NII RCOS
Research Center for Open Science and Data Platform

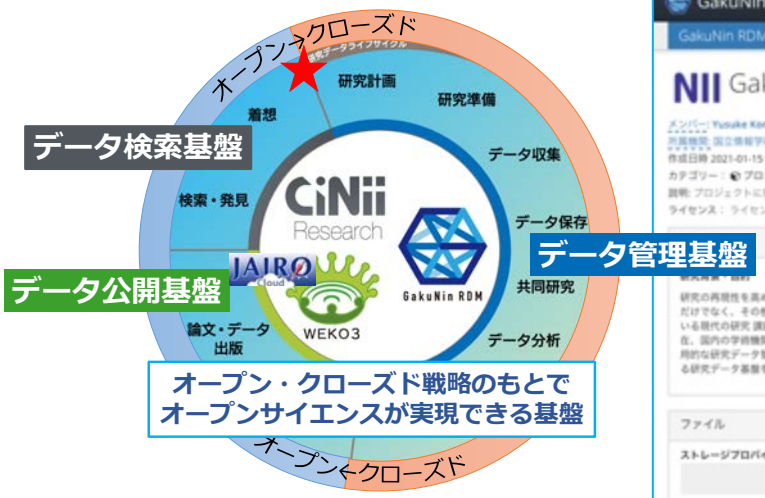
SP側の視点での
次世代認証連携への課題・期待

込山 悠介
国立情報学研究所
2022年12月13日

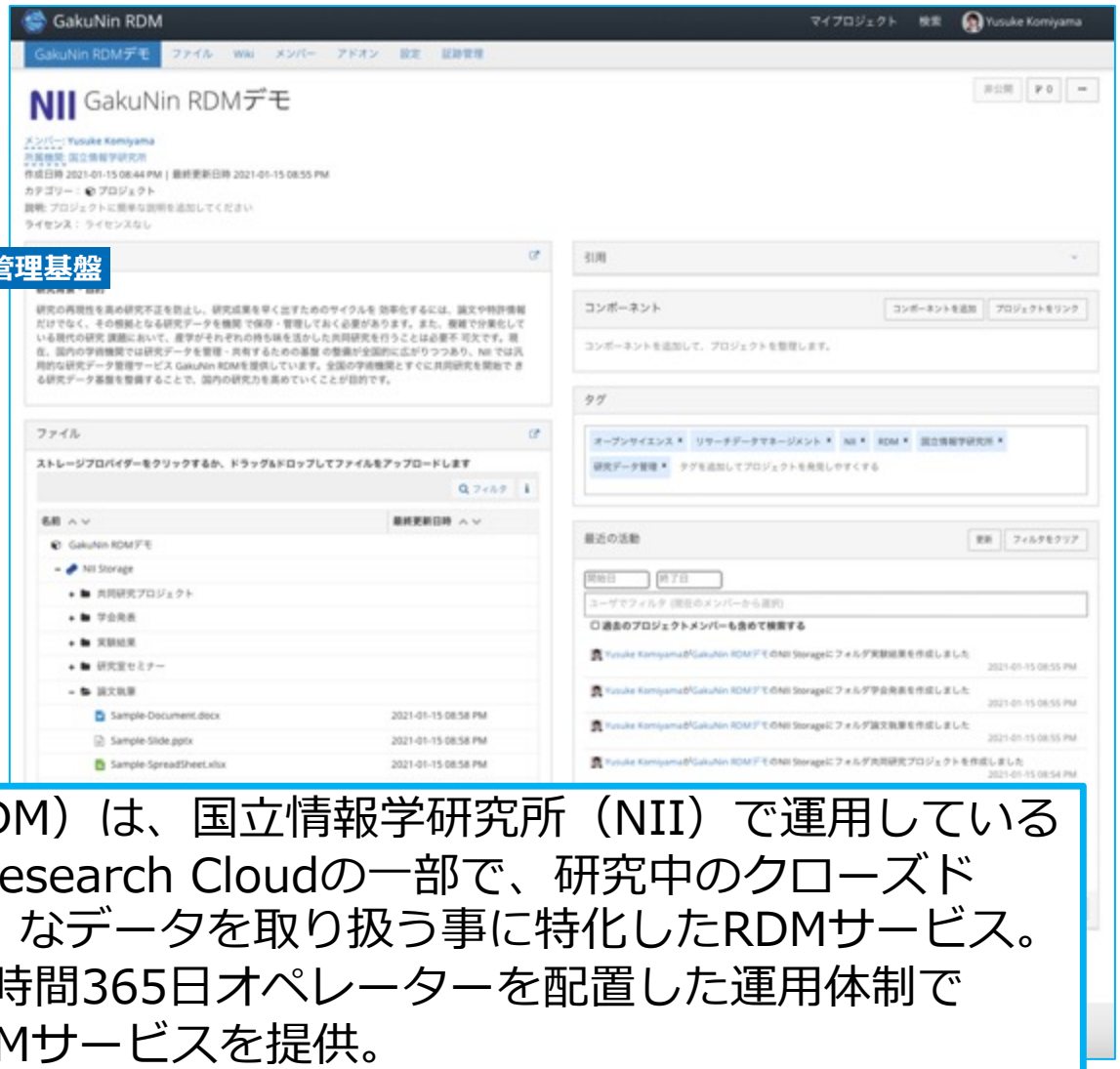
© 2022 National Institute of Informatics

