日本医師会認証局運用規程（CPS）

Version 5.00

令和 4 年 12 月

公益社団法人日本医師会

改定履歴

版数	日付	内容
1.0	2012-11-01	従前の署名用 CPS に認証（人）を加えて「日医認証局 CPS」とした。 地域受付局の対面受付審査を加えた。
1.1	2013-12-01	・組織名変更（社団法人から公益社団法人）に伴う修正 ・SHA256 対応証明書対応に伴う変更 ・発行する国家資格を医師のみに変更 ・「1.5.2　問い合わせ先」変更 ・「3.2.1　私有鍵の所有を証明する方法」修正 ・「3.2.3　個人の認証」登録局へ申請する場合と地域受付局へ申請する場合に整理（以降全体整理） ・その他文言修正
3.0	2015-03-3	・「保健医療福祉分野 PKI 認証局 署名用証明書ポリシ」及び「保健医療福祉分野 PKI 認証局認証用（人）ポリシ」改訂に伴う修正 ・その他文言修正
4.01	2017-4-21	住民票の写し、印鑑登録証明書、在留証明書等の有効期間を 3 ヶ月から 6 ヶ月に変更
4.1	2018-1-10	Web 申請システムを利用した、電子申請を追記した。（・個人番号カードを利用した新規発行申請　・医師資格証を利用した更新発行申請） 4.2.2　証明書申請の承認又は却下 以下を追加「(1) 誤記等の修正と承認 本認証局は、発行申請書の中に明らかな誤記、記載漏れ、判読困難等を発見し、審査のため訂正若しくは追記が必要な場合には、申請者への確認又は同意を得ることなく根拠資料に基づき、訂正若しくは追記をすることができるものとする。」
4.11	2019-1-10	5.5.2　アーカイブを保存する期間 （2）5.5.1（4）～（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。→1 年間保存する。（ＣＰ規定外の書類の保存期限変更。ＣＰで規定される書類類は 10 年間保存で変更なし。）

		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・・・・・本認証局で規定された業務終了手続きを行う。→90 日前までに訂正（ＣＰ規定の 90 日前までに訂正）
4.12	2020-10-2	5.5　記録の保管に関し、「文書」を「記録」に訂正した。 5.5.1　アーカイブ記録の種類 （3） 認証局が発行した全ての電子証明書及び CRL に関し、証明書等の名称を具体的に記載した。 （5） 設備及び安全対策措置に関する記録に関し、自己署名証明書とある誤記を CA 証明書に訂正し、（３）項に移した。 5.5.2　アーカイブを保存する期間に関し、記録の種類別に 10 年間保管又は１年間保管を、一律に「記録が作成された日から最低 10 年間保管する。」に訂正した。
4.20	2021-1-6	保健医療福祉分野 PKI 認証局署名用証明書ポリシ 1.6 版 令和 2 年 12 月 保健医療福祉分野 PKI 認証局認証用（人）証明書ポリシ　1.5 版　令和２年１２月 上記２つの厚生労働省証明書ポリシ（CP）改定に合わせて、本 CPS を次のとおり改定した。 ●3.2　初回の本人性確認　3.2.3　個人の認証　（1） 登録局へ郵送申請する場合　・国家資格 ●4.2　証明書申請手続　4.2.1　本人性及び資格確認　（1） 本人からの申請の場合　・郵送の場合　・持参若しくは交付時に本人が出頭する場合 上記各項目で、「医師免許証のコピー提出の場合、コピーの適当な空欄に実印を捺印させ、印鑑登録証明書を添えて提出する」とされていたが、「本認証局は、医師免許証のコピーの記載内容について、国家資格発行・管理機関若しくはそれに代わる台帳を公的に備えた機関に照会し真正であることを確認し、発行申請書の記載内容が一致することを確認するので、コピー提出時の実印の捺印及び印鑑登録証明書の提出を不要」とした。

4.30	2021-6-30	保健医療福祉分野 PKI 認証局署名用証明書ポリシ 1.7 版 令和 3 年 3 月及び 保健医療福祉分野 PKI 認証局認証用（人）証明書ポリシ 1.6 版 令和 3 年 3 月 上記２つの厚生労働省証明書ポリシ（CP）改定に合わせて、本 CPS を次のとおり改定した。 3.2.2 組織の認証 中央官庁/地方公共団体の運営する組織の場合 「組織が公的機関の場合には、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、若しくは法人組織の場合と同様の書類を提出することによって実在性を立証するとしていたが、公的病院であっても、法人組織の場合と同様の方法で組織の実在性を確認できると考えられるため、「法人組織の場合」と同じ記載とした。」との改定あり、CPS に反映した。 6.3.2 公開鍵証明書の有効期間と鍵ペアの使用期間 「エンドエンティティの加入者の公開鍵証明書の有効期間は 5 年を越えないものとし、その私有鍵の使用は公開鍵証明書の有効期限の１ヶ月前を越えないものとする。」から「エンドエンティティの加入者の公開鍵証明書の有効期間は、発行の日後の加入者の 5 回目（加入者が発行を受けている署名用電子証明書の有効期間が満了する日の前に、CPS で定める更新の期間内に加入者が新たな署名用電子証明書の発行の申請をし、新たな署名用電子証明書の発行を受けるときにあっては 6 回目）の誕生日とする。」の改定があり、CPS に反映した。 7.1.10 保健医療福祉分野の属性（hcRole） 表 7.1.18 HPKI 資格名 テーブ ル（codeDataFreeText の定義）にて、「義肢装具士」及び「柔道整復師」の英語表記を修正と「公認心理師」の追加があるが、当認証局で使用予定がないので反映の対象外とした。
5.00	2022-12-xx	令和 4 年 10 月付厚生労働省 保健医療福祉分野 PKI 認証局署名用ポリシ（CP）1.8 版、同認証用（人）ポリシ（CP）1.7 版への改定に伴う CPS の改定。 （以降、審査後に記載）

― 目次 ―

1. はじめに

日本医師会認証局運用規程（以下、本 CPS と呼ぶ。）は、公益社団法人日本医師会が運営する「日本医師会認証局」（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 署名用証明書ポリシ』（厚生労働省）及び『保健医療福祉分野 PKI 認証局 認証用（人）ポリシ』（厚生労働省）に従う。

