地方公共団体による公的個人認証サービス

岡山県認証局　運用規程

Ver.1.6

2014年4月1日

改訂履歴

Ver	日付	改版内容
1.0	2004 年 1 月 29 日	初版発行
1.1	2005 年 1 月 19 日	施行規則改正等に伴う改版
1.2	2006 年 11 月 1 日	法改正に伴う改版
1.3	2008 年 9 月 19 日	認証局の秘密鍵更新等に伴う改版
1.4	2010 年 4 月 12 日	連絡先所属名の変更に伴う改版
1.5	2013 年 7 月 8 日	住民基本台帳法の一部を改正する法律（平成 21 年法律第 77 号）の施行に伴う改版
1.6	2014 年 4 月 1 日	公的個人認証サービス共通基盤運用会議発足に伴う改正

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を実現するため、住民基本台帳に記録されている者の電子証明書（以下、利用者の証明書を「電子証明書」という。）等を発行する岡山県の公的個人認証サービス都道府県単位認証局（以下「岡山県 CA」という。）の認証業務に関する運営方針を定める。

なお、本運用規程の構成は、IETF(Internet Engineering Task Force)においてPKIX(Public-Key Infrastructure X.509) Working Group による RFC(Request For Comments) 2527 「Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework」に準拠している。但し、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

岡山県 CA は､岡山県の区域内の市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、その申請に応じて、電子証明書を発行し、その他岡山県 CA の運用に必要な証明書を発行するとともに、他の公的個人認証サービスに係る各都道府県単位認証局や政府認証基盤の認証局等と相互認証を行うために設置される公的個人認証サービスブリッジ認証局（以下｢個人認証 BCA｣という。）と相互認証証明書を発行して取り交わす。更に失効情報（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、「電子署名に係る地方公共団体の認証業務に関する法律」（以下「根拠法」という。）第１７条第４項に規定する署名検証者又は同条第６項に規定する団体署名検証者の求めに応じて提供する。

また岡山県 CA 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、本運用規程を岡山県 CA の認証業務に関する運営方針として位置付ける。

1-2 識別

岡山県 CA の証明書ポリシーの識別子は、次のとおりとする。

岡山県 CA 電子証明書等ポリシー

電子証明書ポリシー及び岡山県 CA 相互認証証明書ポリシー
1.2.392.200149.8.5.1.1.10

テスト用電子証明書ポリシー及び岡山県 CA 相互認証証明書ポリシー
1.2.392.200149.8.5.1.0.10

官職証明書検証サーバ証明書ポリシー
1.2.392.200149.8.5.1.200

テスト用官職証明書検証サーバ証明書ポリシー
1.2.392.200149.8.5.1.0.200

OCSP レスポンダ証明書ポリシー
1.2.392.200149.8.5.1.300

テスト用 OCSP レスポンダ証明書ポリシー
1.2.392.200149.8.5.1.0.300

1-3 運用体制と証明書の適用範囲

1-3-1 登場者

(1) 総務大臣

総務大臣は、根拠法の定めるところによって、指定認証機関の指定等を行う。

(2) 公的個人認証サービス共通基盤事業運用会議

公的個人認証サービス共通基盤事業運用会議（以下「運用会議」という。）は、公的個人認証システムの一元的な運営の実現に関する重要事項の連絡及び調整に関する事務を行う。

(3) 岡山県知事

岡山県知事は、以下に示す岡山県 CA（岡山県認証局）の機能を備える。

(4) 岡山県 CA

岡山県 CA は、市町村長と相互に連携・協力して、電子証明書その他の証明書の発行、失効記録（CRL/ARL）の作成、電子証明書の有効性を確認する手段の提供等の証明書発行・失効情報管理業務を行う。岡山県知事の秘密鍵の危殆化時の対応や災害発生等による緊急時の対応も行う。

また、利用者に対して、利用者が国又は地方公共団体の機関からオンラインで受け取った文書の電子署名の検証に必要となる官職及び職責証明書の有効性を確認する手段を提供する。

(5) 個人認証 BCA

個人認証 BCA は、運用会議が策定する運用規程に従い、岡山県 CA 等の各都道府県単位認証局及び政府認証基盤ブリッジ認証局（以下「政府認証基盤 BCA」という。）等と相互認証を行うための証明書の発行等を行う。

(6) 指定認証機関

指定認証機関は、根拠法の定めるところによって、岡山県知事の委任を受け、認証業務の実施に関する事務（以下「認証事務」という。）を行う。

(7) 市町村長

岡山県の区域内の市町村長は、電子証明書の発行申請及び失効申請の受付、申請者の本人確認、岡山県 CA の発行した電子証明書の申請者への交付等を行う。

(8) 申請者／利用者

申請者とは、根拠法第３条１項の規定より、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。但し、この場合には、「電子署名に係る地方公共団体の認証業務に関する法律施行規則」（以下「根拠法の規則」という。）第５条の要件を満たさなければならない。）。利用者とは、住民基本台帳に記録されている者で、電子証明書の発行を受けた者をいう。

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、電子証明書を利用することができる。岡山県知事又は指定認証機関に対して自己に係る認証業務情報（電子証明書の発行記録、失効情報及び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。また、国又は地方公共団体の機関からオンラインで受け取った文書の電子署名の検証に必要な官職及び職責証明書の有効性を確認する。

(9) 署名検証者

次の者のうち、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根拠法第１７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ものであって「電子署名に係る地方公共団体の認証業務に関する法律施行令」（以下「根拠法の政令」という。）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行政機関等及び裁判所に対する申請、届出その他の手続に必要な電磁的記録を提供する団体で根拠法の政令で定めるもの

岡山県 CA から、失効記録（CRL/ARL）の提供等電子証明書の有効性を確認する手段の提供を受け、利用者からのオンライン申請・届出等に係る電子署名を検証する。

(10) 署名確認者

根拠法第１７条第５項の規定に基づき根拠法の政令で定めるものをいう。

以下に定める団体署名検証者から電子証明書の有効性の確認結果の提供を受け、利用者からのオンライン申請・届出等に係る電子署名を検証する。

(11) 団体署名検証者

次の者のうち、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根拠法第１７条第５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法律の規定に基づき他人の依頼を受けて行政機関等及び裁判所に対する申請、届出その他の手続を行う者が所属する団体で根拠法の政令で定めるもの

②行政機関等及び裁判所に対する申請、届出その他の手続に必要な電磁的記録を提供する者が所属する団体又は機関で根拠法の政令で定めるもの

岡山県 CA から、失効記録（CRL/ARL）の提供等電子証明書の有効性を確認する手段の提供を受け、署名確認者より受信した利用者からのオンライン申請・届出等に添付された電子証明書の有効性を確認し、その結果を署名確認者に回答する。

