保健医療福祉分野 PKI 認証局
認証用（人）証明書ポリシ
1.2 版

平成２６年３月

厚生労働省

（C）　Ministry of Health, Labour and Welfare

改定履歴

版数	日付	内容
初版	平成 21 年 11 月	初版発行
1.1 版	平成 22 年 3 月	「保健医療福祉分野 PKI 認証局署名用証明書ポリシ」に合わせ、所要の改定を実施した。
1.2 版	平成 26 年 3 月	「保健医療福祉分野 PKI 認証局署名用証明書ポリシ」に合わせ、所要の改定を実施した。

－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.....4
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
3.2.3　個人の認証 14
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 18
3.4　失効申請時の本人性確認及び認証 18
4　証明書のライフサイクルに対する運用上の要件 19
4.1　証明書申請 19
4.1.1　証明書の申請者 19
4.1.2　申請手続及び責任 19
4.2　証明書申請手続き 20
4.2.1　本人性及び資格確認 20
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 25
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 25
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 26
4.7　証明書の鍵更新（鍵更新を伴う証明書更新） 26
4.7.1　証明書鍵更新の要件 26
4.7.2　鍵更新申請者 26
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 27
4.8.5　変更された証明書の受理 27
4.8.6　認証局による変更証明書の公開 27
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 28
4.9.3　失効申請の処理手順 28
4.9.4　失効における猶予期間 29
4.9.5　認証局による失効申請の処理期間 29
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 30
4.9.10　オンラインでの失効確認要件 30
4.9.11　その他利用可能な失効情報確認手段 30
4.9.12　鍵の危殆化に関する特別な要件 30
4.9.13　証明書一時停止の要件 30
4.9.14　一時停止申請者 30
4.9.15　一時停止申請の処理手順 30
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 31
4.12　私有鍵預託と鍵回復 31
4.12.1　預託と鍵回復ポリシ及び実施 31
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 31
5　建物・関連設備、運用のセキュリティ管理 32
5.1　建物及び物理的管理 32
5.1.1　施設の位置と建物構造 32
5.1.2　物理的アクセス 32
5.1.3　電源及び空調設備 32
5.1.4　水害及び地震対策 32
5.1.5　防火設備 33
5.1.6　記録媒体 33
5.1.7　廃棄物の処理 33
5.1.8　施設外のバックアップ 33
5.2　手続的管理 33
5.2.1　信頼すべき役割 33
5.2.2　職務ごとに必要とされる人数 33
5.2.3　個々の役割に対する本人性確認と認証 33
5.2.4　職務分轄が必要になる役割 34
5.3　要員管理 34
5.3.1　資格、経験及び身分証明の要件 34
5.3.2　経歴の調査手続 34
5.3.3　研修要件 34
5.3.4　再研修の頻度及び要件 34
5.3.5　職務のローテーションの頻度及び要件 34
5.3.6　認められていない行動に対する制裁 35
5.3.7　独立した契約者の要件 35
5.3.8　要員へ提供する資料 35
5.4　監査ログの取扱い 35
5.4.1　記録するイベントの種類 35
5.4.2　監査ログを処理する頻度 35
5.4.3　監査ログを保存する期間 35
5.4.4　監査ログの保護 35
5.4.5　監査ログのバックアップ手続 35

5.4.6　監査ログの収集システム（内部対外部） 36
5.4.7　イベントを起こしたサブジェクトへの通知 36
5.4.8　脆弱性評価 36
5.5　記録の保管 36
5.5.1　アーカイブ記録の種類 36
5.5.2　アーカイブを保存する期間 36
5.5.3　アーカイブの保護 36
5.5.4　アーカイブのバックアップ手続 36
5.5.5　記録にタイムスタンプをつける要件 37
5.5.6　アーカイブ収集システム（内部対外部） 37
5.5.7　アーカイブ情報を入手し、検証する手続 37
5.6　鍵の切り替え 37
5.7　危殆化及び災害からの復旧 37
5.7.1　災害及び CA 私有鍵危殆化からの復旧手続き 37
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 37
5.7.3　CA 私有鍵が危殆化した場合の対処 37
5.7.4　災害等発生後の事業継続性 38
5.8　認証局又は登録局の終了 38

6　技術的なセキュリティ管理 39

6.1　鍵ペアの生成と実装 39
6.1.1　鍵ペアの生成 39
6.1.2　加入者への私有鍵の送付 39
6.1.3　認証局への公開鍵の送付 39
6.1.4　検証者への CA 公開鍵の配付 39
6.1.5　鍵のサイズ 39
6.1.6　公開鍵のパラメータ生成及び品質検査 39
6.1.7　鍵の利用目的 40
6.2　私有鍵の保護及び暗号モジュール技術の管理 40
6.2.1　暗号モジュールの標準及び管理 40
6.2.2　私有鍵の複数人によるコントロール 40
6.2.3　私有鍵のエスクロウ 40
6.2.4　私有鍵のバックアップ 40
6.2.5　私有鍵のアーカイブ 40
6.2.6　暗号モジュールへの私有鍵の格納と取り出し 40
6.2.7　暗号モジュールへの私有鍵の格納 41
6.2.8　私有鍵の活性化方法 41

