【CSR プロファイル】

本実証実験で使用する UPKI サーバ証明書の CSR は，以下の形式となります。

基本領域		設定内容	補
Version		Version 1(0)	-
Subject	Country	C=JP（固定値）	1
	Locality	L=Academe（固定値）	1
	Organization	O="主体者組織名" ＊ 機関毎に任意に指定 例) o= National Institute of Informatics	1
	Organizational Unit	OU="主体者組織単位名" ＊ 証明書毎に任意に指定 例) ou= NII Open Domain CA	1
	commonName	CN="サーバ FQDN" ＊証明書毎に任意に指定 例) cn=www.nii.ac.jp	1
SubjectPublicKeyInfo		主体者の公開鍵　1024 ビット以上 （ただし、例外を認める）	2
attrobites		原則 Null 値とする （ただし、例外を認める）	3
SignatureAlgorithm		SHA1 with RSAEncryption	

1. 上記指定以外の属性を利用する必要がある場合には事前相談すること。少なくとも ST（state or province name）属性は使用しないこと。また、例えば加入者メールアドレスなど本プロジェクトの確認項目対象外の情報を含めないこと。
2. RSA1024bit 以上とする。鍵長 1024bit 未満の場合には事前に登録局へ相談すること。
3. 任意の属性を含めても構わないが、必ずしも証明書に反映されるわけではない。また、含めた属性によっては受理不能とし、当該属性を除いて証明書発行要求の再生成を登録局から求める場合がある。少なくとも SubjectAltName.rfc822Name 属性は使用しないこと。