# Shibboleth 認証基盤構築と学術認証フェデレーションへの参加 : 今後のe リソースサービス基盤にむけて

伊東, 栄典
九州大学情報基盤研究開発センター

片岡, 真
九州大学情報システム部情報基盤グループ

牧瀬, ゆかり
九州大学附属図書館ｅリソースサービス室

https://doi.org/10.15017/18319

出版情報：九州大学附属図書館研究開発室年報. 2009/2010, pp.11-15, 2010-03-31. 九州大学附属図書館
バージョン：
権利関係：

論文

# Shibboleth 認証基盤構築と学術認証フェデレーションへの参加
## － 今後の e リソースサービス基盤にむけて －

伊東 栄典[†]　　片岡　真[‡]　　牧瀬　ゆかり[§]

**<抄録>**

Web 上で提供される電子ジャーナル等の e リソースサイトでは，契約した機関の構成員のみが利用できるようにアクセス制限を行っている。組織間の分散電子認証基盤として Shibboleth システムがあり，その利用が進んでいる。さらには Shibboleth を共通の認証基盤として用いる認証フェデレーションが世界で広がっており，日本国内でも学術認証フェデレーション「Gakunin」が設立されている。我々は，これまで九州大学における Shibboleth の基盤開発を行ってきたが，この度情報統括本部と附属図書館の協力によって，Shibboleth IdP の立ち上げおよび図書館マイアカウントサービスの Shibboleth 対応を行った。本稿では，特に Gakunin フェデレーションに参加する場合の，Shibboleth IdP における属性問題についての検討と解決案を述べる。また，九州大学における Shibboleth 導入と評価について述べる。

**<キーワード>**　e リソース，電子認証，Shibboleth，SSO，認証フェデレーション，Gakunin

# Shibboleth IdP and the National Authentication Federation
## － Toward Next Generation Infrastructure for e-Resource Services －

ITO Eisuke　　KATAOKA Shin　　MAKISE Yukari

### 1. はじめに

図書館が提供する電子ジャーナルを始めとする e リソースの多くは，各機関と出版社等との契約に基づく範囲内で利用が認められており，その認証は，これまで当該機関が持つ IP アドレスによる方法が一般的であった。しかしながら，無線 LAN の発達や iPhone などモバイルデバイスの普及など，Web 上のサービスへのアクセス多様化に伴って，これら e リソースについても，自宅や出張先などから，サービス毎に別々の認証を経ることなく，簡便に利用できるような環境整備が求められている。

そこで注目を集めているのが，Shibboleth[1]である。Shibboleth は，SAML[2]プロトコルに準拠した SSO（Single Sign-On）の仕組みであり，近年これを利用した学術機関の認証フェデレーションが，全国規模または世界規模で広がりを見せている。

我々は，これまで組織間認証連携の研究[3,4,5]と，九州大学における SSO 認証基盤の整備を行ってきた。本稿では，機関認証連携である Shibboleth と，それを利用したフェデレーションについて説明する。また国内のフェデレーションの属性に関する問題とその解決手法の提案を行い，九州大学における Shibboleth IdP の実装・評価・今後の課題についても述べる。

### 2. Shibboleth

米国の Internet2 プロジェクトでは，Shibboleth と名付けられた SSO，ID 連携による利用者認証・認可の基盤の提案および実装を行っている[1]。Shibboleth における認証・認可情報の記述形式は SAML 形式[2]である。

Shibboleth では機関間での認証連携のために，WAYF（Where Are You From ?）または DS (Discovery Service) と名づけられた仕組みを導入している。WAYF を用いることによって，ユーザがどの組織に所属しているか（所属組織の IdP）を特定できる。図 1 に Shibboleth の概念図を示す。

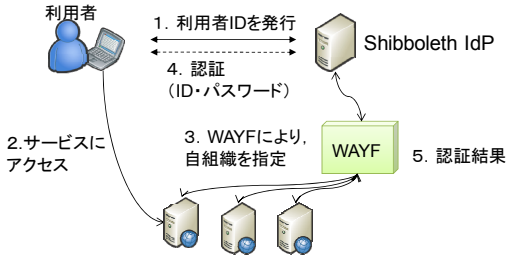



図 1　Shibboleth 概念図

[†] いとう えいすけ　　九州大学情報基盤研究開発センター　E-mail: ito.eisuke.523@m.kyushu-u.ac.jp
[‡] かたおか しん　九州大学情報システム部情報基盤グループ　E-mail: shkata@lib.kyushu-u.ac.jp
[§] まきせ ゆかり　九州大学附属図書館 e リソースサービス室　E-mail: ymakise@lib.kyushu-u.ac.jp

