資　料　6

改定履歴

版数	日付	内容
初版	平成　年　月	初版発行

保健医療福祉分野 PKI 認証局
認証用（組織）証明書ポリシ（案）

平成　　年　　月

厚生労働省

－目次－

1 はじめに 1

1.1 概要 1
1.2 文書の名前と識別 2
1.3 PKI の関係者 3
1.3.1 認証局 3
1.3.2 登録局 3
1.3.3 加入者 3
1.3.4 検証者 3
1.3.5 その他の関係者 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 本ポリシを管理する組織 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 4
1.5.4 CPS 承認手続き 4
1.6 定義と略語 5

2 公開及びリポジトリの責任 11

2.1 リポジトリ 11
2.2 証明書情報の公開 11
2.3 公開の時期又はその頻度 11
2.4 リポジトリへのアクセス管理 11

3 識別及び認証 12

3.1 名称決定 12
3.1.1 名称の種類 12
3.1.2 名称が意味を持つことの必要性 12
3.1.3 加入者の匿名性又は仮名性 12
3.1.4 種々の名称形式を解釈するための規則 12
3.1.5 名称の一意性 12
3.1.6 認識、認証及び商標の役割 12
3.2 初回の本人性確認 12
3.2.1 私有鍵の所持を証明する方法 12
3.2.2 組織の認証 13
3.2.4 確認しない加入者の情報 18
3.2.5 機関の正当性確認 18
3.2.6 相互運用の基準 18
3.3 鍵更新申請時の本人性確認及び認証 18
3.3.1 通常の鍵更新時の本人性確認及び認証 18
3.3.2 証明書失効後の鍵更新の本人性確認及び認証 19
3.4 失効申請時の本人性確認及び認証 19

