シングルサインオンの基礎知識
～Shibbolethの概要～

国立情報学研究所
学術基盤推進部基盤企画課
樋 口 秀 樹

説明をはじめる前に

- 軽井沢セミナーで認証を取り上げるのは4回目です
- 今年は，Shibbolethによるシングルサインオンの実現です
- この数年間，いろいろな認証に手出しをしましたが，NIIのコンテンツ事業のための認証にシフトしてきました

セミナーの目的は

- 認証のシステムだけならば，技術的なハードルはさほど高くありません
- 個人情報を扱うことや学内の調整など，制度面や運用面に高いハードルがあります
- これをクリアするためには，認証の理念，効果，効用を理解し，周囲を説得する必要があります
- これを理解してもらうことが，このセミナー全体の目的です

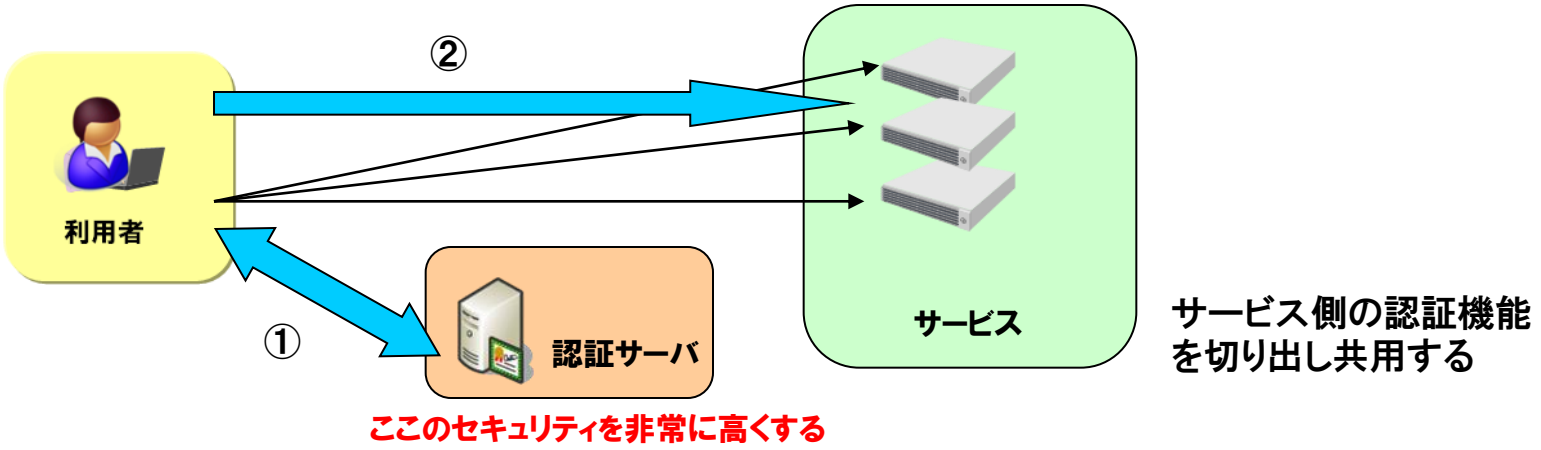
現実の世界とネットワーク内の世界

	現実の世界	ネットワークの世界
本人確認を行う方法は？	見た目で確認 声の感じ 第六感	自己申告 文章の雰囲気 電子証明書
例	10万円以上の振り込みは窓口	

- ネットワークを経由することで，人間の感での判断が難しくなる
- しかしながら，ネットワークは空間を超える利便性がある
- ネットの世界と現実世界をシームレスにして，便利な世界を作りたい
- このためには，電子認証が重要な要素となる

シングルサインオンとは

- 複数のシステムを，1つのID/パスワードで利用できるようにする
- 全システムのID/パスワードを一緒にしても効果は同じ？
  - 例えば，銀行の暗証番号を全部同じにする
  - 一つばれたら，全部盗まれる？
- これまで各サーバにあった認証機能を切り出し，同一の認証機能を用いることで実現可能

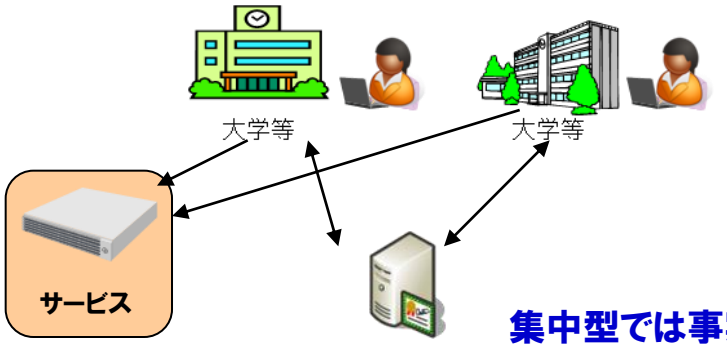


シングルサインオンの効果

- ID/パスワード管理負荷の削減
  - 利用者，サーバ管理者ともに楽になる
  - 人事異動などのメンテナンスが容易
- セキュリティの向上
  - 分散しているID/パスワードを集中させることにより，情報漏洩のリスクを低減できる。
    - 中にはいい加減な管理のサーバもある。
  - ただし，集中させたサーバの管理は非常に厳密に行う必要がある。ハッキングされた場合の被害は甚大。
- サービス部門は個人情報を持たなくても良い
  - 厳密には少々違いますが，これは後ほど。

