公的個人認証サービス

プロファイル仕様書

2.0 版

令和元年 5 **月** 1 **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.「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「①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②署名用電子証明書のプロファイル拡張領域（Extension）		修正

目次

第 1 章 はじめに

本プロファイル仕様書は、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

本プロファイ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、プロファイ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. 署名用電子証明書のプロファイル

① 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
	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 ・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、更新前の有効期限満了日から 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	-	-	
	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	(YYYYMMDDhhmmssxxxxxXXXXXXXXX)	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

② 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]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 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
[2]authorityCertSerialNumber			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		利用者日本語表記	-	-	
extnID			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)
		[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)	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
[0]otherName	利用者の氏名代替文字の使用位置情報	-	-	
substituteCharacterOfCommonName		-	-	
type		OBJECT IDENTIFIER	1 2 392 200149 8 5 5 2 (固定)	「substituteCharacterOfCommonName」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
[0]otherName	利用者の住所代替文字の使用位置情報	-	-	
substituteCharacterOfAddress		-	-	
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	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 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		-	-	
		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	-	-	
extnID			OBJECT IDENTIFIER	2 5 29 32 (固定)	「certificatePolicies」の OID
critical			BOOLEAN	TRUE (固定)	
extnValue			OCTET STRING	-	
	policyIdentifier		OBJECT IDENTIFIER	1 2 392 200149 8 5 1 1 20	公的個人認証サービスの署名用電子証明書ポリシの 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			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

2.1.2. 利用者証明用電子証明書のプロファイル

① 利用者証明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

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 ・電子証明書の更新時で、更新前の有効期限満了日から 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	-	-	
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	（ xxxxxxxxxxxxxxXXXXXXXXX)	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

② 利用者証明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]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
[2]authorityCertSerial		INTEGER	（公開鍵のシリアル番号	認証局の公開鍵を一意に識別する

Number			(16 進数))	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	100000000 (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		-	-	
type		OBJECT IDENTIFIER	2 5 4 11 (固定)	「organizationalUnitName」の OID

value		UTF8String	公的個人認証サービス利用者証明用 (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	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
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		-	-	
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	-	-	
extnID		OBJECT IDENTIFIER	2 5 29 32 (固定)	「certificatePolicies」の OID
critical		BOOLEAN	TRUE (固定)	
extnValue		OCTET STRING	-	
policyIdentifier		OBJECT IDENTIFIER	1 2 392 200149 8 5 1 3 30	公的個人認証サービスの利用者証明用電子証明書ポリシの 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		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
authorityInfoAccess	機関アクセス情報	-	-	-
extnID		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.jpki.go.jp	OCSP レスポンダの URL

2.1.3. 署名用認証局の自己署名証明書のプロファイル

① 署名用認証局の自己署名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

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

② 署名用認証局の自己署名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				
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署名用 (固定)	
organizationalUnitName		-	-	
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		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	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	-	-	

extnID		者の公開鍵の識別子	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

2.1.4. 利用者証明用認証局の自己署名証明書のプロファイル

① 利用者証明用認証局の自己署名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
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

② 利用者証明用認証局の自己署名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				
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		-	-	
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		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
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

2.2. 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、財団法人日本情報処理開発協会電子商取引推進センター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
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
Class20(20)	検証環境署名用認証局証明書ポリシ
Class30(30)	検証環境利用者証明用認証局証明書ポリシ
TLS(100)	検証環境都道府県認証局の SSL 証明書ポリシ（TLS 認証用）
TLS(120)	検証環境署名用認証局の SSL 証明書ポリシ（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（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
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
OCSP(300)	検証環境都道府県認証局の OCSP レスポンダ証明書ポリシ
OCSP(320)	検証環境署名用認証局の OCSP レスポンダ証明書ポリシ
OCSP(330)	検証環境利用者証明用認証局の OCSP レスポンダ証明書ポリシ
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
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
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
digitalSignature(1)	電子署名用
Class10(10)	都道府県認証局証明書ポリシ
Class20(20)	署名用認証局証明書ポリシ
TLS(120)	署名用認証局の SSL 証明書ポリシ（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
OCSP(320)	署名用認証局の OCSP レスポンダ証明書ポリシ
CodeSigning(420)	署名用認証局のコードサイニング証明書ポリシ
Authenticate(3)	利用者証明用
Class30(30)	利用者証明用認証局証明書ポリシ
TLS(130)	利用者証明用認証局の SSL 証明書ポリシ（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
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
TLS(100)	都道府県認証局の SSL 証明書ポリシ(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
OCSP (300)	都道府県認証局の OCSP レスポンダ証明書ポリシ
CodeSigning(400)	都道府県認証局のコードサイニング証明書ポリシ
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

公的個人認証サービス

プロファイル仕様書

第 2.0 版