6.1.7 鍵の利用目的

認証局の鍵は、keyCertSign と cRLSign のビットを使用する。

エンドエンティティの鍵は、DigitalSignature のビットを使用する。

6.2 私有鍵の保護及び暗号モジュール技術の管理

6.2.1 暗号モジュールの標準及び管理

CA 私有鍵の格納モジュールは、US FIPS 140-2 レベル 3 と同等以上の規格に準拠するものとする。

エンドエンティティの加入者私有鍵の格納モジュールは、US FIPS 140-2 レベル 1 と同等以上の規格に準拠するものとする。

6.2.2 私有鍵の複数人によるコントロール

CA 私有鍵の生成には、運用管理者と複数名の権限者を必要とする。また、鍵生成後の私有鍵の操作（活性化、非活性化、バックアップ、搬送、破棄等）においても複数名の権限者を必要とする。

6.2.3 私有鍵のエスクロウ

CA 私有鍵は、法律によって必要とされる場合を除き、エスクロウされないものとする。

エンドエンティティの加入者の私有鍵は、法律によって必要とされる場合を除き、エスクロウされないものとする。

6.2.4 私有鍵のバックアップ

CA 私有鍵のバックアップは、安全な方法で行う。例えば、バックアップ作業の権限を有する複数人の立会いのもとで行うようにしたり、バックアップデータとして CA 私有鍵に関する情報を暗号化したり分散させて保管するなどの方法がある。

6.2.5 私有鍵のアーカイブ

認証局は加入者の私有鍵をアーカイブしない。

6.2.6 暗号モジュールへの私有鍵の格納と取り出し

CA 私有鍵は、安全に格納することとする。例えば、認証設備室内にある暗号モジュール内に格納するなどの方法がある。

外部へのバックアップの転送や外部からのリストアの場合は、セキュアチャネルを通して行うものとする。

6.2.7 暗号モジュールへの私有鍵の格納

私有鍵がエンティティの暗号モジュールで生成されない場合は、IETF RFC 2510「証明書管理プロトコル」に従って、又は同様に安全な方法で、モジュールに入力されるものとする。

6.2.8 私有鍵の活性化方法

CA 私有鍵の活性化の方法は、認証局室内において本 CP「6.2.2 私有鍵の複数人によるコントロール」と同じく、複数名の権限を有する者を必要とする。

6.2.9 私有鍵の非活性化方法

CA 私有鍵の非活性化の方法は、認証局室内において本 CP「6.2.2 私有鍵の複数人によるコントロール」と同じく、複数名の権限を有する者を必要とする。

6.2.10 私有鍵の廃棄方法

CA 私有鍵を破棄しなければならない状況の場合、認証局室内で本 CP「6.2.2 私有鍵の複数人によるコントロール」と同じく、複数名の権限を有する者によって、私有鍵の格納された HSM を完全に初期化し、又は物理的に破壊する。同時に、バックアップの私有鍵に関しても同様の手続きによって破棄する。

加入者私有鍵破棄手続きは、CPS 又は加入者が入手可能な文書に記述するものとする。

6.2.11 暗号モジュールの評価

CA 私有鍵を格納する暗号モジュールは、FIPS 140-2 レベル 3 と同等以上のものを使用する。

エンドエンティティの加入者の私有鍵を格納する暗号モジュールは、FIPS 140-2 レベル 1 と同等以上のものを使用する。

6.3 鍵ペア管理に関するその他の面

6.3.1 公開鍵のアーカイブ

公開鍵は、後日の署名の検証を可能にするために、信頼できる方法でアーカイブする必要がある。認証局は、公開鍵が CPS で定める期間アーカイブされることを保証する責任があるものとする。

6.3.2 公開鍵証明書の有効期間と鍵ペアの使用期間

CA 公開鍵証明書の有効期間は 20 年を越えないものとし、その私有鍵の使用は 10 年を越えないものとする。

エンドエンティティの加入者の公開鍵証明書の有効期間は 2 年を越えないものとし、その私有鍵の使用は 2 年を越えないものとする。

6.4 活性化用データ

6.4.1 活性化データの生成とインストール

認証局において用いられる CA 私有鍵の活性化データは一意で予測不能なものとし、その生成とインストールは認証局で定められた規定に従い実施されるものとする。

エンドエンティティの加入者私有鍵の活性化データが認証局で生成される場合は、活性化データは一意で予測不能なものとし、その生成とインストールは認証局で定められた規定に従い実施され、加入者に安全に伝えられるものとする。

