Shibboleth IdPの構築と実証実験の進捗状況

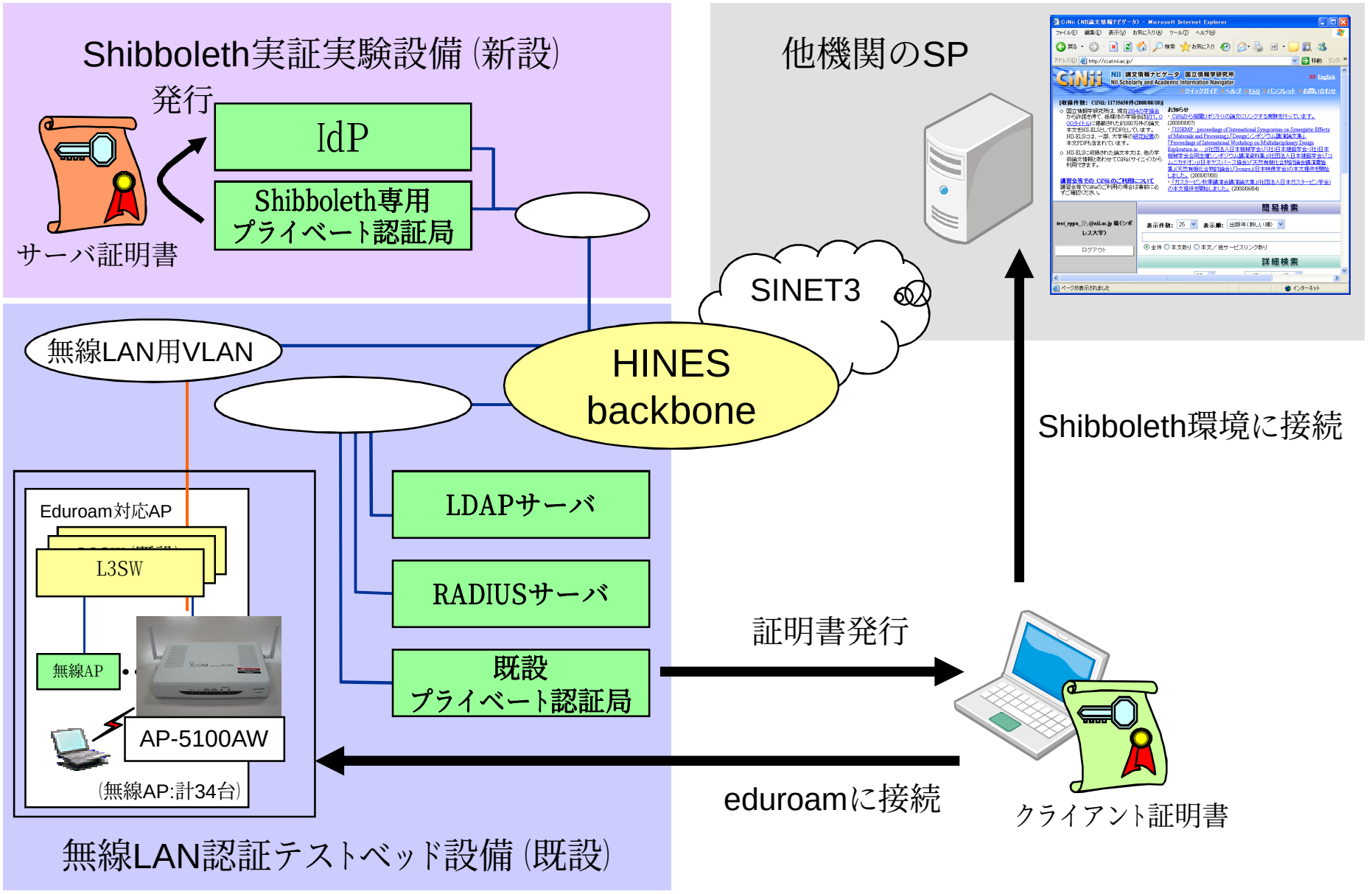
山本 哲寛, 髙井 昌彰
北海道大学情報基盤センター

2008.11.10

北海道大学における実証実験の内容

- IdPの構築
  - 廉価な機器による実装（Let’s note CF-W7）
  - ID/Password認証連携の実証試験
  - PKI認証連携の実証試験
- プライベート認証局の利用
  - 専用のプライベートCAを新設し、IdPサーバ証明書を発行
  - クライアント証明書は既設のプライベートCAから発行
- 既設の無線LAN認証テストベッドの有効活用
  - 新規に構築したサーバは1台（IdP+CA）
  - eduroam用クライアント証明書を流用（新規発行なし）
  - 既設LDAPサーバを利用

