公的個人認証サービス

プロファイル仕様書
（相互認証証明書）

第 1.0 版

公的個人認証サービス 指定認証機関

財団法人　自治体衛星通信機構

第１章　はじめに

本仕様書は、公的個人認証サービスにおける相互認証証明書について定めたものである。

第１節　概要

本仕様書の概要は以下の通りである。

１　プロファイル仕様

電子証明書のプロファイルについて、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。

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。

３　都道府県ローマ字表記一覧

各種証明書の DN に記載される都道府県名のローマ字表記の一覧を記述する。

第２章　諸元

第１節　プロファイル仕様

1　相互認証証明書（都道府県単位認証局－個人認証ブリッジ認証局）のプロファイル

（１）相互認証証明書（都道府県単位認証局－個人認証ブリッジ認証局）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 の意味
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 5(固定)	暗号アルゴリズムの OID(1 2 840 113549 1 1 5 は「Sha-1WithRSAEncryption」)
parameters		NULL	(なし)	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	(都道府県名称の英語表記)	「第３節　都道府県名ローマ字表記一覧」参照
organizationalUnitName		－	－	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	(都道府県知事を指す名称の英語表記)	「第３節　都道府県名ローマ字表記一覧」参照
validity	電子証明書の有効期間	－	－	
notBefore	開始日時	UTCTime	(YYMMDDhhmmssZ)	グリニッジ標準時
notAfter	終了日時	UTCTime	(YYMMDDhhmmssZ)	グリニッジ標準時 notBefore ＋5 年後の前日の 14:59:59（日本時間の 23:59:59 を表す)
subject	電子証明書利用者	－	－	
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	Prefectural Association For JPKI (固定)	「都道府県協議会」の意味
	organizationalUnit Name			―	―	
		type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
		value		UTF8String	BridgeCA(固定)	
subjectPublicKeyInfo			電子証明書利用者の公開鍵に関する情報	―	―	
	algorithm		暗号アルゴリズムのオブジェクト ID	―	―	
		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 の場合はなし
	subjectPublicKey		公開鍵値	BIT STRING	(公開鍵値(16 進数))	鍵長 2048bit

（２） 相互認証証明書（都道府県単位認証局－個人認証ブリッジ認証局）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		OCTET STRING	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	(都道府県名称の英語表記)	「第３節 都道府県名ローマ字表記一覧」参照
organizationalUnitName		－	－	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	(都道府県知事を指す名称の英語表記)	「第３節 都道府県名ローマ字表記一覧」参照
[2]authorityCertSerialNumnber		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	0000011 (固定)	鍵用途を示すビット列「keyCertSign(5) ＆ cRLSign(6)」の意味
basicConstraints	基本的制約	－	－	
extnID		OBJECT IDENTIFIER	2 5 29 19	「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	(都道府県名称の英語表記)	「第３節　都道府県名ローマ字表記一覧」参照
organizationalUnitName		－	－	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	(都道府県知事を指す名称の英語表記)	「第３節　都道府県名ローマ字表記一覧」参照
certificatePolicies	ポリシーに関する情報		－	
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 10	公的個人認証サービスの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
qualifier		IA5String	http://www.jpki.go.jp/cps.html	CPS 公開 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　相互認証証明書（個人認証ブリッジ認証局－都道府県単位認証局）のプロファイル

（1） 相互認証証明書（個人認証ブリッジ認証局－都道府県単位認証局）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 の意味
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 5(固定)	暗号アルゴリズムの OID (1 2 840 113549 1 1 5 は「Sha-1WithRSAEncryption」)
parameters		NULL	(なし)	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	Prefectural Association For JPKI (固定)	「都道府県協議会」の意味
organizationalUnitName		－	－	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	BridgeCA(固定)	
validity	電子証明書の有効期間	－	－	
notBefore	開始日時	UTCTime	(YYMMDDhhmmssZ)	グリニッジ標準時
notAfter	終了日時	UTCTime	(YYMMDDhhmmssZ)	グリニッジ標準時 notBefore ＋5 年後の前日の 14:59:59（日本時間の 23:59:59 を表す)
subject	電子証明書利用者	－	－	
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	(都道府県名称の英語表記)	「第３節　都道府県名ローマ字表記一覧」参照
organizationalUnitName		－	－	

		type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
		value		UTF8String	(都道府県知事を指す名称の英語表記)	「第３節　都道府県名ローマ字表記一覧」参照
subjectPublicKeyInfo			電子証明書利用者の公開鍵に関する情報	－	－	
	algorithm		暗号アルゴリズムのオブジェクト ID	－	－	
		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 の場合はなし
	subjectPublicKey		公開鍵値	BIT STRING	(公開鍵値(16 進数))	鍵長 2048bit

