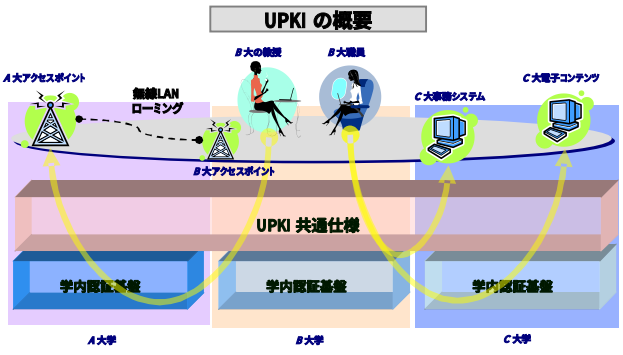
UPKIシングルサインオン実証実験の概要

名古屋大学情報連携基盤センター
(国立情報学研究所(客員))
平野　靖

UPKIについて

大学間連携のための全国共同電子認証基盤 (UPKI) とは

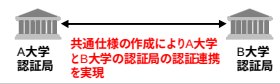
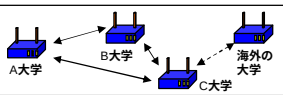
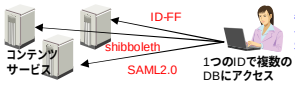
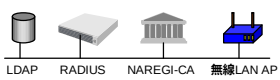
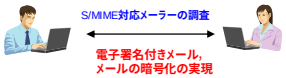
- 最先端学術情報基盤(Cyber Science Infrastructure)実現のため，大学等が保有する，教育・研究用計算機，電子コンテンツ，ネットワークおよび事務システムなどの学術情報資源を安心・安全かつ有効に活用するための電子認証基盤
- PKI (公開鍵認証基盤) を活用



学術力（情報力・研究力・教育力・文化力）の強化

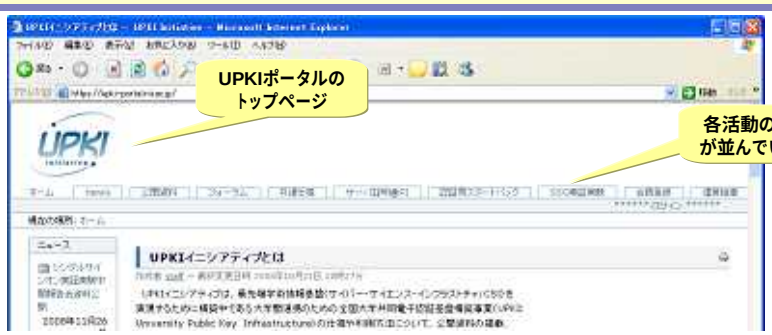
- 30年前は、大型計算機、大型実験設備の保有が研究力・教育力の差に
- 10年前から、インターネットが情報力・研究力・教育力の差に
- 5年前ころから、コンテンツ発信・探索が情報力・研究力・教育力・文化力の差に
- これからは、フェデレーション・コラボレーション・コミュニティのための認証基盤が学術力の差になるのでは・・・・

UPKIの活動

項番	事項	内容
1	「UPKI共通仕様」の作成と配布	 「UPKI共通仕様」の利用により大学での ・学内認証局の構築 ・CP/CPS等の規程の整備 が容易に実現可能に
2	オープンドメイン認証局の構築とサーバ証明書の発行	 オープンドメイン認証局の構築により，全世界に通用するサーバ証明書を発行し，大学のWebサーバの実在性証明と通信の暗号化を実現
3	大学間無線LANローミングの実現	 eduroamによる大学間無線LANローミングを実現。海外のeduroam参加機関との連携も実現
4	コンテンツサービスのシングルサインオン実験	 各種データベースサーバへのシングルサインオンを実現するため，shibboleth，SAML2.0等の仕様を調査し，UPKIにふさわしい方式を検討
5	NAREGI-CAを利用した認証局ソフトウェアパッケージの開発	 オープンソースの認証局ソフトウェアあるNAREGI-CAを用いて，認証局を簡単に構築し，無線LAN認証を容易に実現できるソフトウェアを開発 これにより，大学の認証局構築を促進する
6	S/MIME証明書の試験利用	 S/MIME証明書を，認証関係者間で試験利用するとともに，対応メーラーの調査，WebメールでのS/MIME利用の調査研究を実施

