新学認のフレームワーク：実証の道筋

佐藤周行（学認）

＠第15回佐賀大学統合認証シンポジウム

2023/03/14

3回目

- 統合認証シンポの場をお借りし、「新学認」の説明の場をいただいてきました

#13 (2021) 新しいトラスト
#14 (2022) 次世代学認サービスメニュー:全体像とロードマップ
#15 (2023) 新学認のフレームワーク:実証の道筋

この発表

- 「新学認」への参加のお誘いです
  - 強い認証をサポート
  - 厳格なアカウント管理の実現
- 「中規模実証実験」の開始のアナウンス ＝ **実証の道筋**
  - IdPのアップグレードのために
  - 情報交換のための参加でも結構です

新学認とはなにか（復習）

- 次世代認証連携フレームワークにあるべき姿を求める
  - 強い認証の提供 → 各種オンラインサービス（学内・学外）が要求するセキュリティの提供
    - 身元確認、IdPの構成の統制
    - パスワード（only）に代わる強い認証器運用の推奨とノウハウ提供
    - 「強い認証」がIdPでなされている情報（アサーション）の流通のサポート
  - 共同研究、国際協力、産学連携等のサポート
    - 運用規準の明確化と相互運用性の確保

言葉の説明

- IAL: Identity Assurance Level (身元確認保証レベル)
- AAL: Authenticator Assurance Level (認証器保証レベル⇐一般には当人確認保証レベルと訳す)
  - Authentication Assurance Levelと一部で言っていて、こちらの方が良いような気もする
- FAL: Federation Assurance Level (この発表では触れない)
- 多要素認証器: 説明不要
  - 2FA (2-factor authenticator), MFA (multi-factor authenticator)

気運の醸成（情勢）

- パスワードonlyの不安が共有されるようになった
- 多要素認証のメニューが増え、利用のハードルが下がった
  - FIDO2を含む

- Digital Identity Guideline (NIST SP800-63-4) コメント募集中
  ⇒アップデートがロードマップ上に出現

Notes on NIST SP800-63-4

- 新学認の規準文書は63-3で作りました
- 63-4がコメント募集を始めた段階でチェックしました
  - 身元確認部分：IAL 1に大きな変化⇒IAL2は大きな変更なし
    - 自己申告は少し地位が下がる。検証するかしないかが1と2の差
    - いろいろなところへの配慮（プライバシー、公正さ）を前面に出したのは、多分連邦サービス関係で文書の地位がよりメジャーになったから
  - 当人確認部分：AALの認証器運用については生体認証の部分が充実したほかは大きな変更はない
    - 技術的な面（生体認証の評価、新しい技術の評価）は、評価の定まった部分はより詳細に
      - パスワードの部分は大きな変更はない
      - 新学認では、この部分を「認証器レジストリ」の運用にとじこめた（後述）
  - フェデレーション部分：詳細になった
- 3→4への変更で新学認では大きな改訂は予定しない
  - 改訂は通常のプロセスとして実施

新学認のAALに対する姿勢

- （従来）貴重な（外部）リソースを使うために、SPは強い認証を要求するだろう
  - たとえば共同研究用のリソース
    - これらが、自分で要求する認証レベルを満たすために、独自で認証システムを運用しているのが一般的だった
    - 強い認証は管理がそれなりに面倒
  - IdPが強い認証を提供することによって、これらSPの要求に応えることができる
    - 利用者の一部でOK
    - SPは、認証システムをアウトソースできる（最大のメリット）
- という利用シナリオを考えてきましたが…

- NIIの提供するサービス（RDM）
- HPCのリソース
- データサイエンスのリソース

＝インターネット上の研究活動を円滑に進めるための学術基盤
（NII RCOSの説明から）

それに加えて

- （現実）学内リソースでも、強い認証を提供して厳格な管理をした方が良いものが出てきた（コロナ禍によるリモートワークの一般化が後押しした部分もあるでしょう）
  - **VPN**
- よくよく考えれば、成績管理も厳格な管理をした方が良いのだろう
- （現実）MS ADなどでは、多要素認証をサポートしはじめた
  - Googleの多段階認証は措いておきます（リスク評価が収束していないが）
- スマートフォン等、利用者側でも認証器の格納デバイスがready状態に