4 証明書のライフサイクルに対する運用上の要件 20

4.1 証明書申請 20
4.1.1 証明書の申請者 20
4.1.2 申請手続及び責任 20
4.2 証明書申請手続き 21
4.2.1 本人性及び資格確認 21
4.2.2 証明書申請の承認又は却下 24
4.2.3 証明書申請手続き期間 24
4.3 証明書発行 24
4.3.1 証明書発行時の認証局の機能 24
4.3.2 証明書発行後の通知 25
4.4 証明書の受理 25
4.4.1 証明書の受理 25
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
4.6.1 証明書更新の要件 26
4.6.2 証明書の更新申請者 26
4.6.3 証明書更新の処理手順 26
4.6.4 加入者への新証明書発行通知 26
4.6.5 更新された証明書の受理 26
4.6.6 認証局による更新証明書の公開 26
4.6.7 他のエンティティへの証明書発行通知 27
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
4.8.1 証明書変更の要件 27
4.8.2 証明書の変更申請者 27
4.8.3 証明書変更の処理手順 27
4.8.4 加入者への新証明書発行通知 28
4.8.5 変更された証明書の受理 28
4.8.6 認証局による変更証明書の公開 28
4.8.7 他のエンティティへの証明書発行通知 28
4.9 証明書の失効と一時停止 28
4.9.1 証明書失効の要件 28
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 30
4.9.6 検証者の失効情報確認の要件 30
4.9.7 CRL 発行頻度 30
4.9.8 CRL が公開されない最大期間 30
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 31
4.9.16 一時停止期間の制限 31
4.10 証明書ステータスの確認サービス 31
4.10.1 運用上の特徴 31
4.10.2 サービスの利用可能性 31
4.10.3 オプショナルな仕様 31
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 34
5.2.3 個々の役割に対する本人性確認と認証 34
5.2.4 職務分離が必要になる役割 35
5.3 要員管理 35
5.3.1 資格、経験及び身分証明の要件 35
5.3.2 経歴の調査手続 35
5.3.3 研修要件 35
5.3.4 再研修の頻度及び要件 35
5.3.5 職務のローテーションの頻度及び要件 35
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 36
5.3.8 要員へ提供する資料 36
5.4 監査ログの取扱い 36
5.4.1 記録するイベントの種類 36
5.4.2 監査ログを処理する頻度 36
5.4.3 監査ログを保存する期間 36
5.4.4 監査ログの保護 36
5.4.5 監査ログのバックアップ手続 36
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 37
5.5 記録の保管 37
5.5.1 アーカイブ記録の種類 37
5.5.2 アーカイブを保存する期間 37
5.5.3 アーカイブの保護 37
5.5.4 アーカイブのバックアップ手続 37
5.5.5 記録にタイムスタンプをつける要件 38
5.5.6 アーカイブ収集システム（内部対外部） 38
5.5.7 アーカイブ情報を入手し、検証する手続 38
5.6 鍵の切り替え 38
5.7 危殆化及び災害からの復旧 38
5.7.1 災害及び CA 私有鍵危殆化からの復旧手続き 38
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 38
5.7.3 CA 私有鍵が危殆化した場合の対処 38
5.7.4 災害等発生後の事業継続性 39
5.8 認証局又は登録局の終了 39
6 技術的なセキュリティ管理 40
6.1 鍵ペアの生成と実装 40
6.1.1 鍵ペアの生成 40
6.1.2 加入者への私有鍵の送付 40
6.1.3 認証局への公開鍵の送付 40
6.1.4 検証者への CA 公開鍵の配付 40
6.1.5 鍵のサイズ 40
6.1.6 公開鍵のパラメータ生成及び品質検査 40
6.1.7 鍵の利用目的 41
6.2 私有鍵の保護及び暗号モジュール技術の管理 41
6.2.1 暗号モジュールの標準及び管理 41
6.2.2 私有鍵の複数人によるコントロール 41
6.2.3 私有鍵のエスクロウ 41
6.2.4 私有鍵のバックアップ 41
6.2.5 私有鍵のアーカイブ 41
6.2.6 暗号モジュールへの私有鍵の格納と取り出し 41
6.2.7 暗号モジュールへの私有鍵の格納 42
6.2.8 私有鍵の活性化方法 42
6.2.9 私有鍵の非活性化方法 42
6.2.10 私有鍵の廃棄方法 42
6.2.11 暗号モジュールの評価 42
6.3 鍵ペア管理に関するその他の面 42
6.3.1 公開鍵のアーカイブ 42
6.3.2 公開鍵証明書の有効期間と鍵ペアの使用期間 42
6.4 活性化用データ 43
6.4.1 活性化データの生成とインストール 43
6.4.2 活性化データの保護 43
6.4.3 活性化データのその他の要件 43
6.5 コンピュータのセキュリティ管理 43
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 43
6.5.2 コンピュータセキュリティ評価 44
6.6 ライフサイクルの技術的管理 44
6.6.1 システム開発管理 44
6.6.2 セキュリティ運用管理 44
6.6.3 ライフサイクルのセキュリティ管理 44
6.7 ネットワークのセキュリティ管理 44
6.8 タイムスタンプ 44
7 証明書及び失効リスト及び OCSP のプロファイル 45
7.1 証明書のプロファイル 45
7.1.1 バージョン番号 45
7.1.2 証明書の拡張（保健医療福祉分野の属性を含む） 45
7.1.3 アルゴリズムオブジェクト識別子 45
7.1.4 名称の形式 45
7.1.5 名称制約 45
7.1.6 CP オブジェクト識別子 46
7.1.7 ポリシ制約拡張 46
7.1.8 ポリシ修飾子の構文及び意味 46
7.1.9 証明書ポリシ拡張フィールドの扱い 46
7.1.10 保健医療福祉分野の属性（hcRole） 49
7.2 証明書失効リストのプロファイル 53
7.2.1 バージョン番号 53
7.2.2 CRL と CRL エントリ拡張領域 53
7.3 OCSP プロファイル 54
7.3.1 バージョン番号 54
7.3.2 OCSP 拡張領域 54

