MEDIS ヘルスケア電子証明書発行サービス実施規程

Version.1.6

２０２０年７月

一般財団法人医療情報システム開発センター

改定履歴

版数	日付	内容
1.0	2007 年 3 月 23 日	初版
1.1	2015 年 3 月 27 日	保健医療福祉分野 PKI 認証局 証明書ポリシの項番に合わせた改訂 下位認証局向け CA 認証サービス廃止に伴う改訂 SHA256 対応認証局追加に伴う改修
1.2	2016 年 6 月 1 日	保健医療福祉分野 PKI 認証局 証明書ポリシ 1.5 版に合わせた改訂
1.3	2017 年 1 月 18 日	SHA256 対応認証用認証局追加に伴う改修
1.4	2017 年 3 月 30 日	URL 修正
1.5	2017 年 8 月 1 日	部署名変更に伴う修正
1.6	2020 年 7 月 1 日	SHA1 対応認証局記載削除

目次

1. はじめに 1

1.1 概要 2
1.2 文書の名前と識別 2
1.3 PKI の関係者 3
1.3.1 MEDIS 認証局 3
1.3.2 発行局 3
1.3.3 登録局 3
1.3.4 加入者 3
1.3.5 検証者 4
1.4 証明書の使用方法 4
1.4.1 適切な証明書の使用 4
1.4.2 禁止される証明書の使用 4
1.5 ポリシ管理 4
1.5.1 本 CPS を管理する組織 4
1.5.2 問い合わせ先 4
1.5.3 CPS のポリシ適合性を決定する者 5
1.5.4 CPS 承認手続き 5
1.6 定義と略語 5

2. 公開及びリポジトリの責任 12

2.1 リポジトリ 12
2.2 証明書情報の公開 12
2.3 公開の時期又はその頻度 12
2.4 リポジトリへのアクセス管理 12

3. 識別及び認証 13

3.1 名称決定 13
3.1.1 名称の種類 13
3.1.2 名称が意味を持つことの必要性 13
3.1.3 加入者の匿名性又は仮名性 13
3.1.4 種々の名称形式を解釈するための規則 13
3.1.5 名称の一意性 13
3.1.6 認識、認証及び商標の役割 13
3.2 初回の本人性確認 13
3.2.1 私有鍵の所持を証明する方法 13

3.2.2 組織の認証 13
3.2.3 個人の認証 15
3.2.4 確認しない加入者の情報 20
3.2.5 機関の正当性確認 20
3.2.6 相互運用の基準 20
3.3 鍵更新申請時の本人性確認及び認証 20
3.3.1 通常の鍵更新時の本人性確認及び認証 20
3.3.2 証明書失効後の鍵更新の本人性確認及び認証 20
3.4 失効申請時の本人性確認及び認証 21
4. 証明書のライフサイクルに対する運用上の要件 22
4.1 証明書申請 22
4.1.1 証明書の申請者 22
4.1.2 申請手続及び責任 22
4.2 証明書申請手続き 22
4.2.1 本人性及び資格確認 22
4.2.2 証明書申請の承認又は却下 25
4.2.3 証明書申請手続き期間 25
4.3 証明書発行 25
4.3.1 証明書発行時の認証局の機能 25
4.3.2 証明書発行後の通知 26
4.4 証明書の受理 26
4.4.1 証明書の受理 26
4.4.2 認証局による証明書の公開 26
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 26
4.5 鍵ペアと証明書の利用目的 26
4.5.1 加入者の私有鍵と証明書の利用目的 26
4.5.2 検証者の公開鍵と証明書の利用目的 26
4.6 証明書更新 26
4.7 証明書の鍵更新（鍵更新を伴う証明書更新） 27
4.7.1 証明書鍵更新の要件 27
4.7.2 鍵更新申請者 27
4.7.3 鍵更新申請の処理手順 27
4.7.4 加入者への新証明書発行通知 27
4.7.5 鍵更新された証明書の受理 27
4.7.6 認証局による鍵更新証明書の公開 27

4.7.7 他のエンティティへの証明書発行通知 27
4.8 証明書変更 27
4.9 証明書の失効と一時停止 27
4.9.1 証明書失効の要件 27
4.9.2 失効申請者 29
4.9.3 失効申請の処理手順 29
4.9.4 失効における猶予期間 30
4.9.5 認証局による失効申請の処理期間 31
4.9.6 検証者の失効情報確認の要件 31
4.9.7 CRL 発行頻度 31
4.9.8 CRL が公開されない最大期間 31
4.9.9 オンラインでの失効／ステータス情報の入手方法 31
4.9.10 オンラインでの失効確認要件 31
4.9.11 その他利用可能な失効情報確認手段 31
4.9.12 鍵の危殆化に関する特別な要件 31
4.9.13 証明書一時停止の要件 31
4.9.14 一時停止申請者 31
4.9.15 一時停止申請の処理手順 32
4.9.16 一時停止期間の制限 32
4.10 証明書ステータスの確認サービス 32
4.11 加入の終了 32
4.12 私有鍵預託と鍵回復 32
4.12.1 預託と鍵回復ポリシ及び実施 32
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 32
5. 建物・関連設備、運用のセキュリティ管理 33
5.1 建物及び物理的管理 33
5.1.1 施設の位置と建物構造 33
5.1.2 物理的アクセス 33
5.1.3 電源及び空調設備 33
5.1.4 水害及び地震対策 33
5.1.5 防火設備 34
5.1.6 記録媒体 34
5.1.7 廃棄物の処理 34
5.1.8 施設外のバックアップ 34
5.2 手続き的管理 34

5.2.1 信頼すべき役割.....34
5.2.2 職務ごとに必要とされる人数.....35
5.2.3 個々の役割に対する本人性確認と認証.....35
5.2.4 職務分轄が必要になる役割.....36
5.3 要員管理.....36
5.3.1 資格、経験及び身分証明の要件.....36
5.3.2 経歴の調査手続.....36
5.3.3 研修要件.....36
5.3.4 再研修の頻度及び要件.....36
5.3.5 職務のローテーションの頻度及び要件.....36
5.3.6 認められていない行動に対する制裁.....36
5.3.7 独立した契約者の要件.....37
5.3.8 要員へ提供する資料.....37
5.4 監査ログの取扱い.....37
5.4.1 記録するイベントの種類.....37
5.4.2 監査ログを処理する頻度.....37
5.4.3 監査ログを保存する期間.....37
5.4.4 監査ログの保護.....37
5.4.5 監査ログのバックアップ手続.....37
5.4.6 監査ログの収集システム（内部対外部）.....37
5.4.7 イベントを起こしたサブジェクトへの通知.....37
5.4.8 脆弱性評価.....38
5.5 記録の保管.....38
5.5.1 アーカイブ記録の種類.....38
5.5.2 アーカイブを保存する期間.....39
5.5.3 アーカイブの保護.....39
5.5.4 アーカイブのバックアップ手続.....39
5.5.5 記録にタイムスタンプをつける要件.....39
5.5.6 アーカイブ収集システム（内部対外部）.....39
5.5.7 アーカイブ情報を入手し、検証する手続.....40
5.6 鍵の切り替え.....40
5.7 危殆化及び災害からの復旧.....40
5.7.1 災害及び CA 私有鍵危殆化からの復旧手続き.....40
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.....40
5.7.3 CA 私有鍵が危殆化した場合の対処.....40
5.7.4 災害等発生後の事業継続性.....40

5.8 認証局又は登録局の終了 41
6. 技術的なセキュリティ管理 42
6.1 鍵ペアの生成と実装 42
6.1.1 鍵ペアの生成 42
6.1.2 加入者への私有鍵の送付 42
6.1.3 認証局への公開鍵の送付 42
6.1.4 検証者への CA 公開鍵の配付 42
6.1.5 鍵のサイズ 42
6.1.6 公開鍵のパラメータ生成及び品質検査 42
6.1.7 鍵の利用目的 42
6.2 私有鍵の保護及び暗号モジュール技術の管理 43
6.2.1 暗号モジュールの標準及び管理 43
6.2.2 私有鍵の複数人によるコントロール 43
6.2.3 私有鍵のエスクロウ 43
6.2.4 私有鍵のバックアップ 43
6.2.5 私有鍵のアーカイブ 43
6.2.6 暗号モジュールへの私有鍵の格納と取り出し 43
6.2.7 暗号モジュールへの私有鍵の格納 43
6.2.8 私有鍵の活性化方法 44
6.2.9 私有鍵の非活性化方法 44
6.2.10 私有鍵の廃棄方法 44
6.2.11 暗号モジュールの評価 44
6.3 鍵ペア管理に関するその他の面 44
6.3.1 公開鍵のアーカイブ 44
6.3.2 私有鍵と公開鍵の有効期間 44
6.4 活性化用データ 45
6.4.1 活性化データの生成とインストール 45
6.4.2 活性化データの保護 45
6.4.3 活性化データのその他の要件 45
6.5 コンピュータのセキュリティ管理 45
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 45
6.5.2 コンピュータセキュリティ評価 45
6.6 ライフサイクルの技術的管理 46
6.6.1 システム開発管理 46
6.6.2 セキュリティ運用管理 46

6.6.3 ライフサイクルのセキュリティ管理 46
6.7 ネットワークのセキュリティ管理 46
6.8 タイムスタンプ 46

7. 証明書及び失効リスト及び OCSP のプロファイル 47

7.1 証明書のプロファイル 47
7.1.1 バージョン番号 47
7.1.2 証明書の拡張（保健医療福祉分野の属性を含む） 47
7.1.3 アルゴリズムオブジェクト識別子 47
7.1.4 名称の形式 47
7.1.5 名称制約 48
7.1.6 CPS オブジェクト識別子 48
7.1.7 ポリシ制約拡張 48
7.1.8 ポリシ修飾子の構文及び意味 48
7.1.9 証明書ポリシ拡張フィールドの扱い 48
7.1.10 保健医療福祉分野の属性（hcRole） 61
7.2 証明書失効リストのプロファイル 65
7.2.1 バージョン番号 65
7.2.2 CRL と CRL エントリ拡張領域 65
7.3 OCSP プロファイル 69
7.3.1 バージョン番号 69
7.3.2 OCSP 拡張領域 69

