文書管理番号：B4S3-002000-00000

公的個人認証サービス

利用者証明用認証局　運用規程

第 2.0 版

2019 年 11 月 5 日

変更履歴

版数	日付	変更内容
1.0	平成 27 年 10 月 13 日	新規作成
1.1	平成 28 年 4 月 1 日	機構組織改変に伴う変更
2.0	2019 年 11 月 5 日	5.5.2.2 デジタルデータとして保管する情報 令を以下の説明文に修正 電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律施行令

目次

1. はじめに

本運用規程は、住民と国又は地方公共団体の機関等との間の申請・届出等手続の電子化並びに民間企業のサービスへの活用に資することを目的として、「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律」（以下「法」という。）に基づき、地方公共団体情報システム機構（以下「機構」という。）が発行する利用者証明用電子証明書等のための利用者証明用認証局（以下「利用者証明用CA」という。）の認証業務に関する運営方針を定めるものである。

なお、本運用規程の構成は、IETF(Internet Engineering Task Force)のPKIX(Public-Key Infrastructure X.509)Working GroupによるRFC(Request For Comments) 3647 「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」に準拠している。ただし、他の規程を参照する部分は見出しだけを残し参照内容を明示することとする。

1.1. 概要

利用者証明用CAは、住所地市区町村に備えられている住民基本台帳に記録されている者に対して、その者の申請に応じて、利用者証明用電子証明書を発行し、利用者証明用CAの運用に必要な電子証明書を発行する。さらに利用者証明用電子証明書失効情報（利用者証明用電子証明書の失効に係る情報をいう。以下同じ。）、失効記録（CRL/ARL）（電子証明書等の失効に係る情報を記録したものをいう。以下同じ。）及び失効情報ファイル（失効記録（CRL）のアーカイブをいう。以下同じ。）を作成し、法第36条第1項に規定する利用者証明検証者の求めに応じて提供する。

また利用者証明用CAについては、CP（証明書ポリシー）及びCPS（認証実施規程）をそれぞれ独立したものとせず、本運用規程を利用者証明用CAの認証業務に関する運営方針として位置付ける。

1.2. 文書名と識別

利用者証明用CAの証明書ポリシーの識別子は、次のとおりとする。

利用者証明用CAの証明書ポリシーの識別子 1.2.392.200149.8.5.1.3.30

利用者証明用 CA の SSL 証明書ポリシーの識別子

1.2.392.200149.8.5.1.3.130

利用者証明用CAのOCSPの証明書ポリシーの識別子

1.2.392.200149.8.5.1.3.330

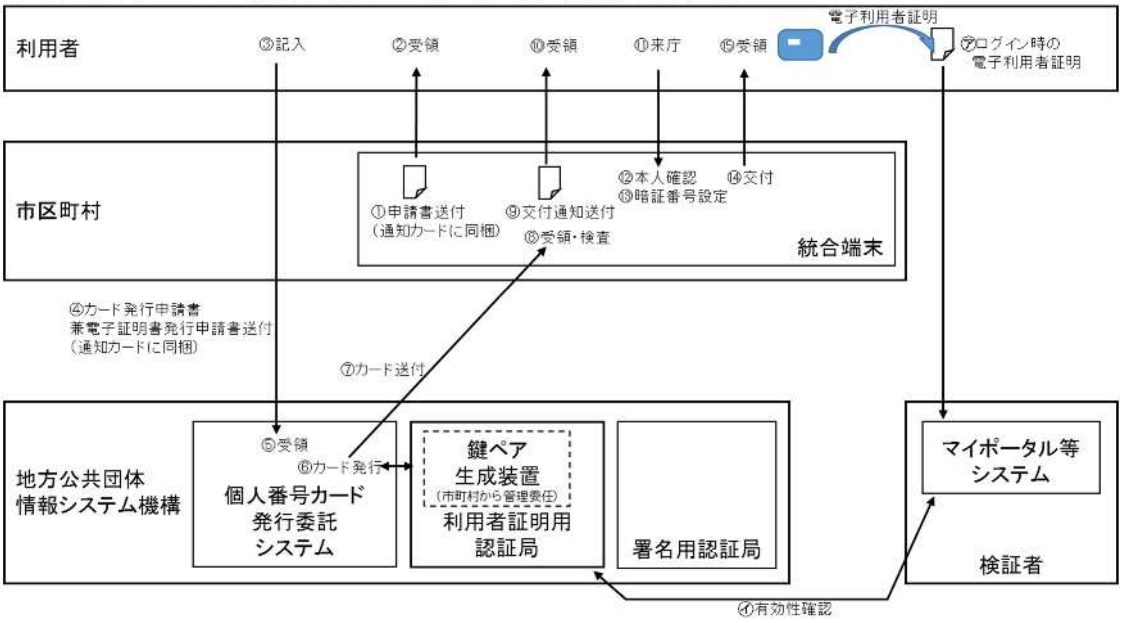
利用者証明用CAのプログラムに付与するコードサイニング証明書ポリシーの識別子 1.2.392.200149.8.5.1.3.430

OID管理表（1.2.392.200149.8.5.1.3(Authenticate)以下）

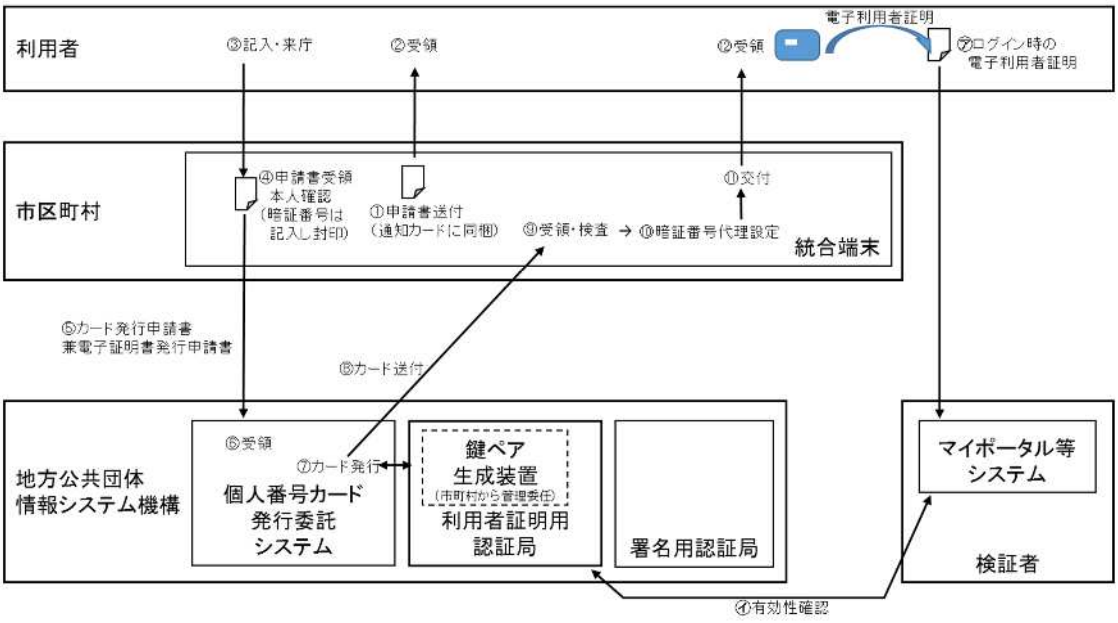
class30(30)	利用者証明用 CA の証明書ポリシー
TLS30(130)	利用者証明用 CA の SSL 証明書ポリシー（TLS 認証）
CVS30(230)	利用者証明用 CA の官職証明書検証サーバ証明書ポリシー （予約）
OCSP30(330)	利用者証明用 CA の OCSP レスポンダ証明書ポリシー
CodeSigning30(430)	利用者証明用 CA のプログラムに付与するコードサイニング証明書ポリシー（予約）

1.3. PKI の関係者

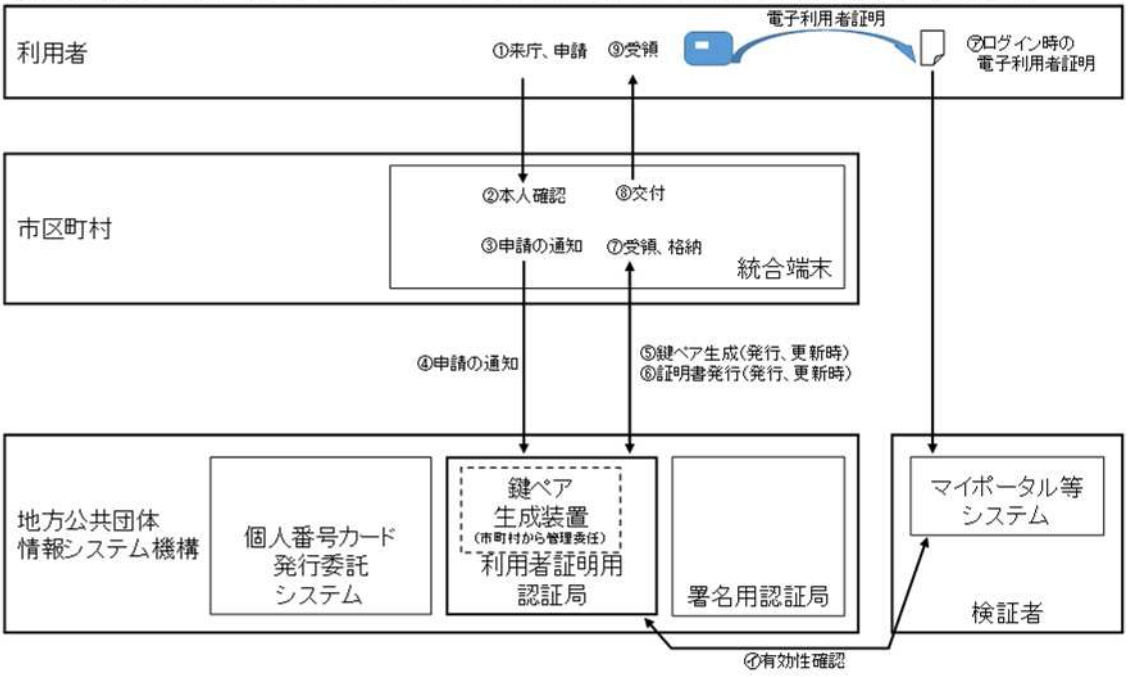
●個人番号カードの発行と同時に電子証明書を発行する場合



●個人番号カードの発行と同時に電子証明書を発行する場合
（住所地市町村長の指定する場所に出頭して交付申請書を提出する場合）



●既に所持している個人番号カードに電子証明書の発行、失効、更新をする場合



1.3.1. 認証局

1.3.1.1. 機構

機構に、以下に示す利用者証明用CAの機能を備える。

1.3.1.2. 利用者証明用 CA

利用者証明用CAは、利用者証明用電子証明書及び発行記録の記録、失効情報の記録（CRL/ARL）、利用者証明用電子証明書の有効性を確認する手段の提供、その他の電子証明書の発行等の認証業務を行う。利用者証明用CAの秘密鍵の危殆化（秘密鍵が紛失、漏えい等により管理不能になった、あるいは、その疑いがあることをいう。以下同じ。）時の対応や災害発生等による緊急時の対応も行う。

1.3.2. 登録局

市区町村長は、利用者証明用電子証明書の発行申請、更新申請、失効申請及び一時保留解除の届出の受付及び申請者の本人確認、利用者証明利用者の秘密鍵の危殆化の届出の受付、申請者の鍵ペア生成、利用者証明用CAへ申請又は届出の通知、申請者の鍵ペアと発行した利用者証明用電子証明書の個人番号カードへの安全な格納と申請者への交付等を行う。

