学認

学内説明用資料雛形

平成25年12月

国立情報学研究所

※本資料は、新たに学認に参加しようとする大学の担当者が、学内の関係者に学認とは何かを説明する際に、説明資料の雛形として利用できるよう作成した文書です。

学術認証フェデレーション（学認：GakuNin） 説明資料

目次

[1 学術認証フェデレーション「学認」とは 2](#_Toc374693787)

[2 大学が学認に参加することのメリット 4](#_Toc374693788)

[2.1 大学のメリット 4](#_Toc374693789)

[2.2 学生・教員のメリット 4](#_Toc374693790)

[2.3 学認参加によりSSOで利用可能になるサービス（平成25年12月現在） 4](#_Toc374693791)

[3 学認参加の要件 6](#_Toc374693792)

[4 大学で用意する必要のあるもの(IdP) 6](#_Toc374693793)

[5 運用体制・委員会について 7](#_Toc374693794)

[6 IdP構築にかかる費用（業者に構築を依頼した場合） 7](#_Toc374693795)

[7 サービス開始までのロードマップ 9](#_Toc374693796)

[8 個人情報の扱い 10](#_Toc374693797)

[9 参考：Shibboleth 、SAML、LoA 11](#_Toc374693798)

## 学術認証フェデレーション「学認」とは

　学術認証フェデレーション（以下「学認」という）とは、国立情報学研究所(以下「NII」という)や大学、出版社等で構成された連合体で、学認で定めた規程のもとにWeb上の認証連携を実現している。

　この連携により、契約済みの電子ジャーナルなどのサービスが、大学の発行したID/パスワードで自宅や出張先から利用できるようになる。また、シングルサインオン機能により、1度の認証で異なるサービスを利用することも可能である。

　認証連携にあたっては、大学とサービス提供者の間に信頼関係が必要となる。サービス提供者は、各大学にて認証されたユーザが正しく管理されているユーザであることを信頼する。各大学においても、サービス提供者に送信した属性情報が不正に利用されないことを信頼する。学認では、参加機関の信頼関係を構築するためのルール作りと、きちんとユーザ管理されているかの定期的な調査を実施している。

　学認への参加機関数は、2013年12月時点で、IdP（Identity Provider：大学等)が90件、SP（Service Provider：サービス提供側）が110件となっている。

[解説]

　学認参加機関の最新情報については、https://www.gakunin.jp/participants/にて公開しておりますので、適宜修正ください。

1. ログインボタンを押す

2. 所属機関を選択する

3. 大学のID/パスワードを入力する

4. 学外からでも大学内からの利用として認識される

図1 学認を利用したCiNiiのログイン

110SP

　　　　　　IdP数(大学等)　　　　　　　　　　　　　　SP数(サービス提供側)

図2 学認参加機関数（平成25年12月現在）

## 大学が学認に参加することのメリット

* 1. 大学のメリット

　認証連携の機能には、Shibboleth（シボレス）[[1]](#footnote-1)と呼ばれる技術が使われており、学内の各サービスをShibboleth対応させていくことで、それぞれで認証用のID/パスワードを持つ必要がなくなり、ID管理業務を軽減することができる。また、リスク対策を一つの認証基盤に集中することができ、セキュリティの向上および対策の効率化が見込まれる。

* 1. 学生・教員のメリット

　大学が契約している電子ジャーナルのうち学認に対応しているジャーナルについては、学外から自身の大学IDで利用可能となる。そのため、電子ジャーナルごとのユーザ登録が不要となり個人情報の露出機会を軽減できる。また、一度のID/パスワードの入力で複数のサービスをまたがって利用できるシングルサインオンにより、別の電子ジャーナルを閲覧する際にも、学認対応機関であれば新たな認証なしに利用可能となる。

　電子ジャーナル以外にも、eduroam[[2]](#footnote-2) 参加機関であればEduroam-Shibサービスを利用してeduroam用の一時アカウントを発行したり、学生の場合はMicrosoftが提供するDreamSparkに代表されるツール等が利用できるようになる。