（以下、『保健医療福祉分野 PKI 認証局 署名用証明書ポリシ』と『保健医療福祉分野 PKI 認証局 認証用（人）ポリシ』を合わせて「HPKI-CP」と呼ぶ。）

なお、本 CPS は、以下の文章に依存して構成される。

- IETF/RFC3647　Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- ISO/IS 17090-1:2008　Health informatics – Public key infrastructure Part1: Framework and overview
- ISO/IS 17090-2:2008　Health informatics – Public key infrastructure Part2: Certificate profile
- ISO/IS 17090-3:2008　Health informatics – Public key infrastructure Part3: 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　(http://csrc.nist.gov/cryptval/)
- 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）

1.1 概要

本認証局は、「日本医師会認証局　HPKI 署名用証明書」及び「日本医師会認証局 HPKI 認証用証明書」を提供し、医師の医師国家資格の所有者に対して署名用公開鍵証明書（以下、署名用証明書と呼ぶ）及び、認証用公開鍵証明書（以下、認証用証明書と呼ぶ。）を発行するものである。（以下、署名用証明書と認証用証明書を区別なく呼ぶ場合は「加入者証明書」と呼ぶ。）

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 署名用証明書ポリシ」及び「保健医療福祉分野 PKI 認証局認証用（人）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「日本医師会認証局運用規程」（以下、「本 CPS」と呼ぶ。）とする。

本ドキュメント及び、認証業務運営主体である日本医師会及び加入者証明書のオブジェクト識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
日本医師会	Japan Medical Association	0.2.440.200134
日本医師会認証局	JMA Certification Authority　(JMA CA)	0.2.440.200134.100.1
日本医師会認証局運用規程	JMA CA CPS	0.2.440.200134.100.1.1
署名用証明書	HPKI 署名用証明書ポリシ	1.2.392.100495.1.5.1.1.3.1
	HPKI 署名テスト用証明書ポリシ	1.2.392.100495.1.5.1.1.0.1
認証用証明書	HPKI 認証用（人）証明書ポリシ	1.2.392.100495.1.5.1.2.3.1
	HPKI 認証テスト用（人）証明書ポリシ	1.2.392.100495.1.5.1.2.0.1

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（CA）は、発行局（IA）と登録局（RA）をその構成要素とし、日本医師会により運営される。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認証業務の一部を外部に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、業務取扱に関する覚書または契約、それと同等のものとして認証局で定める団体登録申請書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。

1.3.3 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。

・ 医師

1.3.4 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、デジタル署名を公開鍵証明書の公開鍵で検証する者である。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。

1.4 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）署名用証明書：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
　　ただし、預託された加入者証明書については、当面の間、電子処方箋での利用に限る。

（2）認証用証明書：医療従事者等の保健医療福祉分野サービス提供者の認証用

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、公益社団法人 日本医師会電子認証センターとする。

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	: 日本医師会　電子認証センター
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	: 03-3942-7050
ＦＡＸ番　　号	: 03-3946-2136
E-mail アドレス	: toiawase@jmaca.med.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「保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議」である。

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（Hardware 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。

・ 医師資格証
HPKI 署名用証明書及びその私有鍵、HPKI 認証用証明書及びその私有鍵を IC カードに格納し、券面に医師であること、医籍登録番号、氏名、生年月日等を記載したカード。

・ 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：OID）
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
本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、デジタル署名の検証に用いる。

・ 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。
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
認証局に電子証明書の利用を申請する主体のこと。

・ 地域受付局（LRA：Local Reception Authority）
日本医師会に団体登録申請書を提出し、覚書または契約書または団体登録申請書で規定する LRA 事務取扱要領で定めた業務を実施する都道府県医師会、郡市区医師会等で運営される受付窓口。

・ 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）
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。認証するサブジェクト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）
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）
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。

・ 認証事務室
加入者若しくは地域受付局から郵送またはオンラインで地域受付局から持ち込まれた申請書及び添付資料を審査・登録するための部屋。

・ 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、FIPS140-1/140-2 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。

・ HPKI カード
本認証局から加入者に交付する、署名用証明書及びその私有鍵、認証用証明書及びその私有鍵を格納した US FIPS 140-2 レベル 2 の IC カード。

・ IA（Issuer Authority）
発行局を参照のこと。

・ LRA（Local Reception Authority）
地域受付局を参照のこと。

・ 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-2（Secure Hash Algorithm 2）
SHA-256 ともいう。グループのハッシュ関数の一つ。任意の長さのデータから 256bit 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、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。但し、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

本認証局の失効リスト公開場所を以下に記載する。

証明書種別	URL
SHA256 対応署名用証明書	http://crl.pki.med.or.jp/repository/crl/crl-sign2.crl
SHA256 対応認証用証明書	http://crl.pki.med.or.jp/repository/crl/crl-auth2.crl

（2） 情報公開用 Web サイト

http://www.jmaca.med.or.jp/

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。

- 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。

- CA 証明書
- 本 CPS
- 利用規約
- 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規定

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医籍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、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は HPKI カードに格納する。

加えて、加入者は、署名用証明書に限り、HPKI カードに格納する加入者私有鍵の申請を前提として、追加で鍵ペアの生成を申請し、その加入者私有鍵のエンドエンティティとして預託先を選択できる。この場合、本認証局は、予め預託先の安全性評価を行い、加入者私有鍵が預託先のエンドエンティティに適切に格納されることを確認し、その内容を契約等で明らかにする。なお、預託先に対しての客観的第三者評価基準がある場合は、それに準じていることを確認する。

また、本認証局（本 CPS の遵守及び個人情報の厳正な取扱いを条件に、業務取扱に関する覚書、または契約を取り交わした組織を含む。以下、同じ。）は、HPKI カードおよび預託された加入者私有鍵の利用を開始するに必要な情報等を正当な加入者に所有させるため、対面による本人性の確認の後に交付する。ただし、それらが同時に実施できず、どちらか一方のみ対面による本人性の確認が実施された場合にあっては、残る一方を発行申請書に記載された住所地への本人限定受取郵便（特例型）での送付をもって行う場合がある。

なお、HPKI カードの 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送付は行わない。

申請者が加入者公開鍵と加入者私有鍵を生成する場合は、加入者公開鍵を提示して本認証局に対し証明書発行要求を行う際、公開鍵証明書と私有鍵との対応を証明するために、認証局からのチャレンジに署名を行い、私有鍵の所有を証明するものとする。あるいは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

