日本医師会組織認証用 PKI 認証局運用規程（CPS）

平成 25～26 年度地域医療連携の普及に向けた健康情報活用基盤実証事業用

Ver.1.0

平成 26 年 6 月

公益社団法人日本医師会

改定履歴

版数	日付	内容
1.0	2014-6-19	本 CPS は、実証用として作成した。

― 目次 ―

1. はじめに

日本医師会組織認証用 PKI 認証局運用規程（以下、本 CPS と呼ぶ。）は、平成 25～26 年度地域医療連携の普及に向けた健康情報活用基盤実証事業（以下、「本実証事業」という。）において利用する組織認証用証明書の発行に関し、公益社団法人日本医師会（以下、「本会」という。）が運営する「日本医師会組織認証用 PKI 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。

1.1 概要

本認証局は、保健医療福祉分野の組織（施設）に、本実証事業の用に供するため、本実証事業期間に限り「日本医師会認証局組織認証用 PKI 証明書」（以下、「組織認証用証明書」という。）を発行するものである。

1.2 文書の名前と識別

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別子を以下のとおりとする。

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
日本医師会組織認証用 PKI 認証局運用規程	JMA Organization PKI CA CPS	0.2.440.200134.100.1.10

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。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（以下、CRL と呼ぶ。）を作成、発行

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

1.3.3 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、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組織（施設）をさす。

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、デジタル署名を公開鍵証明書の公開鍵で検証するモノである。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。

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。

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、本認証局で定める「認証業務運営会議」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

規定しない。

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。

- エンドエンティティ（EndEntity）

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

- オブジェクト識別子（Object Identifier）

  オブジェクトの識別を行うため、オブジェクトに関連付けられた一意な値。

- 活性化（Activate）

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

- 鍵長（Key Length）

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

- 鍵の預託（Key Escrow）

  第三者機関に鍵を預託すること。

・ 鍵ペア（Key Pair）

　私有鍵とそれに対応する公開鍵の対。

・ 加入者（Subscriber）

　認証局から認証のための電子証明書を発行される者。

・ 加入者証明書

　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。

・ 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。

・ 地域受付審査局（LRA：Local Reception Authority）

日本医師会に団体登録申請書を提出し、団体登録申請書で規定する事務取扱要領で定めた業務を実施する審査局のこと。

・ 電子署名（Electronic Signature）

電子文書の正当性を保証するために付けられる署名情報。公開鍵暗号などを利用し、相手が本人であることを確認するとともに、情報が送信途中に改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）

認証局運用についての規定集。認証局が電子証明書を発行するときに採用する実践に関する表明として位置付けられる。

・ 登録設備室

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

・ 認証設備室

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

・ 発行局（Issuer Authority）

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

・ ハッシュ関数（Hash Function）

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

・ プロファイル（Profile）

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

・ リポジトリ（Repository）

電子証明書及び証明書失効リストを格納し公開するデータベース。

・ リンク証明書

CA 鍵を更新する際に、新しい自己署名証明書（NewWithNew）と古い世代の CA 鍵と新しい世代の CA 鍵を紐付けるために発行される電子証明書。リンク証明書によって、世代の異なる CA から電子証明書を発行された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。

（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。

・ 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。

・ IA（Issuer Authority）

発行局を参照のこと。

・ LRA（Local Reception Authority）

地域受付審査局を参照のこと。

・ 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。

・ SHA256（Secure Hash Algorithm 256）

SHA-2 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
組織認証用証明書	http://crl.pki.med.or.jp/repository/crl/auth-o.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。

- 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
- 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、加入者の組織名称（ローマ字表記）を記載する。

3.1.2 名称が意味を持つことの必要性

本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し、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。

3.2.2 組織の認証

本認証局に保険医療機関等の組織の証明書を申請する際は、次の「表 3.2.1、3.2.2　組織の実在性および保健医療機関であることの立証書類」に示す書類を提出し、組織の実在性および保険医療機関等であることを登録局に立証するものとする。

なお、申請者個人の認証は「3.2.3 個人の認証」に定める方法による。

（1） 法人組織の場合および個人事業者の場合

表 3.2.1 組織の実在性および保健医療機関であることの立証書類

<table>
<tr><th></th><th colspan="2">文書名</th><th colspan="2">提出物</th><th>文書要件</th></tr>
<tr><td>①</td><td colspan="2">商業登記簿謄本</td><td rowspan="6">提出書類 A
（①～⑤の内の1点）+
⑥の提出</td><td rowspan="7">A 又は B のいずれかを提出</td><td rowspan="7">①～⑦の書類に、申請時点での組織の管理者の氏名が書かれたものであること。</td></tr>
<tr><td>②</td><td colspan="2">保健医療機関等の開設時に提出した開設届の副本のコピー</td></tr>
<tr><td>③</td><td>医療法 第14条の2（院内掲示義務）</td><td rowspan="3">掲示・提示を求められているもののコピー</td></tr>
<tr><td>④</td><td>薬事法施行規則 第3条（許可証の提示）</td></tr>
<tr><td>⑤</td><td>指定居宅サービス等の人員、設備及び運営に関する基準 第32条及びその準用条項（掲示）</td></tr>
<tr><td>⑥</td><td colspan="2">診療報酬の支払い後、審査支払機関から発行された直近3ヶ月以内の支払通知書のコピー（1か月分）</td></tr>
<tr><td>⑦</td><td colspan="2">保健医療機関等の指定を受けた際に地方厚生局より発行された指定通知書のコピー</td><td>提出書類 B
⑦の1点のみの提出</td></tr>
</table>

