入門LDAP認証（4）
―LDAP認証付きアプリケーション―

平　野　　靖

Ⅰ．はじめに

前回まではLDAPサーバを認証システムとして使うためには，プログラムをどのように書けばよいかを見てきた。プログラムを苦もなく組める人もいるだろうが，認証システムに接続し，認証（Authentication）・認可（権限付与，Authorization）[1]を行い，さらに本来目的とする情報サービスのためのプログラムを組むためには，少なからず労力がいるし，場合によっては資金も必要になる。大規模な情報サービスを構築する際には業者にプログラムの作成を発注する場合もあるだろうが，ごく小規模な情報サービスを構築する場合には，それほど労力も資金もかけられない。とはいえ，中規模，あるいは小規模なコミュニティで認証付きの情報サービスを提供したいという要望は高く，さまざまなフリーウェアが公開されている。そこで，最終回である今回は，極力プログラミングを行わないで認証付きの情報サービスを提供する方法を見ていくことにする。

Ⅱ．コンピュータの利用権限

1．UNIXマシンへのログイン

LinuxやSolarisなど多くのUNIX系OSではユーザ名やパスワード，他のマシンのホスト名などをどのデータベースから得るかを選択することができる。ユーザ名とパスワードについて言えば，研究室などの比較的小規模な組織であればNISサーバを構築し，ユーザ名とパスワードをNISサーバに格納し，他のマシンに提供することが多い。学科や学部，あるいは大学全体のような大規模な組織では，LDAPによる運用が一般的になりつつある。

LDAPサーバを認証に用いるためには，クライアントにpam_ldapとnss_ldapをインストールし，nsswitch.confの書き換えを行う［1］［2］。

なお，pam_ldap-169 ～ 179には無資格者でも認証されてしまうというバグがあるが，180でこの問題が修正されているので，該当のバージョンを使っている場合にはアップデートが必要である［3］。pam_ldapの最新バージョンはhttp://www.padl.com/OSS/pam_ldap.htmlから，nss_ldapの最新バージョンはhttp://www.padl.com/OSS/nss_ldap.htmlからダウンロードできる。

1　AuthenticationとAuthorizationは混同して使用されることが多い用語であり，ともに“認証”と訳されることがある。しかし，前者はユーザが正規の利用者であることを確認することであり，後者はAuthenticationによって確認された利用者に対してリソース（コンピュータやネットワーク，データベースなど）やその一部へのアクセス権限を与えることである。

２．Windowsマシンへのログオン

Windowsマシン群でパスワードの同期を行うにはActive Directory（AD）を使うのが一般的である。しかし，計算機室や研究室などではWindowsマシンとUNIX系OSマシンが混在していたり，デュアルブート環境にしていたりする場合があり，WindowsマシンとUNIX系OSマシンとのパスワードの同期が必要になるため，ADのみでは不十分である。Novell Directory Server（NDS）を利用すれば同期が実現できるが，ここでは一般的なLDAPを使って同期する方法を紹介する。

おそらくもっとも一般的な方法はSambaをドメインコントローラにする方法であろう［4］［5］。つまり，Windowsマシンにログオンするユーザをドメインコントローラとして構成されたSambaサーバで認証し，Sambaサーバは認証機構としてLDAPサーバを使うという方法である［6］。ただし，現在の最新バージョンであるSamba 3.0が提供するドメイン管理機能はNTドメイン互換のもので，Active Directoryドメインの機能は持たないので注意が必要である。

NDSやSamba以外の方法としてWindows Services for UNIX(SFU)［7］やCO-GINA［8］，pGina［9］などを用いる方法もある。どの方法を取るかによって利用できる機能に違いがあるので，適したものを選ぶ必要がある。

Ⅲ．Webアプリケーション

Web技術を用いた情報発信がごく一般的に行われるようになってきている。情報の中には特定の人たちのみに閲覧を許可したい場合があり，情報サービスプロバイダは，ユーザの認証を行い，ユーザに適した情報，あるいはユーザが閲覧することを許可された情報を提供しなければならない。

このような情報提供を行うにあたって，下記のような要望が考えられる。

・学部や学科など多数のユーザを対象にしたいが，ユーザの情報管理の手間を省きたい

・小規模なコミュニティでもユーザの情報管理の手間をなくしたい

・大学内の他の情報サービスと同一のID/パスワードを使いたい

Webアプリケーションを認証付きのものに変えるためには，例えばApacheとmod_ldapを用いることで実現できる。しかし，最近ではコミュニティ向けのWebページ作成のためにCMS（Contents Management System）と呼ばれるソフトウェアが使われたり，SSO（Single Sign-On）を実現したりする技術が使われ始めている。

１．CMS（Contents Management System）

CMS[2]とは，Webページのコンテンツの構成要素であるテキストや画像，レイアウト情報などを一元的に管理し，Webページを構築したり編集したりするソフトウェアのことである。ポータルシステムと呼ばれることもある。CMSの導入により，コンテンツとデザインを分離すること

