# シボレスシステムを用いた属性連携基盤の開発

山地一禎[1]，片岡俊幸[1]，中村素典[1]，曽根原登[2]

1 国立情報学研究所　学術ネットワーク研究開発センター

2 国立情報学研究所　情報社会相関研究系

**概要**

現在，国立情報学研究では，シボレスシステムを用いた学術認証フェデレーションの構築を進めている．フェデレーションでは，大学や研究機関で運用されるIDプロバイダーを利用して，ウェブサービスへのシングルサインオンが実現される．サービス側では，IDプロバイダーから送信される属性に応じて，アクセスレベルの認可判断が可能になる．しかしながら，大学等の機関が送信できるユーザの属性情報は限られている．ユーザがよりリッチなサービスを受けるためには，属性を修飾するためのシステム間連携が重要な鍵となる．本研究では，そうした属性プロバイダーシステムの開発と利用モデルの構築を行った．

**キーワード**

シボレス，フェデレーション，認証，認可，属性，IDプロバイダー，SAML

# Development of Attribute Aggregator System works on Shibboleth based Access Management Federation

Kazutsuna Yamaji[1], Toshiyuki Kataoka[1], Motonori Nakamura[1], Noboru Sonehara[2]

1 Research and Development Center for Academic Networks, National Institute of Informatics

2 Information and Society Research Division, National Institute of Informatics

**Abstract**

UPKI federation is deploying federated identify in Japan by means of the SAML 2.0 standard mainly utilizing Shibboleth middleware. In the federation, single sign on to web service is realized through the authentication by institutional ID providers. Access control of the service is enabled by referring to attributes provided by ID provider. However, each institution provides the attribute just they ensured, suggesting that users can obtain higher level service if the attributes are enriched by other appropriate organization. This study developed an attribute aggregator system and deployed it to the relationship between university IdPs and academic society IdP.

**Keywords**

Shibboleth, Federation, Authentication, Authorization, Attribute, ID Provider, SAML

## 1. はじめに

電子ジャーナルや学術データベースなど，現在では研究を進める過程において，インターネット上のコンテンツやサービスは欠くことのできない存在となっている．これらのサービスの多くが，有料あるいは限られたコミュニティという条件で提供されており，その結果，コンテンツへのアクセスには認証が必要となる．所属機関がサイトライセンス契約を結んでいる電子ジャーナル等は，アクセス元の IP アドレスにより認証（IP 認証）されるため，エンドユーザが認証のための特別なプロセスを意識することはない．この場合でも，文献管理機能やアラート機能など，個人レベルでのカスタマイズが可能なサービスの利用には，個人 ID の取得とそれを用いた認証（ID 認証）が必要となる．また，IP 認証が無効となる機関外からサイトランセンスコンテンツへアクセスする場合は，ID 認証により所属機関を担保することが多い．多くの研究者が，そうした複数のサービスを利用するために，サービス毎の複数の ID を管理しているのが現状である．

インターネットサービスに対する ID 管理の問題を解決する方法として，大きく 2 つの方向性がある．1 つは OpenID[1]などに代表される user-centric identity であり，もう 1 つは SAML[2]などに代表される federated identity である．後者に関しては，欧米では各国の学術機関が中心となり，学術コンテンツやリソースへのアクセスに主眼をおいたフェデレーションの構築が進められている[3]．我が国でも，国立情報学研究所が推進する最先端学術情報基盤において[4]，米国の Internet2 が開発している SAML 準拠のミドルウエア：Shibboleth[5]を利用した学術認証フェデレーションの構築が進められている[6][7]．

欧米では，先に述べたような国レベルでのフェデレーションの他に，地域でのフェデレーションの構築にも発展している[8]．後者のローカルフェデレーションは，前者の中でバーチャル組織（Virtual Organization: VO）を形成しているとみなすこともできる．フェデレーションでは，ID プロバイダーは，ユーザ情報としての属性を付与し，サービスはこれに基づいてアクセスレベルをコントロールする．通常は，大学等の ID プロバイダーが付与できる属性に従ってサービスにアクセスするが，これに VO が付与できる属性を加えることができれば，よりリッチなサービスをユーザに提供できるフレームワークが構築できるものと考えられる．ユーザが一度 ID とパスワードを入力して認証された後は，横断的にサービスを利用できるシングルサインオン（SSO）は，フェデレーションにおける特徴的な機能である．この利便性を損なうことなく，分散管理されたユーザ属性を連携できる機能は，次世代のフェデレーションを考える上でも重要な鍵となる．

