仮認証主体名：〇〇〇

〇〇〇認証局
運用管理規程（素案）

平成３０年３月３０日

〇〇〇

(C)　××××××

改定履歴

版数	日付	内容
初版	平成　年　月	初版発行

－目次－

1　はじめに

1.1　概要

○○○認証局運用規程（以下、本 CPS と呼ぶ。）は、○○○が運営する「○○○認証局」（以下、本認証局と呼ぶ。）の運用規程を定めるものである。

本認証局が発行する加入者証明書の発行方針及び利用に関する要件は、『保健医療福祉分野 PKI 認証局 認証用（組織）証明書ポリシ』（厚生労働省）に従う。

本認証局は、「○○○認証局　組織認証用証明書」を発行するものである。本認証局が発行した電子証明書は、厚生労働省によって規定された「保健医療福祉分野 PKI 認証局 認証用（組織）証明書ポリシ（以下、HPKI-CP と呼ぶ。）」に基づき、組織とその公開鍵及び資格属性等が一意に関連づけられることを証明する。

なお、本 CPS は以下の文書に依存して構成される。

- IETF/RFC3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework
- ISO/IS 17090-1:2013 Health informatics - Public key infrastructure Part 1：Overview of digital certificate services
- ISO/IS 17090-2:2015 Health informatics - Public key infrastructure Part 2：Certificate profile
- ISO/IS 17090-3:2008 Health informatics - Public key infrastructure Part 3：Policy management of certification authority

また、本 CP は以下の文章を参照する。

- IETF/RFC 4210 Internet X.509 Public Key Infrastructure Certificate Management Protocols（CMP）
- IETF/RFC 6712 Internet X.509 Public Key Infrastructure – HTTP Transfer for the Certificate Management Protocol（CMP）
- IETF/RFC 6960 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP
- IETF/RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile
- IETF/RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile
- US FIPS140-2(Federal Information Processing Standard) ： Security Requirements for Cryptographic Modules

(https://csrc.nist.gov/publications/detail/fips/140/2/final/)

- JIS Q 27002:2014：情報技術－セキュリティ技術－情報セキュリティ管理策の実践のための規範
- 電子署名及び認証業務に関する法律（平成 12 年 5 月 31 日　法律第 102 号、最終改正：平成 26 年 6 月 13 日法律第 69 号）
- 電子署名及び認証業務に関する法律施行規則（平成 13 年 3 月 27 日　総務省・法務省・経済産業省令第 2 号、最終改正：平成 27 年 9 月 8 日総務省・法務省・経済産業省令第 1 号）
- 電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針（平成 13 年 4 月 27 日　総務省・法務省・経済産業省告示第 2 号）

1.2　文書の名前と識別

本ドキュメントの名称を「○○○認証局運用規程」とする。本ドキュメント及び、本認証局の運営主体である○○○及び、発行する証明書のオブジェクト識別子を以下の通りとする。

表 1.1　本 CPS で定める OID

名称	オブジェクト識別子
○○○	
○○○認証局	
○○○運用規程	
組織認証用証明書	1.2.392.100495.1.5.1.3.3.1
組織認証用テスト証明書	1.2.392.100495.1.5.1.3.0.1

1.3　PKI の関係者

1.3.1　認証局

認証局（CA）は、発行局（IA）と登録局（RA）をその構成要素とし、○○○により運営される。但し、本 CPS の遵守及び個人情報の厳正な取扱いを条件に、契約等を取り交わすことで認証業務の一部を外部委託することができる。

1.3.2　発行局

発行局は、登録局からの電子証明書発行、失効の要請を受け、電子証明書の発行、失効の業務を行う。また、同時に証明書失効リスト（以下、CRL と呼ぶ。）を作成、発行

する。なお、本 CPS の遵守及び個人情報の厳正な取扱いを条件に、契約等を取り交わすことで発行局業務の一部又は全部を外部委託することができる。

1.3.2　登録局

登録局は、電子証明書発行申請者からの電子証明書の発行、失効の申請受付窓口の業務を行う。また、各種業務において、適切な組織の実在性、有資格性、申請者への電子証明書の交付を行うものとする。

なお、本 CPS の遵守及び個人情報の厳正な取扱いを条件に、契約等を取り交わすことで発行局業務の一部又は全部を外部委託することができる。

1.3.3　加入者

加入者とは、証明書所有者である。証明書所有者とは、証明書発行申請を行い本認証局により証明書を発行される組織をさす。証明書所有者の範囲は次のとおりとする。

- 医療機関等の保健医療福祉分野サービスの提供者及び利用者

具体的には以下の組織を対象とする。

- 保険医療機関
- 保険薬局
- 介護事業者
- 地域医療情報連携ネットワークの事業主体
- 医療情報共有サービスを提供する民間事業者

※以下、地域医療情報連携ネットワークの事業主体と医療情報共有サービスを提供する民間事業者をまとめて「その他組織」と呼ぶ。

1.3.4　検証者

デジタル署名を公開鍵証明書の公開鍵で検証する者。

1.3.5　その他の関係者

規定しない。

1.4　証明書の使用方法

1.4.1　適切な証明書の使用

本 CPS で定める加入者証明書は、証明書の用途に応じてネットワーク認証、クライア

ント認証、Web サーバ認証の用途で使用できる。証明書の種類とその用途の対応は下記のとおりとする。本 CPS では以降特別に断りがない限り 3 種類の証明書を総称して「加入者証明書」という。

本 CPS で定める加入者証明書は、次に定める利用目的にのみ使用できる。

（1） ネットワーク用証明書：ネットワーク認証用

（2） クライアント用証明書：クライアント認証用

（3） Web サーバ用証明書：Web サーバ認証用

1.4.2 禁止される証明書の使用

本認証局で発行される加入者証明書は、本 CPS「1.4.1 適切な証明書の使用」に規定する用途のみに使用するものとする。加入者証明書が用途以外の目的で使用された場合は、本認証局は一切の責任を負わないものとする。

1.5 ポリシ管理

1.5.1 本ポリシを管理する組織

本 CPS の管理組織は、○○○とする。

1.5.2 問い合わせ先

本 CPS に関する問い合わせ先を以下のように定める。

【問い合わせ先】

窓口：○○○

受付時間：××時～××時（平日）

電話番号：××-××××-××××

FAX 番号：××-××××-××××

e-mail アドレス：××@××

1.5.3 CPS のポリシ適合性を決定する者

本 CPS の HPKI-CP への適合性を決定する者は、HPKI 認証局専門家会議とする。

1.5.4 CPS 承認手続き

本 CPS は、認証局代表者が承認する。

1.6 定義と略語

（あ～ん）

・ アーカイブ（Archive）
電子証明書の発行・失効に関わる記録や、認証局のシステム運用に関わる記録等を保管すること。

・ 暗号アルゴリズム（Algorithm）
暗号化／復号には、対になる 2 つの鍵を使う公開鍵暗号と、どちらにも同じ鍵を用いる共通鍵暗号（私有鍵暗号）がある。前者には RSA、ElGamal 暗号、楕円曲線暗号などがあり、後者には米国政府標準の DES や近年新しく DES の後継として決まった AES などがある。

・ 暗号モジュール（Security Module）
私有鍵や証明書等を安全に保管し、鍵ペア生成や署名等の暗号操作を行うハードウェア又はソフトウェアのモジュール。

・エンドエンティティ（EndEntity）
証明書の発行対象者の総称。公開鍵ペアを所有している実体（エンティティ）で、公開鍵証明書を利用するもの。（個人、組織、デバイス、アプリケーションなど）
なお、認証局はエンドエンティティには含まれない。

・ オブジェクト識別子（Object Identifier）
オブジェクトの識別を行うため、オブジェクトに関連付けられた一意な値。

・ 活性化（Activate）
鍵を署名などの運用に使用することができる状態にすること。逆に、使用できなくすることを非活性化という。

・ 鍵長（Key Length）
鍵データのサイズ。鍵アルゴリズムに依存する。暗号鍵の強度は一般に鍵の長さによって決まる。鍵長は長ければ長いほど解読困難になるが、署名や暗号メッセージを作成する際の時間もかかるようになる。情報の価値を見計らって適切な鍵長を選択する必要がある。

・ 鍵の預託（Key Escrow）
第三者機関に鍵を預託すること。

・ 鍵ペア（Key Pair）

私有鍵とそれに対応する公開鍵の対。

- 加入者（Subscriber）
  認証局から認証のための電子証明書を発行される者。

- 加入者証明書
  認証局から加入者に対して発行された公開鍵証明書のこと。

- 危殆化（Compromise）
  私有鍵等の秘密情報が盗難、紛失、漏洩等によって、その秘密性を失うこと。

- 検証者（Relying Party）
  検証者とは、デジタル署名を公開鍵証明書の公開鍵で検証するモノを指す。

- 公開鍵（Public Key）
  私有鍵と対になる鍵で、デジタル署名の検証に用いる。

- 公開鍵証明書（Public Key Certificate）
  加入者の名義と公開鍵を結合して公開鍵の真正性を証明する証明書で、印鑑証明書に相当する。電子証明書あるいは単に証明書ともいう。公開鍵証明書には、公開鍵の加入者情報、公開鍵、CA の情報、その他証明書の利用規則等が記載され、CA の署名が付される。

- 自己署名証明書（Self Signed Certificate）
  認証局が自身のために発行する電子証明書。発行者名と加入者名が同じである。

- 失効（Revocation）
  有効期限前に、何らかの理由（盗難・紛失など）により電子証明書を無効にすること。基本的には、本人からの申告によるが、緊急時には CA の判断で失効されることもある。

- 私有鍵（Private Key）
  公開鍵と対になる鍵。公開せず、他人に漏れないように鍵の所有者だけが管理する。私有鍵で署名したものは、それに対応する公開鍵でのみ検証が可能である。

- 証明書失効リスト（Certificate Revocation List、Authority Revocation List）

失効した電子証明書のリスト。
エンドエンティティの証明書の失効リストを CRL といい、CA の証明書の失効リストを ARL という。

- 証明書発行要求（Certificate Signing Request）
  申請者から認証局に電子証明書発行を求めるための要求。電子証明書を作成するための元となる情報で、その内容には、申請者の所在地、サーバアドレス、公開鍵などの情報が含まれる。

- 証明書ポリシ（Certificate Policy：CP）
  共通のセキュリティ要件を満たし、特定のコミュニティ及び／又はアプリケーションのクラスへの適用性を指定する、名前付けされた規定の集合。

- 申請者
  認証局に電子証明書の発行を申請する主体のこと。

- 電子署名（Electronic Signature）
  電子文書の正当性を保証するために付けられる署名情報。公開鍵暗号などを利用し、相手が本人であることを確認するとともに、情報が送信途中に改ざんされていないことを証明することができる。公開鍵暗号方式を用いて生成した署名はデジタル署名ともいう。

- 登録局（Registration Authority：RA）
  電子証明書発行の申請者の本人を審査・確認し、主として登録業務を行う機関。登録局は、認証局の機能のうち、一部の業務を行う。認証する加入者の識別と本人性認証に責任を負うが、電子証明書に署名したり、発行したりはしない。

- 認証局（Certification Authority：CA）
  電子証明書を発行する機関。認証局は、公開鍵が間違いなく本人のものであると証明可能にする第三者機関で、公正、中立な立場にあり信頼できなければならない。

- 認証実施規程（Certification Practice Statement：CPS）
  証明書ポリシに基づいた認証局運用についての規定集。認証局が電子証明書を発行するときに採用する実践に関する表明として位置付けられる。

- 登録設備室

認証業務用設備のうち、登録業務用設備のみが設置された室をいう。登録業務用設備とは、加入者の登録用端末や、加入者が初めて証明書をダウンロードする際に１度限り使用されるＩＤ、パスワード等を識別する為に用いる設備をいう。

・ 認証設備室
認証業務用設備（電子証明書の作成又は管理に用いる電子計算機その他の設備）が設置された室をいう。ただし、登録業務用設備のみが設置される場合を除く。

・ 発行局（Issuer Authority）
電子証明書の作成・発行を主として発行業務を行う機関。発行局は、認証局の機能のうち、一部の業務を行う。

・ ハッシュ関数（Hash Function）
任意の長さのデータから固定長のランダムな値を生成する計算方法。生成した値は「ハッシュ値」と呼ばれる。ハッシュ値は、ハッシュ値から元のデータを逆算できない一方向性と、異なる 2 つのデータから同一のハッシュ値が生成される衝突性が困難であるという性質を持つ。この性質からデータを送受信する際に、送信側の生成したハッシュ値と受信側でデータのハッシュ値を求めて両者を比較し両者が一致すれば、データが通信途中で改ざんされていないことが確認できる。

