学認クラウド
ゲートウェイサービス

国立情報学研究所　　西村　健

学認クラウドゲートウェイサービス
～ 大学・研究機関の認証基盤とクラウドの橋渡し ～

（以下、「ゲートウェイサービス」と呼びます）

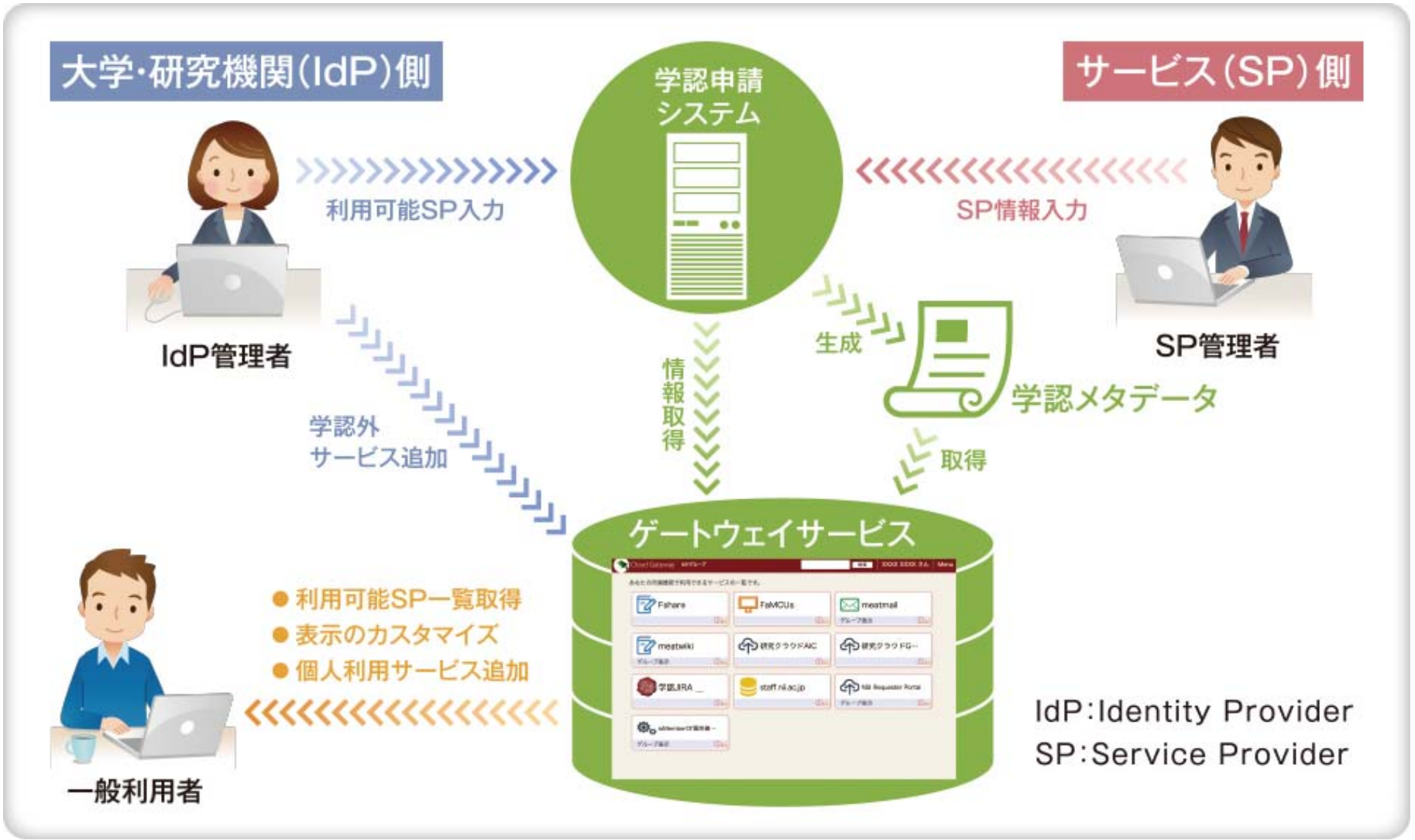
- 自身の所属機関で利用可能なサービスが一覧できる
  - 機関毎のカスタマイズ（契約・連携しているサービスの指定/入力）
  - 個人毎のカスタマイズ（並び順の変更や個人利用サービスの追加）

利用者のアクセス例

- 利用者はゲートウェイサービスを経由してe-Learningサイトやe-Journalサイトにアクセスする

- ゲートウェイサービスに表示されているサービスは利用可能である＝安心してアクセスできる
- ふらっとあるサービス(e-Learning B)にアクセスして利用できなくて困る、ということが無くなる

ゲートウェイサービスの登場人物と役割



大学・研究機関側ができること

- 機関が契約・連携しているサービスを登録できる
  - IdP管理者が登録したサービスは全構成員に提示される
  - 機関で契約しているクラウドサービスや、学内サービスなど

- 学認参加サービス(SP)であれば一覧から選択するだけ
  - IdPがSPへ属性送信設定しているものに合わせて選択する
  - 学認申請システムでの設定 or ゲートウェイサービスに直接入力
  - ここで「利用可能」と指定されたものが、構成員に提示される

制限

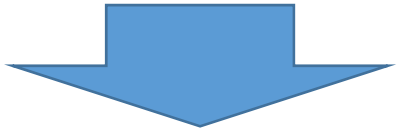
- 学認に参加済みの機関でなければご利用いただけません
  - ゲートウェイサービス自体がSPとして構成員であることを認証するため