特に生体認証の一般化

- スマートフォンでの指紋認証
- Windows Hello
- Face ID
- … (便利さの実感)　これだけでは1要素なんですが…

→ MFA採用への理解

機は熟した

https://www.gakunin.jp/news/20221115

GakuNin

日本語 English

検索

Top お知らせ 概要 IdP・SP一覧 参加情報 技術ガイド イベント 関連情報 情報交換メーリングリスト お問合せ ドキュメント

- 2022年度
- 2021年度
- 2020年度
- 2019年度
- 2018年度
- 2017年度
- 2016年度
- 2015年度
- 2014年度
- 2013年度

次世代認証連携検討作業部会に係る資料の公開について

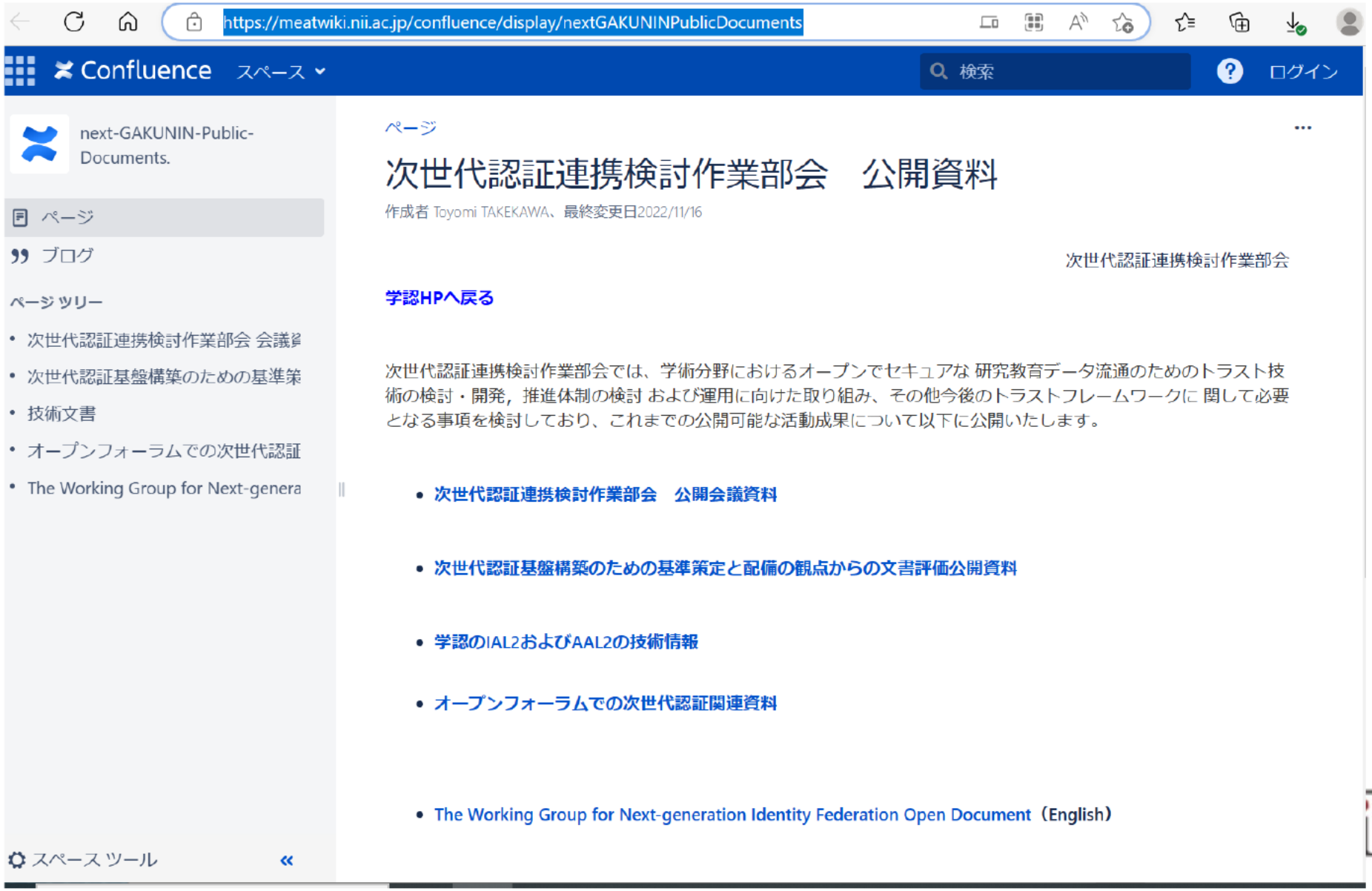
2022-11-15 15:36 by 中川

平素より本サービスの運営にご協力頂きありがとうございます。学認事務局です。

次世代認証連携検討作業部会では、学術分野におけるオープンでセキュアな研究教育データ流通のためのトラスト技術の検討・開発、推進体制の検討および運用に向けた取り組み、その他今後のトラストフレームワークに関して必要となる事項を検討しております。

このたび、これまでの活動成果の公開ページをご用意いたしましたので、お知らせいたします。本お知らせ掲載時点では令和3年度までの活動成果を掲載しておりますが、今後も拡充を予定しております。

公開ページ：


https://meatwiki.nii.ac.jp/confluence/display/nextGAKUNINPublicDocuments
Confluence
スペース
検索
ログイン
next-GAKUNIN-Public-Documents.
ページ
ブログ
ページツリー
次世代認証連携検討作業部会 会議
次世代認証基盤構築のための基準策
技術文書
オープンフォーラムでの次世代認証
The Working Group for Next-genera
