準拠性監査報告書様式（署名用）

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
1	はじめに							
1.1	概要	CPとして監査目標項目なし。						
1.2	文章の名前と識別 本ポリシの名称を「保健医療福祉分野PKI認証局　署名用証明書ポリシ」とする。本ポリシにて発行する証明書及び関連サービスに、厚生労働省より「保健医療福祉分野の公開鍵関連分野」のオブジェクト識別子（OID）を「1.2.392.100495.1」と割り当てる。その基本体系を示す。 以下省略	1)準拠ポリシの名称を「保健医療福祉分野PKI認証局　署名用証明書ポリシ」とすること。 2)HPKI署名用証明書ポリシのOIDが 1.2.392.100495.1.5.1.1.3.1 3)HPKI署名テスト用証明書ポリシのOIDが 1.2.392.100495.1.5.1.1.0.1であること 4）上位認証局を利用する場合はその証明書のOIDも記載すること。	CPS等関連規定を閲覧し、1)、2)、3)および4)のOID項目が満たされていることを確認する。					
1.3	PKIの関係者							
1.3.1	認証局 認証局（CA）は、証明書発行局（IA)と登録局（RA）により構成される。保健医療福祉分野PKIでは、認証局は複数の階層構成をとることができる。また、保健医療福祉分野PKIのルートCA(Root CA)は、本CPに準拠する他の保健医療福祉分野PKI のRoot CAと相互認証を行うことがある。 発行局は証明書の作成、発行、失効及び失効情報の開示及び保管の各業務を行う。 但し、認証局は認証局の運営主体で定めるCPSの遵守及び個人情報の厳正な取り扱いを条件に、契約等を取り交わすことで業務の一部又は全部を外部に委託することができる。	1)認証局（CA）は、証明書発行局（IA)と登録局（RA）により構成されていること。 2)認証局が複数の階層構成をとる場合は頂点の認証局（Root CA)を含めた各階層の認証局の構成、例えば階層図、名称、証明書ポリシのOID等を明確にすること。 他のRoot CAと相互認証を行っている場合はその相手を明確にすること。 3)発行局は証明書の作成、発行、失効及び失効情報の開示及び保管の各業務を行うこと。 4)業務の一部又は全部を外部に委託する場合は、認証局は認証局の運営主体で定めるCPSの遵守及び個人情報の厳正な取り扱いを条件に、契約等を取り交わすこと。	1)CPS等関連規定を閲覧し、認証局が、証明書発行局と登録局により構成されていることを確認する。 2)階層化されている場合は、CPS等関連規定を閲覧し各階層の認証局および、他のRoot CAと相互認証を行っている場合はその相手が明確され構成されていることを確認する。 3)CPS等関連規定を閲覧し、発行局の業務内容が証明書の作成、発行、失効及び失効情報の開示及び保管の各業務となっていることを確認する。 4)業務の一部又は全部を外部に委託する場合は、委託先との契約書等を閲覧し、認証局の運営主体で定めるCPSの遵守及び個人情報の厳正な取り扱いが条件になっていることを確認する。					
1.3.2	登録局 登録局は、適切な申請者の本人確認、登録の業務を行い、発行局への証明書発行要求を行う。なお、証明書登録の業務は、発行、失効を含む。 但し、登録局は認証局の運営主体で定めるCPSの遵守及び個人情報の厳正な取り扱いを条件に、契約等を取り交わすことで業務の一部を外部に委託することができる。	1)登録局は、適切な申請者の本人確認、登録の業務を行い、発行局への証明書発行要求を行うこと。なお、証明書登録の業務は、発行、失効を含めること。 2)登録局が業務の一部を外部に委託する場合は認証局の運営主体で定めるCPSの遵守及び個人情報の厳正な取り扱いを条件にした契約等を取り交わすこと。	1)CPS等関連規定を閲覧し、登録局の業務内容が適切な申請者の本人確認、登録の業務を行い、発行局への証明書発行要求の業務となっていることを確認する。なお、証明書登録の業務は、発行、失効を含めていることを確認する。 2)業務の一部を外部に委託する場合は、委託先との契約書等を閲覧し、認証局の運営主体で定めるCPSの遵守及び個人情報の厳正な取り扱いが条件になっていることを確認する。					
1.3.3	加入者 加入者とは、証明書所有者である。証明書所有者とは、証明書発行申請を行い認証局により証明書を発行される個人をさす。 証明書所有者の範囲は次のとおりとする。 ・保健医療福祉分野サービス提供者及び利用者 上記の提供者の内、以下の者が、その有する資格において、あるいは管理者として署名を行う場合は、「その資格を所有していること」あるいは「管理者であること」を証明書に記載しなくてはならない。 ・保健医療福祉分野に関わる国家資格を有する者 ・医療機関等の管理者	1) 認証局に証明書発行申請を行い認証局により証明書を発行される個人は「保健医療福祉分野サービス提供者及び利用者」とすること。 2) 上記のサービス提供者である以下の者はその資格、役割を証明書内に記載することができること。 ・保健医療福祉分野に関わる国家資格所有者 ・医療機関等の管理者 3)利用者がその有する資格において、あるいは管理者として署名を行う場合は、「その資格を所有していること」あるいは「管理者であること」を証明書に記載しなくてはならないことを、例えば証明書申請時に提出する加入契約書で確約させること。	1)CPS等関連規定を閲覧し、証明書を発行する対象が「保健医療福祉分野サービス提供者及び利用者」であることを確認する。 2) CPS等関連規定を閲覧し、上記のサービス提供者のうち「保健医療福祉分野に関わる国家資格所有者」および「医療機関等の管理者」である場合はその資格、役割を証明書内に記載することができることを確認する。 3)証明書申請時に提出する加入契約書等を閲覧し、その有する資格において、あるいは管理者として署名を行う場合は、「その資格を所有していること」あるいは「管理者であること」を証明書に記載しなくてはならないことを確約させていることを確認する。					
1.3.4	検証者 デジタル署名を公開鍵証明書の公開鍵で検証する者。	「デジタル署名を公開鍵証明書の公開鍵で検証する者。」と定義されていること。	CPS等関連規定を閲覧し、「デジタル署名を公開鍵証明書の公開鍵で検証する。」と定義されていることを確認する。					
1.3.5	その他関係者 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されているか確認する。					

準拠性監査報告書様式（署名用）

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
1.4	証明書の使用方法							
1.4.1	適切な証明書の使用 本CPで定める加入者証明書は、次に定める利用目的にのみ使用できる。 （1）医療従事者等の保健医療福祉分野サービス提供者の署名検証用 （2）患者等の保健医療福祉分野サービス利用者の署名検証用	本CPに準拠する認証局が発行する加入者証明書は、次に定める利用目的にのみ使用できること。 （1）医療従事者等の保健医療福祉分野サービス提供者の署名検証用 （2）患者等の保健医療福祉分野サービス利用者の署名検証用	CPS等関連規定を閲覧し、 （1）医療従事者等の保健医療福祉分野サービス提供者の署名検証用 （2）患者等の保健医療福祉分野サービス利用者の署名検証用 のみに利用されていることを確認する。 また、証明書のKeyUsageがNonRepudiationのビットのみ立てられていることを確認すること。					
1.4.2	禁止される証明書の使用 本CPで定める加入者証明書は、署名検証以外には用いないものとする。	本CPに準拠した認証局が発行する加入者証明書は、署名検証以外には用いられないように、利用者同意書等により明記すること。	利用者同意書等を閲覧し、加入者証明書が、署名検証以外には用いられないように記述されていることを確認する。					
1.5	ポリシ管理							
1.5.1	本ポリシを管理する組織 本CPの管理組織は、「保健医療福祉分野における公開鍵基盤認証局の整備と運営に関する専門家会議」（以下、「HPKI認証局専門家会議」という）とする。	「HPKI認証局専門家会議」に管理されたCPを用いること。	CPS等関連規定を閲覧し、「HPKI認証局専門家会議」に管理されたCPを用いること確認する。					
1.5.2	1.5.2　問い合わせ先 本CPに関する問い合わせ先を以下のように定める。なお、CPSの問い合わせ先は各CPSにより定めるものとする。 【問い合わせ先】 窓口：厚生労働省医政局研究開発振興課医療情報技術推進室 受付時間：10時～17時 電話番号：03-3595-2430(ダイヤルイン) FAX番号：03-3503-0595 e-mailアドレス：hpki-cp@mhlw.go.jp	CPSの問い合わせ先が各認証局における適切な問い合わせ先となっていること。	CPS等関連規定を閲覧し、CPSの問い合わせ先が各認証局における適切な問い合わせ先となっていることを確認する。					
1.5.3	CPSのポリシ適合性を決定する者 CPSの本CPへの適合性を決定する者は、HPKI認証局専門家会議とする。	CPSの適合性を決定する為にHPKI認証局専門家会議に準拠性審査を受けることがCPS等に明記されていること。	CPS等関連規定を閲覧し、HPKI認証局専門家会議に準拠性審査を受けることによりCPに適合していることを決定されることが明記されていることを確認する」					
1.5.4	CPS承認手続き 本CPは、HPKI認証局専門家会議によって承認されるものとする。なお、CPSの承認手続きはCPSにより定めるものとする	CPSの承認手続きが記載されていること。	CPS等関連規定を閲覧し、CPSの承認手続きが記載されていることを確認する。					
1.6	定義と略語	CPとして監査目標項目なし。						
2	公開およびリポジトリの責任							
2.1	リポジトリ リポジトリは認証局の証明書と失効情報及び加入者の失効情報を保持する。	リポジトリは認証局の証明書と失効情報及び加入者の失効情報を保持すること。	CPS等関連規定を閲覧して、リポジトリが認証局の証明書と失効情報及び加入者の失効情報を保持していることを確認する。					
2.2	証明書情報の公開 認証局は、以下の情報を検証者と加入者が入手可能にする。 ＜検証者に公開する事項＞ ・CAの公開鍵証明書 ・本CP ・CRL/ARL ・検証者の表明保証に関する文書 ＜加入者に公開する事項＞ ・認証局の定めるCPS ・認証局の定める加入者に関する各種規定/基準	認証局は、CPにあげた情報を検証者と加入者が入手可能とすること。	CPS等関連規定を閲覧し、CPにあげた情報を検証者と加入者が入手可能となっていることを確認する。					
2.3	公開の時期又はその頻度 認証局は、認証局に関する情報が変更された時点で、その情報を公開するものとする。証明書失効についての情報は、本CP「4.9　証明書の失効と一時停止」に従うものとする。	1）認証局は、認証局に関する情報が変更された時点で、その情報を公開すること。 2）証明書失効についての情報は、CPの「4.9　証明書の失効と一時停止」に従うこと。	CPS等関連規程を閲覧し、認証局に関する情報が変更された時点で、その情報を公開することが定められていることを確認する。また、証明書失効に付いての情報はCPの4．９に従っていることを確認する。					

準拠性監査報告書様式（署名用）

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
2.4	リポジトリへのアクセス管理 CP、CPS、証明書及びそれらの証明書の現在の状態などの公開情報は、加入者及び検証者に対しては読み取り専用として公開する。	CP、CPS、証明書及びそれらの証明書の現在の状態などの公開情報は、加入者及び検証者に対しては読み取り専用として公開すること。	CPS等関連規程を閲覧し、CP、CPS、証明書及びそれらの証明書の現在の状態などの公開情報を、加入者及び検証者に対しては読み取り専用として公開していることを確認する。					
3	識別及び認証							
3.1	名称決定							
3.1.1	名称の種類 本CPに基づいて発行される証明書に使用されるサブジェクト名は加入者名とする。 加入者名はX.500のDistinguished Name を使用する。保健医療福祉分野PKIでは、CはJPとする。またCommonNameは必須で、加入者が自然人である場合、加入者の氏名（ローマ字表記）を記載する。	証明書が以下の要件を満たすこと。 (1)サブジェクト名が加入者名となっていること (2)加入者名に、X.500 の Distinguished Name を使用していること (3)C が JP となっていること (4)CommonName が加入者の氏名でローマ字で表記されていること	CPSまたはプロファイル仕様書等を閲覧し、サブジェクト名が加入者名であり且つ決められたプロファイルになっていることを確認する。					
3.1.2	名称が意味を持つことの必要性 本CPにより発行される証明書の相対識別名は、検証者によって理解され、使用されるよう意味のあるものとする。	CPの証明書プロファイルに従った記載がされていること。	CPSまたはプロファイル仕様書等を閲覧し、相対識別名が決められたプロファイルになっていることを確認する。					
3.1.3	加入者の匿名性又は仮名性 規定しない。	CPとして監査目標項目なし。						
3.1.4	種々の名称形式を解釈するための規則 名称を解釈するための規則は、本CP「7　証明書及び失効リスト及びOCSPのプロファイル」に従う。	CPの証明書プロファイルに従った記載がされていること。	CPSまたはプロファイル仕様書等を閲覧し、名前を解釈する規則が決められたプロファイルになっていることを確認する。					
3.1.5	名称の種類一意性 認証局が発行する電子証明書の加入者名（subjectDN）は、認証局内で一意にするためにシリアル番号（SN）を含むことができる。また、認証局の名称（issuerDN）は、保健医療福祉分野PKI内で、ある特定の認証局を一意に指し示すものである。	(1)証明書内で加入者名が一意に特定されていること。 (2)認証局の名前が、ある特定の認証局を一意に指し示すようにされていること。この際、CommonName は、「HPKI-01-*-forNonRepudiation」とし、* にはHPKI専門家会議により一意とされた文字列を使用すること。	CPSまたはプロファイル仕様書等を閲覧し、加入者名がその認証局として一意に特定されることおよび認証局のCommonNameが規定のフォーマットであり、且つHPKI専門家会議により一意とされたものであることを確認する。					
3.1.6	認識、認証及び商標の役割 規定しない。	CPとして監査目標項目なし。						
3.2	初回の本人性確認							
3.2.1	私有鍵の所持を証明する方法 申請者が生成した鍵ペアの公開鍵を提示して認証局に対し証明書発行要求を行う際、公開鍵証明書と私有鍵との対応を証明するために、認証局からのチャレンジに署名を行い、私有鍵の所有を証明するものとする。あるいは申請者が提出した証明書発行要求（CSR）の署名検証等により、私有鍵の所有を確認するものとする。 認証局側で申請者の鍵ペアを生成する場合はこの限りではない。	申請者が生成した鍵ペアの公開鍵を提示して、証明書発行要求を行う際は、以下のいずれかの要件を満たすこと。 ・認証局からのチャレンジに署名を行い、申請者の私有鍵の所有を証明できること ・証明書発行要求（CSR）の署名検証等により、申請者の私有鍵の所有を証明できること	CPSまたは事務取扱要領を閲覧し、チャレンジに署名またはCSRの署名検証等により、加入者が公開鍵と対応する私有鍵を所持していることを証明するようにしていることを確認する。					

準拠性監査報告書様式（署名用）

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
3.2.2	組織の認証 保健医療福祉分野認証局に医療機関等の管理者の証明書を申請しようとする者は、証明書の交付に先立ち、次のいずれかの方法で自身の所属若しくは運営する組織の実在性を登録局に立証しなくてはならない。 なお、申請者個人の認証は「3.2.3　個人の認証」に定める方法による。 以下省略	申請者からCPで指定した、登記事項証明書、保険医療機関等の開設時に提出した開設届の副本のコピー、保険医療機関等の指定を受けた際に地方厚生局より発行された指定通知書のコピーなど公的機関から発行若しくは受領した証明書、各法等で定められる掲示（医療法第14条2　院内掲示義務等）の書類の提出を求めていること。 組織が公的機関の場合には、認証局が定める書類に公印規則に定められた公印を捺印したもの、もしくは法人組織の場合と同様の書類を提出することを求めていること。 前述の組織の運営区分に係わらず、保健医療福祉分野PKI認証局が発行する管理者向け電子証明書を用いた電子署名もしくは商業登記認証局の発行する電子証明書により実在性を立証できるとされていること。 商業登記認証局の発行する電子証明書を用いる場合は、別途、指定通知書のコピー、診療報酬の支払後、審査支払機関から発行される直近3カ月以内の支払通知書のコピーなど保険医療機関等であることを証明する書類の提出を認証局が定める方法により提出を求めていること。	1)CPSまたは事務取扱要領を閲覧しCPで定められた組織の立証方法が定めれていることを確認する。 2)作業記録等を閲覧し規定どおりに組織の立証作業が実施されていることを確認する。					
3.2.3	個人の認証 保健医療福祉分野認証局に証明書を申請しようとする個人は、証明書の交付に先立ち、CPSの定めに従って、次のいずれかの方法で自身の実在性、本人性及び申請意思を登録局に立証しなくてはならない。また、国家資格を有する者が国家資格を含んだ証明書、医療機関等の管理者が医療機関等の管理者の証明書を申請しようとする場合は、国家資格保有の事実、管理者であることの事実を登録局に立証しなくてはならない。立証に用いる書類については、有効期間外のものや、資格喪失後のものを用いてはならない。 なお、本節の定めは証明書申請者の立証に関わる定めであり、登録局が証明書を交付する場合は、本節の規定に従い申請者の立証を行わせ、4章の規定に則り申請者の審査及び証明書の交付を実施する。 ＜持参もしくは交付時に本人が出頭する場合＞ 　詳細省略 ＜郵送の場合＞ 　詳細省略 ＜オンラインの場合＞ 　詳細省略	＜持参もしくは交付時に本人が出頭する場合＞ (1)住民票の写し及び最低限「氏名、生年月日、性別、住所」を記載した認証局で定める申請書類の提示を求め、実在性を立証させていること。 (2)CPに従って、認証局のCPSで定めた書類の原本の提示を求め、本人性を立証させていること。 (3)対面で実在性及び本人性の立証書類を確認することで、申請意思を確認していること。なお、代理人による申請の場合は、申請者本人の印鑑登録証明書及び認証局で定める委任状に実印を捺印した書類の提示求め、申請意思を立証させていること。 (4)国家資格情報を含んだ証明書を申請している場合は、官公庁の発行した国家資格を証明する書類の原本の提示、もしくは国家資格免許証等のコピーの適当な空欄に実印を捺印して印鑑登録証明書を添えて提出することを求め、国家資格所有の事実を立証させていること。 (5)医療機関等の管理者の証明書を申請している場合は、「3.2.2　組織の認証」で定める書類もしくは公に告知されたパンフレット等の提示を求め、管理者であることの事実を立証させていること。	1)CPSまたは事務取扱要領を閲覧しCPで定められた個人の立証方法が定めれていることを確認する。 2)作業記録等を閲覧し規定どおりに個人の立証作業が実施されていることを確認する。					

