DIT･エントリ仕様

DITの構造

DITの構造と各階層のエントリが持つオブジェクトクラスは以下の通りとする。

↑上位	**dc=jp**			
	dc=ac			
	dc=kyoto-u objectClass: dcObject objectClass: organization			
	o=kogaku objectClass: organization objectClass: eduOrg objectClass: kyoto-uEduOrg			
	ou=organization objectClass: organizationalUnit objectClass: kyoto-uEduOrgUnit	**ou=people** objectClass: organizationalUnit objectClass: kyoto-uEduOrgUnit	**ou=users** objectClass: organizationalUnit objectClass: kyoto-uEduOrgUnit	**ou=groups** objectClass: organizationalUnit objectClass: kyoto-uEduOrgUnit
下位↓	**ou=（組織記号 注1）** ...（階層構造）	**uid=(KEID 注2)** objectClass: top objectClass: person objectClass: organizationalPerson objectClass: inetOrgPerson objectClass: eduPerson ...（フラット構造）	**cn=（アプリケーション名）** objectClass: applicationProcess objectClass: shadowAccount ...（フラット構造）	**cn=（グループ名）** objectClass: groupOfUniqueNames ...（階層構造）

注1: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。エントリを登録する際に重複しない記号を担当者等が任意に決定する。
注2:学内で一意であること。職員証番号から生成した記号を用いる。職員証が無い人については次の方式で生成する。

"X" & md5生成関数(職名 & md5エンコード関数(職名 & 姓ローマ字 & 姓漢字 & 姓よみ & 名ロー

マ字 & 名漢字 & 名よみ)
（md5エンコード関数に入力する文字コードはUTF-8とする。）

cn=(グループ名)の構造は最大２段構造とする。すなわち、以下の２パターンのうち、いずれかとなる。
(1)cn=（グループ名Ａ）,cn=（グループＢ）,ou=groups,o=kogaku,dc=kyoto-u,dc=ac,dc=jp
(2)cn=（グループ名Ａ）,ou=groups,o=kogaku,dc=kyoto-u,dc=ac,dc=jp

(1)のパターンはwebアプリケーションなどが利用するときに必要となるデータをLDAPで持つために使用される。webアプリごとにグループＢのカテゴリでディレクトリを作成し、その下に必要なデータ（主にグループのエントリ）をおくようになる。あくまでもアプリ用なので、ACLなどには使用しない。
(2)のパターンは、LDAP自体へのアクセス制御に使用される。(2)のように定義されたエントリがＡＣＬに直接記述される。

エントリの要素

各エントリに格納する属性は以下の通り。
説明欄に記述のある属性は教職員データベースで使用する。その他の属性は、基本的に使用しないこと。なおアクセス制御については別途記述。

[ou=（識別記号）,ou=organization,o=kogaku,dc=kyoto-u,dc=ac,dc=jp]

属性（またはオブジェクトクラス） **太字は必須属性**	説明	備考
(organizationalUnit)		
ou	識別記号。「00000」～「99999」の5桁の半角数字。「01」や「123」は不適切。必ず5桁であること。	同じ階層内で一意であればよい。エントリを登録する際に重複しない記号を担当者等が任意に決定する。
userPassword		
searchGuide		
seeAlso		
businessCategory		
x121Address		
registeredAddress		
destinationIndicator		
preferredDeliveryMethod		
telexNumber		

teletexTerminalIdentifier		
telephoneNumber	電話番号	複数登録可 ハイフンは含まず、基本的に市外局番から登録。
internationaliSDNNumber		
facsimileTelephoneNumber	FAX番号	複数登録可 ハイフンは含まず、基本的に市外局番から登録。
street		
postOfficeBox		
postalCode	郵便番号	複数登録可
postalAddress	所在地、住所	postalAddress:英語 postalAddress;lang-ja:日本語 複数登録可
physicalDeliveryOfficeName	キャンパス、クラスター、棟、部屋番号など	postalAddress:英語 postalAddress;lang-ja:日本語 複数登録可
st		
l		
description	備考	description:英語 description;lang-ja:日本語 複数登録可
(kyoto-uEduOrgUnit)		
cn	組織の名称、一般的な名称	cn:英語 cn;lang-ja:日本語 cn;lang-ja:かな
kyoto-uEduOrgUniqueNumber	部局ごとに割り当てられた学内で一意の識別番号。 未使用	ダミー値「0」固定とする。
kyoto-uEduOrgUnitUniqueNumber	組織ごとに割り当てられた学内で一意の識別番号。 未使用	ダミー値「0」固定とする。

