日本薬剤師会認証局

HPKI 署名用（人）運用規程

version 1.0

平成 24 年 9 月

（公社）日本薬剤師会

改定履歴

版数	日付	内容
1.0	平成 24 年 9 月	初版発行

― 目次 ―

1. はじめに

日本薬剤師会認証局 HPKI 署名用（人）運用規程（以下、本 CPS と呼ぶ。CPS：Certification Practice Statement）は、公益社団法人日本薬剤師会が運営する「日本薬剤師会認証局」（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 証明書ポリシ』（厚生労働省）（以下、HPKI-CP と呼ぶ。）に従う。

また、本 CPS は、以下の文章を参考に構成するものとする。

- RFC3647　Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- ISO/TS 17090-1:2002　Health informatics – Public key infrastructure Part1: Framework and overview
- ISO/TS 17090-2:2002　Health informatics – Public key infrastructure Part2: Certificate profile
- ISO/TS 17090-3:2002　Health informatics – Public key infrastructure Part3: Policy management of certification authority

1.1 概要

本認証局は、「日本薬剤師会認証局 HPKI 署名用（人）証明書」を提供し、日本薬剤師会会員をはじめとする薬剤師国家資格の所有者に対して署名用公開鍵証明書（以下、加入者証明書と呼ぶ。）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 証明書ポリシ」に基づき、個人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。

また、本認証局の電子証明書（以下、CA 証明書と呼ぶ）は、厚生労働省 HPKI ルート認証局から発行され、本認証局は加入者証明書の発行を行う。

1.2 文書の名前と識別

本ドキュメントの名称を「日本薬剤師会認証局 HPKI 署名用（人）運用規程」とする。

本ドキュメント、認証業務運営主体である日本薬剤師会及び加入者証明書のオブジェクト識別子を以下の通りとする。

表 1.2 オブジェクト識別子

名称	オブジェクト名	オブジェクト識別子
日本薬剤師会	Japan Pharmaceutical Association	0.2.440.200134
日本薬剤師会認証局	JPA Certification Authority （JPA	0.2.440.200134.100.1

	CA）	
日本薬剤師会認証局 運用規程	JPA CA CPS	0.2.440.200134.100.1.1
加入者証明書	HPKI 署名用証明書ポリシ	1.2.392.100495.1.5.1.1.3.1

1.3 PKI の関係者

本 CPS は、本認証局により実施される電子証明書発行及び失効業務に適用される。また、本認証局により発行される全ての電子証明書には本 CPS が適用される。

1.3.1 認証局

認証局（Certification Authority , CA）は、発行局（Issuer Authority ,IA）と登録局（Registration Authority , RA）をその構成要素とし、日本薬剤師会により運営される。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（Certificate Revocation List、CRL）を作成、発行する。

1.3.3 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、適切な本人性確認、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、契約を取り交わすことで登録局業務の一部を外部委託することができる。

1.3.4 加入者

加入者とは、本認証局に電子証明書の利用申請を行い、電子証明書を取得し利用する個人をさす。加入者の範囲は次のとおりとする。

- 薬剤師

1.3.5 検証者

検証者とは、本認証局が発行した電子証明書を信頼し、利用する者である。検証者は、本 CPS の内容について理解し、承諾した上で利用するものとする。

1.3.6 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、次に定める利用用途にのみ使用できる。

（1）医療従事者等の保健医療福祉分野サービス提供者の署名検証用

1.4.2 禁止される証明書の使用

本 CPS で定める加入者証明書は、本 CPS「1.4.1 適切な証明書の使用」で定める用途でのみ利用するものとする。それ以外の用途での使用された場合、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 文書を管理する組織

本 CPS の管理組織は、本認証局で定める「認証業務運営会議」とし、日本薬剤師会内に設置する。

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　　：日本薬剤師会　日本薬剤師会認証局　登録事務局
受付時間　　：月曜日から金曜日（土日、祝祭日、年末年始除く）
　　10:00～12:00、13:00～17:00
電話番号　　：03-3353-1170
FAX 番号　　：03-3353-6270
e-mail アドレス：hpki@nichiyaku.or.jp

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、厚生労働省が設置する HPKI 認証局専門家会議である。

1.5.4 CPS 承認手続き

本 CPS は、認証業務運営会議で審査し、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。

・ 暗号化モジュール（Hardware Security Module）

私有鍵を保管するハードウェア装置。私有鍵とそれに対応する公開鍵を生成、格納する耐タンパ性を持つハードウェア装置を表す。

・ 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）
認証局から電子証明書を発行され、電子証明書内に記載された公開鍵に対応する私有鍵を用いて署名操作を行う者。

・ 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。

・ 公開鍵（Public Key）
私有鍵と対になる鍵で、署名の検証に用いる。公開鍵はたとえ公開されても秘密の私有鍵を類推することが困難である。

・ 公開鍵証明書（Public Key Certificate）
公開鍵の所有者の身分を示す証明書で、印鑑証明に相当する。電子証明書あるいは単に証明書ともいう。公開鍵証明書は、公開鍵の所有者情報、公開鍵、CA の情報、CA の署名からなる。

・ 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。

・ 証明書失効リスト（Certificate Revocation List：CRL、Authority Revocation List：ARL）
失効した電子証明書のリスト。
本認証局においては、加入者証明書の失効リストが CRL に記載され、自己署名証明書及びサブ CA 証明書等の失効リストが ARL に記載される。

・ 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

本認証局に電子証明書の利用を申請する主体のこと。

・ 検証者（Relying Party）

文書の署名を公開鍵証明書の公開鍵で検証する者。

・ 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竄されていないことを証明することができる。公開鍵暗号方式と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な第三者機関で、公正、中立な立場にあり信頼できなければならない。

・ 認証局運用規程（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：IA）

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。

・ 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。

・ 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利用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。本認証局におけるルート CA は、厚生労働省 HPKI ルート認証局が該当する。

（A～Z）

・ ARL （Authority Revocation List）
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。本認証局における CA 証明書は、自己署名証明書である。

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

・ CPS（Certification Practice Statement）
認証局運用規程を参照のこと。

・ CRL（Certificate Revocation List）
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 規格で名前を決定することによって、インターネット全体での固有性が保たれる。

・ FIPS 140-1/140-2（Federal Information Processing Standard）

FIPS とは米国連邦情報処理標準で、FIPS140-1/140-2 は暗号化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。

・ SHA1（Secure Hash Algorithm 1）
ハッシュ関数の一つ。任意の長さのデータから 160bit のハッシュ値を作成する。

・ X.500
ITU-T 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 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、24 時間 365 日運用利用可能なものとし、常に最新に保たれるものとする。ただし、システム保守作業等により予め情報公開用 Web サイト等で通知して、一時的に停止することがある。また、緊急時などやむを得ない場合は、事前に通知できない場合もある。

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 サイトは、以下に示す URL にて公開される。

(1) リポジトリ

ldap://ldap.pki.med.or.jp/

(2) 情報公開用 Web サイト

http://www.nichiyaku.or.jp/hpki

2.2 証明書情報の公開

本認証局では､以下の情報をリポジトリあるいは情報公開用 Web サイトを利用して公開する。

(1) リポジトリで公開される情報

以下の情報をリポジトリに格納し、公開する。

- CA 証明書
- CRL

(2) Web サイト上で公開される情報

以下の情報を情報公開用 Web サイト上で公開する。

- 本 CPS
- 日本薬剤師会認証局　利用約款
- 日本薬剤師会 個人情報保護方針
- その他、本認証局が運営基準とする各種基準

2.3 公開の時期又はその頻度

本 CPS「2.2 証明書情報の公開（1）リポジトリで公開される情報」で定めた情報は、情報の変更が確定してから 24 時間以内に更新されるものとする。また、本 CPS「2.2 証明書情報の公開（2）Web サイト上で公開される情報」で定めた情報は、情報の変更が確定してから速やかに更新されるものとする。

2.4 リポジトリへのアクセス管理

本認証局のリポジトリ及び情報公開用 Web サイトに公開された情報は、インターネットを通じて提供される。なお、公開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。

公開情報は、インターネットなどの媒体を使い速やかに提供されるものとする。

3. 識別及び認証

3.1 名称決定

3.1.1 名称の種類

本認証局が発行する電子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（以下、DN と呼ぶ。）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、加入者の氏名（ローマ字表記）および当該加入者の薬剤師名簿登録番号を記載する。

3.1.2 名称が意味を持つことの必要性

本認証局が発行する電子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。

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 CPS「7. 証明書と CRL/ARL 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シリアル番号（SN）を含む。また、認証局の名称（issuerDN）は、保健医療福祉分野 PKI 内で、本認証局を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

商標使用の権利については、商標権所持者が全ての権利を留保するものとする。但し、本認証局は利用申請において、申請者に関する情報に商標が含まれている場合、当該商標を加入者証明書に記載する権利を有するものとする。

また、本認証局は必要に応じ、商標権所持者に対し、商標に関する出願等の公的書類の提出を求めることができる。

3.2 初回の本人性確認

3.2.1 私有鍵の所有を証明する方法

本認証局は、本認証局で加入者公開鍵と加入者私有鍵を生成する。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を IC カードに格納する。

