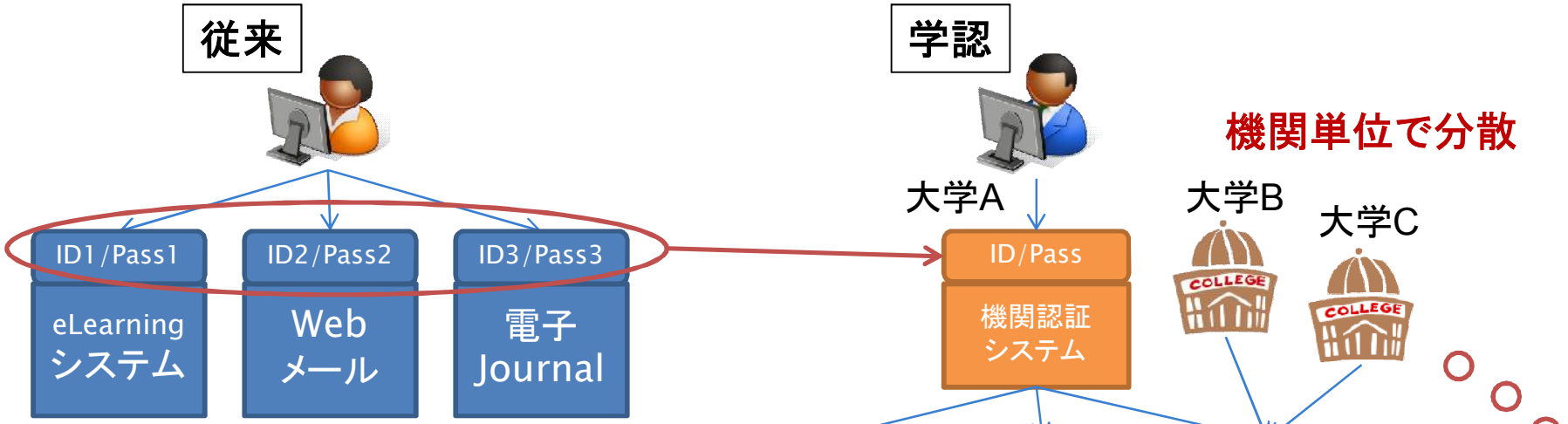

# 学術認証フェデレーションの概要

国立情報学研究所 中村素典

# 学術認証フェデレーション「学認」とは

- Webアプリケーションへのシングル・サイン・オン（SSO）技術を、組織を越えて活用する分散型認証基盤




- Webアプリ毎にIDを管理
  > ID管理コスト大
- Webアプリ毎にログイン作業
  > ユーザのセキュリティ意識低下
- セキュリティレベルの不統一
  > 低セキュリティサイトアクセス時の漏えいリスク

# 学認で主に利用されているミドルウエア

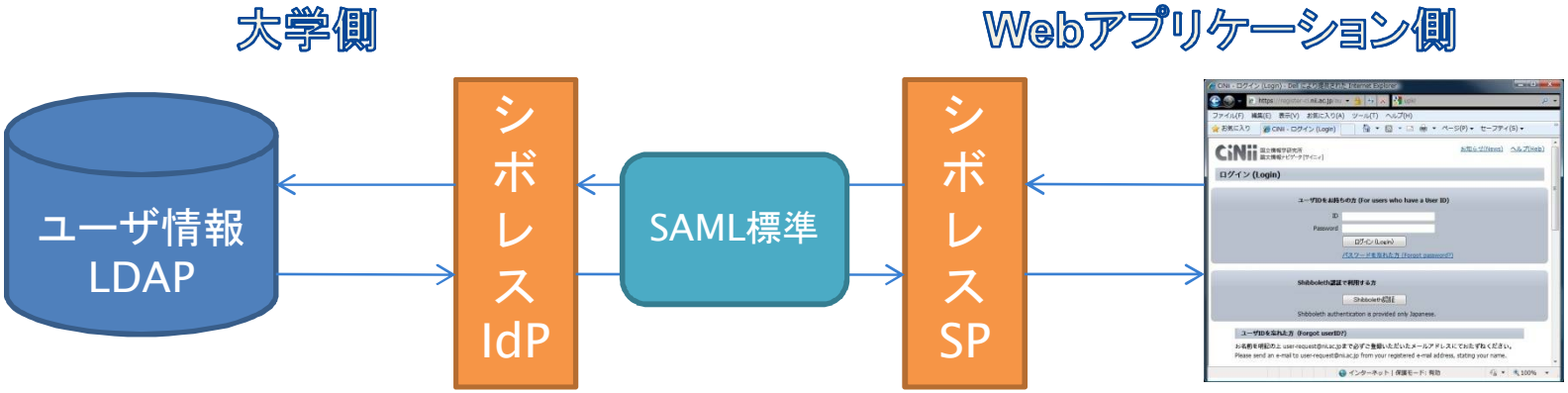
## SAML（サムル：Security Assertion Markup Language）

- セキュリティや個人情報保護法に配慮して，認証・認可の情報交換を行うためのデータ形式
- 標準団体OASISにより策定

## Shibboleth（シボレス）

ShibbolethはSAMLを実現するミドルウエア

- 米国EDUCAUSE／Internet2にて2000年に発足したオープンソースプロジェクト
  - http://shibboleth.internet2.edu/
- SAMLによる認証連携方法として学術界ではデファクトスタンダード
  - 米国、欧州でShibbolethによる学術認証フェデレーションが拡大
- 最新はVersion 2.2
  - 一部、古いSPはまだVersion 1.3を使用（徐々に、2.xへ移行中）

