第１　電磁的記録への記録方式

１　使用する電磁的記録媒体

（１）商業登記規則第 33 条の 6 第 4 項第 1 号の光ディスク（以下「申請用光ディスク」という。）のトラックフォーマットは、産業標準化法（昭和 24 年法律第 185 号）に基づく日本産業規格（以下「日本産業規格」という。）X6241 又は X6281 に適合する直径 120 ミリメートルの光ディスクの再生装置で再生することが可能なものによる。ボリューム及びファイル構成は、日本産業規格 X0606 又は X0610 による。

（２）商業登記規則第 33 条の 6 第 4 項第 2 号の不揮発性半導体記憶装置（以下「申請用メモリ」という。）の構造は、ユーエスビーインプリメンターズフォーラムが定めた USB1.0、USB1.1、USB2.0 又は USB3.0 に適合し、かつ、Standard A 端子を備えたものによる。ボリューム及びファイル構成は、File Allocation Table 16、File Allocation Table 32、NT File System 又は Extended File Allocation Table による。

（３）1 個の申請用光ディスク又は申請用メモリには、1 件の申請に係る商業登記規則第 33 条の 6 第 1 項の電磁的記録（以下第２までにおいて「電磁的記録」という。）のみを記録する。

２　ファイル名

ファイル名は、「SHINSEI」とする。

３　ファイルへの記録の方式

（１）ファイルに所要事項（データ）を格納する際には、次の４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１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、国際標準化機構が定めた規格 8824-1:1998、8824-2:1998、8824-3:1998、8824-4:1998 の抽象構文記法 1（以下「ASN.1」という。）及び付録１に定めるところによる。

（２） データの符号化は、国際標準化機構 ISO/IEC 8825-1 ： 2015 の識別符号化規則（以下「DER」という。）による。

（３）フィールド欄の「－」部分は、フィールドが定義されていないことを表す。以下同じ。

４　証明書発行申請ファイル

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)		○
recipient	GeneralName([4])		
－	Name(RDNSequence)		○
body	PKIBody([0])		
－	CertReqMessages		
－	CertReqMsg		
certReq	CertRequest		
certReqId	INTEGER	0	◎
certTemplate	CertTemplate		

subject	[5]		△ （注２）
-	Name(RDNSequence)		
-	RelativeDistinguishedName		△ （注３）
(organizationName)	AttributeTypeAndValue		
type	OBJECT IDENTIFIER	2.5.4.10	↑◎ （注２）
value	DirectoryString (UTF8String)	商業登記規則第33条の6第6項の規定により商号等の表音等をローマ字等で表示したものを記録する場合には、記録する。（注４）	↑◎ （注２）
-	RelativeDistinguishedName		△ （注５）
(commonName)	AttributeTypeAndValue		
type	OBJECT IDENTIFIER	2.5.4.3	↑◎ （注２）
value	DirectoryString (UTF8String)	商業登記規則第33条の6第6項の規定により氏名の表音をローマ字等で表示したものを記録する場合には、記録する。（注４）	↑◎ （注２）
publicKey	[6] SubjectPublicKeyInfo		
algorithm	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.1	◎
parameters	NULL		△
subjectPublicKey	BIT STRING	日本産業規格 X5731-8 附属書 D に定める方式に従って作成した 2,048 ビットの公開かぎを記録する。	◎
extensions	[9] Extensions		
(registeredCorporationInfo)	Extension		
extnId	OBJECT IDENTIFIER	1.2.392.100300.1.1.3	◎
extnValue	OCTET STRING		
-	RegisteredCorporationInfoSyntax		
corporateName	[0]		
-	DirectoryString (UTF8String)	「商号」を記録する。（注６）	◎
corporateAddress	[2]		
-	DirectoryString (UTF8String)	「本店（被証明者が商号使用者又は支配人であるときは、それぞれ営業所又は支配人を置いた営業所）」を記録する。（注６）	◎
representativeDirectorName	[3]		
-	DirectoryString (UTF8String)	「被証明者の氏名」を記録する。 （注６）	◎
representativeDirectorTitle	[4]		
-	DirectoryString (UTF8String)	「被証明者の資格」を記録する。 （注６）	◎
pop	ProofOfPossession ([1] POPOSigningKey)		
algorithmIdentifier	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.11	◎
parameters	NULL		△
signature	BIT STRING	（注７）	◎
regInfo	SEQUENCE OF AttributeTypeAndValue		
(suspensionSecretCode)	AttributeTypeAndValue		

type	OBJECT IDENTIFIER	1.2.392.100300.1.2.105	◎
value	SuspensionSecretCode		
hashAlg	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	2.16.840.1.101.3.4.2.1	◎
parameters	NULL		△
hashedSecretCode	OCTET STRING	（注８）	◎
(timeLimit)	AttributeTypeAndValue		
type	OBJECT IDENTIFIER	1.2.392.100300.1.2.104	◎
value	TimeLimit	商業登記法第12条の2第1項第2号の期間（月数）を記録する。（注９）	◎

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　商業登記規則第 33 条の 6 第 6 項の規定により電磁的記録に商号又は氏名等の表音等をローマ字等で記録する場合には、このフィールドを設定する。

注３　商業登記規則第 33 条の 6 第 6 項の規定により商号の表音等をローマ字等で表示したものを記録する場合には、このフィールドを設定する。

注４　商号等の表音をローマ字等で表記する場合の文字数は 44 文字以内とし、氏名の表音をローマ字等で表記する場合の文字数は 50 文字以内とする。使用する文字等の範囲は、日本産業規格 X0201-1997 のラテン文字用図形文字集合及びスペースとし、文字の符号化表現は、日本産業規格 X0208-1997 附属書 1 に規定する方式による。

注５　商業登記規則第 33 条の 6 第 6 項の規定により氏名の表音をローマ字等で表示したものを記録する場合には、このフィールドを設定する。

注６　「商号」、「本店（被証明者が商号使用者又は支配人であるときは、それぞれ営業所又は支配人を置いた営業所）」及び「被証明者の資格」の文字数は、各 128 文字以内とし、「被証明者の氏名」の文字数は、126 文字以内とする。使用する文字等の範囲は、日本産業規格 X0208-1997 の 2 バイト図形文字集合とし、この範囲外の文字等は、範囲内の類似の文字等又はその表音を片仮名に置き換えて記録する。文字の符号化表現は、日本産業規格 X0208-1997 附属書 1 に規定する方式による。

なお、営業所又は支配人を置いた営業所を記録する場合においては、当該営業所等に係る表示の末尾に、それぞれ「(営業所)」又は「(支配人を置いた営業所)」と続けて記録する。

注７　「certReq」に属する部分を DER により符号化した値に sha-256WithRSAEncryption による電子署名（日本産業規格 X5007 及び X5603 に規定するオブジェクト識別子（以下「オブジェクト識別子」という。）を「1.2.840.113549.1.1.11」とするアルゴリズムに基づき変換する措置をいう（以下「sha-256WithRSA による電子署名」という。）。）を講じた値を記録する。

注８　商業登記規則第 33 条の 6 第 5 項第 4 号に規定する申請人が定める識別符号を SHA-256（オブジェクト識別子を「2.16.840.1.101.3.4.2.1」とするアルゴリズムをいう。以下同じ。）