・ プロファイル（Profile）
電子証明書や証明書失効リストに記載する事項及び拡張領域の利用方法を定めたもの。

・ リポジトリ（Repository）
電子証明書及び証明書失効リストを格納し公開するデータベース。

・ リンク証明書
CA 鍵を更新する際に、新しい自己署名証明書（NewWithNew）と古い世代の CA 鍵と新しい世代の CA 鍵を紐付けるために発行される電子証明書。リンク証明書によって、世代の異なる CA から電子証明書を発行された加入者間での証明書検証が可能となる。
リンク証明書には、新しい公開鍵に古い私有鍵で署名した証明書（NewWithOld）と、古い公開鍵に新しい私有鍵で署名した証明書（OldWithNew）がある。

・ ルート CA（Root CA）

階層型の認証構造において、階層の最上位に位置する認証局のこと。下位に属する認証局の公開鍵証明書の発行、失効を管理する。

（A～Z）

- ARL （Authority Revocation List）
  認証局の証明書の失効リスト、証明書失効リストを参照のこと。

- CA（Certification Authority）
  認証局を参照のこと。

- CA 証明書
  認証局に対して発行された電子証明書。

- CP（Certificate Policy）
  証明書ポリシを参照のこと。

- CPS（Certification Practice Statement）
  認証実施規程を参照のこと。

- CRL（Certificate Revocation List）
  エンドエンティティの証明書の失効リスト、証明書失効リストを参照のこと。

- CRL 検証
  証明書失効情報が、認証局が発行する CRL に記載されているかを確認すること。

- CSR（Certificate Signing Request）
  証明書発行要求を参照のこと。

- DN（Distinguished Name）
  X.500 規格において定められた識別名。X.500 規格で識別子を決定することによって、加入者の一意性を保障する。

- FIPS 140-2（Federal Information Processing Standard）
  FIPS とは米国連邦情報処理標準で、FIPS140-2 は暗号モジュールが満たすべきセキュリティ要件を規定したもの。各セキュリティ要件に対して 4 段階のセキュリティレベル（最低レベル 1～最高レベル 4）を定めている。

・ IA（Issuer Authority）
発行局を参照のこと。

・ OID（Object ID）
オブジェクト識別子を参照のこと。

・ PKI（Public Key Infrastructure）
公開鍵基盤。公開鍵暗号化方式という暗号技術を基に認証局が公開鍵証明書を発行し、この証明書を用いて署名／署名検証、暗号／復号、認証を可能にする仕組み。

・ RA（Registration Authority）
登録局を参照のこと。

・ RSA
公開鍵暗号方式の一つ。Rivest、Shamir、Adleman の 3 名によって開発され、その名前をとって名付けられた。巨大な整数の素因数分解の困難さを利用したもので、公開鍵暗号の標準として普及している。

・ SHA（Secure Hash Algorithm）
ハッシュ関数の一群。SHA-1 や SHA-2 等があり、任意の長さのデータから 160bit や 256bit 等一定の長さのハッシュ値を作成する。

・ X.500
ITU-T/ISO が定めたディレクトリサービスに関する国際基準。

・ X.509
ITU-T/ISO が定めた電子証明書及び証明書失効リストに関する国際標準。X.509v3 では、電子証明書に拡張領域を設けて、電子証明書の発行者が独自の情報を追加することができる。

2　公開及びリポジトリの責任

2.1　リポジトリ

リポジトリは認証局の証明書と失効情報及び加入者の失効情報を保持する。
リポジトリ及び情報公開用 Web サイトの URL を以下に記載する。

＜リポジトリ＞
http://×××/××.crl

＜情報公開用 Web サイト＞
http://×××/

2.2　証明書情報の公開

本認証局は、以下の情報を公開する。

＜リポジトリで公開する情報＞
- 本認証局の CRL

＜情報公開用 Web サイトで公開する情報＞
- 本 CPS
- 利用規約
- 個人情報保護方針
- 本認証局の CA 証明書
- その他、本認証局が運営基準とする各種規程

2.3　公開の時期又はその頻度

本認証局は、本認証局に関する情報が変更された時点で、その情報を速やかに公開するものとする。証明書失効についての情報は、本 CP「4.9　証明書の失効と一時停止」に従うものとする。

2.4　リポジトリへのアクセス管理

本認証局が公開する情報は、加入者及び検証者に対しては読み取り専用として公開する。

3　識別及び認証

3.1　名称決定

3.1.1　名称の種類

本 CPS に基づいて発行される証明書に使用されるサブジェクト名は加入者名とする。

加入者名は X.500 の Distinguished Name を使用する。保健医療福祉分野 PKI では、C は JP とする。また CommonName は必須で、加入者の組織名称（英語表記もしくはローマ字表記）を記載する。

3.1.2　名称が意味を持つことの必要性

本 CPS により発行する加入者証明書の相対識別名は、検証者によって理解され、使用されるよう意味のあるものとする。

本認証局にて発行される加入者証明書に記載される加入者情報(subject)の識別名(DN)は、証明書申請時に提出される申請書に記載された内容に基づいて、認証局側で設定する。

証明書に設定されている内容の詳細は、ネットワーク用証明書の「subject」については表 7.1.4、クライアント用証明書の「subject」については表 7.1.6、Web サーバ用証明書の「subject」については表 7.1.8 に示す。

3.1.3　加入者の匿名性又は仮名性

規定しない。

3.1.4　種々の名称形式を解釈するための規則

名称を解釈するための規則は、本 CP「7　証明書及び失効リスト及び OCSP のプロファイル」に従う。

3.1.5　名称の一意性

本認証局が発行する電子証明書の加入者名（subjectDN）は、本認証局内で一意にするために、本認証局にて採番するユニーク ID を「OrganizationUnitName（OU）」に設定する。また、本認証局の名称（issuerDN）は、保健医療福祉分野 PKI 内で、一意に指し示すものである。

3.1.6　認識、認証及び商標の役割

商標使用の権利は、商標所持者が全ての権利を保有するものとする。本認証局は、商標について、確認及び認証を行わない。

3.2　初回の本人性確認

3.2.1　私有鍵の所持を証明する方法

本認証局は、証明書種別に応じて以下の方法で加入者私有鍵の所持確認を行う。

ネットワーク用証明書とクライアント用証明書については、加入者公開鍵と加入者私有鍵を認証局で生成し、その加入者公開鍵を含み、加入者公開鍵に対応する加入者私有鍵の所有を証明する加入者証明書を生成する。生成された加入者証明書と加入者私有鍵（以下、加入者証明書と加入者私有鍵を合わせて、「加入者鍵ペア」と呼ぶ。）と加入者鍵ペアの活性化に使用する PIN を、加入者本人に送付する場合は、書留郵便にて郵送し私有鍵の所有を確認するものとする。

加入者鍵ペアと活性化に使用する PIN を別送する場合は、活性化に使用する PIN を加入者宛てに書留郵便にて郵送し、加入者鍵ペアは加入者が指定する送付先に書留郵便にて送付する。この場合、加入者鍵ペアの活性化 PIN を加入者本人のみ保持させることをもって私有鍵の所有を確認するものとする。

Web サーバ用証明書については、申請者が加入者公開鍵と加入者私有鍵を生成し、申請者が提出した証明書発行要求（CSR）の署名検証等により、私有鍵の所有を確認するものとする。

3.2.2　組織の認証

本認証局に加入者証明書の申請を行う組織は、加入者証明書の発行に先立ち、次のいずれかの方法で組織の実在性及び保険医療機関等であることの有資格性を登録局に立証しなくてはならない。

本認証局は、加入者証明書の発行日から約 2 年おきに、その他組織に対して、実在性及び有資格性の確認書類の再提出を求めるものとする。その際、実在性及び有資格性の確認ができない場合は、当該加入者証明書を失効することができる。

なお、申請者個人の認証は「3.2.3　個人の認証」に定める方法による。

＜保険医療機関、保険薬局、介護事業者の場合＞

保険医療機関等の指定を受けた際に地方厚生局、都道府県、市町村から発行された指定通知書（有効期間内）のコピーを提出することによって組織の実在性を立証する。

なお、指定通知書のコピーを提出した場合は、実在性及び保険医療機関等であることの有資格性の立証が同時になされたものとする。

また、これらの立証の際に用いる各種書類には、申請時点において組織の開設者である者の氏名が記載されていなくてはならない。

・ 電子証明書を用いる場合

保健医療福祉分野 PKI 認証局が発行する管理者向け電子署名用証明書を用いた電子署名もしくは商業登記認証局の発行する電子証明書を用いた電子署名により、実在性を立証することができる。

この場合、保健医療福祉分野 PKI 認証局が発行する管理者向け電子署名用証明書による電子署名を用いる場合は、同時に保険医療機関等であることの立証がなされたとみなすが、商業登記認証局の発行する電子証明書を用いる場合は、別途、指定通知書のコピーを提出しなくてはならない。

・ 法令等の要請により発行する場合

保健医療福祉分野 PKI 認証局が法令等の要請により、保険医療機関等の組織の証明書を発行する際は、法令で定められた機関が保険医療機関等の確認を実施し、その結果を登録局に提示することで組織の認証を実施しなくてはならない。

＜その他組織の場合＞

・ 法人組織の場合

登記事項証明書（発行日から 3 ヶ月以内）を提出することによって組織の実在性を立証する。なお、所属する組織によって商業登記を本部組織でのみ行い、登記事象証明書が本部組織のみを証明している場合においては、本部組織の代表者が地方組織の名称を確認の上、認証局が指定する申込書に押印し認証局に提示することにより地方組織の実在性を立証する。また、別途認証局が指定する方法により有資格性の立証をする。

また、三省 4 ガイドライン※2 の適合性について、第三者機関による調査を受けて得た認定又は一般財団法人保健医療福祉情報安全管理適合性評価協会（以下、HISPRO と呼ぶ。）の適合性評価の結果を提出することによって、有資格性を立証する。

※2
厚生労働省
・医療情報システムの安全管理に関するガイドライン
総務省
・ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン
・ASP・SaaS における情報セキュリティ対策ガイドライン
経済産業省
・医療情報を受託管理する情報処理事業者向けガイドライン

・ 個人事業者の場合

青色申告書のコピー、白色申告書のコピーや個人事業の開廃業等届出書のコピー等の組織情報を証明する書類（別紙 1）を提出することによって組織の実在性を立証する。

また、三省 4 ガイドライン※2 の適合性について、第三者機関による調査を受けて得た認定又は HISPRO の適合性評価の結果を提出することによって、有資格性を立証する。

・ 中央官庁/地方公共団体の運営する組織の場合

登記がある場合は、登記事項証明書と本認証局の定める書類に公印規則に定められた公印を捺印したものを提出することによって実在性を立証する。登記がなく職員録や官報、国税庁法人番号公表サイトでも確認出来ない場合は、厚生局発行の公法人証明書を提出することにより実在性を立証する。

また、三省 4 ガイドライン※2 の適合性について、第三者機関による調査を受けて得た認定又は HISPRO の適合性評価の結果を提出することによって、有資格性を立証する。

なお、立証の際に提出する書類には、申請時点において組織の代表者である者の氏名を記載しなくてはならない。

・ 電子証明書を用いる場合

商業登記認証局の発行する電子証明書を用いた電子署名により、法人組織の実在性を立証することができる。

・ 法令等の要請により発行する場合

保健医療福祉分野 PKI 認証局が法令等の要請により、その他組織の証明書を発行する際は、法令で定められた機関がその他組織の実在性及び有資格性の確認を実施し、その結果を登録局に提示することで組織の認証を実施しなくてはならない。

3.2.3 個人の認証

本認証局に加入者証明書を申請しようとする際は、加入者証明書の発行に先立ち、次のいずれかの方法で、組織の開設者もしくは代表者（以下、開設者と代表者を区別しない場合は総称して「管理者」と呼ぶ。）の実在性並びに申請者の実在性、組織所属の事実、組織の証明書申請意思を登録局に立証しなくてはならない。また、組織から委任を受けた者（以下、代理人）が申請する場合は、組織所属の事実に代えて組織からの申請委任の事実を登録局に立証しなくてはならない。立証に用いる書類については、有効期間外のものや、資格喪失後のものを用いてはならない。