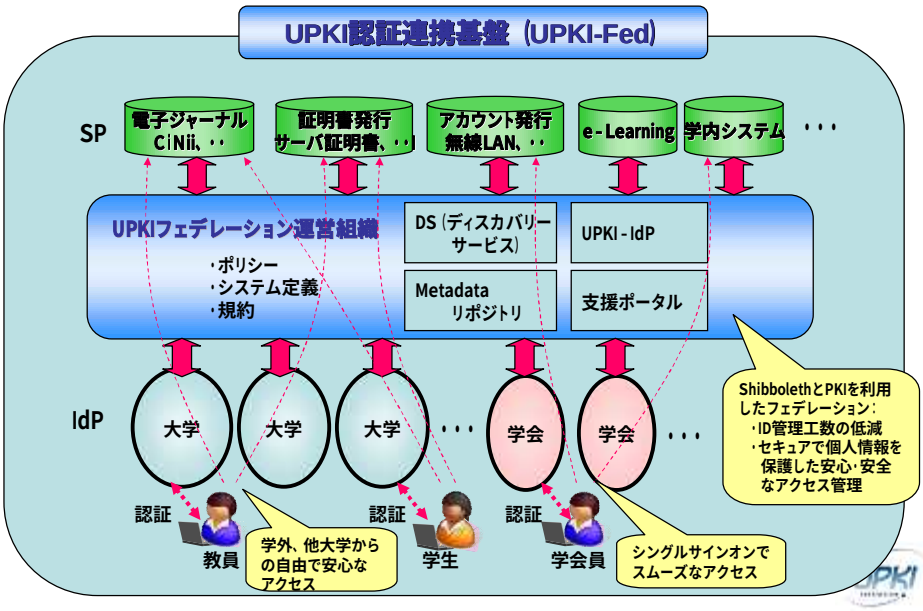
UPKIイニシアティブ

- UPKIの相互運用性，利用促進に関しての意見交換や技術的な検証を行う場として設立（2006年8月16日）
- 運営主体は認証作業部会
- UPKIイニシアティブの活動は，主にホームページ上のUPKIポータルを使用（https://upki-portal.nii.ac.jp/）
- 各活動のページから関連情報、資料を発信



UPKI認証連携基盤
（UPKI-Fed）

UPKI認証連携基盤

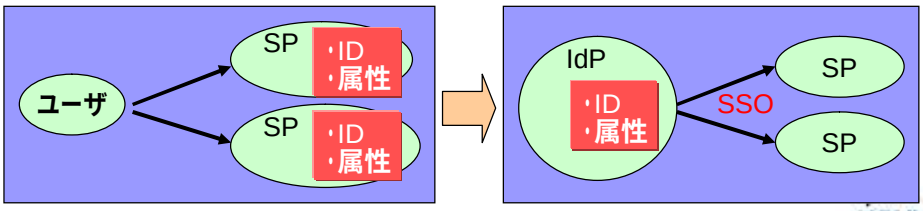


Shibboleth概要

- 米国EDUCAUSE／Internet2にて2000年に発足したプロジェクト
- SAML、eduPerson等の標準仕様を利用した、認可のための属性交換を行う標準仕様とオープンソフト
- 最新はShibboleth V2.1
- 米国、欧州でShibbolethのFederationが運用、拡大

Shibbolethの特徴

(1) 属性の分散管理＝Federation
　IdP (大学) がIDと属性を管理して、SPがこれを利用
(2) プライバシ保護
　ユーザの識別情報をIdP外部に公開しない仕組み
　ユーザは各SPに対する各属性の公開を制御可能
(3) SSO
　Webサービスのシングルサインオン



