組織間異動における認証認可の課題

学認は何ができるか／何をすべきか

Orthros 開発チーム（仮称）

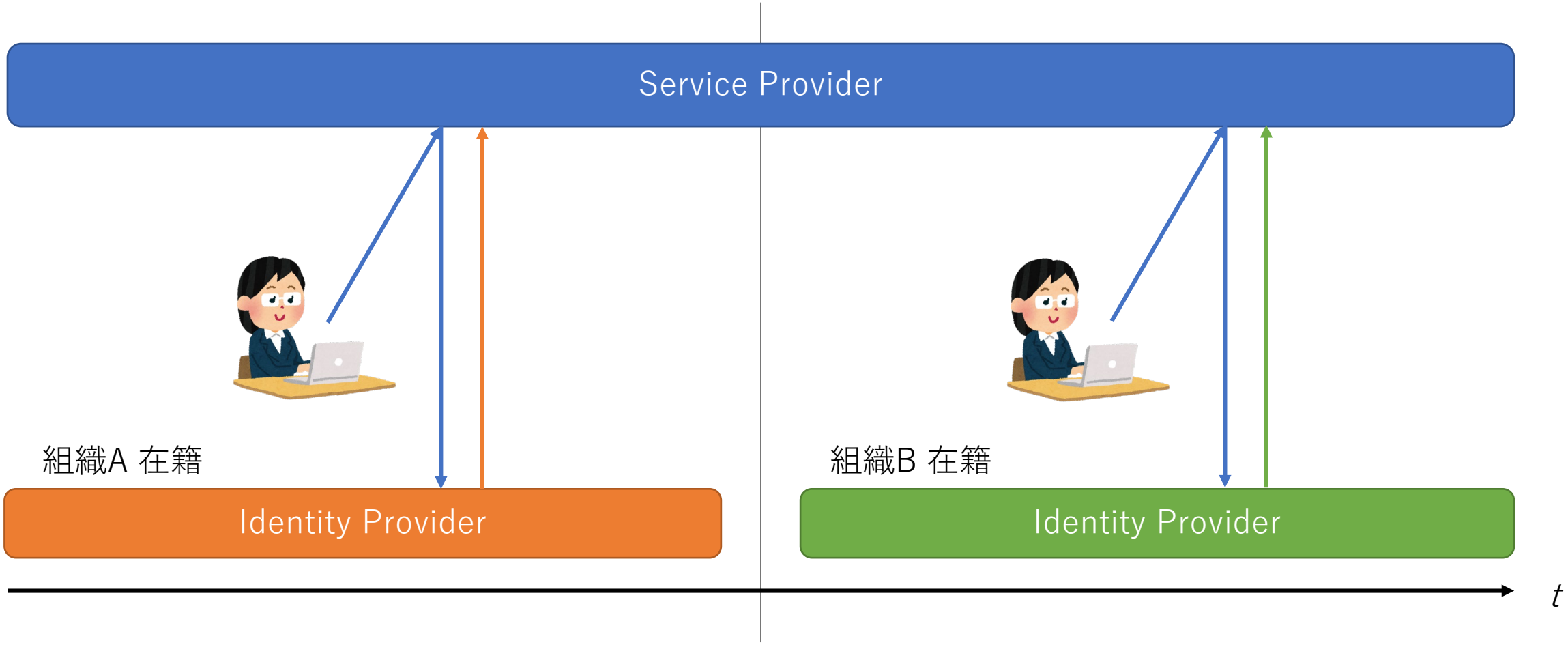
背景

- お題：組織間の**異動に何らかの保証**をするために**何ができるか**に関して、NII の新 OpenIdP とか IdaaS の話が出たが、サービスとして学認参加組織に提供することを検討したい。

