```
EncryptedValue ::= SEQUENCE {
    symmAlg       [1] AlgorithmIdentifier,
    encSymmKey    [2] BIT STRING,
    keyAlg        [3] AlgorithmIdentifier,
    encValue       BIT STRING }

GeneralName ::= CHOICE {
    directoryName         [4] Name }

END
```

付録４　休止届の送信の方式（送受信電文の ASN.１構造とオブジェクト識別子）

１　Explicitly Tagged Module

```
MOJCMPSuspReq { 1 2 392 100300 1 4 21 }

DEFINITIONS EXPLICIT TAGS ::=
BEGIN

IMPORTS

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

      GeneralName, EncryptedValue, CertTemplate, CertId, ReasonFlags
      FROM MOJCRMFSuspReq { 1 2 392 100300 1 4 22 };


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-256 |
                                         des-EDE3-CBC |
                                         sha256Identifier }

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

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

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

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 }
-- subjectPublicKey syntax
RSAPublicKey  ::=  SEQUENCE  {
     modulus INTEGER, -- n
     publicExponent INTEGER -- e
}

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-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,
     &Type
}
WITH SYNTAX { SYNTAX &Type IDENTIFIED BY &id }

InfoSet INFORMATION-ID ::= { genmSuspReqContent |
                             genpSuspResContent |
                             genmInfoReqContent |
                             genpInfoResContent
```