NII RCOS
Research Center for Open Science and Data Platform

サービス提供(SP)側の立場
GakuNin RDMでの次世代認証への課題・期待



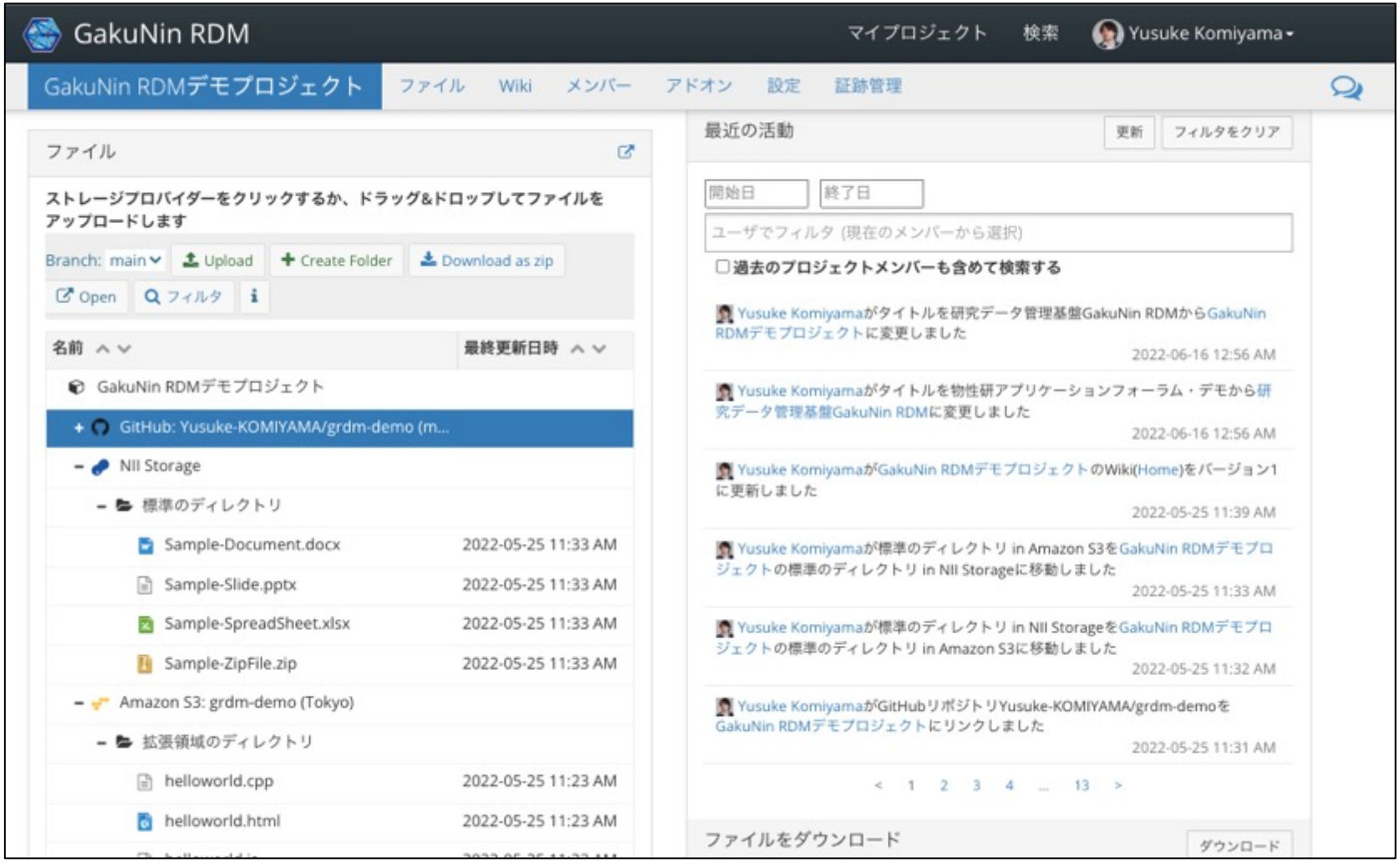
研究データプロセスと
研究データ基盤
NII Research Cloud



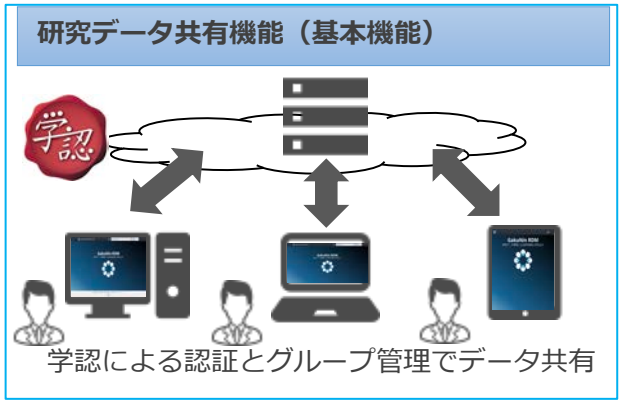