kyoto-uEduOrgAcronym		
mail	メールアドレス	複数登録可
labeledURI	ホームページ等のURL	複数登録可

[uid=(KEID),ou=people,o=kogaku,dc=kyoto-u,dc=ac,dc=jp]

属性（またはオブジェクトクラス） **太字は必須属性**	説明	備考
(person)		
sn	姓	sn:アルファベット sn;lang-ja:漢字 sn;lang-ja:かな 漢字についてはopenldapで扱える漢字のみ扱う。その他の漢字は適宜修正したものが登録されているとする。
cn	一般名（姓、名、その他ミドルネームなどの組み合わせ）	cn:アルファベット cn;lang-ja:漢字 cn;lang-ja:かな 漢字についてはopenldapで扱える漢字のみ扱う。その他の漢字は適宜修正したものが登録されているとする。
userPassword	個人のパスワード。 SMD5形式で暗号化したものを格納する。	SMD5形式はldappasswdコマンドのデフォルト動作。
telephoneNumber	電話番号	複数登録可 ハイフンは含まず、基本的に市外局番から登録。
seeAlso		
description	備考 専門分野、電話番号の親展or共用等。	description:英語 description;lang-ja:日本語 複数登録可
(organizati		

onalPerson)		
title	所属組織ごとの役職名（委員長、センター長、専攻長、学科長、等）	title:英語 title;lang-ja:日本語 複数登録可 eduPersonOrgUnitDNに対応する。 2005.1.4現在、事務員でこの属性値をもつケースは無く、教員のみがこの属性値を持つ可能性がある。
x121Address		
registeredAddress		
destinationIndicator		
preferredDeliveryMethod		
telexNumber		
teletexTerminalIdentifier		
telephoneNumber		(personオブジェクトと同様)
internationaliSDNNumber		
facsimileTelephoneNumber	FAX番号	複数登録可 ハイフンは含まず、基本的に市外局番から登録。
street		
postOfficeBox		
postalCode	郵便番号	複数登録可
postalAddress	所在地、住所	postalAddress:英語 postalAddress;lang-ja:日本語

		複数登録可
physicalDeliveryOfficeName	キャンパス、クラスター、棟、部屋番号など	postalAddress:英語 postalAddress;lang-ja:日本語 複数登録可
ou		
st		
l		
(inetOrgPerson)		
audio		
businessCategory	職名（教授、助教授、講師、助手、部長、課長、掛長、専門職員、主任等）	businessCategory:英語 businessCategory;lang-ja:日本語 複数登録可 大学としての本人の職名なので、eduPersonPrimaryOrgUnitDNに対応すると言える。通常は１つのみ登録する。
carLicense		
departmentNumber		
displayName		
employeeNumber		
employeeType		
givenName	名	sn:アルファベット sn;lang-ja:漢字 sn;lang-ja:かな 漢字についてはopenldapで扱える漢字のみ扱う。その他の漢字は適宜修正したものが登録されているとする。
homePhone		
homePostalA		

ddress		
initials		
jpegPhoto		
labeledURI	ホームページ等のアドレス	複数登録可
mail	メールアドレス	複数登録可
manager		
mobile		
o		
pager		
photo		
roomNumber		
secretary		
uid	KEID	職員証番号から生成したID。小文字アルファベット3文字+数字4文字
userCertificate		
x500uniqueIdentifier		
preferredLanguage		
userSMIMECertificate		
userPKCS12		
(eduPerson)		
eduPersonAffiliation	関係区分（faculty 教員、staff 職員、student 学生、alum 名誉教授または卒業生、extra 派遣職員、member 学内関係者、affiliate 外部関係者、employee その他従業員、laboratory 研究室）	複数登録可 eduPersonAffiliation:英語 「faculty,staff,student,alum,extra,member」は、ディレクトリアクセスについて、それぞれほぼ同じ権限を持つ。「member」は他の3つのどれにも当てはまらない場合に適用する。「affiliate,employee」は、ディレクトリアクセスについて、それぞれほぼ同じ権限を持つ。

