平成25年度
国立情報学研究所
実務研修成果報告会

お茶の水女子大学
図書・情報チーム　兵藤徳和

平成25年12月6日(金)

研修の目的

- 「国立情報学研究所学術基盤推進部におけるOJTを通じて、学術情報流通基盤の構築に向けての企画・立案・実施等の手法と、対応する知識と技術を修得する。また、学術情報流通基盤の構築にかかる総合的かつ長期的視野を持つ。」（NII　実務研修Webページより）

- 今回のミッション「学認に関する知識・技術を習得してお茶大の学認に参加を目指す」

自己紹介

- お茶の水女子大学
  図書･情報チーム　情報基盤係に所属

- 大学卒業後民間企業に2年半
- お茶大採用後
  企画広報課　　5年
  図書･情報チーム　7年

お茶大の組織構成

- TOPに学長
- 学長の下に4人の副学長（総務、教育、国際・研究、学術情報）

- 学術情報担当の副学長が図書館長および情報基盤センター長を兼ねる

お茶大図書館について

- 図書館長（副学長・情報基盤センター長）
- └図書・情報チームリーダー
- ├総務係（図書の購入、庶務全般）
- ├企画・契約係（雑誌業務全般）
- ├資料・管理係（目録業務全般）
- ├情報サービス係（利用者サービス全般）
- └情報基盤係（事務PC、歴史資料全般）

お茶大情報基盤センターについて

- センター長（副学長・附属図書館長）
- └副センター長
- 　　├センター主任
- 　　├講師
- 　　├技術専門職員
- 　　├アソシエイトフェロー
- 　　└非常勤職員　.etc

お茶大の認証基盤の現状

- 全学統合認証基盤としてのLDAPは構築済み
- メールシステム、グループウェア、図書館システムはLDAPと連携
- 教務系システム（学生ポータル、シラバスシステム、Moodle等）はCAS認証でLDAP連携

お茶大の構成員数

- 学部生　2,000名
- 大学院生　1,000名　　合計　3,000名

- 教員　260名
- 附属教員　100名
- 事務職員　100名　＋　非常勤職員

- 合計で4000名程度

お茶大と学認第1期

- 2008年のシングルサインオン実証実験に参加

- IdPの構築まで進んだ

お茶大と学認第2期

- 情報基盤センターの技術専門職員が引継ぎ
- NIIのIdPホスティングサービスを利用させてもらい構築開始
- LDAPとの接続完了

お茶大と学認第3期

- 2013年4月、新しい課長が図書・情報チームに着任
- 情報基盤係職員がセミナー等に参加
- そして実務研修へ

研修内容その1

- 学内説明用の資料作成
- 学認とは何か、大学が学認に参加することのメリット、学認参加の要件、IdPの説明、運用体制について、必要なコスト、ロードマップ等を記載
- 新しい点として、構築にかかる参考コストを業者に依頼した。
- 作成した資料は、研修の成果報告として公開

中規模大学で想定した構築コスト

【想定する大学】
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、適切に属性情報を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

中規模大学で想定した構築コスト

サーバ構築費用

	A社	B社	C社
IdP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**

ハードウェア費用

	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**	

次年度保守

	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**

※参考コストです。
各大学の環境(LDAPの設定状況など)により見積り額は変わりますので、実際の金額については業者に見積もりを依頼ください。

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。

研修内容その2

- 情報処理技術セミナーの講師補助

- 情報処理技術セミナー平成25年度第2回
  25.10.21(月)～10.22(火)
- Shibboleth環境構築セミナー(高専向け)
  25.10.28(月)～10.29(火)

- 質問のあった事項等を学認技術Wikiに追加

研修内容その3

- お茶大のIdPを構築

- 方針として「図書館主導で、電子コンテンツのリモートアクセス環境改善を目標にスモールスタート」

サーバの用意　9/30

- 情報基盤センターに、学内キャンパスクラウド内にIdP用の仮想環境の用意を依頼

- 10/10　センターより、仮想マシンの用意が完了したこと、学認技術ガイドのVMwareイメージをインストールしたとの連絡

- IdPの構築開始

各種ソフトのインストール

- VMwareのソフトは古いので、学認技術ガイドにしたがって、最新版のソフトをインストール

- 設定を行い、動作を確認

テストフェデレーションへの参加 10/26

- 学認申請システムにてテストフェデレーションへ参加

- 動作を確認する。この時点では、大学のLDAPとは未接続

大学にて学認参加の承認

- 情報推進室会議(お茶大の全学情報委員会)にて了承　11/7
- 企画経営統括本部会議(役員レベルの定例会)にて了承 11/12
- 学内にて申請書の決裁文書作成　11/15
- 学認事務局に申請書提出　11/18