加入者私有鍵の活性化データを加入者が生成する場合は、活性化データは予測不能なものとし、その生成とインストールは認証局で定められた規定に従い実施されるものとする。

6.4.2 活性化データの保護

認証局において用いられる CA 私有鍵の活性化データは、認証局で定められた規定に従い安全に保護される。

エンドエンティティの加入者私有鍵の活性化データが認証局で生成される場合は、活性化データが加入者に伝えられた後は、認証局においては完全に破棄し保管しないものとする。また、伝えられた活性化データは、認証局で定められた規定に従い、加入者により安全に保護するものとする。

加入者私有鍵の活性化データを加入者が生成する場合は、認証局で定められた規定に従い、加入者により安全に保護するものとする。

6.4.3 活性化データのその他の要件

規定しない。

6.5 コンピュータのセキュリティ管理

6.5.1 特定のコンピュータのセキュリティに関する技術的要件

認証業務用設備に対する当該電気通信回線を通じて行われる不正なアクセス等を防御するための対策を行うこと。

CA システムへのログイン時には、本 CP「5.2.3 個々の役割に対する本人性確認と認証」で定めるユーザの認証を必須とする。

6.5.2 コンピュータセキュリティ評価

ISO15408 を参考にセキュリティ基準を設ける等の対応を行い、客観的に評価を行うこと。

6.6 ライフサイクルの技術的管理

認証局 のハードウェア及びソフトウェアは、適切なサイクルで最新のセキュリティテクノロジを導入すべく、随時 CPS の見直し及びセキュリティチェックを行う。

6.6.1 システム開発管理

JIS Q 27002:2006「第 12 章 情報システムの取得、開発及び保守」と同等以上の規格に従うものとする。

6.6.2 セキュリティ運用管理

JIS Q 27002:2006「第 12 章 情報システムの取得、開発及び保守」、「第 13 章 情報セキュリティインシデントの管理」、「第 14 章 業務継続管理」と同等以上の規格に従うものとする。

6.6.3 ライフサイクルのセキュリティ管理

規定しない。

6.7 ネットワークのセキュリティ管理

JIS Q 27002:2006 と同等以上の規格に従うものとする。

例えば、JIS Q 27002:2006 の「第 10 章 通信及び運用管理 10.6 ネットワークセキュリティの管理」、「第 11 章 アクセス制御 11.4 ネットワークのアクセス制御」等がこれに相当する。

6.8 タイムスタンプ

認証設備は、アプリケーション等において正確な日付・時刻を使用することとする。例えば、NTP サービスや GPS、電波時計等による時刻同期が挙げられる。

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CP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、基本領域のプロファイルを表7.1.1に示し、拡張領域のプロファイルを表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。

subjectDirectoryAttributes 拡張で用いる保健医療福祉分野の属性（hcRole）については7.1.10で定める。

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)
sha256WithRSAEncryption (1.2.840.113549.1.1.11)
sha384WithRSAEncryption (1.2.840.113549.1.1.12)
sha512WithRSAEncryption (1.2.840.113549.1.1.13)

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 名称の形式

IssureとSubjectの名前の形式は表7.1.1に示される。

7.1.5 名称制約

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-*-forAuthentication-forOrganization」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、SerialNumber は Printable、それ以外は UTF-8 で記述する）
CountryName	◎	c=JP（固定）とする。
LocalityName	△	都道府県名を記載する。
OrganizationName	○	加入者となる医療機関等が運営団体に所属している場合は必須。その場合は所属する運営団体の名称運営団体名をローマ字あるいは英語名で OrganizationName に記載し、OrganizatioUnitName に医療福祉機関の種類を格納する。
OrganizationUnitName	○	
CommonName	◎	医療機関名称を UTF-8 でローマ字あるいは英語名で記載する。
GivenName	×	
SurName	×	
e-Mail	×	
SerialNumber	△	保険医療機関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 7.1.2　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	△	UTF-8 で日本語表記。	FALSE
issuerAltName	△		FALSE
subjectDirectoryAttributes	△		FALSE
AttrType	△		-
AttrValues	△		-
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