なお、本節の定めは証明書申請者の立証に関わる定めであり、登録局が証明書を発行

する場合は、本節の規定に従い申請者の立証を行わせ、4 章の規定に則り申請者の審査及び証明書の発行を実施する。

・ 組織管理者もしくは組織所属者が申請する場合

＜持参の場合＞

1. 組織管理者の実在性

加入者証明書を申請しようとする者は、本認証局の定める申請書類に組織管理者の氏名を記入し、「3.2.2　組織の認証」において、立証書類に組織管理者の氏名が記載されている書類を提出することで、組織管理者の実在性の立証に代えることができる。

2. 申請者の実在性

加入者証明書を申請しようとする者は、本認証局の定める申請書類に、「申請者個人の氏名、所属組織の住所、所属組織の電話番号」を記入し、登録局の窓口に提出することで実在性の立証をしなくてはならない。

3. 申請者の組織所属の事実

加入者証明書を申請しようとする者は、当該組織の管理者の印が押印されている申請者の氏名が記載された申請書類を登録局の窓口に提出することで組織に所属していることの事実を立証しなくてはならない。

4. 組織の証明書申請の意思

申請者が登録局の窓口に各種の書類を持参して申請する場合は、組織管理者の実在性、申請者の実在性及び組織所属の事実の立証を行えば、申請意思の立証がなされたものとみなす。

＜郵送の場合＞

1. 組織管理者の実在性

加入者証明書を申請しようとする者は、本認証局の定める申請書類に組織管理者の氏名を記入し、「3.2.2　組織の認証」において、立証書類に組織管理者の氏名が記載されている書類を提出することで、組織管理者の実在性の立証に代えることができる。

2. 申請者の実在性

加入者証明書を申請しようとする者は、本認証局の定める申請書類に、「申請者個人の氏名、所属組織の住所、所属組織の電話番号」を記入し、登録局に郵送

することで実在性の立証をしなくてはならない。

3. 申請者の組織所属の事実

加入者証明書を申請しようとする者は、当該組織の管理者の印が押印されている申請者の氏名が記載された各認証局で定める申請書類を登録局に郵送することで組織に所属していることの事実を立証しなくてはならない。

4. 組織の証明書申請の意思

申請者が「3.2.2　組織の認証」で定める各種の書類と合わせて、本認証局で定める申請書類に当該組織の管理者の印が押印されている書類を郵送することにより、申請意思の立証がなされたものとみなす。

＜オンラインの場合＞

1. 組織管理者の実在性

「3.2.2　組織の認証」に定める、保健医療福祉分野 PKI 認証局が発行する管理者向け電子署名用証明書を用いた電子署名もしくは商業登記認証局の発行する電子証明書を用いた電子署名により、組織管理者の実在性の立証に代えることができる。

ただし、保健医療機関、保健薬局、介護事業者について、保健医療福祉分野 PKI 認証局が発行する管理者向け電子署名用証明書による電子署名以外を用いる場合は、別途、保険医療機関等であることを立証する書類を提出しなくてはならない。

2. 申請者の実在性、組織所属の事実、組織の証明書申請の意思

加入者証明書を申請しようとする者は、認証局の定める手続きに従い、保健医療福祉分野 PKI 認証局の発行する管理者向け署名用証明書を用いた電子署名により、申請者の実在性、組織所属の事実及び組織の証明書申請の意思を立証しなくてはならない。

なお、保健医療福祉分野 PKI 認証局の管理者向け署名用証明書は組織の管理責任者に発行され、当該証明書による電子署名は、本人にしか実行できないことから、電子署名の提供によりこれらの意思を立証したものとみなす。

・ 代理人が申請する場合

＜持参の場合＞

1. 組織管理者の実在性

加入者証明書を申請しようとする者は、本認証局の定める申請書類に組織管理

者の氏名を記入し、「3.2.2　組織の認証」において、立証書類に組織管理者の氏名が記載されている書類を提出することで、組織管理者の実在性の立証に代えることができる。

2. 代理人の実在性

代理人が加入者証明書を申請しようとする際は、本認証局が定める申請書類に、代理人の「氏名、生年月日、性別、住所、連絡先電話番号」が記入された書類を提出することと併せて「3.代理人の本人性」に掲げる書類の原本を登録局の窓口に提示することで実在性の立証をしなくてはならない。

3. 代理人の本人性

代理人が証明書を申請しようとする際は、次に挙げる書類の原本を登録局の窓口に提示することで代理人の本人性の立証をしなくてはならない。

【1 点で確認できる書類】

・日本国旅券	・電気工事士免状
・運転免許証	・宅地建物取引主任者証
・住民基本台帳カード（写真付のもの）	・無線従事者免許証
・マイナンバーカード（個人番号カード）	・猟銃/空気銃所持許可証
・戦傷病者手帳	・官公庁職員身分証明書（張り替え防止措置済みの写真付）
・海技免状	
・船員手帳	

【2 点提出が必要な書類】

A 欄から 2 点、又は A 欄と B 欄から各 1 点ずつ提出しなくてはならない。

A	・健康保険証	・国民年金手帳（証書）
	・国民健康保険証	・厚生年金手帳（証書）
	・共済組合員証	・共済年金証書
	・船員保険証	・恩給証書
	・介護保険証	・印鑑登録証明書
	・基礎年金番号通知書	

B	・学生証（張り替え防止措置済みの写真付のもの）
	・会社の身分証明書（通行証等は不可、張り替え防止措置済みの写真付のもの）
	・市県民税の納税証明書又は非課税証明書

	（いずれも最新年で 6 ヶ月以内の発行のもの） ・身体障害者手帳 ・源泉徴収票（最新年のもの）

4. 代理人の組織管理者からの委任の事実

代理人が加入者証明書を申請しようとする際は、当該組織管理者の署名捺印のある代理人の氏名が記載された委任状を登録局の窓口に提出することで組織管理者からの委任の事実を立証しなくてはならない。

5. 組織の証明書申請の意思

代理人が登録局の窓口に 1 から 4 で定める各種の書類を持参して申請する場合は、組織の申請意思の立証がなされたものとみなす。

＜郵送の場合＞

代理人による郵送での申請は認めない。

＜オンラインの場合＞

オンラインによる代理人のからの申請は認めない。

・ 法令等の要請により証明書を発行する場合

法令等の要請により、加入者証明書を発行する際は、「3.2.2　組織の認証」の定めに従い組織の認証のみ行い、個人の認証は実施しない。

3.2.4　確認しない加入者の情報

認めない。

3.2.5　機関の正当性確認

規定しない。

3.2.6　相互運用の基準

規定しない。

3.3　鍵更新申請時の本人性確認及び認証

3.3.1　通常の鍵更新時の本人性確認及び認証

本認証局は、利用者証明書の有効期限切れが近づいた時期に、その旨を通知する。利

用者は、その後、利用申込みを行うものとする。この場合、利用者証明書の利用申込みに関する本人性確認は、新規発行時と同様とし、本規程「3.2　初回の本人性確認」の規定に従い行う。

3.3.2　証明書失効後の鍵更新の本人性確認及び認証

初回の証明書発行と同様の手順により申請するものとする。

3.4　失効申請時の本人性確認及び認証

加入者が認証局に失効申請を行うときには、加入者所属の組織からの申請であることの確認を行う。

失効申請書には、発行申請時と同じ組織の組織等管理者が印を押印するとともに、失効する加入者証明書情報及び失効理由を記載する。代理人が失効申請する場合は、当該組織等責任者の委任状の提出を求める。

4　証明書のライフサイクルに対する運用上の要件

4.1　証明書申請

4.1.1　証明書の申請者

(1)　保険医療機関、保険薬局、介護事業者からの申請により発行する場合

加入者証明書の申請者は、保険医療機関等の組織開設者もしくは当該組織所属者もしくは保険医療機関等の組織管理者から委任を受けた代理人とする。

(2)　その他組織からの申請により発行する場合

加入者証明書の申請者は、当該組織の代表者もしくは当該組織所属者もしくは組織代表者から委任を受けた代理人とする。

(3)　法令等の要請により発行する場合

加入者証明書の申請者は、法令等で定められた組織とする。

本認証局は、それ以外からの申請は受け付けない。

4.1.2　申請手続及び責任

加入者証明書の利用を希望する組織は、登録局の申込窓口に対して加入さ証明書の利用申込みを行う。加入者証明書の利用申込みの詳細については、以下のURLに掲載する。加入者証明書の利用を希望する者は、以下の URL に掲載されている本 CPS 及び利用者同意書に、同意しなければならない。

http://×××/

(1)　保険医療機関、保険薬局、介護事業者からの申請により発行する場合

① 持参

保険医療機関等の組織開設者もしくは当該組織所属者もしくは代理人が登録局に「3.2.2　組織の認証」、「3.2.3　個人の認証」及び本認証局の定める書類を持参することにより利用申請を行う。

なお、代理人による申請の場合は、加入者証明書の利用申請に必要な書類に加え、保険医療機関等の組織開設者による委任状及び本 CP「3.2.3 個人の認証」の代理人が申請する場合に定める代理人の本人性を確認可能な書類も同時に提出するものとする。

② 郵送

保険医療機関等の組織開設者もしくは当該組織所属者が登録局に「3.2.2　組織の認証」、「3.2.3　個人の認証」及び本認証局が定める書類を郵送することにより利用申請を行う。

なお、代理人による郵送での申請は認めない。

③ オンライン

保険医療機関等の組織開設者が登録局にオンラインで「3.2.2　組織の認証」、「3.2.3 個人の認証」及び本認証局の定めるデータを送付することにより利用申請を行う。

なお、当該組織所属者及び代理人によるオンラインでの申請は認めない。

また、加入者証明書の利用申請者は、申請にあたり、本 CPS 及び利用規約を理解し、本 CPS に同意した上で利用申請を行うものとする。

(2)　その他組織からの申請により発行する場合

① 持参

組織の代表者もしくは当該組織所属者もしくは代理人が登録局に「3.2.2　組織の認証」、「3.2.3　個人の認証」及び認証局の定める書類を持参することにより利用申請を行う。なお、代理人による申請の場合は、証明書の利用申請に必要な書類に加え、組織代表者による委任状及び本 CP「3.2.3 個人の認証」の代理人が申請する場合に定める代理人の本人性を確認可能な書類も同時に提出するものとする。

② 郵送

組織の代表者もしくは当該組織所属者が登録局に「3.2.2　組織の認証」、「3.2.3　個人の認証」及び認証局が定める書類を郵送することにより利用申請を行う。

なお、代理人による郵送での申請は認めない。

③ オンライン

組織の代表者が登録局にオンラインで「3.2.2　組織の認証」、「3.2.3　個人の認証」及び本認証局の定めるデータを送付することにより利用申請を行う。

なお、当該組織所属者及び代理人によるオンラインでの申請は認めない。

(3)　法令等の要請により証明書を発行する場合

法令等で定められた組織が証明書を申請する場合は、認証局に対し以下の手続きによって証明書の発行申請を行う。

①　根拠となる法令等の明示

本認証局に対して、発行申請の根拠となる法令等を明示する。

② 保険医療機関等の認証手段の提示もしくは開示

法令等で定められた組織が実施した、組織の確認結果を登録局に提示する。

4.2 証明書申請手続き

4.2.1 本人性及び資格確認

(1) 保険医療機関、保険薬局、介護事業者からの申請により発行する場合

本認証局は、加入者証明書の発行時、本 CPS「3.2.2 組織の認証」及び「3.2.3 個人の認証」に定める各立証事項に対して、それぞれ以下の方法で真偽の確認を行う。

＜組織開設者もしくは組織所属者からの申請の場合＞

① 持参の場合

申請者から提示された各種の書類について、以下の確認を行う。

- 発行申請書記載の組織名と開設者名が、指定通知書コピー記載の組織名と開設者名と一致しているか確認する。
- 発行申請書に組織開設者の署名もしくは印が押印されているか確認する。
- 申請者が組織開設者でない組織所属者の場合、社員証等で組織所属の確認をする。
- 組織所属の確認が出来ない場合、発行申請書記載の電話番号に電話し、当該組織に申請者が在籍していることを確認する。
- 保健医療機関、保健薬局の場合は、地方厚生局が所管し公開している全保険医療機関・保険薬局一覧等を用いて存在性を確認する。
- 介護事業者の場合は、都道府県または市町村が所管し公開している情報等を用いて存在性を確認する。
- 地方厚生局、都道府県、市町村の公開情報で存在性が確認出来ない場合は、地方厚生局、都道府県、市町村や発行申請書記載の電話番号に電話し、当該組織が存在していることを確認する。

