学認クラウドゲートウェイサービスの概要およびデモ

2019年5月30日
学術情報基盤オープンフォーラム2019

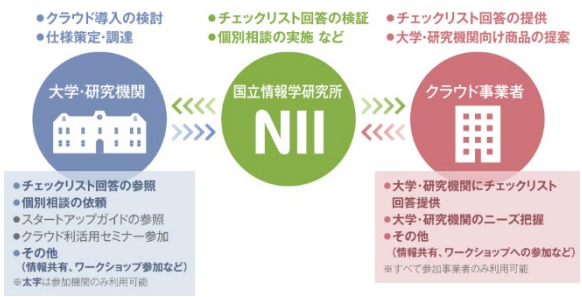
国立情報学研究所
クラウド基盤研究開発センター／クラウド支援室
西村　健

NIIのクラウド利活用支援活動

■ 大学・研究機関のクラウド利活用を様々なシーンでサポート

導入検討　調達　活用

<学認クラウド> 導入支援サービス

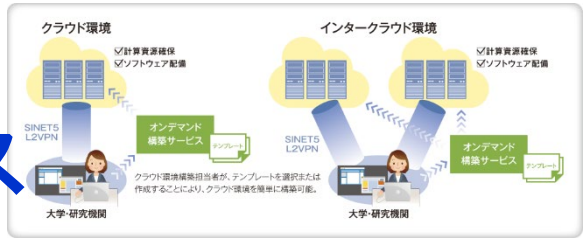


選択の基準や、導入・活用に関わる情報を整備し、お伝えするサービス

<学認クラウド> ゲートウェイサービス

クラウドサービスにワンストップでアクセスするためのポータル機能

<学認クラウド> オンデマンド構築サービス

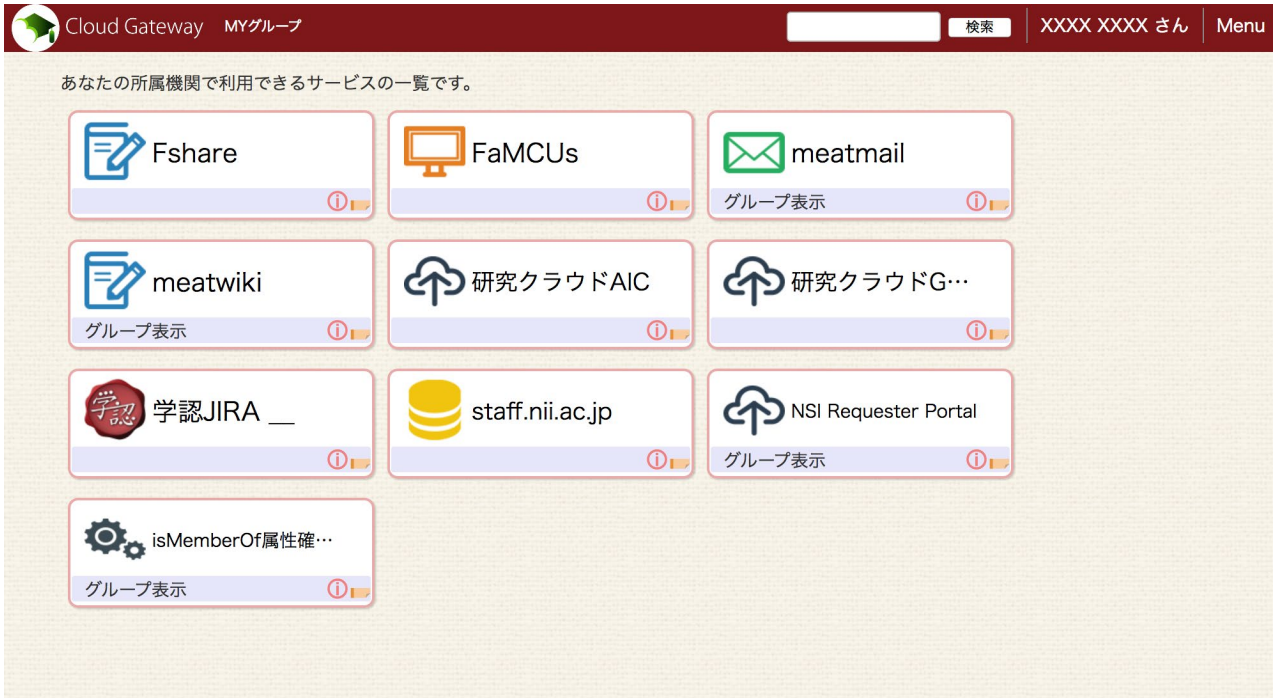


研究教育のためのクラウド環境構築を技術的に支援

2018年10月サービス開始

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～

- 一言でいえば、アクセス者が利用できるサービスを一覧にしたポータル
- 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）