8. 準拠性監査とその他の評価 70

8.1 監査頻度 70
8.2 監査者の身元・資格 70
8.3 監査者と被監査者の関係 70
8.4 監査テーマ 70
8.5 監査指摘事項への対応 70
8.6 監査結果の通知 70

9. その他の業務上及び法務上の事項 72

9.1 料金 72
9.2 財務上の責任 72
9.2.1 保険の適用範囲 72
9.2.2 その他の資産 72
9.2.3 エンドエンティティに対する保険又は保証 72

9.3 業務情報の秘密保護.....72
9.3.1 秘密情報の範囲.....72
9.3.2 秘密情報の範囲外の情報.....72
9.3.3 秘密情報を保護する責任.....73
9.4 個人情報のプライバシー保護.....73
9.4.1 プライバシーポリシ.....73
9.4.2 プライバシーとして保護される情報.....73
9.4.3 プライバシーとはみなされない情報.....73
9.4.4 個人情報を保護する責任.....73
9.4.5 個人情報の使用に関する個人への通知及び同意.....74
9.4.6 司法手続又は行政手続に基づく公開.....74
9.4.7 その他の情報開示条件.....74
9.5 知的財産権.....74
9.6 表明保証.....74
9.6.1 認証局の表明保証.....74
9.6.2 登録局の表明保証.....75
9.6.3 地域受付審査局の表明保証.....76
9.6.4 加入者の表明保証.....76
9.6.5 検証者の表明保証.....76
9.6.6 他の関係者の表明保証.....77
9.7 無保証.....77
9.8 責任制限.....77
9.9 補償.....78
9.10 本 CPS の有効期間と終了.....78
9.10.1 有効期間.....78
9.10.2 終了.....78
9.10.3 終了の影響と存続条項.....78
9.11 関係者間の個々の通知と連絡.....79
9.12 改訂.....79
9.12.1 改訂手続き.....79
9.12.2 通知方法と期間.....79
9.12.3 オブジェクト識別子（OID）の変更理由.....79
9.13 紛争解決手続.....80
9.14 準拠法.....80
9.15 適用法の遵守.....80
9.16 雑則.....80

9.16.1 完全合意条項 80
9.16.2 権利譲渡条項 80
9.16.3 分離条項 80
9.16.4 強制執行条項（弁護士費用及び権利放棄） 80
9.16.5 不可抗力 81
9.17 その他の条項 81

1. はじめに

MEDIS ヘルスケア電子証明書発行サービス実施規程（以下、「本 CPS」と言う。）は、一般財団法人医療情報システム開発センター（以下、「MEDIS」と言う。）が運営する「MEDIS 認証局（以下、「本認証局」と言う。）」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』及び『保健医療福祉分野 PKI 認証局 認証用（人）証明書ポリシ』（厚生労働省）に従う。

なお、本 CPS は、以下の文書に依存して構成される。

- IETF/RFC3647　Internet X.509 Public Key Infrastructure Certificate Policy and Certification 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 CPS 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 Update 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、本 CPS「1.3.4 加入者」に規定する者に対して署名用公開鍵証明書と認証用公開鍵証明書（以下、署名用公開鍵証明書と認証用公開鍵証明書を合わせて「加入者証明書」と言う。）を発行する。本認証局が発行する加入者証明書は、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（以下、「署名用 HPKI-CP」と言う。）」と「保健医療福祉分野 PKI 認証局 認証用（人）証明書ポリシ（以下、「認証用 HPKI-CP」と言う。）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」と言う。）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。

なお、本認証局は、以下の認証局を運営しているが、どちらの認証局も本 CPS に則り業務を実施する。以降、以下認証局を区別しない場合は、本認証局と呼ぶ。

・SHA256 対応署名用 MEDIS 認証局
・SHA256 対応認証用 MEDIS 認証局

1.2　文書の名前と識別

この規程の名称は、「MEDIS ヘルスケア電子証明書発行サービス実施規程」とする。本 CPS、認証業務運営主体である MEDIS 及び本認証局が発行する加入者証明書に関連したオブジェクト識別子（以下、「OID」と言う。）は、表 1.2.1 のとおりである。

表 1.2.1　本 CPS で定める OID

名称	オブジェクト名	オブジェクト識別子
一般財団法人医療情報システム開発センター	MEDIS	1.2.392.200119
MEDIS 認証局	MEDIS Certification Authority	1.2.392.200119.2.1
本 CPS	MEDIS CA CPS	1.2.392.200119.2.1.1
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、本認証局が実施す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。

なお、本認証局から発行する電子証明書を指す場合は「加入者証明書」と呼び、一般論としての電子証明書を指す場合は「電子証明書」と呼ぶ。

1.3.1 MEDIS 認証局

MEDIS 認証局は、発行局と登録局から構成され、厚生労働省のルート認証局を信頼点とした MEDIS が運用する認証局である。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、失効の場合は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、契約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、加入者証明書所有者である。加入者証明書所有者とは、証明書発行申請を行い本認証局により加入者証明書を発行される個人をさす。加入者証明書所有者の範囲は次

のとおりとする。

- 保健医療福祉分野サービスの提供者及び利用者。
- 上記の提供者の内、以下の者がその有する資格において、あるいは管理者として署名または認証を行う場合は、「その資格を有していること」あるいは「管理者であること」を証明書に記載しなくてはならない。
- 保健医療福祉分野に関わる国家資格を有する者。
- 医療機関等の管理者。

1.3.5 検証者

検証者とは、デジタル署名を公開鍵証明書の公開鍵で検証する者。

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の適用範囲は、次の通りとする。

- 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及び認証用。
- 患者等の保健医療福祉分野サービス利用者の署名検証用及び認証用。

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 本 CPS を管理する組織

本 CPS の管理組織は、一般財団法人医療情報システム開発センター 医療情報利活用推進部門とする。

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： 一般財団法人医療情報システム開発センター 医療情報利活用推進部門

受付時間：10：00～17：00 （MEDIS 休業日を除く）

電話番号：03-3267-1922

FAX 番号：03-3267-1931

e-mail アドレス：pki-ad@medis.or.jp

1.5.3 CPS のポリシ適合性を決定する者

本 CPS の策定者は、MEDIS とする。

本 CPS は、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（以下、「HPKI 認証局専門家会議」という。）に準拠性審査を受けることにより HPKI-CP に適合していることを決定される。

1.5.4 CPS 承認手続き

本 CPS は、MEDIS 理事長によって承認されるものとする。

1.6 定義と略語

（あ～ん）

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

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

- 暗号モジュール（Security Module）
  私有鍵や証明書等を安全に保管し、鍵ペア生成や署名等の暗号操作を行うハードウェアまた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（OID：Object Identifier）
  オブジェクトの識別を行うため、オブジェクトに関連付けられた一意な値。

- 活性化（Activate）
  鍵を署名などの運用に使用することができる状態にすること。逆に、使用できなく

することを非活性化という。

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

・ 鍵の預託（Key Escrow）
第三者機関に鍵を預託すること。

・ 鍵ペア（Key Pair）
私有鍵とそれに対応する公開鍵の対。

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

・加入者証明書
認証局から加入者に対して発行された公開鍵証明書のこと。

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

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

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

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

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

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

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

・ 証明書失効リスト（CRL : Certificate Revocation List、Authority Revocation List）
失効した電子証明書のリスト。
エンドエンティティの証明書の失効リストを CRL といい、CA の証明書の失効リストを ARL という。
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、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（CSR：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（CP：Certificate Policy）
共通のセキュリティ要件を満たし、特定のコミュニティ及び／又はアプリケーションのクラスへの適用性を指定する、名前付けされた規定の集合。

・ 申請者
認証局に電子証明書の発行を申請する主体のこと。

・ 地域受付審査局（LRA：Local Reception Authority）
MEDIS と業務委託契約を行い、業務委託契約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（RA：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。認証する加入者の識別と本人性認証に責任を負うが、電子証明書に署名したり、発行したりはしない。

・ 認証局（CA：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にする第三者機関で、公正、中立な立場にあり信頼できなければならない。

・ 認証局システム
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のこと。

・ 認証実施規程（CPS：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（IA：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）
認証局の証明書の失効リスト、前述の「証明書失効リスト」を参照のこと。

・ CA（Certification Authority）
前述の「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、厚生労働省 HPKI ルート認証局から発行されたサブ CA 証明書である。

・ CP（Certificate Policy）
前述の「証明書ポリシ」を参照のこと。

・ CPS（Certification Practice Statement）
前述の「認証実施規程」を参照のこと。

・ CRL（Certificate Revocation List）
前述の「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）
前述の「証明書発行要求」を参照のこと。

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

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

・ IA（Issuer Authority）
前述の「発行局」を参照のこと。

・ LRA（Local Reception Authority）
前述の「地域受付審査局」を参照のこと。

・ OID（Object ID）
前述の「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）
前述の「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）
SHA2 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。

2.2 証明書情報の公開

本認証局は、表 2.2.1 に示す情報をリポジトリに登録し加入者等他の関係者に公開する。それらの情報は、ウェブサイトから入手できる。

表 2.2.1 リポジトリで公開する情報とその URL

情報名称	URL
本認証局の CA 証明書	https://www.medis.or.jp/8_hpki/information.html
本認証局の CA 証明書のハッシュ値	
本 CPS	
SHA256 対応署名用 MEDIS 認証局の CRL	http://cert.medis.or.jp/sign/crl-sign2.crl
SHA256 対応認証用 MEDIS 認証局の CRL	http://cert.medis.or.jp/auth/crl-auth2.crl

また、その他 MEDIS 認証局利用規約は情報公開用ウェブサイトにて公開される。

2.3 公開の時期又はその頻度

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

2.4 リポジトリへのアクセス管理

本認証局は、HPKI-CP、本 CPS、加入者証明書及びそれらの加入者証明書の現在の状態などの公開情報を、加入者及び検証者に対してインターネットを通じて読み取り専用として公開する。

