UPKI 認証連携基盤 属性仕様（案）

1. 概要

本属性仕様は，「UPKI 認証連携基盤」において，認証の際に利用する属性情報について，その仕様を定めたものである。

この属性仕様では，「UPKI 認証連携基盤」に参加する各大学の IdP に格納する属性情報において，基本的な定義を表している。

本属性仕様は，SWITCH，InCommon，UK Access Management 等，海外の Federation において実績のある Service Provider（サービスプロバイダ）が利用する属性情報を考慮に入れ検討を行った。

利用する属性情報は，利用する SP によって，様々異なってくることから，「UPKI 認証連携基盤」では，今後，SP として利用するアプリケーションを検討しながら，本属性仕様について拡張していくことが重要である。

2. 属性情報一覧

No	属性名称		データ例	実装
1	Principal Name (eduPersonPrincipalName)	ユニーク ID （主要名）	12345678@testUniv_A.ac.jp	必須
2	Country （c）	国名	jp	推奨
3	Domain Component (dc)	ドメイン名	ac	推奨
4	User ID (uid)	ユーザ ID	12345678	推奨
5	CommonName (cn)	一般名	jouhou_taro	推奨
6	Surname (surName)	姓	jouhou	推奨
7	Kanji Surname (upkiSurName) -> lang-ja オプションで対応	姓 （日本語）	情報	推奨
8	Given name (givenName)	名	taro	推奨

No	属性名称		データ例	実装
9	Kanji Given name (upkiGivenName) -> lang-ja オプションで対応	名 （日本語）	太郎	推奨
10	Display Name (displayname)	表示名	jouho_taro	任意
11	Kanji Display Name (upkiDisplayName) -> lang-ja オプションで対応	表示名 （日本語）	情報太郎	任意
12	E-mail (mail)	メールアドレス	upki@nii.ac.jp	推奨
13	Home organization (o)	所属組織	National institute of Infromatics	必須
14	Kanji Home organization (upkiOrganization) -> lang-ja オプションで対応	所属組織 （日本語）	国立情報学研究所	推奨
15	Organization path (eduPersonOrgDN)	組織単位	o=nii.dc=ac,c=jp	任意
16	Kanji Home organization type (upkiOrganizationType) -> lang-ja オプションで対応	所属機関タイプ （日本語）	短期大学	任意
17	Organization Unit (ou)	所属組織識別	upki	必須
18	Kanji Organization Unit (upkiOrganizationUnit) -> lang-ja オプションで対応	所属組織識別 （日本語）	理学部	推奨
19	Primary Organization Unit DN (eduPersonPrimaryOrgDN)	主要組織識別名	ou=test,o=Univ_A,dc=org	任意

No	属性名称		データ例	実装
20	Organizational unit path (eduPersonOrgUnitDN)	組織	ou=upki,o=nii,dc=ac,c=jp	任意
21	jpegPhoto （jpegPhoto)	写真データ	（写真データ）	任意
22	description (description)	備考	test_account	任意
23	Entitlement (eduPersonEnTitlement)	資格	urn:mace:dir:entitlement:common-lib-terms	推奨
24	TargetedID (eduPersonTargetedID)	ターゲット ID	13ac5b7d82fa	推奨
25	Affiliation (eduPersonAffiliation)	職種区分	staff	必須
26	Scoped Affiliation (eduPersonScopedAffiliation)	所属内区分	faculty@nii.ac.jp	任意
27	Preferred Language (preferredLanguage)	希望言語	jp	推奨
28	Gender (swissEduPersonGender)	性別	1 (Male)	任意
29	Date of birth (swissEduPersonDateofBirth)	生年月日	19730317	任意
30	Staff category (swissEduPersonStaffCategory)	職種	301(Administrative Personnel)	任意
31	Kanji Staff Category (upkiStaffCategory) -> lang-ja オプションで対応	職種 （日本語）	係長	任意
32	Business postal address (postalAddress)	職場住所	2-1-2 hitotsubashi tiyoda-ku tokyo	任意
33	Kanji business Postal address (upkiPostalAddress) -> lang-ja オプションで対応	職場住所 （日本語）	東京都千代田区一ツ橋 2-1-2	任意

No	属性名称		データ例	実装
34	Business phone number (telephoneNumber)	職場連絡先	81-3-9887-6543	任意
35	Home postal address (homePostalAddress)	自宅住所	1-1-1 kasumigaseki suginami-ku tokyo	任意
36	Kanji Home Postal address (upkiHomePostalAddress) -> lang-ja オプションで対応	自宅住所（日本語）	東京都杉並区霞が関 1-1-1	任意
37	Private phone number (homePhone)	自宅電話番号	+81 3 1234 5678	任意
38	Mobile phone number (mobile)	携帯電話番号	+81 90 1234 5678	任意