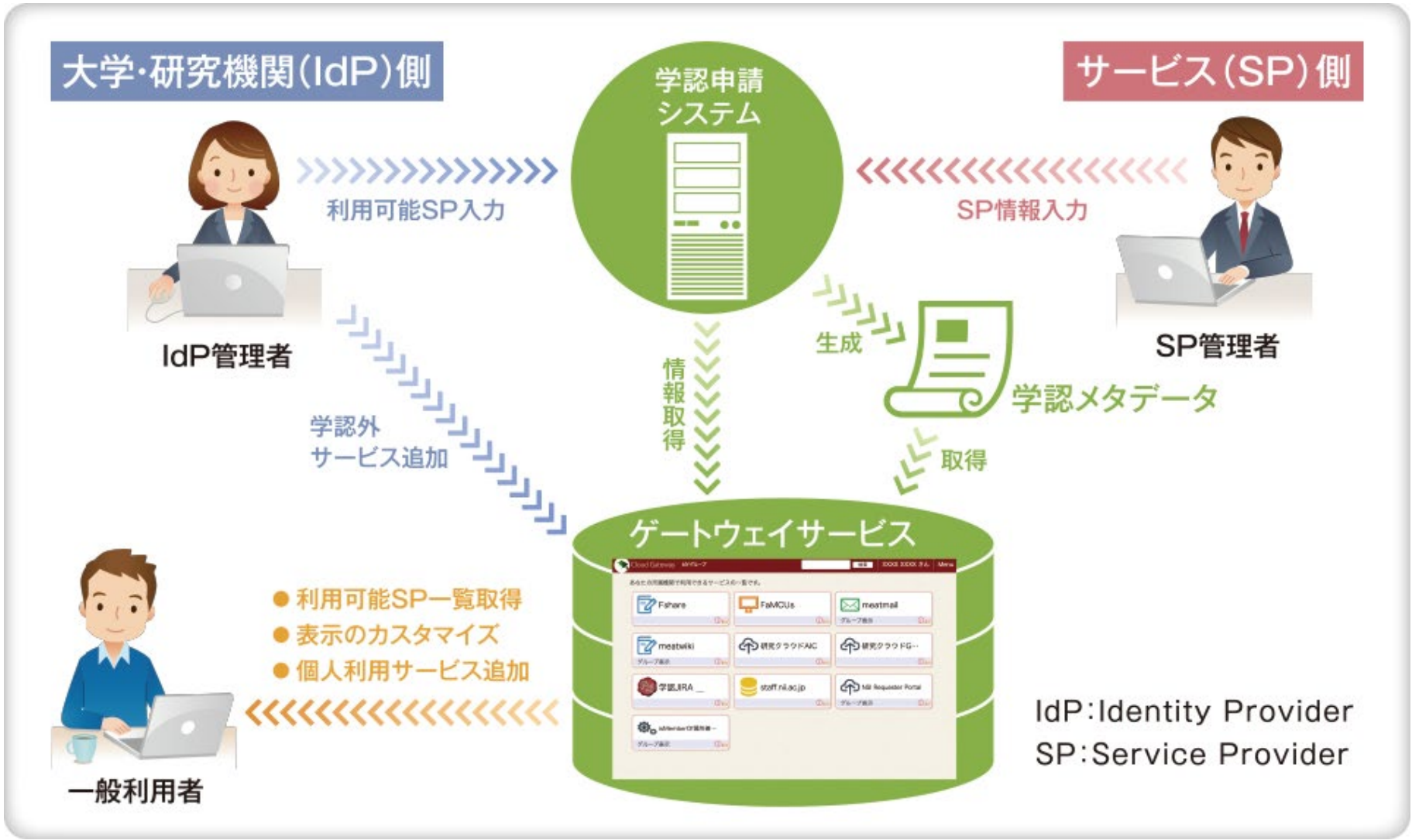


利用者のアクセス例

- 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

- 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、ということがなくなる

ゲートウェイサービスの登場人物と役割



※学認 - 大学・研究機関の認証基盤と商用・非商用のオンラインサービスの間のSSOのための枠組み

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
    - 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が属性送信設定しているSP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