6.2.9　私有鍵の非活性化方法 41
6.2.10　私有鍵の廃棄方法 41
6.2.11　暗号モジュールの評価 41
6.3　鍵ペア管理に関するその他の面 41
6.3.1　公開鍵のアーカイブ 41
6.3.2　公開鍵証明書の有効期間と鍵ペアの使用期間 41
6.4　活性化用データ 42
6.4.1　活性化データの生成とインストール 42
6.4.2　活性化データの保護 42
6.4.3　活性化データのその他の要件 42
6.5　コンピュータのセキュリティ管理 42
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 42
6.5.2　コンピュータセキュリティ評価 43
6.6　ライフサイクルの技術的管理 43
6.6.1　システム開発管理 43
6.6.2　セキュリティ運用管理 43
6.6.3　ライフサイクルのセキュリティ管理 43
6.7　ネットワークのセキュリティ管理 43
6.8　タイムスタンプ 43

7　証明書及び失効リスト及び OCSP のプロファイル 44

7.1　証明書のプロファイル 44
7.1.1　バージョン番号 44
7.1.2　証明書の拡張（保健医療福祉分野の属性を含む） 44
7.1.3　アルゴリズムオブジェクト識別子 44
7.1.4　名称の形式 44
7.1.5　名称制約 44
7.1.6　CP オブジェクト識別子 45
7.1.7　ポリシ制約拡張 45
7.1.8　ポリシ修飾子の構文及び意味 45
7.1.9　証明書ポリシ拡張フィールドの扱い 45
7.1.10　保健医療福祉分野の属性（hcRole） 48
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 61
9.7　無保証 62
9.8　責任制限 62
9.9　補償 62
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 63
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 64
9.16.1　完全合意条項 64
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、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 2 7 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（人）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（人）証明書ポリシ	1.2.392.100495.1.5.1.2.3.1
HPKI 認証用（組織）証明書ポリシ	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（人）証明書ポリシ	1.2.392.100495.1.5.1.2.0.1
HPKI 認証テスト用（組織）証明書ポリシ	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 のルート CA（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個人をさす。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

1.3.4　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）　医療従事者等の保健医療福祉分野サービス提供者の認証用

（2）　患者等の保健医療福祉分野サービス利用者の認証用

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　政策統括官付　情報政策担当参事官室

受付時間：10 時～17 時（平日）

電話番号：03-3595-2314

FAX 番号：03-3595-2198

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）
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（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。

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

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。

・ 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。

・ 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。

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くてはならない。また、国家資格を有する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、登録局が証明書を発行申請する場合は、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。

＜持参の場合＞

1. 個人の実在性

証明書を申請しようとする個人は、住民票の写しに添えて、認証局の定める申請書類に当該個人の「氏名、生年月日、性別、住所」（以下、基本 4 情報という）を記入し、登録局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

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、本 CP では、1 点若しくは 2 点で本人性の確認が可能な書類のリストを記載するものであり、本人性確認に必要な書類については、各認証局がリストから選択し、CPS で定めることとする。

【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
・船員手帳	（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、又は 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） ・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又は非課税証明書 （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. 個人の証明書申請の意思

本人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、実在性及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、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登録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。

＜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、住民票の写しに添えて、認証局の定める申請書類に当該個人の基本 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、次に挙げる書類のいずれか 1 点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、本 CP では、郵送する場合に本人性の確認が可能な書類のリストを記載するものであり、本人性確認に必要な書類については、各認証局がリストから選択し、CPS で定めることとする。

【本人性確認のために必要な書類】

・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
・船員手帳	（張り替え防止措置済みの写真付）
・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	・基礎年金番号通知書

3. 個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、認証局の定める書類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保有の事実を立証しなくてはならない。

この時、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。

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」で提出した書類又は認証局で作成された記録を再び参照するか、加入者の署名を提示することで行える。

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

3.3.2　証明書失効後の鍵更新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。
3. 申請書に認証局が検証可能な電子署名を付して認証局に送信する。電子署名付きの申請ができない場合は、他の手段を用い加入者本人であることを立証する。

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

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若しくはその代理人、保健医療福祉分野のサービス利用者本人若しくはその代理人とする。

2. 国家資格保有者証明書

　国家資格保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を有する者本人若しくはその代理人とする。

3. 医療機関等の管理者証明書

　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若しくはその代理人とする。

本 CP に則り発行される証明書は、それ以外からの申請は受け付けない。

4.1.2　申請手続及び責任

　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きによって証明書の利用申請を行う。

1. 持参

　本人若しくは代理人が登録局に「3.2.3　個人の認証」及び認証局の定める書類を持参することにより利用申請を行う。

　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本 CP「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

