③　届出人は、登記官に識別符号を含むデータ等を登記官の公開かぎを用いて暗号化した「休止届要求電文」を送信する。

④　登記官は、届出人に sha-256WithRSA による電子署名を講じた「休止届応答電文」を送信する。

3　各電文の構成

前記２の各電文の構成は、次の（１）及び（２）に定めるところにより、各項目に該当する設定値を記録し、その次に区切り欄に掲げる制御記号を記録する。

（１）「開始要求電文」及び「休止届要求電文」の構成

項番	項目	設定値	区切り
1	Request-Line	POST△/bin/dcwcgi/DC_HUSR/cert/cert △HTTP/1.1	CR+LF
2	request-header	Host:crca.moj.go.jp	CR+LF
3	entity-header	Content-Type:application/pkixcmp	CR+LF
		Content-Length:N（注１）	CR+LF
4	general-header	Connection:close	CR+LF CR+LF
5	entity-body	（注２）	

注１　「N」は、項番５「entity-body」のバイト長を記録する。

注２　項番５「entity-body」の設定値は、後記４に定めるところによる。

（２）「開始応答電文」及び「休止届応答電文」の構成

項番	名前	設定値	区切り
1	Status-Line	HTTP/1.1△200△OK	CR+LF
2	entity-header	Content-Type:application/pkixcmp	CR+LF
3		Content-Length:N（注１）	CR+LF
4	general-header	Date:（注２）	CR+LF
5		Connection:close	CR+LF
6	response-header	Server:（注３）	CR+LF
7	Set-Cookie	Set-Cookie: （注４）	CR+LF CR+LF
8	entity-body	（注５）	

注１　「N」は、項番８「entity-body」のバイト長を記録する。

注２　送信の日時をグリニッジ標準時により記録する。

注３　「Server:」の次に、登記官が適宜の事項を記録することができる。

注４　「Set-Cookie:」の次に、登記官が適宜の事項を記録することができる。

注５　項番８「entity-body」の設定値は、後記４に定めるところによる。

4　各電文中の「entity-body」の内容

（１）前記３の各電文中の「entity-body」には、次の（２）から（５）までに定めるところにより、「データ型」欄に掲げる形式を用いて、付録４の様式に従って、「フィールド」欄に掲げる事項を記録する。この場合において、「データ型」欄の形式は、ASN.1 及び付録４に定めるところによる。データの符号化は、DER による。

（２）「開始要求電文」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	１バイト以上３２バイト以下の乱数を記録する。	◎
senderNonce	[5]		
－	OCTET STRING	１バイト以上３２バイト以下の乱数を記録する。	◎
Body	PKIBody([21])		
－	GenMsgContent		
－	InfoTypeAndValue		
infoType	OBJECT IDENTIFIER	1.2.392.100300.1.2.21	◎
infoValue	GenmInfoReqContent		
－	NegotiationKey		
symmAlg	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.3.7	◎
parameters	NULL		△
pubAlg	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.1	◎
parameters	NULL		△
hashAlg	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	2.16.840.1.101.3.4.2.1	◎
parameters	NULL		△

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。

（３）「開始応答電文」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]		