なお、組織が中央官庁・地方公共団体の運営する機関で、当該機関の実在性が明らかな場合は、公印の押された申請書類の提出を求めることで、問い合わせによる確認を省略することができる。

② 郵送の場合

申請者から提示された各種の書類について、以下の確認を行う。

- 発行申請書記載の組織名と開設者名が、指定通知書コピー記載の組織名と開設者名と一致しているか確認する。

・　発行申請書に組織開設者の署名もしくは印が押印されているか確認する。
・　発行申請書記載の電話番号に電話し、申請者が在籍していることを確認する。
・　保健医療機関、保健薬局の場合は、地方厚生局が所管し公開している全保険医療機関・保険薬局一覧等を用いて存在性を確認する。
・　介護事業者の場合は、都道府県または市町村が所管し公開している情報等を用いて存在性を確認する。
・　地方厚生局、都道府県、市町村の公開情報で存在性が確認出来ない場合は、地方厚生局、都道府県、市町村や発行申請書記載の電話番号に電話し、当該組織が存在していることを確認する。

③ オンラインの場合

申請者から提示された申請データについて、以下の確認を行う。

・　申請データに付与されている電子署名データの有効性を確認する。
・　電子署名データの電子証明書 Subject の氏名が、申請データの開設者名と一致しているか確認する。
・　電子署名データの電子証明書 Subject の組織名が、申請データの組織名と一致しているか確認する。
・　申請データの組織名と管理者名が、指定通知書のスキャンデータに記載の組織名と開設者名と一致しているか確認する。
・　保健医療機関、保健薬局の場合は、地方厚生局が所管し公開している全保険医療機関・保険薬局一覧等を用いて存在性を確認する。
・　介護事業者の場合は、都道府県または市町村が所管し公開している情報等を用いて存在性を確認する。
・　地方厚生局、都道府県、市町村の公開情報で存在性が確認出来ない場合は、地方厚生局、都道府県、市町村や発行申請書記載の電話番号に電話し、当該組織が存在していることを確認する。

＜代理人からの申請の場合＞

① 持参の場合

代理人から提示された各種の書類について、以下の確認を行う。

・　発行申請書記載の組織名と開設者名が、指定通知書コピー記載の組織名と開設者名と一致しているか確認する。
・　発行申請書に組織開設者の署名もしくは印が押印されているか確認する。
・　委任状に組織開設者の署名もしくは印が押印されているか確認する。
・　委任状記載の代理人氏名と、代理人から提出された本人確認書類記載の氏名が一致していることを確認する。

・　保健医療機関、保健薬局の場合は、地方厚生局が所管し公開している全保険医療機関・保険薬局一覧等を用いて存在性を確認する。
・　介護事業者の場合は、都道府県または市町村が所管し公開している情報等を用いて存在性を確認する。
・　地方厚生局、都道府県、市町村の公開情報で存在性が確認出来ない場合は、地方厚生局、都道府県、市町村や発行申請書記載の電話番号に電話し、当該組織が存在していることを確認する。

なお、組織が中央官庁・地方公共団体の運営する機関で、当該機関の実在性が明らかな場合は、公印の押された申請書類の提出を求めることで、問い合わせによる確認を省略することができる。

② 郵送の場合
代理人による郵送の申請は受け付けない。

③ オンラインの場合
代理人による郵送の申請は受け付けない。

＜法令等の要請により証明書を発行する場合＞
組織の実在性及び有資格性の確認については、法令等で定められた組織が保険医療機関等の実在性、保険医療機関等であることの認証を実施した結果を持って資格確認に変える。

(2)　その他組織からの申請により発行する場合
本認証局は、加入者証明書の発行時、本 CPS「3.2.2　組織の認証」及び「3.2.3 個人の認証」に定める各立証事項に対して、それぞれ以下の方法で真偽の確認を行う。

＜組織管理者もしくは組織所属者からの申請の場合＞
① 持参の場合
申請者から提示された各種の書類について、以下の確認を行う。
・　発行申請書記載の組織名と代表者名が、登記事項証明書もしくは個人事業者であることを証明する書類記載の組織名と代表者名と一致しているか確認する。
・　発行申請書に組織代表者の署名もしくは印が押印されているか確認する。
・　申請者が組織代表者でない組織所属者の場合、社員証等で組織所属の確認をする。
・　組織所属の確認が出来ない場合、発行申請書記載の電話番号に電話し、当該組織に申請者が在籍していることを確認する。

・　法人組織の場合は、国税庁が所管し公開している、法人番号公表サイトを用いて組織の実在性を確認する。
・　個人事業者の場合は、提出書類の確認をもって組織の実在性を確認する。
・　三省 4 ガイドラインの適合性についての書類が提出されていることを確認する。

なお、組織が中央官庁・地方公共団体の運営する機関で、当該機関の実在性が明らかな場合は、公印の押された申請書類の提出を求めることで、問い合わせによる確認を省略することができる。

② 郵送の場合

申請者から提示された各種の書類について、以下の確認を行う。

・　発行申請書記載の組織名と代表者名が、登記事項証明書もしくは個人事業者であることを証明する書類記載の組織名と代表者名と一致しているか確認する。
・　発行申請書に組織代表者の署名もしくは印が押印されているか確認する。
・　発行申請書記載の電話番号に電話し、申請者が在籍していることを確認する。
・　法人組織の場合は、国税庁が所管し公開している、法人番号公表サイトを用いて組織の実在性を確認する。
・　個人事業者の場合は、提出書類の確認をもって組織の実在性を確認する。
・　三省 4 ガイドラインの適合性についての書類が提出されていることを確認する。

③ オンラインの場合

申請者から提示された申請データについて、以下の確認を行う。

・　申請データに付与されている電子署名データの有効性を確認する。
・　電子署名データの電子証明書 Subject の氏名が、申請データの代表者名と一致しているか確認する。
・　電子署名データの電子証明書 Subject の組織名が、申請データの組織名と一致しているか確認する。
・　申請データの組織名と代表者名が、登記事項証明書のスキャンデータに記載の組織名と管理者名と一致しているか確認する。
・　国税庁が所管し公開している、法人番号公表サイトを用いて組織の実在性を確認する。
・　三省 4 ガイドラインの適合性についての書類のデータが提出されていることを確認する。

＜代理人からの申請の場合＞

① 持参の場合

代理人から提示された各種の書類について、以下の確認を行う。

- 発行申請書記載の組織名と代表者名が、登記事項証明書もしくは個人事業者であることを証明する書類記載の組織名と代表者名と一致しているか確認する。
- 発行申請書に組織代表者の署名もしくは印が押印されているか確認する。
- 委任状に組織代表者の署名もしくは印が押印されているか確認する。
- 委任状記載の代理人氏名と、代理人から提出された本人確認書類記載の氏名が一致していることを確認する。
- 法人組織の場合は、国税庁が所管し公開している、法人番号公表サイトを用いて組織の実在性を確認する。
- 個人事業者の場合は、提出書類の確認をもって組織の実在性を確認する。
- 三省 4 ガイドラインの適合性についての書類が提出されていることを確認する。

なお、組織が中央官庁・地方公共団体の運営する機関で、当該機関の実在性が明らかな場合は、公印の押された申請書類の提出を求めることで、問い合わせによる確認を省略することができる。

② 郵送の場合

代理人による郵送の申請は受け付けない。

③ オンラインの場合

代理人による郵送の申請は受け付けない。

＜法令等の要請により証明書を発行する場合＞

組織の実在性及び有資格性の確認については、法令等で定められた組織が当該組織の実在性及び有資格性があることの認証を実施した結果を持って資格確認に変えることができる。

(3) 登録局の審査業務の一部を委託して発行する場合

登録局は、「1.3.2　登録局」で定める条件の下、業務の一部を外部に委託することができるが、そのうち医療関係団体等に、当該団体に加盟・所属する組織へ証明書を発行する際の審査業務を委託することができる。

この場合、本 CPS に則った組織の実在性及び有資格性の確認を当該団体の管理者の責任のもと実施しなくてはならない。

また、本認証局と当該団体の間で委託に係わる契約を取り交わし、委託された業務に関して登録局に課せられると同等の業務内容、責任及び義務を当該団体に負わ

せる。

4.2.2　証明書申請の承認又は却下

本認証局は、書類不備や実在性の確認等の審査過程において疑義が生じた場合に利用申請を不受理とする。

4.2.3　証明書申請手続き期間

本認証局では、加入者証明書申請の手続き期間などを情報公開 Web サイトで公開する。

4.3　証明書発行

4.3.1　証明書発行時の認証局の機能

(1)　認証局が鍵ペアを生成する場合

ネットワーク用証明書及びクライアント用証明書を生成する場合が対象である。

① 本認証局は、登録局にて審査して認めた証明書発行要求データを生成し、発行局に証明書発行要求を行う。
② 発行局は証明書発行要求データを認証局システム（以下、「CA システム」という）に対し登録する。
③ 発行局は、認証設備室にて加入者鍵ペア、加入者証明書を生成し、生成した加入者の私有鍵と加入者証明書を証明書格納媒体に格納する。このとき生成された加入者の私有鍵は証明書格納媒体に格納後、速やかに認証業務用設備から削除する。
④ 生成された加入者鍵ペアと加入者鍵ペアの活性化に使用する PIN を、加入者本人に送付する場合は、書留郵便にて郵送し私有鍵の所有を確認するものとする。
⑤ 加入者鍵ペアと活性化に使用する PIN を別送する場合は、活性化に使用する PIN を加入者宛てに書留郵便にて郵送し、加入者鍵ペアは加入者が指定する送付先に書留郵便にて送付する。この場合、加入者鍵ペアの活性化 PIN を加入者本人のみ保持させることをもって私有鍵の所有を確認するものとする。

(2)　加入者が鍵ペアを生成する場合

Web サーバ用証明書が対象である。

① 加入者は、加入者公開鍵と加入者私有鍵を生成し、登録局に証明書発行要求データ（CSR）を提出する。
② 登録局は、CSR データを確認し登録局で実施した審査結果と情報が相違ないことを確認した上で、発行局に証明書発行依頼を行う。

③　発行局は、CSR データを認証局システム（以下、「CA システム」という）に対し登録する。

④　生成された加入者証明書を、加入者宛てに書留郵便を郵送する。

4.3.2　証明書発行後の通知

本認証局は、加入者証明書を交付することにより加入者証明書を発行したことを通知したものとみなす。

4.4　証明書の受理

4.4.1　証明書の受理

本認証局は、加入者証明書を加入者もしくは加入者が指定した送付先に郵送したことをもって受理したものとみなす。

ただし、法令等の要請により加入者証明書を発行した場合は、法令等に定める方法により加入者証明書を受理した旨を確認する。

4.4.2　認証局による証明書の公開

本認証局は、加入者証明書の公開は行わない。

4.4.3　他のエンティティに対する認証局による証明書発行通知

本認証局は、他エンティティに対する証明書発行通知は行わない。

4.5　鍵ペアと証明書の利用目的

4.5.1　加入者の私有鍵と証明書の利用目的

加入者は、私有鍵を本 CPS「1.4.1 適切な証明書の使用」に規定する用途のみに使用できる。また、本認証局は、加入者証明書が用途以外の目的で使用された場合には、一切の責任を負わない。

4.5.2　検証者の公開鍵と証明書の利用目的

検証者は、加入者の認証用途で公開鍵と証明書を利用する。

4.6　証明書更新

4.6.1　証明書更新の要件

本 CPS に則り認証局から発行される証明書の更新は行わない。

4.6.2　証明書の更新申請者

規定しない。

4.6.3　証明書更新の処理手順

規定しない。

4.6.4　加入者への新証明書発行通知

規定しない。

4.6.5　更新された証明書の受理

規定しない。

4.6.6　認証局による更新証明書の公開

規定しない。

4.6.7　他のエンティティへの証明書発行通知

規定しない。

4.7　証明書の鍵更新（鍵更新を伴う証明書更新）

4.7.1　証明書鍵更新の要件

本 CPS に則り認証局から発行される証明書の更新は行わない。

4.7.2　鍵更新申請者

規定しない。

4.7.3　鍵更新申請の処理手順

規定しない。

4.7.4　加入者への新証明書発行通知

規定しない。

4.7.5　鍵更新された証明書の受理

規定しない。

4.7.6　認証局による鍵更新証明書の公開

規定しない。

4.7.7　他のエンティティへの証明書発行通知

規定しない。

4.8　証明書変更

4.8.1　証明書変更の要件

本 CPS に則り認証局から発行される証明書は、証明書変更を行わない。

4.8.2　証明書の変更申請者

規定しない。

4.8.3　証明書変更の処理手順

規定しない。

4.8.4　加入者への新証明書発行通知

規定しない。

4.8.5　変更された証明書の受理

規定しない。

4.8.6　認証局による変更証明書の公開

規定しない。

4.8.7　他のエンティティへの証明書発行通知

規定しない。

4.9　証明書の失効と一時停止

4.9.1　証明書失効の要件

本認証局は、次の場合に加入者証明書を失効するものとする。

(1)　組織管理者もしくは組織所属者、または代理人からの失効申請の場合
次の各項に該当する場合、失効申請を行わなくてはならない。

本認証局は、組織管理者もしくは組織所属者、または代理人からの失効申請と確認した場合は、理由の如何に関わらず証明書を失効する。

- 加入者私有鍵を紛失した場合
- 加入者私有鍵の盗難を知った場合
- 加入者私有鍵の不正使用を知った場合
- 加入者私有鍵の不正な複製を知った場合
- 加入者私有鍵を削除した場合
- 加入者鍵ペアの活性化 PIN を紛失した場合
- 加入者鍵ペアの活性化 PIN の漏洩を知った場合
- 加入者鍵ペアの活性化 PIN の不正使用を知った場合
- 加入者私有鍵が危殆化又は、危殆化の恐れがある場合
- 加入者証明書の利用を停止する場合
- その他、加入者が加入者証明書を失効させる必要があると判断した場合