GakuNin RDM（GRDM）は、国立情報学研究所（NII）で運用している研究データ基盤NII Research Cloudの一部で、研究中のクローズド（非公開、制限共有）なデータを取り扱う事に特化したRDMサービス。2021年4月からは24時間365日オペレーターを配置した運用体制で全国の学術機関にRDMサービスを提供。

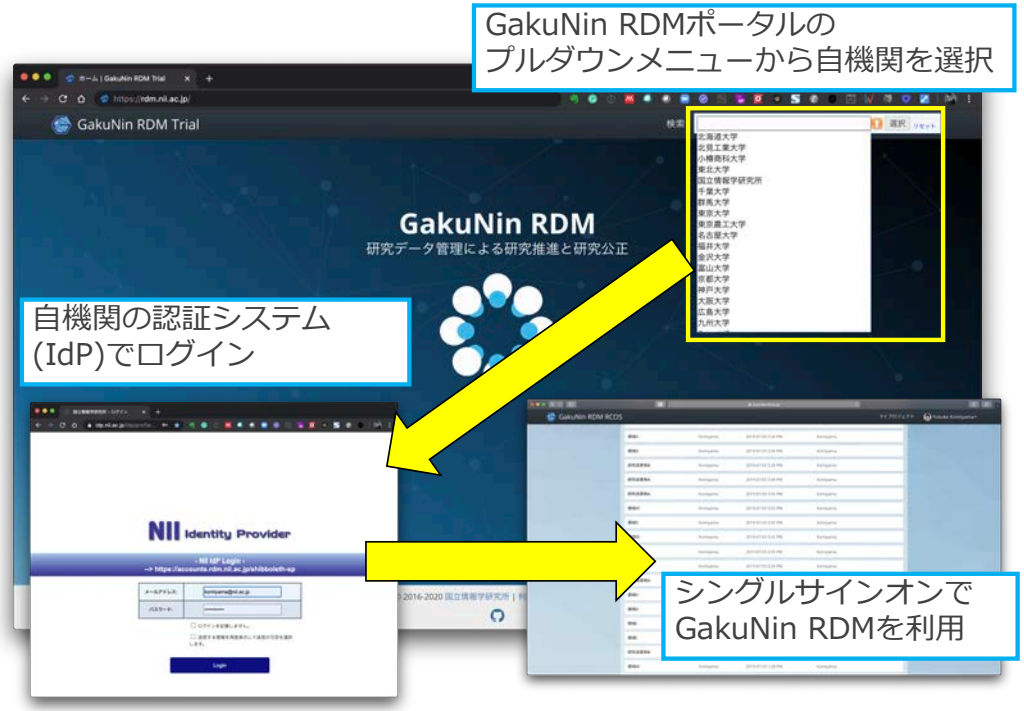
NII RCOS
Research Center for Open Science and Data Platform