そこで本研究では，Shibboleth を利用したフェデレーションにおける，ユーザ属性連携基盤を構築することを目的とする．また，実問題への応用として，学術認証フェデレーションと学会が形成する VO との間で，構築したシステムの実用可能性を実験する．

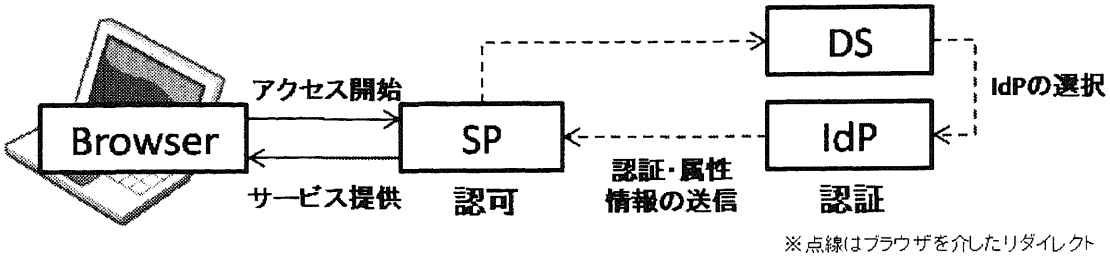


図 1　Shibboleth を利用したフェデレーションにおける認証プロセスの概略

## 2. 学術認証フェデレーションの概略

フェデレーションは，図 1 に示したように，ID を管理する ID プロバイダー（IdP），サービスを提供するサービスプロバイダー（SP），エンドユーザに利用する IdP の選択画面を提示するディスカバリサービス（DS）から構成される．多くの場合，IdP は，大学や研究機関といった学術機関による構築・運用されている．SP は，商用出版社が提供する電子ジャーナルなどを主として，大学が提供する e-learning サイトや研究者コミュニティが提供するデータベースなど，その種類は多岐にわたる．

認証を受けるためには，まず，SP でのログインのリンク先として設定されている DS において，ユーザの所属機関の IdP を選択する．IdP での認証が完了すると，IdP は，SP に対して認証の結果と SP が必要とする属性を送信する．SP はこの属性情報に応じてユーザのアクセスレベルを設定し，サービスを提供する．現在，学術認証フェデレーションで推奨されている属性は，以下の 16 種類である．

| | | |
|---|---|---|
| 1 | mail | 電子メールアドレス |
| 2 | sn | 氏名（姓）の英語表記 |
| 3 | o | 組織名称を英語表記 |
| 4 | ou | 組織内所属名称を英語表記 |
| 5 | givenName | 氏名（名）を英語表記 |
| 6 | displayName | 表示名の英語表記 |
| 7 | eduPersonAffiliation | 利用者が所属する組織内での職種 |
| 8 | eduPersonPrincipalName | フェデレーション内で一意な，かつ，永続的な利用者識別子 |
| 9 | eduPersonEntitlement | 特定のアプリケーションを利用する資格情報 |
| 10 | eduPersonScopedAffiliation | 利用者が所属する組織内での職種のスコープ付き表記 |
| 11 | eduPersonTargetedID | フェ デレーション内で一意な，かつ，SP サイト毎に異なる利用者識別子 |
| 12 | jasn | 氏名（姓）の日本語表記 |
| 13 | jaGivenName | 氏名（名）を日本語表記 |
| 14 | jaDisplayName | 表示名の日本語表記 |
| 15 | jao | 組織名称を日本語表記 |
| 16 | jaou | 組織内所属名称を日本語表記 |

