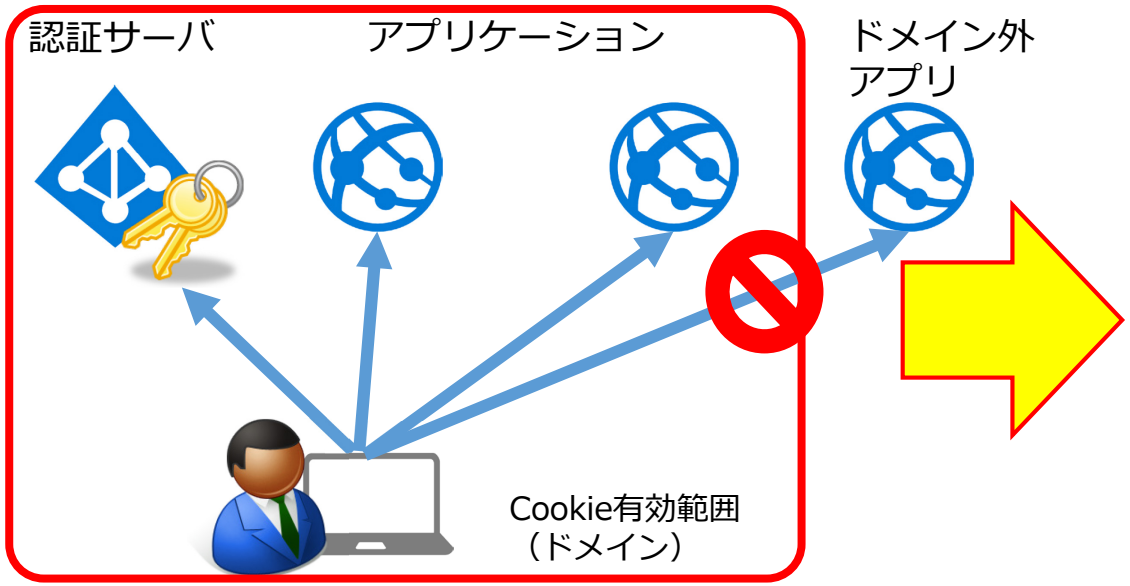
ドメイン内は認証Cookieを共有しSSO



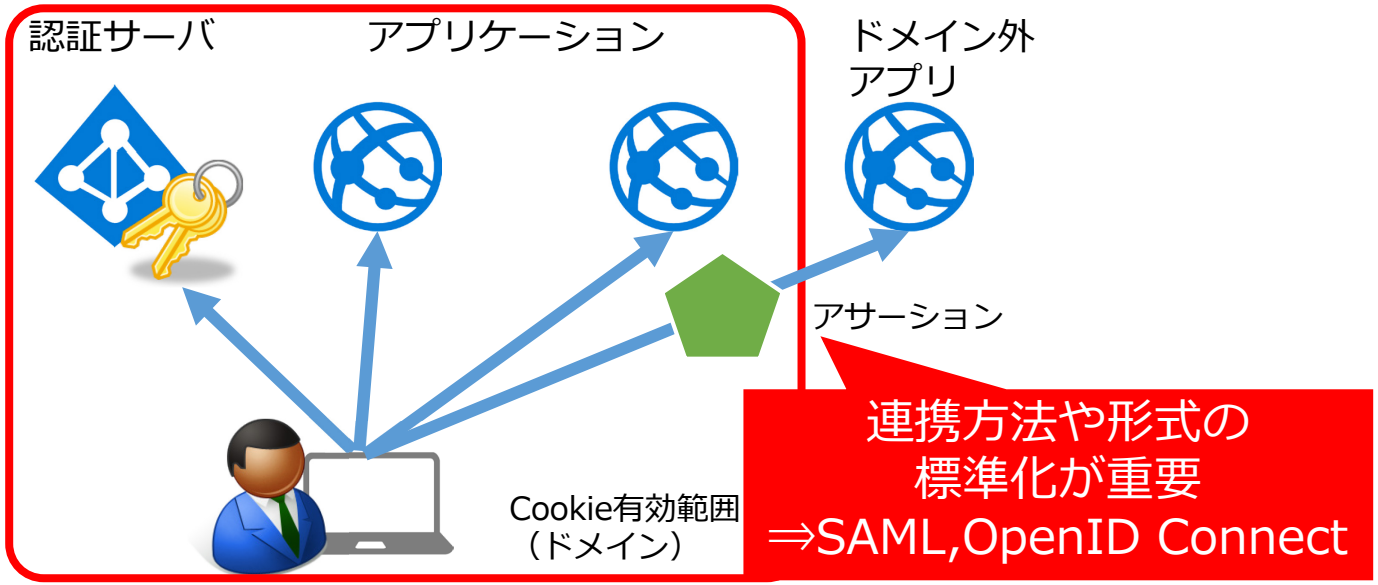
ドメイン内は認証Cookieを共有しSSO
ドメイン外はAgentが認証状態を問い合わせてSSO

認証/シングルサインオン）ID連携/フェデレーション

- ID連携/フェデレーションによる解決
  - 認証結果表明（アサーション）をクライアント（ブラウザ）を経由して受け渡すことにより、Cookieの有効範囲（ドメイン）を超えたSSOを実現
  - アプリケーションと認証サーバ間の直接の通信が不要なので、クラウドに最適