(2)　認証局の職員から失効申請があった場合

次の各項に該当する場合、証明書を失効させる。

- 加入者が、本 CPS、又はその他の契約、規制、あるいは有効な加入者証明書に適用される法に基づく義務を満たさなかった場合
- 加入者私有鍵の危殆化が認識されたか、その疑いがある場合
- 本 CPS に従って加入者証明書が適切に発行されなかったと認証局が判断した場合
- 加入者証明書に含まれる該当の情報が正確でなくなった場合。(例えば、保険医療機関等の保健医療福祉分野専門資格を喪失した場合)
- 認証局の CA 私有鍵が危殆化又は、危殆化の恐れがある場合
- 認証局のオペレーションミスにより加入者証明書の記載事項に誤りがあった場合
- その他の事由により証明書の記載事項に誤りがあった場合
- 加入者の特定ができない場合で、緊急に失効させる必要があると認証局が判断した場合
- 認証局が認証業務を廃止する場合

(3)　法令等で定められた組織から失効申請があった場合

法令等で定められた組織からの失効申請と確認された場合は、理由の如何に関わらず証明書を失効させなくてはならない。

4.9.2　失効申請者

本認証局は、以下の申請者から失効申請を受け付ける。

1. 組織の名前で証明書が発行された当該組織管理者もしくは組織所属者、または代理人
2. 認証局の職員
3. 法令等で定められた組織

4.9.3 失効申請の処理手順

認証局は、失効申請の受領の判断を行い受理する場合は「3.4 失効申請時の本人性確認と認証」に従って、以下の手順を実施した上で加入者証明書の失効を行う。

(1) 組織管理者もしくは組織所属者からの失効申請の場合

失効を要求している申請者が、失効される加入者証明書に記載されている組織の管理者もしくは組織所属者であることを確認する。確認にあたっては、本認証局で保存している「4.2.1 本人性及び組織の認証」で用いた申請者の各種書類を参照し、間違いなく当該組織からの申請であること及び当該加入者証明書であることを確認する。

(2) 代理人からの失効申請の場合

代理人が失効を要求して来た場合は、当該組織等の責任者の委任状を確認することを持って、当該代理人が正当な失効権限を持っていることを確認する。

当該証明書の実際の失効にあたっては、代理人を通じて失効を要求している申請者が、失効される証明書に記されている組織の管理者であることを確認する。確認にあたっては、本認証局で保存している「4.2.1 本人性及び組織の認証」で用いた申請者の各種書類を参照し、間違いなく当該組織からの申請であること及び当該加入者証明書であることを確認する。

上記それぞれの確認と共に、証明書の失効理由を確認し、その真偽についても確認も実施する。

この手順により加入者証明書の失効を実施した場合は、CRL を発行する。また、加入者証明書の失効の事実を加入者に通知する。

(3) 認証局の職員からの失効申請の場合

本認証局は「4.9.1 証明書失効の要件」の中の認証局の職員から失効申請があった場合は、速やかに当該加入者証明書を特定し、失効の事由の真偽の確認を実施する。

また、失効事由が真実であった場合は速やかに加入者証明書を失効させなくてはならない。

加入者証明書の失効を実施した場合は、CRL を発行する。また、加入者証明書の失効の事実を加入者に通知する。

(4)　法令等に定める組織からの失効申請の場合

法令等で定められた組織から提示された確認方法に従い、速やかに当該加入者証明書を特定し失効しなくてはならない。確認にあたっては、本認証局で保存している「4.2.1　本人性及び組織の認証」で用いた申請者の各種書類を参照し、間違いなく当該組織からの申請であること及び当該加入者証明書であることを確認する。

加入者証明書の失効を実施した場合は、CRL を発行する。また、加入者証明書の失効の事実を加入者に通知する。

4.9.4　失効における猶予期間

「4.9.1 証明書失効の要件」に規定されている事由が発生した場合には、速やかに失効申請を行わなければならない。

4.9.5　認証局による失効申請の処理期間

加入者証明書の失効要求の結果として取られる処置は、受領後直ちに開始されるものとする。

4.9.6　検証者の失効情報確認の要件

検証者は、認証者の公開鍵を使う時に有効な CRL/ARL を使用して失効の有無をチェックし、証明書状態の確認を行うものとする。

4.9.7　CRL 発行頻度

本認証局は、CRL の発行頻度を決定し、決定した頻度に従い CRL の更新を行う。

1. CRL の有効期間を 96 時間とし、48 時間ごとに更新する。
2. 加入者証明書の失効を行った場合は、CRL を更新する
3. CA 私有鍵が危殆化し、又はその恐れがある場合は、直ちに発行した全ての加入者証明書を失効させ、CRL を発行する。

4.9.8　CRL が公開されない最大期間

CRL は発行後 24 時間以内に公開される。

4.9.9　オンラインでの失効／ステータス情報の入手方法

規定しない。

4.9.10　オンラインでの失効確認要件

規定しない。

4.9.11　その他利用可能な失効情報確認手段

使用しない。

4.9.12　鍵の危殆化に関する特別な要件

本認証局は、CA 私有鍵の危殆化の際には関連組織に直ちに通知するものとする。

4.9.13　証明書一時停止の要件

一時停止は行わない。

4.9.14　一時停止申請者

一時停止は行わない。

4.9.15　一時停止申請の処理手順

一時停止は行わない。

4.9.16　一時停止期間の制限

一時停止は行わない。

4.10　証明書ステータスの確認サービス

4.10.1　運用上の特徴

規定しない。

4.10.2　サービスの利用可能性

規定しない。

4.10.3　オプショナルな仕様

規定しない。

4.11　加入の終了

加入者が、証明書の利用を終了する場合、本 CPS「4.9 証明書の失効と一時停止」に規定する失効手続きを行うものとする。

4.12　私有鍵預託と鍵回復

私有鍵は、特に法律によって必要とされる場合を除き、預託及び回復を行わない。

4.12.1　預託と鍵回復ポリシ及び実施

規定しない。

4.12.2　セッションキーのカプセル化と鍵回復のポリシ及び実施

規定しない。

5　建物・関連設備、運用のセキュリティ管理

5.1　建物及び物理的管理

5.1.1　施設の位置と建物構造

本認証局の施設は、水害、地震、火災その他の災害の被害を容易に受けない安全な場所に設置し、建物構造上、耐震、耐火、防水、空調機能を有する。また、建物内外に認証局関連施設であることを示す掲示を行わない。

5.1.2　物理的アクセス

本認証局の施設は、その重要度に応じて複数のセキュリティレベルに分かれている。認証局に関する機器を設置する部屋には、認証設備室等がある。

本認証局の施設は予めアクセス可能な人員を定義し、その者以外がアクセスする場合は、定められた手続きをとり、定められた人員が立ち会わなければならない。認証設備へのアクセスは、2 人以上の複数の者による監視の下で行う。

また、各施設の入口には、適切なアクセスコントロールがなされている。施設への入室のログは記録される。

(1)　認証設備室

認証設備室は、認証設備のうち、電子証明書の発行・管理を行う最も重要な機器が設定されている部屋である。

認証設備室への入室及び認証設備へのアクセスにあたっては、権限を有する 2 名以上の者によって可能とする。やむを得ず権限がない者が入室する場合には、事前に設備責任者が許可した者のみ、有権限者の同伴のもとで入室を認めるものとする。

(2)　認証事務室

認証事務室は、加入者から郵送された申請書及び添付資料を審査・登録するための部屋である。

認証事務室においては、関係者以外が容易に立ち入ることが出来ないように施錠され他の区画とは区別されている。

5.1.3　電源及び空調設備

認証設備室においては、運用に十分な電源容量を確保した無停電電源装置を設置している。無停電電源装置とは、瞬断しないように電源そのものに UPS の機能が備わっており、かつ電源が供給されない事態に備えて発電機を用意し、一定時間内に発電機による電源供給に切り替える仕組みを持つ電源の事をいう。また、空調設備を設置し、機器

類の動作環境及び要員の作業環境を適切に維持する。

5.1.4　水害及び地震対策

認証設備室においては、建物の二階以上に設置する。また、空調設備には防水堤と漏水検知機を設置する。

また、建物は耐震構造である。また、認証設備には、通常想定される規模の地震による転倒及び構成部品の落下等を防止するための構成部品の固定やその他の耐震措置を講じる。

5.1.5　防火設備

建物は耐火構造である。認証設備は、建築基準法で規定される防火区画内に設置する。また、自動火災報知器や消化設備を備える。

5.1.6　記録媒体

アーカイブデータ、バックアップデータを含む媒体は、適切な入退室管理が行われている室内に設置された施錠可能な保管庫に保管するとともに、別途本認証局の定める手続きに基づき適切に搬入出管理を行う。

5.1.7　廃棄物の処理

機密扱いとする情報を含む書類・記録媒体の廃棄については、所定の手続きに基づいて適切に廃棄処理を行う。

5.1.8　施設外のバックアップ

規定しない。

5.2　手続的管理

5.2.1　信頼すべき役割

本認証局は、下表に示す認証業務の遂行に必要な認証局員の役割を定めている。

表 5.2 認証局員の各役割

担当名	主な役割
認証局代表者	・本認証局の運営及び管理と業務の総括 ・本 CPS の承認 ・CA 私有鍵の危殆化、又は危殆化の恐れがある場合の対応に関する決定 ・災害などによる緊急事態における対応に関する決定

	・登録局責任者と発行局責任者の任命と解任および人事管理 ・登録局及び発行局の運営及び管理と業務の統括 ・生成された CA 私有鍵のバックアップの保管
登録局責任者	・登録局内全ての設備に対する維持・管理の実施と管理 ・登録局審査員、システム保守員の任命と解任および人事管理 ・審査、登録、発行業務の実施と監督 ・生成された CA 私有鍵のバックアップの保管
登録局審査員	・組織の審査業務 ・審査における組織からの問い合わせ対応
発行局責任者	・認証設備室（CA システム含む）内全ての設備に対する維持・管理の実施と管理 ・発行局操作員、システム保守員の任命と解任および人事管理 ・加入者証明書の発行、失効業務の監督 ・発行局操作員との合議制操作による CA 私有鍵の生成 ・生成された CA 私有鍵のバックアップの保管
発行局操作員	・加入者証明書の発行、失効業務 ・発行局責任者との合議制操作による CA 私有鍵の生成 ・複数の発行局操作員の合議制操作による CA システムの起動および停止 ・複数の発行局操作員の合議制操作による CA 私有鍵のアクティベーションおよび非アクティベーション
システム保守員	・監査ログの収集・保存、システム障害対応・分析・報告、認証設備の各種操作など、認証設備室及び認証事務室の設備に対する維持・管理の遂行

5.2.2　職務ごとに必要とされる人数

各役割に対して本認証局にて別途規定する必要数の担当者を配置する。但し、セキュリティ上問題が無いと判断された場合には１名の担当者が複数の役割を兼務することがある。

5.2.3　個々の役割に対する本人性確認と認証

各役割に応じて部屋毎の入室権限及び認証設備へのアクセス権限を付与し、アクセスコントロールを行う。

認証設備へのアクセスにおいては、電子証明書もしくはID・パスワードによるログイン認証によって、システムは操作者が正当な権限者であることを識別し認証する。また、業務の重要度に応じ、複数の要員による合議操作、立会い等による相互牽制を行うもの

