3. 運用要件

認証局が行う基本的な業務として、認証書の発行･失効に対する審査、認証局の鍵管理、認証書管理、失効管理、加入者秘密情報管理、監査があげられる。
認証局が信頼性を保つためには、これらの業務運用が安全かつ確実に継続されることが必要である。

3.1. 審査

審査は、認証局あるいは登録局が認証書の発行及び失効に先立って、申請者の本人確認及び申請情報の真正性確認を行うためのものである。審査が不十分であれば、本章で述べる他の運用要件及び次章で述べるシステム･設備要件を如何に満たしていようとも、認証書の信頼性は失われてしまう。
仮に、認証局の本人確認が充分でなかった場合には、他人の名前を騙って認証書を入手することが可能となり、その人になりすまして取引ができてしまうことになるからである。従って、申請方式(オンライン・書類送付・出頭）に応じて、どのような本人確認方法を準備するかが重要になってくる。

3.1.1. 認証書の新規発行時の審査

認証書の新規発行申請に対する審査は、一般に本人確認、唯一性確認、審査結果通知、登録などの処理からなる。

3.1.1.1. 本人確認と情報の真正性確認

認証書の信頼性は、対象者の属性情報(名前や所属等)の真正性及び公開鍵が対象者に属していることの確実性に依存する。真正性確認や本人確認の方法はいろいろあるが、基本的には以下のことが必要である。

(1) 申請された情報の真正性確認のために、信頼できる機関・組織・人による証明あるいは確認済みの情報と一致していることを照査する必要がある。より高い真正性確認のために、複数の情報源の情報を利用するのが望ましい。
(2) 申請者の本人確認のために、真正性確認とは異なる手段を用いることが必要である。例えば、審査結果等の通知に際して、申請者に通知が確実に届くような手段(例えば郵便など)を利用する必要がある。より高い信頼性を確保するためには、本人出頭が望ましい。
(3)オンライン申請以外の場合は、認証書の不正発行を防止するために、審査処理を複数人で分担して行なう必要がある。

以下にオンライン申請、書類送付申請、出頭申請のそれぞれの場合における本人確認及び真正性確認の方法を例示する。

- **オンライン申請**
  申請者が認証局に対してオンライン形態で認証書申請を行う方式である。

例えば、カード会員等個人の認証に適した申請方法である。認証局所定の申請フォームを画面上に呼び出し、入力フィールド(申請必要項目）に以下のような情報を複数入力させて認証局に送信する。

・生年月日
・自宅住所
・自宅電話番号
・クレジットカード番号/預金口座番号
・暗証番号(PIN)
・母親旧姓(米国の例)

等々、及びその組合わせが考えられる。本人確認は、これらの情報を信頼できる機関(クレジットカード会社、銀行等)の保有する情報、あるいは自局が保有する情報との突き合わせ、及び審査結果等を簡易書留などで申請者に郵送することによって行なわれる。

● **書類送付申請**

認証局所定の申請書式に必要事項を記載させるとともに、申請者が本人であることを証明する以下のような書類を送付させる。

・印鑑登録証明書(法人・個人)
・戸籍謄本(個人)
・商業登記簿謄本(法人)

等々、およびその組み合わせが考えられる。本人確認は、証明書等の記載事項及び捺印の確認をもって行われる。

● **出頭申請**

申請者本人が出頭しての対面による申請受付のことである。認証局所定の申請書式に必要事項を記載させるとともに、以下のような書類を提示させる。

・運転免許証
・パスポート
・健康保険証

等々、およびその組み合わせが考えられる。本人確認は、証明書等の写真および記載事項の確認をもって行なわれる。

3.1.1.2. 申請の受理と意思確認

(1) 認証申請者からの申請を認証局が受理したことを申請者に対して返答通知するとともに、併せて申請の意思確認を行う必要がある。なお、意思確認は、結果通知による事後的確認であっても構わない。

