カード代替電磁的記録管理用_ルート認証局
運用規程

第 1 版
2025 年 6 月 24 日

地方公共団体情報システム機構
デジタル庁

発行/改定日

版数	改定日	改訂箇所
1.00	2025 年（令和 7 年）6 月 24 日発行	初版

カード代替電磁的記録管理用_ルート認証局 0
運用規程 0
1 はじめに 5

1.1 概要 5
1.2 文書名と識別 5
1.3 関係者 6
1.4 電子証明書の利用用途 7
1.5 ポリシー運用管理 7
1.6 定義と略語 8

2 公開とリポジトリの責任 11

2.1 リポジトリ 11
2.2 電子証明書情報の公開 11
2.3 公開の時期又はその頻度 11
2.4 リポジトリへのアクセス管理 11
2.5 リボジトリを管理する組織 11

3 識別と認証 12

3.1 名称決定 12
3.2 初回の電子証明書発行申請時の識別と認証 12
3.3 鍵更新時の識別と認証 13
3.4 失効申請時の識別と認証 13

4 電子証明書のライフサイクルに関する運用上の要件 15

4.1 電子証明書の申請 15
4.2 電子証明書申請の処理手順 15
4.3 電子証明書の発行 15
4.4 電子証明書の交付 15
4.5 鍵ペアと電子証明書の使用 16
4.6 電子証明書の更新 17
4.7 鍵更新を伴う電子証明書の更新 17
4.8 電子証明書の変更 17
4.9 電子証明書の失効と一時停止 18
4.10 電子証明書状態サービス 20
4.11 登録の終了 20
4.12 秘密鍵の預託と回復 20

5 物理面、管理面、運用面のセキュリティ管理 21

5.1 物理面のセキュリティ管理 21

5.2 手続面のセキュリティ管理 22
5.3 認証局における人事管理面のセキュリティ管理 24
5.4 監査ログの手続 25
5.5 記録の保管（アーカイブ） 27
5.6 認証局の鍵の更新 29
5.7 鍵の危殆化と災害復旧 29
5.8 ルート認証局の運営の終了 30

6 技術面のセキュリティ管理 31

6.1 鍵ペアの生成とインストール 31
6.2 秘密鍵の保護と暗号モジュールの技術管理 31
6.3 鍵ペア生成管理に関する他の局面 33
6.4 活性化データ 33
6.5 コンピュータセキュリティ管理 33
6.6 ライフサイクルセキュリティ管理 34
6.7 ネットワークセキュリティ管理 34
6.8 タイムスタンプ 34

7 電子証明書及び失効記録（CRL）のプロファイル 35

7.1 電子証明書のプロファイル 35
7.2 失効記録（CRL）のプロファイル 37
7.3 OCSP のプロファイル 37

8 準拠性監査 38

8.1 監査員 38
8.2 監査の頻度 38
8.3 監査人の要件 38
8.4 監査人と被監査組織の関係 38
8.5 監査項目 38
8.6 監査指摘事項への対応 38
8.7 監査結果の取扱い 38

9 他の業務上及び法的事項 39

9.1 手数料 39
9.2 財務上の責任 39
9.3 事業情報の秘匿性 39
9.4 個人情報の保護 39
9.5 知的財産権 40
9.6 表明保証 40

9.7 保証の免責事項 41
9.8 責任の制限 41
9.9 補償 41
9.10 有効期間と終了 42
9.11 関係者との個別通知と伝達 42
9.12 改訂 42
9.13 紛争解決手順 42
9.14 準拠法 42
9.15 適用可能な法への準拠性 43
9.16 雑則 43
9.17 他の条項 43

1 はじめに

本運用規程は、「行政手続における特定の個人を識別するための番号の利用等に関する法律」（以下「法」という。）で定める「カード代替電磁的記録」によって、移動端末設備及び確認用プログラムの連携により法上の本人確認等を可能にするため、移動端末設備上に個人番号カードの情報を格納し、発行・管理するシステムのルート認証局（以下「ルート認証局」という。）について、そのセキュリティと運用の実務を記述する証明書ポリシー（CP）及び認証実務規定（CPS）である。

住民と国又は地方公共団体の機関等との間の申請・届出等手続時の本人確認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、法に基づき、地方公共団体情報システム機構（以下「機構」という。）は発行主体として、カード代替電磁的記録を発行する役割を担う。

本運用規程は、このルート認証局における電子証明書の発行、管理及び失効、並びにこの電子証明書の電子証明書利用者と検証者によって充足されるべき要件と責任について説明する。

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

本運用規程は、その実務と管理がどのように実施されるか、以下の標準を基に示す。

- RFC 3647 -Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework 【RFC3647】
- RFC 5280 - Internet X.509 PKI - Certificate and CRL Profile 【RFC5280】
- ISO/IEC 18013-5:2021 - Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence （mDL） application 【ISO/IEC 18013-5】

ルート認証局は、CP 及び CPS をそれぞれ独立したものとせず、本運用規程をルート認証局の運営方針として位置付ける。

本運用規程では、運用に関するセキュリティポリシーを規定し、運用の詳細は、運用手順書等に規定する。

1.2 文書名と識別

本運用規程の識別子は、次の電子証明書ポリシー及び識別子によって表される。

- ルート認証局の自己署名電子証明書ポリシーの識別子
  1.2.392.200149.23220.1.7

・　リンク証明書ポリシーの識別子

1.2.392.200149.23220.1.4

・　カード代替電磁的記録用 Document Signer の電子証明書（以下「DS 電子証明書」という。）ポリシーの識別子

1.2.392. 200149.23220.1.2

1.3 関係者

1.3.1 ルート認証局

次に示す電子証明書を発行する。

- ルート認証局の自己署名電子証明書
- リンク証明書
- DS 電子証明書

1.3.2 電子証明書利用者

1.3.2.1 申請者／電子証明書利用者

申請者とは、電子証明書の発行を申請する者をいう。

電子証明書利用者とは、ルート認証局が発行する電子証明書を管理し、本運用規程に従って電子証明書を利用する者をいう。

1.3.3 検証者

検証者とは、ルート認証局が発行する電子証明書の有効性確認手段の提供を受け、電子署名を検証する者をいう。

1.3.4 その他の関係者

1.3.4.1 Digital Trust Service

ルート認証局が発行する信頼できる X.509v3 電子証明書や電子証明書失効情報などを共有するためのサービスをいう。ルート認証局で生成した電子証明書関連ファイルの管理と、検証者への各種電子証明書の公開を行う。