により変換した値を記録する。同号の規定により申請人が定める識別符号の長さは、8 バイト以上 64 バイト以下とする。使用する文字等の範囲は、日本産業規格 X0201 で規定されたラテン文字用図形文字集合とする。文字等の符号化表現は、日本産業規格 X0208-1997 附属書 1 に規定する方式による。

注９　使用する数字は、日本産業規格 X0201 で規定されたラテン文字用図形文字集合の数字とする。この場合において、1 桁の数字を記録するときは、最初に 0 を記録して 2 桁にしなければならない。文字の符号化表現は、日本産業規格 X0208-1997 附属書 1 に規定する方式による。

第２　電子証明書の方式

１　通則

（１）商業登記規則第 33 条の 8 第 2 項の電子証明書に所要事項（データ）を格納する際には、次の２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２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２に定めるところによる。また、電子認証登記所の登記官（以下「登記官」という。）が商業登記規則第 33 条の 8 第 1 項の規定により電子署名を講ずるのに用いる公開かぎを明らかにするため、次の３に定めるところにより作成する登記官の電子証明書についても同様とする。

（２）データの符号化は、DER による。

２　被証明者の電子証明書

フィールド	データ型	設定値
－	Certificate	
tbsCertificate	TBSCertificate	
version	[0]	
－	Version	2
serialNumber	CertificateSerialNumber	（注１）
signature	AlgorithmIdentifier	
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.11
parameters	NULL	（注２）
issuer	Name(RDNSequence)	
－	RelativeDistinguishedName	
(countryName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.6
value	PrintableString	JP
－	RelativeDistinguishedName	
(organizationName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.10
value	DirectoryString (UTF8String)	Japanese Government
－	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
validity	Validity	
notBefore	Time(UTCTime)	（注３）
notAfter	Time(UTCTime)	（注４）
subject	Name(RDNSequence)	
-	RelativeDistinguishedName	
(countryName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.6
value	PrintableString	JP
-	RelativeDistinguishedName	
(organizationName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.10
value	DirectoryString (UTF8String)	（注５）
-	RelativeDistinguishedName	
(commonName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.3
value	DirectoryString (UTF8String)	（注６）
subjectPublicKeyInfo	SubjectPublicKeyInfo	
algorithm	AlgorithmIdentifier	
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.1
parameters	NULL	（注２）
subjectPublicKey	BIT STRING	（注７）
extensions	[3]	
-	Extensions	
(authorityKeyIdentifier)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.35
extnValue	OCTET STRING	
-	AuthorityKeyIdentifier	
keyIdentifier	[0] KeyIdentifier	（注８）
authorityCertIssuer	[1] GeneralNames	
-	GeneralName([4])	
-	Name(RDNSequence)	
-	RelativeDistinguishedName	
(countryName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.6
value	PrintableString	JP
-	RelativeDistinguishedName	
(organizationName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.10
value	DirectoryString (UTF8String)	Japanese Government
-	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

authorityCertSerialNumber	[2] CertificateSerialNumber	（注９）
(subjectKeyIdentifier)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.14
extnValue	OCTET STRING	
-	SubjectKeyIdentifier	（注１０）
(keyUsage)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.15
critical	BOOLEAN DEFAULT FALSE	TRUE
extnValue	OCTET STRING	
-	keyUsage	1 1 0 0 0 0 0 0 0 (digitalSignature、nonRepudiation)
(certificatePolicies)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.32
extnValue	OCTET STRING	
-	CertificatePoliciesSyntax	
-	PolicyInformation	
policyIdentifier	CertPolicyId	1.2.392.100300.1.3.3（注１１）
policyQualifiers	SEQUENCE OF PolicyQualifierInfo	
-	PolicyQualifierInfo	
policyQualifierId	OBJECT IDENTIFIER	1.3.6.1.5.5.7.2.2
qualifier	UserNotice	
noticeRef	NoticeReference	
organization	DisplayText(VisibleString)	Ministry of Justice
noticeNumbers	SEQUENCE OF INTEGER	
-	INTEGER	1
explicitText	DisplayText(VisibleString)	（注１２）
(authorityInfoAccess)	Extension	
extnId	OBJECT IDENTIFIER	1.3.6.1.5.5.7.1.1
extnValue	OCTET STRING	
-	AuthorityInfoAccessSyntax	
-	AccessDescription	
accessMethod	OBJECT IDENTIFIER	1.3.6.1.5.5.7.48.1
accessLocation	GeneralName([6] IA5String)	http://crca.moj.go.jp/bin/dcwcgi/DC_HUSR/cert/cert
(jCertificatePolicies)	Extension	
extnId	OBJECT IDENTIFIER	1.2.392.100300.1.1.1
extnValue	OCTET STRING	
-	JCertificatePoliciesSyntax	
-	PolicyInformation	
policyIdentifier	CertPolicyId	1.2.392.100300.1.3.4（注１１）
policyQualifiers	SEQUENCE OF PolicyQualifierInfo	
-	PolicyQualifierInfo	
policyQualifierId	OBJECT IDENTIFIER	1.3.6.1.5.5.7.2.2
qualifier	UserNotice	
noticeRef	NoticeReference	
organization	DisplayText(UTF8String)	法務省
noticeNumbers	SEQUENCE OF INTEGER	
-	INTEGER	1
explicitText	DisplayText(UTF8String)	（注１３）
(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
(registeredCorporationInfo)	Extension	
extnId	OBJECT IDENTIFIER	1.2.392.100300.1.1.3

extnValue	OCTET STRING	
-	RegisteredCorporationInfoSyntax	
corporateName	[0]	
-	DirectoryString(UTF8String)	（注１４）
registeredNumber	[1]	
-	PrintableString	（注１５）
corporateAddress	[2]	
-	DirectoryString(UTF8String)	（注１６）
representativeDirectorName	[3]	
-	DirectoryString(UTF8String)	（注１７）
representativeDirectorTitle	[4]	
-	DirectoryString(UTF8String)	（注１８）
registryOffice	[6]	
-	DirectoryString(UTF8String)	（注１９）
(cRLDistributionPoints)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.31
extnValue	OCTET STRING	
DistributionPoint	[0] DistributionPointName	
fullName	[0] GeneralNames	
DirectoryName	[4] Name	
-	RelativeDistinguishedName	
(countryName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.6
value	PrintableString	JP
-	RelativeDistinguishedName	
(organizationName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.10
value	DirectoryString(UTF8String)	Japanese Government
-	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
DistributionPoint	[0] DistributionPointName	
fullName	[0] GeneralNames	
uniformResourceIdentifier	GeneralName([6] IA5String)	http://crca1.moj.go.jp/certificateRevocationList.crl
algorithm	AlgorithmIdentifier	
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.11
parameters	NULL	（注２）
signature	BIT STRING	（注２０）

注１　商業登記規則第 33 条の 8 第 2 項第 2 号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　商業登記規則第 33 条の 8 第 2 項第 3 号の電子証明書の作成日時をグリニッジ標準時により記録する。

注４　電子証明書を作成した日の翌日から起算して、商業登記法第 12 条の 2 第 1 項第 2 号の期間の満了する日の日本時間 23 時 59 分 59 秒をグリニッジ標準時により記録する。

注５　「MOJ No.「会社法人等番号」-「商号等の表音をローマ字等で表示したもの」」の形式で記録する。なお、「-「商号等の表音をローマ字等で表示したもの」」は、電磁的記録に記録がある場合に限り、これを記録する。