3.1.1.3. 唯一性確認

(1)被認証者名について、少なくとも当該認証書を発行する認証局配下では重複がなくユニークであることを確認する必要がある。

(2)申請者の公開鍵について、少なくとも当該認証書を発行する認証局配下では重複していないことを確認するのが望ましい。

(3)認証書に記載される公開鍵に対応する正当な秘密鍵を申請者が所持していることを確認するのが望ましい。

例えば、申請情報に秘密鍵でデジタル署名させるか、あるいはチャレンジデータ[5]にデジタル

---

[5] チャレンジデータは、申請者が予め予想できないようなデータで通常は乱数を使う。

署名させて認証局に送付させる方法等によって行なう。

3.1.1.4. 審査情報の登録

(1)申請情報及び審査情報は、後から利用できるように登録しておく必要がある。
(2)申請時に、予め失効などの事故に対する情報など(例えば、失効申請代行者など)を登録させることが望ましい。

3.1.1.5. 審査結果の通知

(1)審査結果は、通知あるいは問合せに対する回答等によって、申請者に通知する必要がある。

3.1.2. 認証書の定期更新時の審査

(1)認証書の定期更新申請に対する審査は、新規発行時の場合と同様、本人確認、唯一性確認、意思確認、審査結果通知、登録などの処理が必要である。
(2)なお、本人確認や意思確認については、新規発行時とは異なる手段を用いて行なうことも可能である。例えば、名前などの重要な情報に変更がない場合には、申請情報に対して更新前の秘密鍵でデジタル署名させることで本人確認や意思確認を行うことも可能である。

3.1.3. 認証書の失効時の審査

認証書の失効及び一時失効の申請に対する審査は、本人確認、審査結果通知、登録などの処理からなるが、新規発行や定期更新の場合とは多少処理が異なる。
失効申請するのが誰か、また失効の理由として何が考えられるかをまとめると表-1 になる。
なお、一時失効の手続き等は基本的に正規の失効と同様である。

表-1 失効申請のパターン

申請者	失効理由(例)	申請者確認の方法(例)
本人	秘密鍵の漏洩等の危瀕	本人の署名
	秘密鍵の消失(パスワード忘れ、ファイル消去等)	新規発行と同様の手続
	重要な認証情報の変更	同上
第三者機関(登録局)	組織異動	第三者機関の署名
	不正利用	同上
認証局	認証局のミス	認証局が確認
	利用者の虚偽申請	同上

3.1.3.1. 申請者確認

失効における申請者確認は、悪意の第三者が他人の認証を失効させることがあり得るので、それを防ぐために必要である。
(1)申請者の本人確認は、秘密鍵の危瀕時などの場合には迅速に行なう必要がある。
例えば、秘密鍵の危瀕時などの場合には、申請情報にデジタル署名を付したもので受け付けるなど(この場合は、秘密鍵を不正に入手した者、あるいは正当な保持者による失効申請は実効性がある)。
(2)秘密鍵の消失、重要情報の変更の場合は、新規発行と同等の本人確認が必要である。

(3)認証書の誤りや不正使用の検知、本人による失効申請が困難な事由の発生、あるいは認証書の不正発行などの場合は、登録局や認証局あるいは事前に登録されている機関などが本人に代わって失効申請できるようになっていることが必要である。
(4)オンライン申請以外の場合は、認証書の不正な失効を防止するために、審査処理を複数人で分担して行なう必要がある。

3.1.3.2. 失効情報の登録

(1)失効リスト生成などのために使用した申請情報及び審査情報は後から利用出来る様に登録する必要がある。

3.1.3.3. 失効審査結果の通知

(1)失効審査結果は、通知あるいは問合せに対する回答等によって、申請者に通知する必要がある。

3.1.4. 失効後の認証書の再発行時の審査

失効事由によっては認証書の再発行を行なわない場合があるが、再発行する場合には以下の審査を行なう必要がある。
(1)公開鍵や重要情報の変更が伴う失効の場合、失効後の認証書の再発行は、認証書の新規発行と同様の処理が必要である。
(2)本人以外の失効申請に基づく失効の場合、失効後の認証書の再発行は、認証書の新規発行と同様の処理が必要である。

3.2. 認証局の鍵管理

認証局は、認証書や失効リストの署名、鍵の暗号化などに使用する秘密鍵／公開鍵ペア、重要な秘密情報を暗号化するための共通鍵、及び鍵生成時の秘密パラメータ等について、それらの全ライフサイクルにわたって安全で信頼性の高い管理が要求される。