スペース ツール
ページ
次世代認証連携検討作業部会　公開資料
作成者 Toyomi TAKEKAWA、最終変更日2022/11/16
次世代認証連携検討作業部会
学認HPへ戻る
次世代認証連携検討作業部会では、学術分野におけるオープンでセキュアな 研究教育データ流通のためのトラスト技術の検討・開発，推進体制の検討 および運用に向けた取り組み、その他今後のトラストフレームワークに 関して必要となる事項を検討しており、これまでの公開可能な活動成果について以下に公開いたします。
次世代認証連携検討作業部会　公開会議資料
次世代認証基盤構築のための基準策定と配備の観点からの文書評価公開資料
学認のIAL2およびAAL2の技術情報
オープンフォーラムでの次世代認証関連資料
The Working Group for Next-generation Identity Federation Open Document（English）

新学認のAALに対する姿勢（続）

- 規準文書を含む情報を公開しています
  - https://meatwiki.nii.ac.jp/confluence/display/nextGAKUNINPublicDocuments

- AAL ＝ 認証器の強さの評価＋運用の厳格さ
  （学認が責任をもつ）（各機関で適切に設定を期待）
- AAL規準文書は、運用の厳格さについて主に定める
  - 認証器と人の結合の強さが最大の関心事
  - 認証したセッションと人の結合の強さが次の関心事

認証器レジストリ

- セキュアに使える認証器のリストを学認が提供します
  - ラボレベルの検証はしない/できないのですが
  - 各種規格を参照することでセキュリティを評価することになるでしょう
- 第一弾は近日中にレポートが出ると思います
  - **ベンダー、団体の方**の協力が不可欠です
  - この場にも、認証器を提供 and/or 運用できるベンダーの方が参加していると理解しています
  - （この場を借りまして）**ご協力をぜひお願いします**
  - 詳細は学認までお問い合わせください