（２） 相互認証証明書（個人認証ブリッジ認証局－都道府県単位認証局）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		OCTET STRING	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	Prefectural Association For JPKI (固定)	「都道府県協議会」 の意味
organizationalUnitName		－	－	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	BridgeCA(固定)	
[2]authorityCertSerialNumnber		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	0000011 (固定)	鍵用途を示すビット列「keyCertSign(5) ＆ cRLSign(6)」の意味
basicConstraints	基本的制約	－	－	
extnID		OBJECT IDENTIFIER	2 5 29 19	「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	Prefectural Association For JPKI (固定)	「都道府県協議会」の意味
organizationalUnitName		－	－	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	BridgeCA(固定)	
certificatePolicies	ポリシーに関する情報		－	
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 10	公的個人認証サービスの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
qualifier		IA5String	http://www.jpki.go.jp/cps.html	CPS 公開 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

3　相互認証証明書（個人認証ブリッジ認証局－GPKI のブリッジ認証局）のプロファイル

（1） 相互認証証明書（個人認証ブリッジ認証局－GPKI のブリッジ認証局）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 の意味
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 5(固定)	暗号アルゴリズムの OID(1 2 840 113549 1 1 5 は「Sha-1WithRSAEncryption」)
parameters		NULL	(なし)	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	Prefectural Association For JPKI (固定)	「都道府県協議会」の意味
organizationalUnitName		－	－	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	BridgeCA （固定）	
validity	電子証明書の有効期間	－	－	
notBefore	開始日時	UTCTime	(YYMMDDhhmmssZ)	グリニッジ標準時
notAfter	終了日時	UTCTime	(YYMMDDhhmmssZ)	グリニッジ標準時 notBefore ＋5 年後の前日の 14:59:59（日本時間の 23:59:59 を表す)
subject	電子証明書利用者	－	－	
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	Japanese Government	
organizationalUnitName		－	－	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	BridgeCA	

subjectPublicKeyInfo		電子証明書利用者の公開鍵に関する情報	－	－	
	algorithm	暗号アルゴリズムのオブジェクト ID	－	－	
	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 の場合はなし
	subjectPublicKey	公開鍵値	BIT STRING	(公開鍵値(16 進数))	鍵長 2048bit

（２） 相互認証証明書（個人認証ブリッジ認証局－GPKI のブリッジ認証局）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		OCTET STRING	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	Prefectural Association For JPKI (固定)	「都道府県協議会」 の意味
organizationalUnitName		－	－	
Type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	BridgeCA (固定)	
[2]authorityCertSerialNumnber		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	0000011 (固定)	鍵用途を示すビット列「keyCertSign(5) ＆ cRLSign(6)」の意味
policyMappings	ポリシマッピング	－	－	
extnID		OBJECT IDENTIFIER	2 5 29 33	「policyMappings」の OID
critical		BOOLEAN	FALSE	
extnValue		OCTET STRING	－	

issuerDomainPolicy		OBJECT IDENTIFIER	1 2 392 200149 8 5 1 1 10	公的個人認証サービスの電子証明書ポリシーの OID
subjectDomainPolicy		OBJECT IDENTIFIER	Id-bca-cp-ds.class10	GPKI ブリッジ認証局ポリシーの OID（申請時に調整が必要）
basicConstraints	基本制約	－	－	
extnID		OBJECT IDENTIFIER	2 5 29 19	「basicConstraints」の OID
critical		BOOLEAN	TRUE(固定)	
extnValue		OCTET STRING	－	
cA		BOOLEAN	TRUE(固定)	
policyConstraints	ポリシ制約	－	－	
extnID		OBJECT IDENTIFIER	2 5 29 36	
critical		BOOLEAN	TRUE(固定)	
extnValue		OCTET STRING	－	
requireExplicitPolicy		INTEGER	0	ポリシの明示を要求
inhibitPolicyMapping		INTEGER	1	
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	Prefectural Association For JPKI (固定)	「都道府県協議会」の意味
organizationalUnitName		－	－	
type		OBJECT IDENTIFIER	2 5 4 11(固定)	「organizationalUnitName」の OID
value		UTF8String	BridgeCA（固定）	
certificatePolicies	ポリシーに関する情報		－	
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 10	公的個人認証サービスの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

qualifier		IA5String	http://www.jpki.go.jp/cps.html	CPS 公開 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