## 3. 学術認証フェデレーション （Gakunin）

複数機関が共通ポリシーのもとで相互運用する認証フェデレーションが世界各国で構築されている。具体的な認証フェデレーションとして，米国の InCommon や英国の UK Federation などがある。日本では国立情報学研究所が中心となり，「学術認証フェデレーション（愛称：Gakunin）」を発足させている。Gakunin には九州大学を含む多くの大学が参画している。他国のフェデレーションと同様に，日本の Gakunin でも認証連携に Shibboleth を用いている。サービスを受ける機関は，利用者認証機能を提供する Shibboleth IdP（Identity Provider）を構築し，Gakunin などのフェデレーションへ参加する必要がある。またサービス提供者になるには，Shibboleth SP（Service Provider）を構築するとともに，各フェデレーションとの連携設定を行わなければならない。

認証フェデレーションは，認証を提供しサービスを受ける機関（IdP），サービス提供者（SP），および個々の利用者それぞれにメリットがある。利用者は自分の属する機関で認証を行うことができ，個人情報の露出機会を大幅に削減することができる。SP としても ID 管理や，利用者情報の管理から開放され，IdP 側は大学などの情報セキュリティ準拠，コンプライアンスを順守することができる。

## 4. 属性交換の問題

Gakunin に参加する大学が IdP を構築する場合，属性交換に関する問題が二つ有る。一つは，属性の不足または不一致の問題である。二つ目は SP への属性提供制御である。

### 4.1. 属性の不足または不一致

フェデレーションは，共通ポリシーに基づく相互運用を行うものであるため，利用者認証に付随する利用者属性も共通化している。日本のフェデレーションである Gakunin でも参加機関が共通に使う属性を指定しており，それは eduPerson スキーマを日本向けに拡張したものになっている。Gakunin に参加する大学が IdP を構築する場合，Gakunin の指定属性を提供しなくてはならない。

IdP 構築以前に各大学が独自に LDAP サーバ等を用いた認証基盤を整備していた場合，その認証基盤が持つ利用者情報の属性は，Gakunin 指定の属性と異なる場合が多い。九州大学でも IdP 構築以前から認証基盤を整備していたため，利用者の情報は，Gakunin が指定するものとは異なっていた。Gakunin 準拠の IdP を構築するには，大学独自の認証基盤システムを変更するか，何らかの属性変換システムが必要となる。

### 4.2. 属性提供制御

個人情報保護法では，個人を特定できる情報を機関外へ提供することを制限している。学内の SP に利用者の個人情報を提供しても法律上の問題は無いものの，外部機関の SP への氏名・所属機関・利用者 ID 等の属性情報提供は IdP 側で制御する必要がある。基本的に，外部機関の SP には必要以上の利用者情報を提供しないようにする。外部機関の SP で，個人を特定する属性情報が必要となる場合，サービス提供者側と個人情報保護に関する契約や，各利用者に同意を得るといった仕組みが必要となる。

## 5. IdP 構築における属性制御の検討

### 5.1. Gakunin 準拠 IdP 構築のための属性加工

Gakunin 準拠の Shibboleth IdP を構築するためには，大学が持つ利用者データベースまたは利用者認証システムが提供する属性と，Gakunin 指定属性との適切なマッチングが必要となる。その実現について三つの手法を検討した。

一つ目の手法は，利用者データベースのスキーマ変更である。既存の利用者データベースが持つ属性情報に加え，Gakunin 指定の属性および属性値を追加する方法である。業者に利用者データベースや認証基盤の構築・管理を外注している場合，Shibboleth 対応のための金銭的コストが発生する。また，Gakunin 指定の属性を，既存の認証基盤側で以前から使っている場合，その属性を参照するサービス側での変更も必要となる。

二つ目の手法は，IdP 側での属性加工である。Shibboleth IdP には，attribute resolver と名付けられた機能があり，属性値の静的追加や外部スクリプト呼び出しによる動的追加が可能である。既存システムの変更や新たなサーバの管理コストは発生せず，他の手法と比べコストを抑えることができる。ただし，attribute resolver の設定ファイルは XACML（eXtensible Access Control Markup Language）で書かれているため，少し煩雑な設定記述を理解する必要がある。