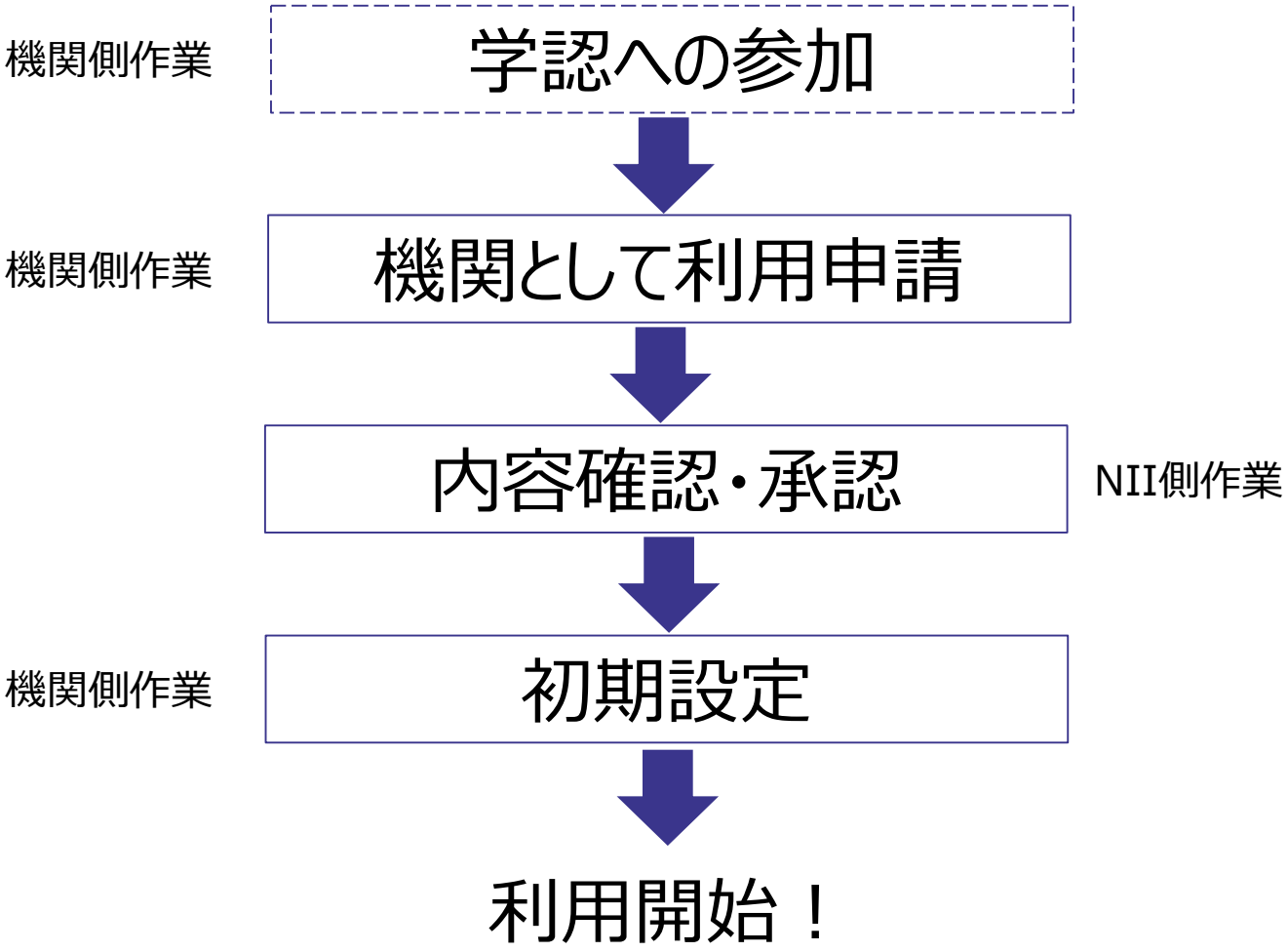
前提

- 学認に参加済みの機関からご利用いただけます
  - ゲートウェイサービスがSPとして所属機関を確認するため

グループごとの利用可能サービス情報も提供

- グループを作成し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
  - グループの例：共同研究グループ、研究室、etc.
  - 学認のGakuNin mAPサービスで培ってきたグループ機能を継承
    - 連携実績あり：meatwiki、しぼすけ等
- 利用者の「自分が使うべきサービス」が一覧できる