本認証局は、正当な加入者に加入者私有鍵を所有させるため、本人限定受取郵便（特例型）にて郵送する。また、IC カード PIN は、加入者にて指定するため本認証局から加入者に対して IC カード PIN の送付は行わない。

3.2.2 組織の認証

規定しない。

3.2.3 個人の認証

本認証局に電子証明書の利用申請を行う個人は、電子証明書の発行に先立ち、次の何れかの方法で自身の実在性、本人性、申請意思及び国家資格所有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。

（1） 個別申請の場合

■郵送による申請

本認証局に電子証明書の利用申請を行う個人は、以下の書類を登録局に郵送する。
代理人による申請は認めない。

a. 個人の実在性

電子証明書の利用申請を行う個人は、住民票の写しに添えて、利用申請書に当該個人の基本 4 情報を記入し、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。

なお、住民票の写しの有効期間は発行日より 3 ヶ月以内とする。但し、発行する地方公共団体が有効期限を設けている場合は、それを優先する。

b. 個人の本人性

電子証明書の利用申請を行う個人は、次に挙げる書類の何れか 1 点を本認証局が定める様式にコピーしたものに実印を捺印して登録局に郵送することで本人性の立証をしなくてはならない。

【郵送時における本人性の立証書類】

・日本国旅券	・健康保険証
・運転免許証	・国民健康保険証
・住民基本台帳カード（写真付のもの）	・共済組合員証
	・介護保険証
・官公庁職員身分証明書（張り替え防止措置済みの写真付のもの）	・基礎年金番号通知書
	・国民年金手帳（証書）
	・厚生年金手帳（証書）
	・共済年金証書

c. 個人の証明書申請の意思

電子証明書の利用申請を行う個人は、印鑑登録証明書を添えて、利用申請書に実印を捺印することで申請者個人の申請意思を立証しなくてはならない。

なお、印鑑登録証明書の有効期間は発行日より 6 ヶ月以内とする。但し、発行する地方公共団体が有効期限を設けている場合は、それを優先する。

d. 国家資格

電子証明書の利用申請を行う個人は、薬剤師免許証のコピーを登録局に郵送することで国家資格所有の事実を立証しなくてはならない。

この時、薬剤師免許証のコピーの適当な空欄に実印を捺印して、印鑑登録証明書を添えて郵送しなくてはならない。

■郵送以外による申請

本認証局では、郵送による申請を基本とするが、特別な場合においては、認証局への持参、または、それと同等の方法により、対面での申請を認める場合がある。ただし、代理人による申請は認めない。

a. 個人の実在性

電子証明書の利用申請を行う個人は、住民票の写しに添えて、利用申請書に当該個人の基本 4 情報を記入し、それを提出することにより、実在性の立証をしなくてはならない。

なお、住民票の写しの有効期間は発行日より 3 ヶ月以内とする。但し、発行する地方公共団体が有効期限を設けている場合は、それを優先する。

b. 個人の本人性

電子証明書の利用申請を行う個人は、次に挙げる書類の何れか１点を用いて、本人性の立証をしなくてはならない。なお、登録局では本人性の立証に用いた書類の複写を保存する。

【本人性の立証書類】

・日本国旅券 ・運転免許証 ・住民基本台帳カード(写真付のもの) ・官公庁職員身分証明書（張り替え防止措置済みの写真付のもの）

c. 個人の証明書申請の意思

電子証明書の利用申請を行う個人は、利用申請書に記名押印または署名を行うことで申請者個人の申請意思を立証しなくてはならない。

d. 国家資格

電子証明書の利用申請を行う個人は、官公庁の発行した薬剤師免許証の正本を登録局に示すことで国家資格所有の事実を立証しなくてはならない。

なお、登録局では国家資格の確認に用いた書類の複写を保存する。

(2) 都道府県薬剤師会からの団体申請の場合

本認証局は、「1.3.2　登録局」で定める業務の一部を都道府県薬剤師会に委託する場合がある。委託業務として、都道府県薬剤師会の会長に、当該薬剤師会に所属する個人へ証明書を発行する際の審査業務を委託する。この場合、本 CPS「3.2.3 個人の認証（１）」に則った個人の認証を都道府県薬剤師会会長の責任のもと実施しなくてはならない。

「3.2.3 個人の認証　（１）」に定められた審査をどこまで委託するかについては、本認証局と都道府県薬剤師会との間で取り交わす業務委託契約の中で定めるものとする。

本認証局に対しての申請については、利用申請を行う個人が所属する都道府県薬剤師会に対して、利用申請を行う個人が、本認証局と都道府県薬剤師会との間で取り交わす業務委託契約で定められた書類を都道府県薬剤師会に提出する。

都道府県薬剤師会会長は、利用申請を行う個人から提出された書類を纏め、団体申請書を作成し会長印を押印した上、本認証局に郵送する。

3.2.4 確認しない加入者の情報

本認証局は、本 CPS で規定した加入者から提出される書類については記載事項等に漏れが無いことを確認す。

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

加入者が鍵更新申請を行う場合、加入者は更新申請書を本認証局に郵送しなければならない。都道府県薬剤師会からの団体申請の場合は、都道府県薬剤師会会長の責任の元、都道府県薬剤師会経由で更新申請書を郵送しなければならない。

本認証局は、当該更新申請者に対して「4.2.1　本人性及び資格確認」が実施された日から 5 年以内であれば、更新申請書と、「3.2.3　個人の認証」で提出した書類又は本認証局で作成した記録を参照し、記載事項に疑義がないかを確認することにより本人性確認及び認証を行う。

また、更新申請を行う加入者が更新前の加入者証明書で更新申請書に電子署名を実施した場合、加入者は電子署名済み更新申請書を本認証局に送付することが出来る。その場合、本認証局は、送付された更新申請書の署名検証を実施することにより本人性確認及び認証を行うものとする。

当該更新申請者に対して「4.2.1　本人性及び資格確認」が実施された日から 5 年が過ぎていた場合は、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。

3.3.2 証明書失効後の鍵更新時の本人性確認

失効時の鍵更新申請を行う場合、初回の利用申請時と同様の手続きを行うものとする。

3.4 失効申請時の本人性確認及び認証

加入者が本認証局に失効申請を行うときには、次の手順に従うものとする。

（1）失効を申請する電子証明書を特定する。

（2）電子証明書を失効する理由を明らかにする。

（3）申請者が加入者本人又は代理人であることを立証する。

本認証局は、失効申請書の記載内容が当該証明書の利用申請書の記載内容と一致していることにより、失効申請者の同一性を確認する。失効申請の真偽の確認は、失効申請書と利用申請時に提出された印鑑登録証明書により行う。代理人が失効申請する場合は、本認証局から代理人連絡先へ連絡を行い代理人であることを立証する。但し、加入者本人の死亡時は、代理人が加入者の死亡事実が記載された戸籍謄本・抄本、死亡診断書の写しまたは裁判所の審判書の写しを本認証局に提出する。また、利用申請時の印鑑登録証明書の内容に変更があった場合、もしくは、これまで印鑑登録証明書を本認証局に提出していない場合は、有効な印鑑登録証明書の提出が必要となる。

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

4.1.2 加入者証明書の申請者は、薬剤師国家資格を有する者本人とする。 申請手続及び責任

加入者証明書の利用を希望する者は、本認証局が定める以下のいずれかの手続きに従い加入者証明書の利用申請を行う。加入者証明書の利用申請者は、本 CPS 及び利用約款を利用申請の前に読み、内容を理解し、それらに同意した上で利用申請を行うものとする。加入者証明書の利用申請に必要となる利用申請書、本 CPS、利用約款及び申請手順は、情報公開用 Web サイト上での公開を基本とする。

(1) 郵送

本人が登録局に「3.2.3 個人の認証」に定める書類を郵送することにより利用申請を行う。なお、代理人による申請は認めない。

(2) 郵送以外による申請

本認証局では、郵送による申請を基本とするが、特別な場合においては、認証局への持参、または、それと同等の方法により、対面での申請を認める場合がある。ただし、代理人による申請は認めない。

4.2 証明書申請手続

4.2.1 本人性及び資格確認

本認証局は、以下に示す方法により申請者の本人性確認及び資格の確認を行う。

(1) 本人からの申請の場合

薬剤師国家資格所有者への証明書発行

本認証局は、薬剤師国家資格所有者への証明書の発行時、本 CPS「3.2.3 個人の認証」に定める申請者の本人性、実在性、申請意思及び薬剤師国家資格所有の立証に対して、それぞれ以下の方法で真偽の確認を行う。

■郵送による申請

申請者の実在性の確認にあたっては、住民票の写しが少なくとも記載内容、形式、有効期限などにおいて真正であることを確認し、且つ基本 4 情報に関して住民票の写しと利用申請書の記載内容が一致することを確認する。

申請者の本人性の確認にあたっては、本人性の立証書類が少なくとも記載内容、形式、有効期限などにおいて真正であることを確認し、立証書類と利用申請書の記載内容が一致すること、且つ立証書類に捺印された実印の印影と印鑑登録証明書の印影が一致することを確認する。

申請者の申請意思の確認にあたっては、印鑑登録証明書が少なくとも記載内容、形式、有効期限などにおいて真正であることを確認し、且つ利用申請書に捺印された実印の印影と印鑑登録証明書の印影が一致することを確認する。