(12) 署名検証者等

署名検証者及び団体署名検証者をいう。

1-3-2 適用性・適用環境など

サービスの種類及び用途は、次の４つである。

①次の用途のための電子証明書の発行。

・行政機関等及び裁判所で行う手続のオンライン申請・届出に係る電子署名

・署名検証者等が行う本人確認

・署名確認者が行う本人確認

なお、電子証明書の有効期間は電子証明書が発行された日から起算して３年とする。

②次の用途のための相互認証証明書の発行。

・個人認証 BCA を経由した政府認証基盤 BCA 等との相互認証

なお、相互認証証明書の有効期間は相互認証証明書を有効とする日から起算して５年とする。

③次の用途のための官職証明書検証サーバ証明書の発行。

・利用者が国又は地方公共団体の機関からオンラインで受け取った文書の電子署名の検証に必要な官職証明書又は職責証明書の有効性を確認する手段の提供

なお、官職証明書検証サーバ証明書の有効期間は官職証明書検証サーバ証明書を有効とする日から起算して１年とする。

④次の用途のための OCSP レスポンダ証明書の発行。

・署名検証者等が OCSP レスポンダ照会方法で電子証明書の有効性を確認する手段の提供

なお、OCSP レスポンダ証明書の有効期間は OCSP レスポンダ証明書を有効とする日から起算して１年とする。

1-3-3 運用規程の責任者

本運用規程の責任者は岡山県知事とする。

1-3-4 連絡先

本運用規程に関する照会窓口を下記に示す。

岡山県

住所：　岡山県岡山市北区内山下二丁目４番６号
部署：　県民生活部情報政策課

受付時間：午前８時 30 分～午後５時 15 分
電　話：086-226-7432
ＦＡＸ：086-235-9737
電子メールアドレス：joho@pref.okayama.lg.jp

2. 一般規定

2-1 義務

2-1-1 総務大臣の義務

(1)指定認証機関の指定、休廃止の許可、指定解除、岡山県知事への通知及び公示
(2)指定認証機関への監督上必要な命令
(3)指定認証機関への必要な報告の要求及び立入検査の実施
(4)指定認証機関の役員の選任及び解任の認可並びに解任命令
(5)指定認証機関の策定した認証事務管理規程及び事業計画の認可及び変更命令
(6)指定認証機関がした処分等に係る不服申立てへの対応
(7)認証業務の用に供する施設等についての技術的基準の策定
(8)認証業務に係る技術の評価に関する調査、研究
(9)署名検証者の認定に係わる事務
(10)署名検証者等への業務実施状況についての必要な報告の要求
(11)公的個人認証サービスに係る情報の利用者への周知、広報

2-1-2 岡山県知事の義務

(1)市町村長からの申請者の氏名・出生の年月日・男女の別・住所（以下「基本 4 情報（申請者が外国人住民であって、当該外国人住民に係る住民票に通称が記載されている場合にあっては、基本 4 情報及び通称。以下同じ。）」という。）及び公開鍵の通知に基づく電子証明書の発行
(2)岡山県 CA と個人認証 BCA との間の相互認証に係る正確な情報の提示及び相互認証証明書の交換
(3)自己署名証明書の発行
(4)リンク証明書の発行
(5)運用のための関連証明書の発行
(6)利用者からオンラインで失効申請を受けた場合の本人確認及び失効情報の作成
(7)市町村窓口において利用者から失効申請を受けた場合の失効情報の作成
(8)利用者の住所若しくは氏名の変更又は死亡の事実が生じた場合における失効情報の作成
(9)利用者の電子証明書の証明事項に関して当該電子証明書に記録されたものと異なるものが発見された場合等における失効情報の作成
(10)岡山県知事の秘密鍵が危殆化（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、なった疑いがあることをいう。以下同じ。）した場合、当該秘密鍵により発行されたすべての証明書の失効情報の作成及び個人認証 BCA への報告
(11)署名検証者等に対する、電子証明書の有効性を確認する方法（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「OCSP レスポンダ照会方法」という。）、失効記録（CRL/ARL）提供方法）の提供
(12)利用者に対する国又は地方公共団体の機関の官職又は職責証明書の有効性を確認する方法の提供
(13)失効情報及び失効情報ファイルの提供状況についての報告書作成と公表
(14)認証業務情報の開示請求に対する開示
(15)認証業務情報の訂正等請求に対する訂正等
(16)岡山県知事の鍵ペアの生成と秘密鍵の安全な管理
(17)監査の実施、監査結果を踏まえた改善等の実施
(18)認証業務実施設備の設置
(19)各証明書の発行、更新及び失効業務に関しては本運用規程に基づくこと

(20)発行済みのすべての証明書及び失効記録（CRL/ARL）について必要な期間の保管、並びに、各証明書の発行、更新及び失効等に関する監査ログ及び保管する情報について必要な期間の保管
(21)システムの稼動監視は常時的確に行い 24 時間の安定的な運用を目標とすること
(22)失効情報は有効期間 72 時間の失効記録（CRL/ARL）を 24 時間ごとに発行すること
(23)利用者からの苦情及び問合せの対応
(24)指定認証機関への認証事務の委任及び総務大臣への報告、公示
(25)異動等失効情報の指定認証機関への通知
(26)必要に応じての指定認証機関への指示
(27)指定認証機関への必要な報告の要求及び立入検査の実施
(28)指定認証機関への委任の解除及び総務大臣への報告、公示
(29)指定認証機関の設定した電子証明書発行手数料及び情報提供手数料についての承認
(30)指定認証機関との認証事務費用についての協議実施とその交付
(31)指定認証機関が認証事務を休廃止した場合等の認証事務の実施
(32)署名検証者等との取決めの締結
(33)署名検証者等への業務実施状況についての必要な報告の要求
(34)認証業務に関する情報の適正な取り扱い
(35)認証業務情報についての秘密保持
(36)公的個人認証サービスに係る情報の利用者への周知、広報
(37)本運用規程の作成及び決定

2-1-3 市町村長の義務

(1)発行時又は失効時の申請者又は失効申請者の本人確認（実在性、本人性）
(2)代理申請者が真正な代理人であることの確認
(3)失効申請について、失効要件の確認
(4)その他申請手続が適切に行われていることの確認
(5)適切な強度を有する鍵ペアを生成する装置の提供（申請者の鍵ペアを生成する装置、以下「鍵ペア生成装置」という。）
(6)申請者の基本 4 情報及び申請者の公開鍵の岡山県知事への通知
(7)失効申請の岡山県知事への通知
(8)電子証明書及び岡山県知事の自己署名証明書の利用者への交付
(9)電子証明書の利用目的の制約、不正利用に関する罰則等の申請者･利用者への説明
(10)鍵ペア生成装置、受付窓口端末等のシステムの保守・安全管理
(11)監査への対応及び監査結果を踏まえた改善等の実施
(12)認証業務に関する情報の適正な取り扱い
(13)認証業務情報についての秘密保持
(14)電子証明書発行申請者からの発行手数料の徴収
(15)認証業務情報の開示請求及び訂正等請求の受付
(16)利用者の申請に基づくパスワードの初期化、ロック解除（5 回以上パスワードの誤入力があったときに悪用防止対策として IC カードが使用不能となった状態を解除することをいう。）、鍵ペア等の消去
(17)利用者端末用の利用者クライアントソフト（電子証明書を利用するために必要なソフトウェア）の入手に関する利用者への支援
(18)利用者からの苦情及び問合せの対応
(19)公的個人認証サービスに係る情報の利用者への周知、広報

2-1-4 指定認証機関の義務

⑴岡山県知事からの委任による認証事務の実施（本運用規程「2-1-2 岡山県知事の義務」内の⑴から⑬まで、⑯及び⑱から㉒までの実施）
⑵認証事務管理規程の策定
⑶事業計画及び収支予算の作成並びに事業報告書及び収支決算書の提出
⑷認証業務情報保護委員会の設置
⑸認証業務に関する情報の適正な取り扱い
⑹認証業務情報についての秘密保持
⑺認証業務情報の開示請求に対する開示
⑻認証業務情報の訂正等請求に対する訂正等
⑼利用者からの苦情及び問合せの対応
⑽署名検証者等からの情報提供手数料の徴収