とする。

5.2.4　職務分轄が必要になる役割

電子証明書の発行、失効などの重要な業務の実施にあたっては、要員の職務権限を明確に分離する。特に登録局 と発行局 の業務の兼任は禁止する。

5.3　要員管理

5.3.1　資格、経験及び身分証明の要件

本認証局の業務運営に関して信頼される役割を担う者は、本認証局運営組織の採用基準に基づき採用された職員とする。CA システムを直接操作する担当者は、専門のトレーニングを受け、PKI の概要とシステムの操作方法等を理解しているものを配置する。

5.3.2　経歴の調査手続

〇〇〇で定める職務規定に従うものとする。

5.3.3　研修要件

本認証局は、認証局員に対し必要に応じて教育・訓練を実施する。また、業務内容、手順等の変更及び指揮命令系統、責任及び権限の変更等が行われた場合、教育・訓練を実施する。

5.3.4　再研修の頻度及び要件

本認証局は、認証局員に対し必要に応じて教育・訓練を実施する。また、業務内容、手順等の変更及び指揮命令系統、責任及び権限の変更等が行われた場合、教育・訓練を実施する。

5.3.5　職務のローテーションの頻度及び要件

規定しない。

5.3.6　認められていない行動に対する制裁

規定しない。

5.3.7　独立した契約者の要件

規定しない。

5.3.8　要員へ提供する資料

規定しない。

5.4　監査ログの取扱い

5.4.1　記録するイベントの種類

本認証局は、CA システム、リポジトリ及び認証設備室内のネットワーク機器に関する記録である監査イベントを監査ログとして記録する。監査ログには、下記のものが含まれる。また、イベントを起こした者への通知は行わない。

1. CA システムの起動・停止等の稼動ログ及び機能変更等の操作ログ
2. CA システムにおける加入者の登録、加入者証明書の発行要求及び失効要求並びに加入者証明書の生成処理及び失効処理に関するログ
3. リポジトリにおける掲載情報の変更記録
4. ファイアウォール等の認証設備室内のネットワークログ

認証設備室の入退室管理装置の動作ログ及び監視カメラの映像記録

5.4.2　監査ログを処理する頻度

本認証局は、監査ログを 3 ヶ月に 1 度以上定期的に検査する。

5.4.3　監査ログを保存する期間

監査ログは、最低 10 年間保存される。

5.4.4　監査ログの保護

認証局は、認可された人員のみが監査ログにアクセスすることができるよう、適切なアクセスコントロールを採用し、権限を持たない者の閲覧や、改ざん、不正な削除から保護する。

5.4.5　監査ログのバックアップ手続

監査ログは、月 1 回の頻度でバックアップする。

5.4.6　監査ログの収集システム（内部対外部）

規定しない。

5.4.7　イベントを起こしたサブジェクトへの通知

規定しない。

5.4.8　脆弱性評価

規定しない。

5.5　記録の保管

5.5.1　アーカイブ記録の種類

認証局 は、以下の情報をアーカイブする。

- 証明書の発行/取消に関する処理履歴
- CRL の発行に関する処理履歴
- 認証局の証明書
- 加入者の証明書
- 証明書申請内容の審議の確認に用いた書類
- 失効の要求に関わる書類

5.5.2　アーカイブを保存する期間

アーカイブする情報は、記録が作成されてから最低 10 年間は保存する。

5.5.3　アーカイブの保護

アーカイブ情報の収められた媒体は物理的セキュリティによって保護され、許可された者しかアクセスできないよう制限された施設に保存され、権限を持たない者の閲覧や持ち出し、改ざん、消去から保護する。また、自然災害、火災及び盗難などから保護された場所に保存する。

5.5.4　アーカイブのバックアップ手続

アーカイブは、月 1 回の頻度でバックアップを実施する。

5.5.5　記録にタイムスタンプをつける要件

本 CPS「5.5.1　アーカイブ記録の種類」で規定する情報の記録時間は、処理を行った日付を記録する。

5.5.6　アーカイブ収集システム（内部対外部）

アーカイブの収集機能は、本認証局の CA システム及びリポジトリの機能とし、業務及びセキュリティに関する重要な事象をアーカイブとして収集する。

5.5.7　アーカイブ情報を入手し、検証する手続

本 CPS「5.5.1　アーカイブ記録の種類」で規定する情報については、本 CPS「5.5.3 アーカイブの保護」で規定する方法により、可用性と完全性が確保された形で安全に保管

される。

5.6　鍵の切り替え

認証局は、定期的に CA 私有鍵の更新を行う。CA 私有鍵は、認証設備室内にて、複数人の立会いのもと、専用の暗号モジュール（HSM）を用いて生成される。

CA 私有鍵の更新と共に自己署名証明書の更新も実施される。この更新においても CA 私有鍵生成の場合と同様に、複数人の立会いのもと執り行われる。

5.7　危殆化及び災害からの復旧

5.7.1　災害及び CA 私有鍵危殆化からの復旧手続き

認証局は、想定される以下の脅威に対する復旧手順を規定し、関係する認証局員全員に適切な教育・訓練を実施する。

- CA 私有鍵の危殆化
- 火災、地震、事故等の自然災害
- システム（ハードウェア、ネットワーク等）の故障

5.7.2　コンピュータのハードウェア、ソフトウェア、データが破損した場合の対処

ハードウェア、ソフトウェア、データが破壊又は損傷した場合、バックアップ用のハードウェア、ソフトウェア、バックアップデータを用いて、速やかに復旧作業を行い、合理的期間内に認証局業務を再開する。また、障害発生時には、可能な限り速やかに、加入者、検証者に情報公開用 Web サイト等により通知する。

5.7.3　CA 私有鍵が危殆化した場合の対処

CA 私有鍵が危殆化又はそのおそれが生じた場合は、認証局代表者の判断により、速やかに認証業務を停止するとともに、認証局で規定された手続きに基づき、全ての加入者証明書の失効を行い、CRL を開示し、CA 私有鍵を廃棄する。更に、原因の追求と再発防止策を講じる。

5.7.4　災害等発生後の事業継続性

災害などにより、認証施設及び設備が被災し、通常の業務継続が困難な場合には、認証局で規定された手続きに基づき、加入者及び検証者に情報を公開する。

5.8　認証局又は登録局の終了

認証局が運営を停止する場合には、運営の終了の 90 日前までに加入者に通知し、認証局の鍵と情報の継続的な保管を手配するものとする。

認証局が終了する場合には、当該認証局の記録の安全な保管又は廃棄を確実にするための取り決めを行うこととする。

登録局の運用を停止する場合は、事前に加入者の同意を得たうえで、登録局が有する加入者の情報と運営を他の登録局に移管し、それを加入者に通知する。

6　技術的なセキュリティ管理

6.1　鍵ペアの生成と実装

6.1.1　鍵ペアの生成

CA 鍵ペアは、認証設備室内に設置された専用の暗号モジュール（HSM）を用いて、複数人の立会いのもと、権限を持った者による操作により生成される。

6.1.2　加入者への私有鍵の送付

加入者の私有鍵が認証局で生成される場合で、鍵ペアと活性化 PIN をいっしょに加入者に送付する場合は、書留郵便にて郵送し私有鍵の所有を確認するものとする。

加入者鍵ペアと活性化に使用する PIN を別送する場合は、活性化に使用する PIN を加入者宛てに書留郵便にて郵送し、加入者鍵ペアは加入者が指定する送付先に書留郵便にて送付する。この場合、加入者鍵ペアの活性化 PIN を加入者本人のみ保持させることをもって私有鍵の所有を確認するものとする。

6.1.3　認証局への公開鍵の送付

加入者の公開鍵が加入者により生成される場合は、IETF RFC 2510「証明書管理プロトコル」に従ってオンライントランザクションで、又は同様に安全な方法によって、認証局に引き渡されるものとする。

6.1.4　検証者への CA 公開鍵の配付

CA 公開鍵は、検証者によるダウンロードを可能とするために、本認証局のリポジトリにて公開するものとする。

6.1.5　鍵のサイズ

鍵の最小サイズは、使用されるアルゴリズムに依存する。CA 証明書の鍵の最小サイズは、RSA アルゴリズムの場合、2048 ビットとする。他のアルゴリズムを使用する CA 証明書の鍵の最小サイズは、同等のセキュリティを提供するサイズとする。

加入者証明書の鍵の最小サイズは、RSA アルゴリズム又は技術的に同等のアルゴリズムの場合、2048 ビットとする。他のアルゴリズムを使用するエンドエンティティの証明書の鍵の最小サイズは、同等のセキュリティを提供するサイズとする。

6.1.6　公開鍵のパラメータ生成及び品質検査

公開鍵パラメータは、信頼できる暗号モジュールによって生成される。公開鍵パラメータの品質検査も暗号モジュールにより行うものとする。

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。

加入者証明書の鍵は、以下とする。

・ネットワーク用証明書：DigitalSignature

・クライアント用証明書：DigitalSignature

・Web サーバ用証明書：DigitalSignature、KeyEncipherment

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

本認証局の CA 私有鍵の生成及び管理は、本認証局の鍵の管理を担う複数人の運営要員よって行われる。

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。

加入者私有鍵は、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

本認証局の CA 私有鍵は､本認証局の鍵の管理を担う複数人の運営要員よって行われ､かつ､そのうちの 1 名だけではできない方法によって認証設備室内でバックアップされ､複数に分割されたバックアップ用の鍵として保管する。バックアップ用の鍵の個々については、一つずつ権限を有する者以外が触れることができないアクセス制御などの措置がされ、耐火等の防災措置がとられた異なる場所に施錠して保管する。

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

本認証局の CA 私有鍵をバックアップ用の鍵からリストア（復元）する場合は、本認証局の鍵の管理を担う複数の運営要員によって認証設備室にて行う。

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、認証設備室内で本 CPS「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。

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

本 CPS「5.5.2　アーカイブを保存する期間」及び「5.5.3　アーカイブの保護」で規定するとおり行う。

6.3.2　公開鍵証明書の有効期間と鍵ペアの使用期間

CA 証明書と加入者証明書の私有鍵と公開鍵の有効期間については、表 6-1 に示す。

表 6-1 鍵の有効期間

証明書種別	私有鍵有効期間	公開鍵有効期間
CA 証明書	10 年	20 年
ネットワーク用証明書	6 年 5 ヶ月	6 年 5 ヶ月
クライアント用証明書	6 年 5 ヶ月	6 年 5 ヶ月
Web サーバ用証明書	6 年 5 ヶ月	6 年 5 ヶ月

なお、加入者証明書の有効期間の設定は以下とする。

＜保険医療機関、保険薬局、介護事業者の場合＞

- 有効期間開始日
  保険医療機関、保険薬局、介護事業者から提出された指定通知書コピーに記載されている指定の期間の開始日を設定する。
- 有効期間終了日
  保険医療機関、保険薬局、介護事業者から提出された指定通知書コピーに記載されている指定の期間の終了日から 5 ヵ月後を設定する。

＜その他組織の場合＞

- 有効期間開始日
  加入者証明書の発行日を設定する。
- 有効期間終了日
  加入者証明書の発行日から 6 年 5 ヶ月－1 日を設定する。

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。

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、加入者に書留郵便にて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。

加入者私有鍵の活性化データを認証局で生成する場合は、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

認証業務用設備は、ファイアウォールを介して外部ネットワークと接続し、不正アクセスを検知・防止する。本認証業務で用いる暗号化装置は、FIPS140-2 レベル 3 同等以上の暗号化装置を用いる。

CA システムへのログイン時には、本 CPS「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

本認証局で使用する製品については、セキュリティに関する情報等を定期的に収集し、最新のセキュリティ技術の最新動向を踏まえて、使用する製品が設けたセキュリティに関する基準を満たすよう維持管理する。

6.6　ライフサイクルの技術的管理

6.6.1　システム開発管理

本認証局のシステムは、適切な品質管理が行われた信頼できる組織で開発されたものを使用する。

本認証局のシステムについては、電磁的記録で保存される記録の内容が表示できるように、当該システムの機器、OS 及びアプリケーションを維持する。

本認証局のシステムに係る機器、OS 及びアプリケーションを更新する場合は、更新前に試験等を行い、互換性を確保する。

6.6.2　セキュリティ運用管理

認証設備及びネットワーク設備の新規導入、機能追加や設定変更等を行う場合は、本認証局で規定された手順に従って実施する。

6.6.3　ライフサイクルのセキュリティ管理

セキュリティの脆弱性に関する情報等を収集し、適切なサイクルで最新のセキュリティ技術を導入するため、随時セキュリティホールチェックを行う。セキュリティ上深刻な問題や脆弱性などがないかを検証環境にて評価し、必要に応じて是正措置を実施する。