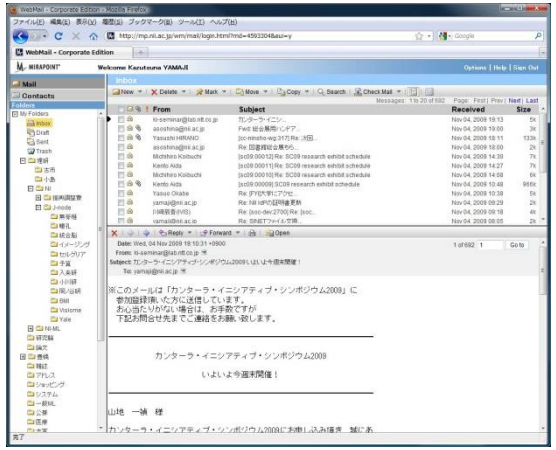



SAML通信のためのフィルターのようなもの

# 具体的な利用例（学内SSOの整備）

- フェデレーション自体は学外リソース利用のためのもの
- フェデレーションへの参加により
  - 学内の統合認証システム構築を加速化
  - 学内システムのSSO化を加速化
- シボレス化による学内の公開Webサービスの
  セキュリティレベルの向上

Webメール



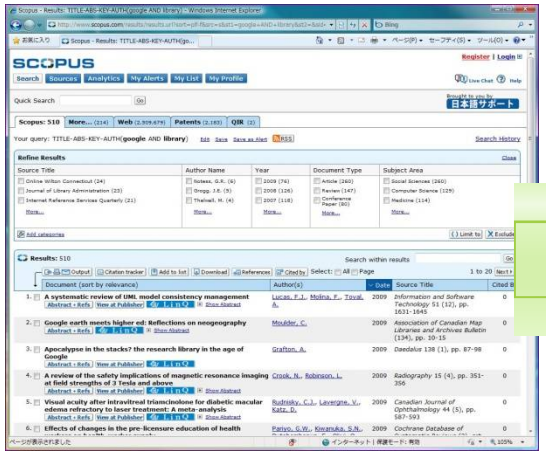
グループウエア

図書館システム

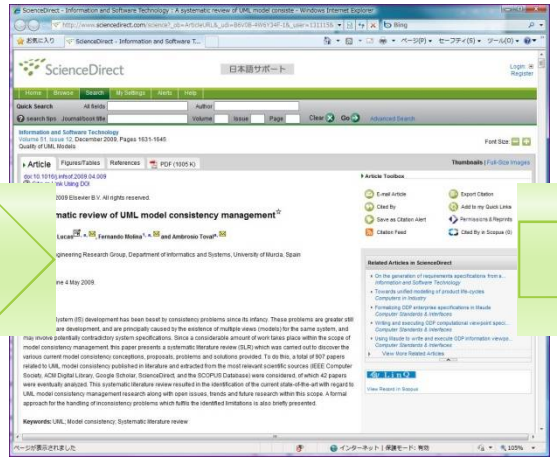
# 具体的な利用例（電子ジャーナル）

- リモートアクセスによる利用頻度の向上
- SSOによるユーザエクスペリエンスの向上

