| | | | |
|---|---|---|---|
| － | 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から注６までについて、前記４の（５）の注１から注６までに同じ。

注７　「休止届要求電文」に異常があったことを示すため、「2」を記録する。

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。

## 第６　電子証明書に係る証明及びその請求の方式

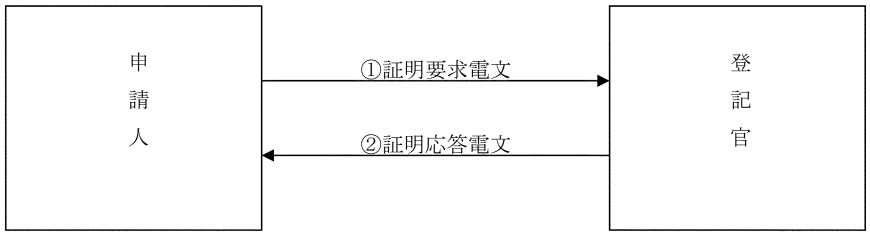
１　通信プロトコル

商業登記規則第33条の15第２項の規定及び同条第３項において準用する第33条の８第１項の規定による送信に用いる通信プロトコルは、HTTP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及び②の各電文の構成については、後記３以下で定める。




①　申請人が登記官に送信する「証明要求電文」は、請求に係る電子証明書に記録された「notAfter」の日時までに、電子認証登記所に到達しなければならない。また、過去の特定の日時（電子証明書の記録された「notBefore」から「notAfter」までの範囲に限る。）についての「証明要求電文」は、請求に係る電子証明書に記録された「notAfter」の日の翌日から起算して７日を超えない日までに、電子認証登記所に到達しなければならない。

②　登記官は、申請人にsha-256WithRSAによる電子署名を講じた「証明応答電文」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）「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