代理人による申請の場合には、「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律施行規則」（以下「規則」という。）第41条第2項第1号の規定に基づく、代理人の本人確認と代理権の存在確認を行う。

利用者証明用電子証明書の失効申請の受付については、法の規定に基づき、電気通信回線を用いて利用者証明利用者の署名用秘密鍵による電子署名の検証により行うことも可能である。

1.3.3. 利用者

1.3.3.1. 申請者／利用者証明利用者

申請者とは、法第22条第1項の規定により、住所地市区町村長へ利用者証明用電子証明書の発行等を申請する者をいう（申請は代理人が行うこともできる。ただし、代理人は、規則第41条第2項第1号の規定を満たすこと。）。

利用者証明利用者とは、住民基本台帳に記録されている者で、利用者証明用電子証明書の発行・交付を受けた者をいう。

利用者証明利用者は、国又は地方公共団体の機関等との間のオンライン申請・届出等において、利用者証明用電子証明書を利用することができる。利用者証明利用者は機構に対して自己に係る認証業務情報（利用者証明用電子証明書の発行記録、利用者証明用電子証明書失効情報及び利用者証明用電子証明書失効

情報ファイルをいう。以下同じ。）について、その開示を請求し、当該開示に係る認証業務情報について、その内容の全部又は一部の訂正、追加又は削除を請求することができる。また、認証事務等に不服がある場合は、総務大臣に対し、行政不服審査法による審査請求をすることができる。

1.3.4. 検証者

1.3.4.1. 利用者証明検証者

次の者のうち、利用者証明用電子証明書の有効性を確認する手段の提供を受けることについて、法第36条第1項の規定に基づきあらかじめ届け出て、アクセス権を付与された者をいう。

① 行政手続等における情報通信の技術の利用に関する法律第2条第2号に規定する行政機関等（以下「行政機関等」という。）
② 裁判所
③ 行政機関等に対する申請、届出その他の手続に随伴して必要となる事項につき、電磁的方式により提供を受け、行政機関等に対し自らこれを提供し、又はその照会に応じて回答する業務を行う者として行政庁が法律の規定に基づき指定し、登録し、認定し、又は承認した者
④ 「電子署名及び認証業務に関する法律」（以下「電子署名法」という。）第8条に規定する認定認証事業者
⑤ 電子署名法第2条第3項に規定する特定認証業務を行う者であって、政令で定める基準に適合するものとして総務大臣が認定する者
⑥ 前各号に掲げる者以外の者であって、利用者証明利用者が行った電子利用者証明について当該利用者証明利用者が当該電子利用者証明を行ったことの確認を政令で定める基準に適合して行うことができるものとして総務大臣が認定するもの

利用者証明用CAから、失効情報（CRL/ARL）の提供等、利用者証明用電子証明書の有効性を確認する手段の提供を受け、利用者証明利用者からの電子利用者証明を検証する。

1.3.5. その他の関係者

1.3.5.1. 署名用認証局（以下、「署名用 CA」という）

住民基本台帳に記録されている者に対して、その者の申請に応じて、署名用電子証明書等を発行する機構の認証局をいう。署名用電子証明書は、その者の個人番号カード内に利用者証明用電子証明書とともに記録される。

1.4. 証明書の利用用途

1.4.1. 適切な証明書の利用用途

利用者証明用CAの発行する電子証明書の種類及び用途は、次のとおり。

① 利用者証明用電子証明書

・ 行政機関等及び裁判所で行うオンライン申請・届出等の手続に係る電子利用者証明
・ 民間企業による電子商取引に係る電子利用者証明

② OCSPレスポンダ証明書
・ 利用者証明検証者がOCSPレスポンダ照会方法（OCSPプロトコルを用いた失効情報の照会に回答する方法。以下同じ。）で電子証明書の有効性を確認する手段の提供

③ SSL証明書
・ 公的個人認証サービスの運用における内部利用

1.4.2. 禁止される証明書の利用用途

利用者証明用CAが発行する証明書は法で制限されている用途に利用してはならない。

1.5. ポリシー運用管理

1.5.1. 文書を管理する組織

本運用規程の責任者は機構の理事長とする。

1.5.2. 連絡先

本運用規程に関する照会窓口を下記に示す。

地方公共団体情報システム機構
個人番号センター公的個人認証部
東京都千代田区一番町25番地
電話：03-5214-8000
メールアドレス：contact@ml.jpki.go.jp

1.5.3. ポリシーに対する適合性を決定する者

利用者証明用CAの運用規程への適合性を決定する者は、機構の個人番号センター長とする。

1.5.4. 運用規程承認手続

機構の理事長の決定をもって有効なものとする。

1.6. 定義と略語

付録　用語集に記載する。

2. 公開とリポジトリの責任

利用者証明用 CA に関する情報は、Web 上及びリポジトリ上で公表する。

2.1. リポジトリ

リポジトリは、24時間365日利用可能とする。ただし、定期保守作業等により、一時的にリポジトリを利用できない場合もある。

2.2. 証明書情報の公開

利用者証明用CAは、機構のWeb上で次の情報を公開する。

- 法及び関係法令
- 本運用規程
- 利用者証明用CAの秘密鍵の危殆化に係る情報等
- 利用者証明用CAの自己署名証明書とフィンガープリント
- 利用者証明用CAの自己署名証明書（バイナリ形式）

利用者証明用CAは、公的個人認証サービスのリポジトリ上で、次の情報を公開する。

- 利用者証明用CAの自己署名証明書
- リンク証明書
- 利用者証明用CAの自己署名証明書、リンク証明書の失効記録（ARL）
- 利用者証明用電子証明書の失効記録（CRL）

なお、失効事由の詳細は公表しない。また、利用者証明用電子証明書の失効情報は法に基づき利用者証明検証者に限定して提供する。

2.3. 公開の時期またはその頻度

公開する情報の更新頻度は次のとおりとする。

- 法、関係法令、本運用規程等は最新版をWeb上に掲載する。
- 利用者証明用CAの自己署名証明書及びリンク証明書は発行・更新の都度公開する。
- 失効記録（CRL/ARL）は毎日1度更新する。

2.4. リポジトリへのアクセス管理

リポジトリ上の次の情報についてはアクセス制限を設けない。

- 利用者証明用CAの自己署名証明書
- リンク証明書
- 利用者証明用CAの自己署名証明書、リンク証明書の失効記録（ARL）

ただし、リポジトリ上に公開する利用者証明用電子証明書の失効記録（CRL）についてはアクセス制限を行う。

3. 識別と認証

3.1. 名称決定

3.1.1. 名称の種類

利用者証明用CAが発行する電子証明書の発行名義人名及び主体者名は、X.500 識別名（DN：Distinguished Name）の形式に従って設定する。

3.1.2. 名称の意味に関する要件

利用者証明用電子証明書の発行名義人名は、機構名を記録する。

3.1.3. 利用者証明利用者の匿名性又は仮名性

利用者証明利用者の匿名、仮名を利用することはできない。

3.1.4. 名称形式を解釈するための規則

X.500 識別名の規程に従う。

3.1.5. 名称の一意性

利用者証明用CAの発行する電子証明書のsubjectフィールドは、一意に割り当てる。

3.1.6. 商標の認識・認証・役割

規定しない。

3.2. 初回の証明書発行申請時の識別と認証

3.2.1. 秘密鍵の所有を証明する方法

3.2.1.1. 利用者証明用電子証明書

住所地市区町村長が利用者証明利用者の秘密鍵と公開鍵の鍵ペアを生成する。そのため、この項目は規定しない。

3.2.1.2. その他の証明書

その他の証明書の秘密鍵の所有を証明する方法に関しては、所定の手続による。

3.2.2. 組織の認証

3.2.2.1. 利用者証明用電子証明書

規定しない。

3.2.2.2. その他の証明書

その他の証明書の組織の認証は、所定の手続による。

3.2.3. 個人の認証

3.2.3.1. 利用者証明用電子証明書

⑴ 個人番号カード発行を伴う利用者証明用電子証明書の発行申請

個人番号カード発行を伴う利用者証明用電子証明書の発行申請の際は、申請者の本人確認を次の方法により行う。

① 住所地市区町村長は、当該申請者が住民基本台帳に記録されている者であることを確認（実在性の確認）

② 交付時、あるいは住所地市町村長の指定する場所に出頭して交付申請書を提出する場合は申請時に、住所地市区町村長は、申請者が住民基本台帳に記録されている者本人であることを公的機関が発行した写真の貼付された身分証明書等（規則第41条第1項に規定された書類）の提示等により確認（本人性及び真正性の確認）

⑵ 個人番号カード発行を伴わない利用者証明用電子証明書の発行申請

個人番号カード発行を伴わない利用者証明用電子証明書の発行申請の際は、申請者の本人確認を次の方法により行う。

① 住所地市区町村長は、当該申請者が住民基本台帳に記録されている者であることを確認（実在性の確認）

② 住所地市区町村長は、申請者が住民基本台帳に記録されている者本人であることを公的機関が発行した写真の貼付された身分証明書等（規則第41条第1項に規定された書類）の提示等により確認（本人性及び真正性の確認）

⑶ 代理申請

代理人による申請の場合、代理人の本人確認及び代理権の存在の確認を次の方法により行う。

① 申請者本人の記名及び押印のある委任状、当該申請者に対して文書で照会したその回答書及び住所地市区町村長が適当と認める書類の確認

② 代理人の本人確認を、公的機関の発行した写真の貼付された身分証明書等（規則第41条第2項第1号に規定された書類）の提示等により確認

3.2.3.2. その他の証明書

規定しない。

3.2.4. 検証されない利用者証明利用者の情報

規定しない。

3.2.5. 権限の正当性確認

権限の正当性確認は、「3.2.3.個人の認証」の手続に準じて行う。

3.3. 鍵更新時の識別と認証

3.3.1. 通常の鍵更新時の識別と認証

3.3.1.1. 利用者証明用電子証明書

「3.2.3.1.（2）個人番号カード発行を伴わない利用者証明用電子証明書の発行申請」の手続に準じる。

なお、更新に伴い失効する利用者証明用電子証明書に係る秘密鍵は、市区町村長が所定の方法により消去する。

3.3.1.2. その他の証明書

その他の証明書更新時における識別と認証は、「3.2.初回の証明書発行申請時の識別と認証」の手続に準じる。

3.3.2. 証明書失効後の鍵更新時の識別と認証

3.3.2.1. 利用者証明用電子証明書

⑴ 証明書失効後の個人番号カード発行を伴う鍵更新時

「3.2.3.1.(1)個人番号カード発行を伴う利用者証明用電子証明書の発行申請」の手続に準じる。

⑵ 証明書失効後の個人番号カード発行を伴わない鍵更新時

「3.2.3.1.(2)個人番号カード発行を伴わない利用者証明用電子証明書の発行申請」の手続に準じる。

3.3.2.2. その他の証明書

その他の証明書失効後の再発行時における識別及び認証は、「3.2. 初回の証明書発行申請時の識別と認証」の手続に準じる。

3.4. 失効申請時の識別と認証

3.4.1. サービスの利用を取りやめるための失効申請

3.4.1.1. 利用者証明用電子証明書

利用者証明利用者は、住所地市区町村の窓口において書面による失効申請を行う。法の規定に基づき、電気通信回線を用いて申請も可能である。

利用者証明利用者の本人確認は、「3.2.3.1.(2)個人番号カード発行を伴わない利用者証明用電子証明書の発行申請」の手続に準じる。

電気通信回線による申請の場合は、本人確認を利用者証明利用者の署名用電子証明書による電子署名の検証により行う。

3.4.1.2. その他の証明書

その他の証明書の失効時における識別及び認証は、「3.2.2.3. その他の証明書」の手続に準じる。

3.4.2. 利用者証明利用者の秘密鍵の危殆化の場合の届出

3.4.2.1. 利用者証明用電子証明書

利用者証明利用者は、速やかに住所地市区町村の窓口に出向き、書面により秘密鍵の漏えいがあった旨の届出を行う。

利用者証明利用者の本人確認は、「3.2.3.1.(2) 個人番号カード発行を伴わない利用者証明用電子証明書の発行申請」の手続に準じる。

3.4.3. 一時保留の届出

3.4.3.1. 利用者証明用電子証明書

利用者証明利用者は、電話により一時保留の届出を行う。利用者証明利用者の実在性確認は、基本4情報を使用して行う。

機構に個人番号カードの一時停止を届出を行うことで、当該個人番号カードに格納した利用者証明用電子証明書の一時保留を行うことができる。その場合、利用者証明利用者の本人確認は所定の本人確認手続による。

