JSiSE Research Report
vol.31,no.2(2016-7)

認証システムのフィルタ機能による LMS アクセス制限の実現

新村 正明[*1], 長谷川 理[*1], 國宗 永佳[*1]
*1 信州大学

Implementation of Access Limitation for LMS using Filtering Function on Authentication System

Masaaki Niimura [*1], Osamu Hasegawa [*1], Hisayoshi Kunimune [*1]
*1 Shinshu University

LMS is used not only for students, but also Faculty Development (FD) and Staff Development (SD). But it mast be block access from students to the LMS used for FD/SD, because it contains many contents only for teachers and staffs. Generally, this access block is implemented by access-list, but in LMS, whenever a user authenticates, the user is registered to the access-list automatically. In many cases, authentication system have both teachers / staffs and students information. To solve this problem, we propose a filtered authentication system. In this method, we put in "filter server" between LMS and the authentication server, and this "filter server" blocks students information. From this system, only teachers and staffs authenticate and use LMS.

キーワード: 研究会報告，書式，執筆要領

1. はじめに

LMS は，その利便性から，教育目的だけでなく FD (Faculty Development) や SD (Staff Development) にも利用されつつあるが，教職員向けの情報が多く掲載されることから，学生による閲覧を禁止する必要がある．このようなアクセス制限は，LMS の設定によっても可能であるが，設定ミス等により誰でも閲覧できてしまう可能性があり，認証時点で学生のアクセスを排除するほうが望ましい．しかし，通常の LMS では学生の認証も行う必要があることから，FD/SD 専用の認証システムを用意する必要がある．

そこで我々は，認証システムにフィルタ機能を設け，LMS 毎に別の認証情報を与えるシステムの構築を行った．

2. 研究背景

2.1 認証と認可

一般的に，あるシステム上でユーザがリソースへアクセスする状況において，「認証」とはシステム上で操作を行っているアカウントが，そのアカウントが発行された対象（人物等）により操作されていることを保証するための仕組みであり，「認可」とは，あるアカウントからあるリソースへのアクセスの可否を制御するための仕組みである．

以下，図 1 により説明する．あるシステムにログインする場合，ユーザ ID とパスワードの組み合わせ等により，アカウントが正当な利用者により操作されているかの「認証」が行われる．この認証に関しては，システム自体がアカウント情報を管理する方法の他，LDAP や Active Directory のように，パスワード等を外部システムで一元管理し，その認証情報に基づいてシステムが認証を行う方法や，Shibboleth などの Single Sign On (SSO) 機能のように，外部の認証専用システムに正当性の確認を委託し，認証機能を代替させる方法も広く用いられている．

次に，「認可」に関しては，システム内のリソース毎に，そのアカウントがアクセスできるかの制御が行われる．たとえば，ログイン時の「認証」が成功した場合，次に，このシステムを利用することができるア

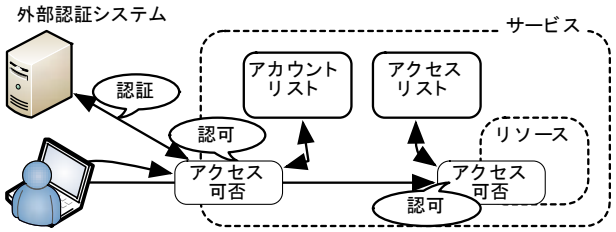

図 1 認証と認可

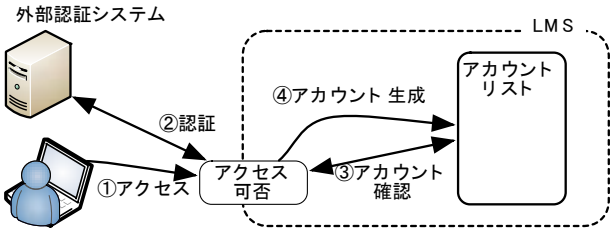

図 2　LMS における認証

カウントであるかの確認が行われる．通常，システム内にアカウントリストがあり，これによりシステム利用の可否が決定される．また，システム内のリソースに関しても,アクセスの可否が判断される場合もある．これは，通常，リソース毎にそのリソースへのアクセスを許可するアカウントのリスト（図 1 中のアクセスリスト）をあらかじめ設定し，アクセスを要求するアカウントがそのリストに含まれるかの確認により行われる．

2.2 本稿の対象とする認証環境

大学のような高等教育機関においては, LMS のような学習支援システムだけでなく，教務システムや図書館システム等，多くのシステムが導入されている．さらに教育機関である性質上，年度毎に多くの学生の入れ替わりが発生する．このため，システム毎にアカウント管理を行うことは，多くの工数が発生する他，アカウント登録漏れ等の問題が発生する可能性が高くなる．そこで，ユーザ管理を一元化し，アカウント情報を各システムに提供する方法が用いられている．このユーザ管理には LDAP や Active Directory 等のシステムが使用されていることが多い．

