

MEDIS-DC ヘルスケア電子署名サービス実施規程

Version 1.0

2007年3月23日

(財)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

目次

1. はじめに	1
1.1 概要	1
1.1.1 この規程の目的	1
1.1.2 この規程の位置付け	1
1.1.3 MEDIS-DC ヘルスケア認証サービスの概要	1
1.1.4 MEDIS ヘルスケア PKI の概要	2
1.2 文書の名前と識別	3
1.3 PKI の関係者	1
1.3.1 MEDIS 認証局	1
1.3.2 加入者	1
1.3.3 検証者	1
1.3.4 MEDIS 登録局と発行局	2
1.4 証明書の使用方法	2
1.4.1 適切な証明書の使用	2
1.4.2 禁止される証明書の使用	2
1.5 ポリシ管理	3
1.5.1 本文章を管理する組織	3
1.5.2 問い合わせ先	3
1.5.3 本実施規程のポリシ適合性を決定する者	3
1.5.4 本実施規程の承認手続き	3
1.6 定義と略語	3
2. 公開及びリポジトリの責任	10
2.1 リポジトリ	10
2.2 証明書情報の公開	10
2.3 公開の時期又はその頻度	10
2.4 リポジトリへのアクセス管理	10
3. 識別及び認証	11
3.1 名前決定	11
3.1.1 名前の種類	11
3.1.2 名前が意味を持つことの必要性	11
3.1.3 加入者の匿名性又は仮名性	11
3.1.4 種々の名前形式を解釈するための規則 (名前を解釈するための規則)	11
3.1.5 名前の一意性	11

3.1.6	認識、認証及び商標の役割.....	11
3.2	初回の本人性確認.....	11
3.2.1	私有鍵の所持を証明する方法.....	11
3.2.2	下位認証局の認証.....	12
3.2.3	組織の認証.....	12
3.2.4	個人の認証.....	12
3.2.5	確認しない所有者の情報.....	16
3.2.6	機関の正当性確認.....	16
3.2.7	相互運用の基準.....	16
3.3	鍵更新申請時の本人性確認及び認証.....	16
3.3.1	通常の鍵更新時の本人性確認及び認証.....	16
3.3.2	証明書失効後の鍵更新の本人性確認及び認証.....	16
3.4	失効申請時の本人性確認及び認証.....	16
4.	証明書のライフサイクルに対する運用上の要件.....	17
4.1	証明書申請.....	17
4.1.1	証明書の申請.....	17
4.1.2	申請手続及び責任.....	17
4.2	証明書申請手続き.....	18
4.2.1	本人性及び資格確認.....	18
4.2.2	証明書申請の承認と却下.....	21
4.2.3	証明書申請手続き期間.....	21
4.3	証明書発行.....	21
4.3.1	証明書発行時の認証局の機能.....	21
4.3.2	証明書発行後の通知.....	22
4.4	証明書の受理.....	22
4.4.1	証明書の受理.....	22
4.4.2	認証局による証明書の公開.....	22
4.4.3	他の機関に対する証明書発行通知.....	22
4.5	鍵ペアと証明書の利用用途.....	22
4.5.1	加入者の秘密鍵と証明書の利用用途.....	22
4.5.2	検証者の公開鍵と証明書の利用用途.....	22
4.6	証明書更新.....	22
4.7	証明書の鍵更新（鍵更新を伴う証明書更新）.....	23
4.7.1	証明書鍵更新の要件.....	23
4.7.2	鍵更新申請者.....	23

4.7.3	鍵更新申請の処理手順	23
4.7.4	申請者への新証明書発行通知	23
4.7.5	鍵更新された証明書の受理	23
4.7.6	認証局による鍵更新証明書の公開	23
4.7.7	他のエンティティへの証明書発行通知	23
4.8	証明書変更	24
4.9	証明書の失効と一時停止	24
4.9.1	証明書失効の要件	24
4.9.2	失効申請者	24
4.9.3	失効申請の処理手順	24
4.9.4	失効における猶予期間	25
4.9.5	認証局による失効申請の処理期間	25
4.9.6	検証者の失効情報確認の要件	25
4.9.7	CRL/ARL 発行頻度	26
4.9.8	CRL/ARL が公開されない最大期間	26
4.9.9	オンラインでの失効/ステータス情報の入手	26
4.9.10	オンラインでの失効確認要件	26
4.9.11	その他利用可能な失効情報確認手段	26
4.9.12	鍵の危殆化に関する特別な要件	26
4.9.13	証明書一時停止の要件	26
4.9.14	一時停止申請者	26
4.9.15	一時停止申請の処理手順	26
4.9.16	一時停止期間の制限	26
4.10	証明書ステータスの確認サービス	26
4.11	加入の終了	27
4.12	私有鍵預託と鍵回復	27
4.12.1	キーエスクローと鍵回復ポリシー及び実施	27
4.12.2	セッションキーのカプセル化と鍵回復のポリシー及び実施	27
5.	建物・関連設備、運用のセキュリティ管理	28
5.1	建物及び関連設備管理	28
5.1.1	施設の位置と建物構造	28
5.1.2	入退管理	28
5.1.3	電源及び空調設備	28
5.1.4	水害及び地震対策	28
5.1.5	防火設備	28

5.1.6	記録媒体	29
5.1.7	廃棄物の処理	29
5.1.8	施設外のバックアップ	29
5.2	手続き的管理	29
5.2.1	信頼すべき役割	29
5.2.2	職務ごとに必要とされる人数	29
5.2.3	個々の役割に対する本人性確認と認証	29
5.2.4	職務分割が必要になる役割	30
5.3	要員管理	30
5.3.1	資格、経験及び身分証明の要件	30
5.3.2	経歴の調査手続	30
5.3.3	研修要件	30
5.3.4	再研修の頻度及び要件	30
5.3.5	職務のローテーションの頻度及び要件	30
5.3.6	認められていない行動に対する制裁	30
5.3.7	独立した契約者の要件	30
5.3.8	要員へ提供する資料	31
5.4	セキュリティ監査の手続き	31
5.4.1	記録するイベントの種類	31
5.4.2	監査ログを処理する頻度	31
5.4.3	監査ログを保存する期間	31
5.4.4	監査ログの保護	31
5.4.5	監査ログのバックアップ手続	31
5.4.6	監査ログの収集システム	31
5.4.7	イベントを起こしたサブジェクトへの通知	31
5.4.8	脆弱性評価	31
5.5	記録の保管	32
5.5.1	アーカイブ記録の種類	32
5.5.2	アーカイブを保存する期間	32
5.5.3	アーカイブの保護	32
5.5.4	アーカイブのバックアップ手続	32
5.5.5	記録にタイムスタンプをつける要件	32
5.5.6	アーカイブ収集システム	32
5.5.7	アーカイブ情報を入手し、検証する手続	32
5.6	鍵の切り替え	33
5.7	危殆化と業務の継続性の保証	33

5.7.1	災害及びCA 私有鍵危殆化からの復旧手続き	33
5.7.2	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	33
5.7.3	CA 私有鍵が危殆化した場合の対処	33
5.7.4	災害等発生後の事業継続性	33
5.8	認証局の終了	33
6.	技術的なセキュリティ管理	35
6.1	鍵ペアの生成と実装	35
6.1.1	鍵ペアの生成	35
6.1.2	所有者への私有鍵の送付	35
6.1.3	認証局への公開鍵の送付	35
6.1.4	検証者へのCA 公開鍵の配付	35
6.1.5	鍵のサイズ	35
6.1.6	公開鍵のパラメータ生成及び品質検査	35
6.1.7	鍵の使用目的	36
6.2	私有鍵の保護及び暗号化モジュール技術の管理	36
6.2.1	暗号化モジュールの標準及び管理	36
6.2.2	複数人による私有鍵の管理	36
6.2.3	私有鍵のエスクロウ	36
6.2.4	私有鍵のバックアップ	36
6.2.5	私有鍵のアーカイブ	36
6.2.6	暗号化モジュールへの私有鍵の格納	36
6.2.7	暗号化モジュールへの私有鍵の格納	37
6.2.8	私有鍵の活性化方法	37
6.2.9	私有鍵の非活性化方法	37
6.2.10	私有鍵の廃棄方法	37
6.2.11	暗号化モジュールの評価	37
6.3	鍵ペア管理に関するその他の面	37
6.3.1	公開鍵のアーカイブ	37
6.3.2	私有鍵と公開鍵の有効期間	37
6.4	活性化用データ	38
6.4.1	活性化データの生成とインストール	38
6.4.2	活性化データの保護	38
6.4.3	活性化データのその他の要件	38
6.5	コンピュータのセキュリティ管理	38
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	38

6.5.2	コンピュータセキュリティ評価	39
6.6	ライフサイクルの技術的管理	39
6.6.1	システム開発管理	39
6.6.2	セキュリティ運用管理	39
6.6.3	ライフサイクルのセキュリティ管理	39
6.7	ネットワークのセキュリティ管理	39
6.8	タイムスタンプ	39
7.	証明書及び失効リストのプロファイル	40
7.1	証明書のプロファイル	40
7.1.1	バージョン番号	40
7.1.2	証明書の拡張	40
7.1.3	アルゴリズムオブジェクト識別子	41
7.1.4	名前の形式	41
7.1.5	名前制約	41
7.1.6	CPS オブジェクト識別子	41
7.1.7	ポリシー制約拡張	41
7.1.8	ポリシー修飾子の構文及び意味	41
7.1.9	証明書ポリシー拡張フィールドの扱い	41
7.1.10	保健医療福祉分野の属性 (hcRole)	45
7.2	証明書失効リストのプロファイル	49
7.2.1	バージョン番号	49
7.2.2	CRL と CRL エントリ拡張領域	49
7.3	OCSP プロファイル	50
7.3.1	バージョン番号	50
7.3.2	OCSP 拡張領域	50
8.	準拠性監査	51
8.1	監査頻度	51
8.2	監査者の身元・資格	51
8.3	監査者と被監査者の関係	51
8.4	監査テーマ	51
8.5	監査指摘事項への対応	51
8.6	監査結果の通知	51
9.	その他の業務上及び法務上の事項	52
9.1	料金	52