　本人が登録局に「3.2.3　個人の認証」及び認証局が定める書類を郵送することにより利用申請を行う。

　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。

3. オンライン

本人若しくは代理人が登録局にオンラインで「3.2.3　個人の認証」及び認証局の定めるデータを送付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には、必要なデータに加え、本人による委任及び本CP「3.2.3 本人の認証」に準じた代理人の本人性が識別可能な措置を講じるものとする。

また、証明書の利用申請者は、申請にあたり、本 CP「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 CP に則り運営される、各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、それらに同意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。なお、オンラインによる場合は、全ての確認手順に渡り電子的手法により実施され、認証局が公的個人認証サービス、署名用保健医療福祉分野 PKI、若しくはそれに準じたサービスを利用することを想定したものであり、本 CP 作成時点で実現できていない項目も含まれる。その場合、他の方法との組み合わせにより、確実な本人性、実在性、申請意思及び資格確認を実施しなくてはならない。

＜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 CP「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

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。

なお、確認に用いた証明書等は登録局でコピーを取り、保存年限を定めて保存しておくものとする。

(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。

この時、申請者本人が登録局に出頭する場合は、電子証明書若しくは電子証明書を生成する符号を、窓口で交付することにより実在性の確認を実施する。郵送で交付する場合は、電子証明書若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、登録局で保存年限を定めて保存しておくものとする。

(3) オンラインの場合

登録局から当該申請者の電子署名の有効性の確認を実施する。

なお、確認に用いた電子署名の付与された申請書は、登録局で保存年限を定めて保存しておくものとする。

2. 国家資格を有する者への証明書発行

認証局は、国家資格を有する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保有の確認を行う。

(1) 持参の場合

官公庁の発行した国家資格免許証等の原本を要求し、対面により国家資格保有の有無を確認する。この時、国家資格発行機関若しくはそれに代わる台帳を備えた機関が、認証局の定める証明書発行期間に十分足る期間内に資格保有の有無の回答を実施している場合は、登録局から資格保有の問い合わせを実施し回答を得ることが望ましい。

なお、資格確認を実施した国家資格免許証等は登録局でコピーを取り、保存年限を定めて保存しておくものとする。

(2) 郵送の場合

官公庁の発行した国家資格免許証等のコピーの郵送を要求し、国家資格保有の有無を確認する。

国家資格免許証等の郵送にあたっては、当該国家資格証明書のコピーの適当な空欄に実印を捺印させ、印鑑登録証明書を添えさせるものとする。

この時、国家資格発行機関若しくはそれに代わる台帳を備えた機関が、認証局の定める証明書発行期間に十分足る期間内に資格保有の有無の回答を

実施している場合は、登録局から資格保有の問い合わせを実施し回答を得ることが望ましい。

なお、確認に用いた証明書等は、登録局で保存年限を定めて保存しておくものとする。

(3) オンラインの場合

登録局からオンラインにより国家資格発行機関若しくはそれに代わる台帳を備えた機関に問い合わせを実施して、国家資格発行機関から申請者の国家資格保持の有無について回答を得る。

国家資格発行機関等によりオンラインの資格確認手段が提供されていない場合は、持参若しくは郵送と同等の資格確認を実施する。

なお、確認に用いた証明書等は、登録局で保存年限を定めて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、少なくとも電話帳などの第 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。オンラインの場合は、「(2) オンラインの場合」に定める方法に従う。

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。

また、確認内容の内、保険医療機関等であることの確認は、地方厚生局が所管し公開している、全保険医療機関・保険薬局一覧等を用いて確認することも可能である。

もしくは、登録局から上記で定める全ての確認手段と同等の信頼のおける台帳やデータベースを保有している機関に問合せをすることが可能な場合は、それを用いて確認をしてもよい。

(1) 持参若しくは郵送の場合

申請時に持参若しくは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登録局でコピーを取り、保存年限を定めて保存しておくものとする。

(2) オンラインの場合

「3.2.2 組織の認証」で定める書類に相当する電子書類の送付を求めると共に、当該書類に管理者による公的個人認証サービス若しくは署名用保健医療福祉分野 PKI 認証局の証明書を利用した電子署名が付されていることを確認する。

申請者が管理者であること及び組織の実在性の確認については、持参若しくは郵送と同等の確認を実施する。例えば、署名用保健医療福祉分野PKI認証局の組織管理者証明書や法務省の運営する「商業登記に基づく電子認証制度」を利用することで申請者が管理者であること及び組織の実在性の確認が行える場合にはこれを利用してもよい。

なお、確認に用いた証明書等は、登録局で保存年限を定めて保存しておくものとする。

＜代理人からの申請の場合＞

認証局は、代理人からの申請の場合、申請者本人の本人性、実在性、申請意思及び資格の確認、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

認証局は、代理人に「3.2.3 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。

この場合も、1 点の書類で確認できる場合と 2 点の書類で確認が必要な場合があり、必要な書類については、「3.2.3 個人の認証」と同様に、各認証局が選択し、CPS で定めることとする。