2-1-5 利用者の義務

⑴電子証明書の発行申請書、失効申請書等への正確な内容の記載
⑵秘密鍵及び当該秘密鍵を格納した IC カードの安全な管理
⑶IC カードに格納されている秘密鍵を活性化するパスワードの定期的な変更及び安全な管理
⑷秘密鍵が危殆化した場合等の速やかな失効申請
⑸電子証明書の目的外利用の禁止
⑹発行手数料の納付

2-1-6 署名検証者の義務

⑴岡山県 CA から発行された電子証明書を利用して付与された電子署名の検証
⑵岡山県 CA から発行された電子証明書の検証（当該電子証明書が岡山県知事から発行されたものであるかどうか、当該電子証明書が失効していないかどうか）
⑶利用者からのオンライン申請・届出等で行われた電子署名の検証を行って利用者の認証を行うこと以外の目的による電子証明書の利用の禁止
⑷失効情報及び失効情報ファイルの提供を受ける際の岡山県知事との取決めの締結
⑸総務大臣及び岡山県知事からの報告要求の受容と実施
⑹失効情報等の秘密保持と適正な使用
⑺失効情報等の安全確保
⑻情報提供手数料の納付

2-1-7 団体署名検証者の義務

⑴岡山県 CA から発行された電子証明書が失効していないことの確認
⑵署名確認者から受領した利用者に係る電子署名の検証を行って利用者の認証を行うこと以外の目的による電子証明書の利用の禁止
⑶失効情報及び失効情報ファイルの提供を受ける際の岡山県知事との取決めの締結
⑷総務大臣及び岡山県知事からの報告要求の受容と実施
⑸失効情報等の秘密保持と適正な使用
⑹失効情報等の安全確保
⑺情報提供手数料の納付

2-1-8 署名確認者の義務

⑴岡山県 CA から発行された電子証明書を利用して付与された電子署名の検証

⑵岡山県 CA から発行された電子証明書の検証（当該電子証明書が岡山県知事から発行されたものであるかどうか、当該電子証明書が失効していないかどうか）
⑶利用者からのオンライン申請・届出等で行われた電子署名の検証を行って利用者の認証を行うこと以外の目的による電子証明書の利用の禁止
⑷団体署名検証者から受領した回答の秘密保持と適正な使用
⑸団体署名検証者から受領した回答の安全確保

2-1-9 リポジトリの義務

岡山県 CA は、失効記録（CRL/ARL）の作成後、リポジトリに公開することにより、署名検証者等が電子証明書の有効性を確認できるようにする。

また、その他の情報を保管し公開する。

2-2 責任

2-2-1 総務大臣の責任

総務大臣は、根拠法の定めるところによって、指定認証機関の指定を行い、指定認証機関が安全かつ適正な認証事務等を実施するよう管理・監督の責任を負う。

2-2-2 岡山県知事の責任

岡山県知事は、電子証明書、相互認証証明書、自己署名証明書、リンク証明書、その他業務運用に必要な証明書の発行及びそれらの証明書に係る失効記録（CRL/ARL）の作成並びに電子証明書及び官職又は職責証明書の有効性を確認する手段の提供等に当たっては、利用者及び署名検証者等に対し、本運用規程に基づき業務を適切に行う。

また、指定認証機関に認証事務の委任を行った場合、指定認証機関が安全かつ適正な認証事務を実施するよう管理・監督の責任を負う。

2-2-3 市町村長の責任

市町村長は、電子証明書の発行及び失効申請の受付、本人確認等に当たっては、本運用規程に基づき業務を適切に行う。

2-2-4 指定認証機関の責任

指定認証機関は、岡山県知事からの委任を受けて次の認証事務を行う。電子証明書、相互認証証明書、自己署名証明書、リンク証明書、その他業務運用に必要な証明書の発行及びそれらの証明書に係る失効記録（CRL/ARL）の作成並びに電子証明書及び官職又は職責証明書の有効性を確認する手段の提供等に当たっては、利用者及び署名検証者等に対し、本運用規程に基づき業務を適切に行う。

2-2-5 利用者の責任

利用者は、本運用規程に従い本サービスを利用する。

2-2-6 署名検証者の責任

署名検証者は、本運用規程に従い電子証明書を検証する。

2-2-7 団体署名検証者の責任

団体署名検証者は、本運用規程に従い電子証明書の有効性を確認する。

2-2-8 署名確認者の責任

署名確認者は、本運用規程に従い電子証明書を検証する。

2-3 財務上の責任

岡山県知事は、岡山県 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。

岡山県 CA に責を帰すべき事由がある場合、岡山県知事は法令等に定める範囲で損害賠償を行うものとする。

2-4 解釈と実行

2-4-1 適用法令

根拠法とその他の関係法令に依拠する。

2-4-2 サービスの細分化や統合、運用体制等の変更と通知

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。

・運用会議の Web
・岡山県の Web

また、指定認証機関は、その名称又は主たる事務所の所在地を変更する場合には、総務大臣及び岡山県知事に届け出る。

2-4-3 監督命令の受容と報告及び立入検査

指定認証機関は、総務大臣より認証事務等の実施に関し監督上必要な命令がある場合及び岡山県知事より認証事務の適正な実施のための指示がある場合には、それを受容しなければならない。

また、指定認証機関は、総務大臣及び岡山県知事より認証事務等の実施状況に関し報告又は立入検査を要求された場合には、それを受容しなければならない。

2-4-4 紛争解決の手続

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

2-5 料金

電子証明書の発行、失効情報及び失効情報ファイルの提供及び認証業務情報の開示に係る料金については、根拠法の規定等に基づきこれを定める。

2-6 公開とリポジトリ

2-6-1 岡山県 CA に関する情報の公開

岡山県 CA は、運用会議の Web 上で次の情報を公開する。

・根拠法及び関係法令
・本運用規程
・岡山県 CA と相互認証した CA の名称
・岡山県 CA と相互認証を取消した CA の名称

・岡山県知事の秘密鍵の危殆化に係る情報　等

岡山県 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。

・自己署名証明書
・相互認証証明書
・リンク証明書
・自己署名証明書、相互認証証明書、リンク証明書の失効記録（ARL）
・利用者の電子証明書等の失効記録（CRL）

2-6-2 公開の頻度

公開する情報の更新頻度は次のとおりとする。

・根拠法及び関係法令並びに本運用規程等の規程は常時最新版を Web 上に掲載する。
・自己署名証明書、相互認証証明書、リンク証明書は発行・更新の都度公開する。
・失効記録（CRL/ARL）は毎日 1 度更新する。

2-6-3 公開情報へのアクセスコントロール

根拠法及び関係法令並びに本運用規程等の規程については、アクセス制限を設けない。

また、リポジトリ上の次の情報についてもアクセス制限を設けない。

・自己署名証明書
・相互認証証明書
・リンク証明書
・自己署名証明書、相互認証証明書、リンク証明書の失効記録（ARL）
　但し、リポジトリ上に公開する利用者の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。