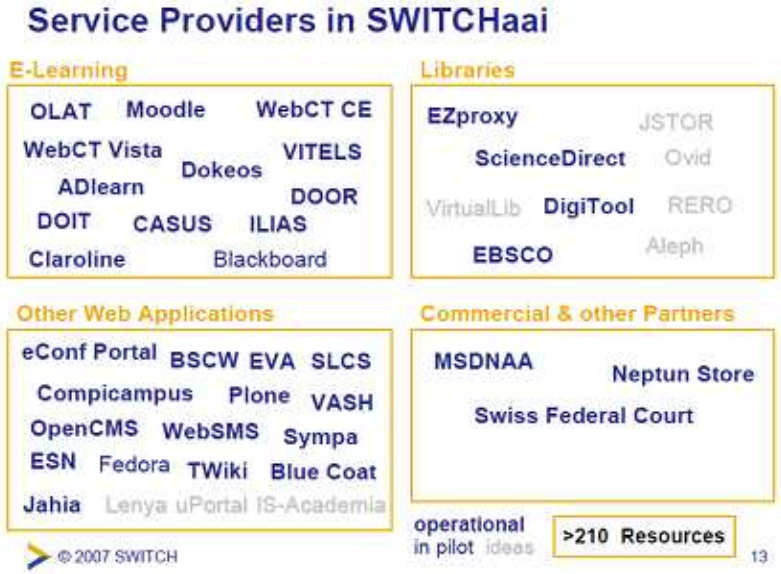
Federationについて

- あるルール (ポリシー) のもとで属性交換の相互運用に合意した組織 (IdP、SP) の集合
- Federation運営組織が、ポリシー策定や認証局の認定、DS、メタデータDLサイトの提供を行う
- 世界のIdP;
  - 米国: InCommon
  - 英国: The UK Access Management Federation
  - スイス: SWITCHaai
  - オーストラリア: MAMS、AAF
  - フィンランド: HAKA
  - フランス: CRU
  - ノルウェイ: FEIDE
  - デンマーク: WAYF
  - ドイツ: DFN-AAI
- 世界のSP;
  - ScienceDirect、 Ovid Technologies、JSTOR、ExLibris、Digitalbrain、Thomson Gale等
  - Blackboard、WebCT、Moodle、OLAT、WebAssign等
  - DSpace, uPOrtal, Napster, Sharepoint, Symplicity, TWiki, Zope+Plone, eAcademy等

スイスのFederation事例

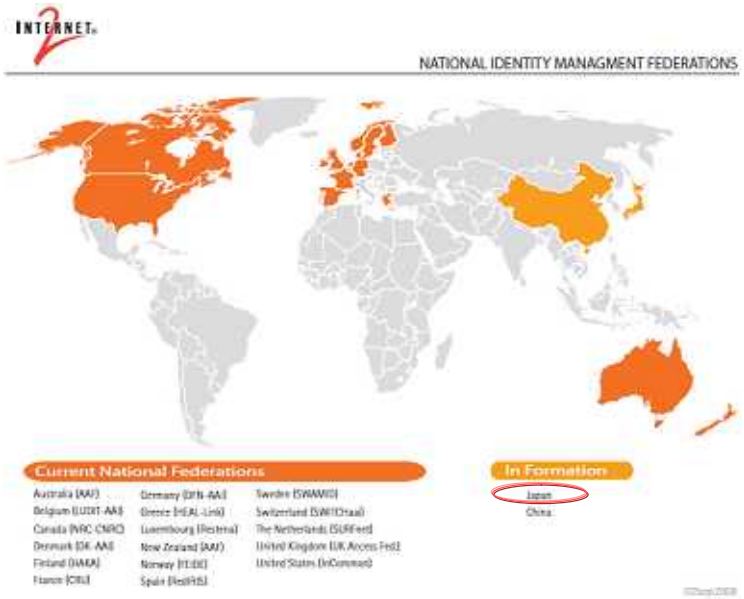
- SWITCH（1987年設立）：
  スイスの大学が出資するPrivate Company。
  スイスの大学に、認証認可基盤を含むネットワークサービス（AAI、Grid、PKI、Mobile）を幅広く提供。
- SWITCHaaiの構築（2005－2007）：
  Shibbolethベースの認証・認可フェデレーションを構築。
  スイス国内75%の大学が利用。
  e-Learning利用基盤からスイス国内標準基盤へ。
- 今後はAAA/SWITCHを展開（2008－2011）：
  ・AAA（Auditing/Accounting/Assurance）
  ・Grid middleware
  ・VO
  ・e-Learning

SWITCHaaiのSP（サービス）



＊ SWITCH “AAI Introductory Tutorial”より引用

(参考) 世界のフェデレーション



Internet2 informatin kits http://www.internet2.edu/pubs/national_federations200809.pdf から引用