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。

7.1.10 保健医療福祉分野の属性（hcRole）

(1) サブジェクトディレクトリ属性拡張での hcRole 属性の使用

本ポリシでは、ISO IS 17090 で規定した hcRole 属性を下記に示すようにプロファイルして用いることにする。

subjectDirectoryAttributes の attrType には hcRole を表す OID {id-hcpki-at-healthcareactor} を設定する。

attrValue は HCActorData で、HCActor の codedData では codeValueData は用いず、codeDataFreeText を用いる。

本ポリシでは coding scheme reference の OID として ISO coding scheme reference を用いず、本 CP の元で定めた表 7.1.3 の組織名を参照する local coding scheme reference の OID は、{ iso(1) member-body(2) jp(392) mhlw(100495) jhpki(1) hcRole(6) national-coding-scheme-reference(1) version(1) }を用いる。組織名は、表 7.1.3 に示すように英語表記を用い UTF8string で設定する。

subject が複数の組織を有する場合、HCActorData に複数の HCActor を設定することはできない。

本拡張は、加入者が保険医療機関等の組織の場合に設定することができる。

表 7.1.3 HPKI 組織名テーブル（codeDataFreeText の定義）

組織名	説明
'insurance medical care facility'	保険医療機関
'insurance pharmacy'	保険薬局

注）組織名のワード間の空白は一個の Space (x20)とする。

(2) HPKI hcRole 属性プロファイル

本 HPKI の CP では、ISO TS 17090 に定められた hcRole 属性の ASN.1 表記を以下のようにプロファイルする。

```
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:
   id-hcpki OBJECT IDENTIFIER :: = {iso (1) standard (0) hcpki (17090)}
   id-hcpki-at OBJECT IDENTIFIER :: = {id-hcpki 0 }
   id-hcpki-at-healthcareactor OBJECT IDENTIFIER :: = {id-hcpki-at 1}
   id-hcpki-cd OBJECT IDENTIFIER :: = {id-hcpki 1}
-- Following values are defined in Japanese HPKI CP:
   id-jhpki OBJECT IDENTIFIER :: =
                    {iso(1) member-body(2) jp(392) mhlw(100495) jhpki(1)}
   id-jhpki-cdata OBJECT IDENTIFIER :: = { id-jhpki 6 1 1 }

-- Definition of data types:
HCActorData :: = SET OF HCActor

HCActor :: = SEQUENCE {
   codedData [0] CodedData,
   regionalHCActorData [1] SEQUENCE OF RegionalData OPTIONAL } -- Note1 (Do not use)

CodedData :: = SET {
   codingSchemeReference [0] OBJECT IDENTIFIER,
   -- Contains the ISO coding scheme Reference
   -- or local coding scheme reference achieving ISO or national registration.
   -- Local coding scheme reference in Japanese HPKI is id-jhpki-cdata (defined above)
   -- In this profile, use this OID: Note 2
   -- At least ONE of the following SHALL be present
   codeDataValue [1] NumericString OPTIONAL, -- Note 3 (Do not use)
   codeDataFreeText [2] DirectoryString } -- Note 4

RegionalData :: = SEQUENCE { } -- Do not define in Japanese HPKI CP
```

Note1： HCActor の regionalHcActorData は、本 CP では使用しない。

Note2： 日本の HPKI CP で定めた local coding scheme reference の OID は、id-jhpki-cdata {iso(1) member-body(2) jp(392) mhlw(100495) jhpki(1) hcRole(6) national-coding-scheme-reference(1) version(1)} とする。この OID は、表 7.1.3 の資格名を参照する。

