

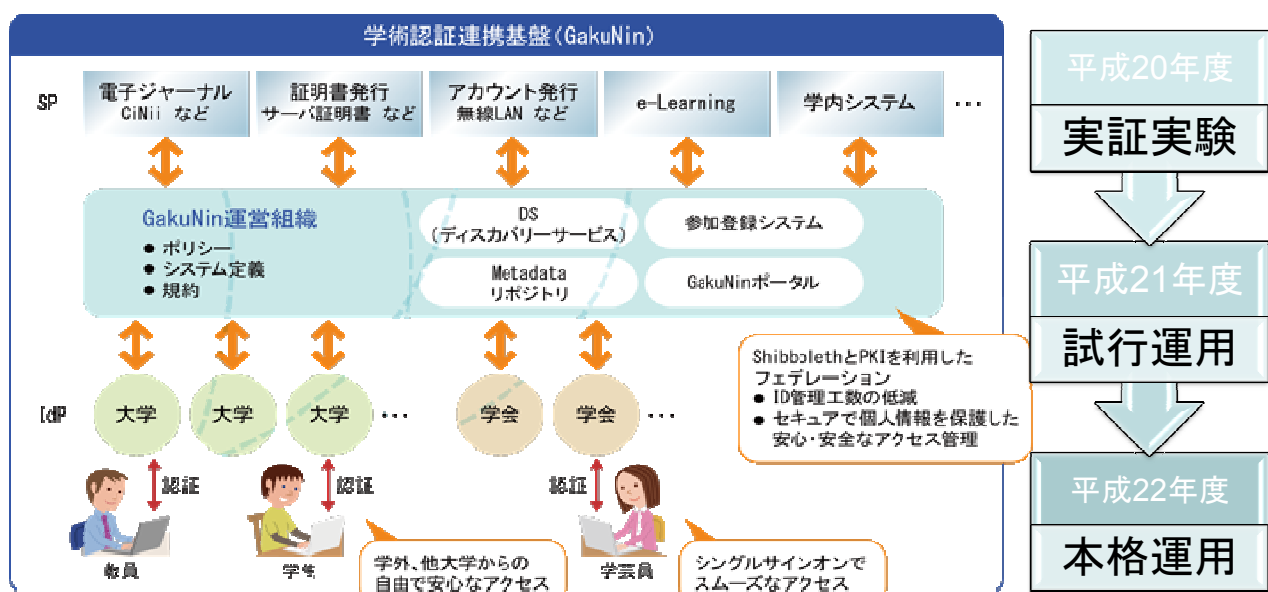
初心者でも分かる学術認証システム -さらに広がる「学認」の輪-

国立情報学研究所 学認タスクフォース

gakunin-office@nii.ac.jp

学認とは

日本における公式Shibbolethフェデレーション

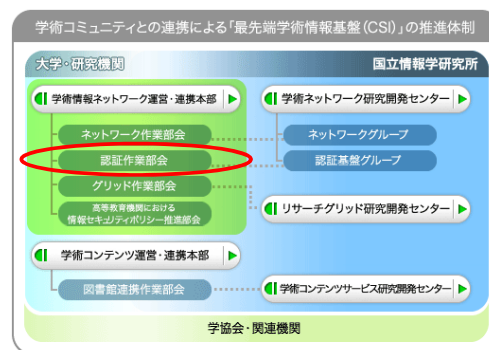


参加者:
利用機関(大学等)
提供機関(コンテンツベンダ等)

企画・運営:
NII学術情報ネットワーク運営・連携本部>認証作業部会>学認タスクフォース
事務局:NII学術基盤推進部

運用ルール:
実施要領(参加資格等)
運用基準(データ,システム定義)

- H22年度より本格運用開始
- 愛称「学認」、ロゴの決定
- タスクフォース(TF)設置
 - システム運用基準の策定と公開(V1.1)
 - DSの運用、改良
 - メタデータ管理
 - 各種有効期間の検討
 - 参加ルールの整理
 - 海外との連携
 - ケーススタディの提供
 - 病院等の参加に関する検討