1.3.4.2 ルート認証局の運営に関する意思決定機関

ルート認証局の運営に関する意思決定は機構及びデジタル庁が行い、電子証明書発行及び運用に関する状況の管理の事務は機構が行う。

これには、機構及びデジタル庁の認証局管理責任者と、ルート認証局の運用管理及びセキュリティ運用を担当するスタッフが含まれる。

1.4 電子証明書の利用用途

1.4.1 適切な電子証明書の利用用途

ルート認証局の発行する電子証明書の種類及び用途は、次のとおり。

① 自己署名電子証明書

ルート認証局の完全性と真正性を確認する手段の提供

② リンク証明書

鍵更新時の新しい鍵の有効性を確認する手段の提供

③ DS 電子証明書

MSO への署名と、カード代替電磁的記録用 Document Signer の完全性と真正性を確認する手段の提供

1.4.2 禁止される電子証明書の利用用途

法で制限されている用途や、「1.4.1 適切な電子証明書の利用用途」以外の目的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、機構及びデジタル庁とする。

1.5.2 連絡先

本運用規程に関する照会は、機構を窓口とする。

窓口の連絡先は、以下の URL に掲示する。

URL： https://www.j-lis.go.jp/pn/mdociaca.html

1.5.3 運用規程承認手続

ルート認証局運用規程は、機構及びデジタル庁の決定をもって有効なものとする。

1.6 定義と略語

単語、略語、頭字語	意味
CA（Certification Authority：認証局）	電子証明書の発行・更新・失効、MSO への署名・更新・失効、認証局等秘密鍵の生成・保護を行う機関。
CP（Certificate Policy：証明書ポリシー）	認証局が各電子証明書を発行する際の運用方針を定めた文書。
CPS（Certification Practices Statement：認証実施規程）	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。
DTS（Digital Trust Service）	認証局が発行する信頼できる X.509v3 電子証明書や電子証明書失効情報などを共有するためのサービス。ルート認証局で生成した電子証明書関連ファイルの管理と、検証者への各種電子証明書の公開を行う。
ECDSA（Elliptic Curve Digital Signature Algorithm）	「楕円曲線暗号方式」参照。
FIPS140-3	NIST（National Institute of Standards and Technology：米国標準技術研究所）が策定した米国連邦情報処理標準のうち、暗号技術に関するセキュリティ要件を規定しているもの。 コンピュータと通信システムの暗号モジュールに対して暗号技術に関する汎用要件を網羅しており、最低レベル 1 から最高レベル 4 までのセキュリティレベルが設定されている。
HSM（Hardware Security Module）	不正アクセスに備えるための機能（耐タンパ機能）を保有した秘密鍵の管理装置。耐タンパ機能とは、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検知機能、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。

MSO（Mobile Security Object）	カード代替電磁的記録内で各データ項目の情報のハッシュ値を配列として格納する Mobile Security Object をいう。カード代替電磁的記録に存在する各データ要素のメッセージダイジェストを計算し、全てのダイジェスト及びカード代替電磁的記録利用者の Device Key 公開鍵を MSO に含める。カード代替電磁的記録用 Document Signer は、カード代替電磁的記録用 Document Signer の秘密鍵を使用して MSO に電子署名する。 X.509 における電子証明書相当の機能を持つ。
RA（Registration Authority：登録局）	次の機能の 1 つ又は複数を担うエンティティ：電子証明書申請者の識別と認証、電子証明書申請の承認又は拒否、特定の状況下での電子証明書の失効の申立、電子証明書の失効を求める電子証明書利用者の要求処理、鍵更新を伴う電子証明書の更新を求める電子証明書利用者の要求の承認又は拒否。ただし、RA は電子証明書の発行は行わない（すなわち、RA は認証局の代わりに特定のタスクを委任される）。
移動端末設備	電気通信事業法（昭和五十九年法律第八十六号）第 12 条の 2 第 4 項第 2 号ロに規定する移動端末設備。
カード代替電磁的記録用 Document Signer	カード代替電磁的記録に対して、電子署名を付与するエンティティを指し、X.509 における下位認証局相当の機能を持つ。
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）を秘密にすることで、他方（公開鍵）を公開することができる。
確認用プログラム	法第 18 条の 4 第 1 号から第 3 号に規定する機能を有するプログラムをいう。
ガバメントクラウド	政府共通のクラウドサービスの利用環境。国の全ての行政機関や地方公共団体が共同で行政システムをクラウドサービスとして利用できるようにした IT 基盤。
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、発行した全ての電子証明書及び署名し

	た全ての MSO の信頼性が失われる。
キーセレモニー	認証局の鍵ペアを生成するために実行される一連の手続のこと。
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。
個人番号カード	氏名、住所、生年月日、性別、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。
識別名（Distinguished Name）	特定のオブジェクトを一意に識別するための文字列。
自己署名電子証明書	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電子証明書。
プロファイル	電子証明書及び CRL に含まれるデータの内容を定義したもの。【ISO/IEC18013-5】にて準拠すべき電子証明書及び CRL のプロファイルが定義されている。
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電子証明書。
楕円曲線暗号方式	楕円曲線上で定義された加減演算を使用して計算を行う暗号方式。パラメータを変えることにより、強度を保つ必要がある。

2 公開とリポジトリの責任

2.1 リポジトリ

ルート認証局に関する情報は、DTS 及び機構の Web 上で公表する。

2.2 電子証明書情報の公開

ルート認証局は、機構の Web 上で次の情報を公開する。

- 本運用規程
- ルート認証局の秘密鍵の危殆化に係る情報等
- カード代替電磁的記録用 Document Signer の秘密鍵の危殆化に係る情報等
- ルート認証局の自己署名電子証明書のフィンガープリント
- ルート認証局の自己署名電子証明書（バイナリ形式）

ルート認証局は、DTS 上で、次の情報を公開する。

- ルート認証局の自己署名電子証明書
- リンク証明書
- 電子証明書失効情報（CRL: Certificate Revocation List）

なお、失効事由の詳細は公表しない。

2.3 公開の時期又はその頻度

公開する情報の更新頻度は次のとおりとする。

- ルート認証局の自己署名電子証明書、リンク証明書は、発行・更新の都度公開する。
- 失効記録（CRL）は、「4.9.7 失効記録（CRL）発行頻度」に定める頻度とする。
- 法、関係法令、本運用規程等は最新版を機構の Web 上に掲載する。

