phpによる認証

概要

phpアプリからLDAPにアクセスして認証を行う場合の構築例を記述する。webサーバのOSはRedHat Enterprise ES3、httpdはapacheを使用する。

主な関数

LDAPへアクセスする手段は、web認証モジュールの他に、phpのLDAP関連関数などの各種APIが存在する。phpの場合における、LDAP接続の基本的な関数は以下の通り。

No	関数名	概要
1	ldap_connect()	セッション(LDAPサーバとの接続単位）を確立する。この関数でリンクIDを取得する。
2	ldap_bind()	ユーザDNとパスワードを指定して認証（バインド）を行う。引数にリンクID、ユーザDN、パスワードを指定する。
3	ldap_unbind()	アンバインドする。

上記ldap_connectを最初に呼び出し、LDAPサーバを指定してセッションを確立する。（実際にはまだ接続されない）
このときに取得したリンクIDで、バインドその他の処理を進めていく。ユーザに認証を行わせる場合は、formなどを使用してユーザからの入力情報を取得し、それをldap_bind関数に代入する処理となる。

バインド後は、検索関数を使用して配列にLDAPのエントリを取り込んだり、更新・追加・削除関数を使用してLDAPのエントリに書き込みすることができる。LDAPへアクセスするときの権限はバインドしたDNの持つ権限となる。複数のDNでバインドし、場合によってリンクIDを使い分ける等の処理も可能。また、webアプリの画面遷移時にバインドした内容を記憶するため、phpのセッション管理関数を使用する場合もある。

管理者用アプリの例

phpを使ったLDAP管理者向けのwebアプリを構築している。

URL:https://www.kogaku.kyoto-u.ac.jp/ldap/index.html
ソース: ldap.tar.gz

機能概要は以下の通り。

- ユーザ認証を行いログインする。
- ログイン後は認証ユーザの権限でLDAPサーバにアクセスできる。

- 表示内容はLDIF形式とし、各エントリのDNをクリックして次の階層に進める。
- 権限に応じてエントリの編集も可能。
- 編集は「LDAP Edit」から該当エントリが表示されている画面までツリーをたどり、
  「変更」ボタンを押す。上部フォームにエントリのLDIFが表示されるので、それを編集して
  「追加・更新」する。

View Edit