9.2 財務上の責任.....	52
9.2.1 保険の適用範囲.....	52
9.2.2 その他の資産.....	52
9.2.3 エンドエンティティに対する保険又は保証.....	52
9.3 企業情報の秘密保護.....	52
9.3.1 秘密情報の範囲.....	52
9.3.2 秘密情報の範囲外の情報.....	53
9.3.3 秘密情報を保護する責任.....	53
9.4 個人情報のプライバシー保護.....	53
9.4.1 プライバシープラン（保護規定）.....	53
9.4.2 プライバシーとして保護される情報.....	54
9.4.3 プライバシーとはみなされない情報.....	54
9.4.4 個人情報を保護する責任.....	55
9.4.5 個人情報の使用に関する個人への通知及び同意.....	55
9.4.6 司法手続又は行政手続に基づく公開.....	55
9.4.7 その他の情報開示条件.....	55
9.5 知的財産権.....	55
9.6 表明保証.....	55
9.6.1 認証局の表明保証.....	55
9.6.2 登録局の表明保証.....	56
9.6.3 証明書所有者の表明保証.....	57
9.6.4 検証者の表明保証.....	57
9.6.5 他の関係者の表明保証.....	58
9.7 無保証.....	58
9.8 責任制限.....	58
9.9 補償.....	59
9.10 文書の有効期間と終了.....	59
9.10.1 有効期間.....	59
9.10.2 終了.....	59
9.10.3 終了の影響と存続条項.....	59
9.11 関係者間の個々の通知と連絡.....	59
9.12 改訂.....	60
9.12.1 改訂手続き.....	60
9.12.2 通知方法と期間.....	60
9.12.3 オブジェクト識別子（OID）などの変更理由.....	60
9.13 紛争解決手続.....	60

9.14 準拠法.....	61
9.15 適用法の遵守.....	61
9.16 雑則	61
9.16.1 完全合意条項.....	61
9.16.2 権利譲渡条項.....	61
9.16.3 分離条項.....	61
9.16.4 強制執行条項.....	61
9.16.5 不可抗力.....	61
9.17 その他の条項.....	62

1. はじめに

1.1 概要

1.1.1 この規程の目的

本規程は、厚生労働省が運用する保健医療福祉サービス提供者および保健医療福祉サービス利用者への署名用公開鍵証明書の発行を目的とした「保健医療福祉分野 PKI 認証局」の証明書ポリシーに準拠した、財団法人医療情報システム開発センター（以下、MEDIS-DC）が運営する、MEDIS-DC ヘルスケア電子署名サービスを定めることを目的とする。

1.1.2 この規程の位置付け

この規程は、次の文書に基づいて作成された。

保健医療福祉分野 PKI 認証局証明書ポリシー(厚生労働省)(以下、「HPKI-CP」という。)

HPKI-CP の問合せ先は、下記の通りである。

厚生労働省 医政局 研究開発振興課 医療機器・情報室

1.1.3 MEDIS-DC ヘルスケア認証サービスの概要

MEDIS-DC の提供するヘルスケア電子署名サービスの運用体制は「図 1.1 電子署名サービスの運用体制」のとおりである。MEDIS-DC 認証局は、MEDIS 上位認証局と MEDIS 下位認証局から構成され、以下の 2 つの認証サービスを提供する。

- (1) 下位認証局向け CA 認証サービス
- (2) 加入者証明書発行サービス

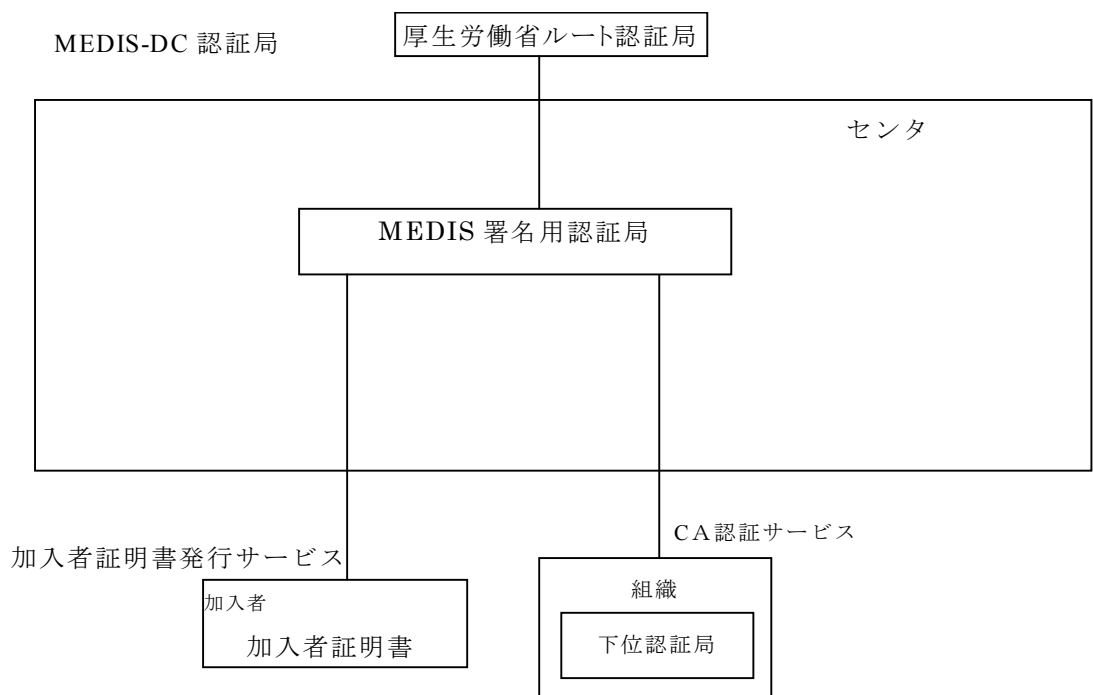


図 1.1 MEDIS 電子証明書サービスの系統

MEDIS 上位認証局は、CA 認証サービスとして、表 1.1.1 の下位署名用認証局証明書を下位署名用認証局に発行し、その更新、失効等のライフサイクルに関する業務を行う。下位署名用認証局証明書の有効期限は、発行日から 5 年間とする。MEDIS 署名用上位認証局が CA 認証サービスで認証する下位署名用認証局は、HPKI-CP および「MEDIS-DC ヘルスケア電子署名サービス実施規程」に従って運用されなければならない。

表 1.1.1 MEDIS 上位認証局が CA 認証サービスで発行する下位認証局証明書

証明書名称	私有鍵所有者	使用目的	有効期限
下位署名用認証局証明書	下位署名用認証局	証明書と失効リストの署名	発行日から 5 年間

1.1.4 MEDIS ヘルスケア PKI の概要

MEDIS-DC が運用する PKI を「MEDIS-ヘルスケア PKI」という。MEDIS ヘルスケア-PKI は、厚生労働省のルート認証局を信頼点とした、MEDIS-DC が運用する MEDIS 署名用認証局の三階層の PKI である。このうち、本 CPS は MEDIS 署名用認証局傘下の下位認証局および加入者への証明書のライフサイクルを規定する。MEDIS 署名用認証局が加入者に加入者証明書を発行することにより加入者を認証する。MEDIS 署名用認証局が下位署名用認証局証明書を発行することにより下位署名用認証局を認証する。下位署名用認証局が加入者に加入者証明書を発行することにより加入者を認証する。下位認証局は、MEDIS-DC

が認証し下位証明書を交付した MEDIS-DC とは独立した組織によって運用される。

1.2 文書の名前と識別

この規程の名称は、「MEDIS-DC ヘルスケア電子署名サービス実施規程」（以下、「本 CPS」という。）とする。この規程を識別するオブジェクト識別子はない。CA 認証サービスが発行する証明書に関連した証明書ポリシーは、表 1.2.1 のとおりである。

表 1.2.1 証明書ポリシー

準拠ポリシー名称	オブジェクト識別子
保健医療福祉分野 PKI 認証	HPKI 署名用証明明書ポリシー 1.2.392.100495.1.5.1.1.3.1
局証明書ポリシー	HPKI 署名テスト用証明書ポリシー 1.2.392.100495.1.5.1.1.0.1

1.3 PKI の関係者

1.3.1 MEDIS 認証局

(1) MEDIS 署名用認証局

厚生労働省のルート認証局を信頼点とした MEDIS-DC が運用する認証局であり、次の業務を行う。

- ① 下位署名用認証局証明書を発行する。
- ② 下位署名用認証局証明書を更新する。
- ③ 下位署名用認証局証明書を失効させる。
- ④ 検証者に対して下位署名用認証局の失効リストを配布する。
- ⑤ 加入者または検証者に対して MEDIS 署名用認証局証明書と下位署名用認証局証明書を配布する。
- ⑥ 加入者証明書および必要なら私有鍵を新規発行する。
- ⑦ 加入者証明書および必要なら私有鍵を更新する。
- ⑧ 加入者証明書を失効させる。
- ⑨ リポジトリを通して失効リストを検証者に配布する。

