7. 証明書と、証明書失効リスト及び OCSP のプロファイル

7.1. 証明書のプロファイル

本認証局が発行する証明書は、X.509 証明書フォーマットのバージョン 3 に従う。証明書プロファイルは、表 7-1 のとおりである。

7.1.1. バージョン番号

本認証局が発行する証明書は全て X.509 バージョン 3 証明書フォーマットに従う。

7.1.2. 証明書拡張

本認証局が発行する証明書に使用される拡張領域を次に示す。

7.1.2.1. authorityKeyIdentifier

keyIdentifier の値として本認証局の公開鍵の 160bit SHA-1 ハッシュ値を使用する。この拡張は non-critical である。

7.1.2.2. subjectKeyIdentifier

当該証明書所有者の公開鍵の 160bit SHA-1 ハッシュ値を使用する。この拡張は non-critical である。

7.1.2.3. keyUsage

契約／資源管理者証明書、資源申請者証明書、JPNIC 職員向け証明書は digitalSignature、keyEncipherment、dataEncipherment を使用する。サーバ証明書は digitalSignature と keyEncipherment のみを使用する。この拡張は non-critical である。

7.1.2.4. certificatePolicies

契約／資源管理者証明書、資源申請者証明書、JPNIC 職員向け証明書は certificatePolicies 拡張を使用する。policyIdentifier の値は本 CPS「7.1.6.証明書ポリ

シ OID」、policyQualifiers の値は本 CPS「7.1.8.ポリシ修飾子の記述と意味」に示す。この拡張は non-critical である。

7.1.2.5. subjectAltName

rfc822Name として証明書所有者の電子メールアドレスを記述する。この拡張は non-critical である。

7.1.2.6. cRLDistributionPoints

本認証局が発行する CRL の URI を記述する。この拡張は non-critical である。

7.1.3. アルゴリズム OID

本認証局が発行する証明書において使用されるアルゴリズム OID は次の 2 つである。

- sha1withRSAEncryption（1.2.840.113549.1.1.5）
- rsaEncryption（1.2.840.113549.1.1.1）

7.1.4. 名前形式

本 CPS「3.1.1.名前の種類」に従う。

7.1.5. 名前制約

本認証局は、発行する全ての証明書において nameConstraints 拡張を使用しない。

7.1.6. 証明書ポリシ OID

資源申請者証明書、契約／資源管理者証明書、JPNIC 職員向け証明書のいずれも本 CPS「1.2.文書の名前と識別」に定める EE 証明書ポリシの OID を使用する。

7.1.7. ポリシ制約拡張

本認証局は、発行する全ての証明書において policyConstraints 拡張を使用しない。

7.1.8. ポリシ修飾子の記述と意味

資源申請者証明書、サーバ証明書共にポリシ修飾子の値として本 CPS が公開されている URI を使用する。

7.1.9. critical な証明書 certificatePolicies 拡張の処理

本認証局が発行する証明書に含まれる certificatePolicies 拡張は全て non-critical であり、本項の規定を行わない。

表 7-1 JPNIC 資源管理認証局が発行する証明書プロファイル

Field	critical flag	契約／資源管理者証明書、資源申請者証明書、JPNIC職員向け証明書
version	NA	2
serialNumber	NA	non-negative integer
signature	NA	
algorithm		sha1withRSAEncryption
parameters		null
issuer	NA	
		PrintableString[*1]
validity	NA	
notBefore		UTCTime
notAfter		UTCTime notBeforeの時刻より2年後
subject	NA	
		PrintableString[*2]
subjectPublicKeyInfo	NA	
algorithm		rsaEncryption
parameters		null
subjectPublicKey		公開鍵のBIT STRING
authorityKeyIdentifier	n	
keyIdentifier		JPNIC IPアドレス認証局 公開鍵の160bit SHA-1 ハッシュ値
authorityCertIssuer		使用しない
authorityCertSerialNumber		使用しない
subjectKeyIdentifier	n	公開鍵の160bit SHA-1ハッシュ値
keyUsage	n	
digitalSignature		1
nonRepudiation		0
keyEncipherment		1
dataEncipherment		1
certificatePolicies	n	
policyIdentifier		本CPのOID
policyQualifiers		
policyQualifierId		CPSUri
qualifier		本CP/CPSを公開するURI
subjectAltName	n	
rfc822Name		メールアドレス
cRLDistributionPoints	n	
DistributionPoint		
distributionPoint		本認証局が CRLを公開するURI
reasons		使用しない
cRLIssuer		使用しない

※1　C=JP, O=Japan Network Information Center, OU=Internet Resource Service, OU=JPNIC Resource Service Certification Authority

※2　C=JP, O=（組織名称）, O=Resource Holder, O=LIR Corporate Administrator, OU=（LIR Corporate Administrator、LIR Administrator、LIR

Hostmaster のいずれか），OU=（JPNIC が資源管理の単位ごとに割り当てるメンテナーコード）CN=（LIR-CO、LIR-AD、LIR-HM、ASN-HLD、JPNIC-AD、JPNIC-CO のいずれか）＋（JPNIC がユーザごとに割り当てる認証 ID）＋（証明書発行対象の名称をアルファベット表記したもの）

7.2. 証明書失効リストのプロファイル

本認証局が発行する CRL は、X.509CRL フォーマットのバージョン 2 に従う。CRL プロファイルは、表 7-2 のとおりである。

7.2.1. バージョン番号

本認証局が発行する CRL は全て X.509 バージョン 2CRL フォーマットに従う。

7.2.2. CRL 及び CRL エントリ拡張

本認証局は次の 2 つの CRL 拡張を使用し、CRL エントリ拡張は使用しない。

7.2.2.1. cRLNumber

本認証局が発行する CRL において一意となる非負の整数を使用する。

7.2.2.2. authorityKeyIdentifier

keyIdentifier の値として本認証局の公開鍵の 160bit SHA-1 ハッシュ値を使用する。この拡張は non-critical である。

表 7-2 JPNIC 資源管理認証局が発行する CRL プロファイル

Field	critical flag	証明書失効リスト
version	NA	1
signature	NA	
algorithm		sha1withRSAEncryption
parameters		null
issuer	NA	
		PrintableString[*1]
thisUpdate	NA	UTCTime
nextUpdate	NA	UTCTime thisUpdateより24時間後
revokedCertificates	NA	
revokedCertificate		
userCertificate		失効された証明書の シリアル番号
revocationDate		UTCTime 証明書の失効された時刻
crlEntryExtensions		
		使用しない
crlExtensions	NA	
cRLNumber	n	non-negative integer
authorityKeyIdentifier	n	本認証局 公開鍵の160bit SHA-1ハッシュ値

※1　C=JP, O=Japan Network Information Center, OU=Internet Resource Service, OU=JPNIC Resource Service Certification Authority

7.3. OCSP プロファイル

7.3.1. バージョン情報

使用しない。

7.3.2. OCSP 拡張

使用しない。