2-6-4 リポジトリに関する要件

リポジトリは、1 日 24 時間、1 年 365 日利用可能とする。但し、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。

2-7 準拠性監査

2-7-1 準拠性監査の頻度

岡山県知事は監査人により年 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。

2-7-2 監査人の識別と資格

岡山県 CA の監査は、監査業務及び認証業務に精通した者が行う。

2-7-3 監査人と被監査部門の関係

岡山県知事は、岡山県 CA と利害関係を有しない者を監査人として選定する。

2-7-4 監査項目

認証業務が、根拠法及び関連法令、並びに本運用規程等に準拠して実施されていることを中心に監査を実施する。

2-7-5 監査結果の取扱い

監査結果は、監査人から岡山県知事に対して監査報告書として提出される。岡山県知事

は、必要に応じて各市町村長、指定認証機関に監査報告書を通知する。

2-7-6 監査指摘事項への対応

指定認証機関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対応を実施する。その結果は評価の上、岡山県知事へ報告する。岡山県知事は、監査指摘事項に対して指定認証機関が対策を実施したことを確認する。

2-8 機密保持と個人情報保護

2-8-1 機密扱いとする情報と個人情報の取扱い

岡山県 CA は、漏えいすることによって岡山県 CA の認証業務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。また利用者の個人情報を適切に保護する。

機密扱いとする情報及び利用者の個人情報を含む情報は、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（本運用規程「5-2-1-1 岡山県 CA における要員」で定める認証局管理責任者とする）、安全に管理する。個人情報の漏えいが発生した場合、別途所定の手続に基づき対策を講ずる。

2-8-2 機密扱いとしない情報

岡山県 CA が保有する情報のうち、自己署名証明書、リンク証明書、相互認証証明書、官職証明書検証サーバ証明書、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、公表する情報として明示的に示すものは機密扱いにしない。

2-8-3 証明書失効情報の公表

岡山県 CA は発行する自己署名証明書、リンク証明書、相互認証証明書及び運営のための関連証明書の失効情報を公表する。失効事由の詳細は公表しない。また電子証明書の失効情報は根拠法に基づき署名検証者等に限定して提供する。

2-8-4 法執行機関への情報開示

規定しない。

2-8-5 民事手続上の情報開示

規定しない。

2-8-6 証明書利用者の請求に基づく情報開示

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、本人確認を実施の上、開示する。

2-8-7 その他の理由に基づく情報開示

規定しない。

2-8-8 証明書利用者の請求に基づく情報の訂正等

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、本人確認を実施の上、訂正等を行う。

2-9 知的財産権

規定しない。

3. 識別と認証

3-1 初回の証明書発行申請

3-1-1 名称の型

電子証明書の発行名義人名及び利用者名は、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、知事の職名により記録する。

また電子証明書に格納される利用者の基本４情報は、電子証明書の拡張領域に記録する。利用者の基本４情報が格納される拡張領域情報を下記に示す。

subjectAltName		
	commonName	氏名（利用者が外国人住民であって、当該外国人住民に係る住民票に通称が記載されている場合にあっては、氏名及び通称）
	dateOfBirth	生年月日
	gender	性別
	address	住所

3-1-3 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。

3-1-4 名称の一意性

岡山県 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。

3-1-5 名称に関する紛争の解決手段

規定しない。

3-1-6 商標の認識・認証・役割

規定しない。

3-1-7 電子証明書の拡張領域に記録する名称の種類と形式

利用者の氏名、通称（電子証明書の交付を受けようとする者が外国人住民であって、当該外国人住民に係る住民票に通称が記載されている場合に限る。）、住所、生年月日、性別を、漢字、ひらがな、カタカナ、アルファベット及びアラビア数字等で記録する。

3-1-8 電子証明書の拡張領域に記録する名称の記録方法に関する規則

氏名等の記録に利用する漢字は住所地市町村の受付窓口端末が採用する文字の種類（JISX0208、JISX0212）の漢字のみ使用可能とする。

氏名等に使用不可能な漢字が存在する場合は、存在する類似の漢字（以下「代替文字」という。）を、利用者の選択等により使用するものとする。

代替文字を使用した場合には、その旨を拡張領域内に表示する。

3-1-9 利用者の識別と認証に関する要件

初回の発行申請の際は、申請者の本人確認を次の方法により行う。但し、本人確認において疑義が生じた場合は、電子証明書を発行しない。

① 発行申請書に記入された基本４情報を住民基本台帳の記録事項と照合することにより、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 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（根拠法の規則第６条第１項に規定された書類）の提示等により確認（本人性の確認）

3-1-10 代理申請の場合の識別と認証に関する要件

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、当該押印に係る印鑑登録証明書、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（根拠法の規則第５条第１項に規定された書類）の提示等により確認

3-1-11 秘密鍵の所有証拠の確認手段

申請者が、住所地市町村に設置される鍵ペア生成装置を用いて、根拠法及び関係法令に基づき鍵ペアの生成を行うことによる。

3-2 電子証明書の更新

電子証明書の更新の際は、利用者の本人確認を次の方法により行う。但し、本人確認において疑義が生じた場合は、電子証明書を更新しない。

① 更新申請書に記入された基本４情報を住民基本台帳の記録事項と照合することにより、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 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の発行した写真の貼付された身分証明書等の提示等により確認（本人性の確認）

なお、更新に伴い失効する電子証明書に係る秘密鍵は、利用者が所定の方法により消去する。

3-3 失効後の再発行

新規発行申請時と同様の本人確認手続を行う。

3-4 失効申請

3-4-1 サービスの利用を取りやめるための失効申請

利用者の秘密鍵により電子署名を付してのオンライン申請又は住所地市町村の窓口における書面による申請により行う。

利用者の本人確認は、オンライン申請の場合は電子署名の検証により行う。住所地市町村の窓口における書面による申請の場合は、電子証明書の発行時と同様の本人確認手続により行う。

3-4-2 利用者の秘密鍵の危殆化の場合の失効申請

速やかに、住所地市町村の窓口に出向き、書面により失効の申請を行う。

利用者の本人確認は、電子証明書の発行時と同様の本人確認手続により行う。

4. 運用要件

4-1 電子証明書の発行申請

4-1-1 発行申請・受付手続

電子証明書の発行申請・受付手続は次のとおり行う。

① 申請者が、住所地市町村において発行申請書を提出するとともに IC カードを提出する。更新の場合は、電子証明書が格納された IC カードを提出する。

② 住所地市町村長は、住民基本台帳の記録内容と照合して、利用者の実在性の確認を行うとともに、運転免許証、旅券等公的機関の発行した写真の貼付された身分証明書等の提示による申請者の本人性の確認を実施。但し、本人確認において疑義が生じた場合は、電子証明書を発行しない。

③ 申請者は、住所地市町村の窓口に備え付けられた鍵ペア生成装置を用いて、鍵ペアを生成。生成した鍵ペアのうち、公開鍵を住所地市町村の窓口に通知。

また、次の手続により、代理人による申請を行うことができる。但し、（1）又は（2）において疑義が生じた場合は、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（押印した印鑑に係る印鑑登録証明書が添付されている場合に限る）及び代理人の本人性を確認するための運転免許証、旅券等の提出又は提示。

（2）代理人は、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、住所地市町村長が適当と認める書類を提示。