ドメイン内は認証Cookieを共有しSSO



ドメイン内は認証Cookieを共有しSSO
ドメイン外はアサーションを渡すことでSSO

関連キーワード解説

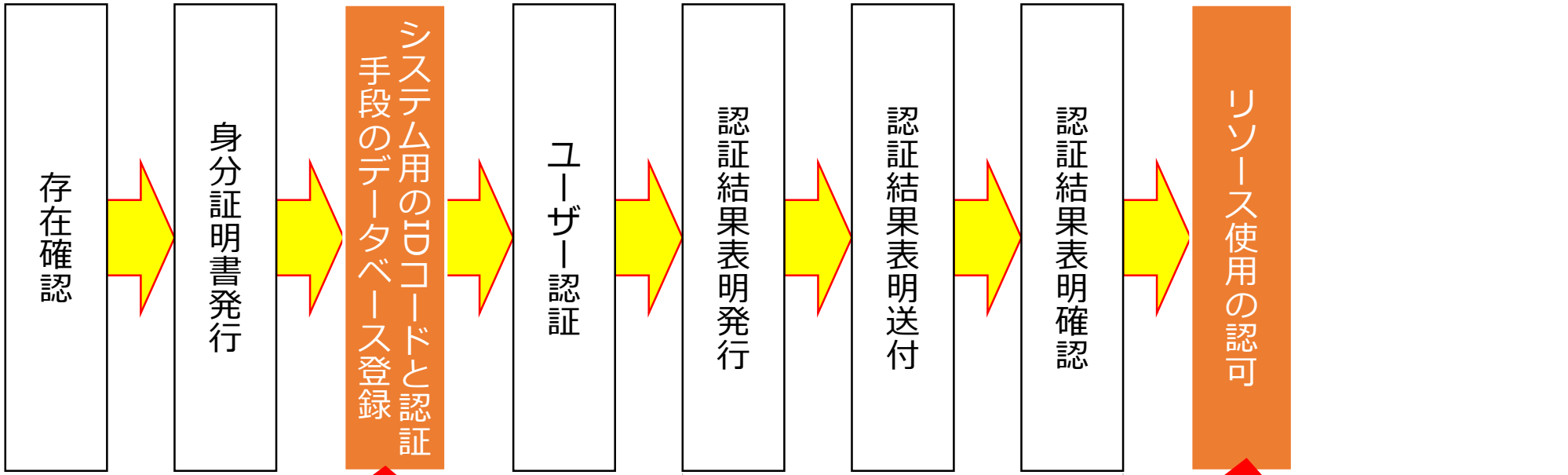
認証/シングルサインオン）構成の比較

構成パターン	ドメイン跨ぎのSSO	アプリケーション構成	アプリ⇒認証サーバ通信	適用対象の例
認証Cookieの共有	不可	同一認証Cookieを利用する必要あり	不要	小規模イントラネット、自前アプリのみ
WAM	可	Agent導入が必要	必要	大規模イントラネット、Agent導入可能アプリのみ
ID連携	可	ID連携プロトコルへの対応が必要	不要	大規模分散環境（イントラ/B2B/クラウド）