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、電子証明書の交付に先立ち、次のいずれかの方法で自身の実在性、本人性、申請意思及び医師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。

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提出する。ただし、代理人による申請は認めない。登録局への提出方法は、対面（郵送による申請の後、出頭して交付する場合を含む。以下同じ）、郵送（交付時に、本人限定受取郵便（特例型）もしくは

本認証局から受領書を送り返送させる場合。以下同じ）、オンライン（公的個人認証サービスによる電子署名もしくは HPKI 電子署名を付与する場合。以下同じ）の 3 種を規定する。

1. 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（広域交付住民票を含む。以下、合わせて住民票とする。）の写し若しくは住民票記載事項証明書、戸籍の謄本又は抄本（現住所の記載がある証明書の提示又は提出を求める場合に限る。）に添えて、発行申請書に当該個人の「氏名、生年月日、性別、住所」（以下、基本 4 情報という。）を記入し、登録局に提出することで実在性の立証をしなくてはならない。

海外移住者等で住民票の写しを有しない申請者からの申請の場合は、住民票、戸籍謄（抄）本に代えて、在留証明書を提出するものとする。

なお、住民票、戸籍謄（抄）本ならびに在留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等が有効期限を設けている場合は、それを優先する。

また、医師国家試験に合格し、新たに医籍登録申請をした者が医師資格情報を含んだ証明書を申請する場合、医師免許証の登録日が明記されていれば、登録日から 3 ヶ月の間は、発行申請書以外の書類の提出を省略できる。

提出方法は、対面を原則とし、本認証局の判断により、郵送での提出を認める場合がある。オンラインで提出する場合は、有効期間内の電子署名を付与すれば、発行申請書（オンラインで送付する申請情報を言う。以下同じ）以外の書類の提出を省略できる。

2. 個人の本人性

電子証明書の利用申請を行う個人は、次に挙げる書類のいずれか 1 点若しくは本認証局が認めるもののコピーを登録局に提出することで本人性の立証をしなくてはならない。

【本人性の立証書類】

- 日本国旅券
- 運転免許証（運転経歴証明書（平成 24 年 4 月 1 日以降発行のもの）を含む、以下、合わせて「運転免許証」という。）
- 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）
- マイナンバーカード（個人番号カード）（コピーは表面のみに限る。）
- 医師資格証（ただし初回発行を除く。）
- その他認証局が認めるもの（以下、合わせて「その他認証局が認めるもの」という。）

- 在留カード、特別永住者証明書、外国人登録証明書、戦傷病者手帳、海技免状、船員手帳、電気工事士免状、宅地建物取引主任者証、無線従事者免許証、猟銃/空気銃所持許可証　など本認証局が認めるもの

提出方法は、対面を原則とし、本認証局の判断により、郵送での提出を認める場合がある。オンラインで提出する場合は、上記書類の画像を本認証局が提供する申請システムにアップロードし、発行申請書と共に有効期間内の電子署名を付与する。

3. 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、自らが自署した発行申請書を提出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。

提出方法は、対面を原則とし、本認証局の判断により、郵送での提出を認める場合がある。なお、申請者が署名を行うことが困難な場合は、発行申請書の署名欄に実印を捺印の上、印鑑登録証明書を提出する。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。オンラインで提出する場合は、発行申請書に有効期間内の電子署名を付与する。

4. 国家資格

電子証明書の利用申請を行う個人は、医師免許証のコピーを登録局に提出する。本認証局は、医師免許証のコピーの記載内容について、資格原本を保有する厚生労働省に真正であることを照会して確認する。

提出方法は、対面を原則とし、本認証局の判断により、郵送での提出を認める場合がある。オンラインで提出する場合は、上記書類の画像を本認証局が提供する申請システムにアップロードし、発行申請書と共に有効期間内の電子署名を付与する。

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る。

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、当該更新申請者に対して当該更新申請者が保有する初回の電子証明書が生成された日から 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か、加入者の電子署名により鍵更新を行う。

そのため本認証局は、初回の電子証明書が生成された日から 5 年後の日（有効期限日）の 3 ヶ月前から更新の申請を受け審査を開始し、有効期限日までに発行が完了する期間内で更新の申請を受付ける。

5 年を過ぎていた場合、若しくは元の書類若しくは記録が無効になっているか廃棄されていた場合は、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、失効に関わる書類の記載内容が当該証明書の発行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。

本認証局は、加入者本人が死亡した場合、並びに加入者本人の電子証明書の管理能力が著しく低下した場合等、本認証局が認めた場合のみ代理人からの失効申請を受け付ける。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。

HPKI カードの返却があった場合は、失効に関わる書類の提出有無にかかわらず、本認証局は HPKI カードに格納された署名用及び認証用電子証明書を失効させ、預託した加入者私有鍵の発行がある場合にはこれを含めて失効させる。

緊急に失効する必要がある場合は、本認証局は FAX 等による失効依頼を受け付けることが出来る。その場合は、認証局が保持する情報を元に失効申請者に電話連絡等を行い、本人確認のうえ失効処理を実施する。ただし、この場合であっても、失効申請者は後日正式に失効に関わる書類を本認証局に提出する、若しくは HPKI カードを返却しなければならない。

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

加入者証明書の申請者は、医師国家資格を有する者本人とする。

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 及び利用規約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。電子申請による利用申請も可とする。

加入者証明書の利用申請に必要となる発行申請書、本 CPS、利用規約及び申請手順は、情報公開用 Web サイト上での公開を基本とする。

（1）対面による場合

本人が登録局に「3.2.3 個人の認証」に定める書類を提出し、提出時もしくは交付時に対面することで利用申請を行う。ただし、代理人による申請は認めない。

（2）郵送による場合

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。ただし代理人による申請は認めない。

（3）オンラインによる場合

本人が「3.2.3 個人の認証」に定める書類をアップロードすること及び電子署名することにより利用申請を行う。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。

本認証局は、保険医療福祉分野に関わる国家医師資格所有者への証明書の交付に先立ち、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。