		運用時はfaculty,staff,alum,extra,member,laboratoryのみを使用することとし、それぞれの意味は次のとおりとする。 faculty：教員 staff：職員（事務員・技術職員） alum：名誉教授（通常は検索の対象外とする） extra：派遣職員など（学外からは検索の対象外とする） member：非常勤職員など affiliate：退職者、転出者（通常は検索の対象外とする） alumとaffiliateに登録した場合はuserPasswordを無効なものに設定すること。 laboratory：研究室の共通アカウントで学生も利用可能（学外からは検索の対象外とする）
eduPersonNickname	ニックネーム	ニックネーム。自由に登録できる。~~直接KEIDを入力して認証する以外に、登録したユーザIDを入力すると、該当するKEIDを一覧表示し、そこからKEIDを選択してパスワード認証するようなインタフェースも作成できる。~~->このような使用方法はセキュリティホールとなるため再検討が必要
eduPersonOrgDN	所属部局のDN	工学部・工学研究科の場合は o=kogaku,dc=kyoto-u,dc=ac,dc=jp となる。
eduPersonOrgUnitDN	所属組織のDN (ou=AAAAA,ou=organization,o=kogaku,dc=kyoto-u,dc=ac,dc=jp)	複数登録可 人事管理上の所属以外に所属している組織（兼任等）、及び内部組織(委員会等) 内部組織のツリーもou=organization以下に設ける。
eduPersonPrimaryAffiliation		
eduPersonPrincipalName	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@kyo	KEIDから自動生成。

	to-u.ac.jp	
eduPersonEntitlement		
eduPersonPrimaryOrgUnitDN	人事管理上の所属組織のDN (ou=AAAAA,ou=organization,o=kogaku,dc=kyoto-u,dc=ac,dc=jp)	人事管理上の所属。
(kyoto-uEduPerson)		
kyoto-uEduPersonOIN		
kyoto-uEduPersonBirthDate		
kyoto-uEduPersonLIN		
kyoto-uEduPersonPrivate	不可視とする属性名	複数登録可 電話番号、FAX番号、メールアドレス、ホームページURL、所在地などの情報のうち、公開しないものの属性名を格納する。Webアプリなどでこれを参照して表示制限などを行う。 なお、LDAPサーバではこの情報をアクセス制御のために使用しない。
kyoto-uEduPersonUniqueMemberOf	メンバーとして所属するグループのDN	複数登録可 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。これにより動的なグループを表現できる。通常は自動で登録される。
kyoto-uEduPersonOwnerOf	所有者として所属するグループのDN	複数登録可 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。これにより動的なグループを表現できる。通常は自動で登録される。

[cn=(アプリケーション名),ou=users,o=kogaku,dc=kyoto-u,dc=ac,dc=jp]

属性（またはオブジェクトクラス）太字は必須属性	説明	備考
(applicationProcess)		
cn	アプリケーション名	一意なアプリケーション名称
seeAlso		
ou		
l		
description	備考	description:英語 description;lang-ja:日本語 複数登録可
(shadowAccount)		
uid	アプリケーション名	cnと同様とする。
userPassword	パスワード SMD5形式で暗号化したものを格納する。	bindする際にパスワードを要求させるようにする。
shadowLastChange		
shadowMin		
shadowMax		
shadowWarning		
shadowInactive		
shadowExpire		
shadowFlag		
description		(applicationProcessと同様)

[cn=(グループ名),ou=groups,o=kogaku,dc=kyoto-u,dc=ac,dc=jp]