最近のニーズにはID連携パターンがマッチ

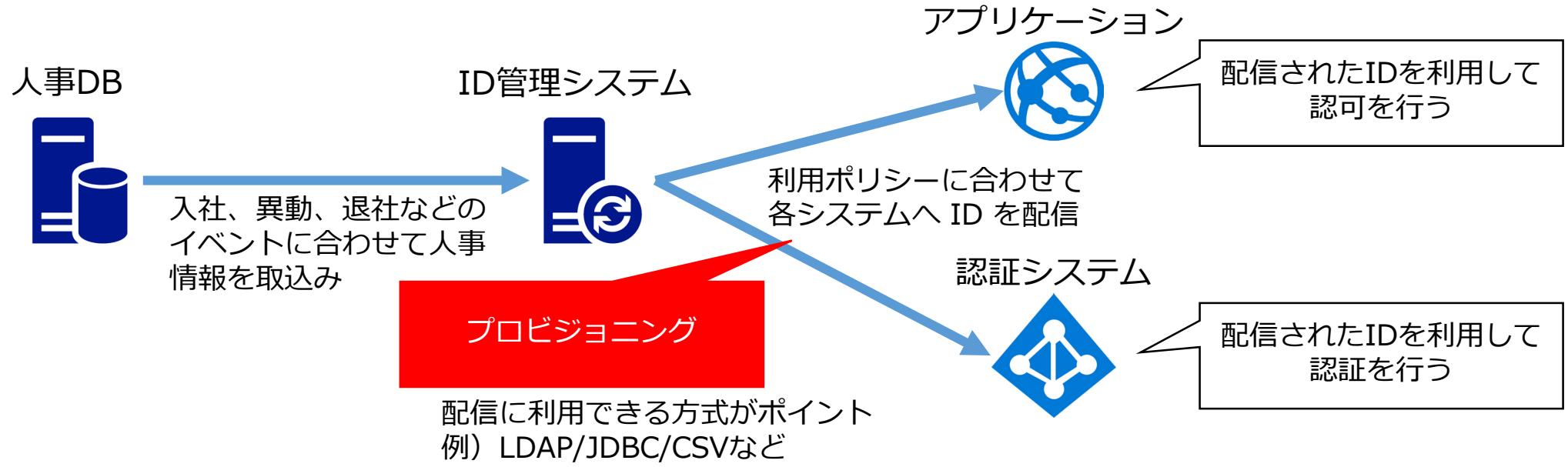
ID管理）プロビジョニング

- 認証/認可の大前提となるIDの登録
  - 「認証の8プロセス」（出典：2015年のIDビジネス/野村総合研究所著）



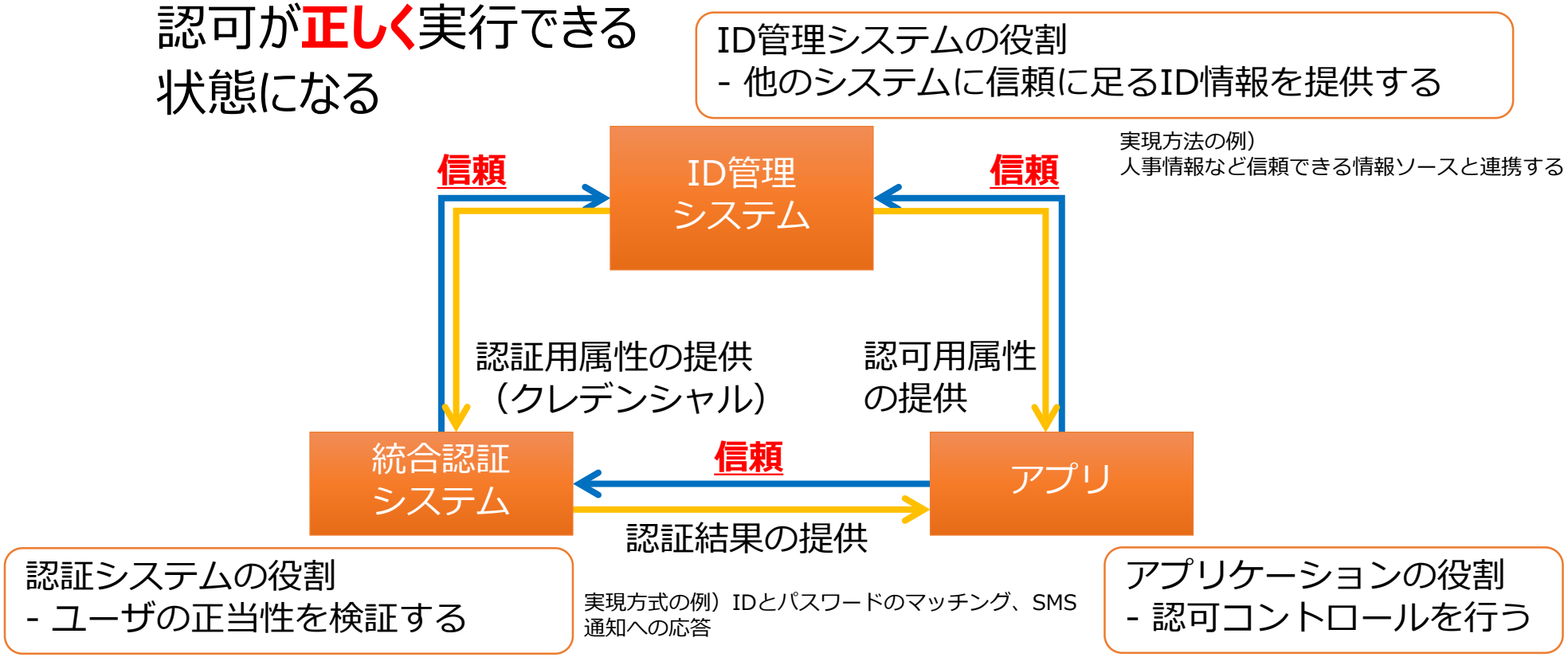
ID管理）プロビジョニング

- 認証/認可の大前提となるIDの登録
  - 認証/認可を**正しく**行うために信頼できるID情報を登録する必要がある
  - 人事DBからID情報を取得し、認証システムや各種アプリケーションへ配信する
    （企業において最も信頼できるID情報の源泉が人事である場合が多いため）