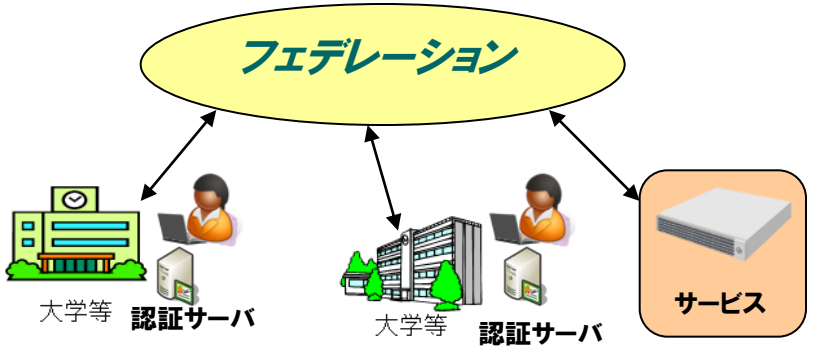
Shibbolethの考え方

- 認証基盤を切り出してシングルサインオンを構築しようとすると一極集中サーバが必要
- 全大学の認証を可能とする認証サーバ構築は非現実的
- 大学に分散した認証基盤を連携させて認証連携を実現
- 分散した認証基盤やサービスとの“信頼”をどう行うのかがポイント（フェデレーションの構築）
- Shibbolethはあくまでも技術要素の1つにすぎない



集中型では事実上運用不可能

リスクが集中する



分散配置された認証基盤を信頼しあうことでリスク分散と運用の容易性を実現

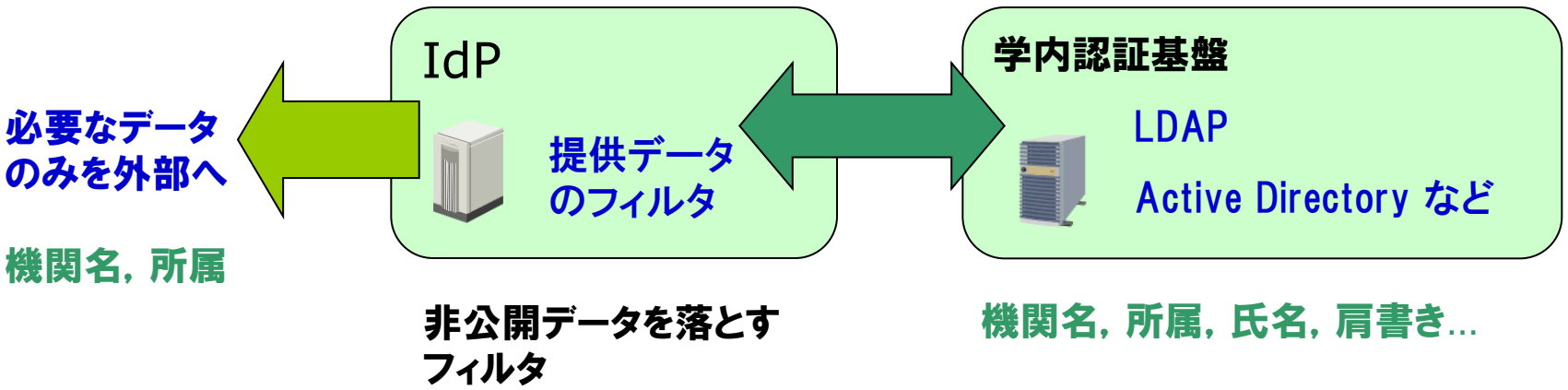
信頼の枠組みである「フェデレーション」を構築

Shibbolethに必要なサーバ

- IdP（ID Provider）
  - フェデレーション内に構成員の情報を流すサーバ
  - フェデレーションに参加する大学等が構築
- SP（Service Provider）
  - Shibbolethで認証を受けた人に対してサービスを行うサーバ
  - 電子ジャーナル，データベース，E-ラーニング等
- DS（Discovery Service）
  - IdPを検索するシステム
  - フェデレーションが運用
  - ここに名前がのることにより「フェデレーションに参加」