注６「「役員番号」-「氏名の表音をローマ字等で表示したもの」」の形式で記録する。
なお、「-「氏名の表音をローマ字等で表示したもの」」は、電磁的記録に記録がある場合に限り、これを記録する。

注７　電磁的記録の「subjectPublicKey」に記録された事項を記録する。日本産業規格 X5731-8 附属書 D に定める方式に従って作成した 2,048 ビットの公開かぎが記録される。

注８　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９　登記官の電子証明書の番号を記録する。

注１０　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１１　法務省ホームページに掲示される電子証明書に関する注意事項等を識別するオブジェクト識別子を記録する。

注１２　電子証明書を利用する際の注意事項を英字により記録する。

注１３　電子証明書を利用する際の注意事項を記録する。

注１４　電磁的記録の「corporateName」に記録された事項を記録する。

注１５　会社法人等番号を記録する。

注１６　電磁的記録の「corporateAddress」に記録された事項を記録する。

注１７　電磁的記録の「representativeDirectorName」に記録された事項を記録する。

注１８　電磁的記録の「representativeDirectorTitle」に記録された事項を記録する。

注１９　商業登記規則第 33 条の 8 第 2 項第 4 号の登記所を記録する。

注２０　「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。

3　登記官の電子証明書

フィールド	データ型	設定値
-	Certificate	
tbsCertificate	TBSCertificate	
Version	[0]	
-	Version	2
serialNumber	CertificateSerialNumber	（注１）
Signature	AlgorithmIdentifier	
Algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.11
Parameters	NULL	（注２）
Issuer	Name(RDNSequence)	
-	RelativeDistinguishedName	
(countryName)	AttributeTypeAndValue	
Type	OBJECT IDENTIFIER	2.5.4.6
Value	PrintableString	JP
-	RelativeDistinguishedName	
(organizationName)	AttributeTypeAndValue	

Type	OBJECT IDENTIFIER	2.5.4.10
Value	DirectoryString (UTF8String)	Japanese Government
-	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
Validity	Validity	
notBefore	Time(UTCTime)	（注３）
notAfter	Time(UTCTime)	（注４）
Subject	Name(RDNSequence)	
-	RelativeDistinguishedName	
(countryName)	AttributeTypeAndValue	
Type	OBJECT IDENTIFIER	2.5.4.6
Value	PrintableString	JP
-	RelativeDistinguishedName	
(organizationName)	AttributeTypeAndValue	
Type	OBJECT IDENTIFIER	2.5.4.10
Value	DirectoryString (UTF8String)	Japanese Government
-	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
subjectPublicKeyInfo	SubjectPublicKeyInfo	
Algorithm	AlgorithmIdentifier	
Algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.1
Parameters	NULL	（注２）
subjectPublicKey	BIT STRING	（注５）
Extensions	[3]	
-	Extensions	
(subjectKeyIdentifier)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.14
extnValue	OCTET STRING	
-	SubjectKeyIdentifier	（注６）
(keyUsage)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.15
critical	BOOLEAN DEFAULT FALSE	TRUE
extnValue	OCTET STRING	
-	KeyUsage	1 0 1 1 0 1 1 0 0 (digitalSignature、keyEncipherment、dataEncipherment、keyCertSign、cRLSign)
(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
(cRLDistributionPoints)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.31
extnValue	OCTET STRING	
DistributionPoint	[0] DistributionPointName	
fullName	[0] GeneralNames	
DirectoryName	[4] Name	
-	RelativeDistinguishedName	
(countryName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.6
value	PrintableString	JP
-	RelativeDistinguishedName	
(organizationName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.10
value	DirectoryString(UTF8String)	Japanese Government
-	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
DistributionPoint	[0] DistributionPointName	
fullName	[0] GeneralNames	
uniformResourceIdentifier	GeneralName([6] IA5String)	http://crca1.moj.go.jp/authorityRevocationList.crl
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、120 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、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

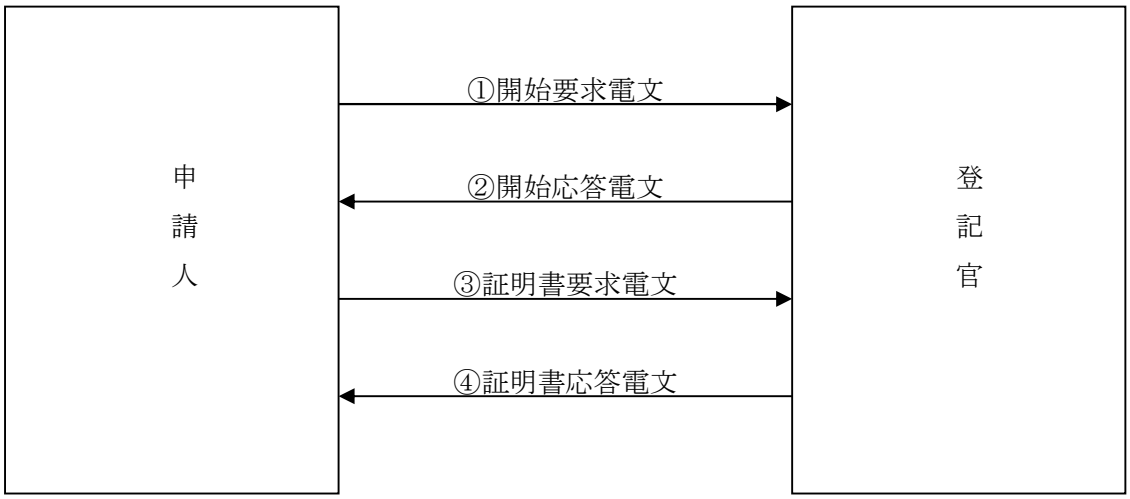
１　通信プロトコル

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。

（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]		
－	OCTET STRING	（注４）	◎
senderNonce	[5]		

-	OCTET STRING	（注５）	◎
recipNonce	[6]		
-	OCTET STRING	（注６）	◎
body	PKIBody([22])		
-	GenRepContent		
-	InfoTypeAndValue		
infoType	OBJECT IDENTIFIER	1.2.392.100300.1.2.22	◎
infoValue	GenpInfoResContent		
status	PKIStatusInfo		
status	PKIStatus	0（注７）	◎
negotiationKeys	SEQUENCE OF NegotiationKey		
-	NegotiationKey		
symmAlg	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.3.7	◎
parameters	NULL	（注２）	○
pubAlg	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.1	◎
parameters	NULL	（注２）	○
hashAlg	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	2.16.840.1.101.3.4.2.1	◎
parameters	NULL	（注２）	○
protection	[0]		
-	PKIProtection	（注８）	◎
extraCerts	[1]		
-	SEQUENCE OF Certificate	（注９）	◎

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。

注２　長さオクテットに「0」を記録する。

注３　注９に記録され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４　「開始要求電文」中の「transactionID」に記録された値を記録する。

