```
-- The max size of Suspdata is 84Bytes. (Max64Bytes + 20Bytes).

GenpSuspResContent ::= SEQUENCE {
      status         PKIStatusInfo,
      -- status information of suspension results
      revCert        CertId
      -- IDs for which revocation was requested (same order as status)
}

GenmInfoReqContent ::= SEQUENCE OF NegotiationKey

NegotiationKey ::= SEQUENCE {
     symmAlg  AlgorithmIdentifier,
     pubAlg   AlgorithmIdentifier,
     hashAlg  AlgorithmIdentifier  }

GenpInfoResContent ::= SEQUENCE {
     status           PKIStatusInfo,
     negotiationKeys  SEQUENCE OF NegotiationKey OPTIONAL  }

END
```

２　Implicitly Tagged Module

```
MOJCRMFSuspReq { 1 2 392 100300 1 4 22 }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS
        AlgorithmIdentifier
        FROM MOJCMPSuspReq { 1 2 392 100300 1 4 21 }

        SubjectPublicKeyInfo, Name, RDNSequence
        FROM MOJCorpCertExplicit { 1 2 392 100300 1 4 1 };


CertTemplate ::= SEQUENCE {
    serialNumber [1] INTEGER,
    issuer       [3] Name }

EncryptedValue ::= SEQUENCE {
    keyAlg        [3] AlgorithmIdentifier,
    encValue       BIT STRING }

CertId ::= SEQUENCE {
    issuer           GeneralName,
    serialNumber     INTEGER }

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

ReasonFlags ::= BIT STRING {
        certificateHold         (6) }

END
```

付録５　電子証明書に係る証明及びその請求の方式（送受信電文の ASN.1 構造とオブジェクト識別子）

```
MOJOCSP { 1 2 392 100300 1 4 31 }

DEFINITIONS EXPLICIT TAGS ::=
BEGIN

IMPORTS

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


OCSPRequest ::=  SEQUENCE {
    tbsRequest                  TBSRequest  }

TBSRequest ::= SEQUENCE {
    version             [0] EXPLICIT Version DEFAULT v1,
    requestList             SEQUENCE OF Request,
    requestExtensions   [2] EXPLICIT Extensions  -- nonce
}

Version ::= INTEGER  { v1(0) }

Request ::= SEQUENCE {
    reqCert                    CertID,
    singleRequestExtensions    [0] EXPLICIT Extensions OPTIONAL  -- confirmationTime
}

CertID ::= SEQUENCE {
    hashAlgorithm      AlgorithmIdentifier,
    issuerNameHash     OCTET STRING, -- Hash of Issuer's DN
    issuerKeyHash      OCTET STRING, -- Hash of Issuers public key
```