



新しいトラスト

佐藤周行（学認）

@NII Open Forum 2021

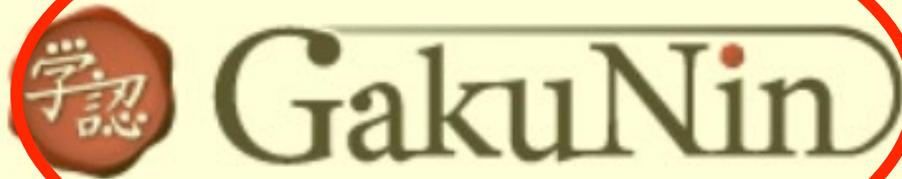
2021/7/8

概要

- この発表は、NIIが構想している「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」についてです
- 研究データ流通、リソース利用のために、トラストを作りなおし、学術コミュニティ全体をカバーし
- ビジネスセクターとも連携し、
- 国際協力を促進するための
- 認証を核としたトラストフレームワークを構築したいと計画しています



全日本・全世界に広げる信頼の輪



大学等研究機関

分野別研究プラットフォームA

分野別研究プラットフォームB



- 安定した運用がなされている「学認」は、「安定」と「普及」を追及してきました
- 現在、参加機関は244（2020/9/1時点）を数えています
- NIIは、技術支援を積極的に行っています
- 毎年「IdP運用状況調査」を行って、運用状況を確認しています
 - 実施要領、技術基準への準拠状況確認
- 「トラストフレームワーク」のお手本的な運用をしています



その一方

- 一部の「高度な」サービスを提供する研究コミュニティ（NIMS、HPCIや GakuNin RDM等）は、大学のアカウントでサービスを利用することを躊躇してきました（組織内でのアカウント作成基準が不明、認証の強度が足りない等）
- 学認は、大学のアカウントで外部サービスを利用可能にするものでしたが、それがいまいち信頼されていないことを表しています
- 結果として、研究コミュニティごとにトラストが形成されることになっていました



Twitterで富岳を応援！
ハッシュタグでつぶやこう

#富岳応援

お問い合わせは
ヘルプデスクまで

課題申請・利用に関する
FAQ

随時募集課題
受付



データサービス DICEとは 利用方法 お知らせ

NIMS 物質・材料データベース (MatNavi)

NIMS 物質・材料データベース(MatNavi)は、新材料の開発、材料の選択に貢献することを目的としています。MatNaviは、高分子データベース、NMRスペクトル・・・)、無機材料データベース(結晶構造、状態図、物性・・・)、金属材料データベース(密度、弾性係数、クリ・・・)など、十数種類の材料データベースで構成された統合データベースシステムのようなアプリケーションも提供しています。これらのデータベースはユーザ登録を行えば、無料で各種データベースを検索・閲覧

MatNaviユーザ登録・認証システム移行に関するお知らせ

NIMS物質・材料データベース(MatNavi)は更なるセキュリティ強化のため、2020年12月1日にMatNaviユーザ登録・認証システムを含む11/30以前にユーザ登録された方は、再度ユーザ登録が必要になります。旧システムにご登録いただいたユーザ情報につきましては、全て破棄され、ユーザ登録は無効となります。皆様には大変ご不便とお手数をおかけ致しますが、ご対応のほどお願い申し上げます。

https://rdm.nii.ac.jp

GakuNin RDM

検索 所属している機関

GakuNin RDM

研究データ管理による研究推進と研究公正

を受けて国立情報学研究所 (NII) がサービスを提供しているものであり、利用にあたり、利用機関が定めた規程が適用されます。また、GakuNin RDMでは、研究データ管理を目的にクッキーを利用しております。GakuNin RDMをご利用されるお客様は、ご同意ください。「同意する」をクリックまたは当サイトの利用を継続されることで、



研究コミュニティと利用者の利便性

- 研究コミュニティ参加者の大きな部分は、学認参加組織のメンバーと被ります（事実）
- 大学の学内システムのアカウントをそのまま、研究プラットフォームで使えないだろうか
 - DBへのアクセス
 - 各種システムへのログイン、またはシステム上のアカウント作成
- 研究コミュニティ側は、権限管理に集中できる
 - 本人のアカウント管理を大学や企業に受け持ってもらう
 - 大学や企業は、アカウントの価値を高めることができるだろう