3.4.4. 一時保留解除の届出

住所地市区町村の窓口において、一時時保留解除の届出を行うことができる。その場合、利用者証明利用者の本人確認は所定の本人確認手続による。

4. 証明書のライフサイクルに関する運用上の要件

4.1. 証明書の申請

4.1.1. 証明書の申請者

4.1.1.1. 利用者証明用電子証明書

法第22条第1項の規定により、電子証明書の発行等を申請する者。（申請は代理人が行うこともできる。代理人による申請については、規則第41条第2項の要件を満たさなければならない。）

4.1.1.2. その他の証明書

その他の証明書の申請者は、所定の手続による。

4.1.2. 登録手続と責任

4.1.2.1. 利用者証明用電子証明書

⑴ 個人番号カード発行を伴う証明書発行申請・受付手続

申請者が、機構に発行申請書を送付する。

⑵ 個人番号カード発行を伴わない証明書発行申請・受付手続

申請者が、住所地市区町村に個人番号カードを添えて発行申請書を提出する。

⑶ 代理人による発行申請・受付手続

次の手続により、代理人による申請を行うことができる。ただし、①又は②において疑義が生じた場合は、利用者証明用電子証明書を発行しない。

① 代理人は、申請者本人の記名及び押印がある委任状及び代理人の本人性を確認するための規則第41条第2項第1号に定める本人確認書類を提示又は提出する。

② 代理人は、利用者証明用電子証明書の発行の申請について、申請者が本人であること及び当該申請が本人の意思に基づくものであることを確認するため、郵便その他住所地市区町村長が適当と認める方法により当該申請者に対して文書で照会したその回答書を提出するとともに、住所地市区町村長が適当と認める書類を提示する。

⑷ 発行申請書の様式、必要な記載事項

発行申請書には、次の事項を記載する。

・申請の年月日
・氏名（ふりがな）、住所、生年月日及び性別
・代理人申請の場合、上記に加え代理人の氏名、住所

4.1.2.2. その他の証明書

その他の証明書の発行申請は、所定の手続による。

4.2. 証明書申請手続

4.2.1. 識別と認証の実行

4.2.1.1. 利用者証明用電子証明書

住所地市区町村長は、申請者の実在性、本人性及び真正性を確認する。
確認の内容は「3.2.3.1.利用者証明用電子証明書」に規定する。

4.2.1.2. その他の証明書

その他の証明書の識別と認証は、所定の手続による。

4.2.2. 証明書申請の承認又は却下

4.2.2.1. 利用者証明用電子証明書

申請者の実在性、本人性及び真正性が確認された場合に、申請は処理される。

4.2.2.2. その他の証明書

その他の証明書の申請の承認又は却下は、所定の手続による。

4.2.3. 証明書申請の処理時間

規定しない。

4.3. 証明書の発行

4.3.1. 証明書発行手続

4.3.1.1. 利用者証明用電子証明書

⑴ 個人番号カード発行を伴う証明書発行手続

① 利用者証明用CAは申請に基づき、市区町村長が生成する申請者の鍵ペアを基に利用者証明用電子証明書を発行し、申請者の秘密鍵、利用者証明用電子証明書及び利用者証明用CAの自己署名証明書を、使用できない状態で申請者に交付する個人番号カードに格納して市区町村長に送付する。
② 市区町村長は、申請者に交付する個人番号カードに正常に格納されていることを確認する。

・ 既に有効又は一時保留状態の利用者証明用電子証明書を取得している場合は、重ねて発行を受けることはできない。
・ ただし、個人番号カードの発行を伴う利用者証明用電子証明書の発行時に、既に有効又は一時保留状態の利用者証明用電子証明書が存在する場合には、当該個人番号カードの交付の際に古い電子証明書を失効させることとし、使用できない状態で当該個人番号カードに格納する。

⑵ 個人番号カード発行を伴わない証明書発行手続

① 住所地市区町村長は利用者証明用CAに対して、申請書の内容等を通知する。
② 利用者証明用CAは、市区町村長が生成する申請者の鍵ペアを基に利用者証明用電子証明書を発行する。
③ 利用者証明用CAは、申請者の秘密鍵、利用者証明用電子証明書及び利用者証明用CAの自己署名用証明書を住所地市区町村長に通知する。

・ 既に有効又は一時保留状態の利用者証明用電子証明書を取得している場合は、重ねて発行を受けることはできない。

⑶ 電子証明書の形式

ITU-T勧告X.509 (03/2000)に準拠する。

4.3.1.2. その他の証明書

その他の証明書の発行は、所定の手続による。

4.3.2. 申請者に対する証明書発行通知

4.3.2.1. 利用者証明用電子証明書

個人番号カード発行を伴う発行の場合は、申請者に交付する個人番号カードに正常に格納されていることを確認し、申請者にカード交付通知書を発行することで、あるいは住所地市町村長の指定する場所に出頭して交付申請書を提出する場合は申請者に個人番号カードを交付又は送付することで、発行の通知とする。

また、個人番号カード発行を伴わない利用者証明用電子証明書の発行の場合は、利用者証明用電子証明書の交付によって発行の通知とする。

4.3.2.2. その他の証明書

その他の証明書の発行の通知は、所定の手続による。

4.4. 証明書の交付

4.4.1. 証明書交付手続

4.4.1.1. 利用者証明用電子証明書

⑴ 個人番号カード発行を伴う証明書交付手続

① 住所地市区町村長は、申請者の個人番号カードに申請者の秘密鍵、利用者証明用電子証明書及び利用者証明用CAの自己署名証明書を記録し、交付する。

② 住所地市区町村長は、利用者証明利用者に対して、本サービスの利用に関する重要な事項について説明する。また、利用者証明利用者が希望する場合には、利用者証明用電子証明書の写しを交付する。

⑵ 個人番号カード発行を伴う証明書交付手続（住所地市町村長の指定する場所に出頭して交付申請書を提出する場合）

① 住所地市区町村長は、申請者又は受け取りを指定された者に対して、申請者の個人番号カードに申請者の秘密鍵、利用者証明用電子証明書及び利用者証明用CAの自己署名証明書を記録し、交付又は送付する。

② 住所地市区町村長は、申請者又は受け取りを指定された者に対して、本サービスの利用に関する重要な事項について説明する。また、利用者証明利用者が希望する場合には、利用者証明用電子証明書の写しを交付する。

⑶ 個人番号カード発行を伴わない証明書交付手続

① 住所地市区町村長は、申請者の個人番号カードに申請者の秘密鍵、利用者証明用電子証明書及び利用者証明用CAの自己署名証明書を記録し、交付する。

② 住所地市区町村長は、利用者証明利用者に対して、本サービスの利用に関する重要な事項について説明する。また、利用者証明利用者が希望する場合には、利用者証明用電子証明書の写しを交付する。

⑷ 説明事項

住所地市区町村長は利用者証明利用者に次の事項を説明する。

- 秘密鍵、その電磁的記録媒体である個人番号カード、個人番号カードを活性化するためのパスワードは、利用者証明利用者の責任において厳重に管理すべきこと
- 秘密鍵又はその電磁的記録媒体である個人番号カードの紛失･盗難等の際は、速やかに、電話による個人番号カードの一時停止の届出による利用者証明用電子証明書の一時保留又は住所地市区町村窓口における届出を行うこと
- 虚偽の申請をして、不実の利用者証明用電子証明書を発行させた者は、法の規定により罰せられること

4.4.1.2. その他の証明書

利用者証明用CA は、発行した証明書を所定の手続に基づき、安全かつ確実な方法で配付する。

4.4.2. 認証局による証明書の公開

4.4.2.1. 利用者証明用電子証明書

利用者証明用CAは、利用者証明用電子証明書の公開を行わない。

4.4.2.2. その他の証明書

利用者証明用CAは、その他の証明書の公開を行わない。

4.4.3. その他の関係者に対する認証局の証明書発行通知

規定しない。

4.5. 鍵ペアと証明書の使用

4.5.1. 利用者証明利用者による秘密鍵及び証明書の使用

利用者証明利用者は、秘密鍵及び利用者証明用電子証明書を本運用規程「1.4.1.適切な証明書の利用用途」で規定する利用用途に即して利用しなければならない。

4.5.2. 利用者証明検証者による公開鍵及び証明書の使用

利用者証明検証者は、本運用規程「1.4.1.適切な証明書の利用用途」で規定された証明書の利用用途に即して利用しなければならない。

4.6. 証明書の更新

4.6.1. 証明書の更新事由

4.6.1.1. 利用者証明用電子証明書

鍵更新を伴わない利用者証明用電子証明書の更新は行わない。

4.6.1.2. その他の証明書

規定しない。

4.6.2. 更新の申請者

4.6.2.1. 利用者証明用電子証明書

規定しない。

4.6.2.2. その他の証明書

規定しない。

4.6.3. 証明書の更新申請手続

4.6.3.1. 利用者証明用電子証明書

規定しない。

4.6.3.2. その他の証明書

規定しない。

4.6.4. 利用者証明利用者に対する新たな証明書の発行通知

4.6.4.1. 利用者証明用電子証明書

規定しない。

4.6.4.2. その他の証明書

規定しない。

4.6.5. 更新された証明書の受領

4.6.5.1. 利用者証明用電子証明書

規定しない。

4.6.5.2. その他の証明書

規定しない。

4.6.6. 認証局による更新された証明書の公開

4.6.6.1. 利用者証明用電子証明書

規定しない。

4.6.6.2. その他の証明書

規定しない。

4.6.7. その他の関係者に対する認証局の証明書発行通知

規定しない。

4.7. 鍵更新を伴う証明書の更新

4.7.1. 鍵更新を伴う証明書の更新事由

4.7.1.1. 利用者証明用電子証明書

利用者証明用電子証明書の更新事由は次のとおりである。
・有効又は一時保留状態の利用者証明用電子証明書の有効期限が満了する場合

4.7.1.2. その他の証明書

規定しない。

4.7.2. 鍵更新を伴う更新の申請者

4.7.2.1. 利用者証明用電子証明書

鍵更新を伴う利用者証明用電子証明書の更新申請を行うことができる者は、本運用規程「4.1.1.1. 利用者証明用電子証明書」に準じる。

4.7.2.2. その他の証明書

その他の証明書の更新申請を行うことができる者は、本運用規程「4.1.1.2. その他の証明書」に準じる。

4.7.3. 鍵更新を伴う証明書の更新申請手続

4.7.3.1. 利用者証明用電子証明書

鍵更新を伴う証明書の更新は、利用者証明用電子証明書の失効手続及び発行手続により行う。

鍵更新を伴う証明書の更新に伴う失効手続は、本運用規程「4.9.証明書の失効と一時保留」の失効手続に準じる。証明書の発行手続は、本運用規程「4.1.証明書の申請」「4.2.証明書申請手続」「4.3.証明書の発行」の個人番号カード発行を伴わない証明書発行手続に準じる。ただし、鍵更新を伴う証明書更新の識別と認証の内容は、本運用規程「3.3.1.通常の鍵更新時の識別と認証」に規定する。