第２節　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。

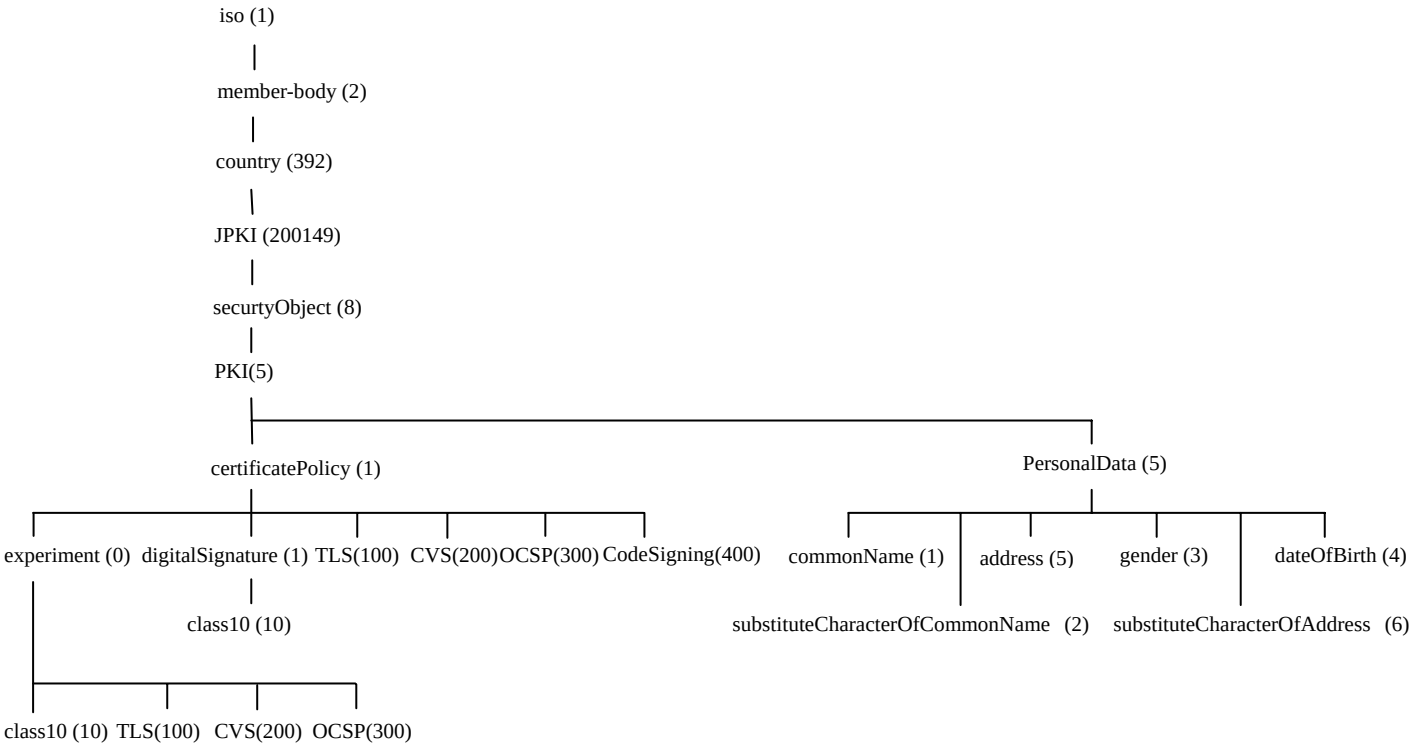

図 ２-１　ＯＩＤ体系

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)	証明書ポリシー
experiment(0)	実験用
Class10(10)	実験用証明書ポリシー
TLS(100)	実験用 TLS 認証
CVS(200)	実験用官職証明書検証サーバ証明書ポリシー
OCSP(300)	実験用 OCSP レスポンダ証明書ポリシー
digitalSignature(1)	電子署名用
Class10(10)	証明書ポリシー
TLS(100)	TLS 認証
CVS(200)	官職証明書検証サーバ証明書ポリシー
OCSP (300)	OCSP レスポンダ証明書ポリシー
CodeSigning(400)	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