シングルサインオン実証実験について

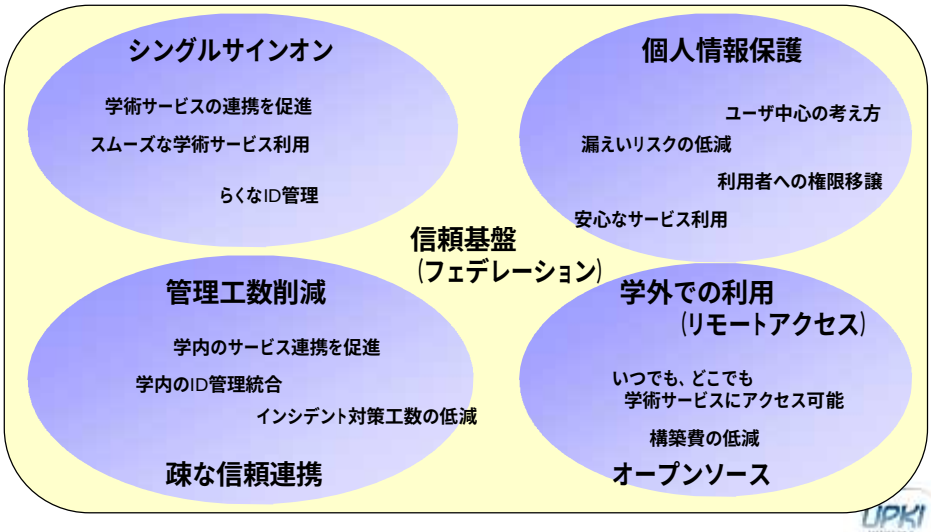
2006年度	2007年度	2008年度	2009年度以降
シングルサインオンの海外状況調査	シングルサインオンの実現方法の検討	電子コンテンツシングルサインオン実証実験	シングルサインオンによる大学間認証連携の実現

「各大学の利用者が、安全・安心かつ有効に
学術サービスを利用するための基盤の実証と検討を行う。」

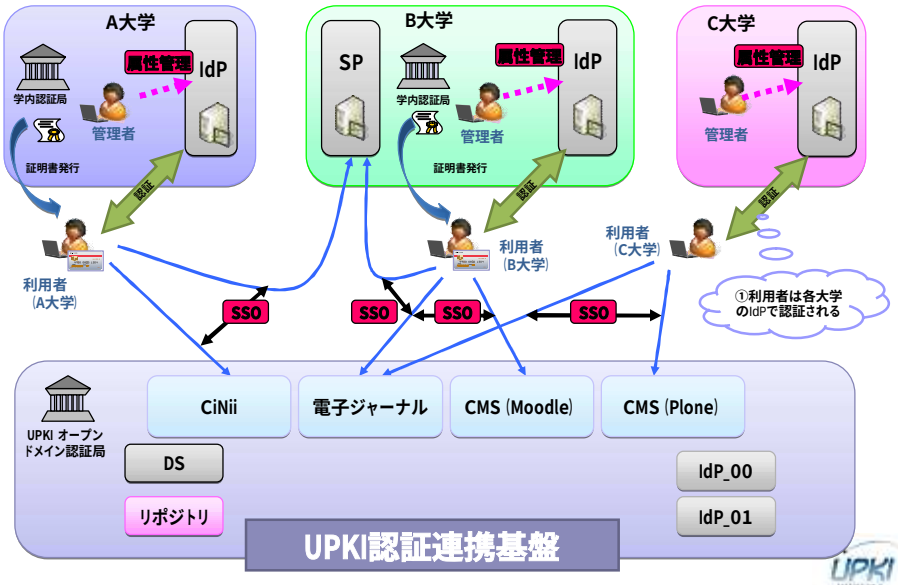
- 各大学間を実際に接続して、ユーザ利便性向上、管理工数削減等、UPKI認証連携基盤が各大学の現実の状況に適合すること、効果があること、運用可能であること等を実証・評価する。
- 今後のUPKI認証連携基盤を実現、運用していくための、アーキテクチャ、運用ポリシー等を検討・策定する。