(2) 下位署名用認証局

CA 認証サービスにより MEDIS 認証局が認証する署名用下位認証局である。本 CPS に従って加入者証明書のライフサイクルに関連した次の業務を行う。

- ① 加入者証明書および必要なら私有鍵を新規発行する。
- ② 加入者証明書および必要なら私有鍵を更新する。
- ③ 加入者証明書を失効させる。
- ④ リポジトリを通して失効リストを検証者に配布する。

1.3.2 加入者

加入者とは、証明書所有者である。証明書所有者とは、証明書発行申請を行い認証局により証明書を発行される自然人をさす。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提供者及び利用者
下記の提供者である以下の者は、その資格、役割を証明書内に記載することができる。
- ・ 保健医療福祉分野に関わる国家資格所有者
- ・ 医療機関等の管理者

1.3.3 検証者

検証者とは、加入者の署名を検証する者をさす。

1.3.4 MEDIS 登録局と発行局

MEDIS 署名用認証局は、それぞれ登録局と発行局から構成される。

登録局は、MEDIS-DC が運用し、次の業務を行う。

- ① 申請者から申請を受けて審査して登録し、下位認証局証明書の発行を発行局に指示しそれを交付する。
- ② 申請者から申請を受けて審査して、下位認証局証明書の更新を発行局に指示しそれを交付する。
- ③ 申請者から失効申請を受けて審査して下位認証局証明書の失効を発行局に指示する。
- ④ 申請者から申請を受けて審査して登録し、加入者証明書の発行を発行局に指示しそれを交付する。
- ⑤ 申請者から申請を受けて審査して、加入者証明書の更新を発行局に指示しそれを交付する。
- ⑥ 申請者から失効申請を受けて審査して加入者認証局証明書の失効を発行局に指示する。

発行局では、登録局からの指示を受けて、次の業務を行う。なお、発行局業務を外部業者に委託できる。

- ① 下位認証局証明書の発行
- ② 下位認証局証明書の更新
- ③ 下位認証局証明書の失効
- ④ 加入者認証局証明書の発行
- ⑤ 加入者認証局証明書の更新
- ⑥ 加入者認証局証明書の失効
- ⑦ 失効情報の開示及び保管

1.4 証明書の使用方法

1.4.1 適切な証明書の使用

本 CPS で定める証明書の適用範囲は、次の通りとする。

- ① 下位認証局証明書
下位署名用認証局の認証用
- ② 署名用加入者証明書
 - ・ 医療従事者等の保健医療福祉分野サービス提供者の署名検証用
 - ・ 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

1.4.2 禁止される証明書の使用

本実施規程で定める加入者証明書は、署名用および署名検証以外には用いないものとする。

1.5 ポリシ管理

1.5.1 本文章を管理する組織

本 CPS の管理組織は、(財)医療情報システム開発センター 研究開発部とする。

1.5.2 問い合わせ先

本実施規程署名用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： (財)医療情報システム開発センター 研究開発部

営業時間： 10:00～17:00 (MEDIS-DC 休業日を除く)

電話番号：03-5805-8203

FAX 番号：03-5805-8211

e-mail アドレス：pki-info@medis.or.jp

1.5.3 本実施規程のポリシ適合性を決定する者

本実施規程の策定者は、(財)医療情報システム開発センターとする。

本 CPS は、HPKI 認証局専門家会議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 本実施規程の承認手続き

本実施規程は、(財)医療情報システム開発センター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 (秘密鍵暗号) がある。前者には RSA、El Gamal 暗号、楕円曲線暗号などがあり、後者には米国政府標準の DES や近年新しく DES の後継として決

まった AES などがある。

- ・ 暗号化モジュール (Hardware Security Module)
私有鍵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。
- ・ 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。
- ・ 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。
- ・ 下位証明書
ルート認証局から下位認証局に対して出される証明書。
- ・ 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。
- ・ 公開鍵 (Public Key)
私有鍵と対になる鍵で、署名の検証に用いる。公開鍵はたとえ公開されても秘密の私有鍵を類推することが困難である。
- ・ 公開鍵証明書 (Public Key Certificate)
所有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、公開鍵の所有者情報、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。
- ・ 証明書失効リスト (Certificate Revocation List、Authority Revocation List)
失効した電子証明書のリスト。
エンドエンティティの証明書の失効リストを CRL といい、CA の証明書の失効リストを ARL という。
- ・ 証明書発行要求 (Certificate Signing Request)
申請者から認証局に電子証明書発行を求めるための要求。電子証明書を作成するための元となる情報で、その内容には、申請者の所在地、サーバアドレス、公開鍵などの情報が含まれる。
- ・ 証明書ポリシー (Certificate Policy : CP)

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

- ・ 申請者
認証局に電子証明書の発行を申請する主体のこと。
- ・ 検証者 (Relying Party)
文書の署名を公開鍵証明書の公開鍵で検証する者。
- ・ 電子署名 (Electronic Signature)
電子文書の正当性を保証するために付けられる署名情報。公開鍵暗号などを利用し、相手が本人であることを確認するとともに、情報が送信途中で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 : RA)
電子証明書発行の申請者の本人を審査・確認し、主として登録業務を行う機関。登録局は、認証局の機能のうち、一部の業務を行う。認証する加入者の識別と本人性認証に責任を負うが、電子証明書に署名したり、発行したりはしない。
- ・ 認証局 (Certification Authority : CA)
電子証明書を発行する機関。認証局は、公開鍵が間違いなく本人のものであると証明可能にする第三者機関で、公正、中立な立場にあり信頼できなければならない。
- ・ 認証局運用規程 (Certification Practice Statement : CPS)
証明書ポリシーに基づいた認証局運用についての規定集。認証局が電子証明書を発行するときに採用する実践に関する表明として位置付けられる。
- ・ 登録設備室
認証業務用設備のうち、登録業務用設備のみが設置された室をいう。登録業務用設備とは、加入者の登録用端末や、加入者が初めて証明書をダウンロードする際に1度限り使用されるID、パスワード等を識別する為に用いる設備をいう。
- ・ 認証設備室
認証業務用設備（電子証明書の作成又は管理に用いる電子計算機その他の設備）が設置された室をいう。ただし、登録業務用設備のみが設置される場合を除く。

- ・ 発行局 (Issuer Authority)

電子証明書の作成・発行を主として発行業務を行う機関。発行局は、認証局の機能のうち、一部の業務を行う。
- ・ ハッシュ関数 (Hash Function)

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

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

電子証明書や証明書失効リストに記載する事項及び拡張領域の利用方法を定めたものの。
- ・ 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秘密鍵で署名した証明書 (NewWithOld) と、古い公開鍵に新しい秘密鍵で署名した証明書 (OldWithNew) がある。
- ・ ルート CA (Root CA)

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

(A～Z)

- ・ **ARL (Authority Revocation List)**
認証局の証明書の失効リスト、証明書失効リストを参照のこと。
- ・ **CA (Certification Authority)**
認証局を参照のこと。
- ・ **CA 証明書**
認証局に対して発行された電子証明書。本認証局における CA 証明書は、自己署名証明書である。
- ・ **CP (Certificate Policy)**
証明書ポリシーを参照のこと。
- ・ **CPS (Certification Practice Statement)**
認証局運用規程を参照のこと。
- ・ **CRL (Certificate Revocation List)**
エンドエンティティの証明書の失効リスト、証明書失効リストを参照のこと。
- ・ **CRL 検証**
証明書失効情報が、認証局が発行する CRL に記載されているかを確認すること。
- ・ **CSR (Certificate Signing Request)**
証明書発行要求を参照のこと。
- ・ **DN (Distinguished Name)**
X.500 規格において定められた識別名。X.500 規格で名前を決定することによって、名前の一意性が保障される。
- ・ **加入者 (End Entity)**
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。加入者と同義語。
- ・ **FIPS 140 (Federal Information Processing Standard)**
FIPS とは米国連邦情報処理標準で、FIPS140-2 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

ティレベル（最低レベル 1～最高レベル 4）を定めている。

- ・ **IA (Issuer Authority)**
発行局を参照のこと。
- ・ **OID (Object ID)**
オブジェクト識別子を参照のこと。
- ・ **PKI (Public Key Infrastructure)**
公開鍵基盤。公開鍵暗号化方式という暗号技術を基に認証局が公開鍵証明書を発行し、この証明書を用いて署名／署名検証、暗号／復号、認証を可能にする仕組み。
- ・ **RA (Registration Authority)**
登録局を参照のこと。
- ・ **RSA**
公開鍵暗号方式の一つ。Rivest、Shamir、Adleman の 3 名によって開発され、その名前をとって名付けられた。巨大な整数の素因数分解の困難さを利用したもので、公開鍵暗号の標準として普及している。
- ・ **SHA1 (Secure Hash Algorithm 1)**
ハッシュ関数の一つ。任意の長さのデータから 160bit のハッシュ値を作成する。
- ・ **X.500**
ITU-T/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

リポジトリには、MEDIS 上位認証局および下位認証局が発行する証明書の最新の失効情報を記載した失効情報等を保持する。

2.2 証明書情報の公開

MEDIS-DC 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 MEDIS 上位認証局がリポジトリで公開する情報とその URL

情報名称	URL
下位認証局証明書の失効情報	http://cert.medis.or.jp/SCA/CRL.crl
CA 自己署名証明書	http://cert.medis.or.jp/TCA/
CA 自己署名証明書のハッシュ値	http://cert.medis.or.jp/TCA/
本 CPS および各種規定	http://cert.medis.or.jp/pols/
本認証局の CRL	http://cert.medis.or.jp/sign/crl-sign.crl

