7　証明書及び失効リスト及びOCSPのプロファイル

7.1　証明書のプロファイル

本ポリシの認証局が発行する証明書は、X509 Version 3 フォーマット証明書形式により作成され、また証明書はX.500識別名（Distinguished Name、以下DNという）により一意に識別されるものとする。

本ポリシに従い発行される電子証明書のプロファイルは、表7.1.1および表7.1.2の通りとする。なお、IssuerのDNはCPS及びその他開示文書に記述されることとする。

7.1.1 バージョン番号

本ポリシの認証局が発行する証明書は、X509 Version 3 フォーマット証明書形式により作成されることとする。

7.1.2　証明書の拡張（保健医療福祉分野の属性を含む）

本ポリシに従い発行される電子証明書の拡張領域のプロファイルは以下の表7.1.2の通りとする。表中の、「◎」は必須、「○」は場合により必須、「△」はオプション、「×」は設定しないことを表す。なお、IssuerのDNは認証局の定めるCPS及びその他開示文書に記述される。

注）サブジェクトディレクトリ属性でのhcRole属性の使用について

attrTypeにはHcRoleを表すOID（{id-hcpki-at-healthcareactor}）を設定する。

本拡張は、加入者が国家資格保有者および医療機関等の管理者の場合は必須、その他(患者等)の場合は省略可とする。

attrValue（HCActorData）には資格に対応する名称をHCActorのcodedDataのcodeDataFreeTextにUTF-8で設定する。subjectが複数の資格を有する場合は、HCActorDataに資格数分のHCActorを設定することができる。

記述する国家資格を示す名称は、次の英語表記を用いる。

Medical Doctor	医師
Dentist	歯科医師
Pharmacist	薬剤師
Medical Technologist	臨床検査技師
Radiological Technologist	診療放射線技師
General Nurse	看護師

Public Health Nurse	保健師
Midwife	助産師
Physical Therapist	理学療法士
Occupational Therapist	作業療法士
Orthoptist	視能訓練士
Speech Therapist	言語聴覚士
Dental Technician	歯科技工士
National Registered Dietitian	管理栄養士
Certified Social Worker	社会福祉士
Certified Care Worker	介護福祉士
Emergency Medical Technician	救急救命士
Psychiatric Social Worker	精神保健福祉士
Clinical Engineer	臨床工学技師
Masseur	あん摩マッサージ指圧師/はり師/きゅう師
Dental Hygienist	歯科衛生士
Prosthetics & Orthctic	義肢装具士
Artificial Limb Fitter	柔道整復師
Clinical Laboratory Technician	衛生検査技師
Care Manager	介護支援専門員

この他に医療機関の管理責任者として、次の属性を使用することができる。

Director of Hospital	病院長
Director of Clinic	診療所院長
Director of Pharmacy	保険薬局の管理責任者
Director	その他の保健医療福祉機関の管理責任者

患者に対して署名付の文書を交付することが多い病院長、診療所院長、保健薬局の管理責任者を HcRole だけで識別できるように定めている。

なお、上記Director 4 属性を使用する場合はSubject フィールドのOrganizationName およびOrganizationUnitName は必須で、OrganizationName に保健医療福祉機関名を英語またはローマ字で格納し、OrganizationUnitName に"Director"の文字列を格納する。

【参考】

ISO TS17090 に定められた hcRole 属性の ASN.1 表記の抜粋は次のとおりである。

```
hcRole ATTRIBUTE ::= {
    WITH SYNTAX                 HCActorData
    EQUALITY MATCHING RULE      hcActorMatch
    SUBSTRINGS MATCHING RULE    hcActorSubstringsMatch
    ID                          id-hcpki-at-healthcareactor}

Assignment of object identifier values
The following values are assigned in this Technical Specification:
{iso (1) standard (0) hcpki (17090)}
    id-hcpki  OBJECT IDENTIFIER ::= 1.0.17090
    id-hcpki-at   OBJECT IDENTIFIER ::= {id-hcpki 0 }
    id-hcpki-at   OBJECT IDENTIFIER ::= 1.0.17090.0
id-hcpki-at-healthcareactor   OBJECT IDENTIFIER ::= {id-hcpki-at 1}
    id-hcpki-at-healthcareactor   OBJECT IDENTIFIER ::= 1.0.17090.0.1
id-hcpki-cd   OBJECT IDENTIFIER ::= {id-hcpki 1}
    id-hcpki-cd   OBJECT IDENTIFIER ::= 1.0.17090.1

Definition of data types:
HCActorData    ::= SET OF HCActor
HCActor      ::= SEQUENCE {
    codedData [0] CodedData OPTIONAL,
    RegionalHCActorData [1]
            SEQUENCE OF RegionalData OPTIONAL }
CodedData ::= SET {
        codingSchemeReference   [0] OBJECT IDENTIFIER,
        ---- Contains the ISO coding scheme Reference
        ---- or local coding scheme reference achieving ISO registration.
        ---- The ISO coding scheme OID is id-hcpki (defined above).
        ---- At least ONE of the following SHALL be present:
    codeDataValue  [1] NumericString OPTIONAL,
    codeDataFreeText  [2] DirectoryString OPTIONAL }
```

(RegionalHcActorData の詳細は本 CP では使用しないために省略)

7.1.3 アルゴリズムオブジェクト識別子

基本領域の Signature アルゴリズムは以下の通りとする。

sha1WithRSAEncryption (1.2.840.113549.1.1.5)

基本領域のsubjectPublicKeyInfoアルゴリズムは以下の通りとする。

RSAEncryption (1.2.840.113549.1.1.1)