Note3： 本 CP では CodedData の codeDataValue は用いない。

Note4： 本 CP では、codeDataFreeText としての DirecroryString には表 7.1.3 に規定した 'insurance medical care facility' などの英語表記の施設名を用いる。また、DirecroryString は UTF8String でエンコードしたものを使う。マッチングルールはバイナリーマッチングによる。

＜参考＞

以下に、hcRole を含めた X.509 SubjectDirectoryAttributes 拡張を DER エンコードしたデータの ASN.1 構造をダンプした例を示す。

insurance medical care facility の例

```
No Type Len Value
------------------------------------------------------------------------
  0 30   61: SEQUENCE {-- SubjectDirectoryAttributes ext.extnValue contents
  2 06    3:   OBJECT IDENTIFIER subjectDirectoryAttributes (2 5 29 9)
  7 04   54:   OCTET STRING, encapsulates {
  9 30   52:     SEQUENCE {-- SubjectDirectoryAttributes
 11 30   50:       SEQUENCE {-- Attribute::hcRoleAttribute
 13 06    6:         OBJECT IDENTIFIER '1 0 17090 0 1'   -- OID::type
 21 31   40:         SET {-- SET of AttributeValue::values
 23 31   38:           SET {-- AttributeValue::HCActorData
 25 30   36:             SEQUENCE {-- HCActor
 27 A0   34:               [0] {-- HCActor
 29 31   32:                 SET {-- CodedData
 31 A0   12:                   [0] {-- codingSchemeReference: local coding scheme
 33 06   10:                     OBJECT IDENTIFIER '1 2 392 100495 1 6 1 1'
          :                     }
 45 A2   16:                   [2] {-- codeDataFreeText
 47 0C   14:                     UTF8String 'insurance medical care facility'
          :                     }
          :                 }
          :               }
          :             }
          :           }
          :         }
          :       }
          :     }
          :   }
```

"--"以降はコメント

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。

7.2.2 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	◎	表 7.1.1 の Signature と同様とする。
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。

8 準拠性監査とその他の評価

準拠性監査は、多くの PKI 相互運用性モデルの不可欠なコンポーネントである。本 CP に従って証明書を発行する認証局は、本 CP の要件に完全に従っているということを検証者、加入者及び HPKI 認証局専門家会議が満足する形で確立するものとする。

8.1 監査頻度

認証局の準拠性監査は、1 年以下の間隔で行われるものとする。但し、移管、譲渡、合併など、認証局の構成に大規模な変更があった場合は直ちに監査を実施するものとする。

8.2 監査者の身元・資格

認証局は、認証局業務を直接行っている部門から独立した、適切な能力を有する監査者に定期監査を委託するものとする。

8.3 監査者と被監査者の関係

監査者は、認証局とは別個の組織に属することによって、被監査者から独立しているものとする。監査者は、被監査者と特別な利害関係を持たないものとする。

8.4 監査テーマ

監査は、本 CP 及び関連する CPS の準拠性をカバーする。

8.5 監査指摘事項への対応

認証局は、認証局代表者の指示のもと、監査における指摘事項に対する改善措置を実施する。

8.6 監査結果の通知

監査者によって証明書の信頼性に影響する重大な欠陥が発見された認証局又は登録局は、加入者、検証者及び HPKI 認証局専門家会議に直ちに通知するものとする。

9 その他の業務上及び法務上の事項

9.1 料金

各種の料金については、本 CP に従い運用される認証局が設定するものとし、本 CP では規定しない。

9.1.1 証明書の発行又は更新料

規定しない。

9.1.2 証明書へのアクセス料金

規定しない。

9.1.3 失効又はステータス情報へのアクセス料金

規定しない。

9.1.4 その他のサービスに対する料金

規定しない。

9.1.5 払い戻し指針

規定しない。

9.2 財務上の責任

本 CP に従い運用される認証局は、その継続的な運営に必要とされる十分な財務的基盤を維持しなくてはならない。

9.2.1 保険の適用範囲

規定しない。

9.2.2 その他の資産

規定しない。

9.2.3 エンドエンティティに対する保険又は保証

規定しない。

9.3 業務情報の秘密保護

9.3.1 秘密情報の範囲

本 CP に従う認証局が保持する個人及び組織の情報は、証明書、CRL 、各認証局が定める CPS の一部として明示的に公表されたものを除き、秘密保持対象として扱われる。認証局は、法の定めによる場合及び加入者による事前の承諾を得た場合を除いてこれらの情報を外部に開示しない。