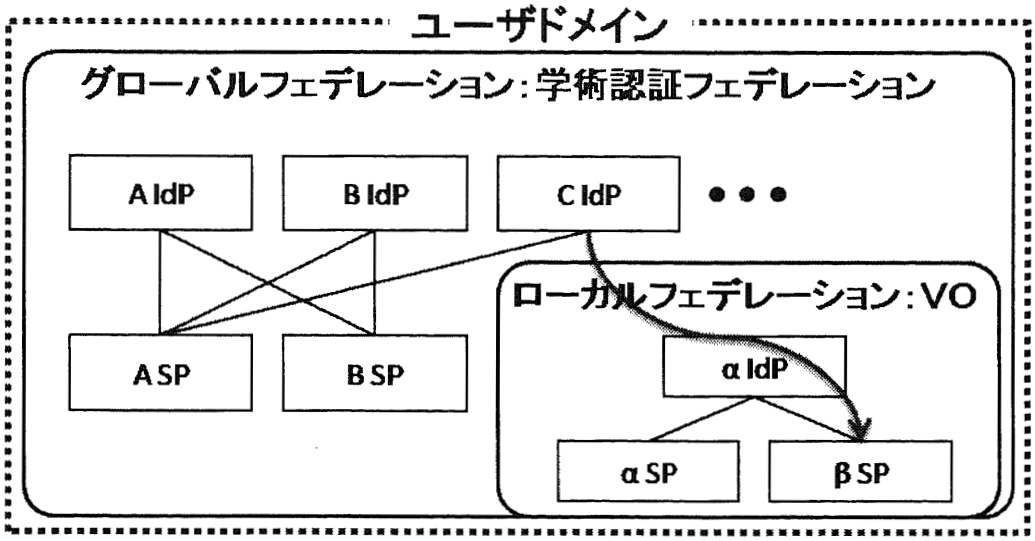


図 2　属性連携システム利用モデル

例えば，電子ジャーナルサイトの利用の場合，サイトライセンス条件での閲覧には，3.o のような所属組織が判別できる属性のみを送信して認可判断を受ける．さらに，文献情報の管理機能などの個人ごとのカスタマイズが必要なサービスを利用する場合は，11.eduPersonTargetedID などの利用者を識別できる属性を必要に応じて送信する．

現段階の学術認証フェデレーションでは，IdP は大学や研究機関が設置するという前提で，機関が送信することの可能な 16 種類の属性を規定している．しかしながら，所属学会やプロジェクトに関する属性など，大学の IdP では付与することが困難であるが，ユーザにリッチなサービスを提供できる可能性のある属性は，この他にも多々ある．本研究では，そうした属性は，フェデレーション内の VO により提供されるというモデルを設定し，属性連携を可能にするシステムを構築する．

## 3. 属性連携システム

### 3.1. 利用モデル

属性連携システムのための利用モデルを，図 2 に示す．学術認証フェデレーションのような，ユーザドメインを広くカバーするフェデレーションをグローバルフェデレーション，その中で構成される VO をローカルフェデレーションと呼ぶことにする．このとき，ローカルフェデレーションの α IdP からは，グローバルフェデレーションにおける IdP（図中，A Idp, B IdP, C IdP が該当）では管理されることなく，かつ，ローカルフェデレーションの SP（図中，α SP，β SP）には必要不可欠な属性が送信されるものとする．通常，α SP や β SP を利用するユーザは，ローカルフェデレーション内の α IdP を利用することになる．しかしながら，その利用形態のままでは，ユーザはローカルフェデレーションとグローバルフェデレーションの複数の ID を使い分ける必要が生じ，フェデレーションの特徴である SSO の利便性を欠くことになる．この問題を解決する属性連携システムとは，図中青矢印