薬剤師の国家資格所有の確認にあたっては、薬剤師免許証のコピーが少なくとも記載内容、形式、有効期限などにおいて真正であることを確認し、薬剤師免許証と利用申請書の記載内容が一致すること、かつ薬剤師免許証のコピーに捺印された実印の印影と印鑑登録証明書の印影が一致することを確認する。

■郵送以外による申請

申請者の実在性の確認にあたっては、住民票の写しが少なくとも記載内容、形式、有効期限などにおいて真正であることを確認し、且つ基本 4 情報に関して住民票の写しと利用申請書の記載内容が一致することを確認する。

申請者の本人性の確認にあたっては、本人性の立証書類が少なくとも記載内容、形式、有効期限などにおいて真正であることを確認し、立証書類と利用申請書の記載内容が一致するを確認する。

申請者の申請意思の確認にあたっては、申請者への対面での意思確認に加え、利用申請書に申請者による記名押印または署名がなされていることを確認する。

薬剤師の国家資格所有の確認にあたっては、薬剤師免許証の正本が少なくとも記載内容、形式、有効期限などにおいて真正であることを確認し、薬剤師免許証と利用申請書の記載内容が一致することを確認する。

(2) 都道府県薬剤師会からの団体申請の場合

本認証局は、都道府県薬剤師会からの団体申請の場合、申請者本人の本人性、実在性、申請意思及び資格の確認は、日本薬剤師会と都道府県薬剤師会との間で締結される業務委託契約の中で定められ、その業務委託契約に従い審査を実施する。

都道府県薬剤師会長からの申請であるかの確認は、団体申請書に押印された都道府県薬剤師会会長印及び会長氏名が、業務委託契約時に押印される会長印及び会長名であるかを確認することにより実施する。

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、本人性の確認等の審査過程において疑義が生じた場合には、利用申請を不受理とする。

4.2.3 証明書申請手続き期間

証明書利用申請の手続き期間は、原則として本認証局が申請を受付けた後 30 日（土日、祝祭日、年末年始除く）以内とする。また、証明書利用申請の手続き期間は、情報公開 Web サイトでも公開する。

4.3 証明書発行

4.3.1 証明書発行時の認証局の機能

本認証局は､登録された電子証明書申請データの情報をもとに､加入者証明書の発行を行う。なお、加入者証明書の発行指示と同時に加入者鍵ペアは、権限を有する複数人の内部牽制のもと、認証局内で生成される。この生成された加入者公開鍵に、CA 私有鍵で署名を付して加入者証明書を発行する。その後、利用者私有鍵及び利用者証明書は、認証局内で IC カードに格納する。IC カード PIN は、権限のある複数人の内部牽制のもと安全に生成する。また、IC カード格納後、加入者鍵ペア及び IC カード PIN は認証設備から完全に消去する。

本認証局は、正当な加入者に加入者私有鍵を所有させるため、郵送の場合は、IC カードを本人限定受取郵便（特例型）にて加入者本人に送付する。郵送以外の場合は、正当な加入者であることを対面で確認した後、交付する。

4.3.2 証明書発行後の通知

本認証局は、郵送の場合は、電子証明書を加入者に送付することにより電子証明書を発行したことを通知する。郵送以外の場合は、加入者に対面で交付することにより、電子証明書を発行したことを通知する。

4.4 証明書の受理

4.4.1 証明書の受理

郵送の場合、加入者は、加入者証明書及び加入者私有鍵が格納されたICカード、及びICカードPINを受領した後、本認証局がICカードを発送した日付より28日以内に到着するように、加入者本人の実印を押印した受領書を認証局に送付しなければならない。本認証局は、受け取った受領書の実印の印影と利用申請書の実印の印影との照合を行う。

なお、本認証局は、ICカード発送日から28日以内に受領書が返信されなかった場合、当該加入者証明書を失効する権限を有する。

対面による交付の場合、加入者は、加入者証明書及び加入者私有鍵が格納されたICカードを受領した後､その場で受領書に記名押印または署名をし､認証局に提出しなければならない。

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を行わない。

4.4.3 他のエンティティに対する証明書発行通知

規定しない。

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、加入者私有鍵を電子署名にのみ利用する。

4.5.2 検証者の公開鍵と証明書の利用目的

検証者は、署名検証の用途で加入者の公開鍵と加入者証明書を利用する。加入者証明書の利用に際しては、本CPS「9.6.4 検証者の表明保証」及び情報公開用Webサイト上にて公開する検証者に対する免責規定に規定された内容について同意しなければならない。

4.6 証明書更新

認証局が発行する全ての電子証明書の更新は鍵ペアの更新を伴うものとし、鍵ペアの更新を伴わない証明書発行は行わない。鍵ペアの更新を伴う証明書更新の要件については､本CPS「4.7 証明書の鍵更新（鍵更新を伴う証明書更新）」に規定する。

4.6.1 証明書更新の要件

規定しない。

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 証明書にる更新証明書の公開

規定しない。

4.6.7 他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）

電子証明書の有効期限切れに伴う証明書更新は、鍵ペアの更新を伴うものとする。

4.7.1 証明書鍵更新の要件

本認証局は、以下の条件を満たす時に証明書の更新申請を受け付ける。

- 更新対象証明書が存在すること。
- 証明書が有効期限終了前のものであること。
- 証明書が失効されていないこと。
- 有効期限終了前で、認証局で定める期間に申請があったこと。

4.7.2 鍵更新申請者

本 CPS「4.1.1　証明書申請者」に定める者からの申請を受け付ける。

4.7.3 鍵更新申請の処理手順

本 CPS「4.2.1　本人性及び資格確認に定める本人性確認並びに資格確認を行う。

但し、本認証局で「4.2.1　本人性及び資格確認」に定める本人確認が完了した日から 5 年以内の場合であれば、本認証局は、上記の代わりに更新申請書に当該加入者証明書による電子署名を実施した電子ファイルをオンラインで受け取り、当該電子ファイルの電子署名を検証することにより本人確認を実施する。

オンラインによる申請方法については、本認証局の情報公開用 Web サイト上で公開する。

4.7.4 加入者への新証明書発行通知

本 CPS「4.3 証明書発行」に示す初回の証明書発行時と同様の通知方法とする。

4.7.5 鍵更新された証明書の受理

本 CPS「4.4.1 証明書の受理」に示す初回の証明書発行時と同様の受理手順とする。

4.7.6 認証局による鍵更新証明書の公開

本認証局は、加入者証明書の公開を行わない。

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

本認証局は、「4.8.1 証明書変更の要件」に示す加入者証明書の記載事項に変更が生じた場合、加入者証明書のみの変更は行わず、当該加入者証明書を失効させ、新規に鍵ペアの生成及び証明書発行を行うものとする。これ以外の変更に関する届出の手続きについては、本 CPS「9.6.2 加入者の表明保証」に示す。

4.8.1 証明書変更の要件

規定しない。

4.8.2 証明書変更申請者

規定しない。

4.8.3 変更申請の処理手順

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、以下に示す場合に加入者証明書を失効するものとする。

(1) 認証局による失効要件

本認証局は、以下に示す加入者証明書の失効事由が発生した場合は、加入者証明書を失効する権限を有するものとする。

- 加入者が本 CPS 及び利用約款に基づく義務に違反した場合
- 加入者私有鍵が危殆化若しくはその恐れがあると本認証局が認めた場合
- 加入者私有鍵又は加入者証明書が不正利用された場合、若しくはその危険性があると本認証局が認めた場合
- 本認証局の CA 私有鍵が危殆化若しくはその恐れがある場合
- 加入者証明書を発送した日から 28 日以内に受領書が本認証局に返送されなかった場合
- 加入者証明書の記載情報に事実と相違があり、又はその情報が変更されたことを本認証局が確認した場合
- 加入者の解散を認証局が確認した場合
- 加入者証明書の規格変更がなされた場合
- その他、本認証局が必要と判断した場合

(2) 加入者による失効要件

加入者は、以下の場合には、直ちにその旨を本認証局に報告し、加入者証明書の失効申請を行わなければならない。なお、本認証局は、加入者若しくはその代理人からの失効申請であると確認した場合、理由の如何に関わらず加入者証明書の失効を行う。

- 加入者証明書の記載事項が事実と異なる場合
- 加入者証明書の記載事項に変更が生じた場合

- IC カードを紛失あるいは破損した場合
- IC カードの盗難あるいは不正使用などを知った場合
- IC カード PIN の紛失、漏洩等による不正使用などを知った場合
- IC カード PIN の入力ミスで IC カードが使用できなくなった場合
- 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
- 加入者証明書の国家資格に変更が生じた場合
- その他、加入者が加入者証明書の失効の必要性を判断した場合

(3) 代理人による失効要件

代理人は、以下の場合に限り本認証局に失効申請することができる。なお、本認証局は、代理人からの失効申請であると確認した場合、理由の如何に関わらず加入者証明書の失効を行う。

