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

2. 国家資格所有者証明書

　国家資格所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所有者本人もしくはその代理人とする。

3. 医療機関等の管理者の証明書

　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も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おこなう。

1. 持参

　本人も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なう。

　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、本人による委任状および本 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」及び認証局定める書類を郵送することにより利用申請を行なう。

　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

本人も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なう。

なお、代理人による申請の場合には、必要なデータに加え、本人による委任および本 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も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、電子証明書も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、電子証明書も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. 国家資格所有者への証明書発行

認証局は、国家資格所有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所有の確認を行う。

(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所有の有無を確認する。この時、国家資格発行機関も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所有の有無の回答を実施している場合は、登録局から資格所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、国家資格所有の有無を確認する。

また、当該国家資格証明書に本人の顔写真が貼付されていない場合は、印鑑登録証明書を添えて、国家資格免許証等のコピーの適当な空欄に実印を捺印させるものとする。

この時、国家資格発行機関も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所有の有無の回答を実施している場合は、登録局から資格所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も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、持参も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およ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、持参もしくは郵送の場合、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) 持参もしくは郵送の場合

申請時に持参も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および組織の実在性の確認については、持参も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およ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、申請意思および資格の確認、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 も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、国家資格所有者の資格所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 条第三号に基づく CPS および事務取扱要領を規定し、運用する。

CPS およ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も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 等を完全に廃棄も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および事務取扱要領を規定し、運用する。

CPSおよ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　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用途

4.5.1 加入者の私有鍵と証明書の利用用途

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用途

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なわない。

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、加入者本人もしくはその代理人を鍵更新申請者として受付ける。

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ならびに資格確認を行なうものとする。

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なうことができる。

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なわない。

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。

＜加入者もしくはその代理人から失効申請があった場合＞

加入者も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も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付ける。

1. 本人の名前で証明書が発行された加入者もしくはその代理人
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なうものとする。

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

一時停止は行なわない。

4.9.14 一時停止申請者

一時停止は行なわない。

4.9.15 一時停止申請の処理手順

一時停止は行なわない。

4.9.16 一時停止期間の制限

一時停止は行なわない。

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。