3. 識別及び認証

3.1 名称決定

3.1.1 名称の種類

本 CPS に基づいて発行する加入者証明書に使用するサブジェクト名は加入者名とする。

加入者名は X.500 の Distinguished Name を使用する。C は JP とする。また CommonName は必須で、加入者が個人である場合、加入者の氏名（ローマ字表記）を記載する。

3.1.2 名称が意味を持つことの必要性

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

3.1.3 加入者の匿名性又は仮名性

加入者証明書に記載される氏名として匿名又は仮名を使用することはできない。

3.1.4 種々の名称形式を解釈するための規則

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

3.1.5 名称の一意性

本認証局が発行する加入者証明書の加入者名（subjectDN）は認証局内で一意とするためにシリアル番号（以下、「SN」と言う。）を含むことができる。

また、本認証局の名称（以下、「issuerDN」と言う。）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

規定しない。

3.2 初回の本人性確認

3.2.1 私有鍵の所持を証明する方法

本認証局においては、加入者側で私有鍵を生成しない。そのため私有鍵の所持の正当性確認については定義しない。

3.2.2 組織の認証

本認証局に医療機関等の管理者の電子証明書を申請しようとする者は、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所属若しくは運営する組織の実在性を登録局に立証しなくてはならない。立証に用いる書類については、有効期間外のものや、資格喪失後のものを用いてはならない。

なお、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

登記事項証明書、保険医療機関等の開設時に提出した開設届の副本のコピー、保険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など公的機関から発行若しくは受領した証明書、各法等で掲示を求められているもの※のコピーのいずれかを提出することによって組織の実在性を立証する。

なお、指定通知書のコピーを提出した場合は、実在性及び保険医療機関等であることの立証が同時になされたものとするが、それ以外の証明書等で実在性を立証した場合、診療報酬の支払後、審査支払機関から発行される直近 3 カ月以内の支払通知書のコピーなど保険医療機関等であることを証明する書類の提出を必須とする。

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

(2) 個人事業者の場合

登記事項証明書、保険医療機関等の開設時に提出した開設届の副本のコピー、保険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など公的機関から発行若しくは受領した証明書、各法等で掲示を求められているもの※のコピー若しくはそれらに順ずる書類のいずれかを提出することによって組織の実在性を立証する。

なお、指定通知書のコピーを提出した場合は、実在性及び保険医療機関等であることの立証が同時になされたものとするが、それ以外の証明書等で実在性を立証した場合、診療報酬の支払後、審査支払機関から発行される直近 3 カ月以内の支払通知書のコピーなど保険医療機関等であることを証明する書類の提出を必須とする。

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

(3) 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、本認証局が定める発行申請書の指定箇所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。

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

※ 「各法等で掲示を求められているもの」とは、以下のようなものを指す。

- 医療法　第 14 条の 2（院内掲示義務）。
- 薬事法施行規則　第 3 条（許可証の掲示）。
- 指定居宅サービス等の事業の人員、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）。

＜電子証明書を用いる場合＞

前述の組織の運営区分に係わらず、保健医療福祉分野 PKI 認証局が発行する管理者向け電子署名用証明書を用いた電子署名若しくは商業登記認証局の発行する電子証明書を用いた電子署名により、実在性を立証することができる。

また、保険医療機関等であることの立証をする場合、保健医療福祉分野 PKI 認証局が発行する管理者向け電子署名用証明書による電子署名を用いる場合は、同時に保険医療機関等であることの立証がなされたとみなすが、商業登記認証局の発行する電子証明書を用いる場合は、別途、指定通知書のコピー、診療報酬の支払後、審査支払機関から発行される直近 3 カ月以内の支払通知書のコピーなど保険医療機関等であることを証明する書類の提出を認証局が定める方法により提出しなくてはならない。

なお、これらの方法を用いる場合でも、立証の際に用いる各種書類には、申請時点において組織の管理者である者の氏名が記載されていなくてはならない。

3.2.3 個人の認証

本認証局に電子証明書を申請しようとする個人は、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、本人性及び申請意思を登録局又は地域受付審査局に立証しなければならない。また、国家資格を有する者が国家資格を含んだ電子証明書、医療機関等の管理者が医療機関等の電子証明書を申請しようとする場合は、国家資格保有の事実、管理者であることの事実を登録局に立証しなくてはならない。立証に用いる書類については、有効期間外のものや、資格喪失後のものを用いてはならない。

なお、本節の定めは証明書申請者の立証に関わる定めであり、本認証局が電子証明書を交付する場合は、申請者が本節の規定に従い自身の実在性、本人性及び申請意思の立証を行い、4 章の規定に則り申請者の審査及び証明書の交付を実施する。

(1)　登録局へ申請する場合

＜持参もしくは交付時に本人が出頭する場合＞

登録局では、郵送による申請のみとする。

＜郵送による申請の場合＞

1. 個人の実在性

電子証明書を申請しようとする個人は、取得後 3 ヶ月以内の住民票（広域交付住民票を含む、以下、合わせて住民票とする）の写しに添えて、「MEDIS　HPKI 電子証明書発行・更新申請書（以下、「利用申請書」と言う。）」に当該個人の「氏名、生年月日、性別、住所」（以下、「基本 4 情報」と言う。）を記入し、登録局に郵送することで実在性の立証をしなくてはならない。

2. 個人の本人性

電子証明書を申請しようとする個人は、次に挙げる書類のコピーの適当な空欄に実印を捺印して登録局に郵送することで本人性の立証をしなくてはならない。なお、有効期限のある書類は、全て有効期限内のもののみが本人性の立証に有効である。

- 日本国旅券
- 運転免許証
  （運転経歴証明書を含む、以下、合わせて運転免許証とする）
- 住民基本台帳カード（写真付のもの）
- 個人番号カード
- 官公庁職員身分証明書（張り替え防止措置済みの写真付）

3. 個人の証明書申請の意思

電子証明書を申請しようとする個人は、印鑑登録証明書を添えて、利用申請書に実印を捺印することで申請者個人の申請意思を立証しなくてはならない。なお、印鑑登録証明書の有効期間は発行日より 6 ヶ月以内とする。但し、発行する地方公共団体が有効期限を設けている場合は、それを優先する。

4. 国家資格及び医療機関等の管理者権限

国家資格を有する者が国家資格情報を含んだ電子証明書を申請する場合は、官公庁の発行した国家資格を証明する書類（以下、「国家資格免許証等」と言う。）のコピーの適当な空欄に実印を捺印して登録局に郵送することで国家資格保有の事実を立証しなくてはならない。

医療機関等の管理者が医療機関等の管理者の電子証明書を申請する場合は、「3.2.2　組織の認証」で定める書類に、申請者本人が管理権限者として記載のある場合は、当該書類を登録局に郵送することで管理権限の事実の立証とみなす。記載がない場合は、申請者本人が管理権限を有すると公に告知している医療機関等のパンフレットなどを登録局に郵送することで、管理者であることの事実を立証しなくてはならない。

＜オンラインによる申請の場合＞

証明書を申請しようとする個人は、認証局の定める手続きに従い、公的個人認証サービスを利用した申請者個人の電子署名、保健医療福祉分野 PKI 認証局の発行する署名用証明書を用いた電子署名、若しくはそれに準じた電子署名を提供することにより、実在性及び本人性及び申請者個人の申請意思を立証しなくてはならない。

なお、公的個人認証サービス、保健医療福祉分野 PKI 認証局の署名用証明書等による電子署名は、当該本人しか実行できないことから、電子署名の提供によりこれらの意思を立証したものとみなされる。

(2)　地域受付審査局へ申請する場合

本認証局は、「1.3.3　登録局」で定める業務の一部を医療機関等に委託する場合がある。委託業務として、医療機関等（以下、「地域受付審査局」と言う。）に、当該地域受付審査局に所属する個人へ証明書を発行する際の審査業務を委託する。この場合、本 CPS「3.2.3 個人の認証（１）」に則った個人の認証を地域受付審査局の責任のもと実施しなくてはならない。

「3.2.3 個人の認証　（１）」に定められた審査の委託範囲については、本認証局と地域受付審査局との間で取り交わす契約の中で定めるものとする。

地域受付審査局は、利用申請を行う個人から提出された書類を纏め、別途定める申請書を作成し、登録局に提出する。

＜持参もしくは交付時に本人が出頭する場合＞

1.　個人の実在性

電子証明書を申請しようとする個人は、取得後 3 ヶ月以内の住民票の写しに添えて、利用申請書に当該個人の基本 4 情報を記入し、地域受付審査局の窓口に提出することで実在性の立証をしなくてはならない。

2.　個人の本人性

電子証明書を申請しようとする個人は、次に挙げる書類の原本を地域受付審査局の窓口で提示することで本人性の立証をしなくてはならない。なお、有効期限のある書類は、全て有効期限内のもののみが本人性の立証に有効である。

【1 点で確認できる書類】

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

【2 点提出が必要な書類】

- 健康保険証
- 国民健康保険証
- 共済組合員証
- 船員保険証
- 介護保険証
- 基礎年金番号通知書
- 国民年金手帳（証書）
- 厚生年金手帳（証書）
- 共済年金証書
- 印鑑登録証明書
  （6 ヶ月以内発行のものと登録印鑑）

3. 個人の証明書申請の意思

電子証明書を申請しようとする個人は、利用申請書に記名捺印または署名捺印を行うことで申請者個人の申請意思の立証がなされたものとみなす。

代理人が窓口で申請する場合は、印鑑登録証明書を添えて、認証局の定める委任状に実印を捺印したもの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。

4. 国家資格及び医療機関等の管理者権限

国家資格を有する者が国家資格情報を含んだ電子証明書を申請する場合は、官公庁の発行した国家資格免許証等の原本を地域受付審査局の窓口で提示、若しくは国家資格免許証等のコピーの適当な空欄に実印を捺印して印鑑登録証明書を添えて提出することで国家資格保有の事実を立証しなくてはならない。

医療機関等の管理者が医療機関等の管理者の電子証明書を申請する場合は、「3.2.2　組織の認証」で定める書類に、申請者本人が管理権限者として記載があれば当該書類を地域受付審査局の窓口で提示することにより管理権限の事実の立証とみなす。記載がない場合は、申請者本人が管理権限を有すると公に告知している医療機関等のパンフレットなどを地域受付審査局の窓口で提示すること