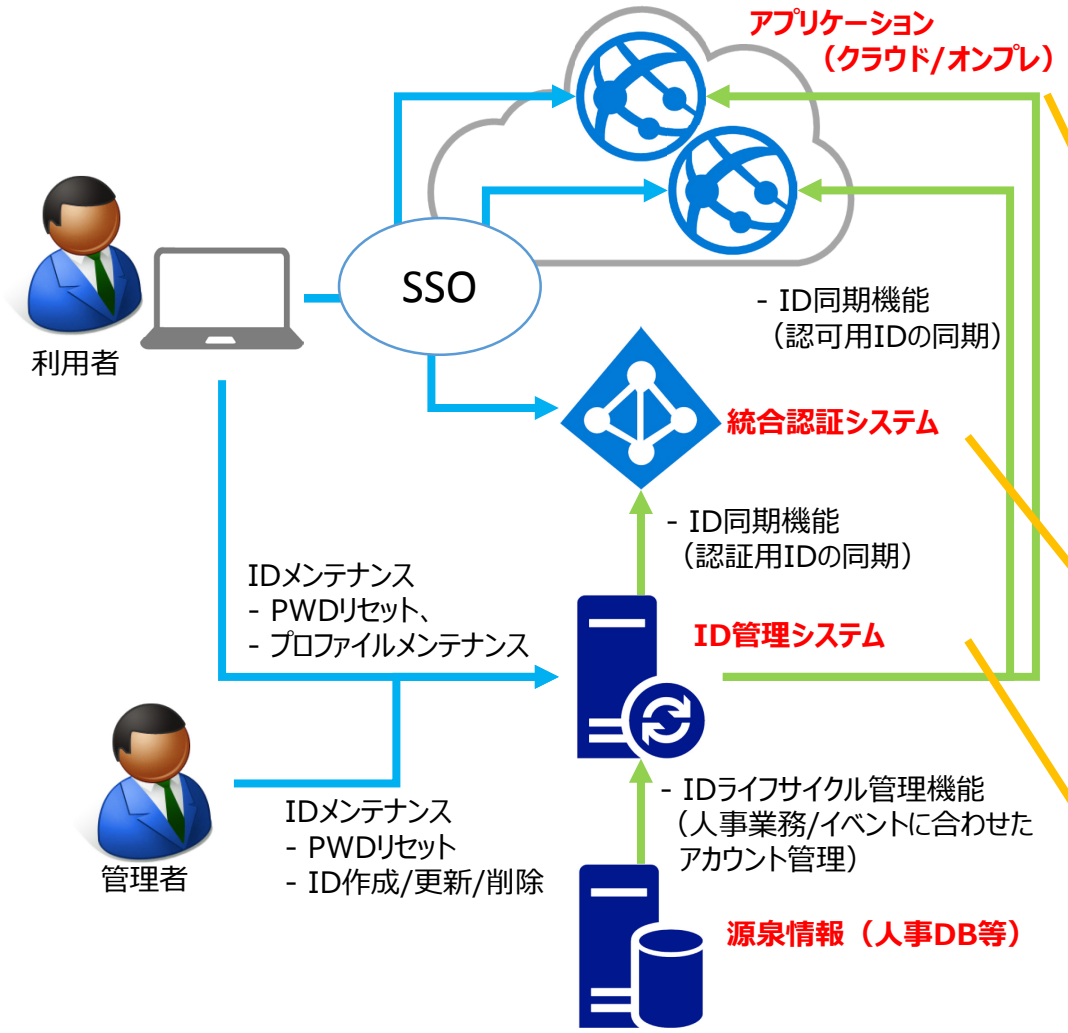
ID管理）プロビジョニング

- プロビジョニングの重要性
  - ID管理システムが**正しく、信頼できる**プロビジョニングを行うことにより識別、認証、認可が**正しく**実行できる状態になる



３．ID管理／認証システム導入の理想と現実

B2Eシナリオにおける理想的なID基盤



理想的な機能分割

アプリケーション

- **全ての**アプリケーションが統合認証システムへ認証機能を委譲（**標準プトロコル**への対応し、**パスワードは持たない**）
- ID管理システムから同期される**共通属性**に基づく認可コントロールだけを行う