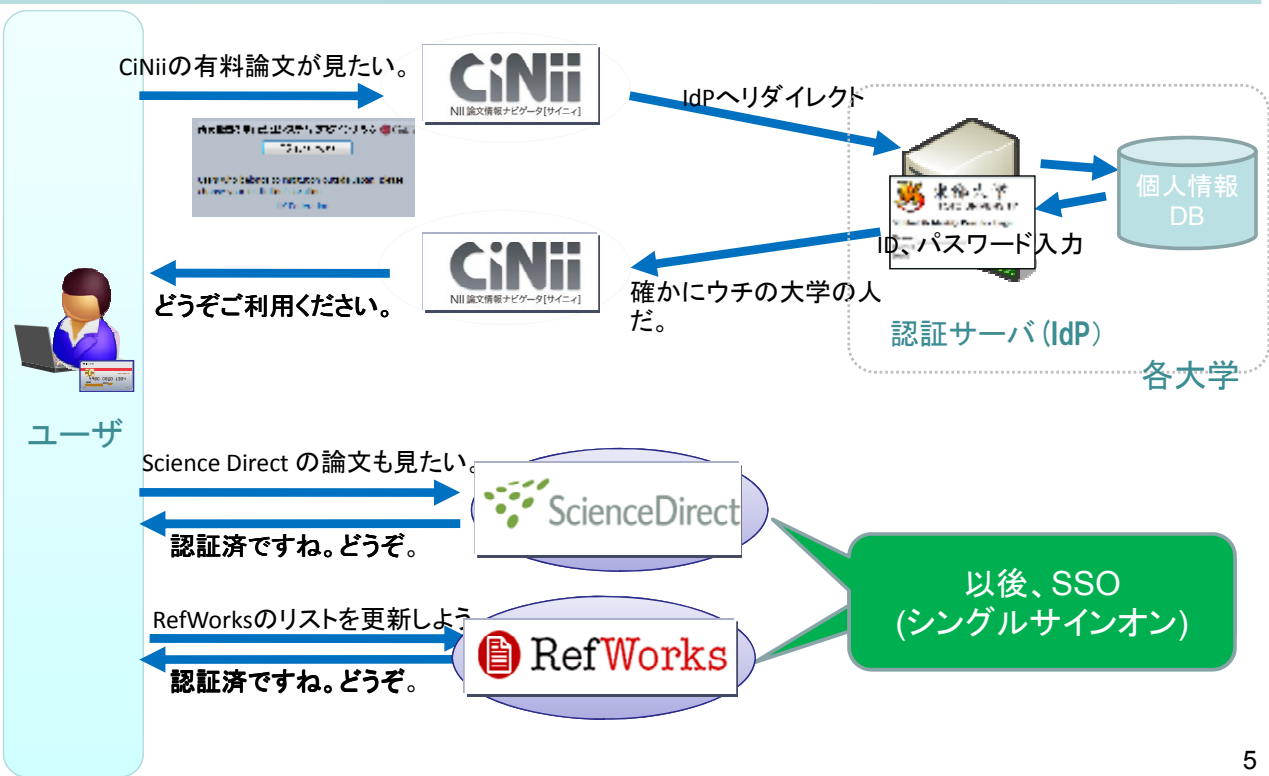
- ▶ 実証実験・試行運用(UPKI-Fed)
 - ▶ 認証作業部会による方針決定
 - ▶ 北大、東北大、東大、名大、京大、阪大、九大、東工大、高エネ研、NII
- ▶ 本格運用(GakuNin)
 - ▶ 認証作業部会下にTFを設置し、権限を委譲
 - ▶ 参加機関の情報基盤センター、図書館などからの、より広い実地メンバーで構成
 - ▶ 各種学術コンテンツとの連携は学認ライブラリチームが主導

TFによりフェデレーションの進め方を検討

IdP = 51 機関	
運用中	
北海道大 旭川医科大 山形大 千葉大 筑波大 東京大 東京農工大 名古屋大 信州大 金沢大 三重大 京都大 神戸大 岡山大	広島大 山口大 九州工業大 九州大 佐賀大 国立情報学研究所 日本大 明治大 東邦大 立教大 成城大 京都産業大 国立 20機関 私立 6機関 計26機関
参加準備中	
参加検討中 約30機関	国立 15機関 公立 2機関 私立 3機関 計25機関
大学以外の参加も可能に	