準拠性監査報告書様式（署名用）

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
		＜郵送の場合＞ (1)住民票の写し及び最低限「氏名、生年月日、性別、住所」を記載した認証局で定める申請書類の郵送を求め、実在性を立証させていること。 (2)CPに従って、認証局のCPSで定めた書類のコピーの郵送を求め、本人性を立証させていること。 (3)申請者の印鑑証明書を添えて、認証局の定める申請書類に実印を捺印したものの郵送を求め、申請意思を立証させていること。 (4)当該申請が代理人からの申請でないことを確認すること。 (5)国家資格情報を含んだ証明書を申請している場合は、顔写真が貼付された官公庁の発行した国家資格を証明する書類のコピーの郵送を求め、国家資格所有の事実を立証させていること。なお、国家資格を証明する書類に顔写真が貼付されていない場合は、当該書類の適当な位置に実印を捺印させて、印鑑登録証明書と共に郵送を求めること。					
		＜オンラインの場合＞ ・認証局の定める手続きに従い、公的個人認証サービスによる申請者個人の電子署名もしくはそれに準じた電子署名の提出を求め、本人性、実在性を立証させ、申請意思の確認をしていること。 ・認証局の定める手続きとは、Web画面を通じた電子的な申請、電子的な申請書類のダウンロード等による取得の後、当該書類に電子署名を付して提出を求めるなどが該当し、認証局のCPSおよび事務取扱要領に当該手続きの詳細を定めていること。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
3.2.4	確認しない加入者の情報 認めない。	CPで指定した提出すべき書類及びその記載事項に漏れがないことを確認していること。	1)CPSまたは事務取扱要領を閲覧しCPで指定した提出すべき書類及びその記載事項に漏れがないことを確認することが定めれていることを確認する。 2)作業記録等を閲覧し規定どおりに確認作業が実施されていることを確認する。					
3.2.5	機関の正当性確認 規定しない。	CPとして監査目標項目なし。						
3.2.6	相互運用の基準 規定しない。	CPとして監査目標項目なし。						
3.3	鍵更新申請時の本人性確認及び認証							
3.3.1	通常の鍵更新時の本人性確認及び認証 加入者情報の通常の鍵更新は、電子証明書が生成された日から5年以内であれば、「3.2.3　個人の認証」で提出した書類又は認証局で作成された記録を再び参照するか、加入者の署名を提示することで行える。 5年を過ぎていた場合、若しくは元の書類若しくは記録が無効になっているか廃棄されていた場合は、初回の証明書発行と同様の手順により申請するものとする。	(1)鍵更新時は、更新申請者の加入者情報を確認すること。 (2)更新申請者が、電子証明書が生成された日から5年以内に更新申請をしてきた場合に限り、以下のいずれかの方法で鍵更新をしてもよい。 ・認証局で保管してある書類を再び参照する 加入者の署名を検証する (3)更新申請者が、電子証明書が生成された日から5年を経過して更新申請をしてきた場合は、新規の申請と同様の確認手続きを実施すること。	1)CPSまたは事務取扱要領を閲覧しCPで定められた本人の確認あるいは検証方式が定められていることを確認する。 2)作業記録等を閲覧し規定どおりに確認作業が実施されていることを確認する。					
3.3.2	証明書失効後の鍵更新の本人性確認及び認証 初回の証明書発行と同様の手順により申請するものとする。	「3.2.2　組織の認証」、「3.2.3　個人の認証」と同様の手続きが取られていること。	1)CPSまたは事務取扱要領を閲覧し「3.2.2　組織の認証」、「3.2.3　個人の認証」と同様の手続きが定められていることを確認する。 2)作業記録等を閲覧し規定どおりに確認作業が実施されていることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
3.4	失効申請時の本人性確認及び認証							
	加入者が認証局に失効申請を行うときには、次の手順に従うものとする。 1. 失効を申請する証明書を特定する。 2. 証明書を失効する理由を明らかにする。 3. 申請書に認証局が検証可能な電子署名を付して認証局に送信する。電子署名付きの申請ができない場合は、他の手段を用い加入者本人であることを立証する。	(1)CPに定める手続き(1. 失効を申請する証明書を特定する。2. 証明書を失効する理由を明らかにする。3. 申請書に私有鍵で署名して認証局に送信する。)をCPS及び事務取扱要領等で明確に規定していること。 (2)加入者が電子署名付きの要求をできない場合の手続きを、CPS及び事務取扱要領等で明確に規定していること。	(1)に対しては 1)CPSまたは事務取扱要領を閲覧しCPSで定める手続きが定められていることを確認する。 2)作業記録等を閲覧し規定どおりに失効作業が実施されていることを確認する。 (2)に対しては 1)CPSまたは事務取扱要領を閲覧し加入者が電子署名付きの要求をできない場合の何らかの手続が定められていることを確認する。 2)作業記録等を閲覧し規定どおりに失効作業が実施されていることを確認する。					
4	証明書のライフサイクルに対する運用上の要件							
4.1	証明書申請							
4.1.1	証明書の申請者 1. 自然人証明書 詳細省略 2. 国家資格保有者証明書 詳細省略 3. 医療機関等の管理者の証明書 詳細省略 本CPに則り発行される証明書は、それ以外からの申請は受け付けない。	認証局において、CPで該当する申請者を定義し、それ以外は受け付けないことを、CPS及び事務取扱要領等で明確に規定していること。	CPSまたは事務取扱要領を閲覧し、CPで該当する申請者を定義し、それ以外は受け付けないことが定められていることを確認する。					
4.1.2	申請手続き及び責任 証明書の利用を希望する者は、認証局で定める以下のいずれかの手続きによって証明書の利用申請を行う。 1. 持参もしくは交付時に本人が出頭する場合　詳細省略 2. 郵送　詳細省略 3. オンライン　詳細省略 また、証明書の利用申請者は、申請にあたり、本CP「1.3 PKIの関係者」と第9章で規定される認証局の責任範囲を理解し、同意した上で利用申請を行うものとする。更に、本CPに則り運営される、各認証局の定める開示文書及び利用約款等も利用申請の前に読み、内容を理解し、それらに同意した上で利用申請を行うものとする。	(1)CPに基づいた認証局のCPSで必要な申請書類を規定し、それらを受領していること。 (2)利用申請者に、CP、CPS、各認証局で定める開示文章、利用約款等を示し、内容を理解させ、同意を得る手続きを事務取扱要領で定めていること。	(1)に対しては 1)CPSまたは事務取扱要領を閲覧しCPSで定める必要な申請書類が定められていることを確認する。 2)作業記録等を閲覧し規定どおりに受領作業が実施されていることを確認する。 (2)に対しては 1)CPSまたは事務取扱要領を閲覧し利用申請者に同意を取る手続が定めれていることを確認する。 2)作業記録等を閲覧し規定どおりに同意を得ていることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
4.2	証明書申請手続き							
4.2.1	本人性及び資格確認 本人性及び資格の確認については、それぞれ以下の方法により実施する。なお、オンラインによる場合は、全ての確認手順に亘り電子的手法により実施され、認証局が公的個人認証サービス若しくはそれに準じたサービスを利用することを想定したものである。したがって、全ての手順が電子的手法で実施できない場合は、他の方法との組み合わせにより、確実な本人性、実在性、申請意思及び資格確認を実施しなくてはならない。 ＜本人からの申請の場合＞ 詳細省略 ＜代理人申請の場合＞ 詳細省略 ＜登録局の業務の一部を委託して交付する場合＞ 登録局は、「1.3.2 登録局」で定める条件の下、業務の一部を外部に委託することができるが、そのうち医療関係団体等に、当該団体に加盟・所属する組織への証明書を交付する際の業務を委託することが考えられる。 この場合、本CP若しくは認証局で定めるCPSに則った組織の実在性及び保険医療機関等の確認を当該団体の管理者の責任のもと実施しなくてはならない。 また、認証局と当該団体の間で委託に係わる契約等を取り交わし、委託された業務に関して登録局に課せられると同等の業務内容、責任及び義務を負うことを定めておかなくてはならない。	(1)「3.2.2　組織の認証」、「3.2.3　個人の認証」で利用申請者から提示もしくは郵送された各種の書類について、記載事項、印影、貼付写真等の真偽を確認していること。 (2)上記の確認手続き及び確認方法について、事務取扱要領で定めていること。 (3)オンライン申請の場合、利用申請者から提示された各種の電子的書類について、その真偽の確認方法をCPS及び事務取扱要領で定めていること。 (4)オンライン申請の場合、全ての手続きが電子的手法により実施されない場合の補足的手続きに関して、事務取扱要領で定めていること。 (5)業務の一部を委託している場合、委託元と委託先で契約等の行為が行われていること。また、契約等の内容に従って、事務取扱要領、個人情報の取り扱い等に関わる規定が定められていること。更に、その業務が適切に実施されていることを委託元が定期的に確認していること。	1)CPSまたは事務取扱要領を閲覧し、CPで定める方法が定められていることを確認する。 2)作業記録等を閲覧し規定どおりに確認作業が実施されていることを確認する。 3)業務の一部を委託している場合、委託元と委託先で契約等が行われていること、遵守すべき規定が整備されていること、その実施状況を確認していることを確認する。				
4.2.2	証明書申請の承認又は却下 認証局は、書類不備や本人性の確認等の審査過程において疑義が生じた場合には、利用申請を不受理とする。	審査過程において疑義が生じた場合の取扱を、CPSまたは事務取扱要領で定めていること。	CPSまたは事務取扱要領を閲覧し、審査過程において疑義が生じた場合の取扱を定めていることを確認する。					
4.2.3	証明書申請手続き期間 認証局では、証明書申請の手続き期間などを情報公開Webサイト等で公開する。	(1)証明書の申請手続きに係わる期間をWebサイト等の公開された媒体を通じて告知していること。 (2)申請手続きに係わる期間を、CPSまたは事務取扱要領で定めていること。また、期間の変更があった場合の手続きも同時に定めていること。	1)Webページ等の公開された媒体を閲覧し、申請手続きに係わる期間を告知していることを確認する。 2)CPSまたは事務取扱要領を閲覧し、申請手続きに係わる期間および期間の変更があった場合の手続きを定めていることを確認する。					
4.3	証明書発行							
4.3.1	証明書発行時の認証局の機能 ＜認証局が鍵ペアを生成する場合＞ 認証局が鍵ペアを生成する場合は、「電子署名及び認証業務に関する法律施行規則」第6条第三号に準じてCPS及び事務取扱要領を規定し、運用する。 CPS及び事務取扱要領の規定としては、最低限以下の項目を含めるものとする。 以下省略 ＜加入者が鍵ペアを生成する場合＞ 詳細省略	CPの規定に従った鍵ペアの生成規定を定め運営していることなお、「電子署名及び認証業務に関する法律施行規則」第6条第三号および第三号ニは以下である。 三　利用者が電子署名を行うために用いる符号（以下「利用者署名符号」という。）を認証事業者が作成する場合においては、当該利用者署名符号を安全かつ確実に利用者に渡すことができる方法により交付し、又は送付し、かつ、当該利用者署名符号及びその複製を直ちに消去すること。	1)CPSまたは事務取扱要領を閲覧し、CPで定める鍵ペア生成方法が定められていることを確認する。 2)作業記録等の閲覧または鍵ペア生成作業を観察し、規定どおりに鍵ペア生成が実施されていることを確認する。					
		三の二　利用者署名符号を利用者が作成する場合において、当該利用者署名符号に対応する利用者署名検証符号を認証事業者が電気通信回線を通じて受信する方法によるときは、あらかじめ、利用者識別符号（認証事業者において、一回に限り利用者の識別に用いる符号であって、容易に推測されないように作成されたものをいう。）を安全かつ確実に当該利用者に渡すことができる方法により交付し、又は送付し、かつ、当該利用者の識別に用いるまでの間、当該利用者以外の者が知り得ないようにすること。						

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
4.3.2	証明書発行後の通知 認証局は、電子証明書を交付することにより電子証明書を発行したことを通知したものとみなす。	CPS、開示文書、利用約款等に、「電子証明書を交付することにより電子証明書を発行したことを通知したものとみなす。」ことを記載し利用申請者に通知すること。	CPS、開示文書、利用約款等を閲覧し、「電子証明書を交付することにより電子証明書を発行したことを通知したものとみなす。」ことを記載し利用申請者に通知していることを確認すること。					
4.4	証明書の受理							
4.4.1	証明書の受理 認証局は、電子証明書を交付した後、受領した旨を確認しなければならない。 また、証明書を交付してから一定の期間内に受領が確認できない場合、証明書を失効させなければならない。これらの方法や期間はCPSで定めるものとする。	(1)利用申請者が証明書を受理したことを確認する方法について確立し、CPSまたは事務取扱要領で定めていること。 (2)受理が確認できない場合について、その期間及び失効に係わる手続きをCPSまたは事務取扱要領で定めていること。	CPSまたは事務取扱要領を閲覧し、利用申請者が証明書を受理したことを確認する方法、および受理が確認できない場合について、その期間及び失効に係わる手続きを定めていることを確認する。					
4.4.2	認証局による証明書の公開 認証局は、加入者の署名用証明書の公開を行わない。	署名用証明書の公開を行っていないこと。	CPSまたは事務取扱要領を閲覧し、署名用証明書の公開を行っていないことを確認する。					
4.4.3	他のエンティティに対する認証局による証明書発行通知 規定しない。	CPとして監査目標項目なし。						

準拠性監査報告書様式（署名用）

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
4.5	鍵ペアと証明書の利用目的							
4.5.1	加入者の私有鍵と証明書の利用目的 加入者は、私有鍵を電子署名にのみ利用する。	認証局は、加入者に対して、私有鍵は電子署名のみに利用するよう告知していること。	CPS、利用約款またはWeb等の公開された媒体を閲覧し、加入者に対して、私有鍵は電子署名のみに利用するよう告知していることを確認する。					
4.5.2	検証者の公開鍵と証明書の利用目的 検証者は、署名検証の用途で公開鍵と証明書を利用する。	認証局は、検証者に対して、署名検証の用途のみで公開鍵と証明書を利用するよう告知していること。	CPS、利用約款またはWeb等の公開された媒体を閲覧し、検証者に対して、署名検証の用途のみで公開鍵と証明書を利用するよう告知していることを確認する。					
4.6	証明書更新							
4.6.1	証明書更新の要件 本CPに則り認証局から発行される証明書は、鍵更新を伴う更新のみを許可する。従って、鍵の更新を伴わない証明書更新は行わない。	鍵更新を伴う更新のみを許可することをCPS及び事務取扱要領、認証局の定める各種文章及び利用約款等で規定すること。	CPS、事務取扱要領あるいは利用約款等を閲覧し、鍵更新を伴う更新のみを許可することを定めていることを確認する。					
4.6.2	証明書の更新申請者 規定しない。	CPとして監査目標項目なし。						
4.6.3	証明書更新の処理手順 規定しない。	CPとして監査目標項目なし。						
4.6.4	加入者へ新証明書発行通知 規定しない。	CPとして監査目標項目なし。						
4.6.5	更新された証明書の受理 規定しない。	CPとして監査目標項目なし。						
4.6.6	認証局による更新証明書の公開 規定しない。	CPとして監査目標項目なし。						
4.6.7	他のエンティティへの証明書発行通知 規定しない。	CPとして監査目標項目なし。						

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
4.7	証明書の鍵更新（鍵更新を伴う証明書更新）							
4.7.1	証明書鍵更新の要件 認証局は、以下の条件を満たす時に証明書の更新申請を受け付ける。 ・ 更新対象証明書が存在すること。 ・ 証明書が有効期限終了前のものであること。 ・ 証明書が失効されていないこと。 ・ 有効期限終了前で、認証局で定める期間に申請があったこと。 これらの要件を満たせば、申請者は更新申請書に署名してオンラインで証明書の更新が申請できる。	以下の要件を満たすか確認を実施していること。また、その手続きについてCPSまたは事務取扱要領で定めていること。 ・更新対象証明書が存在すること ・証明書が有効期限終了前のものであること ・証明書が失効されていないこと ・有効期限終了前で、認証局で定める期間に申請があったこと	1)CPSまたは事務取扱要領を閲覧し、CPで定めた要件をさだめていること確認する。 2)作業記録等を閲覧し、CPで定められた要件を満たすか確認を実施していることを確認する。					
4.7.2	鍵更新申請者 認証局は、加入者本人若しくはその代理人を鍵更新申請者として受け付ける。	(1)更新申請者が加入者本人もしくはその代理人であることを確認すること。 (2)確認方法について、CPSまたは事務取扱要領で定めていること。	1)CPSまたは事務取扱要領を閲覧し、更新申請者が加入者本人もしくはその代理人であることを確認する方法を定めていること確認する。 2)作業記録等を閲覧し、定められた方法で確認を実施していることを確認する。					
4.7.3	鍵更新申請の処理手順 「4.2.1 本人性及び資格確認」に定める本人性確認並びに資格確認を行うものとする。 但し、登録局で電子証明書が生成された日から5年以内の場合は、上記に代わり加入者証明書による本人確認を行うことができる。	(1)「4.2.1　本人性及び資格確認」と同様の確認を行うこと。 (2)事務取扱要領に鍵更新申請の処理手順について定めていること。 (3)加入者証明書による本人確認を実施する場合、電子証明書が生成された日から5年以内の加入者証明書であることを確認すること。また、手続きについて事務取扱要領で定めていること。	1)CPSまたは事務取扱要領を閲覧し、CPに定められた「本人性及び資格確認」方法が定められていることを確認する。 2)作業記録等を閲覧し、CPで定められた方法により「本人性及び資格確認」を行っていることを確認する。					
4.7.4	加入者への新証明書発行通知 認証局は、電子証明書を申請者に交付することにより電子証明書を発行したことを通知したものとみなす。	CPS、開示文書、利用約款等に、「電子証明書を交付することにより新電子証明書を発行したことを通知したものとみなす。」ことを記載し利用申請者に通知すること。	CPS、開示文書、利用約款等を閲覧し、「電子証明書を交付することにより新電子証明書を発行したことを通知したものとみなす。」ことを記載し利用申請者に通知していることを確認すること。					
4.7.5	鍵更新された証明書の受理 認証局は、電子証明書を交付した後、受領した旨を確認しなければならない。 また、証明書を交付してから一定の期間内に受領が確認できない場合、証明書を失効させなければならない。これらの方法や期間はCPSで定めるものとする。	(1)利用申請者が証明書を受理したことを確認する方法について確立し、CPSまたは事務取扱要領で定めていること。 (2)受理が確認できない場合について、その期間及び失効に係わる手続きをCPSまたは事務取扱要領で定めていること。	CPSまたは事務取扱要領を閲覧し、利用申請者が証明書を受理したことを確認する方法、および受理が確認できない場合について、その期間及び失効に係わる手続きを定めていることを確認する。					
4.7.6	認証局による鍵更新証明書の公開 認証局は署名用証明書の公開を行わない。	署名用証明書の公開を行っていないこと。	CPSまたは事務取扱要領を閲覧し、署名用証明書の公開を行っていないことを確認する。					
4.7.8	他のエンティティへの証明書発行通知 規定しない。	CPとして監査目標項目なし。						
4.8	証明書変更							
4.8.1	証明書変更の要件 本CPに則り認証局から発行される証明書は、証明書変更を行わない。	(1)証明書変更を行わないこと。その旨をCPS、事務取扱要領で規定していること。 (2)証明書変更を行わないことをWeb等で告知していること。	1)Webページ等の公開された媒体を閲覧し、証明書変更を行わないことを告知していることを確認する。 2)CPSまたは事務取扱要領を閲覧し、証明書変更を行わないことを定めていることを確認する。					
4.8.2	証明書の変更申請者 規定しない。	CPとして監査目標項目なし。						
4.8.3	証明書変更の処理手順 規定しない。	CPとして監査目標項目なし。						
4.8.4	加入者への新証明書発行通知 規定しない。	CPとして監査目標項目なし。						

