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	1.2.392.100300.1.2.2	◎
infoValue	GenpSuspResContent		
status	PKIStatusInfo		
status	PKIStatus	0（注７）	◎
revCert	CertId		
issuer	GeneralName([4])		
－	Name(RDNSequence)		
－	RelativeDistinguishedName		
(countryName)	AttributeTypeAndValue		
type	OBJECT IDENTIFIER	2.5.4.6	◎
value	PrintableString	JP	◎
－	RelativeDistinguishedName		
(organizationName)	AttributeTypeAndValue		
type	OBJECT IDENTIFIER	2.5.4.10	◎
value	DirectoryString (UTF8String)	Japanese Government	◎
－	RelativeDistinguishedName		
(organizationalUnitName)	AttributeTypeAndValue		
type	OBJECT IDENTIFIER	2.5.4.11	◎
value	DirectoryString (UTF8String)	Ministry of Justice	◎
－	RelativeDistinguishedName		
(commonName)	AttributeTypeAndValue		
type	OBJECT IDENTIFIER	2.5.4.3	◎
value	DirectoryString (UTF8String)	Registrar of Tokyo Legal Affairs Bureau	◎
serialNumber	INTEGER	（注８）	◎
protection	[0]		
－	PKIProtection	（注９）	◎
extraCerts	[1]		
－	SEQUENCE OF Certificate	（注１０）	◎

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１０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　「休止届要求電文」中の「transactionID」に記録された値を記録する。

注５　「休止届要求電文」中の「recipNonce」に記録された値を記録する。

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

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

注８　電子証明書の番号を記録する。

注９　付録４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１０　登記官の最新の電子証明書を記録する。

５　異常時の処理

（１）「開始要求電文」中の「entity-body」が前記４の（２）に定める形式に適合しない場合（後記５の（２）に定める場合を除く。）における登記官の措置については、前記第３の５の（１）による。この場合には、届出人は、「休止届要求電文」を送信することができない。

（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）の定める方式により、次の内容を記録したものを送信する。この場合には、届出人は、「休止届要求電文」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）	◎