お茶大IdP運用体制

- 申請者(申請書に要公印) :附属図書館長
- 運用責任者 :附属図書館長
- 運用担当者:図書・情報チーム情報基盤係
- 審議委員会:情報推進室(既存の全学情報委員会)

※SPの追加等が発生した場合は、適宜、情報推進室にて審議する。

運用フェデレーションへの参加 11/20

- 運用フェデレーションへ参加が認められ、はれて学認参加となる

- 構築～学認参加まで約2ヶ月かかった

- IdPの構築は2週間程度かかったが、サーバ構築になれている人なら、もっと短縮できるだろう

IdP構築の際の問題点

- LDAPとの接続
- eduPersonAffiliationの属性
- 構成員以外のLDAP登録者の扱い

1. LDAPとの接続

- LDAPS（SSL接続）で接続するよう情報基盤センターから依頼
- LDAPだと接続できたものが、LDAPSだとエラーとなってしまう
- 中村先生にご助言いただいて解決

LDAPSでの接続エラーの原因

- 設定ファイルを、IPアドレスで記載していた

- LDAPのサーバ証明書内の記載ホスト名と合致しないため、エラーとなっていた

2. eduPersonAffiliationの値

- LDAPにeduPersonAffiliationにあたる値が存在しない

- LDAPのgidNumber（グループID）によるマッピングを行った

gidNumber	内容	ePA
1	管理者	faculty,member
2	教員	faculty,member
3	職員	staff,member
4	学生	student,member
5	単位互換等聴講生	値無し
6	研修生等	値無し
7	留学生	値無し
8	附属校生徒	値無し

attribute-resolver.xml

```
<!-- Attribute Definition for eduPersonAffiliation -->
   <resolver:AttributeDefinition
      id="eduPersonAffiliation“   xsi:type="Simple"
      xmlns="urn:mace:shibboleth:2.0:resolver:ad">
   <resolver:Dependency ref="mappedAffiliation" />

   <resolver:AttributeEncoder xsi:type="SAML2String“
         xmlns="urn:mace:shibboleth:2.0:attribute:encoder"
          name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
         friendlyName="eduPersonAffiliation" />
   </resolver:AttributeDefinition>

   <!-- mapping definition from gidNumber
                                  to eduPersonAffiliation -->
   <resolver:AttributeDefinition id="mappedAffiliation“
     xsi:type="Mapped"
     xmlns ="urn:mace:shibboleth:2.0:resolver:ad"
     sourceAttributeID="gidNumber">

    <resolver:Dependency ref="myLDAP" />
```

```
     <ValueMap>
      <ReturnValue>faculty</ReturnValue>
      <SourceValue>1</SourceValue>
      <SourceValue>2</SourceValue>
     </ValueMap>

     <ValueMap>
      <ReturnValue>staff</ReturnValue>
      <SourceValue>3</SourceValue>
     </ValueMap>

     <ValueMap>
      <ReturnValue>student</ReturnValue>
      <SourceValue>4</SourceValue>
     </ValueMap>

     <ValueMap>
      <ReturnValue>member</ReturnValue>
      <SourceValue>1</SourceValue>
      <SourceValue>2</SourceValue>
      <SourceValue>3</SourceValue>
      <SourceValue>4</SourceValue>
     </ValueMap>
    </resolver:AttributeDefinition>
```

構成員以外のLDAP登録者の扱い

- お茶大LDAPには大学の構成員以外の登録者がいる
- 例えば、生協職員、学科のOG、大学関係のNPO法人職員
- 学認では、「自組織に所属しない利用者の属性を保証すべきではない。」としているので利用不可としたい