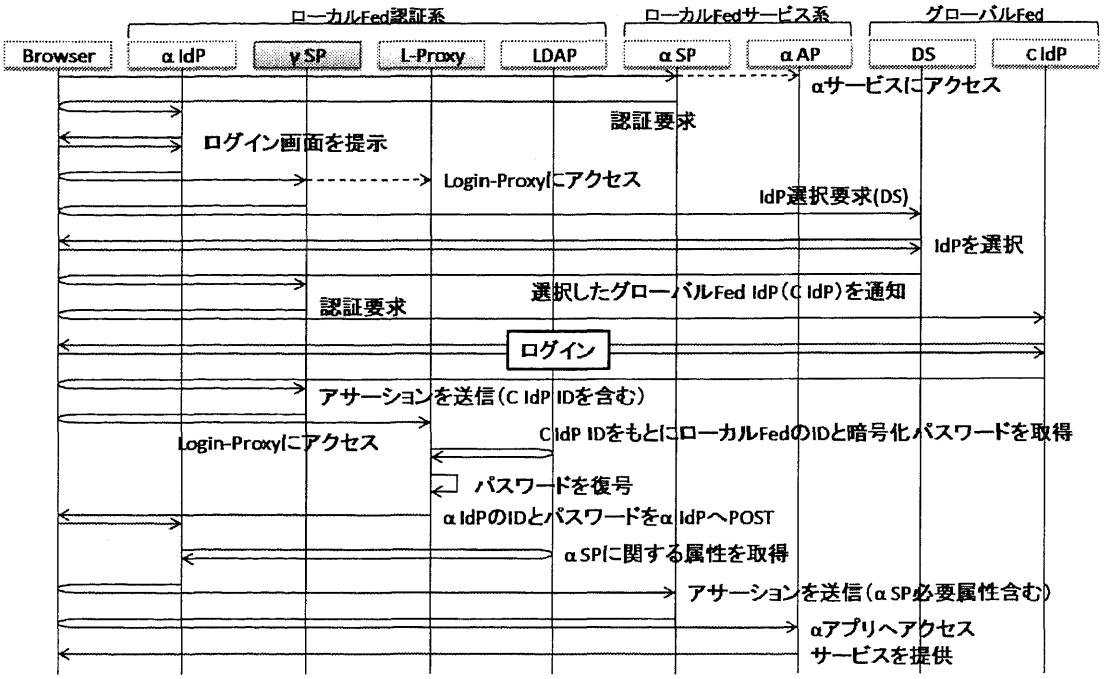


図 3　属性連携システムのシーケンス図

で示したように，C IdP を利用して，βSP を利用することができ，かつ，SSO にてサービスを利用できるシステムを構築することを意味する．

### 3.2. 属性連携システム

構築するシステムの，処理の流れを示したシーケンス図を図 3 に示す．図中緑色で示したオブジェクトブロックは，属性連携がされていない図 2 においても存在するシステムである．本研究では，これに加え，図中青色で示したように，グローバルフェデレーションからローカルフェデレーションに対する API 的な役割を果たすγSP を用意する．また，図中水色で示した L-Proxy と呼ぶシステムを用意し，γSP からαIdP を介してαSP へのアクセスを実現する．これにより，C IdP による認証だけで，αIdP が管理する属性を取得し，αAP のサービスを受けることができる，属性連携システムが実現できることになる．

### 3.3. 動作環境

L-Proxy は，シボレス IdP と同様の Java 言語にて開発し，以下の環境にて動作を確認した．

- OS　　CentOS 5.2
- Java 実行環境　　JDK 1.6.0_11
- Web サーバ　　Apache 2.2.3
- AP サーバ　　Tomcat 6.0.14

また，L-Proxy が利用する依存ライブラリは，以下のとおりである．

| 依存ライブラリ | Ver | 用途 |
|---|---|---|
| commons-configuration | 1.6 | 汎用的な設定 IF を提供する API |
| commons-collections | 3.2 | java.util パッケージの Collection 関係を拡張するライブラリ（commons-configuration 依存） |
| commons-lang | 2.4 | java.lang ライブラリ拡張パッケージ（commons-configuration 依存） |
| commons-logging | 1.1 | ロギング API（commons-configuration 依存） |
| commons-jxpath | 1.3 | XPath インタープリタ（commons-configuration 依存） |
| log4j | 1.2 | ロギングユーティリティー |
| 暗号化ライブラリ | — | PBE と AES に対応したデータの暗号化と復号化を実現するライブラリ．本研究にて独自構築. |