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
4.8.5	変更された証明書の受理 規定しない。	CPとして監査目標項目なし。						
4.8.6	認証局による変更証明書の公開 規定しない。	CPとして監査目標項目なし。						
4.8.7	他のエンティティへの証明書発行通知 規定しない。	CPとして監査目標項目なし。						
4.9	証明書の失効と一時停止							
4.9.1	証明書失効の要件 認証局は、次の場合に証明書を失効するものとする。 以下省略	CPに基づいた失効に係わる要件をCPSに定めていること。	CPSを閲覧し、CPに基づいた失効に係わる要件を定めていることを確認する。					
4.9.2	失効申請者 認証局は、次の1人又はそれ以上の者からの失効申請を受け付ける。 1. 本人の名前で証明書が発行された加入者若しくはその代理人 2. 認証局の職員	以下の者からの失効申請を受付けることをCPS及び事務取扱要領で定めていること。 1. 本人の名前で証明書が発行された加入者もしくはその代理人 2. 認証局の職員						
4.9.3	失効申請の処理手順 認証局は、失効申請の受領の判断を行い受理する場合は「3.4 失効申請時の本人性確認及び認証」に従って、以下の手順を実施した上で証明書の失効を行う。 ＜本人からの失効申請の場合＞ 詳細省略 ＜代理人からの失効申請の場合＞ 詳細省略 ＜認証局の職員からの失効申請の場合＞ 詳細省略	＜本人もしくは代理人からの失効申請の場合＞ (1)失効を要求（電子証明書の返却を含む）している申請者の真偽の確認方法を事務取扱要領で定めていること。 (2)事務取扱要領において、確認書類を特定し、その確認方法についても定めていること。 (3)代理人からの失効申請の場合は、当該代理人が正当な失効権限を持っていることの真偽を確認する方法を事務取扱要領で定めていること。 (4)証明書を失効した場合のCRLの発行手続きを事務取扱要領で定めていること。 (5)証明書の失効の事実を申請者に通知する方法をCPS、事務取扱要領で定めていること。 ＜認証局の職員からの失効申請の場合＞ (1)職員からの失効申請があった場合、失効事由の真偽の確認方法について、事務取扱要領で定めていること。 (2)失効する場合の手続きを事務取扱要領で定めていること。 (3)証明書を失効した場合のCRLの発行手続きを事務取扱要領で定めていること。 (4)証明書の失効の事実を申請者に通知する方法をCPS、事務取扱要領で定めていること。	CPSまたは事務取扱要領を閲覧し、CPに定められた失効申請の処理手順を定め、実施していることを確認する。					
4.9.4	失効における猶予期間 「4.9.1 証明書失効の要件」に規定されている事由が発生した場合には、速やかに失効申請を行わなければならない。その期限はCPSに定めるものとする。	失効に係わる期間をCPSに定めていること。	CPSを閲覧し、失効に係わる期間を定めていることを確認する。					
4.9.5	認証局による失効申請の処理期間 証明書の失効要求の結果として取られる処置は、受領後直ちに開始されるものとする。その期限はCPSに定めるものとする。	(1)失効要求があった場合の処置に係わる期間についてCPSで定めていること。 (2)失効要求を受領した後の手続きについて、事務取扱要領で定めていること。	CPSまたは事務取扱要領を閲覧し、失効要求があった場合の処置に係わる期間、および失効要求を受領した後の手続きについて定めていることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
4.9.6	検証者の失効情報確認の要件 検証者は、署名者の公開鍵を使う時に有効なCRL/ARLを使用して失効の有無をチェックし、証明書状態の確認を行うものとする。	1)検証者が署名者の公開鍵を使う時に有効なCRL/ARLを提供していること。 2)検証者利用約款等に「検証者は、署名者の公開鍵を使う時に有効なCRL/ARLを使用して失効の有無をチェックし、証明書状態の確認を行うものとする。」旨を記載し、Web等の公開媒体に公開し、検証者が閲覧しやすい手段をとること。	1)CRL/ARLを検査またはシステム仕様書を閲覧し、検証者が署名者の公開鍵を使う時に有効なCRL/ARLを提供していることを確認する。 2)検証者利用約款等およびWeb等の公開媒体を閲覧し、「検証者は、署名者の公開鍵を使う時に有効なCRL/ARLを使用して失効の有無をチェックし、証明書状態の確認を行うものとする。」旨を記載し、検証者が閲覧しやすい手段をとっていることを確認する。					
4.9.7	CRL発行頻度 変更がない場合においても、48時間以内に96時間以内の有効期限のCRLを発行する。この具体的な頻度と有効期限はCPSで規定するものとする。 失効の通知は直ちに公開する。CRLに変更があった場合はいつでも更新する。また、認証局私有鍵（以下、CA私有鍵という）、加入者の私有鍵の危殆化等が発生した場合は、CRLを直ちに発行するものとする。	1)CRLの更新頻度及び有効期間をCPSで定めていること。 2)失効の通知は直ちに公開すること。またCRLに変更があった場合はいつでも更新すること。 3)CA私有鍵または加入者の私有鍵の危殆化等が発生した場合は、CRLを直ちに発行させること。	CPSを閲覧し、CRLの不定期な更新時期および定期的な更新頻度及び有効期間をCPSで定めていること。					
4.9.8	CRLが公開されない最大期間 CRLは発行後24時間以内に公開される。	CRLは24時間以内に公開されていること。	CRLを検査またはシステム仕様書を閲覧し、CRLの発行後24時間以内に公開されていることを確認する。					
4.9.9	オンラインでの失効／ステータス情報の入手方法 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されているか確認する。					
4.9.10	オンラインでの失効確認要件 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されているか確認する。					
4.9.11	その他利用可能な失効情報確認手段 使用しない。	CPで定めるもの以外の失効情報確認手段がないこと。	CPSを閲覧し、CPで定めるもの以外の失効情報確認手段がないことを確認する。					
4.9.12	鍵の危殆化に関する特別な要件 認証局は、CA署名鍵の危殆化の際には関連組織に直ちに通知するものとする。	CA署名鍵が危殆化した場合の手続きについて、CPSまたは事務取扱要領で定めていること。	CPSまたは事務取扱要領を閲覧し、CA署名鍵が危殆化した場合の手続きについて定めていることを確認する。					
4.9.13	証明書一時停止の要件 一時停止は行わない。	一時停止を行っていないこと。	CPSまたは事務取扱要領を閲覧し一時停止を行っていないことを確認する。					
4.9.14	一時停止申請者 一時停止は行わない。	一時停止を行っていないこと。	CPSまたは事務取扱要領を閲覧し一時停止を行っていないことを確認する。					
4.9.15	一時停止申請者の処理手順 一時停止は行わない。	一時停止を行っていないこと。	CPSまたは事務取扱要領を閲覧し一時停止を行っていないことを確認する。					
4.9.16	一時停止期間の制限 一時停止は行わない。	一時停止を行っていないこと。	CPSまたは事務取扱要領を閲覧し一時停止を行っていないことを確認する。					
4.10	証明書ステータスの確認サービス							
4.10.1	運用上の特徴 規定しない。	CPとして監査目標項目なし。						
4.10.2	サービスの利用可能性 規定しない。	CPとして監査目標項目なし。						
4.10.3	オプショナルな仕様 規定しない。	CPとして監査目標項目なし。						
4.11	加入の終了							
	加入者が、証明書の利用を終了する場合、本CP「4.9 証明書の失効と一時停止」に規定する失効手続きを行うものとする。	加入の終了手続きについて、CPSまたは事務取扱要領で定めていること。	CPSまたは事務取扱要領を閲覧し、加入の終了手続きについて定めていることを確認する。					

準拠性監査報告書様式（署名用）

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
4.12	私有鍵預託と鍵回復							
	署名のために使用される私有鍵は、法律によって必要とされる場合を除き、預託されないものとする。また、署名目的の私有鍵の回復も行わない。	(1)私有鍵の預託をしていないこと。 (2)法の要請により預託が必要な場合、その法を特定し、事務取扱要領で預託方法について定めていること。 (3)署名目的の私有鍵の回復を行わないこと。	CPSまたは事務取扱要領を閲覧し、私有鍵の預託をしていないこと、法の要請により預託が必要な場合は、その法を特定し、預託方法について定めていることまた、署名目的の私有鍵の回復を行わないことを定めていることを確認する。					
4.12.1	預託と鍵回復ポリシ及び実施 規定しない。	CPとして監査目標項目なし。						
4.12.2	セッションキーのカプセル化と鍵回復のポリシ及び実施 規定しない。	CPとして監査目標項目なし。						
5	建物・関連設備、運用のセキュリティ管理							
5.1	建物及び物理的管理							
5.1.1	施設の位置と建物構造 認証局を運用する施設は、隔壁により区画されていて、施錠できることとする。 認証局システム（以下、CAシステム）を設置する施設は、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、かつ建物構造上、これら災害防止のための対策を講ずる。また、施設内において使用する機器等を、災害及び不正侵入防止策の施された安全な場所に設置すること。	(1)認証局を運用する施設は、隔壁により区画されていて、施錠できること。 (2)認証設備室が設置されている建築物は、地震による被害の恐れの少ない地域に設置されていること。やむを得ない場合は、建築基準法に定める地震強度以上の、十分な耐震強度を有する基礎構造としていること。 (3)認証設備室が設置されている建築物は、水害、火災その他の災害の被害を容易に受けない場所に設置されていること。 (4)認証設備室が設置されている建築物について、停電、地震、火災及び水害その他の災害への対策に関して、事務取扱要領等に明確かつ適切に規定し、必要な措置を講じていること。 例えば (a)認証設備室が設置されている建築物は、建築基準法に規定する構造耐力等の基準に適合していること。 (b)認証設備室が設置されている建築物は、建築基準法に規定する耐火建築物又は準耐火建築物の基準に適合していること。 (5)施設内において使用する機器等を、災害及び不正侵入防止策の施された安全な場所に設置すること。	(1)事務取扱要領書、施設配置図等を閲覧し、認証局を運用する施設は、隔壁により区画されていて、施錠できることを確認する。 (2)(3)事務取扱要領、建築確認通知書、検査済証、地盤調査書等を閲覧し、CAシステムを設置する施設は、災害の被害を容易に受けない場所に設置されていることを確認する。 (4)事務取扱要領、建築確認通知書、検査済証等を閲覧し、CAシステムを設置する施設は、建物構造上、これら災害防止のための対策を講じられていることを確認する。 (5)事務取扱要領書、施設配置図、機器配置図あるいは現地を観察しまたは検査し、施設内において使用する機器等が、災害及び不正侵入防止策の施された安全な場所に設置されていれことを確認する。					
5.1.2	物理的アクセス 認証局を運用する施設は認証業務用設備の所在を示す掲示がされていないこと。また物理的なアクセスを制限する適切なセキュリティ管理設備を装備し、入退出管理を実施すること。入退出者の本人確認はCPSで定める方法により確実に行い、かつ入退出の記録を残すこととする。 認証設備室への立入は、立入に係る権限を有する複数の者により行われることとし、入室者の数と同数の者の退室を管理すること。設備の保守あるいはその他の業務の運営上必要な事情により、やむを得ず、立入に係る権限を有しない者を認証設備室へ立入らせることが必要である場合においては、立入に係る権限を有する複数の者が同行することとする。 登録設備室においては、関係者以外が容易に立入ることが出来ないようにするための施錠等の措置が講じられていること。	Ⅰ．認証業務用設備 (1)認証業務用設備を収容する建築物の外部・エントランス・エレベータ・入口・受付・その他パンフレットなどの広報媒体に、当該施設の所在を明示的又は暗示する名称が看板もしくは表示板等によって掲示されていないこと。 (2)物理的なアクセスを制限する適切なセキュリティ管理設備を装備し、入退出管理を実施すること。 (3)入退出者の本人確認はCPSで定める方法により確実に行い、かつ入退出の記録を残すこととする。	(1)容易に入手できる資料を閲覧あるいは現地を観察し、認証業務用設備の所在を示す掲示がされていないことを確認する。 (2)CPS,事務取扱要領書を閲覧および現地を観察、および検査し、物理的なアクセスを制限する適切なセキュリティ管理設備を装備し、入退出管理を実施していることを確認する。 (3)CPS,事務取扱要領書および入退出記録を閲覧および現地を観察、および検査し、本人確認はCPSで定める方法により確実に行い、かつ入退出の記録を残していることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
		Ⅱ．認証設備室（※室以外にもラック等の躯体も含む） (1)認証設備室への立入は、立入に係わる権限を有する複数の者により行われ、入室者の数と同数の退室を管理していること。 (2)設備保守等のやむを得ない事情により、入室権限者以外が立ち入る場合は、立入権限を有する複数の者が同行するようにしていること。	(1)CPS、事務取扱要領、認証設備室の入退室記録を閲覧および現地を観察、および検査し、認証設備室への立入は、立入に係わる権限を有する複数の者により行われ、入室者の数と同数の退室を管理していることを確認する。 (2)CPS、事務取扱要領、認証設備室の入退室記録を閲覧および現地を観察、および検査し、設備保守等のやむを得ない事情により、入室権限者以外が立ち入る場合は、立入権限を有する複数の者が同行するようにしていることを確認する。					
		Ⅲ．登録設備室 (1)登録用設備室には、関係者以外が容易に立ち入ることができないように施錠等の措置が講じられていること。 (2)入退室の記録を残すこと。	CPS、事務取扱要領、登録設備室の入退室記録もしくは施錠設備の鍵管理簿等を閲覧および現地を観察しおよび検査し、関係者以外が容易に立ち入ることができないように施錠等の措置が講じられ、入退室の記録が残されていることを確認する。					
5.1.3	電源及び空調設備 室内において使用される電源設備について停電に対する措置が講じられていることとする。 また、空調設備により、機器が適切に動作する措置が講じられていることとする。	Ⅰ．電源設備 室内において使用される電源設備について停電に対する措置が講じられていること。 例えば、無停電電源装置（UPS）又は定電圧定周波装置（CVCF）と蓄電池を設置していること。	UPS又はCVCFなどの機器説明書 認証設備室の電源回路図等を閲覧および必要により現地を観察し、電源設備について停電に対する措置が講じられていることを確認する。					
		Ⅱ．空調設備 空調設備により、機器が適切に動作する措置が講じられていること。 例えば次に示すような措置が講じられていること。 ①認証設備室の温湿度が、情報システムの正常稼動範囲にあること。 ②凍結防止の措置を講ずること。 ③水漏れ防止の措置を講ずると共に、漏水の恐れがある場合は該当個所に漏水検知装置等を設置すること。 ④空調設備の配管・ダクト類は、耐火性に優れた材料を使用すること。	空調設備の取り扱い説明書等（空調設備の仕様が分かるもの） 配管・ダクト等の図面及び材質が示されたものを閲覧および現地を観察し機器が適切に動作する措置が講じられていることを確認する。					
5.1.4	水害及び地震対策 水害の防止のための措置が講じられていることとする。 また、認証業務用設備は通常想定される規模の地震による転倒及び構成部品の脱落等を防止するための構成部品の固定や、その他の耐震措置が講じられていることとする。	Ⅰ．水害対策 水害の防止のための措置が講じられていること。 例えば以下のような措置が考えられる。 (1)認証設備室は、次のいずれかを満たしていること。 ①認証設備室を建築物の2階以上に設置すること。 ②認証設備室を建築物の1階以下に設置する場合は、水害に対して十分な措置が講じられていること。 (2)直上階のコンクリート床に、空隙や割れ目がないこと。あれば、防水剤でパテを充てること。 (3)室内に防水カバーを常備するなどして業務用端末等を保護できるようにしていること。 (4)認証設備室には、流し台・給湯器等の水使用設備を設置していないこと。	防水施行図等を閲覧および現地を観察し、水害の防止のための措置が講じられていることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
		Ⅱ．地震対策 認証業務用設備は通常想定される規模の地震による転倒及び構成部品の脱落等を防止するための構成部品の固定や、その他の耐震措置が講じられていること。 例えば以下のような措置が考えられる。 (1)地震に対して、認証設備室は以下のいずれかによる移動・転倒防止策が講じられていること。 ①認証業務用設備が設置してある室のフロアレスポンスに応じて、設備メーカの推奨する設置方式を考慮した移動・転倒防止等の措置が講じられていること。 ②耐震脚、転倒防止装置金具等で建物構造体に固定されていること。 ③建築物全体、認証業務用設備が設置してある床等が耐震構造を持つ、または認証業務用設備が免震台に支持されていること。 (2)ラックが建物構造体に固定される等して移動、転倒防止措置が講じられていること。 (3)認証業務用設備の構成部品は、落下防止金具や耐震バンド等で固定されていること。 (4)フリーアクセスフロアは地震で損壊しないよう、アングルやストリンガー等の補強措置が講じられていること。 (5)地震の際に認証業務用設備に被害を与えないように、認証設備室の什器・備品等に耐震措置が講じられていること。	免震構造の効力を証明する書類、設備メーカの推奨する設置方式等が示された書類等を閲覧し、また現地を観察し耐震措置が講じられていることを確認する。					
5.1.5	防火設備 自動火災報知器及び消火装置が設置されていることとする。また、防火区画内に設置されていることとする。	(1)認証設備室には、消防法施行令に規定された自動火災報知機及び消火装置を設置し、消防署等の検査を受け、定期点検を実施していること。 (2)認証設備室を含む区画は、建築基準法に規定する防火区画であること。	消防用設備等検査済証、定期点検検査報告書、建築図面（防火区画が記されているもの）を閲覧し消化装置が設置され、防火区画内に設置されていることを確認する。					
5.1.6	記録媒体 アーカイブデータ、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、認証局の定める手続きに基づき適切に搬入出管理を行う。	(1)アーカイブデータ、バックアップデータを含む記録媒体は、例えばスマートカード、生体認証、入退室管理簿等により適切な入退室管理が行われた室内の施錠可能な保管庫に保管すること。 (2)記録媒体の搬入出時には、例えば搬入出者、日時等の記録を残し管理することを事務取扱要領等に明確かつ適切に規定する等の措置を講じていること。	CPS、事務取扱要領書、入退室の記録等を閲覧および現地を観察し、記録媒体が適切な入退室管理が行われた室内の施錠可能な保管庫に保管されていること、および適切な搬入出管理が行われていることを確認する。					
5.1.7	廃棄物の処理 機密扱いとする情報を含む書類・記録媒体の廃棄については、所定の手続きに基づいて適切に廃棄処理を行う。	(1)機密扱いとする情報を含む書類・記録媒体の廃棄については、廃棄の記録、機密度に応じた廃棄方法（溶解・裁断・上書きによる消去等）に係わる手続きを事務取扱要領等に明確かつ適切に規定し、必要な措置を講じていること。 (2)第3者の廃棄業者に廃棄を委託する場合は、委託業者との契約書に機密保持、個人情報保護及び廃棄報告の事項を入れること。	事務取扱要領、委託契約書を閲覧し、適切な廃棄処理および第三者との契約がなされていることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
5.1.8	施設外のバックアップ バックアップ媒体は、認証局施設における災害が発生しても、その災害によって損傷しないように、十分に離れた所に置くことが望ましい。	(1)認証サービス等に係わるバックアップ媒体を認証設備室もしくは建築物以外に保管できる場合は、災害等による損傷を避けるため可能な限り分離して保管すること。また、災害発生時の復旧方法について事務取扱要領等で適切に規定し、必要な措置を講じていること。 (2)外部に保管する場合は、その記録媒体の管理に関して、認証設備と同等の管理を実施すること。委託業者に委託する場合は、適切な業者を選定し、契約書等で媒体の取り扱いについて厳格に規定すること。 (3)外部への保管が不可能な場合は、災害等による損傷を極力排除可能なように保管し、その保管方法及び災害発生時の復旧方法について、事務取扱要領等で適切に規定し、必要な措置を講じていること。	(1)(3)事務取扱要領書、委託契約書等を閲覧し、バックアップ媒体が災害等による損傷を避けるため可能な限り分離して保管され、認証設備と同等の管理を実施することされているか、外部への保管が不可能な場合は、災害等による損傷を極力排除可能なように保管されているか確認する。 また、事務取扱要領等を閲覧し、災害発生時の復旧方法について適切に規定し、必要な措置を講じていることを確認する。 (2)事務取扱要領書、委託契約書等を閲覧し、委託業者に委託する場合は、適切な業者を選定し、媒体の取り扱いについて厳格に規定されているか確認する。					
5.2	手続き的管理							
5.2.1	信頼すべき役割 証明書の登録、発行、取消等の業務及び関連する業務に携わる者には、CAシステムの設定やCA私有鍵の活性化等を担当する「CAシステム管理者」、加入者証明書の発行・失効を担当する「登録局管理者」、及び「監査者」などがあり、本CP上信頼される役割を担っている。認証局においては、業務上の役割を特定の個人に集中させず、前述のように複数の役割に権限を分離した上、個人が複数の役割を兼任することは避けること。	認証業務に従事する者の責任及び権限、指揮命令系統に関して、特定の個人に業務が集中しないよう内部牽制を考慮した上で事務取扱要領等に明確かつ適切に規定し、実施していること。 少なくとも「CAシステム管理者」、「登録局管理者」、及び「監査者」は兼任しないこと。	事務取扱要領、指揮命令系統の示された組織体制図を閲覧し、特定の個人に権限が集中していないことを確認する。					
5.2.2	職務ごとに必要とされる人数 CAシステムへの物理的又は論理的に単独でのアクセスを避けることができるような必要人数を定めること。	CAシステムへの物理的又は論理的に単独でのアクセスを避けることができるような必要人数を定めること。 例えば、 CAシステムの私有鍵の生成、管理者・利用者の私有鍵の生成（生成を行う場合）、CAの私有鍵の活性化、CAの機能に関連するソフトウエアの更新等の操作、および高度な安全管理区域への立ち入りが単独の操作者で行えないように必要な人数を定めていること。	CPS、事務取扱要領、指揮命令系統の示された組織体制図等を閲覧し、CAシステムへの物理的又は論理的に単独でのアクセスを避けることができるような必要人数を定めることを確認する。					
5.2.3	個々の役割に対する本人性確認と認証 認証局システム、登録局システムへアクセスし、CA私有鍵の操作や証明書発行、失効に係わる操作等の重要操作を行う権限者は、認証局運営責任者により任命されること。 また、システムへの認証には当該業務へ専用に用いるICカード等のセキュリティデバイスに格納された、本人しか持ち得ない権限者の私有鍵等を用いた強固な認証方式を採用すること。	(1)認証局システム、登録局システムへアクセスし、CA私有鍵の操作や証明書発行、失効に係わる操作等の重要操作を行う権限者は認証局運営責任者により任命され、その任命方法が定められていること。 (2)システムへのアクセス時（システム機器への操作開始時またはシステム室への入退室等のアクセス時の少なくともいずれかにおいて）の本人確認には当該業務へ専用に用いるICカード等のセキュリティデバイスに格納された、本人しか持ち得ない権限者の私有鍵等を用いた強固な認証方式を定めていること。 (入退出時のみにICカードを用いる場合は操作権限者のみが入退出可能な状態に設定されていること。 また、認証設備室外での登録局システム機器の操作時の本人確認にはICカ ー ド等のセキュリティデバイスを 採用すること。）	CPS、事務取扱要領書等を閲覧し、重要な操作を行う権限者は認証局運営責任者により任命されることおよび、本人確認に当たっては操作や入退出等のどこか一箇所以上で本人しか持ち得ない権限者の私有鍵を用いた強固な認証方式を採用していることを確認する。 また、認証設備室外での登録局システム機器の操作時の本人確認にはICカ ー ド等のセキュリティデバイスを 採用していることを確認する。					
5.2.4	職務分轄が必要になる役割 CA私有鍵の操作やCAシステム管理者、登録局システム管理者の登録等の重要操作は、複数人によるコントロールを採用すること。	CA私有鍵の操作やCAシステム管理者、登録局システム管理者の登録等の重要操作は、複数人によるコントロール（例えば、知識分割・鍵分割などの技術的措置による デュアルコントロールや複数人の操作や監視などによる相互牽制）の定めがなされ運用されていること。事務取扱要領には操作後の台帳管理やアクセスログによる監査証跡のチェックを含めること。	1)指揮命令系統の示された組織体制図、CPS、事務取扱要領、運用マニュアル、キーセレモニー記録等を閲覧し、CA私有鍵の操作やCAシステム管理者、登録局システム管理者の登録等の重要操作は、複数人によるコントロールが採用されていることを確認する。 2)作業記録やログ等を閲覧し、複数人によるコントロールで運用していることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
5.3	要員管理							
5.3.1	資格、経験及び身分証明の要件 認証局の業務運営に関して信頼される役割を担う者は、認証局運営組織の採用基準に基づき採用された職員とする。CAシステムを直接操作する担当者は、専門のトレーニングを受け、PKIの概要とシステムの操作方法を理解しているものを配置する。	1)認証局の業務運営に関して信頼される役割を担う者が認証局運営組織の採用基準に基づき採用された職員であることを定めていること。 2)およびCAシステムを直接操作するものはPKIの概要とシステムの操作方法を理解していることを確認してから配置することを定めていること。	CPS、事務取扱要領、組織の採用基準を定めた内規等を閲覧、または、直接面接し質問する等して、認証局の業務運営に関して信頼される役割を担う者がそれらの基準に従って採用され配置されていることを確認する。					
5.3.2	経歴の調査手順 信頼される役割を担う者の信頼性と適格性を、認証局運営組織の規則の要求に従って、任命時及び定期的に検証すること。	信頼される役割を担う者の決定に際して、対象者の履歴、技能、適格性に関する基準を定めていること。	CPS、事務取扱要領、組織の採用基準を定めた内規等を閲覧し、対象者の履歴、技能、適格性に関する基準を定めてあることを確認する。					
5.3.3	研修要件 信頼される役割を担う者は、その業務を行うための適切な教育を定期的に受け、以降必要に応じて再教育を受けなければならない。	信頼される役割を担う者に対しての業務に必要な教育の基準を定め、また就業開始時およびその後の必要時および定期的な教育実施に関する規定を定めていること。	CPS、事務取扱要領等を閲覧し、業務に必要な教育基準および定期的な教育訓練実施に関する規定を定めていることを確認する。					
5.3.4	再研修の頻度及び要件 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されていることを確認する。					
5.3.5	職務のローテーションの頻度及び要件 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されていることを確認する。					
5.3.6	認められていない行動に対する制裁 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されていることを確認する。					
5.3.7	独立した契約者の要件 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されていることを確認する。					
5.3.8	要員へ提供する資料 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されていることを確認する。					
5.4	監査ログの取扱い							
5.4.1	記録するイベントの種類 認証局は、CAシステム、リポジトリシステム、認証局に関するネットワークアクセスの監査証跡やイベント・ログを手動或いは自動で取得できる。	認証局のイベントログを自動または手動で取得できること。例えば、以下のようなログを取得できること。 ●利用者情報の初期化、証明書および私有鍵の生成、活性化、非活性化、更新、修復、削除等に関する操作 ●CA操作者のパスワード、私有鍵および公開鍵の作成、変更、削除、更新、およびCA操作者としてのログインに関する操作 ●リポジトリを用いている場合はリポジトリへの利用者のアクセスが不成功な場合、およびCAによるリポジトリ書き込みおよび読み取り操作 ●CRL操作に関する記録、セキュリティポリシの変更や評価、CAアプリケーションの起動・終了、データベースのバックアップ、クロス証明書や証明書チェインの確認、属性証明書に関する操作、利用者の更新、DNの変更、データベースやログの操作方法の変更、証明書の取り扱いの変更 ●鍵ペアの生成、格納、検索、活性化、非活性化、保存および破壊に関する操作	1)CPS、事務取扱要領を閲覧し、例示したような取得すべきログを規定してあることを確認する。 2)また、関連ソフトウエアの仕様書を閲覧し、実際に取得できる設計になっていること、およびログを閲覧し実際に取得していることを確認する。					
5.4.2	監査ログを処理する頻度 認証局は、監査ログを3ヶ月に1度以上定期的に検査する。	監査ログは最低3ヶ月に一度検査することが定められ実施されていること。	1)CPS、事務取扱要領等を閲覧し、最低3ヶ月に一度以上検査することが定められていることを確認する。 2)また、運用開始後3ヶ月を経過している場合は、作業記録等を閲覧し、実際に検査していることを確認する。					
5.4.3	監査ログを保存する期間 監査ログは、最低10年間保存される。	監査ログは最低10年間保存することが定められていること。	CPS、事務取扱要領等を閲覧し、監査ログを10年保存することが定められているか確認する。					