6.7　ネットワークのセキュリティ管理

本認証局のネットワークについては、別途定めるセキュリティに関する規程に則り、適切な運用を行う。また、定期的な評価を実施し、ネットワーク運用が定められたセキュリティに関する規程を満たすよう、以下の措置を行い、維持する。

(1) 認証業務用設備を構成するネットワーク、及びリポジトリを構成するネットワークに対する不正アクセスを防止・検知するためのファイアウォール及び不正侵入検知システムによる制御・監視
(2) 認証業務用設備を構成するネットワーク上の通信データの漏洩及び盗聴防止のための暗号化
(3) 認証業務用設備を構成するコンピュータへの不正アクセスを防止するための遠隔操作ができない措置。

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。本認証局が発行する電子証明書のプロファイルの詳細は、表 7.1.1 のとおりとする。

表 7.1.1　証明書とプロファイル対応表

証明書種別	基本領域プロファイル	拡張領域プロファイル
CA 証明書	表 7.1.2	表 7.1.3
ネットワーク用証明書	表 7.1.4	表 7.1.5
クライアント用証明書	表 7.1.6	表 7.1.7
Web サーバ用証明書	表 7.1.8	表 7.1.9

7.1.1　バージョン番号

本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）

本認証局が発行する証明書の拡張領域のプロファイルは以下の表 7.1.×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。

sha256WithRSAEncryption (1.2.840.113549.1.1.11)

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

本認証局が発行する加入者証明書のオブジェクト識別子は、表 1.2　の通りである。

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

本 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

HPKI-CP のオブジェクト識別子を格納する。

表 7.1.2　CA 証明書プロファイル（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	○	sha256WithRSAEncryption
Validity	○	
NotBefore	○	発行日時（UTCTime で設定する。）
NotAfter	○	thisUpdate + 20 年（UTCTime で設定する。）
Issuer	○	CountryName は Printable、それ以外は UTF-8 で記述する
CountryName	○	JP
OrganizationName	○	○○○
OrganizationUnitName	○	○○○ Center
CommonName	○	HPKI-01-○○○-forAuthentication-forOrganization
Subject	○	CountryName は Printable、それ以外は UTF-8 で記述する
CountryName	○	JP
OrganizationName	○	○○○
OrganizationUnitName	○	○○○ Center
CommonName	○	HPKI-01-○○○-forAuthentication-forOrganization
SubjectPublicKeyInfo	○	
Algorithm	○	rsaEncryption
SubjectPublicKey	○	RSA 公開鍵値(2048bit)
IssuerUniqueID	×	
SubjectUniqueID	×	
Extensions	○	拡張領域（表 7.1.3）参照

表中の、「○」設定、「×」は設定しないことを表す。

表 7.1.3　CA 証明書プロファイル（拡張領域 Extensions）

項目	設定	説明	Critical
authorityKeyIdentifier	○		FALSE
keyIdentifier	○	上位証明書の公開鍵の SHA-1 ハッシュ値	
authorityCertIssuer	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）	
directoryName	○	c=JP o= ○○○ ou= ○○○ Center cn= HPKI-01-○○○-forAuthentication-forOrganization	
authorityCertSerial	○	この証明書のシリアル番号	
subejctKeyIdentifier	○	この証明書の公開鍵の SHA-1 ハッシュ値	FALSE
KeyUsage	○	KeyCertSign	CRLSign	TRUE
DeciphermentOnly	×		-
extendedKeyUsage	×		-
privateKeyUsagePeriod	×		-
certificatePolicies	×		
policyMapping	×		-
subjectAltName	×		-
issuerAltName	×		-
subjectDirectoryAttributes	×		-
basicConstraints	○		TRUE
CA	○		-
pathLenConstraints	×		-
nameConstraints	×		-
policyConstraints	×		-
cRLDistributionPoints	○		FALSE
distributionPoint	○		
fullName	○		
uniformResource Identifier	○	http://×××/××.crl	
subjectInfoAccess	×		-
authorityInfoAccess	×		-

表中の、「○」は設定、「×」は設定しないことを表す。

表 7.1.4　ネットワーク用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	○	sha256WithRSAEncryption
Validity	○	
NotBefore	○	発行日時（UTCTime で設定する。）
NotAfter	○	発行日時から 6 年 5 ヶ月以下
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	○	JP
OrganizationName	○	○○○
OrganizationUnitName	○	○○○ Center
CommonName	○	HPKI-01-○○○-forAuthentication-forOrganization
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	△	都道府県名を記述する。
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、OrganizationUnitName に表 7.1.10 で定義する保健医療福祉機関等の種類を格納する。
OrganizationUnitName	△	
OrganizationUnitName	○	認証局が採番するユニーク ID を格納する。
CommonName	○	組織名称を UTF-8 でローマ字あるいは英語名で記載する。
SerialNumber	△	保険医療機関番号、保険薬局番号、介護事業所番号、法人番号などを格納する。
SubjectPublicKeyInfo	○	
Algorithm	○	RSAEncryption とする。
SubjectPublicKey	○	
IssuerUniqueID	×	
SubjectUniqueID	×	
Extentions	○	拡張領域（表 7.1.5）参照

表中の、「○」は設定、「△」はオプション、「×」は設定しないことを表す。

表 7.1.5　ネットワーク用証明書のプロファイル（拡張領域 Extensions）

項目	設定	説明	Critical
authorityKeyIdentifier	○		FALSE
keyIdentifier	○	上位証明書の公開鍵の SHA-1 ハッシュ値	
authorityCertIssuer	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）	
directoryName	○	c=JP o= ○○○ ou= ○○○ Centerr cn= HPKI-01-○○○-forAuthentication-forOrganization	
authorityCertSerial	○	上位証明書のシリアル番号	
subejctKeyIdentifier	○	この証明書の公開鍵の SHA-1 ハッシュ値	FALSE
KeyUsage	○	DigitalSignature	TRUE
DeciphermentOnly	×		-
extendedKeyUsage	×		-
privateKeyUsagePeriod	×		-
certificatePolicies	○		TRUE
policyIdentifier	○		
certPolicyId	○	1.2.392.100495.1.5.1.3.3.1	
policyQualifiers	○		
cPSuri	○	http://×××/	
policyMapping	×		-
subjectAltName	△		FALSE
DNSName	△	FQDN を格納する	
iPAddress	△	IP アドレスを格納する	
issuerAltName	×		-
subjectDirectoryAttributes	○	hrRole を格納する。	FALSE
basicConstraints	×		-
CA	×		-
pathLenConstraints	×		-
nameConstraints	×		-
policyConstraints	×		-
cRLDistributionPoints	○		FALSE
distributionPoint	○		
fullName	○		
uniformResource Identifier	○	http://×××/××.crl	
subjectInfoAccess	×		-
authorityInfoAccess	×		-

表中の、「○」は設定、「△」はオプション、「×」は設定しないことを表す。

表 7.1.6　クライアント用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	○	sha256WithRSAEncryption
Validity	○	
NotBefore	○	発行日時（UTCTime で設定する。）
NotAfter	○	発行日時から 6 年 5 ヶ月以下
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	○	JP
OrganizationName	○	○○○
OrganizationUnitName	○	○○○ Center
CommonName	○	HPKI-01-○○○-forAuthentication-forOrganization
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	△	都道府県名を記述する。
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、OrganizationUnitName に表 7.1.10 で定義する保健医療福祉機関等の種類を格納する。
OrganizationUnitName	△	
OrganizationUnitName	○	認証局が採番するユニーク ID を格納する。
CommonName	○	組織名称を UTF-8 でローマ字あるいは英語名で記載する。
SerialNumber	△	保険医療機関番号、保険薬局番号、介護事業所番号、法人番号などを格納する。
SubjectPublicKeyInfo	○	
Algorithm	○	RSAEncryption とする。
SubjectPublicKey	○	
IssuerUniqueID	×	
SubjectUniqueID	×	
Extentions	○	拡張領域（表 7.1.7）参照

表中の、「○」は設定、「△」はオプション、「×」は設定しないことを表す。

表 7.1.7　クライアント用証明書のプロファイル（拡張領域 Extensions）

項目	設定	説明	Critical
authorityKeyIdentifier	○		FALSE
keyIdentifier	○	上位証明書の公開鍵の SHA-1 ハッシュ値	
authorityCertIssuer	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）	
directoryName	○	c=JP o= ○○○ ou= ○○○ Centerr cn= HPKI-01-○○○-forAuthentication-forOrganization	
authorityCertSerial	○	上位証明書のシリアル番号	
subejctKeyIdentifier	○	この証明書の公開鍵の SHA-1 ハッシュ値	FALSE
KeyUsage	○	DigitalSignature	TRUE
DeciphermentOnly	×		-
extendedKeyUsage	○	clientAuth	FALSE
privateKeyUsagePeriod	×		-
certificatePolicies	○		TRUE
policyIdentifier	○		
certPolicyId	○	1.2.392.100495.1.5.1.3.3.1	
policyQualifiers	○		
cPSuri	○	http://×××/	
policyMapping	×		-
subjectAltName	×		-
issuerAltName	×		-
subjectDirectoryAttributes	〇		FALSE
basicConstraints	×		-
CA	×		-
pathLenConstraints	×		-
nameConstraints	×		-
policyConstraints	×		-
cRLDistributionPoints	○		FALSE
distributionPoint	○		
fullName	○		
uniformResource Identifier	○	http://×××/××.crl	
subjectInfoAccess	×		-
authorityInfoAccess	×		-

表中の、「〇」は設定、「×」は設定しないことを表す。

表 7.1.8　Web サーバ用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	○	sha256WithRSAEncryption
Validity	○	
NotBefore	○	発行日時（UTCTime で設定する。）
NotAfter	○	発行日時から 6 年 5 ヶ月以下
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	○	JP
OrganizationName	○	○○○
OrganizationUnitName	○	○○○ Center
CommonName	○	HPKI-01-○○○-forAuthentication-forOrganization
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	△	都道府県名を記述する。
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、OrganizationUnitName に表 7.1.10 で定義する保健医療福祉機関等の種類を格納する。
OrganizationUnitName	○	
OrganizationUnitName	○	認証局が採番するユニーク ID を格納する。
CommonName	○	組織名称を UTF-8 でローマ字あるいは英語名で記載する。
SerialNumber	△	保険医療機関番号、保険薬局番号、介護事業所番号、法人番号などを格納する。
SubjectPublicKeyInfo	○	
Algorithm	○	RSAEncryption とする。
SubjectPublicKey	○	
IssuerUniqueID	×	
SubjectUniqueID	×	
Extentions	○	拡張領域（表 7.1.9）参照

表中の、「○」は設定、「△」はオプション、「×」は設定しないことを表す。

表 7.1.9　Web サーバ用証明書のプロファイル（拡張領域 Extensions）

項目	設定	説明	Critical
authorityKeyIdentifier	○		FALSE
keyIdentifier	○	上位証明書の公開鍵の SHA-1 ハッシュ値	
authorityCertIssuer	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）	
directoryName	○	c=JP o= ○○○ ou= ○○○ Centerr cn= HPKI-01-○○○-forAuthentication-forOrganization	
authorityCertSerial	○	上位証明書のシリアル番号	
subejctKeyIdentifier	○	この証明書の公開鍵の SHA-1 ハッシュ値	FALSE
KeyUsage	○	DigitalSignature ｜ KeyEncipherment	TRUE
DeciphermentOnly	×		-
extendedKeyUsage	○	clientAuth｜serverAuth	FALSE
privateKeyUsagePeriod	×		-
certificatePolicies	○		TRUE
policyIdentifier	○		
certPolicyId	○	1.2.392.100495.1.5.1.3.3.1	
policyQualifiers	○		
cPSuri	○	http://×××/	
policyMapping	×		-
subjectAltName	○		FALSE
dnsName	△	FQDN を格納する。	
iPAddress	△	IP アドレスを格納する。	
issuerAltName	×		-
subjectDirectoryAttributes	○		FALSE
basicConstraints	×		-
CA	×		-
pathLenConstraints	×		-
nameConstraints	×		-
policyConstraints	×		-
cRLDistributionPoints	○		FALSE
distributionPoint	○		
fullName	○		
uniformResource Identifier	○	http://×××/××.crl	
subjectInfoAccess	×		-
authorityInfoAccess	×		-