利用開始までの流れ



ゲートウェイサービスを使うメリット

- 利用者の立場から
  - 自分が使えるサービスが一覧できる
    （使えないサービスで迷わない）
  - サービス一覧をカスタマイズできる

- 学術機関(IdP)の立場から
  - 教員/職員を利用させたいサービスに誘導できる
  - 機関独自にポータルを用意する手間がない

- サービス提供者の立場から
  - サービス掲載によって利用者の目に留まる

デモ

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

- 利用申請受付中！学認に参加している機関の方は是非！
  - https://cloud.gakunin.jp/cgw/
  - 無料でご利用いただけます
- お問い合わせ・ご相談：cld-gateway-entry@nii.ac.jp

学認クラウドゲートウェイサービス アップデート

2019年5月30日
学術情報基盤オープンフォーラム2019

国立情報学研究所
クラウド基盤研究開発センター／クラウド支援室
西村　健

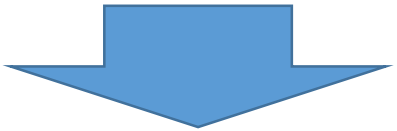
新機能・更新情報のご紹介

昨年オープンフォーラム以降の新機能や更新情報をご紹介します

- パブリッククラウドへのSSO
- コミュニティによるサービス情報更新の仕組み（提供予定）
- mAP Core APIの提供
- 規程類の構成とサービス提供主体・提供範囲の再確認

パブリッククラウドへのSSO(1/2)

- 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）
- ただし機関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
  - “誰”としてサインインしたいかは人により異なるが、その情報を属性として贈らなければならない
    - 同一人物でも複数の役割を持つ場合もある

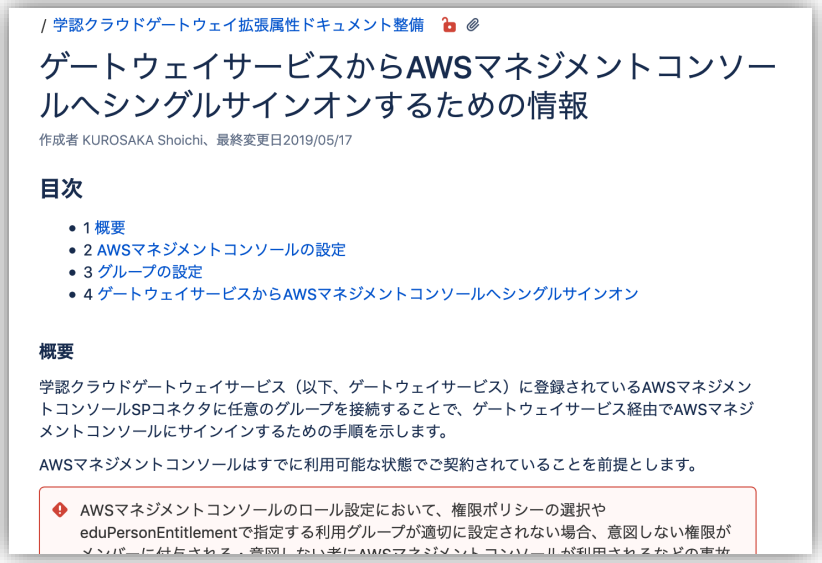


- 機関IdPで認証した上でゲートウェイサービスIdPが必要な属性をAWSに送信する
- 必要な情報はグループ管理者が自由に設定できる
  - 同一グループのメンバーには同一の権限を与えるモデル

※ AWS側にも若干の設定が必要

パブリッククラウドへのSSO(2/2)

■第一弾: 通称AWS連携 ベータ版
ゲートウェイサービスを介してアクセスすることで、機関IdPには手を入れることなく、機関IdPからAWSマネジメントコンソールへSSOできるようになります
手順書：https://meatwiki.nii.ac.jp/confluence/x/9Yp6Ag


/ 学認クラウドゲートウェイ拡張属性ドキュメント整備

ゲートウェイサービスからAWSマネジメントコンソールへシングルサインオンするための情報

作成者 KUROSAKA Shoichi、最終変更日2019/05/17

目次

- 1 概要
- 2 AWSマネジメントコンソールの設定
- 3 グループの設定
- 4 ゲートウェイサービスからAWSマネジメントコンソールへシングルサインオン

概要

学認クラウドゲートウェイサービス（以下、ゲートウェイサービス）に登録されているAWSマネジメントコンソールSPコネクタに任意のグループを接続することで、ゲートウェイサービス経由でAWSマネジメントコンソールにサインインするための手順を示します。

AWSマネジメントコンソールはすでに利用可能な状態でご契約されていることを前提とします。

AWSマネジメントコンソールのロール設定において、権限ポリシーの選択やeduPersonEntitlementで指定する利用グループが適切に設定されない場合、意図しない権限が