（3）代理人は、鍵ペア生成装置を用いて、鍵ペアを生成し、公開鍵を住所地市町村に通知。但し、パスワードの入力（秘密鍵の活性化）は住所地市町村長が行う。

4-1-2 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）、通称（電子証明書の交付を受けようとする者が外国人住民であって、当該外国人住民に係る住民票に通称が記載されている場合に限る。）、住所、生年月日及び性別並びに氏名、通称及び住所に係る代替文字

・代理人申請の場合、上記に加え代理人の氏名、住所

4-1-3 秘密鍵の電磁的記録媒体

耐タンパ性のある IC カードへ格納する。

4-2 電子証明書の発行

4-2-1 発行手続

電子証明書の発行手続は次のとおり行う。

① 住所地市町村長から岡山県知事に対して、申請者の基本 4 情報及び公開鍵を通知。

② 岡山県知事は電子証明書を発行し、住所地市町村長に通知。

4-2-2 電子証明書の形式

ITU-T 勧告 X.509 (03/2000)に準拠し、拡張領域に利用者の氏名、通称、住所、生年月日、性別を漢字、ひらがな、カタカナ、アルファベット及びアラビア数字等で記録する。

また、拡張領域に記録する氏名、通称及び住所の記録に代替文字を使用した場合は、その旨を拡張領域に記録する。

subjectAltName		
	commonName	氏名（利用者が外国人住民であって、当該外国人住民に係る住民票に通称が記載されている場合にあっては、氏名及び通称）
	dateOfBirth	生年月日
	gender	性別
	address	住所
	substituteCharacterOfCommonName	氏名代替文字の使用情報
	substituteCharacterOfAddress	住所代替文字の使用情報

4-2-3 発行申請の拒否

次の事由に該当する場合には、岡山県知事は発行申請を拒否する。

・既に有効な電子証明書を取得しており、失効記録（CRL）にも掲載されていないこと

なお、万が一、二重発行されてしまった場合、岡山県知事は判明次第ただちに発行日の新しい方の電子証明書を失効させる。

4-3 電子証明書の交付

4-3-1 交付手続

電子証明書の交付は次のとおり行う。

① 住所地市町村長は、申請者の IC カードに電子証明書及び岡山県知事の自己署名証明書を記録

② 住所地市町村長は、申請者に対して、本サービスの利用に関する注意事項を告知するとともに、電子証明書の写しを交付

4-3-2 告知事項

住所地市町村長は利用者に次の事項を告知する。

・秘密鍵、その電磁的記録媒体である IC カード、IC カードを活性化するためのパスワードは、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 IC カードの紛失・盗難等の際は、遅滞なく、住所地市町村窓口に届出をし、失効申請を行うこと

4-4 電子証明書の失効及び一時停止

4-4-1 職権失効の事由

4-4-1-1 職権失効の事由

電子証明書の職権失効の事由は次のとおりである。

・利用者の基本４情報等の変更

・利用者の電子証明書に記載された事項について、当該電子証明書に係る利用者に係る住民票に記載されている事項と異なるものが発見された場合等

・電子証明書の二重発行が判明した場合
・岡山県知事の秘密鍵の危殆化

4-4-1-2 証明書を失効できる者

岡山県知事が行う。

4-4-1-3 岡山県知事の秘密鍵の危殆化による失効手続

岡山県知事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職権で失効させ、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。

4-4-2 利用者からの申請による失効

4-4-2-1 利用者からの申請による失効の事由

申請失効の事由は次のとおりである。
・本サービスの利用を取りやめる旨の利用者の申請
・利用者の秘密鍵の危殆化があった旨の申請

4-4-2-2 サービスの利用を取りやめるための失効申請の手続

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。
① 電子署名を付したオンライン申請を受付。失効申請を受理した旨を利用者にオンラインで通知。
② 住所地市町村の窓口において書面による失効申請を受付。岡山県知事に失効処理を依頼。失効申請を受理した旨を記載した書面を利用者に交付。

4-4-2-3 利用者の秘密鍵の危殆化等の場合の失効申請の手続

利用者の秘密鍵の危殆化等の場合の失効手続は次のとおり行う。
① 住所地市町村において書面による失効申請を受付。
② 岡山県知事に失効処理を依頼。失効処理を完了した旨を記載した書面を利用者に交付。

4-4-2-4 利用者の電子証明書が失効した場合の回復手段

一度失効処理した電子証明書の回復は行わず、新たな申請手続により、新たな電子証明書を発行する。

4-4-2-5 利用者の秘密鍵が危殆化した場合の回復手段

新たな申請手続により、新たな電子証明書を発行する。

4-4-3 失効記録（CRL/ARL）の要件

所定の時間までに受付を完了した失効情報を反映して、毎日一度新しい失効記録（CRL/ARL）を作成し、作成した失効記録（CRL/ARL）は許可された署名検証者等に対して速やかに開示する。

また許可された署名検証者等への失効記録（CRL/ARL）の提供は、1 日 24 時間、1 年 365 日利用可能とする。但し、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。

4-4-4 失効情報の提供方法

4-4-4-1 失効情報の提供方法

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）

4-4-4-2 OCSP レスポンダ照会方法の回答内容

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		
1	keyCompromise	利用者の秘密鍵が危殆化した。
2	cACompromise	岡山県知事の秘密鍵が危殆化した。
3	affiliationChanged	電子証明書の記載内容に変更が生じた。
4	superseded	電子証明書を更新した。
5	cessationOfOperation	電子証明書の必要性がなくなった。(使用しなくなった。)

4-4-4-3 OCSP レスポンダ照会方法の要件

事前に岡山県知事まで届け出て、アクセス権の付与を受けることが必要である。

4-4-4-4 失効記録（CRL/ARL）提供方法の回答内容

失効記録（CRL/ARL）のフォーマットは ITU-T 勧告 X.509(03/2000)に準拠する。

失効記録（CRL）は、原則として市町村単位で作成する区分 CRL とし、失効した電子証明書のシリアル番号、失効事由（本運用規程「4-4-4-2 OCSP レスポンダ照会方法の回答内容」の失効事由と同様）及び失効年月日が記載される。署名検証者等はリポジトリに格納された失効記録（CRL/ARL）を適宜取得して電子証明書の検証を行う。

4-4-4-5 失効記録（CRL/ARL）の提供に必要な要件

事前に岡山県知事まで届け出て、アクセス権の付与を受けることが必要である。

4-4-5 一時停止要件

岡山県知事が発行する電子証明書の一時停止は行わない。

4-4-6 一時停止申請者

規定しない。

4-4-7 一時停止要求手続

規定しない。

4-4-8 一時停止期間

規定しない。

4-4-9 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。但し、岡山県知事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。

4-4-10 失効記録（CRL/ARL）の発行最大遅延時間

最後に発行した失効記録（CRL/ARL）の有効期間が満了する前に新たな失効記録（CRL/ARL）を発行する。

4-4-11 失効記録（CRL/ARL）の確認

署名検証者等は岡山県知事の発行する失効記録（CRL/ARL）によって電子証明書の有効性を確認しなければならない。

4-5 失効情報等の提供状況についての報告書作成

指定認証機関は、保存に係る失効情報及び失効情報ファイルの提供状況について報告書を作成する。指定認証機関は、当該報告書を官報に公告し、かつ指定認証機関の事務所に備えて置き、5 年間一般の閲覧に供しなければならない。