注５　1 バイト以上 32 バイト以下の乱数を記録する。

注６　「開始要求電文」中の「senderNonce」に記録された値を記録する。

注７　「開始要求電文」を正常に受信したことを示すため、「0」を記録する。「開始要求電文」に異常があった場合には、後記５による。

注８　付録３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９　登記官の最新の電子証明書を記録する。

（４）「証明書要求電文」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	「開始応答電文」中の「transactionID」を記録する。	◎
senderNonce	[5]		
−	OCTET STRING	「開始応答電文」中の「recipNonce」を記録する。	◎
recipNonce	[6]		
−	OCTET STRING	「開始応答電文」中の「senderNonce」を記録する。	◎
body	PKIBody([0])		
−	CertReqMessages		
−	CertReqMsg		
certReq	CertRequest		
certReqId	INTEGER	0	◎
certTemplate	CertTemplate		
serialNumber	[1] INTEGER	商業登記規則第３３条の８第２項第２号の電子証明書の番号を記録する。	◎
publicKey	[6] SubjectPublicKeyInfo		
algorithm	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.1	◎
parameters	NULL	（注２）	○
subjectPublicKey	BIT STRING	請求に係る公開かぎを記録する。	◎
pop	ProofOfPossession ([1]POPOSigningKey)		
algorithmIdentifier	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.11	◎
parameters	NULL		△
signature	BIT STRING	（注３）	◎

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。

注３　「certReq」に属する部分を 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。ただし、「subjectPublicKey」に記録した公開かぎにより当該電子署名を講じた措置が検証できるものでなければならない。

（５）「証明書応答電文」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]		
−	OCTET STRING	（注４）	◎

senderNonce	[5]	
-	OCTET STRING	（注５）	◎
recipNonce	[6]	
-	OCTET STRING	（注６）	◎
body	PKIBody([1])	
-	CertRepMessage	
response	SEQUENCE OF CertResponse	
-	CertResponse	
certReqId	INTEGER	0	◎
status	PKIStatusInfo	
status	PKIStatus	0（注７）	◎
certifiedKeyPair	CertifiedKeyPair	
certOrEncCert	CertOrEncCert([1])	
-	EncryptedValue	
symmAlg	[1] AlgorithmIdentifier	
algorithm	OBJECT IDENTIFIER	1.2.840.113549.3.7	◎
parameters	CBCParameter	IV	◎
encSymmKey	[2] BIT STRING	（注８）	◎
keyAlg	[3] AlgorithmIdentifier	
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.1	◎
parameters	NULL	（注２）	○
encValue	BIT STRING	（注９）	◎
protection	[0]	
-	PKIProtection	（注１０）	◎
extraCerts	[1]	
-	SEQUENCE OF Certificate	（注１１）	◎

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。

注２　長さオクテットに「0」を記録する。

注３　登記官の最新の電子証明書の「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４　「証明書要求電文」中の「transactionID」に記録された値を記録する。

注５　「証明書要求電文」中の「recipNonce」に記録された値を記録する。

注６　「証明書要求電文」中の「senderNonce」に記録された値を記録する。

注７　「証明書要求電文」を正常に受信したことを示すため、「0」を記録する。「証明書要求電文」に異常があった場合には、後記５による。

注８　電子証明書の暗号化（オブジェクト識別子を「1.2.840.113549.3.7」とする共通かぎ暗号方式によるものに限る。）に用いる共通かぎの値を「証明要求電文」の「subjectPublicKey」に記録された公開かぎを用いて、オブジェクト識別子を「1.2.840.113549.1.1.1」とする暗号アルゴリズムにより暗号化した値を記録する。

注９　電子証明書を注８の共通かぎを用いて暗号化した値を記録する。

注１０　付録３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１１　電子証明書に署名をした登記官の電子証明書を記録する。この場合において、その登記官の電子証明書が最新のものでないときは、最新の電子証明書も併せて記録する。

5　異常時の処理

（１）「開始要求電文」中の「entity-body」の内容が前記４の（２）に定める形式に適合しない場合（後記（２）の場合を除く。）には、登記官は、「開始応答電文」の項番２については、「Content-Type:application/pkixcmp」に代えて「Content-Type:text/html」と記録し、「entity-body」については、前記４の（３）の内容に代えて、次の内容を記録したものを送信する。この場合には、申請人は、「証明書要求電文」を送信することができない。