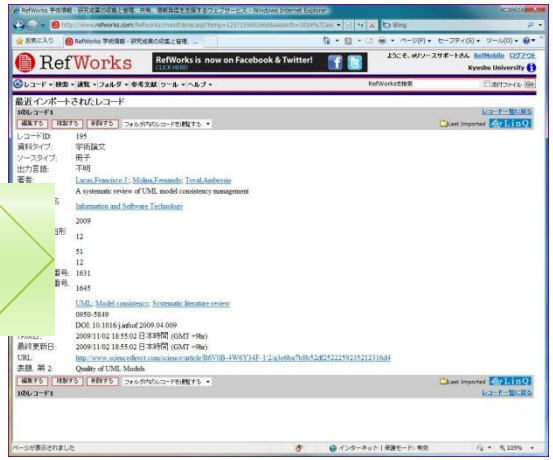
論文を探して




論文を取得して（読んで）



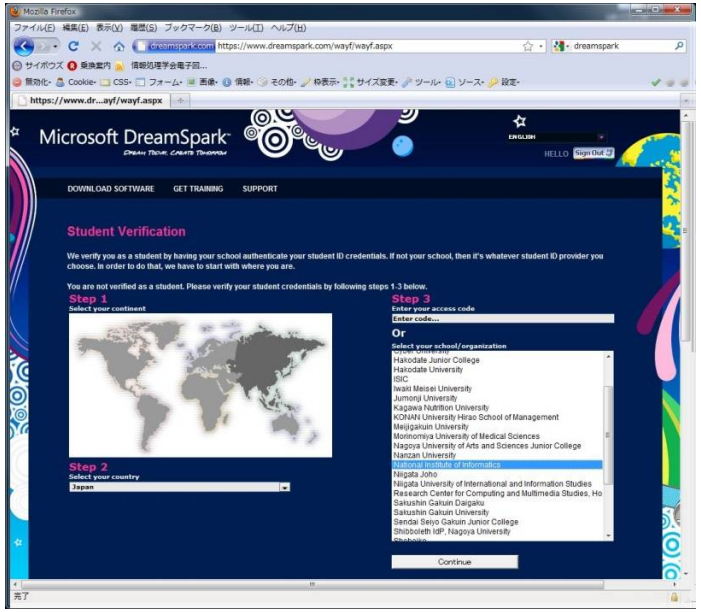

論文を管理する



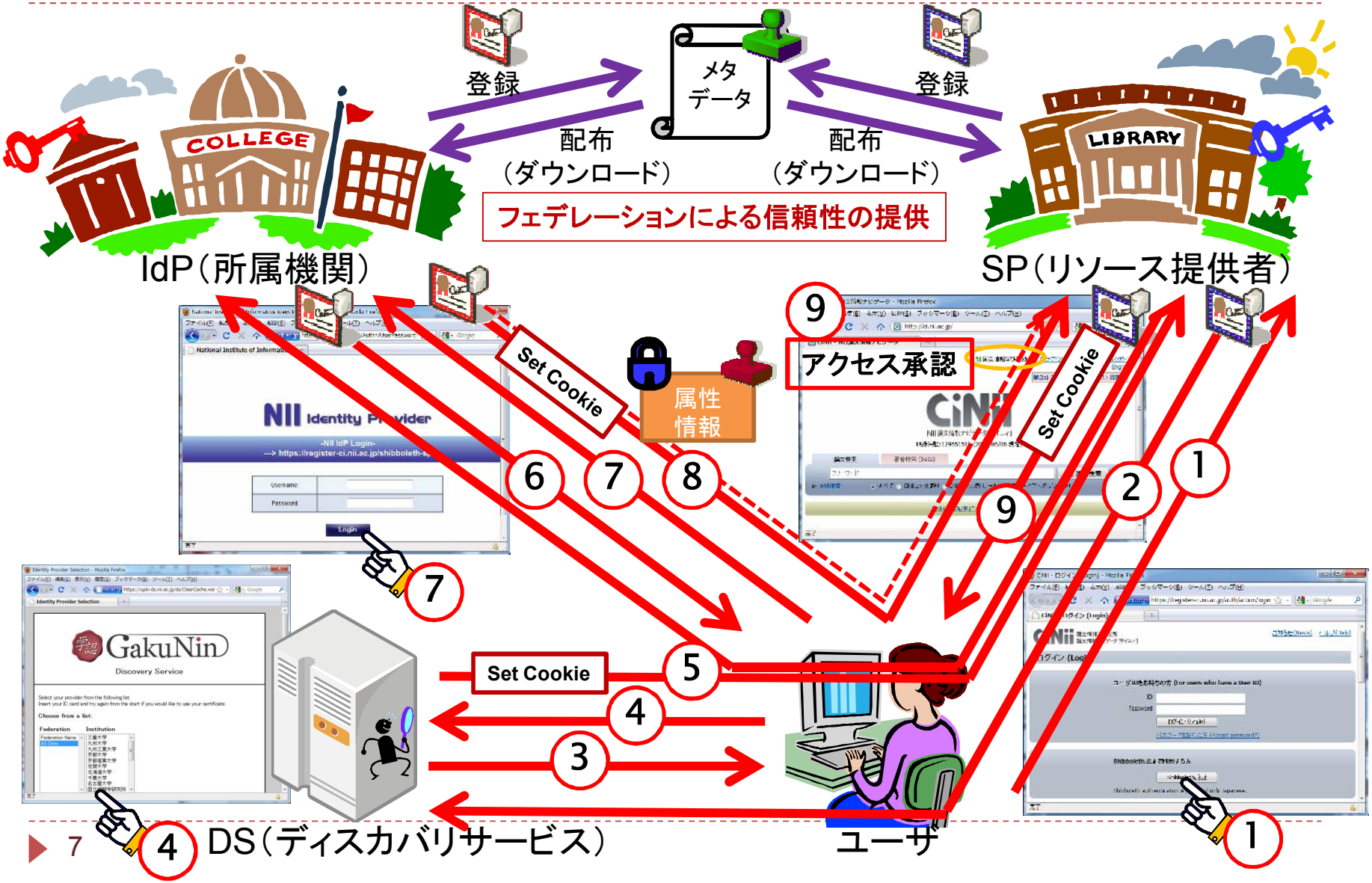

**認証連携によるディープなマッシュアップ**

# 具体的な利用例（アカデミック配付）

- Microsoft DreamSpark
  - 学生を対象にMSのソフトウエア開発環境を無償で提供するプログラム
- 属性により大学構成員であり学生であることを確認
  - eduPersonTargetedID（SP毎に異なるハッシュ化された一意のID）
  - eduPersonScopedAffiliation（例：student@nii.ac.jp）
- 運用フェデレーション参加24時間後に利用可能