新学認のIALに対する姿勢

- 規準文書を公開しています
- IAL = 身元確認の確かさ + IdPへの正しい反映
  + ポリシーのパブリッシュによる説明責任
- 大学等機関では、個別に身元確認を実施するというよりは、一定の社会的な仕組みを使ってシステマティックに身元確認を行い、IdPに反映することが行われている
  - システマティックな身元確認の結果のシステマティックな反映の仕方が関心事になる

システマティックな身元確認とは

- 大学生では入学時
  - 高校からの調査書等
  - 入学願書と実際の入学試験時のチェック
  - 対面での学生証交付又はあらかじめ登録した住所への郵送
  - …
- 教職員は採用時
  - 住民票、パスポート等公的書類の提出
  - …
- ⇒機関等の持つDBへの統制の取れた登録
  - 命をかけて守るもの

- 日本の研究機関では、身元確認の強さは基本的に問題ありません（断言してよい）
  - いわゆる人事給与DB、学務DBがきちんと管理されていないところはないと思います
- それら「ごく良質の」DBの内容をIdPに反映するには、少し汗をかかなければいけないでしょう

- これらのポリシーを説明責任を果たす意味でパブリッシュすることが求められます
  - この文書主義は「面倒」だが、一番説得力を持つ

配備に向けての準備

- 技術的な配備可能性を検証するために、小規模のグループで検討してきました
  - IdPの種類（検討中）
    - SAME, MS AD, Shibboleth (generic)
  - **SPからテスト的に提供されるサービス**
    - 近日発表できると思います
  - 交換される属性（SPの要求にIdPがどれだけ応えるか）
  - …

中規模実験参加機関の募集

- 小規模グループでの経験をシードとして、より広い範囲で実験的に新学認の配備を予定しています
  - 強いIALとその認定（IdP）
  - 強いAALとその認定（IdP）
    - 認証器レジストリの運用を含む
  - サービス提供（SP）
    - 学内リソースの多要素認証化も対象になります
- **参加していただける機関を募集しています**
  - 情報収集を主にするのでもかまいません

中規模実験のお誘い

- 近々正式なアナウンスをすることを予定しています
  - 今までも、情報は一部に先出ししてきました
- この場でのこの発表でアナウンスされたと考えていただいて結構です
- 「運用作業部会」のもとに、場を設けます
- 「小規模グループでの検討結果」をシードとして積極的に提供します