で、管理者であることの事実を立証しなくてはならない。
なお、地域受付審査局では確認に用いた証明書等のコピーを保存する。

＜郵送による申請の場合＞

1. 個人の実在性

電子証明書を申請しようとする個人は、取得後 3 ヶ月以内の住民票の写しに添えて、利用申請書に当該個人の基本 4 情報を記入し、地域受付審査局に郵送することで実在性の立証をしなくてはならない。

2. 個人の本人性

電子証明書を申請しようとする個人は、次に挙げる書類のコピーの適当な空欄に実印を捺印して地域受付審査局に郵送することで本人性の立証をしなくてはならない。なお、有効期限のある書類は、全て有効期限内のもののみが本人性の立証に有効である。

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

3. 個人の証明書申請の意思

電子証明書を申請しようとする個人は、印鑑登録証明書を添えて、利用申請書に実印を捺印することで申請者個人の申請意思を立証しなくてはならない。なお、印鑑登録証明書の有効期間は発行日より 6 ヶ月以内とする。但し、発行する地方公共団体が有効期限を設けている場合は、それを優先する。

4. 国家資格及び医療機関等の管理者権限

国家資格を有する者が国家資格情報を含んだ電子証明書を申請する場合は、官公庁の発行した国家資格免許証等のコピーの適当な空欄に実印を捺印して地域受付審査局に郵送することで国家資格保有の事実を立証しなくてはならない。

医療機関等の管理者が医療機関等の管理者の電子証明書を申請する場合は、「3.2.2　組織の認証」で定める書類に、申請者本人が管理権限者として記載のある場合は、当該書類を地域受付審査局に郵送することで管理権限の事実の立証とみなす。記載がない場合は、申請者本人が管理権限を有すると公に告知している医療機関等のパンフレットなどを地域受付審査局に郵送することで、管理者であ

ることの事実を立証しなくてはならない。

なお、地域受付審査局では確認に用いた証明書等のコピーを保存する。

＜オンラインによる申請の場合＞

地域受付審査局では、オンラインによる申請は受け付けない。

3.2.4　確認しない加入者の情報

認めない

3.2.5　機関の正当性確認

規定しない。

3.2.6　相互運用の基準

規定しない。

3.3　鍵更新申請時の本人性確認及び認証

3.3.1　通常の鍵更新時の本人性確認及び認証

加入者が鍵更新申請を行う場合、加入者は更新申請書を登録局又は地域受付審査局に提出しなければならない。地域受付審査局は、地域受付審査局の責任の元、地域受付審査局経由で更新申請書を登録局に提出しなければならない。

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

ただし、本条件に当てはまるものとしては、更新申請書を登録局か発行申請書を提出した同一の地域受付審査局に申請した場合のみとする。更新申請書を発行申請書を提出した地域受付審査局とは別の地域受付審査局に提出した場合は、「4.2.1　本人性及び資格確認」が実施された日から 5 年以内であっても、「3.2.3 個人の認証」で規定されている書類を再度全て提出しなければならない。

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、初回の電子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及び認証

初回の電子証明書発行と同様の手順により申請するものとする。

3.4　失効申請時の本人性確認及び認証

加入者が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. 失効を申請する加入者証明書を特定する。
2. 加入者証明書を失効する理由を明らかにする。
3. 申請者が加入者本人又は代理人であることを立証する。

本認証局は、失効申請書の記載内容が当該証明書の利用申請書の記載内容と一致していることにより、失効申請者の同一性を確認する。失効申請を郵送で行う場合は、失効申請の真偽の確認は、失効申請書と、いっしょに提出された印鑑登録証明書により行う。失効申請を対面により行う場合は、失効申請の真偽の確認は、対面での本人確認により行う。

本認証局は、加入者本人が死亡し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。

また、利用申請時の印鑑登録証明書の内容に変更があった場合に限らず、印鑑登録証明書は必須とする。

緊急に失効する必要がある場合は、本認証局は FAX 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を行い、本人確認のうえ失効処理を実施する。ただし、失効申請者は後日正式に失効申請書を本認証局に提出しなければならない。

なお、緊急失効を受付できるのは登録局のみとし、地域受付審査局では緊急失効は受け付けないものとする。

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

加入者証明書の申請者は以下とする。

(1) 保健医療福祉分野のサービス提供者本人、保健医療福祉分野のサービス利用者本人。

(2) 保健医療福祉分野に関わる国家資格を有する者本人。

(3) 医療機関等の管理者本人。

本 CPS に則り発行される電子証明書は、それ以外からの申請は受け付けない。

4.1.2 申請手続及び責任

加入者証明書の利用を希望する者は、本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。

また、加入者証明書の申請者は、申請にあたり、本 CPS「1.3 PKI の関係者」と第 9 章で規定される本認証局の責任範囲を理解し、同意した上で申請を行うものとする。更に、本認証局の定める開示文書及び利用約款等も利用申請の前に読み、内容を理解し、同意した上で申請を行うものとする。

(1) 登録局への申請

申請者本人が登録局に「3.2.3 個人の認証（1）登録局へ申請する場合」に定める書類を郵送することにより利用申請を行う。

郵送以外の申請は認めない。

(2) 地域受付審査局への申請

申請者本人が地域受付審査局に「3.2.3 個人の認証（2）地域受付審査局へ申請する場合」に定める書類を持参又は郵送することにより利用申請を行う。

なお、代理人による申請の場合は、証明書の利用申請に必要な書類に加え、本人による委任状及び「3.2.3 個人の認証」に準じた代理人の本人性を確認可能な書類も同時に提出するものとし、窓口交付の場合は本人が出頭する。

本認証局は上記以外の方法での申請は受け付けない。

4.2 証明書申請手続き

4.2.1 本人性及び資格確認

本認証局は、以下に示す方法により申請者の本人性確認及び資格の確認を行う。

1. 保健医療福祉分野のサービス提供者本人、保健医療福祉分野のサービス利用者本人及び保健医療福祉分野に関わる国家資格を有する者本人への交付

本認証局は、本 CPS「3.2.3 個人の認証」に定める申請者の実在性、本人性及び申請意思の立証に対して、それぞれ以下の方法で真偽の確認を行う。

（1）持参もしくは交付時に本人が出頭する場合：地域受付審査局のみ対応

本認証局は、証明書の発行時、本 CPS「3.2.3 個人の認証」に定める申請者の実在性、本人性、申請意思及び国家資格保有の立証に対して、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、住民票の写しが少なくとも記載内容、形式、有効期限などにおいて真正であることを確認し、且つ基本 4 情報に関して住民票の写しと利用申請書の記載内容が一致することを確認する。

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

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

国家資格保有の確認にあたっては､国家資格免許証等の原本若しくはコピーが少なくとも記載内容､形式､有効期限などにおいて真正であることを確認し、各免許証と利用申請書の記載内容が一致することを確認する。また、国家資格免許証等のコピーの場合は、当該国家資格免許証等のコピーの適当な空欄に実印が捺印され、印鑑登録証明書が添えてあることを確認する。

なお、確認に用いた証明書等は登録局で住民票の写しの原本、及び本人性確認書類のコピー、国家資格免許証等のコピーを当該電子証明書の有効期限切れ後 10 年間保存する。地域受付審査局では確認に用いた証明書等のコピーを 5 年間保存する。

（2）郵送の場合：登録局と地域受付審査局で対応

本認証局は、本 CPS「3.2.3 個人の認証」に定める申請者の実在性、本人性、申請意思及び国家資格保有の立証に対して、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、住民票の写しが少なくとも記載内容、形式、有効期限などにおいて真正であることを確認し、且つ基本 4 情報に関して住民票の写しと利用申請書の記載内容が一致することを確認する。

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

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

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

なお、確認に用いた証明書等は登録局で住民票の写しの原本、本人性確認書類のコピー及び国家資格免許証等のコピーを当該電子証明書の有効期限切れ後 10 年間保存する。地域受付審査局では確認に用いた証明書等のコピーを 5 年間保存する。

2. 医療機関等の管理者への電子証明書交付

本認証局は、医療機関等の管理者への電子証明書発行時、「1. 保健医療福祉分野のサービス提供者本人、保健医療福祉分野のサービス利用者本人及び保健医療福祉分野に関わる国家資格を有する者本人への交付」の方法による申請者の確認に加え、「3.2.2 組織の認証」に定める組織の立証に対して真偽の確認及び管理者権限の確認を行う。

組織の立証の真偽の確認をする時は、持参若しくは郵送の場合、電話帳などの第3 者の提供サービスを用いて調査した連絡先へ問い合わせを実施するか、当該組織を管轄する保健所等へ問い合わせを実施することにより申請機関の実在性確認を行うものとする。また、組織の立証のための書類に記載された管理者の氏名と「1. 保健医療福祉分野のサービス提供者本人、保健医療福祉分野のサービス利用者本人及び保健医療福祉分野に関わる国家資格を有する者本人への交付」で確認した書類に記載された氏名が一致することを確認する。

なお、中央官庁・地方公共団体が運営する機関で当該機関の実在性が明らかな場合で、公印の押された認証局の定める書類の提出があった場合は、問い合わせによる確認を省略することができる。

なお、確認に用いた証明書等は登録局で住民票の写しの原本、本人性確認書類のコピー、国家資格免許証等のコピー及び組織確認書類のコピーを当該電子証明書の有効期限切れ後 10 年間保存する。地域受付審査局では確認に用いた証明書等のコピーを 5 年間保存する。

4.2.2 証明書申請の承認又は却下

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

4.2.3 証明書申請手続き期間

本認証局は、電子証明書申請の手続き期間などを本認証局の Web サイト上で公開する。電子証明書申請の手続き期間は、MEDIS の休業日を除く 10：00 から 17：00 とする。電子証明書申請の手続き期間に変更が生じた場合、本認証局の Web サイト上で告知する。

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、利用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、加入者私有鍵及び加入者証明書は、認証局内で証明書格納媒体に格納する。また、証明書格納媒体格納後、加入者鍵ペアは認証設備から完全に消去する。