準拠性監査報告書様式（署名用）

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
5.4.4	監査ログの保護 認証局は、認可された人員のみが監査ログにアクセスできるよう、適切なアクセスコントロールを採用し、権限を持たない者の閲覧や、改ざん、不正な削除から保護する。	監査ログに関するアクセス規則が定められ、技術的もしくは運用的措置による権限管理により、それが保障されるような認証方法が定めれられていること。	CPS、事務取扱要領、関連ソフトウェアの仕様書等を閲覧し、監査ログに関するアクセス規則が定められていることを確認する。					
5.4.5	監査ログのバックアップ手順 監査ログは、オフラインの記録媒体にCPSに定める頻度でバックアップが取られ、それらの媒体はセキュアな保管場所に保管される。	1）監査ログを定期的にオフラインの記録媒体にバックアップされることが頻度を明記して定められていること。 2）また媒体の保管場所について安全性の確保を含めて定められていること。	CPS、事務取扱要領等を閲覧し、オフライン記録媒体へのバックアップ頻度が明記されていることを確認する。また、当該媒体の保管場所について、不正な閲覧、改ざん、滅失、消去などの脅威に対する安全性が確保されていることを確認する。					
5.4.6	監査ログの収集システム（内部対外部） 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されていることを確認する。					
5.4.7	イベントを起こしたサブジェクトへの通知 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されていることを確認する。					
5.4.8	脆弱性評価 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されていることを確認する。					
5.5	記録の保管							
5.5.1	アーカイブ記録の種類 認証局 は、以下の情報をアーカイブする。 ・ 証明書の発行/取消に関する処理履歴 ・ CRLの発行に関する処理履歴 ・ 認証局の証明書 ・ 加入者の証明書 ・ 証明書申請内容の審議の確認に用いた書類 ・ 失効の要求に関わる書類	認証局 は、少なくとも以下の情報をアーカイブすること。 ・証明書の発行/取消に関する処理履歴 ・CRLの発行に関する処理履歴 ・認証局の証明書 ・加入者の証明書 ・証明書申請内容の審議の確認に用いた書類 ・失効の要求に関わる書類	CPS等関連規定を閲覧し、少なくともCPに定める情報をアーカイブしていることを確認する。					
5.5.2	アーカイブを保存する期間 アーカイブする情報は、記録が作成されてから最低10年間は保存する。	アーカイブする情報は、記録が作成されてから最低10年間は保存すること。	CPS等関連規定の閲覧および必要に応じ体制および設備を調査することにより、アーカイブする情報が、記録が作成されてから最低10年間は保存されることを確認する。					
5.5.3	アーカイブの保護 アーカイブ情報の収められた媒体は物理的セキュリティによって保護され、許可された者しかアクセスできないよう制限された施設に保存され、権限を持たない者の閲覧や持ち出し、改ざん、消去から保護する。	アーカイブ情報の収められた媒体は物理的セキュリティによって保護され、許可されたものしかアクセスできないよう制限された施設に保存され、権限を持たない者の閲覧や持ち出し、改ざん、消去から保護されていること。	CPS等関連規定の閲覧および必要に応じ媒体が保管されている設備を調査することにより、アーカイブ情報の収められた媒体が物理的セキュリティによって保護され、許可されたものしかアクセスできないよう制限された施設に保存され、権限を持たない者の閲覧や持ち出し、改ざん、消去から保護されていることを確認する。					
5.5.4	アーカイブのバックアップ手続 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されているか確認する。					
5.5.5	記録にタイムスタンプをつける要件 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されているか確認する。					
5.5.6	アーカイブ収集システム（内部対外部） 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されているか確認する。					
5.5.7	アーカイブ情報を入手し、検証する手続 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されているか確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
5.6	鍵の切り替え							
	認証局は、定期的にCA私有鍵の更新を行う。CA私有鍵は、認証設備室内にて、複数人の立会いのもと、専用の暗号モジュール（HSM）を用いて生成される。 CA私有鍵の更新と共に自己署名証明書の更新も実施される。この更新においてもCA私有鍵生成の場合と同様に、複数人の立会いのもと執り行われる。	1) 認証局は、定期的にCA私有鍵の更新を行うこと。 2) CA私有鍵は、認証設備室内にて、複数人の立会いのもと、専用の暗号モジュール（HSM）を用いて生成されること。CA私有鍵の更新と共に自己署名証明書の更新も実施されること。この更新においてもCA私有鍵生成の場合と同様に、複数人の立会いのもと執り行われること。	1) CPS等関連規定を閲覧し、CA私有鍵が定期的に更新されることを確認する。 2) CPS等関連資料およびキーセレモニー等の記録を閲覧し、必要に応じ体制および設備の調査あるいは、HSMの仕様・認証取得等を確認することにより、認証設備室内にて、複数人の立会いのもと、専用の暗号モジュール（HSM）を用いてCAの私有鍵が生成され、自己証明書が更新されることを確認する。					
5.7	危殆化及び災害からの復旧							
5.7.1	災害及びCA私有鍵危殆化からの復旧手続き 認証局は、想定される以下の脅威に対する復旧手順を規定し、関係する認証局員全員に適切な教育・訓練を実施する。 ・ CA私有鍵の危殆化 ・ 火災、地震、事故等の自然災害 ・ システム（ハードウェア、ネットワーク等）の故障	認証局は、想定される以下の脅威に対する復旧手順を規定し、関係する認証局員全員に適切な教育・訓練を実施していること。 ・ CA私有鍵の危殆化 ・ 火災、地震、事故等の自然災害 ・ システム（ハードウェア、ネットワーク等）の故障	CPS等関連規定を閲覧し、CPに上げる脅威に対する復旧手続を規定しているか確認する。教育履歴簿等および訓練履歴簿等を閲覧し、関係する認証局員全員に適切な教育・訓練を実施していることを確認する。					
5.7.2	コンピュータのハードウェア、ソフトウェア、データが破損した場合の対処 ハードウェア、ソフトウェア、データが破壊又は損傷した場合、バックアップ用のハードウェア、ソフトウェア、バックアップデータを用いて、速やかに復旧作業を行い、合理的期間内に認証局業務を再開する。また、障害発生時の際には、可能な限り速やかに、加入者、検証者に情報公開用Webサイト等により通知する。	1) ハードウェア、ソフトウェア、データが破壊又は損傷した場合、バックアップ用のハードウェア、ソフトウェア、バックアップデータを用いて、速やかに復旧作業を行うことが規定化され、実施体制および設備が整備されていること。 2) また、こうした認証局業務を再開するまでの平均的な目標期間が合理的期間内であらかじめ設定されていること。 3) また、障害発生時の際には、可能な限り速やかに、加入者、検証者に情報公開用Webサイト等により通知することが規定され、実施体制および設備が整備されていること。	CPS等関連規定を閲覧すること並びに必要に応じて体制図を閲覧すること及び設備を検査することにより、復旧作業が合理的な時間で速やかに行われること及び障害発生時に加入者、検証者に情報公開用Webサイト等により通知されることを確認する。					
5.7.3	CA私有鍵が危殆化した場合の対処 CA私有鍵が危殆化又はその恐れが生じた場合は、運用責任者の判断により、速やかに認証業務を停止するとともに、認証局で規定された手続きに基づき、全ての加入者証明書の失効を行い、CRL/ARLを開示し、CA私有鍵を廃棄する。更に、原因の追求と再発防止策を講じる。	1) CA私有鍵が危殆化又は危殆化の恐れが生じた場合は、運用責任者の判断により、速やかに認証業務を停止するための体制が確立されていること。 2) さらに、全ての加入者証明書の失効を行い、CRL/ARLを開示し、CA私有鍵を廃棄するための手順および体制が規定され、実施体制及び設備が準備されていること。 3) 更に、原因の追求と再発防止策を講じるための実現可能な手順および体制が規定されていること。 4)危殆化の原因追求のために、認証局業務従事者以外の者が調査する体制をとること。	1) CPS等関連規定を閲覧することにより CA私有鍵が危殆化又は危殆化の恐れが生じた場合は、運用責任者の判断により、速やかに認証業務を停止するための体制が確立されていることを確認する。 2) さらに、CPS等関連規定を閲覧すること及び必要に応じて設備を検査することにより、全ての加入者証明書の失効を行い、CRL/ARLを開示し、CA私有鍵を廃棄するための手順および体制が規定され、実施体制及び設備が準備されていることを確認する。 3) 4)更に、CPS等関連規定を閲覧し、原因の追求と再発防止策を講じるための実現可能な手順および体制が規定化されていることを確認する。					
5.7.4	災害等発生後の事業継続性 災害などにより、認証施設及び設備が被災し、通常の業務継続が困難な場合には、認証局で規定された手続きに基づき、加入者及び検証者に情報を公開する。	災害などにより、認証施設及び設備が被災し、通常の業務継続が困難な場合には、加入者及び検証者に速やかに情報を公開するための手続きが認証局で規定されていること。	CPS等関連規定を閲覧し、必要に応じ設備を検査することにより、通常の業務継続が困難な場合に、加入者及び検証者に速やかに情報を公開するための手続きが規定されていること。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
5.8	認証局又は登録局の終了							
	認証局が運営を停止する場合には、運営の終了の90日前までに加入者に通知し、認証局の鍵と情報の継続的な保管を手配するものとする。 認証局が終了する場合には、当該認証局の記録の安全な保管又は廃棄を確実にするための取り決めを行うこととする。 登録局の運用を停止する場合は、事前に加入者の同意を得たうえで、登録局が有する加入者の情報と運営を他の登録局に移管し、それを加入者に通知する。	1) 認証局が運営を停止する場合には、運営の終了の90日前までに加入者に通知し、認証局の鍵と情報の継続的な保管方法を手配することが規定され、本規程に基づく体制が整備されていること。認証局が終了する場合には、当該認証局の記録の安全な保管又は廃棄を確実にするための取り決めが規定され、本規程に基づく体制が整備されていること。 2) 登録局の運用を停止する場合は、事前に加入者の同意を得たうえで、登録局が有する加入者の情報と運営を他の登録局に移管し、それを加入者に通知することが規定され、本規定に係る体制が整備されていること。 なお、登録局は、このような場合に他の登録局に加入者の情報や運営を他の登録局に移管することについて、事前に加入者の同意を得ること。 3) 1),2) の取り決め、2)の加入者の同意方法について監査を受け、HPKI専門家会議の審査を受けること。	1) CPS等関連規定および外部に委託している場合は必要に応じ契約書を閲覧することにより、認証局が運営を停止する場合は、運営の終了の90日前までに加入者に通知し、認証局の鍵と情報の継続的な保管方法を手配すること及び当該認証局の記録の安全な保管又は廃棄を確実にするための取り決めが規定され、本規定に基づく体制が整備されていることを確認する。 2) CPS等関連規定および外部に委託している場合は必要に応じ契約書を閲覧することにより、登録局の運用を停止する場合は、事前に加入者の同意を得たうえで、登録局が有する加入者の情報と運営を他の登録局に移管し、それを加入者に通知することおよび、このような場合に他の登録局に加入者の情報や運営を他の登録局に移管することについて、事前に加入者の同意を得ることが規定され、誰がどのように実施するかの体制が整備されていることを確認する。 3) CPS等関連規定を閲覧し、認証局または登録局の終了時の措置に関して監査を受け、HPKI専門家会議の審査を受けることが規定化されていることを確認する。					
6	技術的なセキュリティ管理							
6.1	鍵ペアの生成と実装							
6.1.1	鍵ペアの生成 CA鍵ペアは、認証設備室内に設置された専用の暗号モジュール（HSM）を用いて、複数人の立会いのもと、権限を持った者による操作により生成される。	(1)CA鍵ペアは、認証設備室内に設置された専用の暗号モジュール（HSM）を用いて適切に生成されていること。 例えば 1） 鍵ペアは、FIPS 140-2の適切なセキュリティレベルの要件（CA私有鍵の場合レベル3と同等以上）を満たす安全な暗号モジュールの中で生成されていること。 2） 鍵ペアの生成に使用される乱数発生器は、FIPS 140-2の適切なセキュリティレベル相当を満たしていること。 3） 鍵ペアの生成に使用される素数発生器は、FIPS 140-2の適切なセキュリティレベル相当を満たしていること。 4） 鍵ペアの生成には、ANSI X9又はISOの標準で規定されている鍵アルゴリズム（例えば、RSA署名つきのSHA1）が使われていること。 (2） 鍵ペアの生成には、複数の立会いのもと、権限付与された者により適切に生成されていること。 例えば 1)権限付与された者による複数人によるコントロール（例えば、知識分割・鍵分割などの技術的措置による デュアルコントロールや複数人の操作や監視などによる相互牽制）により生成されていること。 2） 鍵生成に使われるハードウェア又はソフトウェアのインテグリティ及びハードウェアとソフトウェアのインタフェースが使用前にテストされていること。 3) CAの鍵ペアは、その認証局のPAA（ポリシ承認局）がCPS（認証局運用規定）等を承認した後に、生成されていること。	(1)HSMメーカが取得している認定書等、CPS、運用マニュアル、PKIソフトウェア概要書などを閲覧し、CA鍵ペアが、認証設備室内に設置された専用の暗号モジュール（HSM）を用いて適切に生成されていることを確認する。 (2)CPS、運用マニュアル、組織図、認証局構築スケジュール、議事録、作業記録（作業申請書・指示書・報告書等）などを閲覧し、鍵ペアの生成は、複数の立会いのもと、権限付与された者により適切に生成されていることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
6.1.2	加入者への私有鍵の送付 エンドエンティティの加入者の私有鍵が認証局で生成される場合は、IETF RFC 2510「証明書管理プロトコル」に従ってオンライントランザクションで、又は同様に安全な方法によって、加入者に引き渡されるものとする。認証局はオリジナルの私有鍵を引き渡した後は私有鍵のコピーを所有していないことの証明ができるものとする。	(1) CA（又はRA）によって生成された私有鍵を加入者に送付するときは、次のいずれかの方法よって、送付が安全に行われていること。 IETF RFC 2510「証明書管理プロトコル」に準拠した方法で伝送するか、 同様な安全な方法、例えば a. 適切な身元確認を行い、対面で手渡す。 b. 秘密鍵を含むトークンを不正開封防止機能を使用した郵便で送る。 c. SSLセッションの中で伝送する。 (2) CAが加入者の代わりに鍵ペアを生成したとき、その鍵ペアが加入者に引き渡されたなら、CAは、いかなる私有鍵のコピーも保持していないこと。	(1) CPS、運用マニュアル、RAマニュアルを閲覧し、生成された私有鍵を安全に加入者に送付していることを確認する。 (2)CPS、 CAシステム概要書、PKIシステム概要書、運用マニュアルなどを閲覧し、鍵ペアが加入者に引き渡された後、CAは、いかなる私有鍵のコピーも保持していないことを確認する。					
6.1.3	認証局への公開鍵の送付 エンドエンティティの加入者の公開鍵が加入者により生成される場合は、IETF RFC 2510「証明書管理プロトコル」に従ってオンライントランザクションで、又は同様に安全な方法によって、認証局に引き渡されるものとする。	加入者によって生成された公開鍵を認証局に送付するときは、次のいずれかの方法によって、送付が安全に行われていること。 IETF RFC 2510「証明書管理プロトコル」に準拠した方法で伝送するか、 同様に安全な方法、例えば a. 適切な身元確認を行い、対面で手渡す。 b. 秘密鍵を含むトークンを不正開封防止機能を使用した郵便で送る。 c. SSLセッションの中で伝送する。B123	CPS、運用マニュアル、RAマニュアルを閲覧し、加入者によって生成された公開鍵が認証局に安全に送付されていることを確認する。					
6.1.4	検証者へのCA公開鍵の送付 CA公開鍵は、検証者によるダウンロードを可能とするために、本ポリシを公開する機関のサイトで公開するものとする。	(1) CAの公開鍵は、検証者によるダウンロードを可能とするため、本CPとともに、CAのWebサイトで公開されていること。 (2) CAの公開鍵は、定期的に交換（又は再生成）されている、又はされることになっていること。	(1) CPSおよびWebサイトを閲覧し、 CAの公開鍵が、検証者によるダウンロードを可能とするため、本CPとともに、CAのWebサイトで公開されていることを確認する。 (2) CPS、運用マニュアルなどを閲覧し、CAの公開鍵が、定期的に交換（又は再生成）されることになっていることを確認する。					
6.1.5	鍵のサイズ 鍵の最小サイズは、使用されるアルゴリズムに依存する。CA証明書の鍵の最小サイズは、RSAアルゴリズムの場合、2048ビットとする。他のアルゴリズムを使用するCA証明書の鍵の最小サイズは、同等のセキュリティを提供するサイズとする。 エンドエンティティの証明書の鍵の最小サイズは、RSAアルゴリズム又は技術的に同等のアルゴリズムの場合、1024ビットとする。他のアルゴリズムを使用するエンドエンティティの証明書の鍵の最小サイズは、同等のセキュリティを提供するサイズとする。	(1) RSAアルゴリズムを使用する場合、CAの鍵サイズは、2,048ビット以上となっていること。 (2) RSA以外のアルゴリズム使用する場合、CAの鍵サイズは、前項と同等以上のセキュリティ強度となる鍵サイズを使用していること。 (3) RSAアルゴリズムを使用する場合、加入者の鍵サイズは、1,024ビット以上となっていること。 (4) RSA以外のアルゴリズムを使用する場合、加入者の鍵サイズは、前項と同等以上のセキュリティ強度となる鍵サイズを使用していること。	(1)(2)(3)(4) CPS、CAシステム概要書、PKIソフトウェア概要書などを閲覧し、CAの鍵サイズおよび加入者の鍵サイズが指定の値になっていることを確認する。					
6.1.6	公開鍵のパラメータ生成及び品質検査 公開鍵パラメータは、信頼できる暗号モジュールによって生成される。公開鍵パラメータの品質検査も暗号モジュールにより行うものとする。	(1) 公開鍵パラメータは、FIPS 140-2の適切なセキュリティレベルの要件相当を満たす暗号モジュールの中で生成されていること。 (2) 公開鍵パラメータの品質検査が、FIPS 140-2の適切なセキュリティレベルの要件相当を満たす暗号モジュールの中で行われていること。	(1)(2) メーカが取得している認定書、CPS等を閲覧し、公開鍵パラメータ生成および品質管理が信頼できる暗号のジュールで行われていることを確認する。					
