

公的個人認証サービス

プロフィール仕様書

3.1 版

令和6年4月9日

## 変更履歴

版数	日付	内容	承認者名	改訂区分
1.0	平成 26 年 3 月 31 日	新規作成		新規
1.1	平成 27 年 11 月 30 日	設定値の確定に伴う修正及び誤記訂正		修正
1.2	平成 27 年 12 月 25 日	2 章 2.2.1. 「署名用電子証明書のプロファイル基本領域(Basic)」及び 2.2.2 「利用者証明用電子証明書のプロファイル基本領域(Basic)」の validity の説明・備考の修正		修正
2.0	令和元年 5 月 1 日	・新元号「令和」対応に伴い新元号コードの追加及び旧氏対応に伴う修正記載の追加:2.1.1 署名用電子証明書のプロファイル 署名用電子証明書のプロファイル拡張領域(Extension)		修正
2.1	令和元年 11 月 1 日	・省令 29 条対応に伴う修正: 2.1.1 署名用電子証明書のプロファイル 署名用電子証明書のプロファイル基本領域(Basic)終了日時 2.1.2. 利用者証明用電子証明書のプロファイル 利用者証明用電子証明書のプロファイル基本領域(Basic)終了日時		修正
2.2	令和 3 年 4 月 22 日	2.2 オブジェクト識別子(OID) 「財団法人日本情報処理開発協会電子商取引推進センター」を「財団法人日本情報経済社会推進協会」に変更		修正
3.0	令和 5 年 3 月 31 日	移動端末設備用電子証明書のプロファイル追加に伴う修正		修正
3.1	令和 6 年 4 月 9 日	2 章 2.1.1. 「個人番号カード用署名用電子証明書のプロファイル」個人番号カード用署名用電子証明書のプロファイル拡張領域の「住所」に国外転出予定者また		修正

		は国外転出者の場合の記載を追記 2.1.2.「移動端末設備用署名用電子証明書のプロフィール」 移動端末設備用署名用電子証明書のプロフィール拡張領域の「住所」に国外転出予定者または国外転出者の場合の記載を追記		
--	--	--	--	--

## 目次

第 1 章 はじめに .....	1
1.1. 概要 .....	1
1.1.1. プロファイル仕様 .....	1
1.1.2. オブジェクト識別子 .....	1
第 2 章 諸元 .....	2
2.1. プロファイル仕様 .....	2
2.1.1. 個人番号カード用署名用電子証明書のプロファイル .....	2
2.1.2. 移動端末設備用署名用電子証明書のプロファイル .....	11
2.1.3. 個人番号カード用利用者証明用電子証明書のプロファイル .....	19
2.1.4. 移動端末設備用利用者証明用電子証明書のプロファイル .....	27
2.1.5. 署名用認証局の自己署名証明書のプロファイル .....	34
2.1.6. 利用者証明用認証局の自己署名証明書のプロファイル .....	39
2.2. オブジェクト識別子 (OID) .....	44

## 第 1 章 はじめに

本プロフィール仕様書は、公的個人認証サービスにおける各種証明書について定めたものである。

### 1.1. 概要

本プロフィール仕様書の概要について下記に説明する。

#### 1.1.1. プロファイル仕様

各種証明書、プロフィールについて記述する。各種証明書は署名前証明書(X.509 証明書の署名アルゴリズムと署名値を除いた証明書)の基本領域と拡張領域について記述する。

#### 1.1.2. オブジェクト識別子

公的個人認証サービスにおけるオブジェクト識別子の体系について記述する。

第 2 章 諸元

2.1. プロファイル仕様

2.1.1. 個人番号カード用署名用電子証明書のプロファイル

個人番号カード用署名用電子証明書のプロファイル基本領域 (Basic)

項目	項目の意味	データ型	設定値	説明・備考
version	電子証明書 フォーマットの バージョン番号	INTEGER	2(固定)	Version3
serialNumber	電子証明書の シリアル番号	INTEGER	(連番(16進数))	証明書を一意に識別するための正の 値
signature	電子証明書へ	-	-	
algorithm	の署名に関する 情報	OBJECT IDENTIFIER	1 2 840 113549 1 1 11 (固定)	暗号アルゴリズムの OID (1 2 840 113549 1 1 11 は 「Sha-256WithRSAEncryption」)
parameters		NULL	(なし)	暗号アルゴリズムの引数。RSA の場 合はなし
issuer	電子証明書発 行者	-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6(固定)	「countryName」の OID
value		PrintableString	JP(固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10(固定)	「organizationName」の OID
value		UTF8String	JPKI(固定)	「公的個人認証サービス」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	JPKI for digital signature (固定)	「公的個人認証サービス署名用認証 局」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	Japan Agency for Local Authority Information Systems(固定)	「地方公共団体情報システム機構」の 意味

## 第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考
validity	電子証明書の有効期間	-	-	
notBefore	開始日時	UTCTime	(YYMMDDhhmmssZ)	協定世界時
notAfter	終了日時	UTCTime	(YYMMDDhhmmssZ)	協定世界時  ・カード発行を伴う電子証明書の新規発行で、カードの有効期限が電子証明書発行日から 5 回目の誕生日を超える場合：電子証明書発行日から 5 回目の誕生日  ・カード発行を伴う電子証明書の更新時で、カードの有効期限が電子証明書発行日から 6 回目の誕生日を超える場合：電子証明書発行日から 6 回目の誕生日 ( )  ・カード発行を伴わない電子証明書の新規発行または電子証明書更新時で、公的個人認証サービス利用者証明用認証局が発行する有効な利用者証明用電子証明書を所持している場合：利用者証明用電子証明書の有効期間  ・カード発行を伴わない電子証明書の新規発行で、有効な利用者証明用電子証明書を所持せず、電子証明書発行日から 5 回目の誕生日がカード有効期限を超えない場合：電子証明書発行日から 5 回目の誕生日  ・カード発行を伴わない電子証明書の更新時で、有効な利用者証明用電子証明書を所持せず、更新前の有効期間満了日から 5 回目の誕生日がカードの有効期限を超えない場合：更新前の有効期間満了日から 5 回目の誕生日  ・上記以外：カードの有効期限
subject	利用者	-	-	

## 第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6 (固定)	「countryName」の OID
value		PrintableString	JP (固定)	「日本国」の意味
localityName		-	-	
type		OBJECT IDENTIFIER	2 5 4 7 (固定)	「localityName」の OID
value		UTF8String	(都道府県名(ローマ字))	
localityName		-	-	
type		OBJECT IDENTIFIER	2 5 4 7 (固定)	「localityName」の OID
value		UTF8String	(市区町村名(ローマ字))	
commonName		-	-	
type	OBJECT IDENTIFIER	2 5 4 3 (固定)	「commonName」の OID	
value	UTF8String	(YYYYMMDDhhmmssxx xxxXXXXXXXXXX)	発行要求作成日時 + シーケンス番号 + 受付窓口識別記号	
subjectPublicKeyInfo	電子証明書利 用者の公開鍵 に関する情報	-	-	
algorithm		-	-	
algorithm		OBJECT IDENTIFIER	1 2 840 113549 1 1 1 (固定)	公開鍵の暗号アルゴリズム名の OID (1 2 840 113549 1 1 1 は「rsaEncryption」)
parameters		NULL	(なし)	RSA の場合は値なし
subjectPublicKey		BIT STRING	(公開鍵値(16進数))	鍵長 2048bit