・加入者が死亡した場合

4.9.2 失効申請者

本認証局は、次の 1 人又はそれ以上の者からの失効申請を受け付ける。

(1) 本人の名前で証明書が発行された加入者若しくはその代理人

(2) 本認証局員

4.9.3 失効申請の処理手順

本認証局は、失効申請の受領の判断を行い受理する場合は、本 CPS「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) 加入者本人からの失効申請の場合

a. 失効申請

加入者は、加入者証明書の失効を申請する場合、「日本薬剤師会認証局　失効申請書」（以下、失効申請書と呼ぶ。）を本認証局へ郵送する。緊急を要する失効要求の場合、失効申請書を本認証局宛てにメールまたはファクシミリにより通知し、原本を郵送する。なお、失効申請書は情報公開用 Web サイトにて掲載公開しているものを利用する。

b. 失効申請者の本人性確認の方法

本認証局は、加入者証明書の失効申請を受け取った後、失効申請に必要な書類に不備がないこと、失効申請書の記載内容が当該証明書の利用申請書の記載内容と一致していることを確認する。また、失効申請書に記載された失効理由を確認し、その真偽について確認を行う。

失効申請者の本人性確認は、失効申請書に押印されている印影と利用申請時に提出された印鑑登録証明書の印影を照合することにより行う。なお、利用申請時の印鑑登録証明書の内容に変更があった場合、もしくは、これまで印鑑登録証明書を本認証局に提出していない場合は、有効な印鑑登録証明書の提出が必要となる。

c. 失効処理

失効申請者の本人性確認を行い、失効申請が失効要件に該当するか確認した上で、加入者証明書の失効処理を行い、CRL を発行するとともにリポジトリに公開する。また、加入者証明書を失効した場合は、失効した事実を遅滞なく当該加入者に通知する。

(2) 加入者の代理人からの失効申請の場合

a. 失効申請

加入者の代理人は、加入者証明書の失効を申請する場合、失効申請書を本認証局へ郵送する。緊急を要する失効要求の場合、失効申請書を本認証局宛てにメールまたはファクシミリにより通知し、原本を郵送する。なお、失効申請書は情報公開用 Web サイトにて掲載公開しているものを利用する。

b. 失効申請者の正当性確認の方法

本認証局は、加入者証明書の失効申請を受け取った後、失効申請に必要な書類に不備がないこと、失効申請書の記載内容が当該証明書の利用申請書の記載内容と一致していることを確認する。また、失効申請書に記載された失効理由を確認し、その真偽について確認を行う。

加入者の代理人への本人確認は、失効申請書記載の代理人連絡先に電話連絡を実施し代理人であることを確認する。但し、加入者本人の死亡時は、死亡事実が記載された戸籍謄本・抄本、死亡診断書の写しまたは裁判所の審判書の写しにより確認する。

c. 失効処理

失効申請者の正当性の確認を行い、失効申請が失効要件に該当するか確認した上で、加入者証明書の失効処理を行い、CRL を発行するとともにリポジトリに公開する。また、加入者証明書を失効した場合は、失効した事実を遅滞なく当該加入者および代理人に通知する。

(3) 認証局による失効の場合

本認証局は、「4.9.1 証明書失効の要件」に定めた認証局による失効要件に基づく本認証局員からの失効申請があった場合、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行う。失効事由が事実であった場合は速やかに当該加入者証明書の失効処理

を行い、CRL を発行するとともにリポジトリに公開する。また、加入者証明書を失効した場合は、失効した事実を遅滞なく当該加入者に通知する。

4.9.4 失効における猶予期間

加入者は、本 CPS「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

本認証局は、加入者証明書の失効申請を受付けた場合、速やかに失効可否を判断し、当該証明書の失効を行う。

4.9.6 検証者の失効情報確認の要件

検証者は、電子証明書が失効していないことをリポジトリに格納された CRL により確認しなければならない。

なお、加入者証明書の有効期間が終了した場合も当該証明書に係る証明書失効情報は 5 年間 CRL に掲載される。本認証局は、CRL 掲載情報以外の失効の問合せには応じない。

4.9.7 CRL 発行頻度

本認証局は、電子証明書が失効されてから 48 時間以内に 96 時間有効な CRL を発行する。また、変更がない場合においても、前回発行された時から 48 時間以内に 96 時間有効な 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 48 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

利用しない。

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

利用しない。

4.9.12 鍵の危殆化に関する特別な要件

本 CPS「5.7 危殆化及び災害からの復旧」の要件に従う。

4.9.13 証明書一時停止の要件

電子証明書の一時停止は行わない。

4.9.14 一時停止申請者

電子証明書の一時停止は行わない。

4.9.15 一時停止申請の処理手順

電子証明書の一時停止は行わない。

4.9.16 一時停止期間の制限

電子証明書の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

加入者は、加入者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

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、預託されないものとする。また、私有鍵の回復も行わない。

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、隔壁により区画されていて、施錠できることとする。認証局システムを設置する施設（認証設備室）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。

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、二人以上の複数の者による監視の下で行う。

また、認証設備室は、適切なアクセスコントロールを実施し、入退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。

認証事務室で作業を実施する際は、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する。なお、認証事務に用いる機器・資料等の全ては、通常は、本会の鍵管理規定のある設備に保管しておき、認証事務作業を実施する際に所定の手続きをし、必要な機器・資料等を取り出し作業を開始する。作業終了後は、認証事務に用いる機器・資料等の全てを、再度、本会の鍵管理規定のある設備に保管する。

5.1.3 電源及び空調

認証設備が設置された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

認証設備が設置された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

バックアップデータを記録した媒体は、入退室が管理されたセキュアな場所に保管される。また、所定の手続きに基づいて適切に搬入出を行う。

5.1.7 廃棄物の処理

本認証局で扱う重要な情報（機密情報、私有鍵、電子証明書）を記録した紙及び電子媒体の廃棄は、以下の方法により復元できないように廃棄する。

(1) 重要な情報を記録した紙

シュレッダーにかけた後、廃棄する。

(2) 重要な情報を記録した磁気媒体若しくは光媒体

データ抹消用のアプリケーションを使用し、再び復元できないように情報を抹消する。若しくは、物理的に破壊した後に廃棄する。

(3) 重要な情報を記録した IC カード

IC カードチップを物理的に破壊した後に廃棄する。

(4) 重要な情報を記録したコンピュータ機器

データ抹消用のアプリケーションを使用し、再び復元できないように情報を抹消する。若しくは、物理的に破壊した後に廃棄する。

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 ・認証局運用に係る要員の任命と解任および人事管理 ・本 CPS の承認 ・CA 秘密鍵の危殆化、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 ・生成された CA 秘密鍵のバックアップの保管
審査登録業務責任者	・認証事務室内全ての設備に対する維持・管理の実施と管理 ・審査、登録、発行業務の実施と監督
受付審査担当者	・証明書の審査登録業務 ・CA システムへの登録情報及び失効情報の生成
RA 操作員	・証明書の審査登録業務 ・利用申込みが許可された利用者情報の CA システムへの登録 ・CA システムへの利用者証明書失効処理
認証業務責任者	・認証設備室認証業務用設備を含む IC カード発行室内全ての設備に対する維持・管理の実施と管理 ・証明書の発行、失効業務の監督 ・上級 IA 操作員との合議制操作による CA 秘密鍵の生成 ・生成された CA 秘密鍵のバックアップの保管
上級 IA 操作員	・証明書の発行、失効業務 ・認証業務責任者との合議制操作による CA 秘密鍵の生成 ・一般 IA 操作員との合議制操作による CA システムの起動および停止 ・一般 IA 操作員との合議制操作による CA 秘密鍵のアクティベーションおよび非アクティベーション
一般 IA 操作員	・証明書の発行、失効業務 ・上級 IA 操作員との合議制操作による CA システムの起動および停止 ・上級 IA 操作員との合議制操作による CA 秘密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され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 職務分離が必要となる役割

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し、発行局 の業務に携わる者は、本認証局代表者の厳重な管理下に置かれる。また、管理者の承認を受けることなく、認証設備へのアクセスは禁止する。

5.3 要因管理

5.3.1 資格、経験及び身分証明の要件

本認証局の業務に従事する者は、役割と責任に応じて、PKI、セキュリティ等の業務遂行に必要な知識、経験を有する者とする。

また、認証局員の任命の際は、本認証業務によって知り得た情報に対する秘密保持誓約の承諾を得る。

5.3.2 経歴の調査手続

日本薬剤師会で定める職務規定に従うものとする。

5.3.3 研修要件

本認証局の運用に関わる認証局員全員に対して、教育・訓練を行う。

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罰則

認証局員は、故意、過失に関わらず許可されていない行為を行った場合、日本医師会の職務規定に基づき処罰される。

5.3.7 独立した契約書の要件

認証局員は、認証局に関わるための秘密保持誓約書へ署名を行う。

但し、認証業務の一部を外部委託する場合、日本薬剤師会と業務委託先との間で秘密保持契約を締結するものとし、業務委託先の担当者はその契約で締結される秘密保持義務を遵守するものとする。

5.3.8 要員へ提供する文書

認証局員は、その役割、権限に応じた文書にアクセスすることができる。

5.4 監査ログの取扱い

5.4.1 記録するイベントの種類

本認証局が執り行う全ての業務及び、各システム機器やネットワーク周辺の重要な事象を対象に、システム機器毎のアクセスログ、操作ログ、認証ログやその他のログを記録する。これらのログを総称し、監査ログと呼ぶ。