4.7.3.2. その他の証明書

その他の証明書の更新における発行申請、発行の各手続は、本運用規程「4.2.証明書申請手続」、「4.3.1.2. その他の証明書」に準じる。

4.7.4. 利用者証明利用者に対する新たな証明書の発行通知

4.7.4.1. 利用者証明用電子証明書

利用者証明用電子証明書更新における新しい証明書の発行通知の手続は、本運用規程「4.3.2.1. 利用者証明用電子証明書」に準じる。

4.7.4.2. その他の証明書

その他の証明書更新における新しい証明書の発行通知の手続は、本運用規程「4.3.2.2. その他の証明書」に準じる。

4.7.5. 鍵更新された証明書の受領

4.7.5.1. 利用者証明用電子証明書

鍵更新を伴う利用者証明用電子証明書の更新における受領の各手続は、本運用規程
「4.4.1.1. 利用者証明用電子証明書」の個人番号カード発行を伴わない証明書発行手続に準じる。

4.7.5.2. その他の証明書

その他の証明書の更新における受領の各手続は、本運用規程「4.4.1.2. その他の証明書」に準じる。

4.7.6. 認証局による鍵更新された証明書の公開

4.7.6.1. 利用者証明用電子証明書

鍵更新を伴う更新が行われた利用者証明用電子証明書の公開の手続は、本運用規程「4.4.2.1. 利用者証明用電子証明書」に準じる。

4.7.6.2. その他の証明書

更新が行われたその他の証明書の公開の手続は、本運用規程「4.4.2.2. その他の証明書」に準じる。

4.7.7. その他の関係者に対する認証局の証明書発行通知

規定しない。

4.8. 証明書の変更

規定しない。

4.9. 証明書の失効と一時保留

4.9.1. 証明書の失効事由

4.9.1.1. 利用者証明用電子証明書

⑴ 利用者証明利用者の申請又は届出に基づく失効の事由

利用者証明利用者の申請又は届出に基づく利用者証明用電子証明書の失効の事由は次のとおりである。

・ 利用者証明利用者が本サービスの利用を取りやめる旨の申請があった場合
・ 利用者証明利用者の秘密鍵が漏洩し、滅失し、若しくは毀損したとき、又は利用者証明用電子証明書を格納した個人番号カードが使用できなくなった旨の届出があったとき、又は個人番号カードを廃止した場合

⑵ 市区町村長が行う情報の記録に基づく失効の事由

市区町村長が行う情報の記録に基づく利用者証明用電子証明書の失効の事由は次のとおりである。

・ 住民票が消除された場合
・ 利用者証明利用者が転出届をしてから、三十日を経過しても転入届がない場合
・ 利用者証明用電子証明書に係る記録誤り又は記録漏れがあった場合

⑶ 機構が行う失効の事由

・ 利用者証明用CAの秘密鍵が危殆化した場合

4.9.1.2. その他の証明書

その他の証明書の失効の申請については、所定の手続による。

4.9.2. 証明書の失効申請者

4.9.2.1. 利用者証明用電子証明書

利用者証明用電子証明書の失効を申請できる者は以下のとおりである。

・ 利用者証明利用者又はその代理人

秘密鍵が漏洩し、滅失し、若しくは毀損したとき、又は利用者証明用電子証明書を格納した個人番号カードが使用できなくなった旨の届出ができる者は以下のとおりである。

・ 利用者証明利用者又はその代理人

利用者証明用電子証明書の失効につながる情報を記録できる者は以下のとおりである。

・ 市区町村長
・ 機構職員

4.9.2.2. その他の証明書

その他証明書の失効を申請できる者は、所定の手続による。

4.9.3. 証明書失効申請手続

4.9.3.1. 利用者証明用電子証明書

⑴ 利用者証明利用者の申請に基づく失効の手続

本サービスの利用を取りやめるための失効手続については、次のいずれかの方法で行う。

- 住所地市区町村の窓口へ、書面による失効申請と本人確認書類を提出及び提示する。市区町村長は機構に失効申請を通知する。失効処理の完了後、失効申請を受理した旨を記載した書面を利用者証明利用者に交付する。
- 利用者証明利用者の署名用電子証明書を用いて電子署名を付したオンラインによる失効申請を提出する。失効申請を受け付けた後、失効申請を受理した旨を利用者証明利用者にオンラインで通知する。

⑵ 利用者証明利用者の届出に基づく失効の手続

利用者証明利用者の秘密鍵が漏洩し、滅失し、若しくは毀損したとき、又は利用者証明用電子証明書を格納した個人番号カードが使用できなくなった旨の届出による失効については、次のいずれかの方法で行う。

- 住所地市区町村の窓口へ、書面による届出と本人確認書類を提出及び提示する。市区町村長は機構に届出を通知する。機構の失効処理の完了後、届出を受理した旨を記載した書面を利用者証明利用者に交付する。

⑶ 市区町村長が行う情報の記録による失効の手続

市区町村長が次の情報記録を行ったときには、利用者証明用CAは利用者証明用電子証明書の失効を行う。

・住民票の消除
・転出届をした後転入届をせず転出予定日から30日が経過した場合
・利用者証明用電子証明書に係る記録誤り又は記録漏れ

⑷ 機構が行う失効の手続

機構が次の状況を知った場合には、4.9.12.(1)の手続により、対象となる全ての電子証明書の失効を行う。

・利用者証明用CAの秘密鍵の危殆化

4.9.3.2. その他の証明書

その他の証明書の失効申請は、所定の手続による。

4.9.4. 失効申請の猶予期間

失効の申請は、失効すべき事象が発生してから速やかに行われる。

4.9.5. 認証局が失効申請を処理しなければならない期間

利用者証明用CAは、失効申請手続の終了後、速やかに失効処理を行う。
なお、利用者証明用CAの発行した証明書の失効処理に当たっては、その失効処理の取消しは行わない。
証明書を失効した利用者証明用利用者に対して再度証明書を発行する場合は、あらためて発行手続を行う。

4.9.6. 利用者証明検証者等の失効確認の要求

利用者証明用電子証明書の有効性を確認する方法として次の2つの方法を提供する。

① OCSPレスポンダ照会方法（RFC2560に規定されているOCSPプロトコルを利用）
② 失効記録（CRL/ARL）提供方法（RFC2251に規定されているLDAPV3プロトコルを利用）

4.9.7. 失効記録(CRL/ARL)発行頻度

有効期間72時間の失効記録（CRL/ARL）を24時間ごとに発行する。ただし、利用者証明用CAの秘密鍵の危殆化等が発生した場合には、失効記録（CRL/ARL）を直ちに発行する。

4.9.8. 証明書失効リストの発行最大遅延時間

発行した失効記録を速やかにリポジトリに公開する。

4.9.9. オンラインでの失効ステータス確認の適用性

許可された利用者証明検証者等へのOCSPレスポンダ照会の提供は、24時間365日利用可能とする。ただし、定期保守作業等により一時的に利用できない場合もある。

利用者証明用電子証明書の発行者を識別する情報とシリアル番号によるオンラインの照会に対して、照会のあった時点における当該利用者証明用電子証明書の

有効、不明及び失効の別、並びに失効している場合は失効事由を回答する。失効事由は、以下のとおり。

失効事由		
0	unspecified	交付前に破棄した
1	keyCompromise	利用者証明利用者の秘密鍵が危殆化した
2	cACompromise	利用者証明用CAの秘密鍵が危殆化した
3	affiliationChanged	利用者証明用電子証明書の記載内容に変更が生じた
4	superseded	利用者証明用電子証明書を更新した
5	cessationOfOperation	利用者証明用電子証明書の必要性がなくなった（使用しなくなった）
6	certificateHold	秘密鍵の安全性に疑義が生じたため、証明書を一時的に保留した

4.9.10. オンラインでの失効ステータス確認を行うための要件

事前に機構まで届け出て、アクセス権の付与を受けることが必要である。

4.9.11. 他の利用可能な失効通知の形式

規定しない。

4.9.12. 鍵の危殆化に伴う対応

⑴ 利用者証明用CAの秘密鍵の危殆化が発生した場合

利用者証明用CAの秘密鍵の危殆化が発生した場合、当該秘密鍵で署名されたすべての電子証明書を失効させ、失効記録（CRL/ARL）に記録するとともに、Web等により、その旨を公表する。

⑵ 利用者証明利用者の秘密鍵の危殆化が発生した場合

利用者証明利用者の秘密鍵の危殆化の場合の失効手続は次のとおり行う。

① 住所地市区町村の窓口において書面による失効の届出を行う。
② 市区町村長は機構に失効の届出を通知する。機構は失効処理を行い、市区町村長に通知する。市区町村長は失効処理を完了した旨を記載した書面を利用者証明利用者に交付する。

⑶ その他の証明書に係る秘密鍵の危殆化が発生した場合

その他の証明書に係る秘密鍵の危殆化が発生した場合、所定の手続により証明書を失効させ、失効記録（CRL）に記録する。

4.9.13. 証明書の一時保留の事由

利用者証明用電子証明書の一時保留事由は次のとおりである。

・ 利用者証明用電子証明書を格納した個人番号カードの紛失等により、利用者証明利用者の秘密鍵が漏洩した恐れがあると、利用者証明利用者から連絡があり、個人番号カードの一時停止を行った場合

なお、利用者証明用電子証明書の一時保留解除の届出は住所地市区町村の窓口において行う。

4.9.14. 証明書の一時保留及び一時保留解除の届出を行う者

利用者証明用電子証明書の一時保留の届出及び一時保留解除の届出を行うことができる者は以下のとおりである。

・ 利用者証明利用者又はその代理人

4.9.15. 証明書の一時保留及び一時保留解除の手続

① 利用者証明利用者は、個人番号カードを紛失した場合、機構に電話により、個人番号カードの一時停止を届け出ることで、当該個人番号カードに格納された利用者証明用電子証明書の一時保留について届出を行ったものとする。
② 利用者証明用CAは、当該利用者証明用電子証明書を特定し、速やかに一時保留する。
③ 利用者証明利用者は、住所地市町村窓口で一時保留解除の届出を行う。
④ 市町村長は、申請を行った利用者証明利用者の実在性、本人性及び真正性が確認された場合に、申請は処理される。
⑤ 利用者証明用CAは、当該利用者証明用電子証明書を特定し、速やかに一時保留を解除する。

