工学部･工学研究科ディレクトリサービス概要

概要

LDAPデータベースを使用して「ディレクトリサービス」のシステムを構築します。

ディレクトリサービスの一例として、「住所録」サービスがあります。

例：
カリフォルニア・サンタバーバラ大学　http://www.ucsb.edu/
MIT http://web.mit.edu、http://web.mit.edu/referencepubs/directories/toc.html
スタンフォード大学 http://www.stanford.edu/

webとLDAPを組み合わせて教職員の検索システムを実現しています。

ディレクトリサービスとは一種のデータベースです。このデータベースに組織や構成員のデータを格納することで、組織や個人を識別する必要のあるさまざまなアプリケーションを一元的なデータのもとで開発できるようになります。工学部・工学研究科ではディレクトリサービスの中核としてopenLDAPを使用し、それを利用するアプリとして主にphpなどで記述されたwebアプリを開発することで、以下のようなシステムを構築します。

システム	内容
教職員データベース	教職員の基本情報（氏名・所属・肩書き・内線番号など）をwebページから検索して表示することができる。
メーリングリスト自動生成	データベースから自動的にメーリングリストを生成する。所属組織や役職ごとなど、いくつかの基準をもとに分類して作成する。
委員会掲示板アクセス管理	委員会掲示板（webページ）へのアクセス権を管理する。アクセスできる人は自分のID（KEID：後述）とパスワードで認証する。
webアンケート	web上でアンケートを行うシステムを作成する。アンケート対象者のみがアクセスできるように制御する。また、回答者を一意に識別して多重回答制限などの制御を行う。
全学共通教育情報化システムとの融合	高等教育研究開発推進機構で進めている全学共通教育情報化システムのアカウント管理を、本基本認証を用いてできるかどうか検討する。（できればうまく乗せて動かしたい）
webページアクセス制御	webページへのユーザ認証によるアクセス制御を、一意のIDとパスワードで行う。webページとは、上記に挙げたシステム以外の任意のものを指し、そのweb管理者はアクセス可能なユーザリストを認証システムを使用して管理する。アクセスできる人は自分のIDとパスワードで認証する。
データの更新	登録データの更新をweb経由で行う。更新は人事担当者や本人が行い、それぞれ適切なアクセス権を設定する。

※なお、現時点では、主にweb利用に伴うユーザ認証を念頭に開発を進めます。UNIXのシステムアカウントや、Sambaアカウント情報などの統合については、現時点では考慮していません。（より複雑となるため）

LDAPサーバへのアクセスは常にwebサーバを介して行うこととします。LDAPにより一意に管理されたIDとパスワードを使用して、各webサービスを利用できます。

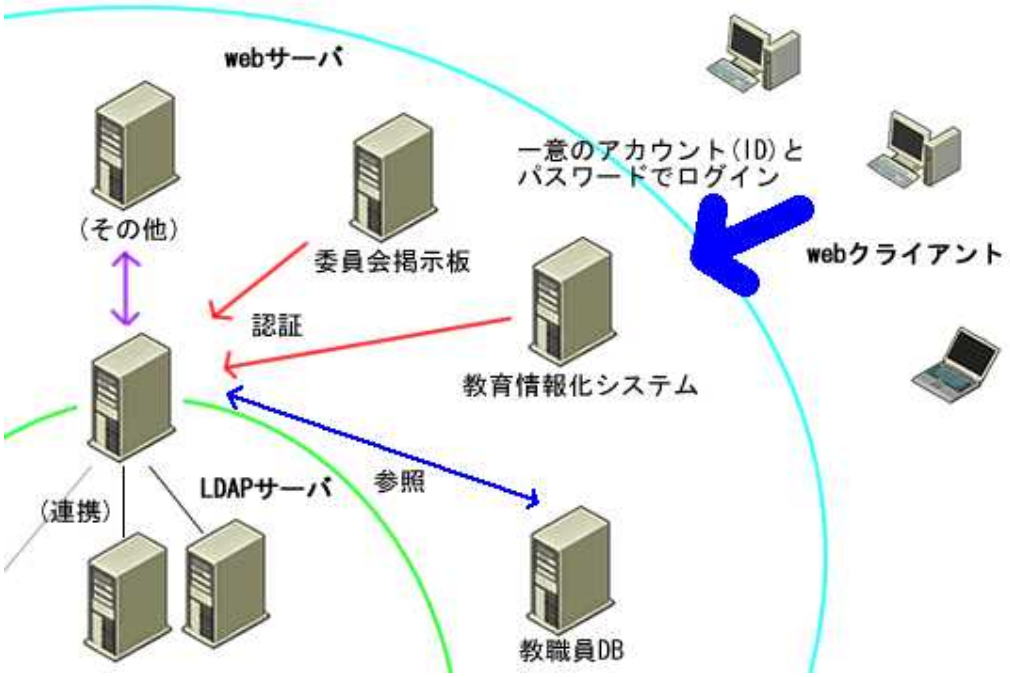

図　LDAPサーバとwebサーバの関連

各webサーバでは、LDAPサーバへアクセスするための設定が必要となります。設定内容は各webサーバの目的や使用しているソフトウェアに依存します。本ドキュメントでは主に、LDAPサーバ自体の構成・データ構成・それらを利用するための手順、およびwebサーバでアクセスする場合の実装例をいくつか記述します。各webサーバ（サービス）の提供者は、本ドキュメントを参照して適切なアクセス設定を行う必要があります。