2.4 リポジトリへのアクセス管理

DTS 上で公表する情報及び機構の Web 上で公表する情報については、特段のアクセス制御は行わない。

2.5 リポジトリを管理する組織

リポジトリを管理する組織は機構とする。

3 識別と認証

3.1 名称決定

3.1.1 名称の種類

3.1.1.1 ルート認証局が発行する電子証明書

ルート認証局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

電子証明書の発行名義人名は、機構名を記録する。

発行する電子証明書において使用する名前は、認証局等の名称とする。

機構が発行する電子証明書の名称は決定されており、電子証明書が使用される組織又はサービスを表す。

3.1.3 電子証明書利用者の匿名性又は仮名性

電子証明書利用者の匿名、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

ルート認証局が発行する各電子証明書に関する命名は、【ITU-T X.509】関連仕様の X.500 識別名の規定に従い処理する。

3.1.5 名称の一意性

ルート認証局が発行する電子証明書の主体者名に含まれる情報により、電子証明書利用者を一意に識別できることを保証する。

3.1.6 商標の認識・認証・役割

規定しない。

3.2 初回の電子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 ルート認証局の自己署名電子証明書

ルート認証局の秘密鍵の所有は、キーセレモニーに参加する、信頼すべき役割を持つ参加者によって保証される。

3.2.1.2 リンク証明書

ルート認証局の秘密鍵の所有は、キーセレモニーに参加する、信頼すべき役割を持つ参加者によって保証される。

3.2.1.3 DS 電子証明書

カード代替電磁的記録用 Document Signer の秘密鍵の所有は、キーセレモニーに参加する、信頼すべき役割を持つ参加者によって保証される。

3.2.2 組織の認証

3.2.2.1 ルート認証局の自己署名電子証明書

ルート認証局の自己署名電子証明書は、ルート認証局の発行主体と同一組織によって申請される。

3.2.2.2 リンク証明書

リンク証明書は、ルート認証局の発行主体と同一組織によって申請される。

3.2.2.3 DS 電子証明書

DS 電子証明書は、ルート認証局の発行主体と同一組織によって申請される。

3.2.3 個人の認証

規定しない。

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 ルート認証局の自己署名電子証明書

「3.2.2.1 ルート認証局の自己署名電子証明書」に準じる。

3.3.1.2 リンク証明書

「3.2.2.2 リンク証明書」に準じる。

3.3.1.3 DS 電子証明書

「3.2.2.3 DS 電子証明書」に準じる。

3.3.2 電子証明書失効後の鍵更新時の識別と認証

3.3.2.1 ルート認証局の自己署名電子証明書

「3.2.2.1 ルート認証局の自己署名電子証明書」に準じる。

3.3.2.2 リンク証明書

「3.2.2.2 リンク証明書」に準じる。

3.3.2.3 DS 電子証明書

「3.2.2.3 DS 電子証明書」に準じる。

3.4 失効申請時の識別と認証

3.4.1 サービスの利用をやめるための失効申請

3.4.1.1 ルート認証局の自己署名電子証明書

「3.2.2.1 ルート認証局の自己署名電子証明書」に準じる。

3.4.1.2 リンク証明書

「3.2.2.2 リンク証明書」に準じる。

3.4.1.3 DS 電子証明書

「3.2.2.3 DS 電子証明書」に準じる。

3.4.2 電子証明書利用者の秘密鍵の危殆化の場合の届出

所定の手続により速やかに危殆化した旨の届出を行う。

3.4.3 一時停止の届出

規定しない。

4 電子証明書のライフサイクルに関する運用上の要件

4.1 電子証明書の申請

4.1.1 電子証明書の申請者

DS 電子証明書は、ルート認証局の発行主体と同一組織によって申請される。

4.1.2 登録手続と責任

当該申請者は、正確な情報を申請するものとする。

・

4.2 電子証明書申請の処理手順

4.2.1 識別と認証の実行

ルート認証局は、「3.2.1 秘密鍵の所有を証明する方法」において定める手続を実施し、申請内容が適切であることを確認する。

4.2.2 電子証明書申請の承認又は却下

電子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 電子証明書の処理時間

規定しない。

4.3 電子証明書の発行

4.3.1 電子証明書発行手続

ルート認証局は、カード代替電磁的記録用 Document Signer が作成した電子的な電子証明書発行要求を基にルート認証局の署名を付して DS 電子証明書を発行する。

4.3.2 DS 電子証明書の登録手続及び責任

DS 電子証明書の発行申請は運用保守責任者および秘密鍵管理者により行われ、当該運用保守責任者は、正確な情報を申請するものとする。

4.3.3 申請者に対する電子証明書発行通知

電子証明書の交付によって電子証明書利用者への発行通知とする。

4.4 電子証明書の交付

4.4.1 DS 電子証明書の交付

4.4.1.1 交付

① ルート認証局が署名して DS 電子証明書を生成後、カード代替電磁的記録に格納して、申請者に交付する。

② 機構及びデジタル庁は、カード代替電磁的記録の利用者に対して、DS 電子証明書の利用に関す

る重要な事項について通知する。また、DS 電子証明書の記録事項を提示する。

4.4.1.2 説明事項

機構は申請者に次の事項を説明する。

- 秘密鍵、その電磁的記録媒体は、申請者の責任において厳重に管理すべきこと。
- 秘密鍵の漏えい時は、速やかに所定の手続による DS 電子証明書の失効申請を行うこと。
- 失効した DS 電子証明書が格納されている MSO は、すべて失効処理を行い、失効した MSO に格納されている DeviceKey の公開鍵が MSO Revocation List に載ること。但し、MSO の有効期限切れの場合は MSO Revocation List には公開鍵は載らない。
- 虚偽の申請をして、不実の DS 電子証明書を発行させないこと。

4.4.2 認証局による電子証明書の公開

4.4.2.1 ルート認証局の自己署名電子証明書

DTS 上で公開する。

4.4.2.2 リンク証明書

DTS 上で公開する。

4.4.2.3 DS 電子証明書

DS 電子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電子証明書発行通知

規定しない。

4.5 鍵ペアと電子証明書の使用

4.5.1 電子証明書利用者による秘密鍵及び電子証明書の使用

電子証明書利用者は、秘密鍵及び電子証明書を本運用規程「1.4.1 適切な電子証明書の利用用途」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 検証者による公開鍵及び電子証明書の使用