（2） 中央官庁/地方公共団体の運営する組織の場合

表 3.2.2 組織の実在性および保健医療機関であることの立証書類

	文書名	提出物	文書要件
①	認証局の定める文書に、公印規定で定める公印をなつ印した文書	提出文書 ①の1点のみの提出	申請時点での組織の管理者の氏名が書かれたものであること。

3.2.3 個人の認証

本認証局に保険医療機関等の組織の証明書を申請する際は、次のいずれかの方法で、組織管理者の実在性並びに申請者の実在性、組織所属の事実、組織の証明書申請意思を登録局に立証するものとする。

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）組織管理者もしくは組織所属者が申請する場合

＜持参の場合＞

表 3.2.3　組織管理者もしくは組織所属者が申請する場合の立証項目と内容＜持参＞

立証項目	内容
組織管理者の実在性	立証書類に組織の管理者の氏名が記載されていること。
申請者の実在性	申請者の氏名、所属組織住所、電話番号が記載され、登録局の窓口または登録局担当者に提出
申請者の組織所属の事実	組織の管理者の印と申請者の氏名が記載された申請書を、登録局の窓口または登録局担当者に提出
組織の申請の意思	申請者が登録局の窓口または登録局担当者に持参

＜郵送の場合＞

表 3.2.4　組織管理者もしくは組織所属者が申請する場合の立証項目と内容＜郵送＞

立証項目	内容
組織管理者の実在性	立証書類に組織の管理者の氏名が記載されていること。
申請者の実在性	申請者の氏名、所属組織住所、電話番号が記載されていること。
申請者の組織所属の事実	組織の管理者の印と申請者の氏名が記載された申請書を、登録局の窓口に郵送
組織の申請の意思	組織の管理者の印があるものを登録局に郵送

（2） 代理人が申請する場合

＜持参の場合＞

表 3.2.5　代理人が申請する場合の立証項目と内容＜持参＞

立証項目	内容
組織管理者の実在性	立証書類に組織の管理者の氏名が記載されていること。
申請者の実在性	申請者の氏名、所属組織住所、電話番号が記載され、登録局の窓口または登録局担当者に提出
申請者の組織所属の事実	組織の管理者の印と申請者の氏名が記載された申請書を、登録局の窓口または登録局担当者に提出

組織の申請の意思	申請者が登録局の窓口または登録局担当者に持参
代理人の実在性	代理人の氏名、生年月日、性別、住所、電話番号が記載された書類の原本を登録局の窓口または登録局担当者に提示
代理人の本人性	上の代理人の実在性を示す身分証明書（※）の原本を登録局の窓口または登録局担当者に提示
代理人の組織管理者からの委任の事実	当該組織の管理者の署名なつ印のある代理人の氏名が記載された委任状を登録局の窓口または登録局担当者に提出

（※）代理人が申請する場合に示す身分証明書は、次の「表 3.2.6　代理人が提示する本人確認書類」のとおり。

表 3.2.6　代理人が提示する本人確認書類

①　日本国旅券の原本	左記の内の１点（必須）
②　運転免許証の原本	
③　住民基本台帳カード（写真付のもの）の原本	
④　官公庁職員身分証明書（張り替え防止措置済みの写真付）の原本	
⑤　所属組織の職員証の原本	必須としないが提出がない場合は、別途所属の確認を行う。

※　提示を受けた原本のコピーを登録局にて保管する。

＜郵送の場合＞

代理人による郵送での申請は認めない。

3.2.4 確認しない加入者の情報

規定しない。

3.2.5 機関の正当性確認

規定しない。

3.2.6 相互運用の基準

規定しない。

3.3 鍵更新申請時の本人性確認および認証

3.3.1 通常の鍵更新時の本人性確認および認証

初回の証明書発行と同様の手順により申請するものとする。

3.3.2 証明書失効後の鍵更新の本人性確認および認証

初回の証明書発行と同様の手順により申請するものとする。

3.4 失効申請時の本人性確認および認証

加入者が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. 医療機関の管理者もしくは申請者は、失効を申請する証明書を特定する。
2. 認証局へのＩＣカードの返却の要否、方法等について、医療機関の管理者もしくは申請者は、認証局の指示に従うものとする。
3. 当該管理者もしくは申請者から失効の申請書を認証局に提出するものとし、認証局はその真偽を確認の上、失効を行うものとする。

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

証明書の申請者は、保険医療機関等の組織管理者とする。

本 CPS に則り発行される証明書は、それ以外からの申請は受け付けない。

4.1.2 申請手続および責任

証明書の利用を希望する組織は、認証局で定める以下のいずれかの手続きによって証明書の利用申請を行う。

1. 持参

保険医療機関等の組織管理者もしくは当該組織に所属する申請者が登録局もしくは登録局担当者に「3.2.2 組織の認証」、「3.2.3 個人の認証」および認証局の定める書類を持参することにより利用申請を行う。

2. 郵送

保険医療機関等の組織管理者もしくは当該組織に所属する申請者が登録局に「3.2.2 組織の認証」、「3.2.3 個人の認証」および認証局が定める書類を郵送することにより利用申請を行う。

4.2 証明書申請手続き

4.2.1 本人性および資格確認

・ 保険医療機関等の組織からの申請により発行する場合

本人性（組織）および資格の確認については、それぞれ以下の方法により実施する。

1. 組織への証明書発行

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

・ 組織管理者もしくは組織所属者からの申請の場合

（1） 持参の場合

申請者から提示された各種の書類について、記載事項が一致していることの確認や有効期限が切れてないことの確認を実施する。また、申請者が組織管理者でない組織所属者の場合、職員証等の組織所属の証明書を所持していれば提示を求め、所持していない場合は、申請書に記載されている組織の電話番号に電話し、組織が存在および申請者が在籍していることを確認する。