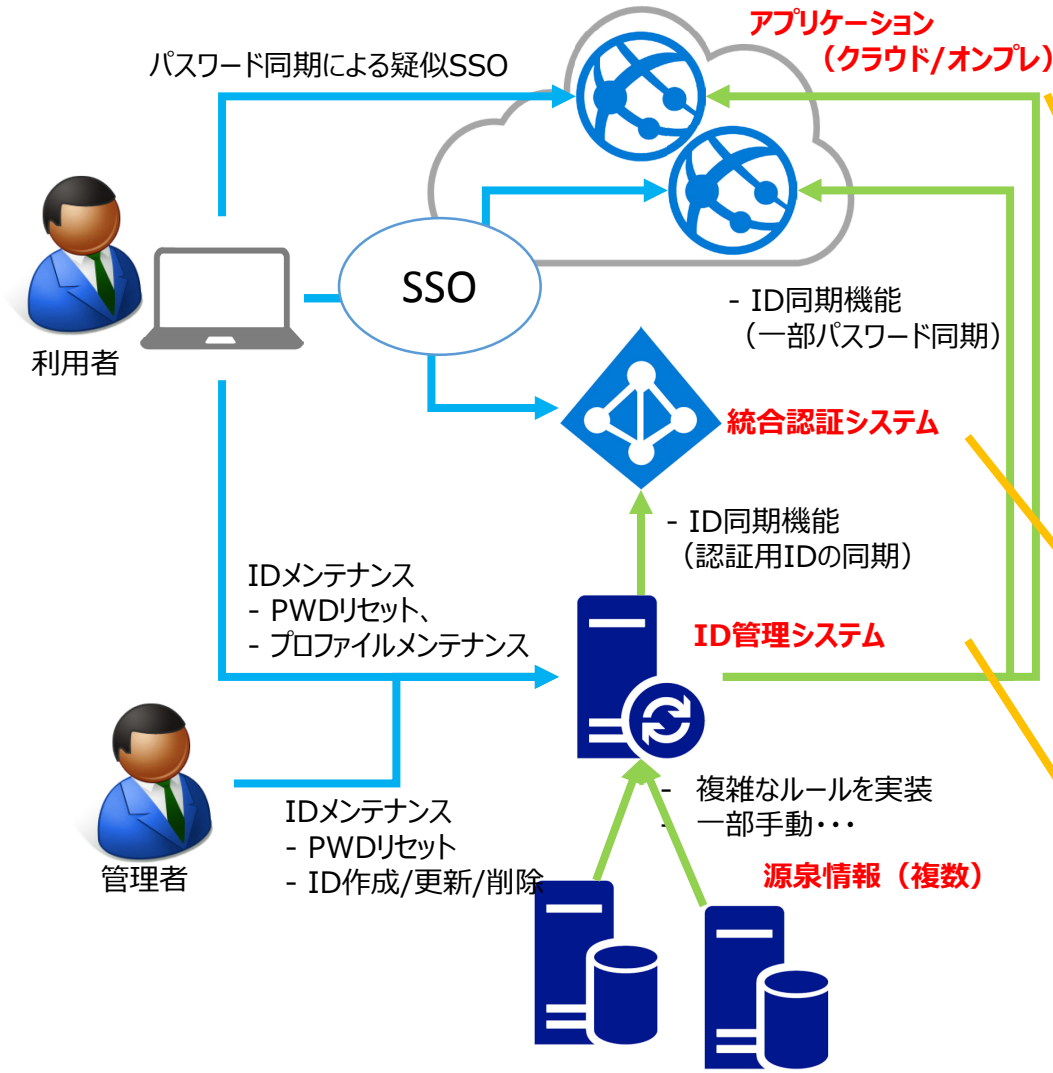
統合認証システム

- 標準プトロコルのサポート
- アプリケーションのコンテキストに応じた認証コントロールを行う（MFAなど）

ID管理システム

- **統合された源泉**（人事等）からIDを取り込み、**精度・鮮度の保証されたID情報**を管理・配布

B2Eシナリオにおける ID基盤の現実



機能分割の現実

アプリケーション

- **一部**のアプリケーションが統合認証システムへ認証機能を委譲
- **ID管理システムからパスワードを同期**
- ID管理システムから同期される属性だけでは認可コントロールが出来ないので**独自管理**

統合認証システム

- 標準プトロコルのサポート
- アプリケーションのコンテキストに応じた認証コントロールを行う（MFAなど）

ID管理システム

- **複数**の源泉（人事やグループウェア）からIDを取り込み、**複雑なルール**を実装。**精度は微妙**

理想と現実、リスクと低減策

構成要素	理想	現実	リスク	低減策
IDソース	統合された単一のソース（人事）	社員：人事 派遣：事業所毎にExcel	派遣の登録忘れ、消し忘れ	自動無効化（有効期限）、棚卸
APL	認証は認証基盤へ委譲 共通属性に基づく認可	個別認証 認可に必要な属性が不足	権限の付け忘れ	棚卸
認証	保護レベルに応じて認証 コンテキスト分離 標準プロトコル対応	個別認証 パスワード同期	パスワードの使いまわし	重要システムを先に統合する MFAなど
ID管理	共通属性のみをしっかり管理 SCIMでI/Fの標準化 ライフサイクルはIDソースと同期	政治に負けていろんな属性を管理 個別のプロビジョニング 個別の事情に基づいたライフサイクル	低保証レベルのプロビジョニング 退職者アカウントの残留による、不正ログイン	棚卸

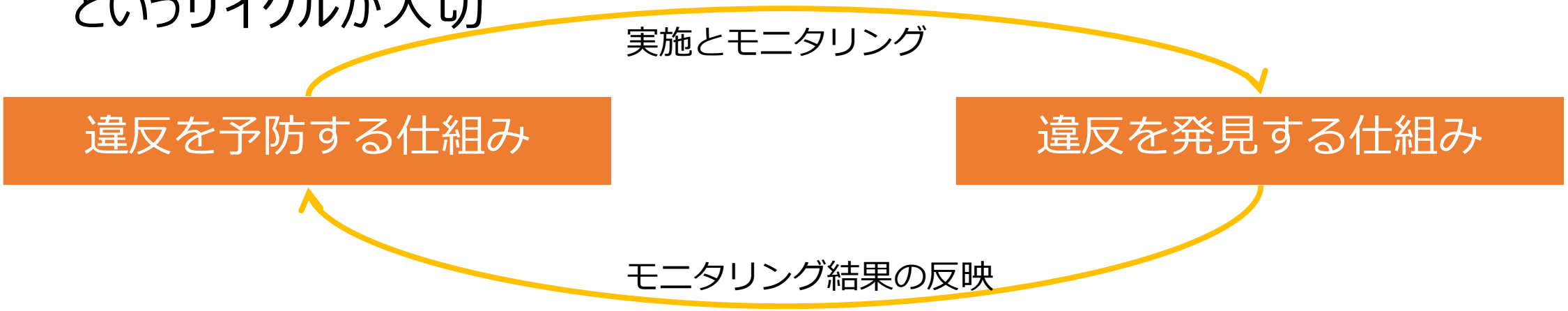
発見的統制が重要

システム化の限界と発見的統制の重要性

			識別	認証	認可
	目標		正しい利用者に業務に必要なITシステムや情報を正しく利用させる		
	ポリシー		例）企業に在籍する者に、役職に応じて情報を開示する		
管理	ルールの定義 プロセスの実行		・社員番号を使って識別する ・入社～退社の間のみ利用させる	・パスワードで認証する ・パスワードは8文字以上とする ・有効期限は90日とする	・利用者の役職属性に応じて情報を開示する
制御	ルールどおりにプロセスを実行させる	予防	・社員番号を人事システムから取得し、ITシステムへ登録する ・入社時に有効化、退社時に無効化する	・パスワードが間違っていると認証しない ・8文字未満のパスワードを登録させない ・有効期限間近に通知する	・人事システムから最新の役職属性の値を取得し、ITシステムへ登録する
		発見	・人事システム以外から登録されたIDの有無を棚卸・確認する ・在籍状態以外のIDの有無を棚卸・確認する	・パスワード間違い履歴を確認する ・パスワード期限切れのユーザー一覧の棚卸をする	・アクセス履歴と利用者の権限の棚卸する