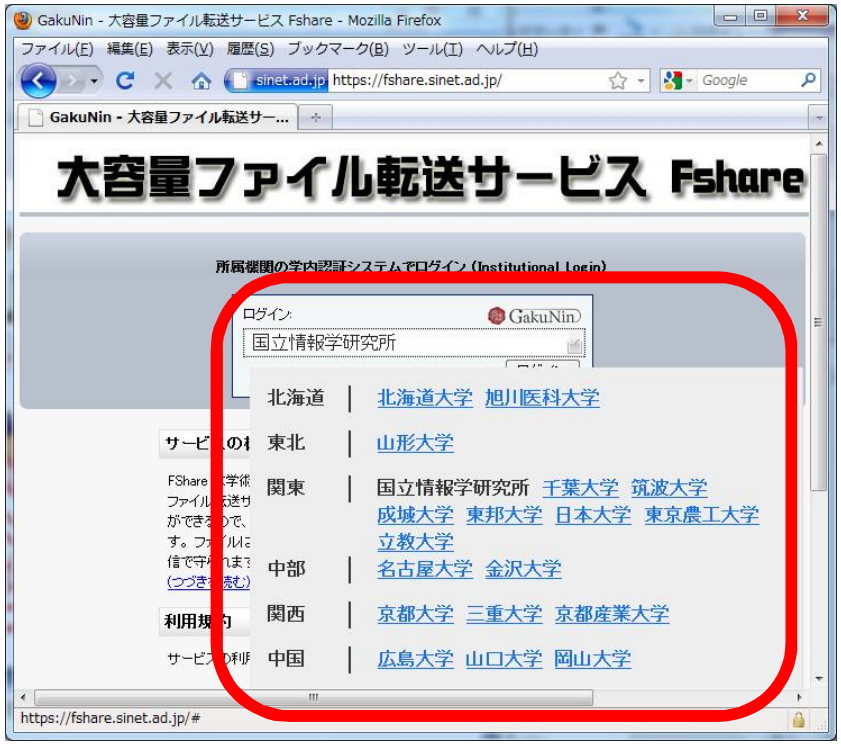

# Shibbolethの動作の仕組み



# ディスカバリサービス(DS)の改良

- SPへのアクセス後、「一旦画面が切り替わってIdP選択、さらに画面が切り替わって、ID/PWの入力」という画面遷移は煩雑
- SP埋め込みDSの採用を検討

  課題：
  - 機関一覧の表示方法
  - 検索の方法
  - 選択結果のSP間での安全な共有



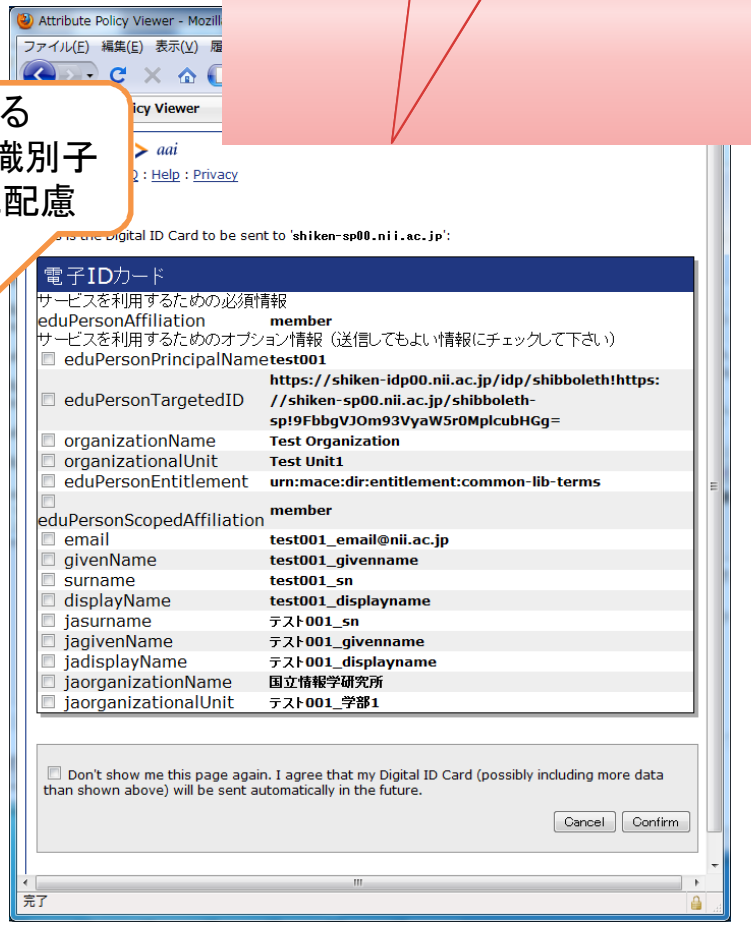
# 学認で扱う属性情報

## 16種類の属性情報を用いてSPが認可判断（機関、ロールベー

| 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(faculty, staff, student, member) |
| eduPersonScopedAffiliation | 職種（@ドメイン名がついた形式） |
| 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 |

