類を提出することと併せて「3.代理人の本人性」に掲げる書類の原本を登録局の窓口に提示することで実在性の立証をしなくてはならない。

3. 代理人の本人性

代理人が証明書を申請しようとする際は、次に挙げる書類の原本を登録局の窓口に提示することで代理人の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	

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）

4. 代理人の組織管理者からの委任の事実

代理人が証明書を申請しようとする際は、当該組織管理者の署名捺印のある代理人の氏名が記載された委任状を登録局の窓口に提出することで組織管理者からの委任の事実を立証しなくてはならない。

なお、委任状の様式については、各認証局が定めることとする。

5. 組織の証明書申請の意思

代理人が登録局の窓口に 1 から 4 で定める各種の書類を持参して申請する場合は、組織の申請意思の立証がなされたものとみなす。

＜郵送の場合＞

代理人による郵送での申請は認めない。

＜オンラインの場合＞

オンラインによる代理人のからの申請は認めない。

・ 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、「3.2.2　組織の認証」の定めに従い保険医療機関等の組織の認証のみ行い、個人の認証は規定しない。

3.2.4　確認しない加入者の情報

認めない。

3.2.5　機関の正当性確認

規定しない。

3.2.6　相互運用の基準

規定しない。

3.3　鍵更新申請時の本人性確認及び認証

3.3.1　通常の鍵更新時の本人性確認及び認証

加入者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

・保険医療機関等の組織からの申請により発行する場合

証明書の申請者は、保険医療機関等の組織管理者若しくは当該組織所属者若しくは保険医療機関等の組織管理者から委任を受けた代理人とする。

・法令等の要請により発行する場合

証明書の申請者は、法令等で定められた組織とする。

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

・保険医療機関等の組織からの申請により発行する場合

証明書の利用を希望する組織は、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

保険医療機関等の組織管理者若しくは当該組織所属者若しくは代理人が登録局に「3.2.2 組織の認証」、「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、保険医療機関等の組織管理者による委任状及び本 CP「3.2.3 個人の認証」の代理人が申請する場合に定める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

保険医療機関等の組織管理者若しくは当該組織所属者が登録局に「3.2.2 組織の認証」、「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、代理人による郵送での申請は認めない。

3. オンライン

保険医療機関等の組織管理者が登録局にオンラインで「3.2.2 組織の認証」、「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、当該組織所属者及び代理人によるオンラインでの申請は認めない。

また、証明書の利用申請者は、申請にあたり、本 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。

・ 法令等の要請により発行する場合

法令等で定められた組織が証明書を申請する場合は、認証局に対し以下の手続きによって証明書の発行申請を行う。

1. 根拠となる法令等の明示
   認証局に対して、発行申請の根拠となる法令等を明示する。

2. 保険医療機関等の認証手段の提示若しくは開示
   法令等で定められた組織が実施した、保険医療機関等の確認結果を登録局に提示する。

なお、本 CP による申請においては、持参、郵送、オンライン等の申請の手段は問わない。

4.2 証明書申請手続き

4.2.1 本人性及び資格確認

・ 保険医療機関等の組織からの申請により発行する場合

本人性（組織）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、認証局が署名用保健医療福祉分野 PKI、商業登記認証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、確実な確認を実施しなくてはならない。

1. 組織への証明書発行
   認証局は、組織への証明書の発行時、本 CP「3.2.2 組織の認証」及び「3.2.3 個人の認証」に定める各立証事項に対して、それぞれ以下の方法で真偽の確認を行う。

   ・ 組織管理者もしくは組織所属者からの申請の場合

(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有効期限が切れてないことの確認を実施する。また、申請者が組織管理者でない組織所属者の場合、社員証等の組織所属の証明書を所持していれば提示を求め、所持していない場合は、申請書に記載されている組織の電話番号に電話し、組織が存在及び申請者が在籍していることを確認する。

ただし、組織が中央官庁・地方公共団体の運営する機関で、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。

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有効期限が切れていないことの確認を実施する。また、申請書記載の組織の電話番号に電話し、組織が存在及び申請者が在籍していることを確認する。

ただし、組織が中央官庁・地方公共団体の運営する機関で、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。

なお、証明書の受け渡しに関して、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。

この場合においても、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、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して確認してもよい。

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。

・ 代理人からの申請の場合

(1) 持参の場合

代理人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有効期限が切れてないことの確認を実施する。また、申請書に記載されている組織の電話番号に電話し、組織及び申請者が存在することを確認し、更に代理人に対する委任の事実を確認する。

ただし、組織が中央官庁・地方公共団体の運営する機関で、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及び委任状を確認することで、問い合わせによる確認を省略することができる。

加えて、代理人に「3.2.3 個人の認証 ・代理人が申請する場合」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各認証局が選択し、CPSで定めることとする。

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。

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

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、代理人によるオンラインの申請を認めない。

・ 法令等の要請により発行する場合

本人性（組織）及び資格の確認については、法令等で定められた組織が保険医療機関等の実在性、保険医療機関等であることの認証を実施した結果を持って資格確認に代えることができる。

・ 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。

ただし、法令等の要請により証明書を発行した場合は、法令等に定める方法により証明書を受理した旨を確認する。

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。

＜組織管理者もしくは組織所属者、または代理人から失効申請があった場合＞

組織管理者もしくは組織所属者、または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、保険医療機関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。

＜法令等で定められた組織から失効申請があった場合＞

法令等で定められた組織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。

4.9.2 失効申請者

認証局は、次の１人又はそれ以上の者及び組織からの失効申請を受け付ける。

1. 組織の名前で証明書が発行された当該組織管理者もしくは組織所属者、または代理人
2. 認証局の職員
3. 法令等で定められた組織

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。

＜組織管理者若しくは組織所属者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組織の管理者若しくは組織所属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組織の管理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。

＜法令等に定める組織からの失効申請の場合＞

法令等で定められた組織から提示された確認方法に従い、速やかに当該証明書を特定し失効しなくてはならない。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。

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。