6.1.7	鍵の利用目的 認証局の鍵は、keyCertSignとcRLSignのビットを使用する。 エンドエンティティの鍵は、nonRepudiationのビットを使用する。	(1) 鍵ペアは、個人、国家資格所有者、医療機関等の管理者などに発行された証明書が、本人と公開鍵が一意に関連することを証明する単一の目的（署名と検証）のためにのみ利用されていること。 (2) CAの鍵は、keyCertSignとcRLSignのビットを使用していること。 (3) 加入者の鍵は、nonRepudiationのビットを使用していること。	(1)(2)(3) CP、CPSを閲覧し、KeyusageがCPの指定どおりになっていることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
6.2	私有鍵の保護及び暗号モジュール技術の管理							
6.2.1	暗号モジュールの標準及び管理 CA私有鍵の格納モジュールは、US FIPS 140-2レベル3と同等以上の規格に準拠するものとする。 エンドエンティティの加入者私有鍵の格納モジュールは、US FIPS 140-2レベル1と同等以上の規格に準拠するものとする。	(1) CA私有鍵を格納する暗号モジュールは、FIPS 140-2のセキュリティレベル3と同等以上の規格に準拠していること。 (2) 加入者私有鍵を格納する暗号モジュールは、FIPS 140-2のセキュリティレベル1と同等以上の規格に準拠していること。	(1)(2) メーカが取得している認定書、CPS等を閲覧し、私有鍵を格納する暗号モジュールが CA私有鍵の場合はFIPS 140-2のセキュリティレベル3および加入者私有鍵の場合はFIPS 140-2のセキュリティレベル1と同等以上の規格に準拠していることを確認する。					
6.2.2	私有鍵の複数人によるコントロール CA私有鍵の生成には、運用管理者と複数名の権限者を必要とする。また、鍵生成後の私有鍵の操作（活性化、非活性化、バックアップ、搬送、破棄等）においても複数名の権限者を必要とする。	CA私有鍵の取り扱い（生成、活性化、非活性化、バックアップ、リカバリ、格納、搬送、破棄など）は、物理的に安全な環境で運用管理者と複数人の権限付与された複数人によるコントロール（例えば、知識分割・鍵分割などの技術的措置によるデュアルコントロールや複数人の操作や監視などによる相互牽制）によって私有鍵の管理が行われていること。	CPS、運用マニュアル、操作マニュアル、業務記録等を閲覧し、物理的に安全な環境で運用管理者と権限付与された複数人によるコントロールによって私有鍵の管理が行われていることを確認する。					
6.2.3	私有鍵のエスクロウ CA私有鍵は、法律によって必要とされる場合を除き、エスクロウされないものとする。 エンドエンティティの加入者の私有鍵は、法律によって必要とされる場合を除き、エスクロウされないものとする。	(1) CA私有鍵は、法律によって必要とされる場合を除き、第三者に預託されていないこと。 (2) CA私有鍵が第三者に預託されている場合、当事者間の賠償責任と救済手段を規定した契約が存在すること。 (3) CA私有鍵が第三者に預託されている場合、預託されたCA私有鍵のコピーは、オリジナルの鍵と同等レベル以上のセキュリティ統制に従っていること。 (4) 加入者の私有鍵は、法律によって必要とされる場合を除き、第三者に預託されていないこと。	(1) (4)CPSを閲覧し、CA私有鍵および加入者の私有鍵が、法律によって必要とされる場合を除き、第三者に預託されていないこととなっていることを確認する。 (2)CPS、契約書を閲覧し、預託された場合、賠償責任と救済手段を規定した契約が存在することを確認する。 (3)CPS、契約書を閲覧し、預託された場合、預託されたCA私有鍵のコピーは、オリジナルの鍵と同等レベル以上のセキュリティ統制に従っていることを確認する。					
6.2.4	私有鍵のバックアップ CA私有鍵のバックアップは、安全な方法で行う。例えば、バックアップ作業の権限を有する複数人の立会いのもとで行うようにしたり、バックアップデータとしてCA私有鍵に関する情報を暗号化したり分散させて保管するなどの方法がある。	(1) CA私有鍵が暗号モジュールからエクスポートされて、バックアップのために安全なストレージに移転される場合、権限付与された複数人によるコントロール（例えば、知識分割・鍵分割などの技術的措置による デュアルコントロールや複数人の操作や監視などによる相互牽制）によって、次のいずれかを含む安全な鍵管理スキームでCA私有鍵をエクスポートしていること。 a. CA私有鍵の関する情報を暗号文として b. CA私有鍵の関する情報又は所有を分散し、暗号化されたフラグメントとして c. 鍵転送デバイスのような別の安全な暗号モジュールの中で (2) CA私有鍵のバックアップコピーは、オリジナルの鍵と同等レベル以上のセキュリティ統制に従っていること。 (3) CA私有鍵のリカバリは、権限付与された複数人によるコントロール（例えば、知識分割・鍵分割などの技術的措置によるデュアルコントロールや複数人の操作や監視などによる相互牽制）によって、バックアッププロセスと同じスキームで実施されていること。	(1)(3) CPS、CAシステム概要書、PKIソフトウェア概要書、運用マニュアルなどを閲覧し、権限付与された複数人によるコントロールでCA私有鍵をエクスポートおよびリカバリーされることを確認する。 (2) CPS、運用マニュアルを閲覧し、CA私有鍵のバックアップコピーは、オリジナルの鍵と同等レベル以上のセキュリティ統制に従っていることを確認する。					
6.2.5	私有鍵のアーカイブ 認証局は加入者の私有鍵をアーカイブしない。	CAは、加入者の私有鍵をアーカイブしないポリシに準拠している。	CPSを閲覧し、加入者の私有鍵をアーカイブしないポリシに準拠していることを確認する。					
6.2.6	暗号モジュールへの私有鍵の格納と取り出し CA私有鍵は、安全に格納することとする。例えば、認証設備室内にある暗号モジュール内に格納するなどの方法がある。 外部へのバックアップの転送や外部からのリストアの場合は、セキュアチャネルを通して行うものとする。	1）CA私有鍵は、安全に格納すること。例えば、認証設備室内にある暗号モジュール内に格納すること。 2）外部へのバックアップの転送や外部からのリストアの場合は、セキュアチャネルを通して行うこと。	CPS、CAシステム概要書、PKIソフトウェア概要書、運用マニュアルなどを閲覧し、CA私有鍵が安全に格納されていること、また、外部へのバックアップや外部からのリストアの場合、セキュアチャネルを通じて行っていることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
6.2.7	暗号モジュールへの私有鍵の格納 私有鍵がエンティティの暗号モジュールで生成されない場合は、IETF RFC 2510「証明書管理プロトコル」に従って、又は同様に安全な方法で、モジュールに入力されるものとする。	鍵ペアは、それが使用されるのと同じ暗号モジュールの中で生成されている、又は、それが生成された暗号モジュールから使用されるデバイスへ次のような方法によって、直接投入されていること。 a. IETF RFC 2510「証明書管理プロトコル」 又は同様に安全な方法、例えば b. 2Key-3DESで転送した後、デバイス内で安全に復号	CPS、HSM概要書、運用マニュアル、CAシステム概要書、PKIソフトウェア概要書、鍵ライフサイクル管理規程などを閲覧し、私有鍵がエンティティの暗号モジュールで生成されない場合は、私有鍵が加入者の暗号モジュールに安全に入力されることを確認する。					
6.2.8	私有鍵の活性化方法 CA私有鍵の活性化の方法は、認証局室内において本CP「6.2.2 私有鍵の複数人によるコントロール」と同じく、複数名の権限を有する者を必要とする。	CA私有鍵の活性化は、物理的に安全な場所（認証局室内等）で、権限を付与された複数人によるコントロール（例えば、知識分割・鍵分割などの技術的措置によるデュアルコントロールや複数人の操作や監視などによる相互牽制）によって行われていること。	CPS、運用マニュアル、鍵ライフサイクル管理規程などを閲覧し、CA私有鍵の活性化は、物理的に安全な場所認証局室内）で、権限を付与された複数人によるコントロールによって行われていることを確認する。					
6.2.9	私有鍵の非活性化方法 CA私有鍵の非活性化の方法は、認証局室内において本CP「6.2.2 私有鍵の複数人によるコントロール」と同じく、複数名の権限を有する者を必要とする。	CA私有鍵の非活性化は、物理的に安全な場所（認証局室内等）で、権限を付与された複数人によるコントロール（例えば、知識分割・鍵分割などの技術的措置によるデュアルコントロールや複数人の操作や監視などによる相互牽制）によって行われていること。	CPS、運用マニュアル、鍵ライフサイクル管理規程などを閲覧し、CA私有鍵の非活性化が、物理的に安全な場所（認証局室内等）で、権限を付与された複数人によるコントロールによって行われていることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
6.2.10	私有鍵の廃棄方法 CA私有鍵を破棄しなければならない状況の場合、認証局室内で本CP「6.2.2　私有鍵の複数人によるコントロール」と同じく、複数名の権限を有する者によって、私有鍵の格納されたHSM を完全に初期化し、又は物理的に破壊する。同時に、バックアップの私有鍵に関しても同様の手続きによって破棄する。 加入者私有鍵破棄手続きは、CPS又は加入者が入手可能な文書に記述するものとする。	(1) CA私有鍵を破棄する場合、物理的に安全な場所(認証局室内等)で、権限を付与された複数人によるコントロール（例えば、知識分割・鍵分割などの技術的措置によるデュアルコントロールや複数人の操作や監視などによる相互牽制）によって、安全な方法（例えばトークンへの新しい鍵・ゼロ又はスペースの上書き、トークンの破壊など）で行われていること。 (2) CA鍵ペアの有効期間が終了するとき、そのCA私有鍵の全てのコピーとフラグメントが、破壊されていること。 (3) アクセス可能な状態にある暗号モジュールが永久にサービスから取り除かれるとき、そのモジュールの中に格納されている全ての鍵が消去されていること。 (4) 加入者の私有鍵の破棄手続が、CPS又は加入者が入手可能な文書に明記されている。	CPS、運用マニュアル、鍵ライフサイクル管理規程などを閲覧し、CA私有鍵および加入者私有鍵が権限を付与された複数人によるコントロールで安全な方法を用いて破棄されることを確認する。					
6.2.11	暗号モジュールの評価 CA私有鍵を格納する暗号モジュールは、FIPS 140-2レベル3と同等以上のものを使用する。 エンドエンティティの加入者の私有鍵を格納する暗号モジュールは、FIPS 140-2レベル1と同等以上のものを使用する。	暗号モジュールは、FIPS 140-2の適切なセキュリティレベル（CA私有鍵の場合レベル3と同等以上、加入者私有鍵の場合レベル1と同等以上）のものを使用していること。	メーカ取得した認定書、CPSを閲覧し、FIPS 140-2の適切なセキュリティレベルのものを使用していることを確認する。					
6.3	鍵ペア管理に関するその他の面							
6.3.1	公開鍵のアーカイブ 公開鍵は、後日の署名の検証を可能にするために、信頼できる方法でアーカイブする必要がある。認証局は、公開鍵がCPSで定める期間アーカイブされることを保証する責任があるものとする。	認証局は、デジタル署名又は適切なインテグリティコントロールによって改ざんを検証又は防止し、CPSが定める期間、CAが生成した全ての公開鍵（CA、レポジトリ、下位CA、RA、加入者及び他の関係者）をアーカイブしていること。	CPS、運用マニュアル、鍵ライフサイクル管理規程などを閲覧し、CPSが定める期間、CAが生成した全ての公開鍵をアーカイブしていることを確認する。					
6.3.2	公開鍵証明書の有効期間と鍵ペアの使用期間 CA公開鍵証明書の有効期間は20年を越えないものとし、その私有鍵の使用は10年を越えないものとする。 エンドエンティティの加入者の公開鍵証明書の有効期間は5年を越えないものとし、その私有鍵の使用は公開鍵証明書の有効期限の1ヶ月前を越えないものとする。	(1) CA公開鍵証明書の有効期間は20年を越えないものとし、その私有鍵の使用は10年を越えないものとしていること。 (2) エンドエンティティの加入者の公開鍵証明書の有効期間は5年を越えないものとし、その私有鍵の使用は公開鍵証明書の有効期限の1ヶ月前を越えないものとしていること。	(1)(2) CPSを閲覧し、私有鍵および公開鍵の有効期間がCPで定める範囲内であることを確認する。					
6.4	活性化用データ							
6.4.1	活性化データの生成とインストール 認証局において用いられるCA私有鍵の活性化データは一意で予測不能なものとし、その生成とインストールは認証局で定められた規定に従い実施されるものとする。 エンドエンティティの加入者私有鍵の活性化データが認証局で生成される場合は、活性化データは一意で予測不能なものとし、その生成とインストールは認証局で定められた規定に従い実施され、加入者に安全に伝えられるものとする。 加入者私有鍵の活性化データを加入者が生成する場合は、活性化データは予測不能なものとし、その生成とインストールは認証局で定められた規定に従い実施されるものとする。	(1) CA私有鍵の活性化データ（PIN、パスフレーズ、鍵分散の断片など）は、一意で予測不能なものになっていること。 (2) CA私有鍵の活性化データの生成及びインストールは、CPS等に準拠し実施されていること。 (3) 加入者私有鍵の活性化データは、一意で予測不能なものになっていること。 (4) 加入者私有鍵の活性化データの生成及びインストールは、CPS等に準拠し実施されていること。	(1)(3) CPS、PKIソフトウェア概要書、鍵ライフサイクル管理規程などを閲覧し、活性化データが一意で予測不能なものになっていることを確認する。 (2)(4) CPS、運用マニュアル、RAマニュアルなどを閲覧、および、実際の操作を観察し活性化データの生成及びインストールが、CPSに準拠して実施されていることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
6.4.2	活性化データの保護 認証局において用いられるCA私有鍵の活性化データは、認証局で定められた規定に従い安全に保護される。 エンドエンティティの加入者私有鍵の活性化データが認証局で生成される場合は、活性化データが加入者に伝えられた後は、認証局においては完全に破棄し保管しないものとする。また、伝えられた活性化データは、認証局で定められた規定に従い、加入者により安全に保護するものとする。 加入者私有鍵の活性化データを加入者が生成する場合は、認証局で定められた規定に従い、加入者により安全に保護するものとする。	(1) CA私有鍵の活性化データの取扱い（保管、バックアップ、転送、廃棄など）は、CPSに準拠し、CA私有鍵と同等に安全に保護されていること。 (2) CA（又はRA）が加入者の活性化データを生成している場合、認証局は、私有鍵の活性化データを、加入者に送付した後、完全に廃棄（消磁、破壊、他のデータの上書きなど）し、保管していないこと。 (3) 加入者は、自ら生成した又は認証局から送付された活性化データを安全に保護するよう、CPS、契約書、サービス約款などで義務付けられていること。	(1) CPS、運用マニュアル、RAマニュアルなどを閲覧、CA私有鍵の活性化データが安全に取扱われていることを確認する。 (2) CPS、PKIソフトウェア概要書、鍵ライフサイクル管理規程などを閲覧し、CA（又はRA）が加入者の活性化データを生成している場合、認証局は、私有鍵の活性化データを、加入者に送付した後、完全に廃棄し、保管していないことを確認する。 (3) CPS、契約書、利用約款などでを閲覧し、加入者が自ら生成した又は認証局から送付された活性化データを安全に保護するよう義務付けられていることを確認する。					
6.4.3	活性化データのその他の要件 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されているか確認する。					
6.5	コンピュータのセキュリティ管理							
6.5.1	特定のコンピュータのセキュリティに関する技術的要件 認証業務用設備に対する当該電気通信回線を通じて行われる不正なアクセス等を防御するための対策を行うこと。 CAシステムへのログイン時には、本CP「5.2.3　個々の役割に対する本人性確認と認証」で定めるユーザの認証を必須とする。	・認証業務用設備に対するアクセスに対する方針（例えば、①職務に対応したアクセス権限付与、②個人識別及び本人確認の方法、③職務分離、④特別なCAオペレーションを遂行するために必要な要員数（n out of m rule））が定められていること。 ・上記アクセス方針は、認証業務用設備に対する不正なアクセス等を防御することに対する対策(具体的には、①個人識別、②本人確認、③権限確認、④アクセスログ取得)を講じていること。 ・認証業務用設備に対するアクセスポイントにおいて、上記アクセス方針に基づく設定が行われていること。 ・CAシステムへのログイン時のプロセスが、本CP「5.2.3　個々の役割に対する本人性確認と認証」で定める方法と同じプロセスにより、ユーザの認証を行っていること。	・認証業務用設備に対して責任を有するものに対する質問により、左記アクセス方針が想定されるリスクに対して十分であると判断している理由等を確認する。 （①CAオペレータのOSアクセス、②DB管理者のDBMSアクセス、RAオペレータのCAアプリケーションアクセスのそれぞれについて、必要に応じCAの構成に応じ確認する） ・認証業務用設備に対する当該電気通信回線へのアクセスに対する方針をレビュし、対策の網羅性、リスクに対する対策強度の十分性を評価する。 ・認証業務用設備に対するアクセスポイントにおいて、左記アクセス方針に従った設定が行われていることを機器等の設定値を閲覧することにより確認する。 ・CAシステムへのログイン時のプロセスが、本CP「5.2.3　個々の役割に対する本人性確認と認証」で定める方法と同じプロセスによりユーザの認証を行っていることを、運用規程等により確認する。					
6.5.2	コンピュータセキュリティ評価 ISO15408を参考にセキュリティ基準を設ける等の対応を行い、客観的に評価を行うこと。	・コンピュータ機器に対するセキュリティ基準を定めること。 ・コンピュータ機器が、上記セキュリティ基準により適切な客観的な評価者による評価を受けていること。 要件として求められるものではないが、例えば CAソフトウェア及びインターネットファイアウォールに関しては、次に掲げる業界基準があり、セキュリティ基準の設定、セキュリティ対策の参考とすることができる。 ①ITSEC－レベルE2 ②TCSEC－レベルC2 ③CC（ISO15408）－レベルEAL3	・責任者に対し質問あるいは評価報告書等を閲覧し、ISO15408等のセキュリティ基準を参考にし、コンピュータ機器に対する想定されるリスクを軽減するための十分なセキュリティ基準を定めていることを確認する。 ・上記セキュリティ基準を閲覧し、想定されるリスクを軽減するために十分なセキュリティ対策が規定されていることを評価する。 ・評価報告書等を閲覧し、コンピュータ機器が、上記セキュリティ基準に照らして客観的な評価者による評価を受けていることを確認する。 ・評価者に質問、又は評価者の評価能力を示す資料を閲覧することにより、上記評価者が十分な評価能力を有していることを確認する。					