検証者は、公開鍵及び電子証明書を本運用規程「1.4.1 適切な電子証明書の利用用途」で規定する利用用途に即して利用しなければならない。

また検証者が電子証明書の利用を適切と判断した場合、検証者は

（1）【ITU-T X.509】で規定されているルート認証局の自己署名証明書と DS 証明書の証明書検証パスを検証しなければならない。

（2）【ISO/IEC 18013-5】で規定されている MSO に格納されている DS 電子証明書を検証しなければならない。

4.6 電子証明書の更新

鍵更新を伴わない電子証明書の更新は行わない。

4.7 鍵更新を伴う電子証明書の更新

4.7.1 鍵更新を伴う電子証明書の更新事由

有効な DS 電子証明書の有効期間が満了する場合

4.7.2 鍵更新を伴う更新の申請者

鍵更新を伴う DS 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 電子証明書の申請者」に準じる。

4.7.3 鍵更新を伴う DS 電子証明書の更新

鍵更新を伴う DS 電子証明書の更新は、DS 電子証明書の失効手続及び発行手続により行う。鍵更新を伴う電子証明書の更新に伴う失効手続は、本運用規程「4.9.3 電子証明書申請の処理手順」の失効手続に準じる。電子証明書の発行手続は、本運用規程「4.1 電子証明書の申請」「4.2 電子証明書申請の処理手順」「4.3 電子証明書の発行」の手続に準じる。ただし、鍵更新を伴う電子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。

認証局は自身が発行した電子証明書のみを更新するものとする。

4.7.4 電子証明書利用者に対する新たな電子証明書の発行通知

新しい電子証明書の発行通知の手続は、本運用規程「4.3.2 申請者に対する電子証明書発行通知」に準じる。

4.7.5 更新された電子証明書の受領

鍵更新を伴う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 電子証明書交付手続」に準じる。

4.7.6 認証局による鍵更新された電子証明書の公開

ルート認証局における鍵ペア更新時に DTS 上でリンク証明書を公開する。

4.7.7 その他の関係者に対する認証局の電子証明書発行通知

規定しない。

4.8 電子証明書の変更

電子証明書に関する公開鍵以外の情報の変更に伴う再発行は行わない。

4.9 電子証明書の失効と一時停止

4.9.1 電子証明書の失効事由

ルート認証局は、DS 電子証明書の有効期間内に次の失効事由が発生した場合、DS 電子証明書を失効させる。

① 電子証明書利用者の申請又は届出に基づく失効の事由

電子証明書利用者が行う電子証明書の失効の事由は次のとおりである。

- 盗難、紛失、漏洩、不正利用等により DS 電子証明書の秘密鍵が危殆化した又は危殆化の恐れがある場合
- 電子証明書の利用を停止した場合
- 電子証明書記載事項の変更があった場合

② 機構が行う失効の事由

機構が行う電子証明書の失効の事由は次のとおりである。

- 電子証明書の内容、利用目的が正しくない場合
- 本運用規程に違反した場合
- ルート認証局の運営を終了した場合
- 電子証明書の記載事項が不正確又は誤解を招く恐れがあると判断した場合
- ポリシーに対する適合性を決定する者又は「5.2.1.1 認証局管理責任者」に規定する認証局管理責任者が必要と判断した場合

4.9.2 電子証明書の失効申請者

DS 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。

- 「5.2.1.1 認証局管理責任者」に規定する認証局管理責任者

4.9.3 電子証明書申請の処理手順

ルート認証局は、「3.2.2 組織の認証」において定める手続に基づき審査を実施し、申請内容が適切である事を確認する。

ルート認証局は、DS 電子証明書の失効処理を行い、CRL を DTS に登録する。

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

ルート認証局は、失効申請手続の終了後、速やかに DS 電子証明書の失効処理を行う。なお、ルート認証局の発行した電子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。電子証明書を失効した電子証明書利用者に対して再度電子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 検証者等の失効確認の要求

ルート認証局の自己署名電子証明書及び DS 電子証明書の有効性を確認する方法として失効記録（RFC2251 に規定されている LDAPV3 プロトコルを利用する CRL）を提供する。

検証者はこれらの方法によってルート認証局の自己署名電子証明書及び DS 電子証明書の有効性を確認しなければならない。ルート認証局は、この確認が行えるよう DTS 上で失効記録を公開する。

4.9.7 失効記録（CRL）発行頻度

ルート認証局の失効記録（CRL）は、3 ヶ月毎の DS 証明書再発行の際にルート認証局から CRL を再発行する。ただし、認証局の秘密鍵の危殆化等が発生した場合には、CRL を直ちに発行する。

ルート認証局は、各エンティティが CRL の完全性及び発行日時を検証できるように、CRL に電子署名する。また前回の発行以降に変更が発生していなくても、CP に規定されているとおり定期的に CRL を発行するものとし、各 CRL はシリアル番号によって管理される。

CRL は、期限切れでない全ての失効した電子証明書を含む。失効された電子証明書の CRL エントリは、少なくともその電子証明書の有効期間の満了まで CRL 上に残る。

4.9.8 電子証明書の発行最大遅延時間

発行した失効記録は速やかに DTS に公開する。認証局は「7.2 失効記録（CRL）のプロファイル」に規定された形式に従って、48 時間以内に CRL を更新する。

4.9.9 オンラインでの失効ステータス確認の適用性

ルート認証局では、OCSP 等によるステータス確認方法は提供しない。ルート認証局の自己署名証明書、リンク証明書及び DS 電子証明書の失効ステータスは CRL を用いて確認する。

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

ルート認証局では、OCSP 等によるステータス確認方法は提供しない。ルート認証局の自己署名証明書、リンク証明書及び DS 電子証明書の失効ステータスは CRL を用いて確認する。

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

カード代替電磁的記録用 Document Signer において秘密鍵の危殆化が発生した場合は、デジタル庁は機構の承認を得た後、直ちにルート認証局で失効処理を行い、機構に報告を行う。

4.9.13 一時停止の事由

規定しない。

4.9.14 一時停止の届出を行う者

規定しない。

4.9.15 一時停止の手続

規定しない。

4.9.16 一時停止期間

規定しない。

4.10 電子証明書状態サービス

規定しない。

4.11 登録の終了

規定しない。

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

ルート認証局、RA 及び DTS 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。

5.1.2 物理的アクセス

5.1.2.1 ルート認証局

ルート認証局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。全ての要員は、目に見える身分証明書を着用し、着用していない者に注意することが奨励される。

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、「5.2.1.1 認証局管理責任者」に規定する認証局管理責任者が付与する。

ルート認証局の施設は、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。

ルート認証局の運用施設を収容する建物の外部ドアを保護するため、侵入検知システムが設置され、定期的に試験される。

5.1.2.2 RA

ガバメントクラウドに設置される RA の設備は、「5.1.2.1 ルート認証局」と同様の対策を講じる。電子証明書の発行・失効はシステムで実施されるため、操作者の認証については定めない。