※水色部分は必須の属性項目を表している。

※lang-ja オプションの利用では，UTF-8 文字列を BASE64 エンコードしたデータで格納する。

3. 属性 Meta 情報と注釈

本仕様で規定する属性は，以下の Meta 情報により定義する。

概　　要	属性情報の概要
セマンティクス	当該属性の持つ意味
実装状況	【必須】：格納することが必要となる属性（UPKI 認証連携基盤に加入するサービスが必要とする属性） 【推奨】：強く格納することが望まれる属性（特別なユーザの認証等の用途に利用される属性） 【任意】：利用判断が任意である属性
利用目的	【認証・認可】：アクセスコントロールのために利用 【課金管理等】：課金管理のために利用 【付加的情報】：上記以外の利用目的で，ユーザに付加的な価値サービスを提供するために利用 【UPKI 利用】：UPKI 認証連携基盤内で利用する特別な属性値
属性起源	本属性値が定義されている源泉（例：RFC4519, eduPerson）
ＯＩＤ	オブジェクトクラスや LDAP で利用する構成要素を一意に指定するためのオブジェクト識別子（Object IDentifier）
属性構文	LDAP 属性構文(RFC 4517)に準じる。 【属性型】 Directory String 1.3.6.1.4.1.1466.115.121.1.15　Unicode (UTF-8)の文字列 IA5String 1.3.6.1.4.1.1466.115.121.1.26　ASCII 文字列 【照合順序】 caseIgnoreMatch 英字の大小文字，先頭・末尾の空白を無視し，連続する空白を 1 つの空白として照合 caseExactMatch 英字の大小文字，空白も考慮して照合
複数値	複数の値を設定することができるかどうか
参考例	属性情報の参考データ例

4. 属性情報定義

4.1. Principal Name (eduPersonPrincipalName)

概　　要	UPKI 認証連携基盤の中で，ユニークな個人の識別子（主要名）
セマンティクス	<unique-ID>@<domain> <unique-ID>：ユニーク ID 各 domain の中でユニークな ID でなければならない。各大学の共通 ID（学内統一 ID）等がこれに相当する。使用する文字列については ASCII 英数字（制御文字を除く）のみとし，日本語は使用不可とする。 <domain>：組織の識別子 利用者の所属する組織の識別子である。各大学の各 domain を持ち，フェデレーション内において一意であることが保証された値を持つ。既に登録されている，所属機関のインターネットドメイン名を利用することを推奨する。
実装状況	必須
利用目的	【認証・認可】
属性起源	eduPerson で定義済み
ＯＩＤ	1.3.6.1.4.1.5923.1.1.1.6
属性構文	【属性型】Directory String ユニーク ID 部分は最少 6 文字とし，属性値全体長は 256 文字までの値とする。 【照合順序】caseIgnoreMatch
複数値	ユニーク値であるため，複数値の設定は許可しない
参考例	1234567@testUniv_A.nii.ac.jp

4.2. Home Organization (o)

概　　要	利用者が所属する組織（domain）を識別する
セマンティクス	利用者の所属組織を記入すること。所属機関のインターネットドメインと同値することを推奨する。
実装状況	必須
利用目的	【認証・認可】
属性起源	Organization schema で必須属性として定義
OID	2.5.4.10
属性構文	【属性型】Directory String 属性値全体長は 256 文字までの値とする。 【照合順序】caseIgnoreMatch
複数値	所属組織自体を表すため，複数値の設定は許可しない
参考例	National Institute of Informatics

4.3.Organization Unit (ou)

概　　要	利用者が所属する組織の所属詳細を識別する
セマンティクス	所属組織内の所属詳細を記述する。
実装状況	必須
利用目的	【認証・認可】
属性起源	Organization schema で定義
OID	2.5.4.11

属 性 構 文	【属性型】Directory String 属性値全体長は 256 文字までの値とする。 【照合順序】caseIgnoreMatch
複 数 値	複数値の設定を許可する。 なお，階層レベルについては，今後検討を要する。
参 考 例	Infrastructure Planning Division

4.4. Affiliation (eduPersonAffiliation)

概 要	利用者の職種区分を識別する
セマンティクス	利用者と所属組織との関係（例：student，faculty，staff 等） 値として”misc”や”other”を利用しないこと。これらの値は，”none of the above”と同値となるからです。これら場合は，本属性値に空白(NULL)を設定すること。
実 装 状 況	必須
利 用 目 的	【認証・認可】
属 性 起 源	eduPerson で定義
OID	1.3.6.1.4.1.5923.1.1.1.1
属 性 構 文	【属性型】Directory String 属性値全体長は 256 文字までの値とする。 【照合順序】caseIgnoreMatch
複 数 値	複数の値を許可する。 なお，兼業等の取り扱いについては，今後検討を要する。
参 考 例	student，faculty，staff，”NULL” のみ利用可能

5. 参考資料

[eduPerson]

EduPerson Object Class Specification

http://www.educause.edu/eduperson/

[IANA]

Internet Assigned Numbers Authority

http://www.iana.org/

[ISO 9834]

ISO/IEC 9834-8:2005 Information Technology - Procedures for the operation of OSI Registration Authorities: Generation and registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 Object Identifier components

[ITU-T E.123]

Notation for national and international telephone numbers, e-mail addresses and Web addresses

http://www.itu.int/rec/T-REC-E.123/en

[LDAP Schema]

LDAP Schema for AAI Attributes

http://www.switch.ch/aai/docs/LDAP-schemas/

[RFC 2119]

RFC 2119: Key words for use in RFCs to Indicate Requirement Levels

http://www.ietf.org/rfc/rfc2119.txt

[RFC 2798]

RFC 2798: Definition of the inetOrgPerson LDAP Object Class

http://www.ietf.org/rfc/rfc2798.txt

[RFC 2849]

RFC 2849: The LDAP Data Interchange Format (LDIF) - Technical Specification

http://www.ietf.org/rfc/rfc2849.txt

[RFC 3339]

RFC 3339: Date and Time on the Internet: Timestamps

http://www.ietf.org/rfc/rfc3339.txt

[RFC 3986]

RFC 3986: Uniform Resource Identifiers (URI): Generic Syntax

http://www.ietf.org/rfc/rfc3986.txt

[RFC 4517]

RFC 4517: Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules

http://www.ietf.org/rfc/rfc4517.txt

[RFC 4646]

RFC 4646: Tags for Identifying Languages

http://www.ietf.org/rfc/rfc4646.txt