加入者の私有鍵は、その加入者によって秘密保持すべき情報である。認証局では、いかなる場合でもこれらの鍵へのアクセス手段を提供しない。

監査ログに含まれる情報及び監査報告書は、秘密保持対象情報である。認証局は、本 CP 「8.6 監査結果の報告」に記載されている場合及び法の定めによる場合を除いて、これらの情報を外部へ開示しない。

9.3.2 秘密情報の範囲外の情報

証明書及び CRL に含まれている情報は秘密情報として扱わない。

その他、次の情報も秘密情報として扱わない。

- 認証局以外の出所から、秘密保持の制限無しに公知となった情報
- 開示に関して加入者によって承認されている情報

9.3.3 秘密情報を保護する責任

認証局は「9.3.1 秘密情報の範囲」で規定された秘密情報を保護するため、内部及び外部からの情報漏洩に係わる脅威に対して合理的な保護対策を実施する責任を負う。

ただし、認証局が保持する秘密情報を、法の定めによる場合及び加入者による事前の承諾を得た場合に開示することがある。その際、その情報を知り得た者は契約あるいは法的な制約によりその情報を第三者に開示することはできない。にもかかわらず、そのような情報が漏洩した場合、その責は漏洩した者が負う。

9.4 個人情報のプライバシー保護

9.4.1 プライバシーポリシ

認証局における個人情報の取り扱いについては、各認証局の CPS で特定される「プライバシーポリシ」を適用するものとする。

9.4.2 プライバシーとして保護される情報

認証局は、次の情報を保護すべき個人情報として取り扱う。

- 登録局が本人確認や各種審査の目的で収集した情報の中で、証明書に含まれない情報。
  例えば、身分証明書、自宅住所、連絡先の詳細など、他の情報と容易に照合することができ、それにより特定の個人を識別することが可能な情報を指す。
- CRL に含まれない加入者の証明書失効又は停止の理由に関する情報。
- その他、認証局が業務遂行上知り得た加入者の個人情報。

9.4.3 プライバシーとはみなされない情報

次の情報は、秘密情報として扱わない。

- 公開鍵証明書
- CRL に記載された情報

9.4.4 個人情報を保護する責任

認証局は「9.4.2 プライバシーとして保護される情報」で規定された情報を保護するため、内部及び外部からの情報漏洩に係わる脅威に対して合理的な保護対策を実施する責任を負う。

9.4.5 個人情報の使用に関する個人への通知及び同意

認証局は、証明書発行業務及びその他の認証業務の利用目的に限り個人情報を利用する。それ以外の目的で個人情報を利用する場合は、法令で除外されている場合を除き、あらかじめ本人の同意を得るものとする。

9.4.6 司法手続又は行政手続に基づく公開

司法機関、行政機関又はその委託を受けたものの決定、命令、勧告等があった場合は、認証局は情報を開示することができる。

9.4.7 その他の情報開示条件

個人情報を提供した本人又はその代理人から当該本人に関する情報の開示を求められた場合、認証局で別途定める手続きに従って情報を開示する。この場合、複製にかかる実費、通信費用等については、情報開示を求める者の負担とする。

9.5 知的財産権

認証局と加入者との間で別段の合意がなされない限り、認証局が提供するサービスに

関わる情報資料及びデータは、次に示す当事者の権利に属するものとする。

- 加入者証明書：認証局に帰属する財産である
- 加入者の私有鍵：私有鍵は、その保存方法又は保存媒体の所有者に関わらず、公開鍵と対になる私有鍵を所有する加入者に帰属する財産である
- 加入者の公開鍵：保存方法又は保存媒体の所有者に関わらず、対になる私有鍵を所有する加入者に帰属する財産である
- CPS：認証局に帰属する財産（著作権を含む）である
- 本 CP：「HPKI 認証局専門家会議」に帰属する財産（著作権を含む）である