GakuNin RDM：研究データ管理のためのSP



学認フェデレーション参加のIdPと連携可能
調達が不要でシステム導入が容易



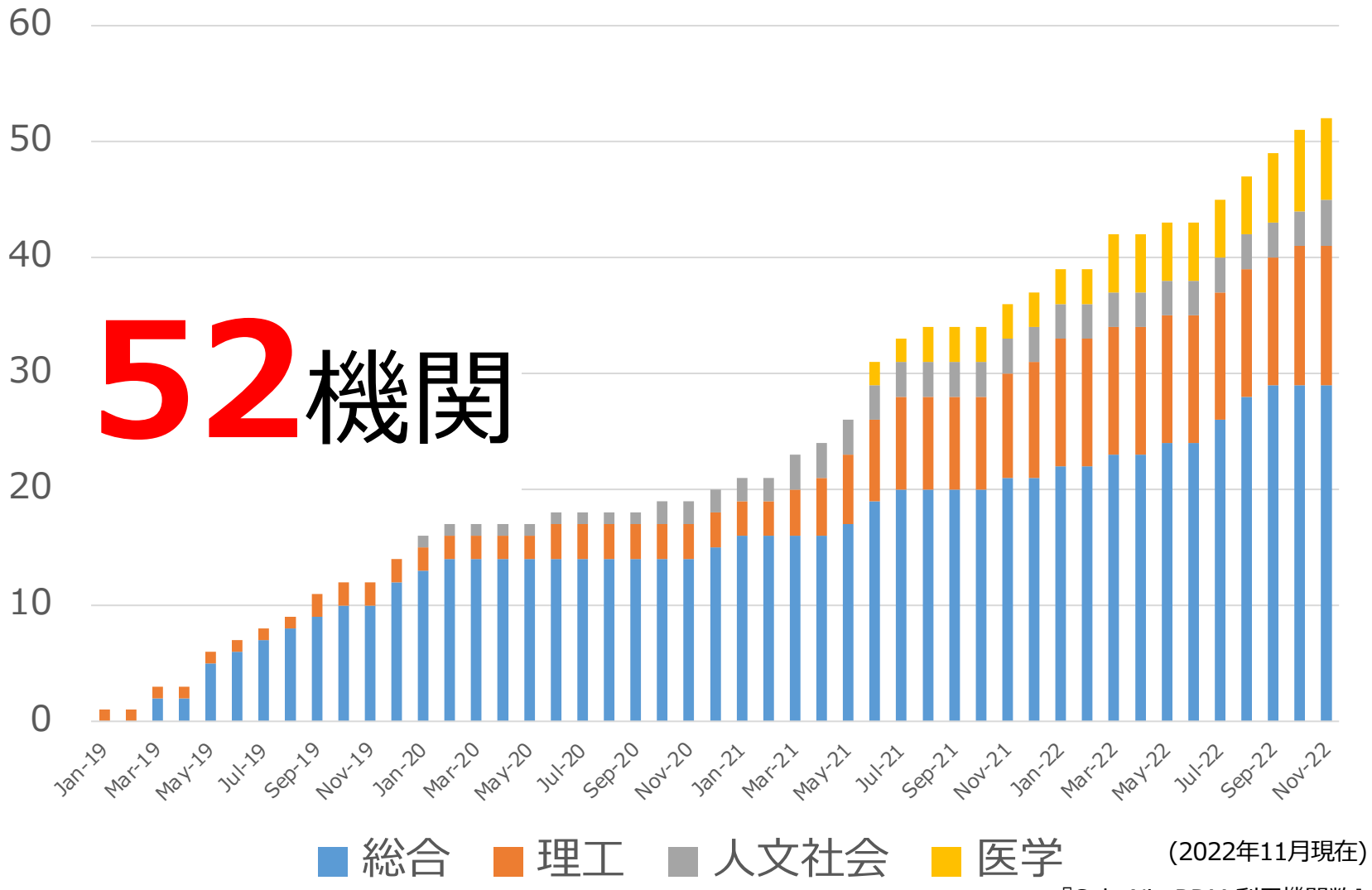


GRDMでは、学術認証（学認）フェデレーションにサービスプロバイダ（SP）として登録済みのため、学認に参加していればアイデンティティプロバイダ（IdP）連携のみで導入が可能。

学認参加前の機関はSPの利用申請とOpenIdPでも利用可。

NII RCOS
Research Center for Open Science and Data Platform

GakuNin RDMの利用機関数の増加



(2022年11月現在)

『GakuNin RDM 利用機関数』
https://support.rdm.nii.ac.jp/about/#a2

課題

NII RCOS
Research Center for Open Science and Data Platform

理化学研究所放射光科学研究センター 様 (SP利用者)からの認証サービスへのニーズ

状況：産学共同利用のデータセンター新設。組織内に技術者・研究者が多くいる。機関のIdPを新設。

視点：

SPring-8/SACLAデータセンターがGakuNin RDM（SP）を利用する観点から

タイムスパン：

- 中期（4年以内）で実現したい機能
  - 企業ユーザ利用に対応できる認証システム
- 長期（4年超）で検討する価値があると思われる機能・運用
  - 大学・国研等のユーザについて以下の情報がわかるIdPの運用を希望。
  - 学部学生、大学院生、職員の区別がつくように属性の値を入れて欲しい。