日本人、中長期在留者(在留資格が高度専門職第2号又は永住者である者)および特別永住者は、カードの有効期限が電子証明書発行日から6回目の誕生日を超える場合:電子証明書発行日から6回目の誕生日となる。その他の中長期在留者は、在留期間の更新が必要なため、カードの有効期限が変更となるタイミングに合わせて電子証明書の発行(更新)を行う。なお、カードの有効期間が発行日から5回目の誕生日を超える場合:電子証明書発行日から5回目の誕生日となる。

個人番号カード用署名用電子証明書のプロフィール拡張領域  
(Extension)

項目	項目の意味	データ型	設定値	説明・備考
Extensions				
authorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報	-	-	
extnID		OBJECT IDENTIFIER	2 5 29 35 (固定)	「authorityKeyIdentifier」の OID
critical		BOOLEAN	FALSE (固定)	
extnValue		OCTET STRING	-	
authorityKeyIdentifier		-	-	
[0]keyIdentifier		OCTET STRING	(公開鍵の識別子(16進数))	
[1]authorityCertificate		-	-	
[4]directoryName		-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6 (固定)	「countryName」の OID
value		PrintableString	JP (固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10 (固定)	「organizationName」の OID
value		UTF8String	JPKI (固定)	「公的個人認証サービス」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
value		UTF8String	JPKI for digital signature (固定)	「公的個人認証サービス署名用認証局」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID

## 第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考
value		UTF8String	Japan Agency for Local Authority Information Systems (固定)	「地方公共団体情報システム機構」の意味
		INTEGER	(公開鍵のシリアル番号 (16 進数))	認証局の公開鍵を一意に識別するための正の値
keyUsage	鍵の使用目的			
extnID		OBJECT IDENTIFIER	2 5 29 15 (固定)	「keyUsage」の OID
critical		BOOLEAN	TRUE (固定)	
extnValue		OCTET STRING	-	
keyUsage		BIT STRING	110000000 (固定)	鍵用途を示すビット列 「digitalSignature(0) & nonRepudiation(1)」の意味
subjectAltName	利用者日本語	-	-	
extnID	表記	OBJECT IDENTIFIER	2 5 29 17 (固定)	「subjectAltName」の OID
critical		BOOLEAN	FALSE (固定)	
extnValue		OCTET STRING	-	
[0]otherName	氏名	-	-	
commonName		-	-	
type		OBJECT IDENTIFIER	1 2 392 200149 8 5 5 1 (固定)	「commonName」の OID (独自)
[0]value		UTF8String	(氏名 姓名、姓名 (通称)、 姓 [旧氏] 名)	JIS 第 1 水準、第 2 水準、補助漢字以外の文字は代替文字に変換 通称ならびに旧氏は当該住民に係る住民票の記載にしたがってセパレート文字と共に氏名に追加・変更される。 最大文字数 100 文字 (セパレート文字を含む)
[0]otherName	生年月日	-	-	
dateOfBirth		-	-	
type		OBJECT IDENTIFIER	1 2 392 200149 8 5 5 4 (固定)	「dateOfBirth」の OID (独自)

## 第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考
[0]value		UTF8String	(生年月日 EYYYYMMDD)	設定値を和暦に変換して表示 E(年号コード) 1:明治、2:大正、3:昭和、4:平成、5: 令和、0:不明 YYYY(西暦年) MM(月) A1:春、A2:夏、A3:秋、A4:冬、00:不 明 DD(日) A1:上旬、A2:中旬、A3:下旬、00:不 明
[0]otherName	性別	-	-	
gender		-	-	
type		OBJECT IDENTIFIER	1 2 392 200149 8 5 5 3 (固定)	「gender」の OID(独自)
[0]value		UTF8String	(性別 1:男、2:女、3:不 明)	
[0]otherName	住所	-	-	
address		-	-	
type		OBJECT IDENTIFIER	1 2 392 200149 8 5 5 5 (固定)	「address」の OID(独自)
[0]value		UTF8String	(住所 住所、国外転出 国 外転出予定日)	JIS 第 1 水準、第 2 水準、補助漢字 以外の文字は代替文字に変換 全角ハイフン設定可能 最大文字数 200 文字 国外転出予定者および国外転出者 は、国外転出者である旨と国外転出 予定日を記載する。 例)国外転出 2024(令和 6)年 6月10日 全て全角とし、「」は全角スペー スの意。
[0]otherName	利用者の氏名	-	-	
substituteCharacte rOfCommonName	代替文字の使 用位置情報	-	-	
type		OBJECT IDENTIFIER	1 2 392 200149 8 5 5 2 (固定)	「substituteCharacterOfCommonNam e」の OID(独自)

第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考
[0]value		UTF8String	(代替文字使用位置を示す数字の文字列)	0 代替文字でない 1 代替文字
[0]otherName	利用者の住所	-	-	
substituteCharacterOfAddress	代替文字の使用位置情報	-	-	
type		OBJECT IDENTIFIER	1 2 392 200149 8 5 5 6 (固定)	「substituteCharacterOfAddress」の OID (独自)
[0]value		UTF8String	(代替文字使用位置を示す数字の文字列)	0 代替文字でない 1 代替文字
issuerAltName	発行者の日本語表記	-	-	
extnID		OBJECT IDENTIFIER	2 5 29 18(固定)	「issuerAltName」の OID
critical		BOOLEAN	FALSE(固定)	
extnValue		OCTET STRING	-	
[4]directoryName		-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6(固定)	「countryName」の OID
value		PrintableString	JP(固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10(固定)	「organizationName」の OID
value		UTF8String	公的個人認証サービス(固定)	
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	公的個人認証サービス署名用(固定)	
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	地方公共団体情報システム機構(固定)	
cRLDistributionPoints		-	-	

第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考
extnID	CRL 配布点に関する情報	OBJECT IDENTIFIER	2 5 29 31 (固定)	「cRLDistributionPoints」の OID
		critical	BOOLEAN	FALSE (固定)
extnValue		OCTET STRING	-	
[0]distributionPoint		-	-	
[0]fullName		-	-	
[4]directoryName		-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6 (固定)	「countryName」の OID
value		PrintableString	JP (固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10 (固定)	「organizationName」の OID
value		UTF8String	JPKI (固定)	「公的個人認証サービス」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
value		UTF8String	JPKI for digital signature (固定)	「公的個人認証サービス署名用認証局」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
value		UTF8String	CRL Distribution Points (固定)	
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
value	UTF8String	都道府県名 (ローマ字)		
commonName	-	-		



2.1.2. 移動端末設備用署名用電子証明書のプロフィール

移動端末設備用署名用電子証明書のプロフィール基本領域 (Basic)

項目	項目の意味	データ型	設定値	説明・備考
version	電子証明書 フォーマットの バージョン番号	INTEGER	2(固定)	Version3
serialNumber	電子証明書の シリアル番号	INTEGER	(連番(16進数))	証明書を一意に識別するための正の 値
signature	電子証明書へ の署名に関する 情報	-	-	
algorithm		OBJECT IDENTIFIER	1 2 840 113549 1 1 11 (固定)	暗号アルゴリズムの OID (1 2 840 113549 1 1 11 は 「Sha-256WithRSAEncryption」)
parameters		NULL	(なし)	暗号アルゴリズムの引数。RSA の場 合はなし
issuer	電子証明書発 行者	-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6(固定)	「countryName」の OID
value		PrintableString	JP(固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10(固定)	「organizationName」の OID
value		UTF8String	JPKI(固定)	「公的個人認証サービス」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	JPKI for digital signature (固定)	「公的個人認証サービス署名用認証 局」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	Japan Agency for Local Authority Information Systems(固定)	「地方公共団体情報システム機構」の 意味
validity	電子証明書の 有効期間	-	-	
notBefore	開始日時	UTCTime	(YYMMDDhhmmssZ)	協定世界時