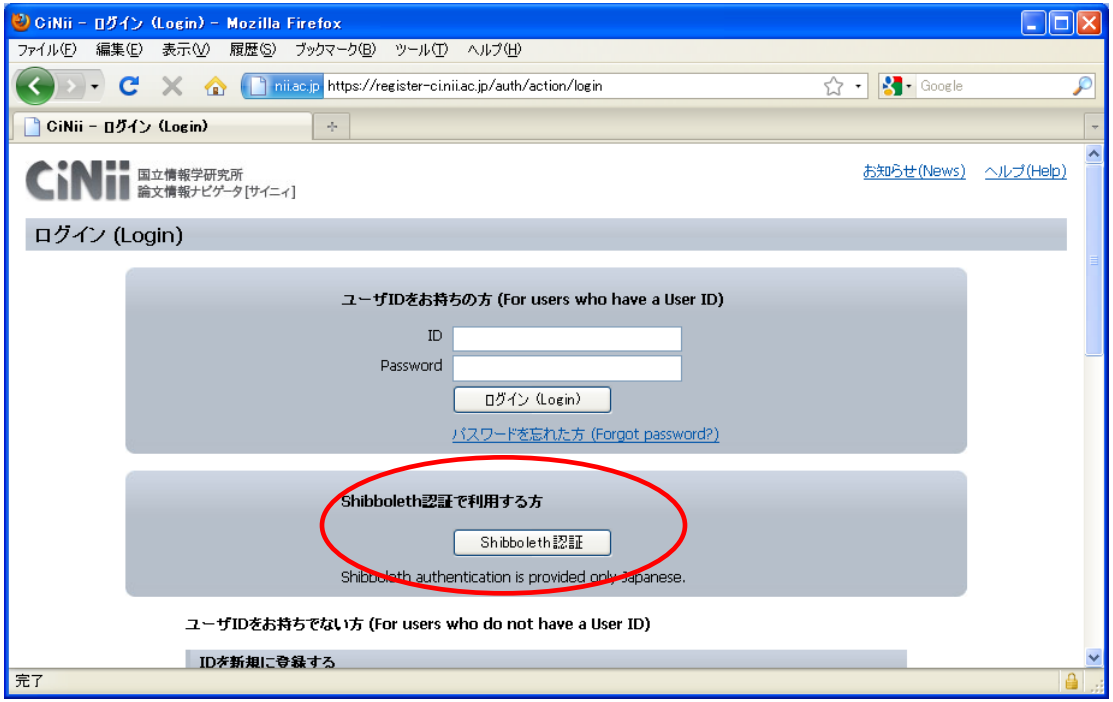
IdP（Id Provider)とは

- フェデレーション内に情報を流すサーバであり，大学等が構築
- IdP自信は情報を持っていない
- 情報はLDAPやActive Directory等，既存の認証基盤を参照
- IdPは単なるフィルタであり，学内認証基盤から特定のデータのみを外部へ公開する
- 公開できるデータの制御が可能である
  - このため，Shibbolethはしばしば個人情報保護に優れていると言われるが，サーバ自体がハッキングに強固という意味ではない。
  - 慎重な操作が必要なのは，LDAPやActive Directoryと同じ



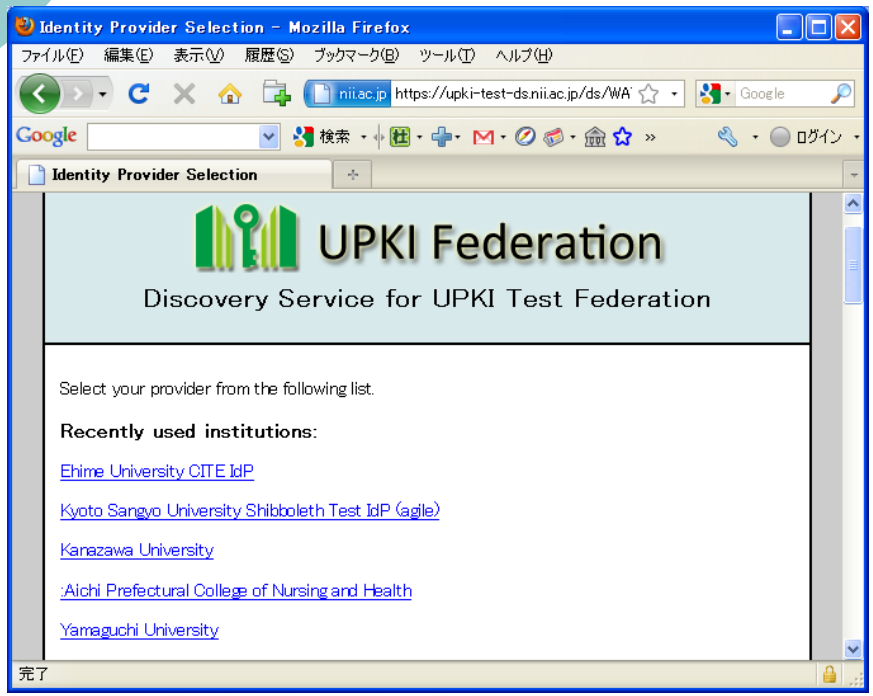
SP（Service Provider）とは

- サービスを提供するWebサーバのこと
- “シボレスログイン”等のボタンがあればShibbolethで利用可能なSPである
- ボタンがあっても使えなければ仲間引き込もう