3.2.1. 鍵の生成

(1)鍵ペアや共通鍵の生成は、信頼できる暗号鍵生成システムを利用して行なう必要がある。なお、暗号鍵生成システムの機能は、暗号鍵管理モジュールの内部に実装されていることが望ましい。
(2)鍵ペアや共通鍵の生成は、複数人管理のもとで行う必要がある。なお、複数人管理では、メンバーを異なる組織の権限を有する者から構成することが望ましい。

3.2.2. 鍵の保管

(1)暗号鍵生成システムによって生成された鍵は、複数の鍵構成要素に知識分散することによって単独では鍵に関する秘密情報を一切知り得ないように保管するか、あるいは暗号鍵管理モジュール内に保管する必要がある。

(2)鍵を知識分散して保管する場合には、知識分散された鍵の情報は各鍵構成要素について、権限を有する者が個別に保管する必要がある。
(3)一方、鍵を暗号鍵管理モジュール内で保管する場合には、複数人の権限を有する者が揃わなければ暗号鍵管理モジュールの持ち出し等ができないよう複数人管理のもとで保管する必要がある。

3.2.3. 鍵の利用

(1)保管されている秘密鍵や共通鍵をデジタル署名や復号に利用する際には、暗号鍵管理モジュールに入れて使用することが必要である。
鍵が知識分散されて保管されている場合には、利用の前に秘密情報を暗号鍵管理モジュールにロードする必要があるが、そのロード処理は複数人管理のもとで行うことが必要である。
(2)暗号鍵管理モジュールを認証書発行システム等に接続したり、暗号鍵管理モジュール内の鍵を利用可能状態にする操作は、複数人管理のもとで行う必要がある。
(3)暗号鍵管理モジュールが接続されたシステムを停止する場合などにおいて、暗号鍵管理モジュール内の鍵を利用可能状態から利用停止状態に切り替える処理は、複数人管理のもとで操作を行う必要がある。
(4)鍵の利用において、より高いセキュリティを確保するため、暗号鍵管理モジュールを含むシステムを必要の都度スタンドアロンで運用することが望ましい。

3.2.4. 鍵のバックアップ

(1)秘密鍵や共通鍵の偶発的な消失等によって、認証局業務の停止、さらに鍵の更新に伴う対応処理の発生などを避けるために、鍵のバックアップを行う必要がある。バックアップにおけるセキュリティ要件は、保管と同程度以上でなければならない。
(2)バックアップされた鍵は、鍵が保管あるいは利用されている場所から離れた所に保管することが望ましい。

3.2.5. 鍵の保存

(1)有効期間が終了した秘密鍵や共通鍵で、それらが有効期間後も必要になるものは(例えば、鍵暗号化鍵を復号するための秘密鍵など)、保存期間を定めて、複数人管理や知識分散による保存を行う必要がある。
(2)認証局の公開鍵は有効期間後も可用性を確保することが必要であり、改竄されないように保存する必要がある。

3.2.6. 鍵の廃棄

(1)有効期間が終了した認証局のデジタル署名用の秘密鍵や、保存期間が終了した鍵などは、その後の不正利用が行われないように廃棄する必要がある。
(2)廃棄は、複数人管理のもとで、秘密情報の一部でも露顕したり残存させたりすることなく行われる必要がある。

3.2.7. 鍵の定期更新

(1) 認証局の鍵は、あらかじめ有効期間を設け、定期的に更新する必要がある。なお、鍵の有効期間の設定は認証局のポリシーによる。

3.2.8. 鍵の危瀕／災害時の復旧

(1)認証局は、認証局の秘密鍵が内部不正によって漏洩したり、第三者によって秘密鍵が解読された場合、さらには災害によって認証局がダメージを受けた場合などの事態に対して、事前に対応策を策定しておく必要がある。
(2)認証局の秘密鍵が危瀕した場合、あるいはその可能性がある場合、認証局は速やかに対応する認証書の失効を行う必要がある。
(3)認証局の秘密鍵が危瀕した場合、その秘密鍵で署名した加入者の認証書を失効させ、失効させたことを加入者に通知する必要がある。また、下記の対応を行う必要がある。
- 申請者からの認証要求を見合わせている旨の開示。
- 利用者が認証局の状況確認を行える窓口の設置。

(4)認証局の秘密鍵の危瀕／災害の事態から復旧する際には下記の対応が必要である。
- 安全な環境に復していることの確認。
- 認証局の鍵と認証書の更新。
- 加入者の認証書の再発行手続き。