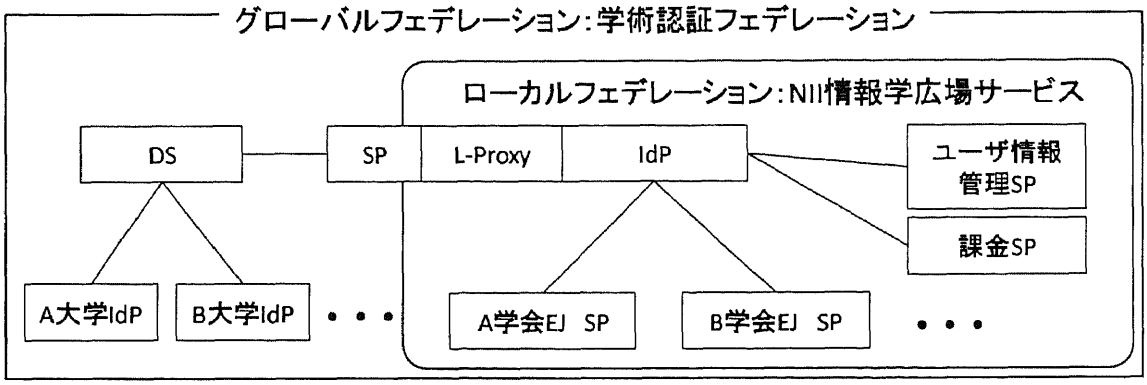


**図 4　属性連携システムの応用例**

## 4. 実システムへの応用

提案した階層型フェデレーションにおける属性連携システムへの応用として，ローカルフェデレーションに属する学会のサービスを，グローバルフェデレーションに属する大学の IdP から利用する実験を行った．ローカルフェデレーションの構成は，図 4 のようになっており，国立情報学研究所の学術コンテンツサービス研究開発センターで開発中のサービス「情報学広場」[9]の認証機能をシボレス化し，本システムを適用した．実験では，

1. 大学の IdP を利用してローカルフェデレーションの SP にアクセスできること
2. その後にグローバルフェデレーション内の SP にも SSO できること

を確認項目とした．なお，試行運用中のサービスで実験を行うために，グローバルフェデレーションとしては，学術認証フェデレーションにおけるテストフェデレーション環境[6]を利用した．

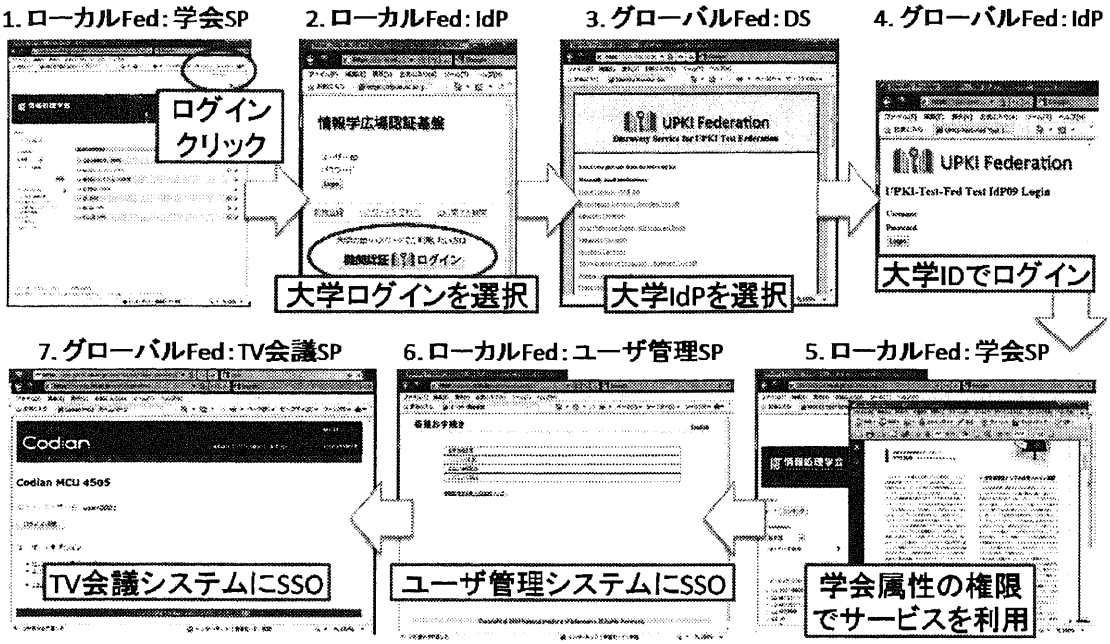


図 5　属性連携システムを利用したサービス遷移

実験過程におけるスクリーンショットを，図 5 に示す．それぞれの画面での動作は以下のようになっており，目的とした上記 2 点のポイントが実現されることを確認した．