8 準拠性監査とその他の評価 55
8.1 監査頻度 55
8.2 監査者の身元・資格 55
8.3 監査者と被監査者の関係 55
8.4 監査テーマ 55
8.5 監査指摘事項への対応 55
8.6 監査結果の通知 55
9 その他の業務上及び法務上の事項 56
9.1 料金 56
9.1.1 証明書の発行又は更新料 56
9.1.2 証明書へのアクセス料金 56
9.1.3 失効又はステータス情報へのアクセス料金 56
9.1.4 その他のサービスに対する料金 56
9.1.5 払い戻し指針 56
9.2 財務上の責任 56
9.2.1 保険の適用範囲 56
9.2.2 その他の資産 56
9.2.3 エンドエンティティに対する保険又は保証 56
9.3 業務情報の秘密保護 57
9.3.1 秘密情報の範囲 57
9.3.2 秘密情報の範囲外の情報 57
9.3.3 秘密情報を保護する責任 57
9.4 個人情報のプライバシー保護 57
9.4.1 プライバシーポリシ 57
9.4.2 プライバシーとして保護される情報 57
9.4.3 プライバシーとはみなされない情報 58
9.4.4 個人情報を保護する責任 58
9.4.5 個人情報の使用に関する個人への通知及び同意 58
9.4.6 司法手続又は行政手続に基づく公開 58
9.4.7 その他の情報開示条件 58
9.5 知的財産権 58
9.6 表明保証 59
9.6.1 認証局の表明保証 59
9.6.2 登録局の表明保証 60
9.6.3 加入者の表明保証 60
9.6.4 検証者の表明保証 61
9.6.5 他の関係者の表明保証 62
9.7 無保証 62
9.8 責任制限 62
9.9 補償 63
9.10 本ポリシの有効期間と終了 63
9.10.1 有効期間 63
9.10.2 終了 63
9.10.3 終了の影響と存続条項 63
9.11 関係者間の個々の通知と連絡 63
9.12 改訂 63
9.12.1 改訂手続き 64
9.12.2 通知方法と期間 64
9.12.3 オブジェクト識別子（OID）の変更理由 64
9.13 紛争解決手続 64
9.14 準拠法 64
9.15 適用法の遵守 64
9.16 雑則 65
9.16.1 完全合意条項 65
9.16.2 権利譲渡条項 65
9.16.3 分離条項 65
9.16.4 強制執行条項（弁護士費用及び権利放棄） 65
9.16.5 不可抗力 65
9.17 その他の条項 65

1 はじめに

1.1 概要

証明書ポリシ（Certificate Policy、以下 CP という）は、証明書発行（失効も含む）に関して「適用範囲」、「セキュリティ基準」、「審査基準」等の一連の規則を定めるものである。また、保健医療福祉分野 PKI は、保健医療福祉分野において情報を連携して利用するための公開鍵基盤である。

本ポリシは、保健医療福祉サービス提供者及び保健医療福祉サービス利用者への認証用公開鍵証明書を発行する「保健医療福祉分野 PKI 認証局」の証明書ポリシである。

保健医療福祉分野 PKI 認証局が発行した証明書は、組織とその公開鍵が一意に関連づけられることを証明するものである。認証局が証明書を発行するにあたって、その審査過程、登録、発行及び失効方法は、CP 及び認証局により開示される文書によって規定される。

加入者及び検証者は、保健医療福祉分野 PKI 認証局によって発行された証明書を利用する時は、CP 及び認証局により開示される文書の内容を、その利用方法に照らして評価する必要がある。

本 CP に準拠する個々の「保健医療福祉分野 PKI 認証局」は、本 CP を基準にして、個々の環境に適合した認証実施規程（Certificate Practice Statement、以下 CPS という）を作成するものとする。なお、CPS が本 CP に抵触する場合は CP が優先する。

本 CP は、電子署名及び認証業務に関する法律（以下、電子署名法という）に規定された「特定認証業務の認定」を受けた認証局のみを対象としているわけではなく、認定を受けない認証局も対象としている。従って、特定認証業務の認定を受ける場合は、本 CP に従い CPS に「特定認証業務の認定」を受けるに足る詳細を規定する必要がある。