■ご興味のある参加機関の方はご一報ください！

コミュニティによるサービス情報更新の仕組み（提供予定）

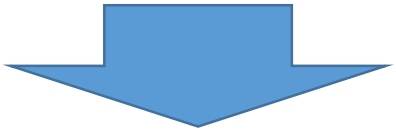
- ゲートウェイサービスに表示される一部サービスの情報が不完全という指摘あり
- SP自身からの情報提供のみでは限界がある
  - 例えば、英語情報しかない
  - サイトの更新に追随できていない場合もある
  - 特に1SPに複数サービスが存在する場合の情報が少ない

- 全参加機関の構成員が読み書きできるWikiスペースを提供します（予定）
- 現在ゲートウェイサービスが保持しているサービス名・アイコン・紹介文・リンク先を1ページで提供します
- いずれかの情報改善案をお持ちの方はコメントでお寄せください
- 定期的にコメントを集約しゲートウェイサービスの設定を更新します

- ご協力お願いします！

mAP Core APIの提供

- 従来ゲートウェイサービスが提供するグループ管理機能はWeb UIで操作する形態
  - メンバーの一括追加・削除が面倒
  - 情報源がSPにある場合にその反映が手間



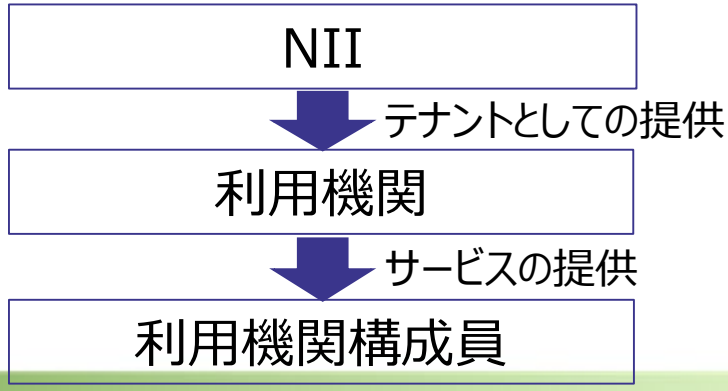
- グループ管理機能をREST APIとして提供します
  - SPがある利用者の権限でAPI呼び出しを行う想定
- クローズドベータ版として提供中
  - ドキュメント整備でき次第公開予定

- ご興味のあるSPの方はご一報ください！

規程類の構成とサービス提供主体・範囲(1/2)

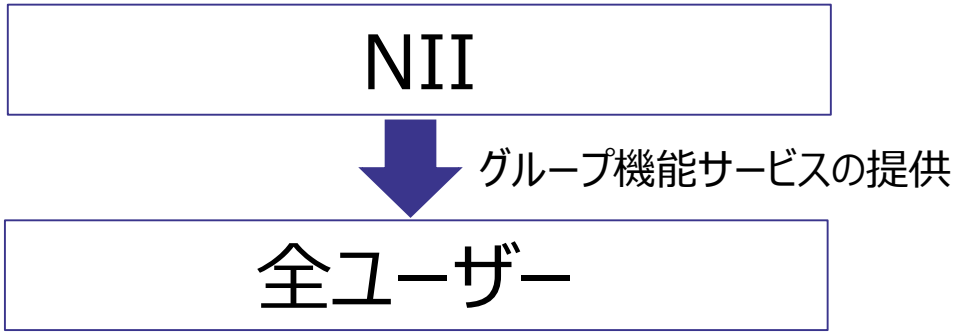
昨年規程類とサービス提供範囲の見直しを行いましたので、再確認の意味も込めて改めて説明します。

- 利用規程
  https://cloud.gakunin.jp/dist/pdf/stipulation_util.pdf
  - オンデマンド構築サービスと共通です
  - 利用機関向けに遵守すべき事項に加えて構成員に遵守させなければならない事項を記載しています
- 利用ガイドライン
  https://meatwiki.nii.ac.jp/confluence/x/K2NHAQ
  - 利用者（利用機関構成員）向けに遵守すべき事項を利用規程から抽出・解釈したものです



規程類の構成とサービス提供主体・範囲(2/2)

- ただしグループ機能は全学認参加IdPの構成員に提供しています
  - 当該機能についてのみサービス提供主体はNII
  - グループ機能利用ガイドライン
    https://meatwiki.nii.ac.jp/confluence/x/_IHyAQ
    - グループ機能の利用にあたって遵守すべき事項を抽出・解釈したものです
    - 利用規程の「利用機関」を「NII」と読み替えています



大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

https://cloud.gakunin.jp/

学認クラウド　検索