三つ目の手法は利用者データベース（または LDAP 認証サーバ）と，IdP との間に，属性変換装置を入れる方法である。利用者データベースが LDAP サーバで提供されている場合，IdP と利用者認証 LDAP サーバの間に OpenLDAP サーバを置くと，OpenLDAP の LDAP proxy 機能と，属性加工モジュールを利用することで，属性変換を実現できる。この方法の場合，既存の利用者データベースに変更を加える必要はない。しかし，属性変換装置の構築と維持管理の作業が追加で発生する。

また, 言うまでもないが, もともと認証基盤側にデータが格納されていない属性は，上記三手法により属性（スキーマ）を設定しても，値を生成できない場合がある。例えば，メールアドレスの情報を認証基盤が保持していない場合は，mail 属性にアドレスを格納することは困難である。表１に３つの手法の比較をまとめる。

表１ 属性加工手法の比較

| | スキーマ変更 | IdP 属性加工 | 属性変換 |
|---|---|---|---|
| 利用者データベース | スキーマ変更 | 変更なし | 変更なし |
| IdP | 変更なし | 属性の追加 | 属性変換用のサーバ追加 |
| 利点 | 追加サーバ不要。設定できてしまえば運用が楽 | 追加サーバ不要 | 設定が比較的簡単。利用者データベースの変更不要 |
| 問題点 | 属性管理システムの変更コスト | 設定が比較的煩雑 | サーバ増による作業負担増 |

### 5.2. SP への属性提供制御

必要以上に外部 SP に属性値を提供しないために属性提供判断方法として二つの手法を検討した。

一つ目の手法は SP 毎の属性提供制御設定を行うことである。Shibboleth IdP では，attribute filter 設定を用いることで，SP 毎の属性提供制御が可能である。この方法は，XACML による制御であるため記述が煩雑であり，また SP 数に応じて設定の煩雑さが増大する。

二つ目の手法は複数 IdP の構築である。例えば，機関内 SP 用の IdP と, 外部機関の SP のための IdP との，２台の IdP を構築し, 外部機関 SP 向けの IdP には必要最低限の属性しか提供しないように設定し, 内部の SP には全属性を提供するように設定する[6]。この手法の場合，内部 SP と外部 SP との間での SSO は実現できない。表２に，属性提供制御の手法をまとめる。

表２ 属性提供制御

| | SP 毎の属性提供制御設定 | 複数 IdP の構築（内部向け IdP と外部向け IdP） |
|---|---|---|
| IdP | 変更なし | 新たなサーバ構築が必要 |
| SP | 変更なし | 変更なし |
| 利用者 | 変更なし | SSO ができない（認証が２回以上になる）場合がある |
| 利点 | SSO が実現可能 | 設定が比較的簡単 |
| 問題点 | SP 毎に属性提供制御の設定を記述する必要がある | IdP サーバが増えることで，管理の手間が増える |

## 6. 九州大学試行 Shibboleth IdP の構築

九州大学では 2007 年 9 月から, LDAP 認証サーバを稼働している。LDAP 認証サーバは，機関内利用者の情報を管理しており，その属性情報を用いて利用者に複数のサービス提供を行っている。この LDAP 認証サーバと連携させることで，Shibboleth IdP を実現させることとした。

### 6.1. 試作システムの構造

Shibboleth IdP の構築にあたり，Gakunin 準拠 IdP 構築のための属性加工には，表１の三つ目の手法，属性変換を用いた。これは LDAP 認証サーバの変更には金銭的コストがかかるため変更を加えず，既存のサービスは変更しない仕様にするためである。

SP への属性提供制御については，表２の SP 毎の属性提供制御設定を用いた。これは，初期の状態では対象とする SP が少ないため，SP への提供属性制御の設定が大変ではないためである。

全体の構成を図２に示す。Shibboleth IdP の環境を表３に，属性加工のための属性変換サーバ（LDAP proxy）の環境を表４に表す。

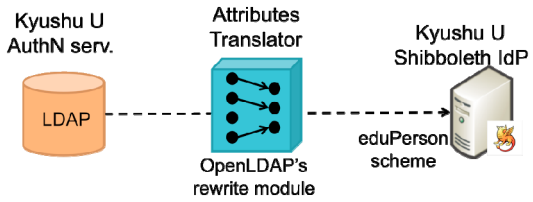



図２ 試作 Shibboleth IdP の構成図

表３ Shibboleth IdP

| 種類 | ソフト名 |
|---|---|
| IdP | Shibboleth IdP 2.0.0 |
| OS | CentOS 5.3 |
| Web | Apache 2.2.3 |
| Web | Tomcat 6.0.18 |