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 //EN">
<HTML lang=”ja”>
<META HTTP-EQUIV=”Content-Type” CONTENT=”text/html; charset=SHIFT_JIS”>
<TITLE> メッセージ異常 </TITLE>
<BODY>
メッセージ内容に問題があるため、処理できませんでした。
</BODY>
</HTML>
```

（２）「開始要求電文」中の「entity-body」に記録された「symmAlg」、「pubAlg」又は「hashAlg」が、前記４の（２）に定める形式に適合しない場合には、登記官は、「開始応答電文」の「entity-body」に、前記４の（３）の内容に代えて、前記４の（１）に定める方式により、次の内容を記録したものを送信する。この場合には、申請人は、「証明書要求電文」を送信することができない。

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]		
－	OCTET STRING	（注４）	◎
senderNonce	[5]		
－	OCTET STRING	（注５）	◎
recipNonce	[6]		
－	OCTET STRING	（注６）	◎
Body	PKIBody([22])		
－	GenRepContent		
－	InfoTypeAndValue		
infoType	OBJECT IDENTIFIER	1.2.392.100300.1.2.22	◎
infoValue	GenpInfoResContent		
Status	PKIStatusInfo		
Status	PKIStatus	2（注７）	◎
Protection	[0]		
－	PKIProtection	（注８）	◎
extraCerts	[1]		
－	SEQUENCE OF Certificate	（注９）	◎

注１から注６まで、注８及び注９については、前記４の（３）の注１から注６まで、注８及び注９に同じ。

注７　「開始要求電文」に異常があったことを示すため、「2」を記録する。

（３）「証明書要求電文」中の「entity-body」が、前記４の（４）に定める形式に適合しない場合（後記５の（４）の場合を除く。）には、登記官は、「証明書応答電文」の「entity-body」に、前記４の（５）の内容に代えて、前記４の（１）に定める方式により、次の内容を記録したものを送信する。この場合には、申請人は、「開始要求電文」を再送信しなければならない。

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]		
－	OCTET STRING	（注４）	◎
senderNonce	[5]		
－	OCTET STRING	（注５）	◎
recipNonce	[6]		
－	OCTET STRING	（注６）	◎
Body	PKIBody([23])		
－	ErrorMsgContent		
pKIStatusInfo	PKIStatusInfo		
Status	PKIStatus	2（注７）	◎
Protection	[0]		
－	PKIProtection	（注８）	◎
extraCerts	[1]		
－	SEQUENCE OF Certificate	（注９）	◎

注１から注６までについては、前記４の（５）の注１から注６までに同じ。

注７　「証明書要求電文」に異常があったことを示すため、「2」を記録する。

注８　付録３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９　登記官の最新の電子証明書を記録する。

（４）「証明書要求電文」中の「entity-body」に記録された「transactionID」、「senderNonce」、「recipNonce」、「serialNumber」又は「subjectPublicKey」が、前記４の（４）に定める形式に適合しないときは、登記官は、「証明書応答電文」の「entity-body」に、前記４の（５）の内容に代えて、前記４の（１）に定める方式により、次の内容を記録したものを送信する。この場合には、申請人は、「開始要求電文」を再送信しなければならない。

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]		
－	OCTET STRING	（注４）	◎
senderNonce	[5]		
－	OCTET STRING	（注５）	◎
recipNonce	[6]		
－	OCTET STRING	（注６）	◎
Body	PKIBody([1])		
－	CertRepMessage		
response	SEQUENCE OF CertResponse		
－	CertResponse		
certReqId	INTEGER	0	◎
status	PKIStatusInfo		
status	PKIStatus	2（注７）	◎
protection	[0]		
－	PKIProtection	（注８）	◎
extraCerts	[1]		
－	SEQUENCE OF Certificate	（注９）	◎

注１から注９までについては、前記（３）の注１から注９までと同じ。

第４　識別符号の変更の届出に使用する電磁的記録への記録の方式

１　使用する電磁的記録媒体及びファイル名

使用する電磁的記録媒体、ファイル名及びファイルへの記録方式については、前記第１の１から３までに定めるところによる。

２　識別符号の変更届出ファイル

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)		○
recipient	GeneralName([4])		
－	Name(RDNSequence)		○
Body	PKIBody([0])		
－	CertReqMessages		
－	CertReqMsg		
certReq	CertRequest		○

regInfo	SEQUENCE OF AttributeTypeAndValue		
(suspensionSecretCode)	AttributeTypeAndValue		
type	OBJECT IDENTIFIER	1.2.392.100300.1.2.105	◎
value	SuspensionSecretCode		
hashAlg	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	2.16.840.1.101.3.4.2.1	◎
parameters	NULL		△
hashedSecretCode	OCTET STRING	（注２）	◎

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　変更後の識別符号を SHA-256 により変換した値を記録する。識別符号の長さは、8 バイト以上 64 バイト以下とする。使用する文字等の範囲は、日本産業規格 X0201 で規定されたラテン文字用図形文字集合とする。文字等の符号化表現は、日本産業規格 X0208-1997 附属書 1 に規定する方式による。

第５　休止届の送信の方式

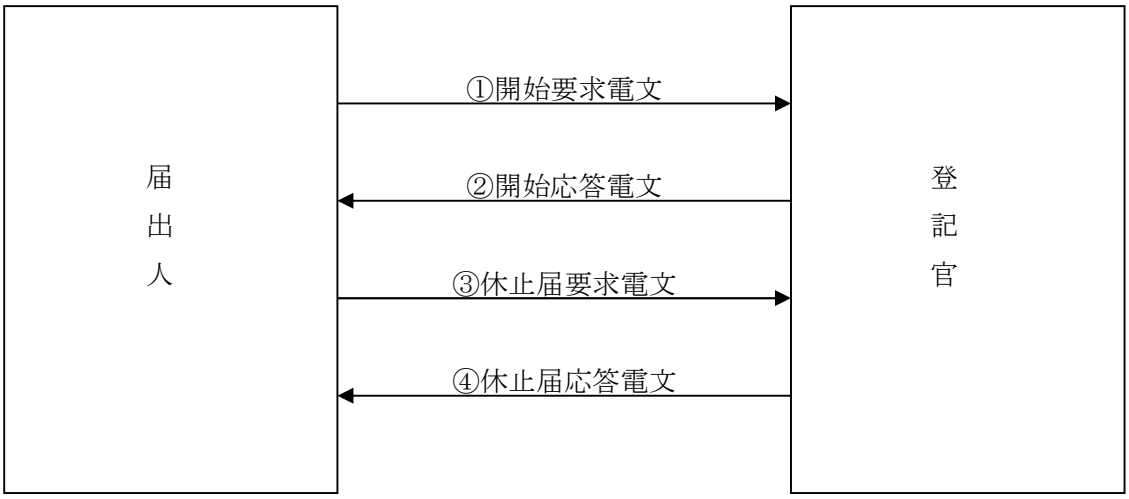
１　通信プロトコル

商業登記規則第 33 条の 13 第 2 項の規定による送信については、登記官が使用する電子計算機と届出人が使用する電子計算機とを接続する電気通信回線を通じて行うものとし、その通信プロトコルは、HTTP とする。

２　電文の送受信の基本形式

登記官と届出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については、後記３以下で定める。



①　届出人は、登記官に「開始要求電文」を送信する。

②　登記官は、届出人に 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　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]		

-	OCTET STRING	（注４）	◎
senderNonce	[5]		
-	OCTET STRING	（注５）	◎
recipNonce	[6]		
-	OCTET STRING	（注６）	◎
Body	PKIBody([22])		
-	GenRepContent		
-	InfoTypeAndValue		
infoType	OBJECT IDENTIFIER	1.2.392.100300.1.2.22	◎
infoValue	GenpInfoResContent		
status	PKIStatusInfo		
status	PKIStatus	0（注７）	◎
negotiationKeys	SEQUENCE OF NegotiationKey		
-	NegotiationKey		
symmAlg	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.3.7	◎
parameters	NULL	（注２）	○
pubAlg	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.1	◎
parameters	NULL	（注２）	○
hashAlg	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	2.16.840.1.101.3.4.2.1	◎
parameters	NULL	（注２）	○
protection	[0]		
-	PKIProtection	（注８）	◎
extraCerts	[1]		
-	SEQUENCE OF Certificate	（注９）	◎

注１から注６までについては、前記第３の４の（３）の注１から注６までに同じ。

注７　「開始要求電文」を正常に受信したことを示すため、「0」を記録する。「開始要求電文」に異常があった場合には、後記５による。

注８　付録４に示す「ProtectedPart」を DER により符号化した sha-256WithRSA による電子署名を講じた値を記録する。

注９　登記官の最新の電子証明書を記録する。

（４）「休止届要求電文」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	「開始応答電文」中の「transactionID」を記録する。	◎
senderNonce	[5]		
-	OCTET STRING	「開始応答電文」中の「recipNonce」を記録する。	◎
recipNonce	[6]		
-	OCTET STRING	「開始応答電文」中の「senderNonce」を記録する。	◎
Body	PKIBody([21])		

−	GenMsgContent		
−	InfoTypeAndValue		
infoType	OBJECT IDENTIFIER	1.2.392.100300.1.2.1	◎
infoValue	GenmSuspReqContent		
certDetails	CertTemplate		
serialNumber	[1] INTEGER	電子証明書の番号を記録する。	◎
issuer	[3]		
−	Name(RDNSequence)		
−	RelativeDistinguishedName		
(countryName)	AttributeTypeAndValue		
type	OBJECT IDENTIFIER	2.5.4.6	◎
value	PrintableString	JP	◎
