```
CRLDistPointsSyntax ::= SEQUENCE SIZE (1..MAX) OF DistributionPoint

DistributionPoint ::= SEQUENCE {
        distributionPoint       [0]     DistributionPointName }

DistributionPointName ::= CHOICE {
        fullName                [0]     GeneralNames }

id-ce   OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) ds(5) 29}

id-ce-subjectKeyIdentifier         OBJECT IDENTIFIER ::= {id-ce 14}
id-ce-keyUsage                     OBJECT IDENTIFIER ::= {id-ce 15}
id-ce-privateKeyUsagePeriod        OBJECT IDENTIFIER ::= {id-ce 16}
id-ce-basicConstraints             OBJECT IDENTIFIER ::= {id-ce 19}
id-ce-cRLDistributionPoints        OBJECT IDENTIFIER ::= {id-ce 31}
id-ce-certificatePolicies          OBJECT IDENTIFIER ::= {id-ce 32}
id-ce-authorityKeyIdentifier       OBJECT IDENTIFIER ::= {id-ce 35}

id-pkix OBJECT IDENTIFIER ::=
  { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) }

id-pe   OBJECT IDENTIFIER ::= { id-pkix 1 }

id-pe-authorityInfoAccess OBJECT IDENTIFIER ::= { id-pe 1 }

id-qt   OBJECT IDENTIFIER ::= { id-pkix 2 }

id-qt-unotice  OBJECT IDENTIFIER ::=  { id-qt 2 }

id-ad   OBJECT IDENTIFIER ::= { id-pkix 48 }

id-ad-ocsp      OBJECT IDENTIFIER ::= { id-ad 1 }

id-registeredcert OBJECT IDENTIFIER ::= { 1 2 392 100300 1 }

id-registeredcert-pe OBJECT IDENTIFIER ::=  { id-registeredcert 1 }

id-registeredcert-pe-jCertificatePolicies OBJECT IDENTIFIER ::= {id-registeredcert-pe 1 }
id-registeredcert-pe-registrar OBJECT IDENTIFIER ::= { id-registeredcert-pe 2 }
id-registeredcert-pe-registeredCorporationInfo OBJECT IDENTIFIER ::= {
     id-registeredcert-pe 3 }

ub-registrar                     INTEGER ::= 128
ub-corporate-name                INTEGER ::= 128
ub-corporate-address             INTEGER ::= 128
ub-representative-director-name  INTEGER ::= 126
ub-representative-director-title  INTEGER ::= 128
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-256 |
                                       des-EDE3-CBC |
                                       des-EDE3-CBC-NoParms |
                                       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 }
```