表４ 属性変換サーバ（LDAP proxy）

| 種類 | ソフト名 |
|---|---|
| OS | FreeBSD 7.1 |
| LDAP | OpenLDAP 2.3.43 |

### 6.2. 稼働の状況

2009 年 12 月から，九州大学附属図書館のマイアカウントサービスである「きゅうと MyLibrary」が Shibboleth SP として提供されている。この SP の認証は上記の環境で構築された試作 Shibboleth IdP を利用している。きゅうと MyLibrary にアクセスすると図３のように Shibboleth 認証画面となり，認証が成功する

と図４のようにログイン後の画面に遷移する。


図３ Shibboleth 認証画面


図４ きゅうと MyLibrary ログイン画面

### 6.3. 試作システムの性能評価

Shibboleth 認証可能で，IdP から SP への属性提供もできており期待した動作を確認した。その後，試作した Shibboleth IdP について，同時トランザクション数（認証処理の数）について調査した。

図５にその結果を示す。認証要求が一人の場合認証処理にかかる時間は 0.7 秒であるが，一度に 10 人アクセスした場合，認証処理にかかる時間は最大 15 秒であった。現在のサーバ能力では同時に５人以上の認証要求が来ると，処理が遅くなる。ただし，処理が終わらないわけではなく，先に述べたように，同時に 10 人からの認証要求が来ても，最大 15 秒待てば認証処理は終了する。

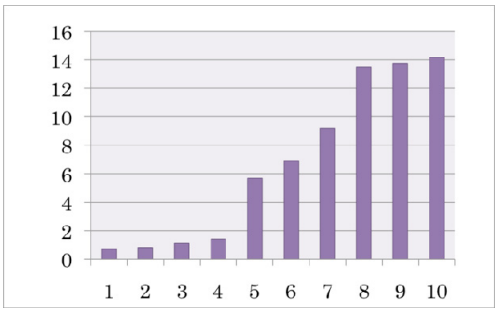
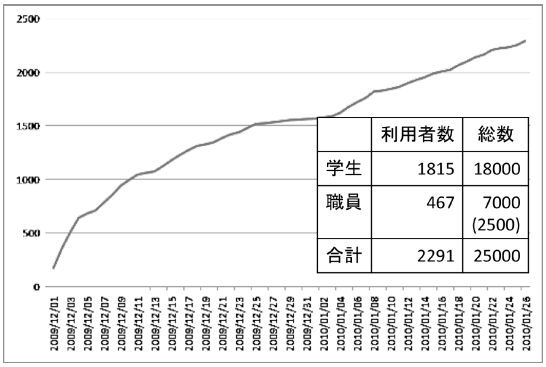



図５ 同時認証トランザクション数と最長ターンアラウンド時間（秒）

５人以上になると急に処理が遅くなる理由は，メモリが 256MB しかないことに問題があると考えられる。大規模なアクセスが想定されるサービスに対応するためにはより性能の高いサーバで Shibboleth IdP を構築する必要がある。

## 7. 試行 Shibboleth IdP の運用状況

2009 年 12 月 1 日，九州大学の Shibboleth IdP を九州大学情報統括本部の試行サービスとして開始した。ここでは 2009 年 12 月 1 日ー2010 年 1 月 26 日までの利用状況を報告する。




| | 利用者数 | 総数 |
|---|---|---|
| 学生 | 1815 | 18000 |
| 職員 | 467 | 7000 (2500) |
| 合計 | 2291 | 25000 |

図６ 利用者数（累計）

図６に示すように，2010 年 1 月 26 日までの約２ヶ月で，2,291 名の利用者が Shibboleth IdP 経由できゅうと MyLibrary へログインした。学生・院生が 1,815 名，教員を含む職員が 467 名である。大学全体の 10%の人数が利用していることになる。