−	RelativeDistinguishedName		
(organizationName)	AttributeTypeAndValue		
type	OBJECT IDENTIFIER	2.5.4.10	◎
value	DirectoryString (UTF8String)	Japanese Government	◎
−	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	◎
revocationReason	ReasonFlags	6	◎
suspensionReasonCode	INTEGER	1	◎
suspensionDetail	EncryptedValue		
keyAlg	[3] AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.1	◎
parameters	NULL		△
encValue	BIT STRING	（注３）	◎

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。

注３　商業登記規則第 33 条の 6 第 5 項第 4 号の識別符号の次に、DER により符号化した「header」部を SHA-1 により変換した値を付加したものを、登記官の公開かぎを用いて、オブジェクト識別子を「1.2.840.113549.1.1.1」とする暗号アルゴリズムにより暗号化した値を記録する。登記官の公開かぎは、「開始応答電文」の注９に記録されたものを使用しなければならない。

（５）「休止届応答電文」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]		
-	OCTET STRING	（注４）	◎
senderNonce	[5]		
-	OCTET STRING	（注５）	◎
recipNonce	[6]		
-	OCTET STRING	（注６）	◎
body	PKIBody([22])		
-	GenRepContent		
-	InfoTypeAndValue		
infoType	OBJECT IDENTIFIER	1.2.392.100300.1.2.2	◎
infoValue	GenpSuspResContent		
status	PKIStatusInfo		
status	PKIStatus	0（注７）	◎
revCert	CertId		
issuer	GeneralName([4])		
-	Name(RDNSequence)		
-	RelativeDistinguishedName		
(countryName)	AttributeTypeAndValue		
type	OBJECT IDENTIFIER	2.5.4.6	◎
value	PrintableString	JP	◎
-	RelativeDistinguishedName		
(organizationName)	AttributeTypeAndValue		
type	OBJECT IDENTIFIER	2.5.4.10	◎
value	DirectoryString (UTF8String)	Japanese Government	◎
-	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　「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。

注２　長さオクテットに「0」を記録する。

注３　注１０に記録され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４　「休止届要求電文」中の「transactionID」に記録された値を記録する。

注５　「休止届要求電文」中の「recipNonce」に記録された値を記録する。

注６　「休止届要求電文」中の「senderNonce」に記録された値を記録する。

注７　「休止届要求電文」を正常に受信したことを示すため、「0」を記録する。「休止届要求電文」に異常があった場合には、後記５による。

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。

５　異常時の処理

（１）「開始要求電文」中の「entity-body」が前記４の（２）に定める形式に適合しない場合（後記５の（２）に定める場合を除く。）における登記官の措置については、前記第３の５の（１）による。この場合には、届出人は、「休止届要求電文」を送信することができない。

（２）「開始要求電文」中の「entity-body」に記録された「symmAlg」、「pubAlg」又は「hashAlg」が前記４の（２）に定める形式に適合しない場合は、登記官は、「開始応答電文」の「entity-body」に、前記４の（３）の内容に代えて、前記４の（１）の定める方式により、次の内容を記録したものを送信する。この場合には、届出人は、「休止届要求電文」を送信することができない。

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]		
－	OCTET STRING	（注４）	◎
senderNonce	[5]		
－	OCTET STRING	（注５）	◎

recipNonce	[6]		
-	OCTET STRING	（注６）	◎
Body	PKIBody([22])		
-	GenRepContent		
-	InfoTypeAndValue		
infoType	OBJECT IDENTIFIER	1.2.392.100300.1.2.22	◎
infoValue	GenpInfoResContent		
status	PKIStatusInfo		
status	PKIStatus	2（注７）	◎
protection	[0]		
-	PKIProtection	（注８）	◎
extraCerts	[1]		
-	SEQUENCE OF Certificate	（注９）	◎

注１から注６までについては、前記第３の４の（３）の注１から注６までに同じ。

注７　「開始要求電文」に異常があったことを示すため、「2」を記録する。

注８　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９　登記官の最新の電子証明書を記録する。

（３）「休止届要求電文」中の「entity-body」が、前記４の（４）に定める形式に適合しない場合（後記（４）の場合を除く。）には、登記官は、「休止届応答電文」の「entity-body」に、前記４の（５）の内容に代えて、前記４の（１）に定める方式により、次の内容を記録したものを送信する。この場合には、届出人は、「開始要求電文」を再送信しなければならない。

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]		
-	OCTET STRING	（注４）	◎
senderNonce	[5]		
-	OCTET STRING	（注５）	◎
recipNonce	[6]		
-	OCTET STRING	（注６）	◎
Body	PKIBody([23])		
-	ErrorMsgContent		
pKIStatusInfo	PKIStatusInfo		
status	PKIStatus	2 （注７）	◎
protection	[0]		
-	PKIProtection	（注８）	◎
extraCerts	[1]		
-	SEQUENCE OF Certificate	（注９）	◎

注１から注６までについては、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　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９　登記官の最新の電子証明書を記録する。

（４）「休止届要求電文」中の「entity-body」に記録された「transactionID」、「senderNonce」、「recipNonce」、「serialNumber」、「issuer」、「suspensionReasonCode」又は「encValue」が、前記４の（４）に定める形式に適合しないときは、登記官は、「休止届応答電文」の「entity-body」に、前記４の（５）の内容に代えて、前記４の（１）に定める方式により、次の内容を記録したものを送信する。この場合には、届出人は、「開始要求電文」を再送信しなければならない。

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]		
－	OCTET STRING	（注４）	◎
senderNonce	[5]		
－	OCTET STRING	（注５）	◎
recipNonce	[6]		
－	OCTET STRING	（注６）	◎
Body	PKIBody([22])		
－	GenRepContent		
－	InfoTypeAndValue		
infoType	OBJECT IDENTIFIER	1.2.392.100300.1.2.2	◎
infoValue	GenpSuspResContent		
status	PKIStatusInfo		
status	PKIStatus	2（注７）	◎
revCert	CertId		
issuer	GeneralName([4])		
－	Name(RDNSequence)		
－	RelativeDistinguishedName		
(countryName)	AttributeTypeAndValue		
type	OBJECT IDENTIFIER	2.5.4.6	◎
value	PrintableString	JP	◎
－	RelativeDistinguishedName		
(organizationName)	AttributeTypeAndValue		
type	OBJECT IDENTIFIER	2.5.4.10	◎
value	DirectoryString (UTF8String)	Japanese Government	◎

-	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

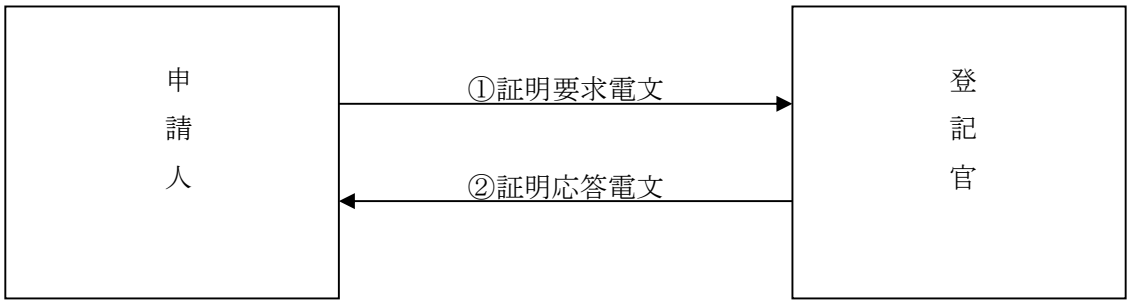
１　通信プロトコル

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

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

（3）「証明応答電文」中の「entity-body」の内容

フィールド	データ型	設定値	必須（注１）
-	OCSPResponse		
responseStatus	OCSPResponseStatus	0（注２）	◎
responseBytes	[0]		
-	ResponseBytes		
responseType	OBJECT IDENTIFIER	1.3.6.1.5.5.7.48.1.1	◎
response	OCTET STRING		
-	BasicOCSPResponse		
tbsResponseData	ResponseData		
responderID	ResponderID([2])		
-	KeyHash	（注３）	◎
producedAt	GeneralizedTime	（注４）	◎
responses	SEQUENCE OF SingleResponse		
-	SingleResponse		
certID	CertID		
hashAlgorithm	AlgorithmIdentifier		