2. 郵送の場合

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

認証局は、電子的に作成された代理人申請書など、認証局が定める書類に付された公的個人認証サービス、署名用保健医療福祉分野 PKI 等を利用した申請者の電子署名の有効性を確認することにより代理人の本人性の確認を実施する。

＜登録局の審査業務の一部を委託して発行する場合＞

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

この場合、本 CP 若しくは認証局で定める CPS に則った組織の実在性及び保険医療機関等の確認を当該団体の管理者の責任のもと実施しなくてはならない。

また、認証局と当該団体の間で委託に係わる契約を取り交わし、委託された業務に関して登録局に課せられると同等の業務内容、責任及び義務を負うことを定めておかなくてはならない。

4.2.2　証明書申請の承認又は却下

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

4.2.3　証明書申請手続き期間

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

4.3　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＞

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 条第三号に準じて CPS 及び事務取扱要領を規定し、運用する。

CPS 及び事務取扱要領の規定としては、最低限以下の項目を含めるものとする。

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

2. 加入者鍵ペアの転送や出力を行う場合も、十分なセキュリティ対策を講じていること。
   また、加入者鍵ペアを転送、出力した後は、速やかに加入者鍵ペアを完全に廃棄若しくは消去すること。

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

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

＜加入者が鍵ペアを生成する場合＞

加入者が鍵ペアを生成し、電気通信回線を通じて受信する場合は、「電子署名及び認証業務に関する法律施行規則」第 6 条第三号の二に基づく CPS 及び事務取扱要領を規定し、運用する。

CPS 及び事務取扱要領の規定としては、最低限以下の項目を含めるものとする。

1. 認証局は、加入者を一意に識別できる識別符号を生成する。また、識別符号は、容易に類推できないものでなくてはならない。

2. 加入者の識別符号は、一度利用した後、それ以降の識別処理に用いられないような措置を講じていること。

3. 加入者の識別符号は、生成した後、加入者以外の第 3 者に渡らないよう安全に交付すること。

4.3.2　証明書発行後の通知

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

4.4　証明書の受理

4.4.1　証明書の受理

認証局は、電子証明書を交付した後、受領した旨を確認しなければならない。

なお、認証局は、証明書を交付してから一定の期間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

認証局は、加入者の認証用証明書の公開を行わない。

4.4.3　他のエンティティに対する認証局による証明書発行通知

規定しない。

4.5　鍵ペアと証明書の利用目的

4.5.1　加入者の私有鍵と証明書の利用目的

加入者は、私有鍵を認証用途にのみ利用する。

4.5.2　検証者の公開鍵と証明書の利用目的

検証者は、加入者の認証用途で公開鍵と証明書を利用する。

4.6　証明書更新

4.6.1　証明書更新の要件

本 CP に則り認証局から発行される証明書は、証明書更新は行わない。

4.6.2　証明書の更新申請者

規定しない。

4.6.3　証明書更新の処理手順

規定しない。

4.6.4　加入者への新証明書発行通知

規定しない。

4.6.5　更新された証明書の受理

規定しない。

4.6.6　認証局による更新証明書の公開

規定しない。

4.6.7　他のエンティティへの証明書発行通知

規定しない。

4.7　証明書の鍵更新（鍵更新を伴う証明書更新）

4.7.1　証明書鍵更新の要件

本 CP に則り認証局から発行される証明書は、証明書鍵変更を行わない。

4.7.2　鍵更新申請者

規定しない。

4.7.3　鍵更新申請の処理手順

規定しない。

4.7.4　加入者への新証明書発行通知

規定しない。

4.7.5　鍵更新された証明書の受理

規定しない。

4.7.6　認証局による鍵更新証明書の公開

規定しない。

4.7.7　他のエンティティへの証明書発行通知

規定しない。

4.8　証明書変更

4.8.1　証明書変更の要件

本 CP に則り認証局から発行される証明書は、証明書変更を行わない。

4.8.2　証明書の変更申請者

規定しない。

4.8.3　証明書変更の処理手順

規定しない。

4.8.4　加入者への新証明書発行通知

規定しない。

4.8.5　変更された証明書の受理

規定しない。

4.8.6　認証局による変更証明書の公開

規定しない。

4.8.7　他のエンティティへの証明書発行通知

規定しない。

4.9　証明書の失効と一時停止

4.9.1　証明書失効の要件

認証局は、次の場合に証明書を失効するものとする。

＜加入者若しくはその代理人から失効申請があった場合＞

加入者若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、本 CP、認証局の定める 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。
- 証明書に含まれる該当の情報が正確でなくなった場合。（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）。
- 本 CP 又は認証局が定める CPS 若しく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認証局が判断した場合。
- 加入者の特定ができない場合で、緊急に失効させる必要があると認証局が判断した場合。

