新学認：Progress in Two Years and Beyond

学認　次世代認証連携検討作業部会
佐藤周行

この発表について

- タイトルとこのページを入れて12ページになります。公演時間は12分を予定しています

本講演の要旨は次のようになります

- 「強い認証」の学認での配備に向けての今までの活動を報告します
- 「強い認証」のご利益と現状について少しお話しします
- 様々な検討を経て、IdPとSPを広く募集して、「強い認証」についての実証実験を開始しようとしています。積極的にご参加ください。

新学認（次世代認証連携）：Motivation

- 学認：2010くらいから
- 学認が広く使われてきていることを前提に
  - SAML（OIDC）を使って認証連携を行うことが当たり前になってきました。アカデミアではSAMLが主流です
  - 学外のサービス利用⇒当初の動機が電子ジャーナルというのは有名ですが、もはやそれに限定されることはなくなりました
  - **学内でも⇒学内共通アカウントのSSOでの利用**
- 便利になったことは実感していることと思います
  - 利用者の観点からも
  - 管理者の観点からも

現状を反省するに

- より広い範囲のサービスを使いたい
  - 現状、「大学等」の提供するアカウントが適切に管理されていることを前提にサービスが提供されている
    - ⇒**正しい！**
  - しかし、そのような「前提」が通用しないところもあるわけで
    - 医療関係、HPC等、自分たちのセキュリティ基準に照らして、上記が十分でないと判断される場合
    - インターフェデレーション（国際研究協力）
- 一段先のブレークスルーがないと、「彼ら」を説得するのは難しい
  - SPの立場からは、「ゆるい管理のアカウントで入ってこられては困る」
- もちろん、学内サービスでも、成績関係、人事関係等、現状より強い保証があればそちらを使いたいと思っているところはあるわけで

次世代学認

- 2021～
- 認証の強度を学認として内外に保証しよう
- 強化した保証認証強度を相手に納得してもらって、今まで提供を躊躇していたサービスを積極的に提供してもらおう

- （世界の情勢）**認証のリスク評価技術が進歩し、皆が納得する基準が成熟してきた**
  - NIST SP800-63, IGTF, …
  - 各種パスワードレス認証方式の提供
- それらを実装することで、フェデレーション内で基準が作られてきた（がなかなか拡大しない。一部はvaporware化している）
  - Kantara, InCommon, REFEDS, …
- 学認は、「強い認証」を本格的に配備し、様々なシーンで「実際に」利用可能にすることを決心しました

利用シナリオ

たとえば…

- さまざまなリソースへの利用登録にあたっての身元確認を大学アカウントを用いてオンラインでできるようにする
  - 共同利用機関等が受け入れている利用者も含むように
- 高価なリソースへのアクセスを大学アカウントでできるようにする

- 学内リソースへのアクセスをMFAを用いてよりセキュアにする

- **SPにもIdPにも**、学外でも学内でもご利益が感じられるように

ルールを決める公表する

- 身元確認のルール：IAL2規準の策定
  - https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=91396153&preview=/91396153/94342909/IAL2_operation-ver2.pdf
  - 多くの大学等で達成が可能ーTrusted DBの運用を前提
  - 組織外の研究者を受け入れる研究機関でも対応可能
    - **eKYC対応**
- 本人確認のルール：AAL2規準の策定
  - https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=91396153&preview=/91396153/94342915/AAL2_operation-ver1.pdf

技術的なサポートを行う

- MFAのうち、AAL2を満たすものを学認が評価し、登録する
  - 学認の**認証器レジストリ**を運用
  - 代表的なもの（スマートフォン上の各種authenticator等）を含むように調整しています