大前提。サイクルが大事

- 現実ばかりを優先すると発見的統制ばかりをシステム化してしまうことに
- 予防的統制が働かない状況で発見的統制をしようとすると非常に効率が悪い
  - 鍵がかかっていない部屋に監視カメラをつける
  - 監視カメラの記録を見て入ってはいけない人が入っていないか一人ずつ確認？
- 予防措置の実行⇒違反を発見できる仕組みを作成⇒予防措置の改善というサイクルが大切



参考）B2Bだと更なるリスクも

構成要素	理想	現実
IDソース	各社で統一ポリシーで管理されている	各社非統一の管理レベル 仕方なく全員を統合DBへ
APL	共通属性に基づく認可	共通属性（ロール）は作れない アプリで個別に管理
認証	ID連携で各社ログイン	個別認証
ID管理	共通属性を管理	共通属性が作れない 信頼済みソースがない

リスク	低減策
退職者の消し忘れ（把握不能）	棚卸
権限の付け忘れ、消し忘れ	棚卸
パスワードの使いまわし ID漏えい	対象アプリの絞込み 早期の統合？ リスクベース認証
低保証レベルのプロビジョニング	棚卸

B2Bの場合は発見に加えて、
対象を絞り込むことも大切

４．技術面からの現実的アプローチ

- ここまでは管理・統制の理想と現実の話
- Internet Weekということで技術的な話も少々
- あくまで一つの例であり、推奨するわけではありません

別の現実

- 組織間の断絶、予算の壁
  - 本来は全社ID管理基盤を用意し運用するはずの情報システム部門
    - 業務部門の統制をとりたい　：　野良クラウドは使わせたくない
    - サポートするリソースや予算がない　：　個別の要望へは応えづらい
  - 効率よく業務を進めたいフロント部門
    - 便利なクラウドサービスを使いたい
    - 社内ADを使ってSSOしたいので、情報システム部門にサポートしてもらいたい

アプローチの例

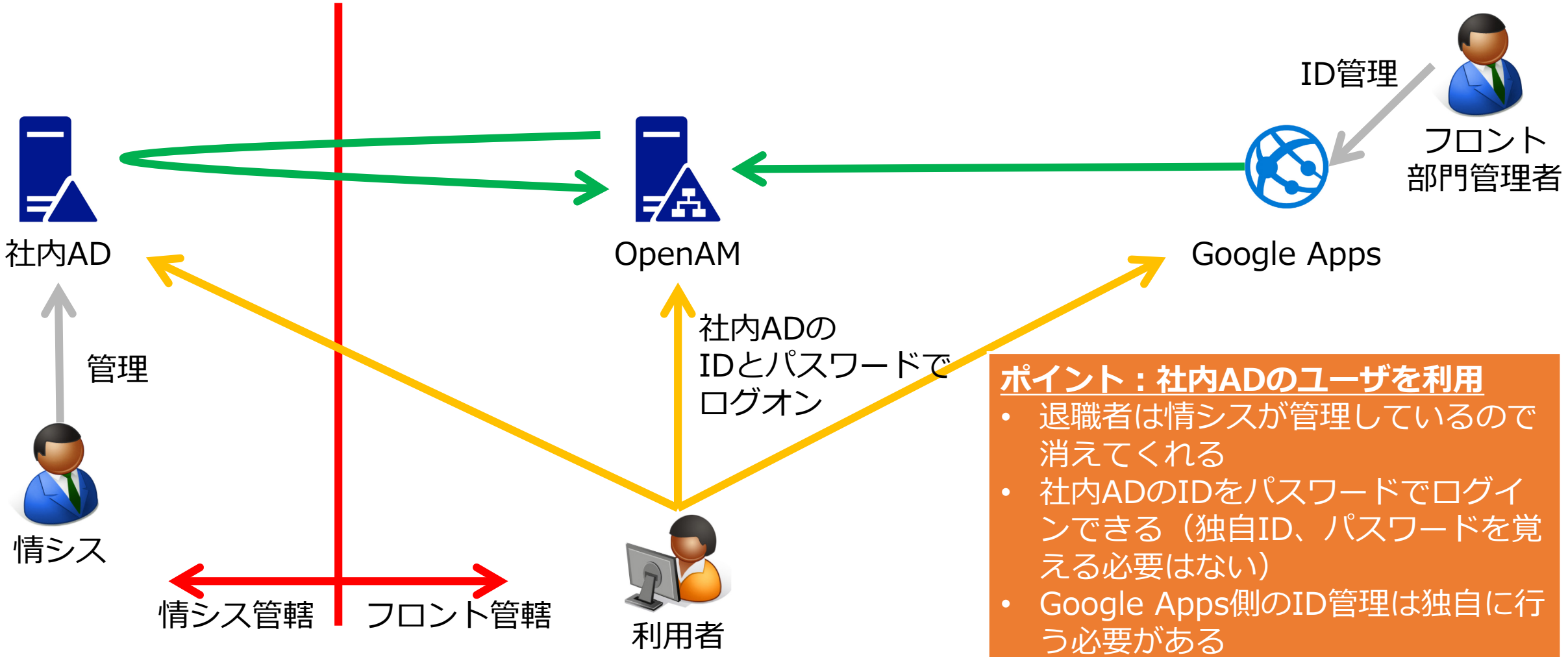
- とりあえず現場で認証基盤をつくり、認証だけは情シス管理のADで行う
- 後から情シスが認証基盤を整備するときにID連携する
- 最終的にアプリ接続先を現場の認証基盤から情シス認証基盤へ切り替える