4.9.2　失効申請者

認証局は、次の 1 人又はそれ以上の者からの失効申請を受け付ける。

1. 本人の名前で証明書が発行された加入者若しくはその代理人
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。

上記それぞれの確認と共に、証明書の失効理由を確認し、その真偽についても確認を実施しなくてはならない。

この手順により証明書の失効を実施した場合は、CRL を発行する。また、証明書の失効の事実を認証局の定める方法により申請者に通知しなくてはならない。

＜認証局の職員からの失効申請の場合＞

認証局は「4.9.1 証明書失効の要件」の中の認証局の職員から失効申請があった場合は、速やかに当該証明書を特定し、失効の事由の真偽の確認を実施しなくてはならない。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なくてはならない。

証明書の失効を実施した場合は、CRL を発行する。また、証明書の失効の事実を認証局の定める方法により申請者に通知しなくてはならない。

4.9.4　失効における猶予期間

「4.9.1 証明書失効の要件」に規定されている事由が発生した場合には、速やかに失効申請を行わなければならない。その期限は CPS に定めるものとする。

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、受領後直ちに開始されるものとする。

その期限はCPSに定めるものとする。

4.9.6　検証者の失効情報確認の要件

検証者は、認証者の公開鍵を使う時に有効なCRL/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。

4.9.7　CRL発行頻度

変更がない場合においても、48時間以内に96時間以内の有効期限のCRLを発行する。この具体的な頻度と有効期限はCPSで規定するものとする。

失効の通知は直ちに公開する。CRLに変更があった場合はいつでも更新する。また、認証局私有鍵（以下、CA私有鍵という）、加入者の私有鍵の危殆化等が発生した場合は、CRLを直ちに発行するものとする。

4.9.8　CRLが公開されない最大期間

CRLは発行後24時間以内に公開される。

4.9.9　オンラインでの失効／ステータス情報の入手方法

規定しない。

4.9.10　オンラインでの失効確認要件

規定しない。

4.9.11　その他利用可能な失効情報確認手段

使用しない。

4.9.12　鍵の危殆化に関する特別な要件

認証局は、CA署名鍵の危殆化の際には関連組織に直ちに通知するものとする。

4.9.13　証明書一時停止の要件

一時停止は行わない。

4.9.14　一時停止申請者

一時停止は行わない。

4.9.15　一時停止申請の処理手順

一時停止は行わない。

4.9.16　一時停止期間の制限

一時停止は行わない。

4.10　証明書ステータスの確認サービス

4.10.1　運用上の特徴

規定しない。

4.10.2　サービスの利用可能性

規定しない。

4.10.3　オプショナルな仕様

規定しない。

4.11　加入の終了

加入者が、証明書の利用を終了する場合、本 CP「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

私有鍵は、特に法律によって必要とされる場合を除き、預託及び回復を行わない。

4.12.1　預託と鍵回復ポリシ及び実施

規定しない。

4.12.2　セッションキーのカプセル化と鍵回復のポリシ及び実施

規定しない。

5　建物・関連設備、運用のセキュリティ管理

これらは、JIS Q 27002:2006 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　建物及び物理的管理

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、かつ建物構造上、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こと。

5.1.2　物理的アクセス

認証局を運用する施設は認証業務用設備の所在を示す掲示がされていないこと。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こと。入退出者の本人確認は CPS で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。

認証設備室への立入は、立入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、立入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、立入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が講じられていること。

5.1.3　電源及び空調設備

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が講じられていることとする。

また、空調設備により、機器が適切に動作する措置が講じられていることとする。

5.1.4　水害及び地震対策

水害の防止のための措置が講じられていることとする。

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や、その他の耐震措置が講じられていることとする。

5.1.5　防火設備

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、認証局の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、所定の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ことが望ましい。

5.2　手続的管理

手続的管理は、JIS Q 27002:2006 と同等以上の規格に従うものとする。例えば、JIS Q 27002:2006 の「第 10 章 通信及び運用管理」がこれに相当する。

5.2.1　信頼すべき役割

証明書の登録、発行、取消等の業務及び関連する業務に携わる者には、CA システムの設定や CA 私有鍵の活性化等を担当する「CA システム管理者」、加入者証明書の発行・失効を担当する「登録局管理者」、及び「監査者」などがあり、本 CP 上信頼される役割を担っている。認証局においては、業務上の役割を特定の個人に集中させず、前述のように複数の役割に権限を分離した上、個人が複数の役割を兼任することは避けること。

5.2.2　職務ごとに必要とされる人数

CA システムへの物理的又は論理的に単独でのアクセスを避けることができるような必要人数を定めること。

5.2.3　個々の役割に対する本人性確認と認証

認証局システム、登録局システムへアクセスし、CA 私有鍵の操作や証明書発行、失効に係わる操作等の重要操作を行う権限者は、認証局運営責任者により任命されること。

また、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、本人しか持ち得ない権限者の私有鍵等を用いた強固な認証方式を採用すること。