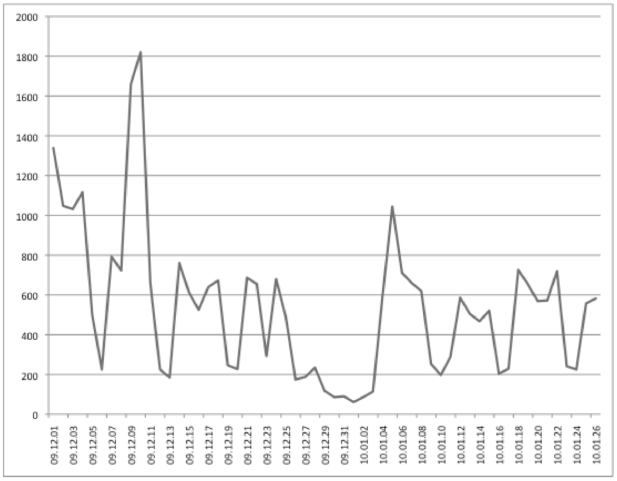



図７ 一日毎の認証数（利用者数）推移

図７には，一日毎の認証数（利用者数）推移を示している。土日には利用者が減り，また年末年始の休みにも利用者数が少ないことがわかる。

## 8. 本運用 Shibboleth IdP の構築

今後の SP 増加と同時利用者数の増加を考える場合，試行 Shibboleth IdP には二つの問題がある。

一つ目は処理性能および可用性の問題である。試行 Shibboleth IdP では低い性能のサーバを用いて実験的に構築しているため，１秒間の同時利用者数が４人までしか耐えられない。また，IdP サーバが１台しかないため，サーバ故障時に対応できない。そこで，処理性能と可用性を向上するため，同時利用者数が多くなっても問題がない程度の高性能 PC サーバを２台購入し，それぞれに IdP をインストールした。

二つ目の問題は，Gakunin 指定属性の不完全さである。電子ジャーナルサイトなどの商用サービスへ認証情報を提供するには，きちんと eduPerson スキーマを満たす必要がある。試行 Shibboleth IdP で使った属性加工では，おおまかな情報は提供できるものの，将来を考えると十分とは言えない。そこで, 九州大学の LDAP 認証サーバの属性拡張を行った。同時に，LDAP サーバにデータを挿入する利用者情報管理サーバの機能拡張も行った。新しい LDAP サーバには eduPerson スキーマも最初から入れており，また eduPerson が指定する各属性の値も可能な限り入れるようにしている。これを用いることで, 十分な情報を持つ Shibboleth IdP を構築可能である。

これらの本運用 Shibboleth IdP サーバは，2010 年度の早い時期に稼働する予定である。

## 9. おわりに

本稿では，情報サービスにおける利用者認証について，Web 情報サービスにおける SSO 技術 Shibboleth を説明し，また Shibboleth を用いた日本国内フェデレーションである Gakunin について説明した。次に，Gakunin 準拠 IdP 構築のための属性加工と，内外の SP への属性提供制御について検討した。最後に，九州大学で構築した試作 Shibboleth IdP について, 構成と運用状況を報告した。

今後，Gakunin に正式参加し，外部の電子ジャーナルサイトや，Refworks などの論文リスト管理サービスを連携していきたい。同時に，大人数利用者時における処理速度の計測やログの分析を行い，大規模利用者時でも安定的に運用できるように処理の分散化などを行なっていきたい。また，外部 SP への属性情報提供についても，文献[7]で示すような，利用者本人に確認を取る仕組みを導入するなど，柔軟な対応をしていきたい。

## 参考文献


[1] The Shibboleth project, http://shibboleth2.edu/.

[2] John Kemp, “Security Assertion Markup Language (SAML) ”, Mar.15, 2005,

[3] 阿部英司，伊東栄典，笠原義晃，中國真教, “認証つきサービスにおける組織間連携のための PKI と OpenID の融合”, IOT-2-2008, pp.17-22, Jul. 2008.

[4] 阿部英司, 伊東栄典, 笠原義晃, “認証フェデレーションにおける IdP の属性制御”, 電子情報通信学会 2010 年総合大会講演論文集, BS-7-7 (pp.S 133-134), March, 2010.

[5] 伊東栄典, “九州大学の取り組み”, UPKI シンポジウム 2010, パネルディスカッション, Mar. 12, 2010.

[6] 金西計英, 松浦健二, 中川真宏, 矢野米雄: 大学間 Web サービス連携における間接的な認可の制御について,平成 21 年度情報教育研究集会 D1-5, Nov.14, 2009.

[7] Tananun Orawiwattanakul, Kazutsuna Yamaji, Motonori Nakamura, Toshiyuki Kataoka, Noboru Sonehara, “User Level Export Control of Personal Information in a Federated SSO Environment Using Shibboleth”, 電子情報通信学会 2010 年総合大会講演論文集, BS-7-3, March, 2010.