格納する情報の種類･項目

情報の種類

LDAPデータベースに格納する情報の種類は主に以下の4種類とします。

- 組織の情報
- 個人の情報
- 管理用ユーザの情報
- 管理用グループの情報

格納される属性の名前や型はLDAPにあらかじめたくさん定義されているので、それらの中から必要なものを組み合わせて情報を構成します。それぞれの中身のうち、代表的な項目は以下の通りです。

組織の情報

部局内の各組織についての情報を格納します。運用で使用する主なものは以下の通り。

識別記号
: 組織を識別するための記号。「00000」～「99999」の5桁の数字とし、同じ階層内で一意であればよい。

組織の名称
: 職員録の記述を参考とする。英語と日本語で登録できる。

郵便番号、所在地（住所）、電話番号、ＦＡＸ番号
: 複数の登録が可能。英語と日本語で登録できる。

キャンパス、クラスター、棟、部屋番号など
: 複数の登録が可能。英語と日本語で登録できる。

組織のメールアドレス、ホームページ等のアドレス
: 複数の登録が可能。

備考
: その他、記述事項などがあれば記述する。複数の登録が可能。英語と日本語で登録できる。

格納する組織は大小問わず登録します。つまりＸ専攻Y講座Z分野という組織がある場合は、X専攻・Y講座・Z分野、それぞれを１つの組織とみなし、独立したデータとして登録します。A課B掛なども同様です。組織間の関係はLDAPの階層構造として表現します。

個人の情報

部局内の各個人についての情報を格納します。実際の人間に1対1で対応します。 運用で使用する主なものは以下の通り。

KEID

個人の識別記号。学内で重複しない記号を割り当てる。生成する際は職員証番号から生成したIDを用いる。（メディアセンターと同様の方式）このIDは英数字7桁で、最初の3桁は小文字アルファベット、次の4桁は数字となる。ただし、認証時はアルファベットの大文字・小文字を区別しない。KEIDは原則的に学内へは公開すべきものとして扱う。また、職員証番号が無い人は別の方式で擬似的なKEIDを作成する。

姓、名

それぞれ、アルファベット・漢字・及びひらがなで登録する。

一般名

氏名をアルファベット、漢字、及びひらがなで登録する。日本人名の場合、普通は「姓(半角スペース)名」となる。外国人などの場合、姓・名・ミドルネームなどの組み合わせとなる場合がある。

パスワード

認証で使用する個人ごとのパスワード。

郵便番号、所在地（住所）、電話番号、ＦＡＸ番号

複数の登録が可能。所在地は英語と日本語で登録できる。

キャンパス、クラスター、棟、部屋番号など

複数の登録が可能。英語と日本語で登録する。

職名

教授、主任、室員等、その人の一意の職名。複数の登録が可能（基本的には１つのみ登録）。英語と日本語で登録する。

関係区分

次のうちから選択して登録する。教員、職員、 学生、退職した教職員または卒業生、学内関係者、外部関係者、その他従業員。関係区分によるアクセス制御等が可能となる。

所属組織のDN

所属する組織のDNを登録する。複数の登録が可能。職員録掲載の所属組織の他に、委員会などの内部組織についても登録する。

所属組織ごとの役職

委員長、センター長、委員、学科長等、組織ごとの役職を登録する。所属組織のDNと順に1対1で対応するものとする。

メールアドレス、ホームページ等のURL

複数の登録が可能。

ユーザID（ニックネーム）

ニックネーム。~~KEIDだけでは不便な場合もあるので予備的に使用する。webなどでネットIDの代わりにユーザIDを入力し、一致するエントリのネットID一覧をいったん表示して選択させ、そのネットIDとパスワードで認証を行うような手続きも可能となる。~~->セキュリティホールとなるためこのような使用方法は再検討が必要

大学間NetID

大学間での認証を行えるようにするため、一意の名前を格納する。KEID@kyoto-u.ac.jp。KEIDから自動生成する。

不可視とする属性名

公開したくない属性を指定すると、ウェブ上などで非表示となる。この属性の扱いはウェブアプリに依存し、LDAPでの制限などは行わない。

メンバーとして所属するグループのDN
所属組織とは別に、メンバーとして所属するグループのDNを登録する。グループは以下の管理用グループとして定義しておく。（静的グループから動的グループへの自動反映も参照）