5.2.4　職務分轄が必要になる役割

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こと。

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。

なお、要員管理は、JIS Q 27002:2006 と同等以上の規格に従うものとする。例えば、JIS Q 27002:2006 の「第 8 章　人的資源のセキュリティ」等がこれに相当する。

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、認証局運営組織の規則の要求に従って、任命時及び定期的に検証すること。

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なければならない。

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

セキュリティ監査手続きは、JIS Q 27002:2006 と同等以上の規格に従うものとする。例えば、JIS Q 27002:2006 の「第 10 章　通信及び運用管理」、「第 11 章　アクセス制御」、「第 12 章　情報システムの取得、開発及び保守」、「第 15 章　順守」等がこれに相当する。

5.4.1　記録するイベントの種類

認証局は、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出来る。

5.4.2　監査ログを処理する頻度

認証局は、監査ログを 3 ヶ月に 1 度以上定期的に検査する。

5.4.3　監査ログを保存する期間

監査ログは、最低 10 年間保存される。

5.4.4　監査ログの保護

認証局は、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 CPS に定める頻度でバックアップが取られ、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（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

記録は、JIS Q 27002:2006 と同等以上の規格に従って保管されるものとする。

例えば、JIS Q 27002:2006 の「第 12 章　情報システムの取得、開発及び保守」、「第 15 章　順守」等がこれに相当する。

5.5.1　アーカイブ記録の種類

認証局 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最低 10 年間は保存する。

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、許可された者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

規定しない。

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

認証局は、定期的に CA 私有鍵の更新を行う。CA 私有鍵は、認証設備室内にて、複数人の立会いのもと、専用の暗号モジュール（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執り行われる。

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

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、バックアップ用のハードウェア、ソフトウェア、バックアップデータを用いて、速やかに復旧作業を行い、合理的期間内に認証局業務を再開する。また、障害発生時には、可能な限り速やかに、加入者、検証者に情報公開用 Web サイト等により通知する。

5.7.3　CA 私有鍵が危殆化した場合の対処

CA 私有鍵が危殆化又はそのおそれが生じた場合は、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、認証局で規定された手続きに基づき、全ての加入者証明書の失効を行い、CRL/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、認証局で規定された手続きに基づき、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

エンドエンティティの加入者の私有鍵が認証局で生成される場合は、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、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ができるものとする。

6.1.3　認証局への公開鍵の送付

エンドエンティティの加入者の公開鍵が加入者により生成される場合は、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、本ポリシを公開する機関のサイトで公開するものとする。

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 証明書の鍵の最小サイズは、RSA アルゴリズムの場合、2048 ビットとする。他のアルゴリズムを使用する CA 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。

エンドエンティティの証明書の鍵の最小サイズは、RSA アルゴリズム又は技術的に同等のアルゴリズムの場合、1024 ビットとする。他のアルゴリズムを使用するエンドエンティティ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、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。例えば、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うようにしたり、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たり分散させて保管するなどの方法がある。

6.2.5　私有鍵のアーカイブ

認証局は加入者の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、安全に格納することとする。例えば、認証設備室内にある暗号モジュール内に格納するなどの方法がある。

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 私有鍵の活性化の方法は、認証局室内において本 CP「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 CP「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 CP「6.2.2　私有鍵の複数人によるコントロール」と同じく、複数名の権限を有する者によって、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。

加入者私有鍵破棄手続きは、CPS 又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　暗号モジュールの評価

CA 私有鍵を格納する暗号モジュールは、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 CPS で定める期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　公開鍵証明書の有効期間と鍵ペアの使用期間

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

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 2 年を越えないものとし、その私有鍵の使用は 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。

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

認証局において用いられる CA 私有鍵の活性化データは、認証局で定められた規定に従い安全に保護される。

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 CP「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

ISO15408 を参考にセキュリティ基準を設ける等の対応を行い、客観的に評価を行うこと。

6.6　ライフサイクルの技術的管理

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 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

JIS Q 27002:2006「第 12 章　情報システムの取得、開発及び保守」と同等以上の規格に従うものとする。

6.6.2　セキュリティ運用管理

JIS Q 27002:2006「第 12 章　情報システムの取得、開発及び保守」、「第 13 章　情報セキュリティインシデントの管理」、「第 14 章　業務継続管理」と同等以上の規格に従うものとする。

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

JIS Q 27002:2006 と同等以上の規格に従うものとする。

例えば、JIS Q 27002:2006 の「第 10 章　通信及び運用管理　10.6　ネットワークセキュリティの管理」、「第 11 章　アクセス制御　11.4　ネットワークのアクセス制御」等がこれに相当する。

6.8　タイムスタンプ

認証設備は、アプリケーション等において正確な日付・時刻を使用することとする。例えば、NTP サービスや GPS、電波時計等による時刻同期が挙げられる。

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 CP 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、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。