属性（またはオブジェクトクラス）太字は必須属性	説明	備考
(groupOfUniqueNames)		
cn	グループ名	
uniqueMember	メンバーのDN cn=(アプリケーション名),ou=users,o=kogaku,dc=kyoto-u,dc=ac,dc=j	グループの属性値を参照(read)できる。 複数登録可

	p cn=(ネットID),ou=people,o=kogaku,dc=kyoto-u,dc=ac,dc=jp 等	
owner	グループ所有者（管理者）のDN cn=(アプリケーション名),ou=users,o=kogaku,dc=kyoto-u,dc=ac,dc=jp cn=(ネットID),ou=people,o=kogaku,dc=kyoto-u,dc=ac,dc=jp 等	グループの属性値を変更(write)できる。 複数登録可
ou		
l		
description	備考	description:英語 description;lang-ja:日本語 複数登録可
(kyoto-uDynGroupOfUniqueMember)	uniqueMemberを動的グループとして自動反映させる	このobjectClassを持つエントリはuniqueMemberが動的なグループに自動反映される。
(kyoto-uDynGroupOfOwner)	ownerを動的グループとして自動反映させる	このobjectClassを持つエントリはownerが動的なグループに自動反映される。

複数登録可である項目の扱い

複数登録可である属性のうち、複数種類の属性が順に対応して意味をなすものについては、データの登録・参照規則を定める必要がある。これらのデータを扱うwebアプリは、以下にしたがって、登録・参照・更新などが正しく行えるようにすること。

- [ou=（識別記号）,ou=organization,o=kogaku,dc=kyoto-u,dc=ac,dc=jp]について

(1)郵便番号と所在地との対応は1対1とする。

例：

postalCode	postalAddress
postalCode1	postalAddress1
postalCode2	postalAddress2
___NULL___03	postalAddress3

postalCode4	___NULL___04
	postalAddress5

（注）「___NULL___」はアンダーバー３つ＋文字列「NULL」＋アンダーバー３つの文字列とする。
postalCodeの５つめは未定義（４つまでしか登録されていない状態）
この場合、参照時には「郵便番号と所在地」の情報が５つ定義されていることとして扱い、次のように対応させる。
「postalCode1 postalAddress1」
「postalCode2 postalAddress2」
「postalAddress3」
「postalCode4」
「postalCode5」

また、登録時にも上記のような対応関係が保存されるように、適当に「___NULL___(2桁の登録順番)」の値を設定する。(この場合postalCodeの５番目を「___NULL___05」としても良い）___NULL___の後に登録順番をつける理由は、同じ値をphp関数のldap_modifyなどで登録しようとするとエラーとなり登録できないためである。

postalCodeとpostalAddressの組をpostalCAで表すこととする。また、「1対1」という関係をR1で表し、
postCA=R1(postalCode, postalAddress)
と書く。

(2)「キャンパス、クラスター、棟、部屋番号など」と電話番号、FAX番号の対応は１対多とする。

例：

physicalDeliveryOfficeName	telephoneNumber	facsimileTelephoneNumber
physicalDeliveryOfficeName1	---01	facsimileTelephoneNumber1
___NULL___02	telephoneNumber2	---02
___NULL___03	---03	facsimileTelephoneNumber3
physicalDeliveryOfficeName4	telephoneNumber4	facsimileTelephoneNumber4
	telephoneNumber5	---05

（注）「---」はハイフン３つ。電話番号、FAX番号は数値型のため、未定義の識別は「___NULL___(2桁の連番)」の代わりに「---(2桁の連番)」を用いる。
以降、簡単のため、それぞれ「___NULL___」「---」で表す。

この場合、参照時には「キャンパス、クラスター、棟、部屋番号など」の情報が２つ定義されていることとして扱い、次のように対応させる。
「physicalDeliveryOfficeName1 telephoneNumber2 facsimileTelephoneNumber1 facsimileTelephoneNumber3」
「physicalDeliveryOfficeName4 telephoneNumber4 facsimiletelephoneNumber5 TelephoneNumber4」

また、登録時にも上記のように１対多の登録ができるようにし、適当に「---」の値を設定する。

(1)と同様に関係式を使用して記述する。１対多の関係をR2、「無関係」の関係をR0とすると、
telfax = R0(telephoneNumber, facsimileTelephoneNumber)
physicalDeliveryOffice = R2(physicalDeliveryOfficeName, telfax)
となる。