ただし、組織が中央官庁・地方公共団体の運営する機関で、当該機関の実在性が明らかな場合は、公印の押された認証局の定める書類の提出を求めることで、問い合わせによる確認を省略する。

また、保険医療機関等であることの確認は、地方厚生局が所管し公開している、全保険医療機関・保険薬局一覧等を用いて確認を行う。

なお、確認に用いた証明書等は登録局でコピーを取り、１０年間保存を行う。

(2)　郵送の場合

申請者から提示された各種の書類について、記載事項が一致していることの確認や有効期限が切れていないことの確認を実施する。また、申請書記載の組織の電話番号に電話し、組織が存在および申請者が在籍していることを確認する。

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

以降、持参の場合と同じ確認を行うものとする。

・ 登録局の審査業務の一部を委託して発行する場合

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

この場合、本 CPS に則った組織の実在性および保険医療機関等の確認を当該団体の管理者の責任のもと実施するものとする。

また、認証局と当該団体の間で委託もしくは委任に係わる契約を取り交わし、委託もしくは委任された業務に関して登録局に課せられると同等の業務内容、責任および義務を負うことを定めるものとする。

4.2.2 証明書申請の承認または却下

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

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

4.1 証明書発行

4.3.1 証明書発行時の認証局の機能

＜認証局が鍵ペアを生成する場合＞

認証局が鍵ペアを生成する場合は、「電子署名および認証業務に関する法律施行規則」第 6 条第三号に準じて CPS を規定し、運用する。

CPS の規定としては、最低限以下の項目を含めるものとする。

加入者鍵ペアの生成は、認証設備室と同等の安全性が確保できる環境下で行い、アクセス権限管理、内部けん制等によりセキュリティ対策を講じていること。

加入者鍵ペアの転送や出力を行う場合も、十分なセキュリティ対策を講じていること。

また、加入者鍵ペアを転送、出力した後は、速やかに加入者鍵ペアを完全に廃棄もしくは消去すること。

加入者鍵ペアの活性化に使用する PIN 等の生成、転送、出力等を行う場合も、十分なセキュリティ対策を講じていること。

また、PIN 等を生成、転送、出力した後は、速やかに PIN 等を完全に廃棄もしくは消去すること。

4.3.2 証明書発行後の通知

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

4.4 証明書の受理

4.4.1 証明書の受理

認証局は、電子証明書を交付した後、受領した旨を「受領書」の受け取りをもって確認する。

なお、認証局は、証明書を交付してから 28 日以内に受領が確認できない場合、証明書を失効させるものとする。

4.4.2 認証局による証明書の公開

認証局は、加入者の認証用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認証局による証明書発行通知

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、私有鍵を認証用途にのみ利用する。

4.5.2 検証者の公開鍵と証明書の利用目的

検証者は、加入者の認証用途で公開鍵と証明書を利用する。

4.6 証明書更新

4.6.1 証明書更新の要件

本 CPS に則り認証局から発行される証明書は、証明書更新は行わない。

4.6.2 証明書の更新申請者

規定しない。

4.6.3 証明書更新の処理手順

規定しない。

4.6.4 加入者への新証明書発行通知

規定しない。

4.6.5 更新された証明書の受理

規定しない。

4.6.6 認証局による更新証明書の公開

規定しない。

4.6.7 他のエンティティへの証明書発行通知

規定しない。

4.7 証明書の鍵更新（鍵更新を伴う証明書更新）

4.7.1 証明書鍵更新の要件

本 CPS に則り認証局から発行される証明書は、証明書鍵変更を行わない。

4.7.2 鍵更新申請者

規定しない。

4.7.3 鍵更新申請の処理手順

規定しない。

4.7.4 加入者への新証明書発行通知

規定しない。

4.7.5 鍵更新された証明書の受理

規定しない。

4.7.6 認証局による鍵更新証明書の公開

規定しない。

4.7.7 他のエンティティへの証明書発行通知

規定しない。

4.8 証明書変更

4.8.1 証明書変更の要件

本 CPS に則り認証局から発行される証明書は、証明書変更を行わない。

4.8.2 証明書の変更申請者

規定しない。

4.8.3 証明書変更の処理手順

規定しない。

4.8.4 加入者への新証明書発行通知

規定しない。

4.8.5 変更された証明書の受理

規定しない。

4.8.6 認証局による変更証明書の公開

規定しない。

4.8.7 他のエンティティへの証明書発行通知

規定しない。

4.9 証明書の失効と一時停止

4.9.1 証明書失効の要件

認証局は、次の場合に証明書を失効するものとする。

＜組織管理者もしくは組織所属者から失効申請があった場合＞

組織管理者もしくは組織所属者からの失効申請と確認された場合は、理由の如何に関わらず証明書を失効させなくてはならない。

＜認証局の職員から失効申請があった場合＞

次の各項に該当する場合、証明書を失効させる。

- 加入者が、本 CPS、またはその他の契約、規制、あるいは有効な証明書に適用される法に基づく義務を満たさなかった場合。
- 私有鍵の危殆化が認識されたか、その疑いがある場合。
- 証明書に含まれる該当の情報が正確でなくなった場合。(例えば、保険医療機関等の保健医療福祉分野専門資格を喪失した場合)。
- 本 CPS に従って証明書が適切に発行されなかったと認証局が判断した場合。
- 加入者の特定ができない場合で、緊急に失効させる必要があると認証局が判断した場合。