本認証局は、正当な加入者に加入者私有鍵を所有させるため、証明書格納媒体を本人限定受取郵便（特例型）にて加入者本人に送付する。

4.3.2　証明書発行後の通知

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

4.4　証明書の受理

4.4.1　証明書の受理

本認証局は、加入者証明書を交付した後、加入者が受領した旨を電子証明書受領証の受領により確認する。

なお、本認証局は、証明書格納媒体発送日から 30 日以内に加入者から受領書が返信されなかった場合、利用者に督促後さらに 7 日を経過しても受領の通知がない場合、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認証局による証明書発行通知

本認証局は、他のエンティティに対する加入者証明書発行の通知を行わない。

4.5　鍵ペアと証明書の利用目的

4.5.1　加入者の私有鍵と証明書の利用目的

加入者は、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「9.6.5 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

本認証局は、鍵更新を伴わない加入者証明書更新は行わない。

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

本認証局は、以下の条件を満たす時に加入者証明書の更新申請を受付ける。

- 更新対象の加入者証明書が存在すること。
- 加入者証明書が有効期限終了前のものであること。
- 加入者証明書が失効されていないこと。
- 加入者証明書の有効期限終了前 60 日以内に更新申請があったこと。

4.7.2　鍵更新申請者

本 CPS「4.1.1　証明書の申請者」に定める者からの申請を受け付ける。

4.7.3　鍵更新申請の処理手順

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

但し、本認証局で「4.2.1 本人性及び資格確認」に定める本人確認が完了した日から 5 年以内の場合は、上記に代わり加入者証明書による本人確認を行うことができる。

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

本認証局は他のエンティティへの加入者証明書発行の通知を行わない。

4.8　証明書変更

本認証局は、加入者証明書の変更を行わない。

4.9　証明書の失効と一時停止

4.9.1　証明書失効の要件

本認証局は、次の場合に加入者証明書を失効するものとする。

(1)　認証局による失効要件

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

- 加入者が本 CPS 及び利用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。
- 加入者証明書を発送した日から 30 日以内に受領書が本認証局に返送されなかった場合。
- 加入者証明書の記載情報に事実と相違があり、又はその情報が変更されたことを本認証局が確認した場合。
- 加入者の解散を認証局が確認した場合。
- 加入者証明書の規格変更がなされた場合。
- 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。

(2)　加入者による失効要件

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

- 加入者証明書の記載事項が事実と異なる場合。
- 加入者証明書の記載事項に変更が生じた場合。
- IC カードを紛失あるいは破損した場合。
- IC カードの盗難あるいは不正使用などを知った場合。
- IC カード PIN の紛失等で PIN が分からなくなった場合。
- IC カード PIN の入力ミスで IC カードが使用できなくなった場合。
- 加入者私有鍵が危殆化又は、危殆化の恐れがある場合。
- 加入者証明書の利用を停止する場合。
- 加入者証明書の国家資格に変更が生じた場合。
- 加入者証明書の返却があった場合。
- その他、加入者が加入者証明書の失効の必要性を判断した場合。

(3)　代理人による失効要件

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

・　加入者が死亡した場合。
・　加入者証明書の返却があった場合。

4.9.2　失効申請者

本認証局は、以下の者からの失効申請を受付ける。

1.　本人の名前で証明書が発行された加入者若しくはその代理人。
2.　認証局員。

4.9.3　失効申請の処理手順

本認証局は、失効申請の受領の判断を行い受理する場合は「3.4 失効申請時の本人性確認及び認証」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。

(1)　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、失効申請書と印鑑登録証明書を登録局に郵送、または初回発行時に申請した地域受付審査局に郵送若しくは持参する。緊急を要する失効要求の場合、失効申請書を登録局宛てに FAX し、原本を後日郵送する。なお、失効申請書は情報公開用 Web サイトにて掲載公開しているものを利用する。

【本人性確認の方法】

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

失効申請者の本人性確認は、持参による失効申請の場合は本人確認書類を対面で確認し実施する。対面申請以外は、失効申請書に押印されている印影と印鑑登録証明書の印影を照合することにより行う。

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

【失効処理】

本認証局は、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郵送にて通知する。

(2) 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、失効申請書と印鑑登録証明書を登録局に郵送、または初回発行時に申請した地域受付審査局に郵送若しくは持参する。代理人からの申請の場合は緊急失効は受け付けない。

【失効申請者の正当性確認の方法】

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

加入者の代理人への本人確認は、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により確認する。

【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郵送にて通知する。

(3) 認証局の職員からの失効申請の場合

本認証局は、「4.9.1 証明書失効の要件」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郵送にて通知する。

4.9.4 失効における猶予期間

加入者は、「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うものとする。

4.9.5　認証局による失効申請の処理期間

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

4.9.6　検証者の失効情報確認の要件

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

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、加入者証明書が失効されてから 24 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

規定しない。

4.9.10　オンラインでの失効確認要件

規定しない。

4.9.11　その他利用可能な失効情報確認手段

使用しない。

4.9.12　鍵の危殆化に関する特別な要件

本 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

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

規定しない。

4.11　加入の終了

加入者証明書所有者が、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

使用される私有鍵は、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。法の要請により預託が必要な場合、法に従った方法で預託される。

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

本認証局を運用する施設は、隔壁により区画されていて、施錠できることとする。

認証局システム（以下、「CAシステム」と言う。）を設置する施設である認証設備室は、水害、地震、火災その他の災害の被害を容易に受けない場所に設置し、且つ建物構造上、これら災害防止のための対策を講ずる。また、施設内において使用する機器等を、災害及び不正侵入防止策の施された安全な場所に設置する。

5.1.2 物理的アクセス

本認証局を運用する施設には認証業務用設備の所在を示す掲示を行わない。また物理的なアクセスを制限する適切なセキュリティ管理設備を装備し、入退出管理を実施する。入退出者の本人確認は別途定める方法により確実に行い、かつ入退出の記録を残すこととする。

認証設備室への立ち入りは、立ち入りに係る権限を有する複数の者により行われることとし、入室者の数と同数の者の退室を管理すること。設備の保守あるいはその他の業務の運営上必要な事情により、やむを得ず、立ち入りに係る権限を有しない者を認証設備室へ立ち入らせることが必要である場合においては、立ち入りに係る権限を有する複数の者が同行することとする。

登録設備室においては、関係者以外が容易に立ち入ることが出来ないようにするための施錠等の措置を講じる。

5.1.3 電源及び空調設備

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

また、空調設備を設置し、機器類の動作環境及び要員の作業環境を適切に維持する。

5.1.4 水害及び地震対策

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

また、建物は耐震構造であり、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

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

5.1.6 記録媒体

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

5.1.7 廃棄物の処理

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

5.1.8 施設外のバックアップ

規定しない。

5.2 手続き的管理

5.2.1 信頼すべき役割

電子証明書の発行、更新、失効等の重要な業務に携わる者は、本 CPS 上信頼される役割を担っている。本認証局では、業務上の役割を特定の個人に集中させず、複数人に権限を分離している。

表 5.2.1 認証局員の各役割

担当名	主な役割
認証局責任者	・本認証局の運営及び管理と業務の総括。 ・審査登録業務責任者と認証業務責任者の任命と解任及び人事管理。 ・本 CPS の承認。 ・CA 私有鍵の危殆化、又は危殆化の恐れがある場合の対応に関する決定。 ・災害などによる緊急事態における対応に関する決定。 ・生成された CA 私有鍵のバックアップの保管。
審査登録業務責任者	・認証事務室内全ての設備に対する維持・管理の実施と管理。 ・受付審査担当者と RA 操作員の任命と解任及び人事管理。

	・審査、登録、発行業務の実施と監督。 ・生成された CA 私有鍵のバックアップの保管。
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。
認証業務責任者	・認証設備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及び人事管理。 ・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 私有鍵の生成。 ・生成された CA 私有鍵のバックアップの保管。
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 私有鍵の生成。 ・一般 IA 操作員との合議制操作による CA システムの起動及び停止。 ・一般 IA 操作員との合議制操作による CA 私有鍵のアクティベーション及び非アクティベーション。
一般 IA 操作員	・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。 ・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 システムの起動及び停止。 ・上級 IA 操作員との合議制操作による CA 私有鍵のアクティベーション及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

CA システムへのアクセス権限者は、認証業務責任者により任命されるものとし、システムへの認証には当該業務へ専用に用いる IC カード等のセキュリティデバイスに格納された証明書等により、本人しか持ち得ない強固な認証方式を採用する。

5.2.4　職務分轄が必要になる役割

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

信頼される役割を担う者は、認証局の業務に関して、操作や管理の責務を負う。認証局の運営においては、これら役割の信頼性、適合性及び合理的な職務執行能力を保証する人事管理がなされ、そのセキュリティを確立するものとする。

5.3.1　資格、経験及び身分証明の要件

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

5.3.2　経歴の調査手続

信頼される役割を担う者の信頼性と適格性を、予め定めた適切な方法を用いてその人物の任命時及び定期的に背景調査を行う。

5.3.3　研修要件

信頼される役割を担う者は、その業務を行うための適切な教育を定期的に受け、以降必要に応じて再教育を受ける。

5.3.4　再研修の頻度及び要件

規定しない。

5.3.5　職務のローテーションの頻度及び要件

規定しない。

5.3.6　認められていない行動に対する制裁

規定しない。

5.3.7　独立した契約者の要件

規定しない。

5.3.8　要員へ提供する資料

規定しない。

5.4　監査ログの取扱い

5.4.1　記録するイベントの種類

CA システムは、CA システム、リポジトリシステム、認証局に関するネットワークアクセスの監査証跡やイベント・ログを手動或いは自動で取得する。

5.4.2　監査ログを処理する頻度

CA システムは、監査ログを 3 ヶ月毎に定期的に精査する。

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 アーカイブを保存する期間」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、セキュアな保管場所に保管される。

5.4.6　監査ログの収集システム（内部対外部）

規定しない。

5.4.7　イベントを起こしたサブジェクトへの通知

規定しない。

5.4.8 脆弱性評価

規定しない。

5.5 記録の保管

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) 加入者証明書の発行申請に関する文書

- 利用申請書/更新申請書。
- 加入者の住民票の写し。
- 加入者の印鑑登録証明書。
- 加入者の国家資格免許証等のコピー。
- 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、加入者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) 加入者証明書の失効申請に関する文書