報告書の記載事項は次のとおりである。

・失効情報等の提供先
・失効情報等の提供を行った年月
・提供した失効情報等の件数
・失効情報等の提供の方法

4-6 相互認証証明書の発行申請

個人認証 BCA に対する相互認証証明書の発行申請は、個人認証 BCA の定める手順に基づいて行う。

4-7 相互認証証明書の発行

岡山県知事は、所定の手続に基づき、個人認証 BCA を運営する者の真偽を確認する。個人認証 BCA の定める手続に基づく接続テスト完了後、個人認証 BCA から提出された証明書発行要求に対し、岡山県知事の署名を付した相互認証証明書を発行する。

4-8 相互認証証明書の受領

岡山県知事は、個人認証 BCA から発行された相互認証証明書を所定の手続に基づいて受け入れ、個人認証 BCA に受領書を渡す。同様にして、岡山県知事は、個人認証 BCA に発行した相互認証証明書を所定の手続に基づいて個人認証 BCA に渡し、受領書を受け取る。これらの受領確認をもって、相互認証証明書の相互の受け入れ完了とする。

また、岡山県知事は、個人認証 BCA と相互に取り交わした相互認証証明書を対にした相互認証証明書ペアを生成し、リポジトリに登録する。

4-9 相互認証証明書の更新

岡山県知事は、次の(1)～(4)の場合には相互認証証明書及び相互認証証明書ペアを更新する。

ここで、相互認証証明書の更新における発行申請、発行及び受領の各手続は、本運用規程「4-6 相互認証証明書の発行申請」、「4-7 相互認証証明書の発行」及び「4-8 相互認証証明書の受領」に準じる。また、リポジトリ上の相互認証証明書ペアは速やかに最新のものに置換する。

(1) 個人認証 BCA から発行された相互認証証明書が有効期限に近づいた場合
(2) 個人認証 BCA に対して発行した相互認証証明書が有効期限に近づいた場合
(3) 個人認証 BCA から発行された相互認証証明書の記載内容に変更が生じる場合
(4) 個人認証 BCA に対して発行した相互認証証明書の記載内容に変更が生じる場合

4-10 相互認証証明書の失効

4-10-1 失効事由

岡山県 CA 又は個人認証 BCA に次の事由が発生した場合には、岡山県 CA は個人認証 BCA に発行した相互認証証明書を失効させ、個人認証 BCA は岡山県 CA に発行した相互認証証明書を失効させる。

・秘密鍵の危殆化
・相互認証証明書の更新
・相互認証の終了（相互認証基準違反に伴う相互認証の終了の場合を含む）

4-10-2 失効申請者

個人認証 BCA から岡山県 CA に対する失効申請は、個人認証 BCA の責任者が行う。
岡山県 CA から個人認証 BCA に対する失効申請は、岡山県知事が行う。

4-10-3 失効申請及び失効処理手順

相互認証証明書の失効申請は、個人認証 BCA の定める手続に基づいて行う。

4-11 セキュリティ監査手続

4-11-1 セキュリティ監査手順

内部監査者（本運用規程「5-2-1 高い信頼性が要求される要員とその役割」を参照）は、岡山県 CA システム及びリポジトリにおける発生事象を記録したログ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。

4-11-2 監査ログに記録する情報

岡山県 CA システム及びリポジトリにおけるセキュリティに関する重要な事項を対象に、アクセスログ及び操作ログ等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
・岡山県知事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
・岡山県 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）

4-11-3 監査ログの検査周期

内部監査者はセキュリティ監査を週次で行う。

4-11-4 監査ログの保管期間

1年間保管する。

4-11-5 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。

4-11-6 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。

4-11-7 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。

4-11-8 脆弱性の検証

監査ログを検査することにより、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。

4-11-9 監査ログの収集システム

監査ログの収集機能は、岡山県 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。

4-12 記録の保管（アーカイブ）

4-12-1 紙で保管する情報

4-12-1-1 保管する情報の種類

次の情報を保管する

(岡山県知事)

・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
・署名検証者等との取り決めに関する書類
・認証業務情報の開示・訂正等に関する書類
・監査報告書　等

(指定認証機関)

・指定認証機関の指定・変更に関する書類
・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・収支予算に関する書類
・事業報告書・収支決算書
・認証業務情報の開示・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
・手数料に関する書類　等

(市町村長)

・電子証明書の発行申請に関する書類（発行申請書等）

・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

4-12-1-2 保管期間

保管期間は、10 年間とする。但し電子証明書の発行申請に関する書類は 13 年とする。

4-12-1-3 保管情報の保護

指定認証機関に保管する情報は、改ざん防止対策とともに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し、温度、湿度等環境に配慮した保護対策を施す。市町村及び都道府県に保管する情報は、適切な場所に保管する。

4-12-1-4 保管情報の検証

保管情報が記載された紙の状態、可読性等の確認を年 1 回行う。

4-12-2 デジタルデータとして保管する情報

4-12-2-1 保管する情報の種類

次の情報を指定認証機関に保管する
・失効申請書（岡山県知事へのオンライン申請の場合）
・電子証明書
・相互認証証明書
・自己署名証明書
・リンク証明書
・官職証明書検証サーバ証明書
・OCSP レスポンダ証明書
・失効情報
・失効記録（CRL/ARL）
・失効情報ファイル
・失効記録（CRL/ARL）提供方法の利用履歴
・OCSP レスポンダ照会方法の利用履歴
・各種ログ（監視用ログ、起動停止ログ、操作ログ）等

4-12-2-2 保管期間

保管期間は、10 年間とする。但し、発行済み電子証明書は 13 年、失効情報は当該失効情報を記録した日から当該失効情報に係る電子証明書の有効期間の満了日までとする。

4-12-2-3 保管情報の保護

保管情報には、アクセス制御を施すとともに、改ざん防止対策を施す。
保管情報は、月次で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。

4-12-2-4 保管情報のバックアップ手順

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。

4-12-2-5 記録に付与するタイムスタンプの要件

保管情報には、タイムスタンプ（時刻情報）を付与する。

4-12-2-6 保管情報の検証

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。

4-13 岡山県知事の鍵の更新

5 年ごとに岡山県知事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。

4-14 鍵の危殆化と災害復旧

4-14-1 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。

4-14-2 岡山県知事の秘密鍵が危殆化した場合の対処

次のとおり対処する。

・電子証明書の発行業務を停止
・その秘密鍵により署名したすべての電子証明書、相互認証証明書等を失効させ、失効記録（CRL/ARL）に記録して、公表する
・個人認証 BCA に通知する

4-14-3 災害等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、予備機を確保し、バックアップデータを用いて運用を行う。

4-15 苦情・問合せ処理

岡山県知事、指定認証機関及び市町村長は認証事務等に関する苦情・問合せに対し、適切かつ迅速な処理に努めなければならない。

4-16 システム運用

安全かつ適切なシステム運用を行う。詳細については別途定める。

4-17 認証業務の終了

規定しない。

4-18 認証事務の休廃止

指定認証機関は、認証事務等の全部又は一部を休止し、又は廃止する場合には、総務大臣の許可を受けなければならない。

また、そのために岡山県知事が認証事務を行うこととなった場合、指定認証機関は、以下の事項を行わなければならない。

・引き継ぐべき認証事務を岡山県知事に引き継ぐ。
・引き継ぐべき認証事務に関する帳簿、書類、資料及び電磁的記録媒体を岡山県知事に引き渡す。

その他総務大臣又は岡山県知事が必要と認める事項を行う。

5. 物理面、手続面、人事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 岡山県 CA

5-1-1-1 施設の位置と建築

岡山県 CA の施設は、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、建物構造上、耐震、耐火及び不正侵入防止のための対策を講じる。また、使用する機器等を災害及び不正侵入から防護された安全な場所に設置する。