問題点

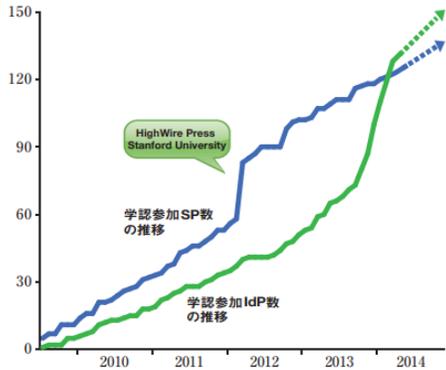
- 高度なサービス、リソースを管理するために「納得するまで」認証を強化するのは当然です
 - コミュニティが自らこの部分を管理するという発想は「あり」です
- しかし、「われわれ」は、研究機関において、内部でアカウントを持っています
 - そのアカウントで外部の高度なサービスを利用できるようにならないだろうか
- そして、学認はその初期からID連携による学術環境の高度化を唱っていましたが⇒今、もう一度初心にかえる



学認の初期 (2014年版パンフレット)

潜在的参加機関数は約800!

全国約800の大学等でインフラ整備が進行中。「学術クラウドには「学認」という時代がやってくる。NIIでは、全国の約800の大学等を結ぶSINET(サイネット)を提供し、学術クラウドの活用を支援しています。これは、これらの機関すべてが「学認」に参加できる基盤を有していることを意味します。もちろん、SINETに接続していない機関からでも「学認」に参加可能です。一方、SPの参加数は現状約120ですが、その伸びは順調に推移しており、機関の増加と共にSP側の参加に対するインセンティブも増大中です。「学術クラウドなら「学認」という時代はすぐそこまで来ています。



学認参加への手順

学認に参加するには、IdPやSPの構築を行うとともに、学認のWebサイトから新規IdP申請または新規SP申請を行います。

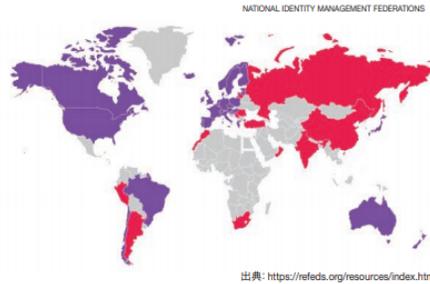
学認WebサイトURL: <https://www.gakunin.jp/>



世界の潮流に乗った技術を採用

標準プロトコル「SAML」による運用で国際化への対応も万全

学認は、世界中の学術認証フェデレーションで採用されているSAML (Security Assertion Markup Language) で運用されています。



出典: <https://refeds.org/resources/index.html>

学認では、IdPとSPにおける認証の通信方法として、標準プロトコルSAMLを採用しています。これを実現するためのデファクトスタンダードソフトウェアが、米国Internet2が開発したシボレス (Shibboleth) です。学認でも、多くのIdPやSPがシボレスを使って運用されています。また、シボレス化されたeLearningシステムやeScienceプラットフォームが世界中で提供されつつあります。将来は、大学や国の枠を超えた国際共同研究への利用が期待されています。

安心・安全でトラブルフリーな導入を実現

学認では参加に際し、接続試験と本格運用の2段階のステップを提供し、安心・安全な導入を実現しています。IdPやSPが学認への参加のためにシステムを構築する際、原則として、まずテスト環境で動作確認した後、運用フェデレーションに移行します。それぞれのフェデレーションへは、学認申請システムから参加申請します。

①テストフェデレーション

接続試験を目的としたテスト環境を提供し、構築したIdPやSPの動作試験を行うための環境。シボレス以外のSAMLに準拠したシステムについても、接続試験を行った上で、運用フェデレーションに参加することが可能です。テストフェデレーションはどなたでもご利用いただけます。

ID連携で学術環境の高度化を加速

クラウド時代の学術コンテンツ流通革命



そして、2021年～

- 次世代認証連携検討委員会を作りました
- 学認が、研究コミュニティに広く役立つための、トラストの再構築を行います
 - 研究コミュニティが信用してくれるような組織アカウントのトラスト
 - 身元確認
 - 認証レベル



解決に向けて検討を開始

- 大学で行う本人確認は、「たいていの場合」しっかりしていることが「わかった」
 - 組織の行う保証、継続的な保証は大きな力
- 従来の組織アカウントの運用だけでは…ということもわかってきました
 - フリーランス、または組織アカウントを持たない研究者は誰が身元を保証するのか（現状、研究コミュニティごとに苦労しながらやっていることが「わかった」）
 - 組織間異動で、身元の異動に便宜を図ることができるか