4.9.2 失効申請者

認証局は、次の 1 人またはそれ以上の者および組織からの失効申請を受け付ける。

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

4.9.3 失効申請の処理手順

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

＜組織管理者もしくは組織所属者からの失効申請の場合＞

失効を要求している申請者が、失効される証明書に記されている組織の管理者もしくは組織所属者であることを確認する。確認にあたっては、最低限、認証局で保存してある「4.2.1 本人性および組織の認証」で用いた申請者の各種書類を参照する。

上記それぞれの確認と共に、証明書の失効理由を確認し、その真偽についても確認を行うものとする。

この手順により証明書の失効を実施した場合は、CRL を発行する。

また、証明書の失効の事実を認証局の定める方法により申請者に通知するものとする。

＜認証局の職員からの失効申請の場合＞

認証局は「4.9.1 証明書失効の要件」の中の認証局の職員から失効申請があった場合は、速やかに当該証明書を特定し、失効の事由の真偽の確認を実施する。また、失効事由が真実であった場合は速やかに証明書を失効させるものとする。

証明書の失効を実施した場合は、CRL を発行する。また、証明書の失効の事実を認証局の定める方法により申請者に通知するものとする。

4.9.4 失効における猶予期間

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

4.9.5 認証局による失効申請の処理期間

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

4.9.6 検証者の失効情報確認の要件

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

4.9.7 CRL 発行頻度

変更がない場合においても、48 時間以内に 96 時間以内の有効期限の CRL を発行する。失効の通知は直ちに公開する。CRL に変更があった場合はいつでも更新する。また、認証局私有鍵（以下、CA 私有鍵という）、加入者の私有鍵の危殆化等が発生した場合は、CRL を直ちに発行するものとする。

4.9.8 CRL が公開されない最大期間

CRL は発行後 24 時間以内に公開される。

4.9.9 オンラインでの失効／ステータス情報の入手方法

規定しない。

4.9.10 オンラインでの失効確認要件

規定しない。

4.9.11 その他利用可能な失効情報確認手段

使用しない。

4.9.12 鍵の危殆化に関する特別な要件

認証局は、CA 署名鍵の危殆化の際には関連組織に直ちに通知するものとする。

4.9.13 証明書一時停止の要件

一時停止は行わない。

4.9.14 一時停止申請者

一時停止は行わない。

4.9.15 一時停止申請の処理手順

一時停止は行わない。

4.9.16 一時停止期間の制限

一時停止は行わない。

4.10 証明書ステータスの確認サービス

4.10.1 運用上の特徴

規定しない。

4.10.2 サービスの利用可能性

規定しない。

4.10.3 オプショナルな仕様

規定しない。

4.11 加入の終了

加入者は、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、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。

（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、加入者もしくは地域受付審査局から郵送または地域受付審査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。

（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 5.2.1 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 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 ・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。

（1）証明書の発行申請に関する文書

- 利用申請書
- 団体申請書
- 加入者の本人性の立証書類のコピー
- 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。

（2）証明書の失効申請に関する文書

- 失効申請書

（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
- 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。

（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、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、本会の判断により対策を決定し、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

本認証業務は、当該実証事業の用に供するものであり、業務の終了に関する諸条件は申請者との合意の下に決定するものとする。また、実証事業の終了をもって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させる。必要な場合にのみリポジトリに CRL を公開する。検証者等に対しては、必要な場合のみ情報公開用 Web サイトにて業務終了等の告知を行う。

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カードに格納する。

本認証局は、個別申請の場合は正当な加入者に加入者私有鍵を所有させるため、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。

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

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 sha1WithRSAEncryption を設定し、、RSA アルゴリズムは 1024bit 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。

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

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。

また、加入者の認証用私有鍵の有効期間は 2 年とし、公開鍵の有効期間は 2 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 のとおりとする。

表 7.1.1　証明書とプロファイル対応表

証明書種別	基本領域プロファイル	拡張領域プロファイル
組織認証用 CA 証明書	表 7.1.2	表 7.1.3
組織認証用証明書	表 7.1.4	表 7.1.5

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 7.1.5　HPKI 組織名テーブル（codeDataFreeText の定義）のとおりとする。

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、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は、表 7.1.1 のとおりである。

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 のとおりである。

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　組織認証用 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	○	sha1WithRSAEncryption
Validity	○	
NotBefore	○	発行日時（UTCTime で設定する。）
NotAfter	○	thisUpdate + 20 年（UTCTime で設定する。）
Issuer	○	CountryName は Printable、それ以外は UTF-8 で記述する
CountryName	○	JP
OrganizationName	○	Japan Medical Association
OrganizationUnitName	○	Regulated Healthcare Professional Union CA
CommonName	○	HPKI-01-HPKI_J-forAuthentication-forOrganization
Subject	○	CountryName は Printable、それ以外は UTF-8 で記述する
CountryName	○	JP
OrganizationName	○	Japan Medical Association
OrganizationUnitName	○	Regulated Healthcare Professional Union CA
CommonName	○	HPKI-01-HPKI_J -forAuthentication-forOrganization
SubjectPublicKeyInfo	○	
Algorithm	○	rsaEncryption
SubjectPublicKey	○	RSA 公開鍵値(2048bit)
IssuerUniqueID	×	
SubjectUniqueID	×	
Extensions	○	拡張領域（表 7.1.3）参照