1. ローカルフェデレーション学会 SP
   学会電子ジャーナルサイト SP にて，所属研究会の PDF を取得するためにログインをスタート．
2. ローカルフェデレーション IdP
   グローバルフェデレーションでの IdP（大学 IdP を想定）を利用してログインするために，L-Proxy システムが提供する「機関認証ログイン」ボタンをクリック
3. グローバルフェデレーション DS
   認証を行う大学の IdP を選択
4. グローバルフェデレーション IdP
   大学より提供される ID とパスワードで認証
5. ローカルフェデレーション学会 SP
   大学の ID でログインしながら，学会の IdP の属性と連携されることで，所属学会のサービスを利用可能（所属学会の権限として PDF をダウンロード可能）
6. ローカルフェデレーションユーザ管理 SP
   学会 SP にログインしたまま，ローカルフェデレーションの他の SP（ユーザ管理 SP）に SSO 可能

7. グローバルフェデレーション TV 会議 SP

ローカルフェデレーション SP からグローバルフェデレーション SP（TV 会議 SP）に移動しても SSO 機能により，ID とパスワードを入力することなくサービスを利用可能

## 5. おわりに

本研究では，Shibboleth を利用したフェデレーションにおける，ユーザ属性連携基盤を構築した．構築したシステムにより，グローバルフェデレーションとローカルフェデレーションで運用される 2 つの IdP において，属性連携が可能であることを実験を通して確認した．現段階では，2 つの IdP 間で主従関係を規定した機能を提供しているが，そうした制約を排除して，相互の IdP から必要とされる属性を交換できるシステムが構築されれば，さらに利用ケースが広まるものと考えられる．また，今回は IdP 間での属性連携を実現したが，これとは別に，フェデレーションにおいて DS, IdP, SP 以外の，属性プロバイダーという新しいエンティティを導入することも考えられる．今後，実サービスとの整合性を考慮しながら，次世代フェデレーションに必要とされるシステムの検討を進めていく予定である．

## 参考文献


[1] OpenID Authentication 2.0 - Final, http://openid.net/specs/openid-authentication-2_0.html (参照 2009年10月10日)

[2] Security Assertion Markup Language (SAML) V2.0, http://saml.xml.org/saml-specifications (参照2009年10月10日)

[3] Research and Education FEDerations, https://refeds.terena.org/ (参照2009年10月10日)

[4] Sakauchi, M., Yamada, S., Sonehara, N., Urushidani, S., Adachi, J., Konishi, K. and Matsuoka, S. :"Cyber Science Infrastructure Initiative for Boosting Japan's Scientific Research", CTWatch Quarterly Journal, Vol.2, No.1, pp.20-26, 2006.

[5] The Shibboleth Project, http://shibboleth.internet2.edu/ (参照2009年10月10日)

[6] Yamaji, K., Kataoka, T., Nishimura, T., Shimaoka, M., Nakamura, M., Sonehara, N. and Okabe, Y. : "UPKI Federation –Pilot Operation–", 28th Asia Pacific Advanced Network Meeting, 2009.

[7] Kataoka, T., Nishimura, T., Shimaoka, M., Yamaji, K., Nakamura, M., Sonehara, N. and Okabe, Y. : "Leveraging PKI in SAML 2.0 Federation for Enhanced Discovery Service" The 9th Annual International Symposium on Applications and the Internet, 2009.

[8] Davies, C. and Shreeve, M. : "Case studies supporting the business case toolkit" http://www.jisc.ac.uk/media/documents/themes/accessmanagement/cc297d002-1.0%20case%20studies%20supplement.pdf, 2007. (参照2009年10月10日)

[9] 山地一禎，青山俊弘，武田英明：「学術資源共有基盤WEKOの開発」，ディジタル図書館, Vol.36, pp.51-61, 2009