所有者として所属するグループのDN
所属組織とは別に、所有者として所属するグループのDNを登録する。グループは以下の管理用グループとして定義しておく。（静的グループから動的グループへの自動反映も参照）

備考
その他、記述事項などがあれば記述する。複数の登録が可能。英語と日本語で登録できる。

属性値を複数持ち、他の属性と順に対応することで意味を成すようなものについて、LDAP自体では順番を管理しません。それらを入力したり表示したりするwebアプリ側で正しく扱えるように実装する必要があります。また「大学間NetID」のように「自動生成」するものも、webアプリ側で自動生成します。

管理用ユーザの情報

管理用ユーザとは、LDAPにアクセスするwebアプリなどがバインド用に使用するエントリのことです。LDAPにアクセスする各アプリについて1対1に割り当てます。エントリを作成後は、webアプリ管理者にDNとパスワード(userPassword)を連絡します。

アプリケーション名
webアプリなど、LDAPにアクセスするアプリケーションの名称を登録する。部局内で一意とし、名称はLDAP管理者が定める。

パスワード
認証で使用するパスワード。

備考
その他、記述事項などがあれば記述する。複数の登録が可能。英語と日本語で登録できる。

管理用グループの情報

管理用グループには2つの役割があります。1つはLDAPサーバへのアクセス権を設定するために使用します。LDAP管理者がユーザやアプリで使用するエントリをグループに分類します。各グループに対してあらかじめLDAPサーバへのアクセス権が設定されており、グループに分類することで各ユーザのアクセス権を設定できます。もう1つは、webサイトなどに対して同じアクセス権を持たせたい人たちを、まとめてグループ化するのに使用します。このようにして使用するグループは一般ユーザに公開されており、グループ編集用のインタフェースを介して、一般ユーザがそれぞれのアプリに関するアクセス権を編集できます。（編集・参照可否に関する条件などの詳細は別途記述）管理用グループの各エントリには、そのグループに所属する管理用ユーザや個人のDNを列挙します。一般に、管理用ユーザや個人は複数の管理用グループに所属します。

グループ名
グループ名。部局内で一意とし、名称はLDAP管理者が定める。

メンバー
グループに所属するメンバー（管理用ユーザ、その他）のDNを登録する。複数の登録が可能。メンバーには当該グループのエントリに対する読み込み（参照）権を与える。

グループ所有者
グループの所有者とするメンバー（管理用ユーザ、その他）のDNを登録する。複数の登録が可能。所有者には当該グループのエントリに対する書き込み（編集）権を与える。

備考
その他、記述事項などがあれば記述する。複数の登録が可能。英語と日本語で登録できる。

グループ分けする理由は、アクセス制御にあります。webアプリなどの管理用ユーザについては、ユーザごとにアクセス制御を定義するのではなく、管理用グループに対して定義します。グループ単位で定義しておき、そのグループに管理用ユーザを登録したり解除したりすることで、柔軟にアクセス制御ができるようになります。また、個人からなるグループについては、グループのオーナーがメンバーを追加したり削除したりすることで、特定のwebサイトなどに対するアクセス権を付与したり削除したりできます。

静的グループから動的グループへの自動反映

LDAPではグループという概念を2つに分けて考えることが出来ます。

静的グループ
あるグループに所属するメンバーや所有者を、グループエントリの要素として列挙して表す。

動的グループ
あるグループに所属するメンバーや所有者を、各メンバーそれぞれのエントリに設けた属性で表す。属性値には所属するグループへのDNを格納する。所属するグループのエントリは別途作成しておく。

基本的にグループは静的メンバーとして登録しますが、場合によっては動的なグループのほうが良い場合があります。そのため、静的なグループの一部を動的なグループに自動反映する（静的なグループのメンバーや所有者を調べて、各メンバー等のエントリにそのグループへ所属情報を書き込む）処理を行います。