申請者の実在性の確認にあたっては、住民票の写し、若しくは住民票記載事項証明書、戸籍の謄本若しくは抄本（現住所の記載がある証明書の提示又は提出を求める場合に限る。）、若しくは海外在留邦人等で住民票の写しを有しない申請者からの申請の場合の在留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、且つ基本 4 情報に関して日本国旅券等と発行申請書の記載内容が一致することを確認する。

なお、住民票の写し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。

医師国家試験に合格し、新たに医籍登録申請をした者が医師資格情報を含んだ証明書の申請をしてきた場合、登録日から 3 ヶ月の間は、住民票等の書類を省略できるため、その際には、提出された医師免許証の複写に記載された氏名、生年月日、医籍登録番号、医籍登録年月日が発行申請書の記載内容と一致することを確認する。

オンラインで申請してきた場合、署名の有効性を検証の上、申請情報と公的個人認証サービスの個人の公開鍵情報とを照合し、記載内容が一致することを確認する。更新時に、HPKI 電子署名を付与してきた場合、電子署名の有効性を検証の上、申請情報と前回申請時の情報を照合し、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、立証書類と発行申請書の記載内容が一致することを確認する。

オンラインで申請してきた場合、上記に加えて電子署名の有効性を検証する。

申請者の申請意思の確認にあたっては、申請者自らが自署した発行申請書を提出しなくてはならないことから、発行申請書の自署欄に自署があることを確認する。申請者が署名を行うことが困難な場合は、発行申請書の署名欄の実印と印鑑登録証明書の陰影が一致することを確認する。また、印鑑登録証明書の有効期間は発行日より 6 ヶ月以内もしくは発行する地方公共団体が有効期限を設けている期間内であるかを確認する。

なお、対面で提出する場合で、書類受領時に対面受付する場合は受領時、郵送による申請の後、出頭して交付する場合は、交付時に申請意思を確認する。

郵送で提出された場合は、本人限定受取郵便（特例型）で交付もしくは本認証局から受領書を送り返送させる方法で申請意思の確認を行う。この際、受領書の返送が 1 ヶ月経過した後もなく、督促をした上でもなお返送がない場合は、電子証明書を失効させる。

オンラインで申請してきた場合は、電子署名の有効性を検証することで申請意思を確認する。

医師の国家資格の確認にあたっては、医師免許証の複写が少なくとも記載内容、形式などにおいて真正であることを確認し、医師免許証と発行申請書の記載内容が一致することを確認する。また、その記載内容について、資格原本を保有する厚生労働省に真正であることを

照会して確認する。オンラインで申請してきた場合、上記に加えて電子署名の有効性を検証する。

なお、上記全てについて、確認に用いた証明書等の書類は認証局でコピーを取り、発行日から 10 年保管する。オンラインで申請された場合、申請情報をアーカイブし、同様に発行日から 10 年保管する。

4.2.2 証明書申請の承認又は却下

（1） 誤記等の修正と承認

本認証局は、発行申請書の中に明らかな誤記、記載漏れ、判読困難等を発見し、審査のため訂正若しくは追記が必要な場合には、申請者への確認又は同意を得ることなく立証書類、日医データ等に基づき、訂正若しくは追記をすることができるものとする。

（発行申請書内容）	（立証書類・日医データ等）
カード ID	認証局記録
申請事由	認証局記録、審査者判断
基本 4 情報	住民票の写し、JPKI 署名検証
日医会員、ID	日医記録
医籍登録番号	厚労省記録
旧姓・通名	旧姓または通名が記載された公的書類
その他	上記各資料又はその他の公的書類

なお、訂正若しくは追記をした場合には、オリジナルの発行申請書等に加えて、訂正若しくは追記情報の記録も保管するものとする。

（2） 却下と再提出

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し、疑義を解消できる書類の再提出を求める。

4.2.3 証明書申請手続き期間

日医電子認証センターWeb 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

本認証局は、発行申請書の情報をもとに、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 HPKI カードに格納する。

なお、加入者が追加で鍵ペアの生成を申請し、その加入者私有鍵のエンドエンティティとして預託先を選択した場合は、本認証局で予め安全性評価（第三者評価がある場合はその評価）を行った預託先であれば、加入者私有鍵を引き渡す。この場合にあっては、契約書等により加入者私有鍵が預託先のエンドエンティティに格納されたことを確認する。

HPKI カードの PIN は、権限のある複数人の内部牽制のもと安全に設定する。また、HPKI カードに格納後、加入者鍵ペアは認証設備から完全に消去する。同様に、加入者の選択で預託された場合も引渡しの後に、加入者鍵ペアは認証設備から完全に消去する。

4.3.2 証明書発行後の通知

本認証局は、電子証明書を発行したことを加入者にハガキ等で通知する。又は電子証明書を本人限定受取郵便（特例型）等の郵便で加入者本人に送付することをもって通知する。

4.4 証明書の受理

4.4.1 証明書の受理

本認証局は、HPKI カードを対面で加入者に交付した場合には、加入者から受領した受領書を確認することにより、加入者証明書及び加入者私有鍵が加入者に交付されたことを確認する。本人限定受取郵便（特例型）等の郵便で加入者本人に郵送した場合には、日本郵便の配達記録を確認することで加入者に交付されたことを確認する。預託先に引き渡す場合は、加入者私有鍵の到達確認（格納ログ）によって確認する。

なお、本認証局は、HPKI カード受け取りに関して連絡もなく証明書発行日から 3 ヶ月以内に加入者への交付確認が得られなかった場合、当該加入者証明書を失効する権限を有する。

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、本規程「1.4.1　適切な証明書の使用」に規定する利用目的にのみ私有鍵と証明書を利用しなければならない。

4.5.2 検証者の公開鍵と証明書の利用目的

検証者は、署名用証明書の場合は署名検証の用途で、認証用証明書の場合は認証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 証明書によ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。
- 有効期限日の 3 ヶ月前から有効期限終了前までに発行できる期間内に申請があること。

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、本認証局で電子証明書が生成された日から 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用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ことができる。

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、CPS「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）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。

- 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
- HPKI カードを紛失あるいは破損した場合
- HPKI カードの盗難あるいは不正使用などを知った場合
- HPKI カード PIN の紛失等で PIN が分からなくなった場合
- HPKI カード PIN の入力ミスで HPKI 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