NII RCOS
Research Center for Open Science and Data Platform

『保健医療分野の国立試験研究機関』様からの認証サービスへの課題１

状況：全国の自治体、地方の機関や研究施設を中央で取りまとめ。組織内にITの研究者、技術者が少ない。機関のIdPは新設。

【国立試験研究機関での問題】

- 認証での課題については、以下がある
- 自施設でサーバを設置する場合、
  - システム部門やSEがいない研究機関では、IdPの設置・維持・管理は難しい。
  - 管理には工数が増大するため、研究者が教育・研究の時間が割かれる。
- 外部サービスを利用する場合、
  - 継続的に利用する財源の確保が難しい。
  - 既存のネットワークとの連携が困難な場合がある。
  - 定期的なネットワーク更新での対応が可能かが心配される。

NII RCOS
Research Center for Open Science and Data Platform

『保健医療分野の国立試験研究機関』様からの認証サービスへの課題２

【自治体などにおける問題】

IdP側課題

- 普段から、自治体からネットワークが繋げられない、ソフトウェアのインストールには申請が必要、添付ファイルは無害化してからでなければ開けないなど、自治体、保健所、地方衛生研究所などの問題があるところも多い。認証について検証してはいないが、上記の理由から問題が生じる可能性は高い。
- 自治体では、個人メールアドレスを付与されておらず、部署共通のメールアドレスを利用している。個人のメールアドレスを業務で登録することの問題、ドメインでの認証ができない問題もある。

SP側課題

- 自治体、保健所、地方衛生研究所などと研究をする場合には、大学機関等ではないため、e-Rad番号はある研究者がいても、GakuNin RDMに参加できない問題がある。大学においても、自治体、保健所、地方衛生研究所などと研究する場合も同様。
- OpenIdPでGakuNin RDM利用可能だが、施設や組織での利用についての承認や申請手続き、研究者によるOpenIdPの申請手続きが円滑にできない可能性がある。

NII RCOS
Research Center for Open Science and Data Platform

SP側での認証の課題整理

- **SPとIdPをセットで導入したいケース**
  - 機関単位でSPを導入したいので、IdPを整備して学認に参加させたいが、組織内ににIT技術者が不足しており、どうすすめてよいのか分からない。
- **学認参加機関以外のSPを利用したいケース**
  - 学認に参加していない企業、自治体、教育機関等のユーザも学認のSPを簡便に利用したい。
- **学認の規程と利用機関現場の実情のミスマッチ**
  - 部署単位でのメールアドレスやアカウントしかない場合ある。個人単位の多要素認証の方法がないケースもある。
  - 学認参加のIdPを持たない、多数の組織所属の少数ユーザを、総括機関・共同利用機関のIdPで管理できると運用が楽になる。
- **次世代認証対応ユースケースの醸成**
  - SPの利用機関ではAAL2/IAL2の必要性は感じているが、具体的なアプリケーションのニーズはこれから。SP側からも提案が必要。

NII RCOS
Research Center for Open Science and Data Platform

SP側の課題解決への取り組み

SP(GakuNin RDM)と次世代認証のIdP連携試験

実験環境

- GakuNin RDMの検証環境のSP
- 認証プロキシサービス(Orthros)の開発用IdP
- IdPホスティングサービスの検証用IdP
- 次世代認証Assurance Level対応の試験IdP(予定)

進捗

- IdP-SP間での認証連携の調整
- OpenIdPユーザが認証プロキシサービスを後継として使った際にSP側で問題がおきないよう検証をすすめる。
- 次世代認証のAssurance LevelへのSP側改修の対応

NII RCOS
Research Center for Open Science and Data Platform

次世代認証サービスへの期待

- **認証プロキシサービス(Orthros)**
  - 学認に参加していない企業、自治体、教育機関等のユーザも学認SPを簡便に利用できるIdPがあること。
  - 学認参加のIdPを持たない、多数の組織所属の少数ユーザを、総括機関・共同利用機関のIdPで管理できること。
- **IdPホスティングサービス**
  - 組織内ににIT技術者が不足してしていても、容易に、機関単位でIdPを整備して学認に参加できるようになること。
  - 部署単位でのメールアドレスやアカウントしかない場合でも利用できること。
- **次世代認証Assurance Level対応IdP**
  - 個人単位で多要素認証のデバイスがないケースでもAAL2でIdPを利用できること。
  - 利用機関での具体的なアプリケーションのニーズに対応したAssurance Levelの機能がSPとIdPで実現されること。

Thank you