参加に当たって

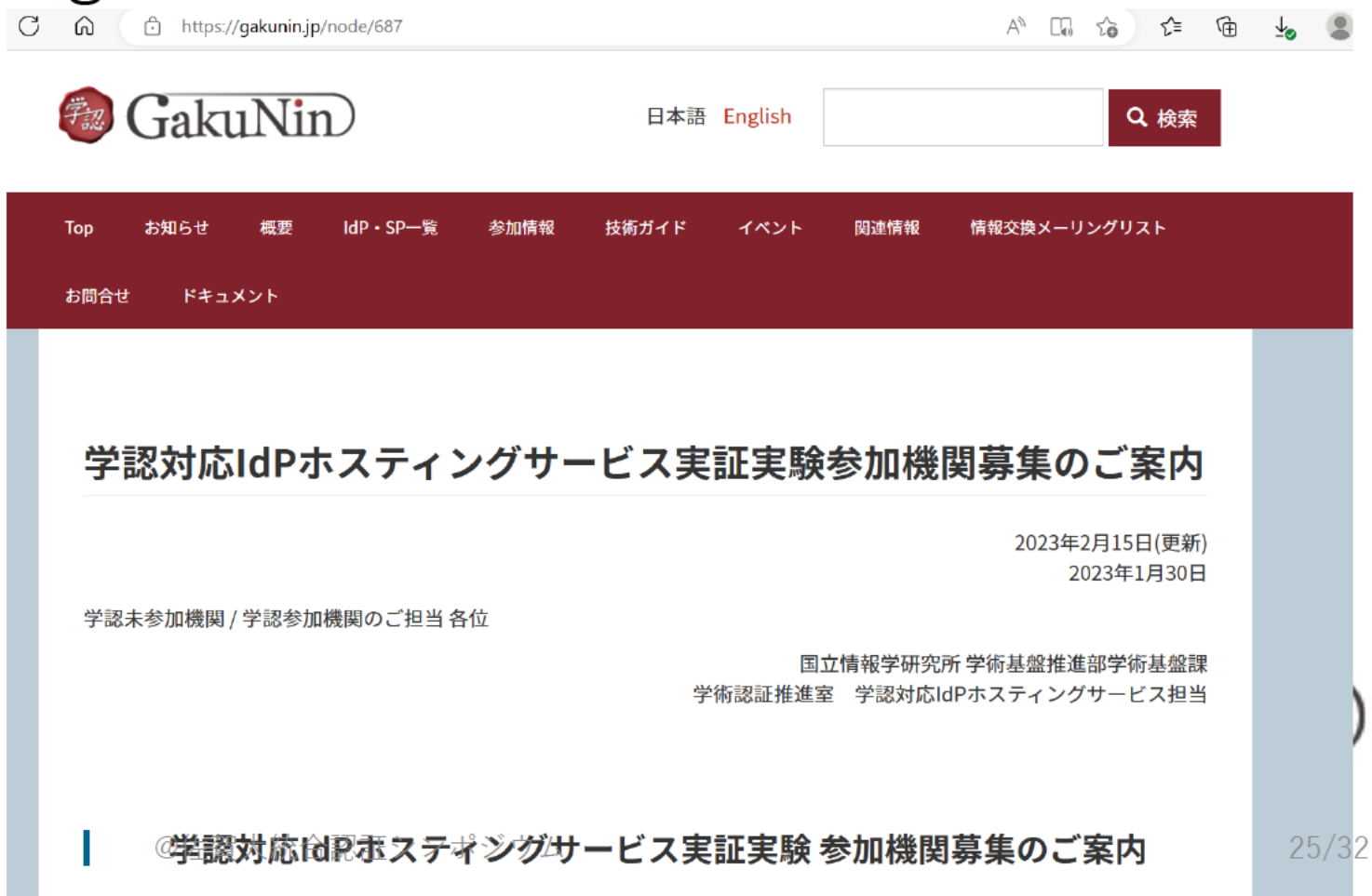
- 参加（含情報収集）をお考えの組織の方々
  - IAL（身元確認とIdPへの反映）整理
  - 日本の組織はだいたい大丈夫です（自信をもって言える）
    - 細かいところを詰める機会になると思います
    - 教職員・学生のアカウントはおおもとのDBから作成されるようになっている
      - おおもとのDBをどう作成するかについては、大学では文科省が正しく規制していることを理解しています
    - その他についても、作成の規則が決まっていて、その通りに作成される
    - アカウント管理に従事する教職員の統制がとれている
      - これはJSOXあたりの配備（21世紀初頭）で「IT全般統制」として話題になりました
  - 「高度なサービスを利用する人だけに適用する」はありです

「高度なサービスを利用する人」

- アサーション内で属性を交換することが求められるようになります
  - Emailや名前に関する情報を含みます
  - 従来の「仮名」でサービスを利用するスキームは、共同研究にはなじまないでしょう。
  - また、学内リソースの利用をするときも「仮名」は不要でしょう
  - ということで、積極的に属性を交換することで、サービスを便利に利用する方向に舵を切ることになるでしょう
- **どのような属性が必要ですか？**
  - 新学認はSPとIdPの交渉の場を提供します