- 失効申請書。
- 代理人の立証書類のコピー。

その他、証明書失効を決定した者に関する書類等、証明書失効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。

(3) 本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) 本認証局の組織管理に関する文書

- 本 CPS 及びその改訂に関する記録。
- 本認証局の要員任命、体制、指揮命令系統などに関する記録。
- 準拠性監査に関する記録。
- 認証業務の一部を他に委託する場合の契約書等。

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

アーカイブ情報の収められた媒体は物理的セキュリティによって保護され、許可されたものしかアクセスできないよう制限された施設に保存され、権限を持たない者の閲覧や持ち出し、改ざん、消去から保護する。

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

CA システムは、正確な時刻源から時刻を取得し、NTP（Network Time Protocol）を使用し認証局システムサーバの時刻同期を行ったうえ、本認証局内で記録される重要情報に対してレコード単位にタイムスタンプを付するものとする。

5.5.6 アーカイブ収集システム（内部対外部）

規定しない。

5.5.7　アーカイブ情報を入手し、検証する手続

規定しない。

5.6　鍵の切り替え

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

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

5.7　危殆化及び災害からの復旧

5.7.1　災害及び CA 私有鍵危殆化からの復旧手続き

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、事故等の自然災害。
- システム（ハードウェア、ネットワーク等）の故障。

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

ハードウェア、ソフトウェア、データが破壊又は損傷した場合、速やかに復旧作業を行い、合理的期間内に認証局業務を再開する。また、障害発生時には、可能な限り速やかに、加入者、検証者に本認証局 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、認証局責任者の判断により、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、別途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、リポジトリに公開し、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

認証局が運営を停止する場合には、運営の終了の 90 日前までに加入者に通知し、認証局の鍵と情報の継続的な保管を手配するものとする。認証局が終了する場合には、当該認証局の記録の安全な保管又は廃棄を確実にするための取り決めを行うこととする。登録局の運用を停止する場合は、事前に加入者の同意を得たうえで、登録局が有する加入者の情報と運営を他の登録局に移管し、それを加入者に通知する。

6. 技術的なセキュリティ管理

6.1 鍵ペアの生成と実装

6.1.1 鍵ペアの生成

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

6.1.2 加入者への私有鍵の送付

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証明書格納媒体に格納する。本認証局は、正当な加入者に加入者私有鍵を所有させるため、証明書格納媒体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、証明書格納媒体に格納後、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 公開鍵の配付

CA 公開鍵は、検証者によるダウンロードを可能とするために、リポジトリで公開するものとする。CA 公開鍵は、定期的に交換される。

6.1.5 鍵のサイズ

鍵の最小サイズは、使用されるアルゴリズムに依存する。CA 証明書の鍵のサイズは、RSA アルゴリズムで 2048 ビットとする。

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 2048 ビットとする。

6.1.6 公開鍵のパラメータ生成及び品質検査

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

6.1.7 鍵の利用目的

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

エンドエンティティの鍵は、署名用公開鍵証明書の場合は nonRepudiation のビットを使用し、認証用公開鍵証明書の場合は DigitalSignature のビットを使用する。

6.2　私有鍵の保護及び暗号モジュール技術の管理

6.2.1　暗号モジュールの標準及び管理

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

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

6.2.2　私有鍵の複数人によるコントロール

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

6.2.3　私有鍵のエスクロウ

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

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

6.2.4　私有鍵のバックアップ

CA 私有鍵のバックアップは、安全な方法で行う。バックアップ作業の権限を有する複数人の立会いのもとで行い、バックアップデータとして CA 私有鍵に関する情報を暗号化し、複数に分散させて保管する。

6.2.5　私有鍵のアーカイブ

本認証局は、加入者私有鍵をアーカイブしない。

6.2.6　暗号モジュールへの私有鍵の格納と取り出し

CA 私有鍵は、認証設備室内にある暗号モジュール内に暗号化されて安全に格納されるものとする。

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

6.2.7　暗号モジュールへの私有鍵の格納

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

6.2.8　私有鍵の活性化方法

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

6.2.11　暗号モジュールの評価

本認証局の私有鍵の格納モジュールは、FIPS 140-2 レベル 3 と同等以上のものを使用する。

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

6.3　鍵ペア管理に関するその他の面

6.3.1　公開鍵のアーカイブ

公開鍵のアーカイブは、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　私有鍵と公開鍵の有効期間

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

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。

6.4　活性化用データ

6.4.1　活性化データの生成とインストール

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

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

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

6.4.2　活性化データの保護

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。

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

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

6.4.3　活性化データのその他の要件

規定しない。

6.5　コンピュータのセキュリティ管理

6.5.1　特定のコンピュータのセキュリティに関する技術的要件

認証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

本認証局は使用する全てのソフトウェア、ハードウェアに対して事前に運用テストを行い、信頼性の確認を行う。

6.6　ライフサイクルの技術的管理

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

6.6.1　システム開発管理

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

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

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

6.6.2　セキュリティ運用管理

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

6.6.3　ライフサイクルのセキュリティ管理

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

6.7　ネットワークのセキュリティ管理

本認証局の存在するネットワークにはファイアウォールを使用し、ファイアウォール外からのアクセスについては必要最低限のプロトコルに制限する。

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

タイムスタンプの使用に関する要件は、本 CPS「5.5.5.記録にタイムスタンプを付ける要件」に規定する。

7. 証明書及び失効リスト及び OCSP のプロファイル

7.1 証明書のプロファイル

本認証局が発行する電子証明書は、X509 Version 3 フォーマット証明書形式により作成され、また電子証明書は X.500 識別名（Distinguished Name、以下 DN という）により一意に識別されるものとする。

本認証局が発行する電子証明書のプロファイルは、表 7.1.1 の通りとする。なお、Issuer の DN は表 7.1.1 に示す。本認証局の Common Name は、HPKI 認証局専門家会議により一意とされたものとする。

7.1.1 バージョン番号

本認証局が発行する電子証明書は、X509 Version 3 フォーマット証明書形式により作成されることとする。

7.1.2 証明書の拡張（保健医療福祉分野の属性を含む）

本 CPS に従い発行される加入者証明書の拡張領域のプロファイルは以下の表 7.1.1 の通りとする。subjectDirectoryAttributes 拡張で用いる保健医療福祉分野の属性（hcRole）については 7.1.10 で定める。

7.1.3 アルゴリズムオブジェクト識別子

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 名称の形式

Issure と Subject の名前の形式を表 7.1.1 に示す。

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
SHA256 対応署名用 CA 証明書	表 7.1.6	表 7.1.7
SHA256 対応署名用証明書	表 7.1.8	表 7.1.9
SHA256 対応認証用 CA 証明書	表 7.1.10	表 7.1.11
SHA256 対応認証用証明書	表 7.1.12	表 7.1.13

表 7.1.2、7.1.3、7.1.4、7.1.5 は SHA1 対応証明書のため、削除。

7.1.5 名称制約

用いない。

7.1.6 CPS オブジェクト識別子

別途規定する。

7.1.7 ポリシ制約拡張

使用しない。

7.1.8 ポリシ修飾子の構文及び意味

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 OID を格納する。

表 7.1.6　SHA256 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	○	MEDIS
OrganizationUnitName	○	MEDIS HPKI CA
CommonName	○	HPKI-01-MedisSignCA2-forNonRepudiation
SubjectPublicKeyInfo	○	
Algorithm	○	rsaEncryption
SubjectPublicKey	○	RSA 公開鍵値(2048bit)
IssuerUniqueID	×	
SubjectUniqueID	×	
Extensions	○	拡張領域（表 7.1.7）参照

表中の、「○」は設定、「×」は設定しないことを表す。

表 7.1.7　SHA256 対応署名用 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 SHA1 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	-
subjectKeyIdentifier	○	この証明書の公開鍵の SHA1 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				×		-

表中の、「○」は設定、「×」は設定しないことを表す。

表 7.1.8　SHA256 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	◎	c=JP
OrganizationName	◎	MEDIS
OrganizationUnitName	◎	MEDIS HPKI CA
CommonName	◎	HPKI-01-MedisSignCA2-forNonRepudiation
Subject	◎	英数字のみ使用する。(CountryName と SerialNumber は Printable、それ以外は UTF-8 で記述する)
CountryName	◎	c=JP（固定）とする。
LocalityName	×	
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あるいは英語名で OrganizationName に記載し、 OrganizatioUnitName に”Director”の文字列を格納する。
OrganizationUnitName	○	
CommonName	◎	加入者の氏名をローマ字で記載する。
GivenName	×	
SurName	×	
e-Mail	×	
SerialNumber	△	医籍登録番号などを記載することができる。
SubjectPublicKeyInfo	◎	
Algorithm	◎	RSAEncryption とする。
SubjectPublicKey	◎	
IssuerUniqueID	×	
SubjectUniqueID	×	
Extentions	◎	拡張領域（表 7.1.9）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 7.1.9　SHA256 対応署名用証明書プロファイル（拡張領域）

項目	設定	説明	Critical
authorityKeyIdentifier	◎		FALSE
keyIdentifier	◎	上位証明書の公開鍵の SHA1 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	-
subjectKeyIdentifier	◎	この証明書の公開鍵の SHA1 ハッシュ値	FALSE
KeyUsage	◎		TRUE
DigitalSignature	×		-
NonRepudiation	◎		-
KeyEncipherment	×		-
DataEncipherment	×		-
KeyAgreement	×		-
KeyCertSign	×		-
CRLSign	×		-
EncipherOnly	×		
DeciphermentOnly	×		-
extendedKeyUsage	×		-
privateKeyUsagePeriod	×		-
certificatePolicies	◎		TRUE
policyIdentifier	◎		-
certPolicyId	◎	1.2.392.100495.1.5.1.1.3.1	-
policyMapping	×		-
subjectAltName	△	漢字で加入者氏名、所属を入れることができる。	FALSE
CountryName	△	C=JP	
OrganizationName	△	加入者の所属組織名等を日本語で記載する	
OrganizationUnitName	△	加入者の所属部署名等を日本語で記載する	
CommonName	△	加入者の氏名日本語で記載する	
SerialNumber	△	医籍登録番号などを記載することができる	
issuerAltName	×		-
subjectDirectoryAttributes	△	医療従事者等の資格（hcRole）を記載。	FALSE

