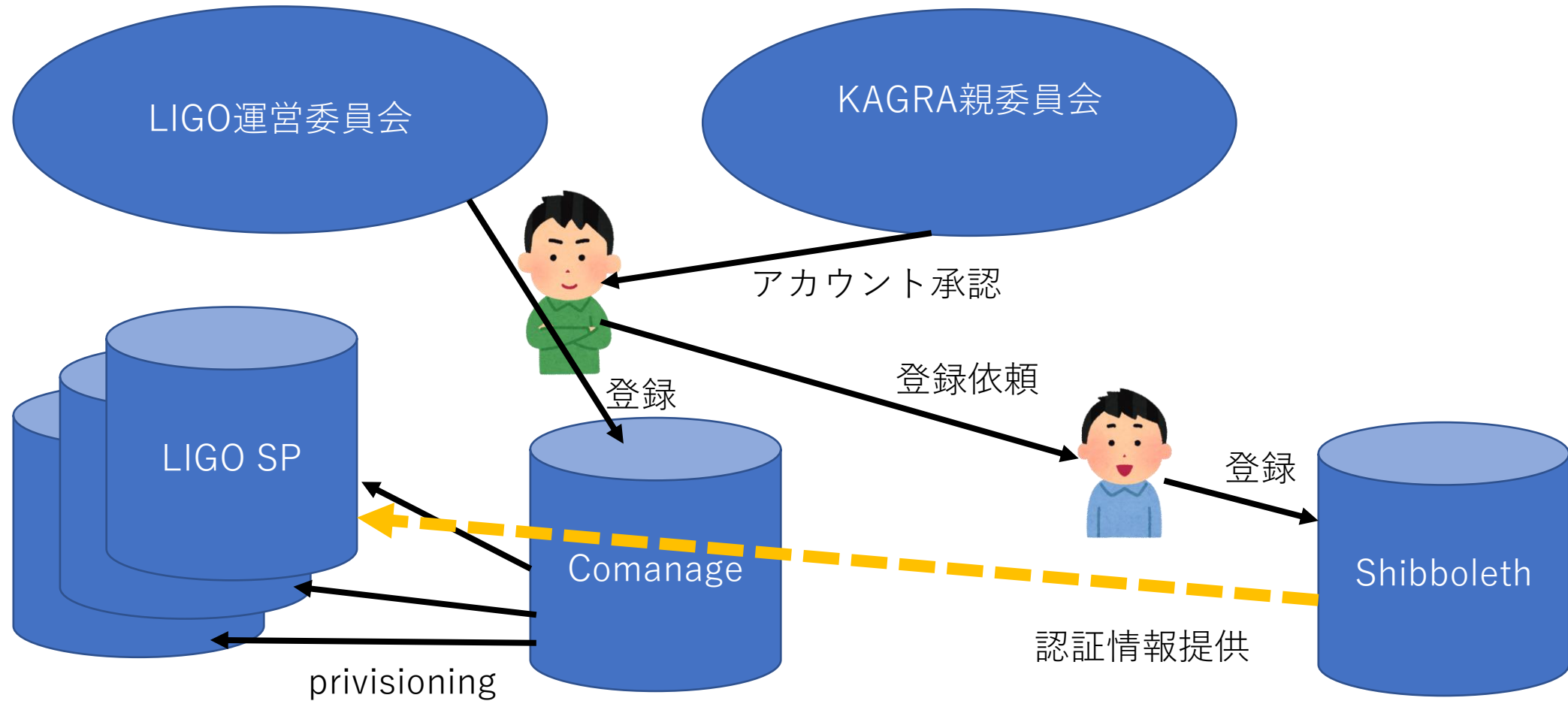


国際共同研究プロジェクト の認証管理例

佐藤周行

立場は…

KAGRA



アカウント統計 (as of 2021/May)

- 総数
 - 利用者数 357
 - 「機関」数 81 (定義：機関=IdPでOUに登録されているもの)
- eduPersonAffiliation別
 - faculty 195/student 146/staff 16
- 機関の地域分布
 - 国内 東大内12/東大外 31
 - 国外 Asia 26/US/7/Europe 4

Page 2 を書き下してみます

- 参加、登録に当たってKAGRAの親委員会の審査がある
 - 研究者コミュニティ間のトラストで動いている
- COmanageで利用者登録⇒LIGO SPにプロビジョニング
- MetadataはeduGainから降りてくる
- IdPは、認証のみ担当。KAGRAからの利用者登録依頼にしたがって処理
- LIGO SPが、より強い認証を要求してきた場合の対応はこれから

LIGOからの提案（数年前）

- 学内アカウントでの認証を可能にする
 - USの大学では、すでに多数の大学IdPが登録されている
 - トラストの問題をどう解決しているかはよくわからない
- 一方、LIGOが直接運用しているIdPも
 - いわゆる「みなしごユーザ」を収容するためにはこの手のIdPはしょうがない
- 日本はその提案を保留中
 - 学認参加IdP…
 - Kagra IdPはなくなる
 - （たとえ東大が学認IdPに移行したとしても）
 - すでに多くの研究機関の「みなしごユーザ」を収容

SPが要求する属性とIdPの対応

- IdPは、SPごとに送出属性を変えることができるようになっていました
 - LIGO SPは、CN, givenName, mail 属性を特に要求します
 - 一般論として日本のIdPでは特にmail属性について過去慎重だった
 - 今はeduPersonTargetedIdもdeprecatedになるくらいで
 - そのうち、Assuranceも要求するでしょう（予想）
 - Identity AssuranceよりもAuthentication Assuranceの方が先か
 - Identity Assuranceは、オフラインおよびコミュニティトラストで十分（?）
 - 属性を送出するかしないかは、IdP（の属する機関）の権限
- たとえば東大IdPをKagra IdPとして利用しようとするすると、送出属性についての調整と合意が必要になります
 - LIGOだけではないかもしれないが
 - たとえばAAに加えてIAなんかも問題になるかもしれない
 - 誰が誰とネゴするのか？