extnValue	OCTET STRING	
-	SubjectKeyIdentifier	（注６）
(keyUsage)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.15
extnValue	OCTET STRING	
-	KeyUsage	１０１１０１１００
(privateKeyUsagePeriod)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.16
extnValue	OCTET STRING	
-	PrivateKeyUsagePeriod	
notBefore	[0] GeneralizedTime	（注７）
notAfter	[1] GeneralizedTime	（注８）
(basicConstraints)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.19
extnValue	OCTET STRING	
-	BasicConstraintsSyntax	
cA	BOOLEAN DEFAULT FALSE	TRUE
(registrar)	Extension	
extnId	OBJECT IDENTIFIER	1.2.392.100300.1.1.2
extnValue	OCTET STRING	
-	RegistrarSyntax(UTF8String)	東京法務局登記官
algorithm	AlgorithmIdentifier	
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.11
parameters	NULL	（注２）
signature	BIT STRING	（注９）

注１　登記官の電子証明書の番号を記録する。

注２　長さオクテットに「0」を記録する。

注３　登記官が電子証明書の使用を開始する日の日本時間０時０分０秒をグリニッジ標準時により記録する。

注４　登記官が電子証明書の使用を開始する日から起算して、39 月を経過した日の日本時間 23 時 59 分 59 秒をグリニッジ標準時により記録する。

注５　登記官の公開かぎを記録する。

注６　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７　登記官が電子証明書の使用を開始する日の日本時間０時０分０秒をグリニッジ標準時により記録する。

注８　登記官が電子証明書の使用を開始する日から起算して、12 月を経過した日の日本時間の 23 時 59 分 59 秒をグリニッジ標準時により記録する。

注９　「tbsCertificate」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。

第３　電子証明書の送信の方式

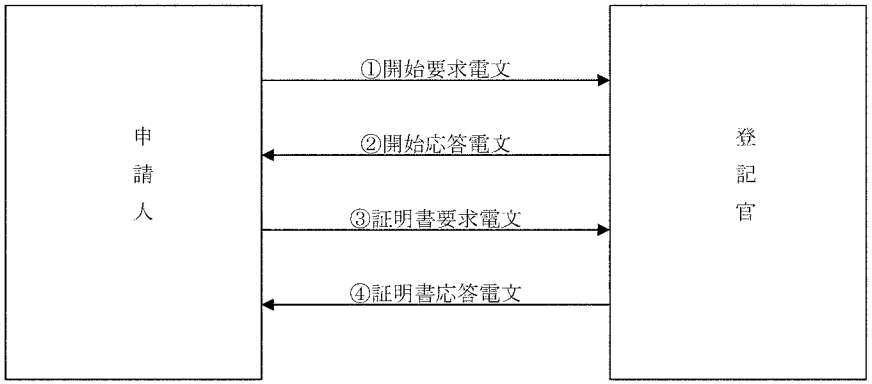
１　通信プロトコル

商業登記規則第 33 条の８第１項の方式による送信に用いる通信プロトコルは、インターネットエンジニアリングタスクフォースが Request for Comments:2616 において定めた Hypertext Transfer Protocol--HTTP/1.1（以下「HTTP」という。）とする。

２　電文の送受信の基本形式

登記官と申請人との間の電文の送受信は、以下の手順による。

なお、①から④までの各電文の構成は、３以下で定める。



①　申請人は、登記官に「開始要求電文」を送信する。

②　登記官は、申請人に sha-256WithRSA による電子署名を講じた「開始応答電文」を送信する。

③　申請人は、登記官に sha-256WithRSA による電子署名を講じた「証明書要求電文」を送信する。sha-256WithRSA は、当分の間、sha1WithRSA によることもできる。

④　登記官は、申請人の電子証明書を共通かぎ暗号方式（共通かぎによる対称アルゴリズムに基づく暗号方式をいう。）により暗号化したもの及び暗号化に用いた共通かぎを申請人の公開かぎを用いて暗号化したものに、sha-256WithRSA による電子署名を講じた「証明書応答電文」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（「CR」は「復帰」を、「LF」は「改行」を示す。以下同じ。）を記録する。

（１）「開始要求電文」及び「証明書要求電文」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（注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２）	CR+LF