監査ログには、以下の項目を含める。

- 各イベントを起こした主体
- 各イベントの種類
- 各イベントの発生日時
- 各イベントの成否

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 度以上の頻度で定期的に検査するものとする。

5.4.3 監査ログを保存する期間

監査ログは、その重要度に応じて、本 CPS「5.5.2 アーカイブ保管期間」で定める期間保存される。

5.4.4 監査ログの保護

監査ログは、定期的に改ざん困難な電子媒体により保存され、保護される。監査ログの閲覧・削除等の処置は権限者のみが行えるものとする。

保存された記録媒体は、本 CPS「5.5.3 アーカイブの保護」で定める方法で保護されるものとする。

5.4.5 監査ログのバックアップ手続

各システム機器において記録された監査ログは、周期的に且つ自動的に別媒体にバックアップされる。バックアップを保存した電子媒体は、施錠付き書庫に保管する。

5.4.6 監査ログの収集システム（内部対外部）

監査ログの収集システムは、各システム機器に内在している。

5.4.7 イベントを引き起こしたサブジェクトへの通知

イベントを引き起こした人への通知は行わない。

5.4.8 脆弱性評価

認証業務用設備については、定期的に脆弱性評価を行う。

5.5 記録の保管

本節では、CA における運用業務関係情報の取り扱いについて規定する。

本認証局は、以下対象となる関係情報（電子的データ及び書類）を適切に保存し、閲覧権限のあるものに対してのみ参照可能とする。保存にあたっては、その取り扱いに注意する。

5.5.1 アーカイブ記録の種類

本認証局では、以下の関係情報をアーカイブ記録として保存する。

（1） 証明書の発行申請に関する文書

- 利用申請書/更新申請書
- 団体申請書

・ 加入者の住民票の写し
・ 加入者の印鑑登録証明書
・ 加入者の薬剤師免許証のコピー
・ 加入者の本人性の立証書類のコピー
・ 加入者から提出される証明書の受領についての書類

その他、証明書の発行の許諾に関する書類等、証明書の発行の際における内部処理の記録は、本認証局で規定された方法に従い保存する。

(2) 証明書の失効申請に関する文書
・ 失効申請書
・ 代理人の立証書類のコピー

その他、証明書失効を決定した者に関する書類等、証明書失効する際における内部処理の記録は、本認証局で規定された方法に従い保存する。

(3) 認証局が発行した全ての電子証明書（CA 証明書、加入者証明書）及び CRL

(4) 認証局の組織管理に関する文書
・ 本 CPS 及びその改訂に関する記録
・ 本認証局の要員任命、体制、指揮命令系統などに関する記録
・ 準拠性監査に関する記録
・ 認証業務の一部を他に委託する場合の委託契約書及び関係する書類

その他、本認証局の組織管理における内部文書及び内部処理の記録は、本認証局で規定された方法に従い保存する。

(5) 設備及び安全対策措置に関する文書
・ 障害及びその復旧に関する記録
・ 不正アクセスがあった際のアクセスログ
・ CA 私有鍵管理（鍵生成、保管、活性化／非活性化、バックアップ／リストア、廃棄）と対応する自己署名証明書発行実施に伴う記録

その他、本認証局の設備や安全対策に関する内部処理の記録は、本認証局で規定された方法に従い保存する。

5.5.2 アーカイブを保存する期間

記録を保存する期間は以下のように定める。

(1) 5.5.1（1）～（4）の文書

当該記録書類にかかる電子証明書の有効期限が満了してから 10 年間保存する。

（2） 5.5.1（5）の文書

当該記録書類を作成又は記録した日から 10 年間保存する。

5.5.3 アーカイブの保護

本認証局で規定された範囲の情報を規定された閲覧権限者にのみ公開するものとする。保管に関しては、改ざん・流出などへの防止措置を取るため、書類は原本を本会の鍵管理規定のある設備に保管する。

なお、個人の署名若しくは押印を求めない記録は、電子媒体（光媒体又は磁気媒体）での保存で対応することができるものとする。

5.5.4 アーカイブのバックアップ手続

電子データの複製（バックアップ）を作成する場合、複数人によりセキュリティ上安全な場所にて実施する。紙媒体については、原本のみを安全に保管する。

また、本認証局は電子的に保存されている情報に関し、その可読性を常に維持するために当該電子媒体の内容を表示可能な機器、ソフトウェアを維持・保管する。機器、ソフトウェアの維持・管理が困難な場合には、当該電子媒体の内容を表示可能な新たな電子媒体へ移すことによってその可読性を維持するものとする。また、この複製の作成にあたっては、複製の完全性・機密性を維持する。

5.5.5 記録にタイムスタンプをつける要件

保存対象となる情報において、日時の記録が必要なものは、原則として日本標準時間を基に記録する。

5.5.6 アーカイブ収集システム（内部対外部）

保存対象となる情報の収集に関しては、常に処理実行者の他に内部牽制のために同伴者を伴い処理を実行する。

5.5.7 アーカイブ情報を入手し、検証する手続

本 CPS 規程「5.5.1　アーカイブの記録の種類」で規定する情報については、本規程「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

本認証局は、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、専用の暗号化モジュール（HSM）を用いて生成される。

CA 私有鍵の更新と共に CA 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。

CA 証明書の更新実行後、本認証局は新しい CA 証明書、CRL を速やかにリポジトリにて公開する。

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

本認証局は、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、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、障害発生時の際には、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危殆化の恐れが生じた場合は、日本薬剤師会役員の判断により、速やかに厚生労働省 HPKI 認証局に連絡を行い認証業務を停止するとともに、本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、本認証局で規定された手続きに基づき、日本医師会常任理事会の判断により対策を決定し、構成労働省 HPKI 認証局に連絡し、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

本認証業務を終了する場合は、業務終了の 60 日前までに、加入者にメールによる通知を行い、認証業務の終了日までに、当該認証業務によって発行された全ての加入者証明書を失効し、リポジトリに CRL を公開し、本認証局で規定された業務終了手続きを行う。また、検証者等に対しては、情報公開用 Web サイトにて業務終了等の告知を行う。

登録局の運用を停止する場合は、登録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。なお、登録局は、このような場合に他の登録局に加入者の情報や運営を他の登録局に移管することについて、事前に加入者の同意を得るものとする。

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化モジュール（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

本認証局で生成した加入者私有鍵は、本認証局内で安全に IC カードに格納され、加入者の住民票の写しに記載の住所へ本人限定受取郵便（特例型）で郵送する。なお、認証局で生成した加入者私有鍵は、IC カードに格納後、遅滞なく認証設備から完全に消去される。

6.1.3 認証局への公開鍵の送付

規定しない。

6.1.4 検証者への CA 公開鍵の配布

CA 公開鍵は、厚生労働省 HPKI 認証局のサブ認証局証明書の形式で配布される。

本認証局は、CA 証明書をリポジトリに格納し、公開する。

6.1.5 鍵のサイズ

本認証局が発行する自己署名証明書に係る鍵は、RSA アルゴリズムで、2048bit とする。加入者証明書に係る鍵は、RSA アルゴリズムで、1024bit 以上の鍵を利用する。

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、信頼できる暗号化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は、暗号化モジュールにより行われる。

6.1.7 鍵の使用目的

本認証局の鍵は、keyCertSign と cRLSign とする。

加入者証明書に係る鍵は、nonRepudiation とする。

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と管理

本認証局の私有鍵の格納モジュールは、FIPS 140-2 レベル 3 の認定を取得したものを用いる。

加入者私有鍵の格納モジュールは、FIPS140-2 レベル 1 相当の IC カードを用いる。

6.2.2 複数人による私有鍵の管理

CA 私有鍵に関わる暗号化モジュールの操作は、認証設備室内において権限を有する複数人の立会いのもとで行う。

6.2.3 私有鍵のエスクロウ

法律によって必要とされる場合を除き、CA 私有鍵の預託は行わない。

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、認証設備室内において権限を有する複数人の立会いのもとで行う。また、バックアップデータは暗号化され、リストアに必要な CA 私有鍵に関する情報は分散され、分散された各断片はそれぞれ異なる場所にある金庫に保管する。

6.2.5 私有鍵のアーカイブ

本認証局は、加入者私有鍵のアーカイブは行わない。

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、認証設備室内にある暗号化モジュール内に暗号化されて格納される。

6.2.7 暗号モジュールへの私有鍵の格納

加入者私有鍵は、安全な方法で暗号モジュールに入力する。

6.2.8 私有鍵の活性化方法

CA 私有鍵は、認証設備室内にある暗号化モジュール内で活性化される。この操作は、権限を有する複数人の立会いのもとで行う。

6.2.9 私有鍵の非活性化方法

CA 私有鍵は、認証設備室内にある暗号化モジュール内で非活性化される。この操作は、権限を有する複数人の立会いのもとで行う。

6.2.10 私有鍵の廃棄方法

CA 私有鍵の廃棄は、複数人の立会いのもとで復元不可能な方法により執り行われる。また、CA 私有鍵のバックアップ媒体も CA 私有鍵の廃棄作業の一環として、物理的に破壊する。