Shibboleth実証実験のためのテストベッド全体構成



実証実験に使用した証明書

	Shibboleth専用プライベートCA発行		既設プライベートCA発行	
	CA証明書	サーバ証明書	CA証明書	クライアント証明書
Issuer	C=JP ST=Hokkaido L=Sapporo O=Hokkaido University OU=Information Initiative Center CN=Hokkaido University Private CA for Shibboleth	C=JP ST=Hokkaido L=Sapporo O=Hokkaido University OU=Information Initiative Center CN=Hokkaido University Private CA for Shibboleth	C=JP ST=Hokkaido L=Sapporo O=Hokkaido University CN=Hokkaido University Test CA	C=JP ST=Hokkaido L=Sapporo O=Hokkaido University CN=Hokkaido University Test CA
Subject	C=JP ST=Hokkaido L=Sapporo O=Hokkaido University OU=Information Initiative Center CN=Hokkaido University Private CA for Shibboleth	C=JP O=Hokkaido University OU=Information Initiative Center L=Academe CN=idp01.iic.hokudai.ac.jp	Subject: C=JP ST=Hokkaido L=Sapporo O=Hokkaido University CN=Hokkaido University Test CA	C=JP O=Pentio OU=network OU=iic OU=hokudai OU=Certificate by PentioPKI PrivateCA CN=et-yamamoto emailAddress=et-yamamoto@iic.hokudai.ac.jp

IdP構築時に困ったこと

- 初期構築時
  - CiNiiにはログインできても、ploneにログインできない
    - 「eduPersonPrincipalName」が渡っていなかった

原因：　attribute-filter.xml内のAttributeRuleエレメント：attributeID属性と
attribute-resolver.xml内のAttributeDefinitionのid属性の値について
大文字・小文字の区別を間違えて記述していた

- 証明書認証移行時
  - 既設LDAPサーバをできるだけいじくりたくない

～「 eduPersonPrincipalName 」を追加したくない～

解決策：LDAPに格納されていた情報「sn」を、「eduPersonPrincipalName」に格納

Attribute-resolver.xmlの変更点

変更前（395行目あたり）

```
<resolver:AttributeDefinition id="principalName" xsi:type="Scoped"
    xmlns="urn:mace:shibboleth:2.0:resolver:ad"
      scope="iic.hokudai.ac.jp"
    sourceAttributeID="eduPersonPrincipalName">
      <resolver:Dependency ref="remoteUser" />
```

変更後（395行目あたり）

```
<resolver:AttributeDefinition id="principalName" xsi:type="Scoped"
    xmlns="urn:mace:shibboleth:2.0:resolver:ad"
      scope="iic.hokudai.ac.jp" sourceAttributeID="sn">
      <resolver:Dependency ref="remoteUser" />
```

まとめと今後の課題

- ID/Password認証連携及びPKI認証連携に成功した
  - ID/Password認証連携（H20.9.5）、PKI認証連携（H20.9.26）
- Shibboleth（IdP）自体の導入は、さほど難しくない
  - NII提供のマニュアル＋MailによるQ&Aでほぼ解決
- 特に高性能なサーバを必要としない
  - 手元にあったNote PCで十分に機能

- 主に附属図書館利用者に対しテストIDを配布（未定）
  - 利用者に使用感などのアンケート実施
- 他機関との時刻同期の問題
  - 時刻同期不備のため、NII提供のploneに接続できなくなることが多々あった
- 実運用に向けた方針の検討
  - 既存システム（LDAP）との親和性
    - 大学職員ID管理とShibboleth連携におけるID管理
      （既設LDAP内の情報とeduPersonPrincipalNameの関係等）