表中の、「○」設定、「×」は設定しないことを表す。

表 7.1.3　組織認証用 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= Japan Medical Association ou= Regulated Healthcare Professional Union CA ou= HPKI-01-HPKI_J-forAuthentication-forOrganization	
authorityCertSerial	○	この証明書のシリアル番号	
subejctKeyIdentifier	○	この証明書の公開鍵の SHA-1 ハッシュ値	FALSE
KeyUsage	○	KeyCertSign	CRLSign	TRUE
DeciphermentOnly	×		-
extendedKeyUsage	×		-
privateKeyUsagePeriod	×		-
certificatePolicies	×		
policyMapping	×		-
subjectAltName	×		-
issuerAltName	×		-
subjectDirectoryAttributes	×		-
basicConstraints	×		TRUE
CA	○		TRUE-
pathLenConstraints	×		-
nameConstraints	×		-
policyConstraints	×		-
cRLDistributionPoints	×		-
subjectInfoAccess	×		-
authorityInfoAccess	×		-

表中の、「○」は設定、「×」は設定しないことを表す。

表 7.1.4　組織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	○	sha1WithRSAEncryption
Validity	○	
NotBefore	○	発行日時（UTCTime で設定する。）
NotAfter	○	thisUpdate + 2 年（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	○	Regulated Healthcare Professional Union CA
CommonName	○	HPKI-01-HPKI_J- forAuthentication-forOrganization
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（固定）
LocalityName	△	都道府県名を記載する。
OrganizationName	○	加入者となる医療機関等が運営団体に所属している場合は必須。その場合は所属する運営団体の名称運営団体名をローマ字あるいは英語名で OrganizationName に記載し、OrganizatioUnitName に医療福祉機関の種類を格納する。
OrganizationUnitName	○	
CommonName	◎	医療機関名称を UTF-8 でローマ字あるいは英語名で記載する。
SerialNumber	△	保険医療機関番号などを記載することができる。
SubjectPublicKeyInfo	○	
Algorithm	○	rsaEncryption
SubjectPublicKey	○	RSA 公開鍵値(1024bit)
IssuerUniqueID	×	
SubjectUniqueID	×	
Extensions	○	拡張領域（表 7.1.4）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 7.1.5　組織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= Japan Medical Association ou= Regulated Healthcare Professional Union CA cn= HPKI-01-HPKI_J-forAuthentication-forOrganization	
authorityCertSerial	○	上位証明書のシリアル番号	
subejctKeyIdentifier	○	この証明書の公開鍵の SHA-1 ハッシュ値	FALSE
KeyUsage	○	DigitalSignature	TRUE
DeciphermentOnly	×		-
extendedKeyUsage	×		-
privateKeyUsagePeriod	×		-
certificatePolicies	○		TRUE
policyIdentifier	○		
certPolicyId	○	1.2.392.100495.1.5.1.3.3.1	
policyQualifiers	○		
cPSuri	○	http://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/auth-o.crl	
subjectInfoAccess	×		-
authorityInfoAccess	×		-

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。組織名は、表 7.1.5 に示すように英語表記を用い UTF8string で設定する。

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

本拡張は、加入者が保険医療機関等の組織の場合に設定することができる。

表 7.1.5　HPKI 組織名テーブル（codeDataFreeText の定義）

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

注）組織名のワード間の空白は一個の Space (x20)とする。

（2）HPKI hcRole 属性プロファイル

本 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 ‘insurance medical care facility’ などの英語表記の資格名を用いる。また、DirecroryString は UTF8String でエンコードしたものを使う。マッチングルールはバイナリーマッチングによる。

7.2 証明書失効リストのプロファイル

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 のとおりとする。

失効リスト種別	基本領域	CRL エントリ拡張領	CRL 拡張領域
組織認証用証明書失効リスト	表 7.2.2	表 7.2.3	表 7.2.4

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　組織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		○	sha1WithRSAEncryption
Issuer		○	CountryName は Printable、それ以外は UTF-8 で記述する
	CountryName	○	JP
	OrganizationName	○	Japan Medical Association
	OrganizationUnitName	○	Regulated Healthcare Professional Union CA
	CommonName	○	HPKI-01-HPKI_J-forAuthentication-forOrganization
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 7.2.3）参照
CrlExtensions		○	拡張領域（表 7.2.4）参照

表 7.2.3　組織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 7.2.4　組織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	○	CountryName は Printable、それ以外は UTF-8 で記述する	
directoryName		c=JP o= Japan Medical Association ou= Regulated Healthcare Professional Union CA ou= HPKI-01-HPKI_J-forAuthentication-forOrganization	
authorityCertSerial	○	認証局証明書の証明書シリアル番号	
IssuerAltName	×		-
CRLNumber	○	128bit 以下の正の整数	
DeltaCRLIndicator	×		-
IssueingDistributionPoint	×		
FreshesCRL	×		-

7.3 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

本認証局は、準拠性監査の適用を受けない。

8.1 監査頻度

規定しない。

8.2 監査者の身元・資格

規定しない。

8.3 監査者と被監査者の関係

規定しない。

8.4 監査テーマ

規定しない。

8.5 監査指摘事項への対応

規定しない。

8.6 監査結果の通知

規定しない。

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。

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 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 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 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）利用規約の遵守責任

加入者の電子証明書は、本 CPS に従って発行される。そのため、加入者は、本 CPS に規定される利用規約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）利用規約の遵守責任

本認証局から発行される電子証明書は、本 CPS に従って発行される。そのため、検証者は、本 CPS に示す規定される利用規約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約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

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、認証局代表者が承認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、本会が無効と宣言した時点又は本認証業務を終了した時点で無効となる。