7.1.4 名前の形式

Issure と Subject の名前の形式は表 7.1.1 に示される。

7.1.5 名前制約

用いない。

7.1.6 CP オブジェクト識別子

別途規定する。

7.1.7 ポリシ制約拡張

使用しない。

7.1.8 ポリシ修飾子の構文及び意味

CPS を参照する URL を含めることができる。

7.1.9 証明書ポリシ拡張フィールドの扱い

本 CP の OID を格納する。

表 7.1.1　証明書のプロファイル（基本領域）

項目	設定	説明
Version	◎	Ver3 とする。
SerialNumber	◎	同一認証局が発行する証明書内でユニークな値とする。
Signature	◎	
Validity	◎	
NotBefore	◎	
NotAfter	◎	
Issuer	◎	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）
CountryName	◎	c=JP（固定）とする。
LocalityName	△	
OrganizationName	◎	
OrganizationUnitName	△	
CommonName	◎	認証局のポリシを示す文字列を記載する。（「HPKI-01-*-forNonRepudiation」とする。なお、文字列中の"01"は、本 CP の版数である"第 1.0 版"を示す。また、"*"は CA を唯一に識別できる文字列とする。）
Subject	◎	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）
CountryName	◎	c=JP（固定）とする。
LocalityName	△	
OrganizationName	○	加入者が医療機関等の管理者の場合は必須。その場合は医療福祉機関名をローマ字あるいは英語名で OrganizationName に記載し、OrganizatioUnitName に”Director”の文字列を格納する。
OrganizationUnitName	○	
CommonName	◎	加入者の氏名をローマ字で記載する。
GivenName	×	
SurName	×	
e-Mail	×	
SerialNumber	△	医籍登録番号などを記載することができる。
SubjectPublicKeyInfo	◎	
Algorithm	◎	RSAEncryption とする。
SubjectPublicKey	◎	
IssuerUniqueID	×	
SubjectUniqueID	×	
Extentions	◎	拡張領域（Extensions）参照

表 7.1.2　証明書のプロファイル（拡張領域 Extensions）

項目	設定	説明	Critical
authorityKeyIdentifier	◎		FALSE
subejctKeyIdentifier	◎		FALSE
keyUsage	◎		TRUE
DigitalSignature	×		-
NonRepudiation	◎		-
KeyEncipherment	×		-
DataEncipherment	×		-
KeyAgreement	×		-
KeyCertSign	×		-
CRLSign	×		-
EncipherOnly	×		-
DeciphermentOnly	×		-
extendedKeyUsage	×		FALSE
privateKeyUsagePeriod	×		FALSE
certificatePolicies	◎		TRUE
policyMapping	×		FALSE
subjectAltName	△		FALSE
issuerAltName	△		FALSE
subjectDirectoryAttributes	◎	医療従事者の資格を記載。	FALSE
attrType	○	加入者が国家資格保有者および医療機関等の管理者の場合は必須。その他(患者等)の場合は省略可。	-
attrValues	○	資格に対応する HCActor を PrintableString で設定する。subject が複数の資格を有する場合は、HCActorData に資格数分の HCActor を設定する。	-
basicConstraints	×		TRUE
CA	×		-
pathLenConstraints	×		-
nameConstraints	×		TRUE
policyConstraints	×		TRUE
cRLDistributionPoints	◎	DirectoryName あるいは URI で、CRL の配布点を指定する。	FALSE
subjectInfoAccess	×		FALSE
authorityInfoAccess	△		FALSE

7.2 証明書失効リストのプロファイル

7.2.1 バージョン番号

認証局が発行する CRL は、X.509CRL フォーマット形式のバージョン 2 に従うものとする。

基本領域のプロファイルは表 7.2.1 に示す。

7.2.1 CRL と CRL エントリ拡張領域

CRL エントリの拡張領域のプロファイルは、以下の表 7.2.2 の通りとする。CRL 拡張領域のプロファイルは、以下の表 7.2.3 の通りとする。

表中の、「◎」は必須、「○」は場合により必須、「△」はオプション、「×」は設定しないことを表す。

表 7.2.1 証明書失効リストのプロファイル（CRL 基本領域）

フィールド	設定	説明
Version	◎	Ver2 とする。
Signature	◎	SHA-1WithRSAEncryption とする。
Issuer	◎	英数字のみ使用する。(CountryName は Printable、それ以外は UTF-8 で記述する)
CountryName	◎	c=JP(固定)とする。
LocalityName	△	
OrganizationName	◎	
OrganizationUnitName	△	
CommonName	◎	認証局のポリシを示す文字列を記載する。
ThisUpdata	◎	
NextUpdate	◎	
RevokedCertificates	◎	
userCertificate	◎	失効した証明書の serialNumber を記載。
revocationDate	◎	失効日時を記載する。
crlEntryExtensions	◎	拡張領域（crlEntryExtentions）参照
crlExtentions	◎	拡張領域（crlExtensions）参照

表 7.2.2　証明書失効リストのプロファイル（CRL エントリ拡張領 crlEntryExtentions）

フィールド	設定	説明	Critical
reasonCode	◎		FALSE
holdInstructionCode	×		FALSE
invalidityDate	×		FALSE
certificateIssure	×		TRUE

表 7.2.3　証明書失効リストのプロファイル（CRL 拡張領域 crlExtentions）

フィールド	設定	説明	Critical
authorityKeyIdentifier	◎		FALSE
issuerAltName	△		FALSE
cRLNumber	◎		FALSE
deltaCRLIndicator	×		TRUE
IssueingDistributionPoint	○	分割 CRL を用いる場合は必須	TRUE
freshesCRL	×		FALSE

7.3　OCSP プロファイル

7.3.1　バージョン番号

規定しない。

7.3.2　OCSP 拡張領域

規定しない。