グループごとの利用可能サービス情報も提供

- 共同研究グループ等グループメンバーを登録しておくと、そのグループ固有のサービスをメンバーのゲートウェイサービス画面に組み込み可能
- 学認のGakuNin mAPサービスで培ってきたグループ機能を継承
  - meatwiki、しぼすけ等
- 利用者にとって、「自分が使うべきサービス」が一覧できる

パブリッククラウドへのSSO（提供予定）

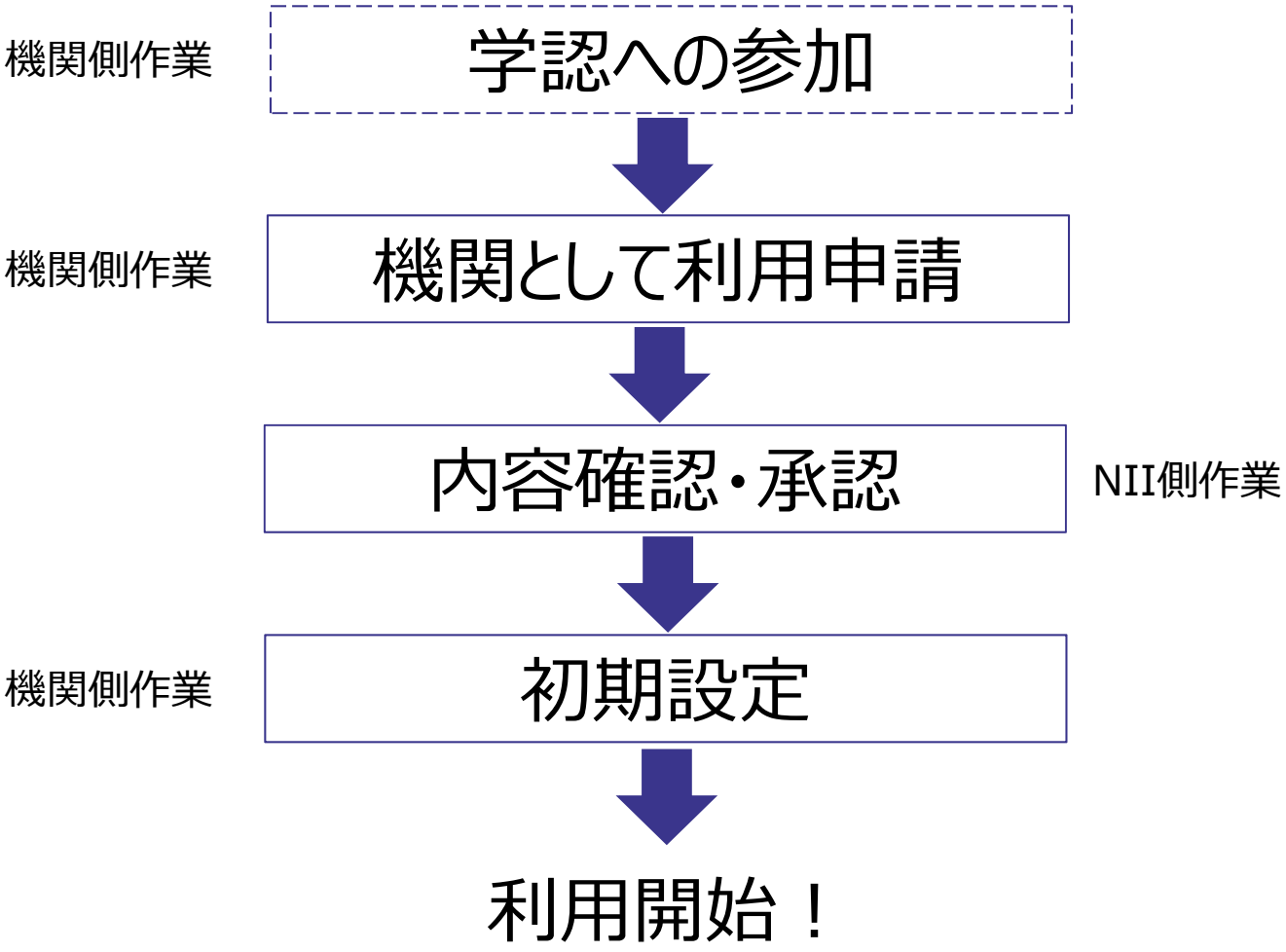
- パブリッククラウド(IaaS)の中にはSAML対応しているものがあり、コンソールにSSOできる（以下例としてAWS）
- ただし学認参加IdPがAWSの要求を満たすには困難が伴う
  - 学認で規定されない特殊な属性を要求している
  - かつ利用料支払い（いわゆるおサイフ）の情報が必要
    - 大学が契約しておサイフが1つだと若干楽



- 学認参加IdPで認証した上でゲートウェイサービスIdPが必要な属性をAWSに送信する
- おサイフの情報はその使用範囲をグループとしてグループに対して自由に設定できる

※ AWS側にも若干の設定が必要

利用開始までの流れ



その他・お問い合わせ先

- 学認クラウドゲートウェイサービスは利用申請をいただいた機関に対してのみ提供しています
  - 機関の担当者（=IdP管理者）が初期設定することが大前提のため
  - ただしグループ管理機能は性格が異なるため未申請機関にも提供

- 「学認クラウドゲートウェイサービス」利用機関募集中！
  - 無料でご利用いただけます
  - https://cloud.gakunin.jp/cgw/

- 学認クラウドゲートウェイサービスに関するお問い合わせ・ご相談は
  - cld-gateway-entry@nii.ac.jp