* 1. 学認参加によりSSOで利用可能になるサービス（平成25年12月現在）

|  |  |  |
| --- | --- | --- |
| **組織名** | **サービス名** | **要契約** |
| Annual Reviews | Annual Reviews | ※ |
| BioOne | BioOne | ※ |
| CUP | Cambridge Journals OnlineCambridge Books Online | ※ |
| Cengage Learning | Cengage Learning | ※ |
| EBSCO | EBSCO host | ※ |
| Elsevier | ScienceDirectScopus | ※ |
| Emerald | Emerald | ※ |
| HighWire Press | HighWire 学認対応電子ジャーナル( <https://meatwiki.nii.ac.jp/confluence/x/F4Df> ) | ※ |
| IEEE (Institute of Electrical and Electronics Engineers) | IEEE Xplore | ※ |
| IOP | IOPscience | ※ |
| Karger | S.Karger AG | ※ |
| Masaryk University | Atlases - Pathology Images |  |
| Microsoft Corp. | Microsoft Academic Verification Engine (DreamSpark) |  |
| Nature Publishing Group | Nature Publishing GroupPalgrave Macmillan | ※ |
| Ovid | OvidSP | ※ |
| ProQuest | RefWorks | ※ |
| ProQuest | ebrary | ※ |
| Royal Society of Chemistry | RSC Publishing | ※ |
| Serials Solutions | 360 Search, 360 Link, Electronic Journal Portal | ※ |
| Springer | SpringerLink | ※ |
| Thomson Reuters | Web of KnowledgeEndNote Web | ※ |
| UNINETT | 予定調整サービス：Foodle |  |
| UQコミュニケーションズ | モバイルWiMAXキャンパスネットワーク接続サービス | ※ |
| アットウェア | しぼすけ |  |
| エルゼビア・ジャパン株式会社 | ナーシング・スキル日本版 | ※ |
| エルゼビア・ジャパン株式会社 | プロシージャーズ・コンサルト日本版 | ※ |
| エルゼビア・ジャパン株式会社 | プロシージャーズ・コンサルト　モバイル | ※ |
| サンメディア | PierOnline | ※ |
| 研究社 | KOD | ※ |
| 佐賀大学 | 無線LANゲスト利用サービス(Opengate) |  |
| 山形大学 | 科学技術の学術情報共有のための双方向コミュニケーションサービス(Communications service for sharing academic information) |  |
| 山形大学 | 大学間連携グループ情報共有サービス（Documents Sharing Service） |  |
| 広島大学 | HINETの無線LANゲスト利用サービス（HINET wlan guest service） |  |
| 金沢大学 | File Transfer Service (ファイル送信サービス) |  |
| 金沢大学 | Kanazawa University Data Repository (金沢大学データリポジトリ) |  |
| 金沢大学 | ARCADE(学術組織間デジタル資料分散共有システム) |  |
| 国立情報学研究所 | CiNii | ※ |
| 国立情報学研究所 | FShare (ファイル共有サービス) |  |
| 国立情報学研究所 | Eduroam-Shib (eduroam用一時アカウント発行サービス) |  |
| 国立情報学研究所 | FaMCUs (テレビ会議多地点接続サービス) |  |
| 国立情報学研究所 | WebELS（オンデマンド学習、多地点遠隔講義、多地点ビデオ会議） |  |
| 国立情報学研究所 | 学認申請システム |  |
| 国立情報学研究所 | NII電子リソースリポジトリ(NII-REO) |  |
| 国立情報学研究所 | edubase Cloud |  |
| 国立情報学研究所 | GakuNin mAP(研究プロジェクト等の仮想グループ作成・管理) |  |
| 国立情報学研究所 | meatwiki(GakuNin mAPグループ用Wiki) |  |
| 国立情報学研究所 | 研究クラウド(Gunnii，tinii，colonii) |  |
| 国立情報学研究所 | 学認連携 Moodle 講習サイト |  |
| 科学技術振興機構 | ReaD&Researchmap |  |

各大学で契約済み、もしくは利用予定のサービスを適宜抽出下さい。

　最新の情報は、こちらを参照下さい。

　https://www.gakunin.jp/participants/

## 学認参加の要件

　学認には、学認実施要領[[3]](#footnote-3) 第5条に該当する機関が参加できる。

|  |
| --- |
| 第５条 学認へ参加できる者の資格は、次の各号の一に該当する機関若しくは機関の部局等とする。一 大学、短期大学、高等専門学校、大学共同利用機関で、IdPまたはSPを構築しようとする機関二 国公立試験研究機関並びに研究又は研究支援を目的とする独立行政法人及び特殊法人で、IdPまたはSPを構築しようとする機関三 前第一号から第二号の機関へ学術サービスを提供することを目的として、SPを構築しようとする機関四 前第一号から第三号の機関が提供する学術サービスを利用することを目的としてIdPを構築しようとする機関で、フェデレーションへの参加が必要であると委員会が特に認めたもの |