第３節　都道府県ローマ字表記一覧

表 2-2　都道府県ローマ字表記一覧

県名	県名ローマ字表記	知事名	知事ローマ字表記
北海道	Hokkaido	北海道知事	the Governor of Hokkaido
青森県	Aomori-ken	青森県知事	the Governor of Aomori-ken
岩手県	Iwate-ken	岩手県知事	the Governor of Iwate-ken
宮城県	Miyagi-ken	宮城県知事	the Governor of Miyagi-ken
秋田県	Akita-ken	秋田県知事	the Governor of Akita-ken
山形県	Yamagata-ken	山形県知事	the Governor of Yamagata-ken
福島県	Fukushima-ken	福島県知事	the Governor of Fukushima-ken
茨城県	Ibaraki-ken	茨城県知事	the Governor of Ibaraki-ken
栃木県	Tochigi-ken	栃木県知事	the Governor of Tochigi-ken
群馬県	Gunma-ken	群馬県知事	the Governor of Gunma-ken
埼玉県	Saitama-ken	埼玉県知事	the Governor of Saitama-ken
千葉県	Chiba-ken	千葉県知事	the Governor of Chiba-ken
東京都	Tokyo-to	東京都知事	the Governor of Tokyo-to
神奈川県	Kanagawa-ken	神奈川県知事	the Governor of Kanagawa-ken
新潟県	Niigata-ken	新潟県知事	the Governor of Niigata-ken
富山県	Toyama-ken	富山県知事	the Governor of Toyama-ken
石川県	Ishikawa-ken	石川県知事	the Governor of Ishikawa-ken
福井県	Fukui-ken	福井県知事	the Governor of Fukui-ken
山梨県	Yamanashi-ken	山梨県知事	the Governor of Yamanashi-ken
長野県	Nagano-ken	長野県知事	the Governor of Nagano-ken
岐阜県	Gifu-ken	岐阜県知事	the Governor of Gifu-ken
静岡県	Shizuoka-ken	静岡県知事	the Governor of Shizuoka-ken
愛知県	Aichi-ken	愛知県知事	the Governor of Aichi-ken
三重県	Mie-ken	三重県知事	the Governor of Mie-ken
滋賀県	Shiga-ken	滋賀県知事	the Governor of Shiga-ken
京都府	Kyoto-fu	京都府知事	the Governor of Kyoto-fu
大阪府	Osaka-fu	大阪府知事	the Governor of Osaka-fu
兵庫県	Hyogo-ken	兵庫県知事	the Governor of Hyogo-ken
奈良県	Nara-ken	奈良県知事	the Governor of Nara-ken
和歌山県	Wakayama-ken	和歌山県知事	the Governor of Wakayama-ken
鳥取県	Tottori-ken	鳥取県知事	the Governor of Tottori-ken
島根県	Shimane-ken	島根県知事	the Governor of Shimane-ken
岡山県	Okayama-ken	岡山県知事	the Governor of Okayama-ken
広島県	Hiroshima-ken	広島県知事	the Governor of Hiroshima-ken
山口県	Yamaguchi-ken	山口県知事	the Governor of Yamaguchi-ken
徳島県	Tokushima-ken	徳島県知事	the Governor of Tokushima-ken
香川県	Kagawa-ken	香川県知事	the Governor of Kagawa-ken
愛媛県	Ehime-ken	愛媛県知事	the Governor of Ehime-ken
高知県	Kochi-ken	高知県知事	the Governor of Kochi-ken
福岡県	Fukuoka-ken	福岡県知事	the Governor of Fukuoka-ken
佐賀県	Saga-ken	佐賀県知事	the Governor of Saga-ken
長崎県	Nagasaki-ken	長崎県知事	the Governor of Nagasaki-ken
熊本県	Kumamoto-ken	熊本県知事	the Governor of Kumamoto-ken
大分県	Oita-ken	大分県知事	the Governor of Oita-ken
宮崎県	Miyazaki-ken	宮崎県知事	the Governor of Miyazaki-ken
鹿児島県	Kagoshima-ken	鹿児島県知事	the Governor of Kagoshima-ken
沖縄県	Okinawa-ken	沖縄県知事	the Governor of Okinawa-ken

公的個人認証サービス

プロファイル仕様書

第 1.0 版