		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。その他(患者等)の場合は省略可。	
basicConstraints	×		-
CA	×		-
pathLenConstraints	×		-
nameConstraints	×		-
policyConstraints	×		-
cRLDistributionPoints	◎		FALSE
distributionPoint	◎		-
fullName	◎		-
uniformResource Identifier	◎	http://cert.medis.or.jp/sign/crl-sign2.crl	-
subjectInfoAccess	×		-
authorityInfoAccess	×		-

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 7.1.10　SHA256 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	○	MEDIS
OrganizationUnitName	○	MEDIS HPKI CA
CommonName	○	HPKI-01-MedisAuthCA2-forAuthentication-forIndividual
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、「○」は設定、「×」は設定しないことを表す。

表 7.1.11　SHA256 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 SHA1 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	-
subjectKeyIdentifier	○	この証明書の公開鍵の SHA1 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				×		-

表中の、「○」は設定、「×」は設定しないことを表す。

表 7.1.12　SHA256 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	◎	c=JP
OrganizationName	◎	MEDIS
OrganizationUnitName	◎	MEDIS HPKI CA
CommonName	◎	HPKI-01-MedisAuthCA2-forAuthentication-forIndividual
Subject	◎	英数字のみ使用する。(CountryName と SerialNumber は Printable、それ以外は UTF-8 で記述する）
CountryName	◎	c=JP（固定）とする。
LocalityName	×	
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あるいは英語名で OrganizationName に記載し、 OrganizatioUnitName に”Director”の文字列を格納する。
OrganizationUnitName	○	
CommonName	◎	加入者の氏名をローマ字で記載する。
GivenName	×	
SurName	×	
e-Mail	×	
SerialNumber	△	医籍登録番号などを記載することができる。
SubjectPublicKeyInfo	◎	
Algorithm	◎	RSAEncryption とする。
SubjectPublicKey	◎	
IssuerUniqueID	×	
SubjectUniqueID	×	
Extentions	◎	拡張領域（表 7.1.13）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 7.1.13　SHA256 対応認証用証明書プロファイル（拡張領域）

項目	設定	説明	Critical
authorityKeyIdentifier	◎		FALSE
keyIdentifier	◎	上位証明書の公開鍵の SHA1 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	-
subjectKeyIdentifier	◎	この証明書の公開鍵の SHA1 ハッシュ値	FALSE
KeyUsage	◎		TRUE
DigitalSignature	◎		-
NonRepudiation	×		-
KeyEncipherment	×		-
DataEncipherment	×		-
KeyAgreement	×		-
KeyCertSign	×		-
CRLSign	×		-
EncipherOnly	×		
DeciphermentOnly	×		-
extendedKeyUsage	×		-
privateKeyUsagePeriod	×		-
certificatePolicies	◎		TRUE
policyIdentifier	◎		-
certPolicyId	◎	1.2.392.100495.1.5.1.2.3.1	-
policyMapping	×		-
subjectAltName	△	漢字で加入者氏名、所属を入れることができる。	FALSE
CountryName	△	C=JP	
OrganizationName	△	加入者の所属組織名等を日本語で記載する	
OrganizationUnitName	△	加入者の所属部署名等を日本語で記載する	
CommonName	△	加入者の氏名日本語で記載する	
SerialNumber	△	医籍登録番号などを記載することができる	
issuerAltName	×		-
subjectDirectoryAttributes	△	医療従事者等の資格（hcRole）を記載。	FALSE

		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。その他(患者等)の場合は省略可。	
basicConstraints	×		-
CA	×		-
pathLenConstraints	×		-
nameConstraints	×		-
policyConstraints	×		-
cRLDistributionPoints	◎		FALSE
distributionPoint	◎		-
fullName	◎		-
uniformResource Identifier	◎	http://cert.medis.or.jp/auth/crl-auth2.crl	-
subjectInfoAccess	×		-
authorityInfoAccess	×		-

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。

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

本認証局が発行する加入者証明書には、HPKI-CP で規定した hcRole 属性を下記に示すように用いる。

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 7.1.14 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 7.1.14 に示すように英語表記を用い UTF8string で設定する。

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、その他(患者等)の場合は省略可とする。

記述する国家資格を示す名称は、次の英語表記を用いる。

表 7.1.14　HPKI 資格名テーブル（codeDataFreeText の定義）

資格名（国家資格）	説明
‘Medical Doctor’	医師
‘Dentist’	歯科医師
‘Pharmacist’	薬剤師
‘Medical Technologist’	臨床検査技師
‘Radiological Technologist’	診療放射線技師
‘Registered Nurse’	看護師
‘Public Health Nurse’	保健師
‘Midwife’	助産師
‘Physical Therapist’	理学療法士
‘Occupational Therapist’	作業療法士
‘Orthoptist’	視能訓練士
‘Speech Therapist’	言語聴覚士
‘Dental Technician’	歯科技工士
‘National Registered Dietitian’	管理栄養士
‘Certified Social Worker’	社会福祉士

‘Certified Care Worker’	介護福祉士
‘Emergency Medical Technician’	救急救命士
‘Psychiatric Social Worker’	精神保健福祉士
‘Clinical Engineer’	臨床工学技士
‘Massage and Finger Pressure Practitioner’	あん摩マッサージ指圧師
‘Acupuncturist’	はり師
‘Moxibustion Practitioner’	きゅう師
‘Dental Hygienist’	歯科衛生士
‘Prosthetics & Orthctic’	義肢装具士
‘Artificial Limb Fitter’	柔道整復師
‘Clinical Laboratory Technician’	衛生検査技師
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