UPKI認証連携基盤の利便性

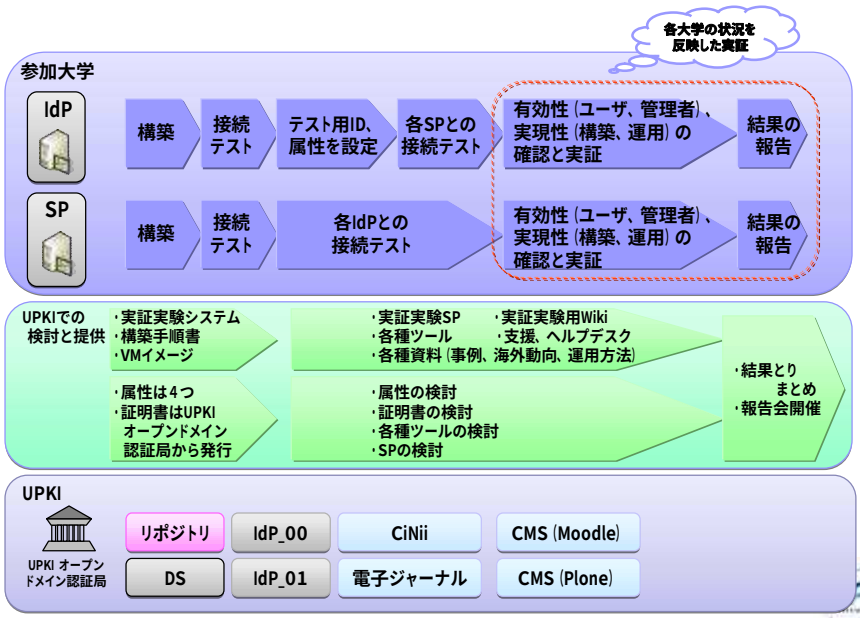
実証実験で、様々な利便性を検証して、枠組みの検討･定義を行う。



実証実験の概要



実証実験のスケジュール



各参加機関の構築状況

参加機関名称	IdP	SP
北海道大学	○	－
東北大学	○＊	－
山形大学	－	－
福島大学	－	－
高ｴﾈﾙｷﾞｰ加速器研究機構	－	－
筑波大学	○2	（未公開）
筑波技術大学	－	－
千葉大学	△	－
東京大学	○＊	－
東京工業大学	○	（未公開）
お茶の水女子大学	－	－
産業技術大学院大学	○2	マルチマウスAP、（構築中）
慶応義塾大学	－	－
国立情報学研究所	○2＊	CiNiiテスト＊

参加機関名称	IdP	SP
金沢大学	○	ファイル送信サービス、DSpace
名古屋大学	○	－
愛知県立看護大学	○	－
京都大学	○	（無線LANｱｶｳﾝﾄ発行）
京都産業大学	－	－
大阪大学	○	（グリッド証明書発行）
愛媛大学	－	－
徳島大学	－	（OpenPNE）
広島大学	○	－
山口大学	○＊	（未公開）＊
九州大学	○	－
熊本大学	○	－
佐賀大学	○＊	（未公開）

○　：構築済み
2　：2ｻｲﾄ構築
△　：接続実験中
＊　：メタデータ自動更新設定済み

実証実験の進め方

Ⅰ. 利用方法の検証:
- 1. ユーザの視点
- 2. 運用者の視点 (IdP)
- 3. 運用者の視点 (SP)

Ⅱ. 連携実験の検証:
- 1. 属性管理
- 2. セキュリティ設定実験
- 3. ツール利用実験

利用方法の検証 (ユーザ)

- 【想定するユーザのメリット】
  - シングルサインオン
    - IDの統合、 (少なくとも) 1つのパスワードを削減
  - 学外からのアクセス
  - ユーザは本人性 (身元) を明かす機会が減少
    - 個人情報は本人と所属機関で管理される
  - 出版社からより良いサービスを提供される
    - 個人情報を保護したマイページの提供
- 【検証項目】
  - 学内、学外からのログイン
  - シングルサインオンの利便性
  - 操作性
  - 安心感
  - 従来方法との比較