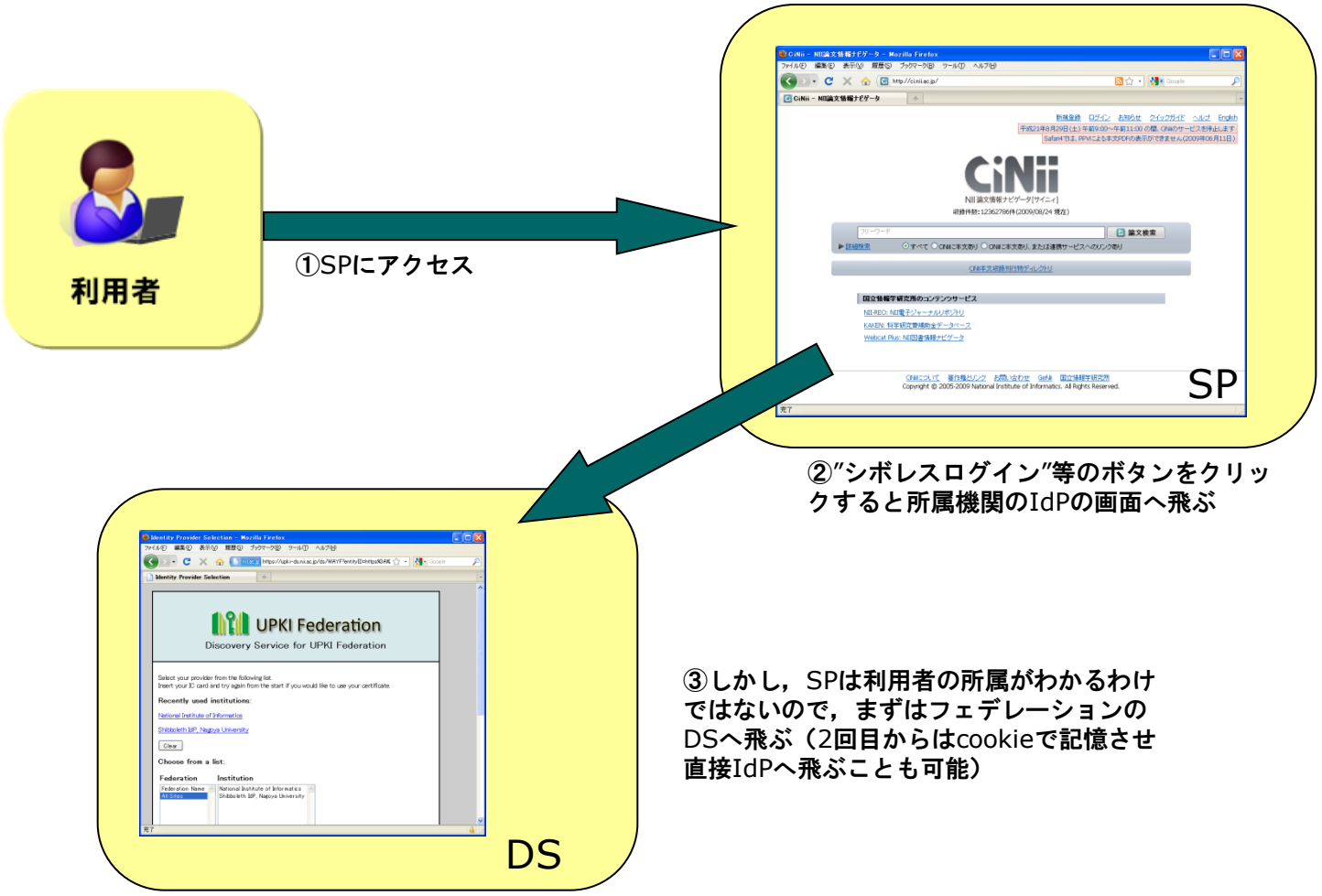


DS（Discovery Service）の機能

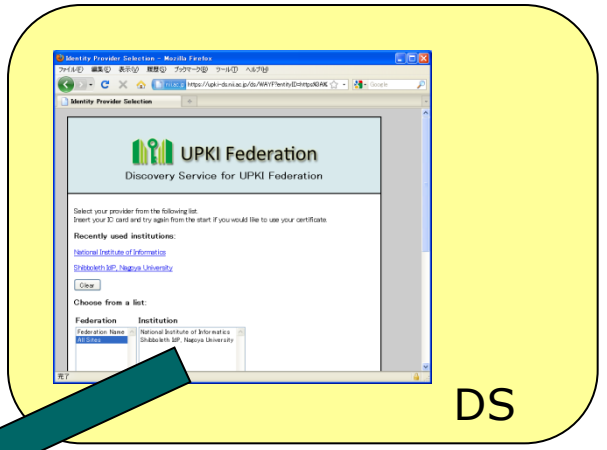
- IdPを選択するのがDSの機能（なぜ選択が必要かは後ほど）
- 見かけは参加機関の一覧表