4.9.16. 一時保留期間

一時保留を継続できる期間は、当該利用者証明用電子証明書の有効期間内とする。

4.10. 証明書状態サービス

規定しない。

4.11. 登録の終了

利用者証明用電子証明書の有効期間が満了し、又は利用者証明用電子証明書が失効された結果、有効な電子証明書をもたなくなった利用者証明利用者は、利

用者証明用電子証明書の利用を終了したものとみなされる。

4.12. 秘密鍵の預託と回復

規定しない。

5. 物理面、管理面、運用面のセキュリティ管理

5.1. 物理面のセキュリティ管理

5.1.1. 立地場所及び構造

5.1.1.1. 認証局の施設

利用者証明用CAの施設は、水害、地震、火災その他の災害や不正侵入を考慮した立地及び構造とする。

5.1.1.2. 登録局の施設

登録局の端末設備は、住所地市区町村に設置される。

5.1.2. 物理的アクセス

5.1.2.1. 認証局の施設

利用者証明用CAの施設内の各室内において行われる業務の重要度に応じ、複数のセキュリティレベルで入退室管理を行う。入退室管理の認証は、操作権限者が識別できるICカード及び生体認証装置により行う。

各室への入退室権限は、本運用規程「5.2.手続面のセキュリティ管理」において定める各要員の業務に応じて、利用者証明用CAの認証局管理責任者が付与する。

利用者証明用CAの施設は、監視員を配置し、監視システムにより24時間365日監視を行う。

5.1.2.2. 登録局の施設

登録局の施設は市区町村の職員の人的監視が行き届く場所に設置する。また、受付窓口端末（CS統合端末のこと。以下同じ。）に係わる保守を適切に行う。

受付窓口端末の操作は申請者等の本人確認等を行う者が実施する。

電子証明書の発行・失効の事務に係る操作者の認証は生体認証方式、事務支援に係る操作者の認証はID/パスワード方式により行う。

5.1.3. 電源及び空調

利用者証明用CAは、機器等の運用のために十分な容量の電源を確保するとともに、瞬断、停電、電圧・周波数の変動に備えた対策を講じる。商用電源が供給されない事態においては、一定時間内に発電機による電源供給に切り替える。

空調設備を設置することにより、機器類の動作環境及び要員の作業環境を適切に維持する。

5.1.4. 水害対策

利用者証明用CAの設備を設置する建物、室には漏水検知機を設置し、天井、床には防水対策を講じる。

5.1.5. 地震対策

利用者証明用CAの設備を設置する建物は制震構造とし、機器･什器の転倒及び落下を防止する対策を講じる。

5.1.6. 火災防止及び火災保護対策

利用者証明用CAの設備を設置する建物は耐火構造、室は防火区画とし、消火設備を備える。

5.1.7. 媒体保管場所

5.1.7.1. 認証局の施設

保管情報、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場所に保管するとともに、所定の手続に基づき適切に搬入出管理を行う。

5.1.7.2. 登録局の施設

本運用規程「5.5.1 アーカイブ記録の種類」に係わる書類は、適切な場所に保管する。

5.1.8. 廃棄物処理

5.1.8.1. 認証局の施設

秘密扱いとする情報を含む書類･記憶媒体については、所定の手続により適切に廃棄処理を行う。

5.1.8.2. 登録局の施設

秘密扱いとする情報を含む書類･記憶媒体及び受付窓口端末等の廃棄については、所定の手続により適切に廃棄処理を行う。

5.1.9. オフサイトバックアップ

規定しない。

5.1.10. 電磁波対策

利用者証明用CAの施設内の各室内において行われる業務の重要度に応じて、電磁波攻撃及び電磁波からの情報漏えいを防ぐ設備を備える。

5.2. 手続面のセキュリティ管理

5.2.1. 信頼すべき役割

5.2.1.1. 利用者証明用 CA における要員

⑴ 認証局管理責任者

認証局管理責任者は、利用者証明用CAの運営に関する責任者であり次の業務を行う。

- 認証業務の統括
- 利用者証明用CAの秘密鍵の危殆化発生及び災害発生時等緊急時における対応の統括
- 要員等への重要な作業の指示及び作業結果の確認
- HSM（利用者証明用CAの秘密鍵を安全に管理する装置）の機能を制御する鍵（以下「管理鍵」という。）の保管及び管理
- 認証業務情報開示請求に対する対応の管理
- 認証業務情報訂正等請求に対する対応の管理
- 問合せ･苦情処理対応の管理
- 認証業務情報保護委員会の開催
- 認証業務等に係る帳簿の備付け
- 失効情報等の提供状況報告書の作成と公示
- 入退室管理
- 準拠性監査への対応及びその指摘事項に対する是正の実施管理
- その他利用者証明用CAの運営及び運用に関する統括
- 個人情報の管理

⑵ 秘密鍵管理者

秘密鍵管理者は、利用者証明用CAの秘密鍵等を使用する業務に関する責任者であり、次の業務を行う。

- HSMの活性化及び非活性化
- 利用者証明用CAの秘密鍵等のバックアップ媒体の保管管理
- 利用者証明用CAの秘密鍵等生成、自己署名証明書発行時のHSMに対する操作
- 利用者証明用CAの秘密鍵等の更新時におけるHSMに対する操作

・ 利用者証明用CAの秘密鍵等のバックアップ、バックアップからのリストア時のHSMに対する操作

⑶ 受付担当者

受付担当者は、その他の証明書の発行、更新及び失効申請の受付を行う。

⑷ 審査担当者

審査担当者は、その他の証明書の発行、更新及び失効申請の審査を行う。

⑸ 審査承認者

審査承認者は、審査担当者からのその他の証明書の発行申請、更新申請及び失効申請の審査の承認を行う。

⑹ 上級操作員

上級操作員は、利用者証明用CAの秘密鍵を使用する次の業務とリポジトリの設定管理に関する業務、利用者証明用CAの運用及び維持管理を行う。

・ 利用者証明用CAの自己署名証明書発行、更新、失効処理
・ OCSPレスポンダ証明書発行、更新、失効処理
・ SSL証明書発行、更新、失効処理
・ 利用者証明用CA電子証明書等ポリシーの設定登録及び変更
・ リポジトリの設定管理に関する業務
・ その他利用者証明用CAシステムの運用管理業務

⑺ 一般操作員

一般操作員は、利用者証明用CAの運用及び維持管理を行う。

⑻ 内部監査者

内部監査者は、利用者証明用CAシステムのログに関する次の業務を行う。

・ 監査ログの検査
・ 監査済みログの削除

5.2.1.2. 登録局における要員

登録局における要員は、電子証明書の発行･失効時における厳格な本人確認及び発行･失効に係わる事務、並びにこれらの事務に用いる機器等の適切な管理等を行う。

5.2.2. 職務ごとに必要とされる人数

秘密鍵管理者及び上級操作員は、「5.2.1 信頼すべき役割」において定める各作業を複数人で行う。

5.2.3. 個々の役割に対する識別と認証

5.2.3.1. 利用者証明用 CA における各要員の識別と認証要件

- 各要員がシステム操作を行う際、システムは運用要員が正当な権限者であることの識別・認証を行う。
- 各要員の認証はICカードやパスワードを用いて実施する。パスワードは定期的に変更する。
- 各要員がその役割に応じてアクセスできる秘密情報は最小限に抑える。

5.2.4. 職務権限の分離が必要な役割

5.2.4.1. 利用者証明用 CA における各要員の職務権限の分離と作業の指示方法

各要員が行う職務権限の分離と作業の指示方法につき次のように定める。

① 権限の分離

人的セキュリティの観点から所定の手続に基づき、職務を分離した上で、権限を付与された複数人の要員によって、施設の運用・管理を行う。

② 認証局管理責任者の権限

重要な業務の指示は、認証局管理責任者が各要員に対して、所定の手続により指示する。

③ 上級操作員の権限

上級操作員は一般操作員等に対し、所定の手続に基づいた各種作業に対する指示及び結果の確認を行う。また、要員の権限に応じた登録及び証明書を発行する。

5.3. 利用者証明用 CA における人事面のセキュリティ管理

5.3.1. 経歴、資格、経験等に関する要求事項

利用者証明用CAの業務に従事する者は、役割と責任に応じて、PKI、セキュリティ等の業務遂行に必要な知識、経験を有する者とする。

5.3.2. 要員の個人の背景のチェックと認可手順

所要の審査手順に従い、雇用前に書類（履歴書、推薦状等）検査により経歴調

査を実施する。

5.3.3. 各要員に対する教育訓練要件

教育訓練計画書に従い、各要員に必要な訓練を実施する。
教育訓練計画書では教育訓練要件、教育訓練の周期について規定する。

5.3.4. 各要員に対する教育訓練の周期

利用者証明用ＣＡは、要員に対し必要に応じて教育･訓練を実施する。また、業務内容、手順等の変更並びに指揮命令系統、責任及び権限の変更が行われた場合、教育･訓練を実施する。

5.3.5. 要員間の業務交代と周期、順序

認証局管理責任者が文書により、業務のローテーション方法を規定する。

5.3.6. 許可されていない行動に対する罰則

各要員が職務権限に違反する行動を行った場合には、所定の手続に基づき処分を行う。

5.3.7. 各要員に対する契約要件

業務の一部を委託する場合は、委託先との間で委託業務に関する機密保持義務等を含む適切な契約を締結する。機構は外部委託先の要員が本運用規程で規定される要件に照らして十分な要件を満たしていることを事前に確認する。

5.3.8. 各要員に提供される文書

各要員は、それぞれのアクセス権に応じて文書（運用手順書、操作手順書等）を閲覧することが可能である。

5.4. 監査ログの手続

内部監査者（本運用規程「5.2.1. 信頼すべき役割」を参照）は、利用者証明用CAシステムにおけるセキュリティに関する重要な事項を対象としたアクセスログや操作ログ等の発生事象の記録（以下、「監査ログ」という）を業務実施記録等と照合し、不正操作等異常な事象を確認するセキュリティ監査を行う。

5.4.1. 監査ログに記録する情報

利用者証明用CAシステムは、以下の監査ログを記録する。

・ 発行手続に関する操作･稼動ログ
・ 失効手続に関する操作･稼動ログ
・ 有効性確認に関するすべてのアクセス･稼動ログ
・ 利用者証明用CAの鍵ペア生成に関する操作ログ
・ システム、各種帳簿等に対するアクセスログ
・ 利用者証明用CAの設備への入退室記録

監査ログには次の情報を含める。
・ 事象又は処理の種類
・ 発生日時
・ 処理の結果
・ 事象の発生元の識別情報（操作員ID、システム名等）

5.4.2. 監査ログの検査周期

内部監査者はセキュリティ監査を定期的に行う。

5.4.3. 監査ログの保管期間

1年間保管する。

5.4.4. 監査ログの保護

監査ログは、改ざん防止対策を施す。また、監査ログのバックアップは月次で外部記憶媒体等に取得し、適切な入退出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。
なお、監査ログの閲覧及び削除は内部監査者が適切に行う。

5.4.5. 監査ログのバックアップ手順

日次でバックアップし、月次で外部記憶媒体等に取得する。

5.4.6. 監査ログの収集システム

監査ログの収集機能は、利用者証明用CAシステムの一機能とし、セキュリティに関する重要な事象をシステムの起動時から監査ログとして収集する。

5.4.7. 監査ログ検査の通知

監査ログの検査は、その事象を発生させた者に通知することなく行う。

5.4.8. 脆弱性評価

定期的に、運用面及びシステム面におけるセキュリティ上の脆弱性を評価する。

5.5. 記録の保管（アーカイブ）

5.5.1. アーカイブ記録の種類

5.5.1.1. 紙で保管する情報

次の情報を保管する。

⑴ 利用者証明用CA

- 本運用規程の作成に関する書類
- キーセレモニーの実施等に関する書類
- 利用者証明検証者等との取決めに関する書類
- 認証業務情報の開示・訂正等に関する書類
- 監査報告書等
- 認証事務管理規程
- 設備及び安全対策に関する書類
- 事業計画・予算に関する書類
- 事業報告書・決算書
- 失効情報及び失効情報ファイルの提供状況の報告書
- 手数料に関する書類等