なお、本 CP 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 Practice Framework
- ISO/IS 17090-1:2008 Health informatics - Public key infrastructure Part 1 : Framework and overview
- ISO/IS 17090-2:2008 Health informatics - Public key infrastructure Part 2 : Certificate profile
- ISO/IS 17090-3:2008 Health informatics - Public key infrastructure Part 3 : Policy management of certification authority

また、本 CP は以下の文章を参照する。

- IETF/RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols
- IETF/RFC 2560 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
- US FIPS140-2(Federal Information Processing Standard) : Security Requirements for Cryptographic Modules (http://csrc.nist.gov/cryptval/)
- JIS Q 27002:2006：情報技術－セキュリティ技術－情報セキュリティマネジメント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）
- 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）
- 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）

1.2 文書の名前と識別

本ポリシの名称を「保健医療福祉分野 PKI 認証局　認証用（組織）証明書ポリシ」とする。本ポリシにて発行する証明書及び関連サービスに、厚生労働省より「保健医療福祉分野の公開鍵関連分野」のオブジェクト識別子（OID）を「1.2.392.100495.1」と割り当てる。その基本体系を示す。

OID の基本体系

{ iso(1) member-body(2) jp(392) mhlw(100495) jhpki(1) ca(5) A B C V}

A：証明書ポリシ　cp（1）

B：認証局の証明書種類　signature(1), authentication for individual(2), authentication for organization(3)

C：セキュリティ保証レベル（n）　n=0, 1, 2, 3, 4　（0 はテスト用、3 は HPKI の業務用）

V：証明書ポリシのメジャーバージョン番号　v(1)

また、本 CP で定める OID を表 1.2 に示す。

表 1.2　本 CP で定める OID

名称	オブジェクト識別子
HPKI 署名用証明書ポリシ	1.2.392.100495.1.5.1.1.3.1
HPKI 認証用証明書ポリシ（人）	1.2.392.100495.1.5.1.2.3.1
HPKI 認証用証明証ポリシ（組織）	1.2.392.100495.1.5.1.3.3.1
HPKI 署名テスト用証明書ポリシ	1.2.392.100495.1.5.1.1.0.1
HPKI 認証テスト用証明書ポリシ（人）	1.2.392.100495.1.5.1.2.0.1
HPKI 認証テスト用証明書ポリシ（組織）	1.2.392.100495.1.5.1.3.0.1

1.3　PKI の関係者

1.3.1　認証局

認証局（CA）は、証明書発行局（IA)と登録局（RA）により構成される。保健医療福祉分野 PKI では、認証局は複数の階層構成をとることができる。また、保健医療福祉分野 PKI の階層構成の頂点の認証局（Root CA）は、本 CP に準拠する他の保健医療福祉分野 PKI の Root CA と相互認証を行うことがある。

発行局は証明書の作成、発行、失効及び失効情報の開示及び保管の各業務を行う。

但し、認証局は認証局の運営主体で定める CPS の遵守及び個人情報の厳正な取り扱いを条件に、契約を取り交わすことで業務の一部又は全部を外部に委託することができる。

1.3.2　登録局

登録局は、適切な申請者の本人確認、登録の業務を行い、発行局への証明書発行要求を行う。なお、証明書登録の業務は、発行、失効を含む。

但し、登録局は認証局の運営主体で定める CPS の遵守及び個人情報の厳正な取り扱いを条件に、契約を取り交わすことで業務の一部を外部に委託することができる。

1.3.3　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組織をさす。証明書所有者の範囲は次のとおりとする。

・ 医療機関等の保健医療福祉分野サービスの提供者及び利用者

1.3.4　検証者

デジタル署名を公開鍵証明書の公開鍵で検証するモノ。

1.3.5　その他の関係者

規定しない。

1.4　証明書の使用方法

1.4.1　適切な証明書の使用

本 CP で定める加入者証明書は、次に定める利用目的にのみ使用できる。

(1)　医療機関等の保健医療福祉分野サービス提供組織の認証用
(2)　保険者等の保健医療福祉分野サービス利用組織の認証用
(3)　保健医療福祉分野サービス提供者もしくは利用者が所有もしくは管理する機器の認証用
(4)　保健医療福祉分野サービス提供者もしくは利用者が所有もしくは管理するアプリケーションの認証用