## 第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考
notAfter	終了日時	UTCTime	(YYMMDDhhmmssZ)	協定世界時  ・移動端末設備用署名用電子証明書の有効期間末日
subject	利用者	-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6 (固定)	「countryName」の OID
value		PrintableString	JP (固定)	「日本国」の意味
localityName		-	-	
type		OBJECT IDENTIFIER	2 5 4 7 (固定)	「localityName」の OID
value		UTF8String	(都道府県名(ローマ字))	
localityName		-	-	
type		OBJECT IDENTIFIER	2 5 4 7 (固定)	「localityName」の OID
value		UTF8String	(市区町村名(ローマ字))	
commonName		-	-	
type		OBJECT IDENTIFIER	2 5 4 3 (固定)	「commonName」の OID
value		UTF8String	(YYYYMMDDhhmmssxxxXXXXXXXXXX)	発行要求作成日時 + シーケンス番号 + 受付窓口識別記号
subjectPublicKeyInfo	電子証明書利用者の公開鍵に関する情報	-	-	
algorithm		-	-	
algorithm		OBJECT IDENTIFIER	1 2 840 113549 1 1 1 (固定)	公開鍵の暗号アルゴリズム名の OID (1 2 840 113549 1 1 1 は「rsaEncryption」)
parameters		NULL	(なし)	RSA の場合は値なし
subjectPublicKey		BIT STRING	(公開鍵値(16進数))	鍵長 2048bit

移動端末設備用署名用電子証明書のプロファイル拡張領域  
(Extension)

項目	項目の意味	データ型	設定値	説明・備考
Extensions				
authorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報	-	-	
extnID		OBJECT IDENTIFIER	2 5 29 35 (固定)	「authorityKeyIdentifier」の OID
critical		BOOLEAN	FALSE (固定)	
extnValue		OCTET STRING	-	
authorityKeyIdentifier		-	-	
[0]keyIdentifier		OCTET STRING	(公開鍵の識別子(16進数))	
[1]authorityCertificate		-	-	
[4]directoryName		-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6 (固定)	「countryName」の OID
value		PrintableString	JP (固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10 (固定)	「organizationName」の OID
value		UTF8String	JPKI (固定)	「公的個人認証サービス」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
value		UTF8String	JPKI for digital signature (固定)	「公的個人認証サービス署名用認証局」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID

## 第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考
value		UTF8String	Japan Agency for Local Authority Information Systems (固定)	「地方公共団体情報システム機構」の意味
		INTEGER	(公開鍵のシリアル番号 (16 進数))	認証局の公開鍵を一意に識別するための正の値
keyUsage	鍵の使用目的			
extnID		OBJECT IDENTIFIER	2 5 29 15 (固定)	「keyUsage」の OID
critical		BOOLEAN	TRUE (固定)	
extnValue		OCTET STRING	-	
keyUsage		BIT STRING	110000000 (固定)	鍵用途を示すビット列 「digitalSignature(0) & nonRepudiation(1)」の意味
subjectAltName	利用者日本語	-	-	
extnID	表記	OBJECT IDENTIFIER	2 5 29 17 (固定)	「subjectAltName」の OID
critical		BOOLEAN	FALSE (固定)	
extnValue		OCTET STRING	-	
[0]otherName	氏名	-	-	
commonName		-	-	
type		OBJECT IDENTIFIER	1 2 392 200149 8 5 5 1 (固定)	「commonName」の OID (独自)
[0]value		UTF8String	(氏名 姓名、姓名 (通称)、 姓 [旧氏] 名)	JIS 第 1 水準、第 2 水準、補助漢字以外の文字は代替文字に変換 通称ならびに旧氏は当該住民に係る住民票の記載にしたがってセパレート文字と共に氏名に追加・変更される。 最大文字数 100 文字 (セパレート文字を含む)
[0]otherName	生年月日	-	-	
dateOfBirth		-	-	
type		OBJECT IDENTIFIER	1 2 392 200149 8 5 5 4 (固定)	「dateOfBirth」の OID (独自)

## 第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考
[0]value		UTF8String	(生年月日 EYYYYMMDD)	設定値を和暦に変換して表示 E(年号コード) 1:明治、2:大正、3:昭和、4:平成、5: 令和、0:不明 YYYY(西暦年) MM(月) A1:春、A2:夏、A3:秋、A4:冬、00:不 明 DD(日) A1:上旬、A2:中旬、A3:下旬、00:不 明
[0]otherName	性別	-	-	
gender		-	-	
type		OBJECT IDENTIFIER	1 2 392 200149 8 5 5 3 (固定)	「gender」の OID(独自)
[0]value		UTF8String	(性別 1:男、2:女、3:不 明)	
[0]otherName	住所	-	-	
address		-	-	
type		OBJECT IDENTIFIER	1 2 392 200149 8 5 5 5 (固定)	「address」の OID(独自)
[0]value		UTF8String	(住所 住所、国外転出 国 外転出予定日)	JIS 第 1 水準、第 2 水準、補助漢字 以外の文字は代替文字に変換 全角ハイフン設定可能 最大文字数 200 文字 国外転出予定者および国外転出者 は、国外転出者である旨と国外転出 予定日を記載する。 例)国外転出 2024(令和 6)年 6月10日 全て全角とし、「」は全角スペー スの意。
[0]otherName	利用者の氏名	-	-	
substituteCharacte rOfCommonName	代替文字の使 用位置情報	-	-	
type		OBJECT IDENTIFIER	1 2 392 200149 8 5 5 2 (固定)	「substituteCharacterOfCommonNam e」の OID(独自)

第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考
[0]value		UTF8String	(代替文字使用位置を示す数字の文字列)	0 代替文字でない 1 代替文字
[0]otherName	利用者の住所	-	-	
substituteCharacterOfAddress	代替文字の使用位置情報	-	-	
type		OBJECT IDENTIFIER	1 2 392 200149 8 5 5 6 (固定)	「substituteCharacterOfAddress」の OID (独自)
[0]value		UTF8String	(代替文字使用位置を示す数字の文字列)	0 代替文字でない 1 代替文字
issuerAltName	発行者の日本語表記	-	-	
extnID		OBJECT IDENTIFIER	2 5 29 18(固定)	「issuerAltName」の OID
critical		BOOLEAN	FALSE(固定)	
extnValue		OCTET STRING	-	
[4]directoryName		-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6(固定)	「countryName」の OID
value		PrintableString	JP(固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10(固定)	「organizationName」の OID
value		UTF8String	公的個人認証サービス(固定)	
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	公的個人認証サービス署名用(固定)	
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	地方公共団体情報システム機構(固定)	
cRLDistributionPoints		-	-	