(5)認証局の秘密鍵が危瀕していないかを確認するため、認証書の利用状況についてサンプリングなどの方法でモニタリングを行うことが望ましい。
(6)認証書の再発行に当っては、認証局側からの自動再発行はせず、加入者からの再発行要求があった場合にのみ行うのが望ましい。

3.2.9. 認証局の公開鍵の管理

(1)認証局は生成した鍵ペアの公開鍵に対して、上位認証局が存在する場合にはその上位認証局から認証書を取得するか、存在しない場合には自らの秘密鍵で署名した認証書を作成する必要がある。
(2)認証局の認証書は広く一般に開示もしくは公開する必要がある。

3.3. 認証書管理

認証局が認証書を作成し申請者に送付する際には、不正な生成や改竄、漏洩等が行われないようにすることが必要であり、また認証書の登録、管理に際しても、不正なアクセスが行われない様に管理する必要がある。

3.3.1. 認証書作成

(1) 認証書作成にあたっては、不正な生成が行なわれないようにする手続きを定める必要がある。特にオフラインで生成する場合には審査処理を分離するとともに、権限を有する者以

外はアクセスできないシステムが必要である。

3.3.2. 認証書送付

(1)認証書送付にあたっては、セキュアな手段を講じることが必要である。
(2)認証書を送付する際、受取りの確認ができる手段を選択することが望ましい。

3.3.3. 認証書の登録・保管

(1)認証局は作成した認証書の登録・保管において、不正アクセスを防止するためにアクセス管理を行なう必要がある。
(2)登録・保管された認証書は、災害もしくは消失等に備えてバックアップをとっておくことが望ましい。

3.3.4. 認証書の開示

(1) 認証局は登録・保管された認証書の開示もしくは非開示等についてポリシーで明らかにする必要がある。開示もしくは公開する場合は、以下の様に開示先・開示方法･開示期間などについても明確にする必要がある。
- 開示先：誰に開示するかを、明確に定める必要がある。
- 開示方法：開示の方法としては、開示サービスの時間帯等と併せて、アクセス方法、開示情報フォーマット等も明確にする必要がある。
- 開示期間：認証書の開示期間は加入者への認証書発行後、その認証書の有効期限内は開示する必要がある。

3.3.5. 認証書の保存

(1)発行した認証書の有効期限が切れた後も、改竄、消去、漏洩等の不正なアクセスがなされないような対策を講じて、認証局は一定の期間認証書を保存する必要がある。

3.4. 失効管理

秘密鍵の危瀕や重要な認証情報の変更等で失効した認証書は、失効リストとして生成され保管、管理される必要があると共に、正当な利用者の問合せに適宜応じる必要がある。

3.4.1. 失効リストの生成

(1)失効リストの生成および認証局による署名は、認証書発行の場合と同等のセキュリテイ管理が必要である。
(2)失効リストの発行は１週間毎、１日毎などというように定期的に行う必要がある。当該期間中に失効がない場合でも、ないことを知らせるために失効リストを発行する必要がある。ど

のような周期で行うかは、利用者に明確に示しておく必要がある。

3.4.2. 失効リストの保管

(1)失効リストは、不正アクセスによる改竄、消去、漏洩等が行われない様に保管する必要がある。
(2)失効リストは災害もしくは消失等に備えバックアップを取っておく事が望ましい。
(3)失効した認証書が膨大になる場合の対応として、失効リストを分散配置したり、高度な失効管理が行える機関にその一部ないし全ての機能を行わせることも可能である。

3.4.3. 失効リストの開示

(1)失効した認証書もしくは認証書の最新ステータスは、失効リスト等によって正当な利用者が問合せ出来る様にする必要がある。

3.4.4. 失効リストの保存

(1)失効した認証書の当初の有効期限経過後も、認証局は一定の期間失効リストおよび関連するデータを保存しなければならない。

3.5. 加入者秘密情報管理

加入者が認証申請時等で認証局に提示した情報は、プライバシ侵害もしくは不正利用等の防止のために、情報のアクセス、保管、開示等について十分なセキュリテイを考慮する必要がある。