(2) 代理人による失効要件

代理人は、加入者が死亡した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若しくは HPKI カードの返却を確認した場合、理由の如何に関わらず加入者証明書（預託先に加入者証明書が格納されている場合はこれを含む）の失効を行う。

(3) 認証局職員による失効要件

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。（預託先に加入者証明書が格納されている場合はこれを含む）

・ 加入者が本 CPS 及び利用規約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
・ 加入者証明書を発行した日から 3 ヶ月以内に、加入者本人への加入者証明書の交付確認ができなかった場合
・ 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
・ 本認証局の責めに帰すべき事由により加入者証明書の誤発行等を行った場合
・ その他、本認証局が必要と判断した場合

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（加入者死亡の場合は）その代理人
(2) 本認証局職員
(3) 加入者証明書預託先組織の職員（預託先に加入者証明書が格納されている場合に限る。）

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。

＜加入者本人からの失効申請の場合＞

・ 失効申請

加入者は、加入者証明書の失効を申請する場合、失効に関わる書類を本認証局へ郵送する。緊急を要する失効要求の場合、失効申請に関わる書類を本認証局宛てに FAX し、原本を後日郵送する。なお、失効に関わる書類は情報公開用 Web サイトにて掲載公開しているものを利用する。

HPKI カードの返却があった場合は、利用の中止になり失効に関わる書類の提出有無にかかわらず、本認証局は電子証明書の失効を受理する。（預託先に加入者証明書が格納されている場合はこれを含む）

・ 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、失効に関わる書類の記載内容が当該証明書の申請書の記載内容と一致していることを確認する。また、失効に関わる書類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。

FAX 等による失効申請の場合は、認証局が保持する情報を元に失効申請者に電話等連絡を行い、本人確認を行いその真偽について確認を行う。

HPKI カードの返却があった場合は、利用の中止になり失効に関わる書類の提出有無にかかわらず、本認証局は電子証明書の失効を受理する。預託先に加入者証明書が格納されている場合はこれを含む。

・ 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。

本認証局は、加入者から失効の申請を受け、必要な場合は失効事由の詳細を確認して、失効の対象を検討する。

HPKI カードの返却があった場合は、利用の中止になり失効に関わる書類の提出有無にかかわらず、本認証局は電子証明書の失効をする。預託先に加入者証明書が格納されている場合はこれを含めて失効する。

＜代理人からの失効申請の場合＞

・ 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、失効申請に関わる書類若しくは電子証明書を本認証局へ郵送する。緊急を要する失効要求の場合、失効に関わる書類を本認証局宛てに FAX 等をし、原本を郵送する。なお、失効に関わる書類書は情報公開用 Web サイトにて掲載公開しているものを利用する。

HPKI カードの返却があった場合は、利用の中止になり失効に関わる書類の提出有無にかかわらず、本認証局は電子証明書の失効を受理する。預託先に加入者証明書が格納されている場合はこれを含む。

・ 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に関わる書類若しくは電子証明書を受け取った後、失効に必要な情報に不備がないこと、失効申請に関わる書類若しくは電子証明書の記載内容が当該証明書内容と一致していることを確認する。また、失効申請に関わる書類に記載された失効事由を確認し、その真偽について確認を行う。

HPKI カードの返却があった場合は、利用の中止になり失効に関わる書類の提出有無にかかわらず、本認証局は電子証明書の失効を受理する。預託先に加入者証明書が格納されている場合はこれを含む。

・ 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代理人に通知する。

HPKI カードの返却があった場合は、利用の中止になり失効に関わる書類の提出有無にかかわらず、本認証局は電子証明書の失効を受理する。預託先に加入者証明書が格納されている場合はこれを含めて失効する。

＜認証局の職員からによる失効申請の場合＞

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。

HPKI カードの返却があった場合は、利用の中止になり失効に関わる書類の提出有無にかかわらず、本認証局は電子証明書の失効を受理する。預託先に加入者証明書が格納されている場合はこれを含めて失効を受理する。

＜加入者証明書預託先組織からの失効申請の場合＞

預託された加入者証明書の漏えい又は漏えい等の恐れが発生した場合は、その預託先組織の職員から失効申請が行われる場合が加わる。

加入者からの失効申請、代理人からの失効申請、認証局職員からの失効申請と同様に、失効申請者の正当性確認の方法を行い、失効処理を行う。

＜各種失効事由と失効処理の組み合わせ＞

本認証局は、各失効申請について失効事由を確認し、必要な場合は申請者と確認の連絡をとり、利用と運用の状況を確認する場合がある。

確認の結果で、失効範囲を選択することができるものとする。

- HPKI カード紛失等で、HPKI 証明書のみを失効又は預託された加入者証明書も失効する。
- 預託された加入者証明書の漏えい又は漏えいの恐れ等で、預託された加入者証明書のみを失効又は HPKI 証明書も失効する。
- 医師資格の停止等で、利用者情報の利用登録を削除する。
- その他

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若しくは HPKI カードの返却を受付けた場合、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、電子証明書が失効されている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。

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 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

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、本人の選択、並びに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

加入者が本 CPS 及び利用規約に同意して、預託する加入者証明書の発行を希望した場合、それを預託先に交付する。鍵回復については規定しない。

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、二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。

・ 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。

・ 認証事務室

認証事務室は、加入者若しくは地域受付局から郵送または地域受付局から持ち込ま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

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

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。

- 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。

- 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。

- 重要な情報を記録した HPKI カード
  HPKI カードチップを物理的に破壊した後に廃棄する。

- 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 ・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
認証局責任者	・登録局及び発行局の運営及び管理と業務の統括 ・審査登録業務責任者と認証業務責任者の任命と解任および人事管理
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 ・受付審査担当者と RA 操作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 秘密鍵のバックアップの保管
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 HPKI 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 ・上級 IA 操作員と一般 IA 操作員とシステム保守員の任命と解任および人事管理 ・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、電子証明書若しくは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

日本医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、日本医師会で定める職務規定に従い秘密保持義務等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。

＜証明書の発行申請に関する記録＞

- 発行申請書/更新申請書等
- 団体申請書
- 加入者の住民票の写し（電子申請の場合は JPKI 検証結果）
- 加入者の医師免許証のコピー（電子申請の場合はアップローされたデータ）
- 加入者の本人性の立証書類のコピー（同上）
- 医療機関等の存在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、本認証局で規定した方法に従い保存する。

