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、60 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

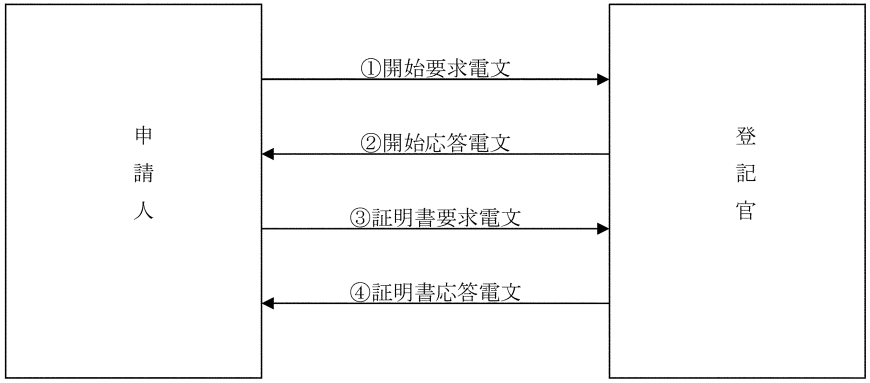
１　通信プロトコル

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（以下「IETF」という。）が Request for Comments（以下「RFC」という。）:9112 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。

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
4	general-header	Connection:close	CR+LF CR+LF
5	entity-body	（注３）	

注１　「△」は、スペース（間隔）を表す。以下同じ。

注２　「N」は、項番５「entity-body」のバイト長を記録する。

注３　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「証明書応答電文」の構成

項番	項目	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３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」欄に掲げる形式は、ASN.1 及び付録３に定めるところによる。データの符号化は、DER による。