5.1.2.3 DTS

ガバメントクラウドに設置される DTS の設備は、「5.1.2.1 ルート認証局」と同様の対策を講じる。

5.1.3 電源、電力、通信及び空調

ルート認証局、RA 及び DTS 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。

また施設内の電力及び通信設備において、データを伝送又は認証局が提供するサービスに使用するケーブルは、傍受や損害から保護される。

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

ルート認証局、RA 及び DTS を設置する建物、室、天井、床には防水対策を講じる。

5.1.5 地震対策

ルート認証局、RA 及び DTS 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

ルート認証局、RA 及び DTS 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

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

5.1.8 廃棄物処理

秘密扱いとする情報を含む書類・記憶媒体及び端末等については、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

ルート認証局、RA 及び DTS 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

ルート認証局における役割は、次のとおりとする。なお、「5.2.1.5 システム技術担当者」「5.2.1.6 PKI 技術担当者」「5.2.1.7 運用保守担当者」「5.2.1.9 施設スタッフ」はルート認証局の機能ごとに複数存在する可能性がある。

5.2.1.1 認証局管理責任者

認証局管理責任者は、ルート認証局の運営に関する責任者であり次の業務を行う。

- ルート認証局に係るシステムの統括
- キーセレモニーにおける総責任者として、作業の正常完了の承認
- インシデント対応における、鍵や電子証明書の危殆化判断と再発行手続の承認
- ルート認証局監査対応における現場責任者としての実行

5.2.1.2 運用保守責任者

運用保守責任者は、システム運用保守業務の責任者であり次の業務を行う。

- ルート認証局に関するインシデント対応における、問題管理、リリース管理における更新の承認

- ルート認証局運用保守業務の責任者として、システムのインストール、設定及び保守
- ルート認証局運用保守業務の責任者としての各ステークホルダーの窓口
- 年間、月次の活動計画の策定及び遂行
- 各ステークホルダーとの会議開催及び活動計画の承認とその遂行実績の報告
- ルート認証局設備の管理
- 定常運用・保守、インシデント対応における運用保守担当者への業務指示及び必要に応じて、各ステークホルダーへのエスカレーション
- キーセレモニーを含むルート認証局の鍵・電子証明書発行業務の実行・報告

5.2.1.3 秘密鍵管理者

ルート認証局の秘密鍵管理者は、ルート認証局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。

- ルート認証局の秘密鍵等のバックアップ媒体の保管管理
- ルート認証局の秘密鍵等生成、自己署名電子証明書発行時の鍵管理装置と HSM に対する操作
- ルート認証局の秘密鍵等の更新時における鍵管理装置と HSM に対する操作
- ルート認証局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鍵管理装置と HSM に対する操作

5.2.1.4 認証局電子証明書発行者

認証局電子証明書発行者は、次の業務を行う。

- キーセレモニーの進行に立会い、構築手順書通りに作業が行われていることを確認
- ルート認証局における電子証明書の生成、失効及び停止の承認

5.2.1.5 システム技術担当者

システム技術担当者は、次の業務を行う。

- ルート認証局システム（ハードウェア、ソフトウェア）の保守、メンテナンス
- 問題管理・インシデント対応、変更管理、リリース管理、構成管理

5.2.1.6 PKI 技術担当者

PKI 技術担当者は、次の業務を行う。

- ルート認証局業務
- キーセレモニーにおける PKI システム操作
- 各種電子証明書の登録、公開

5.2.1.7 運用保守担当者

運用保守担当者は、次の業務を行う。

- 定常業務におけるシステム運転管理、運用ログの取得
- 問い合わせ対応、定期的な報告書の作成
- 手順書に定められる監査対応業務
- 監査に必要となる文書、運用保守実績、ログデータに関する、定められた様式での記録

・　運用手順書の維持管理

5.2.1.8 施設スタッフ

施設スタッフは、次の業務を行う。

・　キーセレモニー参加者の入退室の立会い

5.2.2 職務ごとに必要とされる人数

ルート認証局の秘密鍵管理者及び操作要員は、「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

各要員がシステム操作を行う際、システムは操作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、各要員の認証は IC カード又は役割を認証する認証装置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。

5.2.4 職務権限の分離が必要な役割

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　運用保守責任者の権限

運用保守責任者は各担当者等に対し、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電子証明書を発行する。

5.3 認証局における人事管理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

ルート認証局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

信頼すべき役割を担う全ての要員は、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。

機構及びデジタル庁は、教育計画及び実施、訓練計画及び実施を担う。

5.3.4 各要員に対する教育訓練の周期

定期的に訓練を実施し、要員の知識とプロセスを継続的に更新する。これは（少なくとも 12 カ月毎の）新たな脅威と現行のセキュリティ慣行に関する更新を含む。また、業務内容、手順、指揮命令系統、責任及び権限の変更が行われた場合にも訓練を行う。

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。

一時的な契約スタッフを配備する場合、委託先と運用責任を持つデジタル庁間の契約において、契約スタッフがセキュリティポリシーに違反した場合はデジタル庁が機構の了承を得た上で措置を講じることを許可する旨を明示する。措置には以下のものが含まれる。

① 契約スタッフに対する保証要件
② 契約スタッフの故意の有害行為による損害の補償
③ 金銭的な罰則

リスク評価に基づいて必要な場合には、脅迫をうける可能性のある従業員が脅迫警報を発報することが考えられるが、本システムではサポートしないこととする。

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。デジタル庁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（構築手順書、運用設計書、運用手順書、情報セキュリティポリシー等）を閲覧することが可能である。

5.3.9 キーセレモニーの任名簿

各要員は、認証局管理責任者と認証局電子証明書発行者の承認を受け、任命する運用を行う。

5.4 監査ログの手続

内部監査員は、ルート認証局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

RA を含むルート認証局は、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全てのアクセス・稼動ログ
- 認証局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
- 認証局の設備への入退室記録

監査ログには次の情報を含める。

- 一意性のある端末 ID
- 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（操作要員 ID、システム名等）

ただし監査ログは、いかなる形式（例えば、平文又は暗号化されたもの）においても秘密鍵を記録しない。また電子証明書が有効期限切れになるか、失効するか、一時停止されるかにかかわらず、電子証明書のコピーが適切な期間、保管される。同様に最新でない CRL が適切な期間、保管される。

5.4.2 監査ログの検査周期

監査員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、改ざん防止対策として電子署名を施す。また、定期的に監査ログのバックアップを取得し、監査ログの閲覧及び削除は監査員が適切に行う。

監査ログの署名用秘密鍵は、他の目的に使用されない。

5.4.5 監査ログのバックアップ手順

規定しない。

5.4.6 監査ログの収集システム

監査ログの収集機能は、ルート認証局の一機能とし、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

デジタル庁は次の情報を保管する。ただし、キーセレモニーの実施等に関する書類については最新版のみ紙で保管するものとし、最新でなくなった情報はデジタルデータに変換して保存する。