SPごとに異なる
ハッシュ化された識別子
個人情報開示に配慮

uApprove.jp
プラグイン

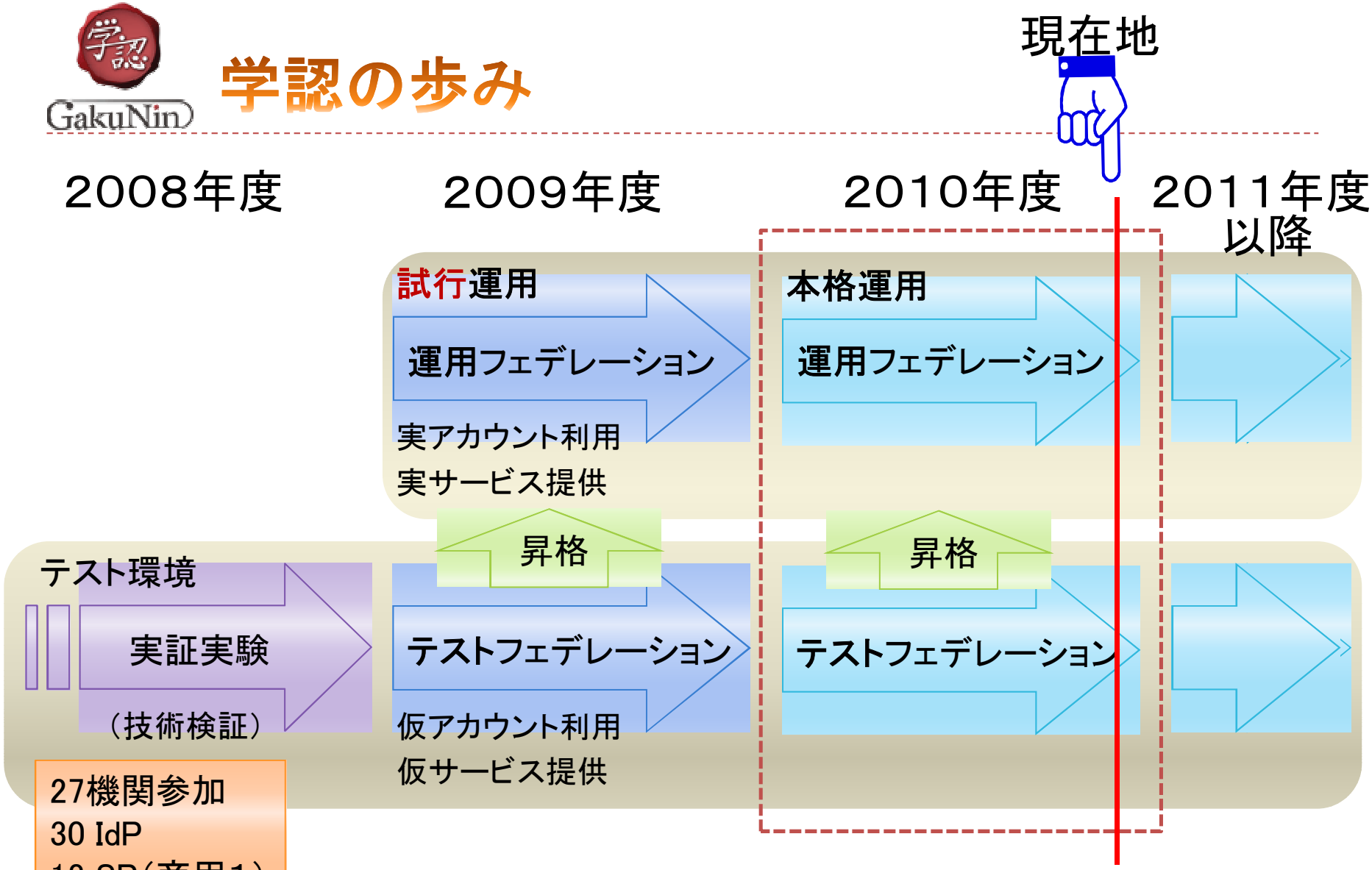



**ユーザは送信する属性の選択が可能**

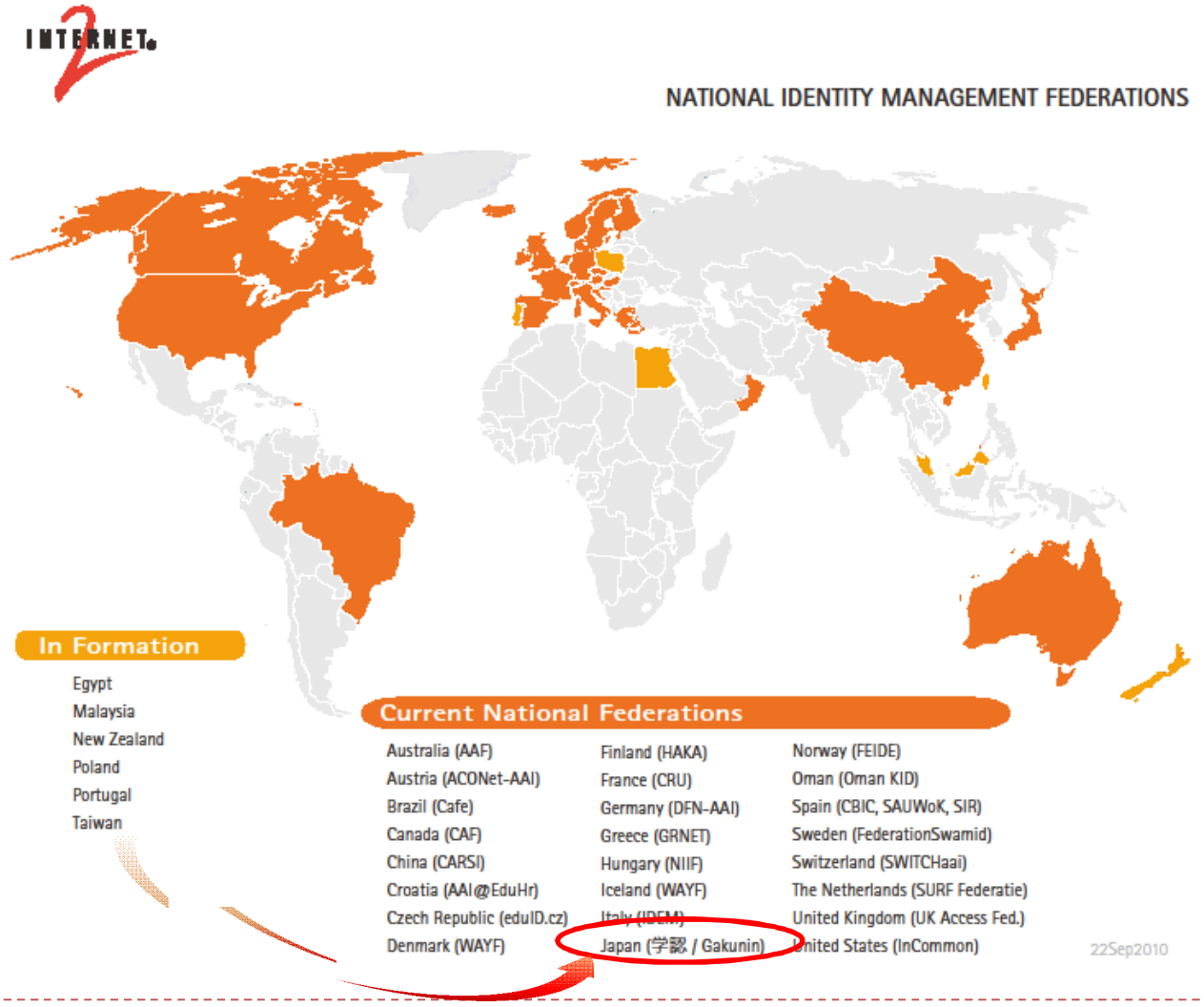


掲載場所：https://upki-portal.nii.ac.jp/docs/fed/technical/attribute

# 学認の歩み


現在地
2008年度
2009年度
2010年度
2011年度以降
試行運用
運用フェデレーション
実アカウント利用
実サービス提供
本格運用
運用フェデレーション
昇格
昇格
テスト環境
実証実験
（技術検証）
テストフェデレーション
仮アカウント利用
仮サービス提供
テストフェデレーション
27機関参加
30 IdP
18 SP（商用1）