準拠性監査報告書様式（署名用）

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
6.6.1	システム開発管理 JIS Q 27002:2006「第12章　情報システムの取得、開発及び保守」と同等以上の規格に従うものとする。	・新規システム又は既存システムの改善に対するビジネス要件定義書には、コントロール要件を具体的に記述すること。(12.1.1) ・認証業務用システムの変更の実施は，正式な変更管理手順の使用によって，管理すること。(12.5.1) ・オペレーティングシステムを変更した場合は、認証業務用システムを閲覧し、運用又はセキュリティに影響を与えないかどうかを確認すること。(12.5.2) ・パッケージソフトウェアの変更は、組み込まれたコントロールとイングリティのプロセスが危殆化する場合やベンダから必要な改定版が得られる場合を除き、極力行わないこと。(12.5.3) ・隠れチャネル及びトロイの木馬が心配される場合には、信頼できるソースからのソフトウェアの購入、コード変更の制限、ソースコードの検査を行うこと。(12.5.4) ・ソフトウェア開発を外部委託する場合には、ライセンス契約、コードの所有権、知的財産権、実施される業務の品質検査、立ち入り監査権、受入検査などについて検討を行うこと。(12.5.5)	・開発・保守管理責任者に質問し、システム開発・保守のための手続きの説明をうけ、統制上の重大なプロセス漏れがないことを確認する。 ・システム開発・保守のための規程・手続書類を閲覧し、想定されるリスクに対して十分な統制活動が組み込まれていることを評価する。 ・システム開発・保守のための申請書等を閲覧し、定められた閲覧・検査・承認が適切に行われていることを確認する。 ・ソフトウェア開発を外部委託する場合の事業者・作業者の選定基準および契約書を閲覧し、想定されるリスクに対して十分な統制活動が組み込まれていることを評価する。					
6.6.2	セキュリティ運用管理 JIS Q 27002:2006「第12章　情報システムの取得、開発及び保守」、「第13章　情報セキュリティインシデントの管理」、「第14章　業務継続管理」と同等以上の規格に従うものとする。	・認証業務用システムに入力されたデータは、正確で適切であることを確かめるために、その妥当性を確認すること。(12.2.1) ・処理エラーや意図的な行為によるデータの改変を検出するために、システムに妥当性の検査を組み込むこと。(12.2.2) ・メッセージ内容のインテグリティを確保すべきセキュリティ要件がCAシステムに存在する場合には、メッセージ認証の適用を考慮すること(12.2.3) ・認証業務用システムからの出力データについては、格納された情報の処理がシステム状況に応じて正しく、適切に行われたことを確かめるために、妥当性を確認をすること。(12.2.4) ・運用システムへのソフトウェアの導入を管理すること。(12.4.1) ・試験データを保護し、管理すること。(12.4.2) ・プログラムソースライブラリへのアクセスを厳密に管理すること。(12.4.3)	・運用規程、運用手順書を閲覧し、認証業務用システムに入力・処理・出力されるデータが、正確で適切であることを確実するために必要な手順が定められていることを確認する。 ・認証業務用システム上のソフトウェアの実行を管理するための運用規程・運用手順書が整備されていることを確認する。					
		情報セキュリティ事象は，適切な管理者への連絡経路を通して，できるだけすみやかに報告すること。(13.1.1) 情報セキュリティインシデントに対する迅速，効果的で整然とした対応を確実にするために，責任体制及び手順を確立すること。(13.2.1) 情報セキュリティインシデント後の個人又は組織への事後処置が法的処置（民事又は刑事）に及ぶ場合には， 関係する法域で定めている証拠に関する規則に従うために，証						
		・組織全体を通じて事業継続計画を開発及び保守するための健全な管理プロセスが整っていること。(14.1.1) ・事業継続計画は、業務プロセスの中断を引き起こし得る事象を明確化することから始めること。(14.1.2) ・重要な業務プロセスの中断又は破綻の後、必要なタイムフレームで、事業運営を維持又は復旧させるための計画を立てること。(14.1.3) ・すべての計画が整合したものになることを確実にするため、また、試験及び保守の優先順位を明確にするために、一つの事業継続計画（ビジネスユニットごとに作成される）に関する共通の枠組みを維持すること。(14.1.4) ・事業継続計画が最新かつ有効であることを確かめるために、定期的に試験すること。(14.1.5) ・事業継続計画の継続的な有効性を確かめるために、定期的な見直し及び更新によって維持すること。(14.1.5)	・認証業務責任者に質問し、認証業務について、事業戦略的な観点から事業継続計画が策定されていることを、確認する。 ・認証業務についての事業継続計画を閲覧し、想定されるリスクに応じて適切な手順であることを評価する。 ・想定されるリスクが適切であることを評価する。 ・認証業務用システムについて、それぞれの業務手続きの中断又は障害の後、認証業務の運営を維持又は要求される時間内に復旧させるための計画を策定していることを確認する。 ・上記事業継続計画が有効に機能するための試験結果を閲覧し、計画の有効性を評価する。 ・認証業務運営会議等の議事録等を閲覧し、上記事業継続計画が、試験結果等に基づき適切に改善されていることを評価する。					
6.6.3	ライフサイクルのセキュリティ管理 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されているか確認する。					

準拠性監査報告書様式（署名用）

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
6.7	ネットワークのセキュリティ管理 JIS Q 27002:2006と同等以上の規格に従うものとする。 例えば、JIS Q 27002:2006 の「第10章　通信及び運用管理 10.6　ネットワークセキュリティの管理」、「第11章　アクセス制御 11.4　ネットワークのアクセス制御」等がこれに相当する。	1)ネットワークにおけるセキュリティを実現し、かつ維持するために、次の事項を含む、一連の管理策を実施すること。(10.6.1) ・ネットワーク運用責任とコンピュータ操作作業を分離すること ・遠隔地に所在する設備がある場合、その管理責任および管理手順を確立すること ・公衆ネットワークを通過するデータの機密性および完全性を保護する管理策を確立すること ・ネットワークに接続したシステムを保護するための管理策を確立すること ・必要に応じネットワークサービスの可用性およびネットワークに接続したコンピュータの可用性を維持するための管理策を確立すること	1)ネットワーク管理に関わる手順書等を閲覧し、管理策が定められていることを確認する。 2)責任者に質問あるいは必要により検査し、管理策が実施されていることを確認する。					
		2)内部及び外部のネットワークを介したサービスは制御されることが望ましい。そのために次の事項を含む一連の管理策を実施すること。(11.4) ・ネットワークサービスの利用者には、使用することが特別に認可されたサービスへの直接のアクセスだけを提供すること。その為に個別方針を明確にすること(11.4.1)	1)利用者に使用を許可するネットワークサービスを想定した文書を閲覧し、次の事項が定められていることを確認する。 ・アクセスが許可されるネットワークおよびネットワークサービス ・アクセス許可の手順 ・ネットワーク接続とネットワークサービスへのアクセスを保護するための管理策と管理手順 2)認証局ネットワークの厚生情報を閲覧し、利用者が使用できるネットワークサービスが、許可されたサービスのみに限定されることを確認する。					
		・遠隔地からの利用者のアクセスには、認証を行うこと。(11.4.2) 認証方法は例えば以下によること。 ・暗号に基づく技術 ・ハードウェアトークン ・チャレンジレスポンス	1)認証局ネットワークの構成図を閲覧し、認証局への遠隔接続の有無を確認する。 2)遠隔接続がある場合、接続時の認証方法を記載した文書を閲覧し、認証が行われていることを確認する。 3)遠隔接続時の認証に関わるコンピュータの設定情報を閲覧し、遠隔接続時に認証が行われるよう設定されていることを確認する。 4)遠隔接続の手順を観察し、規定どおりの認証が行われることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
		診断用及び環境設定用ポートへの物理的及び論理的なアクセスは，制御すること。(11.4.4)	手順書等を閲覧し、遠隔診断ポートへのアクセスは、適切な管理のもとに行われるよう、手順が定められていることを確認する。 設備を視察し、遠隔診断ポートへのアクセスが、安全に管理されているか確認する。					
		・情報サービス、利用者及び情報システムのグループを分割するためのネットワークセグメンテーションの導入を考慮すること。(11.4.5)	認証局のネットワーク構成図を閲覧し、認証局ネットワークが、他のネットワークから物理的あるいは論理的に、分割されていることを確認する。 設備を視察し、物理構成が、構成図と一致していることを確認する。 ネットワーク構成情報を閲覧し、論理構成が構成図と一致していることを確認する。					
		共有ネットワーク，特に，組織の境界を越えて広がっているネットワークについて，アクセス制御方針及び業務用ソフトウェアの要求事項に沿って，利用者のネットワーク接続能力を制限すること。(11.4.6)	認証局に関わる業務用ソフトウェアのアクセス制御方針を閲覧し、利用者が利用可能なサービスが限定されていることを確認する。 ネットワークの構成情報を閲覧し、アクセス制御方針に基づき、利用できるサービスを制限するよう設定されていることを確認する。					
		・共有ネットワークは、コンピュータの接続及び情報の流れが業務用ソフトウェアのアクセス制御方針に違反しないことを確実にするためのルーティング制御（ソースとデスティネーションのアドレスをチェックする機能）を組み込むこと。(11.4.7)	1)共有ネットワークを使用している場合、ネットワークの経路制御の方法を記載した資料を閲覧し、発信元および宛先アドレスの自動的検査による経路制御が適用されているか確認する。 2)ネットワークの構成情報を閲覧し、経路制御について設定されていることを確認する。					
6.8	タイムスタンプ 認証設備は、アプリケーション等において正確な日付・時刻を使用することとする。例えば、NTPサービスやGPS、電波時計等による時刻同期が挙げられる。	認証設備で使用するコンピュータは、アプリケーション等において正確な日付・時刻を使用すること。 例えばNTPサービスやGPS、電波時計等による時刻同期を行うこと。 その選択にあたり、ビジネス要件に基づいて、タイムソースの信頼性、許容時差、調時方法を明確に定め、認証局システムの主要な機器の時刻を調節すること。	1)設計書、手順書等を閲覧し、時刻同期が行われていること、およびその方式を選択するにあたり評価が行われていることを確認する。 2)運用記録等を閲覧し、設計どおりに時刻同期が行われていることを確認する。					
7	証明書及び失効リスト及びOCSPのプロファイル							
7.1	証明書のプロファイル							
	本CPの認証局が発行する証明書は、X509 Version 3 フォーマット証明書形式により作成され、また証明書はX.500識別名（Distinguished Name、以下DNという）により一意に識別されるものとする。 本ポリシに従い発行される電子証明書のプロファイルは、基本領域のプロファイルを表7.1.1に示し、拡張領域のプロファイルを表7.1.2の通りとする。 なお、IssuerのDNはCPS及びその他開示文書に記述されることとする。	1) また証明書はX.500識別名（Distinguished Name、以下DNという）により認証局ごとに一意に識別される体系とすること。 2) 発行される電子証明書のプロファイルの内、基本領域のプロファイルはCP中の表7.1.1に従い、拡張領域のプロファイルは表7.1.2に従うこと。 3) なお、IssuerのDNは他の認証局と重ならないことについて、HPKI認証局専門家会議による確認をうけ、CPS及びその他開示文書に記載すること。	1) CPS等関連規程を閲覧し証明書はX.500識別名（Distinguished Name、以下DNという）により認証局ごとに一意に識別される体系となっていることを確認する。 2) CPS等関連規程および証明書のサンプルデータを閲覧し、電子証明書のプロファイルの内、基本領域のプロファイルはCP中の表7.1.1に従い、拡張領域のプロファイルは表7.1.2に従っていることを確認する。 3) CPS等関連規定を閲覧し、IssuerのDNは他の認証局と重ならないことについて、HPKI認証局専門家会議による確認をうけ、CPS及びその他開示文書に記載していることを確認する。					