9.6 表明保証

9.6.1 認証局の表明保証

認証局は、その運営にあたり、本 CP 及び認証局の定める CPS に基づいて、加入者及び検証者に対して次の認証局としての責任を果たすものとする。

- 提供するサービスと運用のすべてが、本 CP の要件と認証局の定める CPS に従って行われること。
- 証明書の発行時に、申請者の申請内容の真偽の確認を確実に行うこと。ただし、法令等の要請により証明書を発行する場合は、認証局において申請内容の真偽に関する責は負わない。
- 認証局が証明書を発行する時は、証明書に記載されている情報が本 CP に従って検証されたことを保証すること。
- 公開鍵を含む証明書を加入者に確実に届けること。
- 認証局で定める失効ポリシに従って失効事由が生じた場合は、証明書を確実に失効すること。
- CRL、ARL などの重要事項を認証局の定める方法により、速やかに入手できるようにすること。
- 認証局の定める方法で、CP に基づく加入者の権利と義務を各加入者に通知すること。
- 鍵の危殆化のおそれ、証明書又は鍵の更新、サービスの取り消し、及び紛争解決をするための手続きを加入者に通知すること。
- 本 CP「5　建物及び関連施設、運用のセキュリティ」及び「6　技術的セキュリティ管理」に従い認証局を運営し、私有鍵の危殆化を生じさせないこと。
- CA 私有鍵が、証明書及び証明書失効リストに署名するためだけに使用されることを保証すること。

- 申請者の申請内容の真偽の確認において利用した書類を含む、各種の書類の滅失、改ざんを防止し、10 年間保管すること。
- 認証局の発行する証明書の中で、加入者に対して、加入者の名称（subjectDN）の一意性を検証可能にしておくこと。

9.6.2 登録局の表明保証

登録局は、認証局から独立して登録局を運営する場合、加入者、検証者、認証局に対して次の責任を果たすものとする。また、登録局は、認証局に代わって果たす行為について個別に責任を負う。

- 証明書発行にあたり、申請内容の真偽の確認を確実に行い、確認の結果を認証局に対して保証すること。ただし、法令等の要請により証明書を発行する場合は、登録局において申請内容の真偽に関する責は負わない。
- 認証局の発行する証明書の中で、加入者に対して加入者の名称（subjectDN）の一意性を検証可能にしておくこと。
- 証明書申請情報を認証局に安全に送付し、登録記録を安全に保管すること。
- 証明書失効申請を行う場合は、本 CP「4.9.3　失効申請の処理手順」に従って失効申請を開始すること。
- 将来の検証のため、また証明書がどのように、何故生成されたかを管理可能なように、証明書の作成要求又は失効要求などのイベントを、認証局に移管した場合を除き、証明書の有効期間満了後 10 年間保管すること。

9.6.3 加入者の表明保証

本 CP に則り運営される認証局の加入者は、認証局に対して次の責任を果たすものとする。

1. 証明書発行申請内容に対する責任
   証明書発行申請を行う場合、認証局に提示する申請内容が虚偽なく正確であることに対する責任を果たすこと。

2. 証明書記載事項の担保責任
   証明書の記載内容について証明書の受領時に確認を行い、申請内容と相違ないかを確認すること。また、記載内容について現状との乖離が発生した場合には、速やかに当該証明書の失効手続きを行うこと。

3. 鍵などの管理責任
   私有鍵を保護し、紛失、暴露、改ざん、又は盗用されることを防止するために

妥当な措置を取ること。

4. 各種の届出に対する責任

私有鍵の紛失、暴露、その他の危殆化、又はそれらが疑われる時には、認証局の定める CPS に従って速やかに届け出ること。

また、証明書情報に変更があった場合は、認証局の定める CPS に従って速やかに届け出ること。

5. 利用規定の遵守責任

加入者は、本 CP 及び認証局で加入者に対して開示される文章を読み、その利用規定及び禁止規定を遵守すること。

なお、法令等の要請により証明書が発行された場合は、その責任の範囲は当該法令に定める範囲とする。

9.6.4 検証者の表明保証

本 CP に則り運営される認証局の検証者は以下の責任を果たすものとする。

1. 利用規定の遵守責任

検証者は、本 CP 及び認証局で検証者に対して開示される文章を読み、その利用規定及び禁止規定を遵守すること。また、証明書の利用に際しては信頼点の管理を確実に行うこと。

