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）
  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。

・ 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。

・ 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。

・ 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。

・ 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

商業登記簿謄本、開設許可証のコピー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。

・ 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コピー、各法等で定められる掲示※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。

・ 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条及びその準用条項（掲示）

3.2.3 個人の認証

保健医療福祉分野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. 申請書に私有鍵で署名して認証局に送信する。
   私有鍵を含んでいるトークンが紛失又は盗まれた場合等で、加入者が電子署名付きの要求をできない場合は、他の何らか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「3.2.2　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。