1.4.2　禁止される証明書の使用

本 CP で定める加入者証明書は、認証用途以外には用いないものとする。

1.5　ポリシ管理

1.5.1　本ポリシを管理する組織

本 CP の管理組織は、「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）とする。

1.5.2　問い合わせ先

本 CP 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：厚生労働省　医政局　政策医療課　医療技術情報推進室
受付時間：10 時～17 時（平日）
電話番号：03-3595-3412
FAX 番号：03-3501-5712
e-mail アドレス：hpki-cp@mhlw.go.jp

1.5.3　CPS のポリシ適合性を決定する者

CPS の本 CP への適合性を決定する者は、HPKI 認証局専門家会議とする。

1.5.4　CPS 承認手続き

本 CP は、HPKI 認証局専門家会議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、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又はソフトウェアのモジュール。

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

・ オブジェクト識別子 (Object Identifier)
オブジェクトの識別を行うため、オブジェクトに関連付けられた一意な値。

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

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

・ 鍵の預託 (Key Escrow)

第三者機関に鍵を預託すること。

・ 鍵ペア (Key Pair)
私有鍵とそれに対応する公開鍵の対。

・ 加入者 (Subscriber)
認証局から認証のための電子証明書を発行される者。

・ 加入者証明書
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)
デジタル署名を公開鍵証明書の公開鍵で検証するモノ。

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

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

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

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

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

・ 証明書失効リスト（Certificate Revocation List、Authority Revocation List）
失効した電子証明書のリスト。
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（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。

・ 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ざん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。

・ 認証実施規程（Certification Practice Statement：CPS）
証明書ポリシに基づいた認証局運用についての規定集。認証局が電子証明書を発行するときに採用する実践に関する表明として位置付けられる。

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

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

・ 発行局（Issuer Authority）
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加入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。

（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。

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

・ CPS（Certification Practice Statement）
認証実施規程を参照のこと。

・ 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）
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

認証局は、以下の情報を検証者と加入者が入手可能にする。

＜検証者に公開する事項＞

- CA の公開鍵証明書
- 本 CP
- CRL/ARL
- 検証者の表明保証に関する文書

＜加入者に公開する事項＞

- 認証局の定める CPS
- 認証局の定める加入者に関する各種規定/基準

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 CP「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

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は、加入者及び検証者に対しては読み取り専用として公開する。

3　識別及び認証

3.1　名称決定

3.1.1　名称の種類

本 CP 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。保健医療福祉分野 PKI では、C は JP とする。また CommonName は必須で、加入者の組織名称（英語表記若しくはローマ字表記）を記載する。

3.1.2　名称が意味を持つことの必要性

本 CP 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

規定しない。

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 CP「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

認証局が発行する電子証明書の加入者名（subjectDN）は、認証局内で一意にするためにシリアル番号（SN）を含むことができる。また、認証局の名称（issuerDN）は、保健医療福祉分野 PKI 内で、ある特定の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

申請者が生成した鍵ペアの公開鍵を提示して認証局に対し証明書発行要求を行う際、公開鍵証明書と私有鍵との対応を証明するために、認証局からのチャレンジに署名を行い、私有鍵の所有を証明するものとする。あるいは申請者が提出した証明書発行要求（CSR）の署名検証等により、私有鍵の所有を確認するものとする。

認証局側で申請者の鍵ペアを生成する場合はこの限りではない。

3.2.2 組織の認証

保健医療福祉分野 PKI 認証局に保険医療機関等の組織の証明書を申請する際は、証明書の発行に先立ち、次のいずれかの方法で組織の実在性及び保険医療機関等であること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「3.2.3 個人の認証」に定める方法による。

・ 法人組織の場合

商業登記簿謄本、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、各法等で提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。

・ 個人事業者の場合

商業登記簿謄本、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。

・ 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。

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も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。