2.3 公開の時期又はその頻度

認証局は、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、本実施規程「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

MEDIS-DC は、CP、CPS、証明書及びそれらの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読み取り専用として公開する。

3. 識別及び認証

3.1 名前決定

3.1.1 名前の種類

本 CPS に基づいて発行される証明書に使用されるサブジェクト名は加入者名とする。加入者名は X.500 の Distinguished Name を使用する。C は JP とする。また CommonName は必須で、加入者が自然人である場合、加入者の氏名（ローマ字表記）を記載する。

3.1.2 名前が意味を持つことの必要性

本実施規程により発行される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

証明書に記載される名前として匿名又は仮名を使用することはできない。

3.1.4 種々の名前形式を解釈するための規則（名前を解釈するための規則）

名前を解釈するための規則は、本実施規程「7 証明書及び失効リストのプロファイル」に従う。

3.1.5 名前の一意性

認証局が発行する電子証明書の加入者名（「subjectDN」）は認証局内で一意とする。また、加入者用証明書では、一意とするためにシリアルナンバー（「SN」）を含むことができる。

また、認証局の名前（「issuerDN」）は、MEDIS 認証局ドメイン内で、ある特定の認証局を一意に指し示す。

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、商標所持者にすべての権利が留保されるものとする。MEDIS-DC は、必要に応じて、商標所持者に対し、商標に関する出願等の公的書類の提示を求めることがある。

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

MEDIS 認証局においては、申請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 下位認証局の認証

MEDIS 認証局の下位認証局として運営する法人等の認証局の証明書を申請しようとする者は、証明書の発行に先立ち、「3.2.3 組織の認証」に定める方法によって、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。

3.2.3 組織の認証

MEDIS 認証局に医療機関等の管理者の証明書を申請しようとする者は、証明書の発行に先立ち、次のいずれかの方法で自身の所属も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。

なお、申請者個人の認証は「3.2.4 個人の認証」に定める方法による。

(1) 法人組織の場合

商業登記簿謄本、開設許可証の写しなど公的機関から発行される証明書、各法等で定められる掲示*の写し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。

(2) 個人事業者の場合

商業登記簿謄本、公的機関に提出している開設届の写し、各法等で定められる掲示*の写しも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。

(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、認証局の定める書類に公印規則に定められた公印を捺印したものを提出することによって実在性を立証する。

※ 「各法等で定められる掲示」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 条およびその準用条項 (掲示)

3.2.4 個人の認証

MEDIS 認証局に証明書を申請しようとする個人は、証明書の発行に先立ち、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に立証しなければならない。また、国家資格所有者が国家資格を含んだ証明書、医療機関等の管理者が医療機関等の管理者の証明書を申請しようとする場合は、国家資格所有の事実、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。

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、MEDIS 登録局が証明書を発行する場合は、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章の規定により申請者の審査および証明書の発行を実施する。

<持参の場合>

1. 自然人の実在性

証明書を申請しようとする自然人は、取得後 3 ヶ月以内の住民票の写しに添えて、MEDIS HPKI 証明書申請書に当該個人の「氏名、生年月日、性別、住所」（以下、基本 4 情報という）を記入し、MEDIS 登録局の窓口で提出することで実在性の立証をしなくてはならない。

2. 自然人の本人性

証明書を申請しようとする自然人は、次に挙げる書類の原本を MEDIS 登録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	・ 電気工事士免状
・ 運転免許証	・ 宅地建物取引主任者証
・ 住民基本台帳カード(写真付のもの)	・ 無線従事者免許証
・ 戦傷病者手帳	・ 猟銃/空気銃所持許可証
・ 海技免状	・ 官公庁職員身分証明書 (張り替え防止措置済みの写真付)
・ 船員手帳	

【2点提出が必要な書類】

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

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

B	・ 学生証(張り替え防止措置済みの写真付のもの)
---	--------------------------

	<ul style="list-style-type: none"> ・会社の身分証明書（通行証等は不可、張り替え防止措置済みの写真付のもの） ・市県民税の納税証明書または非課税証明書 (いずれも最新年で6ヶ月以内の発行のもの) ・身体障害者手帳 ・源泉徴収票（最新年のもの）
--	--

3. 自然人の証明書申請の意思

本人が登録局の窓口で各種の書類を持参して申請する場合は、実在性および本人性の立証を行えば、申請意思の立証がなされたものとみなす。

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、委任状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。

4. 国家資格および医療機関等の管理者権限

国家資格所有者が国家資格情報を含んだ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）の原本を登録局の窓口で提示することで国家資格所有の事実を立証しなくてはならない。

医療機関等の管理者が医療機関等の管理者の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登録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MEDIS登録局の窓口で提示することで、管理者であること的事实を立証しなくてはならない。

< 郵送の場合 >

1. 個人の実在性

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、HPKI 証明書申請書に当該個人の基本4情報を記入し、登録局に郵送することで実在性の立証をしなくてはならない。

2. 個人の本人性

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を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。

【1点で確認できる書類】

<ul style="list-style-type: none"> ・ 有効期間中の日本国旅券 ・ 運転免許証 ・ 住民基本台帳カード(写真付のもの) ・ 戦傷病者手帳 ・ 海技免状 ・ 船員手帳 	<ul style="list-style-type: none"> ・ 電気工事士免状 ・ 宅地建物取引主任者証 ・ 無線従事者免許証 ・ 猟銃/空気銃所持許可証 ・ 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】

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

A	<ul style="list-style-type: none"> ・ 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 	<ul style="list-style-type: none"> ・ 国民年金手帳(証書) ・ 厚生年金手帳(証書) ・ 共済年金証書 ・ 恩給証書 ・ 印鑑登録証明書 (6ヶ月以内発行のものと登録印鑑)
---	---	---

B	<ul style="list-style-type: none"> ・ 学生証(張り替え防止措置済みの写真付のもの) ・ 会社の身分証明書(通行証等は不可、張り替え防止措置済みの写真付のもの) ・ 市県民税の納税証明書または非課税証明書 (いずれも最新年で6ヶ月以内の発行のもの) ・ 身体障害者手帳 ・ 源泉徴収票(最新年のもの)
---	--

3. 自然人の証明書申請の意思

本人が郵送により申請する場合は、印鑑登録証明書を添えて、HPKI 証明書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、代理人による郵送での申請意思の立証は認めない。

4. 国家資格および医療機関等の管理者権限

国家資格所有者が国家資格情報を含んだ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を登録局に郵送することで国家資格所有の事実を立証しなくてはならない。

この時、国家資格免許証等に本人の顔写真が貼付されていない場合は、国家資

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

医療機関等の管理者が医療機関等の管理者の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 MEDIS 登録局に郵送することで、管理者であることの実を立証しなくてはならない。

3.2.5 確認しない所有者の情報

HPKI-CP で指定した提出すべき書類及びその記載事項に漏れがないことを確認する。

3.2.6 機関の正当性確認

規定しない。

3.2.7 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

加入者情報の通常の鍵更新は、「4.2.1 本人性及び資格確認」が実施された日から 5 年以内であれば、「3.2.3 個人の認証」で提出した書類または認証局で作成された記録を再び参照するか、証明書所有者の署名を提示することで行える。

5 年を過ぎた場合、もしくは元の書類もしくは記録が無効になっているか廃棄されていた場合は、初回の証明書発行と同様の手順により申請するものとする。

3.3.2 証明書失効後の鍵更新の本人性確認及び認証

初回の証明書発行と同様の手順により申請するものとする。

3.4 失効申請時の本人性確認及び認証

加入者が認証局に失効申請を行うときには、次の手順に従うものとする。

1. 失効を申請する証明書を特定する。
2. 証明書を失効する理由を明らかにする。

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

(1) 自然人証明書

自然人証明書の申請者は、保健医療福祉分野のサービス提供者本人もしくはその代理人、保健医療福祉分野のサービス利用者本人もしくはその代理人とする。

(2) 国家資格所有者証明書

国家資格所有者証明書の申請者は、保健医療福祉分野に関わる国家資格所有者本人もしくはその代理人とする。

(3) 管理者証明書

医療機関等の管理者証明書の申請者は、医療機関等の管理者もしくはその代理人とする。

(4) 下位認証局証明書

下位認証局証明書の申請者は、申請する認証局組織の代表者もしくはその代理人とする。

4.1.2 申請手続及び責任

証明書の利用を希望する者は、認証局で定める以下のいずれかの手続によって証明書の利用申請をおこなう。

1. 持参

持参による申請は下位認証局証明書の申請のみ認める。加入者証明書の持参による申請は認めない。

本人もしくは代理人が登録局に「3.2.2 個人の認証」に定める書類を持参することにより利用申請を行なう。

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、本人による委任状および本 CPS「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する。

2. 郵送

加入者証明書の申請は郵送のみとする。

本人が登録局に「3.2.4 個人の認証」及び認証局定める書類を郵送することにより利用申請を行なう。

なお、郵送での利用申請の場合、代理人による申請は認めない。

また、証明書の利用申請者は、申請にあたり、本実施規程「1.3 PKI の適用範囲」と第 9 章で規定される認証局の責任範囲を理解し、同意した上で利用申請を行うものとする。更に、本実施規程に則り運営される、MEDIS 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、同意書に記名捺印した上で利用申請を行うものとする。

