

複数の IdP へのシングルサインオンを 可能にする認証システムの提案

足立 紘 亮^{†1} 新村 正 明^{†2}

Shibboleth の IdP は、ユーザに対して SP へのアクセス制御を行うことはできない。このようにアクセス権限を考慮した認証基盤を構築する場合は、複数の IdP の設置が有効である。しかし、IdP を複数設置した場合、各 IdP に認証を行う必要がある。そこで本研究では、複数の IdP へのシングルサインオンを可能にする認証システムを提案する。

Proposal of the Authentication System for Single Sign-On to multiple IdPs

KOSUKE ADACHI^{†1} and MASAAKI NIIMURA^{†2}

In the Shibboleth System, an IdP can not make access control decisions for user to access SPs. So, multiple IdPs is a good solution for access control to SPs. But, in this case, it is necessary to authenticate to all of IdPs. In this paper, we propose the authentication system for Single Sign-On for multiple IdPs.

1. はじめに

信州大学では、学内サービスのシングルサインオン化や、学術認証フェデレーションへの参加を目的に、Shibboleth を利用した認証基盤を構築し、e-Learning システムや一部のサービスで運用を開始している。

^{†1} 信州大学大学院工学系研究科

Graduate School of Science and Technology, Shinshu University

^{†2} 信州大学 e-Learning センター

Shinshu University e-Learning Center

大学をはじめとする高等教育機関では、学内の学生や教職員に限らず、学内ネットワーク利用アカウントや e-Learning 利用アカウントなど、様々な権限のアカウントを管理している。そのため、学内サービスのシングルサインオン化や、学術認証フェデレーションへの参加に伴い、各アカウントに対して、各サービスへのアクセス制御を行う必要がある。しかし、Shibboleth の Identity Provider (以降 IdP) には、アクセス制御を行う機能は備わっていない。そこで信州大学では、サービスごとのアクセス権限を考慮し、複数の IdP を用いた認証基盤を構築した。しかし、IdP を複数設置したことにより、各 IdP に認証を行う必要性が発生し、ユーザの利便性が低下した。

そこで本研究では、利便性を低下させることなく、アクセス権限を考慮した認証基盤を構築するために、複数の IdP へのシングルサインオンを可能にする認証システムを提案する。

2. Shibboleth を用いた認証基盤

2.1 Shibboleth の動作

Shibboleth とは、Internet2 が展開する、オープンソースミドルウェアであり、教育機関を中心に世界的に利用されている¹⁾。Shibboleth では、認証処理を行う IdP とサービスを提供する Service Provider (以降 SP) を設置することで、認証基盤を構築する。また、SAML を用いた SSO を実装しており、フェデレーションを構築することで、組織間の認証連携を行う。Shibboleth の認証手順を図 1 を用いて説明する。

- (1) ブラウザから SP へアクセスする。
- (2) IdP が未認証の場合、SP は IdP へリダイレクトをかける。
- (3) IdP は、認証画面をブラウザに表示させ、ユーザから ID とパスワードを受取り、認証処理を行う。
- (4) IdP は認証処理が成功すると、SP へリダイレクトをかける。

IdP の認証が済んでいるブラウザで、別の SP へアクセスした場合、(3) の処理が省略され、SP へのシングルサインオンが実現される。

Shibboleth を用いた認証基盤を図 2 に示す。Shibboleth を導入すると、学内サービスや学内ネットワーク、e-Learning システムなどの認証処理を統合化でき、シングルサインオンによるシームレスな利用が可能となる。さらに、学術認証フェデレーションへ参加することで、学外サービスへのシングルサインオンも可能となる。

2.2 学術認証フェデレーション (GakuNin)