表中の、「○」は設定、「△」はオプション、「×」は設定しないことを表す。

7.1.10　保険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 で定められた表 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 7.1.10 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 7.1.10　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
‘insurance nursing care facility’	介護事業者
‘regional medical information network service provider’	地域医療情報連携ネットワーク事業主体
‘medical information service provider’	医療情報共有サービスを提供する民間事業者

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 CPS 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 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 7.1.10 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’ などの英語表記の資格名を用いる。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。

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。

「○」は設定、「×」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。
OrganizationName	○	o= ○○○
OrganizationUnitName	○	ou= ○○○ Center
CommonName	○	cn= HPKI-01-○○○-forAuthentication-forOrganization
ThisUpdata	○	発行日時（UTCTime で設定する。）
NextUpdate	○	thisUpdate + 96 時間（UTCTime で設定する。）
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	×		-

InvalidityDate	×		-
CertificateIssure	×		-

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
keyIdentifier	○	認証局証明書の公開鍵の SHA-1 ハッシュ値	
authorityCertIssuer	○	CountryName は Printable、それ以外は UTF-8 で記述する	
directoryName		c=JP o= ○○○ ou= ○○○ Center ou= HPKI-01-○○○-forAuthentication-forOrganization	
authorityCertSerial	○	認証局証明書の証明書シリアル番号	
IssuerAltName	×		-
CRLNumber	○	128bit 以下の正の整数	
DeltaCRLIndicator	×		-
IssueingDistributionPoint	×		
FreshesCRL	×		-

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

8.1　監査頻度

本認証局の自己監査は１年に一度の定期監査として実施する。

セキュリティに関する重要な変更などについては、都度、自己監査を実施する。

8.2　監査者の身元・資格

監査人は、本認証局運営部門の要員以外から、認証局代表者の指示に基づいて、選定される。

8.3　監査者と被監査者の関係

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、HPKI-CP 及び本 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、本認証局の情報公開用 Web サイトで公開する。

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

9.2.1　保険の適用範囲

本認証局は、本 CPS「9.6.1 認証局の表明保証」に規定する責任及び義務に違反したことにより、加入者及び検証者に損害を与えた場合には、その損害の賠償責任を負うものとする。ただし、本認証局の責に帰すことができない事由から生じた損害及び逸失利益については、賠償責任を負わないものとする。

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

エンドエンティティに対する保証は、下記のとおりとする。

1. 加入者は、加入者が本 CPS で定める範囲以外の用途に加入者証明書を使用した結果生じたトラブルについては、一切の責任を負うものとする。当該トラブルにより、本

認証局及び検証者に損害を与えた場合には、本認証局及び検証者に対し、加入者の責任において損害賠償を行うものとする。

2. 加入者は、加入者が本 CPS で定める失効申請を怠った結果生じたトラブルについては、一切の責任を負うものとする。当該トラブルにより本認証局及び検証者に損害を与えた場合には、本認証局及び検証者に対し、加入者の責任において損害賠償を行うものとする。

9.3 業務情報の秘密保護

9.3.1 秘密情報の範囲

本認証局が保有する情報のうち、加入者証明書、CRL、本 CPS 等の公開文書を除いた情報が、秘密情報の対象として扱われる。本認証局は、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。本認証局では、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。本認証局は、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

本認証局は加入者証明書及び 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。

- 本 CPS 及びその他本認証局の公開文書
- リポジトリで公開される情報
- 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

本認証局は「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、本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

本認証局において提供するサービスの円滑な運営に必要な範囲で、本認証局の加入者の情報を収集する場合がある。収集した情報は利用目的の範囲内で適切に取り扱う。本認証局では、加入者の情報を本認証局が提供する認証業務のサービスを円滑に運営するために、加入者の組織確認、及び加入者証明書の送付先として利用する。

また、本認証局では、収集した情報について、法令に基づく開示請求があった場合、その他特別な理由のある場合を除き、利用目的以外の目的のために自ら利用、又は第三者に提供しない。更に、本認証局は、収集した情報の漏えい、滅失又はき損の防止その他収集した情報の適切な管理のために必要な措置を講じる。

9.4.2　プライバシーとして保護される情報

本認証局は、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。

- 加入者証明書
- CRL に記載された情報

9.4.4　個人情報を保護する責任

本認証局は「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

本認証局は、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、あらかじめ加入者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、本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

本認証局と加入者との間で別段の合意がなされない限り、本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
- 本 CPS：本認証局に帰属する財産（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

本認証局は、加入者及び検証者に対して次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 CPS の要件に従って行われること。
- 加入者証明書の発行時に、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。
- 本認証局が加入者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 CPS 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もしくは加入者が指定した送付先に確実に届けること。
- 本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、加入者証明書を

確実に失効すること。

- CRL などの重要事項を本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。
- 本認証局の定める方法で、本 CPS 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。
- CA 私有鍵の危殆化のおそれ、CA 証明書又は CA 私有鍵の更新、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 CPS「5　建物・関連施設、運用のセキュリティ管理」及び「6　技術的セキュリティ管理」に従い本認証局を運営し、CA 私有鍵の危殆化を生じさせないこと。
- CA 私有鍵が、加入者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。
- 本認証局の発行する加入者証明書の中で、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。

- 加入者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、登録局にて申請内容の真偽に関する責は負わない。
- 本認証局の発行する加入者証明書の中で、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 CPS「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、また加入者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、加入者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

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

加入者証明書発行申請を行う場合、本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

加入者証明書の記載内容について加入者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、速やかに当該加入者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、本 CPS で定める方法で速やかに届け出ること。

また、加入者証明書情報に変更があった場合は、本 CPS で定める方法で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 CPS 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

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 CPS 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、加入者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、加入者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 CPS「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 点の検証を確実に実施すること。
  - OID 及び Issuer の CN が HPKI-CP の規定に一致していること
  - hcRole 及び keyUsage の DigitalSignature 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

本認証局は、本 CPS「9.6.1　認証局の表明保証」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もしくは派生的損害に対する責任を負わない。

また、本 CPS「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、もしくはその他の第三者において損害が生じた場合、或いは「9.17 その他の条項」の規程により本契約を解除した場合に加入者、或いは企業内 RA に損害が生じても、本認証局は一切の責任を負わない。

9.8　責任制限

本 CPS に規定された責任を果たさなかったことに起因して、本認証局が本サービスの加入者に対して損害を与えた場合、証明書発行手数料を上限として、損害を賠償する。ただし、本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加入者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。

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

- 本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 CPS に規定された責任を果たさなかったことに起因して、本認証局が加入者に対して損害を与えた場合、本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 CPS は、作成された後、本認証局が承認することによって有効となり、また、本CPS「9.10.2　終了」に規定する本 CPS の終了まで有効とする。

9.10.2　終了

本 CPS 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、本認証局が無効と宣言した時点、又は本認証局が本認証業務を終了した時点で無効となる。

9.10.3　終了の影響と存続条項

本認証局が終了した場合であっても、本 CPS「9.3　業務情報の秘密保護」、「9.4　個人情報のプライバシー保護」、「9.5　知的財産権」、「9.8　責任制限」、「9.9　補償」、「9.10.3 終了の影響と存続条項」、「9.13　紛争解決手続」、「9.14　準拠法」及び「9.15　適用法の遵守」の各規定については、なお、効力を有する。

9.11　関係者間の個々の通知と連絡

関係者間の個別通知と報告は、下記のとおりとする。

1. 本認証局は、本認証局から加入者及び検証者への通知方法として、電子メール、郵便及びホームページへの掲示等、本認証局が適当と判断した方法により行う。
2. 電子メールによる通知においては、当該電子メールを本認証局が送信し、送信できたことが確認できた時に通知したものとみなす。
3. 郵便による通知においては、当該郵便の消印日をもって通知したものとみなす。

ホームページへの掲示による通知においては、当該ホームページの掲示を本認証局が行い、閲覧できることが確認できた時に通知したものとみなす。

9.12　改訂

9.12.1　改訂手続き

本認証局は、本 CPS 及び別に定める諸規程の仕様を変更することができる。また、本認証局は、加入者及び検証者に事前の了解を得ることなく、本 CPS に定めた仕様の変更をすることができる。仕様変更の内容は、本認証局での審議を経て、電子認証局代表者が変更を承認する。

9.12.2　通知方法と期間

本認証局は、本 CPS に定めた仕様の変更に関する公開と通知を、下記のとおり行い、変更した本 CPS を公開後 15 日以内に、加入者が自己の加入者証明書の失効申請を行わない場合には、変更に同意したものとみなす。

- 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

規定しない。

9.13　紛争解決手続

加入者又は検証者と本認証局又は○○○との間に、訴訟又は法的行為が起こった場合は、××地方裁判所を専属管轄裁判所とする。

9.14　準拠法

本 CPS は、日本国内法及び規則に基づき解釈されるものとする。

9.15　適用法の遵守

本 CPS 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 CPS は、当事者間の完全合意を構成し、本認証業務について記述された又は申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。本 CPS で定める内容は、書面によらずに修正、変更はできない。

9.16.2　権利譲渡条項

関係者は、本 CPS 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。

- 本認証局が登録局に本 CPS に定める業務の委託を行うとき
- 本 CPS 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 CPS 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

本認証局は、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 CPS「9.7 無保証」の規定により認証局は免責される。

- 加入者又は検証者が、加入者証明書を利用する際に発生したコンピュータシステム等のハードウェア又はソフトウェアへの障害
- 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
- 電気通信事業者が電気通信サービスを中断又は停止した場合
- 認証局の責によらない事由で、本 CPS に基づく義務の遂行上必要とする必須の機器、物品、供給物もしくはサービス（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

本認証局は、以下に定める事由が発生したときには、加入者、或いは加入者の関連組織へ通知または催告をすることなく、加入者、或いは加入者の関連組織との契約を解除できるものとする。

① 加入者が暴力団、暴力団員、暴力団関係者、その他反社会的勢力に準ずる者（以下、 暴力団等という）である場合

② 加入者、或いは加入者の関連組織の代表者、責任者、又は実質的に経営権を有する者が暴力団等である場合、又は、暴力団等への資金提供を行う等、密接な交際のある場合

③ 加入者、或いは加入者の関連組織が自ら又は第三者を利用して、他方当事者に対して、詐術、暴力的行為又は脅迫的言辞を用いた場合

④ 加入者、或いは加入者の関連組織が自ら又は第三者を利用して、他方当事者の名誉や信用等を毀損し、又は、毀損するおそれのある行為をした場合

⑤ 加入者、或いは加入者の関連組織が自ら又は第三者を利用して、他方当事者の業務を妨害した場合、又は、妨害するおそれのある行為をした場合

別紙１．組織情報を証明する書類

加入者の所属する組織が個人事業者の場合、下記「表 A-1 組織情報を証明する書類」に示す書類のいずれか1つにより、組織の確認を行なう。

表 A-1 組織情報を証明する書類

No	書類名	有効期限
1	青色又は白色申告書のコピー	直近年のもの
2	個人事業の開廃業等届出書のコピー	直近のもの
3	所得税の青色申告承認申請書のコピー	直近年のもの
4	建設業の許可申請書または通知のコピー	直近のもの
5	測量業者登録申請書または通知のコピー	直近のもの
6	建築士事務所登録申請書または通知のコピー	直近のもの
7	（産業廃棄物および一般廃棄物） 収集運搬業許可申請書または通知のコピー	直近のもの
8	（産業廃棄物および一般廃棄物） 処分（処理）業許可申請書または通知のコピー	直近のもの
9	貨物自動車運送事業許可申請書または通知のコピー	直近のもの
10	貨物運送取扱事業許可申請書または通知のコピー	直近のもの
11	一般旅客自動車運送事業許可申請書または許可証のコピー	直近のもの
12	特定旅客自動車運送事業許可申請書または許可証のコピー	直近のもの
13	登録証明書等（測量業者登録証明書、建設コンサルタント現況報告書、地質調査業者現況報告書、補償コンサルタント現況報告書、建築士事務所登録証明書、土地家屋調査士登録証明書、計量証明事業者登録証明書、不動産鑑定業者登録証明書、弁理士登録証明書、司法書士登録証明書）のコピー	直近のもの
14	納税証明書のコピー	直近年のもの
15	経営規模等評価結果通知書・総合評定値通知書のコピー	直近のもの
16	その他、公的機関又はこれに準ずる機関の印の付いた証明書、組織責任者の実印の付いた証明書、許可証等のコピー	直近のもの