⑵ 市区町村長

- 利用者証明用電子証明書の発行及び更新申請に関する書類（発行申請書等）
- 利用者証明用電子証明書の失効申請に関する書類（失効申請書等）
- 認証業務情報の開示・訂正等に関する書類等
- 利用者証明用電子証明書の更新申請に関する書類（更新申請書等）
- 利用者証明用電子証明書の一時保留解除の届出に関する書類（一時保留解除届等）

5.5.1.2. デジタルデータとして保管する情報

⑴ 利用者証明用CA

- 利用者証明用電子証明書の発行記録
- 失効申請書（機構へのオンライン申請の場合）
- 利用者証明用電子証明書失効申請等情報等
- 利用者証明用電子証明書
- 利用者証明用CAの自己署名証明書
- リンク証明書

・ OCSPレスポンダ証明書
・ SSL証明書
・ 失効情報
・ 失効記録
・ 失効情報ファイル（CRL/ARL）
・ 失効情報ファイル（CRL/ARL）提供履歴
・ OCSPレスポンダ照会履歴
・ 各種ログ（監視用ログ、起動停止ログ、操作ログ）等

⑵ 市区町村長

委託先の機構にて次のデータを保管する。
・ 利用者証明用電子証明書の発行申請書
・ 利用者証明用電子証明書の一時保留の届出に関する記録

5.5.2. アーカイブ保存期間

5.5.2.1. 紙で保管する情報

規則第80条第1号又は第7号に基づき保管する。

5.5.2.2. デジタルデータとして保管する情報

電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律施行令第18条から第23条まで、規則第80条第1号又は第7号に基づき保管する。

5.5.3. アーカイブの保護

5.5.3.1. 紙で保管する情報

利用者証明用CA及びに保管する情報は、適切な入退出管理が行われている室内に設置された施錠可能な場所に保管し、温度、湿度等環境に配慮した保護対策を施す。市区町村に保管する情報は、適切な場所に保管する。

5.5.3.2. デジタルデータとして保管する情報

保管情報には、アクセス制御を施す。
保管情報は、定期的に外部記憶媒体等に取得し、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。

5.5.4. アーカイブのバックアップ手続

5.5.4.1. デジタルデータとして保管する情報

保管情報は、日次でバックアップし、月次で外部記憶媒体等に取得する。

5.5.5. 記録に付与するタイムスタンプの要件

5.5.5.1. デジタルデータとして保管する情報

保管情報には、タイムスタンプ（時刻情報）を付与する。

5.5.6. アーカイブ収集システム

規定しない。

5.5.7. 保管情報の検証

5.5.7.1. 紙で保管する情報

保管情報が記載された紙の保管環境の記録を行い、紙の状態の確認を年1回行う。

5.5.7.2. デジタルデータとして保管する情報

保管情報が記録された外部記憶媒体等の可読性の確認を、年1回行う。

5.6. 利用者証明用 CA の鍵の更新

4年ごとに利用者証明用CAの鍵ペアの更新を行う。
鍵ペア更新時には、古い公開鍵と新しい公開鍵の認証パスを構築するリンク証明書を発行し、リポジトリ上で公開する。

5.7. 鍵の危殆化と災害復旧

5.7.1. 事故及び危殆化の取扱手続

利用者証明用CAは事故及び危殆化が発生した場合に速やかに業務を復旧できるよう、以下を含む事故及び危殆化に対する対応手続（以下、「緊急時対応計画」という。）を策定する。

- ハードウェア、ソフトウェア、データ等の破損、故障
- 利用者証明用CA秘密鍵の危殆化
- 火災、地震等の災害

5.7.2. ハードウェア、ソフトウェア又はデータが破壊された場合の対処

ハードウェア、ソフトウェア又はデータが破壊された場合、バックアップ用のハードウェア、ソフトウェア又はデータにより、速やかに復旧作業を行う。

5.7.3. 利用者証明用 CA の秘密鍵が危殆化した場合の手順

緊急時対応計画に従い対処する。主な対処は次のとおり。

① 利用者証明用電子証明書の発行業務を停止。
② その秘密鍵により署名したすべての利用者証明用電子証明書を失効させ、失効記録（CRL/ARL）に記録して、公表する。

5.7.4. 災害発生時の設備の確保

災害等により設備が被害を受けた場合は、緊急時対応計画に従い運用を行う。

5.8. 認証業務の終了

規定しない。

6. 技術面のセキュリティ管理

6.1. 鍵ペアの生成とインストール

6.1.1. 鍵ペアの生成

6.1.1.1. 利用者証明用 CA の鍵ペアの生成

利用者証明用CAの鍵ペアは、複数人の秘密鍵管理者がFIPS140-2 レベル3相当のHSMを用いて生成する。

6.1.1.2. 利用者証明利用者の鍵ペアの生成

利用者証明利用者の鍵ペアは、市区町村長からの通知により、機構の設置管理する利用者証明用CAがFIPS140-2レベル3相当のHSMを用いて生成する。

6.1.1.3. その他の証明書に係る鍵ペアの生成

その他の証明書に係る鍵ペアは、所定の手続により生成する。

6.1.2. 秘密鍵の配付

6.1.2.1. 利用者証明利用者に対する秘密鍵の配付

申請者の秘密鍵は、利用者証明用電子証明書の発行の際に申請者の個人番号カードに格納し、申請者に交付する。

6.1.2.2. その他の証明書に係る秘密鍵の配付

規定しない。

6.1.3. 認証局への公開鍵の配付

6.1.3.1. 利用者証明用電子証明書

申請者の公開鍵は、市区町村長からの通知により、利用者証明用CAに設置した機器で生成する。

6.1.3.2. その他の証明書

利用者証明用CAへの公開鍵の配付については、所定の手続により行う。

6.1.4. 認証局公開鍵の配付

利用者証明用CAの自己署名証明書は、利用者証明用電子証明書の発行の際に個人番号カードに格納し、利用者証明利用者に交付する。また、安全かつ確実な手段で利用者証明検証者等に配布する。

6.1.5. 鍵サイズ

6.1.5.1. 利用者証明用 CA の鍵の鍵長

RSA暗号方式に基づく2048ビットの鍵を使用する。

6.1.5.2. 利用者証明利用者の鍵の鍵長

RSA暗号方式に基づく2048ビットの鍵を使用する。

6.1.5.3. その他の証明書に係る鍵長

RSA暗号方式に基づく2048ビットの鍵を使用する。

6.1.6. 公開鍵パラメータの生成及び品質検査

規定しない。

6.1.7. 鍵用途の目的

6.1.7.1. 利用者証明用 CA の秘密鍵の利用目的

電子署名用とする。

6.1.7.2. 利用者証明利用者の秘密鍵の利用目的

電子利用者証明用とする。

6.1.7.3. その他の証明書に係る秘密鍵の利用目的

所定の手続により定める。

6.2. 秘密鍵の保護と暗号モジュールの技術管理

6.2.1. 暗号モジュールの標準及び管理

6.2.1.1. 利用者証明用 CA の秘密鍵の保管について、要求される基準

FIPS140-2 レベル3相当のHSMにより保護する。

6.2.1.2. 利用者証明利用者の秘密鍵の保管について、要求される基準

利用者証明利用者の秘密鍵は、物理的に読み出せない個人番号カードの耐タンパ性により保護する。

6.2.1.3. その他の証明書の係る秘密鍵の保管について、要求される基準

所定の手続により保護する。

6.2.2. 秘密鍵の複数人制御

6.2.2.1. 利用者証明用 CA の秘密鍵の複数人制御

利用者証明用CAの秘密鍵は、複数人の秘密鍵管理者により制御するHSMで秘密鍵を保護する。

6.2.2.2. その他の証明書に係る秘密鍵の複数人制御

所定の手続により保護する。

6.2.3. 秘密鍵の預託（エスクロー）

6.2.3.1. 利用者証明用 CA の秘密鍵の預託

利用者証明用CAの秘密鍵の預託は行わない。

6.2.3.2. 利用者証明利用者の秘密鍵の預託

利用者証明用CAが利用者証明利用者の秘密鍵の預託を受けることは行わない。また利用者証明利用者がその秘密鍵を第三者等に預託することを認めない。

6.2.3.3. その他の証明書に係る秘密鍵の預託

その他の証明書に係る秘密鍵の預託は行わない。

6.2.4. 秘密鍵のバックアップ

6.2.4.1. 利用者証明用 CA の秘密鍵のバックアップ

利用者証明用CAの秘密鍵のバックアップは、複数人の秘密鍵管理者による操作で行う。

HSMからバックアップした秘密鍵は、HSM内及び耐タンパ機能を有する記録媒体に暗号化して安全に保管する。ただし秘密鍵管理者は、バックアップ媒体を保管することとされている室の外に持ち出してはならない。

6.2.4.2. 利用者証明利用者の秘密鍵のバックアップ

利用者証明利用者の秘密鍵は、個人番号カード内に保管し、バックアップは行わない。

6.2.4.3. その他の証明書に係る秘密鍵のバックアップ

所定の手続による。

6.2.5. 秘密鍵のアーカイブ

秘密鍵のアーカイブは行わない。

6.2.6. 秘密鍵の暗号モジュールへの転送

利用者証明用CAの秘密鍵の転送は行わない。

利用者証明利用者の秘密鍵の転送は、暗号化した状態で通信及び個人番号カードへの格納を行い、復号化は個人番号カード内で行う。

6.2.7. 暗号モジュールへの秘密鍵の格納

6.2.7.1. ＨＳM内の暗号モジュールへの利用者証明用 CA の秘密鍵の格納

利用者証明用CAの秘密鍵は、複数人の秘密鍵管理者による操作でHSMの中で生成し、HSM内の暗号モジュールへ格納する。

6.2.7.2. 個人番号カード内の暗号モジュールへの利用者の秘密鍵の格納

利用者証明利用者の秘密鍵は、利用者証明用CAの安全な環境下において生成及び暗号化され、暗号化した秘密鍵は住所地市区町村へ転送され、利用者証明利用者の個人番号カードに格納後、個人番号カード内部で復号される。暗号化した秘密鍵は、転送後、利用者証明用CAから完全に削除される。また、個人番号カードへの格納後、暗号化したデータは住所地市区町村から完全に削除される。

6.2.7.3. 暗号モジュールへのその他の証明書に係る秘密鍵の格納

所定の手続による。

6.2.8. 秘密鍵の活性化方法

6.2.8.1. 利用者証明用 CA の秘密鍵の活性化方法

秘密鍵は複数人の秘密鍵管理者による操作により活性化する。

6.2.8.2. 利用者証明利用者の秘密鍵の活性化方法

利用者証明利用者の秘密鍵は、利用者証明利用者により、パスワードを用いて活性化する。

また、利用者証明検証者により、認証業務及びこれに附帯する業務の実施に関する技術的基準（平成15年総務省告示第706号）第4条第2項の規定に基づき総務大臣が指定する方法が実施される場合についても、利用者証明利用者の秘密鍵は活性化する。