準拠性監査報告書様式（署名用）

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
7.1.1	バージョン番号 本ポリシの認証局が発行する証明書は、X509 Version 3 フォーマット証明書形式により作成されることとする。	認証局が発行する証明書は、X509 Version 3 フォーマット証明書形式により作成されること。	CPS等関連規程および証明書のサンプルデータを閲覧し、証明書が、X509 Version 3 フォーマット証明書形式により作成されていることを確認する。					
7.1.2	証明書の拡張（保健医療福祉分野の属性を含む） 本ポリシに従い発行される電子証明書の拡張領域のプロファイルは以下の表7.1.2の通りとする。 subjectDirectoryAttributes拡張で用いる保健医療福祉分野の属性（hcRole）については7.1.10で定める。	発行される電子証明書の拡張領域のプロファイルはCP中の表7.1.2に従うこと。 subjectDirectoryAttributes拡張で用いる保健医療福祉分野の属性（hcRole）については7.1.10項の定めに従うこと。	CPS等関連規程および証明書のサンプルデータを閲覧し、発行される電子証明書の拡張領域のプロファイルはCP中の表7.1.2に従っていること、およびsubjectDirectoryAttributes拡張で用いる保健医療福祉分野の属性（hcRole）については7.1.10項の定めに従っていることを確認する。					
7.1.3	アルゴリズムオブジェクト識別子 基本領域のSignatureアルゴリズムは以下の通りとする。 sha1WithRSAEncryption (1.2.840.113549.1.1.5) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) 基本領域のsubjectPublicKeyInfoアルゴリズムは以下の通りとする。 RSAEncryption (1.2.840.113549.1.1.1)	基本領域のSignatureアルゴリズムは以下のものを採用すること。 sha1WithRSAEncryption (1.2.840.113549.1.1.5) sha256WithRSAEncryption (1.2.840.113549.1.1.11) sha384WithRSAEncryption (1.2.840.113549.1.1.12) sha512WithRSAEncryption (1.2.840.113549.1.1.13) 基本領域のsubjectPublicKeyInfoアルゴリズムは以下を採用すること。 RSAEncryption (1.2.840.113549.1.1.1)	CPS等関連規程および証明書のサンプルデータを閲覧し、SignatureおよびsubjectPublicKeyInfoアルゴリズムがCPで示すものを採用していることを確認する。					
7.1.4	名称の形式 IssureとSubjectの名前の形式は表7.1.1に示される。	IssureとSubjectの名称の形式はCPの表7.1.1に示すプロファイルの規定に従うこと。	CPS等関連規程および証明書のサンプルデータを閲覧し、IssureとSubjectの名前の形式がCPの表7.1.1に示すプロファイルの規定に従っていることを確認する。					
7.1.5	名称制約 用いない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されているか確認する。					
7.1.6	CPオブジェクト識別子 別途規定する。	HPKI署名用証明書ポリシのOIDは1.2.392.100495.1.5.1.1.3.1とすること。	CPS等関連規程および証明書のサンプルデータを閲覧し、OIDが1.2.392.100495.1.5.1.1.3.1であることを確認する。					
7.1.7	ポリシ制約拡張 使用しない。	ポリシ制約のための拡張は使用しないこと。	CPS等関連規程および証明書のサンプルデータを閲覧し、ポリシ制約のための拡張は使用していないことを確認する。					
7.1.8	ポリシ修飾子の構文及び意味 CPSを参照するURLを含めることができる。	CPSを参照するURLを証明書ポリシへ付加する場合はその旨CPS等で明確にすること。	CPSを参照するURLを証明書ポリシへ付加している場合はCPS等関連規程および証明書のサンプルデータを閲覧し、URLが付加されていることを確認する。					
7.1.9	証明書ポリシ拡張フィールドの扱い 本CPのOIDを格納する。	認証局は証明書ポリシとしてCPの規定するOIDを格納すること。	CPS等関連規程および証明書のサンプルデータ閲覧し、証明書ポリシとしてCPの規定するOIDを格納していることを確認する。					
7.1.10	保健医療福祉分野の属性（hcRole） （1）サブジェクトディレクトリ属性拡張でのhcRole属性の使用 以下省略	subjectDirectoryAttributesのattrTypeにはhcRoleを表すOID {1 0 17090 0 1} を設定すること。 coding scheme referenceのOIDとしてはCPの元で定めた表7.1.3の資格名を参照するlocal coding scheme reference のOID{'1 2 392 100495 1 6 1 1}を用いること。 資格名は、CPの表7.1.3に示す英語表記を用いUTF8stringで設定すること。 subjectが複数の資格を有する場合は、HCActorDataに資格数分のHCActorを設定することができる。 本拡張は、加入者が国家資格保有者及び医療機関等の管理者の場合は必須、その他(患者等)の場合は省略可とする。	CPS等関連規程および証明書のサンプルデータを閲覧し、HCActorDataがCPで規定するフォーマットに従っていることを確認する。					

準拠性監査報告書様式（署名用）

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
7.2	証明書失効リストのプロファイル							
7.2.1	バージョン番号 認証局が発行するCRLは、X.509CRLフォーマット形式のバージョン2に従うものとする。 基本領域のプロファイルは表7.2.1に示す。	認証局が発行するCRLは、X.509CRLフォーマット形式のバージョン2に従うこと。 基本領域のプロファイルはCPの表7.2.1に従うこと。	CPS等関連規程およびCRLのサンプルデータを閲覧し、CRLの形式がX.509CRLフォーマット形式のバージョン2に従っていること、および基本領域のプロファイルはCPの表7.2.1にしたがっていることを確認する。					
7.2.2	CRLとCRLエントリ拡張領域 CRLエントリの拡張領域のプロファイルは、以下の表7.2.2の通りとする。CRL拡張領域のプロファイルは、以下の表7.2.3の通りとする。 以下省略	CRLエントリの拡張領域のプロファイルは、CPの表7.2.2に従うこと。また、CRL拡張領域のプロファイルは、CPの表7.2.3に従うこと。	CPS等関連規程およびCRLのサンプルデータを閲覧し、CRLエントリの拡張領域のプロファイルは、CPの表7.2.2に従うこと、および、CRL拡張領域のプロファイルは、CPの表7.2.3に従うことを確認する。					
7.3	OCSPプロファイル							
7.3.1	バージョン番号 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されているか確認する。					
7.3.2	OCSP拡張領域 規定しない。	CPとして監査目標項目なし。	CPS等で規定のある場合は特に規定上問題がないか確認し、規定どおり実施されているか確認する。					
8	準拠性監査とその他の評価							
8.1	監査頻度 認証局の準拠性監査は、1年以下の間隔で行われるものとする。但し、移管、譲渡、合併など、認証局の構成に大規模な変更があった場合は直ちに監査を実施するものとする。	認証局の準拠性監査は、1年以下の間隔で設定すること。但し、移管、譲渡、合併など、認証局の構成に大規模な変更があった場合、直ちに監査を実施すること。	CPS等関連規定を閲覧し、準拠性監査が、1年より長くない間隔で行うことになっていることを確認する。また、移管、譲渡、合併など、認証局の構成に大規模な変更があった場合は直ちに監査を実施することとなっていることを確認する。					
8.2	監査者の身元・資格 認証局は、認証局業務を直接行っている部門から独立した、適切な能力を有する監査者に定期監査を委託するものとする。	認証局は、認証局業務を直接行っている部門から独立した、適切な能力を有する監査者に定期監査を委託すること。	1) 外部機関の発行した資格証明書、または監査者の所属する組織の長が監査者の能力を証明した書類を閲覧し、監査者が適切な能力を有していることを確認する。 2) 内部監査の場合は組織図の閲覧により、監査者が認証局から独立していることを確認する。					
8.3	監査者と被監査者の関係 監査者は、認証局とは別個の組織に属することによって、被監査者から独立しているものとする。監査者は、被監査者と特別な利害関係を持たないものとする。	監査者は、認証局とは別個の組織に属することによって、被監査者から独立していること。監査者は、被監査者に対しての特別な利害関係を持たないこと。	内部監査の場合は組織図の閲覧により、監査者が認証局から独立していることを確認する。CPS等関連規定により外部監査の場合は認証局と独立しているとみなす。また、認証局代表者の誓約書により利害関係のないことを確認する。					
8.4	監査テーマ 監査は、本CP及び関連するCPSの準拠性をカバーする。	監査は、本CP及び関連するCPSへの準拠性をカバーすること。	CPS等関連規定および監査報告書を閲覧し、本CP及び関連するCPSへの準拠性をカバーすること確認する。					
8.5	監査指摘事項への対応 認証局は、認証局代表者の指示のもと、監査における指摘事項に対する改善措置を実施する。	認証局は、認証局代表者の指示のもと改善指摘事項に関する評価を行い、必要な改善を実施すること。	CPS等関連規定を閲覧し、認証局代表者の指示のもと、監査における指摘事項に対する改善措置を実施することになっていることを確認する。					
8.6	監査結果の通知 監査者によって証明書の信頼性に影響する重大な欠陥が発見された認証局又は登録局は、加入者、検証者及びHPKI認証局専門家会議に直ちに通知するものとする。	(1) 監査者によって証明書の信頼性に影響する重大な欠陥が発見された認証局又は登録局は、HPKI認証局専門家会議に直ちに通知すること。 (2) その場合、認証局は、HPKI認証局専門家会議の意見を参考とし、必要に応じて、加入者及び検証者に通知すること。	CPS等関連規定を閲覧し、監査者によって証明書の信頼性に影響する重大な欠陥が発見された場合は、加入者及び検証者及びHPKI認証局専門家会議に直ちに通知することとなっていることを確認する。					
9	その他の業務上及び法務上の事項							
9.1	料金 各種の料金については、本CPに従い運用される認証局が設定するものとし、本CPでは規定しない。	CPとして監査目標項目なし。						

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
9.1.1	証明書の発行又は更新料 規定しない。	CPとして監査目標項目なし。						
9.1.2	証明書へのアクセス料金 規定しない。	CPとして監査目標項目なし。						
9.1.3	失効又はステータス情報へのアクセス料金 規定しない。	CPとして監査目標項目なし。						
9.1.4	その他のサービスに対する料金 規定しない。	CPとして監査目標項目なし。						
9.1.5	払い戻し指針 規定しない。	CPとして監査目標項目なし。						
9.2	財務上の責任 本CPに従い運用される認証局は、その継続的な運営に必要とされる十分な財務的基盤を維持しなくてはならない。	直近の財務諸表において債務超過に陥っていないこと。	直近の3期分の財務諸表を閲覧し、債務超過に陥っていないことを確認する。					
9.2.1	保険の適用範囲 規定しない。	CPとして監査目標項目なし。	CAの裁量で設定されている場合は特に問題がないか確認する。					
9.2.2	その他の資産 規定しない。	CPとして監査目標項目なし。	CAの裁量で設定されている場合は特に問題がないか確認する。					
9.2.3	エンドエンティティに対する保険又は保証 規定しない。	CPとして監査目標項目なし。	CAの裁量で設定されている場合は特に問題がないか確認する。					
9.3	業務情報の秘密保護							
9.3.1	秘密情報の範囲 本CPに従う認証局が保持する個人及び組織の情報は、証明書、CRL 、各認証局が定めるCPSの一部として明示的に公表されたものを除き、秘密保持対象として扱われる。認証局は、法の定めによる場合及び加入者による事前の承諾を得た場合を除いてこれらの情報を外部に開示しない。 加入者の私有鍵は、その加入者によって秘密保持すべき情報である。認証局では、いかなる場合でもこれらの鍵へのアクセス手段を提供していない。 監査ログに含まれる情報及び監査報告書は、秘密保持対象情報である。認証局は、本CP「8.6 監査結果の通知」に記載されている場合及び法の定めによる場合を除いて、これらの情報を外部へ開示しない。	(1)次の情報は、秘密情報として取り扱われ、法の定めによる場合及び加入者による事前の承諾を得た場合を除いてこれらの情報を外部に開示しないこと。 ①CAが保持する個人及び組織に関する情報 ②監査ログに含まれる情報 ③監査報告書 (2)CAは、いかなる場合でも加入者の私有鍵へのアクセス手段を提供しないこと。	CPS、システム設計書あるいは運用マニュアル等を閲覧し、秘密情報としての取り扱い対象がCPに定められた範囲であり、法の定めによる場合及び加入者による事前の承諾を得た場合を除いてこれらの情報を外部に開示しないこと、および加入者の私有鍵に対し、いかなる場合でもアクセス手段を提供していないことを確認する。					
9.3.2	秘密情報の範囲外の情報 証明書及びCRL に含まれている情報は秘密情報として扱わない。 その他、次の情報も秘密情報として扱わない。 ・ 認証局以外の出所から、秘密保持の制限無しに公知となった情報 ・ 開示に関して加入者によって承認されている情報	次の情報は、秘密情報として扱われていないこと。 (1)証明書及びCRLに含まれている情報 (2)CA以外の出所から、秘密保持の制限なしに公知となった情報 (3)開示に関して加入者によって承認されている情報	CPS、運用マニュアル等を閲覧し、CPの9.3.2に定められた範囲は秘密情報として扱っていないことを確認する。					
9.3.3	秘密情報を保護する責任 認証局は「9.3.1　秘密情報の範囲」で規定された秘密情報を保護するため、内部及び外部からの情報漏洩に係わる脅威に対して合理的な保護対策を実施する責任を負う。 ただし、認証局が保持する秘密情報を、法の定めによる場合及び加入者による事前の承諾を得た場合に開示することがある。その際、その情報を知り得た者は契約あるいは法的な制約によりその情報を第三者に開示することはできない。にもかかわらず、そのような情報が漏洩した場合、その責は漏洩した者が負う。	(1)認証局は「9.3.1　秘密情報の範囲」で規定された秘密情報を保護するため、内部及び外部からの情報漏洩の脅威に対して秘密情報を保護するための保護対策を講じていること。 (2)9.3.1.(2)の場合、第三者にそのような情報が漏洩した場合、当該秘密保持契約において、情報漏洩が発生した場合の責任は漏洩者が負うものとされていること。	(1)CPS、システム設計書あるいは運用マニュアル等を閲覧し、「9.3.1　秘密情報の範囲」で規定された秘密情報を保護するため、内部及び外部からの情報漏洩の脅威に対して秘密情報を保護するための保護対策を講じていることを確認する。 (2)CPS等、秘密保持契約書等を閲覧し、情報漏洩が発生した場合の責任は漏洩者が負うものとされていることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
9.4	個人情報のプライバシー保護							
9.4.1	プライバシーポリシ 認証局における個人情報の取り扱いについては、各認証局のCPSで特定される「プライバシーポリシ」を適用するものとする。	認証局における個人情報の取り扱いはCPSで特定されるプライバシーポリシを適用していること。	CPSおよびプライバシーポリシを閲覧し、認証局における個人情報の取り扱いはCPSで特定されるプライバシーポリシを適用していることを確認する。					
9.4.2	プライバシーとして保護される情報 認証局は、次の情報を保護すべき個人情報として取り扱う。 ・ 登録局が本人確認や各種審査の目的で収集した情報の中で、証明書に含まれない情報。 例えば、身分証明書、自宅住所、連絡先の詳細など、他の情報と容易に照合することができ、それにより特定の個人を識別することが可能な情報を指す。 ・ CRLに含まれない加入者の証明書失効又は停止の理由に関する情報。 ・ その他、認証局が業務遂行上知り得た加入者の個人情報。	次の情報は、保護されるべき個人情報として取り扱われていること。 (1)RAが、本人確認及び各種審査目的で収集した情報の中で、証明書に含まれない情報。（例えば身分証明書、自宅住所、連絡先など） (2)CRLに含まれない加入者の証明書失効又は停止の理由に関する情報 (3)CAが業務上知り得た加入者の個人情報	CPSおよびプライバシーポリシを閲覧し、9.4.2で挙げる項目が個人情報として取り扱われていることを確認する。					
9.4.3	プライバシーとはみなされない情報 次の情報は、秘密情報として扱わない。 ・ 公開鍵証明書 ・ CRLに記載された情報	次の情報は、保護されるべきプライバシー情報として取り扱われていないこと。 (1)公開鍵証明書 (2)CRLに記載された情報	CPS、運用マニュアル等を閲覧し、公開鍵証明書およびCRLに記載された情報がプライバシー情報として扱っていないことを確認する。					
9.4.4	個人情報を保護する責任 認証局は「9.4.2　プライバシーとして保護される情報」で規定された情報を保護するため、内部及び外部からの情報漏洩に係わる脅威に対して合理的な保護対策を実施する責任を負う。	内部及び外部からの情報漏洩の脅威に対して9.4.2に定める情報を保護するため、合理的対策を講じていること。	CPS、システム設計書あるいは運用マニュアル等を閲覧し、9.4.2「プライバシーとして保護される秘密情報」で規定された個人情報を保護するため、内部及び外部からの情報漏洩に係わる脅威に対して個人情報を保護するための合理的対策を講じていることを確認する。					
9.4.5	個人情報の使用に関する個人への通知及び同意 認証局は、証明書発行業務及びその他の認証業務の利用目的に限り個人情報を利用する。それ以外の目的で個人情報を利用する場合は、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。	(1)個人情報の利用目的は次の場合に限るとされていること。 ①証明書発行業務 ②認証業務 (2)当該利用目的を超えて個人情報を利用する場合は、法令で定める場合を除き、あらかじめ本人の同意を得るものとされていること。	CPS、運用マニュアル等を閲覧し、個人情報の利用目的は証明書発行業務および認証業務の場合に限るとされていること、および、当該利用目的を超えて個人情報を利用する場合は、法令で定める場合を除き、あらかじめ本人の同意を得るものとされていることを確認する。					
9.4.6	司法手続又は行政手続に基づく公開 司法機関、行政機関又はその委託を受けたものの決定、命令、勧告等があった場合は、認証局は情報を開示することができる。	CAは、司法機関、行政機関またはその委託を受けたものの決定、命令、勧告等があった場合、情報を開示することができるものとされていること。	CPS、運用マニュアル等を閲覧し、司法機関、行政機関またはその委託を受けたものの決定、命令、勧告等があった場合、情報を開示することができるものとされていることを確認する。					
9.4.7	その他の情報開示条件 個人情報を提供した本人又はその代理人から当該本人に関する情報の開示を求められた場合、認証局で別途定める手続きに従って情報を開示する。この場合、複製にかかる実費、通信費用等については、情報開示を求める者の負担とする。	個人情報を提供した本人又はその代理人からの個人情報の開示手続を定めていること。	CPS、運用マニュアル等を閲覧し、個人情報の開示手続きを定めていることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
9.5	知的財産権 認証局と加入者との間で別段の合意がなされない限り、認証局が提供するサービスに関わる情報資料及びデータは、次に示す当事者の権利に属するものとする。 ・ 加入者証明書：認証局に帰属する財産である ・ 加入者の私有鍵：私有鍵は、その保存方法又は保存媒体の所有者に関わらず、公開鍵と対になる私有鍵を所有する加入者に帰属する財産である ・ 加入者の公開鍵：保存方法又は保存媒体の所有者に関わらず、対になる私有鍵を所有する加入者に帰属する財産である ・ CPS：認証局に帰属する財産（著作権を含む）である ・ 本CP：「HPKI認証局専門家会議」に帰属する財産（著作権を含む）である	次に示すものは、次に示す当事者が権利を有するとされていること。 ①加入者証明書：CA ②加入者の私有鍵：公開鍵と対になる私有鍵を所有する加入者 ③加入者の公開鍵：対になる私有鍵を所有する加入者 ④CPS:CA ⑤本CP：HPKI認証局専門家会議	CPS、運用マニュアル等を閲覧し、CPの9.5の示す権利となっていることを確認する。					
9.6	表明保証							
9.6.1	認証局の表明保証 認証局は、その運営にあたり、本CP及び認証局の定めるCPSに基づいて、加入者及び検証者に対して次の認証局としての責任を果たすものとする。 ・ 提供するサービスと運用のすべてが、本CPの要件と認証局の定めるCPSに従って行われること。 ・ 証明書の発行時に、申請者の申請内容の真偽の確認を確実に行うこと。 ・ 認証局が証明書を発行する時は、証明書に記載されている情報が本CPに従って検証されたことを保証すること。 ・ 公開鍵を含む証明書を加入者に確実に届けること。 ・ 認証局で定める失効ポリシに従って失効事由が生じた場合は、証明書を確実に失効すること。 ・ CRL、ARLなどの重要事項を認証局の定める方法により、速やかに入手できるようにすること。 ・ 認証局の定める方法で、CPに基づく加入者の権利と義務を各加入者に通知すること。 ・ 鍵の危殆化のおそれ、証明書又は鍵の更新、サービスの取り消し、及び紛争解決をするための手続きを加入者に通知すること。 ・ 本CP「5　建物・関連施設、運用のセキュリティ」及び「6　技術的なセキュリティ管理」に従い認証局を運営し、私有鍵の危殆化を生じさせないこと。 ・ CA私有鍵が、証明書及び証明書失効リストに署名するためだけに使用されることを保証すること。 ・ 申請者の申請内容の真偽の確認において利用した書類を含む、各種の書類の滅失、改ざんを防止し、10年間保管すること。 ・ 認証局の発行する証明書の中で、加入者に対して、加入者の名称（subjectDN）の一意性を検証可能にしておくこと。	(1)サービスの提供と運用が、本CP及びCPSに従って行われていること。 (2)証明書発行時に、申請者の申請内容の真偽の確認を確実に行っていること。 (3)証明書発行時、証明書記載の情報が本CPに従って検証されたことを保証していること。 (4)公開鍵を含む証明書が加入者に確実に届けられていること。 (5)失効ポリシに従って失効事由が生じた場合、証明書が確実に失効されていること。 (6)CRL,ARLなどを速やかに入手できるようにされていること。 (7)加入者の本CPに基づく権利と義務が、各加入者に通知されていること。 (8)鍵の危殆化のおそれ、証明書又は鍵の更新、サービスの取消し、紛争解決手続が、加入者に通知されている。 (9)本CP「5　建物及び関連施設、運用のセキュリティ」及び「6　技術的セキュリティ管理」に従いCAが運営され、私有鍵の危殆化を生じさせていないこと。 (10)CA私有鍵が、証明書及び証明書失効リストに署名するためだけに使用されることが保証されていること。 (11)各書類は、改ざん及び滅失が防止され、10年間保存されていること。 (12)証明書のなかで加入者の名称(subjectDN)の一意性が検証可能になっていること。	CPS、運用マニュアル等を閲覧し、CPの9.6.1で示す事項を認証局の責任として果たしていることを確認する。				