第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考
extnID	CRL 配布点に関する情報	OBJECT IDENTIFIER	2 5 29 31 (固定)	「cRLDistributionPoints」の OID
		critical	BOOLEAN	FALSE (固定)
extnValue		OCTET STRING	-	
[0]distributionPoint		-	-	
[0]fullName		-	-	
[4]directoryName		-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6 (固定)	「countryName」の OID
value		PrintableString	JP (固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10 (固定)	「organizationName」の OID
value		UTF8String	JPKI (固定)	「公的個人認証サービス」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
value		UTF8String	JPKI for digital signature (固定)	「公的個人認証サービス署名用認証局」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
value		UTF8String	CRL Distribution Points (固定)	
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
value	UTF8String	都道府県名 (ローマ字)		
commonName	-	-		



## 2.1.3. 個人番号カード用利用者証明用電子証明書のプロフィール

個人番号カード用利用者証明用電子証明書のプロフィール基本領域  
(Basic)

項目	項目の意味	データ型	設定値	説明・備考
version	電子証明書 フォーマットの バージョン番号	INTEGER	2(固定)	Version3
serialNumber	電子証明書のシ リアル番号	INTEGER	(連番(16進数))	証明書を一意に識別するための正の 値
signature	電子証明書への 署名に関する情 報	-	-	
algorithm		OBJECT IDENTIFIER	1 2 840 113549 1 1 11 (固定)	暗号アルゴリズムの OID (1 2 840 113549 1 1 11 は 「Sha-256WithRSAEncryption」)
parameters		NULL	(なし)	暗号アルゴリズムの引数。RSA の場 合はなし
issuer	電子証明書発行 者	-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6(固定)	「countryName」の OID
value		PrintableString	JP(固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10(固定)	「organizationName」の OID
value		UTF8String	JPKI(固定)	「公的個人認証サービス」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	JPKI for user authentication(固定)	「公的個人認証サービス利用者証明 用認証局」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	Japan Agency for Local Authority Information Systems(固定)	「地方公共団体情報システム機構」の 意味
validity	電子証明書の有 効期間	-	-	
notBefore	開始日時	UTCTime	(YYMMDDhhmmssZ)	協定世界時

## 第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考
notAfter	終了日時	UTCTime	(YYMMDDhhmmssZ)	<p>協定世界時</p> <p>・カード発行を伴う電子証明書の新規発行で、カードの有効期限が電子証明書発行日から 5 回目の誕生日を超える場合：電子証明書発行日から 5 回目の誕生日</p> <p>・カード発行を伴う電子証明書の更新時で、カードの有効期限が電子証明書発行日から 6 回目の誕生日を超える場合：電子証明書発行日から 6 回目の誕生日( )</p> <p>・カード発行を伴わない電子証明書の新規発行で、電子証明書発行日から 5 回目の誕生日がカード有効期限を超えない場合：電子証明書発行日から 5 回目の誕生日</p> <p>・カード発行を伴わない電子証明書の更新時で、更新前の有効期間満了日から 5 回目の誕生日がカードの有効期限を超えない場合：更新前の有効期間満了日から 5 回目の誕生日</p> <p>・上記以外：カードの有効期限</p>
subject	利用者	-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6(固定)	「countryName」の OID
value		PrintableString	JP(固定)	「日本国」の意味
commonName		-		
type		OBJECT IDENTIFIER	2 5 4 3(固定)	「commonName」の OID
value		UTF8String	( xxxxxxxxxxxxxxxXXX XXXXX)	ランダム文字列 + 受付窓口識別記号
subjectPublicKeyInfo	電子証明書利用者の公開鍵に関する情報	-	-	
algorithm		-	-	
algorithm		OBJECT IDENTIFIER	1 2 840 113549 1 1 1(固定)	公開鍵の暗号アルゴリズム名の OID (1 2 840 113549 1 1 1 は「rsaEncryption」)

## 第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考
parameters		NULL	(なし)	RSA の場合は値なし
subjectPublicKey		BIT STRING	(公開鍵値(16進数))	鍵長 2048bit

日本人、中長期在留者(在留資格が高度専門職第2号又は永住者である者)および特別永住者は、カードの有効期限が電子証明書発行日から6回目の誕生日を超える場合:電子証明書発行日から6回目の誕生日となる。その他の中長期在留者は、在留期間の更新が必要なため、カードの有効期限が変更となるタイミングに合わせて電子証明書の発行(更新)を行う。なお、カードの有効期間が発行日から5回目の誕生日を超える場合:電子証明書発行日から5回目の誕生日となる。

個人番号カード用利用者証明用電子証明書のプロフィール拡張領域  
(Extension)

項目	項目の意味	データ型	設定値	説明・備考
Extensions				
authorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報	-	-	
extnID		OBJECT IDENTIFIER	2 5 29 35 (固定)	「authorityKeyIdentifier」の OID
critical		BOOLEAN	FALSE (固定)	
extnValue		OCTET STRING	-	
authorityKeyIdentifier		-	-	
[0]keyIdentifier		OCTET STRING	(公開鍵の識別子(16進数))	
[1]authorityCertIssuer		-	-	
[4]directoryName		-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6 (固定)	「countryName」の OID
value		PrintableString	JP (固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10 (固定)	「organizationName」の OID
value		UTF8String	JPKI (固定)	「公的個人認証サービス」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
value		UTF8String	JPKI for user authentication (固定)	「公的個人認証サービス利用者証明用認証局」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
value		UTF8String	Japan Agency for Local Authority Information Systems (固定)	「地方公共団体情報システム機構」の意味

## 第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考
[2]authorityCertSerial Number		INTEGER	(公開鍵のシリアル番号 (16進数))	認証局の公開鍵を一意に識別する ための正の値
keyUsage	鍵の使用目的			
extnID		OBJECT IDENTIFIER	2 5 29 15(固定)	「keyUsage」の OID
critical		BOOLEAN	TRUE(固定)	
extnValue		OCTET STRING	-	
keyUsage		BIT STRING	10000000(固定)	鍵用途を示すビット列 「digitalSignature(0)」の意味
extendedKeyUsage	拡張された鍵用 途			
extnID		OBJECT IDENTIFIER	2 5 29 37(固定)	「extkeyUsage」の OID
critical		BOOLEAN	FALSE(固定)	
extnValue		OCTET STRING	-	
extendedKeyUsage		-	-	
KeyPurposeId		OCTET STRING	1 3 6 1 5 5 7 3 2	「id-kp-clientAuth」の OID
issuerAltName	発行者の日本 語表記	-	-	
extnID		OBJECT IDENTIFIER	2 5 29 18(固定)	「issuerAltName」の OID
critical		BOOLEAN	FALSE(固定)	
extnValue		OCTET STRING	-	
[4]directoryName		-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6(固定)	「countryName」の OID
value		PrintableString	JP(固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10(固定)	「organizationName」の OID
value		UTF8String	公的個人認証サービス (固定)	
organizationalUnitName		-	-	