2. 証明書記載事項の確認責任

検証者は、証明書を利用する際に、その有効性を確認する責任がある。有効性の確認には、以下の事項が含まれる。

- 証明書の署名が正しいこと
- 証明書の有効期限が切れていないこと
- 証明書が失効していないこと
- 証明書の記載事項が、本 CP「7 証明書及び失効リスト及び OCSP のプロファイル」に記述されているプロファイルと合致していること。特に、次の 2 点の検証を実施することは HPKI 認証用証明書として重要である。
  - OID 及び Issuer の CN が HPKI の規定に一致していること
  - hcRole 及び keyUsage の DigitalSignature のみが有効と設定されていること

9.6.5 他の関係者の表明保証

規定しない。

9.7 無保証

認証局は、本 CP 「9.6.1 認証局表明保証」及び「9.6.2 登録局の表明保証」に規定する保証に関連して発生するいかなる間接損害、特別損害、付随的損害又は派生的損害に対する責任を負わず、いかなる逸失利益、データの紛失又はその他の間接的若しくは派生的損害に対する責任を負わない。

また、本 CP「9.16.5 不可抗力」で規定される不可抗力によるサービス停止によって加入者、若しくはその他の第三者において損害が生じた場合、認証局は一切の責任を負わない。

9.8 責任制限

認証局は、加入者において電子証明書の利用又は私有鍵の管理その他加入者が注意すべき事項の運用が不適切であったために生じた損害に対して責任を負わない。

また、認証局及び登録局の責任は、認証局及び登録局の怠慢行為により CP、CPS に定められた運用を行わなかった場合に限定する。

なお、本 CP 「9.6 表明保証」に関し、次の場合、認証局は責任を負わない。

- 認証局に起因しない不法行為、不正使用並びに過失等により発生する一切の損害
- 加入者又は検証者が自己の義務の履行を怠ったために生じた損害
- 加入者又は検証者のシステムに起因して発生した一切の損害
- 加入者又は検証者が使用する端末のソフトウェアの瑕疵、不具合あるいはその他の動作自体によって生じた損害
- 認証局の責に帰することのできない事由で電子証明書及び CRL に公開された情報に起因する損害
- 認証局の責に帰することのできない事由で正常な通信が行われない状態で生じた一切の損害
- 証明書の使用に関して発生する業務又は取引上の債務等、一切の損害
- 現時点の予想を超えた、ハードウェア的あるいはソフトウェア的な暗号アルゴリズム解読技術の向上に起因する損害

9.9 補償

本 CP に規定された責任を果たさなかったことに起因して、認証局がサービスの加入者に対して損害を与えた場合、認証局で定める金額を上限として損害を賠償する。

ただし、認証局側の責に帰さない事由から発生した損害、逸失利益、間接損害、又は予見の有無を問わず、特別損害については、いかなる場合でも一切の責任を負わない。

また、加入者は認証局が発行する証明書を申請した時点で、検証者は信頼した時点で、認証局及び関連する組織等に対する損害賠償責任が発生する。

9.10 本ポリシの有効期間と終了

9.10.1 有効期間

本 CP は、作成された後、「HPKI 認証局専門家会議」により審査、承認されることにより有効になる。また、「9.10.2 終了」で記述する本 CP の終了まで有効であるものとする。

9.10.2 終了

本 CP は、「9.10.3 終了の影響と存続条項」で規定する存続条項を除き、「HPKI 認証局専門家会議」が無効と宣言した時点又は「HPKI 認証局専門家会議」が機能を果たさなくなった場合、無効になる。

9.10.3 終了の影響と存続条項

文書が終了した場合であっても、「9.3 企業情報の秘密保護」、「9.4 個人情報のプライバシー保護」、「9.5 知的財産権」に関する責務は存続するものとする。また、「HPKI 認証局専門家会議」において部分的な存続を定めた場合は、当該存続部分は有効なものとする。