＜証明書の失効申請に関する記録＞

- 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、本認証局で規定した方法に従い保存する。

＜認証局が発行した全ての電子証明書及び CRL＞

- 本認証局の CA 証明書
- 本認証局が発行した加入者証明書
- 本認証局が発行した CRL
- 本認証局の 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 CA 証明書発行実施に伴う記録

＜認証局の組織管理に関する記録＞

- 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団体登録申請書

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、本認証局で規定した方法に従い保存する。

＜設備及び安全対策措置に関する記録＞

- 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

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

アーカイブ記録を保存する期間は、記録が作成された日から最低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り、書類は原本を施錠付き書庫に保管する。

記録を保管する書庫は、施錠可能な出入口を持ち、間仕切り又は壁により区画され、かつ防火区画内にある室内に設置される。また、情報の劣化を防ぐために適切な環境下で保存するものとする。

紙媒体で保存される記録は、適切なファイル等に保管する。

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。電子媒体は、適切なケースに入れられ、適切な場所において保管する。

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、認証局代表者の判断により、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、認証局代表者の判断により対策を決定し、厚生労働省 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 90 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 HPKI カードに格納する。なお、加入者の選択により預託する加入者私有鍵を発行した場合、本認証局から預託先へ、適切な方法をもって加入者私有鍵を交付する。

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、対面で受領書を受け取ることで加入者本人に交付する。ただし、本人限定受取郵便（特例型）をもって、これに代えることもできる。また、どちらか一方のみ対面による本人性の確認が実施された場合にあっては、残る一方を発行申請書に記載された住所地への本人限定受取郵便（特例型）での送付をもって行う場合がある。

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、ハッシュアルゴリズムに sha256WithRSAEncryption 以上を設定する場合は、RSA アルゴリズムは 2048bit 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。

署名用証明書に係る鍵は、nonRepudiation とする。

認証用証明書に係る鍵は、DigitalSignature 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、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。

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 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 私有鍵の預託

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。

加入者の私有鍵は、加入者本人の選択、並びに、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。

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施錠可能な保管場所に保管する。

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、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。

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。

6.3 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

CA 公開鍵証明書の有効期間は 20 年を越えないものとし、その私有鍵の使用は 10 年を越えないものとする。新規の発行及び前証明書の有効期限が切れた以降に発行する場合のエンドエンティティの加入者の公開鍵証明書の有効期間は、発行の日後の加入者の 5 回目の誕生日とする。

前証明書の更新又は再発行の有効期間は更新又は再発行の日後の加入者の 5 回目の誕生日までとする。（ただし有効期間が満了する日までの期間が 3 月未満となった場合に、新たな電子証明書の発行を受けるときにあっては、6 回目の誕生日までとする。）

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、電子証明書若しくは 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

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 の通りとする。

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
SHA-256 対応署名用 CA 証明書	表 7.1.10	表 7.1.11
SHA-256 対応認証用 CA 証明書	表 7.1.12	表 7.1.13
SHA-256 対応署名用証明書	表 7.1.14	表 7.1.15
SHA-256 対応認証用証明書	表 7.1.16	表 7.1.17

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証明書の拡張領域のプロファイルは表 7.1.1 の拡張領域プロファイルの通りとする。

なお、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。

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、、sha256WithRSAEncryption (1.2.840.113549.1.1.11)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は、表 7.1.1 の通りである。

7.1.5 名前制約

用いない。

7.1.6 CP オブジェクト識別子

本認証局が発行する署名用証明書及び認証用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

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。

表 7.1.2　SHA-1 対応署名用 CA 証明書プロファイル（基本領域）（SHA-1 削除）
表 7.1.3　SHA-1 対応 CA 証明書プロファイル（拡張領域 Extensions）（SHA-1 削除）
表 7.1.4　SHA-1 対応認証用 CA 証明書プロファイル（基本領域）（SHA-1 削除）
表 7.1.5　SHA-1 対応認証用 CA 証明書プロファイル（拡張領域 Extensions）（SHA-1 削除）
表 7.1.8　SHA-1 対応認証用証明書プロファイル（基本領域）（SHA-1 削除）
表 7.1.9　SHA-1 対応認証用証明書プロファイル（拡張領域 Extensions）（SHA-1 削除）

表 7.1.10　SHA-256 対応署名用 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 年以下（UTCTime で設定する。）
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	○	JP
OrganizationName	○	Ministry of Health, Labour and Welfare
OrganizationUnitName	○	Director-General for Policy Planning and Evaluation
OrganizationUnitName	○	MHLW HPKI Root CA V2
Subject	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）
CountryName	○	JP
OrganizationName	○	Japan Medical Association
OrganizationUnitName	○	Digital Certificate Center
CommonName	○	HPKI-01-HPKI_JV2- forNonRepudiation
SubjectPublicKeyInfo	○	
Algorithm	○	rsaEncryption
SubjectPublicKey	○	RSA 公開鍵値(2048bit)
IssuerUniqueID	×	
SubjectUniqueID	×	
Extensions	○	拡張領域（表 7.1.11）参照

表中の、「○」設定、「×」は設定しないことを表す。

表 7.1.11　SHA-256 対応 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= Ministry of Health, Labour and Welfare ou= Director-General for Policy Planning and Evaluation ou= MHLW HPKI Root CA V2	
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	○	KeyCertSign	CRLSign	TRUE
DeciphermentOnly	×		-
extendedKeyUsage	×		-
privateKeyUsagePeriod	×		-
certificatePolicies	○		TRUE
policyIdentifier	○		
certPolicyId	○	1.2.392.100495.1.5.1.1.3.1	
policyQualifiers	○		
cPSuri	○	http://hpki.mhlw.go.jp/repository/	
policyMapping	×		-
subjectAltName	×		-
issuerAltName	×		-
subjectDirectoryAttributes	×		-
basicConstraints	×		TRUE
CA	○		TRUE-
pathLenConstraints	×		-
nameConstraints	×		-
policyConstraints	×		-
cRLDistributionPoints	○		FALSE
distributionPoint	○		
fullName	○	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= Ministry of Health, Labour and Welfare ou= Director-General for Policy Planning and Evaluation ou=MHLW HPKI Root CA V2 cn=SARL	
uniformResource Identifier	○	http://hpki.mhlw.go.jp/repository/rlist/sarl2.crl	
subjectInfoAccess	×		-
authorityInfoAccess	△		FALSE