学術認証フェデレーション (GakuNin) とは、学術リソースを利用・提供する機関、組

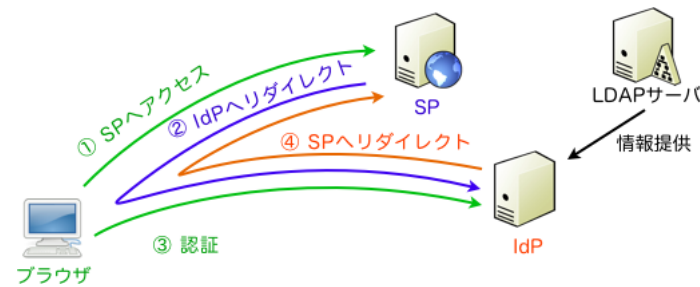


図 1 Shibboleth の認証手順
Fig.1 Shibboleth authentication sequence

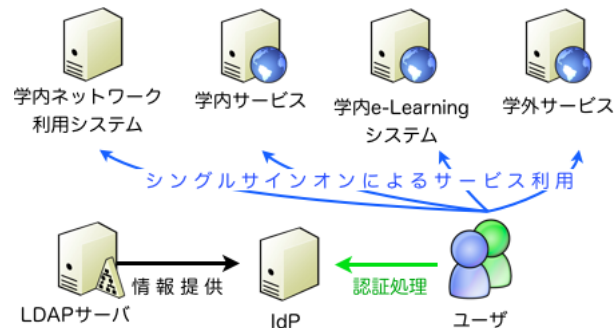


図 2 Shibboleth を用いた認証基盤
Fig.2 Shibboleth authentication platform

織から構成された連合体であり、国立情報学研究所（NII）が運用している²⁾。GakuNin では、各機関が GakuNin で定めたセキュリティポリシーを信頼し合うことで、組織間の認証連携を行う。また、GakuNin は Shibboleth を用いて構築されているため、GakuNin へ参加するには、Shibboleth の導入が必要である。

3. 複数の IdP を用いた認証基盤

3.1 アカウント毎のアクセス制御

図 2 の様に認証基盤を構築した場合、LDAP サーバで管理されている全てのユーザは、IdP による認証が可能となるため、全ての SP をシングルサインオンで利用することができる。しかし、大学をはじめとする高等教育機関では、学内の学生や教職員に限らず、学内ネットワーク利用アカウントや e-Learning 利用アカウントなど、様々な権限のアカウントを管理している。それらのユーザが LDAP サーバで一括で管理されている場合、ネットワーク利用アカウントや e-Learning 利用アカウントにより、学内サービスや学外サービスなどが利用されてしまう恐れがある。そのため各大学では、表 1 のようなセキュリティポリシーを定め、各アカウントに対して各サービスへのアクセス制御を行う必要がある。

3.2 Shibboleth を用いた認証基盤におけるアクセス制御方法

Shibboleth の IdP には、ユーザに対して SP へのアクセス制御を行う機能は備わっていない。そのため、Shibboleth を用いた認証基盤において、アクセス制御を行うには、LDAP サーバで管理されているユーザ権限の属性を用いて、各サービスごとに認可処理を行う必要がある。しかし、学内サービスにおいては、各サービスごとに認可処理の機能を追加することは可能であるが、学外サービスに関しては、学外で管理しているため、自由に機能を追加することはできない。よって、学内サービスと学外サービスの認証を同一の IdP で行う図 2 の様な認証基盤では、アクセス権限を考慮した制御はできない。

表 1 アカウントとアクセス権限
Table 1 Accounts and Access rights

	学内ネットワーク	e-Learning	学内サービス	学外サービス
学生アカウント	○	○	○	○
教職員アカウント	○	○	○	○
学内ネットワーク利用アカウント	○	×	×	×
e-Learning 利用アカウント	×	○	×	×

IdP は認証処理を行う際、LDAP サーバからユーザ情報を取得している。そのため、LDAP サーバで、情報提供するアカウントを制限することで、IdP で認証できるアカウントを制限する。さらに、認証できるアカウントを制限した IdP を、アクセス制限単位ごとに設置する。これにより、サービスへアクセスする前段階でサービスを利用するユーザを制限することが可能となる。よって、認可処理を追加することのできない学外サービスにおいても、アクセス制御が実現できる。