algorithm	OBJECT IDENTIFIER	1.3.14.3.2.26	◎
parameters	NULL	（注５）	○
issuerNameHash	OCTET STRING	（注６）	◎
issuerKeyHash	OCTET STRING	（注７）	◎
serialNumber	CertificateSerialNumber	（注８）	◎
certStatus	CertStatus(CHOICE)		
good	[0] NULL	（注９）	△○（注９）
revoked	[1] RevokedInfo	（注９）	△○（注９）
revocationTime	GeneralizedTime	（注１０）	↑◎
revocationReason	[0] CRLReason	（注１１）	↑◎
unknown	[2] UnknownInfo	（注９）	△○（注９）
thisUpdate	GeneralizedTime	（注１２）	◎
singleExtensions	[1]		
-	Extensions		
(ocspStatusCode)	Extension		
extnId	OBJECT IDENTIFIER	1.2.392.100300.1.2.103	◎
extnValue	OCTET STRING		
-	OcspStatusCode	（注１１）	◎
(confirmationTime)	Extension		△（注１３）
extnId	OBJECT IDENTIFIER	1.2.392.100300.1.2.102	↑◎
extnValue	OCTET STRING		
-	ConfirmationTime	（注１４）	↑◎
responseExtensions	[1]		
-	Extensions		
(nonce)	Extension		
extnId	OBJECT IDENTIFIER	1.3.6.1.5.5.7.48.1.2	◎
extnValue	OCTET STRING		
-	Nonce	（注１５）	◎
signatureAlgorithm	AlgorithmIdentifier		

	algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.11	◎
	parameters	NULL	（注５）	○
signature		BIT STRING	（注１６）	◎
certs		[0]		
	-	SEQUENCE OF Certificate	（注１７）	◎

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。「必須」欄中に△○印のあるフィールドには、注９に定めるところにより、いずれか１のフィールドを必ず設定しなければならない。

注２　「証明要求電文」を正常に受信したことを示すため、「0」を記録する。「証明要求電文」に異常があった場合には、後記５による。

注３　注１６に定める電子署名を行っ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４　この電文を作成した日時をグリニッジ標準時により記録する。

注５　長さオクテットに「0」を記録する。

注６　「証明要求電文」中の「issuerNameHash」に記録された値を記録する。

注７　「証明要求電文」中の「issuerKeyHash」に記録された値を記録する。

注８　「証明要求電文」中の「serialNumber」に記録された値を記録する。

注９　次の表に掲げる事項に該当する場合に、設定内容に定めるフィールドを設定する。

項番	事項	設定内容
1	電子証明書について項番２又は３のいずれの事項にも該当しないこと	「good」
2	注１１の表中、項番１から７までのいずれかの事項に該当すること	「revoked」
3	「証明要求電文」中「issuerNameHash」、「issuerKeyHash」若しくは「serialNumber」に誤りがあり、又は電子証明書に記録された「notAfter」の日時までに「証明要求電文」が電子認証登記所に到達しなかったこと	「unknown」

注１０　注１１の表中項番１から７までのいずれかの事項が記録される場合に、当該事項が生じた日時をグリニッジ標準時により記録する。

注１１　次の表に掲げる「事項」に該当する場合に、「記録内容」に定める数字を記録する。この場合において、項番１から４までの複数の事項に該当するときは、最初に生じた事項についてのみ記録する。項番５から７までのいずれかの事項が生じた時以後に、項番１から４までのいずれかの事項が生じたときは、項番１から４までの事項のうち、最初に生じた事項についてのみ記録する。

項番	事項	記録内容	
		CRL Reason	OcspStatus Code
1	商業登記法第 12 条の 2 第 7 項の届出があったとき	5	1
2	商業登記規則第 33 条の 12 第 1 項第 2 号の規定により電子証明書に記録された登記事項に変更を生ずる登記をした旨の通知があったとき	3	2
3	商業登記規則第 33 条の 16 第 1 項の規定により、登記所の事故により証明をするのが相当でなくなったと認めるとき	2	4
4	商業登記規則第 33 条の 16 第 1 項の規定により、登記所の事故以外の事由により証明をするのが相当でなくなったと認めるとき	5	2
5	商業登記規則第 33 条の 12 第 1 項第 1 号の通知があったとき（同項第 3 号の通知があったときを除く。）	6	2
6	商業登記規則第 33 条の 13 第 1 項の規定により電子証明書の使用の休止の届出があったとき（同条第 5 項の届出があったときを除く。）	6	1
7	項番 5 及び 6 のいずれにも該当するとき	6	3
8	注９により、「good」のフィールドを設定したとき		0
9	注９により、「unknown」のフィールドを設定したとき		0

注１２　登記官が証明の対象を確認した日時をグリニッジ標準時により記録する。

注１３　「証明要求電文」に「ConfirmationTime」が記録されていたときは、これらのフィールドを設ける。

注１４　「証明要求電文」に「ConfirmationTime」が記録されていたときは、フィールドに値を記録する。

注１５　「証明要求電文」の「Nonce」に記録された値を記録する。

注１６　「ResponseData」を DER で符号化した値に sha-256WithRSA による電子署名を講じた値を記録する。

注１７　登記官の最新の電子証明書を記録する。

5　異常時の処理

「証明要求電文」中の「entity-body」の内容が前記４の（２）に定める形式に適合しない場合（前記４の（３）の注９により「unknown」のフィールドを設定する場合を除く。）は、登記官は、「証明応答電文」の「entity-body」に、前記４の（３）の内容に代えて、前記４の（１）の定める方式により、次の内容を記録したものを送信する。

フィールド	データ型	設定値	必須（注１）
-	OCSPResponse		
responseStatus	OCSPResponseStatus	1（注２）	◎

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。

注２　「証明要求電文」に異常があったことを示すため、「1」を記録する。

第７　失効リストの公開

１　通則

失効リスト（Certificate Revocation List 及び Authority Revocation List）は、証明書内の失効リスト配布ポイント（CRL Distribution Points）が示すロケーションで公開される。失効リスト（Certificate Revocation List 及び Authority Revocation List）に所要事項（データ）を格納する際には、次の３及び４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６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６に定めるところによる。データの符号化は、DER による。

２　通信プロトコル

失効リスト配布ポイントが示すロケーションへの通信プロトコルは、HTTP 又は IETF が RFC:4511 において定めた Light-weight Directory Access Protocol Version 3 とする。

３　失効リスト（Certificate Revocation List）

フィールド	データ型	設定値
－	CertificateList	
tbsCertList	TBSCertList	
version	Version	1
signature	AlgorithmIdentifier	
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.11
parameters	NULL	（注１）
issuer	Name(RDNSequence)	
－	RelativeDistinguishedName	
(countryName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.6
value	PrintableString	JP
－	RelativeDistinguishedName	
(organizationName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.10
value	DirectoryString (UTF8String)	Japanese Government
－	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
thisUpdate	Time(UTCTime)	（注２）
nextUpdate	Time(UTCTime)	（注３）
revokedCertificates	SEQUENCE OF SEQUENCE	
userCertificate	CertificateSerialNumber	（注４）
revocationDate	Time(UTCTime)	（注５）
crlEntryExtensions	EntryExtensions	
reasonCode	EntryExtension	
extnId	OBJECT IDENTIFIER	2.5.29.21
extnValue	OCTET STRING	
CRLReason	ENUMERATED	（注６）

crlExtensions	[0]	
-	CRLExtensions	
authorityKeyIdentifier	CRLExtension	
extnId	OBJECT IDENTIFIER	2.5.29.35
extnValue	OCTET STRING	
-	AuthorityKeyIdentifier	
keyIdentifier	[0] KeyIdentifier	（注７）
authorityCertIssuer	[1] GeneralNames	
-	GeneralName([4])	
-	Name(RDNSequence)	
-	RelativeDistinguishedName	
(countryName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.6
value	PrintableString	JP
-	RelativeDistinguishedName	
(organizationName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.10
value	DirectoryString (UTF8String)	Japanese Government