6.2.8.3. その他の証明書に係る秘密鍵の活性化方法

所定の手続による。

6.2.9. 秘密鍵の非活性化方法

6.2.9.1. 利用者証明用 CA の秘密鍵の非活性化方法

秘密鍵は複数人の秘密鍵管理者による操作により非活性化する。

6.2.9.2. 利用者証明利用者の秘密鍵の非活性化方法

個人番号カードの操作により非活性化する。

6.2.9.3. その他の証明書に係る秘密鍵の非活性化方法

所定の手続による。

6.2.10. 秘密鍵の破棄方法

6.2.10.1. 利用者証明用 CA の秘密鍵の破棄方法

暗号モジュール内の秘密鍵の破棄は、複数人の秘密鍵管理者により暗号モジュールを初期化する等の方法により、完全に利用できない状態にする。
また、破棄する秘密鍵のバックアップ用暗号モジュールも同様に破棄する。

6.2.10.2. 利用者証明利用者の秘密鍵の破棄方法

利用者証明利用者の秘密鍵の破棄を行う場合、利用者証明利用者は住所地市区町村の受付窓口端末で破棄する。

6.2.10.3. その他の証明書に係る秘密鍵の破棄方法

所定の手続による。

6.2.11. 暗号モジュールの評価

本運用規程「6.1.1.鍵ペアの生成」及び「6.2.1.暗号モジュールの標準及び管理」において定める。

6.3. 鍵ペア生成管理に関する他の局面

6.3.1. 公開鍵のアーカイブ

6.3.1.1. 利用者証明用 CA の公開鍵のアーカイブ

利用者証明用CAの公開鍵は自己署名証明書に含まれ、改ざん防止措置を施されたアーカイブに、本運用規程「5.5.記録の保管（アーカイブ）」において定める期間、保管する。

6.3.1.2. その他の証明書に係る公開鍵のアーカイブ

その他の証明書に係る公開鍵は証明書のアーカイブに含まれ、本運用規程「5.5.記録の保管（アーカイブ）」において定める期間保管する。

6.3.2. 公開鍵証明書の有効期間と鍵ペアの使用期間

6.3.2.1. 利用者証明用 CA の公開鍵証明書の有効期間と鍵ペアの使用期間

利用者証明用CAの自己署名証明書の有効期間は10年とする。OCSPレスポンダ証明書の有効期間は5年とする。利用者証明用CAの秘密鍵の使用期間は、鍵を生成した日から起算して4年以内に鍵更新を行う。

ただし、暗号方式が脆弱になったと判断した場合は、暗号方式の変更を検討しその時点で鍵更新を行う場合がある。

6.3.2.2. 利用者証明利用者の公開鍵証明書の有効期間と鍵ペアの使用期間

利用者証明利用者の公開鍵と秘密鍵の使用期間は、利用者証明用電子証明書の発行の日から次に掲げる日のうちいずれか早い日までとする。

① 発行の日後の利用者証明利用者の五回目（発行を受けている利用者証明用電子証明書の有効期間が満了する日までの期間が三月未満となった場合において、法第 28 条第 1 項の規定による当該利用者証明用電子証明書の失効を求める旨の届出及び法第 22 条第 1 項の規定による新たな利用者証明用電子証明書の発行の申請をし、当該新たな利用者証明用電子証明書の発行を受けるときにあっては、六回目）の誕生日までとする。

② 当該利用者証明用電子証明書が記録された個人番号カードの有効期間が満了する日までとする。

ただし、暗号方式が脆弱になったと判断した場合は、暗号方式の変更を検討しその時点で鍵更新を行う場合がある。

6.3.2.3. その他の証明書の有効期間と鍵ペアの使用期間

利用者証明用CAが発行するSSL証明書は、インターネット上で使用する場合、有効期間及び秘密鍵の使用期間は1年とする。インターネット上以外で使用する場合、有効期間及び秘密鍵の使用期間は5年以内とする。

6.4. 活性化データ

6.4.1. 活性化データの生成及び設定

6.4.1.1. 利用者証明用 CA の秘密鍵の活性化データの生成及び設定

利用者証明用CAの秘密鍵を格納するHSMの活性化データは、管理鍵により設定する。

6.4.1.2. 利用者証明利用者の秘密鍵の活性化データの生成及び設定

利用者証明利用者の秘密鍵の活性化データ（パスワード）は、利用者証明利用者自身が住所地市区町村窓口の受付窓口端末にて、電子証明書交付時に個人番号カードへ設定する。

6.4.1.3. その他の証明書に係る秘密鍵の活性化データの生成及び設定

その他の証明書に係る秘密鍵の活性化データは、所定の手続により生成、インストールする。

6.4.2. 活性化データの保護

6.4.2.1. 利用者証明用 CA の秘密鍵の活性化データの保護

利用者証明用CAの秘密鍵を格納するHSMの活性化に必要な管理鍵は安全に保管する。

6.4.2.2. 利用者証明利用者の秘密鍵の活性化データの保護

利用者証明利用者の秘密鍵の活性化データは、定期的に変更し、安全に保管しなければならない。
また、利用者証明検証者により、認証業務及びこれに附帯する業務の実施に関する技術的基準（平成15年総務省告示第706号）第4条第2項の規定に基づき総務大臣が指定する方法が実施される場合については、利用者証明検証者により活性化に必要なデータは保護される。

6.4.2.3. その他の証明書に係る秘密鍵の活性化データの保護

その他の証明書に係る秘密鍵の活性化データの保護は、所定の手続による。

6.4.3. 活性化データの他の考慮点

規定しない。

6.5. コンピュータセキュリティ管理

6.5.1. コンピュータのセキュリティに関する技術的要件

利用者証明用CAに係るシステムには、信頼されるOSの使用、アクセス制御、各要員の識別と認証機能、監査ログ及びアーカイブデータの収集機能及びシステムのリカバリ機能等を備える。

6.5.2. コンピュータセキュリティ評価

システムのセキュリティ評価を随時実施する。

6.6. ライフサイクルセキュリティ管理

6.6.1. システム開発管理

本サービスに係るシステムの開発、修正又は変更に当たっては、所定の手続に基づき、信頼できる組織及び環境下において作業を実施する。開発、修正又は変更したシステムは、テスト環境において検証を行い、認証局管理責任者の承認を得たうえで導入する。また、システム仕様及び検証報告については、文書化し保管する。

6.6.2. セキュリティ運用管理

6.6.2.1. 認証局

本サービスに係るシステムを維持管理するため、OS及びソフトウェアのセキュリティチェックを定期的に行う。また、この検証結果を文書化し保管する。

6.6.2.2. 登録局

本サービスに係るシステムを維持管理するため、受付窓口端末等のOS及びソフトウェアのセキュリティ管理を適切に行う。

6.6.3. ライフサイクルのセキュリティ管理

機構は、利用者証明用CAのシステム開発、運用、保守が適切に行われていることを監査等を通じて適宜評価し、必要に応じ改善を行う。

6.7. ネットワークセキュリティ管理

不正アクセスを防止するため、外部ネットワークの通過を許可するネットワークサービスは必要最小限とする。また、不正侵入検知等の十分なセキュリティ保護対策を行う。

リポジトリに保有する情報のうち公開する情報は、ファイアウォールを介して提供する。

6.8. タイムスタンプ

利用者証明用CAは、信頼される時刻源を使用してシステムの時刻同期を行い、システム内で記録される重要な情報に対しレコード単位でタイムスタンプを付与する。

7. 証明書と失効記録(CRL/ARL)のプロファイル

7.1. 証明書のプロファイル

証明書のプロファイルは、プロファイル設計書に定める。

なお、利用者証明用電子証明書、利用者証明用CAの自己署名証明書及びリンク証明書には下記の情報を記載する。

⑴ 利用者証明用電子証明書

- バージョン番号(X.509証明書フォーマットのバージョン番号)
- シリアル番号(利用者証明用CA内で発行済み証明書を識別するための番号)
- 署名アルゴリズム(利用者証明用CAが当該利用者証明用電子証明書へ署名する際に用いたアルゴリズム情報)
- 発行者情報(当該利用者証明用電子証明書を発行した機構名がX.500識別名で記述される)
- 有効期間の開始日(当該利用者証明用電子証明書の発行日)
- 有効期間の終了日(規則第48条に定める有効期間の満了する日(「6.3.2.2. 公開鍵証明書の有効期間と鍵ペアの使用期間」を参照)
- 公開鍵(利用者証明利用者の公開鍵)
- 拡張情報(利用者証明利用者の鍵使用目的等が記載される)

⑵ 自己署名証明書

- バージョン番号(X.509証明書フォーマットのバージョン番号)
- シリアル番号(利用者証明用CA内で発行済み証明書を識別するための番号)
- 署名アルゴリズム(利用者証明用CAが当該自己署名証明書へ署名する際に用いたアルゴリズム情報)
- 発行者情報(当該自己署名証明書を発行した機構名がX.500識別名で記述される)
- 有効期間の開始日(当該自己署名証明書の発行日)
- 有効期間の終了日(発行日の10年後)
- 公開鍵(利用者証明用CAの公開鍵)
- 拡張情報

⑶ リンク証明書

- バージョン番号(X.509証明書フォーマットのバージョン番号)
- シリアル番号(利用者証明用CA内で発行済み証明書を識別するための番号)
- 署名アルゴリズム(利用者証明用CAが当該リンク証明書へ署名する際に用いたアルゴリズム情報)

・ 発行者情報（当該リンク証明書を発行した機構名がX.500識別名で記述される）
・ 有効期間の開始日（OldWithNew：旧世代の鍵ペアを生成した日、NewWithOld：新世代の鍵ペアを生成した日）
・ 有効期間の終了日（OldWithNew：旧世代の自己署名証明書の有効期限の終了日、NewWithOld：旧世代の自己署名証明書の有効期限の終了日）
・ 公開鍵（OldWithNew：旧世代の利用者証明用CAの公開鍵、NewWithOld：新世代の利用者証明用CAの公開鍵）
・ 拡張情報

7.2. 失効記録（CRL/ARL）のプロファイル

失効記録（CRL/ARL）のプロファイルは、技術仕様書に定める。
なお、失効記録（CRL/ARL）には下記の情報を記載する。

⑴ 利用者証明用電子証明書の失効記録（CRL）

・ バージョン番号（CRLのフォーマットのバージョン番号）
・ 署名アルゴリズム（利用者証明用CAが当該CRLへ署名する際に用いたアルゴリズム情報）
・ 発行者情報（当該CRLを発行した機構名がX.500識別名で記述される）
・ 有効期間の開始日（当該CRLを有効とする日）
・ 有効期間の終了日（当該CRLを有効とする日から起算して3日後）
・ 次の更新予定日（当該CRLを有効とする日の1日後）
・ 失効した証明書情報（シリアル番号、失効年月日、失効事由）
・ 拡張情報

⑵ 自己署名証明書の失効記録（ARL）

・ バージョン番号（ARLのフォーマットのバージョン番号）
・ 署名アルゴリズム（利用者証明用CAが当該ARLへ署名する際に用いたアルゴリズム情報）
・ 発行者情報（当該ARLを発行した機構名がX.500識別名で記述される）
・ 有効期間の開始日（当該ARLを有効とする日）
・ 有効期間の終了日（当該ARLを有効とする日から起算して3日後）
・ 次の更新予定日（当該ARLを有効とする日の1日後）
・ 失効した証明書情報（シリアル番号、失効年月日、失効事由）
・ 拡張情報

⑶ リンク証明書の失効記録（ARL）

・ バージョン番号（ARLのフォーマットのバージョン番号）
・ 署名アルゴリズム（利用者証明用CAが当該ARLへ署名する際に用いたアルゴリズム情報）
・ 発行者情報（当該ARLを発行した機構名がX.500識別名で記述される）

・ 有効期間の開始日（当該ARLを有効とする日）
・ 有効期間の終了日（当該ARLを有効とする日から起算して3日後）
・ 次の更新予定日（当該ARLを有効とする日の1日後）
・ 失効した証明書情報（シリアル番号、失効年月日、失効事由）
・ 拡張情報