6.2.11 暗号モジュールの評価

本認証局の私有鍵の格納モジュールは、FIPS 140-2 レベル 3 の認定を取得し、日本国内において稼動実績があるものを使用する。

加入者私有鍵の格納モジュールは、FIPS140-2 レベル 1 相当の IC カードを用いる。

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

公開鍵のアーカイブは、それを含む電子証明書を保管することによって行う。

CA 証明書及び加入者証明書は、その有効期間が満了してから 10 年間保管するものとする。

6.3.2 公開鍵証明書の有効期間と鍵ペアの使用期間

本認証局の私有鍵の有効期間は 10 年とし、公開鍵の有効期間は 20 年とする。但し、鍵長に対する暗号セキュリティが容認できないほど脆弱になった場合は、10 年より早く鍵ペアの更新を行う場合がある。

加入者の私有鍵の有効期間は 2 年とし、公開鍵の有効期間は 5 年とする。

6.4 活性化データ

6.4.1 活性化データの生成とインストール

本認証局において用いられる CA 私有鍵を含む全ての活性化データの生成とインストールは、本認証局で定められた規定に従い実施される。

6.4.2 活性化データの保護

本認証局において用いられる活性化データは、本認証局で定められた規定に従い保護される。

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

認証設備へのアクセスは、予めアクセス権限を設定された者のみが可能であり、電子証明書もしくは ID・パスワードによる操作者の認証を行う機能を備え、操作者を特定できる。

また、認証設備間の通信においては、各認証設備の認証や、通信内容の盗聴及び改ざんの防止措置を講じている。

6.5.2 コンピュータセキュリティ評価

規定しない。

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

本認証局で使用されるソフトウェアは、適切な品質管理及びセキュリティのもとで日本医師会により開発されたものである。

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

認証設備は、外部ネットワークに対してファイアウォールを介して接続を行うとともに、不正侵入検知システムを導入するなど十分なセキュリティ保護対策を講じている。

また、認証設備間の通信においては、各認証設備の認証や、通信内容の盗聴及び改ざんの防止措置を講じている。

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・時刻を使用するため、NTP サービスによる時刻同期を行う。

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電子証明書は、X.509 バージョン 3 フォーマット証明書形式により作成され、また電子証明書は X.500 識別名（DN）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、表 7.1.2、表 7.1.3 及び表 7.1.4 に記載する。

7.1.1 バージョン番号

本認証局が発行する電子証明書は、X.509 バージョン 3 フォーマット証明書形式により作成される。

7.1.2 証明書の拡張領域（保健医療福祉分野の属性含む）

本認証局が発行する電子証明書における拡張領域を以下の表 7.1 に示す。

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

表 7.1　証明書の拡張領域

No	領域名	Critical	CA 証明書	加入者 証明書
1	authorityKeyID	FALSE	○	○
1-1	keyIdentifier		○	○
1-2	authCertIssuer		○	×
1-3	authCertSerialNumber		○	×
2	subjectKeyID	FALSE	○	○
3	keyUsage	FALSE	○	○
4	privateKeyUsagePeriod	FALSE	×	×
5	certificatePolicies	FALSE	○	○
5-1	policyIdentifier		○	○
5-2	policyQualifiers		○	○
6	policyMappings	TRUE/ FALSE	×	×
7	subjectAltName	FALSE	×	△
8	issuerAltName	FALSE	×	△
9	subjectDirectoryAttrs	FALSE	×	○

9-1	attrType		×	△
9-2	attrValues		×	△
10	basicConstraints	TRUE	○	×
10-1	cA		○	×
10-2	pathLenConstraints		×	×
11	nameConstraints	TRUE	×	×
12	policyConstraints	TRUE	×	×
13	extKeyUsage	TRUE/ FALSE	×	×
14	cRLDistributionPts	FALSE	○	○
14-1	distributionPoint		○	○
14-2	reasons		×	×
14-3	cRLIssuer		×	×
15	inhibitAnyPolicy	TRUE	×	×
16	freshestCRL	FALSE	×	×
17	authorityInfoAccess	FALSE	×	△
18	subjectInfoAccess	FALSE	×	×
19	qcStatements	TRUE/ FALSE	×	×

○：必須、×：省略、△：オプション

7.1.3 アルゴリズムオブジェクト識別子

本認証局が発行する電子証明書及び CRL における署名アルゴリズムは、SHA1withRSAEncryption（1.2.840.113549.1.1.5）であり、各電子証明書に記載される電子証明書発行者の公開鍵アルゴリズムは、RSAEncryption（1.2.840.113549.1.1.1）である。

7.1.4 名前の形式

本認証局が発行する各電子証明書における設定内容を以下の表 7.2、表 7.3 に示す。

表 7.2　サブ CA 証明書形式解釈ルール

領域名	識別子	例	解釈のルール	エンコーディング方式
subject	C	JP	電子証明書発行者の国名	PrintableString
	O	Japan Medical Association	電子証明書発行者の組織名のローマ字表記	UTF8String

	CN	HPKI-01- -forNonRep udiation	電子証明書発行者のローマ字表記	UTF8String

表 7.3　加入者証明書の名前の形式解釈ルール

領域名	識別子	例	解釈のルール	エンコーディング方式
Issuer	C	JP	電子証明書発行者の国名	PrintableString
	O	Japan Medical Association	電子証明書発行者の組織名のローマ字表記	UTF8String
	CN	HPKI-01-JMA-CA-forNonRepudiation	電子証明書発行者のローマ字表記	UTF8String
subject	C	JP	電子証明書所有者の国名	PrintableString
	O	（例） JMARI	電子証明書所有者が管理権限を持つ組織名のローマ字表記または英字表記 （管理者の場合のみ記載）	UTF8String
	OU	Director	Director （管理者の場合のみ記載）	UTF8String
	CN	（例） NICHII TARO	電子証明書所有者の氏名 ローマ字表記	UTF8String
	SN	（例） 1234567890	電子証明書所有者の医籍登録番号	UTF8String

7.1.5 名前制約

用いない。

7.1.6 CP オブジェクト識別子

認証局が発行する電子証明書の certificatePolicies に記載される CP オブジェクト識別子は、「1.2.392.100495.1.5.1.1.3.1」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

規定しない。

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。

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 CPS では、HPKI-CP に従い、ISO TS 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 CPS では coding scheme reference の OID として ISO coding scheme reference を用いず、HPKI-CP で定められた表 7.3 の資格名を参照する 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。資格名は、表 7.4 に示すように英語表記を用い UTF8string 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。

本拡張は、加入者が国家資格保有者及び医療機関等の管理者の場合は必須とする。

表 7.4　HPKI 資格名テーブル（codeDataFreeText の定義）

資格名（国家資格）	説明
‘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
資格名（医療機関の管理責任者）	説明
‘Director of Hospital’	病院長
‘Director of Clinic’	診療所院長
‘Director of Pharmacy’	管理薬剤師
‘Director’	その他の保健医療福祉機関の管理責任者

注）資格名のワード間の空白は一個の Space (x20)とする。

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、管理薬剤師を 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 及び OrganizationUnitName は必須で、OrganizationName に保健医療福祉機関名を英語又はローマ字で格納し、OrganizationUnitName に”Director”の文字列を格納する。

(2) HPKI hcRole 属性プロファイル

本 CPS では、HPKI-CP に従い、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 CPS 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 7.4 の資格名を参照する。

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

Note4 : 本 CPS では、codeDataFreeText としての DirecroryString には表 7.4 に規定した ‘Medical Doctor’ 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

本認証局が発行する CRL/ARL のプロファイルの詳細は、別紙 B に記載する。

7.2.1 バージョン番号

本認証局が発行する 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。

7.2.2 CRL と CRL エントリ拡張領域

本認証局が発行する CRL における拡張領域を以下の表 7.5 に示す。

表 7.5　CRL/の拡張領域

No	領域名	Critical	CRL
crlEntryExtensions			
1	reasonCode	FALSE	○
2	holdInstructionCode	FALSE	×
3	invalidityDate	FALSE	×
4	certificateIssuer	TRUE	×
crlExtensions			
5	authorityKeyID	FALSE	○
5-1	keyIdentifier		○
5-2	authCertIssuer		×
5-3	authCertSerialNumber		×
6	issuerAltName	FALSE	×
7	cRLNumber	FALSE	○
8	deltaCRLIndicator	TRUE	×
9	issuingDistributionPt	TRUE	△
9-1	distributionPoint		△
9-2	onlyContsUserCerts		△
9-3	onlyContsCACerts		×
9-4	onlySomeReasons		×
9-5	indirectCRL		×
9-6	onlyContsAttrCerts		×
10	freshestCRL	FALSE	×

○：必須、×：省略、△：オプション

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

本認証局は、認証局代表者が指定する監査人によって、1 年に 1 回の頻度で HPKI-CP への準拠性監査を実施する。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。