　本学は第一項に該当するため、参加の要件を満たしている。IdPについては次項にて記載する。なお、学認参加にかかるNIIへの参加費用や年間費用等は発生しない。

## 大学で用意する必要のあるもの(IdP)

　学認に参加し認証連携を行うために、IdP(Identity Provider)と呼ばれる認証連携用のサーバを構築する必要がある。IdPは、大学の認証基盤と接続し、サービスを利用する際の認証において必要な情報のみをSP(service provider：サービス提供者）に渡すようなフィルタとして機能する。

　例えば、ある電子ジャーナルの利用に必要となる情報がユーザの身分情報および所属機関名だけであれば、IdPはログインが成功したユーザの身分情報のみをLDAP等の認証用サーバから抽出し、機関名と合わせてSPに渡す。SP側は、渡された情報を見て利用の可否を判断しサービスを提供する。

電子ジャーナル等

大学内

ジャーナル

**既存サーバ**

LDAP等

**新規構築サーバ**

IdP

・ログインID

・所属

・身分

・氏名

・e-mail etc.

SP

情報を

送信

必要なデータ

のみを抽出

・学生

・○○大学

・学生

　　＋

・○○大学

図3 IdPの動作例

## 運用体制・委員会について

　IdPの運用・管理は△△センターにて行う。SPの追加等、IdPの運用に関して審議が必要な事項については、担当する部局から△△センターへ連絡のうえ、☆☆委員会にて審議を行う。

　学認参加申請書の発信者（申請者）※要公印：○○　○○（機関の長）

　運用責任者：○○　○○（△△センター長）

　運用担当者：□□　□□（△△センター技術専門職員）

　審議委員会：☆☆委員会

[解説]

　各大学の状況に合わせて適宜修正ください。学認の実施要領やシステム運用基準では、各大学へ委員会の設置を求めてはいませんが、運用を進めるうえで、対応SP増加の審議（特に個人情報の送信が必要な場合）等、大学内のしかるべき組織の承諾を得る事項が発生することがあります。IdP運用のための委員会の設置や、既存の情報委員会等でIdP運用事項を審議できるような体制づくりを検討ください。

　申　請　者：運用フェデレーション参加時の申請書に記載する発信者。学認実施要領 第6条2項により機関の長となる。（例．学長、理事長、等）

　運用責任者：運用フェデレーション参加時に申請書に記載が必要。学認の運用に責任を持つ者。課長職以上もしくは准教授相当以上の者。（例．情報処理センター長、情報担当課長、等）

　運用担当者：IdPの運用に関して実務を担当する者。

　審議委員会：学内にてIdPの運用にかかる事項（例．SPの追加の可否、IdP運用規則の制定、等）を審議する組織。

## IdP構築にかかる費用（業者に構築を依頼した場合）

IdP構築費用（参考）

|  |  |  |  |
| --- | --- | --- | --- |
| 　 | A社 | B社 | C社 |
| IdPサーバ構築作業 | 300,000  | 500,000  | 500,000  |
| uApprove.jp導入作業 | 100,000  | 100,000  | 450,000  |
| SP登録作業（5機関分） | 50,000  | 50,000  | 400,000  |
| テスト作業 | - | - | 500,000  |
| マニュアル | 350,000  | 250,000  | 150,000  |
| 説明会対応、管理等 | 200,000  | - |
| 消費税 | 40,000  | 55,000  | 100,000  |
| 合計 | 840,000  | 1,155,000  | 2,100,000  |

ハードウェア購入費用（参考）

|  |  |  |  |
| --- | --- | --- | --- |
| 　 | A社 | B社 | C社 |
| サーバ本体 | 350,000  | 750,000  | － |
| UPS | 150,000  |
| 消費税 | 17,500  | 45,000  |
| 合計 | 367,500  | 945,000  |

次年度以降保守（参考）

|  |  |  |  |
| --- | --- | --- | --- |
| 　 | A社 | B社 | C社 |
| Shibboleth-IdP(1台構成) 年間保守 | 150,000 | 950,000  | 350,000  |
| uApprove.jpの年間保守 | 150,000  |
| 消費税 | 7,500 | 47,500  | 25,000  |
| 合計 | 157,500 | 997,500  | 525,000  |

[解説]