## 第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考																																																																
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td>type</td> </tr> <tr> <td></td> <td></td> <td>value</td> </tr> <tr> <td colspan="3">organizationalUnitName</td> </tr> <tr> <td></td> <td></td> <td>type</td> </tr> <tr> <td></td> <td></td> <td>value</td> </tr> </table>				type			value	organizationalUnitName					type			value		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID																																																
				type																																																																
			value																																																																	
	organizationalUnitName																																																																			
			type																																																																	
			value																																																																	
		UTF8String	公的個人認証サービス 利用者証明用(固定)																																																																	
		-	-																																																																	
		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID																																																																
		UTF8String	地方公共団体情報システム機構(固定)																																																																	
		-	-																																																																	
cRLDistributionPoints	CRL 配布点に関する情報	-	-																																																																	
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="4">extnID</td> </tr> <tr> <td colspan="4">critical</td> </tr> <tr> <td colspan="4">extnValue</td> </tr> <tr> <td colspan="4">[0]distributionPoint</td> </tr> <tr> <td colspan="4">[0]fullName</td> </tr> <tr> <td colspan="4">[4]directoryName</td> </tr> <tr> <td colspan="4">countryName</td> </tr> <tr> <td></td> <td></td> <td>type</td> <td></td> </tr> <tr> <td></td> <td></td> <td>value</td> <td></td> </tr> <tr> <td colspan="4">organizationName</td> </tr> <tr> <td></td> <td></td> <td>type</td> <td></td> </tr> <tr> <td></td> <td></td> <td>value</td> <td></td> </tr> <tr> <td colspan="4">organizationalUnitName</td> </tr> <tr> <td></td> <td></td> <td>type</td> <td></td> </tr> <tr> <td></td> <td></td> <td>value</td> <td></td> </tr> <tr> <td colspan="4">organizationalUnitName</td> </tr> </table>	extnID				critical				extnValue				[0]distributionPoint				[0]fullName				[4]directoryName				countryName						type				value		organizationName						type				value		organizationalUnitName						type				value		organizationalUnitName				CRL 配布点に関する情報	OBJECT IDENTIFIER	2 5 29 31 (固定)	「cRLDistributionPoints」の OID
extnID																																																																				
critical																																																																				
extnValue																																																																				
[0]distributionPoint																																																																				
[0]fullName																																																																				
[4]directoryName																																																																				
countryName																																																																				
		type																																																																		
		value																																																																		
organizationName																																																																				
		type																																																																		
		value																																																																		
organizationalUnitName																																																																				
		type																																																																		
		value																																																																		
organizationalUnitName																																																																				
		BOOLEAN	FALSE(固定)																																																																	
		OCTET STRING	-																																																																	
		-	-																																																																	
		-	-																																																																	
		-	-																																																																	
		-	-																																																																	
		OBJECT IDENTIFIER	2 5 4 6(固定)	「countryName」の OID																																																																
		PrintableString	JP(固定)	「日本国」の意味																																																																
		-	-																																																																	
		OBJECT IDENTIFIER	2 5 4 10(固定)	「organizationName」の OID																																																																
		UTF8String	JPKI(固定)	「公的個人認証サービス」の意味																																																																
		-	-																																																																	
		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID																																																																
		UTF8String	JPKI for user authentication(固定)	「公的個人認証サービス利用者証明用認証局」の意味																																																																
		-	-																																																																	

## 第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考				
	type	OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID				
	value	UTF8String	CRL Distribution Points (固定)					
	organizationalUnitName	-	-					
	type	OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID				
	value	UTF8String	都道府県名(ローマ字)					
	commonName	-	-					
	type	OBJECT IDENTIFIER	2 5 4 3(固定)	「commonName」の OID				
	value	UTF8String	市区町村名(ローマ字) CRLDP					
certificatePolicies	証明書ポリシー	-	-					
extnID	critical	extnValue	policyIdentifier	OBJECT IDENTIFIER	1 2 392 200149 8 5 1 3 30	公的個人認証サービスの個人番号カード用利用者証明用電子証明書ポリシーの OID		
			policyQualifiers	-	-			
			policyQualifierId	OBJECT IDENTIFIER	1 3 6 1 5 5 7 2 1 (id-qt-cps)	「CPS」の OID		
			pqualifier	IA5String	http://www.jpki.go.jp/cps.html	CPS を掲載する URL		
			subjectKeyIdentifier	電子証明書利用者の公開鍵の識別子	-	-		
			extnID	extnValue	subjectKeyIdentifier	OBJECT IDENTIFIER	2 5 29 14(固定)	「subjectKeyIdentifier」の OID
			critical	keyIdentifier	BOOLEAN	FALSE(固定)		
extnValue	keyIdentifier	OCTET STRING	-					
subjectKeyIdentifier	keyIdentifier	OCTET STRING	(公開鍵のハッシュ値(16進数))	ハッシュ関数は sha-1 を使用				

## 第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考
authorityInfoAccess	機関アクセス情報	-	-	-
extnID	機関アクセス情報	OBJECT IDENTIFIER	1 3 6 1 5 5 7 1 1 (固定)	「authorityInfoAccess」の OID
critical		BOOLEAN	FALSE (固定)	
extnValue		OCTET STRING	-	
accessDiscription		-	-	
accessMethod		OBJECT IDENTIFIER	1 3 6 1 5 5 7 48 1 (固定)	「ocsp」の OID
accessLocation		IA5String	http://ocspauthnorm.jp ki.go.jp	OCSP レスポンドの URL

2.1.4. 移動端末設備用利用者証明用電子証明書のプロフィール

移動端末設備用利用者証明用電子証明書のプロフィール基本領域  
(Basic)

項目	項目の意味	データ型	設定値	説明・備考
version	電子証明書 フォーマットの バージョン番号	INTEGER	2(固定)	Version3
serialNumber	電子証明書のシ リアル番号	INTEGER	(連番(16進数))	証明書を一意に識別するための正の 値
signature	電子証明書への 署名に関する情 報	-	-	
algorithm		OBJECT IDENTIFIER	1 2 840 113549 1 1 11 (固定)	暗号アルゴリズムの OID (1 2 840 113549 1 1 11 は 「Sha-256WithRSAEncryption」)
parameters		NULL	(なし)	暗号アルゴリズムの引数。RSA の場 合はなし
issuer	電子証明書発行 者	-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6(固定)	「countryName」の OID
value		PrintableString	JP(固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10(固定)	「organizationName」の OID
value		UTF8String	JPKI(固定)	「公的個人認証サービス」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	JPKI for user authentication(固定)	「公的個人認証サービス利用者証明 用認証局」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	Japan Agency for Local Authority Information Systems(固定)	「地方公共団体情報システム機構」の 意味
validity	電子証明書の有 効期間	-	-	
notBefore	開始日時	UTCTime	(YYMMDDhhmmssZ)	協定世界時

## 第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考
notAfter	終了日時	UTCTime	(YYMMDDhhmmssZ)	協定世界時  ・移動端末設備用利用者証明用電子 証明書の有効期間末日
subject	利用者	-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6 (固定)	「countryName」の OID
value		PrintableString	JP (固定)	「日本国」の意味
commonName		-		
type		OBJECT IDENTIFIER	2 5 4 3 (固定)	「commonName」の OID
value		UTF8String	( xxxxxxxxxxxxxxxX XXXXX)	ランダム文字列 + 受付窓口識別記 号
subjectPublicKeyInfo	電子証明書利用 者の公開鍵に関 する情報	-	-	
algorithm		-	-	
algorithm		OBJECT IDENTIFIER	1 2 840 113549 1 1 1 (固 定)	公開鍵の暗号アルゴリズム名の OID (1 2 840 113549 1 1 1 は 「rsaEncryption」)
parameters		NULL	(なし)	RSA の場合は値なし
subjectPublicKey		BIT STRING	(公開鍵値(16 進数))	鍵長 2048bit

