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	◎
parameters	NULL		△
signature	BIT STRING	（注３）	◎

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　「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])		
－	EncryptedValue		
symmAlg	[1] AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.3.7	◎
parameters	CBCParameter	IV	◎
encSymmKey	[2] BIT STRING	（注８）	◎
keyAlg	[3] AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.1	◎
parameters	NULL	（注２）	○
encValue	BIT STRING	（注９）	◎
protection	[0]		
－	PKIProtection	（注１０）	◎
extraCerts	[1]		
－	SEQUENCE OF Certificate	（注１１）	◎

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　登記官の最新の電子証明書の「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　「証明書要求電文」中の「transactionID」に記録された値を記録する。

注５　「証明書要求電文」中の「recipNonce」に記録された値を記録する。

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

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

注８　電子証明書の暗号化（オブジェクト識別子を「1.2.840.113549.3.7」とする共通かぎ暗号方式によるものに限る。）に用いる共通かぎの値を「証明要求電文」の「subjectPublicKey」に記録された公開かぎを用いて、オブジェクト識別子を「1.2.840.113549.1.1.1」とする暗号アルゴリズムにより暗号化した値を記録する。

注９　電子証明書を注８の共通かぎを用いて暗号化した値を記録する。

注１０　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１１　電子証明書に署名をした登記官の電子証明書を記録する。この場合において、その登記官の電子証明書が最新のものでないときは、最新の電子証明書も併せて記録する。

５　異常時の処理