SP = 21種類	
運用中	
360 (4)services (Serials Solutions) Cambridge Journals Online(CUP) DreamSpark (Microsoft) Ebrary(ProQuest) EBSCO host(EBSCO) OvidSP (Ovid) Pathology Images (Atlases) RefWorks (ProQuest) Science Direct (Elsevier) SCOPUS (Elsevier) SpringerLink (Springer) Web of Knowledge (Thomson Reuters) KOD:研究社オンラインディクショナリー(研究社) CiNii (NII) ファイル送信サービス(金沢大) IMCデータリポジトリ(金沢大) 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(山形大) HINET wlan guest service (学内無線LANゲスト接続) (広島大) FaMCUs (テレビ会議多地点接続サービス) (NII) Eduroam-Shib (eduroam用アカウント発行サービス) (京大&NII) Fshare(大容量ファイル交換サービス) (NII) WebELS(Web-based e-Learning System) (NII)	参加に向けて調整中 9社 Karger, JSTOR Taylor&Francis, IEEE, IOP, PubMed, PierOnline, Emerald, HighWire
コンテンツサービス 13種類	
ウェブ上の各種ユーティリティ 8種類	

利用機関と提供機関によるn:nの相互信頼によって実現



5

論文を探して

読んで

管理する



- ・ リモートアクセスによる利用頻度の向上
- ・ SSOによるユーザビリティ向上 etc.

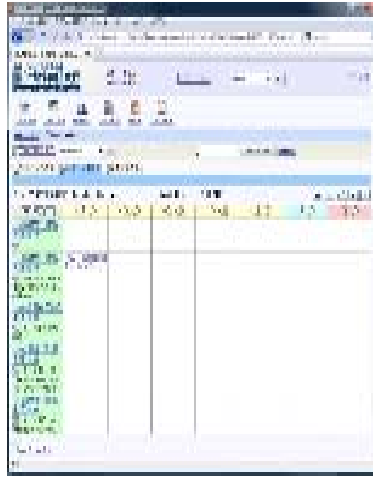


6

Webメール



グループウェア



図書館システム



- Shibboleth認証はeリソース以外にも適用可能。



いつでもどこでも、簡単・セキュアに個人認証され、
ウェブリソースが利用しやすくなる

- ✓記憶するIDは1種類 (統合認証)
- ✓情報入力は1回だけ (SSO)
- ✓学内外、国内外、OK (リモートアクセス)
- ✓ Webブラウザだけ (別ソフト不要)

- 大学等の機関にとって [ID管理側(IdP)]
 - 組織全体の情報セキュリティ方針等への一元的対応が実現。
 - 組織全体のID管理, ユーザサポート業務等の集約化によるコスト削減。
 - ID/パスワード送信時におけるセキュリティ水準の向上。
 - 組織全体へのウェブサービス提供環境の向上。
- ベンダー等にとって [サービス提供者(SP)]
 - サービスのビジビリティ向上
 - 素早いスタートアップ
 - ID管理やユーザサポートの軽減
 - ライセンスにそった適正な利用の促進
- エンドユーザにとって
 - 多数のID/パスワード管理からの解放
 - IPアドレスに依存しないアクセス(自宅や出張先からもアクセス)
 - 個人情報の送信制御, 匿名アクセス(所属機関として認証)
 - SSOによる利便性向上, マッシュアップによるサービス連携

舞台裏では、

1. 技術的基盤 : Shibboleth(シボレス)、
2. システム基盤: 各大学やベンダが構築するIdP・SP、
3. 運用基盤 : 各機関で構成するフェデレーション、

という3つの基盤が機能しています。



- 標準プロトコル(SAML)によって属性情報をやり取りするためのソフトウェア。
- オープンソース(無償)である。
- 米国(Internet2)にて2000年にプロジェクト発足。
 - <http://shibboleth.internet2.edu/>
- 最新はShibboleth V2.3
- 欧米でフェデレーションを通じて実運用拡大。
とりわけ学術系の利用が軸となっている。