5-1-1-2 物理的アクセス

岡山県 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。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、岡山県 CA の認証局管理責任者が付与する。

岡山県 CA の施設は、監視員を配置して監視システムにより、24 時間 365 日監視を行う。

5-1-1-3 電力と空調

岡山県 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。

5-1-1-4 水害対策

岡山県 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。

5-1-1-5 地震対策

岡山県 CA の設備を設置する建物は耐震構造とし、機器・什器の転倒及び落下を防止する対策を講じる。

5-1-1-6 防火対策

岡山県 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。

5-1-1-7 電磁波対策

岡山県 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。

5-1-1-8 媒体（磁気媒体等）管理

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保管庫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。

5-1-1-9 廃棄物処理

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

5-1-1-10 オフサイトバックアップ

規定しない。

5-1-2 市町村の施設

5-1-2-1 施設の位置と建築

住所地市町村の施設とする。

5-1-2-2 物理的アクセス

鍵ペア生成装置、受付窓口端末は住所地市町村の職員の人的監視が行き届く場所に設置する。また鍵ペア生成装置、受付窓口端末に係わる保守を適切に行う。

受付窓口端末の操作は利用者の本人確認等を行う者が実施する。操作者の認証は、ID／パスワード方式にて行う。

5-1-2-3 保管情報管理

本運用規程「4-12-1-1 保管する情報の種類」に係わる書類は、適切な場所に保管する。

5-1-2-4 廃棄物処理

秘密扱いとする情報を含む書類・記憶媒体及び受付窓口端末、鍵ペア生成装置等の廃棄については、所定の手続に基づいて適切に廃棄処理を行う。

5-2 手続面のセキュリティ管理

5-2-1 高い信頼性が要求される要員とその役割

5-2-1-1 岡山県 CA における要員

岡山県 CA のシステム運用に係わる要員は次の通りである。

(1) 認証局管理責任者

認証局管理責任者は､岡山県 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
- 岡山県知事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
- 要員等への作業指示及び作業結果の確認
- HSM（岡山県知事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。）の保守管理
- 認証業務情報開示請求に対する対応管理
- 認証業務情報訂正等請求に対する対応管理
- 問合せ・苦情処理対応管理
- 認証業務情報保護委員会の管理
- 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
- 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実施管理
- その他岡山県 CA の運営及び運用に関する統括

・個人情報の管理

(2) 秘密鍵管理者

秘密鍵管理者は、岡山県知事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。なお、作業は複数人の秘密鍵管理者が行う。

・岡山県知事の秘密鍵等のバックアップ媒体の保管管理

・岡山県知事の秘密鍵等生成、自己署名証明書発行時の HSM に対する操作

・岡山県知事の秘密鍵等の更新時における HSM に対する操作

・岡山県知事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

(3) 受付担当者

受付担当者は、相互認証証明書等の発行、更新及び失効申請の受付、個人認証 BCA との連絡調整業務及び申請書類等の管理を行う。

(4) 審査担当者

審査担当者は、相互認証証明書等の発行、更新及び失効申請の審査業務を行う。

(5) 審査承認者

審査承認者は、審査担当者からの相互認証証明書等の発行申請、更新申請及び失効申請の審査結果に対して承認業務を行う。

(6) 上級操作員

上級操作員は、岡山県知事の秘密鍵を使用する次の業務を行う。また、作業は複数人の上級操作員が行う。

・HSM の活性化及び非活性化

・自己署名証明書発行、更新、失効処理

・相互認証証明書発行、更新、失効処理

・官職証明書検証サーバ証明書発行、更新、失効処理

・OCSP レスポンダ証明書発行、更新、失効処理

・岡山県 CA 電子証明書等ポリシーの設定登録及び変更

・その他岡山県 CA システムの運用管理業務

(7) リポジトリ操作員

リポジトリ操作員は、リポジトリの設定管理に関する業務を行う。

(8) 一般操作員

一般操作員は、ネットワーク機器等の運用及び維持管理を行う。

(9) 内部監査者

内部監査者は、岡山県 CA システム及びリポジトリ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 市町村における要員

市町村における要員は、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 岡山県 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別途定める所定の手続に基づいて指示する。

③ 上級操作員の権限

上級操作員は一般操作員等に対し、別途定める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。

5-2-3 岡山県 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。

5-3 岡山県 CA における人事面のセキュリティ管理

5-3-1 要員の個人の背景のチェックと許可手順

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。

5-3-2 各要員に対する訓練の手順

教育訓練計画書に従い、各要員に必要な訓練を実施する。

5-3-3 要員間の業務交代と頻度、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。

5-3-4 許可されていない行動

各要員が許可されていない行動を行った場合には、あらかじめ定められた懲戒処分を課す。

5-3-5 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。

6. 技術的セキュリティ管理

6-1 鍵ペア生成とインストール

6-1-1 岡山県知事の鍵

6-1-1-1 岡山県知事の鍵ペアを生成する者、生成方法

岡山県知事の鍵ペアは、複数人の秘密鍵管理者が本運用規程「6-1-1-3 鍵ペアを生成するハードウェア／ソフトウェア」に定める設備を用いて生成する。

6-1-1-2 鍵長

RSA 暗号方式に基づく 2048 ビットの鍵を使用する。

6-1-1-3 鍵ペアを生成するハードウェア／ソフトウェア

FIPS140-1 レベル 3 相当の HSM。

6-1-1-4 秘密鍵の利用目的

電子署名用とする。

6-1-1-5 個人認証 BCA の公開鍵の受領

岡山県 CA は相互認証証明書の取り交わしにおいて、個人認証 BCA の公開鍵を安全かつ確実に受取る。

6-1-1-6 岡山県知事の公開鍵の配布

岡山県知事の自己署名証明書は、電子証明書の発行の際に IC カードに格納し、利用者に交付する。また安全かつ確実な手段で署名検証者等に配布する。

6-1-2 利用者の鍵

6-1-2-1 利用者の鍵ペアを生成する者、生成方法

利用者本人が住所地市町村の鍵ペア生成装置により生成する。

6-1-2-2 利用者の公開鍵を住所地市町村等に安全に提供する方法

住所地市町村において、直接利用者から IC カードに格納された公開鍵を受領する。

6-1-2-3 鍵長

RSA 暗号方式に基づく 1024 ビットの鍵を使用する。

6-1-2-4 鍵ペアを生成するハードウェア／ソフトウェア

住所地市町村の鍵ペア生成装置。

6-1-2-5 秘密鍵の利用目的

電子署名用とする。

6-2 秘密鍵保護

6-2-1 岡山県知事の秘密鍵

6-2-1-1 秘密鍵の保管について、要求される基準

FIPS140-1 レベル 3 相当の HSM により保護する。

6-2-1-2 秘密鍵の複数人制御

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。

6-2-1-3 秘密鍵の預託（エスクロー）

秘密鍵の預託は行わない。

6-2-1-4 秘密鍵のバックアップ

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、暗号化して安全に保管する。但し秘密鍵管理者は、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。