5.5.1.1.1 ルート認証局

- 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
- 監査報告書等
- 設備及び安全対策に関する書類

5.5.1.1.2 RA

紙で保管する情報は規定しない。

5.5.1.2 デジタルデータとして保管する情報

デジタル庁は次の情報を保管する。

5.5.1.2.1 ルート認証局

- 検証者等との取決めに関する書類
- ルート認証局の運営情報の開示・訂正等に関する書類
- 失効情報及び失効情報ファイルの提供状況の報告書
- DS 電子証明書の発行記録
- 失効申請書（デジタル庁へのオンライン申請の場合）
- DS 電子証明書失効申請等情報等
- DS 電子証明書
- ルート認証局の自己署名電子証明書
- リンク証明書
- 失効情報
- 失効記録
- 失効情報ファイル（CRL）
- 失効情報ファイル（CRL）提供履歴
- 各種ログ（監視用ログ、起動停止ログ、操作ログ）等

5.5.1.2.2 RA

- 電子証明書の発行申請書
- 電子証明書の失効申請書

5.5.2 アーカイブ保存期間

5.5.2.1 紙で保管する情報

別途定める期間、保管する。

5.5.2.2 デジタルデータとして保管する情報

別途定める期間、保管する。

5.5.3 アーカイブの保護

情報の取り扱い及び保管に関する手順を定めた「情報セキュリティポリシー」に従い、ビジネス上の必要性及び影響を踏まえて情報をラベリングし保護する。

ルート認証局は、アーカイブ化された監査ログを、リスク評価及び法的要求事項によって決定された所定の期間、保管する。また電子証明書及びカード代替電磁的記録の主体以外の関係者からの要求による、アーカイブからの情報開示は、機構の承認を必要とする。

5.5.3.1 紙で保管する情報

認証局に保管する情報は、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。地方公共団体に保管する情報がある場合は、適切な場所に保管する。

アーカイブは、紛失、承認されていない破棄及び改ざんへの対策が講じられる。

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。

アーカイブは、紛失、承認されていない破棄及び改ざんへの対策が講じられる。

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、定期的にバックアップする。

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。

タイムスタンプの日付と時刻は、定期メンテナンス時の校正、および、ガバメントクラウドで提供される機能を用いて補正される。

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 認証局の鍵の更新

5 年ごとにルート認証局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、DTS 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

認証局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
- 認証局秘密鍵の危殆化
- 火災、地震等の災害

「緊急時対応計画」は適切なリスクアセスメントに基づいて策定され、セキュリティ事故報告の正式な手順及び事故報告の受領時に取るべき措置を定めている。これには、責任の割り当てとエスカレーション手順が定義され文書化されている。緊急時は、認証局管理責任者に報告する。

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 認証局の秘密鍵が危殆化した場合の手順

ルート認証局の自己署名電子証明書の秘密鍵が危殆化した場合、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 危殆化したルート認証局の秘密鍵により署名した全ての電子証明書を失効記録（CRL）に記録し、DTS で公開する。
② ルート認証局は DS 電子証明書の発行業務を停止する。
③ 新規のカード代替電磁的記録発行の申請受付業務を停止する。
④ ルート認証局の自己署名電子証明書を再発行する。
⑤ 危殆化したルート認証局の秘密鍵により署名した全ての電子証明書を新たに失効記録（CRL）に記録し、再度 DTS で公開する。
⑥ 新規のカード代替電磁的記録発行の申請受付業務を再開する。

各電子証明書の失効手続については、本運用規程「4.9 電子証明書の失効と一時停止」に規定する。

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。「緊急時対応計画」に

は下記の事項を含む。

① デジタル庁は、障害発生時の障害修正（障害切り分け窓口と連携して障害修正を緊急で実施)、機構へのエスカレーション等を実施する。機構は、対応状況の確認を実施する。
② デジタル庁は、緊急時運用（パンデミック、大規模地震等)、大規模システム故障への対応を実施する。デジタル庁は実施した結果を、機構に報告する。
③ デジタル庁は、インシデント管理に関する実績集計の計画立案、インシデントに関する実績集計、定期報告、インシデントの受付け・応急措置、インシデント管理のモニタリング、苦情/問合せ対応、作業依頼の実施、インシデントに関する改善検討・実施を担う。デジタル庁は改善検討結果を、機構に報告後、実施を行う。

5.8 ルート認証局の運営の終了

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 ルート認証局の鍵ペアの生成

ルート認証局の鍵ペアは、複数人の秘密鍵管理者が FIPS140-3 レベル 3 相当のルート認証局専用の HSM を用いて生成する。

6.1.2 秘密鍵の配布

ルート認証局によって署名される秘密鍵は申請者の設備で生成され、移動してはならない。

6.1.3 認証局への公開鍵の配布

カード代替電磁的記録用 Document Signer の鍵ペアの公開鍵を格納した電子証明書発行要求は、所定の手続によってルート認証局へ配布される。

6.1.4 検証者への認証局公開鍵の配布

ルート認証局の自己署名電子証明書は、DTS により公表し、そのフィンガープリントを機構の Web 上に公表する。機構の Web によるフィンガープリントの公表は、安全かつ確実な方法により行う。

6.1.5 ルート認証局の鍵サイズ

鍵サイズは次のとおりとし、デジタル庁はセキュリティ強度に関する年次レビューにおいて鍵サイズの変更の必要性を確認する。変更の必要性があった場合には機構へ報告を実施し、変更の承認を得る。

6.1.5.1 ルート認証局の鍵ペア

ECDSA 暗号方式に基づく 384 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 鍵の利用目的（X.509 v3 Key Usage Field）

6.1.7.1 ルート認証局の鍵ペア

ルート認証局の自己署名電子証明書、リンク証明書、CRL 及び DS 電子証明書に電子署名するために使用される。

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 ルート認証局の秘密鍵

ルート認証局の秘密鍵をルート認証局専用の HSM へ格納し、FIPS140-3 レベル 3 相当の HSM により保護する

6.2.2 秘密鍵の複数人制御

6.2.2.1 ルート認証局の秘密鍵

ルート認証局の秘密鍵は、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。

6.2.3 秘密鍵の預託（エクスロー）

6.2.3.1 ルート認証局の秘密鍵の預託

ルート認証局の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 ルート認証局の秘密鍵

ルート認証局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。リストアは、複数人の操作により、バックアップと同様にセキュアな方法で実施する。