4.2 証明書申請手続き

4.2.1 本人性及び資格確認

本人性及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。

<本人からの申請の場合>

1. 自然人への証明書発行

認証局は、自然人への証明書の発行時、本実施規程「3.2.3 個人の認証」に定める申請者の本人性、実在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) 持参の場合

持参による加入者証明書の申請は認めない。

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印影が一致していることの確認、貼付された写真と申請者本人との照合などを実施する。

この時、窓口で本人の実在性の確認を実施する。

なお、確認に用いた証明書等は本認証局でコピーを取り、5年間保存する。

(2) 郵送の場合

申請者から提示された各種の書類について、記載事項が一致していることの確認や印影が一致していることの確認を実施する。

電子証明書もしくは電子証明書を生成する符号を、申請者本人へ本人限定受取郵便で送付することにより実在性の確認を行う。

なお、確認に用いた証明書等は本認証局で5年間保存する。

2. 国家資格所有者への証明書発行

認証局は、国家資格所有者への証明書の発行時、「1. 自然人への証明書発行」の方法による申請者の確認に加え、以下の方法により国家資格所有の確認を行う。

(1) 持参の場合

持参による加入者証明書の申請は認めない。

(2) 郵送の場合

官公庁の発行した国家資格証明書等のコピーの郵送を要求し、国家資格所有の有無を確認する。

また、当該国家資格証明書等に本人の顔写真が貼付されていない場合は、印鑑登録証明書を添えて、国家資格証明書の写しの適当な空欄に実印を捺印させるものとする。

なお、確認に用いた証明書等は本登録局で5年間保存しておくものとする。

3. 医療機関等の管理者への証明書発行

認証局は、医療機関等の管理者への証明書発行時、「1. 自然人への証明書発行」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およ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、持参もしくは郵送の場合、電話帳などの第三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实在性確認を行うものとする。

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实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。

(1) 郵送の場合

申請時に郵送され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. 自然人への証明書発行」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。

また、確認に用いた書類は本登録局でコピーを取り、5年間保存しておくものとする。

4. 下位認証局への証明書発行

認証局は、下位認証局への証明書発行時、「1. 自然人への証明書発行」の方法による申請者の確認に加え、「3.2.2 下位認証局の認証」に定める組織の立証に対し

て真偽の確認と、次の確認を行う。

- (1) 認証局申請の意思
法人印鑑を押印した申請書
- (2) 認証局責任者の職務職責
認証局責任者の在職・職責を法人代表者が確認もしくは任命した、法人印鑑を押印した任命書もしくは在職証明書
- (3) 認証局体制
認証局体制図
- (4) 認証サービスの継続性
有価証券報告書、貸借対照表、法人確定申告書、またはこれらに順ずる書類
- (5) ヘルスケア証明書ポリシー準拠
認証局サービス実施規程（CPS）
- (6) 認証局の实在確認
MEDIS 認証局職員が認証局に立ち入り調査を行い、实在性を確認する。
- (7) 認証局の運用体制
MEDIS 認証局職員が認証局に立ち入り調査を行い、認証局の運用体制を確認する。

なお、オンラインでの下位認証局証明書申請は認めない。

<代理人からの申請の場合>

MEDIS 認証局は、代理人からの申請の場合、申請者本人の本人性、实在性、申請意思および資格の確認、委任状による委任の意思確認を実施することに加え、以下の手順により代理人の本人性確認を実施する。

1. 持参の場合

MEDIS 認証局は、代理人に「3.2.4 個人の認証」の<持参の場合>に定める本人性を確認する書類の提示を求め、対面による代理人の本人性の確認を実施する。

2. 郵送の場合

MEDIS 認証局は、代理人による郵送の申請を認めない。

3. オンラインの場合

オンラインによる申請は認めない。

4.2.2 証明書申請の承認と却下

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

< 認証局が鍵ペアを生成する場合 >

本認証局が鍵ペアを生成する場合は、「電子署名及び認証業務に関する法律施行規則」第 6 条第三号に基づく CPS および事務取扱要領に準拠し、下記の通り運用する。

1. 利用者鍵ペアの生成は、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る。
2. 利用者鍵ペアの転送や出力を行う場合も、1 と同等のセキュリティ対策を講じる。また、利用者鍵ペアを転送、出力した後は、速やかに利用者鍵ペアを完全に廃棄もしくは消去する。
3. 利用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、1 と同等のセキュリティ対策を講じる。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。

(1) < 加入者が鍵ペアを生成する場合 >

加入者証明書の申請に際して加入者が鍵ペアを生成することを認めない。

< 下位認証局が鍵ペアを生成し、証明書署要求 (CSR) を持参する場合 >

下位認証局証明書を申請する加入者は、MEDIS 認証局が別途定める様式で記述された CSR を、別途 MEDIS-DC が定める可搬媒体に保存し、申請書に併せて持参または郵送するものとする。

4.3.2 証明書発行後の通知

MEDIS 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

本認証局は、電子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、証明書を交付してから 30 日以内に受領が確認できない場合、証明書を失効させる。

4.4.2 認証局による証明書の公開

本認証局は、加入者および下位認証局の証明書の公開を行わない。

4.4.3 他の機関に対する証明書発行通知

本認証局は、他の機関に対する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用途

4.5.1 加入者の秘密鍵と証明書の利用用途

加入者は、電子署名用私有鍵を電子署名にのみ利用するものとする。

加入者は、私有鍵および証明書の使用に関して、次の責任を負うものとする。

- ・ 証明書記載内容の受領時確認と誤記内容の深刻
- ・ 私有鍵の盗難、漏洩、紛失、他者による不正利用等を防ぐ事への注意と管理
- ・ 鍵の危殆化またはその可能性がある場合の速やかな失効申請

4.5.2 検証者の公開鍵と証明書の利用用途

検証者は、電子署名用公開鍵を電子署名の検証のみに利用するものとする。

4.6 証明書更新

MEDIS 認証局は、鍵更新を伴わない証明書更新は行なわない。

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証明書の更新申請を受付ける。

- ・ 更新対象証明書が存在すること。
- ・ 証明書が有効期限終了前のものであること。
- ・ 証明書が失効されていないこと。
- ・ 加入者証明書においては、有効期限終了前 30 日以内に申請があったこと。下位認証局証明書においては証明書発行から別途定める期間を経過した後に申請があったこと。

4.7.2 鍵更新申請者

本認証局は、証明書所有者本人もしくはその代理人を鍵更新申請者として受付ける。

4.7.3 鍵更新申請の処理手順

「4.2.1 本人性及び資格確認」に定める本人性確認ならびに資格確認を行なうものとする。

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なうことができる。

4.7.4 申請者への新証明書発行通知

本認証局は、電子証明書を申請者に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。

4.7.5 鍵更新された証明書の受理

本認証局は、電子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、証明書を交付してから 60 日以内に受領が確認できない場合、証明書を失効させる。

4.7.6 認証局による鍵更新証明書の公開

本認証局は証明書の公開を行なわない。

4.7.7 他のエンティティへの証明書発行通知

本認証局は他の機関への証明書発行の通知を行なわない。

4.8 証明書変更

本認証局は、証明書変更を認めない。

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。

<証明書所有者もしくはその代理人から失効申請があった場合>

証明書所有者もしくはその代理人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、HPKI-CP、もしくは本 CPS、又はその他の契約、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
 - ・ 証明書発行後、30日を経過しても、加入者が所定の費用を支払わない場合
- 証明書に含まれる該当の情報が正確でなくなったことを本認証局が確認した場合。(例えば、医師資格等の保健医療福祉分野専門資格を喪失した場合)。
- ・ HPKI-CP、もしくは本 CPS またはその双方に従って証明書が適切に発行されなかったと本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

本認証局は、次の1人又はそれ以上の者からの失効申請を受付ける。

1. 本人の名前で証明書が発行された加入者もしくはその代理人。
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。

<本人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加入者であること

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 本人性及び組織の認証」で用いた申請者の各種書類を参照する。

<代理人からの失効申請の場合>

代理人が失効を要求して来た場合は、当該代理人が正当な失効権限を持っていることを確認する。確認にあたっては、加入者の委任状の提出、本人死亡の場合などは、法定代理人と確認できる書類等の提出を求める。

当該証明書の実際の失効にあたっては、代理人を通じて失効を要求している申請者が、失効される証明書に記されている加入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 本人性及び組織の認証」で用いた申請者の各種書類を参照する。

この手順により証明書の失効を実施した場合は、CRLを発行すると共にリポジトリに公開することにより申請者に通知する。

<認証局の職員からの失効申請の場合>

本認証局は「4.9.1 証明書失効の要件」の中の認証局の職員から失効申請があった場合は、速やかに当該証明書を特定し、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。

証明書の失効を実施した場合は、CRLを発行すると共にリポジトリに公開することにより申請者に通知する。

4.9.4 失効における猶予期間

「4.9.1 証明書失効の要件」に規定されている事由が発生した場合には、速やかに失効申請を行うものとする。

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、申請書受領後次営業日中まで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、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なうものとする。

4.9.7 CRL/ARL 発行頻度

変更がない場合においても、48時間毎に96時間の有効期限のCRL/ARL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）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/ARL が公開されない最大期間

CRL/ARL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

規定しない。

4.9.10 オンラインでの失効確認要件

規定しない。

4.9.11 その他利用可能な失効情報確認手段

使用しない。

4.9.12 鍵の危殆化に関する特別な要件

本認証局は、CA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

行なわない。

4.9.14 一時停止申請者

一時停止は行なわない。

4.9.15 一時停止申請の処理手順

一時停止は行なわない。

4.9.16 一時停止期間の制限

規定しない。

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

証明書所有者が、証明書の利用を終了する場合、本実施規程「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 キーエスクローと鍵回復ポリシー及び実施