# 世界のフェデレーションへの仲間入り






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

# 運用フェデレーション参加IdP (22)

- 国立情報学研究所
- 名古屋大学
- 山形大学
- 千葉大学
- 京都大学
- 広島大学
- 金沢大学
- 北海道大学
- 筑波大学
- 佐賀大学
- 山口大学
- 成城大学
- 東邦大学
- 三重大学
- 日本大学
- 旭川医科大学
- 東京農工大学
- 岡山大学
- 九州工業大学
- 京都産業大学
- 立教大学
- 九州大学

（参加順）

（2月20日現在）

**総ID数≒35万ID**

## テストフェデレーション参加機関

旭川医科大学，東北大学，山形大学，福島大学，高エネルギー加速器研究機構，筑波大学，筑波技術大学，東邦大学，東京大学，東京工業大学，東京農工大学，お茶の水女子大学，産業技術大学院大学，慶應義塾大学，愛知県立大学，鈴鹿工業高等専門学校，京都産業大学，大阪大学，徳島大学，愛媛大学，岡山大学，広島工業大学，九州大学，熊本大学

## 参加検討中機関（by オープンフォーラムアンケート）

姫路獨協大学，静岡大学，中部大学，福井大学，神戸大学，東京学芸大学，京都女子大学，岩手大学，浜松医科大学，東京都医学研究機構，宮崎大学，南山大学，岐阜大学，鹿屋体育大学，京都工芸繊維大学，京都府立大学，高知大学，茨城大学，同志社大学，室蘭工業大学，金城学院大学，福井県立大学，北見工業大学，東京都市大学，北九州工業高等専門学校，島根大学，大阪教育大学



最新情報：https://www.gakunin.jp/docs/fed/participants

# 参加のメリット

- ID管理側（IdP）メリット
  - 大学など情報セキュリティ準拠，個人情報保護などへの対応
  - ID管理，ユーザサポート業務、セキュリティ教育の集約によるコスト削減
  - ID/PW送受信時の（サービスに依存しない）セキュリティ水準の向上
  - シームレス（学内外）なアクセス管理システム統合
- サービス側（SP）メリット
  - 学術分野へのサービスのビジビリティの向上
  - 素早いスタートアップ
  - ID管理からの解放，ユーザサポート業務の軽減
  - ライセンス条件にそった適正な利用
- サービス利用者メリット
  - 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できる）
  - 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への期待

# 現時点で利用可能なSP (20)

（2月20日現在）

- 学術コンテンツ
  - Science Direct / SCOPUS (Elsevier)
  - SpringerLink (Springer)
  - Web of Knowledge / EndNote (Thomson Reuters)
  - OvidSP (Ovid)
  - RefWorks (ProQuest)
  - Pathology Images (Atlases)
  - EBSCOhost (EBSCO)
  - CiNii (NII)
  - IMCデータリポジトリ（金沢大学）
- 開発環境
  - DreamSpark (Microsoft)
- ネットワークサービス
  - Fshare（大容量ファイル交換）サービス（NII）
  - FaMCUs (テレビ会議多地点接続)サービス (NII) – 収容拠点数拡大予定
  - Eduroam-Shib（eduroam用一時アカウント発行）サービス（京大&NII）
  - ゲスト用ネットワークアクセス認証（佐賀大学、広島大学）
  - ファイル送信サービス（金沢大学）
  - 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（山形大学）
  - SecurityLearningシステム（NII）
  - WebELS eLearningシステム（NII）