また認証においても，ユーザ管理の一元化と同様な状況から，認証サービスの一元化も進められている．たとえば，国立情報学研究所が提供する学術認証フェデレーション「学認（GakuNin)」には，2016 年 3 月時点で 181 の教育機関（国立大学法人では約 70%）が参加しており(1)，これらの教育機関には全て Shibboleth が導入されている．

そこで本稿では，高等教育機関において，全学向けの認証サービスが提供され, LMS もこの認証サービスの配下にいる状況を想定する．

2.3 LMS における認証と認可

一般的なシステムにおいては，ログイン時に，「認証」によりアカウントを利用している者の正当性を確認したあと，そのアカウントがシステムを利用できるかの検証（「認可」）を行い，システムの利用の可否を決定する．しかし，Moodle のような LMS においては，不特定多数の学習者を対象とすることから，図 2 に示すように,外部の認証専用システムにより「認証」が成功した場合，システム内にそのアカウントがなければ，アカウントを自動生成する機能を有している．

この機能により, LMS にあらかじめ全ユーザアカウントを生成することなく，必要に応じて自動的にアカウント作成がなされるため，ゲスト公開可能なコンテンツへのアクセスを容易に実現することが可能となる．

3. 課題

LMS の有する学習支援機能は非常に有用でかつ簡便に使用することができるものであることから，通常の講義だけでなく，FD／SD といった，教職員向けの教育等にも使用することができる．しかし，教職員向けのコンテンツは，学生に公開することが望ましくないものもあり，教職員のみのアクセスに限定する必要がある．

LMS においては，コース毎に，図 1 に示すアクセスリストがあり，ある科目の受講生のみがその科目のコンテンツが掲載されているコースにアクセスできるよう制御を行っている．FD/SD 用のコースもこのようなアクセスリストによる制限で，教職員のみがアクセスするよう制御することが可能である．しかし，教職員の異動のたびにアクセスリストの修正が必要となるほか，人為的ミスにより，教職員以外の者のアクセスが可能のなってしまう危険性がある．

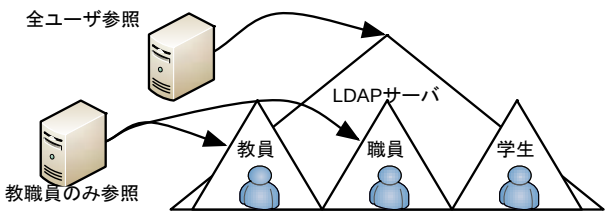

図 3　LDAP における認証

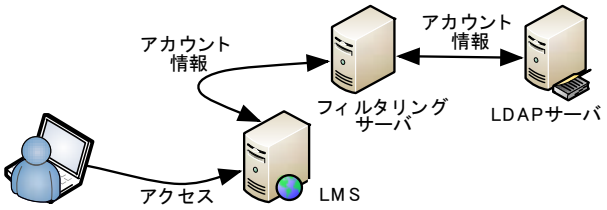

図 4　LDAP における解決方法

4. 提案

このような問題に対し，FD/SD のために専用の LMS を用意し，LMS 内で学生アカウントと混在させないことで，学生がコンテンツを閲覧できてしまう可能性をなくすことが可能となる．しかし，前章で述べたように，LMS には，認証が完了した段階で自動的にアカウントを生成する機能があり，これにより，FD/SD 専用 LMS に学生がアクセスした時点で，学生のアカウントが生成され，ログイン可能な状態となってしまう．

この問題を解決する方法として，FD/SD 専用 LMS にあらかじめ教職員の全アカウントを生成し，アカウント自動生成を禁止する方法がある．しかし，この方法は，前章で述べた，あらかじめアクセスリストを用意する方法と同様に，管理コストが大きいという問題点が残る．

そこで，本稿では，認証システム側にフィルタ機能を設けることで，FD/SD 専用 LMS において学生アカウントを「認証」の時点で拒否する方法を提案する．フィルタ機能を設ける理由は，既存の認証システムの改変を極力少なくし，任意の環境における導入を図るためである．

5. 実現方法

認証システムとして広く用いられている LDAP および Shibboleth の各々について実現方法を説明する．

5.1 LDAP における実現方法

5.1.1 LDAP のユーザ管理方式

LDAP は，図 3 に示すように，構成員をグループで管理すると共に，グループを木構造で管理している．また，外部システムから LDAP へのアカウント情報の問い合わせの際に，木構造の任意の位置を指定し，それ以下の情報のみを参照させることが可能である．この機能を利用し，FD/SD 専用の LMS からは，教職員のグループのみを参照させることで，学生の認証を拒否することが可能となる．

このように LDAP のグループ構造が身分別のグループに基づいている構成であれば，アクセス制限は容易に実現できる．しかし，たとえば大学における学部別などの組織上のグループ構成になっている場合や，木構造ではなくアカウント情報内に身分情報が保持されている場合には，このような方法を利用することはできない．