- STEP１）
  - フロントでとりあえず認証基盤を作ってクラウドサービス利用を開始
    - OpenAMを構築、社内AD連携
    - Google Appsを連携

- STEP2）
  - 情シスがAzure ADを契約
    - Google AppsをAzure ADへ追加
    - SSOは既存認証システム（OpenAM）を利用する様に構成

- STEP3）
  - アプリを情シスが巻き取る
    - Google AppsのSSOをAzure ADへ切り替え

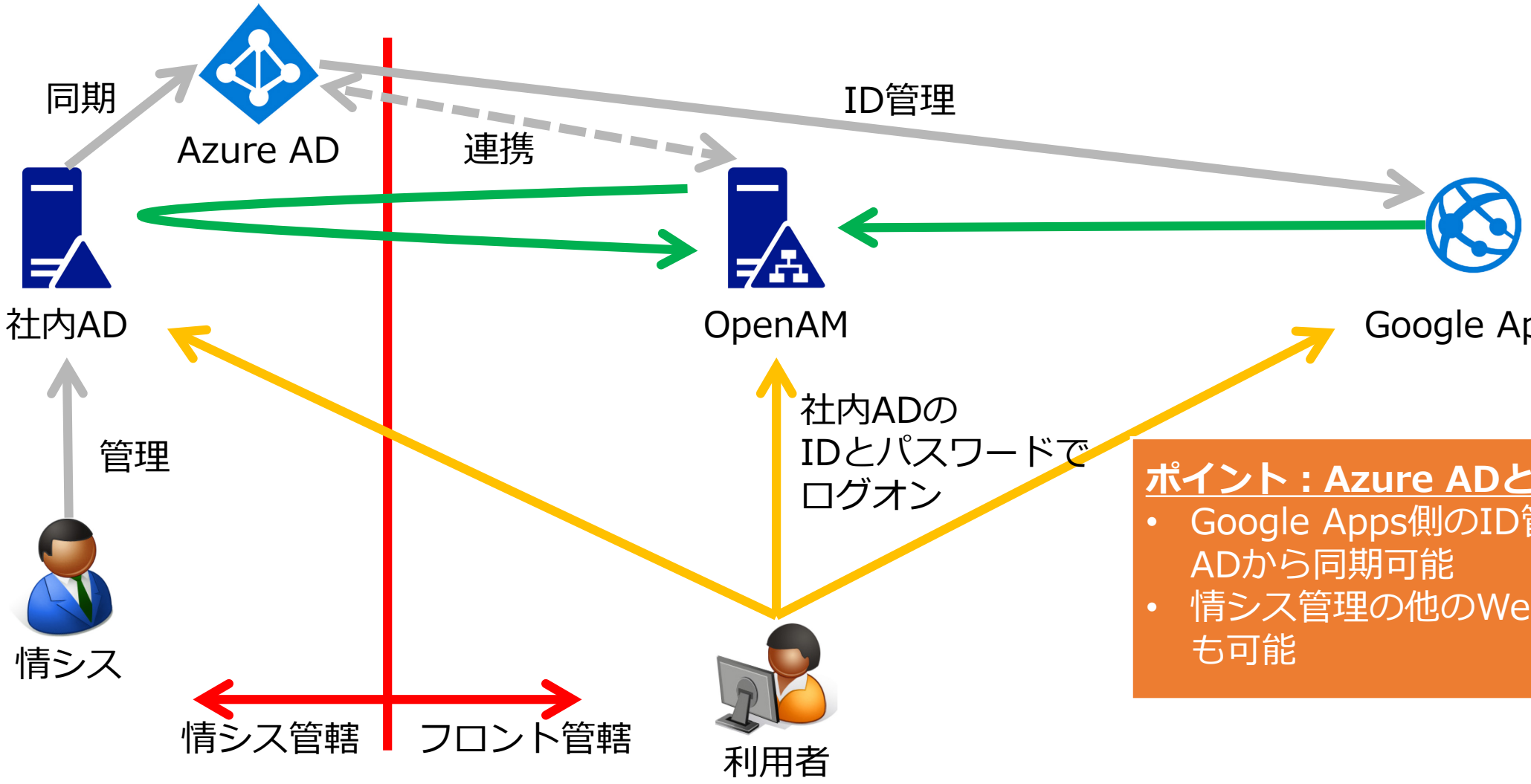
STEP1）フロントでとりあえず認証基盤を作ってクラウドサービス利用を開始



ポイント：社内ADのユーザを利用

- 退職者は情シスが管理しているので消えてくれる
- 社内ADのIDをパスワードでログインできる（独自ID、パスワードを覚える必要はない）
- Google Apps側のID管理は独自に行う必要がある