(3)「郵便番号と所在地」と「『キャンパス、クラスター、棟、部屋番号など』と電話番号、FAX番号」の対応は１対多とする。
(1)(2)で関係を定義した属性のまとまりを、さらに関連付けして全体の関連とする。

例：

postalCA	physicalDeliveryoffice
postalCA1	physicalDeliveryoffice1
___NULL___02	physicalDeliveryoffice2
postlCA3	___NULL___03
___NULL___04	physicalDeliveryoffice4
	physicalDeliveryoffice5

（注意）「___NULL___」はそれぞれの構成要素がすべて「___NULL__」または「---」となっていることを示す。

この場合、参照時には「郵便番号と所在地」の情報が２つ定義されていることとして扱い、次のように対応させる。
「postalCA1 physicalDeliveryoffice1 physicalDeliveryoffice2」
「postalCA3 physicalDeliveryoffice4 physicalDeliveryoffice5」
すなわち、
office = R2(postalCA, physicalDeliveryoffice)
となる。

(4)英語・日本語の対応は1対1とする。

上記までの関係の前提として、英語と日本語の両方が使用できる属性はすべて英語と日本語が1対1に対応するものとする。
attribute = R1(attribute, attribute;lang-ja)

(5)すべて「___NULL___」または「---」のデータの扱い

参照時には無視して扱うこととする。つまり、表示上はこれらのデータが存在してもしなくても結果は変わらないものとする。

- [uid=(KEID),ou=people,o=kogaku,dc=kyoto-u,dc=ac,dc=jp]について

(1) 上記と同様に関係式で定義する。

attribute = R1(attribute, attribute;lang-ja)　ただし、attribute=snおよびattribute=givenName以外
postCA=R1(postalCode, postalAddress)
telfax = R0(telephoneNumber, facsimileTelephoneNumber)
physicalDeliveryOffice = R2(physicalDeliveryOfficeName, telfax)

office = R2(postalCA, physicalDeliveryoffice)
OrgUnitTitles = R2(eduPersonOrgUnitDN, title)

(2)姓（日本語）、名（日本語）の対応は定義順ごとに1対1とする。

例：

sn;lang-ja	givenName;lang-ja
山田	かほる
やまだ	

この場合、参照時には「名」の情報が２つ定義されていることとして扱い、次のように対応させる。
「山田 かほる」
「やまだ かほる」

この場合、 givenName;lang-jaの２番目が「___NULL___02」であっても同じ処理となる。

この関係をR4とすると
sn_givenName;lang-ja = R4(sn;lang-ja, givenName;lang-ja)
となる。

なお、R4は新たに「識別フィールド」を一時的に用いると、R2の組み合わせで表現できる。

sn;lang-ja	givenName;lang-ja	ID
山田	かほる	id1
やまだ		id2

このとき、
R2(sn;lang-ja, ID)
R2(givenName;lang-ja, ID)
となる。

アルファベット変換規則

ひらがなからアルファベット（ローマ字）への変換規則については、アルファベット変換関数に従う。変換関数はphpおよび設定ファイルで構成されている。

内容は web_directory_Roma.zipを参照。
なお、設定ファイルのフォーマットはCannaの変換テーブルに準拠している。

漢字変換規則

UTF-8で扱える漢字以外の漢字については、以下のように変換して登録することとする。

変換前	変換後

スキーマ仕様

以下のオブジェクトクラスについては、スキーマを新たに追加する。

eduPerson：NET@Eduで記述されている内容を元に eduPerson.schemaを作成。

kyoto-uEduPerson：FEIDEで記述されている内容を参考に京都大学用に改造して作成。&ref(): File not found: "kyoto-uEduPerson.schema" at page "Service/LDAP0.5/70000";に格納。
kyoto-uEduOrgUnit：同様。

ただし、kyoto-uEduperson.schemaのOID（属性に対するグローバルなID）については、仮のIDとする。正式にはISOへの登録申請が必要となる。IANAから無料でOID登録ができる。