　A～Cは、以下の仕様で業者に見積もりをした場合の参考コストです。冗長化やLDAPとIdP間の属性情報カスタマイズ等の要素は含んでおりません。各大学の環境により必要なコストは増減しますので、実際の金額については業者に見積もりを依頼して記入ください。

　当然ながら、機関内の既存ハードウェア上に教職員が自ら構築するような場合においては費用は発生しません。

【想定する規模】

　総アカウント数5,000件（学生4,400、教職員600）程度の中規模大学を想定。

　大学内で統一されたLDAPが既に構築済みとする。

【仕様】

　・学認に対応するIdPを構築すること

Shibboleth2.1以上の利用を推奨とし、特段の理由がなければ最新版を仕様すること。その他、学術認証フェデレーション システム運用基準（http://id.nii.ac.jp/1149/00000035/ ）を満たすこと。

　・既存の全学LDAP（1台）と接続し、学認が指定する属性情報のうち、SPが必要としているものを適切に扱えるように設定すること

　・学認に参加する手続きについて必要なサポートを行うこと

　・SP：5機関（大学が契約済み）との接続設定を行うこと。また、内訳にその費用を記載すること

　・uApprove.jpの設定を行うこと。また、内訳にその費用を記載すること

　・納品物として、マニュアル一式（インストール、管理者向け、利用者向け）、システム設計書、利用ソフトのプログラムコピー一式を含むこと

　・管理者向けマニュアルには、新規SP追加時の手順を含むものとし、担当職員に対し、その手順を含む管理者向け説明会を実施すること

　・IdPの冗長化は不要とする

　・必要となるサーバ証明書については、NIIのUPKIオープンドメイン証明書自動発行検証プロジェクトを利用する

## サービス開始までのロードマップ

　学認には、テストフェデレーションと運用フェデレーションの2つの実施環境がある。

　テストフェデレーションは、その名のとおりテスト用の環境で、実際の運用環境に影響を与えないように、構築したIdPの動作確認をすることが可能である。学認には多数の機関が参加しているため、新規加入機関は、まずはテストフェデレーションに参加し、IdPの動作確認が取れた後、本番環境である運用フェデレーションへ参加申請を行う。

サービス開始までのロードマップ

|  |  |  |  |
| --- | --- | --- | --- |
| 年月日 | イベント | 作業内容 | 担当 |
| 平成○年○月 | NII情報処理技術セミナーに参加 | NIIのセミナーに参加しIdP構築の知識を得る。 | △△センター |
| 平成○年○月 | 学認参加の学内了承を得る | ○○委員会にて、学認参加への説明。予算の確保。 | △△センター |
| 平成○年○月 | IdP構築 | IdPを内部構築。（もしくは外部業者に構築を依頼。） | △△センター |
| 平成○年○月 | テストフェデレーション参加 | テストフェデレーションへの参加申請（Web上の学認申請システムより申込み。）IdPの動作確認。 | △△センター |
| 平成○年○月 | 運用フェデレーション参加 | 運用フェデレーションへの参加申請1.学認申請システムより申込み　　　　　↓2.学認事務局にて内容確認　　　　　↓3.申請書をﾀﾞｳﾝﾛｰﾄﾞし公印処理　　　　　↓4.申請文書を学認事務局へ郵送　　　　　↓5.学認事務局より承認の連絡サービスプロバイダへ学認での接続希望を連絡。 | △△センター附属図書館 |
| 平成○年○月 | サービス開始 | Webサイトでの告知等、学内広報を実施。 | △△センター附属図書館 |

[解説]

　サービス開始までのロードマップの一例です。担当部署や学内了承を得るための委員会等は、各大学に合わせて修正ください。

## 個人情報の扱い

　ユーザが学認を使ってサービスを利用する場合、属性情報がサービスの提供者（SP）に送信される。必要となる属性情報はSPにより異なるが、中には個人情報が含まれる場合があり、個人情報の第三者への提供は、あらかじめ利用者の承諾を得ておく必要がある。

　学認ではuApprove.jpという仕組みを用意して承諾を得ることができるようにしており、本学でもこの機能を導入し、送信が任意となっている属性を送信するかどうかを利用者が決めることができるようにする。