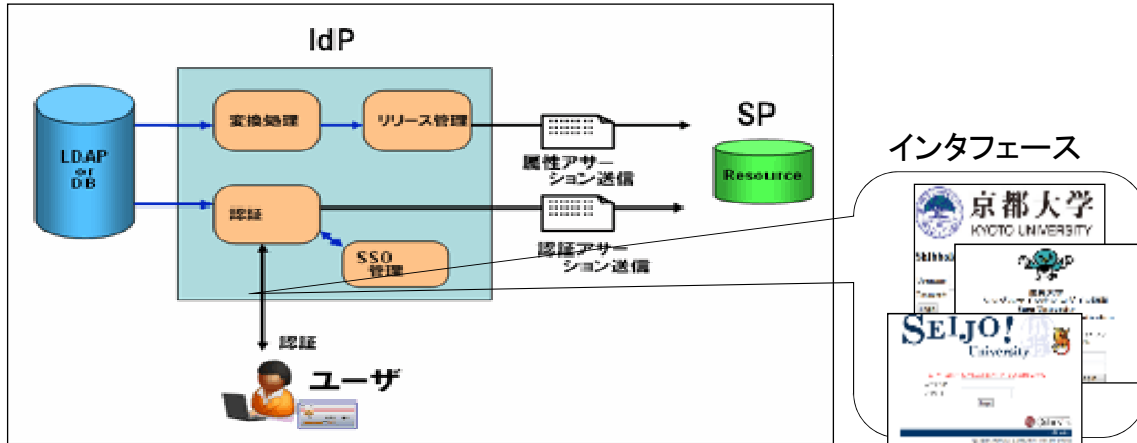
コトバの由来:

ギレアデ人が、逃亡する敵(エフライム人)を識別するため渡し場でshibboleth(ヘブライ語で小川の意)と発音させた。

エフライム人は shが発音できず sibboleth となっ
てしまい、敵だとわかって殺された。旧約聖書(士師記)より。

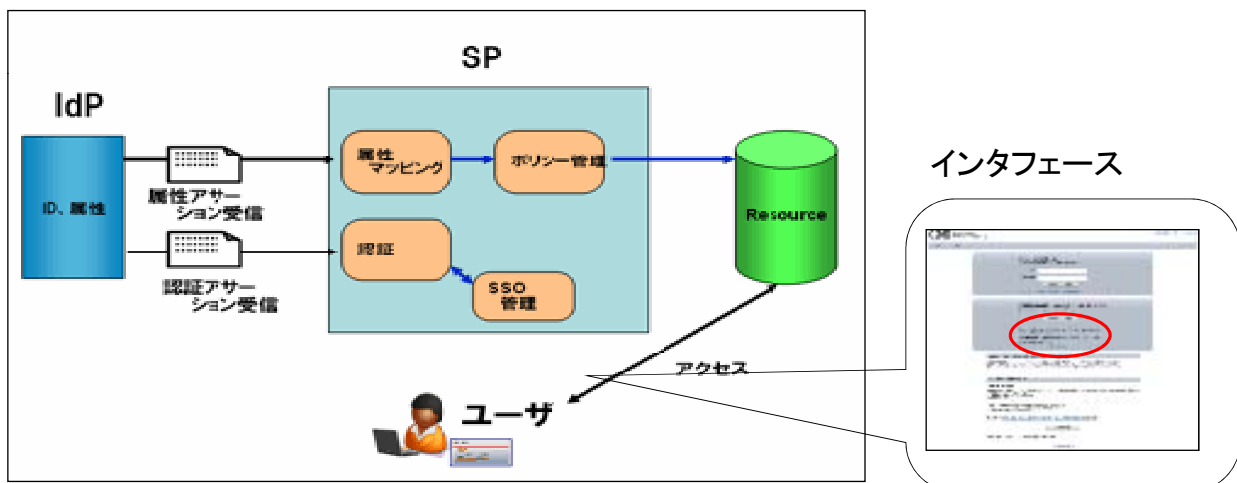
転じて、Shibbolethは英語で合言葉、符丁(仲間内だけに通じる言葉)を指す。

- 大学等が構築する
- IdP自身は属性情報等を保持しない。
- 属性情報はマスターDBである認証基盤(LDAPやActive Directory等)が持っている。
- IdPは認証基盤から特定のデータのみを抽出してSPに提供する。単なるフィルタと言える。