複数の IdP を用いた認証基盤の例を図 3 に示す。この例では、アクセス制御範囲を学内とフェデレーションに分け、それぞれに IdP を設置している。また、LDAP サーバからの情報提供制御を可能にするサーバをフィルタリングサーバと名づけ、新たに構築した。

3.5 問題点

複数の IdP を用いることで、学外サービスへのアクセス制御が実現できる。しかし、すべてのサービスを利用できるアカウントが、学内のサービスとフェデレーションのサービスを同時に利用する場合、それぞれの IdP への認証処理が必要となる。そのため、図 2 の認証基盤と比べ、利便性が低下している。

4. 複数の IdP へのシングルサインオンを可能にする認証システムの提案

3.5 で示した問題点に対し、複数の IdP へのシングルサインオンを可能にする認証システムを提案する。提案するシステムの概要図を図 4 に示す。本システムでは、新しく共通認証サーバを設置し、IdP の認証の統合化を行う。共通認証サーバを用いた場合の認証手順を、図 4 を用いて説明する。

- (1) ブラウザから SP へアクセスする。
- (2) IdP が未認証の場合、SP は IdP へリダイレクトをかける。
- (3) IdP は、IdP の認証画面を表示する代わりに、共通認証サーバへリダイレクトをかける。

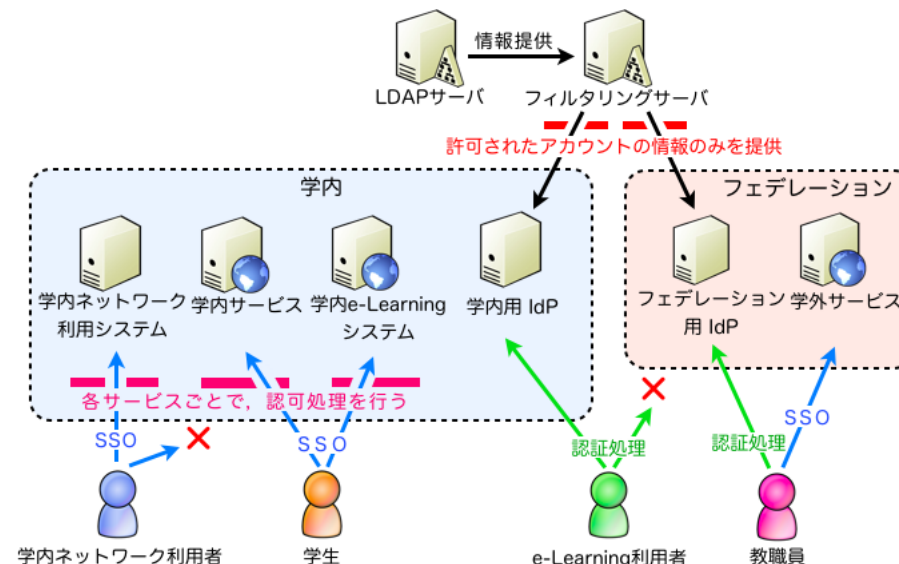


図 3 複数の IdP を用いた認証基盤

Fig.3 The authentication platform with multiple IdPs

- (4) 共通認証サーバは、認証画面をブラウザに表示させ、ユーザから ID とパスワードを受取り、認証処理を行う。
- (5) 共通認証サーバは、認証時に受取った ID とパスワードをセッションで保持する。
- (6) 共通認証サーバは、セッションで保持されている ID とパスワードを IdP へ POST し、IdP への認証を行う。
- (7) IdP は認証処理が成功すると、SP へリダイレクトをかける。

共通認証サーバの認証が済んでいるブラウザで、別の IdP への認証処理を行う際は（４）と（５）の処理が省略され、IdP へのシングルサインオンが実現される。

4.1 共通認証サーバの構築

共通認証サーバを構築する際、必要な機能を述べる。

- LDAP 認証

共通認証サーバは、セッションで保持された ID とパスワードを IdP へ送信することで、IdP への認証を行う。また、IdP の認証処理では、LDAP サーバから提供される情