利用方法の検証（IdP）

- 【想定するIdPサイトのメリット】
  - 個人情報保護法の遵守
  - ユーザへの、より良いサービスの提供
  - 既存のアクセス管理システムとの連携
  - 学内、学外含めた全てのリソースに対する管理方法の統一化
  - 集中管理によるサポート問題の削減
- 【検証項目】
  - 構築状況
    - 難易度、サーバ証明書の種類、認証方式、ネットワーク構成等
  - 運用状況
    - 個人情報管理、属性リリースの設定方法、学内ポリシーとの関係等
  - 構築、運用の課題等

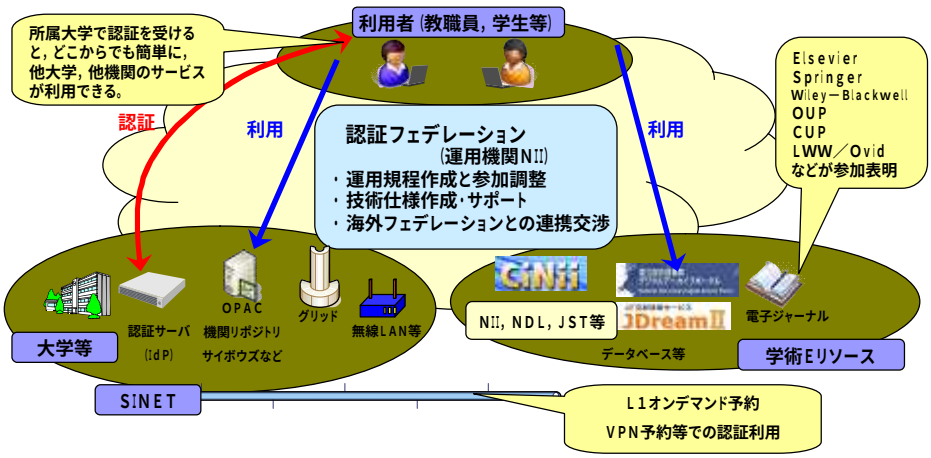
利用方法の検証（SP）

- 【想定するSPサイトのメリット】
  - ユーザデータベースの運用・管理がいらなくなる
    - 認証はIdPで実行
    - 認可は機関、職位、権限で判断
  - ユーザサポート工数の削減
  - 規程遵守のための工数削減
    - 個人情報の蓄積、処理を削減
  - 厳格なライセンス制御管理の実現
  - ID統合により、ユーザのID／パスワード管理が向上
  - サービス利用機関は集中管理により正確な認証を運用・管理可能となる
- 【検証項目】
  - 構築状況
    - 難易度、提供するアプリケーション、必須属性、ネットワーク構成等
  - 運用状況
    - 個人情報管理、ユーザ管理工数等
  - 構築、運用の課題等

連携実験の検証

- 属性管理
  - 各属性の交換
  - 学内LDAPとの接続性
  - SPに対応した属性リリース制御
  - 日本語への対応
- セキュリティ設定実験
  - Metadata自動ダウンロード（実施済み）
  - Metadataの署名と検証
  - SP、IdP間のTLS通信等（UPKI内で実施予定）
- ツール利用実験
  - ArpViewerのインストールと利用