仕組み

- サービスを提供するWebサーバのこと
- “Institutional Login”等のボタンがあればShibbolethで利用可能なSPである
- 電子ジャーナルに限らず、いろいろなサービスをShibboleth化することが可能(例:無線LAN認証, グループウェア等)



仕組み

フェデレーションポリシーで計16種類を使用可能と定めています。

学認の属性情報 一覧

属性	内容
OrganizationName (o)	組織名
jaOrganizationName (jao)	組織名(日本語)
OrganizationalUnit (ou)	組織内所属名称
jaOrganizationalUnit (jaou)	組織内所属名称(日本語)
eduPersonPrincipalName (eppn)	フェデレーション内の共通識別子
eduPersonTargetedID	フェデレーション内の匿名識別子
eduPersonAffiliation	職種
eduPersonScopedAffiliation	職種(スコープ付き)
eduPersonEntitlement	資格
SurName (sn)	氏名(姓)
jaSurName (jasn)	氏名(姓)(日本語)
GivenName	氏名(名)
jaGivenName	氏名(名)(日本語)
displayName	氏名(表示名)
jaDisplayName	氏名(表示名)(日本語)
mail	メールアドレス

実際に使われる属性情報の例

サービスA (1項目必須)

eppn(必須), eduPersonTargetedID

サービスB (1項目必須)

eduPersonScopedAffiliation のみ

サービスC (1項目必須)

eduPersonEntitlement
eduPersonScopedAffiliation
(どちらか必須)

その他全サービスについてはこちら

<http://www.gakunin.jp/docs/fed/technical/connect/sp>

(参考) <https://www.gakunin.jp/docs/fed/technical/attribute>

15

- Shibboleth認証を運用する国/地域単位に設置。
- 当該地域でShibboleth認証を利用する大学、ベンダは参加が必須。
- 規程(交換するデータ形式・内容、プライバシー 等)を作り、メンバー全員が順守する。
- DS(IdP-SPを繋ぐ道しるべサービス)を管理
- 日本のフェデレーションは

「学認(GakuNin)」です。

16

INTERNET2

NATIONAL IDENTITY MANAGEMENT FEDERATIONS


http://www.internet2.edu/pubs/national_federations.pdf

17

- スイスSWITCHhai: 382
- イギリスUK-FAM: 190
- アメリカInCommon: 150以上
- ドイツDFN-AAI: 60
- フィンランドHaka: 65
- フランスFédération Éducation-Recherche : 54
- ノルウェーFEIDE: 50以上

日本国内のサービスの展開がポイント

Step1

- ・ Eリソースの利用契約(当たり前ですが大前提)
- ・ IdPの立上げ
- ・ 学認参加申込み(テストフェデレーション)。接続テストの実施。
- ・ 学認参加申込み(運用フェデレーション)

Step2

- ・ 学認利用することをベンダに申請
- ・ 申請内容, 方式は各社ほぼ共通

Step3

- ・ 学内周知
- ・ 利用開始

19

- ・ NIIによる技術サポート
 - － インストールガイド
 - － 情報交換(メーリングリスト等)
 - － 「Shibboleth環境の構築」講習会

情報処理技術セミナー「Shibboleth環境の構築」(第2回)	2011/08/04-05	国立情報学研究所	募集中
情報処理技術セミナー「Shibboleth環境の構築」(第3回)	2011/11/01-02	国立情報学研究所	募集中

大学向けの技術セミナーを定期的 to開催。
<https://www.gakunin.jp/docs/fed/event>



20

学認webサイトの「参加」ページ参照

<https://www.gakunin.jp/docs/fed/join>

新規IdP申請

申請書ID	入力完了後に確定します		
EntityID	example.ac.jp/ldap/shibboleth		
機関名	(日)	フェデレーション大学	
	(英)	The University of Federation	
機関単位名	(日)		
	(英)		
運用開始日	2010-10-01		
運用責任者:			
名前	(日)	姓 連携	名 次郎
	(英)	姓 RENKEI	名 Jiro
	(ヨミ)	姓 レンケイ	名 ジロウ
部署	情報センター		
職位	事務課長		
メールアドレス	renkei@example.ac.jp		