移動端末設備用利用者証明用電子証明書のプロフィール拡張領域  
(Extension)

項目	項目の意味	データ型	設定値	説明・備考
Extensions				
authorityKeyIdentifier	電子証明書発行者の公開鍵に関する情報	-	-	
extnID		OBJECT IDENTIFIER	2 5 29 35 (固定)	「authorityKeyIdentifier」の OID
critical		BOOLEAN	FALSE (固定)	
extnValue		OCTET STRING	-	
authorityKeyIdentifier		-	-	
[0]keyIdentifier		OCTET STRING	(公開鍵の識別子(16進数))	
[1]authorityCertIssuer		-	-	
[4]directoryName		-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6 (固定)	「countryName」の OID
value		PrintableString	JP (固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10 (固定)	「organizationName」の OID
value		UTF8String	JPKI (固定)	「公的個人認証サービス」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
value		UTF8String	JPKI for user authentication (固定)	「公的個人認証サービス利用者証明用認証局」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
value		UTF8String	Japan Agency for Local Authority Information Systems (固定)	「地方公共団体情報システム機構」の意味

## 第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考
[2]authorityCertSerial Number		INTEGER	(公開鍵のシリアル番号 (16進数))	認証局の公開鍵を一意に識別する ための正の値
keyUsage	鍵の使用目的			
extnID		OBJECT IDENTIFIER	2 5 29 15(固定)	「keyUsage」の OID
critical		BOOLEAN	TRUE(固定)	
extnValue		OCTET STRING	-	
keyUsage		BIT STRING	10000000(固定)	鍵用途を示すビット列 「digitalSignature(0)」の意味
extendedKeyUsage	拡張された鍵用 途			
extnID		OBJECT IDENTIFIER	2 5 29 37(固定)	「extkeyUsage」の OID
critical		BOOLEAN	FALSE(固定)	
extnValue		OCTET STRING	-	
extendedKeyUsage		-	-	
KeyPurposeId		OCTET STRING	1 3 6 1 5 5 7 3 2	「id-kp-clientAuth」の OID
issuerAltName	発行者の日本 語表記	-	-	
extnID		OBJECT IDENTIFIER	2 5 29 18(固定)	「issuerAltName」の OID
critical		BOOLEAN	FALSE(固定)	
extnValue		OCTET STRING	-	
[4]directoryName		-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6(固定)	「countryName」の OID
value		PrintableString	JP(固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10(固定)	「organizationName」の OID
value		UTF8String	公的個人認証サービス (固定)	
organizationalUnitName		-	-	





## 第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考
authorityInfoAccess	機関アクセス情報	-	-	-
extnID	機関アクセス情報	OBJECT IDENTIFIER	1 3 6 1 5 5 7 1 1 (固定)	「authorityInfoAccess」の OID
critical		BOOLEAN	FALSE (固定)	
extnValue		OCTET STRING	-	
accessDiscription		-	-	
accessMethod		OBJECT IDENTIFIER	1 3 6 1 5 5 7 48 1 (固定)	「ocsp」の OID
accessLocation		IA5String	http://ocspauthnorm-mobile.jpki.go.jp	OCSP レスポンスの移動端末設備用 URL

## 2.1.5. 署名用認証局の自己署名証明書のプロフィール

## 署名用認証局の自己署名証明書のプロフィール基本領域 (Basic)

項目	項目の意味	データ型	設定値	説明・備考
version	電子証明書フォーマットのバージョン番号	INTEGER	2(固定)	Version3
serialNumber	電子証明書のシリアル番号	INTEGER	(連番(16進数))	証明書を一意に識別するための正の値
signature	電子証明書への署名に関する情報	-	-	
algorithm		OBJECT IDENTIFIER	1 2 840 113549 1 1 11 (固定)	暗号アルゴリズムの OID (1 2 840 113549 1 1 11 は「Sha-256WithRSAEncryption」)
parameters		NULL	(なし)	暗号アルゴリズムの引数。RSA の場合はなし
issuer	電子証明書発行者	-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6(固定)	「countryName」の OID
value		PrintableString	JP(固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10(固定)	「organizationName」の OID
value		UTF8String	JPKI(固定)	「公的個人認証サービス」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	JPKI for digital signature (固定)	「公的個人認証サービス署名用認証局」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	Japan Agency for Local Authority Information Systems(固定)	「地方公共団体情報システム機構」の意味
validity	電子証明書の有効期間	-	-	
notBefore	開始日時	UTCTime	(YYMMDDhhmmssZ)	協定世界時

## 第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考
notAfter	終了日時	UTCTime	(YYMMDDhhmmssZ)	協定世界時 notBefore + 10 年
subject	利用者	-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6 (固定)	「countryName」の OID
value		PrintableString	JP (固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10 (固定)	「organizationName」の OID
value		UTF8String	JPKI (固定)	「公的個人認証サービス」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
value		UTF8String	JPKI for digital signature (固定)	「公的個人認証サービス署名用認証局」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
value		UTF8String	Japan Agency for Local Authority Information Systems (固定)	「地方公共団体情報システム機構」の意味
subjectPublicKeyInfo		電子証明書利用者の公開鍵に関する情報	-	-
algorithm	-		-	
algorithm	OBJECT IDENTIFIER		1 2 840 113549 1 1 1 (固定)	公開鍵の暗号アルゴリズム名の OID (1 2 840 113549 1 1 1 は「rsaEncryption」)
parameters	NULL		(なし)	RSA の場合は値なし
subjectPublicKey	BIT STRING		(公開鍵値 (16 進数))	鍵長 2048bit

## 署名用認証局の自己署名証明書のプロフィール拡張領域 (Extension)

項目	項目の意味	データ型	設定値	説明・備考
Extensions				
keyUsage	鍵の使用目的			
extnID		OBJECT IDENTIFIER	2 5 29 15(固定)	「keyUsage」の OID
critical		BOOLEAN	TRUE(固定)	
extnValue		OCTET STRING	-	
keyUsage		BIT STRING	000001100(固定)	鍵用途を示すビット列 「keyCertSign(5)」&「cRLSign(6)」の意味
subjectAltName	利用者日本語表記	-	-	
extnID	記	OBJECT IDENTIFIER	2 5 29 17(固定)	「subjectAltName」の OID
critical		BOOLEAN	FALSE(固定)	
extnValue		OCTET STRING	-	
[4]directoryName	氏名	-	-	
commonName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6(固定)	「countryName」の OID
[0]value		PrintableString	JP(固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10(固定)	「organizationName」の OID
[0]value		UTF8String	公的個人認証サービス(固定)	
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
[0]value		UTF8String	公的個人認証サービス署名用(固定)	
organizationalUnitName		-	-	