表中の、「○」は設定、「×」は設定しないことを表す。

表 7.1.12　SHA-256 対応認証用 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 年以下（UTCTime で設定する。）
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	○	JP
OrganizationName	○	Ministry of Health, Labour and Welfare
OrganizationUnitName	○	Director-General for Policy Planning and Evaluation
OrganizationUnitName	○	MHLW HPKI Root CA V2
Subject	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）
CountryName	○	JP
OrganizationName	○	Japan Medical Association
OrganizationUnitName	○	Digital Certificate Center
CommonName	○	HPKI-01-HPKI_JV2-forAuthentication-forIndividual
SubjectPublicKeyInfo	○	
Algorithm	○	rsaEncryption
SubjectPublicKey	○	RSA 公開鍵値(2048bit)
IssuerUniqueID	×	
SubjectUniqueID	×	
Extensions	○	拡張領域（表 7.1.13）参照

表中の、「○」設定、「×」は設定しないことを表す。

表 7.1.13　SHA-256 対応認証用 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= Ministry of Health, Labour and Welfare ou= Director-General for Policy Planning and Evaluation ou= MHLW HPKI Root CA V2	
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	○	KeyCertSign	CRLSign	TRUE
DeciphermentOnly	×		-
extendedKeyUsage	×		-
privateKeyUsagePeriod	×		-
certificatePolicies	○		TRUE
policyIdentifier	○		
certPolicyId	○	1.2.392.100495.1.5.1.2.3.1	
policyQualifiers	○		
cPSuri	○	http://hpki.mhlw.go.jp/repository/	
policyMapping	×		-
subjectAltName	×		-
issuerAltName	×		-
subjectDirectoryAttributes	×		-
basicConstraints	×		TRUE
CA	○		TRUE-
pathLenConstraints	×		-
nameConstraints	×		-
policyConstraints	×		-
cRLDistributionPoints	○		FALSE
distributionPoint	○		
fullName	○	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= Ministry of Health, Labour and Welfare ou= Director-General for Policy Planning and Evaluation ou=MHLW HPKI Root CA V2 cn=SARL	
uniformResource Identifier	○	http://hpki.mhlw.go.jp/repository/rlist/sarl2.crl	
subjectInfoAccess	×		-
authorityInfoAccess	△		FALSE

表中の、「○」は設定、「×」は設定しないことを表す。

表 7.1.14　SHA-256 対応署名用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 + 5 年以下（UTCTime で設定する。）
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	○	JP
OrganizationName	○	Japan Medical Association
OrganizationUnitName	○	Digital Certificate Center
CommonName	○	HPKI-01-HPKI_JV2-forNonRepudiation
Subject	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）
CountryName	◎	JP
OrganizationName	○	加入者が医療機関等の管理者の場合は必須 その場合は医療福祉機関名をローマ字で記載。なお、追加の加入者私有鍵を発行する場合にあっては、当該私有鍵を識別する符号を追加する。
OrganizationUnitName	○	加入者が医療機関等の管理者の場合は必須 「Director」の文字列を格納
CommonName	◎	加入者の氏名をローマ字を記載
SerialNumber	○	医籍登録番号などを記載
SubjectPublicKeyInfo	○	
Algorithm	○	rsaEncryption
SubjectPublicKey	○	RSA 公開鍵値(2048bit)
IssuerUniqueID	×	
SubjectUniqueID	×	
Extensions	○	拡張領域（表 7.1.15）参照

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

表 7.1.15　SHA-256 対応署名用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= Ministry of Health, Labour and Welfare ou= Director-General for Policy Planning and Evaluation ou= MHLW HPKI Root CA V2	
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	○	nonRepudiation	TRUE
DeciphermentOnly	×		-
extendedKeyUsage	×		-
privateKeyUsagePeriod	×		-
certificatePolicies	○		TRUE
policyIdentifier	○		
certPolicyId	○	1.2.392.100495.1.5.1.1.3.1	
policyQualifiers	○		
cPSuri	○	http://www.pki.med.or.jp/certpolicy/	
policyMapping	×		-
subjectAltName	×		-
issuerAltName	×		-
subjectDirectoryAttributes	◎		-
basicConstraints	×		-
CA	×		-
pathLenConstraints	×		-
nameConstraints	×		-
policyConstraints	×		-
cRLDistributionPoints	○		FALSE
distributionPoint	○		
fullName	○		
uniformResource Identifier	○	http://crl.pki.med.or.jp/repository/crl/crl-sign2.crl	
subjectInfoAccess	×		-
authorityInfoAccess	△		FALSE

表中の、「○」は設定、「×」は設定しないことを表す。

表 7.1.16　SHA-256 対応認証用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 + 5 年以下（UTCTime で設定する。）
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	○	JP
OrganizationName	○	Japan Medical Association
OrganizationUnitName	○	Digital Certificate Center
CommonName	○	HPKI-01-HPKI_JV2-forAuthentication-forIndividual
Subject	○	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）
CountryName	◎	JP
OrganizationName	○	加入者が医療機関等の管理者の場合は必須 その場合は医療福祉機関名をローマ字で記載。なお、追加の加入者私有鍵を発行する場合にあっては、当該私有鍵を識別する符号を追加する。
OrganizationUnitName	○	加入者が医療機関等の管理者の場合は必須 「Director」の文字列を格納
CommonName	◎	加入者の氏名をローマ字を記載
SerialNumber	○	医籍登録番号などを記載
SubjectPublicKeyInfo	○	
Algorithm	○	rsaEncryption
SubjectPublicKey	○	RSA 公開鍵値(2048bit)
IssuerUniqueID	×	
SubjectUniqueID	×	
Extensions	○	拡張領域（表 7.1.17）参照

