```
CRLReason ::= ENUMERATED {
        keyCompromise           (1),
        cACompromise            (2),
        affiliationChanged      (3),
        cessationOfOperation    (5),
        certificateHold         (6)
}

Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension

Extension ::= SEQUENCE {
   extnId            EXTENSION.&id ({ExtensionSet}),
   critical          BOOLEAN DEFAULT FALSE,
   extnValue         OCTET STRING }

ExtensionSet  EXTENSION  ::= { ..., -- extensible
                               nonce |
                               confirmationTime |
                               ocspStatusCode
}

EXTENSION ::= CLASS {
   &id          OBJECT IDENTIFIER UNIQUE,
   &ExtnType
}
WITH SYNTAX  {
   SYNTAX         &ExtnType
   IDENTIFIED BY  &id }

nonce EXTENSION ::= {
        SYNTAX  Nonce
        IDENTIFIED BY id-pkix-ocsp-nonce }

Nonce ::= OCTET STRING

confirmationTime EXTENSION ::= {
        SYNTAX  ConfirmationTime
        IDENTIFIED BY id-registeredcert-mg-confirmationtime }

ConfirmationTime ::= GeneralizedTime

ocspStatusCode EXTENSION ::= {
        SYNTAX  OcspStatusCode
        IDENTIFIED BY id-registeredcert-mg-ocspstatuscode }

OcspStatusCode ::= INTEGER

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

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

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

id-pkix-ocsp                OBJECT IDENTIFIER ::= { id-ad-ocsp }
id-pkix-ocsp-basic          OBJECT IDENTIFIER ::= { id-pkix-ocsp 1 }
id-pkix-ocsp-nonce          OBJECT IDENTIFIER ::= { id-pkix-ocsp 2 }
-- The nonce will be identified by the object identifier id-pkix-ocsp-nonce,
-- while the extnValue is the value of the nonce.

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

id-registeredcert-mg OBJECT IDENTIFIER ::= { id-registeredcert 2 }

id-registeredcert-mg-confirmationtime OBJECT IDENTIFIER ::= { id-registeredcert-mg 102 }
id-registeredcert-mg-ocspstatuscode OBJECT IDENTIFIER ::= { id-registeredcert-mg 103 }

END
```

付録６　失効リストの公開（ASN.１構造とオブジェクト識別子）

１　Explicitly Tagged Module

```
MOJCorpCertCRLExplicit { 1 2 392 100300 1 4 51 }

DEFINITIONS EXPLICIT TAGS ::=
BEGIN

-- EXPORTS ALL --

IMPORTS
        AlgorithmIdentifier, Name, Time, CertificateSerialNumber
        FROM MOJCorpCertExplicit { 1 2 392 100300 1 4 1 }
        authorityKeyIdentifier
        FROM MOJCorpCertImplicit { 1 2 392 100300 1 4 2 };
        cRLNumber, issuingDistributionPoint, reasonCode
        FROM MOJCorpCertCRLImplicit { 1 2 392 100300 1 4 52 };

CertificateList ::=  SIGNED { TBSCertList }

TBSCertList ::= SEQUENCE {
```