9.10.3 終了の影響と存続条項

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。

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

本認証局は、以下に定める事由が発生したときには、利用者、或いは契約企業へ通知または催告をすることなく、利用者、或いは契約企業との契約を解除できるものとする。

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

② 利用者、或いは契約企業の代表者、責任者、又は実質的に経営権を有する者が暴力団等である場合、又は、暴力団等への資金提供を行う等、密接な交際のある場合

③ 利用者、或いは契約企業が自ら又は第三者を利用して、他方当事者に対して、自身が暴力団等である旨を伝え、又は、関係者が暴力団である旨を伝えた場合

④ 利用者、或いは契約企業が自ら又は第三者を利用して、他方当事者に対して、詐術、暴力的行為又は脅迫的言辞を用いた場合

⑤　利用者、或いは契約企業が自ら又は第三者を利用して、他方当事者の名誉や信用等を毀損し、又は、毀損するおそれのある行為をした場合

⑥　利用者、或いは契約企業が自ら又は第三者を利用して、他方当事者の業務を妨害した場合、又は、妨害するおそれのある行為をした場合

以上

提出書類について

法人組織もしくは個人事業者の場合、下表の書類を提出願います。

<table>
<tr><th></th><th colspan="3">文書名</th><th colspan="2">提出物</th><th>文書要件</th></tr>
<tr><td rowspan="8">組織の実在性及び保健医療機関であることの立証書類</td><td>①</td><td colspan="2">商業登記簿謄本</td><td rowspan="7"><u>提出書類A</u>
（①②③の内の１点）+⑥の提出</td><td rowspan="8">A又はBのいずれかを提出</td><td rowspan="8">①～⑦の書類に、申請時点での組織の管理者の氏名が書かれたものであること。</td></tr>
<tr><td>②</td><td colspan="2">保健医療機関等の開設時に提出した開設届の副本のコピー</td></tr>
<tr><td>③</td><td>医療法　第１４条の２（院内掲示義務）</td><td rowspan="3">掲示・提示を求められているもののコピー</td></tr>
<tr><td>~~④~~</td><td>~~薬事法施行規則　第3条（許可証の提示）~~</td></tr>
<tr><td>~~⑤~~</td><td>~~指定居宅サービス等の人員、設備及び運営に関する基準　第32条及びその準用条項（掲示）~~</td></tr>
<tr><td>⑥</td><td colspan="2">診療報酬の支払い後、審査支払機関から発行された直近3ヶ月以内の支払通知書のコピー（1ケ月分）</td></tr>
<tr><td>⑦</td><td colspan="2">保健医療機関等の指定を受けた際に地方厚生局より発行された指定通知書のコピー</td><td><u>提出書類B</u>
⑦の１点のみの提出</td></tr>
</table>

組織認証カード利用申請書+別紙　組織認証カード利用者リストと合わせて、
書留（または簡易書留）郵便にて、日医電子認証センターに郵送願います。

2014 年 6 月 24 日 Ver.1.1

日本医師会組織認証カード（補助作業者用）利用規約

平成 25～26 年度地域医療連携の普及に向けた健康情報活用基盤実証事業用

（日本医師会のサービス）

公益社団法人日本医師会（以下、「本会」という。）は、次の各サービスを本会の「公益社団法人日本医師会電子認証センター」（以下、「電子認証センター」という。）を通じて、実証事業用に医師、歯科医師、薬剤師を除く医療従事者向けの「組織認証用PKI電子証明書発行サービス」を提供します。

「日本医師会組織認証カード（補助作業者用）利用規約」（以下、「本規約」という。）は、組織認証カードの利用者が遵守すべき事項を定めます。

第1条 （総則）

本会が定める「日本医師会組織認証用 PKI 認証局運用規程」（CPS: Certification Practice Statement 以下、「CPS」という。）および本規約は、本サービスの変更に伴い変更される場合があります。

第 2 条 （サービス内容）

1. 本会は、申請組織（施設）からの利用申込みを受け付けし、審査の後に、申請組織（施設）の従事者用の組織認証カードを発行します。
2. 本会は、CPSおよび本規約に同意した利用者に対して、利用者公開鍵（利用者署名検証符号）および利用者秘密鍵（利用者署名符号）を生成し、電子証明書を IC カードに格納し、ICカード券面に必要事項を記載した組織認証カードとして提供します。
3. 組織認証カードは、当該実証事業における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途においてのみ利用できるものとします。

第 3 条 （利用者の義務）

1. 組織認証カードの利用に際してはCPSおよび本規約に同意し、遵守するとともに、CPSおよび本規約に記載の用途でのみ組織認証カードを利用しなければなりません。
2. 組織認証カードの利用申込みに際しては、申請組織（施設）が正確な申込み内容を本会に提出しなければなりません。
3. 組織認証カードは、他人に貸与または譲渡してはなりません。
4. 組織認証カードを紛失もしくは破損した場合は、速やかに本会に届け出なければなりません。
5. 組織認証カードの記載事項に変更が生じた場合、また、これらの有効期限が満了した場合の取り扱いについて、本会の指示に従わねばなりません。
6. 組織認証カードの利用者は、電子証明書に対応する秘密鍵とそれに対応する暗証番号を、十分に注意して管理し、秘匿し続けなければなりません。
7. 組織認証カードに記録されている事項に変更が生じた場合もしくは組織認証カードの利用を中止する場合においても、遅滞なく必要な手続きを行わなければなりません。
8. 電子証明書の利用者は、リポジトリを随時閲覧し本サービスに関する情報を適宜取得しなくてはなりません。

第 4 条 （組織認証カードの利用申込み先）

1. 利用申請組織（施設）は、本会認証局の登録局が定める場所で、申し込みを行います。
2. 申請組織（施設）は、登録局の責任者経由で本会に組織認証カードの発行申請がなされることを承諾しなければなりません。