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ー及び実施

規定しない。

5. 建物・関連設備、運用のセキュリティ管理

これらは、JIS X 5080:2002 と同等以上の規格、又は認可された認定あるいは免許基準に従うものとする。これは、次の項目をカバーする。

5.1 建物及び関連設備管理

5.1.1 施設の位置と建物構造

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）を設置する施設は、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 入退管理

CA システムを設置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を行い、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

認証設備室内において使用される電源設備について停電に対する措置を講じる。

また、空調設備により、機器が適切に動作する措置を講じる。

5.1.4 水害及び地震対策

CA システムを設置する施設には水害の防止のための措置を講じる。

また、認証業務用設備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脱落等を防止するための構成部品の固定することや、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施設には自動火災報知器及び消火装置が設置されていること

とする。また、防火区画内に設置されていることとする。

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

バックアップ媒体は、認証局施設における災害が発生しても、その災害によって損傷しないように、十分に離れた所に置く。

5.2 手続き的管理

手続き的管理は、ISO 17799:2000 第 8 章と同等以上の規格に従うものとする。

5.2.1 信頼すべき役割

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。MEDIS 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。

5.2.2 職務ごとに必要とされる人数

CA システムの私有鍵の操作は、権限のある複数の操作員によって行う。その他の CA システムの操作および登録局の端末を用いた発行・失効等の操作は、権限のある操作員によって行う。

CA システム設備の保守、CA システム機器等の故障時対応等において、認証設備室への入室権限を有しない者が入室する必要がある場合は、必ず入室権限者の立会いを必要とする。

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、登録局システムへのアクセス権限者は、認証局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 職務分割が必要になる役割

CA私有鍵の操作やCAシステム管理者、登録局システム管理者の登録等の重要操作は、複数人によるコントロールを採用する。

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 セキュリティ監査の手続き

セキュリティ監査手続きは、ISO 17799-1:2000 と同等以上の規格に従うものとする。

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10年間保存される。

5.4.4 監査ログの保護

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

5.4.5 監査ログのバックアップ手続

監査ログは、オフラインの記録媒体に3ヶ月毎にバックアップがとられ、それらの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

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

記録は、ISO 17799-1:2000 と同等以上の規格に従って保管されるものとする。

5.5.1 アーカイブ記録の種類

CA システム は、以下の情報をアーカイブする。

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

5.5.2 アーカイブを保存する期間

アーカイブする情報は、記録が作成されてから 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

規定しない。

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

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 危殆化と業務の継続性の保証

5.7.1 災害及び CA 私有鍵危殆化からの復旧手続き

MEDIS 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 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、障害発生時の際には、可能な限り速やかに、加入者、検証者に MEDIS 認証局 Web サイトにより通知する。

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、運用責任者の判断により、速やかに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/ARL 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 認証局の終了

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、次の方法を行う

- ①本認証業務の廃止日迄に有効期間の残っている全ての加入者証明書を失効させ、その失効リストはリポジトリに6ヶ月間公開する。
- ②本認証サービスを廃止する場合には、廃止日の90日前迄に、加入者に書面で通知するとともに、リポジトリにその旨を公開する。
- ③廃止時に、CA 秘密鍵を完全に初期化し、そのバックアップ媒体を物理的に完全に破壊する。

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、別途規定する本認証局の記録の安全な保管と確実な破棄の規定に従うものとする。

6. 技術的なセキュリティ管理

6.1 鍵ペアの生成と実装

6.1.1 鍵ペアの生成

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

6.1.2 所有者への私有鍵の送付

加入者以外の加入者の私有鍵が証明書所有予定者によって生成されない場合は、本人限定郵便または同等の安全性を有する輸送法によって、加入者に引き渡されるものとする。

認証局はオリジナルの私有鍵を引き渡した後は私有鍵のコピーを所有していないことの証明を行うものとする。

6.1.3 認証局への公開鍵の送付

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

6.1.4 検証者への CA 公開鍵の配付

CA 公開鍵は、検証者によるダウンロードを可能とするために、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。

認証局以外の証明書の鍵の最小サイズは、RSA アルゴリズムで、1024 ビットとする。他のアルゴリズムを使用する認証局以外の証明書の鍵の最小サイズは、同等のセキュリティを提供するサイズとする。

6.1.6 公開鍵のパラメータ生成及び品質検査

公開鍵パラメータは、信頼できる暗号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も暗号化モジュールにより行うものとする。

6.1.7 鍵の使用目的

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

加入者の鍵は、nonRepudiation のビットを使用する。

6.2 私有鍵の保護及び暗号化モジュール技術の管理

6.2.1 暗号化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。

認証局以外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 複数人による私有鍵の管理

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。

認証局以外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

認証局は証明書所有者の私有鍵をアーカイブしない。

6.2.6 暗号化モジュールへの私有鍵の格納

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 暗号化モジュールへの私有鍵の格納

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

6.2.8 私有鍵の活性化方法

CA 私有鍵の活性化の方法は、認証局室内において本実施規程「6.2.2 秘密鍵の複数人コントロール」と同じく、複数名の権限を有する者を必要とする。

6.2.9 私有鍵の非活性化方法

CA 私有鍵の非活性化の方法は、認証局室内において本実施規程「6.2.2 秘密鍵の複数人コントロール」と同じく、複数名の権限を有する者を必要とする。

6.2.10 私有鍵の廃棄方法

CA 私有鍵を破棄しなければならない状況の場合、認証局室内で本実施規程「6.2.2 秘密鍵の複数人コントロール」と同じく、複数人によって、秘密鍵の格納された HSM を完全に初期化し、又は物理的に破壊する。同時に、バックアップの秘密鍵に関しても同様の手続きによって破棄する。

加入者私有鍵破棄手続きは、加入者が入手可能な文書に記述するものとする。

6.2.11 暗号化モジュールの評価

CA 私有鍵を格納する暗号化モジュールは、FIPS 140-2 レベル 3 と同等以上のものを使用する。

認証局以外の加入者の私有鍵を格納する暗号化モジュールは、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

公開鍵は、後日の署名の検証を可能にするために、信頼できる方法でアーカイブする必要がある。認証局は、公開鍵が 10 年間アーカイブされることを保証する責任があるものとする。

6.3.2 私有鍵と公開鍵の有効期間

CA 私有鍵の有効期間は 10 年とする。また、鍵の使用は 5 年とする。

認証局以外の加入者の私有鍵の有効期間は5年を越えないものとし、その鍵の使用は2年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

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

認証局以外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

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

認証局以外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

認証業務用設備に対する当該電気通信回線を通じて行われる不正なアクセス等を防御するための対策を行うこと。

CA システムへのログイン時には、本認証規程「5.2.3 個々の役割に対する本人性確認と認証」で定めるユーザの認証を必須とする。

6.5.2 コンピュータセキュリティ評価

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

MEDIS 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ーを導入すべく、随時本運用管理規定及び各種運用規程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

MEDIS 認証局は、システムの品質及びセキュリティを保つために、開発時における各工程の管理、導入前の評価等を実施する。

6.6.2 セキュリティ運用管理

MEDIS認証局は、入退室管理、教育を含む要員管理、権限管理等の運用管理の実施、不正侵入対策、ウイルス対策等のシステムのセキュリティ対策、セキュリティ対策ソフトウェアの適時更新等を実施する。

6.6.3 ライフサイクルのセキュリティ管理

規定しない。

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。

本認証局の存在するネットワークに対するアクセスは全て監視、記録され、不正なアクセスを早期に発見可能なシステムとする。

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のプロファイル

7.1 証明書のプロファイル

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

本認証局が発行する加入者証明書のプロファイルは、表 7.1.1 および表 7.1.2 の通りとする。また、本認証局が発行する下位認証局証明書のプロファイルを、表 7.1.3 および表 7.1.4 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 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

本ポリシーの認証局が発行する証明書は、X509 Version 3 フォーマット証明書形式により作成されることとする。

7.1.2 証明書の拡張

本ポリシー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 7.1.2 の通りとする。また、下位認証局証明書の拡張領域のプロファイルは以下の表 7.1.4 の通りとする。表中の、「◎」は必須、「○」は場合により必須、「×」は設定しないことを表す。

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

7.1.3 アルゴリズムオブジェクト識別子

基本領域の Signature アルゴリズムは以下の通りとする。

sha1WithRSAEncryption (1.2.840.113549.1.1.5)

基本領域のsubjectPublicKeyInfoアルゴリズムは以下の通りとする。

RSAEncryption (1.2.840.113549.1.1.1)

7.1.4 名前の形式

Issure と Subject の名前の形式は表 7.1.1 に示される。

7.1.5 名前制約

用いない。

7.1.6 CPS オブジェクト識別子

規定しない

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

CPS を参照する URL を含めることができる。！

7.1.9 証明書ポリシ拡張フィールドの扱い

本 CP の OID を格納する。

表 7.1.1 MEDIS-HPKI 認証局証明書のプロファイル (基本領域)

項目	値または説明
Version	Ver3 (2)
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	YYYYMMDDhhmmssZ
NotAfter	発行日から 20 年間
Issuer	CountryName は Printable、それ以外は UTF-8 で記述する。
CountryName	‘JP’