6-2-1-5 秘密鍵の保管（アーカイブ）

秘密鍵のアーカイブは行わない。

6-2-1-6 暗号モジュールへの秘密鍵の格納

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、暗号モジュールへ格納する。

6-2-1-7 秘密鍵の活性化

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。

6-2-1-8 秘密鍵の非活性化

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。

6-2-1-9 秘密鍵の破棄

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が暗号モジュールを初期化等の方法により完全に利用できない状態にする。なお、暗号モジュールを室外に持ち出す場合は、物理的に暗号モジュールを破壊する。

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こととする。

6-2-2 利用者の秘密鍵

6-2-2-1 秘密鍵の保管について、要求される基準

「公的個人認証サービスカードアプリケーション外部インターフェース仕様書 1.1 版」に準拠したカードアプリケーションを搭載しており、秘密鍵が物理的に読み出せない耐タンパ性を有した IC カードにより保護する。

6-2-2-2 秘密鍵の預託（エスクロー）

岡山県知事が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。

6-2-2-3 秘密鍵のバックアップ

秘密鍵はICカード内に保管し、バックアップは行わない。

6-2-2-4 暗号モジュール（ICカード）への秘密鍵の格納

利用者の秘密鍵は、住所地市町村の鍵ペア生成装置で生成し、利用者のICカードに格納する。ICカードに格納後、鍵ペア生成装置で生成された秘密鍵は、鍵ペア生成装置上から完全に削除されることとする。

6-2-2-5 秘密鍵の活性化

利用者の秘密鍵は、利用者により、パスワードを用いて活性化する。

6-2-2-6 秘密鍵の非活性化

ICカードの操作により非活性化する。

6-2-2-7 秘密鍵の破棄

利用者の秘密鍵の破棄を行う場合、利用者は住所地市町村の受付窓口端末及び鍵ペア生成装置で破棄する。

6-3 鍵ペア生成管理に関する他の局面

6-3-1 岡山県知事の鍵

6-3-1-1 公開鍵の保管

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「4-12 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 公開鍵、秘密鍵の使用期間

岡山県知事の自己署名証明書の有効期間は10年とする。秘密鍵の使用期間は、鍵を生成した日から起算して5年とし、5年ごとに鍵更新を行う。

但し、暗号のセキュリティ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 利用者の鍵

利用者の公開鍵と秘密鍵の使用期間は、鍵を生成した日から起算して3年とする。

但し、暗号のセキュリティ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。

6-4 活性化データ

6-4-1 岡山県知事の鍵

6-4-1-1 活性化データの生成とインストール

岡山県知事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 活性化データの保護

岡山県知事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 利用者の鍵

6-4-2-1 活性化データの生成とインストール

利用者の秘密鍵の活性化データ（パスワード）は、利用者自身が鍵ペア生成装置にて、鍵ペアの生成時に IC カードへ設定する。

6-4-2-2 活性化データの保護

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。

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機能要件

岡山県 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 システム開発におけるセキュリティ管理

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 システム運用面におけるセキュリティ管理

6-6-2-1 岡山県 CA

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 市町村

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

6-7 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、外部ネットワークと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 暗号モジュールの技術管理

本運用規程「6-1-1-3 鍵ペアを生成するハードウェア／ソフトウェア」、「6-2-1-1 秘密鍵の保管について、要求される基準」において定める。

7. 証明書と失効記録（CRL/ARL）の内容

7-1 証明書

7-1-1 電子証明書

電子証明書には下記の情報を記載する。詳細はプロファイル設計書に定める。

・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（岡山県 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（岡山県知事が当該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（当該電子証明書を発行した岡山県知事名が X.500 識別名で記述される）
・有効期間の開始日（当該電子証明書の発行日）
・有効期間の終了日（発行日の 3 年後）
・公開鍵（利用者の公開鍵）
・拡張情報（利用者の基本 4 情報や鍵使用目的等が記載される）

7-1-2 相互認証証明書

個人認証 BCA と相互認証を行う際に必要となる相互認証証明書には下記の情報を記載する。詳細はプロファイル設計書に定める。

・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（岡山県 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（岡山県知事が当該相互認証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（当該相互認証証明書を発行した岡山県知事名が X.500 識別名で記述される）
・有効期間の開始日（当該相互認証証明書を有効とする日）
・有効期間の終了日（当該相互認証証明書を有効とする日から起算して 5 年後）
・公開鍵（相互認証 CA の公開鍵）
・拡張情報

7-1-3 自己署名証明書

岡山県知事の自己署名証明書には下記の情報を記載する。詳細はプロファイル設計書に定める。

・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（岡山県 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（岡山県知事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岡山県知事名が 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（岡山県知事の公開鍵）
・拡張情報

7-1-4 リンク証明書

岡山県知事の鍵更新時に必要となるリンク証明書には下記の情報を記載する。詳細はプロファイル設計書に定める。

・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（岡山県 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（岡山県知事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岡山県知事名が X.500 識別名で記述される）
・有効期間の開始日（OldWithNew：旧世代の鍵ペアを作成した日、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間の終了日、NewWithOld：旧世代の自己署名証明書の有効期間の終了日）
・公開鍵（OldWithNew：旧世代の公開鍵、NewWithOld：新世代の公開鍵）
・拡張情報

7-2 失効記録（CRL/ARL）

7-2-1 電子証明書の失効記録（CRL）

電子証明書失効記録（CRL）には下記の情報を記載する。詳細はプロファイル設計書にある CRL のプロファイルに定める。

・バージョン情報（CRL のフォーマットバージョン番号）
・署名アルゴリズム（岡山県知事が当該 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 を発行した岡山県知事名が 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

7-2-2 相互認証証明書の失効記録（ARL）

相互認証証明書失効記録（ARL）には下記の情報を記載する。詳細はプロファイル設計書にある ARL のプロファイルに定める。

・バージョン情報（ARL のフォーマットバージョン番号）
・署名アルゴリズム（岡山県知事が当該 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 を発行した岡山県知事名が 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

7-2-3 自己署名証明書の失効記録（ARL）

自己署名証明書失効記録（ARL）には下記の情報を記載する。詳細はプロファイル設計書にある ARL のプロファイルに定める。

・バージョン情報（ARL のフォーマットバージョン番号）
・署名アルゴリズム（岡山県知事が当該 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 を発行した岡山県知事名が 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

7-2-4 リンク証明書の失効記録（ARL）

リンク証明書失効記録（ARL）には下記の情報を記載する。詳細はプロファイル設計書にある ARL のプロファイルに定める。

・バージョン情報（ARL のフォーマットバージョン番号）
・署名アルゴリズム（岡山県知事が当該 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 を発行した岡山県知事名が 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

8. 運用規程の管理

8-1 運用規程変更管理

岡山県知事は、本運用規程を必要に応じて変更する。

8-2 開示及び通知

本運用規程を変更した場合には、岡山県知事は速やかに変更した運用規程を Web 上で公表する。これをもって利用者、署名検証者等及び署名確認者への通知とする。

8-3 運用規程承認手続

岡山県知事の決定をもって有効なものとする。