第２―２ 相互認証証明書等の方式

１ 通則

（１）ブリッジ認証局と相互認証を行う際には、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２－２の様式に従って、「フィールド」欄に掲げる事項を記録した相互認証証明書を作成する。また、登記官がかぎを更新する際には、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２－２の様式に従って、「フィールド」欄に掲げる事項を記録したリンク証明書を作成する。

（２）データの符号化は、DER による。

２ 相互認証証明書

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	
(organizationalUnitName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.11
value	DirectoryString (UTF8String)	（注５）
-	RelativeDistinguishedName	
(commonName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.3
value	DirectoryString (UTF8String)	（注５）
subjectPublicKeyInfo	SubjectPublicKeyInfo	
algorithm	AlgorithmIdentifier	
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.1
parameters	NULL	（注２）
subjectPublicKey	BIT STRING	（注６）
extensions	[3]	
-	Extensions	
(authorityKeyIdentifier)	Extension	
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）
(subjectKeyIdentifier)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.14
extnValue	OCTET STRING	
-	SubjectKeyIdentifier	（注９）
(keyUsage)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.15
critical	BOOLEAN DEFAULT FALSE	TRUE
extnValue	OCTET STRING	
-	KeyUsage	0 0 0 0 0 1 1 0 0 (keyCertSign、cRLSign)
(certificatePolicies)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.32

critical	BOOLEAN DEFAULT FALSE	TRUE
extnValue	OCTET STRING	
-	CertificatePoliciesSyntax	
-	PolicyInformation	
policyIdentifier	CertPolicyId	1.2.392.100300.1.3.3（注１０）
(policyMappings)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.33
critical	BOOLEAN DEFAULT FALSE	TRUE
extnValue	OCTET STRING	
-	PolicyMappingsSyntax	
issuerDomainPolicy	CertPolicyId	1.2.392.100300.1.3.3（注１０）
subjectDomainPolicy	CertPolicyId	（注１１）
(basicConstraints)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.19
critical	BOOLEAN DEFAULT FALSE	TRUE
extnValue	OCTET STRING	
-	BasicConstraintsSyntax	
cA	BOOLEAN DEFAULT FALSE	TRUE
(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
(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１２）

注１　相互認証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　相互認証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　相互認証証明書の使用を開始する日から起算して、GPKI で規定された期間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　ブリッジ認証局の識別名を記録する。

注６　ブリッジ認証局の公開かぎを記録する。

注７　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８　登記官の電子証明書の番号を記録する。

注９　「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１０　法務省ホームページに掲示される相互認証証明書等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１１　ブリッジ認証局のポリシーのオブジェクト識別子を記録する。

注１２　「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　リンク証明書（OldWithNew）

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) （注１１）	Japanese Government
-	RelativeDistinguishedName	
(organizationalUnitName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.11
value	DirectoryString (UTF8String) （注１１）	Ministry of Justice
-	RelativeDistinguishedName	
(commonName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.3
value	DirectoryString (UTF8String) （注１１）	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１２）	Japanese Government
-	RelativeDistinguishedName	
(organizationalUnitName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.11
value	DirectoryString (UTF8String) （注１２）	Ministry of Justice
-	RelativeDistinguishedName	
(commonName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.3
value	DirectoryString (UTF8String) （注１２）	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	
(authorityKeyIdentifier)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.35
extnValue	OCTET STRING	
-	AuthorityKeyIdentifier	
keyIdentifier	[0] KeyIdentifier	（注６）
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) （注１１）	Japanese Government
-	RelativeDistinguishedName	
(organizationalUnitName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.11
value	DirectoryString (UTF8String) （注１１）	Ministry of Justice
-	RelativeDistinguishedName	
(commonName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.3
value	DirectoryString (UTF8String) （注１１）	Registrar of Tokyo Legal Affairs Bureau
authorityCertSerialNumber	[2] CertificateSerialNumber	（注７）
(subjectKeyIdentifier)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.14
extnValue	OCTET STRING	
-	SubjectKeyIdentifier	（注８）
(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)
(certificatePolicies)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.32
extnValue	OCTET STRING	
-	CertificatePoliciesSyntax	
-	PolicyInformation	
policyIdentifier	CertPolicyId	2.5.29.32.0 （注９）
(basicConstraints)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.19
critical	BOOLEAN DEFAULT FALSE	TRUE
extnValue	OCTET STRING	
-	BasicConstraintsSyntax	
cA	BOOLEAN DEFAULT FALSE	TRUE
(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
(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１０）

注１　リンク証明書（OldWithNew）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　「subjectPublicKey」に記録された公開かぎ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　「subjectPublicKey」に記録された公開かぎの使用を終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　一世代前の登記官の公開かぎを記録する。

注６　最新の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７　最新の登記官の電子証明書の番号を記録する。

注８　「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　新旧の登記官の証明書をリンクするに当たり、ポリシーに制限を設けないことを意味するオブジェクト識別子を記録する。