3.5.1. 加入者秘密情報の定義

加入者秘密情報とは、認証書あるいは失効リストに記載される情報以外の加入者に関する情報であり、加入者のプライバシーに係る情報および利用履歴等を含む。例えば認証書の発行・更新・失効のために加入者から提示された氏名、生年月日、パスワードその他の記述又は加入者に付された番号、記号その他の符号（当該情報のみでは識別できないが、他の情報と容易に照合する事ができ、それにより当該個人を識別できるもの）が含まれる。

3.5.2. 加入者秘密情報へのアクセス権限

(1) 加入者秘密情報へのアクセスは、機密保持の為に、権限を有する者だけが行なえる様にする必要がある。

3.5.3. 加入者秘密情報の保管

(1) 加入者秘密情報は、不正に改竄・消去・漏洩等がなされないように安全に保管する仕組み、

および必要に応じて取り出せる仕組みを持つことが必要である。
(2) 加入者秘密情報は、災害等により消失することのないように必要に応じてバックアップをとることが望ましい。

3.5.4. 加入者秘密情報の開示

(1) 認証局は、加入者秘密情報を開示してはならない。ただし、以下の場合はその限りではない。
- 加入者本人または本人の代理人から自己の登録情報に関して開示要求があった場合。ただし、認証局はあらかじめ本人であることを確認する要領を定める必要があり、その要領に従って本人確認を実施した後、開示するものとする。
- 法令の定めにより、回答が義務づけられているもの。また、法令の範囲内で本人の同意を得た場合。

3.5.5. 加入者秘密情報の保存

(1) 認証書の有効期限が切れた後も、認証局は一定の期間加入者秘密情報を保存する必要がある。
(2) また、加入者秘密情報は、不正なアクセスによる情報の改竄・消去・漏洩等が無いよう適切な手段を講じて保存する必要がある。

3.6. 監査

認証局は、要求される業務の専門性、信頼性等が十分に保たれているかを監査されなければならない。従って、監査情報の取得・管理、監査人の選定、監査頻度等を明確に規定し監査を受けると共に、監査実施結果を速やかに開示する事が求められる。

3.6.1. 監査の目的

認証局は、CPS 等に定められた基準を遵守しているか否かをマネージメント、運用、設備・システムの面から監査することにより、利用者からの信頼性の維持・確保を図るものとする。

3.6.2. 監査情報の定義

監査情報とは、認証局の CPS ・技術情報・安全対策実施状況・システムイベントの記録等の監査を行うために必要な情報をいう。例えば、監査情報には以下のような情報が含まれる。
- 認証申請の情報：申請書類、申請受付担当者、本人確認手段など
- 認証局の鍵管理履歴：生成、ロード、バックアップ、保管、リカバリー、廃棄など
- 機密情報のアクセス履歴：機密データの入出力・削除、セキュリティプロファイルの変更、システムダウンと復旧処理、監査情報のアクセス、設備等の入退室など
- 受発信データ：認証局が交信したデータ、発行認証書、失効申請など

3.6.3. 監査情報の保管

(1) 監査情報は、そのアクセス権限を明確にし、不正アクセスによる情報の改竄、消去、漏洩等に対して保護し、必要に応じ適正な期間内に提供可能な状態で保管しておく必要がある。
(2) また、監査情報は適正な間隔でバックアップを取り、隔地保管することが望ましい。

3.6.4. 監査人の選定

(1) 監査人は、コンピュータ・セキュリティに関する専門的知識を有するもので、監査対象から独立かつ客観的立場の者を選定することが望ましい。

3.6.5. 監査の頻度

(1) 監査の頻度は、最低年1度行う必要がある。しかし、以下の事態が生じた場合はこの限りではない。
- システム資源の異常な負荷増大、処理件数の異常増加、通常とは異なる時間帯や場所からのアクセスがあった場合
- CPS等に重要な変更があった場合
- 利用者間のトラブルが多発した場合
- その他、監査が必要と判断される場合

3.6.6. 監査結果の開示と対処

(1) 監査実施後は、監査結果を速やかに開示するものとし、監査の結果として欠陥が指摘された場合には、以下の対処を行う必要がある。
- 欠陥が修正されるまでの対処(例えば、運用の停止、利用者に対する十分なアナウンス等)
- 欠陥への対処

3.6.7. 監査後の監査情報及び監査結果の保存

(1) 監査情報及び監査結果の保存は、監査後の保存期間を予め定め、不正なアクセスによる情報の変更・改竄・削除等が無いよう適切かつ合理的な安全対策を講ずる必要がある。