–	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

（１）「開始要求電文」中の「entity-body」の内容が前記４の（２）に定める形式に適合しない場合（後記（２）の場合を除く。）には、登記官は、「開始応答電文」の項番２については、「Content-Type:application/pkixcmp」に代えて「Content-Type:text/html」と記録し、「entity-body」については、前記４の（３）の内容に代えて、次の内容を記録したものを送信する。この場合には、申請人は、「証明書要求電文」を送信することができない。

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 //EN">
<HTML lang="ja">
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=SHIFT_JIS">
<TITLE> メッセージ異常 </TITLE>
<BODY>
メッセージ内容に問題があるため、処理できませんでした。
</BODY>
</HTML>
```

（２）「開始要求電文」中の「entity-body」に記録された「symmAlg」、「pubAlg」又は「hashAlg」が、前記４の（２）に定める形式に適合しない場合には、登記官は、「開始応答電文」の「entity-body」に、前記４の（３）の内容に代えて、前記４の（１）に定める方式により、次の内容を記録したものを送信する。この場合には、申請人は、「証明書要求電文」を送信することができない。

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([22])		
–	GenRepContent		
–	InfoTypeAndValue		
infoType	OBJECT IDENTIFIER	1.2.392.100300.1.2.22	◎
infoValue	GenpInfoResContent		
Status	PKIStatusInfo		
Status	PKIStatus	2（注７）	◎
Protection	[0]		
–	PKIProtection	（注８）	◎
extraCerts	[1]		
–	SEQUENCE OF Certificate	（注９）	◎

注１から注６まで、注８及び注９については、前記４の（３）の注１から注６まで、注８及び注９に同じ。

注７　「開始要求電文」に異常があったことを示すため、「2」を記録する。

（３）「証明書要求電文」中の「entity-body」が、前記４の（４）に定める形式に適合しない場合（後記５の（４）の場合を除く。）には、登記官は、「証明書応答電文」の「entity-body」に、前記４の（５）の内容に代えて、前記４の（１）に定める方式により、次の内容を記録したものを送信する。この場合には、申請人は、「開始要求電文」を再送信しなければならない。