第 5 条 （組織認証カードの利用申込み審査）

本会は、受理した申請書類を、所定の手続に従い審査して、問題が無いことの確認をもって、申請組織（施設）を利用者として位置付け、組織認証カードの発行手続を開始します。

第 6 条 （組織認証カードの送付）

本会は、組織認証カードを安全に利用者に提供するために、安全な手段と方法を使って申請組織（施設）宛に提供します。

第 7 条 （暗証番号の管理）

1. 申請組織（施設）および当該組織（施設）に従事する利用者（以下、これらを区別する必要がない場合は合わせて「利用者」という。）は、組織認証カードの利用開始にあたって初期暗証番号を利用個人のみが知り得る暗証番号に変更して使用するものとするし、暗証番号を紛失したり、盗用されたりしないよう一切の管理義務を負うものとします。
2. 利用者は以下の場合、電子証明書の失効申請手続を行なわなければなりません。また、電子証明書が再度必要な場合は、組織認証カードの再発行等の手続を行わなければなりません。
   （1） 暗証番号を紛失してしまった場合
   （2） 暗証番号の漏洩または、そのおそれがある場合
   （3） 暗証番号が分からなくなった場合
   （4） 暗証番号の入力ミスで IC カードが利用できなくなった場合
   （5） その他 本会が必要と認めた場合
3. 暗証番号は、15 回連続で間違えて入力すると電子証明書を利用することが出来なくなります。暗証番号の再発行もしくは再設定は、本会が定める手続きを行うものとします。

第 8 条 （組織認証カードの有効期間）

1. 組織認証カードの券面記載の有効期限は、組織認証カードの発行から2年となります。
2. 本規約に定める組織認証カードの返却がなされた場合を除き、利用者は電子証明書を有効期限内で利用できます。
3. ただし、実証期間の終了と共に、組織認証カードを返却していただくと共に、当該組織認証カードの失効手続きを行う必要があります。

第 9 条 （本会による電子証明書の失効）

1. 本会は、以下に定める事由が発生したとき、組織認証カードの返却を求める、もしくは電子証明書を失効させる権限を有するものとします。
   （1） 利用者の所属、資格に変更が生じたとき
   （2） 利用者が CPS および本規約に基づく義務に違反した場合
   （3） 電子証明書秘密鍵が危殆化もしくはその恐れがあると本会が認めた場合
   （4） 電子証明書秘密鍵が不正利用された場合、もしくはその危険性があると本会が認めた場合
   （5） 認証局の CA 秘密鍵が危殆化もしくはその恐れがある場合
   （6） 組織認証カードの記載情報に事実と相違があり、またはその情報が変更されたことを本会が確認した場合
   （7） 組織認証カードの規格変更がなされた場合
   （8） その他、本会が必要と判断した場合
2. 本会は、電子証明書失効させたときには、速やかに利用者にこれを通知します。但し、利用者に通知することが不可能な場合には、この限りではありません。利用者は、本会による組織認証カードの返却要求もしくは電子証明書の失効に関し、本会の指示に従わねばなりません。

第 10 条 （組織認証カードの返却）

1. 利用者において、以下の各項に該当する場合は、有効期限内といえども、組織認証カードの返却に関して、本会の指示に従わねばなりません。
   （1） CPS および本規約で定める利用者の義務に反したとき
   （2） 組織認証カードの有効期限が切れたとき
   （3） 利用者（個人）が死亡した場合

（4） 組織認証カードが、利用中止、再発行等、本規約で定める事由が発生したとき
（5） その他、実証事業の終了等、本会が必要と認めたとき

2. 組織認証カードの再発行、組織認証カードの利用中止、不適切な利用もしくは本会が返却を求める場合、本会の指示に従い組織認証カードの返却をしなければなりません。
紛失等で、利用者が組織認証カードを本会に返却できない場合は、その措置について本会の指示に従わなくてはなりません。

第 11 条 （失効情報の公開）

1. 本会は、失効した電子証明書に関する情報を証明書失効リスト「Certification Revocation List」（以下、「CRL」という。）としてすみやかにリポジトリに掲載します。
2. 本会は、CRL を 48 時間ごとに更新します。

第 12 条 （電子証明書失効後の秘密鍵の管理）

1. 利用者は、電子証明書が失効された後も、利用者秘密鍵を適正に管理しなければならないものとします。
2. 前 1 項に定めた管理義務を怠ったことにより利用者が被った損害について、本会は、一切の責任を負わないものとします。

第 13 条 （個人情報の取扱い）

1. CPSおよび本規約において個人情報とは、特定の利用者を識別することができる情報をいいます。
2. 本会は、組織認証カードの利用申込み時に提出される個人情報および失効、再発行等の申請時に提出される個人情報を、組織認証カード、電子証明書に記載するなど認証業務の用以外には、利用者の承諾を得ることなく使用することはありません。

第 14 条 （法執行機関への情報開示）

本会は、本会で取扱う情報に対し、法的根拠に基づいて情報を開示するように請求があった場合には、法の定めに従い、法執行機関へ情報を開示します。

第 15 条 （利用者等の準備事項）

利用者は、自らの責任と負担において本サービスを利用するために必要な機器、ソフトウェアおよび回線等の設備一式を準備するものとします。

第 16 条 （知的財産権）

利用者は、本サービスに関するマニュアル、CPS などについての著作権その他知的財産権など全ての権利が本会に留保されていることを承認するものとします。

第 17 条 （利用者の損害賠償責任）

利用者がCPSおよび本規約で定める範囲以外の用途あるいは本規約で定める失効等の申請を怠った結果、あるいは組織認証カードの紛失もしくは返却義務を果たさない結果で生じたトラブルについは、利用者が一切の責任を負うものとします。当該トラブルにより本会および署名検証者（利用者の組織認証カードの情報に基づき、利用者の電子署名を検証する者（以下同じ））に損害を与えた場合、利用者が本会および署名検証者に対し、損害賠償を行なうものとします。