## 第 2 章 諸元

項目				項目の意味	データ型	設定値	説明・備考
			type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
			[0]value		UTF8String	地方公共団体情報システム機構 (固定)	
basicConstraints				基本的制約	-	-	
			extnID		OBJECT IDENTIFIER	2 5 29 19 (固定)	「basicConstraints」の OID
			critical		BOOLEAN	TRUE (固定)	
			extnValue		OCTET STRING	-	
			cA		BOOLEAN	TRUE (固定)	
cRLDistributionPoints				CRL 配布点に関する情報	-	-	
			extnID	する情報	OBJECT IDENTIFIER	2 5 29 31 (固定)	「cRLDistributionPoints」の OID
			critical		BOOLEAN	FALSE (固定)	
			extnValue		OCTET STRING	-	
			[0]distributionPoint		-	-	
			[0]fullName		-	-	
			[4]directoryName		-	-	
			countryName		-	-	
			type		OBJECT IDENTIFIER	2 5 4 6 (固定)	「countryName」の OID
			value		PrintableString	JP (固定)	「日本国」の意味
			organizationName		-	-	
			type		OBJECT IDENTIFIER	2 5 4 10 (固定)	「organizationName」の OID
			value		UTF8String	JPKI (固定)	「公的個人認証サービス」の意味
			organizationalUnitName		-	-	
			type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
value	UTF8String	JPKI for digital signature (固定)	「公的個人認証サービス署名用認証局」の意味				

## 第 2 章 諸元

項目				項目の意味	データ型	設定値	説明・備考
			organizationalUnitName		-	-	
			type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
			value		UTF8String	Japan Agency for Local Authority Information Systems (固定)	「地方公共団体情報システム機構」の意味
subjectKeyIdentifier				電子証明書利用者の公開鍵の識別子	-	-	
		extnID			OBJECT IDENTIFIER	2 5 29 14 (固定)	「subjectKeyIdentifier」の OID
		critical			BOOLEAN	FALSE (固定)	
		extnValue			OCTET STRING	-	
		subjectKeyIdentifier			-	-	
		keyIdentifier			OCTET STRING	(公開鍵のハッシュ値 (16 進数))	ハッシュ関数は sha-1 を使用

## 2.1.6. 利用者証明用認証局の自己署名証明書のプロフィール

利用者証明用認証局の自己署名証明書のプロフィール基本領域  
(Basic)

項目	項目の意味	データ型	設定値	説明・備考
version	電子証明書 フォーマットの バージョン番号	INTEGER	2(固定)	Version3
serialNumber	電子証明書のシリアル番号	INTEGER	(連番(16進数))	証明書を一意に識別するための正の値
signature	電子証明書への 署名に関する情報	-	-	
algorithm		OBJECT IDENTIFIER	1 2 840 113549 1 1 11 (固定)	暗号アルゴリズムの OID (1 2 840 113549 1 1 11 は 「Sha-256WithRSAEncryption」)
parameters		NULL	(なし)	暗号アルゴリズムの引数。RSA の場合はなし
issuer	電子証明書発行者	-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6(固定)	「countryName」の OID
value		PrintableString	JP(固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10(固定)	「organizationName」の OID
value		UTF8String	JPKI(固定)	「公的個人認証サービス」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	JPKI for user authentication(固定)	「公的個人認証サービス利用者証明 用認証局」の意味
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	Japan Agency for Local Authority Information Systems(固定)	「地方公共団体情報システム機構」の 意味
validity	電子証明書の有効期間	-	-	

## 第 2 章 諸元

項目		項目の意味	データ型	設定値	説明・備考
	notBefore	開始日時	UTCTime	(YYMMDDhhmmssZ)	協定世界時
	notAfter	終了日時	UTCTime	(YYMMDDhhmmssZ)	協定世界時 notBefore + 10 年
subject		利用者	-	-	
countryName			-	-	
	type		OBJECT IDENTIFIER	2 5 4 6 (固定)	「countryName」の OID
	value		PrintableString	JP (固定)	「日本国」の意味
organizationName			-	-	
	type		OBJECT IDENTIFIER	2 5 4 10 (固定)	「organizationName」の OID
	value		UTF8String	JPKI (固定)	「公的個人認証サービス」の意味
organizationalUnitName			-	-	
	type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
	value		UTF8String	JPKI for user authentication (固定)	「公的個人認証サービス利用者証明用認証局」の意味
organizationalUnitName			-	-	
	type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
	value		UTF8String	Japan Agency for Local Authority Information Systems (固定)	「地方公共団体情報システム機構」の意味
subjectPublicKeyInfo		電子証明書利用者の公開鍵に関する情報	-	-	
	algorithm		-	-	
	algorithm		OBJECT IDENTIFIER	1 2 840 113549 1 1 1 (固定)	公開鍵の暗号アルゴリズム名の OID (1 2 840 113549 1 1 1 は「rsaEncryption」)
	parameters		NULL	(なし)	RSA の場合は値なし
	subjectPublicKey		BIT STRING	(公開鍵値 (16 進数))	鍵長 2048bit

利用者証明用認証局の自己署名証明書のプロフィール拡張領域  
(Extension)

項目	項目の意味	データ型	設定値	説明・備考
Extensions				
keyUsage	鍵の使用目的			
extnID		OBJECT IDENTIFIER	2 5 29 15(固定)	「keyUsage」の OID
critical		BOOLEAN	TRUE(固定)	
extnValue		OCTET STRING	-	
keyUsage		BIT STRING	000001100(固定)	鍵用途を示すビット列 「keyCertSign(5)」&「cRLSign(6)」の意味
subjectAltName	利用者日本語表記	-	-	
extnID		OBJECT IDENTIFIER	2 5 29 17(固定)	「subjectAltName」の OID
critical		BOOLEAN	FALSE(固定)	
extnValue		OCTET STRING	-	
[4]directoryName	氏名	-	-	
commonName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6(固定)	「countryName」の OID
[0]value		PrintableString	JP(固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10(固定)	「organizationName」の OID
[0]value		UTF8String	公的個人認証サービス(固定)	
organizationalUnitName		-	-	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
[0]value		UTF8String	公的個人認証サービス利用者証明用(固定)	
organizationalUnitName		-	-	

## 第 2 章 諸元

項目	項目の意味	データ型	設定値	説明・備考
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID
		UTF8String	地方公共団体情報システム機構 (固定)	
[0]value				
basicConstraints	基本的制約	-	-	
extnID		OBJECT IDENTIFIER	2 5 29 19 (固定)	「basicConstraints」の OID
critical		BOOLEAN	TRUE (固定)	
extnValue		OCTET STRING	-	
cA		BOOLEAN	TRUE (固定)	
cRLDistributionPoints	CRL 配布点に関する情報	-	-	
extnID		OBJECT IDENTIFIER	2 5 29 31 (固定)	「cRLDistributionPoints」の OID
critical		BOOLEAN	FALSE (固定)	
extnValue		OCTET STRING	-	
[0]distributionPoint		-	-	
[0]fullName		-	-	
[4]directoryName		-	-	
countryName		-	-	
type		OBJECT IDENTIFIER	2 5 4 6 (固定)	「countryName」の OID
value		PrintableString	JP (固定)	「日本国」の意味
organizationName		-	-	
type		OBJECT IDENTIFIER	2 5 4 10 (固定)	「organizationName」の OID
value		UTF8String	JPKI (固定)	「公的個人認証サービス」の意味
organizationalUnitName		-	-	
type	OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID	
value	UTF8String	JPKI for user authentication (固定)	「公的個人認証サービス利用者証明用認証局」の意味	



2.2. オブジェクト識別子 (OID)

公的個人認証サービスにおけるオブジェクト識別子の体系としては、GPKIのガイドラインにしたがい、日本国政府としての体系を維持する。そのために、財団法人日本情報経済社会推進協会に申請しオブジェクト登録を行うことで、世界的なレベルでのオブジェクト識別子の一意性を確保する。