IdP hosting

- 学認では、IdP hostingの実証実験に参加する機関を募集しています



IdP hostingにおけるIALの検討と整理

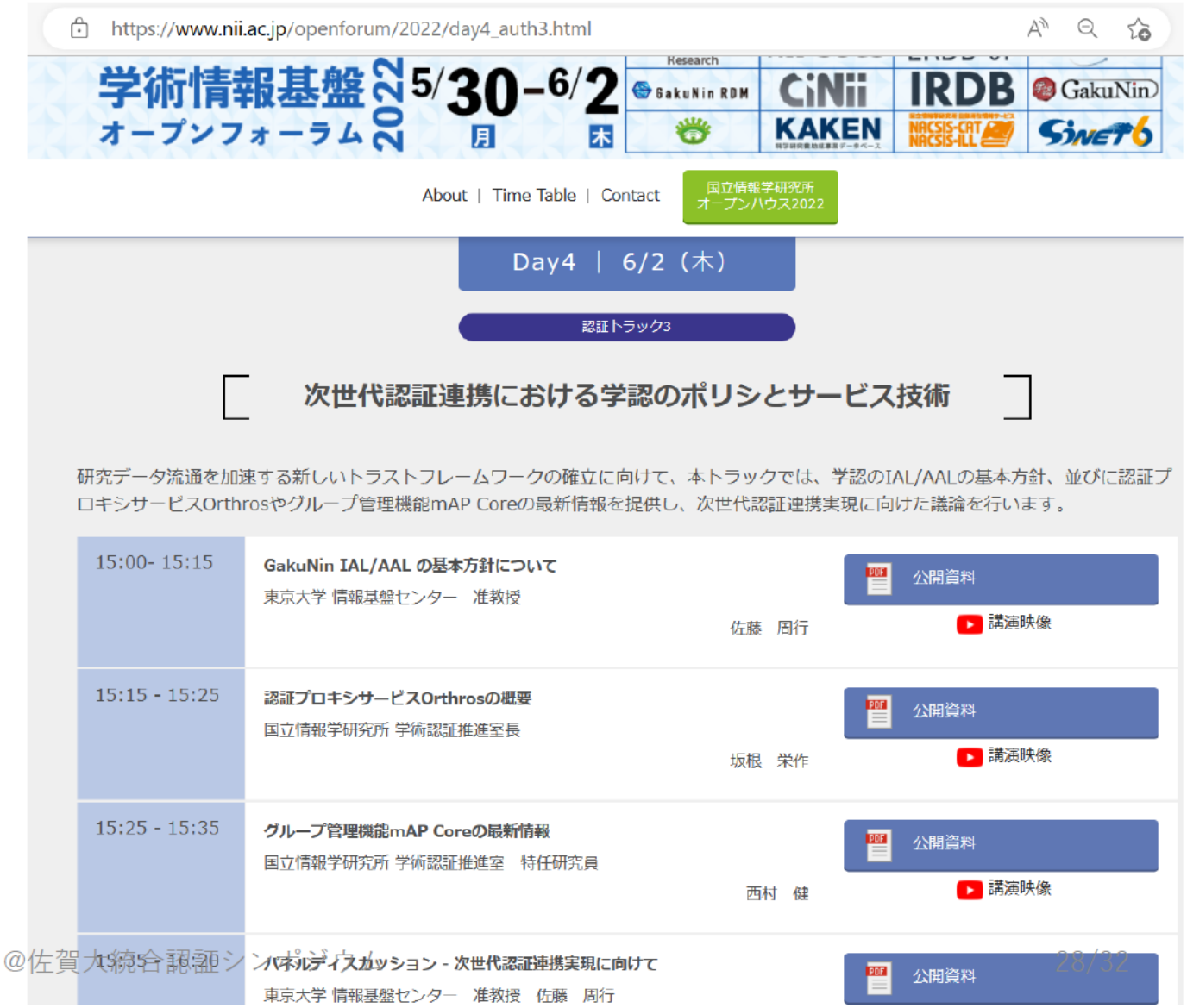
- 新学認のアイデンティティ管理関係には、様々なケースが持ち込まれるであろうことを予想しています
  - 中規模実験は、1. 現状を正しく把握した上で 2. 現状は、改善すべきなのか、その運用は十分受容できる範囲内にあるかを判断し 3. 日本の運用として「大丈夫」なのかを確認するために行います
  - ホスティングサービスに参加していただける機関がどのような問題を抱え、どう解決するかとも密接に関係するでしょう
  - 特に身元確認関係の運用は、国ごとに状況が異なるので、調整の余地があるでしょう　⇒中規模実験でのポイントの一つ
  - これで「大丈夫」となったら、国際的な場での議論