学術フェデレーションの構築（2009年度～）

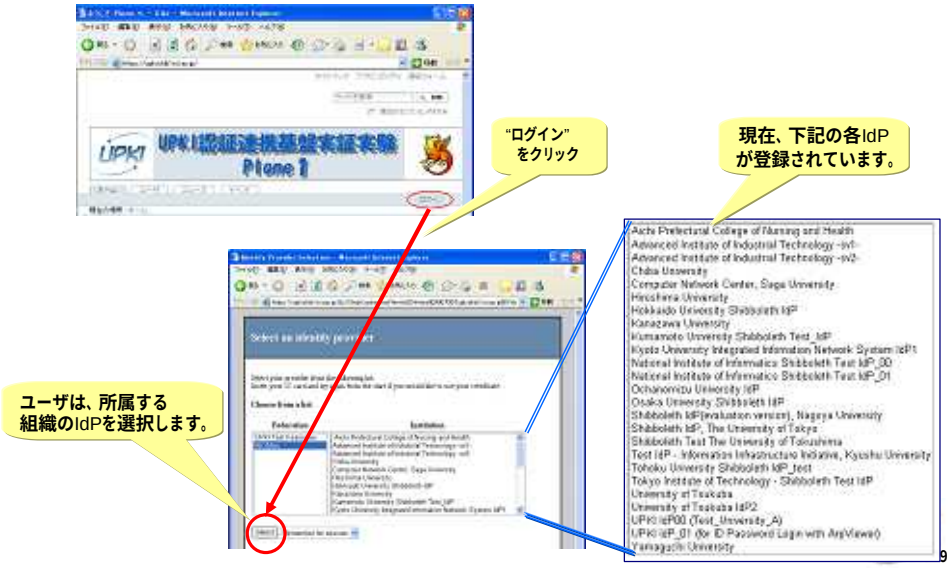


- 大学等とNIIが連携して「認証フェデレーション」を構築・運用する
- 2009年4月からフェデレーション試行運用を開始
- 2009年4月時点で，複数の大学，NII内でのシングルサインオン実現
- 2010年4月からの事業化を目指す

本プレゼンテーションは
国立情報学研究所 片岡俊幸 特任准教授
が作成したものである．

シングルサインオンの動き

1．まず、最初のサービス (SP) にログインします。

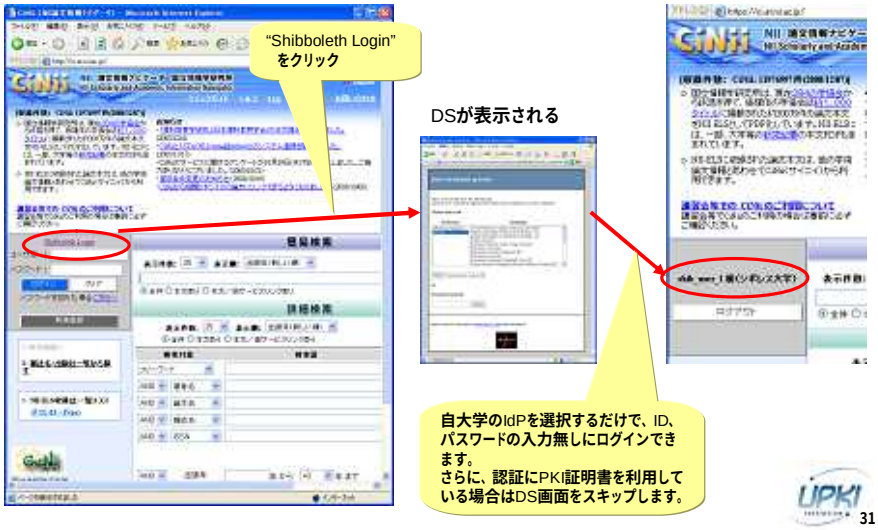


シングルサインオンの動き

2．これで、1番目のサービスに“shib_user_1”としてログインしました。

シングルサインオンの動き

3．2番目のサービス（CiNiiテストログイン）にアクセスして、
シングルサインオンします。



（参考）Shibbolethの対応ｱﾌﾟﾘｹｰｼｮﾝ

Information Providers:

- American Chemical Society
- ArtSTOR
- Atypon
- CSA
- Digitalbrain PLC
- EBSCO Publishing
- Elsevier ScienceDirect
- ExLibris
- JSTOR
- The Literary Encyclopedia
- NSDL
- OCLC
- Ovid Technologies Inc.
- Project MUSE
- Proquest Information and Learning
- Serials Solutions
- SCRAN
- Thomson Gale
- Thomson ISI/Scientific
- Useful Utilities - f2proxy

Learning Management Systems:

- Blackboard
- CLIX
- ILIAS
- Moodle
- OLAT
- Sakai
- WebAssign
- WebCT

Other Systems:

- Bodington.org
- Condor
- Confluence Wiki
- Darwin Streaming Server
- DSpace
- eAcademy
- Fedora
- GridSphere
- GridShib
- Higher Markets
- Horde
- Hupnet
- JISCmail
- LionShare
- Media Wiki
- MyProxy
- Napster
- PHEAA
- Sharepoint@ from Microsoft
- SYMPA
- Symplicity
- TurnItIn
- TWiki
- uPortal
- Zope + Plone

＊“https://wiki.internet2.edu/confluence/display/seas/Home”より引用