「学認申請システム」を通じて申込む。

京都大学

KYOTO UNIVERSITY

Shibboleth Identity Provider Login

Username:

Password:

[Login](#)

NII UPKI Federation

-NII IdP Login-

→ <http://shibboleth.metapress.com/>

Username:

Password:

[Login](#)

千葉大学

千葉大学電子的情報資源統合認証サードス

このサードスには、総合メディア基盤センターの利用IDとパスワードの両方でログインできます。
 固有の利用IDとパスワードを、以下のURLから取得してください。

URL: [http://www.chiba-u.ac.jp/~lib/](#)

お問い合わせは、附属図書館・本館サービスグループまで。
 利用者IDの照会先は、総合メディア基盤センターまでどうぞ。

Chiba University Library / Chiba University Institute of Media and Information Technology.

Shibboleth

Kanazawa University

Shibboleth Identity Provider Login

NetworkID:

Password:

[Login](#)

名古屋大学

名古屋大学ID (Nagoya University ID)

パスワード (Password)

[Login](#)

・ ShibbolethによるID照会システムを利用し、
 ・ 個人IDとパスワードを照会します。URL: <http://www.nagoya-u.ac.jp/~lib/>
 ・ 詳細は、本館サービスグループまで。URL: <http://www3serv.iz.nagoya-u.ac.jp/>

佐賀大学

シングルサインオン ログイン認証

Single Sign-On Login Authentication

ユーザーIDとパスワードを入力してください
 Please input User ID, Password.

ユーザーID:

パスワード:

[ログイン Login](#)

Step1

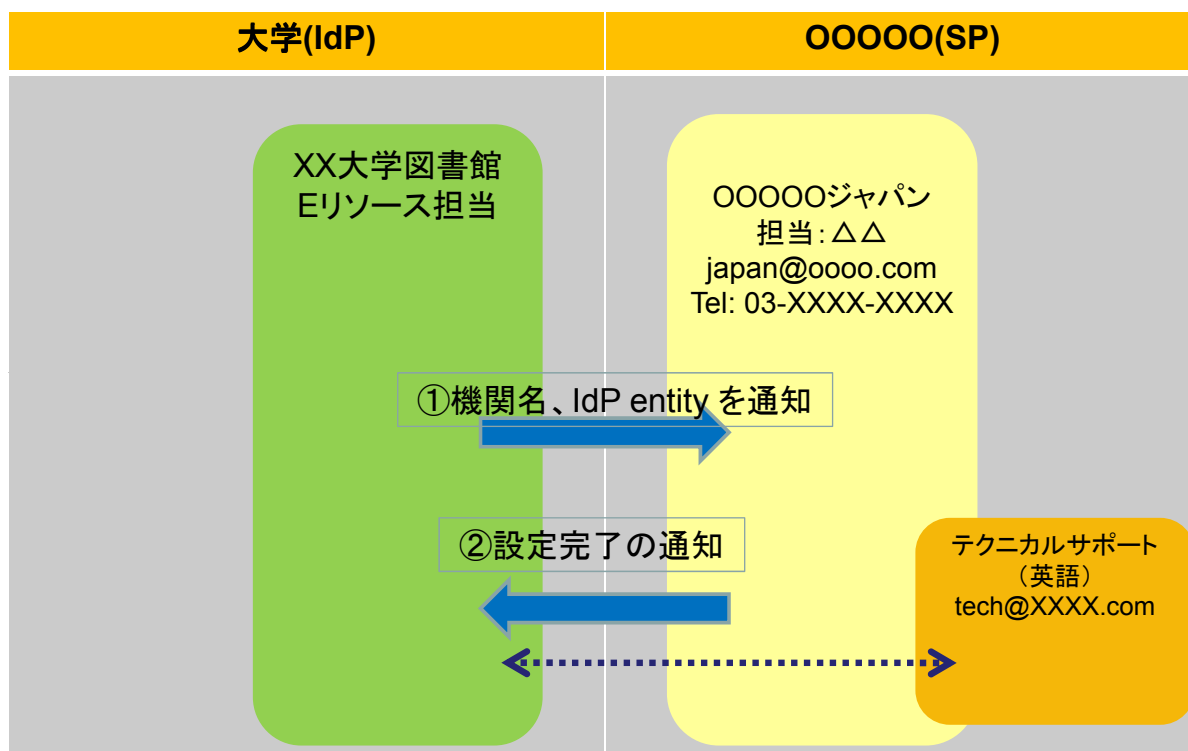
- Eリソースの利用契約(当たり前ですが大前提)
- IdPの立上げ
- IdP設置申込み(テストフェデレーション) → 認証テストの実施。
- IdP設置申込み(運用フェデレーション)