- IDaaSやNIIが最後の砦になってくれるか
 - 強い身元確認を代行してくれる
- 他の研究コミュニティでの保証を援用
 - 学会その他
- アカデミア以外の方法論を援用
 - eKYC
- 多くの人と多くの研究コミュニティに対して身元を広く保証



学認は、この活動を通して

- 身元確認を行う手続きについての基準を提示します
 - 抽象的なものではなく、具体的なもの
 - 抽象的に示さざるを得ないものは、解釈の基準を示します
- 国際的な相互運用性（eduGain, IGTF, Kantara等）に配慮します



国際協力

- これらの動き・問題は、日本に特有のものではありません

The image displays three overlapping browser windows illustrating international collaboration in science:

- Top Window (European Commission):** Shows the URL `https://ec.europa.eu/info/research-and-innovation/strategy/goals-research-and-innovation-polic...`. The page title is "European Open Science Cloud (EOSC)". The content includes "What the cloud is, how it relates to other strategies, how it was developed, and how it will evolve in the future."
- Middle Window (LIGO Scientific Collaboration):** Shows the URL `https://www.ligo.org`. The page title is "LSC LIGO Scientific Collaboration". The navigation menu includes "News", "Detections", "Our science explained", "Multimedia", "Educational resources", "For researchers", "About the LSC", and "LIGO Lab".
- Bottom Window (CILogon):** Shows the URL `https://cilogon.org`. The page title is "CILogon". The content includes "What the European Open Science Cloud (EOSC) is" and "Development of the EOSC until 2020".

On the right side of the slide, there is a plot titled "f gravitational-wave e" showing the frequency f versus the mass M/M_{\odot} . The plot displays several curves representing different gravitational-wave events, with two specific events labeled: GW190412 and GW190521. A dashed line indicates a threshold at $m_2 = 3M_{\odot}$.

eduGainが世界的なプラットフォームを提供

GEANT **eduGAIN**

Members Joining Tools Policy framework Operations Support Wiki Main webpage

Members > Membership and status

Quick filter

Participants (71) Voting-only members (2) Candidates (7)

Participants

- AAF(Australia)
- AAI@EduHr(Croatia)
- AAI@EduMk(North Macedonia)
- ACONet Identity Federation(Austria)
- AFIRE(Armenia)
- ARNaai(Algeria)
- ArnesAAI Slovenska izobraževalno raziskovalna federacija(Slovenia)
- Belnet Federation(Belgium)
- Canadian Access Federation(Canada)
- CAFe(Brazil)
- CAFMoz(Mozambique) ▲
- CARSI(China)
- COFRe(Chile)
- COLFIRE(Colombia)
- CSTCloudFederation(China)
- CyNet Identity Federation(Cyprus)
- DFN-AAI(Germany)
- Edugate(Ireland)
- eduID.cz(Czech Republic)
- eduID.hu(Hungary)
- eduID Luxembourg(Luxembourg)
- eduIDM.ma(Morocco, Western Sahara)
- FEBAS(Belarus)
- φEDUrus(Russia)
- FEIDE(Norway)
- FENIX(Mexico)
- Fédération Éducation-Recherche(France)
- FIDERN(Zambia)
- GakuNin(Japan)
- Grena Identity Federation(Georgia)
- GRNET(Greece)
- HAKA(Finland)

Europe

World

もちろん認証についても

- パスワードを超えた強い認証システムを運用するための技術サポートを計画します
 - スマートフォンを使った認証の運用ガイドライン
 - 電子証明書を使った認証の運用ガイドライン
 - その他、ハードウェアや生体情報を用いた認証の運用ガイドライン
- 認証器（Authenticator）の運用の本人確認のレベルをつくりま
す



学認の役割

- 研究コミュニティに対して
 - 認定した組織、アカウントが十分な認証レベルを持っていることを保証します
 - 「十分な認証レベル」について、認定ポリシーを公開し、運用します
 - IDaaSやOpenIdP等の認定を通して、広い範囲をカバーします
- 大学等組織に対して
 - 研究コミュニティのリソース利用を、大学アカウントでできるように、認定システムをくみ上げます
 - 認定レベルを高く保つための技術的なサポートをします



研究開発

- 「トラストフレームワーク」の構築に必要なものとされてきたものには次のものがあります
 - ポリシー策定と手続きへの具体化
 - 保証レベルのためのプロファイル策定
 - 監査技術
- 前記のような目的を達成するには、+アルファが必要になることがわかっています
 - ポリシー⇒手続き策定のためのリスク評価技術
 - 特に、市場に投入されている様々な認証技術のリスク評価
 - メタデータの効率的な流通のための技術