Shibbolethの挙動(1)

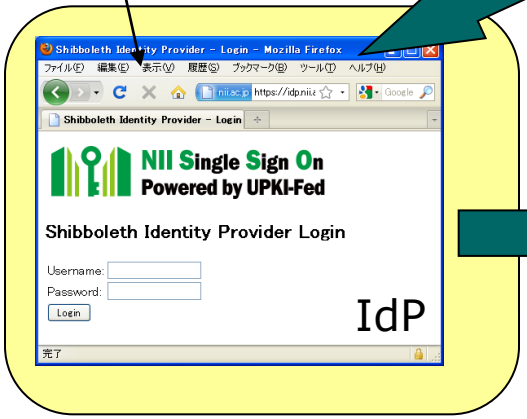


Shibbolethの挙動(2)



⑤所属機関のIdPにID/パスワードを入力

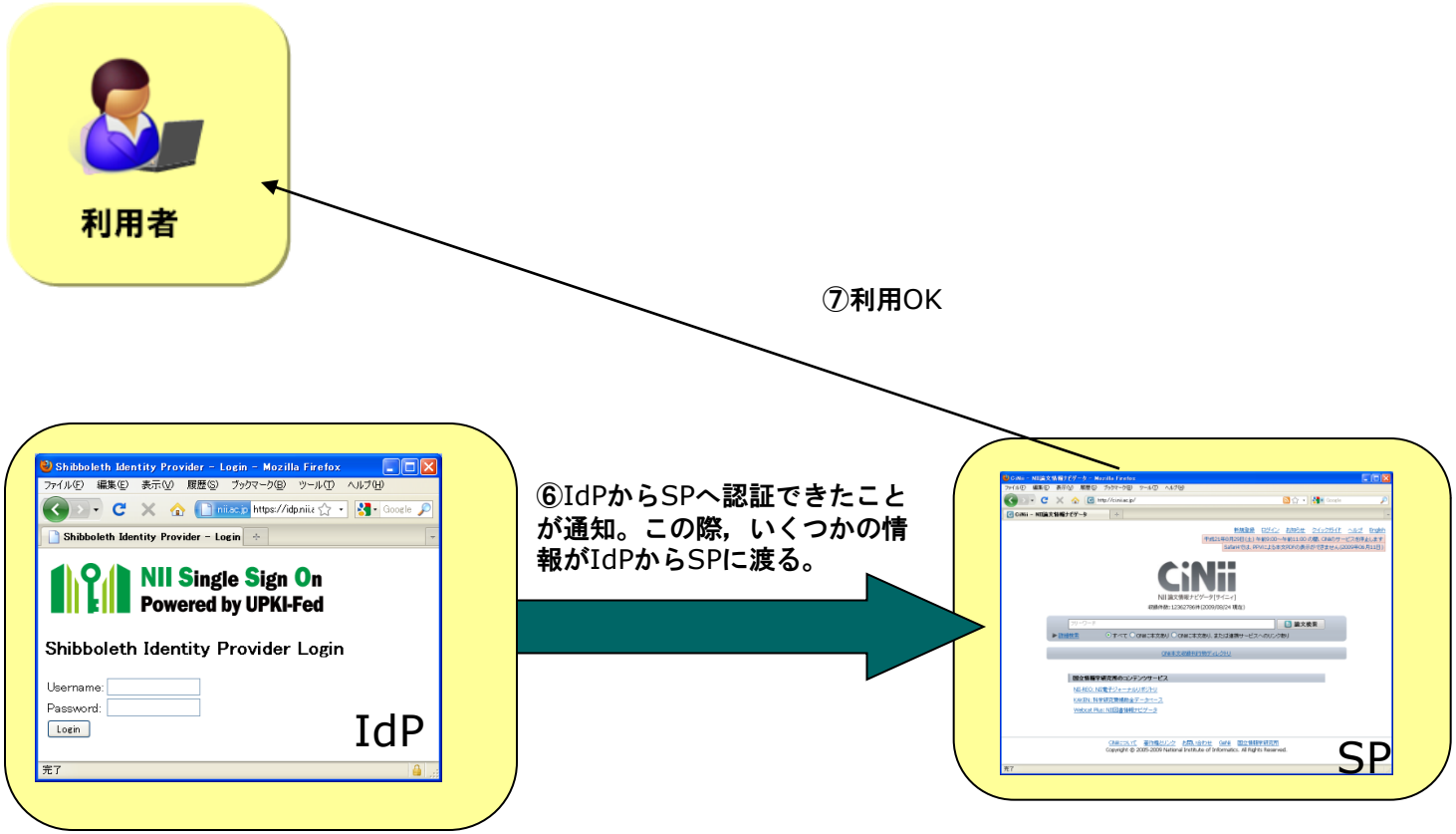
④DSの一覧から所属機関を選択



OK？

NG？

Shibbolethの挙動(3)