2　WebCTやBlackboardなどのCourse Management SystemもCMSと略される。

が可能になり，内容のアップデートをする際のデザインの微調整などをする必要がなくなる。代表的なフリーのCMSとして，Wiki，ZOPE，XOOPSなどが挙げられる。

CMSは誰でも閲覧できるWebサイトを構築するためにも利用されるが，限られたユーザのみのアクセスを許可するWebサイトの構築にも用いられることが多い。このようなWebサイトをユーザ登録型コミュニティサイトとも呼ぶ。CMSの多くはバックエンドにSQLデータベースを持っており，そのデータベースを用いてユーザ情報の管理が可能である。ユーザ情報の管理にはSQLデータベースの代わりにLDAPサーバを用いることができる場合もある。

ZOPE（Z Object Publishing Environment）は，Pythonで書かれており，Linux，BSD，Solaris，MacOS X，Windowsなど多くのOS上で動かすことができる［10］［11］。また，プロダクト（PythonProduct，あるいはZClassProduct）を追加することにより，Webサイトとしての機能を増強することができる。LDAPUserFolderというプロダクトにより，ZOPEのユーザ管理をLDAPサーバを使ってできるようになる［12］。

XOOPS（eXtensible Object Oriented Portal System）はPHPで書かれており，PHPとデータベース（MySQLなど），そしてPHPが利用可能なWebサーバ（Apacheなど）が使用可能な環境であれば，非常に短時間でWebサイトを構築することができる［13］［14］。XOOPSから派生したCMSであるXOOPS Cubeでは，５分でユーザ登録型コミュニティサイトを立ち上げることが可能であることを売り文句にしている［15］。XOOPS Cubeは日本語を含むマルチバイト環境に対応した柔軟性の高いシステムの提供を目指してるとのことであるので，多言語での情報発信を行うにはXOOPS Cubeを利用する方がよいかもしれない。現在はXOOPS CubeでLDAPサーバを用いたユーザ認証はできないが，今後対応していく計画のようである。

２．CAS（Central Authentication Service）

前節で紹介したCMSはそれぞれのWebアプリケーションがLDAPサーバと通信してユーザ認証を行うものである。一方，CASはSSOを実現するためのHTTPベースのプロトコルであり，Yale大学で開発された［16］。CASではLDAPサーバと直接通信するのはCASサーバ（名古屋大学では情報連携基盤センターに設置されている[3]）のみであり，CASクライアント（学内の情報サービス）はユーザと，あるいはCASサーバと通信する。また，ユーザ認証は，ユーザとCASサーバ間で行われ，CASサーバからCASクライアントへは，そのユーザがすでに認証を受けているかどうかという情報が送られるのみである。そのため，パスワードなどの通信内容を保護するためにhttpsにしなければならないのはユーザとCASサーバの間だけとなり，情報サービスプロバイダがサーバ証明書（SSL証明書）を取得する必要がなくなる。

CASクライアントを構築するためのモジュールやサンプルプログラムはApacheやPerl，Java，PHPなど多くの環境や言語用のものが公開されているので，新規の情報サービスを構築する際や，既存の情報サービスをSSO化する際などに参考になるはずである［18］。

3　名古屋大学のCASはYale大学で開発されたものを改造してあり，認証のみならず，認可の機能も有する［17］。

Ⅳ．おわりに

本連載では4回にわたって，情報連携基盤センターに設置されているLDAPサーバを利用する方法を紹介してきた。このLDAPサーバを利用することにより，大学構成員に情報サービスを提供する場合にはユーザ認証や，ユーザ情報の管理の手間を省くことができる。情報サービスを提供している方や，提供を予定している方は本連載をご参考にしていただければ幸いである。

参考文献

［1］ http://www.linux.or.jp/JF/JFdocs/LDAP-Implementation-HOWTO/pamnss.html

［2］ 稲地稔：“OpenLDAP入門―オープンソースではじめるディレクトリサービス―”，技術評論社，東京，2003

［3］ http://securitytracker.com/alerts/2005/Aug/1014788.html

［4］ http://us3.samba.org/

［5］ http://www.samba.gr.jp/

［6］ 武田保真：“徹底解説　Samba LDAPサービス構築”，技術評論社，東京，2004

［7］ http://www.microsoft.com/japan/windows/sfu/

［8］ http://www.co-conv.jp/

［9］ http://pgina.xpasystems.com

［10］ http://www.zope.org/

［11］ http://zope.jp/

［12］ http://www.zope.org/Control_Panel/Products/LDAPUserFolder/Help/Add.stx

［13］ http://www.xoops.org/

［14］ 上田修子：“XOOPSによるポータルサイト構築”，秀和システム，東京，2005

［15］ http://jp.xoops.org/

［16］ http://www.yale.edu/tp/auth/

［17］ 梶田将司，内藤久資，小尻智子，平野靖，間瀬健二：“CASによるセキュアな全学認証基盤の構築”，名古屋大学情報連携基盤センターニュース（第12号），4，3，pp.179-187，2005.08

［18］ http://tp.its.yale.edu/tiki/tiki-index.php?page=CasClients

（ひらの　やすし：名古屋大学情報連携基盤センター大規模計算支援環境研究部門）