9.11 関係者間の個々の通知と連絡

認証局から加入者への通知方法は、別項で特に定めるものを除き、電子メール、ホームページへの掲載、郵送による書面通知など認証局が適当と判断した方法により行うものとする。また、認証局から加入者の届け出た住所、FAX 番号又は電子メールアドレスに宛てて加入者への通知を発した場合には、当該通知が延着又は不着となった場合であっても、通常到達すべき時に到達したものとみなす。

9.12 改訂

9.12.1 改訂手続き

「HPKI 認証局専門家会議」が本 CP の改訂を行う場合は、改訂に先立ち、本 CP に関連する全ての認証局に通知を行い、意見を求める。

本 CP が変更された時は、「HPKI 認証局専門家会議」によって承認する。

9.12.2 通知方法と期間

本 CP が改訂された場合、情報公開用 Web サイト等を通じて、全ての加入者、関連する認証局及び検証者に速やかに公開する。公開の期間については、次のように定める。

- 重要な変更は、通知後 90 日を上限として、通知に定められた告知期間を経て効力を生ずる。なお、通知後、上記で示した方法に従い通知を行うことにより、変更を中止することもあり得る。但し、監査指摘事項などによる緊急を要する重要な変更は、通知後、直ちに効力を生ずる。
- 重要でない変更は、通知後直ちに効力を生ずる。

9.12.3 オブジェクト識別子（OID）の変更理由

本 CP の変更があった場合には、本 CP のバージョン番号を更新する。また、次の場合には、OID を変更する。

- 証明書又は CRL のプロファイルが変更されたとき
- セキュリティ上重要な変更がされたとき
- 本人性、国家資格の確認方法の厳密さに重要な影響を及ぼす変更がされたとき

9.13 紛争解決手続

証明書の発行主体である、各認証局の CPS において定める。

9.14 準拠法

本 CP は、「電子署名及び認証業務に関する法律」、「個人情報の保護に関する法律」及び関連する日本国内法規に準拠している。

9.15 適用法の遵守

本 CP の運用にあたっては、日本国内法及び公的通知等がある場合はそれを優先する。

9.16 雑則

9.16.1 完全合意条項

本 CP は、本 CP に定められたサービスに対して当事者間の完全合意を構成し、認証業務について記述された書面又は口頭による過去の一切の意思表示、合意又は表明事項に取って代わるものである。

9.16.2 権利譲渡条項

関係者は、本 CP に定める権利義務を担保に供することができない。また、次の場合を除き、第三者に譲渡することができない。

- 認証局が登録局に本 CP に定める業務の委託を行うとき
- 本 CP に則った認証局の移管又は譲渡を行うとき

9.16.3 分離条項

本 CP のひとつ又は複数の条項が司法の判断により、無効であると解釈された場合であっても、その他の条項の有効性には影響を与えない。無効と判断された条項は、法令の範囲内で当事者の合理的な意思を反映した規定に読み替える。

9.16.4 強制執行条項（弁護士費用及び権利放棄）

規定しない。

9.16.5 不可抗力

以下に例示されるような通常人の標準的な注意義務を尽くしても、予防・回避できない事象を不可抗力とする。不可抗力によって損害が発生した場合、本 CP「9.7 無保証」の規定により認証局は免責される。

- 火災、雷、噴火、洪水、地震、嵐、台風、天変地異、自然災害、放射能汚染、有害物質による汚染、又は、その他の自然現象
- 暴動、市民暴動、悪意的損害、破壊行為、内乱、戦争（宣戦布告されているか否かを問わない）又は革命
- 裁判所、政府又は地方機関による作為又は不作為
- ストライキ、工場閉鎖、労働争議
- 認証局の責によらない事由で、本 CP に基づく義務の遂行上必要とする必須の機器、物品、供給物若しくはサービス（電力、ネットワークその他の設備を含むがそれに限らない）が利用不能となった場合

9.17 その他の条項

本 CP を採用した認証局又は登録局が別の組織と合併若しくは別の組織に移管、譲渡する場合、新しい組織は本 CP の方針に同意し責任を持ち続けるものとする。