- 求められる保証とは何か？
- そのために何ができるか？

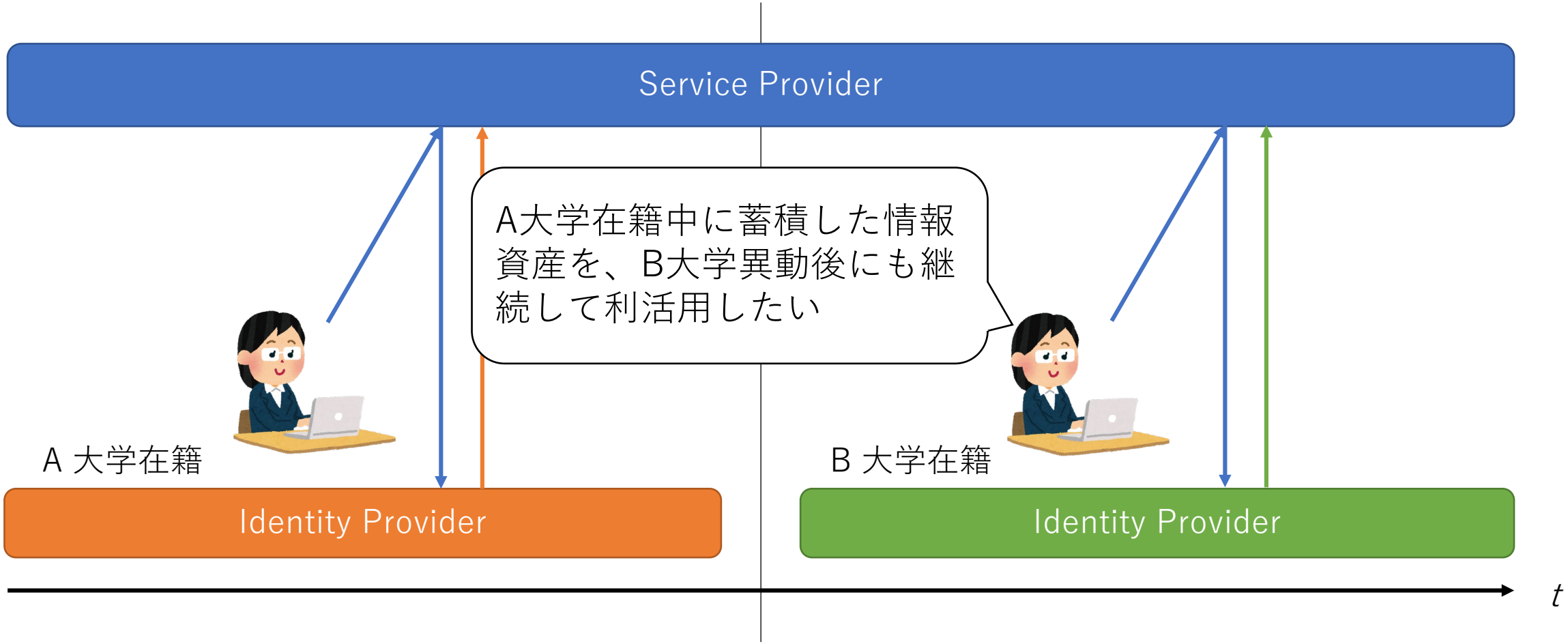
- 組織間異動における Participants
  - end entity（EE: ヒト）
  - ある期間まで EE が在籍した組織 (IdP)（異動元／前）
  - ある期間から EE が在籍する組織 (IdP)（異動先／後）
  - サービス (SP)