厳密にはSPが必要な情報を要求する

必要な準備（学内データの利用）

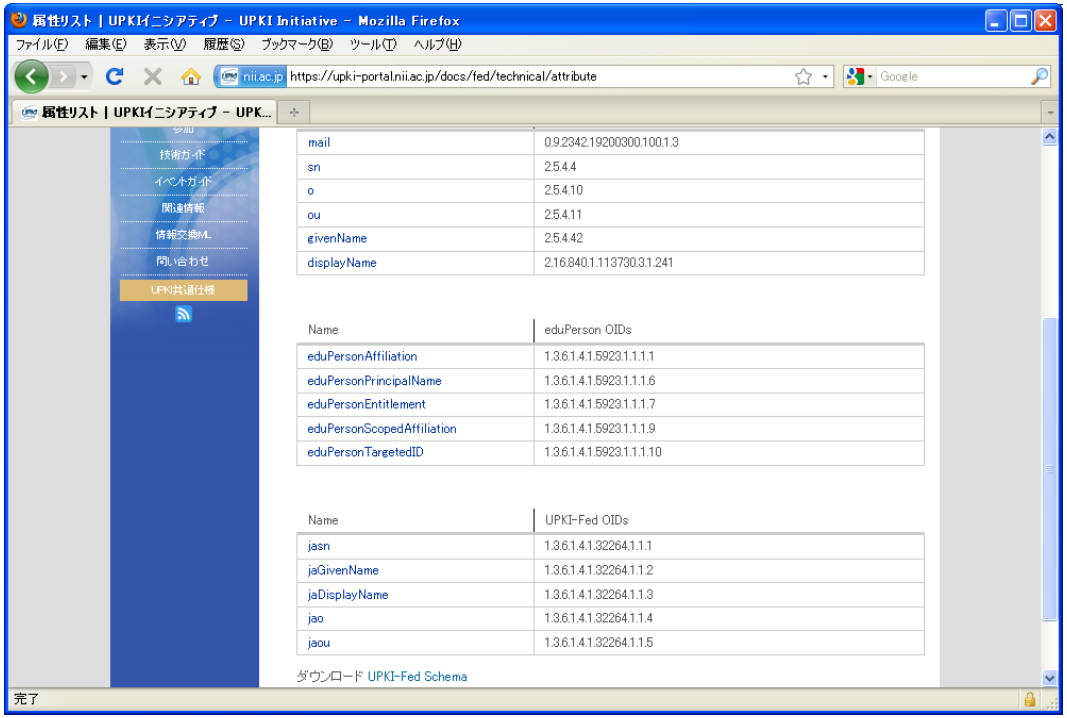
- とにかくIdPを構築しよう
- IdPの裏側にあるDBを準備しよう
- とはいえ，一からDBを準備するのは大変
- 学内の既存データを利用できないか？
  - 学内の合意が必要
  - 周囲に利用できるデータはないのか？
  - データのメンテナンスを誰が行うのか

1機関1IdPの構築が必要

IdPだけでなく，LDAPやActive Directory等のデータベースも必要

必要な準備（属性情報の確保）

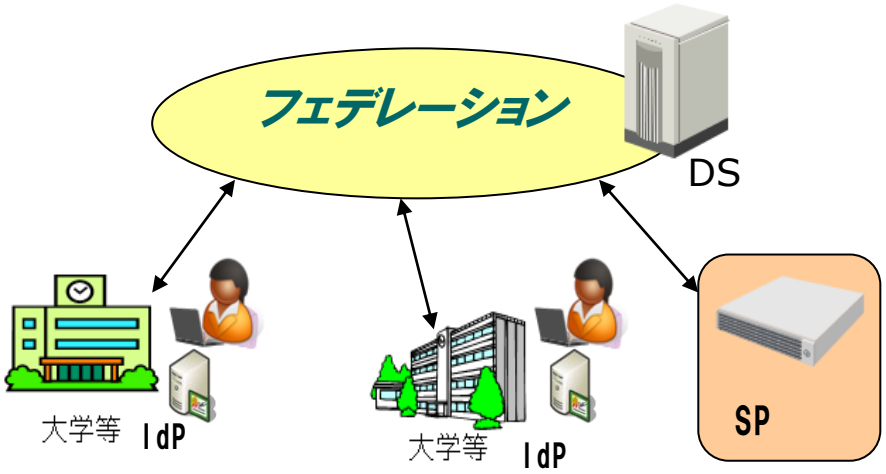
- LDAP, Active Directoryに，必要な項目（属性）があるか確認
- UPKI Fedでは，16の属性を使用
  https://upki-portal.nii.ac.jp/docs/fed/technical/attribute
- すべての項目を用意する必要はないが，SPが要求する項目を用意できない場合は，サービスを利用できない