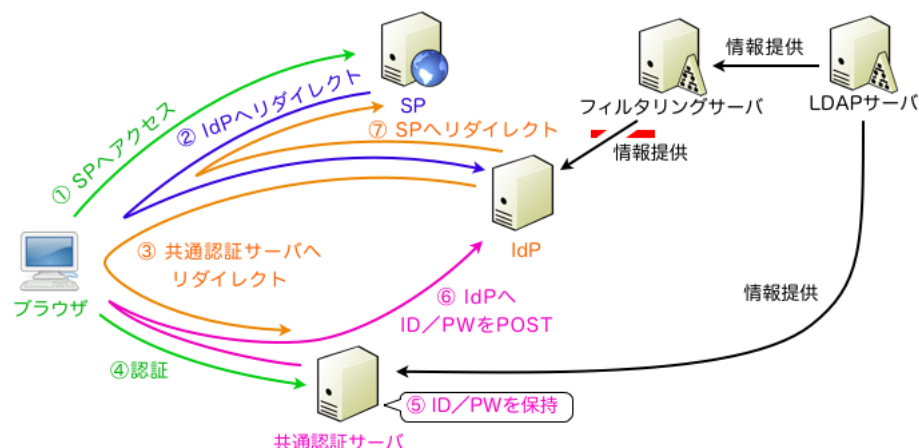


図 4 複数の IdP へのシングルサインオンを可能にする認証システム
Fig. 4 The Authentication System
for Single Sign-On to multiple IdPs

報を利用している。よって、共通認証サーバの認証処理においても、LDAP サーバの
情報を利用する必要がある。LDAP 認証の実装は、各種プログラミング言語で LDAP
認証用のモジュールが用意されているため、容易に行うことができる。

- セッション管理

認証処理後、ID やパスワードなどの認証情報を保持するために、セッション管理をす
る必要がある。

- 許可された IdP への認証情報の POST

共通認証サーバでは、POST 対象となる IdP の URL を表 2 のように ID を振って保
持する。そして、認証手順 (3) において、IdP からリダイレクトする際に、GET パ
ラメータで、対象の IdP の ID を指定する。これにより、許可された IdP へのみ認証
情報が POST されることとなり、認証情報の漏洩を防ぐことができる。

4.2 IdP の認証画面の変更

IdP は通常、SP からのリダイレクトを受けると、認証画面を表示する (図 1 の認証手順
3)。しかし、提案する認証システムでは、認証処理を共通認証サーバで統合的に行うため、
共通認証サーバへリダイレクトをかける必要がある。そこで、IdP の認証画面を、共通認証
サーバへのリダイレクトがかかるように変更する。またリダイレクト先 URL の GET パラ

メータに、認証情報が IdP 自身に POST で返るように ID を指定する。

5. おわりに

本研究では、利便性を低下させることなく、アクセス権限を考慮した認証基盤を構築する
ために、複数の IdP へのシングルサインオンを可能にする認証システムを提案した。今後
は、提案したシステムを構築し、システムの有効性の評価を行う予定である。また、現在学
内で運用しているサービスや、ネットワーク利用システムなどの Shibboleth 化を行うこと
で、ユーザの利便性の向上に努めていく。

参 考 文 献

- 1) Internet2 : Shibboleth®, Internet2 (online),
入手先<<http://shibboleth.internet2.edu/>> (参照 2011-04-02).
- 2) 国立情報学研究所：学術認証フェデレーション, 国立情報学研究所 (オンライン),
入手先<<https://www.gakunin.jp/>> (参照 2011-04-02).

表 2 URL リスト

Table 2 URL list

name	ID	URL
IdP-A	01	https://idp-a.example.ac.jp/idp/Authn/UserPassword
IdP-B	02	https://idp-b.example.ac.jp/idp/Authn/UserPassword