本ポリシに従い発行される電子証明書のプロファイルは、基本領域のプロファイルを表 7.1.1 に示し、拡張領域のプロファイルを表 7.1.2 の通りとする。

なお、Issuer の DN は CPS 及びその他開示文書に記述されることとする。

7.1.1　バージョン番号

本ポリシ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（保健医療福祉分野の属性を含む）

本ポリシに従い発行される電子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。

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)
sha256WithRSAEncryption (1.2.840.113549.1.1.11)
sha384WithRSAEncryption (1.2.840.113549.1.1.12)
sha512WithRSAEncryption (1.2.840.113549.1.1.13)

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　名称の形式

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

7.1.5　名称制約

用いない。

7.1.6　CP 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

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　証明書のプロファイル（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	◎	
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	◎	認証局のポリシを示す文字列を記載する。（「HPKI-01-*-forAuthentication-forIndividual」とする。なお、文字列中の"01"は、本 CP の版数である"第 1.0 版"を示す。また、"*"は CA を唯一に識別できる文字列とする。）
Subject	◎	英数字のみ使用する。（CountryName、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（Extensions）参照

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

表 7.1.2　証明書のプロファイル（拡張領域 Extensions）

項目	設定	説明	Critical
authorityKeyIdentifier	◎		FALSE
subejctKeyIdentifier	◎		FALSE
KeyUsage	◎		TRUE
DigitalSignature	◎		-
NonRepudiation	×		-
KeyEncipherment	×		-
DataEncipherment	×		-
KeyAgreement	×		-
KeyCertSign	×		-
CRLSign	×		-
EncipherOnly	×		-
DeciphermentOnly	×		-
extendedKeyUsage	△		FALSE
privateKeyUsagePeriod	×		FALSE
certificatePolicies	◎		TRUE
policyMapping	×		FALSE
subjectAltName	△		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

表中の、「◎」は必須、「○」は場合により必須、「△」はオプション、「×」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

本ポリシでは、ISO IS 17090 で規定した hcRole 属性を下記に示すようにプロファイルして用いることにする。

subjectDirectoryAttributes の attrType には hcRole を表す OID {id-hcpki-at-healthcareactor} を設定する。

attrValue は HCActorData で、HCActor の codedData では codeValueData は用いず、codeDataFreeText を用いる。

本ポリシでは 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、表 7.1.3 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。

表 7.1.3　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
‘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 & 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

注）資格名のワード間の空白は一個の Space (x20)とする。

代表者としての認証を必要と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) HPKI hcRole 属性プロファイル

本 HPKI の CP では、ISO IS 17090 に定められた hcRole 属性の ASN.1 表記を以下のようにプロファイルする。

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

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

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

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

CodedData :: = SET {
   codingSchemeReference [0] OBJECT IDENTIFIER,
   -- Contains the ISO coding scheme Reference
   -- or local coding scheme reference achieving ISO 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。

＜参考＞

以下に、hcRole を含めた X.509 SubjectDirectoryAttributes 拡張を DER エンコードしたデータの ASN.1 構造をダンプした例を示す。

Medical Doctor の例

```
No Type Len Value
-----------------------------------------------------------------------
   0 30   61: SEQUENCE {-- SubjectDirectoryAttributes ext.extnValue contents
   2 06    3:   OBJECT IDENTIFIER subjectDirectoryAttributes (2 5 29 9)
   7 04   54:   OCTET STRING, encapsulates {
   9 30   52:     SEQUENCE {-- SubjectDirectoryAttributes
  11 30   50:       SEQUENCE {-- Attribute::hcRoleAttribute
  13 06    6:         OBJECT IDENTIFIER '1 0 17090 0 1'   -- OID::type
  21 31   40:         SET {-- SET of AttributeValue::values
  23 31   38:           SET {-- AttributeValue::HCActorData
  25 30   36:             SEQUENCE {-- HCActor
  27 A0   34:               [0] {-- HCActor
  29 31   32:                 SET {-- CodedData
  31 A0   12:                   [0] {-- codingSchemeReference: local coding scheme
  33 06   10:                     OBJECT IDENTIFIER '1 2 392 100495 1 6 1 1'
        :                       }
  45 A2   16:                   [2] {-- codeDataFreeText
  47 0C   14:                     UTF8String 'Medical Doctor'
        :                       }
        :                   }
        :                 }
        :               }
        :             }
        :           }
        :         }
        :       }
        :     }
        :   }
```

"--"以降はコメント

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。

基本領域のプロファイルは表 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は、以下の表 7.2.2 の通りとする。CRL 拡張領域のプロファイルは、以下の表 7.2.3 の通りとする。

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

表 7.2.1　証明書失効リストのプロファイル（CRL 基本領域）

フィールド	設定	説明
Version	◎	Ｖer2 とする。
Signature	◎	表 7.1.1 の Signature と同様とする。
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(固定)とする。
LocalityName	△	
OrganizationName	◎	
OrganizationUnitName	△	
CommonName	◎	認証局のポリシを示す文字列を記載する。
ThisUpdata	◎	
NextUpdate	◎	
RevokedCertificates	◎	
UserCertificate	◎	失効した証明書の serialNumber を記載。
RevocationDate	◎	失効日時を記載する。
CrlEntryExtensions	◎	拡張領域（crlEntryExtentions）参照
CrlExtentions	◎	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
（CRL エントリ拡張領 crlEntryExtentions）