この場合、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。

・ 法令等の要請により発行する場合

保健医療福祉分野 PKI 認証局が法令等の要請により、保険医療機関等の組織の証明書を発行する際は、法令で定められた機関が保険医療機関等の確認を実施し、その結果を登録局に提示することで組織の認証を実施しなくてはならない。

3.2.3 個人の認証

保健医療福祉分野 PKI 認証局に証明書を申請しようとする際は、証明書の発行に先立ち、次のいずれかの方法で、組織管理者の実在性並びに申請者の実在性、組織所属の事実、組織の証明書申請意思を登録局に立証しなくてはならない。また、組織から委任を受けた者（以下、代理人）が申請する場合は、組織所属の事実に代えて組織からの申請委任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、登録局が証明書を発行する場合は、本節の規定に従い申請者の立証を行わせ、4 章の規定に則り申請者の審査

及び証明書の発行を実施する。

・ 組織管理者もしくは組織所属者が申請する場合

＜持参の場合＞

1. 組織管理者の実在性

「3.2.2　組織の認証」において、立証書類に組織管理者の氏名が記載されている書類を提出することで、組織管理者の実在性の立証に代えることができる。

2. 申請者の実在性

証明書を申請しようとする者は、認証局の定める申請書類に、最低限、「申請者個人の氏名、所属組織の住所、所属組織の電話番号」を記入し、登録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。

3. 申請者の組織所属の事実

証明書を申請しようとする者は、当該組織の管理者の印が押印されている申請者の氏名が記載された申請書類を登録局の窓口に提出することで組織に所属していることの事実を立証しなくてはならない。

なお、申請書類の様式については、各認証局が定めることとする。

4. 組織の証明書申請の意思

申請者が登録局の窓口に各種の書類を持参して申請する場合は、組織管理者の実在性、申請者の実在性及び組織所属の事実の立証を行えば、申請意思の立証がなされたものとみなす。

＜郵送の場合＞

1. 組織管理者の実在性

「3.2.2　組織の認証」において、立証書類に組織管理者の氏名が記載されている書類を提出することで、組織管理者の実在性の立証に代えることができる。

2. 申請者の実在性

証明書を申請しようとする者は、認証局の定める申請書類に、最低限、「申請者個人の氏名、所属組織の住所、所属組織の電話番号」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。

3. 申請者の組織所属の事実

証明書を申請しようとする者は、当該組織の管理者の印が押印されている申請

者の氏名が記載された各認証局で定める申請書類を登録局に郵送することで組織に所属していることの事実を立証しなくてはならない。

4. 組織の証明書申請の意思

申請者が「3.2.2　組織の認証」で定める各種の書類と合わせて、各認証局で定める申請書類に当該組織の管理者の印が押印されている書類を郵送することにより、申請意思の立証がなされたものとみなす。

＜オンラインの場合＞

1. 組織管理者の実在性

「3.2.2　組織の認証」に定める、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、組織管理者の実在性の立証に代えることができる。

ただし、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以外を用いる場合は、別途、保険医療機関等であることを立証する書類を認証局が定める方法により提出しなくてはならない。

2. 申請者の実在性、組織所属の事実、組織の証明書申請の意思

証明書を申請しようとする者は、認証局の定める手続きに従い、保健医療福祉分野 PKI 認証局の発行する管理者向け署名用証明書を用いた電子署名により、申請者の実在性、組織所属の事実及び組織の証明書申請の意思を立証しなくてはならない。

なお、保健医療福祉分野 PKI 認証局の管理者向け署名用証明書は組織の管理責任者に発行され、当該証明書による電子署名は、本人に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す。

・ 代理人が申請する場合

＜持参の場合＞

1. 組織管理者の実在性

「3.2.2　組織の認証」において、立証書類に組織管理者の氏名が記載されている書類を提出することで、組織管理者の実在性の立証に代えることができる。

2. 代理人の実在性

代理人が証明書を申請しようとする際は、各認証局が定める申請書類に、最低限、代理人の「氏名、生年月日、性別、住所、連絡先電話番号」が記入された書