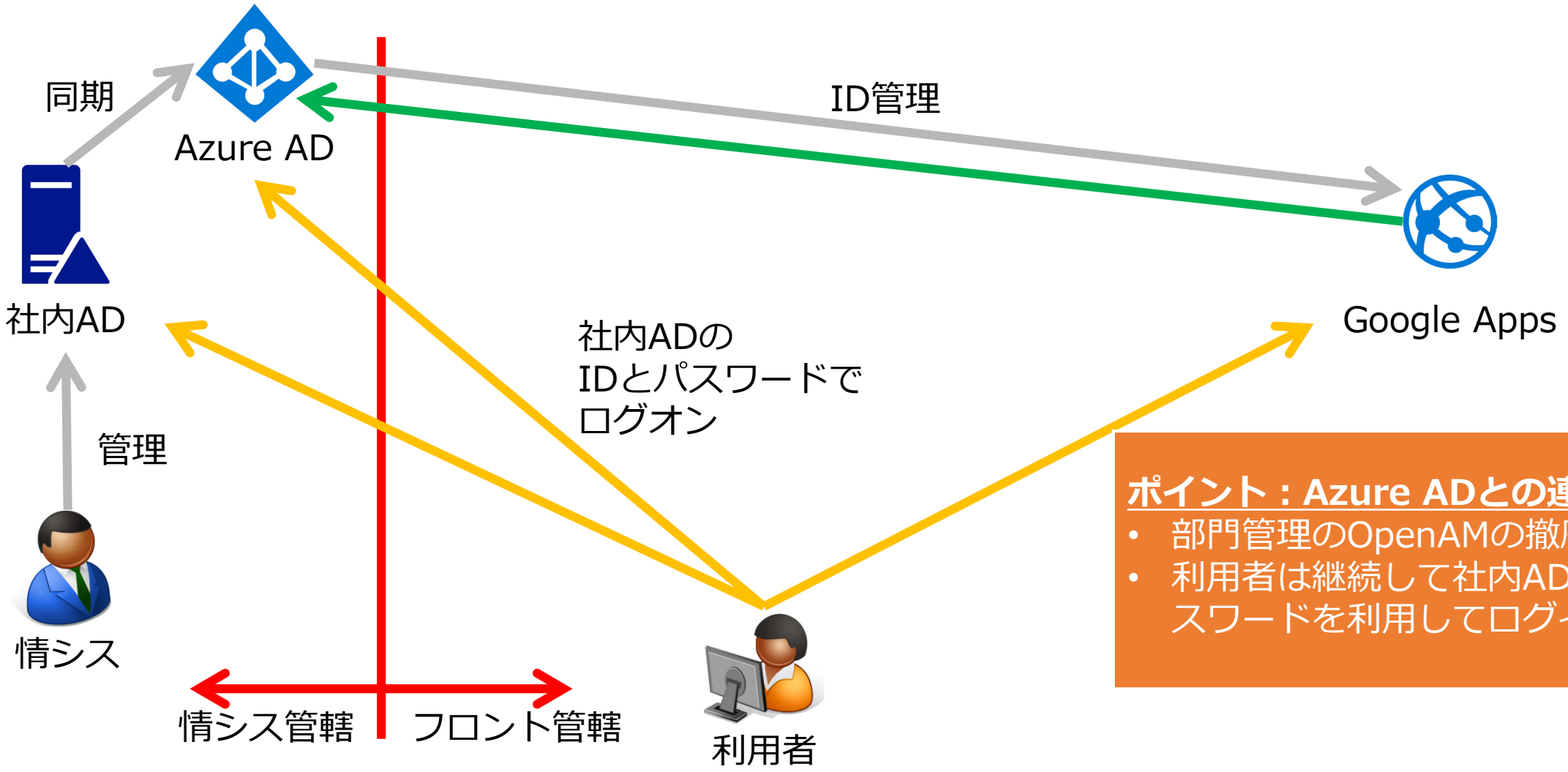
STEP2）情シスがAzure ADを契約



ポイント：Azure ADとの連携

- Google Apps側のID管理をAzure ADから同期可能
- 情シス管理の他のWebアプリとSSOも可能

STEP3）アプリを情シスが巻き取る



<u>ポイント：Azure ADとの連携</u>

- 部門管理のOpenAMの撤廃
- 利用者は継続して社内ADのIDとパスワードを利用してログイン可能

デモ

5. まとめ

まとめ

- 企業におけるIDの用途は「**業務に必要なITシステムや情報を利用させること**」である
- 「正しく」業務を遂行させるためには「**識別**」「**認証**」「**認可**」を「**正しく**」行う必要があり、そのためには「**ID管理**」が重要である。また、効率的にID管理を行うためにシステム化が必要である
- ただし、**一気に理想的な基盤を導入できることは少ない**ため、ITに頼る・頼らないに限らず、**現実とのギャップを埋める方策を決めて実行**することが大切
- ステップ・バイ・ステップのアプローチで**システム化を徐々に進める**ことも検討