フィールド	設定	説明	Critical
ReasonCode	◎		FALSE
HoldInstructionCode	×		FALSE
InvalidityDate	×		FALSE
CertificateIssure	×		TRUE

表 7.2.3　証明書失効リストのプロファイル
（CRL 拡張領域 crlExtentions）

フィールド	設定	説明	Critical
AuthorityKeyIdentifier	◎		FALSE
IssuerAltName	△		FALSE
CRLNumber	◎		FALSE
DeltaCRLIndicator	×		TRUE
IssueingDistributionPoint	○	分割 CRL を用いる場合は必須	TRUE
FreshesCRL	×		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

準拠性監査は、多くの PKI 相互運用性モデルの不可欠なコンポーネントである。本 CP に従って証明書を発行する認証局は、本 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ものとする。

8.1　監査頻度

認証局の準拠性監査は、1 年以下の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っている部門から独立した、適切な能力を有する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、認証局とは別個の組織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、被監査者と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、本 CP 及び関連する 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、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

各種の料金については、本 CP に従い運用される認証局が設定するものとし、本 CP では規定しない。

9.1.1　証明書の発行又は更新料

規定しない。

9.1.2　証明書へのアクセス料金

規定しない。

9.1.3　失効又はステータス情報へのアクセス料金

規定しない。

9.1.4　その他のサービスに対する料金

規定しない。

9.1.5　払い戻し指針

規定しない。

9.2　財務上の責任

本ＣＰに従い運用される認証局は、その継続的な運営に必要とされる十分な財務的基盤を維持しなくてはならない。

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 CP に従う認証局が保持する個人及び組織の情報は、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。

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。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 CP 「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

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

認証局における個人情報の取り扱いについては、各認証局の CPS で特定される「プライバシーポリシ」を適用するものとする。

9.4.2　プライバシーとして保護される情報

認証局は、次の情報を保護すべき個人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。

・ 公開鍵証明書
・ CRL に記載された情報

9.4.4 個人情報を保護する責任

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

認証局は、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、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、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

認証局と加入者との間で別段の合意がなされない限り、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：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
- CPS：認証局に帰属する財産（著作権を含む）である
- 本 CP：「HPKI 認証局専門家会議」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、本 CP 及び認証局の定める 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、本 CP の要件と認証局の定める CPS 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 CP 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。
- 認証局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 などの重要事項を認証局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。
- 認証局の定める方法で、CP に基づく加入者の権利と義務を各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 CP「5　建物・関連施設、運用のセキュリティ」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、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、加入者の名称（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

登録局は、認証局から独立して登録局を運営する場合、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。また、登録局は、認証局に代わって果たす行為について個別に責任を負う。

・ 証明書発行にあたり、申請内容の真偽の確認を確実に行い、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 CP「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 加入者の表明保証

本 CP 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妥当な措置を取ること。

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、認証局の定める CPS に従って速やかに届け出ること。

5. 利用規定の遵守責任

加入者は、本 CP 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 CP 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 CP 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行うこと。

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 CP「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 2 点の検証を実施することは HPKI 認証用証明書として重要である。
  - OID 及び Issuer の CN が HPKI の規定に一致していること
  - hcRole 及び keyUsage の DigitalSignature のみが有効と設定されていること

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 CP 「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 CP「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、認証局及び登録局の責任は、認証局及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 CP 「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又は取引上の債務等、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 CP 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、認証局で定める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　本ポリシの有効期間と終了

9.10.1　有効期間

本 CP 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 CP の終了まで有効であるものとする。

9.10.2　終了

本 CP 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

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した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

「HPKI 認証局専門家会議」が本 CP の改訂を行う場合は、改訂に先立ち、本 CP に関連する全ての認証局に通知を行い、意見を求める。

本 CP が変更された時は、「HPKI 認証局専門家会議」によって承認する。

9.12.2　通知方法と期間

本 CP 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生ずる。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 CP の変更があった場合には、本 CP 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

証明書の発行主体である、各認証局の CPS において定める。

9.14　準拠法

本 CP 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 CP 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 CP は、本 CP 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又は口頭による過去の一切の意思表示、合意又は表明事項に取って代わるものである。

9.16.2　権利譲渡条項

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

9.16.4　強制執行条項（弁護士費用及び権利放棄）

規定しない。

9.16.5　不可抗力

以下に例示されるような通常人の標準的な注意義務を尽くしても、予防・回避できない事象を不可抗力とする。不可抗力によって損害が発生した場合、本 CP「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 CP 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 CP を採用した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 CP の方針に同意し責任を持ち続けるものとする。