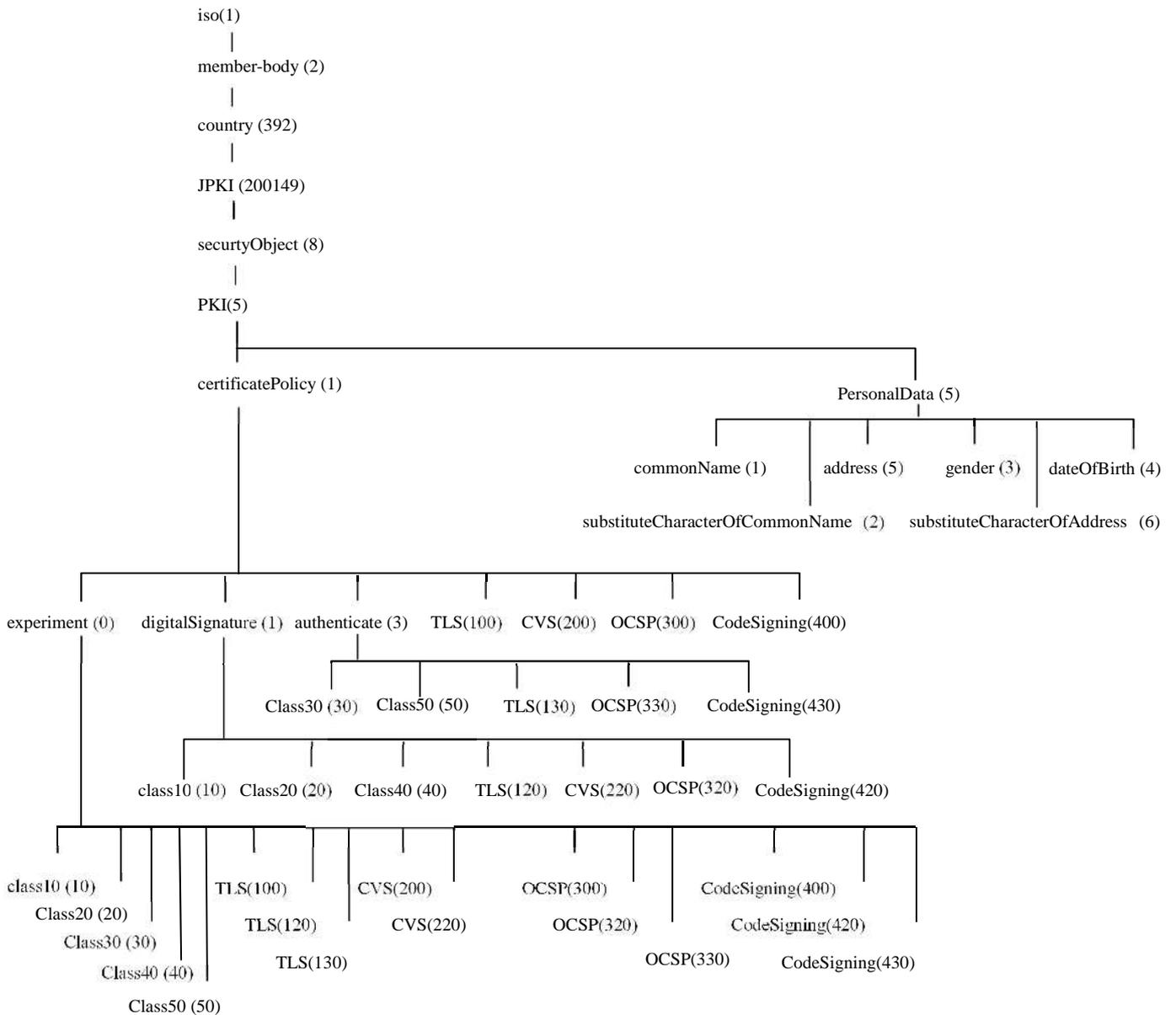


図 2-1 OID 体系

表 2-1 OID 体系

OID 体系		各層の意味
JPKI (200149)		公的個人認証サービス
securityObject(8)		
PKI (5)		
certificatePolicy(1)		証明書ポリシー
experiment(0)		検証環境
Class10(10)		検証環境都道府県認証局証明書ポリシー
Class20(20)		個人番号カード用検証環境署名用認証局証明書ポリシー
Class30(30)		個人番号カード用検証環境利用者証明用認証局証明書ポリシー
Class40(40)		移動端末設備用検証環境署名用認証局証明書ポリシー
Class50(50)		移動端末設備用検証環境利用者証明用認証局証明書ポリシー
TLS(100)		検証環境都道府県認証局の SSL 証明書ポリシー (TLS 認証用)
TLS(120)		検証環境署名用認証局の SSL 証明書ポリシー (TLS 認証用)
TLS(130)		検証環境利用者証明用認証局の SSL 証明書ポリシー (TLS 認証用)
CVS(200)		検証環境都道府県認証局の官職証明書検証サーバ証明書ポリシー
CVS(220)		検証環境署名用認証局の官職証明書検証サーバ証明書ポリシー
OCSP(300)		検証環境都道府県認証局の OCSP レスポンド証明書ポリシー
OCSP(320)		検証環境署名用認証局の OCSP レスポンド証明書ポリシー
OCSP(330)		検証環境利用者証明用認証局の OCSP レスポンド証明書ポリシー
CodeSigning(400)		検証環境都道府県認証局のコードサイニング証明書ポリシー
CodeSigning(420)		検証環境署名用認証局のコードサイニング証明書ポリシー
CodeSigning(430)		検証環境利用者証明用認証局のコードサイニング証明書ポリシー

digitalSignature(1)	電子署名用
Class10(10)	都道府県認証局証明書ポリシー
Class20(20)	個人番号カード用署名用認証局証明書ポリシー
Class40(40)	移動端末設備用検証環境署名用認証局証明書ポリシー
TLS(120)	署名用認証局の SSL 証明書ポリシー ( TLS 用 )
CVS(220)	署名用認証局の官職証明書検証サーバ証明書ポリシー
OCSP(320)	署名用認証局の OCSP レスポンダ証明書ポリシー
CodeSigning(420)	署名用認証局のコードサイニング証明書ポリシー
Authenticate(3)	利用者証明用
Class30(30)	個人番号カード用利用者証明用認証局証明書ポリシー
Class50(50)	移動端末設備用検証環境利用者証明用認証局証明書ポリシー
TLS(130)	利用者証明用認証局の SSL 証明書ポリシー ( TLS 用 )
OCSP(330)	利用者証明用認証局の OCSP レスポンダ証明書ポリシー
CodeSigning(430)	利用者証明用認証局のコードサイニング証明書ポリシー
TLS(100)	都道府県認証局の SSL 証明書ポリシー ( TLS 認証用 )
CVS(200)	都道府県認証局の官職証明書検証サーバ証明書ポリシー
OCSP (300)	都道府県認証局の OCSP レスポンダ証明書ポリシー
CodeSigning(400)	都道府県認証局のコードサイニング証明書ポリシー
PersonalData(5)	利用者基本 4 情報
commonName(1)	氏名
address(5)	住所
gender(3)	男女の別
dateOfBirth(4)	出生の年月日

			substituteCharacterOfCommonName (2)	代替文字の使用：氏名
			substituteCharacterOfAddress (6)	代替文字の使用：住所

禁・無断転載

公的個人認証サービス

プロフィール仕様書

第 3.1 版