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

表 7.1.17　SHA-256 対応認証用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= Ministry of Health, Labour and Welfare ou= Director-General for Policy Planning and Evaluation ou= MHLW HPKI Root CA V2	
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	○	1.2.392.100495.1.5.1.2.3.1	
policyQualifiers	○		
cPSuri	○	http://www.pki.med.or.jp/certpolicy/	
policyMapping	×		-
subjectAltName	×		-
issuerAltName	×		-
subjectDirectoryAttributes	◎		-
basicConstraints	×		-
CA	×		-
pathLenConstraints	×		-
nameConstraints	×		-
policyConstraints	×		-
cRLDistributionPoints	○		FALSE
distributionPoint	○		
fullName	○		
uniformResource Identifier	○	http://crl.pki.med.or.jp/repository/crl/crl-auth2.crl	
subjectInfoAccess	×		-
authorityInfoAccess	△		FALSE

表中の、「○」は設定、「×」は設定しないことを表す。

7.1.10 保健医療福祉分野の属性（hcRole）

（1）サブジェクトディレクトリ属性拡張での hcRole 属性の使用

本 CPS では、HPKI-CP に従い、ISO 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 7.1.5 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 7.1.18　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
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
‘Supervisor of Pharmacy’	管理薬剤師
‘Proprietor of Pharmacy’	薬局開設者
‘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。

上記 Director5 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 IS 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 のプロファイルの詳細は、表 7.2.1 の通りとする。

失効リスト種別	基本領域	CRL エントリ拡張領	CRL 拡張領域
SHA-256 対応 署名用証明書失効リスト	表 7.2.8	表 7.2.9	表 7.2.10
SHA-256 対応 認証用証明書失効リスト	表 7.2.11	表 7.2.12	表 7.2.13

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 のプロファイルを以下に示す。

表 7.2.2　SHA-1 対応署名用証明書失効リストのプロファイル（SHA-1 削除）

表 7.2.3　SHA-1 対応署名用証明書失効リストのプロファイル（SHA-1 削除）
（CRL エントリ拡張領 crlEntryExtensions）

表 7.2.4　SHA-1 対応署名用証明書失効リストのプロファイル（SHA-1 削除）
（CRL 拡張領域 crlExtensions）

表 7.2.5　SHA-1 対応認証用証明書失効リストのプロファイル（SHA-1 削除）

表 7.2.6　SHA-1 対応認証用証明書失効リストのプロファイル（SHA-1 削除）
（CRL エントリ拡張領 crlEntryExtensions）

表 7.2.7　SHA-1 対応認証用証明書失効リストのプロファイル（SHA-1 削除）
（CRL 拡張領域 crlExtensions）

表 7.2.8　SHA-256 対応署名用証明書失効リストのプロファイル

フィールド	設定	説明
Version	○	Ｖer2 とする。
Signature	○	sha256WithRSAEncryption
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	○	Japan Medical Association
OrganizationUnitName	○	Digital Certificate Center
CommonName	○	HPKI-01-HPKI_JV2- forNonRepudiation
ThisUpdata	○	CRL 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（表 7.2.9）参照
CrlExtensions	○	拡張領域（表 7.2.10）参照

表 7.2.9　SHA-256 対応署名用証明書失効リストのプロファイル
（CRL エントリ拡張領 crlEntryExtensions）

フィールド	設定	説明	Critical
ReasonCode	○		FALSE
HoldInstructionCode	×		-
InvalidityDate	×		-
CertificateIssure	×		-

表 7.2.10　SHA-256 対応署名用証明書失効リストのプロファイル

（CRL 拡張領域 crlExtensions）

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	○	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= Ministry of Health, Labour and Welfare ou= Director-General for Policy Planning and Evaluation ou= MHLW HPKI Root CA V2	
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	×		-

表 7.2.11　SHA-256 対応認証用証明書失効リストのプロファイル

フィールド	設定	説明
Version	○	Ver2 とする。
Signature	○	sha256WithRSAEncryption
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	○	Japan Medical Association
OrganizationUnitName	○	Digital Certificate Center
CommonName	○	HPKI-01-HPKI_JV2-forAuthentication-forIndividual
ThisUpdata	○	CRL 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（表 7.2.12）参照
CrlExtensions		○	拡張領域（表 7.2.13）参照

表 7.2.12　SHA-256 対応認証用証明書失効リストのプロファイル
（CRL エントリ拡張領 crlEntryExtensions）

フィールド	設定	説明	Critical
ReasonCode	○		FALSE
HoldInstructionCode	×		-
InvalidityDate	×		-
CertificateIssure	×		-

表 7.2.13　SHA-256 対応認証用証明書失効リストのプロファイル
（CRL 拡張領域 crlExtensions）

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		○	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= Ministry of Health, Labour and Welfare ou= Director-General for Policy Planning and Evaluation ou= MHLW HPKI Root CA V2	
	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

本認証局は、HPKI-CP への準拠性監査を HPKI 認証局専門化会議に依頼し実施する。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。また、1 年以下の間隔で監査を実施する。

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

本認証局が保持する加入者の情報は、証明書、CRL、各認証局が定める CPS の一部として明示

的に公表されたものを除き、秘密保持対象として扱われる。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。

本認証局は、かかる法的手続き、司法手続き、行政手続きあるいは法律で要求されるその他の手続きに関連してアドバイスする法律顧問及び財務顧問に対し、秘密保持対象として扱われる情報を開示することができる。

また組織の合併等に関連してアドバイスする弁護士、会計士、金融機関及びその他の専門家に対しても、本認証局は秘密保持対象として扱われる情報を開示することができる。

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

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等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、「日本医師会 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 HPKI 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

(1) 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
・ 発行局で生成した電子証明書を適切に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

(2) 地域受付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
・ 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

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発行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.はじめに」に示す HPKI-CP に従って発行される。そのため、検証者は、本 CPS 及び HPKI-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。

- 電子証明書の署名が正しいこと
- 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、次の検証を実施すること。

- OID 及び Issuer の CN が HPKI-CP に一致していること
- 署名用証明書の場合 hcRole 及び keyUsage の nonRepudiation のみが立てられていること
- 署名用証明書の場合 hcRole 及び keyUsage の DigitalSignature 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「9.6.1　認証局表明保証」及び「9.6.2　登録局の表明保証」に規定する保証に関連して発生するいかなる間接損害、特別損害、付随的損害又は派生的損害に対する責任を負わず、いかなる逸失利益、データの紛失又はその他の間接的若しくは派生的損害に対する責任を負わない。

また、本 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、若しくはその他の第三者において損害が生じた場合、認証局は一切の責任を負わない。

9.8 責任制限

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し、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。

以上