7.3. OCSP のプロファイル

OCSPのプロファイルは、技術仕様書に定める。

8. 準拠性監査

8.1. 監査の頻度

機構は監査人により年1回定期的準拠性監査を実施する。また、定期監査以外に随時監査を必要に応じて実施する。

8.2. 監査人の要件

利用者証明用CAの監査は、監査業務及び認証業務に精通した者が行う。

8.3. 監査人と被監査人の関係

機構は、利用者証明用CAと利害関係を有しない者を監査人として選定する。

8.4. 監査項目

認証業務が法、関連法令、本運用規程等に準拠して実施されていることの監査を実施する。

8.5. 監査指摘事項への対応

機構は監査指摘事項を確認し、重要性又は緊急性に応じて適切な是正措置を行う。

8.6. 監査結果の取扱い

監査結果は、監査人から機構に対して監査報告書として提出される。

9. 他の業務上及び法的事項

9.1. 手数料

機構は、利用者証明用電子証明書の発行、利用者証明用電子証明書の失効情報及び失効情報ファイルの提供、対応証明書の発行の番号の提供並びに認証業務情報の開示に係る手数料を、法の規定等に基づき総務大臣の認可を受けて定める。

9.2. 財務上の責任

機構は、利用者証明用CAに責を帰すべき事由のない行為によって発生した損害については、一切損害賠償責任を負わないものとする。

9.2.1. 保険の適用範囲

規定しない。

9.2.2. その他の資産

規定しない。

9.2.3. 利用者証明利用者を保護する保険、保証

規定しない。

9.3. 事業情報の秘匿性

9.3.1. 秘密情報の範囲

以下の事項を含む、漏えいすることによって利用者証明用CAの認証業務の信頼性が損なわれる恐れのある情報は機密扱いとする。

- 利用者証明用電子証明書の発行、発行記録、失効情報及び失効情報ファイル並びにそれらに係る電子計算機処理に関する秘密
- 利用者証明用電子証明書の提供に係る電子計算機処理等に関する秘密

9.3.2. 秘密情報の範囲外の情報

利用者証明用CAの自己署名証明書、リンク証明書、OCSPレスポンダ証明書、それらの証明書の失効情報、本運用規程等に加え、法の規定に基づき公表する失効情報、失効情報ファイル及び対応証明書の発行の番号の提供状況に関する報告書は機密扱いとしない。

9.3.3. 秘密情報を保護する責任

機構は、機密扱いとする情報について、当該情報を含む書類及び電磁的記憶媒体の管理責任者を定め、安全に管理する。

9.4. 個人情報の保護

9.4.1. 個人情報保護計画

機構は、機構の「個人情報保護基本方針」に基づき個人情報を適切に保護する。

9.4.2. 個人情報として扱われる情報

認証業務の実施のために申請者又は利用者証明利用者から取得した個人情報である。

9.4.3. 個人情報と見なされない情報

規定しない。

9.4.4. 個人情報を保護する責任

機構、市区町村長、利用者証明検証者は、関係法令に基づき個人情報を適切に保護する。
機構は、当該個人情報を含む書類及び電磁的記憶媒体の管理責任者を定め安全に管理する。

9.4.5. 個人情報の使用に関する個人への通知及び承諾

機構、市区町村長、利用者証明検証者は、関係法令に基づき個人情報を適切に使用する。認証業務以外の目的で個人情報を使用する場合は、関係法令で除外されている場合を除き、あらかじめ本人の同意を得るものとする。

9.4.6. 司法手続又は行政手続に基づく公開

司法機関、行政機関の決定、命令、勧告等があった場合は、機構は情報を開示することができる。

9.4.7. 他の情報公開の場合

9.4.7.1. 利用者証明利用者の請求に基づく情報開示

利用者証明利用者から自己の認証業務情報の開示請求があった場合は、機構は本人確認を実施の上、開示する。

9.4.7.2. 利用者証明利用者の請求に基づく情報の訂正等

利用者証明利用者から自己の認証業務情報の訂正等請求があった場合は、機構は本人確認を実施の上、訂正等を行う。

9.4.7.3. その他の理由に基づく情報開示

規定しない。

9.5. 知的財産権

規定しない。

9.6. 表明保証

9.6.1. 機構の表明保証

機構は、利用者証明用CAによる認証業務の実施に当たり以下の事項を保証する。

- 法の規定に基づき、利用者証明認証業務を適切に行うこと
- 利用者証明用電子証明書及びその失効は本運用規程の定めに基づくこと

9.6.2. 登録局の表明保証

市区町村長は認証業務の実施に当たり以下の事項を保証する。

- 法の規定に基づき、申請者が住民基本台帳に記録されている者であることの確認を含む利用者証明認証業務を適切に行うこと

9.6.3. 利用者証明利用者の表明保証

利用者証明利用者は以下の事項を保証する。

- 秘密鍵の漏えい、滅失及び毀損の防止その他秘密鍵の適切な管理を行うこと等の法の規定に基づく利用者証明利用者の責務を果たすこと
- 利用者証明用電子証明書の発行申請書、失効申請書等に正確な内容を記載すること
- 利用者証明用電子証明書の発行を受けた利用者証明利用者が当該利用者

証明用電子証明書に記録された利用者証明利用者の公開鍵に対応した利用者証明利用者の秘密鍵により生成された電子利用者証明を用いること

9.6.4. 利用者証明検証者の表明保証

9.6.4.1. 利用者証明検証者の表明保証

利用者証明検証者は以下の事項を保証する。

- 法の規定に基づき、利用者証明認証業務を適切に行うこと
- 法の規定に基づき機構と締結する取決めに基づき、利用者証明用電子証明書等の情報の適切な管理を行うこと

9.7. 保証の免責事項

規定しない。

9.8. 責任の制限

機構は、利用者証明用CAに責を帰すべき事由のない行為によって発生した損害については、一切損害賠償責任を負わないものとする。

9.9. 補償

規定しない。

9.10. 有効期間と終了

9.10.1. 有効期間

本運用規程は、機構の理事長の承認により有効となる。
「9.10.2 終了」に規定する終了以前に本運用規程が無効となることはない。

9.10.2. 終了

本運用規程は、「9.10.3 終了の効果と効果継続」に規定する内容を除き利用者証明用CAを終了した時点で無効となる。

9.10.3. 終了の効果と効果継続

利用者証明利用者が利用者証明用電子証明書の利用を終了する場合、又は利用者証明用CAの業務を終了する場合であっても、「9.3 事業情報の秘匿性」、「9.4 個人情報の保護」及び「9.14 準拠法」の規定は、終了の事由を問わず利用者証明利用者、利用者証明検証者、機構に適用されるものとする。

9.11. 関係者との個別通知と伝達

運営体制等に変更がある場合には以下の方法で速やかに公表する。
・機構のWeb

9.12. 改訂

9.12.1. 改訂手続

機構は、本運用規程を必要に応じて変更する。

9.12.2. 通知方法及び期間

本運用規程を変更した場合には、機構は速やかに変更した運用規程を機構のWeb上で公表する。これをもって利用者証明利用者、利用者証明検証者への通知とする。

9.12.3. オブジェクト識別子が変更されなければならない場合

規定しない。

9.13. 紛争解決手順

本運用規程に関して生じた訴訟の際、すべての当事者は東京地方裁判所を第一審の専属管轄裁判所とする。

9.14. 準拠法

日本国の法令に準拠する。

9.15. 適用可能な法への準拠性

日本国の法令に準拠する。

9.16. 雑則

規定しない。

9.17. 他の条項

規定しない。

付録　用語集

項番	用語・略語	説明
1	ARL	(Authority Revocation List) 有効期間中に、失効された自己署名証明書及び相互認証証明書のリスト。
2	CP	(Certificate Policy) 証明書ポリシー。認証局が各証明書を発行する際の運用方針を定めた文書。
3	CPS	(Certification Practice Statement) 認証実施規程。認証局の信頼性、安全性を対外的に示すために、認証局の運用、証明書ポリシー、鍵の生成、管理、責任等に関して定めた文書。CPが何を運用方針にするかを示すのに対して、CPSは運用方針をどのように適用させるかを示す。
4	CRL	(Certificate Revocation List) 無効になった証明書の一覧表、公的個人認証サービスでは、有効期間中に、失効された利用者の電子証明書等の失効情報を掲載する。
5	CS端末	住民基本台帳ネットワークシステムにおいて、コミュニケーションサーバを利用した業務処理を行う端末。
6	HSM	(Hardware Security Module) 不正アクセスに備えるための機能（耐タンパー機能）を保有した秘密鍵の管理装置。耐タンパー機能とは、不正アクセスに対してその侵入の痕跡を残したり、データを消去する機能であり、不正アクセスの証拠を残す不正顕示機能、不正アクセスからデータを防護する不正防護機能、不正アクセスに対してデータを消去する対抗動作を行う不正対抗機能等がある。
7	RFC	インターネットに関する標準文書の総称。 RFC2459:X.509の様式。すべてのCRLで予期される情報の基本セットを定義。頻繁に使用される属性のCRL内での共通の位置や、それらの属性の共通表記方法も定義。 RFC2527：CP又はCPSを作成するためのフレームワーク及びガイドラインを提供。 RFC2560：CRLの要求なしに現在のデジタル証明書の状態を決定するために便利なプロトコル（OCSP）を定義。 RFC3280：RFC2459の改訂版。 RFC3647：RFC2527の改訂版。
8	RSA	(Rivest-Shamir-Adleman) 現在最も一般的な公開鍵暗号方式。十分に大きな2つの素数を掛け合わせた数の素因数分解が難しいことを暗号強度の根拠としている。
9	鍵ペア	公開鍵暗号方式における公開鍵と秘密鍵のペア。一方の鍵から他方の鍵を導き出せない性質を持つため、一方（秘密鍵）の秘密を保ったまま、他方（公開鍵）を公開することができる。
10	官職証明書	ある公開鍵が、記載された処分権者が使用するものであることを保証する電子的な文書。
11	危殆化	信頼性が喪失された可能性のある事態の発生をいう。認証局の場合、認証局の秘密鍵が危殆化することによって、発行したすべての証明書の信頼性が失われる。
12	キーセレモニー	認証局の鍵ペアを生成するための実行される一連の手続きのこと。
13	公開鍵	公開鍵暗号方式において用いられる鍵ペアの一方。秘密鍵に対応する、公開されている鍵。
14	個人番号カード	氏名、住所、生年月日、個人番号、その者の写真その他その者を識別する事項のうち政令で定める事項が記載されたカード。 公的個人認証サービスが発行する署名用電子証明書と利用者証明用電子証明書が格納される。
15	自己署名証明書	自認証局の公開鍵に対して、自認証局の秘密鍵で署名した証明書。
16	リポジトリ	(Repository) 各種証明書及びCRL／ARLを格納し、提供するデータベース。公的個人認証サービスでは、ディレクトリサーバを使用する。
17	リンク証明書	認証局の鍵更新に伴い同時に存在することとなる新しい認証局の鍵ペアと古い認証局の鍵ペアの関係を保証するための証明書。
18	サーバ証明書	Webサーバの実在性を証明するために発行された電子証明書。
19	識別名（DN）	特定のオブジェクトを一意に識別するための文字列。
20	代替文字	住民基本台帳ネットワークシステムで使用する文字の中には一般的なPCで利用できない文字が存在する。それらの文字を、一般的なPCで取り扱い可能な文字に置き換えた文字。