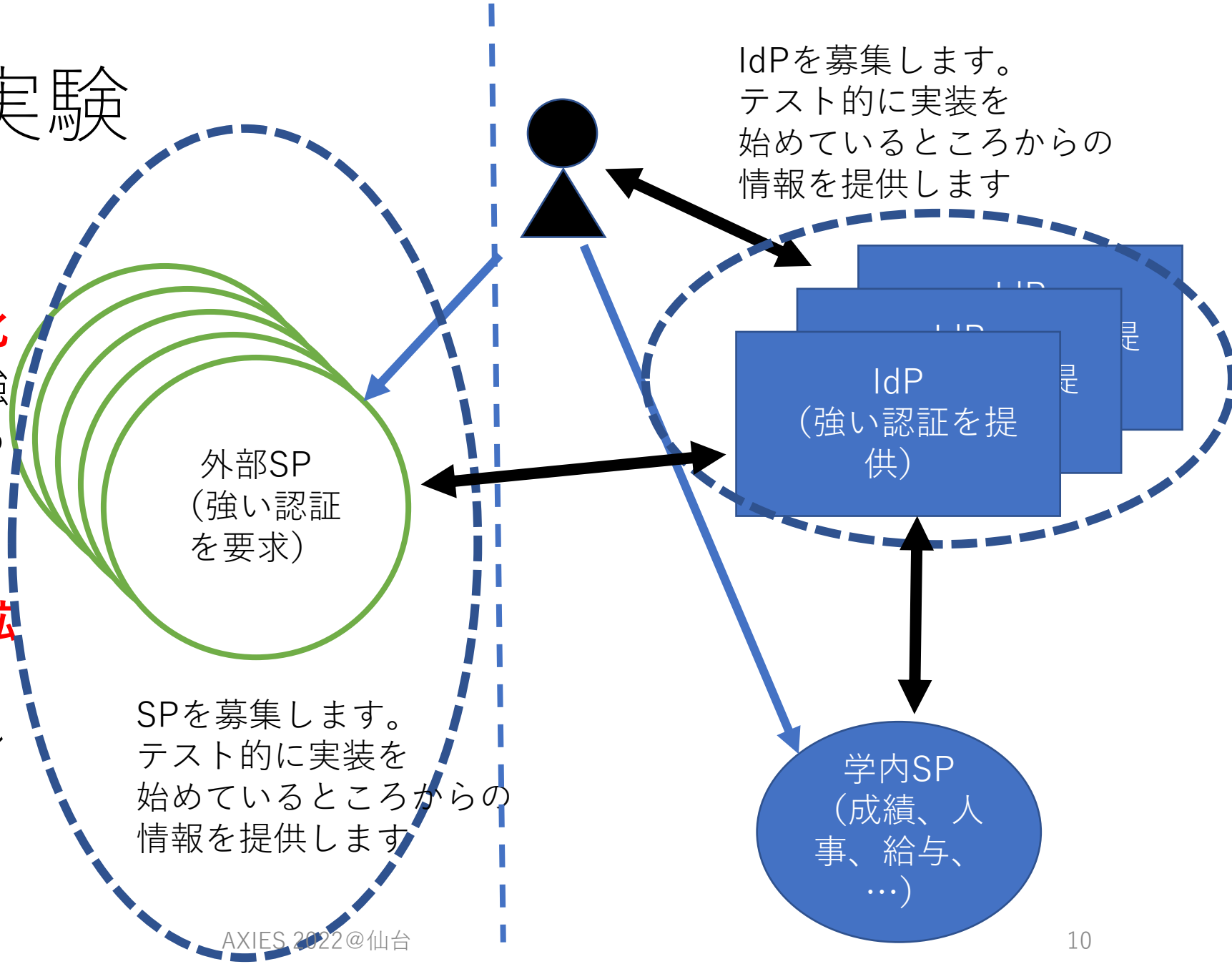
- IAL2, AAL2でIdPとSPが接続するための設定
  - 学認内で使う識別子指定
  - 各種サーバでの設定例
    - https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=91396040
  - 各種IdPでの設定のチェックシートを公開する（検討中）

仲間を増やす、テストをする

- 今まで、小規模のWGを作って、仕様を決め、文書を作ってきました
- ⇒IAL2, AAL2を実装したIdP, SPを実際に作って「高い認証強度」の認証連携を作る
- ⇒中規模実証実験の開始
  - **協力していただけるIdPとSPを募集します**
  - 学認が仕事の場を用意します
    - **運用作業部会内**
  - 学認が技術的サポートをします
    - 今まで作った文書の公開、設定例の公開、議論の場の提供
    - 多くは以下で公開しています
      https://meatwiki.nii.ac.jp/confluence/display/nextGAKUNINPublicDocuments

中規模実証実験

- 目的 for IdP
  - **学内での認証強化**
  - 学外にあって、強い認証を要求するSPを利用する
- 目的 for SP
  - **Onlineサービス拡大**
  - 特に手続きに関して



実験参加のSeeds

- 各種規準⇒meatwiki
- 技術情報⇒meatwiki, + 認証器レジストリ, +チェックリスト
- 運用に向けてのテスト
  - IdP
    - NII（Shibboleth）
    - 京大（SAME）
    - 東大（Azure AD）
    - ＋
  - SP
    - 学認RDM
    - ＋

最後に

- ご興味のある方は、https://www.gakunin.jpの「お問い合わせ」タブからお問い合わせください
- 皆様のご参加をお待ちしています