SPに送信される可能性のある属性情報

（学認技術運用基準 Ver2.0 http://id.nii.ac.jp/1149/00000212/）

|  |  |  |
| --- | --- | --- |
| 属性 | 内容 | 個人情報 |
| organizationName (o) | 組織名（英字） | × |
| jaOrganizationName (jao) | 組織名（日本語） | × |
| organizationalUnitName (ou) | 組織内所属名称（英字） | × |
| jaOrganizationalUnitName (jaou) | 組織内所属名称（日本語） | × |
| eduPersonPrincipalName (eppn) | フェデレーション内の一意なID例：t-ninsyo2009@b-univ.ac.jp | ○ |
| eduPersonTargetedID | フェデレーション内及びSP毎に一意なID例： https://idp.sample.ac.jp/idp/Shibboleth!https://sp.sample.ac.jp/Shibboleth-sp!+Lxxl7QLnCkaKguy5xjNLRBkdDc= | △ |
| eduPersonAffiliation | 職種 | × |
| eduPersonScopedAffiliation | 組織内の職種（@scopeつき） | × |
| eduPersonEntitlement | 特定アプリ利用の資格 | × |
| surname (sn) | 氏名（姓）（英字） | ○ |
| jaSurname (jasn) | 氏名（姓）（日本語） | ○ |
| givenName | 氏名（名）（英字） | ○ |
| jaGivenName | 氏名（名）（日本語） | ○ |
| displayName | 氏名（表示名）（英字） | ○ |
| jaDisplayName | 氏名（表示名）（日本語） | ○ |
| mail | メールアドレス | ○ |
| gakuninScopedPersonalUniqueCode | 学生・職員番号 （@scopeつき） | ○ |
| isMemberOf | 所属するグループ名 | × |

○は個人情報になる可能性があるもの、△は独法個人情報保護法上では個人情報となる可能性があるもの

[解説]

　uApprove.jpにより、送信する属性の利用者承諾を得ることができますが、利用の前に以下の点について留意する必要があります。各大学の事情に合わせて導入を検討下さい。

・各大学・研究機関の個人情報保護ポリシーとの整合性

・学認による個人情報の提供を容認するかどうかのポリシー決め

・uApprove.jpの仕組みの利用者への周知

・SPの個人情報保護ポリシーの確認

## 参考：SAML、Shibboleth、LoA

　学認では、異なる機関が認証連携するために、SAML（Security Assertion Markup Language）[[4]](#footnote-4)と呼ばれる、インターネット上でID/パスワードを交換するための標準仕様を利用している。学認に接続するサーバの構築には、SAMLを用いたShibboleth（シボレス）と呼ばれるソフトウェアを利用することが推奨される。

　Shibbolethは、米国のInternet2（多くの大学や企業が参加する次世代インターネットの研究プロジェクト）にて、2000年にプロジェクトとして始まり、2003年にバージョン1.0がリリースされた。その後、SAMLのバージョンが2.0となり、Shibbolethも2008年にバージョン2.0をリリースしている。

　欧米では、米国のInCommon[[5]](#footnote-5)や、欧州のUK Federation[[6]](#footnote-6)、SWITCHaai[[7]](#footnote-7)など、Shibbolethを用いたフェデレーションが広がっており、様々なサービスが対応している。

　認証連携においては、提供されるサービスを権利のないユーザが利用しないよう、大学側（IdP）が送信するユーザ情報の信頼性が求められる。信頼性評価の世界標準として、Level of Assurance(以下、LoA)が標準化されてきており、学認では、米国OIX(Open Identity Exchange)が提供するLoA1の認定サービスを、学認参加機関を対象として実施しているこの認定を受けた大学は、米国連邦政府機関 NIH（国立衛生研究所）が提供する PubMed等のサービスへのアクセスが可能となる。

|  |  |
| --- | --- |
| Level | Description |
| 1-Low | 身元確認不要、匿名 |
| 2-Medium | 身元識別（身分証明書）、単一要素認証可、失効処理 |
| 3-High | 多要素認証 |
| 4-Very high | 対面による発行、ハードウェアトークン |

1. http://Shibboleth.net/ [↑](#footnote-ref-1)
2. http://www.eduroam.jp/ [↑](#footnote-ref-2)
3. http://id.nii.ac.jp/1149/00000210/ [↑](#footnote-ref-3)
4. https://www.oasis-open.org/committees/tc\_home.php?wg\_abbrev=security [↑](#footnote-ref-4)
5. https://incommon.org/ [↑](#footnote-ref-5)
6. http://www.ukfederation.org.uk/ [↑](#footnote-ref-6)
7. http://www.switch.ch/aai/ [↑](#footnote-ref-7)