注１０　「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。

注１１　最新の登記官の電子証明書の「subject」の値を記録する。

注１２　一世代前の登記官の電子証明書の「subject」の値を記録する。

4 リンク証明書（NewWithOld）

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) （注１１）	Japanese Government
-	RelativeDistinguishedName	
(organizationalUnitName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.11
value	DirectoryString (UTF8String) （注１１）	Ministry of Justice
-	RelativeDistinguishedName	
(commonName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.3
value	DirectoryString (UTF8String) （注１１）	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１２）	Japanese Government
-	RelativeDistinguishedName	
(organizationalUnitName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.11
value	DirectoryString (UTF8String) （注１２）	Ministry of Justice
-	RelativeDistinguishedName	
(commonName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.3
value	DirectoryString (UTF8String) （注１２）	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	
(authorityKeyIdentifier)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.35
extnValue	OCTET STRING	
-	AuthorityKeyIdentifier	
keyIdentifier	[0] KeyIdentifier	（注６）
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) （注１１）	Japanese Government
-	RelativeDistinguishedName	
(organizationalUnitName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.11
value	DirectoryString (UTF8String) （注１１）	Ministry of Justice
-	RelativeDistinguishedName	
(commonName)	AttributeTypeAndValue	
type	OBJECT IDENTIFIER	2.5.4.3
value	DirectoryString (UTF8String) （注１１）	Registrar of Tokyo Legal Affairs Bureau
authorityCertSerialNumber	[2] CertificateSerialNumber	（注７）
(subjectKeyIdentifier)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.14
extnValue	OCTET STRING	
-	SubjectKeyIdentifier	（注８）
(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)
(certificatePolicies)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.32
extnValue	OCTET STRING	
-	CertificatePoliciesSyntax	
-	PolicyInformation	
policyIdentifier	CertPolicyId	2.5.29.32.0 （注９）
(basicConstraints)	Extension	
extnId	OBJECT IDENTIFIER	2.5.29.19
critical	BOOLEAN DEFAULT FALSE	TRUE
extnValue	OCTET STRING	
-	BasicConstraintsSyntax	
cA	BOOLEAN DEFAULT FALSE	TRUE
(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
(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１０）

注１　リンク証明書（NewWithOld）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　「subjectPublicKey」に記録された公開かぎ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　一世代前の登記官の電子証明書の「subjectPublicKey」に記録された公開かぎの使用を終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　最新の登記官の公開かぎを記録する。

注６　一世代前の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７　一世代前の登記官の電子証明書の番号を記録する。

注８　「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　新旧の登記官の証明書をリンクするに当たり、ポリシーに制限を設けないことを意味するオブジェクト識別子を記録する。

注１０　「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。

注１１　一世代前の登記官の電子証明書の「subject」の値を記録する。

注１２　最新の登記官の電子証明書の「subject」の値を記録する。

第３－２ 相互認証証明書等の公開

１ 通則

登記官の電子証明書、相互認証証明書及びリンク証明書（OldWithNew、NewWithOld）、失効リスト（Certificate Revocation List 及び Authority Revocation List）は、ブリッジ認証局の統合リポジトリにおいて公開される。ただし、有効期間を経過し、又は失効されたものについては、この限りでない。

第６―２　相互認証証明書及びリンク証明書の有効性に関する証明及びその請求の方式

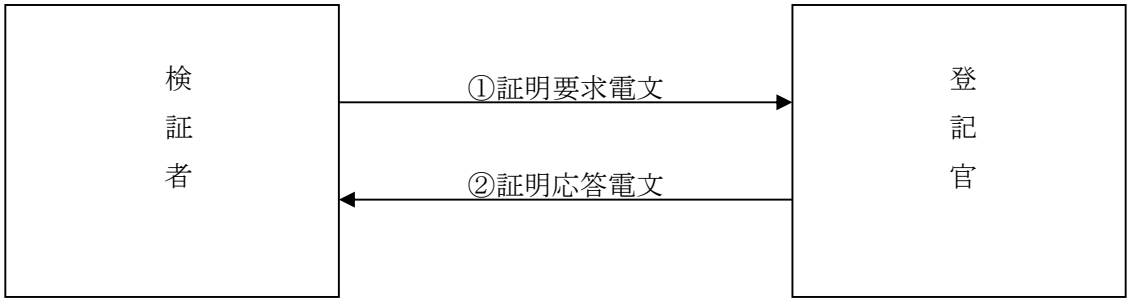
１　通信プロトコル

相互認証証明書及びリンク証明書（以下「相互認証証明書等」という。）の有効性に関する証明及びその請求のための送受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

登記官と検証者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　検証者が登記官に送信する「証明要求電文」は、請求に係る相互認証証明書等に記録された「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（「notBefore」から「notAfter」までの範囲に限る。）についての「証明要求電文」は、請求に係る相互認証証明書等に記録された「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、検証者に 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	証明の対象となる相互認証証明書等の「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	証明の請求に係る相互認証証明書等の番号を記録する。	◎
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　証明の対象となる相互認証証明書等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 証明の対象となる相互認証証明書等に「notAfter」として記録された日時までの間にあっては、相互認証証明書等に「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 相互認証証明書等に「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、相互認証証明書等に「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	相互認証証明書等について項番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４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、又は相互認証証明書等に記録された「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。

項番	事項	記録内容	
		CRL Reason	OcspStatus Code
1	相互認証証明書等の記載内容を変更したとき	3	2
2	ブリッジ認証局の秘密鍵が危殆化したとき	1	5
3	何らかの理由により相互認証を解消したとき	5	1
4	登記官の秘密鍵が危殆化したとき	2	4
5	注９により、「good」のフィールドを設定したとき		0
6	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。