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

秘密鍵の転送は行わない。

6.2.7 暗号モジュールへの秘密鍵の格納

6.2.7.1 ルート認証局の秘密鍵

ルート認証局の秘密鍵は、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で秘匿性を担保する。

6.2.8 秘密鍵の活性化方法

6.2.8.1 ルート認証局の秘密鍵

ルート認証局はオフラインであり、通常は電源が入っていないため、システム起動後に暗号化モジュールで秘密鍵を活性化する必要がある。

ルート認証局の秘密鍵は複数人の操作により活性化する。

秘密鍵の活性化には、ID とパスワードの他に多要素認証を実施する。

6.2.9 秘密鍵の非活性化方法

6.2.9.1 ルート認証局の秘密鍵

ルート認証局はオフラインであり、通常は電源が入っていないため、秘密鍵は使用されない場合は非活性化されている。非活性化するには、HSM およびサーバを正常にシャットダウンした後、電源断の運用を行うこととする。一度鍵が非活性化されると、新しい活性化処理が実施されるまで非活性化状態となる。

6.2.10 秘密鍵の破棄方法

6.2.10.1 ルート認証局の秘密鍵

暗号モジュール内の秘密鍵の破棄は、機構及びデジタル庁の認証局管理責任者の承認を経て実施さ

れ、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、バックアップ用暗号モジュールに格納されている秘密鍵も同様に破棄する。

ただし、事業用途等としての価値を見出せなくなるか、法的義務が終了するまで破棄されない。

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 ルート認証局の公開鍵

ルート認証局の公開鍵は自己署名電子証明書に含まれ、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 ルート認証局の公開鍵証明書の有効期間と鍵ペアの使用期間

ルート認証局の自己署名電子証明書の有効期間は DS 電子証明書の有効期間を考慮して 5 年 4 ヶ月とする。ルート認証局の秘密鍵の使用期間は 5 年とし、鍵を生成した日から起算して 5 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、暗号方式の変更又は鍵長の変更を検討しその時点で鍵更新を行う場合がある。

新しい鍵ペアのための電子証明書は、有効期間を満了する 1 ヶ月前を発行開始期限とする。

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 ルート認証局の秘密鍵

ルート認証局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。

6.4.2 活性化データの保護

6.4.2.1 ルート認証局の秘密鍵

ルート認証局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。

6.4.3 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 コンピュータセキュリティに関する技術的要件

ルート認証局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。また使用する機器は、メーカーの指示及び/又は他の文書化された手順に従って保守される。

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定期的に実施する。

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

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

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。また、適宜ウイルス対策及び不正プログラム対策を行う。

6.6.3 ライフサイクルのセキュリティ管理

デジタル庁は、ルート認証局のシステム開発、運用、保守が適切に行われていることについて監査等を通じて適宜評価し、機構及びデジタル庁は、必要に応じて改善を行う。

6.7 ネットワークセキュリティ管理

ルート認証局は、他のシステムへのネットワーク接続を持たないオフラインの「エアギャップ」システムである。

ルート認証局以外の各コンポーネントに対しては、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。

6.8 タイムスタンプ

ルート認証局は、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 電子証明書及び失効記録（CRL）のプロファイル

7.1 電子証明書のプロファイル

電子証明書のプロファイルは、技術資料に定める。なお、ルート認証局の自己署名電子証明書及びリンク証明書は【ISO/IEC 18013-5】に準拠し、「7.1.2 電子証明書拡張」の情報を記載する。

7.1.1 バージョン番号

【ISO/IEC 18013-5】より、バージョン番号は「3」とする。

7.1.2 電子証明書拡張

X.509 v3 電子証明書向けに定義された拡張は、ユーザ又は公開鍵に追加の属性を関連付け、電子証明書階層を管理するための方法を定義する。ルート認証局の自己署名電子証明書及びリンク証明書に含まれる拡張は【ISO/IEC 18013-5】に準拠する。

7.1.2.1 ルート認証局の自己署名電子証明書/拡張

- バージョン番号（X.509 電子証明書フォーマットのバージョン番号）
- シリアル番号（ルート認証局内で発行済み電子証明書を識別するための番号）
- 署名アルゴリズム（ルート認証局が当該自己署名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（当該自己署名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（当該自己署名電子証明書の発行日）
- 有効期間の終了日（発行日の 5 年 4 ヶ月後）
- 公開鍵（ルート認証局の公開鍵）
- 拡張情報

7.1.2.2 リンク証明書/拡張

- バージョン番号（X.509 電子証明書フォーマットのバージョン番号）
- シリアル番号（ルート認証局内で発行済み電子証明書を識別するための番号）
- 署名アルゴリズム（ルート認証局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：旧世代の自己署名電子証明書の有効期間の終了日、NewWithOld：旧世代の自己署名電子証明書の有効期間の終了日）
- 公開鍵（OldWithNew：旧世代のルート認証局の公開鍵、NewWithOld：新世代のルート認証局の公開鍵）
- 拡張情報

7.1.3 アルゴリズム Object Identifier

ルート認証局では、次の署名アルゴリズムが使用される。

- ルート認証局の自己署名電子証明書及びリンク証明書：ecdsa-with-SHA384（OID 1.2.840.10045.4.3.3）

7.1.4 名称形式

「3.1.1 名称の種類」に準じる。

7.1.5 名称の制約

【ISO/IEC 18013-5】より、name constraints 拡張子を使用してはならない。

7.1.6 証明書ポリシー Object Identifier

証明書ポリシーの OID は、【ISO/IEC 18013-5】で定義された電子証明書プロファイルに従い、電子証明書では記載しない。

7.1.7 ポリシー制約拡張の使用用途

【ISO/IEC 18013-5】より、policy constraints 拡張子を使用してはならない。

7.1.8 ポリシー修飾子の構文とセマンティクス

規定しない。

7.1.9 Critical な証明書ポリシー拡張の処理セマンティクス

検証者は、検証者が認識できない Critical な拡張又は検証者が処理できない情報を含む Critical な拡張を見つけた場合、電子証明書を拒否しなければならない。

7.2 失効記録（CRL）のプロファイル

CRL のプロファイルは、技術仕様書に定める。なお、CRL は【ISO/IEC 18013-5】に準拠し、「7.2.2 CRL と CRL エントリ拡張」の情報を記載する。

電子証明書発行の際、有効期間中は電子証明書が使用されることが想定されている。ただし、様々な状況により、有効期間の満了前に電子証明書が無効になる場合がある。

7.2.1 バージョン番号

【ISO/IEC 18013-5】より、バージョン番号は「2」とする。

7.2.2 CRL と CRL エントリ拡張

X.509 v2CRL 向けに定義された拡張は、CRL に追加の属性を関連付けるための方法を定義する。CRL は有効期間満了前に失効した電子証明書の一覧を含む。

ルート認証局の自己署名証明書、リンク証明書及び DS 電子証明書の失効記録（CRL）には以下の情報を記載する。

- 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（ルート認証局が当該 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）
- 失効した電子証明書情報（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