8.2 監査者の身元・資格

監査者には、システム監査、PKI 及びシステムセキュリティに関する知識と技能を持ち合わせる者が任命される。

8.3 監査者と被監査者の関係

監査者は、公正な準拠性監査を遂行するため、本認証局の運用管理部門以外の監査領域対象から完全に独立し、本認証局との特別な利害関係を持たない者とする。

8.4 監査テーマ

準拠性監査の監査項目は、HPKI-CP、本 CPS 及び事務取扱要領に準拠していることを中心に監査を実施する。

8.5 監査指摘事項への対応

本認証局は、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

本認証局は、証明書の信頼性に影響する重大な欠陥が発見された場合を除き、監査結果を公表しない。証明書の信頼性に影響する重大な欠陥が発見された場合は、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。但し、本認証局は、本認証局の監査人又は法的根拠に基づく開示要求の下で法執行機関に対し監査結果を公表することもある。

9. その他の事業上と法務上の事項

9.1 料金

本認証局に関わる料金が発生する場合は、本 CPS では定めず、情報公開用 Web サイトに記載する。

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

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 事業情報の機密保護

9.3.1 機密情報の範囲

日本薬剤師会認証局においては、次の情報を秘密情報とする。

- 監査ログ・監査記録その他認証局のシステムで生成される情報で、本 CPS 「9.3.2 機密情報の範囲外の情報」で規定された項目以外の情報
- 情報提供者との間であらかじめ機密情報である旨合意され、その旨表示されている情報
- その他、公開することによって認証局のセキュリティに危険を生じる情報

9.3.2 機密情報の範囲外の情報

次の情報は秘密情報として扱わない。

- 電子証明書に含まれている情報
- CRL に含まれている情報
- 本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 機密情報を保護する責任

本認証局は、本 CPS「9.3.1 機密情報の範囲」で規定された機密情報を保護する責任を負う。

但し、本認証局が保持する情報を、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 プライバシープラン

本認証局における個人情報の取り扱いについては、「日本薬剤師会 個人情報保護方針」を適用する。

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。

- 本認証局が本人確認や各種審査の目的で収集した情報の中で、電子証明書に含まれない情報
- CRL に含まれない加入者の電子証明書失効または停止の理由に関する情報
- その他、本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

本認証局は、本 CPS「9.4.2 個人情報扱いする情報」で規定された個人情報を保護する責任を負う。

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、個人情報を、証明書発行業務その他の認証業務において利用する目的で個人情報を利用し、それ以外の目的で個人情報を利用する場合は、本人に対して通知し、予め本人の同意を得るものとする。ただし、下記の場合はこの限りではない。

- 利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
- 利用目的を本人に通知し、又は公表することにより当該個人情報取扱事業者の権利又は正当な利益を害するおそれがある場合
- 国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。

9.4.6 司法手続又は行政手続に基づく公開

司法機関、行政機関その他の公的機関の決定、命令、勧告等があった場合は、本認証局は、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また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は、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：本認証局に帰属する財産である。
- 加入者の私有鍵：保存方法また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：保存方法また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。
- 加入者証明書及び加入者私有鍵を格納する IC カード：本認証局に帰属する財産である。

- 本 CPS：本認証局に帰属する財産（著作権含む）である。
- 本 CPS「1.1.1 関連規定」で示す CP：CP で規定される「HPKI 認証局専門会議」に帰属する財産（著作権含む）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、その運営にあたり、本 CPS に基づいて加入者及び検証者に対して以下の認証局としての責任をもつ。

- 提供するサービスと運用の全てが、本 CPS「1.1.1 関連規定」に示す CP の要件及び本 CPS に従って行われること
- 電子証明書の発行時に、申請者の申請内容の真偽の確認を確実に行うこと
- 申請者の申請に基づいて、申請内容を正確に記載した電子証明書を発行すること
- 公開鍵を含む電子証明書を申請者に確実に届けること
- 加入者からの失効申請を確認、受理した場合、当該証明書について確実に失効処理を行うこと
- CRL、ARL などの重要事項をリポジトリ、情報公開用 Web サイトを通じて速やかに公開すること
- CRL、ARL の運用にあたり、システム保守作業等による一時停止や緊急時等やむを得ない場合の停止を除き、発行後は定期的にリポジトリに登録し、失効対象の電子証明書の有効期間が切れるまで公開し続けること
- 本 CPS「5 物理的、手続き上、人事上の統制」及び「6 技術的セキュリティ管理」に従い、認証設備を運用し、全ての認証局の私有鍵について、公開鍵から類推、算出されるような場合を除き盗難等による危殆化を生じさせないこと
- CA 私有鍵が、電子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
- 電子証明書、CRL 等の形式が発行時点において本 CPS「7 証明書と CRL/ARL のプロファイル」と一致していること
- 申請者の真偽の確認において利用した書類を含む各種の書類を減失、改ざん等が発生しない方法で本 CPS「5.5.2 アーカイブの保管期間」に定める期間保管すること
- 加入者の名称（subjectDN）について、そ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

登録局は以下の項目に対して責任を果たすものとする。

- 証明書発行にあたり、本人性確認など証明書利用申請者の適正な検証を行うこと
- 加入者からの証明書失効の申請にあたり、その申請理由の妥当性などについて適正な検証を行うこと

- 加入者の名称（subjectDN）について、その一意性を検証可能にしておくこと
- 発行局で生成した電子証明書を適切に検証、配布できるようにしておくこと
- 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 証明書失効の処理手続」に従って失効申請を開始すること
- 証明書の検証のため、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 年間保存すること

9.6.3 加入者の表明保証

本認証局の加入者は以下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

本認証局に発行申請を行う場合、登録局に提示する各書面の内容について、虚偽なく正確に記述する責任を果たすこと。

(2) 利用規定の遵守責任

加入者の電子証明書は、本 CPS 及び本 CPS「1.1.1 関連規定」に示す CP に従って発行される。そのため、加入者は、本 CPS 及び本 CPS「1.1.1 関連規定」に示す CP に規定される利用規定及び禁止規定を遵守する責任を果たすこと。

(3) 鍵などの管理責任

加入者は、加入者私有鍵を保護し、紛失、暴露、改ざん、または盗用されることを防止するために妥当な措置をとること。

(4) 証明書記載事項の担保責任

加入者は、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、その後の加入者証明書利用時も、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。

(5) 速やかな失効申請に対する責任

本 CPS「4.9.1 証明書失効の要件」に規定されている事項が発生した場合には、加入者は速やかに失効申請を行う責任を果たすこと。

(6) 証明書記載事項以外の登録情報変更の届け出に対する責任

加入者は、加入者の連絡先（電話番号、FAX 番号、電子メールアドレス）等の加入者証明書に記載されていない利用申請書の記載事項に変更が生じた場合、本認証局に届け出ること。

9.6.4 検証者の表明保証

本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

本認証局から発行される電子証明書は、本 CPS 及び本 CPS「1.1.1 関連規定」に示す CP に従って発行される。そのため、検証者は、本 CPS 及び本 CPS「1.1.1 関連規定」に示す CP に規定される利用規定及び禁止規定を遵守する責任を果たすこと。また、電子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、電子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。

- 電子証明書が改ざんされていないこと
- 電子証明書の有効期限が切れていないこと
- 電子証明書が失効していないこと
- 電子証明書が利用規定に反していないこと
- 電子証明書の署名が正しいこと
- 電子証明書の記載事項が本 CPS「7 証明書と CRL/ARL 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
  - 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 nonRepudiation のみが立てられていること

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 表明保証」で規定される保証を除き、電子証明書についての加入者及び下位認証局における特定の目的に対する適合性に関する黙示的又は明示的保証をしない。

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、下位認証局若しくはその他の第三者において損害が生じた場合、本認証局は、一切の責任を負わない。

9.8 責任制限

本認証局は、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。

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電子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、認証業務運用会議により審査され認証局代表者が承認され、更に HPKI 専門家会議にて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 CPS の終了まで有効であるものとする。

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、「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

本認証局は、本 CPS 等その他加入者が加入者証明書を利用するにあたって必要又は重要な情報を情報公開用 Web サイトにおいて公表する。加入者は、定期的に情報公開用 Web サイトを閲覧してこれらの情報を取得するものとする。

本認証局から加入者への通知方法は、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、本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

本 CPS は、認証局業務運営会議による審査ののち認証局代表者の承認を経て、各加入者に通知し、各加入者が改訂内容に合意した時点で改訂される。ただし、本認証局から変更内容を通知した後、加入者が私有鍵又は電子証明書を使用した場合、又は、通知後 1 か月以内に契約解除の申し出がなかった場合は、各加入者は変更内容に合意したものとみなす。

9.12.2 通知方法と期間

本 CPS が改訂された場合、情報公開用 Web サイト等を通じて、全ての加入者及び検証者が速やかに入手可能な措置をとる。

公開の期間については、以下のように定める。

- 重要な変更は、通知後、15 日（告知期間）を経て効力を発行する。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、即、効力を発する。
- 重要でない変更は、通知後直ちに効力を発する。

9.12.3 オブジェクト識別子（OID）の変更理由

重要な変更の場合には、本 CPS のバージョン番号を更新する。

9.13 紛争解決手続

本認証業務に関連して生じた全ての紛争について、東京地方裁判所をもって合意上の第一審の管轄裁判所とする。

9.14 準拠法

本 CPS は、日本国内法を準拠法とする。

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第三者に譲渡又は担保に供することができない。

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

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。

- 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

・ 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 CPS 及び HPKI-CP の方針に同意し責任を持ち続けるものとする。