運用に関するポリシー

- データベースで扱う情報
  職員録に記載されている教職員や組織の情報とします。学生の情報は扱いません。
- KEIDについて
  個人に対して１対１で割り当てられる識別記号を儲け、KEIDと呼ぶこととします。KEIDはアルファベット３文字＋数字４文字で構成され、アルファベットは大文字・小文字を区別しません。
  KEIDとパスワードにより認証を行います。発行についてはKEIDの重複が起こらないよう、職員証番号から一意に生成します。生成にはメディアセンターで使用しているアルゴリズムと同じものを使用します。

KEID	職員証番号から生成。小文字アルファベット３文字＋数字４文字。アルファベットは大文字・小文字を区別しない。

- データの更新や維持管理
  データの更新を誰が行うのか、以下のように定めます。

個人の	(1)各事務担当者（専攻事務等）あるいは(2)本人。個人データ内の属性ごとに(1)(2)を別途定

データ	めます。指針としては、姓・名などの基本的な人事情報は(1)、メールアドレス、ホームページURLなど付加的な情報は(2)。
組織のデータ	(1)総務掛あるいは(2)その組織配下に属する人。属性ごとに(1)(2)を別途定める。指針は「個人のデータ」と同様。

なおデータの更新手続きは、web画面での作業となります。

- 教職員データベースのWeb公開について
  データベースへの登録情報は、項目を限定した上でホームページを通じて公開します。表示する項目は別途定めます。認証されたユーザであるかどうか、学内からのアクセスか否か、により表示する項目を制御します。また、メールアドレスなどの一覧表示は名簿業者などに利用されやすいので一般的に避けます。

画面遷移例：検索 → インデックスとなる項目のみを一覧表示 → ある項目をクリック → 個別の情報を表示

運用モデル

運用に関わる人々を６つの立場に分けて、それぞれの役割と関連を考えると以下の通りとなります。

(1)LDAP管理者
LDAPのサーバ管理を行う。
初期情報の入力作業を行う。
各web管理者に対し、BindDNとパスワードを発行して管理する。
各web管理者に対し、LDAPサーバへのアクセスAPI仕様や接続例などの技術情報を開示する。

(2)KEID発行者
KEID利用（希望）者に対して登録を受けつけ、KEIDを発行する。
同じ人に重複発行しないようにする等、KEIDの管理をする。

(3)各web管理者
LDAPサーバを利用、あるいはユーザI/Fとなるwebアプリを開発・運用し、他の５者に対して目的に応じて提供する。
[例]ユーザ新規登録、エントリ情報編集、委員会ページ、住所録、その他認証が必要なwebサイト等

(4)KEID利用者
各web管理者の提供するwebアプリをKEIDに与えられた権限で利用する。
自らの個人エントリの内容を編集する。

(5)組織・個人エントリ情報メンテナンス担当者
組織エントリ(ou=organization配下）、個人エントリ（ou=people配下）の情報を編集し、正しい状態に維持する。

(6)web閲覧者（学内外の一般web利用者）
教職員データベースなどの検索システム（webアプリ）を制限された範囲で利用する。

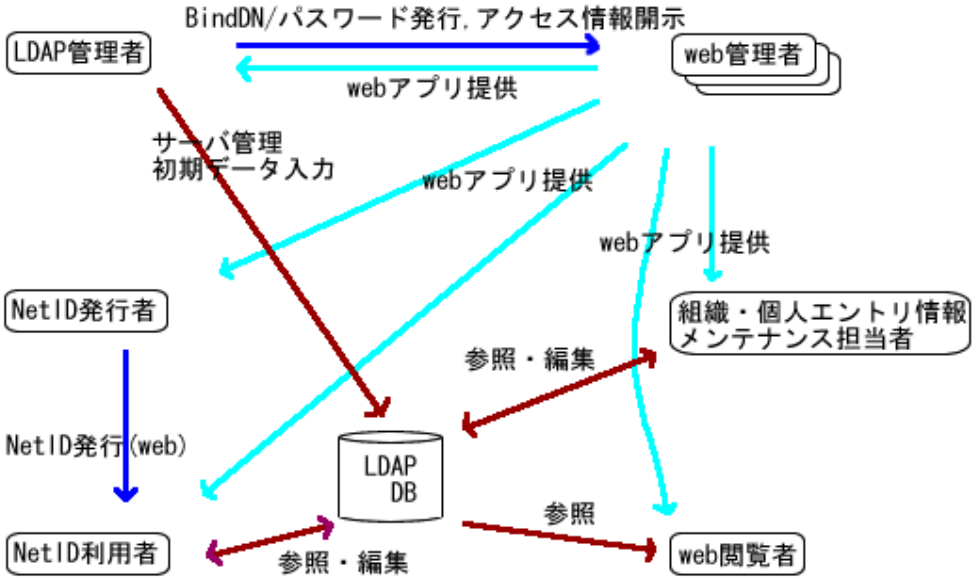

図　役割と関連

工学研究科の場合、実際の担当は以下のようになります。

役割	担当	備考
LDAP管理者	附属情報センター	
KEID発行者	附属情報センター	
各web管理者	基本的なwebアプリは附属情報センター	他は任意
KEID利用者	工学部・工学研究科の教職員	
組織・個人エントリ情報メンテナンス担当者	事務担当者、総務掛、及び各KEID利用者	
web閲覧者	学内外の一般web利用者	

View Edit