モデル化


Service Provider
組織A 在籍
Identity Provider
組織B 在籍
Identity Provider
t

モデルケース：GakuNin RDM

- 課題：組織間異動において情報資産利活用の継続性を担保



- 要件：組織を跨る利用者の同定
  - IdP(B) の EE さんは、IdP(A) の EE さんである

基本設計に向けて

- 基本方針
  - オンラインによる可能な限りの効率化

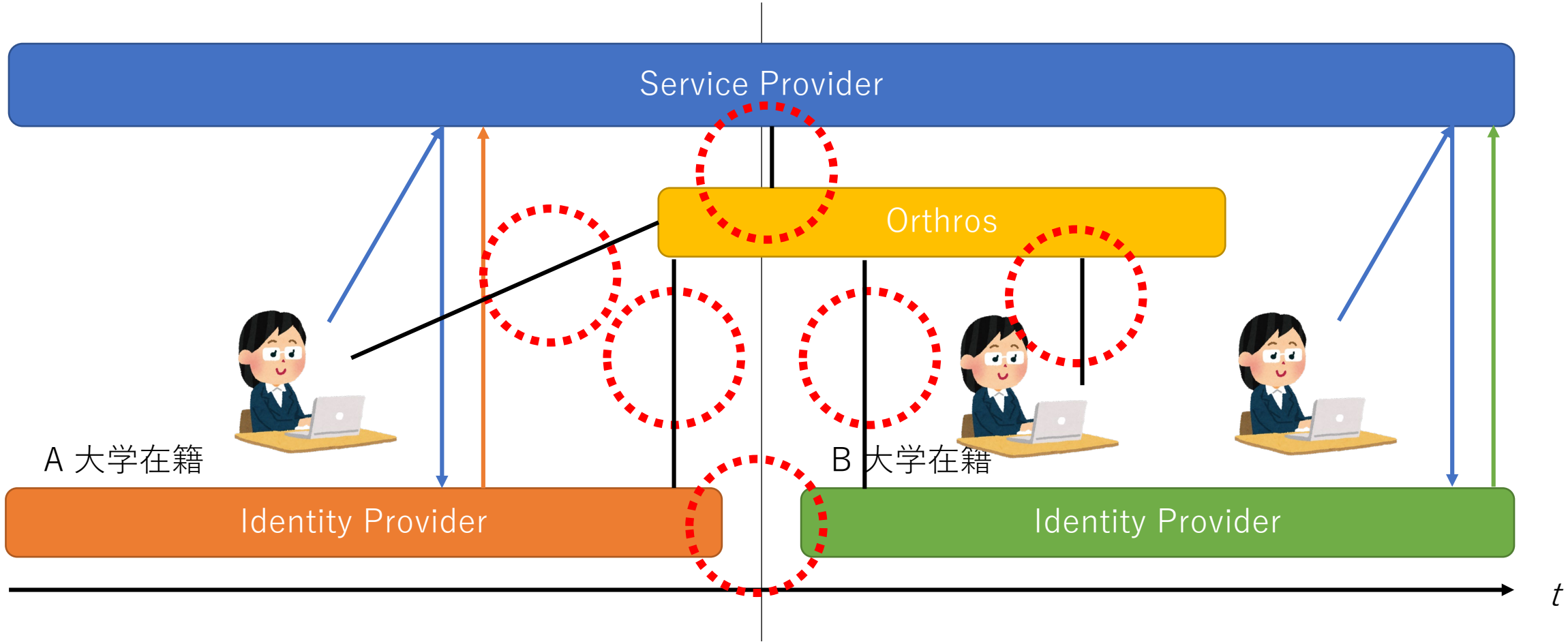
- 識別子の選定
  - 異動前後で不変な EE 識別子をキーに異動前後の認証情報を紐づける
  - そのような識別子は何か（どこが管理しているか）
    - IdP(A)? IdP(B)? SP? それとも…

- 組織間異動における本人確認手続き事例：HPCI
  - 組織を異動すると本人確認手続きを実施
  - 組織異動前後で HPCI-ID は不変（な識別子）
  - 組織異動前後で必ずしも HPCI IdP は変わらない
  - HPCI では単なる属性変更

異動支援シナリオパターン

1. 複数のIdPが一時的にオーバーラップして利用できる場合
   （SPがIdP(ID)の付け替えをサポートする必要がある）
2. SPが複数のIdPとIDの紐づけができる場合
   （SPで一つのID（内部）に複数のIdPと紐づけができる必要がある）
3. 第三者のID紐づけサービス（ORCID等）が利用できる場合
   （SPが外部のIDでIdPの付け替えをサポートする必要がある）
4. Orthros的IDプロキシサービスを利用する場合
   （SPは何もしなくても良いが、Orthrosが機関契約サービスでも利用できる必要がある）
5. 異動後IdPが新しいePPNを教えてくれる場合
6. 異動前IdPが古いePPNを教えてくれる場合
   (eduPersonPrincipalNamePriorで)
7. その他

認証プロキシ Orthros が仲介する異動イメージ



ここまでのまとめ

- 組織間異動における保証サービス案
  - 組織を跨る end entity の同定
    - 「組織を跨る」→「IdP を跨る」

- 今後の検討課題
  - 異動支援シナリオの洗い出し
  - 基本設計、詳細設計、試作実装…

- テーマの展開
  - 組織異動→属性変更
  - 他の属性変更への適用：学部生→大学院生（ロール変更）