OrganizationName	‘MEDIS-DC’
OrganizationUnitName	‘MEDISrootCA’
CommonName	‘HPKI-01- MedisTopCA1-for-nonRepudiation’
Subject	CountryName は Printable、それ以外は UTF-8 で記述する。
CountryName	‘JP’
OrganizationName	‘MEDIS-DC’
OrganizationUnitName	‘MEDISrootCA’
CommonName	‘HPKI-01- MedisTopCA1-for-nonRepudiation’
SubjectPublicKeyInfo	rsaEncryption
Algorithm	SHA1WithRSAEncryption
SubjectPublicKey	公開鍵
Extensions	拡張領域(表 7.1.2)参照

表 7.1.2 MEDIS-HPKI 認証局証明書のプロファイル (拡張領域 Extensions)

項目	説明	Critical
authorityKeyIdentifier	Issuer の公開鍵のハッシュ値	FALSE
subjectKeyIdentifier	Subject の公開鍵のハッシュ値	FALSE
keyUsage	KeyCertSign CRLSign	TRUE
certificatePolicies	policyIdentifier に” 1.2.392.100495.1.5.1.0.3.1”	TRUE
subjectAltName	規定しない	FALSE
issuerAltName	規定しない	FALSE
subjectDirectoryAttributes	設定しない。	FALSE
cRLDistributionPoints	DirectoryName および URI で、CRL の配布点を指定する。	FALSE

表 7.3 加入者用証明書のプロフィール（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	◎	
Validity	◎	
NotBefore	◎	
NotAfter	◎	
Issuer	◎	英数字のみ使用する。（CountryName は Printable、それ以外は UTF-8 で記述する）
CountryName	◎	c=JP（固定）とする。
LocalityName	△	
OrganizationName	◎	
OrganizationUnitName	△	
CommonName	◎	認証局のポリシーを示す文字列を記載する。 HPKI-01- MedisCA3-for-nonRepudiation
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	◎	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、 OrganizationUnitName 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（Extensions）参照

表 7.4 加入者用証明書のプロフィール（基本領域）

項目	設定	説明	Critical
authorityKeyIdentifier	◎		FALSE
subjectKeyIdentifier	◎		FALSE
KeyUsage	◎		TRUE
DigitalSignature	×		-
NonRepudiation	◎		-
KeyEncipherment	×		-
DataEncipherment	×		-
KeyAgreement	×		-
KeyCertSign	×		-
CRLSign	×		-
EncipherOnly	×		-
DeciphermentOnly	×		-
extendedKeyUsage	×		FALSE
privateKeyUsagePeriod	×		FALSE
certificatePolicies	◎		TRUE
policyMapping	×		FALSE
subjectAltName	△	漢字で加入者氏名、所属を入れることができる。	FALSE
issuerAltName	△		FALSE
subjectDirectoryAttributes	◎	医療従事者等の資格（hcRole）を記載。	FALSE
AttrType	○	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。	-
AttrValues	○	HCActor の codeDataFreeText に資格名テーブル表 7.1.3 の英表記を UTF8String で設定。subject が複数の資格を有する場合は、HCActorData に資格数分の HCActor を設定する。	-
basicConstraints	×		TRUE
CA	×		-
pathLenConstraints	×		-
nameConstraints	×		TRUE
policyConstraints	×		TRUE
cRLDistributionPoints	◎	DirectoryName あるいは URI で、CRL の配布点を指定する。	FALSE
subjectInfoAccess	×		FALSE
authorityInfoAccess	△		FALSE

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での hcRole 属性の使用

MEDIS HPKI 認証局が発行する加入者証明書には、HPKI ポリシで規定した 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。

本ポリシでは coding scheme reference の OID として ISO coding scheme reference を用いず、本 CP の元で定めた表 7.1.3 の資格名を参照する local coding scheme reference の OID は、 { iso(1) member-body(2) jp(392) mhlw(100495)jhpki(1) hcRole(6) national-coding-scheme-reference(1) version(1) } を用いる。資格名は、下記に示すように英語表記を用い UTF8string で設定する。

subject が複数の資格を有する場合は、HCActorData に資格数分の HCActor を設定することができる。本拡張は、加入者が国家資格保有者及び医療機関等の管理者の場合は必須、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。

Medical Doctor	医師
Dentist	歯科医師
Pharmacist	薬剤師
Medical Technologist	臨床検査技師
Radiological Technologist	診療放射線技師
General Nurse	看護師
Public Health Nurse	保健師
Midwife	助産師
Physical Therapist	理学療法士
Occupational Therapist	作業療法士
Orthoptist	視能訓練士
Speech Therapist	言語聴覚士
Dental Technician	歯科技工士
National Registered Dietitian	管理栄養士
Certified Social Worker	社会福祉士
Certified Care Worker	介護福祉士
Emergency Medical Technician	救急救命士
Psychiatric Social Worker	精神保健福祉士
Clinical Engineer	臨床工学技師

Masseur	あん摩マッサージ指圧師/はり師/きゅう師
Dental Hygienist	歯科衛生士
Prosthetics & Orthetic	義肢装具士
Artificial Limb Fitter	柔道整復師
Clinical Laboratory Technician	衛生検査技師
Care Manager	介護支援専門員

この他に医療機関の管理責任者として、次の属性を使用することができる。

Director of Hospital	病院長
Director of Clinic	診療所院長
Director of Pharmacy	保険薬局の管理責任者
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病院長、診療所院長、保険薬局の管理責任者を **HcRole** だけで識別できるように定めている。

なお、上記 **Director** 4 属性を使用する場合は **Subject** フィールドの **OrganizationName** および **OrganizationUnitName** は必須で、**OrganizationName** に保健医療福祉機関名を英語またはローマ字で格納し、**OrganizationUnitName** に”Director”の文字列を格納する。

(2)hcRole のプロファイル

MEDIS HPKI 認証局が発行する加入者証明書の 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
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 CP では使用しない。
- Note2 : 日本の HPKI CP で定めた local coding scheme reference の OID は、
id-jhpki-cdata{iso(1) member-body(2) jp(392) mhlw(100495) jhpki(1) hcRole(6)
national-coding-scheme-reference(1) version(1)} とする。この OID は、表 7.1.3
の資格名を参照する。
- Note3 : 本 CP では CodedData の codeDataValue は用いない。
- Note4 : 本 CP では、codeDataFreeText としての DirecroryString には表 7.1.3 に規定
した ‘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

7.2.1 バージョン番号

認証局が発行する CRL は、X.509CRL フォーマット形式のバージョン 2 に従うものとする。MEDIS-HPKI 認証局の CRL の基本領域のプロファイルを表 7.2.1 に示す。

7.2.2 CRL と CRL エントリ拡張領域

CRL エントリの拡張領域のプロファイルを表 7.2.2 に示す。CRL 拡張領域のプロファイルを表 7.2.3 に示す。

表 7.2.1 証明書失効リストのプロファイル

フィールド	説明
Version	Ver2 (1)
Signature	SHA-1WithRSAEncryption
Issuer	CountryName は Printable、それ以外は UTF-8 で記述する。
CountryName	‘JP’
OrganizationName	‘MEDIS-DC’
OrganizationUnitName	‘MEDISrootCA’
CommonName	‘HPKI-01- MedisCA3-for-nonRepudiation’
ThisUpdate	YYYYMMDDhhmmssZ
NextUpdate	YYYYMMDDhhmmssZ
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 7.2.2 の拡張領域 (crlEntryExtentions) 参照
crlExtentions	表 7.2.3 の拡張領域 (crlExtensions) 参照

表 7.2.2 証明書失効リストのプロファイル

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

表 7.2.3 証明書失効リストのプロファイル

フィールド	説明	Critical
authorityKeyIdentifier	Issuer の公開鍵のハッシュ値	FALSE
cRLNumber	MEDISHPKI 上位認証局が採番する。	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

MEDIS 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、利用者および HPKI ポリシ準拠性評価機関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

MEDIS 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

認証局は、認証局業務を直接行なっている研究開発部以外の、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 MEDIS 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

監査は、HPKI-CP および本 CPS の準拠性をカバーする。

8.5 監査指摘事項への対応

認証局は、認証局代表者の指示のもと、監査における指摘事項に対する改善措置を実施する。

8.6 監査結果の通知

監査者によって証明書の信頼性に影響する重大な欠陥が発見された認証局又は登録局は、証明書所有者及び検証者および準拠性評価機関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、別途定めるものとし、事前に関係者に周知する。

9.2 財務上の責任

MEDIS-DC は、本 CPS に規定した内容を遵守して認証サービスを提供し、本 CPS の範囲内で、本認証局の私有鍵の信頼性を含む認証業務の信頼性の確保を保証する。

MEDIS-DC は、MEDIS-DC 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 企業情報の秘密保護

9.3.1 秘密情報の範囲

本実施規程に従う認証局が保持する個人および組織の情報は、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。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。

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および財務顧問に対し、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、買収あるいは再編成に関連してアドバイスする弁護士、会計士、金融機関およびその他の専門家に対しても、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。

加入者の秘密鍵は、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。認証局は、本実施規程「8.6 監査結果の報告」に記載されている場合およ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

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

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

ただし、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もの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、その責は漏洩したものが負う。

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（保護規定）

MEDIS-認証局は、個人情報の重要性を認識し、次のように取扱う。

- ① 個人情報を取扱う部門ごとに管理責任者を置き、個人情報の適切な管理を行う。
- ② 個人情報を収集する場合、収集目的を知らせた上で、必要な範囲の情報のみを適法かつ公正な手段で収集する。
- ③ 下位認証局または加入者から提出を受けた個人情報は、以下の目的にのみ使用する。
 - ・ 下位認証局または加入者との本サービス上の責任を果たすため
 - ・ 下位認証局または加入者によりよいサービス・商品を提供するため
 - ・ 下位認証局または加入者に有用な情報を提供するため
 - ・ その他の正当な目的のため
- ④ 下位認証局または加入者の同意がある場合および法令に基づく場合を除き、個人情報を業務委託先以外の第三者に開示することはしない。業務委託先に開示する場合は、当該業務委託先に対しこの規程と同等の条件を義務付けるものと