-	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
authorityCertSerialNumber	[2] CertificateSerialNumber	（注８）
cRLNumber	CRLExtension	
extnId	OBJECT IDENTIFIER	2.5.29.20
extnValue	OCTET STRING	
CRLNumber	INTEGER	（注９）
IssuingDistributionPoint	CRLExtension	
extnId	OBJECT IDENTIFIER	2.5.29.28
critical	BOOLEAN DEFAULT FALSE	TRUE
extnValue	OCTET STRING	
distributionPoint	[0] DistributionPointName	
fullName	[0] GeneralNames	
DirectoryName	[4] Name	
-	RelativeDistinguishedName	
(countryName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.6
value	PrintableString	JP
-	RelativeDistinguishedName	
(organizationName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.10
value	DirectoryString (UTF8String)	Japanese Government
-	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
uniformResourceIdentifier	[6] IA5String	http://crca1.moj.go.jp/certificateRevocationList.crl
onlyContainsUserCerts	[1] BOOLEAN DEFAULT FALSE	TRUE
signatureAlgorithm	AlgorithmIdentifier	
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.11
parameters	NULL	（注１）
signatureValue	BIT STRING	（注１０）

注１　長さオクテットに「0」を記録する。

注２　失効リストの発行日時をグリニッジ標準時により記録する。

注３　失効リストが次に発行される日時をグリニッジ標準時により記録する。指定された日時より前に発行されることがあるが、指定された日時より後に発行されることはない。

注４　失効した電子証明書のシリアル番号を記録する。

注５　電子証明書が失効した時刻をグリニッジ標準時により記録する。

注６　次の表に掲げる「事項」に該当する場合に、「記録内容」に定める数字を記録する。この場合において、項番１から４までの複数の事項に該当するときは、最初に生じた事項についてのみ記録する。項番５から７までのいずれかの事項が生じた時以後に、項番１から４までのいずれかの事項が生じたときは、項番１から４までの事項のうち、最初に生じた事項についてのみ記録する。

項番	事項	記録内容
1	商業登記法第 12 条の 2 第 7 項の届出があったとき	5
2	商業登記規則第 33 条の 12 第 1 項第 2 号の規定により電子証明書に記録された登記事項に変更を生ずる登記をした旨の通知があったとき	3
3	商業登記規則第 33 条の 16 第 1 項の規定により、登記所の事故により証明をするのが相当でなくなったと認めるとき	2
4	商業登記規則第 33 条の 16 第 1 項の規定により、登記所の事故以外の事由により証明をするのが相当でなくなったと認めるとき	5
5	商業登記規則第 33 条の 12 第 1 項第 1 号の通知があったとき（同項第 3 号の通知があったときを除く。）	6
6	商業登記規則第 33 条の 13 第 1 項の規定により電子証明書の使用の休止の届出があったとき（同条第 5 項の届出があったときを除く。）	6
7	項番 5 及び 6 のいずれにも該当するとき	6

注７　署名を検証するために使用される公開鍵識別子を記録する。

注８　登記官の電子証明書の番号を記録する。

注９　CRL シーケンス番号（最大 20 オクテットを超えない値）を記録する。

注１０　「tbsCertList」を DER で符号化した値に sha-256WithRSA による電子署名を講じた値を記録する。

4　失効リスト（Authority Revocation List）

フィールド	データ型	設定値
-	CertificateList	
tbsCertList	TBSCertList	
version	Version	1

signature	AlgorithmIdentifier	
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.11
parameters	NULL	（注１）
issuer	Name(RDNSequence)	
-	RelativeDistinguishedName	
(countryName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.6
value	PrintableString	JP
-	RelativeDistinguishedName	
(organizationName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.10
value	DirectoryString (UTF8String)	Japanese Government
-	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
thisUpdate	Time(UTCTime)	（注２）
nextUpdate	Time(UTCTime)	（注３）
revokedCertificates	SEQUENCE OF SEQUENCE	
userCertificate	CertificateSerialNumber	（注４）
revocationDate	Time(UTCTime)	（注５）
crlEntryExtensions	EntryExtensions	
reasonCode	EntryExtension	
extnId	OBJECT IDENTIFIER	2.5.29.21
extnValue	OCTET STRING	
CRLReason	ENUMERATED	（注６）
crlExtensions	[0]	
-	CRLExtensions	
authorityKeyIdentifier	CRLExtension	
extnId	OBJECT IDENTIFIER	2.5.29.35
extnValue	OCTET STRING	
-	AuthorityKeyIdentifier	
keyIdentifier	[0] KeyIdentifier	（注７）
authorityCertIssuer	[1] GeneralNames	
-	GeneralName([4])	
-	Name(RDNSequence)	
-	RelativeDistinguishedName	
(countryName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.6
value	PrintableString	JP
-	RelativeDistinguishedName	
(organizationName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.10
value	DirectoryString (UTF8String)	Japanese Government
-	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
authorityCertSerialNumber	[2] CertificateSerialNumber	（注８）
cRLNumber	CRLExtension	
extnId	OBJECT IDENTIFIER	2.5.29.20
extnValue	OCTET STRING	
CRLNumber	INTEGER	（注９）
IssuingDistributionPoint	CRLExtension	
extnId	OBJECT IDENTIFIER	2.5.29.28
critical	BOOLEAN DEFAULT FALSE	TRUE
extnValue	OCTET STRING	
distributionPoint	[0] DistributionPointName	
fullName	[0] GeneralNames	
DirectoryName	[4] Name	
-	RelativeDistinguishedName	
(countryName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.6
value	PrintableString	JP
-	RelativeDistinguishedName	
(organizationName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.10
value	DirectoryString (UTF8String)	Japanese Government
-	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
uniformResourceIdentifier	[6] IA5String	http://crca1.moj.go.jp/authorityRevocationList.crl
onlyContainsCACerts	[2] BOOLEAN DEFAULT FALSE	TRUE
signatureAlgorithm	AlgorithmIdentifier	
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.11
parameters	NULL	（注１）
signatureValue	BIT STRING	（注１０）

注１　長さオクテットに「0」を記録する。

注２　失効リストの発行日時をグリニッジ標準時により記録する。

注３　失効リストが次に発行される日時をグリニッジ標準時により記録する。指定された日時より前に発行されることがあるが、指定された日時より後に発行されることはない。

注４　失効した電子証明書のシリアル番号を記録する。

注５　注６の表中項番１から４までのいずれかの事項が記録される場合に、当該事項が生じた日時をグリニッジ標準時により記録する。

注６　次の表に掲げる「事項」に該当する場合に、「記録内容」に定める数字を記録する。

項番	事項	記録内容
1	相互認証証明書等の記載内容を変更したとき	3

2	ブリッジ認証局の秘密鍵が危殆化したとき	1
3	何らかの理由により相互認証を解消したとき	5
4	登記官の秘密鍵が危殆化したとき	2

注７　署名を検証するために使用される公開鍵識別子を記録する。

注８　登記官の電子証明書の番号を記録する。

注９　CRL シーケンス番号（最大 20 オクテットを超えない値）を記録する。

注１０　「tbsCertList」を DER で符号化した値に sha-256WithRSA による電子署名を講じた値を記録する。