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）「証明要求電文」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/ocsp-request	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の「entity-body」のバイト長を記録する。

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

（２）「証明応答電文」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/ocsp-response	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の「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）又は（３）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５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５に定めるところによる。データの符号化は、DER による。

（２）「証明要求電文」中の「entity-body」の内容

フィールド	データ型	設定値	必須（注１）
－	OCSPRequest		
tbsRequest	TBSRequest		
requestList	SEQUENCE OF Request		
－	Request		
reqCert	CertID		
hashAlgorithm	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	1.3.14.3.2.26	◎
parameters	NULL		△
issuerNameHash	OCTET STRING	証明の対象となる電子証明書の「issuer」に属する部分を、DER により符号化した値を、SHA-1 により変換した値を記録する。	◎
issuerKeyHash	OCTET STRING	（注２）	◎
serialNumber	CertificateSerialNumber	証明の請求に係る電子証明書の番号を記録する。	◎
singleRequestExtensions	[0]		△（注３）
－	Extensions		
(confirmationTime)	Extension		
extnId	OBJECT IDENTIFIER	1.2.392.100300.1.2.102	↑◎
extnValue	OCTET STRING		
－	ConfirmationTime	証明の対象となる過去の特定の日時をグリニッジ標準時により記録する（注４）。	↑◎
requestExtensions	[2]		
－	Extensions		
(nonce)	Extension		
extnId	OBJECT IDENTIFIER	1.3.6.1.5.5.7.48.1.2	◎
extnValue	OCTET STRING		
－	Nonce	1バイト以上32バイト以下の乱数を記録する。	◎

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。「必須」欄中に↑◎印のあるフィールドには、上欄にフィールドを設けたときは、必ず値を記録しなければならない。

注２　証明の対象となる電子証明書を作成し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３　本フィールドを設定することにより、過去の特定の日時についての証明を請求することができる。

注４　「過去の特定の日時」とは、次の①又は②とする。

①　証明の対象となる電子証明書に「notAfter」として記録された日時までの間　にあっては、電子証明書に「notBefore」として記録された日時から証明を請求するまでの間の任意の日時

②　電子証明書に「notAfter」として記録された日時以降から「notAfter」として記録された日を経過してから 7 日を超えない日までの間にあっては、電子証明書に「notBefore」として記録された日時から「notAfter」として記録された日時までの間の任意の日時