属性の詳細は，試行運用を実施しながら検討する

IdPとSPを関連づけるもの

- 他の機関のIdPをSPが信用するためには，誰かがIdPの保証をする必要がある
- IdPもSPが信頼できるものでないと属性情報は渡せない
- この信頼の枠組みを「フェデレーション」という



フェデレーションの仕事

- 運用規程（ポリシー）の策定
- 参加機関の承認
- DSの運用
- IdPとSPが交換する属性情報の決定
- メタデータの交換

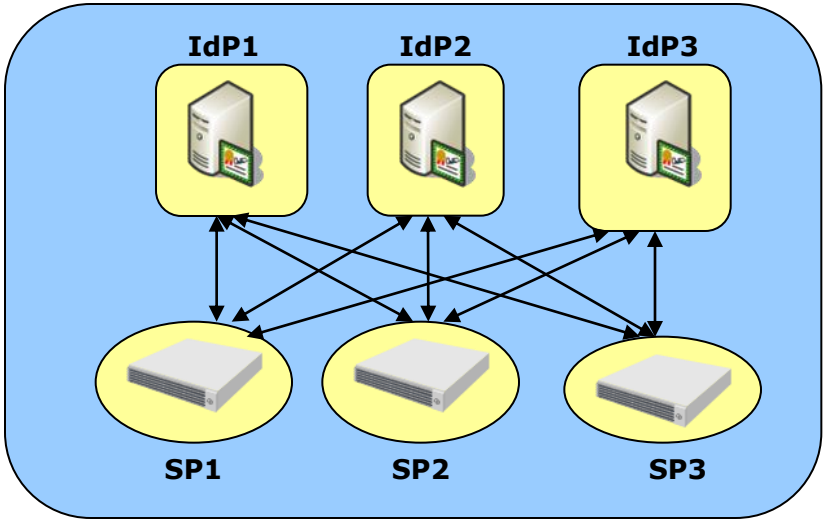
メタデータ（といっても検索はしない）

- フェデレーション内のSPとIdPが個別に信頼し，登録するのは大変
- そもそも信頼できる相手なのかの判断ができない
- フェデレーションが参加機関の情報をまとめたデータを作成
- XML形式で作成されたこのデータを「メタデータ」という
- メタデータは，フェデレーションが運用するサーバから配布される（SP, IdPともに自動ダウンロード）


```
<EntityDescriptor entityID="https://idp.nii.ac.jp/idp/shibboleth">
-
<IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol urn:mace:shibboleth:1.0
urn:oasis:names:tc:SAML:2.0:protocol">
-
<Extensions>
<shibmd:Scope regexp="false">nii.ac.jp</shibmd:Scope>
</Extensions>
-
<KeyDescriptor>
-
<ds:KeyInfo>
-
<ds:X509Data>
-
<ds:X509Certificate>

MIIFljCCBAqgAwIBAgIERcdlfzANBgkqhkiG9w0BAQUFADB3MQswCQYDVQQGEwJK
UDEOMAwGA1UEBxMHOWNhZGVtZTEqMCgGA1UEChMhTmF0aW9uYWwgSW5zdGl0dXRl
IG9mIEluZm9ybWF0aWNzMQ0wCwYDVQQLEwRVUEtJMRswGQYDVQQLExJOSUkgT3Bl
biBEb21haW4gQ0EwHhcNMDkwMTI4MDUwNzU0WhcNMTAwNjMwMTQ1OTU5WjCBizEL
MAkGA1UEBhMCSIAxEDA0BgNVBAcTB0FjYWRlbWUxKjAoBgNVBAoTIU5hdG1vbmFs
IEluc3RpdHV0ZSBvZiBJbmZvcm1hdGljczEmMCQGA1UECxMdSW5mb3JtYXRpb24g
VGVja G5vbG9neSBDZW50ZXIxFjAUBgNVBAMTDWlkcC5uaWkuYWMuanAwgZ8wD0YJ
```


