pubAlg	AlgorithmIdentifier	
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.1 ◎
parameters	NULL	（注２） ○
hashAlg	AlgorithmIdentifier	
algorithm	OBJECT IDENTIFIER	2.16.840.1.101.3.4.2.1 ◎
parameters	NULL	（注２） ○
protection	[0]	
－	PKIProtection	（注８） ◎
extraCerts	[1]	
－	SEQUENCE OF Certificate	（注９） ◎

注１　「必須」欄中に◎印のあるフィールドには、必ず値を記録しなければならない。「必須」欄中に○印のあるフィールドは、必ず設けなければならない。

注２　長さオクテットに「0」を記録する。

注３　注９に記録された登記官の電子証明書の「subjectPublicKey」の値（識別子オクテット、長さオクテット及び未使用ビットを除く。）を SHA-1 により変換した値を記録する。

注４　「開始要求電文」中の「transactionID」に記録された値を記録する。

注５　１バイト以上 32 バイト以下の乱数を記録する。

注６　「開始要求電文」中の「senderNonce」に記録された値を記録する。

注７　「開始要求電文」を正常に受信したことを示すため、「0」を記録する。「開始要求電文」に異常があった場合には、後記５による。

注８　付録３に示す「ProtectedPart」を DER により符号化した値に sha-256WithRSA による電子署名を講じた値を記録する。

注９　登記官の最新の電子証明書を記録する。

（４）「証明書要求電文」中の「entity-body」の内容

フィールド	データ型	設定値	必須（注１）
－	PKIMessage		
header	PKIHeader		
pvno	INTEGER	1	◎
sender	GeneralName([4])		
－	Name(RDNSequence)	（注２）	○
recipient	GeneralName([4])		
－	Name(RDNSequence)	（注２）	○
transactionID	[4]		
－	OCTET STRING	「開始応答電文」中の「transactionID」を記録する。	◎
senderNonce	[5]		
－	OCTET STRING	「開始応答電文」中の「recipNonce」を記録する。	◎
recipNonce	[6]		
－	OCTET STRING	「開始応答電文」中の「senderNonce」を記録する。	◎
body	PKIBody([0])		
－	CertReqMessages		
－	CertReqMsg		
certReq	CertRequest		
certReqId	INTEGER	0	◎
certTemplate	CertTemplate		
serialNumber	[1] INTEGER	商業登記規則第３３条の８第２項第２号の電子証明書の番号を記録する。	◎
publicKey	[6] SubjectPublicKeyInfo		
algorithm	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.1	◎
parameters	NULL	（注２）	○
subjectPublicKey	BIT STRING	請求に係る公開かぎを記録する。	◎
pop	ProofOfPossession ([1]POPOSigningKey)		
algorithmIdentifier	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.11（注３）	◎
parameters	NULL		△
signature	BIT STRING	（注４）	◎

注１　「必須」欄中に◎印のあるフィールドには、必ず値を記録しなければならない。「必須」欄中に○印のあるフィールドは、必ず設けなければならない。「必須」欄中に△印のあるフィールドは、記録する内容によって任意に設けることができる。

注２　長さオクテットに「0」を記録する。

注３　当分の間、sha1WithRSA によることもできる。

注４　「certReq」に属する部分を DER により符号化した値に sha-256WithRSA による電子署名を講じた値を記録する。ただし、「subjectPublicKey」に記録した公開かぎにより当該電子署名を講じた措置が検証できるものでなければならない。

（５）「証明書応答電文」中の「entity-body」の内容

フィールド	データ型	設定値	必須（注１）
－	PKIMessage		
header	PKIHeader		
pvno	INTEGER	1	◎
sender	GeneralName([4])		
－	Name(RDNSequence)	（注２）	○
recipient	GeneralName([4])		
－	Name(RDNSequence)	（注２）	○
protectionAlg	[1]		
－	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.11	◎
parameters	NULL	（注２）	○
senderKID	[2]		
－	KeyIdentifier	（注３）	◎
transactionID	[4]		
－	OCTET STRING	（注４）	◎
senderNonce	[5]		
－	OCTET STRING	（注５）	◎
recipNonce	[6]		
－	OCTET STRING	（注６）	◎
body	PKIBody([1])		
－	CertRepMessage		
response	SEQUENCE OF CertResponse		
－	CertResponse		
certReqId	INTEGER	0	◎
status	PKIStatusInfo		
status	PKIStatus	0（注７）	◎
certifiedKeyPair	CertifiedKeyPair		
certOrEncCert	CertOrEncCert([1])		