(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。

(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、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。

注）登録局業務の医療機関等への委託

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。

委託業務として、医療機関の管理者や医療従事者団体の代表者（以下、医療機関等の管理者）に、当該組織に所属する個人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 に則った自然人の本人性、実在性、申請意思確認、国家資格を有する者の資格保有の事実確認を医療機関等の管理者の責任のもと実施しなくてはならない。

また、登録局と医療機関等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、加入者の署名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、私有鍵を電子署名にのみ利用する。

4.5.2 検証者の公開鍵と証明書の利用目的

検証者は、署名検証の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、鍵更新を伴う更新のみを許可する。従って、鍵の更新を伴わない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

認証局は、以下の条件を満たす時に証明書の更新申請を受け付ける。

- 更新対象証明書が存在すること。
- 証明書が有効期限終了前のものであること。
- 証明書が失効されていないこと。
- 有効期限終了前で、認証局で定める期間に申請があったこと。

これらの要件を満たせば、申請者は更新申請書に署名してオンラインで証明書の更新が申請できる。

4.7.2 鍵更新申請者

認証局は、加入者本人若しくはその代理人を鍵更新申請者として受け付ける。

4.7.3 鍵更新申請の処理手順

「4.2.1 本人性及び資格確認」に定める本人性確認並びに資格確認を行うものとする。

但し、登録局で「4.2.1 本人性及び資格確認」に定める本人確認が完了した日から 5 年以内の場合は、上記に代わり加入者証明書による本人確認を行うことができる。

4.7.4 加入者への新証明書発行通知

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

4.7.5 鍵更新された証明書の受理

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。

4.7.6 認証局による鍵更新証明書の公開

認証局は署名用証明書の公開を行わない。

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、署名者の公開鍵を使う時に有効な CRL/ARL を使用して失効の有無をチェックし、証明書状態の確認を行うものとする。

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

署名のために使用される私有鍵は、法律によって必要とされる場合を除き、預託されないものとする。また、署名目的の私有鍵の回復も行わない。

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

5.1　建物及び物理的管理

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 X 5080:2002 と同等以上の規格に従うものとする。例えば、JIS X 5080:2002 の「第 8 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 X 5080:2002 と同等以上の規格に従うものとする。例えば、JIS X 5080:2002 の「第 6 章　人的セキュリティ」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。