5.1.2 フィルタサーバによる解決

この問題を解決するために，図 4 に示すように，LMS と LDAP サーバに間でフィルタリングを行うサーバを設置する．このサーバは LDAP の問い合わせを中継するサーバとして動作し，中継の際に指定されたアカウントのみを透過させる機能を有する．このフィルタリングサーバは，我々の先行研究(2)において開発されたものであり，アカウント情報内の任意の項目を条件にしてフィルタリングを行うことができる．これにより，教職員のみを透過する設定することで，LMS からは教職員アカウントのみが登録された LDAP サーバのように見えることとなる．

5.2 Shibboleth における実現方法

Shibboleth による認証では，図 5 に示すように，認証自体を担当する IdP(Identity Provider) と，LMS のように IdP に認証を委託する SP(Service Provider) により構成される．通常，教職員も学生も同じ IdP で認証を受けることから，教職員も学生も，全ての SP を利用することが可能となってしまう．

このような問題に対して，Shibboleth には，SP 毎

に利用者の制限を行う機能が用意されている. これは, ある SP からの認証要求に対し, 特定のグループに属する利用者しか認証を成功させない機能であり, IdP Ver.2 では FPSP(Filter Per SP) プラグインとして, IdP Ver.3 では組み込み機能として実現されている.

また, IdP は認証機能を提供するもので, ユーザ管理の機能は別途用意する必要がある. このユーザ管理には, 通常, LDAP サーバが用いられ, LDAP のアカウント情報が Shibboleth が定義するユーザ属性情報にマッピングされ提供される.

そこで, IdP と LDAP サーバの間に前節で説明したフィルタリングサーバを設置し, IdP に渡す情報に教職員グループあるいは学生グループに所属していることを示す情報を付与することで, 前述の FPSP に相当する機能を有効にすることが可能となる.

6. 実装例

本稿で提案したアクセス制限方法の信州大学における実装例を示す.

信州大学では, LMS として Moodle を採用しており, 学部・年度毎に独立した Moodle の運用を行っている(3). これは, 各学部固有の要求に答えること, 不要なユーザ登録を避け Moodle の動作を軽くすること, さらに, Moodle のバージョンアップに伴う後方互換性の欠落に対応するためである.

また, これとは別に, 講義以外の用途, たとえば就職活動支援やセキュリティ教育, 論文収集等, 多用途向けサイトの運営を行っている. 以上は, 学生向け主体のサイトであるが, これに加えて,「教職員専用サイト」として, FD/SD 用のサイトの運用も行っている.

このような多数の Moodle を効率的に運用するために, 1 つのサーバ内に複数の独立した Moodle が稼働する仕組みを開発し運用を行っている(3). また, 複数の Moodle へのログインを容易に行うことができるよう, Shibboleth による SSO 環境を提供している.

しかし, 5.2 で示した Shibboleth での実現方法では SP 毎に利用者制限を行うが, 1 つのサーバで複数の Moodle を運用する場合には, サーバが SP となることから, Moodle 単位での利用者制限が困難となる.

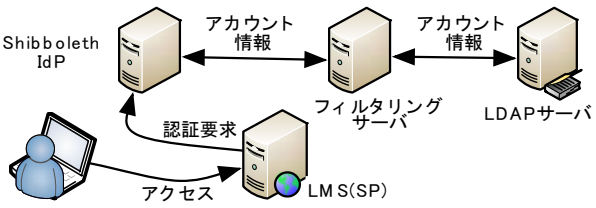

図 5　Shibboleth における解決方法

そこで, FD/SD 専用サーバのみ LDAP による認証を行うこととし, 参照先をフィルタリングサーバにすることで利用者制限を行うこととした.

Moodle は認証がプラグインの形式で提供されており, 標準の LDAP 認証プラグインでは, 認証情報を参照する LDAP のツリー内の位置を複数指定することが可能となっている. これを利用し, フィルタリングサーバで図 3 のような教員・職員・学生のグループ別のツリーになるよう変換し, 教員・職員の 2 つのツリーを指定することで, 学生の認証を排除するよう設定を行った.

7. まとめ

本稿では, LMS に対する認証情報を制御することで不要な利用者のアクセスを排除する方法を提案した. また, 認証システム側にフィルタ機能を付与することで, 既存の認証システムおよび利用者情報に修正を加えることなく実現することが可能となった. 今後は, 学部毎のアクセス制御など, より汎用性のある利用方法を検討していく予定である.

参 考 文 献

(1) 学術認証フェデレーション参加 IdP・SP 一覧, https://www.gakunin.jp/participants/ (2016 年 5 月 10 日確認)

(2) 足立紘亮, 新村正明: “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”, 電子情報通信学会技術研究報告. ICM, 情報通信マネジメント 111(30), 95-98,(2011)

(3) 新村正明, 五月女雄一, 足立紘亮, 長谷川理, 國宗永佳: “LMS 大規模運用のための複数サイト構築手法の提案と実装”, 教育システム情報学会研究報告,28(7), 129-134(2014)