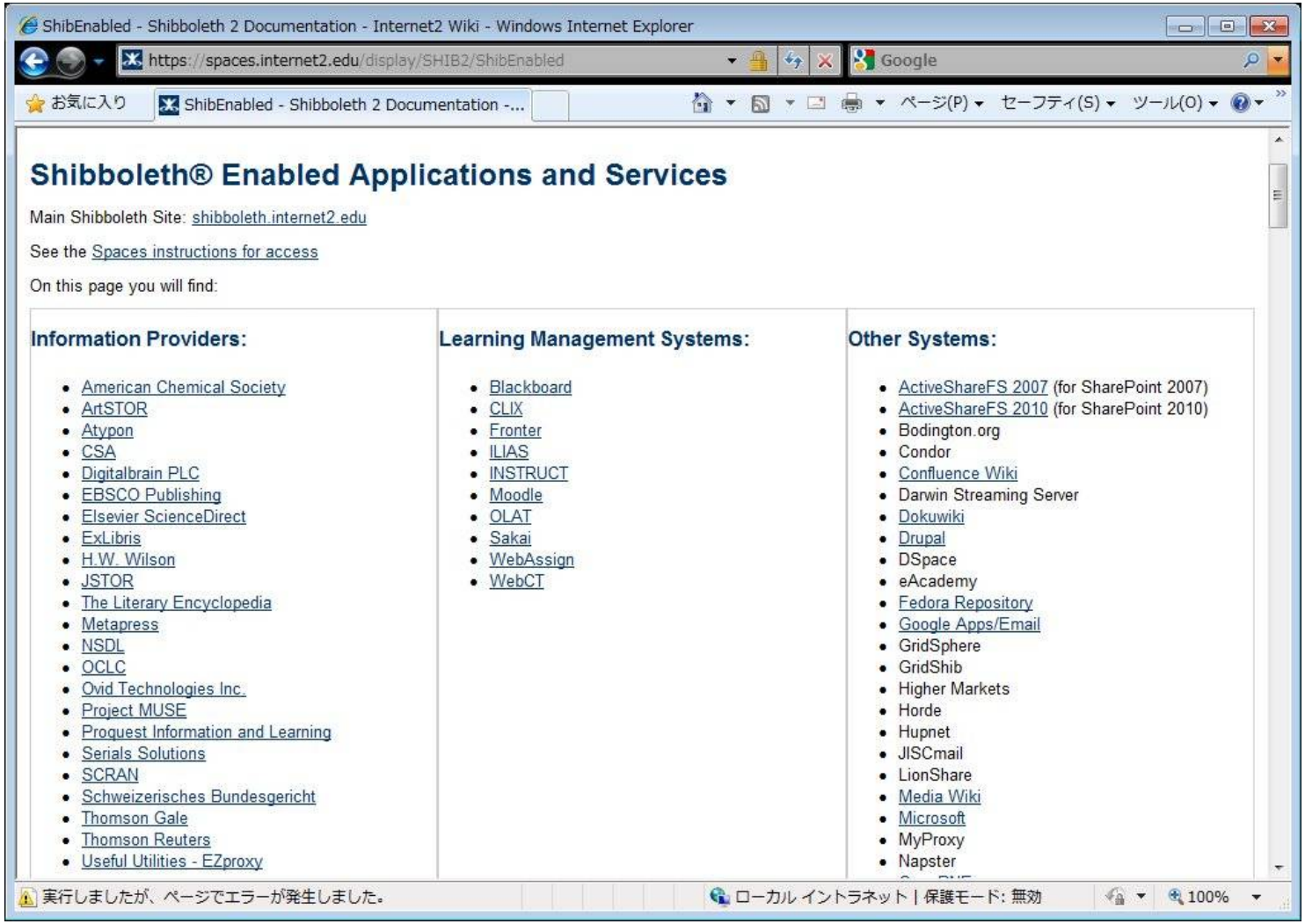
## 接続作業中

- Karger
- jSTOR
- Ebrary
- Tavlor&Francis
- IEEE
- IOP
- PubMed
- Emerald
- SUNMEDIA
- …



最新情報：https://upki-portal.nii.ac.jp/docs/fed/participants

# シボレス化されたアプリケーション例






https://spaces.internet2.edu/display/SHIB2/ShibEnabled

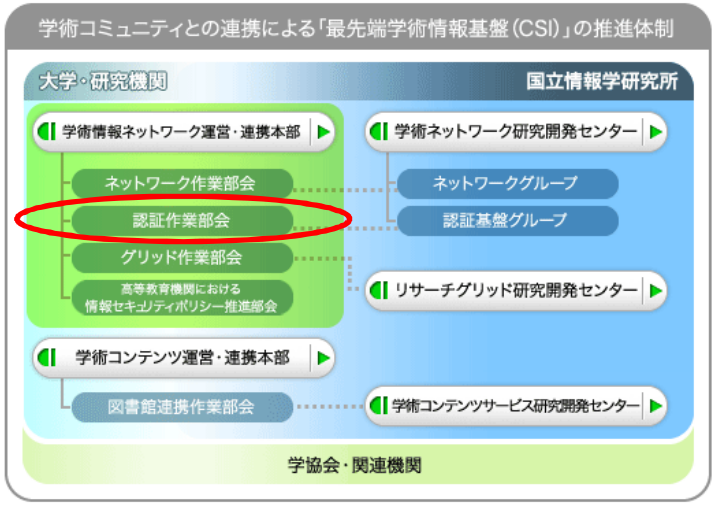
# e-Rad
# （府省共通研究開発管理システム）

- 科研費申請をはじめとする公的研究資金応募システム
  - 多くの研究者にとって馴染みのある、学外サイトの一つ
  - 毎年の申請ごとに、専用のID/PWが分からなくて苦労する
  - アンケート調査実施中

    是非皆様の声を!
    - 実施期間
      - 平成23年3月1日（火）～14日（月）
    - 対象者
      - e-Radの利用経験のある方
    - 実施目的
      - e-Radの運用及びシステム改修に反映し、より質の高いサービスを提供するため

# 「学認」としての活動の開始

- 本格運用の開始
- 「学認」愛称、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
  - テストフェデレーション参加ルールの整理
  - 海外フェデレーション等との連携
  - ケーススタディの提供
  - 病院の参加に関する検討

