ユーザ認証を利用したディレクトリ単位のアクセス制限の試み

若松 進

名古屋大学全学技術センター 工学系技術支援室 情報通信技術系

1. はじめに

工学研究科事務部において、工学研究科に関連した全ての規程・内規(以下、規則集と称する)を Web 上で閲覧制限付きで公開するという計画が持ち上り、そのシステム開発が当情報通信技術系に依頼された。

この様な場合、公開するコンテンツを特定ディレクトリ内に保存し、そのディレクトリに対して Basic 認証を行う方法が一般的であるが、ユーザ認証として名古屋大学 ID(以後、名大 ID と略す)を利用する事が要求されていたので、Ldap 認証(名大 ID)とデータベース認証を連携させたシステム開発にトライすることにした。しかし、この連携方法について有益な情報が得られなかったので、全てのコンテンツに対してアクセス制限処理を施したシステムとして完成させた。

2. システム開発の経緯

工学研究科の規則集を Web 公開するシステムの開発に対して、

・ユーザ認証には、名大 ID を利用すること

・閲覧は、工学研究科に所属する教職員に限定すること

という事務部からの要望があった。

開発を行う上で、規則集のコンテンツが約 300 に上るため、特定のディレクトリ内にこれらのコンテンツを保存し、そのディレクトリに対して「データベースによる Basic 認証」を利用する方法に Ldap 認証を連携させることを想定した。開発を開始する前に、この様な認証方法についてネット上で検索してみたが、有用な情報が得られなかったこと、システム開発期限内に完了すること等により、別の方法で対応することにした。

3. 閲覧システムの概要

今回、開発システムは「2. システム開発の経緯」で記述した事務部の要望を満たす必要があり、以下の方法で対応することにした。

(1) 運用・開発環境

・システム運用は、本システム専用のサーバ（OS：CentOS-5.5）を新しく構築し、Web サーバに Tomcat、ユーザ認証に名大 ID を利用するため OpenSSL も利用することにした。

・システム開発は、名大 ID を利用したユーザ認証の開発実績により、Java + JSP + MySQL で行った。

(2) ユーザ認証

・ユーザ認証は Ldap 認証を利用して、①ログインした名大 ID／パスワードが確かめられる。正しい時は、所属コードが取得される(図 1.参照)。

(3) 閲覧権限

・各コンテンツ(html ファイル)を JSP ファイルに変換した。

・また、セッション管理を利用する事で、直接のアクセスにはエラー処理(ログイン画面へのリンク処理)を施した。

・図 1.の ②で、Ldap 認証後に得られた所属コードについてローカ

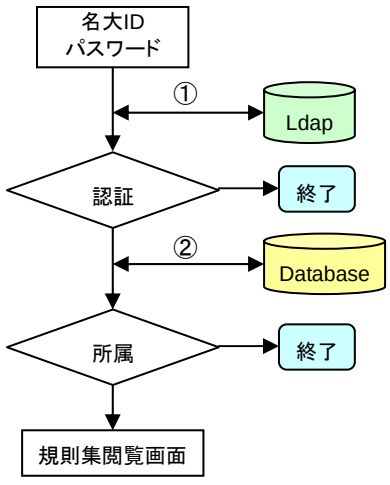


図 1 ユーザ認証の流れ

ルのデータベース上で定義されているかどうかの確認がされる。

・設定されていれば、規則集が表示される。

なお、工学研究科の研究内容は広範に渡っているため、他部局に所属していて工学研究科に関連のある教員の方も多くおられるため、(事務部からの要望されていないが)所属コードによる権限設定のほか名大 ID による権限設定も可能なように対応しておいた。

(4) 権限の設定

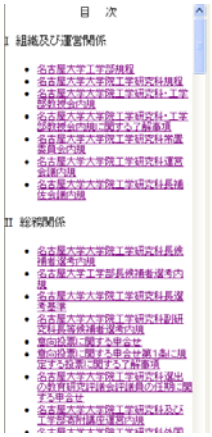
閲覧権限のデータベースへの設定は、現在直接 MySQL にアクセスして、SQL を発行することで対応している(現在、128 の所属コードが設定中)。しかし、この方法では設定ミスの可能性があること、本システムの開発者が権限設定をする必要があること等から、Web 上からの設定が可能となるサブシステムの導入し、その管理をシステム運用者(総務課の事務職員)で担当してもらうことにした。

なお、このサブシステムは現在開発中で発表当日までには完成する予定である。

(5) システム表示例

本システムの表示例として、ログイン画面と認証後の表示画面を以下に示す。

図 2 ログイン画面



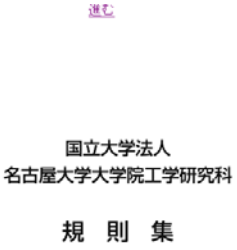


図 3 ユーザ認証後の表示画面

(6) 使用データベース

本システム用いたデータベースは、次の 3 つのテーブルで構成した。

・部局コードで閲覧許可を設定する section_code テーブル

・名大 ID で閲覧許可を設定する personal_code テーブル

・サブシステムの利用許可を設定する superuser_code テーブル

4. まとめ

今回、名大 ID 認証を利用した「規則集閲覧システム」の開発を行い、期限内に開発が完了したことと開発依頼者(総務課)の要望に応えるシステムとして完成した事等、一応の成果を上げる事ができた。

しかし、本システムの開発にあたり、「データベースを利用した Basic 認証」による特定ディレクトリへのアクセス制限への試みについては、達成する事ができなかった。今後、同様なシステムでしかもコンテンツ量が膨大なシステム開発が依頼された時の対応策を考えておく必要があり、この様な方法について、技術研究会への出席者と意見交換ができればと考えている。

5. 参考文献

田中ナルミ／阿部忠光、「標準 MySQL RDBMS の理解から Web アプリケーションの開発・運用まで」、ソフトバンク、2007、ISBN978-4-7973-3955-0