第 18 条 （本会の損害賠償責任）

1. 本会は、CPSおよび本規約に定める責任に違反したことにより、利用者に損害を与えた場合には、その損害の賠償責任を負うものとします。但し、本会の責に帰すことができない事由から生じた損害および逸失利益については、賠償責任を負わないものとします。
2. 本会が損害賠償責任を負う場合には、その賠償額において本会が現に受領した対価の合計額を超過しない範囲に限るものとします。
3. 具体的な賠償の方法については、問題発生ごとに利用者に明示します。

第 19 条 （免責事項）

1. 本会は、利用者が第 2 条第 3 項で定める用途以外に組織認証カードを使用することに対して、一切の責任を負わないものとします。
2. 本会は、組織認証カードの紛失、盗難、不正な使用などによって利用者が被った損害に対して、一切の責任を負わないものとします。
3. 本会は、IC カードに格納されている利用者秘密鍵の盗難、不正使用などによって利用者が被った損害に対して、一切の責任を負わないものとします。
4. 本会は、利用者の暗証番号の盗難、不正使用などによって利用者が被った損害に対して、一切の責任を負わないものとします。
5. 本会は、電子証明書の失効申請に対し、遅滞なく失効をおこなった場合、リポジトリへの CRL の公開前に発生した利用者の被害に対し、一切責任を負わないものとします。
6. 本会は、利用者が、電子証明書を利用する際に発生したコンピュータシステムなどのハードウェアもしくはソフトウェアへの障害について、一切の賠償責任を負わないものとします。
7. 本会は、以下に定める事由による本サービスの全部または一部の停止によって利用者が被った損害については、一切の損害賠償責任を負わないものとします。
（1） 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、または、その他の自然現象
（2） 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）または革命
（3） 裁判所、政府または地方機関による作為または不作為
（4） ストライキ、工場閉鎖、労働争議
（5） 本 CPS および本規約に基づく義務の遂行上必要とする必須の機器、物品、供給物もしくはサービス（電力、ネットワークその他の設備を含むがそれに限らない）が利用不能となった場合

本会は、その他本会の責に帰すべきでない事由から生じた利用者の損害については、一切の損害賠償責任を負わないものとします。

第 20 条 （通知）

1. 本会は、利用者への通知方法として、郵便、FAX、電子メールまたは電子認証センターのホームページへの掲示など、本会が適当と判断した方法により行います。
2. 第 1 項に定める郵便による通知においては、当該郵便の消印を利用者への到達時とみなします。
3. 第 1 項に定める FAX による通知においては、当該 FAX を本会が送信し、送信できたことが確認できた時点とみなします。
4. 第 1 項に定める電子メールによる通知においては、当該電子メールを本会の運営要員が送信し、送信できたことが確認できた時点とみなします。
5. 第 1 項に定める電子認証センターのホームページへの掲示による通知においては、当該掲示の掲載日を利用者への到達時とみなします。

第 21 条 （譲渡の禁止）

利用者は、本サービスの提供を受ける権利を第三者に譲渡することができないものとします。

第 22 条 （認証サービスの変更）

本会は本サービスの全部または一部を変更することができます。
利用者や署名検証者への変更通知は、本サービスの仕様を変更後、速やかに CPS をリポジトリにて公開することにより、実施されたものとします。

第 23 条 （管轄裁判所）

利用者と本会との間に訴訟や法的行為が起こる場合、東京地方裁判所を管轄裁判所とします。

以上

公益社団法人日本医師会電子認証センター　宛
〒113-0021　東京都文京区本駒込2-28-8
文京グリーンコート17F

法人組織・個人事業者医療機関用

平成25～26年度地域医療連携の普及に向けた健康情報活用基盤実証事業用

組織認証カード利用申請書（事務職用）

申請日　平成　26　年　　月　　日

申請医療機関情報	保険医療機関番号 （レセプト申請時の7桁番号）		
	医療機関名		印
	院長氏名		
	医療機関住所		
	申請責任者所属・氏名	（所属）	（氏名）
	申請責任者電話番号		
	申請責任者E-MAIL		
	種別区分	□病院　□一般診療所　□有床診療所　□歯科診療所　□その他（　　）	
	設立形態	□法人組織　□個人事業者	

医療機関名（英語またはローマ字） 組織認証カード券面に印刷されます。	

本院は、当施設の従事者である別紙「組織証カード利用者リスト」に記載の者に実証システムの利用をさせたいので、組織認証カードの発行を申請します。

利用に当っては、「平成25～26年度地域医療連携の普及に向けた健康情報活用基盤実証事業用」にのみ使用すること、「実証事業システム利用規約」、「日本医師会組織認証カード（補助作業者用）利用規約」、「日本医師会組織認証用PKI認証局運用規程（CPS）」を遵守します。

看護師、管理栄養士など国家資格保有者は、本組織認証カードの利用申込書でなく、別途の手続きを願います。

別紙　組織認証カード利用者リスト

	氏名	氏名のヨミガナ	所属	資格・職種	初期パスワード（※）
記入例	能登　花子	ノト　ハナコ	医事課	事務	3356
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					
25					

（※）初期パスワードは、数字　4桁。 ご自分で決めて大きな文字で、判り易く記入ください。
初期パスワードでカードの利用を開始したら、ご自分のみが知るパスワードに変更して利用ください。