Step2

- 学認利用することをベンダに申請
- 申請内容, 方式は各社ほぼ共通

Step3

- 学内周知
- 利用開始



Step1

- Eリソースの利用契約(当たり前ですが大前提)
- IdPの立上げ
- 学認参加申込み(テストフェデレーション)。接続テストの実施。
- 学認参加申込み(運用フェデレーション)

Step2

- 学認利用することをベンダに申請
- 申請内容, 方式は各社ほぼ共通

Step3

- 学内周知
- 利用開始

全学 学外からの電子ジャーナル利用が便利になりました

投稿日時: 20

学外からの電子ジャーナル利用が、今までよりも便利になりました。

千葉大学で契約している電子ジャーナルや論文情報データベース等が、大学外からも総合メディア基盤センター発行のント(統合メールシステムの"利用者番号"と"パスワード")でログインして利用できます。

2010年3月現在、このシステムを利用できるサービスは以下のとおりです。

Cinii	NII論文情報ナビゲータ
Scopus	Elsevier社 書誌・引用文献データベース
ScienceDirect	Elsevier社 電子ジャーナル
SpringerLink	Springer社 電子ジャーナル
Cambridge Journals Online	Cambridge Univ. Press 電子ジャーナル
RefWorks	ProQuest社 文献管理ソフトウェア

各サービスの「Institution login」「Shibboleth login」等からログインしてご利用下さい。
各サービスの詳しい利用方法は、[こちらのページ](#)をご覧ください。

必読！ 千葉大学の事例紹介(同大附属図書館 野田英明氏)

「図書館目線でShibboleth認証」 https://upki-portal.nii.ac.jp/docs/files/8_野田.pdf

「Shibbolethを用いた連携認証による電子リソース利用」(図書館雑誌2010.6)

Shibboleth 認証サービスがスタート 学外からの電子リソースの使い方

東邦大学で契約している電子リソース(電子ジャーナル・電子ブック・データベース・文献管理ソフト)などの一部が、ご自宅や出向先など学内LANに接続されていないパソコンからも利用できるようになりました。

利用はwebmailのログインID・パスワードで

利用にはネットワークセンター発行のアカウント(WebmailのログインID/パスワード)が必要です。

●ご利用できる方:東邦大学に所属している学生および教職員
【パスワードを忘れたら】ネットワークセンターまでお問い合わせください。
【ログインできない/WebMailのログインID・パスワードをお持ちでない教職員の方は】
5月11/10 10:30~ 学認フォーラムにて紹介予定!



学外からも
利用可能!

11/10 10:30~
学認フォーラムにて
紹介予定!

<https://www.gakunin.jp/>

参加一覧
各ベンダ毎の設定情報 等

参加方法の説明
学認申請システム 等

IdP,SP 構築の説明
属性情報、メタデータの詳細 等

シンポジウムや講習会の案内 等

各大学の活用事例集
英国Federation関連和訳資料 等

情報交換メーリングリスト
過去ログも公開



学認/Shibbolethに
関するポータルサイト

UKフェデレーション紹介映像(和訳付き)

<https://www.gakunin.jp/docs/fed/info>



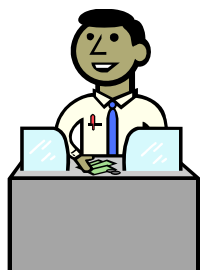
必見！

29

どんな事でもお気軽に

- 参加に関する質問。
- 学内説明等の個別のご相談。
- ご意見、ご感想、ご提案。

etc.



連絡先

国立情報学研究所(学認担当)

gakunin-office@nii.ac.jp