AALの検討と整理

- 先ほども述べましたが、成績管理等の学内リソースでも、そろそろパスワードonlyでは危ないと思います
- どのような多要素認証器が利用可能か⇒学認の提供する「**認証器レジストリ**」で技術的なサポートをします
- **現状、採用するIdPのサポートする多要素認証器を使うしかない**わけで…
  - 何が便利かについて、情報交換できると思います（⇒次スライド）
  - 例えば MS ADでは、電子証明書のサポートが遅れているとか
  - SMSを使うものは、フィッシング耐性の面でどうなのか、とか
  - 生体認証は何を採用するのが良いのか、とか

多要素認証は運用可能か

- 実は昨年、盛り上がりまして
  - 多要素認証は、現在どのIdPでも最低一つは利用可能になっていて
  - すぐにでも運用可能になる状態（「機は熟した」状態）
- しかし、細部のツメはなかなか簡単ではなく
  - 多要素認証の運用コストはそれなりに大きい
  - 怪しい認証器もあって
    - スマートフォンの通知画面にOTPが表示される仕様になっているものとか…



AALの運用の実際

- IALと異なり、AALはグローバルな基準で運用ができると思います
- 実は、どのIdPを採用するかでどの多要素認証器を利用可能かが決まってしまうのが現状です
- どのIdPで、どの（多要素）認証器が利用可能かについての情報交換の場を提供します
  - ベンダーの公式サポート・非公式利用
  - Configの書き方
  - Shibboleth（Generic）については、NIIが得意とするところです
- 小規模グループで、いくつかのシステムについて対応可能性を検討してきました

フェデレーションのサポート

- 学認では、IAL, AALに関係する情報を交換するためのプロトコルを定めます
  - 現在のIdPのConfigを少し変更すればOKになるはずですが、
  - 属性の一部については、簡単な変更では対応できないかもしれません
  - この点についても実験で確認していきたいと思います

終わりに

- 強い認証を運用する機は熟しました
- サービスの価値を高めるためにも、強い認証を利用者に提供することが必要です
- 学認は、規準文書を公開し、中規模実験でその実現可能性をテストすることにしました

- IdPを運用する機関と、それに加えて、技術を提供するベンダー、団体の協力があると心強く思います。ぜひ参加をご検討ください。→**お問い合わせは学認まで**

https://www.gakunin.jp

GakuNin

日本語 English

検索

Top お知らせ 概要 IdP・SP一覧 参加情報 技術ガイド イベント 関連情報 情報交換メーリングリス… お問合せ …キュメント

学術認証フェデレーションとは

学術認証フェデレーションとは、学術e-リソースを利用する大学，学術e-リソースを提供する機関・出版社等から構成された連合体のことです。
各機関はフェデレーションが定めた規程（ポリシー）を信頼しあうことで，相互に認証連携を実現することが可能となります。

学術認証フェデレーション「学認（GakuNin）」に参加を希望される方へ

全国の大学等とNIIが連携して構築する学術認証フェデレーション「学認（GakuNin）」では、運用フェデレーションとテストフェデレーションの2種類のフェデレーションを提供しています。

IdPやSPの構築の際には、原則として、参加情報に示すように、まずテスト環境で動作確認していただいた後に、運用フェデレーションに移行していただくようお願いしております。

「学認（GakuNin）」に接続するIdPあるいはSPの構築には、学認技術運用基準（参加情報以下を参照）に従い、本サイトの技術ガイドを参考にしてください。また、構築・設定に関する質問は、情報交換メールをご利用ください。国立情報学研究所（NII）による支援および先行大学からの、適切なアドバイスを受けることができます。

技術ガイド