メタデータの例



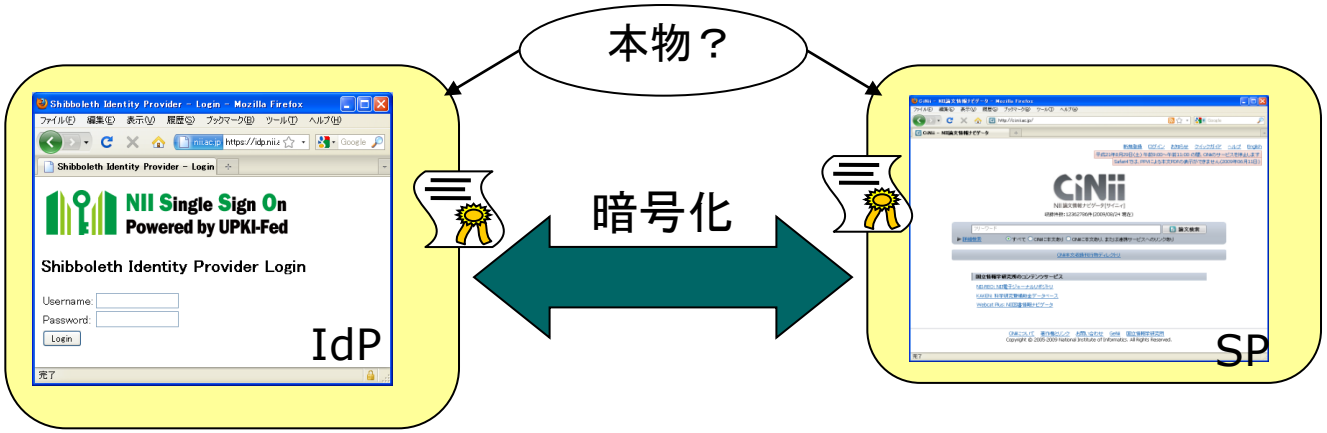
信頼関係の構築（3対3でも9通り）

メールの連絡を信頼して良いのか？

- 参加機関がIdPやSPを構築した場合，メタデータを作成して，フェデレーションに送付する
- この際，メールで送ることになるが，もしその情報が嘘だったら？
- 偽物のIdPやSPがフェデレーション内に構築されたら，フェデレーションそのものの信頼に関わる
- このため，メタデータを送る際に署名をし，受け取った側はその署名の検証を行い，正しいメタデータであることを確認する
- また，ダウンロードしたメタデータにも署名はされている

証明書の利用

- IdPとSP間の通信には，属性情報が流れます
- 平文でデータが流れるのは危険です
- また，IdP・SPが本物であるか確認する必要があります
- そのため，IdP・SPともにサーバ証明書を使用します
- サーバ証明書は，フェデレーションの定めた証明書を用います
- UPKIの「証明書プロジェクト」と「フェデレーション」がここで一つにつながります
- 証明書がなぜ安全なのか等は後ほど西村先生の講義で



ところでSPは何があるのか

- 電子ジャーナル
- データベース
- 無線LAN
- E-ラーニング
- グリッドコンピュータ

  - マイページの必要なSPは，IdPの情報とSPの情報の紐付けにより，Shibboleth化を行う

SPを充実させよう

- IdPだけあっても何も使えない
- やはりSPの充実は必要
- 商用は電子ジャーナルが先行している
- これは，必要な属性情報が少ないから
- 学内のみのサービスであれば，属性情報の利用も可能なはず
- サービスを考えよう

学内利用と学外利用の使い分け

- 属性情報を学外に出すことには，学内の承認が必要
- 属性を出すことには抵抗がある
- でも，大学名ぐらいなら何とか出せないか
- それ以外の属性は，学内サービスからスタートしてはどうか

今後の展開

- まずはフェデレーション「UPKI Fed」の試行運用を開始
- 電子ジャーナルを中心に，SPを拡大
- もちろん，CiNiiもSPとして参加
- 技術的検証を行うために，「テストフェデレーション」も準備
- サーバの準備ができたら，テストフェデレーションの参加を

実習の内容(1)

- IdPの構築
  - Shibbolethのインストールと基本設定
  - LDAPの構築
  - メタデータの作成・DSへの登録
  - メタデータの自動更新・検証
  - 属性送信の設定
- SPの構築
  - Shibbolethのインストールと基本設定
  - メタデータの作成・DSへの登録
  - 属性一覧の設定

実習の内容(2)

- IdP, SPの接続検証
- 属性送受信の確認
  - LDAP内のデータとIdP設定の調整
  - SP毎に異なる属性を送信することの確認
- メタデータ関連のテスト
  - 署名と署名検証
  - 自動ダウンロード

- 事前にTeraTerm等のエミュレータをインストールしておいてください

まとめ

- 今回のセミナーは，Shibbolethの技術だけのものではありません
- 運用するためには，学内の調整や部門間の連携が必要となります
- 技術的にも，証明書を使用して信頼しているとはいえ，人的なつながりに勝るものはありません
- そして，日本のフェデレーション構築の先導者となってください