拒否する方法

- 学認技術ガイドで公開されているFilter Per SPというプラグインを用いて拒否する

- ただし、Filter Per SPでは属性情報を必要としないSPは拒否設定できない

- 西村先生に助言いただき、エラーの場合のみに属性値が設定される属性を生成

gidNumber	内容	ePA	kyohi_flag
1	管理者	faculty,member	値無し
2	教員	faculty,member	値無し
3	職員	staff,member	値無し
4	学生	student,member	値無し
5	単位互換等聴講生	値無し	flag_on
6	研修生等	値無し	flag_on
7	留学生	値無し	flag_on
8	附属校生徒	値無し	flag_on

attribute-filter.xml

```
<!--  Release the transient ID to anyone -->
  <AttributeFilterPolicy id="PolicyforAnyone">
    <PolicyRequirementRule xsi:type="basic:ANY" />

    <AttributeRule attributeID="transientId">
      <PermitValueRule xsi:type="basic:ANY" />
    </AttributeRule>

    <AttributeRule attributeID="kyohi_flag">
      <PermitValueRule xsi:type="basic:ANY" />
    </AttributeRule>

  </AttributeFilterPolicy>
```

Filter Per SpのSampleFilterPerSP.javaを修正

```
        // コンフィグの設定と比較
        System.out.println("SampleFilterPerSP spEntityId = " + spEntityId);
        if (allow_config.containsKey(spEntityId)) {
            Map filterpersp = allow_config.get(spEntityId);
            for (BaseAttribute baseattrval : attributes.values()) {
                if (filterpersp.containsKey(baseattrval.getId())) {
                    Set val = (Set)filterpersp.get(baseattrval.getId());
                    for (Object obj: baseattrval.getValues()) {
                        if (obj != null && !obj.toString().trim().equals("")) {

                            String attrval = obj.toString();
                            if (val.contains(attrval)) {
                                //for debug
                                System.out.println("SampleFilterPerSP checked " + baseattrval.getId() + "=" + attrval);
                                filterChain.doFilter(servletRequest, servletResponse);
                                return;
                            }
                        }
                    }
                }
            }
        }
        //for debug
        System.out.println("SampleFilterPerSP don't match any attributes.");
        for (BaseAttribute baseattrval : attributes.values()) {
            for (Object obj: baseattrval.getValues()) {
                if (obj != null && !obj.toString().trim().equals("")) {
                    String attrval = obj.toString();
                    System.out.println("SampleFilterPerSP " + baseattrval.getId() + "=" + attrval);
                    if (attrval.equals("flag_on")) {
                        System.out.println("SampleFilterPerSP match deny user : " + spEntityId +" " + userName);
                        doError(servletRequest, servletResponse, spEntityId, userName);
                        return;
                    }
                }
            }
        }

        doError(servletRequest, servletResponse, spEntityId, userName);
        return;
    }

    filterChain.doFilter(servletRequest, servletResponse);
}
```

拒否する方法2

- login.configのLDAPフィルタを設定し拒否する

```
edu.vt.middleware.ldap.jaas.LdapLoginModule required
     ldapUrl="ldaps://ldapxx.cc.ocha.ac.jp"
     baseDn="ou=xxxxx,dc=xx,dc=ocha,dc=ac,dc=jp"
     ssl="true"
     userFilter="uid={0}"
     subtreeSearch="true"

     authorizationFilter="(|(gidNumber=1)(gidNumber=2)(gidNumber=3)(gidNumber=4))"
     ;
```

- 設定としては、こちらの方が簡単なので、この方法で拒否することにする

IdPの動作確認　11/25

- 拒否設定も出来たので、IdPの設定をテストフェデレーションから運用フェデレーションへ変更

- Fshare、CiNiiの利用登録。動作確認。

- 12/2 Elsevier、EBSCO、Springerに学認による接続を依頼。当日～翌日には設定完了の連絡あり。

その他、追加で設定した事

- uApprove.jp(ユーザ同意取得システム)

  https://meatwiki.nii.ac.jp/confluence/x/ZwLO

- attribute-filterの自動生成機能

  https://meatwiki.nii.ac.jp/confluence/x/A4Lf

今後の予定

- 図書館および情報基盤センターで動作確認
- 学認を使った電子ジャーナル等の利用案内作成
- SPへの学認接続申請
- 学内広報を年明けごろ？
- eduPersonAffiliationの値をマッピングではなく、直接LDAPから取得できるよう調整中

課題事項

- IdP運用内規の制定
- サーバの冗長化
- LoA1の取得
- Eduroam-Shibの利用

研修内容その4

- 各種イベントへの参加、委員会へ陪席

- 学術認証運営委員会
- UPKIサーバ証明書打合せ
- 文部科学省学術情報委員会
- 図書館総合展
- SINET取材
- SINET&学認説明会　　等々

- 謝辞

- ご清聴ありがとうございました。

お茶の水女子大学
図書・情報チーム　兵藤