```
ub-registry-office                INTEGER ::= 128

END
```

付録３　電子証明書の送信の方式（送受信電文の ASN.１構造とオブジェクト識別子）

１　Explicitly Tagged Module

```
MOJCMPCertReq { 1 2 392 100300 1 4 11 }

DEFINITIONS EXPLICIT TAGS ::=
BEGIN

IMPORTS

      Certificate
            FROM MOJCorpCertExplicit { 1 2 392 100300 1 4 1 }

      GeneralName, CertReqMessages, EncryptedValue
            FROM MOJCRMFCertReq { 1 2 392 100300 1 4 12 };

AlgorithmIdentifier ::= SEQUENCE {
   algorithm            ALGORITHM-ID.&id ({SupportedAlgorithms}),
   parameters           ALGORITHM-ID.&Type ({SupportedAlgorithms}
                                        {@algorithm }) OPTIONAL }

ALGORITHM-ID ::= CLASS {
     &id    OBJECT IDENTIFIER UNIQUE,
     &Type  OPTIONAL
}
WITH SYNTAX { OID &id [PARMS &Type] }

SupportedAlgorithms ALGORITHM-ID ::= { ..., -- extensible
                                       rsaPublicKey |
                                       rsaSHA-1 |
                                       rsaSHA-256 |
                                       des-EDE3-CBC |
                                       des-EDE3-CBC-NoParms |
                                       sha1Identifier }
                                       sha256Identifier }

rsaPublicKey ALGORITHM-ID ::= { OID rsaEncryption PARMS NULL }

rsaSHA-1 ALGORITHM-ID ::= { OID sha1WithRSAEncryption PARMS NULL }

rsaSHA-256 ALGORITHM-ID ::= { OID sha256WithRSAEncryption PARMS NULL }

des-EDE3-CBC ALGORITHM-ID ::= { OID dES-EDE3-CBC PARMS CBCParameter }

des-EDE3-CBC-NoParms ALGORITHM-ID ::= { OID dES-EDE3-CBC PARMS NULL }

sha1Identifier ALGORITHM-ID ::= { OID id-SHA1 PARMS NULL }

sha256Identifier ALGORITHM-ID ::= { OID id-SHA256 PARMS NULL }


pkcs-1 OBJECT IDENTIFIER ::= {
     iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 }

rsaEncryption OBJECT IDENTIFIER ::=  { pkcs-1 1 }
-- Public key syntax
RSAPublicKey  ::=  SEQUENCE  {
     modulus INTEGER, -- n
     publicExponent INTEGER -- e
}

sha1WithRSAEncryption OBJECT IDENTIFIER  ::=  { pkcs-1 5 }

sha256WithRSAEncryption OBJECT IDENTIFIER  ::=  { pkcs-1 11 }

dES-EDE3-CBC OBJECT IDENTIFIER  ::=  {
     iso(1) member-body(2) us(840) rsadsi(113549) encryptionAlgorithm(3) 7 }
-- dES-EDE3-CBC parameters
CBCParameter ::= IV
IV ::= OCTET STRING (SIZE (8..8))

id-SHA1 OBJECT IDENTIFIER ::= {
     iso(1) identified-organization(3) oiw(14) secsig(3) algorithms(2) 26 }

id-SHA256 OBJECT IDENTIFIER ::= {
     joint-iso-itu-t(2) country(16) us(840) organization(1)
     gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }


InfoTypeAndValue ::= SEQUENCE {
      infoType       INFORMATION-ID.&id({InfoSet}),
      infoValue      INFORMATION-ID.&Type({InfoSet}{@infoType})
}

INFORMATION-ID ::= CLASS {
     &id    OBJECT IDENTIFIER UNIQUE,
```