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
9.6.2	登録局の表明保証 登録局は、認証局から独立して登録局を運営する場合、加入者、検証者、認証局に対して次の責任を果たすものとする。また、登録局は、認証局に代わって果たす行為について個別に責任を負う。 ・ 証明書発行にあたり、申請内容の真偽の確認を確実に行い、確認の結果を認証局に対して保証すること。 ・ 認証局の発行する証明書の中で、加入者に対して加入者の名称（subjectDN）の一意性を検証可能にしておくこと。 ・ 証明書申請情報を認証局に安全に送付し、登録記録を安全に保管すること。 ・ 証明書失効申請を行う場合は、本CP「4.9.3　失効申請の処理手順」に従って失効申請を開始すること。 ・ 将来の検証のため、また証明書がどのように、何故生成されたかを管理可能なように、証明書の作成要求又は失効要求などのイベントを、認証局に移管した場合を除き、証明書の有効期間満了後10年間保管すること。	(1)証明書発行にあたり、加入者の申請内容の真偽の確認を確実に行っていること。 (2)当該確認の結果をCAに対して保証していること。 (3)CAの発行する証明書のなかで、加入者に対して加入者の名称(subjectDN)の一意性が検証可能になっていること。 (4)証明書申請情報をCAに対し安全に送付していること。 (5)登録記録を安全に保管していること。 (6)証明書失効申請は、本CP4.9.3に従って行われていること。 (7)証明書の作成要求又は失効要求などは、証明書の有効期間満了後10年間保管されていること。	CPS、運用マニュアル等を閲覧し、CPの9.6.2で示す事項を認証局の責任として果たしていることを確認する。					
9.6.3	加入者の表明保証 本CPに則り運営される認証局の加入者は、認証局に対して次の責任を果たすものとする。 1. 証明書発行申請内容に対する責任 証明書発行申請を行う場合、認証局に提示する申請内容が虚偽なく正確であることに対する責任を果たすこと。 2. 証明書記載事項の担保責任 証明書の記載内容について証明書の受領時に確認を行い、申請内容と相違ないかを確認すること。また、記載内容について現状との乖離が発生した場合には、速やかに当該証明書の失効手続きを行うこと。 3. 鍵などの管理責任 私有鍵を保護し、紛失、暴露、改ざん、又は盗用されることを防止するために妥当な措置を取ること。 4. 各種の届出に対する責任 私有鍵の紛失、暴露、その他の危殆化、又はそれらが疑われる時には、認証局の定めるCPSに従って速やかに届け出ること。また、証明書情報に変更があった場合は、認証局の定めるCPSに従って速やかに届け出ること。 5. 利用規定の遵守責任 加入者は、本CP及び認証局で加入者に対して開示される文章を読み、その利用規定及び禁止規定を遵守すること。	認証局は加入者が9.6.3で定める以下の責任を果たすような措置をとること。例えば証明書申請時に提出する加入契約書で確約させる等の方法がある。 (1)加入者による証明書発行申請内容には、虚偽がなく正確であること。 (2)加入者は証明書の受領時に、証明書の記載内容が申請内容と相違ないことを確認していること。 (3)証明書の記載内容が現状と乖離している場合、加入者は速やかに当該証明書の失効手続を行うこと。 (4)加入者は、私有鍵の盗難紛失等を防止するための妥当な措置をとっていること。 (5)加入者は、私有鍵の紛失、危殆化等、またはそれらが疑われるときは、CPSに従い速やかに届け出ること。 (6)加入者は、証明書情報に変更があった場合、CPSに従って速やかに届け出ること。 (7)加入者は、本CP、及びCAにて加入者に対して開示される文章を読み、その利用規定及び禁止規定を遵守すること。	CPS、運用マニュアル、加入者申請書等を閲覧し、CPの9.6.3で示す事項について加入者が了解し、自らの責任として履行することができるよう規定されていることを確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
9.6.4	検証者の表明保証 本CPに則り運営される認証局の検証者は以下の責任を果たすものとする。 1. 利用規定の遵守責任 検証者は、本CP及び認証局で検証者に対して開示される文章を読み、その利用規定及び禁止規定を遵守すること。また、証明書の利用に際しては信頼点の管理を確実に行うこと。 2. 証明書記載事項の確認責任 検証者は、証明書を利用する際に、その有効性を確認する責任がある。有効性の確認には、以下の事項が含まれる。 ・ 証明書の署名が正しいこと ・ 証明書の有効期限が切れていないこと ・ 証明書が失効していないこと ・ 証明書の記載事項が、本CP「7　証明書及び失効リスト及びOCSPのプロファイル」に記述されているプロファイルと合致していること。特に、次の2点の検証を実施することはHPKI署名用証明書として重要である。 – OID及びIssuerのCNがHPKIの規定に一致していること – hcRole及びkeyUsageのnonRepudiationのみが立てられていること	認証局は検証者が9.6.4で定める以下の事項につき以下の責任を果たせるように措置をとること。例えば認証局のポータルサイトに掲示をするとか、加入者の証明書申請時に使用時は検証者に9.6.4の責任を果たしているかの確認あるいは注意を促す必要があることを了解させるなどの措置が考えられる。 (1)検証者は、本CP、及びCAにて検証者に対して開示される文章を読んでいる。 (2)検証者は、それらに関する利用規定及び禁止規定を遵守している。 (3)検証者は、証明書を利用する際、次の諸点に関する証明書の有効性を確認している。 ①証明書の署名が正しいこと ②証明書の有効期限が経過していないこと ③証明書が失効していないこと ④証明書の記載事項が本CP7に記述されているプロファイルと合致していること（とくに、OID及びIssuerのCNがHPKIの規定に一致していること、hcRole及びkeyUsageのnonRepudiationのみが立てられていること）	CPS、運用マニュアル等を閲覧し、CPの9.6.4で示す事項を検証者の責任として果たすための措置をしていることを確認する。					
9.6.5	他の関係者の表明保証 規定しない。	CPとして監査目標項目なし。	CAの裁量で設定されている場合は特に問題がないか確認する。					
9.7	無保証 認証局は、本CP「9.6.1　認証局の表明保証」及び「9.6.2　登録局の表明保証」に規定する保証に関連して発生するいかなる間接損害、特別損害、付随的損害又は派生的損害に対する責任を負わず、いかなる逸失利益、データの紛失又はその他の間接的若しくは派生的損害に対する責任を負わない。 また、本CP「9.16.5　不可抗力」で規定される不可抗力によるサービス停止によって加入者、若しくはその他の第三者において損害が生じた場合、認証局は一切の責任を負わない。	本CPの規定と矛盾がないこと。	CPS、運用マニュアル等を閲覧し、本CPの規定と矛盾がないことを確認する。					
9.8	責任制限 認証局は、加入者において電子証明書の利用又は私有鍵の管理その他加入者が注意すべき事項の運用が不適切であったために生じた損害に対して責任を負わない。 また、認証局及び登録局の責任は、認証局及び登録局の怠慢行為によりCP、CPSに定められた運用を行わなかった場合に限定する。 なお、本CP「9.6　表明保証」に関し、次の場合、認証局は責任を負わない。 （以下省略）	本CPの規定と矛盾がないこと。	CPS、運用マニュアル等を閲覧し、本CPの規定と矛盾がないことを確認する。					

準拠性監査報告書様式（署名用）

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
9.9	補償 本CPに規定された責任を果たさなかったことに起因して、認証局がサービスの加入者に対して損害を与えた場合、認証局で定める金額を上限として損害を賠償する。 ただし、認証局側の責に帰さない事由から発生した損害、逸失利益、間接損害、又は予見の有無を問わず、特別損害については、いかなる場合でも一切の責任を負わない。 また、加入者は認証局が発行する証明書を申請した時点で、検証者は信頼した時点で、認証局及び関連する組織等に対する損害賠償責任が発生する。	補償に関していは最低限以下の条件を包含すること。これを上回る補償条件を設定することを妨げるものではない。 (1)本CPに規定された責任を果たさなかったことに起因して、CAがサービスの加入者に対して損害を与えた場合、CAで定める金額を上限として損害を賠償する。 (2)CAの責に帰さない事由から発生した損害、逸失利益、間接損害、特別損害については、責任を負わない。 (3)加入者がCAに対して証明書を申請した時点、検証者が信頼した時点で、CA及び関連する組織の損害賠償責任が発生する。	CPS、運用マニュアル等を閲覧し補償金額が定められ、9.9で定められた補償条件が確保されていることを確認する。 CAの裁量で標準ポリシを上回る条件が設定されている場合は問題がないか確認する。					
9.10	本ポリシの有効期間と終了							
9.10.1	有効期間 本CPは、作成された後、「HPKI認証局専門家会議」により審査、承認されることにより有効になる。また、「9.10.2 終了」で記述する本CPの終了まで有効であるものとする。	本CPは、HPKI認証局専門家会議により審査、承認されたときに、有効とすること。 また、「9.10.2 終了」で記述する本CPの終了まで有効であるものとすること。	CPS、運用マニュアル等を閲覧し、有効期間がHPKI認証局専門家会議により審査、承認されたときに、有効とされ、「9.10.2 終了」で記述する本CPの終了まで有効であるとしていることを確認する。					
9.10.2	終了 本CPは、「9.10.3 終了の影響と存続条項」で規定する存続条項を除き、「HPKI認証局専門家会議」が無効と宣言した時点又は「HPKI認証局専門家会議」が機能を果たさなくなった場合、無効になる。	CPは以下の場合無効となるものとすること。 (1)本CPは、HPKI認証局専門家会議が無効と宣言した時点、または、HPKI認証局専門家会議が機能を果たさなくなった場合、無効となる。但し、9.10.3の場合を除く。 (2)無効とされた本CPの部分に対応するCPSの規定も、無効となる。	CPS、運用マニュアル等を閲覧し、9.10.2で定める条件を無効の条件としていることを確認する。					
9.10.3	終了の影響と存続条項 文書が終了した場合であっても、「9.3　業務情報の秘密保護」、「9.4　個人情報のプライバシー保護」、「9.5　知的財産権」に関する責務は存続するものとする。また、「HPKI認証局専門家会議」において部分的な存続を定めた場合は、当該存続部分は有効なものとする。	本CPが無効となった後も、9.3,9.4,9.5に関する責務、及び、HPKI認証局専門家会議が部分的な存続を認めた部分は、有効とすること。	CPS、運用マニュアル等を閲覧し、9.10.3で定める条項を最低限の存続条項としていることを確認する。					
9.11	関係者間の個々の通知と連絡 認証局から加入者への通知方法は、別項で特に定めるものを除き、電子メール、ホームページへの掲載、郵送による書面通知など認証局が適当と判断した方法により行うものとする。また、認証局から加入者の届け出た住所、FAX番号又は電子メールアドレスに宛てて加入者への通知を発した場合には、当該通知が延着又は不着となった場合であっても、通常到達すべき時に到達したものとみなす。	(1)CAから加入者への通知は、電子メール、HPへの掲載、郵送による書面通知など認証局が適当と判断された方法により行われていること。 (2)CAから加入者の届け出た住所、FAX番号、電子メールアドレスにあてて加入者への通知を発した場合には、当該通知が延着又は不着となった場合でも、通常到達すべき時に到達したものとみなすこと。 ただし、CAの裁量で加入者に有利なように条件を配慮することを妨げるものではない。	CPS、運用マニュアル等を閲覧し、認証局が適当と判断した方法により通知が行われていること、また、通常の到達すべき時を延着時や付着時の時刻としていることを確認する。 ただし、CAの裁量で加入者に有利なように設定されている場合は特に問題ないか確認する。					
9.12	改訂							
9.12.1	改訂手続き 「HPKI認証局専門家会議」が本CPの改訂を行う場合は、改訂に先立ち、本CPに関連する全ての認証局に通知を行い、意見を求める。 本CPが変更された時は、「HPKI認証局専門家会議」によって承認する。	CPとして監査目標項目なし。	CPS、運用マニュアル等を閲覧し、改訂手続きの記載がある場合は問題ないか確認する。					

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
9.12.2	通知方法と期間 本CPが改訂された場合、情報公開用Webサイト等を通じて、全ての加入者、関連する認証局及び検証者に速やかに公開する。公開の期間については、次のように定める。 ・ 重要な変更は、通知後90日を上限として、通知に定められた告知期間を経て効力を生ずる。なお、通知後、上記で示した方法に従い通知を行うことにより、変更を中止することもあり得る。但し、監査指摘事項などによる緊急を要する重要な変更は、通知後、直ちに、効力を生ずる。 ・ 重要でない変更は、通知後直ちに効力を生ずる。	(1)CPS,運用マニュアル等が改訂された場合、情報公開用Webサイト等を通じて、全ての加入者、関連する認証局、検証者に速やかに(2)(3)に規定する公開期間に従って公開するすることによって通知すること。 (2)重要な変更は、通知後９０日を上限として、通知に定められた告知期間を経て効力を生ずる。 (3)監査指摘事項などによる緊急を要する重要な変更、及び、重要でない変更は、通知後直ちに効力を生ずる。	CPS、運用マニュアル等を閲覧し、CPが改訂された場合の通知方法と公開期間が9.12.2に従って行われることを確認する。					
9.12.3	オブジェクト識別子（OID）の変更理由 本CPの変更があった場合には、本CPのバージョン番号を更新する。 また、次の場合には、OIDを変更する。 ・ 証明書又はCRLのプロファイルが変更されたとき ・ セキュリティ上重要な変更がされたとき ・ 本人性、国家資格の確認方法の厳密さに重要な影響を及ぼす変更がされたとき	以下の事由の場合にバージョン番号あるいはOIDが変更されることを了解し、対応すること。 (1)本CPの変更があった場合には、本CPのバージョン番号を更新する。 (2)次の場合、OIDを変更する。 ①証明書又はCRLのプロファイルが変更されたとき ②セキュリティ上重要な変更がされたとき ③本人性、国家資格の確認方法の厳密さに重要な影響を及ぼす変更がされたとき	CPS、運用マニュアル等を閲覧し、9.12.3の事由の場合にバージョン番号あるいはOIDが変更されることを了解し、対応することを確認すること。					
9.13	紛争解決手続 証明書の発行主体である、各認証局のCPSにおいて定める。	CPSにおいて紛争解決が定められていること、その場合、法令に準拠していること。	CPS、運用マニュアル等を閲覧し紛争解決手段が定められ、法令に準拠していることを確認する。					
9.14	準拠法 本CPは、「電子署名及び認証業務に関する法律」、「個人情報の保護に関する法律」及び関連する日本国内法規に準拠している。	本項はCPの準拠法を述べているだけなので特に監査目標は設定しない。	CPS、運用マニュアル等を閲覧し、なんらかの根拠法が設定されている場合は日本国内法が適用されているか確認する。					
9.15	適用法の遵守 本CPの運用にあたっては、日本国内法及び公的通知等がある場合はそれを優先する。	日本国内法の強行法規及び公的通知等は、本CP及びCPSより優先適用されていること。	CPS、運用マニュアル等を閲覧し、日本国内法の強行法規及び公的通知等が、CP及びCPSより優先適用されていることを確認する。					
9.16	雑則							
9.16.1	完全合意条項 本CPは、本CPに定められたサービスに対して当事者間の完全合意を構成し、認証業務について記述された書面又は口頭による過去の一切の意思表示、合意又は表明事項に取って代わるものである。	本CPに定められたサービスに対して当事者間の完全合意を構成し、認証業務について記述された書面又は口頭による過去の一切の意思表示、合意、表明事項にとって代わるものとすること。	CPS、運用マニュアル等を閲覧し、CPが過去の一切の意思表示、合意又は表明事項に取って代わるものとしていることを確認する。					
9.16.2	権利譲渡条項 関係者は、本CPに定める権利義務を担保に供することができない。また、次の場合を除き、第三者に譲渡することができない。 ・ 認証局が登録局に本CPに定める業務の委託を行うとき ・ 本CPに則った認証局の移管又は譲渡を行うとき	(1)関係者は、本CPに定める権利義務を担保に供することができないとされていること。 (2)関係者は、本CPに定める権利を第三者に譲渡することができない。但し ①CAがRAに本CPに定める業務の委託を行うとき、及び ②本CPに則ったCAの移管又は譲渡を行うときは、この限りでないとされていること。	CPS、運用マニュアル等を閲覧し、権利譲渡条項が9.16.2で定める条項を満たしていることを確認する。					
9.16.3	分離条項 本CPのひとつ又は複数の条項が司法の判断により、無効であると解釈された場合であっても、その他の条項の有効性には影響を与えない。無効と判断された条項は、法令の範囲内で当事者の合理的な意思を反映した規定に読み替える。	(1)本CPのひとつ又は複数の条項が、司法判断により無効であると解釈された場合であっても、その他の条項の有効性には影響を与えないとされていること。 (2)司法判断により無効と判断された条項は、法令の範囲内で当事者の合理的意思を反映した規定に読み替えることとされていること。	CPS、運用マニュアル等を閲覧し、司法判断に対する措置が9.16.3を満足していることを確認する。					
9.16.4	強制執行条項（弁護士費用及び権利放棄） 規定しない。	本CPでは規定されないので監査目標は設定しない。	CAの裁量で設定されている場合は特に問題がないか確認する。					

準拠性監査報告書様式（署名用）

証明書ポリシ		監査目標	監査手順例	措置状況	対応CPS番号および/または書類名	監査エビデンス（具体的な確認事項／方法）	CA監査者評価およびコメント	専門家会議評価およびコメント
9.16.5	不可抗力 以下に例示されるような通常人の標準的な注意義務を尽くしても、予防・回避できない事象を不可抗力とする。不可抗力によって損害が発生した場合、本CP「9.7 無保証」の規定により認証局は免責される。 （以下省略）	(1)次の事象が不可抗力とされていること。 ①火災、雷、洪水、地震、台風、有害物質による汚染など ②暴動、戦争など ③裁判所、行政府、地方機関による行為または判断 ④ストライキ、労働争議、工場閉鎖 ⑤CAの責めによらない事由により、本CPに基づく義務の遂行上必要とする必須の機器、物品、供給物もしくはサービスが利用不能となった場合。 (2)不可抗力によって損害が発生した場合、本CP9.7の規定により、CAは免責されるとされていること。 ただし、CAの裁量で責任を負うことを妨げるものではない。	CPS、運用マニュアル等を閲覧し、不可抗力の事象および免責条項が9.16.5を満足していることを確認する。、CAの裁量でなんらかの責任が設定されている場合は特に問題がないか確認する。					
9.17	その他の条項 本CPを採用した認証局又は登録局が別の組織と合併若しくは別の組織に移管、譲渡する場合、新しい組織は本CPの方針に同意し責任を持ち続けるものとする。	本CPを採用したCAもしくはRAが、別の組織と合併、または別の組織に移管、譲渡する場合、新しい組織は本CPの方針に同意し、責任を持ち続けているものとすること。	CPS、運用マニュアル等を閲覧し、認証局が別の組織と合併、または別の組織に移管、譲渡する場合、新しい組織はCPの方針に同意し、責任を持ちつづけているものとされていることを確認する。					