患者に対して署名付の文書を交付することが多い医療機関等の管理責任者を hcRole だけで識別できるように定めている。

なお、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） HPKIhcRole 属性プロファイル

本認証局が発行する加入者証明書の ISO IS 17090 に定められた hcRole 属性の ASN.1 表記は次のとおりとする。

```
hcRole ATTRIBUTE : := {
    WITH SYNTAX                    HCActorData
    EQUALITY MATCHING RULE     hcActorMatch
    SUBSTRINGS MATCHING RULE hcActorSubstringsMatch
    ID                                  id-hcpki-at-healthcareactor}

-- Assignment of object identifier values
-- The following values are assigned in this Technical Specification:
    id-hcpki   OBJECT IDENTIFIER   :: =   {iso (1) standard (0) hcpki (17090)}
    id-hcpki-at   OBJECT IDENTIFIER :: = {id-hcpki 0 }
    id-hcpki-at-healthcareactor OBJECT IDENTIFIER :: = {id-hcpki-at 1}
    id-hcpki-cd OBJECT IDENTIFIER :: = {id-hcpki 1}
-- Following values are defined in Japanese HPKI CP:
    id-jhpki OBJECT IDENTIFIER :: =
                        {iso(1) member-body(2) jp(392) mhlw(100495) jhpki(1)}
    id-jhpki-cdata OBJECT IDENTIFIER :: = { id-jhpki 6 1 1 }

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

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

CodedData :: = SET {
    codingSchemeReference [0] OBJECT IDENTIFIER,
    -- Contains the ISO coding scheme Reference
    -- or local coding scheme reference achieving ISO or national registration.
    -- Local coding scheme reference in Japanese HPKI is id-jhpki-cdata
(defined above)
    -- In this profile, use this OID: Note 2
    -- At least ONE of the following SHALL be present
```

```
    codeDataValue [1] NumericString OPTIONAL, -- Note 3 (Do not use)
    codeDataFreeText [2] DirectoryString } -- Note 4

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

Note1： HCActor の regionalHcActorData は、本 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 7.1.14 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 7.1.14 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。

表 7.2.1　証明書失効リストのプロファイル

失効リスト種別	基本領域	CRL エントリ拡張領域	CRL 拡張領域
SHA256 対応 署名用証明書失効リスト	表 7.2.5	表 7.2.6	表 7.2.7
SHA256 対応 認証用証明書失効リスト	表 7.2.8	表 7.2.9	表 7.2.10

表 7.2.2、7.2.3、7.2.4 は SHA1 対応署名用証明書失効リストのため、削除。

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 7.2.5　SHA256 対応署名用証明書失効リストのプロファイル（基本領域）

フィールド		説明
Version		Ver2 (1)
Signature		SHA256WithRSAEncryption
Issuer		CountryName は Printable、それ以外は UTF-8 で記述する。
	CountryName	JP
	OrganizationName	MEDIS
	OrganizationUnitName	MEDIS HPKI CA
	CommonName	HPKI-01-MedisSignCA2-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	表 7.2.6 の拡張領域（crlEntryExtentions）参照
crlExtentions		表 7.2.7 の拡張領域（crlExtensions）参照

表 7.2.6　SHA256 対応署名用証明書失効リストのプロファイル
（CRL エントリ拡張領域 crlEntryExtensions）

フィールド	説明	Critical
reasonCode	申請に基づくコードを記載	FALSE

表 7.2.7　SHA256 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			説明	Critical
authorityKeyIdentifier				FALSE
	keyIdentifier		認証局証明書の公開鍵の SHA1 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	-
cRLNumber			128bit 以下の正の整数。	FALSE

表 7.2.8　SHA256 対応認証用証明書失効リストのプロファイル（基本領域）

フィールド		説明
Version		Ver2 (1)
Signature		SHA256WithRSAEncryption
Issuer		CountryName は Printable、それ以外は UTF-8 で記述する。
	CountryName	JP
	OrganizationName	MEDIS
	OrganizationUnitName	MEDIS HPKI CA
	CommonName	HPKI-01-MedisAuthCA2-for Authentication-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	表 7.2.9 の拡張領域（crlEntryExtentions）参照
crlExtentions		表 7.2.10 の拡張領域（crlExtensions）参照

表 7.2.9　SHA256 対応認証用証明書失効リストのプロファイル
（CRL エントリ拡張領域 crlEntryExtensions）

フィールド	説明	Critical
reasonCode	申請に基づくコードを記載	FALSE

表 7.2.10　SHA256 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			説明	Critical
authorityKeyIdentifier				FALSE
	keyIdentifier		認証局証明書の公開鍵の SHA1 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	-
cRLNumber			128bit 以下の正の整数。	FALSE

7.3　OCSP プロファイル

7.3.1　バージョン番号

規定しない。

7.3.2　OCSP 拡張領域

規定しない。

8. 準拠性監査とその他の評価

本認証局が HPKI-CP の要件に完全に従っているということを検証者、加入者及び HPKI 認証局専門家会議が満足する形で確立することを保証するために下記の通り内部監査を行うものとする。

8.1 監査頻度

本認証局の内部監査は、1 年より長くない間隔で行われるものとする。

但し、移管、譲渡、合併など、認証局の構成に大規模な変更があった場合は直ちに監査を実施するものとする。

8.2 監査者の身元・資格

本認証局は、認証局業務を直接行っている者以外の、認証局責任者が任命した監査者に定期監査を委託するものとする。

8.3 監査者と被監査者の関係

監査者は、いかなる本認証局の業務とは独立なものとする。また、別個の指揮系統に属することによって、被監査者から独立しているものとする。監査者は、被監査者に対しての特別な利害関係を持たないものとする。

8.4 監査テーマ

準拠性監査の監査項目は、HPKI-CP 及び本 CPS 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。

9. その他の業務上及び法務上の事項

9.1 料金

本認証局が発行する加入者証明書に関わる発行料金、更新料金、利用料金等は、別途定めるものとする。

9.2 財務上の責任

MEDIS は、本認証局の運営を維持し、かつその義務を履行するために十分な財務的基盤を維持するものとする。

9.2.1 保険の適用範囲

規定しない。

9.2.2 その他の資産

規定しない。

9.2.3 エンドエンティティに対する保険又は保証

規定しない。

9.3 業務情報の秘密保護

9.3.1 秘密情報の範囲

本認証局が保持する加入者の情報は、加入者証明書、CRL、本 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。

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

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

9.3.2 秘密情報の範囲外の情報

電子証明書及び CRL に含まれている情報は秘密情報として扱わない。

その他、次の情報も秘密情報として扱わない。

- 認証局以外の出所から、秘密保持の制限無しに公知となった情報。

・ 開示に関して加入者によって承認されている情報。

9.3.3 秘密情報を保護する責任

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

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

9.4 個人情報のプライバシー保護

9.4.1 プライバシーポリシ

本認証局における個人情報の取り扱いについては、「MEDIS　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。
  例えば、身分証明書、自宅住所、連絡先の詳細など、他の情報と容易に照合することができ、それにより特定の個人を識別することが可能な情報を指す。
- CRL に含まれない加入者の証明書失効又は停止の理由に関する情報。
- その他、認証局が業務遂行上知り得た加入者の個人情報。

9.4.3 プライバシーとはみなされない情報

次の情報は、秘密情報として扱わない。

- 加入者証明書に記載された情報。
- CRL に記載された情報

9.4.4 個人情報を保護する責任

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

9.4.5　個人情報の使用に関する個人への通知及び同意

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

9.4.6　司法手続又は行政手続に基づく公開

司法機関、行政機関又はその委託を受けたものの決定、命令、勧告等があった場合は、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又はその代理人から当該本人に関する情報の開示を求められた場合、本認証局で別途定める手続きに従って情報を開示する。この場合、複製にかかる実費、通信費用等については、情報開示を求める者の負担とする。

9.5　知的財産権

本認証局と加入者との間で別段の合意がなされない限り、本認証局が提供するサービスに関わる情報資料及びデータは、次に示す当事者の権利に属するものとする。

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

9.6　表明保証

9.6.1　認証局の表明保証

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

- 提供するサービスと運用のすべてが、HPKI-CP の要件と本 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。
- 公開鍵を含む証明書を加入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。

- 本 CPS で定める失効ポリシに従って失効事由が生じた場合は、証明書を確実に失効すること。
- CRL、ARL などの重要事項を本 CPS の定める方法により、速やかに入手できるようにすること。
- 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 に定める方法で、HPKI-CP 及び本 CPS に基づく加入者の権利と義務を加入者に通知すること。
- 鍵の危殆化のおそれ、証明書又は鍵の更新、サービスの取り消し、及び紛争解決をするための手続きを加入者に通知すること。
- 本 CPS「5　建物・関連設備、運用のセキュリティ管理」及び「6　技術的なセキュリティ管理」に従い認証局を運営し、私有鍵の危殆化を生じさせないこと。
- CA 私有鍵が、証明書及び証明書失効リストに署名するためだけに使用されることを保証すること。
- 申請者の申請内容の真偽の確認において利用した書類を含む、各種の書類の滅失、改ざんを防止し、本 CPS「5.5.2 アーカイブを保存する期間」に定める期間保管すること。
- 認証局の発行する電子証明書の中で、加入者に対して、加入者の名称（subjectDN）の一意性を検証可能にしておくこと。
- 電子証明書、CRL 等の形式が発行時点において本 CPS「7 証明書及び失効リスト及び OCSP のプロファイル」と一致していること。

9.6.2　登録局の表明保証

登録局は、次の責任を果たすものとする。

- 加入者証明書発行にあたり、申請内容の真偽の確認を確実に行うこと。
- 認証局の発行する加入者証明書の中で、加入者に対して加入者の名称（subjectDN）の一意性を検証可能にしておくこと。
- 証明書申請情報を発行局に安全に送付し、登録記録の原本を安全に保管すること。
- 加入者証明書失効申請を行う場合は、本 CPS「4.9.3　失効申請の処理手順」に従って失効申請を開始すること。
- 将来の検証のため、また電子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、電子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、電子証明書の有効期間満了後 10 年間保管すること。

9.6.3 地域受付審査局の表明保証

地域受付審査局は、次の責任を果たすものとする。

- 加入者証明書発行にあたり、申請内容の真偽の確認を確実に行うこと。
- 加入者証明書失効申請を行う場合は、本 CPS「4.9.3　失効申請の処理手順」に従って失効申請を開始すること。
- 証明書申請情報を登録局に安全に送付し、登録記録のコピーを安全に保管すること。

9.6.4 加入者の表明保証

本認証局の加入者は、次の責任を果たすものとする。

1. 証明書発行申請内容に対する責任

   証明書発行申請を行う場合、登録局または地域受付審査局に提示する申請内容が虚偽なく正確であることに対する責任を果たすこと。

2. 証明書記載事項の担保責任

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

3. 鍵などの管理責任

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

4. 各種の届出に対する責任

   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。

5. 利用規定の遵守責任

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

9.6.5 検証者の表明保証

検証者は、次の責任を果たすものとする。

1. 利用規定の遵守責任

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

2. 証明書記載事項の確認責任

   検証者は、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　証明書及び失効リスト及び OCSP のプロファイル」に記述されているプロファイルと合致していること。特に、次の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。
  - 認証用証明書の場合 hcRole 及び keyUsage の DigitalSignature のみが立てられていること。

9.6.6　他の関係者の表明保証

規定しない。

9.7　無保証

本認証局は、本 CPS 「9.6.1　認証局の表明保証」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、本認証局は一切の責任を負わない。

9.8　責任制限

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

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

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

- 本認証局に起因しない不法行為、不正使用並びに過失等により発生する一切の損害。
- 加入者又は検証者が自己の義務の履行を怠ったために生じた損害。

- 加入者又は検証者のシステムに起因して発生した一切の損害。
- 加入者又は検証者が使用する端末のソフトウェアの瑕疵、不具合あるいはその他の動作自体によって生じた損害。
- 本認証局の責に帰することのできない事由で電子証明書及びCRL に公開された情報に起因する損害。
- 本認証局の責に帰することのできない事由で正常な通信が行われない状態で生じた一切の損害。
- 本証明書の使用に関して発生する業務または取引上の債務等、一切の損害。
- 現時点の予想を超えた、ハードウェア的あるいはソフトウェア的な暗号アルゴリズム解読技術の向上に起因する損害。

9.9 補償

本 CPS に規定された責任を果たさなかったことに起因して、本認証局がサービスの加入者に対して損害を与えた場合、加入者が本認証局に支払った金額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、加入者は本認証局が発行する証明書を申請した時点で、検証者は信頼した時点で、認証局及び関連する組織等に対する損害賠償責任が発生する。

9.10 本 CPS の有効期間と終了

9.10.1 有効期間

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

9.10.2 終了

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

9.10.3 終了の影響と存続条項

文書が終了した場合であっても、「9.3 業務情報の秘密保護」、「9.4 個人情報のプライバシー保護」、「9.5 知的財産権」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、別項で特に定めるものを除き、電子メール、ホームページへの掲載、郵送による書面通知など認証局が適当と判断する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 の改訂は、MEDIS 理事長の承認を経て、改訂案をウェブサイト等本認証局が適当と判断する媒体を通じて公開し、各加入者に通知し意見を求め、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、関連する認証局及び検証者に速やかに公開する。公開の期間については、次のように定める。

- 重要な変更は、通知後 90 日を上限として、通知に定められた告知期間を経て効力を発する。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、直ちに効力を生ずる。
- 重要でない変更は、通知後直ちに効力を生ずる。

9.12.3　オブジェクト識別子（OID）の変更理由

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

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

9.13　紛争解決手続

本 CPS に関する一切の紛争については、東京地方裁判所を第一審の専属的合意管轄裁判所として紛争を解決するものとする。

9.14　準拠法

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

9.15　適用法の遵守

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

9.16.2　権利譲渡条項

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

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

9.16.3　分離条項

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

9.16.4　強制執行条項（弁護士費用及び権利放棄）

規定しない。

9.16.5　不可抗力

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

- 火災、雷、噴火、洪水、地震、嵐、台風、天変地異、自然災害、放射能汚染、有害物質による汚染、又は、その他の自然現象。
- 暴動、市民暴動、悪意的損害、破壊行為、内乱、戦争（宣戦布告されているか否かを問わない）又は革命。
- 裁判所、政府又は地方機関による作為又は不作為。
- ストライキ、工場閉鎖、労働争議。
- 認証局の責によらない事由で、本 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。