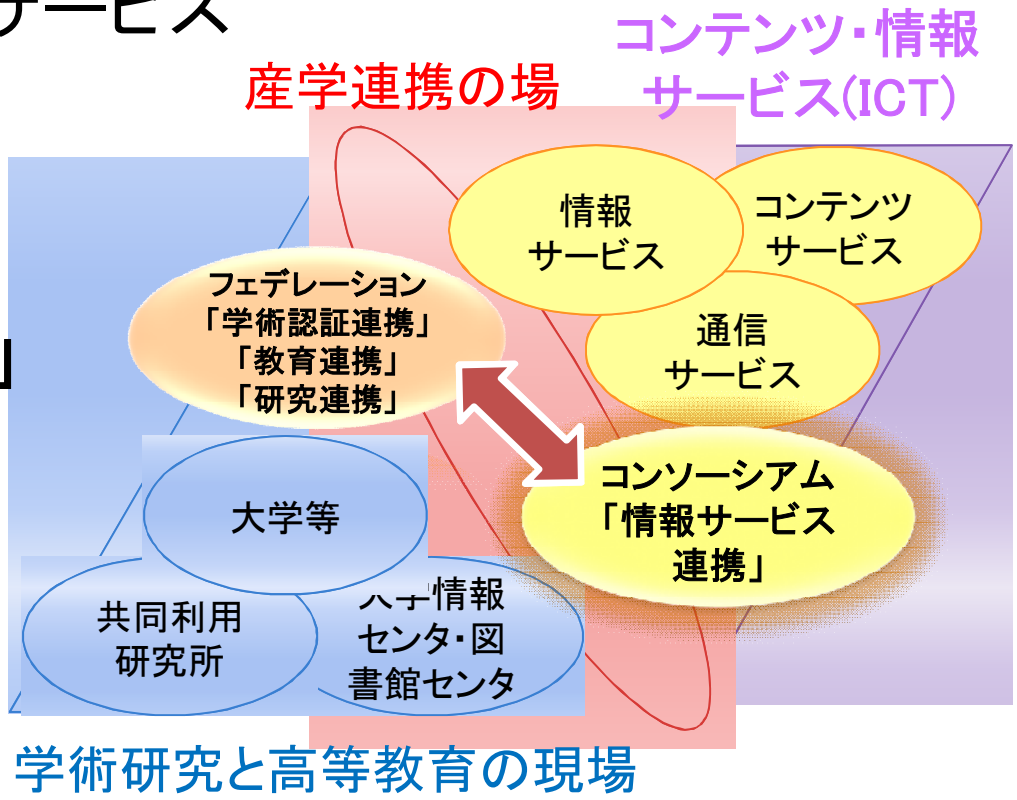



- 実証実験・試行運用(UPKI-Fed)
  - 認証作業部会による方針決定
    - 北大，東北大，東大，名大，京大，阪大，九大，東工大，高エネ研，NII
- 本格運用(GakuNin)
  - 認証作業部会下にTFを設置し，権限を委譲
    - 参加機関の情報基盤センター，図書館などからの，より広い実地メンバーで構成
    - 各種学術コンテンツとの連携は学認ライブラリチームが主導

TFによりフェデレーションの進め方を検討

# 情報サービス連携コンソーシアム（2010年8月発足）

- 「*グローバル ICT 基盤の進展*」を踏まえた、新たな国際「産学」連携の仕組みの構築
- 大学の「*IdM Identity managementの進展*」を前提とした「産学連携による情報サービス連携」体制の構築
- 多様な業界を横断した情報サービス連携の「*ID属性連携(i-Japan)*」基盤構築への貢献




http://ictsfc.org/

# 2010年度の主なイベント

| 日時 | 名称 | 会場 |
|---|---|---|
| 5月20日 | ITRC研究会 GakuNin現状と参加説明 | NICT |
| 6月3-4日 | NIIオープンハウス GakuNinブース出展 | NII |
| 6月29日 | Sunmedia学術情報ソリューションセミナー　GakuNin説明 | 大阪 |
| 7月02日 | Sunmedia学術情報ソリューションセミナー　GakuNin説明 | 六本木 |
| 7月7, 8日 | シボレスIdP, SP研修会 | NII |
| 7月15日 | 第7回国立大学法人情報系センター協議会 | 海洋大学 |
| 7月19日-23日 | IEEE SAINT GakuNinブース出展 | ソウル |
| 7月28日 | e-Learningワールド GakuNinブース出展 | 東京ビックサイト |
| 9月09日 | 第5回情報系センター研究交流・連絡会議 | 和歌山 |
| 9月16-17日 | シボレスIdP, SP研修会 | NII |
| 9月27-28日 | TOPICネットワーク担当職員研修会 | 岩手 |
| 10月7-8日 | シボレスIdP, SP研修会 | NII |
| 11月01日- | Internet2 Fall Meeting 出展 | アトランタ |
| 11月15-16日 | シボレスIdP, SP研修会 | NII(募集中) |
| 11月24日- | 図書館総合展 | パシフィコ横浜 |
| 11月10日 | [SINET]オープンフォーラム | NII |
| 11月～12月 | SINET4説明会 | 札幌, 東京, 名古屋, 京都, 福岡 |
| 12月10日 | 情報処理学会CLE研究会 | 京都 |
| 12月14日 | カンターライニシアティブ 技術セミナー 2010 | 新宿 |
| 1月11-12日 | シボレスIdP, SP研修会 | NII |
| 1月20-21日, 24-25日 | シボレスIdP, SP研修会 | NII |
| 2月24日 | APAN31 Middleware WG発表 | 香港 |
| 3月7日 | 学認シンポジウム | 一橋記念講堂 |

# シボレス環境構築研修

- 2009年度までは，NII情報処理軽井沢セミナーにて実施
- 2010年度からは，NII講習システムを用いて実施
  - 2日間コース
    - IdP構築実習（1日目）
    - SP構築実習（2日目）
  - 計8回実施
    - 大学向け3回
    - 大学＋企業向け5回
      - 計120名以上が受講
- 2011年度も引き続き実施
  - 大学向け（3回を予定）
    - 6/20–21，8/4–5，11/1–2
  - 大学＋企業向け（調整中）

大学向け研修会詳細　http://www.nii.ac.jp/hrd/index.html に掲載予定
大学＋企業向け研修会　https://www.gakunin.jp/docs/news/ に掲載予定

# 学認への参加方法

- 学認申請システム
  - 学認への参加申請，メタデータ登録・更新等がWebを通してオンラインで可能になります
- テストフェデレーション
  1. 匿名での申請情報登録（およびアカウント作成）
  2. 事務局での参加承認
  3. フェデレーションメタデータの自動更新

通常一日で
参加完了
利用開始可能

学認が提供するテストSPやIDPを利用して接続確認

- 運用フェデレーションの場合は？
  - オフラインによる確認が1ステップ増えるだけ

実施要領，システム運用基準が守られていることが前提

# さらなる学認の展開に向けて

- 技術開発
  - 新しい利用形態、活用方法の検討（電子ブック、属性プロバイダ）
  - プライバシー保護のための機構(uApprove.jp)
  - 学認申請システム
- 体制、ドキュメント等の整備
  - 学認タスクフォース、学認ライブラリチーム
  - 各種ドキュメントの整備、見直し、英語化
- 導入事例の提供
  - 先行する各大学でのケーススタディ **（本日配布中!）**
- 広報、協力のためのチャンネルの拡充
  - NIIオープンフォーラム
  - 大学ICT推進協議会
  - 情報サービス連携コンソーシアム (ictsfc.org)
  - その他…