別紙 A. 証明書のプロファイル

CA 証明書、及び加入者証明書のプロファイルを示す。プロファイル中の「×」は設定しないことを表している。

(1) CA 証明書

CA 証明書の有効期間は 20 年とし、10 年毎に更新する。

表 A-1 CA 証明書のプロファイル

項目	説明	設定値	Critical
基本領域			
version	version3	2	－
serialNumber	証明書のシリアル番号 （一意な 20 バイト以内の正整数）	正の整数	－
signature	証明書の署名に使用された暗号アルゴリズム		－
algorithm	アルゴリズムの OID SHA1withRSAEncryption を利用	1.2.840.113549.1.1.5	
parameters	暗号アルゴリズムの引数		
issuer	証明書発行者（本認証局）の DN	C =JP O =Japan Pharmaceutical Association CN=HPKI-01-JPA-CA-forNonRepudiation	－
validity	証明書の有効期間（20 年有効） ※グリニッジ標準時で記述		－
notBefore	有期期間の開始日時	yymmddhhmmssZ	
notAfter	有効期間の終了日時	yymmddhhmmssZ	
subject	証明書所有者の DN	C =JP O =Japan Pharmaceutical Association CN=HPKI-01-JPA-CA-forNonRepudiation	－
subjectPublicKeyInfo	証明書所有者の公開鍵に関する情報		－
algorithm	RSAEncryption を利用	1.2.840.113549.1.1	
parameters	暗号アルゴリズムの引数		
subjectPublicKey	RSA 公開鍵値（2048bit）		
issuerUniqueID	×		－
subjectUniqueID	×		－
拡張領域			
authorityKeyID	証明書発行者の公開鍵に関する情報		FALSE

keyIdentifier	ルート CA 公開鍵の SHA1 ハッシュ値		
authCertIssuer	ルート CA 証明書の DN	C=JP O=Ministry of Health, Labour and Wwlfare OU=Health Policy Bureau OU=MHLW HPKI Root CA	
authCertSerialNumber	ルート CA 証明書のシリアル番号	00	
subjectKeyID	証明書所有者の公開鍵に関する情報 subjectPublicKey の SHA1 ハッシュ値		FALSE
keyUsage	鍵の使用目的 KeyCertSign と cRLSign を設定		TRUE
privateKeyUsagePeriod	×		FALSE
certificatePolicies	証明書ポリシーの情報		TRUE
policyIdentifier	証明書ポリシーの OID	1.2.392.100495.1.5.1.1.3.1	
policyQualifiers	CPS 公開先 URL	http://hpki.mhlw.go.jp/repository/	
policyMappings	×		TRUE/FALSE
subjectAltName	×		FALSE
issuerAltName	×		FALSE
subjectDirectoryAttrs	×		FALSE
attrType	×		
attrValues	×		
basicConstraints	基本的制約		TRUE
cA		TRUE	
pathLenConstraints	×		
nameConstraints	×		TRUE
policyConstraints	×		TRUE
extKeyUsage	×		TRUE/FALSE
cRLDistributionPts	CRL のリポジトリ登録先		FALSE
	リポジトリ登録先	C=JP O=Ministry of Health, Labour and Wwlfare OU=Health Policy Bureau OU=MHLW HPKI Root CA CN=SARL	

distributionPoint	リポジトリ登録先	http://hpki.mhlw.go.jp/repository/rlist/sarl.cr.	
reasons	×		
cRLIssuer	×		
inhibitAnyPolicy	×		TRUE
freshestCRL	×		FALSE
authorityInfoAccess	×		FALSE
subjectInfoAccess	×		FALSE
qcStatements	×		TRUE/ FALSE

(2) 加入者証明書

subject 及び subjectDirectoryAttributes に記している値は、設定値ではなく例示であり、加入者毎に異なる値が設定される。

表 A-3 加入者証明書のプロファイル

項目	説明	設定値	Critical
基本領域			
version	version3	2	－
serialNumber	証明書のシリアル番号 （一意な 20 バイト以内の正整数）	正の整数	－
signature	証明書の署名に使用された暗号アルゴリズム		－
algorithm	アルゴリズムの OID SHA1withRSAEncryption を利用	1.2.840.113549.1.1.5	
parameters	暗号アルゴリズムの引数		
issuer	証明書発行者（本認証局）の DN	C =JP O =Japan Medical Association CN=HPKI-01-JPA-CA-forNonRepudiation	－
validity	証明書の有効期間 ※グリニッジ標準時で記述		－
notBefore	有期期間の開始日時	yymmddhhmmssZ	
notAfter	有効期間の終了日時	yymmddhhmmssZ	
subject	証明書所有者の DN C : 証明書所有者の国名（JP 固定） O : 証明書所有者が管理権限を持つ組織名（管理者の証明書の場合のみ設定） OU : Director（管理者の証明書の場合のみ設定） CN : 証明書所有者の氏名 SN : 証明書所有者の医籍登録番号	（例） C =JP L =Tokyo O =JPA OU=Director CN=NICHIYAKU TARO SN=123456780	－
subjectPublicKeyInfo	証明書所有者の公開鍵に関する情報		－
algorithm	RSAEncryption を利用	1.2.840.113549.1.1	
parameters	暗号アルゴリズムの引数		
subjectPublicKey	RSA 公開鍵値（1024bit 以上）		
issuerUniqueID	×		－
subjectUniqueID	×		－
拡張領域			
authorityKeyID	証明書発行者の公開鍵に関する情報		FALSE
keyIdentifier	CA 公開鍵の SHA1 ハッシュ値		
authCertIssuer	×		
authCertSerialNumber	×		

subjectKeyID	証明書所有者の公開鍵に関する情報 subjectPublicKey の SHA1 ハッシュ値		FALSE
keyUsage	鍵の使用目的 NonRepudiation を設定		FALSE
privateKeyUsagePeriod	×		FALSE
certificatePolicies	証明書ポリシーの情報		FALSE
policyIdentifier	証明書ポリシーの OID	0.2.440.200134.100.1.1	
policyQualifiers	CPS 公開先 URL	http://www.nichiyaku.or.jp/hpki	
policyMappings	×		TRUE/ FALSE
subjectAltName	×		FALSE
issuerAltName	×		FALSE
subjectDirectoryAttrs	医療従事者等の資格（hcRole）を記載		FALSE
attrType	hcRole の attrType		
attrValues	HcRole の attrValue（HCActor Data）に、証明書所有者が所有する資格の英字表記を設定		
basicConstraints	×		TRUE
cA	×		
pathLenConstraints	×		
nameConstraints	×		TRUE
policyConstraints	×		TRUE
extKeyUsage	×		TRUE/ FALSE
cRLDistributionPts	CRL のリポジトリ登録先		FALSE
distributionPoint	リポジトリ登録先	http://www.pki.med.or.jp/crl	
reasons	×		
cRLIssuer	×		
inhibitAnyPolicy	×		TRUE
freshestCRL	×		FALSE
authorityInfoAccess	×		FALSE
subjectInfoAccess	×		FALSE
qcStatements	×		TRUE/ FALSE

別紙 B. CRL のプロファイル

CRL のプロファイルを示す。プロファイル中の「×」は設定しないことを表している。

(1) CRL

表 B-1 CRL のプロファイル

項目	説明	設定値	Critical
基本領域			
version	version2	1	－
signature	失効リストへの署名に使用された暗号アルゴリズム		－
algorithm	アルゴリズム SHA1withRSAEncryption を利用		
parameters	暗号アルゴリズムの引数		
issuer	失効リスト発行者の DN	C =JP O =Japan Pharmaceutical Association CN=HPKI-01-JPA-CA-forNonRepudiation	－
thisUpdate	失効リストの今回更新日時（実績） ※グリニッジ標準日時で記述	yymmddhhmmssZ	－
nextUpdate	失効リストの次回更新日時（予定） thisUpdate の 48 時間後 ※グリニッジ標準日時で記述	yymmddhhmmssZ	－
revokedCertificates	加入者の公開鍵証明書の失効情報		－
userCertificate	失効した証明書のシリアル番号		
revocationDate	証明書の失効日時 ※グリニッジ標準日時で記述	yymmddhhmmssZ	
crlEntryExtensions			
crlExtentions			－
crlEntryExtensions			
reasonCode	失効理由コード ※以下は使用しない [0]unspecified [6]certificateHold [8]removeFromCRL		FALSE
holdInstructionCode	×		FALSE
invalidtityDate	×		FALSE
certificateIssuer	×		FALSE
crlExtentions			
authorityKeyID	CRL 発行者の公開鍵に関する情報		FALSE
keyIdentifier	CA 公開鍵の SHA1 ハッシュ値		
authCertIssuer	×		

authCertSerialNumber	×		
issuerAltName	×		FALSE
cRLNumber	一意な 20 バイト以内の正整数		FALSE
deltaCRLIndicator	×		TRUE
issuingDistributionPt	オプション。将来の利用を想定したもので、当面は付与しない。		TRUE
distributionPoint	オプション 付与する場合、リポジトリ登録先		
onlyContsUserCerts	オプション 付与する場合、TRUE を設定		
onlyContsCACerts			
onlySomeReasons	×		
indirectCRL	×		
onlyContsAttrCerts	×		
freahestCRL	×		FALSE