する。

- ⑤ 個人情報の管理責任者は、適切な安全対策を講じて、個人情報を不正アクセス、紛失、破壊、改ざんおよび漏洩等から保護する責任を持ち、これに努める。
- ⑥ 下位認証局または加入者の個人情報について開示を求められた場合、第三者への個人情報の漏洩を防止するため、下位認証局または加入者自身であることが **MEDIS**-認証局において確認できた場合に限り、**MEDIS**-認証局において保管している下位認証局または加入者の個人情報を本人に開示する。また、下位認証局または加入者の個人情報に誤りや変更がある場合には、下位認証局または加入者からの申し出に基づき、合理的な範囲で速やかに、不正確な情報または古い情報を修正または削除する。下位認証局または加入者は **MEDIS**-認証局に開示を求める場合、「9.4.7 その他の情報開示条件」に記述された方法により申請を行うものとする。
- ⑦ **MEDIS**-認証局は、認証局職員に対して個人情報保護の教育啓蒙活動を実施している。
- ⑧ 下位認証局または加入者の個人情報に関して適用される法令、規範を遵守するとともに、適切な個人情報保護を維持するために、個人情報保護のポリシーを適宜見直し、改善を行う。

9.4.2 プライバシーとして保護される情報

認証局は、次の情報を秘密情報として取り扱う。

- ・ 登録局が本人確認や各種審査の目的で収集した情報の中で、証明書に含まれない情報。
例えば、身分証明書、自宅住所、連絡先の詳細など、他の情報と容易に照合することができ、それにより特定の個人を識別することが可能な情報を指す。
- ・ **CRL** に含まれない証明書所有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。

- ・ 公開鍵証明書及び **CRL** に記載された情報
- ・ **CRL** に記載された情報

9.4.4 個人情報保護責任

MEDIS-DC 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

MEDIS-DC は、証明書発行業務及びその他の認証業務の利用目的に限り個人情報を利用する。それ以外の目的で個人情報を利用する場合は、法令で除外されている場合を除き、あらかじめ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、MEDIS-DC 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、MEDIS—DC 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

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

- ・ 加入者証明書：認証局に帰属する財産である。
- ・ 加入者の私有鍵：私有鍵は、その保存方法又は保存媒体の所有者にかかわらず、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かかわらず、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、
- ・ 本実施規程：MEDIS-DC 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

認証局は、その運営にあたり、HPKI—CP と本実施規定に基づいて、証明書所有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 の要件と本実施規定に従って行われること。
- ・ 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。
- ・ 認証局が証明書を発行する時は、証明書に記載されている情報が本実施規程に従って検証されたことを保証すること。
- ・ 公開鍵を含む証明書を加入者に確実に届けること。
- ・ 本実施規程で定める失効ポリシー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実施規程により、速やかに入手できるようにすること。
- ・ 本実施規程に定める方法で、HPKI 証明書ポリシーおよび本実施規定に基づく証明書所有者の権利と義務を各証明書所有者に通知すること。
- ・ 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証明書所有者に通知すること。
- ・ 本実施規程「5 建物及び関連施設、運用のセキュリティ」及び「6 技術的セキュリティ管理」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、10年間保管すること。
- ・ 認証局の発行する証明書の中で、加入者に対して、所有者の名称 (subjectDN) の一意性を検証可能にしておくこと。

9.6.2 登録局の表明保証

MEDIS 登録局は、加入者、検証者、認証局に対して次の責任を果たすものとする。ま

- ・ 証明書発行にあたり、申請内容の真偽の確認を確実にを行い、確認の結果を認証局に対して保証すること。
- ・ 認証局の発行する証明書の中で、加入者に対して所有者の名称 (subjectDN) の一意性を検証可能にしておくこと。
- ・ 証明書申請情報を認証局に安全に送付し、登録記録を安全に保管すること。
- ・ 証明書失効申請を行う場合は、本実施規程「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年間保管すること。

9.6.3 証明書所有者の表明保証

本実施規程に則り運営される認証局の加入者は、認証局に対して次の責任を果たすものとする。

1. 証明書発行申請内容に対する責任
証明書発行申請を行う場合、認証局に提示する申請内容が虚偽なく正確であることに対する責任を果たすこと。
2. 証明書記載事項の担保責任
証明書の記載内容について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
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適切な措置を取ること。
4. 各種の届出に対する責任
私有鍵の紛失、暴露、その他の危殆化、又はそれらが疑われる時には、認証局の定める CPS に従って速やかに届け出ること。
また、証明書情報に変更があった場合は、本実施規定に従って速やかに届け出ること。
5. 利用規定の遵守責任
証明書所有者は、本実施規程及び認証局で加入者に対して開示される文章を読み、その利用規定及び禁止規定を遵守すること。

9.6.4 検証者の表明保証

本実施規程に則り運営される認証局の検証者は以下の責任を果たすものとする。

1. 利用規定の遵守責任
検証者は、本実施規程及び認証局で検証者に対して開示される文章を読み、その利用規定及び禁止規定を遵守すること。また、証明書の利用に際しては信頼点の管理を確実にすること。
2. 証明書記載事項の確認責任
検証者は、証明書を利用する際に、その有効性を確認する責任がある。有効性の確認には、以下の事項が含まれる。
 - ・ 証明書の署名が正しいこと
 - ・ 証明書の有効期限が切れていないこと

- ・ 証明書が失効していないこと
- ・ 証明書の記載事項が、本実施規程「7 証明書及び失効リストのプロファイル」に記述されているプロファイルと合致していること。特に、次の 2 点の検証を実施することは HPKI 署名用証明書として重要である。
 - OID および Issuer の CN が HPKI の規定に一致していること
 - hcRole および keyUsage の nonRepudiation のみが立てられていること

9.6.5 他の関係者の表明保証

規定しない。

9.7 無保証

認証局は、本実施規程「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、本実施規程「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

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。

また、認証局および登録局の責任は、認証局および登録局の怠慢行為により CP、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、本実施規程「9.6 表明保証」に関し、次の場合、認証局は責任を負わない。

- ・ 認証局に起因しない不法行為、不正使用並びに過失等により発生する一切の損害
- ・ 加入者又は検証者が自己の義務の履行を怠ったために生じた損害
- ・ 加入者又は検証者のシステムに起因して発生した一切の損害
- ・ 加入者又は検証者が使用する端末のソフトウェアの瑕疵、不具合あるいはその他の動作自体によって生じた損害
- ・ 認証局の責に帰することのできない事由で電子証明書及び CRL に公開された情報に起因する損害
- ・ 認証局の責に帰することのできない事由で正常な通信が行われない状態で生じた一切の損害

- ・ 証明書の使用に関して発生する業務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

本実施規程に規定された責任を果たさなかったことに起因して、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 MEDIS-DC に支払った金額を上限として損害を賠償する。

ただし、認証局側の責に帰さない事由から発生した損害、逸失利益、間接損害、又は予見の有無を問わず特別損害については、いかなる場合でも一切の責任を負わない。

また、加入者は認証局が発行する証明書を申請した時点で、検証者は信頼した時点で、認証局及び関連する組織等に対する損害賠償責任が発生する。

9.10 文書の有効期間と終了

9.10.1 有効期間

本実施規程は、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」で記述する本実施規程の終了まで有効であるものとする。

9.10.2 終了

本実施規程は、「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、「MEDIS-DC 理事長」が無効と宣言した時点又は「CPS 管理組織? どちらか?」が機能を果たさなくなった場合、無効になる。

9.10.3 終了の影響と存続条項

文書が終了した場合であっても、「9.3 企業情報の秘密保護」、「9.4 個人情報のプライバシー保護」、「9.5 知的財産権」に関する責務は存続するものとする。また、「CPS 管理組織」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

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、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發した場合には、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

「CPS 管理組織」が本実施規程の改訂を行う場合は、改訂に先立ち、改定案をウェブサイト等 MEDIS-DC が適当と判断する媒体を通じて公開し、意見を求める。

本実施規程が変更された時は、HPKI 認証局専門家会議によって承認される。

9.12.2 通知方法と期間

本実施規程が改訂された場合、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發する。なお、通知後、上記で示した方法に従い告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、効力を發する。
- ・ 重要でない変更は、通知後直ちに効力を發する。

9.12.3 オブジェクト識別子 (OID) などの変更理由

本実施規程の変更があった場合には、本実施規程のバージョン番号を更新する。また、次の場合には、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

本実施規程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

加入者及び検証者の所在地に関わらず、本実施規程の解釈、有効性及び本認証局の証明書発行に関わる紛争については、日本国の法令が適用される。

9.15 適用法の遵守

本実施規程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

本実施規程は、本実施規程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、本実施規程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実施規程に定める業務の委託を行うとき
- ・ 本実施規程に則った認証局の移管もしくは譲渡を行うとき

9.16.3 分離条項

本実施規程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

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とする。不可抗力によって損害が発生した場合、本実施規程「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、本実施規程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

本実施規程を採用した認証局又は登録局が別の組織と合併もしくは別の組織に移管、譲渡する場合、新しい組織は本実施規程の方針に同意し責任を持ちつづけるものとする。