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([23])		
－	ErrorMsgContent		
pKIStatusInfo	PKIStatusInfo		
Status	PKIStatus	2（注７）	◎
Protection	[0]		
－	PKIProtection	（注８）	◎
extraCerts	[1]		
－	SEQUENCE OF Certificate	（注９）	◎

注１から注６までについては、前記４の（５）の注１から注６までに同じ。

注７　「証明書要求電文」に異常があったことを示すため、「2」を記録する。

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」に記録された「transactionID」、「senderNonce」、「recipNonce」、「serialNumber」又は「subjectPublicKey」が、前記４の（４）に定める形式に適合しないときは、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。

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	2（注７）	◎
protection	[0]		
－	PKIProtection	（注８）	◎
extraCerts	[1]		
－	SEQUENCE OF Certificate	（注９）	◎

注１から注９までについては、前記（３）の注１から注９までと同じ。

第４　識別符号の変更の届出に使用する磁気ディスクへの記録の方式

１　使用する磁気ディスク及びファイル名

使用する磁気ディスク、ファイル名及びファイルへの記録方式については、前記第１の１から３までに定めるところによる。

２　識別符号の変更届出ファイル

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)		○
recipient	GeneralName([4])		
－	Name(RDNSequence)		○
Body	PKIBody([0])		
－	CertReqMessages		
－	CertReqMsg		
certReq	CertRequest		○
regInfo	SEQUENCE OF AttributeTypeAndValue		
(suspensionSecretCode)	AttributeTypeAndValue		
type	OBJECT IDENTIFIER	1.2.392.100300.1.2.105	◎
value	SuspensionSecretCode		
hashAlg	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	2.16.840.1.101.3.4.2.1（注２）	◎
parameters	NULL		△
hashedSecretCode	OCTET 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」