IdPで認証時にエラー

→ IdPが運用フェデレーションとテストフェデレーションの双方に同一のentityIDで参加している場合に、認証エラーとなることがあります。これはテストフェデレーション側のメタデータに掲載されている証明書情報が誤って取り込まれることが原因と推定されています。テストフェデレーション側のIdPについて実運用のIdPと異なるentityIDを利用するなどし、テストフェデレーション側のIdPは廃止申請すると問題の切り分けが行いやすくなります。

→ 関連して、運用フェデレーションで実運用中のIdPにおいて、テストフェデレーションのメタデータを読み込んでいる場合には、テストフェデレーションのメタデータ読み込み設定を削除してください。運用フェデレーションのメタデータのみを読み込む設定としたほうがより原因を追究しやすい状態となります。

→ transientIdが必須となっているSPにおいて、IdP側でtransientIdの送出が制限されている場合にエラーとなる場合があります。要求されている属性が正しく送出されているにも関わらず認証エラーとなる場合にはtransientIdの送出の有無を確認しておくと問題の切り分けに役立ちます。

→ SPが要求している属性と異なる属性を送出している場合にもエラーとなります。学認のIdP・SP一覧（https://www.gakunin.jp/participants/）で指定されている属性とattribute-filter.xmlの設定が一致しているか見直してください。attribute-filter.xmlを設定後、 設定・運用・カスタマイズ#SPに対してどのような属性が送出されるか確認する方法 の手順で実際に送出される属性を確認することができます。特に「eduPersonAffiliation （スコープなし）」と「eduPersonScopedAffiliation （スコープあり）」は似ていることもあり、間違えやすいことから注意が必要です。