ルート認証局は OCSP サービスを提供しない。

8 準拠性監査

8.1 監査員

監査員は、次の業務を行う。

- 定期的な監査
- キーセレモニー進行への立会い及び手順書通りに作業が行われていることの確認

8.2 監査の頻度

デジタル庁は監査人により年次又は隔年次で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。デジタル庁は監査の結果を機構に報告する。

8.3 監査人の要件

ルート認証局の監査は、監査業務及び認証局の運営に精通した者が行う。

8.4 監査人と被監査組織の関係

デジタル庁は、ルート認証局と利害関係を有しない者を監査人として選定する。

8.5 監査項目

認証局の運営が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。

8.6 監査指摘事項への対応

デジタル庁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。デジタル庁は重要な是正措置を行う場合には、機構に報告して承認を得る。

8.7 監査結果の取扱い

監査結果は、監査人からデジタル庁に対して監査報告書として提出される。デジタル庁は監査法人から提出された監査報告書を機構へ提出する。

認証局管理責任者は、ルート認証局の運営に関する意思決定機関に監査結果を報告する。

9 他の業務上及び法的事項

9.1 手数料

規定しない。

9.2 財務上の責任

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

ルート認証局は、漏えいすることによってルート認証局の運営の信頼性が損なわれる恐れのある情報を機密扱いとする。

9.3.2 秘密情報の範囲外の情報

ルート認証局の自己署名電子証明書、リンク証明書、それらの電子証明書の失効情報、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電子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

機構及びデジタル庁は、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。またこれらの情報が不要となった際又はルート認証局が運用終了した際は、適切に制限される。

9.4 個人情報の保護

9.4.1 個人情報保護計画

機構及びデジタル庁は、「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

カード代替電磁的記録の発行のために申請者又は電子証明書利用者から取得した個人情報である。

9.4.3 個人情報としてみなされない情報

規定しない。

9.4.4 個人情報を保護する責任

機構及びデジタル庁、検証者は、関係法令に基づき個人情報を適切に保護する。

機構及びデジタル庁は、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

機構及びデジタル庁、検証者は、関係法令に基づき個人情報を適切に使用する。カード代替電磁的記録の発行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、機構及びデジタル庁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

規定しない。

9.5 知的財産権

ルート認証局が発行する電子証明書は機構に帰属するものとする。本運用規程及び関連するプログラム等の知的財産権は、デジタル庁に帰属するものとする。

資料やソフトウェア製品の使用にあたり、知的財産権に関わる法令を遵守する。

9.6 表明保証

9.6.1 認証局の表明保証

9.6.1.1 ルート認証局の表明保証

ルート認証局は、ルート認証局の運営に関して次の内容を表明し、保証する。

- 本運用規程に基づき、ルート認証局の自己署名電子証明書、リンク証明書及び DS 電子証明書を発行、更新、失効すること。
- 「2.2 電子証明情報の公開」に定める情報を公表すること。
- ルート認証局の自己署名証明書、リンク証明書及び DS 電子証明書について、CRL を「4.9.7 失効記録（CRL）発行頻度」に定める期間ごとに発行すること。
- ルート認証局の秘密鍵を安全に管理すること。
- ルート認証局の秘密鍵が危殆化した場合は、速やかに危殆化に関する情報を公表すること。
- 電子証明書の発行、更新、失効等に関する監査ログ及びアーカイブを必要な期間保管すること。
- システムの稼動監視を行うこと。

9.6.2 RA の表明保証

RA は、RA の業務に関して次の内容を表明し、保証する。

- 申請者からのルート認証局の自己署名証明書、リンク証明書及び DS 電子証明書の発行、更新及び失効申請に際して、受付、申請者の真偽の確認及び申請内容の確認を確実に行うこと。
- 認証局に対して、安全に電子証明書の発行、それらの更新及び失効申請を行うこと。
- 電子証明書利用者に対して、電子証明書の発行完了及び失効完了を通知すること。

・ 各申請手続において入手した電子証明書利用者情報を安全に保管すること。

9.6.3 電子証明書利用者の表明保証

9.6.3.1 申請者/電子証明書利用者の表明保証

申請者/電子証明書利用者は、「4.5.1 電子証明書利用者による秘密鍵及び電子証明書の使用」に定める内容及び以下に定める内容を遵守することについて表明し、保証する。

・ RA に対し、電子証明書を発行及び失効するための正確な情報を申請すること。
・ 電子証明書を受領する時点で、電子証明書の情報が正しいことを確認すること。
・ 電子証明書の記載事項が変更となる場合は、速やかに RA に申請すること。

9.6.4 検証者の表明保証

検証者は、「4.5.2 検証者による公開鍵及び電子証明書の使用」に定める内容を遵守することについて表明し、保証する。

9.6.5 その他の関係者の表明保証

9.6.5.1 Digital Trust Service の表明保証

DTS は、「2.1 リポジトリ」に定める内容を遵守することについて表明し、保証する。

9.6.5.2 ルート認証局の運営に関する意思決定機関の表明保証

機構及びデジタル庁は、ルート認証局の運営に当たり以下の事項を保証する。

・ 法の規定に基づき、ルート認証局の運営業務を適切に行うこと。
・ 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。
・ ルート認証局の役割及び各機能の一部を別の事業者へ委譲することを選択した場合、機構及びデジタル庁は、委譲された機能の完了及びその CPS に関する表明の定義と維持に関する責任を持つこと。

9.7 保証の免責事項

規定しない。

9.8 責任の制限

機構及びデジタル庁は、ルート認証局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、機構及びデジタル庁の認証局管理責任者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ルート認証局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

電子証明書利用者が電子証明書の利用を終了する場合又はルート認証局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電子証明書利用者、検証者、機構及びデジタル庁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

本運用規程上必要とされ又は許容されるルート認証局に対する通知、請求、要求、依頼その他の連絡は機構を窓口とする。連絡先は「1.5.2 連絡先」に規定する。

9.12 改訂

9.12.1 改訂手続

機構及びデジタル庁は、本運用規程を必要に応じて変更する。

9.12.2 通知方法及び機関

本運用規程を変更した場合には、機構及びデジタル庁は速やかに変更した本運用規程を機構の Web 上で公表する。これをもって電子証明書利用者、検証者等への通知とする。

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、全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。